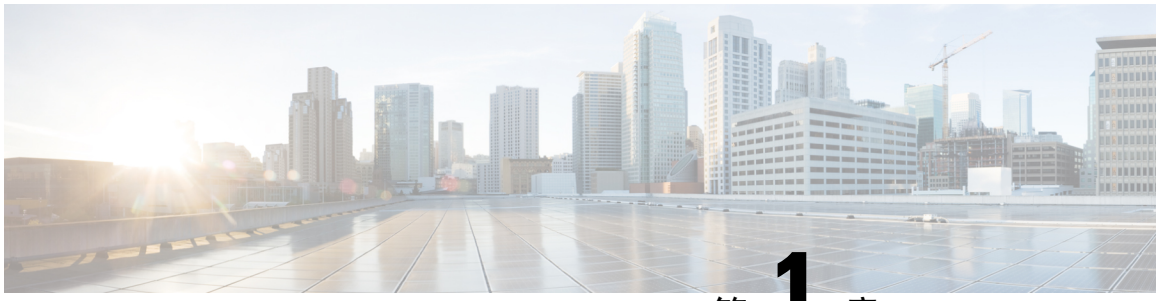
Cisco Secure Firewall ASA 升级指南

上次修改日期: 2022 年 6 月 6 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

目录



第 1 章

规划升级

在升级 Cisco Secure Firewall ASA 之前，应进行以下准备：

- 检查不同版本操作系统之间的兼容性；例如，确保 ASA 版本与 ASA FirePOWER 模块版本兼容。
- 检查当前版本到目标版本的升级路径；确保为每个操作系统所需的任何中间版本做好计划。
- 检查影响您的中间及目标版本的准则和限制，或者会影响故障转移和集群零停机升级。
- 从 Cisco.com 下载所需的全部软件包。
- 备份配置，特别是有配置迁移时。

以下主题说明如何升级 ASA。

升级前的重要准则

检查升级准则和限制，以及每个操作系统的配置迁移。

ASA 升级准则

在升级之前，请检查迁移和所有其他准则。

版本特定的准则和迁移

根据当前的版本，您可能会遇到一次或多次配置迁移，并且在升级时必须考虑适用于起始版本与结束版本之间所有版本的配置准则。

9.19 准则

- **ASDM 7.19(1) 需要 Oracle Java 版本 8u261 或更高版本** - 在升级到 ASDM 7.19 之前，请务必将 Oracle Java（如已使用）更新到 8u261 或更高版本。此版本支持 TLSv1.3，这是升级 ASDM 启动程序所必需的。OpenJRE 不受影响。

9.18 准则

- **9.18(2)/7.18(1.152) 及更高版本中的 ASDM 签名映像支持** - ASA 现在会验证 ASDM 映像是否为思科数字签名映像。如果您尝试使用具有此修复程序的 ASA 版本来运行较早的 ASDM 映像，则系统将阻止 ASDM 并在 ASA CLI 上显示消息“%错误：签名对文件 disk0:/<filename> 无效 (%ERROR: Signature not valid for file disk0:/<filename>)”。ASDM 版本 7.18(1.152) 及更高版本向后兼容所有 ASA 版本，即使是没有安装此修补程序的版本。(CSCwb05291, CSCwb05264)
- **在同一个接口上启用了 HTTPS/ASDM（通过 HTTPS 身份验证）和 SSL 并使用相同的端口时的 9.18(1) 升级问题** - 如果在同一接口上同时启用 SSL（**webvpn** > **启用 (enable)** 接口 *(interface)*）和 HTTPS/ASDM (**http**) 访问，则可以从 **https://***ip_address* 访问 AnyConnect 并从 **https://***ip_address***/admin** 访问 ASDM（均通过端口 443）。但是，如果还启用了 HTTPS 身份验证（**aaa 身份验证 http 控制台**），则从 9.18(1) 开始必须为 ASDM 访问指定其他端口。请确保在使用 **http** 命令升级之前更改端口。(CSCvz92016)
- **ASDM 升级向导** - 由于 ASD API 迁移，您必须使用 ASDM 7.18 或更高版本升级到 ASA 9.18 或更高版本。由于 ASDM 向后兼容较早的 ASA 版本，因此您可以将任何 ASA 版本的 ASDM 升级到 7.18 或更高版本。

9.17 准则

- **9.17(1.13)/7.18(1.152) 及更高版本中的 ASDM 签名映像支持** - ASA 现在会验证 ASDM 映像是否为思科数字签名映像。如果您尝试使用具有此修复程序的 ASA 版本来运行较早的 ASDM 映像，则系统将阻止 ASDM 并在 ASA CLI 上显示消息“%错误：签名对文件 disk0:/<filename> 无效 (%ERROR: Signature not valid for file disk0:/<filename>)”。ASDM 版本 7.18(1.152) 及更高版本向后兼容所有 ASA 版本，即使是没有安装此修补程序的版本。(CSCwb05291, CSCwb05264)
- **在 9.17(1) 及更高版本中不支持无客户端 SSL VPN** - 不再支持无客户端 SSL VPN。
  - **webvpn** - 删除了以下子命令：
    - **apcf**
    - **java-trustpoint**
    - **onscreen-keyboard**
    - **port-forward**
    - **portal-access-rule**
    - **rewrite**
    - **smart-tunnel**

  - **group-policy webvpn** - 删除了以下子命令：
    - **port-forward**
    - **smart-tunnel**
    - **ssl-clientless**

- **ASDM 升级向导** - 由于内部更改，从 2022 年 3 月起，升级向导将不再适用于 ASDM 7.17(1.152) 之前的版本。您必须手动升级到 7.17(1.152) 才能使用向导。

9.16 准则

- **9.16(3.19)/7.18(1.152) 及更高版本中的 ASDM 签名映像支持** - ASA 现在会验证 ASDM 映像是否为思科数字签名映像。如果您尝试使用具有此修复程序的ASA版本来运行较早的ASDM映像，则系统将阻止 ASDM 并在 ASA CLI 上显示消息“%错误：签名对文件 disk0:/<filename> 无效 (%ERROR: Signature not valid for file disk0:/<filename>)”。ASDM 版本 7.18(1.152) 及更高版本向后兼容所有 ASA 版本，即使是没有安装此修补程序的版本。(CSCwb05291, CSCwb05264)
- **不再支持使用 MD5 散列和 DES 加密的 SNMPv3 用户，并且在升级到 9.16(1) 时将删除用户** - 请确保在升级之前使用 **snmp-server user** 命令将任何用户配置更改为更高安全性的算法。
- **9.16(1) 中要求的 SSH 主机密钥操作** - 除了 RSA，我们还增加了对 SSH 的 EDDSA 和 ECDSA 主机密钥的支持。ASA 尝试按以下顺序使用密钥（如存在）：EDDSA、ECDSA，然后是 RSA。当您升级到 9.16(1) 时，ASA 将回退到使用现有 RSA 密钥。但是，我们建议您使用 **crypto key generate** {**eddsa** | **ecdsa**} 命令生成安全性更高的密钥。此外，如果使用 **ssh key-exchange hostkey rsa** 命令将 ASA 明确配置为使用 RSA 密钥，则必须生成 2048 位或更高的密钥。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。
- **在 9.16 及更高版本中，具有 RSA 密钥的证书与 ECDSA 密码不兼容** - 在使用 ECDHE_ECDSA 密码组时，请使用包含支持 ECDSA 的密钥的证书配置信任点。
- **ssh version 命令已在 9.16(1) 中删除** - 已删除此命令。仅支持 SSH 版本 2。
- **SAMLv1 功能已在 9.16(1) 中删除** - 已删除对 SAMLv1 的支持。
- **不支持 9.16(1) 中的 DH 组 2、5 和 24** - 已删除对 SSL DH 组配置中的 DH 组 2、5 和 24 的支持。**ssl dh-group** 命令已更新，以删除命令选项 **group2**、**group5** 和 **group24**。

9.15 准则

- **ASA 9.15(1) 及更高版本中不支持 ASA 5525-X、ASA 5545-X 和ASA 5555-X** - ASA 9.14(x) 是最后支持的版本。对于 ASA FirePOWER 模块，最后支持的版本为 6.6。
- **思科宣布从 ASA 9.17(1) 版本起取消无客户端 SSL VPN 的功能** - 9.17(1) 之前的版本将继续提供有限的支持。
- **对于 Firepower 1010，无效的 VLAN ID 可能会导致问题** - 在升级到 9.15(1) 之前，请确保未将 VLAN 用于 3968 到 4047 范围内的交换机端口。这些 ID 仅用于内部使用，并且 9.15(1) 包含一

项检查，以确保您未使用这些 ID。例如，如果这些 ID 在升级故障转移对后仍在使用，则故障转移对将进入暂停状态。有关详细信息，请参阅 CSCvw33057。

- **SAMLv1 功能弃用** - 已弃用 SAMLv1 支持。
- **ASA 9.15(1) 中的低安全性密码删除** - 已删除对 IKE 和 IPsec 使用的以下不太安全的密码的支持：
  - Diffie-Hellman 组：2 和 24
  - 加密算法：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256、NULL、ESP-3DES、ESP-DES、ESP-MD5-HMAC
  - 散列算法：MD5

注释 尚未删除低安全性 SSH 和 SSL 密码。

在从早期版本的 ASA 升级到版本 9.15(1) 之前，必须更新 VPN 配置以使用 9.15(1) 中支持的密码，否则旧配置将被拒绝。当配置被拒绝时，将根据命令执行以下操作之一：

- 该命令将使用默认密码。
- 将会删除此命令。

在升级之前修复配置对于集群或故障转移部署尤其重要。例如，如果辅助设备升级到 9.15(1)，并且删除的密码从主设备同步到此设备，则辅助设备将拒绝配置。此拒绝可能会导致意外行为，例如无法加入集群。

IKEv1：删除了以下子命令：

- **crypto ikev1 policy** *priority*：
  - **hash md5**
  - **encryption 3des**
  - **encryption des**
  - **group 2**

IKEv2：删除了以下子命令：

- **crypto ikev2 policy** *priority*:
  - **prf md5**
  - **integrity md5**
  - **group 2**
  - **group 24**
  - **encryption 3des**

- **encryption des**
- **encryption null**

IPsec：删除了以下子命令：

- **crypto ipsec ikev1 transform-set *name* esp-3des esp-des esp-md5-hmac**
- **crypto ipsec ikev2 ipsec-proposal *name***
  - **protocol esp integrity md5**
  - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**
- **crypto ipsec profile *name***
  - **set pfs group2 group24**

加密映射：已删除以下子命令：

- **crypto map *name sequence* set pfs group2**
- **crypto map *name sequence* set pfs group24**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group2**

- **重新引入 CRL 分发点配置** - 在 **match-certificate** 命令中重新引入了在 9.13(1) 中删除的静态 CDP URL 配置选项。
- **恢复绕过证书有效性检查选项** - 恢复由于 CRL 或 OCSP 服务器的连接问题而绕过撤销检查的选项。

  恢复了以下子命令：
  - **revocation-check crl none**
  - **revocation-check ocsp none**
  - **revocation-check crl ocsp none**
  - **revocation-check ocsp crl none**

9.14 准则

- **9.14(4.14)/7.18(1.152) 及更高版本中的 ASDM 签名映像支持** - ASA 现在会验证 ASDM 映像是否为思科数字签名映像。如果您尝试使用具有此修复程序的 ASA 版本来运行较早的 ASDM 映像，则系统将阻止 ASDM 并在 ASA CLI 上显示消息“%错误：签名对文件 disk0:/<filename> 无效 (%ERROR: Signature not valid for file disk0:/<filename>)”。ASDM 版本 7.18(1.152) 及更高版本向后兼容所有 ASA 版本，即使是没有安装此修补程序的版本。(CSCwb05291, CSCwb05264)
- **在设备模式下，ASDM Cisco.com 升级向导在 Firepower 1000 和 2100 上失败**，ASDM Cisco.com 升级向导无法升级到 9.14（“**工具**”（**Tools**）>“**检查 ASA/ASDM 更新**”（**Check for ASA /**

ASDM Updates）。该向导可以将 ASDM 从 7.13 升级到 7.14，但 ASA 映像升级显示为灰色。(CSCvt72183) 作为解决方法，请使用以下方法之一：

- 使用 ASA 和 ASDM 上的 **Tools > Upgrade Software from Local** Computer。请注意，9.14(1) 捆绑包中的 ASDM 映像 (7.14(1)) 也存在漏洞 CSCvt72183；您应下载较新的 7.14(1.46) 映像以启用向导的正确功能。
- 使用“工具”（**Tools**）>“检查 ASA/ASDM 更新”（**Check for ASA / ASDM Updates**）升级到 ASDM 7.14（版本为 7.14(1.46)）；然后使用新的 ASDM 升级 ASA 映像。请注意，您可能会看到**严重安装错误**；在这种情况下，请点击**确定**。然后，您必须在**配置**> **设备管理**> **系统映像/配置** > **引导映像/配置**上手动设置启动映像。保存配置并重新加载 ASA。

- **对于 9.14(1)+ 中的故障转移对，ASA 不再与其对等体共享 SNMP 客户端引擎数据。**
- **ASA 9.14(1)+中不支持 cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OIDs (**CSCvy22526**)。**
- **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)
- **已从 inspect skinny 命令中删除了 tls-proxy 关键字，以及对 SCCP/Skinny 加密检测的支持。**
- **ASDM U 升级导航 -** 由于内部更改，此向导仅支持使用 ASDM 7.10(1) 及更高版本；此外，由于映像命名更改，您必须使用 ASDM 7.12(1) 或更高版本以升级到 ASA 9.10(1) 及更高版本。由于 ASDM 向后兼容较早的 ASA 版本，因此您可以升级 ASDM，无论您运行的是哪个 ASA 版本。请注意，ASDM 7.13 和 7.14 不支持 ASA 5512-X、5515-X、5585-X 或 ASASM；您必须升级到 ASDM 7.13(1.101) 或 7.14(1.48) 才能恢复 ASDM 支持。

9.13 准则

- **9.13(1) 及更高版本中 ASAv 需要 2GB 内存 -** 从 9.13(1) 开始，ASAv 的最低内存要求为 2GB。如果当前 ASAv 的内存少于 2GB，您将无法在不增加 ASAv VM 内存的情况下，从早期版本升级到 9.13(1)。在升级之前，您必须调整内存大小。有关 9.13(1) 版本中支持的资源分配（vCPU 和内存）的信息，请参阅 ASAv 入门指南 。
- **在平台模式下将 Firepower 2100 从 9.13 降级到 9.12 或更早版本的降级问题 -** 对于已转换为平台模式的新安装 9.13 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）。您需要将版本恢复为 9.13，或者需要使用 FXOS 擦除配置命令清除配置。如果您最初从早期版本升级到 9.13，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)
- **9.13(1) 中的集群控制链路 MTU 更改 -** 从 9.13(1) 开始，许多集群控制数据包都比以前的版本大。集群控制链路的推荐 MTU 始终为 1600 或更高，并且此值合适。但是，如果将 MTU 设置为 1600，但未能在连接的交换机上匹配 MTU（例如，您在交换机上将 MTU 保留为 1500），则

您将开始看到此不匹配对丢弃的集群控制数据包的影响。请务必将集群控制链路上的所有设备设置为同一 MTU，尤其是 1600 或更高。

- **从 9.13(1) 开始，仅当满足以下任一认证条件时，ASA 才会建立 LDAP/SSL 连接：**
  - LDAP 服务器证书受信任（存在于信任点或 ASA 信任池中）且有效。
  - 来自服务器颁发链的 CA 证书是受信任的（存在于信任点或 ASA 信任池）中，链中的所有从属 CA 证书都已完成且有效。

- **9.13(1) 中已删除本地 CA 服务器** - 当 ASA 配置为本地 CA 服务器时，系统会启用该服务器以颁发数字证书、发布证书吊销列表 (CRL)，并安全地撤销已颁发的证书。此功能已过时，因此已删除 **crypto ca server** 命令。

- **删除 CRL 分发点命令** - 静态 CDP URL 配置命令，即 **crypto-ca-trustpoint crl** 和 **crl url** 已通过其他相关逻辑删除。CDP URL 已移动到 match certificate 命令。

注释 CDP URL 配置得到增强，允许多个 CDP 实例覆盖单个映射（请参阅 CSCvu05216）。

- **删除绕过证书有效性检查选项** - 删除由于 CRL 或 OCSP 服务器的连接问题而绕过撤销检查的选项。

  删除了以下子命令：

  - **revocation-check crl none**
  - **revocation-check ocsp none**
  - **revocation-check crl ocsp none**
  - **revocation-check ocsp crl none**

  因此，在升级后，不再受支持的任何 revocation-check 命令将通过忽略尾随的 none 而过渡到新行为。

注释 这些命令稍后已恢复（请参阅 CSCtb41710）。

- **低安全性密码弃用** - ASA IKE、IPsec 和 SSH 模块使用的多个加密密码被视为不安全，已被弃用。它们将在以后的版本中删除。

  IKEv1：已弃用以下子命令：

  - **crypto ikev1 policy** *priority*：
    - **hash md5**
    - **encryption 3des**

- **encryption des**
- **group 2**
- **group 5**

IKEv2：已弃用以下子命令：

- **crypto ikev2 policy** *priority*
  - **integrity md5**
  - **prf md5**
  - **group 2**
  - **group 5**
  - **group 24**
  - **encryption 3des**
  - **encryption des**（仅当您拥有 DES 加密许可证时，此命令仍然可用）
  - **encryption null**

IPsec：以下命令已弃用：

- **crypto ipsec ikev1 transform-set** *name* **esp-3des esp-des esp-md5-hmac**
- **crypto ipsec ikev2 ipsec-proposal** *name*
  - **protocol esp integrity md5**
  - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**
- **crypto ipsec profile** *name*
  - **set pfs group2 group5 group24**

SSH：已弃用以下命令：

- **ssh cipher integrity custom hmac-sha1-96:hmac-md5: hmac-md5-96**
- **ssh key-exchange group dh-group1-sha1**

SSL：以下命令已弃用：

- **ssl dh-group group2**
- **ssl dh-group group5**
- **ssl dh-group group24**

加密映射：以下命令已弃用：

- **crypto map *name sequence* set pfs group2**
- **crypto map *name sequence* set pfs group5**
- **crypto map *name sequence* set pfs group24**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group2**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group5**

- **在 9.13(1) 中，Diffie-Hellman 组 14** 现在是使用 **crypto map set pfs**、**crypto ipsec profile**、**crypto dynamic-map set pfs** 和 **crypto map set ikev1 phase1-mode**的 IPsec PFS 的 **crypto ikev1 policy**、**ssl dh-group** 和 **crypto ikev2 policy** 下的 **group** 命令的默认设置。以前的默认 Diffie-Hellman 组是组 2。

  当您从 9.13(1) 之前的版本升级时，如果您需要使用旧的默认值（Diffie-Hellman 组 2），则必须手动将 DH 组配置为**组 2**，否则隧道将默认为组 14。由于组 2 将在未来版本中删除，因此您应将隧道尽快移至组 14。

9.12 准则

- **9.12(4.50)/7.18(1.152) 及更高版本中的 ASDM 签名映像支持** - ASA 现在会验证 ASDM 映像是否为思科数字签名映像。如果您尝试使用具有此修复程序的 ASA 版本来运行较早的 ASDM 映像，则系统将阻止 ASDM 并在 ASA CLI 上显示消息“%错误：签名对文件 disk0:/<filename> 无效 (%ERROR: Signature not valid for file disk0:/<filename>)”。ASDM 版本 7.18(1.152) 及更高版本向后兼容所有 ASA 版本，即使是没有安装此修补程序的版本。(CSCwb05291, CSCwb05264)
- ASDM U升级导航 - 由于内部更改，此向导仅支持使用 ASDM 7.10(1) 及更高版本；此外，由于映像命名更改，您必须使用 ASDM 7.12(1) 或更高版本以升级到 ASA 9.10(1) 及更高版本。由于 ASDM 向后兼容较早的 ASA 版本，因此您可以升级 ASDM，无论您运行的是哪个 ASA 版本。
- 9.12(1) 中的 SSH 安全改进和新默认值 - 请参阅以下 SSH 安全改进：
  - 不再支持 SSH 版本 1；仅支持版本 2。**ssh version 1** 命令将迁移到 **ssh version 2**。
  - 支持 Diffie-Hellman 组 14 SHA256 密钥交换。此设置现在为默认值（**ssh key-exchange group dh-group14-sha256**）。先前默认值为组 1 SHA1。请确保 SSH 客户端支持 Diffie-hellman 组 14SHA256。否则，您可能会看到一个错误，例如“不同意密钥交换算法”。例如，OpenSSH 支持 Diffie-hellman 组 14 SHA256。
  - 支持 HMAC-SHA256 完整性加密。默认值现在是高安全性的密码集（hmac-sha1 和 hmac-sha2-256，如 **ssh cipher integrity high**命令所定义）。先前默认值为介质集。
- NULL-SHA TLSv1 密码已弃用并已从 9.12(1) 中删除 - 因为 NULL-SHA 不提供加密，不再是针对现代威胁的安全保护，所以在 **tls-proxy** 模式命令/选项和 **show ssl ciphers all** 输出中列出 TLSv1 支持的密码时，系统将会删除该密码。**ssl cipher tlsv1 all** 和 **ssl cipher tlsv1 custom NULL-SHA** 命令也将被弃用并删除。

- 9.12(1) 中删除了默认信任池 - 为符合 PSB 要求，SEC-AUT-DEFROOT，将从 ASA 映像中删除“默认”受信任 CA 捆绑包。因此， **crypto ca trustpool import default** 和 **crypto ca trustpool import clean default** 命令也会随其他相关逻辑一起删除。但是，在现有部署中的以前使用这些命令导入的证书将保留在原来的位置。
- 9.12(1) 中删除了 **ssl encryption** 命令 - 在 9.3(2) 中，已宣布弃用该命令并将其替换为 **ssl cipher**。在 9.12(1) 中，**ssl encryption** 已删除，不再受支持。

9.10 准则

- 由于内部更改，ASDM 升级向导仅支持使用 ASDM 7.10(1) 及更高版本；此外，由于映像命名更改，您必须使用 ASDM 7.12(1) 或更高版本以升级到 ASA 9.10(1) 及更高版本。由于 ASDM 向后兼容较早的 ASA 版本，因此您可以升级 ASDM，无论您运行的是哪个 ASA 版本。

9.9 准则

- 9.9(2) 及更高版本上大型配置的 ASA 5506-X 内存问题 - 如果升级到 9.9(2) 或更高版本，则由于内存不足，可能会拒绝超大型配置的某些部分，并出现以下消息：“错误：内存不足，无法安装规则”。一种选择是输入 **object-group-search access-control** 命令来提高 ACL 的内存使用率；但是，性能可能会受到影响。或者，您可以降级到 9.9(1)。

9.8 准则

- **9.8(4.45)/7.18(1.152) 及更高版本中的 ASDM 签名映像支持** - ASA 现在会验证 ASDM 映像是否为思科数字签名映像。如果您尝试使用具有此修复程序的 ASA 版本来运行较早的 ASDM 映像，则系统将阻止 ASDM 并在 ASA CLI 上显示消息“%错误：签名对文件 disk0:/<filename> 无效 (%ERROR: Signature not valid for file disk0:/<filename>)”。ASDM 版本 7.18(1.152) 及更高版本向后兼容所有 ASA 版本，即使是没有安装此修补程序的版本。(CSCwb05291, CSCwb05264)
- 在升级到 9.8(2) 或更高版本之前，FIPS 模式要求故障转移密钥至少为 14 个字符 - 在 FIPS 模式下升级到 9.8(2) 或更高版本之前，必须将 **failover key** 或 **failover ipsec pre-shared-key** 更改为至少 14 个字符长。如果故障转移密钥太短，则在升级第一台设备时，系统会拒绝故障转移密钥，并且两台设备都将变为主用状态，直到您将故障转移密钥设置为有效值。
- 请勿将 Amazon Web 服务上的 ASAv 升级到 9.8(1) - 由于存在 CSCve56153，因此不应升级到 9.8(1)。升级后，ASAv 将无法连接。改为升级到 9.8(1.5) 或更高版本。

9.7 准则

- VTI 和 VXLAN VNI 9.7(1) 至 9.7(1.x) 及更高版本的升级问题 - 如果您同时配置虚拟隧道接口 (VTI) 和 VXLAN 虚拟网络标识符 (VNI) 接口，则您无法执行零停机时间升级以进行故障转移；在两台设备的版本相同之前，这些接口类型上的连接将不会复制到备用设备。(CSCvc83062)

9.6 准则

- （ASA 9.6(2) 到 9.7(x)）使用 SSH 公钥身份验证时的升级影响 - 由于对 SSH 身份验证的更新，需要其他配置来启用 SSH 公钥身份验证；因此，使用公钥身份验证的现有 SSH 配置在升级后不再有效。公钥身份验证是 Amazon Web 服务 (AWS) 上的 ASAv 的默认设置，因此 AWS 用户会

遇到此问题。为避免断开SSH连接，您可以在升级之前 更新您的配置。或者，您可以在升级之后使用 ASDM（如果您启用了 ASDM 访问）修复配置。

注释 在 9.8(1) 中恢复了原始行为。

用户名“admin”原始配置示例：

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
  07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

要在升级之前使用 **ssh authentication** 命令，请输入以下命令：

```
aaa authentication ssh console LOCAL
username admin password <password> privilege 15
```

我们建议为该用户名设置一个密码，而不是保留 **nopassword** 关键字（如果存在）。**nopassword** 关键字表示可以输入任何 密码，而不是不能 输入任何密码。在 9.6(2) 之前，SSH 公钥身份验证不需要 **aaa** 命令，因此未触发 **nopassword** 关键字。现在，由于需要 **aaa** 命令，因此如果已经有 **password**（或 **nopassword**）关键字，则它会自动允许对 **username** 进行常规密码身份验证。

在升级之后，**username** 命令不再需要 **password** 或 **nopassword** 关键字；您可以要求用户不能输入密码。因此，要仅强制实施公钥身份验证，请重新输入 **username** 命令：

```
username admin privilege 15
```

- 在 Firepower 9300 上升级 ASA 时的升级影响 - 由于后端的许可证授权命名更改，当您升级到 ASA 9.6(1)/FXOS 1.1(4) 时，启动配置在初始重新加载期间可能无法正确解析；与附加设备授权对应的配置会被拒绝。

  对于独立 ASA，在设备重新加载新版本后，等待至所有授权均得到处理且处于“已授权”状态（**show license all** 或**监控 > 属性 > 智能许可证**），然后只需再次重新加载（**reload** 或**工具 > 系统重新加载**），无需 保存配置。在重新加载后，将正确解析启动配置。

  对于故障转移对，如果您有任何附加设备授权，请按照FXOS发行说明中的升级程序进行操作，但在重新加载每台设备后重置故障转移（**failover reset** 或 **监听 > 属性 > 故障转移 > 状态**，**监听 > 故障转移 > 系统**，或**监听 > 故障转移 > 故障转移组**，然后点击**重置故障转移**）。

  对于集群，请按照 FXOS 版本说明中的升级程序进行操作；无需执行其他操作。

9.5 准则和迁移

- 9.5(2) 新运营商许可证 - 新运营商许可证取代现有的 GTP/GPRS 许可证，还包括对 SCTP 和 Diameter 检测的支持。对于 Firepower 9300 ASA 安全模块，**feature mobile-sp** 命令将自动迁移至 **feature carrier** 命令。
- 9.5(2) 弃用电子邮件代理命令 - 在 ASA 版本 9.5(2) 中，不再支持电子邮件代理命令（**imap4s**、**pop3s**、**smtps**）及子命令。
- 9.5(2) 弃用或迁移 CSD 命令 - 在 ASA 版本 9.5(2) 中，不再支持 CSD 命令（**csd image**、**show webvpn csd image**、**show webvpn csd**、**show webvpn csd hostscan**、**show webvpn csd hostscan image**）。

  以下 CSD 命令将迁移：**csd enable** 迁移至 **hostscan enable**；**csd hostscan image** 迁移至 **hostscan image**。
- 9.5(2) 弃用选择 AAA 命令 - 在 ASA 版本 9.5(2) 中，不再支持以下 AAA 命令及子命令（**override-account-disable**、**authentication crack**）。
- 9.5(1) 弃用了以下命令： **timeout gsn**
- 升级至 9.5(x) 或更高版本时的 ASA 5508-X 和 5516-X 升级问题 - 在升级到 ASA 9.5(x) 或更高版本之前，如果您从未启用巨帧预留，则必须检查最大内存空间。由于制造缺陷，可能应用了错误的软件内存限制。如果在执行以下修复之前升级到 9.5 (x) 或更高版本，则您的设备将在启动时崩溃；在这种情况下，您必须使用 ROMMON 降级到 9.4（使用 ROMMON 加载 ASA 5500-X 系列的映像），执行下面的程序，然后再次升级。

  1. 输入以下命令以检查故障条件：

     ```
     ciscoasa# show memory detail | include Max memory footprint
     Max memory footprint        =    456384512
     Max memory footprint        =            0
     Max memory footprint        =    456384512
     ```

     如果对于“Max memory footprint”返回小于 **456,384,512** 的值，则表示存在故障条件，您必须在升级之前完成余下的步骤。如果显示的内存为 456,384,512 或更大值，则可以跳过此程序的剩余步骤，升级会正常进行。

  2. 进入全局配置模式：

     ```
     ciscoasa# configure terminal
     ciscoasa(config)#
     ```

  3. 暂时启用巨帧预留：

     ```
     ciscoasa(config)# jumbo-frame reservation
     WARNING: This command will take effect after the running-config
     is saved and the system has been rebooted. Command accepted.
     INFO: Interface MTU should be increased to avoid fragmenting
     jumbo frames during transmit
     ```

注释 不要重新加载 ASA。

4. 保存配置：

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

5. 禁用巨帧预留：

```
ciscoasa(config)# no jumbo-frame reservation
WARNING: This command will take effect after the running-config is saved and
the system has been rebooted. Command accepted.
```

注释 不要重新加载 ASA。

6. 再次保存配置：

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

7. 现在，您可以升级到 9.5(x) 或更高版本。

9.4 准则和迁移

- 9.4(1) 统一通信电话代理和公司间媒体引擎代理已弃用 - ASA 9.4 版本不再支持电话代理和 IME 代理。

9.3 准则和迁移

- 9.3(2) 传输层安全 (TLS) 版本 1.2 支持 - 我们现在支持使用 TLS 版本 1.2 面向 ASDM、Clientless SSVPN 和 AnyConnect VPN 进行安全的消息传输。引入或修改了以下命令：ssl client-version、ssl server-version、ssl cipher、ssl trust-point、ssl dh-group。弃用了以下命令：ssl encryption
- 9.3(1) 删除了 AAA Windows NT 域身份验证 - 我们删除了远程 VPN 用户的 NTLM 支持。弃用了以下命令：aaa-server protocol nt

9.2 准则和迁移

自动更新服务器证书验证

默认情况下会启用 9.2(1) 自动更新服务器证书验证。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.
```

配置将迁移为明确不配置验证：

auto-update server no-verification

升级对 ASDM 登录的影响

在从 9.2(2.4) 以前的版本升级到 9.2(2.4) 或更高版本时，升级对 ASDM 登录的影响。如果您从 9.2(2.4) 以前的版本升级到 ASA 版本 9.2(2.4) 或更高版本，并且使用命令授权和 ASDM 定义的用户角色，则具有只读权限的用户将无法登录到 ASDM。必须在升级到权限级别 5 之前或之后更改 **more** 命令；只有管理员级别的用户才能进行此项更改。请注意，对于已定义的用户角色，ASDM 版本 7.3(2) 和更高版本在级别 5 包括 **more** 命令，但预先存在的配置需要手动修复。

ASDM：

1. 依次选择**配置 > 设备管理 > 用户/AAA > AAA 访问 > 授权**，然后点击**配置命令权限**。
2. 选择 **more**，然后点击**编辑**。

3. 将**权限级别**更改为 5，然后点击**确定**。
4. 点击**确定**，然后点击**应用**。

CLI：

```
ciscoasa(config)# privilege cmd level 5 mode exec command more
```

9.1 准则和迁移

- 最大 MTU 现在为 9198 字节 - 如果您的 MTU 设置为高于 9198 的值，则当您升级时，MTU 会自动降级。有时，此 MTU 更改可能导致 MTU 不匹配；请务必将所有连接的设备设置为使用新的 MTU 值。ASA 可使用的最大 MTU 为 9198 字节（通过 CLI 帮助可检查型号的确切限制）。此值不包括第 2 层报头。以前，ASA 允许您将最大 MTU 指定为 65535 字节，这不准确，并可能引发问题。

9.0 准则和迁移

- **IPv6 ACL 迁移** - IPv6 ACL (**ipv6 access-list**) 将迁移至扩展后的 ACL (**access-list extended**)；IPv6 ACL 不再受支持。

如果在接口的同一方向上应用IPv4和IPv6 ACL（**access-group**命令），则这些ACL将会合并：

- 如果在任何非访问组中的位置都未同时使用 IPv4 和 IPv6 ACL，则使用 IPv4 ACL 的名称作为合并的 ACL；IPv6 访问列表将被删除。
- 如果在其他功能中使用了其中至少一个 ACL，将会创建一个名为 *IPv4-ACL-name_IPv6-ACL-name* 的新 ACL；正在使用的 ACL 继续用于其他功能。未在使用的 ACL 将被删除。如果 IPv6 ACL 正在为其他功能所用，它将迁移至同名的扩展 ACL。

- **ACL 任意关键字迁移** - 由于 ACL 同时支持 IPv4 和 IPv6，**any** 关键字现在代表“所有 IPv4 和 IPv6 流量”。任何使用 **any** 关键字的现有 ACL 将全部改为使用 **any4** 关键字，表示“所有 IPv4 流量”。

  此外，还引入了一个单独的关键字来指示“所有 IPv6 流量”：**any6**。

  any4 和 **any6** 关键字不能用于使用 **any** 关键字的所有命令。例如，NAT 功能仅使用 **any** 关键字；any 可表示 IPv4 流量或 IPv6 流量，具体取决于特定 NAT 命令中的上下文。

- **支持端口转换的静态 NAT 升级前要求** - 在版本 9.0 及更高版本中，支持端口转换的静态 NAT 规则仅限访问指定端口的目标 IP 地址。如果您尝试访问其他端口上 NAT 规则未涵盖的的目标 IP 地址，连接将被阻止。两次 NAT 的这一行为也是如此。此外，如果流量与两次 NAT 规则的源 IP 地址不匹配，但与目标 IP 地址匹配，流量将被丢弃，不管目标端口为何。因此，在升级前，必须为允许发送到目标 IP 地址的所有其他流量添加额外规则。

  例如，您具有以下对象 NAT 规则，用于在端口 80 和端口 8080 之间转换传输至内部服务器的 HTTP 流量：

