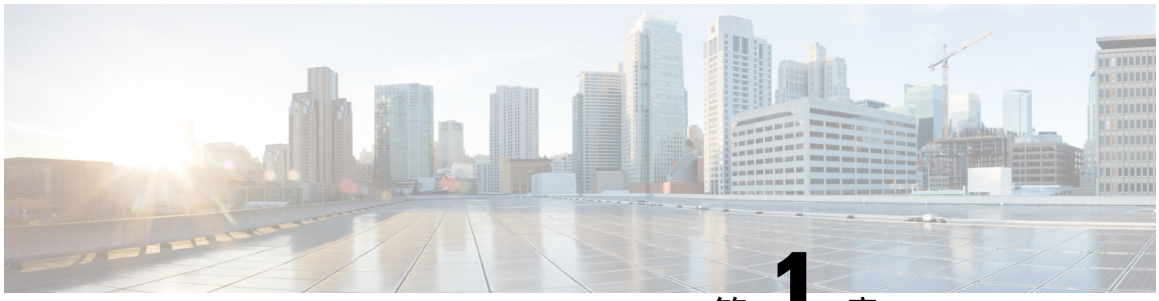
《思科 Firepower Management Center Virtual 快速入门指南》

首次发布日期: 2015 年 11 月 10 日

上次修改日期: 2021 年 6 月 25 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

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。

FMCv 平台和支持

内存和资源要求

为确保最优性能，每个 FMCv 实例在目标平台上具有最低资源分配要求：内存、CPU 数和磁盘空间。

重要事项 升级 FMCv 时，请查看最新的 Firepower 发行说明，详细了解新版本是否会影响您的环境。您可能需要增加资源才能部署最新版本的 Firepower。

升级 Firepower 时，您可以添加最新的功能和修复补丁，以帮助提高 Firepower 部署的安全功能和性能。

FMCv 需要 28 GB RAM 用于升级 (6.6.0+)

FMCv 平台在升级期间引入了新的内存检查。如果为虚拟设备分配的 RAM 少于 28 GB，FMCv 升级到 6.6.0+ 版本时将会失败。

重要事项 我们建议您不要降低默认设置：为大多数 FMCv 实例分配 32 GB RAM，为 FMCv 300 分配 64 GB。为了提高性能，您总是可以根据可用的资源来增加虚拟设备的内存和 CPU 数量。

由于此内存检查，我们将无法在支持的平台上支持较低内存实例。有关重要的 FMCv 升级信息，请参阅关于虚拟设备性能，第 3 页。

FMCv 初始设置 (6.5.0+)

从版本 6.5 开始，FMCv 改进了初始设置体验，其中包括以下更改和增强：

- **管理上的 DHCP** — 在管理接口 (eth0) 上，DHCP 在默认模式下启用。

  FMCv 管理接口已预配置为接受 DHCP 分配的 IP4 地址。咨询您的系统管理员，确定您的 DHCP 已配置为分配给 FMCv 的 IP 地址。在没有可用 DHCP 的情况下，FMC 管理接口使用 IPv4 地址 192.168.45.45。

- **Web 界面 URL** — FMCv Web 界面的默认 URL 已更改为 *https://<FMC-IP>:*<端口>*/ui/login*。
- **密码重置** — 要确保系统安全和隐私，首次登录 FMC 时，您需要更改**管理员**密码。当出现“更改密码”(Change Password) 向导屏幕时，您有两个选项：在**新密码 (New Password)**和**确认密码 (Confirm Password)**文本框中输入新密码。密码必须符合对话框中列出的条件。
- **网络设置** — FMCv 现在包含一个安装向导，用于完成初始设置：
  - **完全限定域名** — 接受默认值（如果显示），或者输入完全限定域名（语法 <主机名>. <域>）或主机名。
  - **用于 IPV4 连接的引导协议** — 选择 DHCP 或静态/手动作为 IP 地址分配方法。
  - **DNS 组** — FMCv 的默认域名服务器组是 Cisco Umbrella DNS。
  - **NTP 组服务器** — 默认网络时间协议组设置为 Sourcefire NTP 池。
- **RAM 要求** — 建议的 RAM 大小为 FMCV 的 32GB。
- **FMCv-300 for VMware** — 新的可扩展 FMCv 映像可在支持管理多达 300 设备的 VMware 平台上使用，具有更高的磁盘容量。

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。
- **Microsoft Azure** - 您可以在 Azure 云中部署虚拟 Firepower 管理中心。

注释 高可用性 (HA) 配置仅在 VMWare 上的 Firepower 管理中心虚拟部署上支持；有关高可用性的系统要求信息，请参阅《Firepower 管理中心配置指南》中的关于 *Firepower* 管理中心高可用性。

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 Cisco 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 2 台、10 台、25 台或 300 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 Cisco 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。

FMCv 默认和最低内存要求

所有 FMCv 实施现在具有相同的 RAM 要求：建议 32 GB，需要 28 GB（FMCv 300 需要 64 GB）。如果为虚拟设备分配的 RAM 少于 28 GB，升级到 6.6.0+ 版本时将会失败。升级后，如果您降低内存分配，运行状况监视器将会告警。

这些新的内存要求在所有虚拟环境之间实施统一的要求，可以提高性能，使您能够利用各种新功能特性。我们建议不要降低默认设置。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。

重要事项 从版本 6.6.0 开始，基于云的 FMCv 部署（AWS、Azure）低内存实例类型已被完全弃用。您不能使用它们建新的 FMCv 实例，即使是早期 Firepower 版本也不例外。您可以继续运行现有实例。

下表汇总了低内存 FMCv 部署的升级前要求。

表 *1:* 版本 *6.6.0+* 升级的 *FMCv* 内存要求

平台	升级前操作	详细信息
VMware	分配 28 GB 最低值/32 GB 建议值。	先关闭虚拟机的电源。 有关说明，请参阅 VMware 文档。
KVM	分配 28 GB 最低值/32 GB 建议值。	有关说明，请参阅 KVM 环境对应的文档。

平台	升级前操作	详细信息
AWS	调整实例大小： • 从 c3.xlarge 到 c3.4xlarge。 • 从 c3.2.xlarge 到 c3.4xlarge。 • 从 c4.xlarge 到 c4.4xlarge。 • 从 c4.2xlarge 到 c4.4xlarge。 我们还提供用于新部署的 c5.4xlarge 实例。	在调整大小之前停止实例。请注意，当您执行此操作时，实例存储卷上的数据将丢失，因此请先迁移实例存储支持的实例。此外，如果您的管理接口没有弹性 IP 地址，将释放其公共 IP 地址。 有关说明，请参阅 Linux 实例 AWS 用户指南中有关更改实例类型的文档。
Azure	调整实例大小： • 从 Standard_D3_v2 到 Standard_D4_v2。	使用 Azure 门户或 PowerShell。您无需在调整大小之前停止实例，但停止可能会显示额外的大小。调整大小将重新启动正在运行的虚拟机。 有关说明，请参阅有关调整 Windows 虚拟机大小的 Azure 文档。

下载Firepower Management Center Virtual部署软件包

您可以从 Cisco.com 下载Firepower Management Center Virtual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Firepower Management Center Virtual部署软件包，请执行以下步骤：

步骤 1 导航至思科软件下载 (Software Download) 页面。

注释 需要 Cisco.com 登录信息和思科服务合同。

步骤 2 单击**浏览全部 (Browse all)** 以搜索Firepower Management Center Virtual部署软件包。

步骤 3 选择 **安全 (Security)** > **防火墙 (Firewalls)** > **防火墙管理 (Firewall Management)**，然后选择 **虚拟 Firepower 管理中心设备 (Firepower Management Center Virtual Appliance)**。

步骤 4 选择型号 > **FireSIGHT 系统软件 (FireSIGHT System Software)** > 版本。

下表列出 Cisco.com 上提供的Firepower Management Center Virtual软件的命名约定及相关信息。

型号	软件包类型	软件包名称
Firepower Management Center Virtual	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。
	Firepower 软件安装：Azure	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。

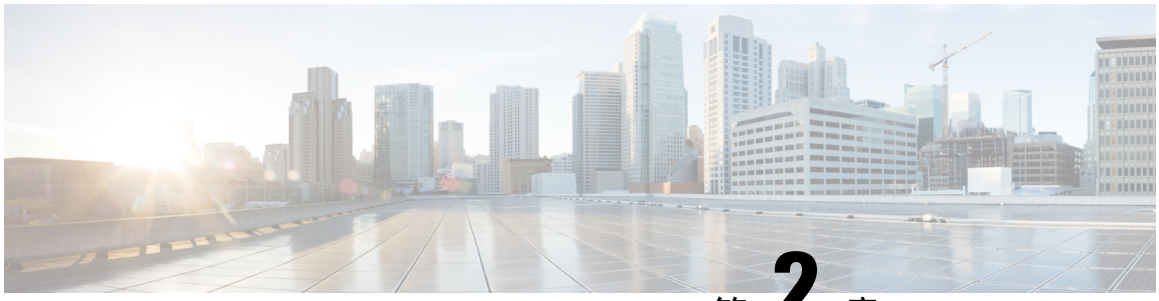
许多软件包名称类似，因此请确保下载正确的软件包。

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Firepower Management Center Virtual，第 7 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 19 页。
- 要在 AWS 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 31 页。
- 要在 Azure 中部署虚拟 Firepower 管理中心，请参阅在 Microsoft Azure 云上部署虚拟 Firepower 管理中心，第 43 页。



第 2 章

使用 VMware 部署Firepower Management Center Virtual

您可以使用 VMware 部署Firepower Management Center Virtual (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

特性	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。	否	FMC 与受管设备之间存在不同步风险。请参阅 快照支持， 第 12 页 .
暂停和恢复	VM 暂停，然后恢复。	是	–

特性	说明	支持（是/否）	备注
vCloud Director	允许自动部署 VM。	否	–
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 12 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

FMCv 需要 28 GB RAM 用于升级 (6.6.0+)

FMCv 平台在升级期间引入了新的内存检查。如果为虚拟设备分配的 RAM 少于 28 GB，FMCv 升级到 6.6.0+ 版本时将会失败。

重要事项 我们建议您不要降低默认设置：为大多数 FMCv 实例分配 32 GB RAM，为 FMCv 300 分配 64 GB。为了提高性能，您总是可以根据可用的资源来增加虚拟设备的内存和 CPU 数量。

由于此内存检查，我们将无法在支持的平台上支持较低内存实例。

内存和资源要求

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Firepower Management Center Virtual。有关虚拟机监控程序兼容性的信息，请参阅 Cisco Firepower 兼容性指南。

重要事项 升级 FMCv 时，请查看最新的 Firepower 发行说明，详细了解新版本是否会影响您的环境。您可能需要增加资源才能部署最新版本的 Firepower。

升级 Firepower 时，您可以添加最新的功能和修复补丁，以帮助提高 Firepower 部署的安全功能和性能。

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。

下表列出 FMCv 设备的建议设置和默认设置。

重要事项 请务必分配足够的内存，以确保的最佳性能FMCv。如果FMCv的内存少于32 GB，则系统可能会遇到策略部署问题。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。默认设置是运行系统软件的最低要求，不能降低。

表 *3: FMCv* 虚拟设备设置

设置	最小	默认	建议	设置可调节？
内存	28 GB	32 GB	32 GB	有限制。 **重要事项** FMCv平台在升级期间引入了新的内存检查。如果为虚拟设备分配的 RAM 少于 28 GB，FMCv 升级到 6.6.0+ 版本时将会失败。
虚拟 CPU	4	4	8	是，最多 8 个
硬盘调配容量	250 GB	250 GB	不适用	否，取决于所选磁盘格式

表 *4: FMCv300* 虚拟设备设置

设置	默认	设置可调节？
内存	64 GB	是
虚拟 CPU	32	否
硬盘调配容量	2.2 TB	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*。

FMCv 和 VMware 的准则和限制

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 模板进行部署，则在安装过程中，您可以执行 FMCv 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 *5: 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	确认您要安装的设备 (FMCv) 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。
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 (Storage)	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 (Disk Format)	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。

时间与时间同步

使用网络时间协议 (NTP) 服务器同步 FMCv 和受管设备上的系统时间。通常在 FMCv 初始配置期间指定 NTP 服务器；有关默认 NTP 服务器的信息，请参阅Firepower Management Center Virtual 初始设置，第 97 页。

要使 Firepower 系统成功运行，必须在 FMCv及其受管设备上同步系统时间。在 VMware ESXi 服务器上配置 NTP 以匹配 FMCv 的 NTP 设置时，您可以执行额外的步骤以确保时间同步。

您可以使用 vSphere Client 在 ESXi 主机上配置 NTP。有关具体说明，请参考 VMware 文档。此外，VMware KB 2012069 介绍了如何使用 vSphere Client 在 ESX/ESXi 主机上配置 NTP。

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 FMCv 移至其他主机，使用本地存储会造成错误。

快照支持

VMware 快照是虚拟机的磁盘文件 (VMDK) 在给定时间点的副本。快照为虚拟磁盘提供更改日志，可用于在发生故障或系统错误时将 VM 恢复到特定的时间点。快照自身不提供备份，不应将其用作备份。

如果需要配置备份，请使用 Firepower Management Center 的备份和恢复功能（**系统** > **工具** > **备份/恢复**）。

ESXi 上的 VMware 快照功能可能会耗尽 VM 存储容量，影响 FMC 虚拟设备的性能。请参阅以下 VMware 知识文库文章：

- 在 vSphere 环境中使用快照的最佳实践（VMware KB 1025279）。
- 了解 ESXi 中的 VM 快照（VMware KB 1015180）。

高可用性 (HA) 支持

您可以在 VMware ESXi 上的两个 FMCv 虚拟设备之间建立高可用性 (HA)。

- 两种 FMCv 型号均支持 FMCv HA：FMCv 和 FMCv 300。
- 高可用性配置中的两个 FMCv 虚拟设备型号必须相同。不能将 FMCv 与 FMCv 300 配对。
- 要建立 FMCv HA，FMCv 需要为其在 HA 配置中管理的每个 FTD 设备额外提供 Firepower 管理中心虚拟 (MCv) 许可证授权。但是，无论 FMCv HA 配置如何，每个 FTD 设备所需的 FTD 功能许可证授权都没有变化。有关许可的指南，请参阅《Firepower管理中心配置指南》中的高可用性对中 *FTD* 设备的许可证要求。
- 如果分开 FMCv HA 对，则会释放额外的 Firepower 管理中心虚拟 (MCv) 许可证授权，并且每个 FTD 设备只需要一个授权。

