



Cisco Catalyst SD-WAN スタートアップガイド

最終更新：2025 年 9 月 1 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019–2025 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	最初にお読みください	1
第 2 章	Cisco IOS XE (SD-WAN) および Cisco Catalyst SD-WAN リリースにおける新機能	3
第 3 章	Cisco Catalyst SD-WAN ソリューション	5
	Cisco Catalyst SD-WAN ソリューション	5
	Cisco Catalyst SD-WAN ソリューション	5
	Cisco Catalyst SD-WAN ソリューションの必要性	5
	従来のネットワーク設計における課題	6
	Cisco Catalyst SD-WAN ソリューション	6
	仮想 IP ファブリック	8
	Cisco Catalyst SD-WAN のコンポーネント	15
	Cisco Catalyst SD-WAN の主要コンポーネント	15
	Cisco Catalyst SD-WAN Manager	16
	Cisco Catalyst SD-WAN コントローラ	17
	Cisco Catalyst SD-WAN Validator	19
	Cisco vEdge デバイス および Cisco IOS XE Catalyst SD-WAN デバイス	20
	Cisco Catalyst SD-WAN 制御接続	22
	Cisco Catalyst SD-WAN 制御接続に関する情報	22
	Cisco Catalyst SD-WAN 制御接続の TLS 1.3 の利点	23
	Cisco Catalyst SD-WAN 制御接続の確認	23
	Cisco Catalyst SD-WAN ソリューション	26
	Cloud onRamp for SaaS	27
	Cisco Catalyst SD-WAN Analytics	27

Cisco Catalyst SD-WAN ポータル	28
Cisco SD-AVC	29
Cisco Catalyst SD-WAN との連携	29
Cisco vEdge デバイス を使用した基本的なオーバーレイネットワークの構築	29
Cisco Catalyst SD-WAN に関する用語	34
ドメイン ID	35
OMP ルート	35
サイト ID	36
システム IP アドレス	36
TLOC	37
その他の情報	37

第 4 章

ハードウェアとソフトウェアの設置	39
サーバー推奨事項	40
モジュールの追加または削除後の Cisco IOS XE Catalyst SD-WAN デバイス のデバイス設定 のリセット	40
Cisco Catalyst SD-WAN デバイスのオンサイト ブートストラップ プロセス	41
SHA2 エンタープライズ証明書を使用した Cisco vEdge 5000 のオンサイト ブートストラップ プロセス	44
CLI を使用した Cisco IOS XE Catalyst SD-WAN デバイス のブートストラップファイルの生成	50
ワンタッチプロビジョニング：汎用ブートストラップ構成を使用した Cisco IOS XE Catalyst SD-WAN デバイス のオンボード	52
Cisco SD-AVC のインストール（Cisco vManage 20.1.1 以前）	57
Cisco SD-WAN Manager での SD-AVC の有効化	58
Cisco IOS XE Catalyst SD-WAN デバイス での SD-AVC の有効化	59
Cisco SD-AVC のインストール（Cisco vManage リリース 20.3.1 以降）	60
Cisco SD-AVC、Cisco vManage リリース 20.3.1 以降の有効化	60
Cisco IOS XE Catalyst SD-WAN デバイス での SD-AVC の有効化	61
Cisco SD-AVC Cloud Connector、Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降の有 効化	63

Cisco Catalyst SD-WAN Manager リリース 20.13.x を使用する Cisco SD-AVC Cloud Connector の有効化	64
クラウドサービスの有効化	73
Cisco IOS XE ルータのソフトウェアのインストールとアップグレード	74
は始める前に	74
Cisco IOS XE SD-WAN リリース 16.12 以前の Cisco IOS XE Catalyst SD-WAN ソフトウェア のダウンロード	76
Cisco IOS XE SD-WAN リリース 16.12 以前の Cisco IOS XE Catalyst SD-WAN ソフトウェア のインストール	77
CLI を使用した IOS XE ルータの設定	80
IOS XE デバイスのプラグアンドプレイポータルへの追加	82
ROMMON のアップグレードまたはダウングレード	83
工場出荷時の状態へのリセット	84
デフォルトパスワードの復元	85
vEdge ルータのソフトウェアのインストールとアップグレード	85
ソフトウェアイメージの署名	86
ソフトウェアバージョンの互換性	86
ソフトウェアのインストール	86
ソフトウェアのアップグレード	87
ソフトウェアアップグレードのベストプラクティス	88
Cisco Catalyst SD-WAN からのソフトウェアイメージの取得	90
リポジトリへの新しいソフトウェアイメージの追加	91
ソフトウェアイメージのアップグレード	92
新しいソフトウェアイメージのアクティブ化	93
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	93
CLI からのソフトウェアイメージのアップグレード	94
冗長ソフトウェアイメージ	95
Cisco vEdge デバイス の古いソフトウェアイメージへのダウングレード	95
Cisco Catalyst SD-WAN Manager をホストしている仮想マシンでのメモリおよび vCPU リソー スのアップグレード	96
セカンダリディスクサイズの拡大 (Cisco Catalyst SD-WAN Manager リリース 20.12.x 以前)	98

Cisco IOS XE Catalyst SD-WAN デバイスのソフトウェア メンテナンス アップグレード	99
ソフトウェア メンテナンス アップグレードについて	99
ソフトウェア メンテナンス アップグレードでサポートされるデバイス	101
ソフトウェア メンテナンス アップグレード イメージの管理	101
CLI を使用したソフトウェア メンテナンス アップグレード イメージの管理	103
ソフトウェア メンテナンス アップグレード イメージのステータスの検証	105

第 5 章

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のインストールとアップグレード 109

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のインストールおよびアップグレード	110
コントローラモードでサポートされるプラットフォーム	111
Cisco IOS XE イメージの互換性	112
アップグレードの考慮事項	112
機能制限	114
自己署名済みトラストポイント	115
自律モードとコントローラモードの概要	115
Cisco IOS XE ルータのソフトウェアのインストール	116
Cisco IOS XE リリース 17.2.1r 以降のソフトウェアのダウンロード	116
Cisco ASR、Cisco ISR および Cisco ENCS プラットフォームでのソフトウェアのインストール	116
Cisco CSR 1000v プラットフォームでのソフトウェアのインストール	116
Cisco Catalyst 8000V Edge ソフトウェア プラットフォームのインストール	117
Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のリリースでのプラグアンドプレイ	118
プラグアンドプレイのオンボーディング ワークフロー	118
プラグ アンド プレイ オンボーディングによるモードの検出	119
IP アドレスの自動検出	120
PnP 以外のオンボーディング	122
Cisco Catalyst SD-WAN ブートストラップ設定ファイルの作成	122
新規インストール：モード変更デバイスのデイズゼロシナリオ	122
Cisco CLI を使用したモードの切り替え	123
デバイスのコントローラモードへの変更	124

ブートストラップファイルによるモード検出とモード変更	126
コントローラモード設定のリセット	128
モードスイッチング：追加情報	130
モード切り替え中の設定の永続性	130
コントローラモードと自律モードの検証	130
コントローラモードのコマンド出力の表示	130
自律モードでの show コマンド出力	131
インストール後のコンソールポートアクセスの変更（コントローラモード）	132
Cisco IOS XE リリース 17.2.1r 以降へのアップグレード	134
サポートされるアップグレード	134
Cisco Catalyst SD-WAN を使用したアップグレード	136
CLI を使用したアップグレード	136
Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のリリースからのダウングレード	138
Cisco IOS XE Catalyst SD-WAN デバイスの以前にインストールされたソフトウェアイメージへのダウングレード	138
Cisco IOS XE Catalyst SD-WAN デバイスの古いソフトウェアイメージへのダウングレード	139
Cisco IOS XE リリース 17.2.x のダウングレードシナリオ	140
スマートライセンスとスマートライセンス予約の復元	140
スマートライセンスの復元	141
スマートライセンス予約の復元	141
クラウドサービスによってホストされる Cisco Catalyst 8000V Edge ソフトウェアのオンボード（PAYG ライセンスを使用）	141
Cisco Catalyst 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	143
トラブルシューティング	145
ソフトウェアインストールのトラブルシューティング	145
ブート後にルータが以前のソフトウェアバージョンをロードする	145
第 6 章	
Cisco Catalyst SD-WAN オーバーレイネットワークの起動プロセス	147
ネットワークオーバーレイの起動	147
Cisco SD-WAN Manager ペルソナおよびストレージデバイス	148
稼働イベントシーケンス	149

