改訂：2024 年 8 月 22 日

SD ルーティング：Cisco SD-WAN Manager へのルーティングデバイスのオンボーディング

概要

このドキュメントでは、シスコのルーティングデバイスをエンタープライズ SD-WAN インフラストラクチャに導入するためのガイダンスを提供します。これらの物理または仮想ルーティングデバイス（別名：自律デバイス）は、利用可能な方法（自動、ブートストラップ、手動）のいずれかを使用してオンボーディングできます。このドキュメントでは、プレインストールされたデフォルトの証明書やエンタープライズルート CA 証明書を使用したデバイス展開の具体的なユースエースを紹介するとともに、利用可能な各オンボーディングオプションの設定手順に焦点を当てています。

前提条件

Cisco SD-WAN Manager への自律ルーティングデバイスのオンボーディングを開始する前に、次のことを理解しておくことをお勧めします。

表 *1*：一般的な前提条件

条件の内容	理由
SD-WAN アーキテクチャについて	主要なコンポーネントと、それらのコンポーネント間の情報の流れを理解します。SD-WAN アーキテクチャの詳細については、https://www.cisco.com/c/en/us/support/routers/sd-wan/series.html の『*Cisco Catalyst SD-WAN Getting Started Guide*』[英語] を参照してください。

条件の内容	理由
エンタープライズネットワークと証明書の役割について	証明書を使用してデバイスアイデンティティを検証する方法について理解します。 制御コンポーネントの証明書の署名およびインストールプロセスを実行するには、さまざまな方法があります。 • （推奨）：ネットワークで Cisco Public Key Infrastructure（PKI）を使用している場合は、証明書をアップロードする必要はありません。PKI の理解については、https://www.cisco.com/c/en/us/tech/security-vpn/public-key-infrastructure-pki/index.html および https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book/sec-pki-overview.html のガイド [英語] を参照してください。 • エンタープライズネットワークの場合は、ルート CA をアップロードします。 詳細については、https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-controller-cert-deploy-guide.html [英語] を参照してください。
すべてのオンボーディングオプションの前提条件	http://software.cisco.com の Cisco Plug and Play（PnP）Connect サーバーに、ルーティングデバイスを追加し、vBond コントローラプロファイルに関連付けておく必要があります。このアクションにより、そのデバイスが SD-WAN Validator のデバイス許可リストに確実に含まれるようになります。許可リストのプロビジョニングファイルは、PnP ポータルからダウンロードして SD-WAN Manager にアップロードしたり、スマートアカウント同期オプションを使用して SD-WAN Manager と同期したりできます。SD-WAN Manager は、後でこの許可リストを Validator に配布します。 仮想環境に展開されたソフトウェア ルーティング デバイスには、シャーシ番号やシリアル番号がありません。このようなデバイスの場合、ソフトウェアデバイスが PnP ポータルに追加されると、PnP サーバーは一意のシリアル番号を生成します。 デバイスの追加方法の詳細については、Plug and Play Connect ポータルへのルーティングデバイスの追加 （6 ページ）を参照してください。

条件の内容	理由
特定の導入シナリオについて	要件に最適なオンボーディング方法を決定するのに役立ちます。新しいデバイスか既存のデバイスかによって異なります。優先オンボーディングオプション （5 ページ）を参照してください。

表 *2*: デバイス固有の前提条件

最小リリースバージョン	ルーティングデバイス：Cisco IOS XE 17.12.1a です。デバイスを起動するにはインストールモードにする必要があります。 Cisco SD-WAN - 20.12.1
ルーティングデバイスの設定	• Cisco SD-WAN Manager からの管理に必要な DMI を有効にするために、netconf-yang モデルを有効にする必要があります。 • オンボーディングする前に、デバイスが自律モードで動作している必要があります • デバイスは、WAN インターフェイスを介して Cisco SD-WAN Manager および Cisco SD-WAN Validator に到達するように設定する必要があります。インターフェイスは、スタティック IP アドレスを使用して設定するか、DHCP を介して設定する必要があります。また、**no shut** 状態である必要があります。
ルーティングデバイスの詳細	オンボーディング時に必要です。工場出荷時のルーティングデバイスは、FQDN の devicehelper.cisco.com を解決し、シスコのクラウドホスト型 PnP Connect サーバーに到達して、vBond コントローラ情報、組織名、およびエンタープライズルート CA 証明書を取得できる必要があります（エンタープライズルート CA 証明書を使用する場合）。 • サイト ID • 組織名 • Cisco SD-WAN Validator 情報（Cisco SD-WAN Validator サーバーの IP アドレスまたは FQDN ） • Cisco SD-WAN Manager に接続するためのインターフェイス（物理、サブインターフェイス、ループバック） • システム IP

サポートされる WAN エッジデバイス

サポートされている WAN エッジプラットフォームとオンボーディングオプションを次の表に示します。

表 *3 :* サポートされている *WAN* エッジプラットフォームとオンボーディングオプション

プラットフォーム	自動	ブートストラップ	手動
Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ			
ASR1001-HX	対応	対応	対応
ASR1002-HX	対応	対応	対応
Cisco 4400 シリーズ サービス統合型ルータ			
Cisco 4431 ISR	対応	対応	対応
Cisco 4451 ISR	対応	対応	対応
Cisco 4461 ISR	対応	対応	対応
Cisco 4300 シリーズ サービス統合型ルータ			
Cisco 4321 ISR	対応	対応	対応
Cisco 4331 ISR	対応	対応	対応
Cisco 4351 ISR	対応	対応	対応
Cisco 4200 シリーズ サービス統合型ルータ			
Cisco 4221 ISR	対応	対応	対応
Cisco 100 シリーズ サービス統合型ルータ			
Cisco 1000 ISR	対応	対応	対応
Cisco Catalyst 8000V シリーズ エッジ プラットフォーム			
Cisco Catalyst 8000V	非対応 （注） 自動オンボーディングは、ハードウェアデバイスのみが対象です。	対応	対応
Cisco Catalyst 8200 シリーズ エッジ プラットフォーム			
C8200-1N-4T	対応	対応	対応

プラットフォーム	自動	ブートストラップ	手動
C8200L-1N-4T	対応	対応	対応
Cisco Catalyst 8300 シリーズ エッジ プラットフォーム			
C8300-1N1S-4T2X|6T	対応	対応	対応
C8300-2N2S-4T2X|6T	対応	対応	対応
Cisco Catalyst 8500 シリーズ エッジプラットフォーム			
C8500-12X4QC	対応	対応	対応
C8500-12X	対応	対応	対応
C8500L-8S4X	対応	対応	対応
C8500-20X6C	対応	対応	対応

優先オンボーディングオプション

展開シナリオやデバイスのタイプに応じて、デバイスのオンボーディングに最適な方法を選択できます。

表 *4*:優先オンボーディング方法

デバイスタイプ	優先オンボーディングオプション
新規デバイス	
ハードウェア（物理）デバイス	PnP および Quick Connect を使用
	Cisco Catalyst SD-WAN Manager で汎用ブートストラップを使用
ソフトウェア（仮想）デバイス	Cisco Catalyst SD-WAN Manager でデバイス固有のブートストラップを使用
既存デバイス	
ハードウェアデバイス	手動オンボーディング
	ブートストラップ オンボーディング
	ワンタッチプロビジョニング
ソフトウェア（仮想）デバイス	
	手動オンボーディング
	シャーシ番号とトークン CLI オンボーディング

制限事項

- Cisco SD-WAN Manager への Cisco SD ルーティングデバイスのオンボーディングは、universalk9 イメージでのみサポートされます。ペイロード暗号化機能のない（NPE）イメージはサポートされていません。
- Cisco SD ルーティングデバイスは、コントローラに到達可能なインターフェイスから Cisco SD-WAN Manager への制御接続を 1 つだけ確立できます。
- Cicso SD ルーティングデバイスでは、Cisco SD-WAN コントローラとのアクティブな接続が確立されません。
- Cisco SD-WAN Manager への接続では、専用の管理インターフェイスはサポートされていません。

