VMware への Firewall Management Center Virtual の展開

VMware を使用して Firewall Management Center Virtual を導入できます。

Firewall Management Center Virtual の VMware 機能のサポート

次の表に、Firewall Management Center Virtual の VMware 機能のサポートを示します。

表 *1 : Firewall Management Center Virtual* の *VMware* 機能のサポート

機能	説明	サポート（あり/なし）	コメント
コールド クローン	クローニング中に VM の電源がオフになります。	なし	–
ホット追加	追加時に VM が動作しています。	なし	–
ホット クローン	クローニング中に VM が動作しています。	なし	–
ホット リムーブ	取り外し中に VM が動作しています。	なし	–

機能	説明	サポート（あり/なし）	コメント
スナップショット	VMが数秒間フリーズします。	なし	FMC と管理対象デバイス間で同期されていない状況のリスクがあります。スナップショットのサポート（8 ページ）を参照してください。
一時停止と再開	VM が一時停止され、その後再開します。	あり	–
vCloud Director	VM の自動配置が可能になります。	なし	–
VM の移行	移行中に VM の電源がオフになります。	あり	–
VMotion	VM のライブ マイグレーションに使用されます。	あり	共有ストレージを使用します。vMotion のサポート （8 ページ）を参照してください。
VMware FT	VM の HA に使用されます。	なし	–
VMware HA	ESXiおよびサーバーの障害に使用されます。	あり	–
VM ハートビートの VMware HA	VM 障害に使用されます。	なし	–
VMware vSphere スタンドアロン Windows クライアント	VM を導入するために使用されます。	あり	–
VMware vSphere Web Client	VM を導入するために使用されます。	あり	–

システム要件

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

VMware ESX および ESXi ハイパーバイザでホストされる VMware vSphere プロビジョニングを使用して Firewall Management Center Virtual を導入できます。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ば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。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。

リソースの割り当てに合わせてCPUとメモリのリソースを予約することを強くお勧めします。これを行わない場合は Firewall Management Center Virtual のパフォーマンスと安定性に大きく影響することがあります。

次の表に、Firewall Management Center Virtual アプライアンスの推奨設定とデフォルト設定を示します。

重要 Firewall Management Center Virtual の最適なパフォーマンスを確保するには、十分なメモリを割り当ててください。Firewall Management Center Virtual のメモリが 32 GB 未満の場合は、システムでポリシーの展開に問題が発生する可能性があります。使用可能なリソースによっては、パフォーマンスを向上させるために仮想アプライアンスのメモリと CPU の数を増やすことができます。デフォルトの設定は、システム ソフトウェアの実行の最小要件であるため、減らさないでください。

表 *2 : Firewall Management Center Virtual* アプライアンスの設定

設定	最小	デフォルト	推奨	設定調整の可否
メモリ	28 GB	32 GB	32 GB	制限あり **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。
仮想 CPU	4	4	16	あり。最大 16
ハード ディスク プロビジョニング サイズ	250 GB	250 GB	適用対象外	×

表 *3 : Firewall Management Center Virtual 300*（*FMCv300*）仮想アプライアンスの設定

設定	デフォルト	設定調整の可否
メモリ	64 GB	あり
仮想 CPU	32	なし
ハードディスク プロビジョニング サイズ	2.2 TB	非対応

（注） Firewall Management Center Virtual 10.0 では、VMware vSphere/ESXi 8.0 プラットフォームでのデプロイメントがサポートされています。

RAM の割り当て量が不十分な場合、メモリ不足（OOM）イベントが原因でプロセスが再起動します。データベースプロセスを再起動すると、データベースが破損することもあります。そのような場合は、RAM を必要な割り当て量にアップグレードし、データベースを頻繁にバックアップして、データベースの破損による中断を回避してください。

VMware vCenter Server と ESXi のインスタンスを実行するシステムは、特定のハードウェアおよびオペレーティングシステム要件を満たす必要があります。サポートされるプラットフォームのリストについては、オンラインの『VMware Compatibility Guide』を参照してください。

