思科虚拟 **Firepower** 管理中心部署指南

首次发布日期: 2015 年 11 月 10 日

上次修改日期: 2018 年 12 月 3 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

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克利分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。© 1981，加州大学董事会。

无论本手册中是否有任何其他保证，这些供应商的所有文档文件和软件均按“原样”提供，并可能包含缺陷。思科和上面所提及的提供商拒绝所有明示或暗示保证，包括（但不限于）适销性、特定用途适用性和无侵权保证，或者因买卖或使用以及商业惯例所引发的保证。

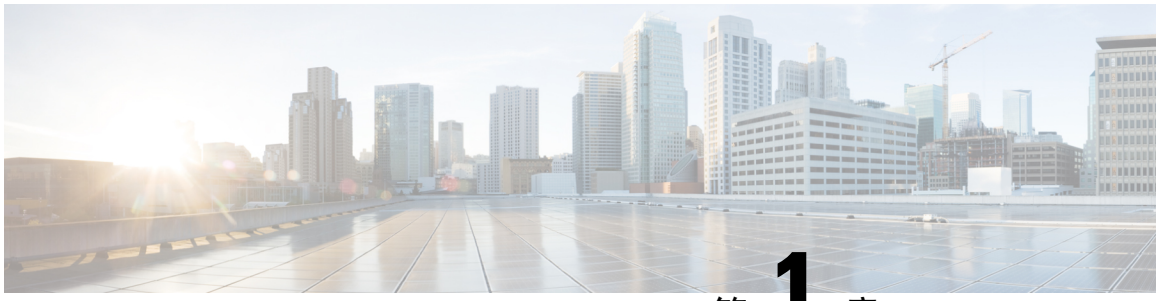
在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

本文档的所有打印副本和复制的电子副本均被视为非受控副本。有关最新版本，请参阅当前在线版本。

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 上列出了各办事处的地址和电话号码。

目录



第 1 章

思科虚拟 Firepower 管理中心设备简介

思科虚拟 Firepower 管理中心 (FMCv) 设备可为虚拟环境提供全面的防火墙功能，从而确保数据中心流量和多租户环境的安全。虚拟 Firepower 管理中心可管理物理和虚拟的 Firepower 威胁防御、Firepower NGIPS 和 FirePOWER 设备。

适用于虚拟 Firepower 管理中心的平台和相关支持

支持的平台

思科虚拟 Firepower 管理中心可以在以下平台上进行部署：

- **VMware vSphere 虚拟机监控程序 (ESXi)** - 您可以在 VMware ESXi 上将虚拟 Firepower 管理中心作为访客虚拟机部署。
- **内核虚拟化模块 (KVM)** - 您可以在运行 KVM 虚拟机监控程序的 Linux 服务器上部署虚拟 Firepower 管理中心。
- **Amazon Web 服务 (AWS)** - 您可以在 AWS 云的 EC2 实例上部署虚拟 Firepower 管理中心。

虚拟机监控程序和版本支持

有关虚拟机监控程序和版本支持的信息，请参阅思科 Firepower 兼容性。

Firepower 管理中心虚拟许可证

Firepower 管理中心虚拟许可证是平台许可证，而非功能许可证。您购买的虚拟许可证版本将确定您可以通过 Firepower 管理中心管理的设备数量。例如，您可以购买能够管理两台、10 台或 25 台设备的许可证。

关于 Firepower 功能许可证

您可以许可各种功能，为您的组织创建最佳 Firepower 系统部署。您可以通过 Firepower 管理中心管理这些功能许可证并将它们分配给您的设备。

注释 Firepower 管理中心可以管理设备的功能许可证，但使用 Firepower 管理中心无需功能许可证。

Firepower 功能许可证取决于您的设备类型：

- Firepower 威胁防御和虚拟 Firepower 威胁防御设备可以使用智能许可证。
- 7000 和 8000 系列、ASA FirePOWER 和 NGIPSv 设备可以使用经典许可证。

使用经典许可证的设备有时也称为经典设备。单个 Firepower 管理中心可以同时管理经典许可证和智能许可证。

除了“使用权”功能许可证以外，许多功能都需要服务订用。使用权许可证不会过期，但服务订用需要定期续订。

有关各个平台上智能许可证与经典许可证的详细信息，请参阅思科 Firepower 系统功能许可证文档。

关于智能许可、经典许可、使用权许可证和服务订用的常见问题的答案，请参阅关于 Firepower 许可的常见问题解答 (FAQ) 文档。

关于虚拟设备性能

虚拟设备的吞吐量和处理能力无法准确预测。虚拟设备的性能在很大程度上会受到多种因素的影响，例如：

- 主机的内存数量和 CPU 容量
- 主机上运行的虚拟机总数量
- 网络性能、接口速度和部署的感应接口数量
- 为每台虚拟设备分配的资源量
- 共享主机的其他虚拟设备的活动水平
- 应用到虚拟设备的策略复杂度

如果吞吐量不理想，请调整分配给共享主机的虚拟设备的资源。

您创建的每台虚拟设备均需要使用主机的一定数量的内存、CPU 和硬盘空间。默认设置是运行系统软件的最低要求，不能降低。但是，为了提高性能，您可以根据可用的资源来增加虚拟设备的内存和 CPU 数量。

下表列出虚拟 Firepower 管理中心设备的默认设置。

表 *1:* 虚拟 *Firepower* 管理中心设备的默认设置

设置	默认	设置可调节？
内存	8 GB	是
虚拟 CPU	4	是，最多 8 个
硬盘调配容量	250 GB	否，取决于所选磁盘格式

下载虚拟 Firepower 管理中心部署软件包

您可以从 Cisco.com 下载虚拟 Firepower 管理中心部署软件包；如果要下载补丁和热修补程序，则可以从 Firepower 管理中心下载。

要下载虚拟 Firepower 管理中心部署软件包，请执行以下步骤：

步骤 1 导航至思科软件下载页面。

注释 需要 Cisco.com 登录信息和思科服务合同。

步骤 2 点击**浏览全部**以搜索虚拟 Firepower 管理中心部署软件包。

步骤 3 选择 **安全** > **防火墙** > **防火墙管理**，然后选择 **虚拟 Firepower 管理中心设备**。

步骤 4 选择型号 > **FireSIGHT 系统软件** > 版本。

下表列出 Cisco.com 上提供的虚拟 Firepower 管理中心软件的命名约定及相关信息。

型号	软件包类型	软件包名称
虚拟 Firepower 管理中心	Firepower 软件安装：VMware	Cisco_Firepower_Management_Center_Virtual_VMware-*version*.**tar.gz**
	Firepower 软件安装：KVM	Cisco_Firepower_Management_Center_Virtual-*version*.**qcow2**
	Firepower 软件安装：AWS	登录到云服务并从市场部署。

步骤 5 找到部署软件包，并将其下载到服务器或管理计算机中。

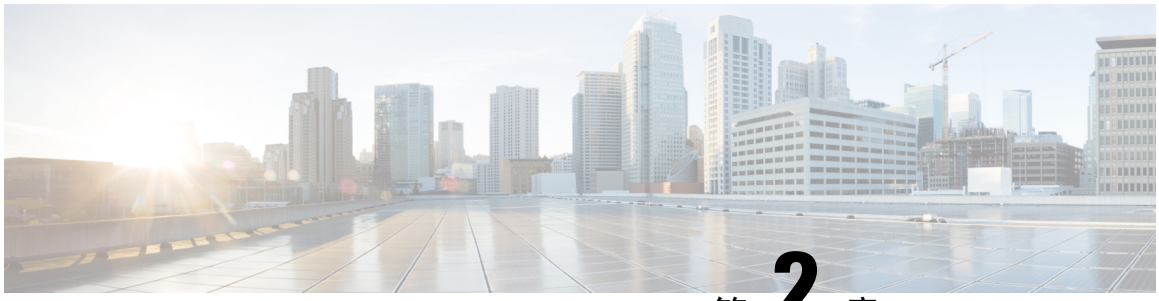
许多软件包名称类似，因此请确保下载正确的软件包。

直接从思科支持和下载站点下载。如果通过邮件传输部署软件包，可能会损坏该软件包。

下一步做什么

请参阅适用于部署平台的章节：

- 要在 VMware ESXi 上将虚拟 Firepower 管理中心作为访客虚拟机部署，请参阅使用 VMware 部署虚拟 Firepower 管理中心，第 5 页。
- 要在运行 KVM 虚拟机监控程序的 Linux 服务器上部署虚拟 Firepower 管理中心，请参阅使用 KVM 部署虚拟 Firepower 管理中心，第 15 页。
- 要在 AWS 云中部署虚拟 Firepower 管理中心，请参阅在 AWS 云上部署虚拟 Firepower 管理中心，第 27 页。



第 2 章

使用 VMware 部署虚拟 Firepower 管理中心

您可以使用 VMware 部署虚拟 Firepower 管理中心 (FMCv)。

虚拟 Firepower 管理中心支持的 VMware 功能

下表列出 FMCv 支持的 VMware 功能。

表 *2: FMCv* 支持的 *VMware* 功能

功能	说明	支持（是/否）	备注
冷克隆	VM 在克隆过程中关闭。	否	–
热添加	VM 在添加过程中运行。	否	–
热克隆	VM 在克隆过程中运行。	否	–
热删除	VM 在删除过程中运行。	否	–
快照	VM 会冻结几秒钟。	是	请谨慎使用。您可能会失去流量。可能出现故障切换。
暂停和恢复	VM 暂停，然后恢复。	是	–
vCloud Director	允许自动部署 VM。	否	–

功能	说明	支持（是/否）	备注
VM 迁移	VM 在迁移过程中关闭。	是	–
vMotion	用于实时迁移 VM。	是	使用共享存储。请参阅 vMotion 支持，第 9 页。
VMware FT	用于 VM 上的 HA。	否	–
VMware HA	用于 ESXi 和服务器故障。	是	–
带 VM 心跳信号的 VMware HA	用于 VM 故障。	否	–
VMware vSphere 独立 Windows 客户端	用于部署 VM。	是	–
VMware vSphere Web 客户端	用于部署 VM。	是	–