有关高可用性的指南，请参阅《Firepower 管理中心配置指南》中的建立 *Firepower* 管理中心高可用性。

INIT 重生错误消息现象

您可能会在运行 ESXi 6 或 ESXi 6.5 的 FMCv 控制台上看到以下错误消息：

```
"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. 右键单击虚拟机，然后选择**编辑设置 (Edit Settings)**。
2. 在虚拟硬件选项卡中，从**新设备 (New device)** 下拉菜单中选择**串行端口 (Serial port)**，然后单击**添加 (Add)**。

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

   单击**确定 (OK)** 保存设置。

限制

针对 Vmware 进行部署时，有以下限制：

- FMCv 设备没有序列号。**系统 (System)** > **配置 (Configuration)**页面将会显示**无 (None)** 或**未指定 (Not Specified)**，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。
- 不支持无法识别 OVF 封装的 VMware 工作站、播放器、服务器和 Fusion。

配置 VMXNET3 接口

重要事项

从 6.4 版本开始，当您创建虚拟设备时，VMware 上的 FTDv 和 FMCv 默认为 vmxnet3 接口。先前，默认值为 e1000。如果您使用的是 e1000 接口，我们**强烈建议**您切换。vmxnet3 设备驱动器和网络处理与 ESXi 虚拟机监控程序集成，因此其使用更少的资源并提供更好的网络性能。

要将 e1000 接口更改为 vmxnet3，必须删除所有接口，然后使用 vmxnet3 驱动程序重新安装。

虽然可以在部署中混合使用不同类型的接口（例如在虚拟 Firepower 管理中心上使用 e1000 接口，在受管虚拟设备上使用 vmxnet3 接口），但不能在同一虚拟设备中混合使用不同类型的接口。虚拟设备上的所有传感接口和管理接口必须为相同类型。

步骤 1 断开 FTDv 或 FMCv 虚拟机电源。

要更改接口，必须关闭设备电源。

步骤 2 右键单击清单中的 FTDv 或 FMCv 虚拟机，然后选择**编辑设置 (Edit Settings)**。

步骤 3 选择适用的网络适配器，然后选择**删除 (Remove)**。

步骤 4 单击**添加 (Add)** 以打开**添加硬件向导 (Add Hardware Wizard)**。

步骤 5 选择**以太网适配器 (Ethernet adapter)**，然后单击**下一步 (Next)**。

步骤 6 选择 vmxnet3 适配器，然后选择网络标签。

步骤 7 对 FTDv 上的所有接口重复上述操作。

下一步做什么

- 从 VMware 控制台接通 FTDv 或 FMCv 电源。

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 (Software Download) 页面。

注释 需要 Cisco.com 登录信息和思科服务合同。

步骤 2 单击**浏览全部 (Browse all)** 以搜索虚拟 Firepower 管理中心部署软件包。

步骤 3 选择 **安全 (Security)** > **防火墙 (Firewalls)** > **防火墙管理 (Firewall Management)**，然后选择 **虚拟 Firepower 管理中心设备 (Firepower Management Center Virtual Appliance)**。

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 单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 15 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，单击**下一步 (Next)** 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 (File)** > **部署 OVF 模板 (Deploy OVF Template)**。

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 (OVF Template Details)** 页面，然后单击**下一步 (Next)**。

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单击**下一步 (Next)**。

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，然后单击**下一步 (Next)**。

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，然后单击“下一步”(Next)。

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，然后单击**下一步 (Next)**。

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，然后单击**下一步 (Next)**。

在此页面上，您可以从目标集群或主机上已配置的数据存储中选择。虚拟机配置文件和虚拟磁盘文件均存储在 Datastore 上。选择一个足够大的数据存储，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，然后单击**下一步 (Next)**。

如果选择**密集调配 (Thick Provisioned)**，则会立即分配所有存储。如果选择**精简调配 (Thin Provisioned)**，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，然后单击**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，然后单击**下一步 (Next)**。

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 (Power on after deployment)** 选项启动虚拟 Firepower 管理中心，然后单击**完成 (Finish)**。

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 **Global Information** 区域的 **Recent Tasks** 窗格中看到“初始化 OVF 部署”状态。

完成后，您会看到 Deploy OVF Template 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 17 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 (Edit Settings)**，或在主窗口的**开始 (Getting Started)**选项卡中单击**编辑虚拟机设置 (Edit virtual machine settings)**。

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 (Provisioned Size)**，请点击**硬盘 1 (Hard disk 1)**。

步骤 3 或者，通过单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 单击**确定 (OK)**。

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 17 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 *Cisco 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。

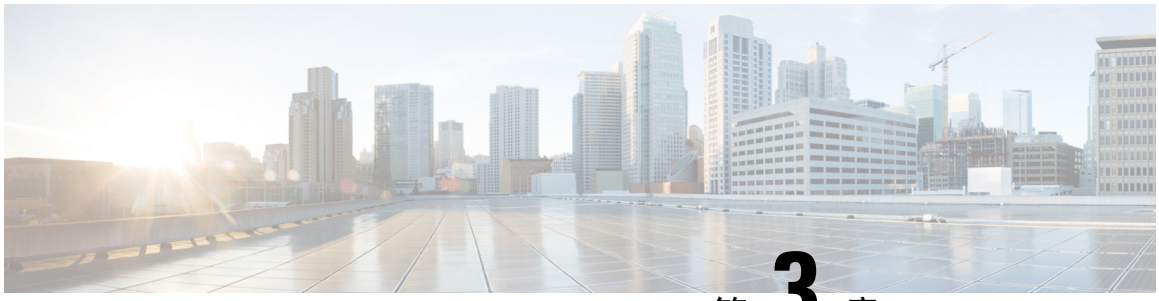
在 vSphere 客户端中，右键单击库存清单中虚拟设备的名称，然后从上下文菜单中选择**电源 (Power)** > **打开电源 (Power On)**。

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Firepower Management Center Virtual 初始设置，第 97 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 105 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）。

FMCv 需要 28 GB RAM 用于升级 (6.6.0+)

FMCv 平台在升级期间引入了新的内存检查。如果为虚拟设备分配的 RAM 少于 28 GB，FMCv 升级到 6.6.0+ 版本时将会失败。

重要事项 我们建议您不要降低默认设置：为大多数 FMCv 实例分配 32 GB RAM，为 FMCv 300 分配 64 GB。为了提高性能，您总是可以根据可用的资源来增加虚拟设备的内存和 CPU 数量。

由于此内存检查，我们将无法在支持的平台上支持较低内存实例。

内存和资源要求

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。有关虚拟机监控程序兼容性的信息，请参阅 Cisco Firepower 兼容性指南。

重要事项 升级 FMCv 时，请查看最新的 Firepower 发行说明，详细了解新版本是否会影响您的环境。您可能需要增加资源才能部署最新版本的 Firepower。

升级 Firepower 时，您可以添加最新的功能和修复补丁，以帮助提高 Firepower 部署的安全功能和性能。

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。

下面列出了 KVM 上 FMCv 设备的建议设置和默认设置：

- 处理器
  - 需要 4 个 vCPU
- 内存
  - 最低要求 28 GB RAM/建议（默认）32 GB RAM

  重要事项 FMCv 平台在升级期间引入了新的内存检查。如果为虚拟设备分配的 RAM 少于 28 GB，FMCv 升级到 6.6.0+ 版本时将会失败。
- 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。

- 为了在本文档中提供示例部署，我们假设您使用 Ubuntu 18.04 LTS。在 Ubuntu 18.04 LTS 主机之上安装以下软件包：
  - 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 18.04 LTS 的有用优化包括以下各项：
  - 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 - 增加内存页面大小，在 Ubuntu 18.04 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 的分布的信息，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 (System)** > **配置 (Configuration)**页面将会显示**无 (None)**或**未指定 (Not Specified)**，具体取决于虚拟平台。
- 不支持嵌套虚拟机管理程序（运行在 VMware/ESXi 上的 KVM）。只支持裸机 KVM 部署。
- 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 28 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。

- 将两个 DNS 条目留空，以使用默认 Cisco Umbrella DNS 服务器。要在非 DNS 环境中运行，请将两个条目都设置为“无”（不区分大小写）。

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": "10.1.1.5",
    "DNS2": "192.168.1.67",

    "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 25 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 23 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 25 页。
- 使用 OpenStack - 使用 OpenStack 环境启动 FMCv；请参阅使用 OpenStack 启动，第 26 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 \
    --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 单击左上角的按钮，打开**新建虚拟机 (New VM)** 向导。

步骤 3 输入虚拟机的详细信息：

a) 对于操作系统，选择**导入现有的磁盘映像 (Import existing disk image)**。

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）。

b) 单击**继续 (Forward)** 继续操作。

步骤 4 加载磁盘映像：

a) 单击**浏览...(Browse...)**，选择映像文件。
b) 选择使用通用 *(Use Generic)* 作为**操作系统类型 (OS type)**。
c) 单击**继续 (Forward)** 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) 单击**继续 (Forward)**继续操作。

步骤 6 选中**安装前自定义配置 (Customize configuration before install)** 框，指定一个**名称 (Name)**，然后单击**完成 (Finish)**。

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 (Configuration)** > **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 (Disk 1)**。
b) 选择**高级选项 (Advanced options)**。
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 (Console)**。
b) 选择**删除 (Remove)**，删除默认的控制台。
c) 单击**添加硬件 (Add Hardware)**，添加一台串行设备。
d) 对于**设备类型 (Device Type)**，选择 *TCP net* 控制台 *(tcp) (TCP net console [tcp])* 。

e) 对于**模式 (Mode)**，选择服务器模式（绑定）*(Server mode [bind])*。
f) 对于**主机**，输入 **0.0.0.0** 作为 IP 地址，然后输入唯一的**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) 单击**添加硬件 (Add Hardware)**，添加一台看门狗设备。
b) 对于**型号 (Model)**，选择默认值 *(default)*。
c) 对于**操作 (Action)**，选择强制重置访客 *(Forcefully reset the guest)*。

步骤 11 配置虚拟网络接口。

选择 **macvtap** 或指定共享设备名称（使用桥名称）。

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) 单击**添加硬件(Add Hardware)**。
b) 选择**存储 (Storage)**。
c) 单击**选择托管或其他现有存储 (Select managed or other existing storage)**，然后浏览至 ISO 文件的位置。
d) 对于**设备类型 (Device type)**，选择 *IDE CDROM*。

步骤 13 配置虚拟机的硬件后，单击**应用 (Apply)**。

步骤 14 单击**开始安装 (Begin installation)**，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，然后单击**登录 (Sign In)**。

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 (Admin)** > **系统面板 (System Panel)** > **风格 (Flavor)**。

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 (Create Flavor)**。

步骤 5 从菜单中选择**管理员 (Admin)** > **系统面板 (System Panel)** > **映像 (Images)**。

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 (Create Image)**。

查看新创建的映像。

步骤 8 从菜单中选择**项目 (Project)** > **计算 (Compute)** > **实例 (Instances)**。

步骤 9 单击**启动实例 (Launch Instance)**。

步骤 10 在**启动实例 (Launch Instance)** > **详细信息 (Details)** 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 *(Boot from image)*。
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 (Launch Instance)** > **网络 (Networking)** 选项卡中，选择虚拟 Firepower 管理中心实例的管理网络。

步骤 12 单击**启动 (Launch)**。

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 (Console)** 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。

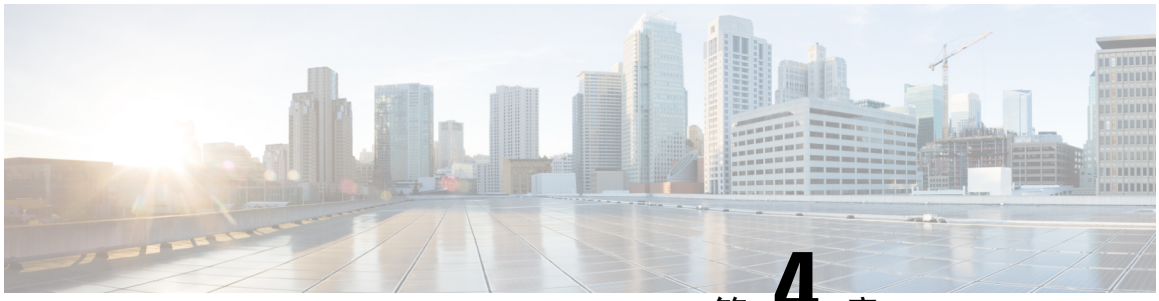
系统将显示设置页面。必须更改管理员密码，指定网络设置（若尚未指定），并接受 EULA。

步骤 3 完成设置后，单击**应用 (Apply)**。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Firepower Management Center Virtual 初始设置，第 97 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 105 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 FMCv 部署和 AWS

FMCv 需要 28 GB RAM 用于升级 (6.6.0+)

FMCv 平台在升级期间引入了新的内存检查。如果为虚拟设备分配的 RAM 少于 28 GB，FMCv 升级到 6.6.0+ 版本时将会失败。

重要事项

从版本 6.6.0 开始，基于云的 FMCv 部署（AWS、Azure）低内存实例类型已被完全弃用。您不能使用它们建新的 FMCv 实例，即使是早期 Firepower 版本也不例外。您可以继续运行现有实例。请参阅表 6: 不同版本受 AWS 支持的实例FMCv，第 32 页。

由于此内存检查，我们将无法在支持的平台上支持较低内存实例。

下表汇总了 FMCv 支持的 AWS 实例类型、版本 6.5.x 及更早版本支持的 AWS 实例类型，以及版本 6.6.0+ 支持的 AWS 实例类型。

注释

Firepower 版本 6.6 加入了对下表中所示 C5 实例类型的支持。较大的实例类型可为 AWS 虚拟机提供更多 CPU 资源，从而提高性能，有些则提供更多网络接口。

表 *6:* 不同版本受 *AWS* 支持的实例*FMCv*

平台	版本 **6.6.0+**	版本 **6.5.x** 及更早版本*
FMCv	c3.4xlarge：16 个 vCPU，30 GB	c3.xlarge：4 个 vCPU，7.5 GB
	c4.4xlarge：16 个 vCPU，30 GB	c3.2xlarge：8 个 vCPU，15 GB
	c5.4xlarge：16 个 vCPU，32 GB	c4.xlarge：4 个 vCPU，7.5 GB
	-	c4.2xlarge：8 个 vCPU，15 GB
	*请注意，FMCv 自版本 6.6.0 发布后将不再支持这些实例类型。从版本 6.6.0 开始，您必须使用至少具有 28 GB RAM 的实例部署 FMCv（任何版本）。请参阅调整实例大小，第 32 页。	

表 *7: FMCv 300* 的 *AWS* 支持实例

平台	版本 **7.1.0+**
FMCv 300	c5.9xlarge：36 vCPUs，72 GB SSD 存储：2000 GB

已弃用的实例

您可以继续运行您当前的版本 6.5.x 及更早版本的 FMCv 部署，但无法使用以下实例启动新的 FMCv 部署（任何版本）：

- c3.xlarge - 4 个 vCPU，7.5 GB（版本 6.6.0+ 之后为 FMCv 禁用）
- c3.2xlarge - 8 个 vCPU，15 GB（版本 6.6.0+ 之后为 FMCv 禁用）
- c4.xlarge - 4 个 vCPU，7.5 GB（版本 6.6.0+ 之后为 FMCv 禁用）
- c4.2xlarge - 8 个 vCPU，15 GB（版本 6.6.0+ 之后为 FMCv 禁用）

调整实例大小

由于从任何早期版本的 FMCv（6.2.x、6.3.x、6.4.x 和 6.5.x）升级到版本 6.6.0 的升级路径包括 28 GB RAM 内存检查，因此需要将当前实例类型的大小调整为支持版本 6.6.0 的大小（请参阅表 6: 不同版本受 AWS 支持的实例FMCv，第 32 页）。

如果当前实例类型与所需的新实例类型兼容，则可以调整实例的大小。对于 FMCv 部署：

- 将任何 c3.xlarge 或 c3.2xlarge 的大小调整为 c3.4xlarge 实例类型。
- 将任何 c4.xlarge 或 c4.2xlarge 的大小调整为 c4.4xlarge 实例类型。

在调整实例大小之前，请注意以下事项：

- 您必须先停止实例，然后再更改实例类型。

- 验证当前实例类型是否与您选择的新实例类型兼容。
- 如果此实例具有实例存储卷，则停止该实例后，其上的所有数据都将丢失。在调整大小之前迁移实例存储支持的实例。
- 如果不使用弹性 IP 地址，则在停止实例时会释放公共 IP 地址。

有关如何调整实例大小的说明，请参阅 AWS 文档《更改实例类型》(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-resize.html)。

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 环境之外不可下载。

AWS 部署准则和限制

支持的功能 (7.1.0+)

- **FMCv 300 for AWS** - 新的可扩展 FMCv 映像可在支持管理多达 300 设备的 AWS 平台上使用，具有更高的磁盘容量。
- 两种 FMCv 型号均支持 FMCv 高可用性：FMCv 和 FMCv 300。

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 3 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 Cisco 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 (System)** > **配置 (Configuration)**页面将会显示**无 (None)**或**未指定 (Not Specified)**，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。

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

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 单击**服务 (Services)** > **VPC**。

步骤 3 单击**VPC 控制面板 (VPC Dashboard)** > **您的 VPC (Your VPCs)**。

步骤 4 单击**创建 VPC (Create 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 单击**是，创建 (Yes, Create)** 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 单击**服务 (Services)** > **VPC**。

步骤 2 单击**VPC 控制面板 (VPC Dashboard)** > **互联网网关 (Internet Gateways)**，然后单击**创建互联网网关 (Create Internet Gateway)**。

步骤 3 输入用户自定义的名称标签以标识网关，然后单击“是，创建”(Yes, Create) 以创建网关。

步骤 4 选择上一步中创建的网关。

步骤 5 单击**连接到 VPC (Attach to VPC)** 并选择之前创建的 VPC。

步骤 6 单击**是，连接 (Yes, Attach)**，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 单击**服务 (Services)** > **VPC**。

步骤 2 单击**VPC 控制面板 (VPC Dashboard)** > **子网 (Subnets)**，然后单击**创建子网 (Create Subnet)**。

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”(No Preference)，由 Amazon 来选择区域。
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 单击**是，创建 (Yes, Create)** 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 单击**服务 (Services)** > **VPC**。

步骤 2 单击**VPC 控制面板 (VPC Dashboard)** > **路由表 (Route Tables)**，然后单击**创建路由表 (Create Route Table)**。

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 单击**是，创建 (Yes, Create)**以创建路由表。

步骤 6 选择刚创建的路由表。

步骤 7 单击**路由 (Routes)** 选项卡，以在详细信息窗格中显示路由信息。

步骤 8 单击**编辑 (Edit)**，然后单击**添加其他路由 (Add another route)**。

a) 在**目的地址**列中，输入**0.0.0.0/0**。

b) 在**目标 (Target)** 列中，选择上面创建的互联网网关。

步骤 9 单击**保存 (Save)**。

步骤 10 单击**子网关联 (Subnet Associations)** 选项卡，然后单击**编辑 (Edit)**。

步骤 11 选中要用于 FMCv 管理接口的子网对应的复选框，然后单击**保存 (Save)**。

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 单击**服务 (Services)** > **EC2**。

步骤 2 单击 **EC2 控制面板** > **安全组**。

步骤 3 单击**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) 单击**入站 (Inbound)** 选项卡，然后单击**添加规则 (Add Rule)**。

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 (Outbound)** 选项卡，然后单击**添加规则 (Add Rule)** 以添加出站流量规则，或保留**所有流量 (All traffic)**（作为**类型 (Type)**）和**任意位置 (Anywhere)**（作为**目标 (Destination)**） 的默认设置。

步骤 6 单击**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 单击**服务 (Services)** > **EC2**。

步骤 2 单击 **EC2 控制面板 (EC2 Dashboard)** > **网络接口 (Network Interfaces)**。

步骤 3 单击**创建网络接口 (Yes, Create)**。

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 (Subnet)**。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 (auto-assign)**。
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 单击**是，创建 (Yes, Create)** 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 (Disabled)**，然后单击**保存 (Save)**。

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 单击**服务 (Services)** > **EC2**。

步骤 2 单击 **EC2 控制面板 (EC2 Dashboard)** > **弹性 IP (Elastic IPs)**。

步骤 3 单击**分配新地址 (Allocate New Address)**。

根据弹性/公共 IP 地址分配需要，重复此步骤。

步骤 4 单击**是，分配 (Yes, Allocate)** 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。

注释 除非您在初始部署期间使用用户数据（**高级详细信息 (Advanced Details)** > **用户数据 (User Data)**）来定义默认密码，否则默认管理员密码为 AWS 实例 ID。

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

步骤 2 登录到 Amazon Marketplace 后，单击为虚拟 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 单击**继续 (Continue)**，然后单击**手动启动 (Manual Launch)** 选项卡。

步骤 4 单击**接受条款 (Accept Terms)**。

步骤 5 在期望的区域单击**使用 EC2 控制台启动 (Launch with EC2 Console)**。

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 FMCv 部署和 AWS。

步骤 7 单击屏幕底部的**下一步：配置实例详细信息 (Next: Configure Instance Details)** 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 (Advanced Details)** > **用户数据 (User Data)**，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。

在 7.0 及更高版本中，除非您在初始部署期间使用用户数据（**高级详细信息 (Advanced Details)** > **用户数据 (User Data)**）来定义默认密码，否则默认管理员密码为 AWS 实例 ID。

在早期版本中，默认管理员密码为 **Admin123**。

步骤 8 单击**下一步：添加存储 (Next: Add Storage)**，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 单击**下一步：标记实例 (Next: Tag Instance)**。

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 (Next: Configure Security Group)**。

步骤 11 单击**选择现有安全组 (Select an existing Security Group)** 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 单击**检查和启动 (Review and Launch)**。

步骤 13 单击**启动 (Launch)**。

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 单击**启动实例 (Launch Instances)**。

步骤 16 单击 **EC2 控制面板 (EC2 Dashboard)** > **弹性 IP (Elastic IPs)**，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 (Associate Address)**。

找到要选择的实例或网络接口，然后单击“关联”(Associate)。

步骤 18 单击 **EC2 控制面板 (EC2 Dashboard)** > **实例 (Instances)**。

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 (Settings)** > **获取实例屏幕截图 (Get Instance Screenshot)**。

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：

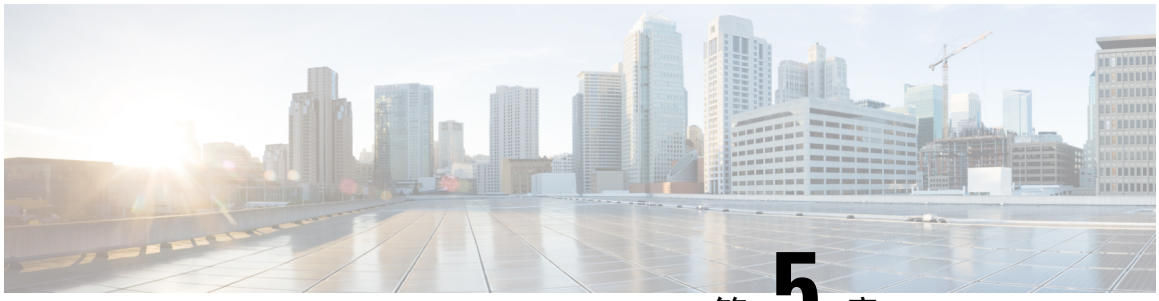
- 确保部署已完成。FMCv VM 实例屏幕截图应显示一条类似于“适CiscoFirepower Management Center for AWS vW.X.Y (build ZZ)”的消息，后面可能跟着一些其他的输出行。
- 确保拥有弹性 IP 地址，已将该地址关联 Firepower 管理中心的管理网络接口 (eni)，并且正连接到该 IP 地址。
- 确保 VPC 已关联互联网网关 (igw)。
- 确保管理子网已关联路由表。
- 确保管理子网关联的路由表具有指向互联网网关 (igw) 的路由（目的地址为“0.0.0.0/0”）。
- 确保安全组允许传入连接所用 IP 地址产生的 SSH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

在 Microsoft Azure 云上部署虚拟 Firepower 管理中心

您可以在 Microsoft Azure 云上部署 Firepower Management Center Virtual (FMCv)。

重要事项

在 Microsoft Azure 上，从 Cisco Firepower 6.4 及更高版本软件开始支持运行 FMCv。

关于 FMCv 部署和 Azure

您可以使用 Azure 市场中提供的解决方案模板，在 Microsoft Azure 中部署 Firepower Management Center Virtual (FMCv)。使用 Azure 门户部署 FMCv 时，您可以使用现有的空资源组和存储帐户（或创建新帐户）。解决方案模板会引导您完成一组配置参数，这些参数可提供您 FMCv 的初始设置，允许您在首次 FMCv 启动后登录到 web 界面。

FMCv 需要 28 GB RAM 用于升级 (6.6.0+)

FMCv 平台在升级期间引入了新的内存检查。如果为虚拟设备分配的 RAM 少于 28 GB，FMCv 升级到 6.6.0+ 版本时将会失败。

重要事项 从版本 6.6.0 开始，基于云的 FMCv 部署（AWS、Azure）低内存实例类型已被完全弃用。您不能使用它们建新的 FMCv 实例，即使是早期 Firepower 版本也不例外。您可以继续运行现有实例。请参阅表 8: 不同版本受 Azure 支持的实例FMCv，第 44 页。

由于此内存检查，我们将无法在支持的平台上支持较低内存实例。

Azure 上的 FMCv 必须使用资源管理器部署模式在虚拟网络 (VNet) 中加以部署。您可以在标准 Azure 公有云环境中部署 FMCv。FMCv Azure 市场支持自带许可证（BYOL）模型。

下表汇总了 FMCv 支持的 Azure 实例类型、版本 6.5.x 及更早版本支持的 Azure 实例类型，以及版本 6.6.0+ 支持的 Azure 实例类型。

表 *8:* 不同版本受 *Azure* 支持的实例*FMCv*

平台	版本 6.6.0+	版本 6.5.x 及更早版本*
FMCv	Standard_D4_v2：8 个 vCPU，28 GB	Standard_D3_v2：4 个 vCPU，14 GB
	-	Standard_D4_v2：8 个 vCPU，28 GB
	*请注意，FMCv 自版本 6.6.0 发布后将不再支持 Standard_D3_v2 实例。从版本 6.6.0 开始，您必须使用至少具有 28 GB RAM 的实例部署 FMCv（任何版本）。请参阅调整实例大小，第 44 页。	

已弃用的实例

您可以继续使用 Standard_D3_v2 运行当前版本 6.5.x 及更早版本的 FMCv 部署，但不能使用此实例启动新的 FMCv 部署（任何版本）。

调整实例大小

由于从任何早期版本的 FMCv（6.2.x、6.3.x、6.4.x 和 6.5.x）升级到版本 6.6.0 的升级路径包括 28 GB RAM 内存检查，因此，如果您使用 Standard_D3_v2，则需要将实例类型大小调整为 Standard_D4_v2（请参阅表 8: 不同版本受 Azure 支持的实例FMCv，第 44 页）。

您可以使用 Azure 门户或 PowerShell 调整实例的大小。如果虚拟机当前正在运行，更改其大小将导致其重新启动。停止虚拟机可能会显示额外的大小。

有关如何调整实例大小的说明，请参阅 Azure 文档《调整 Windows 虚拟机大小》(https://docs.microsoft.com/en-us/azure/virtual-machines/windows/resize-vm)。

前提条件和系统要求

FMCv对 Microsoft Azure 的支持是 Firepower 版本 6.4.0 的新功能。有关 Firepower Management Center Virtual 与 Firepower 系统的兼容性，请参阅《Cisco Firepower 威胁防御虚拟兼容性》。

FMCv在 Azure 中部署之前，请验证以下内容：

- 在 Azure.com 上创建帐户。

  在 Microsoft Azure 上创建帐户后，您可以登录该市场，搜索思科 Firepower Management Center Virtual 市场，然后选择“Cisco Firepower Management Center (FMCv) BYOL”产品。

- 思科智能账户。可以在思科软件中心 https://software.cisco.com/ 创建一个帐户。

准则和限制

支持的功能

- 支持的 Azure 实例
  - 标准 D3_v2-4 Vcpu，14GB memory，250GB 磁盘大小
  - 标准 D4_v2—8 vCPU，28GB memory，400GB 磁盘大小
- 公共 IP 寻址
  - 为管理 0/0 分配了一个公共 IP 地址。

许可

在FMCv Azure 公共市场中，支持自带许可证 (BYOL) 模型。对于 FMCv，这是平台许可证，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 Management Center Virtual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。

- 许可模式：
  - 仅智能许可证

有关许可的详细信息，请参阅《*Firepower* 管理中心配置指南》中的Firepower 系统许可，以了解有关如何管理许可证的详细信息；有关Firepower 系统功能许可证的概述（包括有用的链接），请参阅 Cisco Firepower 系统功能许可证。

系统关闭和重新启动

请勿在“Azure 虚拟机概述”(Azure Virtual machine overview) 页面上使用**重启 (Restart)** 和**停止 (Stop)** 控件打开 FMCv 虚拟机。这些不是正常关机机制，可能导致数据库损坏。

使用 FMCv 的网络界面中可用的**系统 (System)** > **配置 (Configuration)** 选项关闭或重新启动虚拟设备。

从 FMCv 命令行界面使用 `shutdown` 和 `restart` 命令关闭或重新启动设备。

不支持的功能

- 许可模式：

  - 现收现付 (PAYG) 许可。
  - 永久许可证预留 (PLR)。
- 管理
  - Azure 门户“重置密码”功能。
  - 基于控制台的密码恢复；由于用户没有实时访问控制台的权限，所以无法恢复密码。无法启动密码恢复映像。唯一的办法是部署新的 FMCv 虚拟机。
- 高可用性（活动/备用）
- 虚拟机导入/导出

在部署期间创建的资源

在 Azure 中部署 FMCv 时，会创建以下资源：

- 具有单个 FMCv 接口的 Cisco 虚拟机 (VM)（需要新的虚拟网络或现有含 1 个子网的虚拟网络）。
- 一个资源组。

  FMCv 始终会部署到新的资源组中。不过，您可以将其附加到另一个资源组的现有虚拟网络。
- 一个名为 *vm name*-mgmt-SecurityGroup 的安全组。

  此安全组将附加到虚拟机的 Nic0。

  该安全组包括允许 SSH（TCP 端口 22）和 Firepower 管理中心接口（TCP 端口 8305）的管理流量的规则。您可以在部署后修改这些值。
- 公共 IP 地址（根据您在部署期间选择的值命名）。

  该公共 IP 地址与虚拟机 Nic0 相关联，后者映射到管理接口。

  注释 您可以创建新的公共 IP 地址，或者选择现有 IP 地址。您也可以选择**无 (NONE)**。如果没有公共 IP 地址，则与 FMCv 之间的任何通信均必须源自 Azure 虚拟网络内
- 该子网的路由表（如果已存在，则相应更新）。
- 所选存储帐户中的启动诊断文件。

  启动诊断文件将在 Blobs（二进制大对象）中。
- 所选存储帐户中位于 Blobs 和容器 VHD 下的两个文件，名为 *vm name*-disk.vhd 和 *VM name*-<uuid>.status。
- 一个存储帐户（除非您选择了现有的存储帐户）。

重要事项 在删除虚拟机时，必须逐个删除每个资源（您要保留的任何资源除外）。

部署虚拟 Firepower 管理中心

您可以使用模板在 Azure 中部署 Firepower Management Center Virtual。Cisco 提供两种类型的模板：

- **Azure 市场中的解决方案模板**-使用 Azure 市场中提供的解决方案模板， FMCv使用 Azure 门户部署。您可以使用现有资源组和存储帐户（或创建新的资源组和存储帐户）来部署虚拟设备。要使用解决方案模板，请参阅从 Azure 市场使用解决方案模板部署，第 47 页。
- **GitHub 存储库中的 ARM 模板** — 除了基于市场的部署，Cisco 还在 GitHub 存储库中提供 Azure Resource Manager (ARM) 模板，以简化在 Azure 上部署 FMCv 的过程。使用托管映像和两个 JSON 文件（一个模板文件和一个参数文件），您可以在单次协调操作中为 FMCv 部署并调配所有资源。

从 Azure 市场使用解决方案模板部署

使用 Azure Firepower Management Center Virtual市场FMCv中提供的解决方案模板，从 Azure 门户部署。以下程序概要列出在 Microsoft Azure 环境中设置 FMCv 威胁防御虚拟的步骤。如需了解详细的 Azure 设置步骤，请参阅《Azure 入门》。

在 Azure 中部署 FMCv 时，会自动生成各种配置，例如资源、公共 IP 地址和路由表。您可以在部署后进一步管理这些配置。例如，您可能需要更改超时值较低的“空闲超时”默认值。

步骤 1 使用您的 Microsoft 帐户凭证登录 Azure 门户（https://portal.azure.com）。

Azure 门户显示与当前帐户和订用相关联的虚拟要素，与数据中心位置无关。

步骤 2 单击**创建资源 (Create a Resource)**。

步骤 3 在市场中搜索“Cisco Firepower Management Center (FMCv)”，选择产品，然后单击**创建 (Create)**。

步骤 4 配置 **基本**设置：

a) 在 **Azure 中的 FMC VM**字段中，输入虚拟机的名称。此名称应在您的 Azure 订用中具有唯一性。

注意 确保不要使用现有的名称，否则部署将失败。

b) （可选）从下拉列表中选择 **FMC 软件版本 (FMC Software Version)**。

这应默认为最新的可用版本。

c) 在**主要帐户用户名**）字段中，输入 Azure 帐户管理员的用户名。

名称“admin”是 Azure 中的预留名称，不能使用。

注意　此处输入的用户名用于Azure帐户，而不是FMCv管理员访问权限。请勿使用此用户名登录FMCv。

d) 选择身份验证类型：**密码 (Password)**或 **SSH 公钥 (SSH public key)**。

如果您选择**密码 (Password)**，请输入密码并确认。密码必须介于 12 到 72 个字符之间，并且必须包含以下 3 项：1 个小写字符、1 个大写字符、1 个数字和 1 个非“\”或“-”的特殊字符。

如果选择 **SSH 公钥 (SSH public key)**，请指定远程对等体的 RSA 公共密钥。

e) 输入 FMCv 的 **FMC 主机名**。

f) 输入**管理密码**。

这是您以管理员身份登录到 FMCv 的 Web 界面时使用的密码。 FMCv

g) 选择**订用 (Subscription)** 类型。

通常仅列出一个选项。

h) 创建**资源组**。

FMCv 始终会部署到新的资源组中。仅当现有资源组为空时，部署到现有资源组的选项才有效。

不过，您可以在后续步骤中配置网络选项时将 FMCv 附加到另一个资源组的现有虚拟网络。

i) 选择地理**位置 (Location)**。

对于此部署中使用的所有资源，应使用相同的位置。FMCv、网络、存储帐户等均应使用相同的位置。

j) 单击**确定 (OK)**。

步骤 5 接下来，完成 **Cisco FMCv 设置**下的初始配置：

a) 确认所选的**虚拟机大小 (Virtual machine size)**，或单击**更改大小 (Change size)** 链接以查看 VM 大小选项。单击**选择 (Select)** 以确认。

仅显示受支持的虚拟机大小。

b) 配置**存储帐户**。您可以使用现有存储帐户，也可以创建新的存储帐户。

- 输入存储帐户的**名称 (Name)**，然后单击**确定 (OK)**。存储帐户名称只能包含小写字母和数字。它不能包含特殊字符。
- 在此版本中， FMCv 仅支持通用的标准性能存储。

c) 配置**公有 IP 地址**。您可以使用现有 IP 地址，也可以创建新 IP 地址。

- 单击**新建 (Create new)** 对话框，以创建一个新的公共IP地址。在**名称 (Name)** 字段中输入IP地址的标签，选择 SKU 选项的**标准 (Standard)**，然后单击**确定 (OK)**。

  注释　Azure会创建一个动态公共IP地址，无论此步骤中选择的是动态还是静态。当虚拟机停止和重启时，该公共IP可能会变化。如果您更喜欢固定的IP地址，可以在部署后编辑公共IP地址，将其从动态地址更改为静态地址。

- 如果您不想将公共 IP 地址分配给 FMCv，可以选择**无 (NONE)**。如果没有公共 IP 地址，则与 FMCv 之间的任何通信均必须源自 Azure 虚拟网络内。

d) 添加与公共 IP 标签匹配的 **DNS 标签**。

完全限定域名等于 DNS 标签加上 Azure URL：*<dnslabel>.<location>.cloudapp.azure.com*

e) 选择现有的**虚拟网络 (Virtual network)**，或创建新的虚拟网络，然后单击**确定 (OK)**。

f) 配置 FMCv 的管理子网。

定义**管理子网名称**并查看**管理子网前缀**。建议的子网名称为“management”。

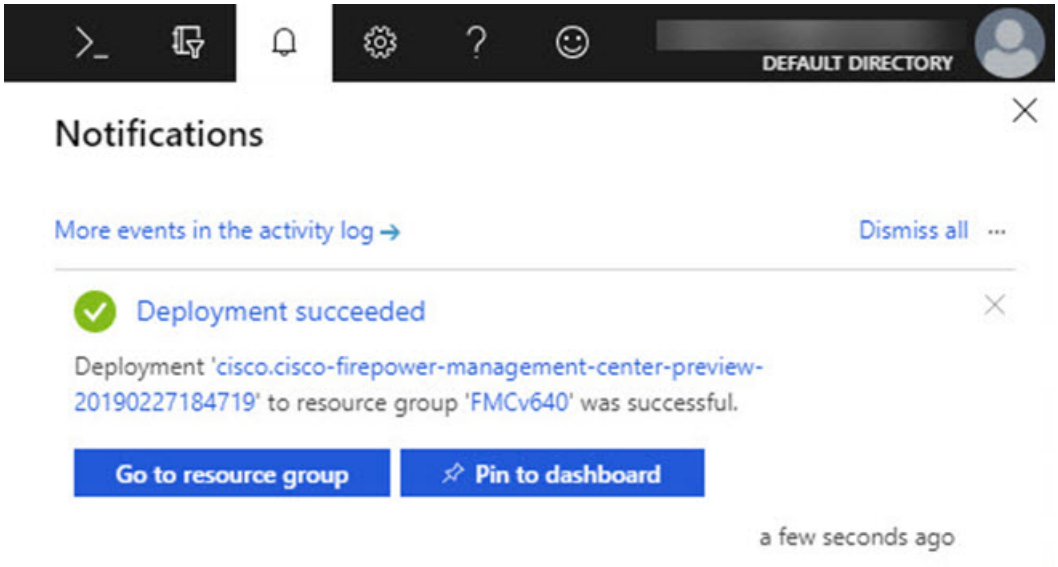
g) 单击**确定 (OK)**。

步骤 6 查看配置摘要，然后点击**确定 (OK)**。

步骤 7 查看使用条款，然后单击**创建 (Create)**。

步骤 8 选择门户顶部的**通知 (Notifications)**（电铃图标）以查看部署的状态。

图 *1: Azure* 通知



在这里，您可以单击部署以查看更多详细信息，或在部署成功后转至资源组。FMCv 可用前的总时间约为 30 分钟。部署时间在 Azure 中有所不同。请等候，直到 Azure 报告 FMCv 虚拟机正在运行。

步骤 9 （可选）Azure提供了许多工具来帮助您监控虚拟机的状态，包括**引导诊断**和**串行控制台**。这些工具允许您在启动时查看虚拟机的状态。

a) 在左侧菜单中，选择**虚拟机 (Virtual machines)**。

b) 在列表FMCv中选择您的 VM。系统将打开虚拟机的“概述”页面。

c) 向下滚动到“**支持 + 故障排除 (Support + troubleshooting)**”部分，选择**引导诊断 (Boot diagnostics)** 或**串行控制台 (Serial console)**。系统将打开一个新窗格，其中包含引导诊断**屏幕截图**和**串行日志**或基于文本的**串行控制台**，并开始连接。

如果在启动诊断 FMCv 或串行控制台上看到登录提示，则会确认 Web 界面的就绪状态。

示例：

