



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

初版：2015年11月10日

最終更新：2023年9月7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/](http://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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2015–2022 Cisco Systems, Inc. All rights reserved.



## 目次

---

第 1 章	<b>Secure Firewall Management Center Virtual アプライアンスの概要</b>	<b>1</b>
	Management Center Virtual のプラットフォームとサポート	1
	Management Center Virtual ライセンス	4
	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
	Management Center Virtual 導入パッケージのダウンロード	8

---

第 2 章	<b>VMware を使用した Management Center Virtual の導入</b>	<b>11</b>
	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	20
	Management Center Virtual の導入	22
	仮想マシンのプロパティの確認	24
	仮想アプライアンスの電源投入と初期設定	25

---

第 3 章	<b>KVM を使用した Management Center Virtual の導入</b>	<b>27</b>
	概要	27
	前提条件	29
	注意事項と制約事項	30
	第 0 日のコンフィギュレーションファイルの準備	31
	Management Center Virtual の導入	33
	導入スクリプトを使用した起動	33

Management Center Virtual の導入	34
OpenStack を使用した起動	36
OpenStack でのコマンドラインを使用した起動	37
OpenStack でのダッシュボードを使用した起動	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 クラウドへの Management Center Virtual の導入 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	47
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	50
Management Center Virtual の導入	51

---

**第 5 章****Microsoft Azure クラウドへの Management Center Virtual の導入 55**

概要	55
前提条件	57
注意事項と制約事項	57
導入時に作成されるリソース	59
Management Center Virtual の導入	60
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	61
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	65
Azure での IPv6 サポート対象 Secure Firewall Management Center Virtual の展開	68

Azure での IPv6 をサポートする展開について	68
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	70
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	76
Management Center Virtual 展開の確認	82
モニタリングおよびトラブルシューティング	85
機能の履歴	86

---

**第 6 章****Google Cloud Platform への Management Center Virtual の展開 87**

概要	87
前提条件	88
注意事項と制約事項	89
ネットワークトポロジの例	89
Management Center Virtual の導入	90
VPC ネットワークの作成	90
ファイアウォールルールの作成	91
GCP 上の Management Center Virtual インスタンスの作成	91
GCP 上の Management Center Virtual インスタンスへのアクセス	93
シリアルコンソールを使用した Management Center Virtual インスタンスへの接続	94
外部 IP を使用した Management Center Virtual インスタンスへの接続	94
Gcloud を使用した Management Center Virtual インスタンスへの接続	95

---

**第 7 章****Oracle Cloud Infrastructure への Management Center Virtual の展開 97**

概要	97
前提条件	99
注意事項と制約事項	99
ネットワークトポロジの例	100
Management Center Virtual の導入	100
仮想クラウドネットワーク (VCN) の設定	100
ネットワークセキュリティグループの作成	101
インターネットゲートウェイの作成	101
サブネットの作成	102

OCI での Management Center Virtual インスタンスの作成	103
OCI 上の Management Center Virtual インスタンスへのアクセス	104
PuTTY を使用した Management Center Virtual インスタンスへの接続	105
SSH を使用した Management Center Virtual インスタンスへの接続	106
OpenSSH を使用した Management Center Virtual インスタンスへの接続	106

---

**第 8 章****OpenStack を使用した Management Center Virtual の展開 109**

概要	109
前提条件	110
注意事項と制約事項	111
システム要件	112
ネットワークトポロジーの例	114
Management Center Virtual の導入	114
OpenStack への Management Center Virtual イメージのアップロード	115
OpenStack と Management Center Virtual のネットワーク インフラストラクチャの作成	115
OpenStack での Management Center Virtual インスタンスの作成	117

---

**第 9 章****Cisco HyperFlex を使用した Management Center Virtual の展開 119**

システム要件	119
注意事項と制約事項	121
Management Center Virtual の導入	122
仮想アプライアンスの電源投入と初期設定	124

---

**第 10 章****Nutanix を使用した Management Center Virtual の展開 125**

システム要件	125
前提条件	126
注意事項と制約事項	127
Management Center Virtual の導入	128
Management Center Virtual QCOW2 ファイルを Nutanix にアップロード	128
第 0 日のコンフィギュレーション ファイルの準備	129
Nutanix への Management Center Virtual の展開	130

Management Center Virtual のセットアップの完了	132
スクリプトを使用したネットワーク設定の構成	133
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	134

---

**第 11 章**
**Hyper-V での Management Center Virtual の展開 135**

概要	135
Hyper-V での Management Center Virtual のトポロジ例	136
Management Center Virtual でサポートされる Windows Server	136
Hyper-V での Management Center Virtual のガイドラインと制限事項	137
Hyper-V での Management Center Virtual の展開用ライセンス	137
Hyper-V での Management Center Virtual の展開に必要な前提条件	137
Management Center Virtual の展開	138
Management Center Virtual の VHD イメージをダウンロード	138
第 0 日のコンフィギュレーション ファイルの準備	138
仮想スイッチの新規作成	139
仮想マシンの新規作成	140
展開の確認	140
最初のブートログへのアクセス	141
Management Center Virtual のシャットダウン	142
Management Center Virtual の再起動	142
Management Center Virtual の削除	142
トラブルシューティング	142

---

**第 12 章**
**Management Center Virtual 初期設定 145**

Management CenterCLI (バージョン 6.5 以降) を使用した初期セットアップ	145
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)	148
バージョン 6.5 以降の自動初期設定の確認	152

---

**第 13 章**
**Management Center Virtual 初期管理および設定 155**

個別のユーザー アカウント	155
デバイス登録	156

ヘルス ポリシーとシステム ポリシー 156  
ソフトウェアとデータベースの更新 157





# 第 1 章

## Secure Firewall Management Center Virtual アプライアンスの概要

Secure Firewall Management Center Virtual（旧 Firepower Management Center Virtual）は、仮想化環境に包括的なファイアウォール機能を提供し、データセンタートラフィックとマルチテナント環境のセキュリティを強化します。Management Center Virtual は物理アプライアンスおよび Secure Firewall Threat Defense Virtual（旧 Firepower Threat Defense Virtual）アプライアンスを管理して、完全な NGIPS アプライアンスと FirePOWER アプライアンスを提供できます。

- [Management Center Virtual のプラットフォームとサポート（1 ページ）](#)
- [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）](#)
- [Management Center Virtual 導入パッケージのダウンロード（8 ページ）](#)

## 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

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** 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。

## 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 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、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 Management Center Virtual インスタンスでは 32 GB RAM、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 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。

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

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、次の点の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。

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 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、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、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、Management Center に接続し（ホスト名または新しい IP アドレスを使用）、**システム (⚙️) > [構成 (Configuration)] > [管理インターフェイス (Management Interfaces)]** の順に選択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**：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、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。

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** : 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** : 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** : 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 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

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)** : 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)** : 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)** : 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** : Management Center Virtual を Azure Cloud に導入できます。
- **Google Cloud Platform (GCP)** : Management Center Virtual をパブリック GCP に導入できます。
- **Oracle Cloud Infrastructure (OCI)** : Management Center Virtual を OCI に導入できます。
- **OpenStack** : 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** : 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 Management Center Virtual を Nutanix 環境に導入できます。
- **Alibaba Cloud** : Management Center Virtual を Alibaba Cloud に導入できます。



- (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 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。

## Management Center Virtual ライセンス

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、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。

## 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。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) Management Center はデバイスの機能ライセンスを管理しますが、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。

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 Threat Defense および 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 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 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
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

コンポーネント	FMCv2/FMCv10/FMCv25	FMCv300
最大イベントレート (イベント数/秒)	5,000	12,000 eps

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

すべての Management Center Virtual 実装に同じ RAM 要件が適用され、32 GB が推奨、28 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メモリが 28 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 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 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 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 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	28 GB 以上 (推奨 32 GB) 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	28 GB 以上 (推奨 32 GB) 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	<p>インスタンスのサイズを変更します。</p> <ul style="list-style-type: none"> <li>• c3.xlarge から c3.4xlarge へ。</li> <li>• c3.2.xlarge から c3.4xlarge へ。</li> <li>• c4.xlarge から c4.4xlarge へ。</li> <li>• c4.2xlarge から c4.4xlarge へ。</li> </ul> <p>また、新規展開用に c5.4xlarge インスタンスも用意しています。</p>	<p>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。</p> <p>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。</p>
Azure	<p>インスタンスのサイズを変更します。</p> <ul style="list-style-type: none"> <li>• Standard_D3_v2 から Standard_D4_v2 へ。</li> </ul>	<p>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。</p> <p>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。</p>
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、「 <a href="#">GCP マシンタイプのサポート</a> 」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、「 <a href="#">OCI のコンピューティングシェイプ</a> 」を参照してください。
OpenStack	28 GB 以上（推奨 32 GB）を割り当てます。	詳細については、「 <a href="#">メモリとリソースの要件</a> 」を参照してください。
[HyperFlex]	28 GB 以上（推奨 32 GB）を割り当てます。	詳細については、「 <a href="#">ホストシステム要件</a> 」を参照してください。
Nutanix	28 GB 以上（推奨 32 GB）を割り当てます。	詳細については、「 <a href="#">ホストシステム要件</a> 」を参照してください。

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

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 Management Center 内からダウンロードできます。

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。

**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 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、[Firepower Management Center Virtual アプライアンス (Firepower Management Center Virtual Appliance)] 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 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
Management Center Virtual	ソフトウェアのインストール: VMware	Cisco_Firepower_Management_Center_Virtual_VMware-version.tar.gz
	ソフトウェアのインストール: KVM	Cisco_Firepower_Management_Center_Virtual-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。