自動化されたワークフローを使用した新しいハードウェア（物理）ルーティングデバイスのオンボーディング

自動化されたプラグアンドプレイ（PnP）プロセスは、SD-WAN ネットワークに参加するためのルーティングデバイスの検出、インストール、およびプロビジョニングを行うための簡単で安全な手順を提供します。このオンボーディング方法は、新規導入の対象となる新しいハードウェアデバイスで使用できます。

自動化されたワークフローを使用して自律ルーティングデバイスをオンボードするには、次の手順を実行します。

タスク	説明
ルーティングデバイス情報を使用したプラグアンドプレイ（PnP）Connect ポータルの設定	PnP ポータルには、Cisco Commerce Workplace（CCW）からデバイスを注文するときに、スマートアカウントとバーチャルアカウントから収集されたデバイス情報が入力されます。CCW 以外の新しいデバイスをオンボードする場合は、最初にそれらを PnP ポータルに追加する必要があります。
Quick Connect ワークフローを使用した Cisco SD-WAN Manager への自律ルーティングデバイスの追加	Cisco PnP ポータルから SD-WAN Manager にデバイス情報を自動同期します。
SD ルーティングデバイスのオンボーディングの完了	ルーティングデバイスは、SD-WAN Manager および SD-WAN Validator とのセキュアな接続を開始して確立し、SD-WAN ネットワークに参加します。
SD ルーティングデバイスのオンボーディングステータスの確認	制御接続を確認します。

Plug and Play Connect ポータルへのルーティングデバイスの追加

Plug and Play Connect（PnP）ポータルへのアクセス権、およびアクティブなスマートアカウントと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、スマートアカウントまたはアカウントの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。

Cisco PnP ポータルには、特定のコントローラに関連付けられているデバイスのリストが含まれています。

PnP Connect ポータルにデバイスを追加するには、次の手順を実行します。

ステップ 1 software.cisco.com に移動し、[Network Plug and Play] > [Manage Devices] の順に選択し、 **Plug and Play Connect ポータル**にログインします。

ステップ 2 [Controller Profiles] タブで [Add Profile] をクリックして、コントローラタイプが VBond のプロファイルを作成します。

ステップ 3 [Add Controller Profile] ウィンドウで、必要なプロファイル設定を入力します。

ステップ 4 オーバーレイネットワークがエンタープライズネットワークの場合は、ルート CA をアップロードし、[Next] をクリックします。

（注） オーバーレイネットワークが **Cisco PKI** の場合、証明書をアップロードする必要はありません。

ステップ 5 デバイスを PnP 接続に追加します。[Identify Device] ウィンドウで、次の情報を入力します。

- シリアル番号
- ベース PID
- （任意）証明書シリアル番号

ステップ 6 次に、デバイスを追加する方法を選択します。次のオプションのいずれかを選択します。
task_pdf_choices

- [Import using a CSV file]（任意）：オンボードするデバイスが複数ある場合に実行します。
- [Enter Device info manually]（任意だが推奨）：これを行うには、Cisco PnP SA/VA の SD ルーティングデバイス固有の情報が必要です。これは、SD ルーティングデバイスで次の CLI コマンドを入力することで取得できます。

  Router# show crypto pki certificate CISCO_IDEVID_SUDI

- PnP Connect で **show pnp udi** コマンドまたは **show pnp version** コマンドを実行して取得したシリアル番号を使用してデバイスを追加します。

ステップ 7 以前に作成したコントローラプロファイルを選択して、デバイスをバリデータ（Cisco Catalyst SD-WAN Validator）コントローラプロファイルに関連付けます。

ステップ 8 デバイスを SD ルーティングモードで動作させるには、[Device Mode] で [AUTONOMOUS] を選択します。

article_task_postreq

Quick Connect ワークフローを使用して、Catalyst SD-WAN Manager にルーティングデバイスを追加/インポート/同期します。

Quick Connect ワークフローを使用した Cisco SD-WAN Manager でのデバイスの追加

Quick Connect ワークフローを使用してルーティングデバイス情報を Cisco SD-WAN Manager と同期するには、次の手順を実行します。

始める前に

SD ルーティングデバイスが PnP ポータルに追加されている必要があります。

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

ステップ 2 [Sync Smart Account] オプションを使用して、ルーティングデバイスを Cisco SD-WAN Manager に追加します。


（注）

Cisco Catalyst SD-WAN Manager にスマートアカウントのログイン情報が保存されていることを確認します。**[Administration]** > **[Settings]** > **[Smart Account Credentials]**に移動し、詳細を入力します。ログイン情報を保存した後にのみ、スマートアカウントの同期が可能です。

デバイスが [Edge Devices] の下に表示されます。

ステップ 3 オンボードするデバイスを選択し、[Next] をクリックします。

ステップ 4 [Add and Review Device Configuration] ダイアログボックスで、サイト ID、システム IP（必須）、ホスト名を入力し、[Apply] をクリックします。

ステップ 5 （任意）タグを追加して、[Next] をクリックします。

ステップ 6 デバイスの詳細を確認して [Onboard] をクリックします。
PnP Connect に追加されたデバイスは、Cisco SD-WAN Manager と同期されてから、Validator に送信され、デバイスの許可リストに追加されます。

ステップ 7 追加されたデバイスを確認するには、**[Configuration]** > **[Devices]** > **[WAN Edge List]**に移動します。
ネットワーク内の SD ルーティングデバイスのリストに各ルータに関する詳細情報が表示され、ステータスが [Unreachable] と示されます。

---

article_task_postreq

次に行う作業：

デバイスを起動し、接続を確認します。

SD ルーティングデバイスの起動

SD ルーティングデバイスを起動するには、次の手順を実行します。

ステップ 1 Day-0 状態でデバイスを起動します。デバイスが Day-0 状態でない場合は、**reload** オプションとともに **controller-mode reset** または **writer erase** コマンドを使用して、Day-0 状態にします。

ステップ 2 SD ルーティングデバイスの WAN インターフェイスを DHCP 対応 WAN リンクに接続し、電源をオンにします。デバイスが Gigabit Etherner0 インターフェイス以外のいずれかのインターフェイスで DHCP を介して IP アドレスを取得していることを確認します。また、デバイスが devicehelper.cisco.com および Cisco SD-WAN Validator に到達可能であることを確認します。

（注） Cisco SD-WAN Manager への接続では、専用の管理インターフェイスはサポートされていません。

デバイス制御接続が Cisco SD-WAN Manager で稼働します。

ステップ 3 ルーティングデバイスの制御接続ステータスを確認します。**show sd-routing system status**、**show sd-routing local-properties summary**、および **show sd-routing connections summary** コマンドを入力します。

例：

```
Router#show sd-routing connections summary

PEER                                          PEER
PEER     PEER  PEER             SITE        PEER                                  PRIV
PEER                                    PUB
TYPE     PROT  SYSTEM IP        ID          PRIVATE IP                            PORT   PUBLIC
 IP                                PORT   STATE   UPTIME
------------------------------------------------------------------------------------------------
Cisco SD-WAN Manager  dtls  172.16.255.22    200         10.0.12.22
12446  10.0.12.22                               12446  up      12:05:29:3
```

ステップ 4 Catalyst SD-WAN Manager で**[Configuration]** > **[Devices]**に移動して、デバイスのステータスが [In Sync] および [Reachable] と表示されていることを確認します。

汎用ブートストラップを使用した新しいハードウェア（物理）ルーティングデバイスのオンボーディング

ブートストラップファイルのオンボーディングオプションでは、Quick Connect ワークフローを使用して PnP ポータルから Catalyst SD-WAN Manager に新しいハードウェアルーティング（物理）デバイス情報を追加し、汎用ブートストラップファイルを使用してデバイスをオンボーディングします。新しいデバイスを使用した新規展開で、情報を提供する DHCP サーバーがない場合は、この方法を使用します。このような場合、SD-WAN Manager を使用してブートストラップファイルを生成し、生成したブートストラップファイルを使用して SD-WAN フレームワークへの SD ルーティングデバイスとしてオンボードできます。

デバイスが PnP ポータルに追加されていることを確認します。Cisco PnP ポータルには、特定のコントローラに関連付けられているデバイスのリストが含まれています。PnP ポータルにデバイスを追加する方法については、Plug and Play Connect ポータルへのルーティングデバイスの追加 （6 ページ）を参照してください。