```
Cisco Firepower Management Center for Azure v6.4.0 (build 44)
FMCv64East login:
```

下一步做什么

- 确认 FMCv 部署已经成功。Azure 控制面板在“资源组”下列出新 FMCv VM，以及所有相关资源（存储、网络、路由表等）。

验证虚拟 Firepower 管理中心虚拟部署

创建 FMCv VM 后，Microsoft Azure 控制板将在资源组下列出新的 FMCv VM。此外，还会创建并列出相应的存储帐户和网络资源。控制板提供您的 Azure 资产的统一视图，并提供对运行状况和性能的简单的评估概览 FMCv。

开始之前

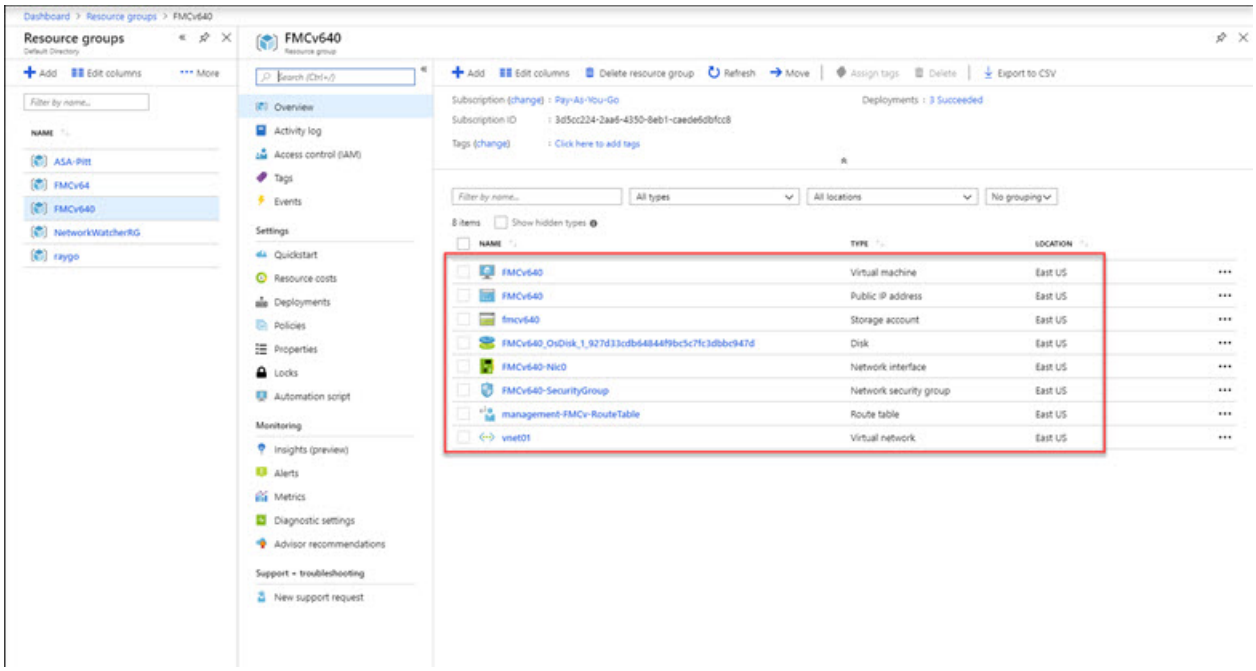
FMCv VM 将自动启动。在部署过程中，状态列为“正在创建”，而 Azure 创建虚拟机，然后在部署完成后，状态将更改为“正在运行”。

注释 请记住，部署时间在 Azure 中有所不同，FMCv 可使用所需的总时间大约为 30 分钟，即使 Azure 控制板将 FMCv VM 的状态显示为“正在运行”。

步骤 1 要在部署完成后查看 FMCv 资源组及其资源，请从左侧菜单窗格中单击**资源组 (Resource groups)** 以访问“资源组”(Resource groups) 页面。

下图显示了 Microsoft Azure 门户中的“资源组”页面的示例。请注意 FMCv VM 及其相应的资源（存储帐户、网络资源等）。

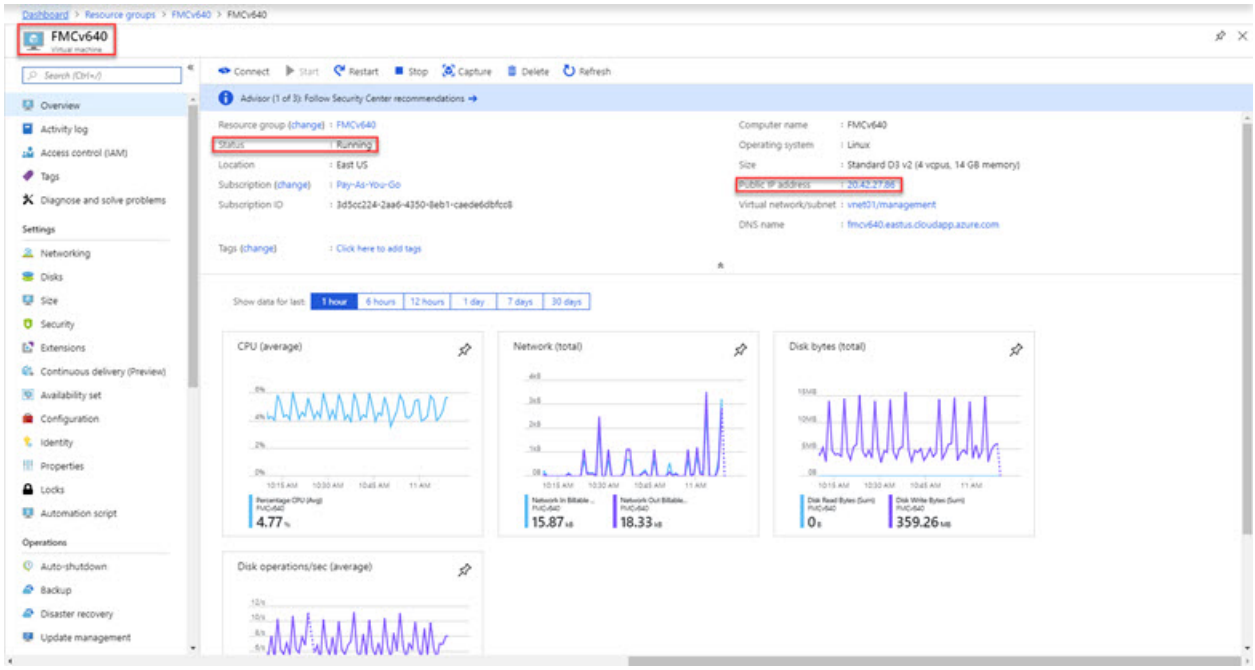
图 *2: Azure FMCv* 资源组页面



步骤 2 要查看与资源组关联的 FMCv VM 的详细信息，请单击 FMCv VM 的名称。

下图显示了与 FMCv VM 关联的**虚拟机 (Virtual machine)** 概述页面的示例。您可以从“资源组”(Resources groups) 页面访问此概述。

图 *3:* 虚拟机概述



观察状态是否为“正在运行”。您可以从 Microsoft Azure 门户中的**虚拟机 (Virtual machine)** 页面停止、启动、重新启动和删除 FMCv VM。请注意，这些控制不是 FMCv 的正常关闭机制；有关正常关闭的信息，请参阅准则和限制，第 45 页。

步骤 3 在**虚拟机 (Virtual machine)** 页面中，查找分配给的 FMCv 的**公共 IP 地址**。

注释　　您可以将鼠标悬停在 IP 地址上，然后选择**单击复制 (Click to copy)** 以复制 IP 地址。

步骤 4 通过浏览器访问 **https://***public_ip/*，其中 *public_ip* 是在部署 VM 时分配给 FMCv 管理接口的 IP 地址。

随即显示登录页面。

步骤 5 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。

下一步做什么

- 我们建议您完成一些管理任务，使部署更易于管理，例如创建用户和查看运行状况和系统策略。有关如何开始的概述，请参阅虚拟 Firepower 管理中心初始管理和配置，第 105 页。
- 您还应检查设备注册和许可要求。
- 有关如何开始配置 Firepower 系统的信息，请参阅您的版本完整《Firepower 管理中心配置指南》。

监控和故障排除

本部分包括 Micosoft Azure 中部署的 Firepower Management Center Virtual 设备的常规监控和故障排除指南。监控和故障排除可以与 Azure 中的 VM 部署或 FMCv 设备本身相关。

Azure 监控的虚拟机部署

Azure 提供**支持 + 故障排除**菜单下的许多工具，提供对工具和资源的快速访问，以帮助您诊断和解决问题并获得更多帮助。值得关注的两项包括：

- **引导程序诊断** — 允许您在启动时查看FMCv虚拟机的状态。引导诊断程序从虚拟机和屏幕截图收集串行日志信息。这可以帮助您诊断任何启动问题。
- **串联控制台** — Azure 门户中的 VM 串行控制台支持访问基于文本的控制台。此串行连接连接到虚拟机的 COM1 串行端口，通过分配给的公共 IP 地址，提供FMCv对的命令行界面的串行和 SSH 访问FMCv。

FMCv 监控与日志记录

故障排除和常规日志记录操作遵循与当前 FMC 和 FMCv 型号相同的程序。有关您的版本，请参阅《*Firepower* 管理中心配置指南》中的系统监控和故障排除部分。

此外，Microsoft Azure Linux 代理 (waagent) 管理与 Azure 交换矩阵控制器的 Linux 调配和 VM 交互。因此，以下是故障排除的重要日志：

- **/var/log/waagent.log** — 此日志将包含与 Azure FMC 调配相关的任何错误。
- **/var/log/firstboot.S07install_waagent** — 此日志将包含 waagent 安装中的任何错误。

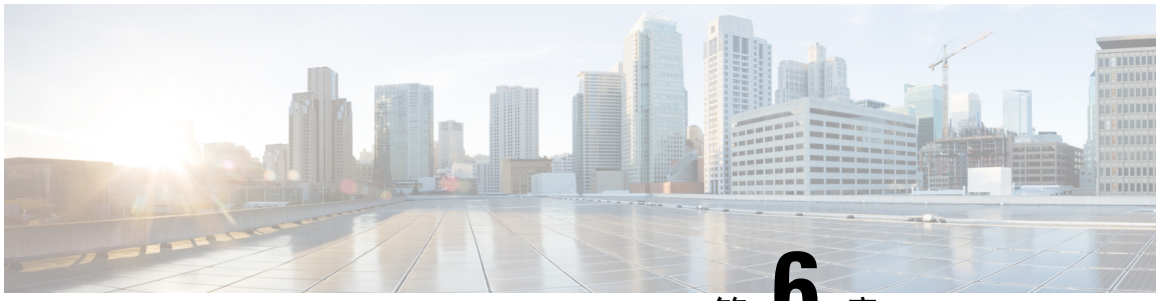
Azure 调配失败

使用 Azure Marketplace 解决方案模板调配错误不常见。但是，如果您遇到调配错误，请记住以下要点：

- Azure 为虚拟机调配 waagent 时20分钟超时，此时它会重新启动。
- FMC如果由于任何原因而无法进行调配，则20分钟计时器往往会在FMC数据库初始化过程中结束，从而可能导致部署失败。
- 如果在FMC 20 分钟内无法调配，我们建议您重新开始。
- 您可以参考*/var/log/waagent.log*了解故障排除信息。
- 如果在串行控制台中看到 HTTP 连接错误，则表明 waagent 无法与交换矩阵通信。您应在重新部署时检查网络设置。

Microsoft Azure 云上的 FMCv 历史

功能名称	版本	功能信息
在 Microsoft Azure 云上部署虚拟 Firepower 管理中心 (FMCv)。	6.4.0	初始支持。



第 6 章

在 Google 云平台上部署虚拟 Firepower 管理中心

Google 云平台 (GCP) 是 Google 提供的公共云服务，允许您构建和托管 Google 的可扩展基础设施应用。Google 的虚拟私有云 (VPC) 可让您灵活地扩展和控制工作负载在区域和全球范围内的连接方式。GCP 允许您在 Google 的公共基础设施之上构建自己的 VPC。

您可以在 GCP 上部署 Firepower Management Center Virtual (FMCv)。

关于 FMCv 部署和 GCP

Cisco Firepower Management Center Virtual (FMCv) 运行与物理思科 FMC 相同的软件，以虚拟形式提供成熟的安全功能。FMCv 可以部署在公共 GCP 中。然后可以将其配置为管理虚拟和物理 Firepower 设备。

GCP 计算机类型支持

FMCv 支持计算优化和通用计算机高内存计算机类型，以及高 CPU 计算机类型。FMCv 支持以下 GCP 计算机类型。

注释 支持的计算机类型可能会更改，恕不另行通知。

表 *9:* 支持的计算优化计算机类型

计算优化计算机类型	属性	
	vCPU	**随机存取存储器(GB)**
c2-standard-8	8	32 GB
c2-standard-16	16	64 GB

表 *10:* 支持的通用计算机类型

通用计算机类型	属性	
	vCPU	**随机存取存储器(GB)**
n1-standard-8	8	30 GB
n1-standard-16	16	60 GB
n2-standard-8	8	32
n2-standard-16	16	64
n1-highcpu-32	32	28.8
n2-highcpu-32	32	32
n1-highmem-8	8	52
n1-highmem-16	16	104
n2-highmem-4	4	32
n2-highmem-8	8	64

GCP 上 FMCv 的前提条件

- 在 https://cloud.google.com 上创建 GCP 帐户。
- 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。
  - 从 Firepower Management Center 配置安全服务的所有许可证授权。
  - 有关如何管理许可证的更多信息，请参阅《Firepower 管理中心配置指南》中的“Firepower 系统许可”。

- 接口要求：
  - 管理接口 - 用于将 Firepower 威胁防御设备连接到 Firepower 管理中心。
- 通信路径：
  - 用于管理访问 FMCv 的公共 IP。
- 对于 Firepower Management Center Virtual 和 Firepower 系统的兼容性，请参阅《Cisco Firepower 兼容性》。

FMCv 和 GCP 的准则和限制

支持的功能

- 在 GCP 计算引擎中部署
- 每个实例最多 32 个 vCPU（基于 GCP 计算机类型）
- 许可 - 仅支持 BYOL

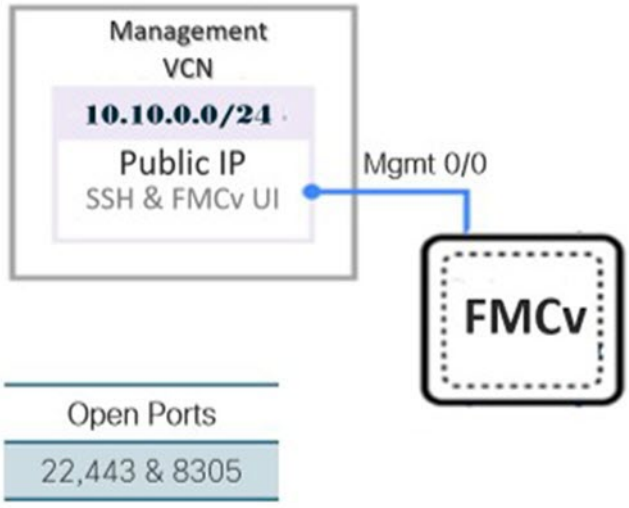
不支持的功能

- IPv6
- FMCv 本地 HA
- 自动缩放
- 透明/内联/被动模式
- 多情景模式

GCP 上 FMCv 的网络拓扑

下图显示了在 GCP 中配置了 1 个子网的 FMCv 的典型拓扑。

图 *4: GCP* 上 *FMCv* 部署的拓扑示例



在 GCP 上部署 FMCv

以下程序介绍了如何准备 GCP 环境并启动 FMCv 实例。

创建 VPC 网络

FMCv 部署需要为管理 FMCv 使用管理 VPC。请参阅第 3 页的图 1 作为指南。

步骤 1 在 GCP 控制台中，选择 **VPC 网络 (VPC networks)**，然后单击**创建 VPC 网络 (Create VPC Network)**。
步骤 2 在**名称 (Name)** 字段中，为 VPC 网络输入描述性名称。
步骤 3 在**子网创建模式 (Subnet creation mode)**，下，单击**自定义 (Custom)**。
步骤 4 在**新子网 (New subnet)** 下的**名称 (Name)** 字段中输入所需的名称。
步骤 5 从**区域 (Region)** 下拉列表中，选择适合您的部署的区域。
步骤 6 从 **IP 地址范围 (IP address range)** 字段中，输入 CIDR 格式的第一个网络子网，例如 10.10.0.0/24。
步骤 7 接受所有其他设置的默认设置，然后单击**创建 (Create)**。

创建防火墙规则

每个 VPC 网络都需要防火墙规则来允许 SSH 和流量。为每个 VPC 网络创建防火墙规则。

步骤 1 在 GCP 控制台中，依次选择**网络 (Networking)** > **VPC 网络 (VPC network)** > **防火墙 (Firewall)**，然后单击**创建防火墙规则 (Create Firewall Rule)**。

步骤 2 在**名称 (Name)** 字段中，为防火墙规则输入描述性名称，例如：*vpc-asiasouth-mgmt-ssh*。

步骤 3 从**网络 (Network)** 下拉列表中，选择要为其创建防火墙规则的 VPC 网络的名称，例如 *fmcv-south-mgmt*。

步骤 4 从**目标 (Targets)** 下拉列表中，选择适用于防火墙规则的选项，例如：**网络中的所有实例**。

步骤 5 在**源 IP 范围 (Source IP ranges)** 字段中，以 CIDR 格式输入源 IP 地址范围，例如 0.0.0.0/0。

仅允许自这些 IP 地址范围内的源的流量。

步骤 6 在**协议和端口 (Protocols and ports)**下，选择**指定的协议和端口 (Specified protocols and ports)**。

步骤 7 添加安全规则：

a) 添加规则以允许 SSH (TCP/22)。

b) 添加规则以允许 TCP 端口 443。

您访问的 FMCv UI 需要为 HTTPS 连接打开端口 443。

步骤 8 单击**创建 (Create)**。

在 GCP 上创建 FMCv 实例

您可以按照以下步骤从 GCP 控制台部署 FMCv 实例。

步骤 1 登录到 GCP 控制台。

步骤 2 单击**导航菜单** > **市场 (Marketplace)**。

步骤 3 在市场中搜索“Cisco Firepower Management Center (FMCv) BYOL”并选择产品。

步骤 4 单击**启动 (Launch)**。

a) **部署名称 (Deployment name)** - 为实例指定唯一的名称。

b) **映像版本 (Image version)** - 从下拉列表中选择版本。

c) **区域 (Zone)** - 选择要部署 FMCv 的区域。

d) **计算机类型 (Machine type)** - 根据 GCP 计算机类型支持，第 55 页 选择正确的计算机类型。

e) **SSH 密钥（可选）(SSH key [optional])** - 从 SSH 密钥对粘贴公钥。

密钥对由GCP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。

f) 选择是允许还是**阻止使用项目级别的 SSH 密钥 (Block project-wide SSH keys)** 来访问此实例。请参阅 Google 文档允许或阻止使用项目级别的公共 SSH 密钥访问 Linux 实例。

g) **启动脚本 (Startup script)** - 为 FMCv 提供 day0 配置。

以下示例显示可以在**启动脚本 (Startup script)** 字段中复制和粘贴的 day0 配置示例：

