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ることで、エンタープライズアプリケーションにリアルタイムの柔軟性を提供します。

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

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 *1:* 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 Management Center Virtual のバージョン	属性	
		oCPU	RAM（GB）
インテル VM.StandardB1.4	7.3.0 以降	4	48
インテル VM.Standard2.4	7.1.0 以降	4	60
インテル VM.Standard3.Flex	7.3.0 以降	4	32
インテル VM.Optimized3.Flex	7.3.0 以降	4	32
AMD VM.Standard.E4.Flex	7.3.0 以降	4	32

バージョン Management Center Virtual7.3 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がありません。

表 *2: 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 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 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

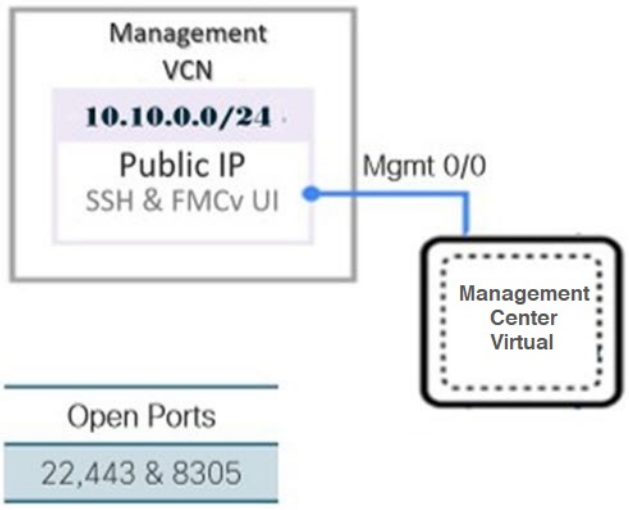
サポートされる機能

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

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

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

ステップ 4 インターネットゲートウェイへのルートを追加します。

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

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

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

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

e) 宛先 CIDR のブロックを入力します（例：0.0.0.0/0）。

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

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

サブネットの作成

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

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

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

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

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

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

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

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

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

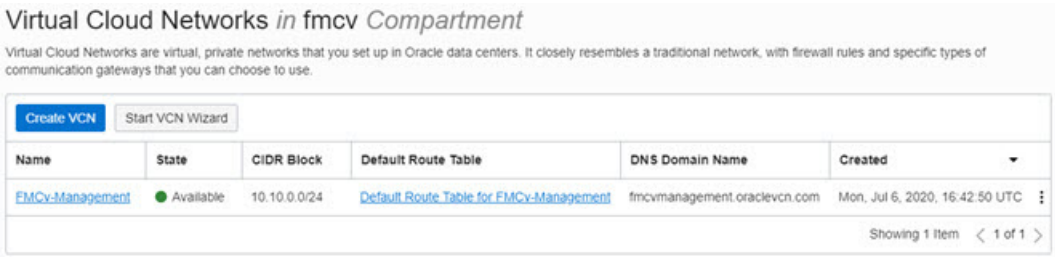
ステップ 8 以前作成した **[セキュリティリスト（Security List）]** を選択します。

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

次のタスク

管理 VCN を設定すると、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 *2 : Management Center Virtual* 仮想クラウドネットワーク



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 （1 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。

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。