



Cisco SD-WAN オーバーレイネットワークの起動プロセス

- [Cisco vManage ペルソナおよびストレージデバイス](#) (1 ページ)
- [稼働イベントシーケンス](#) (3 ページ)
- [ソフトウェアのダウンロード](#) (36 ページ)
- [Cisco vManage の導入](#) (37 ページ)
- [Cisco vBond オーケストレーションの導入](#) (51 ページ)
- [vContainer ホスト](#) (69 ページ)
- [Cisco vSmart コントローラの導入](#) (69 ページ)
- [クラウドサービスプロバイダーポータルを使用した Cisco Catalyst 8000V の展開](#) (84 ページ)
- [クラウドサービスプロバイダーポータルを使用した Cisco CSR 1000v の展開](#) (85 ページ)
- [Alibaba Cloud への Cisco Catalyst 8000V Edge ソフトウェアの展開](#) (85 ページ)
- [vEdge クラウドルータの展開](#) (87 ページ)

Cisco vManage ペルソナおよびストレージデバイス

Cisco vManage を展開すると、Cisco vManage のインストール後にサーバーが初めて起動するときに、Cisco vManage サーバーのペルソナ (Cisco vManage リリース 20.6.1 以降) とストレージデバイスを選択するように求められます。

Cisco vManage ペルソナ

Cisco vManage リリース 20.6.1 以降、各 Cisco vManage サーバーにはペルソナがあります。ペルソナは、サーバーで実行されるサービスを定義し、Cisco vManage クラスタ内でサーバーが持つ役割を定義します。Cisco vManage ペルソナの関連情報については、「Cisco vManage クラスタ」を参照してください。

Cisco vManage サーバー用に設定されたペルソナは変更できません。

Cisco vManage は次のペルソナをサポートします。

- **Compute + Data** : アプリケーション、統計、構成、メッセージング、および調整に使用されるサービスを含む、Cisco vManage に必要なすべてのサービスが含まれます。このペルソナは、スタンドアロンノード、および Cisco vManage クラスタ内の最初のノードに使用する必要があります。
- **Compute** : アプリケーション、構成、メッセージング、および調整に使用されるサービスが含まれます。このペルソナには、統計に使用されるサービスは含まれません。このペルソナを持つノードはスタンドアロンノードとして動作できず、Cisco vManage クラスタの一部である必要があります。
- **Data** : アプリケーションと統計に使用されるサービスのみが含まれます。このペルソナを持つノードはスタンドアロンノードとして動作できず、Cisco vManage クラスタの一部である必要があります。

Cisco vManage のインストール後にサーバーが初めて起動するときに、Cisco vManage サーバーのペルソナを選択するように求められます。このプロンプトはコマンドラインに次のように表示されます。

```
1) COMPUTE_AND_DATA
2) DATA
3) COMPUTE
Select persona for vManage (1, 2 or 3):
```

このプロンプトが表示されたら、**Compute+Data** ペルソナを選択する場合は 1 を入力し、**Compute** ペルソナを選択する場合は 2 を入力し、**Data** ペルソナを選択する場合は 3 を入力します。次に、選択の確認のために表示される **[Are you sure]** プロンプトで **[y]** を入力します。

サーバーに設定するペルソナを決定するときは、Cisco vManage クラスタが次のいずれかのノードの展開をサポートしていることに注意してください。

- 3 つの **Compute+Data** ノード
- 3 つの **Compute+Data** ノードと 3 つの **Data** ノード
- 3 つの **Compute** ノードと 3 つの **Data** ノード (既存の展開からのアップグレードでのみサポートされます)

ノードの異なる組み合わせが必要な場合は、シスコの代理店にお問い合わせください。

Cisco vManage ストレージデバイス

各 Cisco vManage サーバーには、ストレージデバイスが割り当てられています。ストレージデバイスは、Cisco vManage サーバーに接続され、データベースおよびその他の設定情報が保存される **/opt/data** パーティションを含むハードドライブです。

Cisco vManage のインストール後にサーバーが初めて起動するときに、Cisco vManage サーバーのストレージデバイスを選択するように求められます。ストレージデバイスをフォーマットするかどうか尋ねられます。

ストレージデバイスの割り当てプロンプトは、コマンドラインに次のように表示されます。

```
Available storage devices:
```

プロンプトに続いて、使用可能なストレージデバイスのリストが表示され、それぞれの前に番号が付いています。サーバーに使用するストレージデバイスに対応する番号を入力します。

ストレージデバイスを選択すると、ストレージデバイスをフォーマットするかどうかを尋ねるプロンプトが表示されます。[y]を入力してストレージデバイスをフォーマットするか、[n]を入力してフォーマットをスキップします。ストレージデバイスをフォーマットすると、デバイス上のすべてのデータが完全に削除されます。

稼働イベントシーケンス

エッジデバイスの稼働プロセス（すべてのデバイスの認証と検証、機能するオーバーレイネットワークの確立など）は、最小限のユーザー入力のみで実行されます。概念的な観点から見ると、稼働プロセスを2つの部分に分けることができます。1つはユーザー入力を必要とする部分で、もう一つは自動的に実行される部分です。

1. 最初の部分では、ネットワークを設計し、クラウドルータの仮想マシン（VM）インスタンスを作成し、ハードウェアルータを設置して起動します。次に、Cisco vManage で、ネットワークにルータを追加し、各ルータの設定を作成します。このプロセスについては、「[稼働シーケンスのユーザー部分の概要](#)」で説明します。
2. 稼働プロセスの2つ目の部分は、自動的に実行され、Cisco SD-WAN ソフトウェアによってオーケストレーションされます。ルータは、オーバーレイネットワークに参加すると、それら自体の検証と認証を自動的に実行し、相互にセキュアな通信チャネルを確立します。Cisco vBond オーケストレーションと Cisco vSmart コントローラ については、ネットワーク管理者が必要な認証関連ファイルを Cisco vManage からダウンロードする必要があり、その後、これらの Cisco vSmart コントローラ と Cisco vBond オーケストレーションが Cisco vManage からそれらの設定を自動的に受信します。vEdge クラウドルータ については、証明書署名要求（CSR）を生成し、受信した証明書をインストールしてから、証明書に含まれているシリアル番号を Cisco vManage にアップロードする必要があります。シスコのハードウェアルータは、起動すると、ネットワーク上で認証され、ゼロタッチプロビジョニング（ZTP）と呼ばれるプロセスを通じて Cisco vManage から自動的に設定を受信します。このプロセスについては、「[稼働シーケンスの自動部分](#)」で説明します。

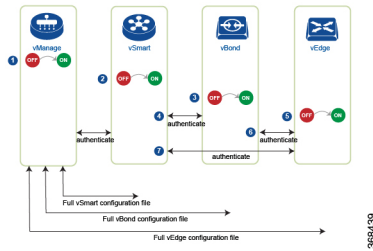
この2つの部分からなるプロセスの最終結果は、運用可能なオーバーレイネットワークです。

このトピックでは、稼働プロセスの実行中に発生するイベントシーケンスについて説明します。まずユーザー部分を説明し、次に自動認証およびデバイス検証の動作方法を説明します。

稼働プロセスのイベントシーケンス

機能的な観点から見ると、オーバーレイネットワークでルータを稼働させるタスクは、次の順序で実行されます。

図 1: 稼働イベントシーケンス



1. Cisco vManage ソフトウェアが、データセンター内のサーバーで起動します。
2. Cisco vBond オーケストレーションが、DMZ 内のサーバーで起動します。
3. Cisco vSmart コントローラが、データセンター内のサーバーで起動します。
4. Cisco vManage と Cisco vBond オーケストレーションが相互に認証し、Cisco vManage と Cisco vSmart コントローラが相互に認証し、Cisco vSmart コントローラ と Cisco vBond オーケストレーションが相互にセキュアに認証します。
5. Cisco vManage が、Cisco vSmart コントローラ と Cisco vBond オーケストレーションに設定を送信します。
6. ルータが、ネットワーク内で起動します。
7. ルータが、それ自体を Cisco vBond オーケストレーションで認証します。
8. ルータが、それ自体を Cisco vManage で認証します。
9. ルータが、それ自体を Cisco vSmart コントローラで認証します。
10. Cisco vManage が、ルータに設定を送信します。

稼働プロセスを開始する前に、次の点に注意してください。

- 最高レベルのセキュリティを実現するために、認証および許可されたルータのみが Cisco SD-WAN オーバーレイネットワークにアクセスして参加することができます。この目的のために、Cisco vSmart コントローラは、すべてのルータがネットワークを介してデータトラフィックを送信する前に、すべてのルータに対する自動認証を実行します。
- ルータが認証されると、ルータがプライベートアドレス空間（NATゲートウェイの後ろ）にあるかパブリックアドレス空間にあるかにかかわらず、データトラフィックフローが発生します。

Cisco SD-WAN オーバーレイネットワークでハードウェアおよびソフトウェアコンポーネントを稼働させるには、すべてのルータおよびその他のネットワーク ハードウェア コンポーネントを接続するトランスポートネットワーク（「トランスポートクラウド」とも呼ばれる）が使用可能である必要があります。通常、これらのコンポーネントは、データセンターおよびブランチオフィスにあります。トランスポートネットワークの唯一の目的は、ドメイン内のすべてのネットワークデバイスを接続することです。Cisco SD-WAN ソリューションは、トランスポートネットワークに依存しないため、任意のタイプ（インターネット、マルチプロトコルラ

ベルスイッチング (MPLS)、レイヤ2スイッチング、レイヤ3ルーティング、ロングタームエボリューション (LTE) など) またはトランスポートの任意の組み合わせにすることができます。

ハードウェアルータの場合は、Cisco SD-WAN ゼロタッチプロビジョニング (ZTP) SaaS を使用してルータを稼働させることができます。オーバーレイネットワークでハードウェアを起動するための自動プロセスの詳細については、「[ZTP用にルータを準備する](#)」を参照してください。

オーバーレイネットワークの起動手順

オーバーレイネットワークの起動

次の表に、Cisco vManage 使用してオーバーレイネットワークを起動するためのタスクを示します。

表 1:

起動タスク	ステップごとの手順
ステップ 1 : Cisco vManage を起動します。	<ol style="list-style-type: none"> 1. ハイパーバイザで、VM インスタンスを作成します。 2. Cisco vManage サーバーを起動し、VM を起動して、ログイン情報を入力します。 3. Cisco vManage メニューから、[Administration] > [Settings]の順に選択し、証明書認証設定を設定します。[Automated]を選択すると、コントローラデバイスの CSR の生成時に証明書生成プロセスが自動的に実行されます。 4. Cisco vManage メニューから、[Configuration] > [Certificates]の順に選択して CSR を生成します。 5. リクエストを受け取ったことを示すシマンテックからの確認メールを確認します。 6. Viptela がリクエストを承認し、証明書が署名されたことを示すシマンテックからの電子メールを確認します。 7. Cisco vManage メニューから、[Configuration] > [Devices]の順に選択し、証明書がインストールされているか確認します。

起動タスク	ステップごとの手順
ステップ 2 : Cisco vBond オーケストレーションを起動します。	<ol style="list-style-type: none"> 1. ハイパーバイザで、VM インスタンスを作成します。 2. vBond サーバーを起動し、VM を起動します。 3. Cisco vManage メニューから、[Configuration] > [Devices] > [Controllers] の順に選択し、Cisco vBond オーケストレーションを追加して CSR を生成します。 4. リクエストを受け取ったことを示すシマンテックからの確認メールを確認します。 5. Viptela がリクエストを承認し、証明書が署名されたことを示すシマンテックからの電子メールを確認します。 6. Cisco vManage メニューから、[Configuration] > [Devices] の順に選択し、証明書がインストールされているか確認します。 7. Cisco vManage メニューから、[Configuration] > [Templates] の順に選択します。 <ol style="list-style-type: none"> 1. Cisco vBond オーケストレーションの構成テンプレートを作成します。 2. テンプレートを Cisco vBond オーケストレーションに添付します。 8. Cisco vManage メニューから、[Monitor] > [Overview] の順に選択し、Cisco vBond オーケストレーションが動作していることを確認します。 Cisco vManage リリース 20.6.x 以前 : Cisco vManage メニューから、[Dashboard] > [Main Dashboard] の順に選択し、Cisco vBond オーケストレーションが動作していることを確認します。

起動タスク	ステップごとの手順
ステップ3 : Cisco vSmart コントローラを起動します。	<ol style="list-style-type: none"> 1. ハイパーバイザで、VM インスタンスを作成します。 2. vSmart サーバーを起動し、VM を起動します。 3. Cisco vManage メニューから、[Configuration] > [Devices] > [Controller]の順に選択し、Cisco vSmart コントローラを追加してCSRを生成します。 4. リクエストを受け取ったことを示すシマンテックからの確認メールを確認します。 5. Viptelaがリクエストを承認し、証明書が署名されたことを示すシマンテックからの電子メールを確認します。 6. Cisco vManage メニューから、[Configuration] > [Devices]の順に選択し、証明書がインストールされていることを確認します。 7. Cisco vManage メニューから、[Configuration] > [Templates]の順に選択します。 <ol style="list-style-type: none"> 1. Cisco vSmart コントローラの構成テンプレートを作成します。 2. テンプレートをCisco vSmart コントローラに添付します。 8. Cisco vManage メニューから、[Monitor] > [Overview]の順に選択し、Cisco vSmart コントローラが動作していることを確認します。 Cisco vManage リリース 20.6.x 以前 : Cisco vManage メニューから、[Dashboard] > [Main Dashboard]の順に選択し、Cisco vSmart コントローラが動作していることを確認します。

起動タスク	ステップごとの手順
ステップ 4：ルータを設定します。	<ol style="list-style-type: none"> 1. Cisco vManage メニューから、[Configuration] > [Devices] > [WAN Edge List]の順に選択し、ルータ認定シリアル番号ファイルをアップロードします。 2. Cisco vManage メニューから、[Configuration] > [Certificates] > [WAN Edge List]の順に選択し、ルータのシャーシ番号とシリアル番号がリストにあることを確認します。 3. Cisco vManage メニューから、[Configuration] > [Certificates] > [WAN Edge List]の順に選択し、[Validity]列で[Valid]とマークして各ルータを認証します。 4. Cisco vManage メニューから、[Configuration] > [Certificates] > [WAN Edge List]の順に選択し、WAN エッジリストをコントローラデバイスに送信します。 5. Cisco vManage メニューから、[Configuration] > [Templates]の順に選択します。 <ol style="list-style-type: none"> 1. ルータの構成テンプレートを作成します。 2. テンプレートをルータに添付します。
ステップ 5：AC 電源を接続し、ハードウェアルータを起動します。	<ol style="list-style-type: none"> 1. AC 電源をルータに接続します。 2. 必要に応じて、ルータの背面にあるオン/オフスイッチをオンの位置に切り替えます。 3. Cisco vManage メニューから、[Monitor] > [Overview]を選択するか、[Monitor] > [Devices] > [Device Dashboard]の順に選択して、ルータが動作していることを確認します。 Cisco vManage リリース 20.6.x 以前：Cisco vManage メニューから、[Dashboard] > [Main Dashboard]を選択するか、[Monitor] > [Network] > [Device Dashboard]の順に選択して、ルータが動作していることを確認します。

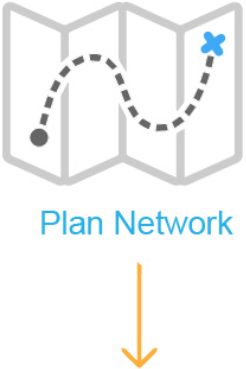
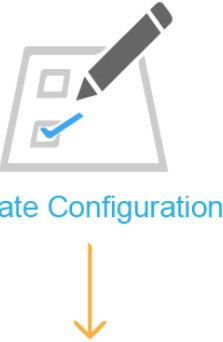
稼働シーケンスのユーザー部分の概要


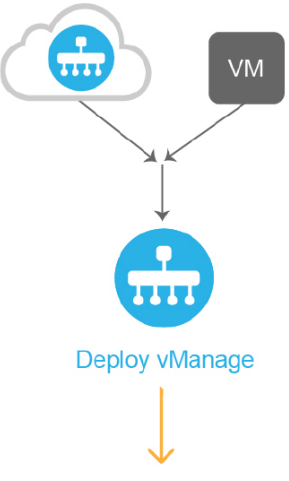
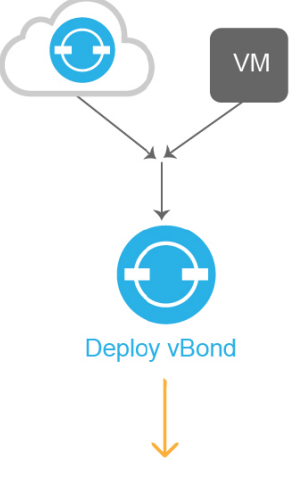
一般に、Cisco SD-WAN オーバーレイネットワークを起動するために実行する作業は、ネットワークを起動するための作業です。ネットワークを計画し、デバイス構成を作成してから、ネットワークハードウェアおよびソフトウェアコンポーネントを展開します。展開するコンポーネントには、すべての Cisco vEdge デバイス、オーバーレイネットワークに参加するすべての従来のルータ、およびオーバーレイネットワーク全体で共有サービス（ファイアウォール、ロードバランサ、IDP システムなど）を提供するすべてのネットワークデバイスが含まれます。

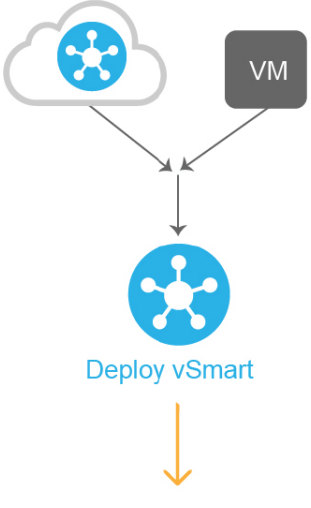
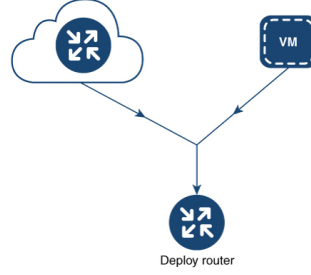
次の表に、Cisco SD-WAN オーバーレイネットワークの稼働シーケンスのユーザー部分における手順の概要を示します。各手順の詳細については、「手順」列に示されている手順のリンク先を参照してください。Cisco vEdge デバイスは任意の順序で起動できますが、以下に記載されている順序で展開することを推奨します。これは、デバイスがデバイス自体を検証および認証する機能的な順序です。

ネットワークにファイアウォールデバイスがある場合は、「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。

表 2:

	ワークフロー	手順
1	 Plan Network	オーバーレイネットワークを計画します。「Cisco SD-WAN ソリューションのコンポーネント」を参照してください。
2	 Create Configuration	紙上で、必要なアーキテクチャと機能を実装するデバイス構成を作成します。ソフトウェアリリースのソフトウェアドキュメントを参照してください。

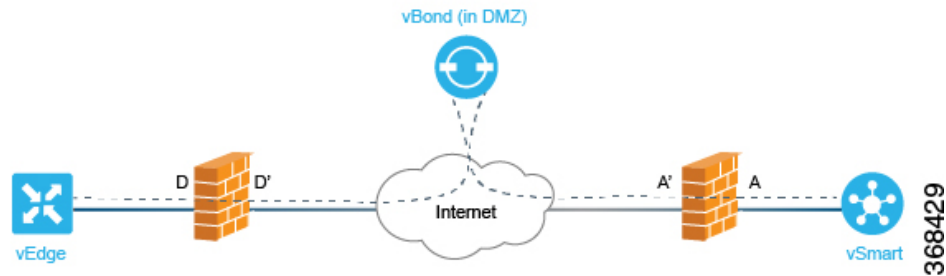
	ワークフロー	手順
3	 <p style="text-align: right; font-size: small;">368184</p>	<p>ソフトウェアイメージをダウンロードします。</p>
4	 <p style="text-align: right; font-size: small;">368185</p>	<p>データセンターに Cisco vManage を展開します。</p> <ol style="list-style-type: none"> 1. ESXi または KVM ハイパーバイザのいずれかで Cisco vManage VM インスタンスを作成します。 2. Cisco vManage サーバーごとに最小構成または完全な構成を作成します。 3. 証明書の設定を設定し、Cisco vManage の証明書を生成します。 4. Cisco vManage クラスタを作成します。
5	 <p style="text-align: right; font-size: small;">368186</p>	<p>Cisco vBond オーケストレーションを導入します。</p> <ol style="list-style-type: none"> 1. ESXi または KVM ハイパーバイザのいずれかで Cisco vBond オーケストレーション VM インスタンスを作成します。 2. Cisco vBond オーケストレーションの最小構成を作成します。 3. Cisco vBond オーケストレーションをオーバーレイネットワークに追加します。このプロセス中に、Cisco vBond オーケストレーションの証明書を生成します。 4. Cisco vBond オーケストレーションの完全な構成を作成します。

ワークフロー	手順
<p>6</p>  <p style="text-align: right; font-size: small;">908187</p>	<p>データセンターに Cisco vSmart コントローラ を展開します。</p> <ol style="list-style-type: none"> 1. ESXi または KVM ハイパーバイザのいずれかで Cisco vSmart コントローラ VM インスタンスを作成します。 2. Cisco vSmart コントローラ の最小構成を作成します。 3. Cisco vSmart コントローラ をオーバーレイネットワークに追加します。このプロセス中に、Cisco vSmart コントローラ の証明書を生成します。 4. Cisco vSmart コントローラ の完全な構成を作成します。
<p>7</p>  <p style="text-align: right; font-size: small;">908188</p>	<p>オーバーレイネットワークに Cisco vEdge ルータを展開します。</p> <ol style="list-style-type: none"> 1. ソフトウェア vEdge クラウドルータ の場合、AWS サーバー、あるいは ESXi または KVM ハイパーバイザのいずれかで VM インスタンスを作成します。 2. ソフトウェア vEdge クラウドルータ の場合、証明書署名要求をシマンテック社に送信し、署名済み証明書をルータにインストールします。 3. Cisco vManage から、すべての Cisco vEdge ルータのシリアル番号をオーバーレイネットワーク内の Cisco vSmart コントローラ および Cisco vBond オーケストレーションに送信します。 4. Cisco vEdge ルータの完全な構成を作成します。

起動シーケンスの自動部分

Cisco vEdge デバイスが起動し、初期構成で稼働を開始すると、起動プロセスの 2 番目の部分が自動的に開始されます。この自動プロセスは、Cisco vBond オーケストレーションによって導かれます。次の図を参照してください。Cisco vBond オーケストレーション ソフトウェアのリーダーシップの下で、Cisco vEdge デバイスはデバイス間で暗号化された通信チャンネルを設定します。これらのチャンネルを介して、デバイス間の検証と認証が自動的に実行され、動作可能なオーバーレイネットワークが確立されます。オーバーレイネットワークが稼働すると、Cisco vEdge デバイスは Cisco vManage サーバーから完全な構成を自動的に受信してアクティブ化します。（Cisco vManage は例外です。各 Cisco vManage サーバー自体を手動で構成する必要があります）。

図 2: Cisco vBond Orchestrator 自動起動シーケンス



次のセクションでは、起動プロセスの自動部分の間に、内部で実行される内容について説明します。この説明は、Cisco SD-WAN ソフトウェアの詳細な動作の理解に役立つように提供されており、ネットワーク要件をサポートするための高度に安全なオーバーレイフレームワークを Cisco SD-WAN ソリューションが作成する手段を十分に理解できます。

ZTP 自動認証プロセスに必要なユーザー入力

稼働プロセスの実行中に発生する Cisco vEdge デバイスの自動検証および認証は、Cisco vSmart コントローラと Cisco vBond オーケストレーションが、ネットワークで許可されているデバイスのシリアル番号およびシャーシ番号を認識している場合にのみ行われます。まず、これらの 2 つの用語を定義します。

- シリアル番号：各 Cisco vEdge デバイスにシリアル番号があります。これは、デバイスの証明書に含まれる 40 バイトの番号です。Cisco vBond オーケストレーションおよび Cisco vSmart コントローラの場合、証明書は Symantec またはエンタープライズルート CA によって提供されます。vEdge ルータの場合、証明書はハードウェアの信頼できるボード ID チップで提供されます。
- シャーシ番号：シリアル番号に加えて、各 vEdge ルータはシャーシ番号によって識別されます。vEdge ルータは唯一の Cisco SD-WAN 製造ハードウェアであるため、シャーシ番号を持つのは Cisco vEdge デバイスのみです。vEdge ルータのシリアル番号とそのシャーシ番号の間には 1 対 1 のマッピングが存在します。

Cisco vSmart コントローラおよび Cisco vBond オーケストレーションは、次のデバイスの初期構成中にシリアル番号とシャーシ番号を学習します。

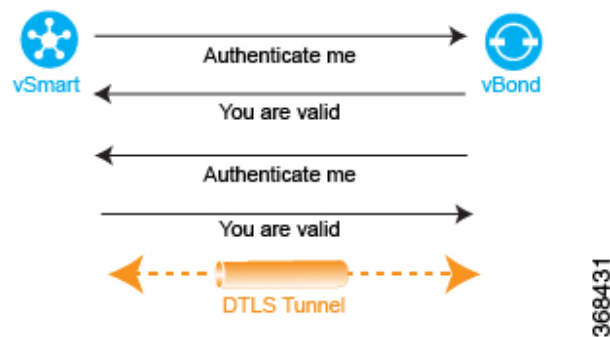
- vSmart 認定シリアル番号：Cisco vManage は、CSR を作成して署名付き証明書をインストールするときに、ネットワーク内に存在することが許可されているすべての Cisco vSmart コントローラのシリアル番号を学習します。これらのシリアル番号を Cisco vBond オーケストレーションにダウンロードすると、Cisco vBond オーケストレーションは、それらを自動認証プロセス中に Cisco vSmart コントローラにプッシュします。
- vEdge 認定シリアル番号ファイル：このファイルには、ネットワーク内に存在することが許可されているすべての vEdge ルータのシリアル番号とシャーシ番号が含まれています。このファイルを Cisco vBond オーケストレーションおよび Cisco vSmart コントローラにアップロードします。

自動検証および認証の手順は、デバイスのシリアル番号およびシャーシ番号に加えて、各デバイスに同じ組織名が設定されているかどうかによって異なります。Cisco vManage でこの名前を設定すると、すべてのデバイスの構成ファイルに含まれます。組織名は、1つの組織に属するすべてのデバイスで同一である必要があります（名前は大文字と小文字が区別されます）。組織名は、Cisco SD-WAN またはエンタープライズルート CA によって作成される各デバイスの証明書にも含まれます。

Cisco vSmart コントローラ と Cisco vBond オーケストレーション の間の認証

機能の観点からは、相互に検証および認証する Cisco SD-WAN オーバーレイネットワーク上の最初の2つのデバイスは Cisco vSmart コントローラ と Cisco vBond オーケストレーション です。このプロセスは、Cisco vSmart コントローラ によって開始されます。

図 3: Cisco vSmart コントローラ と Cisco vBond Orchestrator の認証



Cisco vSmart コントローラ は、起動すると、Cisco vBond オーケストレーション への接続を開始します。それにより、Cisco vBond オーケストレーション が Cisco vSmart コントローラ について学習します。これらの2つのデバイスは、自動的に双方向の認証プロセスを開始します

(Cisco vSmart コントローラ はそれ自体を Cisco vBond オーケストレーション で認証し、Cisco vBond オーケストレーション はそれ自体を Cisco vSmart コントローラ で認証します)。認証プロセスにおける2つのデバイス間の双方向ハンドシェイクは、並行して行われます。ただし、分かりやすくするために、この図には認証手順の概要が示されており、ハンドシェイクが順次的に表現されています。認証ハンドシェイクが成功すると、Cisco vSmart コントローラ デバイスと Cisco vBond オーケストレーション デバイスの間に永続的な DTLS 通信チャネルが確立されます。認証手順のいずれかが失敗すると、失敗を通知しているデバイスが2つのデバイス間の接続を切断し、認証の試行が終了します。

設定時にプロビジョニングするパラメータの一つが Cisco vBond オーケストレーション の IP アドレスまたは DNS 名であるため、Cisco vSmart コントローラ は Cisco vBond オーケストレーション に到達する方法を認識しています。次の理由から、Cisco vBond オーケストレーション は、Cisco vSmart コントローラ からのリクエストに応答する準備が整っています。

- この情報が Cisco vBond オーケストレーション の構成に含まれているため、その役割が認証システムになることであると認識しています。

- vSmart 認定シリアル番号を Cisco vManage から Cisco vBond オーケストレーション にダウンロードしています。

Cisco vSmart コントローラ が認証プロセスを開始するときに、Cisco vBond オーケストレーションがまだ起動していない場合、Cisco vSmart コントローラ は、試行が成功するまで定期的に接続の開始を試みます。

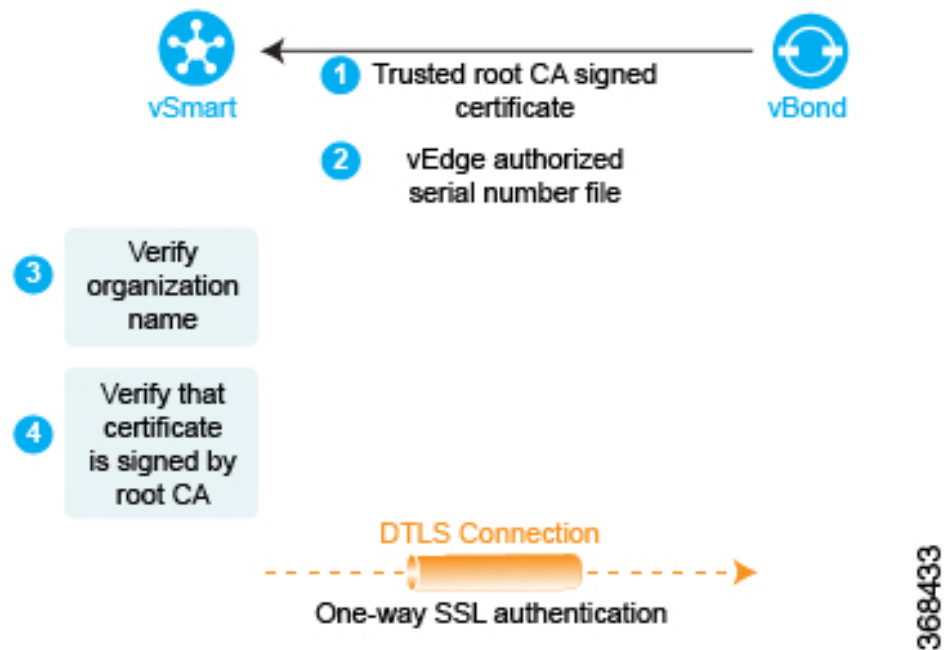
以下では、Cisco vSmart コントローラ と Cisco vBond オーケストレーション の間で自動認証がどのように行われるかについて、詳しくステップバイステップで説明します。

Cisco vSmart コントローラ と Cisco vBond オーケストレーション の間でセッションを開始するために、Cisco vSmart コントローラ が Cisco vBond オーケストレーション への暗号化された DTLS 接続を開始します。暗号化は RSA によって提供されます。各デバイスは、起動時に RSA の秘密キーと公開キーのペアを自動生成します。

この暗号化されたチャンネルを介して、Cisco vSmart コントローラ と Cisco vBond オーケストレーション が相互に認証します。各デバイスは、並行して他方のデバイスを認証します。分かりやすくするために、Cisco vBond オーケストレーション の Cisco vSmart コントローラ 認証から説明します。

1. Cisco vBond オーケストレーション は信頼できるルート CA 署名付き証明書を vSmart コントローラ に送信します。
2. Cisco vBond オーケストレーション は vEdge 認定シリアル番号ファイルを vSmart コントローラ に送信します。
3. Cisco vSmart コントローラ は、信頼のチェーンを使用して証明書から組織名を抽出し、それを Cisco vSmart コントローラ に設定されている組織名と比較します。2つの組織名が一致する場合、Cisco vSmart コントローラ は、Cisco vBond オーケストレーション の組織が適切であると認識します。組織名が一致しない場合、Cisco vSmart コントローラ は DTLS 接続を切断します。
4. Cisco vSmart コントローラ は、ルート CA チェーンを使用して、証明書が実際にルート CA (Symantec またはエンタープライズ CA) によって署名されていることを確認します。署名が正しい場合、Cisco vSmart コントローラ は証明書自体が有効であることを認識します。署名が正しくない場合、Cisco vSmart コントローラ は DTLS 接続を切断します。

図 4: Cisco vSmart コントローラが Cisco vBond Orchestrator を認証

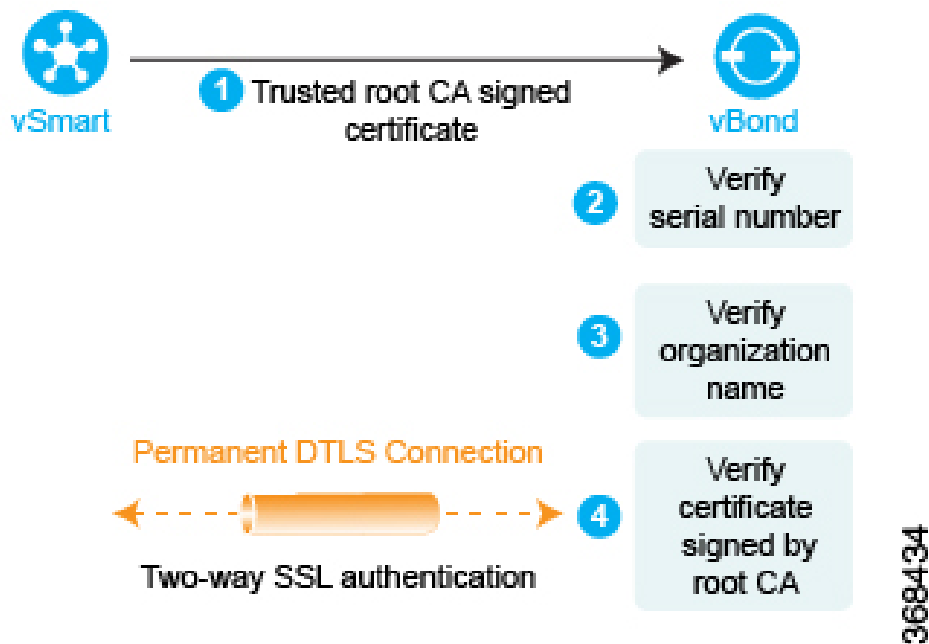


この2つのチェックを実行すると、Cisco vBond オークストレーションの Cisco vSmart コントローラ 認証が完了します。

反対方向では、Cisco vBond オークストレーションが Cisco vSmart コントローラ を認証しません。

1. Cisco vSmart コントローラ は信頼できるルート CA 署名付き証明書を Cisco vBond オークストレーションに送信します。
2. Cisco vBond オークストレーションは、信頼のチェーンを使用して証明書から Cisco vSmart コントローラ のシリアル番号を抽出します。シリアル番号は、vSmart 認定シリアル番号ファイルの番号の1つと一致する必要があります。一致しない場合、Cisco vBond オークストレーションは DTLS 接続を切断します。
3. Cisco vBond オークストレーションは、信頼のチェーンを使用して証明書から組織名を抽出し、それを Cisco vBond オークストレーションに設定されている組織名と比較します。2つの組織名が一致する場合、vBond Orchestrator は Cisco vSmart コントローラの組織が適切であると認識します。組織名が一致しない場合、Cisco vBond オークストレーションは DTLS 接続を切断します。
4. vBond Orchestrator は、ルート CA チェーンを使用して、証明書が実際にルート CA (Symantec またはエンタープライズ CA) によって署名されていることを確認します。署名が正しい場合、Cisco vBond オークストレーションは証明書自体が有効であることを認識します。署名が正しくない場合、Cisco vBond オークストレーションは DTLS 接続を切断します。

図 5: Cisco vBond Orchestrator が Cisco vSmart コントローラを認証



この3つのチェックを実行すると、Cisco vSmart コントローラの Cisco vBond オーケストレーション認証が完了します。

2つのデバイス間の双方向認証が完了すると、Cisco vBond オーケストレーションと Cisco vSmart コントローラ 間の DTLS 接続が一時的な接続から永続的な接続に移行し、2つのデバイスはその接続を介して OMP セッションを確立します。

冗長性のために複数の Cisco vSmart コントローラがあるドメインでは、このプロセスが vSmart デバイスと vBond デバイスの各ペア間で繰り返されます。Cisco vSmart コントローラは、Cisco vBond オーケストレーションと連携して、互いについて学習し、ルート情報を同期させます。可用性を高めるために、異なる vSmart コントローラを、異なる NAT デバイスを介して WAN ネットワークに接続することをお勧めします。

