在 OpenStack 上部署 Firewall Threat Defense Virtual

概述

本指南介绍如何在 OpenStack 环境中部署 Firewall Threat Defense Virtual。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。

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）。

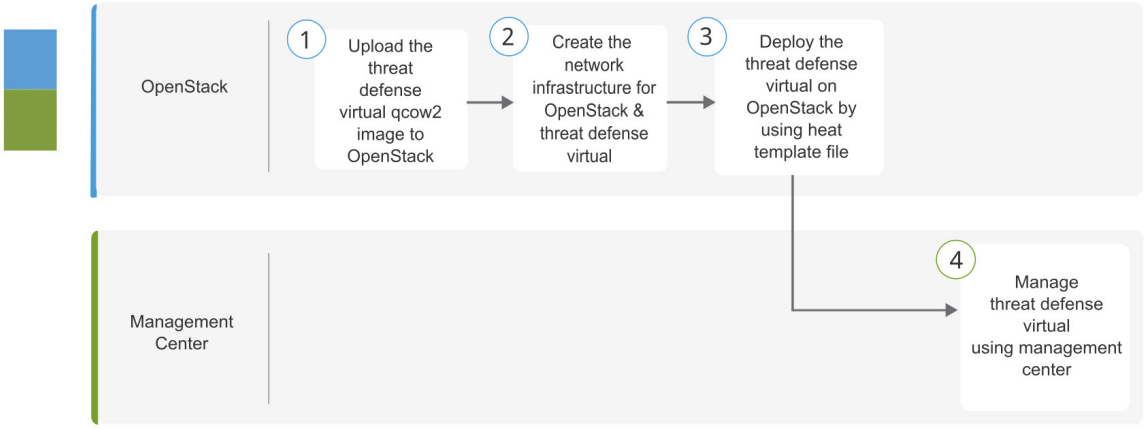
您可以使用 KVM 来运行多个运行未修改的操作系统映像的虚拟机。每个虚拟机都有专用的虚拟化硬件：网卡、磁盘、图形适配器等等。

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。

注释　OpenStack 上的 Firewall Threat Defense Virtual 可以安装在任何优化的多节点环境中。

端到端程序

以下流程图说明了在 OpenStack 上部署 Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	OpenStack	在 OpenStack 上部署 Threat Defense Virtual：将 Threat Defense Virtual 映像上传到 OpenStack。
2	OpenStack	在 OpenStack 上部署 Threat Defense Virtual：为 OpenStack 和 Threat Defense Virtual 创建网络基础设施。
3	OpenStack	在 OpenStack 上部署 Threat Defense Virtual：使用 Threat Defense Virtual Heat 模板文件在 OpenStack 上部署 Threat Defense Virtual。
4	管理中心	使用管理中心管理 Threat Defense Virtual

前提条件

- 从 software.cisco.com 获取 qcow2 Firewall Threat Defense Virtual 映像。
- Firewall Threat Defense Virtual支持在开放源码 OpenStack 环境和思科 VIM 托管 OpenStack 环境中进行部署。

  根据 OpenStack 准则来设置 OpenStack 环境。

  - 请参阅开放源码 OpenStack 文档：

    Caracal 版本 - https://docs.openstack.org/project-deploy-guide/openstack-ansible/2024.1/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，4.4.3

- 思科智能账户。您可以在 Cisco 软件中心创建一个。
- 许可 Firewall Threat Defense Virtual。
  - 所有安全服务的许可证授权均在 防火墙管理中心中配置。
  - 有关如何管理许可证的详细信息，请参阅《 *Cisco Secure Firewall Management Center* 管理指南》中的“许可”。
- 接口要求：
  - 管理接口 (2) - 一个用于将 Firewall Threat Defense Virtual 连接到 防火墙管理中心，另一个用于诊断；无法用于直通流量。
  - 内部和外部接口 - 用于将 Firewall Threat Defense Virtual 连接到内部主机和公共网络。
- 通信路径：
  - 用于访问 Firewall Threat Defense Virtual 的浮动 IP。
- 最低支持的 Firewall Threat Defense Virtual 版本：
  - 版本 7.0
- 有关 OpenStack 要求，请参阅系统要求，第 5 页。
- 有关 Firewall Threat Defense Virtual 和系统兼容性，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。

准则和限制

支持的功能

OpenStack 上的 Firewall Threat Defense Virtual 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 Firewall Threat Defense Virtual。
- OpenStack CLI
- 基于 Heat 模板的部署
- OpenStack Horizon 控制面板
- IPv6
- 高可用性

