



Nutanix への Firewall Management Center Virtual の展開

Nutanix AHV は、ネイティブ ベアメタル タイプ 1 ハイパーバイザであり、クラウド対応の機能を備えたハイパーコンバージドインフラストラクチャ（HCI）です。

この章では、AHV ハイパーバイザを含む Nutanix 環境内における Firewall Management Center Virtual の機能について解説し、機能のサポート、システム要件、ガイドライン、制限事項などを説明します。

Nutanix AHV に Firewall Management Center Virtual を展開できます。

- [システム要件（1 ページ）](#)
- [前提条件（2 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）](#)

システム要件

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

- Nutanix AHV 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。
- 最新のリリースノート参照し、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。
- Nutanix AHV 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 GB/推奨（デフォルト）32 GB RAM



重要 仮想アプライアンスに割り当てる RAM が 28 GB 未満の場合、Firewall Management Center Virtual プラットフォームは動作しません。

- 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
 - 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

前提条件

バージョン

マネージャバージョン	デバイスバージョン
Firewall Device Manager 7.0	Firewall Threat Defense 7.0
7.0	

Firewall 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。

Cisco.com から qcow2 ファイルをダウンロードし、Nutanix Prism Web コンソールに格納します。

<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。

Firewall Management Center Virtual ライセンス

- からセキュリティ サービスのすべてのライセンス資格を設定します。
- ライセンスの管理方法の詳細については、『[Cisco Secure Firewall Management Center Configuration Guide](#)』の「*Licensing the System*」を参照してください。

Nutanix のコンポーネントとバージョン

コンポーネント	バージョン
Nutanix Acropolis OS (AOS)	5.15.5 LTS 以降 (VPC サポートなし)。 6.8 以降 (VPC サポートあり)。
Nutanix クラスタチェック (NCC)	4.0.0.1
Nutanix AHV	20201105.12 以降
Nutanix Prism Web コンソール	。

注意事項と制約事項

サポートされる機能

展開モード：スタンドアロン

サポートされない機能

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 (ESXi 上で動作する Nutanix AHV) はサポートされていません。Nutanix スタンドアロンクラスタの展開のみがサポートされます。
- ハイ アベイラビリティはサポートされません。

- Nutanix AHV は SR-IOV および DPDK-OVS をサポートしていません。

関連資料

- [Nutanix Release Notes](#)
- [Nutanix Field Installation Guide](#)
- [Nutanix でのハードウェアのサポート](#)

Firewall Management Center Virtual の導入

ステップ	タスク	詳細情報
1	前提条件を確認します。	前提条件 (2 ページ)
2	Firewall Management Center Virtual qcow2 ファイルを Nutanix 環境にアップロードします。	Firewall Management Center Virtual QCOW2 ファイルを Nutanix にアップロード (4 ページ)
3	(オプション) 仮想マシンの展開時に適用される初期設定データを含む第 0 日の構成ファイルを準備します。	第 0 日のコンフィギュレーションファイルの準備 (5 ページ)
4	Firewall Management Center Virtual を Nutanix 環境に展開します。	Nutanix への Management Center Virtual の展開
5	(任意) Firewall Management Center Virtual のセットアップに Day 0 の構成ファイルを使用しなかった場合は、CLI にログインして、セットアップを完了します。	Firewall Management Center Virtual のセットアップの完了 (9 ページ)

Firewall Management Center Virtual QCOW2 ファイルを Nutanix にアップロード

Firewall Management Center Virtual を Nutanix 環境に展開するには、Prism Web コンソールで Firewall Management Center Virtual qcow2 ディスクファイルからイメージを作成する必要があります。

始める前に

Cisco.com から Firewall Management Center Virtual qcow2 ディスクファイルをダウンロードします (<https://software.cisco.com/download/navigator.html>)。

手順

ステップ 1 Nutanix Prism Web コンソールにログインします。

ステップ 2 歯車アイコンをクリックして [設定 (Settings)] ページを開きます。

ステップ 3 左側のペインで [イメージの設定 (Image Configuration)] をクリックします。

ステップ 4 [Upload Image] をクリックします。

ステップ 5 イメージを作成します。

1. イメージの名前を入力します。
2. [イメージタイプ (Image Type)] ドロップダウンリストから、[ディスク (DISK)] を選択します。
3. [ストレージコンテナ (Storage Container)] ドロップダウンリストから、目的のコンテナを選択します。
4. Firewall Management Center Virtual qcow2 ディスクファイルの場所を指定します。
URL を指定して Web サーバーからファイルをインポートすることも、ワークステーションからファイルをアップロードすることもできます。
5. [保存 (Save)] をクリックします。

