迁移您的管理中心

在 管理中心 型号之间迁移

“安全 管理中心 迁移”向导让您能够从一种 管理中心 型号迁移至另一种 管理中心 型号。该向导可简化您的迁移体验。迁移后，源 管理中心 的配置和事件可在目标 管理中心 使用。

有两种迁移 管理中心 的方法：

- 连接模式：连接到源 管理中心 以进行迁移。当源和目标 管理中心 可以通过 HTTPS 相互连接时，使用此方法。
- 迁移捆绑包模式：在源 管理中心 中创建迁移捆绑包，然后将其上传到目标 管理中心。当源和目标 管理中心 无法通过 HTTPS 相互连接时，使用此方法。

使用安全 管理中心 迁移向导的优势

- 简化迁移：使用直观的向导无缝迁移 管理中心 型号。
- 不受影响的源 管理中心：无论迁移成功还是失败，都确保源 管理中心 不受影响。
- 全面的就绪性检查：通过提供详细的就绪性检查，最大限度地减少型号之间迁移时的错误。
- 实时监控：使用用户界面跟踪迁移进度。
- 广泛许可支持：为所有许可模式提供支持，例如评估、已连接和特定许可证预留 (SLR)。

支持的迁移路径

有关将 管理中心 1000/2500/4500/1600/2600/4600 迁移到 云交付的防火墙管理中心 (cdFMC) 的信息，请参阅《使用 *Security Cloud Control* 中的云交付防火墙管理中心管理防火墙威胁防御》中的“将本地管理中心托管的 Cisco Secure Firewall Threat Defense 迁移到云交付的防火墙管理中心”一章。

表格列出了可从源 管理中心 型号迁移到的受支持目标 管理中心 型号。

最大托管设备数	源型号	目标型号											
		FMC 1600	**FMC 2600**	**FMC 4600**	**管理中心 1700**	**管理中心 2700**	**管理中心 4700**	**管理中心 1800**	**管理中心 2800**	**管理中心 4800**	**FMCv300 (VMware)**	**FMCv300 (AWS)**	**FMCv300 (Azure)**
2	FMCv2 (VMware)	支持	支持	支持	—	—	—	—	—	—	支持	—	—
10	FMCv10 (VMware)	支持	支持	支持	—	—	—	—	—	—	支持	—	—
25	FMCv25 (VMware)	支持	支持	支持	—	—	—	—	—	—	支持	—	—
25	FMCv25 (Azure)	—	—	—	—	—	—	—	—	—	—	—	支持
50	FMC 1000	支持	支持	支持	支持	支持	支持	—	—	—	支持	—	—
50	FMC 1600	—	支持	支持	支持	支持	支持	支持	支持	支持	支持	—	—
250	FMC 2000	—	支持	支持	—	—	—	—	—	—	支持	—	—
300	FMC 2500	—	支持	支持	—	支持	支持	—	—	—	支持	—	—
300	FMC 2600	—	—	支持	—	支持	支持	—	支持	支持	支持	—	—
300	FMCv300 (VMware)	—	支持	支持	—	—	—	—	—	—	—	—	—
750	FMC 4000	—	—	支持	—	—	—	—	—	—	—	—	—
750	FMC 4500	—	—	支持	—	—	支持	—	—	—	—	—	—
750	FMC 4600	—	—	—	—	—	支持	—	—	支持	是	支持	支持
50	管理中心 1700	—	—	—	—	支持	支持	—	—	—	—	—	—
300	管理中心 2700	—	—	—	—	—	支持	—	—	—	—	—	—

最大托管设备数	源型号	目标型号											
		FMC 1600	**FMC 2600**	**FMC 4600**	管理中心 **1700**	管理中心 **2700**	管理中心 **4700**	管理中心 **1800**	管理中心 **2800**	管理中心 **4800**	**FMCv300 (VMware)**	**FMCv300 (AWS)**	**FMCv300 (Azure)**
1000	管理中心 4700	—	—	—	—	—	—	—	—	—	—	—	—
50	管理中心 1800	—	—	—	—	—	—	—	支持	支持	—	—	—
300	管理中心 2800	—	—	—	—	—	—	—	—	支持	—	—	—
1,500	管理中心 4800	—	—	—	—	—	—	—	—	—	—	—	—