主机系统要求

您可以通过调配在 VMware ESX 和 ESXi 虚拟机监控程序上托管的 VMware vSphere 来部署虚拟 Firepower 管理中心。有关虚拟机监控程序兼容性的信息，请参阅思科 Firepower 兼容性指南。

根据所需部署的实例数量和使用要求，FMCv部署所使用的具体硬件可能会有所不同。创建的每台虚拟设备都需要主机满足最低资源配置要求，包括内存、CPU 数量和磁盘空间。

默认设置是运行系统软件的最低要求，不能降低。但是，为了提高性能，您可以根据可用的资源来增加虚拟设备的内存和 CPU 数量。

下表列出 FMCv 设备的默认设置。

表 *3:* 虚拟设备默认设置

设置	默认	设置可调节？
内存	8 GB	是
虚拟 CPU	4	是，最多 8 个
硬盘调配容量	250 GB	否，取决于所选磁盘格式

运行 VMware vCenter 服务器和 ESXi 实例的系统必须满足特定的硬件和操作系统要求。有关支持平台的列表，请参阅 VMware 在线兼容性指南。

对虚拟化技术的支持

用作 ESXi 主机的计算机必须满足以下要求：

- 必须具有可提供虚拟化支持的 64 位 CPU，并采用英特尔虚拟化技术 (VT) 或 AMD Virtualization™ (AMD-V™) 技术。
- 必须在 BIOS 设置中启用虚拟化技术

注释 英特尔和 AMD 都提供在线处理器识别实用程序来帮助您识别 CPU 并确定它们的性能。许多服务器虽含有支持的 VT 的 CPU，但默认状态下会禁用 VT，您必须手动启用 VT。请查阅制造商文档，了解如何在您的系统中启用 VT 支持。

- 如果您的 CPU 支持 VT，但您在 BIOS 中没有看到此选项，请联系您的供应商，获取可让您启用 VT 支持的 BIOS 版本。
- 必须具有与英特尔 E1000 驱动程序（如 PRO1000MT 双端口服务器适配器或 PRO1000GT 台式机适配器）兼容的网络界面，用以托管虚拟设备。

验证 CPU 支持

您可以使用 Linux 命令行获取 CPU 硬件的相关信息。例如，**/proc/cpuinfo** 文件包含每个 CPU 核心的详细信息。运行 **less** 或 **cat** 命令，可输出其中的内容。

您可以前往“flags”部分查看以下值：

- vmx — Intel VT 扩展
- svm — AMD-V 扩展

要快速查看文件中是否包含这些值，请使用 **grep** 运行以下命令：

```
egrep “vmx|svm” /proc/cpuinfo
```

如果您的系统支持 VT，您会在“flags”列表中看到 *vmx* 或 *svm*。

适用于虚拟 Firepower 管理中心和 VMware 的准则、限制和已知问题

OVF 文件准则

虚拟设备使用开放虚拟化格式 (OVF) 封装。您需要使用虚拟基础设施 (VI) 或 ESXi OVF 模板部署虚拟设备。OVF 文件的选择取决于部署目标，详细如下：

- 在 vCenter 上部署 - Cisco_Firepower_Management_Center_Virtual_VMware-**VI**-*X.X.X-xxx*.ovf
- 在 ESXi（无 vCenter）上部署 - Cisco_Firepower_Management_Center_Virtual_VMware-**ESXi**-*X.X.X-xxx*.ovf

其中，*X.X.X-xxx* 是要部署的 Firepower 系统软件的版本和内部版本号。请参阅

- 如果使用 VI OVF 模板部署，安装过程将允许您执行虚拟 Firepower 管理中心设备的整个初始设置。可以指定：
  - 管理员账户的新密码。
  - 使设备可以在管理网络上进行通信的网络设置。

  注释 必须使用 VMware vCenter 管理此虚拟设备。
- 如果使用 ESXi OVF 模板部署，必须在安装后配置 Firepower 系统所需的设置。可以使用 VMware vCenter 来管理此虚拟设备，或将其用作独立设备。

部署 OVF 模板时需提供以下信息：

表 *4: VMware OFV* 模板设置

设置	ESXi 或 VI	操作
导入/部署 OVF 模板 (Import/Deploy OVF Template)	两者	浏览至您从 Cisco.com 下载的 OVF 模板。
OVF 模板详细信息 (OVF Template Details)	两者	确认正在安装的设备（思科虚拟 Firepower 管理中心）和部署选项（VI 或 ESXi）。
接受 EULA (Accept EULA)	仅 VI	同意接受 OVF 模板中包含的许可条款。
名称和位置 (Name and Location)	两者	为虚拟设备输入一个有意义的唯一名称，然后选择设备的资产位置。
主机/集群 (Host / Cluster)	两者	选择要部署虚拟设备的主机或集群。

设置	ESXi 或 VI	操作
资源池 (Resource Pool)	两者	通过建立有意义的层次结构，管理您在主机或集群内的计算资源。虚拟机和子资源池共享父资源池的资源。
存储	两者	选择一个 datastore 来存储与虚拟机关联的所有文件。
磁盘格式化	两者	选择存储虚拟磁盘的格式：密集调配延迟置零、密集调配快速置零或精简调配。
网络映射 (Network Mapping)	两者	选择虚拟设备的管理接口。
属性 (Properties)	仅 VI	自定义虚拟机初始配置设置。

vMotion 支持

如果计划使用 vMotion，建议仅使用共享存储。在部署过程中，如果有主机集群，则可以在本地（特定主机上）或在共享主机上调配存储。但是，如果您尝试使用 vMotion 将虚拟 Firepower 管理中心迁移到另一台主机，则使用本地存储将会产生错误。

INIT 重生错误消息现象

您可能会在 ESXi 6 和 ESXi 6.5 上运行的虚拟 Firepower 管理中心控制台看到以下错误消息：

```
"INIT: Id "fmcv" respawning too fast: disabled for 5 minutes"
```

解决方法 - 在设备电源关闭时，编辑 vSphere 中的虚拟机设置添加串行端口。

1. 右键点击虚拟机，然后选择**编辑设置**。
2. 在虚拟硬件选项卡中，从**新建设备**下拉菜单中选择**串行端口**，然后点击**添加**。

   虚拟设备列表的底部将会显示串行端口。
3. 在**虚拟硬件**选项卡中，展开**串行端口**，并选择连接类型**使用物理串行端口**。
4. 取消选中**在启动时连接**复选框。

   点击**确定**保存设置。

限制

针对 Vmware 进行部署时，有以下限制：

- 思科虚拟 Firepower 管理中心设备没有序列号。**系统**>**配置**页面将会显示**无**或**未指定**，具体取决于虚拟平台。
- 不支持克隆虚拟机。
- 不支持使用快照恢复虚拟机。

- 不支持恢复备份。
- 不支持无法识别 OVF 封装的 VMware 工作站、播放器、服务器和 Fusion。

下载安装软件包

思科在其支持网站上以压缩存档文件形式 (.tar.gz) 提供适用于 VMware ESX 和 ESXi 主机环境的打包虚拟设备。思科虚拟设备被封装成虚拟机（虚拟硬件版本 7）的形式。每个存档包含适用于 ESXi 或 VI 部署目标的 OVF 模板和清单文件，以及虚拟机磁盘格式 (vmdk) 文件。

从 Cisco.com 下载虚拟 Firepower 管理中心安装软件包，并将其保存到本地磁盘。思科建议始终使用所提供的最新软件包。虚拟设备包通常与系统软件的主要版本（例如，6.1 或 6.2）关联。

步骤 1 导航至思科软件下载页面。

注释 需要 Cisco.com 登录信息和思科服务合同。

步骤 2 点击**浏览全部**以搜索虚拟 Firepower 管理中心部署软件包。

步骤 3 选择 **安全** > **防火墙** > **防火墙管理**，然后选择 **虚拟 Firepower 管理中心设备**。

步骤 4 使用以下命名约定，查找要为虚拟 Firepower 管理中心设备下载的 VMware 安装软件包：

Cisco_Firepower_Management_Center_Virtual_VMware-X.X.X-xxx.tar.gz

其中，*X.X.X-xxx* 是要下载的安装软件包的版本和内部版本号。

步骤 5 点击要下载的安装软件包。

注释 在登录支持站点时，思科建议下载虚拟设备的所有可用更新，这样，在将虚拟设备安装到主版本之后，就可以更新其系统软件。应始终运行设备支持的最新版本的系统软件。对于思科虚拟 Firepower 管理中心，您还需下载所有新的入侵规则和漏洞数据库 (VDB) 更新。

步骤 6 将安装软件包复制到正在运行 vSphere 客户端的工作站或服务器可访问的位置。

注意 请勿通过邮件传输存档文件；否则，文件会被损坏。

步骤 7 使用您偏好的工具解压缩安装软件包存档文件，然后提取安装文件。思科虚拟 Firepower 管理中心的安装软件包存档文件如下：

- Cisco_Firepower_Management_Center_Virtual_VMware-X.X.X-xxx-disk1.vmdk
- Cisco_Firepower_Management_Center_Virtual_VMware ESXi X.X.X xxx.ovf
- Cisco_Firepower_Management_Center_Virtual_VMware ESXi X.X.X xxx.mf
- Cisco_Firepower_Management_Center_Virtual_VMware-VI-X.X.X-xxx.ovf
- Cisco_Firepower_Management_Center_Virtual_VMware-VI-X.X.X-xxx.mf

其中，*X.X.X-xxx* 是已下载的存档文件的版本和内部版本号。

注释　请确保将所有文件存放在同一目录中。

下一步做什么

- 确定部署目标（VI 或 ESXi）并继续，请参阅使用 VMware vSphere 进行部署，第 11 页。

使用 VMware vSphere 进行部署

您可以使用 VMware vSphere vCenter、vSphere 客户端、vSphere Web 客户端或 ESXi 虚拟机监控程序（用于单机 ESXi 部署）部署虚拟 Firepower 管理中心。您可以使用 VI 或ESXi OVF 模板进行部署：

- 如果使用 VI OVF 模板部署，设备必须由 VMware vCenter 管理。
- 如果使用 ESXi OVF 模板部署，设备可由 VMware vCenter 管理，或部署到独立 ESXi 主机。无论是哪种情况，都必须在安装后配置 Firepower 系统所需的设置。