ブートストラップオプションを使用して新しいハードウェアデバイスをオンボードするには、次の手順を実行します。

ステップ 1 デバイスインベントリを同期します。SD-WAN Manager で [Workflows] > [Quick Connect] に移動し、[Get Started] をクリックします。次のいずれかのオプションを使用して、デバイスを追加します。
task_pdf_choices

- **スマートアカウントにログイン**：（推奨）ログイン情報を入力して、デバイスを SD-WAN Manager に追加します。デバイス情報は PnP Connect ポータルから同期され、**[Configuration]** > **[Devices]**ページの下に一覧表示されます。

  または

- **シリアル番号を含むファイルのアップロード**：デバイス情報を含む .csv ファイルをアップロードします。この情報を収集するには、ルーティングデバイスで CLI コマンドを入力します。

  ```
  Device# show crypto pki certificate CISCO_IDEVID_SUDI
  ```

  csv ファイルの例を以下に示します。

シャーシ番号	製品 ID	証明書のシリアル番号	SUDI シリアル	mode
ISR4461/K9-FDU1231M56W	ISR4461/K9	0215ZS7X	FDU1231M56W	自律

  デバイスが [Edge Devices] の下に表示されます。

  1. オンボードするデバイスを選択し、[Next] をクリックします。
  2. [Add and Review Device Configuration] ダイアログボックスで、サイト ID、システム IP（必須）、ホスト名を入力し、[Apply] をクリックします。
  3. デバイスの詳細を確認して [Onboard] をクリックします。追加されたデバイスを確認するには、**[Configuration]** > **[Devices]** > **[WAN Edge List]**に移動します。ネットワーク内のルータのリストに各ルータに関する詳細情報が表示され、ステータスが [Unreachable] と示されます。

ステップ 2 Cisco SD-WAN Manager のメニューから **[Configuration]** > **[Devices]**に移動し、ブートストラップを生成するデバイスを選択します。

ステップ 3 [Export Bootstrap Configuration] ダイアログボックスをクリックし、**WAN インターフェイス名**を入力し、[SD-Routing] のチェックボックスをオン にしてブートストラップファイルを生成します。ブートストラップファイルには、組織名、Cisco SD-WAN Validator の IP、およびルート CA 証明書が含まれます。エンタープライズ ネットワークの場合は、エンタープライズルート CA 証明書が含まれます。

（注） 管理インターフェイス名は、Cisco IOS XE デバイスのモデルによって異なる場合があります。オンボードするモデルに基づいて、Cisco SD-WAN Validator および Cisco SD-WAN Manager に到達できるインターフェイス名を指定します。ルーティングデバイスのインターフェイスを確認し、両方に接続されていることを確認します。

ステップ 4 ハードウェアデバイスに適用可能な *.cfg* 形式の汎用ブートストラップをダウンロードします。ファイルを解凍し、ファイル名を **ciscosdwan.cfg** に変更します。

ステップ 5 ブートストラップファイルを **ciscosdwan.cfg** というファイル名でデバイスの内部ブートフラッシュにコピーします。

ダウンロードされたブートストラップファイルはユーザーデータフィールドとして追加され、SD ルーティングモードでデバイスを起動し、Cisco Catalyst SD-WAN Validator および Cisco SD-WAN Manager との接続を確立します。

ステップ 6 デバイスを Day-0 状態にするには、**controller-mode reset** または **writer erase with reload** コマンドを使用してデバイスをリロードします。

ステップ 7 デバイスで次のコマンドを使用して、制御接続を確認します。

例：

```
Router# show sd-routing connections summary

Router# show sd-routing system status

Router# show sd-routing local-properties summary
```

ステップ 8 Catalyst SD-WAN Manager で**[Configuration]** > **[Devices]**に移動して、デバイスのステータスが [In Sync] および [Reachable] と表示されていることを確認します。

デバイス固有のブートストラップを使用した新しいソフトウェア（仮想）ルーティングデバイスのオンボーディング

ブートストラップファイルのオンボーディングオプションでは、Quick Connect ワークフローを使用して PnP ポータルから Catalyst SD-WAN Manager に新しいソフトウェアルーティング（仮想）デバイス情報を追加し、デバイス固有のブートストラップファイルを使用してデバイスをオンボーディングします。新しいデバイスを使用した新規展開で、情報を提供する DHCP サーバーがない場合は、この方法を使用します。このような場合、SD-WAN Manager を使用してブートストラップファイルを生成し、生成したブートストラップファイルを使用して SD-WAN フレームワークへの SD ルーティングデバイスとしてオンボードできます。

デバイスが PnP ポータルに追加されていることを確認します。Cisco PnP ポータルには、特定のコントローラに関連付けられているデバイスのリストが含まれています。PnP ポータルにデバイスを追加する方法については、Plug and Play Connect ポータルへのルーティングデバイスの追加 （6 ページ）を参照してください。

- オーバーレイネットワークを確認します。特記事項：
  - オーバーレイが CiscoPKI、Symantec/Digicert の場合は、ルート CA 証明書を追加してインストールする必要はありません。
  - オーバーレイがエンタープライズの場合、 コマンドを使用して、対応するルート CA と署名付き証明書をインストールします。

    ```
    Router# request platform software sd-routing root-cert-chain install bootflash:cacert.pem
    ```

    証明書署名要求（CSR）を生成して署名する必要はありません。トークンを使用してデバイスをアクティブ化すると、CSR が生成されます。

ブートストラップオプションを使用して新しい SD ルーティング ソフトウェア デバイスをオンボードするには、次の手順を実行します。

ステップ 1 デバイスインベントリを同期します。SD-WAN Manager で [Workflows] > [Quick Connect] に移動し、[Get Started] をクリックします。次のいずれかのオプションを使用して、デバイスを追加します。
task_pdf_choices

- **スマートアカウントにログイン**：（推奨）ログイン情報を入力して、デバイスを SD-WAN Manager に追加します。デバイス情報は PnP Connect ポータルから同期され、**[Configuration]** > **[Devices]**ページの下に一覧表示されます。

  または

- **シリアル番号を含むファイルのアップロード**：PnP Connectからダウンロードしたデバイス情報を含む serial.viptela ファイルをアップロードします（[Controller Profiles] にあり、PnP Connect ポータルの [Download the Provisioning file] をクリックします）。デバイスが [Edge Devices] の下に表示されます。。

  1. オンボードするデバイスを選択し、[Next] をクリックします。
  2. [Add and Review Device Configuration] ダイアログボックスで、サイト ID、システム IP（必須）、ホスト名を入力し、[Apply] をクリックします。
  3. デバイスの詳細を確認して [Onboard] をクリックします。追加されたデバイスを確認するには、**[Configuration]** > **[Devices]** > **[WAN Edge List]**に移動します。ネットワーク内のルータのリストに各ルータに関する詳細情報が表示され、ステータスが [Unreachable] と示されます。

ステップ 2 エンタープライズ証明書を使用している場合は、**[Administration]** > **[Settings]** > **[Trust and Privacy]** > **[Controller Certificate Authorization]**に移動し、[Enterprise Root Certificate] を選択して、エンタープライズルート証明書を貼り付けます。これにより、ブートストラップファイルにエンタープライズルート証明書を確実に追加できます。

ステップ 3 **[Configuration]** > **[Devices]**に移動し、ブートストラップを生成するデバイスを選択します。

ステップ 4 ウィンドウの右側のペインで [...] をクリックし、[Generate Bootstrap Configuration] を選択してから、VPN0 インターフェイス名として **GigabitEthernet1** と入力します。エンタープライズ証明書が使用されている場合は、指定されたフィールドに情報を入力します。

（注） 選択したインターフェイスで DHCP が有効になっており、Cisco Catalyst SD-WAN Validator と Cisco SD-WAN Manager に到達可能であることを確認します。

ステップ 5 [OK] をクリックして、デバイスにイメージをダウンロードします。次に、証明書を使用する場合と使用しない場合のサンプルファイルタイプの例を示します。

例：

```
ciscosdwan_cloud_init.cfg
```

```
ciscosdwan_cloud_init_with_ent_cert.cfg
```

