Cisco SD-WAN Manager を使用した SD ルーティングデバイスの管理

この章では、Cisco SD-WAN Manager を使用した SD ルーティングデバイスの管理とモニタリングについて説明します。ここで説明する内容は、次のとおりです。

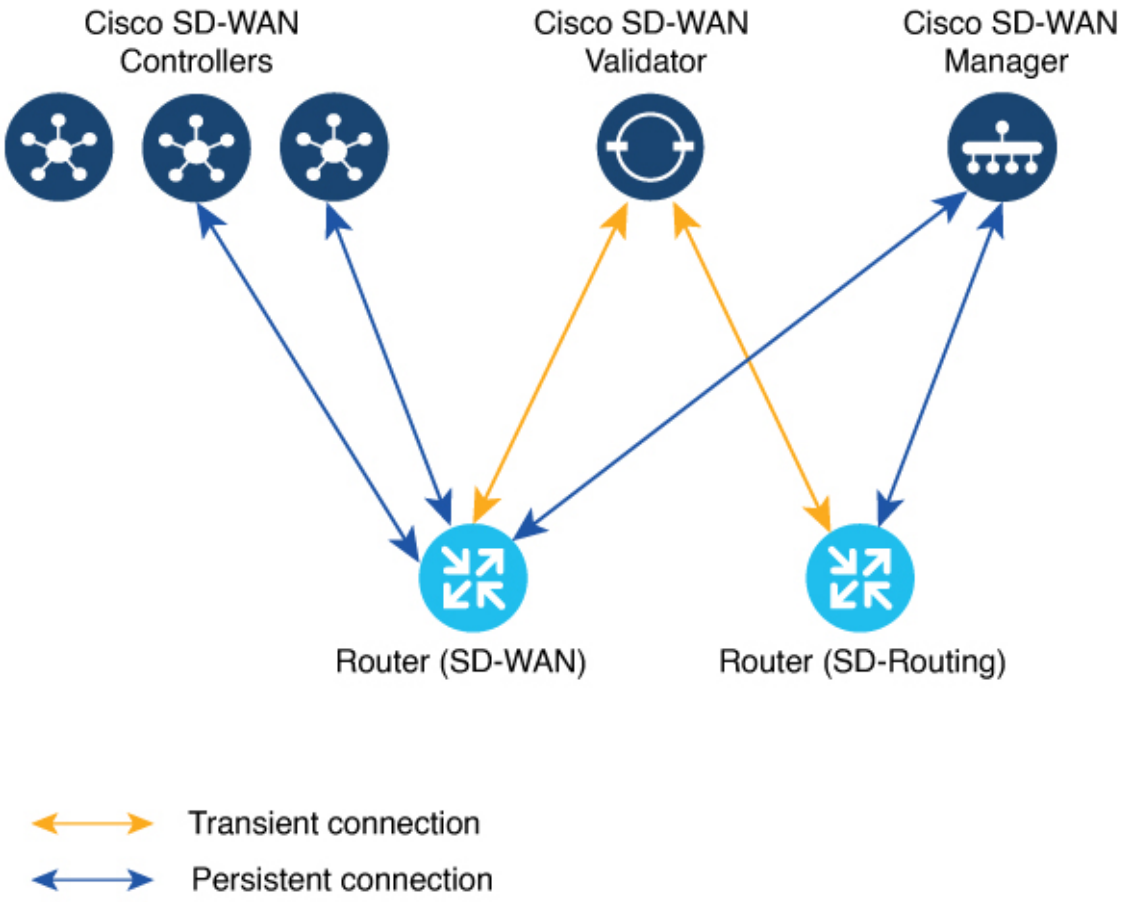
Cisco SD-WAN Manager を使用した SD ルーティングデバイスのモニタリングについて

この機能を使用すると、非 SD-WAN モードで動作している Cisco IOS XE デバイスで Cisco SD-WAN Manager を使用して基本的な管理機能を実行できます。Cisco IOS XE 17.12.1a 以降、このようなデバイスは SD ルーティングデバイスと呼ばれます。単一のネットワーク管理システム（NSM）（Cisco SD-WAN Manager）を使用して、すべての Cisco IOS XE ルータを管理およびモニタリングすることで、ソリューションの導入を簡素化できます。

（注） Cisco IOS-XE ソフトウェアの No Payload Encryption（NPE）または No Lawful Intercept and No Payload Encryption（NOLI/NPE）イメージは、Cisco SD-WAN Manager 機能を使用した SD ルーティングデバイスの管理をサポートしていません。

（注） この機能に必要な最小ソフトウェアバージョンは、Cisco IOS XE 17.12.1a および Cisco SD-WAN リリース 20.12.1 です。

図 *1 : SD* ルーティングデバイスの管理



Cisco SD-WAN Manager を使用して SD ルーティングデバイスを管理するメリット

1. エンタープライズ ネットワークでは、1 つの NMS（Cisco SD-WAN Manager）で Cisco Catalyst SD-WAN 環境と SD ルーティング環境に対応できます。
2. 同じ Cisco SD-WAN Manager 上で Cisco SD-WAN デバイスと SD ルーティングデバイスが共存できます。

前提条件

SD ルーティングデバイスをオンボードするための前提条件は次のとおりです。

- デバイスがインストールモードで Cisco IOS XE 17.12.1a イメージを実行していることを確認します。これらのモードの詳細については、「Switch Modes Using Cisco CLI」[英語] を参照してください。
- Cisco SD-WAN Manager インスタンスがオンプレミスまたはクラウドでホストされていること。
- デバイスから Cisco SD-WAN Manager への接続が確立されていること。
- 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 モデルを有効にします。
- 自律モードで動作するデバイスは、コントローラ（Cisco SD-WAN Validator および Cisco SD-WAN Manager）とのセキュアな制御接続を確立するために、次の基本設定を手動で行う必要があります。
  - システムのプロパティ：
    - システム IP
    - 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 ）
  - インターフェイス設定
    - 静的または動的 IP アドレスとサブネットマスクを持つ物理インターフェイス
    - Cisco SD-WAN Validator または Cisco SD-WAN Manager への到達可能性を提供するダイナミックルーティングまたはデフォルトルート

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 IOS XE 17.12.1a リリースでは、基本的なモニタリングがサポートされており、後続のリリースで追加機能をサポート予定です。サポートされている機能の詳細については、プラットフォーム固有のリリースノートを参照してください。
- 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。

