プロビジョニング

クラウドホスト型コントローラへのアクセスの取得

シスコ マネージド クラウドホスト型コントローラは、デフォルトで管理アクセス用にクローズされています。シスコでは、セキュリティ上の理由から、クラウドホスト型 SD-WAN コントローラ向けの 0.0.0.0/0 へのアクセスを許可していません。お客様のエンタープライズ VPN 内にアクセス用の特定のパブリック IP プレフィックスがあると考えられるため、そのパブリック IP プレフィックスのみがアクセス用にオープンされます。特定の送信元 IP プレフィックスについては、https と ssh のみを許可リストに含めるようにリクエストして、アクセスを制限できます。シスコは、すべての宛先ポートおよびプロトコルへのアクセスを許可するように、お客様が指定したすべての送信元 IP プレフィックスをデフォルトでマークします。

クラウドホスト型コントローラのインターフェイスにはプライベート IP があります。各プライベート IP には、クラウド上のパブリック IP への 1 対 1 NAT があります。これらの IP は、インターフェイスが静的 IP または DHCP のどちらで設定されているかどうかにかかわらず、変更されません。インスタンスが復旧または交換された場合にのみ IP が変更されます。

許可リストは、パブリック IP アドレスを持つすべてのコントローラのすべてのネットワークインターフェイスに適用されます。クラウドホスト型コントローラセットに適用される許可リストを更新または表示するには、Cisco TAC でケースをオープンします。

クラウド セキュリティ グループの許可リストを追加、削除、または変更するには、次のいずれかのオプションを使用します。

- https://ssp.sdwan.cisco.com でシスコ セルフサービス ポータルにログインし、アクセスリストを管理します。オーバーレイ コントローラ プロファイルを基本とするスマートアカウントの Cisco PNP スマートアカウント管理者である必要があります。
- Cisco TAC サポートケースをオープンして、次の情報を入力します。
  - オーバーレイ/VA 名

- Cisco vManage IP/FQDN
- 許可リストで追加、削除、または変更する必要があるプレフィックス/ルール（vManage GUI アクセス）
- IP アドレス
- すべてのトラフィックまたは選択したトラフィック（https、SSH など）で IP アドレスを許可するかどうかの指定

Cisco SD-WAN セルフサービスポータルについて、シスコではスマートアカウント管理者に Cisco SD-WAN セルフサービスポータルにアクセスする権限を付与しています。スマートアカウント管理者は、コントローラの IP アドレスの表示やコントローラの IP アクセスリストの変更など、顧客のホスト型コントローラインフラストラクチャに関連する運用タスクを表示および実行できます。このアクセスを特定のユーザに付与しない場合は、Cisco Software Central の [Manage Smart Account] セクションに移動し、それらのユーザをスマートアカウント管理者から削除するか、IDP（ID プロバイダー）オンボーディング機能を使用して、Cisco SD-WAN セルフサービスポータルへのアクセスを IDP の信頼できるユーザに基づいて付与してください。

クラウドホスト型コントローラ IP のプロビジョニング

Cisco vManage完全修飾ドメイン名（FQDN）は VPN 512 パブリック IP にマップされ、管理アクセスに使用されます。ただし、エッジノードは、VPN 0 上にあり、異なるパブリック IP アドレスを持つ Cisco vManage のトランスポート インターフェイスでトンネルを形成します。シスコは、クラウドホスティングのために Cisco vManage と Cisco vBond オーケストレーションに FQDN を割り当てています。

Cisco vBond オーケストレーション では HTTP アクセスは使用できず、Cisco vManage のみが Web サーバーと Web/https へのアクセスを使用できます。

各コントローラインスタンスには、パブリック IP 1:1 に NAT 処理されるプライベート IP インターフェイスがあります。一般に、インスタンス インターフェイスのパブリック IP およびプライベート IP アドレスは変更されません。Cisco vBond オーケストレーション/Cisco vSmart コントローラ/Cisco vManage のプライベート/パブリック IP は、インスタンスを置き換えるか、新しいリージョンに移動する必要がある場合にのみ変更されます。