Cisco vBond オーケストレーションには、ネットワークトポロジ内の Cisco vSmart コントローラの数と同じ数の永続的な DTLS 接続しかありません。これらの DTLS 接続は、ネットワークのコントロールプレーンの一部であり、データトラフィックがそれらを介して送信されることはありません。すべての Cisco vSmart コントローラが Cisco vBond オーケストレーションに登録されると、Cisco vBond オーケストレーションおよび Cisco vSmart コントローラは Cisco SD-WAN ネットワーク内の vEdge ルータを検証および認証できる状態になっています。

Cisco vSmart コントローラ 間の認証

複数の Cisco vSmart コントローラがあるドメインでは、OMP ルートを同期するために、コントローラ間で永続的な DTLS 接続のフルメッシュを確立できるように、コントローラを相互認証する必要があります。Cisco vSmart コントローラは Cisco vBond オーケストレーションから相手の Cisco vSmart コントローラの IP アドレスを学習します。

Cisco vSmart コントローラは、vBond Orchestrator との認証ハンドシェイク中に、vSmart 認証シリアル番号ファイルのコピーを受信した場合、ネットワーク上に他の Cisco vSmart コントローラが存在する可能性について学習します。このファイルに複数のシリアル番号が含まれている場合、ある時点で、ネットワークに複数の Cisco vSmart コントローラが存在した可能性を示しています。

1つの Cisco vSmart コントローラが Cisco vBond オーケストレーションで認証されると、Cisco vBond オーケストレーションは Cisco vSmart コントローラに認証されている他 Cisco vSmart コントローラの IP アドレスを送信します。Cisco vBond オーケストレーションは後で別の Cisco vSmart コントローラを学習すると、そのコントローラのアドレスをすでに認証されている他の Cisco vSmart コントローラに送信します。

次に、Cisco vSmart コントローラは以下の手順を実行して相互に認証します。再び、各デバイスは並行して他のデバイスを認証しますが、わかりやすくするために、プロセスを順番に説明します。

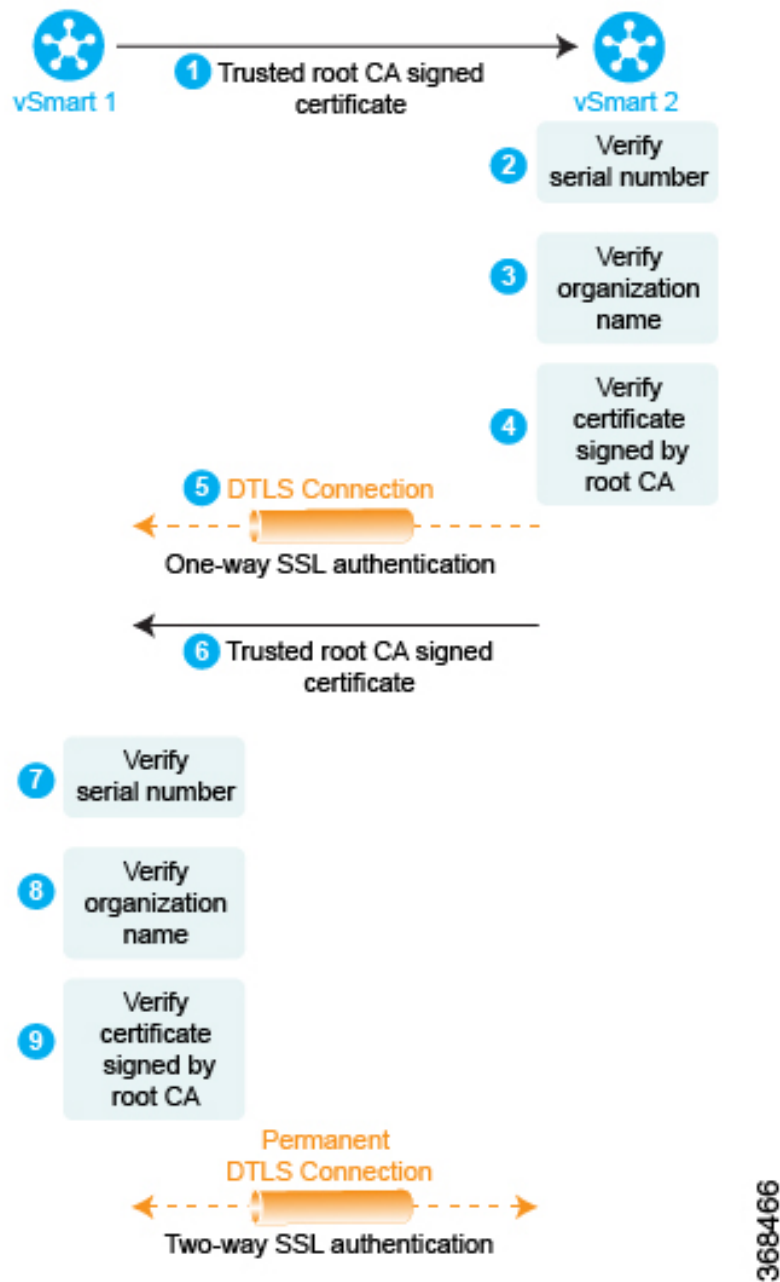
1. vSmart1 は、vSmart2 への暗号化された DTLS 接続を開始し、信頼できるルート CA 署名付き証明書を vSmart2 に送信します。
2. vSmart2 は、その信頼チェーンを使用して vSmart1 のシリアル番号を抽出します。シリアル番号は、vSmart 認証シリアル番号ファイルの番号の1つと一致する必要があります。一致しない場合、vSmart2 は DTLS 接続を切断します。
3. vSmart2 は、その信頼チェーンを使用して証明書から組織名を抽出し、ローカルに設定された組織名と比較します。2つの組織名が一致する場合、vSmart2 は、vSmart1 の組織が適切であると認識します。組織名が一致しない場合、vSmart2 は DTLS 接続を切断します。
4. vSmart2 は、ルート CA チェーンを使用して、証明書が実際にルート CA（シマンテックまたはエンタープライズ CA）によって署名されていることを確認します。署名が正しい場合、vSmart2 は証明書自体が有効であることを認識します。署名が正しくない場合、vSmart2 は DTLS 接続を切断します。

この3つのチェックを実行すると、vSmart1 の vSmart2 認証が完了します。

これで、vSmart1 は vSmart2 を認証するので、前述の同じ手順を実行します。

1. まず、vSmart2 は、その信頼できるルート CA 署名付き証明書を vSmart1 に送信します。
2. vSmart1 は、その信頼チェーンを使用して vSmart2 のシリアル番号を抽出します。シリアル番号は、vSmart 認証シリアル番号ファイルの番号の1つと一致する必要があります。一致しない場合、vSmart1 は DTLS 接続を切断します。
3. vSmart1 は、その信頼チェーンを使用して証明書から組織名を抽出し、ローカルに設定された組織名と比較します。2つの組織名が一致する場合、vSmart2 は、vSmart2 の組織が適切であると認識します。組織名が一致しない場合、vSmart1 は DTLS 接続を切断します。
4. vSmart1 は、ルート CA チェーンを使用して、証明書が実際にルート CA（シマンテックまたはエンタープライズ CA）によって署名されていることを確認します。署名が正しい場合、vSmart2 は証明書自体が有効であることを認識します。署名が正しくない場合、vSmart1 は DTLS 接続を切断します。

図 6: Cisco vSmart コントローラの認証



この3つのチェックを実行すると、vSmart2のvSmart1認証が完了し、2つのデバイス間の一時的なDTLS接続が永続的になります。

すべてのCisco vSmartコントローラがCisco vBondオーケストレーションに登録されると、Cisco vBondオーケストレーションおよびCisco vSmartコントローラはCisco SD-WANネットワーク内のvEdgeルータを検証および認証できる状態になっています。

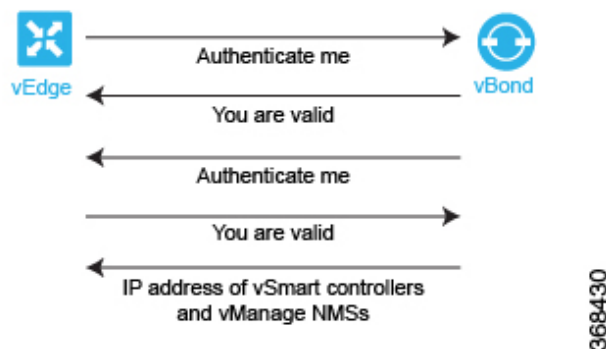
Cisco vBond オーケストレーション と Cisco vEdge ルータの間の認証

ネットワークに Cisco vEdge ルータを展開する場合、最初に次の2つのことを行う必要があります。

- Cisco vManage とのセキュアな接続を確立して、完全な構成を受信できるようにします。
- Cisco vSmart コントローラ とのセキュアな接続を確立して、Cisco SD-WAN オーバーレイネットワークへの参加を開始できるようにします。

Cisco vEdge デバイスは、起動すると、Cisco vManage と Cisco vSmart コントローラ を自動検出し、接続を確立します。その際、Cisco vBond オーケストレーションの助けを借ります。Cisco vEdge ルータの初期構成には、vBond システムの IP アドレス（または DNS 名）が含まれます。この情報を使用して、Cisco vEdge ルータは Cisco vBond オーケストレーション との DTLS 接続を確立します。2つのデバイスは相互に認証して、それらが有効な Cisco vEdge デバイスであることを確認します。繰り返しになりますが、この認証は自動的に行われる双方向プロセスです。認証が正常に完了すると、Cisco vBond オーケストレーションは、Cisco vEdge ルータに Cisco vManage と Cisco vSmart コントローラの IP アドレスを送信します。その後、Cisco vEdge ルータは、Cisco vBond オーケストレーション との接続を切断し、他の2つのデバイスとのセキュアな DTLS 接続の確立を開始します。

図 7: Cisco vEdge ルータと Cisco vBond Orchestrator の自動認証



Cisco vEdge ルータを起動し、初期構成を手動で実行すると、Cisco vBond オーケストレーションの検索が自動的に開始されます。Cisco vBond オーケストレーションと Cisco vSmart コントローラは、それらに Cisco vEdge 認証済みデバイスリストファイルがインストールされていることもあり、Cisco vEdge ルータを認識して認証することができます。

Cisco vEdge ルータを起動した後、初期構成を手動で実行し、少なくとも Cisco vBond オーケストレーションの DNS 名または IP アドレスを設定します。Cisco vEdge ルータは、このアドレス情報を使用して Cisco vBond オーケストレーションに到達します。次の理由により、Cisco vBond オーケストレーションは、Cisco vEdge ルータからの要求に応答する準備ができています。

- この情報が vBond の初期構成に含まれているため、その役割が認証システムになるとして認識しています。

- 初期構成の一部として、Cisco vEdge 認定シリアル番号ファイルが Cisco vBond オーケストレーションにインストールされています。

Cisco vEdge ルータが認証プロセスを開始するときに、Cisco vBond オーケストレーションがまだ起動していない場合、Cisco vEdge ルータは、試行が成功するまで定期的に接続の開始を試みます。

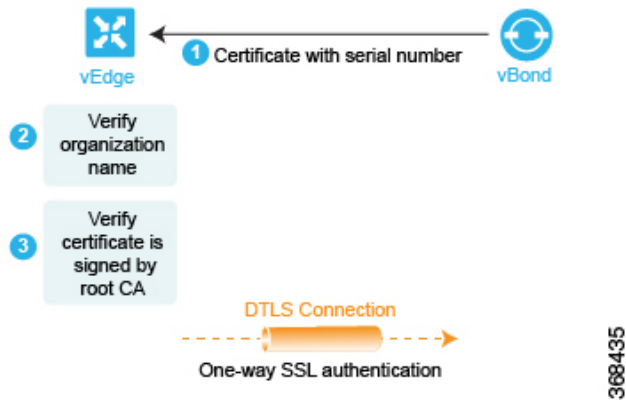
以下では、Cisco vBond オーケストレーションと Cisco vEdge ルータの間に自動認証がどのように行われるかについて、詳しくステップバイステップで説明します。

まず、Cisco vEdge ルータは、Cisco vBond オーケストレーションのパブリック IP アドレスへの暗号化された DTLS 接続を開始します。暗号化は RSA によって提供されます。各デバイスは、起動時に RSA 秘密キーと公開キーのペアを自動的に生成します。Cisco vBond オーケストレーションは、Cisco vEdge ルータの元のインターフェイスアドレスを受信し、受信したパケットの外部 IP アドレスを使用して、Cisco vEdge ルータが NAT の背後にあるかどうかを判断します。その場合、Cisco vBond オーケストレーションは Cisco vEdge ルータのパブリック IP アドレスとポートのプライベート IP アドレスへのマッピングを作成します。

この暗号化された DTLS チャンネルを介して、Cisco vEdge ルータと Cisco vBond オーケストレーションの相互認証に進みます。他のデバイス認証と同様に、Cisco vEdge ルータと Cisco vBond オーケストレーションの相互認証は並行して処理されます。Cisco vEdge ルータが Cisco vBond オーケストレーションをどのように認証するか説明から議論を開始します。

1. Cisco vBond オーケストレーションは信頼できるルート CA 署名付き証明書を Cisco vEdge ルータに送信します。
2. Cisco vEdge ルータは、信頼のチェーンを使用して証明書から組織名を抽出し、それをルータ自体に設定されている組織名と比較します。2つの組織名が一致する場合、Cisco vEdge ルータは Cisco vBond オーケストレーションの組織が適切であると認識します。それらが一致しない場合、Cisco vEdge ルータは DTLS 接続を切断します。
3. Cisco vEdge ルータは、ルート CA チェーンを使用して、証明書が実際にルート CA（シマンテックまたはエンタープライズ CA）によって署名されていることを確認します。署名が正しい場合、Cisco vEdge ルータは証明書自体が有効であることを認識します。署名が正しくない場合、Cisco vEdge ルータは DTLS 接続を切断します。

図 8 : Cisco vEdge ルータが Cisco vBond Orchestrator を認証

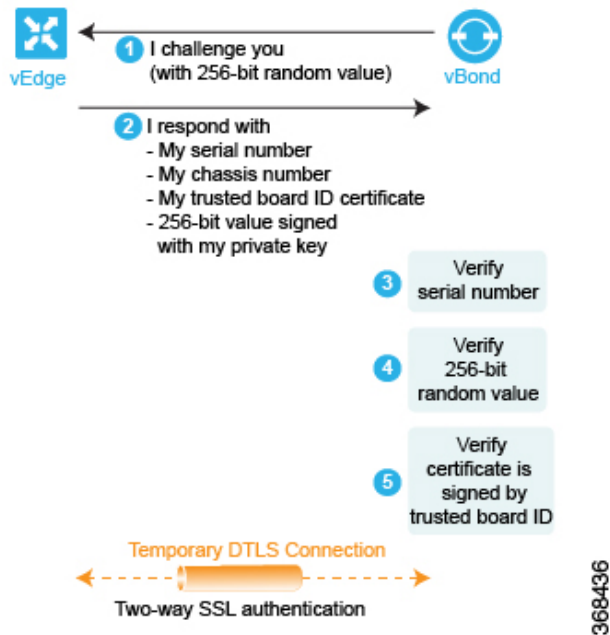


これらの2つのチェックを実行した後、Cisco vEdge ルータは Cisco vBond オーケストレーションが有効であることを認識し、Cisco vBond オーケストレーションの認証が完了します。

反対方向では、Cisco vBond オーケストレーションが Cisco vEdge ルータを認証します。

1. Cisco vBond オーケストレーションは Cisco vEdge ルータにチャレンジを送信します。チャレンジは 256 ビットのランダム値です。
2. Cisco vEdge ルータは、次の内容を含むチャレンジへの応答を送信します。
 - Cisco vEdge のシリアル番号
 - Cisco vEdge のシャシー番号
 - Cisco vEdge のボード ID 証明書
 - Cisco vEdge ルータの秘密キーによって署名された 256 ビットのランダム値
3. Cisco vBond オーケストレーションは、シリアル番号とシャシー番号を Cisco vEdge 認証済みデバイスリストファイルのリストと比較します。数値は、ファイル内の数値ペアのいずれかと一致する必要があります。一致しない場合、Cisco vBond オーケストレーションは DTLS 接続を切断します。
4. Cisco vBond オーケストレーションは 256 ビットのランダム値の署名が適切であることを確認します。これは、ルータのボード ID 証明書から抽出する Cisco vEdge ルータの公開キーを使用して行います。署名が正しくない場合、Cisco vBond オーケストレーションは DTLS 接続を切断します。
5. Cisco vBond オーケストレーションは、Cisco vEdge ルータのボード ID 証明書からのルート CA チェーンを使用して、ボード ID 証明書自体が有効であることを検証します。証明書が有効でない場合、Cisco vBond オーケストレーションは DTLS 接続を切断します。

図 9: Cisco vBond Orchestrator が Cisco vEdge ルータを認証



これらの3つのチェックを実行した後、Cisco vBond オーケストレーションはCisco vEdge ルータが有効であることを認識し、ルータの認証が完了します。

双方向認証が成功すると、Cisco vBond オーケストレーションは、オーケストレーションの最終ステップを実行し、メッセージをCisco vEdge ルータとCisco vSmart コントローラに同時に送信します。Cisco vEdge ルータにCisco vBond オーケストレーションが次のものを送信します。

- Cisco vEdge ルータがネットワーク内のCisco vSmart コントローラへの接続を開始することを可能にする、それらのIPアドレス。このアドレスは、パブリックIPアドレスか、NAT ゲートウェイの背後にあるコントローラの場合は、パブリックおよびプライベートIPアドレスとポート番号のリストです。Cisco vEdge ルータがNAT ゲートウェイの背後にある場合、Cisco vBond オーケストレーションは、Cisco vEdge ルータがCisco vSmart コントローラとのセッションを開始することを要求します。
- ネットワークへの参加が承認されているCisco vSmart コントローラのシリアル番号。

Cisco vSmart コントローラにCisco vBond オーケストレーションが次のものを送信します。

- ドメイン内の新しいCisco vEdge ルータを通知するメッセージ。
- Cisco vEdge ルータがNAT ゲートウェイの背後にある場合、Cisco vBond オーケストレーションは、Cisco vSmart コントローラにCisco vEdge ルータとセッションを開始することの要求を送信します。

その後、Cisco vEdge ルータは、Cisco vBond Orchestrator とのDTLS 接続を切断します。

Cisco vEdge ルータと Cisco vManage 間の認証

Cisco vEdge ルータと Cisco vBond オーケストレーションの相互認証の後、Cisco vEdge ルータは、Cisco vManage との DTLS 接続を介して完全な設定を受け取ります。

1. Cisco vEdge ルータは Cisco vManage との DTLS 接続を確立します。
2. Cisco vManage サーバーは設定ファイルを Cisco vEdge ルータに送信します。
3. Cisco vEdge ルータが設定ファイルを受信すると、その完全な設定をアクティブ化します。
4. Cisco vEdge ルータは Cisco vSmart コントローラ へのプレフィックスのアドバタイズを開始します。

Cisco vManage を使用していない場合は、Cisco vEdge ルータにログインして、その設定ファイルを手動でロードするか、手動でルータを設定します。

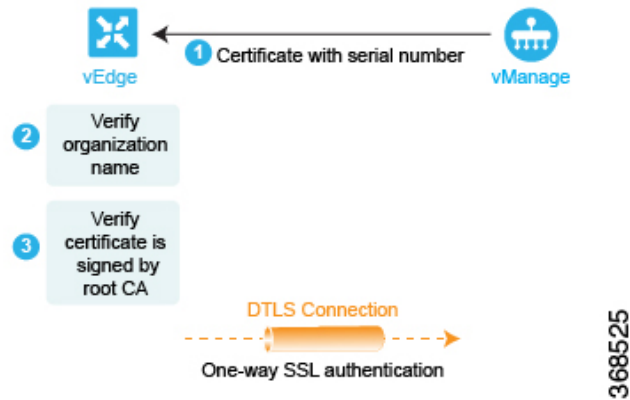
以下では、Cisco vEdge ルータと Cisco vManage の間で自動認証がどのように行われるかについて、詳しくステップバイステップで説明します。

まず、Cisco vEdge ルータは、Cisco vManage の IP アドレスへの暗号化された DTLS 接続を開始します。暗号化は RSA によって提供されます。各デバイスは、起動時に RSA 秘密キーと公開キーのペアを自動的に生成します。Cisco vManage は、Cisco vEdge ルータの元のインターフェイスアドレスを受信し、受信したパケットの外部 IP アドレスを使用して、Cisco vEdge ルータが NAT の背後にあるかどうかを判断します。その場合、Cisco vManage は Cisco vEdge ルータのパブリック IP アドレスとポートのプライベート IP アドレスへのマッピングを作成します。

この暗号化された DTLS チャンネルを介して、Cisco vEdge ルータと Cisco vManage の相互認証に進みます。他のデバイス認証と同様に、Cisco vEdge ルータと Cisco vManage の相互認証は並行して処理されます。Cisco vEdge ルータが Cisco vManage をどのように認証するか説明から議論を開始します。

1. Cisco vManage は信頼できるルート CA 署名付き証明書を Cisco vEdge ルータに送信します。
2. Cisco vEdge ルータは、信頼のチェーンを使用して証明書から組織名を抽出し、それをルータ自体に設定されている組織名と比較します。2つの組織名が一致する場合、Cisco vEdge ルータは Cisco vManage の組織が適切であると認識します。それらが一致しない場合、Cisco vEdge ルータは DTLS 接続を切断します。
3. Cisco vEdge ルータは、ルート CA チェーンを使用して、証明書が実際にルート CA（シマンテックまたはエンタープライズ CA）によって署名されていることを確認します。署名が正しい場合、Cisco vEdge ルータは証明書自体が有効であることを認識します。署名が正しくない場合、Cisco vEdge ルータは DTLS 接続を切断します。

図 10: Cisco vEdge ルータによる Cisco vManage の認証

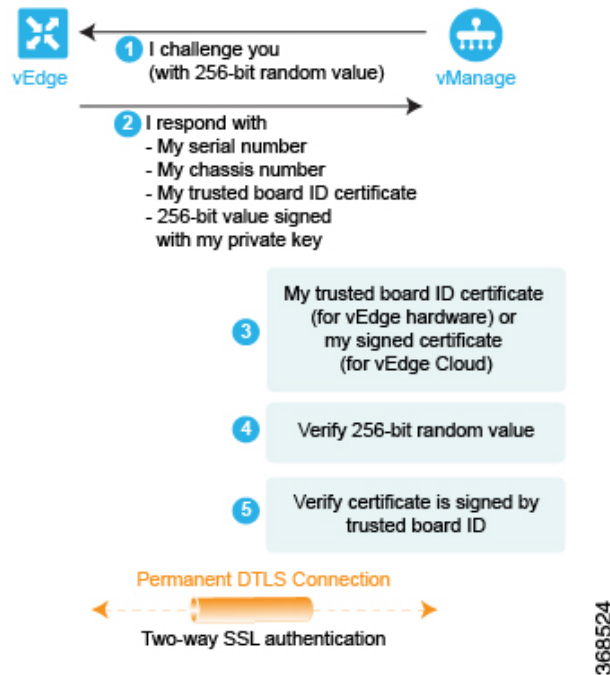


これらの2つのチェックを実行した後、Cisco vEdge ルータは Cisco vManage が有効であることを認識し、Cisco vManage の認証が完了します。

反対方向では、Cisco vManage が Cisco vEdge ルータを認証します。

1. Cisco vManage は Cisco vEdge ルータにチャレンジを送信します。チャレンジは 256 ビットのランダム値です。
2. Cisco vEdge ルータは、次の内容を含むチャレンジへの応答を送信します。
 - Cisco vEdge のシリアル番号
 - Cisco vEdge のシャーシ番号
 - Cisco vEdge ボード ID 証明書（ハードウェア Cisco vEdge ルータの場合）または署名付き証明書（Cisco vEdge Cloud ルータの場合）
 - Cisco vEdge ルータの秘密キーによって署名された 256 ビットのランダム値
3. Cisco vManage は、シリアル番号とシャーシ番号を Cisco vEdge 認証済みデバイスリストファイルのリストと比較します。数値は、ファイル内の数値ペアのいずれかと一致する必要があります。一致しない場合、Cisco vManage vManage NMS は DTLS 接続を切断します。
4. Cisco vManage は 256 ビットのランダム値の署名が適切であることを確認します。これは、ルータのボード ID 証明書から抽出する Cisco vEdge ルータの公開キーを使用して行います。署名が正しくない場合、Cisco vManage は DTLS 接続を切断します。
5. Cisco vManage は、Cisco vEdge ルータのボード ID 証明書からのルート CA チェーンを使用して、ボード ID 証明書自体が有効であることを検証します。証明書が有効でない場合、Cisco vManage は DTLS 接続を切断します。

図 11 : Cisco vManage による Cisco vEdge ルータの認証



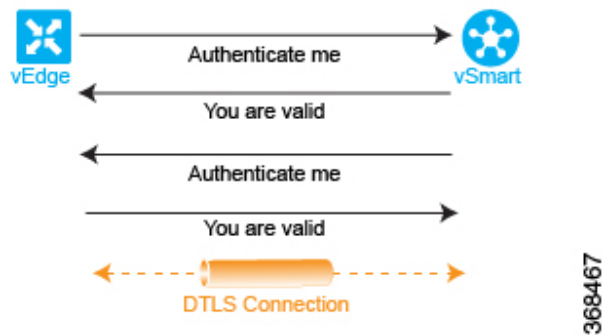
これらの3つのチェックを実行した後、Cisco vManage は Cisco vEdge ルータが有効であることを認識し、ルータの認証が完了します。

双方向認証が成功すると、Cisco vManage サーバーは設定ファイルを Cisco vEdge ルータに送信します。Cisco vEdge ルータが設定ファイルを受信すると、その完全な設定をアクティブ化し、Cisco vSmart コントローラ へのプレフィックスのアドバタイズを開始します。

Cisco vSmart コントローラ と Cisco vEdge ルータの間の認証

自動認証プロセスの最後のステップは、Cisco vSmart コントローラ と Cisco vEdge ルータが相互に認証することです。このステップでは、Cisco vSmart コントローラ が認証を実行して Cisco vEdge ルータがそのネットワークに属していることを確認し、Cisco vEdge ルータも Cisco vSmart コントローラ を認証します。認証が完了すると、2つのデバイス間の DTLS 接続が永続的になり、Cisco vSmart コントローラ が、DTLS 接続を介して実行される OMP ピアリングセッションを確立します。その後、Cisco vEdge ルータは、Cisco SD-WAN オーバーレイネットワークを介したデータトラフィックの送信を開始します。

図 12: Cisco vSmart コントローラ と Cisco vEdge ルータの認証



ここでは、Cisco vSmart コントローラ と Cisco vEdge ルータの間で自動認証がどのように行われるかについて、詳しくステップバイステップで説明します。

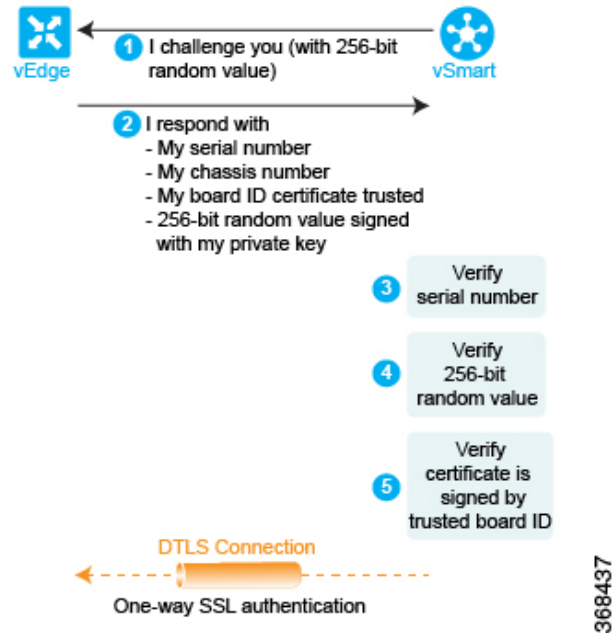
Cisco vSmart コントローラ と Cisco vEdge ルータの間でセッションを開始するために、2つのデバイス的一方が他方への暗号化された DTLS 接続を開始します。暗号化は RSA によって提供されます。各デバイスは、起動時に RSA の秘密キーと公開キーのペアを自動生成します。

Cisco vSmart コントローラ と Cisco vEdge ルータの間の認証は、並行して行われる双方向プロセスです。以降で、Cisco vSmart コントローラ が Cisco vEdge ルータを認証する方法について説明します。

1. Cisco vSmart コントローラ は Cisco vEdge ルータにチャレンジを送信します。チャレンジは 256 ビットのランダム値です。
2. Cisco vEdge ルータは、次の内容を含むチャレンジへの応答を送信します。
 - Cisco vEdge のシリアル番号
 - Cisco vEdge のシャーシ番号
 - Cisco vEdge のボード ID 証明書
 - Cisco vEdge ルータの秘密キーによって署名された 256 ビットのランダム値
3. Cisco vSmart コントローラ は、シリアル番号とシャーシ番号を Cisco vEdge 認証済みデバイスリストファイルのリストと比較します。数値は、ファイル内の数値ペアのいずれかと一致する必要があります。一致しない場合、Cisco vSmart コントローラ は DTLS 接続を切断します。
4. Cisco vSmart コントローラ は 256 ビットのランダム値の署名が適切であることを確認します。これは、ルータのボード ID 証明書から抽出する Cisco vEdge ルータの公開キーを使用して行います。署名が正しくない場合、Cisco vSmart コントローラ は DTLS 接続を切断します。
5. Cisco vSmart コントローラ は、Cisco vEdge ルータのボード ID 証明書からのルート CA チェーンを使用して、ボード ID 証明書自体が有効であることを検証します。証明書が有効でない場合、Cisco vSmart コントローラ は DTLS 接続を切断します。

6. Cisco vSmart コントローラ は、応答を元のチャレンジと比較します。Cisco vBond オーケストレーション が発行したチャレンジと応答が一致する場合、2つのデバイス間で認証が行われます。それ以外の場合は、Cisco vSmart コントローラ が DTLS 接続を切断します。

図 13: Cisco vSmart コントローラ が Cisco vEdge ルータを認証

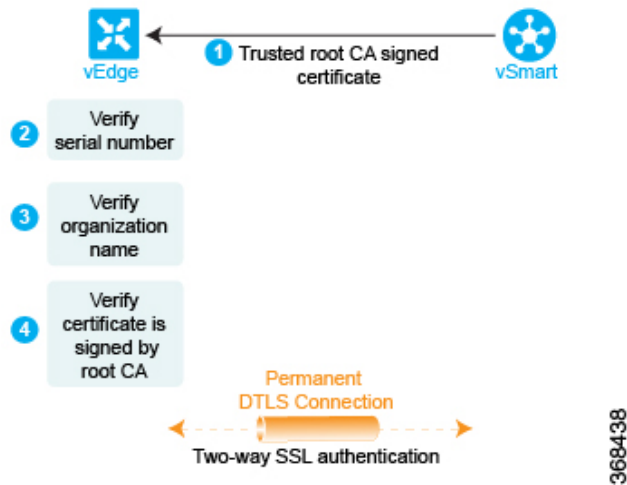


これらの3つのチェックを実行した後、Cisco vSmart コントローラ は Cisco vEdge ルータが有効であることを認識し、ルータの認証が完了します。

反対方向では、Cisco vEdge ルータが Cisco vSmart コントローラ を認証します。

1. Cisco vSmart コントローラ は信頼できるルート CA 署名付き証明書を Cisco vEdge ルータに送信します。
2. Cisco vEdge ルータは、信頼のチェーンを使用して証明書から Cisco vSmart コントローラのシリアル番号を抽出します。シリアル番号は、vSmart 認定シリアル番号ファイルの番号の1つと一致する必要があります。一致しない場合、Cisco vEdge ルータは DTLS 接続を切断します。
3. Edge ルータは、信頼のチェーンを使用して証明書から組織名を抽出し、それを Cisco vEdge ルータに設定されている組織名と比較します。2つの組織名が一致する場合、Cisco vEdge ルータは Cisco vSmart コントローラ の組織が適切であると認識します。それらが一致しない場合、Cisco vEdge ルータは DTLS 接続を切断します。
4. Cisco vEdge ルータは、ルート CA チェーンを使用して、証明書が実際にルート CA (シマンテックまたはエンタープライズ CA) によって署名されていることを確認します。署名が正しい場合、Cisco vEdge ルータは証明書自体が有効であることを認識します。署名が正しくない場合、Cisco vEdge ルータは DTLS 接続を切断します。

図 14: Cisco vEdge ルータが Cisco vSmart コントローラを認証



この3つのチェックを実行すると、Cisco vSmart コントローラの Cisco vEdge 認証が完了します。認証に使用される DTLS 接続は永続的な（一時的ではない）接続になり、2つのデバイスは、コントロールプレーントラフィックの交換に使用される、その接続を介した OMP セッションを確立します。

この認証手順は、オーバーレイネットワークに導入する Cisco vSmart コントローラ ごとおよび Cisco vEdge ルータごとに繰り返されます。

ネットワーク内の各 Cisco vEdge ルータは、少なくとも1つの Cisco vSmart コントローラ に接続する必要があります。つまり、各 Cisco vEdge ルータと1つ Cisco vSmart コントローラ の間に DTLS 接続が正常に確立されている必要があります。Cisco SD-WAN ネットワークにはドメインの概念があります。ドメイン内では、冗長性のために複数の Cisco vSmart コントローラ を使用することをお勧めします。その後、各 Cisco vEdge ルータは複数の Cisco vSmart コントローラ に接続できます。

OMP セッションを介して、Cisco vEdge ルータはさまざまなコントロールプレーン関連情報を Cisco vSmart コントローラ にリレーして、Cisco vSmart コントローラ がネットワークトポロジを学習できるようにします。

- Cisco vEdge ルータは、ローカルの静的および動的（BGP と OSPF）ルーティングプロトコルから学習したサービス側のプレフィックスとルートをアドバタイズします。
- 各 Cisco vEdge ルータには、TLOC（トランスポートロケーション）と呼ばれるトランスポートアドレスがあります。これは、WAN トランスポートネットワーク（インターネットなど）または NAT ゲートウェイ（WAN トランスポートに接続）に接続するインターフェイスのアドレスです。Cisco vEdge ルータと Cisco vSmart コントローラ の間で DTLS 接続が確立されると、OMP は TLOC を Cisco vSmart コントローラ に登録します。
- Cisco vEdge ルータは、サービス側ネットワークにあるすべてのサービス（ファイアウォールや侵入検知デバイスなど）の IP アドレスをアドバタイズします。

Cisco vSmart コントローラは、これらの OMP ルートをそのルーティングデータベースにインストールし、それらを Cisco SD-WAN オーバーレイネットワーク内の他の Cisco vEdge ルータにアドバタイズします。また、Cisco vSmart コントローラは、ネットワーク内の他の Cisco vEdge ルータから学習した OMP ルート情報で Cisco vEdge ルータを更新します。Cisco vSmart コントローラは、受信したルートおよびプレフィックスをルーティングテーブルにインストールする前に、それらにインバウンドポリシーを適用でき、ルーティングテーブルからルートをアドバタイズする前にアウトバウンドポリシーを適用できます。

Cisco SD-WAN 展開のためのファイアウォールレポート

この記事では、Cisco SD-WAN デバイスが使用するポートについて説明します。ネットワークにファイアウォールデバイスがある場合は、Cisco SD-WAN オーバーレイネットワーク内のデバイスがトラフィックを交換できるように、ファイアウォールでこれらのポートを開く必要があります。

Cisco SD-WAN 固有のポートの用語

デフォルトでは、すべての Cisco vEdge デバイスがベースポート 12346 を使用して接続を確立し、オーバーレイネットワークでの制御とトラフィックを処理します。各デバイスは、このポートを使用して他の Cisco vEdge デバイスに接続します。

ポートオフセット

複数の Cisco vEdge デバイスが 1 つの NAT デバイスの背後に配置されている場合は、デバイスごとに異なるポート番号を設定できます。これにより、NAT は、個別のデバイスをそれぞれ正確に識別できます。これを実行するには、ベースポート 12346 からのポートオフセットを設定します。たとえば、デバイスで 1 のポートオフセットを設定すると、そのデバイスはポート 12347 を使用します。ポートオフセットには、0 ~ 19 の値を指定できます。デフォルトのポートオフセットは 0 です。

NAT の背後にあるデバイスを区別できる NAT デバイスの場合、ポートオフセットを設定する必要はありません。

ポートホッピング

Cisco SD-WAN オーバーレイネットワークのコンテキストでは、ポートホッピングというプロセスがあり、デバイスが最初のポートでの接続試行に失敗すると、異なるポートで相互接続の確立を試みます。このような失敗の後、ポート値がインクリメントされ、接続が再試行されます。ソフトウェアは、接続試行ごとに待機時間を延長しながら、合計 5 つのベースポートを巡回します。

