AWS Cloud での Cisco SD-WAN コントローラの展開

表 *1* : 機能の履歴

機能名	リリース情報	説明
AWS での Cisco SD-WAN コントローラの展開	Cisco vManage リリース 20.6.1	この機能により、Amazon AWS 環境に Cisco SD-WAN コントローラ（Cisco vManage、Cisco vSmart コントローラ、および Cisco vBond オーケストレーション）を展開できます。

AWS での Cisco SD-WAN コントローラの展開について

サポートされる最小のコントローライメージ：Cisco vManage リリース 20.6.1、Cisco vSmart コントローラリリース 20.6.1、および Cisco vBond Orchestrator リリース 20.6.1。

Amazon Machine Images（AMI）を使用して、Amazon Web Services（AWS）環境に次の Cisco SD-WAN コントローラを展開できます。Cisco vManage、Cisco vSmart コントローラ、および Cisco vBond オーケストレーション。

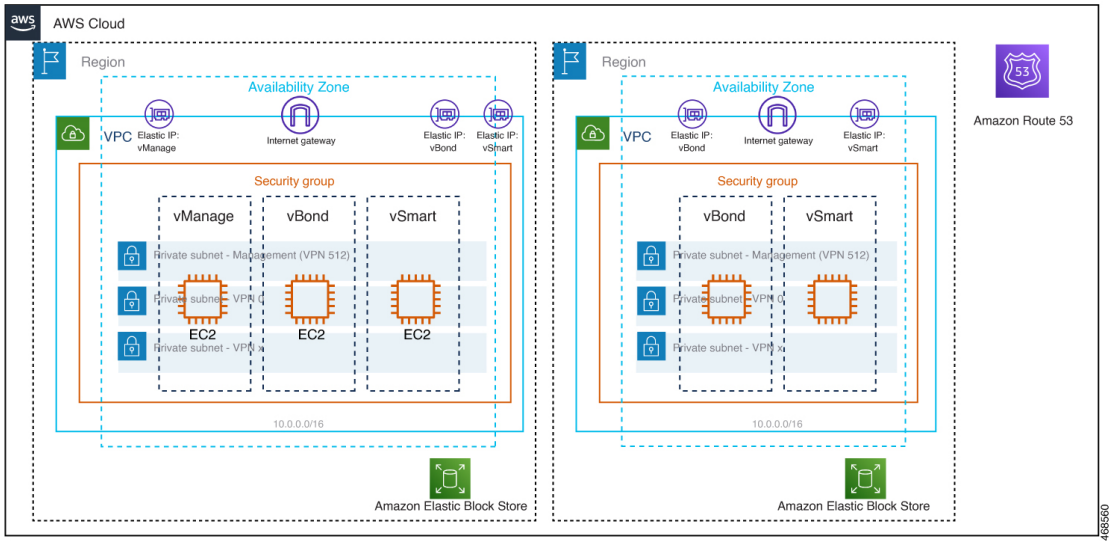
シスコが提供する AMI イメージは対象のユーザー専用です。他の人と共有しないでください。次を実行できます。

- 注文数量に応じた数のコントローラを展開できます。たとえば、50 個の Cisco vManage コントローラ PID を注文した場合、AWS アカウント内に展開できる Cisco vManage コントローラは 50 個のみです。

- 注文した PID の数を超えなければ、リージョン間および独自の AWS アカウント間で AMI をコピーできます。
- コントローラの初期展開後は、アップグレードまたはダウングレードをユーザーが実行する必要があります。

次の図は、AWS リージョン、仮想プライベートクラウド（VPC）、セキュリティグループなどのアーキテクチャを示しており、アーキテクチャ内で Cisco SD-WAN コントローラが機能する場所を示しています。

図 *1 : AWS* 内の *Cisco SD-WAN* コントローラ



AWS に Cisco SD-WAN コントローラをインストールする前の考慮事項

- Cisco SD-WAN コントローラ AMI は、Cisco Software Download サイトや AWS マーケットプレイスでは入手できません。AMI は、AWS クラウドアカウントで Cisco SD-WAN コントローラをセットアップするための有効なビジネスケースとともにリクエストした場合にのみ提供されます。
- AWS で使用する Cisco SD-WAN コントローラの注文については、シスコアカウントチームまたはシスコパートナーにお問い合わせください。
- シスコは、コントローラのプロビジョニングまたはインストール中にクラウドインフラストラクチャで発生する問題のサポートを提供していません。
- トラブルシューティング：
  - 機能の問題：機能の問題については、Cisco TAC ケースを開いてください。
  - インフラストラクチャの問題：インフラストラクチャの管理、監視、およびトラブルシューティングはお客様が行う必要があります。コントローラがプロビジョニングされ、クラウドアカウントで実行されると、シスコはクラウドインフラストラクチャ関連の問題のサポートを提供しません。

