Cisco Cisco Secure Firewall Management Center Virtual スタートアップガイド

最終更新：2026 年 4 月 23 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章 **Firewall Management Center Virtual の概要** 1

Firewall Management Center Virtual のプラットフォームとサポート 1

Firewall Management Center Virtual ライセンス 4

Firewall Management Center 機能ライセンスについて 4

仮想アプライアンスのパフォーマンスについて 5

Firewall Management Center Virtual 導入パッケージのダウンロード 8

第 2 章 **VMware への Firewall Management Center Virtual の展開** 11

Firewall Management Center Virtual の VMware 機能のサポート 11

システム要件 13

注意事項と制約事項 16

VMXNET3 インターフェイスの設定 20

インストール パッケージのダウンロード 21

Firewall Management Center Virtual の導入 22

仮想マシンのプロパティの確認 25

仮想アプライアンスの電源投入と初期設定 26

第 3 章 **Firewall Management Center Virtual の KVM への展開** 29

概要 29

前提条件 31

注意事項と制約事項 32

第 0 日のコンフィギュレーション ファイルの準備 33

Firewall Management Center Virtual の導入 35

導入スクリプトを使用した起動 35

Firewall Management Center Virtual の導入 37
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 39
スクリプトを使用したネットワーク設定の構成 39
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 40

第 4 章 AWS での Firewall Management Center Virtual の展開 41
概要 41
AWS ソリューションの概要 43
注意事項と制約事項 44
AWS 環境の設定 45
VPC の作成 46
インターネット ゲートウェイの追加 47
サブネットの追加 48
ルート テーブルの追加 48
セキュリティ グループの作成 49
ネットワーク インターフェイスの作成 50
Elastic IP の作成 51
Firewall Management Center Virtual の導入 52

第 5 章 Azure での Firewall Management Center Virtual の展開 57
概要 57
前提条件 59
注意事項と制約事項 60
導入時に作成されるリソース 61
Firewall Management Center Virtual の導入 62
ソリューションテンプレートを使用した Azure Marketplace からの展開 63
VHD およびリソーステンプレートを使用した Azure からの展開 67
制限付きの Azure プライベート マーケットプレイス環境での Azure マーケットプレイスオファーの展開 71
Azure での IPv6 サポート対象 Secure Firewall Management Center Virtual の展開 73
Azure での IPv6 をサポートする展開について 73

Marketplace イメージ参照を含むカスタム IPv6 テンプレートを使用した Azure からの展開 75
VHD およびカスタム IPv6 テンプレートを使用した Azure からの展開 81
Firewall Management Center Virtual 展開の確認 87
モニターリングおよびトラブルシューティング 90
機能の履歴 91

第 6 章 GCP への Firewall Management Center Virtual の展開 93
概要 93
前提条件 94
注意事項と制約事項 95
ネットワークトポロジの例 95
Firewall Management Center Virtual の導入 96
VPC ネットワークの作成 96
ファイアウォールルールの作成 97
GCP 上の Firewall Management Center Virtual インスタンスの作成 97
GCP 上の Firewall Management Center Virtual インスタンスへのアクセス 99
シリアルコンソールを使用した Firewall Management Center Virtual インスタンスへの接続 100
外部 IP を使用した Firewall Management Center Virtual インスタンスへの接続 100
Gcloud を使用した Firewall Management Center Virtual インスタンスへの接続 101

第 7 章 OCI への Firewall Management Center Virtual の導入 103
概要 103
前提条件 105
注意事項と制約事項 106
ネットワークトポロジの例 106
Firewall Management Center Virtual の導入 107
仮想クラウドネットワーク（VCN）の設定 107
ネットワーク セキュリティ グループの作成 108
インターネットゲートウェイの作成 108
サブネットの作成 109

OCI での Firewall Management Center Virtual インスタンスの作成 110
OCI 上の Firewall Management Center Virtual インスタンスへのアクセス 112
PuTTY を使用した Firewall Management Center Virtual インスタンスへの接続 112
SSH を使用した Firewall Management Center Virtual インスタンスへの接続 113
OpenSSH を使用した Firewall Management Center Virtual インスタンスへの接続 114

第 8 章 **OpenStack への Firewall Management Center Virtual の展開 117**
概要 117
前提条件 118
注意事項と制約事項 119
システム要件 120
ネットワークトポロジの例 121
Firewall Management Center Virtual の導入 122
OpenStack への Firewall Management Center Virtual イメージのアップロード 122
OpenStack と Firewall Management Center Virtual のネットワーク インフラストラクチャの作成 123
OpenStack での Firewall Management Center Virtual インスタンスの作成 124

第 9 章 **Cisco HyperFlex への Firewall Management Center Virtual の展開 127**
システム要件 127
注意事項と制約事項 129
Firewall Management Center Virtual の導入 130
仮想アプライアンスの電源投入と初期設定 132

第 10 章 **Nutanix への Firewall Management Center Virtual の展開 135**
システム要件 135
前提条件 136
注意事項と制約事項 137
Firewall Management Center Virtual の導入 138
Firewall Management Center Virtual QCOW2 ファイルを Nutanix にアップロード 138
第 0 日のコンフィギュレーション ファイルの準備 139

Nutanix への Firewall Management Center Virtual の展開 140
Firewall Management Center Virtual のセットアップの完了 143
スクリプトを使用したネットワーク設定の構成 143
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 144

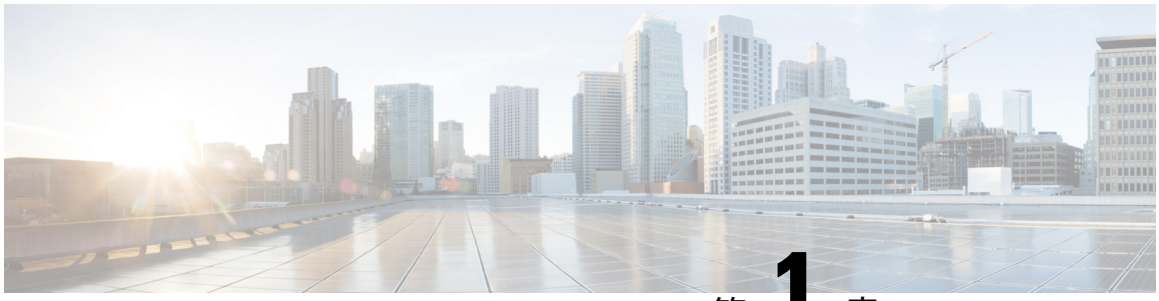
第 11 章 **Alibaba クラウドへの Cisco Secure Firewall Management Center Virtual の展開 147**
概要 147
注意事項と制約事項 148
前提条件 149
Firewall Management Center Virtual の導入 149

第 12 章 **Hyper-V での Firewall Management Center Virtual の展開 153**
概要 153
Hyper-V での Management Center Virtual のトポロジ例 154
Management Center Virtual でサポートされる Windows Server 154
Hyper-V での Management Center Virtual のガイドラインと制限事項 155
Hyper-V での Management Center Virtual の展開用ライセンス 155
Hyper-V での Management Center Virtual の展開に必要な前提条件 155
Management Center Virtual の展開 156
Management Center Virtual の VHD イメージをダウンロード 156
第 0 日のコンフィギュレーション ファイルの準備 156
仮想スイッチの新規作成 157
仮想マシンの新規作成 158
展開の確認 159
最初のブートログへのアクセス 159
Management Center Virtual のシャットダウン 160
Management Center Virtual の再起動 160
Management Center Virtual の削除 160
トラブルシューティング 161

第 13 章 **Firewall Management Center Virtual 初期設定 163**

Firewall Management CenterCLI（バージョン 6.5 以降）を使用した初期セットアップ 163
Web インターフェイスを使用したプラットフォームの初期設定（バージョン 6.5 以降） 166
バージョン 6.5 以降の自動初期設定の確認 171

第 14 章 **Firewall Management Center Virtual 初期管理および設定 173**
個別のユーザー アカウント 173
デバイス登録 174
ヘルス ポリシーとシステム ポリシー 175
ソフトウェアとデータベースの更新 175
トラブルシューティング 176



第 1 章

Firewall Management Center Virtual の概要

Cisco Secure Firewall Management Center Virtual（旧 Firepower Management Center Virtual）は、仮想環境に包括的なファイアウォール機能を提供し、データセンター通信とマルチテナント環境のセキュリティを強化します。

- Firewall Management Center Virtual のプラットフォームとサポート （1 ページ）
- Firewall Management Center Virtual ライセンス （4 ページ）
- 仮想アプライアンスのパフォーマンスについて （5 ページ）
- Firewall Management Center Virtual 導入パッケージのダウンロード （8 ページ）

Firewall Management Center Virtual のプラットフォームとサポート

メモリとリソースの要件

Firewall Management Center Virtual の各インスタンスには、パフォーマンスを最適化するため、ターゲットプラットフォーム上に最小リソース割り当て（メモリ容量、CPU 数、およびディスク容量）が必要です。

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 のアップグレード（6.6.0 以降）には 32 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 32 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。重要な Firewall Management Center Virtual アップグレード情報については、仮想アプライアンスのパフォーマンスについて（5ページ）を参照してください。

Firewall Management Center Virtual の初期セットアップ（6.5.0 以降）

Firewall Management Center Virtual バージョン 6.5 以降では、初期セットアップのエクスペリエンスが改善され、次の点が変更および機能拡張されています。

- **管理の DHCP**：管理インターフェイス（eth0）では、DHCP がデフォルトモードで有効になっています。

  Firewall Management Center Virtual 管理インターフェイスは、DHCP によって割り当てられた IPv4 または IPv6 アドレスを受け入れるように事前設定されています。DHCP により Firewall Management Center Virtual に割り当てるように設定されている IP アドレスを確認するには、システム管理者に問い合わせてください。DHCP を使用できないシナリオでは、Cisco Secure Firewall Management Center （旧 Firepower Management Center）管理インターフェイスは、IPv4 アドレス 192.168.45.45 または IPv6 アドレスを使用します（例：2001:db8::a111:b221:1:abca/96）を使用します。

（注） DHCP を使用する場合は、割り当てられたアドレスが変更されないように、DHCP 予約を使用する必要があります。DHCP アドレスが変更されると、Firewall Management Center ネットワーク設定が同期しなくなるため、デバイスの登録は失敗します。DHCP アドレスの変更から回復するには、（ホスト名または新しい IP アドレスを使用して）Firewall Management Center に接続し、**[システム（System）] > [設定（Configuration）] > [管理インターフェイス（Management Interfaces）]**に移動してネットワークをリセットします。

- **Web インターフェイスの URL**：Firewall Management Center Virtual Web インターフェイスのデフォルトの URL が https://<-IP>:<port>/ui/login に変更されました。
- **パスワードのリセット**：システムのセキュリティやプライバシーを確保するために、Firewall Management Center に初めてログインするときは、**admin** のパスワードを変更する必要があります。[パスワードの変更（Change Password）] ウィザード画面が表示されると、2 つのオプションが示されます。[新しいパスワード（New Password）] と [パスワードの確認（Confirm password）] テキストボックスに新しいパスワードを入力します。パスワードは、ダイアログに示された条件を満たす必要があります。

- **ネットワーク設定**：Firewall Management Center Virtual に、初期セットアップを実行するためのインストールウィザードが含まれるようになりました。
  - **完全修飾ドメイン名**：デフォルト値が表示されている場合は、デフォルト値を受け入れるか、完全修飾ドメイン名（構文 <hostname>.<domain>）またはホスト名を入力します。
  - **IPV4 または IPv6 接続のブートプロトコル**：IP アドレスの割り当て方法として DHCP またはスタティック/手動のいずれかを選択します。
  - **DNS グループ**：Firewall Management Center Virtual のデフォルトのドメイン ネーム サーバー グループは Cisco Umbrella DNS です。
  - **NTPグループサーバー**：デフォルトのネットワーク タイム プロトコル グループは、Sourcefire NTP プールに設定されます。
- **RAM 要件**：Firewall Management Center Virtual の RAM の推奨サイズは 32GB です。
- **VMware 用 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 VMware プラットフォームで使用できます。

対応プラットフォーム

Firewall Management Center Virtual は、次のプラットフォームに導入できます。

- **VMware vSphere Hypervisor（ESXi）**：Firewall Management Center Virtual を VMware ESXi 上のゲスト仮想マシンとして導入できます。
- **カーネル仮想化モジュール（KVM）**：Firewall Management Center Virtual を KVM ハイパーバイザを実行している Linux サーバーに導入できます。
- **Amazon Web Services（AWS）**：Firewall Management Center Virtual を AWS クラウドの EC2 インスタンスに導入できます。
- **Microsoft Azure**：Firewall Management Center Virtual を Azure Cloud に導入できます。
- **Google Cloud Platform（GCP）**：Firewall Management Center Virtual をパブリック GCP に導入できます。
- **Oracle Cloud Infrastructure（OCI）**：Firewall Management Center Virtual を OCI に導入できます。
- **OpenStack**：Firewall Management Center Virtual を OpenStack に導入できます。この展開では、KVM ハイパーバイザを使用して仮想リソースを管理します。
- **Cisco HyperFlex**：Firewall Management Center Virtual を Cisco HyperFlex に導入できます。
- **Nutanix**：AHV ハイパーバイザを使用して Firewall Management Center Virtual を Nutanix 環境に導入できます。
- **Alibaba Cloud**：Firewall Management Center Virtual を Alibaba Cloud に導入できます。

- **Microsoft Hyper-V** : Microsoft Hyper-V に Firewall Management Center Virtual を展開できます。

（注） ハイアベイラビリティ（HA）の設定は、VMware、AWS、Azure、KVM、OCI、およびHyperFlexでの Firewall Management Center Virtual の導入でサポートされています。ハイアベイラビリティのシステム要件については、『Management Center Administration Guide』の「*High Availability*」を参照してください。

ハイパーバイザとバージョンのサポート

ハイパーバイザとバージョンのサポートについては、『Cisco Secure Firewall Threat Defense Compatibility』を参照してください。

Firewall Management Center Virtual ライセンス

Firewall Management Center Virtual ライセンスは、機能ライセンスではなく、プラットフォームライセンスです。ご購入いただく仮想ライセンスのバージョンによって、Firewall Management Center を介して管理可能なデバイスの数が決まります。たとえば、2 台、10 台、25 台、300 台のデバイスを管理可能なライセンスをご購入いただけます。

Firewall Management Center 機能ライセンスについて

組織にとって最適なシステムの展開を実現するために、さまざまな機能のライセンスを付与できます。Firewall Management Center では、これらの機能ライセンスを管理してデバイスに割り当てることができます。

（注） Firewall Management Center はデバイスの機能ライセンスを管理しますが、Firewall Management Center を使用するための機能ライセンスは必要ありません。

Firewall Management Center 機能ライセンスは、デバイスタイプに応じて異なります。

- スマートライセンスは Firewall Threat Defense および Firewall Threat Defense Virtual デバイスに使用可能です。
- 7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv デバイスにはクラシック ライセンスを使用できます。

従来のライセンスを使用するデバイスは、クラシック デバイスと呼ばれることもあります。1 つの Firewall Management Center で従来のライセンスとスマート ライセンスの両方を管理できます。

「使用権」機能ライセンスに加えて、多くの機能にはサービス サブスクリプションが必要です。使用権ライセンスに有効期限はありませんが、サービス サブスクリプションは定期的に更新する必要があります。

ライセンスプラットフォームの詳細については、『Cisco Secure Firewall Management Center Administration Guide』の「Licenses」を参照してください。

スマートライセンス、クラシックライセンス、使用権ライセンス、およびサービスサブスクリプションに関するよくある質問への回答については、『Cisco Secure Firewall Management Center Feature Licenses』を参照してください。

仮想アプライアンスのパフォーマンスについて

仮想アプライアンスのスループットおよび処理能力を正確に予測することは不可能です。次のように、多数の要因がパフォーマンスに大きく影響します。

- ホストのメモリと CPU の容量
- ホストで実行されている仮想マシンの総数
- 導入されるセンシング インターフェイスのネットワーク パフォーマンス、インターフェイス速度、および数
- 各仮想アプライアンスに割り当てられたリソースの量
- ホストを共有する他の仮想アプライアンスのアクティビティのレベル
- 仮想デバイスに適用されるポリシーの複雑さ

スループットに満足できない場合は、ホストを共有する仮想アプライアンスに割り当てられたリソースを調整します。

作成する各仮想アプライアンスでは、ホストに一定量のメモリ、CPU、およびハードディスクスペースが必要です。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。ただし、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。

次の表は、サポートされる Firewall Management Center Virtual の制限について一覧表示したものです。

表 *1 :* サポートされる *Management Center Virtual* の制限

コンポーネント	FMCv2/FMCv10/FMCv25	FMCv300
vCPU	8/4 vCPU	32 vCPU
メモリ	32 GB	64 GB
イベント記憶域	250 GB	2.2 TB

コンポーネント	FMCv2/FMCv10/FMCv25	FMCv300
最大ネットワークマップサイズ（ホスト/ユーザー）	50,000/50,000	150,000/150,000
最大イベントレート（イベント数/秒）	5,000	12,000 eps

Firewall Management Center Virtual のデフォルトおよび最小メモリ要件

すべての Firewall Management Center Virtual 実装に同じ RAM 要件が適用され、32 GB が必須となりました（FMCv300 の場合は 64 GB）。 仮想アプライアンスに割り当てられた RAM が 32 GB 未満の場合、バージョン 6.6.0+ へのアップグレードは失敗します。アップグレード後、メモリ割り当てを引き下げると、正常性モニターがアラートを発行します。

これらの新しいメモリ要件は、すべての仮想環境にわたって一貫した要件を適用し、パフォーマンスを向上させ、新しい機能を利用できるようにします。デフォルト設定を引き下げないことをお勧めします。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。

重要 バージョン 6.6.0 リリースの時点で、クラウドベースの Firewall Management Center Virtual の展開（AWS、Azure）でのメモリ不足インスタンスのタイプが完全に廃止されました。以前のバージョンであっても、それらを使用して新しい Firewall Management Center Virtual インスタンスは作成できません。既存のインスタンスは引き続き実行できます。

次の表に、メモリが不足している Firewall Management Center Virtual 展開のアップグレード前の要件を示します。

表 *2:* バージョン *6.6.0* 以降 にアップグレードする場合の *Firewall Management Center Virtual* のメモリ要件

プラットフォーム	アップグレード前のアクション	詳細
VMware	32 GB 以上を割り当てます。	最初に仮想マシンの電源をオフにします。 手順については、VMware のマニュアルを参照してください。
KVM	32 GB 以上を割り当てます。	手順については、ご使用の KVM 環境のマニュアルを参照してください。

プラットフォーム	アップグレード前のアクション	詳細
AWS	インスタンスのサイズを変更します。 • c3.xlarge から c3.4xlarge へ。 • c3.2.xlarge から c3.4xlarge へ。 • c4.xlarge から c4.4xlarge へ。 • c4.2xlarge から c4.4xlarge へ。 また、新規展開用に c5.4xlarge インスタンスも用意しています。	サイズを変更する前にインスタンスを停止します。これを行うと、インスタンスストアのボリューム上のデータが失われるため、最初にインスタンスストアによってバックアップされたインスタンスを最初に移行してください。さらに、管理インターフェイスに復元力のある IP アドレスがない場合は、そのパブリック IP アドレスが解放されます。 手順については、Linux インスタンスの AWS ユーザーガイドのインスタンスタイプの変更に関するマニュアルを参照してください。
Azure	インスタンスのサイズを変更します。 • Standard_D3_v2 から Standard_D4_v2 へ。	Azure ポータルまたは PowerShell を使用します。サイズを変更する前にインスタンスを停止する必要はありませんが、停止すると追加のサイズが表示される場合があります。サイズ変更により、実行中の仮想マシンが再起動されます。 手順については、Windows VM のサイズ変更に関する Azure のマニュアルを参照してください。
GCP	GCP インスタンスタイプに基づいてメモリを割り当てます。	詳細については、「GCP マシンタイプのサポート」を参照してください。
OCI	OCI インスタンスタイプに基づいてメモリを割り当てます。	詳細については、「OCI のコンピューティングシェイプ」を参照してください。
OpenStack	32 GB 以上を割り当てます。	詳細については、「メモリとリソースの要件」を参照してください。
[HyperFlex]	32 GB 以上を割り当てます。	詳細については、「ホストシステム要件」を参照してください。
Nutanix	32 GB 以上を割り当てます。	詳細については、「ホストシステム要件」を参照してください。

Firewall Management Center Virtual 導入パッケージのダウンロード

Firewall Management Center Virtual 導入パッケージは Cisco.com からダウンロードできます。パッチまたはホットフィックスの場合は Firewall Management Center 内からダウンロードできます。

Firewall Management Center Virtual 導入パッケージをダウンロードするには、次の手順に従います。

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 ご使用のモデル > [FireSIGHT システム ソフトウェア（FireSIGHT System Software）] > バージョンの順に選択します。

次の表に、Cisco.com 上の Firewall Management Center Virtual ソフトウェアについての命名規則と情報を示します。

モデル	パッケージ タイプ	パッケージ名
Firewall Management Center Virtual	ソフトウェアのインストール：VMware	Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-*version*.**tar.gz**
	ソフトウェアのインストール：KVM	Cisco_Secure_FW_Mgmt_Center_Virtual_KVM-*version*.**qcow2**
	ソフトウェアのインストール：AWS	クラウド サービスにログインし、マーケットプレイスから展開します。
	ソフトウェアのインストール：Azure	クラウド サービスにログインし、マーケットプレイスから展開します。

ステップ 5 導入パッケージを見つけ、サーバーまたは管理コンピュータにダウンロードします。

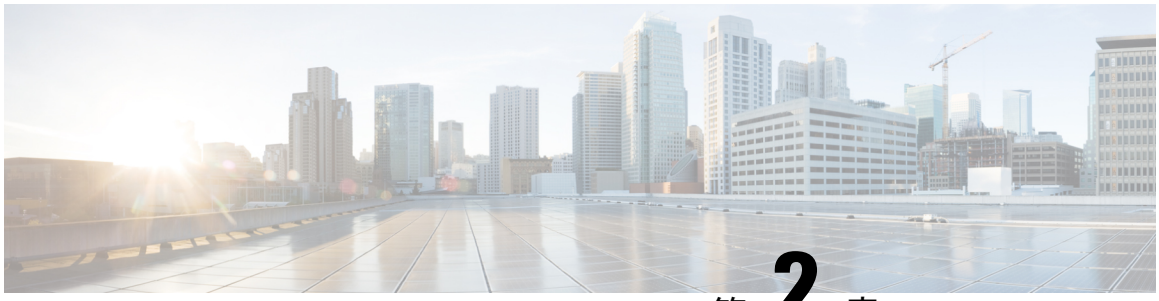
名前が似ているパッケージが多数あります。確認して正しいものをダウンロードしてください。

シスコサポートおよびダウンロードサイトから直接ダウンロードします。電子メールで導入パッケージを転送すると、破損する可能性があります。

次のタスク

導入プラットフォームに対応する章を参照してください。

- Firewall Management Center Virtual を VMware ESXi 上にゲスト仮想マシンとして展開する場合は、VMware への Firewall Management Center Virtual の展開 （11 ページ）を参照してください。
- KVM ハイパーバイザを実行している Linux サーバーで Firepower Management Center Virtual を展開するには、Firewall Management Center Virtual の KVM への展開 （29 ページ） を参照してください。
- Firewall Management Center Virtual を AWS に展開する場合は、AWS での Firewall Management Center Virtual の展開 （41 ページ）を参照してください。
- Firewall Management Center Virtual を Azure に展開する場合は、Azure での Firewall Management Center Virtual の展開 （57 ページ）を参照してください。
- Firewall Management Center Virtual を Google Cloud Platform に展開する場合は、「Google Cloud Platform への Management Center Virtual の展開」を参照してください。
- Firewall Management Center Virtual を Oracle Cloud Infrastructure に展開する場合は、「Oracle Cloud Infrastructure への Management Center Virtual の展開」を参照してください。
- OpenStack を使用して Firewall Management Center Virtual を展開する場合は、「OpenStack を使用した Management Center Virtual の展開」を参照してください。
- Cisco HyperFlex を使用して Firewall Management Center Virtual を展開する場合は、「Cisco HyperFlex を使用した Management Center Virtual の展開」を参照してください。
- Nutanix を使用して Firewall Management Center Virtual を展開する場合は、「Nutanix を使用した Management Center Virtual の展開」を参照してください。
- Firewall Management Center Virtual を Hyper-V に展開する場合は、Hyper-V での Firewall Management Center Virtual の展開 （153 ページ）を参照してください。



第 2 章

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 （11 ページ）
- システム要件 （13 ページ）
- 注意事項と制約事項 （16 ページ）
- インストール パッケージのダウンロード （21 ページ）
- Firewall Management Center Virtual の導入 （22 ページ）
- 仮想マシンのプロパティの確認 （25 ページ）
- 仮想アプライアンスの電源投入と初期設定 （26 ページ）

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 *3 : 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（18 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 （18 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 *4 : 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 *5 : 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 *6 : 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 （163 ページ）」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、Firewall Management Center 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（Firewall Management Center 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（22 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、Firewall Management Center 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 （25 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 （26 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。

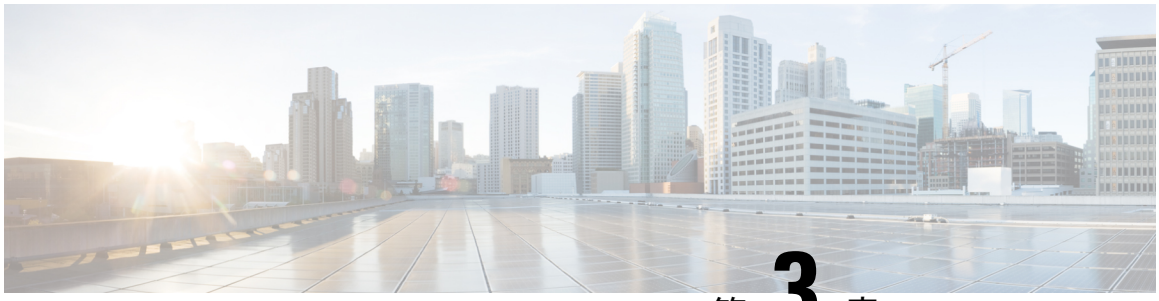
ステップ 2 VMware コンソール タブで初期化を監視します。

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 （163 ページ）」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。



第 3 章

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 （29 ページ）
- 前提条件 （31 ページ）
- 注意事項と制約事項 （32 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 （33 ページ）
- Firewall Management Center Virtual の導入 （35 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 （39 ページ）

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 （39 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 （37 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 （35 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 （37 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 Firewall Management Center 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。

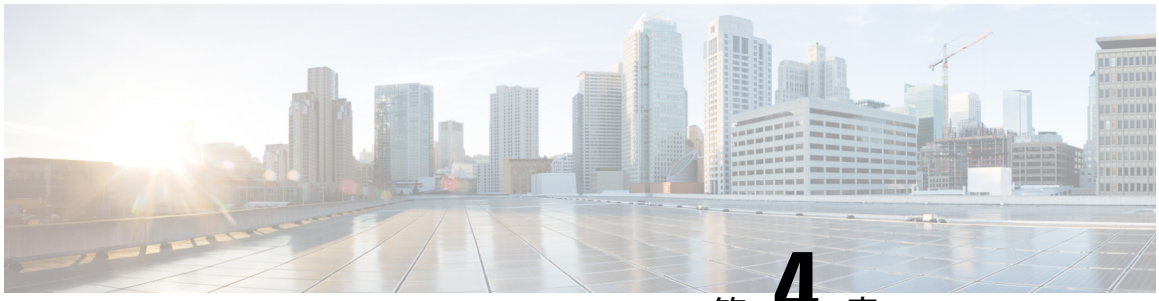
設定ページが表示されます。管理者のパスワード変更と、ネットワーク設定の指定をまだ行っていない場合はこれらの 2 つを実行し、EULA に同意する必要があります。

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 （163 ページ）」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 （173 ページ）」の章を参照してください。



第 4 章

AWS での Firewall Management Center Virtual の展開

Amazon Virtual Private Cloud（VPC）は、お客様が定義する仮想ネットワークで Amazon Web Services（AWS）のリソースを起動できるようにします。この仮想ネットワークは、お客様自身のデータセンターで運用されている可能性がある従来型のネットワークとよく似ているだけでなく、AWS のスケーラブルなインフラストラクチャを活用するというメリットがあります。

Firewall Management Center Virtual を AWS クラウドに展開できます。

- 概要 （41 ページ）
- 注意事項と制約事項 （44 ページ）
- AWS 環境の設定 （45 ページ）
- Firewall Management Center Virtual の導入 （52 ページ）

概要

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 バージョン 6.6.0 リリースの時点で、クラウドベースの Firewall Management Center Virtual の展開（AWS、Azure）でのメモリ不足インスタンスのタイプが完全に廃止されました。以前のバージョンであっても、それらを使用して新しい Firewall Management Center Virtual インスタンスは作成できません。既存のインスタンスは引き続き実行できます。表 7 : Firewall Management Center Virtual について、AWS でサポートされているインスタンスタイプ （42 ページ）を参照してください。

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。

次の表に、Firewall Management Center Virtual でサポートされる AWS インスタンスのタイプを示します。バージョン 6.5.x 以前でサポートされるタイプとバージョン 6.6.0 以降でサポートされるタイプがあります。

（注） 次の表に示すように、バージョン 6.6 では C5 インスタンスタイプのサポートが追加されています。インスタンスが大きくなるほど、AWS VM により多くの CPU リソースが提供され、パフォーマンスが向上し、さらに多くのネットワークインターフェイスが実現します。

表 *7 : Firewall Management Center Virtual* について、*AWS* でサポートされているインスタンスタイプ

プラットフォーム	バージョン 6.6.0+	vCPU	メモリ（GB）	インターフェイスの最大数	バージョン 6.5.x 以前	vCPU	メモリ（GB）	インターフェイスの最大数
Firewall Management Center Virtual	c3.4xlarge	16	30	8	c3.xlarge*	4	7.5	4
	c4.4xlarge	16	30	8	c3.2xlarge*	8	15	4
	c5.4xlarge	16	32	8	c3.4xlarge	16	30	8
	c6i.4xlarge	16	32	8	c4.xlarge*	4	7.5	4
	c6a.4xlarge	16	32	8	c4.2xlarge	8	15	4
	c6in.4xlarge	16	32	8	c4.4xlarge	16	30	8
	* Firewall Management Center Virtual のバージョン 6.6.0 では、これらのインスタンスタイプがサポートされなくなります。バージョン 6.6.0 以降では、28 GB 以上の RAM を搭載したインスタンスを使用して Firewall Management Center Virtual（任意のバージョン）を展開する必要があります。詳細については、「非推奨のインスタンスタイプ」と「インスタンスタイプのサイズ変更 （43 ページ）」を参照してください。							

表 *8 : Firewall Management Center Virtual 300* について、*AWS* でサポートされているインスタンスタイプ

プラットフォーム	バージョン 7.1.0 以降
Firewall Management Center Virtual 300（FMCv300）	c5.9xlarge：36 個の vCPU、72 GB SSD ストレージ：2,000 GB

非推奨のインスタンスタイプ

現在のバージョン 6.5.x 以前の Firewall Management Center Virtual デプロイメントは引き続き実行できますが、以下のインスタンスタイプを使用して新しい Firewall Management Center Virtual のデプロイメント（バージョンに関係なく）は開始できません。