```
{
"AdminPassword": "myPassword@123456",
"Hostname": "cisco-fmcv"
}
```

提示 为防止执行错误，您应使用 JSON 验证器来验证 day0 配置。

h) 从下拉列表中选择**启动磁盘类型 (Boot disk type)**。

默认情况下会选中**标准持久磁盘 (Standard Persistent Disk)**。思科建议您使用默认启动磁盘类型。

i) **启动磁盘大小 (GB) (Boot disk size in GB)** 默认值为 250 GB。思科建议您保留默认启动磁盘大小。它不能小于 250 GB。

j) 单击**添加网络接口 (Add network interface)** 以配置管理接口。

注释 创建实例后，无法将接口添加到实例。如果使用不正确的接口配置创建实例，则必须删除该实例并使用正确的接口配置重新创建实例。

- 从**网络 (Network)** 下拉列表中，选择一个 VPC 网络，例如 *vpc-branch-mgmt*。
- 从**外部 IP (External IP)** 下拉列表中，选择适当的选项。

  对于管理接口，将**外部 IP (External IP)** 选择为**临时 (Ephemeral)**。
- 单击**完成 (Done)**。

k) **防火墙 (Firewall)** - 应用防火墙规则。

- 选中**允许来自 Internet（SSH 访问）的 TCP 端口 22 流量 (Allow TCP port 22 traffic from the Internet [SSH access])** 复选框以允许 SSH。
- 选中**允许来自 Internet (FMC GUI) 的 HTTPS 流量 (Allow HTTPS traffic from the Internet [FMC GUI])** 复选框以允许 HTTPS 连接。
- 选中**允许来自 Internet (SFTunnel comm) TCP 端口 8305 流量 (Allow TCP port 8305 traffic from the Internet [SFTunnel comm])** 复选框以允许 FMCv 和受管设备使用双向 SSL 加密通信通道进行通信。

l) 单击**更多 (More)** 展开视图并确保 **IP 转发 (IP Forwarding)** 设置为**开 (On)**。

步骤 5 单击**部署 (Deploy)**。

注释 启动时间取决于多种因素，包括资源的可用性。最多可能需要 35 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。

下一步做什么

从 GCP 控制台的 VM 实例页面查看实例详细信息。您将找到内部 IP 地址、外部 IP 地址以及用于停止和启动实例的控件。如果需要编辑实例，则需要停止实例。

在 GCP 上访问 FMCv 实例

确保您已创建防火墙规则以允许 SSH（通过端口 22 的 TCP 连接）；有关详细信息，请参阅创建防火墙规则，第 58 页。

此防火墙规则允许访问 FMCv 实例，并允许您使用以下方法连接到实例。

- 外部 IP
  - 浏览器窗口
  - 任何其他 SSH 客户端或第三方工具
- 串行控制台
  - Gcloud 命令行

有关详细信息，请参阅 Google 文档连接到实例 (Connecting to instances)。

注释 如果选择不添加 Day0 配置，则可以使用默认凭证登录到 FMCv 实例。系统会提示您在首次登录时设置密码。

使用串行控制台连接至 FMCv 实例

步骤 1 在 GCP 控制台中，选择**计算引擎 (Compute Engine)** > **VM 实例 (VM instances)**。

步骤 2 单击 FMCv 实例名称以打开 **VM 实例详细信息 (VM instance details)** 页面。

步骤 3 在**详细信息 (Details)** 选项卡下，单击**连接到串行控制台 (Connect to serial console)**。

有关详细信息，请参阅 Google 文档与串行控制台交互 (Interacting with the serial console)。

使用外部 IP 连接至 FMCv 实例

FMCv 实例分配有内部 IP 和外部 IP。您可以使用外部 IP 来访问 FMCv 实例。

步骤 1 在 GCP 控制台中，选择**计算引擎 (Compute Engine)** > **VM 实例 (VM instances)**。

步骤 2 单击 FMCv 实例名称以打开 **VM 实例详细信息 (VM instance details)** 页面。

步骤 3 在**详细信息 (Details)** 选项卡下，单击 **SSH** 字段的下拉菜单。

步骤 4 从 **SSH** 下拉菜单中选择所需的选项。

您可以使用以下方法连接到 FMCv 实例。

- 任何其他 SSH 客户端或第三方工具 - 有关详细信息，请参阅 Google 文档使用第三方工具连接 (Connecting using third-party tools)。

使用 Gcloud 连接至 FMCv 实例

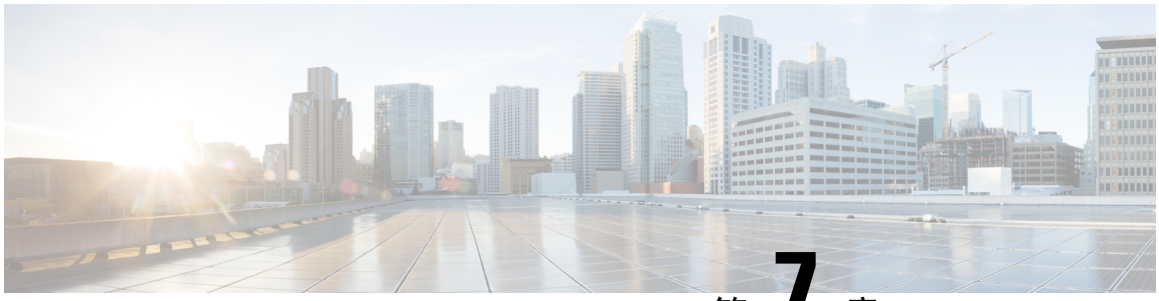
步骤 1 在 GCP 控制台中，选择**计算引擎 (Compute Engine)** > **VM 实例 (VM instances)**。

步骤 2 单击 FMCv 实例名称以打开 **VM 实例详细信息 (VM instance details)** 页面。

步骤 3 在**详细信息 (Details)** 选项卡下，单击 **SSH** 字段的下拉菜单。

步骤 4 单击**查看 gcloud 命令 (View gcloud command)** > **在云 Shell 中运行 (Run in Cloud Shell)**。

此时将打开“云 Shell”(Cloud Shell) 终端窗口。有关详细信息，请参阅 Google 文档，gcloud 命令行工具概述 (gcloud command-line tool overview) 和 gcloud compute ssh。



第 7 章

在 Oracle 云基础设施上部署虚拟 Firepower 管理中心

Oracle 云基础设施 (OCI) 是一种公共云计算服务，使您能够在 Oracle 提供的高可用性托管环境中运行应用程序。OCI 通过将 Oracle 的自主服务、集成安全和无服务器计算相结合，为企业应用带来实时弹性。

您可以在 OCI 上部署 Firepower Management Center Virtual (FMCv)。

关于 FMCv 部署和 OCI

Cisco Firepower Management Center Virtual (FMCv) 运行与物理思科 FMC 相同的软件，以虚拟形式提供成熟的安全功能。FMCv 可以部署在公共 OCI 中。然后可以将其配置为管理虚拟和物理 Firepower 设备。

OCI 计算形状

形状是确定分配给实例的 CPU 数量、内存量和其他资源的模板。FMCv支持以下 OCI 形状类型：

表 *11:* 支持的计算形状 *FMCv*

形状类型	属性	
	oCPU	**随机存取存储器(GB)**
VM.Standard2.4	4	60 GB

表 *12: FMCv 300 (7.1.0+)* 支持的计算形状

形状类型	属性	
	oCPU	**随机存取存储器(GB)**
VM.Standard2.16	16	240 GB SSD 存储：2000 GB

注释 支持的形状类型可能会更改，恕不另行通知。

- 在 OCI 中，1 个 oCPU 等于 2 个 vCPU。
- FMCv 需要 1 个接口。

您可在 OCI 上创建帐户，使用 Oracle 云市场上的Cisco Firepower Management Center virtual (FMCv) 产品来启动计算实例，然后选择 OCI 形状。

OCI 上 FMCv 的前提条件

- 在 https://www.oracle.com/cloud/ 创建一个 OCI 帐户。
- 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。
  - 从 Firepower Management Center 配置安全服务的所有许可证授权。
  - 有关如何管理许可证的更多信息，请参阅《Firepower管理中心配置指南》中的“Firepower系统许可”。
- 接口要求：
  - 管理接口 - 用于将 Firepower 威胁防御设备连接到 Firepower 管理中心。
- 通信路径：
  - 用于对 FMCv 进行管理访问的公共 IP。
- 对于 Firepower Management Center Virtual 和 Firepower 系统的兼容性，请参阅《Cisco Firepower兼容性》。

FMCv 和 OCI 的准则和限制

支持的功能

- 在 OCI 虚拟云网络 (VCN) 中部署
- 每个实例最多 8 个 vCPU
- 路由模式（默认）
- 许可 - 仅支持 BYOL
- **FMCv 300 for OCI** - 新的可扩展 FMCv 映像可在支持管理多达 300 设备的 OCI 平台上使用，具有更高的磁盘容量 (7.1.0+)。
- 两种 FMCv 型号均支持 FMCv 高可用性：FMCv 和 FMCv 300 (7.1.0+)。

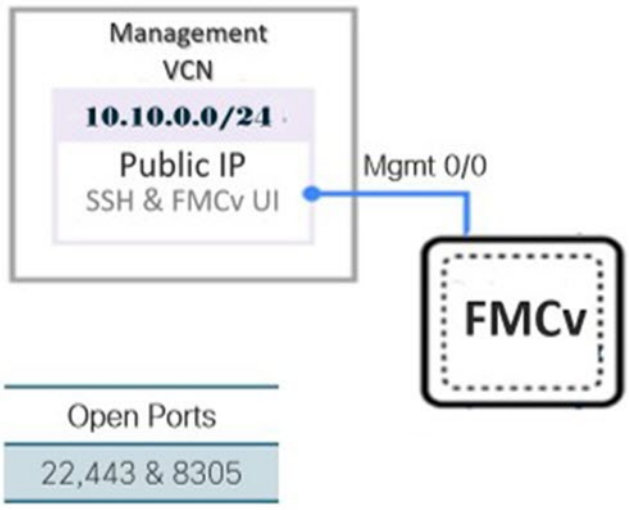
不支持的功能

- IPv6
- 自动缩放
- 透明/内联/被动模式
- 多情景模式

OCI 上 FMCv 的网络拓扑示例

下图说明在 OCI 中配置了 1 个子网的 FMCv 的典型拓扑。

图 *5:* 在 *OCI* 上部署 *FMCv* 的拓扑示例



在 OCI 上部署 FMCv

配置虚拟云网络 (VCN)

您可以为 FMCv 部署配置虚拟云网络 (VCN)。

开始之前

注释 从导航菜单中选择服务后，左侧的菜单包括隔间列表。隔间可帮助您组织资源，以便更轻松地控制对资源的访问。您的根隔间由Oracle在调配租用时为您创建。管理员可以在根隔间中创建更多隔间，然后添加访问规则以控制哪些用户可以在其中查看和执行操作。有关详细信息，请参阅 Oracle 文档“管理隔间”(Managing Compartments)。

步骤 1 登录 OCI 并选择您的区域。

OCI 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 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)**，然后单击**创建 VCN (Create VCN)**。

步骤 3 输入 VCN 的描述性**名称**，例如 *FMCv-Management*。

步骤 4 输入 VCN 的 **CIDR 块**。

步骤 5 单击**创建 VCN (Create VCN)**。

下一步做什么

您可以继续执行以下程序来完成管理 VCN。

创建网络安全组

网络安全组由一组 vNIC 和一组应用于 vNIC 的安全规则组成。

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **网络安全组 (Network Security Groups)**，然后单击**创建网络安全组 (Create Network Security Group)**。

步骤 2 输入网络安全组的描述性**名称**，例如 *FMCv-Mgmt-Allow-22-443-8305*。

步骤 3 单击**下一步 (Next)**。

步骤 4 添加安全规则：

a) 添加规则以允许 TCP 端口 22 用于 SSH 访问。
b) 添加规则以允许 TCP 端口 443 用于 HTTPS 访问。
c) 添加规则以允许 TCP 端口 8305。

可以通过 FMCv 管理 Firepower 设备 FMCv，这需要为 HTTPS 连接打开端口 8305。您需要端口 443 来访问 Firepower 管理中心本身。

步骤 5 单击**创建 (Create)**。

创建互联网网关

要使管理子网可公开访问，则需要互联网网关。

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **互联网网关 (Internet Gateways)**，然后单击**创建互联网网关 (Create Internet Gateway)**。

步骤 2 输入您的互联网网关的描述性**名称**，例如 *FMCv-IG*。

步骤 3 单击**创建互联网网关 (Create Internet Gateway)**。

步骤 4 将路由添加至互联网网关：

a) 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **路由表 (Route Tables)**。
b) 单击默认路由表的链接以添加路由规则。
c) 单击**添加路由规则 (Add Route Rules)**。
d) 从**目标类型 (Target Type)** 下拉列表中，选择**互联网网关 (Internet Gateway)**。
e) 输入目标 CIDR 块，例如 0.0.0.0/0。
f) 从**目标互联网网关 (Target Internet Gateway)** 下拉列表中选择您创建的网关。
g) 单击**添加路由规则 (Add Route Rules)**。

创建子网

每个 VCN 至少有一个子网。您将为管理 VCN 创建一个管理子网。

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **子网 (Subnets)**，然后单击**创建子网 (Create Subnet)**。

步骤 2 输入子网的描述性**名称 (Name)**，例如管理 *(Management)*。

步骤 3 选择**子网类型 (Subnet Type)**（保留建议的默认值**区域 (Regional)**）。

步骤 4 输入**CIDR 块 (CIDR Block)**，例如 10.10.0.0/24。子网的内部（非公共）IP 地址可从此 CIDR 块获取。

步骤 5 从**路由表 (Route Table)** 下拉列表中选择您之前创建的路由表之一。

步骤 6 为您的子网选择**子网访问 (Subnet Access)**。

对于“管理”(Management) 子网，这必须是**公共子网 (Public Subnet)**。

步骤 7 选择 **DHCP 选项 (DHCP Option)**。

步骤 8 选择您之前创建的**安全列表**。

步骤 9 单击**创建子网 (Create Subnet)**。

下一步做什么

配置管理 VCN 后，您便可以启动 FMCv。有关 FMCv VCN 配置的示例，请参见下图。

图 *6: FMCv* 虚拟云网络

在 OCI 上创建 FMCv 实例

您使用 Oracle 云市场上的 Cisco Firepower Management Center Virtual (FMCv) - BYOL 产品通过计算实例在 OCI 上部署 FMCv。您可以根据 CPU 数量、内存量和网络资源等特征来选择最合适的计算机形状。

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**市场 (Marketplace)** > **应用程序 (Applications)**。

步骤 3 在市场中搜索“Cisco Firepower Management Center virtual (FMCv)”并选择产品。

步骤 4 查看条款和条件，然后选中**我已阅读并接受的Oracle使用条款和合作伙伴条款和条件 (I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions)** 复选框。

步骤 5 单击**启动实例 (Launch Instance)**。

步骤 6 输入您的实例的描述性**名称**，例如 *Cisco-FMCv*。

步骤 7 单击**更改形状 (Change Shape)**，然后选择包含 FMCv 所需 CPU 数量、RAM 量和所需接口数量的形状，例如 VM.Standard2.4（请参阅OCI 计算形状，第 63 页）。

步骤 8 从**虚拟云网络 (Virtual Cloud Network)** 下拉列表中选择管理 VCN。

步骤 9 从**子网 (Subnet)** 下拉列表中选择管理子网（如果未自动填充）。

步骤 10 选中**使用网络安全组控制流量 (Use Network Security Groups to Control Traffic)**，然后选择为管理 VCN 配置的安全组。

步骤 11 单击**分配公共 IP 地址 (Assign a Public Ip Address)** 单选按钮。

步骤 12 在**添加 SSH 密钥 (Add SSH keys)** 下，单击**粘贴公共密钥 (Paste Public Keys)** 单选按钮并粘贴 SSH 密钥。

基于 Linux 的实例使用 SSH 密钥对而不是密码来对远程用户进行身份验证。密钥对包括私钥和公共密钥。您可以在创建实例时将私钥保留在计算机上并提供公共密钥。有关准则，请参阅管理 Linux 实例上的密钥对。

步骤 13 单击**显示高级选项 (Show Advanced Options)** 链接以展开选项。

步骤 14 在**初始化脚本 (Initialization Script)** 下，单击**粘贴云初始化脚本 (Paste Cloud-Init Script)** 单选按钮来为 FMCv 提供 day0 配置。day0 配置会在首次引导 FMCv 期间应用。

以下示例显示您可以在**云初始化脚本 (Cloud-Init Script)** 字段中复制和粘贴的示例 day0 配置：

