AWS クラウドへの Firepower Management Center Virtual の展開

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。

Firepower Management Center Virtual（FMCv）は AWS クラウドに導入できます。

AWS クラウドへの展開の概要

AWS は、プライベート Xen ハイパーバイザを使用するパブリック クラウド環境です。FMCv は、Xen ハイパーバイザの AWS 環境内でゲストとして実行されます。

AWS 上の FMCv は、次のインスタンス タイプをサポートします。

- c3.xlarge と c4.xlarge：4 つの vCPU、7.5 GB、2 つのインターフェイス、1 つの管理インターフェイス
- c3.2xlarge と c4.2xlarge：8 つの vCPU、15 GB、3 つのインターフェイス、1 つの管理インターフェイス

（注） FMCv は AWS 環境外部の Xen ハイパーバイザをサポートしていません。

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、FMCv を導入する際には、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。

AWS 展開に関するガイドラインおよび制限事項

前提条件

次に、AWS 上の FMCv 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。
- FMCv 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、[Firepower Management Center Virtual ライセンス]を参照してください。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。
- FMCv 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：

- FMCv にアクセスするためのパブリック IP/Elastic IP。

- FMCv と Firepower System の互換性については、『Cisco Firepower Compatibility Guide』を参照してください。

ガイドライン

次に、AWS 上の FMCv 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導入

制限事項

次に、AWS 上の FMCv に関する制限事項を示します。

- Cisco Firepower Management Center Virtual の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 アドレス設定は（CLI から設定したものでも Firepower Management Center から設定したものでも）AWS コンソールで作成されたものと一致する必要があります。展開時に設定を書き留めてください。
- IPv6 は現時点でサポートされていません。
- 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。
- ハイ アベイラビリティはサポートされません。

AWS 環境の設定

FMCv 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、FMCv 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

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。Firepower Management Center Virtual のインスタンスなどの AWS リソースを VPC で起動できます。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Firepower Management Center Virtual のインスタンスに使用できることを確認します。

ステップ 1 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に確認してください。

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 を識別するユーザ定義の [Name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

- FMCv 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 ユーザ定義の [Name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

Firepower 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。Firepower Threat Defense Virtual の場合、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定義の [Name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定義の [Name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 FMCv 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。

a) セキュリティ グループを識別するユーザ定義の [セキュリティグループ名（Security group name）]。

b) このセキュリティ グループの [説明（Description）]。

c) 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。

a) [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） FMCv 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、FMCv と FTDv 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。

b) [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、FMCv 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。

a) 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定義の [説明（Description）]。

b) ドロップダウン リストから [サブネット（Subnet）] を選択します。Firepower 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。

c) [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。

d) [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、FMCv 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、FMCv に 1 つの Elastic IP アドレス、Firepower 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、FMCv を展開します。

Firepower Management Center Virtual のインスタンスの展開

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 FMCv 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 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、Firepower 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 Firepower 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、「AWS クラウドへの展開の概要」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）] の下で、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。

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、FMCv 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に数行の出力が続きます。

これで、SSH または HTTP を使用して、新規に作成した FMCv 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 FMCv 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 FMCv 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。FMCv 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に数行の出力が続きます。
- Elastic IP を保持し、それが Firepower 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

Firepower 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、Firepower Management Center ユーザ インターフェイスを使用して AWS で実行している Firepower Threat Defense Virtual 用のデバイス管理設定を構成したり、アクセス コントロール ポリシーや Firepower Threat Defense Virtual のデバイスを使用してトラフィックを管理するためのその他の関連ポリシーを設定および適用することができます。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、Firepower Threat Defense Virtual で提供されるサービスを制御します。Firepower Threat Defense Virtual で Firepower Management Center を使用してセキュリティ 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、Firepower の構成ガイドまたは Firepower Management Center のオンライン ヘルプを参照してください。

-