Nutanix への Threat Defense Virtual の展開

この章では、Threat Defense Virtual を Nutanix 環境に展開する際の手順について説明します。

概要

Cisco Secure Firewall Threat Defense Virtual（旧称 Firepower Threat Defense Virtual）は、Cisco Secure Firewall 機能を仮想化環境にもたらします。物理環境、仮想環境、クラウド環境全体を通して、またクラウド間で一貫性のあるセキュリティポリシーを実現し、ワークロードをサポートします。

この章では、AHV ハイパーバイザを含む Nutanix 環境内における Threat Defense Virtual の機能について解説し、機能のサポート、システム要件、ガイドライン、制限事項などを説明します。また、この章では Threat Defense Virtual を管理するためのオプションについても説明します。

展開を開始する前に、管理オプションを理解しておくことが重要です。Secure Firewall Management Center（旧称 Firepower Management Center）または Secure Firewall Device Manager （旧称 Firepower Device Manager）を使用して Threat Defense Virtual を管理および監視できます。

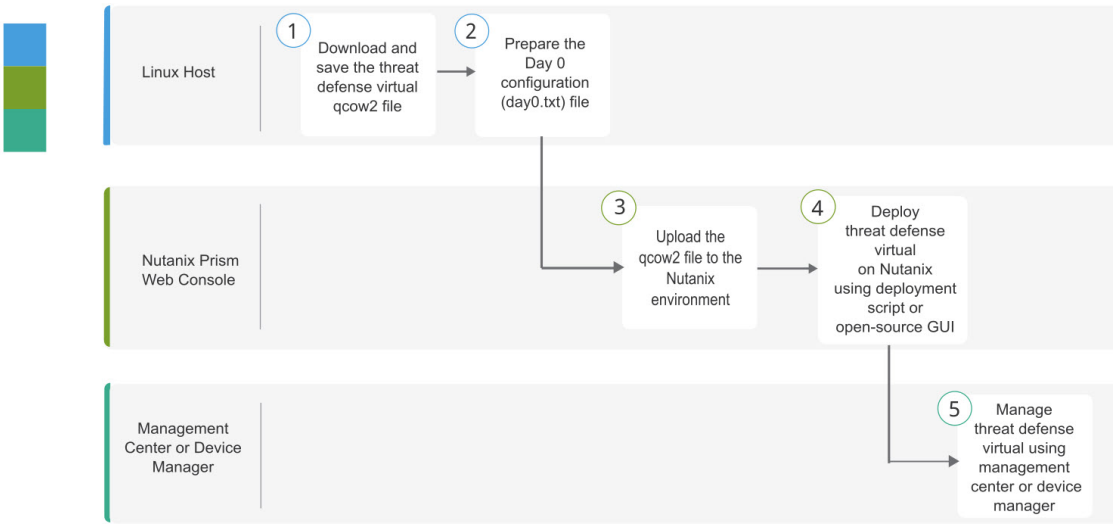
Nutanix への Threat Defense Virtual の展開について

Nutanix Enterprise Cloud Platform は、仮想マシンのホスティングと格納用に構築された、統合型のスケールアウト対応コンピューティングおよびストレージシステムです。Nutanix AHV を

使用して、修正されていない Threat Defense Virtual の 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。