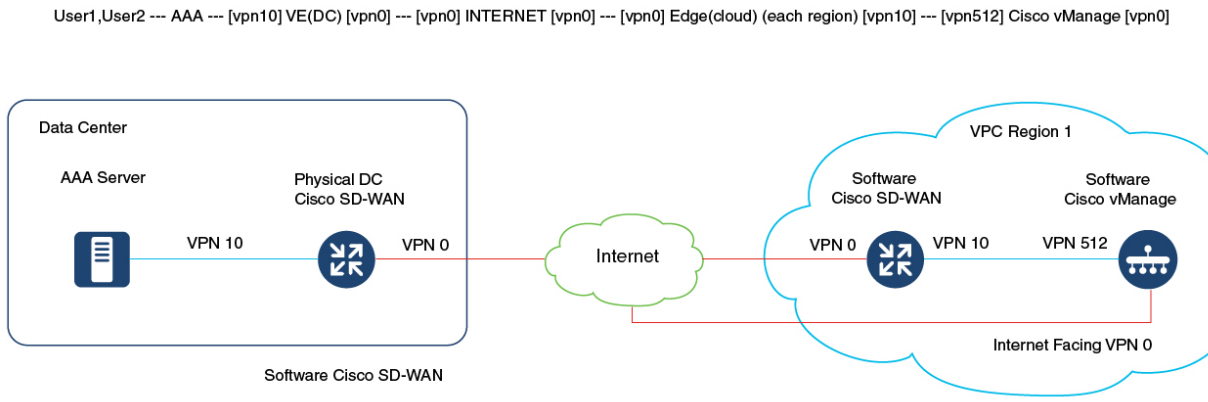
すべてのエッジはDTLS/TLS ポートを介してコントローラと通信するため、これらのDTLS/TLS ポートの任意の IP、またはクラウドコントローラの現在のパブリック IP に対してファイアウォールを開くことができます。DTLS/TLS ポートの詳細については、「複数の vCPU を実行する Cisco SD-WAN デバイスで使用されるポート」セクションの表 3 を参照してください。

クラウドホスト型コントローラのカスタムIPプレフィックス

一部のユースケースでは、管理アクセスと制御のため、クラウド コントローラ インターフェイスでカスタム ネットワーク プレフィックスに基づく IP が必要になる場合があります。次に例を示します。

- AAA または TACACS ベースの認証を使用した Cisco SD-WAN トンネル経由の 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 のデバイスの管理 VPN 512 にアクセスする。
- VPN 512 を介して Cisco vManage から Cisco SD-WAN トンネル経由で syslog サーバーに syslog を送信する。

図 *1 : AAA TACAS*



デフォルトでは、シスコ マネージド クラウドホスト型コントローラは、VPN 512 サブネットを含む 10.0.0.0/16 ベースのサブネットで展開されます。クラウド Cisco SD-WAN を追加し、VPN 512 サブネットをファブリック内の到達可能なサブネットとして使用すると、既存のサブネットと競合する可能性があります。

このような場合は、コントローラの展開の 2 つのリージョンごとに /24 プレフィックスを共有する必要があります。これらの IP プレフィックスはコントローラの作成に使用され、サブネットは Cisco SD-WAN ファブリック内で使用できるように設定されます。

オーバーレイ プロビジョニング後の AAA/TACAC を目的としたクラウド vEdge へのリクエスト

TAC-CSOne で CloudOps のケースをオープンして、次の詳細を確認および実行します。

1. AAA または TACAC の有効化をリクエストするには、既存のファブリック内で使用されていない IP プレフィックスを指定する必要があり、そのプレフィックスを使用してコントローラを作成できます（元のコントローラはシャットダウンされてスナップショットが作成され、複製されます）。

コントローラが設定されている各リージョンは、1 つの /24 ファブリックに関する一意のカスタムサブネットを持ちます。各オーバーレイには 2 つのリージョンがあるため、2 つのサブネットが必要となります。

2. Cisco vBond オーケストレーション、Cisco vSmart コントローラ、および Cisco vManage デバイスへの管理者クレデンシャルがあります。
3. CloudOps エンジニアによる事前承認と事前チェックの完了後、8 時間のメンテナンス期間をスケジュールできます。
4. プロセスを開始する前に、Cisco vBond オーケストレーション の DNS を有効にし、すべてのコントローラを設定します。
5. Cisco SD-WAN または Cisco vSmart コントローラ デバイスで、GR がデフォルトで 12 時間以上に設定されていることを確認します。
6. 2 つの使用可能なクラウド Cisco SD-WAN UUID を PNP 経由で予約し、Cisco vManage に接続します。
7. プロビジョニングされたコントローラ用にはシングルテナントかつシングルノードの Cisco vManage オーバーレイ、およびシングルテナントかつクラスタノードの Cisco vManage オーバーレイでのみサポートされ、プロビジョニング予定のコントローラセットに対してはすべて新規となります。この機能は、Cisco Multi-tenant vManage クラスタオーバーレイではサポートされません。
8. Cisco vBond オーケストレーション、Cisco vSmart コントローラ、およびもしあればシスコ提供のクラウド Cisco SD-WAN デバイスに、Cisco vManage のテンプレートを接続することをお勧めします。