注释 在同一型号的 管理中心 1800、2800 或 4800 中迁移之前，请使用备份和恢复数据。

迁移的前提条件

支持的版本

- 源 管理中心 必须为 10.0。
- 目标 管理中心 必须为版本 10.0。
- 托管 威胁防御 设备的版本必须为 7.3 及更高版本。

一般前提条件

- 请参阅支持的迁移路径， 第 2 页以确定可从源型号迁移到的目标型号。
- 确保目标 管理中心 没有托管设备。
- 确保目标 管理中心 与您的源 管理中心具有相同数量的接口。
- 手动更正源或目标 管理中心 的 UTC 时间。
- 验证目标 管理中心 和源 管理中心 的漏洞数据库 (VDB)、轻量级安全软件包 (LSP) 和 Snort 规则更新 (SRU) 版本是否相同。
- 成功完成所有待部署任务。

许可证前提条件

- 您必须具有以下许可模式之一：评估、已连接、特定许可证预留(SLR)或永久许可证预留(PLR)。
- 您必须在思科智能软件管理器 (CSSM) 中验证 威胁防御 权限。
- 在将您的 管理中心 型号迁移到其他型号之前，您必须获取其他 威胁防御 设备所需的许可证（如有）。
- 如果您的目标 管理中心 是虚拟的，则必须获取 管理中心 Virtual (FMCv) 的许可证。

使用连接模式的前提条件

- 我们建议源和目标 管理中心 位于同一子网中，因为目标 管理中心 会采用源 管理中心 的原始 IP 地址。
- 确保可通过 HTTPS（端口 443）从目标 管理中心 访问源 管理中心。如果无法访问，则使用迁移的迁移捆绑包模式。
- 确保您有两个用户 — 一个用于登录源 管理中心 UI，另一个管理员用户用于执行型号迁移。
- 确保已启用 REST API（**管理 > 配置 > REST API 首选项 > 启用 REST API**）。

使用迁移捆绑包模式的前提条件。

1. 将 **/etc/rc.d/modelmigrationboot.d/modelmigrationboot.d.tar.gz** 从目标 管理中心 传输到源 管理中心，然后将复制的位置指定为：

   ```
   /etc/rc.d/modelmigrationboot.d# fmc_model_migration_cli.pl --script-path
   /path/to/modelmigrationboot.d.tar.gz
   ```

   modelmigrationboot.d.tar.gz 包含为生成模型迁移捆绑包而必须在源 管理中心 中运行的所有模型迁移脚本。

2. 在源 管理中心 中，在专家模式下运行 **sudo fmc_model_migration_cli.pl** 脚本。

注释 该脚本会在 **/var/log/sf** 中创建迁移捆绑包文件 **source_database_content.tgz**。请勿更改迁移捆绑包的文件格式。

3. 下载迁移捆绑包。

我们建议源和目标 管理中心 位于同一子网中，因为目标 管理中心 会采用源 管理中心 的原始 IP 地址。

高可用性的前提条件

- 确保满足所有 HA 要求。有关详细信息，请参阅管理中心高可用性的前提条件。
- 如果源 管理中心 是 HA 的一部分，则必须连接到主用 管理中心。
- 确保目标 管理中心 不是 HA 对的一部分。

管理中心 虚拟迁移的前提条件

- 在将 管理中心 Virtual (FMCv) 迁移到公共云中的另一个 管理中心 Virtual 时，我们建议如下：
  - 使用保留的静态公共 IP 地址，而不是默认公共 IP 地址。
  - 使用 FQDN 或 DNS 名称，因为它可以在公共 IP 地址之间移动。
  - 如果您不想更新目标 管理中心 Virtual 的公网 IP 地址，请在 威胁防御 设备 CLI 中运行以下命令：

    configure manager add DONTRESOLVE *any_key any_key_for_nat_field_input*

    运行此命令之前，请确保 管理中心 Virtual 可以连接到 威胁防御 设备。
  - 如果您没有运行 **configure manager add DONTRESOLVE** *any_key any_key_for_nat_field_input* 命令，请在 威胁防御 设备 CLI 中使用以下命令更新 威胁防御 设备中的 管理中心 虚拟 IP 地址：

    configure manager edit *fmc_uuid* **displayname** *fmc_ipaddress*
  - 当您从适用于 Azure 的 管理中心 4600 迁移到 管理中心 Virtual 300 (FMCv300) 时：
    - 更新 管理中心 Virtual 300 的网络配置，以满足 Azure 网络要求。
    - 通过 SSH 连接到每个托管 威胁防御，并使用 **configure manager edit** 命令更新 管理中心 管理器地址。