- 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 を使用した Management Center Virtual の導入 \(11 ページ\)](#) を参照してください。
- Management Center Virtual を、KVM ハイパーバイザを実行している Linux サーバーに展開する場合は、[KVM を使用した Management Center Virtual の導入 \(27 ページ\)](#) を参照してください。
- Management Center Virtual を AWS に展開する場合は、[AWS クラウドへの Management Center Virtual の導入 \(41 ページ\)](#) を参照してください。
- Management Center Virtual を Azure に展開する場合は、[Microsoft Azure クラウドへの Management Center Virtual の導入 \(55 ページ\)](#) を参照してください。
- 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。
- 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 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 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 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。
- Management Center Virtual を Hyper-V に展開する場合は、[Hyper-V での Management Center Virtual の展開 \(135 ページ\)](#) を参照してください。





## 第 2 章

# VMware を使用した Management Center Virtual の導入

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

- [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](#) (20 ページ)
- [Management Center Virtual の導入](#) (22 ページ)
- [仮想マシンのプロパティの確認](#) (24 ページ)
- [仮想アプライアンスの電源投入と初期設定](#) (25 ページ)

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

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

表 3: 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 が動作していません。	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。 <a href="#">スナップショットのサポート (18 ページ)</a> 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。 <a href="#">vMotion のサポート (18 ページ)</a> 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

## 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 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、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 Management Center Virtual インスタンスでは 32 GB RAM、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 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 Firepower Compatibility Guide](#)』を参照してください。



**重要** 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。

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 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、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** 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。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: 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 <b>重要</b> アップグレード時の新しいメモリ診断機能が 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、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	8	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: 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

設定	デフォルト	設定調整の可否
ハードディスク プロビジョニング サイズ	2.2 TB	非対応

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™)テクノロジー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 への導入用 : Cisco\_Firepower\_Management\_Center\_Virtual\_VMware-VI-X.X.X-xxx.ovf
- ESXi (vCenter なし) への導入用 :  
Cisco\_Firepower\_Management\_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、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 OVF 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 (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)、シック プロビジョニング (Eager Zeroed)、シンプロビジョニングの中から選択します。
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

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、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、「[Management Center Virtual 初期設定 \(145 ページ\)](#)」を参照してください。

システムを正常に動作させるには、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。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、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、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 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 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。
- Management Center Virtual HA を確立するには、Management Center Virtual では、HA 構成で管理する 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 Threat Defense 機能のライセンス権限は、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、[Firepower Management Center コンフィギュレーションガイド](#)の「License Requirements for FTD Devices in a High Availability Pair」を参照してください。

- Management Center Virtual HA ペアを解除すると、追加の Management Center Virtual ライセンス権限が解放され、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、[Firepower Management Center コンフィギュレーションガイド](#)の「Establishing Firepower Management Center High Availability」を参照してください。

### INIT Respanning 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 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 device)] 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。

- 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 のリリース以降、VMware 上の Threat Defense Virtual と Management Center Virtual では、仮想デバイスを作成する際のデフォルトインターフェイスが vmxnet3 になりました。以前は、デフォルトは e1000 でした。e1000 インターフェイスを使用している場合は、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。

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（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。

**ステップ 1** Threat Defense Virtual または 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 Threat Defense Virtual または 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** 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 Threat Defense Virtual または 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。

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 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)。

**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 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、[Firepower Management Center Virtual アプライアンス (Firepower Management Center Virtual Appliance)] 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 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_Firepower_Management_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。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。Management Center Virtual の場合 :

- `Cisco_Firepower_Management_Center_Virtual_VMware-X.X.X-xxx-disk1.vmdk`
- `Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-X.X.X-xxx.ovf`
- `Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-X.X.X-xxx.mf`
- `Cisco_Firepower_Management_Center_Virtual_VMware-VI-X.X.X-xxx.ovf`
- `Cisco_Firepower_Management_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、「[Management Center Virtual の導入 \(22 ページ\)](#)」に進みます。

## 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 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。

- VIOVF 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。

- 
- 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、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\_Firepower\_Management\_Center\_Virtual\_VMware-VI-X.X.X-xxx.ovf
  - Cisco\_Firepower\_Management\_Center\_Virtual\_VMware-ESXi-X.X.X-xxx.ovf
  - Cisco\_Firepower\_Management\_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、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** 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** 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。[シンプロビジョン (Thin Provisioned)] を選択すると、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。
- ステップ 10** [ネットワークマッピング (Network Mapping)] 画面で、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、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、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、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。

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、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 Management Center Virtual を正常に登録するには、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 \(24 ページ\)](#)」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。

---

**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、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 \(25 ページ\)](#)」を参照してください。
- オプションで、アプライアンスの電源を入れる前に、他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 Firepower NGIPSv Quick Start Guide for VMware』を参照)。

## 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。

**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

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、Management Center Virtual のセットアップは 2 ステップのプロセスです。

- Management Center Virtual の初期セットアップを完了するには、「[Management Center Virtual 初期設定 \(145 ページ\)](#)」を参照してください。
- Management Center Virtual の展開に必要な次のステップの概要については、[Management Center Virtual 初期管理および設定](#) を参照してください。



## 第 3 章

# KVM を使用した Management Center Virtual の導入

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

- [概要 \(27 ページ\)](#)
- [前提条件 \(29 ページ\)](#)
- [注意事項と制約事項 \(30 ページ\)](#)
- [第 0 日のコンフィギュレーション ファイルの準備 \(31 ページ\)](#)
- [Management Center Virtual の導入 \(33 ページ\)](#)
- [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。

### 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 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、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 Management Center Virtual インスタンスでは 32 GB RAM、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 Firepower Compatibility Guide』を参照してください。



**重要** 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。

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 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 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、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
  - 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 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

- 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 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。
- 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 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。
- Management Center Virtual HA を確立するには、Management Center Virtual では、HA 構成で管理する 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 Threat Defense 機能のライセンス権限は、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。
- Management Center Virtual HA ペアを解除すると、追加の Management Center Virtual ライセンス権限が解放され、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

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 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）。

**ステップ 1** 「day0-config」というテキストファイルに 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 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。「[Management Center Virtual の導入 \(34 ページ\)](#)」を参照してください。



# Management Center Virtual の導入

次の方法で、KVM で 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 Management Center Virtual を起動します。「[導入スクリプトを使用した起動 \(33 ページ\)](#)」を参照してください。
- Virtual Machine Manager の使用：virt-manager を使用して 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。「[Management Center Virtual の導入 \(34 ページ\)](#)」を参照してください。
- OpenStack の使用：OpenStack 環境を使用して Management Center Virtual を起動します。「[OpenStack を使用した起動 \(36 ページ\)](#)」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 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 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せん。*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があります。
- `--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があります。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。

**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。

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。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。

## Management Center Virtual の導入

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

**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。
- 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。
  - [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。
- [参照... (Browse...)] をクリックしてイメージファイルを選択します。
  - [OSタイプ (OS type)] には [汎用 (Use Generic)] を選択します。
  - [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。
- [メモリ (RAM) (Memory (RAM))] を 28672 に設定します。
  - [CPU (CPUs)] を 4 に設定します。
  - [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。
- 左側のパネルから [ディスク 1 (Disk 1)] を選択します。
  - [詳細オプション (Advanced Options)] をクリックします。
  - [ディスクバス (Disk bus)] を [Virtio] に設定します。
  - [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。
- 左側のパネルから [コンソール (Console)] を選択します。
  - [削除 (Remove)] を選択してデフォルト コンソールを削除します。
  - [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。
  - [デバイスタイプ (Device Type)] で、[TCP net console (tcp)] を選択します。
  - [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。
  - [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グ 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、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。

## OpenStack を使用した起動

OpenStack 環境に Management Center Virtual を展開できます。OpenStack は、パブリッククラウドとプライベートクラウドの、クラウドコンピューティングプラットフォームを構築および管理するための一連のソフトウェア ツールで、KVM ハイパーバイザと緊密に統合されています。

### OpenStack での 第 0 日のコンフィギュレーション ファイルについて

OpenStack では、ブート時にインスタンスに接続される特殊な設定ドライブ (config-drive) を使った設定データの提供をサポートしています。第 0 日のコンフィギュレーションを含む Management Center Virtual インスタンスを nova boot コマンドを使用して展開するには、次の行を含めます。

```
--config-drive true --file day0-config=/home/user/day0-config \
```

--config-drive コマンドが有効な場合、nova クライアントが呼び出される Linux ファイルシステムにあるファイル=/home/user/day0-config が仮想 CDROM の仮想マシンに渡されます。



- (注) VM はこのファイルを *day0-config* という名前で認識しますが、OpenStack では通常このファイルの内容を */openstack/content/xxxx* として保存します。この *xxxx* は、割り当てられた 4 桁の数字 (*/openstack/content/0000* など) です。これは、OpenStack ディストリビューションによって異なる場合があります。

## OpenStack でのコマンドラインを使用した起動

nova boot コマンドを使用して Management Center Virtual インスタンスを作成およびブートします。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<p>イメージ、フレーバー、インターフェイス、および第 0 日のコンフィギュレーション情報を使用して Management Center Virtual インスタンスをブートします。</p> <p>例 :</p> <pre>local@maas:~\$ nova boot \   --image=6883ee2e-62b1-4ad7-b4c6-cd62ee73d1aa \   --flavor=a6541d78-0bb3-4dc3-97c2-7b87f886b1ba \   --nic net-id=5bf6b1a9-c871-41d3-82a3-2ecee26840b1 \ --config-drive true --file day0-config=/home/local/day0-config \</pre>	Management Center Virtual には 1 つの管理インターフェイスが必要です。

