软件和配置

本章介绍如何管理 ASA 软件和配置。

升级软件

有关完整的升级过程，请参阅《思科 ASA 升级指南》。

使用 ROMMON 加载映像（ISA 3000）

要使用 TFTP 从 ROMMON 模式下将软件映像加载到 ASA，请执行以下步骤。

过程

步骤 1 根据访问 ISA 3000 控制台中的说明连接到 ASA 控制台端口。

步骤 2 关闭 ASA，然后重新启动。

步骤 3 在启动过程中，当系统提示您进入 ROMMON 模式时，请按 **Escape** 键。

步骤 4 在 ROMMOM 模式下，定义 ASA 的接口设置，包括 IP 地址、TFTP 服务器地址、网关地址、软件映像文件和端口，如下所示：

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

注释　请确保已存在网络连接。

interface 命令在 ASA 5506-X、ASA 5508-X、ASA 5516-X 和 ISA 3000 平台上将被忽略，您必须从管理 1/1 接口对这些平台执行 TFTP 恢复。

步骤 5 验证您的设置：

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

步骤 6 对 TFTP 服务器执行 ping 操作：

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

步骤 7 保存网络设置，以备将来使用：

```
rommon #8> sync
Updating NVRAM Parameters...
```

步骤 8 加载软件映像：

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21
```

```
Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

成功加载软件映像后，ASA 会自动退出 ROMMON 模式。

步骤 9 从ROMMON 模式启动 ASA 不会在重新加载时保留系统映像；您仍需将映像下载到闪存。有关完整的升级过程，请参阅《思科 ASA 升级指南 》。

升级 ROMMON 映像（ISA 3000）

按照以下步骤升级 ISA 3000 的 ROMMON 映像。对于 ASA 型号，系统上的 ROMMON 版本必须为 1.1.8 或更高版本。我们建议您将引擎升级到最新版本。

您只能升级到新版本；无法降级。

⚠

注意 适用于 1.1.15 的 ASA 5506-X，5508-X 和 5516-X ROMMON 升级，以及适用于 1.0 的 ISA 3000 ROMMON 升级。并且，1.0.5 的 ISA 3000 ROMMON 升级时间为过去 ROMMON 版本的两倍，大约需要 15 分钟。升级流程中**请勿**重启设备 。如果升级未在 30 分钟内完成或升级失败，请联系思科技术支持； **请勿**重启或重置设备。

开始之前

从Cisco.com 获取新的ROMMON映像，并将其放在服务器上以复制到 ASA。ASA 支持FTP、TFTP、SCP、HTTP(S) 和 SMB 服务器。请从以下网址下载映像：

- ISA 3000：https://software.cisco.com/download/home/286288493/type

过程

步骤 1 将 ROMMON 映像复制到 ASA 闪存。此程序显示 FTP 副本；输入 **copy ?**，使用其他服务器类型的语法。

copy ftp://[*username*:*password*@]*server_ip*/**asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

步骤 2 要查看当前版本，请输入 **show module** 命令并在 MAC 地址范围表中查看 Mod 1 的输出中的固件版本：

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
```

```
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

步骤 3 升级 ROMMON 映像：

upgrade rommon disk0:asa5500-firmware-*xxxx*.SPA

示例：

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

步骤 4 当出现提示时，确认重新加载 ASA。

ASA 将升级 ROMMON 映像，然后重新加载操作系统。

降级软件

在许多情况下，您可以降级ASA软件并从以前的软件版本恢复备份配置。降级方法取决于您的ASA平台。

降级的准则和限制

降级前请参阅以下准则：

- **没有对集群的官方零停机降级支持**-但是，在某些情况下，零停机降级将起作用。关于降级，请参阅以下已知问题；请注意，可能会有其他需要您重新加载集群设备的问题，这会导致停机。

- **降级到具有集群功能的 9.9(1) 以前版本**- 9.9(1) 及更高版本包含备份分发方面的改进。如果您的集群中有 3 个或更多个设备，您必须执行以下步骤：
  1. 从集群中删除所有辅助设备（使得集群仅包含主设备）。
  2. 将 1 个辅助设备降级，然后重新加入集群。
  3. 禁用主设备上的集群功能；将其降级，然后重新加入集群。
  4. 一次一个，将剩余的辅助设备降级，然后重新加入集群。
- **在启用集群站点冗余时降级到 9.9(1) 以前的版本**- 如果您想要降级（或如果您想要将 9.9(1) 以前版本的设备添加到集群），您应该禁用站点冗余。否则，您会看到副作用，例如运行旧版本的设备上出现虚拟转发数据流。
- **在集群和加密映射的情况下从 9.8(1) 降级**- 如果配置了加密映射，则在从 9.8(1) 降级时，将没有零停机时间降级支持。应在降级之前清除加密映射配置，在降级之后再重新应用该配置。
- **在将集群设备运行状态检查设置为 0.3 到 0.7 秒的情况下从 9.8(1) 降级**- 如果在将保持时间 (**health-check holdtime**) 设置为 0.3 - 0.7 秒后降级 ASA 软件，则此设置将恢复为 3 秒的默认值，因为不支持新设置。
- **在集群的情况下从 9.5(2) 或更高版本降级到 9.5(1) 或早期版本 (CSCuv82933)**-在从 9.5(2) 降级时，将没有零停机时间降级支持。您必须大致在同一时间重新加载所有设备，这样当设备恢复在线时可形成新的集群。如果您等待所有设备按顺序重新加载完，则无法形成集群。
- **在集群的情况下从 9.2(1) 或更高版本降级到 9.1 或早期版本**- 不支持零停机时间降级。