ポートオフセットを設定していない場合、デフォルトのベースポートは 12346 であり、ポートホッピングはポート 12346、12366、12386、12406、および 12426 の間で順次実行され、その後ポート 12346 に戻ります。

ポートオフセットを設定している場合は、その初期ポート値が使用され、次のポートは 20 ずつインクリメントされます。たとえば、オフセットが 2 に設定されているポートの場合、ポー

トホッピングはポート 12348、12368、12388、12408、および 12428 の間で順次実行され、その後ポート 12348 に戻ります。

ポートを 20 ずつインクリメントすることで、可能なベースポート番号が重複しないようになります。

Cisco vEdge デバイスは、Cisco vManage、Cisco vBond オーケストレーション、および Cisco vSmart コントローラ への接続を確立しようと試みるときにポートホッピングを使用します。Cisco vEdge デバイスにポートホッピングを手動で要求することもできます。

Cisco vSmart コントローラ および Cisco vManage インスタンスは通常、適切に動作する NAT デバイスの背後にインストールされるため、一般的にはポートホッピングは必要なく、これらのデバイスで発生することはありません。

Cisco vBond オーケストレーションは常にポート 12346 を使用して他の Cisco vEdge デバイスに接続します。ポートホッピングは使用されません。

デフォルトのベースポートが 12346 である Cisco vEdge デバイスの例を使用して、ポートホッピングがどのように機能するかを説明します。ルータが別の Cisco vEdge デバイス ルータへの接続を試みたにも関わらず、一定の時間内に接続できなかった場合、ルータは次のベースポートにホップし、そのポートで接続を確立しようとします。



- (注) ポートホップはデフォルト設定であるため、デバイスは Cisco vBond オーケストレーションに新しい制御接続を要求します。新しい制御接続が確立されると、エッジデバイスはピアへの TLOC 更新情報の送信を開始します。制御接続が不安定な間に TLOC 更新メッセージが失われる可能性があり、デバイスとピア間の IPSec セキュリティアソシエーションが同期しなくなると、その結果として BFD セッションが失敗します。

この問題を回避するため、データセンターのデバイスではポートホップまたは静的エントリを設定しないことをお勧めします。以下のコマンドで IP の順序を変更することで、すべてのエッジを単一の Cisco vBond オーケストレーションに接続するか、2 つの Cisco vBond オーケストレーション間でエッジのバランスをとることができます。

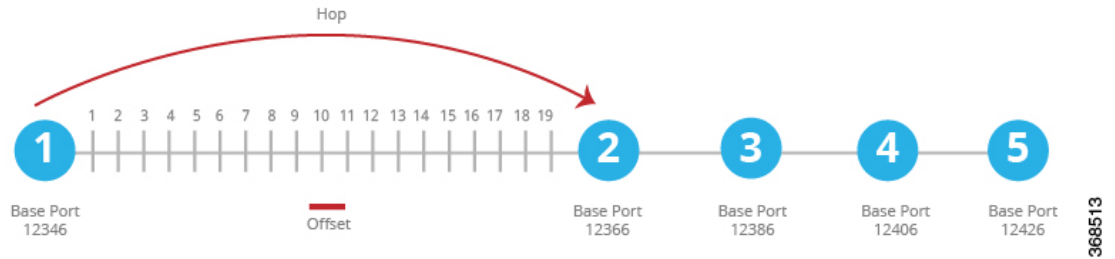
静的エントリの場合、次のコマンドでデータセンターのデバイスの IP アドレスを設定できます。

```
system
  vbond <vBond FQDN>
  vpn 0
  host <vBond FQDN> ip <vBond ip1> <vBond ip2>
```

ポートホッピングを設定しないように選択した場合は、次のコマンドを使用します。

```
system
  no port-hop
```

図 15: Cisco vEdge デバイスのポートホッピングの例



最初のベースポートでの初回接続試行が約 1 分経過しても成功しない場合、ルータはポート 12366 にホップします。約 2 分後、ルータはポート 12386 にホップします。約 5 分後、ポート 12406 にホップします。約 6 分後、ポート 12426 にホップします。その後、サイクルは最初のポートである 12346 に戻ります。

フルコン NAT デバイスでは、特定の Cisco vEdge デバイスによって開始されたすべての接続のソースポートは、Cisco vEdge デバイスによって開始されたすべてのセッションで一貫性を保ちます。たとえば、ルータがパブリックソースポート 12346 でセッションを開始する場合、このポートがすべての通信に使用されます。

ポートホッピングの効果

Cisco vEdge デバイスは、ポートホッピングを使用して、オーバーレイネットワークのコントロールプレーンを稼働状態に保つためにあらゆる試みを行います。コントローラデバイス（Cisco vBond オーケストレーション、Cisco vManage、または Cisco vSmart コントローラ）が何らかの理由でダウンし、Cisco vEdge デバイスが稼働したままになっている場合、コントローラデバイスが復旧すると、そのデバイスと Cisco vEdge デバイスの間の接続がシャットダウンして再起動する可能性があり、場合によっては、Cisco vEdge デバイスがシャットダウンして再起動します。この動作は、ポートホッピングが原因で発生します。つまり、あるデバイスが別のデバイスへの制御接続を失うと、接続を再確立しようとして、別のポートへのポートホッピングを実行します。

次の 2 つの例は、これが発生する可能性のある状況を示しています。

- Cisco vBond オーケストレーションがクラッシュすると、Cisco vManage は、Cisco vEdge デバイスへのすべての接続をダウンさせる可能性があります。発生するイベントの順序は次のとおりです：Cisco vBond オーケストレーションがクラッシュすると、Cisco vManage がすべての制御接続を失うか閉じる可能性があります。次に、Cisco vManage が、ポートホッピングを実行して、別のポートでの Cisco vSmart コントローラへの接続確立を試みます。Cisco vManage でのこのポートホッピングにより、Cisco vEdge デバイスへの制御接続を含むすべての制御接続がシャットダウンし、再起動します。
- すべての Cisco vSmart コントローラでのすべての制御セッションがダウンし、Cisco vEdge デバイスでの BFD セッションは稼働したままになります。Cisco vSmart コントローラのいずれかが稼働状態に戻ると、ルータの BFD セッションがダウンしてから稼働状態に戻ります。これは、Cisco vEdge デバイスが、Cisco vSmart コントローラへの再接続の試みにおいて、すでに別のポートへのポートホッピングを実行しているためです。



- (注) Cisco vSmart コントローラの **graceful-restart timers** を変更すると、**port-hop** が有効になっているかどうかに関係なく、OMP ピアのフラッピングが発生します。Cisco vSmart コントローラの **graceful-restart timers** は、冗長 Cisco vSmart コントローラ ピアリングで変更するか（一度に1つの Cisco vSmart コントローラ 構成のみを変更）、データプレーンの中断を許容できるメンテナンス期間中に変更することをお勧めします。

Cisco vEdge デバイス が使用するポート

Cisco vEdge デバイスは、オーバーレイネットワークに参加すると、コントローラデバイス（Cisco vBond オーケストレーション、Cisco vManage、および Cisco vSmart コントローラ）との DTLS コントロールプレーン接続を確立します。ルータは、これらの制御接続を使用して、Cisco vBond オーケストレーションから Cisco vSmart コントローラの場所を学習し、その構成を Cisco vManage から受信して、そのポリシーとポリシーの更新を Cisco vSmart コントローラから受信します。これらの DTLS 接続を最初に確立するとき、Cisco vEdge デバイスはベースポート 12346 を使用します。このベースポートを使用して接続を確立できない場合は、3つのコントローラデバイスとの DTLS 接続が正常に確立するまで、ポート 12366、12386、12406、および 12426 を介してポートホッピングが実行され、必要に応じて 12346 に戻ります。この同じポート番号が、オーバーレイネットワーク内の他の Cisco vEdge デバイス への IPSec 接続および BFD セッションを確立するために使用されます。vEdge 構成にポートオフセットが含まれている場合は、ベースポート番号と4つの後続のポート番号が、設定されたオフセットによって増分されることに注意してください。

DTLS と BFD が制御接続とデータ接続に使用しているポートを確認するには、**show control local-properties** コマンドの出力の [Private Port] 列を調べます。このコマンド出力には、インターフェイスが使用しているパブリックポート番号も示されます。Cisco vEdge デバイスの WAN ポートが NAT デバイスに接続されていない場合、プライベートポート番号とパブリックポート番号は同じです。NAT デバイスが存在する場合、[Public Port] 列にリストされているポート番号は、NAT デバイスによって使用されているポート番号であり、BFD が使用しているポートです。このパブリックポート番号は、リモート Cisco vEdge デバイスがローカルサイトにトラフィックを送信するために使用する番号です。

NAT デバイスが存在する場合、[Public Port] 列にリストされているポート番号は、NAT デバイスおよび BFD によって使用されます。このパブリックポート番号は、トラフィックをローカルサイトに送信するためにリモート Cisco vEdge デバイスによって使用されます。

ファイアウォールデバイスのあるネットワークでは、ファイアウォールデバイスの Cisco SD-WAN ベースポートを開いて、トラフィックがオーバーレイネットワークを通過できるようにする必要があります。ネットワーク内の Cisco vEdge デバイス が使用する可能性のあるすべてのベースポートを開きます。これらは、デフォルトのベースポートと、ルータによるポートホッピングが可能な4つのベースポートです。



- (注) 通常、ポートホッピングは Cisco vSmart コントローラ および Cisco vManage では必要ありません。

SD-WAN デバイス接続用の DTLS、TLS、および IPSec ポートの詳細については、「ファイアウォールポートの考慮事項」を参照してください。<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html#FirewallPortConsiderations>

UDP を使用する DTLS トンネルを使用するように設定された Cisco vEdge デバイスでは、少なくとも、デフォルトのポートオフセットが 0 の Cisco vEdge デバイスで使用される 5 つのベースポートを開く必要があります。具体的には、次のポートを開きます。

- ポート 12346
- ポート 12366
- ポート 12386
- ポート 12406
- ポート 12426

いずれかの Cisco vEdge デバイス でポートオフセット値を設定した場合は、ポートオフセット値で設定されたポートを開く必要もあります。

- ポート (12346 + ポートオフセット値)
- ポート (12366 + ポートオフセット値)
- ポート (12386 + ポートオフセット値)
- ポート (12406 + ポートオフセット値)
- ポート (12426 + ポートオフセット値)

複数の vCPU を実行している Cisco SD-WAN デバイスで使用されるポート

Cisco vSmart コントローラは、最大 8 つの仮想 CPU (vCPU) を備えた仮想マシン (VM) で実行できます。Cisco vManage は最小 16 個の vCPU に設定でき、8 個の vCPU が接続ポートの制御に使用されます。vCPU は、Core0 ~ Core7 として指定されます。

各コアには、制御接続用に個別のベースポートが割り当てられます。ベースポートは、接続が DTLS トンネル (UDP を使用) または TLS トンネル (TCP を使用) のどちらを経由しているかによって異なります。



- (注) Cisco vBond オーケストレーションは複数のコアをサポートしていません。Cisco vBond オーケストレーションは常に DTLS トンネルを使用して、他の Cisco vEdge デバイス と制御接続を確立するため、常に UDP を使用します。UDP ポートは 12346 です。

次の表に、Cisco vManage の各 vCPU コアが使用するポートを示します。オフセットが設定されている場合、各ポートは設定されたポートオフセットによって増分されます。

コア番号	DTLS (UDP) のポート	TLS (TCP) のポート
Core0	12346	23456
Core1	12446	23556
Core2	12546	23656
Core3	12646	23756
Core4	12746	23856
Core5	12846	23956
Core6	12946	24056
Core7	13046	24156

Cisco vManage によって使用される管理ポート

Cisco vManage は、プロトコル固有の通信に次の管理ポートを使用します。

目的	トラフィックの方向	プロトコル	ポート番号
Netconf	双方向 Cisco vManage と Cisco vSmart コントローラまたは Cisco vBond オーケストレーションの間。このポートは、Cisco vManage で最初の検出を確立するために使用されます。	TCP	830
HTTPS	着信	TCP	443
SNMP クエリー	着信	UDP	161
SSH	着信 コントローラ間で DTLS/TLS 接続がまだ形成されていない場合、Cisco vManage は SCP を使用して署名付き証明書をコントローラ上にインストールします。SSH は TCP 宛先ポート 22 を使用します。	TCP	22
RADIUS	発信	UDP	1812
SNMP トラップ	発信	UDP	162
Syslog	発信	UDP	514

目的	トラフィックの方向	プロトコル	ポート番号
TACACS	発信	TCP	49

vManage クラスタは、クラスタを構成する NMS 間の通信に次のポートを使用します。

vManage サービス	トラフィックの方向	Protocol	ポート番号
アプリケーションサーバー	双方向	TCP	80、443、7600、8080、8443、57600
コンフィギュレーションデータベース	双方向	TCP	2424、2434、5000、7474、7687
調整サーバー	双方向	TCP	2181、2888、3888
メッセージバス	双方向	TCP	4222、6222、8222
統計データベース	双方向	TCP	9200、9300
デバイス構成のトラッキング (NCS および NETCONF)	双方向	TCP	830
Cloud Agent	双方向	TCP	8553
SD-AVC	双方向	TCP	10502、10503
Cloud Agent V2	双方向	TCP	50051

ポートオフセットの設定

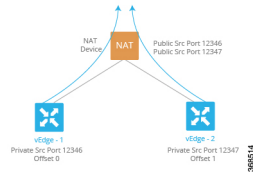
2 つ以上の Cisco vEdge デバイス が同じフルコーン NAT デバイスの背後にある場合、1 つのデバイスはデフォルトのポートオフセットを使用できますが、残りのデバイスではポートオフセットを設定する必要があります。

```
Device(config)# system port-offset number
```

ポートオフセットには、0 ～ 19 の値を指定できます。デフォルトのポートオフセットは 0 です。

次の例では、vEdge-1 はデフォルトのポートオフセット 0 を使用しており、vEdge-2 ではポートオフセットが 1 に設定されています。

図 16: ポートオフセット設定の例



この例では、次のようになります。

- vEdge-1 は、最初にベースポート 12346 を使用して接続を試みます。接続できなかった場合、ルータはポート 12366、12386、12406、および 12426 で接続を試みます。
- vEdge-2 のポートオフセットは 1 であるため、接続を試みる最初のポートは 12347（12346 にオフセット 1 を加えた番号）です。ポート 12347 を使用した接続に失敗した場合、ルータは 20 ずつホップし、ポート 12367、12387、12407、および 12427 で接続を試みます。

ポートホッピングの手動実行

Cisco vEdge デバイスにポートホッピングを手動で要求できます。

```
vEdge# request port-hop
```

このコマンドを使用する理由の一つは、ルータの制御接続は稼働しているが、BFD が起動していない場合です。request port-hop コマンドにより、次のポート番号で制御接続が再開し、BFD も起動します。

ソフトウェアのダウンロード

Cisco SD-WAN ソフトウェアは [Cisco Software Download](#) サイトからダウンロードできます。

Cisco SD-WAN ソフトウェアをダウンロードするための直接リンクは [こちら](#) です。

以下のコンポーネントと、Cisco SD-WAN のインストールに必要なその他のソフトウェアをダウンロードします。Cisco SD-WAN コントローラは、サーバー上の仮想マシンとして動作します。

コンポーネント	注
Cisco vBond オーケストレーション	Cisco vBond オーケストレーションが Cisco vEdge Cloud デバイスとして展開されているため、ダウンロードページに vEDGE Cloud として表示されます。
Cisco vManage	ダウンロードページに vManage ソフトウェアとして表示されます。
Cisco vSmart コントローラ	ダウンロードページに vSmart ソフトウェアとして表示されません。

Cisco vManage の導入

Cisco vManage は、オーバーレイネットワーク内のすべての Cisco vEdge デバイス およびリンクを容易にモニタ、設定、および維持するための GUI インターフェイスを提供する、集中型ネットワーク管理システムです。Cisco vManage は、ネットワークサーバー上で仮想マシン (VM) として実行されます。

SD-WAN オーバーレイネットワークは単一の Cisco vManage で管理することも、少なくとも 3 つの Cisco vManage インスタンスで構成されるクラスターで管理することもできます。ネットワーク (特に大規模なネットワーク) の場合、vManage クラスターで構築することをお勧めします。Cisco vManage は、オーバーレイネットワーク内のすべての Cisco vEdge デバイスを管理し、ダッシュボードとデバイス操作の詳細ビューを提供し、デバイス設定と証明書を制御します。

Cisco vManage インスタンスを展開するには、次の手順を実行します。

1. ESXi または KVM ハイパーバイザのいずれかで vManage VM インスタンスを作成します。
2. Cisco vManage インスタンスごとに最小限の設定または完全な設定を作成します。デバイス設定テンプレートを作成して Cisco vManage を設定することも、SSH を使用して CLI セッションを開き、その後 Cisco vManage を手動で設定することもできます。設定を手動で作成し、後でデバイス設定テンプレートを作成して Cisco vManage にアタッチした場合、Cisco vManage 上の既存の設定は上書きされます。クラスター内のそれぞれの Cisco vManage を、その vManage サーバー自体から個別に設定する必要があることに注意してください。1 つの vManage サーバーで vManage 設定テンプレートを作成し、そのデバイステンプレートに他の Cisco vManage をアタッチすることはできません。
3. 証明書の設定を設定し、Cisco vManage の証明書を生成します。
4. vManage クラスターを作成します。

vManage Web サーバー暗号

リリース 16.3.0 以降、vManage Web サーバーは次の暗号をサポートしています。

- TLS_DHE_DSS_WITH_AES_128_GCM_<wbr/>SHA256
- TLS_DHE_DSS_WITH_AES_256_GCM_<wbr/>SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_<wbr/>SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_<wbr/>SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_<wbr/>GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_<wbr/>GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_<wbr/>GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_<wbr/>GCM_SHA384

リリース 16.2 では、vManage Web サーバーは次の暗号をサポートしています。

- TLS_ECDHE_ECDSA_WITH_AES_128_<wbr/>CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_<wbr/>CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

ESXi での vManage VM インスタンスの作成

Cisco vManage を実行するには、ハイパーバイザソフトウェアを実行しているサーバー上に仮想マシン (VM) インスタンスを作成する必要があります。このトピックでは、VMware vSphere ESXi ハイパーバイザを実行しているサーバー上に仮想マシンを作成する方法について説明します。カーネルベースの仮想マシン (KVM) ハイパーバイザを実行しているサーバー上に仮想マシンを作成することもできます。

サーバーの要件については、「サーバーハードウェアの推奨事項」を参照してください。

ESXi ハイパーバイザで Cisco vManage 仮想マシンインスタンスを作成するには、次の手順を実行します。

1. vSphere Client を起動し、Cisco vManage VM インスタンスを作成します。
2. Cisco vManage データベース用に少なくとも 100 GB のボリュームがある新しい仮想ディスクを作成します。
3. 別の vNIC を追加します。
4. Cisco vManage VM インスタンスの起動と Cisco vManage コンソールへの接続
5. Cisco vManage クラスタを作成するには、ステップ 1 から 4 を繰り返して、Cisco vManage インスタンスごとに VM を作成します。

VMware vCenter Server を使用して Cisco vManage VM インスタンスを作成している場合は、同じ手順に従います。

vSphere クライアントの起動および vManage VM インスタンスの作成

1. VMware vSphere Client アプリケーションを起動し、ESXi サーバーの IP アドレスまたは名前、ユーザー名、およびパスワードを入力します。[Login] をクリックして、ESXi サーバーにログインします。
[ESXi] 画面が表示されます。
2. [File] > [Deploy OVF Template] をクリックして、仮想マシンを展開します。
3. [Deploy OVF Template] 画面で、OVF パッケージをインストールしてダウンロードする場所を入力します。このパッケージは、サポートページからダウンロードした vmanage.ova ファイルです。[Next] をクリックします。
4. [Next] をクリックして、OVF テンプレートの詳細を確認します。
5. 展開したテンプレートの名前を入力し、[Next] をクリックします。

6. [Next] をクリックして、仮想ディスクのデフォルトのフォーマットを受け入れます。
7. [Destination Networks] ドロップダウンリストから、展開された OVF テンプレートの宛先ネットワークを選択し、[Next] をクリックします。
8. [Ready to Complete] 画面で、[Finish] をクリックして Cisco vManage VM インスタンスの展開を完了します。

定義したパラメータを使用して VM インスタンスが正常に作成され、[Getting Started] タブが選択された状態で [vSphere Client] 画面が表示されます。デフォルトでは、vNIC が 1 つ含まれています。この vNIC は、トンネルインターフェイスに使用されます。

新しい仮想ディスクの作成

Cisco vManage データベース用に少なくとも 100 GB のボリュームがある新しい仮想ディスクを作成する必要があります。

1. [vSphere Client] 画面の左側にあるナビゲーションバーで、作成した Cisco vManage VM インスタンスを選択し、[Edit virtual machine settings] をクリックします。
2. [vManage Virtual Machine Properties] 画面で、[Add] をクリックして新しい仮想ディスクを追加し、[OK] をクリックします。
3. [Add Hardware] 画面で、VM に追加するデバイスタイプとして [Hard Disk] を選択し、[Next] をクリックします。
4. [Select a Disk] 画面で、[Create a new virtual disk] を選択し、[Next] をクリックします。
5. [Create a Disk] 画面で、Cisco vManage データベースのディスク容量を 100 GB に指定し、[Next] をクリックします。
6. [Advanced Options] 画面で、仮想ストレージデバイスとして [IDE] (Cisco vManage リリース 20.3.1 以降では [SCSI]) を選択し、[Next] をクリックします。Cisco vManage リリース 20.3.1 より前のリリースに IDE を使用している場合、仮想ストアデバイスは IDE である必要があります。
7. [Ready to Complete] 画面で [Finish] をクリックして、キャパシティが 500 GB の新しい仮想ディスクの作成を完了します。

[vSphere Client] 画面が、[Getting Started] が選択された状態で表示されます。

vNIC の追加

管理インターフェイスとメッセージバスに別の vNIC を追加するには、次の手順を実行します。

1. vSphere Client の左側のナビゲーションバーで、作成した Cisco vManage VM インスタンスを選択し、[Edit virtual machine settings] をクリックします。
2. [Cisco vManage – Virtual Machine Properties] 画面で、[Add] をクリックして、管理インターフェイス用の新しい vNIC を追加します。次に [OK] をクリックします。
3. 追加するデバイスタイプの [Ethernet Adapter] をクリックして、[Next] をクリックします。

4. [Adapter Type] ドロップダウンで、追加する vNIC の VMXNET3 を選択して、[Next] をクリックします。
5. [Ready to Complete] 画面で、[Finish] をクリックします。
6. [Cisco vManage –Virtual Machine Properties] 画面が開き、新しい vNIC が追加されていることが示されます。[OK] をクリックして [vSphere Client] 画面に戻ります。
7. Cisco vManage インスタンスがクラスタの一部である場合は、手順 2 ~ 6 を繰り返して 3 番目の vNIC を作成します。この vNIC はメッセージバスに使用されます。

Cisco vManage コンソール への Cisco vManage VM インスタンスの接続

1. vSphere Client の左側のナビゲーションバーで、作成した Cisco vManage VM インスタンスを選択し、[Power on the virtual machine] をクリックします。Cisco vManage 仮想マシンの電源が入ります。
2. [Console] タブを選択して、Cisco vManage コンソールに接続します。Cisco vManage コンソールが表示されます。Cisco vManage にログインします。
3. 使用するストレージデバイスを選択します。
4. [hdc] (Cisco vManage データベース用に追加した新しいパーティション) を選択します。
5. 新しいパーティション (**hdc**) をフォーマットすることを確認します。その後、システムが再起動し、Cisco vManage インスタンスが表示されます。
6. Web ブラウザを使用して Cisco vManage インスタンスに接続するために、Cisco vManage インスタンスの IP アドレスを設定します。

1. Cisco vManage にログインします。
2. 管理 VPN (VPN 512) で、インターフェイス eth0 に IP アドレスを設定します。ご使用のネットワークで到達可能な IP アドレスを指定してください。必要に応じて、デフォルトルートを追加します。

```
# config
(config)# vpn 512
(config)# ip route prefix/length next-hop-ip-address
(config-vpn-512)# interface eth0
(config-interface-eth0)# ip address ip-address
(config-interface-eth0)# no shutdown
(config-interface-eth0)# commit and-quit
#
```

7. Cisco vManage インスタンスに接続するために、URL として次の文字列を入力します。

```
https:// ip-address :8443/
```

8. ログインします。

KVM での vManage VM インスタンスの作成

Cisco vManage を実行するには、ハイパーバイザソフトウェアを実行しているサーバー上に仮想マシン (VM) インスタンスを作成する必要があります。このトピックでは、VMware カーネルベースの仮想マシン (KVM) ハイパーバイザを実行しているサーバー上に VM を作成するプロセスについて説明します。VMware vSphere ESXi ハイパーバイザを実行しているサーバー上に VM を作成することもできます。

サーバーの要件に関しては、サーバーのハードウェア要件を参照してください。

KVM ハイパーバイザでの Cisco vManage VM インスタンスの作成

KVM ハイパーバイザで Cisco vManage VM インスタンスを作成するには、次の手順を実行します。

1. Virtual Machine Manager クライアント アプリケーションを起動します。[Virtual Machine Manager] 画面が表示されます。
2. [New] をクリックして、仮想マシンを展開します。[Create a new virtual machine] 画面が開きます。
3. 仮想マシンの名前を入力します。
 1. [Import existing disk image] オプションボタンを選択します。
 2. [続行 (Forward)] をクリックします。仮想ディスクがインポートされ、作成中の VM インスタンスに関連付けられます。
4. [Provide the existing storage path] ボックスで、[Browse] をクリックして Cisco vManage ソフトウェアイメージを選択します。
 1. [OS Type] フィールドで、[Linux] を選択します。
 2. [Version] フィールドで、実行している Linux バージョンを選択します。
 3. [続行 (Forward)] をクリックします。
5. ネットワークトポロジとサイトの数に基づいてメモリと CPU を指定し、[Forward] をクリックします。
6. [Customize configuration before install] をオンにして、[Finish] をクリックします。
7. 左側のナビゲーションバーで [Disk 1] を選択します。
 1. [Advanced Options] をクリックします。
 2. [Disk Bus] フィールドで、[IDE] (Cisco vManage リリース 20.3.1 以降では、[SCSI]) を選択します。
 3. [Storage Format] フィールドで、[qcow2] を選択します。

4. [Apply] をクリックして、定義したパラメータで VM インスタンスを作成します。デフォルトでは、この VM インスタンスに、トンネルインターフェイスに使用される 1 つの vNIC が含まれます。



(注) Cisco SD-WAN は VMXNET3 vNIC のみをサポートします。

8. [Cisco vManage Virtual Machine] ウィンドウで、[Add Hardware] をクリックして、Cisco vManage データベースの新しい仮想ディスクを追加します。
9. [Add New Virtual Hardware] 画面で、新しい仮想ディスクに関して次のように指定します。
 1. [Create a disk image on the computer's hard drive] で、Cisco vManage データベースのディスク容量を 100GB に指定します。
 2. [Device Type] フィールドで、仮想ストレージに IDE ディスク (Cisco vManage リリース 20.3.1 以降では、SCSI ディスク) を指定します。
 3. [Storage Format] フィールドで、[qcow2] を指定します。
 4. [Finish] をクリックして、容量が 100GB の新しい仮想ディスクの作成を完了します。
10. [Cisco vManage Virtual Machine] 画面で、[Add Hardware] をクリックして、管理インターフェイスに別の vNIC を追加します。
11. [Add New Virtual Hardware] 画面で [Network] をクリックします。
 1. [Host Device] フィールドで、適切なホストデバイスを選択します。
 2. [Finish] をクリックします。

新しく作成された vNIC が左側のペインに表示されます。この vNIC は、管理インターフェイスに使用されます。

12. Cisco vManage インスタンスがクラスタの一部である場合は、手順 10 および 11 を繰り返して 3 番目の vNIC を作成します。この vNIC はメッセージバスに使用されます。
13. [Cisco vManage Virtual Machine] 画面で、画面の左上隅にある [Begin Installation] をクリックします。
14. 仮想マシンインスタンスが作成され、Cisco vManage コンソールが表示されます。
15. ログインプロンプトで、デフォルトのユーザー名 **admin** およびデフォルトのパスワード **admin** を使用してログインします。使用するストレージデバイスを選択するように求められます。
16. [hdc] (vManage データベース用に追加した新しいパーティション) を選択します。
17. 新しいパーティション (**hdc**) をフォーマットすることを確認します。システムが再起動し、Cisco vManage インスタンスが表示されます。

18. Cisco vManage クラスタを作成するには、手順1～17を繰り返して、Cisco vManage インスタンスごとに VM を作成します。

Cisco vManage インスタンスへの接続

Web ブラウザを使用して Cisco vManage インスタンスに接続するために、Cisco vManage インスタンスの IP アドレスを設定します。

1. デフォルトのユーザー名とパスワードを使用してログインします。

```
Login: admin password: admin #
```

2. 管理 VPN (VPN 512) で、インターフェイス eth0 に IP アドレスを設定します。ご使用のネットワークで到達可能な IP アドレスを指定してください。必要に応じて、デフォルトルートを追加します。

```
# config
(config)# vpn 512
(config)# ip route prefix/length next-hop-ip-address
(config-vpn-512)# interface eth0
(config-interface-eth0)# ip address ip-address
(config-interface-eth0)# no shutdown
(config-interface-eth0)# command and-quit
#
```

3. vManage インスタンスに接続するために、URL として次の文字列を入力します。

```
https:// ip-address :8443/
```

4. ユーザー名 **admin** とパスワード **admin** を使用してログインします。

Cisco vManage の構成テンプレートの作成

Cisco vManage の構成テンプレートを作成する必要があります。

設定要件

セキュリティの前提条件

Cisco SD-WAN オーバーレイネットワークで Cisco vManage を設定する前に、証明書を生成して、デバイスにインストールしておく必要があります。「証明書の生成」を参照してください。

変数スプレッドシート

作成する機能テンプレートには変数が含まれます。Cisco vManage の場合、デバイステンプレートをデバイスに添付するときに変数に実際の値を入力するには、値を手動で入力するか、右上隅にある [Import File] をクリックして、変数値を含む CSV 形式の Excel ファイルをロードします。

スプレッドシートでは、ヘッダー行に変数名が含まれ、後続の各行はデバイスに対応し、変数の値が定義されます。スプレッドシートの最初の3つの列は順番どおりである必要があります。

- csv-deviceId : デバイスのシリアル番号 (デバイスを一意に識別するために使用)。
- csv-deviceIP : デバイスのシステム IP アドレス (**system ip address** コマンドの入力に使用)。
- csv-host-name : デバイスのホスト名 (**system hostname** コマンドの入力に使用)。

オーバーレイネットワーク内のすべてのデバイス (Cisco vManage、ルータ、Cisco vSmart コントローラ、および Cisco vBond オーケストレーション) に対して1つのスプレッドシートを作成できます。全デバイスのすべての変数に値を指定する必要はありません。

Cisco vManage の機能テンプレート

次の機能は Cisco vManage の操作に必須であるため、それぞれの機能テンプレートを作成する必要があります。

表 3:

機能	テンプレート名
認証、許可、アカウントिंग (AAA)	AAA
セキュリティ	セキュリティ
システム全体のパラメータ	システム
トランスポート VPN (VPN 0)	VPN、VPN ID を 0 に設定。
管理 VPN (アウトオブバンド管理トラフィック用)	VPN、VPN ID を 512 に設定。

機能テンプレートの作成

機能テンプレートは、Cisco vManage の完全な構成の構成要素です。Cisco vManage で有効にできる機能ごとに、その機能に必要なパラメータを入力するテンプレートフォームが提供されます。

必須の Cisco vManage 機能の機能テンプレートを作成する必要があります。

同じ機能に対して複数のテンプレートを作成できます。

vManage 機能テンプレートを作成するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration] > [Templates]**の順に選択します。
2. **[Feature Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] は [Feature] と呼ばれます。

3. [Add template] をクリックします。
4. 左側のペインの [Select Devices] から [vManage] を選択します。Cisco vManage と他のデバイスの両方で使用できる機能に対して、1 つの機能テンプレートを作成できます。ただし、Cisco vManage でのみ使用できるソフトウェア機能については、別の機能テンプレートを作成する必要があります。
5. 右側のペインで、テンプレートを選択します。テンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部にはそのテンプレートで使用可能なパラメータを定義するためのフィールドがあります。オプションのパラメータは通常、グレー表示されています。同じパラメータに複数のエントリを追加できる場合は、右側にプラス (+) 記号が表示されます。
6. テンプレート名と説明を入力します。これらのフィールドは必須です。テンプレート名には特殊文字を使用できません。
7. 必要な各パラメータについて、目的の値を選択し、該当する場合はパラメータの範囲を選択します。各パラメータフィールドの左側にあるドロップダウンメニューから範囲を選択します。
8. 必要なパラメータの下にあるプラス記号 (+) をクリックして、必要に応じて追加パラメータの値を設定します。
9. [作成 (Create)] をクリックします。
10. 前のセクションにリストされている必要な機能ごとに機能テンプレートを作成します。
 1. トランスポート VPN の場合は、VPN-vManage というテンプレートを使用し、[VPN Template] セクションで VPN を 0 に設定し、範囲を [Global] にします。
 2. 管理 VPN の場合は、VPN-vManage というテンプレートを使用し、[VPN Template] セクションで VPN を 512 に設定し、範囲を [Global] にします。
11. Cisco vManage で有効にするオプション機能ごとに、追加の機能テンプレートを作成します。

リリース情報

リリース 15.3 で Cisco vManage が導入されました。

Cisco vManage の設定

Cisco vManage 用の仮想マシン (VM) をセットアップして起動すると、仮想マシンは工場出荷時のデフォルト設定で起動します。その後、デバイス構成テンプレートを作成することによ

り、Cisco vManage サーバー自体から直接各 Cisco vManage インスタンスを設定して、Cisco vManage が認証および検証され、オーバーレイネットワークに参加できるようにします。少なくとも、ネットワークの Cisco vBond オーケストレーションの IP アドレス、デバイスのシステム IP アドレス、および VPN 0 のトンネルインターフェイスを設定して、ネットワーク コントローラ デバイス (Cisco vBond オーケストレーション、Cisco vManage、および Cisco vSmart コントローラ デバイス) 間で制御トラフィックを交換するために使用する必要があります。

オーバーレイネットワークを動作させ、Cisco vManage インスタンスをオーバーレイネットワークに参加させるには、次の手順を実行する必要があります。

- VPN 0 の少なくとも 1 つのインターフェイスでトンネルインターフェイスを設定します。このインターフェイスは、すべての Cisco vEdge デバイス からアクセス可能な WAN トランスポートネットワークに接続する必要があります。VPN 0 は、オーバーレイネットワーク内の Cisco vEdge デバイス 間ですべてのコントロールプレーントラフィックを伝送します。
- オーバーレイ管理プロトコル (OMP) が有効になっていることを確認します。OMP は、Cisco SD-WAN コントロールプレーンの確立と維持を行うプロトコルで、デフォルトで有効になっており、無効にすることはできません。CLI から設定を編集する場合は、**omp** 設定コマンドを削除しないでください。



(注) vManage クラスタの場合は、クラスタ内の各 Cisco vManage インスタンスを、その Cisco vManage サーバー自体から個別に設定する必要があります。1 つの Cisco vManage サーバーで Cisco vManage 構成テンプレートを作成し、そのデバイステンプレートに他の Cisco vManage をアタッチすることはできません。

デバイス構成テンプレートによる Cisco vManage の設定

Cisco vManage を設定するには、デバイス構成テンプレートを作成します。

1. Cisco vBond オーケストレーション のアドレスを設定します。
 1. Cisco vManage メニューから、**[Administration]** > **[Settings]** の順に選択します。
 2. vBond について、**[Edit]** をクリックします。
 3. **[vBond DNS/IP Address: Port]** フィールドに、Cisco vBond オーケストレーション を指す DNS 名または Cisco vBond オーケストレーション の IP アドレスと、それへの接続に使用するポート番号を入力します。
 4. **[Save]** をクリックします。
2. Cisco vManage メニューから、**[Configuration]** > **[Templates]** の順に選択します。
3. **[Device Templates]** をクリックし、テンプレートを選択します。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。

4. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
5. [Device Model] ドロップダウンリストから [vManage] を選択します。Cisco vManage に、Cisco vManage を設定するためのすべての機能テンプレートが表示されます。必須の機能テンプレートはアスタリスク (*) で示され、残りのテンプレートはオプションです。デフォルトでは、各機能の工場出荷時のデフォルトテンプレートが選択されています。
6. [Template Name] フィールドに、デバイステンプレートの名前を入力します。このフィールドは必須で、使用できるのは、英大文字と小文字、0～9の数字、ハイフン (-)、下線 (_) のみです。スペースやその他の文字を含めることはできません。
7. [Description] フィールドにデバイステンプレートの説明を入力します。このフィールドは必須であり、任意の文字とスペースを含めることができます。
8. システム機能テンプレートで、サイト ID、システム IP アドレス、ホスト名、ロケーション、タイムゾーン、および GPS ロケーションの設定を指定します。
9. AAA 機能テンプレートの場合は、[Local] をクリックし、[Users] を選択して、ユーザー「admin」のパスワードを変更します。
10. VPN 0 機能テンプレートの場合は、[VPN 0] を選択し、システム IP アドレスと DNS サーバーのアドレスまたはホスト名を設定します。必要に応じて、[Route] をクリックしてスタティックルートを追加します。



