管理访问

本章介绍如何通过 Telnet、SSH 和 HTTPS（使用 ASDM）访问 ASA 进行系统管理，如何对用户进行身份验证和授权以及如何创建登录横幅。

配置管理远程访问

本节介绍如何为 ASDM、Telnet 或 SSH 配置 ASA 访问，以及其他管理参数，例如登录横幅。

配置 SSH 访问

如要确定客户端 IP 地址并定义允许使用 SSH 连接至 ASA 的用户，请执行以下步骤：请参阅以下准则：

- 要访问 ASA 接口以进行 SSH 访问，亦无需允许主机 IP 地址的访问规则。您只需按照本部分配置 SSH。
- 除了进入 ASA 时所经由的接口以外，不支持对其他接口进行 SSH 访问。例如，如果 SSH 主机位于外部接口上，则只能直接向外部接口发起管理连接。此规则的唯一例外是通过VPN连接。请参阅配置 VPN 隧道上的管理访问，第 12 页。
- ASA 允许每个情景/单模式最多有 5 个并发 SSH 连接，在所有情景中最多分为 100 个连接。但是，由于配置命令可能会锁定正在更改的资源，因此您应一次在一个SSH会话中进行更改，以确保正确应用所有更改。
- 默认情况下，ASA使用专有SSH堆栈。您可以改为启用基于OpenSSH的CiscoSSH堆栈。默认堆栈继续为ASA堆栈。思科SSH支持：
  - FIPS 合规性
  - 定期更新，包括来自思科和开源社区的更新

请注意，思科SSH堆栈不支持：

- 通过VPN通过SSH连接到其他接口（管理访问）
- EDDSA密钥对
- FIPS模式下的RSA密钥对

如果需要这些功能，应继续使用ASA SSH堆栈。

CiscoSSH 堆栈的 SCP 功能略有变化：要使用 ASA **copy** 命令将文件复制到 SCP 服务器或从 SCP 服务器复制文件，您必须使用 **ssh** 命令在 ASA 上为 SCP 服务器子网/主机启用 SSH 访问。

- （8.4 及更高版本）不再支持 SSH 默认用户名。使用 SSH 以及 **pix** 或 **asa** 用户名和登录密码无法再连接至 ASA。要使用 SSH，您必须使用 **aaa authenticationsshconsoleLOCAL** 命令配置 AAA 身份验证；然后通过输入 **username** 命令定义本地用户。如果要使用 AAA 服务器而不是本地数据库进行身份验证，建议也将本地身份验证配置为备用方法。
- 仅支持 SSH 版本 2。

开始之前

- 在多情景模式下，请在情景执行空间中完成本程序。要从系统配置切换至情景配置，请输入 **changeto context** *name*。

过程

步骤 1 （可选） 使用CiscoSSH堆栈而不是默认ASA SSH堆栈。

ssh stack ciscossh

要返回到ASA SSH堆栈，请使用。**no ssh stack ciscossh**

步骤 2 生成 SSH 必需的密钥对（仅适用于物理 ASA）。

对于 ASA 虚拟，会在部署后自动创建密钥对。ASA 虚拟 仅支持 RSA 密钥。

a) 生成密钥对。

crypto key generate {**eddsa edwards-curve ed25519** | **ecdsa elliptic-curve** *size* |**rsa modulus** *size*}

示例：

```
ciscoasa(config)# crypto key generate ecdsa elliptic-curve 521
```

- **eddsa edwards-curve ed25519**-密钥大小为256位。 不支持CiscoSSH堆栈。
- size-以位为单位的大小为256、384或521。**ecdsa elliptic-curve**
- size-大小（以位为单位）为2048、3072或4096。**rsa modulus** 更高版本中将会删除对 RAS 密钥的支持，因此我们建议改为使用其他支持的密钥类型。

指定的密钥大小越大，生成密钥对所需的时间就越长。SSH按以下顺序尝试密钥：EdDSA，ECDSA，然后是RSA。使用{|||}命令。**show crypto key mypubkeyeddsaecdsarsa** SSH使用的密钥称为<Default- type -Key>。

b) （可选） 如果您不想使用默认密钥顺序（EdDSA，ECDSA和RSA），请确定要使用的密钥对。

ssh key-exchange hostkey {**rsa** | **eddsa** | **ecdsa**}

如果选择RSA，则必须使用2048或更大的密钥。为了实现升级兼容性，仅在使用默认密钥顺序时才支持较小的密钥。更高版本中将会删除对 RAS 密钥的支持，因此我们建议改为使用其他支持的密钥类型。

示例：

```
ciscoasa(config)# ssh key-exchange hostkey ecdsa
```

步骤 3 将密钥保存到永久性闪存中。

write memory

示例：

```
ciscoasa(config)# write memory
```

步骤 4 在本地数据库中创建可用于 SSH 访问的用户。您也可以使用 AAA 服务器进行用户访问，但建议使用本地用户名。

username *name* [**password** *password*] **privilege** *level*

示例：

```
ciscoasa(config)# username admin password Far$cape1999 privilege 15
```

默认情况下，特权级别为 2；输入介于 0 和 15 之间的级别，其中 15 具有所有特权。如果要强制用户使用公共密钥身份验证而不是密码身份验证 (**ssh authentication**)，您可能需要不使用密码创建用户。若您在 **username** 命令中配置公钥身份验证以及密码，则如果您在此程序中明确配置 AAA 身份验证，用户可使用任一种方法登录。**注意：**请勿使用 **username** 命令 **nopassword** 选项，；**nopassword** 选项允许输入任何密码，而不是无密码。

步骤 5 （可选） 允许用户使用公钥身份验证代替/以及密码身份验证，并在 ASA 上输入公钥：

username 名称 **attributes**

ssh authentication {**pkf** | **publickey** *key*}

示例：

```
ciscoasa(config)# username admin attributes
ciscoasa(config-username)# ssh authentication pkf

Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "256-bit ED25519, converted by dean@dwinchester-mac from "
```

```
AAAAC3NzaC1lZDI1NTE5AAAAIDmIeTNfEOnuH0094p1MKX80fW2O216g4trnf7gwWe5Q
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
```

对于本地 **username**，您可以启用公钥身份验证代替/以及密码身份验证。您可以使用任何可生成 ssh-rsa、ecdsa-sha2-nistp 或 ssh-ed25519 原始密钥（不带证书）的 SSH 密钥生成软件（如 ssh keygen）生成公钥/私钥对。在 ASA 上输入该公钥。然后，SSH 客户端使用私钥（以及用于创建密钥对的口令）连接至 ASA。

对于 **pkf** 密钥，系统将提示您粘贴 PKF 格式的密钥，最长 4096 位。此格式用于由于过长而无法以 Base64 格式内嵌粘贴的密钥。例如，可以使用 ssh keygen 生成 4096 位的密钥，然后将其转换为 PKF，并使用 **pkf** 关键字作为密钥提示。**注意**：您可以将 **pkf** 选项与故障转移一起使用，但 PKF 密钥不会自动复制到备用系统。您必须输入 **write standby** 命令才能同步 PKF 密钥。

对于密钥，密钥是Base64编码的公钥。**publickey** 您可以使用任何可生成 ssh-rsa、ecdsa-sha2-nistp 或 ssh-ed25519 原始密钥（不带证书）的 SSH 密钥生成软件（如 ssh keygen）生成密钥对。

步骤 6 （对于密码访问）启用 SSH 访问的本地（或 AAA 服务器)身份验证：

aaa authentication ssh console {**LOCAL** | *server_group* [**LOCAL**]}

示例：

```
ciscoasa(config)# aaa authentication ssh console LOCAL
```

对于使用 **ssh authentication** 命令的用户名，此命令不影响本地公钥身份验证。ASA 隐式地使用本地数据库进行公钥身份验证。此命令仅影响具有密码的用户名。如果要允许本地用户使用公钥认证或密码，则需要使用此命令显式地配置本地身份验证以允许密码访问。

步骤 7 确定 ASA 从其接受每个地址或子网的连接的 IP 地址，以及可在其上使用 SSH 的接口。

ssh *source_IP_address mask source_interface*

- *source_interface* - 指定任何已命名的接口。对于网桥组，请指定网桥组成员接口。对于仅 VPN 管理访问（请参阅 配置 VPN 隧道上的管理访问，第 12 页），请指定命名的 BVI 接口。

与 Telnet 不同，您可以在最低安全级别的接口上使用 SSH。

示例：

```
ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside
```

步骤 8 （可选） 设置在 ASA 断开 SSH 会话之前，会话可空闲的持续时间。

ssh timeout 分钟

示例：

```
ciscoasa(config)# ssh timeout 30
```

设置超时时间，范围为 1 到 60 分钟。默认值为 5 分钟。在大多数情况下，默认持续时间都太短，应增加为直到完成所有前期测试和故障排除所需的时间。

步骤 9 （可选） 配置 SSH 密码加密算法：

ssh cipher encryption {**all** | **fips** | **high** | **low** | **medium** | **custom** *colon-delimited_list_of_encryption_ciphers*}

示例：

```
ciscoasa(config)# ssh cipher encryption custom 3des-cbc:aes128-cbc:aes192-cbc
```

默认值为 **medium**。密码按其列出的顺序使用。对于预定义列表，从最高安全级别到最低安全级别列出。

- **all** 关键字指定使用所有密码：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr chacha20-poly1305@openssh.com aes192-ctr aes256-ctr
- **custom** 关键字指定自定义密码加密配置字符串，以冒号分隔。
- **fips** 关键字指定仅符合 FIPS 的密码：aes128-cbc aes256-cbc
- **high** 关键字指定仅高强度密码：aes256-cbc chacha20-poly1305@openssh.com aes256-ctr
- **low** 关键字指定低、中和高强度密码：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr
- **medium** 关键字指定中和高强度密码（默认设置）：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr

步骤 10 （可选） 配置 SSH 密码完整性算法：

{|||||||||冒号分隔的list_of_integrity_ciphers} **ssh cipher integrityallfipshighlowmediumcustom**

示例：

```
ciscoasa(config)# ssh cipher integrity custom hmac-sha1-96:hmac-md5
```

默认值为 **high**。

- **all** 关键字指定使用所有密码：hmac-sha1 hmac-sha1-96 hmac-sha2-256 hmac-md5 hmac-md5-96
- **custom** 关键字指定自定义密码加密配置字符串，以冒号分隔。
- **fips** 关键字指定仅符合 FIPS 的密码：hmac-sha1 hmac-sha2-256
- **high** 关键字指定仅高 强度密码： hmac-sha2-256
- **low** 关键字指定低、中和高强度密码：hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96 hmac-sha2-256
- **medium** 关键字指定中和高强度密码：hmac-sha1 hmac-sha1-96 hmac-sha2-256

步骤 11 （可选） (Admin context only) - 设置 Diffie-Hellman (DH) 密钥交换模式：

{| | | | | | | } **ssh key-exchange groupcurve25519-sha256dh-group1-sha1dh-group14-sha1dh-group14-sha256ecdh-sha2-nistp256**

示例：

```
ciscoasa(config)# ssh key-exchange group dh-group14-sha1
```

默认为 **dh-group14-sha256**

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。您只能在管理情景中设置密钥交换；此值供所有情景使用。

示例

以下示例展示如何使用 PKF 格式的密钥进行身份验证：

```
ciscoasa(config)# crypto key generate eddsa edwards-curve ed25519
ciscoasa(config)# write memory
ciscoasa(config)# username dean password examplepassword1 privilege 15
ciscoasa(config)# username dean attributes
ciscoasa(config-username)# ssh authentication pkf
Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "256-bit ED25519, converted by dean@dwinchester-mac from "
AAAAC3NzaC1lZDI1NTE5AAAAIDmIeTNfEOnuH0094p1MKX80fW2O216g4trnf7gwWe5Q
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config)#
```