- 许可 - 仅支持 BYOL
- 仅使用 防火墙管理中心 来管理 Firewall Threat Defense Virtual。
- 驱动程序 - virtIO 和 SR-IOV

Firewall Threat Defense Virtual 智能许可的性能层

Firewall Threat Defense Virtual 支持性能层许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

表 *1:* 基于授权的 ***Firewall Threat Defense Virtual*** 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5	4 核/8 GB	100Mbps	50
FTDv10	4 核/8 GB	1Gbps	250
FTDv20	4 核/8 GB	3 Gbps	250
FTDv30	8 核/16 GB	5Gbps	250
FTDv50	12 核/24 GB	10Gbps	750
FTDv100	16 核/32 GB	16Gbps	10,000

请参阅《*Cisco Secure Firewall Management Center* 管理员指南》中的“许可”一章，了解在许可 Firewall Threat Defense Virtual 设备时的准则。

性能优化

为实现 Firewall Threat Defense Virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅 OpenStack 上的虚拟化调整和优化。

接收端扩展 - Firewall Threat Defense Virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

部署

运行版本 7.4.3 或更高版本的 Threat Defense Virtual 实例会在首次启动期间执行多项初始化任务，这会导致控制台在大约五分钟后可用。这种延迟是正常的。如果设备在首次启动后大约两分钟内关闭，重要的初始化步骤可能会中断，从而可能导致设置不完整和意外行为。

要解决此问题，必须使用新映像重新安装虚拟平台。

Snort

- 如果您观察到异常行为，例如 Snort 需要很长时间才能关闭，或者 VM 通常缓慢，或者在执行某个进程时，请从 Firewall Threat Defense Virtual 和 VM 主机收集日志。收集总体 CPU 使用情况、内存、I/O 使用情况和读/写速度日志将有助于对问题进行故障排除。
- 当 Snort 关闭时，观察到高 CPU 和 I/O 使用率。如果在内存不足且没有专用 CPU 的单个主机上创建了大量 Firewall Threat Defense Virtual 实例，则 Snort 将需要很长时间才能关闭，这将导致创建 Snort 核心。

不支持的功能

OpenStack 上的 Firewall Threat Defense Virtual 不支持以下各项：

- Autoscale
- 集群

升级限制和局限性

恢复升级限制

⚠

注意 不支持恢复升级。

确保在升级前进行备份。升级到 Threat Defense Virtual 10.0.0 后，您无法回滚到以前的软件版本。要返回到较早的版本，必须重新部署管理中心。

系统要求

OpenStack 环境必须符合以下支持的硬件和软件要求。

表 *2:* 开源 *OpenStack* 的硬件和软件要求

类别	支持的版本	说明
服务器硬件	UCS C240 M5	建议使用 2 台 UCS 服务器，分别用于 os-controller 和 os-compute 节点。
驱动因素	VIRTIO、IXGBE 和 I40E	这些是支持的驱动程序。
操作系统	Ubuntu Server 22.04	这是 UCS 服务器上的建议操作系统。

类别	支持的版本	说明
OpenStack 版本	Caracal 版本	有关各种 OpenStack 版本的详细信息，请访问： https://releases.openstack.org/

