# Deploy the Firewall Management Center Virtual on OpenStack

You can deploy the Firewall Management Center Virtual on OpenStack.

## Overview

This guide describes how to deploy the Firewall Management Center Virtual in an OpenStack environment. OpenStack is a free open standard cloud computing platform, mostly deployed as infrastructure-as-a-service (IaaS) in both public and private clouds where virtual servers and other resources are made available to users.

The Firewall Management Center Virtual runs the same software as physical Firewall Management Center to deliver proven security functionality in a virtual form factor. The Firewall Management Center Virtual can be deployed on OpenStack. It can then be configured to manage virtual and physical devices.

This deployment uses a KVM hypervisor to manage virtual resources. KVM is a full virtualization solution for Linux on x86 hardware containing virtualization extensions (such as Intel VT). It consists of a loadable kernel module, kvm.ko, that provides the core virtualization infrastructure and a processor specific module, such as kvm-intel.ko. You can run multiple virtual machines running unmodified OS images using KVM. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, and so forth.

Because the devices are already supported on the KVM hypervisor, no additional kernel packages or drivers are needed to enable OpenStack support.

## Prerequisites

- Download the Firewall Management Center Virtual qcow2 file from software.cisco.com and put it on your Linux host:

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

- A software.cisco.com and Cisco service contract are required.
- The Firewall Management Center Virtual supports deployment on opensource OpenStack environment and Cisco VIM managed OpenStack environment.

  Set up the OpenStack environment according to the OpenStack guidelines.

  - See the opensource OpenStack document:

    Caracal Release - https://docs.openstack.org/project-deploy-guide/openstack-ansible/2024.1/overview.html

  - See the Cisco Virtualized Infrastructure Manager (VIM) OpenStack document: Cisco Virtualized Infrastructure Manager Documentation, 4.4.3.

- Licensing:
  - You configure license entitlements for the security services from the Firewall Management Center.
  - See "Licensing the System" in the *Secure Firewall Management Center Configuration Guide* for more information about how to manage licenses.

- Memory and resource requirements:
  - Processors
    - Requires 4 vCPUs or 8 vCPUs
  - Memory
    - Minimum required 28 GB / Recommended (default) 32 GB RAM
  - Host storage per Virtual Machine
    - The Firewall Management Center Virtual requires 250 GB

**Note** You can modify the vCPU and memory values as per your requirement.

- Interface requirements:
  - Management interface — One used to connect the device to the Firewall Management Center.
- Communications paths:
  - Floating IPs for access into the Firewall Management Center Virtual.
- Minimum supported Firewall Management Center Virtual version:
  - Version 7.0.
- For OpenStack requirements, see System Requirements, on page 3.
- For Firewall Management Center Virtual and System compatibility, see Cisco Secure Firewall Threat Defense Compatibility Guide.

# Guidelines and Limitations

### Supported Features

The Firewall Management Center Virtual on OpenStack supports the following features:

- Deployment the Firewall Management Center Virtual on the KVM hypervisor running on a compute node in your OpenStack environment.
- OpenStack CLI
- Heat template-based deployment
- Licensing — Only BYOL is supported
- Drivers - VIRTIO
- IPv6 is supported

### Unsupported Features

The Firewall Management Center Virtual on OpenStack does not support the following:

- Autoscale
- Cluster

# System Requirements

The OpenStack environment must conform to the following supported hardware and software requirements.

***Table 1: Hardware and Software Requirements***

| Category | Supported Versions | Notes |
|---|---|---|
| Server | UCS C240 M5 | 2 UCS servers are recommended, one each for os-controller and os-compute nodes. |
| Driver | VIRTIO | These are the supported drivers. |
| Operating System | Ubuntu Server 22.04 | This is the recommended OS on UCS servers. |
| OpenStack Version | Caracal release | Details of the various OpenStack releases are available at:<br>https://releases.openstack.org/ |

