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（ISA 3000）加载映像

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 和 ASA 5516-X 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。请参阅升级软件，第 1 页。

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。

降级的指南和限制

降级前请参阅以下指南：

- **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。
- **在将群集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。
- **在平台模式下将 Firepower 2100 的降级问题从 9.13/9.14 降级到 9.12 或更早版本**—对于全新安装的 9.13 或 9.14 转换为平台模式的 Firepower 2100：如果降级到 9.12 或更早版本，您将无法配置新接口或编辑 FXOS 中的现有接口（请注意，9.12 及更早版本仅支持平台模式）。您需要将版本恢复到9.13或更高版本，或者需要使用FXOS擦除配置命令清除配置。如果您最初从较早版本升级到9.13或9.14，则不会发生此问题；仅新安装的设备会受到影响，例如新设备或重新映像的设备。(CSCvr19755)
- **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 虚拟从版本 9.5(2.200) 降级**- ASA 虚拟 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“特定于版本的指南和迁移”。

另请参阅中的已知降级问题。降级的指南和限制 ，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、2100 设备模式和 Cisco Secure Firewall 3100

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，故障切换或集群部署的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。对于故障切换，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**。

在平台模式下降级 Firepower 2100

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。

过程

步骤 1 在ASA CLI中，将备份ASA配置复制到启动配置。对于故障切换，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:/9.12.4_cfg.sav startup-config
```

步骤 2 在FXOS中，使用 机箱管理器或FXOS CLI，按照独立，故障切换或集群部署的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。

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。对于故障切换或集群，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，故障切换或集群部署的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，故障切换或集群部署的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

ASA CLI：降级软件并恢复旧配置。

downgrade [**/noconfirm**] *old_image_url old_config_url* [**activation-key** *old_key*]

示例：

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

/noconfirm 选项用于在不进行提示的情况下执行降级。*image_url* 是旧映像在 disk0、disk1、tftp、ftp 或 smb 上的路径。*old_config_url* 是到已保存的预迁移配置的路径。如果需要恢复至 8.3 版本之前的激活密钥，则可输入旧的激活密钥。

管理文件

查看闪存中的文件

您可以查看闪存中的文件，并参阅有关文件的信息。

过程

步骤 1 查看闪存中的文件：

dir [**disk0:** | **disk1:**]

示例：

```
hostname# dir

Directory of disk0:/
500    -rw-  4958208     22:56:20 Nov 29 2004  cdisk.bin
2513   -rw-  4634        19:32:48 Sep 17 2004  first-backup
2788   -rw-  21601       20:51:46 Nov 23 2004  backup.cfg
2927   -rw-  8670632     20:42:48 Dec 08 2004  asdmfile.bin
```

对于内部闪存，请输入 **disk0:**。**disk1:** 关键字表示外部闪存。默认为内部闪存。

步骤 2 查看有关特定文件的扩展信息：

show file information [path:/]*filename*

示例：

```
hostname# show file information cdisk.bin

disk0:/cdisk.bin:
  type is image (XXX) []
  file size is 4976640 bytes version 7.0(1)
```

所列的文件大小仅用作示例。

默认路径是内部闪存的根目录 (disk0:/)。

从闪存中删除文件

您可以从闪存中删除不再需要的文件。

过程

从闪存中删除文件：

delete disk0: *filename*

默认情况下，如果未指定路径，将从当前工作目录中删除文件。删除文件时，可以使用通配符。系统会提示您要删除的文件的文件名，然后您必须确认删除。

擦除闪存文件系统

要清除闪存文件系统，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 输入 **erase** 命令，这会覆盖所有文件并清除文件系统，包括隐藏的系统文件：

rommon #1> **erase** [**disk0:** | **disk1:** | **flash:**]

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

将 FTP 模式设置为被动：

ftp mode passive

示例：

```
ciscoasa(config)# ftp mode passive
```

将 ASA 配置为安全复制服务器

您可以在 ASA 上启用安全复制 (SCP) 服务器。只有经允许使用 SSH 访问 ASA 的客户端才能建立安全复制连接。

开始之前

- 服务器没有目录支持。缺少目录支持会限制远程客户端访问 ASA 内部文件。
- 服务器不支持横幅或通配符。
- 根据配置 SSH 访问，在 ASA 上启用 SSH。
- 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。要从该情景更改到系统执行空间，请输入 **changeto system** 命令。如果您尚未进入系统配置模式，请在 窗格中双击主用设备 IP 地址下的 **System**。
- 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。要更改建议的密码，可使用 **ssh cipher encryption** command；例如 **ssh cipher encryption custom aes128-cbc**

过程

步骤 1 启用 SCP 服务器：

ssh scopy enable

步骤 2 （可选）在 ASA 数据库中手动添加或删除服务器及其密钥。

ssh pubkey-chain [**no**]**server** *ip_address* {**key-string** *key_string* **exit**| **key-hash** {**md5** | **sha256**} *fingerprint*}

示例：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
ciscoasa(config-ssh-pubkey-server)# show running-config ssh pubkey-chain
ssh pubkey-chain
  server 10.7.8.9
    key-hash sha256 f1:22:49:47:b6:76:74:b2:db:26:fb:13:65:d8:99:19:
e7:9e:24:46:59:be:13:7f:25:27:70:9b:0e:d2:86:12
```