```
object network my-http-server
  host 10.10.10.1
  nat (inside,outside) static 192.168.1.1 80 8080
```

  如果您希望任何其他服务到达服务器（如 FTP），则必须明确允许它们：

```
object network my-ftp-server
  host 10.10.10.1
  nat (inside,outside) static 192.168.1.1 ftp ftp
```

  或者，要允许流量传输到服务器的其他端口，您可以添加将与所有其他端口匹配的一般静态 NAT 规则：

```
object network my-server-1
  host 10.10.10.1
  nat (inside,outside) static 192.168.1.1
```

  对于两次 NAT，您具有以下规则，允许从 192.168.1.0/24 到内部服务器的 HTTP 流量，并在端口 80 和端口 8080 之间进行转换：

```
object network my-real-server
  host 10.10.10.1
object network my-mapped-server
  host 192.168.1.1
```

```
object network outside-real-hosts
  subnet 192.168.1.0 255.255.255.0
object network outside-mapped-hosts
  subnet 10.10.11.0 255.255.255.0
object service http-real
  service tcp destination eq 80
object service http-mapped
  service tcp destination eq 8080
object service ftp-real
  service tcp destination eq 21
nat (outside,inside) source static outside-real-hosts outside-mapped-hosts destination
 static my-mapped-server my-real-server service http-mapped http-real
```

如果希望外部主机访问内部服务器上的其他服务，请为该服务添加另一个NAT规则，例如FTP：

```
nat (outside,inside) source static outside-real-hosts outside-mapped-hosts destination
 static my-mapped-server my-real-server ftp-real ftp-real
```

如果希望其他源地址到达任何其他端口上的内部服务器，则可以为该特定 IP 地址或任何源 IP 地址添加另一个 NAT 规则。确保一般规则的顺序位于特定规则之后。

