



OpenStack への Firewall Management Center Virtual の展開

OpenStack に Firewall Management Center Virtual を導入できます。

- [概要 \(1 ページ\)](#)
- [前提条件 \(2 ページ\)](#)
- [注意事項と制約事項 \(3 ページ\)](#)
- [システム要件 \(3 ページ\)](#)
- [ネットワークトポロジの例 \(5 ページ\)](#)
- [Firewall Management Center Virtual の導入 \(5 ページ\)](#)

概要

このガイドでは、OpenStack 環境で Firewall Management Center Virtual を展開する方法について説明します。OpenStack は無料のオープンな標準規格のクラウドコンピューティングプラットフォームであり、ほとんどの場合は、ユーザーが仮想サーバーやその他のリソースを利用できるように Infrastructure-as-a-Service (IaaS) としてパブリッククラウドとプライベートクラウドの両方に展開します。

Firewall Management Center Virtual は、物理と同じソフトウェアを実行し、仮想フォームファクタにおいて実証済みのセキュリティ機能を提供します。Firewall Management Center Virtual は OpenStack に展開できます。その後、仮想デバイスおよび物理デバイスを管理するように設定できます。

この展開では、KVM ハイパーバイザを使用して仮想リソースを管理します。KVM は、仮想化拡張機能 (Intel VT など) を搭載した x86 ハードウェア上の Linux 向け完全仮想化ソリューションです。KVM は、コア仮想化インフラストラクチャを提供するロード可能なカーネルモジュール (kvm.ko) と kvm-intel.ko などのプロセッサ固有のモジュールで構成されています。KVM を使用して、修正されていない OS イメージを実行している複数の仮想マシンを実行できます。各仮想マシンには、ネットワークカード、ディスク、グラフィックアダプタなどのプライベートな仮想化ハードウェアが搭載されています。

デバイスは KVM ハイパーバイザですでにサポートされているため、OpenStack サポートを有効にするために必要な追加のカーネルパッケージやドライバはありません。

前提条件

- software.cisco.com から Firewall Management Center Virtual qcow2 ファイルをダウンロードし、Linux ホストに格納します。
<https://software.cisco.com/download/navigator.html>
- software.cisco.com および Cisco Service Contract が必要です。
- Firewall Management Center Virtual は、オープンソースの OpenStack 環境と Cisco VIM 管理対象 OpenStack 環境での展開をサポートします。

OpenStack のガイドラインに従って OpenStack 環境をセットアップします。

- オープンソースの OpenStack ドキュメントを参照してください。

Caracal リリース : <https://docs.openstack.org/project-deploy-guide/openstack-ansible/2024.1/overview.html>

- Cisco Virtualized Infrastructure Manager (VIM) OpenStack のドキュメント ([Cisco Virtualized Infrastructure Manager のマニュアル、4.4.3](#)) を参照してください。

- ライセンス :

- からセキュリティサービスのソフトウェア利用資格を設定します。
- ライセンスの管理方法の詳細については、『*Cisco Secure Firewall Management Center Configuration Guide*』の「Licensing the System」を参照してください。

- メモリとリソースの要件 :

- プロセッサ
 - 4 個の vCPU が必要
- メモリ
 - 最小要件 28 GB/推奨 (デフォルト) 32 GB RAM
- 仮想マシンあたりのホストストレージ
 - Firewall Management Center Virtual には 250 GB が必要



(注) 要件に応じて、vCPU とメモリの値を変更できます。

- インターフェイスの要件 :

- 管理インターフェイス：デバイスを に接続するために使用されるインターフェイス。
- 通信パス：
 - Firewall Management Center Virtual にアクセスするためのフローティング IP。
- サポートされている Firewall Management Center Virtual の最小バージョン：
 - バージョン 7.0。
- OpenStack の要件については、[システム要件（3 ページ）](#) を参照してください。
- Firewall Management Center Virtual とシステムの互換性については、『[Cisco Secure Firewall Threat Defense Compatibility Guide](#)』を参照してください。

注意事項と制約事項

サポートされる機能

OpenStack 上の Firewall Management Center Virtual は次の機能をサポートします。

- OpenStack 環境のコンピューティングノードで実行されている KVM ハイパーバイザへの Firewall Management Center Virtual の展開
- OpenStack CLI
- Heat テンプレートベースの展開
- ライセンス：BYOL のみをサポート
- ドライバ：VIRTIO
- IPv6 はサポートされます。

サポートされない機能

OpenStack 上の Firewall Management Center Virtual は以下をサポートしません。

- 自動スケール
- クラスタ

システム要件

OpenStack 環境は、サポートされているハードウェアとソフトウェアの次の要件に準拠している必要があります。

表 1: ハードウェアおよびソフトウェアの要件

カテゴリ	サポートされるバージョン	注記
サーバー	UCS C240 M5	2 台の UCS サーバーを推奨します。os-controller ノードと os-compute ノードに 1 台ずつです。
要因	VIRTIO	サポートされているドライバは次のとおりです。
オペレーティング システム	Ubuntu Server 22.04	これは、UCS サーバーで推奨されている OS です。
OpenStack バージョン	Caracal リリース	さまざまな OpenStack リリースの詳細については、次の URL を参照してください。 https://releases.openstack.org/

