



## Cloud OnRamp for IaaS

簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

- [Cisco Catalyst SD-WAN Cloud OnRamp for IaaS \(2 ページ\)](#)
- [概要 \(2 ページ\)](#)
- [サポートされている Cisco Cloud Service プロバイダーとサポートされている Cisco Catalyst SD-WAN クラウドデバイス \(4 ページ\)](#)
- [Cisco Catalyst SD-WAN クラウドデバイスの前提条件 \(5 ページ\)](#)
- [AWS の前提条件 \(9 ページ\)](#)
- [AWS での Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定 \(10 ページ\)](#)
- [ホストおよびトランジット VPC の管理 \(16 ページ\)](#)
- [Microsoft Azure の前提条件 \(21 ページ\)](#)
- [Microsoft Azure の Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定 \(25 ページ\)](#)
- [ホストおよびトランジット VNet の管理 \(30 ページ\)](#)
- [Cisco Catalyst SD-WAN Cloud OnRamp for IaaS のトラブルシューティング \(32 ページ\)](#)
- [機能テンプレートの設定例 \(36 ページ\)](#)
- [デバイステンプレート変数値の例 \(43 ページ\)](#)
- [Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の例 \(43 ページ\)](#)

# Cisco Catalyst SD-WAN Cloud OnRamp for IaaS

表 1: 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイスの Azure Government クラウドのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a	この機能により、Microsoft Azure Government クラウドで Cisco Catalyst 8000V デバイスを設定できます。これらのクラウドデバイスが Microsoft Azure Government クラウドでサポートされるようになったことで、Government クラウドのお客様は、Azure パブリッククラウドですでに利用可能なものと同じ高度なルーティングとセキュリティの利点を利用できます。
	Cisco vManage リリース 20.4.1	
Cisco IOS XE Catalyst SD-WAN デバイスの AWS Government クラウドのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a	この機能により、Amazon Web Services (AWS) Government クラウドで Cisco CSR1000V を設定できます。Cisco CSR1000V が AWS Government クラウドでサポートされるようになったことで、Government クラウドのお客様は、ルーティングのすべての利点を利用して、機密性の高いワークロードをクラウドに移動し、データを安全に管理することができます。
	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a	
	Cisco vManage リリース 20.4.1	このリリース以降では、AWS Government クラウドで Cisco Catalyst 8000V デバイスがサポートされます。

## 概要



- (注) Cisco vManage リリース 20.9.1 以降では、Cloud OnRamp for Multicloud を使用してクラウドインフラストラクチャを設定することを推奨します。Cloud OnRamp for IaaS は、今後のリリースで段階的に廃止されます。

Cisco Catalyst SD-WAN Cloud OnRamp for Infrastructure as a Service (IaaS) は、Cisco Catalyst SD-WAN オーバーレイネットワークのファブリックをパブリッククラウドインスタンスに拡張します。Cisco Catalyst SD-WAN Cloud OnRamp for IaaS を使用すると、Cisco Cloud Services Router 1000V シリーズと Cisco Catalyst 8000V デバイスを備えたブランチがパブリッククラウドアプリケーションプロバイダーに直接接続できます。物理データセンターの必要性を排除することで、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS は SaaS アプリケーションのパフォーマンスを向上させます。

Cisco Catalyst 8000V デバイスの詳細については、『[Cisco Catalyst 8000V Edge Software Configuration Guide](#)』を参照してください。

オーバーレイネットワークとパブリッククラウドアプリケーションの間の接続は、1～4つのペアの冗長 Cisco Catalyst SD-WAN クラウドデバイスによって提供されます。これらのデバイスは、オーバーレイネットワークとアプリケーションの間のトランジットとして連携して機能します。冗長デバイスを使用してトランジットを形成することで、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS によりパブリッククラウドに対するパスの復元力を得ることができます。さらに、冗長ルータを使用すると電圧低下保護に役立ち、パブリッククラウドアプリケーションの可用性が向上します。2つのルータが連携することで、電圧低下時に発生する可能性のあるリンクの通信品質の低下を修復できます。これらのデバイスは、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS ワークフローの一環として設定できます。

Amazon Web Services (AWS) および Microsoft Azure Government クラウド (GovCloud) での Cisco Catalyst SD-WAN Cloud OnRamp for IaaS サポートにより、機密データをホストするように Cisco CSR1000V および Cisco Catalyst 8000V デバイスを設定することができます。AWS または Microsoft Azure GovCloud (米国) は、米国政府の機関および取引先が機密性の高いワークロードを政府機関のクラウドに移動できるようにする、分離された AWS または Azure リージョンです。取引先は、ルーティング機能を提供し、強力な暗号スイートによるフルパス暗号化をサポートしているこれらのデバイスを使用できます。Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定中に選択できるリージョンは、AWS または Microsoft Azure GovCloud の仕様に関連しています。GovCloud (米国) アカウントの設定の詳細については、AWS GovCloud のドキュメントおよび Microsoft Azure GovCloud のドキュメントを参照してください。

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS は、AWS Virtual Private Cloud (VPC) および Azure Virtual Network (VNet) と連携して動作します。

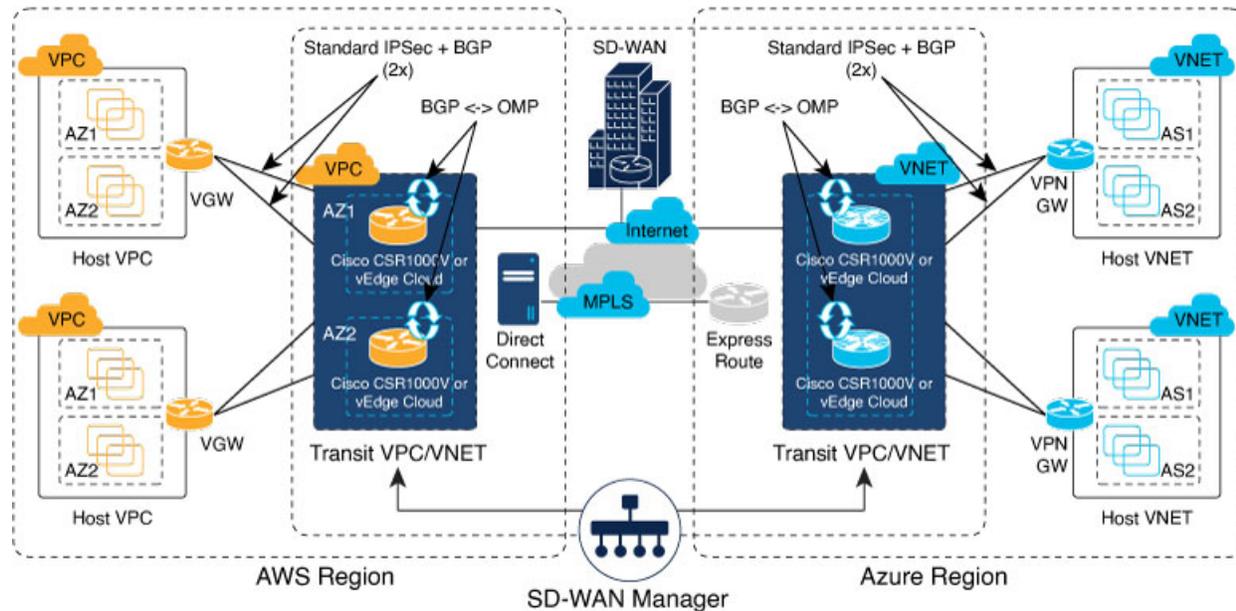
Cisco Catalyst SD-WAN Cloud OnRamp for IaaS ソリューションを展開するための主な手順は次のとおりです。

1. Cisco Catalyst SD-WAN Cloud OnRamp for IaaS に使用できる Cisco SD-WAN Manager 内の未使用の Cisco Catalyst SD-WAN クラウドデバイスのペアを 1～4 つ特定します。
2. 基本的なデバイステンプレートを設定し、両方の Cisco Catalyst SD-WAN クラウドデバイスにアタッチします。
3. Cisco SD-WAN Manager を使用して設定する場合は、AWS または Azure API のログイン情報 (アクセスキーと秘密キー) を入力します。
4. トランジット仮想プライベートクラウド (VPC) またはトランジット仮想ネットワーク (VNet) の設定を追加します。
5. ホスト VPC またはホスト VNet を検出し、トランジット VPC またはトランジット VNet にマッピングします。

次の図は、AWS と Microsoft Azure が統合された Cisco Catalyst SD-WAN Cloud OnRamp for IaaS のトポロジを示しています。オンプレミス上および複数のクラウド上にあるすべての Cisco Catalyst SD-WAN デバイスの単一サーバーとして Cisco SD-WAN Manager を使用して、すべての場所で同じポリシー、セキュリティ、およびその他の Cisco Catalyst SD-WAN のポリシーを適用することができます。AWS と Microsoft Azure のインフラストラクチャは、Cisco Catalyst

SD-WAN ファブリックにシームレスに統合できます。Cisco Catalyst SD-WAN Cloud OnRamp for IaaS ワークフローがすべての手順を自動化し、Cisco SD-WAN Manager サーバーが数分以内にソリューション全体を構築します。

図 1: Cisco Catalyst SD-WAN Cloud OnRamp for IaaS のトポロジ



## サポートされている Cisco Cloud Service プロバイダーと サポートされている Cisco Catalyst SD-WAN クラウドデバイス

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS では、次の IaaS パブリック クラウド プロバイダーがサポートされています。

- Amazon AWS
- Microsoft Azure

次のデバイスがサポートされています。

- Cisco Cloud Services Router 1000V シリーズ (Cisco CSR1000V)
- Cisco Catalyst 8000V Edge ソフトウェア (Cisco Catalyst 8000V)



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降では、Cisco Catalyst 8000V は Cisco CSR1000V に置き換わっています。そのため、Azure Government クラウドのサポートは Cisco Catalyst 8000V でのみ使用可能であり、Cisco Catalyst 8000V デバイスを使用することを推奨します。

このドキュメントでは、サポートされているデバイスをまとめて Cisco Catalyst SD-WAN クラウドデバイスと呼びます。

## Cisco Catalyst SD-WAN クラウドデバイスの前提条件

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS を設定する前に、次のデバイス要件を満たしていることを確認してください。

- Cisco SD-WAN Manager で、少なくとも 2 つの Cisco CSR1000V または Cisco Catalyst 8000V デバイスに使用可能なトークンまたはライセンスがあることを確認します。[Cisco SD-WAN Manager](#) での [Cisco Catalyst SD-WAN クラウドデバイスの有無の確認 \(6 ページ\)](#) を参照してください。
- 設定時に、トランジット VPC または VNet 内で使用する Cisco CSR1000V または Cisco Catalyst 8000V デバイスの機能テンプレートとデバイステンプレートを設定します。[Cisco Catalyst SD-WAN クラウドデバイスのデバイステンプレートの設定 \(7 ページ\)](#) を参照してください。
- トランジット VPC または VNet 内で使用する Cisco CSR1000V または Cisco Catalyst 8000V デバイスを表すソフトウェアトークンに、デバイステンプレートをアタッチします。[Cisco Catalyst SD-WAN クラウドデバイスへのデバイステンプレートのアタッチ \(7 ページ\)](#) を参照してください。