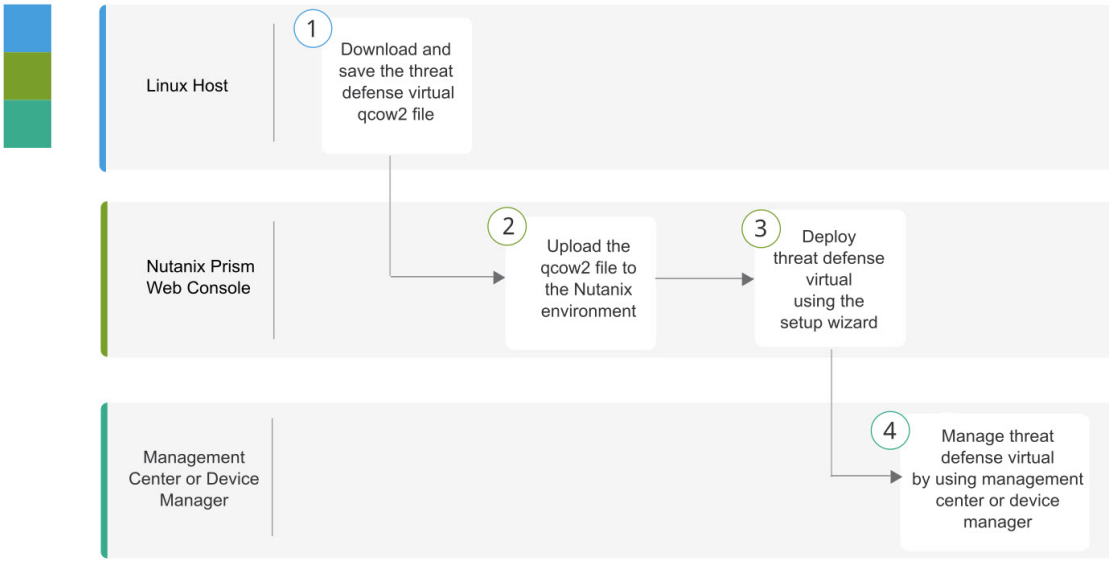
エンドツーエンドの手順

次のフローチャートは、Day 0 の構成ファイルを使用して Nutanix プラットフォームに 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	Linux ホスト	Threat Defense Virtual の導入：Threat Defense Virtual の qcow2 ファイルをダウンロードして保存します。
2	Linux ホスト	Threat Defense Virtual QCOW2 ファイルを Nutanix にアップロード：qcow2 ファイルを Nutanix 環境にアップロードします。
3	Nutanix Prism Web コンソール	第 0 日のコンフィギュレーション ファイルの準備：Day-0 構成ファイルを準備します（**テキストファイル** > **構成の詳細を入力** > **day0-config.txt のファイル名で保存**）。
4	Nutanix Prism Web コンソール	Threat Defense Virtual の導入：Nutanix に Threat Defense Virtual を展開します。
5	Management Center または Device Manager	Threat Defense Virtual の管理： • Management Center を使用 • Device Manager を使用

次のフローチャートは、Day 0 の構成ファイルを使用せずに Nutanix プラットフォームに 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	Linux ホスト	Threat Defense Virtual の導入：Threat Defense Virtual の qcow2 ファイルをダウンロードして保存します。
2	Nutanix Prism Web コンソール	Threat Defense Virtual QCOW2 ファイルを Nutanix にアップロード：qcow2 ファイルを Nutanix 環境にアップロードします。
3	Nutanix Prism Web コンソール	Threat Defense Virtual の導入：Nutanix に Threat Defense Virtual を展開します。
4	Management Center または Device Manager	Threat Defense Virtual の管理： • Management Center を使用 • Device Manager を使用

システム要件

バージョン

マネージャバージョン	デバイスバージョン
Device Manager 7.0	Threat Defense 7.0
Management Center 7.0	

Threat Defense Virtual のハイパーバイザのサポートに関する最新情報については、『Cisco Firepower Compatibility Guide』を参照してください。

Threat Defense Virtual のメモリ、vCPU、およびディスクのサイジング

Threat Defense Virtual の導入に使用される特定のハードウェアは、導入されるインスタンスの数や使用要件によって異なります。Threat Defense Virtual の各インスタンスには、サーバー上での最小リソース割り当て（メモリ容量、CPU 数、およびディスク容量）が必要です。