仮想化テクノロジーのサポート

ESXi ホストとして動作するコンピュータは、次の要件を満たす必要があります。

- 仮想化サポートとして、Intel® Virtualization Technology（VT）または AMD Virtualization™（AMD-V™)テクノロジのいずれかを実現する 64 ビット CPU が必要
- 仮想化は、BIOS 設定で有効化する必要がある

（注） Intel と AMD はどちらも、CPU を識別して機能を確認するために役立つオンラインプロセッサ識別ユーティリティを提供しています。VT をサポートする CPU を搭載する多くのサーバーでは、VT がデフォルトで無効になっている可能性があります。その場合は、VT を手動で有効にする必要があります。システムで VT のサポートを有効にする手順については、製造元のマニュアルを参照してください。

- CPU が VT をサポートしているにもかかわらず BIOS にこのオプションが表示されない場合は、ベンダーに連絡して、VT のサポートを有効にすることができるバージョンの BIOS を要求してください。
- 仮想デバイスをホストするために、コンピュータには Intel e1000 ドライバと互換性があるネットワーク インターフェイスが必要です（PRO 1000MT デュアル ポート サーバー アダプタまたは PRO 1000GT デスクトップ アダプタなど）。

CPU のサポートの確認

Linux コマンドラインを使用して、CPU ハードウェアに関する情報を取得できます。たとえば、**/proc/cpuinfo** ファイルには個々の CPU コアに関する詳細情報が含まれています。**less** または **cat** により、その内容を出力できます。

フラグ セクションで次の値を確認できます。

- vmx：インテル VT 拡張機能
- svm：AMD-V拡張機能

grep を使用すると、次のコマンドを実行して、ファイルにこれらの値が存在するかどうかを素早く確認することができます。

```
egrep "vmx|svm" /proc/cpuinfo
```

システムが VT をサポートしている場合は、フラグのリストに *vmx* または *svm* が表示されます。

注意事項と制約事項

OVF ファイルのガイドライン

仮想アプライアンスは Open Virtual Format（OVF）パッケージを使用します。仮想アプライアンスは、仮想インフラストラクチャ（VI）または ESXi OVF テンプレートを使用して展開します。導入対象に基づいて、OVF ファイルを選択します。

- vCenter へのデプロイメント用：
  Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-**VI**-*X.X.X-xxx*.ovf
- ESXi（vCenter なし）へのデプロイメント用：
  Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-**ESXi**-*X.X.X-xxx*.ovf

ここで、X.X.X-xxx は、展開するシステムソフトウェアのバージョンとビルド番号を表します。
参照先

- VI OVF テンプレートを使用して展開する場合、インストールプロセスで、Firewall Management Center Virtual 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。
  - 管理者アカウントの新しいパスワード。
  - 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。

（注） VMware vCenter を使用してこの仮想アプライアンスを管理する必要があります。

- ESXi OVF テンプレートを使用して導入する場合、インストール後にシステムの必須設定を行う必要があります。この仮想アプライアンスは VMware vCenter を使用して管理するか、スタンドアロン アプライアンス として使用できます。

OVF テンプレートを展開する際に、以下の情報を指定します。

表 *4 : VMware OFV* テンプレートの設定

設定	ESXi または VI	操作
OVF テンプレートのインポート/展開	両方	Cisco.com からダウンロードした OVF テンプレートを参照します。
OVF テンプレートの詳細	両方	設置するアプライアンス（Firewall Management Center Virtual）および展開オプション（VI または ESXi）を確認します。
使用許諾契約の同意	VI のみ	OVF テンプレートに含まれるライセンス条項を受け入れることに同意します。
名前と場所	両方	仮想アプライアンスの一意のわかりやすい名前を入力し、アプライアンスのインベントリの場所を選択します。
ホスト/クラスタ	両方	仮想アプライアンスを展開するホストまたはクラスタを選択します。
リソース プール	両方	ホストやクラスタ内のコンピューティング リソースを、わかりやすい階層を設定して管理します。仮想マシンと子リソース プールは親リソース プールのリソースを共有します。
ストレージ	両方	仮想マシンに関連付けられるすべてのファイルを格納するデータストアを選択します。
ディスクの書式設定	両方	仮想ディスクを保存する形式を、シックプロビジョニング（Lazy Zeroed）またはシックプロビジョニング（Eager Zeroed）のどちらにするか選択します。 （注） 最適なパフォーマンスを確保するために、シックプロビジョニングされたディスク形式を使用することを推奨します。
ネットワーク マッピング	両方	仮想アプライアンスの管理インターフェイスを選択します。
プロパティ	VI のみ	仮想マシンの初期設定をカスタマイズします。

