AWS 環境でのコントローラのインストール

Amazon Web Services の概要

コントローラは、パブリック クラウド ソリューション用に Amazon Web Service（AWS）に導入できます。

前提条件

AWS でコントローラの起動を試みる前に、次の前提条件を満たす必要があります。

- AWS アカウントを作成します。
- コントローラ コンソールにアクセスするには、SSH クライアント（Windows 場合の Putty、Macintosh の場合はターミナルなど）が必要です。
- 導入するインスタンス タイプを決定します。
- IAM ユーザを作成します。
- キー ペアを作成します。
- VPC を作成します。

- セキュリティ グループを作成します。
- VPN ゲートウェイを作成します。
- サブネットを作成します。
- リモート サイトごとに次を作成します。
  - カスタマ ゲートウェイを作成します。
  - VPN 接続を作成します。

一般情報

- パブリック クラウド内のすべてのインターフェイスがレイヤ 3 です。トランク インターフェイスはありません。
- パブリック クラウドのすべての IP 割り当てはパブリック クラウドの DHCP を使用して実行されます。コントローラに割り当てる IP を決めることができます。
- インターフェイスは 1 つのみがサポートされます。このインターフェイスはデバイス管理とワイヤレス管理で共有されます。

仮想プライベート クラウドの作成

次の手順に従って AWS で VPC を設定します。

始める前に

- VPC は AWS アカウント専用の仮想ネットワークで、AWS クラウド内の他の仮想ネットワークからは論理的に分離されています。
- VPC の IP アドレス範囲の指定、サブネットの追加、セキュリティ グループの関連付け、およびルート テーブルの設定を行えます。
- 必要に応じて、IPsec AWS 管理対象の VPN 接続を使用して VPC を会社のデータセンターに接続し、AWS クラウドをデータセンターとして拡張します。

（注） VPN 接続は、VPC に接続されている仮想プライベート ゲートウェイと、データセンターにあるカスタマ ゲートウェイで構成されます。仮想プライベート ゲートウェイは VPN 接続の Amazon 側の VPN コンセントレータです。カスタマ ゲートウェイは VPN 接続のユーザ側の物理デバイスまたはソフトウェア アプライアンスです。

ステップ 1 ナビゲーション パス（[AWS Console] > [VPC Dashboard] > [Launch VPC Wizard] > [VPC with a Private Subnet Only and Hardware VPN Access] ）を使用して VPN 設定を選択します。

ステップ 2 [VPC with a Private Subnet Only and Hardware VPN Access] ウィンドウで詳細を入力します。

ステップ 3 ナビゲーション パス（[VPC Console] > [Subnets] > [Create Subnet]）を使用してサブネットを作成します。

ステップ 4 ナビゲーション パス（[VPC Console] > [Security Groups] > [Create Security Group]）を使用してセキュリティ グループを作成します。

セキュリティ グループは、1 つ以上のインスタンスで発着信するトラフィックを制御する仮想ファイアウォールです。インスタンスが起動すると、1 つ以上のセキュリティ グループをそのインスタンスに関連付けることができます。インスタンスに対してデフォルトのセキュリティ グループを使用できますが、インスタンスのロールを反映するセキュリティ グループを作成することをお勧めします。

