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 *1: 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 6 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 6 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32GB，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 *2: 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 *3: 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 *4: VMware OFV* 模板设置

设置	ESXi 或 VI	操作
导入/部署 OVF 模板 (Import/Deploy OVF Template)	两者	浏览至您从 Cisco.com 下载的 OVF 模板。
OVF 模板详细信息 (OVF Template Details)	两者	确认您要安装的设备 (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。

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 9 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 11 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 11 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。
- 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。