Threat Defense Virtual の KVM への展開

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

- 概要 （1 ページ）
- システム要件 （2 ページ）
- 注意事項と制約事項 （4 ページ）
- Secure Firewall Threat Defense Virtual デバイスの管理方法 （8 ページ）
- 前提条件 （9 ページ）
- エンドツーエンドの手順 （11 ページ）
- 第 0 日のコンフィギュレーション ファイルの準備 （12 ページ）
- Threat Defense Virtual の起動 （15 ページ）
- トラブルシューティング （21 ページ）

概要

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。

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、100Mbps	4 コア/8 GB	100Mbps	50
FTDv10、1Gbps	4 コア/8 GB	1Gbps	250
FTDv20、3Gbps	4 コア/8 GB	3 Gbps	250
FTDv30、5Gbps	8 コア/16 GB	5 Gbps	250
FTDv50、10Gbps	12 コア/24 GB	10 Gbps	750
FTDv100、16 Gbps	16 コア/32 GB	16 Gbps	10,000

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、『*Cisco Secure Firewall Management Center*』の「Licensing the System」の章を参照してください。

システム要件

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 Secure Firewall Threat Defense Compatibility Guide』を参照してください。

Threat Defense Virtual の導入に使用される特定のハードウェアは、導入するインスタンス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。

表 *2 : Threat Defense Virtual* アプライアンスのリソース要件

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、『*Cisco Secure Firewall Management Center Configuration*』の「Licensing the System」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。
コアおよびメモリの数	**バージョン 6.4 からバージョン 6.7** Threat Defense Virtual は、調整可能な vCPU およびメモリリソースを使用して展開されます。サポートされている vCPU/メモリのペアの値は、次の 3 つです。 • 4 vCPU/8 GB（デフォルト） • 8 vCPU/16 GB • 12 vCPU/24 GB （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。上記の 3 つの組み合わせだけがサポートされます。

設定	値
	バージョン 6.3 以前 Threat Defense Virtual は、固定の vCPU およびメモリリソースを使用して展開されます。サポートされている vCPU/メモリのペアの値は次の 1 つだけです。 • 4 vCPU/8 GB （注） vCPU とメモリの調整はサポートされていません。
ハードディスク プロビジョニング サイズ	• 50 GB • 調整可能な設定です。virtio ブロック デバイスをサポート
vNIC	KVM の Threat Defense Virtual は次の仮想ネットワークアダプタをサポートしています。 • **VIRTIO**：Virtio は、KVM の IO 仮想化のメインプラットフォームであり、IO 仮想化のハイパーバイザに共通のフレームワークを提供します。ホストの実装はユーザー空間（QEMU）にあるため、ホストにドライバは必要ありません。 • **IXGBE-VF**：ixgbe-vf（10 ギガビット/秒）ドライバは、SR-IOV をサポートするカーネルでのみアクティブ化できる仮想関数デバイスをサポートしています。SR-IOV には適切なプラットフォームおよび OS のサポートが必要です。詳細については、「SR-IOV のサポート」を参照してください。

注意事項と制約事項

- 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

（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。

- Virtio ドライバをサポート
- SR-IOV の ixgbe-vf ドライバをサポート

- 合計 11 個のインターフェイスをサポート。

- Threat Defense Virtual のデフォルト設定は、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ことを前提としています（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 11 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 9 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。
  - 管理インターフェイス（1）（必須）

（注） 6.7 以降では、管理インターフェイスの代わりに、必要に応じて、データインターフェイスを Management Center の管理に使用できます。管理インターフェイスはデータインターフェイス管理の前提条件であるため、初期設定でこれを設定する必要があります。データインターフェイスから Management Center へのアクセスは、高可用性の展開ではサポートされません。Management Center へのアクセスに関するデータインターフェイス設定の詳細については、『FTD command reference』の **configure network management-data-interface** コマンドを参照してください。

  - 診断インターフェイス（2）（必須）
  - 外部インターフェイス（3）（必須）
  - 内部インターフェイス（4）（必須）
  - データインターフェイス（5 ～ 11）（オプション）

