



Cisco HyperFlex への Firewall Management Center Virtual の展開

Cisco HyperFlex システムは、あらゆる場所であらゆるアプリケーションにハイパーコンバージェンスを提供します。Cisco Unified Computing System (Cisco UCS) テクノロジーを備える HyperFlex は、Cisco Intersight クラウド運用プラットフォームを通じて管理され、場所を問わずアプリケーションとデータを強力にサポートし、コアデータセンターからエッジ、そしてパブリッククラウドまでの運用を最適化し、DevOps 手法を推進して俊敏性を高めることができます。

Cisco HyperFlex に Firewall Management Center Virtual を展開できます。

- [システム要件 \(1 ページ\)](#)
- [注意事項と制約事項 \(3 ページ\)](#)
- [Firewall Management Center Virtual の導入 \(4 ページ\)](#)
- [仮想アプライアンスの電源投入と初期設定 \(6 ページ\)](#)

システム要件

Firewall Management Center Virtual 28 GB の RAM が必要

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 の値を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。

メモリとリソースの要件

- HyperFlex ESX および ESXi ハイパーバイザでホストされる HyperFlex クラスタのプロビジョニングを使用して Firewall Management Center Virtual を展開できます。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。

- Firewall Management Center Virtual の場合、最新のリリースノートを参照し、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。
- 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。
- 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。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 1: Firewall Management Center Virtual 仮想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
仮想 CPU	4	4	8	あり。最大 8
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	なし。ディスク形式の選択に基づく

表 2: Firewall Management Center Virtual300 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	なし。ディスク形式の選択に基づく

サポートされているプラットフォームのリスト、および特定のハードウェアとオペレーティングシステムの要件については、『[Compatibility Guide](#)』を参照してください。

注意事項と制約事項

制限事項

Cisco HyperFlex 用に Firewall Management Center Virtual を展開する場合、次の制限があります。

- 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。

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) OVF テンプレートを使用して展開します。展開対象に基づいて、OVF ファイルを選択します。

vCenter でのデプロイメント用: Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-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。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セットアップ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。

高可用性のサポート

HyperFlex ホストに展開された 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 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 Firewall 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 デバイス設定ガイド](#)』の「License Requirements for FTD 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。

ハイアベイラビリティのガイドラインについては、『[Cisco Secure Firewall Management Center アドミニストレーションガイド](#)』の「High Availability」を参照してください。

関連資料

[『Release Notes for Cisco HX Data Platform』](#)

[Configuration Guides for Cisco HX Data Platform](#)

[Cisco HyperFlex 4.0 for Virtual Server Infrastructure with VMware ESXi](#)

[Cisco HyperFlex Systems Solutions Overview](#)

[Cisco HyperFlex Systems ドキュメンテーション ロードマップ](#)

Firewall Management Center Virtual の導入

以下の手順を使用して、vSphere vCenter Server 上の Cisco HyperFlex に Firewall Management Center Virtual アプライアンスを展開します。

始める前に

- Cisco HyperFlex を展開してインストール後の構成タスクをすべて実行済みであることを確認します。詳細については、『[Cisco HyperFlex Systems Documentation Roadmap](#)』を参照してください。
- Firewall Management Center Virtual を導入する前に、vSphere（管理用）で少なくとも 1 つのネットワークを設定しておく必要があります。
- [Cisco.com](#) から Firewall Management Center Virtual VI OVF テンプレートファイル、*Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-X.X.X-xxx.ovf*、をダウンロードします。*X.X.X-xxx* はバージョンとビルド番号です。

手順

-
- ステップ 1** vSphere Web クライアントにログインします。
- ステップ 2** Firewall Management Center Virtual を展開する Hyperflex クラスタを選択し、**[アクション (ACTIONS)] > [OVFテンプレートの展開 (Deploy OVF Template)]** の順にクリックします。
- ステップ 3** ファイルシステムで OVF テンプレートソースの場所を参照し、**[次へ (NEXT)]** をクリックします。
- 次の Firewall Management Center Virtual VI OVF テンプレートを選択できます。
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-X.X.X-xxx.ovf*

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。

- ステップ 4** Firewall Management Center Virtual 展開の名前とフォルダを指定し、[次へ (NEXT)] をクリックします。
- ステップ 5** コンピューティングリソースを選択し、互換性チェックが完了するまで待ちます。互換性チェックが成功したら、[次へ (NEXT)] をクリックします。
- ステップ 6** OVF テンプレートの情報（製品名、ベンダー、バージョン、ダウンロードサイズ、ディスク上のサイズ、説明）を確認して、[次へ (NEXT)] をクリックします。
- ステップ 7** OVF テンプレート（VI テンプレートのみ）でパッケージ化されたライセンス契約書を確認して承認し、[次へ (NEXT)] をクリックします。
- ステップ 8** ストレージの場所と仮想ディスク形式を選択し、[次へ (NEXT)] をクリックします。

このウィンドウで、宛先の HyperFlex クラスタ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。

[シックプロビジョン (Thick Provisioned)] を仮想ディスク形式として選択すると、すべてのストレージがただちに割り当てられます。[シンプロビジョン (Thin Provisioned)] を仮想ディスク形式として選択すると、データが仮想ディスクに書き込まれるときに、必要に応じてストレージが割り当てられます。また、シンプロビジョニングにより、仮想アプライアンスの展開に要する時間を短縮できます。

- ステップ 9** OVF テンプレートで指定されたネットワークをインベントリ内のネットワークにマッピングし、[次へ (NEXT)] をクリックします。
- ステップ 10** OVF テンプレートでパッケージ化された、ユーザー設定可能なプロパティを設定します。

（注）

このステップでは、必須のカスタマイズ項目をすべて設定する必要があります。

a) パスワード

Firewall Management Center Virtual 管理アクセス用のパスワードを設定します。

b) ネットワーク

完全修飾ドメイン名 (FQDN)、DNS、ネットワークプロトコル (IPv4 または IPv6) などのネットワーク情報を設定します。

c) [次へ (NEXT)] をクリックします。

- ステップ 11** 表示された情報を確認して検証します。これらの設定を使用して展開を開始するには、[終了 (FINISH)] をクリックします。変更を加えるには、[戻る (BACK)] をクリックして前の各画面に戻ります。

ウィザードが完了すると、vSphere Web Client によって仮想マシンが処理されます。[グローバル情報 (Global Information)] 領域の [最近使用したタスク (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 テンプレートの展開 (Deploy OVF Template)] 完了ステータスが表示されます。

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。

(注)

Cisco Licensing Authority に Firewall Management Center Virtual を正常に登録するには、インターネットアクセスが必要です。インターネットアクセスを実行して正常にライセンス登録するには、展開後に追加の構成が必要になります。ライセンス登録には DNS サーバー構成が必須です。

次のタスク

仮想アプライアンスを初期化します。[仮想アプライアンスの電源投入と初期設定](#)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 VM コンソール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。

HyperFlex で VI 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 のデプロイメントに必要な次のステップの概要については、[『Cisco Secure Firewall Management Center Virtual スタートアップガイド』](#)の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。