## OpenStack でのダッシュボードを使用した起動

Horizon は、OpenStack のダッシュボードであり、Nova、Swift、Keystone などの OpenStack サービスへの Web ベース ユーザー インターフェイスを提供します。

### 始める前に

- Cisco.com から Management Center Virtual qcow2 ファイルをダウンロードし、ローカル MAAS サーバーに格納します。

<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。

- ステップ 1 [ログイン (Log In)] ページで、ユーザー名とパスワードを入力し、[サインイン (Sign In)] をクリックします。

ダッシュボードに表示されるタグと機能は、ログインしているユーザーのアクセス権限（権限）によって異なります。

- ステップ 2** メニューから [管理 (Admin)] > [システム パネル (System Panel)] > [フレーバー (Flavor)] を選択します。
- 仮想ハードウェアのテンプレートは OpenStack でフレーバーと呼ばれ、RAM、ディスクのサイズ、コア数を定義します。
- ステップ 3** [フレーバー情報 (Flavor Info)] ウィンドウに必要な情報を入力します。
- [名前 (Name)] : インスタンスを簡単に識別するわかりやすい名前を入力します。たとえば、「FMC-4vCPU-8GB」と入力します。
  - [VCPU の数 (VCPUs)] : [4] を選択します。
  - [RAM MB] : 28672 を選択します。
- ステップ 4** [フレーバーの作成 (Create Flavor)] を選択します。
- ステップ 5** メニューから [管理 (Admin)] > [システム パネル (System Panel)] > [イメージ (Images)] を選択します。
- ステップ 6** [イメージの作成 (Create An Image)] ウィンドウに必要な情報を入力します。
- [名前 (Name)] : イメージを簡単に識別する名前を入力します。たとえば、「FMC-Version-Build」と入力します。
  - [説明 (Description)] : (オプション) イメージファイルの説明を入力します。
  - [Browse] : 前に Cisco.com からダウンロードした Management Center Virtual qcow2 ファイルを選択します。
  - [形式 (Format)] : 形式タイプとして [QCOW2-QEMU Emulator] を選択します。
  - [公開 (Public)] ボックスをオンにします。
- ステップ 7** [イメージの作成 (Create Image)] を選択します。
- 新しく作成されたイメージを表示します。
- ステップ 8** メニューから [プロジェクト (Project)] > [コンピューティング (Compute)] > [インスタンス (Instances)] を選択します。
- ステップ 9** [インスタンスの起動 (Launch Instance)] をクリックします。
- ステップ 10** [インスタンスの起動 (Launch Instance)] > [詳細 (Details)] タブに必要な情報を入力します。
- [インスタンス名 (Instance Name)] : インスタンスを簡単に識別する名前を入力します。たとえば、「FMC-Version-Build」と入力します。
  - [フレーバー (Flavor)] : 前の手順 3 で作成したフレーバーを選択します。イメージファイルの説明を入力します。
  - [Instance Boot Source] : [Boot from image] を選択します。
  - [イメージ名 (Image Name)] : 前に手順 6 で作成したイメージを選択します。
- ステップ 11** [インスタンスの起動 (Launch Instance)] > [ネットワーキング (Networking)] タブから、Management Center Virtual インスタンスの管理ネットワークを選択します。
- ステップ 12** [作成 (Launch)] をクリックします。

インスタンスはクラウド内のコンピューティング ノードから開始します。[インスタンス (Instances) ] ウィンドウから新しく作成したインスタンスを表示します。

**ステップ 13** Management Center Virtual インスタンスを選択します。

**ステップ 14** [コンソール (Console) ] タブを選択します。

**ステップ 15** コンソールで仮想アプライアンスにログインします。

## 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 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、Management Center Virtual のセットアップは 2 ステップのプロセスです。

- 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、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、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。

**ステップ 1** コンソールから、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
```

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、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、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。

ステップ1 ブラウザで 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 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。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。

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

- Management Center Virtual の初期セットアップについて詳しくは、「[Management Center Virtual 初期設定 \(145 ページ\)](#)」を参照してください。
- Management Center Virtual の導入に必要な次の手順の概要については、「[Management Center Virtual 初期管理および設定 \(155 ページ\)](#)」の章を参照してください。





## 第 4 章

# AWS クラウドへの Management Center Virtual の導入

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。

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 \(45 ページ\)](#)
- [Management Center Virtual の導入 \(51 ページ\)](#)

## 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 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、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 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 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 : Management Center Virtual に対して AWS でサポートされているインスタンス \(42 ページ\)](#) 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、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: Management Center Virtual に対して AWS でサポートされているインスタンス

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
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
	—	—	—	—	c4.xlarge*	4	7.5	4
	—	—	—	—	c4.2xlarge	8	15	4
	—	—	—	—	c4.4xlarge	16	30	8
	* 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 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、「 <a href="#">廃止されたインスタンス</a> 」と「 <a href="#">インスタンスのサイズ変更 (43 ページ)</a> 」を参照してください。							

表 8: Management Center Virtual 300 に対して AWS でサポートされているインスタンス

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

### 廃止されたインスタンス

現在のバージョン 6.5.x 以前の Management Center Virtual 展開は引き続き実行できますが、以下のインスタンスを使用して新しい Management Center Virtual の展開 (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 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 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 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 Management Center Virtual では無効)

### インスタンスのサイズ変更

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: Management Center Virtual に対して AWS でサポートされているインスタンス (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。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](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、Management Center Virtual を導入するには、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 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。
- 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 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。
- 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、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、『Firepower Management Center コンフィギュレーションガイド』の「Licensing the System」を参照してください。
- 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：
  - Management Center Virtual にアクセスするためのパブリック IP/Elastic IP。
- Management Center Virtual とシステムの互換性については、[Cisco Firepower 互換性ガイド \[英語\]](#) を参照してください。

## ガイドライン

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

- 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 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。

# AWS 環境の設定

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、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 \(47 ページ\)](#)
- [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이스の作成 \(50 ページ\)](#)
- [Elastic IP の作成 \(50 ページ\)](#)

## 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。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 Management Center Virtual インスタンスで使用できることを確認します。

---

**ステップ 1** [aws.amazon.com](https://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を確認してください。

**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ッ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

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

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

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。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。

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。

**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** 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。

**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。

- 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) ]。
- このセキュリティ グループの [説明 (Description) ]。
- 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。

- [インバウンド (Inbound) ] タブをクリックして、[ルールの追加 (Add Rule) ] をクリックします。

(注) 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、Management Center Virtual と 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。

- [アウトバウンド (Outbound) ] タブをクリックしてから、[ルールの追加 (Add Rule) ] をクリックして、アウトバウンドトラフィックのルールを追加するか、デフォルトの [すべてのトラフィック (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 グループを作成するには、[作成 (Create) ] をクリックします。

### 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、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。

**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。

- 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)]。
- 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。
- [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。
- [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、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、Management Center Virtual に 1 つの Elastic IP アドレス、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。

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、Management Center Virtual を展開します。