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。

表 *3*：送信元から宛先ネットワークへのマッピング

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*	Diagnostic 0-0	Diagnostic0/0	診断
vnic2	GigabitEthernet0-0	GigabitEthernet 0/0	外部

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
vnic3*	GigabitEthernet0-1	GigabitEthernet 0/1	内部
* 重要同じサブネットに接続します。			

- 仮想マシンの複製はサポートされません。
- コンソールアクセスでは、Telnet を介したターミナルサーバーをサポートします。

CPU モード

KVM は、さまざまな種類の CPU をエミュレートできます。VM の場合、通常はホストシステムの CPU に厳密に一致するプロセッサタイプを選択する必要があります。これにより、ホストの CPU 機能（CPU フラグとも呼ばれます）が VM で使用できるようになります。CPU タイプを**ホスト**に設定する必要があります。その場合、VMはホストシステムとまったく同じCPUフラグを持ちます。

クラスタリング

バージョン 7.2 以降、クラスタリングは KVM で展開された Threat Defense Virtual インスタンスでサポートされます。詳細については、『プライベートクラウドにおける Threat Defense Virtual のクラスタリング』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、「KVM 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。

SR-IOV のサポート

SR-IOV 仮想機能には特定のシステムリソースが必要です。SR-IOV 対応 PCIe アダプタに加えて、SR-IOV をサポートするサーバーが必要です。

SR-IOV インターフェイスを使用する KVM 上の Threat Defense Virtual では、インターフェイスタイプの混在がサポートされています。管理インターフェイスには SR-IOV または VMXNET3 を使用し、データインターフェイスには SR-IOV を使用することができます。

以下のハードウェア検討事項に留意する必要があります。

- 使用可能な VF の数を含む SR-IOV NIC の機能は、ベンダーやデバイスによって異なります。次の NIC がサポートされています。

- Intel Ethernet Server Adapter X710
- Intel Ethernet Server Adapter X520 - DA2
- Intel Ethernet Network Adapter E810-CQDA2
  - ファームウェア (NVM イメージ) とネットワークドライバーは、NVM ユーティリティツールを使用して Intel® Network Adapter E810 で更新されます。不揮発性メモリ (NVM) イメージとネットワークドライバーは、Intel® Network Adapter E810 上で組み合わせて更新する互換性のあるコンポーネントのセットです。NVM とソフトウェアの互換性マトリックスについては、「Intel® Ethernet Controller E810 データシート」を参照して、Intel® Network Adapter E810 の正しいファームウェアドライバーを更新してください。

- すべての PCIe スロットが SR-IOV をサポートしているわけではありません。
- SR-IOV 対応 PCIe スロットは機能が異なる場合があります。
- x86_64 マルチコア CPU：Intel Sandy Bridge 以降（推奨）。

（注） シスコでは、Threat Defense Virtual を 2.3GHz の Intel Broadwell CPU（E5-2699-v4）でテストしました。

- コア
  - CPU ソケットあたり 8 個以上の物理コア。
  - 単一のソケット上で 8 コアにする必要があります。

（注） CPU ピンニングは、フルスループットを実現するために推奨されています。

- メーカーのマニュアルで、お使いのシステムの SR-IOV サポートを確認する必要があります。KVM の場合は、SR-IOV サポートの CPU の互換性を確認できます。KVM 上の Threat Defense Virtual では、x86 ハードウェアしかサポートされないことに注意してください。

ixgbe-vf インターフェイスの使用の制限事項

ixgbe-vf インターフェイスを使用する場合、次の制限事項があります。

- ゲスト VM では、VF を無差別モードに設定できません。そのため、ixgbe-vf の使用時はトランスペアレント モードがサポートされません。
- ゲスト VM では、VF 上で MAC アドレスを設定できません。そのため、HA 中は MAC アドレスが転送されません。他の Threat Defense Virtual プラットフォームや他のインターフェ