設定	値
パフォーマンス階層	**バージョン 7.0 以降** 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。 • FTDv5 4vCPU/8GB（100 Mbps） • FTDv10 4vCPU/8GB（1 Gbps） • FTDv20 4vCPU/8GB（3 Gbps） • FTDv30 8vCPU/16GB（5 Gbps） • FTDv50 12vCPU/24GB（10 Gbps） • FTDv100 16vCPU/32GB（16 Gbps） Threat Defense Virtual 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* コンフィギュレーション ガイド』の「Firepower システムのライセンス」の章を参照してください。 （注） vCPU/メモリの値を変更するには、最初に Threat Defense Virtual デバイスの電源をオフにする必要があります。
ストレージ	50 GB（調整可能） • virtio ブロック デバイスをサポート

（注） Threat Defense Virtual 向けネットワークのデータインターフェイスの最小数は 4 つ（管理、診断、外部、内部）です。

Threat Defense Virtual ライセンス

- 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、『Firepower Management Center コンフィギュレーション ガイド』の「*Firepower* システムのライセンス」を参照してください。

Nutanix のコンポーネントとバージョン

コンポーネント	バージョン
Nutanix Acropolis OS（AOS）	5.15.5 LTS 以降
Nutanix クラスタチェック（NCC）	4.0.0.1
Nutanix AHV	20201105.12 以降
Nutanix Prism Web コンソール	-

注意事項と制約事項

サポートされる機能

- 展開モード：ルーテッド（スタンドアロン）、ルーテッド（HA）、インラインタップ、インライン、パッシブ、およびトランスペアレント
- ライセンス：BYOL のみ
- IPv6
- Threat Defense Virtual ネイティブ HA
- Device Manager
- ジャンボフレーム
- VirtIO

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、「Nutanix 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

- Nutanix AHV 上の Threat Defense Virtual は、インターフェイスのホットプラグをサポートしていません。Threat Defense Virtual の電源が入っているときに、インターフェイスの追加や削除を試みないでください。
- Nutanix AHV は SR-IOV および DPDK-OVS をサポートしていません。

（注） Nutanix AHV は、VirtIO を使用したゲスト内 DPDK をサポートします。詳細については、「AHV での DPDK サポート」を参照してください。

一般的なガイドライン

- ブートするには 2 つの管理インターフェイスと 2 つのデータ インターフェイスが必要合計 10 個のインターフェイスをサポート。

（注）
- Threat Defense Virtual のデフォルト設定では、管理インターフェイス、診断インターフェイス、および内部インターフェイスは同じサブネットに配置されます。
- ネットワーク インターフェイスを変更するときは、Threat Defense Virtual デバイスをオフにする必要があります。

- Threat Defense Virtual のデフォルト設定では、管理インターフェイス（管理と診断）および内部インターフェイスが**同じサブネット**上にあり、管理アドレスはインターネットへのゲートウェイとして内部アドレスを使用すると仮定します（外部インターフェイス経由）。
- Threat Defense Virtual は、少なくとも 4 つのインターフェイスを備え、firstboot で電源がオンになる必要があります。4 つのインターフェイスがなければ展開は実行されません。

- Threat Defense Virtual では、合計で 10 個のインターフェイスをサポートします（管理インターフェイス X 1 個、診断インターフェイス X 1 個、データトラフィック用ネットワークインターフェイス X 最大 8 個）。ネットワークへのインターフェイスの割り当ては、次の順番であることが必要です。
  1. 管理インターフェイス（必須）
  2. 診断インターフェイス（必須）
  3. 外部インターフェイス（必須）
  4. 内部インターフェイス（必須）
  5. 5 ～ 10 個のデータインターフェイス（オプション）

（注） Threat Defense Virtual 向けネットワークのデータインターフェイスの最小数は 3 つです。

- コンソールアクセスの場合、ターミナルサーバーは telnet を介してサポートされます。
- サポートされている vCPU とメモリのパラメータは次のとおりです。

CPU	メモリ	Threat Defense Virtual プラットフォームのサイズ
4	8 GB	4vCPU/8GB（デフォルト）
8	16 GB	8vCPU/16GB
12	24 GB	12 vCPU/24 GB
16	32 GB	16vCPU/32GB