- **从 9.18 或更高版本降级问题**- 9.18 中的行为发生变化，其中 **访问组** 命令将在其 **访问组** 命令之前列出。如果降级， **访问组** 命令将被拒绝，因为它尚未加载 **访问组** 命令。即使您之前已启用 **forward-reference enable** 命令，也会出现此结果，因为该命令现在已被删除。在降级之前，请确保手动复制所有 **访问组** 命令，然后在降级后重新输入这些命令。
- **从9.10（1）降级以进行智能许可**-由于智能代理中的更改，如果您进行降级，则必须将设备重新注册到思科智能软件管理器。新的智能代理使用加密文件，因此您需要重新注册才能使用旧智能代理所需的未加密文件。
- **使用 PBKDF2（基于密码的密钥派生功能 2）散列处理，利用密码降级到 9.5 和早期版本**- 9.6 以前的版本不支持 PBKDF2 散列处理。在 9.6(1) 中，长度超过 32 个字符的 **enable** 和 **username** 密码使用 PBKDF2 散列处理。在 9.7(1) 中，所有长度的新密码都将使用 PBKDF2 散列处理（现有密码继续使用 MD5 散列处理）。如果降级，则 **enable** 密码将恢复为默认值（空白）。用户名不会正确解析，并将删除 **username** 命令。必须重新创建本地用户。
- **对于 ASA Virtual从版本 9.5(2.200) 降级**- ASA virtual 不会保留许可注册状态。您需使用 **license smart register idtoken id_token force** 命令重新注册（对于 ASDM：请参阅 **Configuration > Device Management > Licensing > Smart Licensing** 页面，并使用 **Force registration** 选）；从智能软件管理器中获取 ID 令牌。

- **即使备用设备运行的软件版本不支持原始隧道协商的密码套件，也会将VPN隧道复制到备用设备**—此情景在降级时出现。在此情况下，请断开 VPN 连接，然后再重新连接。

降级后删除了不兼容的配置

当您降级到旧版本时，更高版本中引入的命令将从配置中删除。在降级之前，无法自动根据目标版本检查配置。您可以按版本查看何时在ASA新功能中添加了新命令。https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asa_new_features.html

您可以在使用命令降级后查看被拒绝的命令。**show startup-config errors** 如果可以在实验设备上执行降级，则可以使用此命令预览效果，然后在生产设备上执行降级。

在某些情况下，ASA会在升级时自动将命令迁移到新表单，因此根据您的版本，即使您没有手动配置新命令，降级也可能会受到配置迁移的影响。我们建议您对旧配置进行备份，可供您在降级时使用。在升级到 8.3 的情况下，将自动创建备份 (<old_version>_startup_cfg.sav)。其他迁移不会创建备份。有关可能影响降级的自动命令迁移的详细信息，请参阅《ASA 升级指南》中的“特定于版本的准则和迁移”。

另请参阅中的已知降级问题。降级的准则和限制，第 4 页

例如，运行9.8（2）版本的ASA包括以下命令：

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz privilege 15
snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted auth
 md5 12:ab:34 priv aes 128 12:ab:34
```

当您降级到9.0（4）时，您将在启动时看到以下错误：

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
                                  ^
ERROR: % Invalid input detected at '^' marker.

username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz pbkdf2 privilege 15
                                                               ^
ERROR: % Invalid input detected at '^' marker.

snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted auth
 md5 12:ab:34 priv aes 128 12:ab:34
                                       ^
ERROR: % Invalid input detected at '^' marker.
```

在本例中，在版本9.5（2）中添加了对access-list extended命令中sctp的支持，在版本9.6（1）中添加了对username命令中pbkdf2的支持，并在snmp-server user命令中支持engineID是在9.5（3）版本中添加的。

降级 Firepower 1000、Cisco Secure Firewall 3100/4200

通过将 ASA 版本设置为旧版本，将备份配置恢复为启动配置，然后重新加载，可以降级 ASA 软件版本。

开始之前

此程序需要在升级之前对ASA进行备份配置，以便可以恢复旧配置。如果不恢复旧配置，则可能存在表示新功能或更改功能不兼容的命令。加载旧软件版本时，将会拒绝任何新命令。

过程

步骤 1 使用独立部署，故障转移或集群部署的ASA升级指南中的升级程序加载旧ASA软件版本。https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html在这种情况下，请指定旧ASA版本而不是新版本。重要提示：请不要重新加载ASA。

步骤 2 在ASA CLI中，将备份ASA配置复制到启动配置。对于故障转移，请在主用设备上执行此步骤。此步骤会将命令复制到备用设备。

copy *old_config_url* **startup-config**

请务必不要使用;将运行配置保存到启动配置。此命令将覆盖您的备份配置。**write memory**

示例：

```
ciscoasa# copy disk0:/9.13.1_cfg.sav startup-config
```

步骤 3 重新加载 ASA。

ASA CLI

reload

ASDM

依次选择 **Tool** > **System Reload**。

降级 Firepower 4100/9300

您可以通过将备份配置恢复为启动配置，将 ASA 版本设置为旧版本，然后重新加载来降级 ASA 软件版本。

开始之前

- 此程序需要在升级之前对ASA进行备份配置，以便可以恢复旧配置。如果不恢复旧配置，则可能存在表示新功能或更改功能不兼容的命令。加载旧软件版本时，将会拒绝任何新命令。
- 确保旧ASA版本与当前FXOS版本兼容。否则，请在恢复旧ASA配置之前先将FXOS降级。只需确保降级的FXOS也与当前ASA版本兼容（在降级之前）。如果无法实现兼容性，我们建议您不要执行降级。

过程

步骤 1 在ASA CLI中，将备份ASA配置复制到启动配置。对于故障转移或集群，请在主用/控制设备上执行此步骤。此步骤会将命令复制到备用/数据单元。

copy *old_config_url* **startup-config**

请务必不要使用;将运行配置保存到启动配置。此命令将覆盖您的备份配置。**write memory**

示例：

```
ciscoasa# copy disk0:/9.8.4_cfg.sav startup-config
```

步骤 2 在FXOS中，使用 机箱管理器或FXOS CLI，按照独立，故障转移或集群部署的ASA升级指南中的升级程序使用旧ASA软件版本。在这种情况下，请指定旧ASA版本而不是新版本。

步骤 3 如果您还降级FXOS，请使用 机箱管理器 或FXOS CLI将旧的FXOS软件版本设置为当前版本，使用独立部署，故障转移或集群部署的ASA升级指南中的升级程序。

降级 ISA 3000

降级功能提供了 ASA 5500-X and ISA 3000 型号完成以下功能的快捷方式：

- 清除引导映像配置 (**clear configure boot**)。
- 将引导映像设置为旧映像 (**boot system**)。
- （可选）输入新的激活密钥 (**activation-key**)。
- 将运行配置保存到启动 (**write memory**)。此操作会将 BOOT 环境变量设置为旧映像，因此，当您重新加载时，将会加载旧映像。
- 将旧配置备份复制到启动配置 (**copy***old_config_url***startup-config**)。
- 正在重新加载 (**reload**)。