ASA 为与之连接的每个 SCP 服务器存储 SSH 主机密钥。如果需要，可以手动管理密钥。

对于每个服务器，可以指定 SSH 主机的 **key-string**（公钥）或 **key-hash**（散列值）。

key_string 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。

key-hash{**md5** | **sha256**}*fingerprint* 可用于输入已经过散列处理的密钥（使用 MD5 或 SHA-256 密钥）；例如，您从 **show** 命令输出复制的密钥。

步骤 3 （可选） 启用或禁用 SSH 主机密钥检查。对于多情景模式，在管理情景中输入此命令。

[**no**] **ssh stricthostkeycheck**

示例：

```
ciscoasa# ssh stricthostkeycheck
ciscoasa# copy x scp://cisco@10.86.95.9/x
The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established.
RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts.
Source filename [x]?

Address or name of remote host [10.86.95.9]?

Destination username [cisco]?

Destination password []? cisco123

Destination filename [x]?
```

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。

示例

从外部主机上的客户端执行 SCP 文件传输。例如，在 Linux 中输入以下命令：

scp -v -pw *password* [*path*/]*source_filename*
username@asa_address:{**disk0**|**disk1**}:/[*path*/]*dest_filename*

-v 表示详细，如果您未指定 **-pw**，则会提示您输入密码。

以下示例为 10.86.94.170 上的服务器添加经过散列处理的主机密钥：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256 65:d9:9d:fe:1a:bc:61:aa:
64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

以下示例为 10.7.8.9 上的服务器添加主机字符串密钥：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:
46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

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

预定义用于 **configure net** 和 **copy** 命令的 TFTP 服务器地址和文件名。

tftp-server *interface_name server_ip filename*

示例：

```
ciscoasa(config)# tftp-server inside 10.1.4.7 files/config1.cfg
ciscoasa(config)# copy tftp: test.cfg

Address or name of remote host [10.1.4.7]?

Source filename [files/config1.cfg]?config2.cfg

Destination filename [test.cfg]?

Accessing tftp://10.1.4.7/files/config2.cfg;int=outside...
```

输入命令时，可以覆盖文件名；例如，当使用 **copy** 命令时，可以利用预定义的 TFTP 服务器地址，但仍然在交互式提示符处输入任意文件名。

对于 **copy** 命令，输入 **tftp:** 以使用 tftp-server 值而非 **tftp://***url*。

将文件复制到 ASA

本节介绍如何复制应用映像、ASDM 软件、配置文件，或者任何其他需要从 TFTP、FTP、SMB、HTTP、HTTPS 或 SCP 服务器下载至内部或外部闪存的文件。

开始之前

- 您不能在闪存中的同一目录下具有两个名称相同但字母大小写不同的文件。例如，如果尝试将文件 Config.cfg 下载至包含 config.cfg 文件的位置，则会收到以下错误消息：

```
%Error opening disk0:/Config.cfg (File exists)
```

- 有关安装 Cisco SSL VPN 客户端的信息，请参阅 *Cisco Secure* 客户端的 *Cisco AnyConnect VPN* 客户端 管理员指南。有关在 ASA 上安装思科安全桌面的信息，请参阅面向思科 *ASA 5500* 系列管理员的思科安全桌面配置指南。
- 要在您安装了多个映像时或是将这些映像安装在外部闪存上时，将 ASA 配置为使用特定应用映像或 ASDM 映像，请参阅设置 ASA 映像、ASDM 和启动配置，第 19 页。
- 对于多情景模式，您必须处于系统执行空间中。
- （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。
- 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，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。请参阅 配置 SSH 访问。

过程

使用以下服务器类型之一复制文件。

- 从 TFTP 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **tftp:**//*server*[/*path*]/*src_filename* {**disk0**|**disk1**}**:**/[*path*/]*dest_filename*

  示例：

```
ciscoasa# copy tftp://10.1.1.67/files/context1.cfg disk0:/context1.cfg

Address or name of remote host [10.1.1.67]?

Source filename [files/context1.cfg]?

Destination filename [context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- 从 FTP 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **ftp:**//[*user*[**:***password*]**@**]*server*[/*path*]/*src_filename* {**disk0**|**disk1**}**:**/[*path*/]*dest_filename*

  示例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/context1.cfg
```

```
disk0:/contexts/context1.cfg

Address or name of remote host [10.1.1.67]?

Source username [jcrichton]?

Source password [aeryn]?

Source filename [files/context1.cfg]?

Destination filename [contexts/context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- 从 HTTP(S) 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]*/src_filename* {**disk0**|**disk1**}**:/**[*path/*]*dest_filename*

  示例：

```
ciscoasa# copy https://asun:john@10.1.1.67/files/moya.cfg disk0:/contexts/moya.cfg

Address or name of remote host [10.1.1.67]?