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。

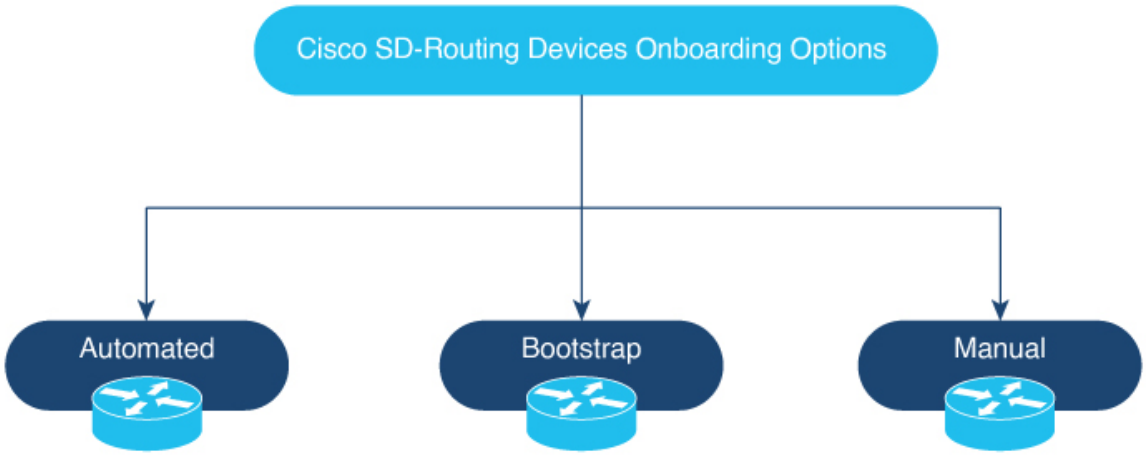
表 *1:* サポートされている *WAN* エッジプラットフォームとオンボーディングオプション

プラットフォーム	Automated	Bootstrap	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

プラットフォーム	Automated	Bootstrap	手動
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	該当なし （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
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

SD ルーティングデバイスのオンボーディング

ここでは、SD ルーティングデバイスをオンボードするためのワークフローについて説明します。



- SD ルーティングデバイスのオンボーディング
  - 自動オンボーディング：Dynamic Host Configuration Protocol（DHCP）および Cisco Plug and Play（PNP）を使用して、デバイスを Cisco SD-WAN Manager に自動的にオンボードします。
  - ブートストラップ オンボーディング：ブートフラッシュまたは USB 上のブートストラップファイルを使用し、Cisco SD-WAN Manager に到達するために必要な最小構成でデバイスを設定します。
  - 手動オンボーディング：IOS-XE コマンドを使用してデバイスを手動で設定し、Cisco SD-WAN Manager にデバイスをオンボードします。

SD ルーティングデバイスをオンボードするための前提条件は次のとおりです。

- システム IP

手動オンボーディングの前提条件は次のとおりです。

- 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）

自動化されたワークフローを使用した SD ルーティングデバイスのオンボーディング

自動化されたワークフローを使用して SD 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。

- プラグアンドプレイ接続ポータルを設定します
- Quick Connect ワークフローを使用して Cisco SD-WAN Manager を設定します
- Day-0 モードでデバイスを起動します

プラグアンドプレイ接続ポータルの設定

PnP 接続ポータルを設定するには、次の手順を実行します。

始める前に

シスコユーザー ID を使用して、PnP 接続ポータル、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にアクセスでき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） [Cisco SD-WAN Managerの設定（Cisco SD-WAN Manager Settings）] ページでスマートアカウントのログイン情報を入力した後にのみ、プラグアンドプレイ接続の同期を有効にできます。

ステップ 1 sotware.cisco.com > [Network Plug and Play] > [Manage Devices] に移動し、スマートアカウントとバーチャルアカウントにアクセスできることを確認します。

ステップ 2 コントローラプロファイルを作成し、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。

（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 3 コントローラプロファイルとコントローラタイプを入力し、[Next] をクリックします。

ステップ 4 [Add Controller Profile] に必要なパラメータを入力し、[Next] をクリックします。

ステップ 5 デバイスを PnP 接続に追加します。デバイスを追加する場合は、[Device Mode] フィールドで、ドロップダウンリストから SD ルーティングモードのデバイスに対して [AUTONOMOUS] を選択します。

Quick Connect ワークフローを使用した Cisco SD-WAN Manager の設定

Quick Connect ワークフローを使用して Cisco SD-WAN Manager を設定するには、次の手順を実行します。

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

ステップ 2 [Get Started] をクリックします。

ステップ 3 [Next] をクリックします。

ステップ 4 プロビジョニングファイル（.csv または .viptela）を PnP から Cisco SD-WAN Manager にアップロードしていない場合は、**.csv upload**、**.viptela upload**、[Sync Smart Account] オプションのいずれかを使用して、デバイスを Cisco SD-WAN Manager に追加できます。デバイスがすでに Cisco SD-WAN Manager に追加されている場合は、[skip for now] オプションを選択します。

（注） .csv ファイルは、ハードウェアデバイスにのみ適用できます。.viptela ファイルは、ハードウェアデバイスとソフトウェアデバイスの両方に適用できます。

ステップ 5 まだ同期していない場合は、[Sync Smart Account] をクリックします。デバイスの表にデバイスがリストされているはずです。

[Sync Smart Account]をクリックします。

ステップ 6 **[Next]** をクリックします。

ステップ 7 [Add and Review Device Configuration] ダイアログボックスで、サイト ID、システム IP、ホスト名を入力し、[Apply] をクリックします。

ステップ 8 **[Next]** をクリックします。

ステップ 9 オプションタグを追加し、[Next] をクリックします。

ステップ 10 追加されたデバイスを確認するには、[Configuration] > [Devices] の順に選択し、[Table Settings] で [enable Device Model] をクリックします。

ステップ 11 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。デバイスが追加されたことを確認するには、**[Configuration]** > **[Certificates]** の順に選択します。

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 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。

ステップ 3 デバイス制御接続が Cisco SD-WAN Manager で稼働します。

ステップ 4 **show sd-routing connections summary** コマンドを使用して、エッジ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
------------------------------------------------------------------------------------------------
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 5 Cisco SD-WAN Manager で制御接続ステータスを確認します。