```
nat (outside,inside) source static any any destination static my-mapped-server
my-real-server
```

8.4 准则和迁移

- 透明模式的配置迁移 - 在 8.4 中，所有透明模式接口现在都属于网桥组。升级到 8.4 后，现有的两个接口归入网桥组 1 中，管理 IP 地址指定给网桥组虚拟接口 (BVI)。当使用一个网桥组时，功能保持不变。现在，可以利用网桥组功能为每个网桥组配置多达四个接口，并且在单模式下或每个情景中，可以创建多达八个网桥组。

注释 请注意，在 8.3 及更早的版本中，作为一项不受支持的配置，您无需 IP 地址即可配置管理接口，并且可以使用设备管理地址访问接口。在 8.4 中，设备管理地址分配至 BVI，管理接口无法再使用该 IP 地址进行访问；管理接口需要其自己的 IP 地址。

- 从 8.3(1)、8.3(2) 和 8.4(1) 升级至 8.4(2) 时，所有身份 NAT 配置此时都将包含 **no-proxy-arp** 和 **route-lookup** 关键字，以便维持现有功能。**unidirectional** 关键字将被删除。

8.3 准则和迁移

请参阅以下指南，它介绍了从 8.3 以前版本的思科 ASA 5500 操作系统 (OS) 升级到版本 8.3 时的配置迁移过程：

思科 ASA 5500 迁移到版本 8.3

集群准则

除以下例外情况，对 ASA 集群的零停机升级没有特殊要求。

注释 未正式支持集群的零停机降级。

- 数据流分流的 Firepower 4100/9300 故障转移和集群无中断升级要求 - 由于数据流分流功能中的漏洞修复，FXOS 和 ASA 的某些组合不支持数据流分流（请参阅Firepower 4100/9300 与 ASA 和威胁防御 的兼容性）。默认情况下会为 ASA 禁用数据流分流。要在使用数据流分流时执行故障转移或集群无中断升级，您需要遵循以下升级路径，以确保在升级到 FXOS 2.3.1.130 或更高版本时始终运行兼容的组合：

  1. 将 ASA 升级到 9.8(3) 或更高版本
  2. 将 FXOS 升级到 2.3.1.130 或更高版本
  3. 将 ASA 升级到您的最终版本

  例如，您运行 FXOS 2.2.2.26/ASA 9.8(1)，希望升级到 FXOS 2.6.1/ASA 9.12(1)，则可以：

  1. 将 ASA 升级到 9.8(4)
  2. 将 FXOS 升级到 2.6.1
  3. 将 ASA 升级到 9.12(1)

- Firepower 4100/9300 集群升级到 FXOS 2.3/ASA 9.9(2) - 运行 ASA 9.8 及更低版本的数据单元无法重新加入控制单元运行 FXOS 2.3/ASA 9.9(2) 或更高版本的集群；在您将 ASA 版本升级到 9.9(2)+ [CSCvi54844] 后，它们将会加入。

- 分布式站点间 VPN - 发生故障的设备上的分布式站点间 VPN 会话最多需要 30 分钟才能在其他设备上稳定。在这段时间内，其他设备故障可能会导致会话丢失。因此，在集群升级期间，要避免流量丢失，请执行以下步骤。请参阅 FXOS/ASA 集群升级过程，以便您可以将这些步骤集成到升级任务中。

注释 从 9.9(1) 升级到 9.9(2) 或更高版本时，分布式站点间 VPN 不支持零停机升级。在 9.9(2) 中，由于主用会话重新分发增强，您不能运行 9.9(2) 上的部分设备和 9.9(1) 上的其他设备。

1. 在没有控制单元的机箱上，使用 ASA 控制台禁用一个模块上的集群。

   cluster group *name*

   no enable

   如果要在机箱及 ASA 上升级 FXOS，请保存配置，以便在机箱重新引导后将禁用集群：

   write memory

2. 等待集群稳定；验证是否已创建所有备份会话。

   show cluster vpn-sessiondb summary

3. 对此机箱上的每个模块重复第 1 步和第 2 步。
4. 使用 FXOS CLI 或 Firepower 机箱管理器在机箱上升级 FXOS。
5. 在机箱联机后，使用 FXOS CLI 或 Firepower 机箱管理器更新每个模块上的 ASA 映像。
6. 在模块联机后，在 ASA 控制台重新启用每个模块上的集群。

   cluster group *name*

   enable

   write memory

7. 在第二个机箱上重复第 1 步至第 6 步，确保先在数据单元上禁用集群，最后是控制单元。

   系统将从升级的机箱中选择一个新的控制单元。

8. 在集群稳定之后，使用主设备上的ASA控制台在集群中的所有模块之间重新分发活动会话。

   cluster redistribute vpn-sessiondb

- 具有集群功能的 9.9(1) 及更高版本的升级问题 - 9.9(1) 及更高版本包含备份分发方面的改进。您应按照如下所述执行升级到 9.9(1) 或更高版本，以利用新的备份分发方法；否则，升级的设备将继续使用旧方法。

  1. 从集群中删除所有辅助设备（使得集群仅包含主设备）。
  2. 升级 1 个辅助设备，然后重新加入集群。
  3. 禁用主设备上的集群功能；将其升级，然后重新加入集群。
  4. 一次一个，升级剩余的辅助设备，然后重新加入集群。

- Firepower 4100/9300 集群升级到 ASA 9.8(1) 及更低版本 - 作为升级过程的一部分，当您在数据设备 (**no enable**) 上禁用集群时，定向到该设备的流量在重定向到新的所有者 [CSCvc85008] 之前，最长可能丢包三秒。
- 升级到具有 CSCvb24585 修复程序的以下版本时，可能不支持零停机升级。此修复将 3DES 从默认（中） SSL 密码移动到低密码集。如果设置仅包含 3DES 的自定义密码，则当连接的另一端使用不再包含 3DES 的默认（中）密码时，可能会出现不匹配情况。
  - 9.1(7.12)
  - 9.2(4.18)
  - 9.4(3.12)
  - 9.4(4)
  - 9.5(3.2)
  - 9.6(2.4)

- 9.6(3)
- 9.7(1)
- 9.8(1)

- 完全限定域名 (FQDN) ACL 的升级问题 - 由于 CSCuv92371，包含 FQDN 的 ACL 可能会导致将 ACL 复制到集群或故障转移对中的到辅助设备时不完整。此漏洞存在于 9.1(7)、9.5(2)、9.6(1) 以及某些临时版本中。我们建议您升级到包括 CSCuy34265 修复的版本：9.1(7.6) 或更高版本、9.5(3) 或更高版本、9.6(2) 或更高版本。不过，由于配置复制的性质，零停机时间升级将不可用。有关不同升级方法的详细信息，请参阅 CSCuy34265。
- Firepower 威胁防御版本 6.1.0 集群不支持站点间集群功能（从 6.2.0 开始，您可以使用 FlexConfig 配置站点间功能）。如果在 FXOS 2.1.1 中部署或重新部署了 6.1.0 集群，并且输入了（不受支持的）站点 ID 值，请删除 FXOS 中每个设备上的站点 ID（设置为 **0**），然后升级到 6.2.3。否则，升级后设备将无法重新加入集群。如果已升级，请在每台设备上将站点 ID 更改为 **0**，以解决问题。请参阅 FXOS 配置指南以查看或更改站点 ID
- 升级至 9.5(2) 或更高版本 (CSCuv82933) - 如果您在升级控制单元之前输入 **show cluster info**，则升级后的数据单元会显示“DEPUTY_BULK_SYNC”；其他不匹配的状态也会显示。您可以忽略此显示；当您升级完所有设备后，状态将正确显示。
- 从 9.0(1) 升级至 9.1(1)(CSCue72961) - 不支持零停机时间升级。

故障转移准则

除以下例外情况，对故障转移的零停机时间升级没有特殊要求：

- 对于 Firepower 1010，无效的 VLAN ID 可能会导致问题 - 在升级到 9.15(1) 之前，请确保未将 VLAN 用于 3968 到 4047 范围内的交换机端口。这些 ID 仅用于内部使用，并且 9.15(1) 包含一项检查，以确保您未使用这些 ID。例如，如果这些 ID 在升级故障转移对后仍在使用，则故障转移对将进入暂停状态。有关详细信息，请参阅 CSCvw33057。
- 数据流分流的 Firepower 4100/9300 故障转移和集群无中断升级要求 - 由于数据流分流功能中的漏洞修复，FXOS 和 ASA 的某些组合不支持数据流分流（请参阅Firepower 4100/9300 与 ASA 和威胁防御 的兼容性）。默认情况下会为 ASA 禁用数据流分流。要在使用数据流分流时执行故障转移或集群无中断升级，您需要遵循以下升级路径，以确保在升级到 FXOS 2.3.1.130 或更高版本时始终运行兼容的组合：

  1. 将 ASA 升级到 9.8(3) 或更高版本
  2. 将 FXOS 升级到 2.3.1.130 或更高版本
  3. 将 ASA 升级到您的最终版本

  例如，您运行 FXOS 2.2.2.26/ASA 9.8(1)，希望升级到 FXOS 2.6.1/ASA 9.12(1)，则可以：

  1. 将 ASA 升级到 9.8(4)
  2. 将 FXOS 升级到 2.6.1

3. 将 ASA 升级到 9.12(1)

- 8.4(6)、9.0(2) 和 9.1(2) 的升级问题 - 由于 CSCug88962，您不能对 8.4(6)、9.0(2) 或 9.1(3) 执行零停机时间升级。您应代之以升级到 8.4(5) 或 9.0(3)。要升级 9.1(1)，由于 CSCuh25271，不能直接升级到 9.1(3) 版本，因此对于零停机时间升级没有解决方法；在升级到 9.1(3) 或更高版本之前，必须先升级到 9.1(2)。
- 完全限定域名 (FQDN) ACL 的升级问题 - 由于 CSCuv92371，包含 FQDN 的 ACL 可能会导致将 ACL 复制到集群或故障转移对中的到辅助设备时不完整。此漏洞存在于 9.1(7)、9.5(2)、9.6(1) 以及某些临时版本中。我们建议您升级到包括 CSCuy34265 修复的版本：9.1(7.6) 或更高版本、9.5(3) 或更高版本、9.6(2) 或更高版本。不过，由于配置复制的性质，零停机时间升级将不可用。有关不同升级方法的详细信息，请参阅 CSCuy34265。
- VTI 和 VXLAN VNI 9.7(1) 至 9.7(1.x) 及更高版本的升级问题 - 如果您同时配置虚拟隧道接口 (VTI) 和 VXLAN 虚拟网络标识符 (VNI) 接口，则您无法执行零停机时间升级以进行故障转移；在两台设备的版本相同之前，这些接口类型上的连接将不会复制到备用设备。(CSCvc83062)
- 在升级到 9.8(2) 或更高版本之前，FIPS 模式要求故障转移密钥至少为 14 个字符 - 在 FIPS 模式下升级到 9.8(2) 或更高版本之前，必须将 **failover key** 或 **failover ipsec pre-shared-key** 更改为至少 14 个字符长。如果故障转移密钥太短，则在升级第一台设备时，系统会拒绝故障转移密钥，并且两台设备都将变为主用状态，直到您将故障转移密钥设置为有效值。
- GTP 检测的升级问题 - 在升级过程中可能会有一些停机时间，因为 GTP 数据结构不会复制到新节点。

其他准则

- 思科 ASA 无客户端 SSL VPN 门户自定义完整性漏洞 - 为 ASA 软件中的无客户端 SSL VPN 修复了多个漏洞，因此您应将软件升级到已修复的版本。有关漏洞的详细信息和已修复 ASA 版本的列表，请参阅 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141008-asa。此外，如果您运行的是具有易受攻击配置的更早 ASA 版本，则无论当前运行什么版本，都应确认门户自定义未受到危害。如果攻击者之前已经危害到自定义对象，则受到危害的对象在您将 ASA 升级到已修复版本后仍保持不变。升级 ASA 可防止此漏洞受到进一步利用，但是它不会修改任何已遭受危害的任何自定义对象，这些对象仍存在于系统上。

Firepower 管理中心升级准则

在升级之前，请检查《FMC 升级指南》中的 Firepower 管理中心准则。

FXOS 升级准则

在升级之前，请阅读所选升级路径中每个 FXOS 版本的发行说明。发行说明包含有关每个 FXOS 版本的重要信息，包括新功能和更改的功能。

升级可能需要必须解决的配置更改。例如，FXOS 版本中支持的新硬件可能还需要您更新 FXOS 固件。

FXOS 发行说明在此处提供： https://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html。

ASA 升级核对表

要计划升级，请使用此核对表。

1. ASA 型号 (ASA 升级路径，第 60 页)：_____

   当前 ASA 版本 (ASA 升级路径，第 60 页)：_____

2. 检查每个型号的 ASA/ASDM 兼容性 (每个机型的 ASA 与 ASDM 兼容性，第 23 页)。

   目标 ASA 版本：_____

   目标 ASDM 版本：_____

3. 检查 ASA 的升级路径 (ASA 升级路径，第 60 页)。是否具有所需的中间版本？是_____ 否_____

   如果是，中间 ASA 版本：_____

4. 下载目标和中间 ASA/ASDM 版本 (下载 ASA 软件，第 79 页)。

   注释 ASDM 包含在 FXOS 软件包的 ASA 中。

5. 您是否具有 ASA FirePOWER 模块？是_____ 否_____

   如果是：

   1. 当前的 ASA FirePOWER 版本：_____

      查看您的当前版本：ASDM (升级路径：ASA FirePOWER 与 ASDM，第 69 页) 或 管理中心 (升级路径：Cisco Secure Firewall Management Center，第 74 页)。

   2. 检查 ASA/FirePOWER 兼容性 (ASA 与 ASA FirePOWER 模块的兼容性，第 33 页)。

      目标 ASA FirePOWER 版本：_____

   3. 检查 ASA FirePOWER 的升级路径 (升级路径：ASA FirePOWER 与 ASDM，第 69 页 或 升级路径：带有 FMC 的 ASA FirePOWER，第 72 页)。是否具有所需的中间版本？是_____ 否_____

      如果是，中间 ASA FirePOWER 版本：

      _____

   4. 下载目标及中间 ASA FirePOWER 版本 (下载 ASA FirePOWER 软件，第 88 页)。

   5. 您是否使用 管理中心 来管理模块？是_____ 否_____

      如果是：

1. 管理中心 型号 (升级路径：Cisco Secure Firewall Management Center， 第 74 页)：
   _____

   当前 管理中心 版本 (升级路径：Cisco Secure Firewall Management Center， 第 74 页)：
   _____
2. 检查 管理中心 的升级路径 (升级路径：Cisco Secure Firewall Management Center， 第 74 页)。是否具有所需的中间版本？是_____ 否_____

   如果是，中间 ASA FirePOWER 版本：
   _____
3. 检查 管理中心 与托管设备的兼容性 (Cisco Secure Firewall Management Center 与 ASA FirePOWER 的兼容性， 第 47 页)。请确保您计划升级 ASA FirePOWER 模块时与 管理中心 的升级步调一致。
4. 下载 管理中心 的目标及中间版本（管理中心升级指南）。

6. 您的 ASA 型号是否是 Firepower 4100 或 9300？是_____ 否_____

   如果是：

   1. 当前 FXOS 版本：_____
   2. 检查 ASA/Firepower 4100 和 9300 兼容性 (Firepower 4100/9300 与 ASA 和 威胁防御 的兼容性， 第 48 页)。

      目标 FXOS 版本：_____
   3. 检查 FXOS 的升级路径 (升级路径：适用于 Firepower 4100/9300 的 FXOS ， 第 77 页)。是否具有所需的中间版本？是_____ 否_____

      如果是，中间 FXOS 版本：_____

      请确保您计划升级 ASA 时与 FXOS 的升级步调一致，以保持兼容性。

      升级期间保持兼容所需的中间 ASA 版本：
      _____
   4. 下载目标及中间 FXOS 版本 (下载适用于 Firepower 4100/9300 的 FXOS， 第 91 页)。

      下载中间 ASA 版本 (下载 ASA 软件， 第 79 页)。
   5. 您是否使用 Radware DefensePro 装饰器应用程序？是_____ 否_____

      如果是：

      1. 当前的 DefensePro 版本：_____
      2. 检查 ASA/FXOS/DefensePro 兼容性 (Radware DefensePro 兼容性， 第 56 页)。

         目标 DefensePro 版本：_____
      3. 下载目标 DefensePro 版本。

7. 检查每个操作系统的升级指南。
   - ASA 升级准则，第 1 页.
   - ASA FirePOWER 准则：请参阅《FMC 升级指南》。
   - 管理中心 准则：请参阅《FMC 升级指南》。
   - FXOS 准则：请参阅每个中间及目标版本的《FXOS 发行说明》。
8. 备份配置。有关备份方法，请参阅每个操作系统的配置指南。

兼容性

本部分包括一些显示平台、操作系统和应用程序间兼容性的表。

每个机型的 ASA 与 ASDM 兼容性

下表列出了当前型号的 ASA 和 ASDM 兼容性。对于较旧的版本和型号，请参阅 Cisco ASA 兼容性。

ASA 9.19

粗体显示的版本是建议版本。

注释
- ASA 9.18(x) 是 Firepower 4110、4120、4140、4150 以及用于 Firepower 9300 的安全模块 SM-24、SM-36 和 SM-44 的最终版本。
- 除非另有说明，否则 ASDM 版本与所有以前的 ASA 版本向后兼容。例如，ASDM 7.19(1) 可以在 ASA 9.10(1) 上管理 ASA 5516-X。
- 新的 ASA 版本需要协调 ASDM 版本或更高版本；您不能将旧版本的 ASDM 与新版本的 ASA 配合使用。例如，您不能将 ASDM 7.18 与 ASA 9.19 配合使用。对于 ASA 临时设备，您可以继续使用当前的 ASDM 版本，除非另有说明。例如，您可以将 ASA 9.19(1.2) 与 ASDM 7.19(1) 配合使用。

表 *1: ASA* 与 *ASDM* 兼容性： *9.19*

ASA	ASDM	ASA 型号							
		ASA 虚拟	Firepower 1010 1120 1140 1150		Firepower 2110 2120 2130 2140	Cisco Secure Firewall 3110 3120 3130 3140	Firepower 4112 4115 4125 4145	Firepower 9300	ISA 3000
9.19(1)	7.19(1)	是	是		是	是	是	是	是

ASA 9.18 至 9.17

粗体显示的版本是建议版本。

注释

- ASA 9.16(x) 是 ASA 5506-X、5506H-X、5506W-X、5508-X 和 5516-X 的最终版本。
- 除非另有说明，否则 ASDM 版本与所有以前的 ASA 版本向后兼容。例如，ASDM 7.17(1) 可以在 ASA 9.10(1) 上管理 ASA 5516-X。
- 新的 ASA 版本需要协调 ASDM 版本或更高版本；您不能将旧版本的 ASDM 与新版本的 ASA 配合使用。例如，您不能将 ASDM 7.17 与 ASA 9.18 配合使用。对于 ASA 临时设备，您可以继续使用当前的 ASDM 版本，除非另有说明。例如，您可以将 ASA 9.17(1.2) 与 ASDM 7.17(1) 配合使用。
- ASA 9.17(1.13) 和 9.18(2) 及更高版本需要使用 ASDM 7.18(1.152) 或更高版本。ASA 现在会验证 ASDM 映像是否为思科数字签名映像。如果您尝试使用具有此修复程序的 ASA 版本来运行 7.18(1.152) 之前的 ASDM 映像，则系统将阻止 ASDM 并在 ASA CLI 上显示消息“%错误：签名对文件 disk0:/<filename> 无效 (%ERROR: Signature not valid for file disk0:/<filename>)”。(CSCwb05291, CSCwb05264)

表 *2: ASA* 与 *ASDM* 兼容性：*9.18* 至 *9.17*

ASA	ASDM	ASA 型号							
		ASA 虚拟	Firepower 1010 1120 1140 1150		Firepower 2110 2120 2130 2140	Secure Firewall 3110 3120 3130 3140	Firepower 4110 4112 4115 4120 4125 4140 4145 4150	Firepower 9300	ISA 3000
9.18(3)	7.19(1.90)	是	是		是	是	是	是	是
9.18(2)	7.18(1.152)	是	是	-	是	是	是	是	是
9.18(1)	7.18(1)	是	是	-	是	是	是	是	是
9.17(1.13)	7.18(1.152)	是	是	-	是	是	是	是	是
9.17(1)	7.17(1)	是	是	-	是	是	是	是	是

ASA 9.16 至 9.15

粗体显示的版本是建议的版本。

注释

- ASA 9.16(x) 是 ASA 5506-X、5506H-X、5506W-X、5508-X 和 5516-X 的最终版本。
- ASA 9.14(x) 是 ASA 5525-X、5545-X 和 5555-X 的最终版本。
- 除非另有说明，否则 ASDM 版本向后兼容所有以前的 ASA 版本。例如，ASDM 7.15(1) 可以管理 ASA 9.10(1) 上的 ASA 5516-X。
- 新的 ASA 版本需要协调 ASDM 版本或更高版本；您不能将旧版本的 ASDM 与新版本的 ASA 配合使用。例如，您不能将 ASDM 7.15 与 ASA 9.16 配合使用。对于 ASA 临时设备，您可以继续使用当前的 ASDM 版本，除非另有说明。例如，您可以将 ASA 9.16(1.15) 与 ASDM 7.16(1) 配合使用。
- ASA 9.16(3.19) 及更高版本需要使用 ASDM 7.18(1.152) 或更高版本。ASA 现在会验证 ASDM 映像是否为思科数字签名映像。如果您尝试使用具有此修复程序的 ASA 版本来运行 7.18(1.152) 之前的 ASDM 映像，则系统将阻止 ASDM 并在 ASA CLI 上显示消息“%错误：签名对文件 disk0:/<filename> 无效 (%ERROR: Signature not valid for file disk0:/<filename>)”。(CSCwb05291, CSCwb05264)

表 *3: ASA* 与 *ASDM* 兼容性：*9.16* 到 *9.15*

ASA	ASDM	ASA 型号						
		ASA 5506-X **5506H-X** **5506W-X** **5508-X** **5516-X**	**ASAv**	**Firepower 1010** **1120** **1140** **1150**	**Firepower 2110** **2120** **2130** **2140**	**Firepower 4110** **4112** **4115** **4120** **4125** **4140** **4145** **4150**	**Firepower 9300**	**ISA 3000**
9.16(4)	7.18(1.152)	是	是	是	是	是	是	是
9.16(3.19)	7.18(1.152)	是	是	是	是	是	是	是
9.16(3)	7.16(1.150)	是	是	是	是	是	是	是
9.16(2)	7.16(1.150)	是	是	是	是	是	是	是
9.16(1)	7.16(1)	是	是	是	是	是	是	是
9.15(1)	7.15(1)	是	是	是	是	是	是	是

ASA 9.14 至 9.13

粗体显示的版本是建议的版本。

注释

- ASA 9.14(x) 是 ASA 5525-X、5545-X 和 5555-X 的最终版本。
- ASA 9.12(x) 是 ASA 5512-X、5515-X、5585-X 和 ASASM 的最终版本。
- 除非另有说明，否则 ASDM 版本与所有以前的 ASA 版本向后兼容。例如，ASDM 7.13(1) 可以在 ASA 9.10(1) 上管理 ASA 5516-X。ASDM 7.13(1) 和 ASDM 7.14(1) 不支持 ASA 5512-X、5515-X、5585-X 和 ASASM；您必须升级到 ASDM 7.13(1.101) 或 7.14(1.48) 才能恢复 ASDM 支持。
- 新的 ASA 版本需要协调 ASDM 版本或更高版本；您不能将旧版本的 ASDM 与新版本的 ASA 配合使用。例如，您不能将 ASDM 7.13 与 ASA 9.14 配合使用。对于 ASA 临时设备，您可以继续使用当前的 ASDM 版本，除非另有说明。例如，您可以将 ASA 9.14(1.2) 与 ASDM 7.14(1) 配合使用。
- ASA 9.14(4.14) 及更高版本需要使用 ASDM 7.18(1.152) 或更高版本。ASA 现在会验证 ASDM 映像是否为思科数字签名映像。如果您尝试使用具有此修复程序的 ASA 版本来运行 7.18(1.152) 之前的 ASDM 映像，则系统将阻止 ASDM 并在 ASA CLI 上显示消息“%错误：签名对文件 disk0:/<filename> 无效 (%ERROR: Signature not valid for file disk0:/<filename>)”。(CSCwb05291, CSCwb05264)

表 *4: ASA* 与 *ASDM* 兼容性：*9.14* 至 *9.13*

ASA	ASDM	ASA 型号							
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5525-X 5545-X 5555-X	ASAv	Firepower 1010 1120 1140 1150	Firepower 2110 2120 2130 2140	Firepower 4110 4112 4115 4120 4125 4140 4145 4150	Firepower 9300	ISA 3000
9.14(4.14)	7.18(1.152)	是	是	是	是	是	是	是	是
9.14(4.6)	7.17(1.152)	是	是	是	是	是	是	是	是
9.14(4)	7.17(1)	是	是	是	是	是	是	是	是
9.14(3)	7.16(1.150)	是	是	是	是	是	是	是	是
9.14(2)	7.14(1.48)	是	是	是	是	是	是	是	是
9.14(1.30)	7.14(1.48)	是	是	是	是	是	是	是	是

ASA	ASDM	ASA 型号							
		ASA 5506-X **5506H-X** **5506W-X** **5508-X** **5516-X**	**ASA 5525-X** **5545-X** **5555-X**	**ASAv**	**Firepower 1010** **1120** **1140** **1150**	**Firepower 2110** **2120** **2130** **2140**	**Firepower 4110** **4112** **4115** **4120** **4125** **4140** **4145** **4150**	**Firepower 9300**	**ISA 3000**
9.14(1.6)	7.14(1.48)	-	-	是 (+ASAv100)	-	-	-	-	-
9.14(1)	7.14(1)	是	是	是	是	是	是	是	是
9.13(1)	7.13(1)	是	是	是	是	是	是（4112 除外）	是	是

ASA 9.12 至 9.5

粗体显示的版本是建议版本。

注释

- ASA 9.12(x) 是 ASA 5512-X、5515-X、5585-X 和 ASASM 的最终版本。
- 除非另有说明，否则 ASDM 版本向后兼容所有以前的 ASA 版本。例如，ASDM 7.12(1) 可以管理 ASA 9.10(1) 上的 ASA 5515-X。
- 新的 ASA 版本需要协调 ASDM 版本或更高版本；您不能将旧版本的 ASDM 与新版本的 ASA 配合使用。例如，您不能将 ASDM 7.10 与 ASA 9.12 配合使用。对于 ASA 临时设备，您可以继续使用当前的 ASDM 版本，除非另有说明。例如，您可以将 ASA 9.12(1.15) 与 ASDM 7.12(1) 配合使用。
- ASA 9.8(4.45) 和 9.12(4.50) 及更高版本需要 ASDM 7.18(1.152) 或更高版本。ASA 现在会验证 ASDM 映像是否为思科数字签名映像。如果您尝试使用具有此修复程序的 ASA 版本来运行 7.18(1.152) 之前的 ASDM 映像，则系统将阻止 ASDM 并在 ASA CLI 上显示消息“%错误：签名对文件 disk0:/<filename> 无效 (%ERROR: Signature not valid for file disk0:/<filename>)”。(CSCwb05291, CSCwb05264)

表 *5: ASA* 与 *ASDM* 兼容性：*9.12* 到 *9.5*

ASA	ASDM	ASA 型号									
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM	Firepower 2110 2120 2130 2140	Firepower 4110 4120 4140 4150	Firepower 4115 4125 4145	Firepower 9300	ISA 3000
9.12(4.50)	7.18(1.152)	是	是	是	是	是	是	是	是	是	是
9.12(4)	7.13(1.101)	是	是	是	是	是	是	是	是	是	是
9.12(3)	7.12(2)	是	是	是	是	是	是	是	是	是	是
9.12(2)	7.12(2)	是	是	是	是	是	是	是	是	是	是
9.12(1)	7.12(1)	是	是	是	是	是	是	是	是	是	是
9.10(1)	7.10(1)	是	是	是	是	是	是	是	-	是	是
9.9(2)	7.9(2)	是	是	是	是	是	是	是	-	是	是
9.9(1)	7.9(1)	是	是	是	是	是	是	是	-	是	是
9.8(4.45)	7.18(1.152)	是	是	是	是	是	是	是	-	是	是
9.8(4)	7.12(1)	是	是	是	是	是	是	是	-	是	是
9.8(3)	7.9(2.152)	是	是	是	是	是	是	是	-	是	是
9.8(2)	7.8(2)	是	是	是	是	是	是	是	-	是	是
9.8(1.200)	不支持	-	-	-	是	-	-	-	-	-	-
9.8(1)	7.8(1)	是	是	是	是 (+ASAv50)	是	-	是	-	是	是
9.7(1.4)	7.7(1)	是	是	是	是	是	-	是	-	是	是
9.6(4)	7.9(1)	是	是	是	是	是	-	是	-	是	是
9.6(3.1)	7.7(1)	是	是	是	是	是	-	是	-	是	是
9.6(2)	7.6(2)	是	是	是	是	是	-	是	-	是	是

ASA	ASDM	ASA 型号									
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM	Firepower 2110 2120 2130 2140	Firepower 4110 4120 4140 4150	Firepower 4115 4125 4145	Firepower 9300	ISA 3000
9.6(1)	7.6(1)	是	是	是	是	是	-	是（4150 除外）	-	是	是
9.5(3.9)	7.6(2)	是	是	是	是	是	-	-	-	-	是
9.5(2.200)	7.5(2.153)	-	-	-	是	-	-	-	-	-	-
9.5.2.2	7.5(2)	-	-	-	-	-	-	-	-	是	-
9.5(2.1)	7.5(2)	-	-	-	-	-	-	-	-	是	-
9.5(2)	7.5(2)	是	是	是	是	是	-	-	-	-	是
9.5(1.200)	7.5(1)	-	-	-	是	-	-	-	-	-	-
9.5(1.5)	7.5(1.112)	是	是	是	是	是	-	-	-	-	-
9.5(1)	7.5(1)	是	是	是	是	是	-	-	-	-	—

ASA 9.4 至 9.3

注释

- ASA 9.2(x) 版本是适用于 ASA 5505 的最终版本。更高版本的 ASDM 继续支持 ASA 5505。
- 除非另有说明，否则 ASDM 版本向后兼容所有以前的 ASA 版本。例如，ASDM 7.6(2) 可以管理 ASA 9.3(3) 上的 ASA 5516-X。

表 *6: ASA* 与 *ASDM* 兼容性：*9.4* 到 *9.3*

ASA	ASDM	ASA 型号						
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM	Firepower 9300	ISA 3000
9.4(4.5)	7.6(2)	是	是	是	是	是	-	-
9.4(3)	7.6(1)	是	是	是	是	是	-	-
9.4(2.146)	7.5(1.112)	-	-	-	-	-	是	-
9.4(2.145)	7.5(1.112)	-	-	-	-	-	是	-
9.4(2)	7.5(1)	是	是	是	是	是	-	-
9.4(1.225)	7.5(1)	-	-	-	-	-	-	是
9.4(1.200)	7.4(2)	-	-	-	是	-	-	-
9.4(1.152)	7.4(3)	-	-	-	-	-	是	-
9.4(1)	7.4(1)	是	是	是	是	是	-	-
9.3(3.8)	7.4(1)	是	是	是	是	是	-	-
9.3(3)	7.4(1)	是	是	是	是	是	-	-
9.3(2.200)	7.3(2)	-	-	-	是	-	-	-
9.3(2)	7.3(3)	是（仅限 5506-X）	是	是	是	是	-	-
	7.3(2)	是（仅限 5506-X）	是	是	是	是	-	-
9.3(1)	7.3(1)	-	是	是	是	是	-	—

ASA 9.2 至 9.1

注释

- ASA 9.2(x) 版本是适用于 ASA 5505 的最终版本。更高版本的 ASDM 继续支持 ASA 5505。
- 除非另有说明，否则 ASDM 版本向后兼容所有以前的 ASA 版本。例如，ASDM 7.4(3) 可以管理 ASA 9.1(1) 上的 ASA 5505。

表 *7: ASA* 与 *ASDM* 兼容性：*9.2* 到 *9.1*

ASA	ASDM	ASA 型号				
		ASA 5505	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM
9.2(4.5)	7.4(3)	是	是	是	是	是
9.2(4)	7.4(3)	是	是	是	是	是
9.2(3)	7.3(1.101)	是	是	是	是	是
9.2(2.4)	7.2(2)	是	是	是	是	是
9.2(1)	7.2(1)	是	是	是	是	是
9.1(7.4)	7.5(2)	是	是	是	-	是
9.1(6)	7.1(7)	是	是	是	-	是
9.1(5)	7.1(6)	是	是	是	-	是
9.1(4)	7.1(5)	是	是	是	-	是
9.1(3)	7.1(4)	是	是	是	-	是
9.1(2)	7.1(3)	是	是	是	-	是
9.1(1)	7.1(1)	是	是	是	-	是

ASA 与 ASA FirePOWER 模块的兼容性

兼容性表

下表显示 ASA、ASDM 和 ASA FirePOWER 支持。如果您使用 FMC 来管理 ASA FirePOWER，则可以忽略 ASDM 要求。

请注意：

- ASA 9.16(x)/ASDM 7.16(x)/Firepower 7.0.0/7.0.x 是 ASA 5508-X、5516-X 和 ISA 3000 上的 ASA FirePOWER 模块的最终版本。
- ASA 9.14(x)/ASDM 7.14(x)/FirePOWER 6.6.0/6.6.x 是 ASA 5525-X、5545-X 和 5555-X 上的 ASA FirePOWER 模块的最终版本。
- ASA 9.12(x)/ASDM 7.12(x)/FirePOWER 6.4.0 是 ASA 5515-X 和 5585-X 上的 ASA FirePOWER 模块的最终版本。
- ASA 9.9(x)/ASDM 7.9(2)/FirePOWER 6.2.3 是 ASA 5506-X 系列和 5512-X 上的 ASA FirePOWER 模块的最终版本。

注释

- 除非另有说明，否则 ASDM 版本与所有以前的 ASA 版本向后兼容。例如，ASDM 7.13(1) 可以在 ASA 9.10(1) 上管理 ASA 5516-X。
- ASA 9.8(4.45)+、9.12(4.50)+、9.14(4.14)+ 和 9.16(3.19)+ 不支持将 ASDM 用于 FirePOWER 模块管理；您必须使用 FMC 来管理具有这些版本的模块。这些 ASA 版本需要使用 ASDM 7.18(1.152) 或更高版本，但 7.16 之后不再为 ASA FirePOWER 模块提供 ASDM 支持。
- ASDM 7.13(1) 和 ASDM 7.14(1) 不支持 ASA 5512-X、5515-X、5585-X 和 ASASM；您必须升级到 ASDM 7.13(1.101) 或 7.14(1.48) 才能恢复 ASDM 支持。

表 *8: ASA* 和 *ASA FirePOWER* 兼容性

ASA FirePOWER 版本	**ASDM** 版本（用于本地管理）	**ASA** 版本	**ASA** 型号						
			5506-X 系列	**5508-X** **5516-X**	**5512-X**	**5515-X**	**5525-X** **5545-X** **5555-X**	**5585-X**（有关 **SSP** 备注，请参阅下文）	**ISA 3000**
7.0.x	ASDM 7.16(1)	ASA 9.16(x) ASA 9.15(x) ASA 9.14(x) ASA 9.13(x) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)	-	是	-	-	-	-	是
6.7.x	ASDM 7.15(1)	ASA 9.16(x) ASA 9.15(x) ASA 9.14(x) ASA 9.13(x) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)	-	是	-	-	-	-	是

ASA FirePOWER 版本	ASDM 版本（用于本地管理）	ASA 版本	ASA 型号						
			5506-X 系列	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（有关 SSP 备注，请参阅下文）	ISA 3000
6.6.x	ASDM 7.14(1)	ASA 9.16(x)（无 5525-X、5545-X、5555-X） ASA 9.15(x)（无 5525-X、5545-X、5555-X） ASA 9.14(x) ASA 9.13(x) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)	-	是	-	-	是	-	是
6.5.0	ASDM 7.13(1)	ASA 9.16(x)（无 5525-X、5545-X、5555-X） ASA 9.15(x)（无 5525-X、5545-X、5555-X） ASA 9.14(x) ASA 9.13(x) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)	-	是	-	-	是	-	是

ASA FirePOWER 版本	ASDM 版本（用于本地管理）	ASA 版本	ASA 型号						
			5506-X 系列	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（有关 SSP 备注，请参阅下文）	ISA 3000
6.4.0	ASDM 7.12(1)	ASA 9.16(x)（无 5515-X、5525-X、5545-X、5555-X、5585-X） ASA 9.15(x)（无 5515-X、5525-X、5545-X、5555-X、5585-X） ASA 9.14(x)（无 5515-X、5585-X） ASA 9.13(x)（无 5515-X、5585-X） ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)	-	是	-	是	是	是	是

ASA FirePOWER 版本	ASDM 版本（用于本地管理）	ASA 版本	ASA 型号						
			5506-X 系列	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（有关 SSP 备注，请参阅下文）	ISA 3000
6.3.0	ASDM 7.10(1)	ASA 9.16(x)（无 5515-X、5525-X、5545-X、5555-X、5585-X） ASA 9.15(x)（无 5515-X、5525-X、5545-X、5555-X、5585-X） ASA 9.14(x)（无 5515-X、5585-X） ASA 9.13(x)（无 5515-X、5585-X） ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)	-	是	-	是	是	是	是

ASA FirePOWER 版本	ASDM 版本（用于本地管理）	ASA 版本	ASA 型号						
			5506-X 系列	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（有关 SSP 备注，请参阅下文）	ISA 3000
6.2.3	ASDM 7.9(2)	ASA 9.16(x)（无 5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X） ASA 9.15(x)（无 5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X） ASA 9.14(x)（无 5506-X、5512-X、5515-X、5585-X） ASA 9.13(x)（无 5506-X、5512-X、5515-X、5585-X） ASA 9.12(x)（无 5506-X、5512-X） ASA 9.10(x)（无 5506-X、5512-X） ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)（无 5506-X）	是	是	是	是	是	是	-

ASA FirePOWER 版本	ASDM 版本（用于本地管理）	ASA 版本	ASA 型号						
			5506-X 系列	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（有关 SSP 备注，请参阅下文）	ISA 3000
6.2.2	ASDM 7.8(2)	ASA 9.16(x)（无 5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X） ASA 9.15(x)（无 5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X） ASA 9.14(x)（无 5506-X、5512-X、5515-X、5585-X） ASA 9.13(x)（无 5506-X、5512-X、5515-X、5585-X） ASA 9.12(x)（无 5506-X、5512-X） ASA 9.10(x)（无 5506-X、5512-X） ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)（无 5506-X）	是	是	是	是	是	是	-

ASA FirePOWER 版本	ASDM 版本（用于本地管理）	ASA 版本	ASA 型号						
			5506-X 系列	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（有关 SSP 备注，请参阅下文）	ISA 3000
6.2.0	ASDM 7.7(1)	ASA 9.16(x)（无 5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X） ASA 9.15(x)（无 5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X） ASA 9.14(x)（无 5506-X、5512-X、5515-X、5585-X） ASA 9.13(x)（无 5506-X、5512-X、5515-X、5585-X） ASA 9.12(x)（无 5506-X、5512-X） ASA 9.10(x)（无 5506-X、5512-X） ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)（无 5506-X）	是	是	是	是	是	是	-

ASA FirePOWER 版本	ASDM 版本（用于本地管理）	ASA 版本	ASA 型号						
			5506-X 系列	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（有关 SSP 备注，请参阅下文）	ISA 3000
6.1.0	ASDM 7.6(2)	ASA 9.16(x)（无 5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X） ASA 9.15(x)（无 5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X） ASA 9.14(x)（无 5506-X、5512-X、5515-X、5585-X） ASA 9.13(x)（无 5506-X、5512-X、5515-X、5585-X） ASA 9.12(x)（无 5506-X、5512-X） ASA 9.10(x)（无 5506-X、5512-X） ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)（无 5506-X）	是	是	是	是	是	是	-

ASA FirePOWER 版本	ASDM 版本（用于本地管理）	ASA 版本	ASA 型号						
			5506-X 系列	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（有关 SSP 备注，请参阅下文）	ISA 3000
6.0.1	ASDM 7.6(1)（没有支持 ASDM 的 ASA 9.4(x)；仅限 FMC）	ASA 9.6(x) ASA 9.5(1.5)、9.5(2)、9.5(3) ASA 9.4(x) 由于 CSCuv91730，我们建议升级到 9.4(2) 及更高版本。	是	是	是	是	是	是	-
6.0.0	ASDM 7.5(1.112)（没有支持 ASDM 的 ASA 9.4(x)；仅限 FMC）	ASA 9.6(x) ASA 9.5(1.5)、9.5(2)、9.5(3) ASA 9.4(x) 由于 CSCuv91730，我们建议升级到 9.4(2) 及更高版本。	是	是	是	是	是	是	-

ASA FirePOWER 版本	ASDM 版本（用于本地管理）	ASA 版本	ASA 型号						
			5506-X 系列	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（有关 SSP 备注，请参阅下文）	ISA 3000
5.4.1.7 及更高版本	ASDM 7.5(1.112)（没有支持 ASDM 的 ASA 9.4(x)；仅限 FMC）		是	是	-	-	-	-	是

ASA FirePOWER 版本	ASDM 版本（用于本地管理）	ASA 版本	ASA 型号						
			5506-X 系列	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（有关 SSP 备注，请参阅下文）	ISA 3000
		ASA 9.16(x)（无 5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X） ASA 9.15(x)（无 5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X） ASA 9.14(x)（无 5506-X） ASA 9.13(x)（无 5506-X） ASA 9.12(x)（无 5506-X） ASA 9.10(x)（无 5506-X） ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3) ASA 9.4(x) ASA 9.4(1.225)（仅限 ISA 3000） ASA 9.3(2)、9.3(3)（无 5508-X 或 5516-X） 由于 CSCuv91730，我们建议升级到 9.3(3.8) 或 9.4(2) 及							

ASA FirePOWER 版本	ASDM 版本（用于本地管理）	ASA 版本	ASA 型号						
			5506-X 系列	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（有关 SSP 备注，请参阅下文）	ISA 3000
		更高版本。							
5.4.1	ASDM 7.3(3)	ASA 9.16(x)（无 5506-X） ASA 9.15(x)（无 5506-X） ASA 9.14(x)（无 5506-X） ASA 9.13(x)（无 5506-X） ASA 9.12(x)（无 5506-X） ASA 9.10(x)（无 5506-X） ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(1.5)、9.5(2)、9.5(3) ASA 9.4(x) ASA 9.3(2)、9.3(3)（仅限 5506-X） 由于 CSCuv91730，我们建议升级到 9.3(3.8) 或 9.4(2) 及更高版本。	是	是	-	-	-	-	-

ASA FirePOWER 版本	ASDM 版本（用于本地管理）	ASA 版本	ASA 型号						
			5506-X 系列	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（有关 SSP 备注，请参阅下文）	ISA 3000
5.4.0.2 +	—	ASA 9.14(x)（无 5512-X、5515-X、5585-X） ASA 9.13(x)（无 5512-X、5515-X、5585-X） ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(1.5)、9.5(2)、9.5(3) ASA 9.4(x) ASA 9.3(2)、9.3(3) 由于 CSCuv91730，我们建议升级到 9.3(3.8) 或 9.4(2) 及更高版本。	-	-	是	是	是	是	-
5.4.0.1	-	ASA 9.2(2.4)、9.2(3)、9.2(4) 由于 CSCuv91730，我们建议升级到 9.2(4.5) 及更高版本。	-	-	是	是	是	是	-

ASA FirePOWER 版本	ASDM 版本（用于本地管理）	ASA 版本	ASA 型号						
			5506-X 系列	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（有关 SSP 备注，请参阅下文）	ISA 3000
5.3.1	-	ASA 9.2(2.4)、9.2(3)、9.2(4) 由于 CSCuv91730，我们建议升级到 9.2(4.5) 及更高版本。	-	-	是	是	是	是	-

ASA 5585-X SSP 兼容性

相同级别的 SSP

ASA FirePOWER SSP-10、-20、-40 和 -60

要求：安装在插槽 *1* 中，在插槽 *0* 中使用匹配级别的 *ASA SSP*

混合级别 SSP

版本 5.4.0.1 开始支持以下组合。

- ASA SSP-10/ASA FirePOWER SSP-40
- ASA SSP-20/ASA FirePOWER SSP-60
- ASA SSP-40/ASA FirePOWER SSP-60

要求：*ASA SSP* 在插槽 *0* 中，*ASA FirePOWER SSP* 在插槽 *1* 中

注释 对于 SSP40/60 组合，您可能会看到一条错误消息，指出此组合不受支持。您可以忽略此消息。

Cisco Secure Firewall Management Center 与 ASA FirePOWER 的兼容性

所有设备均支持通过管理中心 来进行远程管理，但其必须运行与其受管设备相同或更高的版本。这意味着：

- 您可以使用较新的 管理中心（通常有几个主要版本）来管理较旧的设备。但是，我们建议您始终更新整个部署。新功能和已解决的问题通常同时需要 管理中心 及其托管设备上的最新版本。
- 您不能将设备升级超过 管理中心。即使对于维护（第三位数）版本，您也必须首先升级 管理中心。

请注意，在大多数情况下，您可以将较早的设备直接升级到管理中心的主要或维护版本。但有时您可以管理无法直接升级的旧设备，即使该设备支持目标版本。在极少数情况下，特定管理中心设备组合会出现问题。有关版本特定的要求，请参阅版本说明。

表 *9:* 客户部署的 管理中心 设备兼容性

管理中心 版本	您可以管理的最旧设备版本
7.3	6.7
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3
6.5	6.2.3
6.4	6.1
6.3	6.1
6.2.3	6.1
6.2.2	6.1
6.2.1	6.1
6.2	6.1
6.1	5.4.0.2/5.4.1.1
6.0.1	5.4.0.2/5.4.1.1
6.0	5.4.0.2/5.4.1.1
5.4.1	适用于 ASA-5506-X 系列、ASA5508-X 和 ASA5516-X 上的 ASA FirePOWER 的 5.4.1。 适用于 ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X 和 ASA-5585-X 系列上的 ASA FirePOWER 的 5.3.1。 适用于 Firepower 7000/8000 系列和传统设备的 5.3.0。

Firepower 4100/9300 与 ASA 和 威胁防御 的兼容性

下表列出了 ASA 或 威胁防御 应用与 Firepower 4100/9300 之间的兼容性。

下面列出的**粗体**版本是特别鉴别的配套版本。您应尽可能使用这些软件组合，因为 Cisco 会对这些组合执行增强型测试。

有关升级，请参阅以下准则：

- FXOS - 对于 2.2.2 及更高版本，您可以直接升级到更高版本。从 2.2.2 之前的版本升级时，您需要升级到每个中间版本。请注意，您不能将 FXOS 升级到不支持当前逻辑设备版本的版本。您需要分步进行升级：将 FXOS 升级到支持当前逻辑设备的最高版本；然后再将逻辑设备升级到该 FXOS 版本支持的最高版本。例如，如果要从 FXOS 2.2/ASA 9.8 升级到 FXOS 2.13/ASA 9.19，则您必须执行以下升级：
  1. FXOS 2.2→FXOS 2.11（支持 9.8 的最高版本）
  2. ASA 9.8→ASA 9.17（2.11 支持的最高版本）
  3. FXOS 2.11→FXOS 2.13
  4. ASA 9.17→ASA 9.19
- 威胁防御 - 除上述 FXOS 要求外，威胁防御 可能还需要进行临时升级。有关确切的升级路径，请参阅您的版本的管理中心升级指南。
- ASA - ASA 允许您直接从当前版本升级到任何更高版本，但要注意上述 FXOS 要求。

注释 本节仅适用于 Firepower 4100/9300。其他型号只会将 FXOS 用作 ASA 和 威胁防御 统一映像捆绑包中包含的基础操作系统。

注释 FXOS 2.8(1.125)+ 和更高版本不支持用于 ASA SNMP 轮询和陷阱的 ASA 9.14(1) 或 9.14(1.10)；您必须使用 9.14(1.15)+。9.13 或 9.12 等其他版本不受影响。

注释 FXOS 2.12/ASA 9.18/威胁防御 7.2 是 Firepower 4110、4120、4140、4150 以及用于 Firepower 9300 的安全模块 SM-24、SM-36 和 SM-44 的最终版本。

表 *10: ASA* 或 威胁防御 与 *Firepower 4100/9300* 的兼容性

FXOS 版本	Model	ASA 版本	威胁防御版本
2.13	Firepower 4112	**9.19**（推荐） 9.18 9.17 9.16 9.15 9.14	**7.3**（推荐） 7.2 7.1 7.0 6.7 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.19**（推荐） 9.18 9.17 9.16 9.15 9.14 9.13 9.12	**7.3**（推荐） 7.2 7.1 7.0 6.7 6.6 6.5 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

FXOS 版本	Model	ASA 版本	威胁防御版本
2.12	Firepower 4112	**9.18**（推荐） 9.17 9.16 9.15 9.14	**7.2**（推荐） 7.1 7.0 6.7 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.18**（推荐） 9.17 9.16 9.15 9.14 9.13 9.12	**7.2**（推荐） 7.1 7.0 6.7 6.6 6.5 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.18**（推荐） 9.17 9.16 9.15 9.14 9.13 9.12	**7.2**（推荐） 7.1 7.0 6.7 6.6 6.5 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS 版本	Model	ASA 版本	威胁防御版本
2.11	Firepower 4112	**9.17**（推荐） 9.16 9.15 9.14	**7.1**（推荐） 7.0 6.7 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.17**（推荐） 9.16 9.15 9.14 9.13 9.12	**7.1**（推荐） 7.0 6.7 6.6 6.5 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.17**（推荐） 9.16 9.15 9.14 9.13 9.12 9.9 9.8	**7.1**（推荐） 7.0 6.7 6.6 6.5 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS 版本	Model	ASA 版本	威胁防御版本