Source username [asun]?

Source password [john]?

Source filename [files/moya.cfg]?

Destination filename [contexts/moya.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- 从 SMB 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**disk0**|**disk1**}**:/**[*path/*]*dest_filename*

  示例：

```
ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/test.xml disk0:/test.xml

Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- 从 SCP 服务器进行复制：

  ;int=*interface* 选项会绕过路由查找，并始终使用指定接口来访问 SCP 服务器。

  copy [**/noconfirm**] [*interface_name*]
  scp://[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*]
  {**disk0**|**disk1**}**:/**[*path/*]*dest_filename*

  示例：

```
ciscoasa# copy scp://pilot@10.86.94.170/test.cfg disk0:/test.cfg

Address or name of remote host [10.86.94.170]?

Source username [pilot]?

Destination filename [test.cfg]?

The authenticity of host '10.86.94.170 (10.86.94.170)' can't be established.
RSA key fingerprint is
<65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19>(SHA256).
Are you sure you want to continue connecting (yes/no)? yes

Please use the following commands to add the hash key to the configuration:
  ssh pubkey-chain
    server 10.86.94.170
      key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19


Password: <type in password>
!!!!!!
6006 bytes copied in 8.160 secs (750 bytes/sec)
```

将文件复制到启动配置或运行配置

您可以将文本文件从TFTP、FTP、SMB、HTTP(S)或SCP服务器或者从闪存下载至运行配置或启动配置。

开始之前

将配置复制到运行配置时，会合并这两个配置。合并会将新配置中的所有新命令添加到运行配置中。如果配置相同，则不会发生任何更改。如果命令冲突或命令影响情景的运行，则合并的影响取决于命令。可能会发生错误，也可能出现意外结果。

（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。

过程

要将文件复制到启动配置或运行配置，请针对相应的下载服务器，输入以下命令之一：

- 从 TFTP 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **tftp:**//*server*[/*path*]/*src_filename* {**startup-config** | **running-config**}

  示例：

  ```
  ciscoasa# copy tftp://10.1.1.67/files/old-running.cfg running-config
  ```

- 从 FTP 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **ftp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  示例：

  ```
  ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/old-startup.cfg startup-config
  ```

- 从 HTTP(S) 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]*/src_filename* {**startup-config** | **running-config**}

  示例：

  ```
  ciscoasa# copy https://asun:john@10.1.1.67/files/new-running.cfg running-config
  ```

- 从 SMB 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  示例：

  ```
  ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/new-running.cfg running-config
  ```

- 从 SCP 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*] {**startup-config** | **running-config**}

  示例：

  ```
  ciscoasa# copy scp://pilot:moya@10.86.94.170/new-startup.cfg startup-config
  ```

  ;Int=interface*interface* 选项 会绕过路由查询并始终使用指定的接口 到达 SCP 服务器。

示例

例如，要从 TFTP 服务器复制配置，请输入以下命令：

```
ciscoasa# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

要从 FTP 服务器复制配置，请输入以下命令：

```
ciscoasa# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg startup-config
```

要从 HTTP 服务器复制配置，请输入以下命令：

```
ciscoasa# copy http://209.165.200.228/configs/startup.cfg startup-config
```

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，可以随意指定配置文件。

请参阅以下模型指南：

- 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。
- 平台模式中的 Firepower 2100 - ASA、ASDM 和 FXOS 映像被捆绑成一个单个的包。包更新由 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。您不能单独升级 ASA 和 FXOS；它们始终捆绑在一起。
- 设备模式下的 Firepower 1000、 2100、Cisco Secure Firewall 3100 - 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。平台模式上的 Firepower 2100 和 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 虚拟 - ASA 虚拟 包的初始部署会将 ASA 映像放在只读的 boot:/ 分区中。升级 ASA 虚拟 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 (**clear configure all**)，则 ASA 虚拟 将还原为加载原始部署映像。初始部署 ASA 虚拟 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、2100、Cisco Secure Firewall 3100 - 启动先前运行的启动映像。
- 其他 Physical ASA — 启动 ASA 在内部闪存中找到的第一个应用映像。
- ASA 虚拟 - 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。
- 平台模式中的 Firepower 2100 — FXOS 系统确定要引导的 ASA/FXOS 包。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 设置 ASA 启动映像位置：

boot system *url*

示例：

```
ciscoasa(config)# boot system disk0:/images/asa921.bin
```

URL 可以是：

- {**disk0:/** | **disk1:/**}[*path*/]*filename*
- **tftp://**[*user*[**:***password*]**@**]*server*[**:***port*]/[*path*/]*filename*