## 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 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。

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、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** 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、「概要」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、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 (Instance Screenshot) ] に「AWS vW.X.Y (ビルド ZZ) 用 Cisco Firepower Management Center (Cisco Firepower Management Center for AWS vW.X.Y (build ZZ)) 」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 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 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 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。Management Center Virtual VM の [インスタンスのスクリーンショット (Instance Screenshot) ] に「AWS vW.X.Y (ビルド ZZ) 用 Cisco Firepower Management Center (Cisco Firepower Management Center for AWS vW.X.Y (build ZZ)) 」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数行の出力が続きます。

- Elastic IP を保持し、それが 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

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、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 Threat Defense Virtual のデバイス管理設定を設定できます。また、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、Threat Defense Virtual で提供されるサービスを制御します。Management Center を使用して、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

# Microsoft Azure クラウドへの Management Center Virtual の導入

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



**重要** 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 \(55 ページ\)](#)
- [前提条件 \(57 ページ\)](#)
- [注意事項と制約事項 \(57 ページ\)](#)
- [導入時に作成されるリソース \(59 ページ\)](#)
- [Management Center Virtual の導入 \(60 ページ\)](#)
- [Azure での IPv6 サポート対象 Secure Firewall Management Center Virtual の展開 \(68 ページ\)](#)
- [Azure での IPv6 をサポートする展開について \(68 ページ\)](#)
- [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 \(70 ページ\)](#)
- [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 \(76 ページ\)](#)
- [Management Center Virtual 展開の確認 \(82 ページ\)](#)
- [モニターリングおよびトラブルシューティング \(85 ページ\)](#)
- [機能の履歴 \(86 ページ\)](#)

## 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、Management Center Virtual を Microsoft Azure に展開します。Azure ポータルを使用して 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、

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 Management Center Virtual Web インターフェイスにログインできます。

### 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 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、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 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 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 9：Management Center Virtual に対して Azure でサポートされているインスタンス（56 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。

Azure 上の 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 Management Center Virtual を展開できます。Azure Marketplace の 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、Management Center Virtual でサポートされる Azure 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。

表 9：Management Center Virtual に対して Azure でサポートされているインスタンス

プラットフォーム	バージョン 6.6.0+	バージョン 6.5.x 以前 *
Management Center Virtual	Standard_D4_v2 : 8 vCPU、28 GB	Standard_D3_v2 : 4 vCPUs、14 GB
	—	Standard_D4_v2 : 8 vCPU、28 GB
	* バージョン 6.6.0 のリリース以降、Standard_D3_v2 インスタンスは Management Center Virtual で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 Management Center Virtual（任意のバージョン）を展開する必要があります。 <a href="#">インスタンスのサイズ変更（57 ページ）</a> を参照してください。	

### 廃止されたインスタンス

Standard\_D3\_v2 を使用して現在のバージョン 6.5.x 以前の Management Center Virtual は展開できますが、このインスタンスを使用して新しい Management Center Virtual の展開（バージョンに関係なく）は開始できません。



## インスタンスのサイズ変更

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、インスタンスタイプのサイズを Standard\_D4\_v2 に変更する必要があります (表9: Management Center Virtual に対して Azure でサポートされているインスタンス (56 ページ) を参照)。

Azure ポータルまたは PowerShell を使用してインスタンス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。

インスタンス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 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。Management Center Virtual とシステムの互換性については、[Cisco Firepower Threat Defense Virtual の互換性 \[英語\]](#) を参照してください。

Azure に 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](https://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 Management Center Virtual を検索し、「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

- サポートされている Azure インスタンス
  - 標準 D3\_v2 : 4 つの vCPU、14 GB のメモリ、250 GB のディスクサイズ
  - 標準 D4\_v2 : 8 つの vCPU、28 GB のメモリ、400 GB のディスクサイズ
- パブリック IP アドレッシング
  - Management 0/0 にはパブリック IP アドレスが割り当てられます。

## ライセンスング

Azure パブリック マーケットプレースの Management Center Virtual は、Bring Your Own License (BYOL) モデルをサポートしています。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、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、『[Firepower Management Center コンフィギュレーションガイド](#)』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 Firepower システム機能ライセンス](#)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

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。

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。

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。

## 高可用性のサポート

- Management Center Virtual 高可用性 (HA) は、Management Center Virtual モデルでサポートされます。
- Management Center Virtual HA を確立するには、Management Center Virtual では、HA 構成で管理する 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 Threat Defense 機能のライセンス権限は、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。
- Management Center Virtual HA ペアを解除すると、追加の Management Center Virtual ライセンス権限が解放され、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。

### 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 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
- 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 へ移行または更新、およびその逆

## 導入時に作成されるリソース

Azure に 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 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

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せん。

- 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、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、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) 内に配置されません。
- 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。

## Management Center Virtual の導入

テンプレートを使用して、Azure に 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 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 \(61 ページ\)](#)」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 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 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。

## 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 Management Center Virtual を展開します。次の手順は、Microsoft Azure 環境で 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 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。

**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「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、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、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) 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、Management Center Virtual を設定するために管理者として 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。  
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、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。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、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 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、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) 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関開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ー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。

- [選択したポートを許可 (Allow selected ports)] をクリックして、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。

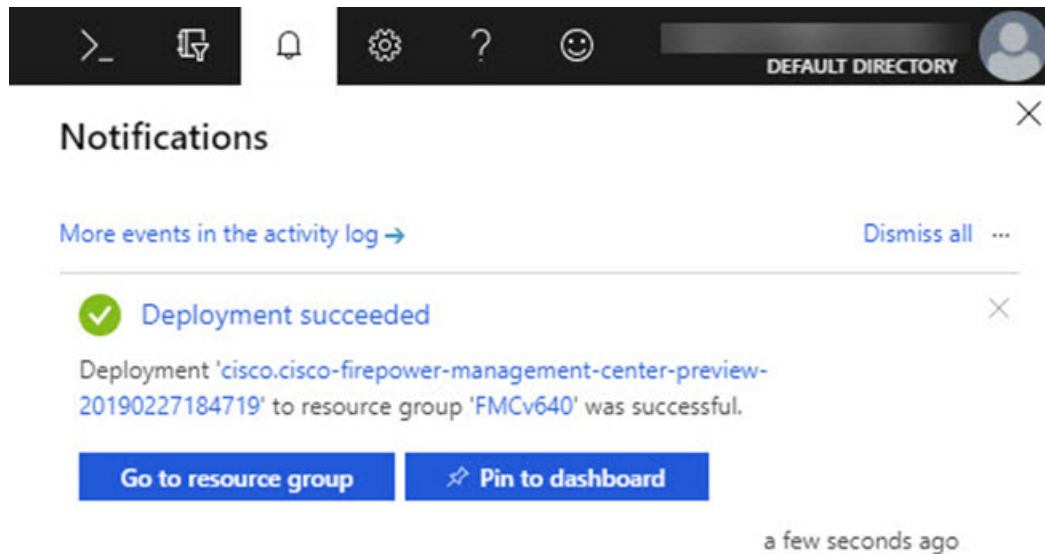
h) [OK] をクリックします。

**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。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。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。

- 左側のメニューで、[仮想マシン (Virtual machines)] を選択します。
- リストから Management Center Virtual VM を選択します。VM の概要ページが開きます。
- [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、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 Firepower Management Center for Azure v6.4.0 (build 44)
FMCv64East login:
```