将 管理中心 1600、2600 或 4600 迁移到 管理中心 1700、2700 或 4700 的前提条件

在迁移 管理中心 1600、2600 或 4600 之前，您必须将其升级到 7.4.x 或 7.6.x。有关此升级的更多信息，请参阅《适用于管理中心的 *Cisco Secure Firewall Threat Defense* 升级指南》。

将 管理中心 4600 迁移到适用于 AWS 或 VMware 的 管理中心 Virtual 300 (FMCv300) 的前提条件

- 请注意，管理中心 Virtual 300 的限制低于 管理中心 4600 的限制。建议您在迁移之前查看表 1。

表 *1:* 将 管理中心 *4600* 迁移到适用于 *AWS* 或 *VMware* 的 管理中心 *Virtual 300* 的兼容性检查

性能和功能	管理中心 4600（当前配置）	管理中心 Virtual 300（最大限制）
总体大小（事件存储空间）	3.2 TB	2 TB
总设备数	750	300
IPS 事件的最大数量	3 亿	6000 万
Memory	128 GB	64 GB
CPU	两个 Intel Xeon 4214 处理器	32 个 vCPU
最大网络映射大小（主机/用户）	600,000/600,000	150,000/150,000

性能和功能	管理中心 **4600**（当前配置）	管理中心 **Virtual 300**（最大限制）
最大事件速率（每秒事件数）	20,000 eps	12,000 eps

- 要将适用于 AWS 或 VMware 的 管理中心 4600 迁移到 管理中心 Virtual 300 (FMCv300)：
  - 确保源 管理中心 的版本为 7.4.x 或 7.6.x。
  - 确保适用于 AWS 或 VMware 的 管理中心 Virtual 300 具有许可证，您必须在迁移后应用该许可证。

使用连接模式迁移 管理中心

开始之前

确保可从目标 管理中心 访问源 管理中心。

过程

步骤 1 选择**管理** > **高级** > **迁移管理中心** 。

步骤 2 在**选择迁移方法**下：

a) 在**源 Firewall Management Center IP 地址**字段中，输入源 管理中心 的 IP 地址或 FQDN。您可以使用 IPv4 或 IPv6 地址。