2.10 注释 要与 7.0.2+ 和 9.16(3.11)+ 兼容，您需要安装 FXOS 2.10(1.179)+。	Firepower 4112	**9.16**（推荐） 9.15 9.14	**7.0**（推荐） 6.7 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.16**（推荐） 9.15 9.14	**7.0**（推荐） 6.7 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.13 9.12	6.5 6.4
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.16**（推荐） 9.15 9.14 9.13	**7.0**（推荐） 6.7 6.6 6.5
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.12 9.9 9.8	6.4
2.9	Firepower 4112	**9.15**（推荐） 9.14	**6.7**（推荐） 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.15**（推荐） 9.14 9.13	**6.7**（推荐） 6.6 6.5
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.12	6.4
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.15**（推荐） 9.14 9.13 9.12	**6.7**（推荐） 6.6 6.5 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.9 9.8	

FXOS 版本	Model	ASA 版本	威胁防御版本
2.8	Firepower 4112	**9.14**	**6.6** 注释 6.6.1+ 需要 FXOS 2.8(1.125)+。
	Firepower 4145 Firepower 4125 Firepower 4115	**9.14**（推荐） 9.13 9.12 注释 Firepower 9300 SM-56 需要 ASA 9.12(2)+	**6.6**（推荐） 注释 6.6.1+ 需要 FXOS 2.8(1.125)+。 6.5 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.14**（推荐） 9.13 9.12 9.9 9.8	**6.6**（推荐） 注释 6.6.1+ 需要 FXOS 2.8(1.125)+。 6.5 6.4 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.7	Firepower 4145 Firepower 4125 Firepower 4115	**9.13**（推荐） 9.12 注释 Firepower 9300 SM-56 需要 ASA 9.12.2+	**6.5**（推荐） 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.13**（推荐） 9.12 9.9 9.8	**6.5**（推荐） 6.4 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS 版本	Model	ASA 版本	威胁防御版本
2.6(1.157)+ 注释 现在，您可以在同一 Firepower 9300 机箱中的不同模块上运行 ASA 9.12 + 和 FTD 6.4+	Firepower 4145 Firepower 4125 Firepower 4115	**9.12** 注释 Firepower 9300 SM-56 需要 ASA 9.12.2+	**6.4**
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12**（推荐） 9.9 9.8	**6.4**（推荐） 6.2.3 6.1
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	**9.12**	不支持
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12**（推荐） 9.9 9.8	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.73)+	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.9**（推荐） 9.8 注释 运行 FXOS 2.3(1.130)+ 时，数据流分流需要 9.8(2.12)+。	**6.2.3**（推荐） 注释 6.2.3.16+ 需要 FXOS 2.3.1.157+ 6.1
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS 版本	Model	ASA 版本	威胁防御版本
2.3(1.66) 2.3(1.58)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.9**（推荐） 9.8 注释 运行 FXOS 2.3(1.130)+ 时，数据流分流需要 9.8(2.12)+。	6.1
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.2	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.8**	威胁防御 版本为 EoL
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.0(1)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	ASA 版本为 EoL	**6.1.0**
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Radware DefensePro 兼容性

下表列出各个型号的安全设备及相关逻辑设备支持的 Radware DefensePro 版本。

表 *11: Radware DefensePro* 兼容性

FXOS 版本	ASA	威胁防御	Radware DefensePro	安全设备型号
2.12.0	9.18(1)	7.2	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.11.1	9.17(1)	7.1	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.10.1	9.16(1)	7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

FXOS 版本	ASA	威胁防御	Radware DefensePro	安全设备型号
2.10.1	9.16(1)	7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.9.1	9.15(1)	6.7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.8.1	9.14(1)	6.6.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

FXOS 版本	ASA	威胁防御	Radware DefensePro	安全设备型号
2.7(1)	9.13(1)	6.5	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.6(1)	9.12(1) 9.10(1)	6.4.0 6.3.0	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.4(1)	9.9(2) 9.10(1)	6.2.3 6.3	8.13.01.09-2	Firepower 9300 Firepower 4110 Firepower 4120 Firepower 4140 Firepower 4150
2.3(1)	9.9(1) 9.9(2)	6.2.2 6.2.3	8.13.01.09-2	Firepower 9300 Firepower 4110（仅限 Firepower 威胁防御） Firepower 4120 Firepower 4140 Firepower 4150
2.2(2)	9.8(1) 9.8(2) 9.8(3)	6.2.0 6.2.2	8.10.01.17-2	Firepower 9300 Firepower 4110（仅限 Firepower 威胁防御） Firepower 4120 Firepower 4140 Firepower 4150

FXOS 版本	ASA	威胁防御	Radware DefensePro	安全设备型号
2.2(1)	9.7(1) 9.8(1)	6.2.0	8.10.01.17-2	Firepower 9300 Firepower 4110（仅限 Firepower 威胁防御） Firepower 4120 Firepower 4140 Firepower 4150
2.1(1)	9.6(2) 9.6(3) 9.6(4) 9.7(1)	不支持	8.10.01.16-5	Firepower 9300 Firepower 4120 Firepower 4140 Firepower 4150
2.0(1)	9.6(1) 9.6(2) 9.6(3) 9.6(4)	不支持	8.10.01.16-5	Firepower 9300 Firepower 4120 Firepower 4140 Firepower 4150
1.1(4)	9.6(1)	不支持	1.1(2.32-3)	9300

升级路径

对于要升级的每个操作系统，请检查支持的升级路径。在某些情况下，可能需要安装过渡升级程序，然后才能升级到最终版本。

ASA 升级路径

要查看您当前的版本和型号，请使用以下方法之一：

- ASDM：选择**主页** > **设备控制面板** > **设备信息**。
- CLI：使用 **show version** 命令。

此表提供ASA的升级路径。某些早期版本需要先进行中间升级，然后才能升级到较新版本。建议的版本以**粗体显示**。

注释 请务必查看起始版本和结束版本之间的每个版本的升级准则。在某些情况下，您可能需要在升级之前更改配置，否则可能会遇到中断。请参阅ASA 升级准则，第 1 页。

注释 有关 ASA 上的安全问题以及哪些版本包含每个问题的修复的指南，请参阅 ASA安全公告。

注释 9.18(x) 是 Firepower 4110、4120、4140、4150 以及用于 Firepower 9300 的安全模块 SM-24、SM-36 和 SM-44 的最终版本。

ASA 9.16(x) 是 ASA 5506-X、5508-X 和 5516-X 的最终版本。

ASA 9.14(x) 是 ASA 5525-X、5545-X 和 5555-X 的最终版本。

ASA 9.12(x) 是 ASA 5512-X、5515-X、5585-X 和 ASASM 的最终版本。

ASA 9.2(x) 版本是适用于 ASA 5505 的最终版本。

ASA 9.1(x) 是 ASA 5510、5520、5540、5550 和 5580 的最终版本。

当前版本	临时升级版本	目标版本
9.18(x)	—	以下任何一个： → **9.19(x)**
9.17(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)**
9.16(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)** → 9.17(x)
9.15(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)**

当前版本	临时升级版本	目标版本
9.14(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x)
9.13(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x)
9.12(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x)
9.10(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)

当前版本	临时升级版本	目标版本
9.9(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)
9.8(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)
9.7(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)

当前版本	临时升级版本	目标版本
9.6(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.5(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.4(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)

当前版本	临时升级版本	目标版本
9.3(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.2(x)	—	以下任何一个： → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.1(2)、9.1(3)、9.1(4)、9.1(5)、9.1(6) 或 9.1(7.4)	—	以下任何一个： → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	以下任何一个： → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)

当前版本	临时升级版本	目标版本
9.0(2), 9.0(3), or 9.0(4)	—	以下任何一个： → 9.14(x) → **9.12(x)** → 9.8(x) → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	以下任何一个： → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	以下任何一个： → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	以下任何一个： → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.4(5+)	—	以下任何一个： → **9.12(x)** → 9.8(x) → 9.1(7.4) → 9.0(4)
8.4(1) 至 8.4(4)	→ 9.0(4)	→ **9.12(x)** → 9.8(x) → 9.1(7.4)

当前版本	临时升级版本	目标版本
8.3(x)	→ 9.0(4)	以下任何一个： → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.2(x) 及更早版本	→ 9.0(4)	以下任何一个： → **9.12(x)** → 9.8(x) → 9.1(7.4)

升级路径：适用于 Firepower 4100/9300 的 ASA 逻辑设备

要查看您当前的版本和型号，请使用以下方法之一：

- Firepower 机箱管理器：选择**概述**，并查看顶部的**型号**和**版本**字段。
- CLI：对于版本，请使用 **show version** 命令，并查看“软件包版本：字段。对于型号，请输入 **scope chassis 1**，然后输入 **show inventory**。

下表提供了 Firepower 4100/9300 上 ASA 逻辑设备的升级路径。

注释 如果要使用在单独的模块上运行的 FTD 和 ASA 逻辑设备升级 Firepower 9300 机箱，请参阅思科 Firepower 4100/9300 升级指南，Firepower 6.0.1 – 7.0.x 或 ASA 9.4(1) – 9.16(x) 包括 FXOS 1.1.1 – 2.10.1。

在左列中查找您的当前版本组合。您可以升级到右列中列出的任何版本组合。这是一个多步骤过程：首先升级 FXOS，然后升级逻辑设备。

请注意，此表仅列出思科的特殊限定版本组合。由于您必须首先升级 FXOS，因此您将短暂运行受支持（但不推荐）的组合，其中 FXOS 位于逻辑设备之前。如需了解最小内部版本和其他详细的兼容性信息，请参阅思科 Firepower 4100/9300 FXOS 兼容性。

注释 对于 FXOS 的早期版本，您必须升级到当前版本与目标版本之间的所有中间版本。到达 FXOS 2.2.2 后，您的升级选项会更广泛。

表 *12:* 升级路径：具有 *ASA* 逻辑设备的 *Firepower 4100/9300*

当前版本	目标版本
具有 ASA 9.15(x) 的 FXOS 2.9.1	→具有 ASA 9.16(x) 的 FXOS 2.10.1

当前版本	目标版本
具有 ASA 9.14(x) 的 FXOS 2.8.1	以下项中的任一个： →具有 ASA 9.16(x) 的 FXOS 2.10.1 → 具有 ASA 9.15(x) 的 FXOS 2.9.1
具有 ASA 9.13(x) 的 FXOS 2.7.1	以下项中的任一个： →具有 ASA 9.16(x) 的 FXOS 2.10.1 → 具有 ASA 9.15(x) 的 FXOS 2.9.1 → 具有 ASA 9.14(x) 的 FXOS 2.8.1
具有 ASA 9.12(x) 的 FXOS 2.6.1	以下项中的任一个： →具有 ASA 9.16(x) 的 FXOS 2.10.1 → 具有 ASA 9.15(x) 的 FXOS 2.9.1 → 具有 ASA 9.14(x) 的 FXOS 2.8.1 →具有 ASA 9.13(x) 的 FXOS 2.7.1
具有 ASA 9.10(x) 的 FXOS 2.4.1	以下项中的任一个： →具有 ASA 9.16(x) 的 FXOS 2.10.1 → 具有 ASA 9.15(x) 的 FXOS 2.9.1 → 具有 ASA 9.14(x) 的 FXOS 2.8.1 →具有 ASA 9.13(x) 的 FXOS 2.7.1 → 具有 ASA 9.12(x) 的 FXOS 2.6.1
具有 ASA 9.9(x) 的 FXOS 2.3.1	以下项中的任一个： →具有 ASA 9.16(x) 的 FXOS 2.10.1 → 具有 ASA 9.15(x) 的 FXOS 2.9.1 → 具有 ASA 9.14(x) 的 FXOS 2.8.1 →具有 ASA 9.13(x) 的 FXOS 2.7.1 → 具有 ASA 9.12(x) 的 FXOS 2.6.1 →具有 ASA 9.10(1) 的 FXOS 2.4.1

当前版本	目标版本
具有 ASA 9.8(x) 的 FXOS 2.2.2	以下项中的任一个： →具有 ASA 9.16(x) 的 FXOS 2.10.1 → 具有 ASA 9.15(x) 的 FXOS 2.9.1 → 具有 ASA 9.14(x) 的 FXOS 2.8.1 →具有 ASA 9.13(x) 的 FXOS 2.7.1 → 具有 ASA 9.12(x) 的 FXOS 2.6.1 → 具有 ASA 9.10(x) 的 FXOS 2.4.1 → 具有 ASA 9.9(x) 的 FXOS 2.3.1
具有 ASA 9.8(1) 的 FXOS 2.2.1	→ 具有 ASA 9.8(x) 的 FXOS 2.2.2
具有 ASA 9.7(x) 的 FXOS 2.1.1	→ 具有 ASA 9.8(1) 的 FXOS 2.2.1
具有 ASA 9.6(2)、9.6(3) 或 9.6(4) 的 FXOS 2.0.1	→ 具有 ASA 9.7(x) 的 FXOS 2.1.1
具有 ASA 9.6(1) 的 FXOS 1.1.4	→ 具有 ASA 9.6(2)、9.6(3) 或 9.6(4) 的 FXOS 2.0.1
具有 ASA 9.5(2) 或 9.5(3) 的 FXOS 1.1.3	→具有 ASA 9.6(1) 的 FXOS 1.1.4
具有 ASA 9.4(2) 的 FXOS 1.1.2	→具有 ASA 9.5(2) 或 9.5(3) 的 FXOS 1.1.3
具有 ASA 9.4(1) 的 FXOS 1.1.1	→FXOS 1.1.2 与 ASA 9.4(2)

降级说明

官方不支持 FXOS 映像降级。思科唯一支持的 FXOS 映像版本降级方法是对设备执行完整的重新映像。

升级路径：ASA FirePOWER 与 ASDM

此表提供由 ASDM FirePOWER 模块管理的升级路径。

通过选择**主页** > **ASA FirePOWER 控制板**，查看 ASDM 中的当前版本。

请注意：

- ASA 9.16(x)/ASDM 7.16(x)/Firepower 7.0.0/7.0.x 是 ASA 5508-X、5516-X 和 ISA 3000 上的 ASA FirePOWER 模块的最终版本。
- ASA 9.14(x)/ASDM 7.14(x)/FirePOWER 6.6.0/6.6.x 是 ASA 5525-X、5545-X 和 5555-X 上的 ASA FirePOWER 模块的最终版本。

- ASA 9.12(x)/ASDM 7.12(x)/FirePOWER 6.4.0 是 ASA 5515-X 和 5585-X 上的 ASA FirePOWER 模块的最终版本。
- ASA 9.9(x)/ASDM 7.9(2)/FirePOWER 6.2.3 是 ASA 5506-X 系列和 5512-X 上的 ASA FirePOWER 模块的最终版本。

在左列中查找当前版本。您可以直接升级到右列中列出的任何版本。

表 *13:* 升级路径：*ASA FirePOWER*（采用 *ASDM*）

当前版本	目标版本
7.0.0 7.0.x 在任何平台上最后支持的 ASA FirePOWER。	→任何更高版本的 7.0.x 维护版本
6.7.0 6.7.x	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.x 以后的任何维护版本
6.6.0 6.6.x ASA 5525-X，5545-X 和 5555-X 的最后 ASA FirePOWER 支持。	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.x 以后的任何维护版本
6.5.0	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本
6.4.0 ASA 5585-X 系列和 ASA 5515-X 的最后 ASA FirePOWER 支持。	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本 → 6.5.0

当前版本	目标版本
6.3.0	以下项中的任一个： →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本 → 6.5.0 → 6.4.0
6.2.3 ASA 5506-X 系列和 ASA 5512-X 的最后 ASA FirePOWER 支持。	以下项中的任一个： →任何 6.6.x 维护版本 → 6.5.0 → 6.4.0 → 6.3.0 由于 CSCvu50400，您不应将具有 ASDM 的 ASA FirePOWER 直接从版本 6.2.3 升级到 6.6.0。虽然升级会成功，但您将遇到严重的性能问题，必须联系 Cisco TAC 寻求修复。相反，我们建议您直接升级到版本 6.6.1 或任何更高版本的维护版本。如果要运行版本 6.6.0，请先升级到中间版本。
6.2.2	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3
6.2.1 此平台上不支持。	-
6.2.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	以下项中的任一个： → 6.2.0
6.0.1	以下项中的任一个： → 6.1.0

当前版本	目标版本
6.0.0	以下项中的任一个： → 6.0.1
5.4.0.2 或 5.4.1.1	以下项中的任一个： → 6.0.0 需要预安装包：FireSIGHT 系统发行说明版本 6.0.0 预安装。

升级路径：带有 FMC 的 ASA FirePOWER

此表提供由 FMC 管理的 ASA FirePOWER 模块 的升级路径。

请注意：

- ASA 9.16(x)/ASDM 7.16(x)/Firepower 7.0.0/7.0.x 是 ASA 5508-X、5516-X 和 ISA 3000 上的 ASA FirePOWER 模块的最终版本。
- ASA 9.14(x)/ASDM 7.14(x)/FirePOWER 6.6.0/6.6.x 是 ASA 5525-X、5545-X 和 5555-X 上的 ASA FirePOWER 模块的最终版本。
- ASA 9.12(x)/ASDM 7.12(x)/FirePOWER 6.4.0 是 ASA 5515-X 和 5585-X 上的 ASA FirePOWER 模块的最终版本。
- ASA 9.9(x)/ASDM 7.9(2)/FirePOWER 6.2.3 是 ASA 5506-X 系列和 5512-X 上的 ASA FirePOWER 模块的最终版本。

在左列中查找当前版本。您可以直接升级到右列中列出的任何版本。

如果需要，您还可以升级 ASA。ASA 与 ASA FirePOWER 版本之间有广泛的兼容性。但通过升级，您可以利用新功能和已解决的问题。有关 ASA 升级路径，请参阅 ASA 升级路径，第 60 页。

表 *14:* 升级路径：带有 *FMC* 的 *ASA FirePOWER*

当前版本	目标版本
7.0.0 7.0.x 在任何平台上最后支持的 ASA FirePOWER。	→任何更高版本的 7.0.x 维护版本
6.7.0 6.7.x	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.x 以后的任何维护版本

当前版本	目标版本
6.6.0 6.6.x ASA 5525-X，5545-X 和 5555-X 的最后 ASA FirePOWER 支持。	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.x 以后的任何维护版本
6.5.0	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本
6.4.0 ASA 5585-X 系列和 ASA 5515-X 的最后 ASA FirePOWER 支持。	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本 → 6.5.0
6.3.0	以下项中的任一个： →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本 → 6.5.0 → 6.4.0
6.2.3 ASA 5506-X 系列和 ASA 5512-X 的最后 ASA FirePOWER 支持。	以下项中的任一个： →6.6.0 或任何 6.6.x 维护版本 → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3
6.2.1 此平台上不支持。	-

当前版本	目标版本
6.2.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	以下项中的任一个： → 6.1.0
6.0.0	以下项中的任一个： → 6.0.1
5.4.0.2 或 5.4.1.1	以下项中的任一个： → 6.0.0 需要预安装包：FireSIGHT 系统发行说明版本 6.0.0 预安装。

升级路径：Cisco Secure Firewall Management Center

此表提供了 FMC 的升级路径，包括 FMCv。

在左列中查找当前版本。您可以直接升级到右列中列出的任何版本。

注释 如果当前版本是在目标版本之后的某个日期发布的，则您可能无法如表中所列进行升级。在这些情况下，升级会快速失败并显示错误，说明两个版本之间存在数据存储不兼容问题。 当前和目标版本的会列出任何特定限制。

表 *15: FMC* 直接升级

当前版本	目标版本
7.0.0 7.0.x 最后支持 FMC 1000、2500 和 4500	→任何更高版本的 7.0.x 维护版本
6.7.0 6.7.x	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.x 以后的任何维护版本
6.6.0 6.6.x 最后支持 FMC 2000 和 4000。	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.x 以后的任何维护版本 **注：**由于数据存储不兼容，您无法从版本 6.6.5+ 升级到版本 6.7.0。我们建议您直接升级到版本 7.0.0+。
6.5.0	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本
6.4.0 最后支持 FMC 750、1500 和 3500。	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本 → 6.5.0
6.3.0	以下项中的任一个： →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本 → 6.5.0 → 6.4.0

当前版本	目标版本
6.2.3	以下项中的任一个： →6.6.0 或任何 6.6.x 维护版本 → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3
6.2.1	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.2.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	以下项中的任一个： → 6.1.0
6.0.0	以下项中的任一个： → 6.0.1 需要预安装包：Firepower 系统发行说明版本 6.0.1 预安装。

当前版本	目标版本
5.4.1.1	以下项中的任一个： → 6.0.0 需要预安装包：FireSIGHT 系统发行说明版本 6.0.0 预安装。

升级路径：适用于 Firepower 4100/9300 的 FXOS

下表提供了 Firepower 4100/9300 机箱的 FXOS 升级路径，无需配置任何逻辑设备。

在左列中查找当前版本。您可以直接升级到右列中列出的任何版本。通常，我们推荐版本序列中的最新 FXOS 内部版本。

注释 对于 FXOS 的早期版本，您必须升级到当前版本与目标版本之间的所有中间版本。到达 FXOS 2.2.2 后，您的升级选项会更广泛。

表 *16:* 升级路径：*Firepower 4100/9300* 上的 *FXOS*

当前 FXOS 版本	目标 FXOS 版本
2.9.1	→ 2.10.1
2.8.1	以下项中的任一个： → 2.10.1 → 2.9.1
2.7.1	以下项中的任一个： → 2.10.1 → 2.9.1 → 2.8.1
2.6.1	以下项中的任一个： → 2.10.1 → 2.9.1 → 2.8.1 → 2.7.1

当前 FXOS 版本	目标 FXOS 版本
2.4.1	以下项中的任一个： → 2.10.1 → 2.9.1 → 2.8.1 → 2.7.1 → 2.6.1
2.3.1	以下项中的任一个： → 2.10.1 → 2.9.1 → 2.8.1 → 2.7.1 → 2.6.1 → 2.4.1
2.2.2	以下项中的任一个： → 2.10.1 → 2.9.1 → 2.8.1 → 2.7.1 → 2.6.1 → 2.4.1 → 2.3.1
2.2.1	→ 2.2.2
2.1.1	→ 2.2.1
2.0.1	→ 2.1.1
1.1.4	→ 2.0.1
1.1.3	→ 1.1.4
1.1.2	→ 1.1.3
1.1.1	→ 1.1.2

从 Cisco.com 下载软件

在开始升级之前，请从 Cisco.com 下载所有软件包。根据操作系统以及使用 CLI 还是 GUI，您应将映像放在服务器上或管理计算机上。有关支持的文件位置的详细信息，请参阅每个安装过程。

注释 需要 Cisco.com 登录信息和思科服务合同。

下载 ASA 软件

如果您正在使用 ASDM 升级向导，则不必预先下载软件。如果要进行手动升级，例如故障转移升级，请将映像下载至您的本地计算机。

对于 CLI 升级，可以将软件置于许多类型的服务器上，包括 TFTP、HTTP 和 FTP。请参阅 ASA 命令参考中的 **copy** 命令。

ASA 软件可以从 Cisco.com 下载。此表包含有关 ASA 的命名约定和信息。

ASA 型号	下载位置	软件包
ASA 5506-X、ASA 5508-X 和 ASA 5516-X	http://www.cisco.com/go/asa-firepower-sw	
	ASA 软件 选择您的型号 > **Adaptive Security Appliance (ASA) Software** > 版本。	ASA 软件文件都有一个文件名，例如：asa962-**lfbff-k8.SPA**。
	ASDM 软件 选择您的型号 > **Adaptive Security Appliance (ASA) Device Manager** > 版本。	ASDM 软件文件都有一个文件名，例如：asdm-762**.bin**。
	REST API 软件 选择您的型号 > **Adaptive Security Appliance REST API Plugin** > 版本。	API 软件文件的文件名类似于 asa-restapi-132-**lfbff-k8.SPA**。要安装 REST API，请参阅 API 快速启动指南。
	ROMMON 软件 选择您的型号 > **ASA Rommon Software** > 版本。	ROMMON 软件文件的文件名类似于 asa5500-firmware-1108**.SPA**。

ASA 型号	下载位置	软件包
ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X	http://www.cisco.com/go/asa-software	
	ASA 软件 选择您的型号 > **Software on Chassis** > **Adaptive Security Appliance (ASA) Software** > 版本。	ASA 软件文件都有一个文件名，例如：asa962-**smp-k8.bin**。ASA 软件文件的文件名类似于 asa962-smp-k8.bin。
	ASDM 软件 选择您的型号 > **Software on Chassis** > **Adaptive Security Appliance (ASA) Device Manager** > 版本。	ASDM 软件文件都有一个文件名，例如：asdm-762**.bin**。
	REST API 软件 选择您的型号 > **Software on Chassis** > **Adaptive Security Appliance REST API Plugin** > 版本。	API 软件文件的文件名类似于 asa-restapi-132-**lfbff-k8.SPA**。要安装 REST API，请参阅 API 快速启动指南。
	适用于思科应用策略基础设施控制器 (APIC) 的 ASA 设备软件包 选择您的型号 > **Software on Chassis** > **ASA for Application Centric Infrastructure (ACI) Device Packages** > 版本。	对于 APIC 1.2(7) 及更高版本，请选择 Policy Orchestration with Fabric Insertion 或 Fabric Insertion-only 软件包。设备软件包软件文件的文件名类似于 asa-device-pkg-1.2.7.10**.zip**。要安装 ASA 设备软件包，请参阅思科 APIC 第 4 层至第 7 层服务部署指南中的“导入设备软件包”一章。

ASA 型号	下载位置	软件包
ASA 5585-X	http://www.cisco.com/go/asa-software	
	ASA 软件 选择您的型号 > **Software on Chassis** > **Adaptive Security Appliance (ASA) Software** > 版本。	ASA 软件文件都有一个文件名，例如：asa962-**smp-k8.bin**。ASA 软件文件的文件名类似于 asa962-smp-k8.bin。
	ASDM 软件 选择您的型号 > **Software on Chassis** > **Adaptive Security Appliance (ASA) Device Manager** > 版本。	ASDM 软件文件都有一个文件名，例如：asdm-762**.bin**。
	REST API 软件 选择您的型号 > **Software on Chassis** > **Adaptive Security Appliance REST API Plugin** > 版本。	API 软件文件的文件名类似于 asa-restapi-132-**lfbff-k8.SPA**。要安装 REST API，请参阅 API 快速启动指南。
	适用于思科应用策略基础设施控制器 (APIC) 的 ASA 设备软件包 选择您的型号 > **Software on Chassis** > **ASA for Application Centric Infrastructure (ACI) Device Packages** > 版本。	对于 APIC 1.2(7) 及更高版本，请选择 Policy Orchestration with Fabric Insertion 或 Fabric Insertion-only 软件包。设备软件包软件文件的文件名类似于 asa-device-pkg-1.2.7.10**.zip**。要安装 ASA 设备软件包，请参阅思科 APIC 第 4 层至第 7 层服务部署指南中的“导入设备软件包”一章。

ASA 型号	下载位置	软件包
ASA 虚拟	http://www.cisco.com/go/asav-software	
	ASA 软件（升级） 依次选择**自适应安全设备 (ASA) 软件** > 版本。	ASA 虚拟升级文件具有 asa962-**smp-k8**等文件名;将此升级文件用于所有虚拟机监控程序。**注意：**.Zip （VMware）、.vhdx （Hyper-v）和 .qcow2 (KVM) 文件仅用于初始部署。 **注释** 要为公共云服务（例如 Amazon Web 服务）升级 ASA 虚拟机，您可以从 Cisco.com 下载上述映像（需要登录 Cisco.com 并获得思科服务合同），并按照本指南中的说明执行升级。无法从公共云服务获取升级映像。
	ASDM 软件（升级） 选择 **Adaptive Security Appliance (ASA) Device Manager** > 版本。	ASDM 软件文件都有一个文件名，例如：asdm-762**.bin**。
	REST API 软件 依次选择**自适应安全设备 REST API 插件** > 版本。	API 软件文件的文件名类似于 asa-restapi-132-**lfbff-k8.SPA**。要安装 REST API，请参阅 API 快速启动指南。
	适用于思科应用策略基础设施控制器 (APIC) 的 ASA 设备软件包 依次选择**适用于以应用为中心的基础设施 (ACI) 的 ASA 设备软件包** > 版本。	对于 APIC 1.2(7) 及更高版本，请选择 Policy Orchestration with Fabric Insertion 或 Fabric Insertion-only 软件包。设备软件包软件文件的文件名类似于 asa-device-pkg-1.2.7.10**.zip**。要安装 ASA 设备软件包，请参阅思科 APIC 第 4 层至第 7 层服务部署指南中的“导入设备软件包”一章。

ASA 型号	下载位置	软件包
Firepower 1010、Firepower 1120、Firepower 1140 和 Firepower 1150	http://www.cisco.com/go/asa-firepower-sw	
	ASA、ASDM 和 FXOS 软件 选择您的型号 > **Adaptive Security Appliance (ASA) Software** > 版本。	ASA 软件包中包括 ASA、ASDM 和 FXOS 软件。ASA 软件包具有文件名，如 cisco-asa-fp1k.9.13.1.**SPA**。
	ASDM 软件（升级） 选择您的型号 > **Adaptive Security Appliance (ASA) Device Manager** > 版本。	使用此映像可使用当前 ASDM 或 ASA CLI 升级到更高版本的 ASDM。ASDM 软件文件都有一个文件名，例如：asdm-7131.**bin**。 **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-7131.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 型号	下载位置	软件包
Firepower 2110、Firepower 2120、Firepower 2130、Firepower 2140	http://www.cisco.com/go/asa-firepower-sw	
	ASA、ASDM 和 FXOS 软件 选择您的型号 > **Adaptive Security Appliance (ASA) Software** > 版本。	ASA 软件包中包括 ASA、ASDM 和 FXOS 软件。ASA 软件包具有文件名，如 cisco-asa-fp2k.9.8.2**.SPA**。
	ASDM 软件（升级） 选择您的型号 > **Adaptive Security Appliance (ASA) Device Manager** > 版本。	使用此映像可使用当前 ASDM 或 ASA CLI 升级到更高版本的 ASDM。ASDM 软件文件都有一个文件名，例如：asdm-782**.bin**。 **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 型号	下载位置	软件包
Cisco Secure Firewall 3110、Cisco Secure Firewall 3120、Cisco Secure Firewall 3130、Cisco Secure Firewall 3140	https://cisco.com/go/asa-secure-firewall-sw	
	ASA、ASDM 和 FXOS 软件 选择您的型号 > **Adaptive Security Appliance (ASA) Software** > 版本。	ASA 软件包中包括 ASA、ASDM 和 FXOS 软件。ASA 软件包具有文件名，如 cisco-asa-fp3k.9.17.1.**SPA**。
	ASDM 软件（升级） 选择您的型号 > **Adaptive Security Appliance (ASA) Device Manager** > 版本。	使用此映像可使用当前 ASDM 或 ASA CLI 升级到更高版本的 ASDM。ASDM 软件文件都有一个文件名，例如：asdm-7171.**bin**。 **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-7171.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 型号	下载位置	软件包
Firepower 4110、Firepower 4112、Firepower 4115、Firepower 4120、Firepower 4125、Firepower 4140、Firepower 4145、Firepower 4150 上的 ASA	http://www.cisco.com/go/firepower4100-software	
	ASA 和 ASDM 软件 选择您的型号 > **Adaptive Security Appliance (ASA) Software** > 版本。	ASA 软件包中同时包括 ASA 和 ASDM。ASA 软件包的文件名类似于 cisco-asa.9.6.2**.SPA.csp**。
	ASDM 软件（升级） 选择您的型号 > **Adaptive Security Appliance (ASA) Device Manager** > 版本。	使用此映像可使用当前 ASDM 或 ASA CLI 升级到更高版本的 ASDM。ASDM 软件文件都有一个文件名，例如：asdm-762**.bin**。 **注释** 在 FXOS 中升级 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**)。
	REST API 软件 选择您的型号 > **Adaptive Security Appliance REST API Plugin** > 版本。	API 软件文件的文件名类似于 asa-restapi-132-**lfbff-k8.SPA**。要安装 REST API，请参阅 API 快速启动指南。

ASA 型号	下载位置	软件包
Firepower 9300 上的 ASA	http://www.cisco.com/go/firepower9300-software	
	ASA 和 ASDM 软件 选择 **Adaptive Security Appliance (ASA) Software** > 版本。	ASA 软件包中同时包括 ASA 和 ASDM。ASA 软件包的文件名类似于 cisco-asa.9.6.2.**SPA.csp**。
	ASDM 软件（升级） 选择 **Adaptive Security Appliance (ASA) Device Manager** > 版本。	使用此映像可使用当前 ASDM 或 ASA CLI 升级到更高版本的 ASDM。ASDM 软件文件都有一个文件名，例如：asdm-762.**bin**。 注释 在 FXOS 中升级 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**)。
	REST API 软件 依次选择**自适应安全设备 REST API 插件** > 版本。	API 软件文件的文件名类似于 asa-restapi-132-**lfbff-k8.SPA**。要安装 REST API，请参阅 API 快速启动指南。
ASA 服务模块	**ASA 软件** http://www.cisco.com/go/asasm-software 选择您的版本。	ASA 软件文件都有一个文件名，例如：asa962-**smp-k8.bin**。ASA 软件文件的文件名类似于 asa962-smp-k8.bin。
	ASDM 软件 http://www.cisco.com/go/asdm-software 选择 **Adaptive Security Appliance (ASA) Device Manager** > 版本。	ASDM 软件文件都有一个文件名，例如：asdm-762.**bin**。ASDM 软件文件的文件名类似于 asdm-762.bin。

ASA 型号	下载位置	软件包
ISA 3000	http://www.cisco.com/go/isa3000-software	
	ASA 软件 选择您的型号 > **Adaptive Security Appliance (ASA) Software** > 版本。	ASA 软件文件都有一个文件名，例如：asa962-**lfbff-k8.SPA**。
	ASDM 软件 选择您的型号 > **Adaptive Security Appliance (ASA) Device Manager** > 版本。	ASDM 软件文件都有一个文件名，例如：asdm-762**.bin**。
	REST API 软件 选择您的型号 > **Adaptive Security Appliance REST API Plugin** > 版本。	API 软件文件的文件名类似于 asa-restapi-132-**lfbff-k8.SPA**。要安装 REST API，请参阅 API 快速启动指南。

下载 ASA FirePOWER 软件

如果您使用 ASDM 管理 ASA FirePOWER 模块，请从 Cisco.com 下载软件。

如果您使用 Cisco Secure Firewall Management Center 软件管理 ASA FirePOWER 模块，则可以使用以下方法之一下载软件：

- 对于次要版本（补丁和修补程序），请使用**系统** > **更新**页上的 Cisco Secure Firewall Management Center **下载更新**功能，该功能可下载 Cisco Secure Firewall Management Center 及其当前正在管理的设备的所有次要升级版本
- 对于主要版本，请从 Cisco.com 下载软件。

下表列出 Cisco.com 上提供的 ASA FirePOWER 软件的命名约定及相关信息。

ASA 型号	下载位置	软件包
ASA 5506-X、ASA 5508-X 和 ASA 5516-X	http://www.cisco.com/go/asa-firepower-sw 依次选择型号 > **ASA FirePOWER 服务软件** > 版本。	• **预安装软件** - 预安装文件（适用于某些升级）具有如下形式的名称：Cisco_Network_Sensor_6.1.0_**Pre-install**-6.0.1.999-32**.sh**。 • **升级软件** - 升级文件具有如下形式的名称：Cisco_Network_Sensor_**Upgrade**-6.2.0-362**.sh**。 • **修补程序软件** - 修补程序文件具有如下形式的名称：Cisco_Network_Sensor_**Hotfix**_AF-6.1.0.2-1**.sh**。 • **引导映像** - 引导映像仅用于重新映像，并且具有如下形式的文件名：asasfr-5500x-**boot**-6.1.0-330**.img**。 • **系统软件安装软件包** - 系统软件安装软件包仅用于重新映像，并具有如下形式的文件名：asasfr-**sys**-6.1.0-330**.pkg**。 • **补丁文件** - 补丁文件具有如下形式的名称：Cisco_Network_Sensor_**Patch**-6.1.0.1-53**.sh**。
ASA 5512-X 至 ASA 5555-X	http://www.cisco.com/go/asa-firepower-sw 依次选择型号 > **ASA FirePOWER 服务软件** > 版本。	• **预安装软件** - 预安装文件（适用于某些升级）具有如下形式的名称：Cisco_Network_Sensor_6.1.0_**Pre-install**-6.0.1.999-32**.sh**。 • **升级软件** - 升级文件具有如下形式的名称：Cisco_Network_Sensor_**Upgrade**-6.2.0-362**.sh**。 • **修补程序软件** - 修补程序文件具有如下形式的名称：Cisco_Network_Sensor_**Hotfix**_AF-6.1.0.2-1**.sh**。 • **引导映像** - 引导映像仅用于重新映像，并且具有如下形式的文件名：asasfr-5500x-**boot**-6.1.0-330**.img**。 • **系统软件安装软件包** - 系统软件安装软件包仅用于重新映像，并具有如下形式的文件名：asasfr-**sys**-6.1.0-330**.pkg**。 • **补丁文件** - 补丁文件具有如下形式的名称：Cisco_Network_Sensor_**Patch**-6.1.0.1-53**.sh**。

ASA 型号	下载位置	软件包
ASA 5585-X	http://www.cisco.com/go/asa-firepower-sw 选择您的型号 > 版本。	• **预安装软件** - 预安装文件（适用于某些升级）具有如下形式的名称：Cisco_Network_Sensor_6.1.0_**Pre-install**-6.0.1.999-32**.sh**。 • **升级软件** - 升级文件具有如下形式的名称：Cisco_Network_Sensor_**Upgrade**-6.2.0-362**.sh**。 • **修补程序软件** - 修补程序文件具有如下形式的名称：Cisco_Network_Sensor_**Hotfix**_AF-6.1.0.2-1**.sh**。 • **引导映像** - 引导映像仅用于重新映像，并且具有如下形式的文件名：asasfr-5500x-**boot**-6.1.0-330**.img**。 • **系统软件安装软件包** - 系统软件安装软件包仅用于重新映像，并具有如下形式的文件名：asasfr-**sys**-6.1.0-330**.pkg**。 • **补丁文件** - 补丁文件具有如下形式的名称：Cisco_Network_Sensor_**Patch**-6.1.0.1-53**.sh**。
ISA 3000	http://www.cisco.com/go/isa3000-software 依次选择型号 > **ASA FirePOWER 服务软件** > 版本。	• **修补程序软件** - 修补程序文件具有如下形式的名称：Cisco_Network_Sensor_**Hotfix**_CX-5.4.1.9-1**.tar**。 • **引导映像** - 引导映像具有如下形式的文件名：asasfr-ISA-3000-**boot**-5.4.1-213**.img**。 • **系统软件安装软件包** - 系统软件安装软件包具有如下形式的文件名：asasfr-sys-5.4.1-213**.pkg**。 • **补丁文件** - 补丁文件具有如下形式的名称：Cisco_Network_Sensor_**Patch**-5.4.1.10-33**.sh**。

下载 Cisco Secure Firewall Management Center软件

Cisco Secure Firewall Management Center 软件位于 思科支持和下载站点。可访问互联网的 管理中心可以直接从思科下载一些补丁和维护版本，大约在两周后即可手动下载。主要版本不支持从思科直接下载。

下载适用于 Firepower 4100/9300 的 FXOS

思科支持和下载站点 上提供适用于 Firepower 4100/9300 的 FXOS 软件包。

- Firepower 4100 系列：http://www.cisco.com/go/firepower4100-software
- Firepower 9300：http://www.cisco.com/go/firepower9300-software

要查找 FXOS 软件包，请选择或搜索您的 Firepower 设备型号，然后浏览至目标版本的 Firepower 可扩展操作系统下载页面。

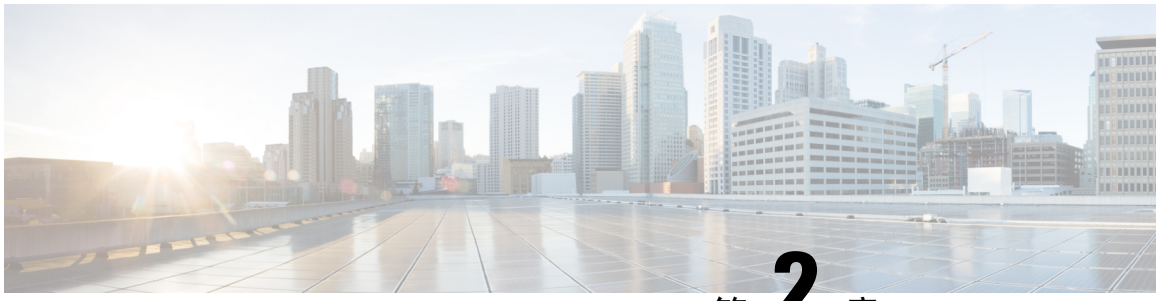
注释 如果计划使用 CLI 升级 FXOS，请将升级软件包复制到 Firepower 4100/9300 可以使用 SCP、SFTP、TFTP 或 FTP 访问的服务器。

表 *17:* 适用于 *Firepower 4100/9300* 的 *FXOS* 软件包

软件包类型	数据包
FXOS 映像	fxos-k9.版本**.SPA**
恢复 (kickstart)	fxos-k9-**kickstart**.版本**.SPA**
恢复（管理器）	fxos-k9-**manager**.版本**.SPA**
恢复（系统）	fxos-k9-**system**.版本**.SPA**
MIB	fxos-**mibs**-fp9k-fp4k.版本**.zip**
固件：Firepower 4100 系列	fxos-k9-fpr4k-**firmware**.版本**.SPA**
固件：Firepower 9300	fxos-k9-fpr9k-**firmware**.版本**.SPA**

备份配置

我们建议您在升级之前备份配置和其他关键文件，尤其是在有配置迁移的情况下。每个操作系统都有不同的执行备份的方法。有关详细信息，请查看 ASA、ASDM、ASA FirePOWER 本地管理、Firepower 管理中心和 FXOS 配置指南。



第 2 章

升级 ASA 设备或 ASA 虚拟

根据本文档中的步骤，升级 ASA 5500-X、Firepower 1000、Firepower 2100、Cisco Secure Firewall 3100、ASA 虚拟、ASASM 和 ISA 3000。

- 升级 Firepower 1000、2100、Cisco Secure Firewall 3100 ， 第 93 页
- 升级 ASA 5500-X、ASA 虚拟、ASASM 或 ISA 3000 ， 第 122 页

升级 Firepower 1000、2100、Cisco Secure Firewall 3100

本文档介绍如何在 Firepower 1000、2100、Cisco Secure Firewall 3100 上为单机或故障转移计划和实施 ASA、FXOS 和 ASDM 升级。

对于 9.12 及更低版本中的 Firepower 2100，仅平台模式可用。在 9.13 及更高版本中，设备模式为默认模式。在 ASA CLI 中使用 **show fxos mode** 命令检查模式。

在 Cisco Secure Firewall 3100 的设备模式下升级 Firepower 1000、2100

本文档介绍如何在 Cisco Secure Firewall 3100 的设备模式下为 Firepower 1000、2100 的单机或故障转移部署计划和实施 ASA、FXOS 和 ASDM 升级。在版本9.13之前，Firepower 2100仅支持平台模式。在9.14及更高版本中，设备模式为默认模式。在9.14及更高版本中，使用ASA上的命令确定当前模式。**show fxos mode** 有关平台模式的程序，请参阅。在平台模式下升级 Firepower 2100 ， 第 106 页

升级独立设备

使用 CLI 或 ASDM 升级独立设备。

使用 CLI 升级独立设备

本节介绍如何在 Cisco Secure Firewall 3100 的设备模式下为 Firepower 1000、Firepower 2100 上安装 ASDM 和 ASA 映像。

开始之前

此程序使用 FTP。对于 TFTP、HTTP 或其他服务器类型，请参阅 ASA 命令参考中的 **copy** 命令。

过程

步骤 1 在特权 EXEC 模式下，将 ASA 软件复制到闪存。

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

步骤 2 将 ASDM 映像复制到闪存中。

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7141.bin disk0:/asdm-7141.bin
```

