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

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 1 : Management Center Virtual に対して Azure でサポートされているインスタンス （2 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 *1 : 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。インスタンスのサイズ変更 （3 ページ）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 1 : Management Center Virtual に対して Azure でサポートされているインスタンス（2 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 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。

ライセンシング

Azure パブリック マーケットプレイスの 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す。
- セキュリティグループ（名前は、*vm name*-mgmt-SecurityGroup）

  セキュリティグループは VM の Nic0 にアタッチされます。

  このセキュリティグループには、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）内に配置されます。
- 選択したストレージアカウントのブロブおよびコンテナ VHD にある 2 つのファイル（名前は、*VM name*-disk.vhd および *VM name*-<uuid>.status）
- ストレージアカウント（既存のストレージアカウントが選択されていない場合）

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

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 （7 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開くかどうかを示します。デフォルトでは、[なし（None）] が選択されています。

- Azure のデフォルトのセキュリティルールを使用してネットワーク セキュリティ グループを作成し、管理インターフェイスに接続するには、[なし（None）] をクリックします。このオプションを選択すると、同じ仮想ネットワーク内の送信元からのトラフィックと Azure ロードバランサからのトラフィックが許可されます。
- [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。

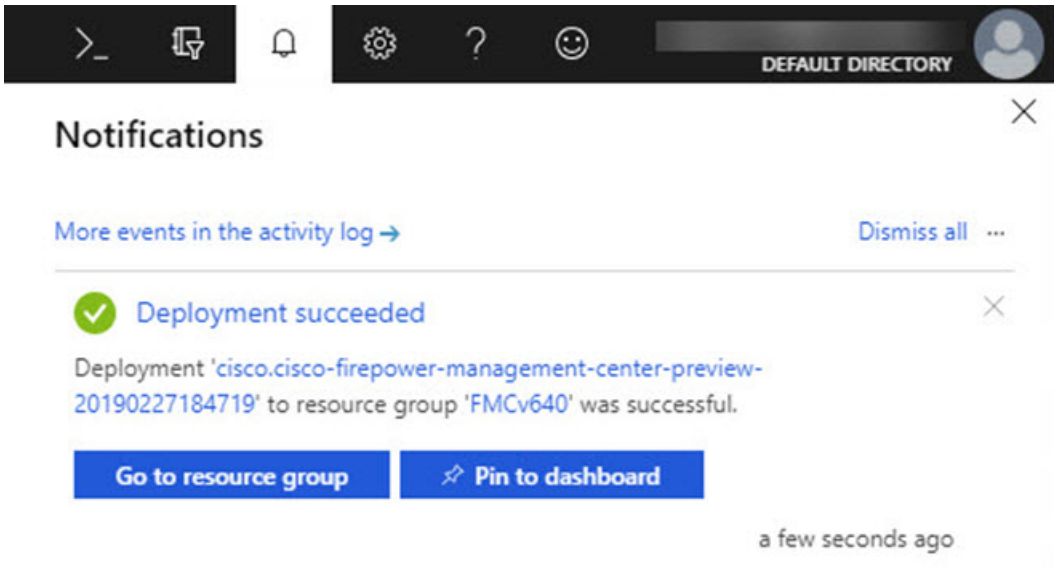
h) [OK] をクリックします。

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。

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

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

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

起動時診断またはシリアルコンソールのいずれかにログインプロンプトが表示されれば、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。

a) Azure ポータルで、[イメージ（Images）] を選択します。
b) [追加（Add）] をクリックして、新しいイメージを作成します。
c) 次の情報を入力します。

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

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

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

d) [作成（Create）] をクリックします。

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

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

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

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

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

リソース ID は、次の形式を取ります。

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

ステップ 8 管理対象イメージおよびリソーステンプレートを使用して、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 （16 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 （22 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 *2:*

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。 • Azure Marketplace 参照イメージを使用したカスタム IPv6 テンプレート。 カスタム IPv6（ARM）テンプレートを使用した VHD イメージ。
4	カスタム IPv6（ARM）テンプレートの IPv6 パラメータを更新します。 （注） Marketplace イメージバージョンに相当するソフトウェア イメージ バージョンのパラメータ値は、Marketplace イメージ参照でカスタム IPv6 テンプレートを使用して 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想要素を表示します。