以下示例将在 Linux 或 Macintosh 系统上为 SSH 生成一个共享密钥，并将其导入 ASA：

1. 在计算机上生成 的 EdDSA 公钥和私钥：

```
dwinchester-mac:~ dean$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/Users/dean/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase): key-pa$$phrase
Enter same passphrase again: key-pa$$phrase
Your identification has been saved in /Users/dean/.ssh/id_ed25519.
Your public key has been saved in /Users/dean/.ssh/id_ed25519.pub.
The key fingerprint is:
SHA256:ZHOjfJa3DpZG+qPAp9A5PyCEY0+Vzo2rkGHJpplpw8Q dean@dwinchester-mac

The key's randomart image is:
+--[ED25519 256]--+
|       .         |
|      o          |
|.  . + o+ o      |
|.E+ o ++.+ o     |
|B=.=   .S = .    |
|**  ooo. = o .   |
|.....o*.o = .    |
```

```
|  o .. *.+.o     |
|   .  . oo...    |
+----[SHA256]-----+
dwinchester-mac:~ dean$
```

2. 将密钥转换为 PKF 格式：

```
dwinchester-mac:~ dean$ cd .ssh
dwinchester-mac:.ssh dean$ ssh-keygen -e -f id_ed25519.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "256-bit ED25519, converted by dean@dwinchester-mac from "
AAAAC3NzaC1lZDI1NTE5AAAAIDmIeTNfEOnuH0094p1MKX80fW2O216g4trnf7gwWe5Q
---- END SSH2 PUBLIC KEY ----
dwinchester-mac:.ssh dean$
```

3. 将密钥复制到剪贴板。
4. 在 ASDM 中，依次选择 **配置** > **设备管理** > **用户/AAA** > **用户帐户**，选择用户名，然后点击**编辑**。点击 **Public Key Using PKF** 并将密钥粘贴到窗口中：
5. 验证用户是否可以通过 SSH 连接到 ASA。对于密码，请输入您在创建密钥对时指定的 SSH 密钥密码。

```
dwinchester-mac:.ssh dean$ ssh dean@10.89.5.26
The authenticity of host '10.89.5.26 (10.89.5.26)' can't be established.
ED25519 key fingerprint is SHA256:6d1g2fe2Ovnh0GHJ5aag7GxZ68h6TD6txDy2vEwIeYE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.89.5.26' (ED25519) to the list of known hosts.
dean@10.89.5.26's password: key-pa$$phrase
User dean logged in to asa
Logins over the last 5 days: 2.  Last login: 18:18:13 UTC Jan 20 2021 from 10.19.41.227
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
asa>
```

配置 Telnet 访问

要识别允许使用 Telnet 连接至 ASA 的客户端 IP 地址，请执行以下步骤。请参阅以下准则：

- 如要访问 ASA 接口进行 Telnet 访问，也不需要允许主机 IP 地址的访问规则，您只需根据本部分配置 Telnet 访问。
- 除了进入 ASA 时所经由的接口以外，不支持对其他接口进行 Telnet 访问。例如，如果 Telnet 主机位于外部接口上，则只能发起直接到外部接口的 Telnet 连接。此规则的唯一例外是通过 VPN 连接。请参阅配置 VPN 隧道上的管理访问，第 12 页。
- 除非使用 VPN 隧道中的 Telnet，否则无法使用 Telnet 访问最低安全级别的接口。
- 每个情景/单模式最多 5 个并发 Telnet 连接，在所有情景中最多分为 100 个连接。

开始之前

- 在多情景模式下，请在情景执行空间中完成本程序。要从系统配置切换至情景配置，请输入 **changeto context** *name*。
- 要使用 Telnet 访问 ASA CLI，请输入通过 **password** 命令设置的登录密码。使用 Telnet 前必须手动设置该密码。

过程

步骤 1 识别 ASA 为位于特定接口的每个地址或子网接收连接的 IP 地址。

telnet *source_IP_address mask source_interface*

- *source_interface* - 指定任何已命名的接口。对于网桥组，请指定网桥组成员接口。对于仅 VPN 管理访问（请参阅 配置 VPN 隧道上的管理访问，第 12 页），请指定命名的 BVI 接口。

如果只有一个接口，只要接口的安全级别为 100，您就可以配置 Telnet 以访问该接口。

示例：

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

步骤 2 设置 ASA 与 Telnet 会话断开连接之前，该会话可以持续空闲多长时间。

telnet timeout 分钟

示例：

```
ciscoasa(config)#  telnet timeout 30
```

设置超时时间，范围为 1 到 1440 分钟。默认值为 5 分钟。在大多数情况下，默认持续时间都太短，应增加为直到完成所有前期测试和故障排除所需的时间。

示例

下列显示如何让一台内部接口上的地址为 192.168.1.2 的主机访问 ASA：

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

下例显示如何允许 192.168.3.0 网络上的所有用户在内部接口上访问 ASA：

```
ciscoasa(config)# telnet 192.168.3.0. 255.255.255.255 inside
```

配置用于 ASDM 的 HTTPS 访问、其他客户端

如要使用 ASDM 或 CSM 等其他 HTTPS 客户端，则需要启用 HTTPS 服务器，并允许至 ASA 的 HTTPS 连接。HTTPS 访问已作为出厂默认配置的一部分启用。如要配置 HTTPS 访问，请执行以下步骤。请参阅以下准则：

- 要访问 ASA 接口以进行 HTTPS 访问，亦无需允许主机 IP 地址的访问规则。您只需按照本部分配置 HTTPS。但是，如果您配置 HTTP 重定向以将 HTTP 连接自动重定向至 HTTPS，则必须启用允许 HTTP 的访问规则；否则，该接口无法侦听 HTTP 端口。
- 除了进入ASA时所经由的接口以外，不支持对其他接口进行管理访问。例如，如果管理主机位于外部接口上，则只能直接向外部接口发起管理连接。此规则的唯一例外是通过VPN连接。请参阅配置 VPN 隧道上的管理访问，第 12 页。
- 在单情景模式下，最多可以有 30 个 ASDM 并发会话。在多情景模式下，每个情景最多 5 个并发 ASDM 会话，在所有情景中最多分为 32 个 ASDM 实例。

  ASDM会话使用两个HTTPS连接：一个用于监控（始终存在），另一个用于进行配置更改（仅当进行更改时才存在）。例如，多情景模式系统限制为 32 个 ASDM 会话表示 HTTPS 会话数限制为 64。
- ASA 允许在单情景模式或每个情景（如果可用）中最多允许 6 个并发非 ASDM HTTPS 会话，所有情景中最多允许 100 个 HTTPS 会话。
- 如果在同一接口上同时启用 SSL (**webvpn** > **启用** 接口) 和 HTTPS 访问，则可以从 **https://***ip_address* 访问 Secure Client，从 **https://***ip_address*/**admin** 访问端口 443。如果还启用了 **aaa 身份验证 http 控制台**，则必须为 ASDM 访问指定其他端口。

开始之前

- 在多情景模式下，请在情景执行空间中完成本程序。要从系统配置切换至情景配置，请输入 **changeto context** *name*。

过程

步骤 1 识别 ASA 为位于特定接口的每个地址或子网接收 HTTPS 连接的 IP 地址。

http *source_IP_address mask source_interface*

- *source_interface* - 指定任何已命名的接口。对于网桥组，请指定网桥组成员接口。对于仅 VPN 管理访问（请参阅 配置 VPN 隧道上的管理访问，第 12 页），请指定命名的 BVI 接口。

示例：

```
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

步骤 2 启用 HTTPS 服务器。

http server enable [*port*]

示例：

```
ciscoasa(config)# http server enable 444
```

默认情况下，端口为 443。如果更改端口号，请务必将其包括在 ASDM 访问 URL 中。例如，如果将端口号更改为 444，请输入以下 URL：

https://10.1.1.1:444

步骤 3 允许基于非浏览器的 HTTPS 客户端访问 ASA 上的 HTTPS 服务。默认情况下，允许 ASDM、CSM 和 REST API。

http server basic-auth-client *user_agent*

- *user_agent* - 在 HTTP 请求的 HTTP 报头中指定客户端的用户代理字符串。您可以指定完整字符串或部分字符串；部分字符串必须与用户代理字符串的开头匹配。建议使用完整的字符串以提高安全性。请注意，文件夹名称区分大小写。

  例如，**curl** 将匹配以下用户代理字符串：

  curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2

  curl 将不匹配以下用户代理字符串：

  abcd curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2

  CURL 将不匹配以下用户代理字符串：

  curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2

使用单独的命令输入每个客户端字符串。 许多专业客户端（例如，python 库、curl 和 wget）不支持跨站请求伪造 (CSRF) 基于令牌的身份验证，因此，您需要特别允许这些客户端使用 ASA 基本身份验证方法。出于安全考虑，您应该只允许所需的客户端。

示例：

```
ciscoasa(config)# http server basic-auth-client curl
```

步骤 4 （可选） 设置连接和会话超时。

http server idle-timeout分钟

http server session-timeout分钟

http connection idle-timeout秒

- **http server idle-timeout**分钟 - 设置 ASDM 连接的空闲超时，范围为 1-1440 分钟。默认值为 20 分钟。ASA 会断开在设置的时间段内处于空闲状态的 ASDM 连接。
- **http server session-timeout**分钟 - 设置 ASDM 会话的会话超时，范围为 1-1440 分钟。此超时默认处于禁用状态。ASA 会断开超过设置时间段的 ASDM 会话。

- **http connection idle-timeout***seconds* - 设置所有 HTTPS 连接（包括 ASDM、WebVPN 和其他客户端）的空闲超时，范围为 10-86400 秒。此超时默认处于禁用状态。ASA 会断开在设置的时间段内处于空闲状态的连接。如果同时设置 **http server idle-timeout** 和 **http connection idle-timeout** 命令，则 **http connection idle-timeout** 优先执行。

示例：

```
ciscoasa(config)# http server idle-timeout 30
ciscoasa(config)# http server session-timeout 120
```

示例

以下示例显示如何启用 HTTPS 服务器并使内部接口上地址为 192.168.1.2 的主机访问 ASDM：

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

以下示例显示如何使 192.168.3.0/24 网络上的所有用户可以访问内部接口上的 ASDM：

```
ciscoasa(config)# http 192.168.3.0 255.255.255.0 inside
```

为 ASDM 访问或无客户端 SSL VPN 配置 HTTP 重定向

您必须使用 HTTPS 连接至使用 ASDM 或无客户端 SSL VPN 的 ASA。为了方便起见，可以将 HTTP 管理连接重定向至 HTTPS。例如，通过重定向 HTTP，输入 **http://10.1.8.4/admin/** 或 **https://10.1.8.4/admin/** 均可访问位于该 HTTPS 地址的 ASDM 启动页面。

您可以重定向 IPv4 和 IPv6 流量。

开始之前

通常，您无需允许主机 IP 地址的访问规则。但是，对于 HTTP 重定向，您必须启用允许 HTTP 的访问规则；否则，该接口无法侦听 HTTP 端口。

过程

启用 HTTP 重定向：

http redirect *interface_name* [*port*]

示例：