ブートストラップを使用したSDルーティングデバイスのオンボーディング

ブートストラップを使用して SD 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。

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

ステップ 2 [Get Started] をクリックします。

ステップ 3 [Next] をクリックします。

ステップ 4 プロビジョニングファイル（*.csv* または *.viptela*）を PnP から Cisco SD-WAN Manager にアップロードしていない場合は、**.csv upload**、**.viptela upload**、[Sync Smart Account] オプションのいずれかを使用して、デバイスを Cisco SD-WAN Manager に追加できます。デバイスがすでに Cisco SD-WAN Manager に追加されている場合は、[skip for now] オプションを選択します。

（注） .csv ファイルは、ハードウェアデバイスにのみ適用できます。.viptela ファイルは、ハードウェアデバイスとソフトウェアデバイスの両方に適用できます。

ステップ 5 導入準備するデバイスを選択し、[Next] をクリックします。

ステップ 6 [Add and Review Configuration] ダイアログボックスで、サイト ID、システム IP、ホスト名を入力し、[Apply] をクリックします。

ステップ 7 追加されたデバイスを確認するには、[Configuration] > [Devices] の順に選択し、[Table Settings] で [enable Device Model] をクリックします。

ステップ 8 [Configuration] > [Certificate] ページで、デバイスが有効な状態であることを確認します。

ステップ 9 Cisco SD-WAN Manager のメニューから、[Configuration] > [Devices] の順に選択します。

ステップ 10 Cisco SD ルーティング ソフトウェア デバイス（Cisco c8000V）の場合は、次の手順を実行してブートストラップを生成し、デバイスをオンボードします。

（注） ハードウェアデバイスの場合は、ステップ 11 の手順に従います。

a) ウィンドウの右側のペインで [...] をクリックし、[Generate Bootstrap Configuration] を選択します。

b) [Cloud-init] オプションを選択し、WAN インターフェイス名の名前を入力して、[OK] をクリックします。

（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 SD-WAN Validator と Cisco SD-WAN Manager に到達可能であることを確認します。また、ソフトウェアデバイスの場合は、VPN0 インターフェイスとしてギガビットイーサネット 1 インターフェイスのみを使用します。

c) [Download] 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。

例：

サンプルイメージ：*ciscosdwan_cloud_init.cfg*

証明書付きのサンプルイメージ：*ciscosdwan_cloud_init_with_ent_cert.cfg*

d) クラウドベースのコントローラの場合、ダウンロードしたブートストラップファイルは、デバイスの導入時にユーザーデータフィールドとして追加できます。コントローラを SD ルーティングモードで起動し、Cisco SD-WAN Validator および Cisco SD-WAN Manager との接続を確立します。

ステップ 11 ハードウェアデバイスの場合は、次の手順を実行してブートストラップを生成し、デバイスをオンボードします。

a) デバイスページの Cisco SD-WAN Manager のメニューから、[Export Bootstrap Configuration] をクリックします。

b) [SD-Routing] のチェックボックスをオンにします。[Export Bootstrap Configuration] ダイアログボックスで、[WAN Interface name] を入力します。

（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。

c) [Generate Generic Configuration] をクリックして、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 *ciscosdawn.cfg* に変更します。

（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 SD-WAN ValidatorとCisco SD-WAN Managerに到達可能であることを確認します。

ブートストラップファイルには、組織名、Cisco SD-WAN 検証 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。

d) 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ブートフラッシュにコピーします。

e) **sd-routing bootstrap load bootflash:ciscosdwan.cfg** コマンドを実行します。

例：

```
Router# sd-routing bootstrap load bootflash:ciscosdwan.cfg
Located the file. Beginning to extract the data
Extraction summary
-Organization name - "aniltb2"
```

```
-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
```

f) **show sd-routing system status**、**show sd-routing system status**、および **show sd-routing local-properties summary** コマンドを使用して、制御接続を確認します。

デバイスの手動でのオンボーディング

SD 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 Cisco SD-WAN Manager のメニューから、[Workflows] > [Quick Connect] の順に選択します。

ステップ 2 [Get Started] をクリックします。

ステップ 3 [Next] をクリックします。

ステップ 4 プロビジョニングファイル（.csv または .viptela）を PnP から Cisco SD-WAN Manager にアップロードしていない場合は、**.csv upload**、**.viptela upload**、[Sync Smart Account] オプションのいずれかを使用して、デバイスを Cisco SD-WAN Manager に追加できます。デバイスがすでに Cisco SD-WAN Manager に追加されている場合は、[skip for now] オプションを選択します。

（注） .csv ファイルは、ハードウェアデバイスにのみ適用できます。.viptela ファイルは、ハードウェアデバイスとソフトウェアデバイスの両方に適用できます。

ステップ 5 導入準備するデバイスを選択し、[Next] をクリックします。

ステップ 6 [Add and Review Configuration] ダイアログボックスで、サイト ID、システム IP、ホスト名を入力し、[Apply] をクリックします。

ステップ 7 追加されたデバイスを確認するには、[Configuration] > [Devices] の順に選択し、[Table Settings] で [enable Device Model] をクリックします。

ステップ 8 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。デバイスが追加されたことを確認するには、**[Configuration]** > **[Certificates]** の順に選択します。

ステップ 9 手動でオンボードするデバイスに応じて、次の手順のいずれかを実行します。

a) ハードウェアデバイスの場合は、システムの起動後に IOS コマンドを使用して、最初の Day-0 設定を入力します。

b) Cisco SD ルーティング ソフトウェア デバイスの場合は、ブートストラップなしで Amazon Web Services（AWS）または Azure に Cisco c8000v を導入します。

ステップ 10 Cisco SD-WAN Manager で制御接続を有効にするための最小限のパラメータを設定します。

例：

```
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
```

ステップ 11 SD ルーティングモードを有効にするために必要なパラメータを設定します。

a) 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。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。

b) Validator の IP または Validator の名前を設定します。

c) 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 12 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 13 企業向けのオーバーレイネットワークの場合は、**request platform software sd-routing root-cert-chain install bootflash:cacert.pem** コマンドを使用してルート証明書をインストールします。Cisco SD-WAN Manager

が **Cisco PKI** ではなくエンタープライズ証明書で設定されている場合は、デバイスにルート証明書をインストールする必要があります。

ステップ 14 デバイスに応じて、次のいずれかの手順を実行します。

a) Cisco 8000v デバイスの場合は、CA から Cisco 8000v にルート証明書をコピーします。

b) 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。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る場合は、**request platform software sd-routing root-cert-chain install** <*path-to-root-cert*> コマンドを使用します。