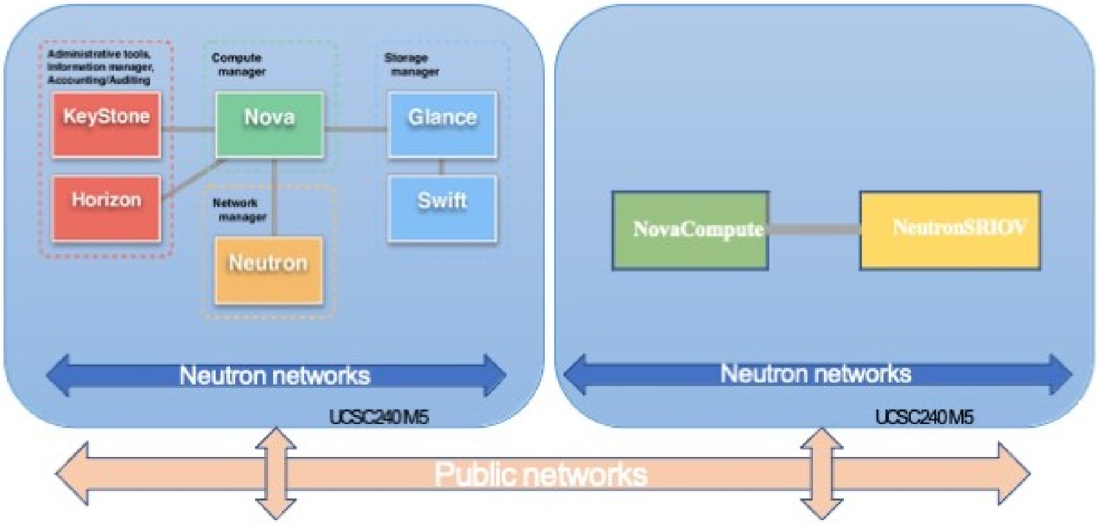
*Table 2: Hardware and Software Requirements for Cisco VIM Managed OpenStack*

| Category | Supported Versions | Notes |
|---|---|---|
| Server Hardware | UCS C220-M5/UCS C240-M4 | 5 UCS servers are recommended, three each for os-controller and Two or more for os-compute nodes. |
| Drivers | VIRTIO | These are the supported drivers. |
| Cisco VIM Version | Cisco VIM 4.4.3<br>Supported on:<br>• Operating System - Red Hat Enterprise Linux 8.4<br>• OpenStack version - OpenStack 16.2 (Train Release) | See Cisco Virtualized Infrastructure Manager Documentation, 4.4.3 for more information. |

### OpenStack Platform Topology

The following figure shows the recommended topology to support deployments in OpenStack using two UCS servers.

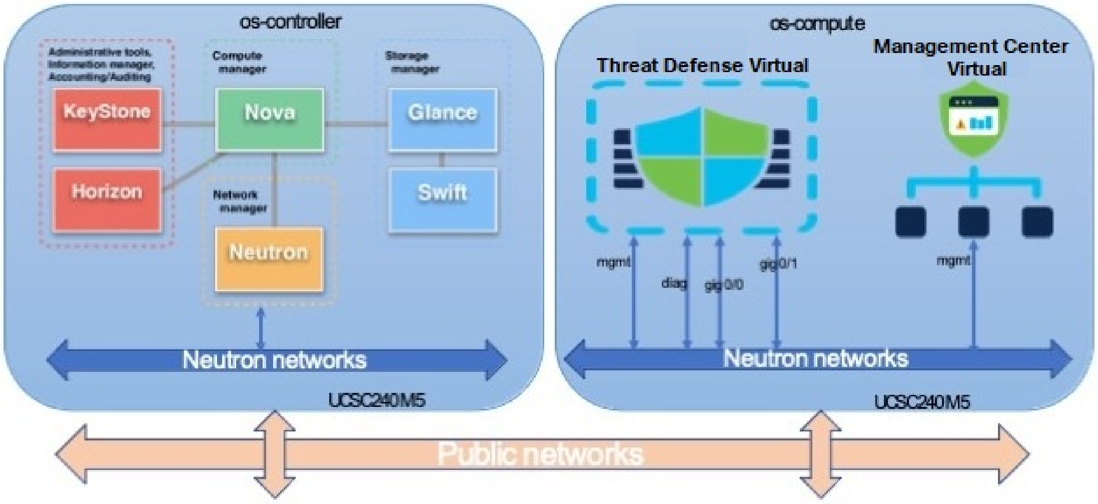
*Figure 1: OpenStack Platform Topology*



# Sample Network Topology

The following figure shows a network topology example for the Firewall Management Center Virtual in OpenStack.