```
ciscoasa(config)# http redirect outside 88
```

port 确定接口从其重定向 HTTP 连接的端口。默认值为 80。

配置 VPN 隧道上的管理访问

如果 VPN 隧道在一个接口上终止，但是您需要通过访问不同的接口来管理 ASA，则必须将该接口标识为管理访问接口。例如，如果从外部接口进入 ASA，通过此功能可以使用 ASDM、SSH、 或 Telnet 连接到内部接口；或者，当从外部接口进入时，可以 Ping 内部接口。

注释 如果使用 CiscoSSH 堆栈，则 SSH 不支持此功能。

注释 SNMP 不支持此功能。 对于基于 VPN 的 SNMP，我们建议在环回接口上启用 SNMP。您无需启用管理访问功能即可在环回接口上使用 SNMP。环回接口也适用于 SSH。

除了进入 ASA 时所经由的接口以外，不支持对其他接口进行 VPN 访问。例如，如果 VPN 访问位于外部接口上，则只能直接向外部接口发起连接。应在 ASA 的可直接访问的接口上启用 VPN，并使用域名解析，以便您不必记住多个地址。

通过以下类型的 VPN 隧道可以实现管理访问： IPsec 客户端、IPsec 站点间的简单 VPN 和 Secure Client SSL VPN 客户端。

开始之前

由于使用单独的管理和数据路由表时的路由注意事项，VPN 终端接口和管理访问接口必须属于相同类型：二者必须是管理专用接口或常规数据接口。

过程

指定从另一个接口进入 ASA 时要访问的管理接口的名称。

management-access *management_interface*

对于 Easy VPN 和站点间隧道，可以指定命名 BVI（在路由模式下）。

示例：

```
ciscoasa(config)# management-access inside
```

在 Firepower 2100 平台模式数据接口上配置对 FXOS 的管理访问

在平台模式下，如果要从数据接口管理 Firepower 2100 上的 FXOS，可以配置 SSH、HTTPS 和 SNMP 访问。如果要远程管理设备，但又要保持管理 1/1（这是访问 FXOS 的本机方式）位于独立网络中，则此功能非常有用。如果启用此功能，则仅可以继续使用管理 1/1 进行本地访问。但是，您不能在使用此功能时允许对或通过 FXOS 的管理 1/1 进行远程访问。此功能需要通过背板将流量转发到 ASA 数据接口（默认），并且您只能使用内部路径（默认下）指定一个 FXOS 管理网关。

ASA 使用非标准端口进行 FXOS 访问；标准端口将被保留以供同一接口上的 ASA 使用。当 ASA 将流量转发到 FXOS 时，它会针对每个协议将非标准目标端口转换为 FXOS 端口（不会更改 FXOS 中的 HTTPS 端口）。数据包目标 IP 地址（即 ASA 接口 IP 地址）也会被转换为内部地址，供 FXOS 使用。源地址保持不变。为了返回流量，ASA 使用其数据路由表来确定正确的出口接口。当您访问管理应用的 ASA 数据 IP 地址时，必须使用 FXOS 用户名登录；ASA 用户名只适用于 ASA 管理访问。

您还可以在 ASA 数据接口上启用 FXOS 管理流量 启动 ，这是 SNMP 陷阱或进行 NTP 和 DNS 服务器等所需的。默认情况下，将为 ASA 外部接口启用 FXOS 管理流量启动，以进行 DNS 和 NTP 服务器通信（这是进行智能软件许可通信所必需的）。

开始之前

- 仅限单一情景模式。
- 不包括 ASA 仅管理接口。
- 不能直接通过 VPN 隧道连接至 ASA 数据接口，也不能直接访问 FXOS。作为 SSH 的一种变通方法，可以通过 VPN 连接到 ASA，访问 *ASA* CLI，然后使用 **connect fxos** 命令访问 FXOS CLI。请注意，SSH、HTTPS 和 SNMPv3 已经加密/可以加密，因此直接连接到数据接口是安全的。
- 确保 FXOS 网关已设置为将流量转发到 ASA 数据接口（默认值）。有关设置网关的更多信息，请参阅《入门指南》。

过程

步骤 1 启用 FXOS 远程管理。

fxos {**https** | **ssh** | **snmp**} **permit** {*ipv4_address netmask* | *ipv6_address/prefix_length*} *interface_name*

示例：

```
ciscoasa(config)# fxos https permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos https permit 2001:DB8::34/64 inside
ciscoasa(config)# fxos ssh permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos ssh permit 2001:DB8::34/64 inside
```

步骤 2 （可选） 更改服务的默认端口。

fxos {**https** | **ssh** | **snmp**} **port** *port*

请参阅以下默认值：

- HTTPS 默认端口 - 3443
- SNMP 默认端口 - 3061
- SSH 默认端口 - 3022

示例：

```
ciscoasa(config)# fxos https port 6666
ciscoasa(config)# fxos ssh port 7777
```

步骤 3 允许 FXOS 从 ASA 接口启动管理连接。

ip-client *interface_name*

默认情况下，外部接口处于启用状态。

示例：

```
ciscoasa(config)# ip-client outside
ciscoasa(config)# ip-client services
```

步骤 4 在管理 1/1 上连接到 机箱管理器 （默认情况下网址为 https://192.168.45.45，用户名为 **admin**，密码为 **Admin123**）。

步骤 5 点击**平台设置 (Platform Settings)** 选项卡，然后启用 **SSH**、**HTTPS** 或 **SNMP**。

默认情况下，SSH 和 HTTPS 处于启用状态。

步骤 6 将**平台设置 (Platform Settings)** 选项卡上的**访问列表 (Access List)** 配置为允许您的管理地址。默认情况下，SSH 和 HTTPS 只允许管理 1/1 192.168.45.0 网络。您需要允许在 ASA 上的 **FXOS 远程管理 (FXOS Remote Management)** 配置中指定的任何地址。

更改控制台超时

控制台超时设置连接可保持处于特权 EXEC 模式下或配置模式下的时间；当达到超时时间后，会话将进入用户 EXEC 模式。默认情况下，会话不会超时。此设置不会影响可与控制台端口保持连接的时间，该连接永不超时。

过程

指定授权会话结束后的空闲时间（0-60，以分钟为单位）。

console timeout *number*

示例：

```
ciscoasa(config)# console timeout 0
```

默认超时为 0，表示会话不会超时。

自定义 CLI 提示符

利用为提示符添加信息这项功能，可以大体了解在您有多个模块时登录哪一台 ASA。故障转移起价你，如果两台 ASA 具有相同的主机名，则此功能非常有用。

在多情景模式中，您可以在登录到系统执行空间或管理情景时查看扩展的提示符。在非管理情景中，您仅可看到默认提示符，即主机名和情景名称。

默认情况下，提示符显示 ASA 的主机名。在多情景模式下，提示符还显示情景名称。在 CLI 提示符中可以显示以下项目：

cluster-unit	显示集群设备名称。集群中的每台设备都有一个唯一的名称。
context	（仅多情景模式）显示当前情景的名称。
domain	显示域名。
hostname	显示主机名。
priority	显示故障转移优先级 pri（主要）或 sec（辅助）。
state	显示设备的流量传递状态或角色。 对于故障转移，会面向 state 关键字显示以下值： • **act** - 已启用故障转移，设备正在传递流量。 • **stby** - 已启用故障转移，设备未在传递流量，并且处于备用、故障或其他非活动状态。 • **actNoFailover** - 未启用故障转移，设备正在传递流量。 • **stbyNoFailover** - 未启用故障转移，设备未在传递流量。这可能会在待机设备上存在阈值以上的接口故障时发生。 对于集群，会显示控制和数据的值。

过程

通过输入以下命令自定义 CLI 提示符：

prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]}

示例：

```
ciscoasa(config)# prompt hostname context slot state priority
ciscoasa/admin/pri/act(config)#
```

输入关键字的顺序确定提示符中各元素的顺序（各元素以斜线 (/) 分隔）。

配置登录横幅

您可以配置在用户连接至 ASA 时、在用户登录之前或在用户进入特权 EXEC 模式之前将显示的消息。

开始之前

- 从安全角度来看，重要的是横幅阻止未经授权的访问。请勿使用“欢迎”或“请”等措辞，因为它们像是在邀请入侵者。以下横幅为未经授权的访问设置正确的语调：

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk possible criminal consequences.
```

- 在添加横幅后，如果有以下情况，可能会关闭至 ASA 的 Telnet 或 SSH 会话：
  - 没有足够的系统内存可用来处理横幅消息。
  - 在尝试显示横幅消息时发生 TCP 写入错误。
- 有关横幅消息的准则，请参阅 RFC 2196。

过程

添加在以下三个时间之一要显示的横幅：在用户首次连接时 (message-of-the-day (motd))，在用户登录时 (login)，以及在用户访问特权 EXEC 模式时 (exec)。

banner {**exec** | **login** | **motd**} *text*

示例：

```
ciscoasa(config)# banner motd Only authorized access is allowed to $(hostname).
```

当用户连接至 ASA 时，系统首先显示 message-of-the-day 横幅，然后显示 login 横幅和提示符。在用户成功登录 ASA 后，系统将显示 exec 横幅。

如要添加一行以上，请将**banner** 命令放在每行之前。

对于横幅文本：

- 允许包含空格，但使用 CLI 时无法输入制表符。
- 除了 RAM 和闪存对横幅长度的限制外，无其他长度限制。
- 通过包含字符串 **$(hostname)** 和 **$(domain)**，可以动态添加 ASA 的主机名或域名。

- 如果在系统配置中配置横幅，可以通过在情景配置中使用**$(system)**字符串来在情景中使用该横幅文本。

示例

以下示例显示如何添加 message-of-the-day 横幅：

```
ciscoasa(config)# banner motd Only authorized access is allowed to $(hostname).

ciscoasa(config)# banner motd Contact me at admin@example.com for any issues.
```

设置管理会话配额

可以在 ASA 上建立允许的最大同时 ASDM、SSH 和 Telnet 会话数量。如果达到最大值，则不允许其他会话，并生成系统日志消息。如要防止系统锁定，则管理会话配额机制无法阻止控制台会话。

注释 在多情景模式下，如果最大 ASDM 会话数固定为 5，则无法配置会话数。

注释 如果您还为最大管理会话（SSH等）的每个情景设置资源限制，则将使用较低的值。

开始之前

在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请输入 **changeto context**名称 命令。

过程

步骤 1 请输入以下命令：

quota management-session [**ssh** | **telnet** | **http** | **user**] *number*

- **ssh**-设置最大SSH会话数（介于1和5之间）。默认值为 5。
- **telnet**-设置最大Telnet会话数，介于1和5之间。默认值为 5。
- **http**-设置最大HTTPS（ASDM）会话数，介于1和5之间。默认值为 5。
- **user**-设置每个用户的最大会话数，介于1和5之间。默认值为 5。
- number-设置介于0（无限制）和10000之间的会话总数。 当不带任何其他关键字输入时，此参数设置介于1到15之间的会话总数。默认值为 15。

示例：

```
ciscoasa(config)# quota management-session ssh 3
ciscoasa(config)# quota management-session telnet 1
ciscoasa(config)# quota management-session http 4
ciscoasa(config)# quota management-session user 2
```

步骤 2 查看当前正在使用的会话。

show quota management-session [**ssh** | **telnet** | **http** | **user**]

示例：

```
ciscoasa(config)#show quota management-session

#Sessions               ConnectionType                  Username
1                              SSH                      cisco
2                              TELNET                   cisco
1                              SSH                      cisco1
```