例：

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

ステップ 15 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。

（注） デフォルトでは、証明書はハードウェアデバイスにロードされます。この手順は、ソフトウェアデバイスを手動でオンボードする場合を対象としています。

ステップ 16 **request platform software sd-routing csr upload** <*bootflash:ctrl_mng/test*> 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。*bootflash:ctrl_mng/* ディレクトリ内に作成されたフォルダには、任意の名前を指定できます。

ステップ 17 生成された CSR ファイルを、エンタープライズ CA があるディレクトリにコピーします。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 形式の証明書ファイルを生成できます。

ステップ 18 生成された *certificate.pem* ファイルをデバイスにコピーし、**request platform software sd-routing certificate install** <*path-to-certificate-file*> コマンドを使用して、デバイスに証明書をインストールします。

ステップ 19 証明書のインストールステータスを確認します。

例：

```
SJC_Primary# 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 20 Cisco SD-WAN Manager でデバイスをオンボードします。クライアント証明書をインストールする場合は、Cisco SD-WAN Manager に以下を追加します。

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、**how 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) **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。

または

c) シャーシ番号とシリアル番号を使用して *.viptela* ファイルを作成し、そのファイルを Cisco SD-WAN Manager にアップロードしてコントローラに送信します。

ステップ 21 Cisco SD-WAN Manager で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
```

トークンを使用したシャーシのアクティブ化によるデバイスのオンボーディング

シャーシ番号をアクティブ化にするには、次の手順を実行します。

（注） この方法は、Cisco SD-WAN ソフトウェアデバイス（Cisco c8000v）でのみ使用できます。

ステップ 1 PnP スマート同期方式を使用して Cisco SD-WAN Manager にデバイスを追加します。

ステップ 2 sotware.cisco.com > [Network Plug and Play] > [Manage Devices] に移動し、スマートアカウントとバーチャルアカウントにアクセスできることを確認します。

ステップ 3 コントローラプロファイルを作成し、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。

ステップ 4 コントローラタイプに vBond と入力し、[Next] をクリックします。

ステップ 5 [Add Controller Profile] に必要なパラメータを入力し、[Next] をクリックします。

ステップ 6 デバイスを PnP 接続に追加します。デバイスを追加する場合は、[Device Mode] フィールドで、ドロップダウンリストから SD ルーティングモードのデバイスに対して [AUTONOMOUS] を選択します。

ステップ 7 Cisco SD-WAN Manager のメニューから **[Administration]** > **[Settings]** の順に選択します。

ステップ 8 [Smart Account Credentials] に移動し、[Edit] をクリックします。

ステップ 9 ユーザー名とパスワードを入力し、[Save] をクリックします。

ステップ 10 次の方法を使用して、PnP Connect ポータルからデバイスリストをインポートできます。

a) [Configuration] > [Devices] の順に選択し、[Sync Smart Account] をクリックします。

または

a) PnP Connect からダウンロードした *.viptela* をアップロードします。[Controller profiles] に移動し、[Download the Provisioning file] をクリックします。
b) Cisco SD-WAN Manager のメニューから、[Configuration] > [Devices] > [Upload WAN Edge List] の順に選択します。

ステップ 11 デバイスは、スタートアップ コンフィギュレーションで自律モードになります。デバイスは Day-0 モードになりません。

ステップ 12 デバイスに最小設定を適用します。

例：

```
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 13 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 14 ソフトウェア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、**request platform soft sd-routing activate chassis** <新たにアップロードされたシャーシ ID> **token** <Cisco SD-WAN Manager によって生成されたトークン> コマンドを使用します。

ステップ 15 企業向けのオーバーレイネットワークの場合は、**request platform software sd-routing root-cert-chain install bootflash:cacert.pem** コマンドを使用してエンタープライズルート証明書をインストールします。オーバーレイネットワークが **Cisco PKI** の場合、ルート証明書をインストールする必要はありません。

（注） 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。CSR は、ステップ 14 の実行中に生成されます。

ステップ 16 次のコマンドを使用して、エッジ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
```

マルチテナント SD ルーティングデバイスのオンボーディング

ここでは、マルチテナント SD ルーティングデバイスをオンボードするためのワークフローについて説明します。

- 自動オンボーディング
- 手動オンボーディング

自動化されたワークフローを使用したマルチテナント SD ルーティングデバイスのオンボーディング

マルチテナント SD 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。

ステップ 1 sotware.cisco.com > [Network Plug and Play] > [Manage Devices] に移動し、スマートアカウントとバーチャルアカウントにアクセスできることを確認します。

a) 仮想アカウントを作成します。
b) コントローラプロファイルを作成し、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。
c) コントローラタイプに vBond と入力し、[Next] をクリックします。
d) [Add Controller Profile] に必要なパラメータを入力し、[Next] をクリックします。
e) デバイスを PnP 接続に追加します。デバイスを追加する場合は、[Device Mode] フィールドで、ドロップダウンリストから SD ルーティングモードのデバイスに対して [AUTONOMOUS] を選択します。

または

ステップ 2 Cisco SD-WAN Manager のメニューから、[Workflows] > [Quick Connect] の順に選択します。

ステップ 3 [Get Started] をクリックします。

ステップ 4 [Next] をクリックします。

ステップ 5 .csv ファイルを Cisco SD-WAN Manager にアップロードしていない場合は、いずれかのアップロードオプションを使用してファイルをアップロードします。ファイルをアップロード済みの場合は、[skip for now] オプションを選択します。

ステップ 6 [Sync Smart account]、[csv upload]、[.viptela upload] のいずれかをクリックします。デバイスの表にデバイスがリストされているはずです。

ステップ 7 ソフトウェアデバイスの場合は、前の項で説明したようにブートストラップファイルを生成し、c8000v ユーザー設定ファイルとして追加します。

（注） マルチテナント設定の場合は、システム IP を設定する際に、Quick Connect ワークフローを使用する必要があります。CLI オプションを使用してシステム IP を設定しないでください。

ステップ 8 デバイスタイプに基づいて、次のいずれかの手順を実行します。

a) ソフトウェアデバイスの場合は、Azure または AWS に Cisco c8000v を展開し、カスタムデータまたはユーザーデータ入力としてブートストラップファイルを入力します。

b) ハードウェアデバイスの場合は、デバイスを Day-0 状態で起動します。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 9 デバイスで Cisco SD-WAN Manager が起動します。