ステップ 6 ブートストラップファイルを **ciscosdwan.cfg** というファイル名でデバイスの内部ブートフラッシュにコピーします。
ダウンロードされたブートストラップファイルはユーザーデータフィールドとして追加され、SDルーティングモードでデバイスを起動し、Cisco Catalyst SD-WAN Validator および Cisco SD-WAN Manager との接続を確立します。

ステップ 7 デバイスを Day-0 状態にするには、**controller-mode reset** または **writer erase with reload** コマンドを使用してデバイスをリロードします。

ステップ 8 デバイスで次のコマンドを使用して、制御接続を確認します。

例：

```
Router# show sd-routing connections summary

Router# show sd-routing system status

Router# show sd-routing local-properties summary
```

ステップ 9 Catalyst SD-WAN Manager で**[Configuration]** > **[Devices]**に移動して、デバイスのステータスが [In Sync] および [Reachable] と表示されていることを確認します。

既存のハードウェア（物理）ルーティングデバイスの手動オンボーディング

このオンボーディングオプションでは、Quick Connect ワークフローを使用して PnP ポータルから Catalyst SD-WAN Manager にハードウェア ルーティング デバイス情報を手動で追加し、ルーティングデバイスで追加の設定を行いオンボーディングします。この方法を使用するのは、デバイスが分離されている場合、Cisco SD-WAN Manager インスタンスが Cisco PnP ポータルに接続できない場合、または Cisco SD-WAN Manager とスマートアカウントを同期するために必要な自動同期オプションを使用しない場合です。PnP ディスカバリを停止し、デバイスにスタートアップ コンフィギュレーション（または任意の設定）があり、Day-0 状態ではないことを確認する必要があります。

- デバイスが PnP ポータルに追加されていることを確認します。Cisco PnP ポータルには、特定のコントローラに関連付けられているデバイスのリストが含まれています。PnP ポータルにデバイスを追加する方法については、Plug and Play Connect ポータルへのルーティングデバイスの追加 （6 ページ）を参照してください。
- オーバーレイネットワークを確認します。特記事項：
  - オーバーレイが Ciscopki、Symantec/Digicert の場合は、ルート CA 証明書を追加してインストールする必要はありません。
  - オーバーレイがエンタープライズネットワークの場合、 コマンドを使用して、対応するルート CA と署名付き証明書をインストールします。

    Router# request platform software sd-routing root-cert-chain install bootflash:cacert.pem

ハードウェア ルーティング デバイスを手動でオンボードするには、次の手順を実行します。

ステップ 1 デバイスインベントリを同期します。SD-WAN Manager で [Workflows] > [Quick Connect] に移動し、[Get Started] をクリックします。次のいずれかのオプションを使用して、デバイスを追加します。
task_pdf_choices

- **スマートアカウントにログイン**：（推奨）ログイン情報を入力して、デバイスを SD-WAN Manager に追加します。デバイス情報は PnP Connect ポータルから同期され、**[Configuration]** > **[Devices]**ページの下に一覧表示されます。

  または

- **シリアル番号を含むファイルのアップロード**：デバイス情報を含む .csv ファイルをアップロードします。この情報を収集するには、ルーティングデバイスで CLI コマンドを入力します。

```
Device# show crypto pki certificate CISCO_IDEVID_SUDI
```

csv ファイルの例を以下に示します。

シャーシ番号	製品 ID	証明書のシリアル番号	SUDI シリアル	mode
ISR4461/K9-FDU1231M56W	ISR4461/K9	0215ZS7X	FDU1231M56W	自律

デバイスが [Edge Devices] の下に表示されます。

1. オンボードするデバイスを選択し、[Next] をクリックします。
2. [Add and Review Device Configuration] ダイアログボックスで、サイト ID、システム IP（必須）、ホスト名を入力し、[Apply] をクリックします。
3. デバイスの詳細を確認して [Onboard] をクリックします。追加されたデバイスを確認するには、**[Configuration]** > **[Devices]** > **[WAN Edge List]**に移動します。ネットワーク内のルータのリストに各ルータに関する詳細情報が表示され、ステータスが [Unreachable] と示されます。

ステップ 2 Cisco SD-WAN Manager との制御接続を有効にするための最小限のパラメータをルーティングデバイスで設定します。

例：

```
router(config)# netconf-yang

sd-routing
  no ipv6-strict-control
  organization-name "%Your Org. Name%"
  site-id %id%
  system-ip %system ip%
  vbond name %vbond name or vbond ip%
  vbond port 12346
  wan-interface %uplink interface%

ip route 0.0.0.0 0.0.0.0 %next hop ip%

interface %uplink interface%
   ip address  %dhcp or static%
   no shutdown
```

（注） インターフェイスが静的 IP アドレスまたは DHCP を使用して設定されていることを確認します。Cisco Catalyst SD-WAN Manager と Cisco Catalyst Validator の両方に対して IP 的に到達可能である必要があります。また、インターフェイスは **no shut** 状態である必要があります。

ルーティングデバイス、バリデータ、および Catalyst SD-WAN Manager の間で制御接続が確立されます。

ステップ 3 SD ルーティングデバイスで次のコマンドを使用して、制御接続を確認します。

例：

```
Router# show platform software yang-management process status
Router# show sd-routing connections summary

Router# show sd-routing system status

Router# show sd-routing local-properties summary
```

ステップ 4 Cisco Catalyst SD-WAN Manager で**[Configuration]** > **[Devices]**に移動して、デバイスのステータスが [In Sync] および [Reachable] と表示されていることを確認します。

article_task_postreq

実行コンフィギュレーションの確認：これを行うには、デバイスの横にある [(…)] をクリックして、メニューを起動します。

デバイスのモニタリング：これを行うには、**[Monitor]** > **[Device]**に移動します。デバイスを選択し、[(…)] をクリックしてメニューを起動し、アラーム、イベント、トラブルシューティングなどを確認します。

ブートストラップを使用した既存のハードウェア（物理）ルーティングデバイスのオンボーディング

オンサイト ブートストラップ プロセスには、ブート可能な USB ドライブまたは内部ブートフラッシュから SD ルーティングをサポートするデバイスにロードするブートストラップ構成ファイルの生成が含まれます。デバイスの電源が入ると、SD ルーティング設定が既存の設定に追加され、デバイスをリロードせずにネットワークで起動します。

PnP ディスカバリを停止する必要があります。デバイスには、スタートアップ コンフィギュレーションまたは任意のコンフィギュレーションが必要です。また、Day-0 状態であってはなりません。この方法は、Cisco PnP SA/VA にすでに追加されているルーティングデバイスでも機能します。

ブートストラップオプションを使用して既存のハードウェア（物理）デバイスをオンボードするには、次の手順を実行します。

ステップ 1 デバイスインベントリを同期します。SD-WAN Manager で [Workflows] > [Quick Connect] に移動し、[Get Started] をクリックします。次のいずれかのオプションを使用して、デバイスを追加します。
task_pdf_choices

- **スマートアカウントにログイン**：（推奨）ログイン情報を入力して、デバイスを SD-WAN Manager に追加します。デバイス情報は PnP Connect ポータルから同期され、**[Configuration]** > **[Devices]**ページの下に一覧表示されます。

  または

- **シリアル番号を含むファイルのアップロード**：デバイス情報を含む .csv ファイルをアップロードします。この情報を収集するには、ルーティングデバイスで CLI コマンドを入力します。

  ```
  Device# show crypto pki certificate CISCO_IDEVID_SUDI
  ```

  csv ファイルの例を以下に示します。

シャーシ番号	製品 ID	証明書のシリアル番号	SUDI シリアル	mode
ISR4461/K9-FDU1231M56W	ISR4461/K9	0215ZS7X	FDU1231M56W	自律

デバイスが [Edge Devices] の下に表示されます。

1. オンボードするデバイスを選択し、[Next] をクリックします。
2. [Add and Review Device Configuration] ダイアログボックスで、サイト ID、システム IP（必須）、ホスト名を入力し、[Apply] をクリックします。
3. デバイスの詳細を確認して [Onboard] をクリックします。追加されたデバイスを確認するには、**[Configuration]** > **[Devices]** > **[WAN Edge List]**に移動します。ネットワーク内のルータのリストに各ルータに関する詳細情報が表示され、ステータスが [Unreachable] と示されます。