*Figure 2: Topology Example with the Firewall Management Center Virtual on OpenStack*



# Deploy the Firewall Management Center Virtual

Cisco provides sample heat templates for deploying the Firewall Management Center Virtual. Steps for creating the OpenStack infrastructure resources are combined in a heat template (`deploy_os_infra.yaml`) file to create networks, subnets, and router interfaces. At a high-level, the Firewall Management Center Virtual deployment steps are categorized into the following sections.

- Upload the Firewall Management Center Virtual qcow2 image to the OpenStack Glance service.
- Create the network infrastructure.
  - Network
  - Subnet
  - Router interface
- Create the Firewall Management Center Virtual instance.
  - Flavor
  - Security Groups
  - Floating IP
  - Instance

You can deploy the Firewall Management Center Virtual on OpenStack using the following steps.

## Upload the Firewall Management Center Virtual Image to OpenStack

Copy the Firewall Management Center Virtual qcow2 image to the OpenStack controller node, and then upload the image to the OpenStack Glance service.

### Before you begin

- Download the Firewall Management Center Virtual qcow2 file from Cisco.com and put it on your Linux host:

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

### Procedure

**Step 1** Copy the qcow2 image file to the OpenStack controller node.

**Step 2** Upload the Firewall Management Center Virtual image to the OpenStack Glance service.

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

**Step 3** Verify if the Firewall Management Center Virtual image upload is successful.

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

**Example:**

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

The uploaded image and its status is displayed.

### What to do next

Create the network infrastructure using the `deploy_os_infra.yaml` template.

## Create the Network Infrastructure for the OpenStack and the Firewall Management Center Virtual

Deploy the OpenStack infrastructure heat template to create the network infrastructure.

### Before you begin

Heat template files are required to create the network infrastructure and the required components for the Firewall Management Center Virtual, such as flavor, networks, subnets, router interfaces, and security group rules:

- `env.yaml` — Defines the resources created to support the Firewall Management Center Virtual on the compute node, such as the image name, interfaces, and IP addresses.
- `deploy_os_infra.yaml` — Defines the environment for the Firewall Management Center Virtual, such as the network and subnets.

Templates for your Firewall Management Center Virtual version are available from the GitHub repository at FMCv OpenStack heat template.

**Important**

Note that Cisco-provided templates are provided as open source examples, and are not covered within the regular Cisco TAC support scope. Check GitHub regularly for updates and ReadMe instructions.

### Procedure

**Step 1** Deploy the infrastructure heat template file.

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

**Example:**

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

**Step 2** Verify if the infrastructure stack is created successfully.

**root@ucs-os-controller:$ openstackstack list**

**Example:**

```
root@ucs-os-controller:$ openstack stack list
+----------------------------------+------------+------------------------------+---------------+
| ID                                | Stack Name  | Project                       | Stack Status
    |
+----------------------------------+------------+------------------------------+---------------+
| b30d5875-ce3a-4258-a841-bf2d09275929 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
+----------------------------------+------------+------------------------------+---------------+
```

#### What to do next

Create the Firewall Management Center Virtual instance on OpenStack.

## Create the Firewall Management Center Virtual Instance on OpenStack

Use the sample heat template to deploy the Firewall Management Center Virtual on OpenStack.

#### Before you begin

A heat template is required to deploy the Firewall Management Center Virtual on OpenStack:

- `deploy_fmcv.yaml`

Templates for your Firewall Management Center Virtual version are available from the GitHub repository at FMCv OpenStack heat template.

**Important**

Note that Cisco-provided templates are provided as open source examples, and are not covered within the regular Cisco TAC support scope. Check GitHub regularly for updates and ReadMe instructions.

### Procedure

**Step 1** Deploy the Firewall Management Center Virtual heat template file (`deploy_fmcv.yaml`) to create the Firewall Management Center Virtual instance.

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

**Example:**

```
+---------------------+-----------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| id                  | 96c8c126-107b-4733-8f6c-eb15a637219f |
| stack_name          | fmcv-stack                           |
| description         | FMCv template                        |
| updated_time        | None                                 |
| stack_status        | CREATE_IN_PROGRESS                   |
| stack_status_reason | Stack CREATE started                 |
+---------------------+--------------------------------------+
```

**Step 2** Verify that your Firewall Management Center Virtual stack is created successfully.

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

**Example:**

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