步骤 3 访问全局配置模式。

configure terminal

示例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

步骤 4 显示当前配置的引导映像（如存在）。

show running-config boot system

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。

示例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

步骤 5 如果**boot system**已配置命令，请将其删除，以便您可以输入新的引导映像。

no boot system disk*n***:/**[*path*/]*asa_image_name*

如果未配置 **boot system** 命令，请跳过此步骤。

示例：

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

步骤 6 将 ASA 映像设置为引导映像（您刚上传的映像）。

boot system disk*n***:/**[*path*/]*asa_image_name*

只能输入 **boot system** 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**无引导系统**命令从引导位置删除新映像，以便当前映像将继续运行。

示例：

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.14.1.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 9.14.1 will do the following:
   - upgrade to the new platform version 2.8.1
   - upgrade to the CSP ASA version 9.14.1
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
ciscoasa(config)#
```

步骤 7 设置要使用的 ASDM 映像（您刚上传的映像）。

asdm image disk*n*:/[*path*/]*asdm_image_name*

您只能配置一个要使用的 ASDM 映像，在这种情况下您不需要先删除现有配置。

示例：

```
ciscoasa(config)# asdm image disk0:/asdm-7141.bin
```

步骤 8 将新设置保存至启动配置：

write memory

步骤 9 重新加载 ASA：

reload

使用 ASDM 从本地计算机升级独立设备

使用**本地计算机中的升级软件**工具，可将映像文件从计算机上传到闪存文件系统以便在Cisco Secure Firewall 3100 的设备模式下升级 Firepower 1000、Firepower 2100。

过程

步骤 1 在主 ASDM 应用窗口中，依次选择**工具** > **从本地计算机升级软件**。

系统将显示**升级软件**对话框。

步骤 2 从**要上传的映像**下拉列表中选择 **ASDM**。

步骤 3 在**本地文件路径**字段中，点击**浏览本地文件**以查找您的 PC 上的文件。

步骤 4 在**闪存文件系统路径**字段中，点击**浏览闪存**以在闪存文件系统中查找目录或文件。

步骤 5 点击**上传映像**。

上传过程可能需要数分钟。

步骤 6 系统会提示您将此映像设置为 ASDM 映像。点击**是**。

步骤 7 系统会提示您退出 ASDM 并保存配置。点击**确定**。

您会退出 **Upgrade** 工具。**注意**：在升级 ASA 软件之后，您将保存配置并重新连接到 ASDM。

步骤 8 重复上述步骤，从**要上传的映像**下拉列表中选择 **ASA**。您也可以使用此程序上传其他文件类型。

步骤 9 依次选择**工具** > **重新加载系统**以重新加载 ASA。

系统将显示新窗口，要求您确认重新加载的详细信息。

a) 点击**重新加载时保存运行配置**单选按钮（默认）。
b) 选择重新加载的时间（例如，默认值 **Now**）。
c) 点击**计划重新加载**。

重新加载开始后，系统将显示**重新加载状态**窗口，指示正在执行重新加载。系统还提供了退出ASDM的选项。

步骤 10 在 ASA 重新加载后，重启 ASDM。

您可以从控制台端口检查重新加载状态，也可以等待几分钟，并尝试使用 ASDM 进行连接，直到成功。

使用 ASDM Cisco.com 向导升级独立设备

Cisco.com 向导中的升级软件工具允许您在 Cisco Secure Firewall 3100 的设备模式下为 Firepower 1000、Firepower 2100 将 ASDM 和 ASA 升级为更新的版本。

在此向导中，您可以执行以下操作：

- 选择 ASA 映像文件和/或 ASDM 映像文件以执行升级。

注释 ASDM 会下载最新的映像版本，其版本号包括内部版本号。例如，如果要下载 9.9(1)，则下载可能是 9.9(1.2)。这是预期行为，因此您可以继续执行计划的升级。

- 查看您所做的升级更改。
- 下载一个或多个映像，并进行安装。

- 查看安装的状态。
- 如果安装成功完成，请重新加载 ASA 以保存配置并完成升级。

开始之前

由于内部更改，此向导仅支持使用ASDM 7.10(1)及更高版本；此外，由于映像命名更改，您必须使用 ASDM 7.12(1) 或更高版本以升级到 ASA 9.10(1) 及更高版本。由于 ASDM 向后兼容较早的 ASA 版本，因此您可以升级 ASDM，无论您运行的是哪个 ASA 版本。

过程

步骤 1 依次选择**工具** > **检查 ASA/ASDM 更新**。

在多情景模式中，从“系统”访问此菜单。

系统将显示 **Cisco.com 身份验证**对话框。

步骤 2 输入 Cisco.com 用户名和密码，然后点击 **Login**。

系统将显示 **Cisco.com 升级向导**。

注释 如果无可用升级，系统将显示对话框。点击**确定**退出向导。

步骤 3 点击**下一步**显示**选择软件**屏幕。

系统将显示当前的 ASA 版本和 ASDM 版本。

步骤 4 如要升级 ASA 版本和 ASDM 版本，请执行以下步骤：

a) 在 **ASA** 区域，选中**升级到**复选框，然后从下拉列表中选择要升级的目标 ASA 版本。
b) 在 **ASDM** 区域，选中**升级到**复选框，然后从下拉列表中选择要升级的目标 ASDM 版本。

步骤 5 点击**下一步**，显示**检查更改**屏幕。

步骤 6 请验证以下项目：

- 已下载的文件是正确的 ASA 映像文件和/或 ASDM 映像文件。
- 希望上传的文件是正确的 ASA 映像文件和/或 ASDM 映像文件。
- 已选择正确的 ASA 启动映像。

步骤 7 点击**下一步**，开始升级安装。

然后，您可以在升级安装过程中查看其状态。

系统将显示**结果**屏幕，其中提供详细信息，如升级安装状态（成功或失败）。

步骤 8 如果升级安装成功，为了使升级版本生效，请选中 **Save configuration and reload device now** 复选框来重新启动 ASA，然后重新启动 ASDM。

步骤 9 点击**完成**，退出向导，保存对配置的更改。

注释　　如要升级到下一个较高版本（如可用），您必须重新启动向导。

步骤 10　在 ASA 重新加载后，重启 ASDM。

您可以从控制台端口检查重新加载状态，也可以等待几分钟，并尝试使用 ASDM 进行连接，直到成功。

升级主用/备用故障转移对

使用 CLI 或 ASDM 升级主用/备用故障转移对，以实现零停机升级。

使用 CLI 升级主用/备用故障转移对

要在 Cisco Secure Firewall 3100 的设备模式下为 Firepower 1000、Firepower 2100 升级主用/备用故障转移对，请执行以下步骤。

开始之前

- 在主用设备上执行以下步骤。对于 SSH 访问，请连接到主用 IP 地址；主用设备始终拥有此 IP 地址。当连接到 CLI 时，通过查看 ASA 提示符确定故障转移状态；您可以配置 ASA 提示符以显示故障转移状态和优先级（主设备或辅助设备），这可用于确定连接到的设备。请参阅 prompt 命令。或者，输入 **show failover** 命令，以查看此设备的状态和优先级（主设备或辅助设备）。
- 此程序使用 FTP。对于 TFTP、HTTP 或其他服务器类型，请参阅 ASA 命令参考中的 **copy** 命令。

过程

步骤 1　在主用设备的特权 EXEC 模式下，将 ASA 软件复制到主用设备闪存：

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

步骤 2　将软件复制到备用设备；请确保指定与主用设备相同的路径：

failover exec mate copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
asa/act# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA disk0:/cisco-asa-fp1k.9.14.1.SPA
```

步骤 3 将 ASDM 映像复制至主用设备闪存：

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7141.bin disk0:/asdm-7141.bin
```

步骤 4 将 ASDM 映像复制至备用设备；请确保指定与主用设备相同的路径：

failover exec mate copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-7141.bin
disk0:/asdm-7141.bin.bin
```

步骤 5 如果您当前未处于全局配置模式，请访问全局配置模式：

configure terminal

步骤 6 显示当前配置的引导映像（如存在）。

show running-config boot system

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。

示例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

步骤 7 如果**boot system**已配置命令，请将其删除，以便您可以输入新的引导映像。

no boot system disk*n***:/**[*path*/]*asa_image_name*

如果未配置 **boot system** 命令，请跳过此步骤。

示例：

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

步骤 8 将 ASA 映像设置为引导映像（您刚上传的映像）。

boot system disk*n***:/**[*path*/]*asa_image_name*

只能输入 **boot system** 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**无引导系统**命令从引导位置删除新映像，以便当前映像将继续运行。

示例：

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.14.1.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 9.14.1 will do the following:
   - upgrade to the new platform version 2.8.1
   - upgrade to the CSP ASA version 9.14.1
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
ciscoasa(config)#
```

步骤 9 设置要使用的 ASDM 映像（您刚上传的映像）：

asdm image disk*n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act(config)# asdm image disk0:/asdm-7141.bin
```

您只能配置一个要使用的 ASDM 映像，在这种情况下您不需要先删除现有配置。

步骤 10 将新设置保存至启动配置：

write memory

这些配置更改会自动保存到备用设备上。

步骤 11 重新加载备用设备，以便启动新映像：

failover reload-standby

等待备用设备完成加载。使用 **show failover** 命令确认备用设备处于备用就绪状态。

步骤 12 强行要求主用设备故障转移至备用设备。

no failover active

如果您从 SSH 会话中断开连接，请重新连接到主 IP 地址（现位于新的主用/以前的备用设备上）。

步骤 13 在新的主用设备上，重新加载以前的主用设备（现为新的备用设备）。

failover reload-standby

示例：

```
asa/act# failover reload-standby
```

注释　如果连接到以前的主用设备控制台端口，应改为输入 **reload** 命令来重新加载以前的主用设备。

使用 ASDM 升级主用/备用故障转移对

要升级主用/备用故障转移对，请在 Cisco Secure Firewall 3100 的设备模式下对 Firepower 1000、Firepower 2100 执行以下步骤。

开始之前

将 ASA 和 ASDM 映像放置在本地管理计算机上。

过程

步骤 1　通过连接到备用 IP 地址，在备用设备上启动 ASDM。

步骤 2　在主 ASDM 应用窗口中，依次选择**工具** > **从本地计算机升级软件**。

系统将显示**升级软件**对话框。

步骤 3　从**要上传的映像**下拉列表中选择 **ASDM**。

步骤 4　在**本地文件路径 (Local File Path)** 字段中，输入指向计算机中文件的本地路径，或者点击**浏览本地文件 (Browse Local Files)** 在计算机中查找该文件。

步骤 5　在 **Flash 文件系统路径 (Flash File System Path)** 字段中，输入闪存文件系统的路径，或者点击**浏览 Flash (Browse Flash)** 在 Flash 文件系统中查找目录或文件。

步骤 6　点击**上传映像**。上传过程可能需要数分钟。

系统提示您将此映像设置为 ASDM 映像时，点击**否 (No)**。您会退出 Upgrade 工具。

步骤 7　重复这些步骤，从**要上传的映像**下拉列表中选择 **ASA**。

当系统提示您将此映像设置为 ASA 映像时，点击**否 (No)**。您会退出 Upgrade 工具。

步骤 8　通过连接到主 IP 地址，将 ASDM 连接到主用 设备，然后使用与您用于备用设备相同的文件位置上传 ASDM 软件。

步骤 9　当系统提示您将该映像设置为 ASDM 映像时，点击**是 (Yes)**。

系统会提示您退出 ASDM 并保存配置。点击**确定**。您会退出 Upgrade 工具。**注意**：在升级 ASA 软件之后，您将保存配置并重新加载 ASDM。

步骤 10　使用与备用设备相同的文件位置上传 ASA 软件。

步骤 11　当系统提示您将该映像设置为 ASA 映像时，点击**是 (Yes)**。

系统将提示您重新加载 ASA 以使用新映像。点击**确定**。您会退出 Upgrade 工具。

步骤 12　点击工具栏上的**保存**图标，保存配置更改。

这些配置更改将自动保存在备用设备上。

步骤 13 通过依次选择**监控** > **属性** > **故障转移** > **状态**，然后点击**重新加载备用**，重新加载备用设备。

留在**系统**窗格中，以监控备用设备何时重新加载。

步骤 14 重新加载备用设备后，强制主用设备执行故障转移到备用设备，方法为：选择**监控** > **属性** > **故障转移** > **状态**，然后点击**设为备用**。

ASDM 将自动重新连接到新主用设备。

步骤 15 重新加载（新）备用设备，方法为：选择**监控** > **属性** > **故障转移** > **状态**，然后点击**重新加载备用**。

升级主用/主用故障转移对

使用 CLI 或 ASDM 升级主用/主用故障转移对，以实现零停机升级。

使用 CLI 升级主用/主用故障转移对

要在主用/主用故障转移配置中升级两台设备，请在 Cisco Secure Firewall 3100 的设备模式下对 Firepower 1000、Firepower 2100 执行以下步骤。

开始之前

- 在主设备上执行这些步骤。
- 在系统执行空间中执行以下步骤。
- 此程序使用 FTP。对于 TFTP、HTTP 或其他服务器类型，请参阅 ASA 命令参考中的 **copy** 命令。

过程

步骤 1 在主设备的特权 EXEC 模式下，将 ASA 软件复制到闪存：

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

步骤 2 将软件复制至辅助设备；请确保指定与主设备相同的路径：

failover exec mate copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
asa/act/pri# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA disk0:/cisco-asa-fp1k.9.14.1.SPA
```

步骤 3 将 ASDM 映像复制至主设备闪存：

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act/pri# ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7141.bin disk0:/asdm-7141.bin
```

步骤 4 将 ASDM 映像复制到辅助设备中；务必指定与主设备相同的路径：

failover exec mate copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-7141.bin
 disk0:/asdm-7141.bin
```

步骤 5 如果您当前未处于全局配置模式，请访问全局配置模式：

configure terminal

步骤 6 显示当前配置的引导映像（如存在）。

show running-config boot system

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。

示例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

步骤 7 如果**boot system**已配置命令，请将其删除，以便您可以输入新的引导映像。

no boot system disk*n***:/**[*path*/]*asa_image_name*

如果未配置 **boot system** 命令，请跳过此步骤。

示例：

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

步骤 8 将 ASA 映像设置为引导映像（您刚上传的映像）。

boot system disk*n***:/**[*path*/]*asa_image_name*

只能输入 **boot system** 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**无引导系统**命令从引导位置删除新映像，以便当前映像将继续运行。

示例：

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.14.1.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 9.14.1 will do the following:
   - upgrade to the new platform version 2.8.1
   - upgrade to the CSP ASA version 9.14.1
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
ciscoasa(config)#
```

步骤 9 设置要使用的 ASDM 映像（您刚上传的映像）。

asdm image disk*n***:/**[*path*/]*asdm_image_name*

示例：

```
asa/act/pri(config)# asdm image disk0:/asdm-7141.bin
```

您只能配置一个要使用的 ASDM 映像，在这种情况下您不需要先删除现有配置。

步骤 10 将新设置保存至启动配置。

write memory

这些配置更改会自动保存到辅助设备上。

步骤 11 使两个故障转移组在主设备上均处于活动状态。

failover active group 1

failover active group 2

示例：

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

步骤 12 重新加载辅助设备，以便启动新映像：

failover reload-standby

等待辅助设备完成加载。使用 **show failover** 命令确认两个故障转移组均处于备用就绪状态。

步骤 13 强行要求两个故障转移组在辅助设备上变为活动状态：

no failover active group 1

no failover active group 2

示例：

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

如果您从 SSH 会话中断开连接，请重新连接到故障转移组 1 IP 地址（现位于辅助设备上）。

步骤 14 重新加载主设备：

failover reload-standby

示例：

```
asa/act/sec# failover reload-standby
```

注释　　如果已连接到主设备控制台端口，应改为输入 **reload** 命令来重新加载主设备。

您可能从 SSH 会话中断开连接。

步骤 15 如果故障转移组配置了 **preempt** 命令，则抢占延迟过后，它们将在其指定设备上自动变为主用状态。

使用 ASDM 升级主用/主用故障转移对

要在主用/主用故障转移配置中升级两台设备，请在 Cisco Secure Firewall 3100 的设备模式下对 Firepower 1000、Firepower 2100 执行以下步骤。

开始之前

- 在系统执行空间中执行以下步骤。
- 将 ASA 和 ASDM 映像放置在本地管理计算机上。

过程

步骤 1 通过连接到故障转移组 2 中的管理地址，在辅助设备上启动 ASDM。

步骤 2 在主 ASDM 应用窗口中，依次选择**工具** > **从本地计算机升级软件**。

系统将显示**升级软件**对话框。

步骤 3 从**要上传的映像**下拉列表中选择 **ASDM**。

步骤 4 在**本地文件路径 (Local File Path)** 字段中，输入指向计算机中文件的本地路径，或者点击**浏览本地文件 (Browse Local Files)** 在 PC 中查找文件。

步骤 5 在 **Flash 文件系统路径 (Flash File System Path)** 字段中，输入闪存文件系统的路径，或者点击**浏览 Flash (Browse Flash)** 在闪存文件系统中查找目录或文件。

步骤 6 点击**上传映像**。上传过程可能需要数分钟。

系统提示您将此映像设置为 ASDM 映像时，点击**否 (No)**。您会退出 Upgrade 工具。

步骤 7 重复上述步骤，从**要上传的映像**下拉列表中选择 **ASA**。

当系统提示您将此映像设置为 ASA 映像时，点击**否 (No)**。您会退出 Upgrade 工具。

步骤 8 通过连接至故障转移组 1 中的管理 IP 地址，将 ASDM 连接至主设备，并使用辅助设备上所用的相同文件位置上传 ASDM 软件。

步骤 9 当系统提示您将该映像设置为 ASDM 映像时，点击**是 (Yes)**。

系统会提示您退出 ASDM 并保存配置。点击**确定**。您会退出 Upgrade 工具。**注意**：在升级 ASA 软件之后，您将保存配置并重新加载 ASDM。

步骤 10 使用与辅助设备相同的文件位置上传 ASA 软件。

步骤 11 当系统提示您将该映像设置为 ASA 映像时，点击**是 (Yes)**。

系统将提示您重新加载 ASA 以使用新映像。点击**确定**。您会退出 Upgrade 工具。

步骤 12 点击工具栏上的**保存**图标，保存配置更改。

这些配置更改在辅助设备上会自动保存。

步骤 13 通过选择**监控** > **故障转移** > **故障转移组号**（其中**编号**是您要移动至主设备的故障转移组的编号）并点击**设为主用**，使两个故障转移组在主设备上均处于活动状态。

步骤 14 重新加载辅助设备，方法为：选择**监控** > **故障转移** > **系统**，然后点击**重新加载备用**。

保持在**系统**窗格上，以监控辅助设备何时加载。

步骤 15 辅助设备启动后，通过选择**监控** > **故障转移** > **故障转移组号**（其中**号**是您要移动至辅助设备的故障转移组的编号）并点击**设为备用**，使两个故障转移组在辅助设备上均处于活动状态。

ASDM 将自动重新连接到辅助设备上的故障转移组 1 IP 地址。

步骤 16 重新加载主设备，方法为：选择**监控** > **故障转移** > **系统**，然后点击**重新加载备用**。

步骤 17 如果故障转移组被配置为“启用抢占”，在抢占延迟过后，它们会在其指定设备上自动变为活动状态。ASDM 将自动重新连接到主设备上的故障转移组 1 IP 地址。

在平台模式下升级 Firepower 2100

本文档介绍如何处于平台模式下的 Firepower 2100 的单机或故障转移部署计划和实施 ASA、FXOS 和 ASDM 升级。在版本9.13之前，Firepower 2100仅支持平台模式。在9.14及更高版本中，设备模式为默认模式。在9.14及更高版本中，使用ASA上的命令确定当前模式。**show fxos mode** 有关设备模式的程序，请参阅。在 Cisco Secure Firewall 3100 的设备模式下升级 Firepower 1000、2100 ，第 93 页

升级独立设备

使用 FXOS CLI 或 Firepower 机箱管理器升级独立设备。

使用 Firepower 机箱管理器升级独立设备

本部分介绍如何升级独立设备的 ASA 捆绑包。您将从管理计算机上传软件包。

过程

步骤 1 连接 Firepower 机箱管理器。

步骤 2 依次选择**系统** > **更新**。
可用更新部分显示机箱上的可用软件包列表。

步骤 3 点击**上传映像**，从管理计算机上传新软件包。

步骤 4 点击**选择文件**，导航到并选择要上传的软件包。

步骤 5 点击**上传**。

所选软件包将上传到机箱。**上传映像**对话框显示上传状态。等待出现**成功**对话框，然后点击**确定**。完成上传后，系统会自动验证映像的完整性。

步骤 6 点击新软件包右侧的**升级**图标。

步骤 7 点击**是**以确认要继续安装。

没有指示正在加载新软件包的指标。在升级过程开始时，仍会看到Firepower机箱管理器。系统重新引导时，会将您注销。您必须等待系统恢复，然后才能登录Firepower机箱管理器。重新引导过程大约需要 20 分钟。重新引导后，您将看到登录屏幕。

使用 FXOS CLI 升级独立设备

本部分介绍如何升级独立设备的ASA 捆绑包。可以使用FTP、SCP、SFTP 或 TFTP 将软件包复制到 Firepower 2100 机箱。

过程

步骤 1 通过控制台端口（首选）或使用 SSH 连接到 FXOS CLI。

步骤 2 将软件包下载到机箱。

a) 进入固件模式。

scope firmware

示例：

```
firepower-2110# scope firmware
firepower-2110 /firmware#
```

b) 下载软件包。

download image *url*

使用以下各项之一，为正在导入的文件指定 URL：

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*

示例：

```
firepower-2110 /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

c) 监控下载过程。

show download-task

示例：

```
firepower-2110 /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
firepower-2110 /firmware #
```

步骤 3 当新软件包完成下载（**已下载**状态）时，启动软件包。

a) 查看新软件包的版本号。

show package

示例：

```
firepower-2110 /firmware # show package
Name                                         Package-Vers
-------------------------------------------- ------------
cisco-asa-fp2k.9.8.2.SPA                     9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                   9.8.2.2
firepower-2110 /firmware #
```

b) 安装软件包。

scope auto-install

install security-pack version *version*

在 **show package** 输出中，复制与 **security-pack version** 号对应的 **Package-Vers** 值。机箱会安装 ASA 映像并重新启动。

示例：

```
firepower-2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
firepower-2110 /firmware/auto-install #
```

步骤 4 等待机箱完成重新启动（5 - 10 分钟）。

虽然 FXOS 已经启动，但您仍然需要等待 ASA 启动（5 分钟）。请等待，直至显示以下消息：

```
firepower-2110#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

升级主用/备用故障转移对

使用 FXOS CLI 或 Firepower 机箱管理器升级主用/备用故障转移对，以实现零停机升级。

使用 Firepower 机箱管理器升级主用/备用故障转移对

本节介绍如何升级主用/备用故障转移对的 ASA 捆绑包。您将从管理计算机上传软件包。

开始之前

您需要确定哪一个设备是主用设备，哪一个是备用设备：将 ASDM 连接到活动 ASA IP 地址。主用设备始终拥有活动 IP 地址。然后，选择**监控** > **属性** > **故障转移** > **状态** 以查看此设备的优先级（主设备或辅助设备），以便知道您连接到哪一个设备。

过程

步骤 1 升级备用 设备。

a) 连接到备用 设备上的 Firepower 机箱管理器。
b) 选择**系统** > **更新**。
可用更新部分显示机箱上的可用软件包列表。
c) 点击**上传映像**，从管理计算机上传新软件包。
d) 点击**选择文件**，导航到并选择要上传的软件包。
e) 点击**上传**。

所选软件包将上传到机箱。**上传映像**对话框显示上传状态。等待出现**成功**对话框，然后点击**确定**。完成上传后，系统会自动验证映像的完整性。

f) 点击新软件包右侧的**升级**图标。
g) 点击**是**以确认要继续安装。

没有指示正在加载新软件包的指标。在升级过程开始时，仍会看到 Firepower 机箱管理器。系统重新引导时，会将您注销。您必须等待系统恢复，然后才能登录 Firepower 机箱管理器。重新引导过程大约需要 20 分钟。重新引导后，您将看到登录屏幕。

步骤 2 将刚才升级的设备设为主用设备，以使流量流向已升级的设备。

a) 通过连接到备用 ASA IP 地址，在备用 设备上启动 ASDM。
b) 通过选择**监控** > **属性** > **故障转移** > **状态**，然后点击**设为主用**，强制备用设备变为主用。

步骤 3 升级以前的主用 设备。

a) 连接到之前主用 设备上的 Firepower 机箱管理器。
b) 选择**系统** > **更新**。
可用更新部分显示机箱上的可用软件包列表。
c) 点击**上传映像**，从管理计算机上传新软件包。
d) 点击**选择文件**，导航到并选择要上传的软件包。
e) 点击**上传**。

所选软件包将上传到机箱。**上传映像**对话框显示上传状态。等待出现**成功**对话框，然后点击**确定**。完成上传后，系统会自动验证映像的完整性。

f) 点击新软件包右侧的**升级**图标。
g) 点击**是**以确认要继续安装。

没有指示正在加载新软件包的指标。在升级过程开始时，仍会看到 Firepower 机箱管理器。系统重新引导时，会将您注销。您必须等待系统恢复，然后才能登录 Firepower 机箱管理器。重新引导过程大约需要 20 分钟。重新引导后，您将看到登录屏幕。

使用 FXOS CLI 升级主用/备用故障转移对

本节介绍如何升级主用/备用故障转移对的 ASA 捆绑包。可以使用 FTP、SCP、SFTP 或 TFTP 将软件包复制到 Firepower 2100 机箱。

开始之前

您需要确定哪一个设备是主用设备，哪一个是备用设备。要确定故障转移状态，请查看 ASA 提示符；您可以配置ASA提示符以显示故障转移状态和优先级（主设备或辅助设备），这可用于确定连接到的设备。请参阅 prompt 命令。但是，FXOS 提示符并不知道 ASA 故障转移。或者，输入 **show failover** 命令，以查看此设备的状态和优先级（主设备或辅助设备）。

过程

步骤 1 升级备用 设备。

a) 通过控制台端口（首选）或使用 SSH，连接到备用 设备上的 FXOS CLI。

b) 进入固件模式。

scope firmware

示例：

```
2110-sec# scope firmware
2110-sec /firmware#
```

c) 下载软件包。

download image *url*

使用以下各项之一，为正在导入的文件指定 URL：

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*

示例：

```
2110-sec /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

d) 监控下载过程。

show download-task

示例：

```
2110-sec /firmware # show download
```

```
Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-sec /firmware #
```

e) 当新软件包完成下载（已下载状态）时，启动软件包。查看新软件包的版本号。

show package

示例：

```
2110-sec /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-sec /firmware #
```

f) 安装软件包。

scope auto-install

install security-pack version *version*

在 **show package** 输出中，复制与 **security-pack version** 号对应的 **Package-Vers** 值。机箱会安装 ASA 映像并重新启动。

示例：

```
2110-sec /firmware # scope auto-install
2110-sec /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-sec /firmware/auto-install #
```

g) 等待机箱完成重新启动（5 - 10 分钟）。

虽然 FXOS 已经启动，但您仍然需要等待 ASA 启动（5 分钟）。请等待，直至显示以下消息：

```
2110-sec#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

步骤 2 将刚才升级的设备设为主用设备，以使流量流向已升级的设备。

a) 从 FXOS 连接到备用 ASA CLI。

connect asa

enable

默认情况下，启用密码为空。

示例：

```
2110-sec# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
asa/stby/sec> enable
Password: <blank>
asa/stby/sec#
```

b) 强制进入备用设备以使其变为主用状态。

failover active

示例：

```
asa/stby/sec> failover active
asa/act/sec#
```

c) 要返回到 FXOS 控制台，请输入 **Ctrl+a**，**d**。

步骤 3 升级以前的主用 设备。

a) 通过控制台端口（首选）或使用 SSH，连接到主用 设备上的 FXOS CLI。

b) 进入固件模式。

scope firmware

示例：

```
2110-pri# scope firmware
2110-pri /firmware#
```

c) 下载软件包。

download image *url*

使用以下各项之一，为正在导入的文件指定 URL：

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*

示例：

```
2110-pri /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

d) 监控下载过程。

show download-task

示例：

```
2110-pri /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-pri /firmware #
```

e) 当新软件包完成下载（**已下载**状态）时，启动软件包。查看新软件包的版本号。

show package

示例：

```
2110-pri /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-pri /firmware #
```

f) 安装软件包。

scope auto-install

install security-pack version *version*

在 **show package** 输出中，复制与 **security-pack version** 号对应的 **Package-Vers** 值。机箱会安装 ASA 映像并重新启动。

示例：

```
2110-pri /firmware # scope auto-install
2110-pri /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-pri /firmware/auto-install #
```

g) 等待机箱完成重新启动（5 - 10 分钟）。

虽然 FXOS 已经启动，但您仍然需要等待 ASA 启动（5 分钟）。请等待，直至显示以下消息：

```
2110-pri#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

升级主用/主用故障转移对

使用 FXOS CLI 或 Firepower 机箱管理器升级主用/主用故障转移对，以实现零停机升级。

使用 Firepower 机箱管理器升级主用/主用故障转移对

本节介绍如何升级主用/主用故障转移对的 ASA 捆绑包。您将从管理计算机上传软件包。

过程

步骤 1 使两个故障转移组在主 设备上均处于活动状态。

a) 通过连接故障转移组 1 中的管理地址，在主 设备（或故障转移组 1 处于活动状态的设备）上启动 ASDM。
b) 选择**监控** > **故障转移** > **故障转移组 2**，然后点击**设为主用**。
c) 在后续步骤中，与此设备上的 ASDM 保持连接。

步骤 2 升级辅助 设备。

a) 连接到辅助 设备上的 Firepower 机箱管理器。
b) 依次选择**系统** > **更新**。
可用更新部分显示机箱上的可用软件包列表。
c) 点击**上传映像**，从管理计算机上传新软件包。
d) 点击**选择文件**，导航到并选择要上传的软件包。
e) 点击**上传**。

所选软件包将上传到机箱。**上传映像**对话框显示上传状态。等待出现**成功**对话框，然后点击**确定**。完成上传后，系统会自动验证映像的完整性。

f) 点击新软件包右侧的**升级**图标。
g) 点击**是**以确认要继续安装。

没有指示正在加载新软件包的指标。在升级过程开始时，仍会看到 Firepower 机箱管理器。系统重新引导时，会将您注销。您必须等待系统恢复，然后才能登录 Firepower 机箱管理器。重新引导过程大约需要 20 分钟。重新引导后，您将看到登录屏幕。

步骤 3 使两个故障转移组在辅助设备上均处于活动状态。在主 设备上的 ASDM 中，依次选择**监控** > **故障转移** > **故障转移组 1**，然后点击**设为备用**。

ASDM 将自动重新连接到辅助设备上的故障转移组 1 IP 地址。

步骤 4 升级主 设备。

a) 连接到主 设备上的 Firepower 机箱管理器。
b) 依次选择**系统** > **更新**。
可用更新部分显示机箱上的可用软件包列表。
c) 点击**上传映像**，从管理计算机上传新软件包。
d) 点击**选择文件**，导航到并选择要上传的软件包。
e) 点击**上传**。

所选软件包将上传到机箱。**上传映像**对话框显示上传状态。等待出现**成功**对话框，然后点击**确定**。完成上传后，系统会自动验证映像的完整性。

f) 点击新软件包右侧的**升级**图标。
g) 点击**是**以确认要继续安装。

没有指示正在加载新软件包的指标。在升级过程开始时，仍会看到 Firepower 机箱管理器。系统重新引导时，会将您注销。您必须等待系统恢复，然后才能登录 Firepower 机箱管理器。重新引导过程大约需要 20 分钟。重新引导后，您将看到登录屏幕。

步骤 5 如果故障转移组被配置为“启用抢占”，在抢占延迟过后，它们会在其指定设备上自动变为活动状态。如果故障转移组未被配置为启用抢占，则可以使用 **监控 > 故障转移 > 故障转移组号** 窗格使其在指定设备上恢复为活动状态。

使用 FXOS CLI 升级主用/主用故障转移对

本节介绍如何升级主用/主用故障转移对的 ASA 捆绑包。可以使用 FTP、SCP、SFTP 或 TFTP 将软件包复制到 Firepower 2100 机箱。

过程

步骤 1 通过控制台端口（首选）或使用 SSH，连接到辅助 设备上的 FXOS CLI。

步骤 2 使两个故障转移组在主设备上均处于活动状态。

a) 从 FXOS 连接到 ASA CLI。

connect asa

enable

默认情况下，启用密码为空。

示例：

```
2110-sec# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
asa/act/sec> enable
Password: <blank>
asa/act/sec#
```

b) 使两个故障转移组在主设备上均处于活动状态。

no failover active group 1

no failover active group 2

示例：

```
asa/act/sec# no failover active group 1
asa/act/sec# no failover active group 2
```

c) 输入 **Ctrl+a**, **d** 以返回 FXOS 控制台。

步骤 3 升级辅助 设备。

a) 在 FXOS 中，进入固件模式。

scope firmware

示例：

```
2110-sec# scope firmware
```

```
2110-sec /firmware#
```

b) 下载软件包。

download image *url*

使用以下各项之一，为正在导入的文件指定 URL：

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*

示例：

```
2110-sec /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

c) 监控下载过程。

show download-task

示例：

```
2110-sec /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-sec /firmware #
```

d) 当新软件包完成下载（**已下载**状态）时，启动软件包。查看新软件包的版本号。

show package

示例：

```
2110-sec /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-sec /firmware #
```

e) 安装软件包。

scope auto-install

install security-pack version *version*

在 **show package** 输出中，复制与 **security-pack version** 号对应的 **Package-Vers** 值。机箱会安装 ASA 映像并重新启动。

示例：

```
2110-sec /firmware # scope auto-install
2110-sec /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-sec /firmware/auto-install #
```

f) 等待机箱完成重新启动（5 - 10 分钟）。

虽然 FXOS 已经启动，但您仍然需要等待 ASA 启动（5 分钟）。请等待，直至显示以下消息：

```
2110-sec#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

步骤 4 使两个故障转移组在辅助设备上均处于活动状态。

a) 从 FXOS 连接到 ASA CLI。

connect asa

enable

默认情况下，启用密码为空。

示例：

```
2110-sec# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
asa/stby/sec> enable
Password: <blank>
asa/stby/sec#
```

b) 使两个故障转移组在辅助设备上均处于活动状态。

failover active group 1

failover active group 2

示例：

```
asa/stby/sec# failover active group 1
asa/act/sec# failover active group 2
```

c) 输入 **Ctrl+a**, **d** 以返回 FXOS 控制台。

步骤 5 升级主 设备。

a) 通过控制台端口（首选）或使用 SSH，连接到主 设备上的 FXOS CLI。

b) 进入固件模式。

scope firmware

示例：

```
2110-pri# scope firmware
2110-pri /firmware#
```

c) 下载软件包。

download image *url*

使用以下各项之一，为正在导入的文件指定 URL：

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*

示例：

```
2110-pri /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

d) 监控下载过程。

show download-task

示例：

```
2110-pri /firmware # show download
```

```
Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-pri /firmware #
```

e) 当新软件包完成下载（**已下载**状态）时，启动软件包。查看新软件包的版本号。

show package

示例：

```
2110-pri /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-pri /firmware #
```

f) 安装软件包。

scope auto-install

install security-pack version *version*

在 **show package** 输出中，复制与 **security-pack version** 号对应的 **Package-Vers** 值。机箱会安装 ASA 映像并重新启动。

示例：

```
2110-pri /firmware # scope auto-install
2110-pri /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-pri /firmware/auto-install #
```

g) 等待机箱完成重新启动（5 - 10 分钟）。

虽然 FXOS 已经启动，但您仍然需要等待 ASA 启动（5 分钟）。请等待，直至显示以下消息：

```
2110-pri#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

步骤 6 如果故障转移组配置了 ASA **preempt** 命令，则抢占延迟过后，它们将在其指定设备上自动变为主用状态。如果故障转移组未配置 **preempt** 命令，您可以连接 ASA CLI 并使用 **failover active group** 命令，使之在指定设备上恢复为活动状态。

升级 ASA 5500-X、ASA 虚拟、ASASM 或 ISA 3000

本文档介绍如何为单机、故障转移或集群部署计划和实施 ASA 5500-X、ASA 虚拟、ASASM 或 ISA 3000 的 ASA 和 ASDM 升级。

升级独立设备

使用 CLI 或 ASDM 升级独立设备。

使用 CLI 升级独立设备

本部分介绍如何安装 ASDM 和 ASA 映像，以及何时升级 ASA FirePOWER 模块。

开始之前

此程序使用 FTP。对于 TFTP、HTTP 或其他服务器类型，请参阅 ASA 命令参考中的 **copy** 命令。

过程

步骤 1 在特权 EXEC 模式下，将 ASA 软件复制到闪存。

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asa-9-12-1-smp-k8.bin
disk0:/asa-9-12-1-smp-k8.bin
```

步骤 2 将 ASDM 映像复制到闪存中。

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7121.bin disk0:/asdm-7121.bin
```