## Cisco SD-WAN Manager サーバーのプロビジョニング

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS を設定する前に、Cisco SD-WAN Manager サーバーをプロビジョニングします。

1. Cisco SD-WAN Manager サーバーがインターネットにアクセスできることを確認し、AWS または Microsoft Azure に到達できるように DNS サーバーを設定します。DNS サーバーを設定するには、Cisco SD-WAN Manager VPN 機能設定テンプレートで DNS サーバーの IP アドレスを入力します。次に、Cisco SD-WAN Manager を使用して設定テンプレートを VPN 機能に再アタッチします。
2. Cisco Catalyst SD-WAN Cloud OnRamp for IaaS を起動するには、少なくとも 2 つの Cisco Catalyst SD-WAN クラウドデバイスを Cisco SD-WAN Manager サーバーに追加してください。これら 2 つの Cisco Catalyst SD-WAN クラウドデバイスを適切な設定テンプレートにアタッチします。これらのデバイスの設定に次の属性が含まれていることを確認します。
  - ホストネーム

- Cisco Catalyst SD-WAN Validator の IP アドレス
- サイト ID
- 組織名
- eth1 インターフェイスでのトンネルインターフェイスの設定

Cisco CSR1000V または Cisco Catalyst 8000V デバイスでは、トンネルインターフェイスは GigabitEthernet2 インターフェイス上にあります。

3. Cisco SD-WAN Manager サーバーを現在の時刻と同期していることを確認します。現在の時刻を確認するには、Cisco SD-WAN Manager 画面の上部バーにある [Help (?)] アイコンをクリックします。[Timestamp] フィールドに現在の時刻が表示されます。時刻が正しくない場合は、Cisco SD-WAN Manager サーバーの時刻が Google NTP サーバーなどの NTP タイムサーバーを指すように設定します。サーバータイムを設定するには、Cisco SD-WAN Manager NTP 機能設定テンプレートで、NTP サーバーのホスト名を入力します。次に、Cisco SD-WAN Manager を使用して設定テンプレートを NTP 機能に再アタッチします。Google NTP サーバーは、time.google.com、time2.google.com、time3.google.com、time4.google.com などです。

## Cisco SD-WAN Manager での Cisco Catalyst SD-WAN クラウドデバイスの有無の確認

### 手順

---

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Devices]** の順に選択します。

ステップ 2 [Device listing] ページで、まだ使用されていない有効な Cisco CSR1000V または Cisco Catalyst 8000V デバイスが少なくとも 2 つあることを確認します。

以下が、有効な未使用のデバイスです。

- [Validity] 列に "valid" という単語があるデバイス。
- [Assigned Template]、[Device Status]、[Hostname]、[System IP]、および [Site ID] 列が空白のデバイス。

Cisco CSR1000V または Cisco Catalyst 8000V デバイスが不足している場合は、[software.cisco.com](https://software.cisco.com) にアクセスし、Plug and Play Connect ポータルを使用してトークンまたはライセンスを追加します。

---

# Cisco Catalyst SD-WAN クラウドデバイスのデバイステンプレートの設定

Cisco SD-WAN Manager 内で 2 つの Cisco CSR1000V または Cisco Catalyst 8000V デバイスに少なくとも最小限のデバイステンプレートが割り当てられていることを確認します。最小限のデバイステンプレートは、デバイステンプレート内の工場出荷時のデフォルトの機能テンプレートを使用するテンプレートです。デバイステンプレート内で、少なくとも 1 つのサービス VPN と管理 (VPN 512) インターフェイスが設定されている必要があります。ただし、カスタム機能テンプレート内の展開に固有の設定を含む、完全に機能するデバイステンプレートを設定することを推奨します。Cisco SD-WAN Manager を使用して個々の機能テンプレートとデバイステンプレートを作成する手順については、「[Configure the Cisco SD-WAN Routers](#)」を参照してください。

これらのテンプレートをデバイステンプレートにアタッチし、Cloud onRamp for IaaS を使用して設定した後は、機能テンプレートを変更しないでください。Cloud onRamp for IaaS の設定は、変更されたこれらの機能テンプレートの設定を上書きします。

「[機能テンプレートの設定例](#)」トピック内に、デバイステンプレートの例と、デバイステンプレートを構成するさまざまな機能テンプレートがあり、Cisco CSR1000V または Cisco Catalyst 8000V デバイスに使用できます。

## Cisco Catalyst SD-WAN クラウドデバイスへのデバイステンプレートのアタッチ

デバイステンプレートを Cisco CSR1000V または Cisco Catalyst 8000V デバイスにアタッチすると、Cisco SD-WAN Manager が機能テンプレートに基づいて設定を作成してから、指定された Cisco CSR1000V または Cisco Catalyst 8000V デバイスに設定を保存します。設定を作成して保存する前に、デバイステンプレートにアタッチされている機能テンプレート内のすべての変数を定義します。

.csv ファイルをアップロードする代わりに、Cisco SD-WAN Manager を使用して変数の値を手動で入力するには、次の手順を実行します。

### 手順

- ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration] > [Templates] > [Device Templates]** を選択します。  
(注) Cisco vManage リリース 20.7.1 以前のリリースでは、**[Device Templates]** のタイトルは **[Device]** です。
- ステップ 2** 目的のデバイステンプレートについて、**[...]** をクリックし、**[Attach Devices]** を選択します。  
この設定にアタッチできる使用可能なデバイスが一覧表示されるポップアップウィンドウが表示されません。使用可能なデバイスのリストには、次のいずれかが含まれています。

- デバイスのホスト名と IP アドレス（Cisco SD-WAN Manager を使用していて既知の場合）。
- デバイスのシャーシのシリアル番号（ネットワーク上で使用できず、Cisco SD-WAN Manager に認識されていない場合）。

Cisco CSR1000V または Cisco Catalyst 8000V デバイスには物理シャーシはありませんが、シャーシのシリアル番号が割り当てられます。このリストには、デバイステンプレートの作成時に定義されたデバイスモデルのみが含まれています。

**ステップ 3** 設定テンプレートを適用するには、1つ以上のデバイスを [Available Devices] から選択し、[Selected Devices] に移動します。

(注) このドキュメントでは、2つの Cisco Catalyst SD-WAN クラウドデバイスを使用して、設定を適用します。

**ステップ 4** [Attach] をクリックします。

表示されたウィンドウに、選択した Cisco Catalyst SD-WAN クラウドデバイスが一覧表示されます。

**ステップ 5** 最初の Cisco CSR1000V または Cisco Catalyst 8000V デバイスに対して、[...] をクリックし、[Edit Device Template] を選択します。

ポップアップウィンドウが表示され、変数のリストと空のテキストボックスが表示されます。チェックボックスを使用してオンとオフの値を示す変数もあります。すべてのテキストボックスに入力してください。[デバイステンプレート変数値の例 \(43 ページ\)](#) のトピックにあるサンプル情報を使用して、変数値を入力することができます。

**ステップ 6** [Update] をクリックします。

**ステップ 7** 2 番目の Cisco CSR1000V または Cisco Catalyst 8000V デバイスに対してステップ 5 ~ 6 を繰り返します。将来使用するために、変数値を .csv ファイルにダウンロードすることができます。

**ステップ 8** [Next] をクリックします。

ウィンドウに、1つのデバイステンプレートにアタッチされている2つのデバイスに設定アクションが適用されていることが示されます。

左側のペインからデバイスを選択して、Cisco Catalyst SD-WAN クラウドデバイスに保存されている設定を表示することができます。

**ステップ 9** [Configure Devices] をクリックします。

**ステップ 10** 表示されたポップアップウィンドウで、[Confirm configuration changes on 2 devices] をオンにします。

**ステップ 11** [OK] をクリックします。

[Task View] ウィンドウが表示されます。

しばらくすると、2つの Cisco CSR1000V または Cisco Catalyst 8000V デバイスのステータスが [Done - Scheduled] になり、デバイスがオフラインであり、オンラインになるとテンプレートがデバイスにアタッチされることを示すメッセージが表示されます。

## 次のタスク

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS を使用して、AWS トランジット VPC または Azure トランジット VNet 内に 2 つの Cisco CSR1000V または Cisco Catalyst 8000V デバイスを展開できるようにしました。

# AWS の前提条件

## 手順

**ステップ 1** 有効な AWS アカウントを用意します。

**ステップ 2** GovCloud にアクセスするための有効な AWS Government アカウントを用意します。

**ステップ 3** AWS Marketplace 内で、使用しているアカウントで Cisco CSR1000V、Cisco Catalyst 8000V デバイスの Amazon マシンイメージ (AMI) に登録します。AWS Marketplace 内で、使用しているアカウントで Amazon マシンイメージ (AMI) に登録するには、次の手順を実行します。

a) [Amazon Web Services Marketplace](#) にログインします。

b) AWS Marketplace で「Cisco CSR1000V または Cisco Catalyst 8000V デバイス」を検索します。

AMI のリストが表示されます。

c) リストから、展開する予定の Cisco CSR1000V または Cisco Catalyst 8000V デバイスのリンクをクリックします。

サブスクリプション画面が表示され、Cisco CSR1000V または Cisco Catalyst 8000V デバイスの AMI に登録できます。

d) [引き続きサブスクライブする (Continue to Subscribe)] をクリックして登録します。

e) [条件に同意する (Accept Terms)] をクリックします。

しばらくすると、Cisco CSR1000V または Cisco Catalyst 8000V デバイスの AMI を使用するために登録されたことを示すメッセージが表示されます。

(注) Cisco Catalyst SD-WAN Cloud OnRamp for IaaS はトランジット VPC の作成時に Cisco Catalyst SD-WAN クラウドデバイスを自動的に設定するため、[Continue to Configuration] はクリックしないでください。

f) AWS Marketplace からログアウトします。

# AWS での Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定

## 考慮すべき点

- トランジット VPC は、シスコのオーバーレイネットワークとホスト VPC で実行されているクラウドベースのアプリケーション間の接続を提供します。ブランチからホスト VPC へのトラフィックのトランジットポイントとして機能する専用の各 VPC 内で、冗長 Cisco Catalyst SD-WAN クラウドデバイスのペアを最大 4 つまでプロビジョニングできます。各冗長ペアの個々の Cisco Catalyst SD-WAN デバイスは、トランジット VPC の AWS リージョン内の異なる可用性ゾーン内に展開されます。複数の Cisco Catalyst SD-WAN デバイスは、オーバーレイネットワークとクラウドベースのアプリケーション間の接続に冗長性を提供します。これら 2 つの Cisco Catalyst SD-WAN クラウドデバイスのそれぞれで、トランスポート VPN (VPN 0) はブランチルータに接続し、サービス側 VPN (VPN 0 と VPN 512 を除く VPN) はパブリッククラウド内のアプリケーションおよびアプリケーションプロバイダーに接続します。
- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS ワークフローは、2 番目の WAN インターフェイスのパブリック IP アドレスを使用して、ホスト VPC をトランジット VPC にマッピングするためのカスタマーゲートウェイ (ipsec トンネル) を設定します。WAN インターフェイスのパブリック IP アドレスを追加するには、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS で使用されるデバイスの VPN インターフェイスイーサネットテンプレートを GigabitEthernet2 インターフェイスを使用して設定します。Cisco CSR1000V および Cisco Catalyst 8000V デバイスでは、トンネルインターフェイスは GigabitEthernet2 インターフェイス上にあります。[VPN0 インターフェイス機能テンプレート \(40 ページ\)](#) の VPN インターフェイスイーサネットテンプレートの設定例を参照してください。
- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS は AWS の自動スケールをサポートしています。AWS の自動スケール機能を使用するには、Cisco Catalyst SD-WAN クラウドデバイスの 1 ~ 4 つのペアをトランジット VPC に関連付けていることを確認します。
- ホスト VPC は、クラウドベースのアプリケーションが存在する仮想プライベートクラウドです。トランジット VPC がアプリケーションまたはアプリケーションプロバイダーに接続する場合は、ホスト VPC に接続するだけです。
- すべてのホスト VPC が同じ AWS アカウントに属することも、各ホスト VPC が異なるアカウントに属することもできます。ある AWS アカウントに属するホストを、別のアカウントに属するトランジット VPC にマッピングすることができます。Cloud OnRamp 構成ウィザードを使用して、クラウドインスタンスまたはクラウドアカウントを設定します。