Threat Defense Virtual 软件版本和支持的操作系统：

- **对于 Threat Defense Virtual 版本 10.0 (Caracal)：**

  Caracal 版本支持在以下操作系统上进行部署：

  - Ubuntu 20.04、22.04 和 24.04
  - RHEL 版本 8.4，带有 CVIM/HVIM 版本：5.0.3

- **对于 7.2.9 之前的 Threat Defense Virtual 版本 (Wallaby)：**

  Wallaby 版本支持在以下位置部署：

  - Ubuntu 20.04
  - RHEL 版本 8.4，带有 CVIM/HVIM 版本：5.0.3

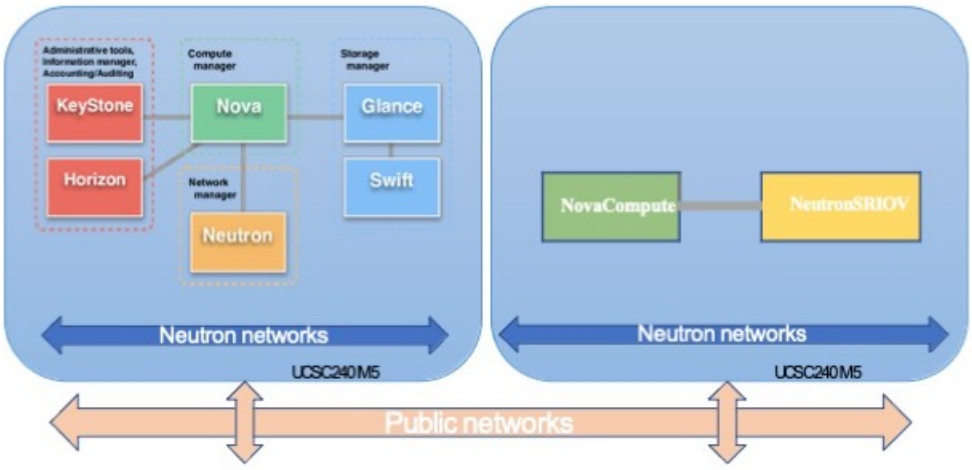
表 *3:* 思科 *VIM* 托管 *OpenStack* 的硬件和软件要求

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、IXGBE 和 I40E	这些是支持的驱动程序。
思科 VIM 版本	思科 VIM 4.4.3 支持的型号： • 操作系统 - Red Hat Enterprise Linux 8.4 • OpenStack 版本 - OpenStack 16.2（培训版本）	有关详细信息，请参阅思科虚拟化基础设施管理器文档 4.4.3。

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 中的部署。

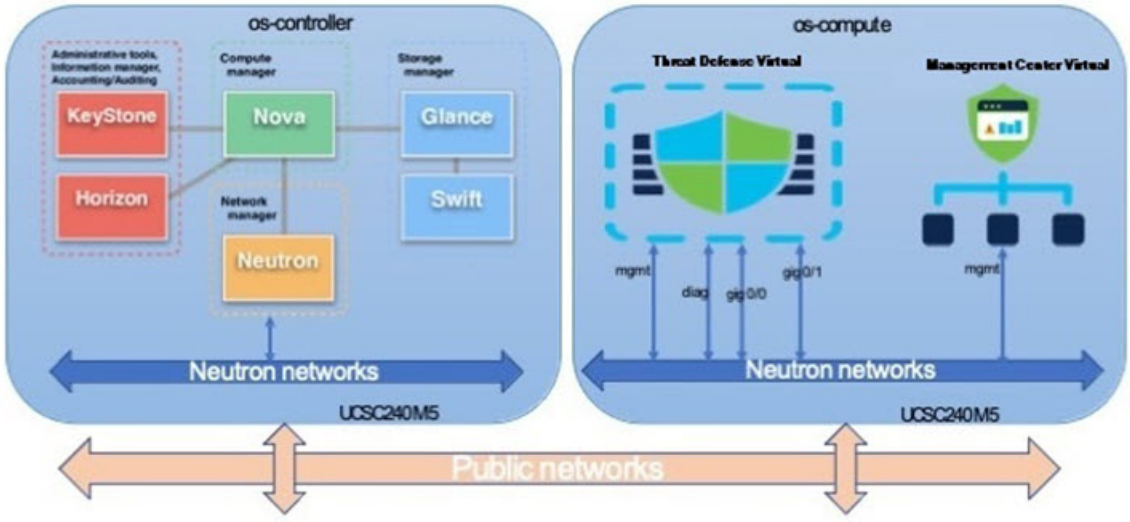
图 *1: OpenStack* 平台拓扑



OpenStack 上 Firewall Threat Defense Virtual 的网络拓扑示例

下图显示了在路由防火墙模式下 Firewall Threat Defense Virtual 的网络拓扑示例，在 OpenStack 中为 Firewall Threat Defense Virtual 配置了 4 个子网（管理、诊断、内部和外部）。

图 *2: OpenStack* 上使用 *Firewall Threat Defense Virtual* 和 *Firewall Management Center Virtual* 的拓扑示例



如何管理 Secure Firewall Threat Defense Virtual 设备

您有两个选择来管理您的 Secure Firewall Threat Defense Virtual。

Secure Firewall Management Center

如果要管理大量设备或要使用 Firewall Threat Defense 支持的更复杂的功能和配置，请使用 防火墙管理中心（而不是集成的 防火墙设备管理器）来配置您的设备。有关详细信息，请参阅使用 Secure Firewall Management Center 来管理 Secure Firewall Threat Defense Virtual

重要事项 您不能同时使用 防火墙设备管理器 和 防火墙管理中心 来管理 Firewall Threat Defense 设备。在启用 防火墙设备管理器 集成管理功能后，将无法使用 防火墙管理中心 来管理 Firewall Threat Defense 设备，除非您禁用本地管理功能并重新配置管理功能以使用防火墙管理中心。另一方面，当您向Firewall Threat Defense 注册 防火墙管理中心 设备时，防火墙设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 防火墙设备管理器 配置迁移到 防火墙管理中心 的选项，反之亦然。选择为 Firewall Threat Defense 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