- c3.xlarge：4 個の vCPU、7.5 GB（バージョン 6.6.0 以降の Firewall Management Center Virtual では無効）
- c3.2xlarge：8 個の vCPU、15 GB（バージョン 6.6.0 以降の Firewall Management Center Virtual では無効）
- c4.xlarge：4 個の vCPU、7.5 GB（バージョン 6.6.0 以降の Firewall Management Center Virtual では無効）
- c4.2xlarge：8 個の vCPU、15 GB（バージョン 6.6.0 以降の Firewall Management Center Virtual では無効）

インスタンスタイプのサイズ変更

Firewall Management Center Virtual の以前のバージョン（6.2.x、6.3.x、6.4.x、および 6.5.x）からバージョン 6.6.0 へのアップグレード時に、28 GB の RAM メモリ診断が実行されるため、現在のインスタンスタイプのサイズをバージョン 6.6.0 でサポートされるサイズに変更する必要があります（表 7 : Firewall Management Center Virtual について、AWS でサポートされているインスタンスタイプ （42 ページ）を参照）。

現在のインスタンスタイプと新しいインスタンスタイプに互換性がある場合は、インスタンスのサイズを変更できます。Firewall Management Center Virtual の展開の場合：

- c3.xlarge または c3.2xlarge のサイズを c3.4xlarge インスタンスタイプに変更します。
- c4.xlarge または c4.2xlarge のサイズを c4.4xlarge インスタンスタイプに変更します。

インスタンスのサイズを変更する前に、次の点に注意してください。

- インスタンスタイプを変更する前に、インスタンスを停止する必要があります。
- 現在のインスタンスタイプが、新たに選択したインスタンスタイプと互換性があることを確認します。
- インスタンスにインスタンス ストア ボリュームがある場合、そのインスタンス上のすべてのデータは失われます。サイズ変更する前に、インスタンスストアのバックアップインスタンスを移行します。
- Elastic IP アドレスを使用していない場合は、インスタンスを停止するとパブリック IP アドレスが解放されます。

インスタンスのサイズを変更する方法については、AWS のドキュメント『インスタンスタイプを変更する』（https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/ec2-instance-resize.html）を参照してください。

AWS ソリューションの概要

AWS は、Amazon.com によって提供されるリモート コンピューティング サービスの集合で、Web サービスとも呼ばれており、クラウド コンピューティング プラットフォームを構成しま

す。これらのサービスは、世界の 11 の地理的地域で運用されます。通常、Firewall Management Center Virtual を導入する際には、次の AWS サービスに精通している必要があります。

- Amazon Elastic Compute Cloud（EC2）：仮想コンピュータをレンタルして、お客様独自のアプリケーションおよびサービス（ファイアウォールなど）を Amazon のデータセンターで起動および管理できるようにする Web サービス。
- Amazon Virtual Private Cloud（VPC）：Amazon パブリック クラウド内の隔離されたプライベート ネットワークを設定できるようにする Web サービス。EC2 インスタンスは VPC 内で実行されます。
- Amazon Simple Storage Service（S3）：データ ストレージ インフラストラクチャを提供する Web サービス。

AWS でアカウントを作成し、VPC および EC2 コンポーネントを（AWS ウィザードまたは手動設定のいずれかを使用して）設定し、Amazon Machine Image（AMI）インスタンスを選択します。AMI は、インスタンスを起動するために必要なソフトウェア構成を含むテンプレートです。

（注） AMI イメージは AWS 環境の外部ではダウンロードできません。

注意事項と制約事項

サポートされる機能（7.1.0 以降）

- **AWS 用 Management Center Virtual 300（FMCv300）**：新しく拡張された 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 AWS プラットフォームで使用できます。
- 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。

前提条件

次に、AWS 上の Firewall Management Center Virtual に関する前提条件を示します。

- Amazon アカウント。aws.amazon.com で作成できます。
- Cisco スマートアカウント。Cisco Software Central（https://software.cisco.com/）で作成できます。
- Firewall Management Center Virtual へのライセンス付与。仮想プラットフォームライセンスに関する一般的なガイドラインについては、Firewall Management Center Virtual ライセンス（4 ページ） を参照してください。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。

- Firewall Management Center Virtual インターフェイスの要件：
  - 管理インターフェイス。
- 通信パス：
  - Firewall Management Center Virtual にアクセスするためのパブリック IP/Elastic IP。
- Firewall Management Center Virtual とシステム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。

ガイドライン

次に、AWS 上の Firewall Management Center Virtual に関するガイドラインを示します。

- 仮想プライベート クラウド（VPC）への導入
- 拡張ネットワーク（SR-IOV）（使用可能な場合）
- Amazon マーケットプレイスからの導入
- インスタンスあたり最大 4 つの vCPU
- L3 ネットワークのユーザー導入
- IPv6 がサポートされます。

制限事項

次に、AWS 上の Firewall Management Center Virtual に関する制限事項を示します。

- 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。
- IP アドレス設定（CLI または Firewall Management Center から設定）は、AWS コンソールで作成した設定と一致している必要があります。展開時に設定を書き留めてください。
- ブート後にインターフェイスを追加することはできません。
- 複製/スナップショットは現時点でサポートされていません。
- Transport Layer Security（TLS）サーバーアイデンティティ検出は、AWS での Geneve シングルアームセットアップではサポートされていません。

AWS 環境の設定

Firewall Management Center Virtual を AWS に展開するには、展開に固有の要件および設定を使用して Amazon VPC を設定する必要があります。ほとんどの環境では、セットアップ ウィザードに従ってセットアップを実行できます。AWS では、概要から詳細機能に至るまで、サービ

スに関する有用な情報を扱ったオンラインドキュメントを提供しています。詳細については、AWS の使用開始ドキュメントを参照してください。

AWS のセットアップを適切に制御するために、続くセクションでは、Firewall Management Center Virtual インスタンスの起動前の VPC および EC2 構成について説明します。

- VPC の作成 （46 ページ）
- インターネット ゲートウェイの追加 （47 ページ）
- サブネットの追加 （48 ページ）
- ルート テーブルの追加 （48 ページ）
- セキュリティ グループの作成 （49 ページ）
- ネットワーク インターフェイスの作成 （50 ページ）
- Elastic IP の作成 （51 ページ）

VPC の作成

仮想プライベート クラウド（VPC）は、AWS アカウント専用の仮想ネットワークです。これは、AWS クラウド内の他の仮想ネットワークから論理的に分離されています。Firewall Management Center Virtual インスタンスなどの AWS リソースを VPC に起動できます。VPC を設定できます。さらに、その IP アドレス範囲を選択し、サブネットを作成し、ルート テーブル、ネットワーク ゲートウェイ、およびセキュリティ設定を作成できます。

始める前に

- AWS アカウントを作成します。
- AMI が Firewall Management Center Virtual インスタンスで使用できることを確認します。

手順

ステップ 1 aws.amazon.com にログインし、地域を選択します。

AWSは互いに分かれた複数の地域に分割されています。地域は、画面の右上隅に表示されます。ある地域内のリソースは、別の地域には表示されません。目的の地域内に存在していることを定期的に確認してください。

ステップ 2 **[サービス（Services）] > [VPC]** の順にクリックします。

ステップ 3 **[VPC ダッシュボード（VPC Dashboard）] > [使用するVPC（Your VPCs）]** の順にクリックします。

ステップ 4 [VPCの作成（Create VPC）] をクリックします。

ステップ 5 [VPCの作成（Create VPC）] ダイアログボックスで、次のものを入力します。

a) VPC を識別するユーザー定義の [名前タグ（Name tag）]。

b) IP アドレスの [CIDRブロック（CIDR block）]。 CIDR（クラスレス ドメイン間ルーティング）の表記法は、IP アドレスとそれに関連付けられているルーティング プレフィクスのコンパクトな表現です。たとえば、「10.0.0.0/24」と入力します。

c) [デフォルト（Default）] の [テナント（Tenancy）] 設定。この VPC で起動されたインスタンスが、起動時に指定されたテナント属性を使用するようにします。

ステップ 6 [はい、作成します（Yes, Create）] をクリックして、VPC を作成します。

次のタスク

次のセクションで説明されているように、VPC にインターネット ゲートウェイを追加します。

インターネット ゲートウェイの追加

VPC をインターネットに接続するために、インターネット ゲートウェイを追加できます。VPC の外部の IP アドレスのトラフィックをインターネット ゲートウェイにルーティングできます。

始める前に

- Firewall Management Center Virtual のインスタンスの VPC を作成します。

手順

ステップ 1 **[サービス（Services）] > [VPC]** の順にクリックします。

ステップ 2 **[VPC ダッシュボード（VPC Dashboard）] > [インターネット ゲートウェイ（Internet Gateway）]** の順にクリックしてから、[インターネット ゲートウェイの作成（Create Internet Gateway）] をクリックします。

ステップ 3 ユーザー定義の [名前タグ（Name tag）] を入力してゲートウェイを特定し、[はい、作成します（Yes, Create）] をクリックしてゲートウェイを作成します。

ステップ 4 前のステップで作成したゲートウェイを選択します。

ステップ 5 [VPC に接続（Attach to VPC）] をクリックして、以前に作成した VPC を選択します。

ステップ 6 [はい、接続します（Yes, Attach）] をクリックして、ゲートウェイを VPC に追加します。

デフォルトでは、ゲートウェイが作成されて VPC に接続されるまで、VPC で起動されたインスタンスはインターネットと通信できません。

次のタスク

次のセクションで説明されているように、VPC にサブネットを追加します。

サブネットの追加

Firewall Management Center Virtual のインスタンスが接続できる VPC の IP アドレス範囲をセグメント化することができます。セキュリティおよび運用のニーズに応じて、インスタンスをグループ化するためのサブネットを作成できます。Firewall Threat Defense Virtual では、管理用のサブネットとトラフィック用のサブネットを作成する必要があります。

手順

ステップ 1 **[サービス（Services）]** > **[VPC]** の順にクリックします。

ステップ 2 **[VPC ダッシュボード（VPC Dashboard）]** > **[サブネット（Subnets）]** の順にクリックして、[サブネットの作成（Create Subnet）] をクリックします。

ステップ 3 [サブネットの作成（Create Subnet）] ダイアログボックスで、次のものを入力します。

a) サブネットを識別するユーザー定義の [名前タグ（Name tag）]。

b) このサブネットに使用する [VPC]。

c) このサブネットが存在する [可用性ゾーン（Availability Zone）]。 [設定なし（No Preference）] を選択して、Amazon が選択するゾーンを選びます。

d) IP アドレスの [CIDRブロック（CIDR block）]。 サブネットの IP アドレスの範囲は、VPC の IP アドレス範囲のサブセットである必要があります。ブロック サイズは、/16 ネットワーク マスクから /28 ネットワーク マスクの範囲で指定する必要があります。サブネットのサイズは VPC のサイズと同じにすることができます。

ステップ 4 [はい、作成します（Yes, Create）] をクリックして、サブネットを作成します。

ステップ 5 必要な数のサブネットについて、手順を繰り返します。管理トラフィックには別のサブネットを作成し、データ トラフィックに必要な数のサブネットを作成します。

次のタスク

次のセクションで説明されているように、VPC にルート テーブルを追加します。

ルート テーブルの追加

VPC 用に設定したゲートウェイにルート テーブルを接続できます。また、複数のサブネットを 1 つのルート テーブルに関連付けることができます。しかし、1 つのサブネットは一度に 1 つのルート テーブルにしか関連付けることができません。

手順

ステップ 1 **[サービス（Services）]** > **[VPC]** の順にクリックします。

ステップ 2 **[VPC ダッシュボード（VPC Dashboard）]** > **[ルート テーブル（Route Tables）]** の順にクリックしてから、[ルート テーブルの作成（Create Route Table）] をクリックします。

ステップ 3 ルート テーブルを識別するユーザー定義の [名前タグ（Name tag）] を入力します。

ステップ 4 このルート テーブルを使用する [VPC] をドロップダウン リストから選択します。

ステップ 5 [はい、作成します（Yes, Create）] をクリックして、ルート テーブルを作成します。

ステップ 6 作成したルート テーブルを選択します。

ステップ 7 [ルート（Routes）] タブをクリックして、詳細ペインにルート情報を表示します。

ステップ 8 [編集（Edit）] をクリックして、[別のルートを追加（Add another route）] をクリックします。

a) [宛先（Destination）] 列に、0.0.0.0/0 を入力します。

b) [ターゲット（Target）] 列で、先ほど作成したインターネット ゲートウェイを選択します。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 [サブネットアソシエーション（Subnet Associations）] タブをクリックし、[編集（Edit）] をクリックします。

ステップ 11 Firewall Management Center Virtual の管理インターフェイスに使用されるサブネットの隣にあるチェックボックスを選択し、[保存（Save）] をクリックします。

次のタスク

次のセクションで説明するように、セキュリティ グループを作成します。

セキュリティ グループの作成

許可されるプロトコル、ポート、送信元 IP 範囲を指定するルールを使用して、セキュリティ グループを作成できます。各インスタンスに割り当てることができる、さまざまな異なるルールを使用して、複数のセキュリティ グループを作成できます。AWS では、セキュリティ グループにまだ精通していないお客様のために、この機能に関する詳しい資料を用意しています。

手順

ステップ 1 **[サービス（Services）]** > **[EC2]** をクリックします。

ステップ 2 **[EC2 ダッシュボード（EC2 Dashboard）]** > **[セキュリティ グループ（Security Groups）]** の順にクリックします。

ステップ 3 [セキュリティグループの作成（Create Security Group）] をクリックします。

ステップ 4 [セキュリティ グループの作成（Create Security Group）] ダイアログボックスで、次のものを入力します。

a) セキュリティ グループを識別するユーザー定義の [セキュリティグループ名（Security group name）]。

b) このセキュリティ グループの [説明（Description）]。

c) このセキュリティ グループに関連付けられた VPC。

ステップ 5 [セキュリティグループルール（Security group rules）] を設定します。

a) [セキュリティグループの作成（Create Security Group）] をクリックします。

b) **[インバウンド（Inbound）]** セクションで、**[ルールの追加（Add Rule）]**をクリックします。

[タイプ（Type）] ドロップダウンリストから、インターネットによるアクセス用に開かれる以下のいずれかのインバウンドポートを選択します。デフォルトでは、**[すべての通信（All Traffic）]** タイプが選択されています。

- SSH（22）
- カスタム TCP（8305）
- HTTP（443）

（注）
Firewall Management Center Virtual を AWS の外部から管理するには、HTTPS および SSH アクセスが必要です。それに基づいて、送信元 IP アドレスを指定する必要があります。また、Firewall Management Center Virtual と Firewall Threat Defense Virtual の両方を AWS VPC 内で設定している場合、プライベート IP 管理サブネットアクセスを許可する必要があります。

c) **[アウトバウンド（Outbound）]** セクションで、**[ルールの追加（Add Rule）]** をクリックしてアウトバウンド通信のルールを追加するか、デフォルトの **[すべての通信（All traffic）]**（**[タイプ（Type）]** の場合）および **[任意の宛先（Anywhere）]**（**[宛先（Destination）]** の場合）のままにします。

ステップ 6 **[セキュリティグループの作成（Create security group）]** をクリックして、セキュリティグループを作成します。

次のタスク

次のセクションで説明されているように、ネットワーク インターフェイスを作成します。

ネットワーク インターフェイスの作成

スタティック IP アドレスを使用して、Firewall Management Center Virtual のネットワーク インターフェイスを作成できます。具体的な展開の必要に応じてネットワーク インターフェイス（内部および外部）を作成します。

手順

ステップ 1 **[サービス（Services）]** > **[EC2]** をクリックします。

ステップ 2 **[EC2 ダッシュボード（EC2 Dashboard）]** > **[ネットワーク インターフェイス（Network Interfaces）]** の順にクリックします。

ステップ 3 [ネットワークインターフェイスの作成（Create Network Interface）] をクリックします。

ステップ 4 [ネットワークインターフェイスの作成（Create Network Interface）] ダイアログボックスで、次のものを入力します。

a) ネットワーク インターフェイスに関するオプションのユーザー定義の [説明（Description）]。
b) ドロップダウン リストから [サブネット（Subnet）] を選択します。インスタンスを作成する VPC のサブネットが選択されていることを確認します。
c) [プライベートIP（Private IP）] アドレスを入力します。**自動割り当て**ではなく、スタティック IP アドレスを使用することが推奨されています。
d) [セキュリティグループ（Security groups）] を 1 つ以上選択します。セキュリティ グループの必要なポートがすべて開いていることを確認します。

ステップ 5 [はい、作成します（Yes, Create）] をクリックして、ネットワーク インターフェイスを作成します。

ステップ 6 作成したネットワーク インターフェイスを選択します。

ステップ 7 右クリックして、[送信元/宛先の変更の確認（Change Source/Dest. Check）]を選択します。

ステップ 8 [無効（Disabled）] を選択し、[保存（Save）] をクリックします。

作成したすべてのネットワーク インターフェイスについて、この操作を繰り返します。

次のタスク

次のセクションで説明するように、Elastic IP アドレスを作成します。

Elastic IP の作成

インスタンスが作成されると、パブリック IP アドレスはそのインスタンスに関連付けられます。インスタンスを停止してから開始すると、そのパブリック IP アドレスは自動的に変更されます。この問題を解決するには、Elastic IP アドレッシングを使用して、永続的なパブリック IP アドレスをそのインスタンスに割り当てます。Elastic IP は、Firewall Management Center Virtual および他のインスタンスへのリモートアクセスに使用されるパブリック IP 用に予約されます。AWS では、Elastic IP にまだ精通していないお客様のために、この機能に関する詳しい資料を用意しています。

（注） 少なくとも、Firewall Management Center Virtual に 1 つの Elastic IP アドレス、Firewall Threat Defense Virtual の管理および診断インターフェイスに 2 つの Elastic IP アドレスを作成します。

手順

ステップ 1 **[サービス（Services）]** > **[EC2]** をクリックします。

ステップ 2 **[EC2ダッシュボード（EC2 Dashboard）]** > **[Elastic IP]** の順にクリックします。

ステップ 3 [新規アドレスの割り当て（Allocate New Address）] をクリックします。

必要な数の Elastic IP およびパブリック IP について、この手順を繰り返します。

ステップ 4 [はい、割り当てます（Yes, Allocate）] をクリックして、Elastic IP を作成します。

ステップ 5 展開に必要な数の Elastic IP について、この手順を繰り返します。

次のタスク

次のセクションで説明されているように、Firewall Management Center Virtual を展開します。

Firewall Management Center Virtual の導入

始める前に

- 「AWS 環境の設定」の説明に従って、AWS VPC および EC2 のエレメントを設定します。
- AMI が Firewall Management Center Virtual インスタンスで使用できることを確認します。

（注） 初期展開時にユーザーデータを使用してデフォルトのパスワードを定義（**[高度な詳細（Advanced Details）] > [ユーザーデータ（User Data）]**）していなければ、デフォルトの管理者パスワードは AWS のインスタンス ID です。

手順

ステップ 1 https://aws.amazon.com/marketplace（Amazon マーケットプレイス）に移動してサインインします。

ステップ 2 Amazon マーケットプレイスにログインしたら、Firewall Management Center Virtual 用のリンクをクリックします。

（注）
すでに AWS を使用していた場合、リンクを有効にするには、いったんサインアウトしてから、サインインし直す必要があります。

ステップ 3 [続行（Continue）] をクリックしてから、[手動開始（Manual Launch）] タブをクリックします。

ステップ 4 [条件に同意する（Accept Terms）] をクリックします。

ステップ 5 [EC2コンソールを使用して起動する（Launch with EC2 Console）] をクリックします。

ステップ 6 Firewall Management Center Virtual でサポートされる [インスタンスタイプ（Instance Type）] を選択します。サポートされるインスタンスタイプについては、「About Deployment On the AWS Cloud」を参照してください。

ステップ 7 画面下部にある [次：インスタンスの詳細の設定（Next: Configure Instance Details）] ボタンをクリックします。

a) 前に作成した VPC に一致するように [ネットワーク（Network）] を変更します。
b) 前に作成した管理サブネットに一致するように [サブネット（Subnet）] を変更します。IP アドレスを指定するか、または自動生成を使用できます。
c) **[高度な詳細（Advanced Details）] > [ユーザーデータ（User Data）]** で、デフォルトのログイン情報を追加します。

デバイス名とパスワードの要件に合わせて、以下の例を変更してください。

ログイン設定の例：

```
#FMC
{
"AdminPassword": "<enter_your_password>",
"Hostname": "<Hostname-vFMC>"
}
```

注意
[高度な詳細（Advanced Details）] フィールドにデータを入力する際には、プレーン テキストのみを使用してください。テキスト エディタからこの情報をコピーする場合、プレーン テキストとしてのみコピーしてください。[高度な詳細（Advanced Details）] フィールドに Unicode データ（空白を含む）をコピーする場合、インスタンスが破損する可能性があります。その場合、インスタンスを終了して、作成し直す必要があります。

バージョン 7.0 以降では、初期展開時にユーザーデータを使用してデフォルトのパスワードを定義（**[高度な詳細（Advanced Details）] > [ユーザーデータ（User Data）]**）していなければ、デフォルトの管理者パスワードは AWS のインスタンス ID です。

以前のリリースでは、デフォルトの管理者パスワードは **Admin123** でした。

ステップ 8 [次：ストレージの追加（Next: Add Storage）] をクリックして、ストレージ デバイスの設定を構成します。

ルート ボリュームの設定を編集して、ボリュームのサイズ（GiB）を 250 GiB にします。250 GiB 未満はイベント ストレージを制限し、サポートされません。

ステップ 9 [次：タグ インスタンス（Next: Tag Instance）] をクリックします。

タグは大文字と小文字を区別するキーと値のペアで構成されます。たとえば、[キー（Key）]=名前、[値（Value）] = 管理でタグを定義できます。

ステップ 10 [次：セキュリティ グループの設定（Next: Configure Security Group）] を選択します。

ステップ 11 [既存のセキュリティグループを選択する（Select an existing Security Group）] をクリックして、以前に設定されたセキュリティ グループを選択するか、または新しいセキュリティ グループを作成できます。セキュリティ グループの作成の詳細については、AWS の資料を参照してください。

ステップ 12 [確認して起動する（Review and Launch）] をクリックします。

ステップ 13 [起動（Launch）] をクリックします。

ステップ 14 既存のキー ペアを選択するか、新しいキー ペアを作成します。

（注）

既存のキー ペアを選択することも、新しいキー ペアを作成することもできます。キー ペアは、AWS が保存する公開キーと、ユーザーが保存する秘密キー ファイルで構成されます。これらを一緒に使用すると、インスタンスに安全に接続できます。キー ペアはインスタンスへの接続に必要となる場合があるため、必ず既知の場所に保存してください。

ステップ 15 [インスタンスの起動（Launch Instances）] をクリックします。

ステップ 16 **[EC2ダッシュボード（EC2 Dashboard）]** > **[Elastic IP]** の順にクリックし、以前に割り当てられた IP を検索するか、新しい IP を割り当てます。

ステップ 17 Elastic IP を選択し、右クリックして [アドレスの関連付け（Associate Address）] を選択します。

インスタンスまたはネットワーク インターフェイスを検索して選択し、[関連付け（Associate）] をクリックします。

ステップ 18 **[EC2 ダッシュボード（EC2 Dashboard）]** > **[インスタンス（Instances）]** の順にクリックします。

ステップ 19 わずか数分後に、Firewall Management Center Virtual インスタンスの状態が [実行中（running）] と表示され、[ステータスチェック（Status checks）] に「2/2チェック（2/2 checks）」のパスが表示されます。ただし、展開と初期セットアップのプロセスが完了するまでには 30 ～ 40 分ほどかかります。ステータスを表示するには、インスタンスを右クリックし、**[インスタンス設定（Instance Settings）]** > **[インスタンスのスクリーンショットを取得（Get Instance Screenshot）]** を選択します。

セットアップが完了したら（約 30 ～ 40 分後）、**インスタンスのスクリーンショット**に「AWS vW.X.Y（ビルド ZZ）用 Cisco Secure Firewall Management Center」というようなメッセージが表示され、場合によってはその後に数行の出力が続きます。

これで、SSH または HTTP を使用して、新たに作成した Firewall Management Center Virtual にログインできるはずです。実際の展開時間は、お住まいの地域の AWS の負荷によって異なる場合があります。

SSH を使用して Firewall Management Center Virtual にアクセスできます。

```
ssh -i <key_pair>.pem admin@<Public_Elastic_IP>
```

SSH 認証は、キー ペアによって処理されます。パスワードは必要ありません。パスワードの入力を求められた場合、セットアップはまだ実行中です。

HTTPS を使用して Firewall Management Center Virtual にアクセスできます。

```
https//<Public_Elastic_IP>
```

（注）
「システム起動プロセスはまだ実行中です（system startup processes are still running）」が表示された場合、セットアップはまだ完了していません。

SSH や HTTPS から応答がない場合は、次の項目を再確認してください。

- 展開が完了していることを確認します。Firewall Management Center Virtual VM インスタンスのスクリーンショットに、「AWS vW.X.Y（ビルド ZZ）用 Cisco Secure Firewall Management Center」というようなメッセージが表示され、場合によってはその後に数行の出力が続きます。
- Elastic IP を保持し、それが Firewall Management Center の管理ネットワーク インターフェイス（eni）に関連付けられ、現在その IP アドレスに接続していることを確認します。

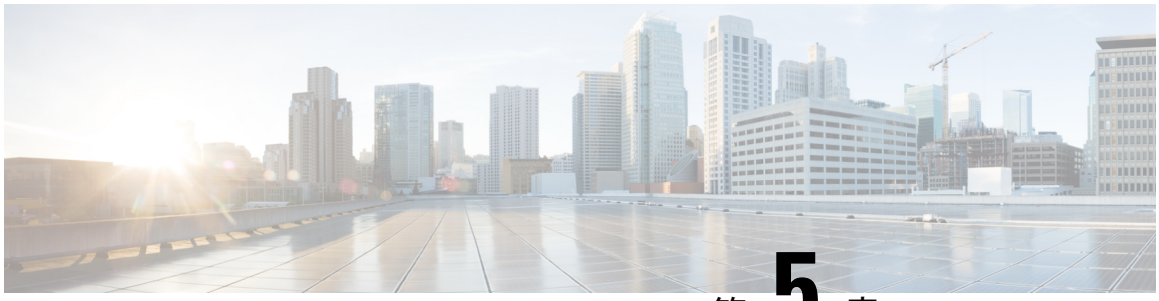
- VPC に関連付けられたインターネット ゲートウェイ（igw）があることを確認します。
- 管理サブネットにルート テーブルが関連付けられていることを確認します。
- 管理サブネットに関連付けられたルート テーブルに、インターネット ゲートウェイ（igw）を指す「0.0.0.0/0」へのルートがあることを確認します。
- セキュリティ グループでは、接続元の IP アドレスから SSH や HTTPS の着信を許可していることを確認します。

次のタスク

ポリシーとデバイス設定の設定

Firewall Threat Defense Virtual をインストールして、デバイスを Management Center に追加すると、Firewall Management Center ユーザーインターフェイスを使用して、AWS 上で実行する Firewall Threat Defense Virtual のデバイス管理設定を設定できます。また、Firewall Threat Defense Virtual デバイスを使用してトラフィックを管理するためのアクセス制御ポリシーやその他の関連ポリシーを設定して適用できます。セキュリティ ポリシーは、Next Generation IPS のフィルタリングやアプリケーションのフィルタリングなど、Firewall Threat Defense Virtual で提供されるサービスを制御します。Firewall Management Center を使用して、Firewall Threat Defense Virtual 上でセキュリティ ポリシーを設定します。セキュリティポリシーの設定方法の詳細については、コンフィギュレーション ガイドまたは Management Center のオンラインヘルプを参照してください。

-



第 5 章

Azure での Firewall Management Center Virtual の展開

Microsoft Azure パブリッククラウドに仮想マシンとして Firewall Management Center Virtual を展開できます。

重要 Firewall Management Center Virtual は、Cisco ソフトウェアバージョン 6.4 以降、Microsoft Azure でサポートされます。

- 概要 （57 ページ）
- 前提条件 （59 ページ）
- 注意事項と制約事項 （60 ページ）
- 導入時に作成されるリソース （61 ページ）
- Firewall Management Center Virtual の導入 （62 ページ）
- 制限付きの Azure プライベート マーケットプレイス環境での Azure マーケットプレイスオファーの展開 （71 ページ）
- Azure での IPv6 サポート対象 Secure Firewall Management Center Virtual の展開 （73 ページ）
- Azure での IPv6 をサポートする展開について （73 ページ）
- Marketplace イメージ参照を含むカスタム IPv6 テンプレートを使用した Azure からの展開 （75 ページ）
- VHD およびカスタム IPv6 テンプレートを使用した Azure からの展開 （81 ページ）
- Firewall Management Center Virtual 展開の確認 （87 ページ）
- モニターリングおよびトラブルシューティング （90 ページ）
- 機能の履歴 （91 ページ）

概要

Azure Marketplace で使用可能なソリューションテンプレートを使用して、Firewall Management Center Virtual を Microsoft Azure に展開します。Azure ポータルを使用して Firewall Management

Center Virtual を展開する場合は、既存の空のリソースグループとストレージアカウントを使用することができます（あるいは、それらを新規に作成できます）。ソリューションテンプレートによって、Firewall Management Center Virtual の初期セットアップを行う一連の設定パラメータを確認し、最初の起動後に Firewall Management Center Virtual Web インターフェイスにログインできます。

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 バージョン 6.6.0 リリースの時点で、クラウドベースの Firewall Management Center Virtual のデプロイメント（AWS、Azure）向けの低メモリの VM サイズが完全に廃止されました。以前のバージョンであっても、それらを使用して新しい Firewall Management Center Virtual インスタンスは作成できません。既存の VM サイズは引き続き実行できます。#unique_50 unique_50_Connect_42_table_n1j_dqb_2lbを参照してください。

このメモリチェックの結果として、サポート対象のプラットフォームで低メモリの VM サイズはサポートできなくなります。

Azure 上の Firewall Management Center Virtual は、Resource Manager 展開モードを使用して仮想ネットワーク（VNet）に展開する必要があります。標準の Azure パブリッククラウド環境に Firewall Management Center Virtual を展開できます。Azure Marketplace の Firewall Management Center Virtual は、Bring Your Own License（BYOL）モデルをサポートしています。

次の表に、Firewall Management Center Virtual でサポートされる Azure VM サイズを示します。バージョン 6.5.x 以前でサポートされるタイプとバージョン 6.6.0 以降でサポートされるタイプがあります。

表 *9 : Azure* でサポートされる *VM* サイズと *Firewall Management Center Virtual* バージョン

Azure VMサイズ	属性		Firewall Management Center Virtual バージョン
	vCPU	メモリ（GB）	
Standard_D3_v2	4	14	6.5 以前
Standard_D4_v2	8	36	6.6 以降
Standard_D8_v4	8	32	7.7.10 以降
Standard_D16_v4	16	64	7.7.10 以降
Standard_D8s_v4	8	32	7.7.10 以降
Standard_D16s_v4	16	64	7.7.10 以降

Azure VMサイズ	属性		Firewall Management Center Virtual バージョン
	vCPU	メモリ（GB）	
Standard_D8_v5	8	32	7.7.10 以降
Standard_D16_v5	16	64	7.7.10 以降
Standard_D8s_v5	8	32	7.7.10 以降
Standard_D16s_v5	16	64	7.7.10 以降

非推奨の VM サイズ

Standard_D3_v2 を使用して現在のバージョン 6.5.x 以前の Firewall Management Center Virtual デプロイメントは引き続き実行できますが、この VM サイズを使用して新しい Firewall Management Center Virtual デプロイメント（バージョンに関係なく）は開始できなくなります。