(注) スタンドアロンまたはクラスタモードでの Cisco vManage の IP 構成には DHCP を使用しないことをお勧めします。

11. VPN-Interface-Ethernet 機能テンプレートで、WAN トランスポートネットワークに接続するためのトンネルインターフェイスとして使用する VPN 0 のインターフェイスを設定します。[Shutdown] で [No] をクリックし、インターフェイス名を入力して、インターフェイスに動的または静的アドレスを割り当てます。[Interface Tunnel] をクリックし、[Tunnel Interface] を選択して、[On] をクリックします。その後、トンネルインターフェイスにカラーを割り当て、トンネルで許可する目的のサービスを選択します。



(注) オーバーレイネットワークが起動し、Cisco vManage がオーバーレイネットワークに参加できるようにするには、VPN 0 の少なくとも 1 つのインターフェイスでトンネルインターフェイスを設定する必要があります。このインターフェイスは、すべての Cisco vEdge デバイスからアクセス可能な WAN トランスポートネットワークに接続する必要があります。VPN 0 は、オーバーレイネットワーク内の Cisco vEdge デバイス間ですべてのコントロールプレーントラフィックを伝送します。

12. セキュリティ機能テンプレートで、コントロールプレーンプロトコルを設定します。
13. 必要に応じて、デフォルトのアーカイブ、バナー、ロギング、NTP、および SNMP 機能テンプレートを変更します。バナーテンプレートを使用して、CLI を介してデバイスにログインしたときに表示される MOTD および ログインバナーを設定します。Cisco vManage サーバーへのログイン時に表示されるログインバナーを作成するには、**[Administration]** > **[Settings]** > **[Banner]** を選択します。
14. **[Create]** をクリックします。新しい設定テンプレートが **[Device Template]** テーブルに表示されます。**[Feature Templates]** 列には、デバイステンプレートに含まれている機能テンプレートの数が表示され、**[Type]** 列には、デバイステンプレートが機能テンプレートのコレクションから作成されたことを示す「Feature」が表示されます。
15. 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。
16. **[Attach Devices]** 列で **[Available Devices]** リストからローカル Cisco vManage を選択し、右向き矢印をクリックしてそれを **[Selected Devices]** 列に移動させます。
17. **[Attach]** をクリックします。

CLI 構成例

以下は、簡単な Cisco vManage 構成の例です。この構成には、工場出荷時のデフォルト設定の設定が多数含まれており、多数のデフォルト設定値が示されています。

```
vManage# show running-config
system
 host-name          vManage
 gps-location latitude 40.7127837
 gps-location longitude -74.00594130000002
 system-ip          172.16.255.22
 site-id            200
 organization-name "Cisco"
 clock timezone America/Los_Angeles
 vbond 10.1.14.14
aaa
 auth-order local radius tacacs
 usergroup basic
  task system read write
  task interface read write
 !
 usergroup netadmin
 !
 usergroup operator
  task system read
  task interface read
  task policy read
  task routing read
  task security read
 !
 user admin
  password encrypted-password
 !
 !
 logging
 disk
```



```
        enable
    !
    !
    !
snmp
no shutdown
view v2
  oid 1.3.6.1
  !
  community private
    view v2
    authorization read-only
  !
trap target vpn 0 10.0.1.1 16662
  group-name Cisco
  community-name private
  !
trap group test
  all
  level critical major minor
  exit
exit
exit
!
vpn 0
interface eth1
  ip address 10.0.12.22/24
  tunnel-interface
  color public-internet
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  allow-service netconf
  no allow-service ntp
  no allow-service stun
  allow-service https
  !
  no shutdown
  !
  ip route 0.0.0.0/0 10.0.12.13
  !
vpn 512
interface eth0
  ip 172.16.14.145/23
  no shutdown
  !
  ip route 0.0.0.0/0 172.16.14.1
  !
```

証明書の設定

オーバーレイネットワークの新しいコントローラデバイス（Cisco vManage インスタンス、Cisco vBond オーケストレーション、および Cisco vSmart コントローラ）は、署名付き証明書を使用して認証されます。Cisco vManage から、証明書署名要求（CSR）を自動的に生成し、生成された証明書を取得して、それらをすべてのコントローラデバイスに、それらのデバイスがネットワークに追加されたときにインストールできます。



- (注) すべてのコントローラデバイスは、証明書がインストールされていないとオーバーレイネットワークに参加できません。

証明書の生成およびインストールプロセスを自動化するには、コントローラデバイスをネットワークに追加する前に、組織の名前と証明書承認設定を指定します。

証明書設定の指定の詳細については、「[証明書](#)」を参照してください。

Cisco vManage 証明書の生成

Cisco vManage がオーバーレイネットワークに参加できるようにするには、Cisco vManage インスタンスの証明書署名要求 (CSR) を生成する必要があります。Cisco vManage は、生成された証明書を自動的に取得してインストールします。

Cisco vManage 証明書の生成の詳細については、「[証明書](#)」を参照してください。
<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/manage-certificates.html>

vManage クラスタの作成

vManage クラスタは、Cisco SD-WAN オーバーレイ ネットワーク ドメイン内に存在する3つ以上の Cisco vManage インスタンスの集合体です。このクラスタは、共同で、ネットワーク内のすべての Cisco vEdge デバイスにネットワーク管理サービスを提供します。一部のサービス（どの vManage インスタンスがルータに接続して要求を処理するか決定など）は自動的に分散されますが、その他のサービス（統計および構成データベース、メッセージングサーバー）は、そのサービスを処理する Cisco vManage インスタンスを管理者が設定します。

Cisco vManage クラスタの作成の詳細については、「[クラスタ管理](#)」を参照してください。

Cisco vManage クライアントセッションのタイムアウト値の有効化

デフォルトでは、Cisco vManage クライアントへのユーザーのセッションは無期限に確立されたままになり、タイムアウトになることはありません。

Cisco vManage クライアントセッションの非アクティブ時間を設定して、その時間が経過するとユーザーがログアウトされるようにするには、次の手順を実行します。

1. Cisco vManage メニューから、**[Administration]** > **[Settings]** を選択します。
2. **[Client Session Timeout]** オプションで、**[Edit]** をクリックします。
3. **[Enabled]** をクリックし、タイムアウト値を分単位で入力します。この値は 10 ~ 180 分に指定することができます。
4. **[Save]** をクリックします。

クライアントセッションのタイムアウト値は、Cisco vManage クラスタ内のすべての Cisco vManage サーバーに適用されます。

Cisco vBond オーケストレーションの導入

Cisco vBond オーケストレーションは、オーバーレイネットワーク内の Cisco vSmart コントローラと vEdge ルータを認証し、デバイス間の接続を調整するソフトウェアモジュールです。ネットワーク内のすべての Cisco vEdge デバイスが接続できるように、パブリック IP アドレスが必要です（パブリックアドレスを持つ必要があるのは1つの Cisco vEdge デバイスだけです）。Cisco vBond オーケストレーションはネットワーク内の任意の場所に配置できますが、DMZ に配置することを強く推奨します。オーケストレータにパブリック IP アドレスを割り当てると、異なる NAT ゲートウェイの背後で保護されたプライベートアドレス空間に配置された Cisco vSmart コントローラと vEdge ルータが相互に通信接続を確立できます。Cisco vBond オーケストレーションはネットワークサーバー上で VM として実行されます。

Cisco SD-WAN オーバーレイネットワークには、1つ以上の Cisco vBond オーケストレーションを含めることができます。

Cisco vBond オーケストレーションを展開するには、次の手順を実行します。

1. ESXi または KVM ハイパーバイザで vBond VM インスタンスを作成します。
2. Cisco vBond オーケストレーションの最小限の構成を作成し、ネットワーク上でアクセスできるようにします。作成するには、SSH を使用して Cisco vBond オーケストレーションへの CLI セッションを開き、デバイスを手動で設定します。
3. Cisco vBond オーケストレーションをオーバーレイネットワークに追加して、Cisco vManage が認識できるようにします。
4. Cisco SD-WAN ゼロタッチプロビジョニング (ZTP) vBond サーバーをホストしている企業の場合は、このロールを実行するように Cisco vBond オーケストレーションを1つ設定します。
5. Cisco vBond オーケストレーションの完全な構成を作成します。SSH を使用して初期構成を作成し、Cisco vBond オーケストレーションへの CLI セッションを開きます。次に、Cisco vManage で構成テンプレートを作成し、テンプレートを Cisco vBond オーケストレーションに添付することにより、完全な構成を作成します。構成テンプレートを Cisco vBond オーケストレーションに添付すると、テンプレート内の構成パラメータによって初期構成が上書きされます。

ESXi での vBond VM インスタンスの作成

Cisco vBond オーケストレーションを開始するには、ハイパーバイザソフトウェアを実行しているサーバー上に仮想マシン (VM) インスタンスを作成する必要があります。ここでは、VMware vSphere ESXi ハイパーバイザを実行しているサーバー上に VM を作成する方法について説明します。カーネルベースの仮想マシン (KVM) ハイパーバイザソフトウェアを実行しているサーバー上に VM を作成することもできます。

サーバー情報については、「サーバーハードウェアの推奨事項」を参照してください。

ESXi ハイパーバイザで vBond VM インスタンスを作成するには、次の手順を実行します。

1. vSphere Client を起動し、vBond VM インスタンスを作成します。
2. トンネルインターフェイスの vNIC を追加します。
3. vBond VM インスタンスの起動とコンソールへの接続

各ステップの詳細を以下に示します。

VMware vCenter Server を使用して vBond VM インスタンスを作成している場合は、同じ手順に従います。ただし、vCenter Server のページは、手順に示されている vSphere Client のページとは異なることに注意してください。

vSphere Client の起動および vBond VM インスタンスの作成

1. VMware vSphere Client アプリケーションを起動し、ESXi サーバーの IP アドレスまたは名前、ユーザー名、およびパスワードを入力します。[Login] をクリックして、ESXi サーバーにログインします。
2. [File] > [Deploy OVF Template] をクリックして、仮想マシンを展開します。
3. [Deploy OVF Template] ページで、OVF パッケージをインストールしてダウンロードする場所を入力します。このパッケージは、シスコからダウンロードした `vedge.ova` ファイルです。次に、[Next] をクリックします。
4. [Next] をクリックして、OVF テンプレートの詳細を確認します。
5. 展開したテンプレートの名前を入力し、[Next] をクリックします。次の図は、vBond インスタンスの名前を示しています。
6. [Next] をクリックして、仮想ディスクのデフォルトのフォーマットを受け入れます。
7. [Next] をクリックして、展開された OVF テンプレートの宛先ネットワークとして、使用している宛先ネットワーク名を受け入れます。この例では、CorpNet が宛先ネットワークです。
8. [Ready to Complete] ページで [Finish] をクリックします。次の図は、vBond インスタンスの名前を示しています。

定義したパラメータを使用して VM インスタンスが正常に作成され、[Getting Started] が選択された状態で [vSphere Client] ページが表示されます。デフォルトでは、vNIC が 1 つ含まれています。この vNIC は、管理インターフェイスに使用されます。

トンネルインターフェイス用の vNIC の追加

1. vSphere Client の左側のナビゲーションバーで、作成した vBond VM インスタンスを選択し、[Edit virtual machine settings] をクリックします。

2. [vEdge Cloud – Virtual Machine Properties] ページで、[Add] をクリックして、管理インターフェイスの新しい vNIC を追加します。次に [OK] をクリックします。
3. 追加するデバイスタイプの [Ethernet Adapter] をクリックして、[Next] をクリックします。
4. [Adapter Type] ドロップダウンで、追加する vNIC の VMXNET3 を選択して、[Next] をクリックします。
5. [Ready to Complete] ページで [Finish] をクリックします。
6. [vEdge Cloud – Virtual Machine Properties] ページが開き、新しい vNIC が追加されていることが示されます。[OK] をクリックして [vSphere Client] ページに戻ります。

vBond VM インスタンスの起動とコンソールへの接続

1. vSphere Client の左側のナビゲーションバーで、作成した vBond 仮想マシンインスタンスを選択し、[Power on the virtual machine] をクリックします。vBond 仮想マシンの電源が入ります。
2. [Console] を選択して、vBond コンソールに接続します。
3. ログインプロンプトで、デフォルトのユーザー名 **admin** およびデフォルトのパスワード **admin** を使用してログインします。

次のステップ

「Cisco vBond オーケストレーション の設定」を参照してください。

KVM での vBond VM インスタンスの作成

Cisco vBond オーケストレーションを開始するには、ハイパーバイザソフトウェアを実行しているサーバー上に仮想マシン (VM) インスタンスを作成する必要があります。ここでは、カーネルベースの仮想マシン (KVM) ハイパーバイザを実行しているサーバー上に VM を作成する方法について説明します。vSphere ESXi ハイパーバイザソフトウェアを実行しているサーバー上に VM を作成することもできます。

サーバー情報については、「サーバーハードウェアの推奨事項」を参照してください。

KVM ハイパーバイザで vBond VM インスタンスを作成するには、次の手順を実行します。

1. Virtual Machine Manager (virt-manager) クライアントアプリケーションを起動します。[Virtual Machine Manager] ページが表示されます。
2. [New] をクリックして、仮想マシンを展開します。[Create a new virtual machine] ページが開きます。
3. 仮想マシンの名前を入力します。次の図は、vBond インスタンスの名前を示しています。
 1. [Import existing disk image] オプションを選択してオペレーティングシステムをインストールします。

2. [続行 (Forward)] をクリックします。
4. [Provide the existing storage path] で [Browse] をクリックして vBond ソフトウェアイメージを選択します。
 1. [OS Type] で [Linux] を選択します。
 2. [Version] で、実行している Linux バージョンを選択します。
 3. [続行 (Forward)] をクリックします。
5. ネットワークトポロジとサイトの数に基づいてメモリと CPU を指定し、[Forward] をクリックします。
6. [Customize configuration before install] をオンにします。その後、[Finish] をクリックします。
7. 左側のナビゲーションバーで [Disk 1] を選択します。実行されるアクション
 1. [Advanced Options] をクリックします。
 2. [Disk Bus] で [IDE] を選択します。
 3. [Storage Format] で [qcow2] を選択します。
 4. [Apply] をクリックして、定義したパラメータで VM インスタンスを作成します。デフォルトでは、vNIC が 1 つ含まれています。この vNIC は、管理インターフェイスに使用されます。



(注) ソフトウェアは VMXNET3 vNIC のみをサポートします。

8. [vEdge Cloud Virtual Machine] ページで、[Add Hardware] をクリックして、トンネルインターフェイスに 2 番目の vNIC を追加します。
9. [Add New Virtual Hardware] ページで [Network] をクリックします。
 1. [Host Device] で、適切なホストデバイスを選択します。
 2. [Finish] をクリックします。

新しく作成された vNIC が左側のペインに表示されます。この vNIC は、トンネルインターフェイスに使用されます。
10. [vBond Virtual Machine] ページで、ページの左上隅にある [Begin Installation] をクリックします。
11. 仮想マシンインスタンスが作成され、vBond コンソールが表示されます。
12. ログインページで、デフォルトのユーザー名 **admin** およびデフォルトのパスワード **admin** を使用してログインします。

次のステップ

「Cisco vBond オーケストレーションの設定」を参照してください。

Cisco vBond オーケストレーションの設定

オーバーレイネットワークで Cisco vBond オーケストレーションの仮想マシン (VM) をセットアップして起動すると、Cisco vBond オーケストレーションが工場出荷時のデフォルト設定で起動します。その後、デバイスが認証および検証され、オーバーレイネットワークに参加できるように、いくつかの基本的な機能を手動で設定する必要があります。これらの機能の設定において、デバイスを、システム IP アドレスを提供する Cisco vBond オーケストレーションとして設定し、インターネットに接続する WAN インターフェイスを設定します。オーバーレイネットワーク内のすべての Cisco vEdge デバイスが Cisco vBond オーケストレーションに接続できるように、このインターフェイスにはパブリック IP アドレスが必要です。

SSH を使用して初期構成を作成し、Cisco vBond オーケストレーションへの CLI セッションを開きます。

初期構成を作成したら、Cisco vManage で構成テンプレートを作成し、そのテンプレートを Cisco vBond オーケストレーションにアタッチすることにより、完全な構成を作成します。構成テンプレートを Cisco vBond オーケストレーションに添付すると、テンプレート内の構成パラメータによって初期構成が上書きされます。

Cisco vBond オーケストレーションの初期構成の作成

CLI セッションを使用して Cisco vBond オーケストレーションで初期構成を作成するには、次の手順を実行します。

1. SSH 経由で Cisco vEdge デバイスへの CLI セッションを開きます。
2. **admin** ユーザーとして、デフォルトのパスワード **admin** を使用してログインします。CLI プロンプトが表示されます。
3. コンフィギュレーションモードに入ります。

```
vBond#config  
vBond(config)#
```

4. ホスト名を設定します。

```
vBond(config)#system host-name hostname
```

ホスト名の設定は任意ですが、ホスト名は CLI のプロンプトの一部として含まれ、さまざまな Cisco vManage 画面でデバイスを参照するために使用されるため、設定することを推奨します。

5. システム IP アドレスを設定します。

```
vBond(config-system)#system-ip ip-address
```

Cisco vManage は、システム IP アドレスを使用してデバイスを識別し、NMS が完全な設定をデバイスにダウンロードできるようにします。

6. Cisco vBond オーケストレーションの IP アドレスを設定します。Cisco vBond オーケストレーションの IP アドレスは、オーバーレイネットワーク内のすべての Cisco vEdge デバイスが Cisco vBond オーケストレーションに到達できるように、パブリック IP アドレスにする必要があります。

```
vBond(config-system) #vbond ip-address local
```

リリース 16.3 以降では、アドレスは IPv4 または IPv6 アドレスになります。以前のリリースでは、IPv4 アドレスである必要があります。vBond Orchestrator は、事実上、オーケストレータ機能のみを実行する vEdge ルータです。[local] オプションは、デバイスが vEdge ルータではなく Cisco vBond オーケストレーションであることを指定します。Cisco vBond オーケストレーションは、スタンドアロンの仮想マシン (VM) またはハードウェアルータで動作する必要があります。ソフトウェアまたはハードウェアの vEdge ルータと同じデバイスに共存することはできません。

7. ソフトウェアアップグレードの成功を確認するための時間制限を設定します。

```
vBond(config-system) #upgrade-confirm minutes
```

時間の範囲は 1 ~ 60 分です。この時間制限を設定する場合、デバイスのソフトウェアアップグレード時、Cisco vManage の起動時、または設定された分数以内にソフトウェアアップグレードが成功することを確認する必要があります。設定時間内に確認メッセージを受信しない場合、デバイスは以前のソフトウェアイメージに戻ります。

8. ユーザー「admin」のパスワードを変更します。

```
vBond(config-system) #user admin password password
```

デフォルトのパスワードは「admin」です。

9. インターネットまたはその他の WAN トランスポートネットワークに接続するために、VPN 0 のインターフェイスを設定します。リリース 16.3 以降では、IP アドレスは IPv4 または IPv6 アドレスになります。以前のリリースでは、IPv4 アドレスである必要があります。インターフェイスに構成するプレフィックスに、**vbond local** コマンドで設定する IP アドレスが含まれていることを確認します。

```
vBond(config) #vpn 0 interface interface-name
vBond(config-interface) #ip address ipv4-prefix/length
vBond(config-interface) #ipv6 address ipv6-prefix/length
vBond(config-interface) #no shutdown
```



- (注) オーバーレイネットワーク内のすべてのデバイスが Cisco vBond オーケストレーションに到達できるように、IP アドレスはパブリックアドレスである必要があります。

10. 設定をコミットします。

```
vBond(config) #commit and-quit
vBond#
```

11. 設定が正しく、完全であることを確認します。

```
vBond#show running-config
```


オーバーレイネットワークが起動して動作可能になったら、初期構成パラメータを含むvBond構成テンプレートをCisco vManageで作成します。次のvManage機能テンプレートを使用します。

- ホスト名、システムIPアドレス、およびvBond機能を設定するためのシステム機能テンプレート。
- 「admin」ユーザーのパスワードを設定するためのAAA機能テンプレート。
- VPN 0のインターフェイスを設定するためのVPNインターフェイスイーサネット機能テンプレート。

さらに、次の一般的なシステムパラメータを設定することを推奨します。

- Cisco vManageメニューから、**[Administration]** > **[Settings]**の順に選択し、組織名を設定します。
- Cisco vManageメニューから、**[Configuration]** > **[Templates]**の順に選択します。**[System configuration template]** ドロップダウンから、**[create template]**を選択し、タイムゾーン、NTPサーバー、およびデバイスの物理的な場所を設定します。
- **[Additional Templates]** をクリックし、バナー機能テンプレートのドロップダウンから**[Create Template]**を選択します。ログインバナーを設定します。
- **[System feature configuration template]** ドロップダウンから、**[Create Template]**を選択し、ディスクとサーバーのパラメータを設定します。
- **[AAA feature configuration template]** ドロップダウンから、**[Create Template]**を選択し、AAA、RADIUS、およびTACACSサーバーを設定します。
- **[Additional Templates]** をクリックし、SNMP機能テンプレートのドロップダウンから**[Create Template]**を選択して、SNMPを設定します。



(注) オーバーレイネットワーク内のすべてのデバイスがCisco vBondオーケストレーションに到達できるように、IPアドレスはパブリックアドレスである必要があります。

CLI 初期構成の例

以下は、Cisco vBondオーケストレーションでの簡単な構成の例です。この構成には、工場出荷時のデフォルト設定の設定が多数含まれており、多数のデフォルト設定値が示されています。

```
vBond#show running-config
system
 host-name          vBond
 gps-location latitude 40.7127837
 gps-location longitude -74.00594130000002
 system-ip          172.16.240.161
 organization-name "Cisco"
 clock timezone America/Los_Angeles
 vbond 11.1.1.14 local
```

```
aaa
  auth-order local radius tacacs
  usergroup basic
    task system read write
    task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
    task system read
    task interface read
    task policy read
    task routing read
    task security read
  !
  user admin
    password encrypted-password
  !
  !
  logging
    disk
    enable
  !
  !
  vpn 0
    interface ge0/0
      ip address 11.1.1.14/24
      no shutdown
    !
    ip route 0.0.0.0/0 11.1.1.1
  !
  !
  vpn 512
    interface eth0
      ip dhcp-client
      no shutdown
    !
  !
```

次のステップ

「Cisco vBond オーケストレーションをオーバーレイネットワークに追加」を参照してください。

Cisco vBond オーケストレーションの構成テンプレートの作成

ここでは、Cisco vManage によって管理されている Cisco vBond オーケストレーションの設定方法について説明します。これらのデバイスは、Cisco vManage から設定する必要があります。ルータの CLI から直接設定すると、Cisco vManage により、NMS システムに保存されている設定で設定が上書きされます。

設定要件

セキュリティの前提条件

Cisco SD-WAN オーバーレイネットワークで Cisco vBond オークストレーションを設定する前に、Cisco vBond オークストレーションの証明書を生成して、証明書をデバイスにインストールしておく必要があります。「証明書の生成」を参照してください。

変数スプレッドシート

作成する機能テンプレートには、ほとんどの場合、変数が含まれます。デバイステンプレートをデバイスにアタッチするときに、Cisco vManage が変数に実際の値を入力するようにするには、値を手動で入力するか、右上隅にある [Import File] をクリックして、変数値を含む CSV 形式の Excel ファイルをロードします。

スプレッドシートでは、ヘッダー行に変数名が含まれ、後続の各行はデバイスに対応し、変数の値が定義されます。スプレッドシートの最初の3つの列は以下に示す順番どおりである必要があります。

- csv-deviceId : デバイスのシリアル番号 (デバイスを一意に識別するために使用)。
- csv-deviceIP : デバイスのシステム IP アドレス (**system ip address** コマンドの入力に使用)。
- csv-host-name : デバイスのホスト名 (**system hostname** コマンドの入力に使用)。

オーバーレイネットワーク内のすべてのデバイス (ルータ、Cisco vSmart コントローラ、および Cisco vBond オークストレーション) に対して 1 つのスプレッドシートを作成できます。全デバイスのすべての変数に値を指定する必要はありません。

Cisco vBond オークストレーションの機能テンプレート

次の機能は Cisco vBond オークストレーションの操作に必須であるため、それぞれの機能テンプレートを作成する必要があります。

機能	テンプレート名
認証、許可、アカウントティング (AAA)	AAA
セキュリティ	セキュリティ
システム全体のパラメータ	システム
トランスポート VPN (VPN 0)	VPN、VPN ID を 0 に設定
管理VPN (アウトオブバンド管理トラフィック用)	VPN、VPN ID を 512 に設定

機能テンプレートの作成

機能テンプレートは、Cisco vBond オーケストレーションの完全な構成の構成要素です。Cisco vBond オーケストレーションで有効にできる機能ごとに、Cisco vManage では、その機能に必要なパラメータを入力するテンプレートフォームが提供されます。

必須の Cisco vBond オーケストレーション 機能の機能テンプレートを作成する必要があります。

同じ機能に対して複数のテンプレートを作成できます。

vBond 機能テンプレートを作成するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration] > [Templates]** を選択します。
2. **[Feature Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Feature Templates]** は **[Feature]** と呼ばれます。

3. **[Add Template]** を選択します。
4. 左側のペインで、**[Select Devices]** から **[Cloud router]** を選択します。
5. 右側のペインで、テンプレートを選択します。テンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部にはそのテンプレートで使用できる必要なパラメータを定義するためのフィールドがあります。オプションのパラメータは通常、グレー表示されています。同じパラメータに複数のエントリを追加できる場合は、右側にプラス記号 (+) が表示されます。
6. テンプレート名と説明を入力します。これらのフィールドは必須です。テンプレート名には特殊文字を使用できません。
7. 必要な各パラメータについて、目的の値を選択し、該当する場合はパラメータの範囲を選択します。各パラメータの値ボックスの左側にあるドロップダウンメニューから範囲を選択します。
8. 必要なパラメータの下にあるプラス記号 (+) をクリックして、必要に応じて追加パラメータの値を設定します。
9. **[作成 (Create)]** をクリックします。
10. 前のセクションにリストされている必要な機能ごとに機能テンプレートを作成します。
 1. システムテンプレートの上部で、**[Controller Groups]**、**[Maximum Controllers]**、および **[Maximum OMP Sessions]** を除くすべての必要なパラメータを設定します。これらのパラメータはルータに固有であり、Cisco vBond オーケストレーションには関係しません。**[Advanced Options]** 領域にある **[vBond Only]** と **[Local vBond]** で、**[On]** をクリックします。これらの2つのパラメータにより、Cisco vBond オーケストレーションがインスタンス化されます。

2. VPN 0（インターネットまたは他のパブリック トランスポート ネットワークに接続する VPN）用と VPN 512（アウトオブバンド管理トラフィックを処理する VPN）用の 2 つの VPN テンプレートを作成します。
 3. AAA テンプレートとセキュリティテンプレートを作成します。
11. Cisco vBond オーケストレーション で有効にする機能ごとに、機能テンプレートを作成します。
 1. アーカイブテンプレートおよびバナーテンプレートの作成
 2. Cisco vBond オーケストレーション で設定する追加のイーサネット インターフェイスごとに 1 つのインターフェイス イーサネット テンプレートを作成します。Cisco vBond オーケストレーション については、トンネルインターフェイス（またはあらゆる種類のトンネル）を作成しないでください。

デバイステンプレートの作成

デバイステンプレートには、デバイスの完全な運用設定のすべてまたは大部分が含まれています。デバイステンプレートは、個々の機能テンプレートを統合して作成します。Cisco vManage で CLI テキスト形式の設定を直接入力して作成することもできます。どちらのスタイルのデバイステンプレートも、Cisco vBond オーケストレーション を設定するときに使用できます。

機能テンプレートから vBond デバイステンプレートを作成するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** の順に選択します。
2. **[Device Template]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Templates]** は **[Device]** と呼ばれます。

3. **[Create Template]** ドロップダウンから、**[From Feature Template]** を選択します。
4. **[Device Model]** ドロップダウンから、**[Cloud router]** を選択します。
5. Cisco vBond オーケストレーション デバイステンプレートの名前と説明を入力します。これらのフィールドは必須です。テンプレート名には特殊文字を使用できません。
6. **[Load Running config from reachable device]** ドロップダウンから、必要なテンプレートのグループを選択します。
7. 各セクションで、目的のテンプレートを選択します。必須テンプレートにはすべて、アスタリスク (*) のマークが付いています。最初は、各テンプレートのドロップダウンにデフォルトの機能テンプレートが一覧表示されます。
 1. 必須およびオプションの各テンプレートについて、ドロップダウンから機能テンプレートを選択します。これらのテンプレートは以前に作成したものです（上の「機能テン

プレートの作成」を参照)。Cisco vBond オーケストレーションでは BFD または OMP テンプレートを選択しないでください。

- 追加のテンプレートについては、テンプレート名の横にあるプラス (+) 記号をクリックし、ドロップダウンから機能テンプレートを選択します。
- [作成 (Create)] をクリックします。新しいデバイステンプレートが [Templates] テーブルに表示されます。[Feature Templates] 列には、デバイステンプレートに含まれている機能テンプレートの数が表示され、[Type] 列には、デバイステンプレートが機能テンプレートのコレクションから作成されたことを示す「Feature」が表示されます。

Cisco vManage で直接 CLI テキスト形式の設定を入力してデバイステンプレートを作成するには、次の手順を実行します。

- Cisco vManage メニューから、[Configuration] > [Templates] の順に選択します。
- [Device Template] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。

- [Create Template] ドロップダウンから、[CLI Template] を選択します。
- テンプレート名と説明を入力します。
- [Config Preview] ウィンドウに設定を入力します。タイプ入力、カットアンドペースト、またはファイルをアップロードします。
- 実際の設定値を変数に変換するには、値を選択して [Create Variable] をクリックします。変数名を入力し、[Create Variable] をクリックします。{{variable-name}} の形式で変数名を直接入力することもできます ({{hostname}} など)。
- [Add] をクリックします。新しいデバイステンプレートが [Templates] テーブルに表示されます。[Feature Templates] 列には、デバイステンプレートに含まれている機能テンプレートの数が表示され、[Type] 列には、デバイステンプレートが CLI テキストから作成されたことを示す「CLI」が表示されます。

Cisco vBond オーケストレーションへのデバイステンプレートのアタッチ

Cisco vBond オーケストレーションを設定するには、1つのデバイステンプレートをオーケストレータにアタッチします。同じテンプレートを複数の Cisco vBond オーケストレーションに同時にアタッチできます。

Cisco vBond オーケストレーションにデバイステンプレートをアタッチするには、次の手順を実行します。

- Cisco vManage メニューから、[Configuration] > [Templates] の順に選択します。

2. [Device Template] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。

3. 目的のデバイステンプレートを選択します。
4. 選択した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。
5. [Attach Devices] 列で [Available Devices] リストから目的の Cisco vBond オーケストレーションを選択し、右向き矢印をクリックしてそれらを [Selected Devices] 列に移動させます。1 つ以上のオーケストレータを選択できます。リストされているすべてのオーケストレータを選択するには、[Select All] をクリックします。
6. [Attach] をクリックします。

オーバーレイネットワークへの Cisco vBond オーケストレーションの追加

Cisco vBond オーケストレーションの最小限の構成を作成したら、Cisco vManage に Cisco vBond オーケストレーションを認識させてオーバーレイネットワークに構成を追加する必要があります。Cisco vBond オーケストレーションを追加すると、署名付き証明書が生成され、オーケストレータの検証と認証に使用されます。

Cisco vBond オーケストレーションの追加と証明書の生成

Cisco vBond オーケストレーションをネットワークに追加するには、CSR を自動的に生成させ、署名付き証明書をインストールします。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]** の順に選択します。
2. **[Controllers]** をクリックし、**[Add Controller]** ドロップダウンから **[vBond]** を選択します。
3. **[Add vBond]** ウィンドウで、次の手順を実行します。
 1. vBond の管理 IP アドレスを入力します。
 2. ユーザ名とパスワードを入力して、Cisco vBond オーケストレーションにアクセスします。
 3. **[Generate CSR]** チェックボックスをオンにして、証明書生成プロセスを自動的に実行できるようにします。
 4. **[Add]** をクリックします。

Cisco vManage は CSR を生成し、生成した証明書を取得して、Cisco vBond オークストレーションに自動的にインストールします。新しいコントローラデバイスは、コントローラタイプ、コントローラのホスト名、IP アドレス、サイト ID、およびその他の詳細とともに [Controller] テーブルに表示されます。

証明書のインストールの確認

Cisco vBond オークストレーションに証明書がインストールされていることを確認するには、次の手順を実行します。

1. Cisco vManage メニューから、[Configuration] > [Devices] の順に選択します。
2. 表示されている新しいデバイスを選択し、[Certificate Status] 列をチェックして、証明書がインストールされていることを確認します。

エンタープライズ ZTP サーバーの起動

ZTP サーバーは、ZTP ワークフローを開始する前に設定する必要があります。

Cisco SD-WAN ゼロタッチプロビジョニング (ZTP) Cisco vBond オークストレーションサーバーをホストしている企業の場合は、このロールを実行するように Cisco vBond オークストレーションを 1 つ設定する必要があります。この Cisco vBond オークストレーションがオーバーレイネットワークの Cisco vEdge デバイスにエンタープライズ Cisco vBond オークストレーションの IP アドレスとエンタープライズルート CA チェーンを提供します。この Cisco vBond オークストレーションサーバーは、インターネットのトップレベルドメインサーバーと同様のトップレベル Cisco vBond オークストレーションと考えることができます。

Cisco SD-WAN ZTP ホステッドサービスを使用している場合は、トップレベル Cisco vBond オークストレーションを設定する必要はありません。

このセクションでは、Cisco vBond オークストレーションを起動して初期設定を実行する方法について、段階を追って説明します。

ZTP の要件

Cisco vBond オークストレーション ソフトウェアを起動するには、次のハードウェアおよびソフトウェアコンポーネントが必要です。

- Cisco vBond オークストレーション ソフトウェアがインストールされている Cisco vEdge デバイス、またはハイパーバイザー上の Cisco vBond オークストレーション VM インスタンス。
- 適切な電源ケーブル。ハードウェアプラットフォームの梱包明細書を参照してください。
- URL `ztp.cisco.com` をエンタープライズ ZTP サーバーにリダイレクトする、レコードを使用して設定されたエンタープライズ DNS サーバー。このエンタープライズサーバーの推奨 URL は `ztp.local-domain` です。
- 証明書署名要求 (CSR) の結果として生成された証明書。

- エンタープライズルート CA チェーン。
- Cisco vEdge デバイスの Cisco SD-WAN リリース 20.1.1 のリリースの場合、ZTP サーバーとして動作する Cisco vBond オーケストレーションに必要な Cisco vEdge デバイス シャーシ情報を含む CSV ファイル。CSV ファイルの各行には、各 Cisco vEdge デバイス について次の情報が含まれている必要があります。



(注) ztp-server は、cisco-pki または symantec (Digicert) から署名された csr-cert である必要があります。



(注) Microsoft Windows を含む一部のオペレーティングシステムでは、このファイルの各行の最後にキャリッジリターンの特殊文字 (^M など) が追加される場合があります。ファイルをアップロードする前に、テキストエディタを使用してこれらの文字を削除してください。

- vEdge ルータのシャーシ番号
 - vEdge ルータのシリアル番号
 - 有効性 (有効または無効)
 - Cisco vBond オーケストレーションの IP アドレス
 - Cisco vBond オーケストレーションのポート番号 (値の入力はオプション)
 - デバイス証明書で指定されている組織名
 - エンタープライズルート証明書へのパス (値の入力はオプション)
-
- Cisco vEdge デバイスの Cisco SD-WAN リリース 20.3.1 以降のリリースの場合、ZTP サーバーとして動作する Cisco vBond オーケストレーションのルータシャーシ情報を含む JSON ファイル。このファイルは、PNP ポータルでダウンロードした zip バンドルデバイスファイルから抽出されます。JSON ファイルには、各ルータに関する次の情報が含まれています。
 - デバイス証明書で指定されている組織名
 - 証明書情報
 - ルータのシャーシ番号
 - ルータのシリアル番号
 - 有効性 (有効または無効)
 - Cisco vBond オーケストレーションの IP アドレス

- Cisco vBond オーケストレーション のポート番号 (任意)