時刻および時刻同期

Firewall Management Center Virtual と管理対象デバイスのシステム時刻を同期させるには、Network Time Protocol（NTP）サーバーを使用します。通常、Firewall Management Center Virtual

の初期設定時にNTPサーバーを指定します。デフォルトのNTPサーバーについては、「Firewall Management Center Virtual 初期設定」を参照してください。

システムを正常に動作させるには、Firewall Management Center Virtual とその管理対象デバイスのシステム時刻を同期させる必要があります。Firewall Management Center Virtual の NTP 設定と一致するように VMware ESXi サーバーで NTP を設定する場合は、追加の手順を実行して時刻を同期します。

vSphere Client を使用して、ESXi ホストで NTP を設定できます。具体的な手順については、VMware のマニュアルを参照してください。さらに、VMware KB 2012069 では、vSphere Client を使用して ESX/ESXi ホストで NTP を設定する方法について説明されています。

vMotion のサポート

vMotion を使用する場合、共有ストレージのみを使用することをお勧めします。導入時に、ホストクラスタがある場合は、ストレージをローカルに（特定のホスト上）または共有ホスト上でプロビジョニングできます。ただし、Firewall Management Center Virtual を vMotion を使用して別のホストに移行する場合、ローカル ストレージを使用するとエラーが発生します。

スナップショットのサポート

VMware スナップショットは、特定の時点での仮想マシンのディスクファイル（VMDK）のコピーです。スナップショットは、仮想ディスクの変更ログを提供し、障害またはシステムエラーが発生した特定の時点にVMを復元するために使用できます。スナップショットだけではバックアップが提供されないため、バックアップとして使用しないでください。

設定のバックアップが必要な場合は、 の Backup and Restore 機能を使用します（**[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]**）。

ESXi の VMware スナップショット機能は、VM ストレージ容量を使い果たし、FMC 仮想アプライアンスのパフォーマンスに影響を与える可能性があります。次のVMwareナレッジベースの記事を参照してください。

- vSphere 環境でのスナップショットの使用に関するベストプラクティス（VMware KB 1025279）。
- ESXi での VM スナップショットの理解（VMware KB 1015180）。

高可用性（HA）のサポート

VMware ESXi 上の 2 つの Firewall Management Center Virtual アプライアンス間で高可用性（HA）を確立できます。

- 高可用性構成の 2 つの Firewall Management Center Virtual 仮想アプライアンスは、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 Firewall Management Center Virtual ライセンス権限が必要です。ただし、Firewall 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 Device Configuration Guide』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。

高可用性に関するガイドラインについては、『Cisco Secure Firewall Management Center Administration Guide』の「*Establishing Management Center High Availability*」を参照してください。

INIT Respawning エラーメッセージの症状

ESXi 6 および ESXi 6.5 で実行されている Firewall Management Center Virtual コンソールに次のエラーメッセージが表示される場合があります。

```
"INIT: Id "fmcv" respawning too fast: disabled for 5 minutes"
```

回避策：デバイスの電源がオフになっているときに、vSphere で仮想マシンの設定を編集してシリアルポートを追加します。

1. 仮想マシンを右クリックして、[設定の編集（Edit Settings）] をクリックします。
2. [仮想ハードウェア（Virtual Hardware）] タブで、[新規デバイス（New devide）] ドロップダウンメニューから [シリアルポート（Serial port）] を選択し、[追加（Add）] をクリックします。

   シリアルポートがバーチャルデバイスリストの一番下に表示されます。
3. [仮想ハードウェア（Virtual Hardware）] タブで、[シリアルポート（Serial Port）] を展開し、接続タイプとして [物理シリアルポートを使用（Use physical serial port）] を選択します。
4. [パワーオン時に接続（Connect at power on）] チェックボックスをオフにします。