VM のサイズ変更

Firewall Management Center Virtual の以前のバージョン（6.2.x、6.3.x、6.4.x、および 6.5.x）からバージョン 6.6.0 へのアップグレード時に、28 GB の RAM メモリ診断が実行されるため、Standard_D3_v2 を使用している場合は、VM のサイズを Standard_D4_v2 に変更する必要があります（#unique_50 unique_50_Connect_42_table_n1j_dqb_2lb を参照）。

Azure ポータルまたは PowerShell を使用して VM のサイズを変更できます。仮想マシンが稼働中の場合、サイズを変更すると仮想マシンが再起動されます。仮想マシンを停止すると、追加のサイズがわかります。

VM のサイズを変更する方法については、Azure のマニュアル『Windows VM のサイズ変更』（https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/resize-vm）を参照してください。

前提条件

Microsoft Azure での Firewall Management Center Virtual のサポートは、バージョン 6.4.0 のリリースで新たに追加されています。Firewall Management Center Virtual とシステム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。

Azure に Firewall Management Center Virtual を展開する前に、次のことを確認してください。

- Azure.com でアカウントを作成します。

  Microsoft Azure でアカウントを作成したら、ログインしてマーケットプレイスで Firewall Management Center Virtual を検索し、「Firewall Management Center BYOL」サービスを選択できます。

- Cisco スマートアカウント。Cisco Software Central （https://software.cisco.com/）で作成できます。

注意事項と制約事項

サポートされる機能

- サポートされる Azure VM のサイズ
  - Standard_D3_v2—4 vCPU、14GB のメモリ、250GB のディスクサイズ
  - Standard_D4_v2—8 vCPU、28GB のメモリ、400GB のディスクサイズ

ライセンシング

Azure パブリック マーケットプレイスの Firewall Management Center Virtual は、Bring Your Own License（BYOL）モデルをサポートしています。Firewall Management Center Virtual の場合、これは、機能ライセンスではなく、プラットフォームライセンスです。ご購入いただく仮想ライセンスのバージョンによって、Firewall Management Center Virtual を介して管理可能なデバイスの数が決まります。たとえば、2 台、10 台、または 25 台のデバイスを管理可能なライセンスをご購入いただけます。

- ライセンス モード
  - スマートライセンスのみ

ライセンスの管理方法の詳細については、『Secure Firewall Management Center Configuration Guide』および『』の「*Licensing the System*」を参照してください。システムの機能ライセンスの概要（有用なリンクを含む）については、「Cisco Secure Firewall Management Center Feature Licenses」および「」を参照してください。

システムのシャットダウンと再起動

Firewall Management Center Virtual VM の電源をオンにするために Azure 仮想マシンの [概要（Overview）] ページで、[再起動（Restart）] と [停止（Stop）] のコントロールを使用しないでください。これらはグレースフル シャットダウン メカニズムではなく、データベースの破損につながる可能性があります。

Firewall Management Center Virtual の Web インターフェイスで使用可能な **[システム（System）]** > **[設定（Configuration）]** オプションを使用して、仮想アプライアンスをシャットダウンまたは再起動します。

Firewall Management Center Virtual のコマンド ライン インターフェイスから `shutdown` および `restart` コマンドを使用して、アプライアンスをシャットダウンまたは再起動します。

サポートされない機能

- ライセンス モード
  - Pay As You Go（PAYG）ライセンシング

- パーマネントライセンス予約（PLR）

- 管理
  - Azure ポータルの「パスワードのリセット」機能
  - コンソールベースのパスワード回復。ユーザーはコンソールにリアルタイムアクセスができないため、パスワードの回復もできません。パスワード回復イメージの起動ができません。唯一の方法は、新しい Firewall Management Center Virtual VM を展開することです。

- VM のインポート/エクスポート
- Cisco Secure Firewall バージョン 7.4.1 以前のバージョンでは、HA はサポートされていません。
- Azure での Gen 2 VM の生成
- 展開後の VM のサイズ変更
- VM の OS ディスクの Azure ストレージ SKU を Premium から Standard SKU に移行または更新、およびその逆

導入時に作成されるリソース

Azure に Firewall Management Center Virtual を展開すると、次のリソースが作成されます。

- 1 つのインターフェイスを備えた Firewall Management Center Virtual マシン（1 つのサブネットを持つ新規または既存の仮想ネットワークが必要）。
- リソースグループ

  Firewall Management Center Virtual は常に新しいリソースグループに配置されます。ただし、Firepower Threat Defense Virtual を別のリソースグループ内の既存仮想ネットワークにアタッチすることはできます。

- セキュリティグループ（名前は、*vm name*-mgmt-SecurityGroup）

  セキュリティグループは VM の Nic0 にアタッチされます。

  このセキュリティグループには、Firewall Management Center インターフェイス（TCP ポート 8305）用の SSH（TCP ポート 22）および管理トラフィックを許可するルールが含まれます。導入後に、これらの値を変更できます。

- パブリック IP アドレス（導入時に選択した値に従って命名）

  パブリック IP アドレスは、Management にマッピングされる VM の Nic0 に関連付けられます。

（注） 新しいパブリック IP を作成することも、既存のパブリック IP を選択することもできます。[なし（NONE）] を選択することもできます。パブリック IP アドレスがない場合、Firewall Management Center Virtual へのすべての通信は Azure 仮想ネットワーク内から発信する必要があります。

- サブネットのルーティングテーブル（既存の場合は最新のもの）
- 選択したストレージアカウントの起動時診断ファイル

  起動時診断ファイルは、ブロブ（サイズの大きいバイナリオブジェクト）内に配置されます。
- 選択したストレージアカウントのブロブおよびコンテナ VHD にある 2 つのファイル（名前は、*VM name*-disk.vhd および *VM name*-<uuid>.status）
- ストレージアカウント（既存のストレージアカウントが選択されていない場合）

重要 VM を削除すると、保持を希望する任意のリソースを除き、これらの各リソースを個別に削除する必要があります。

Firewall Management Center Virtual の導入

テンプレートを使用して、Azure に Firewall Management Center Virtual を展開できます。2 種類のテンプレートが用意されています。

- **Azure マーケットプレイスのソリューションテンプレート**：Azure マーケットプレイスで使用可能なソリューションテンプレートを使用すると、Azure ポータルを使用して Firewall Management Center Virtual を展開できます。既存のリソースグループおよびストレージアカウントを使用して（あるいは、それらを新規に作成して）、仮想アプライアンスを展開できます。ソリューションテンプレートを使用するには、「ソリューションテンプレートを使用した Azure Marketplace からの展開 （63 ページ）」を参照してください。
- **GitHub リポジトリ内の ARM テンプレート**：マーケットプレイスベースの展開の他に、GitHub リポジトリに Azure Resource Manager（ARM）テンプレートが提供され、Azure に Firewall Management Center Virtual を展開するプロセスが簡素化されます。管理対象イメージと 2 つの JSON ファイル（テンプレートファイルおよびパラメータファイル）を使用して、単一の協調操作で Firewall Management Center Virtual のすべてのリソースを展開およびプロビジョニングできます。

（注） マーケットプレイスでシスコのオファーを検索すると、アプリケーションオファーと仮想マシンオファーという、名前は似ているものの、オファーのタイプが異なる2つの異なるオファーが見つかる場合があります。

マーケットプレイス展開の場合は、アプリケーションオファーのみを使用します。

マーケットプレイスでは、VMSR（仮想マシンソフトウェア予約）プランを持つ仮想マシンオファーが表示される場合があります。これらは、特にチャネル/リセールのための特定のマルチパーティ プライベート オファー プランであり、通常の展開では無視するべきものです。

アプリケーション マーケットプレイスで利用可能なアプリケーションオファー

- Cisco Secure Firewall Management Center Virtual – BYOL
- Cisco Firepower Management Center 300 Virtual（FMCv300）

ソリューションテンプレートを使用したAzure Marketplaceからの展開

Azure Marketplace で入手できるソリューションテンプレートを使用して Azure ポータルから Firewall Management Center Virtual を展開します。次の手順は、Microsoft Azure 環境で Firewall Management Center Virtual をセットアップする手順の概略です。Azure の設定の詳細な手順については、『Azure を使ってみる』を参照してください。

Azure に Firewall Management Center Virtual を導入すると、リソース、パブリック IP アドレス、ルートテーブルなどのさまざまな設定が自動的に生成されます。導入後に、これらの設定をさらに管理できます。たとえば、アイドルタイムアウト値を、デフォルトの短いタイムアウトから変更することができます。

手順

ステップ 1 Microsoft アカウントのクレデンシャルを使用して Azure ポータル（https://portal.azure.com）にログインします。

Azure ポータルは、データセンターの場所に関係なく、現在のアカウントとサブスクリプションに関連付けられた仮想要素を表示します。

ステップ 2 [リソースの作成（Create a Resource）] をクリックします。

ステップ 3 マーケットプレイスで「Firewall Management Center」検索し、サービスを選択して、[作成（Create）] をクリックします。

ステップ 4 [基本（Basics）] で設定を行います。

a) [AzureでのFMC VM名（FMC VM name in Azure）] フィールドに、仮想マシンの名前を入力します。この名前は Azure サブスクリプション内で一意である必要があります。

注目
既存の名前を使用していないことを確認します。使用すると、展開は失敗します。

b) （オプション）ドロップダウンリストから [FMCソフトウェアバージョン（FMC Software Version）] を選択します。

デフォルトでは、使用可能な最新のバージョンに設定されています。

c) [プライマリアカウントのユーザー名（Username for primary account）] フィールドに、Azure アカウント管理者のユーザー名を入力します。

「admin」という名前は Azure で予約されており、使用できません。

注目
ここで入力したユーザー名は、Firewall Management Center Virtual 管理者アクセス用ではなく、Azure アカウント用です。このユーザー名を使用して、Firewall Management Center Virtual にログインしないでください。

d) 認証タイプとして、[パスワード（Password）] または [SSH公開キー（SSH public key）] を選択します。

[パスワード（Password）] を選択した場合は、パスワードを入力して確定します。パスワードは 12 ～ 72 文字で指定し、小文字 1 文字、大文字 1 文字、数字 1 文字、および「\」または「-」以外の特殊文字を含める必要があります。

[SSH公開キー（SSH public key）] を選択した場合は、リモートピアの RSA 公開キーを指定します。

e) Firewall Management Center Virtual の [FMC ホスト名（FMC Hostname）] を入力します。

f) [管理者パスワード（Admin Password）] を入力します。

これは、Firewall Management Center Virtual を設定するために管理者として Firewall Management Center Virtual の Web インターフェイスにログインするときに使用するパスワードです。

g) [サブスクリプションの種類（Subscription type）] を選択します。

通常は、1 つのオプションのみが表示されます。

h) 新しい [リソースグループ（Resource group）] を作成します。

Firewall Management Center Virtual は新しいリソースグループに導入する必要があります。既存のリソースグループに展開するオプションは、既存のリソースグループが空の場合にのみ機能します。

ただし、後の手順でネットワークオプションを設定する際に、Firewall Management Center Virtual を別のリソースグループ内に存在している仮想ネットワークへ接続できます。

i) 地理的な [場所（Location）] を選択します。

この展開で使用されているすべてのリソースに同じ場所を使用する必要があります。Firewall Management Center Virtual、ネットワーク、ストレージアカウントなどは、すべて同じ場所を使用する必要があります。

j) [OK] をクリックします。

ステップ 5 次に、[Cisco FMCv設定（Cisco FMCv Settings）] で初期設定を実行します。

a) 選択した [仮想マシンのサイズ（Virtual machine size）] を確認するか、[サイズ変更（Change size）] リンクをクリックして VM サイズのオプションを表示します。[選択（Select）] をクリックして確認します。

サポートされている仮想マシンのサイズのみ表示されます。

b) [ストレージアカウント（Storage account）] を設定します。既存のストレージアカウントを使用するほか、新規に作成することもできます。

- ストレージアカウントの [名前（Name）] を入力し、[OK] をクリックします。ストレージアカウント名には、小文字と数字のみを使用できます。特殊文字を含めることはできません
- このリリースの時点では、Firewall Management Center Virtual は汎用的な標準のパフォーマンスストレージのみをサポートしています。

c) [パブリックIPアドレス（Public IP address）] を設定します。ユーザーは既存の IP を使用することも、新規の IP を作成することもできます。

- [新規作成（Create new）] をクリックして、新しいパブリック IP アドレスを作成します。[名前（Name）] フィールドに IP アドレスのラベルを入力し、[SKU] オプションとして [標準（Standard）] を選択し、[OK] をクリックします。

  （注）
  このステップで動的/静的のいずれを選択しても、Azure は動的なパブリック IP アドレスを作成します。VM を停止させて再起動すると、パブリック IP が変わることがあります。固定 IP アドレスを優先する場合は、展開後にパブリック IP を編集して、ダイナミックアドレスからスタティックアドレスに変更します。

- パブリック IP アドレスを Firewall Management Center Virtual に割り当てない場合は、[なし（NONE）] を選択できます。パブリック IP アドレスがない場合、Firewall Management Center Virtual へのすべての通信は Azure 仮想ネットワーク内から発信する必要があります。

d) パブリック IP のラベルと一致する [DNSラベル（DNS label）] を追加します。

完全修飾ドメイン名は、DNS ラベルと Azure URL の組み合わせで、*<dnslabel>.<location>.cloudapp.azure.com* の形式になります。

e) 既存の [仮想ネットワーク（Virtual network）] を選択するか、新しい仮想ネットワークを作成し、[OK] をクリックします。

f) Firewall Management Center Virtual の管理サブネットを設定します。

[管理サブネット名（Management subnet name）] を定義し、[管理サブネットのプレフィックス（Management subnet prefix）] を確認します。推奨されるサブネット名は「management」です。

g) [パブリックインバウンドポート（mgmt.interface）（Public inbound ports (mgmt.interface)）] の入力を指定して、ポートをパブリック用に開くかどうかを示します。デフォルトでは、[なし（None）] が選択されています。

- Azure のデフォルトのセキュリティルールを使用してネットワーク セキュリティ グループを作成し、管理インターフェイスに接続するには、[なし（None）] をクリックします。このオプションを選択すると、同じ仮想ネットワーク内の送信元からのトラフィックと Azure ロードバランサからのトラフィックが許可されます。
- インターネットでアクセスするために開くインバウンドポートを表示および選択するには、[選択したポートを許可（Allow selected ports）] をクリックします。[インバウンドポートの選択（Select

Inbound Ports）] ドロップダウンリストから、次のいずれかのポートを選択します。デフォルトでは、[HTTPS] が選択されています。

- SSH（22）
- SFTunnel（8305）
- HTTPS（443）

（注）
[パブリックIP（Public IP）] は、[選択したポートを許可（Allow selected ports）] または [パブリック着信ポート（Public inbound ports）] の値には考慮されません。

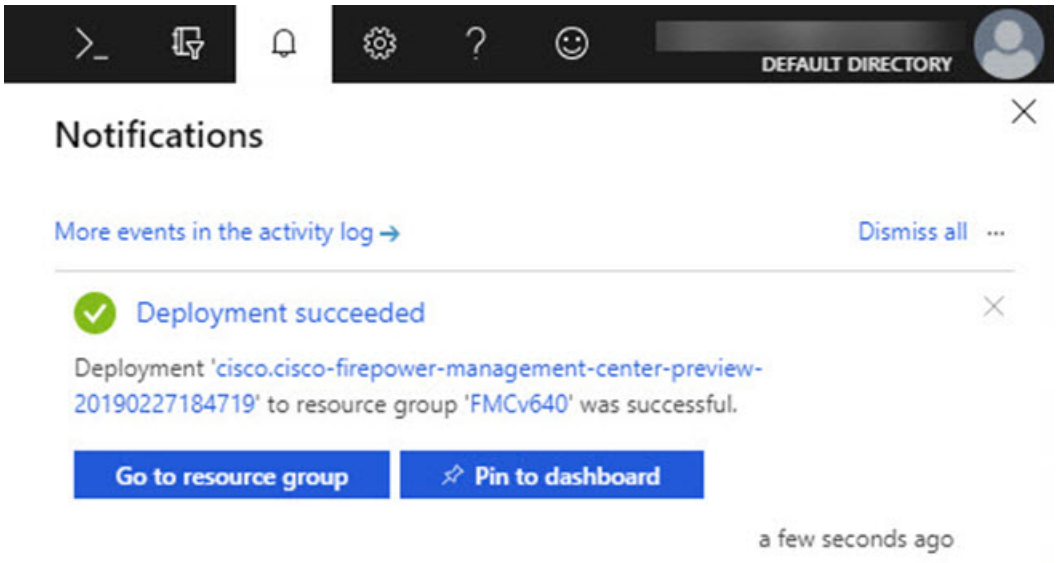
h) [OK] をクリックします。

ステップ 6 構成サマリを確認し、[OK] をクリックします。

ステップ 7 利用条件を確認し、[作成（Create）] をクリックします。

ステップ 8 ポータルの上部にある [通知（Notifications）]（ベルアイコン）を選択して、展開のステータスを表示します。

図 *1 : Azure* 通知



ここから、展開をクリックして詳細を表示したり、展開が成功した後にリソースグループに移動することができます。Firewall Management Center Virtual が使用可能になるまでの合計時間は約 30 分です。導入時間は Azure によって異なります。Firewall Management Center Virtual VM が実行されていることが Azure から報告されるまで待機します。

ステップ 9 （オプション）Azure には、[起動時診断（Boot diagnostics）] や [シリアルコンソール（Serial console）] など、VMの状態をモニターするのに役立つ多数のツールが用意されています。これらのツールを使用して、起動時に仮想マシンの状態を確認できます。

a) 左側のメニューで、[仮想マシン（Virtual machines）] を選択します。

b) リストから Firewall Management Center Virtual VM を選択します。VM の概要ページが開きます。

c) [サポート+トラブルシューティング（Support + troubleshooting）] セクションまで下にスクロールし、[起動時診断（Boot diagnostics）] または [シリアルコンソール（Serial console）] を選択します。起動時診断の [スクリーンショット（Screenshot）] と [シリアルログ（Serial log）] またはテキストベースの [シリアルコンソール（Serial console）] のいずれかを示す新しいペインが開き、接続が開始されます。

起動時診断またはシリアルコンソールのいずれかにログインプロンプトが表示されれば、Firewall Management Center Virtual の Web インターフェイスが準備できていることを確認できます。

例：

```
Cisco Secure Firewall Management Center for Azure v7.6.0 (build 44)
FMCv76East login:
```

次のタスク

- Firewall Management Center Virtual の展開が成功したことを確認します。Azure ダッシュボードの [リソースグループ（Resource Groups）] には、新しい Firewall Management Center Virtual VM と、すべての関連リソース（ストレージ、ネットワーク、ルートテーブルなど）がリストされます。

VHD およびリソーステンプレートを使用した Azure からの展開

シスコが提供する圧縮 VHD イメージを使用して、独自のカスタム Firewall Management Center Virtual イメージを作成できます。VHD イメージを使用して展開するには、Azure ストレージアカウントに VHD イメージをアップロードする必要があります。次に、アップロードしたディスクイメージおよび Azure Resource Manager テンプレートを使用して、管理対象イメージを作成できます。Azure テンプレートは、リソースの説明とパラメータの定義が含まれている JSON ファイルです。

始める前に

- Firewall Management Center Virtual テンプレートの展開には、JSON テンプレートおよび対応する JSON パラメータファイルが必要です。これらのファイルは、GitHub リポジトリからダウンロードできます。
- この手順では、Azure に Linux VM が存在している必要があります。一時的な Linux VM（Ubuntu 16.04 など）を使用して、Azure に圧縮 VHD イメージをアップロードすることを推奨します。このイメージを解凍するには、約 50 GB のストレージが必要です。また、Azure の Linux VM から Azure ストレージへのアップロード時間が短縮されます。

  VM を作成する必要がある場合は、次のいずれかの方法を使用します。

  - Azure CLI による Linux 仮想マシンの作成
  - Azure ポータルによる Linux 仮想マシンの作成

- Azure サブスクリプションには、Firewall Management Center Virtual を展開する場所で使用可能なストレージアカウントが必要です。

手順

ステップ 1 シスコ ダウンロード ソフトウェア ページから Firewall Management Center Virtual 圧縮 VHD イメージをダウンロードします。

a) [製品（Products）] > [セキュリティ（Security）] > [ファイアウォール（Firewalls）] > ファイアウォール管理（Cisco Secure Firewall Threat Defense Virtual）] > [Cisco Secure Firewall Management Center Virtual] の順に移動します。

b) [Firepower Management Centerソフトウェア（Firepower Management Center Software）] をクリックします。

手順に従ってイメージをダウンロードしてください。

例：Cisco_Secure_FW_Mgmt_Center_Virtual_Azure-7.3.0-69.vhd.bz2

ステップ 2 Azure の Linux VM に圧縮 VHD イメージをコピーします。

Azure との間でファイルをやり取りするために使用できるオプションが数多くあります。この例では、SCP（セキュアコピー）を示します。

```
# scp /username@remotehost.com/dir/Cisco_Secure_FW_Mgmt_Center_Virtual_Azure-7.3.0-69.vhd.bz2
<linux-ip>
```

ステップ 3 Azure の Linux VM にログインし、圧縮 VHD イメージをコピーしたディレクトリに移動します。

ステップ 4 Firewall Management Center Virtual VHD イメージを解凍します。

ファイルを解凍または圧縮解除するために使用できるオプションが数多くあります。この例では Bzip2 ユーティリティを示しますが、Windows ベースのユーティリティも正常に機能します。

```
# bunzip2 Cisco_Secure_FW_Mgmt_Center_Virtual_Azure-7.3.0-69.vhd.bz2
```

ステップ 5 Azure ストレージアカウントのコンテナに VHD をアップロードします。既存のストレージアカウントを使用するほか、新規に作成することもできます。ストレージアカウント名には、小文字と数字のみを使用できます。

ストレージアカウントに VHD をアップロードするために使用できるオプションが数多くあります。AzCopy、Azure Storage Copy Blob API、Azure Storage Explorer、Azure CLI、Azure ポータルなどです。Firewall Management Center Virtual VHD ほどの容量があるファイルには、Azure ポータルを使用しないことを推奨します。

次の例は、Azure CLI を使用した構文を示しています。

```
azure storage blob upload \
       --file <unzipped vhd> \
       --account-name <azure storage account> \
       --account-key yX7txxxxxxxx1dnQ== \
       --container <container> \
       --blob <desired vhd name in azure> \
       --blobtype page
```

ステップ 6 VHD から管理対象イメージを作成します。

a) Azure ポータルで、[イメージ（Images）] を選択します。

b) [追加（Add）] をクリックして、新しいイメージを作成します。

c) 次の情報を入力します。

- [サブスクリプション（Subscription）]：ドロップダウンリストからサブスクリプションを選択します。
- [リソースグループ（Resource group）]：既存のリソースグループを選択するか、新しいリソースグループを作成します。
- [名前（Name）]：管理対象イメージのユーザー定義の名前を入力します。
- [リージョン（Region）]：VM が展開されるリージョンを選択します。
- [OSタイプ（OS type）]：OS タイプとして [Linux] を選択します。
- **[VMの世代（VM Generation）]**

  BIOS ブートモードの場合は **[第1世代（Generation 1）]** を選択します。

  UEFI ブートモードの場合は **[第2世代（Generation 2）]** を選択します。
- [ストレージブロブ（Storage blob）]：ストレージアカウントを参照して、アップロードした VHD を選択します。
- [アカウントタイプ（Account type）]：要件に応じて、ドロップダウンリストから [Standard HDD]、[Standard SSD]、または [Premium SSD] を選択します。

  このイメージの展開用に計画している VM サイズを選択する場合は、選択したアカウントタイプがその VM サイズでサポートされていることを確認します。
- [ホストキャッシング（Host caching）]：ドロップダウンリストから [読み取り/書き込み（Read/write）] を選択します。
- [データディスク（Data disks）]：デフォルトのままにして、データディスクを追加しないでください。

d) [作成（Create）] をクリックします。

「イメージが正常に作成されました（Successfully created image）」というメッセージが [通知（Notifications）] タブの下に表示されるまで待ちます。

（注）
管理対象イメージが作成されたら、アップロードした VHD とアップロード ストレージ アカウントを削除できます。

ステップ 7 新規に作成した管理対象イメージのリソース ID を取得します。

Azure の内部では、あらゆるリソースがリソース ID に関連付けられています。リソース ID は、この管理対象イメージから新しい Firewall Management Center Virtual インスタンスを展開するときに必要になります。

a) Azure ポータルで、[イメージ（Images）] を選択します。
b) 前のステップで作成した管理対象イメージを選択します。
c) [概要（Overview）] をクリックして、イメージのプロパティを表示します。
d) クリップボードに**リソース ID** をコピーします。

リソース ID は、次の形式を取ります。

/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>

ステップ 8 管理対象イメージおよびリソーステンプレートを使用して、Firewall Management Center Virtual インスタンスを構築します。

a) Azure GUIで、**カスタムデプロイメント**を検索します。
b) **[テンプレートを選択（Select a template）]**の下で、**[エディタで独自のテンプレートを構築する（Build your own template in the editor）]** をクリックします。

カスタマイズできる空白のテンプレートが作成されます。テンプレートファイルについては、「GitHub 」を参照してください。

c) カスタマイズした JSON テンプレートコードをウィンドウに貼り付け、[保存（Save）] をクリックします。
d) ドロップダウンリストから [サブスクリプション（Subscription）] を選択します。
e) 既存の [リソースグループ（Resource group）]を選択するか、新しいリソースグループを作成します。
f) ドロップダウンリストから **[リージョン（Region）]** を選択します。
g) 前のステップの管理対象イメージの **[リソースID（Resource ID）]** を **[VMイメージID（Vm Image Id）]** フィールドに貼り付けます。
h) 診断インターフェイスなしで Threat Defense Virtual を展開するには、[カスタムデータ（Custom Data）] フィールドにキーと値のペア **Diagnostic: OFF** を含む Day-0 構成スクリプトを入力します。次に、Day 0 構成スクリプトの例を示します。

```
{
"AdminPassword": "E28@2OiUrhx!",
"Hostname": "ciscothreatdefensevirtual",
"FirewallMode": "routed",
"ManageLocally": "No",
"Diagnostic": "OFF"
}
```

（注）
キーと値のペア "Diagnostic": "ON/OFF" では、大文字と小文字が区別されます。

新規デプロイメントに使用される ARM テンプレートの [カスタムデータ（Custom Data）] フィールドのスクリプトも変更できます。

ステップ 9 [カスタム展開（Custom deployment）] ページの最上部にある [パラメータの編集（Edit parameters）] をクリックします。カスタマイズできるパラメータテンプレートが作成されます。

a) [ファイルのロード（Load file）] をクリックし、カスタマイズした Firewall Management Center Virtual パラメータファイルを参照します。テンプレートパラメータについては、「GitHub」を参照してください。

b) カスタマイズした JSON パラメータコードをウィンドウに貼り付け、[保存（Save）] をクリックします。

ステップ 10 カスタム展開の詳細を確認します。[基本（Basics）] と [設定（Settings）] の情報（[リソースID（Resource ID）] など）が、想定した展開設定に一致することを確認します。

ステップ 11 利用規約を確認し、[上記の利用規約に同意します（I agree to the terms and conditions stated above）] チェックボックスをオンにします。

ステップ 12 [購入（Purchase）] をクリックし、管理対象イメージおよびカスタムテンプレートを使用して Firewall Management Center Virtual インスタンスを展開します。

テンプレートファイルとパラメータファイルに競合がなければ、展開が正常に完了しているはずです。

管理対象イメージは、同じサブスクリプションおよび地域内の複数の展開に使用できます。

次のタスク

- Azure で Firewall Management Center Virtual の IP 設定を更新します。

制限付きの Azure プライベート マーケットプレイス環境での Azure マーケットプレイスオファーの展開

これは、Azure プライベート マーケットプレイスのユーザーにのみ適用されます。Azure プライベート マーケットプレイスを使用している場合は、それぞれのプライベート マーケットプレイスで、ユーザーに対してアプリケーション オファーおよび必要な仮想マシンオファー（非表示）の両方が有効になっていることを確認します。

仮想マシンのオファーとプラン（非表示）：

- パブリッシャー ID：**cisco**
- Cisco Secure Firewall Management Center Virtual VM オファー（両方の Cisco Secure Firewall Management Center Virtual アプリケーションオファーに使用）
  - オファー ID：**cisco-fmcv**
  - BYOL プラン ID：**fmcv-azure-byol**
- Cisco Firepower Management Center 300 Virtual
  - オファー ID：**cisco-fmcv300**
  - BYOL プラン ID：**fmcv300-azure-byol**

ユーザーがマーケットプレイスから表示されているアプリケーションオファーを展開すると、VM オファープランから対応するイメージが参照され、展開されます。

したがって、展開を機能させるには、アプリケーションと VM の両方のオファーが Azure テナント/サブスクリプションのプライベート マーケットプレイスで有効になっていて、利用できる必要があります。

プライベート マーケットプレイスでこれらのアプリケーションオファーと VM オファーを有効にする方法については、Azure のドキュメントを参照してください。

- プライベート Azure マーケットプレイスを使用してガバメントとコントロールを実施する [英語]
- プライベート マーケットプレイスにオファーを追加する [英語]
- Set-AzMarketplacePrivateStoreOffer [英語]

アプリケーションオファーはマーケットプレイスに表示されるため、Azure UI を介して簡単に有効にできます。

プライベート マーケットプレイスで非表示の仮想マシンオファーを有効にするには、CLI コマンドの使用が必要となる場合があります（このドキュメントの作成時点では、CLI の方法のみが可能です）。

サンプルコマンド

Cisco Secure Firewall Management Center Virtual BYOL プランは、次に示すようなサンプルコマンドを使用して有効にできます：

```
$Params = @{
  privateStoreId = '<private-store-id>'
  offerId = '<publisher-id>.<vm-offer-id>'
  SpecificPlanIdsLimitation =@('<plan-id-under-vm-offer>')
}
Set-AzMarketplacePrivateStoreOffer @Params

$Params = @{
  privateStoreId = '<private-store-id>'
  offerId = 'cisco.cisco-fmcv'
  SpecificPlanIdsLimitation =@('fmcv-azure-byol')
}
Set-AzMarketplacePrivateStoreOffer @Params
```

（注） サンプルコマンドは参考用です。詳細については、Azure のドキュメントを確認してください。

参照エラーメッセージ

```
{
  "code": "MarketplacePurchaseEligibilityFailed",
  "details": [
    {
      "code": "BadRequest",
      "message": "Offer with PublisherId: 'cisco', OfferId: 'cisco-XXXX' cannot be
purchased due to validation errors. For more information see details.
Correlation Id: 'XXXXX`
This plan is not available for purchase because it needs to be added to your tenant's
Private Marketplace. Contact your admin to request adding the plan.
Link to plan: <URL>.
Plan: '<PLAN NAME>'(planId=<VM-OFFER-PLAN-ID>),
```

```
Offer: <OFFER_NAME>, Publisher: 'Cisco Systems, Inc.'(publisherId='cisco').
…
…
    }
  ],
  "message": "Marketplace purchase eligibilty check returned errors. See inner errors
for details. "
}
```

マーケットプレイスオファーの展開中には、上記のエラーが発生することがあります。これを解決するには、アプリケーションと VM の両方のオファーを Azure テナント/サブスクリプションで有効にし、利用可能にする必要があります。

Azure での IPv6 サポート対象 Secure Firewall Management Center Virtual の展開

この章では、Azure ポータルから IPv6 サポート対象の Firewall Management Center Virtual を展開する方法について説明します。

Azure での IPv6 をサポートする展開について

Firewall Management Center Virtual 製品は、7.3 以降、IPv4 と IPv6 の両方をサポートします。Azure では、仮想ネットワークを作成または使用する Marketplace サービスから Firewall Management Center Virtual を直接展開できますが、現在、Azure の制限により、Marketplace アプリケーション製品は、IPv4 ベースの VNet/サブネットのみを使用または作成するように制限されています。IPv6 アドレスを既存の VNet に手動で設定することはできますが、IPv6 サブネットで設定された VNet に新しい Firewall Management Center Virtual インスタンスを追加することはできません。Azure では、Marketplace を介してリソースを展開する方法以外の代替アプローチを使用してサードパーティのリソースを展開するように、一定の制限を課しています。

シスコは現在、IPv6 アドレッシングをサポートするために Firewall Management Center Virtual を展開する 2 つの方法を提供しています。

次の 2 つの異なるカスタム IPv6 テンプレートが提供されます。

- [カスタムIPv6テンプレート（ARMテンプレート）（Custom IPv6 template (ARM template)）]：Azure 上の Marketplace イメージを内部的に参照する Azure Resource Manager（ARM）テンプレートを使用して、IPv6 設定の Firewall Management Center Virtual を展開するために提供されます。このテンプレートには、IPv6 サポート対象の Firewall Management Center Virtual を展開するように設定可能なリソースとパラメータ定義を含む JSON ファイルが含まれています。このテンプレートを使用するには、「Marketplace イメージ参照を含むカスタム IPv6 テンプレートを使用した Azure からの展開 （75 ページ）」を参照してください。

  プログラムによる展開は、PowerShell、Azure CLI、ARM テンプレート、または API を介してカスタムテンプレートを展開するために、Azure Marketplace 上の VM イメージへのアクセスを許可するプロセスです。VM へのアクセスを許可せずに、これらのカスタムテン

プレートを VM に展開することは制限されています。このようなカスタムテンプレートを VM に展開しようとすると、次のエラーメッセージが表示されます。

Legal terms have not been accepted for this item on this subscription. To accept legal terms ….and configure programmatic deployment for the Marketplace item …..