- (注) エッジデバイスをアップグレードする前に、オンプレミスの ZTP サーバーが、Cisco vManage、Cisco vSmart、および Cisco vBond に使用している Cisco SD-WAN コントローラのリリースと同じリリース番号 (またはそれ以降) を使用していることを確認してください。たとえば、Cisco vManage リリース 20.6.x から Cisco vManage リリース 20.9.x にアップグレードする前に、ZTP サーバーがリリース 20.9 以降を使用していることを確認してください。

Cisco SD-WAN リリース 20.4.1 以降、PNP ポータルのコントローラプロファイルでマルチテナント機能が有効になっている場合、JSON ファイルには SP 組織名も含まれます。

Cisco SD-WAN リリース 20.3.1 の場合、PNP ポータルからシャーシ ZIP ファイルをダウンロードし、そこから JSON ファイルを抽出します。次のコマンドを使用して、JSON ファイルを ZTP サーバーにアップロードします。

```
vBond# request device-upload chassis-file JSON-file-name
```

JSON ファイルの例を次に示します。

```
{
    "version": "1.1",
    "organization": "vIptela Inc Regression",
    "overlay": "vIptela Inc Regression",
    "root_cert_bundle": "-----BEGIN CERTIFICATE-----
<certificate>
----END CERTIFICATE-----\n-----BEGIN CERTIFICATE-----
<certificate>
----END CERTIFICATE-----",
    "controller_details": {
        "primary_ipv4": "10.0.12.26",
        "primary_port": "12346"
    },
    "chassis_list": [{
        "chassis": "JAE214906FZ",
        "SKU": "ASR1002-HX",
        "HWPID": "ASR1002-HX",
        "serial_list": [{
            "sudi_subject_serial": "JAE214906FX",
            "sudi_cert_serial": "021C0203",
            "HWPID": "ASR1002-HX"}]
        }
    ],
    "timestamp": "2019-10-21 23:40:02.248"
}
```

Cisco SD-WAN リリース 20.3.2 以降、PNP ポータルからダウンロードしたシャーシの ZIP ファイルから JSON ファイルを抽出する必要はなくなります。request device-upload chassis-file コマンドを使用して、PNP ポータルからダウンロードした serialFile.Viptela ファイルを ZTP サーバーにアップロードします。ZTP サーバーは、serialFile.Viptela から JSON ファイルを抽出し、シャーシエントリをデータベースにロードします。

```
vBond# request device-upload chassis-file /home/admin/serialFile.viptela
Uploading chassis numbers via VPN 0
Copying ... /home/admin/serialFile.viptela via VPN 0
file: /tmp/tmp.DkaQ18u3aM/viptela_serial_file
PnP
Verifying public key received from PnP against production root cert
is_public_key_ok against production root ca: 0 = Cisco, CN = MMI Signer STG - DEV
error 20 at 0 depth lookup:unable to get local issuer certificate
Verifying public key received from PnP against engineering root cert
is_public_key_ok against engineering root ca: OK
Signature verified for viptela_serial_file
final file: /tmp/tmp.DkaQ18u3aM/viptela_serial_file
Removing unsigned file (cisco_cert.cer).
Signature verification Succeeded.
Success: Serial file is /tmp/tmp.DkaQ18u3aM/viptela_serial_file
INFO: Input File specified was '/usr/share/viptela/chassis_numbers.tmp'
INFO: Root Cert File is /home/admin/vIPtela Inc Regression.crt
INFO: # of complete chassis entries written: 19
Json to CSV conversion succeeded!
Successfully loaded the chassis numbers file to the database.
```

必要に応じて、**request device** コマンドを使用して Cisco vEdge デバイスの情報を手動で設定できます。

ルータを ZTP サーバーに設定する

トップレベル Cisco vBond オーケストレーション ソフトウェアを起動して初期設定を行うには、次の手順を実行します。

1. Cisco vEdge デバイスをブートします。
2. コンソールケーブルを使用して、PC を Cisco vEdge デバイスに接続します。
3. デフォルトのユーザー名 **admin** とデフォルトのパスワード **admin** を使用して Cisco vEdge デバイスにログインします。CLI プロンプトが表示されます。
4. Cisco vEdge デバイスをトップレベル Cisco vBond オーケストレーションに設定します。

```
vBond# config
vBond(config)# system vbond ip-address local ztp-server
```

トランスポートネットワークを介してすべての vSmart コントローラおよび Cisco vEdge デバイスが Cisco vBond オーケストレーションに到達できるように、IP アドレスはパブリックアドレスである必要があります。**local** オプションは、この Cisco vEdge デバイスが Cisco vBond オーケストレーションとして機能していることを示します。このオプションが、Cisco vEdge デバイスで Cisco vBond オーケストレーションソフトウェアプロセスを開始します。**ztp-server** オプションは、この Cisco vBond オーケストレーションを ZTP サーバーとして規定します。

5. トランスポートネットワークに接続するインターフェイスの IP アドレスを設定します。

```
vBond(config)# vpn 0 interface ge slot/port
vBond(config-ge)# ip address prefix/length
vBond(config-ge)# no shutdown
```

6. 設定をコミットします。

```
vBond(config)# commit
```

7. コンフィギュレーション モードを終了します。

```
vBond(config)# exit
```

8. 設定が正しく、完全であることを確認します。

```
vBond# show running-config
system
  host-name                vm3
  system-ip                172.16.255.2
  admin-tech-on-failure
  route-consistency-check
  organization-name        "Cisco Inc"
  vbond 10.1.15.13 local  ztp-server
```

9. CSR を手動で生成します。

```
vbond_ztp# request csr upload home/admin/vbond_ztp.csr
```

10. CSR に手動で署名し、PNP Connect Cisco PKI を介して証明書を生成するか、クラウド運用を介して Symantec 証明書を生成します。

11. 証明書のインストール :

```
vbond_ztp# request certificate install/home/admin/vbond_ztp.cer
```

12. Cisco IOS XE SD-WAN の root-ca チェーンに Cisco root-ca-cert または Symantec root-ca-cert があることを確認します。

13. vBond_ZTP と Cisco IOS XE SD-WAN のクロックを確認します。

14. ルータシャーシ情報を含む JSON ファイルを ZTP サーバーにアップロードします。

```
vBond# request device-upload chassis-file path
```

path は、FTP、TFTP、HTTP、または SCP 経由で到達可能なローカルファイルまたはリモートデバイス上のファイルへのパスです。

15. 次のいずれかのコマンドを使用して、Cisco vEdge デバイスシャーシ番号のリストが Cisco vBond オーケストレーションに存在することを確認します。

```
vBond# show ztp entries
vBond# show orchestrator valid-devices
```

トップレベル Cisco vBond オーケストレーション の設定例を次に示します。

```
vBond# show running-config vpn 0
interface ge0/0
  ip address 75.1.15.27/24
  !
  no shutdown
  !

vBond# show running-config system
system
  vbond 75.1.15.27 local  ztp-server
  !
```

次のステップ

vSmart コントローラの展開を参照してください。

vContainer ホスト

vContainer ホストのサポートは延期されました。vContainer ホストの詳細については、[延期の通知](#)を参照してください。

Cisco vSmart コントローラの導入

Cisco vSmart コントローラは、Cisco SD-WAN オーバーレイネットワークの集中型コントロールプレーンの頭脳であり、集中型ルーティングテーブルと集中型ルーティングポリシーを維持します。ネットワークが運用可能になると、Cisco vSmart コントローラは、各 vEdge ルータへの DTLS コントロールプレーンの直接接続を維持することにより、その制御に影響を与えません。Cisco vSmart コントローラは、ネットワークサーバー上で仮想マシン (VM) として動作します。

Cisco SD-WAN オーバーレイネットワークには、1 つ以上の Cisco vSmart コントローラを含めることができます。Cisco vSmart コントローラは、オーバーレイネットワーク全体のデータトラフィックフローを制御する手段を提供します。冗長性を実現するために、オーバーレイネットワークに 2 つ以上の Cisco vSmart コントローラを含めることをお勧めします。単一の Cisco vSmart コントローラで最大 2,000 の制御セッション (つまり、最大 2,000 の TLOC) をサポートできます。Cisco vManage または vManage クラスタは、オーバーレイネットワーク内の最大 20 の Cisco vSmart コントローラをサポートできます。

Cisco vSmart コントローラを展開するには、次の手順を実行します。

1. ESXi または KVM ハイパーバイザのいずれかで vSmart VM インスタンスを作成します。
2. Cisco vSmart コントローラの最小限の構成を作成し、ネットワーク上でアクセスできるようにします。作成するには、SSH を使用して Cisco vSmart コントローラへの CLI セッションを開き、デバイスを手動で設定します。
3. Cisco vSmart コントローラをオーバーレイネットワークに追加して、Cisco vManage が認識できるようにします。
4. Cisco vSmart コントローラの完全な構成を作成します。これを行うには、Cisco vSmart コントローラの vManage テンプレートを作成し、そのテンプレートをコントローラにアタッチします。vManage テンプレートをアタッチすると、初期の最小限の構成が上書きされます。

ESXi での vSmart VM インスタンスの作成

Cisco vSmart コントローラを起動するには、ハイパーバイザソフトウェアを実行しているサーバー上にその仮想マシン (VM) インスタンスを作成する必要があります。ここでは、VMware vSphere ESXi ハイパーバイザソフトウェアを実行しているサーバー上に VM を作成する方法について説明します。カーネルベースの仮想マシン (KVM) ハイパーバイザソフトウェアを実行しているサーバー上に VM を作成することもできます。

サーバーの要件については、「サーバーハードウェアの推奨事項」を参照してください。
ESXi ハイパーバイザで vSmart VM インスタンスを作成するには、次の手順を実行します。

1. vSphere Client を起動し、vSmart VM インスタンスを作成します。
2. 管理インターフェイス用の vNIC を追加します。
3. vSmart VM インスタンスを起動し、コンソールに接続します。

各ステップの詳細を以下に示します。

VMware vCenter Server を使用して vSmart VM インスタンスを作成している場合は、同じ手順に従います。ただし、vCenter Server のページは、手順に示されている vSphere Client のページとは異なることに注意してください。

vSphere Client の起動および vSmart VM インスタンスの作成

1. VMware vSphere Client アプリケーションを起動し、ESXi サーバーの IP アドレスまたは名前、ユーザー名、およびパスワードを入力します。[Login] をクリックして、ESXi サーバーにログインします。
[ESXi] 画面が表示されます。
2. [File] > [Deploy OVF Template] をクリックして、仮想マシンを展開します。
3. [Deploy OVF Template] 画面で、OVF パッケージをインストールしてダウンロードする場所を入力します。このパッケージは、シスコからダウンロードした vsmart.ova ファイルです。次に、[Next] をクリックします。
4. [Next] をクリックして、OVF テンプレートの詳細を確認します。
5. 展開したテンプレートの名前を入力し、[Next] をクリックします。次の図は、vSmart インスタンスの名前を示しています。
6. [Next] をクリックして、仮想ディスクのデフォルトのフォーマットを受け入れます。
7. [Next] をクリックして、展開された OVF テンプレートの宛先ネットワークとして、使用している宛先ネットワークを受け入れます。下の図では、CorpNet が宛先ネットワークです。
8. [Ready to Complete] ページで [Finish] をクリックします。次の図は、vSmart インスタンスの名前を示しています。

定義したパラメータを使用して VM インスタンスが正常に作成され、[Getting Started] が選択された状態で [vSphere Client] ページが表示されます。デフォルトでは、vNIC が 1 つ含まれています。この vNIC は、トンネルインターフェイスに使用されます。

管理インターフェイス用の vNIC の追加

1. vSphere Client の左側のナビゲーションバーで、作成したばかりの vManage VM インスタンスを選択し、[Edit virtual machine settings] をクリックします。

2. [vManage – Virtual Machine Properties] ページで、[Add] をクリックして、管理インターフェイス用の新しい vNIC を追加します。次に [OK] をクリックします。
3. 追加するデバイスのタイプの [Ethernet Adapter] をクリックします。次に、[Next] をクリックします。
4. [Adapter Type] ドロップダウンで、追加する vNIC の VMXNET3 を選択して、[Next] をクリックします。
5. [Ready to Complete] ページで [Finish] をクリックします。
6. [vManage – Virtual Machine Properties] ページが開き、新しい vNIC が追加されていることが示されます。[OK] をクリックして [vSphere Client] ページに戻ります。

vSmart VM インスタンスの起動とコンソールへの接続

1. vSphere Client の左側のナビゲーションバーで、作成した仮想マシンインスタンスを選択し、[Power on the virtual machine] をクリックします。vSmart 仮想マシンの電源が入ります。
2. [Console] を選択して、vSmart コンソールに接続します。
3. ログインプロンプトで、デフォルトのユーザー名 **admin** およびデフォルトのパスワード **admin** を使用してログインします。

次のステップ

「Cisco vSmart コントローラ の設定」を参照してください。

KVM での vSmart VM インスタンスの作成

vSmart コントローラを起動するには、ハイパーバイザソフトウェアを実行しているサーバー上に vSmart コントローラの仮想マシン (VM) インスタンスを作成する必要があります。ここでは、カーネルベースの仮想マシン (KVM) ハイパーバイザソフトウェアを実行しているサーバー上に VM を作成する方法について説明します。VMware vSphere ESXi ハイパーバイザソフトウェアを実行しているサーバー上に VM を作成することもできます。

サーバーの要件については、「サーバーハードウェアの推奨事項」を参照してください。

KVM ハイパーバイザで vSmart VM インスタンスを作成するには、次の手順を実行します。

1. Virtual Machine Manager (virt-manager) クライアントアプリケーションを起動します。[Virtual Machine Manager] ページが表示されます。
2. [New] をクリックして、仮想マシンを展開します。[Create a new virtual machine] ページが開きます。
3. 仮想マシンの名前を入力します。次の図は、vSmart インスタンスの名前を示しています。
 1. [Import existing disk image] を選択します。

2. [続行 (Forward)] をクリックします。
4. [Provide the existing storage path] フィールドで、[Browse to find the vEdge Cloud software image] をクリックします。
 1. [OS Type] は [Linux] を選択します。
 2. [Version] で、実行している Linux バージョンを選択します。
 3. [続行 (Forward)] をクリックします。
5. ネットワークトポロジとサイトの数に基づいてメモリと CPU を指定し、[Forward] をクリックします。
6. [Customize configuration before install] チェックボックスをオンにします。その後、[Finish] をクリックします。
7. 左側のナビゲーションバーで [Disk 1] を選択します。実行されるアクション
 1. [Advanced Options] をクリックします。
 2. [Disk Bus] フィールドで、[IDE] を選択します。
 3. [Storage Format] フィールドで、[qcow2] を選択します。
 4. [Apply] をクリックして、定義したパラメータで VM インスタンスを作成します。デフォルトでは、vNIC が 1 つ含まれています。この vNIC は、トンネルインターフェイスに使用されます。



(注) ソフトウェアは VMXNET3 vNIC のみをサポートします。

8. [vSmart Virtual Machine] ページで、[Add Hardware] をクリックして、管理インターフェイスに 2 つ目の vNIC を追加します。
9. [Add New Virtual Hardware] ページで [Network] をクリックします。
 1. [Host Device] フィールドで、適切なホストデバイスを選択します。
 2. [Finish] をクリックします。
新しく作成された vNIC が左側のペインに表示されます。この vNIC は、管理インターフェイスに使用されます。
10. [vSmart Virtual Machine] ページで、画面の左上隅にある [Begin Installation] をクリックします。
11. 仮想マシンインスタンスが作成され、vSmart コンソールが表示されます。
12. ログインプロンプトで、デフォルトのユーザー名 **admin** およびデフォルトのパスワード **admin** を使用してログインします。

次のステップ

「Cisco vSmart コントローラ の設定」を参照してください。

vSmart コントローラの設定

オーバーレイネットワークで vSmart コントローラ用の仮想マシン (VM) をセットアップして起動すると、仮想マシンは工場出荷時のデフォルト設定で起動します。次に、デバイスが認証および検証され、オーバーレイネットワークに参加できるように、いくつかの基本的な機能を手動で設定する必要があります。設定する機能には、ネットワークの vBond Orchestrator の IP アドレス、デバイスのシステム IP アドレス、およびネットワーク コントローラ デバイス (vBond、vManage、および vSmart デバイス) 間で制御トラフィックを交換するために使用する VPN 0 のトンネルインターフェイスが含まれます。

オーバーレイネットワークを動作させ、vSmart コントローラをオーバーレイネットワークに参加させるには、次の手順を実行します。

- VPN 0 の少なくとも 1 つのインターフェイスでトンネルインターフェイスを設定します。トンネルインターフェイスは、すべての Cisco vEdge デバイスからアクセス可能な WAN トランスポートネットワークに接続する必要があります。VPN 0 は、オーバーレイネットワーク内の Cisco vEdge デバイス間ですべてのコントロールプレーントラフィックを伝送します。
- オーバーレイ管理プロトコル (OMP) が有効になっていることを確認します。OMP は、Cisco SD-WAN コントロールプレーンの確立と維持を行うプロトコルで、デフォルトで有効になっており、無効化できません。CLI から構成を編集する場合は、**omp** 構成コマンドを削除しないでください。

これらの初期構成を作成するには、SSH を使用して vSmart コントローラへの CLI セッションを開きます。

初期構成を作成したら、vManage NMS で構成テンプレートを作成し、vSmart コントローラに添付することにより、完全な構成を作成します。構成テンプレートを vSmart コントローラに添付すると、テンプレートの構成パラメータによって初期構成が上書きされます。

この初期構成では、システム IP アドレスを vSmart コントローラに割り当てる必要があります。このアドレスは、Cisco 以外の SD-WAN ルータのルータ ID に似ており、インターフェイスアドレスとは独立してコントローラを識別する永続的なアドレスです。システム IP は、デバイスの TLOC アドレスのコンポーネントです。デバイスのシステム IP アドレスを設定すると、Cisco vEdge デバイスの到達可能性に影響を与えることなく、必要に応じてインターフェイスの番号を付け直すことができます。vSmart コントローラと vEdge ルータ間、および vSmart コントローラと vBond Orchestrator 間のセキュアな DTLS または TLS 接続を介した制御トラフィックは、システム IP アドレスによって識別されるシステムインターフェイスを介して送信されます。トランスポート VPN (VPN 0) では、システム IP アドレスがデバイスのループバックアドレスとして使用されます。同じアドレスを VPN 0 の別のインターフェイスに使用することはできません。



- (注) オーバーレイネットワークが適切かつ予測どおりに機能するには、すべての vSmart コントローラに設定されているポリシーが同一である必要があります。

vSmart コントローラの初期構成の作成

CLI セッションから vSmart コントローラで初期構成を作成するには、次の手順を実行します。

1. SSH 経由で Cisco vEdge デバイスへの CLI セッションを開きます。
2. **admin** ユーザーとして、デフォルトのパスワード **admin** を使用してログインします。CLI プロンプトが表示されます。
3. コンフィギュレーション モードに入ります。

```
vSmart# config
vSmart(config)#
```

4. ホスト名を設定します。

```
Cisco(config)# system host-name hostname
```

ホスト名の設定は任意ですが、ホスト名は CLI のプロンプトの一部として含まれ、さまざまな Cisco vManage ページでデバイスを参照するために使用されるため、設定することを推奨します。

5. システム IP アドレスを設定します。リリース 16.3 以降では、IP アドレスは IPv4 または IPv6 アドレスになります。以前のリリースでは、IPv4 アドレスである必要があります。リリース 19.1 以降では、IPv6 の一意のローカルアドレスは設定できません。リリース 19.1 以降では、FC00::/7 プレフィックス範囲から IPv6 アドレスを設定します。



- (注) Cisco SD-WAN コントローラリリース 20.9.x リリース以降は、一意のローカル IPv6 アドレスを設定できます。これより前のリリースでは、FC00::/7 プレフィックス範囲から IPv6 アドレスを設定できません。

```
vSmart(config-system)#system-ip ip-address
```

Cisco vManage はシステム IP アドレスを使用してデバイスを識別し、NMS が完全な構成をデバイスにダウンロードできるようにします。

6. デバイスが配置されているサイトの数値識別子を設定します。

```
vSmart(config-system)# site-id site-id
```

7. デバイスが配置されているドメインの数値識別子を設定します。

```
vSmart(config-system)# domain-id domain-id
```

8. Cisco vBond オーケストレーションの IP アドレスか、Cisco vBond オーケストレーションを指す DNS 名を設定します。Cisco vBond オーケストレーションの IP アドレスは、オー

オーバーレイネットワーク内のすべての Cisco vEdge デバイスが到達できるように、パブリック IP アドレスにする必要があります。

```
vSmart(config-system)# vbond (dns-name | ip-address)
```

9. ソフトウェアアップグレードの成功を確認するための時間制限を設定します。

```
vSmart(config-system)# upgrade-confirm minutes
```

時間の範囲は 1 ~ 60 分です。この時間制限を設定する場合、デバイスのソフトウェアアップグレード時、Cisco vManage の起動時、または設定された分数以内にソフトウェアアップグレードが成功することを確認する必要があります。設定時間内に確認メッセージを受信しない場合、デバイスは以前のソフトウェアイメージに戻ります。

10. ユーザー「admin」のパスワードを変更します。

```
vSmart(config-system)# user admin password password
```

デフォルトのパスワードは「admin」です。

11. VPN 0 のインターフェイスをトンネルインターフェイスとして使用するよう設定します。VPN 0 は WAN トランスポート VPN であり、トンネルインターフェイスはオーバーレイネットワーク内のデバイス間で制御トラフィックを伝送します。インターフェイス名の形式は **eth** 番号です。インターフェイスを有効にして、その IP アドレスを静的アドレスとして、または DHCP サーバーから受信した動的に割り当てられたアドレスとして設定する必要があります。リリース 16.3 以降では、アドレスを IPv4 または IPv6 アドレスにするか、両方を設定してデュアルスタック操作を有効にできます。以前のリリースでは、IPv4 アドレスである必要があります。

```
vSmart(config)# vpn 0
vSmart(config-vpn-0)# interface interface-name
vSmart(config-interface)# ( ip dhcp-client | ip address prefix/length)
vSmart(config-interface)# (ipv6 address ipv6-prefix/length | ipv6 dhcp-client [
dhcp-distance number | dhcp-rapid-commit])
vSmart(config-interface)# no shutdown
vSmart(config-interface)# tunnel-interface
vSmart(config-tunnel-interface)# allow-service netconf
```



- (注) オーバーレイネットワークが起動し、Cisco vSmart コントローラがオーバーレイネットワークに参加できるようにするには、VPN 0 の少なくとも 1 つのインターフェイスでトンネルインターフェイスを設定する必要があります。トンネルインターフェイスは、すべての Cisco vEdge デバイスからアクセス可能な WAN トランスポートネットワークに接続する必要があります。VPN 0 は、オーバーレイネットワーク内の Cisco vEdge デバイス間ですべてのコントロールプレーントラフィックを伝送します。

12. WAN トランスポートのタイプを識別するために、トンネルの色を設定します。デフォルトの色 (**default**) を使用できますが、実際の WAN トランスポートに応じて、**mpls** や **metro-ethernet** など、より適切な色も設定できます。

```
vSmart(config-tunnel-interface)# color color
```

13. WAN トランスポートネットワークへのデフォルトルートを設定します。

```
vSmart(config-vpn-0)# ip route 0.0.0.0/0 next-hop
```

14. 設定をコミットします。

```
vSmart(config)# commit and-quit
vSmart#
```

15. 設定が正しく、完全であることを確認します。

```
vSmart# show running-config
```

オーバーレイネットワークが起動して動作可能になったら、初期構成パラメータを含むvSmart構成テンプレートをCisco vManageで作成します。次のvManage機能テンプレートを使用します。

- ホスト名、システム IP アドレス、および vBond 機能を設定するためのシステム機能テンプレート。
- 「admin」ユーザーのパスワードを設定するための AAA 機能テンプレート。
- インターフェイス、デフォルトルート、および VPN 0 の DNS サーバーを設定するための VPN インターフェイスイーサネット機能テンプレート。

さらに、次の一般的なシステムパラメータを設定することを推奨します。

- Cisco vManage メニューから、**[Administration]** > **[Settings]**の順に選択し、組織名を設定します。
- Cisco vManage メニューから、**[Configuration]** > **[Templates]**の順に選択し、以下の項目を設定します。
- NTP およびシステム機能構成テンプレートの場合、タイムゾーン、NTP サーバー、およびデバイスの物理的な場所を設定します。
- バナー機能テンプレートの場合、ログインバナーを設定します。
- ログ機能構成テンプレートの場合、ログ機能パラメータを設定します。
- AAA 機能構成テンプレートの場合、AAA、RADIUS、および TACACS+ サーバーを設定します。
- SNMP 機能構成テンプレートの場合、SNMP を設定します。

CLI 初期設定の例

以下は、vSmart コントローラの単純な構成の例です。この構成には、工場出荷時のデフォルト設定の設定が多数含まれており、多数のデフォルト設定値が示されています。

```
vSmart# show running-config
system
 host-name          vSmart
 gps-location latitude 40.7127837
 gps-location longitude -74.00594130000002
 system-ip          172.16.240.172
 site-id            200
 organization-name  "Cisco"
```

```
clock timezone America/Los_Angeles
upgrade-confirm 15
vbond 184.122.2.2
aaa
  auth-order local radius tacacs
  usergroup basic
    task system read write
    task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
    task system read
    task interface read
    task policy read
    task routing read
    task security read
  !
  user admin
    password encrypted-password
  !
!
logging
  disk
  enable
!
server 192.168.48.11
  vpn 512
  priority warm
exit
!
!
omp
  no shutdown
  graceful-restart
!
snmp
  no shutdown
  view v2
  oid 1.3.6.1
!
community private
  view v2
  authorization read-only
!
trap target vpn 0 10.0.1.1 16662
  group-name Cisco
  community-name private
!
trap group test
  all
  level critical major minor
  exit
exit
!
vpn 0
  interface eth1
  ip address 10.0.12.22/24
  tunnel-interface
  color public-internet
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
```

```

    allow-service netconf
    no allow-service ntp
    no allow-service stun
    !
    no shutdown
    !
    vpn 512
    interface eth0
    ip dhcp-client
    no shutdown
    !
    !

```

次のステップ

「オーバーレイネットワークへの vSmart コントローラの追加」を参照してください。

Cisco vSmart コントローラの構成テンプレートの作成

Cisco vManage によって管理されている Cisco vSmart コントローラの場合は、Cisco vManage から設定する必要があります。Cisco vSmart コントローラで CLI から直接設定すると、Cisco vManage により Cisco vManage に保存されている設定で上書きされます。

設定要件

セキュリティの前提条件

シスコのオーバーレイネットワークで Cisco vSmart コントローラを設定する前に、Cisco vSmart コントローラの証明書を生成して、証明書をデバイスにインストールしておく必要があります。「証明書の生成」を参照してください。

変数スプレッドシート

作成する機能テンプレートには、ほとんどの場合、変数が含まれます。デバイステンプレートをデバイスにアタッチするときに、Cisco vManage が変数に実際の値を入力するには、値を手動で入力するか、右上隅にある [Import File] をクリックして、変数値を含む CSV 形式の Excel ファイルをロードします。

スプレッドシートでは、ヘッダー行に変数名が含まれ、後続の各行はデバイスに対応し、変数の値が定義されます。スプレッドシートの最初の 3 つの列は順番どおりである必要があります。

- csv-deviceId : デバイスのシリアル番号 (デバイスを一意に識別するために使用)。
- csv-deviceIP : デバイスのシステム IP アドレス (**system ip address** コマンドの入力に使用)。
- csv-host-name : デバイスのホスト名 (**system hostname** コマンドの入力に使用)。

オーバーレイネットワーク内のすべてのデバイス (ルータ、Cisco vSmart コントローラ、および Cisco vBond オーケストレーション) に対して 1 つのスプレッドシートを作成できます。全デバイスのすべての変数に値を指定する必要はありません。

Cisco vSmart コントローラの機能テンプレート

次の機能はCisco vSmart コントローラの操作に必須であるため、それぞれの機能テンプレートを作成する必要があります。

機能	テンプレート名
認証、許可、アカウントिंग (AAA)	AAA
オーバーレイ マネジメント プロトコル (OMP)	OMP
セキュリティ	セキュリティ
システム全体のパラメータ	システム
トランスポート VPN (VPN 0)	VPN ID が 0 に設定された VPN
管理VPN (アウトオブバンド管理トラフィック用)	VPN ID が 512 に設定された VPN

機能テンプレートの作成

機能テンプレートは、Cisco vSmart コントローラの完全な構成の構成要素です。Cisco vSmart コントローラ で有効にできる機能ごとに、Cisco vManage では、その機能に必要なパラメータを入力するテンプレートフォームが提供されます。

必須の Cisco vSmart コントローラ 機能の機能テンプレートを作成する必要があります。

同じ機能に対して複数のテンプレートを作成できます。

vSmart 機能テンプレートを作成するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration] > [Templates]**の順に選択します。
2. **[Feature Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Feature Templates]** は **[Feature]** と呼ばれます。

3. **[Add Template]** を選択します。
4. 左側のペインで、**[Select Devices]** から **[vSmart]** を選択します。Cisco vSmart コントローラ と他のデバイスの両方で使用できる機能に対して、1つの機能テンプレートを作成できます。ただし、Cisco vSmart コントローラ でのみ使用できるソフトウェア機能については、別の機能テンプレートを作成する必要があります。
5. 右側のペインで、テンプレートを選択します。テンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部にはそのテンプレートで使用可能なパラメータを定義するためのフィールドがあります。オブ

ションのパラメータは通常、グレー表示されています。同じパラメータに複数のエントリーを追加できる場合は、右側にプラス記号 (+) が表示されます。

6. テンプレート名と説明を入力します。これらのフィールドは必須です。テンプレート名には特殊文字を使用できません。
7. 必要な各パラメータについて、目的の値を選択し、該当する場合はパラメータの範囲を選択します。各パラメータフィールドの左側にあるドロップダウンメニューから範囲を選択します。
8. 必要なパラメータの下にあるプラス記号 (+) をクリックして、必要に応じて追加パラメータの値を設定します。
9. [作成 (Create)] をクリックします。
10. 前のセクションにリストされている必要な機能ごとに機能テンプレートを作成します。トランスポート VPN の場合は、VPN-vSmart というテンプレートを使用し、[VPN Template] セクションで、VPN を 0 に設定し、範囲を [Global] にします。管理 VPN の場合は、VPN-vSmart というテンプレートを使用し、[VPN Template] セクションで、VPN を 512 に設定し、範囲を [Global] にします。
11. Cisco vSmart コントローラ で有効にするオプション機能ごとに、追加の機能テンプレートを作成します。

デバイステンプレートの作成

デバイステンプレートは、デバイスの完全な運用構成が含まれます。デバイステンプレートは、個々の機能テンプレートを統合して作成します。Cisco vManage で CLI テキスト形式の設定を直接入力して作成することもできます。

Cisco vSmart コントローラ を設定するためにアタッチできるデバイステンプレートは1つだけであるため、少なくとも vSmart 構成の必要なすべての部分が含まれている必要があります。そうでない場合、Cisco vManage はエラーメッセージを返します。Cisco vSmart コントローラに2つ目のデバイステンプレートをアタッチすると、1つ目のデバイステンプレートが上書きされます。

機能テンプレートからデバイステンプレートを作成するには、次の手順を実行します。

1. Cisco vManage メニューから、[Configuration] > [Templates] の順に選択します。
2. [Device Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。

3. [Create Template] ドロップダウンから [From Feature Template] を選択します。
4. [Device Model] ドロップダウンリストから [vSmart] を選択します。

5. vSmart デバイステンプレートの名前と説明を入力します。これらのフィールドは必須です。テンプレート名には特殊文字を使用できません。
6. [Required Templates] セクションに入力します。必須テンプレートにはすべて、アスタリスクが付いています。
 1. 必須の各テンプレートについて、ドロップダウンリストから機能テンプレートを選択します。これらのテンプレートは以前に作成したものです（上の「機能テンプレートの作成」を参照）。テンプレートを選択すると、テンプレート名の横の円が緑色に変わり、緑色のチェックマークが表示されます。
 2. サブテンプレートのあるテンプレートの場合は、プラス (+) 記号またはサブテンプレートのタイトルをクリックして、サブテンプレートのリストを表示します。サブテンプレートを選択すると、サブテンプレートの名前とドロップダウンが表示されます。サブテンプレートが必須の場合は、その名前にアスタリスクが付いています。
 3. 目的のサブテンプレートを選択します。
7. 必要に応じて、[Optional Templates] セクションに入力します。次の手順を実行します。
 1. [Optional Templates] をクリックして、オプションの機能テンプレートをデバイステンプレートに追加します。
 2. 追加するテンプレートを選択します。
 3. テンプレート名をクリックし、特定の機能テンプレートを選択します。
8. [作成 (Create)] をクリックします。新しいデバイステンプレートが [Templates] テーブルに表示されます。[Feature Templates] 列には、デバイステンプレートに含まれている機能テンプレートの数が表示され、[Type] 列には、デバイステンプレートが機能テンプレートのコレクションから作成されたことを示す「Feature」が表示されます。

Cisco vManage で直接 CLI テキスト形式の設定を入力してデバイステンプレートを作成するには、次の手順を実行します。

1. Cisco vManage メニューから、[Configuration] > [Templates] の順に選択します。
2. [Device Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。

3. [Create Template] ドロップダウンリストから、[CLI Template] を選択します。
4. [Add Device CLI Template] ウィンドウで、テンプレートの名前と説明を入力し、[vSmart] を選択します。
5. [CLI Configuration] ボックスに構成を入力します（タイプ入力するか、切り取って貼り付けるか、ファイルをアップロードすることによって入力してください）。

6. 実際の設定値を変数に変換するには、値を選択して [Create Variable] をクリックします。変数名を入力し、[Create Variable] をクリックします。{{variable-name}} の形式で変数名を直接入力することもできます ({{hostname}} など)。
7. [Add] をクリックします。画面の右側にあるペインに、新しいデバイステンプレートのリストが表示されます。[Feature Templates] 列には、デバイステンプレートに含まれている機能テンプレートが表示され、[Type] 列には、デバイステンプレートが CLI テキストから作成されたことを示す「CLI」が表示されます。

Cisco vSmart コントローラ へのデバイステンプレートのアタッチ

Cisco vSmart コントローラ を設定するには、1 つのデバイステンプレートをコントローラにアタッチします。同じテンプレートを複数の Cisco vSmart コントローラ に同時にアタッチできます。

デバイステンプレートを Cisco vSmart コントローラ にアタッチするには、次の手順を実行します。

1. Cisco vManage メニューから、[Configuration] > [Templates] の順に選択します。
2. [Device Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。

3. 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。
4. [Attach Devices] ウィンドウで [Available Devices] 列から目的の Cisco vSmart コントローラ を選択し、右向き矢印をクリックしてそれらを [Selected Devices] 列に移動させます。1 つ以上のコントローラを選択できます。リストされているすべてのコントローラを選択するには、[Select All] をクリックします。
5. [Attach] をクリックします。
6. [Next] をクリックします。
7. Cisco vSmart コントローラ に送信しようとしている構成をプレビューするには、左側のペインでデバイスをクリックします。構成は、[Device Configuration Preview] ウィンドウの右側のペインに表示されます。
8. デバイステンプレートの構成を Cisco vSmart コントローラ に送信するには、[Configure Devices] をクリックします。

オーバーレイネットワークへの Cisco vSmart コントローラ の追加

Cisco vSmart コントローラ の最小限の設定を作成したら、コントローラに Cisco vManage を認識させてオーバーレイネットワークに設定を追加する必要があります。Cisco vSmart コントローラ を追加すると、署名付き証明書が生成され、コントローラの検証と認証に使用されます。

Cisco vManage はネットワーク内で最大 20 の Cisco vSmart コントローラ をサポートできます。

Cisco vSmart コントローラ の追加と証明書の生成

Cisco vSmart コントローラ をネットワークに追加するには、CSR を自動的に生成させ、署名付き証明書をインストールします。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]** を選択します。
2. **[Controllers]** をクリックし、**[Add Controller]** ドロップダウンメニューから **[vSmart]** を選択します。
3. **[Add vSmart]** ウィンドウで、次の手順を実行します。
 1. Cisco vSmart コントローラ のシステム IP アドレスを入力します。
 2. ユーザ名とパスワードを入力して、Cisco vSmart コントローラ にアクセスします。
 3. コントロールプレーン接続に使用するプロトコルを選択します。デフォルトは DTLS です。
 4. TLS を選択する場合は、TLS 接続に使用するポート番号を入力します。デフォルトは 23456 です。
 5. 証明書生成プロセスを自動的に実行できるように、**[Generate CSR]** チェックボックスをオンにします。
 6. **[Add]** をクリックします。

Cisco vManage は CSR を自動的に生成し、生成した証明書を取得して、Cisco vSmart コントローラ にインストールします。新しいコントローラは、コントローラタイプ、コントローラのホスト名、IP アドレス、サイト ID、およびその他の詳細とともに **[Controller]** テーブルに表示されます。