## 次のタスク

- 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 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 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

- 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、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。

**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 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** 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。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。

- Azure ポータルで、[イメージ (Images)] を選択します。
- [追加 (Add)] をクリックして、新しいイメージを作成します。
- 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)] : [世代1 (Gen 1)] を選択します。

(注) [世代2 (Gen 2)] はサポートされていません。

- [ストレージブLOB (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 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>/<vhname>
```

**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、Management Center Virtual インスタンスを構築します。

- a) [新規 (New) ] を選択し、オプションから選択できるようになるまで [テンプレート展開 (Template Deployment) ] を検索します。
- b) [作成 (Create) ] を選択します。
- c) [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) ] を選択します。  
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。
- d) 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。

- e) 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。
- f) 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。
- g) ドロップダウンリストから [ロケーション (Location)] を選択します。
- h) 前ステップからの管理対象イメージの [リソースID (Resource ID)] を [VM管理対象イメージID (Vm Managed Image Id)] フィールドに貼り付けます。

**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 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 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 Management Center Virtual の IP 設定を更新します。

## 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 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

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 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 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 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 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 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 \(70 ページ\)](#)」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 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 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 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 \(76 ページ\)](#) 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 Management Center Virtual を展開するプロセス。

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 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 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。 <ul style="list-style-type: none"> <li>• 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。</li> </ul>
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 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 Management Center Virtual を展開するプロセス。

**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。

- [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 [プログラムによる展開 (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 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 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、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 Management Center Virtual バージョンを選択します。

Management Center Virtual の IPv6 サポート展開の場合は、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、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 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	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。



パラメータ名	許可される値/タイプの例	説明
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
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@40iUrhx!\", \"Hostname\": \"cisco-mcv\", \"IPv6Mode\"}	第 0 日構成で 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。 <ul style="list-style-type: none"> <li>「admin」ユーザーパスワード</li> <li>Management Center Virtual ホスト名</li> <li>管理用の Management Center Virtual ホスト名または CSF-DM。</li> </ul> 「ManageLocally : yes」：これにより、CSF-DM が 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。  Management Center Virtual を Threat Defense Virtual マネージャとして設定し、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

パラメータ名	許可される値/タイプの例	説明
		new の場合、この値はテンプレートの展開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、「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、

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。
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。
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	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 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、Secure Firewall Management Center を使用して 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、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 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 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 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、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。

**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 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] の順に選択します。
- 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** 「[HD およびリソーステンプレートをを使用した 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 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 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、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 Management Center Virtual VM に名前を付けます。
vmImageId	/subscriptions/{subscription-id}/resourceGroups/{resource-group}/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。
adminUsername	hjohn	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 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

パラメータ名	許可される値/タイプの例	説明
		<p>次の 3 つのキーと値のペアがあります。</p> <ul style="list-style-type: none"> <li>「admin」 ユーザーパスワード</li> <li>CSF-MCv ホスト名</li> <li>管理用の CSF-MCv ホスト名または CSF-DM。</li> </ul> <p>「ManageLocally : yes」 : これにより、CSF-DM が 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。</p> <p>CSF-MCv を 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。</p>
virtualNetworkResourceGroup	cisco-fmcv	<p>仮想ネットワークを含むリソースグループの名前。</p> <p>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。</p>
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。

パラメータ名	許可される値/タイプの例	説明
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、「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



パラメータ名	許可される値/タイプの例	説明
		「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。
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

パラメータ名	許可される値/タイプの例	説明
		「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	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 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

## Management Center Virtual 展開の確認

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 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、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

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。

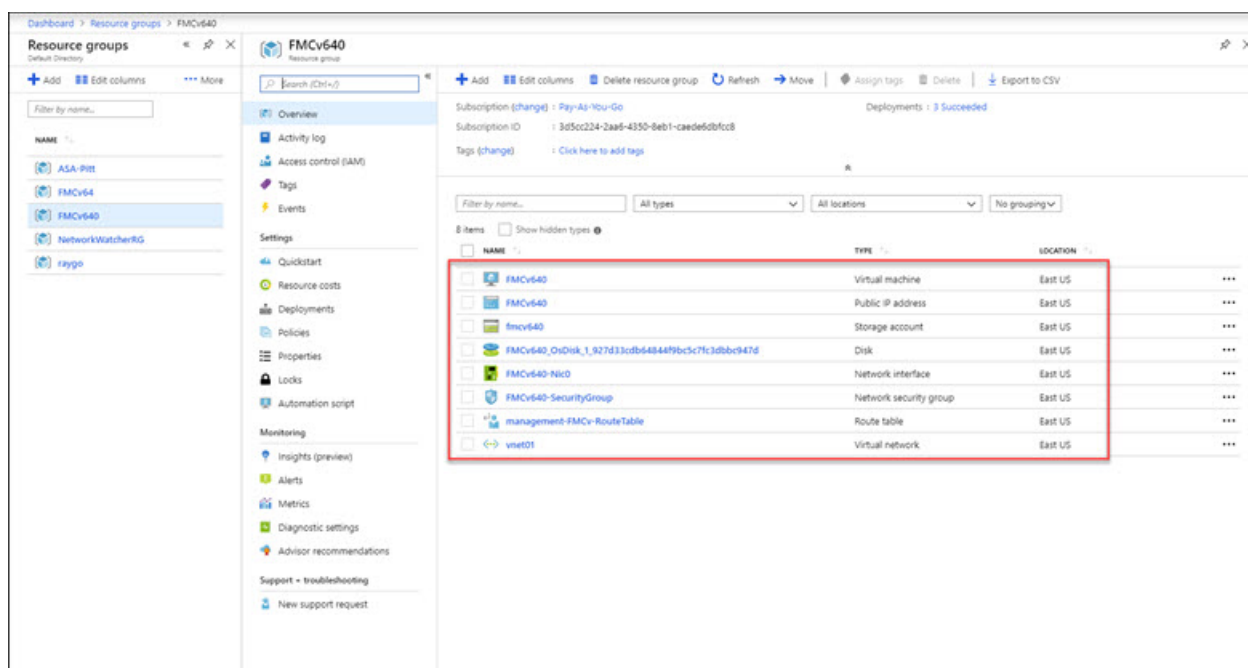


- (注) 展開時間は Azure によって異なることに注意してください。また、Azure ダッシュボードに Management Center Virtual VM のステータスが [実行中 (Running)] と表示されている場合でも、Management Center Virtual が使用可能になるまで合計では約 30 分かかります。

**ステップ 1** 展開が完了した後に 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 ポータルでの [リソースグループ (Resource groups)] ページの例を示しています。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。

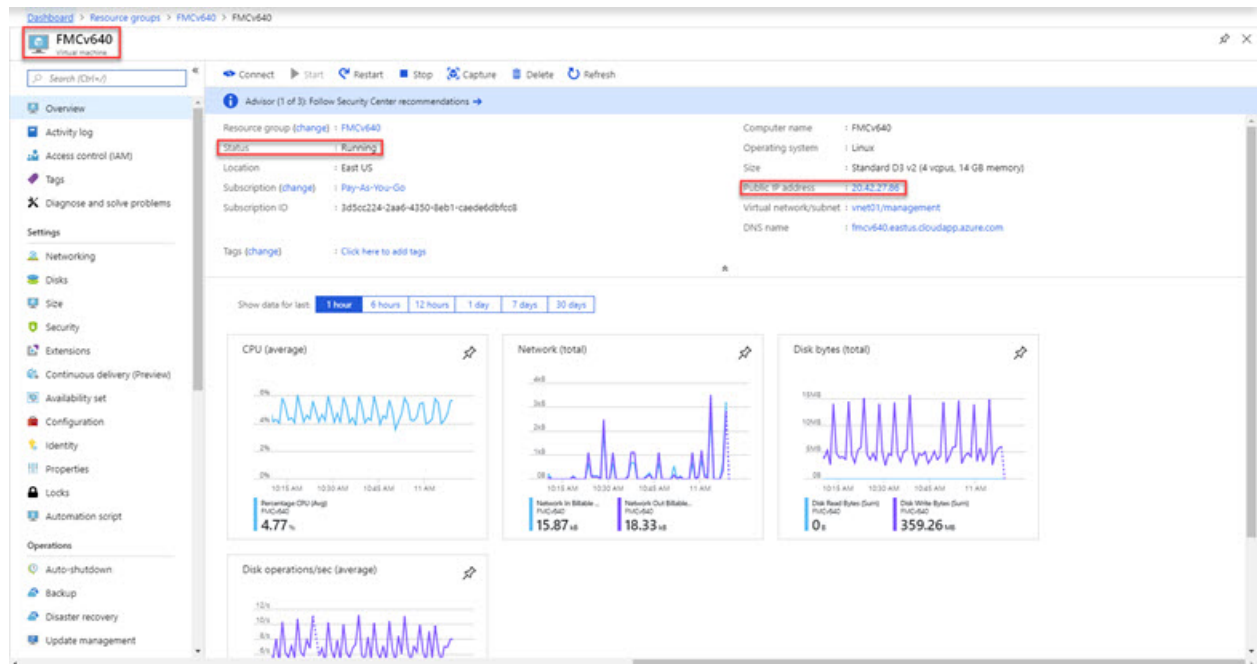
図 2: Azure Management Center Virtual の [リソースグループ (Resource Group)] ページ



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

次の図は、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 ポータルでの[仮想マシン (Virtual machine)] ページから 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、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 \(57 ページ\)](#)」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、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/](https://public_ip/) にアクセスします。ここで、*public\_ip* は VM の展開時に 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、「[Management Center Virtual 初期管理および設定 \(155 ページ\)](#)」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があります。

- 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『[Firepower Management Center コンフィギュレーションガイド](#)』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、Microsoft Azure に展開された 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 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 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、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、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。

### 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 Management Center および 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『[Firepower Management Center Configuration Guide](#)』の「System Monitoring and Troubleshooting」の項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 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。
- 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 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。
- 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
高可用性 (HA) のサポート	7.3.0	Management Center Virtual 高可用性 (HA) は、Center Virtual モデルでサポートされます。
Microsoft Azure パブリッククラウドに Management Center Virtual を導入します。	6.4.0	初期サポート。



## 第 6 章

# Google Cloud Platform への 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。

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

- [概要 \(87 ページ\)](#)
- [前提条件 \(88 ページ\)](#)
- [注意事項と制約事項 \(89 ページ\)](#)
- [ネットワークトポロジの例 \(89 ページ\)](#)
- [Management Center Virtual の導入 \(90 ページ\)](#)
- [GCP 上の Management Center Virtual インスタンスへのアクセス \(93 ページ\)](#)

## 概要

Management Center Virtual は、物理 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。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

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。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。

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)
c2-standard-8	8	32 GB
c2-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)
n1-standard-8	8	30 GB
n1-standard-16	16	60 GB
n2-standard-8	8	32
n2-standard-16	16	64
n1-highcpu-32	32	28.8
n2-highcpu-32	32	32
n1-highmem-8	8	52
n1-highmem-16	16	104
n2-highmem-4	4	32
n2-highmem-8	8	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。
  - 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、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：Threat Defense デバイスを 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：
  - Management Center への管理アクセス用のパブリック IP。
- Management Center Virtual とシステムの互換性については、Cisco Firepower 互換性ガイド [英語] 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

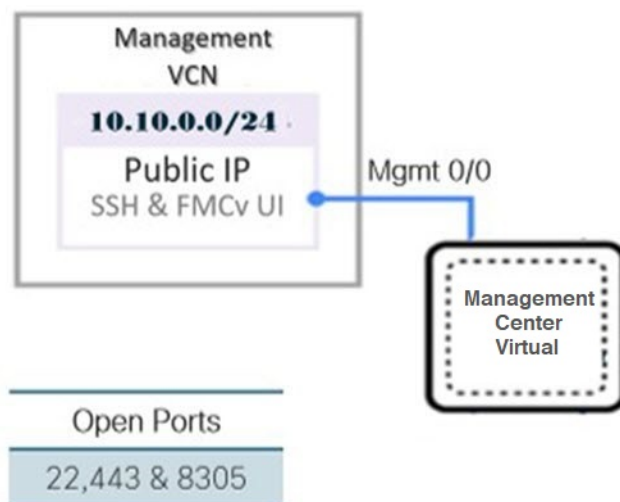
### サポートされない機能

- IPv6
- 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 Management Center Virtual の標準的なトポロジを示しています。

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



## Management Center Virtual の導入

次の手順では、GCP 環境を準備し、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

Management Center Virtual の展開には、管理 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。

- 
- 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、[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。

- ステップ 1 GCP コンソールで、[ネットワーク (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: `fncv-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 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 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 Management Center Virtual インスタンスを展開できます。

- 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「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)] : 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 \(87 ページ\)](#) 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)]** : 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-fmfv"
}
```
- 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、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、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、ライセンスを削除して、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 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 \(91 ページ\)](#) 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、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 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 Management Center Virtual インスタンスへの接続

- 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 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 Management Center Virtual インスタンスへの接続

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 Management Center Virtual インスタンスにアクセスできます。

- 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 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 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 Management Center Virtual インスタンスへの接続

---

- 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 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

# Oracle Cloud Infrastructure への Management Center Virtual の展開

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て、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 Management Center Virtual を展開できます。

- [概要 \(97 ページ\)](#)
- [前提条件 \(99 ページ\)](#)
- [注意事項と制約事項 \(99 ページ\)](#)
- [ネットワークトポロジーの例 \(100 ページ\)](#)
- [Management Center Virtual の導入 \(100 ページ\)](#)
- [OCI 上の Management Center Virtual インスタンスへのアクセス \(104 ページ\)](#)

## 概要

Management Center Virtual は、物理 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。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。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 *Management Center Virtual*

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

バージョン 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、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。
- 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、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 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はありません。

