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

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 *1*：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 *2*：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

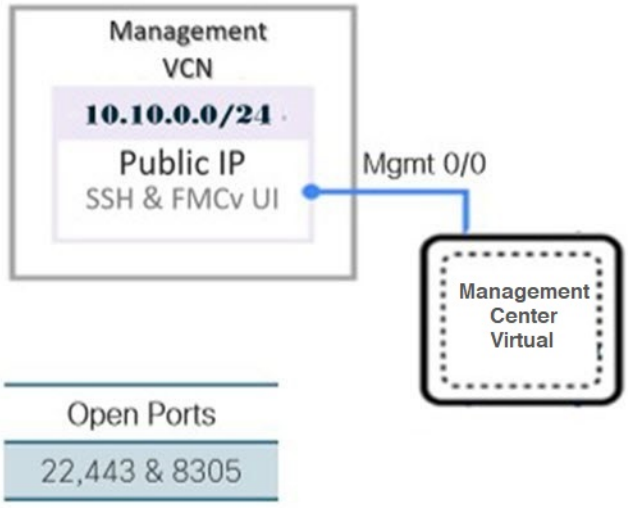
サポートされない機能

- 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 *1 : 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で、**[作成（Create）]** をクリックします。

ファイアウォールルールの作成

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

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

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

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

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

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

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

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

ステップ 7 セキュリティルールを追加します。

a) SSH（TCP/22）を許可するルールを追加します。

b) TCP ポート 443 を許可するルールを追加します。

HTTPS 接続用にポート 443 を開く必要がある 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 （1 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-fmcv"
}
```

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

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

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

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

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

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

- **[ネットワーク（Network）]** ドロップダウンリストから、[VPC network（VPC ネットワーク）]（*vpc-branch-mgmt* など）を選択します。
- **[外部 IP（External IP）]** ドロップダウンリストから、適切なオプションを選択します。

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

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

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

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

ステップ 5 [展開（Deploy）] をクリックします。

（注） 起動時間は、リソースの可用性など、さまざまな要因によって異なります。初期化が完了するまでに最大で35分かかることがあります。初期化は中断しないでください。中断すると、アプライアンスを削除して、最初からやり直さなければならないことがあります。

次のタスク

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

GCP 上の 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 （5 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。

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。