- Threat Defense Virtual インターフェイスのネットワークアダプタ、送信元ネットワーク、宛先ネットワークに関する以下の用語索引を参照してください。

ネットワーク アダプタ	送信元ネットワーク	宛先ネットワーク	機能
vnic0*	Management0-0	Management0/0	管理
vnic1	診断	診断	診断
vnic2*	GigabitEthernet0-0	GigabitEthernet 0/0	外部
vnic3*	GigabitEthernet0-1	GigabitEthernet 0/1	内部
* 同じサブネットに接続します。			

関連資料

- Nutanix Release Notes
- Nutanix Field Installation Guide
- Nutanix でのハードウェアのサポート

Secure Firewall Threat Defense Virtual デバイスの管理方法

Secure Firewall Threat Defense Virtual デバイスの管理には次の 2 つのオプションを選択できます。

Secure Firewall Device Manager

Device Manager はオンボード統合マネージャです。

Device Manager は一部の Threat Defense デバイスに搭載された Web ベースの設定インターフェイスです。Device Manager では、小規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。また、これは多くの Threat Defense デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

（注） Device Manager をサポートする Threat Defense デバイスのリストについては、「Cisco Secure Firewall Device Manager Configuration Guide」を参照してください。

Secure Firewall Management Center

多数のデバイスを管理している場合、または Threat Defense で許可される、より複雑な機能や設定を使用したい場合は、組み込みの Device Manager の代わりに Management Center を使用してデバイスを設定します。

重要 Device Manager と Management Center の両方を使用して Threat Defense デバイスを管理することはできません。いったん Device Manager の統合管理を有効にすると、ローカル管理を無効にして、Management Center を使用するように管理を再設定しない限り、Management Center を使用して Threat Defense デバイスを管理することはできなくなります。一方、Threat Defense デバイスを Management Center に登録すると、Device Manager のオンボード管理サービスは無効になります。

注意 現在、シスコには Device Manager の設定を Management Center に移行するオプションはありません。その逆も同様です。Threat Defense デバイス用に設定する管理のタイプを選択する際は、このことを考慮してください。

Nutanix に展開するための前提条件

- Cisco.com から Threat Defense Virtual qcow2 ファイルをダウンロードします（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。

- 「概要 （1 ページ）」の章を確認します。
- Nutanix とシステムの互換性については、『Cisco Firepower Threat Defense Virtual Compatibility Guide』[英語] を参照してください。

Nutanix に Threat Defense Virtual を展開する方法

ステップ	タスク	詳細情報
1	前提条件を確認します。	Nutanix に展開するための前提条件 （9 ページ）
2	Threat Defense Virtual qcow2 ファイルを Nutanix 環境にアップロードします。	Threat Defense Virtual QCOW2 ファイルを Nutanix にアップロード （10 ページ）
3	（オプション）仮想マシンの展開時に適用される初期設定データを含む第 0 日の構成ファイルを準備します。	第 0 日のコンフィギュレーション ファイルの準備 （10 ページ）
4	Threat Defense Virtual を Nutanix 環境に展開します。	Threat Defense Virtual の導入 （12 ページ）
5	（任意）Threat Defense Virtual のセットアップに Day 0 の構成ファイルを使用しなかった場合は、CLI にログインして、セットアップを完了します。	Threat Defense Virtual のセットアップの完了 （14 ページ）

Threat Defense Virtual QCOW2 ファイルを Nutanix にアップロード

Threat Defense Virtual を Nutanix 環境に展開するには、Prism Web コンソールで Threat Defense Virtual qcow2 ディスクファイルからイメージを作成する必要があります。

始める前に

Cisco.com から Threat Defense Virtual qcow2 ディスクファイルをダウンロードします（https://software.cisco.com/download/navigator.html）。