ステップ 10 デバイスのステータスを確認するには、**show sd-routing connection summary status** および **show sd-routing local-properties summary** コマンドを使用します。

マルチテナント SD ルーティングデバイスの手動によるオンボーディング

マルチテナント SD 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 Cisco Catalyst 8000v を自律モードで Azure または AWS に展開します。

a) sotware.cisco.com > [Network Plug and Play] > [Manage Devices] に移動し、スマートアカウントとバーチャルアカウントにアクセスできることを確認します。
b) 仮想アカウントを作成します。
c) コントローラプロファイルを作成し、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。
d) コントローラタイプに vBond と入力し、[Next] をクリックします。
e) [Add Controller Profile] に必要なパラメータを入力し、[Next] をクリックします。
f) デバイスを PnP 接続に追加します。デバイスを追加する場合は、[Device Mode] フィールドで、ドロップダウンリストから SD ルーティングモードのデバイスに対して [AUTONOMOUS] を選択します。

ステップ 2 Netconf-Yang を有効にするための最小パラメータを設定します。

例：

```
config terminal
 netconf-yang
end
```

ステップ 3 **show platform software yang-management process state** コマンドを使用して、Netconf-Yang のステータスを確認します。

ステップ 4 Cisco SD ルーティングモードを有効にするために必要なパラメータを設定します。

a) 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。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。
b) Cisco SD-WAN Validator の IP または Cisco SD-WAN Validator の名前を設定します。
c) Cisco SD-WAN Validator、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。

（注） マルチテナント設定の場合は、システム IP を設定する際に、Quick Connect ワークフローを使用する必要があります。CLI オプションを使用してシステム IP を設定しないでください。ただし、マルチテナント展開では、SD ルーティングデバイスの SP 組織名を設定するために CLI オプションを使用できます。この組織名は、マルチテナント展開のテナントの組織名を指します。デバイスがオンボードされた後、**show sd-routing local-properties summary** コマンドでのみ表示されます。

ステップ 5 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 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 6 エッジデバイスの SD ルーティング設定を確認します。また、署名用のシャーシ番号を取得し、Cisco SD-WAN Manager WAN エッジリストにアップロードします。

ステップ 7 デバイスのステータスを確認するには、**show sd-routing local-properties summary** コマンドを使用します。

ステップ 8 root-ca-chain.crt 証明書を Cisco SD-WAN Manager から SD ルーティングデバイスにコピーします。

（注） この手順は、エンタープライズ証明書方式を使用している場合にのみ必要です。**Cisco PKI** 方式を使用している場合は、この手順をスキップできます。

ステップ 9 SD ルーティングデバイスに *root-ca-chain.crt* をインストールします。

ステップ 10 プロビジョニングファイル（*.Viptela*）を PnP から Cisco SD-WAN Manager WAN エッジリストにアップロードし、コントローラに送信します。

ステップ 11 シャーシ番号、シリアル番号を使用して *.viptela* ファイルを作成し、署名します。ファイルを Cisco SD-WAN Manager にアップロードし、コントローラに送信します。

ステップ 12 Cisco SD-WAN Manager からトークンを取得します。Cisco SD-WAN Validator および Cisco SD-WAN Manager との制御接続を確立してデバイスをオンボードするには、**request platform software sd-routing activate chassis-number** <*chassis-num*> **token** <*token*> コマンドを使用します。

ステップ 13 デバイスのステータスを確認するには、**show sd-routing connection summary status** および **show sd-routing local-properties summary** コマンドを使用します。

ワンタッチプロビジョニングを使用した Cisco SD-WAN Manager へのデバイスのオンボーディング

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。

始める前に

ワンタッチプロビジョニングを使用してデバイスを設定する場合は、プロセスが次の要件を満たしていることを確認します。

- デバイスが自律モードになっている必要があります。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コンフィギュレーションが必要です。デバイスが Day-0 状態であってはなりません。
- デバイスは、WAN インターフェイスを介して Cisco SD-WAN Validator および Cisco SD-WAN に到達するように設定する必要があります。

  デバイスには、SD ルーティング機能がコントローラと通信するために必要な最小限の設定が必要です。

また、ワンタッチプロビジョニング方式を使用してデバイスを Cisco SD-WAN Manager にオンボーディングすると、デバイスを追加するための次の手順が不要になります。

- **.csv** 、**.viptela**、または **sync smart account** を使用した Cisco SD-WAN Manager への WAN エッジデバイスの追加。
- シスコデバイスは SD ルーティングモードで設定する必要があります。Cisco SD-WAN Manager にデバイスを追加せずにデバイスを設定するには、手動またはブートストラップ方式を使用する必要があります。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Administration] > [Settings] の順に選択し、[One Touch Provisioning] を有効にします。

ステップ 2 [One Touch Provisioning] が [Enabled] になっているか確認します。[Enabled] の場合は、ステップ 5 に進みます。

ステップ 3 [One Touch Provisioning] が [Disabled] になっている場合は、[Edit] をクリックします。

ステップ 4 [Enable Claim WAN Edges] 設定で、[Enabled] を選択して [Save] をクリックします。

ステップ 5 [Configuration] > [Devices] > [Unclaimed Devices] に移動します。

a) 要求するデバイスを選択し、[Claim Device(s)] をクリックします。

b) デバイスは、[Unclaimed WAN Edges] から削除され、[WAN Edge List] に表示されます。

ステップ 6 デバイスのステータスを確認するには、**show sd-routing system status** および **show sd-routing local-properties summary** コマンドを使用します。

機能のプロビジョニング解除

機能のプロビジョニングを解除するには、次の手順を実行します。

ステップ 1 デバイスから SD ルーティング機能の設定を削除します。

例：

（注） これにより、すべての証明書が削除されます。すべての証明書を再インストールする必要があります。

例：

```
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no sd-routing
Warning! Disabling this feature will result in deleting client certificates. Please backup the
certificates and use the CLIs to reinstall them on enabling this feature again.
Do you want to continue? (y/n)[n]: y
```

ステップ 2 デバイスを無効にします。手順については、「デバイスの手動でのオンボーディング （11 ページ）」の項にある手順 4 を参照してください。

ステップ 3 デバイスを削除する手順は、次のとおりです。

a) Cisco SD-WAN Manager のメニューから、[Configuration] > [Devices] の順に選択します。
b) [WAN Edge List] をクリックし、無効にするデバイスを選択します。
c) [Delete WAN Edge] をクリックします。
d) メッセージを読んで、[Yes] をクリックします。

