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 10 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 7 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 5 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 7 页。
- 使用 OpenStack - 使用 OpenStack 环境启动 FMCv；请参阅使用 OpenStack 启动，第 8 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。
- 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。