オーバーレイネットワークの起動手順	152
稼働シーケンスのユーザー部分の概要	155
起動シーケンスの自動部分	158
ZTP 自動認証プロセスに必要なユーザー入力	159
Cisco Catalyst SD-WAN コントローラ と Cisco Catalyst SD-WAN Validator の間の認証	160
Cisco Catalyst SD-WAN コントローラ 間の認証	163
Cisco Catalyst SD-WAN Validator と Cisco vEdge ルータの間の認証	167
Cisco vEdge ルータ と Cisco SD-WAN Manager 間の認証	171
Cisco Catalyst SD-WAN コントローラ と Cisco vEdge ルータの間の認証	173
Cisco Catalyst SD-WAN 展開のためのファイアウォールポート	177
Cisco Catalyst SD-WAN 固有のポートの用語	177
ポートオフセット	177
ポートホッピング	178
ポートホッピングの効果	180
Cisco vEdge デバイス が使用するポート	180
複数の vCPU を実行している Cisco Catalyst SD-WAN デバイスで使用されるポート	182
Cisco SD-WAN Manager によって使用される管理ポート	183
ポートオフセットの設定	184
ポートホッピングの手動実行	184
ソフトウェアのダウンロード	185
Cisco SD-WAN Manager の導入	186
ESXi での Cisco Catalyst SD-WAN Manager VM インスタンスの作成	187
vSphere クライアントの起動および Cisco Catalyst SD-WAN Manager VM インスタンスの作成	187
新しい仮想ディスクの作成	188
vNIC の追加	188
Cisco Catalyst SD-WAN Manager コンソール への Cisco Catalyst SD-WAN Manager VM インスタンスの接続	189
KVM での Cisco Catalyst SD-WAN Manager VM インスタンスの作成	190
KVM ハイパーバイザでの Cisco Catalyst SD-WAN Manager VM インスタンスの作成	190
Cisco Catalyst SD-WAN Manager インスタンスへの接続	192

Cisco Catalyst SD-WAN Manager の設定	192
証明書の設定	196
Cisco Catalyst SD-WAN Manager 証明書の生成	196
Cisco Catalyst SD-WAN Manager クラスタの作成	196
Cisco SD-WAN Manager クライアントセッションのタイムアウト値の有効化	197
Cisco Catalyst SD-WAN Validator の導入	197
ESXi での Cisco Catalyst SD-WAN Validator VM インスタンスの作成	198
vSphere クライアントの起動および Cisco Catalyst SD-WAN Validator VM インスタンスの作成	198
トンネルインターフェイス用の vNIC の追加	199
Cisco Catalyst SD-WAN Validator VM インスタンスの起動とコンソールへの接続	199
KVM での Cisco Catalyst SD-WAN Validator VM インスタンスの作成	200
Cisco Catalyst SD-WAN Validator の設定	201
Cisco Catalyst SD-WAN Validator の構成テンプレートの作成	205
設定要件	205
Cisco Catalyst SD-WAN Validator の機能テンプレート	206
機能テンプレートの作成	206
デバイステンプレートの作成	207
Cisco Catalyst SD-WAN Validator へのデバイステンプレートのアタッチ	209
オーバーレイネットワークへの Cisco Catalyst SD-WAN Validator の追加	210
エンタープライズ ZTP サーバーの起動	210
ZTP の要件	211
ルータを ZTP サーバーに設定する	213
vContainer ホスト	215
Cisco Catalyst SD-WAN コントローラ の導入	215
ESXi での Cisco Catalyst SD-WAN コントローラ VM インスタンスの作成	216
vSphere クライアントの起動および Cisco Catalyst SD-WAN コントローラ VM インスタンスの作成	217
管理インターフェイス用の vNIC の追加	217
Cisco Catalyst SD-WAN コントローラ VM インスタンスの起動とコンソールへの接続	218
KVM での Cisco Catalyst SD-WAN コントローラ VM インスタンスの作成	218

Cisco Catalyst SD-WAN コントローラ の設定	219
Cisco Catalyst SD-WAN コントローラ の構成テンプレートの作成	225
設定要件	225
Cisco Catalyst SD-WAN コントローラ の機能テンプレート	225
機能テンプレートの作成	226
デバイステンプレートの作成	227
Cisco SD-WAN コントローラ へのデバイステンプレートのアタッチ	229
オーバーレイネットワークへの Cisco Catalyst SD-WAN コントローラ の追加	229
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	231
注意事項と制限事項	232
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	232
Alibaba Cloud への Cisco Catalyst 8000V Edge ソフトウェア の展開	232
機能	232
Cisco Catalyst 8000V インスタンスの要件	233
Cisco Catalyst SD-WAN に接続するための Cisco Catalyst 8000V インスタンスの設定	233
Cisco Catalyst SD-WAN 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	233
vEdge クラウドルータ の展開	234
AWS での vEdge クラウドルータ VM インスタンスの作成	235
Azure での vEdge クラウドルータ VM インスタンスの作成	241
ESXi での vEdge Cloud VM インスタンスの作成	244
KVM での vEdge Cloud VM インスタンスの作成	248
WAN エッジルータの証明書認証設定の設定	251
vEdge Cloud ルータへの署名付き証明書のインストール	251
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	260
ルータ認定シリアル番号ファイルのアップロード方法	261
vEdge ルータの設定	264
WAN エッジルータからのデータストリーム収集の有効化	274
ZTP 用にルータを準備する	275

Quick Connect ワークフロー	282
Quick Connect ワークフローを使用するための前提条件	282
Quick Connect ワークフローの制約事項	283
Quick Connect について	284
Quick Connect ワークフローの概要	284
自動同期を使用したデバイスのアップロード	284
デバイスの手動アップロード	286
Quick Connect ワークフローへのアクセス	287

第 8 章

クラスタの管理 289

クラスタ管理に関する情報	289
Cisco Catalyst SD-WAN Manager クラスタのガイドライン	290
利用可能なクラスタサービスの表示	292
Cisco Catalyst SD-WAN Manager サーバーのクラスタ IP アドレスの設定	292
Cisco Catalyst SD-WAN Manager サーバーのクラスタへの追加	294
Cisco Catalyst SD-WAN Manager サービスの詳細の表示	298
Cisco Catalyst SD-WAN Manager パラメータの編集	299
設定データベースのログイン情報の更新	299
Cisco Catalyst SD-WAN Manager のダウングレード	301
Cisco SD-WAN Manager クラスタのアップグレード	301
クラスタのアップグレードに関する情報	302
クラスタのアップグレードの前提条件	303
CLI を使用したクラスタのアップグレード	304
Cisco Catalyst SD-WAN Manager プロセスの手動再起動	306
クラスタからの Cisco Catalyst SD-WAN Manager ノードの削除	308

第 9 章

証明書の管理 311

Cisco Catalyst SD-WAN Manager での証明書の管理	311
WAN Edge ルータ証明書ステータスの確認	313
WAN Edge ルータの検証	313
WAN エッジルータのステージング	313

WAN エッジルータの無効化	314
コントローラのシリアル番号を Cisco Catalyst SD-WAN Validator に送信する	314
署名付き証明書のインストール	315
ルート証明書のエクスポート	315
証明書署名要求の表示	316
デバイス証明書署名要求の表示	316
証明書の表示	317
証明書署名要求の生成	317
コントローラ証明書署名要求の生成	317
機能証明書署名要求の生成	317
WAN エッジデバイス証明書署名要求の生成	318
RSA キーペアのリセット	318
制御コンポーネントの無効化	319
認定アクティビティログの表示	319
署名付き証明書の表示	319
証明書の失効	320
証明書の失効に関する情報	320
証明書の失効に関する制約事項	321
証明書の失効の設定	321
Cisco SD-WAN Manager を使用した Cisco IOS XE Catalyst SD-WAN デバイス へのサードパー ティ CA 証明書の設定	322
Cisco SD-WAN Manager を使用した CA 証明書の設定に関する情報	322
CA 証明書のアップロードでサポートされるデバイス	323
CA 証明書を設定するための前提条件	323
CA 証明書のアップロードの制約事項	323
CA 証明書のアップロード	323
Cisco SD-WAN Manager を使用した CA 証明書の設定	324
CA 証明書の取り消し	325
CA 証明書の更新	325
CA 証明書と PKI トラストポイントの監視	326
CRLベースの検疫	327

CRL ベースの検疫に関する情報	327
CRL ベースの検疫の制限	328
CRLベースの検疫の構成	328
Cisco Catalyst SD-WAN Manager でのルート認証局証明書の管理	329
ルート証明機関証明書の追加	329
ルート認証局証明書の表示	330
ルート証明書の削除	330
エンタープライズ証明書	330
Cisco SD-WAN コントローラ のエンタープライズ証明書の設定	332
エンタープライズ証明書に関する情報	332
エンタープライズ証明書の OU フィールドへの依存関係	333
エンタープライズ証明書をサポートするデバイス	334
エンタープライズ証明書の設定	334
デバイス証明書の無効化	338
エンタープライズルート証明書のコントローラ証明書の承認	338
ブートストラップ構成の生成	339
Cisco PKI コントローラの証明書	340
使用例：ソフトウェアバージョン 19.x 以降によるシスコがホストするクラウドのオーバーレイ	341
ユースケース：証明書更新時の DigiCert 証明書から Cisco PKI コントローラ証明書へのアクティブな既存オーバーレイの移行	343
使用例：オンプレミスコントローラでの CSR の送信と証明書のダウンロード	347
Cisco SD-WAN Manager の Web サーバー証明書	348

第 10 章

期限切れのエンタープライズ証明書の表示と検疫	351
期限切れの証明書の表示と検疫	351
期限切れの証明書の表示と検疫について	352
証明書が期限切れのデバイスの検疫の有効化	353
期限切れ証明書の検疫におけるデバイスの表示と修復	353

第 11 章

リバースプロキシ	355

リバースプロキシ	355
リバースプロキシについて	355
プライベートネットワークとパブリックインターネット接続の両方によるデバイスのサ ポート	357
リバースプロキシに関する制約事項	358
リバースプロキシでの証明書のプロビジョニング	359
Cisco SD-WAN Manager を使用したリバースプロキシの設定	360
リバースプロキシの設定	360
Cisco SD-WAN コントローラでのリバースプロキシの設定	361
リバースプロキシの無効化	362
CLI を使用したリバースプロキシの監視	362
CLI を使用したリバースプロキシの監視	366