イスタイプを使用した場合は転送されます。HA フェールオーバーは、IP アドレスをアクティブからスタンバイに移行することによって機能します。

（注） この制限は、i40e-vf インターフェイスにも適用されます。

- Cisco UCSB サーバーは ixgbe-vf の vNIC をサポートしません。
- フェールオーバー セットアップでは、ペアになっている Threat Defense Virtual（プライマリ装置）に障害が発生すると、スタンバイ Threat Defense Virtual 装置がプライマリ装置のロールを引き継ぎ、そのインターフェイス IP アドレスがスタンバイ Threat Defense Virtual 装置の新しい MAC アドレスで更新されます。その後、Threat Defense Virtual は Gratuitous Address Resolution Protocol（ARP）更新を送信して、インターフェイス IP アドレスの MAC アドレスの変更を同じネットワーク上の他のデバイスに通知します。ただし、インターフェイスタイプの非互換性により、Gratuitous ARP 更新は、インターフェイス IP アドレスをグローバル IP アドレスに変換するための NAT または PAT ステートメントで定義されているグローバル IP アドレスに送信されません。

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。

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

Secure Firewall Threat Defense Virtual を管理するには、2 つのオプションがあります。

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。

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。

前提条件

- 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。

- このマニュアルの導入例では、ユーザーが Ubuntu 18.04 LTS を使用していることを前提としています。Ubuntu 18.04 LTS ホストの最上部に次のパッケージをインストールします。
  - qemu-kvm
  - libvirt bin

- bridge-utils
- Virt-Manager
- virtinst
- virsh tools
- genisoimage

- パフォーマンスはホストとその設定の影響を受けます。ホストを調整することで、KVM での Threat Defense Virtual のスループットを最大化できます。一般的なホスト調整の概念については、『Network Function Virtualization: Quality of Service in Broadband Remote Access Servers with Linux and Intel Architecture』を参照してください。
- 以下の機能は Ubuntu 18.04 LTS の最適化に役立ちます。
  - macvtap：高性能の Linux ブリッジ。Linux ブリッジの代わりに macvtap を使用できます。ただし、Linux ブリッジの代わりに macvtap を使用する場合は、特定の設定を行う必要があります。
  - Transparent Huge Pages：メモリ ページ サイズを増加させます。Ubuntu 18.04 では、デフォルトでオンになっています。
  - Hyperthread disabled：2 つの vCPUを 1 つのシングル コアに削減します。
  - txqueuelength：デフォルトの txqueuelength を 4000 パケットに増加させ、ドロップ レートを低減します。
  - pinning：qemu および vhost プロセスを特定のCPU コア にピン接続します。特定の条件下では、ピン接続によってパフォーマンスが大幅に向上します。
- RHEL ベースのディストリビューションの最適化については、『Red Hat Enterprise Linux6 Virtualization Tuning and Optimization Guide』を参照してください。
- KVM 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。
- 次の方法で、仮想マシンが KVM を実行しているかどうかを確認します。
  - **lsmod** を実行して、Linux カーネルのモジュールの一覧を表示します。KVM が実行されている場合は、次の出力が表示されます。

    root@kvm-host:~$ lsmod | grep kvm

    kvm_intel 123675 0

    kvm 257361 1 kvm_intel

- **ls -l /dev/kvm** が対象の VM に存在しない場合は、おそらく **QEMU** を実行しており、KVM ハードウェアアシスト機能を利用していません。

