Firepower Threat Defense Virtual と OpenStack のスタートアップガイド

OpenStack 環境のコンピューティングノードで実行しているカーネルベースの仮想マシン（KVM）ハイパーバイザに Firepower Threat Defense Virtual（FTDv）を展開できます。

OpenStack への FTDv 展開について

このガイドでは、OpenStack 環境で FTDv 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。

Firepower 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 FTDv 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。

FTDv と OpenStack の前提条件

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

    Stein リリース：https://docs.openstack.org/project-deploy-guide/openstack-ansible/stein/overview.html

    Queens リリース：https://docs.openstack.org/project-deploy-guide/openstack-ansible/queens/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、3.4.3 ～ 3.4.5）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。
- Firepower Threat Defense Virtual のライセンス。
  - Firepower 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。
  - ライセンスを管理する方法の詳細については、『*Firepower Management Center Configuration Guide*』の「Licensing the Firepower System」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 Firepower Threat Defense Virtual を Firepower 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：Firepower 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：
  - Firepower 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 FTDv の最小バージョン：
  - バージョン 7.0
- OpenStack の要件については、Firepower 展開での OpenStack の要件 （4 ページ）を参照してください。

- FTDv システムの要件については、『Cisco Firepower Compatibility』[英語] を参照してください。

FTDv と OpenStack のガイドラインと制限事項

サポートされる機能

OpenStack の FTDv は次の機能をサポートしています。

- 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 FTDv 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
- ルーテッド モード（デフォルト）
- ライセンス：BYOL のみをサポート
- FMC を使用した FTDv 管理
- ドライバ：VIRTIO、VPP、および SRIOV

FTDv スマートライセンスのパフォーマンス階層

FTDv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 : FTDv* 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（Rate Limit）	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	3Gbps	250
FTDv30	8 コア/16 GB	5Gbps	250
FTDv50	12 コア/24 GB	10Gbps	750
FTDv100	16 コア/32 GB	16Gbps	10,000

FTDvデバイスのライセンスを取得する場合のガイドラインについては、『*Firepower Management Center Configuration Guide*』の「Firepower システムのライセンス」の章を参照してください。

サポートされない機能

OpenStack の FTDv は、以下をサポートしていません。

- 自動スケール
- OpenStack Stein リリースと Queens リリース以外の OpenStack リリース
- Ubuntu 18.04 バージョンと Red Hat Enterprise Linux（RHEL）7.6 以外のオペレーティングシステム

Firepower 展開での OpenStack の要件

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*: 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 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、I40E	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 18.04	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	Stein 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

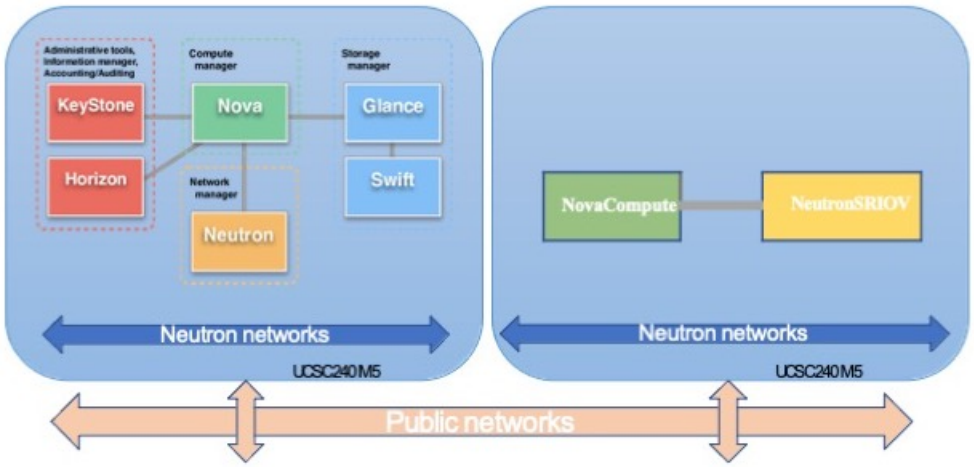
カテゴリ（**Category**）	サポートされるバージョン	注記（**Notes**）
サーバ ハードウェア	UCS C220-M5/UCS C240-M4	os-controller ノードごとに 3 台、os-compute ノードに 2 台以上で、5 台の UCS サーバーを推奨します。
ドライバ（Drivers）	VIRTIO、SRIOV、および VPP	サポートされているドライバは次のとおりです。

カテゴリ（Category）	サポートされるバージョン	注記（Notes）
オペレーティング システム	Red Hat Enterprise Linux 7.6	これが推奨 OS です。
OpenStack バージョン	OpenStack 13.0（Queens 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/
Cisco VIM バージョン	Cisco VIM 3.4.4	Cisco VIM OpenStack のドキュメント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 Firepower 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 での FTDv のネットワークトポロジの例

次の図に、FTDv 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 FTDv のネットワークトポロジの例を示します。

図 *2 : OpenStack* で *FTDv* と *FMCv* を使用したトポロジの例