ステップ 2 Cisco SD-WAN Manager のメニューから **[Configuration]** > **[Devices]**に移動し、ブートストラップを生成するデバイスを選択します。

ステップ 3 [Export Bootstrap Configuration] ダイアログボックスをクリックし、**WAN インターフェイス名**を入力してブートストラップファイルを生成します。ブートストラップファイルには、組織名、Cisco SD-WAN Validator の IP、およびルート CA 証明書が含まれます。エンタープライズ ネットワークの場合は、エンタープライズルート CA 証明書が含まれます。

（注） 管理インターフェイス名は、Cisco IOS XE デバイスのモデルによって異なる場合があります。オンボードするモデルに基づいて、Cisco SD-WAN Validator および Cisco SD-WAN Controller に到達できるインターフェイス名を指定します。ルーティングデバイスのインターフェイスを確認し、両方に接続されていることを確認します。

ステップ 4 ハードウェアデバイスに適用可能な *.cfg* 形式の汎用ブートストラップをダウンロードします。ファイルを解凍し、ファイル名を **ciscosdwan.cfg** に変更します。

ステップ 5 ブートストラップファイルを **ciscosdwan.cfg** というファイル名でデバイスの内部ブートフラッシュにコピーします。

ステップ 6 ルーティングデバイスで **sd-routing bootstrap load bootflash:ciscosdwan.cfg** コマンドを入力します。

例：

```
Router# sd-routing bootstrap load bootflash:ciscosdwan.cfg
Located the file. Beginning to extract the data
Extraction summary
-Organization name - "testb2"
-Interface - GigabitEthernet0/0/0
-vbond  - 99.99.1.51
Successfully extracted root-cert info

Do you want to proceed and apply extracted
parameters to enable sd-routing feature?? (yes/[no]): yes
Successfully configured bootstrap extracted parameters
Router#
*May 10 08:56:11.159: %SYS-5-CONFIG_P: Configured programmatically by process Exec from console as console
*May 10 09:05:11.751: %DMI-5-AUTH_PASSED: R0/0: dmiauthd: User 'vmanage-admin' authenticated successfully from
201.201.201.1:41902  for netconf over ssh. External groups
```

これにより、SD ルーティングモードでデバイスが起動し、Cisco Catalyst SD-WAN Validator および Cisco SD-WAN Manager との接続が確立されます。

ステップ 7 デバイスで次のコマンドを使用して、制御接続を確認します。

例：

```
Router# show sd-routing connections summary

Router# show sd-routing system status

Router# show sd-routing local-properties summary
```

ステップ 8 Catalyst SD-WAN Manager で**[Configuration]** > **[Devices]**に移動して、デバイスのステータスが [In Sync] および [Reachable] と表示されていることを確認します。また、SD ルーティングデバイスとして **[Monitor]** > **[Device]**にも表示されます。

ワンタッチプロビジョニングを使用した既存のハードウェア（物理）ルーティングデバイスのオンボーディング

このタスクでは、ワンタッチプロビジョニングを使用してルーティングデバイスを Catalyst SD-WAN Manager にオンボーディングする手順について説明します。ワンタッチプロビジョニングにより、デバイスをオンボーディングする前にルーティングデバイスを Cisco PnP SA/VA に追加し、デバイスリストを Catalyst SD-WAN Manager に同期またはアップロードする必要がなくなります。既存のデバイスが多い大規模なネットワークの場合は、この方法を使用します。デバイスのオンボーディングを開始する前に、PnP ディスカバリを停止してください。

デバイスのワンタッチプロビジョニングを実行するには、次の手順に従います。

ステップ 1 オンボーディングする SD ルーティングデバイスで、次のコマンドを入力します。

例：

```
Router(config)# netconf-yang

sd-routing
  no ipv6-strict-control
  organization-name "%Your Org. Name%"
  site-id %id%
  system-ip %system ip%
  vbond name <FQDN> or vbond ip <ipaddress>
  vbond port 12346
  wan-interface %uplink interface%

ip route 0.0.0.0 0.0.0.0 %next hop ip%

interface %uplink interface%
   ip address  %dhcp or static%
   no shutdown
```

このアクションにより、Cisco Catalyst SD-WAN Validator との通信が開始され、デバイスが **[Cisco Catalyst SD-WAN Manager]** > **[Devices]** > **[Unclaimed WAN Edges]**のリストに追加されます。

ステップ 2 Cisco Catalyst SD-WAN Manager で **[Configuration]** > **[Devices]** > **[Unclaimed WAN Edges]**ページに移動し、デバイスのシリアル番号を確認してから、[Validate the uploaded vEdge List and send to controllers] チェックボックスをオンにして SD ルーティングデバイスを要求します。

これにより、デバイスが [Unclaimed WAN Edges] カテゴリから [WAN Edges List] カテゴリに移動し、SD ルーティングデバイスが Catalyst SD-WAN Manager との制御接続を確立して、オンボーディングプロセスを完了できるようになります。

ステップ 3 SD ルーティングデバイスで次のコマンドを使用して、Cisco SD-WAN Manager への制御接続を確認します。

例：

```
Router# show sd-routing connections summary

Router# show sd-routing system status

Router# show sd-routing local-properties summary

Router# show sd-routing connection history
```

ステップ 4 Catalyst SD-WAN Manager で**[Configuration]** > **[Devices]**に移動して、デバイスのステータスが [In Sync] および [Reachable] と表示されていることを確認します。

既存のソフトウェア（仮想）ルーティングデバイスの手動オンボーディング

このオンボーディングオプションでは、Quick Connect ワークフローを使用して PnP ポータルから Catalyst SD-WAN Manager にソフトウェア（仮想）ルーティングデバイス情報を手動で追加し、ルーティングデバイスで追加の設定を行いオンボーディングします。

デバイスが PnP ポータルに追加されていることを確認します。Cisco PnP ポータルには、特定のコントローラに関連付けられているデバイスのリストが含まれています。PnP ポータルにデバイスを追加する方法については、Plug and Play Connect ポータルへのルーティングデバイスの追加 （6 ページ）を参照してください。このデバイスの PnP ディスカバリを停止する必要があります。デバイスにはスタートアップコンフィギュレーションが必要です。また、Day-0 状態であってはなりません。

既存のソフトウェア ルーティング デバイスを手動でオンボードするには、次の手順を実行します。

ステップ 1 デバイスインベントリを同期します。SD-WAN Manager で [Workflows] > [Quick Connect] に移動し、[Get Started] をクリックします。次のいずれかのオプションを使用して、デバイスを追加します。
task_pdf_choices

- **スマートアカウントにログイン**：（推奨）ログイン情報を入力して、デバイスを SD-WAN Manager に追加します。デバイス情報は PnP Connect ポータルから同期され、**[Configuration]** > **[Devices]**ページの下に一覧表示されます。

  または

- **シリアル番号を含むファイルのアップロード**：PnP Connect からダウンロードしたデバイス情報を含む serial.viptela ファイルをアップロードします（[Controller Profiles] にあり、PnP Connect ポータルの [Download the Provisioning file] をクリックします）。デバイスが [Edge Devices] の下に表示されます。

  1. オンボードするデバイスを選択し、[Next] をクリックします。

2. [Add and Review Device Configuration] ダイアログボックスで、サイト ID、システム IP（必須）、ホスト名を入力し、[Apply] をクリックします。
3. デバイスの詳細を確認して [Onboard] をクリックします。追加されたデバイスを確認するには、**[Configuration]** > **[Devices]** > **[WAN Edge List]**に移動します。ネットワーク内のルータのリストに各ルータに関する詳細情報が表示され、ステータスが [Unreachable] と示されます。

ステップ 2 Cisco SD-WAN Manager との制御接続を有効にするための最小限のパラメータをルーティングデバイスで設定します。

例：

```
Router(config)# netconf-yang

sd-routing
  no ipv6-strict-control
  organization-name "%Your Org. Name%"
  site-id %id%
  system-ip %system ip%
  vbond name %vbond name or vbond ip%
  vbond port 12346
  wan-interface %uplink interface%

ip route 0.0.0.0 0.0.0.0 %next hop ip%

interface %uplink interface%
   ip address  %dhcp or static%
   no shutdown
```

