# Microsoft Azure 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 |
|---|---|---|
| Azure 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、Microsoft Azure 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。 |



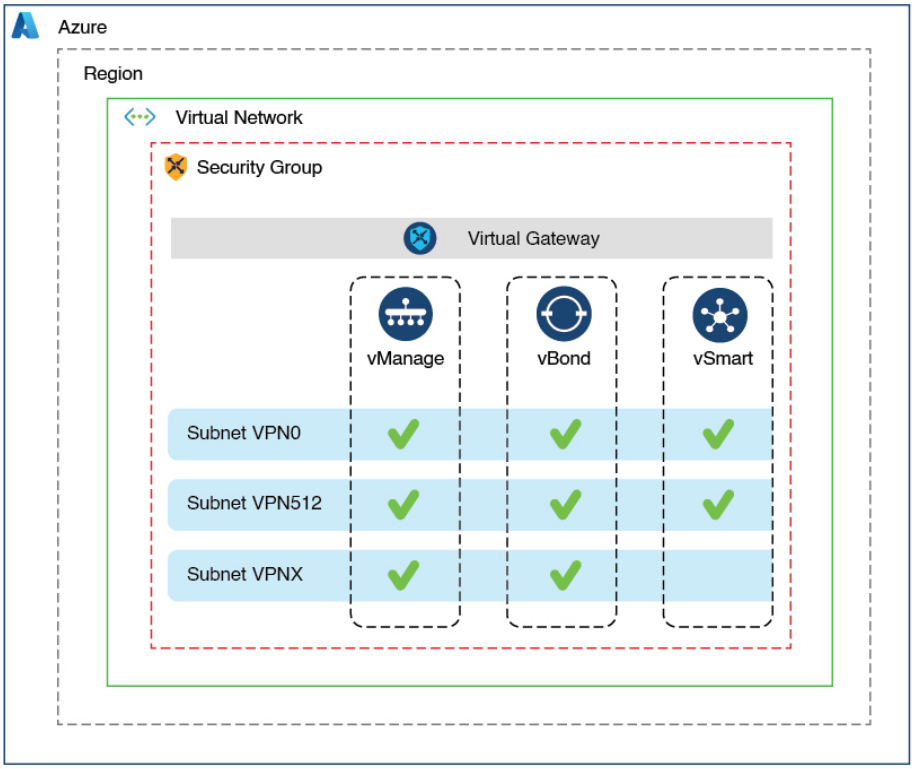
# Azure での Cisco SD-WAN コントローラの展開について

サポートされる最小限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 オーケストレーション リリース 20.6.1

Azure 環境には、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、Cisco vBond オーケストレーション。

次の図は、Azure リージョン、仮想ネットワーク、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 : Azure* での *Cisco SD-WAN* コントローラ




# Azure 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：Azure 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：Azure は、セキュアなホスティング環境を提供。
- 拡張性：Azure 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。

# Azure 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 Microsoft Azure サブスクリプションが必要です。

# Azure での Cisco SD-WAN コントローラの展開の使用例

すでに Azure を使用している Cisco SD-WAN 展開（Cisco Catalyst 8000V Edge ソフトウェアなど）の場合、Azure で Cisco SD-WAN コントローラをホストすることは、すべてのサービスの整合性を保つための論理的かつ効率的な選択です。

# Azure 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：Azure でのコントローライメージの作成

### はじめる前に

シスコの「Software Download」ページで、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）のイメージをダウンロードします。ダウンロードしたファイル（.tar 形式）を圧縮解除します。各コントローラのイメージファイルは、仮想ハードディスク（VHD）形式です。

Azure でのコントローライメージの作成

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

Azure ポータルで次の手順を実行します。

1. Azure のストレージアカウントをまだ持っていない場合は、今すぐ作成します。
   - ストレージアカウントの名前、場所などを指定します。
   - ネットワーク接続については、接続方式、ルーティング設定、データ保護、およびセキュアな転送に関するデフォルトオプションを使用します。
   - 必要に応じて、タグを入力してストレージアカウントを分類できます。
2. ストレージアカウントに新しいプライベートコンテナを作成します。コントローラを展開する予定のリージョンでストレージアカウントを選択します。

（注） 各コントローラには個別のコンテナが必要です。

3. コントローラの VHD ファイルをコンテナにアップロードします。

   アップロード手順の実行中に、Blob タイプとして [Page Blob] を選択します。

（注） Blob タイプの選択については、Azure のドキュメントを参照してください。

4. 前の手順でアップロードした VHD ファイルを選択して、新しいイメージを作成します。

   イメージを作成するときは、次のアクションを実行してください。

   - 有効なサブスクリプションを選択します。
   - 既存のリソースグループを選択するか、新しいリソースグループを作成します。
   - イメージの名前とリージョンを入力します。
   - OS については、[Linux] を選択します。
   - VM の世代については、[Gen 1] を選択します。
   - アカウントタイプについては、[Premium SSD] を選択します。
   - ホストキャッシングについては、[read/write] を選択します。
   - 暗号化については、デフォルト設定を選択します。
   - 必要に応じて、タグを入力してイメージを分類できます。