ステップ 1 Nutanix Prism Web コンソールにログインします。

ステップ 2 歯車アイコンをクリックして [設定（Settings）] ページを開きます。

ステップ 3 左側のペインで [イメージの設定（Image Configuration）] をクリックします。

ステップ 4 [Upload Image] をクリックします。

ステップ 5 イメージを作成します。

1. イメージの名前を入力します。
2. [イメージタイプ（Image Type）] ドロップダウンリストから、[ディスク（DISK）] を選択します。
3. [ストレージコンテナ（Storage Container）] ドロップダウンリストから、目的のコンテナを選択します。
4. Threat Defense Virtual qcow2 ディスクファイルの場所を指定します。

   URL を指定して Web サーバーからファイルをインポートすることも、ワークステーションからファイルをアップロードすることもできます。
5. [保存（Save）] をクリックします。

ステップ 6 [イメージの設定（Image Configuration）] ページに新しいイメージが表示されるまで待ちます。

第 0 日のコンフィギュレーション ファイルの準備

Threat Defense Virtual を展開する前に、Day 0 の構成ファイルを準備できます。このファイルは、仮想マシンの導入時に適用される初期設定データを含むテキスト ファイルです。

次の点を考慮してください。

- 導入時に Day 0 の構成ファイルを使用すると、導入プロセスで Threat Defense Virtual アプライアンスの初期設定をすべて実行できます。
- 導入時に Day 0 の構成ファイルを使用しない場合は、起動後にシステムの必須設定を指定する必要があります。詳細については、「Threat Defense Virtual のセットアップの完了（14 ページ）」を参照してください。

次を指定することができます。

- エンド ユーザー ライセンス契約書（EULA）の承認。
- システムのホスト名。
- 管理者アカウントの新しい管理者パスワード。
- 最初のファイアウォール モード。最初のファイアウォール モード（**ルーテッド**または**トランスペアレント**）を設定します。

  ローカルの Device Manager を使用して展開を管理する予定の場合は、ファイアウォール モードに**ルーテッド**のみ設定できます。Device Manager を使用してトランスペアレント ファイアウォール モードのインターフェイスは設定できません。
- 管理モード。Secure Firewall Threat Defense Virtual デバイスの管理方法を参照してください。

  [ローカルに管理（ManageLocally）] を [はい（Yes）] に設定するか、または Management Center フィールド（[FmcIp]、[FmcRegKey]、および [FmcNatId]）に情報を入力することができます。使用していない管理モードでは、フィールドを空のままにします。
- アプライアンスが管理ネットワークで通信することを許可するネットワーク設定。

ステップ 1 任意のテキストエディタを使用して、新しいテキストファイルを作成します。

ステップ 2 次の例に示すように、テキストファイルに構成の詳細を入力します。

例：

```
#Firepower Threat Defense
{
    "EULA": "accept",
    "Hostname": "ftdv-production",
    "AdminPassword": "Admin123",
    "FirewallMode": "routed",
    "DNS1": "1.1.1.1",
    "DNS2": "1.1.1.2",
    "DNS3": "",
    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.44",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "disabled",
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
    "FmcIp": "",
    "FmcRegKey": "",
    "FmcNatId": "",
    "ManageLocally":"Yes"
}
```