   [OK] をクリックして設定を保存します。

制限事項

VMware 向けに展開する際には次の制約があります。

- 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。
- 仮想マシンの複製はサポートされません。
- スナップショットによる仮想マシンの復元はサポートされません。

- VMware Workstation、Player、Server、および Fusion は OVF パッケージを認識しないため、サポートされません。

VMXNET3 インターフェイスの設定

重要

- 6.4 リリース以降、e1000 インターフェイスを使用している場合は、VMXNET3 インターフェイスに切り替えることを**強く推奨します**。VMXNET3 のデバイスドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。
- 7.4 以前のリリースでは、FMCv300 は e1000 インターフェイスのみをサポートします。

  7.6 リリース以降、FMCv300 は e1000 インターフェイスと VMXNET3 インターフェイスの両方をサポートします。デフォルトでは、VMware 上の Management Center Virtual は、VM を展開すると e1000 インターフェイスになります。VMXNET3 インターフェイスに切り替えることを強く推奨します。
- 10.0.0 リリース以降、VM を展開すると、VMware 上の Threat Defense Virtual および Management Center Virtual はデフォルトで VMXNET3 インターフェイスになります。

e1000 インターフェイスを vmxnet3 に変更するには、「すべての」インターフェイスを削除し、vmxnet3 ドライバを使用してそれらを再インストールする必要があります。

展開内でインターフェイスを混在させることはできますが（で e1000 インターフェイス、およびその管理対象仮想デバイスで vmxnet3 インターフェイスなど）、同じ仮想アプライアンス上でインターフェイスを混在させることはできません。仮想アプライアンス上のすべてのセンサーインターフェイスと管理インターフェイスは同じタイプである必要があります。

手順

ステップ 1 Firewall Threat Defense Virtual または Firewall Management Center Virtual マシンの電源をオフにします。

インターフェイスを変更するには、アプライアンスの電源をオフにする必要があります。

ステップ 2 インベントリ内の Firewall Threat Defense Virtual または Firewall Management Center Virtual マシンを右クリックして、[設定の編集（Edit Settings）] をクリックします。

ステップ 3 該当するネットワークアダプタを選択し、[削除（Remove）] を選択します。

ステップ 4 [追加（Add）] をクリックして、[ハードウェアの追加ウィザード（Add Hardware Wizard）] を開きます。

ステップ 5 [イーサネットアダプタ（Ethernet Adapter）] を選択し、[次へ（Next）] をクリックします。

ステップ 6 vmxnet3 アダプタを選択し、ネットワークラベルを選択します。

ステップ 7 Firewall Threat Defense Virtual のすべてのインターフェイスについて手順を繰り返します。

次のタスク

- VMware コンソールから Firewall Threat Defense Virtual または Firewall Management Center Virtual の電源をオンにします。

インストール パッケージのダウンロード

シスコは VMware ESX および ESXi ホスト環境用にパッケージ化した仮想アプライアンスを、圧縮アーカイブ（.tar.gz）ファイルとしてサポート サイトで提供します。シスコの仮想アプライアンスは、仮想ハードウェアのバージョン 7 の仮想マシンとしてパッケージ化されています。各アーカイブには、ESXi または VI 導入ターゲット用の OVF テンプレートとマニフェスト ファイル、および仮想マシンディスク フォーマット（vmdk）ファイルが含まれています。

Cisco.com から Firewall Management Center Virtual インストールパッケージをダウンロードして、ローカルディスクに保存します。シスコでは、常に最新のパッケージを使用することを推奨します。仮想アプライアンスのパッケージは、通常、システム ソフトウェアのメジャーバージョンに関連付けられています（たとえば 6.1 または 6.2 など）。

始める前に

ディレクトリから VMDK ファイルを抽出した後、SHA1 チェックサムを検証します。

手順

ステップ 1 シスコのソフトウェア ダウンロード ページに移動します。

（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。

ステップ 2 [すべて参照（Browse all）] をクリックして Firewall Management Center Virtual 導入パッケージを検索します。