表 14: *Management Center Virtual 300 (FMCv300)* のバージョン **7.1.0** 以降でサポートされるコンピューティングシェイプ

| シェイプタイプ         | 属性   |                                |
|-----------------|------|--------------------------------|
|                 | oCPU | RAM (GB)                       |
| VM.Standard2.16 | 16   | 240 GB<br>SSD ストレージ : 2,000 GB |



(注) サポートされるシェイプタイプは、予告なく変更されることがあります。

- OCI では、1 つの oCPU は 2 つの vCPU に相当します。
- 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 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。
  - 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、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。
- インターフェースの要件：
  - 管理インターフェイス：Threat Defense デバイスを 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：
  - Management Center Virtual への管理アクセス用のパブリック IP。
- Management Center Virtual とシステムの互換性については、[Cisco Firepower 互換性ガイド](#) [英語] を参照してください。

## 注意事項と制約事項

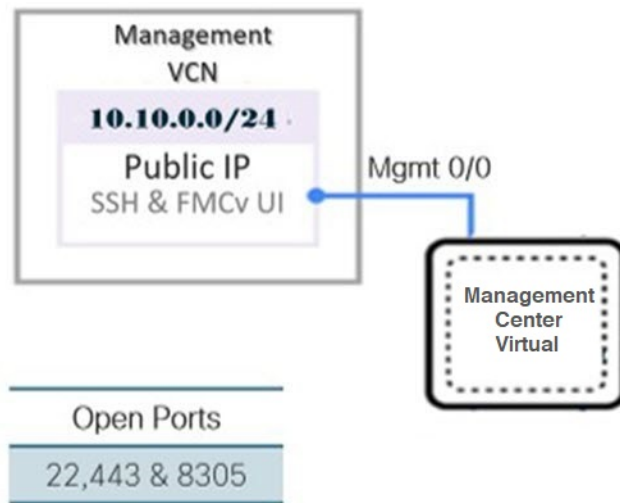
### サポートされる機能

- 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 Management Center Virtual 300 (FMCv300)**：新しい拡張された 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)。
- 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 Management Center Virtual の標準的なトポロジを示しています。

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



## Management Center Virtual の導入

### 仮想クラウドネットワーク（VCN）の設定

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。

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。

- 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 Management Center Virtual は 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。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。

- 
- ステップ 1** [ネットワークング (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。
- [ネットワークング (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。
  - 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。
  - [ルートルールの追加 (Add Route Rules)] をクリックします。
  - [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。
  - 宛先 CIDR のブロックを入力します (例: 0.0.0.0/0)。
  - [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。
  - [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。

---

- ステップ 1** [ネットワークング (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、Management Center Virtual を起動する準備が整います。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: Management Center Virtual 仮想クラウドネットワーク

Virtual Cloud Networks in *fmcv* Compartment

Virtual Cloud Networks are virtual, private networks that you set up in Oracle data centers. It closely resembles a traditional network, with firewall rules and specific types of communication gateways that you can choose to use.

| Name                            | State     | CIDR Block   | Default Route Table                                     | DNS Domain Name              | Created                        |
|---------------------------------|-----------|--------------|---------------------------------------------------------|------------------------------|--------------------------------|
| <a href="#">FMCv-Management</a> | Available | 10.10.0.0/24 | <a href="#">Default Route Table for FMCv-Management</a> | fmcvmanagement.oraclevcn.com | Mon, Jul 6, 2020, 16:42:50 UTC |

Showing 1 item < 1 of 1 >

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

Oracle Cloud Marketplace の 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 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。

- 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「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、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 (97 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)』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、Management Center Virtual の Day0 構成を指定します。day0 構成は、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 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。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、Management Center Virtual の起動が完了したことを示します。

## OCI 上の 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なになります。
- 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 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 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 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。

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、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 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 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。

**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、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 Management Center Virtual インスタンスへの接続

Windows システムから 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。

**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>
```

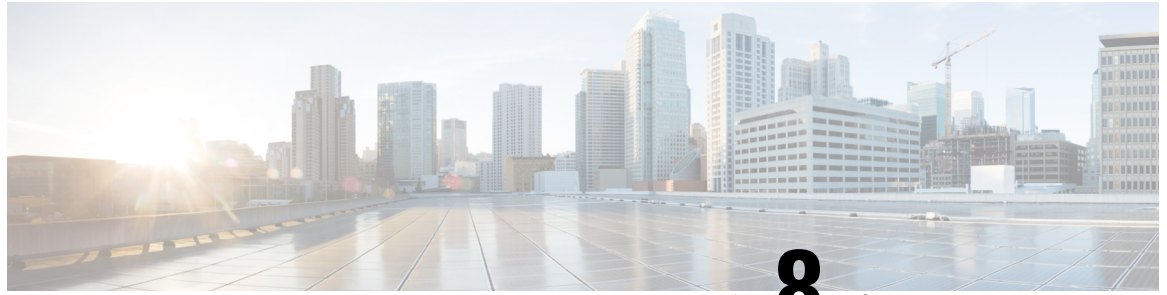
ここで、

<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、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 を使用した Management Center Virtual の展開

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

- [概要 \(109 ページ\)](#)
- [前提条件 \(110 ページ\)](#)
- [注意事項と制約事項 \(111 ページ\)](#)
- [システム要件 \(112 ページ\)](#)
- [ネットワークポロジの例 \(114 ページ\)](#)
- [Management Center Virtual の導入 \(114 ページ\)](#)

## 概要

このガイドでは、OpenStack 環境で 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。

Management Center Virtual は、物理 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。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](https://software.cisco.com) から 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](https://software.cisco.com) および Cisco Service Contract が必要です。
- 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。

Stein リリース : <https://docs.openstack.org/project-deploy-guide/openstack-ansible/stein/overview.html>

Queens リリース : <https://docs.openstack.org/project-deploy-guide/openstack-ansible/queens/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](#)、3.4.3 ~ 3.4.5) を参照してください。

- ライセンス :
  - 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、『[Firepower Management Center コンフィギュレーションガイド](#)』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
  - 16 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
  - 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 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：
  - 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 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 \(112 ページ\)](#) を参照してください。
- Management Center Virtual とシステムの互換性については、[Cisco Firepower 互換性ガイド \[英語\]](#) 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 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 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、VPP、および SRIOV
- IPv6 はサポートされます。

### サポートされない機能

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

- 自動スケール
- OpenStack Stein リリースと Queens リリース以外の OpenStack リリース

- Ubuntu 18.04 バージョンと Red Hat Enterprise Linux (RHEL) 7.6 以外のオペレーティングシステム

## 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、IXGBE、I40E   | 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 18.04 | 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 | Stein 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。<br><a href="https://releases.openstack.org/">https://releases.openstack.org/</a> |

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、SRIOV、および VPP    | サポートされているドライバは次のとおりです。                                               |

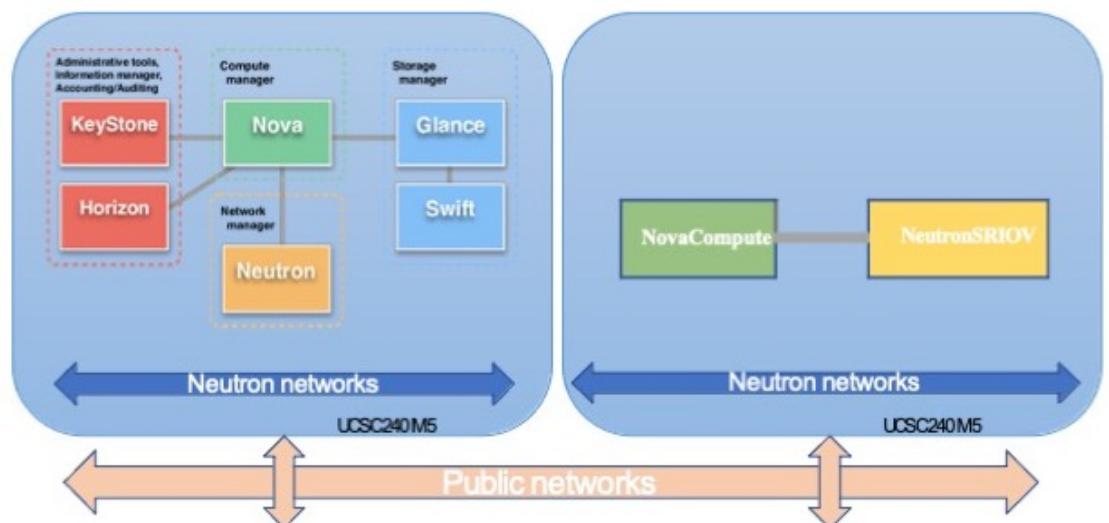


| カテゴリ            | サポートされるバージョン                                                                                                                                                                     | 注記                                                                                                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco VIM バージョン | Cisco VIM 3.4.4<br>サポート対象： <ul style="list-style-type: none"> <li>オペレーティングシステム - Red Hat Enterprise Linux 7.6</li> <li>OpenStack バージョン - OpenStack 13.0 (Queens リリース)</li> </ul> | 詳細については、 <a href="#">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 3.4.3 ~ 3.4.5</a> を参照してください。<br>さまざまな OpenStack リリースの詳細については、 <a href="https://releases.openstack.org/">https://releases.openstack.org/</a> を参照してください。 |
|                 | Cisco VIM 4.2.1<br>サポート対象： <ul style="list-style-type: none"> <li>オペレーティングシステム - Red Hat Enterprise Linux 8.2</li> <li>OpenStack バージョン - OpenStack 16.1 (トレイン リリース)</li> </ul>   | 詳細については、 <a href="#">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 4.2.1</a> を参照してください。<br>さまざまな OpenStack リリースの詳細については、 <a href="https://releases.openstack.org/">https://releases.openstack.org/</a> 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。

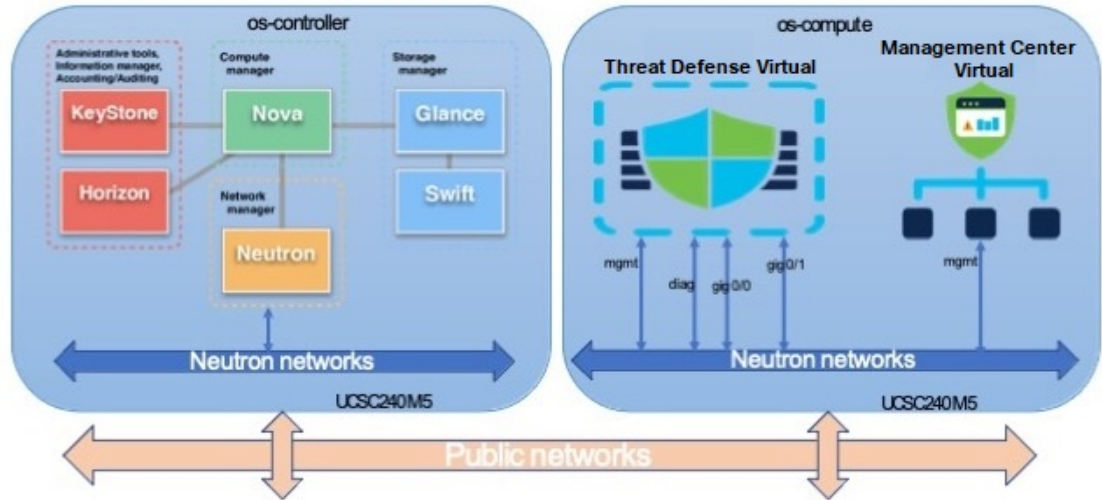
図 7: OpenStack プラットフォームトポロジ



## ネットワークトポロジの例

次の図に、OpenStack の 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 Management Center Virtual を使用したトポロジの例



## Management Center Virtual の導入

シスコでは、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。Management Center Virtual の展開手順は大まかに次の部分に分類されます。

- 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
- 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 Management Center Virtual を展開できます。

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

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 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>

**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** 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** 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
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 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、ルーティングインターフェイス、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 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 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、Management Center Virtual の環境を定義します。

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 を定期的を確認してください。

**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 | Creation Time | Updated Time |
+-----+-----+-----+-----+-----+-----+
--+
| b30d5875-ce3a-4258-a841-bf2d09275929 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE | 2020-12-07T15:10:24Z | None |
+-----+-----+-----+-----+-----+-----+
--+
```