証明書のインストールの確認

Cisco vSmart コントローラ に証明書がインストールされていることを確認するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]** を選択します。
2. 表示されている新しいコントローラを選択し、**[Certificate Status]** 列をチェックして、証明書がインストールされていることを確認します。



- (注) Cisco vSmart コントローラ と Cisco vBond オーケストレーション のシステム IP アドレスが同じ場合、それらはデバイスまたはコントローラとして Cisco vManage に表示されません。Cisco vSmart コントローラ と Cisco vBond オーケストレーション の証明書ステータスも表示されません。ただし、制御接続は引き続き正常に確立されます。

次のステップ

vEdge ルータの展開を参照してください。

クラウドサービスプロバイダーポータルを使用した Cisco Catalyst 8000V の展開

表 4: 機能の履歴

機能名	リリース情報	説明
サポートされているクラウドサービスプロバイダープラットフォームに対する Cisco Catalyst 8000V インスタンスの展開のサポート	Cisco IOS XE リリース 17.4.1a	このリリース以降、Cisco Catalyst 8000V インスタンスは、Google Cloud Platform、Microsoft Azure、Amazon Web Services などのクラウドサービスプロバイダーポータルに展開できます
Alibaba Cloud での Cisco Catalyst 8000V インスタンスの展開のサポート	Cisco IOS XE リリース 17.5.1a	このリリース以降、Cisco Catalyst 8000V インスタンスを Alibaba Cloud に展開できるようになりました。

Cisco Catalyst 8000V のサポートされているインスタンスと、サポートされているクラウドサービスプロバイダーポータルにインスタンスを展開する方法については、次のリンクを参照してください。

- [Amazon Web Services での Cisco Catalyst 8000V Edge ソフトウェア の展開](#)
- [Microsoft Azure での Cisco Catalyst 8000V Edge ソフトウェア の展開](#)
- [Google Cloud Platform での Cisco Catalyst 8000V Edge ソフトウェア の展開](#)
- [Alibaba Cloud 向け Cisco Catalyst 8000V Edge ソフトウェア導入ガイド \[英語\]](#)

注意事項と制限事項

- スナップショットによる新しい Cisco Catalyst 8000V インスタンスの作成：スナップショット（複製）によって新しい Cisco Catalyst 8000V インスタンスを作成すると、元のインスタンスと同じシリアル番号を持つ新しいインスタンスが作成されます。そのため、Cisco SD-WAN に競合が発生します。スナップショット（複製）機能を使用して新しいインスタンスを作成できるのは、新しいインスタンスが既存のインスタンスを置き換える場合に限られます。これにより、シリアル番号が1つの Cisco Catalyst 8000V インスタンスでのみ使用されるようになります。

クラウドサービスプロバイダーポータルを使用した Cisco CSR 1000v の展開

Cisco CSR 1000v ルータのサポートされているインスタンスと、サポートされているクラウドサービスプロバイダーポータルにそれらのインスタンスを展開する方法については、次の各リンクを参照してください。

- [Amazon Web Services 向け Cisco CSR 1000v シリーズクラウドサービスルータ導入ガイド \[英語\]](#)
- [Microsoft Azure 向け Cisco CSR 1000 v 導入ガイド \[英語\]](#)

Alibaba Cloud への Cisco Catalyst 8000V Edge ソフトウェアの展開

このセクションでは、Alibaba Cloud インスタンスを Cisco SD-WAN とともに使用するとき役立つ情報を提供します。Cisco Catalyst 8000V Edge ソフトウェアの展開プロセスの詳細については、[Alibaba Cloud 向け Cisco Catalyst 8000V Edge ソフトウェア導入ガイド \[英語\]](#) を参照してください。

機能

Cisco SD-WAN の一部として動作している場合、Alibaba Cloud の導入では次の Cisco Catalyst 8000V 機能はサポートされません。

表 5: サポートされない機能

機能	その他の情報
展開とライセンス	

機能	その他の情報
Cisco SD-WAN Cloud onRamp の統合	Cisco vManage を使用した Cisco Catalyst 8000V インスタンスのブートストラップファイルの作成 (86 ページ) で説明されているように、ブートストラップファイルを作成して Cisco Catalyst 8000V を Cisco SD-WAN に接続します。Cloud onRamp による展開はサポートされていません。
ペイアズユーゴー (PAYG) ライセンス	なし

Cisco Catalyst 8000V インスタンスの要件

Cisco SD-WAN と連携するには、Alibaba Cloud に展開された Cisco Catalyst 8000V インスタンスが次の要件を満たしている必要があります。

- Alibaba Cloud Elastic Compute Service (ECS) のインスタンスタイプ : G5ne
- vCPU : 2
- RAM : 8 GB

Cisco SD-WAN では次の 2 つのイメージオプションがサポートされています。

- ecs.g5ne.large : 2 vCPU および 8 GB RAM
- ecs.g5ne.xlarge : 4 vCPU および 16 GB RAM
- ecs.g5ne.2xlarge : 8 vCPU および 32 GB RAM

Cisco SD-WAN に接続するための Cisco Catalyst 8000V インスタンスの設定

Alibaba Cloud で Cisco SD-WAN インスタンスを作成するときは、Cisco vManage を使用して Day 0 ブートストラップファイルを作成し、Cisco Catalyst 8000V インスタンスでこのブートストラップファイルを使用して、インスタンスを Cisco SD-WAN にオンボードします。インスタンスはブートストラップファイルを使用して起動すると、Cisco vBond オーケストレーションおよび Cisco vManage コントローラに接続します。

Cisco vManage を使用した Cisco Catalyst 8000V インスタンスのブートストラップファイルの作成

1. Cisco vManage を使用して、クラウドホスト型デバイスのブートストラップファイルを作成する手順については、「Cisco SD-WAN クラウドホスト型デバイスのブートストラッププロセス」を参照してください。

2. Alibaba Cloud ポータルで、Cisco Catalyst 8000V のインスタンスを作成します。インスタンスを構成するときは、Cisco vManage で作成したブートストラップ構成を使用します。

vEdge クラウドルータ の展開

vEdge ルータは、その名前が示すように、オーバーレイネットワーク内のサイト（リモートオフィス、ブランチ、キャンパス、データセンターなど）の境界に配置されたエッジルータです。オーバーレイネットワークを介して、サイトとの間でデータトラフィックをルーティングします。

vEdge ルータは、ハイパーバイザまたはAWS サーバーで仮想マシンとして実行される物理ハードウェアルータまたはソフトウェア vEdge クラウドルータ です。

オーバーレイネットワークは、少数または多数の vEdge ルータで構成できます。1 つの Cisco vManage で、vEdge ルータに管理および構成サービスを提供し、最大約 2,000 のルータをサポートできます。vManage クラスタは最大約 6,000 のルータをサポートできます。

vEdge クラウドルータ を展開するには、次の手順を実行します。

1. ソフトウェア vEdge クラウドルータ の場合、AWS サーバー、あるいは ESXi または KVM ハイパーバイザのいずれかで VM インスタンスを作成します。
2. vEdge クラウドルータ ソフトウェアの場合、ルータに署名付き証明書をインストールします。リリース 17.1 以降では、Cisco vManage は認証局 (CA) として機能し、署名付き証明書を自動的に生成して vEdge クラウドルータ にインストールできます。以前のリリースでは、証明書署名要求をシマンテックに送信し、その証明書をルータにインストールすることで、ルータを認証してオーバーレイネットワークに参加させることができました。
3. Cisco vManage から、すべての vEdge クラウドルータ のシリアル番号をオーバーレイネットワーク内の Cisco vSmart コントローラ および Cisco vBond オーケストレーションに送信します。
4. vEdge クラウドルータ の完全な構成を作成します。そのためには、Cisco vBond オーケストレーションの vManage テンプレートを作成して、オーケストレータに添付します。vManage テンプレートを添付すると、初期の最小構成が上書きされます。
5. Cisco SD-WAN ゼロタッチプロビジョニング (ZTP) ツールを使用して実行される自動プロビジョニング用のハードウェア vEdge クラウドルータ を準備します。ZTP プロセスにより、ハードウェアルータはオーバーレイネットワークに自動的に参加できます。

リリース 18.2.0 以降、米国政府の禁輸措置の影響を受ける国でホストされている vEdge クラウドルータは、Cisco Cloud でホストされているオーバーレイ ネットワーク コントローラ (Cisco vBond オーケストレーション、Cisco vManage、および Cisco vSmart コントローラ) に接続できません。これらのコントローラの 1 つに接続しようとする禁輸国からの vEdge クラウドルータ アクセスは無効になります。(ただし、vEdge クラウドルータ は他のクラウドでホストされているコントローラに接続できます)。その結果、vEdge クラウドルータ が最初に Cisco Cloud 内のコントローラに接続しようとしたときに、Cisco vBond オーケストレーションと Cisco

vManage が相互に通信できない場合、または Cisco Cloud サーバーがダウンしている場合、ルータが起動せず、保留状態のままになることがあります。

AWS での vEdge クラウドルータ VM インスタンスの作成

ソフトウェア vEdge クラウドルータ を起動するには、起動用の仮想マシン (VM) インスタンスを作成する必要があります。この記事では、Amazon AWS で VM インスタンスを作成する方法について説明します。また、vSphere ESXi ハイパーバイザソフトウェアまたはカーネルベースの仮想マシン (KVM) ハイパーバイザソフトウェアを実行しているサーバー上に VM を作成することもできます。

Amazon AWS で vEdge クラウドルータ 仮想マシン (VM) インスタンスを起動するには、まず、仮想プライベートクラウド (VPC) を作成します。VPC は、ネットワークを構築するために必要なインフラストラクチャを構築する自己完結型の環境です。

VPC を作成する前に、ネットワークのアドレス指定を慎重に計画してください。VPC は管理者が指定する範囲内のアドレスのみを使用でき、VPC を作成した後は、それを変更できません。ネットワークのアドレス指定要件が変更された場合は、VPC を削除して新しいものを作成する必要があります。

Cisco SD-WAN 18.4 リリース以降、Cisco Cloud Services 1000v (CSR 1000v) ルータ SD-WAN バージョンが AWS でサポートされます。

Amazon AWS で vEdge クラウドルータ を起動するには、次の手順を実行します。

1. VPC を作成します。
2. vEdge クラウドルータ VM インスタンスをセットアップします。
3. 追加のインターフェイスを定義します。

VPC の作成

VPC を作成する前に、ネットワークのアドレスブロックを慎重に計画してください。VPC を作成した後は、それを変更できません。ネットワークのアドレス指定を変更するには、VPC を削除して新しいものを作成する必要があります。

1. AWS にログインします。AWS ホームページの [Networking] セクションで、[VPC] をクリックします。
2. 開いたページで、[Start VPC] をクリックします。
3. [Select a VPC Configuration] ページで、[VPC with Public and Private Subnets] を選択します。
4. [VPC with Public and Private Subnets] 画面で、次の手順を実行します。
 1. [IP CIDR Block] に、目的の IP アドレス指定ブロックを入力します。VPC は、この範囲のアドレスのみを使用できます。
 2. IP CIDR ブロック内からパブリックサブネットとプライベートサブネットを指定します。

3. [Elastic IP Allocation ID] にインターネットゲートウェイのアドレスを入力します。このゲートウェイは、パブリックインターネットに配信するために内部トラフィックを変換します。
4. 拡張ストレージ領域が必要な場合（大規模なデータベースなど）にのみ、S3のエンドポイントを追加します。
5. DNS への IP アドレスの AWS 自動登録を使用するために、DNS ホスト名を有効にします。
6. 目的のハードウェアテナント（共有または専用）を選択します。AWS ハードウェアを他の AWS クライアントと共有することも、専用のハードウェアを持つこともできます。専用ハードウェアを使用する場合、ユーザーに割り当てられたデバイスは、そのユーザーのデータのみをホストできます。ただし、コストは高くなります。
7. [VPCの作成 (Create VPC)] をクリックします。

VPC ダッシュボードに「VPC Successfully Created」というメッセージが表示されるまで、数分待ちます。

これでインフラストラクチャが完成し、アプリケーション、アプライアンス、および vEdge クラウドルータを展開する準備が整いました。左側にあるリンクをクリックして、VPC のサブネット、ルートテーブル、インターネットゲートウェイ、および NAT アドレス変換ポイントを確認してください。

vEdge クラウドルータ VM インスタンスのセットアップ

1. [Services] > [EC2] の順にクリックして EC2 ダッシュボードを開き、[Launch Instance] をクリックします。
1. Amazon マシンイメージ (AMI) を選択します。Cisco SD-WAN AMI には、「release-number-vEdge」という形式の名前（16.1.0-vEdge など）が付いています。Cisco SD-WAN AMI はプライベートです。共有できる Cisco SD-WAN の営業担当者にお問い合わせください。
2. Cisco SD-WAN AMI を選択し、[Select] をクリックします。
3. [Choose an Instance Type] 画面が表示されます。次の表を参照して、ニーズに最適なインスタンスタイプを判断してください。最小要件は 2 vCPU です。

表 6: 表 1: vEdge クラウドルータをサポートする EC2 インスタンスタイプ

	vCPU	メモリ (GB)	インスタンスストレージ (GB)
汎用：現在の世代			
m4.large	2	8	EBS のみ
m4.xlarge	4	16	EBS のみ

	vCPU	メモリ (GB)	インスタンスストレージ (GB)
m4.2xlarge	8	32	EBS のみ
m4.4xlarge	16	64	EBS のみ
m4.10xlarge	40	160	EBS のみ
コンピューティング最適化：現在の世代			
c4.large	2	3.75	EBS のみ
c4.xlarge	4	7.5	EBS のみ
c4.2xlarge	8	15	EBS のみ
c4.4xlarge	16	30	EBS のみ
c4.8xlarge	36	60	EBS のみ
c3.large	2	3.75	2 x 16 SSD
c3.xlarge	4	7.5	2 x 40 SSD
c3.2xlarge	8	15	2 x 80 SSD
c3.4xlarge	16	30	2 x 160 SSD
c3.8xlarge	32	60	2 x 320 SSD

4. 優先するインスタンスタイプを選択し、[Next: Configure Instance Details] をクリックします。

インスタンスの詳細設定

[Configure Instance Details] 画面で、次の手順を実行します。

1. [Network] で、作成した VPC を選択します。
2. [Subnet] で、最初のインターフェイスのサブネットを選択します。
3. [Network Interfaces] で、[Add Device] をクリックし、追加の各インターフェイスのサブネットを選択します。



- (注) Cisco SD-WAN リリース 20.5.1 以降では、デフォルトのユーザー名とパスワード (admin/admin) を持つ Cisco vEdge Cloud ルータ VM は、AWS に展開できません。そのため、サードパーティクラウドプロバイダーを使用して Cisco vEdge Cloud ルータ VM を展開する場合は、次のクラウド設定を使用して、引き続きデフォルトのログイン情報を使用します。

[User Data] フィールドに、次のクラウド構成を入力します。

```
#cloud-config

hostname: vedge
write_files:
- content: "vedge\n"
  owner: root:root
  path: /etc/default/personality
  permissions: '0644'
- content: "1\n"
  owner: root:root
  path: /etc/default/ined
  permissions: '0600'
- path: /etc/confd/init/zcloud.xml
  content: |
    <config xmlns="http://tail-f.com/ns/config/1.0">
      <system xmlns="http://viptela.com/system">
        <aaa>
          <user>
            <name>admin</name>

<password>$6$9ac6af765f1cd0c0$jR/rCPsQ56JLDU/1s9H7zhksy/EZHv37zDJKzMRn/IU/FsrItbBILw3AVI5kChE9WmgP8CsGk.4PrjC22/</password>

          <group>netadmin</group>
        </user>
      </aaa>
    </system>
  </config>
```

このクラウド構成により、admin/admin のログイン情報を使用して VM が設定され、初回ログイン時にパスワードの変更が強制されます。

5. [Next: Add Storage] をクリックします。
6. [Add Storage] ページが開きます。この画面で設定を変更する必要はありません。[次: タグインスタンス (Next: Tag Instance)] をクリックします。
7. [Tag Instance] ページが開きます。目的のキーと値を入力し、[Next: Configure Security Group] をクリックします。
8. [セキュリティ グループの設定 (Configure Security Group)] ページが開きます。ファイアウォール設定を指定するルールを追加します。これらのルールは、vEdgeクラウドルータに着信する外部トラフィックに適用されます。
 1. [Type] で、[SSH] を選択します。
 2. [Source] で、[My IP] を選択します。
9. [Add Rule] をクリックし、次のようにフィールドに入力します。
 1. [Type] で、[Custom UDP Rule] を選択します。
 2. [Port Range] で、「12346」と入力します。
 3. [Source] で、[Anywhere] を選択します。12346 は IPSec のデフォルトポートです。

4. ポートホッピングが有効になっている場合は、さらにルールを追加する必要がある場合があります。
10. [Review and Launch] をクリックします。[Review Instance Launch] 画面が開きます。[作成 (Launch)] をクリックします。
11. [Proceed without a key pair] を選択し、確認応答チェックボックスをクリックしてから、[Launch Instances] をクリックします。
12. 数分待ちます。インスタンスが初期化されます。vEdge クラウドルータ が動作するようになりました。最初のインターフェイスである eth0 は、常に管理インターフェイスです。2 つ目のインターフェイスである ge0/0 は、VPN 0 に表示されますが、別の VPN に存在するように設定できます。

追加のインターフェイスの定義

vEdge クラウドルータ は、合計 9 つのインターフェイスをサポートします。最初のインターフェイスは常に管理インターフェイスであり、残りの 8 つはトランスポートインターフェイスとサービスインターフェイスです。追加のインターフェイスを設定するには、次の手順を実行します。

1. 左側のペインで、[Network Interfaces] をクリックします。
2. [ネットワークインターフェイスの作成 (Create Network Interface)] をクリックします。[Subnet and Security group] を選択し、[Yes, Create] をクリックします。同じルーティングドメイン内の 2 つのインターフェイスは、同じサブネット内に存在できないことに注意してください。
3. 新しいインターフェイスの左側にあるチェックボックスをオンにして、[Attach] をクリックします。
4. vEdge クラウドルータ を選択し、[Attach] をクリックします。
5. vEdge クラウドルータ は起動プロセス中にのみインターフェイスを検出するため、vEdge クラウドルータ を再起動します。

これで、新しいインターフェイスが稼働します。VPN 0 のインターフェイスは、WAN トランスポート (インターネットなど) に接続します。VPN 1 のインターフェイスは、サービス側ネットワークに面しており、アプライアンスやアプリケーションに使用できます。VPN 512 のインターフェイスは、アウトオブバンド管理専用です。

6. インターフェイスがジャンボフレーム (MTU が 2000 バイトの packets) を伝送できるようにするには、CLI から MTU を設定します。次に例を示します。

```
Router# show interface
```

VPN	INTERFACE	TYPE	IP ADDRESS	STATUS	IF	IF	MTU	HWADDR
					ADMIN	OPER		
						RX	ENCAP	
						TX	PACKETS	
					UP	PACKETS		
					UP			
0	ge0/0	ipv4	10.66.15.15/24	Up	Up	null	service	1500

```

00:0c:29:db:f0:62 1000 full 1420 0:14:05:07 545682 545226
0 ge0/1 ipv4 10.1.17.15/24 Up Up null service 1500
00:0c:29:db:f0:6c 1000 full 1420 0:14:21:19 0 10
0 ge0/2 ipv4 - Down Up null service 1500
00:0c:29:db:f0:76 1000 full 1420 0:14:21:47 0 0
0 ge0/3 ipv4 10.0.20.15/24 Up Up null service 1500
00:0c:29:db:f0:80 1000 full 1420 0:14:21:19 0 10
0 ge0/6 ipv4 172.17.1.15/24 Up Up null service 1500
00:0c:29:db:f0:9e 1000 full 1420 0:14:21:19 0 10
0 ge0/7 ipv4 10.0.100.15/24 Up Up null service 1500
00:0c:29:db:f0:a8 1000 full 1420 0:14:21:19 770 705
0 system ipv4 172.16.255.15/32 Up Up null loopback 1500
00:00:00:00:00:00 0 full 1420 0:14:21:30 0 0
0 loopback3 ipv4 10.1.15.15/24 Up Up null transport 2000
00:00:00:00:00:00 10 full 1920 0:14:21:22 0 0
1 ge0/4 ipv4 10.20.24.15/24 Up Up null service 2000
00:0c:29:db:f0:8a 1000 full 1920 0:14:21:15 52014 52055
1 ge0/5 ipv4 172.16.1.15/24 Up Up null service 1500
00:0c:29:db:f0:94 1000 full 1420 0:14:21:15 0 8
512 eth0 ipv4 10.0.1.15/24 Up Up null service 1500
00:50:56:00:01:05 0 full 0 0:14:21:16 28826 29599

```

```

Router# config
Entering configuration mode terminal
Router(config)# vpn 0 interface ge0/3 mtu 2000
Router(config-interface-ge0/3)# commit
Commit complete.
vEdge(config-interface-ge0/3)# end
vEdge# show interface

```

VPN	INTERFACE	AF	TYPE	IP ADDRESS	MSS	TCP	IF	IF	ADMIN	OPER	ENCAP	STATUS	STATUS	RX	TX	TYPE	PORT	MTU	HWADDR
0	ge0/0	ipv4	10.66.15.15/24	1000	full	1420	Up	Up	Up	Up	null	service	1500	0:14:05:30	546018	545562			
0	ge0/1	ipv4	10.1.17.15/24	1000	full	1420	Up	Up	Up	Up	null	service	1500	0:14:21:42	0	10			
0	ge0/2	ipv4	-	1000	full	1420	Down	Up	Down	Up	null	service	1500	0:14:22:10	0	0			
0	ge0/3	ipv4	10.0.20.15/24	1000	full	1920	Up	Up	Up	Up	null	service	2000	0:14:21:42	0	10			
0	ge0/6	ipv4	172.17.1.15/24	1000	full	1420	Up	Up	Up	Up	null	service	1500	0:14:21:42	0	10			
0	ge0/7	ipv4	10.0.100.15/24	1000	full	1420	Up	Up	Up	Up	null	service	1500	0:14:21:42	773	708			
0	system	ipv4	172.16.255.15/32	1000	full	1420	Up	Up	Up	Up	null	loopback	1500	0:14:21:54	0	0			
0	loopback3	ipv4	10.1.15.15/24	1000	full	1420	Up	Up	Up	Up	null	transport	2000	0:14:21:46	0	0			
1	ge0/4	ipv4	10.20.24.15/24	1000	full	1920	Up	Up	Up	Up	null	service	2000	0:14:21:38	52038	52079			
1	ge0/5	ipv4	172.16.1.15/24	1000	full	1420	Up	Up	Up	Up	null	service	1500	0:14:21:38	0	8			
512	eth0	ipv4	10.0.1.15/24	1000	full	1420	Up	Up	Up	Up	null	service	1500	0:14:21:39	28926	29663			

次のインスタンスは、ジャンボフレームをサポートしています。

- 高速コンピューティング : CG1、G2、P2

- コンピューティング最適化 : C3、C4、CC2
- 汎用 : M3、M4、T2
- メモリ最適化 : CR1、R3、R4、X1
- ストレージ最適化 : D2、HI1、HS1、I2

次のステップ

「vEdge Cloud ルータへの署名付き証明書のインストール」を参照してください。

Azure での vEdge クラウドルータ VM インスタンスの作成

ソフトウェア vEdge クラウドルータ を起動するには、起動用の仮想マシン (VM) インスタンスを作成する必要があります。この記事では、Microsoft Azure で VM インスタンスを作成する方法について説明します。Amazon AWS に、または vSphere ESXi ハイパーバイザソフトウェアやカーネルベースの仮想マシン (KVM) ハイパーバイザソフトウェアを実行しているサーバーに VM を作成することもできます。

注 : Cisco SD-WAN は、vEdge クラウドルータ の所有ライセンス持ち込み (BYOL) のみを提供するため、実際に Cisco SD-WAN 製品を購入するわけではありません。VNET インスタンスは時間単位で課金されます。

サーバーの要件については、「サーバーハードウェアの推奨事項」を参照してください。

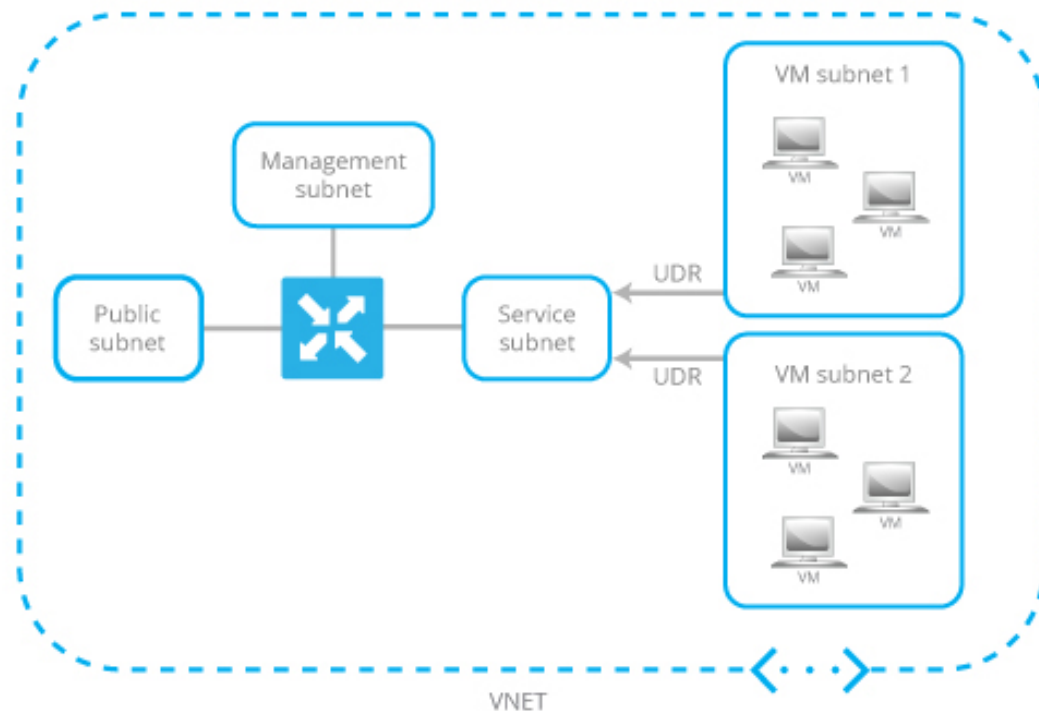
Azure Marketplace の起動と vEdge クラウドルータ VM インスタンスの作成

1. Azure Marketplace アプリケーションを起動します。
 1. 左側のペインで、[New] をクリックして、新しい vEdge クラウドルータ VM インスタンスを作成します。
 2. [Search] ボックスで、「Cisco」を検索します。
2. 右側のペインで、[Cisco vEdge クラウドルータ (3 NICs) (Staged)] を選択します。
3. [Cisco vEdge クラウドルータ (3 NICs) (Staged)] 画面で、左側のペインの [Basic] をクリックして、vEdge クラウドルータ VM の基本設定を指定します。
 1. [VM Name] フィールドに、vEdge クラウドルータ VM インスタンスの名前を入力します。
 2. [Username] フィールドに、VM インスタンスにアクセスできるユーザーの名前を入力します。
 3. [Authentication type] フィールドで、[Password] または [SSH public key] を選択します。
 4. [Password] を選択した場合は、パスワードを入力し、確認します。ユーザー名とパスワードを使用して、VM インスタンスへの SSH セッションを開きます。

5. [SSH public key] を選択した場合は、Linux VM の SSH キーペアを生成する方法の手順について、<https://docs.microsoft.com/en-us/azu...reate-ssh-keys> を参照してください。
 6. [Subscription] フィールドで、ドロップダウンメニューから [Pay-As-You-Go] を選択します。
 7. [Resource Group] フィールドで、[Create new] をクリックして新しいリソースグループを作成するか、[Use existing] をクリックしてドロップダウンメニューから既存のリソースグループを選択します。
 8. [Location] フィールドで、vEdge クラウドルータ VM インスタンスを起動する場所を選択します。
 9. [OK] をクリックします。
4. 左側のペインで、[vEdge Settings] をクリックして vEdge クラウドルータ インフラストラクチャの設定を指定します。
 5. [Infrastructure Settings] ペインで、次の手順を実行します。
 1. [Size] をクリックします。[Choose a size] ペインで、インスタンスタイプとして [D3_V2 Standard] を選択し、[Select] をクリックします。これが推奨されるインスタンスタイプです。
 2. [Storage Account] をクリックします。[Choose storage account] ペインで、[Create New] をクリックして新しいストレージアカウントを作成するか、ストレージアカウントのリストからいずれかのアカウントを選択します。次に [OK] をクリックします。
 3. [Public IP Address] をクリックします。[Choose public IP address] ペインで、[Create New] をクリックして新しいパブリック IP アドレスを作成するか、パブリック IP アドレスのリストから、パブリック IP サブネットに使用するいずれかのアドレスを選択します。次に [OK] をクリックします。
 4. [Domain Name] フィールドで、ドロップダウンメニューから [vedge] を選択します。
 5. [Virtual Network] をクリックします。[Choose virtual network] ペインで、[Create New] をクリックして新しい仮想ネットワーク (VNET) を作成するか、vEdge Cloud インスタンスを起動する既存の VNET を選択します。その後、[OK] をクリックします。
 6. 既存の VNET を選択した場合は、ドロップダウンメニューを使用して、VNET 内で使用可能なサブネットを選択します。次に [OK] をクリックします。

VNET 内で3つのサブネットを使用できる必要があります。そうでない場合、vEdge クラウドルータ VM インスタンスは起動に失敗します。また、VM サブネットに関連付けられたルートテーブルに、vEdge クラウドルータ のサービスサブネットへのユーザー定義ルート (UDR) があることを確認してください。UDR によって、VM サブネットが vEdge クラウドルータ を確実にゲートウェイとして使用します。以下のトポロジ例を参照してください。

図 17: VM サブネットを使用した VNET のトポロジ例



7. 新しい VNET を作成した場合は、その VNET 内のアドレス空間を定義します。次に、[Subnets] ペインで [OK] をクリックします。

Cisco SD-WAN はサブネット名を事前に入力し、定義した VNET アドレス空間からサブネットごとに IP アドレスを割り当てます。vEdge クラウドルータに関連付けられたサービスサブネットを介して VNET インスタンスを接続する場合は、ルートテーブルを更新する必要はありません。

6. [Summary] ペインで、[OK] をクリックします。[Summary] ペインで、vEdge クラウドルータ VM インスタンスに対して定義した構成が検証および表示されます。
7. [Buy to purchase] をクリックします。次に、[Purchase] ペインで [Purchase] をクリックします。



- (注) Cisco SD-WAN は、vEdge クラウドルータ の所有ライセンス持ち込み (BYOL) のみを提供するため、実際に Viptela 製品を購入するわけではありません。VNET インスタンスは時間単位で課金されます。

システムによって vEdge クラウドルータ VM インスタンスが作成され、展開が成功したことが通知されます。

8. 作成した vEdge VM インスタンスをクリックします。

vEdge クラウドルータ VM インスタンスのパブリック IP アドレスと DNS 名が表示されます。

9. vEdge クラウドルータ VM インスタンスのパブリック IP アドレスに SSH 接続します。
10. ログインプロンプトで、手順 3 で作成したユーザー名とパスワードを使用してログインします。vEdge クラウドルータ のデフォルト設定を表示するには、次のコマンドを入力します。

```
vEdge# show running-config
```

vEdge クラウドルータ VM を作成すると、以下に示すセキュリティグループの設定が、パブリックサブネットに関連付けられた NIC に適用されます。このセキュリティグループは、特定のソースからのトラフィックは制限しませんが、特定のサービスは制限します。Cisco SD-WAN 制御プロトコルに対して有効にする必要がある、TCP および UDP のカスタムサービスも自動的に設定されます。セキュリティグループの設定は、要件に合わせて変更できます。

vEdge Cloud ルータのインターフェイスとサブネットマッピング

Azure Marketplace で vEdge クラウドルータ VM インスタンスを作成するには、最低 3 つの NIC が必要です（管理、サービス、およびトランスポート用にそれぞれ 1 つずつ）。以下の表は、これらの NIC に関連付けられたサブネットと vEdge クラウドルータ インターフェイスのマッピングを示しています。

vEdge Cloud ルータのインターフェイス	サブネット	説明
eth0	管理サブネット	インバンド管理
ge0/1	サービスサブネット	vEdge クラウドルータ をゲートウェイデバイスとして接続
ge0/0	トランスポートサブネット	トランスポート/WAN リンク

次のステップ

「vEdge Cloud ルータへの署名付き証明書のインストール」を参照してください。

ESXi での vEdge Cloud VM インスタンスの作成

ソフトウェア vEdge Cloud ルータを起動するには、起動用の仮想マシン (VM) インスタンスを作成する必要があります。ここでは、vSphere ESXi ハイパーバイザソフトウェアを実行しているサーバー上に VM インスタンスを作成する方法について説明します。Amazon AWS、またはカーネルベースの仮想マシン (KVM) ハイパーバイザソフトウェアを実行しているサーバーに VM を作成することもできます。

サーバーの要件については、「サーバーハードウェアの推奨事項」を参照してください。

ESXi ハイパーバイザで vEdge Cloud VM インスタンスを作成するには、次の手順を実行します。

1. vSphere Client を起動し、vEdge Cloud VM インスタンスを作成します。
2. トンネルインターフェイスの vNIC を追加します。
3. vEdge Cloud VM インスタンスの起動とコンソールへの接続

各ステップの詳細を以下に示します。

VMware vCenter Server を使用して vEdge Cloud VM インスタンスを作成している場合は、同じ手順に従います。ただし、vCenter Server の画面は、手順に示されている vSphere Client の画面とは異なることに注意してください。

vSphere Client を起動し、vEdge Cloud VM インスタンスを作成します

1. VMware vSphere Client アプリケーションを起動し、ESXi サーバーの IP アドレスまたは名前、ユーザー名、およびパスワードを入力します。[Login] をクリックして、ESXi サーバーにログインします。

[ESXi] 画面が表示されます。

2. [File] > [Deploy OVF Template] をクリックして、仮想マシンを展開します。
3. [Deploy OVF Template] 画面で、OVF パッケージをインストールしてダウンロードする場所を入力します。このパッケージは、シスコからダウンロードした vedge.ova ファイルです。次に、[Next] をクリックします。
4. [Next] をクリックして、OVF テンプレートの詳細を確認します。
5. 展開したテンプレートの名前を入力し、[Next] をクリックします。次の図は、vEdge インスタンスの名前を示しています。
6. [Next] をクリックして、仮想ディスクのデフォルトのフォーマットを受け入れます。
7. [Next] をクリックして、展開された OVF テンプレートの宛先ネットワークとして、使用している宛先ネットワーク名を受け入れます。下の図では、CorpNet が宛先ネットワークです。
8. [Ready to Complete] 画面で、[Finish] をクリックします。

定義したパラメータを使用して VM インスタンスが正常に作成され、[Getting Started] タブが選択された状態で [vSphere Client] 画面が表示されます。デフォルトの画面には、管理、トンネル、またはサービスインターフェイスに使用できる 4 つの vNIC が含まれています。

新しい vNIC の追加

1. vSphere Client の左側のナビゲーションバーで、作成した vEdge Cloud VM インスタンスを選択し、[Edit virtual machine settings] をクリックします。

2. [vEdge Cloud – Virtual Machine Properties] 画面で、[Add] をクリックして新しい vNIC を追加します。次に [OK] をクリックします。
3. 追加するデバイスタイプの [Ethernet Adapter] をクリックして、[Next] をクリックします。
4. [Adapter Type] ドロップダウンで、追加する vNIC の VMXNET3 を選択して、[Next] をクリックします。
5. [Ready to Complete] 画面で、[Finish] をクリックします。
6. [vEdge Cloud – Virtual Machine Properties] 画面が開き、新しい vNIC が追加されていることが示されます。[OK] をクリックして [vSphere Client] 画面に戻ります。

vSwitch の MTU の変更

インターフェイスがジャンボフレーム（MTU が 2000 バイトのパケット）を伝送できるようにするには、各仮想スイッチ（vSwitch）の MTU を設定します。

1. ESXi ハイパーバイザを起動し、[Configuration] タブを選択します。
2. [Hardware] リストで、[Networking] をクリックします。追加したネットワークアダプタが右側のペインに表示されます。
 1. MTU を変更する vSwitch の [Properties] をクリックします。
3. [vSwitch Properties] 画面で、[Edit] をクリックします。
4. [Advanced Properties MTU] ドロップダウンで、vSwitch MTU を目的の値に変更します。値の範囲は 2000 ～ 9000 です。次に [OK] をクリックします。

vEdge Cloud VM インスタンスの起動とコンソールへの接続

1. vSphere Client の左側のナビゲーションバーで、作成した vEdge Cloud VM インスタンスを選択し、[Power on the virtual machine] をクリックします。vEdge Cloud 仮想マシンの電源が入ります。
2. [Console] タブを選択して、vEdge Cloud コンソールに接続します。
3. ログインプロンプトで、デフォルトのユーザー名 **admin** およびデフォルトのパスワード **admin** を使用してログインします。vEdge Cloud ルータのデフォルト設定を表示するには、次のコマンドを入力します。

```
vEdge# show running-config
```