## 手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for IaaS]** を選択します。

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS を初めて設定する場合、クラウドインスタンスは画面に表示されません。クラウドインスタンスは、AWS リージョン内で作成された 1 つ以上のトランジット VPC を持つ AWS アカウントに対応しています。

**ステップ 2** [Add New Cloud Instance] をクリックします。

**ステップ 3** [Amazon Web Services (AWS)] オプションボタンをクリックします。

**ステップ 4** 次のポップアップウィンドウで、次の手順を実行します。

- a) クラウドサーバーにログインするために、[IAM Role] または [Key] をクリックします。[IAM Role] を使用することを推奨します。
- b) [IAM Role] をクリックした場合は、Cisco SD-WAN Manager が提供する [External ID] を使用して IAM ロールを作成します。ウィンドウに表示された外部 ID をメモして、IAM ロールの作成時に使用できる [Role ARN] 値を指定します。

Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降では、IAM ロールを作成するには、AWS 管理コンソールを使用して Cisco SD-WAN Manager から提供された外部 ID をポリシーに入力する必要があります。次の手順を実行します。

1. 既存の Cisco SD-WAN Manager EC2 インスタンスに IAM ロールをアタッチします。

1. ポリシーを作成するには、[AWS ドキュメント](#)の IAM ロールの作成（コンソール）のトピックを参照してください。AWS の [Create policy] ウィザードで、[JSON] をクリックし、次の JSON ポリシードキュメントを入力します。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "*"
  }]
}
```

2. IAM ロールを作成し、ステップ 1 で作成したポリシーに基づいて Cisco SD-WAN Manager EC2 インスタンスにアタッチする方法については、[AWS Security Blog](#) の「Easily Replace or Attach an IAM Role to an Existing EC2 Instance by Using the EC2 Console」ブログを参照してください。

(注) [Attach permissions policy] ウィンドウで、ステップ 1 で作成した AWS 管理ポリシーを選択します。

2. Cisco Catalyst SD-WAN Cloud OnRamp for IaaS に使用する AWS アカウントで IAM ロールを作成します。

1. [AWS ドキュメント](#)の IAM ロールの作成（コンソール）のトピックを参照して、[Require external ID]をオンにし、ステップ4 (b) でメモした外部IDを貼り付けて、IAM ロールを作成します。
2. ロールを担当できるユーザーを変更するには、[AWS ドキュメント](#) のロール信頼ポリシーの変更（コンソール）のトピックを参照してください。

[IAM Roles] ウィンドウで、下にスクロールして、前の手順で作成したロールをクリックします。

[Summary] ウィンドウで、[Role ARN] をメモします。

(注) ステップ 4 (b) で IAM ロールを選択した場合は、このロール ARN 値を入力できます。

3. 信頼関係を変更したら、[JSON] をクリックし、次の JSON ドキュメントを入力します。変更内容を保存します。

(注) 次の JSON ドキュメントのアカウント ID は、Cisco SD-WAN Manager EC2 インスタンスです。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::[Account ID from Part 1]:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "[vManage provided External ID]"
        }
      }
    }
  ]
}
```

c) [Key] オプションボタンをクリックした場合は、次の手順を実行します。

1. [API Key] フィールドに、Amazon API キーを入力します。
2. [Secret Key] フィールドに、API キーに関連付けられたパスワードを入力します。
3. [Environment] ドロップダウンリストから、[commercial] または [govcloud] を選択します。

デフォルトでは、[commercial] 環境が選択されています。環境の仕様に基づいて地理的なリージョンを選択できます。

**ステップ 5** [Login] をクリックして、クラウドサーバーにログインします。

クラウドインスタンス構成ウィザードが表示されます。このウィザードは、リージョンの選択、トランジット VPC の追加、ホスト VPC の検出、およびトランジット VPC へのホスト VPC のマッピングに使用する、3つの画面で構成されています。各ウィザード画面のグラフィックは、クラウドインスタンスの設定プロセスの手順を示しています。まだ完了していない手順は、明るいグレーで表示されます。現在の手順は、

青いボックス内に強調表示されます。完了した手順は緑色のチェックマークで示され、明るいオレンジで表示されます。

#### ステップ6 リージョンを選択します。

[Choose Region] ドロップダウンリストから、トランジット VPC を作成するリージョンを選択します。

#### ステップ7 トランジット VPC を追加します。

a) [Transit VPC Name] フィールドに、トランジット VPC 名を入力します。

名前には、128 文字の英数字、ハイフン (-)、および下線 (\_) を含めることができます。スペースやその他の文字を含めることはできません。

b) [Device Information] で、トランジット VPC に関する情報を入力します。

1. [WAN Edge Version] ドロップダウンリストで、トランジット VPC で実行する Cisco Catalyst SD-WAN クラウドデバイスのソフトウェアバージョンを選択します。

2. [Size of Transit WAN Edge] ドロップダウンリストで、トランジット VPC で実行される各 Cisco Catalyst SD-WAN クラウドデバイスに使用できるメモリと CPU を決定するオプションを選択します。

- 『Cisco CSR 1000v Series Cloud Services Router Deployment Guide for Amazon Web Services』の Cisco CSR1000V デバイスの「[Supported Instance Types](#)」のトピックを参照してください。

- 「Deploying Cisco Catalyst 8000V on Amazon Web Services」の Cisco Catalyst 8000V の「[Supported Instance Types](#)」のトピックを参照してください。

(注) 次のサイズを選択することを推奨します。

Cisco CSR1000V および Cisco Catalyst 8000V には、4 つ以上の vCPU を持つ c5 インスタンスタイプを選択します ([c5.xlarge (4 vCPU)] など)。

3. [Max. Host VPCs per Device Pair] フィールドで、トランジット VPC の各デバイスペアにマッピングできるホスト VPC の最大数を選択します。有効な値は 1 ~ 32 です。

4. ダイレクトインターネットアクセス (DIA) 用にトランジット VPC デバイスを設定するには、次のいずれかをクリックします。

- [Disabled] : インターネットアクセスなし。

- [Enabled via Transport] : デバイスの WAN インターフェイスに対して NAT を設定または有効化します。

- [Enabled via Umbrella SIG] : デバイスでセキュアな DIA を有効にするように Cisco Umbrella を設定します。

5. [Device Pair 1#] フィールドで、ペアの各デバイスのシリアル番号を選択します。デバイスのシリアル番号を削除するには、フィールドに表示される [X] をクリックします。

表示されるデバイスのシリアル番号は設定テンプレートに関連付けられていて、ステップ1で選択した Cisco Catalyst SD-WAN WAN エッジバージョンをサポートしています。

6. デバイスペアをさらに追加するには、 をクリックします。  
デバイスペアを削除するには、 をクリックします。  
トランジット VPC は、1～4つのデバイスペアに関連付けることができます。AWS で自動スケール機能を有効にするには、少なくとも2つのデバイスペアをトランジット VPC に関連付けます。
7. より具体的な設定オプションを入力する場合は、[Advanced] をクリックします。
  1. [Transit VPC CIDR] フィールドに、16～25の範囲のネットワークマスクを持つカスタム CIDR を入力します。このフィールドを空のままにすると、トランジット VPC はデフォルト CIDR の 10.0.0.0/16 を使用して作成されます。CIDR ブロック内に6つのサブネットを作成するために十分なアドレス空間が必要です。
  2. (オプション) [SSH PEM Key] ドロップダウンリストで、インスタンスにログインするための PEM キーペアを選択します。このキーペアはリージョン固有です。キーペアの作成手順については、[AWS のドキュメント](#)を参照してください。
8. [Save and Finish] をクリックしてトランジット VPC の設定を完了するか、必要に応じて [Proceed to Discovery and Mapping] をクリックしてウィザードを続行します。  
このクラウドインスタンスでは、2つの Cisco Catalyst SD-WAN クラウドデバイスがある単一のトランジット VPC が作成されています。単一のクラウドインスタンス（リージョン内の AWS アカウント）内に複数のトランジット VPC を設定できます。クラウドインスタンス内に複数のトランジット VPC が存在する場合は、ホスト VPC をいずれかのトランジット VPC にマッピングすることができます。
9. ホスト VPC を検出します。
  1. [Select an account to discover] フィールドで、ホスト VPC を検出する AWS アカウントを選択します。  
または、ホスト VPC を検出する新しい AWS アカウントを追加するには、[New Account] をクリックします。
  2. [Discover Host VPCs] をクリックします。  
トランジット VPC にマッピングできる VPC を示すテーブルが表示されます。選択した AWS アカウント内の、トランジット VPC と同じ AWS リージョン内のホスト VPC のみが表示されます。
  3. 表示されたテーブルで、トランジット VPC にマッピングする1つ以上のホストのチェックボックスをオンにします。  
検索結果をフィルタリングするには、検索バーの [Filter] オプションを使用して、特定の検索条件に一致するホスト VPC のみを表示します。  
[Refresh] アイコンをクリックすると、テーブルが最新の情報で更新されます。  
テーブルに表示される列を指定するには、[Show Table Columns] アイコンをクリックします。

10. ホスト VPC をトランジット VPC にマッピングします。
  1. すべてのホスト VPC のテーブルで、目的のホスト VPC を選択します。
  2. [Map VPCs] をクリックします。[Map Host VPCs] ポップアップが開きます。
  3. [Transit VPC] ドロップダウンリストで、ホスト VPC にマッピングするトランジット VPC を選択します。
  4. [VPN] ドロップダウンリストで、マッピングを配置するオーバーレイネットワーク内のサービス VPN を選択します。
  5. Cisco SD-WAN Manager がホスト VPC ルートテーブルにルートを自動的に伝達する場合は、[Route Propagation] オプションを有効にします。  
デフォルトでは、[Route Propagation] は無効になっています。
  6. [Map VPCs] をクリックします。

数分後に [Task View] 画面が表示されるので、ホスト VPC がトランジット VPC にマッピングされたことを確認します。

(注) トランジット VPC を形成する 2 つの Cisco Catalyst SD-WAN クラウドデバイスの VPN 0 の VPN 機能テンプレートを設定する場合は、トンネルインターフェイスに割り当てる色がプライベートの色ではなくパブリックの色であることを確認します。パブリックの色は次のとおりです。