第 12 章

モジュラ型 Cisco ASR 1000 シリーズインターフェイスのオンボーディング	371
Cisco ASR 1006-X と RP3 モジュール	371
RP3 モジュールを搭載した Cisco ASR 1006-X に関する情報	371
ハードウェア構成	372
ROM モニタ ソフトウェア バージョン	374
オンボーディング ワークフロー	374
Cisco ASR 1006-X シャーシの RMA 交換	374
Cisco RP3 モジュールの RMA 交換	378

第 13 章

API クロスサイト リクエスト フォージェリの防止	383
Cisco Catalyst SD-WAN REST API トークンベース認証	383
トークンの使用	384
API ドキュメント	384
サードパーティ製アプリケーションのユーザー	384

第 14 章

Microsoft Azure への Cisco SD-WAN コントローラ の展開	389
Azure での Cisco SD-WAN コントローラの展開に関する情報	389
Cisco SD-WAN コントローラを Azure に展開する利点	390

Azure で Cisco SD-WAN コントローラ を展開するための前提条件	390
Azure に Cisco SD-WAN コントローラ を展開するユースケース	391
Azure での Cisco SD-WAN コントローラ の展開：タスク	391
タスク 1：Azure でのコントローライメージの作成	391
タスク 2：Azure での仮想ネットワーク、サブネット、およびネットワーク セキュリティグループの作成	392
タスク 3：コントローラの仮想マシンの作成	394
タスク 4：ネットワーク セキュリティ グループの設定	396
Azure での Cisco SD-WAN コントローラの展開の確認	397
Azure での Cisco SD-WAN コントローラ の展開の監視	398

第 15 章

AWS クラウドでの Cisco SD-WAN コントローラ の展開	399
AWS での Cisco SD-WAN コントローラの展開について	399
AWS で Cisco SD-WAN コントローラ を展開する利点	401
AWS で Cisco SD-WAN コントローラ を展開するための前提条件	401
AWS に Cisco SD-WAN コントローラ を展開するユースケース	401
AWS での Cisco SD-WAN コントローラ の展開：タスク	402
タスク 1：AWS AMI イメージのリクエスト	402
タスク 2：AWS で VPC、サブネット、およびセキュリティグループを作成する	402
タスク 3：コントローラの仮想マシンの作成	404
タスク 4：セキュリティグループの設定	406
AWS での Cisco SD-WAN コントローラの展開の確認	407
AWS での Cisco Catalyst SD-WAN コントローラ の展開の監視	408

第 16 章

Cisco Catalyst SD-WAN ソリューションのトラブルシューティング	409
概要	409
サポート記事	409
フィードバックのリクエスト	412
免責事項と注意事項	412

第 17 章

付録：Cisco Catalyst SD-WAN Manager How-To マニュアル	413

Cisco Catalyst SD-WAN Manager の RESTful API	413
vEdge ルータの交換	416
Cisco IOS XE Catalyst SD-WAN デバイス の交換	418
異なるサーバーでの Cisco Catalyst SD-WAN Manager の使用	421
Cisco Catalyst SD-WAN Manager Web アプリケーションサーバーへのログイン	422



第 1 章

最初にお読みください



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

参考資料

- [Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations](#) [英語]
- [Cisco Catalyst SD-WAN Device Compatibility](#) [英語]

ユーザーマニュアル

- [User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17](#) [英語]
- [User Documentation for Cisco SD-WAN Release 20](#) [英語]

通信、サービス、およびその他の情報

- [Cisco Profile Manager](#) で、シスコの E メールニュースレターおよびその他の情報にサインアップしてください。
- ネットワーク運用の信頼性を高めるための最新のテクニカルサービス、アドバンストサービス、リモートサービスについては、[シスコサービス](#) にアクセスしてください。

- 安全かつ検証されたエンタープライズクラスのアプリケーション、製品、ソリューション、サービスをお求めの場合は、[Cisco DevNet](#) にアクセスしてください。
- Cisco Press 出版社による一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。
- リリースで未解決および解決済みのバグをご覧になる場合は、[Cisco Bug Search Tool](#) にアクセスしてください。
- サービス リクエストを送信するには、[シスコサポート](#) にアクセスしてください。

マニュアルに関するフィードバック

シスコのテクニカルマニュアルに関するフィードバックを提供するには、それぞれのオンラインマニュアルの右側のペインにあるフィードバックフォームを使用してください。



第 2 章

Cisco IOS XE (SD-WAN) および Cisco Catalyst SD-WAN リリースにおける新機能

シスコでは、リリースごとに Cisco Catalyst SD-WAN ソリューションを継続的に強化しています。また、コンテンツも最新の強化に合致したものとなるように努めています。次のリンクには、コンフィギュレーションガイド、コマンドリファレンスガイド、およびハードウェア設置ガイドに記載されているリリースごとの新機能と変更された機能が含まれています。Cisco Catalyst SD-WAN ソリューションに関する追加機能と修正については、リリースノートの「解決されたバグおよび未解決のバグ」セクションを参照してください。

[What's New in Cisco IOS XE Catalyst SD-WAN Release 17.x](#) [英語]

[What's New in Cisco IOS XE Catalyst SD-WAN Release 16.x](#) [英語]

[What's New in Cisco SD-WAN \(vEdge\) Release 20.x](#) [英語]

[What's New in Cisco SD-WAN \(vEdge\) Release 19.x](#) [英語]



第 3 章

Cisco Catalyst SD-WAN ソリューション

- [Cisco Catalyst SD-WAN ソリューション \(5 ページ\)](#)
- [Cisco Catalyst SD-WAN ソリューション \(5 ページ\)](#)
- [Cisco Catalyst SD-WAN のコンポーネント \(15 ページ\)](#)
- [Cisco Catalyst SD-WAN との連携 \(29 ページ\)](#)

Cisco Catalyst SD-WAN ソリューション

表 1:機能の履歴

機能名	リリース情報	機能説明
Cisco Catalyst SD-WAN 制御接続の TLS 1.3 プロトコルのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a Cisco Catalyst SD-WAN Manager リリース 20.13.1	この機能は、Cisco Catalyst SD-WAN 制御接続の Transport Layer Security (TLS) 1.3 プロトコルのサポートを追加します。

Cisco Catalyst SD-WAN ソリューション

Cisco Catalyst SD-WAN ソリューションの必要性

従来のネットワークテクノロジーは、ますます高価で複雑になってきており、現代のマルチサイト企業のニーズに合わせて拡張することができません。Cisco Catalyst SD-WAN ソリューションは、実績のあるネットワークの要素に基づいており、エンタープライズネットワークの運用コストを削減する洗練されたソフトウェアベースのソリューションを提供し、複数の場所と地域にまたがって分散した大規模で複雑なネットワークのプロビジョニングと管理を簡素化する簡単なツールを提供します。Cisco Catalyst SD-WAN ソリューションには、ネットワークとそのデータトラフィックの安全性とプライバシーを確保する固有の認証およびセキュリティプロセスが組み込まれています。

Cisco Catalyst SD-WAN ソリューションは、古いハードウェアベースのモデルから、安全なソフトウェアベースの仮想IPファブリックにネットワークが進化したことを表しています。オーバーレイネットワークとも呼ばれる Cisco Catalyst SD-WAN ファブリックは、パブリックインターネット、MPLS、ブロードバンドなどの標準ネットワークトランスポートサービス上で実行されるソフトウェアオーバーレイを形成します。オーバーレイネットワークは、次世代のソフトウェアサービスもサポートしているため、クラウドネットワーキングへの移行が促進されます。

従来のネットワーク設計における課題

ネットワーク設計に対する従来のアプローチでは、次の4つの根本的原因により、現代のニーズに合わせて拡張できません。

- **コスト**：従来のネットワークはルータやスイッチなどの高価なハードウェア上で動作し、時間のかかる設定とメンテナンスが必要です。さらに、これらのネットワークでは、ネットワークを保護してセグメント化するために、高価なトランスポート接続またはキャリア回線が必要です。
- **複雑性**：従来のネットワークは古いモデルの分散型コントロールプレーンで動作します。つまり、ネットワーク内のすべてのノードにルーティングとセキュリティルールを設定する必要があります。リモートサイトの管理、変更管理、およびネットワークのメンテナンスは、ロジスティクス上の主要な課題となっています。
- **設置に長い時間がかかる**：専用のキャリア回線で動作する従来のネットワークでは、新しい回線の設置がキャリアに依存しており、数ヵ月かかる場合があります。これにより、新しいブランチの立ち上げが大幅に遅れる可能性があります。
- **制御**：キャリア回線で動作する従来のネットワークは、ネットワーク設計から設定、監視に至るまで、ISP に対する制御を犠牲にしています。ISP から変更を要求すると、余分な時間がかかり、通信エラーが発生しやすくなります。

次のような現代の要件に直面すると、従来のネットワークのコストと複雑性はさらに高まります。

- 徹底したエンドツーエンドのセキュリティ
- 個別のトランスポート ネットワーク
- 複数のデータセンターでホストされる高帯域幅のクラウドアプリケーション
- モバイルエンドユーザーの人数の継続的な増加
- 流体トポロジ経由の Any-to-Any 接続
- 特定のビジネスに固有のニーズ