インターフェイスへの vNIC のマッピング

前のセクションの手順で ESXi に vEdge Cloud ルータ VM インスタンスを作成する場合、管理インターフェイスに使用される vNIC 1 とトンネルインターフェイスとして使用される vNIC 2 の 2 つの vNIC を作成します。VM 自体の観点から、この 2 つの vNIC は、それぞれ eth0 および eth1 インターフェイスにマッピングされます。vEdge Cloud ルータの Cisco SD-WAN ソフトウェアの観点から、この 2 つの vNIC は、VPN 512 の mgmt0 インターフェイスおよび VPN 0

の ge0/0 インターフェイスにそれぞれマッピングされます。これらのマッピングは変更できません。

VM ホストには、3 から 7 の番号が付けられた最大 5 つの追加 vNIC を構成できます。それらの vNIC は、必要に応じて、インターフェイス eth2 ~ eth7、および Cisco SD-WAN インターフェイス ge0/1 ~ ge0/7 にマッピングできます。

次の表は、vNIC、VM ホストインターフェイス、および vEdge Cloud インターフェイス間のマッピングをまとめたものです。

表 7:

vNIC	VM ホストのインターフェイス	vEdge Cloud 設定のインターフェイス
vNIC 1	eth0	VPN 512 の mgmt0
vNIC 2	eth1	ge0/0
vNIC 3 ~ 7	eth2 ~ eth7	ge0/1 ~ ge0/7



(注) VRRP の MAC アドレスは、vEdge イーサネット インターフェイスに関連付けられた ESXi の仮想ソフトウェアスイッチによって学習されないため、VRRP IP 宛でのトラフィックは ESXi によって転送されません。これは、VMWare ESXi の制限によるもので、vNIC では複数のユニキャスト MAC アドレス設定は許可されていません。回避策として、vNIC を無差別モードにして、ソフトウェアで MAC フィルタリングを実行します。Cisco vEdge ソフトウェアでインターフェイスを無差別モードにできるようにするには、仮想ソフトウェアスイッチのポートグループまたはスイッチ設定を同じことを許可するように変更する必要があります。ESXi VSS は、ポートグループまたはスイッチに接続されているすべての仮想マシンにすべてのパケットを転送することに注意してください。その結果、ESXi ホストの他の仮想マシンのパフォーマンスに悪影響を与える可能性があります。また、vEdge パケット処理のパフォーマンスにも悪影響を及ぼす可能性があります。パフォーマンスへの影響を避けるために、ネットワークは慎重に設計してください。

次のステップ

「vEdge Cloud ルータへの署名付き証明書のインストール」を参照してください。

KVM での vEdge Cloud VM インスタンスの作成

ソフトウェア vEdge Cloud ルータを起動するには、起動用の仮想マシン (VM) インスタンスを作成する必要があります。ここでは、カーネルベースの仮想マシン (KVM) ハイパーバイザソフトウェアを実行しているサーバー上に VM インスタンスを作成する方法について説明します。Amazon AWS、または vSphere ESXi ハイパーバイザソフトウェアを実行しているサーバーに VM を作成することもできます。

サーバーの要件については、「サーバーハードウェアの推奨事項」を参照してください。

KVM ハイパーバイザでの vEdge Cloud VM インスタンスの作成

KVM ハイパーバイザで vEdge Cloud VM インスタンスを作成するには、次の手順を実行します。

1. Virtual Machine Manager (virt-manager) クライアントアプリケーションを起動します。
[Virtual Machine Manager] 画面が表示されます。
2. [New] をクリックして、仮想マシンを展開します。新しい仮想マシンの作成画面が開きます。
3. 仮想マシンの名前を入力します。次の図は、vEdge Cloud インスタンスの名前を示しています。
 1. [Import existing disk image] を選択します。
 2. [続行 (Forward)] をクリックします。
4. [Provide the existing storage path] フィールドで、[Browse to find the vEdge Cloud software image] をクリックします。
 1. [OS Type] フィールドで、[Linux] を選択します。
 2. [Version] フィールドで、実行している Linux バージョンを選択します。
 3. [続行 (Forward)] をクリックします。
5. ネットワークトポロジ、およびサイトの数に基づいて、メモリと CPU を指定します。
[続行 (Forward)] をクリックします。
6. [Customize configuration before install] チェックボックスをオンにします。その後、[Finish] をクリックします。
7. 左側のナビゲーションバーで [Disk 1] を選択します。実行されるアクション
 1. [Advanced Options] をクリックします。
 2. [Disk Bus] フィールドで、[IDE] を選択します。
 3. [Storage Format] フィールドで、[qcow2] を選択します。
 4. [Apply] をクリックして、定義したパラメータで VM インスタンスを作成します。デフォルトでは、vNIC が 1 つ含まれています。この vNIC は、管理インターフェイスに使用されます。



(注) Cisco SD-WAN ソフトウェアは、VMXNET3 および Virtio vNIC をサポートしていますが、Virtio vNIC を使用することを推奨します。

8. [vEdge Cloud Virtual Machine] 画面で、[Add Hardware] をクリックして、トンネルインターフェイスに 2 番目の vNIC を追加します。
9. [Add New Virtual Hardware] 画面で [Network] をクリックします。
 1. [Host Device] フィールドで、適切なホストデバイスを選択します。
 2. [Finish] をクリックします。

新しく作成された vNIC が左側のペインに表示されます。この vNIC は、トンネルインターフェイスに使用されます。

10. vEdge Cloud ルータの cloud-init 設定を含む ISO ファイルを作成します。



- (注) Cisco SD-WAN リリース 20.7.1 以降、cloud-init 構成ファイルには、Cisco vManage への制御接続をセットアップするために必要な最小限の構成のみが含まれている必要があります。VPN0 やクリアテキストパスワードなどの他の設定は、Cisco vManage のアドオン CLI テンプレートを介してプッシュする必要があります。

11. [Virtual Machine Manager] 画面で、[Add Hardware] をクリックして、作成した ISO ファイルを添付します。
12. [Add New Virtual Hardware] 画面で、次の手順を実行します。
 1. [Select managed or other existing storage] をクリックします。
 2. [Browse] をクリックし、作成した ISO ファイルを選択します。
 3. [Device Type] フィールドで、[IDE CDROM] を選択します。
 4. [Finish] をクリックします。
13. インターフェイスでジャンボフレーム (MTU が 2000 バイトのパケット) を伝送できるようにするには、各仮想ネットワーク (vnet) および仮想ブリッジ NIC を含む VNET (virbr-nic) インターフェイスの MTU を 2000 ~ 9000 の範囲に設定します。
 1. VM シェルから次のコマンドを発行して、vnet および virbr-nic インターフェイスの MTU を特定します。

```
user@vm:~$ ifconfig -a
virbr1-nic Link encap:Ethernet HWaddr 52:54:00:14:4e:6f
           BROADCAST MULTICAST MTU:1500 Metric
           RX packets:0 errors:0 dropped:0 overruns:0 frame:0
           TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:500
           RX bytes:0 (0.0 B) TX bytes:0 (0.0B)
           ...
vnet0     Link encap:Ethernet HWaddr fe:50:56:00:10:1e
           inet6 addr: fe80::fc50:56ff:fe00:11e/64 Scope:Link
           UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
           RX packets:167850 errors:0 dropped:0 overruns:0 frame:0
           TX packets:663186 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:500
```

```
RX bytes:19257426 (19.2 MB) TX bytes:42008544 (42.0 MB)
```

```
...
```

2. 各 vnet の MTU を変更します。

```
user@vm:~$ sudo ifconfig vnet number mtu 2000
```

3. 各 virbr-nic の MTU を変更します。

```
user@vm:~$ sudo ifconfig virbr-nic number mtu 2000
```

4. MTU 値を確認します。

```
user@vm:~$ ifconfig -a
```

14. [vEdge Cloud Virtual Machine] ページで、画面の左上隅にある [Begin Installation] をクリックします。
15. 仮想マシンインスタンスが作成され、vEdge Cloud コンソールが表示されます。
16. ログインプロンプトで、デフォルトのユーザー名 **admin** およびデフォルトのパスワード **admin** を使用してログインします。vEdge Cloud ルータのデフォルト設定を表示するには、次のコマンドを入力します。

```
vEdge# show running-config
```

Cisco SD-WAN ソフトウェアは、VMXNET3 および Virtio vNIC をサポートしていますが、Virtio vNIC を使用することを推奨します。

インターフェイスへの vNIC のマッピング

前のセクションの手順で KVM に vEdge Cloud ルータ VM インスタンスを作成する場合、管理インターフェイスに使用される vNIC 1 とトンネルインターフェイスとして使用される vNIC 2 の 2 つの vNIC を作成します。VM 自体の観点から、この 2 つの vNIC は、それぞれ eth0 および eth1 インターフェイスにマッピングされます。vEdge Cloud ルータの Cisco SD-WAN ソフトウェアの観点から、この 2 つの vNIC は、VPN 512 の mgmt0 インターフェイスおよび VPN 0 の ge0/0 インターフェイスにそれぞれマッピングされます。これらのマッピングは変更できません。

VM ホストには、3 から 7 の番号が付けられた最大 5 つの追加 vNIC を構成できます。それらの vNIC は、必要に応じて、インターフェイス eth2 ~ eth7、および Cisco SD-WAN インターフェイス ge0/1 ~ ge0/7 にマッピングできます。

次の表は、vNIC、VM ホストインターフェイス、および vEdge Cloud インターフェイス間のマッピングをまとめたものです。

表 8:

vNIC	VM ホストのインターフェイス	vEdge Cloud 設定のインターフェイス
vNIC 1	eth0	VPN 512 の mgmt0
vNIC 2	eth1	ge0/0

vNIC	VM ホストのインターフェイス	vEdge Cloud 設定のインターフェイス
vNIC 3 ~ 7	eth2 ~ eth7	ge0/1 ~ ge0/7

次のステップ

「vEdge Cloud ルータへの署名付き証明書のインストール」を参照してください。

WAN エッジルータの証明書認証設定の設定

証明書は、オーバーレイネットワーク内のルータの認証に使用されます。認証が完了すると、ルータはオーバーレイネットワーク内の他のデバイスとのセキュアなセッションを確立できます。

デフォルトでは、WAN エッジクラウド証明書認証は自動化されています。これは推奨の設定です。

サードパーティの証明書承認を使用する場合は、証明書承認を手動に設定します。

1. Cisco vManage メニューから、**[Administration]** > **[Settings]**の順に選択します。
2. ハードウェア WAN エッジ証明書の認証の場合は **[Edit]** をクリックします。
3. **[Security]** で、**[Enterprise Certificate]** (エンタープライズ CA による署名付き) を選択します。
4. **[Save]** をクリックします。

vEdge Cloud ルータへの署名付き証明書のインストール

vEdge Cloud ルータの仮想マシン (VM) インスタンスが起動すると、ルータの起動を許可する工場出荷時のデフォルト構成になります。ただし、ルータはオーバーレイネットワークに参加できません。ルータがオーバーレイネットワークに参加できるようにするには、そのルータに署名付き証明書をインストールする必要があります。署名付き証明書は、ルータのシリアル番号に基づいて生成され、ルータがオーバーレイネットワークに参加することを承認するために使用されます。

リリース 17.1 以降、Cisco vManage は認証局 (CA) として機能でき、このロールでは、署名付き証明書を自動的に生成して vEdge Cloud ルータにインストールすることができます。別の CA を使用し、署名付き証明書を手動でインストールすることもできます。リリース 16.3 以前の場合は、署名付きの Symantec 証明書を vEdge Cloud ルータに手動でインストールしてください。

署名付き証明書をインストールするには、次の手順を実行します。

1. vEdge 認定シリアル番号ファイルを取得します。このファイルには、オーバーレイネットワークへの参加が許可されているすべての vEdge ルータのシリアル番号が含まれています。

2. vEdge 認定シリアル番号ファイルを Cisco vManage にアップロードします。
3. 各 vEdge Cloud ルータに署名付き証明書をインストールします。

vEdge 認定シリアル番号ファイルの取得

1. <http://viptela.com/support/> にアクセスしてログインします。
2. [Download] をクリックします。
3. [My Serial Number Files] をクリックします。画面にシリアル番号ファイルが表示されます。リリース 17.1 以降、ファイル名の拡張子は .viptela です。リリース 16.3 以前の場合、ファイル名の拡張子は .txt です。
4. 最新のシリアル番号ファイルをクリックしてダウンロードします。

vEdge 認定シリアル番号ファイルのアップロード

1. Cisco vManage メニューから、[Configuration] > [Devices] の順に選択します。
2. [vEdge List] をクリックし、[Upload vEdge List] を選択します。
3. [Upload vEdge] ウィンドウで、次の手順を実行します。
 1. [Choose File] をクリックし、シスコからダウンロードした vEdge 認定シリアル番号ファイルを選択します。
 2. vEdge ルータを自動的に検証してシリアル番号をコントローラに送信するには、[Validate the Uploaded vEdge List and Send to Controllers] チェックボックスをクリックしてオンにします。このオプションをオフにする場合は、[Configuration] > [Certificates] > [vEdge List] ページで各ルータを個別に検証する必要があります。
4. [Upload] をクリックします。

vEdge 認定シリアル番号ファイルのアップロードプロセス中に、Cisco vManage は、ファイルにリストされている各 vEdge Cloud ルータのトークンを生成します。このトークンは、ルータのワンタイムパスワードとして使用されます。Cisco vManage は、トークンを vBond Orchestrator と vSmart コントローラに送信します。

vEdge 認定シリアル番号ファイルがアップロードされると、ネットワーク内の vEdge ルータのリストが [Configuration] > [Devices] ページの [vEdge Routers] テーブルに表示され、ルータのシャーン番号とそのトークンを含む各ルータの詳細情報が示されます。

リリース 17.1 以降での署名付き証明書のインストール

リリース 17.1 以降、署名付き証明書を vEdge Cloud ルータにインストールするには、最初に、そのルータのブートストラップ構成ファイルを生成してダウンロードします。このファイルには、Cisco vManage による vEdge Cloud ルータの署名付き証明書の生成を可能にするために必要なすべての情報が含まれています。次に、このファイルの内容をルータの VM インスタンスの構成にコピーします。この方式を使用するには、ルータと Cisco vManage の両方がリリース

17.1以降を実行している必要があります。最後に、署名付き証明書をルータにダウンロードします。これを自動または手動で実行するように Cisco vManage を設定できます。

ブートストラップ構成ファイルには次の情報が含まれています。

- **UUID**。これは、ルータのシャーシ番号として使用されます。
- **トークン**。これは、ルータが vBond Orchestrator と Cisco vManage で自身を認証するために使用する、ランダムに生成されるワンタイムパスワードです。
- **vBond Orchestrator の IP アドレスまたは DNS 名**。
- **組織名**。
- **デバイス構成テンプレートをすでに作成し、vEdge Cloud ルータにアタッチしている場合、ブートストラップ構成ファイルにはこの構成が含まれています。構成テンプレートの作成およびアタッチについては、「vEdge ルータの構成テンプレートの作成」を参照してください。**

個別のルータまたは複数のルータに関する情報を含むブートストラップ構成ファイルを生成できます。

リリース 17.1以降では、後で説明するように、各ルータに手動でインストールする署名付き証明書を Symantec に生成させることもできますが、その方式は推奨されません。

Cisco vBond オーケストレーション および組織名の設定

ブートストラップ構成ファイルを生成するには、vBond Orchestrator の DNS 名またはアドレスと組織名を設定する必要があります。

1. Cisco vManage メニューから、**[Administration] > [Settings]** の順に選択します。
2. vBond の場合は、**[Edit]** をクリックします。
3. **[vBond DNS/IP Address: Port]** フィールドに vBond Orchestrator の DNS 名または IP アドレスを入力します。
4. **[Save]** をクリックします。
5. 組織名の場合は、**[View]** をクリックし、設定されている組織名を確認します。この名前は、Cisco vBond オーケストレーション で設定されたものと同じである必要があります。
6. **[Save]** をクリックします。

自動または手動の vEdge Cloud 認証の設定

ルータのオーバーレイネットワークへの参加が承認されるように、署名付き証明書を各 vEdge Cloud ルータにインストールする必要があります。Cisco vManage を CA として使用して署名付き証明書を生成およびインストールするか、エンタープライズ CA を使用して署名付き証明書をインストールすることができます。

Cisco vManage を CA として使用することをお勧めします。このロールでは、Cisco vManage が署名付き証明書を自動的に生成して vEdge Cloud ルータにインストールします。Cisco vManage

を CA として機能させることがデフォルト設定です。この設定は、Cisco vManage の **[Administration]** > **[Settings]** ページにある **[WAN vEdge Cloud Certificate Authorization]** で確認できます。

エンタープライズ CA を使用して vEdge Cloud ルータの署名付き証明書を生成するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Administration]** > **[Settings]** の順に選択します。
2. **[WAN Edge Cloud Certificate Authorization]** で **[Manual]** を選択します。
3. **[Save]** をクリックします。

ブートストラップ構成ファイルの生成

vEdge Cloud ルータのブートストラップ構成ファイルを生成するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]** の順に選択します。
2. 1 つ以上の vEdge Cloud ルータのブートストラップ構成ファイルを生成するには、次の手順を実行します。
 1. **[WAN Edge List]** をクリックし、**[Export Bootstrap Configuration]** を選択します。
 2. **[Generate Bootstrap Configuration]** フィールドで、ファイル形式を選択します。
 - KVM ハイパーバイザまたは AWS サーバー上の vEdge Cloud ルータの場合は、**[Cloud-Init]** を選択して、トークン、vBond Orchestrator の IP アドレス、vEdge Cloud ルータの UUID、および組織名を生成します。
 - VMware ハイパーバイザ上の vEdge Cloud ルータの場合は、**[Encoded String]** を選択して、エンコードされた文字列を生成します。
 3. **[Available Devices]** 列から、1 つ以上のルータを選択します。
 4. 右向きの矢印をクリックして、選択したルータを **[Selected Devices]** 列に移動させます。
 5. **[Generate Generic Configuration]** をクリックします。ブートストラップ構成は、ルータごとに 1 つの .cfg ファイルが含まれている .zip ファイルでダウンロードされます。
3. vEdge Cloud ルータごとに個別にブートストラップ構成ファイルを生成するには、次の手順を実行します。
 1. **[WAN Edge List]** をクリックし、目的の vEdge Cloud ルータを選択します。
 2. 目的の vEdge Cloud ルータについて、**[...]** をクリックし、**[Generate Bootstrap Configuration]** を選択します。
 3. **[Generate Bootstrap Configuration]** ウィンドウで、ファイル形式を選択します。
 - KVM ハイパーバイザまたは AWS サーバー上の vEdge Cloud ルータの場合は、**[Cloud-Init]** を選択して、トークン、vBond Orchestrator の IP アドレス、vEdge Cloud ルータの UUID、および組織名を生成します。

- VMware ハイパーバイザ上の vEdge Cloud ルータの場合は、[Encoded String] を選択して、エンコードされた文字列を生成します。



(注) Cisco vManage リリース 20.7.1 以降、Cisco vEdge デバイスのブートストラップ構成ファイルを生成するときに使用できるオプションがあり、2つの異なる形式のブートストラップ構成ファイルを生成できます。

- Cisco SD-WAN リリース 20.4.x 以前を使用している Cisco vEdge デバイスのブートストラップ構成ファイルを生成している場合は、[The version of this device is 20.4.x or earlier] チェックボックスをオンにします。
- Cisco SD-WAN リリース 20.5.1 以降を使用している Cisco vEdge デバイスのブートストラップ構成を生成する場合は、チェックボックスを使用しないでください。

4. [Download] をクリックしてブートストラップ構成をダウンロードします。ブートストラップ構成は、.cfg ファイルでダウンロードされます。

その後、ブートストラップ構成ファイルの内容を使用して、AWS、ESXi、またはKVMのvEdge Cloud ルータインスタンスを設定します。たとえば、AWS のルータインスタンスを設定するには、Cloud-Init 構成のテキストを [User data] フィールドに貼り付けます。

デフォルトでは、**ge0/0** インターフェイスがルータのトンネルインターフェイスであり、DHCP クライアントとして設定されています。別のインターフェイスを使用するか静的 IP アドレスを使用する場合、デバイス構成テンプレートをルータにアタッチしていないときは、CLI から vEdge Cloud ルータの構成を変更します。「ネットワーク インターフェイスの設定」を参照してください。

vEdge Cloud ルータへの証明書のインストール

デフォルトの自動化された vEdge Cloud 証明書認証を使用している場合、vEdge Cloud ルータインスタンスを設定すると、Cisco vManage によって証明書がルータに自動的にインストールされ、ルータのトークンがシリアル番号に変更されます。ルータのシリアル番号は[Configuration]> [Devices] ページで確認できます。Cisco vManage へのルータの制御接続が確立されると、ルータにアタッチされたテンプレートがルータに自動的にプッシュされます。

手動の vEdge Cloud 証明書認証を使用している場合は、vEdge Cloud ルータインスタンスを設定した後、次の手順に従ってルータに証明書をインストールします。

1. ルータにエンタープライズルート証明書チェーンをインストールします。

```
vEdge# request root-cert-chain install filename [vpn vpn-id]
```

その後、Cisco vManage が CSR を生成します。

2. CSR をダウンロードします。

1. Cisco vManage メニューから、[Configuration] > [Certificates] の順に選択します。

2. 証明書に署名するために選択した vEdge Cloud ルータについて、[...] をクリックし、[View CSR] を選択します。
3. CSR をダウンロードするには、[Download] をクリックします。
3. 証明書をサードパーティの署名機関に送信して、署名してもらいます。
4. 証明書をデバイスにインポートします。
 1. Cisco vManage メニューから、[Configuration] > [Certificates] の順に選択します。
 2. [Controllers] をクリックし、[Install Certificate] を選択します。
 3. [Install Certificate] ページで証明書を [Certificate Text] フィールドに貼り付けるか、[Select a File] をクリックしてファイルの証明書をアップロードします。
 4. [Install] をクリックします。
5. Cisco vManage の IP アドレスを指定して、次の REST API コールを発行します。

```
https://vmanage-ip-address/dataservice/system/device/sync/rootcertchain
```

CLI からの vEdge Cloud ルータブートストラップ構成の作成

Cisco vManage を使用して vEdge Cloud ルータのブートストラップ構成を生成することをお勧めします。何らかの理由でこれを実行できない場合は、CLI を使用してブートストラップ構成を作成できます。ただし、このプロセスでは、引き続き Cisco vManage を使用する必要があります。ブートストラップ構成に関するこの情報の一部を Cisco vManage から収集し、ブートストラップ構成を作成した後に、Cisco vManage を使用して署名付き証明書をルータにインストールします。

CLI からブートストラップ構成を作成して署名付き証明書をインストールするには、次の 3 つの手順を実行します。

1. ルータの構成ファイルを編集して vBond Orchestrator の DNS 名または IP アドレスと組織名を追加します。
2. ルータのシャーン番号とトークン番号を Cisco vManage に送信します。
3. Cisco vManage に vEdge Cloud ルータを認証させ、署名付き証明書をルータにインストールさせます。

CLI から vEdge Cloud ルータの構成ファイルを編集するには、次の手順を実行します。

1. SSH 経由で vEdge Cloud ルータへの CLI セッションを開きます。Cisco vManage でこれを実行するには、[Tools] > [SSH Terminal] ページを選択し、目的のルータを選択します。
2. **admin** ユーザーとして、デフォルトのパスワード **admin** を使用してログインします。CLI プロンプトが表示されます。
3. コンフィギュレーション モードに入ります。

```
vEdge# config
vEdge(config)#
```

4. vBond Orchestrator の IP アドレスまたは vBond Orchestrator を指す DNS 名を設定します。vBond Orchestrator の IP アドレスは、パブリック IP アドレスである必要があります。

```
vEdge(config)# system vbond (dns-name | ip-address)
```

5. 組織名を設定します。

```
vEdge(config-system)# organization-name name
```

6. 設定をコミットします。

```
vEdge(config)# commit and-quit
vEdge#
```

vEdge Cloud ルータのシャーン番号とトークン番号を Cisco vManage に送信するには、次の手順を実行します。

1. vEdge Cloud ルータのトークン番号とシャーン番号を確認します。
 1. Cisco vManage メニューから、**[Configuration] > [Devices]** の順に選択します。
 2. **[WAN Edge List]** をクリックし、目的の vEdge Cloud ルータを確認します。
 3. vEdge Cloud ルータの **[Serial No./Token]** 列と **[Chassis Number]** 列の値を書き留めます。
2. ルータのブートストラップ構成情報を Cisco vManage に送信します。

```
vEdge# request vedge-cloud activate chassis-number chassis-number token token-number
```

ルータで **show control local-properties** コマンドを発行して、vBond の IP アドレス、組織名、シャーン番号、およびトークンを確認します。証明書が有効かどうかを確認することもできます。

最後に、Cisco vManage に vEdge Cloud ルータを認証させ、署名付き証明書をルータにインストールさせます。

デフォルトの自動化された vEdge Cloud 証明書認証を使用している場合は、Cisco vManage がシャーン番号とトークン番号を使用してルータを認証します。その後、Cisco vManage によって証明書がルータに自動的にインストールされ、ルータのトークンがシリアル番号に変更されます。ルータのシリアル番号は **[Configuration] > [Devices]** ページで確認できます。Cisco vManage へのルータの制御接続が確立されると、ルータにアタッチされたテンプレートがルータに自動的にプッシュされます。

手動の vEdge Cloud 証明書認証を使用している場合は、vEdge Cloud ルータインスタンスを設定した後、次の手順に従ってルータに証明書をインストールします。

1. ルータにエンタープライズルート証明書チェーンをインストールします。

```
vEdge# request root-cert-chain install filename [vpn vpn-id]
```

ルートチェーン証明書をルータにインストールした後に、Cisco vManage がシャーン番号とトークン番号を受け取ると、Cisco vManage が CSR を生成します。

2. CSR をダウンロードします。

1. Cisco vManage メニューから、**[Configuration]** > **[Certificates]** の順に選択します。
2. 証明書に署名するために選択した vEdge Cloud ルータについて、[...] をクリックし、**[View CSR]** を選択します。
3. CSR をダウンロードするには、**[Download]** をクリックします。
3. 証明書をサードパーティの署名機関に送信して、署名してもらいます。
4. 証明書をデバイスにインポートします。
 1. Cisco vManage メニューから、**[Configuration]** > **[Certificates]** の順に選択します。
 2. **[Controllers]** をクリックし、**[Install Certificate]** を選択します。
 3. **[Install Certificate]** ページで証明書を **[Certificate Text]** フィールドに貼り付けるか、**[Select a File]** をクリックしてファイルの証明書をアップロードします。
 4. **[Install]** をクリックします。
5. Cisco vManage の IP アドレスを指定して、次の REST API コールを発行します。
<https://vmanage-ip-address/dataservice/system/device/sync/rootcertchain>

リリース 16.3 以前での署名付き証明書のインストール

リリース 16.3 以前を実行している vEdge Cloud ルータ仮想マシン (VM) インスタンスの場合、vEdge Cloud ルータ VM が起動すると、工場出荷時のデフォルト構成になりますが、署名付き証明書がインストールされていないため、オーバーレイネットワークに参加できません。vEdge Cloud ルータがオーバーレイネットワークに参加できるように、署名付き Symantec 証明書をルータにインストールする必要があります。

証明書署名要求 (CSR) を生成し、署名付き証明書を vEdge Cloud ルータにインストールするには、次の手順を実行します。

1. デフォルトパスワードの **admin** を使用して、ユーザー **admin** として vEdge Cloud ルータにログインします。vEdge Cloud ルータが AWS を通じて提供されている場合は、AWS キーペアを使用してログインします。CLI プロンプトが表示されます。
2. vEdge Cloud ルータの CSR を生成します。

```
vEdge# request csr upload path
```

path は、CSR をアップロードする完全なパスおよびファイル名です。このパスには、ローカルデバイスのディレクトリか、FTP、HTTP、SCP、または TFTP を介して到達可能なリモートデバイスのディレクトリを設定できます。SCP を使用している場合は、ディレクトリ名とファイル名の入力を求められます。ファイルパス名は提供されません。プロンプトが表示されたら、組織名を入力して確認します。次に例を示します。

```
vEdge# request csr upload home/admin/vm9.csr
Uploading CSR via VPN 0
Enter organization name          : Cisco
Re-enter organization name       : Cisco
Generating CSR for this vEdge device
```

```
..... [DONE]
Copying ... /home/admin/vm9.csr via VPN 0
CSR upload successful
```

3. Symantec 証明書登録ポータルにログインします。

https://catmanager.websecurity.symantec.com/mcep/enroll/index?jur_hash=f422d7ceb508a24e32ea7de4f78d37

4. [Select Certificate Type] ドロップダウンで、[Standard Intranet SSL] を選択し、[Go] をクリックします。[Certificate Enrollment] ページが表示されます。Cisco SD-WAN は、このフォームで入力された情報を使用して、証明書要求者の ID を確認し、証明書要求を承認します。証明書登録フォームに入力するには、次の手順を実行します。

1. [Your Contact Information] セクションに、要求者の名、姓、および電子メールアドレスを入力します。
2. [Server Platform and Certificate Signing] セクションの [Select Server Platform] ドロップダウンから [Apache] を選択します。[Enter Certificate Signing Request (CSR)] ボックスで、生成された CSR ファイルをアップロードするか、CSR ファイルの内容をコピーして貼り付けます（この実行方法の詳細については、support.viptela.com にログインし、[Certificate] をクリックして、Symantec 証明書の説明を参照してください）。
3. [Certificate Options] セクションに、証明書の有効期間を入力します。
4. [Challenge Phrase] セクションに、チャレンジフレーズを入力し、その後、再入力します。Symantec カスタマーポータルで、チャレンジフレーズを使用して、証明書を更新し、必要に応じて失効させます。CSR ごとに異なるチャレンジフレーズを指定することをお勧めします。
5. 加入者契約に同意します。システムが確認メッセージを生成し、証明書要求確認の電子メールを要求者に送信します。また、CSR 承認のための電子メールをシスコに送信します。

5. シスコが CSR を承認すると、Symantec は署名付き証明書を要求者に送信します。署名付き証明書は、Symantec 登録ポータルからも入手できます。

6. vEdge Cloud ルータに証明書をインストールします。

```
vEdge# request certificate install filename [vpn vpn-id]
```

このファイルは、ローカルデバイスのホームディレクトリか、FTP、HTTP、SCP、または TFTP を介して到達可能なリモートデバイスに保存できます。SCP を使用している場合は、ディレクトリ名とファイル名の入力を求められます。ファイルパス名は提供されません。

7. 証明書がインストールされており、有効であることを確認します。

```
vEdge# show certificate validity
```

vEdge Cloud ルータに証明書をインストールすると、vBond Orchestrator はルータを検証および認証できるようになり、ルータはオーバーレイネットワークに参加できるようになります。

次のステップ

「vEdge のシリアル番号をコントローラデバイスに送信する」を参照してください。

ルータのシリアル番号をコントローラデバイスに送信する

表 9: 機能の履歴

機能名	リリース情報	説明
デバイスのオンボーディングの機能強化	Cisco IOS XE リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能は、.csv ファイルを直接アップロードすることにより、Cisco vManage へのデバイスのオンボードを強化します。

許可されたルータのみがオーバーレイネットワークに参加できます。コントローラデバイス 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は、ルータ認定シリアル番号ファイルから、オーバーレイネットワークへの参加を認可されているルータを学習します。これは、シスコから受け取るファイルです。ルータ認定シリアル番号ファイルには、すべての認定ルータのシリアル番号と対応するシャーシ番号がリストされています。ネットワーク内の Cisco vManage の 1 つにファイルをアップロードすると、そのファイルがコントローラに配布されます。

ルータのシリアル番号ファイルをアップロードすると、ルータを次のいずれかの状態にできます。

- 無効：電源投入時、ルータはオーバーレイネットワークへの参加を承認されません。
- ステージング：電源投入時、ルータは検証され、オーバーレイネットワークへの参加が承認され、コントロールプレーンへの接続のみを確立できます。コントロールプレーンを介して、ルータは Cisco vManage からその設定を受信します。ただし、ルータはデータプレーン接続を確立できないため、ネットワーク内の他のルータと通信できません。ステージング状態は、ルータを 1 つの場所で準備し、インストールのために別のサイトにルータを送信する場合に役立ちます。ルータが最終的な宛先に到達したら、状態をステージングから有効に変更して、ルータがデータプレーン接続を確立し、オーバーレイネットワークに完全に参加できるようにします。
- 有効：電源投入時、ルータは検証され、オーバーレイネットワークへの参加が承認され、ネットワーク内でコントロールプレーンとデータプレーンの両方の接続を確立できます。コントロールプレーンを介して、ルータは Cisco vManage からその設定を受信します。また、データプレーンを介して他のルータと通信できます。有効な状態は、ルータが最終的な宛先にインストールされているときに役立ちます。

ルータ認定シリアル番号ファイルのアップロード方法

次のセクションでは、ルータの認証済みシリアル番号ファイルを Cisco vManage にアップロードして、すべてのオーバーレイネットワークのコントローラにファイルを配布する方法について説明します。

PnP Connect Sync の有効化 (オプション)

アップロードされたデバイスをスマートアカウントまたはバーチャルアカウントに同期させ、デバイスが PnP (Plug and Play) Connect ポータルに反映されるようにするには、署名のない .csv ファイルが Cisco vManage を介してアップロードされたときに、PnP Connect Sync を有効にします。

PnP (Plug and Play) Connect ポータルへのアクティブな接続と、アクティブなスマートアカウントおよびバーチャルアカウントがあることを確認します。また、PnP Connect ポータルで、アカウントのスマートアカウントまたはバーチャルアカウント管理者として関連付けられている CCO ID を使用する必要があります。



(注) PnP Connect Sync は、.csv ファイルのアップロードにのみ適用されます。.viptela ファイル (PnP Connect ポータルからダウンロード) のアップロードプロセスには影響しません。



(注) スマートアカウントのログイン情報を入力した場合にのみ、PnP Connect Sync を有効にできます。

PnP Connect Sync を有効にするには、次の手順を実行します。

1. Cisco vManage メニューから、**[Administration]** > **[Settings]** の順に選択します。
2. **[Smart Account Credentials]** に移動し、**[Edit]** をクリックします。
3. ユーザー名とパスワードを入力し、**[Save]** をクリックします。
4. **[PnP Connect Sync]** に移動し、**[Edit]** をクリックします。
5. **[Enabled]** をクリックし、**[Save]** をクリックします。

ルータを有効状態にする

ルータがコントロールプレーンおよびデータプレーン接続を確立し、Cisco vManage から設定を受信できるようにルータを有効状態にするには、次のタスクを実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]** の順に選択します。
2. **[WAN Edge List]** をクリックし、**[Upload WAN Edge List]** をクリックします。
3. WAN エッジデバイスは、次の 2 つの方法でアップロードできます。
 - 署名付きファイル (.viptela ファイル) をアップロードします。この .viptela ファイルは、Plug and Play Connect ポータルからダウンロードできます。
 - Cisco vManage リリース 20.3.1 以降では、署名されていないファイル (.csv ファイル) をアップロードできます。この拡張機能は、ハードウェアプラットフォームをオンデマンドで Cisco vManage に追加する場合にのみ適用されます。.csv ファイルをアップロードするには、次の操作を実行します。

1. [Sample CSV] をクリックします。エクセルファイルがダウンロードされます。
2. ダウンロードした .csv ファイルを開きます。次のパラメータを入力します。
 - シャーシ番号
 - 製品 ID (Cisco vEdge デバイス では必須、他のすべてのデバイスの場合は空白の値)
 - Serial number
 - SUDI シリアル

Cisco IOS XE SD-WAN デバイス では、シャーシ番号に加えてシリアル番号または SUDI 番号のいずれかが必須です。Cisco ASR1002-X は例外で、シリアル番号または SUDI 番号は必要ありません。 .csv ファイルのシャーシ番号のみでオンボードできます。

3. Cisco vManage でデバイスの詳細を表示するには、[Tools] > [SSH Terminal] に移動します。 デバイスを選択し、次のいずれかのコマンドを使用します。
show certificate serial (Cisco vEdge デバイスの場合)
show sdwan certificate serial (Cisco IOS XE SD-WAN デバイス の場合)
4. ダウンロードした .csv ファイルに具体的なデバイスの詳細を入力します。