ステップ 6 [イメージの設定 (Image Configuration)] ページに新しいイメージが表示されるまで待ちます。

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 を展開する前に、Day 0 の構成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。

次の点を考慮してください。

- 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。
- 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、「[Firewall Management Center Virtual のセットアップの完了 \(9 ページ\)](#)」を参照してください。

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。
- 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。

手順

ステップ 1 任意のテキストエディタを使用して、新しいテキストファイルを作成します。

ステップ 2 次の例に示すように、テキストファイルに構成の詳細を入力します。テキストは JSON 形式であることに注意してください。テキストをコピーする前に、検証ツールを使用してテキストを検証できます。

例：

```
#FMC
{
  "EULA": "accept",
  "Hostname": "FMC-Production",
  "AdminPassword": "Admin123",
  "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": "disabled",
  "IPv6Addr": "",
  "IPv6Mask": "",
  "IPv6Gw": "",
}
```

ステップ 3 ファイルを「day0-config.txt」として保存します。

ステップ 4 ステップ 1 ～ 3 を繰り返して、展開する Firewall Management Center Virtual ごとに一意のデフォルト構成ファイルを作成します。

Nutanix への Firewall Management Center Virtual の展開

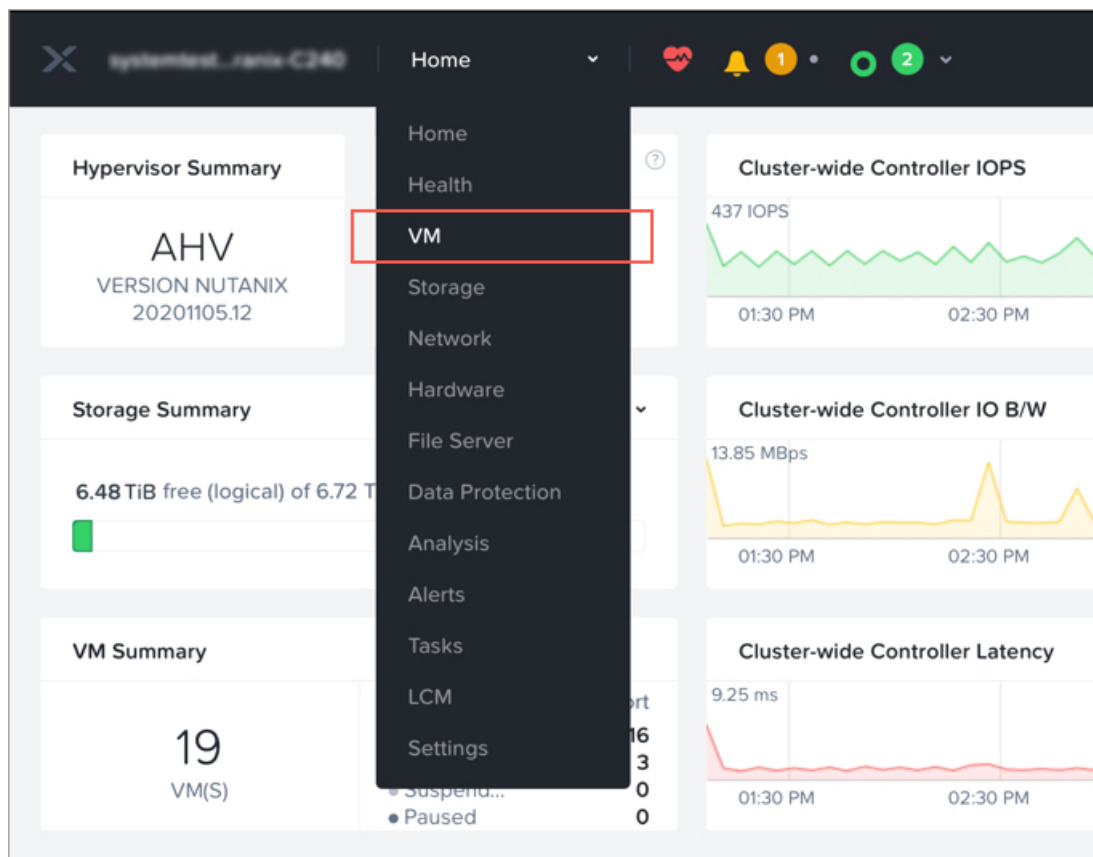
始める前に

展開する Firewall Management Center Virtual のイメージが [イメージの設定 (Image Configuration)] ページに表示されていることを確認します。