  并非所有型号都支持 TFTP 选项。

设备模式下的 **Firepower 1000**、**2100**、**Cisco Secure Firewall 3100**：您只能输入一个 **boot system** 命令。如果要升级到新映像，则必须输入 **no boot system** 以删除您设置的上一个映像。请注意，您的配置中不能有 **boot system** 命令；例如，如果您从 ROMMON 安装了映像，有新设备，或者手动删除了该命令。此 **boot system** 命令会在您输入时执行操作：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改变主意，可以输入 **no boot system** 命令从引导位置删除新映像，这样当前映像将继续运行。输入此命令后，您甚至可以从 ASA 闪存中删除原始映像文件，ASA 将从引导位置正确引导；但是，我们建议将要使用的任何映像保留在闪存中，因为 **boot system** 命令仅适用于闪存中的映像。与其他模型不同，启动配置中的此命令不会影响启动映像，并且实质上是有修饰的。最后加载的启动图像将始终在重新加载时运行。如果在输入此命令后未保存配置，则在重新加载时，旧命令将存在于您的配置中，即使新映像已启动。请务必保存配置，以便配置保持同步。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。您还可以通过加载威胁防御映像来重新映像到 威胁防御。在这种情况下，系统会提示您立即重新加载。

其他模型: 您可以输入最多四个 **boot system** 命令条目，以指定要按顺序从中引导的不同映像；ASA 将引导其成功找到的第一个映像。当输入 **boot system** 命令时，该命令会在列表的底部添加一个条目。要对启动条目重新排序，必须使用 **clear configure boot system** 命令删除所有条目，然后按所需顺序重新输入这些条目。只能配置一个 **boot system tftp** 命令，并且该命令必须是配置的第一个命令。

注释 如果 ASA 陷入不断启动的循环中，则可以将 ASA 重新引导至 ROMMON 模式下。有关 ROMMON 模式的详细信息，请参阅查看调试消息。

示例：

```
firepower-2110(config)# boot system disk0:/cisco-asa-fp2k.9.13.2.SPA
The system is currently installed with security software package 9.13.1, which has:
   - The platform version:  2.7.1
   - The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.13.2 will do the following:
   - upgrade to the new platform version 2.7.2
   - upgrade to the CSP ASA version 9.13.2
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready...........
Install_status: validating-images.....
Install_status: update-software-pack-completed
firepower-2110(config)#
```

步骤 2 设置要启动的 ASDM 映像：

asdm image {**disk0:/** | **disk1:/**}[*path*/]*filename*

示例：

```
ciscoasa(config)# asdm image disk0:/images/asdm721.bin
```

如果不指定要启动的映像，即使仅安装了一个映像，ASA 也会在运行配置中插入 **asdm image** 命令。为了避免自动更新（如已配置）发生问题，以及避免在每次启动时都搜索映像，您应在启动配置中指定要启动的 ASDM 映像。

步骤 3 （可选）将启动配置设置为一个已知文件，而不是默认的隐藏文件。

boot config {**disk0:/** | **disk1:/**}[*path*/]*filename*

示例：

```
ciscoasa(config)# boot config disk0:/configs/startup1.cfg
```

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 tar.gz 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。
- 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。
- 如果使用故障切换，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

    AnyConnect 客户端 (SVC) 映像和配置文件

AnyConnect 客户端 (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。

过程

步骤 1 备份系统：

backup [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**passphrase** *value*] [**location** *path*]

示例：

```
ciscoasa# backup location disk0:/sample-backup]
Backup location [disk0:/sample-backup]?
```

如果不指定 **interface** *name*，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。

在系统执行空间中的多情景模式下，输入 **context** 关键字以备份指定的情景。每个情景必须单独备份；也就是说，针对每个文件重新输入 **backup** 命令。

在VPN证书和预共享密钥的备份期间，需要由**passphrase**关键字标识的密钥才可对证书进行编码。必须提供要用于编码和解码PKCS12格式的证书的口令。备份仅包含绑定到证书的RSA密钥对，不包括任何独立证书。

备份 **location** 可以是本地磁盘或远程 URL。如果不提供位置，则会使用以下默认名称：

- 单模式 - disk0:*hostname*.backup.*timestamp*.tar.gz
- 多模式 - disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz

步骤 2 按照提示操作：

示例：

```
ciscoasa# backup location disk0:/sample-backup
Backup location [disk0:/sample-backup]?

Begin backup…
Backing up [ASA version] … Done!
Backing up [Running Config] … Done!
Backing up [Startup Config]  … Done!

Enter a passphrase to encrypt identity certificates. The default is cisco.
You will be required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] … Done!

IMPORTANT: This device uses master passphrase encryption. If this backup file
is used to restore to a device with a different master passphrase,
you will need to provide the current master passphrase during restore.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

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。

过程

步骤 1 从备份文件恢复系统。

restore [**/noconfirm**] [**context** *ctx-name*] [**passphrase** *value*] [**location** *path*]

示例：

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?
```

当使用**context**关键字恢复多个情景时，必须单独恢复每个备份的情景文件；也就是说，为每个文件重新输入 **restore** 命令。

步骤 2 按照提示操作：

示例：

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?