ソフトウェアイメージの管理

ここでは、ソフトウェアイメージをアップグレードするプロセスについて説明します。Cisco SD-WAN Manager は、事前にパッケージ化された tar.gz 形式のシスコ仮想マシンイメージ、または qcow2 形式のイメージのアップロードをサポートします。qcow2 イメージファイルを選択した場合は、スキャフォールドファイルをアップロードする必要があります。同様に、サービスチェーンの作成中に仮想ネットワーク機能（VNF）を設定するときに、イメージパッケージファイル、またはスキャフォールドファイルを含む qcow2 イメージファイルを選択できるようになりました。Cisco SD-WAN Manager は NETCONF と通信し、自律モードデバイスが Cisco SD-WAN Manager にオンボーディングされたときに、シンプルなリモートプロシージャコールを使用して運用データを取得します。NETCONF は、ネットワークデバイスと通信する標準的なトランスポートプロトコルであり、設定データを編集するためのメカニズムを提供します。SD ルーティングデバイスの Cisco SD-WAN Manager アップグレードワークフローは、コントローラモードのワークフローに似ています。

（注） この機能を動作させるために必要な最小限のソフトウェアバージョンは、Cisco IOS XE 17.12.1a です。

CLI を使用したソフトウェアアップグレード

ソフトウェアをアップグレードするには、次の手順を実行します。

始める前に

- ディスク容量の確認：イメージのダウンロードと展開に使用可能なブートフラッシュ容量を確認します。
- イメージリポジトリの確認：リモートサーバーの到達可能性を確認します。
- 自動ブートの有効化：デバイスで自動ブートが有効になっているかどうかを確認します。

ステップ 1 ソフトウェアページの https://software.cisco.com から Cisco IOS XE リリース 17.12 イメージをダウンロードします。

ステップ 2 イメージをデバイスにアップロードします。

ステップ 3 **install add file <bootflash:/file name> activate commit** コマンドを使用して新規ソフトウェアをインストールし、アクティブ化します。

例：

```
Device# install add file <bootflash:/c8000v-universalk9.17.12.01.0.166070.SSA.bin activate commit
```

アクティベーションが完了すると、デバイスがリロードされます。

（注） これはインタラクティブなコマンドであり、確認して同意するように求められます。デバイスに保存されていない設定がある場合、このコマンドの実行に失敗します。**write memory** コマンドを実行して、ソフトウェアを再インストールする必要があります。

ステップ 4 **install commit** コマンドを使用してアップグレードを確認します。

リポジトリへのソフトウェアイメージの追加

SD ルーティングデバイスまたは Cisco SD-WAN Manager のソフトウェアを新しいソフトウェアバージョンにアップグレードする前に、ソフトウェアイメージを Cisco SD-WAN Manager ソフトウェアリポジトリに追加する必要があります。Cisco SD-WAN Manger とリモートサーバーを使用して Cisco SD-WAN コントローラに Cisco Catalyst 8000v エッジソフトウェアをアップロードする方法の詳細については、『Cisco SD-WAN Monitor and Maintain Configuration Guide』[英語] の「Manage Software Repository」の項を参照してください。

Cisco SD-WAN Manager を使用したソフトウェアのアップグレード

デバイスでソフトウェアイメージをアップグレードするには、次の手順を実行します。

始める前に

- ここで説明する手順では、旧ソフトウェアバージョンにダウングレードすることはできません。ダウングレードする必要がある場合は、『Cisco SD-WAN Getting Started Guide』の「Downgrade a Cisco vEdge Device to an Older Software Image」[英語] を参照してください。

- Cisco SD-WAN Manager クラスタのアップグレードを実行する場合は、「Upgrade Cisco vManage Cluster」[英語] を参照してください。
- 自動ブートの有効化：デバイスで自動ブートが有効になっているかどうかを確認します。

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

ステップ 2 ソフトウェアをアップグレードするデバイスのタイプに基づいて、[WAN Edge]、[Control Components]、[Manager] のいずれかをクリックします。

ステップ 3 デバイステーブルで、アップグレードするデバイスの左端にあるチェックボックスをオンにして選択します。

（注） Cisco SD-WAN Manager クラスタのアップグレード時に、テーブル内に表示されるクラスタのすべてのノードを選択します。

ステップ 4 [Upgrade] をクリックします。

ステップ 5 [Software Upgrade] スライドイン ペインで、次の手順を実行します。

a) どのサーバーからデバイスにイメージをダウンロードするかを選択します。[Manager]、[Remote Server]、[Remote Server – Manager] のいずれかです。

（注）
- [Remote Server] を選択する場合は、デバイスがリモートサーバーに到達可能になっていることを確認してください。
- リモートサーバーからイメージを手動でダウンロードする際に、次の有効な文字のみが使用されていることを確認してください。
  - ユーザー ID：a ～ z、0 ～ 9、.、_、-
  - パスワード：a ～ z、A ～ Z、0 ～ 9、_、*、.、+、=、%、-
  - URL 名またはパス：a ～ z、A ～ Z、0 ～ 9、_、*、.、+、=、%、-、:、/、@、?、~

b) [SD-WAN Manager] の場合は、[Version] ドロップダウンリストからイメージのバージョンを選択します。

c) [Remote Server – SD-WAN Manager] の場合、ドロップダウンリストから [vManage OOB VPN] を選択し、[Version] ドロップダウンリストからイメージのバージョンを選択します。

d) [Activate and Reboot] チェックボックスをオンにします。

このチェックボックスをオフにすると、ソフトウェアイメージはダウンロードされてデバイスにインストールされますが、イメージはアクティブ化されず、デバイスは再起動されません。アップグレードタスクが完了したら、イメージをアクティブ化する必要があります。

（注） Cisco SD-WAN Manager ソフトウェアのアップグレード中は、[Activate and Reboot] オプションは使用できません。アップグレードタスクが完了して Cisco SD-WAN Manager が再起動したら、イメージをアクティブ化する必要があります。

e) [Upgrade] をクリックします。

現在のデバイス構成が保持したままで、新しいソフトウェアバージョンを使用してデバイスが再起動します。[Task View] ページが開き、デバイスのアップグレードの進行状況が表示されます。