- インターフェイスが静的 IP アドレスまたは DHCP を使用して設定されていることを確認します。Cisco Catalyst SD-WAN Manager と Cisco Catalyst Validator の両方に対して IP 的に到達可能である必要があります。また、インターフェイスは **no shut** 状態である必要があります。
- Validator の IP または Validator の名前を設定します。
- システム IP、サイト ID、組織名、および WAN インターフェイスを設定します。

ステップ 3 vdaemon のステータスをチェックして、この機能が有効になっていることを確認します。

例：

```
Router# show platform software yang-management process state
Confd Status: Started


Process              Status              State
------------------------------------------------------
nesd                 Running             Active
syncfd               Running             Active
ncsshd               Running             Not Applicable
dmiauthd             Running             Active
nginx                Running             Not Applicable
ndbmand              Running             Active
pubd                 Running             Active
```

```
Router#show platform software process list r0 name vdaemon
Name: vdaemon
  Process id       : 29075
  Parent process id: 29070
```

```
Group id         : 29075
Status           : S
Session id       : 8829
User time        : 263002
Kernel time      : 347183
Priority         : 20
Virtual bytes    : 405110784
Resident pages   : 12195
Resident limit   : 18446744073709551615
Minor page faults: 716496
Major page faults: 9130
```

ステップ 4 Cisco デバイスは、デフォルトで PKI および Symantec ルート証明書とともにロードされます。オーバーレイネットワークがエンタープライズ用の場合は、エンタープライズルート証明書をインストールする必要があります。ルート証明書を認証局（CA）から Cisco 8000v にコピーします。**scp** root-ca-chain.crt cisco@<**c8kv**>:root-ca-chain.crt および **request platform software controller-managed root-cert-chain install**<*path-to-root-cert*> コマンドを入力します。

例：

```
Router# scp root-ca-chain.crt cisco@<c8kv>:root-ca-chain.crt
```

例：

```
Router#  request platform software sd-routing root-cert-chain install bootflash:root-ca-chain.crt
```

ステップ 5 クライアントのエンタープライズルート証明書をインストールします。

a) **request platform software sd-routing csr upload bootflash: tmp_cert_dir/***C8kCsrFile*.csr コマンドを使用して、デバイスの証明書署名付き要求（CSR）を生成します。*tmp_cert_dir/*ディレクトリ内に作成されるフォルダには、任意の名前を指定できます。

b) c8k デバイスからエンタープライズ CA があるディレクトリに、生成された CSR ファイルをコピーします。ルートキーとルート CA 証明書を使用して証明書を署名し、pem/crt 形式の証明書ファイルを生成できます。

- エンタープライズ CA：scp cisco@<c8kv ip>:tmp_cert_dir/C8kCsrFile.csr
- openssl x509 -req -in C8kCsrFile.csr -CA root-ca-chain.crt -CAkey rootCA.key -CAcreateserial -out C8kCsrFile.crt -days 3650 -sha256

c) 生成された crt ファイル（署名付き）を c8000v デバイスにコピーします。エンタープライズ CA：**C8kCsrFile.crt** cisco@<**c8kv ip**>:**C8kCsrFile.crt**

d) **request platform software sd-routing certificate install bootflash:C8kCsrFile.crt** コマンドを使用して、コピーした証明書をデバイスにインストールします。

ステップ 6 証明書のインストールステータスを確認します。

例：

```
Router# show sd-routing local-properties summary
……....

certificate-status               Installed
certificate-validity             Valid
certificate-not-valid-before     Apr 25 00:55:28 2023 GMT
certificate-not-valid-after      Apr 24 00:55:28 2024 GMT
……........
dns-name                         Validator
site-id                          100
```

```
tls-port                        0
system-ip                       172.16.255.11
chassis-num/unique-id           C8K-aa079ca1-c141-4ac6-9b76-05864005f94e
serial-num                      12345707
```

ステップ 7 CLI を使用してクライアント証明書をインストールする場合、または何らかの理由で CSR の生成と証明書のインストールをやり直す必要があった場合は、Cisco SD-WAN Manager にデバイス情報を追加して、Cisco SD-WAN Manager との制御接続を開始します。手順は以下のとおりです。

a) シャーシ番号とシリアル番号を取得します。シャーシ番号とシリアル番号を取得するには、**show sd-routing local-properties** または **show sd-routing certificate serial** コマンドを使用します。

```
Router# show sd-routing local-properties summary
chassis-num/unique-id             C8K-aa079ca1-c141-4ac6-9b76-05864005f94e
serial-num                        12345707
```

b) SD-WAN Manager および SD-WAN Validator で **request vedge add chassis-num <Chassis id> org-name <Org Name> serial-num <Serial number from c8kv>** コマンドを使用して、シャーシ ID をアップロードします。

ステップ 8 SD ルーティングデバイスの制御接続ステータスを確認します。

例：

```
Router#show sd-routing connections summary

PEER                                          PEER
PEER     PEER  PEER             SITE        PEER                                  PRIV
PEER                                    PUB
TYPE     PROT  SYSTEM IP        ID          PRIVATE IP                            PORT   PUBLIC
 IP                                  PORT   STATE   UPTIME
------------------------------------------------------------------------------------------------
vmanage  dtls  172.16.255.22    200         10.0.12.22                            12446
10.0.12.22                              12446  up      12:05:29:3
```

ステップ 9 Cisco Catalyst SD-WAN Manager で**[Configuration]** > **[Devices]**に移動して、デバイスのステータスが [In Sync] および [Reachable] と表示されていることを確認します。

トークンを使用したシャーシのアクティブ化による既存のソフトウェア（仮想）ルーティングデバイスのオンボーディング

このオンボーディングオプションでは、Quick Connect ワークフロー（SyncSmart または serial.viptela ファイル）を使用して PnP ポータルから Catalyst SD-WAN Manager に仮想ルーティングデバイス情報を追加し、トークンをアクティブ化してルーティングデバイスをオンボーディングします。

（注）

この方法は、Cisco SD-WAN 仮想デバイス（Cisco c8000v）でのみ使用できます。

- Cisco Catalyst SD-WAN Manager にスマートアカウントのログイン情報が保存されていることを確認してください。Cisco Catalyst SD-WAN Manager でこれを行うには、**[Administration]** > **[Settings]** > **[Smart Account Credentials]**の順

に選択します。スマートアカウントのログイン情報は、Cisco SD-WAN Manager でスマートアカウントやバーチャルアカウントの情報を同期するために後で使用されます。

- オーバーレイネットワークを確認します。特記事項：
  - オーバーレイが Ciscopki、Symantec/Digicert の場合は、ルート CA 証明書を追加してインストールする必要はありません。
  - オーバーレイがエンタープライズの場合、 コマンドを使用して、対応するルート CA と署名付き証明書をインストールします。

    ```
    Router# request platform software sd-routing root-cert-chain install bootflash:cacert.pem
    ```

    証明書署名要求（CSR）を生成して署名する必要はありません。トークンを使用してデバイスをアクティブ化すると、CSR が生成されます。

シャーシ番号をアクティブ化してデバイスをオンボードするには、次の手順を実行します。

ステップ 1 デバイスインベントリを同期します。SD-WAN Manager で [Workflows] > [Quick Connect] に移動し、[Get Started] をクリックします。次のいずれかのオプションを使用して、デバイスを追加します。
task_pdf_choices

- **スマートアカウントにログイン**：（推奨）ログイン情報を入力して、デバイスを SD-WAN Manager に追加します。デバイス情報は PnP Connect ポータルから同期され、**[Configuration]** > **[Devices]**ページの下に一覧表示されます。

  または

- **シリアル番号を含むファイルのアップロード**：PnP Connectからダウンロードしたデバイス情報を含む serial.viptela ファイルをアップロードします（[Controller Profiles] にあり、PnP Connect ポータルの [Download the Provisioning file] をクリックします）。デバイスが [Edge Devices] の下に表示されます。