```
{
"AdminPassword": "myPassword@123456",
"Hostname": "cisco-fmcv"
}
```

步骤 15 单击**创建 (Create)**。

下一步做什么

监控 FMCv 实例，单击**创建 (Create)** 按钮后，状态会显示为“正在调配”(Provisioning)。监控状态非常重要。查找要从调配状态转换为运行状态的 FMCv 实例，这表示 FMCv 启动已完成。

在 OCI 上访问 FMCv 实例

您可以使用安全外壳 (SSH) 连接来连接到正在运行的实例。

- 大多数 UNIX 风格的系统均默认包含 SSH 客户端。
- Windows 10 和 Windows Server 2019 系统应包含 OpenSSH 客户端，如果使用 Oracle 云基础设施生成的 SSH 密钥来创建实例，则需要使用此客户端。
- 对于其他 Windows 版本，您可以从 http://www.putty.org 下载免费的 SSH 客户端 PuTTY。

必备条件

您需要以下信息才能连接到实例：

- 产品实例的公共 IP 地址。您可以从控制台的“实例详细信息”(Instance Details) 页面获取地址。打开导航菜单。在**核心基础设施 (Core Infrastructure)**，转到**计算 (Compute)** 并单击**实例 (Instances)**。然后，选择您的实例。或者，您可以使用核心服务 ListVnicAttachments 和 GetVnic 操作。
- 实例的用户名和密码。
- 启动实例时使用的 SSH 密钥对的私钥部分的完整路径。

  有关密钥对的详细信息，请参阅关于 Linux 实例的管理密钥对。

注释 如果选择不添加 Day0 配置，则可以使用默认凭证 (admin/Admin123) 登录到 FMCv 实例。

系统会提示您在首次登录时设置密码。

使用 PuTTY连接到 FMCv 实例

要使用 PuTTY 从 Windows 系统连接到 FMCv 实例，请执行以下操作：

步骤 1 打开 PuTTY。

步骤 2 在**类别 (Category)** 窗格中，选择**会话 (Session)** 并输入以下内容：

- **主机名（或 IP 地址）：**

  <username>@<public-ip-address>

  其中：

  <username> 是 FMCv 实例的用户名。

  <public-ip-address> 是您从控制台检索的实例公共 IP 地址。

- **端口：** 22
- **连接类型：** SSH

步骤 3 在**类别 (Category)** 窗格中，展开**窗口 (Window)**，然后选择**转换 (Translation)**。

步骤 4 在**远程字符集 (Remote character set)** 下拉列表中，选择 **UTF-8**。

基于 Linux 的实例的默认区域设置为 UTF-8，这样会将 PuTTY 配置为使用相同的区域设置。

步骤 5 在**类别 (Category)** 窗格中，依次展开**连接 (Connection)** 和 **SSH**，然后单击**身份验证 (Auth)**。

步骤 6 单击**浏览 (Browse)**，然后选择您的私钥。

步骤 7 单击**打开 (Open)** 以启动会话。

如果这是第一次连接到实例，您可能会看到一条消息，表明服务器的主机密钥未缓存在注册表中。单击**是 (Yes)** 以继续连接。

使用 SSH 连接到 FMCv 实例

要从 Unix 风格的系统连接到 FMCv 实例，请使用 SSH 登录实例。

步骤 1 使用以下命令设置文件权限，以便只有您可以读取文件：

```
$ chmod 400 <private_key>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

