



# KVM による Firepower Management Center Virtual の展開

Cisco Firepower Management Center Virtual (FMCv) は KVM に導入できます。

- [KVM を使用した導入について \(1 ページ\)](#)
- [KVM を使用した導入の前提条件 \(2 ページ\)](#)
- [注意事項と制約事項 \(3 ページ\)](#)
- [第 0 日のコンフィギュレーション ファイルの準備 \(3 ページ\)](#)
- [の起動 FMCv \(5 ページ\)](#)
- [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導入 \(11 ページ\)](#)

## KVM を使用した導入について

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。

KVM 上の Firepower Management Center Virtual (FMCv) は次をサポートします。

- プロセッサ
  - 4 個の vCPU が必要
- メモリ
  - 32 GB の RAM が必要
- ネットワーキング
  - virtio ドライバをサポート

- 1 個の管理インターフェイスをサポート
- 仮想マシンあたりのホスト ストレージ
  - FMCv には 250 GB が必要
  - virtio および scsi ブロック デバイスをサポート
- コンソール
  - Telnet を介したターミナル サーバをサポート

## KVM を使用した導入の前提条件

- Cisco.com から Firepower 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>
- 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、ユーザが Ubuntu 14.04 LTS を使用していることを前提としています。Ubuntu 14.04 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 14.04 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 14.04 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。

## 注意事項と制約事項

- Firepower Management Center Virtual のアプライアンスにシリアル番号はありません。[システム (System)] > [設定 (Configuration)] ページには、仮想プラットフォームに応じて、[なし (None)] または [未指定 (Not Specified)] のいずれかが表示されます。
- 仮想マシンの複製はサポートされません。
- ハイ アベイラビリティはサポートされません。

## 第 0 日のコンフィギュレーション ファイルの準備

FMCv 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。第 0 日のコンフィギュレーションは、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。



(注) 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。

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、プロセスで、FMCv アプライアンスの初期設定全体を実行できます。次を指定することができます。

- EULA への同意
- 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
- アプライアンスが管理ネットワーク上で通信できるようにするネットワーク設定 : 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で導入する場合、起動後に Firepower システムの必須設定を実行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導入 \(11 ページ\)](#)』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。

- デフォルトの Cisco Umbrella DNS サーバを使用するには、両方の DNS エントリを空のままにします。非 DNS 環境で動作するには、両方のエントリを「None」に設定します（大文字と小文字は区別しない）。

**ステップ 1** 「day0-config」というテキストファイルに FMCv のネットワーク設定の CLI 設定を記入します。

例：

```
#FMC
{
  "EULA": "accept",
  "Hostname": "FMC-Production",
  "AdminPassword": "Admin123",
  "DNS1": "64.102.6.247",
  "DNS2": "64.102.6.248",

  "IPv4Mode": "manual",
  "IPv4Addr": "10.12.129.45",
  "IPv4Mask": "255.255.0.0",
  "IPv4Gw": "10.12.0.1",
  "IPv6Mode": "disabled",
  "IPv6Addr": "",
  "IPv6Mask": "",
  "IPv6Gw": ""
}
```

**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 FMCv 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。「[Virtual Machine Manager を使用した起動 \(6 ページ\)](#)」を参照してください。

## の起動 FMCv

次の方法で、KVM で FMCv を起動できます。

- 導入スクリプトの使用 : virt-install ベースの導入スクリプトを使用して FMCv を起動します。「[導入スクリプトを使用した起動 \(5 ページ\)](#)」を参照してください。
- Virtual Machine Manager の使用 : virt-manager を使用して FMCv を起動します。virt-manager は、KVM 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。「[Virtual Machine Manager を使用した起動 \(6 ページ\)](#)」を参照してください。
- OpenStack の使用 : OpenStack 環境を使用して FMCv を起動します。「[OpenStack を使用した起動 \(8 ページ\)](#)」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なしで FMCv を導入することもできます。これには、アプライアンスの CLI または Web インターフェイスを使用して初期セットアップを完了する必要があります。

## 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 Firepower Management Center Virtual を起動できます。

### 始める前に

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。

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

Firepower Management Center Virtual インスタンスの名前は、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。Firepower Management Center Virtual は、1つのネットワーク インターフェイスをサポートできます。仮想 NIC は Virtio でなければなりません。