Copying Backup file to local disk... Done!
Extracting the backup file ... Done!
Warning: The ASA version of the device is not the same as the backup version,
some configurations might not work after restore!
 Do you want to continue? [confirm] y
Begin restore ...
IMPORTANT: This backup configuration uses master passphrase encryption.
Master passphrase is required to restore running configuration,
startup configuration and VPN pre-shared keys.
Backing up [VPN Pre-shared keys] ⋯ Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] ⋯ Done!
Backing up [SSL VPN Configurations: Bookmarks]⋯ Done!
Backing up [SSL VPN Configurations: Customization] ⋯ Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] ⋯ Done!
Backing up [SSL VPN Configurations: Plug-in] ⋯ Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] ⋯ Done!
Backing up [SSL VPN Configurations: Proxy auto-config] ⋯ Done!
Backing up [SSL VPN Configurations: Translation table] ⋯ Done!
Backing up [SSL VPN Configurations: Web Content] ⋯ Done!
Backing up [Anyconnect(SVC) client images and profiles] ⋯ Done!
Backing up [Anyconnect(SVC) customizations and transforms] ⋯ Done!
Backing up [Cisco Secure Desktop and Host Scan images] ⋯ Done!
Backing up [UC-IME tickets] ⋯ Done!
Restoring [Running Configuration]
Following messages are as a result of applying the backup running-configuration to
this device, please note them for future reference.

ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside,
the IP is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside,
the IP is already used as media-termination address on interface inside.
WARNING: PAC settings will override http- and https-proxy configurations.
Do not overwrite configuration file if you want to preserve the old http-
and https-proxy configurations.
```

```
Cryptochecksum (changed): 98d23c2c ccb31dc3 e51acf88 19f04e28
 Done!
Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates.
The default is cisco. If the passphrase is not correct, certificates will not be restored.

No passphrase was provided for identity certificates.
Using the default value: cisco. If the passphrase is not correct,
certificates will not be restored.
Restoring Certificates ...
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully
. Done!
Cleaning up ... Done!
Restore finished!
```

配置自动备份和恢复 (ISA 3000)

在 ISA 3000 上，每次使用保存配置时，都可以使用 **write memory**将自动备份配置到特定位置。

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，都可以使用 **write memory**将自动备份配置到特定位置。

开始之前

此功能在 ISA 3000 上不可用。

过程

步骤 1 设置备份包参数：

backup-package backup [**interface** *name*] **location** {**disk***n***:** | *url*} [**passphrase** *string*]

- **interface** *name* - 指定接口访问备份 URL（如果指定了设备外存储）。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** {**disk***n***:** | *url*} - 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。请注意，自动恢复的默认设置使用 disk3。
- **passphrase** *string* - 设置用于保护备份数据的密码。请注意，自动恢复的默认设置使用“cisco”作为口令。

默认情况下，这些设置也会与手动 **backup** 命令一起使用。请参阅 备份系统，第 23 页。请注意，如果在启用自动备份或恢复时使用手动**backup** 命令，则系统会保存指定名称的备份文件，以及自动备份和恢复使用的“auto-backup-asa.tgz”名称。

示例：

```
ciscoasa(config)# backup-package backup location disk3: passphrase cisco
```

步骤 2 启动自动模式进行备份和恢复：

backup-package backup auto

使用 **write memory** 时保存配置时，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”。要禁用自动备份，请使用此命令的 **no** 形式。

示例：

```
ciscoasa(config)# backup-package backup auto
```

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 23 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 设置恢复包参数。

backup-package restore location {**disk***n***:** | *url*} [**passphrase** *string*]

- **location disk***n***:** - 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。
- **passphrase** *string* - 设置用于读取备份数据的密码。默认值为“cisco”。

默认情况下，这些设置也会与手动 **restore** 命令一起使用。请参阅 备份系统，第 23 页。

示例：

```
ciscoasa(config)# backup-package restore location disk1: passphrase $upe3rnatural
```

步骤 2 启动或禁用自动模式进行恢复。

[**no**] **backup-package restore auto**

恢复的文件的名称为“auto-backup-asa.tgz”。

示例：