步骤 2 使用以下 SSH 命令访问实例。

```
$ ssh  -i <private_key> <username>@<public-ip-address>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

<username> 是 FMCv 实例的用户名。

<public-ip-address> 是您从控制台检索的实例 IP 地址。

使用 OpenSSH 连接到 FMCv 实例

要从 Windows 系统连接到 FMCv 实例，请使用 OpenSSH 登录实例。

步骤 1 如果这是您首次使用此密钥对，则必须设置文件权限，以便只有您能读取文件。

执行以下操作：

a) 在 Windows 资源管理器中，导航至私钥文件，右键单击该文件，然后单击**属性 (Properties)**。
b) 在**安全 (Security)** 选项卡上，单击**高级 (Advanced)**。
c) 确保**所有者 (Owner)** 是您的用户帐户。
d) 单击**禁用继承 (Disable Inheritance)**，然后选择**将此对象的继承权限转换为显式权限 (Convert inherited permissions into explicit permissions on this object)**。
e) 选择不是您的用户帐户的每个权限条目，然后单击**删除 (Remove)**。
f) 确保您的用户帐户的访问权限为**完全控制 (Full control)**。
g) 保存更改。

步骤 2 要连接到实例，请打开 Windows PowerShell 并运行以下命令：

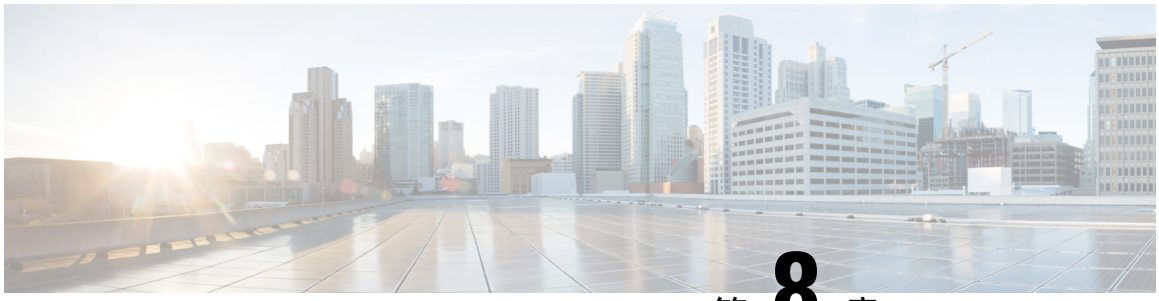
$ ssh -i <private_key> <username>@<public-ip-address>

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

<username> 是 FMCv 实例的用户名。

<public-ip-address> 是您从控制台检索的实例 IP 地址。



第 8 章

使用 OpenStack 部署虚拟 Firepower 管理中心

您可以在 OpenStack 上部署思科 Firepower Management Center Virtual (FMCv)。

关于在 OpenStack 上的 FMCv 部署

本指南介绍如何在 OpenStack 环境中部署 Firepower Management Center Virtual (FMCv)。OpenStack 是一个免费的开放标准云计算平台，主要作为公共服务和私有云中的基础设施即服务 (IaaS) 部署，其中虚拟服务器和其他资源可供用户使用。

FMCv 运行与物理思科 Firepower 管理中心 相同的软件，以虚拟形式提供成熟的安全功能。FMCv 可以部署在 OpenStack 上。然后可以将其配置为管理虚拟和物理 Firepower 设备。

此部署使用 KVM 虚拟机监控程序来管理虚拟资源。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。

由于 KVM 虚拟机监控程序已支持 Firepower 设备，因此无需其他内核软件包或驱动程序即可启用 OpenStack 支持。

FMCv 和 OpenStack 的前提条件

- 从 software.cisco.com 下载 FMCv qcow2 文件并将其放在 Linux 主机上：

  https://software.cisco.com/download/navigator.html

- 需要 software.cisco.com 和思科服务合同。
- FMCv 支持在开源 OpenStack 环境和思科 VIM 托管 OpenStack 环境中进行部署。

  根据 OpenStack 指南来设置 OpenStack 环境。

  - 请参阅开源 OpenStack 文档： https://docs.openstack.org/project-deploy-guide/openstack-ansible/stein/overview.html
  - 请参阅思科虚拟化基础设施管理器 (VIM) OpenStack文档：思科虚拟化基础设施管理器文档，3.4.3 至 3.4.5

- 许可：
  - 您可以在 Firepower 管理中心中配置安全服务的许可证授权。
  - 有关如何管理许可证的更多信息，请参阅《*Firepower* 管理中心配置指南》中的“Firepower 系统许可”。
- 接口要求：
  - 管理接口 - 用于将 Firepower 设备连接到 Firepower 管理中心 的接口。
- 通信路径：
  - 用于访问 FMCv 的浮动 IP。
- 最低支持的 FMCv 版本：
  - Firepower 版本 7.0.
- 有关 OpenStack 要求，请参阅Firepower 部署的 OpenStack 要求 ，第 75 页。
- 对于 Firepower Management Center Virtual 和 Firepower 系统的兼容性，请参阅《Cisco Firepower 兼容性》。

FMCv 和 OpenStack 的准则和限制

支持的功能

OpenStack 上的 FMCv 支持以下功能：

- 在 OpenStack 环境中在计算节点上运行的 KVM 虚拟机监控程序上部署 FMCv。
- OpenStack CLI
- 基于 Heat 模板的部署
- 许可 - 仅支持 BYOL
- 驱动程序 - VIRTIO、VPP 和 SRIOV

不支持的功能

OpenStack 上的 FMCv 不支持以下各项：

- 自动缩放
- OpenStack 版本，而不是 OpenStack Stein 和 Queens 版本
- Ubuntu 18.04 版本和 Red Hat Enterprise Linux (RHEL) 7.6 之外的操作系统

Firepower 部署的 OpenStack 要求

OpenStack 环境必须符合以下支持的硬件和软件要求。

表 *13:* 硬件和软件要求

类别	支持的版本	说明
服务器	UCS C240 M5	建议使用 2 台 UCS 服务器，分别用于 os-controller 和 os-compute 节点。
驱动程序	VIRTIO、IXGBE、I40E	这些是支持的驱动程序。
操作系统	Ubuntu Server 18.04	这是 UCS 服务器上的建议操作系统。
OpenStack 版本	Stein 版本	有关各种 OpenStack 版本的详细信息，请访问： https://releases.openstack.org/

表 *14:* 思科 *VIM* 托管 *OpenStack* 的硬件和软件要求

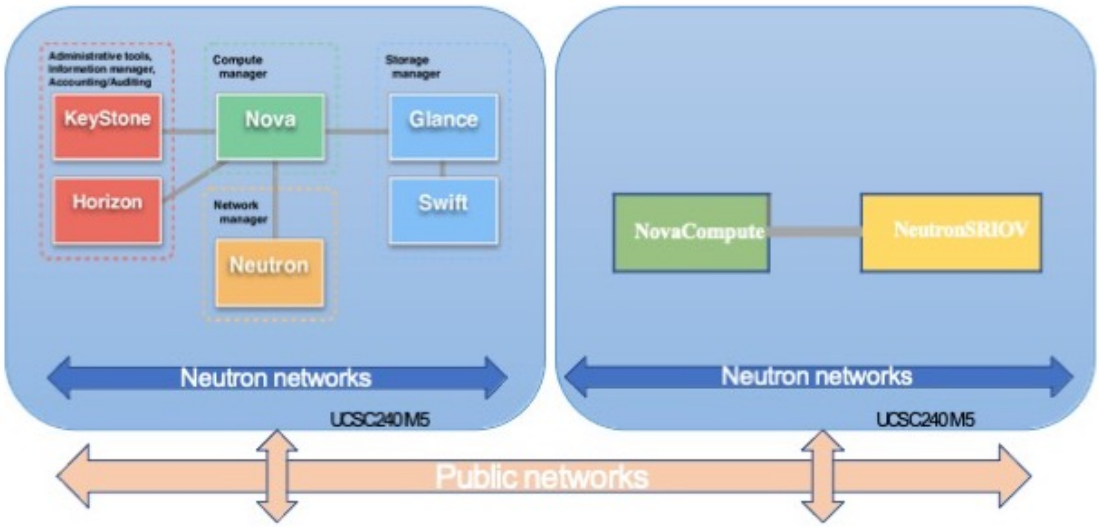
类别	支持的版本	说明
服务器硬件	UCS C220-M5/UCS C240-M4	建议使用 5 台 UCS 服务器，其中 3 台用于 os-controller，两台或更多用于 os-compute 节点。
驱动因素	VIRTIO、SRIOV 和 VPP	这些是支持的驱动程序。
操作系统	Red Hat Enterprise Linux 7.6	这是建议的操作系统。
OpenStack 版本	OpenStack 13.0（Queens 版本）	有关各种 OpenStack 版本的详细信息，请访问： https://releases.openstack.org/

类别	支持的版本	说明
思科 VIM 版本	思科 VIM 3.4.4	请参阅思科 VIM OpenStack 文档。

OpenStack 平台拓扑

下图显示了建议的拓扑，以支持使用两个 UCS 服务器的 OpenStack 中的 Firepower 部署。

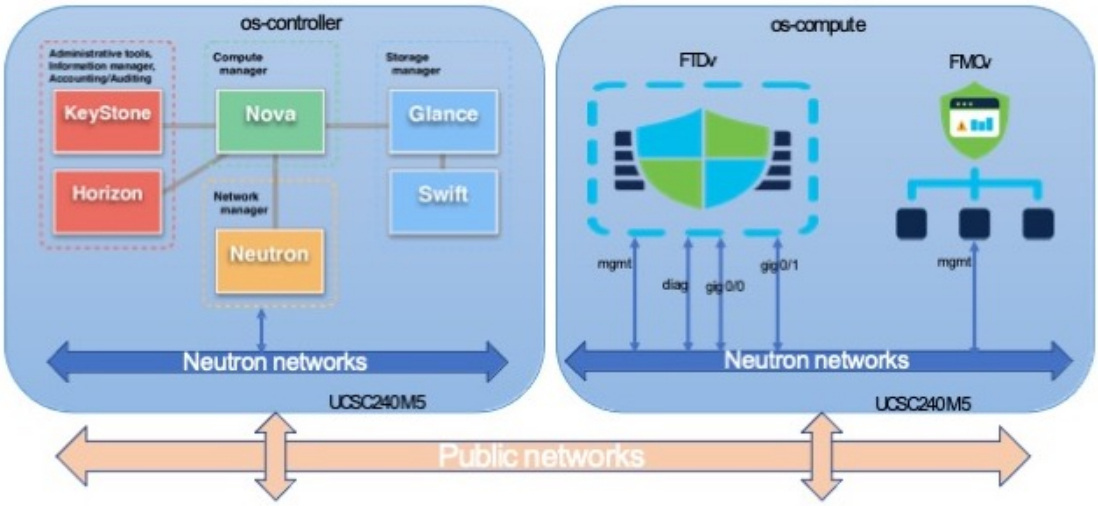
图 *7: OpenStack* 平台拓扑



OpenStack 上 FMCv 的网络拓扑示例

下图显示了 OpenStack 中 FMCv 的的网络拓扑示例。

图 *8: OpenStack* 上使用 *FMCv* 和 *Firepower* 的拓扑示例



在 OpenStack 上部署 FMCv

思科提供用于部署 FMCv 的示例 Heat 模板。创建 OpenStack 基础设施资源的步骤汇总在 Heat 热模板 (`Deploy_os_infra.yaml`) 文件中，以创建网络、子网和路由器接口。总体而言，FMCv 部署步骤分为以下几个部分。

- 将 FMCv qcow2 映像上传到 OpenStack Glance 服务。
- 创建网络基础设施。
  - 网络
  - 子网
  - 路由器接口
- 创建 FMCv 实例。
  - 类型
  - 安全组
  - 浮动 IP
  - 实例

您可以按照以下步骤在 OpenStack 上部署 FMCv。

将 FMCv 映像上传到 OpenStack

将 FMCv qcow2 映像复制到 OpenStack 控制器节点，然后将映像上传到 OpenStack Glance 服务。

开始之前

- 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

步骤 1 将 qcow2 映像文件复制到 OpenStack 控制器节点。

步骤 2 将 FMCv 映像上传到 OpenStack Glance 服务。

```
root@ucs-os-controller:$ openstack image create <fmcv_image> --public --disk-
format qcow2 --container-format bare --file ./<fmcv_qcow2_file>
```

步骤 3 验证 FMCv 映像上传是否成功。

root@ucs-os-controller:$ openstack 映像列表

示例：

```
root@ucs-os-controller:$ openstack image
list+--------------------------------------+------------------+--------+
| ID                                   | Name               | Status
|+--------------------------------------+------------------+--------+
| b957b5f9-ed1b-4975-b226-4cddf5887991 | fmcv-7-0-image | active
|+--------------------------------------+------------------+--------+
```

系统将显示已上传的映像及其状态。

下一步做什么

使用 `deploy_os_infra.yaml` 模板来创建网络基础设施。

为 OpenStack 和 FMCv 创建网络基础设施

部署 OpenStack 基础设施 Heat 模板以创建网络基础设施。

开始之前

需要使用 Heat 模板文件来创建网络基础设施和 FMCv 所需的组件，例如终端、网络、子网、路由器接口和安全组规则：

- `env.yaml` - 定义为支持计算节点上的 FMCv 而创建的资源，例如映像名称、接口和 IP 地址。
- `deploy_os_infra.yaml` -定义 FMCv 的环境，例如网络和子网。

您的 FMCv 版本的模板可从 GitHub 存储库获取：

- https://github.com/CiscoDevNet/cisco-ftdv

重要事项 请注意，思科提供的模板作为开源示例提供，不在常规思科 TAC 支持范围内。定期检查 GitHub 以了解更新和自述文件说明。

步骤 1 部署基础设施 Heat 模板文件。

root@ucs-os-controller:$ openstack stack create <stack-name> -e <environment files name> -t <deployment file name>

示例：

```
root@ucs-os-controller:$ openstack stack create infra-stack -e env.yaml -t deploy_os_infra.yaml
```

步骤 2 验证是否已成功创建基础设施堆栈。

root@ucs-os-controller:$ openstackstack list

示例：

```
root@ucs-os-controller:$ openstack stack list
+--------------------------------------+-----------+----------------------------------+--------------+----------------------+----------
--+
| ID | Stack Name | Project | Stack Status | Creation Time | Updated Time |
+--------------------------------------+-----------+----------------------------------+--------------+----------------------+----------
--+
| b30d5875-ce3a-4258-a841-bf2d09275929 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 | CREATE_COMPLETE
 | 2020-12-07T15:10:24Z | None |
+--------------------------------------+-----------+----------------------------------+--------------+----------------------+----------
--+
```

下一步做什么

在 OpenStack 上创建 FMCv 实例。

在 OpenStack 上创建 FMCv 实例

使用示例 Heat 模板在 OpenStack 上部署 FMCv。

开始之前

在 OpenStack上部署 FMCv 需要 Heat 模板：

- `deploy_fmcv.yaml`

您的 FMCv 版本的模板可从 GitHub 存储库获取：

- https://github.com/CiscoDevNet/cisco-ftdv

重要事项 请注意，思科提供的模板作为开源示例提供，不在常规思科 TAC 支持范围内。定期检查 GitHub 以了解更新和自述文件说明。

步骤 1 部署 FMCv Heat 模板文件 (`Deploy_fmcv.yaml`) 以创建 FMCv 实例。

root@ucs-os-controller:$ openstack stack create fmcv-stack -e env.yaml-t deploy_fmcv.yaml

示例：

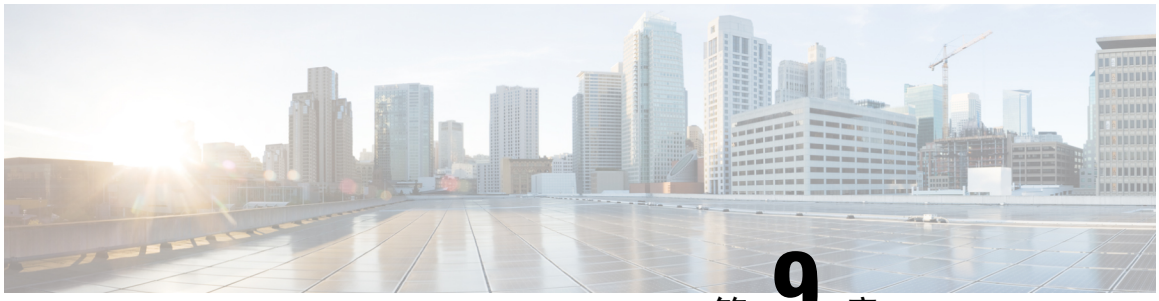
```
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| id                  | 96c8c126-107b-4733-8f6c-eb15a637219f |
| stack_name          | fmcv-stack                           |
| description         | FMCv template                         |
| creation_time       | 2020-12-07T14:55:05Z                 |
| updated_time        | None                                 |
| stack_status        | CREATE_IN_PROGRESS                   |
| stack_status_reason | Stack CREATE started                 |
+---------------------+--------------------------------------+
```

步骤 2 验证是否已成功创建 FMCv 堆栈。

root@ucs-os-controller:$ openstack stack list

示例：