  root@kvm-host:~$ ls -l /dev/kvm

  crw------- 1 root root 10, 232 Mar 23 13:53 /dev/kvm

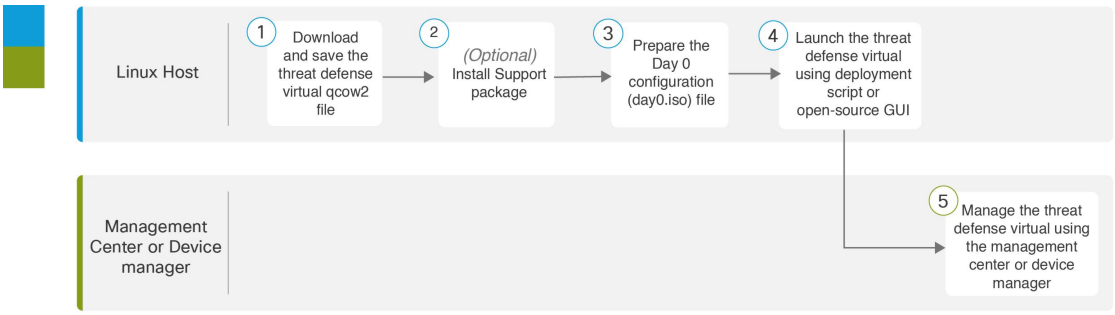
- 次のコマンドを実行して、ホストマシンが KVM をサポートしているかどうかも確認します。

  root@kvm-host:~$ sudo kvm-ok

- KVM アクセラレーションを使用することもできます。

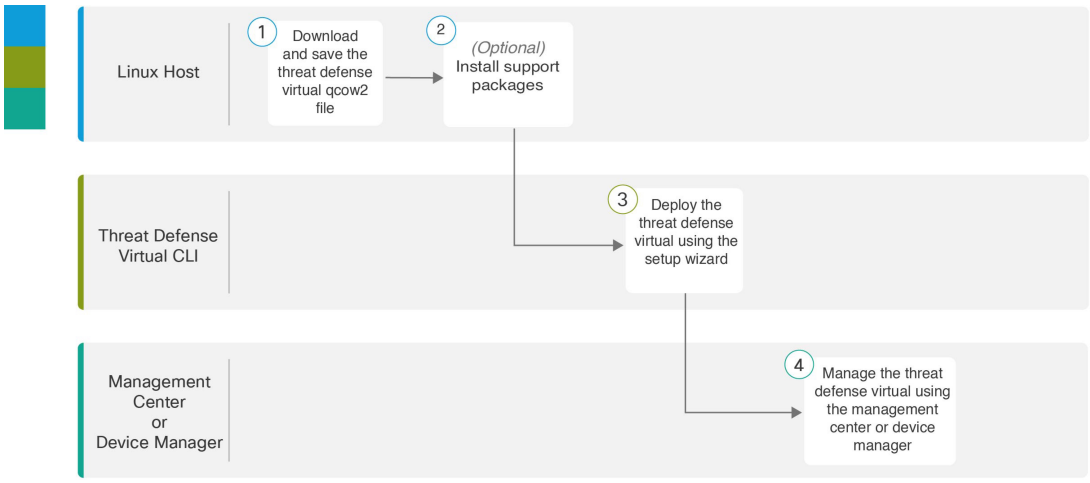
エンドツーエンドの手順

次のフローチャートは、Day 0 の構成ファイルを使用して KVM インスタンスに 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	前提条件 （9 ページ） ：Linux ホストに Threat Defense Virtual qcow2 ファイルをダウンロードして保存します。
2	Linux ホスト	前提条件 （9 ページ） ：サポートパッケージをインストールします。
3	Linux ホスト	第 0 日のコンフィギュレーション ファイルの準備
4	Linux ホスト	Threat Defense Virtual の起動： • 導入スクリプトを使用した起動 • グラフィカル ユーザー インターフェイス（GUI）の起動
5	Management Center	Management Center を使用した Threat Defense Virtual の管理：

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 KVM インスタンスに 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	前提条件 （9 ページ） ：Linux ホストに Threat Defense Virtual qcow2 ファイルをダウンロードして保存します。
2	Linux ホスト	前提条件 （9 ページ） ：サポートパッケージをインストールします。
3	Threat Defense Virtual CLI	第 0 日のコンフィギュレーション ファイルを使用しない起動：セットアップウィザードを使用して Threat Defense Virtual を展開します。
4	Management Center	Management Center を使用した Threat Defense Virtual の管理

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 を起動する前に、第 0 日用のコンフィギュレーション 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。この初期設定は、「day0-config」というテキスト ファイルとして指定の作業ディレクトリに格納され、さらに day0.iso ファイルへと処理されます。この day0.iso ファイルが最初の起動時にマウントされて読み取られます。

