Firewall Management Center Virtual の KVM への展開

Firewall Management Center Virtual を KVM に展開できます。

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。

Firewall Management Center Virtual のアップグレード（6.6.0 以降）には 28 GB の RAM が必要

アップグレード時の新しいメモリ診断機能が Firewall Management Center Virtual プラットフォームに導入されました。仮想アプライアンスに割り当てた RAM が 28 GB 未満の場合、Firewall Management Center Virtual のバージョン 6.6.0 以降へのアップグレードは失敗します。

重要 デフォルト設定（ほとんどの Firewall Management Center Virtual インスタンスでは 32 GB RAM、Firewall Management Center Virtual 300（FMCv300）では 64 GB RAM）の値より小さくすることは推奨しません。パフォーマンスを向上させるためには、使用可能なリソースに応じて、仮想アプライアンスのメモリや CPU 数をいつでも増やすことができます。

サポート対象のプラットフォームにおいて、このメモリ診断の結果より低いメモリのインスタンスをサポートできません。

メモリとリソースの要件

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。ハイパーバイザ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。

重要 Firewall Management Center Virtual をアップグレードする際、最新のリリースノートで詳細を参照し、新しいリリースが環境に影響を及ぼさないことを確認してください。最新バージョンを展開するには、リソースの拡張が必要な場合があります。

アップグレードすることで、展開環境のセキュリティ機能とパフォーマンスの向上に役立つ最新の機能と修正プログラムが追加されます。

Firewall Management Center 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。作成する各仮想アプライアンスには、ホストマシン上での最小リソース割り当て（メモリ、CPU 数、およびディスク容量）が必要です。

KVM の Firewall Management Center Virtual アプライアンスの推奨設定およびデフォルト設定を次の表に示します。

- プロセッサ
  - 4 個の vCPU が必要
- メモリ
  - 最小要件 28/推奨（デフォルト）32 GB RAM

重要 アップグレード時の新しいメモリ診断機能が Firewall Management Center Virtual プラットフォームに導入されました。仮想アプライアンスに割り当てた RAM が 28 GB 未満の場合、Firewall Management Center Virtual のバージョン 6.6.0 以降へのアップグレードは失敗します。

- 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
  - IPv6
- 仮想マシンあたりのホスト ストレージ
  - Firewall Management Center Virtual 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 サーバーをサポート

バージョン 7.3 以降、KVM で Management Center Virtual 300（FMCv300）がサポートされます。KVM の FMCv300 アプライアンスの推奨設定およびデフォルト設定を次に示します。

- プロセッサ
  - 32 個の vCPU が必要
- メモリ
  - 推奨（デフォルト）64 GB RAM
- 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
  - FMCv300 には 2 TB 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 サーバーをサポート

前提条件

- Cisco.com から Firewall 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。

注意事項と制約事項

- Firewall Management Center Virtual 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。
- ネストされたハイパーバイザ（VMware/ESXi 上で動作する KVM）はサポートされていません。ベアメタル KVM の展開のみがサポートされます。
- 仮想マシンの複製はサポートされません。

高可用性のサポート

- KVM 用 Management Center Virtual 300（FMCv300）：新しい拡張された Firewall Management Center Virtual イメージは、最大 300 台のデバイスを管理でき、ディスク容量が大きい KVM で使用できます。
- Firewall Management Center Virtual ハイアベイラビリティ（HA）がサポートされています。

- 高可用性構成の 2 つの Firewall Management Center Virtual アプライアンスは、同じモデルである必要があります。
- Firewall Management Center Virtual HA を確立するには、Firewall Management Center Virtual では、HA 構成で管理する Cisco Secure Firewall Threat Defense（旧 Firepower Threat Defense）デバイスごとに追加の Management Center Virtual ライセンス権限が必要です。ただし、Threat Defense デバイスごとに必要な Firewall Threat Defense 機能のライセンス権限は、Firewall Management Center Virtual HA 構成に関係なく変更されません。ライセンスに関するガイドラインについては、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド [英語] の「License Requirements for threat defense devices in a High Availability Pair」を参照してください。
- Firewall Management Center Virtual HA ペアを解除すると、追加の Firewall Management Center Virtual ライセンス権限が解放され、Firewall Threat Defense デバイスごとに 1 つの権限のみが必要になります。高可用性に関する詳細とガイドラインについては、『Secure Firewall Management Center Device Configuration Guide』[英語] の「*High Availability*」を参照してください。

第 0 日のコンフィギュレーション ファイルの準備

Firewall Management Center 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。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。

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 Firewall Management Center 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。

- 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展開する場合、起動後にシステムの必須設定を設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 サーバーを使用するには、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）。

手順

ステップ 1 「day0-config」というテキスト ファイルに Firewall Management Center Virtual 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": "r2M$9^Uk69##",
    "DNS1": "10.1.1.5",
    "DNS2": "192.168.1.67",

    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.45",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "enabled",
    "IPv6Addr": "2001:db8::a111:b221:1:abca/96",
    "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 Firewall Management Center Virtual 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。「Firewall Management Center Virtual の導入 （9 ページ）」を参照してください。

Firewall Management Center Virtual の導入

次の方法で、KVM で Firewall Management Center Virtual 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 Firewall Management Center Virtual を起動します。「導入スクリプトを使用した起動 （7 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 Firewall Management Center Virtual 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。「Firewall Management Center Virtual の導入 （9 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 Firewall Management Center Virtual 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 Firewall 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。

手順

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。

Firewall 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）全体で一意である必要があります。Firewall 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=28672 \
    --os-type=generic \
    --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
```

（注）
展開スクリプトで、展開プロセスの --os-type パラメータの値を **generic** に設定し、仮想インスタンスが展開されるプラットフォームが正しく識別されるようにします。

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。

Firewall Management Center Virtual の導入

virt-manager（Virtual Machine Manager とも呼ばれる）を使用して Firewall 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。

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（Use 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。

a) [メモリ（RAM）（Memory (RAM)）] を *28672* に設定します。
b) [CPU（CPUs）] を *4* に設定します。
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 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。

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 仮想ネットワーク インターフェイスを設定します。

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）
デフォルトでは、Firewall Management Center Virtual インスタンスは、1 つのインターフェイスで起動し、その後設定できます。

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。

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 についても、設定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、Firewall Management Center Virtual のセットアップは 2 ステップのプロセスです。

- Firewall Management Center Virtual 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、Firewall Management Center Virtual 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、Firewall Management Center Virtual で CLI を使用して初期セットアップを完了する方法について説明します。

手順

ステップ 1 コンソールから、Firewall Management Center Virtual アプライアンスにログインします。ユーザー名として **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
```

Firewall Management Center Virtual 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。

IPv4 管理設定を設定（または無効化）します次に、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、Firewall Management Center Virtual 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、Firewall Management Center Virtual で 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方法について説明します。

手順

ステップ 1 ブラウザで Firewall Management Center Virtual 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 Firewall Management Center Virtual アプライアンスにログインします。ユーザー名として **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。Firewall Management Center Virtual 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 ユーザーとして Web インターフェイスにログインしています。

Firewall Management Center Virtual 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 ユーザーとして Web インターフェイスにログインしています。

次のタスク

- Firewall Management Center Virtual の初期セットアップについて詳しくは、「Firewall Management Center Virtual 初期設定」を参照してください。
- Firewall Management Center Virtual の導入で必要な次の手順の概要については、「Firewall Management Center Virtual 初期管理および設定」の章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。