- 3g
- biz-internet
- blue
- bronze
- custom1
- custom2
- custom3
- default
- gold
- green
- lte
- metro-ethernet
- mpls
- public-internet
- red
- silver

---

## ホストおよびトランジット VPC の管理

### ホスト VPC の表示

#### 手順

**ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration] > [Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

デフォルトでは、[Mapped Host VPCs] フィールドが選択され、マッピングされたホスト VPC の下のテーブルには、マッピングされたホストとトランジット VPC、トランジット VPC の状態、および VPN ID が一覧表示されます。

- ステップ 2** マッピングされていないホスト VPC を一覧表示するには、[Un-Mapped Host VPCs] をクリックします。次に、[Discover Host VPCs] をクリックします。
- ステップ 3** トランジット VPC を表示するには、[Transit VPCs] をクリックします。

---

## トランジット VPC へのホスト VPC のマッピング

### 手順

- 
- ステップ 1** Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud onRamp for IaaS] を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。
- ステップ 2** [Un-Mapped Host VPCs] をクリックします。
- ステップ 3** [Select an account to discover] フィールドで、ホスト VPC を検出する AWS アカウントを選択します。
- ステップ 4** [Discover Host VPCs] をクリックします。
- ステップ 5** 検出されたホスト VPC のリストから、目的のホスト VPC を選択します。
- ステップ 6** [Map VPCs] をクリックします。[Map Host VPCs] ポップアップが開きます。
- ステップ 7** [Transit VPC] ドロップダウンリストから、目的のトランジット VPC を選択します。
- ステップ 8** [VPN] ドロップダウンリストで、マッピングを配置するオーバーレイネットワーク内の VPN を選択します。
- ステップ 9** [Map VPCs] をクリックします。

---

## ホスト VPC のマッピング解除

### 手順

- 
- ステップ 1** Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud onRamp for IaaS] を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。
- ステップ 2** [Mapped Host VPCs] をクリックします。
- ステップ 3** VPC のリストから、マッピングを解除するホスト VPC を選択します。
- ステップ 4** [Un-Map VPCs] をクリックします。
- ステップ 5** [OK] をクリックして、マッピングの解除を確定します。

---

ホスト VPC のマッピングを解除すると、ホスト VPC 内の VPN ゲートウェイへのすべての VPN 接続が削除されてから、VPN ゲートウェイが削除されます。マッピングされたホスト VPC へ

の VPN 接続を追加している場合、その接続はマッピング解除プロセスの一環として終了されます。

## トランジット VPC の表示

### 手順

**ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration] > [Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

**ステップ 2** [Transit VPCs] をクリックします。

## トランジット VPC の追加

### 手順

**ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration] > [Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

**ステップ 2** [Transit VPCs] をクリックします。

**ステップ 3** [Add Transit VPC] をクリックします。

トランジット VPC を追加するには、[AWS での Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定 \(10 ページ\)](#) のステップ 7 の手順に従います。

## デバイスペアの削除



(注) オンラインデバイスペアの最後のペアを削除するには、トランジット VPC を削除してください。

### 始める前に

削除するデバイスペアはオフラインである必要があります。

## 手順

- 
- ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration] > [Cloud onRamp for IaaS]** を選択します。
  - ステップ 2** デバイスペア ID をクリックします。
  - ステップ 3** デバイスペアのステータスがオフラインであることを確認します。
  - ステップ 4** デバイスペアのスケールを解除するには、**[Action]**列の下にあるごみ箱アイコンをクリックするか、**[Trigger Autoscale]** をクリックします。
- 

## トランジット VPC の削除



- 
- (注) オンラインデバイスペアの最後のペアを削除するには、トランジット VPC を削除する必要があります。
- 

### 始める前に

トランジット VPC に関連付けられているデバイスペアを削除します。

## 手順

- 
- ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration] > [Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。**[Host VPCs/Transit VPCs]** ウィンドウが開きます。
  - ステップ 2** **[Host VPCs]** をクリックします。
  - ステップ 3** すべてのホスト VPC を選択し、**[Un-Map VPCs]** をクリックします。  
トランジット VPC にマッピングされていたすべてのホスト VPC のマッピングが解除されたことを確認します。
  - ステップ 4** **[OK]** をクリックして、マッピングの解除を確定します。
  - ステップ 5** **[Transit VPCs]** をクリックします。
  - ステップ 6** 削除するトランジット VPC のごみ箱アイコンをクリックします。  
(注) トランジット VPC の最後のデバイスペアでは、ごみ箱アイコンは使用できません。そのため、最後のデバイスペアを削除するには、**[Delete Transit]** ドロップダウンリスト項目をクリックします。ごみ箱アイコンは、2 番目以降のデバイスペアでのみ使用できます。
  - ステップ 7** **[OK]** をクリックして確定します。
-

## デバイスペアの追加

### 手順

**ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

**ステップ 2** [Transit VPCs] をクリックします。

トランジット VPC のリストを含むテーブルが表示されます。

**ステップ 3** 目的のトランジット VPC について、[...] をクリックし、[Add Device Pair] を選択します。

**ステップ 4** [Add Device Pairs] ダイアログボックスで、[Add] をクリックしてデバイスペアを追加します。

(注) 追加するデバイスがすでにデバイステンプレートに関連付けられていることを確認します。

トランジット VPC には最大で合計 4 つのデバイスペアを追加できます。

**ステップ 5** [Save] をクリックします。

## トランジット VPC のデバイスペアの履歴

### 手順

**ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

**ステップ 2** [Transit VPCs] をクリックします。

トランジット VPC のリストを含むテーブルが表示されます。

**ステップ 3** 目的のトランジット VPC について、[...] をクリックし、[History for a device pair] を選択します。

これにより、対応するすべてのイベントが含まれている [Transit VPC Connection History] ページが表示されます。

**ステップ 4** 過去 1 時間に発生したイベントのヒストグラムと、選択したトランジット VPC のすべてのイベントのテーブルが表示されます。このテーブルには、トランジット VPC で生成されたすべてのイベントが一覧表示されます。イベントは次のいずれかです。

- Device Pair Added
- Device Pair Spun Up
- Device Pair Spun Down
- Device Pair Removed

- Host Vpc Mapped
- Host Vpc Unmapped
- Host Vpc Moved
- Transit Vpc Created
- Transit Vpc Removed

---

## 中継 VPC の編集

### 手順

---

**ステップ 1** Cisco SD-WAN Manager のメニューから、[**Configuration**] > [**Cloud onRamp for IaaS**] を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

**ステップ 2** [Transit VPCs] をクリックします。

トランジット VPC のリストを含むテーブルが表示されます。

**ステップ 3** 目的のトランジット VPC について、[...] をクリックして選択し、[Edit Transit Details] をクリックします。

**ステップ 4** DIA 情報を入力するには、[AWS での Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定 \(10 ページ\)](#) のステップ 7 (iv) の手順に従います。

この操作により、必要に応じて自動スケールがトリガーされる場合があります。

---

## Microsoft Azure の前提条件

1. 有効な Microsoft Azure アカウントを用意します。
2. GovCloud にアクセスするための有効な Azure Government アカウントを用意します。



---

(注) Azure Government クラウドのサポートは Cisco Catalyst 8000V でのみ利用できます。

---

3. [Azure Marketplace](#) で、Cisco CSR1000V または Cisco Catalyst 8000V デバイスの利用規約に同意します。

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS ワークフローの一部として Cisco Catalyst SD-WAN クラウドルータを使用するには、仮想マシン (VM) の使用に関するマーケットプレースの条件に同意する必要があります。次のいずれかの方法で Azure の利用規約に同意できます。

- ポータルでクラウドデバイスを手動で起動し、オンボーディングウィザードの最終ページの一部の条件に同意します。
- Azure API または Powershell/Cloud Shell スクリプトで、[Set-AzureRmMarketplaceTerms](#) コマンドを使用します。

4. Microsoft Azure でアプリケーション登録を作成し、Azure アカウントのログイン情報を取得します。Cisco Catalyst SD-WAN Cloud OnRamp for IaaS で、これらのログイン情報が、Azure で Cisco SD-WAN Manager サーバーを認証し、VNet および仮想マシンインスタンスを起動するために使用されます。

Azure ログイン情報を作成および取得するには、所有者権限を使用して Azure でアプリケーション登録を作成します。

1. [Microsoft Azure ポータル](#)を開きます。
2. Azure Active Directory (AD) の権限を確認します。[Azure Active Directory] を選択し、ロールをメモします。Azure AD テナントにアプリケーションを登録できるのは、管理者権限を持つロールのみです。
3. サブスクリプションの権限を確認します。

Azure AD に関連付けられているロールと権限を確認したら、Azure サブスクリプションアカウントに、Azure AD アプリケーションにロールを割り当てるための [Microsoft.Authorization/\*/\*Write] のアクセス権があることを確認します。このアクセス権は、所有者ロールまたはユーザーアクセス管理者ロールにのみ関連付けられます。

1. Azure ポータルで、[Subscriptions] をクリックします。
2. [Subscriptions] サービスに移動し、行の右側にある [More Actions] アイコンをクリックします。  
[Microsoft Azure Enterprise] ページが表示されます。
3. [My permissions] を選択します。次に、[Click here to view complete access details for this subscription] をクリックします。
4. [View my access] をクリックして、割り当てられたロールを表示します。
5. AD アプリケーションにロールを割り当てるための適切な権限があるかどうかを確認します。ない場合は、[User Access Administrator] ロールを自分に追加するように、Azure サブスクリプション管理者に依頼します。

4. アプリケーション ID とサービスプリンシパルを作成します。
  1. Azure ポータルの左側のペインで、[Azure Active Directory] をクリックします。
  2. サブメニューから、[App registrations] をクリックします。
  3. [新規登録 (New Registration)] をクリックします。[Register an application] 画面が表示されます。
  4. [Name] フィールドに、CloudOnRampApp などのわかりやすい名前を入力します。

5. [Supported account types] で、[Accounts in this organizational directory only (Microsoft only - Single tenant)] を選択します。
6. [Redirect URI] で、作成するアプリケーションのタイプとして [Web] を選択します。
7. 値を設定したら、[Register] をクリックします。

これで、Azure AD アプリケーションとサービスプリンシパルが作成されました。

5. Cloud OnRamp アプリケーションの秘密キーを作成します。
  1. Azure AD の [App registrations] で、使用するアプリケーションをクリックします。
  2. 左側のペインで、[Certificates & secrets] をクリックします。
  3. [Client secrets] の下で、[New client secret] をクリックします。
  4. 秘密キーの説明と、秘密キーの有効期限を入力します。
  5. [Add] をクリックします。

クライアントシークレットを保存すると、クライアントシークレットの値またはキーの値が表示されます。必要に応じて後でキーを取得することはできないため、この値をメモしてください。作成したアプリケーションにサインインするには、アプリケーション ID とともにキー値を指定する必要があります。

6. サブスクリプション ID を取得します。
  1. Azure ポータルで、[Subscriptions] をクリックします。
  2. [Subscriptions] サービスに移動し、行の右側にある [More Actions] アイコンをクリックします。  
[Microsoft Azure Enterprise] ページが表示されます。
  3. このページの [Subscription ID] をメモします。