例 :

```
virt-install \
  --connect=qemu:///system \
  --network network=default,model=virtio \
  --name=fmcv \
  --arch=x86_64 \
  --cpu host \
  --vcpus=4 \
  --ram=8192 \
  --os-type=linux \
  --os-variant=virtio26 \
  --virt-type=kvm \
  --import \
  --watchdog i6300esb,action=reset \
  --disk path=<fmc_filename>.qcow2,format=qcow2,device=disk,bus=virtio,cache=writethrough \
  --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_fmc.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。

## Virtual Machine Manager を使用した起動

`virt-manager` (Virtual Machine Manager と呼ばれる) を使用して Firepower Management Center 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。

- 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。
- [名前 (Name)] を指定します。
  - 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。
  - [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。
- [参照... (Browse...)] をクリックしてイメージファイルを選択します。
  - [OSタイプ (OS type)] に [Linux] を選択します。
  - [バージョン (Version)] に [virtioを含む汎用2.6.25以降のカーネル (Generic 2.6.25 or later kernel with virtio)] を選択します。
  - [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。
- [メモリ (RAM) (Memory (RAM))] を 8192 に設定します。
  - [CPU (CPUs)] を 4 に設定します。
  - [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、[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 設定を変更します。
- 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 モデルと設定が仮想マシンに適用されます。
- ステップ 8** 8. 仮想ディスクを設定します。
- 左側のパネルから [ディスク1 (Disk 1)] を選択します。
  - [詳細オプション (Advanced Options)] をクリックします。
  - [ディスクバス (Disk bus)] を [Virtio] に設定します。
  - [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、[サーバモード (バインド) (Server mode (bind))] を選択します。
- f) [ホスト (Host)] には IP アドレスと [ポート (Port)] 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グ 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** 仮想ネットワーク インターフェイスを設定します。

- a) [送信元デバイス (Source device)] で、[macvtap] を選択します。
- b) [デバイスモデル (Device model)] で、[virtio] を選択します。
- c) [送信元モード (Source mode)] で、[ブリッジ (Bridge)] を選択します。

(注) デフォルトでは、Firepower Management Center Virtual 仮想インスタンスは、1つのインターフェイスで起動し、その後に設定することができます。

**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。

## OpenStack を使用した起動

Firepower Management Center Virtual は OpenStack 環境に展開できます。OpenStack は、パブリッククラウドとプライベートクラウドの、クラウドコンピューティングプラットフォームを構築および管理するための一連のソフトウェア ツールで、KVM ハイパーバイザと緊密に統合されています。



### OpenStack での第 0 日のコンフィギュレーション ファイルについて

OpenStack では、ブート時にインスタンスに接続される特殊な設定ドライブ (config-drive) を使った設定データの提供をサポートしています。第 0 日のコンフィギュレーションファイルを含む Firepower Management Center Virtual インスタンスを nova boot コマンドを使用して導入するには、次の行を含めます。