# タスク 2：Azure での仮想ネットワーク、サブネット、およびネットワーク セキュリティ グループの作成

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

Azure ポータルで次の手順を実行します。

1. 仮想ネットワークを作成するためのワークフローを開始します。

   仮想ネットワークを作成するときは、次のアクションを実行してください。

   - 有効なサブスクリプションを選択します。
   - 既存のリソースグループを選択するか、新しいリソースグループを作成します。

（注） リソースグループは、リージョン全体に展開したすべてのリソースを含む Azure の論理構造です。Cisco SD-WAN オーバーレイごとに 1 つのリソースグループを定義することをお勧めします。

- 仮想ネットワークの名前とリージョンを入力します。
- 仮想ネットワーク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 つのサブネットを仮想ネットワークに追加し、Cisco vManage クラスタを使用している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 VM ネットワーク インターフェイスに関連付けます。

  例：

  10.0.1.0/24
  10.0.2.0/24
  10.0.3.0/24

- 必要に応じて、タグを入力して仮想ネットワークを分類できます。

2. ネットワーク セキュリティ グループ（NSG）を作成するためのワークフローを開始します。

   ネットワーク セキュリティ グループを作成するときは、次のアクションを実行してください。

   - 有効なサブスクリプションを選択します。
   - 仮想ネットワークを作成するワークフローの一部として、前の手順で作成したリソースグループを選択します。
   - NSG の名前とリージョンを入力します。
   - 必要に応じて、タグを入力して NSG を分類できます。

3. 新たに作成した NSG を、前の手順で作成したサブネットに関連付けます。

# タスク 3：コントローラの仮想マシンの作成

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

Azure ポータルで次の手順を実行します。

1. 仮想マシン（VM）を作成するためのワークフローを開始します。

   VM 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 で作成した仮想ネットワークに VM を展開します。
   - 仮想ネットワークを作成するワークフローの間に、前のタスクで作成したリソースグループを選択します。
   - VM の名前とリージョンを入力します。
   - イメージには、アップロードされたコントローライメージを選択します。

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

   - VM 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サーバー要件については、「Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations」[英語] 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（Azure では P30 と呼ばれます）以上のディスクサイズを選択します。

         Azure 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 Controller Compatibility Matrix and Server Recommendations」[英語] 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仮想ネットワーク、サブネット、および NSG を選択します。
   - パブリック IP アドレスについては、次のオプションを選択します。
     - SKU：[Basic]
     - 割り当て：[static]

（注） Cisco SD-WAN にはコントローラの静的 IP アドレスが必要です。

- 必要に応じて、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できます。
- （コントローラリリース 20.6.1 以降）必要に応じて、カスタムデータ機能（詳細オプション）を使用して、再起動時に VM が実行するコマンドを入力できます。
- 必要に応じて、コントローラを分類するタグを追加できます。

2. VM を作成したら、VM 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。

   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。

   - 前のタスクで作成した仮想ネットワーク、サブネット、および NSG を指定します。
   - 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、VM 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。

3. 使用するすべてのコントローラに静的パブリック IP を作成し、そのパブリック IP を NIC 1 に関連付けます。

（注） Azure 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。

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。

4. VM を停止し、停止したことを確認します。
5. 新たに作成した NIC を VM 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 VM 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 VM に接続します。
6. VM を再起動します。

   VM が再起動したことを Azure ポータルで確認します。

# タスク 4：ネットワーク セキュリティ グループの設定

### はじめる前に

NSG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。NSGを設定するときは、Cisco SD-WANのファイアウォールポートの構成を把握していると便利です。ファイアウォールポートの詳細については、[Firewall Ports for Cisco SD-WAN Deployments]https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#c_Firewall_Ports_for_Viptela_Deployments_8690.xml を参照してください。

### ネットワーク セキュリティ グループの設定

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

1. Azure ポータルを使用し、前のタスクで作成した NSG 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。

NSG 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、コントローラの VM の IP アドレスをすべて許可し、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。

2. 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 VM にログインします。

# Azure 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：

  Azure 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、Azure ポータルを使用して、各コントローラをホストする VM がアクティブであることを確認します。

- 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 VM への ping が成功することを確認します。
  2. Cisco vManage にログインします。
  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。

# Azure 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、Azure 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。