```
ciscoasa(config)# no backup-package restore auto
```

备份单模式配置或多模式系统配置

在单情景模式下，或是在多情景模式下的系统配置中，可以将启动配置或运行配置复制到外部服务器或本地闪存。

开始之前

（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。

过程

使用以下服务器类型之一来备份配置：

- 复制到 TFTP 服务器：

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **tftp://***server*[*/path*]*/dst_filename*

  示例：

  ```
  ciscoasa# copy running-config tftp://10.1.1.67/files/new-running.cfg
  ```

- 复制到 FTP 服务器：

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **ftp://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  示例：

  ```
  ciscoasa# copy startup-config ftp://jcrichton:aeryn@10.1.1.67/files/new-startup.cfg
  ```

- 复制到 SMB 服务器：

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  示例：

  ```
  ciscoasa# copy /noconfirm running-config smb://chiana:dargo@10.1.1.67/new-running.cfg
  ```

- 复制到 SCP 服务器：

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*[**;int=***interface_name*]

  示例：

  ```
  ciscoasa# copy startup-config
  scp://pilot:moya@10.86.94.170/new-startup.cfg
  ```

  ;Int=interface*interface* 选项 会绕过路由查询并始终使用指定的接口 到达 SCP 服务器。

- 复制到本地闪存：

  copy [**/noconfirm**] {**startup-config** | **running-config**} {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  示例：

  ```
  ciscoasa# copy /noconfirm running-config disk0:/new-running.cfg
  ```

请确保目标目录存在。如果不存在，请先使用 **mkdir** 命令创建该目录。

备份闪存中的情景配置或其他文件

通过在系统执行空间中输入以下命令之一来复制本地闪存中的情景配置或其他文件。

开始之前

（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。

过程

使用以下服务器类型之一备份情景配置：

- 从闪存复制到 TFTP 服务器：

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **tftp://***server*[*/path*]*/dst_filename*

  示例：

  ```
  ciscoasa# copy disk0:/asa-os.bin tftp://10.1.1.67/files/asa-os.bin
  ```

- 从闪存复制到 FTP 服务器：

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  ftp://[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  示例：

  ```
  ciscoasa# copy disk0:/asa-os.bin ftp://jcrichton:aeryn@10.1.1.67/files/asa-os.bin
  ```

- 从闪存复制到 SMB 服务器：

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  smb://[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  示例：

  ```
  ciscoasa# copy /noconfirm copy disk0:/asdm.bin
  smb://chiana:dargo@10.1.1.67/asdm.bin
  ```

- 从闪存复制到 SCP 服务器：

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  scp://[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*[**;int=***interface_name*]

  示例：

```
ciscoasa# copy disk0:/context1.cfg
scp://pilot:moya@10.86.94.170/context1.cfg
```

;Int=interface*interface* 选项 会绕过路由查询并始终使用指定的接口 到达 SCP 服务器。

- 从闪存复制到本地闪存：

  copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  示例：

  ```
  ciscoasa# copy /noconfirm disk1:/file1.cfg disk0:/file1.cfgnew-running.cfg
  ```

  请确保目标目录存在。如果不存在，请先使用 **mkdir** 命令创建该目录。

在情景中备份情景配置

在多情景模式下，您可以从情景中执行以下备份操作：

过程

步骤 1 将运行配置复制到已连接至情景网络的启动配置服务器：

```
ciscoasa/contexta# copy running-config startup-config
```

步骤 2 将运行配置复制到已连接至情景网络的 TFTP 服务器：

```
ciscoasa/contexta# copy running-config tftp:/server[/path]/filename
```

从终端显示复制配置

过程

步骤 1 将配置列显到终端：

more system:running-config

步骤 2 请复制此命令的输出，然后将配置粘贴到文本文件。

使用 Export 和 Import 命令备份附加文件：

对您的配置至关重要的其他文件可能包括以下文件：

- 您使用 **import webvpn** 命令导入的文件。目前，这些文件包括自定义、URL 列表、网络内容、插件和语言转换文件。
- DAP 策略 (dap.xml)。
- CSD 配置 (data.xml)。
- 数字密钥和证书。
- 本地 CA 用户数据库和证书状态文件。

通过 CLI 可以使用 **export** 和 **import** 命令备份和恢复配置的各个元素。

要备份这些文件，比如您使用 **import webvpn** 命令或证书导入的文件，请执行以下步骤。

过程

步骤 1 运行适用的 **show** 命令，如下所示：

```
ciscoasa # show import webvpn plug-in
ica
rdp
ssh, telnet
vnc
```

步骤 2 对于要备份的文件，请运行 **export** 命令（在本示例中为 rdp 文件）：