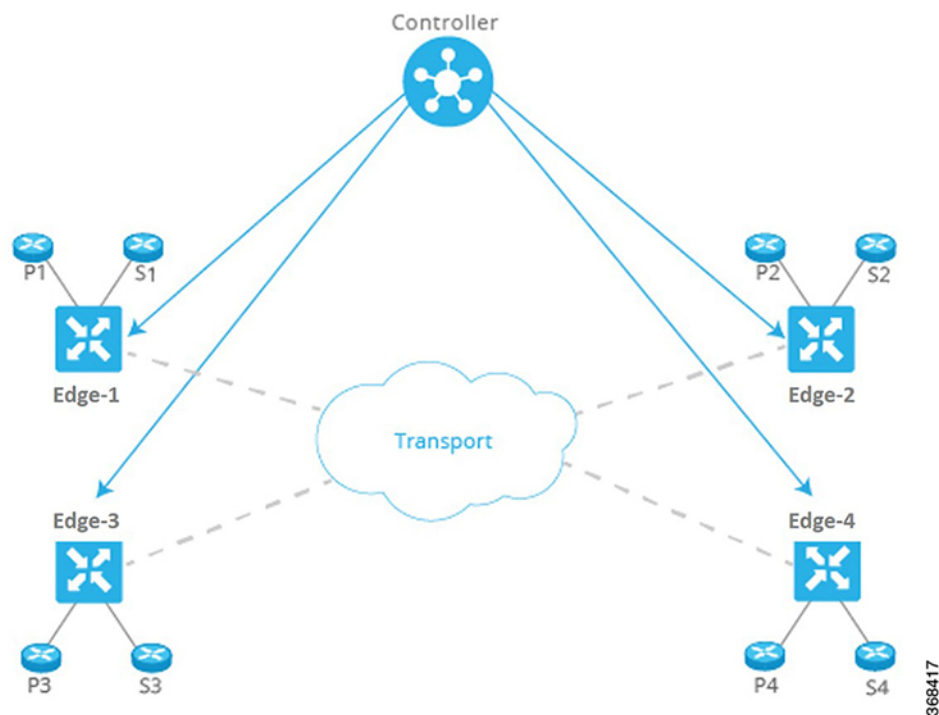
Cisco Catalyst SD-WAN ソリューション

Cisco Catalyst SD-WAN ソリューションは、ソフトウェア定義型 WAN (SD-WAN) です。すべての SD-WAN と同様に、1990 年代と 2000 年代にインターネットの拡張を可能にしたものと同

じルーティング原則に基づいています。Cisco Catalyst SD-WAN が他の SD-WAN と異なる点は、WAN を新世代のエンタープライズ ネットワークに合わせて再解釈し、データプレーンをコントロールプレーンから分離し、それまでは専用ハードウェアを必要としていたルーティングの多くを仮想化したことです。

仮想化されたネットワークは、物理ルータまたは仮想デバイスのいずれであっても、費用対効果の高いハードウェアのオーバーレイとして動作します。Cisco SD-WAN Validator と呼ばれる集中型コントローラは、ファブリックのコントロールプレーンを監視し、Cisco Catalyst SD-WAN オーバーレイネットワーク全体のプロビジョニング、メンテナンス、セキュリティを効率的に管理します。Cisco SD-WAN Validator と呼ばれる別のデバイスは、Cisco Catalyst SD-WAN オーバーレイネットワークに参加するときに、他のすべての Cisco vEdge デバイスを自動的に認証します。

図 1: Cisco Catalyst SD-WAN ソリューションのコンポーネント



この分業により、ネットワークレイヤーはそれぞれが最も得意とすることに集中できます。コントロールプレーンはオーバーレイネットワークを介したトラフィックのルーティングルールを管理し、データプレーンは実際のデータパケットをネットワークデバイスに渡します。コントロールプレーンとデータプレーンは、柔軟で堅牢なファブリックの縦糸と横糸となり、ニーズとスケジュールに従って、既存の回路に織り込むことができます。

Cisco SD-WAN Manager は、オーバーレイネットワーク内のすべてのデバイスのネットワークパフォーマンスを集中監視ステーションから監視するための、シンプルでありながら強力なグラフィカルダッシュボードのセットを提供します。また、Cisco SD-WAN Manager では、ソフトウェアのインストール、アップグレード、プロビジョニングも一元化され、単一のデバイスでも複数のデバイスでも一括で処理できます。

Cisco Catalyst SD-WANはクラウドネットワーキングのニーズに最適です。Cisco Catalyst SD-WAN 仮想 IP ファブリックは、クラウドネットワーキングを合理化および最適化するソフトウェア サービスをサポートし、個々のクラウドアプリケーションのオーバーレイネットワークの機能を最大限に活用できるようにします。



(注)

- Cisco SD-WAN コントローラは専用のカスタムスタックです。オープンソースの Linux コンポーネントが使用されていますが、当社のカスタム オペレーティング システム スタックは、使用されているオープンソースの Linux コンポーネントとは類似していません。Linux コンポーネントは、それらが使用されるカスタム オペレーティング システム スタックと同じ強化要件の対象ではありません。
- Cisco SD-WAN コントローラではルートアクセスが無効になっており、ユーザースペースからアクセスできません。
- 当社はFedRAMP、FIPS、CCなどのコンプライアンス基準と要件を満たしています。このコンプライアンスは、当社のオペレーティングシステムのセキュリティ検証の証拠であると見なされます。
- 当社は[こちら](#)で概説されている安全な開発ライフサイクルに準拠しています。
- また、Cisco Product Security Incident Response Team (PSIRT) によって実行される明確に定義されたプロセスに従って、CVEなどの新しいエクスプロイトや攻撃に対処しています。
- Cisco SD-WAN コントローラのプラットフォームのセキュリティについて引き続き懸念がある場合は、サードパーティを通じて、独立したペネトレーションテストを実施することをお勧めします。

仮想 IP ファブリック

従来のエンタープライズ ネットワークの複雑さは、次の3つの主な原因に起因します。

- データトラフィックを交換するエンティティと、それらのエンティティを結合するトランスポートネットワークの間に明確な区別はありません。つまり、ネットワークのサービス側にあるホスト、デバイス、サーバー間、およびネットワークのトランスポート側にあるルータ間の相互接続は明確に区別されていません。
- ポリシーと制御の判断は、エンタープライズネットワーク全体のすべてのホップに組み込まれています。
- セキュリティは時間のかかる手動の作業であり、ネットワーク内のすべてのノードで、または集中型セキュリティサーバーを使用してセキュリティサーバーを管理することによって、セキュリティ管理を実装する必要があります。

Cisco Catalyst SD-WAN は、実績のあるネットワーク要素を革新的な方法で使用して、安全な仮想 IP ファブリックを構築します。ネットワーク要素には次のものが含まれます。

- ルーティングおよびルーティングアドバタイズメントを使用して、ネットワーク全体のトラフィックフローを確立および維持します。
- レイヤ3セグメンテーション（仮想ルーティングおよび転送（VRF）と呼ばれることもある）はトラフィックのさまざまなフローを分離します。これは、企業内のさまざまなお客様やビジネス組織のトラフィックを分離するのに役立ちます。
- プロトコルエンティティのペア間の双方向接続を設定および維持するためのピアツーピアの概念
- 認証および暗号化
- ルーティングとデータトラフィックのポリシー

Cisco Catalyst SD-WAN 仮想 IP ファブリックでは、5つの簡単なステップで、複雑な従来のネットワークが管理しやすいスケーラブルなネットワークに変換されます。

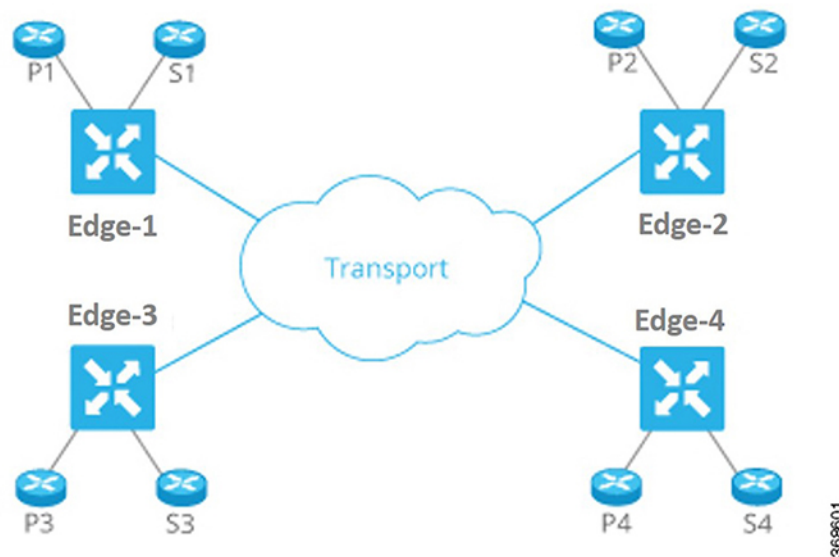
- ステップ1：ネットワークのサービス側からトランスポートを分離する
- ステップ2：ルーティングインテリジェンスを一元化し、セグメンテーションを有効にする
- ステップ3：ネットワークを自動的に保護する
- ステップ4：一元化されたポリシーを通じて到達可能性に影響を与える
- ステップ5：オーケストレーションとプロビジョニングを簡素化する