ステップ 5 [Create] をクリックします。

これにより VPC が作成されます。

仮想プライベート ゲートウェイの作成

次の手順に従って、AWS 仮想プライベート ゲートウェイを作成します。

始める前に

ステップ 1 [VPN Connections] > [Virtual Private Gateway] をクリックします。

[Create Virtual Private Gateway] ウィンドウが表示されます。次の詳細を入力します。

a) 名前タグを入力します。

AWS VPN ルータ名を使用します。

b) ASN を選択します。

カスタム ASN を使用するか、または Amazon ゲートウェイによって選択されたデフォルトの ASN のいずれかを使用します。

（注） AWS VPN ゲートウェイを作成した後は切断と表示されるため、VPC に接続する必要があります。

ステップ 2 [Actions] ボタンをクリックし、[Attach to VPC] を選択します。

ステップ 3 ポップアップ ウィンドウで、以前作成した VPC を選択します。

VPC に AWS VPN を接続します。

カスタマ ゲートウェイの作成

次の手順に従ってカスタマ ゲートウェイを作成します。

ステップ 1 AWS コンソールから [VPC] ダッシュ ボードに移動します。

ステップ 2 [VPN Connections] > [Customer Gateways] をクリックします。

ステップ 3 [Create Customer Gateway] をクリックします。

[Create Customer Gateway] ウィンドウが表示されます。次の詳細を入力します。

a) VPN ルータの名前。
b) [dynamic] または [static] としてルーティングを選択します。
c) ルータまたはファイアウォールの外部のインターネットのルーティング可能なアドレスを入力します。

ステップ 4 [Create Customer Gateway] をクリックします。

VPN 接続の作成

次の手順に従ってカスタマ ゲートウェイを作成します。

ステップ 1 AWS コンソールから [VPC] ダッシュ ボードに移動します。

ステップ 2 [VPN Connections] > [VPN Connections] をクリックします。

ステップ 3 [Create VPN Connection] をクリックします。

[Create VPN Connection] ウィンドウが表示されます。次の詳細を入力します。

a) VPN 接続の名前。
b) AWS VPN ゲートウェイとカスタム ゲートウェイを選択します。
c) [dynamic] または [static] としてルーティングを選択します。
d) VPN を通じて到達可能なリモート サブネットを入力します。

リモート サブネットは、AP がオンプレミスとなるリモート ネットワークです。

ステップ 4 （オプション）IPSEC VPN のトンネル インターフェイスにサブネットとキーを割り当てます。

AWS は冗長性を確保するために 2 つのインターフェイスを作成します。詳細を指定しなかった場合は、AWS はランダムにトンネル オブジェクトを生成します。

ステップ 5 [Create VPN Connection] をクリックします。

これにより、VPN 接続が作成されます。接続をセットアップし、ステータスを [pending] から [available] に変化させるまでに数分かかります。

ステップ 6 VPN を作成している間に、設定をダウンロードして、カスタマ VPN ルータに導入できます。[Download Configuration] をクリックします。

ステップ 7 ポップアップ ウィンドウで、カスタマ VPN ルータのブランドとタイプを選択します。

ステップ 8 [Download] をクリックします。

キー ペアの作成

次の手順に従ってカスタマ ゲートウェイを作成します。

ステップ 1 AWS コンソールから **EC2** ダッシュ ボードに移動します。

ステップ 2 [Network & Security] > [Key pairs] をクリックします。

ステップ 3 [Create Key Pair] をクリックします。

Cloud Formation テンプレートを使用した AWS でのコントローラのインストール

始める前に

- VPC はコントローラ管理インターフェイスに適切なサブネットで作成します。
- エンタープライズ サイトから VPC に管理対象の VPN 接続が作成されます。
- AWS マーケットプレイスから CloudFormation テンプレートをダウンロードし、コンピュータに保存します。

ステップ 1 AWS コンソールから [CloudFormation] ページに移動します。

ステップ 2 [Create Stack] をクリックします。

ステップ 3 [Choose a template] セクションで、[upload template to Amazon S3] オプションを選択します。

これにより、*json* ファイルを AWS を直接ロードします。

ステップ 4 [Next] をクリックします。

これにより、[Specify Details] ページが表示されます。

ステップ 5 [Stack] と [Instance Details] に入力します。

必要なスタックの名前を入力します。ホスト名はコントローラの名前です。インスタンスのキー ペアはキー ペアの名前です。AMI ID は EC2 インスタンスの AMI です。

ステップ 6 [Next] をクリックします。

これにより、[Network Details] ページが開きます。

ステップ 7 [Network] と [User] に詳細を入力します。

管理ネットワークと管理セキュリティについては、ドロップダウンを使用してサブネットとセキュリティグループを選択します。ユーザ名とパスワードを入力し、インスタンスをリモートから接続します。