```
+--------------------------------------+------------+----------------------------------+--------------+----------------------+------+
| ID                                   | Stack Name  | Project                          | Stack Status
   | Creation Time    | Updated Time |
+--------------------------------------+------------+----------------------------------+--------------+----------------------+------+
| 14624af1-e5fa-4096-bd86-c453bc2928ae | fmcv-stack  | 13206e49b48740fdafca83796c6f4ad5 | CREATE_COMPLETE
 | 2020-12-07T14:55:05Z | None         |
| 198336cb-1186-45ab-858f-15ccd3b909c8 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 | CREATE_COMPLETE
 | 2020-12-03T10:46:50Z | None         |
+--------------------------------------+------------+----------------------------------+--------------+----------------------+------+
```



第 9 章

使用思科 Hyperflex 部署虚拟 Firepower 管理中心

思科 HyperFlex 系统可为任何应用程序和任何位置提供超融合。通过思科 Intersight 云运营平台管理的 HyperFlex 采用了思科统一计算系统 (Cisco UCS) 技术，可以在任何地方为应用程序和数据提供支持，优化从核心数据中心到边缘和公共云的运营，从而通过加速 DevOps 实践来提高灵活性。

您可以在思科 Hyperflex 上部署 Firepower Management Center Virtual (FMCv)。

主机系统要求

Firepower Management Center Virtual 需要 28 GB RAM

我们建议您不要降低默认设置：为大多数 Firepower Management Center Virtual (FMCv) 实例分配 32 GB RAM，为 FMCv 300 分配 64 GB。为了提高性能，您总是可以根据可用的资源来增加虚拟设备的内存和 CPU 数量。

内存和资源要求

- 您可以通过在 HyperFlex ESX 和 ESXi 虚拟机监控程序上托管的 HyperFlex 集群调配来部署 Firepower Management Center Virtual。有关虚拟机监控程序兼容性的信息，请参阅 Cisco Firepower 兼容性指南。
- 对于 FMCv，查看最新的 Firepower 发行说明，详细了解新版本是否会影响您的环境。您可能需要增加资源才能部署最新版本的 Firepower。
- 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。
- 下表列出 FMCv 设备的建议设置和默认设置。

重要事项 请务必分配足够的内存，以确保的最佳性能FMCv。如果FMCv的内存少于 32 GB，则系统可能会遇到策略部署问题。默认设置是运行系统软件的最低要求，不能降低。

表 *15: FMCv*虚拟设备设置

设置	最小	默认	建议	设置可调节？
内存	28 GB	32 GB	32 GB	有限制。
虚拟 CPU	4	4	8	是，最多 8 个
硬盘调配容量	250 GB	250 GB	不适用	否，取决于所选磁盘格式

表 *16: FMCv300* 虚拟设备设置

设置	默认	设置可调节？
内存	64 GB	是
虚拟 CPU	32	否
硬盘调配容量	2.2 TB	否，取决于所选磁盘格式

有关支持的平台以及特定硬件和操作系统要求的列表，请参阅《兼容性指南》。

思科 HyperFlex 上 Firepower Management Center Virtual 的限制和准则

限制

为思科 HyperFlex 部署 Firepower Management Center Virtual 时存在以下限制：

- FMCv 设备没有序列号。**系统 (System)** > **配置 (Configuration)** 页面会显示**无 (None)** 或**未指定 (Not Specified)**，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。
- 不支持无法识别 OVF 封装的 VMware 工作站、播放器、服务器和 Fusion。

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) OVF 模板部署虚拟设备。OVF 文件的选择取决于部署目标

在 vCenter 上部署 - Cisco_Firepower_Management_Center_Virtual_VMware-**VI**-*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。在安装过程中，您可以执行 FMCv 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。

高可用性支持

您可以在 Hyperflex 主机上部署的两个 Firepower Management Center Virtual (FMCv) 虚拟设备之间建立高可用性 (HA)：

- 两种 FMCv 型号均支持 FMCv HA：FMCv 和 FMCv 300。
- 高可用性配置中的两个 FMCv 虚拟设备型号必须相同。不能将 FMCv 与 FMCv 300 配对。
- 要建立 FMCv HA，FMCv 需要为其在 HA 配置中管理的每个 FTD 设备额外提供 FMCv 许可证授权。但是，无论 FMCv HA 配置如何，每个 FTD 设备所需的 FTD 功能许可证授权都没有变化。有关许可的指南，请参阅《Firepower 管理中心配置指南》中的高可用性对中 *FTD* 设备的许可证要求。
- 如果分开 FMCv HA 对，则会释放额外的 FMCv 许可证授权，并且每个 FTD 设备只需要一个授权。

有关高可用性的指南，请参阅《Firepower 管理中心配置指南》中的建立 *Firepower* 管理中心高可用性。

相关文档

思科 HX 数据平台的版本说明

Cisco HX 数据平台配置指南

适用于采用 VMware ESXi 的虚拟服务器基础设施的思科 HyperFlex 4.0

思科 HyperFlex 系统解决方案概述

思科 HyperFlex 系统文档规划图

在 vSphere vCenter 服务器上将 FMCv 部署到思科 Hyperflex

使用此程序将 Firepower Management Center Virtual (FMCv) 设备部署到 vSphere vCenter 服务器上的思科 Hyperflex。

开始之前

- 确保您已部署思科 HyperFlex 并执行了所有安装后配置任务。有关详细信息，请参阅思科 HyperFlex 系统文档规划图。
- 在部署 FMCv 之前，您必须在 vSphere 中配置至少一个网络（用于管理）。
- 从 Cisco.com 下载 FMCv VI OVF 模板文件：*Cisco_Firepower_Management_Center_Virtual-VI-X.X.X-xxx.ovf*，其中 *X.X.X-xxx* 是版本和内部版本号。

步骤 1 登录 vSphere Web 客户端。

步骤 2 选择要部署 FMCv 的 Hyperflex 集群，然后单击**操作 (ACTIONS)** > **部署 OVF 模板 (Deploy OVF Template)**。

步骤 3 浏览文件系统以找到 OVF 模板源位置，然后单击**下一步 (NEXT)**。

选择 Firepower Management Center Virtual VI OVF 模板：

Cisco_Firepower_Management_Center_Virtual-VI-X.X.X-xxx.ovf

其中，*X.X.X-xxx* 是已下载的存档文件的版本和内部版本号。

步骤 4 指定 FMCv 部署的名称和文件夹，然后单击**下一步 (NEXT)**。

步骤 5 选择计算资源，并等待兼容性检查完成。如果兼容性检查成功，请单击**下一步 (NEXT)**。

步骤 6 查看 OVF 模板信息（产品名称、供应商、版本、下载大小、磁盘上的大小和说明），然后单击**下一步 (NEXT)**。

步骤 7 审查并接受与 OVF 模板一起打包的许可协议（仅限 VI 模板），然后单击**下一步 (NEXT)**。

步骤 8 选择存储位置和虚拟磁盘格式，然后单击**下一步 (NEXT)**。

在此窗口中，您可以从目标 HyperFlex 集群上已配置的数据存储中选择。虚拟机配置文件和虚拟磁盘文件均存储在 Datastore 上。选择一个足够大的数据存储，以容纳虚拟机及其所有虚拟磁盘文件。

如果选择**密集调配 (Thick Provisioned)** 作为虚拟磁盘格式，则会立即分配所有存储。如果选择**精简调配 (Thin Provisioned)** 作为虚拟磁盘格式，则会在数据写入虚拟磁盘时将按需分配存储。精简调配还可缩短虚拟设备的部署时间。

步骤 9 将 OVF 模板中指定的网络映射到清单中的网络，然后单击**下一步 (NEXT)**。

步骤 10 设置与 OVF 模板一起打包的用户可配置的属性：

注释 您必须在此步骤中强制配置所有必需的自定义设置。

a) **Password**

设置 FMCv 管理员访问的密码。

b) **网络**

设置网络信息，包括完全限定的域名 (FQDN)、DNS 和网络协议（IPv4 或 IPv6）。

c) 单击**下一步 (NEXT)**。

步骤 11 查看并验证显示的信息。要使用这些设置开始部署，单击**完成 (FINISH)**。要进行更改，单击**后退 (BACK)** 以在屏幕中向后导航。

完成该向导后，vSphere Web 客户端将处理虚拟机；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。

“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 Cisco Firepower Management Center Virtual，Firepower 管理中心需要互联网访问权限。部署之后，需要执行其他配置，以实现互联网访问和成功注册许可证。许可证注册必须配置 DNS 服务器。

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 17 页

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 (Power)** > **打开电源 (Power On)**。

步骤 2 监控 VM 控制台上的初始化。

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 Hyperflex 上使用 VI 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Firepower Management Center Virtual 初始设置 ， 第 97 页。
- 有关 FMCv 部署所需后续步骤的概述，请参阅Firepower 管理中心虚拟初始管理和配置。

第 10 章

使用 Nutanix 部署虚拟 Firepower 管理中心

Nutanix AHV 是一种本地裸机第 1 类虚拟机监控程序，是具有云功能的超融合基础设施 HCI。

本章介绍了具有 AHV 虚拟机管理程序的 Nutanix 环境中的 FMCv 功能，包括功能支持、系统要求、指南和限制。

您可以在 Nutanix AHV 上部署Firepower 管理中心虚拟 (FMCv)。

主机系统要求

我们建议您不要降低默认设置：为大多数 Firepower 管理中心 (FMCv) 实例分配 32 GB RAM，为 FMCv 300 分配 64 GB。为了提高性能，您总是可以根据可用的资源来增加虚拟设备的内存和 CPU 数量。

内存和资源要求

- 您可以使用 Nutanix AHV 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。有关虚拟机监控程序兼容性的信息，请参阅 Cisco Firepower 兼容性指南。
- 查看最新的Firepower发行说明，详细了解新版本是否会影响您的环境。您可能需要增加资源才能部署最新版本的 Firepower。
- 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。
- 下面列出了 Nutanix AHV 上 FMCv 设备的建议设置和默认设置：
- 处理器
    - 需要 4 个 vCPU

- 内存
  - 最低要求 28 GB RAM/建议（默认）32 GB RAM

重要事项 如果为虚拟设备分配的内存少于 28 GB，则 Firepower 管理中心 (FMCv) 平台会出现故障。

- 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

在 Nutanix 上部署 Firepower Management Center Virtual 的前提条件

Firepower 版本

管理器版本	设备版本
Firepower 设备管理器 7.0	Firepower Threat Defense 7.0
Firepower Management Center Virtual 7.0	

有关 Firepower Threat Defense Virtual 支持的虚拟机管理程序的最新信息，请参阅《Cisco Firepower 兼容性指南》。

从 Cisco.com 下载 Firepower 管理中心 qcow2 文件并将其放在 Nutanix Prism Web 控制台上：

https://software.cisco.com/download/navigator.html

注释 需要 Cisco.com 登录信息和思科服务合同。

Firepower Management Center Virtual许可证

- 从 Firepower Management Center 配置安全服务的所有许可证授权。
- 有关如何管理许可证的更多信息，请参阅《Firepower 管理中心配置指南》中的*Firepower* 系统许可。

Nutanix 组件和版本

组件	版本
Nutanix Acropolis操作系统 (AOS)	5.15.5 LTS 及更高版本
Nutanix 集群检查 (NCC)	4.0.0.1
Nutanix AHV	20201105.12 及更高版本
Nutanix Prism Web 控制台	-

Firepower Management Center Virtual 和 Nutanix 准则和限制

支持的功能

部署模式 - 独立

不支持的功能

Firepower Management Center Virtual 设备没有序列号。**系统 (System)** > **配置 (Configuration)** 页面会显示**无 (None)** 或**未指定 (Not Specified)**，具体取决于虚拟平台。

- 不支持嵌套虚拟机监控程序（运行在 ESXi 上的 Nutanix AHV）。仅支持 Nutanix 独立集群部署。
- 不支持高可用性。
- Nutanix AHV 不支持 SR-IOV 和 DPDK-OVS

相关文档

- Nutanix 发行说明
- Nutanix 现场安装指南
- Nutanix 上的硬件支持

如何在 Nutanix 上部署虚拟 Firepower 管理中心

步骤	任务	更多信息
1	查看先决条件。	在 Nutanix 上部署 Firepower Management Center Virtual 的前提条件，第 88 页
2	将 Firepower Management Center Virtual qcow2 文件上传到 Nutanix 环境。	将虚拟 Firepower 管理中心 QCOW2 文件上传到 Nutanix，第 90 页
3	（可选）准备一个 Day 0 配置文件，其中包含了在部署虚拟机时需要应用的初始配置数据。	准备 Day 0 配置文件，第 91 页
4	将 Firepower Management Center Virtual 部署到 Nutanix 环境。	将虚拟 Firepower 管理中心部署到 Nutanix，第 92 页
5	（可选）如果未使用 Day 0 配置文件来设置 Firepower Management Center Virtual，请通过登录 CLI 完成设置。	完成 FMCv 设置，第 93 页

将虚拟 Firepower 管理中心 QCOW2 文件上传到 Nutanix

要将 FMCv 部署到 Nutanix 环境，则必须在 Prism Web 控制台中从 FMCv qcow2 磁盘文件创建映像。

开始之前

从 Cisco.com 下载 FMCv qcow2 磁盘文件：https://software.cisco.com/download/navigator.html

步骤 1 登录到 Nutanix Prism Web 控制台。

步骤 2 打击齿轮图标打开**设置 (Settings)** 页面。

步骤 3 单击左侧窗格中的**映像配置 (Image Configuration)**。

步骤 4 点击**上传映像 (Upload Image)**。

步骤 5 创建映像。

1. 为映像输入名称。
2. 从**映像类型 (Image Type)** 下拉列表中选择**磁盘 (DISK)**。
3. 从**存储容器 (Storage Container)** 下拉列表中选择所需的容器。
4. 指定 FMCv qcow2 磁盘文件的位置。

   您可以指定 URL（以便从 Web 服务器导入文件）或从工作站上传文件。
5. 单击**保存 (Save)**。

步骤 6 请等待，直到新映像出现在**映像配置 (Image Configuration)** 页面中。

准备 Day 0 配置文件

在部署 FMCv 之前，您可以准备一个 Day 0 配置文件。此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。

请记住：

- 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。
- 如果您在没有 Day 0 配置文件的情况下进行部署，则必须在启动后配置 Firepower 系统所需的设置；有关更多信息，请参阅完成 FMCv 设置，第 93 页。

可以指定：

- 接受《最终用户许可协议》(EULA)。
- 系统的主机名。
- 管理员账户的新管理员密码。
- 使设备可以在管理网络上进行通信的网络设置。

步骤 1 使用您选择的文本编辑器来创建一个新的文本文件。

步骤 2 在文本文件中输入配置详细信息，如下例所示。请注意，文本采用 JSON 格式。您可以在复制文本之前使用验证器工具来验证文本。

示例：

```
#FMC
{
    "EULA": "accept",
    "Hostname": "FMC-Production",
    "AdminPassword": "Admin123",
    "DNS1": "10.1.1.5",
    "DNS2": "192.168.1.67",
    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.45",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "disabled",
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
}
```

步骤 3 将文件另存为“**day0-config.txt**”。

步骤 4 为每个要部署的 FMCv 重复步骤 1-3 以创建唯一的默认配置文件。

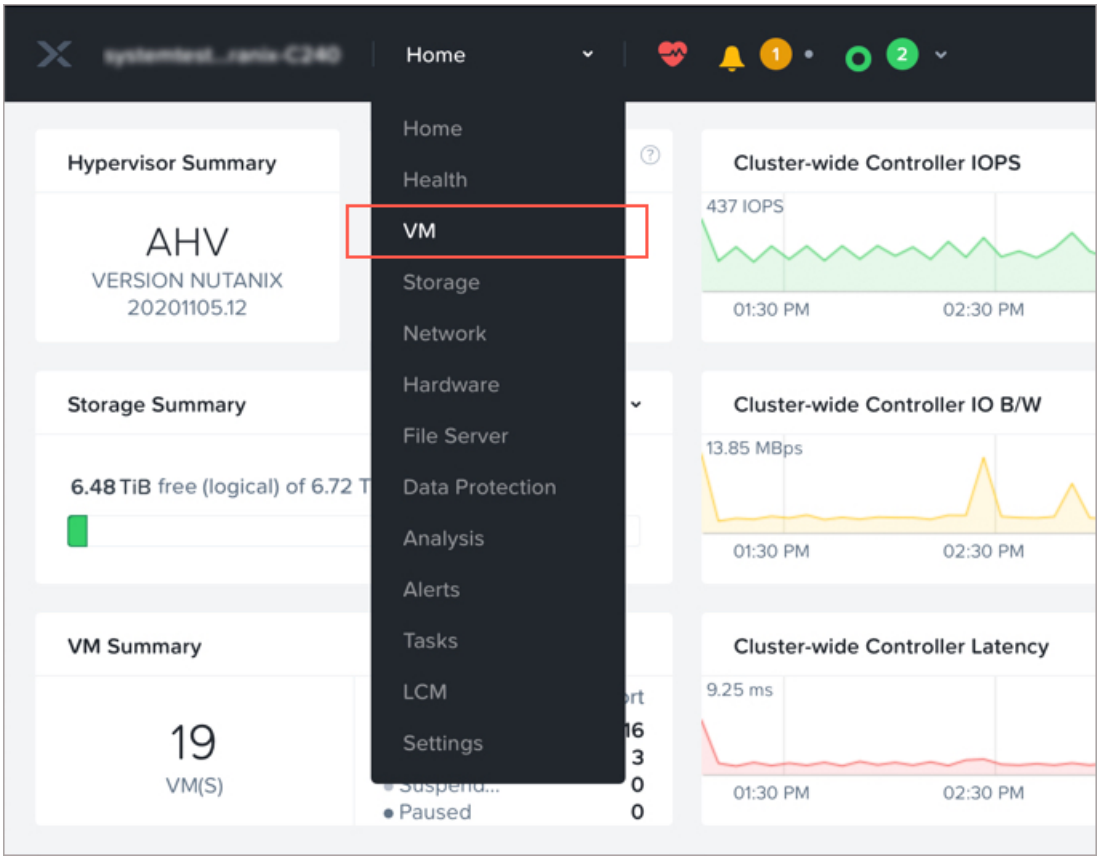
将虚拟 Firepower 管理中心部署到 Nutanix

开始之前

确保您计划部署的 FMCv 的映像显示在**映像配置 (Image Configuration)** 页面上。

步骤 1 登录到 Nutanix Prism Web 控制台。

步骤 2 从主菜单栏中，单击视图下拉列表，然后选择 **VM**。



步骤 3 在 VM 控制面板上，单击**创建 VM (Create VM)**。

步骤 4 执行以下操作：

1. 输入 FMCv 实例的名称。
2. （可选）输入 FMCv 实例的说明。
3. 选择您希望 FMCv 实例使用的时区。

步骤 5 输入计算详细信息。

1. 输入要分配给 FMCv 实例的虚拟 CPU 数量。
2. 输入必须分配给每个虚拟 CPU 的核心数。

3. 输入要分配给 FMCv 实例的内存量 (GB)。

步骤 6 将磁盘连接到 FMCv 实例。

1. 在**磁盘 (Disks)**，单击**添加新磁盘 (Add New Disk)**。
2. 从**类型 (Type)** 下拉列表中选择**磁盘 (DISK)**。
3. 从**操作 (Operation)** 下拉列表中，选择**从映像服务克隆 (Clone from Image Service)**。
4. 从**总线类型 (Bus Type)** 下拉列表中，选择 **SCSI**、**PCI** 或 **SATA**。
5. 从**映像 (Image)** 下拉列表中，选择要使用的映像。
6. 单击**添加 (Add)**。

步骤 7 在**网络适配器 (NIC) (Network Adapters [NIC])** 下，单击**添加新 NIC (Add New NIC)**，选择网络，然后单击**添加 (Add)**。

步骤 8 配置 FMCv 的关联策略。

在 **VM 主机关联 (VM Host Affinity)** 下，单击**设置关联 (Set Affinity)**，选择主机，然后单击**保存 (Save)**。

选择多个主机以确保即使节点出现故障也可运行 FMCv。

步骤 9 如果您已准备了 Day 0 配置文件，请执行以下操作：

1. 选择**自定义脚本 (Custom Script)**。
2. 单击**上传文件 (Upload A File)**，，然后选择 Day 0 配置文件 (**day0-config.txt**)。

注释 此版本中不支持所有其他自定义脚本选项。

步骤 10 单击**保存 (Save)** 以部署 FMCv。FMCv 实例会显示在 VM 表格视图中。

步骤 11 在 VM 表格视图中，选择新创建的 FMCv 实例，然后单击**打开电源 (Power On)**。

步骤 12 在 FMCv 通电后，验证状态。前往**主页 (Home)** > **VM** > 您部署的 FMCv 并登录。

完成 FMCv 设置

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：

步骤 1 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。

步骤 2 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。

步骤 3 使用 CLI 在 FMCv 上完成初始设置。请参阅使用脚本配置网络设置，第 94 页。

步骤 4 使用管理网络上的计算机访问 FMCv 的 Web 界面，完成设置过程。请参阅使用 Web 界面执行初始设置，第 94 页。

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。如果使用的是 Nutanix 控制台，则默认密码为 **Admin123**。

如果系统提示，请重置密码。

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。如果系统提示，请重置密码。

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，单击**应用 (Apply)**。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Firepower Management Center Virtual 初始设置 ， 第 97 页。
- 有关 FMCv 部署所需后续步骤的概述，请参阅Firepower 管理中心虚拟初始管理和配置一章。

第 11 章

Firepower Management Center Virtual 初始设置

本章描述部署Firepower Management Center Virtual (FMCv) 设备之后，需要执行的初始设置过程。

使用 CLI 进行初始设置（6.5 和更高版本）

部署 FMCv 后，您可以i访问设备控制台进行初始设置。作为使用 Web 界面的替代方法，您可以使用 CLI 执行初始设置。您必须完成初始配置向导来配置新设备，以便在受信任的管理网络上进行通信。向导需要您更改管理员密码并接受最终用户许可协议 (EULA) 并更改管理员密码。

开始之前

- 请确保您拥有FMCv 在您的管理网络上通信所需的以下信息：
  - IPv4 管理 IP 地址。

    FMC 管理接口已预配置为接受 DHCP 分配的 IP4 地址。要确定您的 DHCP 已配置什么 IP 地址来分配 FMC MAC 地址，请咨询您的系统管理员。在 DHCP 不可用的情况下，FMC 管理接口使用 IPv4 地址 192.168.45.45。
  - 网络掩码和默认网关（如果不使用 DHCP）。

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

步骤 2 在出现提示时，按 **Enter** 以显示最终用户许可协议 (EULA)。

步骤 3 审查 the EULA。在出现提示时，输入 **yes**、**YES**，或按 **Enter** 接受 EULA。

重要事项 不接受 EULA 您无法继续。如果您回复 **yes**、 **YES** 或 **Enter** 以外的内容，系统会将您注销。

步骤 4 为了确保系统安全和隐私，您第一次登录FMC时，必须更改**admin**密码。当系统提示您设置新密码时，输入符合所示限制的新密码，然后在系统提示确认时再次输入相同的密码。

注释 FMC 会将您的密码与密码破解词典进行比较，该词典不仅会检查许多英语词典单词，还会检查其他容易被常用密码破解技术破解的字符串。例如，初始配置脚本可能会拒绝 "abcdefg" 或 "passw0rd" 等密码。

注释 完成初始配置过程后，系统会将两个 **admin** 帐户（一个用于 Web 访问，另一个用于 CLI 访问）的密码设置为相同的值，符合您版本的《*Firepower* 管理中心配置指南》中所述的强密码要求。如果您在此后更改任一 **admin** 帐户的密码，两个密码将不再相同，并且强密码要求可以从 Web 界面 **admin** 帐户中删除。

步骤 5 回答提示以配置网络设置。

按照提示操作时，如遇单选问题，选项会列在括号内，例如 **(y/n)**。默认值会列在方括号内，例如 **[y]**。回复提示时注意以下要点：

- 按 **Enter** 接受默认值。
- 对于主机名，请提供完全限定域名（<主机名>．<域>）或主机名。此栏必填。
- 如果您选择手动配置 IPv4 ，系统会提示您设置 IPv4 d地址、网络掩码和默认网关。如果您选择 DHCP，系统会使用 DHCP 来分配这些默认值。如果您选择不适用 DHCP，你您必须为这些字段提供值；使用标准点分十进制表示法。
- 可以配置DNS服务器；要指定无DNS服务器，输入**none**。否则，指定一个或两个DNS服务器的IPv4地址。如果指定两个地址，请用逗号将它们分隔开来。（如果指定两台以上的DNS服务器，系统将忽略其他条目。）如果 FMC 不能访问互联网，您将无法使用本地网络之外的 DNS。

  注释 如果使用的是评估许可证，则这一次指定 DNS 是可选操作，但使用永久许可证进行部署时必须有 DNS。

- 您必须输入至少一个通过您网络可到达的完全限定域名 or IP 地址。（如果未使用 DHCP，则不能指定 NTP 服务器的FQDN。）您可以指定两个服务器（一个主服务器，一个辅助服务器）；用逗号将它们的信息分隔开。（如果指定两台以上的 DNS 服务器，系统将忽略其他条目。）如果 FMC 不能访问互联网，您将无法使用本地网络之外的 NTP 服务器。

示例：