ステップ1：ネットワークのサービス側からトランスポートを分離する

トランスポートネットワークの役割は、トランスポートルータ間でパケットを運ぶことです。トランスポートネットワークは、次のホップまたは宛先ルータに到達するために通過するルータのみ認識している必要があります。非トランスポートルータ（ローカルサービスネットワーク内のトランスポートルータの背後にあるルータ）のプレフィックスを認識する必要はありません。

ネットワークトランスポートをネットワークのサービス側から分離することにより、ネットワーク管理者は、ユーザー間またはホスト間の通信とは無関係に、ルータ間通信に影響を与えることができます。

図 2: サービスネットワークから分離された転送ネットワーク



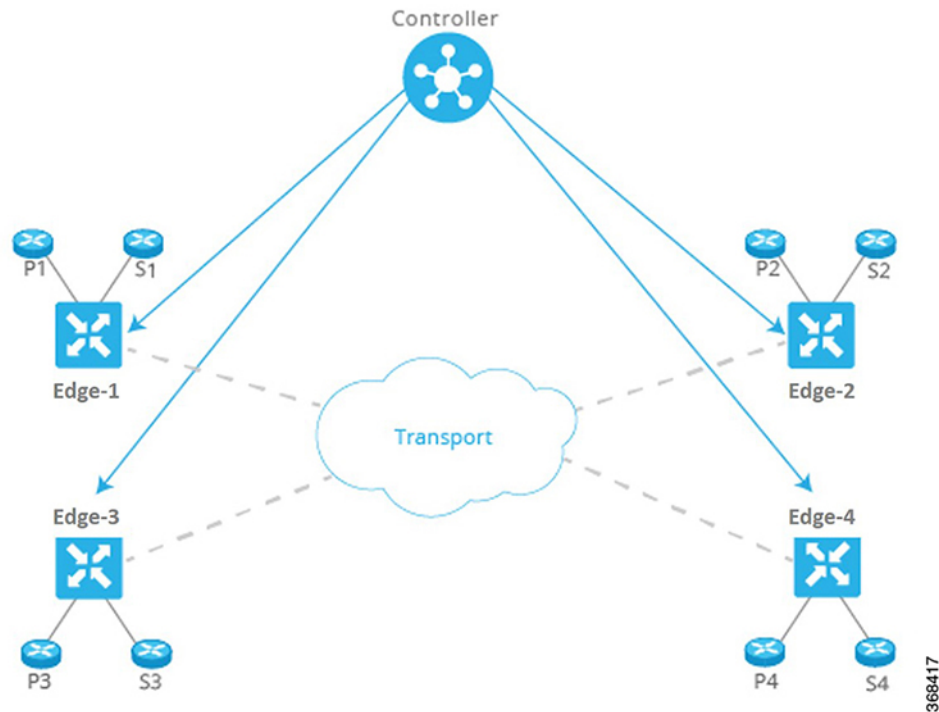
このアプローチには多くの利点があります。

- ネットワーク管理者は、SLA とコストに基づいてトランスポート回線を選択できます。
- ルーティングシステムは、最適なルーティング、ロードバランシング、およびポリシーベースのルーティングのために、属性をトランスポートリンクに割り当てることができます。

ステップ 2: ルーティング インテリジェンスを一元化し、セグメンテーションを有効にする

ネットワークのエッジにあるすべてのルータには、ルーティング用の 2 つの側があります。1 つはトランスポートネットワーク向けで、もう 1 つはネットワークのサービス側です。すべてのルータ間で Any-to-Any 通信を行うには、すべてのルータがすべてのプレフィックスを学習する必要があります。伝統的に、ルータは、フルメッシュ IGP/BGP を使用するか、オーバーレイトンネルでルーティングを有効にすることで、プレフィックスを学習します（MPLS または GRE を介した BGP または IGP など）。BGP にルートリフレクタを使用するなど、さまざまな手法により、フルメッシュルーティング隣接関係に関連する拡張性の問題を軽減または排除できます。

図 3: 集中型コントローラによるルーティング インテリジェンスの集中化



Cisco Catalyst SD-WAN ファブリックは、ルーティング インテリジェンスを一元化することにより、ルートリフレクタモデルに基づいて構築されます。基本的に、ルータのサービス側から学習したプレフィックスはすべて中央のコントローラにアドバタイズされてから、ネットワークのコントロールプレーンを介して他のルータに情報が反映されます。コントローラはデータトラフィックを一切処理しません。データトラフィックはコントロールプレーン通信にのみ関係します。

このアプローチには多くの利点があります。

- 集中型コントローラは、コントロールプレーンの処理に安価なサーバーや市販のサーバーを使用できます。
- ルータには既成のシリコンを使用できるため、規模の経済によるコストメリットを得られます。
- ネットワークのトランスポート側でのフルメッシュルーティングに関連する拡張性の問題が解消されます。
- ネットワーク管理者は、複雑なシグナリングプロトコルを使用せずに、複数のセグメントを作成できます。たとえば、この図では、すべての Px プレフィックスを 1 つの VPN の一部にし、すべての Sx プレフィックスを別の VPN の一部にできます。



- (注) 集中型コントローラは、ルータのルーティングにのみ「影響」を与えます。コントローラは、ネットワークを通過するすべてのフローに参加したり、サービス側のルーティングに参加したりしません。この設計により、ルータはローカルインテリジェンス（ローカルサイトの決定を迅速に行うのに十分なインテリジェンス）を得ることができます。

ステップ 3：ネットワークとリンクを自動的に保護する

Cisco Catalyst SD-WAN ファブリックは、トランスポート側のリンクを識別し、サイト間のトラフィックを自動的に暗号化します。関連付けられた暗号化キーは、集中型コントローラとのセキュアなセッションを介して交換されます。コントローラとのセキュアなセッションは、RSA と証明書インフラストラクチャを使用して自動的に設定されます。

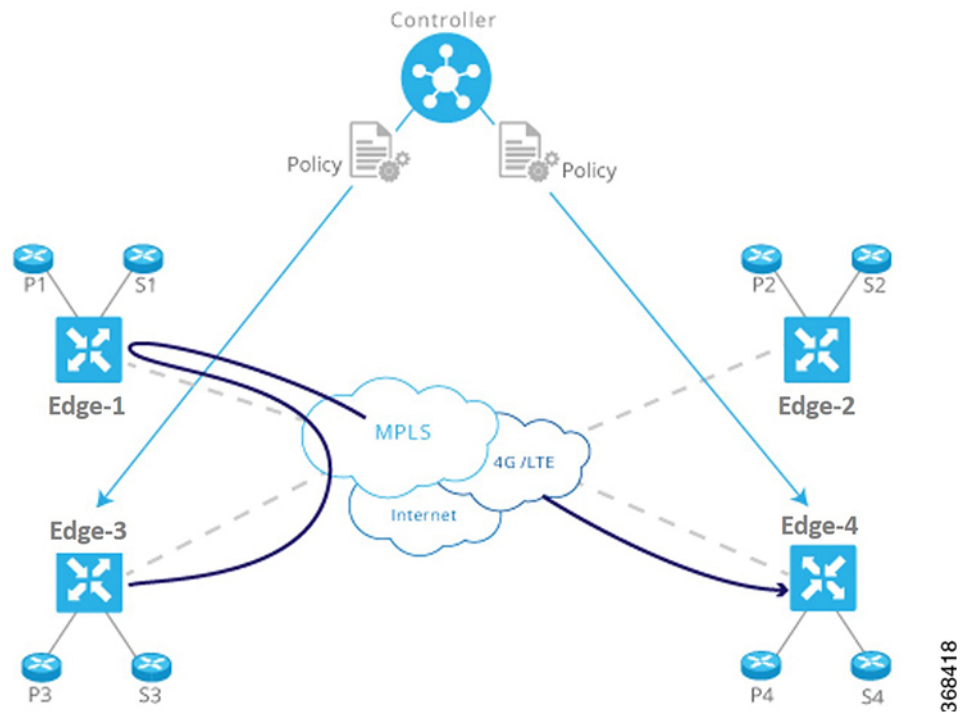
このアプローチには多くの利点があります。

- Cisco Catalyst SD-WAN ファブリック自体が、ネットワークに参加しているすべてのデバイスを認証します。これは、インフラストラクチャを保護するための重要なステップです。
- ファブリックは、トランスポートリンクに関連する暗号化キーを自動的に交換するため、多数のペアワイズキーを設定する必要がなくなります。
- ファブリックにより、ネットワークはトランスポート側からの攻撃を受けにくくなります。

ステップ 4：一元化されたポリシーを通じて到達可能性に影響を与える

集中型コントローラに設定されたポリシーは、ルータ間でプレフィックスがアドバタイズされる方法に大きく影響します。たとえば、この図のルータ P3 と P4 間のすべてのトラフィックがルータ vEdge-1 で U ターンする必要がある場合、ネットワーク管理者は集中型コントローラに単純なルートポリシーを適用できます。その後、コントローラが影響を受けるエッジルータにポリシーを渡します。ネットワーク管理者は、ルータごとにポリシーをプロビジョニングする必要はありません。