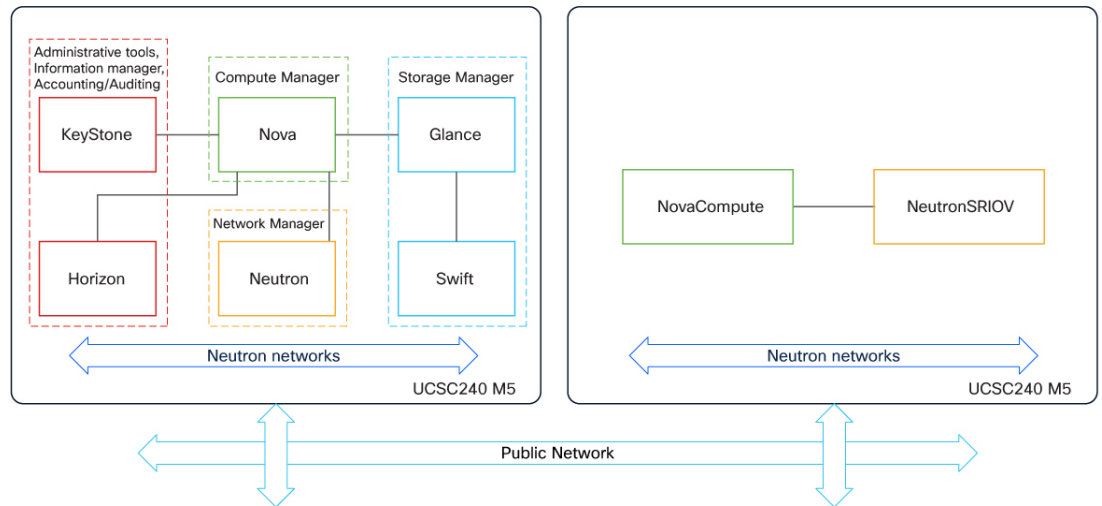
表 2: Cisco VIM Managed OpenStack のハードウェアとソフトウェアの要件

カテゴリ	サポートされるバージョン	注記
サーバ ハードウェア	UCS C220-M5/UCS C240-M4	os-controller ノードごとに 3 台、os-compute ノードに 2 台以上で、5 台の UCS サーバーを推奨します。
ドライバ (Drivers)	VIRTIO	サポートされているドライバは次のとおりです。
Cisco VIM バージョン	Cisco VIM 4.4.3 サポート対象 : - オペレーティングシステム - Red Hat Enterprise Linux 8.4 - OpenStack バージョン - OpenStack 16.2 (トレイン リリース)	詳細については、 シスコ仮想インフラストラクチャ マネージャのドキュメント 4.4.3 を参照してください。

OpenStack プラットフォームトポロジ

次の図に、2 台の UCS サーバーを使用して OpenStack での展開をサポートするための推奨トポロジを示します。

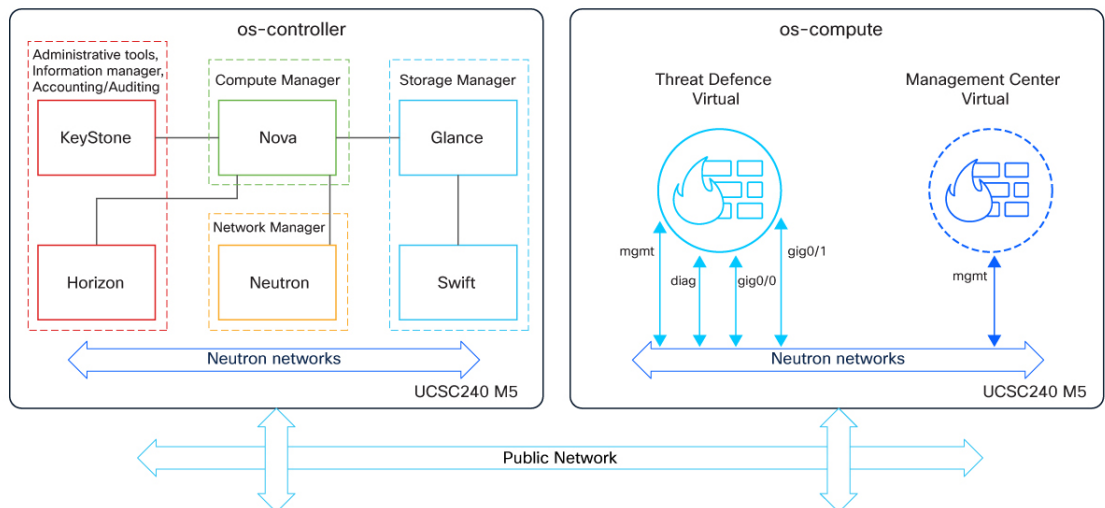
図 1: OpenStack プラットフォームトポロジ



ネットワークトポロジの例

次の図に、OpenStack の Firewall Management Center Virtual のネットワークトポロジの例を示します。

図 2: OpenStack で Firewall Management Center Virtual を使用したトポロジの例



Firewall Management Center Virtual の導入

シスコでは、Firewall Management Center Virtual を展開するためのサンプルの Heat テンプレートを提供しています。OpenStack インフラストラクチャのリソースを作成する手順は、ネット