```
Enter a hostname or fully qualified domain name for this system [firepower]: fmc
Configure IPv4 via DHCP or manually? (dhcp/manual) [DHCP]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.0.66
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.224
Enter the IPv4 default gateway for the management interface [ ]: 10.10.0.65
Enter a comma-separated list of DNS servers or 'none' [CiscoUmbrella]: 208.67.222.222,208.67.220.220
Enter a comma-separated list of NTP servers [0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org]:
```

步骤 6 系统会显示配置选项的摘要。检查输入的设置。

示例：

```
Hostname:                           fmc
IPv4 configured via:                manual configuration
Management interface IPv4 address:  10.10.0.66
Management interface IPv4 netmask:  255.255.255.224
```

```
Management interface IPv4 gateway:  10.10.0.65
DNS servers:                        208.67.222.222,208.67.220.220
NTP servers:                        0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org
```

步骤 7 最后的提示会让您确认设置。

- 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。系统再次提示设置信息，从主机名开始。

示例：

```
Are these settings correct? (y/n) y
If your networking information has changed, you will need to reconnect.

Updated network configuration.
```

步骤 8 在接受设置后，您可以输入 **exit** 退出 FMC CLI。

下一步做什么

- 您可以使用刚才配置的网络信息连接到 FMCv Web 界面。
- 查看初始配置过程中 FMC 自动配置的每周维护活动。这些活动旨在使系统保持最新状态并备份您的数据。请参阅检查版本6.5 及更高版本的自动初始配置，第 102 页。
- 完成初始设置后，您可以使用 Web 界面配置 FMC 的 IPv6 地址如您版本的《Firepower 管理中心配置指南》。

在 Web 界面上执行初始设置（6.5 和更高版本）

在部署 FMCv 后，则可以在设备 Web 界面上使用 HTTPS 执行初始设置。

第一次登录 FMC Web 界面时，FMC 将显示初始配置向导，可让您快速轻松地配置设备的基本设置。此向导包含三个屏幕和一个弹出对话框：

- 第一个屏幕会强制您将 **admin** 用户的密码从默认值 **Admin123** 改为其他密码。
- 第二个屏幕显示最终用户许可协议 (EULA)，必须接受该协议才能使用设备。
- 第三个屏幕允许您更改设备管理接口的网络设置。此页面预先填充了当前设置，您可以更改。
- 向导将对您在此屏幕上输入的值执行验证，以确认以下内容：
  - 语法正确性
  - 输入值的兼容性（例如，在使用 FQDN 指定 NTP 服务器时提供的兼容 IP 地址和网关或 DNS）
  - FMCv 与 DNS 和 NTP 服务器之间的网络连接

向导会在屏幕上实时显示这些测试的结果，您可以先更正并测试配置的可行性，再单击屏幕底部的**完成**。NTP 和 DNS 连接测试无阻塞；在向导完成连接测试之前，您可以单击**完成**。如果系统在单击**完成**后报告连接问题，则无法更改向导中的设置，但在完成初始设置后，您可以使用 Web 界面配置这些连接。

如果您输入的配置值会导致 FMCv 和浏览器之间的现有连接中断，系统不会执行连接测试。在这种情况下，向导不会显示 DNS 或 NTP 的连接状态信息。

- 在三个向导屏幕上完成操作后，系统会弹出一个对话框，您可以快速轻松地在该对话框中设置智能许可。

如版本对应的《Firepower Management Center 配置指南》中的“设备管理基础知识”中所述，当完成初始配置向导并完成或消除“智能许可”对话框后，系统将显示设备管理页面。

开始之前

- 请确保您拥有 FMC 在您的管理网络上通信所需的以下信息：
  - IPv4 管理 IP 地址。

    FMC 管理接口已预配置为接受 DHCP 分配的 IP4 地址。要确定您的 DHCP 已配置什么 IP 地址来分配 FMC MAC 地址，请咨询您的系统管理员。在 DHCP 不可用的情况下，FMC 管理接口使用 IPv4 地址 192.168.45.45。
  - 网络掩码和默认网关（如果不使用 DHCP）。
- 如果未使用 DHCP，请使用以下网络设置配置本地计算机：
  - IP 地址：192.168.45.2
  - 子网掩码：255.255.255.0
  - 默认网关：192.168.45.1

  禁用此计算机上的任何其他网络连接。

步骤 1 使用网络浏览器导航到 FMCvIP 地址：*https://<FMC-IP>*。

随即显示登录页面。

步骤 2 使用以下管理员帐户登录到 FMCv：用户名 **admin**，密码 **Admin123**。密码区分大小写。

步骤 3 在**更改密码**屏幕：

a) （可选）选中**显示密码**复选框可在使用此屏幕时查看密码。

b) 单击**生成密码**按钮，让系统为您创建符合所列条件的密码。（生成的密码是非助记密码；如果您选择此选项，请仔细记下密码。）

c) 要设置您选择的密码，在**新密码 (New Password)** 和**确认密码 (Confirm Password)** 文本框中输入新密码。

密码必须符合对话框中列出的条件。

注释　FMC 会将您的密码与密码破解词典进行比较，该词典不仅会检查许多英语词典单词，还会检查其他容易被常用密码破解技术破解的字符串。例如，初始配置脚本可能会拒绝 "abcdefg" 或 "passw0rd" 等密码。

注释　完成初始配置过程后，系统会将两个 **admin** 帐户（一个用于 Web 访问，另一个用于 CLI 访问）的密码设置为相同的值。密码必须符合版本对应《Firepower Management Center 配置指南》中所述的强密码要求。如果您在此后更改任一 **admin** 帐户的密码，两个密码将不再相同，并且强密码要求可以从 Web 界面 **admin** 帐户中删除。

d) 单击**下一步**。

在**更改密码**屏幕上单击**下一步**后，向导已接受新的 **admin** 密码，即使您未完成剩余的向导活动，该密码也对 Web 界面和 CLI **admin** 帐户有效。

步骤 4 在**用户协议**屏幕阅读 EULA，然后单击**接受**继续。

如果单击**拒绝**，向导会将您从 FMCv 中注销。

步骤 5 单击**下一步**。

步骤 6 在**更改网络设置**屏幕：

a) 输入**完全限定域名**。如果显示默认值，并且与您的网络配置兼容，则您可以使用该值。否则，输入完全限定域名（语法<主机名>.<域>）或主机名。

b) 选择**配置 IPv4 (Configure IPv4)** 选项的引导协议：**使用 DHCP (Using DHCP)** 或**使用静态/手动 (Using Static/Manual)**。

c) 对于 **IPv4 地址**，接受显示的值（如果显示），或输入新值。使用点分十进制格式（例如 192.168.45.45）。

注释　如果在初始配置期间更改 IP 地址，则需要使用新的网络信息重新连接到 FMC。

d) 接受显示的**网络掩码**值（如果有显示）或输入新值。使用点分十进制格式（例如 255.255.0.0）。

注释　如果在初始配置期间更改网络掩码，则需要使用新的网络信息重新连接到 FMC。

e) 您可以接受显示的**网关**值（如果有显示）或输入新的默认网关。使用点分十进制格式（例如 192.168.0.1）。

注释　如果在初始配置期间更改网关地址，则可能需要使用新的网络信息重新连接到 FMC。

f) （可选）对于**DNS 组**接受默认值 **Cisco Umbrella DNS**。

要更改 DNS 设置，从下拉列表中选择**自定义 DNS 服务器 (Custom DNS Servers)**，然后输入**主 DNS (Primary DNS)** 和**辅助 DNS (Secondary DNS)** 的 IPv4 地址。如果 FMC 不能访问互联网，您将无法使用本地网络之外的 DNS。从下拉列表中选择**自定义 DNS 服务器 (Custom DNS Servers)**，并将**主 DNS (Primary DNS)** 和**辅助 DNS (Secondary DNS)** 字段留空，不配置 DNS 服务器。

注释　如果使用 FQDN 而不是 IP 地址来指定 NTP 服务器，则必须在此时指定 DNS。如果您使用评估许可证，则 DNS 是可选的，但需要 DNS 才能使用永久许可证进行部署。

g) 对于 **NTP 组服务器**，您可以接受默认值**默认 NTP 服务器**。在这种情况下，系统会将 **0.sourcefire.pool.ntp.org** 用作主 NTP 服务器，将 **1.sourcefire.pool.ntp.org** 用作辅助 NTP 服务器。

要配置其他 NTP 服务器，从下拉列表中选择**自定义 NTP 组 服务器 (Custom NTP Group Servers)**，然后输入一个或两个从您的网络可到达的 FQDN 或 IP 地址。如果 FMC 不能访问互联网，您将无法使用本地网络之外的 NTP 服务器。

注释 如果在初始配置期间更改网络设置，则需要使用新的网络信息重新连接到 FMC。

步骤 7 单击**完成**。

向导会对您在此屏幕上输入的值，以确认语法正确性、输入值的兼容性，以及 FMC 和 DNS 及 NTP 服务器之间的连接性。如果系统在单击**完成**后报告连接问题，则无法更改向导中的设置，但在完成初始设置后，您可以使用FMC Web 界面配置这些连接。

下一步做什么

- 系统会显示弹出对话框，您可以快速、轻松地设置 Smart Licensing。此对话框供选择性使用；如果您的 FMCv 将管理 Firepower 威胁防御设备，并且您熟悉智能许可，请使用此对话框。否则，请关闭此对话框，并参阅您版本的《Firepower 管理中心配置指南》中的“许可 Firepower 系统”。
- 查看初始配置过程中 FMC 自动配置的每周维护活动。这些活动旨在使系统保持最新状态并备份您的数据。请参阅检查版本6.5 及更高版本的自动初始配置，第 102 页。
- 如版本对应的《*Firepower Management Center* 配置指南》中所述，当完成初始配置向导并完成或消除“智能许可”对话框后，系统将显示设备管理页面。
- 完成初始设置后，您可以使用 Web 界面配置 FMC 的 IPv6 地址如您版本的《Firepower 管理中心配置指南》。

检查版本6.5 及更高版本的自动初始配置

在初始化配置期间（无论是通过初始配置向导还是通过 CLI 执行），FMC 都会自动配置维护任务，使系统保持最新状态并持续备份您的数据。

这些任务计划为 UTC，这意味着在本地发生时，取决于日期和您的特定位置。此外，由于任务是以 UTC 为单位进行计划的，因此它们不会针对夏令时、夏季时间或您在地点可能观察到的任何季节性调整进行调整。如果受影响，则根据当地时间，计划任务会在夏天比冬季“晚”一个小时开始。

注释 我们强烈 建议您查看自动安排的配置，确认 FMC 已成功建立这些配置，并在必要时进行调整。

- 每周 GeoDB 更新

  FMC 会自动安排每周在同一随机选择的时间进行 GeoDB 更新。您可以使用 Web 界面消息中心观察此更新的状态。您可以在 **系统** > **更新** > **地理位置更新**>**周期性地理位置更新**下看到此自动

更新的配置。如果系统无法配置更新，并且您的FMC有互联网访问权限，我们建议您根据您的版本对应的《Firepower 管理中心配置指南》中所述，配置常规 GeoDB 更新。

- 每周 FMC 软件更新

  FMC 会自动安排每周任务，以下载 FMC 及其托管设备的最新软件。此任务计划在 UTC 星期天凌晨 2 点至 3 点之间进行； 根据日期和您的特定位置，这可能在当地时间星期六下午至星期日下午的任何时间发生。您可以使用 Web 界面消息中心观察此任务的状态。您可以在 **系统** > **工具** > **计划** 下的 Web 界面中看到此任务的配置。如果任务安排失败，并且您的 FMC 有互联网访问权限，我们建议您根据您的版本对应的《Firepower 管理中心配置指南》中所述，安排一项周期性任务来下载软件更新。

  此任务仅下载设备当前正在运行的版本的软件修补程序和修补程序更新；您有责任安装此任务下载的所有更新。有关详细信息，请参阅思科《*Firepower* 管理中心升级指南》。

- 每周 FMC 配置备份

  FMC 会自动安排每周任务，在 UTC 星期一的早上凌晨 2 点执行本地存储的仅配置备份；根据日期和您的具体位置，这可能发生在当地时间星期六下午至星期日下午的任何时间。您可以使用 Web 界面消息中心观察此任务的状态。您可以在 **系统** > **工具** > **计划** 下的 Web 界面中看到此任务的配置。如果任务安排失败，我们建议您根据您的版本对应的《Firepower 管理中心配置指南》中所述，安排一项周期性任务来执行备份。

- 漏洞数据库更新

  在版本 6.6+ 中，FMC 从 Cisco 支持站点下载并安装最新的漏洞数据库 (VDB) 更新。这是一次性操作。您可以使用 Web 界面消息中心观察此更新的状态。您可以在 **系统** > **工具** > **计划** 下的 Web 界面中看到此任务的配置。注：根据 Luu Vo 称，系统团队未来将以增强功能的形式实施此特性；请在 6.6 中将其注释掉。（CLR 3/24/20）为使系统保持最新状态，如果 FMC 能够访问互联网，我们建议按照版本对应的 Firepower Management Center 配置指南中所述，安排任务以自动执行周期性 VDB 更新下载和安装。

- 每日入侵规则更新

  在版本 6.6+ 中，FMC 从 Cisco 支持站点配置每日自动入侵规则更新。当 FMC 下一次部署受影响的策略时，将向受影响的受管设备部署自动化入侵规则更新。您可以使用 Web 界面消息中心观察此任务的状态。您可以在 **系统** > **更新** > **规则更新** 下的 Web 界面中看到此任务的配置。如果配置更新失败，并且您的 FMC 能够访问互联网，我们建议按照版本对应的 Firepower Management Center 配置指南中所述，配置定期入侵规则更新。

第 12 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**帐户（和管理员角色），以保障安全，便于审计。在 FMC GUI 的**系统 (System)** > **用户 (Users)** > **用户 (User)**页面管理用户账户。

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

为使用系统的每个人创建独立帐户，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 Threat Defense- 提供统一的下一代防火墙和下一代 IPS 设备。
- Firepower Threat Defense Virtual- 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。

要注册托管设备到 FMC，使用 FMC GUI 的**设备 (Devices)** > **设备管理 (Device Management)** 页面；请参阅您的版本对应的《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。

如果您的 FMC 运行的是 6.5 版以上的 Firepower：

作为配置的一部分，FMC 建立以下活动以保持系统处于最新状态，并持续备份您的数据：

- 每周自动更新 GeoDB
- 为 FMC 及其托管设备下载最新软件的每周任务

重要事项 此任务仅将软件更新下载到FMC。您负责安装此任务下载的任何更新。有关详细信息，请参阅思科《*Firepower* 管理中心升级指南》。

- 执行本地存储的仅配置 FMC 备份的每周任务

如果您的 FMC 运行 Firepower 版本 6.6+，则作为初始配置的一部分，FMC 会从 Cisco 支持站点下载并安装最新漏洞 (VDB) 更新。这是一次性操作。

您可以使用 Web 界面消息中心观察这些活动的状态。如果系统无法配置任何活动，并且您的 FMC 有互联网访问权限，我们建议您根据您的版本对应的《*Firepower* 管理中心配置指南》中所述，自行配置这些活动。