ステップ 3 **[セキュリティ（Security）] > [ファイアウォール（Firewalls）] > [ファイアウォールの管理（Firewall Management）]** を選択し、**[Secure Firewall Management Center Virtual]** を選択します。

ステップ 4 次の命名規則を使用して、ダウンロードする Firewall Management Center Virtual アプライアンスの VMware インストールパッケージを検索します。

Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-X.X.X-xxx.tar.gz

ここで、*X.X.X-xxx* は、ダウンロードするインストール パッケージのバージョンとビルド番号を表します。

ステップ 5 ダウンロードするインストール パッケージをクリックします。

（注）
サポート サイトにログインしている間、シスコは、仮想アプライアンスの使用可能なすべての更新をダウンロードすることを推奨します。こうすることで、仮想アプライアンスをメジャー バージョンにインストールした後で、システム ソフトウェアを更新できるようになります。アプライアンスによってサポート

されるシステム ソフトウェアの最新バージョンを常に実行する必要があります。Firewall Management Center Virtual の場合、新しい侵入ルールと脆弱性データベース（VDB）の更新もダウンロードする必要があります。

ステップ 6 vSphere クライアントを実行中のワークステーションまたはサーバーからアクセス可能な場所に、インストール パッケージをコピーします。

注意
アーカイブ ファイルを電子メールで転送しないでください。ファイルが破損することがあります。

ステップ 7 任意のツールを使用してインストール パッケージの圧縮を解除し、インストール ファイルを抽出します。Firewall Management Center Virtualの場合：

- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-X.X.X-xxx-disk1.vmdk
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-X.X.X-xxx.ovf
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-X.X.X-xxx.mf
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-X.X.X-xxx.ovf
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-X.X.X-xxx.mf

ここで、*X.X.X-xxx* は、ダウンロードしたアーカイブ ファイルのバージョンとビルド番号を表します。

（注）
必ずすべてのファイルを同じディレクトリ内に保持してください。

次のタスク

- 導入ターゲット（VI または ESXi）を決定し、「Firewall Management Center Virtual の導入（12 ページ）」に進みます。

Firewall Management Center Virtual の導入

VMware vSphere vCenter、vSphere クライアント、vSphere Web クライアント、または ESXi ハイパーバイザ（スタンドアロン ESXi 導入用）を使用して Firewall Management Center Virtual を導入できます。VI または ESXi OVF テンプレートによる導入が可能です。

- VI OVF テンプレートを使用して導入する場合、アプライアンスは VMware vCenter によって管理する必要があります。
- ESXi OVF テンプレートを使用して導入する場合、アプライアンスは VMware vCenter によって管理するか、またはスタンドアロン ESXi ホストに導入できます。いずれの場合も、インストール後にシステムの必須設定を設定する必要があります。

ウィザードの各ページで設定を指定してから、[次へ（Next）] をクリックして続行します。ユーザーの利便性のために、ウィザードの最終ページでは、手順を完了する前に、設定を確認することができます。

手順

ステップ 1 [vSphere クライアント（vSphere Client）] で、**[ファイル（File）]** > **[OVF テンプレートの展開（Deploy OVF Template）]** を選択します。

ステップ 2 ドロップダウンリストから、Firewall Management Center Virtual の展開に使用する OVF テンプレートを選択します。

- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-*X.X.X-xxx*.ovf
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-*X.X.X-xxx*.ovf
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-X.X.X-xxx-disk1.vmdk

ここで、*X.X.X-xxx* は、Cisco.com からダウンロードしたインストール パッケージのバージョンとビルド番号を表します。

ステップ 3 [OVF テンプレートの詳細（OVF Template Details）] ページが表示されるので [次へ（Next）] をクリックします。

ステップ 4 ライセンス契約書が OVF テンプレート（VI テンプレートのみ）に含まれている場合は、[エンドユーザーライセンス契約（End User License Agreement）] のページが表示されます。ライセンス条項に同意し、[次へ（Next）] をクリックすることに同意します。

ステップ 5 （任意）名前を編集し、Firewall Management Center Virtual を配置するインベントリ内のフォルダの場所を選択して、[次へ（Next）] をクリックします。