为系统管理员配置 AAA

本部分介绍如何为系统管理员配置身份验证、管理授权和命令授权。

配置管理验证

配置用于 CLI 和 ASDM 访问的身份验证。

关于管理验证

如何登录 ASA 取决于是否启用身份验证。

关于 SSH 身份验证

请参阅以下行为了解在有身份验证和无身份验证的情况下进行 SSH 访问：

- 无身份验证时 - 在无身份验证的情况下，SSH 不可用。
- 身份验证 - 如果启用身份验证，请输入在 AAA 服务器或本地用户数据库中所定义的用户名和密码。对于公钥身份验证，ASA 仅支持本地数据库。 如果配置 SSH 公钥身份验证，则 ASA 隐式使用本地数据库。当您使用用户名和密码登录时，只需要明确配置 SSH 身份验证。您将进入用户 EXEC 模式。

关于 Telnet 身份验证

有关在使用身份验证和不使用身份验证的情况下的 Telnet 访问，请参阅以下行为：

- 无身份验证 - 如果不为 Telnet 启用任何身份验证，请勿输入用户名；您应该输入登录密码（使用 **password** 命令设置）。没有默认密码，因此您必须设置一个，才能通过 Telnet 连接到 ASA。您将进入用户 EXEC 模式。
- 有身份验证 - 如果启用 Telnet 身份验证，请输入在 AAA 服务器或本地用户数据库中所定义的用户名和密码。您将进入用户 EXEC 模式。

关于 ASDM 身份验证

有关在使用身份验证和不使用身份验证的情况下的 ASDM 访问，请参阅以下行为。您还可以配置证书身份验证，而不管是否使用 AAA 身份验证。

- 无身份验证 - 默认情况下，可以使用空的用户名以及通过 **enable password** 命令设置的启用密码（默认为空）登录 ASDM。建议您尽快更改启用密码，不要再保持空白状态；请参阅 设置主机名、域名及启用密码和 Telnet 密码。首次在CLI中输入命令时，系统会提示您更改密码；登录 ASDM时不会强制执行此行为。 **enable** 请注意，如果在登录屏幕输入用户名和密码（而不是将用户名留空），则 ASDM 将检查本地数据库是否有匹配项。
- 证书身份验证 -（仅限单个、路由模式）您可以要求用户具备有效的证书。输入证书用户名和密码，ASA 会根据 PKI 信任点对证书进行验证。
- AAA 身份验证 - 启用 ASDM (HTTPS) 身份验证时，需要输入 AAA 服务器或本地用户数据库中定义的用户名和密码。不能再使用空用户名和启用密码登录 ASDM。
- AAA 身份验证加证书身份验证 -（仅限单个、路由模式）启用 ASDM (HTTPS) 身份验证时，需要输入 AAA 服务器或本地用户数据库中定义的用户名和密码。如果用户名和密码对于证书身份验证是不同的，系统将提示您输入它们。您可以选择预填充从证书派生的用户名。

关于串行身份验证

请参阅以下行为了解在有身份验证和无身份验证的情况下访问串行控制台端口：

- 无身份验证 - 如果不为串行访问启用任何身份验证，则不输入用户名或密码。您将进入用户 EXEC 模式。
- 身份验证 - 如果为串行访问启用身份验证，请输入在 AAA 服务器或本地用户数据库中所定义的用户名和密码。您将进入用户 EXEC 模式。

关于 Enable 身份验证

如要在登录后进入特权 EXEC 模式，请输入 **enable** 命令。此命令的工作方式取决于是否启用身份验证：

- No Authentication - 如果不配置 enable 身份验证，在输入 **enable** 命令时输入系统启用密码（通过 **enable password** 命令设置），该密码默认留空。第一次输入 **enable** 命令时，系统会提示您更改密码。但是，如果不使用 enable 身份验证，在输入 **enable** 命令后，则不再以特定用户身份登录，这会影响基于用户的功能，如命令授权。为了保留用户名，请使用 enable 身份验证。

- Authentication - 如果配置 enable 身份验证，ASA 会提示您输入在 AAA 服务器或本地用户数据库上定义的用户名和密码。当执行命令授权时此功能特别有用，因为用户名在确定用户可以输入的命令时非常重要。

对于使用本地数据库的 enable 身份验证，可以使用 **login** 命令，来代替 **enable** 命令。**login** 命令会保留用户名，但不需要配置开启身份验证。

⚠

注意 如果您将可以访问 CLI 但您不希望其进入特权 EXEC 模式的用户添加到本地数据库中，则应该配置命令授权。在无命令授权的情况下，如果用户的权限级别为 2 或更高（2 是默认值），则用户可以在 CLI 使用自己的密码访问特权 EXEC 模式（以及所有命令）。或者，您可以使用 AAA 服务器而不是本地数据库进行身份验证，或将所有本地用户都设置为 1 级，以阻止使用 login 命令，这样就可以控制谁可以使用系统启用密码访问特权 EXEC 模式。

从主机操作系统到 ASA 的会话

有些平台支持将 ASA 作为单独的应用运行：例如，Catalyst 6500 上的 ASASM 或 Firepower 4100/9300 上的 ASA。对于从主机操作系统到 ASA 的会话，您可以配置串行和 Telnet 身份验证，具体取决于连接类型。例如，**connect asa**Firepower 2100 在平台模式下的 FXOS 中的命令使用串行连接。

多情景模式下，无法在系统配置中配置任何 AAA 命令。但是，如果在管理员情景中配置 Telnet 或串行身份验证，则身份验证也适用于这些会话。在此情况下，使用管理员情景 AAA 服务器或本地用户数据库。

配置用于 CLI 和 ASDM访问的身份验证

开始之前

- 配置 Telnet、SSH 或 HTTP 访问。
- 对于外部身份验证，请配置 AAA 服务器组。对于本地身份验证，请向本地数据库添加用户。
- HTTP 管理身份验证不支持 AAA 服务器组的 SDI 协议。
- 此功能不影响使用 **ssh authentication** 命令对本地用户名进行 SSH 公共密钥身份验证。ASA 隐式使用本地数据库进行公共密钥身份验证。此功能仅影响用户名与密码。如果要允许本地用户进行公共密钥身份验证或使用密码，您需要使用此程序显式配置本地身份验证，以允许进行密码访问。

过程

对用户进行管理访问的身份验证。

aaa authentication {**telnet** | **ssh** | **http** | **serial**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

示例：

```
ciscoasa(config)# aaa authentication ssh console radius_1 LOCAL
ciscoasa(config)# aaa authentication http console radius_1 LOCAL
```

```
ciscoasa(config)# aaa authentication serial console LOCAL
```

telnet 关键字控制 Telnet 访问。**ssh** 关键字控制 SSH 访问（仅密码；公共密钥身份验证隐式使用本地数据库）。**http** 关键字控制 ASDM 访问。**serial** 关键字控制控制台端口访问。对于平台模式下的 Firepower 2100，此关键字会影响使用 **connect asa** 命令从 FXOS 访问的虚拟控制台。

如果使用 AAA 服务器组进行身份验证，可以将 ASA 配置为在 AAA 服务器不可用时使用本地数据库作为回退方法。指定服务器组名后跟 **LOCAL**（区分大小写）。建议在本地数据库中使用与 AAA 服务器相同的用户名和密码，因为ASA提示符不会给出使用何种方法的任何指示。或者，您可以只输入 **LOCAL**，以将本地数据库用作主要的身份验证方法（不使用回退）。

配置 Enable 身份验证（特权 EXEC 模式）

您可以在用户输入 **enable** 命令时对他们进行身份验证。

开始之前

请参阅关于 Enable 身份验证，第 19 页。

过程

选择以下选项之一用于对用户进行身份验证：

- 如要使用 AAA 服务器或本地数据库对用户进行身份验证，请输入以下命令：

  aaa authentication enable console {**LOCAL** | *server_group* [**LOCAL**]}

  示例：

  ```
  ciscoasa(config)# aaa authentication enable console LOCAL
  ```

  系统提示用户输入用户名和密码。

  如果使用 AAA 服务器组进行身份验证，可以将 ASA 配置为在 AAA 服务器不可用时使用本地数据库作为回退方法。指定服务器组名后跟 **LOCAL**（区分大小写）。建议在本地数据库中使用与 AAA 服务器相同的用户名和密码，因为 ASA 提示符不会给出使用何种方法的任何指示。

  或者，您可以只输入 **LOCAL**，以将本地数据库用作主要的身份验证方法（不使用回退）。

- 如要以本地数据库中用户的身份登录，请输入以下命令：

  login

  示例：

  ```
  ciscoasa# login
  ```

  ASA 提示输入用户名和密码。在输入密码后，ASA 将该用户置于本地数据库指定的权限级别中。

用户可以使用自己的用户名和密码登录来访问特权 EXEC 模式，因此无需为每个人提供系统使能口令。如要允许用户在登录后访问特权 EXEC 模式（以及所有命令），请将用户权限级别设置为 2（默认）到 15。如果配置本地命令授权，则用户只能输入分配给该权限级别或更低级别的命令。

配置 ASDM 证书身份验证

无论是否有 AAA 身份验证，您都可以要求进行证书身份验证。ASA 将针对 PKI 信任点验证证书。

开始之前

仅在单个路由模式中支持此功能。

过程

步骤 1 启用证书身份验证：

http authentication-certificate *interface_name*[**match** *certificate_map_name*]

示例：

```
ciscoasa(config)# crypto ca certificate map map1 10
ciscoasa(config-ca-cert-map)# subject-name emailAddress www.example.com
ciscoasa(config)# http authentication-certificate outside match map1
```

您应为每个接口配置证书身份验证，使得受信任/内部接口上的连接无需提供证书。您可以多次使用该命令，以在多个接口上启用证书身份验证。

若要要求证书匹配证书映射，请指定 **match** 关键字和映射名称。使用 **crypto ca certificate map** 命令配置映射。

步骤 2 （可选） 设置 ASDM 用于从证书派生用户名的属性：

http username-from-certificate{*primary-attr* [*secondary-attr*] | **use-entire-name** | **use-script**} [**pre-fill-username**]

示例：

```
ciscoasa(config)# http username-from-certificate CN pre-fill-username
```

默认情况下，ASDM 使用 CN OU 属性。

- *primary-attr* 参数指定要用于派生用户名的属性。*secondary-attr* 参数指定要与主要属性配合用于派生用户名的其他属性。您可以使用以下属性：
  - C - 国家/地区
  - CN - 公用名
  - DNQ - DN 限定符

- emailAddress - 邮件地址
- GENQ - 世代限定符
- GN - 名
- I - 首字母
- L - 位置
- N - 名称
- O - 组织
- OU - 组织单位
- SER - 序列号
- SN - 姓氏
- SP - 州/省
- T - 职位
- UID - 用户 ID
- UPN - 用户主体名称

- **use-entire-name** 关键字使用完整 DN 名称。
- **use-script** 关键字使用 ASDM 生成的 Lua 脚本。
- **pre-fill-username** 关键字在提示身份验证时预填充用户名。如果用户名与您最初输入的不同，系统将显示一个新对话框，其中含有预填充的用户名。然后，您可以输入身份验证的密码。

使用管理授权控制 CLI 和 ASDM 访问

ASA 使您可以在管理用户和远程访问用户进行身份验证时对他们加以区分。用户角色的区分可防止远程访问 VPN 和网络访问用户建立到 ASA 的管理连接。

开始之前

RADIUS 或 LDAP（映射的）用户

当用户通过 LDAP 进行身份验证时，可将本地 LDAP 属性及其值映射到 ASA 属性来提供特定授权功能。配置具有 0 和 15 之间的值的特权级别的 Cisco VSA CVPN3000-Privilege-Level。然后，使用 **ldap map-attributes** 命令将 LDAP 属性映射到 Cisco VAS CVPN3000-Privilege-Level。