开始之前

- 此程序需要在升级之前对 ASA 进行备份配置，以便可以恢复旧配置。

过程

步骤 1 依次选择**工具** > **降级软件**。

系统将显示 Downgrade Software 对话框。

步骤 2 对于 **ASA 映像 (ASA Image)**，请点击**选择映像文件 (Select Image File)**。

系统将显示 **Browse File Locations** 对话框。

步骤 3 点击以下单选按钮之一：

- **Remote Server** - 从下拉列表中选择 ftp、smb 或 http，然后键入旧映像文件的路径。
- **闪存文件系统 (Flash File System)** - 点击**浏览闪存 (Browse Flash)** 以选择本地闪存文件系统上的旧映像文件。

步骤 4 对于**配置 (Configuration)**，请点击**浏览闪存 (Browse Flash)** 以选择预迁移配置文件。

步骤 5 （可选） 在 **Activation Key** 字段中，输入旧的激活密钥（如果您需要恢复到 8.3 版本之前的激活密钥）。

步骤 6 点击**降级 (Downgrade)**。

管理文件

ASDM 提供一组文件管理工具来帮助您执行基本文件管理任务。通过 File Management 工具可查看、移动、复制和删除存储在闪存中的文件，传输文件和管理远程存储设备（装载点）上的文件。

注释 在多情景模式下，此工具仅适用于系统安全情景。

配置文件访问

ASA 可以使用 FTP 客户端、安全复制客户端或 TFTP 客户端。您也可以将 ASA 配置为安全复制服务器，以便可以在计算机上使用安全复制客户端。

配置 FTP 客户端模式

ASA 可使用 FTP 在 FTP 服务器中上传或下载映像文件或配置文件。在被动 FTP 中，客户端同时启动控制连接和数据连接。服务器（被动模式下数据连接的接收方）通过它用于侦听特定连接的端口号进行响应。

过程

步骤 1 从 Configuration > Device Management > Management Access > File Access > FTP Client 窗格中，选中 **Specify FTP mode as passive** 复选框。

步骤 2 点击 **Apply**。

系统会更改 FTP 客户端配置并将更改保存到运行配置。

配置 ASA 安全复制服务器

当 ASA 被用作 SCP 客户端时，可以使用 **copy** 命令来配置 SCP 设置。

SCP 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。要更改建议的密码，可使用 **配置 (Configuration)** > **设备管理 (Device Management)** > **高级 (Advanced)** > **SSH 密码 (SSH Ciphers)** 窗格；例如，选择**自定义 (Custom)** 并将其设置为 aes128-cbc。

开始之前

- ASA 许可证必须具有强加密 (3DES/AES) 许可证，才能支持 SSH V2 连接。
- 除非另有规定，否则对于多情景模式，请在系统执行空间中完成本程序。如果您尚未进入系统配置模式，请在 Configuration > Device List 窗格中双击主用设备 IP 地址下的 **System**。
- 对于 SCP 服务器，请根据 配置用于 ASDM 的 HTTPS 访问、其他客户端在 ASA 上启用 SSH。

过程

步骤 1 视情景模式而定：

- 对于单模式，依次选择 **Configuration > Device Management > Management Access > File Access > Secure Copy (SCP)**。
- 对于系统中的多模式，依次选择 **Configuration > Device Management > Device Administration > Secure Copy**。

步骤 2 （可选）ASA 为与之连接的每个 SCP 服务器存储 SSH 主机密钥。如果需要，可以在 ASA 数据库中手动添加或删除服务器及其密钥。

要添加密钥，请执行以下操作：

a) 点击**添加 (Add)**（对于新服务器），或者从“受信任 SSH 主机”(Trusted SSH Hosts) 表中选择服务器，然后点击**编辑 (Edit)**。
b) 对于新服务器，在 Host 字段中，输入服务器 IP 地址。
c) 选中 **Add public key for the trusted SSH host** 复选框。
d) 指定以下密钥之一：

- Fingerprint - 输入已经过散列处理的密钥；例如，您从 **show** 命令输出复制的密钥。
- Key - 输入 SSH 主机的公钥或经过散列处理的值。密钥字符串是远端对等体的采用 Base64 编码的 RSA 公钥。您可以从打开的 SSH 客户端（即 .ssh/id_rsa.pub 文件）获得公钥值。在您提交采用 Base64 编码的公钥之后，系统会通过 SHA-256 对其进行散列处理。

要删除密钥，从“受信任 SSH 主机”(Trusted SSH Hosts) 表中选择服务器，然后点击**删除 (Delete)**。

步骤 3 （可选）要在检测到新主机密钥时收到通知，请选中 **Inform me when a new host key is detected** 复选框。

默认情况下，系统会启用此选项。当启用此选项时，如果ASA中尚未存储主机密钥，系统会提示您接受或拒绝主机密钥。当禁用此选项时，如果以前未存储主机密钥，ASA 会自动接受主机密钥。

步骤 4 点击**应用**。

配置 ASA TFTP 客户端路径

TFTP 是一种简单的客户端/服务器文件传输协议，RFC 783 和 RFC 1350 第 2 修订版对其进行了说明。您可以将 ASA 配置为 TFTP 客户端，以便它可以与 TFTP 服务器之间进行双向文件复制。按照这种方式，您可以备份配置文件并将其传播到多台 ASA。

按照本节所述可以预定义 TFTP 服务器的路径，从而无需在诸如 **copy** 和 **configure net** 等命令中输入该路径。

过程

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **文件访问** > **TFTP 客户端**，然后选中**启用**复选框。

步骤 2 从 Interface Name 下拉列表中，选择要用作 TFTP 客户端的接口。

步骤 3 在 IP Address 字段中，输入将保存配置文件的 TFTP 服务器的 IP 地址。

步骤 4 在 Path 字段中，输入将保存配置文件的 TFTP 服务器的路径。

例如：/tftpboot/asa/config3

步骤 5 点击 **Apply**。

添加装载点

您可以添加 CIFS 或 FTP 装载点。

添加 CIFS 装载点

要定义通用互联网文件系统 (CIFS) 装载点，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **文件访问** > **装载点**，然后点击**添加** > **CIFS 装载点**。

