OpenStack への Threat Defense Virtual の展開

概要

このガイドでは、OpenStack 環境で Threat Defense 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。

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。

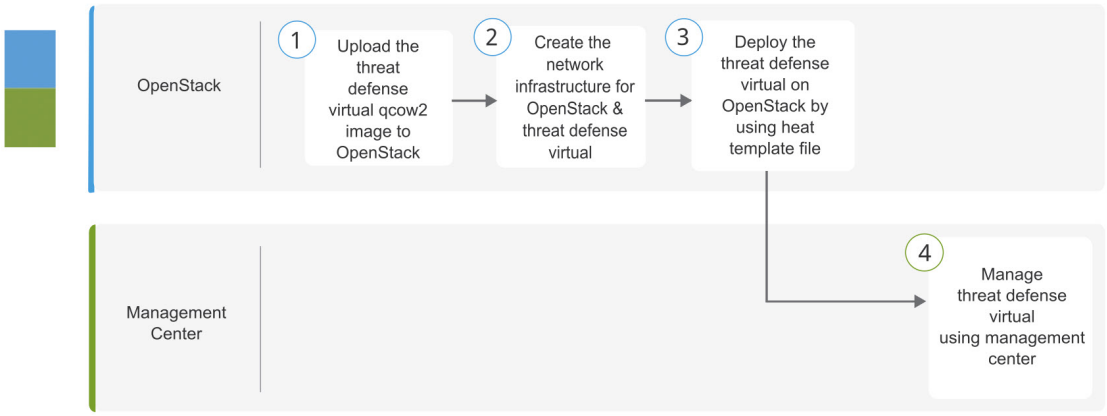
KVM を使用して、修正されていない OS イメージを実行している複数の仮想マシンを実行できます。各仮想マシンには、ネットワーク カード、ディスク、グラフィック アダプタなどのプライベートな仮想化ハードウェアが搭載されています。

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。

（注） OpenStack の Threat Defense Virtual は、最適化されたマルチノード環境にインストールできます。

エンドツーエンドの手順

次のフローチャートは、OpenStack に Threat Defense Virtual を展開する際のワークフローを示しています。



	ワークスペース	手順
1	OpenStack	OpenStack への Threat Defense Virtual イメージのアップロード：Threat Defense Virtual のイメージを OpenStack にアップロードします。
2	OpenStack	OpenStack と Threat Defense Virtual のネットワーク インフラストラクチャの作成：OpenStack および Threat Defense Virtual のネットワーク インフラストラクチャを作成します。
3	OpenStack	OpenStack への Threat Defense Virtual の展開：Threat Defense Virtual の Heat テンプレートファイルを使用して、Threat Defense Virtual を OpenStack に展開します。
4	Management Center	Management Center を使用した Threat Defense Virtual の管理

前提条件

- software.cisco.com から qcow2 Threat Defense Virtual イメージを取得します。
- Threat Defense 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。

    Wallaby リリース：https://docs.openstack.org/project-deploy-guide/openstack-ansible/wallaby/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。

- Cisco スマートアカウント。Cisco Software Central で作成できます。
- Threat Defense Virtual へのライセンス付与。
  - Management Center からセキュリティ サービスのすべてのライセンス資格を設定します。
  - ライセンスの管理方法の詳細については、『*Secure Firewall Management Center Admin Guide*』の「Licensing」を参照してください。
- インターフェイスの要件：
  - 管理インターフェイス（2）：1 つは Threat Defense Virtual を Management Center に接続するために使用されます。もう 1 つは診断目的に使用され、通過トラフィックには使用できません。
  - 内部インターフェイスと外部インターフェイス：Threat Defense Virtual を内部のホストとパブリックインターフェイスに接続するために使用します。
- 通信パス：
  - Threat Defense 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 Threat Defense 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 （5 ページ）を参照してください。
- Threat Defense Virtual のシステム要件については、『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 Threat Defense 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 Threat Defense Virtual の展開
- OpenStack CLI
- Heat テンプレートベースの展開
- OpenStack Horizon ダッシュボード
- ライセンス：BYOL のみをサポート
- Management Center のみを使用した Threat Defense Virtual の管理。
- ドライバ：VirtIO および SR-IOV