在向导的每个页面指定设置后，点击**下一步**继续。为方便起见，向导的最后一个页面允许您在完成操作步骤之前确认设置。

步骤 1　从 VMware vSphere 客户端中选择**文件** > **部署 OVF 模板**。

步骤 2　从下拉列表中，选择想要用于部署虚拟 Firepower 管理中心的 OVF 模板：

- Cisco_Firepower_Management_Center_Virtual_VMware-VI-*X.X.X-xxx*.ovf
- Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-*X.X.X-xxx*.ovf

其中，*X.X.X-xxx* 是从 Cisco.com 下载的安装软件包的版本和内部版本号。

步骤 3　查看 **OVF 模板详细信息**页面，然后点击**下一步**。

步骤 4　如果许可协议封装在OVF模板内（仅VI模板），系统会显示**最终用户许可协议**页面。同意接受许可条款并点击**下一步**。

步骤 5　（可选）编辑名称并选择库存中虚拟 Firepower 管理中心所在的文件夹位置，然后点击**下一步**。

注释　当 vSphere 客户端直接连接到 ESXi 主机时，不会出现选择文件夹位置的选项。

步骤 6　选择要部署虚拟 Firepower 管理中心的主机或集群，然后点击“下一步”。

步骤 7　导航至想要在其中运行虚拟 Firepower 管理中心的资源池并将其选中，然后点击**下一步**。

仅当集群包含资源池时，系统才会显示此页面。

步骤 8　选择要存储虚拟机文件的存储位置，然后点击**下一步**。

在此页面上，您可以从目标集群或主机上已配置的 Datastore 中选择。虚拟机配置文件和虚拟磁盘文件均存储在 Datastore 上。选择一个足够大的 Datastore，以容纳虚拟机及其所有虚拟磁盘文件。

步骤 9　选择磁盘格式以存储虚拟机虚拟磁盘，然后点击**下一步**。

如果选择**密集调配**，则会立即分配所有存储。如果选择**精简调配**，则会在数据写入虚拟磁盘时将按需分配存储。

步骤 10 将虚拟 Firepower 管理中心的管理接口与网络映射屏幕上的 VMware 网络关联。

右键单击您的基础设施中的**目标网络 (Destination Networks)** 列，选中一个网络以建立网络映射，然后点击**下一步 (Next)**。

步骤 11 如果用户可配置属性封装在 OVF 模板（仅 VI 模板）内，则设置可配置属性，然后点击**下一步**。

步骤 12 查看并验证**准备完成**窗口中的设置。

步骤 13 （可选）选中**部署后启动**选项启动虚拟 Firepower 管理中心，然后点击**完成** 。

如果您选择不在部署后启动，可以稍后从 VMware 控制台执行此操作；请参阅初始化虚拟设备。

步骤 14 完成安装后，关闭状态窗口。

步骤 15 完成该向导后，vSphere Web 客户端将处理 VM；您可以在**全局信息**区域的**最近任务**窗格中看到“初始化 OVF 部署”状态。

完成后，您会看到“部署 OVF 模板”完成状态。

然后“库存”中的指定数据中心下会显示思科虚拟 Firepower 管理中心实例。启动新的 VM 最多可能需要 30 分钟。

注释 为成功向思科许可授权机构注册虚拟 Firepower 管理中心，Firepower 管理中心需要互联网访问权限。部署之后，可能需要执行其他配置，以实现互联网访问和成功注册许可证。

下一步做什么

- 请确认虚拟设备的硬件和内存设置是否满足部署需求（参阅验证虚拟机属性 ， 第 12 页）。

验证虚拟机属性

使用 VMware 虚拟机“属性”对话框为选定的虚拟机调整主机资源分配。您可以从此选项卡更改 CPU、内存、磁盘和高级 CPU 资源。也可以更改适用于虚拟机的虚拟以太网适配器配置的启动连接设置、MAC 地址和网络连接。

步骤 1 右键单击新虚拟设备名称，然后从上下文菜单中选择**编辑设置**，或在主窗口的**开始**选项卡中点击**编辑虚拟机设置**。

步骤 2 确保**内存**、**CPU** 和**硬盘 1** 的设置不低于默认设置（如第 4 页“虚拟设备的默认设置”中所述）。

窗口左侧列出了设备的内存设置和虚拟 CPU 数量。要查看硬盘的**调配容量**，请点击**硬盘 1**。

步骤 3 或者，通过点击窗口左侧的相应设置并在窗口右侧执行更改，增加内存和虚拟 CPU 的数量。

步骤 4 确认**网络适配器 1** 设置如下，必要时执行更改：

a) 在**设备状态**下，启用**打开电源时连接**复选框。

b) 在 **MAC 地址**下，手动设置虚拟设备管理接口的 MAC 地址。

将 MAC 地址手动分配到虚拟设备，以避免 MAC 地址更改或动态池中的其他系统出现冲突。

此外，对于思科虚拟 Firepower 管理中心，如果必须重新映像虚拟设备，手动设置其 MAC 地址可确保不需要再次向思科申请许可证。

c) 在**网络连接**下，将**网络标签**设置为虚拟设备管理网络的名称。

步骤 5 点击**确定**。

下一步做什么

- 初始化虚拟设备；请参阅启动并初始化虚拟设备，第 13 页。
- 或者，在启动设备之前，您可以创建一个额外的管理接口；相关详细信息，请参阅适用于 *VMware* 的思科 *Firepower NGIPSv* 快速入门指南。

启动并初始化虚拟设备

完成虚拟设备的部署后，在首次启动虚拟设备时，会自动启动初始化。

注意 启动时间取决于多种因素，包括服务器资源的可用性。最多可能需要40分钟来完成初始化。请勿中断初始化，否则您可能需要删除设备并重新开始。

步骤 1 启动设备。

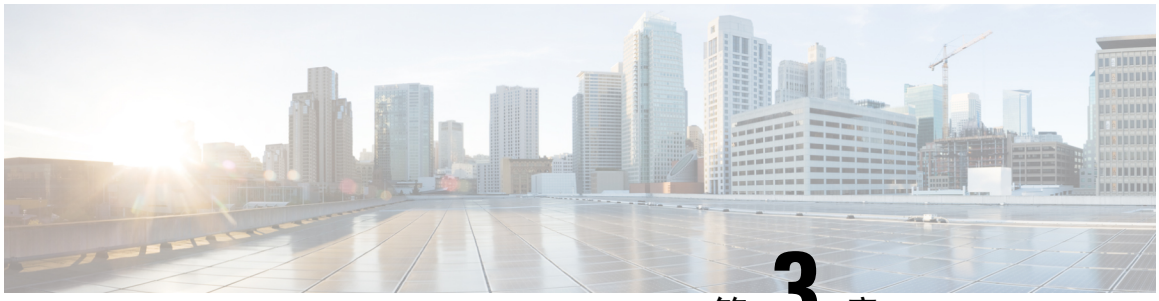
在 vSphere 客户端中，右键单击库存清单中虚拟设备的名称，然后从上下文菜单中选择**电源** > **打开电源**。

步骤 2 在 VMware 控制台选项卡上监控初始化。

下一步做什么

部署 FMCv 后，必须通过设置过程完成对新设备的配置，以便新设备能够在可信管理网络上通信。如果在 VMware 上使用 ESXi OVF 模板部署，则 FMCv 设置分为两步。

- 要完成 FMCv 的初始设置，请参阅虚拟 Firepower 管理中心 初始设置，第 37 页。
- FMCv 部署所需后续步骤的概述，请参阅虚拟 Firepower 管理中心初始管理和配置，第 41 页。



第 3 章

使用 KVM 部署虚拟 Firepower 管理中心

您可以在 KVM 上部署思科虚拟 Firepower 管理中心 (FMCv) 。

关于使用 KVM 的 部署

KVM 是适用于基于 x86 硬件的 Linux 且包含虚拟化扩展（例如英特尔 VT）的完全虚拟化解决方案。其中包含可加载的内核模块 kvm.ko（用于提供核心虚拟化基础设施）和一个处理器特定模块（例如 kvm-intel.ko）。

您可以使用 KVM 来运行多个运行未修改的操作系统映像的虚拟机。每个虚拟机都有专用的虚拟化硬件：网卡、磁盘、图形适配器等等。

KVM 上的虚拟 Firepower 管理中心 (FMCv) 支持以下配置：

- 处理器
  - 需要 4 个 vCPU
- 内存
  - 需要 8 GB RAM
- 网络
  - 支持 virtio 驱动程序
  - 支持一个管理接口
- 每个虚拟机的主机存储

- FMCv 需要 250 GB
- 支持 Virtio 和 SCSI 块设备

- 控制台
  - 通过 telnet 支持终端服务器

使用 KVM 进行部署的前提条件

- 从 Cisco.com 下载虚拟 Firepower 管理中心 qcow2 文件并将其放在 Linux 主机上：

  https://software.cisco.com/download/navigator.html
- 需要 Cisco.com 登录信息和思科服务合同。
- 为与本文档中的部署示例吻合，我们假定您使用 Ubuntu 14.04 LTS。将以下数据包安装在 Ubuntu 14.04 LTS 主机之上：
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager
  - virtinst
  - virsh tools
  - genisoimage
- 性能受主机及其配置的影响。通过调整主机，您可以最大化 KVM 上的吞吐量。有关通用的主机调整概念，请参阅网络功能虚拟化：具备 Linux 和 Intel 架构的宽带远程访问服务器的服务质量。
- Ubuntu 14.04 LTS 的有用优化包括以下内容：
  - macvtap - 高性能 Linux 网桥；您可以使用 macvtap，而不是 Linux 网桥。注意，您必须配置特定设置才能使用 macvtap，而不是 Linux 网桥。
  - 透明大页面 - 用于增加内存页面大小，在 Ubuntu 14.04 中默认开启。
  - 禁用超线程 - 用于将两个 vCPU 减少到一个单核。
  - txqueuelength - 用于将默认 txqueuelength 增加到 4000 个数据包并减少丢包率。
  - 固定 - 用于将 qemu 和 vhost 进程固定到特定 CPU 内核；在某些情况下，固定可显著提高性能。
- 有关优化基于 RHEL 的分发的信息，请参阅Red Hat Enterprise Linux6 虚拟化调整和优化指南。