図 4:集中型コントローラで設定されたポリシー



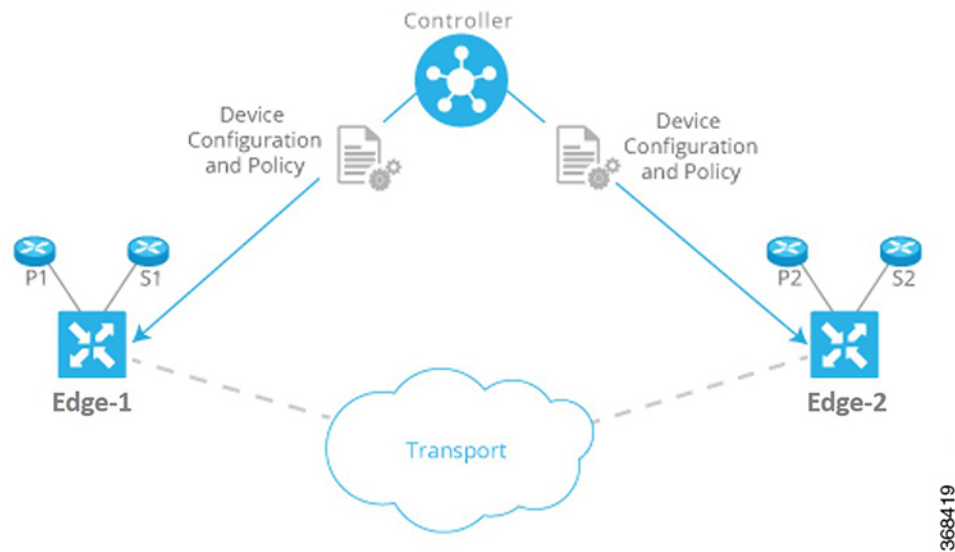
このアプローチには多くの利点があります。

- コントローラは、アクセス制御、つまり、VPN内で相互に通信できるプレフィックスに集中的に影響を与えます。
- コントローラは、SLAまたはその他の属性に基づいてトランスポートリンクの選択に影響を与えることにより、ユーザーエクスペリエンスを最適化します。ネットワーク管理者は、トランスポートリンクに色（ゴールドやブロンズなど）を付け、アプリケーションがその色を適切なトランスポートリンクにマッピングするようにできます。
- ネットワーク管理者は、一元化されたポイントからビジネスロジックをマッピングできます。
- ネットワークは、リスクの高い国からのトラフィックをすべて中間地点を経由してルーティングするなど、計画的または予期しない状況に迅速に対応できます。
- ネットワークは、ファイアウォール、IDP、IDSなどのサービスを一元化できます。ネットワーク管理者は、これらのサービスをすべてのブランチやキャンパスのネットワーク全体に分散させる代わりに、機能を一元化して、規模の効率性を達成し、プロビジョニングのタッチポイント数を最小限に抑えることができます。

ステップ 5：プロビジョニングと管理を簡素化する

従来のネットワークデバイスは、CLI を介して手動でプロビジョニングおよび監視されます。ネットワーク管理者は、ステータス情報を取得して読み取るために、構成を 1 行ずつ入力し、個々のデバイスで一度に 1 つずつ操作コマンドを入力する必要があります。この方法は、ネットワークのプロビジョニングとトラブルシューティングの際にエラーが発生しやすく、時間がかかります。また、デバイスが遠隔地にある場合や管理ポートにアクセスできない場合は、深刻な問題が発生する可能性があります。

図 5: Cisco Catalyst SD-WAN によるネットワークの簡素化されたプロビジョニングと管理



Cisco Catalyst SD-WAN は、Cisco SD-WAN Manager を介して、プロビジョニングと管理を一元化して大幅に簡素化します。Cisco SD-WAN Manager 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 とリンクを監視、設定、および維持できる使いやすいグラフィカルダッシュボードを提供します。たとえば、GUI ダッシュボードには、サービスのプロビジョニングを容易にするさまざまな構成のテンプレートビューが用意されているため、すべての一般的な要素（AAA サーバーや企業固有のサーバーなど）を 1 回のクリックで複数のデバイスに 1 か所からプッシュできます。

このアプローチには多くの利点があります。

- ネットワーク管理者は、個々のデバイスを一度に 1 つずつ処理する断片的なアプローチとは対照的に、ネットワーク全体を効率的かつ簡単にプロビジョニングおよび管理できます。
- ネットワーク管理者は、1 か所からネットワークの可視性（ネットワーク全体の VPN 統計の表示など）を改善できます。
- トラブルシューティングタスクは簡素化され、視覚的に表示されます。ネットワーク管理者は、個々のデバイスから長い構成や出力を読み取る必要がありません。

Cisco Catalyst SD-WAN のコンポーネント

Cisco Catalyst SD-WAN の主要コンポーネント

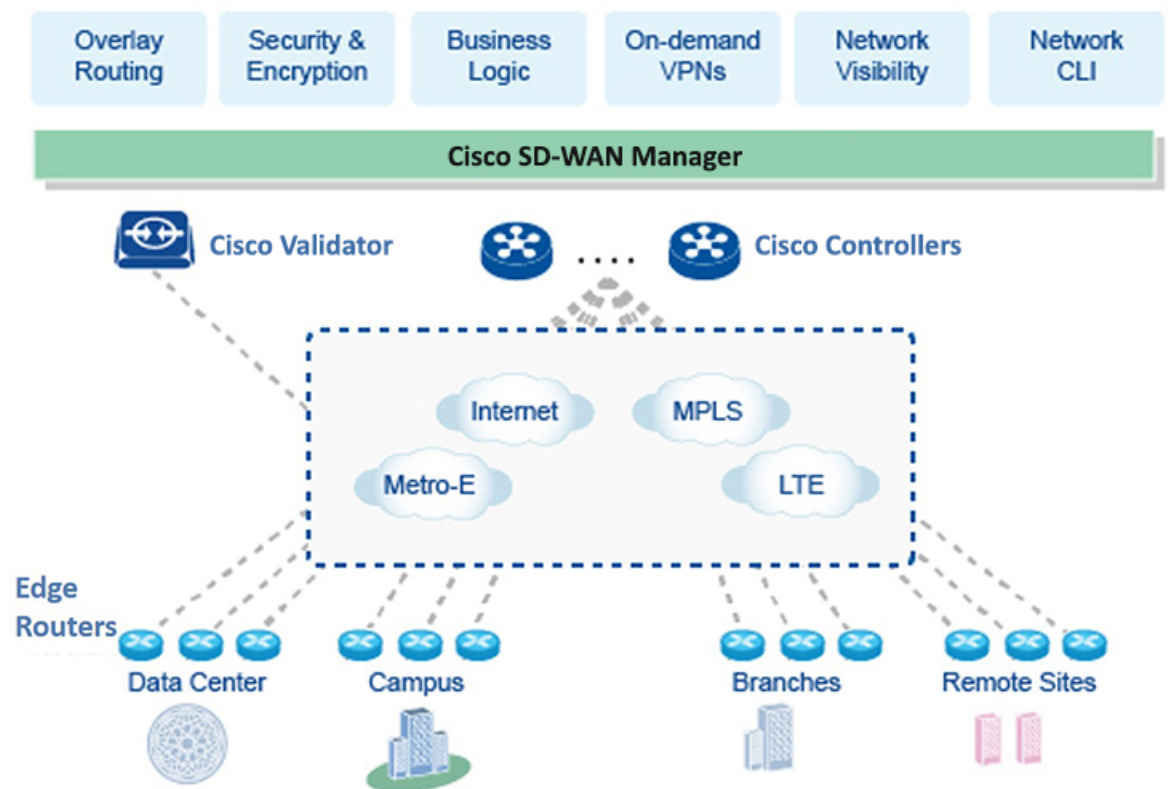
Cisco Catalyst SD-WAN のセキュアな仮想 IP ファブリックは、次の 4 つの基本的なコンポーネントで構成されています。

- **Cisco SD-WAN Manager** : Cisco SD-WAN Manager は、シンプルなグラフィカルダッシュボードからオーバーレイネットワーク全体の設定と管理を可能にする中央集中型のネットワーク管理システムです。
- **Cisco SD-WAN コントローラ** : Cisco SD-WAN コントローラ は Cisco Catalyst SD-WAN ソリューションの中心的な要素であり、ネットワーク全体のデータトラフィックの流れを制御します。Cisco SD-WAN コントローラ は Cisco SD-WAN Validator と連携して、Cisco vEdge デバイスがネットワークに参加するときに認証し、エッジルータ間の接続を調整します。
- **Cisco SD-WAN Validator** : Cisco SD-WAN Validator は、エッジルータと Cisco SD-WAN コントローラ の間の接続を自動的に調整します。任意のエッジルータまたは Cisco SD-WAN コントローラ コントローラが NAT の背後にある場合、Cisco SD-WAN Validator は最初の NAT トラバーサル オーケストレータとしても機能します。
- **Cisco IOS XE Catalyst SD-WAN および Cisco vEdge デバイス** : エッジルータはサイトの境界（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）に配置され、サイト間の接続を提供します。これらは、ハードウェアデバイスまたは仮想マシンとして実行されるソフトウェア（クラウドルータ）のいずれかです。エッジルータは、データトラフィックの送信を処理します。