次のいずれかの方法を使用して、Azure でのプログラムによる展開を有効にして、Marketplace イメージを参照するカスタム IPv6（ARM）テンプレートを展開できます。

- **Azure ポータル**：カスタム IPv6 テンプレート（ARM テンプレート）を展開するために、Azure Marketplace で利用可能な Firewall Management Center Virtual の提供に対応するプログラムによる展開オプションを有効にします。
- **Azure CLI**：CLI コマンドを実行して、カスタム IPv6（ARM テンプレート）を展開するためのプログラムによる展開を有効にします。

- **カスタム VHD イメージと IPv6 テンプレート（ARM テンプレート）**：Azure で VHD イメージと ARM テンプレートを使用して管理対象イメージを作成します。このプロセスは、VHD とリソーステンプレートを使用した Firewall Management Center Virtual の展開に似ています。このテンプレートは、展開中に管理対象イメージを参照し、IPv6 サポート対象の Firewall Management Center Virtual を展開するために Azure にアップロードして設定できる ARM テンプレートを使用します。VHD およびカスタム IPv6 テンプレートを使用した Azure からの展開 （81 ページ）を参照してください。

カスタム IPv6 テンプレートを使用した Marketplace イメージまたは VHD イメージを参照して、カスタム IPv6 テンプレート（ARM テンプレート）を使用して Firewall Management Center Virtual を展開するプロセス。

Firewall Management Center Virtual の展開に含まれる手順は次のとおりです。

表 *10*：

手順	プロセス
1	IPv6 サポート対象の Firewall Management Center Virtual の展開を計画している Azure で、Linux VM を作成します。
2	Marketplace イメージ参照でカスタム IPv6 テンプレートを使用して Firewall Management Center Virtual を展開する場合に**のみ**、Azure ポータルまたは Azure CLI でプログラムによる展開オプションを有効にします。
3	展開のタイプに応じて、次のカスタムテンプレートをダウンロードします。 • Azure Marketplace 参照イメージを使用したカスタム IPv6 テンプレート。 カスタム IPv6（ARM）テンプレートを使用した VHD イメージ。

4	カスタム IPv6（ARM）テンプレートの IPv6 パラメータを更新します。 （注） Marketplaceイメージバージョンに相当するソフトウェアイメージバージョンのパラメータ値は、Marketplace イメージ参照でカスタム IPv6 テンプレートを使用して Firewall Management Center Virtual を展開する場合にのみ必要です。ソフトウェアバージョンの詳細を取得するには、コマンドを実行する必要があります。
5	Azure ポータルまたは Azure CLI を使用して ARM テンプレートを展開します。

Marketplaceイメージ参照を含むカスタムIPv6テンプレートを使用した Azure からの展開

Marketplaceイメージを参照し、カスタムIPv6テンプレート（ARMテンプレート）を使用して Firewall Management Center Virtual を展開するプロセス。

手順

ステップ 1 Azure ポータルにログインします。

Azure ポータルは、データセンターの場所に関係なく、現在のアカウントとサブスクリプションに関連付けられた仮想要素を表示します。

ステップ 2 次の方法で、Azure ポータルまたは Azure CLI を使用してプログラムによる展開を有効にします。

Azure ポータルでこのオプションを有効にするには、次の手順を実行します。

a) [Azure（サービス）（Azure Services）] で [サブスクリプション（Subscriptions）] をクリックして、サブスクリプション ブレード ページを表示します。
b) 左側のペインで、[設定（Settings）] オプションの [プラグラムによる展開（Programmatic Deployment）] をクリックします。

VM に展開されたすべてのタイプのリソースが、関連するサブスクリプション製品とともに表示されます。

c) [ステータス（Status）] 列で、カスタム IPv6 テンプレートのプログラムによる展開のために取得する Firewall Management Center Virtual 製品に対応する [有効化（Enable）] ボタンをクリックします。

または

Azure CLI を使用してこのオプションを有効にするには、次の手順を実行します。

a) Linux VM に移動します。
b) 次の CLI コマンドを実行して、カスタム IPv6（ARM テンプレート）を展開するためのプログラムによる展開を有効にします。

コマンドの実行時に、イメージのサブスクリプションごとに1回だけ規約に同意する必要があります。

 # Accept terms

az vm image terms accept -p <publisher> -f <offer> --plan <SKU/plan>

 # Review that terms were accepted (i.e., accepted=true)

az vm image terms show -p <publisher> -f <offer> --plan <SKU/plan>

それぞれの説明は次のとおりです。

- **<publisher>**：'cisco'。
- **<offer>**：'cisco-fmcv'
- **<sku/plan>**：'fmcv-azure-byol'

以下は、BYOL サブスクリプションプランで展開するためのプログラムによる Firewall Management Center Virtual の展開を有効にするコマンドスクリプトの例です。

- **az vm image terms show -p cisco -f cisco-ftdv --plan fmcv-azure-byol**

ステップ 3 次のコマンドを実行して、Marketplaceイメージバージョンに相当するソフトウェアバージョンの詳細を取得します。

az vm image list --all -p <publisher> -f <offer> -s <sku>

それぞれの説明は次のとおりです。

- **<publisher>**：'cisco'。
- **<offer>**：'cisco-fmcv'
- **<sku>**：'fmcv-azure-byol'

以下は、 Firewall Management Center Virtual 用の Marketplace イメージバージョンに相当するソフトウェアバージョンの詳細を取得するコマンドスクリプトの例です。

az vm image list --all -p cisco -f cisco-ftdv -s fmcv-azure-byol

ステップ 4 表示される使用可能なMarketplaceイメージバージョンのリストから、いずれかのFirewall Management Center Virtual バージョンを選択します。

Firewall Management Center Virtual の IPv6 サポート展開の場合は、 Firewall Management Center Virtual バージョンを 73* 以上として選択する必要があります。

ステップ 5 Cisco GitHub リポジトリから Marketplace カスタム IPv6 テンプレート（ARM テンプレート）をダウンロードします。

ステップ 6 パラメータ テンプレート ファイル（JSON）で展開値を指定して、パラメータファイルを準備します。

次の表で、 Firewall Management Center Virtual カスタム展開用のカスタム IPv6 テンプレートパラメータに入力する必要がある展開値について説明します。

パラメータ名	許可される値/タイプの例	説明
vmName	cisco-fmcv	Azure で Firewall Management Center Virtual VM に名前を付けます。
softwareVersion	730.33.0	Marketplace イメージバージョンのソフトウェアバージョン。
billingType	BYOL	ライセンス方式は BYOL または PAYG です。 BYOL ライセンスは PAYG と比較して費用対効果が高いため、BYOL サブスクライブ展開を選択することをお勧めします。
adminUsername	hjohn	Firewall Management Center Virtual にログインするユーザー名。 管理者に割り当てられる予約名「admin」は使用できません。
adminPassword	E28@4OiUrhx!	管理者アカウントのパスワード。 パスワードの組み合わせは、12 ～ 72 文字の英数字である必要があります。小文字、大文字、数字、特殊文字を組み合わせたパスワードにする必要があります。
vmStorageAccount	hjohnvmsa	Azure ストレージアカウント。既存のストレージアカウントを使用するほか、新規に作成することもできます。ストレージアカウント名は、3 ～ 24 文字の長さにする必要があります。小文字と数字のみを組み合わせたパスワードにする必要があります。
availabilityZone	0	展開の可用性ゾーンを指定すると、指定した可用性ゾーンにパブリック IP と仮想マシンが作成されます。 可用性ゾーンの設定が必要ない場合は、「**0**」に設定します。選択した地域が可用性ゾーンをサポートしており、入力された値が正しいことを確認してください。（値は 0 ～ 3 の整数である必要があります）。
ipAllocationMethod	動的	Azure からの IP 割り当て。静的：手動、動的：DHCP

パラメータ名	許可される値/タイプの例	説明
mgmtSubnetName	mgmt	mgmt インターフェイスの Management Center IP（例：192.168.0.10）
mgmtSubnetIP	10.4.1.15	mgmt インターフェイスの FMC IP（例：192.168.0.10）
mgmtSubnetIPv6	ace:cab:deca:dddd::c3	mgmtインターフェイスのFMC IPv6（例：ace:cab:deca:dddd::6）
customData	{\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\": \"cisco-mcv\", \"IPv6Mode\"	第 0 日構成で Firewall Management Center Virtual に表示されるフィールド。デフォルトでは、設定対象となる次の3つのキーと値のペアがあります。 • 「admin」ユーザーパスワード • Firewall Management Center Virtualホスト名 • 管理用の Firewall Management Center Virtual ホスト名または CSF-DM。 「ManageLocally : yes」：これにより、CSF-DM が Firewall Threat Defense Virtual マネージャとして使用されるように設定されます。 Firewall Management Center Virtual を Firewall Threat Defense Virtual マネージャとして設定し、Firewall Management Center Virtual で同じ設定をするのに必要なフィールドに入力することもできます。
virtualNetworkResourceGroup	cisco-mcv-rg	仮想ネットワークを含むリソースグループの名前。virtualNetworkNewOrExisting が new の場合、この値はテンプレートの展開用に選択されたリソースグループと同じである必要があります。
virtualNetworkName	cisco-mcv-vnet	仮想ネットワークの名前。
virtualNetworkNewOrExisting	new	このパラメータによって、新しい仮想ネットワークを作成するか、既存の仮想ネットワークを使用するかが決まります。
virtualNetworkAddressPrefixes	10.151.0.0/16	これは仮想ネットワークの IPv4 アドレスプレフィックスで、

パラメータ名	許可される値/タイプの例	説明
		「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	これは仮想ネットワークの IPv6 アドレスプレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet1Name	mgmt	管理サブネット名。
Subnet1Prefix	10.151.1.0/24	これは管理サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	これは管理サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet1StartAddress	10.151.1.4	管理インターフェイスの IPv4 アドレス。
subnet1v6StartAddress	ace:cab:deca:1111::6	管理インターフェイスの IPv6 アドレス。
Subnet2Name	diag	データインターフェイス 1 のサブネット名。
Subnet2Prefix	10.151.2.0/24	これはデータインターフェイス 1 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	これはデータインターフェイス 1 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet2StartAddress	10.151.2.4	データインターフェイス 1 の IPv4 アドレス。
subnet2v6StartAddress	ace:cab:deca:2222::6	データインターフェイス 1 の IPv6 アドレス。
Subnet3Name	inside	データインターフェイス 2 のサブネット名。

パラメータ名	許可される値/タイプの例	説明
Subnet3Prefix	10.151.3.0/24	これはデータインターフェイス2サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	これはデータインターフェイス2サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet3StartAddress	10.151.3.4	データインターフェイス 2 の IPv4 アドレス。
subnet3v6StartAddress	ace:cab:deca:3333::6	データインターフェイス 2 の IPv6 アドレス。
Subnet4Name	outside	データインターフェイス 3 のサブネット名。
Subnet4Prefix	10.151.4.0/24	これはデータインターフェイス3サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	これはデータインターフェイス3サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet4StartAddress	10.151.4.4	データインターフェイス 3 の IPv4 アドレス。
subnet4v6StartAddress	ace:cab:deca:4444::6	データインターフェイス 3 の IPv6 アドレス。
vmSize	Standard_D4_v2	Firewall Management Center Virtual VM のサイズ。。Standard_D4_v2 がデフォルトです。

ステップ 7 ARM テンプレートを使用して、Azure ポータルまたは Azure CLI で Firewall Management Center Virtual ファイアウォールを展開します。Azure での ARM テンプレートの展開については、次の Azure ドキュメントを参照してください。

- 『Create and deploy ARM templates by using the Azure portal』

- 『Deploy a local ARM template through CLI』

次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャーを有効にする（Enable Local Manager）] で [いいえ（No）] を選択した場合は、Cisco Secure Firewall Management Center を使用して Firewall Threat Defense Virtual を管理します。「Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Management Center」を参照してください。
- [ローカルマネージャーを有効にする（Enable Local Manager）] で [はい（Yes）] を選択した場合は、Cisco Secure Firewall Device Manager を使用して を管理します。「Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall device manager」を参照してください。

  管理オプションを選択する方法の概要については、「How to Manage Your Secure Firewall Threat Defense Virtual Device」を参照してください。

Management Center の仮想展開が成功したことを確認します。Azure ダッシュボードの [リソースグループ（Resource Groups）] には、新しい Management Center 仮想 VM と、すべての関連リソース（ストレージ、ネットワーク、ルートテーブルなど）が一覧表示されます。

VHD およびカスタム IPv6 テンプレートを使用した Azure からの展開

シスコが提供する圧縮 VHD イメージを使用して、独自のカスタム Firewall Management Center Virtual イメージを作成できます。このプロセスは、VHD とリソーステンプレートを使用した Firewall Management Center Virtual の展開に似ています。

始める前に

- Github の VHD および ARM の最新テンプレートを使用した Firewall Management Center Virtual の展開には、JSON テンプレートおよび対応する JSON パラメータファイルが必要です。ここでは、テンプレートとパラメータファイルの作成方法を確認できます。
- この手順では、Azure に Linux VM が存在している必要があります。一時的な Linux VM（Ubuntu 16.04 など）を使用して、Azure に圧縮 VHD イメージをアップロードすることをお勧めします。このイメージを解凍するには、約 50 GB のストレージが必要です。また、Azure の Linux VM から Azure ストレージへのアップロード時間が短くなります。

  VM を作成する必要がある場合は、次のいずれかの方法を使用します。

  - Azure CLI による Linux 仮想マシンの作成

- Azure ポータルによる Linux 仮想マシンの作成

- Azure サブスクリプションには、 Firewall Management Center Virtual を展開する場所で使用可能なストレージアカウントが必要です。

手順

ステップ 1 シスコ ダウンロード ソフトウェア ページから Firewall Management Center Virtual 圧縮 VHD イメージ（*.bz2）をダウンロードします。

a) [製品（Products）] > [セキュリティ（Security）] > [ファイアウォール（Firewalls）] > ファイアウォール管理（Cisco Secure Firewall Threat Defense Virtual）] > [Cisco Secure Firewall Management Center Virtual] の順に移動します。

b) [Firepower Management Centerソフトウェア（Firepower Management Center Software）] をクリックします。

手順に従ってイメージをダウンロードしてください。

Cisco_Secure_Firewall_Threat_Defense_Virtual-X.X.X-xxx.vhd.bz2

例：Cisco_Secure_FW_Mgmt_Center_Virtual_Azure-7.3.0-69.vhd.bz2

ステップ 2 「VHD およびリソーステンプレートを使用した Azure からの展開」で示されている展開手順を実行します。

ステップ 3 [カスタム展開（Custom deployment）] ページの最上部にある [パラメータの編集（Edit parameters）] をクリックします。カスタマイズできるパラメータテンプレートが作成されます。

a) [ファイルのロード（Load file）] をクリックし、カスタマイズした Firewall Management Center Virtual パラメータファイルを参照します。VHD およびカスタム IPv6（ARM）テンプレートを使用した Azure への Firewall Management Center Virtual の展開例は、Github を参照してください。ここでは、テンプレートとパラメータファイルの作成方法を確認できます。

b) カスタマイズした JSON パラメータコードをウィンドウに貼り付け、[保存（Save）] をクリックします。

次の表で、 Firewall Management Center Virtual 展開用のカスタム IPv6 テンプレートパラメータに入力する必要がある展開値について説明します。

パラメータ名	許可される値/タイプの例	説明
vmName	cisco-fmcv	Azure で Firewall Management Center Virtual VM に名前を付けます。
vmImageId	/subscriptions/{subscription-id}/resourceGroups/{resource-group-name}/providers/Microsoft.Compute/images/{image-name}	展開に使用されるイメージの ID。Azure の内部では、あらゆるリソースがリソース ID に関連付けられています。

パラメータ名	許可される値/タイプの例	説明
adminUsername	hjohn	Firewall Management Center Virtual にログインするユーザー名。 管理者に割り当てられる予約名「admin」は使用できません。
adminPassword	E28@4OiUrhx!	管理者アカウントのパスワード。 パスワードの組み合わせは、12 ～ 72 文字の英数字である必要があります。小文字、大文字、数字、特殊文字を組み合わせたパスワードにする必要があります。
vmStorageAccount	hjohnvmsa	Azure ストレージアカウント。既存のストレージアカウントを使用するほか、新規に作成することもできます。ストレージアカウント名は、3 ～ 24 文字の長さにする必要があります。小文字と数字のみを組み合わせたパスワードにする必要があります。
availabilityZone	0	展開の可用性ゾーンを指定すると、指定した可用性ゾーンにパブリック IP と仮想マシンが作成されます。 可用性ゾーンの設定が必要ない場合は、「**0**」に設定します。選択した地域が可用性ゾーンをサポートしており、入力された値が正しいことを確認してください。（値は 0 ～ 3 の整数である必要があります）。
customData	`{\"AdminPassword\": \"E28@4OiUrhx\",\"Hostname\": \"cisco-mcv\", \"IPv6Mode\": \"DHCP\"}`	第 0 日構成で Firewall Management Center Virtual に表示されるフィールド。デフォルトでは、設定対象となる次の 3 つのキーと値のペアがあります。 • 「admin」ユーザーパスワード • CSF-MCv ホスト名 • 管理用の CSF-MCv ホスト名または CSF-DM。

パラメータ名	許可される値/タイプの例	説明
		「ManageLocally : yes」：これにより、CSF-DM が Firewall Threat Defense Virtual マネージャとして使用されるように設定されます。 CSF-MCv を Firewall Threat Defense Virtual マネージャとして設定し、CSF-MCv で同じ設定をするのに必要なフィールドに入力することもできます。
virtualNetworkResourceGroup	cisco-fmcv	仮想ネットワークを含むリソースグループの名前。virtualNetworkNewOrExisting が new の場合、この値はテンプレートの展開用に選択されたリソースグループと同じである必要があります。
virtualNetworkName	cisco-mcv-vnet	仮想ネットワークの名前。
ipAllocationMethod	動的	Azure からの IP 割り当て。静的：手動、動的：DHCP
mgmtSubnetName	mgmt	mgmt インターフェイスの Management Center IP（例：192.168.0.10）
mgmtSubnetIP	10.4.1.15	mgmt インターフェイスの FMC IP（例：192.168.0.10）
mgmtSubnetIPv6	ace:cab:deca:dddd::c3	mgmt インターフェイスの FMC IPv6（例：ace:cab:deca:dddd::6）
virtualNetworkNewOrExisting	new	このパラメータによって、新しい仮想ネットワークを作成するか、既存の仮想ネットワークを使用するかが決まります。
virtualNetworkAddressPrefixes	10.151.0.0/16	これは仮想ネットワークの IPv4 アドレスプレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	これは仮想ネットワークの IPv6 アドレスプレフィックスで、

パラメータ名	許可される値/タイプの例	説明
		「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet1Name	mgmt-ipv6	管理サブネット名。
Subnet1Prefix	10.151.1.0/24	これは管理サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	これは管理サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet1StartAddress	10.151.1.4	管理インターフェイスの IPv4 アドレス。
subnet1v6StartAddress	ace:cab:deca:1111::6	管理インターフェイスの IPv6 アドレス。
Subnet2Name	diag	データインターフェイス 1 のサブネット名。
Subnet2Prefix	10.151.2.0/24	これはデータインターフェイス 1 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	これはデータインターフェイス 1 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet2StartAddress	10.151.2.4	データインターフェイス 1 の IPv4 アドレス。
subnet2v6StartAddress	ace:cab:deca:2222::6	データインターフェイス 1 の IPv6 アドレス。

パラメータ名	許可される値/タイプの例	説明
Subnet3Name	inside	データインターフェイス 2 のサブネット名。
Subnet3Prefix	10.151.3.0/24	これはデータインターフェイス 2 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	これはデータインターフェイス 2 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet3StartAddress	10.151.3.4	データインターフェイス 2 の IPv4 アドレス。
subnet3v6StartAddress	ace:cab:deca:3333::6	データインターフェイス 2 の IPv6 アドレス。
Subnet4Name	outside	データインターフェイス 3 のサブネット名。
Subnet4Prefix	10.151.4.0/24	これはデータインターフェイス 3 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	これはデータインターフェイス 3 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet4StartAddress	10.151.4.4	データインターフェイス 3 の IPv4 アドレス。
subnet4v6StartAddress	ace:cab:deca:4444::6	データインターフェイス 3 の IPv6 アドレス。

パラメータ名	許可される値/タイプの例	説明
vmSize	Standard_D4_v2	Firewall Management Center Virtual VM のサイズ。。Standard_D4_v2 がデフォルトです。

ステップ 4 ARM テンプレートを使用して、Azure ポータルまたは Azure CLI で Firewall Management Center Virtual ファイアウォールを展開します。Azure での ARM テンプレートの展開については、次の Azure ドキュメントを参照してください。

- 『Create and deploy ARM templates by using the Azure portal』
- 『Deploy a local ARM template through CLI』

次のタスク

Firewall Management Center Virtual 展開の確認

Firewall Management Center Virtual VM が作成されると、Microsoft Azure ダッシュボードの [リソースグループ（Resource groups）] に新しい Firewall Management Center Virtual VM が一覧表示されます。対応するストレージアカウントとネットワークリソースも作成され、リストされます。ダッシュボードには、Azure 資産の統合ビューがあり、Firewall Management Center Virtual のヘルスとパフォーマンスを一目で簡単に評価できます。

始める前に

Firewall Management Center Virtual VM は自動的に起動します。展開時、Azure が VM を作成している間はステータスが [作成中（Creating）] として表示され、展開が完了するとステータスが [実行中（Running）] に変わります。

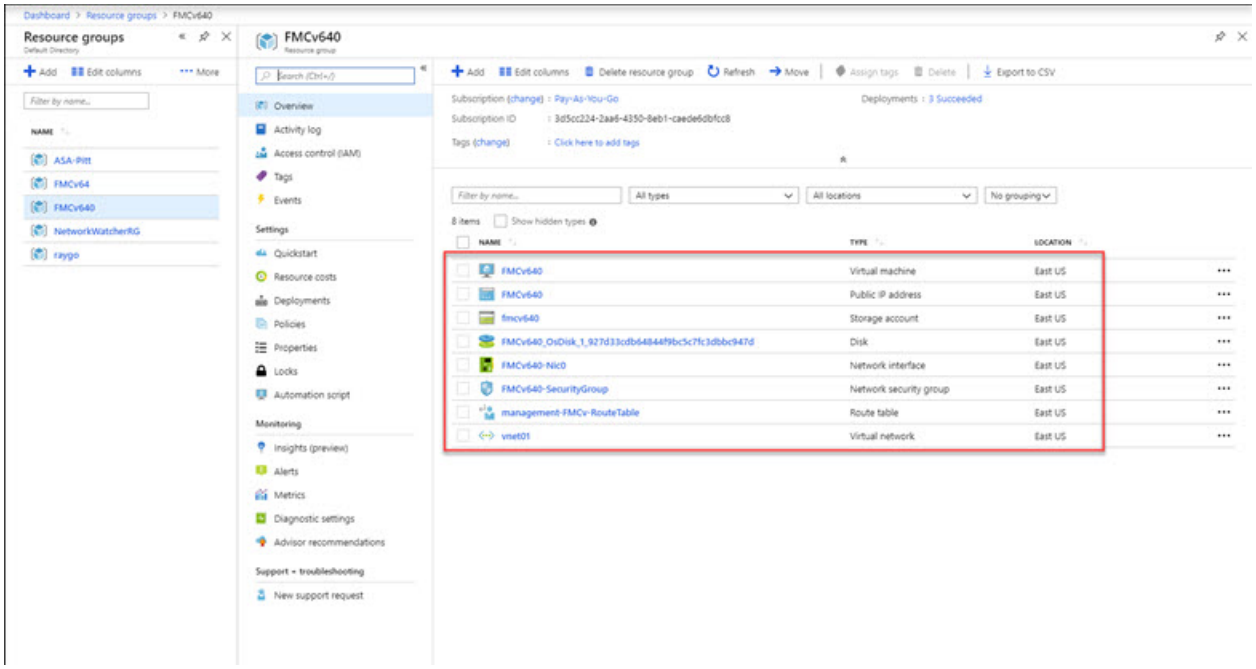
（注） 展開時間は Azure によって異なることに注意してください。また、Azure ダッシュボードに Firewall Management Center Virtual VM のステータスが [実行中（Running）] と表示されている場合でも、Firewall Management Center Virtual が使用可能になるまで合計では約 30 分かかります。

手順

ステップ 1 展開が完了した後に Firewall Management Center Virtual のリソースグループとそのリソースを表示するには、左側のメニューペインで [リソースグループ（Resource groups）] をクリックして、[リソースグループ（Resource groups）] ページにアクセスします。

次の図は、Microsoft Azure ポータルの [リソースグループ（Resource groups）] ページの例を示しています。Firewall Management Center Virtual VM およびそれに対応するリソース（ストレージアカウント、ネットワークリソースなど）に注目してください。

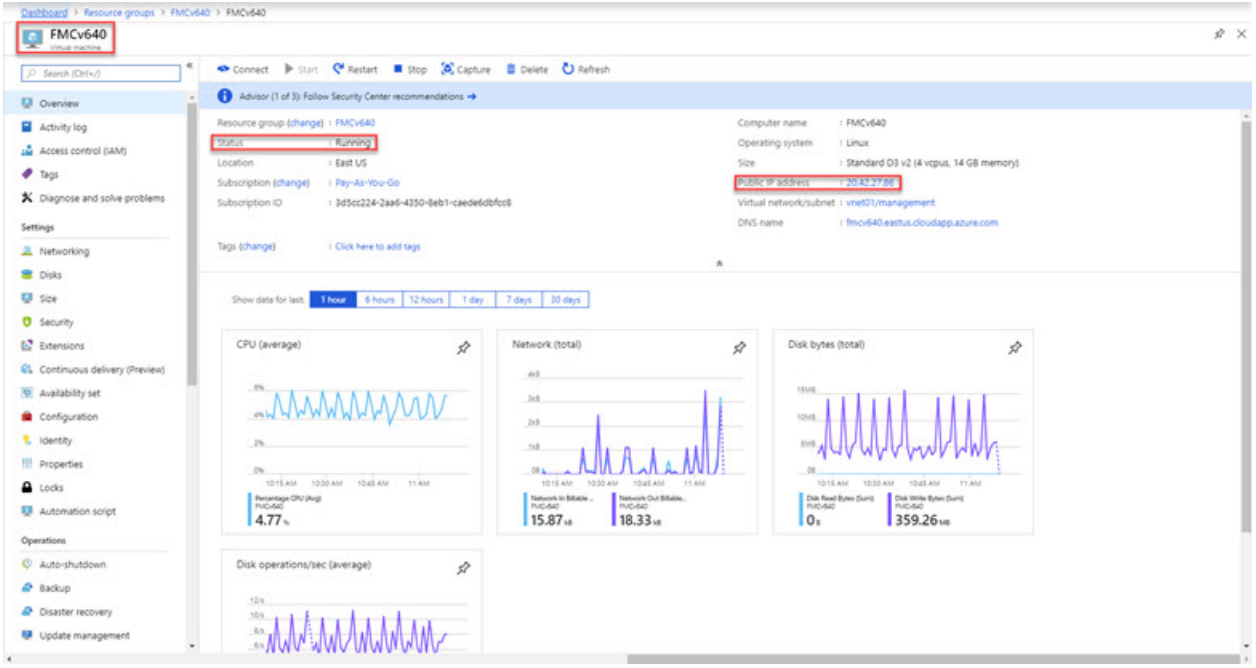
図 *2 : Azure Firewall Management Center Virtual* の [リソースグループ（*Resource Group*）] ページ



ステップ 2 リソースグループに関連付けられている Firewall Management Center Virtual VM の詳細を表示するには、Firewall Management Center Virtual VM の名前をクリックします。

次の図は、Firewall Management Center Virtual VM に関連付けられている [仮想マシン（Virtual machine）] の [概要（Overview）] ページの例を示しています。この概要には、[リソースグループ（Resource groups）] ページからアクセスします。

図 *3*:仮想マシンの概要



ステータスが [実行中（Running）] であることを確認します。Microsoft Azure ポータルの [仮想マシン（Virtual machine）] ページから Firewall Management Center Virtual VM を停止、開始、再起動、および削除できます。これらのコントロールは、Firewall Management Center Virtual のグレースフル シャットダウン メカニズムではないことに注意してください。グレースフルシャットダウンの情報については、「注意事項と制約事項（60 ページ）」を参照してください。

ステップ 3 [仮想マシン（Virtual machine）] ページで、Firewall Management Center Virtual に割り当てられている [パブリック IP アドレス（Public IP address）] を見つけます。

（注）
IP アドレスの上にカーソルを置き、[コピーするにはクリックします（Click to copy）] を選択して IP アドレスをコピーすることができます。

ステップ 4 ブラウザで **https://***public_ip*/ にアクセスします。ここで、*public_ip* は VM の展開時に Firewall Management Center Virtual の管理インターフェイスに割り当てられた IP アドレスです。

ログイン ページが表示されます。

ステップ 5 ユーザー名 **admin** と、VM の展開時に指定した管理者アカウントのパスワードを使用してログインします。

次のタスク

- ユーザーの作成やヘルスとシステムポリシーの確認など、展開を容易に管理できるように、いくつかの管理タスクを完了することをお勧めします。実行方法の概要については、「Firewall Management Center Virtual 初期管理および設定 （173 ページ）」を参照してください。

- また、デバイスの登録とライセンスの要件を確認する必要もあります。
- システム設定の開始方法の詳細については、ご使用のソフトウェアバージョンの『Secure Firewall Management Center Configuration Guide』『』を参照してください。