（注）
vSphere クライアントが ESXi ホストに直接接続されている場合、フォルダの場所を選択するオプションは表示されません。

ステップ 6 Firewall Management Center Virtual を展開するホストまたはクラスタを選択して、[次へ（Next）] をクリックします。

ステップ 7 Firewall Management Center Virtual を実行するリソース プールに移動して選択し、[次へ（Next）] をクリックします。

このページは、クラスタにリソースプールが含まれている場合にのみ表示されます。

ステップ 8 仮想マシン ファイルを保存する場所を選択し、[次へ（Next）] をクリックします。

このページで、宛先クラスタまたはホストですでに設定されているデータストアから選択します。仮想マシン コンフィギュレーション ファイルおよび仮想ディスク ファイルが、このデータストアに保存されます。仮想マシンとそのすべての仮想ディスクファイルを保存できる十分なサイズのデータストアを選択してください。

ステップ 9 仮想マシンの仮想ディスクを保存するためのディスク形式を選択し、[次へ（Next）] をクリックします。

[シックプロビジョン（Thick Provisioned）] を選択すると、すべてのストレージは、ただちに割り当てられます。

（注）
最適なパフォーマンスを確保するために、シックプロビジョニングされたディスク形式を使用することを推奨します。

ステップ 10 [ネットワークマッピング（Network Mapping）] 画面で、Firewall Management Center Virtual 管理インターフェイスを VMware ネットワークと関連付けます。

インフラストラクチャの [宛先ネットワーク（Destination Networks）] 列を右クリックしてネットワークを選択し、ネットワーク マッピングをセットアップして、[次へ（Next）] をクリックします。

ステップ 11 ユーザー設定可能なプロパティが OVF テンプレート（VI テンプレートのみ）に含まれている場合は、設定可能なプロパティを設定し、[次へ（Next）] をクリックします。

ステップ 12 [終了準備の完了（Ready to Complete）] ウィンドウで設定を見直し、確認します。

ステップ 13 （任意）[導入後に電源をオン（Power on after deployment）] オプションにチェックマークを付けて、Firewall Management Center Virtual の電源をオンにし、[終了（Finish）] をクリックします。

注：展開後に電源を入れないことを選択した場合は、後で VMware コンソールから電源を入れることができます（「仮想アプライアンスの初期化」を参照）。

ステップ 14 インストールが完了したら、ステータス ウィンドウを閉じます。

ステップ 15 ウィザードが完了すると、vSphere Web Client は VM を処理します。[グローバル情報（Global Information）] 領域の [最近のタスク（Recent Tasks）] ペインで [OVF展開の初期設定（Initialize OVF deployment）] ステータスを確認できます。

この手順が終了すると、[OVFテンプレートの導入（Deploy OVF Template）] 完了ステータスが表示されます。

その後、Firewall Management Center Virtual インスタンスがインベントリ内の指定されたデータセンターの下に表示されます。新しい VM の起動には、最大 30 分かかることがあります。

使用している OVF テンプレートに応じて、Firewall Management Center Virtual を導入後、VMware vSphere vCenter、vSphere クライアント、vSphere Web クライアント、または ESXi ハイパーバイザ（スタンドアロン ESXi 導入用）に ISO イメージ **_ovfenv-<hostname>.iso** がマウントされます。この ISO イメージには、IP アドレスのネットマスク、ホスト名、HA ロールなどの OVF 環境変数があります。これらの環境変数は vSphere によって生成され、起動プロセス中に使用されます。

Firewall Management Center Virtual VM の起動後にイメージをマウント解除することもできます。ただし、VMware vSphere **Network Adapter Configuration** で [パワーオン時に接続（Connect at power on）] がオフになっている場合でも、Firewall Management Center Virtual の電源がオン/オフされるたびにイメージがマウントされます。

（注）

Cisco Licensing Authority に Firewall Management Center Virtual を正常に登録するには、 にインターネットアクセスが必要です。インターネットに接続してライセンス登録を完了させるには、導入後に追加の設定が必要になることがあります。