重要 day0.iso ファイルは、最初のブート時に使用できる必要があります。

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。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。
- 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。
- 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 モードには**ルーテッド**のみを設定できます。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。
- 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。
- Threat Defense Virtual をクラスタモードで展開するかスタンドアロンモードで展開するかを指定できる展開タイプ。

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、「第 0 日のコンフィギュレーション ファイルを使用しない起動 （20 ページ）」を参照してください。

（注） この例では Linux が使用されていますが、Windows の場合にも同様のユーティリティがあります。

手順の概要

1. 「day0-config」というテキスト ファイルに Threat Defense Virtual の CLI 設定を記入します。ネットワーク設定と Management Center の管理に関する情報を追加します。
2. テキスト ファイルを ISO ファイルに変換して仮想CD-ROM を生成します。
3. 手順を繰り返して、導入する Device Manager ごとに一意のデフォルト設定ファイルを作成します。

手順の詳細

手順

ステップ 1 「day0-config」というテキスト ファイルに Threat Defense Virtual の CLI 設定を記入します。ネットワーク設定と Management Center の管理に関する情報を追加します。

例：

```
#Firepower Threat Defense
{
```

```
    "EULA": "accept",
    "Hostname": "ftdv-production",
    "AdminPassword": "r2M$9^Uk69##",
    "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": "",
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
    "FmcIp": "",
    "FmcRegKey": "",
    "FmcNatId": "",
    "ManageLocally":"No"
}
```

ローカルの Device Manager を使用するには、Day 0 の構成ファイル内で [ローカルに管理（ManageLocally）] に対して [はい（Yes）] と入力します。または、Management Center のフィールド（[FmcIp]、[FmcRegKey]、および [FmcNatId]）に入力します。使用していない管理オプションの場合は、これらのフィールドを空白のままにします。

ステップ 2 テキスト ファイルを ISO ファイルに変換して仮想CD-ROM を生成します。

例：

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

または

例：

```
/usr/bin/mkisofs -r -o day0.iso day0-config
```

ステップ 3 手順を繰り返して、導入する Device Manager ごとに一意のデフォルト設定ファイルを作成します。

次のタスク

- virt-install を使用している場合は、virt-install コマンドに次の行を追加します。

  ```
  --disk path=/home/user/day0.iso,format=iso,device=cdrom \
  ```

- virt-manager を使用している場合、virt-manager の GUI を使用して仮想 CD-ROM を作成できます。「グラフィカル ユーザー インターフェイス（GUI）の起動 （17 ページ）」を参照してください。

Threat Defense Virtual の起動

導入スクリプトを使用した起動

virt-install ベースの導入スクリプトを使用して Threat Defense Virtual を起動できます。

環境に最適なゲスト キャッシング モードを選択してパフォーマンスを最適化できることに注意してください。使用中のキャッシュ モードは、データ損失が発生するかどうかに影響を与え、キャッシュ モードはディスクのパフォーマンスにも影響します。

各 KVM ゲスト ディスク インターフェイスで、指定されたいずれかのキャッシュモード（*writethrough*、*writeback*、*none*、*directsync*、または *unsafe*）を指定できます。*writethrough* モードは読み取りキャッシュを提供します。*writeback* は読み取り/書き込みキャッシュを提供します。*directsync* はホストページキャッシュをバイパスします。*unsafe* はすべてのコンテンツをキャッシュし、ゲストからのフラッシュ要求を無視する可能性があります。

- *cache=writethrough* は、ホストで突然の停電が発生した場合の KVM ゲスト マシン上のファイル破損を低減できます。*writethrough* モードの使用をお勧めします。
- ただし、*cache=writethrough* は、*cache=none* よりディスク I/O 書き込みが多いため、ディスク パフォーマンスに影響する可能性もあります。
- *--disk* オプションの cache パラメータを削除する場合、デフォルトは *writethrough* になります。
- キャッシュ オプションを指定しないと、VM を作成するために必要な時間も大幅に短縮される場合もあります。これは、古いRAID コントローラにはディスク キャッシング能力が低いものがあることが原因です。そのため、ディスク キャッシングを無効にして（*ache=none*）、*writethrough* をデフォルトに設定すると、データの整合性を確保できます。
- Threat Defense Virtual のバージョン 6.4 以降は、調整可能な vCPU およびメモリリソースを使用して展開されます。6.4 より前のバージョンの Threat Defense Virtual は、固定構成の 4 vCPU/8 GB デバイスとして展開されていました。各 Threat Defense Virtual プラットフォームサイズの --vcpus および --ram パラメータでサポートされている値については、次の表を参照してください。