- ソフトウェアのアップグレード：コントローラソフトウェアのアップグレードに AMI イメージは不要です。『*Cisco SD-WAN* モニタリングおよびメンテナンス コンフィギュレーション ガイド』の「Manage Software Upgrade and Repository」の章の説明に従って、Cisco Software Download サイトからコントローライメージをダウンロードし、コントローラソフトウェアをアップグレードできます。https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And-Maintain/monitor-maintain-book/maintain.html

AWS で Cisco SD-WAN コントローラを展開する利点

- セットアップコスト：追加のデータセンターインフラストラクチャを購入する必要がないため、オンプレミスホスティングと比較して初期セットアップコストが低い。
- 展開：クラウドベースの展開の容易さ。
- 管理：世界中のデバイスを管理する機能。
- 安定性：AWS ホスティングは、その信頼性により、Cisco SD-WAN コントローラに安定した環境を提供。
- セキュリティ：AWS は、セキュアなホスティング環境を提供。
- 拡張性：AWS は、Cisco SD-WAN ネットワークの規模を拡大する容易な方法を提供。

AWS で Cisco SD-WAN コントローラを展開するための前提条件

- 有効（かつアクティブ）な AWS およびシスコアカウントが必要です。
- クラウドの導入に適したコントローラ PID を注文するための PID 情報については、シスコアカウントチームにお問い合わせください。

AWS に Cisco SD-WAN コントローラを展開するユースケース

- ユースケース 1：独自のパブリッククラウドアカウントを使用して、コントローラのプロビジョニング、管理、監視、および拡張性を完全に制御します。
- ユースケース 2：特定のアーキテクチャまたはセキュリティ態勢の要件。

AWS での Cisco SD-WAN コントローラの展開：タスク

（注） ここで説明する手順は、3 つのタイプの Cisco SD-WAN コントローラ（Cisco vManage、Cisco vSmart コントローラ、および Cisco vBond オーケストレーション）に適用されます。特定のコントローラについて指示が異なる場合は、その旨を示します。

タスク 1：AWS AMI イメージのリクエスト

AMI イメージを使用して AWS アカウントに Cisco SD-WAN コントローラを展開できます。

1. Cisco SD-WAN コントローラ AMI は、Cisco CloudOps チーム（sdwan-cloudops-pm@cisco.com）に電子メールでリクエストしてください。リクエストには次の詳細情報を記載してください。
   - 顧客名
   - 要件：ビジネスケースの詳細
   - コントローラ PID を含む注文番号
   - SW バージョン要件
   - AWS アカウント番号
   - コントローラを展開する地域
2. 顧客が管理する Cisco SD-WAN コントローラ PID の注文情報を検証した後、Cisco CloudOps チームは AWS クラウドアカウントで Cisco SD-WAN コントローラの AWS AMI イメージを公開します。

（注） CloudOps チームが提供する AMI イメージは対象のユーザー専用です。他の人と共有しないでください。イメージが他の人と共有された場合、シスコはイメージを削除し、イメージが共有されないようにするために必要な措置を講じる権利を留保します。

タスク 2：AWS で VPC、サブネット、およびセキュリティグループを作成する

（注） AWS のタスクの詳細については、AWS のドキュメントを参照してください。

AWS ポータルで次の手順を実行します。

1. 仮想プライベートクラウド（VPC）を作成し、VPC の作成中に次のアクションを実行してください。
   - VPC の名前とリージョンを入力します。
   - VPC のアドレス空間を入力します。例：10.0.0.0/16
   - 少なくとも 2 つのサブネットを VPC に追加し、Cisco vManage クラスタを作成する予定の場合は追加のサブネットを追加します。サブネットごとに、サブネットの名前とアドレス空間を指定します。後の手順で、追加したサブネットを仮想マシンのネットワーク インターフェイスに関連付けます。