b) 在**用户名**和**密码**字段中，输入凭证。

c) 点击**连接 (Connect)**。

连接到源 管理中心 后，系统将显示其证书。

步骤 3 在**准备并开始迁移**下：

向导会自动运行兼容性检查，以确保 管理中心 已准备好进行迁移。如果发现任何问题，则会显示错误或警告消息，或同时显示这两种消息。

注释
物理 威胁防御 设备的设备限制显示为 0。您可以忽略此值并继续迁移。

a) 查看消息并执行所需操作。

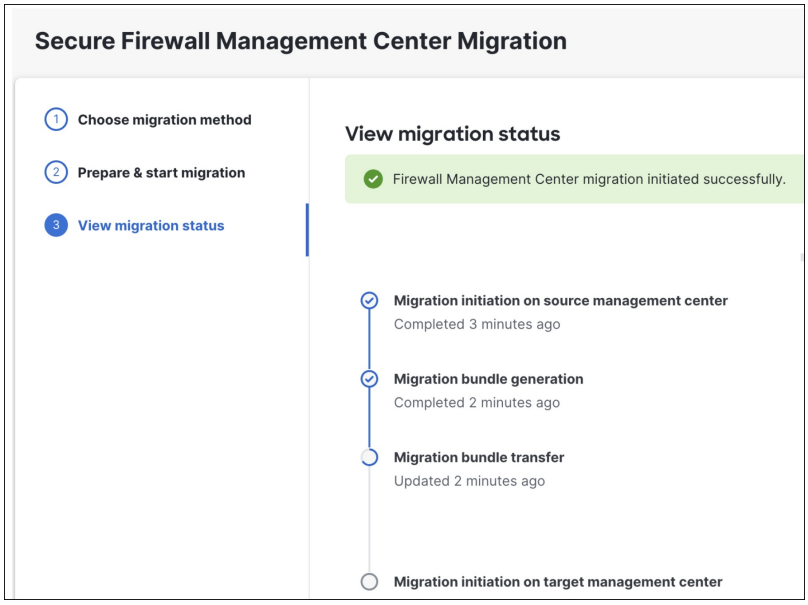
b) （可选）根据需要选中**迁移事件**复选框。

请注意，事件迁移可能需要很长时间，具体取决于事件数据库的大小。

c) 点击**开始迁移**。

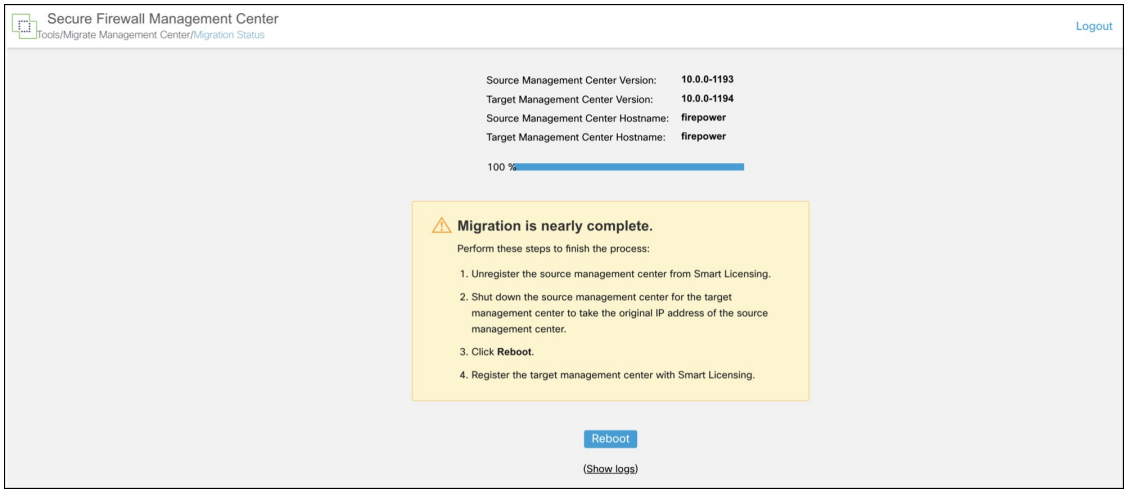
步骤 4 在**查看迁移状态**下：

迁移显示为四个主要任务（请参阅列表）。每项主任务完成时，系统都会显示蓝色复选标记。



1. 在源 管理中心 上启动迁移
2. 迁移包生成
3. 迁移包传输
4. 在目标 管理中心 上启动迁移

成功完成前三个迁移阶段后，系统将显示临时用户界面。进度条会显示迁移进度。点击**显示日志**以查看迁移日志。



a) 登录目标 管理中心 Web 界面。
b) 在**用户名**和**密码**字段中，输入您的凭证。
c) 点击**登录**。

步骤 5 迁移完成后，点击**重启**以重新启动目标 管理中心。

注释
在点击**重启**之前，请从智能许可中取消注册源 管理中心，并将其关闭。

步骤 6 重新引导后，在智能许可中注册目标 管理中心。

下一步做什么

执行 迁移后活动的建议，第 12 页 中描述的任务。

使用迁移包迁移 管理中心。

开始之前

创建并下载迁移捆绑包文件。有关详细信息，请参阅使用迁移捆绑包模式的前提条件。，第 4 页。

过程

步骤 1 选择**管理** > **高级** > **迁移管理中心** 。

步骤 2 在**选择迁移方法**下：

a) 点击**上传迁移捆绑包**。
b) 点击**上传迁移捆绑包**对话框中的**浏览**。
c) 从本地驱动器中选择迁移捆绑包，然后点击**打开**。

默认情况下，迁移捆绑包的最大文件大小为 100 GB。

（可选）要上传超过 100 GB 的迁移捆绑包，您必须使用命令增加文件大小限制。在目标 管理中心 中运行 **/usr/local/sf/bin/update_max_upload_limit.sh** 命令以提高文件大小限制。