准则和限制

- 虚拟 Firepower 管理中心设备没有序列号。**系统**>**配置**页面将会显示**无**或**未指定**，具体取决于虚拟平台。
- 不支持克隆虚拟机。
- 不支持高可用性。

准备 Day 0 配置文件

在启动 FMCv之前，您可以准备一个 Day 0 配置文件。Day 0 配置文件是一个文本文件，其中包含了在部署虚拟机时需要应用的初始配置数据。此初始配置将放入您选择的工作目录中名为“day0-config”的文本文件，并写入首次启动时安装和读取的 day0.iso 文件。

注释 该 day0.iso 文件必须在首次启动期间可用。

如果使用 Day 0 配置文件进行部署，该过程将允许您执行 FMCv 设备的整个初始设置。可以指定：

- 接受 EULA
- 系统的主机名
- 管理员账户的新管理员密码
- 使设备能在管理网络上通信的网络设置。如果部署未使用 Day 0 配置文件，则必须在启动后配置 Firepower 系统所需的设置；相关详细信息，请参阅在没有 Day 0 配置文件的情况下部署，第 24 页。

注释 我们在本示例中使用的是 Linux，但对于 Windows 也有类似的实用程序。

步骤 1 在名为“day0-config”的文本文件中输入 FMCv 网络设置的 CLI 配置。

示例：

```
#FMC
{
    "EULA": "accept",
    "Hostname": "FMC-Production",
    "AdminPassword": "Admin123",
    "DNS1": "64.102.6.247",
    "DNS2": "64.102.6.248",
    "DNS3": "",
    "IPv4Mode": "manual",
```

```
    "IPv4Addr": "10.12.129.45",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "disabled",
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
}
```

步骤 2 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：

示例：

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

或

示例：

```
/usr/bin/mkisofs -r -o day0.iso day0-config
```

步骤 3 为每个要部署的 FMCv重复创建唯一的默认配置文件。

下一步做什么

- 如果使用 virt-install，请在 virt-install 命令中添加以下行：

  ```
  --disk path=/home/user/day0.iso,format=iso,device=cdrom \
  ```

- 如果使用 virt-manager，则可以使用 virt-manager GUI 创建虚拟 CD-ROM；请参阅使用虚拟机管理器启动，第 20 页。

启动 FMCv

您可以使用以下方法在 KVM 上启动 FMCv：

- 使用部署脚本 - 使用基于 virt-install 的部署脚本启动 FMCv；请参阅使用部署脚本启动，第 19 页。
- 使用虚拟机管理器 - 使用 virt-manager（用于创建和管理 KVM 访客虚拟机的图形化工具）启动 FMCv；请参阅使用虚拟机管理器启动，第 20 页。
- 使用 OpenStack - 使用 OpenStack 环境启动 FMCv；请参阅使用 OpenStack 启动，第 21 页。

您还可以选择在不使用 Day 0 配置文件的情况下部署 FMCv。此时，您需要使用设备的 CLI 或 Web 界面完成初始设置。

使用部署脚本启动

可以使用基于 virt-install 的部署脚本启动虚拟 Firepower 管理中心。

开始之前

请注意，您可以通过选择适合您环境的最佳访客缓存模式来优化性能。正在使用的缓存模式不仅会影响到是否发生数据丢失，还会影响到磁盘性能。

可以为每个 KVM 访客磁盘接口指定以下缓存模式之一：*writethrough*、*writeback*、*none*、*directsync* 或 *unsafe*。*Writethrough* 模式提供读取缓存；*writeback* 提供读取和写入缓存；*directsync* 绕过主机页面缓存；*unsafe* 可能会缓存所有内容，并忽略来自访客的刷新请求。

- 当主机遇到突然断电时，*cache=writethrough* 有助于降低 KVM 访客计算机上的文件损坏。建议使用 writethrough 模式。
- 但是，由于 *cache=writethrough* 的磁盘 I/O 写入次数高于 *cache=none*，所以该模式也会影响磁盘性能。
- 如果删除了 *--disk* 选项上的 cache 参数，则默认值为 *writethrough*。
- 未指定缓存选项还有可能大幅减少创建虚拟机所需的时间。这是因为，一些较旧的 RAID 控制器的磁盘缓存能力较差。因此，禁用磁盘缓存 (*cache=none*)，从而使用默认值 *writethrough*，有助于确保数据完整性。

步骤 1 创建名为“virt_install_fmc.sh”的 virt-install 脚本。

虚拟 Firepower 管理中心实例的名称在此 KVM 主机上的所有其他虚拟机 (VM) 中必须是唯一的。虚拟 Firepower 管理中心可支持一个网络接口。虚拟 NIC 必须是 Virtio。

示例：

```
virt-install \
    --connect=qemu:///system \
    --network network=default,model=virtio \
    --name=fmcv \
    --arch=x86_64 \
    --cpu host \
    --vcpus=4 \
    --ram=8192 \
    --os-type=linux \
    --os-variant=virtio26 \
    --virt-type=kvm \
    --import \
    --watchdog i6300esb,action=reset \
    --disk path=<fmc_filename>.qcow2,format=qcow2,device=disk,bus=virtio,cache=writethrough \
    --disk path=<day0_filename>.iso,format=iso,device=cdrom \
    --console pty,target_type=serial \
    --serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \
    --force
```

步骤 2 运行 virt_install 脚本：

示例：

```
/usr/bin/virt_install_fmc.sh
Starting install...
Creating domain...
```

此时将出现一个窗口，其中显示虚拟机的控制台。您可以看到虚拟机正在启动。启动虚拟机需要几分钟时间。在虚拟机停止启动后，您可以从控制台屏幕发出 CLI 命令。

使用虚拟机管理器启动

使用 virt-manager（也称为虚拟机管理器）启动虚拟 Firepower 管理中心。Virt-manager 是用于创建和管理访客虚拟机的图形化工具。

步骤 1 启动 virt-manager（**应用** > **系统工具** > **虚拟机管理器**）。

系统可能要求您选择虚拟机监控程序和/或输入您的 root 口令。

步骤 2 点击左上角的按钮，打开**新建虚拟机**向导。

步骤 3 输入虚拟机的详细信息：

a) 指定**名称**。

b) 对于操作系统，选择**导入现有的磁盘映像**。

此方法允许您向其导入磁盘映像（包含预安装的可启动操作系统）。

c) 点击**继续**继续操作。

步骤 4 加载磁盘映像：

a) 点击**浏览...**，选择映像文件。

b) 对于**操作系统类型**，选择 *Linux*。

c) 对于**版本**，选择通用 *2.6.25* 或更高版本 *virtio* 内核。

d) 点击**继续**继续操作。

步骤 5 配置内存和 CPU 选项：

a) 将**内存 (RAM)** 设为 *8192*。

b) 将 **CPU** 设为 *4*。

c) 点击**继续**继续操作。

步骤 6 选中**安装前自定义配置**复选框，然后点击**完成**。

执行此操作将会打开另一个向导，您可以在其中添加、删除和配置虚拟机的硬件设置。

步骤 7 修改 CPU 配置。

从左侧面板中，选择处理器，然后选择**配置** > **复制主机 CPU 配置**。

这会将物理主机的 CPU 型号和配置应用于您的虚拟机。

步骤 8 8. 配置虚拟磁盘：

a) 从左侧面板中，选择**磁盘 1**。
b) 选择**高级选项**。
c) 将**磁盘总线**设为 *Virtio*。
d) 将**存储格式**设为 *qcow2*。

步骤 9 配置串行控制台：

a) 从左侧面板中，选择**控制台**。
b) 选择**删除**，删除默认的控制台。
c) 点击**添加硬件**，添加一台串行设备。
d) 对于**设备类型**，选择 *TCP net* 控制台 *(tcp)* 。
e) 对于**模式**，选择服务器模式（绑定）。
f) 对于**主机**，输入 IP 地址和**端口**号。
g) 选中**使用 Telnet** 框。
h) 配置设备参数。

步骤 10 配置看门狗设备，在 KVM 访客挂起或崩溃时自动触发某项操作：

a) 点击**添加硬件**，添加一台看门狗设备。
b) 对于**型号**，选择默认值。
c) 对于**操作**，选择强制重置访客。

步骤 11 配置虚拟网络接口：

a) 对于**源设备**，选择 *macvtap*。
b) 对于**设备型号**，选择 *virtio*。
c) 对于**源模式**，选择网桥。

注释 默认情况下，虚拟 Firepower 管理中心的虚拟实例通过接口启动，然后您可以配置该接口。

步骤 12 如果使用 Day 0 配置文件进行部署，则为 ISO 创建虚拟 CD-ROM：

a) 点击**添加硬件**。
b) 选择**存储**。
c) 点击**选择托管或其他现有存储**，然后浏览至 ISO 文件的位置。
d) 对于**设备类型**，选择 *IDE CDROM*。

步骤 13 配置虚拟机的硬件后，点击**应用**。

步骤 14 点击**开始安装**，以便 virt-manager 使用您指定的硬件设置创建虚拟机。

使用 OpenStack 启动

您可以在 OpenStack 环境中部署虚拟 Firepower 管理中心。OpenStack 是一套用于构建和管理适用于公共云和私有云的云计算平台的软件工具，并且与 KVM 虚拟机监控程序紧密集成。

关于 OpenStack 上的 Day 0 配置文件

OpenStack 支持通过特殊的配置驱动器 (config-drive) 提供配置数据，该驱动器在 OpenStack 启动时连接到实例。要使用 nova boot 命令和 Day 0 配置部署虚拟 Firepower 管理中心实例，请包括以下行：

```
--config-drive true --file day0-config=/home/user/day0-config \
```

启用 --config-drive 命令后，在调用 nova 客户端的 Linux 文件系统上找到的文件 =/home/user/day0-config，将被传递到虚拟 CDROM 上的虚拟机。

注释 虚拟机可能看到此文件名为 *day0-config*，而 OpenStack 通常将文件内容存储为 /openstack/content/xxxx，其中 xxxx 是分配的四位数编号（例如 /openstack/content/0000）。这可能因 OpenStack 的发行版本而异。