モニターリングおよびトラブルシューティング

このセクションでは、Micosoft Azure に展開された Firewall Management Center Virtual アプライアンスの一般的なモニターリングおよびトラブルシューティングのガイドラインを示します。モニターリングとトラブルシューティングは、Azure への VM の展開、または Firewall Management Center Virtual アプライアンスそのものに関連することがあります。

Azure による VM 展開のモニターリング

Azure の [サポート + トラブルシューティング（Support + troubleshooting）] メニューには、ツールやリソースへの迅速なアクセス、問題の診断と解決、および追加のサポートを受けることができるツールが多数用意されています。関係する項目は次の 2 つです。

- [起動時診断（Boot diagnostic）]：起動時に Firewall Management Center Virtual VM の状態を表示できます。起動時診断は、VM およびスクリーンショットからシリアルログ情報を収集します。これは、起動時の問題を診断するのに役立ちます。
- [シリアルコンソール（Serial console）]：Azure ポータルの VM シリアルコンソールを使用して、テキストベースのコンソールにアクセスできます。このシリアル接続は、仮想マシンの COM1 シリアルポートに接続し、Firewall Management Center Virtual に割り当てられたパブリック IP アドレスを使用して、Firewall Management Center Virtual のコマンドライン インターフェイスへのシリアルおよび SSH アクセスを提供します。

Firewall Management Center Virtual モニターリングとロギング

トラブルシューティングと一般的なロギング操作は、現在の Firewall Management Center および Firewall Management Center Virtual モデルと同じ手順に従います。ご使用のバージョンの『Cisco Secure Firewall Management Center Configuration Guide』『』の「*System Monitoring and Troubleshooting*」セクションを参照してください。

さらに、Microsoft Azure Linux エージェント（waagent）は、Linux のプロビジョニングと、Azure ファブリックコントローラーと VM の相互動作を管理します。同様に、以下はトラブルシューティング用の重要なログです。

- **/var/log/waagent.log**：このログには、Azure での Firewall Management Center のプロビジョニングのエラーが記録されます。
- **/var/log/firstboot.S07install_waagent**：このログには、waagent のインストールのエラーが記録されます。

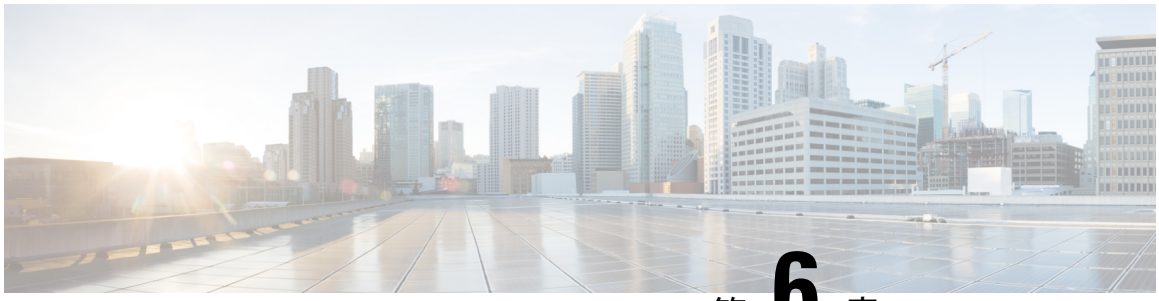
Azure プロビジョニングのエラー

Azure Marketplace ソリューションテンプレートを使用したプロビジョニングエラーは一般的ではありません。ただし、プロビジョニングエラーが発生した場合は、次の点に注意してください。

- Azure では、仮想マシンでの waagent を使用したプロビジョニングのタイムアウトが 20 分に設定され、タイムアウトすると再起動します。
- Firewall Management Center が何らかの理由でプロビジョニングできない場合、20 分のタイマーが Firewall Management Center データベースの初期化の途中で終了する傾向があり、その結果、展開が失敗する可能性があります。
- Firewall Management Center が 20 分以内にプロビジョニングできない場合は、最初からやり直すことをお勧めします。
- トラブルシューティングの情報については、*/var/log/waagent.log* で確認できます。
- シリアルコンソールに HTTP 接続エラーが表示される場合は、waagent がファブリックと通信できないことを示しています。再展開時にネットワーク設定を確認する必要があります。

機能の履歴

機能名	リリース	機能情報
Microsoft Azure パブリッククラウドに Firewall Management Center Virtual を導入します。	6.4.0	初期サポート。



第 6 章

GCP への Firewall Management Center Virtual の展開

Google Cloud Platform（GCP）は、Google が提供するパブリッククラウドサービスで、Google のスケーラブルなインフラストラクチャを構築してホストすることができます。Google の仮想プライベートクラウド（VPC）は、ワークロードが地域およびグローバルに接続する方法を、拡張および制御する柔軟性を提供します。GCP では、Google のパブリック インフラストラクチャ上に独自の VPC を構築できます。

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

- 概要 （93 ページ）
- 前提条件 （94 ページ）
- 注意事項と制約事項 （95 ページ）
- ネットワークトポロジの例 （95 ページ）
- Firewall Management Center Virtual の導入 （96 ページ）
- GCP 上の Firewall Management Center Virtual インスタンスへのアクセス （99 ページ）

概要

Firewall Management Center Virtual は、物理 Firewall Management Center と同じソフトウェアを実行し、仮想フォームファクタにおいて実証済みのセキュリティ機能を提供します。Firewall Management Center Virtualは、パブリック GCP に展開できます。その後、仮想デバイスおよび物理デバイスを管理するように設定できます。

GCP マシンタイプのサポート

Firewall Management Center Virtualは、コンピューティング最適化された汎用マシンのハイメモリマシンタイプ、および高CPUマシンタイプの両方をサポートしています。Firewall Management Center Virtualは、次の GCP マシンタイプをサポートしています。

（注） サポートされるマシンタイプは、予告なく変更されることがあります。

（注） マシンタイプの選択は制限されています。ユーザーは、選択された特定の Firewall Management Center Virtual のバージョンでサポートされているマシンタイプのみを選択できます。

表 *11*：サポートされるコンピューティング最適化マシンタイプ

コンピューティング最適化マシンタイプ	属性	
	vCPU	**RAM（GB）**
c2d-standard-8	8	32 GB
c2d-standard-16	16	64 GB

表 *12*：サポートされる汎用マシンタイプ

汎用マシンタイプ	属性	
	vCPU	**RAM（GB）**
e2-standard-8	8	32
e2-standard-16	16	64
e2-highmem-8	8	64
e2-highmem-16	16	128
n1-highmem-8	8	52
n1-highmem-16	16	104
n2d-standard-8	8	32
n2d-standard-16	16	64

前提条件

- https://cloud.google.com で GCP アカウントを作成します。
- Cisco スマートアカウント。Cisco Software Central（https://software.cisco.com/）で作成できます。
  - Firewall Management Center 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、Firewall Management Center コンフィギュレーション ガイド [英語] の「Licensing the System」を参照してください。

- インターフェイスの要件：
  - 管理インターフェイス：Firewall Threat Defense デバイスを Firewall Management Center に接続するために使用されるインターフェイス。
- 通信パス：
  - Firewall Management Center への管理アクセス用のパブリック IP。
- Firewall Management Center Virtual とシステム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。

注意事項と制約事項

サポートされる機能

- GCP Compute Engine での展開
- インスタンスごとに最大 32 個の vCPU（GCP マシンタイプに基づく）
- ライセンス：BYOL のみをサポート

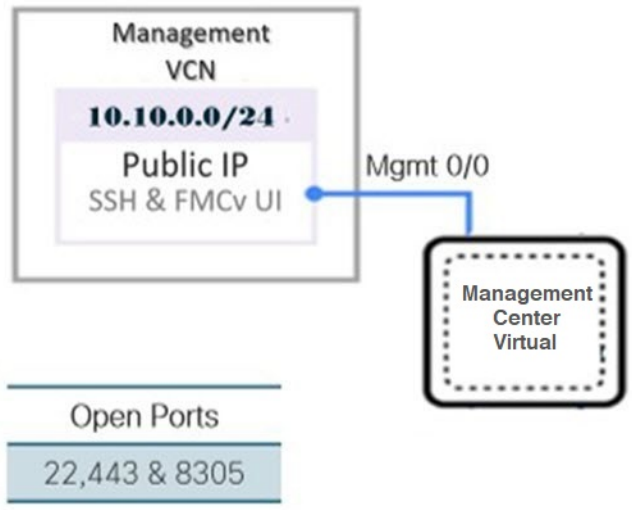
サポートされない機能

- IPv6
- Firewall Management Center Virtual ネイティブ HA
- 自動スケール
- トランスペアレント/インライン/パッシブ モード
- マルチ コンテキスト モード

ネットワークトポロジの例

次の図は、GCP で 1 つのサブネットが設定された Firewall Management Center Virtual の標準的なトポロジを示しています。

図 *4 : GCP* での *Firewall Management Center Virtual* 展開のトポロジ例



Firewall Management Center Virtual の導入

次の手順では、GCP 環境を準備し、Firewall Management Center Virtualインスタンスを起動する方法について説明します。

VPC ネットワークの作成

Firewall Management Center Virtual の展開には、管理 Firewall Management Center Virtual の管理 VPC が必要です。3 ページの図 1 を参照してください。

手順

ステップ 1 GCP コンソールで、**[VPC ネットワーク（VPC networks）]** を選択し、**[VPC ネットワークの作成（Create VPC Network）]** をクリックします。

ステップ 2 **[名前（Name）]** フィールドに、VPC ネットワークを記述する名前を入力します。

ステップ 3 **サブネット作成モード**で、**[カスタム（Custom）]** をクリックします。

ステップ 4 **新しいサブネット**で **[名前（Name）]** フィールドに、特定の名前を入力します。

ステップ 5 **[地域（Region）]** ドロップダウンリストから、展開に適した地域を選択します。

ステップ 6 **[IP アドレス範囲（IP address range）]** フィールドで、最初のネットワークのサブネットを CIDR 形式（10.10.0.0/24 など）で入力します。

ステップ 7 その他すべての設定はデフォルトのままで、 **[作成（Create）]** をクリックします。

ファイアウォールルールの作成

各 VPC ネットワークには、SSH とトラフィックを許可するファイアウォールルールが必要です。各 VPC ネットワークのファイアウォールルールを作成します。

手順

ステップ 1 GCP コンソールで、**[ネットワーキング（Networking）]** > **[VPC ネットワーク（VPC network）]** > **[ファイアウォール（Firewall）]**を選択し、**[ファイアウォールルールの作成（Create Firewall Rule）]** をクリックします。

ステップ 2 **[名前（Name）]** フィールドに、ファイアウォールルールのわかりやすい名前を入力します（例：*vpc-asiasouth-mgmt-ssh*）。

ステップ 3 **[ネットワーク（Network）]** ドロップダウンリストから、ファイアウォールルールを作成する VPC ネットワークの名前を選択します（例：*fmcv-south-mgmt*）。

ステップ 4 **[ターゲット（Targets）]** ドロップダウンリストから、ファイアウォールルールに適用可能なオプションを選択します（例：**[ネットワーク内のすべてのインスタンス（All instances in the network）]**）。

ステップ 5 **[送信元 IP 範囲（Source IP Ranges）]** フィールドに、送信元 IP アドレスの範囲を CIDR 形式で入力します（例：0.0.0.0/0）。

トラフィックは、これらの IP アドレス範囲内の送信元からのみ許可されます。

ステップ 6 **[プロトコルとポート（Protocols and ports）]** の下で、**[指定されたプロトコルとポート（Specified protocols and ports）]** を選択します。

ステップ 7 セキュリティルールを追加します。

a) SSH（TCP/22）を許可するルールを追加します。

b) TCP ポート 443 を許可するルールを追加します。

HTTPS 接続用にポート 443 を開く必要がある Firewall Management Center Virtual UI にアクセスします。

ステップ 8 [作成（Create）] をクリックします。

GCP 上の Firewall Management Center Virtual インスタンスの作成

次の手順に従って、GCP コンソールから Firewall Management Center Virtual インスタンスを展開できます。

手順

ステップ 1 GCP コンソールにログインします。

ステップ 2 **ナビゲーションメニューの** > **[マーケットプレイス（Marketplace）]**をクリックします。

ステップ 3 マーケットプレイスで「Firewall Management Center BYOL」を検索して、サービスを選択します。

ステップ 4 [作成（Launch）] をクリックします。

a) **[展開名（Deployment name）]**：インスタンスの一意の名前を指定します。

b) **[イメージバージョン（Image version）]**：ドロップダウンリストからバージョンを選択します。

c) **[ゾーン（Zone）]**：Firewall Management Center Virtualを展開するゾーンを選択します。

d) **[マシンタイプ（Machine type）]**：GCP マシンタイプのサポート （93 ページ）に基づいて正しいマシンタイプを選択します。

e) **[SSH キー（SSH key）]（オプション）**：SSH キーペアから公開キーを貼り付けます。

キーペアは、GCP が保存する公開キーと、ユーザーが保存する秘密キーファイルで構成されます。これらを一緒に使用すると、インスタンスに安全に接続できます。キーペアはインスタンスへの接続に必要となるため、必ず既知の場所に保存してください。

f) このインスタンスにアクセスするための**プロジェクト全体の SSH キーをブロック**するか許可するかを選択します。Google ドキュメント『Linux インスタンスによるプロジェクト全体の公開 SSH 認証鍵の使用を許可またはブロックする（Allowing or blocking project-wide public SSH keys from a Linux instance）』https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#block-project-keysを参照してください。

g) [起動スクリプト（Startup script）]：Firewall Management Center Virtual の Day0 構成を指定します。

次に、**[起動スクリプト（Startup script）]** フィールドにコピーして貼り付けることができる day0 構成の例を示します。

```
{
"AdminPassword": "myPassword@123456",
"Hostname": "cisco-fmcv"
}
```

ヒント
実行エラーを防ぐには、JSON 検証ツールを使用して day0 構成を検証する必要があります。

h) ドロップダウンリストから **[起動ディスクの種類（Boot disk type）]** を選択します。

デフォルトでは、**[標準の永続ディスク（Standard Persistent Disk）]** が選択されています。デフォルトの起動ディスクの種類を使用することを推奨します。

i) **[起動ディスクのサイズ（GB 単位）（Boot disk size in GB）]** のデフォルト値は 250 GB です。シスコでは、デフォルトの起動ディスクのサイズを維持することを推奨しています。250 GB 未満にすることはできません。

j) 管理インターフェイスを設定するには、**[ネットワークインターフェイスの追加（Add network interface）]** をクリックします。

（注）
インスタンスを作成した後では、インスタンスにインターフェイスを追加できません。不適切なインターフェイス構成でインスタンスを作成した場合は、インスタンスを削除し、適切なインターフェイス構成で再作成する必要があります。

- **[ネットワーク（Network）]** ドロップダウンリストから、[VPC network（VPC ネットワーク）]（*vpc-branch-mgmt* など）を選択します。

- **[外部 IP（External IP）]** ドロップダウンリストから、適切なオプションを選択します。

  管理インターフェイスには、[外部 IP からエフェメラルへ（External IP to Ephemeral）] を選択します。

- [完了（Done）] をクリックします。

k) **[ファイアウォール（Firewall）]**：ファイアウォールルールを適用します。

- **[インターネットからの TCP ポート 22 のトラフィックを許可する（SSH アクセス）（Allow TCP port 22 traffic from the Internet (SSH access)）]** チェックボックスをオンにして、SSH を許可します。
- **[インターネットからの HTTPS トラフィックを許可する（FMC GUI）（Allow HTTPS traffic from the Internet (FMC GUI)）]** チェックボックスをオンにして、HTTPS 接続を許可します。
- **[インターネットからの TCP ポート 8305 のトラフィックを許可する（SFTunnel comm.）（Allow TCP port 8305 traffic from the Internet (SFTunnel comm.)）]** チェックボックスをオンにして、Firewall Management Center Virtualおよび管理対象デバイスが双方向の SSL 暗号化通信チャネルを使用して通信できるようにします。

l) **[詳細（More）]** をクリックしてビューを展開し、**[IP 転送（IP Forwarding）]**が**[オン（On）]**に設定されていることを確認します。

ステップ 5 [展開（Deploy）] をクリックします。

（注）
起動時間は、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 35 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。

次のタスク

GCP コンソールの [VM インスタンス（VM instance）] ページからインスタンスの詳細を表示します。インスタンスを停止および開始するための内部 IP アドレス、外部 IP アドレス、およびコントロールが表示されます。編集する場合は、インスタンスを停止する必要があります。

GCP 上の Firewall Management Center Virtual インスタンスへのアクセス

SSH（ポート 22 経由の TCP 接続）を許可するファイアウォールルールがすでに作成されていることを確認します。詳細については、ファイアウォールルールの作成 （97 ページ）を参照してください。

このファイアウォールルールにより、Firewall Management Center Virtual インスタンスへのアクセスが可能になり、次の方法を使用してインスタンスに接続できます。

- 外部 IP（External IP）
  - ブラウザ ウィンドウ
  - その他の SSH クライアントまたはサードパーティ製ツール
- シリアル コンソール
  - Gcloud コマンドライン

詳細については、Google ドキュメントの 『Connecting to instances』を参照してください。

（注） Day0 構成を追加しない場合は、デフォルトのログイン情報を使用して Firewall Management Center Virtual インスタンスにログインできます。最初のログイン試行時にパスワードを設定するように求められます。

シリアルコンソールを使用した Firewall Management Center Virtual インスタンスへの接続

手順

ステップ 1 GCP コンソールで、**[コンピューティングエンジン（Compute Engine）]**>**[VM インスタンス（VM instances）]** を選択します。

ステップ 2 Firewall Management Center Virtualのインスタンス名をクリックすると、**[VM インスタンスの詳細（VM instance details）]** ページが開きます。

ステップ 3 **[詳細（Details）]** タブで、**[シリアルコンソールへの接続（Connect to serial console）]** をクリックします。

詳細については、Google ドキュメントの「シリアルコンソールとのやり取り」を参照してください。

外部 IP を使用した Firewall Management Center Virtual インスタンスへの接続

Firewall Management Center Virtualインスタンスには、内部 IP と外部 IP が割り当てられます。外部 IP を使用してFirewall Management Center Virtualインスタンスにアクセスできます。

手順

ステップ 1 GCP コンソールで、**[コンピューティングエンジン（Compute Engine）]**>**[VM インスタンス（VM instances）]** を選択します。

ステップ 2 Firewall Management Center Virtual のインスタンス名をクリックすると、[VMインスタンスの詳細（VM instance details）] ページが開きます。

ステップ 3 **[詳細（Details）]** タブで、**[SSH]** フィールドのドロップダウンメニューをクリックします。

ステップ 4 **[SSH]** ドロップダウンメニューから、目的のオプションを選択します。

次の方法を使用してFirewall Management Center Virtualインスタンスに接続できます。

- その他の SSH クライアントまたはサードパーティ製ツール：詳細については、Google ドキュメントの「Connecting using third-party tools」を参照してください。

Gcloud を使用した Firewall Management Center Virtual インスタンスへの接続

手順

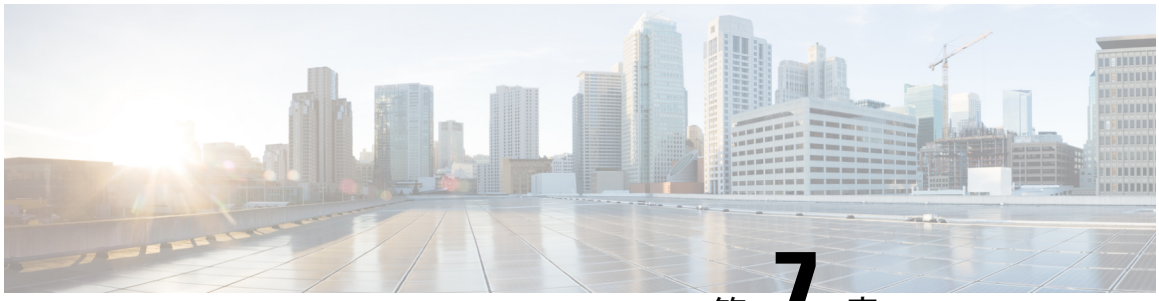
ステップ 1 GCP コンソールで、**[コンピューティングエンジン（Compute Engine）]**>**[VM インスタンス（VM instances）]** を選択します。

ステップ 2 Firewall Management Center Virtualのインスタンス名をクリックすると、**[VM インスタンスの詳細（VM instance details）]** ページが開きます。

ステップ 3 **[詳細（Details）]** タブで、**[SSH]** フィールドのドロップダウンメニューをクリックします。

ステップ 4 **[gcloud コマンドを表示（View gcloud command）]** > **[Cloud Shell で実行（Run in Cloud Shell）]**をクリックします。

[Cloud Shell] ターミナルウィンドウが開きます。詳細については、Google ドキュメントの「gcloud コマンドラインツールの概要」、および「gcloud compute ssh」を参照してください。



第 7 章

OCI への Firewall Management Center Virtual の導入

Oracle Cloud Infrastructure（OCI）は、オラクルが提供する可用性の高いホスト環境でアプリケーションを実行できるパブリック クラウド コンピューティング サービスです。OCI は、Oracle の自律型サービス、統合セキュリティ、およびサーバーレス コンピューティングを組み合わせることで、エンタープライズアプリケーションにリアルタイムの柔軟性を提供します。

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

- 概要 （103 ページ）
- 前提条件 （105 ページ）
- 注意事項と制約事項 （106 ページ）
- ネットワークトポロジの例 （106 ページ）
- Firewall Management Center Virtual の導入 （107 ページ）
- OCI 上の Firewall Management Center Virtual インスタンスへのアクセス （112 ページ）

概要

Firewall Management Center Virtual は、物理 Firewall Management Center と同じソフトウェアを実行し、仮想フォームファクタにおいて実証済みのセキュリティ機能を提供します。Firewall Management Center Virtual は、パブリック OCI で展開できます。その後、仮想デバイスおよび物理デバイスを管理するように設定できます。

OCI のコンピューティングシェイプ

シェイプは、インスタンスに割り当てられる CPU の数、メモリの量、およびその他のリソースを決定するテンプレートです。Firewall Management Center Virtual は、次の OCI のシェイプタイプをサポートします。

表 *13 :* でサポートされるコンピューティングシェイプ *Firewall Management Center Virtual*

OCI シェイプ	サポートされる Firewall Management Center Virtual のバージョン	属性	
		oCPU	RAM（GB）
インテル VM.StandardB1.4	7.3.0 以降	4	48
インテル VM.Standard2.4	7.1.0 以降	4	60
インテル VM.Standard3.Flex	7.3.0 以降	4	32
インテル VM.Optimized3.Flex	7.3.0 以降	4	32
AMD VM.Standard.E4.Flex	7.3.0 以降	4	32
AMD VM.Standard.E5.Flex	7.6.4 のみ	4	32
AMD VM.Standard.E6.Flex	7.6.4 のみ	4	32

Firewall Management Center Virtual バージョン 7.3 以降でサポートされている OCI コンピューティングシェイプの使用に関する推奨事項。

- OCI マーケットプレイス イメージ バージョン **7.3.0-69-v3** 以降は、Firewall Management Center Virtual 7.3 以降の OCI コンピューティングシェイプとのみ互換性があります。
- Firewall Management Center Virtual 7.3 以降でサポートされている OCI コンピューティングシェイプは、新しい展開でのみ使用できます。
- OCI コンピューティング シェイプ バージョン **7.3.0-69-v3** 以降は、Firewall Management Center Virtual 7.3 より前の OCI コンピューティング シェイプ バージョンを使用して Firewall Management Center Virtual で展開された VM をアップグレードすることと互換性がありません。

表 *14 : Firewall Management Center Virtual 300*（*FMCv300*）でサポートされているコンピューティングシェイプ

OCI シェイプ	サポートされている Firewall Management Center Virtual 300 バージョン	属性	
		oCPU	RAM（GB）
VM.Standard2.16	7.1.0 以降	16	64 GB

OCI シェイプ	サポートされている Firewall Management Center Virtual 300 バージョン	属性	
		oCPU	RAM（GB）
インテル VM.Standard3.Flex	7.3 以降	16	64 GB
インテル VM.Optimized3.Flex	7.3 以降	16	64 GB
AMD VM.Standard.E4.Flex	7.3 以降	16	64 GB
AMD VM.Standard.E5.Flex	7.6.4 のみ	16	64 GB
AMD VM.Standard.E6.Flex	7.6.4 のみ	16	64 GB

（注） Flex コンピューティングシェイプを使用することを推奨します。

（注） サポートされているコンピューティングシェイプの可用性は、CSPによって変わる場合があります。

- OCI では、1 つの oCPU は 2 つの vCPU に相当します。
- Firewall Management Center Virtual には 1 つのインターフェイスが必要です。

ユーザーは、OCI でアカウントを作成し、Oracle Cloud Marketplace の Firewall Management Center Virtual を使用してコンピューティング インスタンスを起動し、OCI のシェイプを選択します。

前提条件

- https://www.oracle.com/cloud/ で OCI アカウントを作成します。
- Cisco スマートアカウント。Cisco Software Central（https://software.cisco.com/）で作成できます。
  - Firewall Management Center 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、Firewall Management Center コンフィギュレーション ガイド [英語] の「Licensing the System」を参照してください。

- インターフェイスの要件：
  - 管理インターフェイス：Firewall Threat Defense デバイスを Firewall Management Center に接続するために使用されるインターフェイス。
- 通信パス：
  - Firewall Management Center Virtual への管理アクセス用のパブリック IP。
- Firewall Management Center Virtual とシステム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。

注意事項と制約事項

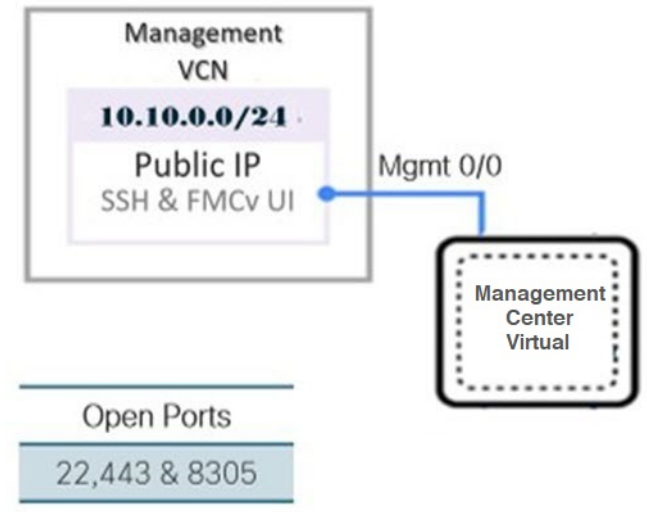
サポートされる機能

- OCI 仮想クラウドネットワーク（VCN）での展開
- インスタンスあたり最大 8 つの vCPU
- ルーテッド モード（デフォルト）
- ライセンス：BYOL のみをサポート
- IPv6
- **OCI 用 Firewall 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 OCI プラットフォームで使用できます（7.1.0 以降）。
- 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

ネットワークトポロジの例

次の図は、OCI で 1 つのサブネットが設定された Firewall Management Center Virtual の標準的なトポロジを示しています。

図 *5 : OCI* での *Firewall Management Center Virtual* 展開のトポロジ例



Firewall Management Center Virtual の導入

仮想クラウドネットワーク（VCN）の設定

Firewall Management Center Virtual 展開用の仮想クラウドネットワーク（VCN）を設定します。

始める前に

（注） ナビゲーションメニューからサービスを選択すると、左側のメニューにコンパートメントリストが表示されます。コンパートメントはリソースの整理に役立ち、リソースへのアクセスを制御しやすくなります。ルートコンパートメントは、テナントがプロビジョニングされるときにOracleによって作成されます。管理者は、ルートコンパートメントにさらに多くのコンパートメントを作成し、アクセスルールを追加して、どのユーザーがそれらのコンパートメントを表示してアクションを実行できるかを制御できます。詳細については、Oracle のドキュメント『コンパートメントの管理（Managing Compartments）』を参照してください。

手順

ステップ 1 OCI にログインし、地域を選択します。

OCI は互いに分かれた複数の地域に分割されています。地域は、画面の右上隅に表示されます。ある地域内のリソースは、別の地域には表示されません。目的の地域内に存在していることを定期的に確認してください。

ステップ 2 **[ネットワーキング（Networking）] > [仮想クラウドネットワーク（Virtual Cloud Networks）]**を選択し、**[VCN の作成（Create VCN）]** をクリックします。

ステップ 3 VCN のわかりやすい**名前**を入力します（例：*FMCv-Management*）。

ステップ 4 VCN の **CIDR ブロック**を入力します。

ステップ 5 **[VCN の作成（Create VCN）]** をクリックします。

次のタスク

次の手順に進み、管理 VCN を完了できます。

ネットワーク セキュリティ グループの作成

ネットワーク セキュリティ グループは、一連の vNIC と、vNIC に適用される一連のセキュリティルールで構成されます。

手順

ステップ 1 **[ネットワーキング（Networking）] > [仮想クラウドネットワーク（Virtual Cloud Networks）] > [仮想クラウドネットワークの詳細（Virtual Cloud Network Details）] > [ネットワーク セキュリティ グループ（Network Security Groups）]**を選択し、**[ネットワーク セキュリティ グループの作成（Create Network Security Group）]** をクリックします。

ステップ 2 ネットワーク セキュリティ グループのわかりやすい**名前**を入力します（例：*FMCv-Mgmt-Allow-22-443-8305*）。

ステップ 3 [Next] をクリックします。

ステップ 4 セキュリティルールを追加します。

a) SSH アクセスに TCP ポート 22 を許可するルールを追加します。

b) HTTPS アクセス用に TCP ポート 443 を許可するルールを追加します。

c) TCP ポート 8305 を許可するルールを追加します。

デバイス Firewall Management Center Virtual は Firewall Management Center Virtual を介して管理できます。管理するためには、HTTPS 接続用にポート 8305 を開く必要があります。Firewall Management Center 自体にアクセスするには、ポート 443 が必要です。

ステップ 5 [作成（Create）] をクリックします。

インターネットゲートウェイの作成

管理サブネットを公的にアクセス可能にするには、インターネットゲートウェイが必要です。

手順

ステップ 1 **[ネットワーキング（Networking）]** > **[仮想クラウドネットワーク（Virtual Cloud Networks）]** > **[仮想クラウドネットワークの詳細（Virtual Cloud Network Details）]** > **[インターネットゲートウェイ（Internet Gateways）]**を選択し、**[インターネットゲートウェイの作成（Create Internet Gateway）]** をクリックします。

ステップ 2 インターネットゲートウェイのわかりやすい**名前**を入力します（例：*FMCv-IG*）。

ステップ 3 **[インターネットゲートウェイの作成（Create Internet Gateway）** をクリックします。

ステップ 4 インターネットゲートウェイへのルートを追加します。

a) **[ネットワーキング（Networking）]** > **[仮想クラウドネットワーク（Virtual Cloud Networks）]** > **[仮想クラウドネットワークの詳細（Virtual Cloud Network Details）]** > **[ルートテーブル（Route Tables）]**を選択します。

b) ルートルールを追加するには、デフォルトのルートテーブルのリンクをクリックします。

c) **[ルートルールの追加（Add Route Rules）]** をクリックします。

d) **[ターゲットタイプ（Target Type）]** ドロップダウンから、**[インターネットゲートウェイ（Internet Gateway）]** を選択します。

e) 宛先 CIDR のブロックを入力します（例：0.0.0.0/0）。

f) **[ターゲット インターネット ゲートウェイ（Target Internet Gateway）]** ドロップダウンから、作成したゲートウェイを選択します。

g) **[ルートルールの追加（Add Route Rules）]** をクリックします。

サブネットの作成

各 VCN には、少なくとも 1 つのサブネットがあります。管理 VCN の管理サブネットを作成します。

手順

ステップ 1 **[ネットワーキング（Networking）]** > **[仮想クラウドネットワーク（Virtual Cloud Networks）]** > **[仮想クラウドネットワークの詳細（Virtual Cloud Network Details）]** > **[サブネット（Subnets）]**を選択し、**[サブネットの作成（Create Subnet）]** をクリックします。