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

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

a) [Azure（サービス）（Azure Services）] で [サブスクリプション（Subscriptions）] をクリックして、サブスクリプション ブレード ページを表示します。

b) 左側のペインで、[設定（Settings）] オプションの [プ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@4OiUrhx!\",\"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。 • 「admin」ユーザーパスワード • Management Center Virtualホスト名 • 管理用の Management Center Virtual ホスト名または CSF-DM。 「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用に選択されたリソースグループと同じである必要があります。
virtualNetworkName	cisco-mcv-vnet	仮想ネットワークの名前。
virtualNetworkNewOrExisting	new	このパラメータによって、新しい仮想ネットワークを作成するか、既存の仮想ネットワークを使用するかが決まります。
virtualNetworkAddressPrefixes	10.151.0.0/16	これは仮想ネットワークの IPv4 アドレスプレフィックスで、「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
		次の 3 つのキーと値のペアがあります。 • 「admin」ユーザーパスワード • CSF-MCv ホスト名 • 管理用の CSF-MCv ホスト名または CSF-DM。 「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。 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。
virtualNetworkResourceGroup	cisco-fmcv	仮想ネットワークを含むリソースグループの名前。virtualNetworkNewOrExisting が new の場合、この値はテンプレートの展開用に選択されたリソースグループと同じである必要があります。
virtualNetworkName	cisco-mcv-vnet	仮想ネットワークの名前。
ipAllocationMethod	動的	Azure からの IP 割り当て。静的：手動、動的：DHCP
mgmtSubnetName	mgmt	mgmt インターフェイスの Management Center IP（例：192.168.0.10）
mgmtSubnetIP	10.4.1.15	mgmt インターフェイスの FMC IP（例：192.168.0.10）
mgmtSubnetIPv6	ace:cab:deca:dddd::c3	mgmt インターフェイスの FMC IPv6（例：ace:cab:deca:dddd::6）
virtualNetworkNewOrExisting	new	このパラメータによって、新しい仮想ネットワークを作成するか、既存の仮想ネットワークを使用するかが決まります。

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

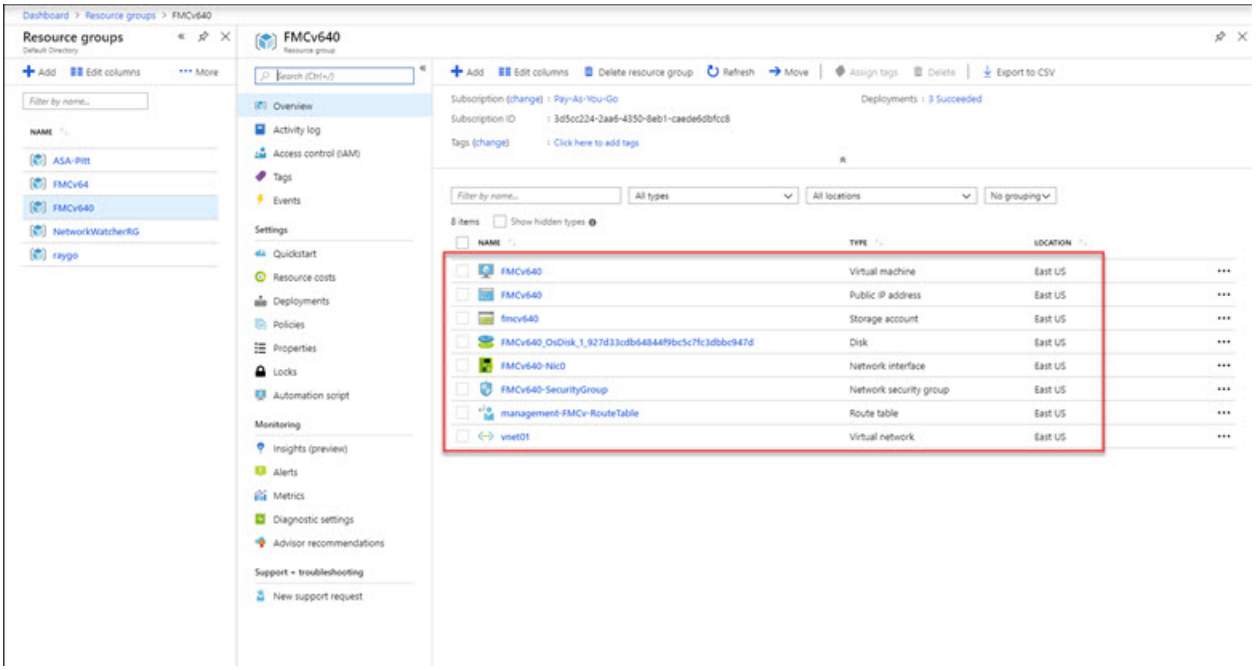
Management Center Virtual VM は自動的に起動します。展開時、Azure が VM を作成している間はステータスが [作成中（Creating）] として表示され、展開が完了するとステータスが [実行中（Running）] に変わります。