```
--config-drive true --file day0-config=/home/user/day0-config \
```

--config-drive コマンドが有効な場合、nova クライアントが呼び出される Linux ファイルシステムにあるファイル=/home/user/day0-config が仮想 CDROM の仮想マシンに渡されます。



- (注) VM はこのファイルを *day0-config* という名前で認識しますが、OpenStack では通常このファイルの内容を /openstack/content/xxxx として保存します。この xxxx は、割り当てられた 4 桁の数字 (/openstack/content/0000 など) です。これは、OpenStack ディストリビューションによって異なる場合があります。

## OpenStack でのコマンドラインを使用した起動

nova boot コマンドを使用して FMCv インスタンスを作成およびブートします。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<p>イメージ、フレーバー、インターフェイス、および第 0 日の設定情報を使用して FMCv インスタンスをブートします。</p> <p>例 :</p> <pre>local@maas:~\$ nova boot \   --image=6883ee2e-62b1-4ad7-b4c6-cd62ee73d1aa \   --flavor=a6541d78-0bb3-4dc3-97c2-7b87f886b1ba \   --nic net-id=5bf6b1a9-c871-41d3-82a3-2ecee26840b1 \   --config-drive true --file day0-config=/home/local/day0-config \</pre>	FMCv には 1 つの管理インターフェイスが必要です。

## OpenStack でのダッシュボードを使用した起動

Horizon は、OpenStack のダッシュボードであり、Nova、Swift、Keystone などの OpenStack サービスへの Web ベース ユーザインターフェイスを提供します。

## 始める前に

- Cisco.com から FMCv qcow2 ファイルをダウンロードし、ローカル MAAS サーバに格納します。

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

- Cisco.com のログインおよびシスコ サービス契約が必要です。

- 
- ステップ 1** [ログイン (Log In)] ページで、ユーザ名とパスワードを入力し、[サインイン (Sign In)] をクリックします。
- ダッシュボードに表示されるタグと機能は、ログインしているユーザのアクセス権限 (権限) によって異なります。
- ステップ 2** メニューから [管理 (Admin)] > [システム パネル (System Panel)] > [フレーバー (Flavor)] を選択します。
- 仮想ハードウェアのテンプレートは OpenStack でフレーバーと呼ばれ、RAM、ディスクのサイズ、コア数を定義します。
- ステップ 3** [フレーバー情報 (Flavor Info)] ウィンドウに必要な情報を入力します。
- [名前 (Name)] : インスタンスを簡単に識別するわかりやすい名前を入力します。たとえば、「FMC-4vCPU-8GB」と入力します。
  - [VCPU の数 (VCPUs)] : [4] を選択します。
  - [RAM MB] : 8192 を選択します。
- ステップ 4** [フレーバーの作成 (Create Flavor)] を選択します。
- ステップ 5** メニューから [管理 (Admin)] > [システム パネル (System Panel)] > [イメージ (Images)] を選択します。
- ステップ 6** [イメージの作成 (Create An Image)] ウィンドウに必要な情報を入力します。
- [名前 (Name)] : イメージを簡単に識別する名前を入力します。たとえば、「FMC-Version-Build」と入力します。
  - [説明 (Description)] : (オプション) イメージファイルの説明を入力します。
  - [参照 (Browse)] : 前に Cisco.com からダウンロードした Firepower Management Center Virtual qcow2 ファイルを選択します。
  - [形式 (Format)] : 形式タイプとして [QCOW2-QEMU Emulator] を選択します。
  - [公開 (Public)] ボックスをオンにします。
- ステップ 7** [イメージの作成 (Create Image)] を選択します。
- 新しく作成されたイメージを表示します。
- ステップ 8** メニューから [プロジェクト (Project)] > [コンピューティング (Compute)] > [インスタンス (Instances)] を選択します。
- ステップ 9** [インスタンスの起動 (Launch Instance)] をクリックします。
- ステップ 10** [インスタンスの起動 (Launch Instance)] > [詳細 (Details)] タブに必要な情報を入力します。

- a) [インスタンス名 (InstanceName)]: インスタンスを簡単に識別する名前を入力します。たとえば、「*FMC-Version-Build*」と入力します。
- b) [フレーバー (Flavor)]: 前の手順 3 で作成したフレーバーを選択します。イメージファイルの説明を入力します。
- c) [Instance Boot Source]: [Boot from image] を選択します。
- d) [イメージ名 (Image Name)]: 前に手順 6 で作成したイメージを選択します。

**ステップ 11** [インスタンスの起動 (Launch Instance)] > [ネットワーキング (Networking)] タブから、Firepower Management Center Virtual インスタンスの管理ネットワークを選択します。

**ステップ 12** [作成 (Launch)] をクリックします。

インスタンスはクラウド内のコンピューティング ノードから開始します。[インスタンス (Instances)] ウィンドウから新しく作成したインスタンスを表示します。

**ステップ 13** Firepower Management Center Virtual のインスタンスを選択します。

**ステップ 14** [コンソール (Console)] タブを選択します。

**ステップ 15** コンソールで仮想アプライアンスにログインします。

## 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導入

どの Firepower Management Center についても、セットアッププロセスを完了する必要があります。このプロセスにより、管理ネットワーク上でアプライアンスが通信できるようになります。第 0 日のコンフィギュレーション ファイルを使用せずに導入する場合、FMCv のセットアップは 2 ステップのプロセスです。

- FMCv を初期化した後に、アプライアンス コンソールでスクリプトを実行します。これにより、管理ネットワーク上で通信するアプライアンスを設定できます。
- 次に、管理ネットワーク上のコンピュータを使用して、FMCv の Web インターフェイスを参照するための設定プロセスを完了します。

## スクリプトを使用したネットワーク設定の構成

次の手順では、FMCv で CLI を使用して初期設定を完了する方法について説明します。

**ステップ 1** コンソールから、FMCv アプライアンスにログインします。ユーザ名として **admin** を、パスワードとして **Admin123** を使用します。

**ステップ 2** admin プロンプトで、次のスクリプトを実行します。

例:

```
sudo /usr/local/sf/bin/configure-network
```

FMCv に初めて接続すると、起動後の設定を求めるメッセージが表示されます。

**ステップ 3** スクリプトのプロンプトに従ってください。

最初に IPv4 管理設定を構成（または無効に）してから、IPv6 に移ります。ネットワーク設定を手動で指定する場合は、IPv4 または IPv6 アドレスを入力する必要があります。

**ステップ 4** 設定値が正しいことを確認します。

**ステップ 5** アプライアンスからログアウトします。

---

#### 次のタスク

- 管理ネットワーク上のコンピュータを使用して、FMCv の Web インターフェイスを参照するための設定プロセスを完了します。

## Web インターフェイスを使用した初期セットアップの実行

次の手順では、FMCv で Web インターフェイスを使用して初期設定を完了する方法について説明します。

**ステップ 1** ブラウザで FMCv の管理インターフェイスのデフォルト IP アドレスにアクセスします。

例：

`https://192.168.45.45`

**ステップ 2** Firepower Management Center Virtual アプライアンスにログインします。ユーザ名として **admin** を、パスワードとして **Admin123** を使用します。設定ページが表示されます。

設定ページが表示されます。管理者のパスワード変更と、ネットワーク設定の指定をまだ行っていない場合はこれらの 2 つを実行し、EULA に同意する必要があります。

**ステップ 3** 完了したら、[適用 (Apply)] をクリックします。FMCv が選択内容に従って設定されます。中間ページが表示されたら、管理者ロールを持つ **admin** ユーザとして Web インターフェイスにログインしています。

FMCv が選択内容に従って設定されます。中間ページが表示されたら、管理者ロールを持つ **admin** ユーザとして Web インターフェイスにログインしています。

---

#### 次のタスク

- FMCv の初期セットアップについて詳しくは、「[Firepower Management Center Virtual 初期セットアップ](#)」を参照してください。
- FMCv の導入に必要な次の手順の概要については、「[Firepower Management Center Virtual の初期管理および設定](#)」の章を参照してください。