     例：
     - サブネット 0 をアドレス 10.0.1.0/24 で追加します。これは、コントローラのプライマリインターフェイスとして使用される VPN 512 になります。
     - サブネット 1 をアドレス 10.0.2.0/24 で追加します。これは、VPN 0 のコントローラのトランスポートまたはトンネルインターフェイスとして使用されます。
     - サブネット 2 をアドレス 10.0.3.0/24 で追加します。これは Cisco vManage クラスタリングに使用されます（Cisco vManage クラスタの展開で必要な場合のみ）。
   - （オプション）VPC を分類するタグを入力します。
2. VPC に必要なリソースを作成して、コントローラインスタンスを実行するための環境を形成します。
   - セキュリティグループには、次のものが含まれている必要があります。
     - 管理目的でコントローラにアクセスするためのユーザー NOC センターの送信元パブリック IP アドレス。
     - すべてのエッジがコントローラに参加するための TLS/DTLS に対するすべての TCP/UDP ポートのアドレス 0.0.0.0/0。
     - 各コントローラが他のコントローラに到達するためのパブリック IP を有効にします。
   - セキュリティグループの名前とリージョンを入力します。
   - （オプション）セキュリティグループを分類するタグを入力します。
3. 新たに作成したセキュリティグループを、手順 1 で作成したサブネットに関連付けます。
4. インターネットゲートウェイを作成し、VPC に関連付けます。
5. ルーティングテーブルを作成し、VPC に関連付けます。インターネットゲートウェイを指すデフォルトルートエントリを追加します。

タスク 3：コントローラの仮想マシンの作成

（注） AWS のタスクの詳細については、AWS のドキュメントを参照してください。

AWS ポータルで次の手順を実行します。

1. 仮想マシンを作成するためのワークフローを開始します。仮想マシンを作成するときは、次のアクションを実行してください。
   - タスク 2 で作成した仮想プライベートクラウド（VPC）に仮想マシンを展開します。
   - 仮想マシンの名前とリージョンを入力します。
   - イメージの場合は、Cisco vManage、Cisco vBond オーケストレーション、または Cisco vSmart コントローラ に対して適切な共有コントローラ AMI を選択します。

（注） カスタムイメージを見つける方法については、AWS のドキュメントを参照してください。

   - 仮想マシンのサイズについては、コントローラに使用する CPU とメモリの数を含むオプションを選択します。Cisco SD-WAN コントローラ デバイスの互換性と Cisco SD-WAN コントローラ サーバの要件については、『Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations』 を参照してください。
   - 認証タイプ（SSH 公開キーやパスワードなど）を選択し、必要に応じてログイン情報を入力します。
   - ディスクリソースについては、次のいずれかを実行します。
     - Cisco vSmart コントローラ または Cisco vBond オーケストレーション を展開する場合、デフォルト以外の追加のディスクリソースは必要ありません。
     - Cisco vManage コントローラを展開する場合は、ディスクを 1 つ選択します。
       - Premium SSD オプションとデフォルトの暗号化を選択します。
       - 1 TiB（AWS では P30 と呼ばれる）以上のディスクサイズを選択します。

         AWS のコントローラに関連するサーバーの推奨事項については、「Cisco SD-WAN コントローラの互換性マトリックスとサーバーの推奨事項」を参照してください。

       - ディスクホストキャッシュを読み取り/書き込みとして設定します。

     - ネットワークの詳細については、前の手順で作成した VPC、サブネット、およびセキュリティグループを選択します。各仮想マシンには 2 つのネットワーク イン

ターフェイスが必要です。1 つは VPN 512 管理サブネット用、もう 1 つは VPN 0 トンネルサブネット用です。

- Elastic IP アドレスを各コントローラの VPN 0 および VPN 512 ネットワーク インターフェイスに割り当てます。
- （オプション）高度なブート診断（管理オプション）を有効にして、診断ログを格納するための追加のストレージアカウントをリソースグループに作成します。
- Cisco SD-WAN コントローラリリース 20.6.1 以降では、必要に応じてカスタムデータ機能を使用して、再起動時に仮想マシンが実行するコマンドを入力できます。
- （オプション）タグを追加してコントローラを分類します。

2. 仮想マシンを作成したら、仮想マシン用に追加のネットワーク インターフェイス（NIC）を作成します。前のタスクで作成したリソースグループにネットワーク インターフェイスを作成します。
   - Cisco vSmart コントローラ または Cisco vBond オーケストレーション を展開している場合は、追加のネットワーク インターフェイスを 1 つ作成します。
   - Cisco vManage コントローラを展開する場合は、2 つの追加のネットワーク インターフェイスを作成します。
   - クラスタに Cisco vManage コントローラを展開している場合は、Cisco vManage アウトオブバンドインターフェイスの詳細について、「クラスタの管理」と「Cisco vManage の展開」を参照してください。
3. ネットワーク インターフェイスを作成するときは、次のアクションを実行してください。
   - タスク 2 で作成した VPC、サブネット、およびセキュリティグループを指定します。
   - NIC をサブネットに関連付けます。