表 *4 : virt-install* でサポートされる *vCPU* およびメモリ パラメータ

--vcpus	--ram	Threat Defense Virtual プラットフォームのサイズ
4	8192	4vCPU/8GB（デフォルト）
8	16384	8vCPU/16GB
12	24576	12vCPU/24GB

手順

ステップ 1 「virt_install_ftdv.sh」という virt-install スクリプトを作成します。

Threat Defense Virtual VM の名前は、この KVM ホスト上の他の仮想マシン（VM）全体において一意であることが必要です。Threat Defense Virtual は最大 10 個のネットワーク インターフェイスをサポートできます。この例では、4 つのインターフェイスを使用しています。仮想 NIC は VirtIO にする必要があります。

（注）
Threat Defense Virtual のデフォルト設定は、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を**同じサブネット**上に配置することを前提としてます。システムでは、少なくとも 4 つのインターフェイスが正常に起動する必要があります。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)（任意）データインターフェイス：最大6

例：

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=ftdv \
   --arch=x86_64 \
   --cpu host \
   --vcpus=8 \
   --ram=16384 \
   --os-type=linux \
   --os-variant=generic26 \
   --virt-type=kvm \
   --import \
   --watchdog i6300esb,action=reset \
   --disk path=<ftd_filename>.qcow2,format=qcow2,device=disk,bus=virtio,cache=none \
   --disk path=<day0_filename>.iso,format=iso,device=cdrom \
   --console pty,target_type=serial \
   --serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \
   --force
```

ステップ 2 virt_install スクリプトを実行します。

例：