### 次のタスク

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

## OpenStack での 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 Management Center Virtual を展開します。

### 始める前に

OpenStack で 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`

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。

**ステップ 1** Management Center Virtual Heat テンプレートファイル (`ddeploy_fmcv.yaml`) を展開して、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
creation_time	2020-12-07T14:55:05Z
updated_time	None
stack_status	CREATE_IN_PROGRESS
stack_status_reason	Stack CREATE started
+-----+
```

**ステップ 2** 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 | Creation Time | Updated Time |
+-----+-----+-----+-----+-----+-----+
| 14624af1-e5fa-4096-bd86-c453bc2928ae | fmcv-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE | 2020-12-07T14:55:05Z | None |
| 198336cb-1186-45ab-858f-15ccd3b909c8 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE | 2020-12-03T10:46:50Z | None |
+-----+-----+-----+-----+-----+-----+
```





## 第 9 章

# Cisco HyperFlex を使用した 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 Management Center Virtual を展開できます。

- [システム要件 \(119 ページ\)](#)
- [注意事項と制約事項 \(121 ページ\)](#)
- [Management Center Virtual の導入 \(122 ページ\)](#)
- [仮想アプライアンスの電源投入と初期設定 \(124 ページ\)](#)

## システム要件

### Management Center Virtual 28 GB の RAM が必要

デフォルト設定 (ほとんどの 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 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 Firepower Compatibility Guide](#)』を参照してください。
- 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。

- 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、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** 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。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: 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<br>プロビジョ<br>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: 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<br>プロビジョニング<br>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 Management Center Virtual を展開する場合、次の制限があります。

- 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 への導入用: Cisco\_Firepower\_Management\_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、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 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 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。
- Management Center Virtual HA を確立するには、Management Center Virtual では、HA 構成で管理する 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 Threat Defense 機能のライセンス権限は、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](#)』の「License Requirements for FTD Devices in a High Availability Pair」を参照してください。

- Management Center Virtual HA ペアを解除すると、追加の Management Center Virtual ライセンス権限が解放され、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](#)

## Management Center Virtual の導入

以下の手順を使用して、vSphere vCenter Server 上の Cisco HyperFlex に 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。
- 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 Management Center Virtual VI OVF テンプレートファイル、*Cisco\_Firepower\_Management\_Center\_Virtual-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。

- 
- 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** 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 Management Center Virtual VI OVF テンプレートを選択できます。
- Cisco\_Firepower\_Management\_Center\_Virtual-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** 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

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。

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 Management Center Virtual を正常に登録するには、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 \(25 ページ\)](#) 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。

---

**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

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 VIOVF テンプレートを使用して展開する場合、Management Center Virtual のセットアップは 2 ステップのプロセスです。

- Management Center Virtual の初期セットアップを完了するには、「[Management Center Virtual 初期設定 \(145 ページ\)](#)」を参照してください。
- Management Center Virtual の展開に必要な次のステップの概要については、「[Firepower Management Center Virtual の初期管理および設定](#)」を参照してください。



## 第 10 章

# Nutanix を使用した 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 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 Management Center Virtual を展開できます。

- [システム要件 \(125 ページ\)](#)
- [前提条件 \(126 ページ\)](#)
- [注意事項と制約事項 \(127 ページ\)](#)
- [Management Center Virtual の導入 \(128 ページ\)](#)

## システム要件

デフォルト設定 (ほとんどの 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 Firepower Compatibility Guide](#)』を参照してください。
- 最新のリリースノート参照し、新しいリリースが環境に影響を及ぼさないことを確認してください。最新バージョンを展開するには、リソースの拡張が必要な場合があります。

- 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 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、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
  - 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          |
|-----------------------|--------------------|
| Device Manager 7.0    | Threat Defense 7.0 |
| Management Center 7.0 |                    |

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 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。

### Management Center Virtual ライセンス

- 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、『[Firepower Management Center コンフィギュレーションガイド](#)』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  |
| 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

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](#)

## 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。                                                                                | <a href="#">前提条件 (126 ページ)</a>                                                  |
| 2    | Management Center Virtual qcow2 ファイルを Nutanix 環境にアップロードします。                                | <a href="#">Management Center Virtual QCOW2 ファイルを Nutanix にアップロード (128 ページ)</a> |
| 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。                                       | <a href="#">第 0 日のコンフィギュレーションファイルの準備 (129 ページ)</a>                              |
| 4    | Management Center Virtual を Nutanix 環境に展開します。                                              | <a href="#">Nutanix への Management Center Virtual の展開</a>                        |
| 5    | (任意) 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。 | <a href="#">Management Center Virtual のセットアップの完了 (132 ページ)</a>                  |

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

Management Center Virtual を Nutanix 環境に展開するには、Prism Web コンソールで 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 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>)。

**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. 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

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 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、「[Management Center Virtual のセットアップの完了 \(132 ページ\)](#)」を参照してください。

次を指定することができます。

- エンドユーザー ライセンス契約書 (EULA) の承認。
- システムのホスト名。
- 管理者アカウントの新しい管理者パスワード。
- アプライアンスが管理ネットワークで通信することを許可するネットワーク設定。

---

**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 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 Management Center Virtual の展開