手順

ステップ 1 Nutanix Prism Web コンソールにログインします。

ステップ 2 メインメニューバーで、表示ドロップダウンリストをクリックし、[VM] を選択します。



ステップ 3 VM ダッシュボードで、[VMの作成 (Create VM)] をクリックします。

ステップ 4 次の手順を実行します。

1. Firewall Management Center Virtual インスタンスの名前を入力します。
2. 必要に応じて、Firewall Management Center Virtual インスタンスの説明を入力します。
3. Firewall Management Center Virtual インスタンスで使用するタイムゾーンを選択します。

ステップ 5 コンピューティングの詳細を入力します。

1. Firewall Management Center Virtual インスタンスに割り当てる仮想 CPU の数を入力します。
2. 各仮想 CPU に割り当てる必要があるコアの数を入力します。
3. Firewall Management Center Virtual インスタンスに割り当てるメモリの量 (GB) を入力します。

ステップ 6 Firewall Management Center Virtual インスタンスにディスクを接続します。

1. [ディスク (Disks)] で、[新しいディスクの追加 (Add New Disk)] をクリックします。
2. [タイプ (Type)] ドロップダウンリストから、[ディスク (DISK)] を選択します。
3. [操作 (Operation)] ドロップダウンリストから、[イメージサービスから複製 (Clone from Image Service)] を選択します。

4. [バスタイプ (Bus Type)] ドロップダウンリストから、[SCSI]、[PCI]、または [SATA] を選択します。
5. [イメージ (Image)] ドロップダウンリストから、使用するイメージを選択します。
6. [追加 (Add)] をクリックします。

ステップ 7 [ネットワークアダプタ (NIC) (Network Adapters (NIC))] で、[新しいNIC の追加 (Add New NIC)] をクリックし、ネットワークを選択して、[追加 (Add)] をクリックします。

ステップ 8 Firewall Management Center Virtual のアフィニティポリシーを設定します。

[VMホストアフィニティ (VM Host Affinity)] で、[アフィニティの設定 (Set Affinity)] をクリックし、ホストを選択して、[保存 (Save)] をクリックします。

ノードに障害が発生した場合でも Firewall Management Center Virtual を実行できるようにするには、1 つ以上のホストを選択します。

ステップ 9 第 0 日の構成ファイルを準備済みの場合は、次の手順を実行します。

1. [カスタムスクリプト (Custom Script)] を選択します。
2. [ファイルをアップロード (Upload A File)] をクリックし、第 0 日の構成ファイル (**day0-config.txt**) を選択します。

(注)

他のすべてのカスタム スクリプト オプションは、このリリースではサポートされていません。

ステップ 10 [保存 (Save)] をクリックして、Firewall Management Center Virtual を展開します。VM テーブルビューに Firewall Management Center Virtual インスタンスが表示されます。

ステップ 11 仮想シリアルポートを作成して、Management Center Virtual に接続します。これを行うには、SSH を介して Nutanix コントローラ VM (CVM) にログインし、以下の Acropolis CLI (aCLI) コマンドを実行します。aCLI の詳細については、『[aCLI Command Reference](#)』を参照してください。

Nutanix AHV バージョン 6.8 以前のコマンド :

```
vm.serial_port_create <management-center-virtual-VM-name> type=kServer index=0
```

```
vm.update <management-center-virtual-VM-name> disable_branding=true
```

```
vm.update <management-center-virtual-VM-name> extra_flags="enable_hyperv_clock=False"
```

Nutanix AHV バージョン 6.8.1 以降のコマンド :

```
vm.serial_port_create <management-center-virtual-VM-name> type=kServer index=0
```

```
vm.update <management-center-virtual-VM-name> disable_branding=true
```

```
vm.update <management-center-virtual-VM-name> disable_hyperv=True
```

ステップ 12 VM テーブルビューに移動し、新たに作成した Firewall Management Center Virtual インスタンスを選択して、[電源オン (Power On)] をクリックします。

- ステップ 13** Firewall Management Center Virtual の電源がオンになったら、ステータスを確認します。[ホーム (Home)] > [VM] > 展開した Firewall Management Center Virtual の順に移動し、ログインします。

Firewall Management Center Virtual のセットアップの完了

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。

手順

- ステップ 1** 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。
- ステップ 2** 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。
- ステップ 3** CLI を使用して、Firewall Management Center Virtual での初期セットアップを完了します。「[スクリプトを使用したネットワーク設定の構成 \(9 ページ\)](#)」を参照してください。
- ステップ 4** 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 \(10 ページ\)](#) を参照してください。

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。Nutanix コンソールを使用している場合、デフォルトのパスワードは **Admin123** です。

プロンプトが表示されたら、パスワードをリセットします。

- 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。プロンプトが表示されたら、パスワードをリセットします。

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。