これら 4 つのコンポーネントのうち、エッジルータは Cisco Catalyst SD-WAN ハードウェアデバイスまたは仮想マシンとして実行されるソフトウェアであり、残りの 3 つのコンポーネントはソフトウェアのみのコンポーネントです。クラウドルータ、Cisco SD-WAN Manager および Cisco SD-WAN コントローラ ソフトウェアはサーバー上で実行され、Cisco SD-WAN Validator ソフトウェアはエッジルータ上でプロセス（デーモン）として実行されます。

下の図は、Cisco Catalyst SD-WAN のコンポーネントを示しています。以下のセクションでは、各コンポーネントについて詳しく説明します。

図 6: のコンポーネント Cisco Catalyst SD-WAN



368420

Cisco Catalyst SD-WAN Manager

Cisco SD-WAN Manager は集中ネットワーク管理システムです。Cisco SD-WAN Manager ダッシュボードは、ネットワークへの視覚的なウィンドウを提供し、Cisco エッジネットワークデバイスを設定および管理できます。Cisco SD-WAN Manager ソフトウェアは、ネットワーク内のサーバー上で実行されます。このサーバーは通常、データセンターなどの一元化された場所にあります。Cisco SD-WAN Manager ソフトウェアは、Cisco SD-WAN コントローラソフトウェアと同じ物理サーバー上で実行できます。

Cisco SD-WAN Manager を使用すると、証明書のクレデンシャルを保存したり、すべての Cisco エッジ ネットワーク コンポーネントの設定を作成および保存したりできます。これらのコンポーネントがネットワークでオンラインになると、Cisco SD-WAN Manager から証明書と設定を要求します。Cisco SD-WAN Manager がこれらの要求を受信すると、証明書と設定を Cisco エッジ ネットワーク デバイスにプッシュします。

クラウドルータの場合、Cisco SD-WAN Manager は証明書に署名してブートストラップ設定を生成することもでき、デバイスをデコミッションすることもできます。

vmanage-admin アカウントによるデバイスおよびコントローラとのセキュアな通信

Cisco SD-WAN Manager は、Datagram Transport Layer Security (DTLS) トンネルまたは Transport Layer Security (TLS) トンネルのいずれかのセキュアチャネルを使用して、エッジデバイスおよびコントローラと通信します。このセキュアチャネル内で、SSH セッション内で NETCONF プロトコルを使用してデバイスまたはコントローラと通信します。デバイスまたはコントローラで内部使用専用のパスワードレス「vmanage-admin」ユーザーアカウントを使用します。vmanage-admin アカウントは、デバイスまたはコントローラの初期セットアップ時に作成されます。Cisco SD-WAN Manager は、このセキュアチャネルを使用して、次の各項目をモニタリング、設定、および管理します。

- エッジデバイス
- クラスタ内の Cisco SD-WAN Manager ノード
- Cisco SD-WAN Validator
- Cisco SD-WAN コントローラについて

前述のように、vmanage-admin ユーザーアカウントにはパスワードが関連付けられていないため、Cisco SD-WAN Manager はパスワードなしの手順を使用してアカウントにログインします。これを実現するために、Cisco SD-WAN Manager は非対称暗号化の公開キーと秘密キーのペアを生成します。Cisco Catalyst SD-WAN ファブリックまたはコントローラインスタンスへのエッジデバイスの展開中に、Cisco SD-WAN Manager は、生成した公開キーをエッジデバイスまたはインスタンスにコピーします。セキュアチャネル (DTLS または TLS トンネル) 内で、独自のプロトコルを使用して公開キーを送信します。

Cisco SD-WAN Manager が vmanage-admin アカウントを使用して実行するアクティビティは、syslog メッセージおよび特定の **show** コマンドの出力に表示されます。syslog メッセージは、他のユーザーアカウントを介して実行されたアクティビティと同じレベルの詳細でログに記録されます。syslog の詳細レベルは、デバイスの syslog 設定によって異なります。

Cisco SD-WAN Manager では、デバイスをモニター、設定、および管理するために、ファブリック内のデバイスの vmanage-admin アカウントが必要です。デバイスでこのアカウントを削除、無効化、または変更すると、Cisco SD-WAN Manager がこれらのアクティビティを実行できなくなるので、サポートされていません。

Cisco Catalyst SD-WAN コントローラ

Cisco SD-WAN コントローラ は、Cisco Catalyst SD-WAN オーバーレイネットワークのコントロールプレーンを監視し、Cisco Catalyst SD-WAN ファブリックを形成する接続を確立、調整、および維持します。

Cisco SD-WAN コントローラ の主要なコンポーネントは次のとおりです。

- コントロールプレーン接続：それぞれの Cisco SD-WAN コントローラ がオーバーレイネットワーク内の各エッジルータとのコントロールプレーン接続を確立および維持します（複数の Cisco SD-WAN コントローラ があるネットワークでは、ロードバランシングのために、単一の Cisco SD-WAN コントローラ がエッジルータのサブセットのみに接続している場合があります。）DTLS トンネルとして実行される各接続は、デバイス認証が成功した

後に確立され、Cisco SD-WAN コントローラ とエッジルータの間で暗号化されたペイロードを伝送します。このペイロードは、Cisco SD-WAN コントローラ がネットワークトポロジを決定し、ネットワークの宛先への最適なルートを計算し、このルート情報をエッジルータに配布するために必要なルート情報で構成されます。Cisco SD-WAN コントローラ とエッジルータ間の DTLS 接続は、永続的な接続です。Cisco SD-WAN コントローラ には、サービス側でエッジルータが接続されているデバイスとの直接のピアリング関係はありません。

- **OMP（オーバーレイ管理プロトコル）**：OMP プロトコルは、Cisco Catalyst SD-WAN オーバーレイネットワークを管理する BGP に似たルーティングプロトコルです。OMP は DTLS コントロールプレーン接続内で実行され、オーバーレイネットワークの確立と維持に必要なルート、ネクストホップ、キー、およびポリシー情報を伝送します。OMP は Cisco SD-WAN コントローラ とエッジルータの間で実行され、コントロールプレーン情報のみを伝送します。Cisco SD-WAN コントローラ はルートを処理し、これらのルートから学習した到達可能性情報をオーバーレイネットワーク内の他のエッジルータにアドバタイズします。
- **認証**：Cisco SD-WAN コントローラ には、オンラインになったすべての新しいエッジルータを認証できるクレデンシャルが事前にインストールされています。これらのクレデンシャルにより、認証されたデバイスのみがネットワークにアクセスできるようになります。
- **キーリフレクション**：Cisco SD-WAN コントローラ は、エッジルータからデータプレーンキーを受信し、データプレーンのトラフィックを送信する必要がある他の関連するエッジルータにそれらを反映します。
- **ポリシーエンジン**：Cisco SD-WAN コントローラ は、ルーティング情報、アクセス制御、セグメンテーション、エクストラネット、およびサービスチェイニングを操作するための豊富なインバウンド/アウトバウンドポリシー構成を提供します。
- **Netconf と CLI**：Netconf は、Cisco SD-WAN コントローラ をプロビジョニングするために Cisco SD-WAN Manager によって使用される標準ベースのプロトコルです。さらに、各 Cisco SD-WAN コントローラ がローカル CLI アクセスと AAA を提供します。

Cisco SD-WAN コントローラ は、エッジルータおよび Cisco Catalyst SD-WAN オーバーレイネットワーク内の他の Cisco SD-WAN コントローラ から学習した OMP ルートと呼ばれるルート情報を格納する、集中型ルートテーブルを維持します。Cisco SD-WAN コントローラ は、設定されたポリシーに基づいて、このルート情報をネットワーク内の Cisco エッジネットワークデバイスと共有して、相互に通信できるようにします。

Cisco SD-WAN コントローラ は、ESXi または VMware ハイパーバイザソフトウェアで設定されたサーバー上で仮想マシンとして実行されるソフトウェアです。Cisco SD-WAN コントローラ ソフトウェアイメージは、Cisco Catalyst SD-WAN Web サイトからダウンロード可能な署名付きイメージです。すべての Cisco SD-WAN コントローラ ソフトウェアイメージには、単一の Root of Trust（信頼の基点）となる Cisco Catalyst SD-WAN 公開証明書が埋め込まれています。

Cisco SD-WAN コントローラ の初回起動時に、コントローラと Cisco SD-WAN Validator の IP アドレスなどの最小限の設定情報を入力します。Cisco SD-WAN コントローラ は、この情報と

信頼の基点のパブリック証明書を使用して、ネットワーク上で自身を認証し、Cisco SD-WAN Validator との DTLS 制御接続を確立し、ドメインに存在する場合は完全な設定を Cisco SD-WAN Manager から受信してアクティブ化します（または、設定ファイルを手動でダウンロードするか、コンソール接続を介して Cisco SD-WAN コントローラ で直接設定を作成できます）。これで、Cisco SD-WAN コントローラ でもドメイン内のエッジルータからの接続を受け入れる準備ができました。