Cisco SD-WAN Manager に Azure サブスクリプションへのプログラムによるアクセスを提供するには、サブスクリプション ID が必要です。

複数のサブスクリプションがある場合は、CloudOnRampApp の設定に使用する予定のサブスクリプション ID をコピーして保存します。

7. テナント ID を表示します。
  1. Azure ポータルの左側のペインで、[Azure Active Directory] をクリックします。
  2. 左側のペインで、[Properties] をクリックします。テナント ID に相当するディレクトリ ID が表示されます。
8. アプリケーションに所有者ロールを割り当てます。

このガイドでは、すべてのアクセスと管理が可能な所有者ロールを割り当てる手順を説明しました。



- (注) アプリケーションの適切なロールについては、Azure 管理者にお問い合わせください。
1. Azure ポータルの左側のペインで、[Subscriptions] をクリックします。
  2. サブスクリプションをクリックして、Cloud OnRamp アプリケーションに割り当てます。
  3. サブスクリプションペインで、[Access Control (IAM)] に移動します。
  4. [Add a role assignment] をクリックします。[Add role assignment] ポップアップが表示されます。
  5. [Role] ドロップダウンリストから、[Owner] を選択します。
  6. [Assign Access To] ドロップダウンリストで、デフォルト値の [Azure AD user, group, or service principal] を選択します。
  7. [Select] ドロップダウンリストから、ステップ d で作成した Cloud OnRamp アプリケーションを選択します。
  8. [Save] をクリックします。

その範囲のロールを持つユーザーのリストに、使用するアプリケーションが表示されます。

これで、作成して保存した Azure ログイン情報を使用して Cloud OnRamp アプリケーションにログインすることができます。

5. Azure ポータルで使用するサブスクリプションに移動して、アカウントに関連付けられている Azure の制限を確認します。[Settings] の下で、[Usage + Quotas] を選択します。
  1. [All Providers] ドロップダウンリストからプロバイダーを選択します。
  2. [Microsoft.Network] を確認します。

このサブスクリプションで使用可能な可用性セットの量を表示できます。アカウントで次のリソースを作成できるように、可用性セットが十分であることを確認します。

- トランジット VNet の作成に必要な 1 つの VNet。
- トランジット VNet での仮想マシンの配布に必要な 1 つの可用性セット。
- トランジットクラウドルーターに関連付けられた 6 つのスタティックパブリック IP アドレス。
- ホスト VNet ごとに 1 つの Azure Virtual Network トランジットと 2 つのスタティックパブリック IP アドレス
- 各ホスト VNet をマッピングするための 4 つの VPN 接続



(注) F シリーズの Azure VM (F4 および F8) が、Cisco Catalyst SD-WAN クラウドデバイスでサポートされています。

## Microsoft Azure の Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定

設定プロセスでは、1つ以上のホスト VNet を単一のトランジット VNet にマッピングします。マッピング時に、ブランチユーザーがアクセスできるクラウドベースのアプリケーションを設定します。

マッピングプロセスにより、トランジット VNet と各ホスト VNet の間に IPsec および BGP 接続が確立されます。トランジット VNet とホスト VNet を接続する IPsec トンネルは、接続のセキュリティを提供するために IKE を実行します。Azure の場合、IPsec トンネルは IKE バージョン 2 を使用します。セキュアな IPsec トンネルを介して確立された BGP 接続により、トランジット VNet とホスト VNet はルートを交換できます。その後、BGP 接続または BGP ルートが Cisco Catalyst SD-WAN クラウドデバイス内の OMP に再配布され、これによりドメイン内の Cisco SD-WAN コントローラに OMP ルートがアドバタイズされます。トランジット VNet は、その後、ブランチから適切なホスト VNet および適切なクラウドベースのアプリケーションにトラフィックを転送できます。

マッピングプロセス中に、IPsec トンネルと BGP ピアリングセッションが自動的に設定および確立されます。マッピングを確立した後は、VPN インターフェイスの IPsec および BGP 機能設定テンプレートで IPsec および BGP 設定を表示し、必要に応じて変更することができます。

### 考慮すべき点 :

Azure で Cisco Catalyst SD-WAN Cloud OnRamp for IaaS を設定するには、それぞれがルータのペアで構成される Azure トランジット VNet を作成します。次に、Azure クラウドに存在するトランジット VNet にホスト VNet をマッピングします。すべての VNet は同じリソースグループ内に存在します。

- トランジット VNet は、オーバーレイネットワークとホスト VNet で実行されているクラウドベースのアプリケーション間の接続を提供します。各トランジット VNet は、独自の VNet に存在する 2 つのクラウドデバイスで構成されます。2 つのクラウドデバイスは、オーバーレイネットワークとクラウドベースのアプリケーション間の接続に冗長性を提供します。これら 2 つのクラウドデバイスのそれぞれで、トランスポート VPN (VPN 0) はシミュレートされたブランチデバイスに接続し、サービス側 VPN (VPN 0 と VPN 512 を除く VPN) はパブリッククラウド内のアプリケーションおよびアプリケーションプロバイダーに接続します。
- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS ワークフローは、2 番目の WAN インターフェイスのパブリック IP アドレスを使用して、ホスト VNet をトランジット VNet にマッピングするためのカスタマーゲートウェイ (ipsec トンネル) を設定します。WAN イン

ターフェイスのパブリック IP アドレスを追加するには、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS で使用されるデバイスの VPN インターフェイスイーサネットテンプレートを GigabitEthernet2 インターフェイスを使用して設定します。Cisco CSR1000V および Cisco Catalyst 8000V では、トンネルインターフェイスは GigabitEthernet2 インターフェイス上にあります。[VPN0 インターフェイス機能テンプレート \(40 ページ\)](#) の VPN インターフェイスイーサネットテンプレートの設定例を参照してください。

- ホスト VNet は、クラウドベースのアプリケーションが存在する仮想プライベートクラウドです。トランジット VNet がアプリケーションまたはアプリケーションプロバイダーに接続する場合は、ホスト VNet に接続するだけです。

## 手順

**ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for IaaS]** を選択します。

**ステップ 2** **[Add New Cloud Instance]** をクリックします

**ステップ 3** **[Microsoft Azure]** オプションボタンをクリックします。

**ステップ 4** 次のポップアップ画面で、次の手順を実行します。

- [Subscription ID]** フィールドに、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS ワークフローの一環として使用する Microsoft Azure サブスクリプションの ID を入力します。
- [Client ID]** フィールドに既存のアプリケーションの ID を入力するか、新しいアプリケーションを作成します。アプリケーションを作成するには、**[Azure Active Directory]** > **[App Registrations]** > **[New registration]** に移動します。アプリケーションの作成の詳細については、Microsoft Azure のドキュメントを参照してください。
- [Tenant ID]** フィールドに、アカウントの ID を入力します。テナント ID を見つけるには、Microsoft Azure Active Directory に移動し、**[Properties]** をクリックします。
- [Secret Key]** フィールドに、クライアント ID に関連付けられたパスワードを入力します。
- [Environment]** フィールドで、**[commercial]** または **[GovCloud]** を選択します。

デフォルトでは、**[commercial]** 環境が選択されています。環境の仕様に基づいて地理的な場所を選択できます。

- [ログイン (Login)]** をクリックします。

クラウドインスタンス構成ウィザードが開きます。

このウィザードは、場所の選択、トランジット VNet の追加、ホスト VNet の検出、およびトランジット VNet へのホスト VNet のマッピングに使用する、3 つの画面で構成されています。各ウィザード画面の右側のグラフィックは、クラウドインスタンスの設定プロセスの手順を示しています。まだ完了していない手順は、明るいグレーで表示されます。現在の手順は、青いボックス内に強調表示されます。完了したすべての手順は緑色のチェックマークで示され、明るいオレンジで表示されます。

**ステップ 5** **[Choose Location]** ドロップダウンリストから、トランジット VNet を作成する場所を選択します。

使用可能な場所は、商用クラウドか GovCloud かの選択に基づいています。

**ステップ 6** トランジット VNet を追加します。

- a) [Transit VNet Name] フィールドに、トランジット VNet の名前を入力します。
- 名前には、32 文字の英数字、ハイフン (-)、および下線 (\_) を含めることができます。スペースやその他の文字を含めることはできません。
- b) [Device Information] で、トランジット VNet に関する情報を入力します。
- [WAN Edge Version] ドロップダウンリストで、トランジット VNet で実行するソフトウェアバージョンを選択します。このドロップダウンリストには、Microsoft Azure マーケットプレイスで公開されているデバイスソフトウェアのバージョンが含まれています。
  - [Size of Transit WAN Edge] ドロップダウンリストで、トランジット VNet で実行される各 Cisco Catalyst SD-WAN クラウドデバイスに使用できるメモリと CPU を決定するオプションを選択します。
    - 『Cisco CSR 1000v Deployment Guide for Microsoft Azure』の Cisco CSR1000V の「[Supported Instance Types](#)」を参照してください。
    - 「Deploying Cisco Catalyst 8000V on Microsoft Azure」の Cisco Catalyst 8000V の「[Supported Instance Types](#)」を参照してください。

(注) 次のサイズを選択することを推奨します。

Cisco CSR1000V および Cisco Catalyst 8000V には、4 つ以上の vCPU を持つ DS3 インスタンスタイプを選択します ([Standard DS3 v2 (4vCPU)] など)。
  - ダイレクトインターネットアクセス (DIA) 用にトランジット VNet デバイスを設定するには、次のいずれかをクリックします。
    - [Disabled] : インターネットアクセスなし。
    - [Enabled via Transport] : デバイスの WAN インターフェイスに対して NAT を設定または有効化します。
    - [Enabled via Umbrella SIG] : デバイスでセキュアな DIA を有効にするように Cisco Umbrella を設定します。
  - [Device 1] ドロップダウンリストで、最初のデバイスのシリアル番号を選択します。
  - [Device 2] ドロップダウンリストで、デバイスペアの 2 番目のデバイスのシリアル番号を選択します。
  - より具体的な設定オプションを入力する場合は、[Advanced] をクリックします。
  - [Transit VNet CIDR] フィールドに、16 ~ 25 の範囲のネットワークマスクを持つカスタム CIDR を入力します。このフィールドを空のままにすると、トランジット VNet はデフォルト CIDR の 10.0.0.0/16 を使用して作成されます。
- c) [Save and Finish] をクリックしてトランジット VNet の設定を完了するか、必要に応じて [Proceed to Discovery and Mapping] をクリックしてウィザードを続行します。

**ステップ 7** ホスト VNet をトランジット VNet にマッピングします。

- a) [Select an account to discover] ドロップダウンリストで、Azure サブスクリプション ID を選択します。または、ホスト VNet を検出する新しい Azure アカウントを追加するには、[New Account] をクリックします。
- b) [Discover Host VNets] をクリックします。
- c) [Select a VNet] ドロップダウンリストで、目的のホスト VNet を選択します。
- d) [Next] をクリックします。
- e) ホスト VNet のテーブルから、目的のホスト VNet を選択します。
- f) [Map VNets] をクリックします。[Map Host VNets] ポップアップが表示されます。
- g) [Transit VNet] ドロップダウンリストで、ホスト VNet にマッピングするトランジット VNet を選択します。
- h) [VPN] ドロップダウンリストで、マッピングを配置するオーバーレイネットワーク内の VPN を選択します。
- i) [IPSec Tunnel CIDR] セクションで、Azure Virtual Network トランジットに到達するように IPSec トンネルを設定するには、Cisco CSR1000V または Cisco Catalyst 8000V デバイスのそれぞれに対して、インターフェイス IP アドレスの 2 つのペアと、ループバック IP アドレスのペアを入力します。IP アドレスが /30 サブネット内のネットワークアドレスであり、オーバーレイネットワーク全体で一貫しており、ホスト VNet CIDR の一部ではないことを確認します。ホスト VNet CIDR の一部である場合、トランジット VNet への VPN 接続を作成しようとすると、Microsoft Azure からエラーが返されます。

