



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，第 1 页](#)
- [FMCv 和 OpenStack 的前提条件，第 1 页](#)
- [FMCv 和 OpenStack 的准则和限制，第 2 页](#)
- [Firepower 部署的 OpenStack 要求，第 3 页](#)
- [OpenStack 上 FMCv 的网络拓扑示例，第 4 页](#)
- [在 OpenStack 上部署 FMCv，第 5 页](#)

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。

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 3 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 1: 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 2: 思科 VIM 托管 OpenStack 的硬件和软件要求

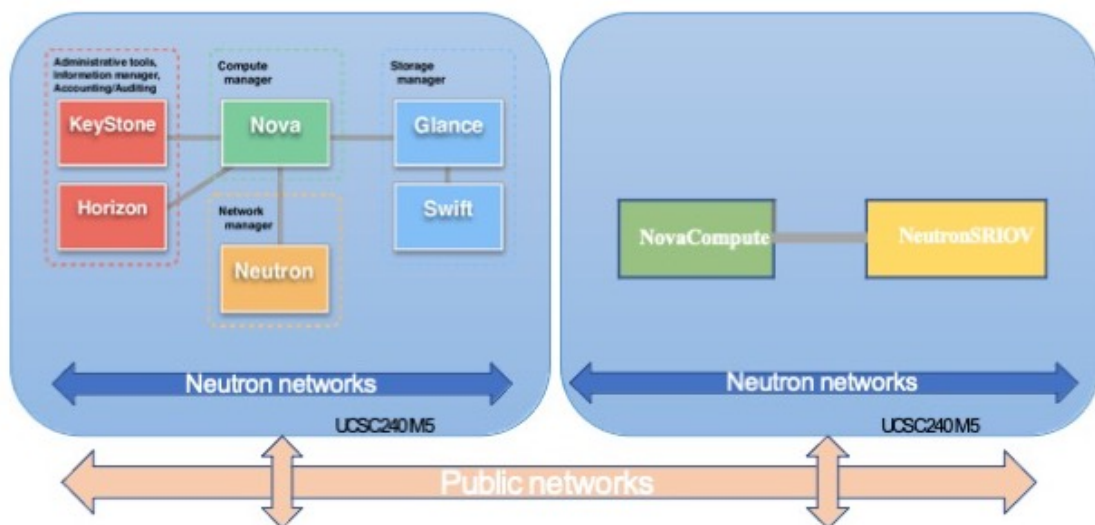
类别	支持的版本	说明
服务器硬件	UCS C220-M5/UCS C240-M4	建议使用 5 台 UCS 服务器，其中 3 台用于 os-controller，两台或更多用于 os-compute 节点。
驱动因素	VIRTIO、SRIOV 和 VPP	这些是支持的驱动程序。
操作系统	Red Hat Enterprise Linux 7.6	这是建议的操作系统。
OpenStack 版本	OpenStack 13.0 (Queens 版本)	有关各种 OpenStack 版本的详细信息，请访问： https://releases.openstack.org/

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。

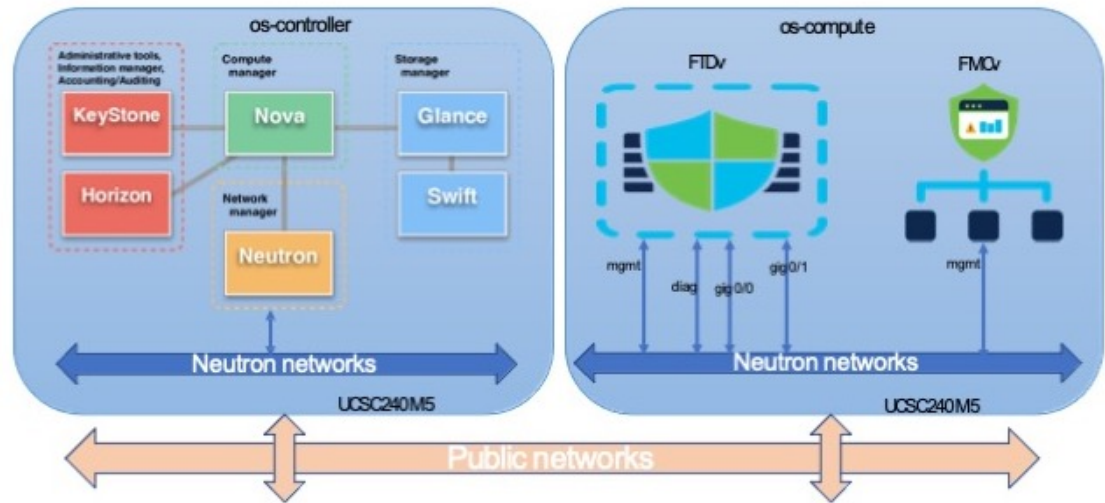
图 1: OpenStack 平台拓扑



OpenStack 上 FMCv 的网络拓扑示例

下图显示了 OpenStack 中 FMCv 的网络拓扑示例。

图 2: 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              | Creation Time | Updated Time | Stack Name | Project | Stack Status |
+-----+-----+-----+-----+-----+-----+
| 14624af1-e5fa-4096-bd86-c453bc2928ae | 2020-12-07T14:55:05Z | None | fmcv-stack | 13206e49b48740fdafca83796c6f4ad5 | CREATE_COMPLETE |
| 198336cb-1186-45ab-858f-15ccd3b909c8 | 2020-12-03T10:46:50Z | None | infra-stack | 13206e49b48740fdafca83796c6f4ad5 | CREATE_COMPLETE |
+-----+-----+-----+-----+-----+-----+
```