次のタスク

- 仮想アプライアンスのハードウェアおよびメモリの設定が導入の要件を満たしていることを確認します（「仮想マシンのプロパティの確認 （15 ページ）」を参照）。

仮想マシンのプロパティの確認

[VMware 仮想マシンプロパティ（ VMware Virtual Machine Properties）] ダイアログボックスを使用して、選択した仮想マシンのホスト リソースの割り当てを調整できます。このタブで、CPU、メモリ、ディスク、および拡張 CPU リソースを変更できます。また、仮想マシンの仮想イーサネット アダプタ設定の電源接続設定、MAC アドレス、およびネットワーク接続を変更できます。

手順

ステップ 1 新しい仮想アプライアンスの名前を右クリックし、コンテキストメニューから [設定の編集（Edit Settings）] を選択するか、メイン ウィンドウの [作業の開始（Getting Started）] タブから [仮想マシン設定の編集（Edit virtual machine settings）] をクリックします。

ステップ 2 「デフォルトの仮想アプライアンスの設定」（4 ページ）に示すように、[メモリ（Memory）] 、[CPU（CPUs）] 、および [ハードディスク 1（Hard disk 1）] の設定がデフォルト値以上になっていることを確認します。

アプライアンスのメモリ設定および仮想 CPU の数は、ウィンドウの左側に表示されます。ハードディスクの [プロビジョニングサイズ（Provisioned Size）] を表示するには、[ハードディスク 1（Hard disk 1）] をクリックします。

ステップ 3 オプションで、ウィンドウの左側の適切な設定をクリックしてメモリと仮想CPUの数を増やし、ウィンドウの右側で変更します。

ステップ 4 [ネットワークアダプタ 1（Network adapter 1）] 設定が次のようになっていることを確認し、必要に応じて変更します。

a) [デバイスのステータス（Device Status）] の下で、[パワーオン時に接続（Connect at power on）] チェックボックスを有効にします。

b) [MACアドレス（MAC Address）] の下で、仮想アプライアンスの管理インターフェイスの MAC アドレスを手動で設定します。

仮想アプライアンスに手動で MAC アドレスを割り当て、ダイナミック プール内の他のシステムによる MAC アドレスの変更または競合を回避します。

また、Firewall Management Center Virtual の場合、MAC アドレスを手動で設定することにより、アプライアンスの再イメージ化が必要になった場合、シスコからのライセンスを再要求する必要がありません。

c) [ネットワーク接続（Network Connection）] の下で、[ネットワークラベル（Network label）] に仮想アプライアンスの管理ネットワーク名を設定します。

ステップ 5 [OK] をクリックします。

次のタスク

- 仮想アプライアンスの初期設定の方法については、「仮想アプライアンスの電源投入と初期設定 （16 ページ）」を参照してください。
- 必要に応じて、アプライアンスの電源を入れる前に、追加の管理インターフェイスを作成できます。詳細については、『*Cisco Secure Firewall Management Center Virtual* スタートアップガイド』の「*Deploy the Management Center Virtual Using VMware*」の章と、』を参照してください。

仮想アプライアンスの電源投入と初期設定

仮想アプライアンスを導入を完了した後、仮想アプライアンスに初めて電源を入れると初期化が自動的に開始されます。

注意 起動時間は、サーバーリソースの可用性など、さまざまな要因によって異なります。初期化が完了するまでに最大で 40 分かかることがあります。初期化は中断しないでください。中断すると、アプライアンスを削除して、最初からやり直さなければならないことがあります。

手順

ステップ 1 アプライアンスの電源をオンにします。

vSphere クライアントで、インベントリ リストの仮想アプライアンスの名前を右クリックし、コンテキスト メニューで **[電源（Power）] > [電源オン（Power On）]** を選択します。

ステップ 2 VMware コンソール タブで初期化を監視します。

次のタスク

Firewall Management Center Virtual を展開したら、セットアッププロセスを完了して、信頼できる管理ネットワーク上で通信するように新しいアプライアンスを設定する必要があります。

VMware で ESXi OVF テンプレートを使用して展開する場合、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 の初期セットアップを完了するには、「Firewall Management Center Virtual 初期設定」を参照してください。
- Firewall Management Center Virtual の展開に必要な次のステップの概要については、x` 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。