```
ciscoasa # export webvpn plug-in protocol rdp tftp://tftpserver/backupfilename
```

使用脚本备份和恢复文件

您可以使用脚本来备份和恢复 ASA 上的配置文件，包括通过 **import webvpn** CLI 命令导入的所有扩展文件、CSD 配置 XML 文件和 DAP 配置 XML 文件。出于安全原因，我们不建议对数字密钥和证书或者本地 CA 密钥执行自动备份。

本部分对此操作提供说明，并包含您可以按原样使用或根据环境要求修改后使用的样本脚本。此样本脚本特定于 Linux 系统。要将其用于 Microsoft Windows 系统，需要运用此样本的逻辑对其进行修改。

注释 或者，可以使用 **backup** 和 **restore** 命令。有关详细信息，请参阅执行全面系统备份或还原，第 22 页。

在开始使用备份和恢复脚本之前

要使用脚本来备份和恢复 ASA 配置，请先执行以下任务：

- 使用 Expect 模块安装 Perl。
- 安装可以访问 ASA 的 SSH 客户端。
- 安装 TFTP 服务器，以将文件从 ASA 发送到备份站点。

另一个选项是使用商用工具。您可以将此脚本的逻辑运用于此类工具。

运行脚本

要运行备份和恢复脚本，请执行以下步骤：

过程

步骤 1 将脚本文件下载或剪切并粘贴到系统上的任意位置。

步骤 2 在命令行中，输入 **Perl***scriptname*，其中 *scriptname* 是脚本文件的名称。

步骤 3 按 **Enter** 键。

步骤 4 系统会提示您输入每个选项的值。或者，可以在输入 **Perl***scriptname* 命令时，按 **Enter** 键之前输入选项的值。无论采用哪种方式，脚本都要求输入每个选项的值。

步骤 5 脚本会开始运行，显示其发出的命令，这可以为您提供 CLI 记录。您可以在日后恢复时使用这些 CLI，这在您希望仅恢复一两个文件时特别有用。

样本脚本

```
#!/usr/bin/perl
#Description: The objective of this script is to show how to back up
configurations/extensions.
# It currently backs up the running configuration, all extensions imported via "import
webvpn" command, the CSD configuration XML file, and the DAP configuration XML file.
#Requirements: Perl with Expect, SSH to the ASA, and a TFTP server.
#Usage: backupasa -option option_value
#       -h: ASA hostname or IP address
#       -u: User name to log in via SSH
#       -w: Password to log in via SSH
#       -e: The Enable password on the security appliance
#       -p: Global configuration mode prompt
#       -s: Host name or IP address of the TFTP server to store the configurations
#       -r: Restore with an argument that specifies the file name. This file is produced
during backup.
```

```
#If you don't enter an option, the script will prompt for it prior to backup.
#
#Make sure that you can SSH to the ASA.

use Expect;
use Getopt::Std;

#global variables
%options=();
$restore = 0; #does backup by default
$restore_file = '';
$asa = '';
$storage = '';
$user = '';
$password = '';
$enable = '';
$prompt = '';
$date =  ‘date +%F ‘;
chop($date);
my $exp = new Expect();

getopts("h:u:p:w:e:s:r:",\%options);
do process_options();

do login($exp);
do enable($exp);
if ($restore) {
   do restore($exp,$restore_file);
}
else {
   $restore_file = "$prompt-restore-$date.cli";
   open(OUT,">$restore_file") or die "Can't open $restore_file\n";
   do running_config($exp);
   do lang_trans($exp);
   do customization($exp);
   do plugin($exp);
   do url_list($exp);
   do webcontent($exp);
   do dap($exp);
   do csd($exp);
   close(OUT);
}
do finish($exp);

sub enable {
   $obj = shift;
   $obj->send("enable\n");
   unless ($obj->expect(15, 'Password:')) {
      print "timed out waiting for Password:\n";
   }
   $obj->send("$enable\n");
   unless ($obj->expect(15, "$prompt#")) {
      print "timed out waiting for $prompt#\n";
   }
}

sub lang_trans {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn translation-table\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);
```

```
   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /Translation Tables/;
     next unless (/^.+\s+.+$/);
     ($lang, $transtable) = split(/\s+/,$_);
     $cli = "export webvpn translation-table $transtable language $lang
$storage/$prompt-$date-$transtable-$lang.po";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub running_config {
  $obj = shift;
  $obj->clear_accum();
  $cli ="copy /noconfirm running-config $storage/$prompt-$date.cfg";
  print "$cli\n";
  $obj->send("$cli\n");
  $obj->expect(15, "$prompt#" );
}


sub customization {
  $obj = shift;
  $obj->clear_accum();
  $obj->send("show import webvpn customization\n");
  $obj->expect(15, "$prompt#" );
  $output = $obj->before();
  @items = split(/\n+/, $output);

  for (@items) {
    chop;
    next if /^Template/ or /show import/ or /^\s*$/;
    $cli = "export webvpn customization $_ $storage/$prompt-$date-cust-$_.xml";
    $ocli = $cli;
    $ocli =~ s/^export/import/;
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
  }
}

sub plugin {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn plug-in\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/;
     $cli = "export webvpn plug-in protocol $_ $storage/$prompt-$date-plugin-$_.jar";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
```