使用命令行在 OpenStack 上启动

使用“nova boot”命令创建和启动 FMCv 实例。

过程

	命令或操作	目的

步骤 1	使用映像、风格、接口和 Day 0 配置信息启动 FMCv实例。
	示例：
	`local@maas:~$ nova boot \`
	`--image=6883ee2e-62b1-4ad7-b4c6-cd62ee73d1aa \`
	`--flavor=a6541d78-0bb3-4dc3-97c2-7b87f886b1ba \`
	`--nic net-id=5bf6b1a9-c871-41d3-82a3-2ecee26840b1 \`
	`--config-drive true --file day0-config=/home/local/day0-config \`
		FMCv 需要一个管理接口。

使用控制面板在 OpenStack 上启动

Horizon 是一个为 OpenStack 服务（包括 Nova、Swift、Keystone 等等）提供基于 Web 的用户界面的 OpenStack 控制面板。

开始之前

- 从 Cisco.com 下载 FMCv qcow2 文件并将其放在本地的 MAAS 服务器上：
  https://software.cisco.com/download/navigator.html
- 需要 Cisco.com 登录信息和思科服务合同。

步骤 1 在登录页面上，输入您的用户名和密码，然后点击**登录**。

控制面板中显示的选项卡和功能取决于已登录用户的访问权限或角色。

步骤 2 从菜单中选择**管理员** > **系统面板** > **风格**。

在 OpenStack 中，虚拟硬件模板被称为风格，定义了 RAM 和磁盘大小、核心数量，等等。

步骤 3 在**风格信息**窗口中输入需要的信息：

a) **名称** - 输入可轻松标识该实例的描述性名称。例如，FMC-4vCPU-8GB。
b) **VCPU** - 选择 4。
c) **RAM MB** - 选择 8192。

步骤 4 选择**创建风格**。

步骤 5 从菜单中选择**管理员** > **系统面板** > **映像**。

步骤 6 在创建映像窗口中输入需要的信息：

a) **名称** - 输入可轻松标识该映像的名称。例如，*FMC-Version-Build*。
b) **说明** -（可选）输入此映像文件的说明。
c) **浏览** - 选择之前从 Cisco.com 下载的虚拟 Firepower 管理中心 qcow2 文件。
d) **格式** - 选择 *QCOW2-QEMU* 仿真器作为格式类型。
e) 选中**公共**复选框。

步骤 7 选择**创建映像**。

查看新创建的映像。

步骤 8 从菜单中选择**项目** > **计算** > **实例**。

步骤 9 点击**启动实例**。

步骤 10 在**启动实例** > **详细信息**选项卡中输入需要的信息：

a) **实例名称** - 输入可轻松标识该实例的名称。例如，*FMC-Version-Build*。
b) **风格** - 选择先前在第 3 步中创建的风格。输入此映像文件的说明。
c) **实例启动源** - 选择从映像启动。
d) **映像名称** - 选择先前在第 6 步中创建的映像。

步骤 11 从**启动实例** > **网络**选项卡中，选择虚拟 Firepower 管理中心实例的管理网络。

步骤 12 点击**启动**。

在云计算节点上启动实例。从实例窗口中查看新创建的实例。

步骤 13 选择虚拟 Firepower 管理中心实例。

步骤 14 选择**控制台**选项卡。

步骤 15 在控制台上登录到虚拟设备。

在没有 Day 0 配置文件的情况下部署

对于所有的Firepower管理中心，必须完成设置过程，以便设备能够在管理网络上通信。如果部署不使用 Day 0 配置文件，设置 FMCv 分为两步：

- 初始化 FMCv 后，在设备控制台运行设备配置脚本，从而使设备可在管理网络上通信。
- 然后，使用管理网络上的计算机访问 FMCv 的 Web 界面，完成设置过程。

使用脚本配置网络设置

以下程序描述如何使用 CLI 在 FMCv 上完成初始设置。

步骤 1 在控制台上登录 FMCv 设备。使用 **admin** 作为用户名，**Admin123** 作为密码。

步骤 2 在管理员提示符下，运行以下脚本：

示例：

```
sudo /usr/local/sf/bin/configure-network
```

第一次连接到 FMCv 时，系统会提示您执行启动后配置。

步骤 3 按脚本提示执行操作。

首先配置（或禁用）IPv4 管理设置，然后是 IPv6 管理设置。如果手动指定网络设置，则必须输入 IPv4 或 IPv6 地址。

步骤 4 确认设置正确。

步骤 5 从设备注销。

下一步做什么

- 使用管理网络上的计算机访问 FMCv 的 Web 界面，完成设置过程。

使用 Web 界面执行初始设置

以下程序描述如何使用 Web 界面在 FMCv 上完成初始设置。

步骤 1 通过浏览器访问 FMCv 管理接口的默认 IP 地址：

示例：

```
https://192.168.45.45
```

步骤 2 登录到虚拟 Firepower 管理中心设备。使用 **admin** 作为用户名，**Admin123** 作为密码。系统将显示设置页面。

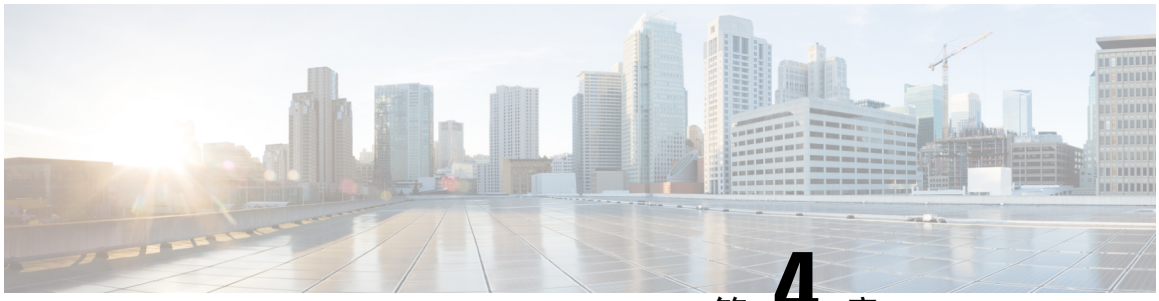
系统将显示设置页面。必须更改管理员密码，指定网络设置（若尚未指定），并接受 EULA。

步骤 3 完成设置后，点击**应用**。FMCv会根据您的选择进行配置。在系统显示中间页面后，您已经以管理员用户（具有管理员角色）身份登录 Web 界面。

FMCv会根据您的选择进行配置。在系统显示中间页面后，您已经以管理员用户（具有管理员角色）身份登录Web界面。

下一步做什么

- 有关 FMCv 初始设置的详细信息，请参阅虚拟 Firepower 管理中心 初始设置，第 37 页。
- FMCv 部署所需后续步骤的概述，请参阅虚拟 Firepower 管理中心初始管理和配置，第 41 页。



第 4 章

在 AWS 云上部署虚拟 Firepower 管理中心

Amazon 虚拟私有云 (Amazon VPC) 使您可以在自定义的虚拟网络中启动 Amazon Web 服务 (AWS) 资源。此虚拟网络非常类似于您可能在自有数据中心内运行的传统网络，并且具有使用 AWS 可扩展基础设施所带来的优势。

您可以在 AWS 云上部署虚拟 Firepower 管理中心 (FMCv)。

关于 AWS 云上的部署

AWS 是一个使用私有 Xen 虚拟机监控程序的公共云环境。FMCv 在 Xen 虚拟机监控程序的 AWS 环境中以访客的身份运行。

AWS 上的 FMCv 支持以下实例类型：

- c3.xlarge 和 c4.xlarge - 4 个 vCPU，7.5 GB，2 个接口，1 个管理接口
- c3.2xlarge 和 c4.2xlarge - 8 个 vCPU，15 GB，3 个接口，1 个管理接口

注释 FMCv 在 AWS 环境之外不支持 Xen 虚拟机监控程序。

AWS 解决方案概述

AWS 是由 Amazon.com 提供并构成云计算平台的一系列远程计算服务（也称为 Web 服务）。这些服务遍布全球 11 个地区。一般情况下，您在部署 FMCv 时，应熟悉以下 AWS 服务：

- Amazon 弹性计算云 (EC2) - 使您能够通过租用虚拟计算机，在 Amazon 数据中心启动和管理自己的应用和服务（例如防火墙）的 Web 服务。

- Amazon 虚拟私有云 (VPC) - 使您能够配置 Amazon 公共云中的隔离专用网络的 Web 服务。您可以在 VPC 内运行自己的 EC2 实例。
- Amazon 简单存储服务 (S3) - 提供数据存储基础设施的 Web 服务。

您可以在 AWS 上创建账户，设置 VPC 和 EC2 组件（使用 AWS 向导或手动配置），并选择 Amazon 系统映像 (AMI) 实例。AMI 是一种模板，其中包含启动您的实例所需的软件配置。

注释 AMI 映像在 AWS 环境之外不可供下载。

AWS 部署准则和限制

前提条件

在 AWS 上部署 FMCv 需满足以下前提条件：

- 拥有 Amazon 账户。可以在 aws.amazon.com 创建一个账户。
- 思科智能账户。可以在思科软件中心 (https://software.cisco.com/) 创建一个账户。
- 许可 FMCv。有关虚拟平台许可证的一般准则，请参阅Firepower 管理中心虚拟许可证，第 1 页；有关如何管理许可证的更多详细信息，请参阅《*Firepower* 管理中心配置指南》中的“Firepower 系统许可”。
- FMCv 接口要求：
  - 管理接口。
- 通信路径：
  - 通过公共/弹性 IP 地址访问 FMCv。
- 有关 FMCv 与 Firepower 系统的兼容性，请参阅思科 Firepower 兼容性指南。

准则

在 AWS 上部署 FMCv 适用以下准则：

- 在虚拟私有云 (VPC) 中部署
- 增强型联网 (SR-IOV)（若可用）
- 从 Amazon Marketplace 部署
- 每个实例最多四个 vCPU
- 第 3 层网络的用户部署

限制

在 AWS 上部署 FMCv 具有以下限制：

- 思科虚拟 Firepower 管理中心设备没有序列号。**系统**>**配置**页面将会显示**无**或**未指定**，具体取决于虚拟平台。
- 通过 CLI 或 Firepower 管理中心完成的任何 IP 地址配置必须与 AWS 控制台中创建的内容一致；在部署期间应注意配置。
- 目前不支持 IPv6。
- 在启动后无法添加接口。
- 目前不支持克隆/快照。
- 不支持高可用性。

