



降级 ASA

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，第 1 页](#)
- [降级后删除了不兼容的配置，第 2 页](#)
- [在 Cisco Secure Firewall 3100 的设备模式下降级 Firepower 1000、2100，第 3 页](#)
- [在平台模式下降级 Firepower 2100，第 4 页](#)
- [降级 Firepower 4100/9300，第 5 页](#)
- [降级 ISA 3000，第 5 页](#)

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[版本特定的准则和迁移](#)。

另请参阅中的已知降级问题。[降级的准则和限制，第 1 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$1234$abcdefghijklmnopqrstuvwxy privilege 15
snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxy 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$1234$abcdefghijklmnopqrstuvwxy pbkdf2 privilege 15
                                     ^
ERROR: % Invalid input detected at '^' marker.

snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxy 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。

在 Cisco Secure Firewall 3100 的设备模式下降级 Firepower 1000、2100

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。在 [Cisco Secure Firewall 3100 的设备模式下升级 Firepower 1000、2100](#) 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**。

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:/9.12.4_cfg.sav startup-config
```

步骤 2 在FXOS中，使用 机箱管理器或 FXOS CLI，按照独立，故障转移或集群部署的级在平台模式下升级 [Firepower 2100](#) 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级升级 [Firepower 4100/9300](#) 上的 ASA 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中的升级程序。[升级 Firepower 4100/9300 上的 ASA](#)

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 (**copyold_config_urlstartup-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 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。

步骤 2 ASDM: 依次选择工具 > 降级软件。

系统将显示 Downgrade Software 对话框。

步骤 3 对于 ASA 映像，请点击 **Select Image File**。

系统将显示 **Browse File Locations** 对话框。

步骤 4 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。
- **Flash File System** - 点击 **Browse Flash** 以选择本地闪存文件系统上的旧映像文件。

步骤 5 对于 **Configuration**，请点击 **Browse Flash** 以选择预迁移配置文件。

步骤 6 (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 7 点击 **Downgrade**。

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。