ステップ 2 サブネットのわかりやすい**名前**を入力します（例：*Management*）。

ステップ 3 **[サブネットタイプ（Subnet Type）]** を選択します（推奨されるデフォルトの **[地域（Regional）]** のままにします）。

ステップ 4 **CIDR ブロック**を入力します（例：10.10.0.0/24）。サブネットの内部（非公開）IP アドレスは、この CIDR ブロックから取得されます。

ステップ 5 **[ルートテーブル（Route Table）]** ドロップダウンから、以前に作成したルートテーブルのいずれかを選択します。

ステップ 6 サブネットの **[サブネットアクセス（Subnet Access）]** を選択します。

管理サブネットの場合、これは**パブリックサブネット**である必要があります。

ステップ 7 **[DHCP オプション（DHCP Option）]** を選択します。

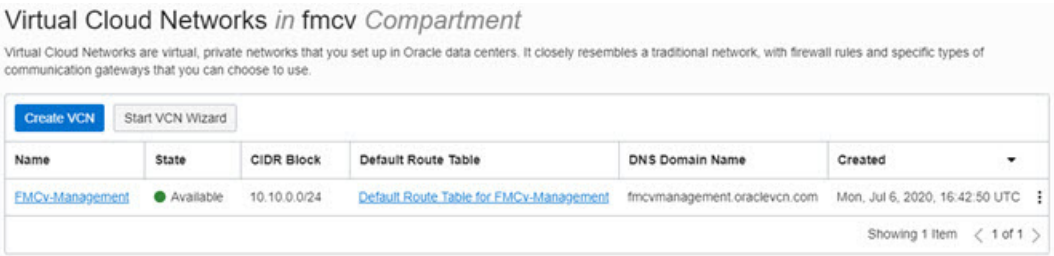
ステップ 8 以前作成した **[セキュリティリスト（Security List）]** を選択します。

ステップ 9 **[サブネットの作成（Create Subnet）]** をクリックします。

次のタスク

管理 VCN を設定すると、Firewall Management Center Virtual を起動する準備が整います。Firewall Management Center Virtual VCN 構成の例については、次の図を参照してください。

図 *6 : Firewall Management Center Virtual* 仮想クラウドネットワーク



OCI での Firewall Management Center Virtual インスタンスの作成

Oracle Cloud Marketplace の Firewall Management Center Virtual（BYOL）サービスを使用して、コンピューティング インスタンスを介して OCI に Firewall Management Center Virtual を展開します。CPU の数、メモリの量、ネットワークリソースなどの特性に基づいて、最適なマシンシェイプを選択します。

手順

ステップ 1 OCI ポータルにログインします。

地域は、画面の右上隅に表示されます。目的の地域内に存在していることを確認してください。

ステップ 2 **[マーケットプレイス（Marketplace）]** > **[アプリケーション（Applications）]**を選択します。

ステップ 3 マーケットプレイスで「Firewall Management Center Virtual BYOL」を検索して、サービスを選択します。

ステップ 4 契約条件を確認し、[Oracle の利用規約とパートナーの契約条件を確認して同意します。（I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions.）] チェックボックスをオンにします。

ステップ 5 [インスタンスの起動（Launch Instance）] をクリックします。

ステップ 6 インスタンスのわかりやすい**名前**を入力します（例：*Cisco-FMCv*）。

ステップ 7 **[シェイプの変更（Change Shape）]** をクリックし、Firewall Management Center Virtual に必要な CPU の数、RAM の量、およびインターフェイスの数が指定されたシェイプ（VM.Standard2.4 など）を選択します（OCI のコンピューティングシェイプ （103 ページ）を参照）。

ステップ 8 **[仮想クラウドネットワーク（Virtual Cloud Network）]** ドロップダウンから、[管理 VCN（Management VCN）] を選択します。

ステップ 9 自動入力されていない場合は、**[サブネット（Subnet）]** ドロップダウンから [管理サブネット（Management subnet）] を選択します。

ステップ 10 **[ネットワーク セキュリティ グループを使用してトラフィックを制御する（Use Network Security Groups to Control Traffic）]** にチェックを入れ、管理 VCN に設定したセキュリティグループを選択します。

ステップ 11 **[パブリック IP アドレスの割り当て（Assign a Public Ip Address）]** オプションボタンをクリックします。

ステップ 12 **[SSH キーの追加（Add SSH keys）]** の下で、**[公開キーの貼り付け（Paste Public Keys）]** オプションボタンをクリックして、SSH キーを貼り付けます。

Linux ベースのインスタンスは、パスワードの代わりに SSH キーペアを使用してリモートユーザーを認証します。キーペアは、秘密キーと公開キーで構成されます。インスタンスを作成するときに、秘密キーをコンピュータに保持し、公開キーを提供します。ガイドラインについては、『Linux インスタンスでのキーペアの管理（Managing Key Pairs on Linux Instances）』https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/Tasks/managingkeypairs.htmを参照してください。

ステップ 13 **[詳細オプションの表示（Show Advanced Options）]** リンクをクリックして、オプションを展開します。

ステップ 14 [スクリプトの初期化（Initialization Script）] の下で、[クラウド初期化スクリプトの貼り付け（Paste Cloud-Init Script）] オプションボタンをクリックして、Firewall Management Center Virtual の Day0 構成を指定します。day0 構成は、Firewall Management Center Virtual の初回起動時に適用されます。

次に、**[クラウド初期化スクリプト（Cloud-Init Script）]** フィールドにコピーして貼り付けることができる day0 構成の例を示します。

```
{
"AdminPassword": "myPassword@123456",
"Hostname": "cisco-fmcv"
}
```

ステップ 15 [作成（Create）] をクリックします。

次のタスク

[作成（Create）] ボタンをクリックした後、状態が [プロビジョニング（Provisioning）] として表示される Firewall Management Center Virtual インスタンスをモニターします。ステータスをモニターすることが重要です。Firewall Management Center Virtual インスタンスが [プロビジョニング（Provisioning）] 状態から [実行（Running）] 状態になることを確認します。これは、Firewall Management Center Virtual の起動が完了したことを示します。

OCI 上の Firewall Management Center Virtual インスタンスへのアクセス

セキュアシェル（SSH）接続を使用して、実行中のインスタンスに接続できます。

- ほとんどの UNIX スタイルのシステムには、デフォルトで SSH クライアントが含まれています。
- Windows 10 および Windows Server 2019 システムには、OpenSSH クライアントが含まれている必要があります。Oracle Cloud Infrastructure によって生成された SSH キーを使用してインスタンスを作成した場合に必要になります。
- その他の Windows バージョンの場合は、http://www.putty.org から無償の SSH クライアントである PuTTY をダウンロードできます。

前提条件

インスタンスに接続するには、次の情報が必要です。

- インスタンスのパブリック IP アドレス。アドレスは、コンソールの [インスタンスの詳細（Instance Details）] ページから取得できます。ナビゲーションメニューを開きます。**[コアインフラストラクチャ（Core Infrastructure）]** の下で、**[コンピューティング（Compute）]** に移動し、**[インスタンス（Instances）]** をクリックします。次に、インスタンスを選択します。あるいは、コアサービス API の ListVnicAttachments および GetVnic 操作を使用できます。
- インスタンスのユーザー名とパスワード。
- インスタンスを起動したときに使用した SSH キーペアの秘密キー部分へのフルパス。

  キーペアの詳細については、「Managing Key Pairs on Linux Instances」を参照してください。

（注） Day0 構成を追加しない場合は、デフォルトのログイン情報（admin/Admin123）を使用して Firewall Management Center Virtual インスタンスにログインできます。

最初のログイン試行時にパスワードを設定するように求められます。

PuTTY を使用した Firewall Management Center Virtual インスタンスへの接続

PuTTY を使用して Windows システムから Firewall Management Center Virtual インスタンスに接続するには、次の手順を実行します。

手順

ステップ 1 PuTTY を開きます。

ステップ 2 **[カテゴリ（Category）]** ペインで、**[セッション（Session）]** を選択し、次の内容を入力します。

- **ホスト名または IP アドレス**：

  <username>@<public-ip-address>

  ここで、

  <username> は、Firewall Management Center Virtual インスタンスのユーザー名です。

  <public-ip-address> は、コンソールから取得したインスタンスのパブリック IP アドレスです。

- **ポート**： 22
- **接続タイプ**： SSH

ステップ 3 **[カテゴリ（Category）]** ペインで、**[Window]** を展開し、**[変換（Translation）]** を選択します。

ステップ 4 **[リモート文字セット（Remote character set）]** ドロップダウンリストで、**[UTF-8]** を選択します。

Linuxベースのインスタンスでデフォルトのロケール設定はUTF-8です。これにより、PuTTYは同じロケールを使用するように設定されます。

ステップ 5 **[カテゴリ（Category）]** ペインで、**[接続（Connection）]**、**[SSH]** の順に展開し、**[認証（Auth）]** をクリックします。

ステップ 6 **[参照（Browse）]** をクリックして、秘密キーを選択します。

ステップ 7 **[開く（Open）]** をクリックして、セッションを開始します。

インスタンスに初めて接続する場合は、「サーバーのホストキーがレジストリにキャッシュされていない（the server's host key is not cached in the registry）」というメッセージが表示されることがあります。**[はい（Yes）]** をクリックして、接続を続行します。

SSH を使用した Firewall Management Center Virtual インスタンスへの接続

UNIX スタイルのシステムから Firewall Management Center Virtual インスタンスに接続するには、SSH を使用してインスタンスにログインします。

手順

ステップ 1 次のコマンドを使用して、ファイルの権限を設定し、自分だけがファイルを読み取れるようにします。

```
$ chmod 400 <private_key>
```

ここで、

<private_key> は、アクセスするインスタンスに関連付けられた秘密キーを含むファイルのフルパスと名前です。

ステップ 2 インスタンスにアクセスするには、次の SSH コマンドを使用します。

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

<private_key> は、アクセスするインスタンスに関連付けられた秘密キーを含むファイルのフルパスと名前です。

<username> は、Firewall Management Center Virtual インスタンスのユーザー名です。

<public-ip-address> は、コンソールから取得したインスタンスの IP アドレスです。

OpenSSH を使用した Firewall Management Center Virtual インスタンスへの接続

Windows システムから Firewall Management Center Virtual インスタンスに接続するには、OpenSSH を使用してインスタンスにログインします。

手順

ステップ 1 このキーペアを初めて使用する場合は、自分だけがファイルを読み取れるようにファイルの権限を設定する必要があります。

次の手順を実行します。

a) Windows Explorer で、秘密キーファイルに移動し、ファイルを右クリックして **[プロパティ（Properties）]** をクリックします。
b) **[セキュリティ（Security）]** タブで、**[詳細設定（Advanced）]** をクリックします。
c) **[オーナー（Owner）]** が自分のユーザーアカウントであることを確認します。
d) **[継承の無効化（Disable Inheritance）]** をクリックし、**[継承された権限をこのオブジェクトの明示的な権限に変換する（Convert inherited permissions into explicit permissions on this object）]** を選択します。
e) 自分のユーザーアカウントではない各権限エントリを選択し、**[削除（Remove）]** をクリックします。
f) 自分のユーザーアカウントのアクセス権限が **[フルコントロール（Full Control）]** であることを確認します。
g) 変更を保存します。

ステップ 2 インスタンスに接続するには、Windows PowerShell を開き、次のコマンドを実行します。

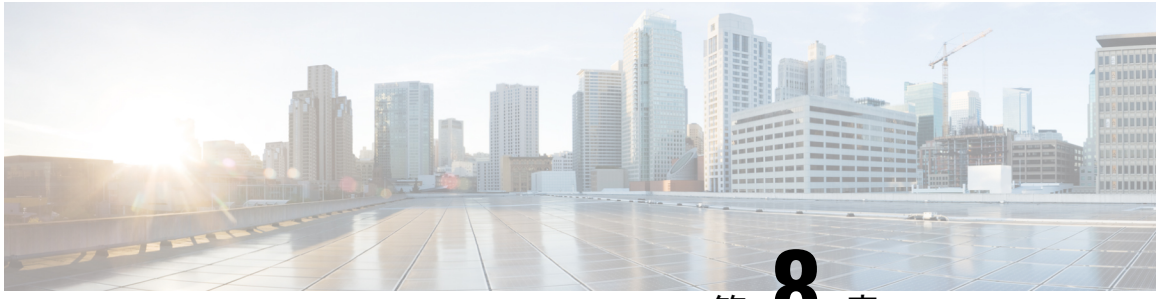
```
$ ssh -i <private_key> <username>@<public-ip-address>
```

ここで、

<private_key> は、アクセスするインスタンスに関連付けられた秘密キーを含むファイルのフルパスと名前です。

<username> は、Firewall Management Center Virtual インスタンスのユーザー名です。

<public-ip-address> は、コンソールから取得したインスタンスの IP アドレスです。



第 8 章

OpenStack への Firewall Management Center Virtual の展開

OpenStack に Firewall Management Center Virtual を導入できます。

- 概要 （117 ページ）
- 前提条件 （118 ページ）
- 注意事項と制約事項 （119 ページ）
- システム要件 （120 ページ）
- ネットワークトポロジの例 （121 ページ）
- Firewall Management Center Virtual の導入 （122 ページ）

概要

このガイドでは、OpenStack 環境で Firewall Management Center Virtual を展開する方法について説明します。OpenStack は無料のオープンな標準規格のクラウドコンピューティングプラットフォームであり、ほとんどの場合は、ユーザーが仮想サーバーやその他のリソースを利用できるように Infrastructure-as-a-Service（IaaS）としてパブリッククラウドとプライベートクラウドの両方に展開します。

Firewall Management Center Virtual は、物理 Firewall Management Center と同じソフトウェアを実行し、仮想フォームファクタにおいて実証済みのセキュリティ機能を提供します。Firewall Management Center Virtual は OpenStack に展開できます。その後、仮想デバイスおよび物理デバイスを管理するように設定できます。

この展開では、KVM ハイパーバイザを使用して仮想リソースを管理します。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。

デバイスは KVM ハイパーバイザですでにサポートされているため、OpenStack サポートを有効にするために必要な追加のカーネルパッケージやドライバはありません。

前提条件

- software.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

- software.cisco.com および Cisco Service Contract が必要です。
- Firewall Management Center Virtual は、オープンソースの OpenStack 環境と Cisco VIM 管理対象 OpenStack 環境での展開をサポートします。

  OpenStack のガイドラインに従って OpenStack 環境をセットアップします。

  - オープンソースの OpenStack ドキュメントを参照してください。

    Caracalリリース：https://docs.openstack.org/project-deploy-guide/openstack-ansible/2024.1/overview.html

  - Cisco Virtualized Infrastructure Manager（VIM）OpenStack のドキュメント（Cisco Virtualized Infrastructure Manager のマニュアル、4.4.3）を参照してください。

- ライセンス：
  - Firewall Management Center からセキュリティサービスのソフトウェア利用資格を設定します。
  - 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。
- メモリとリソースの要件：
  - 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
  - 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

（注） 要件に応じて、vCPU とメモリの値を変更できます。

- インターフェイスの要件：
  - 管理インターフェイス：デバイスを Firewall Management Center に接続するために使用されるインターフェイス。
- 通信パス：
  - Firewall Management Center Virtual にアクセスするためのフローティング IP。
- サポートされている Firewall Management Center Virtual の最小バージョン：
  - バージョン 7.0。
- OpenStack の要件については、システム要件 （120 ページ）を参照してください。
- Firewall Management Center Virtual とシステム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。

注意事項と制約事項

サポートされる機能

OpenStack 上の Firewall Management Center Virtual は次の機能をサポートします。

- OpenStack 環境のコンピューティングノードで実行されている KVM ハイパーバイザへの Firewall Management Center Virtual の展開
- OpenStack CLI
- Heat テンプレートベースの展開
- ライセンス：BYOL のみをサポート
- ドライバ：VIRTIO
- IPv6 はサポートされます。

サポートされない機能

OpenStack 上の Firewall Management Center Virtual は以下をサポートしません。

- 自動スケール
- クラスタ

システム要件

OpenStack 環境は、サポートされているハードウェアとソフトウェアの次の要件に準拠している必要があります。

表 *15 :* ハードウェアおよびソフトウェアの要件

カテゴリ	サポートされるバージョン	注記
サーバー	UCS C240 M5	2 台の UCS サーバーを推奨します。os-controller ノードと os-compute ノードに 1 台ずつです。
要因	VIRTIO	サポートされているドライバは次のとおりです。
オペレーティング システム	Ubuntu Server 22.04	これは、UCS サーバーで推奨されている OS です。
OpenStack バージョン	Caracal リリース	さまざまな OpenStack リリースの詳細については、次の URL を参照してください。 https://releases.openstack.org/

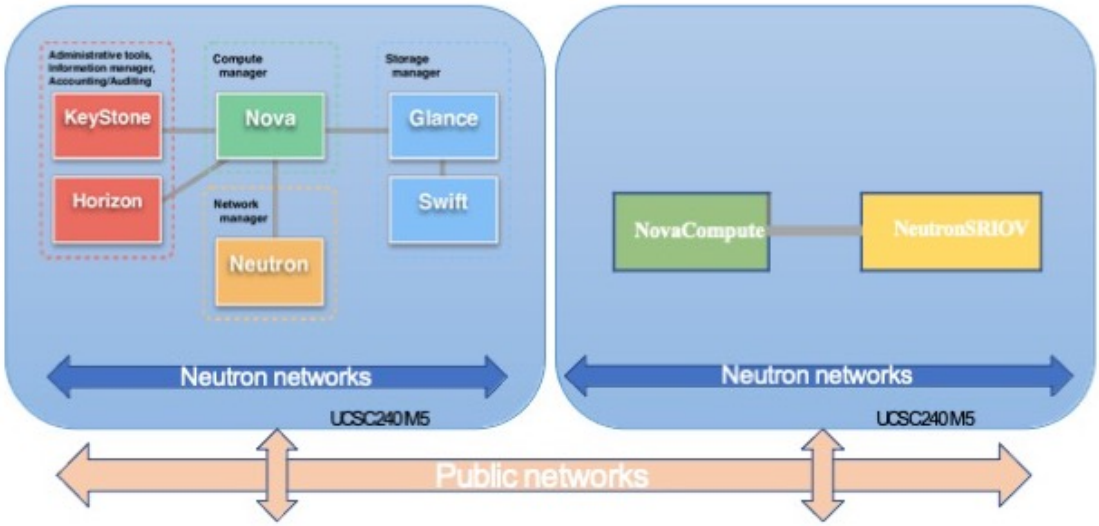
表 *16 : Cisco VIM Managed OpenStack* のハードウェアとソフトウェアの要件

カテゴリ	サポートされるバージョン	注記
サーバ ハードウェア	UCS C220-M5/UCS C240-M4	os-controller ノードごとに 3 台、os-compute ノードに 2 台以上で、5 台の UCS サーバーを推奨します。
ドライバ（Drivers）	VIRTIO	サポートされているドライバは次のとおりです。
Cisco VIM バージョン	Cisco VIM 4.4.3 サポート対象： • オペレーティングシステム - Red Hat Enterprise Linux 8.4 • OpenStack バージョン - OpenStack 16.2（トレインリリース）	詳細については、シスコ仮想インフラストラクチャ マネージャのドキュメント 4.4.3 を参照してください。

OpenStack プラットフォームトポロジ

次の図に、2 台の UCS サーバーを使用して OpenStack での展開をサポートするための推奨トポロジを示します。

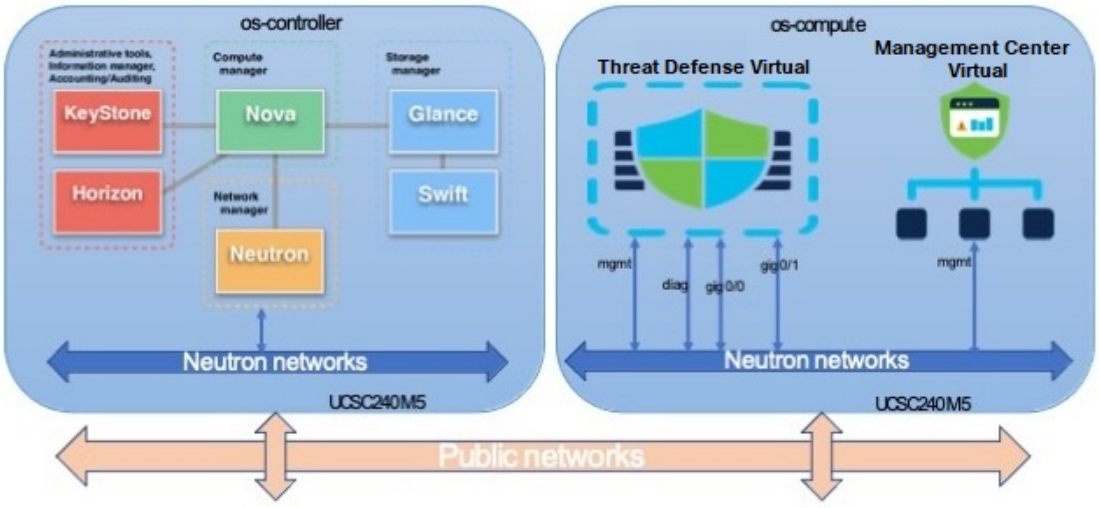
図 *7 : OpenStack* プラットフォームトポロジ



ネットワークトポロジの例

次の図に、OpenStack の Firewall Management Center Virtual のネットワークトポロジの例を示します。

図 *8 : OpenStack* で *Firewall Management Center Virtual* を使用したトポロジの例



Firewall Management Center Virtual の導入

シスコでは、Firewall Management Center Virtual を展開するためのサンプルの Heat テンプレートを提供しています。OpenStack インフラストラクチャのリソースを作成する手順は、ネットワーク、サブネット、およびルータインターフェイスを作成するために、Heat テンプレート（`deploy_os_infra.yaml`）ファイルで結合されます。Firewall Management Center Virtual の展開手順は大まかに次の部分に分類されます。

- Firewall Management Center Virtual qcow2 イメージを OpenStack Glance サービスにアップロードします。
- ネットワーク インフラストラクチャを作成します。
  - ネットワーク
  - サブネット
  - ルータ インターフェイス
- Firewall Management Center Virtual インスタンスを作成します。
  - フレーバ
  - セキュリティ グループ
  - フローティング IP
  - インスタンス

次の手順を使用して、OpenStack に Firewall Management Center Virtual を展開できます。

OpenStack への Firewall Management Center Virtual イメージのアップロード

Firewall Management Center Virtual qcow2 イメージを OpenStack コントローラノードにコピーし、イメージを OpenStack Glance サービスにアップロードします。

始める前に

- 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

手順

ステップ 1 qcow2 イメージファイルを OpenStack コントローラノードにコピーします。

ステップ 2 Firewall Management Center Virtual イメージを OpenStack Glance サービスにアップロードします。

```
root@ucs-os-controller:$ openstack image create <fmcv_image> --public --disk-
format qcow2 --container-format bare --file ./<fmcv_qcow2_file>
```

ステップ 3 Firewall Management Center Virtual イメージが正常にアップロードされたことを確認します。

root@ucs-os-controller:$ openstack image list

例：

```
root@ucs-os-controller:$ openstack image list
+--------------------------------------+-------------------+---------+
| ID                                   | Name              | Status |+
| b957b5f9-ed1b-4975-b226-4cddf5887991 | fmcv-7-0-image    | active |+
```

アップロードしたイメージとそのステータスが表示されます。

次のタスク

`deploy_os_infra.yaml` テンプレートを使用してネットワーク インフラストラクチャを作成します。

OpenStack と Firewall Management Center Virtual のネットワーク インフラストラクチャの作成

OpenStack インフラストラクチャの Heat テンプレートを展開して、ネットワーク インフラストラクチャを作成します。

始める前に

Heatテンプレートファイルは、フレーバ、ネットワーク、サブネット、ルータインターフェイス、セキュリティグループルールなど、ネットワーク インフラストラクチャ、および Firewall Management Center Virtual に必要なコンポーネントを作成するために必要です。

- `env.yaml`：イメージ名、インターフェイス、IPアドレスなど、コンピューティングノードで Firewall Management Center Virtual をサポートするために作成するリソースを定義します。
- `deploy_os_infra.yaml`：ネットワークやサブネットなど、Firewall Management Center Virtual の環境を定義します。

Firewall Management Center Virtual バージョンのテンプレートは、GitHub リポジトリの FMCv OpenStack Heat テンプレートから入手できます。

重要 シスコが提供するテンプレートはオープンソースの例として提供しているものであり、通常の Cisco TAC サポートの範囲内では扱われていません。更新と ReadMe の手順については、GitHub を定期的に確認してください。

手順

ステップ 1 インフラストラクチャ Heat テンプレートファイルを展開します。

root@ucs-os-controller:$ openstack stack create <stack-name> -e <environment files name> -t <deployment file name>

例：

```
root@ucs-os-controller:$ openstack stack create infra-stack -e env.yaml -t deploy_os_infra.yaml
```

ステップ 2 インフラストラクチャ スタックが正常に作成されたかどうかを確認します。

root@ucs-os-controller:$ openstackstack list

例：

```
root@ucs-os-controller:$ openstack stack list
+--------------------------------------+------------+----------------------------------+-----------------+
| ID                                   | Stack Name  | Project                          | Stack
Status    |
+--------------------------------------+------------+----------------------------------+-----------------+
| b30d5875-ce3a-4258-a841-bf2d09275929 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
+--------------------------------------+------------+----------------------------------+-----------------+
```

次のタスク

OpenStack で Firewall Management Center Virtual インスタンスを作成します。

OpenStack での Firewall Management Center Virtual インスタンスの作成

Heat テンプレートのサンプルを使用して、OpenStack に Firewall Management Center Virtual を展開します。

始める前に

OpenStack で Firewall Management Center Virtual を展開するには、次の Heat テンプレートが必要です。

- `deploy_fmcv.yaml`

Firewall Management Center Virtual バージョンのテンプレートは、GitHub リポジトリの FMCv OpenStack Heat テンプレートから入手できます。

重要 シスコが提供するテンプレートはオープンソースの例として提供しているものであり、通常の Cisco TAC サポートの範囲内では扱われていません。更新と ReadMe の手順については、GitHub を定期的に確認してください。

手順

ステップ 1 Firewall Management Center Virtual Heat テンプレートファイル（`ddeploy_fmcv.yaml`）を展開して、Firewall Management Center Virtual インスタンスを作成します。

root@ucs-os-controller:$ openstack stack create fmcv-stack -e env.yaml-t deploy_fmcv.yaml

例：

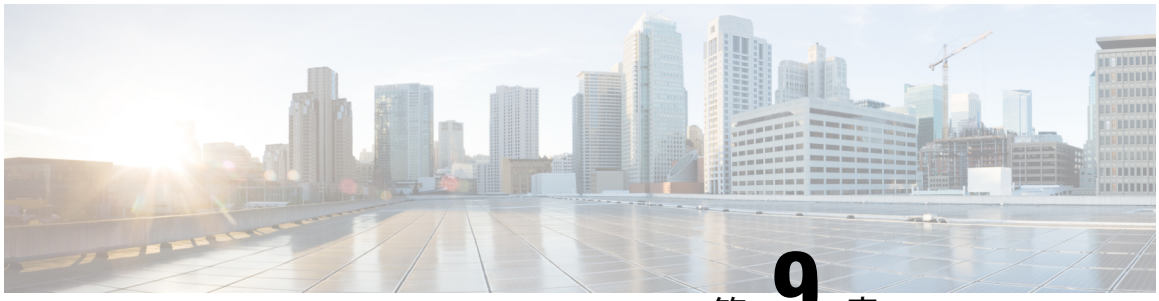
```
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| id                  | 96c8c126-107b-4733-8f6c-eb15a637219f |
| stack_name          | fmcv-stack                           |
| description         | FMCv template                        |
| updated_time        | None                                 |
| stack_status        | CREATE_IN_PROGRESS                   |
| stack_status_reason | Stack CREATE started                 |
+---------------------+--------------------------------------+
```

ステップ 2 Firewall Management Center Virtual スタックが正常に作成されたことを確認します。

root@ucs-os-controller:$ openstack stack list

例：

```
+--------------------------------------+-------------+----------------------------------+--------+
| ID                                   | Stack Name  | Project                          | Stack
Status    |
+--------------------------------------+-------------+----------------------------------+----------------+
| 14624af1-e5fa-4096-bd86-c453bc2928ae | fmcv-stack  | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
| 198336cb-1186-45ab-858f-15ccd3b909c8 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
+--------------------------------------+-------------+----------------------------------+----------------+
```



第 9 章

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 （127 ページ）
- 注意事項と制約事項 （129 ページ）
- Firewall Management Center Virtual の導入 （130 ページ）
- 仮想アプライアンスの電源投入と初期設定 （132 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 *17 : 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 *18 : 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、Firewall Management Center に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 （26ページ）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 （163 ページ）」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。

第 10 章

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 （135 ページ）
- 前提条件 （136 ページ）
- 注意事項と制約事項 （137 ページ）
- Firewall Management Center Virtual の導入 （138 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。
- 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
Firewall Management Center 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 Firewall Management Center 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

- Firewall Management Center 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 （136 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 （138 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 （139 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 （143 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 （143 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。

Nutanix への Firewall Management Center Virtual の展開

- 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

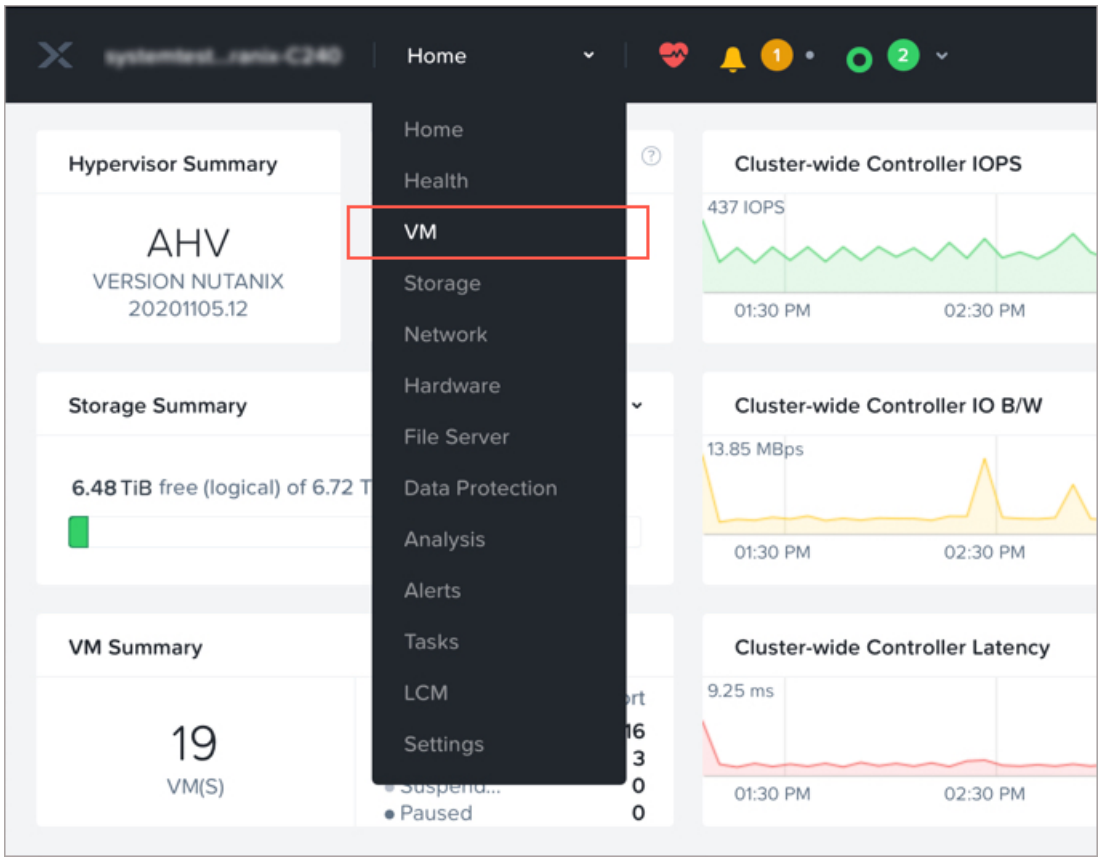
展開する Firewall Management Center Virtual のイメージが [イメージの設定（Image Configuration）] ページに表示されていることを確認します。