配置 AWS 环境

要在 AWS 上部署 FMCv，需要根据部署的特定要求和设置来配置 Amazon VPC。在大多数情况下，设置向导将引导您完成设置过程。AWS 提供在线文档，其中您可以找到与服务（从简介到高级功能）相关的有用信息。有关详细信息，请参阅 AWS 入门 。

为更好地控制 AWS 设置，以下部分提供有关在启动 FMCv 之前如何配置 VPC 和 EC2 的指南：

- 创建 VPC， 第 29 页
- 添加互联网网关， 第 30 页
- 添加子网， 第 31 页
- 添加路由表， 第 31 页
- 创建安全组， 第 32 页
- 创建网络接口， 第 32 页
- 创建弹性 IP 地址， 第 33 页

创建 VPC

虚拟私有云 (VPC) 是 AWS 账户专用的虚拟网络。该网络逻辑上与 AWS 云中的其他虚拟网络相隔离。您可以在自己的 VPC 中启动 AWS 资源，例如虚拟 Firepower 管理中心实例。您可以配置 VPC，选择其 IP 地址范围，创建子网，并配置路由表、网络网关和安全设置。

开始之前

- 创建 AWS 账户。
- 确认存在适用于虚拟 Firepower 管理中心实例的 AMI。

步骤 1 登录到 aws.amazon.com，选择您所在的区域。

AWS 划分为彼此隔离的多个区域。区域显示在屏幕的右上角。一个区域中的资源不会出现在另一个区域中。请定期检查以确保您在预期的区域内。

步骤 2 点击**服务** > **VPC**。

步骤 3 点击**VPC 控制面板** > **我的 VPC**。

步骤 4 点击**创建 VPC**。

步骤 5 在**创建 VPC**对话框中输入以下信息：

a) 用于标识 VPC 的用户自定义**名称标签**。

b) IP 地址 **CIDR 块**。CIDR（无类别域间路由） 是 IP 地址及其关联路由前缀的紧凑表示。例如，10.0.0.0/24。

c) 默认的**租户**设置，以确保在此 VPC 中启动的实例启动时使用指定的租户属性。

步骤 6 点击**是，创建**以创建 VPC。

下一步做什么

添加互联网网关到 VPC 中，详见下一部分。

添加互联网网关

您可以添加互联网网关以控制 VPC 与互联网的连接。您可以将 VPC 之外的 IP 地址流量路由至互联网网关。

开始之前

- 为 FMCv实例创建 VPC。

步骤 1 点击**服务** > **VPC**。

步骤 2 点击**VPC 控制板** > **互联网网关**，然后点击**创建互联网网关**。

步骤 3 输入用于标识网关的用户自定义名称标签，然后点击“是，创建”以创建网关。

步骤 4 选择上一步中创建的网关。

步骤 5 点击**连接到 VPC**并选择之前创建的 VPC。

步骤 6 点击**是，连接**，以将网关连接到 VPC。

默认情况下，在创建网关并将其连接到 VPC 之前，在 VPC 上启动的实例无法与互联网通信。

下一步做什么

添加子网到 VPC 中，详见下一部分。

添加子网

您可以将虚拟 Firepower 管理中心可连接的 VPC 分割为多个 IP 地址范围。您可以根据安全和运营需要创建子网，以实现实例的分组。对于虚拟 Firepower 协议防御，您需要创建一个管理子网和一个流量子网。

步骤 1 点击**服务** > **VPC**。

步骤 2 点击**VPC 控制面板** > **子网**，然后点击**创建子网**。

步骤 3 在**创建子网**对话框中输入以下信息：

a) 用于标识子网的用户自定义**名称标签**。

b) 子网所在的 **VPC**。

c) 此子网将驻留的**可用区域**。选择“无首选项”，以让 Amazon 选择区域。

d) IP 地址 **CIDR 块**。子网 IP 地址范围必须为 VPC 的 IP 地址范围的子集。地址块大小必须介于网络掩码 /16 和 /28 之间。子网大小可以与 VPC 相等。

步骤 4 点击**是，创建**以创建子网。

步骤 5 如需多个子网，重复以上步骤。为管理流量创建单独的子网，根据需要为数据流量创建多个子网。

下一步做什么

添加路由表到 VPC 中，详见下一部分。

添加路由表

您可以将路由表连接到为 VPC 配置的网关。您还可以关联多个子网与单个路由表，但子网一次只可以关联一个路由表。

步骤 1 点击**服务** > **VPC**。

步骤 2 点击**VPC 控制面板** > **路由表**，然后点击**创建路由表**。

步骤 3 输入用于标识路由表的用户自定义**名称标签**。

步骤 4 从下拉列表中选择将使用此路由表的 **VPC** 。

步骤 5 点击**是，创建**以创建路由表。

步骤 6 选择刚创建的路由表。

步骤 7 点击**路由**选项卡，以在详细信息窗格中显示路由信息。

步骤 8 点击**编辑**，然后点击**添加其他路由**。

a) 在**目的地址**列中，输入**0.0.0.0/0**。

b) 在**目标**列中，选择上面创建的互联网网关。

步骤 9 点击**保存**。

步骤 10 点击**子网关联**选项卡，然后点击**编辑**。

步骤 11 选中要用于 FMCv 管理接口的子网对应的复选框，然后点击**保存**。

下一步做什么

创建安全组，详见下一部分。

创建安全组

您可以创建安全组，并在安全组中通过规则指定允许的协议、端口和源 IP 地址范围。可以创建具有不同规则的多个安全组；可以将这些规则分配给每个实例。如果您不熟悉此功能，可参阅 AWS 提供的安全组相关的详细文档。

步骤 1 点击**服务** > **EC2**。

步骤 2 点击 **EC2 控制面板** > **安全组**。

步骤 3 点击**创建安全组**。

步骤 4 在**创建安全组**对话框中输入以下信息：

a) 用于标识安全组的用户自定义**安全组名称**。

b) 此安全组的**说明**。

c) 与此安全组关联的 **VPC**。

步骤 5 配置**安全组规则**：

a) 点击**入站**选项卡，然后点击**添加规则**。

注释 如需从 AWS 外部管理 FMCv，则需要 HTTPS 和 SSH 访问权限。您应指定相应的源 IP 地址。此外，如果在 AWS VPC 内同时配置 FMCv 和 FTDv，应允许专用 IP 管理子网访问权限。

b) 单击**出站**选项卡，然后点击**添加规则**以添加出站流量规则，或保留**所有流量**（面向**类型**）和**任何地方**（面向**目的地址**） 的默认设置。

步骤 6 点击**创建**以创建安全组。

下一步做什么

创建网络接口，详见下一部分。

创建网络接口

您可以使用静态 IP 地址为 FMCv 创建网络接口。根据具体部署需要，创建网络接口（外部和内部）。

步骤 1 点击**服务** > **EC2**。

步骤 2 点击 **EC2 控制面板** > **网络接口**。

步骤 3 点击**创建网络接口**。

步骤 4 在**创建网络接口**对话框中输入以下信息：

a) 网络接口的用户自定义**说明**（可选）。

b) 从下拉列表中选择**子网**。确保选择要创建 Firepower 实例所在 VPC 的子网。

c) 输入**专用 IP** 地址。建议使用静态 IP 地址，而不是选择**自动分配**。

d) 选择一个或多个**安全组**。确保安全组已打开所有必需的端口。

步骤 5 点击**是，创建**以创建网络接口。

步骤 6 选择刚创建的网络接口。

步骤 7 右键单击并选择**更改源/目的地址检查**。

步骤 8 选择**禁用**，然后点击**保存**。

对于创建的任何网络接口，都要重复此操作。

下一步做什么

创建弹性 IP 地址，详见下一部分。

创建弹性 IP 地址

创建实例时，实例会关联一个公共 IP 地址。停止和启动实例时，该公共 IP 地址会自动更改。要解决此问题，可使用弹性 IP 地址为实例分配一个永久性的公共 IP 地址。弹性 IP 地址是用于远程访问 FMCv 及其他实例的保留公共 IP 地址。如果您不熟悉此功能，可参阅 AWS 提供的弹性 IP 相关的详细文档。

注释 至少需要为 FMCv 创建一个弹性 IP 地址，为虚拟 Firepower 威胁防御的管理和诊断接口创建两个弹性 IP 地址。

步骤 1 点击**服务** > **EC2**。

步骤 2 点击**EC2 控制面板** > **弹性 IP**。

步骤 3 点击**分配新地址**。

根据弹性/公共 IP 地址分配需要，重复此步骤。

步骤 4 点击**是，分配**以创建弹性 IP 地址。

步骤 5 根据部署需要，重复上述步骤以创建其他弹性 IP 地址。

下一步做什么

部署 FMCv，详见下一部分。

部署虚拟 Firepower 管理中心实例

开始之前

- 配置 AWS VPC 和 EC2 要素，详见配置 AWS 环境。
- 确认可供 FMCv 实例使用的 AMI。

步骤 1 前往 https://aws.amazon.com/marketplace(Amazon Marketplace) 并登录。

步骤 2 登录到 Amazon Marketplace 后，点击为虚拟 Firepower 管理中心提供的链接。

注释 如果之前已登录 AWS，您可能需要注销并重新登录，以确保链接有效。

步骤 3 点击**继续**，然后点击**手动启动**选项卡。

步骤 4 点击**接受条款**。

步骤 5 在期望的区域点击**使用 EC2 控制台启动**。

步骤 6 选择虚拟 Firepower 管理中心支持的**实例类型**；有关支持的实例类型，请参阅关于 AWS 云上的部署。

步骤 7 点击屏幕底部的**下一步：配置实例详细信息**按钮：

a) 更改**网络**，以匹配先前创建的 VPC。

b) 更改**子网**，以匹配先前创建的管理子网。您可以指定 IP 地址或使用自动生成。

c) 在**高级详细信息**下方，添加默认的登录信息。

修改以下示例，以满足设备名称和密码要求。

示例配置：

```
#FMC
{
"AdminPassword": "<enter_your_password>",
"Hostname": "<Hostname-vFMC>"
}
```