步骤 3 在**准备并开始迁移**下：

该向导将运行兼容性检查，以确保管理中心 已准备好进行迁移。如果发现任何问题，则会显示错误和/或警告。

a) 查看错误和警告，并对设备采取必要的措施。
b) （可选）根据需要选中**迁移事件**复选框。

请注意，迁移事件可能需要很长时间，具体取决于事件数据库的大小。如果捆绑包没有任何事件，则禁用此复选框。

c) 点击**开始迁移**。

步骤 4 在**查看迁移状态**下：

迁移分四个主要阶段进行：

1. 在源 管理中心 上启动迁移
2. 迁移包生成
3. 迁移包传输
4. 在目标 管理中心 上启动迁移

因为您已上传迁移捆绑包，所以该向导会跳过前三个步骤。在第四个阶段之后，系统将显示一个临时用户界面。

a) 登录目标 管理中心 Web 界面。
b) 在**用户名**和**密码**字段中，输入您的凭证。
c) 点击**登录**。

进度条会显示迁移进度。点击**显示日志**以查看迁移日志。

步骤 5 迁移完成后，执行以下步骤：

a) 从智能许可中取消注册源 管理中心。
b) 关闭源 管理中心。
c) 点击**重新启动**。

步骤 6 重新引导后，在智能许可中注册目标 管理中心。

下一步做什么

执行 迁移后活动的建议，第 12 页。

迁移高可用性 管理中心 型号

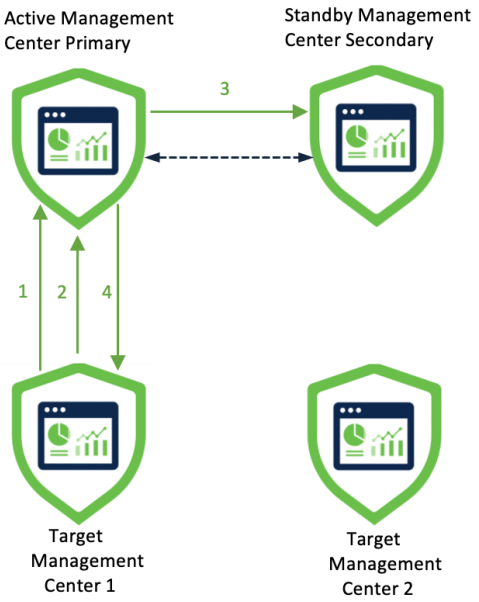
您可以使用 管理中心 型号迁移向导来迁移 管理中心 HA 设置。

当源 管理中心 采用 HA 配置时，我们建议您从主用对等体启动迁移。源 管理中心 会将备用 管理中心 升级为主用设备。

process_summary

本部分介绍高可用性设置中 管理中心 的不同迁移阶段。

图 *1: HA* 设置中的源和目标 管理中心。



在图 1 中，主用 管理中心 主设备和备用 管理中心 从设备是源 管理中心。

注释 您必须从智能许可中取消注册源 管理中心。请关闭 管理中心 后再重启。

迁移后：

- 目标 管理中心 1 成为主用 管理中心 主设备。
- 目标 管理中心 2 成为主用 管理中心 从设备。

以下阶段描述主用 管理中心 主设备如何迁移到目标 管理中心 1：

1. 目标 管理中心 1 连接到主用源 管理中心。
2. 目标 管理中心 1 启动迁移捆绑包生成。
3. 主用 管理中心 将备用 管理中心 升级到主用状态。
4. 目标 管理中心 1 会下载迁移捆绑包并启动迁移。

process_workflow

图 *2:* 迁移主用 管理中心 从设备

在图 2 中，第一次迁移后，目标 管理中心 1 是主用 管理中心 主设备。

开始将源主用 管理中心 从设备迁移到目标 管理中心 2。以下阶段描述了此迁移：

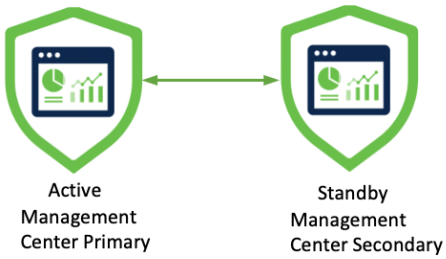
1. 目标 管理中心 2 连接到主用源 管理中心。
2. 目标 管理中心 2 启动迁移捆绑包生成。
3. 目标 管理中心 2 会下载迁移捆绑包并启动迁移。

