# Oracle Cloud Infrastructure への FMCv の展開

**最終更新日:** 2020 年 11 月 16 日

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。

Firepower Management Center Virtual（FMCv）は OCI に展開できます。


- FMCv の展開と OCI について（1 ページ）
- OCI での FMCv の前提条件（2 ページ）
- FMCv と OCI のガイドラインおよび制限事項（2 ページ）
- OCI での FMCv のネットワークトポロジの例（3 ページ）
- OCI への FMCv の展開（3 ページ）
- OCI での FMCv インスタンスへのアクセス（7 ページ）


## FMCv の展開と OCI について

Cisco Firepower Management Center Virtual（FMCv）は、物理の Cisco FMC と同じソフトウェアを実行して、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。FMCv は、パブリック OCI で展開できます。その後、仮想および物理の Firepower Threat Defense 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。FMCv は、次の OCI のシェイプタイプをサポートします。

**表 1　OCI でサポートされるシェイプタイプ**

| OCI のシェイプ | 属性 | | インターフェイス |
|---|---|---|---|
| | oCPU | RAM（GB） | |
| VM.Standard2.4 | 4 | 60 GB | 最小 3、最大 4 |

- OCI では、1 つの oCPU は 2 つの vCPU に相当します。
- FMCv にはインターフェイスが 1 つ必要です。

ユーザは、OCI でアカウントを作成し、FMCv イメージをアップロードしてカスタムイメージを作成後、OCI シェイプを選択します。

# OCI での FMCv の前提条件

- 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。
  - Firepower 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。
  - ライセンスを管理する方法の詳細については、『Firepower Management Center Configuration Guide』の「Licensing the Firepower 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 – Firepower Threat Defense Virtual を Firepower Management Center に接続するために使用されます。
- 通信パス：
  - Firepower Management Center Virtual にアクセスするためのパブリック IP。
- Firepower Threat Defense Virtual と Firepower System の互換性については、『Cisco Firepower Compatibility』を参照してください。

# FMCv と OCI のガイドラインおよび制限事項

### 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

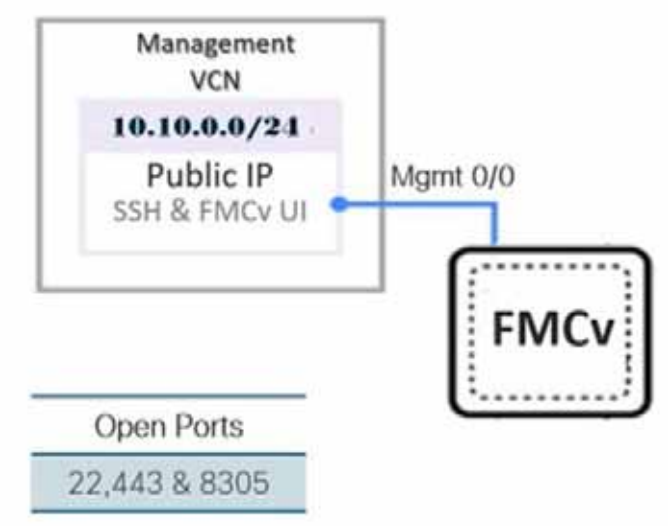
### サポートされない機能

- IPv6
- FMCv 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

# OCI での FMCv のネットワークトポロジの例

図 1(3 ページ)に、OCI でサブネットが 1 つ設定された FMCv の推奨トポロジを示します。

**図 1　OCI での FMCv 展開のトポロジ例**




# OCI への FMCv の展開

次の手順では、OCI 環境を準備し、FMCv インスタンスを起動する方法について説明します。FMCv の起動後、トラフィックを送信元と宛先に応じて Management Center に転送するようルートテーブルを設定する必要があります。

## 仮想クラウドネットワーク(VCN)の設定

FMCv 展開用の仮想クラウドネットワーク(VCN)を設定します。

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、どのユーザがそれらのコンパートメントを表示してアクションを実行できるかを制御できます。詳細については、Oracle のドキュメント『コンパートメントの管理(Managing Compartments)』を参照してください。