(注) IP アドレスは、ホスト VNet およびトランジット VPC CIDR の一部ではありません。

Microsoft Azure は、IPSec トンネルを介した単一の仮想プライベートゲートウェイ (VGW) の設定をサポートし、単一のトンネルを介して冗長性を提供します。そのため、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS は冗長性のために 2 つの VGW をサポートしています。VGW の計画的なメンテナンスまたは計画外のイベント中に、VGW からクラウドデバイスへの IPSec トンネルが切断されます。この接続が失われると、クラウドデバイスは IPSec トンネルを介した Cisco SD-WAN Manager との BGP ピアリングを失います。IPSec トンネルの IP アドレスではなくクラウドルータとの BGP ピアリングを有効にするには、各クラウドデバイスにループバックアドレスを指定します。

(注) BGP ピアリングのループバックオプションは、Azure クラウドでの単一および複数の仮想ゲートウェイ、カスタマーゲートウェイ、またはその両方の設定をサポートしています。ループバックオプションは、トランジット VNet にマッピングされた新しいホスト VNet にのみ適用され、既存の VNet には適用されません。

- j) [Azure Information] セクションで、次の手順を実行します。
  1. [BGP ASN] フィールドに、ホスト VNet 内で起動される Azure Virtual Network ゲートウェイで設定する ASN を入力します。Azure の既存の設定に含まれていない ASN を使用します。許容可能な ASN 値については、Microsoft Azure のドキュメントを参照してください。
  2. [Host VNet Gateway Subnet] フィールドに、仮想ネットワークゲートウェイを配置できるホスト VNet サブネットを入力します。/28 以上のサブネットを使用することを推奨します。VNet 内にすでに作成されているサブネットは指定しないでください。

(注) ホスト VNet CIDR 内に未使用の CIDR があることを確認します。

- k) [Map VNets] をクリックします。
- l) [Save and Complete] をクリックします。

(注) トランジット VNet を形成する 2 つの Cisco Catalyst SD-WAN クラウドデバイスの VPN 0 の VPN 機能テンプレートを設定する場合は、トンネルインターフェイスに割り当てる色がプライベートの色ではなくパブリックの色であることを確認します。パブリックの色は次のとおりです。

- **3g**
- **biz-internet**
- **blue**
- **bronze**
- **custom1**
- **custom2**
- **custom3**
- **default**
- **gold**
- **green**
- **lte**
- **metro-ethernet**
- **mpls**
- **public-internet**
- **red**
- **silver**

[Task View] 画面が表示されるので、ホスト VNet がトランジット VNet に正常にマッピングされたことを確認します。

VNet ゲートウェイの作成には、最大で 45 分かかる場合があります。

# ホストおよびトランジット VNet の管理

## ホスト VNet の表示

### 手順

---

**ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration] > [Cloud onRamp for IaaS]** を選択します。目的の VNet をクリックします。[Host VNets/Transit VNets] ウィンドウが開きます。

デフォルトでは、[Mapped Host VNets] フィールドが選択され、マッピングされたホスト VNet の下のテーブルには、マッピングされたホストとトランジット VNet、トランジット VNet の状態、および VPN ID が一覧表示されます。

**ステップ 2** マッピングされていないホスト VNet を一覧表示するには、[Un-Mapped Host VNets] をクリックします。次に、[Discover Host VNets] をクリックします。

**ステップ 3** トランジット VNet を表示するには、[Transit VNets] をクリックします。

---

## 既存のトランジット VNet へのホスト VNet のマッピング

### 手順

---

**ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration] > [Cloud onRamp for IaaS]** を選択します。目的の VNet をクリックします。[Host VNets/Transit VNets] ウィンドウが開きます。

**ステップ 2** [Un-Mapped Host VNets] をクリックします。

**ステップ 3** [Discover Host VNets] をクリックします。

**ステップ 4** 検出されたホスト VNet のリストから、目的のホスト VNet を選択します。

**ステップ 5** [Map VNet] をクリックします。[Map Host VNets] ポップアップが開きます。

**ステップ 6** [Transit VNet] ドロップダウンリストから、目的のトランジット VNet を選択します。

**ステップ 7** [VPN] ドロップダウンリストで、マッピングを配置するオーバーレイネットワーク内の VPN を選択します。

**ステップ 8** [Map VNets] をクリックします。

---

## ホスト VNet のマッピング解除

### 手順

- ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration] > [Cloud onRamp for IaaS]** を選択します。目的の VNet をクリックします。[Host VNets/Transit VNets] ウィンドウが開きます。
- ステップ 2 [Mapped Host VNets] をクリックします。
- ステップ 3 VNet のリストから、目的のホスト VNet を選択します。一度に 1 つの VNet のマッピングを解除することを推奨します。複数の VNet のマッピングを解除する場合は、1 回のマッピング解除操作で 4 つ以上選択しないでください。
- ステップ 4 [Un-Map VNets] をクリックします。
- ステップ 5 [OK] をクリックして、マッピングの解除を確定します。

## トランジット VNet の表示

### 手順

- ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration] > [Cloud onRamp for IaaS]** を選択します。目的の VNet をクリックします。[Host VNets/Transit VNets] ウィンドウが開きます。
- ステップ 2 [Transit VNets] をクリックします。

テーブルに、すべてのトランジット VNet が一覧表示されます。

## トランジット VNet の追加

### 手順

- ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration] > [Cloud onRamp for IaaS]** を選択します。目的の VNet をクリックします。[Host VNets/Transit VNets] ウィンドウが開きます。
- ステップ 2 [Transit VNets] をクリックします。
- ステップ 3 [Add Transit VNet] をクリックします。

トランジット VNet を追加するには、[Microsoft Azure の Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定 \(25 ページ\)](#) のステップ 5 の手順に従います。

## トランジット VNet の削除

### 手順

- ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VNet をクリックします。[Host VNets/Transit VNets] ウィンドウが開きます。
- ステップ 2 [Mapped Host VNets] をクリックします。
- ステップ 3 目的のホスト VNet を選択し、[Un-Map VNets] をクリックします。  
削除するトランジット VNet にマッピングされているすべてのホスト VNet のマッピングを解除してください。
- ステップ 4 [OK] をクリックして、マッピングの解除を確定します。
- ステップ 5 [Transit VNets] をクリックします。
- ステップ 6 削除するトランジット VNet のごみ箱アイコンをクリックします。
- ステップ 7 [OK] をクリックして確定します。

## Cisco Catalyst SD-WAN Cloud OnRamp for IaaS のトラブルシューティング

この項では、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の一般的な問題のトラブルシューティングの方法について説明します。

### 2つの Cisco CSR1000V または Cisco Catalyst 8000V デバイスが使用できない

Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。[Add New Cloud Instance] をクリックすると、2つの Cisco CSR1000V または Cisco Catalyst 8000V デバイスが使用できないことを示すエラーメッセージが表示されます。

#### 問題の解決方法

Cisco SD-WAN Manager サーバーに、ライセンスが有効な Cisco Catalyst SD-WAN ソフトウェアを実行している2つの Cisco CSR1000V または Cisco Catalyst 8000V デバイスがありません。オペレーションズチームに連絡して、必要な Cisco CSR1000V または Cisco Catalyst 8000V デバイスを作成できるようにします。

Cisco CSR1000V または Cisco Catalyst 8000V デバイスが存在し、エラーメッセージが引き続き表示される場合は、2つのデバイスが設定テンプレートにアタッチされていません。Cisco SD-WAN Manager の **[Configuration]** > **[Templates]** [Device] ウィンドウで、これらのテンプレートをアタッチします。目的のデバイステンプレートについて、[...] をクリックし、[Attach Devices] を選択します。

### 必要な API 権限が使用できない

API キーを入力すると、このユーザーに必要な権限がないことを示すエラーメッセージが表示されます。

#### 問題の解決方法

Cisco SD-WAN Manager サーバーがインターネットに到達できることと、AWS または Microsoft Azure に到達できるように DNS サーバーが設定されていることを確認します。DNS サーバーを設定するには、Cisco SD-WAN Manager VPN 機能設定テンプレートで DNS サーバーの IP アドレスを入力し、設定テンプレートを Cisco SD-WAN Manager サーバーに再アタッチします。

AWS の場合は、AWS アカウントに属する API キーを確認します。キーが正しくないと思われる場合は、別のキーのペアを生成します。

AWS で、正しいキーを入力してもエラーメッセージが引き続き表示される場合は、キーに必要な権限がありません。キーに関連付けられているユーザー権限を確認します。VPC と EC2 インスタンスを作成および編集するために必要な権限をユーザーに付与します。

エラーメッセージが引き続き表示される場合は、Cisco SD-WAN Manager サーバーの時刻を確認して、現在の時刻に設定されていることを確認します。そうでない場合は、Cisco SD-WAN Manager のサーバータイムが Google NTP サーバーを示すように設定します。サーバータイムを設定するには、Cisco SD-WAN Manager NTP 機能設定テンプレートで、NTP サーバーのホスト名を入力します。次に、Cisco SD-WAN Manager を使用して設定テンプレートを NTP 機能に再アタッチします。Google NTP サーバーは、time.google.com、time2.google.com、time3.google.com、time4.google.com などです。

### AWS の設定時に WAN エッジルータのソフトウェアバージョンがドロップダウンに表示されない

#### 問題に関する説明

トランジット VPC のトランジット VPC パラメータの設定を試みたときに、Cisco CSR1000V および Cisco Catalyst 8000V デバイスのソフトウェアバージョンがドロップダウンリストに表示されません。

#### 問題の解決方法

AWS Marketplace 内で、使用しているアカウントで Cisco CSR1000V または Cisco Catalyst 8000V デバイスの Amazon マシンイメージ (AMI) に登録していることを確認します。

Cisco CSR1000V がソフトウェアリリース 16.12.1b 以降を使用していて、Cisco Catalyst 8000V がソフトウェアリリース 17.4.1a 以降を使用していることを確認します。

### 設定中に VPN がリストにない

#### 問題に関する説明

マッピングするホスト VPC または VNet を選択した後に、VPN がドロップダウンリストに表示されません。

#### 問題の解決方法

この問題は、Cisco Catalyst SD-WAN クラウドデバイスにアタッチされたデバイス設定テンプレートにサービス側VPNが含まれていない場合に発生します。トランジットおよびホストVPCまたはVNet用に選択した2つのCisco Catalyst SD-WAN クラウドデバイス間のIPsec接続を設定するには、サービス側VPN（VPN 0 およびVPN 512 以外のVPN）が必要です。