图 *3:* 已迁移 管理中心

在图 3 中，迁移后，两个目标 管理中心 都将处于主用状态，并自动相互连接。

注释 HA 进入“裂脑”状态，在此状态下，两个对等体都成为主用设备。要解决此状态，请将其中一台指定为主用设备，而将另一台指定为备用设备。

图 *4:* 已迁移 管理中心 的最终状态



迁移后活动的建议

成功迁移后，我们建议一些最佳实践和其他任务：

- 您必须更新以下参数：
  - （可选）目标 管理中心 的 IP 地址。默认情况下，在成功迁移后，目标 管理中心 将获取源管理中心 的 IP 地址。

- 所有托管 威胁防御 设备中的管理器详细信息。有关详细信息，请参阅更新 Firewall Threat Defense 设备上的管理中心 IP 地址或主机名，第 14 页。如果 管理中心 的 IP 地址发生变化，请确保在 威胁防御 设备中编辑管理器。如果 管理中心 可以访问 威胁防御 设备，则无需执行此操作。

- 在迁移后，要在源 管理中心 管理另一组 威胁防御 设备：
  - 确保源 管理中心 无法访问过时的 威胁防御 设备。
  - 从源 管理中心 中删除当前由目标 管理中心 管理的过时设备。

注释 如果源 管理中心 可以访问过时的设备，则这些设备将从目标 管理中心 注销。

- 如果源 管理中心 是高可用性的一部分，则在迁移后，您必须将 管理中心 配置为主用或备用 管理中心。

许可证相关活动。

- 智能许可：从源 管理中心 取消注册许可证，并在目标 管理中心 中注册许可证。
- 评估许可证：如果源 管理中心 具有评估许可证，则在迁移后，目标 管理中心 将具有评估许可证。
- 对于虚拟 管理中心，请确保虚拟 管理中心管理中心 具有许可证。例如，从 FMCv25 迁移到 FMCv300 时，应在迁移后应用 FMCv300 许可证。

针对公共云将 管理中心 4600 迁移到 管理中心 Virtual 300 (FMCv300) 后

1. 使用控制台登录到面向公共云的 管理中心 Virtual 300。
2. 更新分配给 管理中心 Virtual 300 的专用 IP 地址，因为在迁移后，FMCv300 会保留源 管理中心 的 IP 地址。
3. 通过 SSH 连接到每台托管 威胁防御 设备，并使用 **configure manager edit** 命令更新 管理中心 管理器地址。有关详细信息，请参阅更新 Firewall Threat Defense 设备上的管理中心 IP 地址或主机名，第 14 页。

思科安全动态属性连接器活动

迁移后，思科安全动态属性连接器(CSDAC)的值或动态对象会被删除。必须下载与该对象关联的IP地址并重新配置这些值。

安全认证合规性

如果源 管理中心 符合统一功能批准产品列表 (UCAPL) 或通用标准 (CC)，则迁移后，目标 管理中心 也将符合 UCAPL 或 CC 标准。

故障排除

- 如果使用迁移捆绑包模式时迁移失败，则在重试迁移时请勿重新使用该捆绑包。生成新的迁移捆绑包。
- 如果迁移失败，且您无法登录目标 管理中心 的 UI，则必须重新映像目标 管理中心。

更新 Firewall Threat Defense 设备上的管理中心 IP 地址或主机名

在迁移后，如果目标 防火墙管理中心 的网络配置与源 防火墙管理中心 的网络配置不同，则必须更新每个 Firewall Threat Defense 设备上的 IP 地址或 防火墙管理中心 主机名。

过程

步骤 1 在 Firewall Threat Defense CLI 中运行 **show managers** 命令以获取 防火墙管理中心 的唯一标识符：

示例：

```
> show managers
Type                      : Manager
Host                      : xx.xx.x.x
Display name              : xx.xx.x.x
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration and analytics
```

步骤 2 运行 **configure manager** 命令更新 防火墙管理中心 IP 地址或主机名：

configure manager edit *fmc_uuid* **hostname** *fmc_ipaddress*

示例：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname xx.xx.x.x
Updating hostname from xx.xx.x.x to xx.xx.x.x
Manager hostname updated.
```

步骤 3 运行 **configure manager** 命令更新 防火墙管理中心 显示名称：

configure manager edit *fmc_uuid* **displayname** *fmc_ipaddress*

示例：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 displayname xx.xx.x.x
Updating displayname from xx.xx.x.x to xx.xx.x.x
Manager displayname updated.
```

步骤 4 运行 **show manager** 命令验证更新的 防火墙管理中心 配置。

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。

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。

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。

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。