ワーク、サブネット、およびルータインターフェイスを作成するために、Heat テンプレート（`deploy_os_infra.yaml`）ファイルで結合されます。Firewall Management Center Virtual の展開手順は大まかに次の部分に分類されます。

- Firewall Management Center Virtual qcow2 イメージを OpenStack Glance サービスにアップロードします。
- ネットワーク インフラストラクチャを作成します。
 - ネットワーク
 - サブネット
 - ルータ インターフェイス
- Firewall Management Center Virtual インスタンスを作成します。
 - フレーバ
 - セキュリティ グループ
 - フローティング IP
 - インスタンス

次の手順を使用して、OpenStack に Firewall Management Center Virtual を展開できます。

OpenStack への Firewall Management Center Virtual イメージのアップロード

Firewall Management Center Virtual qcow2 イメージを OpenStack コントローラノードにコピーし、イメージを OpenStack Glance サービスにアップロードします。

始める前に

- Cisco.com から Firewall Management Center Virtual qcow2 ファイルをダウンロードし、Linux ホストに格納します。

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

手順

ステップ 1 qcow2 イメージファイルを OpenStack コントローラノードにコピーします。

ステップ 2 Firewall Management Center Virtual イメージを OpenStack Glance サービスにアップロードします。

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

ステップ 3 Firewall Management Center Virtual イメージが正常にアップロードされたことを確認します。

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

例 :

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

```
+-----+-----+-----+
| ID                                           | Name                               | Status |
+-----+-----+-----+
| b957b5f9-ed1b-4975-b226-4cddf5887991      | fmcv-7-0-image                   | active |
+-----+-----+-----+
```

アップロードしたイメージとそのステータスが表示されます。

次のタスク

deploy_os_infra.yaml テンプレートを使用してネットワーク インフラストラクチャを作成します。

OpenStack と Firewall Management Center Virtual のネットワーク インフラストラクチャの作成

OpenStack インフラストラクチャの Heat テンプレートを展開して、ネットワーク インフラストラクチャを作成します。

始める前に

Heat テンプレートファイルは、フレーバ、ネットワーク、サブネット、ルータインターフェイス、セキュリティグループルールなど、ネットワーク インフラストラクチャ、および Firewall Management Center Virtual に必要なコンポーネントを作成するために必要です。

- env.yaml : イメージ名、インターフェイス、IP アドレスなど、コンピューティングノードで Firewall Management Center Virtual をサポートするために作成するリソースを定義します。
- deploy_os_infra.yaml : ネットワークやサブネットなど、Firewall Management Center Virtual の環境を定義します。

Firewall Management Center Virtual バージョンのテンプレートは、GitHub リポジトリの [FMCv OpenStack Heat テンプレート](#) から入手できます。



重要

シスコが提供するテンプレートはオープンソースの例として提供しているものであり、通常の Cisco TAC サポートの範囲内では扱われていません。更新と ReadMe の手順については、GitHub を定期的に確認してください。

手順

ステップ 1 インフラストラクチャ Heat テンプレートファイルを展開します。

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

例 :

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

ステップ 2 インフラストラクチャ スタックが正常に作成されたかどうかを確認します。

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

例 :

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

```
+-----+-----+-----+-----+
| ID                               | Stack Name | Project                               | Stack |
| Status                           |            |                                       |       |
+-----+-----+-----+-----+
| b30d5875-ce3a-4258-a841-bf2d09275929 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |      |
| CREATE_COMPLETE                     |            |                                       |      |
+-----+-----+-----+-----+
```

次のタスク

OpenStack で Firewall Management Center Virtual インスタンスを作成します。

OpenStack での Firewall Management Center Virtual インスタンスの作成

Heat テンプレートのサンプルを使用して、OpenStack に Firewall Management Center Virtual を展開します。

始める前に

OpenStack で Firewall Management Center Virtual を展開するには、次の Heat テンプレートが必要です。

- deploy_fmcv.yaml

Firewall Management Center Virtual バージョンのテンプレートは、GitHub リポジトリの [FMCv OpenStack Heat テンプレート](#) から入手できます。



重要

シスコが提供するテンプレートはオープンソースの例として提供しているものであり、通常の Cisco TAC サポートの範囲内では扱われていません。更新と ReadMe の手順については、GitHub を定期的に確認してください。

手順

ステップ 1 Firewall Management Center Virtual Heat テンプレートファイル (ddeploy_fmcv.yaml) を展開して、Firewall Management Center Virtual インスタンスを作成します。

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

例 :

```
+-----+-----+
| 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                 |
+-----+-----+
```

ステップ 2 Firewall Management Center Virtual スタックが正常に作成されたことを確認します。

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

例 :

```
+-----+-----+-----+-----+
| 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 |
+-----+-----+-----+-----+
```


翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。