当 RADIUS IETF **service-type** 属性作为 RADIUS 身份验证和授权请求的结果在访问接受消息中进行发送时，其用于表示授予通过身份验证的用户的服务类型

在访问接受消息中发送 RADIUS Cisco VSA **privilege-level** 属性 (Vendor ID 3076, sub-ID 220) 时，该属性用于表示用户的权限级别。

TACACS+ 用户

使用“service=shell”请求授权，服务器以 PASS 或 FAIL 作为响应。

本地用户

为给定用户名设置 **service-type** 命令。默认情况下，service-type 是 admin，允许对 **aaa authenticationconsole** 命令指定的任何服务进行完全访问。

管理授权属性

请参阅下表，了解管理授权的 AAA 服务器类型和有效值。ASA 使用这些值来确定管理访问的级别。

管理级别	**RADIUS/LDAP**（映射的）属性	**TACACS+** 属性	本地数据库属性
完全访问 - 允许完全访问**aaa authenticationconsole** 命令所指定的任何服务	Service-Type 6（管理），Privilege-Level 1	PASS，特权级别 1	admin
部分访问 - 允许在您配置**aaa authenticationconsole** 命令时访问 CLI 或 ASDM。但是，如果您使用**aaa authenticationenableconsole** 命令配置 **enable** 身份验证，则 CLI 用户无法使用 **enable** 命令访问 EXEC 特权模式。	Service-Type 7（NAS 提示），Privilege-Level 2 及更高级别 Framed (2) 和 Login (1) 服务类型按同一方式处理。	PASS，特权级别 2 及更高级别	nas-prompt
No Access - 拒绝管理访问。用户无法使用由 **aaa authenticationconsole** 命令 选项指定的任何服务（不包括 **serial**关键字；允许串行访问）。远程访问（IPsec 和 SSL）用户仍可对其远程访问会话进行身份验证并终止会话。所有其他服务类型（Voice、FAX 等）按同一方式处理。	Service-Type 5（出站）	FAIL	remote-access

其他准则

- 串行控制台访问不包含在管理授权中。
- 您还必须为管理访问配置 AAA 身份验证才能使用此功能。请参阅配置用于 CLI 和 ASDM访问的身份验证，第 20 页。
- 如果您使用外部身份验证，则必须在启用此功能之前预配置 AAA 服务器组。
- HTTP 授权仅在单个路由模式下受支持。

过程

步骤 1 为 Telnet 和 SSH 启用管理授权：

aaa authorization exec {**authentication-server** | **LOCAL**} [**auto-enable**]

auto-enable 关键字允许具有足够授权权限的管理员在登录时自动进入特权 EXEC 模式。

示例：

```
ciscoasa(config)# aaa authentication ssh console RADIUS
ciscoasa(config)# aaa authorization exec authentication-server auto-enable
```

步骤 2 为 HTTPS (ASDM) 启用管理授权：

aaa authorization http console {**authentication-server** | **LOCAL**}

示例：

```
ciscoasa(config)# aaa authentication http console RADIUS
ciscoasa(config)# aaa authorization http console authentication-server
```

步骤 3

示例

以下示例显示如何定义 LDAP 属性映射。在本示例中，安全策略指定正在通过 LDAP 进行身份验证的用户将用户记录字段或参数标题和公司分别到映射 IETF-RADIUS service-type 和 privilege-level。

```
ciscoasa(config)# ldap attribute-map admin-control
ciscoasa(config-ldap-attribute-map)# map-name title IETF-RADIUS-Service-Type
ciscoasa(config-ldap-attribute-map)# map-name company
```

以下示例向 LDAP AAA 服务器 应用 LDAP 属性映射：

```
ciscoasa(config)# aaa-server ldap-server (dmz1) host 10.20.30.1
ciscoasa(config-aaa-server-host)# ldap attribute-map admin-control
```

配置命令授权

如果要控制对命令的访问，可以通过ASA配置命令授权，在其中确定可供用户使用的命令。默认情况下，登录时可以访问用户 EXEC 模式，此模式仅提供最小数量的命令。输入 **enable** 命令时（或在使用本地数据库时输入 **login** 命令时），可以进入特权 EXEC 模式并访问高级命令（包括配置命令）。

可以使用两种命令授权方法之一：

- 本地权限级别
- TACACS+ 服务器权限级别

关于命令授权

您可以启用命令授权，以便只有授权用户可以输入命令。

支持的命令授权方法

可以使用两种命令授权方法之一：

- 本地权限级别 - 在 ASA 上配置命令权限级别。当本地、RADIUS 或 LDAP（如果将 LDAP 属性映射到 RADIUS 属性）用户面向 CLI 访问进行身份验证时，ASA 会为该用户指定由本地数据库、RADIUS 或 LDAP 服务器定义的权限级别。用户可以访问分配的权限级别及以下级别的命令。请注意，所有用户首次登录时都会进入用户 EXEC 模式（命令级别为 0 或 1）。用户需要使用 **enable** 命令再次进行身份验证才能进入特权 EXEC 模式（命令级别为 2 或更高），或使用 **login** 命令登录（仅限本地数据库）。

注释 您可以在本地数据库中没有任何用户，以及没有 CLI 也没有 **enable** 身份验证的情况下，使用本地命令授权。输入 **enable** 命令时，您需要输入系统启用密码，ASA 会为您指定级别 15。然后，您可以为每个级别创建启用密码，以便在输入 **enable** *n*（2 至 15）时，ASA 为您指定级别 *n*。除非启用本地命令授权，否则不使用这些级别。

- TACACS+ 服务器权限级别 - 在 TACACS+ 服务器上，配置用户或组在进行 CLI 访问的身份验证后可以使用的命令。用户在 CLI 输入的每个命令都使用 TACACS+ 服务器进行验证。

安全情景和命令授权

每个情景的 AAA 设置相互独立，不同情景之间不会共享这些设置。

配置命令授权时，必须分别配置每个安全情景。此配置能够实现对不同安全情境执行不同的命令授权。

当在安全情景之间切换时，管理员应知道登录时指定的用户名允许的命令在新情景会话中可能有所差异，或在新情景中可能根本无法配置该命令授权。如果管理员不知道安全情境之间的命令授权可能有所差异，就可能会对其造成困扰。

注释 系统执行空间不支持 AAA 命令；因此，命令授权在系统执行空间不可用。

命令权限级别

默认情况下，会为以下命令分配 0 级权限，为所有其他命令分配 15 级权限。

- **show checksum**

- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

如果将任何配置模式命令移到低于 15 的级别，请确保也将“**configure**”命令移到同一级别，否则用户将无法进入配置模式。

配置本地命令授权

通过本地命令授权可以为 16 个权限级别（0 到 15）之一分配命令。默认情况下，会向每个命令分配 0 级或 15 级权限。您可以将每个用户定义在特定权限级别，每个用户可以输入分配的权限级别或以下级别的任何命令。ASA 支持在本地数据库、RADIUS 服务器或 LDAP 服务器（如果将 LDAP 属性映射到 RADIUS 属性）中定义的用户权限级别。

过程

步骤 1 将命令分配到权限级别。

privilege [**show** | **clear** | **cmd**] **level** *level* [**mode** {**enable** | **cmd**}] **command** *command*

示例：

```
ciscoasa(config)# privilege show level 5 command filter
```

对要重新分配的每个命令重复此命令。

此命令中的选项如下：

- **show** | **clear** | **cmd** - 这些可选关键字可用于仅为命令的显示、清除或配置形式设置权限。命令的配置形式通常是导致配置更改的形式，或者是以未修改的命令形式（无 **show**或 **clear** 前缀），或者是以 **no** 形式。如果不使用其中一个关键字，则会影响命令的所有形式。
- **level***level* - 介于 0 和 15 之间的级别。

- **mode** {**enable** | **configure**} - 如果某个命令可以在用户 EXEC 模式或特权 EXEC 模式下以及配置模式下输入，并且该命令在每个模式下执行不同的操作，则可以分别设置其在这些模式下的权限级别：
  - **enable** - 指定用户 EXEC 模式和特权 EXEC 模式。
  - **configure** - 指定配置模式，可以使用 **configure terminal** 命令进行访问。
- **command***command* - 将要配置的命令。您只能配置主命令的权限级别。例如，可以配置所有 **aaa** 命令的级别，但是不可以单独配置 **aaa authentication** 命令和 **aaa authorization** 命令的级别。

步骤 2 （可选） 为命令授权启用 AAA 用户。如果没有此命令，则 ASA 仅支持本地数据库用户的权限级别，并将所有其他类型的用户默认设置为 15 级。

aaa authorization exec authentication-server [auto-enable]

示例：

```
ciscoasa(config)# aaa authorization exec authentication-server
```

此命令还将启用管理授权。请参阅使用管理授权控制 CLI 和 ASDM 访问 ， 第 23 页。

步骤 3 启用使用本地命令权限级别：

aaa authorization command LOCAL

示例：

```
ciscoasa(config)# aaa authorization command LOCAL
```

在设置命令权限级别时，除非使用此命令来配置命令授权，否则不会进行命令授权。

示例

filter 命令具有以下形式：

- **filter**（表示为 **configure** 选项）
- **show running-config filter**
- **clear configure filter**

您可以为每种形式分别设置权限级别，或通过忽略此选项为所有形式设置同一权限级别。以下示例显示如何分别设置每种形式：

```
ciscoasa(config)# privilege show level 5 command filter
ciscoasa(config)# privilege clear level 10 command filter
ciscoasa(config)# privilege cmd level 10 command filter
```

或者， 以下示例显示如何将所有 filter 命令设置为同一级别：

```
ciscoasa(config)# privilege level 5 command filter
```

show privilege 命令分隔显示的形式。

以下示例显示 **mode** 关键字的使用。必须从用户 EXEC 模式输入 **enable** 命令，而可在配置模式中访问的 **enable password** 命令则要求最高的权限级别：

```
ciscoasa(config)# privilege cmd level 0 mode enable command enable
ciscoasa(config)# privilege cmd level 15 mode cmd command enable
ciscoasa(config)# privilege show level 15 mode cmd command enable
```

以下示例显示 使用 **configure** 关键字的附加命令 **mode** 命令：

```
ciscoasa(config)# privilege show level 5 mode cmd command configure
ciscoasa(config)# privilege clear level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode enable command configure
```

注释 此最后一行用于 **configure terminal** 命令。

在 Commands TACACS+ 服务器上配置命令

您可以在思科安全访问控制服务器 (ACS) TACACS+ 服务器上，为组或为单个用户将命令配置为共享配置文件组件。对于第三方 TACACS+ 服务器，请参阅服务器文档了解有关命令授权支持的详细信息。

请参阅以下在思科安全 ACS 3.1 版本中配置命令的准则；其中许多原则也适用于第三方服务器。

- ASA 将待授权的命令作为外壳命令发送，因此请在 TACACS+ 服务器上将命令配置为外壳命令。

注释 思科安全 ACS 可能包括名为“pix-shell”的命令类型。请勿将此类型用于 ASA 命令授权。

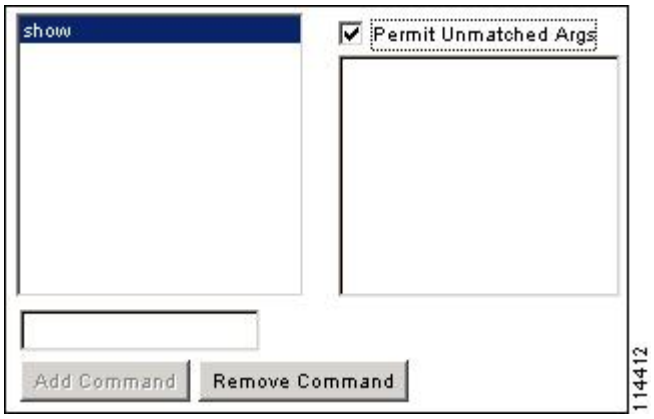
- 命令的第一个词被视为主命令。所有附加的单词都被视为参数，需要在其前面放置 **permit** 或 **deny**。