系统将显示 Add CIFS Mount Point 对话框。

步骤 2 选中**启用装载点**复选框。

此选项将 ASA 上的 CIFS 文件系统连接至 UNIX 文件树。

步骤 3 在 Mount Point Name 字段中，输入现有 CIFS 位置的名称。

步骤 4 在 Server Name 或 IP Address 字段中，输入装载点所在服务器的名称或 IP 地址。

步骤 5 在 Share Name 字段中，输入 CIFS 服务器上的文件夹名称。

步骤 6 在 NT Domain Name 字段中，输入服务器所在 NT 域的名称。

步骤 7 在 User Name 字段中，输入已获授权可在服务器上装载文件系统的用户的名称。

步骤 8 在 Password 字段中，输入已获授权可在服务器上装载文件系统的用户的密码。

步骤 9 在 Confirm Password 字段中，重新输入密码。

步骤 10 点击 **OK**。

系统将关闭 Add CIFS Mount Point 对话框。

步骤 11 点击**应用**。

添加 FTP 装载点

对于 FTP 安装点，FTP 服务器必须采用 UNIX 目录列表样式。Microsoft FTP 服务器默认采用 MS-DOS 目录列表样式。

过程

步骤 1 依次选择**配置** > **设备管理** > **管理访问** > **文件访问** > **装载点**，然后点击**添加** > **FTP 装载点**。

系统将显示 Add FTP Mount Point 对话框。

步骤 2 选中 **Enable** 复选框。

此选项将 ASA 上的 FTP 文件系统连接至 UNIX 文件树。

步骤 3 在 Mount Point Name 字段中，输入现有 FTP 位置的名称。

步骤 4 在 Server Name 或 IP Address 字段中，输入装载点所在服务器的名称或 IP 地址。

步骤 5 在 Mode 字段中，点击 FTP 模式对应的单选按钮（**Active** 或 **Passive**）。当选择 Passive 模式时，客户端会发起 FTP 控制连接和数据连接。服务器会使用其用于此连接的监听端口号进行响应。

步骤 6 在 Path to Mount 字段中，输入 FTP 文件服务器的目录路径名称。

步骤 7 在 User Name 字段中，输入已获授权可在服务器上装载文件系统的用户的名称。

步骤 8 在 Password 字段中，输入已获授权可在服务器上装载文件系统的用户的密码。

步骤 9 在 Confirm Password 字段中，重新输入密码。

步骤 10 点击 **OK**。

系统将关闭 Add FTP Mount Point 对话框。

步骤 11 点击**应用**。

访问文件管理工具

要使用文件管理工具，请执行以下步骤：

过程

步骤 1 在 ASDM 主应用程序窗口中，依次选择**工具** > **文件管理**。

系统将显示 File Management 对话框。

- Folders 窗格显示磁盘上的可用文件夹。
- Flash Space 显示闪存总量，以及可用的内存量。
- Files 区域显示选定文件夹中的文件的以下有关信息：
  - Path
  - Filename
  - Size (bytes)
  - Time Modified
  - Status，表明将所选文件指定为启动配置文件、启动映像文件、ASDM 映像文件、SVC 映像文件、CSD 映像文件，还是 APCF 映像文件。

步骤 2 点击 **View** 以在浏览器中显示选定文件。

步骤 3 点击 **Cut** 以剪切选定文件，从而将其粘贴到其他目录。

步骤 4 点击 **Copy** 以复制选定文件，从而将其粘贴到其他目录。

步骤 5 点击 **Paste** 以将复制的文件粘贴到选定目标。

步骤 6 点击 **Delete** 以将从选定文件从闪存中删除。

步骤 7 点击 **Rename** 以重命名文件。

步骤 8 点击 **New Directory** 以创建用于存储文件的新目录。

步骤 9 点击 **File Transfer** 以打开 File Transfer 对话框。有关详细信息，请参阅传输文件，第 13 页。

步骤 10 点击 **Mount Points** 以打开 Manage Mount Points 对话框。有关详细信息，请参阅添加装载点，第 11 页。

传输文件

通过 File Transfer 工具，可以传输来自本地或远程位置的文件。您可以将您计算机或闪存文件系统上的本地文件传输到 ASA，也可以从中传出文件。您可以使用 HTTP、HTTPS、TFTP、FTP 或 SMB 将远程文件传输到 ASA，也可以从中传出文件。

注释 对于 IPS SSP 软件模块，在将 IPS 软件下载至 disk0 之前，请确保至少 50% 的闪存可用。当安装 IPS 时，IPS 会为其文件系统保留 50% 的内部闪存。

在本地 PC 和闪存之间传输文件

要在您的本地计算机和闪存文件系统之间传输文件，请执行以下步骤。

过程

步骤 1 在 ASDM 主应用程序窗口中，依次选择**工具** > **文件管理**。

系统将显示 File Management 对话框。

步骤 2 点击 **File Transfer** 旁边的向下箭头，然后点击 **Between Local PC and Flash**。

系统将显示 File Transfer 对话框。

步骤 3 从您的本地计算机或闪存文件系统中，选择并拖动要上传或下载至所需位置的文件。或者，从您的本地计算机或闪存文件系统中，选择要上传或下载的文件，然后点击向右箭头或向左箭头，以便将文件传输到所需位置。

步骤 4 完成后点击 **Close**。

在远程服务器和闪存之间传输文件

要在远程服务器和闪存文件系统之间传输文件，请执行以下步骤。

过程

步骤 1 在 ASDM 主应用程序窗口中，依次选择**工具** > **文件管理**。

系统将显示 File Management 对话框。

步骤 2 点击“文件传输”(File Transfer) 下拉列表中的向下箭头，然后点击**在远程服务器和闪存之间 (Between Remote Server and Flash)**。