**手順**

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。

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。
3. VCN のわかりやすい**名前**を入力します(例:*FMCv-Management*)。
4. VCN の **CIDR ブロック**を入力します。
5. [VCN の作成(Create VCN)] をクリックします。

### 次の作業

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 VNICS と、VNICS に適用される一連のセキュリティルールで構成されます。

### 手順

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。
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* )。
3. [次へ(Next)] をクリックします。
4. 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(TCP/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。

      Firepower デバイスは Firepower Management Center を介して管理できます。これには、HTTPS 接続用にポート 8305 を開く必要があります。Firepower Management Center 自体にアクセスするには、ポート 443 が必要です。
5. [作成(Create)] をクリックします。

## インターネットゲートウェイの作成

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

### 手順

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。
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*)。
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。
4. インターネットゲートウェイへのルートを追加します。
   a. [ネットワーキング(Networking)] > [仮想クラウドネットワーク(Virtual Cloud Networks)] > [仮想クラウドネットワークの詳細(Virtual Cloud Network Details)] > [ルートテーブル(Route Tables)] を選択します。
   b. ルートルールを追加するには、デフォルトのルートテーブルのリンクをクリックします。
   c. [ルートルールの追加(Add Route Rules)] をクリックします。
   d. [ターゲットタイプ(Target Type)] ドロップダウンから、[インターネットゲートウェイ(Internet Gateway)] を選択します。
   e. 宛先 CIDR のブロックを入力します(例:0.0.0.0/0)。
   f. [ターゲットインターネットゲートウェイ(Target Internet Gateway)] ドロップダウンから、作成したゲートウェイを選択します。
   g. [ルートルールの追加(Add Route Rules)] をクリックします。

## サブネットの作成

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

### 手順

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。
2. サブネットのわかりやすい**名前**を入力します(例:*Management*)。
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)。
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。
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。
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。
7. [DHCP オプション(DHCP Option)] を選択します。
8. 以前作成した [セキュリティリスト(Security List)] を選択します。
9. [サブネットの作成(Create Subnet)] をクリックします。

### 次の作業

管理 VCN を設定すると、FMCv を起動する準備が整います。FMCv VCN 構成の例については、図 2 FMCv 仮想クラウドネットワーク(5 ページ)を参照してください。

**図 2　FMCv 仮想クラウドネットワーク**


# OCI での FMCv インスタンスの作成

Oracle Cloud Marketplace で Cisco Firepower Management Center Virtual(FMCv)- BYOL の製品を使用して、コンピューティング インスタンス経由で OCI に FMCv を展開します。CPU の数、メモリの量、ネットワークリソースなどの特性に基づいて、最適なマシンシェイプを選択します。

### 手順

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。
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。

3. [マーケットプレイス(Marketplace)] で「Cisco Firepower Management Center Virtual(FMCv)」を検索し、製品を選択します。
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。
5. [インスタンスの起動(Launch Instance)] をクリックします。
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*)。
7. [シェイプの変更(Change Shape)] をクリックし、FMCv 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(表 1 OCI でサポートされるシェイプタイプ(1 ページ)を参照)。
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。
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。
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。
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。
12. [SSH キーの追加(Add SSH keys)] の下で、[SSH キーの貼り付け(Paste SSH 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。
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。
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、FMCv の day0 構成を指定します。

    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"
}
```

[作成(Create)] をクリックします。

### 次の作業

[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 FMCv インスタンスをモニタします。ステータスをモニタすることが重要です。FMCv 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。

# OCI での FMCv 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、『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。

**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 FMCv 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。

# SSH を使用した FMCv インスタンスへの接続

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

### 手順

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。

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>
   ```

   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、FMCv インスタンスのユーザ名です。

   *<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 FMCv インスタンスへの接続

Windows システムから FMCv 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。

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。
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、FMCv インスタンスのユーザ名です。

   *<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。

# PuTTY を使用した FMCv インスタンスへの接続

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

1. PuTTY を開きます。
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、FMCv インスタンスのユーザ名です。

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

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

OCI での FMCv インスタンスへのアクセス