ステップ 6 アップグレードが完了するまで待ちます。完了までに数分かかります。[Status] 列に「Success」と表示されたら、アップグレードは完了です。

ステップ 7 Cisco SD-WAN Manager のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択し、デバイスを表示します。

ステップ 8 ソフトウェアをアップグレードするデバイスのタイプに基づいて、[WAN Edge]、[Control Components]、[Manager] のいずれかをクリックします。

ステップ 9 デバイステーブルで、アップグレードされたデバイスの [Current Version] 列に新しいバージョンが表示されていることを確認します。[Reachability] 列に「reachable」と表示されていることを確認します。

（注）
- Cisco SD-WAN Manager への制御接続が、設定された時間制限内に確立されない場合、Cisco SD-WAN Manager は自動的に、デバイスを以前実行されていたソフトウェアイメージに戻します。
- コントローラデバイスで実行されているバージョンよりも高いバージョンに Cisco VEdge ソフトウェアをアップグレードすると、ソフトウェアの非互換性が発生する可能性があることを伝える警告メッセージが表示されます。Cisco VEdge ソフトウェアをアップグレードする前に、コントローラのソフトウェアをアップグレードすることを推奨します。

ソフトウェアイメージの削除

SD ルーティングデバイスからソフトウェアイメージを削除するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択します。
2. [WAN Edge]、[Controller]、[vManage] のいずれかをクリックします。
3. ソフトウェアイメージを削除するデバイスを 1 つ以上選択します。
4. [Delete Available Software] をクリックします。

   [Delete Available Software] ダイアログボックスが開きます。
5. 削除するソフトウェアバージョンを選択します。
6. [Delete] をクリックします。

ソフトウェア アップグレード アクティビティ ログの表示

1. Cisco SD-WAN Manager のツールバーからタスクアイコンをクリックします。

   Cisco SD-WAN Manager には、実行中のすべてのタスクのリストが、成功と失敗の合計数とともに表示されます。

2. 矢印アイコンをクリックして、タスクの詳細を表示します。Cisco SD-WAN Manager ではステータスウィンドウが開き、タスクのステータスとタスクが実行されたデバイスの詳細が表示されます。

Cisco SD-WAN Manager を使用したデバイスのモニタリング

[Monitor] ウィンドウは、 Cisco SD ルーティングデバイスのすべてのモニタリングコンポーネントとサービスの統合ビューに対応した単一ページのリアルタイムのユーザーインターフェイスを提供します。次のオプションを使用して接続を確立し、デバイスをモニタリングできます。

- SSH ターミナル
- ping
- traceroute

また、圧縮された .tar ファイルでシステムステータス情報を収集できます。Cisco SD-WAN Manager は、デバイスから ,tar ファイルを取得してダウンロードできます。ファイルを取得した後、デバイス上のファイルのコピーを削除して、ディスク領域を解放できます。

SD ルーティングモードを有効にすると、この機能はデバイスと Cisco SD-WAN Manager でデフォルトで有効になります。

SSH を使用したデバイスのモニタリング

SSH オプションを使用して接続を確立し、デバイスをモニタリングするには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから [Monitor] > [Devices] の順に選択します。
ステップ 2 表示されるデバイスのリストからデバイスを選択します。
ステップ 3 単一デバイスの場合は、目的のデバイスで **[. .]** をクリックして、[SSH Terminal] を選択します。

（または）

ステップ 4 Cisco SD-WAN Manage のメニューから、[Tools] > [SSH Terminal] の順に選択します。
ステップ 5 端末でパスワードを 2 回入力し（SD ルーティングと同じ）、デバイスとの接続を確立します。
ステップ 6 端末から **show** コマンドを実行して、デバイスをモニタリングします。

デバイスに対する ping の実行

デバイスに対して ping を実行するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから [Monitor] > [Devices] の順に選択します。
ステップ 2 表示されるデバイスのリストからデバイスを選択します。
ステップ 3 単一デバイスの場合は、目的のデバイスで **[. .]** をクリックして、[Ping] を選択します。
ステップ 4 [Monitor] ページで宛先 IP アドレスを入力します。
ステップ 5 [Ping] をクリックします。

ping の結果が下のウィンドウに出力されます。

ルートのトレース

トレースルートオプションを使用して、接続を確立した後にデバイスをモニタリングするには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから [Monitor] > [Devices] の順に選択します。
ステップ 2 表示されるデバイスのリストからデバイスを選択します。
ステップ 3 単一デバイスの場合は、目的のデバイスで **[. .]** をクリックして、[Trace Route] を選択します。
ステップ 4 [Trace Route] ページで、宛先 IP アドレスを入力します。
ステップ 5 [Start] ボタンをクリックして、トレースを開始します。

アラームおよびイベント

オーバーレイネットワーク内の個々のデバイスでイベントが発生すると、デバイスは Cisco SD-WAN Manager に通知を送信してそれを報告します。Cisco SD-WAN Manager は、イベント通知をフィルタリングし、関連するイベントを関連付け、やや重大なイベントと重大なイベントをアラームに統合します。

[Alarms] 画面では、オーバーレイネットワーク内の SD ルーティングデバイスによって生成されたアラームに関する詳細情報を表示できます。

アラームとイベントのモニタリング

上部のバーにあるベルアイコンをクリックすると、Cisco SD-WAN Manager ダッシュボードからアラームを表示できます。アラームは、アクティブアラームまたはクリア済みアラームにグ

ループ化されています。デフォルトでは、過去 24 時間のアラームが表示されます。または、次の手順に従って、Cisco SD-WAN Manager の [Alarms] 画面からアラームを表示します。

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

ステップ 2 Cisco SD-WAN Manager のメニューから [Monitor] > [Alarms] の順に選択します。

アラームはグラフィック形式と表形式で表示されます。

ステップ 3 特定のアラームの詳細を表示するには、目的のアラームで […] をクリックしてから、[Alarm Details] をクリックします。

[Alarm Details] ウィンドウが開き、アラームの考えられる原因、影響を受けるエンティティなどの詳細が表示されます。

admin-techファイル

admin-tech ファイルがデバイスで利用可能な場合、いつでも生成された admin-tech ファイルを表示できます。

生成された admin-tech ファイルのリストを表示し、SD ルーティングデバイスから Cisco SD-WAN Manager にコピーするファイルを決定できます。その後、選択した admin-tech ファイルをローカルデバイスにダウンロードするか、ダウンロードした admin-tech ファイルを Cisco SD-WAN Manager、デバイス、またはその両方から削除できます。