  1. オンボードするデバイスを選択し、[Next] をクリックします。
  2. [Add and Review Device Configuration] ダイアログボックスで、サイト ID、システム IP（必須）、ホスト名を入力し、[Apply] をクリックします。
  3. デバイスの詳細を確認して [Onboard] をクリックします。追加されたデバイスを確認するには、**[Configuration]** > **[Devices]** > **[WAN Edge List]**に移動します。ネットワーク内のルータのリストに各ルータに関する詳細情報が表示され、ステータスが [Unreachable] と示されます。

ステップ 2 ルーティングデバイスで、次のコマンドを実行して最小設定を適用します。

例：

```
Router(config)# netconf-yang
!
sd-routing
 no ipv6-strict-control
 organization-name "vIptela Inc Regression"
 site-id 500
 system-ip 172.16.255.15
```

```
 vbond ip 10.0.12.26
 vbond port 12346
 wan-interface GigabitEthernet2
!
ip route 0.0.0.0 0.0.0.0 10.0.5.13
!
ip interface GigabitEthernet2
 ip address 10.0.5.11 255.255.255.0
 no shutdown
!
```

ステップ 3 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Certificates]**の順に選択し、オンボードするデバイスの UUID とワンタイムパスワード（OTP）を取得します。

ステップ 4 仮想デバイスによって生成されたシャーシ番号を上書きするには、仮想ルーティングデバイスで CLI コマンドを実行します。

例：

```
request platform software sd-routing activate chassis newly uploaded chassis id from vmanage
token token generated by SD-WAN Manager
```

ステップ 5 次のコマンドを使用して、ルーティングデバイスの制御接続ステータスを確認します。

例：

```
show sd-routing local-properties summary
show sd-routing local-properties wan ipv4
show sd-routing connections summary
show sd-routing connections history
```

ステップ 6 Catalyst SD-WAN Manager で**[Configuration]** > **[Devices]**に移動して、SD ルーティングデバイスのステータスが [In Sync] および [Reachable] と表示されていることを確認します。

オンボーディングに関する問題のトラブルシューティング

ルーティングデバイスのオンボーディングに関連する一般的な問題と解決策を以下に示します。問題の解決策がここに記載されていない場合は、シスコサポートでサポートチケットを発行することを推奨します。

デバイスでの必須チェック

考えられる原因 SD ルーティング機能が有効になっていません。

解決法 デバイスの動作モードを確認します。

```
Router#show version | include mode
cisco ASR1002-HX (2KH) processor (revision 2KH) with 6756077K/6147K bytes of memory.
Processor board ID FXS2304Q345
Router operating mode: Autonomous (SD-Routing)
Crypto Hardware Module present
8 Gigabit Ethernet interfaces
8 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
16777216K bytes of physical memory.
29401087K bytes of eUSB flash at bootflash:.
```

解決法 confd が開始されているかどうかを確認します。

```
Router#show platform software yang-management process state
Confd Status: Started


Process              Status              State
------------------------------------------------------
nesd                 Running             Active
syncfd               Running             Active
ncsshd               Running             Not Applicable
dmiauthd             Running             Active
nginx                Running             Not Applicable
ndbmand              Running             Active
pubd                 Running             Active
```

解決法 vdaemon が起動しているかどうかを確認します。

```
Router#show platform software process list r0 name vdaemon
Name: vdaemon
  Process id       : 29075
  Parent process id: 29070
  Group id         : 29075
  Status           : S
  Session id       : 8829
  User time        : 263002
  Kernel time      : 347183
  Priority         : 20
  Virtual bytes    : 405110784
  Resident pages   : 12195
  Resident limit   : 18446744073709551615
  Minor page faults: 716496
  Major page faults: 9130
```

解決法 show コマンドを使用して確認します。

```
Router#show sd-routing local-properties summary
personality                       vedge
sp-organization-name              vIPtela Inc Regression
organization-name                 vIPtela Inc Regression
root-ca-chain-status              Installed
root-ca-crl-status                Not-Installed

certificate-status                Installed
certificate-validity              Valid
certificate-not-valid-before      May  8 17:49:38 2023 GMT
certificate-not-valid-after       May  7 17:49:38 2024 GMT

enterprise-cert-status            Not Applicable
enterprise-cert-validity          Not Applicable
enterprise-cert-not-valid-before  Not Applicable
enterprise-cert-not-valid-after   Not Applicable
dns-name                          vbond
site-id                           100
tls-port                          0
system-ip                         172.16.255.11
chassis-num/unique-id             C8K-7d921537-5402-4c3c-a3b5-a273dafc44d9
serial-num                        12345707
subject-serial-num                N/A
enterprise-serial-num             Not Applicable
token                             Invalid
keygen-interval                   0:02:00:00
retry-interval                    0:00:00:19
no-activity-exp-interval          0:00:00:20
dns-cache-ttl                     0:00:02:00
port-hopped                       FALSE
time-since-last-port-hop          0:00:00:00
```

```
embargo-check                    success
number-vbond-peers               2
number-active-wan-interfaces     1
```

WAN インターフェイスと IP に到達できない

考えられる原因 WAN インターフェイスに有効な IP アドレスがありません。

解決法 WAN インターフェイスの状態と IP を確認します。使用するコマンド

```
Router#show sd-routing local-properties wan ipv4
                              PUBLIC           PUBLIC  PRIVATE          PRIVATE
INTERFACE                     IPv4             PORT    IPv4             PORT     STATE
-------------------------------------------------------------------------------------
GigabitEthernet2              10.0.5.11        12386   10.0.5.11        12386    up
```

解決法 WAN インターフェイスに有効な IP アドレスがあり、UP 状態であることを確認します。

Cisco Validator 関連の問題

Cisco Validator（vBond）情報が見つからない

考えられる原因 ルーティングデバイスが Cisco Validator（vBond）に関連付けられていません。

解決法 Cisco Validator（vBond）情報を確認します。

```
Router#show sd-routing local-properties vbond
INDEX    IP                                      PORT
-----------------------------------------------------
0        10.0.12.26                              12346
1        2001:a0:c::1a                           12346
```

解決法 SD ルーティングデバイスが少なくとも 1 つの Validator に接続されていることを確認します。

制御接続の問題のトラブルシューティング

オンボーディング後にルーティングデバイスが SD-WAN Manager に接続できない

解決法 次のコマンドを使用して、ルーティングデバイスの接続ステータスを確認します。

```
Router#show sd-routing connections ?
detail   Display connections in detail
history  Control connections history
summary  Display connections summary
```

問題 **sd-routing connections summary** コマンドの結果が空になる

考えられる原因 SD-WAN Manager に接続されていない可能性があります。

解決法 次のコマンドを使用して、ルーティングデバイスの接続ステータスを確認します。

解決法 アクティブな接続がない場合、CLI からの出力はありません。

```
Router#show sd-routing connections summary
Router#
```

解決法 アクティブな接続がある場合は、下記のビューにそのことが示されます。

```
Router#show sd-routing connections summary
                                                        PEER                    PEER
PEER     PEER  PEER             SITE        PEER        PRIV   PEER             PUB
TYPE     PROT  SYSTEM IP        ID          PRIVATE IP  PORT   PUBLIC IP        PORT   STATE   UPTIME
```

```
-------------------------------------------------------------------------------------------------------------
vmanage  dtls  172.16.255.22    200         10.0.12.22    12446  10.0.12.22      12446  up      0:00:14:58
```

解決法 次のコマンドを使用して、ルーティングデバイスの接続ステータスを確認します。

```
Router# sh sd-routing connections history
PEER                          PEER
PEER      PEER      PEER              SITE         PEER              PRIVATE   PEER              PUBLIC
              LOCAL       REMOTE      REPEAT
TYPE      PROTOCOL  SYSTEM IP         ID           PRIVATE IP        PORT      PUBLIC IP         PORT     STATE
           ERROR       ERROR       COUNT  DOWNTIME
-------------------------------------------------------------------------------------------------------------
vmanage   dtls      172.16.255.22     200          10.0.12.22        12446     10.0.12.22        12446
tear_down         DISTLOC     NOERR       0      2023-04-26T17:08:13+0000
vbond     dtls      0.0.0.0           0            2001:a0:c::1a     12346     2001:a0:c::1a     12346
connect           DCONFAIL    NOERR       18     2023-04-25T01:04:08+0000
vbond     dtls      0.0.0.0           0            10.0.12.26        12346     10.0.12.26        12346
connect           DCONFAIL    NOERR       8      2023-04-25T00:59:09+0000
```