```
      $obj->send("$cli\n");
      $obj->expect(15, "$prompt#" );
    }
}

sub url_list {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("show import webvpn url-list\n");
    $obj->expect(15, "$prompt#" );
    $output = $obj->before();
    @items = split(/\n+/, $output);

    for (@items) {
      chop;
      next if /^Template/ or /show import/ or /^\s*$/ or /No bookmarks/;
      $cli="export webvpn url-list $_ $storage/$prompt-$date-urllist-$_.xml";
      $ocli = $cli;
      $ocli =~ s/^export/import/;
      print "$cli\n";
      print OUT "$ocli\n";
      $obj->send("$cli\n");
      $obj->expect(15, "$prompt#" );
    }
}

sub dap {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("dir dap.xml\n");
    $obj->expect(15, "$prompt#" );

    $output = $obj->before();
    return 0 if($output =~ /Error/);

    $cli="copy /noconfirm dap.xml $storage/$prompt-$date-dap.xml";
    $ocli="copy /noconfirm $storage/$prompt-$date-dap.xml disk0:/dap.xml";
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
}

sub csd {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("dir sdesktop\n");
    $obj->expect(15, "$prompt#" );

    $output = $obj->before();
    return 0 if($output =~ /Error/);

    $cli="copy /noconfirm sdesktop/data.xml $storage/$prompt-$date-data.xml";
    $ocli="copy /noconfirm $storage/$prompt-$date-data.xml disk0:/sdesktop/data.xml";
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
}

sub webcontent {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("show import webvpn webcontent\n");
```

```
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /No custom/;
     next unless (/^.+\s+.+$/);
     ($url, $type) = split(/\s+/,$_);
     $turl = $url;
     $turl =~ s/\/\+//;
     $turl =~ s/\+\//-/;
     $cli = "export webvpn webcontent $url $storage/$prompt-$date-$turl";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub login {
    $obj = shift;
    $obj->raw_pty(1);
    $obj->log_stdout(0); #turn off console logging.
    $obj->spawn("/usr/bin/ssh $user\@$asa") or die "can't spawn ssh\n";
    unless ($obj->expect(15, "password:" )) {
        die "timeout waiting for password:\n";
    }

    $obj->send("$password\n");

    unless ($obj->expect(15, "$prompt>" )) {
        die "timeout waiting for $prompt>\n";
    }
}

sub finish {
    $obj = shift;
    $obj->hard_close();
    print "\n\n";

}

sub restore {
   $obj = shift;
   my $file = shift;
   my $output;
   open(IN,"$file") or die "can't open $file\n";
   while (<IN>) {
      $obj->send("$_");
      $obj->expect(15, "$prompt#" );
      $output = $obj->before();
      print "$output\n";
   }
   close(IN);
}

sub process_options {
  if (defined($options{s})) {
      $tstr= $options{s};
      $storage = "tftp://$tstr";
```

```
    }
    else {
        print "Enter TFTP host name or IP address:";
        chop($tstr=<>);
        $storage = "tftp://$tstr";
    }
    if (defined($options{h})) {
        $asa = $options{h};
    }
    else {
        print "Enter ASA host name or IP address:";
        chop($asa=<>);
    }

    if (defined ($options{u})) {
        $user= $options{u};
    }
    else {
        print "Enter user name:";
        chop($user=<>);
    }

    if (defined ($options{w})) {
        $password= $options{w};
    }
    else {
        print "Enter password:";
        chop($password=<>);
    }
    if (defined ($options{p})) {
        $prompt= $options{p};
    }
    else {
        print "Enter ASA prompt:";
        chop($prompt=<>);
    }
    if (defined ($options{e})) {
        $enable = $options{e};
    }
    else {
        print "Enter enable password:";
        chop($enable=<>);
    }

    if (defined ($options{r})) {
       $restore = 1;
       $restore_file = $options{r};
    }
}
```

Cisco Secure Firewall 3100 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。 引入了以下命令：**ssh pubkey-chain**、**server (ssh pubkey-chain)**、**key-string**、**key-hash** 和 **ssh stricthostkeycheck**。 修改了以下命令：**copy scp**。
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**
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。 **auto-update server no-verification** 修改了以下命令：**auto-update server** {**verify-certificate** | **no-verification**}。
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。 引入了以下命令：**backup** 和 **restore**。

功能名称	平台版本	功能信息
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。 引入了以下命令：**hw-module module wlan recover image**。
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。 引入了以下命令：**backup-package location**、**backup-package auto**、**show backup-package status**、**show backup-package summary**
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/主机上启用 ASA 访问。
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，则它们会组成软件 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。