从版本 7.6.4 开始，可以使用 防火墙设备管理器 管理 OpenStack 上的 Firewall Threat Defense 实例。防火墙设备管理器 是大多数 Firewall Threat Defense 设备上都包含的 Web界面。它可以配置小型网络最常用的软件基本功能。此产品专为仅包含一台或几台设备的网络而设计，在这种网络中，无需使用高性能多设备管理器来控制包含大量设备的大型网络。有关详细信息，请参阅使用 Cisco Secure Firewall 设备管理器 来管理 Secure Firewall Threat Defense Virtual

注释 有关支持的 防火墙设备管理器 设备的列表，请参阅*Cisco Secure Firewall Threat Defense* 兼容性指南。

部署 Firewall Threat Defense Virtual

思科提供用于部署 Firewall Threat Defense Virtual 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，Firewall Threat Defense Virtual 部署步骤分为以下几个部分。

- 将 Firewall Threat Defense Virtual qcow2 映像上传到 OpenStack Glance 服务。
- 创建网络基础设施：

- 网络
- 子网 (Subnets)
- 路由器接口

- 创建 Firewall Threat Defense Virtual 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 Firewall Threat Defense Virtual。

将 Firewall Threat Defense Virtual映像上传到 OpenStack

将 Firewall Threat Defense Virtual 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 Firewall Threat Defense Virtual qcow2 文件并将其放在 Linux 主机上：

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

注释 需要 Cisco.com 登录信息和思科服务合同。

过程

步骤 1 将 qcow2 映像文件复制到 OpenStack 控制器节点。

步骤 2 将 Firewall Threat Defense Virtual 映像上传到 OpenStack Glance 服务。

```
root@ucs-os-controller:$ openstack image create <image_name> --public --disk-
format qcow2 --container-format bare --file ./<ftdv_qcow2_file>
```

步骤 3 验证 Firewall Threat Defense Virtual 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 |+
| 06dd7975-0b6e-45b8-810a-4ff98546a39d | ftdv-7-0-image    | active |+
```

系统将显示已上传的映像及其状态。

步骤 4 配置镜像属性

镜像的创建和配置：

启用 UEFI：

```
openstack image set <your_image> --property hw_firmware_type=uefi --property hw_machine_type=q35
```

启用 UEFI（使用安全启动）：

```
openstack image set <your_image> --property hw_firmware_type=uefi --property os_secure_boot=required
--property hw_machine_type=q35
```

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 Firewall Threat Defense Virtual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 Firewall Threat Defense Virtual 所需的组件，例如终端、网络、子网、路由器接口和安全组规则：

- `deploy_os_infra.yaml`
- `env.yaml`

您的 Firewall Threat Defense Virtual 版本的模板可通过 FTDv OpenStack Heat 模板从 GitHub 存储库获取。

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。

过程

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:$ openstack stack list

下一步做什么

在 OpenStack 上创建 Firewall Threat Defense Virtual 实例。

在 OpenStack 上部署 Firewall Threat Defense Virtual

使用示例 Firewall Threat Defense Virtual Heat 模板在 OpenStack 上部署 Firewall Threat Defense Virtual。

开始之前

在 OpenStack上部署 Firewall Threat Defense Virtual 需要 Heat 模板：

- `deploy_ftdv.yaml`

您的 Firewall Threat Defense Virtual 版本的模板可通过 FTDv OpenStack Heat 模板从 GitHub 存储库获取。

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。

过程

步骤 1 部署 Firewall Threat Defense Virtual Heat 模板文件 (`deploy_ftdv.yaml`) 以创建 Firewall Threat Defense Virtual 实例。

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

示例：

```
+---------------------+------------------------------+
| Field               | Value                        |
+---------------------+--------------------------------------+
| id                  | 14624af1-e5fa-4096-bd86-c453bc2928ae |
| stack_name          | ftdv-stack                           |
| description         | FTDvtemplate                         |
| 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 Firewall Threat Defense Virtual 堆栈。

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

在 OpenStack 上部署 Firewall Threat Defense Virtual

示例：

```
+--------------------------------------+-------------+----------------------------------+--------+
| ID                                   | Stack Name  | Project                          | Stack Status
   |
+--------------------------------------+-------------+----------------------------------+-----------------+
| 14624af1-e5fa-4096-bd86-c453bc2928ae | ftdv-stack  | 13206e49b48740fdafca83796c6f4ad5 | CREATE_COMPLETE
 |
| 198336cb-1186-45ab-858f-15ccd3b909c8 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 | CREATE_COMPLETE
 |
+--------------------------------------+-------------+----------------------------------+-----------------+
```

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。