步骤 3 访问全局配置模式。

configure terminal

示例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

步骤 4 显示当前配置的启动映像（最多 4 个）：

show running-config boot system

ASA 按列示顺序使用映像；如果第一个映像不可用，则使用下一个映像，以此类推。不能在列表顶部插入新映像 URL；要将新的映像指定为第一个映像，必须删除所有现有条目，再根据后续步骤按所需顺序输入映像 URL。

示例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

步骤 5 删除所有现有的引导映像配置，以便将新的引导映像作为首选输入：

no boot system disk*n***:/**[路径/]*asa_image_name*

示例：

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa931-smp-k8.bin
```

步骤 6 将 ASA 映像设置为引导映像（您刚上传的映像）：

boot system disk*n***:/**[路径/]*asa_image_name*

如果此映像不可用，请对要使用的任何备份映像重复执行此命令。例如，您可以重新输入以前删除的映像。

示例：

```
ciscoasa(config)# boot system disk0:/asa-9-12-1-smp-k8.bin
```

步骤 7 设置要使用的 ASDM 映像（您刚上传的映像）：

asdm image disk*n***:/**[路径/]*asdm_image_name*

您只能配置一个要使用的 ASDM 映像，因此您不需要先删除现有配置。

示例：

```
ciscoasa(config)# asdm image disk0:/asdm-7121.bin
```

步骤 8 将新设置保存至启动配置：

write memory

步骤 9 重新加载 ASA：

reload

步骤 10 如果您要升级 ASA FirePOWER 模块，请禁用 ASA REST API，否则升级将失败。

no rest-api agent

您可以在升级后重新启用它：

rest-api agent

注释 如果您运行的是 FirePOWER 模块 6.0 或更高版本，则 ASA 5506-X 系列不支持 ASA REST API。

步骤 11 升级 ASA FirePOWER 模块。

使用 ASDM 从本地计算机升级独立设备

使用**本地计算机中的升级软件**工具，可将映像文件从计算机上传到闪存文件系统来升级 ASA。

过程

步骤 1 在主 ASDM 应用窗口中，依次选择**工具** > **从本地计算机升级软件**。

系统将显示**升级软件**对话框。

步骤 2 从**要上传的映像**下拉列表中选择 **ASDM**。

步骤 3 在**本地文件路径**字段中，点击**浏览本地文件**以查找您的 PC 上的文件。

步骤 4 在**闪存文件系统路径**字段中，点击**浏览闪存**以在闪存文件系统中查找目录或文件。

步骤 5 点击**上传映像**。

上传过程可能需要数分钟。

步骤 6 系统会提示您将此映像设置为 ASDM 映像。点击**是**。

步骤 7 系统会提示您退出 ASDM 并保存配置。点击**确定**。

您会退出 **Upgrade** 工具。**注意**：在升级 ASA 软件之后，您将保存配置并重新连接到 ASDM。

步骤 8 重复上述步骤，从**要上传的映像**下拉列表中选择 **ASA**。您也可以使用此程序上传其他文件类型。

步骤 9 依次选择**工具** > **重新加载系统**以重新加载 ASA。

系统将显示新窗口，要求您确认重新加载的详细信息。

a) 点击**重新加载时保存运行配置**单选按钮（默认）。
b) 选择重新加载的时间（例如，默认值 **Now**）。
c) 点击**计划重新加载**。

重新加载开始后，系统将显示**重新加载状态**窗口，指示正在执行重新加载。系统还提供了退出ASDM的选项。

步骤 10 在 ASA 重新加载后，重启 ASDM。

您可以从控制台端口检查重新加载状态，也可以等待几分钟，并尝试使用 ASDM 进行连接，直到成功。

步骤 11 如果要升级 ASA FirePOWER 模块，请通过选择**工具** > **命令行界面**，然后输入 **no rest-api agent** 以禁用 ASA REST API。

如果不禁用 REST API，ASA FirePOWER 模块升级将会失败。您可以在升级后重新启用它：

rest-api agent

注释 如果您运行的是FirePOWER模块6.0或更高版本，则ASA 5506-X系列不支持ASA REST API。

步骤 12 升级 ASA FirePOWER 模块。

使用 ASDM Cisco.com 向导升级独立设备

Cisco.com 向导中的升级软件工具允许您将 ASDM 和 ASA 自动升级至更加新的版本。

在此向导中，您可以执行以下操作：

- 选择 ASA 映像文件和/或 ASDM 映像文件以执行升级。

注释 ASDM会下载最新的映像版本，其版本号包括内部版本号。例如，如果要下载9.9(1)，则下载可能是9.9(1.2)。这是预期行为，因此您可以继续执行计划的升级。

- 查看您所做的升级更改。
- 下载一个或多个映像，并进行安装。
- 查看安装的状态。
- 如果安装成功完成，请重新加载 ASA 以保存配置并完成升级。

开始之前

由于内部更改，此向导仅支持使用ASDM 7.10(1)及更高版本；此外，由于映像命名更改，您必须使用 ASDM 7.12(1) 或更高版本以升级到 ASA 9.10(1) 及更高版本。由于 ASDM 向后兼容较早的 ASA 版本，因此您可以升级 ASDM，无论您运行的是哪个 ASA 版本。

过程

步骤 1 依次选择**工具** > **检查 ASA/ASDM 更新**。

在多情景模式中，从“系统”访问此菜单。

系统将显示 **Cisco.com 身份验证**对话框。

步骤 2 输入 Cisco.com 用户名和密码，然后点击 **Login**。

系统将显示 **Cisco.com 升级向导**。

注释 如果无可用升级，系统将显示对话框。点击**确定**退出向导。

步骤 3 点击**下一步**显示**选择软件**屏幕。

系统将显示当前的 ASA 版本和 ASDM 版本。

步骤 4 如要升级 ASA 版本和 ASDM 版本，请执行以下步骤：

a) 在 **ASA** 区域，选中**升级到**复选框，然后从下拉列表中选择要升级的目标 ASA 版本。

b) 在 **ASDM** 区域，选中**升级到**复选框，然后从下拉列表中选择要升级的目标 ASDM 版本。

步骤 5 点击**下一步**，显示**检查更改**屏幕。

步骤 6 请验证以下项目：

- 已下载的文件是正确的 ASA 映像文件和/或 ASDM 映像文件。
- 希望上传的文件是正确的 ASA 映像文件和/或 ASDM 映像文件。
- 已选择正确的 ASA 启动映像。

步骤 7 点击**下一步**，开始升级安装。

然后，您可以在升级安装过程中查看其状态。

系统将显示**结果**屏幕，其中提供详细信息，如升级安装状态（成功或失败）。

步骤 8 如果升级安装成功，为了使升级版本生效，请选中 **Save configuration and reload device now** 复选框来重新启动 ASA，然后重新启动 ASDM。

步骤 9 点击**完成**，退出向导，保存对配置的更改。

注释 如要升级到下一个较高版本（如可用），您必须重新启动向导。

步骤 10 在 ASA 重新加载后，重启 ASDM。

您可以从控制台端口检查重新加载状态，也可以等待几分钟，并尝试使用 ASDM 进行连接，直到成功。

步骤 11 如果要升级 ASA FirePOWER 模块，请通过选择**工具** > **命令行界面**，然后输入 **no rest-api agent** 以禁用 ASA REST API。

如果不禁用 REST API，ASA FirePOWER 模块升级将会失败。您可以在升级后重新启用它：

rest-api agent

注释 如果您运行的是 FirePOWER 模块 6.0 或更高版本，则 ASA 5506-X 系列不支持 ASA REST API。

步骤 12 升级 ASA FirePOWER 模块。

升级主用/备用故障转移对

使用 CLI 或 ASDM 升级主用/备用故障转移对，以实现零停机升级。

使用 CLI 升级主用/备用故障转移对

要升级主用/备用故障转移对，请执行以下步骤。

开始之前

- 在主用设备上执行以下步骤。对于 SSH 访问，请连接到主用 IP 地址；主用设备始终拥有此 IP 地址。当连接到 CLI 时，通过查看 ASA 提示符确定故障转移状态；您可以配置 ASA 提示符以显示故障转移状态和优先级（主设备或辅助设备），这可用于确定连接到的设备。请参阅 prompt 命令。或者，输入 **show failover** 命令，以查看此设备的状态和优先级（主设备或辅助设备）。
- 此程序使用 FTP。对于 TFTP、HTTP 或其他服务器类型，请参阅 ASA 命令参考中的 **copy** 命令。

过程

步骤 1 在主用设备的特权 EXEC 模式下，将 ASA 软件复制到主用设备闪存：

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin disk0:/asa9-15-1-smp-k8.bin
```

步骤 2 将软件复制到备用设备；请确保指定与主用设备相同的路径：

failover exec mate copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
asa/act# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin disk0:/asa9-15-1-smp-k8.bin
```

步骤 3 将 ASDM 映像复制至主用设备闪存：

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin disk0:/asdm-77171417151.bin
```

步骤 4 将 ASDM 映像复制至备用设备；请确保指定与主用设备相同的路径：

failover exec mate copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin disk0:/asdm-77171417151.bin
```

步骤 5 如果您当前未处于全局配置模式，请访问全局配置模式：

configure terminal

步骤 6 显示当前配置的启动映像（最多 4 个）：

show running-config boot system

示例：

```
asa/act(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA 按列示顺序使用映像；如果第一个映像不可用，则使用下一个映像，以此类推。不能在列表顶部插入新映像 URL；要将新的映像指定为第一个映像，必须删除所有现有条目，再根据后续步骤按所需顺序输入映像 URL。

步骤 7 删除所有现有的引导映像配置，以便将新的引导映像作为首选输入：

no boot system disk*n***:/**[路径/]*asa_image_name*

示例：

```
asa/act(config)# no boot system disk0:/cdisk.bin
asa/act(config)# no boot system disk0:/asa931-smp-k8.bin
```

步骤 8 将 ASA 映像设置为引导映像（您刚上传的映像）：

boot system disk*n*:/[路径/]*asa_image_name*

示例：

```
asa/act(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

如果此映像不可用，请对要使用的任何备份映像重复执行此命令。例如，您可以重新输入以前删除的映像。

步骤 9 设置要使用的 ASDM 映像（您刚上传的映像）：

asdm image disk*n*:/[路径/]*asdm_image_name*

示例：

```
asa/act(config)# asdm image disk0:/asdm-77171417151.bin
```

您只能配置一个要使用的 ASDM 映像，因此您不需要先删除现有配置。

步骤 10 将新设置保存至启动配置：

write memory

这些配置更改会自动保存到备用设备上。

步骤 11 如果您要升级 ASA FirePOWER 模块，请禁用 ASA REST API，否则升级将失败。

no rest-api agent

步骤 12 升级备用设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到备用 管理 IP 地址。等待升级完成。

步骤 13 重新加载备用设备，以便启动新映像：

failover reload-standby

等待备用设备完成加载。使用 **show failover** 命令确认备用设备处于备用就绪状态。

步骤 14 强行要求主用设备故障转移至备用设备。

no failover active

如果您从 SSH 会话中断开连接，请重新连接到主 IP 地址（现位于新的主用/以前的备用设备上）。

步骤 15 升级以前主用设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到备用 管理 IP 地址。等待升级完成。

步骤 16 在新的主用设备上，重新加载以前的主用设备（现为新的备用设备）。

failover reload-standby

示例：

```
asa/act# failover reload-standby
```

注释　如果连接到以前的主用设备控制台端口，应改为输入 **reload** 命令来重新加载以前的主用设备。

使用 ASDM 升级主用/备用故障转移对

要升级主用/备用故障转移对，请执行以下步骤。

开始之前

将 ASA 和 ASDM 映像放置在本地管理计算机上。

过程

步骤 1　通过连接到备用 IP 地址，在备用 设备上启动 ASDM。

步骤 2　在主 ASDM 应用窗口中，依次选择**工具** > **从本地计算机升级软件**。

系统将显示**升级软件**对话框。

步骤 3　从**要上传的映像**下拉列表中选择 **ASDM**。

步骤 4　在**本地文件路径 (Local File Path)** 字段中，输入指向计算机中文件的本地路径，或者点击**浏览本地文件 (Browse Local Files)** 在计算机中查找该文件。

步骤 5　在 **Flash 文件系统路径 (Flash File System Path)** 字段中，输入闪存文件系统的路径，或者点击**浏览 Flash (Browse Flash)** 在 Flash 文件系统中查找目录或文件。

步骤 6　点击**上传映像**。上传过程可能需要数分钟。

系统提示您将此映像设置为 ASDM 映像时，点击**否 (No)**。您会退出 Upgrade 工具。

步骤 7　重复这些步骤，从**要上传的映像**下拉列表中选择 **ASA**。

当系统提示您将此映像设置为 ASA 映像时，点击**否 (No)**。您会退出 Upgrade 工具。

步骤 8　通过连接到主 IP 地址，将 ASDM 连接到主用 设备，然后使用与您用于备用设备相同的文件位置上传 ASDM 软件。

步骤 9　当系统提示您将该映像设置为 ASDM 映像时，点击**是 (Yes)**。

系统会提示您退出 ASDM 并保存配置。点击**确定**。您会退出 Upgrade 工具。**注意**：在升级 ASA 软件之后，您将保存配置并重新加载 ASDM。

步骤 10　使用与备用设备相同的文件位置上传 ASA 软件。

步骤 11　当系统提示您将该映像设置为 ASA 映像时，点击**是 (Yes)**。

系统将提示您重新加载 ASA 以使用新映像。点击**确定**。您会退出 Upgrade 工具。

步骤 12 点击工具栏上的**保存**图标，保存配置更改。

这些配置更改将自动保存在备用设备上。

步骤 13 如果要升级 ASA FirePOWER 模块，请选择**工具** > **命令行界面**，然后输入 **no rest-api enable** 以禁用 ASA REST API。

如果不禁用 REST API，ASA FirePOWER 模块升级将会失败。

步骤 14 升级备用设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到备用 管理 IP 地址。等待升级完成后，将 ASDM 连接回主用设备。

步骤 15 通过依次选择**监控 (Monitoring)** > **属性 (Properties)** > **故障转移 (Failover)** > **状态 (Status)**，然后点击**重新加载备用 (Reload Standby)**，重新加载备用设备。

留在**系统**窗格中，以监控备用设备何时重新加载。

步骤 16 重新加载备用设备后，强制主用设备执行故障转移到备用设备，方法为：选择**监控 (Monitoring)** > **属性 (Properties)** > **故障转移 (Failover)** > **状态 (Status)**，然后点击**设为备用 (Make Standby)**。

ASDM 将自动重新连接到新主用设备。

步骤 17 升级以前主用设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到备用 管理 IP 地址。等待升级完成后，将 ASDM 连接回主用设备。

步骤 18 重新加载（新）备用设备，方法为：选择**监控 (Monitoring)** > **属性 (Properties)** > **故障转移 (Failover)** > **状态 (Status)**，然后点击**重新加载备用 (Reload Standby)**。

升级主用/主用故障转移对

使用 CLI 或 ASDM 升级主用/主用故障转移对，以实现零停机升级。

使用 CLI 升级主用/主用故障转移对

要升级主用/主用故障转移配置中的两台设备，请执行以下步骤。

开始之前

- 在主设备上执行这些步骤。
- 在系统执行空间中执行以下步骤。
- 此程序使用 FTP。对于 TFTP、HTTP 或其他服务器类型，请参阅 ASA 命令参考中的 **copy** 命令。

过程

步骤 1 在主设备的特权 EXEC 模式下，将 ASA 软件复制到闪存：

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin
disk0:/asa9-15-1-smp-k8.bin
```

步骤 2 将软件复制至辅助设备；请确保指定与主设备相同的路径：

failover exec mate copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
asa/act/pri# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin disk0:/asa9-15-1-smp-k8.bin
```

步骤 3 将 ASDM 映像复制至主设备闪存：

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act/pri# ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin
disk0:/asdm-77171417151.bin
```

步骤 4 将 ASDM 映像复制到辅助设备中；务必指定与主设备相同的路径：

failover exec mate copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act/pri# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin disk0:/asdm-77171417151.bin
```

步骤 5 如果您当前未处于全局配置模式，请访问全局配置模式：

configure terminal

步骤 6 显示当前配置的启动映像（最多 4 个）：

show running-config boot system

示例：

```
asa/act/pri(config)# show running-config boot system
boot system disk0:/cdisk.bin
```

```
boot system disk0:/asa931-smp-k8.bin
```

ASA 按列示顺序使用映像；如果第一个映像不可用，则使用下一个映像，以此类推。不能在列表顶部插入新映像 URL；要将新的映像指定为第一个映像，必须删除所有现有条目，再根据后续步骤按所需顺序输入映像 URL。

步骤 7 删除所有现有的引导映像配置，以便将新的引导映像作为首选输入：

no boot system disk*n***:/**[路径/]*asa_image_name*

示例：

```
asa/act/pri(config)# no boot system disk0:/cdisk.bin
asa/act/pri(config)# no boot system disk0:/asa931-smp-k8.bin
```

步骤 8 将 ASA 映像设置为引导映像（您刚上传的映像）：

boot system disk*n***:/**[路径/]*asa_image_name*

示例：

```
asa/act/pri(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

如果此映像不可用，请对要使用的任何备份映像重复执行此命令。例如，您可以重新输入以前删除的映像。

步骤 9 设置要使用的 ASDM 映像（您刚上传的映像）：

asdm image disk*n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act/pri(config)# asdm image disk0:/asdm-77171417151.bin
```

您只能配置一个要使用的 ASDM 映像，因此您不需要先删除现有配置。

步骤 10 将新设置保存至启动配置：

write memory

这些配置更改会自动保存到辅助设备上。

步骤 11 如果您要升级 ASA FirePOWER 模块，请禁用 ASA REST API，否则升级将失败。

no rest-api agent

步骤 12 使两个故障转移组在主设备上均处于活动状态：

failover active group 1

failover active group 2

示例：

```
asa/act/pri(config)# failover active group 1
```

```
asa/act/pri(config)# failover active group 2
```

步骤 13 升级辅助设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到故障转移组 1 或 2 的备用管理 IP 地址。等待升级完成。

步骤 14 重新加载辅助设备，以便启动新映像：

failover reload-standby

等待辅助设备完成加载。使用 **show failover** 命令确认两个故障转移组均处于备用就绪状态。

步骤 15 强行要求两个故障转移组在辅助设备上变为活动状态：

no failover active group 1

no failover active group 2

示例：

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

如果您从 SSH 会话中断开连接，请重新连接到故障转移组 1 IP 地址（现位于辅助设备上）。

步骤 16 升级主设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到故障转移组 1 或 2 的备用管理 IP 地址。等待升级完成。

步骤 17 重新加载主设备：

failover reload-standby

示例：

```
asa/act/sec# failover reload-standby
```

注释 如果已连接到主设备控制台端口，应改为输入 **reload** 命令来重新加载主设备。

您可能从 SSH 会话中断开连接。

步骤 18 如果故障转移组配置了 **preempt** 命令，则抢占延迟过后，它们将在其指定设备上自动变为主用状态。

使用 ASDM 升级主用/主用故障转移对

要升级主用/主用故障转移配置中的两台设备，请执行以下步骤。

开始之前

- 在系统执行空间中执行以下步骤。

- 将 ASA 和 ASDM 映像放置在本地管理计算机上。

过程

步骤 1 通过连接到故障转移组 2 中的管理地址，在辅助 设备上启动 ASDM。

步骤 2 在主 ASDM 应用窗口中，依次选择**工具** > **从本地计算机升级软件**。

系统将显示**升级软件**对话框。

步骤 3 从**要上传的映像**下拉列表中选择 **ASDM**。

步骤 4 在**本地文件路径 (Local File Path)** 字段中，输入指向计算机中文件的本地路径，或者点击**浏览本地文件 (Browse Local Files)** 在 PC 中查找文件。

步骤 5 在 **Flash 文件系统路径 (Flash File System Path)** 字段中，输入闪存文件系统的路径，或者点击**浏览 Flash (Browse Flash)** 在闪存文件系统中查找目录或文件。

步骤 6 点击**上传映像**。上传过程可能需要数分钟。

系统提示您将此映像设置为 ASDM 映像时，点击**否 (No)**。您会退出 Upgrade 工具。

步骤 7 重复上述步骤，从**要上传的映像**下拉列表中选择 **ASA**。

当系统提示您将此映像设置为 ASA 映像时，点击**否 (No)**。您会退出 Upgrade 工具。

步骤 8 通过连接至故障转移组 1 中的管理 IP 地址，将 ASDM 连接至主设备，并使用辅助设备上所用的相同文件位置上传 ASDM 软件。

步骤 9 当系统提示您将该映像设置为 ASDM 映像时，点击**是 (Yes)**。

系统会提示您退出 ASDM 并保存配置。点击**确定**。您会退出 Upgrade 工具。**注意**：在升级 ASA 软件之后，您将保存配置并重新加载 ASDM。

步骤 10 使用与辅助设备相同的文件位置上传 ASA 软件。

步骤 11 当系统提示您将该映像设置为 ASA 映像时，点击**是 (Yes)**。

系统将提示您重新加载 ASA 以使用新映像。点击**确定**。您会退出 Upgrade 工具。

步骤 12 点击工具栏上的**保存**图标，保存配置更改。

这些配置更改在辅助设备上会自动保存。

步骤 13 如果要升级 ASA FirePOWER 模块，请选择**工具** > **命令行界面**，然后输入 **no rest-api enable** 以禁用 ASA REST API。

如果不禁用 REST API，ASA FirePOWER 模块升级将会失败。

步骤 14 通过选择**监控 (Monitoring)** > **故障转移 (Failover)** > **故障转移组号 (Failover Group #)**（其中**组号**是您要移动至主设备的故障转移组的编号）并点击**设为主用 (Make Active)**，使两个故障转移组在主设备上均处于活动状态。

步骤 15 升级辅助设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到故障转移组 1 或 2 的备用管理 IP 地址。等待升级完成后，将 ASDM 连接回主设备。

步骤 16 重新加载辅助设备，方法为：选择**监控 (Monitoring)** > **故障转移 (Failover)** > **系统 (System)**，然后点击**重新加载备用 (Reload Standby)**。

保持在**系统**窗格上，以监控辅助设备何时加载。

步骤 17 辅助设备启动后，通过选择**监控 (Monitoring)** > **故障转移 (Failover)** > **故障转移组号 (Failover Group #)**（其中**组号**是您要移动至辅助设备的故障转移组的编号）并点击**设为备用 (Make Standby)**，使两个故障转移组在辅助设备上均处于活动状态。

ASDM 将自动重新连接到辅助设备上的故障转移组 1 IP 地址。

步骤 18 升级主设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到故障转移组 1 或 2 的备用管理 IP 地址。等待升级完成后，将 ASDM 连接回辅助设备。

步骤 19 重新加载主设备，方法为：选择**监控 (Monitoring)** > **故障转移 (Failover)** > **系统 (System)**，然后点击**重新加载备用 (Reload Standby)**。

步骤 20 如果故障转移组被配置为“启用抢占”，在抢占延迟过后，它们会在其指定设备上自动变为活动状态。ASDM 将自动重新连接到主设备上的故障转移组 1 IP 地址。

升级 ASA 集群

使用 CLI 或 ASDM 升级 ASA 集群，以实现零停机升级。

使用 CLI 升级 ASA 集群

要升级 ASA 集群中的所有设备，请执行以下步骤。此程序使用 FTP。对于 TFTP、HTTP 或其他服务器类型，请参阅 ASA 命令参考中的 **copy** 命令。

开始之前

- 在控制单元上执行这些步骤。如果您还要升级 ASA FirePOWER 模块，则需要在每台数据单元上访问控制台或ASDM。您可以将ASA提示符配置为显示集群设备和状态（控制或数据），这些信息有助于确定您连接的目标设备。请参阅 prompt 命令。或者，输入 **show cluster info** 命令以查看每台设备的角色。
- 您必须使用控制台端口；不能通过远程 CLI 连接启用或禁用集群。
- 对于多情景模式，在系统执行空间中执行以下步骤。

过程

步骤 1 在特权 EXEC 模式下，将控制单元的上的 ASA 软件复制到集群中的所有设备。

cluster exec copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin disk0:/asa9-15-1-smp-k8.bin
```

步骤 2 将 ASDM 映像复制至集群中的所有设备：

cluster exec copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin disk0:/asdm-77171417151.bin
```

步骤 3 如果您当前未处于全局配置模式，请立即访问该模式。

configure terminal

示例：

```
asa/unit1/master# configure terminal
asa/unit1/master(config)#
```

步骤 4 显示当前配置的引导映像（最多 4 个）。

show running-config boot system

示例：

```
asa/unit1/master(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA 按列示顺序使用映像；如果第一个映像不可用，则使用下一个映像，以此类推。不能在列表顶部插入新映像 URL；要将新的映像指定为第一个映像，必须删除所有现有条目，再根据后续步骤按所需顺序输入映像 URL。

步骤 5 删除所有现有的引导映像配置，以便将新的引导映像作为首选输入：

no boot system disk*n***:/**[路径/]*asa_image_name*

示例：

```
asa/unit1/master(config)# no boot system disk0:/cdisk.bin
asa/unit1/master(config)# no boot system disk0:/asa931-smp-k8.bin
```

步骤 6 将 ASA 映像设置为引导映像（您刚上传的映像）：

boot system disk*n***:/**[路径/]*asa_image_name*

示例：

```
asa/unit1/master(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

如果此映像不可用，请对要使用的任何备份映像重复执行此命令。例如，您可以重新输入以前删除的映像。

步骤 7 设置要使用的 ASDM 映像（您刚上传的映像）：

asdm image disk*n***:/**[路径/]*asdm_image_name*

示例：

```
asa/unit1/master(config)# asdm image disk0:/asdm-77171417151.bin
```

您只能配置一个要使用的 ASDM 映像，因此您不需要先删除现有配置。

步骤 8 将新设置保存至启动配置：

write memory

这些配置更改会自动保存到数据单元。

步骤 9 如果您要升级 ASA FirePOWER 模块，请禁用 ASA REST API，否则 ASA FirePOWER 模块升级将失败。

no rest-api agent

步骤 10 如果您要升级由 ASDM 管理的 ASA FirePOWER 模块，就需要将 ASDM 连接到单个 管理 IP 地址，因此您需要记下每台设备的 IP 地址。

show running-config interface *management_interface_id*

记下使用的 **cluster-pool** 池名称。

show ip[**v6**] **local pool** 池名称

记下集群设备的 IP 地址。

示例：

```
asa/unit2/slave# show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.86.118.1 255.255.252.0 cluster-pool inside-pool
asa/unit2/slave# show ip local pool inside-pool
Begin           End             Mask            Free     Held     In use
10.86.118.16    10.86.118.17    255.255.252.0       0        0        2

Cluster Unit                    IP Address Allocated
unit2                           10.86.118.16
unit1                           10.86.118.17
asa1/unit2/slave#
```

步骤 11 升级数据单元。

选择下面的程序，具体取决于您是否还要升级 ASA FirePOWER 模块。如果也需要升级 ASA FirePOWER 模块，ASA FirePOWER 程序可以最大限度地减少 ASA 重新加载的次数。您可以在执行这些程序时选用数据单元控制台或 ASDM。如果您还无权访问所有控制台端口，但可以通过网络访问 ASDM，则可能需要使用 ASDM 而不是控制台。

注释 在升级过程中，切勿使用 **cluster master unit** 命令强制将某个数据单元变为控制单元；否则可能导致网络连接和集群稳定相关的问题。您必须先升级并重新加载所有数据单元，然后继续此过程以确保从当前控制单元顺利地过渡到新的控制单元。

如果不进行 ASA FirePOWER 模块升级：

a) 在控制单元上，要查看成员名称，请输入 **cluster exec unit ?**，或输入 **show cluster info** 命令。

b) 重新加载数据单元。

cluster exec unit *data-unit* **reload noconfirm**

示例：

```
asa/unit1/master# cluster exec unit unit2 reload noconfirm
```

c) 对每个从属数据单元上述操作。

为避免失去连接并使流量稳定下来，请等待每个设备恢复运行并重新加入集群（大约需要 5 分钟），然后再对下一个设备重复执行上述步骤。要查看设备何时重新加入集群，请输入 **show cluster info**。

如果还要进行 ASA FirePOWER 模块升级（使用数据控制台）：

a) 连接到数据单元的控制台端口，然后进入全局配置模式。

enable

configure terminal

示例：

```
asa/unit2/slave> enable
Password:
asa/unit2/slave# configure terminal
asa/unit2/slave(config)#
```

b) 禁用集群。

cluster group *name*

no enable

不保存此配置；您希望在重新加载时启用集群。您需要禁用集群，以避免在升级过程中出现多次失败和重新加入；此设备应仅在所有升级和重新加载过程完成后才进行重新加入。

示例：

```
asa/unit2/slave(config)# cluster group cluster1
```

```
asa/unit2/slave(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover
either enable clustering or remove cluster group configuration.

Cluster unit unit2 transitioned from SLAVE to DISABLED
asa/unit2/ClusterDisabled(cfg-cluster)#
```

c) 在此数据单元上升级 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到您之前记下的单个 管理 IP 地址。等待升级完成。

d) 重新加载数据单元。

reload noconfirm

e) 对每个从属数据单元上述操作。

为避免失去连接并使流量稳定下来，请等待每个设备恢复运行并重新加入集群（大约需要 5 分钟），然后再对下一个设备重复执行上述步骤。要查看设备何时重新加入集群，请输入 **show cluster info**。

如果还要进行 ASA FirePOWER 模块升级（使用 ASDM）：

a) 将 ASDM 连接到您之前记下的此数据单元的单个 管理 IP 地址。
b) 依次选择**配置** > **设备管理高可用性和可扩展性** > **ASA 集群** > **集群配置** > 。
c) 取消选中**加入 ASA 集群**复选框。

您需要禁用集群，以避免在升级过程中出现多次失败和重新加入；此设备应仅在所有升级和重新加载过程完成后才进行重新加入。

请勿取消选中**配置 ASA 集群设置**复选框，此操作会清除所有集群配置并关闭所有接口，包括 ASDM 连接到的管理接口。在此情况下，要恢复连接，您需要在控制台端口上访问 CLI。

注释 某些旧版本的 ASDM 不支持在此屏幕上禁用集群；在此情况下，请使用**工具** > **命令行界面**工具，点击**多行**单选按钮，然后输入 **cluster group** 名称 和 **no enable**。您可以在**主页** > **设置控制面板** > **设备信息** > **ASA 集群**区域中查看集群组名称。

d) 点击**应用**。
e) 系统会提示您退出 ASDM。将 ASDM 重新连接到相同的 IP 地址。
f) 升级 ASA FirePOWER 模块。

等待升级完成。

g) 在 ASDM 中，选择**工具** > **系统重新加载**。
h) 点击**重新加载而不保存运行配置**单选按钮。

请勿保存配置；在主设备重新加载后，您需要在其上启用集群。

i) 点击**计划重新加载**。
j) 请点击**是**继续重新加载。
k) 对每个从属数据单元上述操作。

为避免失去连接并使流量稳定下来，请等待每个设备恢复运行并重新加入集群（大约需要 5 分钟），然后再对下一个设备重复执行上述步骤。要查看设备重新加入集群的时间，请查看控制单元上的**监控** > **ASA 集群** > **集群摘要**窗格。

步骤 12 升级控制单元。

a) 禁用集群。

cluster group *name*

no enable

最多等待 5 分钟，以便选择新的控制单元且流量稳定下来。

不保存此配置；您希望在重新加载时启用集群。

我们建议在控制单元上手动禁用集群（如果可能），以便尽可能快速顺畅地选择新的控制单元。

示例：

```
asa/unit1/master(config)# cluster group cluster1
asa/unit1/master(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover
either enable clustering or remove cluster group configuration.