系统将显示 File Transfer 对话框。

步骤 3 要从远程服务器传输文件，请点击**远程服务器 (Remote server)** 选项。

步骤 4 定义要传输的源文件。

a) （可选）指定 ASA 与服务器进行通信所使用的接口。如果不指定接口，ASA 将查看仅管理路由表；如果没有匹配，则会查看数据路由表。

b) 选择文件所在位置的路径，包括服务器的 IP 地址。

注释 文件传输支持 IPv4 和 IPv6 地址。

c) 输入远程服务器的类型（如果路径是 FTP）或端口号（如果路径是 HTTP 或 HTTPS）。有效的 FTP 类型如下：

- ap - 被动模式下的 ASCII 文件
- an - 非被动模式下的 ASCII 文件
- ip - 被动模式下的二进制映像文件
- in - 非被动模式下的二进制映像文件

步骤 5 要从闪存文件系统传输文件，请点击**闪存文件系统 (Flash file system)** 选项。

步骤 6 输入文件所在位置的路径，或者点击**浏览闪存 (Browse Flash)** 以查找文件位置。

步骤 7 此外，可以通过 CLI 从启动配置、运行配置或 SMB 文件系统中复制文件。有关使用 **copy** 命令的说明，请参阅《CLI 配置指南》。

步骤 8 定义要传输的文件的目标位置。

a) 要将文件传输到闪存文件系统，请选择 **Flash file system** 选项。
b) 输入文件所在位置的路径，或者点击**浏览闪存 (Browse Flash)** 以查找文件位置。

步骤 9 要将文件传输到远程服务器，请选择 **Remote server** 选项。

a) （可选）指定 ASA 与服务器进行通信所使用的接口。如果不指定接口，ASA 将查看仅管理路由表；如果没有匹配，则会查看数据路由表。
b) 输入文件所在位置的路径。
c) 对于 FTP 传输，请输入类型。有效的类型如下：

- ap - 被动模式下的 ASCII 文件
- an - 非被动模式下的 ASCII 文件
- ip - 被动模式下的二进制映像文件
- in - 非被动模式下的二进制映像文件

步骤 10 点击**传输 (Transfer)** 以开始文件传输。

系统将显示 Enter Username and Password 对话框。

步骤 11 输入远程服务器的用户名、密码和域（如果需要）。

步骤 12 点击**确定 (OK)** 以继续文件传输。

文件传输过程可能需要几分钟的时间；请确保等待其完成为止。

步骤 13 文件传输完成后，点击**关闭 (Close)**。

设置 ASA 映像、ASDM 和启动配置

如果您有多个 ASA 或 ASDM 映像，则应指定要启动的映像。如果不设置映像，则会使用默认启动映像，并且该映像可能不是计划使用的映像。对于启动配置，您可以选择在可见文件系统中指定文件，而不是隐藏目录。

请参阅以下模型准则：

- Firepower 4100/9300 机箱 - ASA 升级由 FXOS 管理；您无法在 ASA 操作系统中升级 ASA，因此不要对 ASA 映像使用此过程。您可以单独升级 ASA 和 FXOS，并且它们是单独列在 FXOS 目录列表中。ASA 包始终包括 ASDM。
- 设备模式下的 Firepower 1000 Cisco Secure Firewall 3100/4200-ASA、ASDM 和 FXOS 映像被捆绑成一个单个的包。ASA 使用此过程进行管理软件包更新。虽然这些平台使用 ASA 来识别要引导的映像，但基础机制与传统 ASA 不同。有关详细信息，请参阅下面的命令说明。
- 模型的 ASDM - ASDM 可以从 ASA 操作系统内部升级，因此您无需只使用捆绑的 ASDM 映像。对于 Firepower 4100/9300， 手动上传的 ASDM 映像不会出现在 FXOS 映像列表中；您必须从 ASA 管理 ASDM 映像。

注释 升级 ASA 捆绑包时，捆绑包中的 ASDM 映像将替换 ASA 上以前的 ASDM 捆绑包映像，因为它们具有相同的名称 (**asdm.bin**)。但是，如果您手动选择了您上传的其他 ASDM 映像（例如，**asdm-782.bin**），那么即使捆绑包升级之后，您仍可继续使用该映像。为了确保您运行的是兼容版本的 ASDM，您应该在升级捆绑包之前先升级 ASDM，或者应该在升级 ASA 捆绑包之前，或将 ASA 重新配置为使用捆绑的 ASDM 映像 (**asdm.bin**)。

- ASA Virtual - ASA virtual 包的初始部署会将 ASA 映像放在只读的 boot:/ 分区中。升级 ASA virtual 时，可以在闪存中指定不同的映像。请注意，如果您随后清除配置，则 ASA virtual 将还原为加载原始部署映像。初始部署 ASA virtual 包还包括它在闪存中放置的 ASDM 映像。您可以单独升级 ASDM 映像。

请参阅以下默认设置：

- ASA 映像：
  - 设备模式下的 Firepower 1000 Cisco Secure Firewall3100/4200-启动先前运行的启动映像。
  - ISA 3000 - 启动 ASA 在内部闪存中找到的第一个应用映像。
  - ASA Virtual - 启动您在首次部署时创建的只读 boot:/ 分区中的映像。
  - Firepower 4100/9300 机箱— FXOS 系统确定要引导的 ASA 映像。不能使用此过程来设置 ASA 映像。
- 所有 ASA 上的 ASDM 映像 - 启动 ASA 在内部闪存中找到的第一个 ASDM 映像，或者，如果此位置不存在映像，则在外部闪存中查找。

- 启动配置 - 默认情况下，ASA 从隐藏文件形式的启动配置进行引导。

过程

步骤 1 选择**配置** > **设备管理** > **系统映像/配置** > **引导映像/配置**。

设备模式下的 Firepower 1000Cisco Secure Firewall 3100/4200：您只能添加一个映像。如果升级到新映像，则必须删除所设置的上一个映像。当您应用此更改时，系统会执行操作：系统验证并解压缩映像，并将其复制到引导位置（FXOS 管理的 disk0 上的内部位置）。重新加载 ASA 时，系统将加载新图像。如果在重新加载之前更改主意，则可以删除**启动映像位置**并重新应用以从引导位置删除新映像，从而使当前映像继续运行。您甚至可以在应用此更改后从 ASA 闪存中删除原始映像文件，并且ASA将从启动位置正确启动。与其他模型不同，启动配置中的此命令不会影响启动映像。最后加载的启动图像将始终在重新加载时运行。您只能从思科下载站点使用原始文件名加载图像。如果更改文件名，将不会加载。