```
/usr/bin/virt_install_ftdv.sh
```

```
Starting install...
Creating domain...
```

ウィンドウが開き、VMのコンソールが表示されます。VMが起動中であることを確認できます。VMが起動するまでに数分かかります。VM が起動したら、コンソール画面から CLI コマンドを実行できます。

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。

- [ローカルに管理（Manage Locally）] 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。

グラフィカル ユーザー インターフェイス（GUI）の起動

GUI を使用して KVM 仮想マシンを管理するためのオープンソースオプションがいくつかあります。以下の手順では、virt-manager（Virtual Machine Manager とも呼ばれる）を使用して Threat Defense Virtual を起動します。virt-manager は、ゲスト仮想マシンを作成および管理するためのグラフィカルツールです。

（注） KVM は、さまざまな種類の CPU をエミュレートできます。VM の場合、通常はホストシステムの CPU に厳密に一致するプロセッサタイプを選択する必要があります。これにより、ホストの CPU 機能（CPU フラグとも呼ばれます）が VM で使用できるようになります。CPU タイプを**ホスト**に設定する必要があります。その場合、VMはホストシステムとまったく同じCPUフラグを持ちます。

手順

ステップ 1 virt-manager を起動します（**[アプリケーション（Applications）] > [システムツール（System Tools）] > [仮想マシンマネージャ（Virtual Machine Manager）]**）。

ハイパーバイザの選択、およびルート パスワードの入力を求められる可能性があります。

ステップ 2 左上隅のボタンをクリックし、[VMの新規作成（New VM）] ウィザードを開きます。

ステップ 3 仮想マシンの詳細を入力します。

a) オペレーティング システムの場合、[既存のディスクイメージをインポート（Import existing disk image）] を選択します。

この方法でディスク イメージ（事前にインストールされた、ブート可能なオペレーティング システムを含んでいるもの）をインポートできます。

b) [次へ（Forward）] をクリックして続行します。

ステップ 4 ディスク イメージをロードします。

a) [参照...（Browse...）] をクリックしてイメージ ファイルを選択します。
b) [OSタイプ（OS type）] には [汎用（Generic）] を選択します。
c) [次へ（Forward）] をクリックして続行します。

ステップ 5 メモリおよび CPU オプションを設定します。

重要
Threat Defense Virtual のバージョン 7.0 以降は、展開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。バージョン 7.0 より前は、Threat Defense Virtual の展開で vCPU やメモリ構成のオプションに制限がありました。「システム要件（2 ページ）」を参照してください。

各 Threat Defense Virtual プラットフォームの --vcpus および --ram パラメータでサポートされているパフォーマンス階層と値については、次の表を参照してください。

表 5：仮想マシンマネージャでサポートされる *vCPU* およびメモリパラメータ

CPU	メモリ	Threat Defense Virtual プラットフォームのサイズ
4	8192	4vCPU/8GB（デフォルト）
8	16384	8vCPU/16GB
12	24576	12vCPU/24GB

a) Threat Defense Virtual プラットフォームサイズに対応する**メモリ（RAM）**パラメータを設定します。
b) Threat Defense Virtual プラットフォームサイズに対応する **CPU** パラメータを設定します。
c) [次へ（Forward）] をクリックして続行します。

ステップ 6 [インストール前に設定をカスタマイズする（Customize configuration before install）] チェックボックスをオンにして、[名前（Name）] を指定してから [完了（Finish）] をクリックします。

この操作を行うと、別のウィザードが開き、仮想マシンのハードウェア設定を追加、削除、設定することができます。

ステップ 7 CPU 構成を次のように変更します。

左側のパネルから [プロセッサ（Processor）] を選択し、**[設定（Configuration）]** > **[ホストCPU構成のコピー（Copy host CPU configuration）]** を選択します。

これによって、物理ホストの CPU モデルと設定が VM に適用されます。

ステップ 8 仮想ディスクを設定します。

a) 左側のパネルから [ディスク1（Disk 1）] を選択します。
b) [詳細オプション（Advanced Options）] をクリックします。

c) [ディスクバス（Disk bus）] を [Virtio] に設定します。
d) [ストレージ形式（Storage format）] を [qcow2] に設定します。

ステップ 9 シリアル コンソールを設定します。

a) 左側のパネルから [コンソール（Console）] を選択します。
b) [削除（Remove）] を選択してデフォルト コンソールを削除します。
c) [ハードウェアを追加（Add Hardware）] をクリックしてシリアル デバイスを追加します。
d) [デバイスタイプ（Device Type）] で、[TCP net console (tcp)] を選択します。
e) [モード（Mode）] で、[サーバーモード（バインド）（Server mode (bind)）] を選択します。
f) [ホスト（Host）] には「**0.0.0.0**」と入力し、IP アドレスと一意の**ポート**番号を入力します。
g) [Telnetを使用（Use Telnet）] ボックスをオンにします。
h) デバイス パラメータを設定します。

ステップ 10 KVMゲストがハングまたはクラッシュしたときに何らかのアクションが自動でトリガーされるようウォッチドッグ デバイスを設定します。

a) [ハードウェアを追加（Add Hardware）] をクリックしてウォッチドック デバイスを追加します。
b) [モデル（Model）] で、[デフォルト（default）] を選択します。