（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。

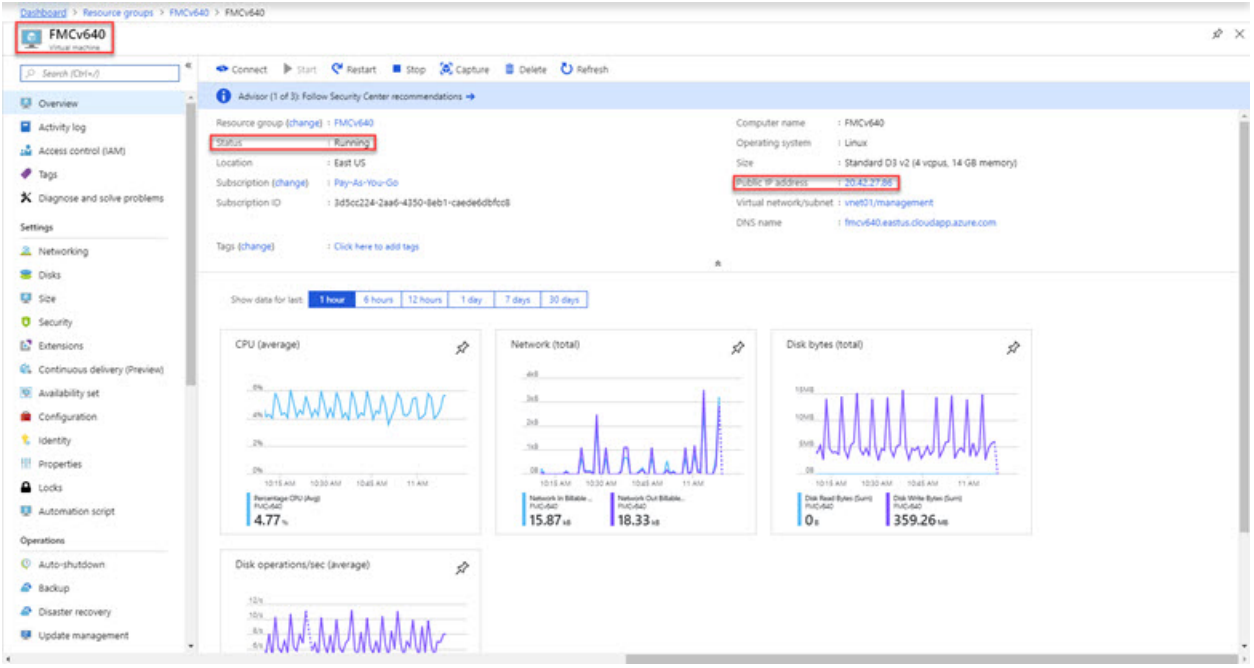
図 *2 : Azure Management Center Virtual* の *[リソースグループ（Resource Group）]* ページ



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 （3 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*/ 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」を参照してください。
- また、デバイスの登録とライセンスの要件を確認する必要もあります。

- システム設定の開始方法の詳細については、ご使用のソフトウェアバージョンの『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、Micosoft 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。

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。