  例如，如要允许 **show running-configuration aaa-server** 命令，请向命令字段添加 **show running-configuration**，然后在参数字段键入 **permit aaa-server**。

- 通过选中 **Permit Unmatched Args** 复选框，可以允许未明确拒绝的所有命令参数。

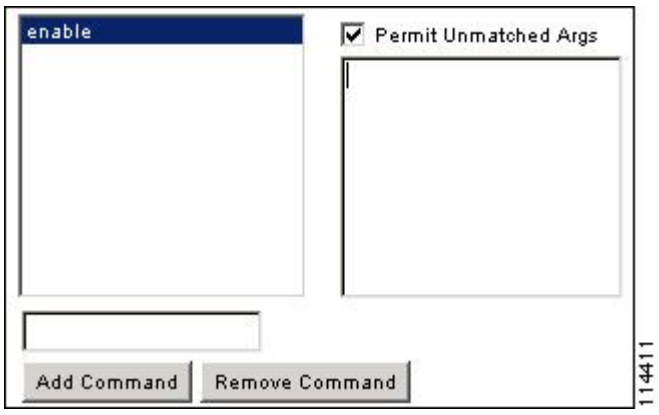
  例如，您可以仅配置 **show** 命令，那么将允许所有 **show** 命令。建议使用此方法，这样您就无需预测命令的每个变体（包括缩写和问号），其显示 CLI 的使用情况（请参阅下图）。

图 *1:* 允许所有相关命令



- 对于单个单词的命令，即使命令没有参数，也必须允许不匹配的参数，例如 **enable** 或 **help**（请参见下图）。

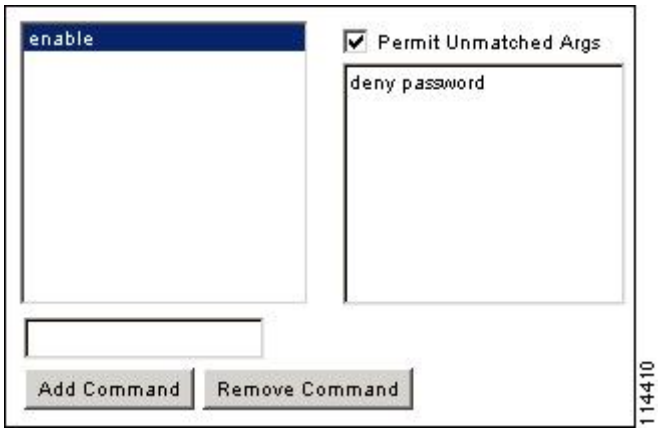
图 *2:* 允许单个单词的命令



- 如要禁止某些参数，请输入参数并在前面放置 **deny**。

  例如，如要允许 **enable**，但不允许 **enable password**，请在命令字段中输入 **enable**，在参数字段内输入 **deny password**。确保选中 **Permit Unmatched Args** 复选框，这样仍能允许单独使用的 **enable**（请参见下图）。

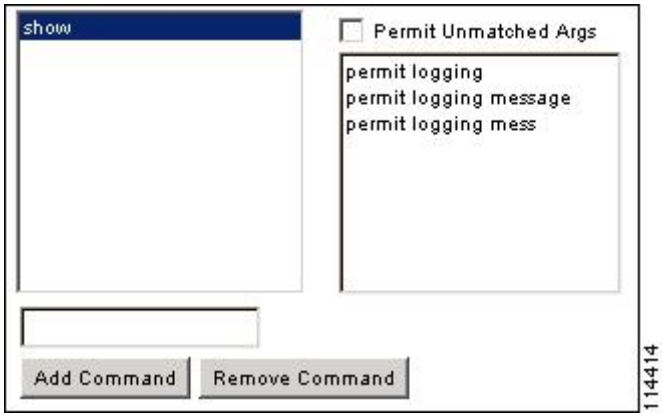
图 *3:* 禁止参数



- 当您在命令行中缩写命令时，ASA 会将前缀和主命令扩展为全文，但对附加的参数却按照您输入的原样发送到 TACACS+ 服务器。

  例如，如果您输入 **sh log**，那么 ASA 将整个 **show logging** 命令发送到 TACACS+ 服务器。但是，如果您输入 **sh log mess**，那么 ASA 将 **show logging mess** 命令发送到 TACACS+ 服务器，而不是发送扩展的 **show logging message** 命令。您可以配置同一个参数的多种拼法以便预测其缩写（请参阅下图）。

图 *4:* 指定缩写



- 建议您允许所有用户使用以下基本命令：
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**

- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

配置 TACACS+ 命令授权

如果启用TACACS+命令授权，且用户在CLI上输入命令，ASA会将命令和用户名发送到TACACS+服务器以确定命令是否已授权。

在启用 TACACS+ 命令授权之前，请务必以 TACACS+ 服务器上定义的用户身份登录 ASA，并确保您具有必要的命令授权来继续配置 ASA。例如，您应该以获得所有命令授权的管理员用户身份登录。否则，可能会意外锁定。

在您确定配置会按预期方式运行之前，请勿保存配置。如果您因错误被锁定，通常可以通过重启 ASA 来恢复访问。

请确保您的TACACS+系统完全稳定且可靠。必要的可靠性级别通常需要您具有完全冗余的TACACS+服务器系统和完全冗余的与 ASA 的连接性。例如，在您的 TACACS+ 服务器池中包括一个与接口 1 连接的服务器和另一个与接口 2 连接的服务器。您还可以将本地命令授权配置为在 TACACS+ 服务器不可用时的回退方法。

如要使用 TACACS+ 服务器配置命令授权，请执行以下步骤：

过程

输入以下命令：

aaa authorization command *tacacs+_server_group* [**LOCAL**]

示例：

```
ciscoasa(config)# aaa authorization command tacacs+_server_group [LOCAL]
```

您可以将 ASA 配置为在 TACACS+ 服务器不可用时使用本地数据库作为回退方法。如要启用回退，请指定服务器组名后跟 **LOCAL**（**LOCAL** 区分大小写）。建议在本地数据库中使用与 TACACS+ 服务器相同的用户名和密码，因为 ASA 提示符不会给出使用何种方法的任何指示。请确保在本地数据库和命令权限级别中配置用户。

为本地数据库用户配置密码策略

使用本地数据库配置用于CLI或ASDM访问的身份验证时，可以配置密码策略来要求用户在指定时间后更改密码并规定密码标准，例如最短长度和更改后的最小字符数。

密码策略仅适用于使用本地数据库的管理用户，而不适用于可以使用本地数据库的其他流量类型（例如用于网络访问的VPN或AAA流量），也不适用于通过AAA服务器进行身份验证的用户。

配置密码策略后，当您更改密码（自己本人的或其他用户的）时，密码策略将应用于新密码。所有现有密码都将成为祖父。新策略将应用于使用**username**命令以及**change-password** 命令更改密码。

开始之前

- 使用本地数据库为 CLI 或 ASDM 访问配置 AAA 身份验证。
- 在本地数据库中制定用户名。

过程

步骤 1 （可选）设置远程用户的密码多久之后到期（以天为单位）。

password-policy lifetime 天

示例：

```
ciscoasa(config)# password-policy lifetime 180
```

注释 控制台端口的用户不会由于密码到期而锁定。

有效值为 0 到 65536 天。默认值为 0 天，表示密码不会到期。

密码到期之前七天，将会显示一条警告消息。在密码到期后，拒绝远程用户访问系统。如要在到期后访问，请执行以下操作之一：

- 请另一位管理员使用 **username** 命令更改密码。
- 登录到物理控制台端口更改密码。

步骤 2 （可选）设置与旧密码相比，新密码中必须更改的最小字符数。

password-policy minimum-changes *value*

示例：

```
ciscoasa(config)# password-policy minimum-changes 2
```

有效值为 0 和 64 个字符之间。默认值为 0。

字符匹配与位置无关，意味着只有新密码字符不在当前密码的任何地方出现时才视为被更改。

步骤 3 （可选）设置密码最小长度。

password-policy minimum-length 值

示例：

```
ciscoasa(config)# password-policy minimum-length 8
```

有效值为 3 和 64 个字符之间。建议最小密码长度为 8 个字符。

步骤 4 （可选）设置密码必须具有的最小大写字符数。

password-policy minimum-uppercase 值

示例：

```
ciscoasa(config)# password-policy  minimum-uppercase 3
```

有效值为 0 和 64 个字符之间。默认值为 0，表示无最小数。

步骤 5 （可选）设置密码必须具有的最小小写字符数。

password-policy minimum-lowercase 值

示例：

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

有效值为 0 和 64 个字符之间。默认值为 0，表示无最小数。

步骤 6 （可选）设置密码必须具有的最小数字字符数。

password-policy minimum-numeric *value*

示例：

```
ciscoasa(config)# password-policy minimum-numeric 1
```

有效值为 0 和 64 个字符之间。默认值为 0，表示无最小数。

步骤 7 （可选）设置密码必须具有的最小特殊字符数。

password-policy minimum-special 值

示例：

```
ciscoasa(config)# password-policy minimum-special 2
```

有效值为 0 和 64 个字符之间。特殊字符包括以下字符：!、@、#、$、%、^、&、*、“（”和“）”。默认值为 0，表示无最小数。

步骤 8 禁止重用密码：

password-policy reuse-interval 值

示例：

```
ciscoasa(config)# password-policy reuse-interval 5
```

您可以禁止重用与之前使用的密码（2 至 7 个之前的密码）相匹配的密码。之前的密码使用 **password-history** 命令以加密形式存储在每个用户名下的配置中；此命令用户不可配置。

步骤 9 禁止使用与用户名匹配的密码：

password-policy username-check

步骤 10 （可选）设置用户是否必须使用 **change-password** 命令更改密码，而不是让用户使用 **username** 命令更改密码。

password-policy authenticate enable

示例：

```
ciscoasa(config)# password-policy authenticate enable
```

默认设置为禁用：用户可以使用其中任一种方法更改密码。

如果启用此功能并尝试使用 **username** 命令更改密码，将会出现以下错误消息：

```
ERROR: Changing your own password is prohibited
```

也不能使用 **clear configure username** 命令删除自己的帐户。如果尝试这样做，系统将会显示以下错误消息：

```
ERROR: You cannot delete all usernames because you are not allowed to delete yourself
```

更改密码

如果在密码策略中配置了密码有效期，则需要在旧密码到期时将密码更改为新密码。如果启用密码策略身份验证，则要求用此密码更改方法。如果未启用密码策略身份验证，则既可以使用此方法也可以直接更改用户帐户。

如要更改用户名密码，请执行以下步骤：

过程

输入以下命令：

change-password [**old-password** *old_password* [**new-password** *new_password*]]

示例：

```
ciscoasa# change-password old-password j0hncr1chton new-password a3rynsun
```

如果未在命令中输入旧密码和新密码，ASA 会提示您输入。

启用和查看登录历史

默认情况下，登录历史记录将保存 90 天。可以禁用此功能，也可更改持续时间，最多 365 天。

开始之前

- 登录历史仅按设备保存；在故障转移和集群环境中，每台设备都仅保留其自己的登录历史。
- 在重新加载后，不会保留登录历史数据。
- 当您为一种或多种 CLI 管理方法（SSH、ASDM、串行控制台）启用本地 AAA 身份验证时，此功能将适用于本地数据库中或来自 AAA 服务器的用户名。ASDM 登录不会保存在历史中。