c) [アクション（Action）] で、[ゲストを強制的にリセット（Forcefully reset the guest）] を選択します。

ステップ 11 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。

[ハードウェアの追加（Add Hardware）] をクリックしてインターフェイスを追加し、**macvtap** を選択するか、共有デバイス名を指定します（ブリッジ名を使用）。

（注）
KVM 上の Threat Defense Virtual では、合計で 11 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 9 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 ～ 10：データインターフェイス（オプション）

重要
vnic0、vnic1、および vnic3 は、必ず同じサブネットにマップするようにしてください。

ステップ 12 第 0 日のコンフィギュレーション ファイルを使用して展開する場合、ISO の仮想 CD-ROM を作成します。

a) [ハードウェアを追加（Add Hardware）] をクリックします。
b) [ストレージ（Storage）] を選択します。
c) [管理対象またはその他既存のストレージを選択（Select managed or other existing storage）] をクリックし、ISO ファイルの場所を参照します。
d) [デバイスタイプ（Device type）] で、[IDE CDROM] を選択します。

ステップ 13 仮想マシンのハードウェアを設定した後、[適用（Apply）] をクリックします。

ステップ 14 virt-manager の [インストールの開始（Begin installation）] をクリックして、指定したハードウェア設定で仮想マシンを作成します。

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。

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。

第 0 日のコンフィギュレーション ファイルを使用しない起動

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。

新しく展開されたデバイスに初めてログインするときに、EULA を読んで同意する必要があります。次に、セットアッププロンプトに従って管理パスワードを変更し、デバイスのネットワーク設定およびファイアウォールモードを設定します。

セットアッププロンプトに従う際に、複数の選択肢がある質問では、選択肢が (*y/n*) のように括弧で囲まれて示されます。デフォルト値は、[*y*] のように大カッコ内に列挙されます。選択を確定するには、Enter キーを押します。

（注） 初期セットアップの完了後に仮想デバイスに関するこれらの設定を変更するには、CLI を使用する必要があります。

手順

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 の構成
- IPv4 の DHCP 設定
- 管理ポートの IPv4 アドレスとサブネットマスク
- 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。

トラブルシューティング

ここでは、仮想マシンへの KVM 導入に関連する基本的なトラブルシューティング手順について説明します。

仮想マシンが KVM を実行しているかどうかを確認

次の方法で、仮想マシンが KVM を実行しているかどうかを確認します。

- **lsmod** コマンドを実行して、Linux カーネルのモジュールの一覧を表示します。KVM が実行されている場合は、次の出力が表示されます。

  root@kvm-host:~$ lsmod | grep kvm

  kvm_intel 123675 0

kvm 257361 1 kvm_intel

- **ls -l /dev/kvm** コマンドが対象の VM に存在しない場合は、おそらく **QEMU** を実行しており、KVM ハードウェアアシスト機能を利用していません。

  root@kvm-host:~$ ls -l /dev/kvm

  crw------- 1 root root 10, 232 Mar 23 13:53 /dev/kvm

- 次のコマンドを実行して、ホストマシンが KVM をサポートしているかどうかも確認します。

  root@kvm-host:~$ sudo kvm-ok

- KVM アクセラレーションを使用することもできます。

Threat Defense Virtual の導入中にブートループが発生する

仮想マシンでブートループが発生した場合は、次のことを確認する必要があります。

- 導入先の VM が 8 GB 以上のメモリを備えているかを確認します。
- 導入先の VM が 4 つ以上のインターフェイスを備えているかを確認します。
- 導入先の VM が 4 つ以上の vCPU を備えているかを確認します。
- QEMU プロセスがサーバークラスの CPU（SandyBridge、IvyBridge、Haswell など）を使用しているかを確認します。**ps -edaf | grep qemu** コマンドを使用してプロセスのパラメータを調べます。

Management Center Virtual の導入中にブートループが発生する

仮想マシンでブートループが発生した場合は、次のことを確認する必要があります。

- 導入先の VM が 28 GB 以上のメモリを備えているかを確認します。
- 導入先の VM が 4 つ以上のインターフェイスを備えているかを確認します。
- 導入先の VM が 4 つ以上の vCPU を備えているかを確認します。
- QEMU プロセスがサーバークラスの CPU（SandyBridge、IvyBridge、Haswell など）を使用しているかを確認します。**ps -edaf | grep qemu** コマンドを使用してプロセスのパラメータを調べます。

導入後のトラブルシューティング

Threat Defense Virtual で **system generate-troubleshoot <space> ALL** コマンドを実行して問題を確認し、デバッグ用のログをキャプチャします。

または、**system generate-troubleshoot <space>** の後に疑問符（**?**）または**タブ**ボタンを使用すると、使用可能なオプションやコマンドが表示されます。

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。