ステップ 8 [Next] をクリックします。

ステータスが「CREATE_IN_PROGRESS」から「CREATE_COMPLETE」に移行するまで待機します。

ステップ 9 [Instance Type] を選択します。

ステップ 10 **EC2** ダッシュボードに移動して [Running Instances] をクリックします。

新しいインスタンスは、[Status Checks]（システム ステータス チェックおよびインスタンス ステータス チェック）が [Initializing] と表示されます。緑色に変わるまで数分待ちます。

ステータスが緑色に変わったら、クラウドのコントローラを使用する準備が整います。定義されたクレデンシャルを使用するか、.pem ファイルを使用し、SSH で接続できます。

AWSコンソールを使用したコントローラのインストール

次の手順を従い、AWS コンソールでコントローラをインストールします。

ステップ 1 AWS コンソールから [EC2 Management] ページに移動します。

ステップ 2 [Launch Instance] をクリックします。

ステップ 3 [My AMIs] をクリックし、クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ の AMI を選択します。

ステップ 4 [Instance Type] を選択します。

要件に従ってインスタンスを選択することをお勧めします。

ステップ 5 [Instance Details] を設定します。

a) [Availability Zone] を選択します。
b) [Network] を選択します。
c) [Subnet] を選択します。
d) 他のユーザに、インスタンスの使用を制限または許可する IAM を関連付けます。

（注） 起動中にパブリック IP を無効にする必要があります。

ステップ 6 [Add Storage] ページに移動します。

このオプションのステップを使用して、インスタンスに接続する追加のボリュームを指定します。

ステップ 7 [Add Tags] ページに移動します。

a) [Tag Volumes] に入力します。

b) [Interfaces] を選択します。

c) [Instance] を選択します。

ステップ 8 [Configure Security Group] に移動します。セキュリティ グループを選択します。関連するセキュリティ グループがない場合は、新しいものを作成します。

ステップ 9 [Review and Launch] をクリックします。インスタンスの設定を確認します。

ステップ 10 [Launch Instances] をクリックします。

インスタンスを起動する前に、インスタンスにアクセスするキー ペアが必要です。キー ペアは、AWS が保存する公開キーとユーザが保存するプライベート キーで構成されます。キーがない場合は、[Create a new keypair] をクリックして新しいキーを作成するか、または既存のキーペアを選択します。

次のタスク

インスタンスが起動したら、次の unix コマンドを端末上で使用して クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ インスタンスに接続することができます。

```
ssh -i path_to_pem_file ec2-user@[public-ip|DNS name]
```

EC2 インスタンス コンソールのインスタンスの説明から IP と DNS 名を取得できます。

AWS のブートストラップのプロパティ

表 *1 : AWS* のブートストラップのプロパティ

プロパティ	説明
hostname	次の例に示すように、ルータのホスト名を設定します。 `hostname="c9800-aws-instance"`
domain-name	次の例に示すように、ネットワーク ドメイン名を設定します。 `domain-name="cisco.com"`
mgmt-ipv4-gateway	次の例に示すように、IPv4 管理用のデフォルトのゲートウェイ アドレスを設定します。 `mgmt-ipv4-gateway="dhcp"`

プロパティ	説明

ios-config	Cisco IOS コマンドの実行を有効にします。複数のコマンドを実行するには、複数の ios-config のインスタンスと各インスタンスに付加されている番号（ios-config-1、ios-config-2 など）を使用します。
	
	Cisco IOS コマンドを指定すると、エスケープ文字を使用してコマンド内にある特殊文字（アンパサンド（&）、二重引用符（”）、一重引用符（'）、よりも小さい（<）、またはよりも大きい（>））を渡します。次の例の「ios-config-5」を参照してください。
	
	`ios-config-1="username cisco priv 15 pass ciscoxyz"`
	`ios-config-2="ip scp server enable"`
	`ios-config-3="ip domain lookup"`
	`ios-config-4="ip domain name cisco.com”`
	`ios-config-5="event syslog pattern "\(Tunnel1\) is down: BFD peer down notified""`