（注） 第 0 日の構成ファイルの内容は、JSON 形式である必要があります。JSON 検証ツールを使用してテキストを検証する必要があります。

ステップ 3 ファイルを「**day0-config.txt**」として保存します。

ステップ 4 ステップ 1 ～ 3 を繰り返して、展開する Threat Defense Virtual ごとに一意のデフォルト構成ファイルを作成します。

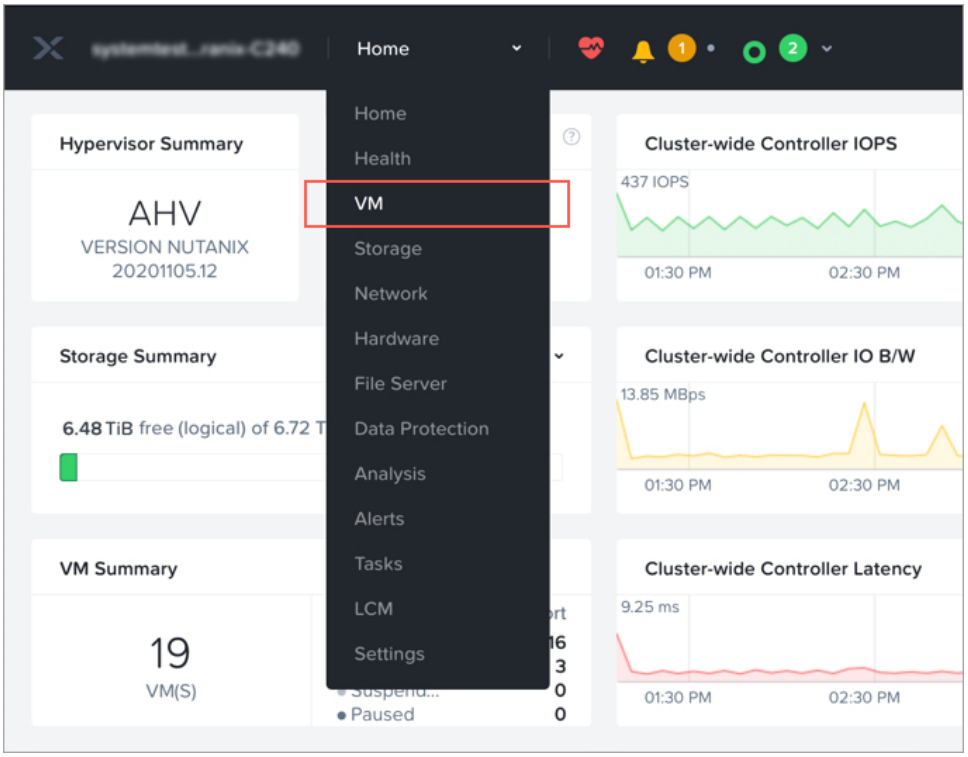
Threat Defense Virtual の導入

始める前に

展開する Threat Defense Virtual のイメージが [イメージの設定（Image Configuration）] ページに表示されていることを確認します。

ステップ 1 Nutanix Prism Web コンソールにログインします。

ステップ 2 メインメニューバーで、表示ドロップダウンリストをクリックし、[VM] を選択します。



ステップ 3 VM ダッシュボードで、[VMの作成（Create VM）] をクリックします。

ステップ 4 次の手順を実行します。

1. Threat Defense Virtual インスタンスの名前を入力します。
2. 必要に応じて、Threat Defense Virtual インスタンスの説明を入力します。
3. Threat Defense Virtual インスタンスで使用するタイムゾーンを選択します。

ステップ 5 コンピューティングの詳細を入力します。

1. Threat Defense Virtual インスタンスに割り当てる仮想 CPU の数を入力します。
2. 各仮想 CPU に割り当てる必要があるコアの数を入力します。
3. Threat Defense Virtual インスタンスに割り当てるメモリの量（GB）を入力します。

ステップ 6 Threat Defense Virtual インスタンスにディスクを接続します。

1. [ディスク（Disks）] で、[新しいディスクの追加（Add New Disk）] をクリックします。
2. [タイプ（Type）] ドロップダウンリストから、[ディスク（DISK）] を選択します。
3. [操作（Operation）] ドロップダウンリストから、[イメージサービスから複製（Clone from Image Service）] を選択します。
4. [バスタイプ（Bus Type）] ドロップダウンリストから、[PCI] または [SCSI] を選択します。
5. [イメージ（Image）] ドロップダウンリストから、使用するイメージを選択します。
6. [追加（Add）] をクリックします。

ステップ 7 少なくとも 4 つの仮想ネットワーク インターフェイスを設定します。

[ネットワークアダプタ（NIC）（Network Adapters (NIC)）] で、[新しいNIC の追加（Add New NIC）] をクリックし、ネットワークを選択して、[追加（Add）] をクリックします。