注意 在**高级详细信息**字段输入数据时，请使用纯文本。如果从文本编辑器复制此信息，请确保仅以纯文本形式复制。如果将任何 Unicode 数据（包括空格）复制到**高级详细信息**字段，可能会造成实例损坏，然后您必须终止此实例并重新创建实例。

步骤 8 点击**下一步：添加存储**，以配置存储设备设置。

编辑根卷设置，使得卷大小 (GiB) 为 250 GiB。不支持卷大小低于 250 GiB，否则会限制事件存储。

步骤 9 点击**下一步：标记实例**。

标签由区分大小写的键值对组成。例如，您可以按照“**Key** = 名称”和“**Value** = 管理”的格式定义标签。

步骤 10 选择**下一步：配置安全组**。

步骤 11 点击**选择现有安全组**并选择先前配置的安全组，或创建新的安全组；有关创建安全组的详细信息，请参阅 AWS 文档。

步骤 12 点击**检查和启动**。

步骤 13 点击**启动**。

步骤 14 选择现有的密钥对或创建新的密钥对。

注释 您可以选择现有的密钥对或者创建新的密钥对。密钥对由 AWS 存储的一个公共密钥和用户存储的一个专用密钥文件组成。两者共同确保安全连接到实例。请务必将密钥对保存到已知位置，以备连接到实例之需。

步骤 15 点击**启动实例**。

步骤 16 点击**EC2 控制面板** > **弹性 IP**，找到之前分配的 IP 地址，或分配一个新地址。

步骤 17 选择弹性 IP 地址，右键单击并选择**关联地址**。

找到要选择的实例或网络接口，然后点击“关联”。

步骤 18 点击**EC2 控制面板** > **实例**。

步骤 19 几分钟后，FMCv 实例状态将显示为"运行"，状态检查中"2/2 检查"将显示为通过。但是，部署和初始设置过程大约需要花费 30 到 40 分钟。要查看实例状态，右键单击此实例，然后选择实例**设置** > **获取实例屏幕截图**。

设置完成后（大约 30 到 40 分钟后），**实例屏幕截图**应显示一条类似于“Cisco Firepower Management Center for AWS vW.X.Y (build ZZ)”的消息，后面可能跟着一些其他的输出行。

然后您应该能够通过 SSH 或 HTTPS 登录到新创建的 FMCv。实际部署时间可能有所差异，具体取决于您所在地区的 AWS 负载。

您可以通过 SSH 访问 FMCv：

```
ssh -i <key_pair>.pem admin@<Public_Elastic_IP>
```

SSH 身份验证由密钥对处理。不需要密码。如果系统提示您输入密码，则表明设置仍在运行。

您还可以通过 HTTPS 访问 FMCv：

```
https//<Public_Elastic_IP>
```

注释 如果看到“系统启动进程仍在运行”消息，则表明设置尚未完成。

如果未得到 SSH 或 HTTPS 响应，请检查以下项目：

- 确保部署已完成。FMCv VM 实例屏幕截图应显示一条类似于“适CiscoFirepower Management Center for AWS vW.X.Y (build ZZ)”的消息，后面可能跟着一些其他的输出行。
- 确保拥有弹性 IP 地址，已将该地址关联 Firepower 管理中心的管理网络接口 (eni)，并且正连接到该 IP 地址。
- 确保 VPC 已关联互联网网关 (igw)。
- 确保管理子网已关联路由表。
- 确保管理子网关联的路由表具有指向互联网网关 (igw) 的路由（目的地址为“0.0.0.0/0”）。

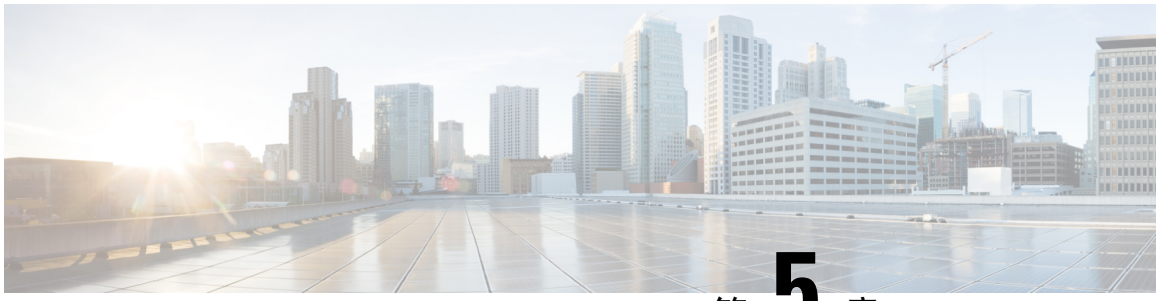
- 确保安全组允许传入连接所用 IP 地址产生的 SSH 和/或 HTTPS 流量。

下一步做什么

配置策略和设备设置

安装虚拟 Firepower 威胁防御并将设备添加到管理中心后，您可以使用 Firepower 管理中心用户界面为 AWS 上运行的虚拟 Firepower 威胁防御配置设备管理设置，还可以使用该界面配置并应用访问控制策略和其他相关策略，以利用虚拟Firepower威胁防御设备管理流量。安全策略可控制虚拟Firepower威胁防御提供的服务（例如下一代 IPS 过滤和应用过滤）。您可以通过 Firepower 管理中心在虚拟 Firepower 威胁防御上配置安全策略。有关如何配置安全策略的详细信息，请参阅《Firepower 配置指南》或 Firepower 管理中心中的在线帮助。

-



第 5 章

虚拟 Firepower 管理中心 初始设置

本章描述部署虚拟 Firepower 管理中心 (FMCv) 设备之后，需要执行的初始设置过程。

初始设置概述

部署虚拟 Firepower 管理中心 (FMCv) 后，必须通过设置过程完成对新设备的配置，以便新设备能够在可信管理网络上通信。您还必须执行管理级别的初始任务，例如更改管理员密码、接受《最终用户许可协议》(EULA)、设置时间以及制定更新计划。设置和注册过程中所选择的选项决定系统将要创建并应用到受管设备的默认接口、内联集、区域和策略。

在某些部署场景中，您可以预定义 Firepower 系统所需的设置（例如管理员账户的密码，使设备能在管理网络上通信的设置等）。这些包括在 VMware 上使用 VI OVF 模板的部署以及在 KVM 上使用 Day 0 配置文件的部署。

如果在 VMware 上使用 ESXi OVF 模板部署，或在 KVM 上未使用 Day 0 配置文件部署，设置 FMCv 分为两步。初始化 FMCv 后，在设备控制台运行设备配置脚本，从而使设备可在管理网络上通信。然后，使用管理网络上的计算机访问 FMCv 的 Web 界面，完成设置过程。

使用脚本配置网络设置

新的 FMCv 设备初始化以后，您必须配置可使设备在管理网络上通信的设置。通过在设备控制台运行脚本完成该步骤。

Firepower 系统为 IPv4 和 IPv6 管理环境提供了双堆栈实施。首先，脚本提示您配置（或禁用）IPv4 管理设置，然后配置（或禁用）IPv6 管理设置。对于 IPv6 部署，您可以从本地路由器检索设置。

必须提供 IPv4 或 IPv6 管理 IP 地址、网络掩码或前缀长度以及默认网关。按照脚本提示操作时，如遇单选问题，选项会在小括号内列出，例如 (y/n)。默认值会列在方括号内，例如 [y]。按 **Enter** 键确认选择。

开始之前

- 确保 FMCv 设备 VM 完成初始化和启动过程。

步骤 1 在设备控制台使用管理员账户（用户名：**admin**，密码：**Admin123**）登录到 FMCv。注意密码区分大小写。

注释 如果在初始部署期间更改密码，则输入部署 FMCv 时指定的密码。

步骤 2 在管理员提示符下，运行以下脚本：

示例：

```
sudo /usr/local/sf/bin/configure-network
```

第一次连接到 FMCv 时，系统会提示您执行启动后配置。

步骤 3 按脚本提示执行操作。

回答系统的提示问题，以便为设备提供 IPv4 和 IPv6（可选）配置信息。

步骤 4 最后的提示会让您确认设置。

示例：

```
Are these settings correct: (y or n)?
```

检查输入的设置。

- 如果设置正确，输入 **y**，然后按 **Enter**键接受设置并继续。
- 如果设置不正确，输入 **n**，然后按 **Enter**键。系统将提示重新输入信息。

步骤 5 在接受设置后，输入 **logout** 可退出。

下一步做什么

- 继续执行初始设置；请参阅执行虚拟 Firepower 管理中心初始设置 ，第 38 页。

执行虚拟 Firepower 管理中心初始设置

对于所有的 FMCv，您必须通过登录 FMCv 的网络界面并在设置页面指定初始配置选项来完成设置流程。必须至少更改管理员密码，指定网络设置（若尚未指定），并接受 EULA。

步骤 1 通过浏览器访问 https://*mgmt_ip*/，其中 *mgmt_ip* 是在部署 VM 时分配给 FMCv 管理接口的 IP 地址（或主机名）。

随即显示登录页面。

步骤 2 使用用户名 **admin** 以及部署 VM 时指定的管理员账户密码登录设备。如果部署期间未更改密码，使用 **Admin123** 作为密码。

系统将显示设置页面。有关完成设置的详细信息，请参阅以下各节：

步骤 3 在“设置”页面的**更改密码**部分，更改管理员账户的密码。Web界面的管理员账户具有管理员特权，无法删除。建议使用强密码，其中应至少包含8个大小写混合的字母数字字符和至少一个数字字符。应避免使用词典中的单词。

注释 通过外壳访问 FMCv 的管理员账户与使用 Web 界面访问 FMCv 的管理员账户并不相同，两者可能使用不同的密码。此设置将两个管理员密码都更改为相同的值。

步骤 4 FMCv 的网络设置使其能够在管理网络上通信。在“设置”页面的**网络设置**部分配置以下设置：

- 如果在部署 VM 时已配置设备访问所需的网络设置，“设置”页面的**网络设置**部分可能已预填充。
- 如果设置值未在**网络设置**部分预填充，或想要更改预填充的值，则必须选择管理网络协议。Firepower 系统为 IPv4 和 IPv6 管理环境提供了双堆栈实施；您可以指定 IPv4 或IPv6，或同时指定两者。