4. .viptela または .csv ファイルを Cisco vManage にアップロードするには、[Choose file] をクリックして、デバイスの製品 ID、シリアル番号、およびシャーシ番号を含むファイルをアップロードします。



- (注) PnP Sync Connect を有効にしている場合、.csv ファイルには最大 25 個のデバイスを含めることができます。25 個を超えるデバイスがある場合は、複数のファイルに分割してアップロードできます。

5. [Validate the uploaded vEdge List and send to controllers] の隣にあるチェックボックスをオンにします。
6. [Upload] をクリックします。
7. デバイスの表にデバイスがリストされているはずですが、
以前に PnP Sync Connect を有効にしている場合、デバイスは PnP ポータルにも反映されません。

ネットワーク内のルータのリストが表示され、各ルータに関する詳細情報が表示されます。ルータが有効な状態であることを確認するには、[Configuration] > [Certificates] を選択します。

ルータを無効な状態にする

認証シリアル番号ファイルを Cisco vManage にアップロードし、ルータを無効な状態にして、コントロールプレーンまたはデータプレーン接続を確立できず、Cisco vManage から設定を受信できないようにするには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration] > [Devices]**の順に選択します。
2. **[WAN Edge List]** をクリックし、**[Upload WAN Edge List]** をクリックします。
3. **[Upload WAN Edge List]** ダイアログボックスで、アップロードするファイルを選択します。
4. ルータのシリアル番号ファイルをアップロードするには、**[Upload]** をクリックします。
Cisco vManage

ネットワーク内のルータのリストが表示され、各ルータに関する詳細情報が表示されます。ルータが無効な状態であることを確認するには、Cisco vManage メニューから、**[Configuration] > [Certificates]**の順に選択します。

ルータをステージング状態にする

ルータを無効状態からステージング状態に移行させ、シリアル番号ファイルをコントローラに送信するには、次の手順を実行します。ステージング状態では、ルータは、コントロールプレーン接続を確立し、それを介して Cisco vManage から構成を受信できます。ただし、ルータは、データプレーン接続を確立できません。

1. Cisco vManage メニューから、**[Configuration] > [Certificates]** の順に選択します。
2. **[WAN Edge List]** をクリックします。
3. **[Validate]** 列で、各ルータの **[Staging]** をクリックします。
4. **[Send to Controller]** をクリックします。
5. ルータをオーバーレイネットワークのデータプレーンに参加させる準備ができたなら、**[Validate]** 列で、各ルータの **[Valid]** をクリックし、**[Send to Controller]** をクリックします。ルータを有効状態にすると、データプレーン接続を確立し、オーバーレイネットワーク内の他のルータと通信できるようになります。

vEdge ルータの設定

vEdge クラウドルータの仮想マシン (VM) を設定して起動し、オーバーレイネットワークでハードウェア vEdge ルータをセットアップして起動すると、工場出荷時のデフォルト設定で起動します。



- (注) **デバイスへの初回ログイン** : Cisco SD-WAN オーバーレイネットワークを初めて展開するときは、Cisco vBond オーケストレーション、Cisco vManage、および Cisco vSmart コントローラにログインして、デバイスの初期設定を手動で作成します。ルータは、工場出荷時のデフォルト設定で出荷されています。この設定を手動で変更する場合は、ルータのコンソールポートからログインします。

オーバーレイネットワークを動作可能にし、vEdge ルータがオーバーレイネットワークに参加できるようにするには、次の手順を実行する必要があります。

- VPN 0 の少なくとも 1 つのインターフェイスでトンネルインターフェイスを設定します。このインターフェイスは、すべての Cisco vEdge デバイスにアクセス可能な WAN トランスポートネットワークに接続する必要があります。VPN 0 は、オーバーレイネットワーク内の Cisco vEdge デバイス間ですべてのコントロールプレーントラフィックを伝送します。
- オーバーレイ管理プロトコル (OMP) が有効になっていることを確認します。OMP は、Cisco SD-WAN コントロールプレーンの確立と維持を行うプロトコルで、デフォルトで有効になっており、無効にすることはできません。CLI から設定を編集する場合は、**omp** 設定コマンドを削除しないでください。
- BFD が有効になっていることを確認します。BFD は、vEdge ルータのトランスポートトンネルがオーバーレイネットワーク経由でデータトラフィックを送信するために使用するプロトコルです。BFD はデフォルトで有効になっており、無効にすることはできません。CLI から設定を編集する場合は、**bfd color** コマンドを削除しないでください。
- ネットワークの vBond オーケストレーターの DNS 名の IP アドレスを設定します。
- ルータの IP アドレスを設定します。



- (注) DNS キャッシュのタイムアウトは、DNS が解決する必要がある Cisco vBond オーケストレーションの IP アドレスの数に比例する必要があります。そうしないと、リンク障害中に Cisco vManage の制御接続が行われない可能性があります。これは、チェック対象の IP アドレスが 6 つ以上ある場合 (デフォルトの DNS キャッシュタイムアウトは現在 2 分であるため、これは推奨数です)、最も優先されるインターフェイスがすべての vBond IP アドレスを試行しても、別の色にフェールオーバーする前に、DNS キャッシュタイマーが期限切れになるためです。たとえば、1 つの IP アドレスへの接続を試みるのに約 20 秒かかります。したがって、解決する IP アドレスが 8 つある場合、DNS キャッシュのタイムアウトは $20 \times 8 = 160$ 秒、つまり 3 分になります。

また、各 vEdge ルータにシステム IP アドレスを割り当てる必要があります。このアドレスは、Cisco vEdge 以外のデバイスのルータ ID に似ており、インターフェイスアドレスとは独立して

ルータを識別する永続的なアドレスです。システム IP は、デバイスの TLOC アドレスのコンポーネントです。デバイスのシステム IP アドレスを設定すると、Cisco vEdge デバイスの到達可能性に影響を与えることなく、必要に応じてインターフェイスの番号を付け直すことができます。Cisco vSmart コントローラと vEdge ルータ間、および Cisco vSmart コントローラと Cisco vBond オーケストレーション間のセキュアな DTLS または TLS 接続を介した制御トラフィックは、システム IP アドレスによって識別されるシステムインターフェイスを介して送信されます。トランスポート VPN (VPN 0) では、システム IP アドレスがデバイスのループバックアドレスとして使用されます。同じアドレスを VPN0 の別のインターフェイスに使用することはできません。

ネットワークトポロジに必要なその他の機能を設定することもできます。

Cisco vManage で設定テンプレートを作成して、vEdge ルータを設定します。設定テンプレートごとに1つまたは複数の機能テンプレートを作成し、それを vEdge ルータのデバイステンプレートに統合します。次に、デバイステンプレートを vEdge ルータにアタッチします。vEdge ルータがオーバーレイネットワークに参加すると、Cisco vManage は設定テンプレートをルータに自動的にプッシュします。

Cisco vManage で設定テンプレートを作成して、vEdge ルータの完全な設定を作成することを強くお勧めします。Cisco vManage は、オーバーレイネットワーク内のルータを検出すると、適切な設定テンプレートをデバイスにプッシュします。設定テンプレートの設定パラメータは、初期設定を上書きします。

vEdge ルータの設定テンプレートの作成

vEdge 設定テンプレートを作成するには、最初に機能テンプレートを作成します。

1. Cisco vManage メニューから、**[Configuration] > [Templates]** を選択します。
2. **[Feature Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Feature Templates]** は **[Feature]** と呼ばれません。

3. **[Add template]** をクリックします。
4. 左ペインで、vEdge Cloud またはルータモデルを選択します。
5. 右ペインで、**[System feature template]** を選択します。次のパラメータを設定します。
 1. テンプレート名
 2. 説明
 3. サイト ID
 4. システム IP
 5. Timezone
 6. ホスト名

7. コンソールのボーレート (vEdge ハードウェアルータのみ)
8. GPS 位置情報
6. [Save] をクリックして、システムテンプレートを保存します。
7. 右ペインで、[VPN-Interface-Ethernet feature template] を選択します。次のパラメータを設定します。
 1. テンプレート名
 2. 説明
 3. シャットダウン番号
 4. インターフェイス名
 5. IPv4 アドレス (静的または DHCP)
 6. IPv6 アドレス (DHCPv6 の静的) (リリース 16.3 以降必要に応じて)
 7. トンネルインターフェイス (VPN 0 の場合)、色、カプセル化、および許可するサービス。
8. [Save] をクリックして、VPN インターフェイスイーサネットテンプレートを保存します。
9. 右ペインで、他のテンプレートを選択して、必要な機能を設定します。設定が完了したら、各テンプレートを保存します。vEdge 100m および vEdge 100wm ルータのセルラーパラメータの設定については、この記事の次のセクションを参照してください。

設定テンプレートとパラメータについては、ご使用のソフトウェアリリースの vManage 設定ヘルプ記事を参照してください。

次に、vEdge ルータのすべての機能テンプレートを組み込んだデバイステンプレートを作成します。

1. Cisco vManage メニューから、[Configuration] > [Templates] の順に選択します。
2. [Device Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。

3. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
4. [Device Model] ドロップダウンから、デバイステンプレートを作成するデバイスのタイプを選択します。Cisco vManage には選択したデバイスタイプの機能テンプレートが表示されます。必須のテンプレートはアスタリスク (*) で示されます。
5. デバイステンプレートの名前と説明を入力します。これらのフィールドは必須です。テンプレート名には特殊文字は使用できません。

6. [Transport & Management VPN] セクションの [VPN 0] で、使用可能なテンプレートのドロップダウンリストから、目的の機能テンプレートを選択します。使用可能なテンプレートのリストには、以前に作成したテンプレートが表示されます。
7. デバイステンプレートに追加の機能テンプレートを含めるには、残りのセクションで機能テンプレートを順に選択し、使用可能なテンプレートのドロップダウンリストから目的のテンプレートを選択します。使用可能なテンプレートのリストは、以前に作成したテンプレートです。すべての必須機能テンプレート、および目的の任意の機能テンプレートのテンプレートを選択していることを確認してください。
8. [Create] をクリックしてデバイステンプレートを作成します。

デバイステンプレートをデバイスにアタッチするには、次の手順を実行します。

1. Cisco vManage メニューから、[Configuration] > [Templates] の順に選択します。
2. [Device Templates] をクリックし、テンプレートを選択します。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。

3. 選択したデバイステンプレートについて、[...] をクリックし、[Attach Device] を選択します。
4. [Attach Device] ウィンドウで、デバイスを検索するか、[Available Device(s)] 列からデバイスを選択します。
5. 右向きの矢印をクリックして、デバイスを右側の [Selected Devices] 列に移動します。
6. [Attach] をクリックします。

vEdge ルータがオーバーレイネットワークに参加したことを検出すると、Cisco vManage は設定テンプレートをルータにプッシュします。

セルラールータの設定

vEdge 100m および vEdge 100wm ルータの場合、VPN インターフェイスセルラー機能テンプレートでセルラーインターフェイスパラメータを設定します。このテンプレートでは、デフォルトのプロファイル ID は 0 であり、自動プロファイル選択が有効になります。自動プロファイルはルータの SIM カードのモバイル国コード/モバイルネットワークコード (MCC/MNC) の値を使用します。プロファイルが 0 の場合、セルラールータは Cisco SD-WAN ZTP 自動プロビジョニングプロセス中にオーバーレイネットワークに自動的に参加できます。

MCC/MNC がサポートされていない場合、自動プロファイル選択プロセスは失敗し、ZTP プロセスはルータを自動検出できません。この場合、次のようにセルラープロファイルを設定する必要があります。

1. 右ペインで、[Cellular Profile feature template] を選択します。

2. プロファイル ID を 1 ～ 15 の値に設定し、必要なセルラーパラメータを設定します。
3. セルラープロファイル機能テンプレートを保存します。
4. 右ペインで、[VPN-Interface-Cellular template] を選択します。
5. 手順 2 で設定したプロファイル ID を選択し、[Shutdown] で [Yes] をクリックします。
6. VPN インターフェイスセルラー機能テンプレートを保存します。
7. セルラープロファイルと VPN インターフェイス セルラー テンプレートをデバイステンプレートに含めます。
8. デバイステンプレートを vEdge ルータにアタッチして、MCC/MCN をアクティブにします。
9. 右ペインで、[VPN-Interface-Cellular template] を選択します。
10. [Shutdown] で [No] をクリックして、セルラーインターフェイスを有効にします。
11. VPN インターフェイスセルラー機能テンプレートを保存します。
12. デバイステンプレートを vEdge ルータに再プッシュします。これは手順 8 でプッシュしたデバイステンプレートです。

CLI からの vEdge ルータの設定

通常、vEdge ルータ設定は vManage 設定テンプレートを使用して作成します。ただし、ネットワークテストや概念実証（POC）環境など、状況によっては、設定プロセスを高速化する目的で、またはテスト環境に Cisco vManage が含まれていないことが原因で、vEdge ルータの手動設定が必要になる場合があります。このような状況では、ルータの CLI から vEdge ルータを設定できます。



- (注) CLI から手動で vEdge ルータを設定し、その後ルータが Cisco vManage によって管理されるようになった場合、Cisco vManage がルータを検出すると、ルータの設定が vManage サーバーからルータにプッシュされ、既存の設定が上書きされます。

vEdge Cloud ルータの場合、SSH を使用してルータへの CLI セッションを開きます。ハードウェア vEdge ルータの場合は、管理コンソール経由でルータに接続します。

CLI からの最小限のパラメータの設定

CLI セッションから Cisco vEdge デバイスで初期設定を作成するには、次の手順を実行します。

1. SSH またはコンソールポートを使用して Cisco vEdge デバイス への CLI セッションを開きます。
2. **admin** ユーザーとして、デフォルトのパスワード **admin** を使用してログインします。CLI プロンプトが表示されます。

3. コンフィギュレーション モードに入ります。

```
vEdge# config
vEdge (config) #
```

4. ホスト名を設定します。

```
vEdge (config) # system host-name hostname
```

ホスト名の設定は任意ですが、ホスト名は CLI のプロンプトの一部として含まれ、さまざまな Cisco vManage ページでデバイスを参照するために使用されるため、設定することを推奨します。

5. システム IP アドレスを設定します。リリース 16.3 以降では、IP アドレスは IPv4 または IPv6 アドレスになります。以前のリリースでは、IPv4 アドレスである必要があります。

```
vEdge (config-system) #system-ip ip-address
```

Cisco vManage は、システム IP アドレスを使用してデバイスを識別し、NMS が完全な設定をデバイスにダウンロードできるようにします。

6. デバイスが配置されているサイトの数値識別子を設定します。

```
vEdge (config-system) # site-id site-id
```

7. 組織名を設定します。

```
vEdge (config-system) # organization-name organization-name
```

8. Cisco vBond オーケストレーションの IP アドレスか、Cisco vBond オーケストレーションを指す DNS 名を設定します。Cisco vBond オーケストレーションの IP アドレスは、オーバーレイネットワーク内のすべての Cisco vEdge デバイスが Cisco vBond オーケストレーションに到達できるように、パブリック IP アドレスにする必要があります。

```
vEdge (config-system) # vbond (dns-name | ip-address)
```

9. ソフトウェアアップグレードの成功を確認するための時間制限を設定します。

```
vEdge (config-system) # upgrade-confirm minutes
```

時間の範囲は 1 ~ 60 分です。この時間制限を設定する場合、デバイスのソフトウェアアップグレード時、Cisco vManage の起動時、または設定された分数以内にソフトウェアアップグレードが成功することを確認する必要があります。設定時間内に確認メッセージを受信しない場合、デバイスは以前のソフトウェアイメージに戻ります。

10. ユーザー「admin」のパスワードを変更します。

```
vEdge (config-system) # user admin password password
```

デフォルトのパスワードは「admin」です。

11. VPN 0 のインターフェイスをトンネルインターフェイスとして使用するよう設定します。VPN 0 は WAN トランスポート VPN であり、トンネルインターフェイスはオーバーレイネットワーク内のデバイス間で制御トラフィックを伝送します。vEdge Cloud ルータの場合、インターフェイス名の形式は **eth number** です。ハードウェア vEdge ルータの場合、インターフェイス名の形式は **ge slot / port** です。インターフェイスを有効にして、その IP アドレスを静的アドレスとして、または DHCP サーバーから受信した動的に割り当てられたアドレスとして設定する必要があります。リリース 16.3 以降では、アドレス

を IPv4 または IPv6 アドレスにするか、両方を設定してデュアルスタック運用を有効にできます。以前のリリースでは、IPv4 アドレスである必要があります。

```
vEdge(config)# vpn 0
vEdge(config-vpn-0)# interface interface-name
vEdge(config-interface)# (ip dhcp-client | ip address prefix/length)
vSmart(config-interface)# (ipv6 address ipv6-prefix/length | ipv6 dhcp-client
[dhcp-distance number | dhcp-rapid-commit])
vEdge(config-interface)# no shutdown
vEdge(config-interface)# tunnel-interface
```



(注) オーバーレイネットワークが起動し、Cisco vManage がオーバーレイネットワークに参加できるようにするには、VPN 0 の少なくとも 1 つのインターフェイスでトンネルインターフェイスを設定する必要があります。トンネルインターフェイスは、すべての Cisco vEdge デバイスからアクセス可能な WAN トランスポートネットワークに接続する必要があります。VPN 0 は、オーバーレイネットワーク内の Cisco vEdge デバイス間ですべてのコントロールプレーントラフィックを伝送します。

12. WAN トランスポートのタイプを識別するために、トンネルの色を設定します。デフォルトの色 (**default**) を使用できますが、実際の WAN トランスポートに応じて、**mpls** や **metro-ethernet** など、より適切な色も設定できます。

```
vEdge(config-tunnel-interface)# color color
```

13. WAN トランスポートネットワークへのデフォルトルートを設定します。

```
vEdge(config-vpn-0)# ip route 0.0.0.0/0 next-hop
```

14. 設定をコミットします。

```
vEdge(config)# commit and-quit
vEdge#
```

15. 設定が正しく、完全であることを確認します。

```
vEdge# show running-config
```

オーバーレイネットワークが起動して動作可能になったら、初期設定パラメータを含む vEdge 設定テンプレートを Cisco vManage で作成します。次の vManage 機能テンプレートを使用します。

- ホスト名、システム IP アドレス、および vBond 機能を設定するためのシステム機能テンプレート。
- 「admin」ユーザーのパスワードを設定するための AAA 機能テンプレート。
- VPN 0 のインターフェイスを設定するための VPN インターフェイスイーサネット機能テンプレート。

さらに、次の一般的なシステムパラメータを設定することを推奨します。

- Cisco vManage メニューから、**[Administration] > [Settings]**の順に選択し、組織名を設定します。

- Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。NTP およびシステム機能設定テンプレートの場合、タイムゾーン、NTP サーバー、およびデバイスの物理的な場所を設定します。
 - バナー機能設定テンプレートの場合、ログインバナーを設定します。
 - ロギング機能設定テンプレートの場合、ロギングパラメータを設定します。
 - AAA 機能構成テンプレートの場合、AAA、RADIUS サーバーおよび TACACS+ サーバーを設定します。
 - SNMP 機能構成テンプレートの場合、SNMP を設定します。

CLI 初期設定の例

以下は、vEdge ルータでの簡単な設定の例です。この構成には、工場出荷時のデフォルト設定の設定が多数含まれており、多数のデフォルト設定値が示されています。

```
vEdge# show running-config
system
 host-name          vEdge
 gps-location latitude 40.7127837
 gps-location longitude -74.00594130000002
 system-ip          172.16.251.20
 site-id            200
 max-controllers    1
 organization-name "Cisco"
 clock timezone America/Los_Angeles
 upgrade-confirm    15
 vbond 184.122.2.2
 aaa
  auth-order local radius tacacs
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password encrypted-password
  !
 logging
  disk
  enable
  !
 ntp
  keys
   authentication 1 md5 $4$L3rwZmsIic8zj4BgLEFXKw==
   authentication 2 md5 $4$LyLwZmsIif8BvrJgLEFXKw==
   authentication 60124 md5 $4$LXbzZmcKj5Bd+/BgLEFXKw==
  trusted 1 2 60124
```

```
!
server 180.20.1.2
  key 1
  source-interface ge0/3
  vpn 1
  version 4
exit
!
radius
server 180.20.1.2
  vpn 1
  source-interface ge0/3
  secret-key $4$L3rwZmsIic8zj4BgLEFXKw==
exit
!
tacacs
server 180.20.1.2
  vpn 1024
  source-interface ge0/3
  secret-key $4$L3rwZmsIic8zj4BgLEFXKw==
exit
!
!
omp
no shutdown
gradeful-restart
advertise bgp
advertise connected
advertise static
!
security
ipsec
  authentication-type ah-shal-hmac shal-hman
!
!
snmp
no shutdown
view v2
  oid 1.3.6.1
!
community private
  view v2
  authorization read-only
!
trap target vpn 0 10.0.1.1 16662
  group-name Cisco
  community-name private
!
trap group test
  all
  level critical major minor
exit
exit
!
vpn 0
interface ge0/0
ip address 184.111.20.2/24
tunnel-interface
  encapsulation ipsec
  color mpls restrict
  no allow-service bgp
  allow-service dhcp
  allow-service dns
```

```

    allow-service icmp
    no allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service ospf
    no allow-service stune
    !
    no shutdown
    bandwidth-upstream 60
    bandwidth-downstream 60
    !
    interface ge0/1
    no shutdown
    !
    interface ge0/2
    no shutdown
    !
    ip route 0.0.0.0/0 184.111.20.1

    !
    vpn 1
    router
    bgp 111000
    neighbor 172.16.1.20
    no shutdown
    remote-as 111000
    password $4$LzLwZj1ApK4zj4BgLEFXKw==
    !
    !
    ospf
    timers spf 200 1000 10000
    area 0
    interface ge0/1
    authentication type message-direct
    authentication message-digest message-digest-key 1 md5 $4$LzLwZj1ApK4zj4BgLEFXKw==

    exit
    exit
    !
    !
    !

```

WAN エッジルータからのデータストリーム収集の有効化

デフォルトでは、ネットワークデバイスからのデータストリームの収集は有効になっていません。

オーバーレイネットワークの WAN エッジルータからデータストリームを収集するには、次の手順を実行します。

データストリームを収集するには、Cisco SD-WAN ネットワークで VPN 512 を設定する必要があります。

1. Cisco vManage メニューから、**[Administration]** > **[Settings]**の順に選択します。
2. **[Data Stream]** で、**[Edit]** をクリックします。
3. **[Enabled]** をクリックします。

4. Cisco vManage リリース 20.4.1 から、次の [IP Address Type] オプションのいずれかを選択します。

- [Transport] : このオプションをクリックすると、デバイスが接続されている Cisco vManage ノードのトランスポート IP アドレスにデータストリームが送信されます。
- [Management] : このオプションをクリックすると、デバイスが接続されている Cisco vManage ノードの管理 IP アドレスにデータストリームが送信されます。
- [System] : このオプションをクリックすると、デバイスが接続されている Cisco vManage ノードの内部的に設定されたシステム IP アドレスにデータストリームが送信されます。

Cisco vManage クラスタ展開では、[System] を選択して、クラスタ内のすべての Cisco vManage インスタンスによって管理されるエッジデバイスからデータストリームが収集されるようにすることを推奨します。

5. Cisco vManage リリース 20.4.1 から、次のいずれかの操作を実行します。

- IP アドレスタイプとして [Transport] を選択した場合は、[Hostname] フィールドに、ルータへの接続に使用されるパブリックトランスポートの IP アドレスを入力します。
この IP アドレスを確認するには、SSH クライアントを使用してルータにアクセスし、**show interface** CLI コマンドを入力します。
- IP アドレスタイプとして [Management] を選択した場合は、[Hostname] フィールドに、データを収集するホストの IP アドレスまたは名前を入力します。
このホストは、アウトオブバンド管理に使用するホストであり、管理 VPN に配置することを推奨します。

[IP Address Type] が [System] の場合、この [Hostname] オプションはグレー表示されます。

6. [VPN] フィールドには、ホストが配置されている VPN の番号を入力します。

この VPN は管理 VPN（通常は VPN 512）にすることを推奨します。

[IP Address Type] が [System] の場合、この [VPN] オプションはグレー表示されます。

7. [Save] をクリックします。

ZTP 用にルータを準備する

Cisco SD-WAN は、ゼロタッチプロビジョニング (ZTP) と呼ばれるサービスとしての自動プロビジョニングソフトウェア (SaaS) を提供し、ハードウェア vEdge ルータがオーバーレイネットワークに自動的に参加できるようにしています。ZTP プロセスは、ハードウェア vEdge ルータの電源を初めてオンにしたときに開始されます。

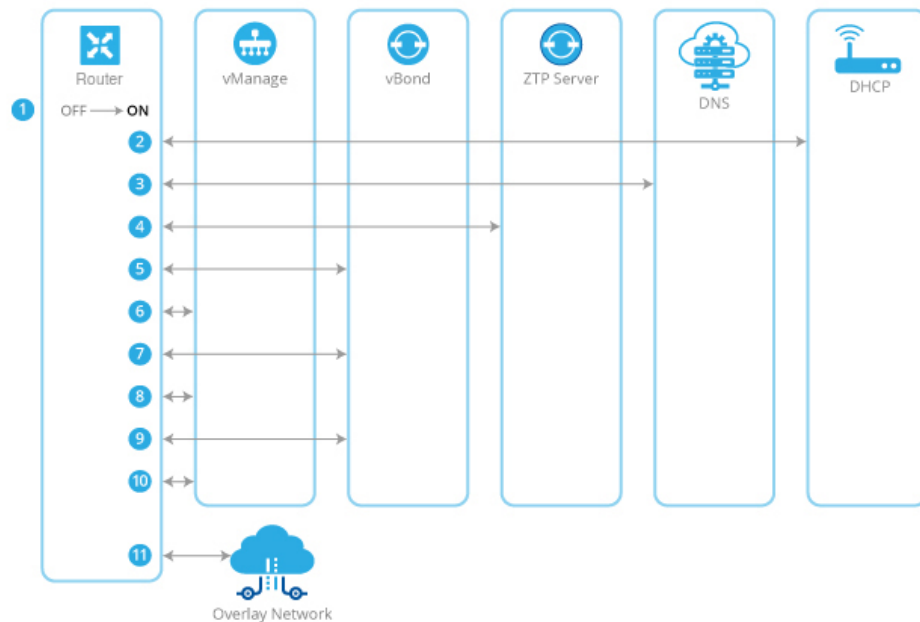
ZTP プロセスが機能するには:

ZTP 用にルータを準備する

- ハードウェア vEdge ルータが配置されているサイトのエッジルータまたはゲートウェイルータがパブリック DNS サーバーに到達できる必要があります。Google パブリック DNS サーバーに到達するようにルータを設定することをお勧めします。
- Cisco vEdge デバイス の場合、サイトのエッジルータまたはゲートウェイルータが `ztp.viptela.com` に到達できる必要があります。
- Cisco IOS XE SD-WAN デバイス の場合、サイトのエッジルータまたはゲートウェイルータが `ztp.local-domain` に到達できる必要があります。
- ハードウェアルータが ZTP に使用するインターフェイスにネットワークケーブルを接続する必要があります。これらのインターフェイスは次のとおりです。
 - Cisco vEdge 1000 ルータの場合 : `ge0/0`
 - Cisco vEdge 2000 ルータの場合 : `ge2/0`
 - Cisco vEdge 100 シリーズ ルータの場合 : `ge0/4`
 - Cisco IOS XE SD-WAN デバイス の場合、ZTP サーバーへの接続に使用される特定のインターフェイスはありません。ルータは一度に1つのインターフェイスで DHCP IP アドレスを取得しようとします。ルータは、DHCP IP アドレスを取得する最初のインターフェイスを使用して、ドメイン名 `ztp.local-domain` を ZTP サーバーの IP アドレスに解決します。

ZTP プロセスは、次の順序で発生します。

図 18: ZTP プロセスのシーケンスフロー



1. ハードウェアルータの電源を入れます。

520628

2. ルータは DHCP サーバーへの接続を試み、DHCP ディスカバリメッセージを送信します。
 1. DHCP サーバーがネットワークに存在する場合、ルータは、その ZTP インターフェイスの IP アドレスを含む DHCP オファーメッセージを受信します。その後、ZTP プロセスは手順 3 に進みます。
 2. Cisco vEdge デバイス、および Cisco IOS XE リリース 17.7.1a の Cisco IOS XE SD-WAN デバイスでは、DHCP サーバーが存在しない場合、ルータは DHCP オファーを受け取りません。この場合、ルータは自動 IP アドレス検出プロセス（自動 IP とも呼ばれます）を開始します。このプロセスは、サブネットワーク上の ARP パケットを調べ、これらのパケットから ZTP インターフェイスの IP アドレスを推測します。その後、ZTP プロセスは手順 3 に進みます。

Cisco IOS XE リリース 17.7.1a 以前の Cisco IOS XE SD-WAN デバイスでは、DHCP サーバーが存在しない場合、ZTP プロセスは続行されません。
3. ルータは DNS サーバーに接続してホスト名 `ztp.viptela.com`（Cisco vEdge デバイス）または `ztp.local-domain`（Cisco IOS XE SD-WAN デバイス）を解決し、Cisco SD-WAN ZTP サーバーの IP アドレスを受信します。
4. ルータは ZTP サーバーに接続します。ZTP サーバーは vEdge ルータを確認し、Cisco vBond オーケストレーションの IP アドレスを送信します。この Cisco vBond オーケストレーションの組織名は、vEdge ルータと同じです。
5. ルータは Cisco vBond オーケストレーションへの一時的な接続を確立し、シャーシ ID とシリアル番号を送信します（ZTP プロセスのこの時点では、ルータにはシステム IP アドレスがないため、ヌルのシステム IP アドレスを使用して接続が確立されます）。Cisco vBond オーケストレーションは、シャーシ ID とシリアル番号を使用してルータを確認します。次に、Cisco vBond オーケストレーションはルータに Cisco vManage の IP アドレスを送信します。
6. ルータは Cisco vManage への接続を確立し、vManage によってルータが検証されます。Cisco vManage はルータにシステム IP アドレスを送信します。
7. ルータは、システム IP アドレスを使用して Cisco vBond オーケストレーションへの接続を再確立します。
8. ルータは、システム IP アドレスを使用して Cisco vManage への接続を再確立します。

Cisco vEdge デバイスでは、必要に応じて、Cisco vManage が適切なソフトウェアイメージを vEdge ルータにプッシュします。ソフトウェアイメージのインストールの一環として、ルータが再起動します。
9. 再起動後、ルータは Cisco vBond オーケストレーションへの接続を再確立し、オーケストレーションはルータを再度検証します。
10. ルータは Cisco vManage への接続を確立し、vManage はすべての設定をルータにプッシュします（ルータが再起動すると、Cisco vManage への接続が再確立されます）。
11. ルータは組織のオーバーレイネットワークに参加します。



- (注) ZTP プロセスを成功させるには、Cisco vManage に vEdge ルータのデバイス設定テンプレートが含まれている必要があります。Cisco vManage インスタンスにテンプレートがない場合、ZTP プロセスは失敗します。設定プレビューとインテント設定では、`device-model` と `ztp-status` の表示は無視します。この情報は、デバイス側で設定をプッシュした後に表示されます。

非ワイヤレスルータでの ZTP の使用

非ワイヤレスハードウェア vEdge ルータの出荷時のデフォルト設定には、ZTP プロセスを自動的に実行できるようにする次のコマンドが含まれています。

- **system vbond ztp.viptela.com** : 最初の Cisco vBond オーケストレーションを Cisco SD-WAN ZTP SaaS サーバーに設定します。
- **vpn 0 interface ip dhcp-client** : VPN 0 のインターフェイスのいずれかで DHCP を有効にします (これがトランスポートインターフェイスです)。デフォルト設定の実際のインターフェイスは、ルータのモデルによって異なることに注意してください。このインターフェイスは、インターネット、MPLS、メトロイーサネット、またはその他の WAN ネットワークに接続している必要があります。

警告 : ZTP を機能させるには、vEdge ルータを WAN に接続する前に、これらの設定コマンドを変更または削除しないでください。

ワイヤレスルータでの ZTP の使用

vEdge 100m および vEdge 100wm はワイヤレスルータです。これらのルータでは、セルラーインターフェイスとイーサネットインターフェイスの両方を使用して ZTP がサポートされています。



- (注) リリース 16.3 では、vEdge 1000 ルータの LTE USB ドングルを ZTP に使用することはできません。

vEdge 100m ルータは、ソフトウェアリリース 16.1 以降をサポートします。vEdge 100m ルータがリリース 16.2.10 以降を実行している場合、ZTP を実行するときに、Cisco vManage でもリリース 16.2.10 以降を実行することをお勧めします。

vEdge 100wm ルータは、ソフトウェアリリース 16.3 以降をサポートします。

ワイヤレスハードウェア vEdge ルータの出荷時のデフォルト設定には、セルラーインターフェイスで ZTP プロセスを自動的に実行できるようにする次のコマンドが含まれています。

- **system vbond ztp.viptela.com** : 最初の Cisco vBond オーケストレーションを Cisco SD-WAN ZTP SaaS サーバーに設定します。

- **vpn 0 interface cellular0 ip dhcp-client** : VPN 0 の **cellular0** と呼ばれるセルラーインターフェイスのいずれかで DHCP を有効にします（これがトランスポートインターフェイスです）。このインターフェイスはセルラーネットワークに接続している必要があります。
- **vpn 0 interface cellular0 technology** : 無線アクセステクノロジー（RAT）をセルラーインターフェイスに関連付けます。デフォルト設定では、RAT は **lte** に設定されています。ZTP を機能させるには、この値を **auto** に変更する必要があります。
- **vpn 0 interface cellular0 profile 0** : 自動でのプロファイル選択を有効にします。ファームウェアに依存するモバイルキャリアの場合、自動プロファイルはファームウェアのデフォルト値を使用します。他のキャリアの場合、自動プロファイルは SIM カードのモバイル国コード/モバイルネットワークコード（MCC/MNC）の値を使用します。唯一の例外が vEdge 100m-NT であり、自動プロファイルはファームウェアのデフォルト（NTT ドコモ）の前に OCN MVNO APN を試行します。ルータが一致するエントリを見つけると、プロファイル 16 が自動作成され、ZTP 接続に使用されます。アクティブな ZTP 接続に使用されているプロファイルを確認するには、**show cellular sessions** コマンド出力でアクティブなプロファイルのエントリを調べます。

profile 0 設定コマンドは、[vEdge SKU 情報テーブル](#)にリストされている MCC と MCN を認識します。MCC/MNC がサポートされている場合は、セルラープロファイル機能テンプレートまたは **profile** コマンドでそれらを設定する必要はありません。MCC/MNC がサポートされていない場合は、セルラープロファイル設定テンプレートまたは **profile CLI** コマンドを使用して、手動で設定する必要があります。

Cisco vManage 設定テンプレートを使用して、ZTP を自動的に実行できるようにするデフォルト設定の一部を作成する必要がある場合は、VPN-Interface-Cellular 機能テンプレートを使用します。このテンプレートでは、**[Profile ID]** フィールドが 0 に設定され、トンネルインターフェイスが有効になっています。リリース 16.3.1 以降、**[Technology]** フィールドが追加されており、デフォルト値は「lte」です。vEdge ルータの ZTP cellular0 設定に一致させるため、値を「auto」に変更します。

[Advanced] をクリックして、デフォルトのセルラー MTU 設定が 1428 バイトであることを確認します。

次のガイドラインは、ワイヤレスルータから ZTP を使用するときが発生する可能性のある問題のトラブルシューティングにお役立てください。

- ZTP が正しく機能するためには、正しい SIM および正しいモデムモデル（SKU）を使用していることを確認してください。
- デフォルトのプロファイル APN が正しく設定されていない場合、ZTP プロセスは正しく機能しません。ZTP が機能しない場合は、**showcellular status** コマンドを発行してエラーを表示します。エラーが発生した場合は、適切な APN を設定し、ZTP プロセスを再試行します。
- 汎用（MC7304）や北米（MC7354）SKU など、既定のプロファイル APN 設定がない SKU で、自動プロファイル選択で SIM カードの APN が検出されない場合は、APN を含むプロファイルを設定します。ルータに Cisco vManage にアクセス可能な 2 番目の回線がある場合は、APN を含むプロファイル情報を機能設定テンプレートに追加してから、デバイステ

ンプレートをセルラールータにプッシュします。それ以外の場合は、セルラールータで APN を含むプロファイルを CLI から設定します。

- ルータが SIM カードを検出できないかどうかを確認するには、**showcellular status** コマンドを発行します。SIM 読み取りエラーがないか確認します。この問題を解決するには、SIM カードをルータに正しく挿入します。
- リリース 16.3.0 では、セルラールータで ZTP を実行した後、セルラーインターフェイスが **no shutdown** 状態になりません。このため、Cisco vManage はデバイス設定テンプレートをルータにプッシュできません。この問題を修正するには、ルータの CLI から、セルラーインターフェイスの状態が **shutdown** 状態になるように設定します。

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。