この問題は、トランジットVPCまたはVNet用に選択した2つのCisco Catalyst SD-WAN クラウドデバイスに重複するサービス側VPNがない場合にも発生する可能性があります。2つのCisco Cloud Services Router 1000V またはCisco Catalyst 8000V デバイスがアクティブ-アクティブのペアを形成するため、両方のデバイスで同じサービス側VPNを設定します。

サービス側VPNを設定するには、Cisco SD-WAN Manager VPN 機能設定テンプレートで、少なくとも1つのサービス側VPNを設定します。両方のルータで、少なくとも1つのサービス側VPNが同じであることを確認します。次に、設定テンプレートをルータに再アタッチします。

### Cisco Catalyst SD-WAN Cloud OnRamp for IaaS タスクが失敗する

#### 問題に関する説明

ホストVPCからトランジットVPCへのマッピング、またはホストVNetからトランジットVNetへのマッピングが完了した後に、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定が失敗します。

#### 問題の解決方法

画面に表示されたタスク情報を確認して、タスクが失敗した理由を特定します。エラーがAWSまたはAzureのリソースに関連している場合は、必要なすべてのリソースが配置されていることを確認します。

### Cisco Catalyst SD-WAN Cloud OnRamp for IaaS タスクは成功するが、Cisco Catalyst SD-WAN クラウドデバイスがダウンしている

#### 問題に関する説明

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS タスクは成功しましたが、Cisco Catalyst SD-WAN クラウドデバイスが引き続きダウン状態です。

#### 問題の解決方法

設定テンプレートを確認します。

- ポリシーを含む、Cisco Catalyst SD-WAN クラウドデバイス設定のすべての部分が有効で正しいことを確認します。設定が無効な場合、設定はルータに適用されず、ルータは起動しません。
- Cisco Catalyst SD-WAN Validator の設定が正しいことを確認します。Cisco Catalyst SD-WAN Validator で設定されたDNS名またはIPアドレスが間違っている場合、Cisco CSR1000V またはCisco Catalyst 8000V デバイスはCisco Catalyst SD-WAN Validator に到達できないため、オーバーレイネットワークに参加できません。

設定の問題を特定したら、次の手順を実行します。

1. Cisco Catalyst SD-WAN Cloud OnRamp for IaaS コンポーネントを削除します。
  1. ホスト VPC または VNet とトランジット VPC または VNet のマッピングを解除します。
  2. Cisco CSR1000V または Cisco Catalyst 8000V デバイスのトランジット VPC を削除します。
2. 設定テンプレートを編集し、Cisco Catalyst SD-WAN クラウドデバイスに再アタッチします。
3. Cisco Catalyst SD-WAN Cloud OnRamp for IaaS 設定プロセスを繰り返します。

### 必要なルートが交換されない

#### 問題に関する説明

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS 設定ワークフローが成功し、Cisco CSR1000V または Cisco Catalyst 8000V デバイスが使用可能で実行されていますが、目的のルートが交換されていません。

#### 問題の解決方法

Cisco SD-WAN Manager で、トランジットクラウドルータの BGP 設定を確認します。マッピングプロセス中に Cisco Catalyst SD-WAN Cloud OnRamp for IaaS サービスを設定すると、BGP はネットワークアドレス 0.0.0.0/0 をアドバタイズするように設定されます。サービス側 VPN に、0.0.0.0/0 を指す IP ルートが含まれていることを確認します。必要に応じて、VPN 機能設定テンプレートにスタティックルートを追加し、トランジット VPC または VNet 用に選択した 2 つのクラウドルータに設定を再アタッチします。

AWS で、ホスト VPC に移動し、ルートテーブルを確認します。ルートテーブルで、[Enable route propagation] をクリックして、VPC がルートを受信するようにします。

### エンドツーエンドの ping が失敗する

#### 問題に関する説明

ルーティングは正常に機能していますが、エンドツーエンドの ping が機能していません。

#### 問題の解決方法

AWS で、ホスト VPC のセキュリティグループルールを確認します。Azure で、ホスト VNet のネットワークセキュリティグループルールを確認します。セキュリティグループルールでは、オンプレミスまたはブランチ側のデバイスの送信元 IP アドレス範囲のサブネットで、ブランチからのトラフィックが AWS に到達することが許可されるようにする必要があります。

# 機能テンプレートの設定例

## 機能テンプレート

次に、Cisco CSR1000V、Cisco Catalyst 8000V デバイスのさまざまな機能テンプレートの設定例を示します。

### システム機能テンプレート

テンプレート : Basic Information/Cisco System

テンプレート名 : Cisco\_System\_cEdge\_Template

説明 : System Template

表 2: システム機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
基本設定	サイト ID	デバイス固定	system_site_id
	システム IP	デバイス固定	system_system_ip
	ホストネーム	デバイス固定	system_host_name
	デバイスグループ	デバイス固定	system_device_groups
	Console Baud Rate	グローバル	115200
GPS	Latitude	デバイス固定	system_latitude
	Longitude	デバイス固定	system_longitude
Advanced	ポートホッピング	デバイス固定	system_port_hop
	ポートオフセット	デバイス固定	system_port_offset

### ロギング機能テンプレート

テンプレート : Other Templates/Cisco Logging

テンプレート名 : Cisco\_Logging\_cEdge\_Template

説明 : Logging Template

表 3: ログ機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
Server (オプション)	Hostname/IP address	グローバル	10.1.0.68
	VPN ID	デバイス固定	logging_server_vpn

Logging\_Template 内のログサーバーはオプションです。

### BFD 機能テンプレート

テンプレート : Basic Information/Cisco BFD\_Template

テンプレート名 : BFD\_cEdge\_Template

説明 : BFD Template

表 4: BFD 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
基本設定	Poll Interval	グローバル	120000
Color (Biz Internet)	色	ドロップダウン リスト	Biz Internet
	Hello Interval (milliseconds)	デバイス固定	biz_internet_bfd_hello_interval
	Path MTU	グローバル	オフ

### VPN512 機能テンプレート

テンプレート : VPN/Cisco VPN

テンプレート名 : Cisco\_Transit\_VPN512\_Template\_cEdge\_Template

説明 : VPN 512 Out-of-Band Management

表 5: VPN512 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
基本設定	VPN	グローバル	512
	Name	グローバル	管理VPN

**VPN512 インターフェイス イーサネット機能テンプレート**

テンプレート : VPN / Cisco VPN Interface Ethernet

テンプレート名 : Cisco\_Transit\_VPN512\_Interface\_Template\_cEdge\_Template

説明 : VPN 512 Management Interface

表 6: VPN512 インターフェイス イーサネット機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
基本設定	シャットダウン	グローバル	非対応
	Interface Name	デバイス固定	vpn512_mgmt_int
	説明	グローバル	管理インターフェイス
IPv4 の設定	IPv4 アドレス	オプションボタン (Radio Button)	Dynamic

**NTP 機能テンプレート**

テンプレート : Basic Information/Cisco NTP

テンプレート名 : Cisco\_NTP\_cEdge\_Template

説明 : NTP Template

表 7: NTP 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
サーバー (Server)	Hostname/IP address	グローバル	time.nist.gov

既知の信頼できる NTP サーバーのみを使用するように注意する必要があります。時刻同期の中断は、トランジット VPC またはトランジット VNet 内の Cisco Catalyst SD-WAN クラウドデバイスが Cisco SD-WAN 制御コンポーネントに接続する機能、および他の Cisco Catalyst SD-WAN デバイスへの IPsec 接続を確立する機能に影響を与える可能性があります。

### AAA 機能テンプレート

テンプレート : Basic Information/Cisco AAA

テンプレート名 : Cisco\_AAA\_cEdge\_Template

説明 : AAA Template

表 8 : Cisco AAA 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
Local	User/admin/Password	グローバル	<自分の管理者パスワード>
	User/admin/Privilege	グローバル	15
AAA	ServerGroups priority order	グローバル	local

### OMP 機能テンプレート

テンプレート : Basic Information/Cisco OMP

テンプレート名 : Cisco\_OMP\_cEdge\_Template

説明 : OMP Template

表 9 : Cisco OMP 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
OMP	Number of Paths Advertised per Prefix	グローバル	Factory_Default_Cisco_OMP_ipv46_Template

### セキュリティ機能テンプレート

テンプレート : Basic Information/Cisco Security

テンプレート名 : Cisco\_Security\_cEdge\_Template

説明 : Security Template

表 10: セキュリティ機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
セキュリティ	Replay window	グローバル/ドロップダウンリスト	Factory_Default_Cisco_Security_Template

**VPN0 機能テンプレート**

テンプレート : VPN/Cisco VPN

テンプレート名 : Cisco\_Transit\_VPN0\_cEdge\_Template

説明 : VPN0 Transport Template

表 11: VPN0 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
Basic configuration	VPN	グローバル	0
	Name	グローバル	トランスポート VPN

**VPN0 インターフェイス機能テンプレート**

テンプレート : VPN/Cisco VPN Interface Ethernet

テンプレート名 : Cisco\_Transit\_VPN0\_cEdge\_gigabit-ethernet2

説明 : VPN0 Transport Interface

表 12: Cisco VPN0 インターフェイス機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
Basic configuration	シャットダウン	デバイス固定	vpn0_inet_int_shutdown
	Interface Name	ドロップダウンリスト	GigabitEthernet2/
	説明	グローバル	Internet Interface
IPv4 の設定	IPv4 アドレス	オプション ボタン (Radio Button)	Dynamic
	Bandwidth Upstream	デバイス固定	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	デバイス固定	vpn0_inet_int_bandwidth_down

セクション	パラメータ	タイプ	変数/値
Tunnel	トンネル インターフェイス	グローバル	オン
	色	グローバル	biz-internet
	[Allow Service] > [All]	グローバル	オン
[Tunnel] > [Advanced Options] > [Encapsulation]	IPsec Preference	デバイス固定	vpn0_inet_tunnel_ipsec_preference
Advanced	TCP MSS	グローバル	1350

### VPN1 機能テンプレート

テンプレート : VPN/Cisco VPN

テンプレート名 : Cisco\_Transit\_VPN1\_cEdge\_Template

説明 : VPN1 Service Template

表 13: VPN1 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
Basic configuration	VPN	グローバル	1
	Name	グローバル	Service VPN 1
	Enhance ECMP Keying	グローバル	オン
OMP のアドバタイズ	BGP (IPv4)	グローバル	オン
	Connected (IPv4)	グローバル	オン

### VPN2 機能テンプレート

テンプレート : VPN/Cisco VPN

テンプレート名 : Cisco\_Transit\_VPN2\_cEdge\_Template

説明 : VPN2 Service Template

表 14: VPN2 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
Basic configuration	VPN	グローバル	2
	Name	グローバル	Service VPN 2
	Enhance ECMP Keying	グローバル	オン
OMP のアドバタイズ	BGP (IPv4)	グローバル	オン