問題 **show sd-routing connections history** コマンドを実行しても結果が表示されない

考えられる原因 Validator と接続されていない可能性があります。

解決法 ルーティングデバイスで **ping vbond** コマンドを使用して、 Validator への到達可能性を確認します。

```
Router#ping vbond
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:A0:C::1A, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/30 ms
Router#
```

DTLS 接続障害（DCONFAIL）

これは制御接続の一般的な問題の 1 つであり、制御接続が確立されません。考えられる原因は、ファイアウォールまたはその他の接続の問題です。

考えられる原因 一部またはすべてのパケットがどこかでドロップ/フィルタリングされている可能性があります。ここでは、大量のパケットによる例が、`tcpdump` の結果に示されています。

- **考えられる原因** ネクストホップ（NH）ルータに到達できません。
- **考えられる原因** デフォルトゲートウェイがルーティング情報ベース（RIB）にインストールされていません。
- **考えられる原因** コントローラで Datagram Transport Layer Security（DTLS）ポートが開いていません。

解決法 デフォルト GW の ARP テーブルを確認します。

```
Router# show arp
```

解決法 デフォルト GW に ping を実行します。

```
ping <...>
```

解決法 Google DNSに ping を実行します。

```
ping 8.8.8.8
```

解決法 vBond で ICMP が許可されている場合は、vBond に ping を実行します。

```
ping <vBond IP>
```

解決法 vBond DNS にトレースルートを実行します。

```
traceroute <...>
```

Board-ID が初期化されていない（BIDNTPR）

これは制御接続の一般的な問題の1つであり、制御接続が確立されません。考えられる原因は、ファイアウォールまたはその他の接続の問題です。

考えられる原因 ルーティングデバイスのシャーシ番号/固有 ID/シリアル番号が Validator によって拒否されたことを示します。

- **考えられる原因** ネクストホップ（NH）ルータに到達できません。
- **考えられる原因** デフォルトゲートウェイがルーティング情報ベース（RIB）にインストールされていません。
- **考えられる原因** コントローラで Datagram Transport Layer Security（DTLS）ポートが開いていません。

解決法 ルーティングデバイスのシリアル番号を確認します。

```
Router#show sd-routing certificate serial
Chassis number: C8K-b596f134-0fa6-445f-9275-23f76ba90de0 serial number: 12345707 Subject S/N: N/A
```

解決法 この情報が Cisco Validator の有効なルーティングデバイスのリストに存在することを確認します。

```
vBond#  show orchestrator valid-vedges
HARDWARE

 INSTALLED  SUBJECT

 SERIAL     SERIAL
CHASSIS NUMBER                          SERIAL NUMBER                    VALIDITY  ORG
 NUMBER     NUMBER
-------------------------------------------------------------------------------------------------------------------------------
C8K-AA079CA1-C141-4AC6-9B76-05864005F94E  12345707                       valid     vIPtela Inc Regression
 N/A        N/A        N/A
```

解決法 ルーティングデバイスのエントリが存在しない場合は、次のことを確認します。

- **解決法** スマートアカウントにルーティングデバイスを追加済み
- **解決法** SD-WAN Manager に情報をアップロード済み
- **解決法** **[Configuration]** > **[Certificates]** > **[Send to Controllers]**から Validator にこの情報をプッシュ済み

解決法 シリアル番号が存在する場合は、有効な vEdge テーブルに重複するエントリがないか確認し、Cisco Technical Assistance Center（TAC）に連絡してさらにトラブルシューティングを行います。

シリアル番号が存在しない（CRTREJSER、BIDNTVRFD）

ルーティングデバイスのシャーシ番号/固有 ID/シリアル番号が Validator によって拒否されて、制御接続に失敗したことを示します。

考えられる原因 デバイスとコントローラ間の情報が一致していません。

- **解決法** ルーティングデバイスのシャーシ ID/シリアル番号を確認します。`Router#show sd-routing local-properties summary` コマンドを使用して情報を取得し、`vBond#show Orchestrator valid-vedges` コマンドを使用して取得した情報を Validator で確認します。

- **解決法** 不一致がある場合は、正しい情報を確認し、スマートアカウントまたは SD-WAN Manager にアップロードします。
- **解決法** デバイスとコントローラで使用されている**組織名**が同じであることを確認します。

証明書関連の問題

ルーティングデバイスのシャーシ番号/固有 ID/シリアル番号が Validator によって拒否されて、制御接続に失敗したことを示します。

考えられる原因 デバイスとコントローラ間の情報が一致していません。

解決法 次のコマンドを使用して証明書を表示し、問題を特定します。

```
Router#show sd-routing certificate installed

Router#show sd-routing certificate root-ca-cert

Router#show sd-routing certificate serial

Router#show logging process vdaemon internal
```

ログを使用した制御接続の問題のデバッグ

解決法 次のコマンドを使用して vdaemon BTrace ログを表示し、問題を特定します。

```
Router#show logging process vdaemon internal
Logging display requested on 2023/05/09 14:38:32 (UTC) for Hostname: [vm1], Model: [C8000V], Version: [17.13.01],
 SN: [9HP3SG7HKUU], MD_SN: [SSI130300YK]

Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis local ...
Unified Decoder Library Init .. DONE
Found 1 UTF Streams

2023/05/09 14:29:18.917119471 {vdaemon_R0-0}{255}: [vdaemon-cert] [18612]: (note): Validating certificate..
ou_check enabled
2023/05/09 14:29:18.917189711 {vdaemon_R0-0}{255}: [bss] [18612]: (note): not found
"/C=US/CN=b6ebad1f-43b6-4900-b355-e699449c84ac/O=Cisco Systems":307542112 at idx -1
2023/05/09 14:29:18.917387747 {vdaemon_R0-0}{255}: [bss] [18612]: (note): x509_verify_cert Success crl_loaded
 0
2023/05/09 14:29:18.993555137 {vdaemon_R0-0}{255}: [vdaemon-cert] [18612]: (note): Validating certificate..
ou_check enabled
2023/05/09 14:29:18.993572400 {vdaemon_R0-0}{255}: [bss] [18612]: (note): not found
"/C=US/CN=b6ebad1f-43b6-4900-b355-e699449c84ac/O=Cisco Systems":307542112 at idx -1
```

テクニカルサポートのリクエスト

ルーティングデバイスで **request tech-support** コマンドを使用すると、ログ、コア、および show コマンドの出力を含む tar ファイルを生成できます。

```
Router#request tech-support
11:51:06.396 UTC Thu Jul 20 2023 : Collecting 'show tech-support'...
11:51:42.549 UTC Thu Jul 20 2023 : 'show tech-support' collected successfully!
11:51:43.798 UTC Thu Jul 20 2023 : Collecting binary traces...
11:51:43.965 UTC Thu Jul 20 2023 : Binary traces collected successfully!
11:51:43.967 UTC Thu Jul 20 2023 : Collecting platform-dependent files...
11:52:39.007 UTC Thu Jul 20 2023 : Platform-dependent files collected successfully!
11:52:39.013 UTC Thu Jul 20 2023 : Generating tech-support bundle...
11:52:46.873 UTC Thu Jul 20 2023 : Tech-support bundle file
bootflash:core/vm1-debug_bundle_20230720-115143-UTC.tar.gz [size: 22358 KB]
```

```
11:52:46.873 UTC Thu Jul 20 2023 : Tech-support bundle generated successfully!

Router#dir bootflash:/core
Directory of bootflash:/core/

186     -rw-            10849  Jul 20 2023 11:52:46 +00:00  vm1-debug_bundle_20230720-115143-UTC-info.txt
192     -rw-         22893633  Jul 20 2023 11:52:44 +00:00  vm1-debug_bundle_20230720-115143-UTC.tar.gz
38      drwx             4096  Jul 18 2023 20:33:36 +00:00  modules

5173313536 bytes total (3922272256 bytes free)
vm1#
```

（注）

*.txt ファイルには、tar.gz にバンドルされているすべてのファイルのリストが含まれています。

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。