ASA virtual 和 ISA 3000：您可以指定最多四个用作启动映像的本地二进制映像文件，以及一个位于 TFTP 服务器上用于设备从其启动的映像。如果指定位于 TFTP 服务器上的映像，则该映像必须是列表中的第一个映像。如果设备无法访问 TFTP 服务器以加载映像，则它会尝试加载位于闪存中的列表中的下一个映像文件。

步骤 2 点击 Boot Image/Configuration 窗格中的 **Add**。

步骤 3 浏览至要从其启动的映像。对于 TFTP 映像，请在 File Name 字段中输入 TFTP URL。点击**确定**。

步骤 4 使用 Move Up 和 Move Down 按钮按顺序排放映像。

步骤 5 （可选）在 Boot Configuration File Path 字段中，通过点击 **Browse Flash** 并选择配置来指定启动配置文件。点击**确定**。

当您使用不适合隐藏目录的大型配置时，此功能非常重要。如果保存大型配置并看到以下错误消息，请务必使用此命令将配置保存到新文件：

```
%错误写入。nvram:/startup-config（设备上没有剩余空间）
```

步骤 6 在 ASDM Image File Path 字段中，通过点击 **Browse Flash** 并选择映像来指定 ASDM 映像。点击**确定**。

步骤 7 点击**应用**。

备份和恢复配置或其他文件

我们建议您对配置和其他系统文件进行定期备份以防止系统故障。

执行全面系统备份或还原

以下程序介绍如何将配置和映像备份至 zip 文件并将该文件传输到本地计算机。

开始备份或恢复之前

- 在您启动备份或恢复之前，您在备份或恢复位置应至少有 300 MB 的可用磁盘空间。
- ASA 必须处于单情景模式下。
- 如果您在备份期间或之后进行任何配置更改，则这些更改将不会包含在备份中。如果在进行备份后更改配置，然后执行恢复后的，则会覆盖此配置更改。因此，ASA 的行为可能会有所不同。
- 一次只能启动一个备份或恢复。
- 只能将配置恢复为与执行原始备份时相同的 ASA 版本。无法使用恢复工具将配置从一个 ASA 版本迁移到另一个版本。如果需要迁移配置，ASA 会在加载新 ASA OS 时自动升级驻留的启动配置。
- 如果使用集群，则只能备份或恢复启动配置、运行配置和身份证书。必须为每台设备单独创建和恢复备份。
- 如果使用故障转移，则必须为主用设备和备用设备单独创建和恢复备份。
- 如果您针对 ASA 设置主口令，则需要该主口令短语来恢复您使用此程序创建的备份配置。如果您不知道 ASA 的主口令，请参阅配置主密码，以了解在继续备份之前如何重置该口令。
- 如果导入 PKCS12 数据（使用 **crypto ca trustpoint** 命令）并且信任点使用 RSA 密钥，则会为导入的密钥对分配与信任点相同的名称。由于此限制，如果在恢复 ASDM 配置后为信任点及其密钥对指定其他名称，则启动配置将与原始配置相同，但运行配置将包含其他密钥对名称。这意味着，如果对密钥对和信任点使用不同的名称，则无法恢复原始配置。要解决此问题，请确保对信任点及其密钥对使用同一名称。
- 无法使用 CLI 进行备份及使用 ASDM 进行恢复，反之亦然。
- 每个备份文件包含以下内容：
  - 运行配置
  - 启动配置
  - 所有安全映像

    思科安全桌面和主机扫描映像

    思科安全桌面和主机扫描设置

    Secure Client (SVC) 映像和配置文件

    Secure Client (SVC) 自定义和转换
  - 身份证书（包括绑定到身份证书的 RSA 密钥对；独立密钥除外）
  - VPN 预共享密钥
  - SSL VPN 配置
  - 应用配置文件自定义框架 (APCF)

- 书签
- 自定义
- 动态访问策略 (DAP)
- 插件
- 连接配置文件的预填充脚本
- 代理自动配置
- 转换表
- Web 内容
- 版本信息

备份系统

本程序介绍如何执行完整系统备份。

注释 如果备份过程停滞，则 ASDM 可能没有足够的内存来加载配置。您可以监控 Java 控制台是否显示了“java.lang.OutOfMemoryError”消息，以查看是否存在内存不足问题。要增加 ASDM 内存，请参阅增加 ASDM 配置内存。

过程

步骤 1 在计算机上创建用于存储备份文件的文件夹，从而在今后需要恢复时，可以轻松找到这些文件。

步骤 2 依次选择**工具** > **备份配置**。

系统将显示 Backup Configurations 对话框。点击 **SSL VPN Configuration** 区域中的向下箭头，以查看 SSL VPN 配置的备份选项。默认情况下，会选中并备份所有配置文件（如果可用）。如果要备份列表中的所有文件，请转至步骤 5。

步骤 3 如果要选择将备份的配置，请取消选中 **Backup All** 复选框。

步骤 4 选中要备份的选项旁边的复选框。

步骤 5 点击 **Browse Local** 以指定 .zip 备份文件的目录和文件名。

步骤 6 在 Select 对话框中，选择要在其中存储备份文件的目录。

步骤 7 点击 **Select**。在 Backup File 字段中将显示路径。

步骤 8 在目录路径后输入目标备份文件的名称。备份文件名的长度必须介于 3 到 232 个字符之间。

步骤 9 点击 **Backup**。除非备份的是证书或者 ASA 使用的是主口令，否则将立即进行备份。

步骤 10 如果您在ASA上配置并启用了主口令，而且您不知道该密码，则在继续备份之前，您会收到一条警告消息，建议您更改主口令。如果您知道主口令，请点击 Yes 以继续进行备份。除非备份的是身份证书，否则将立即进行备份。

步骤 11 如果备份的是身份证书，则系统会要求您输入一个单独的口令，该口令将用于对 PKCS12 格式的证书进行编码。您可以输入口令，也可以跳过此步骤。

注释 此过程仅备份身份证书。

- 要加密证书，请在 Certificate Passphrase 对话框中输入并确认您的证书口令，然后点击 OK。恢复证书时，您将需要记得在此对话框中输入的密码。
- 点击 **Cancel** 会跳过此步骤且不对证书进行备份。