Threat Defense Virtual スマートライセンスのパフォーマンス階層

Threat Defense Virtual は、導入要件に基づいて異なるスループットレベルと VPN 接続制限を提供するパフォーマンス階層型ライセンスをサポートしています。

表 *1 : Threat Defense Virtual* 権限付与に基づくライセンス機能の制限

パフォーマンス階層	デバイス仕様（コア/RAM）	レート制限	RA VPN セッション制限
FTDv5	4 コア/8 GB	100Mbps	50
FTDv10	4 コア/8 GB	1Gbps	250
FTDv20	4 コア/8 GB	3 Gbps	250
FTDv30	8 コア/16 GB	5 Gbps	250
FTDv50	12 コア/24 GB	10 Gbps	750
FTDv100	16 コア/32 GB	16 Gbps	10,000

Threat Defense Virtual デバイスのライセンス取得のガイドラインについては、『*Secure Firewall Management Center Admin Guide*』の「Licensing」の章を参照してください。

パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「OpenStack での仮想化の調整と最適化」を参照してください。

Receive Side Scaling：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラフィックを分散するために使用されるテクノロジーです。バージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」を参照してください。

Snort

- Snort のシャットダウンに時間がかかったり、VM が全体的に遅くなったりといった異常な動作が見られる場合や、特定のプロセスが実行されるときには、Threat Defense Virtual および VM ホストからログを収集します。全体的な CPU 使用率、メモリ、I/O 使用率、および読み取り/書き込み速度のログの収集は、問題のトラブルシューティングに役立ちます。
- Snort のシャットダウン時には、CPU と I/O の使用率が高くなります。十分なメモリがなく、専用の CPU がない単一のホスト上に多数の Threat Defense Virtual インスタンスが作成されている場合は、Snort のシャットダウンに時間がかかって Snort コアが作成されます。

サポートされない機能

OpenStack 上の Threat Defense 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 *2 : Open Source 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 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。
ドライバ	VIRTIO、IXGBE、および I40E	サポートされているドライバは次のとおりです。

カテゴリ	サポートされるバージョン	注記
オペレーティングシステム	Ubuntu Server 20.04	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	Wallaby 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/

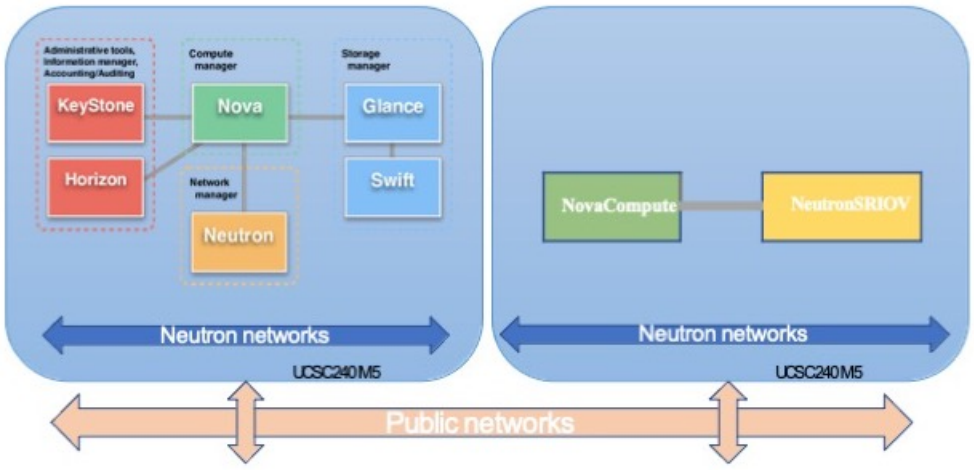
表 *3 : Cisco VIM Managed OpenStack* のハードウェアとソフトウェアの要件

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、IXGBE、および I40E	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。