  根据您的协议选择，“设置”页面将显示多种字段，其中您必须设置 FMC 的 IPv4 或 IPv6 管理 IP 地址、网络掩码或前缀长度以及默认网关：还可以指定最多三个 DNS 服务器以及设备的主机名和域。

  - 对于 IPv4，必须以点分十进制格式输入地址和网络掩码（例如：网络掩码 255.255.0.0）。
  - 对于 IPv6 网络，选择**使用路由器自动配置分配 IPv6 地址** 复选框，自动分配 IPv6 网络设置。否则，必须以冒号隔开的十六进制格式设置地址和前缀的位数（例如：前缀长度为 112）。

步骤 5 （可选）在“设置”页面的**时间设置**部分，您可以通过两种方式设置 FMCv 时间：手动设置或通过网络时间协议 (NTP) 从 NTP 服务器接收时间。

- 要使用网络时间协议 (NTP) 设置时间，选中**通过 NTP 从服务器接收**，并指定 FMCv 可以访问的 NTP 服务器。
- 要手动设置时间，选中**手动**，并在显示的字段中输入当前时间。

要为管理员账户选择本地 Web 界面上使用的时区，点击当前时区值，并从弹出窗口中选择时区。

重要事项 思科建议使用物理 NTP 服务器设置时间。

步骤 6 （可选）如果计划在部署中执行入侵检测和预防，建议在“设置”页面的**周期性规则更新导入**部分，选中**启用从支持网站导入周期性规则更新**。

可以指定**导入频率**并配置系统，使系统在每项规则更新后执行入侵**策略部署**。要在初始配置过程中执行规则更新，请选中**立即安装**。

随着新的漏洞为大家所知，漏洞研究团队 (VRT) 发布了入侵规则更新。规则更新提供新的和更新后的入侵规则和预处理器规则、现有规则的修改后状态以及修改后的默认入侵策略设置。规则更新也可以删除规则并提供新规则类别和系统变量。

规则更新可能包含新的二进制文件。请确保下载和安装规则更新的过程符合安全策略。此外，规则更新内容可能很多，因此，请确保在网络使用量较低的时段导入规则。

步骤 7 （可选）如果计划在部署中执行地理位置相关的分析，建议在“设置”页面的**周期性地理位置更新**部分，选中**启用从支持站点获取周期性每周更新**，并通过相应字段指定**更新开始时间**。要在初始配置过程中执行GeoDB更新，请选中**立即安装**。

GeoDB 的更新内容可能很多，下载后的安装过程可能需要长达 45 分钟。应在网络使用量较低的时段更新 GeoDB。

FMCv可显示与系统生成的事件相关的路由 IP 地址的地理信息，并监控控制面板和 Context Explorer 中的地理位置统计信息。FMC 的地理位置数据库 (GeoDB) 包含用于支持此功能的各种信息，如 IP 地址相关的 ISP、连接类型、代理信息和准确位置。启用定期 GeoDB 更新可确保系统使用最新的地理位置信息。

步骤 8 （可选）在“设置”页面的**自动备份**部分，可以选中**启用自动备份**创建计划任务，从而每周在 FMCv 上创建配置备份，出现故障的情况下可以恢复备份数据。

步骤 9 您可使用 FMCv 为其管理的设备管理许可证。Firepower 系统提供的许可证类型取决于要管理的设备类型：

- 对于 7000 和 8000 系列、具备 FirePOWER 服务的 ASA 和 NGIPSv 设备，必须使用经典许可证。使用经典许可证的设备有时也称为经典设备。

  只有在受管设备上启用经典许可证，才能使用许可的功能。可以在 FMCv 的初始设置期间或将设备添加到 FMCv 时启用许可证，或者在添加设备后通过编辑设备的常规属性来启用许可证。

  如果计划管理使用经典许可证的设备，请参阅 Firepower 管理中心配置指南中的“适用于 Firepower 系统的经典许可”。

- 对于 FTD 物理和虚拟设备，必须使用智能许可证。

  如果计划管理使用思科智能软件许可的设备，有关添加智能许可证到 FMCv 的详细信息，请参阅相应设备的产品文档。

Firepower 管理中心配置指南提供有关经典许可证和智能许可证、各类许可证的类型以及如何在部署中管理许可证的详细信息。

步骤 10 请仔细阅读**最终用户许可协议**；如果同意遵守协议规定，则选中**我已阅读并同意最终用户许可协议**。

步骤 11 确保提供的所有信息都正确无误后，请点击**应用**。

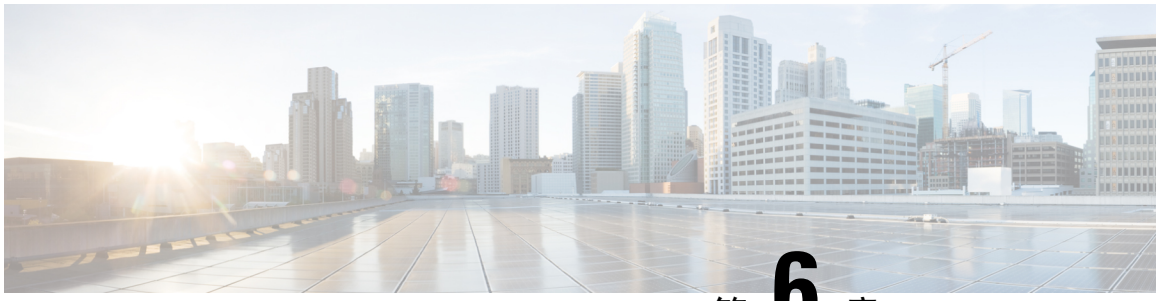
FMCv根据选择应用配置，显示“摘要控制面板”页面，并使您作为管理员用户（具有管理员角色）登录到Web界面。FMCv 加载摘要控制面板可能需要几分钟。

步骤 12 在管理网络内的计算机上打开浏览器，通过刚配置的 IP 地址或主机名访问 FMCv GUI，以完成本指南中的剩余步骤。

步骤 13 通过监控消息中心中的**任务**选项卡，验证初始设置成功。

下一步做什么

- 执行虚拟 Firepower 管理中心初始管理和配置，第 41 页中所述的活动。



第 6 章

虚拟 Firepower 管理中心初始管理和配置

在完成虚拟 Firepower 管理中心 (FMCv) 的初始设置过程并验证其成功后，建议完成各种管理任务，以使部署更易于管理。此外，还应该完成在初始设置过程中跳过的所有任务，例如许可。有关以下各部分中描述的任何任务的详细信息，以及有关如何开始配置部署的信息，请参阅适用于相应设备版本的完整 Firepower 管理中心配置指南。

单个用户账户

完成初始设置后，系统上的唯一 Web 界面用户是管理员用户，此用户具备管理员角色和访问权限。管理员角色用户具有对系统的完整菜单和配置访问权限。建议限制使用管理员账户（和管理员角色），以保障安全，便于审计。在 FMC GUI 的**系统** > **用户** > **用户**页面管理用户账户。

注释 通过外壳访问 FMC 的管理员账户与使用 Web 界面访问 FMC 的管理员账户并不相同，两者可能使用不同的密码。

为使用系统的每个人创建独立账户，不仅可以让公司审计每个用户所做的操作和更改，还能限制每个人的相关用户访问角色。这点对于FMC来说尤其重要，因为您需要在其中执行大多数的配置和分析任务。例如，分析师需要访问事件数据来分析网络的安全性，但不需要访问用于部署的管理功能。

系统包含 10 个专为使用 Web 界面的各种管理员和分析师设计的预定义用户角色。还可以创建具有专用访问权限的自定义用户角色。

设备注册

FMC 可以管理 Firepower 当前支持的任何物理或虚拟设备：

- Firepower 威胁防御- 提供统一的下一代防火墙和下一代 IPS 设备。

- Firepower 威胁防御虚拟- 可运行于多种虚拟机监控程序环境、旨在减少管理开销并提高运营效率的 64 位虚拟设备。
- 思科具备 FirePOWER 服务的 ASA（或 ASA FirePOWER 模块）- 提供最重要的系统策略，并将流量传递到 FirePOWER 系统进行发现和访问控制。但是无法使用 FMC 的 Web 界面来配置 ASA FirePOWER 接口。思科具备 FirePOWER 服务的 ASA提供 ASA 平台特有的软件和 CLI，可以用于安装系统以及执行平台特定的其他管理任务。
- 7000 和 8000 系列设备 - 专为 Firepower 系统打造的专用物理设备。7000 和 8000 系列设备吞吐量各异，但是大部分功能都相同。一般来说，8000 系列设备比 7000 系列设备功能更强大；它们还支持其他功能，如 8000 系列快速路径规则、链路汇聚和堆叠。在将设备注册至 FMC 之前，必须在设备上配置远程管理。
- NGIPSv - 在 VMware VSphere 环境中部署的 64 位虚拟设备。NGIPSv 设备不支持系统任何基于硬件的功能，如冗余和资源共享、交换和路由等。

要注册受管设备到 FMC，使用 FMC GUI 的**设备** > **设备管理**页面；请参阅Firepower 管理中心配置指南中的设备管理信息。

运行状况和系统策略

默认情况下，所有设备都应用了初始系统策略。系统策略管理同一部署中多台设备可能使用的相似设置，例如邮件中继主机首选项和时间同步设置。建议使用 FMC 将同一系统策略应用到管理中心本身以及它管理的所有设备上。

默认情况下，FMC还应用了运行状况策略。作为运行状况监控功能的一部分，运行状况策略为系统提供了用以持续监控部署中设备的性能的标准。建议使用 FMC 将运行状况策略应用到其管理的所有设备上。

软件和数据库更新

在开始任何部署之前，应更新设备上的系统软件。建议部署的所有设备都运行 Firepower 系统的最新版本。如果您正在部署中使用这些设备，还应当安装最新的入侵规则更新、VDB 和 GeoDB。

⚠

注意 在更新 Firepower 系统的任何部分之前，必须阅读随更新提供的版本说明或建议文本。版本说明提供重要信息，包括支持的平台、兼容性、先决条件、警告以及具体安装和卸载说明。