点击 OK 或 Cancel 后，备份将会立即开始。

步骤 12 备份完成后，系统将会关闭状态窗口，并显示 Backup Statistics 对话框以提供成功或失败消息。

注释 备份“失败消息”最有可能是由于缺少指定类型的现有配置所导致。

步骤 13 点击 **OK** 以关闭 Backup Statistics 对话框。

恢复备份

您可以指定要在您的本地计算机上从 zip 备份 tar.gz 文件恢复的配置和映像。

注释 如果恢复过程停滞，则ASDM可能没有足够的内存来加载配置。您可以监控Java控制台是否显示了“java.lang.OutOfMemoryError”消息，以查看是否存在内存不足问题。要增加ASDM内存，请参阅增加 ASDM 配置内存。

过程

步骤 1 依次选择**工具** > **恢复配置**。

步骤 2 在 Restore Configurations 对话框中，点击 **Browse Local Directory**，在您的本地计算机上选择包含要恢复的配置的 zip 文件，然后点击 **Select**。路径和 zip 文件名会显示在 **Local File** 字段中。

必须通过依次选择 **Tools > Backup Configurations** 选项创建要恢复的 zip 文件。

步骤 3 点击**Next**。系统将会显示第二个Restore Configuration对话框。选中要恢复的配置旁边的复选框。默认情况下，会选中所有可用的 SSL VPN 配置。

步骤 4 点击 **Restore**。

步骤 5 如果您在创建备份文件时指定了用于加密证书的证书口令，则 ASDM 会提示您输入该口令。

步骤 6 如果您选择恢复运行配置，系统会询问您是希望合并运行配置，替换运行配置，还是跳过恢复过程的这一部分。

- 合并配置会整合当前运行配置和已备份的运行配置。
- 替换运行配置仅使用已备份的运行配置。
- 跳过此步骤将不会恢复备份的运行配置。

ASDM 会显示状态对话框，直至恢复操作完成。

步骤 7 如果您替换或合并了运行配置，请关闭 ASDM，然后将其重新启动。如果未恢复运行配置，请刷新 ASDM 会话以使更改生效。

配置自动备份和恢复 (ISA 3000)

在 ISA 3000 上，每次使用保存配置时，都可以。

通过自动恢复，您可以轻松地使用在 SD 闪存卡上加载的完整配置来配置新设备。默认出厂配置中启用自动恢复。

配置自动备份 (ISA 3000)

在 ISA 3000 上，每次使用保存配置时，都可以。

开始之前

此功能在 ISA 3000 上不可用。

过程

步骤 1 依次选择**配置** > **设备管理** > **自动备份和恢复配置**。

步骤 2 选中或取消选中“**自动备份配置**”，可以启用或禁用自动备份。

如果启用自动备份，则在保存配置时，系统会自动将配置保存到备份位置以及启动配置。备份文件的名称为“auto-backup-asa.tgz”。

设置以下参数：

- **接口** - 如果您指定设备外存储，则指定要访问备份 URL 的接口。如果不指定接口名称，ASA 将查看仅管理路由表；如果没有匹配，则会查看数据路由表。
- **Location** - 指定用于备份数据的存储介质。您可以指定 URL 或本地存储。disk0 是内部闪存驱动器；disk1 是 USB 1 上的可选 USB 记忆棒；disk2 是 USB 2 上的可选 USB 记忆棒。disk3 是 SD 存储卡。自动恢复的默认值为 disk3:。
- **Passphrase** - 设置用于读取备份数据的口令。自动恢复的默认值为“cisco”。

配置自动恢复 (ISA 3000)

自动恢复模式可在没有任何用户干预的情况下恢复设备上的系统配置。例如，将包含已保存备份配置的 SD 存储卡插入新设备，然后打开设备电源。设备启动后会检查 SD 卡，以确定是否需要恢复系统配置。（仅当备份文件具有不同设备的“指纹”时，才会启动恢复。在备份或恢复操作期间，备份文件的指纹会更新为与当前设备匹配。因此，如果设备已完成恢复，或者已创建自己的备份，则系统会跳过自动恢复。）如果指纹显示需要恢复，则设备会替换系统配置（startup-config、running-config、SSL VPN 配置等；有关备份内容的详细信息，请参阅 备份系统，第 19 页）。当设备完成启动时，系统会运行保存的配置。

自动恢复在默认出厂配置中启用，因此您可以轻松地使用加载到 SD 存储卡上的完整配置来配置新设备，而无需执行设备的任何预配置。

由于设备需要在启动过程中尽早决定是否需要恢复系统配置，因此它会检查 ROMMON 变量来确定设备是否处于自动恢复模式，并获取备份配置的位置。使用以下 ROMMON 变量：

- **RESTORE_MODE =** {**auto** |**manual**}

  默认为**自动**。

- **RESTORE_LOCATION =** {**disk0:** | **disk1:** | **disk2:** | **disk3:**}

  默认值为 **disk3:**。

- **RESTORE_PASSPHRASE** = 密钥

  默认值为 **cisco**。

要更改自动恢复设置，请完成以下程序。

开始之前

- 此功能在 ISA 3000 上不可用。
- 如果使用默认恢复设置，则需要安装 SD 存储卡（部件号 SD-IE-1GB =）。
- 如果需要恢复默认配置以确保启用自动恢复，请使用 **configure factory default** 命令。此命令仅在透明防火墙模式下可用，因此，如果您处于路由防火墙模式，请首先使用 **firewall transparent** 命令。

过程

步骤 1 依次选择**配置** > **设备管理** > **自动备份和恢复配置**。

步骤 2 选中或取消选中**自动恢复配置**，可以启用或禁用自动恢复。

恢复的文件的名称为“auto-backup-asa.tgz”。如果启用自动恢复，请设置以下参数：

- **位置** - 指定用于恢复数据的存储介质。disk0 是内部闪存驱动器；disk1是 USB 1 上的可选 USB 记忆棒；disk2 是 USB 2 上的可选 USB 记忆棒。disk3 是 SD 存储卡。默认值为 disk3。