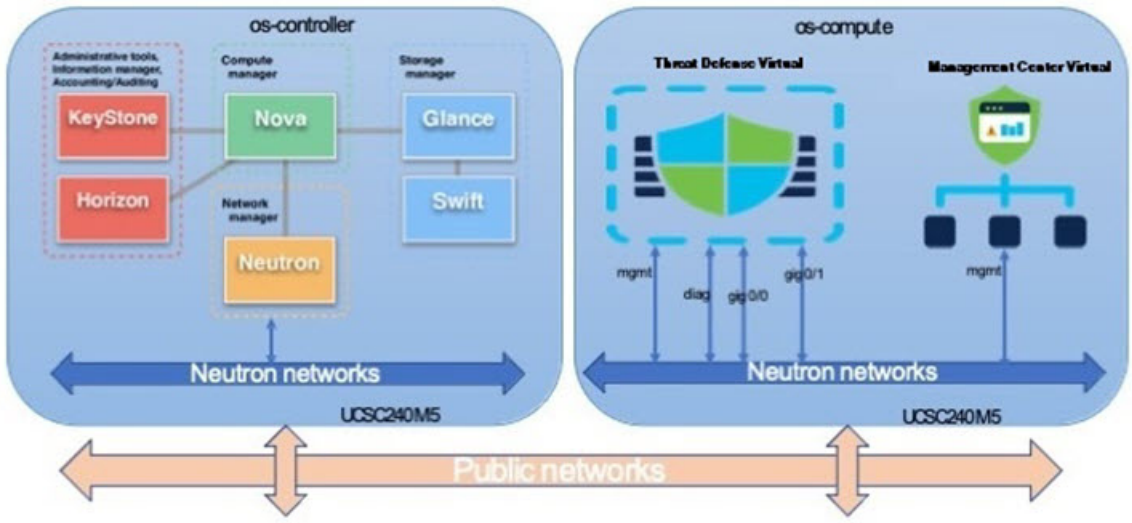
図 *1 : OpenStack* プラットフォームトポロジ



OpenStack 上の Threat Defense Virtual のネットワークトポロジ例

次の図に、Threat Defense Virtual 用の OpenStack に設定された 4 つのサブネット（管理、診断、内部、および外部）を備えたルーテッド ファイアウォール モードの Threat Defense Virtual のネットワークトポロジの例を示します。

図 *2 : OpenStack* で *Threat Defense Virtual* と *Management Center Virtual* を使用したトポロジの例



Threat Defense Virtual の導入

シスコでは、Threat Defense 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。Threat Defense Virtual の展開手順は大まかに次の部分に分類されます。

- Threat Defense 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
- Threat Defense 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 Threat Defense Virtual を展開できます。

OpenStack への Threat Defense Virtual イメージのアップロード

Threat Defense 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 Threat Defense 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

（注） Cisco.com のログインおよびシスコ サービス契約が必要です。

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 Threat Defense 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 <image_name> --public --disk-
format qcow2 --container-format bare --file ./<ftdv_qcow2_file>
```

ステップ 3 Threat Defense 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 |+
| 06dd7975-0b6e-45b8-810a-4ff98546a39d | ftdv-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 Threat Defense Virtual のネットワーク インフラストラクチャの作成

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と Threat Defense Virtual に必要なコンポーネントを作成するために必要です。

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

Threat Defense Virtual バージョンのテンプレートは、GitHub リポジトリの FTDv 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。

OpenStack への Threat Defense Virtual の展開

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:$ openstack stack list

次のタスク

OpenStack で Threat Defense Virtual インスタンスを作成します。

OpenStack への Threat Defense Virtual の展開

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

始める前に

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

- `deploy_ftdv.yaml`

Threat Defense Virtual バージョンのテンプレートは、GitHub リポジトリの FTDv 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 Threat Defense Virtual Heat テンプレートファイル（`deploy_ftdv.yaml`）を展開して、Threat Defense Virtual インスタンスを作成します。

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

OpenStack への Threat Defense Virtual の展開

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

ステップ 2 Threat Defense 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 | ftdv-stack  | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
| 198336cb-1186-45ab-858f-15ccd3b909c8 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
+--------------------------------------+-------------+----------------------------------+--------+
```

OpenStack への Threat Defense Virtual の展開

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。