Cluster unit unit1 transitioned from MASTER to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

b) 在此设备上升级 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到您之前记下的单个管理 IP 地址。主集群 IP 地址现在属于新的控制单元；此以前的控制单元仍可通过其单独的管理 IP 地址进行访问。

等待升级完成。

c) 重新加载此设备。

reload noconfirm

当以前的控制单元重新加入集群时，它将成为数据单元。

使用 ASDM 升级 ASA 集群

要升级 ASA 集群中的所有设备，请执行以下步骤。

开始之前

- 在控制单元上执行这些步骤。如果您还要升级 ASA FirePOWER 模块，则需要 ASDM 访问每台数据单元。
- 对于多情景模式，在系统执行空间中执行以下步骤。

- 将 ASA 和 ASDM 映像放置在本地管理计算机上。

过程

步骤 1 通过连接到主集群 IP 地址，在控制单元上启动 ASDM。

此 IP 地址始终属于控制单元。

步骤 2 在主 ASDM 应用窗口中，依次选择**工具** > **从本地计算机升级软件**。

系统将显示**从本地计算机升级软件**对话框。

步骤 3 点击**集群中的所有设备 (All devices in the cluster)** 单选按钮。

系统将显示**升级软件**对话框。

步骤 4 从**要上传的映像**下拉列表中选择 **ASDM**。

步骤 5 在**本地文件路径 (Local File Path)** 字段中，点击**浏览本地文件 (Browse Local Files)** 以查找您计算机上的文件。

步骤 6 （可选） 在 **Flash 文件系统路径 (Flash File System Path)** 字段中，输入闪存文件系统的路径，或者点击**浏览 Flash (Browse Flash)** 在闪存文件系统中查找目录或文件。

默认情况下，此字段预先填充有以下路径：**disk0:**/*filename*。

步骤 7 点击**上传映像**。上传过程可能需要数分钟。

步骤 8 系统会提示您将此映像设置为 ASDM 映像。点击**是**。

步骤 9 系统会提示您退出 ASDM 并保存配置。点击**确定**。

您会退出 Upgrade 工具。**注意**：在升级 ASA 软件之后，您将保存配置并重新加载 ASDM。

步骤 10 重复上述步骤，从**要上传的映像**下拉列表中选择 **ASA**。

步骤 11 点击工具栏上的**保存**图标，保存配置更改。

这些配置更改会自动保存到数据单元。

步骤 12 请记下**配置** > **设备管理** > **高可用性和可扩展性** > **ASA 集群** > **集群成员**上每个设备的单独管理 IP 地址，以便您以后可以将 ASDM 直接连接到数据单元。

步骤 13 如果要升级 ASA FirePOWER 模块，请选择**工具** > **命令行界面**，然后输入 **no rest-api enable** 以禁用 ASA REST API。

如果不禁用 REST API，ASA FirePOWER 模块升级将会失败。

步骤 14 升级数据单元。

选择下面的程序，具体取决于您是否还要升级 ASA FirePOWER 模块。ASA FirePOWER 程序最大程度减少了升级 ASA FirePOWER 模块时的 ASA 重新加载次数。

注释 在升级过程中，请勿使用**监控** > **ASA 集群** > **集群摘要**将控制单元更改为页面强制数据单元成为控制单元；否则会导致网络连接性和集群稳定性相关的问题。您必须先重新加载所有数据单元，然后继续此过程以确保从当前控制单元顺利地过渡到新的控制单元。

如果不进行 **ASA FirePOWER** 模块升级：

a) 在控制单元上，选择**工具** > **系统重新加载**。
b) 从**设备**下拉列表中，选择数据单元名称。
c) 点击**计划重新加载**。
d) 请点击**是**继续重新加载。
e) 对每个从属数据单元上述操作。

为避免失去连接并使流量稳定下来，请等待每个设备恢复运行并重新加入集群（大约需要 5 分钟），然后再对下一个设备重复执行上述步骤。要查看设备重新加入集群的时间，请查看**监控**> **ASA 集群** > **集群摘要**窗格。

如果还要进行 **ASA FirePOWER** 模块升级：

a) 在控制单元上，选择**配置** > **设备管理** > **高可用性和稳定性** > **ASA 集群** > **集群成员**。
b) 选择要升级的数据单元，然后点击**删除 (Delete)**。
c) 点击**应用 (Apply)**。
d) 退出 ASDM，然后通过连接到您之前记下的单个管理 IP 地址，将 ASDM 连接到数据单元。
e) 升级 ASA FirePOWER 模块。

等待升级完成。

f) 在 ASDM 中，选择**工具** > **系统重新加载**。
g) 点击**重新加载而不保存运行配置**单选按钮。

请勿保存配置；在主设备重新加载后，您需要在其上启用集群。

h) 点击**计划重新加载**。
i) 请点击**是**继续重新加载。
j) 对每个从属数据单元上述操作。

为避免失去连接并使流量稳定下来，请等待每个设备恢复运行并重新加入集群（大约需要 5 分钟），然后再对下一个设备重复执行上述步骤。要查看设备重新加入集群的时间，请查看**监控** > **ASA 集群** > **集群摘要**窗格。

步骤 15 升级控制单元。

a) 在控制单元上的 ASDM 中，选择**配置** > **设备管理** > **高可用性和可扩展性** > **ASA 集群** > **集群配置**窗格。
b) 取消选中**加入 ASA 集群 (Participate in ASA cluster)** 复选框，然后点击**应用 (Apply)**。

系统会提示您退出 ASDM。

c) 最多等待 5 分钟，以便选择新的控制单元且流量稳定下来。

当以前的控制单元重新加入集群时，它将成为数据单元。

d) 通过连接到您之前记下的单个 管理 IP 地址，将 ASDM 重新连接到之前的控制单元。

主集群 IP 地址现在属于新的控制单元；此以前的控制单元仍可通过其单独的管理 IP 地址进行访问。

e) 升级 ASA FirePOWER 模块。

等待升级完成。

f) 依次选择**工具** > **重新加载系统**。

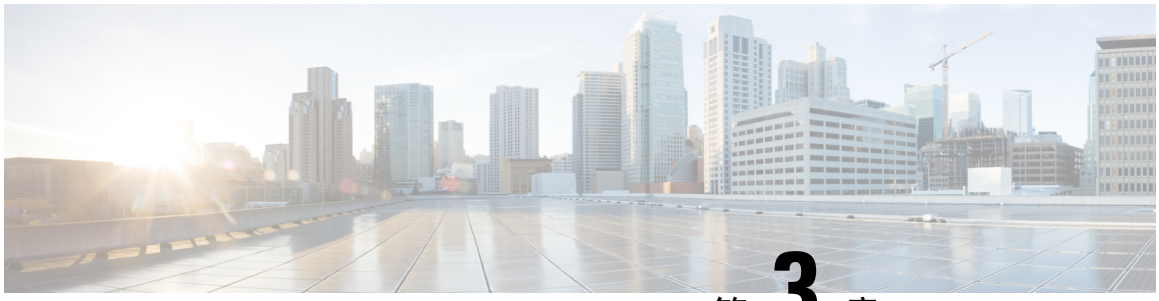
g) 点击**重新加载而不保存运行配置**单选按钮。

请勿保存配置；在主设备重新加载后，您需要在其上启用集群。

h) 点击**计划重新加载**。

i) 请点击**是**继续重新加载。

系统会提示您退出 ASDM。在主集群 IP 地址上重启 ASDM；您将重新连接到新的控制单元。



第 3 章

升级 ASA FirePOWER 模块

本文档介绍如何使用 ASDM 或 管理中心升级 ASA FirePOWER 模块，具体取决于您的管理选择。请参阅升级 ASA 设备或 ASA 虚拟，第 93 页以确定何时应在单机、故障转移或集群场景中执行 FirePOWER 升级。

流量和检查

当执行以下操作时，会发生流量中断和检查：

- 重启设备。
- 升级设备软件、操作系统或虚拟托管环境。
- 卸载或恢复设备软件。
- 在域之间移动设备。
- 部署配置更改（Snort 进程重新启动）。

设备类型、高可用性/可扩展性配置和接口配置决定了中断的性质。我们强烈建议在维护窗口或者中断对部署的影响最小时执行这些任务。

升级具有 ASDM 的 ASA FirePOWER 模块

使用以下步骤升级由 ASDM 管理的 ASA FirePOWER 模块。

⚠

注意 不要 更改配置、手动重新引导或关闭升级模块。请勿重启正在进行的升级。升级过程在预检查期间可能会显示为非活动；这是预期行为。如果您遇到升级问题，包括升级失败或设备无响应，请联系 Cisco TAC。

过程

步骤 1 确保您运行的是受支持的 ASA 版本。

ASA 与 ASA FirePOWER 版本之间没有广泛的兼容性。但是，即使并非严格要求进行 ASA 升级，但是解决问题可能需要升级到支持的最新版本。

有关何时按顺序升级 ASA FirePOWER 模块，请参阅适用于独立、故障转移和集群场景的 ASA 升级程序。即使不升级 ASA 软件，您仍应参阅 ASA 故障转移和集群升级程序，以便在模块升级之前在设备上执行故障转移或禁用集群，避免流量丢失。例如，在集群中，您应连续升级每个辅助设备（包括禁用集群、升级模块，然后重新启用集群），然后升级主设备。

步骤 2 从 Cisco.com 下载升级包。

对于主要版本：

- 升级到版本 6.0 至 6.2.2 - Cisco_Network_Sensor_**Upgrade**-[版本]-[内部版本].**sh**
- 升级到版本 6.2.3+ - Cisco_Network_Sensor_**Upgrade**-[版本]-[内部版本].**sh.REL.tar**

对于修补程序：

- 升级到 5.4.1.x 至 6.2.1.x - Cisco_Network_Sensor_**Patch**-[版本]-[内部版本].**sh**
- 升级到版本 6.2.2.1+ - Cisco_Network_Sensor_**Patch**-[版本]-[内部版本].**sh.REL.tar**

直接从思科支持和下载站点下载。如果通过邮件传输软件包，可能会损坏该软件包。请注意，从 6.2.2+ 开始的升级包经过签名，以 .sh.REL.tar 结尾，而不是简单的 .sh。请勿解压已签名的升级软件包。

步骤 3 使用 ASDM 连接到 ASA 并上传升级软件包。

a) 选择**配置** > **ASA FirePOWER 配置** > **更新**。
b) 点击**上传更新**。
c) 点击**选择文件**以导航到并选择更新文件。
d) 点击**上传**。

步骤 4 部署待处理配置更改。否则，升级可能失败。

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重启 Snort，这会中断流量检测，并且根据您的设备处理流量的方式，可能会中断流量，直至重启完成。有关详细信息，请参阅流量和检查，第 145 页。

步骤 5 （升级到 6.1.0 一直到 6.3.0.x）禁用 ASA REST API。

如果不禁用REST API，升级将会失败。请注意，如果您还在运行6.0及更高版本的ASA FirePOWER模块，则 ASA 5506-X 系列设备不支持 ASA REST API。

在 ASA 上使用 CLI 以禁用 REST API：

no rest-api agent

您可以在升级后重新启用它：

rest-api agent

步骤 6 选择**监控** > **ASA FirePOWER 监控** > **任务状态**，确保完成必要任务。

在升级开始时运行的任务已停止，成为失败的任务，且不能恢复。您可以稍后手动删除具有失败状态的消息。

步骤 7 选择**配置** > **ASA FirePOWER 配置** > **更新**。

步骤 8 点击上传的升级包旁边的安装图标，然后确认要升级并重新引导模块。

流量要么在升级过程中丢弃，要么不经检测直接穿过网络，具体取决于模块的配置方式。有关详细信息，请参阅 流量和检查，第 145 页。

步骤 9 在“任务状态”页面上监控升级进度。

在模块升级期间，不要更改配置。即使升级状态在数分钟内不显示进度，或指示升级失败，也不要重新开始升级或重新引导模块。而是联系思科 TAC。

步骤 10 升级完成后，将 ASDM 重新连接到 ASA。

步骤 11 选择**配置** > **ASA FirePOWER 配置**，然后点击**刷新**。否则，界面可能会出现意外行为。

步骤 12 依次选择**配置** > **ASA FirePOWER 配置** > **系统信息**，确认模块具有正确的软件版本。

步骤 13 如果支持站点上提供的入侵规则更新或漏洞数据库 (VDB) 比当前运行的版本新，请安装新版本。

步骤 14 完成发行说明中所述的任何升级后配置更改。

步骤 15 重新部署配置。

升级 Firepower 管理中心

如果使用 Firepower 管理中心管理 ASA FirePOWER 模块，则需要先升级管理中心，然后再升级该模块。

升级独立 Cisco Secure Firewall Management Center

使用此程序可升级独立的 Cisco Secure Firewall Management Center，包括 Cisco Secure Firewall Management Center Virtual。

⚠

注意 升级 FMC 过程中，不要进行或部署配置更改、手动重启或关闭设备。请勿 重启正在进行的升级。升级过程在预检查期间可能会显示为非活动；这是预期行为。如果您遇到升级问题，升级失败的升级或无响应的设备，请联系 思科 TAC。

开始之前

完成预升级核对表。确保部署中的设备保持正常运行，并且能够成功通信。

过程

步骤 1 选择**系统** > **更新**。

步骤 2 点击您想要使用的升级软件包旁边的安装图标，然后选择 FMC。

步骤 3 点击**安装 (Install)** 以开始升级。

确认您要升极和重启。

步骤 4 监控预检查进度，直到注销。在此期间，请勿更改配置。

步骤 5 在可以时登录回。

- 次要升级（补丁和热修复程序）：您可以在升级完成且重启后再次登录。
- 主要升级（补丁和热修复程序）：您可以在升级完成且重启后再次登录。系统会显示一个页面，供您用于监控升级进度，查看升级日志和任何错误消息。升级完成且系统重启时，您会再次注销。重新引导后，再次登录。

步骤 6 如果系统显示相应提示，则阅读并接受《最终用户许可协议 (EULA)》。

步骤 7 验证升级是否成功。

如果在您登录时系统未通知您升级成功，请选择**帮助** > **关于**以显示当前软件版本信息。

步骤 8 更新入侵规则 (SRU/LSP) 和漏洞数据库 (VDB)。

如果 思科支持和下载站点 上提供的组件比当前运行的版本新，请安装新版本。请注意，在更新入侵规则时，不需要自动重新应用策略。您可以稍后执行该操作。

步骤 9 完成发行说明中所述的任何升级后配置更改。

步骤 10 重新部署配置。

重新部署到所有 受管设备。如果不部署到设备，其最终升级可能会失败，而且您可能需要对其重新映像。

升级高可用性 Firepower 管理中心

使用此程序可在高可用性对中的 FMC 上升级 Firepower 软件。

您需要逐一升级对等设备。在暂停同步的情况下，首先升级备用设备，然后升级主用设备。当备用开始预检查时，其状态从备用切换到主用，以便两个对等设备都处于主用状态。此临时状态称为 集群裂脑，仅 在升级期间受支持。请勿 在对处于集群脑裂的情况下执行或部署配置更改。重启同步后，您所做的更改将丢失。

注意 升级 FMC 过程中，不要进行或部署配置更改、手动重启或关闭设备。请勿 重启正在进行的升级。升级过程在预检查期间可能会显示为非活动；这是预期行为。如果您遇到升级问题，升级失败的升级或无响应的设备，请联系 思科 TAC。

开始之前

完成两个对等设备的升级前检查表。确保部署中的设备保持正常运行，并且能够成功通信。

过程

步骤 1 暂停同步。

a) 选择**系统** > **集成**。

b) 在**高可用性 (High Availability)**选项卡，点击**暂停同步 (Pause Synchronization)**。

步骤 2 将升级包上传到备用设备。

在 FMC 高可用性部署中，必须将 FMC 升级软件包上传到两个对等设备，在将软件包传输到备用设备之前暂停同步。要限制 HA 同步的中断，您可以在升级准备阶段将数据包传输到主用对等设备，并在暂停同步后将其作为实际升级过程的一部分传输到备用对等设备。

步骤 3 逐一升级对等体，先是备用设备，再是主用设备。

请按照升级独立 Cisco Secure Firewall Management Center，第 147 页中的说明进行操作，在验证每个对等体上的更新均成功后停止操作。总而言之，对于每个对等体：

a) 在**系统 (System)** > **更新 (Updates)**页面上，安装升级程序。

b) 监控进度，直到您注销，然后在可以时重新登录（在主要升级情况下这会发生两次）。

c) 验证升级是否成功。

请勿 在对处于集群脑裂的情况下执行或部署配置更改。

步骤 4 重启同步。

a) 登录到想到将其设置为主用对等体的 FMC。

b) 选择**系统** > **集成**。

c) 在**高可用性 (High Availability)**选项卡，点击**设为主用 (Make-Me-Active)**。

d) 等待直至同步重新开始，并且其他 FMC 切换到备用模式。

步骤 5 更新入侵规则 (SRU/LSP) 和漏洞数据库 (VDB)。

如果思科支持和下载站点上提供的组件比当前运行的版本新，请安装新版本。请注意，在更新入侵规则时，不需要自动重新应用策略。您可以稍后执行该操作。

步骤 6 完成发行说明中所述的任何升级后配置更改。

步骤 7 重新部署配置。

重新部署到所有 受管设备。如果不部署到设备，其最终升级可能会失败，而且您可能需要对其重新映像。

升级带有 FMC 的 ASA FirePOWER 模块

使用此程序升级由 FMC 管理的 ASA FirePOWER 模块。何时升级模块取决于是否升级 ASA，以及 ASA 部署。

- 独立 ASA 设备：如果您同时还在升级 ASA，请在升级 ASA 后立即升级 ASA FirePOWER 模块，然后重新加载。
- ASA 集群和故障转移对：为避免流量和检查出现中断，请逐一完全升级这些设备。如果还要升级 ASA，请在重新加载每个单元以升级 ASA 之前升级 ASA FirePOWER 模块。

有关详细信息，请参阅 升级路径：带有 FMC 的 ASA FirePOWER，第 72 页 和 ASA 升级程序。

开始之前

完成预升级核对表。确保部署中的设备保持正常运行，并且能够成功通信。

过程

步骤 1 选择**系统** > **更新**。

步骤 2 点击您想要使用的升级软件包旁边的安装图标，然后选择要升级的设备。

如果您想要升级的设备未列出，则表示您选择了错误的升级软件包。

注释 我们强烈 建议同时从“系统更新”页面升级的设备数不超过五个。不能在所有选定设备完成升级过程之前停止升级。如果任何一个设备升级存在问题，则必须等待所有设备均完成升级，然后才可以解决该问题。

步骤 3 点击**安装 (Install)**，然后确认您要升级并重启设备。

流量在整个升级过程中丢弃还是不进行检测就穿过网络，取决于您的设备的配置和部署方式。有关详细信息，请参阅目标版本的思科 Firepower 发行说明中的升级软件一章。

步骤 4 监控升级进度。

注意 请勿将更改部署到正在升级的设备或部署更改到，手动重启正在升级的设备，或者关闭正在升级的设备。请勿重启正在进行的设备升级。升级过程在预检查期间可能会显示为非活动；这是预期行为。如果您遇到升级问题，升级失败的升级或无响应的设备，请联系 思科 TAC。

步骤 5 验证升级是否成功。

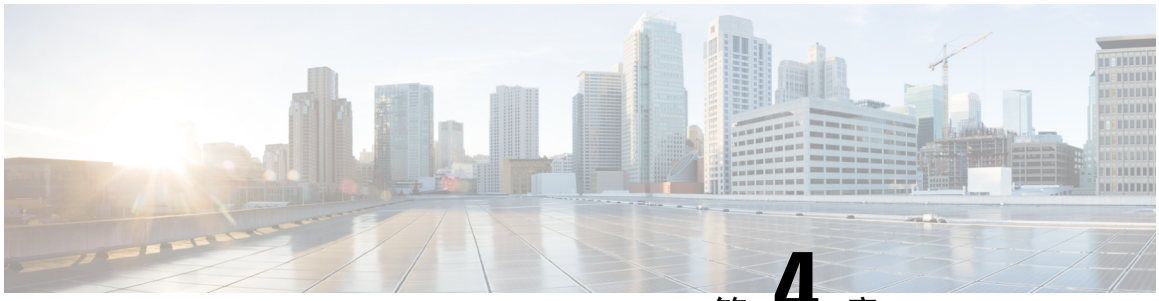
升级过程完成后，选择**设备** > **设备管理**，并确认您升级的设备具有正确的软件版本。

步骤 6 更新入侵规则 (SRU/LSP) 和漏洞数据库 (VDB)。

如果 思科支持和下载站点上提供的组件比当前运行的版本新，请安装新版本。请注意，在更新入侵规则时，不需要自动重新应用策略。您可以稍后执行该操作。

步骤 7 完成发行说明中所述的任何升级后配置更改。

步骤 8 将配置重新部署到将刚才升级的设备。



第 4 章

升级 Firepower 4100/9300 上的 ASA

本文档介绍如何在Firepower 4100/9300上升级ASA。

升级 FXOS 和 ASA 独立设备或机箱内集群

使用 FXOS CLI 或 Firepower 机箱管理器升级 Firepower 9300 上的 FXOS 和 ASA 独立设备或 ASA 机箱内集群。

使用以下设备升级 FXOS 和 ASA 独立设备或机箱内集群 Cisco Secure Firewall 机箱管理器

升级过程最多可能需要 45 分钟。在设备升级时，流量不会穿过设备。请相应规划您的升级活动。

开始之前

开始升级之前，请确保您已完成以下操作：

- 下载要升级到的 FXOS 和 ASA 软件包。
- 备份您的 FXOS 和 ASA 配置。

过程

步骤 1 在 Cisco Secure Firewall 机箱管理器 中，选择**系统** > **更新**。
可用更新部分显示机箱上的可用软件包列表。

步骤 2 上传新的 FXOS 平台捆绑包映像和 ASA 软件映像：

注释 如果要升级到 FXOS 2.3.1 之前的版本，则在升级 FXOS 平台捆绑包软件之前，请不要将 ASA CSP 映像上传到安全设备。

a) 点击**上传映像**。
b) 点击**选择文件**，可导航到并选择想要上传的映像。
c) 点击**上传**。
所选映像将上传到机箱。

步骤 3 成功上传新的 FXOS 平台捆绑包映像后，点击要升级到的 FXOS 平台捆绑包对应的**升级**图标。

系统将首先验证想要安装的软件包。它会告知您当前已安装的应用程序与指定的 FXOS 平台软件包之间的所有不兼容问题。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。只要 ASA 版本在兼容性表中列为可升级版本，就可以忽略这些警告。

步骤 4 点击**是**以确认要继续安装。

FXOS 打开捆绑包，升级/重新加载组件。

步骤 5 Firepower 机箱管理器在升级期间将不可用。您可以使用 FXOS CLI 监控升级过程（请参阅监控升级进度，第 187 页）。

步骤 6 成功升级所有组件后，验证安全模块/安全引擎和任何已安装的应用程序的状态（请参阅确认安装，第 188 页）。

步骤 7 选择**逻辑设备**。
此时会打开**逻辑设备**页面以显示机箱上已配置的逻辑设备列表。

步骤 8 对于要升级的每个 ASA 逻辑设备：

a) 点击想要更新的逻辑设备对应的**设置版本**图标，打开**更新映像版本**对话框。
b) 对于**新版本**，选择要升级到的软件版本。
c) 点击**确定**。

步骤 9 升级过程完成后，确认应用程序在线且成功升级：

a) 选择**逻辑设备**。
b) 验证应用程序版本和运行状态。

使用 FXOS CLI 升级 FXOS 和 ASA 独立设备或机箱内集群

升级过程最多可能需要 45 分钟。在设备升级时，流量不会穿过设备。请相应规划您的升级活动。

开始之前

开始升级之前，请确保您已完成以下操作：

- 下载要升级到的 FXOS 和 ASA 软件包。
- 备份您的 FXOS 和 ASA 配置。

- 收集将软件映像下载到机箱所需的以下信息：
  - 您从其复制映像的服务器的 IP 地址和身份验证凭证。
  - 映像文件的完全限定名称。

过程

步骤 1 连接到 FXOS CLI。

步骤 2 将新的 FXOS 平台捆绑包映像下载到机箱：

a) 进入固件模式：

scope firmware

b) 下载 FXOS 平台捆绑包软件映像：

download image *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://用户名@服务器/路径/*image_name*
- **scp**://用户名@服务器/路径/*image_name*
- **sftp**://用户名@服务器/路径/*image_name*
- **tftp**://服务器**:**端口号/路径/*image_name*

c) 要监控下载过程，请执行以下操作：

scope download-task *image_name*

show detail

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

步骤 3 成功下载新的 FXOS 平台捆绑包映像后，升级 FXOS 捆绑包：

a) 如有必要，请返回到固件模式：

up

b) 记下要安装的 FXOS 平台捆绑包的版本号：

show package

c) 进入自动安装模式：

scope auto-install

d) 安装 FXOS 平台捆绑包：

install platform platform-vers *version_number*

version_number 是您要安装的 FXOS 平台捆绑包的版本号，例如 2.3(1.58)。

e) 系统将首先验证想要安装的软件包。它会告知您当前已安装的应用程序与指定的FXOS平台软件包之间的所有不兼容问题。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。只要 ASA 版本在兼容性表中列为可升级版本，就可以忽略这些警告。

输入 **yes**，确认您想要继续验证。

f) 输入 **yes**确认您想要继续安装，或者输入 **no**取消安装。

FXOS 打开捆绑包，升级/重新加载组件。

g) 要监控升级流程，请参阅监控升级进度，第 187 页：

步骤 4 成功升级所有组件后，验证安全模块/安全引擎和任何已安装的应用程序的状态（请参阅确认安装，第 188 页）。

步骤 5 将新的 ASA 软件映像下载到机箱：

a) 进入安全服务模式：

top

scope ssa

b) 进入应用软件模式：

scope app-software

c) 下载逻辑设备软件映像：

download image *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://用户名@服务器/路径
- **scp**://用户名@服务器/路径
- **sftp**://用户名@服务器/路径
- **tftp**://服务器:端口号/路径

d) 要监控下载过程，请执行以下操作：

show download-task

e) 要查看已下载的应用，请执行以下操作：

up

show app

记下您下载的软件包的 ASA 版本。在后面的步骤中，您将需要使用准确的版本字符串来启用应用程序。

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

步骤 6 对于要升级的每个 ASA 逻辑设备：

a) 进入安全服务模式：

top

scope ssa

b) 将范围设置为您正在更新的安全模块：

scope slot*slot_number*

c) 将范围设置为 ASA 应用程序：

对于 FXOS 2.3.1 及更低版本： **scope app-instance asa**

对于 FXOS 2.4.1 及更高版本：**scope app-instance asa** *instance_name*

d) 将启动版本设置为新的 ASA 软件版本：

set startup-version *version_number*

步骤 7 提交配置：

commit-buffer

提交系统配置任务。应用映像已更新，应用重新启动。

步骤 8 要验证安全模块/安全引擎和任何已安装的应用程序的状态，请参阅确认安装，第 188 页。

升级 FXOS 和 ASA 主用/备用故障转移对

使用 FXOS CLI 或 Firepower 机箱管理器升级 FXOS 和 ASA 主用/备用故障转移对。

使用 Firepower 机箱管理器升级 FXOS 和 ASA 主用/备用故障转移对

每个机箱的升级过程最多可能需要 45 分钟。请相应规划您的升级活动。

开始之前

开始升级之前，请确保您已完成以下操作：

- 您需要确定哪一个设备是主用设备，哪一个是备用设备：将 ASDM 连接到活动 ASA IP 地址。主用设备始终拥有活动 IP 地址。然后，选择**监控** > **属性** > **故障转移** > **状态** 以查看此设备的优先级（主设备或辅助设备），以便知道您连接到哪一个设备。
- 下载要升级到的 FXOS 和 ASA 软件包。
- 备份您的 FXOS 和 ASA 配置。

过程

步骤 1 在包含备用 ASA 逻辑设备的 Firepower 安全设备上，上传新的 FXOS 平台捆绑包映像和 ASA 软件映像：

注释 如果要升级到 FXOS 2.3.1 之前的版本，则在升级 FXOS 平台捆绑包软件之前，请不要将 ASA CSP 映像上传到安全设备。

a) 在 Cisco Secure Firewall 机箱管理器中，选择**系统** > **更新**。
可用更新部分显示机箱上的可用软件包列表。
b) 点击**上传映像**。
c) 点击**选择文件**，可导航到并选择想要上传的映像。
d) 点击**上传**。
所选映像将上传到机箱。

步骤 2 在成功上传新的 FXOS 平台捆绑包映像后，在包含备用 ASA 逻辑设备的 Firepower 安全设备上升级 FXOS 捆绑包：

a) 点击要升级到的 FXOS 平台捆绑包所对应的**升级**图标。

系统将首先验证想要安装的软件包。它会告知您当前已安装的应用程序与指定的FXOS平台软件包之间的所有不兼容问题。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。只要 ASA 版本在兼容性表中列为可升级版本，就可以忽略这些警告。

b) 点击**是**以确认要继续安装。

FXOS 打开捆绑包，升级/重新加载组件。

步骤 3 Firepower 机箱管理器在升级期间将不可用。您可以使用 FXOS CLI 监控升级过程（请参阅监控升级进度，第 187 页）。

步骤 4 成功升级所有组件后，验证安全模块/安全引擎和任何已安装的应用程序的状态（请参阅确认安装，第 188 页）。

步骤 5 升级 ASA 逻辑设备映像：

a) 选择**逻辑设备**打开“逻辑设备”页面。
此时会打开**逻辑设备**页面以显示机箱上已配置的逻辑设备列表。

b) 点击想要更新的逻辑设备对应的**设置版本**图标，打开**更新映像版本**对话框。

c) 对于**新版本 (New Version)**，选择想要更新的软件版本。

d) 点击**确定**。

步骤 6 升级过程完成后，确认应用程序在线且成功升级：

a) 选择**逻辑设备**。

b) 验证应用程序版本和运行状态。

步骤 7 将刚才升级的设备设为活动 设备，以使流量流向已升级的设备：

a) 通过连接到备用 ASA IP 地址，在备用 设备上启动 ASDM。

b) 通过选择**监控** > **属性** > **故障转移** > **状态**，然后点击**设为主用**，强制备用设备变为主用。

步骤 8 在包含新的备用 ASA 逻辑设备的 Firepower 安全设备上，上传新的 FXOS 平台捆绑包映像和 ASA 软件映像：

注释 如果要升级到 FXOS 2.3.1 之前的版本，则在升级 FXOS 平台捆绑包软件之前，请不要将 ASA CSP 映像上传到安全设备。

a) 在 Cisco Secure Firewall 机箱管理器中，选择**系统** > **更新**。
可用更新部分显示机箱上的可用软件包列表。

b) 点击**上传映像**。

c) 点击**选择文件**，可导航到并选择想要上传的映像。

d) 点击**上传**。
所选映像将上传到机箱。

步骤 9 在成功上传新的 FXOS 平台捆绑包映像后，在包含新的备用 ASA 逻辑设备的 Firepower 安全设备上升级 FXOS 捆绑包：

a) 点击要升级到的 FXOS 平台捆绑包所对应的**升级**图标。

系统将首先验证想要安装的软件包。它会告知您当前已安装的应用程序与指定的FXOS平台软件包之间的所有不兼容问题。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。只要 ASA 版本在兼容性表中列为可升级版本，就可以忽略这些警告。

b) 点击**是**以确认要继续安装。

FXOS 打开捆绑包，升级/重新加载组件。

步骤 10 Firepower 机箱管理器在升级期间将不可用。您可以使用 FXOS CLI 监控升级过程（请参阅监控升级进度，第 187 页）。

步骤 11 成功升级所有组件后，验证安全模块/安全引擎和任何已安装的应用程序的状态（请参阅确认安装，第 188 页）。

步骤 12 升级 ASA 逻辑设备映像：

a) 选择**逻辑设备**。
此时会打开**逻辑设备**页面以显示机箱上已配置的逻辑设备列表。如果尚未配置任何逻辑设备，则系统将显示一条表明此情况的消息。

b) 点击想要更新的逻辑设备对应的**设置版本**图标，打开**更新映像版本**对话框。

c) 对于**新版本 (New Version)**，选择想要更新的软件版本。

d) 点击**确定**。

步骤 13 升级过程完成后，确认应用程序在线且成功升级：

a) 选择**逻辑设备**。

b) 验证应用程序版本和运行状态。

步骤 14 （可选）将刚才升级的设备设为主用 设备，同升级前一样：

a) 通过连接到备用 ASA IP 地址，在备用 设备上启动 ASDM。

b) 通过选择**监控** > **属性** > **故障转移** > **状态**，然后点击**设为主用**，强制备用设备变为主用。

使用 FXOS CLI 升级 FXOS 和 ASA 主用/备用故障转移对

每个机箱的升级过程最多可能需要 45 分钟。请相应规划您的升级活动。

开始之前

开始升级之前，请确保您已完成以下操作：

- 您需要确定哪一个设备是主用设备，哪一个是备用设备：连接到 Firepower 安全设备上的 ASA 控制台，并 **show failover** 输入该命令以查看设备的主用/备用状态。
- 下载要升级到的 FXOS 和 ASA 软件包。
- 备份您的 FXOS 和 ASA 配置。
- 收集将软件映像下载到机箱所需的以下信息：
  - 您从其复制映像的服务器的 IP 地址和身份验证凭证。
  - 映像文件的完全限定名称。

过程

步骤 1 在包含备用 ASA 逻辑设备的 Firepower 安全设备上，下载新的 FXOS 平台捆绑包映像：

a) 连接到 FXOS CLI。

b) 进入固件模式：

scope firmware

c) 下载 FXOS 平台捆绑包软件映像：

download image *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://用户名@服务器/路径/*image_name*
- **scp**://用户名@服务器/路径/*image_name*
- **sftp**://用户名@服务器/路径/*image_name*
- **tftp**://服务器**:**端口号/路径/*image_name*

d) 要监控下载过程，请执行以下操作：

scope download-task *image_name*

show detail

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

步骤 2 成功下载新的 FXOS 平台捆绑包映像后，升级 FXOS 捆绑包：

a) 如有必要，请返回到固件模式：

up

b) 记下要安装的 FXOS 平台捆绑包的版本号：

show package

c) 进入自动安装模式：

scope auto-install

d) 安装 FXOS 平台捆绑包：

install platform platform-vers *version_number*

version_number 是您要安装的 FXOS 平台捆绑包的版本号，例如 2.3(1.58)。

e) 系统将首先验证想要安装的软件包。它会告知您当前已安装的应用程序与指定的FXOS平台软件包之间的所有不兼容问题。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。只要 ASA 版本在兼容性表中列为可升级版本，就可以忽略这些警告。