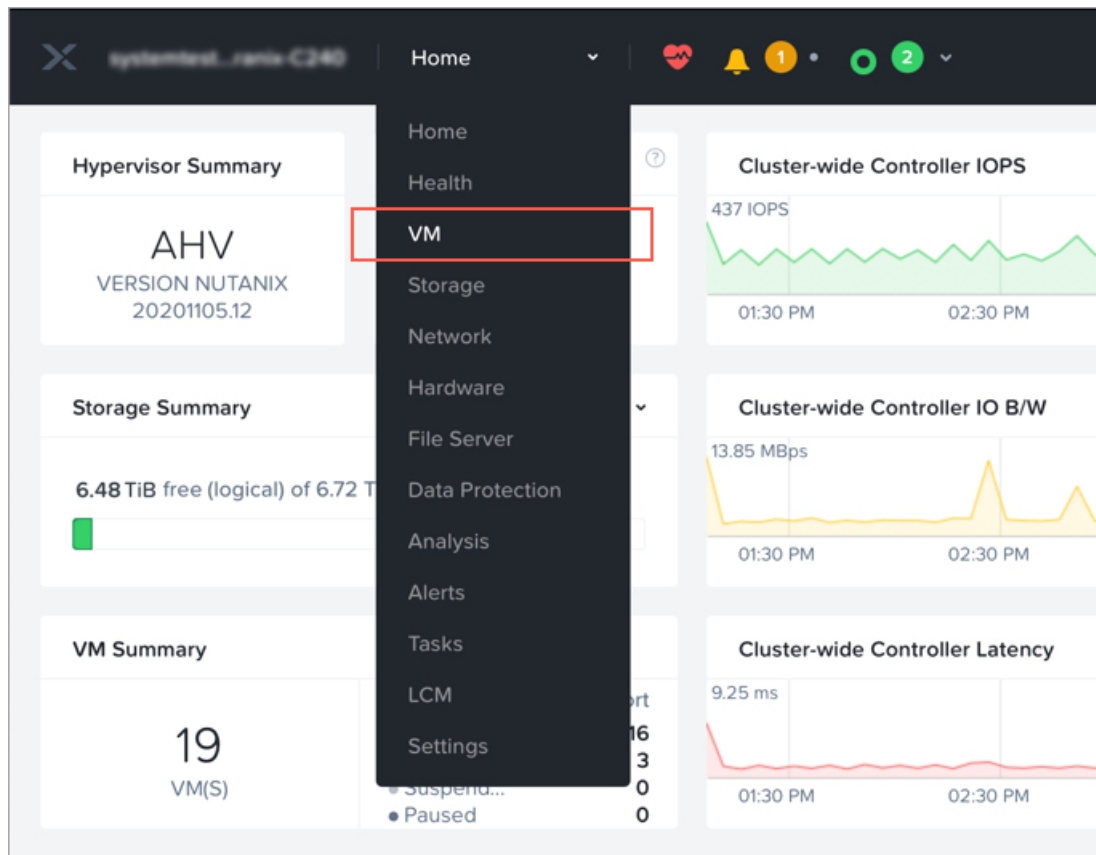
### 始める前に

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。

---

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

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



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

**ステップ 4** 次の手順を実行します。

1. 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、Management Center Virtual インスタンスの説明を入力します。
3. 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. 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. 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** Management Center Virtual インスタンスにディスクを接続します。

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

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

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

**ステップ 8** 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 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、Management Center Virtual を展開します。VM テーブルビューに 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。

```
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"
```

**ステップ 12** VM テーブルビューに移動し、新たに作成した 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** 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 Management Center Virtual の順に移動し、ログインします。

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

どの 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、Management Center Virtual のセットアップは2ステップのプロセスです。

- 
- ステップ 1** 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、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、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 \(133 ページ\)](#)」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、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 \(134 ページ\)](#) 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、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。

- 
- ステップ 1** コンソールから、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
```

  
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、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、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。

---

**ステップ 1** ブラウザで 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** 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。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。

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

- Management Center Virtual の初期セットアップについて詳しくは、「[Management Center Virtual 初期設定 \(145 ページ\)](#)」を参照してください。
- Management Center Virtual の展開に必要な次のステップの概要については、「[Firepower Management Center Virtual の初期管理および設定](#)」の章を参照してください。



## 第 11 章

# Hyper-V での 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。

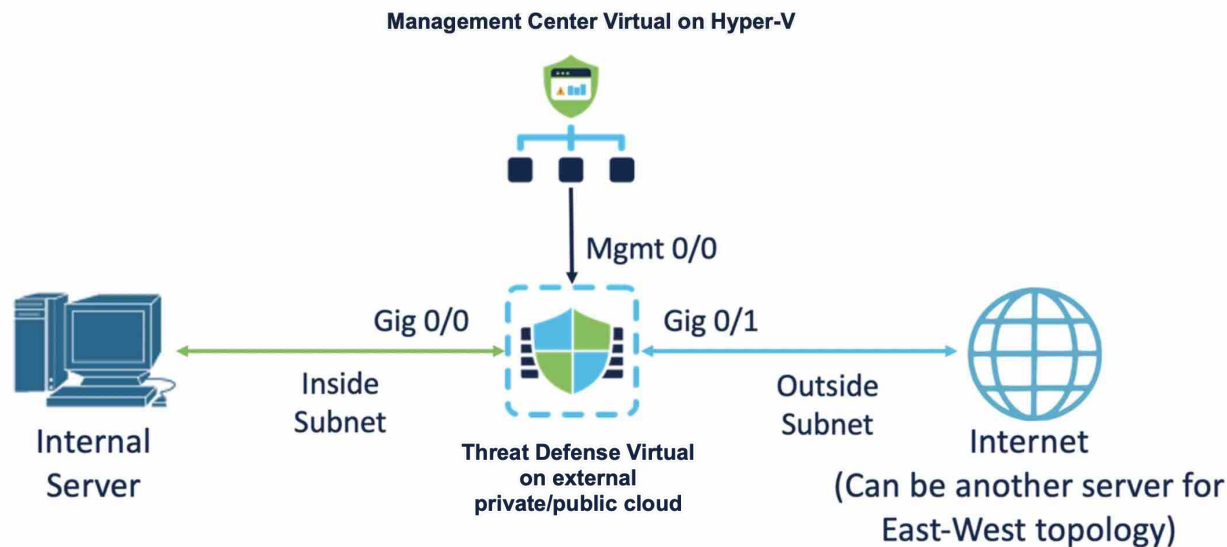
- [概要 \(135 ページ\)](#)
- [Hyper-V での Management Center Virtual のトポロジ例 \(136 ページ\)](#)
- [Management Center Virtual でサポートされる Windows Server \(136 ページ\)](#)
- [Hyper-V での Management Center Virtual のガイドラインと制限事項 \(137 ページ\)](#)
- [Hyper-V での Management Center Virtual の展開用ライセンス \(137 ページ\)](#)
- [Hyper-V での Management Center Virtual の展開に必要な前提条件 \(137 ページ\)](#)
- [Management Center Virtual の展開 \(138 ページ\)](#)
- [展開の確認 \(140 ページ\)](#)
- [最初のブートログへのアクセス \(141 ページ\)](#)
- [Management Center Virtual のシャットダウン \(142 ページ\)](#)
- [Management Center Virtual の再起動 \(142 ページ\)](#)
- [Management Center Virtual の削除 \(142 ページ\)](#)
- [トラブルシューティング \(142 ページ\)](#)

## 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 Standard エディション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。

---

**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。

**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。

---

- 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。
- 

## 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。

```
rm-Production login: admin
Password:

Copyright 2004-2022, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v82.14.0 (build 205)
Cisco Secure Firewall Management Center for Hyper-U v7.4.0 (build 1493)

> show version
-----[ rm-Production ]-----
Model                : Secure Firewall Management Center for Hyper-U (66)
Version 7.4.0 (Build 1493)
UUID                 : 3f775634-7f7d-11ed-b8f5-0c0e70c660f3
Rules update version : 2022-01-06-001-vrt
LSP version          : lsp-rel-20221214-1542
UDB version          : 361
```

## 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。

- 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 12 章

# Management Center Virtual 初期設定

この章では、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。

- [Management Center CLI \(バージョン 6.5 以降\) を使用した初期セットアップ \(145 ページ\)](#)
- [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 \(バージョン 6.5 以降\) \(148 ページ\)](#)
- [バージョン 6.5 以降の自動初期設定の確認 \(152 ページ\)](#)

## Management Center CLI (バージョン 6.5 以降) を使用した初期セットアップ

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

- 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
- 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 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、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)。

**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 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、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) 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、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、Management Center に接続し (ホスト名または新しい IP アドレスを使用)、**システム (⚙)** > **[構成 (Configuration)]** > **[管理インターフェイス (Management Interfaces)]** の順に選択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) 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) 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 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 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、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 \(152 ページ\)](#) 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 コンフィギュレーション 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 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、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。

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 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)

- 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。

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 コンフィギュレーションガイド](#) で「Device Management」を参照してください。

### 始める前に

- 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  
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 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、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。

**ステップ 1** Web ブラウザを使用して、Management Center Virtual の IP アドレス : `https://<Firepower 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 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) Management Center では、パスワードをパスワードクラッキング辞書と照合して、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、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、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、Management Center に接続し (ホスト名または新しいIPアドレスを使用)、システム (⚙) > [構成 (Configuration)] > [管理インターフェイス (Management Interfaces)] の順に選択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、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。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。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 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、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 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

- スマートライセンス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、Management Center Virtual で脅威に対する防御を管理する場合は、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、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 \(152 ページ\)](#) を参照してください。
- 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 Firepower Management Center コンフィギュレーションガイド \[英語\]](#) 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 コンフィギュレーションガイド](#) 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 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）、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、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

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、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。

- Management Center の週次ソフトウェアアップデート

Management Center では、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となります。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、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 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 Management Center 設定バックアップ

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となります。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

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、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

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 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、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 13 章

# Management Center Virtual 初期管理および設定

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、および展開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に対応する『[Firepower Management Center Configuration Guide](#)』を参照してください。

- [個別のユーザー アカウント \(155 ページ\)](#)
- [デバイス登録 \(156 ページ\)](#)
- [ヘルス ポリシーとシステム ポリシー \(156 ページ\)](#)
- [ソフトウェアとデータベースの更新 \(157 ページ\)](#)

## 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、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 Management Center Virtual へのアクセスと Web インターフェイスを使用した 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 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

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。

- **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。
- **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、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的なソフトウェアと 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 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。

Management Center に管理対象デバイスを登録するには、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 [Firepower Management Center コンフィギュレーション ガイド](#) 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、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、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、ヘルスマ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、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。

**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。**

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
- 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、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 Firepower Management Center Upgrade Guide』を参照してください。

- ローカルに保存された設定のみの Management Center バックアップを実行する週次タスク。

**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、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、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『Firepower Management Center Configuration Guide』で説明されているように、これらのアクティビティを自分で設定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。