- **口令** - 设置用于读取备份数据的口令。默认值为“cisco”。

将运行配置保存到 TFTP 服务器

此功能可在 TFTP 服务器上存储当前运行配置文件的副本。

过程

步骤 1 依次选择**文件** > **将运行配置保存至 TFTP 服务器**。

系统将显示 Save Running Configuration to TFTP Server 对话框。

步骤 2 输入 TFTP 服务器的 IP 地址，以及将会在其中保存配置文件的文件路径，然后点击 **Save Configuration**。

注释 要配置默认 TFTP 设置，请依次选择 **Configuration > Device Management > Management Access > File Access > TFTP Client**。在配置此设置后，TFTP 服务器的 IP 地址和 TFTP 服务器上的文件路径会自动显示在此对话框中。

计划系统重新启动

通过 System Reload 工具可计划系统重新启动，或者取消挂起的重新启动。

过程

步骤 1 依次选择**工具** > **重新加载系统**。

步骤 2 在 Reload Scheduling 区域中，定义以下设置：

a) 对于 Configuration State，请选择在重新启动时保存或放弃运行配置。

b) 对于 Reload Start Time，请从以下选项中进行选择：

- 点击 **Now** 以立即执行重新启动。
- 点击 **Delay by** 以将重新启动延迟指定的时长。以小时和分钟或仅以分钟为单位，输入开始重新启动之前的时间。
- 点击 **Schedule at** 以计划在特定的时间和日期进行重新启动。输入将要进行重新启动的时间，并选择计划的重新启动的日期。

c) 在 Reload Message 字段中，输入重新启动时要发送到 ASDM 打开实例的消息。

d) 选中 **On reload failure force immediate reload after** 复选框，从而以小时和分钟或仅以分钟为单位，显示再次尝试重新启动之前的耗用时间。

e) 点击 **Schedule Reload** 以按配置来计划重新启动。

Reload Status 区域显示重新启动的状态。

步骤 3 选择以下其中一个选项：

- 点击 **Cancel Reload** 以停止计划的重新启动。
- 点击 **Refresh** 以在计划的重新启动完成后刷新 Reload Status 显示。
- 点击 **Details** 以显示计划的重新启动的结果。

Cisco Secure Firewall 3100/4200上的热插拔 SSD

如果您有两个SSD，它们会在您启动时形成RAID。防火墙启动时，您可以在CLI上执行以下任务：

- 热插拔其中一个 SSD - 如果 SSD 出现故障，您可以更换它。请注意，如果您只有一个 SSD，则无法在防火墙开启时将其删除。
- 删除一个 SSD - 如果您有两个 SSD，可以删除一个。
- 添加第二个 SSD - 如果您有一个 SSD，可以添加第二个 SSD 并形成 RAID。

⚠

注意 请勿在未使用此程序从 RAID 中移除 SSD 的情况下将其移除。可能会导致数据丢失。

过程

步骤 1 删除其中一个 SSD。

a) 从 RAID 中删除 SSD。

raid remove-secure local-disk {**1** | **2**}

remove-secure 关键字将从 RAID 中删除 SSD，禁用自加密磁盘功能，并对 SSD 执行安全擦除。如果您只想从 RAID 中删除 SSD 并保持数据不变，可以使用 **remove** 关键字。

示例：

```
ciscoasa(config)# raid remove-secure local-disk 2
```

b) 监控 RAID 状态，直到 SSD 不再显示在清单中。

show raid

从 RAID 中删除 SSD 后， **可操作性** 和 **驱动器状态** 将显示为 **降级**。第二个驱动器将不再列为成员磁盘。

示例：

```
ciscoasa# show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

ciscoasa# show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
```

```
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) 从机箱中取出 SSD。

步骤 2 添加 SSD。

a) 将 SSD 物理添加到空插槽。

b) 将 SSD 添加到 RAID。

raid add local-disk {**1** | **2**}

将新 SSD 同步到 RAID 可能需要几个小时，在此期间防火墙完全正常运行。您甚至可以重新启动，同步将在启动后继续。使用 **show raid** 命令显示状态。

如果您安装的 SSD 以前在另一个系统上使用过，并且仍处于锁定状态，请输入以下命令：

raid add local-disk {**1** | **2**} *psid*

Psid 印在 SSD 背面的标签上。或者，您可以重新启动系统，SSD 将被重新格式化并添加到 RAID。

软件和配置的历史记录

功能名称	平台版本	功能信息
安全复制客户端和服务器	9.1(5)/9.2(1)	ASA 现在支持安全复制 (SCP) 客户端和服务器，从而与 SCP 服务器进行双向文件传输。 修改了以下菜单项： Tools > File Management > File Transfer > Between Remote Server and Flash **Configuration > Device Management > Management Access > File Access > Secure Copy (SCP) Server**
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**。 引入了以下屏幕：**Configuration** > **Device Management** > **Advanced** > **SSH Ciphers**

功能名称	平台版本	功能信息
默认情况下会启用自动更新服务器证书验证	9.2(1)	现在，默认情况下会启用自动更新服务器证书验证；对于新的配置，必须明确禁用证书验证。如果您是从较早版本升级且未启用证书验证，则不会启用证书验证，并会显示以下警告： `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` 配置将被迁移，以明确不配置 验证。 修改了以下屏幕：Configuration > Device Management > System/Image Configuration > Auto Update > Add Auto Update Server。
使用 CLI 的系统备份和恢复	9.3(2)	您现在可以使用 CLI 来备份和恢复完整系统配置，包括映像和证书。 未修改任何 ASDM 屏幕。
恢复和加载新的 ASA 5506W-X 映像	9.4(1)	我们现在支持恢复和加载新的 ASA 5506W-X 映像。 未修改任何 ASDM 屏幕。
ISA 3000 的自动备份和自动恢复	9.7(1)	可以使用 pre-set parameters in the backup 和 restore 命令中的预设参数来启用自动备份和/或自动恢复功能。这些功能的使用情形包括从外部介质的初始配置；设备更换；回滚到某一可操作状态。 引入了以下菜单项：**配置** > **设备管理** > **自动备份和恢复配置**
思科 SSH 堆栈在使用 SCP 客户端时需要 SSH 访问权限	9.17(1)	如果使用 CiscoSSH 堆栈，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，必须使用 **ssh** 命令在 SCP 服务器子网/主机上
Cisco Secure Firewall 3100 上的 SSD 支持 RAID	9.17(1)	SSD 是自加密驱动器 (SED)，如果您有 2 个 SSD，它们会形成软件 RAID。 新增/修改的命令：**raid, show raid, show ssd**

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。