     例：NIC 1 をサブネット 1 に関連付けます。
     - Cisco vManage コントローラを展開している場合は、NIC 2 をサブネット 2 に関連付けます。
     - Cisco vManage クラスタを使用している場合は、NIC 3 をサブネット 3 に関連付けます。

（注） NIC をサブネットに関連付けると、仮想マシンがサブネットに接続できるようになります。

   - NIC ごとに、展開するコントローラに使用するタグを入力します。
4. 使用するすべてのコントローラの静的パブリック IP を作成し、このパブリック IP を NIC 1 に関連付けます。

（注） AWS の IP 構成オプションを使用して、パブリック IP を作成します。

5. パブリック IP を作成するときは、次のアクションを実行してください。
   - 割り当てには、[static] を選択します。
   - NIC 1 を指定する場合は、関連付けオプションを使用します。
6. 仮想マシンを停止し、停止したことを確認します。
7. 新たに作成した NIC を仮想マシンに接続します。
   - Cisco vSmart コントローラ または Cisco vBond オーケストレーション を展開している場合は、NIC を仮想マシンに接続します。
   - Cisco vManage を展開している場合は、新たに作成した両方の NIC を仮想マシンに接続します。
8. 仮想マシンを再起動します。AWS ポータルで、仮想マシンが再起動したことを確認します。

タスク 4：セキュリティグループの設定

はじめる前に

セキュリティグループは、ファイアウォールポリシーに機能的に関連しています。セキュリティグループを設定するときは、Cisco SD-WAN のファイアウォールポートの設定を把握していると便利です。Cisco SD-WAN 展開のためのファイアウォールポートを参照してください。

（注） AWS のタスクの詳細については、AWS のドキュメントを参照してください。

セキュリティグループの設定

1. AWS ポータルを使用し、前のタスクで作成したセキュリティグループにインバウンド セキュリティ ルールを追加して、以下のために必要な IP 範囲からのインバウンドトラフィックを許可します。
   - 各 Cisco SD-WAN コントローラ間の制御接続の確立。コントローラが相互に接続されていない場合、コントロールプレーンとデータプレーンは動作できません。
   - HTTPS または SSH プロトコルを使用したコントローラへのアクセス。

2. セキュリティグループについては、インバウンドセキュリティルールを追加するオプションを使用します。ルールを使用して、すべてのコントローラの仮想マシンのIPアドレスを許可し、Cisco SD-WAN コントローラ間で必要な接続を有効にします。

   新しいインバウンド セキュリティ ルールを作成するときは、次のアクションを実行してください。

   - IP 範囲、プロトコルなどを指定します。
   - ルールのアクションについては、トラフィックを許可するオプションを選択します。

3. 接続を確認するには、Cisco vManage の NIC 0 パブリック IP を使用して仮想マシンにログインします。

AWS での Cisco SD-WAN コントローラの展開の確認

- インフラストラクチャ：AWS の仮想マシン内の Cisco SD-WAN コントローラの展開を確認するには、AWS ポータルを使用して、各コントローラをホストする仮想マシンがアクティブかどうかを確認します。
- サービス：コントローラの展開後に Cisco SD-WAN サービスが動作していることを確認するには、次の手順を使用します。

  1. Cisco vManage をホストする仮想マシンへの ping が成功することを確認します。
  2. AWS コンソールを使用して、admin ユーザーとしてコントローラインスタンスにログインします。新しいパスワードの設定を求められる場合があります。設定したら、コントローラのパブリック IP への SSH 経由のログインを確認します。
  3. SSH を使用して Cisco vManage に接続し、 **request nms all status** コマンドを使用します。出力には、すべての Cisco vManage サービスのステータスが表示されます。アプリケーションサーバーがアクティブになっていることを確認します。

     次の **request nms all status** コマンド出力の抜粋は、アプリケーションサーバーがアクティブであることを示しています。

     ```
     vmanage# request nms all status
     NMS service proxy
             Enabled: true
             Status: running PID:2881 for 9479s
     NMS service proxy rate limit
             Enabled: true
             Status: running PID:4359 for 9521s
     NMS application server
             Enabled: true
             Status:  running PID:6131 for 9419s
     ...
     ```

  4. コントローラをインストール後、「Cisco SD-WAN オーバーレイネットワークの起動プロセス」の手順に従って、コントローラの制御接続を確立し、各コントローラが動作していることを確認します。

AWS での Cisco SD-WAN コントローラの展開の監視

インフラストラクチャのステータス（CPU 使用率やディスク使用率など）を監視するには、AWS ポータルの監視ツールを使用します。

Cisco SD-WAN サービスのステータスのモニタリングについては、Cisco SD-WAN モニタリングおよびメンテナンスガイド [英語] 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。