过程

步骤 1 设置登录历史持续时间：

aaa authentication login-history duration 天

示例：

```
ciscoasa(config)# aaa authentication login-history duration 365
```

可以将 *days* 设置为 1 到 365 之间。默认值为 90。要禁用登录历史记录，请输入 **no aaa authentication login-history**。

当用户登录时，他们将看到其自己的登录历史，如此 SSH 示例：

```
cugel@10.86.194.108's password:
The privilege level for user cugel is 15.  The privilege level at the previous login was
2.
User cugel logged in to ciscoasa at 21:04:10 UTC Dec 14 2016
Last login: 21:01:44 UTC Dec 14 2016 from ciscoasa console
Successful logins over the last 90 days: 6
Authentication failures since the last login: 0
Type help or '?' for a list of available commands.
ciscoasa>
```

步骤 2 查看登录历史：

show aaa login-history [**user** 名称]

示例：

```
ciscoasa(config)# show aaa login-history
Login history for user:    turjan
Logins in last   1 days:   1
```

```
Last successful login:     16:44:32 UTC Jul 23 2018 from console
Failures since last login: 0
Last failed login:         None
Privilege level:                                    14
Privilege level changed from 11 to 14 at:           14:07:30 UTC Aug 21 2018
```

配置管理访问记帐

在 CLI 中输入 **show** 命令之外的任何命令时，可以将记帐消息发送到 TACACS+ 记帐服务器。您可以配置在用户登录时、输入 **enable** 命令时或者发出命令时记帐。

对于命令记帐，只能使用 TACACS+ 服务器。

如要配置管理访问和 enable 命令记帐，请执行以下步骤：

过程

步骤 1 输入以下命令：

aaa accounting {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag*

示例：

```
ciscoasa(config)# aaa accounting telnet console group_1
```

有效的服务器组协议是 RADIUS 和 TACACS+。

步骤 2 启用命令记帐。只有 TACACS+ 服务器支持命令记帐。

aaa accounting command [**privilege** *level*] *server-tag*

示例：

```
ciscoasa(config)# aaa accounting command privilege 15 group_1
```

privilege *level* 关键字参数对是最低权限级别，而 *server-tag* 参数是 ASA 应将命令记帐消息发送到的 TACACS+ 服务器组的名称。

从锁定中恢复

在某些情况下，当您打开命令授权或 CLI 身份验证时，可能会被锁定退出 ASA CLI。通常，重启 ASA 即可恢复访问。但是，如果您已经保存配置，则可能会被锁定。

下表列出了常见锁定条件以及如何从中恢复：

表 *1: CLI* 身份验证和命令授权锁定情景

功能	锁定条件	说明	解决方法： 单模	解决方法： 多模
本地 CLI 身份验证	未在本地数据库中配置用户。	如果本地数据库中没有用户，则您无法登录，并且无法添加任何用户。	登录并重置密码和 **aaa** 命令。	使用会话从交换机登录 ASA。您可以从系统执行空间更改为情景并添加用户。
TACACS+ 命令授权 TACACS+ CLI 身份验证 RADIUS CLI 身份验证	服务器关闭或无法访问，且没有配置回退方法。	如果服务器无法访问，则您无法登录或无法输入任何命令。	**1.** 登录并重置密码和 AAA 命令。 **2.** 将本地数据库配置为回退方法，这样您就不会在服务器关闭时被锁定。	**1.** 如果由于 ASA 上的网络配置不正确而无法访问服务器，请使用会话从交换机登录 ASA。您可以从系统执行空间更改为情景并重新配置网络设置。 **2.** 将本地数据库配置为回退方法，这样您就不会在服务器关闭时被锁定。
TACACS+ 命令授权	您以没有足够权限的用户身份或不存在的用户身份登录。	启用命令授权，但是随后发现用户无法再输入任何命令。	修复 TACACS+ 服务器用户帐户。 如果您没有访问 TACACS+ 服务器的权限并需要立即配置 ASA，可登录到维护分区并重置密码和 **aaa** 命令。	使用会话从交换机登录 ASA。您可以从系统执行空间更改为情景并完成配置更改。您也可以禁用命令授权，直到修复 TACACS+ 配置。
本地命令授权	您以没有足够权限的用户身份登录。	启用命令授权，但是随后发现用户无法再输入任何命令。	登录并重置密码和 **aaa** 命令。	使用会话从交换机登录 ASA。您可以从系统执行空间更改为情景并更改用户级别。

监控设备访问

请参阅以下命令来监控设备访问：

- **show running-config all privilege all**

  此命令显示所有命令的权限级别。

  对于 **show running-config all privilege all** 命令，ASA 将显示当前为每个 CLI 命令分配的权限级别。以下是此命令的输出示例：

```
ciscoasa(config)# show running-config all  privilege all
```

```
privilege show level 15 command aaa
privilege clear level 15 command aaa
privilege configure level 15 command aaa
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
privilege show level 15 command activation-key
privilege configure level 15 command activation-key
...
```

- **show running-config privilege level** 级别

  此命令显示特定权限级别的命令。level 参数是介于 0 和 15 之间的整数。

  以下示例显示 10 级权限的命令分配：

```
ciscoasa(config)# show running-config all privilege level 10
privilege show level 10 command aaa
```

- **show running-config privilege command** 命令

  此命令用于显示特定命令的权限级别。

  以下示例显示 **access-list** 命令的命令分配：

```
ciscoasa(config)# show running-config all privilege command access-list
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
```

- **show curpriv**

  此命令用于显示当前登录的用户。

  以下是 **show curpriv** 命令的输出示例：

```
ciscoasa# show curpriv
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```

  下表显示 **show curpriv** 命令的输出。

表 *2: show curpriv* 命令输出说明

字段	说明
用户名	用户名、如果您以默认用户身份登录，则名称是 enable_1（用户 EXEC）或 enable_15（特权 EXEC）。

字段	说明
Current privilege level	级别范围为0到15。除非您配置本地命令授权并为中间权限级别分配命令，否则只能使用 0 级和 15 级。
Current Modes	可用的访问模式如下： • P_UNPR - 用户 EXEC 模式（0 级和 1 级） • P_PRIV - 特权 EXEC 模式（2 级到 15 级） • P_CONF - 配置模式

- **show quota management-session** [**ssh** | **telnet** | **http** | **username** *user*]

  此命令用于显示当前正在使用的会话。

  以下是 **show quota management-session** 命令的输出示例：

```
ciscoasa(config)#show quota management-session

#Sessions               ConnectionType                  Username
1                             SSH                        cisco
2                             TELNET                     cisco
1                             SSH                        cisco1
```

- **show aaa login-history** [**user** 名称]

  此命令用于显示每个用户的登录历史记录。

  以下是 **show aaa login-history** 命令的输出示例。