输入 **yes**，确认您想要继续验证。

f) 输入 **yes**确认您想要继续安装，或者输入 **no**取消安装。

FXOS 打开捆绑包，升级/重新加载组件。

g) 要监控升级流程，请参阅监控升级进度，第 187 页：

步骤 3 成功升级所有组件后，验证安全模块/安全引擎和任何已安装的应用程序的状态（请参阅确认安装，第 188 页）。

步骤 4 将新的 ASA 软件映像下载到机箱：

a) 进入安全服务模式：

top

scope ssa

b) 进入应用软件模式：

scope app-software

c) 下载逻辑设备软件映像：

download image *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://用户名@服务器/路径
- **scp**://用户名@服务器/路径
- **sftp**://用户名@服务器/路径
- **tftp**://服务器:端口号/路径

d) 要监控下载过程，请执行以下操作：

show download-task

e) 要查看已下载的应用，请执行以下操作：

up

show app

记下您下载的软件包的 ASA 版本。在后面的步骤中，您将需要使用准确的版本字符串来启用应用程序。

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

步骤 5 升级 ASA 逻辑设备映像：

a) 进入安全服务模式：

top

scope ssa

b) 将范围设置为您正在更新的安全模块：

scope slot*slot_number*

c) 将范围设置为 ASA 应用程序：

对于 FXOS 2.3.1 及更低版本： **scope app-instance asa**

对于 FXOS 2.4.1 及更高版本：**scope app-instance asa** *instance_name*

d) 将入门版本设置为想要更新的版本：

set startup-version *version_number*

e) 提交配置：

commit-buffer

提交系统配置任务。应用映像已更新，应用重新启动。

步骤 6 要验证安全模块/安全引擎和任何已安装的应用程序的状态，请参阅确认安装，第 188 页。

步骤 7 将刚才升级的设备设为活动 设备，以使流量流向已升级的设备：

a) 在包含备用 ASA 逻辑设备的 Firepower 安全设备上，使用控制台连接或 Telnet 连接连接到模块 CLI。

connect module *slot_number* {**console** | **telnet**}

要连接至不支持多个安全模块的设备的安全引擎，请使用 **1** 作为 *slot_number*。

示例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) 连接到应用控制台。

connect asa

示例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) 将此设备设为活动状态：

failover active

d) 保存配置：

write memory

e) 验证设备是否处于活动状态：

show failover

步骤 8 退出应用控制台到 FXOS 模块 CLI。

输入 **Ctrl-a, d**

步骤 9 返回 FXOS CLI 的管理引擎层。

退出控制台：

a) 输入 **~**

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

telnet>**quit**

退出 **Telnet** 会话：

a) 输入 **Ctrl-],**。

步骤 10 在包含新的备用 ASA 逻辑设备的 Firepower 安全设备上，下载新的 FXOS 平台捆绑包映像：

a) 连接到 FXOS CLI。

b) 进入固件模式：

scope firmware

c) 下载 FXOS 平台捆绑包软件映像：

download image *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://用户名@服务器/路径/*image_name*
- **scp**://用户名@服务器/路径/*image_name*
- **sftp**://用户名@服务器/路径/*image_name*
- **tftp**://服务器**:**端口号/路径/*image_name*

d) 要监控下载过程，请执行以下操作：

scope download-task *image_name*

show detail

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

步骤 11 成功下载新的 FXOS 平台捆绑包映像后，升级 FXOS 捆绑包：

a) 如有必要，请返回到固件模式：

up

b) 记下要安装的 FXOS 平台捆绑包的版本号：

show package

c) 进入自动安装模式：

scope auto-install

d) 安装 FXOS 平台捆绑包：

install platform platform-vers *version_number*

version_number 是您要安装的 FXOS 平台捆绑包的版本号，例如 2.3(1.58)。

e) 系统将首先验证想要安装的软件包。它会告知您当前已安装的应用程序与指定的FXOS平台软件包之间的所有不兼容问题。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。只要 ASA 版本在兼容性表中列为可升级版本，就可以忽略这些警告。

输入 **yes**，确认您想要继续验证。

f) 输入 **yes**确认您想要继续安装，或者输入 **no**取消安装。

FXOS 打开捆绑包，升级/重新加载组件。

g) 要监控升级流程，请参阅监控升级进度，第 187 页：

步骤 12 成功升级所有组件后，验证安全模块/安全引擎和任何已安装的应用程序的状态（请参阅确认安装，第 188 页）。

步骤 13 将新的 ASA 软件映像下载到机箱：

a) 进入安全服务模式：

top

scope ssa

b) 进入应用软件模式：

scope app-software

c) 下载逻辑设备软件映像：

download image *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://用户名@服务器/路径
- **scp**://用户名@服务器/路径
- **sftp**://用户名@服务器/路径
- **tftp**://服务器:端口号/路径

d) 要监控下载过程，请执行以下操作：

show download-task

e) 要查看已下载的应用，请执行以下操作：

up

show app

记下您下载的软件包的 ASA 版本。在后面的步骤中，您将需要使用准确的版本字符串来启用应用程序。

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

步骤 14 升级 ASA 逻辑设备映像：

a) 进入安全服务模式：

top

scope ssa

b) 将范围设置为您正在更新的安全模块：

scope slot*slot_number*

c) 将范围设置为 ASA 应用程序：

对于 FXOS 2.3.1 及更低版本： **scope app-instance asa**

对于 FXOS 2.4.1 及更高版本：**scope app-instance asa** *instance_name*

d) 将入门版本设置为想要更新的版本：

set startup-version *version_number*

e) 提交配置：

commit-buffer

提交系统配置任务。应用映像已更新，应用重新启动。

步骤 15 要验证安全模块/安全引擎和任何已安装的应用程序的状态，请参阅确认安装，第 188 页。

步骤 16 （可选）将刚才升级的设备设为主用 设备，同升级前一样：

a) 在包含备用 ASA 逻辑设备的 Firepower 安全设备上，使用控制台连接或 Telnet 连接连接到模块 CLI。

connect module *slot_number* {**console** | **telnet**}

要连接至不支持多个安全模块的设备的安全引擎，请使用 **1** 作为 *slot_number*。

示例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) 连接到应用控制台。

connect asa

示例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) 将此设备设为活动状态：

failover active

d) 保存配置：

write memory

e) 验证设备是否处于活动状态：

show failover

升级 FXOS 和 ASA 主用/主用故障转移对

使用 FXOS CLI 或 Firepower 机箱管理器升级 FXOS 和 ASA 主用/主用故障转移对。

使用 Firepower 机箱管理器升级 FXOS 和 ASA 主用/主用故障转移对

每个机箱的升级过程最多可能需要 45 分钟。请相应规划您的升级活动。

开始之前

开始升级之前，请确保您已完成以下操作：

- 您需要确定哪一个设备是主设备：连接 ASDM，然后选择**监控** > **属性** > **故障转移** > **状态**以查看此设备的优先级（主设备或辅助设备），以便知道您连接到哪一个设备。
- 下载要升级到的 FXOS 和 ASA 软件包。
- 备份您的 FXOS 和 ASA 配置。

过程

步骤 1 使两个故障转移组在主 设备上均处于活动状态。

a) 通过连接故障转移组 1 中的管理地址，在主 设备（或故障转移组 1 处于活动状态的设备）上启动 ASDM。
b) 选择**监控** > **故障转移** > **故障转移组 2**，然后点击**设为主用**。
c) 在后续步骤中，与此设备上的 ASDM 保持连接。

步骤 2 在包含辅助 ASA 逻辑设备的 Firepower 安全设备上，上传新的 FXOS 平台捆绑包映像和 ASA 软件映像：

注释 如果要升级到 FXOS 2.3.1 之前的版本，则在升级 FXOS 平台捆绑包软件之前，请不要将 ASA CSP 映像上传到安全设备。

a) 连接到辅助 设备上的 Firepower 机箱管理器。
b) 依次选择**系统** > **更新**。
可用更新部分显示机箱上的可用软件包列表。
c) 点击**上传映像**。
d) 点击**选择文件**，可导航到并选择想要上传的映像。
e) 点击**上传**。
所选映像将上传到机箱。

步骤 3 在成功上传新的 FXOS 平台捆绑包映像后，在包含辅助 ASA 逻辑设备的 Firepower 安全设备上升级 FXOS 捆绑包：

a) 点击要升级到的 FXOS 平台捆绑包所对应的**升级**图标。

系统将首先验证想要安装的软件包。它会告知您当前已安装的应用程序与指定的FXOS平台软件包之间的所有不兼容问题。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。只要 ASA 版本在兼容性表中列为可升级版本，就可以忽略这些警告。

b) 点击**是**以确认要继续安装。

FXOS 打开捆绑包，升级/重新加载组件。

步骤 4 Firepower 机箱管理器在升级期间将不可用。您可以使用 FXOS CLI 监控升级过程（请参阅监控升级进度，第 187 页）。

步骤 5 成功升级所有组件后，验证安全模块/安全引擎和任何已安装的应用程序的状态（请参阅确认安装，第 188 页）。

步骤 6 升级 ASA 逻辑设备映像：

a) 选择**逻辑设备**。
此时会打开**逻辑设备**页面以显示机箱上已配置的逻辑设备列表。
b) 点击想要更新的逻辑设备对应的**设置版本**图标，打开**更新映像版本**对话框。
c) 对于**新版本 (New Version)**，选择想要更新的软件版本。
d) 点击**确定**。

步骤 7 升级过程完成后，确认应用程序在线且成功升级：

a) 选择**逻辑设备**。
b) 验证应用程序版本和运行状态。

步骤 8 使两个故障转移组在辅助 设备上均处于活动状态。

a) 通过连接故障转移组 1 中的管理地址，在主 设备（或故障转移组 1 处于活动状态的设备）上启动 ASDM。
b) 依次选择**监控** > **故障转移** > **故障转移组 1**，然后点击**设为备用**。
c) 依次选择**监控** > **故障转移** > **故障转移组 2**，然后点击**设为备用**。

ASDM 将自动重新连接到辅助设备上的故障转移组 1 IP 地址。

步骤 9 在包含主 ASA 逻辑设备的 Firepower 安全设备上，上传新的 FXOS 平台捆绑包映像和 ASA 软件映像：

注释 如果要升级到 FXOS 2.3.1 之前的版本，则在升级 FXOS 平台捆绑包软件之前，请不要将 ASA CSP 映像上传到安全设备。

a) 连接到主 设备上的 Firepower 机箱管理器。
b) 依次选择**系统** > **更新**。
可用更新部分显示机箱上的可用软件包列表。
c) 点击**上传映像**，可打开“上传映像”对话框。
d) 点击**选择文件**，可导航到并选择想要上传的映像。
e) 点击**上传**。
所选软件包将上传到机箱。
f) 对于某些软件映像，上传映像后，系统将显示一份最终用户许可协议。请按照系统提示接受这份最终用户许可协议。

步骤 10 在成功上传新的 FXOS 平台捆绑包映像后，在包含主 ASA 逻辑设备的 Firepower 安全设备上升级 FXOS 捆绑包：

a) 点击要升级到的 FXOS 平台捆绑包所对应的**升级**图标。

系统将首先验证想要安装的软件包。它会告知您当前已安装的应用程序与指定的FXOS平台软件包之间的所有不兼容问题。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。只要 ASA 版本在兼容性表中列为可升级版本，就可以忽略这些警告。

b) 点击**是**以确认要继续安装。

FXOS 打开捆绑包，升级/重新加载组件。

步骤 11 Firepower 机箱管理器在升级期间将不可用。您可以使用 FXOS CLI 监控升级过程（请参阅监控升级进度，第 187 页）。

步骤 12 成功升级所有组件后，验证安全模块/安全引擎和任何已安装的应用程序的状态（请参阅确认安装，第 188 页）。

步骤 13 升级 ASA 逻辑设备映像：

a) 选择**逻辑设备**。
此时会打开**逻辑设备**页面以显示机箱上已配置的逻辑设备列表。

b) 点击想要更新的逻辑设备对应的**设置版本**图标，打开**更新映像版本**对话框。

c) 对于**新版本 (New Version)**，选择想要更新的软件版本。

d) 点击**确定**。

步骤 14 升级过程完成后，确认应用程序在线且成功升级：

a) 选择**逻辑设备**。

b) 验证应用程序版本和运行状态。

步骤 15 如果故障转移组被配置为“启用抢占”，在抢占延迟过后，它们会在其指定设备上自动变为活动状态。如果故障转移组未被配置为启用抢占，则可以使用 **监控 > 故障转移 > 故障转移组号** 窗格使其在指定设备上恢复为活动状态。

使用 FXOS CLI 升级 FXOS 和 ASA 主用/主用故障转移对

每个机箱的升级过程最多可能需要 45 分钟。请相应规划您的升级活动。

开始之前

开始升级之前，请确保您已完成以下操作：

- 您需要确定哪个设备是主设备：连接到 Firepower 安全设备上的 ASA 控制台，并输入 **show failover** 命令以查看设备的状态和优先级（主要或辅助）。
- 下载要升级到的 FXOS 和 ASA 软件包。
- 备份您的 FXOS 和 ASA 配置。
- 收集将软件映像下载到机箱所需的以下信息：
  - 您从其复制映像的服务器的 IP 地址和身份验证凭证。
  - 映像文件的完全限定名称。

过程

步骤 1 通过控制台端口（首选）或使用 SSH，连接到辅助 设备上的 FXOS CLI。

步骤 2 使两个故障转移组在主设备上均处于活动状态。

a) 使用控制台连接或 Telnet 连接来连接至模块 CLI。

connect module *slot_number* {**console** | **telnet**}

要连接至不支持多个安全模块的设备的安全引擎，请使用 **1** 作为 *slot_number*。

示例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) 连接到应用控制台。

connect asa

示例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) 使两个故障转移组在主设备上均处于活动状态。

enable

默认情况下，启用密码为空。

no failover active group 1

no failover active group 2

示例：

```
asa> enable
Password: <blank>
asa# no failover active group 1
asa# no failover active group 2
```

步骤 3 退出应用控制台到 FXOS 模块 CLI。

输入 **Ctrl-a, d**

步骤 4 返回 FXOS CLI 的管理引擎层。

退出控制台：

a) 输入 **~**

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

telnet>**quit**

退出 Telnet 会话：

a) 输入 **Ctrl-],**。

步骤 5 在包含辅助 ASA 逻辑设备的 Firepower 安全设备上，下载新的 FXOS 平台捆绑包映像和 ASA 软件映像：

a) 连接到 FXOS CLI。

b) 进入固件模式：

scope firmware

c) 下载 FXOS 平台捆绑包软件映像：

download image *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://用户名@服务器/路径/*image_name*
- **scp**://用户名@服务器/路径/*image_name*
- **sftp**://用户名@服务器/路径/*image_name*
- **tftp**://服务器**:**端口号/路径/*image_name*

d) 要监控下载过程，请执行以下操作：

scope download-task *image_name*

show detail

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

步骤 6 成功下载新的 FXOS 平台捆绑包映像后，升级 FXOS 捆绑包：

a) 如有必要，请返回到固件模式：

top

scope firmware

b) 记下要安装的 FXOS 平台捆绑包的版本号：

show package

c) 进入自动安装模式：

scope auto-install

d) 安装 FXOS 平台捆绑包：

install platform platform-vers *version_number*

version_number 是您要安装的 FXOS 平台捆绑包的版本号，例如 2.3(1.58)。

e) 系统将首先验证想要安装的软件包。它会告知您当前已安装的应用程序与指定的FXOS平台软件包之间的所有不兼容问题。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。只要 ASA 版本在兼容性表中列为可升级版本，就可以忽略这些警告。

输入 **yes**，确认您想要继续验证。

f) 输入 **yes**确认您想要继续安装，或者输入 **no**取消安装。

FXOS 打开捆绑包，升级/重新加载组件。

g) 要监控升级流程，请参阅监控升级进度，第 187 页：

步骤 7 成功升级所有组件后，验证安全模块/安全引擎和任何已安装的应用程序的状态（请参阅确认安装，第 188 页）。

步骤 8 将新的 ASA 软件映像下载到机箱：

a) 进入安全服务模式：

top

scope ssa

b) 进入应用软件模式：

scope app-software

c) 下载逻辑设备软件映像：

download image *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://用户名@服务器/路径
- **scp**://用户名@服务器/路径
- **sftp**://用户名@服务器/路径
- tftp://*server*:*port-num*/*path*

d) 要监控下载过程，请执行以下操作：

show download-task

e) 要查看已下载的应用，请执行以下操作：

up

show app

记下您下载的软件包的 ASA 版本。在后面的步骤中，您将需要使用准确的版本字符串来启用应用程序。

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

步骤 9 升级 ASA 逻辑设备映像：

a) 进入安全服务模式：

top

scope ssa

b) 将范围设置为您正在更新的安全模块：

scope slot*slot_number*

c) 将范围设置为 ASA 应用程序：

对于 FXOS 2.3.1 及更低版本： **scope app-instance asa**

对于 FXOS 2.4.1 及更高版本：**scope app-instance asa** *instance_name*

d) 将入门版本设置为想要更新的版本：

set startup-version *version_number*

e) 提交配置：

commit-buffer

提交系统配置任务。应用映像已更新，应用重新启动。

步骤 10 要验证安全模块/安全引擎和任何已安装的应用程序的状态，请参阅确认安装，第 188 页。

步骤 11 使两个故障转移组在辅助 设备上均处于活动状态。

a) 使用控制台连接或 Telnet 连接来连接至模块 CLI。

connect module *slot_number* {**console** | **telnet**}

要连接至不支持多个安全模块的设备的安全引擎，请使用 **1** 作为 *slot_number*。

示例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) 连接到应用控制台。

connect asa

示例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) 使两个故障转移组在辅助 设备上均处于活动状态。

enable

默认情况下，启用密码为空。

failover active group 1

failover active group 2

示例：

```
asa> enable
Password: <blank>
asa# failover active group 1
asa# failover active group 2
```

步骤 12 退出应用控制台到 FXOS 模块 CLI。

输入 **Ctrl-a, d**

步骤 13 返回 FXOS CLI 的管理引擎层。

退出控制台：

a) 输入 **~**

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

telnet>**quit**

退出 Telnet 会话：

a) 输入 **Ctrl-],**。

步骤 14 在包含主 ASA 逻辑设备的 Firepower 安全设备上，下载新的 FXOS 平台捆绑包映像和 ASA 软件映像：

a) 连接到 FXOS CLI。

b) 进入固件模式：

scope firmware

c) 下载 FXOS 平台捆绑包软件映像：

download image *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://用户名@服务器/路径/*image_name*
- **scp**://用户名@服务器/路径/*image_name*
- **sftp**://用户名@服务器/路径/*image_name*
- tftp://*server*:*port-num*/*path*/*image_name*

d) 要监控下载过程，请执行以下操作：

scope download-task *image_name*

show detail

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
```

```
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

步骤 15 成功下载新的 FXOS 平台捆绑包映像后，升级 FXOS 捆绑包：

a) 如有必要，请返回到固件模式：

up

b) 记下要安装的 FXOS 平台捆绑包的版本号：

show package

c) 进入自动安装模式：

scope auto-install

d) 安装 FXOS 平台捆绑包：

install platform platform-vers *version_number*

version_number 是您要安装的 FXOS 平台捆绑包的版本号，例如 2.3(1.58)。

e) 系统将首先验证想要安装的软件包。它会告知您当前已安装的应用程序与指定的FXOS平台软件包之间的所有不兼容问题。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。只要 ASA 版本在兼容性表中列为可升级版本，就可以忽略这些警告。

输入 **yes**，确认您想要继续验证。

f) 输入 **yes**确认您想要继续安装，或者输入 **no**取消安装。

FXOS 打开捆绑包，升级/重新加载组件。

g) 要监控升级流程，请参阅监控升级进度，第 187 页：

步骤 16 成功升级所有组件后，验证安全模块/安全引擎和任何已安装的应用程序的状态（请参阅确认安装，第 188 页）。

步骤 17 将新的 ASA 软件映像下载到机箱：

a) 进入安全服务模式：

top

scope ssa

b) 进入应用软件模式：

scope app-software

c) 下载逻辑设备软件映像：

download image *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://用户名@服务器/路径
- **scp**://用户名@服务器/路径
- **sftp**://用户名@服务器/路径

- **tftp**://服务器:端口号/路径

d) 要监控下载过程，请执行以下操作：

show download-task

e) 要查看已下载的应用，请执行以下操作：

up

show app

记下您下载的软件包的 ASA 版本。在后面的步骤中，您将需要使用准确的版本字符串来启用应用程序。

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

步骤 18 升级 ASA 逻辑设备映像：

a) 进入安全服务模式：

top

scope ssa

b) 将范围设置为您正在更新的安全模块：

scope slot*slot_number*

c) 将范围设置为 ASA 应用程序：

对于 FXOS 2.3.1 及更低版本： **scope app-instance asa**

对于 FXOS 2.4.1 及更高版本：**scope app-instance asa** *instance_name*

d) 将入门版本设置为想要更新的版本：

set startup-version *version_number*

e) 提交配置：

commit-buffer

提交系统配置任务。应用映像已更新，应用重新启动。

步骤 19 要验证安全模块/安全引擎和任何已安装的应用程序的状态，请参阅确认安装，第 188 页。

步骤 20 如果故障转移组被配置为“启用抢占”，在抢占延迟过后，它们会在其指定设备上自动变为活动状态。如果故障转移组未被配置为启用抢占，则可以使用 **监控 > 故障转移 > 故障转移组号** 窗格使其在指定设备上恢复为活动状态。

升级 FXOS 和 ASA 机箱间集群

使用 FXOS CLI 或 Firepower 机箱管理器在机箱间集群中的所有机箱上升级 FXOS 和 ASA。

使用 Firepower 机箱管理器升级 FXOS 和 ASA 机箱间集群

每个机箱的升级过程最多可能需要 45 分钟。请相应规划您的升级活动。

开始之前

开始升级之前，请确保您已完成以下操作：

- 下载要升级到的 FXOS 和 ASA 软件包。
- 备份您的 FXOS 和 ASA 配置。

过程

步骤 1 确定哪个机箱具有控制单元。您将在最后升级此机箱：

a) 连接到 Cisco Secure Firewall 机箱管理器。
b) 选择**逻辑设备**。
c) 点击加号 (+) 以查看集群中包含的安全模块的属性。
d) 确认主设备位于该机箱中。应存在**集群角色**设置为“主”的 ASA 实例。

步骤 2 连接到集群中没有控制单元的机箱上的 Cisco Secure Firewall 机箱管理器。

步骤 3 上传新的 FXOS 平台捆绑包映像和 ASA 软件映像：

注释 如果要升级到 FXOS 2.3.1 之前的版本，则在升级 FXOS 平台捆绑包软件之前，请不要将 ASA CSP 映像上传到安全设备。

a) 在 Cisco Secure Firewall 机箱管理器中，选择**系统 > 更新**。
可用更新部分显示机箱上的可用软件包列表。
b) 点击**上传映像**。

c) 点击**选择文件**，可导航到并选择想要上传的映像。
d) 点击**上传**。
所选映像将上传到机箱。
e) 等待映像成功上传，然后再继续操作。

步骤 4 （FXOS 2.4.1 或更早版本）禁用机箱上所有安全模块的每个应用实例：

注 - 如果从 FXOS 版本 2.6.1 或更高版本升级，则可以跳过此步骤。

a) 选择**逻辑设备**。
b) 点击每个应用的**禁用**滑块，以禁用集群中包含的每个应用实例。
集群运行状态更改为“不在集群内”。

步骤 5 升级 FXOS 捆绑包：

a) 依次选择**系统** > **更新**。
b) 点击要升级到的 FXOS 平台捆绑包所对应的**升级**图标。

系统将首先验证想要安装的软件包。它会告知您当前已安装的应用程序与指定的FXOS平台软件包之间的所有不兼容问题。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。只要 ASA 版本在兼容性表中列为可升级版本，就可以忽略这些警告。

c) 点击**是**以确认要继续安装。

FXOS 打开捆绑包，升级/重新加载组件。

步骤 6 Firepower 机箱管理器在升级期间将不可用。您可以使用 FXOS CLI 监控升级过程（请参阅监控升级进度，第 187 页）。

步骤 7 成功升级所有组件后，验证安全模块/安全引擎和任何已安装的应用程序的状态（请参阅确认安装，第 188 页）。

步骤 8 在每个安全模块上升级 ASA 逻辑设备映像：

a) 选择**逻辑设备**。
此时会打开**逻辑设备**页面以显示机箱上已配置的逻辑设备列表。
b) 点击想要更新的逻辑设备对应的**设置版本**图标，打开**更新映像版本**对话框。
c) 对于**新版本 (New Version)**，选择想要更新的软件版本。
d) 点击**确定**。

步骤 9 升级过程完成后，确认应用程序在线且成功升级：

a) 选择**逻辑设备**。
b) 验证应用程序版本和运行状态。

步骤 10 （FXOS 2.4.1 或更早版本）为机箱上所有安全模块重新启用集群：

注 - 如果从 FXOS 版本 2.6.1 或更高版本升级，则可以跳过此步骤。

a) 选择**逻辑设备**。
b) 点击集群中包含的每个安全模块的**启用**开关。
集群运行状态更改为“在集群内”。

步骤 11 对集群中没有控制单元的所有剩余机箱重复步骤 2-10。

步骤 12 升级集群中没有控制单元的所有机箱后，在具有控制单元的机箱上重复步骤 2-10，要确保先在数据单元上禁用集群，最后是控制单元。
系统将从先前升级的机箱之一中选择一个新的控制单元。

步骤 13 对于分布式 VPN 集群模式，在集群稳定之后，您可以使用主设备上的 ASA 控制台在集群中的所有模块之间重新分发活动会话。

cluster redistribute vpn-sessiondb

下一步做什么

设置机箱站点 ID。有关如何设置机箱站点 ID 的详细信息，请参阅 Cisco.com 上“在 Firepower 4100/9300 上为 ASA 部署集群以实现可扩展性和高可用性”中的站点间集群主题。

使用 FXOS CLI 机箱管理器升级 FXOS 和 ASA 机箱间集群

每个机箱的升级过程最多可能需要 45 分钟。请相应规划您的升级活动。

开始之前

开始升级之前，请确保您已完成以下操作：

- 下载要升级到的 FXOS 和 ASA 软件包。
- 备份您的 FXOS 和 ASA 配置。
- 收集将软件映像下载到机箱所需的以下信息：
  - 您从其复制映像的服务器的 IP 地址和身份验证凭证。
  - 映像文件的完全限定名称。

过程

步骤 1 确定哪个机箱具有控制单元。您将在最后升级此机箱：

a) 连接到 FXOS CLI。
b) 确认主设备位于该机箱中。应存在“集群角色”设置为“主”的 ASA 实例：

scope ssa

show app-instance

步骤 2 连接到集群中没有控制单元的机箱上的 FXOS CLI。

步骤 3 禁用机箱上所有安全模块的每个应用实例。对于机箱上的每个 ASA 应用，请执行以下步骤：

a) 将 ASA 应用实例范围设置在给定插槽 ：

scope slot *slot_number*

scope app-instance asa

注释　　要连接至不支持多个安全模块的设备的安全引擎，请使用 **1** 作为 *slot_number*。

b) 禁用 ASA 应用：

disable

c) 提交配置：

commit-buffer

步骤 4　将新的 FXOS 平台捆绑包映像下载到机箱：

a) 进入固件模式：

scope firmware

b) 下载 FXOS 平台捆绑包软件映像：

download image *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://用户名@服务器/路径/*image_name*
- **scp**://用户名@服务器/路径/*image_name*
- **sftp**://用户名@服务器/路径/*image_name*
- **tftp**://服务器**:**端口号/路径/*image_name*

c) 要监控下载过程，请执行以下操作：

scope download-task *image_name*

show detail

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

步骤 5　返回 FXOS CLI 的管理引擎层。

退出控制台：

a) 输入 ~

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

telnet>**quit**

退出 Telnet 会话：

a) 输入 **Ctrl-],**。

步骤 6 升级 FXOS 捆绑包：

a) 如有必要，请返回到固件模式：

top

scope firmware

b) 记下要安装的 FXOS 平台捆绑包的版本号：

show package

c) 进入自动安装模式：

scope auto-install

d) 安装 FXOS 平台捆绑包：

install platform platform-vers *version_number*

version_number 是您要安装的 FXOS 平台捆绑包的版本号，例如 2.3(1.58)。

e) 系统将首先验证想要安装的软件包。它会告知您当前已安装的应用程序与指定的FXOS平台软件包之间的所有不兼容问题。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。只要 ASA 版本在兼容性表中列为可升级版本，就可以忽略这些警告。

输入 **yes**，确认您想要继续验证。

f) 输入 **yes**确认您想要继续安装，或者输入 **no**取消安装。

FXOS 打开捆绑包，升级/重新加载组件。

g) 要监控升级流程，请参阅监控升级进度，第 187 页：

步骤 7 成功升级所有组件后，验证安全模块/安全引擎和任何已安装的应用程序的状态（请参阅确认安装，第 188 页）。

步骤 8 将新的 ASA 软件映像下载到机箱：

a) 进入安全服务模式：

top

scope ssa

b) 进入应用软件模式：

scope app-software

c) 下载逻辑设备软件映像：

download image *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://用户名@服务器/路径
- **scp**://用户名@服务器/路径
- **sftp**://用户名@服务器/路径
- **tftp**://服务器:端口号/路径

d) 要监控下载过程，请执行以下操作：

show download-task

e) 要查看已下载的应用，请执行以下操作：

up

show app

记下您下载的软件包的 ASA 版本。在后面的步骤中，您将需要使用准确的版本字符串来启用应用程序。

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

步骤 9 升级 ASA 逻辑设备映像：

a) 进入安全服务模式：

top

scope ssa

b) 将范围设置为您正在更新的安全模块：

scope slot*slot_number*

c) 将范围设置为 ASA 应用程序：

对于 FXOS 2.3.1 及更低版本： **scope app-instance asa**

对于 FXOS 2.4.1 及更高版本：**scope app-instance asa** *instance_name*

d) 将入门版本设置为想要更新的版本：

set startup-version *version_number*

e) 提交配置：

commit-buffer

提交系统配置任务。应用映像已更新，应用重新启动。

步骤 10 要验证安全模块/安全引擎和任何已安装的应用程序的状态，请参阅确认安装，第 188 页。

步骤 11 在升级后的安全模块联机后，为机箱上的所有安全模块重新启用集群：

a) 使用控制台连接或 Telnet 连接来连接至模块 CLI。

connect module *slot_number* {**console** | **telnet**}

要连接至不支持多个安全模块的设备的安全引擎，请使用 **1** 作为 *slot_number*。

示例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) 连接到应用控制台。

connect asa

示例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) 在其中一个安全模块上禁用集群：

cluster group *name*

enable

write memory

d) 对此机箱上的每个安全模块重复步骤 12。

步骤 12 退出应用控制台到 FXOS 模块 CLI。

输入 **Ctrl-a, d**

步骤 13 返回 FXOS CLI 的管理引擎层。

退出控制台：

a) 输入 **~**

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

telnet>**quit**

退出 Telnet 会话：

a) 输入 **Ctrl-],**。

步骤 14 对集群中没有控制单元的所有剩余机箱重复步骤 2-14。

步骤 15 升级集群中没有控制单元的所有机箱后，在具有控制单元的机箱上重复步骤 2-14，要确保先在数据单元上禁用集群，最后是控制单元。
系统将从先前升级的机箱之一中选择一个新的控制单元。

步骤 16 对于分布式 VPN 集群模式，在集群稳定之后，您可以使用主设备上的 ASA 控制台在集群中的所有模块之间重新分发活动会话。

cluster redistribute vpn-sessiondb

下一步做什么

设置机箱站点 ID。有关如何设置机箱站点 ID 的详细信息，请参阅 Cisco.com 上“在 Firepower 4100/9300 上为 ASA 部署集群以实现可扩展性和高可用性”中的站点间集群主题。

监控升级进度

您可以使用 FXOS CLI 监控升级过程：

过程

步骤 1 连接到 FXOS CLI。

步骤 2 输入 **scope system**。

步骤 3 输入 **show firmware monitor**。

步骤 4 等待所有组件（FPRM、交换矩阵互联和机箱）显示升级状态：就绪。

注释　　升级 FPRM 组件后，系统将重启，然后继续升级其他组件。

示例

```
Firepower-chassis# scope system
Firepower-chassis /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

确认安装

输入以下命令以验证安全模块/安全引擎和任何已安装的应用的状态：

过程

步骤 1 连接到 FXOS CLI。

步骤 2 输入 **top**。

步骤 3 输入 **scope ssa**。

步骤 4 输入 **show slot**。

步骤 5 验证 Firepower 4100 系列设备上的安全引擎或 Firepower 9300 设备上安装的任何安全模块的管理状态是否为正常，且操作状态是否为联机。

示例：

步骤 6 输入 **show app-instance**。

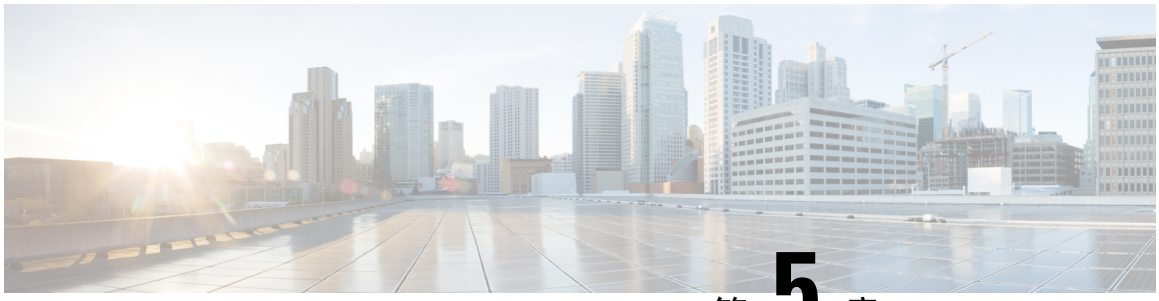
步骤 7 确认机箱上安装的任何逻辑设备的运行状态为联机，并且列出正确的版本。

如果此机箱位于集群中，则确认机箱中安装的所有安全模块的集群运行状态为“在集群内”。此外，确认控制单元不在您要升级的机箱上，不应有任何集群角色设置为“主”的实例。

示例

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
Firepower-chassis /ssa #
Firepower-chassis /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 --------------- ------------
asa        asa1       1          Enabled     Online           9.10.0.85       9.10.0.85
    Not Applicable  None
asa        asa2       2          Enabled     Online           9.10.0.85       9.10.0.85
    Not Applicable  None
Firepower-chassis /ssa #
```



第 5 章

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

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，第 1 页。

另请参阅中的已知降级问题。降级的准则和限制，第 191 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。

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 ，第 93 页在这种情况下，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， 第 106 页程序使用旧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， 第 153 页程序使用旧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， 第 153 页

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 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。