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。

Nutanix への Firewall Management Center Virtual の展開



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。

Nutanix への Firewall Management Center Virtual の展開

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 Firewall Management Center 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 （143 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 （144 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。

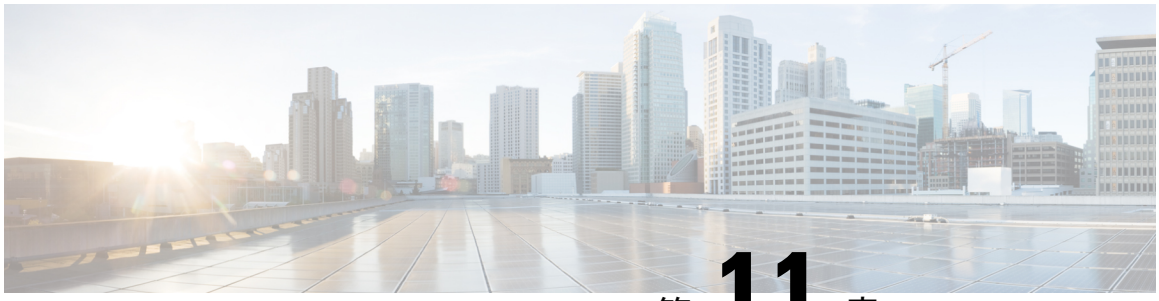
ステップ 3 完了したら、[適用（Apply）] をクリックします。Firewall Management Center Virtual が選択内容に従って設定されます。中間ページが表示されたら、管理者ロールを持つ admin ユーザーとして Web インターフェイスにログインしています。

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 （163 ページ）」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。



第 11 章

Alibaba クラウドへの Cisco Secure Firewall Management Center Virtual の展開

- 概要 （147 ページ）
- 注意事項と制約事項 （148 ページ）
- 前提条件 （149 ページ）
- Firewall Management Center Virtual の導入 （149 ページ）

概要

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。

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。

（注） Alibaba Cloud 上の Management Center Virtual は、Cisco Secure Firewall バージョン 7.2 以降のリリースでサポートされています。

Alibaba Cloud がサポートするインスタンスタイプ

Alibaba Cloud 上の Management Center Virtual では、次の表に記載されているインスタンスタイプを使用できます。

ネットワーク拡張マシンタイプ		
設定	vCPU の数	メモリ（GB）
ecs.r6.xlarge	4	32

（注） Management Center Virtual では、インスタンスをサポートするために少なくとも 1 つのインターフェイス（ENI）が必要です。

ネットワーク要件

- 基本的な Management Center Virtual サポート用に、最低 1 つの vSwitch（サブネット）を持つ VPC を 1 つ作成します。
- インスタンスの展開先と同じゾーンに vSwitch がない場合は作成する必要があります。

関連資料

インスタンスタイプと各タイプの設定の詳細については、Alibaba Cloud を参照してください。

注意事項と制約事項

サポートされる機能

- QCOW2 イメージパッケージ
- 基本的な製品の稼働
- Day-0 構成
- 公開キーまたはパスワードを使用した SSH。
- Alibaba Cloud UI の停止/再起動
- サポートされるインスタンスタイプ：ecs.r6.xlarge。
- BYOL ライセンスのサポート

サポートされない機能

- FDM
- 高可用性
- 自動スケーリング
- IPv6
- SR-IOV

制限事項

- Alibaba Cloud では、トランスペアレントモード、インラインモード、およびパッシブモードはサポートされていません。
- East-West トラフィックは、Alibaba Cloud ではサポートされていません。
- ジャンボフレームは、Alibaba Cloud のいくつかのインスタンスタイプに限定されているため、サポートされていません。詳細については、Alibaba Cloud を参照してください。

前提条件

- Alibaba Cloud のアカウント。https://www.alibaba.com/ で 1 つ作成できます。
- Management Center Virtual のコンソールにアクセスするには、SSH クライアント（例：Windows の場合は PuTTY、Macintosh の場合はターミナル）が必要です。
- Cisco.com から Management Center Virtual の QCOW2 ファイルをダウンロードします。
- 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。

- Cisco スマートアカウント。Cisco Software Central で作成できます。 https://software.cisco.com/
- Firewall Management Center 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 Admin Guide』 の「Licenses」を参照してください。

Firewall Management Center Virtual の導入

展開する 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 https://www.alibabacloud.com/ にログインし、地域を選択します。

（注）
Alibaba Cloud は互いに分離された複数の地域に分割されています。地域は、ウィンドウの右上隅に表示されます。ある地域内のリソースは、別の地域には表示されません。目的の地域内に存在していることを定期的に確認してください。

ステップ 2 カスタム仮想化イメージを作成します。

Alibaba Cloud は QCOW2 イメージのみをサポートしています。

a) Object Storage Service（OSS）に移動して、QCOW2 イメージを含むバケットを作成し、以下を実行します。

バケット名は、Alibaba Cloud プロジェクト内でグローバルに一意である必要があります。

1. ローカルディレクトリから Alibaba Cloud バケットに QCOW2 イメージをアップロードします。
2. 左側のナビゲーションウィンドウで、**[バケット（Buckets）] > [Management Center Virtualバケット（management center virtualbucket）] > [アップロード（Upload）]**の順にクリックします。
3. アップロードが正常に完了したら、[プライベート（Private）] を ACL として選択し、オブジェクトの詳細に記載されている OSS オブジェクトアドレスをコピーします。
4. バケットからカスタムイメージの OSS オブジェクトアドレスを貼り付けます。
5. [Linux] を OS としてを選択し、[その他のLinux（Others Linux）] をバリアントタイプとして選択します。
6. システムアーキテクチャには [x86_64] をシステムアーキテクチャとして選択します。
7. イメージ形式には [QCOW2] を選択します。
8. [BYOL] をライセンス タイプとして 選択します。

b) 前のステップの準仮想化イメージからインスタンスを作成します。

1. 左側のナビゲーションウィンドウで、**[イメージ（Images）]>[カスタムイメージ（Custom Image）]> [アクション（Actions）] > [インスタンスの作成（Create Instance）]**の順にクリックします。

ステップ 3 カスタム仮想化イメージからインスタンスを作成します。

a) **Elasticコンピューティング サービス（Elastic Compute Service）] > [インスタンスの作成（Create Instance）]**に移動して、以下を選択します。

1. [課金方式 （Billing Method）] : 従量制課金（Pay-As-You-Go）
2. [地域（Region）] : 要件に従って選択。
3. [インスタンスタイプ（Instance Type）] : ecs.r6.xlarge
4. [数量（Quantity）] : 必要に応じて設定。
5. [イメージ（Image）] : 前の項で作成したカスタム イメージ。
6. [システムディスク（System Disk）] : 最小値の 250GB（またはデフォルト値）。

b) さらに続行するには、以下を実行します。

1. [VPC] : Management Center Virtual が導入される VPC。
2. [Vswitch] : プライマリインターフェイスのサブネット。

3. [パブリックIPv4アドレスの割り当て（Assign Public IPv4 Address）]：SSH を使用して接続する必要があります（選択されていない場合、Management Center Virtual には、UI から Alibaba Cloud のコンソール接続を介してのみアクセスできます）。
4. [セキュリティグループ（Security Group）] : 適切なセキュリティグループを選択します。
5. [インターフェイス（Interfaces）] : プライマリ インターフェイスは、手順2で選択したサブネットに属しています。Management Center Virtual には 1 つのインターフェイスのみ必要です。

c) 次のセクションに移動して、以下を実行します。

1. [キーペア（Key-Pair）] : キーベースのログインの場合、まだ行われていない場合はキー ペアを生成します。パスワードを使用してインスタンスにアクセスすることもできます。

（注）
既存のキーペアを選択するか、新しいキーペアを作成できます。キーペアは、Alibaba Cloud が保存する公開キーと、ユーザーが保存する秘密キーファイルで構成されます。これらを一緒に使用すると、インスタンスに安全に接続できます。キーペアはインスタンスへの接続に必要な場合があるため、必ず既知の場所に保存してください。

2. [インスタンス名（Instance-name）] : 適切なインスタンスの名前。
3. [Day-0（ユーザーデータ）（Day-0 (User Data)）] : 要件に従って Day-0 構成を指定します（**Base64** でのエンコードは選択しないでください）。

Management Center を使用して Management Center Virtual を管理するためのサンプル Day-0 構成：

```
#FMC
{
"AdminPassword": "<enter_your_password>",
"Hostname": "<Hostname-vFMC>"
}
```

（注）
Day-0 構成でユーザーがパスワードを指定しない場合、デフォルトのパスワードは、Alibaba Cloud コンソールまたは CLI に表示される FMCv のインスタンス ID になります。

d) 利用規約に同意してインスタンスを作成します。

ステップ 4 [確認して起動する（Review and Launch）] をクリックします。
ステップ 5 [起動（Launch）] をクリックします。
ステップ 6 既存のキー ペアを選択するか、新しいキー ペアを作成します。
ステップ 7 [インスタンスの起動（Launch Instances）] をクリックします。
ステップ 8 [起動の表示（View Launch）] をクリックし、プロンプトに従います。
ステップ 9 **[インスタンス（Instance）] > [詳細（More）] > [運用とトラブルシューティング（Operations and Troubleshooting）] > [インスタンスシステムログの取得（Get Instance System Logs）]**に移動します。

第 12 章

Hyper-V での Firewall Management Center Virtual の展開

Microsoft Hyper-V は、「ハイパーバイザ」とも呼ばれる Microsoft のハードウェア仮想化プラットフォームです。Hyper-V を使用すると、管理者は同じ物理サーバーを使用して複数の仮想マシンを実行することで、ハードウェアをより効率的に使用できます。

仮想マシンは、物理ハードウェア上で1つのオペレーティングシステムのみを実行するよりも柔軟性が高く、コストを削減できるので、より効率的にハードウェアを使用できます。

この章は、次の項で構成されています。

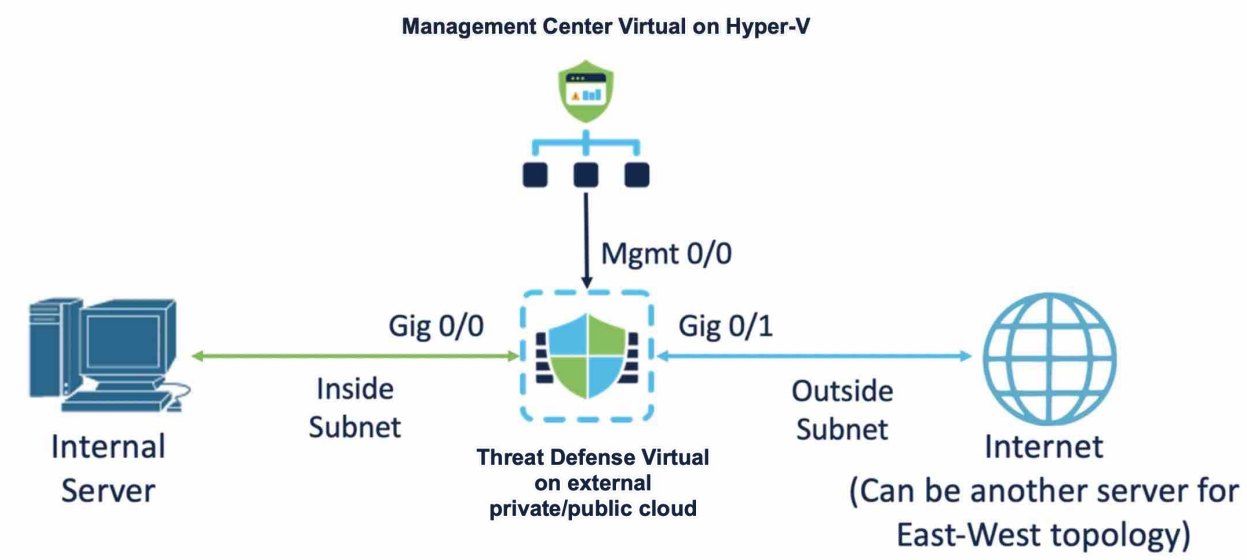
- 概要 （153 ページ）
- Hyper-V での Management Center Virtual のトポロジ例 （154 ページ）
- Management Center Virtual でサポートされる Windows Server （154 ページ）
- Hyper-V での Management Center Virtual のガイドラインと制限事項 （155 ページ）
- Hyper-V での Management Center Virtual の展開用ライセンス （155 ページ）
- Hyper-V での Management Center Virtual の展開に必要な前提条件 （155 ページ）
- Management Center Virtual の展開 （156 ページ）
- 展開の確認 （159 ページ）
- 最初のブートログへのアクセス （159 ページ）
- Management Center Virtual のシャットダウン （160 ページ）
- Management Center Virtual の再起動 （160 ページ）
- Management Center Virtual の削除 （160 ページ）
- トラブルシューティング （161 ページ）

概要

Management Center Virtual は、Cisco.com で入手可能な VHD イメージを使用して Hyper-V に展開されます。管理インターフェイスの基本的な VM 制御機能（コンソールアクセス、停止/再起動、IPv4、IPv6 のサポート）がサポートされています。初期設定は、Day-0 構成スクリプトを使用して行われます。高可用性はサポートされていません。

Hyper-V での Management Center Virtual のトポロジ例

このトポロジ例では、Management Center Virtual が外部のプライベートクラウドまたはパブリッククラウドに展開された Threat Defense Virtual の管理ポートに接続されます。Threat Defense Virtual はインターネットと内部サーバーの両方に接続されています。インターネットは、East-West トラフィックフロートポロジ内の別のサーバーにすることもできます。



Management Center Virtual でサポートされる Windows Server

Management Center Virtual 25 は、Windows Server 2019 および Windows Server 2025 Standard Edition でサポートされています。Management Center Virtual の最小リソース要件は次のとおりです。

- CPU：vCPU x 4
- RAM：28 GB（32 GB を推奨）
- ディスクストレージ：250 GB
- インターフェイスの最小数：1

Hyper-V での Management Center Virtual のガイドラインと制限事項

- Hyper-V に展開された Management Center Virtual を使用して、他のパブリッククラウドまたはプライベートクラウドに展開されている Threat Defense Virtual クラスタを管理できます。ただし、パブリッククラウドに展開された Threat Defense Virtual クラスタを管理するには、Management Center Virtual にクラスタを手動で登録する必要があります。「Add the Cluster to the Management Center (Manual Deployment)」を参照してください。
- クローニングはサポートされていません。

Hyper-V での Management Center Virtual の展開用ライセンス

次のライセンスタイプがサポートされています。

- BYOL
  - スマートライセンス
  - 特定のライセンス予約（SLR）
  - ユニバーサル永久ライセンス登録（PLR）
- 評価ライセンス

Hyper-V での Management Center Virtual の展開に必要な前提条件

- Hyper-V ロールと Hyper-V マネージャがインストールされた Microsoft Windows Server。『Get Started with Hyper-V on Windows Server』を参照してください。
- Cisco.com から Management Center Virtual の圧縮 VHD イメージをダウンロードします。
- BYOL ライセンス
- 新しい仮想スイッチ（vSwitch）と仮想マシン（VM）

Management Center Virtual の展開

Hyper-V に Management Center Virtual を展開するには、次の手順を実行します。

Management Center Virtual の VHD イメージをダウンロード

シスコ ダウンロード ソフトウェアページから Management Center Virtual 圧縮 VHD イメージをダウンロードします。

1. [製品（Products）] > [セキュリティ（Security）] > [ファイアウォール（Firewalls）] > [ファイアウォール管理（Firewall Management）] > [Cisco Secure Firewall Management Center Virtual] の順に移動します。
2. [Firepower Management Centerソフトウェア（Firepower Management Center Software）] をクリックし、必要な VHD イメージをダウンロードします。例：Cisco_Secure_FW_Mgmt_Center_Virtual_Azure-7.4.0- xxxx.vhd.tar.

第 0 日のコンフィギュレーション ファイルの準備

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 ファイルを準備する必要があります。このファイルは、VM 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ローカルマシンに格納され、さらに day0.iso ファイルへと変換されます。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 ファイルで次のパラメータを指定します。

- 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。

（注） 次の例では 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。

手順

ステップ 1 「**day0-config**」というテキストファイルに Management Center Virtual の CLI 設定を記入します。ネットワーク設定と Management Center Virtual の管理に関する情報を追加します。

```
{
"EULA": "accept",
"Hostname": "virtual731265",
"AdminPassword": "r2M$9^Uk69##",
"DNS1": "208.67.222.222",
"DNS2": "208.67.222.222",
"IPv4Mode": "Manual",
"IPv4Addr": "10.10.0.92",
"IPv4Mask": "255.255.255.224",
"IPv4Gw": "10.10.0.65",
"IPv6Mode": "Manual",
"IPv6Addr": "2001:420:5440:2010:600:0:45:45",
"IPv6Mask": "112",
"IPv6Gw": "2001:420:5440:2010:600:0:45:1"
}
```

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。

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

または

```
/ usr/bin/mkisofs -r -o day0.iso day0-config
```

仮想スイッチの新規作成

仮想スイッチ（vSwitch）を新規作成するには、次の手順を実行します。

手順

ステップ 1 Hyper-V マネージャの [アクション（Action）] タブで、[仮想スイッチマネージャ（Virtual Switch Manager）] をクリックします。

ステップ 2 [仮想スイッチ（Virtual Switches）] > [新しい仮想ネットワークスイッチ（New virtual network switch）] をクリックします。

ステップ 3 [仮想スイッチの作成（Create virtual switch）] ウィンドウで、[外部（External）] を選択します。

ステップ 4 [仮想スイッチを作成する（Create Virtual Switch）] をクリックします。

ステップ 5 [仮想スイッチのプロパティ（Virtual Switch Properties）] ウィンドウで、仮想スイッチの名前を入力します。

ステップ 6 外部または内部 vSwitch を作成します。

- 外部 vSwitch を作成するには、[外部ネットワーク（External network）] を選択し、ドロップダウンリストから必要な物理アダプタを選択します。

- 内部 vSwitch を作成するには、[内部ネットワーク（Internal network）] または [プライベートネットワーク（Private network）] を選択します。

ステップ 7 [VLAN ID] で、[管理オペレーティングシステムの仮想LAN IDを有効にする（Enable virtual LAN identification for management operating system）] の横にあるチェックボックスをオンにします。

ステップ 8 [OK] をクリックします。

仮想マシンの新規作成

次の手順に従って、VM を新規作成します。

手順

ステップ 1 Hyper-V マネージャで、[アクション（Action）] > [新規（New）] > [仮想マシン（Virtual Machine）] をクリックします。

ステップ 2 [新規仮想マシンウィザード（New Virtual Machine Wizard）] ダイアログボックスで [次へ（Next）] をクリックします。

ステップ 3 VM の名前を入力し、[Next] をクリックします。

ステップ 4 [世代1（Generation 1）] を選択し、[次へ（Next）] をクリックします。

ステップ 5 VM に割り当てる必要がある起動メモリまたは RAM の容量を MB 単位で指定します（28672 MB 以上、32768 MB を推奨）

ステップ 6 ドロップダウンリストから必要な vSwitch の接続方法を選択します。

ステップ 7 [既存の仮想ハードディスクを使用する（Use an existing virtual hard disk）] を選択し、[参照（Browse）] をクリックして、ダウンロードした Management Center Virtual の VHD イメージを選択します。

ステップ 8 [終了（Finish）] をクリックして、VM を作成します。

ステップ 9 仮想マシンを作成した後は、仮想マシンの仮想プロセッサ（vCPU）の数を増やすことが重要です。デフォルト値は *1* に設定されています。

a) **Hyper-V マネージャ**で、作成した仮想マシンを右クリックして **[設定（Settings）]** をクリックします。
仮想マシンの **[設定（Settings）]** ウィンドウが表示されます。

b) 左側のペインで、**[ハードウェア（Hardware）]** の下にある **[プロセッサ（Processor）]** をクリックします。
[プロセッサ（Processor）] ダイアログボックスが右側のペインに表示されます。

c) **[仮想プロセッサ数：（Number of virtual processors:）]** フィールドで、値を **4** に設定します。

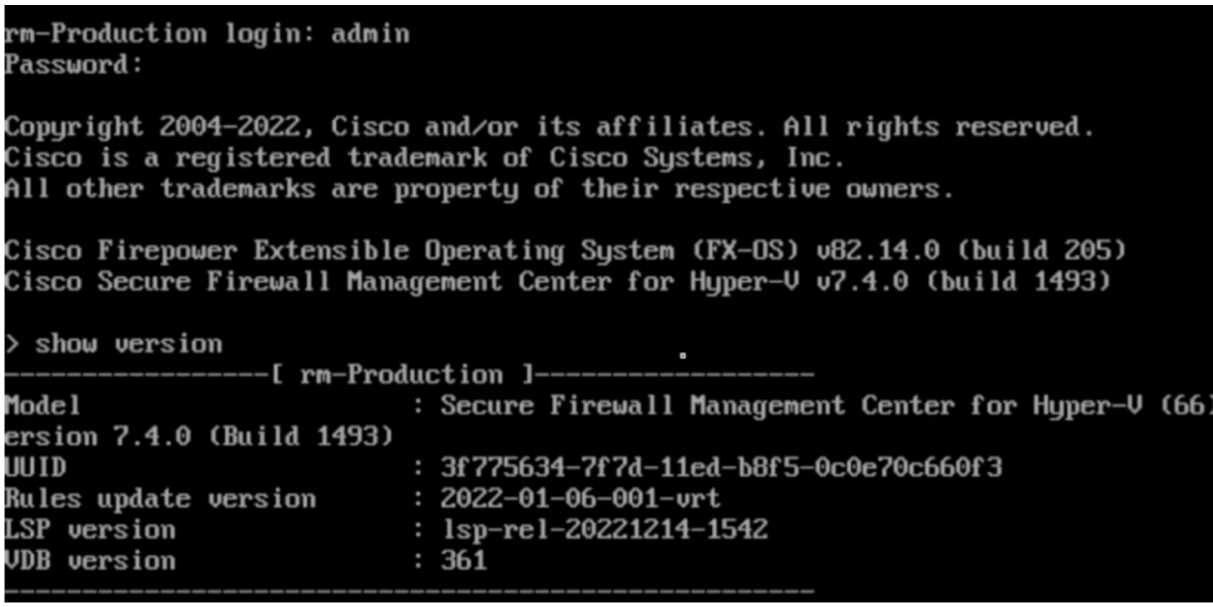
（注）
最適なパフォーマンスを得るには、vCPU（仮想プロセッサ）の値を *8* に設定することを推奨します。仮想マシンには、少なくとも *4* つの vCPU（仮想プロセッサ）が必要であることに注意してください。

最小リソース要件の詳細については、Management Center Virtual でサポートされる Windows Server （154 ページ） を参照してください。

d) [OK] をクリックします。

展開の確認

シリアルコンソールで **show version** コマンドを実行し、Management Center Virtual が Hyper-V に展開されていることを確認します。



最初のブートログへのアクセス

最初のブートログにアクセスするには、Hyper-V マネージャで作成した VM をオンにする前に、次の手順を実行します。

手順

ステップ 1 Hyper-V マネージャで新しく作成した VM を選択し、ウィンドウの右側にある [アクション（Actions）] セクションで [設定（Settings）] をクリックします。

ステップ 2 [ハードウェア（Hardware）] セクションで [COM1] をクリックし、[Named Pipe（名前付きパイプ）] を選択します。

ステップ 3 パイプの名前を入力します。たとえば、**virtual1** のようになります。名前付きパイプのパスをメモします。

ステップ 4 [適用 (Apply)] をクリックし、[OK] をクリックします。

ステップ 5 作成した VM をクリックし、ウィンドウの右側にある [アクション（Actions）] ウィンドウで [開始（Start）] をクリックします。VM の [状態（State）] が [起動（Starting）] から [実行中（Running）] に変わります。

ステップ 6 ここで、作成した名前付きパイプを PuTTY などのシリアルクライアントに接続する必要があります。

ステップ 7 ローカルホストに移動し、[PuTTY] ウィンドウを表示します。

ステップ 8 [シリアル回線（Serial line）] フィールドに、先ほどメモしておいた名前付きパイプのパスを入力します。

例：\\.*pipe**virtual1*

ステップ 9 [開く（Open）] をクリックします。[PuTTY] ウィンドウで最初のブートログを確認できるようになりました。

Management Center Virtual のシャットダウン

Hyper-V マネージャで、シャットダウンする VM を右クリックし、[オフにする（Turn Off）] をクリックします。

Management Center Virtual の再起動

Management Center Virtual CLI の **expert** モードで **sudo reboot** コマンドを実行し、グレースフルリブートを開始します。

```
Cisco Firepower Extensible Operating System (FX-OS) v82.14.0
(build 205)
Cisco Secure Firewall Management Center for Hyper-V v7.4.0
(build 1493)
> expert
admin@hyperv-automation:~$ sudo reboot
```

または、Hyper-V マネージャに移動し、シャットダウンする VM を右クリックして、[オフにする（Turn Off）] をクリックすることもできます。

Management Center Virtual の削除

VM がシャットダウンされたら、VM を右クリックして [削除（Delete）] をクリックします。

（注） VM を削除しても、VM に接続されているディスクは削除されません。ディスクは手動で削除する必要があります。

トラブルシューティング

- 問題：VM を起動できず、メモリを初期化できませんでした

  シナリオ：この問題は、VM を初期化するのに十分なディスク容量がない場合に発生します。

  回避策：VHD ファイルが配置されているディスクの容量を確保します。

- 問題：VM をプロビジョニングまたは起動できません。添付ファイルを開けませんでした。

  シナリオ：この問題は、別の VM が新しい VM と同じイメージを使用している場合に発生します。

  回避策：古い VM を削除します。

- 問題：VM の起動に失敗しました。システムメモリが不足しています

  シナリオ：この問題は、設定されたメモリを VM にプロビジョニングするのに十分な RAM がホスト オペレーティング システムで使用できない場合に発生します。

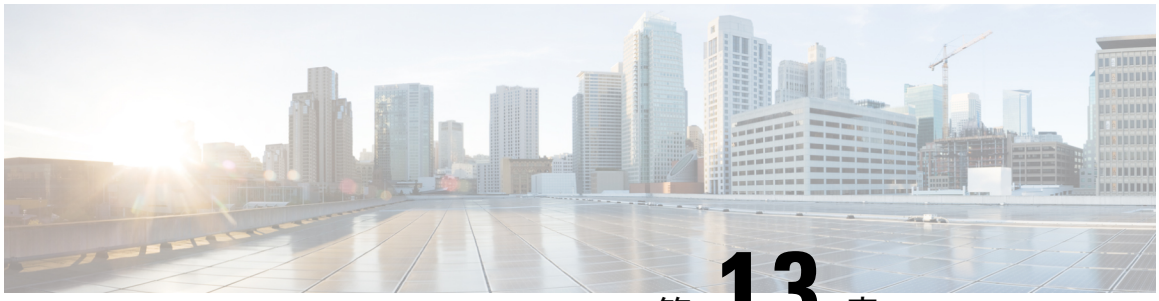
  回避策：必要な RAM がホスト オペレーティング システムで使用可能であることを確認します。

- 問題：Management Center Virtual に SSH 接続できないか、外部ホストから Management Center Virtual の UI をロードできません。

  回避策：Windows ファイアウォールのインバウンドおよびアウトバウンドルールで、ポート 22（SSH）、443（HTTPS）、80（HTTP）を許可します。

- 問題：デバイスがインターネットにアクセスできません。

  回避策：デバイスが外部 vSwitch を使用している場合は、VLAN のゲートウェイが正しく設定されていることを確認します。



第 13 章

Firewall Management Center Virtual 初期設定

この章では、Firewall Management Center Virtual アプライアンスの導入後に実行する必要がある初期セットアッププロセスについて説明します。

- Firewall Management CenterCLI（バージョン 6.5 以降）を使用した初期セットアップ （163 ページ）
- Web インターフェイスを使用したプラットフォームの初期設定（バージョン 6.5 以降）（166 ページ）
- バージョン 6.5 以降の自動初期設定の確認 （171 ページ）

Firewall Management CenterCLI（バージョン 6.5 以降）を使用した初期セットアップ

Firewall Management Center Virtual を展開した後、初期セットアップのためにアプライアンスコンソールにアクセスできます。Web インターフェイスを使用する代わりに、CLI を使用して初期設定を実行できます。初期構成ウィザードを完了させ、信頼できる管理ネットワーク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。ウィザードでは、エンドユーザーライセンス契約（EULA）に同意し、管理者パスワードを変更する必要があります。

始める前に

- Firewall Management Center Virtual が管理ネットワーク上で通信するために必要な次の情報があることを確認してください。
  - IPv4 管理 IP アドレス

    Firewall Management Center インターフェイスは、DHCP によって割り当てられた IPv4 アドレスを受け入れるように事前設定されています。DHCP が Firewall Management Center MAC アドレスに割り当てるように設定されている IP アドレスを確認するには、システム管理者に問い合わせてください。DHCP が使用できないシナリオでは、Firewall Management Center インターフェイスは IPv4 アドレス 192.168.45.45 を使用します。
  - ネットワークマスクとデフォルトゲートウェイ（DHCP を使用しない場合）。

手順

ステップ 1 **admin** アカウントのユーザー名に **admin** を、パスワードに **Admin123** を使用して、コンソールで Firewall Management Center Virtual にログインします。パスワードでは、大文字と小文字が区別されることに注意してください。

ステップ 2 プロンプトが表示されたら、Enter を押してエンドユーザーライセンス契約（EULA）を表示します。

ステップ 3 EULA を確認します。プロンプトが表示されたら、**yes**、**YES** を入力するか、Enter を押して EULA に同意します。

重要
EULA に同意せずに続行することはできません。**yes**、**YES**、または Enter 以外で応答すると、ログアウトされます。

ステップ 4 システムのセキュリティやプライバシーを確保するために、Firewall Management Center に初めてログインするときは、**admin** のパスワードを変更する必要があります。新しいパスワードの入力を求めるプロンプトが表示されたら、表示された制限に従って新しいパスワードを入力し、確認のプロンプトが表示されたら同じパスワードを再度入力します。

（注）
Firewall Management Center では、パスワードをパスワード クラッキング ディクショナリと照合して、英語の辞書に載っている多くの単語だけでなく、一般的なパスワードハッキング技術で簡単に解読できるその他の文字列についてもチェックします。たとえば、「abcdefg」や「passw0rd」などのパスワードは初期設定スクリプトによって拒否される場合があります。