```
ciscoasa(config)# show aaa login-history
Login history for user:    turjan
Logins in last   1 days:   1
Last successful login:     16:44:32 UTC Jul 23 2018 from console
Failures since last login: 0
Last failed login:         None
Privilege level:                                    14
Privilege level changed from 11 to 14 at:           14:07:30 UTC Aug 21 2018
```

管理访问的历史记录

表 *3:* 管理访问的历史记录

功能名称	平台版本	说明
环回接口支持 SSH 和 Telnet	9.18(2)	您现在可以添加环回接口并用于以下功能： • SSH • Telnet 新增/修改的命令：**interface loopback**、**ssh**、**telnet**
思科 SSH 堆栈	9.17(1)	ASA 使用专有 SSH 堆栈进行 SSH 连接。现在，您可以选择使用基于 OpenSSH 的 CiscoSSH 堆栈。默认堆栈继续为ASA堆栈。思科SSH支持： • FIPS 合规性 • 定期更新，包括来自思科和开源社区的更新 请注意，CiscoSSH 堆栈不支持以下功能： • 通过VPN通过SSH连接到其他接口（管理访问） • EdDSA 密钥对 • FIPS模式下的RSA密钥对 如果需要这些功能，应继续使用ASA SSH堆栈。 CiscoSSH 堆栈的 SCP 功能略有变化：要使用 ASA **copy** 命令将文件复制到 SCP 服务器或从 SCP 服务器复制文件，您必须使用**ssh**命令在 ASA 上为 SCP 服务器子网/主机启用 SSH 访问权限。 新增/修改的命令：**ssh stack ciscossh**
本地用户锁定更改	9.17(1)	ASA 可以在登录尝试失败达到可配置次数之后锁定账户。此功能不适用于权限级别为 15 的用户。此外，用户将被无限期锁定，直到管理员解锁其账户。现在，用户将在 10 分钟后解锁，除非管理员在此之前使用 **clear aaa local user lockout** 命令。权限级别为 15 的用户现在也受锁定设置的影响。 新增/修改的命令：**aaa local authentication attempts max-fail** 、**show aaa local user**

功能名称	平台版本	说明
SSH 和 Telnet 密码更改提示	9.17(1)	本地用户首次使用 SSH 或 Telnet 登录 ASA 时，系统会提示他们更改密码。在管理员更改密码后，系统还会提示他们进行首次登录。但是，如果 ASA 重新加载，则系统不会提示用户，即使是首次登录也是如此。 请注意，任何使用本地用户数据库的服务（例如 VPN）也必须使用在 SSH 或 Telnet 登录期间更改的新密码。 新增/修改的命令：**show aaa local user**
SSH 安全性改进	9.16（1）	SSH 现在支持以下安全性改进： • 主机密钥格式 - **crypto key generate** {**eddsa** | **ecdsa**}. 除了 RSA，我们还增加了对 EdDSA 和 ECDSA 主机密钥的支持。如果密钥存在，ASA 会尝试按以下顺序使用：EdDSA、ECDSA，然后是 RSA。如果使用 **ssh key-exchange hostkey rsa** 命令将 ASA 显式配置为使用 RSA 密钥，则必须生成 2048 位或更高位的密钥。为了实现升级兼容性，仅当使用默认主机密钥设置时，ASA才会使用较小的RSA主机密钥。RSA支持将在更高版本中删除。 • 密钥交换算法 - **ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**} • 加密算法 -**ssh cipher encryption chacha20-poly1305@openssh.com** • 不再支持 SSH 版本 1 - 已删除 **ssh version** 命令。 新增/修改的命令： **crypto key generate eddsa**、 **crypto key zeroize eddsa**、 **show crypto key mypubkey**、 **ssh cipher encryption chacha20-poly1305@openssh.com**、 **ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**}、 **ssh key-exchange hostkey**、 **ssh version**
SNMP 的管理访问	9.14(2)	在配置通过 VPN 隧道的管理访问时，在加密映射访问列表中包含外部接口的 IP 地址，作为通过站点间 VPN 进行安全 SNMP 轮询的 VPN 配置的一部分。
HTTPS 空闲超时设置	9.14(1)	现在，您可以为 ASA 的所有 HTTPS 连接设置空闲超时，包括 ASDM、WebVPN 和其他客户端。以前，使用 **http server idle-timeout** 命令只能设置 ASDM 空闲超时。如果同时设置两个超时，新命令优先执行。 新增/修改的命令：**http connection idle-timeout**

功能名称	平台版本	说明
SSH加密密码现在按预定义列表的安全性从最高到最低的顺序列出	9.13(1)	SSH加密密码现在按预定义列表（例如中等或高安全性）的安全性从最高到最低的顺序列出。在较早的版本中，它们是按从最低到最高的顺序列出的，这意味着低安全性密码的提议先于高安全性密码。 新增/修改的命令：**ssh cipher encryption**
仅限在管理情景中设置SSH密钥交换模式	9.12(2)	您必须在 Admin 情景中设置 SSH 密钥交换；所有其他情景将继承此设置。 新增/修改的命令：**ssh key-exchange**
现在登录时需要更改 **enable** 密码	9.12(1)	**enable**默认密码为空。现在，如果您尝试在ASA上进入特权EXEC模式，系统会要求您将密码改为一个至少包含3个字符的值，而不能将密码留空。**no enable password** 命令今后将不受支持。 在 CLI 中，您可以使用 **enable** 命令、**login** 命令（用户权限级别应在 2 级以上）或者 SSH 或 Telnet 会话（如果启用 **aaa authorization exec auto-enable**）来进入特权 EXEC 模式。无论使用哪种方法，您都必须设置密码。 但是在登录ASDM时，则没有这项更改密码的要求。默认情况下，在 ASDM 中，您无需使用用户名和 **enable** 密码即可登录。 新增/修改的命令：**enable password**
可配置管理会话限制	9.12(1)	现在，您可以配置汇聚管理会话数、每用户管理会话数和每协议管理会话数的最大值。以前，您只能配置汇聚会话数。此功能不会影响控制台会话。需要注意的是，在多情景模式下，如果最大HTTPS会话数固定为5，则无法配置会话数。此外，系统配置中也不再接受**quota management-session** 命令，您只能在情景配置中进行此设置。现在，最大汇聚会话数为 15。如果您已将其配置为 0（无限制）或大于 16 的值，在升级设备时，此值会自动更改为 15。 新增/修改的命令： **quota management-session**、**show quota management-session**
管理权限级别更改通知	9.12(1)	现在，在您授予访问权限 (**aaa authentication enable console**) 或允许直接进行特权 EXEC 访问 (**aaa authorization exec auto-enable**) 后，如果用户已分配的访问权限级别在上次登录后发生更改，ASA 会向用户显示通知。 新增/修改的命令：**show aaa login-history**

功能名称	平台版本	说明
SSH 增强安全性	9.12(1)	请参阅以下 SSH 安全改进： • 支持 Diffie-Hellman 组 14 SHA256 密钥交换。此设置现在为默认值。先前默认值为组 1 SHA1。 • 支持 HMAC-SHA256 完整性加密。默认值现在是高安全性密码组（仅 hmac-sha2-256）。先前默认值为介质集。 新增/修改的命令：**ssh cipher integrity** 、**ssh key-exchange group dh-group14-sha256**
允许基于非浏览器的 HTTPS 客户端访问 ASA	9.12(1)	您可以允许基于非浏览器的 HTTPS 客户端访问 ASA 上的 HTTPS 服务。默认情况下，允许 ASDM、CSM 和 REST API。 新增/修改的命令：**http server basic-auth-client**
RSA 密钥对支持 3072 位密钥	9.9(2)	您现在可以将模数长度设为 3072。 新增或修改的命令：**crypto key generate rsa modulus**
网桥虚拟机 (BVI) 上的 VPN 管理访问	9.9(2)	现在，如果在 BVI 上启用了 VPN **management-access**，可以在该 BVI 上启用管理服务（例如 **telnet**、**http** 和 **ssh**）。对于非 VPN 管理访问，应在网桥组成员接口上继续配置这些服务。 新增或修改的命令：**https**、**telnet**、**ssh**、**management-access**
已弃用 SSH 版本 1	9.9(1)	SSH 版本 1 已弃用，未来不再发行。默认设置已从 SSH v1 和 v2 更改为仅 SSH v2。 新增/修改的命令：**ssh version**
对使用SSH公钥身份验证的用户和具有密码的用户分别进行单独的身份验证	9.6(3)/9.8(1)	在 9.6(2) 以前的版本中，您在启用 SSH 公钥身份验证 (**ssh authentication**)时，可以不必明确启用基于本地用户数据库的AAA SSH 身份验证 (**aaa authentication ssh console LOCAL**)。在 9.6(2) 中，ASA 要求明确启用 AAA SSH 身份验证。在此版本中，您不再需要明确启用 AAA SSH 身份验证；当您为用户配置 **ssh authentication** 命令时，默认情况下会为使用此类型身份验证的用户启用本地身份验证。此外，在明确配置 AAA SSH 身份验证时，此配置将仅适用于具有密码的用户名，并且可以使用任何 AAA 服务器类型（例如 **aaa authentication ssh console radius_1**）。例如，某些用户可以使用公钥身份验证（使用本地数据库），而其他用户则可配合使用密码和 RADIUS。 未修改任何命令。

功能名称	平台版本	说明
登录历史	9.8(1)	默认情况下，登录历史记录将保存 90 天。可以禁用此功能，也可更改持续时间，最多365天。仅当为一种或多种管理方法（SSH、ASDM、Telnet 等）启用本地 AAA 身份验证时，此功能才适用于本地数据库中的用户名。 引入了以下命令：**aaa authentication login-history**、**show aaa login-history**
禁止重复使用密码以及禁止使用与某一用户名匹配的密码的密码策略实施	9.8(1)	现在，可以禁止重复使用过去的密码（最多7代），还可以禁止使用与某一用户名匹配的密码。 引入了以下命令：**password-history**、**password-policy reuse-interval**、**password-policy username-check**
ASDM 的 ASA SSL 服务器模式匹配	9.6(2)	对于通过证书进行身份验证的 ASDM 用户，您现在可以要求证书与证书映射匹配。 修改了以下命令：**http authentication-certificate match**
SSH 公钥身份验证改进	9.6(2)	在更早的版本中，您在启用SSH 公钥身份验证 (**ssh authentication**) 时，可以不必启用基于本地用户数据库的 AAA SSH 身份验证 (**aaa authentication ssh console LOCAL**)。该配置现在已修复，您必须明确启用 AAA SSH 身份验证。要禁止用户使用密码而不是私钥，现在您可以创建未定义任何密码的用户名。 修改了以下命令：**ssh authentication**、**username**。
ASDM 管理授权	9.4(1)	现在可以单独为 HTTP 访问与 Telnet 和 SSH 访问配置管理授权。 引入了以下命令：**aaa authorization http console**
证书配置中的 ASDM 用户名	9.4(1)	当启用 ASDM 证书身份验证 (**http authentication-certificate**) 时，可以配置 ASDM 从证书提取用户名的方式；还可以在出现登录提示时启用用户名预填充功能。 引入了以下命令：**http username-from-certificate**
改进的一次性密码身份验证	9.2(1)	有足够授权权限的管理员可以通过输入自己的身份验证凭证一次进入特权 EXEC 模式。**aaa authorization exec** 命令中添加了 **auto-enable** 选项。 修改了以下命令：**aaa authorization exec**。
对 IPV6 的 HTTP 重定向支持	9.1(7)/9.6(1)	现在，在为 ASDM 接入或无客户端 SSL VPN 启用 HTTP 重定向到 HTTPS 时，可将已发送的流量重定向到 IPv6 地址。 向以下命令添加了功能：**http redirect**

功能名称	平台版本	说明
可配置 SSH 加密和完整性密码	9.1(7)9.4(3)9.5(3)9.6(1)	用户可在执行 SSH 加密管理时选择密码模式，并可配置 HMAC 和加密来改变密钥交换算法。根据您的应用，您可能希望将密码变得更加严格或更不严格。请注意，安全复制的性能部分取决于所使用的加密密码。默认情况下，ASA 会按顺序协商以下其中一种算法：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr。如果选择建议的第一种算法 (3des-cbc)，则性能会远远慢于 128-cbc 等更高效的算法。例如，要更改所需的密码，请使用 **ssh cipher encryption custom aes128-cbc**。 引入了以下命令：**ssh cipher encryption, ssh cipher integrity**。
SSH 的 AES-CTR 加密	9.1(2)	ASA 中的 SSH 服务器实施现在支持 AES-CTR 模式加密。
改进的 SSH 重新生成密钥间隔	9.1(2)	在连接时间达到 60 分钟后或数据流量达到 1 GB 后，SSH 连接重新生成密钥。 引入了以下命令：**show ssh sessions detail**。
对于在多情景模式下的 ASASM，支持从交换机进行 Telnet 和虚拟控制台身份验证。	8.5(1)	虽然从多情景模式下的交换机连接至 ASASM 将连接至系统执行空间，但是可以在管理员情景中配置身份验证来监管这些连接。
使用本地数据库时，支持管理员密码策略	8.4(4.1)、9.1(2)	使用本地数据库配置用于 CLI 或 ASDM 访问的身份验证时，可以配置密码策略来要求用户在指定时间后更改密码并规定密码标准，例如最短长度和更改后的最小字符数。 引入了以下命令：**change-password**、**password-policy lifetime**、**password-policy minimum changes**、**password-policy minimum-length**、**password-policy minimum-lowercase**、**password-policy minimum-uppercase**、**password-policy minimum-numeric**、**password-policy minimum-special**、**password-policy authenticate enable**、**clear configure password-policy**、**show running-config password-policy**。
支持 SSH 公钥身份验证	8.4(4.1)、9.1(2)	对于与 ASA 的 SSH 连接，您可以基于每个用户启用公钥身份验证。您可以指定公钥文件 (PKF) 格式的密钥或 Base64 密钥。PKF 密钥的长度可达 4096 位。对于由于过长而导致 ASA 不支持使用 Base64 格式（限长 2048 位）的密钥，请使用 PKF 格式。 引入了以下命令：**ssh authentication**。 仅在 *9.1(2)* 及更高版本中支持 *PKF* 密钥格式。
支持用于 SSH 密钥交换的 Diffie-Hellman 组 14	8.4(4.1)、9.1(2)	已添加支持 Diffie-Hellman 组 14 进行 SSH 密钥交换。以前，只支持组 1。 引入了以下命令：**ssh key-exchange**。

功能名称	平台版本	说明
支持的管理会话最大数量	8.4(4.1)、9.1(2)	您可以设置并发 ASDM、SSH 和 Telnet 会话的最大数量。 引入了以下命令：**quota management-session**、**show running-config quota management-session**、**show quota management-session**。
提高了 SSH 安全性；不再支持 SSH 默认用户名。	8.4(2)	从 8.4(2) 开始，您无法再使用 pix 或 asa 用户名和登录密码通过 SSH 连接至 ASA。如要使用 SSH，必须使用 **aaa authentication ssh console LOCAL** 命令 (CLI) 或“配置 \> 设备管理 \> 用户/AAA \> AAA 访问 \> 身份验证 (ASDM)”来配置 AAA 身份验证；然后通过输入 **username** 命令 (CLI) 或依次选择“配置 \> 设备管理 \> 用户/AAA \> 用户帐户 (ASDM)”来定义本地用户。如果要使用 AAA 服务器而不是本地数据库进行身份验证，建议也将本地身份验证配置为备用方法。
管理访问	7.0(1)	引入了此功能。 引入了以下命令： **show running-config all privilege all**、**show running-config privilege level**、**show running-config privilege command**、**telnet**、**telnet timeout**、**ssh**、**ssh timeout**、**http**、**http server enable**、**asdm image disk**、**banner**、**console timeout**、**icmp**、**ipv6 icmp**、**management access**、**aaa authentication console**、**aaa authentication enable console**、**aaa authentication telnet | ssh console**、**service-type**、**login**、**privilege**、**aaa authentication exec authentication-server**、**aaa authentication command LOCAL**、**aaa accounting serial | telnet | ssh | enable console**、**show curpriv**、**aaa accounting command privilege**。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。