シスコプロビジョニング後のクラウド vEdge の構成

1. Cisco CloudOps がクラウドホスト型コントローラの横にあるクラウド vEdge のプロビジョニングを完了すると、CloudOps は各クラウド vEdge の顧客へのパブリックおよびプライベート IP 割り当てを共有します。フォーマットは（VPN 512, VPN 0, VPN X）です。

   Cisco CloudOps は、新しくプロビジョニングされたクラウド vEdge のログイン情報を共有します。

2. クラウド vEdge の VPN 512 および VPN X インターフェイスは、そのリージョンのコントローラの VPN 512 と同じサブネットにあります。

   Cisco CloudOps によってプロビジョニングされるクラウド vEdge は、特に AAA/TACACS を目的とし、常に上記のネットワーク レイアウト フォーマットで作成されます。

   クラウド vEdge への到達可能性に問題がある場合は、一般に、クラウド vEdge のインターフェイス IP またはルート構成に問題があります。

3. また、パブリック IP とプライベート IP は 1:1 NAT されており、クラウド vEdge インターフェイスに割り当てられています。vEdge インターフェイス自体は dhcp で設定できますが、常に同じ IP をクラウドから取得します。

VPN X インターフェイスの場合は、Cisco CloudOps で共有されているものとまったく同じ静的 IP を設定する必要があります。

サブネット内のランダム IP は使用できません。

4. クラウド vEdge は、オーバーレイごとに同じ固有の環境でプロビジョニングされるため、コントローラと同じインバウンド許可アクセスリストの対象となります。

   パブリック IP と提供されたログイン情報で、SSH 経由で vEdge にログインする必要があります。

5. 次に、必要な構成を使用して新しいクラウド vEdge を設定する必要があります。たとえば、サイト ID、システム IP、組織名、vBond DNS または IP などです。

6. エンタープライズルート CA を使用している場合は、クラウド vEdge にも同様にアップロードしてインストールする必要があります。

7. viptelatac/ciscotacro/ciscotacrw ユーザーが有効になっているローカルで auth-fallback を使用して Cisco vManage 上の AAA/TACACS をローカルに設定できます。これにより、シスコサポートは必要に応じてログインし、問題のトラブルシュートを行うことができます。

8. プロビジョニングされたクラウド vEdge ごとに 1 つずつ、Cisco vManage のデバイスリストから未使用のクラウド vEdge UUID を取得する必要があります。

   使用している Cisco vManage の WAN エッジデバイスリストで使用可能なクラウド vEdge UUID がない場合は、Cisco PNP ポータルにログインし、オーバーレイに関連付けられているスマートアカウントとバーチャルアカウントにログインし、ソフトウェアデバイス（VEDGE-CLOUD- DNA）を追加してから、Cisco vManage 上でスマートアカウントを同期する必要があります。

9. 次に、クラウド vEdge で UUID をアクティブにして、Cisco vManage によって認証され、Cisco SD-WAN ファブリックに参加できるようにする必要があります。

10. クラウド vEdge の VPN X 静的 IP を指すように、（管理用のコントローラにアクセスするための顧客管理チームからの）顧客のエンタープライズサブネット用の特定の静的ルートを使用して、コントローラ（Cisco vManage、Cisco vBond オーケストレーション、Cisco vSmart コントローラ）の vpn 512 を設定する必要があります。

11. Azure でシスコがホストするオーバーレイの場合は、Cisco TAC ケースを開き、特定のエンタープライズサブネットプレフィックスを指定してください。ここから、コントローラの vpn 512 への接続が必須となります。

    Azure サブネットのデフォルトゲートウェイは、vEdge サービスの VPN IP をエンタープライズサブネットのゲートウェイとして構成した場合でも、事実上のゲートウェイです。したがって、コントローラの vpn 512 での構成に加えて、Azure 側で追加の構成が必要になります。シスコは、必要なエンタープライズサブネットごとに Azure ルート テーブル（RT）エントリを適用し、クラウド vEdge インターフェイスで IP 転送を有効にします。

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。