（注）
初期設定プロセスの完了時に、2 つの **admin** アカウント（Web アクセス用と CLI アクセス用）のパスワードは同じ値に設定されます。これは、ご使用のバージョンの『Cisco Secure Firewall Management Center アドミニストレーション ガイド』に記載されている強力なパスワードの要件に準拠しています。その後、いずれかの **admin** アカウントのパスワードを変更すると、パスワードは同じではなくなり、Web インターフェイスの **admin** アカウントから強力なパスワード要件を削除できます。

ステップ 5 プロンプトに応答して、ネットワーク設定を行います。

セットアッププロンプトに従う際に、複数の選択肢がある質問では、選択肢が **(y/n)** のように括弧で囲まれて示されます。デフォルト値は、**[y]** のように大カッコ内に列挙されます。プロンプトに応答する場合は、次の点に注意してください。

- Enter を押して、デフォルトを受け入れます。
- ホスト名に関しては、完全修飾ドメイン名（<hostname>.<domain>）またはホスト名を入力します。このフィールドは必須です。
- DHCP を使用する場合は、割り当てられたアドレスが変更されないように、DHCP 予約を使用する必要があります。DHCP アドレスが変更されると、Firewall Management Center ネットワーク設定が同期しなくなるため、デバイスの登録は失敗します。DHCP アドレスの変更から回復するには、（ホスト名または新しい IP アドレスを使用して）Firewall Management Center に接続し、**[システム（System）]** >

[設定（Configuration）]>**[管理インターフェイス（Management Interfaces）]**に移動してネットワークをリセットします。

- IPv4 を手動で設定することを選択した場合、IPv4 アドレス、ネットマスク、およびデフォルトゲートウェイの入力が求められます。
- DNS サーバーの設定はオプションです。DNS サーバーを指定しない場合は **none** を入力します。それ以外の場合は、1 つまたは 2 つの DNS サーバーに IPv4 アドレスを指定します。2 つのアドレスを指定する場合は、カンマで区切ります。（3 つ以上の DNS サーバーを指定した場合、システムは追加のエントリを無視します）Firewall Management Center にインターネットアクセスがない場合は、ローカルネットワークを出て DNS を使用できません。

  （注）
  評価ライセンスを使用している場合、この時点での DNS の指定はオプションですが、展開の際に永続ライセンスを使用するには DNS が必要です。

- ネットワークから到達可能な少なくとも 1 つの NTP サーバーの完全修飾ドメイン名または IP アドレスを入力する必要があります。（DHCP を使用していない場合は、NTP サーバーの FQDN を指定できません）2 つのサーバー（プライマリとセカンダリ）を指定できます。情報はカンマで区切ります。（3 つ以上の DNS サーバーを指定した場合、システムは追加のエントリを無視します）Firewall Management Center からインターネットにアクセスできない場合は、ローカルネットワークを出て NTP サーバーを使用できません。

例：

```
Enter a hostname or fully qualified domain name for this system [firepower]: fmc
Configure IPv4 via DHCP or manually? (dhcp/manual) [DHCP]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.0.66
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.224
Enter the IPv4 default gateway for the management interface [ ]: 10.10.0.65
Enter a comma-separated list of DNS servers or 'none' [CiscoUmbrella]: 208.67.222.222,208.67.220.220
Enter a comma-separated list of NTP servers [0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org]:
```

ステップ 6 システムによって、設定の選択内容の概要が表示されます。入力した設定を確認してください。

例：

```
Hostname:                           fmc
IPv4 configured via:                manual configuration
Management interface IPv4 address:  10.10.0.66
Management interface IPv4 netmask:  255.255.255.224
Management interface IPv4 gateway:  10.10.0.65
DNS servers:                        208.67.222.222,208.67.220.220
NTP servers:                        0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org
```

ステップ 7 最後のプロンプトで設定を確認することができます。

- 設定が正しい場合は、**y** を入力して **Enter** を押し、設定を承認して続行します。
- 設定が間違っている場合は、 **n** を入力し **Enter** を押します。ホスト名で始まる情報を再入力するように求められます。

例：

```
Are these settings correct? (y/n) y
If your networking information has changed, you will need to reconnect.

Updated network configuration.
```

ステップ 8 設定を承認したら、**exit** と入力して Firewall Management Center CLI を終了します。

次のタスク

- 設定したネットワーク情報を使用して Firewall Management Center Virtual の Web インターフェイスに接続できます。
- 初期設定プロセスの一環として、Firewall Management Center で自動的に設定される週次メンテナンスアクティビティを確認します。このアクティビティは、システムを最新の状態に保ち、データをバックアップする目的で設計されています。バージョン 6.5 以降の自動初期設定の確認 （171 ページ）を参照してください。
- ご使用のバージョンの *Cisco Secure Firewall Management Center* デバイス設定ガイド の説明に従い、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した後で、IPv6 アドレッシング用に Firewall Management Center を設定できます。

Web インターフェイスを使用したプラットフォームの初期設定（バージョン 6.5 以降）

を展開した後、Firewall Management Center Virtualアプライアンスの Web インターフェイスで HTTPS を使用して初期設定を実行できます。

Firewall Management Center の Web インターフェイスへの初回ログイン時に、初期設定ウィザードが Firewall Management Center に表示され、アプライアンスの基本設定をすばやく簡単に実行できます。このウィザードは、次の 3 つの画面と 1 つのポップアップ ダイアログ ボックスで構成されています。

- 最初の画面では、**admin** ユーザーのパスワードをデフォルト値の **Admin123** から変更するよう求められます。
- 2 番目の画面では、シスコ エンドユーザー ライセンス契約（EULA）が表示されます。アプライアンスを使用するには、この内容に同意する必要があります。
- 3 番目の画面では、アプライアンス管理インターフェイスのネットワーク設定を変更できます。このページには現在の設定があらかじめ入力されており、必要に応じて変更できます。
- この画面で入力した値については、ウィザードによる検証が実行されて、次の点が確認されます。
  - 構文の正確性

- 入力値の互換性（たとえば、IPアドレスやゲートウェイに互換性があるか、またFQDNを使用して NTP サーバーが指定されている場合は設定された DNS に互換性があるか）
- Firewall Management Center Virtual と DNS サーバーおよび NTP サーバーとの間のネットワーク接続

これらのテストの結果はリアルタイムで画面上に表示されます。したがって、必要な修正を行い、設定の妥当性をテストしてから、画面の下部にある [終了（Finish）] をクリックできます。NTP および DNS 接続テストは非ブロッキングです。ウィザードが接続テストを完了する前に [終了（Finish）] をクリックすることもできます。[終了（Finish）] をクリックした後に接続の問題が見つかった場合は、このウィザードで設定を変更することはできませんが、初期設定の完了後に Web インターフェイスを使用してその接続を設定できます。

Firewall Management Center Virtual とブラウザとの間の既存の接続を切断することになる設定値を入力した場合、接続テストは実行されません。この場合、DNS または NTP の接続ステータス情報はウィザードに表示されません。

- 3 つのウィザード画面に続いて、ポップアップ ダイアログ ボックスが表示され、必要に応じてスマートライセンスをすばやく簡単に設定できます。

初期設定ウィザードと [スマートライセンス（Smart Licensing）] ダイアログの終了後、[デバイス管理（Device Management）] ページが表示されます。ご使用のバージョンの *Cisco Secure Firewall Management Center デバイス設定ガイド* で「Device Management」を参照してください。

始める前に

- Firewall Management Center が管理ネットワーク上で通信するために必要な次の情報があることを確認してください。
  - IPv4 管理 IP アドレス

    Firewall Management Center インターフェイスは、DHCP によって割り当てられた IPv4 アドレスを受け入れるように事前設定されています。DHCP が Firewall Management Center MAC アドレスに割り当てるように設定されている IP アドレスを確認するには、システム管理者に問い合わせてください。DHCP が使用できないシナリオでは、Firewall Management Center インターフェイスは IPv4 アドレス 192.168.45.45 を使用します。
  - ネットワークマスクとデフォルトゲートウェイ（DHCP を使用しない場合）。
- DHCP を使用していない場合は、次のネットワーク設定を使用して、ローカルコンピュータを設定します。
  - IP アドレス：192.168.45.2
  - ネットマスク：255.255.255.0
  - デフォルト ゲートウェイ：192.168.45.1

このコンピュータの他のネットワーク接続をすべて無効にします。

手順

ステップ 1 Web ブラウザを使用して、 Firewall Management Center Virtual の IP アドレス：*https://<Management Center-IP>* に移動します。

ログイン ページが表示されます。

ステップ 2 管理者アカウントのユーザー名に **admin** を、パスワードに **Admin123** を使用して Firewall Management Center Virtual にログインします（パスワードでは大文字と小文字が区別されます）。

ステップ 3 [パスワードの変更（Change Password）] 画面で、次のようにします。

a) （オプション）この画面の使用中にパスワードが表示されるようにするには、[パスワードの表示（Show password）] チェックボックスをオンにします。

b) （オプション）[パスワードの生成（Generate Password）] ボタンをクリックして、表示されている条件に準拠するパスワードを自動的に作成します（生成されたパスワードは非ニーモニックです。このオプションを選択する場合は、パスワードをメモしてください）。

c) 任意のパスワードを設定するには、[新しいパスワード（New Password）] テキストボックスと [パスワードの確認（Confirm Password）] テキストボックスに新しいパスワードを入力します。

パスワードは、ダイアログに示された条件を満たす必要があります。

（注）
Firewall Management Center では、パスワードをパスワード クラッキング ディクショナリと照合して、英語の辞書に載っている多くの単語だけでなく、一般的なパスワードハッキング技術で簡単に解読できるその他の文字列についてもチェックします。たとえば、「abcdefg」や「passw0rd」などのパスワードは初期設定スクリプトによって拒否される場合があります。

（注）
初期設定プロセスが完了すると、システムは 2 つの **admin** アカウント（1 つは Web アクセス用、もう 1 つは CLI アクセス用）のパスワードを同じ値に設定します。パスワードは、ご使用のバージョンの *Cisco Secure Firewall Management Center アドミニストレーション ガイド* に記載されている強力なパスワード要件に準拠している必要があります。その後、いずれかの **admin** アカウントのパスワードを変更すると、パスワードは同じではなくなり、Web インターフェイスの **admin** アカウントから強力なパスワード要件を削除できます。

d) [次へ（Next）] をクリックします。

[パスワードの変更（Change Password）] 画面で [次へ（Next）] をクリックし、**admin** の新しいパスワードが承認されると、残りのウィザードの手順が完了していなくても、Web インターフェイスと CLI の両方の **admin** アカウントでそのパスワードが有効になります。

ステップ 4 [ユーザー契約（User Agreement）] 画面では、EULA を読み、[同意する（Accept）] をクリックし続行します。

[同意しない（Decline）] をクリックすると、Firewall Management Center Virtual からログアウトされます。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [ネットワークの設定の変更（Change Network Settings）] 画面では次を実行します。

a) [完全修飾ドメイン名（Fully Qualified Domain Name）] を入力します。デフォルト値が表示される場合、ネットワーク設定に対応していれば、それを使用できます。あるいは、完全修飾ドメイン名（シンタックス：`<hostname>.<domain>`）またはホスト名を入力します。

b) [IPv4の設定（Configure IPv4）] オプションでブートプロトコルとして、[DHCPの使用（Using DHCP）] または [スタティック/手動の使用（Using Static/Manual）] を選択します。

DHCP を使用する場合は、割り当てられたアドレスが変更されないように、DHCP 予約を使用する必要があります。DHCP アドレスが変更されると、Firewall Management Center ネットワーク設定が同期しなくなるため、デバイスの登録は失敗します。DHCP アドレスの変更から回復するには、（ホスト名または新しい IP アドレスを使用して）Firewall Management Center に接続し、**[システム（System）]** > **[設定（Configuration）]** > **[管理インターフェイス（Management Interfaces）]**に移動してネットワークをリセットします。

c) [IPv4アドレス（IPv4 Address）] に表示されている値を使用するか（値が表示されている場合）、新しい値を入力できます。ドット付き 10 進法形式を使用します（192.168.45.45 など）。

（注）
初期設定中に IP アドレスを変更した場合は、新しいネットワーク情報を使用して Firewall Management Center に再接続する必要があります。

d) [ネットワークマスク（Network Mask）] に表示されている値を使用するか（値が表示されている場合）、または新しい値を入力できます。ドット付き 10 進法形式を使用します（255.255.0.0 など）。

（注）
初期設定中にネットワークマスクを変更した場合は、新しいネットワーク情報を使用して Firewall Management Center に再接続する必要があります。

e) [ゲートウェイ（Gateway）] に表示されている値を使用するか（値が表示されている場合）、または新しいデフォルトゲートウェイを入力できます。ドット付き 10 進法形式を使用します（192.168.0.1 など）。

（注）
初期設定中にゲートウェイアドレスを変更した場合は、新しいネットワーク情報を使用して、Firewall Management Center への再接続が必要になる場合があります。

f) （オプション）[DNSグループ（DNS Group）] の場合は、デフォルト値の [Cisco Umbrella DNS] を使用します。

DNS 設定を変更するには、ドロップダウンリストから [カスタムDNSサーバー（Custom DNS Servers）] を選択し、[プライマリDNS（Primary DNS）] と [セカンダリDNS（Secondary DNS）] の IPv4 アドレスを入力します。Firewall Management Center にインターネットアクセスがない場合は、ローカルネットワークの外部で DNS を使用することはできません。ドロップダウンリストから [カスタムDNSサーバー（Custom DNS Servers）] を選択し、[プライマリDNS（Primary DNS）] フィールドと [セカンダリDNS（Secondary DNS）] フィールドを空白のままにして、DNS サーバーを設定しません。

（注）

IP アドレスではなく FQDN を使用して NTP サーバーを指定する場合は、この時点で DNS を指定する必要があります。評価ライセンスを使用している場合、DNS はオプションですが、展開の際に永続ライセンスを使用するには DNS が必要です。

g) [NTPグループサーバー（NTP Group Servers）] の場合は、デフォルト値の [デフォルトNTPサーバー（Default NTP Servers）] を受け入れることができます。この場合は、システムでは **0.sourcefire.pool.ntp.org** がプライマリ NTP サーバーとして使用され、**1.sourcefire.pool.ntp.org** がセカンダリ NTP サーバーとして使用されます。

他のNTPサーバーを設定するには、ドロップダウンリストから[カスタムNTPグループサーバー（Custom NTP Group Servers）] を選択し、ネットワークから到達可能な 1 台または 2 台の NTP サーバーの FQDN または IP アドレスを入力します。Firewall Management Center からインターネットにアクセスできない場合は、ローカルネットワークを出て NTP サーバーを使用できません。

（注）
初期設定中にネットワーク設定を変更する場合は、新しいネットワーク情報を使用して Firewall Management Center に再接続する必要があります。

ステップ 7 [終了（Finish）] をクリックします。

ウィザードでは、この画面で入力した値の検証を実行して、構文の正確性、入力した値の互換性、Firewall Management Center と DNS および NTP サーバー間のネットワーク接続を確認します。[終了（Finish）] をクリックした後に接続の問題が見つかった場合は、このウィザードで設定を変更することはできませんが、初期設定の完了後に Firewall Management Center Web インターフェイスを使用してその接続を設定できます。

次のタスク

- スマートライセンシングを迅速かつ簡単にセットアップできるポップアップ ダイアログ ボックスが表示されます。このダイアログボックスの使用は任意です。スマートライセンスについて十分な知識があり、Firewall Management Center Virtual で Firewall Threat Defense を管理する場合は、このダイアログを使用してください。それ以外の場合は、このダイアログを閉じて、ご使用のバージョンの *Cisco Secure Firewall Management Center* アドミニストレーション ガイド で「Licensing」を参照してください。
- 初期設定プロセスの一環として、Firewall Management Center で自動的に設定される週次メンテナンスアクティビティを確認します。このアクティビティは、システムを最新の状態に保ち、データをバックアップする目的で設計されています。バージョン 6.5 以降の自動初期設定の確認 （171 ページ）を参照してください。
- 初期構成ウィザードを完了し、スマートライセンスのダイアログを完了または却下すると、『*Cisco Secure Firewall Management Center Device Configuration Guide*』に記載されている、[デバイス管理（Device Management）] ページが表示されます。
- ご使用のバージョンの *Cisco Secure Firewall Management Center* デバイス設定ガイド の説明に従い、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した後で、IPv6 アドレッシング用に Firewall Management Center を設定できます。

バージョン 6.5 以降の自動初期設定の確認

初期設定の一環として（初期設定ウィザードまたは CLI のどちらで実行しても）、Firewall Management Center によって、メンテナンスタスクが自動的に設定され、システムが最新の状態に保たれるとともに、データがバックアップされます。

タスクは UTC でスケジュールされるため、いつ現地で実行されるかは、日付と場所によって異なります。また、タスクは UTC でスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受ける場合、スケジュールされたタスクは、現地時間を基準とすると、夏期では冬期の場合よりも 1 時間「遅れて」実行されることになります。

（注） 自動スケジュール設定を検証し、Firewall Management Center がスケジュールを正しく確立し、必要に応じて調整しているかを確認することを強くお勧めします。

- 週次 GeoDB 更新

  Firewall Management Center では、毎週、ランダムに選択された時刻に行われるように、GeoDB の更新が自動的にスケジュールされます。Web インターフェイスのメッセージ センターを使用して、この更新のステータスを確認できます。この自動更新の設定は、Web インターフェイスの **[システム（System）]** > **[更新（Updates）]** > **[地理位置情報の更新（Geolocation Updates）]** > [位置情報の定期的な更新（Recurring Geolocation Updates）] で確認できます。システムが更新を設定できず、Firewall Management Center からインターネットに接続できる場合は、ご使用のバージョンの *Cisco Secure Firewall Management Center アドミニストレーション ガイド* の説明に従って、通常の GeoDB 更新を設定することを推奨します。

- Firewall Management Center の週次ソフトウェアアップデート

  Firewall Management Center では、Firewall Management Center およびその管理対象デバイスの最新ソフトウェアをダウンロードするための週次タスクが自動的にスケジュールされます。このタスクは、UTC で日曜日の午前 2 ～ 3 時の間に行われるようにスケジュールされます。したがって、日付と場所に応じて、現地時間では、土曜日の午後から日曜日の午後の範囲内のいずれかの時間帯に行われることになります。Web インターフェイスのメッセージセンターを使用して、このタスクのステータスを確認できます。このタスクの設定は、Web インターフェイスの **[システム（System）]** > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** で確認できます。タスクのスケジューリングに失敗するが、Firewall Management Center がインターネットにアクセスできる場合は、ご使用のバージョンの *Cisco Secure Firewall Management Center アドミニストレーション ガイド* の説明に従って、ソフトウェアの更新をダウンロードする定期タスクをスケジュールすることを推奨します。

  このタスクでは、アプライアンスで現在実行されているバージョンに対するソフトウェア パッチおよびホットフィックスをダウンロードするだけです。このタスクでダウンロードされた更新プログラムのインストールは、別に行う必要があります。詳細については、Cisco Firewall Management Center アップグレードガイド [英語] を参照してください。

- 週次の Firewall Management Center 設定バックアップ

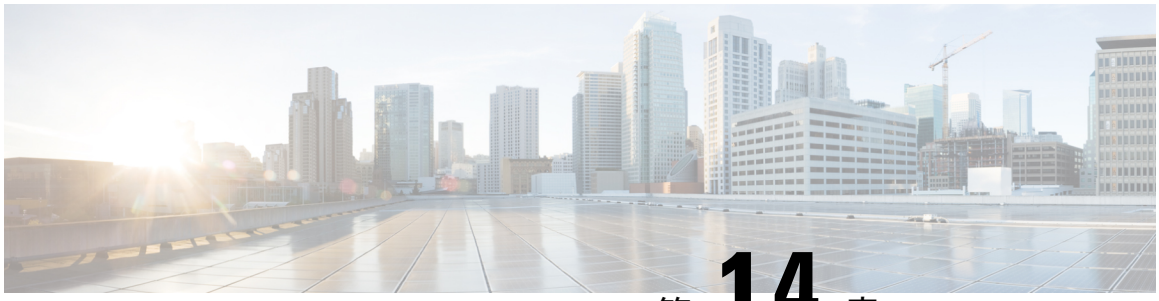
  Firewall Management Center では、ローカルに保存された設定のみのバックアップを実行するための週次タスクが自動的にスケジュールされます。このタスクは、UTC で月曜日の午前 2 時に行われるようにスケジュールされます。したがって、日付と場所に応じて、現地時間では、日曜日の午後から月曜日の午後の範囲内のいずれかの時間帯に行われることになります。Web インターフェイスのメッセージセンターを使用して、このタスクのステータスを確認できます。このタスクの設定は、Web インターフェイスの **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** で確認できます。タスクのスケジューリングに失敗する場合は、ご使用のバージョン *Cisco Secure Firewall Management Center アドミニストレーション ガイド* の説明に従って、バックアップを実行する定期タスクをスケジュールすることを推奨します。

- 脆弱性データベースの更新

  Firewall Management Center バージョン 6.6+ では、 シスコのサポートサイトから最新の脆弱性データベース（VDB）の更新ファイルがダウンロードおよびインストールされます。これは 1 回限りの操作です。Web インターフェイスのメッセージ センターを使用して、この更新のステータスを確認できます。システムを最新の状態に保つために、Firewall Management Center がインターネットにアクセスできる場合は、ご使用のバージョンの *Cisco Secure Firewall Management Center アドミニストレーション ガイド* の説明に従って、自動の定期 VDB 更新のダウンロードとインストールを実行するタスクをスケジュールすることを推奨します。

- 侵入ルールの更新

  Firewall Management Center のバージョン 6.6+ では、 侵入ルールがシスコのサポートサイトから自動的に日次更新されるように設定されます。影響を受けるポリシーが Firewall Management Center で次に展開される際、該当する管理対象デバイスに対して自動侵入ルールの更新が展開されます。Web インターフェイスのメッセージ センターを使用して、このタスクのステータスを確認できます。このタスクの設定は、Web インターフェイスの **[システム（System）] > [更新（Updates）] > [ルールの更新（Rule Updates）]** で確認できます。更新の設定に失敗するが、Firewall Management Center がインターネットにアクセスできる場合は、ご使用のバージョンの *Cisco Secure Firewall Management Center アドミニストレーション ガイド* の説明に従って、通常の侵入ルールの更新を設定することを推奨します。



第 14 章

Firewall Management Center Virtual 初期管理および設定

Firewall Management Center Virtual の初期セットアッププロセスが完了し、正常にセットアップされたことを確認したら、展開の管理を容易にするさまざまな管理タスクを実行することを推奨します。また、ライセンスの取得など、初期設定で省略したタスクも完了する必要があります。以下のセクションで説明するタスクの詳細、およびデプロイメントの設定を開始する方法の詳細については、ご使用のバージョンの『Secure Firewall Management Center Configuration Guide』『』の全文を参照してください。

- 個別のユーザー アカウント （173 ページ）
- デバイス登録 （174 ページ）
- ヘルス ポリシーとシステム ポリシー （175 ページ）
- ソフトウェアとデータベースの更新 （175 ページ）
- トラブルシューティング （176 ページ）

個別のユーザー アカウント

初期設定が完了した時点で、システム上の唯一の Web インターフェイスのユーザーは、管理者ロールとアクセス権を持つ**admin**ユーザーです。その役割を持つユーザーはシステムへのすべてのメニューと設定にアクセスできます。セキュリティおよび監査上の理由から、**admin**アカウント（およびAdministrator ロール）の使用を制限することをお勧めします。ユーザーアカウントは、Firewall Management Center Virtual GUI の **[システム（System）]** > **[ユーザー（Users）]** > **[ユーザー（User）]** ページで管理します。

（注） シェルを使用した Firewall Management Center Virtual へのアクセスと Web インターフェイスを使用した Firewall Management Center Virtual へのアクセスのための **admin** アカウントは異なるため、別のパスワードを使用できます。

システムを使用する各ユーザーに対して個別のアカウントを作成すると、各ユーザーによって行われたアクションと変更を組織で監査できるほか、各ユーザーに関連付けられたユーザーア

クセスロールを制限することができます。これは、ほとんどの設定および分析タスクを実行する Firewall Management Center Virtual で特に重要です。たとえば、アナリストはネットワークのセキュリティを分析するためにイベントデータにアクセスする必要がありますが、展開の管理機能にアクセスする必要はありません。

システムには、Web インターフェイスを使用してさまざまな管理者およびアナリスト用に設計された 10 個の事前定義のユーザー ロールが用意されています。また、特別なアクセス権限を持つカスタム ユーザー ロールを作成することもできます。

デバイス登録

Firewall Management Center は、現在システムでサポートされているすべてのデバイス（物理または仮想）を管理できます。

- Firewall Threat Defense：統合した次世代ファイアウォールと次世代 IPS デバイスを提供します。
- Firewall Threat Defense Virtual：複数のハイパーバイザ環境で作業し、管理オーバーヘッドを削減し、運用効率を向上させるために設計された 64 ビットのバーチャル デバイス。
- Cisco ASA with FirePOWER Services（または ASA FirePOWER モジュール）：最も重要なシステムポリシーを提供し、検出とアクセス制御のために、システムにトラフィックを渡します。ただし、Firewall Management Center の Web インターフェイスを使用して ASA FirePOWER のインターフェイスを設定することはできません。Cisco ASA with FirePOWER Services には、ASA プラットフォームに一意なソフトウェアと CLI があり、これらを使用してシステムをインストールし、他のプラットフォーム固有の管理タスクを実行することができます。
- 7000 および 8000 シリーズ アプライアンス：システム用に特別に設計された物理デバイス。7000 および 8000 シリーズ デバイスのスループットはさまざまですが、多くの同じ機能が共有されます。一般に、8000 シリーズ デバイスは 7000 シリーズ デバイスよりも高性能で、8000 シリーズ 高速パス ルール、リンク集約、およびスタックなどの追加機能もサポートします。デバイスを Firewall Management Center に登録する前に、そのデバイス上でリモート管理を設定する必要があります。
- NGIPSv：VMware vSphere 環境で展開する 64 ビットのバーチャル デバイス。NGIPSv のデバイスは、冗長性とリソースの共有、スイッチ、およびルーティングのようなシステムのハードウェアベースの機能のどちらもサポートしていません。

Firewall Management Center に管理対象デバイスを登録するには、Firewall Management Center GUI の**[デバイス（Device）]** > **[デバイス管理（Device Management）]**ページを使用します。ご使用のバージョンの『Secure Firewall Management Center Configuration Guide』でデバイス管理情報を参照してください。

ヘルス ポリシーとシステム ポリシー

デフォルトでは、すべてのアプライアンスにシステムの初期ポリシーが適用されます。システム ポリシーは、メール リレー ホストのプリファレンスや時間同期の設定など、展開内の複数のアプライアンスで共通している可能性が高い設定を管理します。シスコでは、Firewall Management Center を使用して、それ自体およびその管理対象デバイスすべてに同じシステム ポリシーを適用することを推奨しています。

デフォルトで、Firewall Management Center にはヘルス ポリシーも適用されます。ヘルスポリシーは、ヘルスモニターリング機能の一部として、システムが展開環境内でアプライアンスのパフォーマンスを継続して監視するための基準を提供します。シスコでは、Firewall Management Center を使用して、その管理対象デバイスすべてにヘルス ポリシーを適用することを推奨しています。

ソフトウェアとデータベースの更新

展開を開始する前に、アプライアンス上でシステム ソフトウェアを更新する必要があります。展開環境内のすべてのアプライアンスでシステムの最新のバージョンを実行することを推奨します。展開環境でこれらのアプライアンスを使用する場合は、最新の侵入ルール更新、VDB、および GeoDB もインストールする必要があります。

注意 システムの一部分を更新する前に、その更新に関するリリースノートまたはアドバイザリテキストを読んでおく必要があります。リリースノートでは、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストールおよびアンインストールの手順など重要なデータが提供されます。

Firewall Management Center でバージョン 6.5 以降を実行している場合は、次のようになります。

Firewall Management Center は設定の一環として次のアクティビティを確立し、システムを最新の状態に保ち、データをバックアップします。

- 週次自動 GeoDB 更新
- Firewall Management Center とその管理対象デバイスにおける最新ソフトウェアをダウンロードする週次タスク。

重要 このタスクは、Firewall Management Center にソフトウェアの更新のみをダウンロードします。ユーザーは、このタスクがダウンロードした更新をインストールする必要があります。詳細については、『*Cisco Secure Firewall Management Center Upgrade Guide*』および『』を参照してください。

- ローカルに保存された設定のみの Firewall Management Center バックアップを実行する週次タスク。

Firewall Management Center でバージョン 6.6 以降を実行している場合、初期設定の一環として、Firewall Management Center はシスコのサポートサイトから最新の脆弱性データベース（VDB）の更新をダウンロードしてインストールします。これは 1 回限りの操作です。

Web インターフェイスのメッセージセンターを使用して、これらのアクティビティのステータスを確認できます。システムがこれらのアクティビティのいずれかを設定できず、Firewall Management Center がインターネットにアクセスできる場合は、ご使用のバージョンの『*Secure Firewall Management Center Configuration Guide*』およびの説明に従って、これらのアクティビティをご自身で設定することをお勧めします。

トラブルシューティング

このセクションでは、仮想マシンへの Firewall Management Center Virtual デプロイメントに関連する基本的な障害対応手順について説明します。

SSH 接続の失敗

Firewall Management Center Virtual は完全に動作しており、SSH 接続を除き、ユーザーインターフェイスとコンソール接続は正しく機能しています。特定のシナリオでは、Firewall Management Center Virtual の初回起動中に SSH ホストキーファイルが破損して、SSH 接続が失敗することがあります。

SSH 接続の失敗を示唆する次のような兆候を確認できます。

1. Firewall Management Center Virtual の初回起動中、特に SSH デーモン（sshd）が起動しているときに、ディスク I/O エラーが発生する場合があります。これにより、SSH キーファイル（sshd によって生成される ssh_host* ファイル）が空になります。

```
ls -lrt /etc/ssh total 16

-rw-r--r-- 1 root root 1746 Jan 17 23:31 ssh_config-openssh
-rw-r--r-- 1 root root 6027 Jan 17 23:42 sshd_config
-rw-r--r-- 1 root root 1293 Jan 17 23:42 ssh_config
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_dsa_key
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_dsa_key.pub
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ecdsa_key
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ecdsa_key.pub
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ed25519_key
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_rsa_key
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_rsa_key.pub
```

2. ディスク I/O の問題については、`/var/log/messages` ファイルを確認できます。このファイルには、SSH キーファイルが生成されたときと同じタイムスタンプの前後に（I/O エラーを示す）誤ったデータが含まれている可能性があります。

前述したような、Firewall Management Center Virtual の初回起動中に発生する可能性のある SSH 障害を解決するには、次の手順を実行する必要があります。

1. Firewall Management Center Virtual にログインします。

2. Firewall Management Center Virtual CLI で**エキスパート**モードで **sudo reboot** コマンドを実行し、正常なリブートを開始します。
3. 次のコマンドを実行して、空の SSH キーファイルを削除します。

```
cd /etc/ssh/
rm ssh_host*
```

4. 次のコマンドを実行して `sshd` サービスを再起動し、SSH キーファイルを適切に再生成します。

```
/etc/rc.d/init.d/sshd stop
/etc/rc.d/init.d/sshd start
```

（注） SSH キーファイルが空であることがわかっている場合にのみ、この回避手順を実行してください。不明な場合は、TAC ケースを送信して詳細に調査することをお勧めします。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。