このプロセスを繰り返して、ネットワーク インターフェイスをさらに追加します。

Nutanix 上の Threat Defense Virtual は、合計で 10 個のインターフェイスをサポートします（管理インターフェイス X 1 個、診断インターフェイス X 1 個、データトラフィック用ネットワーク インターフェイス X 最大 8 個）。ネットワークへのインターフェイスの割り当ては、次の順番であることが必要です。

- vnic0：管理インターフェイス（必須）
- vnic1：診断インターフェイス（必須）
- vnic2：外部インターフェイス（必須）
- vnic3：内部インターフェイス（必須）
- vnic4-9：データ インターフェイス（オプション）

ステップ 8 Threat Defense Virtual のアフィニティポリシーを設定します。

[VMホストアフィニティ（VM Host Affinity）] で、[アフィニティの設定（Set Affinity）] をクリックし、ホストを選択して、[保存（Save）] をクリックします。

ノードに障害が発生した場合でも Threat Defense Virtual を実行できるようにするには、1 つ以上のホストを選択します。

ステップ 9 第 0 日の構成ファイルを準備済みの場合は、次の手順を実行します。

1. [カスタムスクリプト（Custom Script）] を選択します。

2. [ファイルをアップロード（Upload A File）] をクリックし、第 0 日の構成ファイル（**day0-config.txt**）を選択します。

（注） 他のすべてのカスタム スクリプト オプションは、このリリースではサポートされていません。

ステップ 10 [保存（Save）] をクリックして、Threat Defense Virtual を展開します。VM テーブルビューに Threat Defense Virtual インスタンスが表示されます。

ステップ 11 VM テーブルビューで、新しく作成した Threat Defense Virtual インスタンスを選択し、[電源オン（Power On）] をクリックします。

次のタスク

- Day 0 構成ファイルを使用して Threat Defense Virtual をセットアップした場合、次の手順は選択した管理モードによって異なります。
  - [ローカルに管理（ManageLocally）] で [いいえ（No）] を選択した場合は、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理」を参照してください。
- Threat Defense Virtual のセットアップに Day 0 の構成ファイルを使用しなかった場合は、CLI にログインして、Threat Defense Virtual のセットアップを完了します。この説明については、Threat Defense Virtual のセットアップの完了 （14 ページ） を参照してください。

Threat Defense Virtual のセットアップの完了

Threat Defense Virtual アプライアンスには Web インターフェイスがないため、Day 0 の構成ファイルを使用せずに導入した場合には、CLI を使用して仮想デバイスを設定する必要があります。

ステップ 1 Threat Defense Virtual でコンソールを開きます。

ステップ 2 [firepower ログイン（firepower login）] プロンプトで、ユーザー名 *admin* とパスワード *Admin123* のデフォルトのクレデンシャルでログインします。

ステップ 3 Threat Defense Virtual システムが起動すると、セットアップウィザードでシステムの設定に必要な次の情報の入力が求められます。

- 使用許諾契約の同意
- 新しい管理者パスワード
- IPv4 または IPv6 の構成
- IPv4 または IPv6 の DHCP 設定
- 管理ポートの IPv4 アドレスとサブネットマスク、または IPv6 アドレスとプレフィックス

- システム名
- デフォルトゲートウェイ
- DNS セットアップ
- HTTP プロキシ
- 管理モード（ローカル管理が必要）

ステップ 4 セットアップウィザードの設定を確認します。デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

ステップ 5 プロンプトに従ってシステム設定を行います。

ステップ 6 コンソールが # プロンプトに戻るときに、設定が正常に行われたことを確認します。

ステップ 7 CLI を閉じます。

次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャを有効にする（Enable Local Manager）] で [いいえ（No）] を選択した場合は、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理」を参照してください。

管理オプションの選択方法の概要については、「Secure Firewall Threat Defense Virtual デバイスの管理方法」を参照してください。

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。