### デバイステンプレート

次の表に、Cisco CSR1000V または Cisco Catalyst 8000V デバイスのデバイステンプレートの概要を示します。

テンプレート名 : Cloud\_OnRamp\_cEdge\_Template

表 15: トランジット VPC または トランジット VNet デバイステンプレート

[Template Type]	テンプレートのサブタイプ	テンプレート名
Cisco System		Cisco_System_cEdge_Template
	Cisco ロギング	Cisco_Logging_cEdge_Template
	Cisco NTP	Cisco_NTP_cEdge_Template
	Cisco AAA	Cisco_AAA_cEdge_Template
Cisco BFD		BFD_cEdge_Template
Cisco OMP		Cisco_OMP_cEdge_Template
シスコのセキュリティ		Cisco_Security_cEdge_Template
Cisco VPN0		Cisco_Transit_VPN0_cEdge_Template
	Cisco VPN インターフェイス ネット	Cisco_Transit_VPN0_cEdge_gigabit-ethernet2

[Template Type]	テンプレートのサブタイプ	テンプレート名
Cisco VPN512		Cisco_Transit_VPN512_Template_cEdge_Template
	Cisco VPN インターフェイス ネットワーク	Cisco_Transit_VPN512_Interface_Template_cEdge_Template
Cisco VPN1		Cisco_Transit_VPN1_cEdge_Template
VPN2		Cisco_Transit_VPN2_cEdge_Template

## デバイステンプレート変数値の例

次のサンプル情報は、1 番目と 2 番目の Cisco CSR1000V または Cisco Catalyst 8000V デバイスに使用できるデバイステンプレート変数値を示しています。

表 16: 最初のデバイスの **Cisco CSR1000V** または **Cisco Catalyst 8000V** のデバイステンプレート変数値

変数	値
ホスト名 (system_host_name)	CSR_CoR1
システム IP (system_system_ip)	209.165.200.225
サイト ID (system_site_id)	115001

表 17: 2 番目のデバイスの **Cisco CSR1000V** または **Cisco Catalyst 8000V** のデバイステンプレート変数値

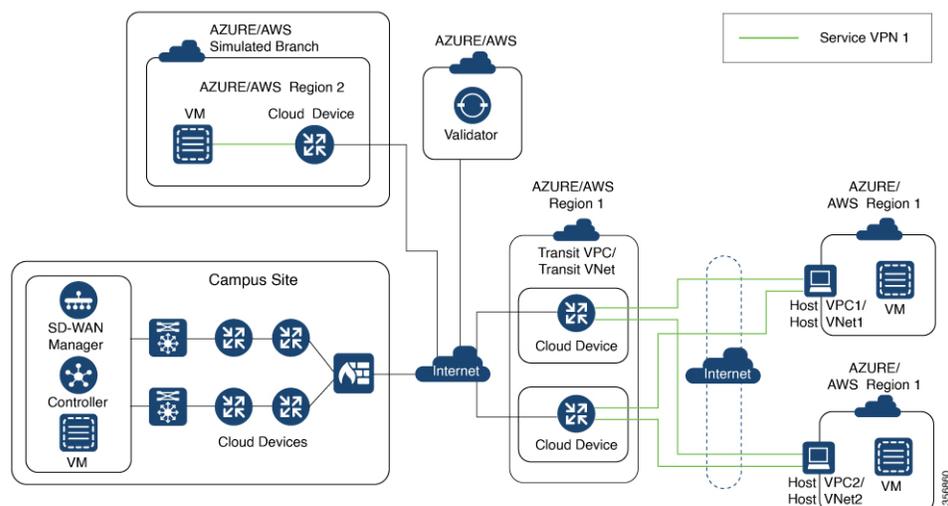
変数	値
ホスト名 (system_host_name)	CSR_CoR2
システム IP (system_system_ip)	209.165.201.1
サイト ID (system_site_id)	115001

## Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の例

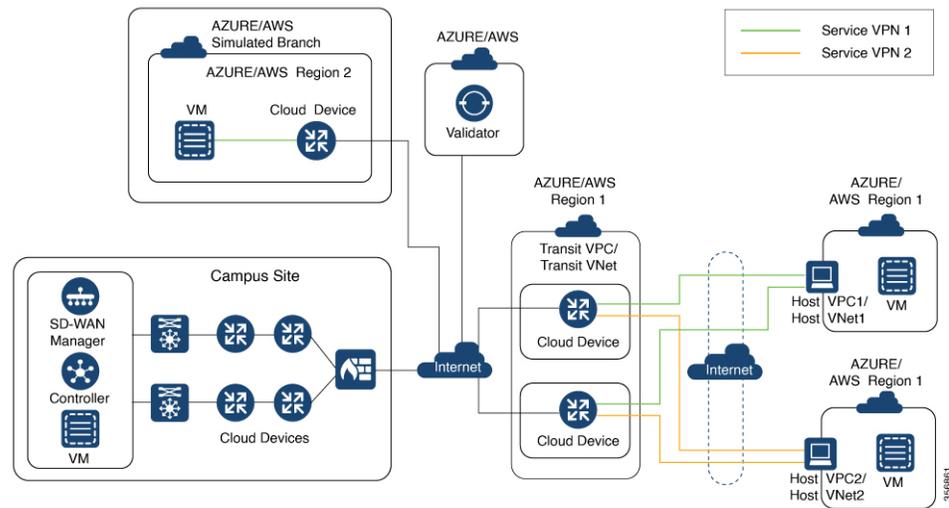
この例では、単一のトランジット VPC または VNet が AWS または Microsoft Azure のリージョン内に作成され、同じリージョン内の 2 つの既存のホスト VPC または VNet をトランジット VPC または VNet にマッピングします。その後、キャンパスおよびシミュレートされたブランチの場所からホスト VPC または VNet にアクセスできます。

Cisco Catalyst SD-WAN 展開では、0～512の範囲のさまざまなVPNを使用して接続を実装します。VPN 0はトランスポート（WAN）ネットワークを表し、VPN 512は管理ネットワークを表します。残りのVPN（1～511）をサービスVPNとして使用します。Cisco Catalyst SD-WAN Cloud OnRamp for IaaSの展開では次の2つのシナリオが考慮されます。

- 完全接続：両方のホストVPCまたはVNetを、トランジットVPCまたはVNet内のサービスVPN 1にマッピングします。サービスVPN 1は、キャンパス内に展開されているCisco CSR1000VまたはCisco Catalyst 8000Vデバイス、およびシミュレートされたブランチ内に展開されているCisco CSR1000VまたはCisco Catalyst 8000Vデバイスのサービス側で設定できます。この接続により、キャンパスサイトとブランチサイトの両方から、いずれかのホストVPC内のAWS Elastic Compute Cloud（EC2）インスタンスへの通信が可能になります。また、この接続により、2つのホストVPC内に展開されたAWSまたはAzure EC2インスタンス間の通信も可能になります。この展開では、組織内のすべてのエンティティが、組織によって展開されたパブリッククラウドリソースに完全に接続できるシナリオを示しています。次の図は、この最初のシナリオを示しています。



- クラウドプロバイダーに対するセグメンテーション：片方のホストVPCまたはVNetをサービスVPN 1にマッピングし、もう片方のホストVPCまたはVNetをトランジットVPCまたはVNet内のサービスVPN 2にマッピングします。このマッピングによりセグメンテーションが提供されるため、2つのホストVPCまたはVNet間のトラフィックが分離されます。サービスVPN 1にのみキャンパスを設定し、最初のホストVPC内のAWSまたはAzure EC2インスタンスと通信できるようにすることができます。サービスVPN 2のブランチを設定し、2番目のホストVPC内のAWSまたはAzure EC2インスタンスと通信できるようにします。この展開では、組織内のさまざまなエンティティが、特定のパブリッククラウドリソースへのアクセスのみを必要とするシナリオを示しています。次の図は、この2番目のシナリオを示しています。



### 同じサービス VPN 内のトランジット VPC または VNet へのホスト VPC または VNet のマッピング

両方のホスト VPC または VNet を、トランジット VPC または VNet 内のサービス VPN 1 にマッピングするには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration] > [Cloud onRamp for IaaS]** を選択します。マッピングする両方のホスト VPC またはホスト VNet を選択し、**[Map VPCs]** または **[Map VNet]** をクリックします。

[Map Host VPCs] または [Map Host VNet] ポップアップが開きます。

2. [Transit VPC] または [Transit VNet] ドロップダウンリストで、ホスト VPC または VNet にマッピングするトランジット VPC または VNet を選択します。
3. [VPN] ドロップダウンリストで、[1] を選択します。

ホスト VPC またはホスト VNet を同じサービス VPN にマッピングすると、ホスト VPC または VNet 間の通信が可能になります。

4. AWS 設定の場合は、[Route Propagation] を無効にします。

ルート伝達を有効にすると、マッピング用に選択されたホスト VPC に BGP ルートが伝達されます。

5. [Map VPCs] または [Map VNet] をクリックします。

数分後に [Task View] ウィンドウが表示されるので、ホスト VPC または VNet がトランジット VPC または VNet にマッピングされたことを確認します。

これらの手順により、サービス VPN 1 への両方のホスト VPC または VNet のマッピングが完了します。各ホスト VPC または VNet での EC2 インスタンス間の接続を確認するには、それらの間に SSH 接続を確立します。同様に、キャンパスとブランチの両方をサービス VPN 1 にマッピングして、キャンパスとブランチからホスト VPC または VNet 内の EC2 インスタンスへの SSH 接続を確立することで、両方のホスト VPC または VNet への接続を確認できます。

## 異なるサービス VPN 内のトランジット VPC または VNet への各ホスト VPC または VNet のマッピング

片方のホスト VPC または VNet をサービス VPN 1 にマッピングし、もう片方のホスト VPC または VNet をサービス VPN 2 にマッピングするには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。マッピングするホスト VPC または VNet を選択し、**[Map VPCs]** または **[Map VNets]** をクリックします。

[Map Host VPCs] または [Map Host VNets] ポップアップが開きます。

2. **[Transit VPC]** または **[Transit VNet]** ドロップダウンリストで、ホスト VPC または VNet にマッピングするトランジット VPC または VNet を選択します。

3. **[VPN]** ドロップダウンリストで、**[1]** を選択します。

これで、最初のホスト VPC または VNet がサービス VPN 1 にマッピングされました。

4. **[Map VPCs]** または **[Map VNets]** をクリックします。

数分後に **[Task View]** ウィンドウが表示されるので、ホスト VPC または VNet がトランジット VPC または VNet にマッピングされたことを確認します。

5. 2 番目のホスト VPC または VNet に対してステップ 1 ~ 3 を繰り返します

VPN 値を選択するときは、ホスト VPC または VNet をサービス VPN 2 にマッピングします。

このプロセスにより、サービス VPN 1 への最初のホスト VPC または VNet のマッピングと、サービス VPN 2 への 2 番目のホスト VPC または VNet のマッピングが完了します。

キャンパスをサービス VPN 1 にマッピングして、キャンパスから最初のホスト VPC または VNet 内の EC2 インスタンスへの SSH 接続を確立することで、最初のホスト VPC または VNet への接続を確認できます。ただし、キャンパスから 2 番目のホスト VPC または VNet 内の EC2 インスタンスへの SSH 接続は確立できません。ブランチをサービス VPN 2 にマッピングして、ブランチから 2 番目のホスト VPC または VNet 内の EC2 インスタンスへの SSH 接続を確立することで、2 番目のホスト VPC または VNet への接続を確認できます。ただし、ブランチから最初のホスト VPC または VNet 内の EC2 インスタンスへの SSH 接続は確立できません。

## 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。