Cisco SD-WAN Manager を使用した admin-tech ファイルの要求

admin-tech ファイルは、特定の問題のトラブルシューティングに使用される一連のシステムステータス情報です。admin-tech ファイルを要求するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから [Tools] > [Operational Commands] の順に選択します。

ステップ 2 単一デバイスの場合は、目的のデバイスで **[. .]** をクリックし、[Generate Admin Tech] を選択します。

ステップ 3 必要に応じて [Generate admin-tech File] ウィンドウで、admin-tech tar ファイルの内容を制限します。

a) デフォルトでは、[Include Logs] チェックボックスがオンになっています。圧縮された tar ファイルからログファイルを除外するには、このチェックボックスをオフにします。

b) コアファイルを含めるには、[Include Cores] チェックボックスをオンにします。

（注） コアファイルは、ローカルデバイスの *bootflash:/core* または *harddisk:/core* ディレクトリに保存されます。

c) デバイスプロセス（デーモン）、メモリの詳細、およびオペレーションに関連するファイルを含めるには、[Include Tech] チェックボックスをオンにします。

ステップ 4 [Generate] をクリックします。

Cisco SD-WAN Manager が admin-tech ファイルを作成します。ファイル名の形式は、*hostname-date-time-admin-tech.tar.gz* です。

ステップ 5 生成された admin-tech ファイルを表示するには、Cisco SD-WAN Manager のメニューから [Tools] > [Operational Commands] > [Show Admin Tech List] の順に選択します。

CLI を使用した admin-tech ファイルの要求

CLI を使用して admin-tech ファイルを要求するには、次の手順を実行します。

admin-tech ファイルを生成するには、**request tech-support** コマンドを使用します。

```
Device#request tech-support
21:03:46.447 UTC Thu Aug 10 2023 : Collecting 'show tech-support'...
21:04:51.880 UTC Thu Aug 10 2023 : 'show tech-support' collected successfully!
21:04:55.091 UTC Thu Aug 10 2023 : Collecting binary traces...
21:04:55.216 UTC Thu Aug 10 2023 : Binary traces collected successfully!
21:04:55.219 UTC Thu Aug 10 2023 : Collecting platform-dependent files...
21:05:43.467 UTC Thu Aug 10 2023 : Platform-dependent files collected successfully!
21:05:43.475 UTC Thu Aug 10 2023 : Generating tech-support bundle...
21:05:56.648 UTC Thu Aug 10 2023 : Tech-support bundle file
bootflash:core/1HX-2017-debug_bundle_20230810-210346-UTC.tar.gz [size: 8648 KB]
21:05:56.648 UTC Thu Aug 10 2023 : Tech-support bundle generated successfully!

1HX-2017#
1HX-2017#dir bootflash:core
Directory of bootflash:/core/

1471682  -rw-                1  Aug 11 2023 04:26:51 +00:00  .callhome
45       -rw-            25429  Aug 10 2023 21:05:56 +00:00
1HX-2017_RP_0-debug_bundle_20230810-210346-UTC-info.txt
49       -rw-          8854997  Aug 10 2023 21:05:54 +00:00
1HX-2017-debug_bundle_20230810-210346-UTC.tar.gz
1471685  drwx             4096  Mar 22 2021 20:03:54 +00:00  modules

29633794048 bytes total (16795193344 bytes free)
1HX-2017#
```

リアルタイムデータのモニタリング

デバイスに対して ping を実行するには、次の手順を実行します。

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

ステップ 2 表示されるデバイスのリストからデバイスを選択します。

ステップ 3 単一デバイスの場合は、目的のデバイスで **[. .]** をクリックして、[Real Time] を選択します。

ステップ 4 [Device Options] ドロップダウンリストからデータのカテゴリを選択します。

結果が表示されます。

設定例

ここでは、設定例を紹介します。

例：Cisco SD-WAN Manager での制御接続の有効化

Cisco SD-WAN Manager で制御接続を有効にする例を以下に示します。

```
(config) sd-routing
(config-sd-routing) system-ip  172.16.255.15
(config-sd-routing) organization-name viptela
(config-sd-routing) vbond ip 10.0.12.26
(config-sd-routing) site-id 500
(config-sd-routing) wan-interface GigabitEthernet2
```

例：制御接続の有効化の確認

接続ステータスを確認するには、**show platform software yang-management process state** コマンドを使用します。

```
Device#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
```

vdaemon のステータスを確認するには、**show platform software yang-management process list r0 name vdaemon** コマンドを使用します。

```
Device#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
```

例：ルート証明書のインストール

ルート証明書をインストールする例を以下に示します。

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

例：ルート証明書のインストールの確認

ルート証明書のインストールステータスを確認するには、**show sd-routing local-properties summary** コマンドを使用します。

```
Device#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

Device#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                        vbond
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
```

トラブルシューティング

ここでは、Cisco SD-WAN Manager を使用して SD ルーティングデバイスを管理およびモニタリングする際に発生する一般的な問題のトラブルシューティングに使用できるコマンドについて説明します。

- **Show version**

（注） 動作モードは **show version** コマンドに含まれています。

```
When sd-routing feature is enabled:
Device#show version | include mode
Router operating mode: Autonomous (SD-Routing)
Device#

When sd-routing feature is not enabled:
Device#show version | include mode
Router operating mode: Autonomous
Device#
```

- **show platform software yang-management process state**
- **show sd-routing system status**
- **show sd-routing connections summary**
- **show platform software process list r0 name vdaemon**
- **show sd-routing local-properties summary**
- **show sd-routing local-properties wan ipv4**
- **show sd-routing local-properties vbond**
- **show sd-routing connections history**

Cisco SD-WAN Manager を使用した SD ルーティングデバイスの管理に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *2 : Cisco SD-WAN Manager* を使用した *SD* ルーティングデバイスに関する機能情報

機能名	リリース	機能情報
Cisco SD-WAN Manager を使用した SD ルーティングデバイスの管理	Cisco IOS XE リリース 17.12.1a	この機能を使用すると、Cisco SD-WAN Manager を使用して SD ルーティングデバイスの管理操作を実行できます。単一のネットワーク管理システム（Cisco SD-WAN Manager）を使用してすべての SD ルーティングデバイスをモニタリングできるため、ソリューションの導入が簡素化されます。

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。