冗長性と高可用性を提供するために、一般的なオーバーレイネットワークには、各ドメインに複数の Cisco SD-WAN コントローラ が含まれています。ドメインには最大 20 の Cisco SD-WAN コントローラ を含めることができます。OMP ネットワークルートの同期を維持するには、すべての Cisco SD-WAN コントローラ でポリシーと OMP の設定を同じにする必要があります。ただし、インターフェイスの場所とアドレス、システム ID、ホスト名など、デバイス固有の情報の設定は異なっても構いません。冗長な Cisco SD-WAN コントローラ を持つネットワークでは、Cisco SD-WAN Validator は Cisco SD-WAN コントローラ にお互いについての情報を伝え、ドメイン内のどのエッジルータからの制御接続を受け入れる必要があるかをそれぞれの Cisco SD-WAN コントローラ に伝えます（ロードバランシングを提供するために、同じドメイン内の異なるエッジルータは、異なる Cisco SD-WAN コントローラ に接続します）。1 つの Cisco SD-WAN コントローラ が使用できなくなった場合、他のコントローラ がオーバーレイネットワークの機能を自動的にかつ即座に維持します。

Cisco Catalyst SD-WAN Validator

Cisco SD-WAN Validator は、Cisco SD-WAN コントローラ とエッジルータの初期起動を自動的に調整し、Cisco SD-WAN コントローラ とエッジルータ間の接続を容易にします。立ち上げプロセス中に、Cisco SD-WAN Validator はオーバーレイネットワークへの参加を希望するデバイスを認証および検証します。この自動オーケストレーションプロセスにより、面倒でエラーが発生しやすい手動での起動を行う必要がなくなります。

Cisco SD-WAN Validator は、パブリックアドレス空間にある唯一の Cisco vEdge デバイスです。この設計により、Cisco SD-WAN Validator は Cisco SD-WAN コントローラ および NAT デバイスの背後にあるエッジルータと通信でき、Cisco SD-WAN Validator はこれらの Cisco vEdge デバイスの NAT トラバーサルの問題を解決できます。

Cisco SD-WAN Validator の主要なコンポーネントは次のとおりです。

- **コントロールプレーン接続**：それぞれの Cisco SD-WAN Validator に、ドメイン内のそれぞれの Cisco Catalyst SD-WAN コントローラ との DTLS トンネル形式の永続的なコントロールプレーン接続があります。さらに、Cisco SD-WAN Validator は DTLS 接続を使用して、エッジルータがオンラインになったときにそれらと通信し、ルータを認証し、ルータがネットワークに参加できるようにします。エッジルータの基本認証は、証明書と RSA 暗号化を使用して行われます。
- **NAT トラバーサル**：Cisco SD-WAN Validator は、エッジルータと Cisco SD-WAN コントローラ の一方または両方が NAT デバイスの背後にある場合に、それらの間の最初のオーケストレーションを促進します。このオーケストレーションを促進するために、標準のピアツーピア技術が使用されます。

- ロードバランシング：Cisco SD-WAN コントローラ が複数あるドメインでは、ルータがオンラインになると、Cisco SD-WAN Validator は Cisco SD-WAN コントローラ を介してエッジルータのロードバランシングを自動的に実行します。

Cisco SD-WAN Validator は、オーバーレイネットワーク内の Cisco SD-WAN コントローラ とエッジルータを認証し、それらの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が必要な Cisco vEdge デバイス はこれだけです）。

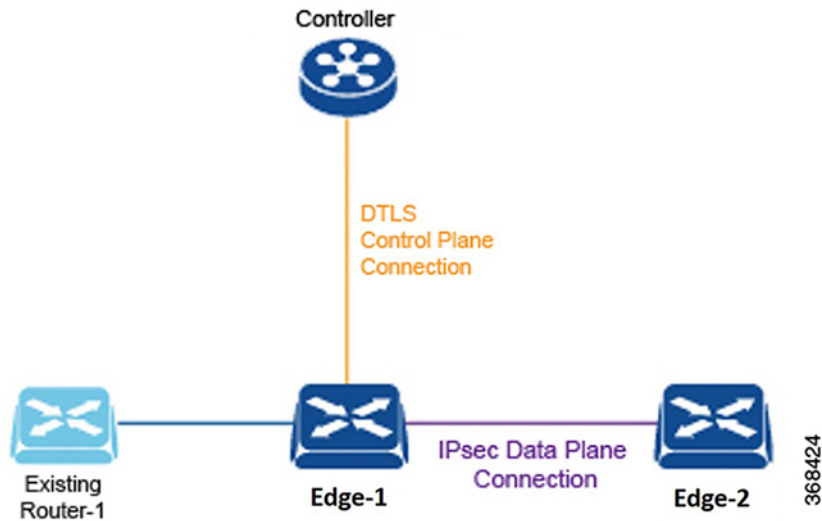
Cisco SD-WAN Validator は、Cisco SD-WAN コントローラ とエッジルータ間の初期制御接続のオーケストレーションを行います。Cisco SD-WAN コントローラ およびエッジルータへの DTLS トンネルを作成して、コントロールプレーン接続を要求している各ノードを認証します。この認証動作により、有効な顧客ノードのみが Cisco Catalyst SD-WAN オーバーレイネットワークに参加できることが保証されます。Cisco SD-WAN コントローラ との DTLS 接続は永続的であるため、エッジルータがネットワークに参加すると Cisco SD-WAN Validator コントローラ は Cisco SD-WAN コントローラ に通知できます。エッジルータとの DTLS 接続は一時的なものであるため、Cisco SD-WAN Validator がエッジルータを Cisco Catalyst SD-WAN コントローラ と一致させた後は、Cisco SD-WAN Validator とエッジルータが相互に通信する必要はなくなります。Cisco SD-WAN Validator は、コントロールプレーン接続に必要な情報のみを共有し、適切なエッジルータと Cisco SD-WAN コントローラ に対して、相互に安全な接続を開始するように指示します。Cisco SD-WAN Validator では状態は保持されません。

Cisco SD-WAN Validator に冗長性を提供するために、ネットワークに複数の Cisco SD-WAN Validator エンティティを作成し、すべてのエッジルータをそれらの Cisco SD-WAN Validator に向けることができます。それぞれの Cisco SD-WAN Validator は、ネットワーク内のそれぞれの Cisco Catalyst SD-WAN コントローラ と永続的な DTLS 接続を維持します。1 つの Cisco SD-WAN Validator が使用できなくなった場合、他のネットワークは自動的および即座にオーバーレイネットワークの機能を維持できます。複数の Cisco SD-WAN コントローラ があるドメインでは、Cisco SD-WAN Validator はエッジルータと Cisco SD-WAN コントローラ のいずれかをペアにして、ロードバランシングを提供します。

Cisco vEdge デバイス および Cisco IOS XE Catalyst SD-WAN デバイス

エッジルータは、ハードウェアデバイスであるかソフトウェアデバイスであるかにかかわらず、ネットワークを介して送信されるデータトラフィックを処理します。エッジルータを既存のネットワークに配置すると、標準ルータとして表示されます。

図 7: 既存のネットワークに配置されたエッジルータ



これを説明するため、ここに示す図では、標準のイーサネットインターフェイスによって接続されたエッジルータと既存のルータを示しています。これら2つのルータは互いにレイヤ3エンドポイントのように見え、2つのデバイス間でルーティングが必要な場合は、インターフェイス上でOSPFまたはBGPを有効にすることができます。このインターフェイスでは、VLANタグging、QoS、ACL、ルートポリシーなどの標準ルータ機能も使用できます。

エッジルータのコンポーネントは次のとおりです。

- **DTLS コントロールプレーン接続**：各エッジルータには、通信する各 Cisco SD-WAN コントローラ に対して 1 つの永続的な DTLS 接続があります。この永続的な 接続は、デバイス認証が成功した後に確立され、エッジルータと Cisco SD-WAN コントローラ の間で暗号化されたペイロードを伝送します。このペイロードは、Cisco SD-WAN コントローラ がネットワークトポロジを決定し、ネットワークの宛先への最適なルートを計算し、このルート情報をエッジルータに配布するために必要なルート情報で構成されます。
- **OMP (オーバーレイ管理プロトコル)**：Cisco SD-WAN コントローラ で説明したように、OMP は DTLS 接続内で実行され、オーバーレイネットワークを確立および維持するために必要なルート、ネクストホップ、キー、およびポリシー情報を伝送します。OMP はエッジルータと Cisco SD-WAN コントローラ の間で実行され、制御情報のみを伝送します。
- **プロトコル**：エッジルータは、OSPF、BGP、VRRP、BFD などの標準プロトコルをサポートしています。
- **ルーティング情報ベース (RIB)**：各エッジルータには、直接インターフェイスルート、静的ルート、および BGP および OSPF を介して学習した動的ルートが自動的に入力される複数のルートテーブルがあります。ルートポリシーは、どのルートが RIB に保存されるかに影響を与える可能性があります。
- **転送情報ベース (FIB)**：これは、エッジルータの CPU がパケットを転送するために使用する RIB の抽出バージョンです。

- **Netconf と CLI** : Netconf は、Cisco SD-WAN Manager がエッジルータのプロビジョニングのために使用する標準ベースのプロトコルです。さらに、各エッジルータはローカル CLI アクセスと AAA を提供します。
- **キー管理** : エッジルータは、標準の IPsec プロトコルを使用して、他のエッジルータとの安全な通信に使用される対称キーを生成します。
- **データプレーン** : エッジルータは、IP 転送、IPsec、BFD、QoS、ACL、ミラーリング、ポリシーベースの転送など、データプレーン機能の豊富なセットを提供します。

エッジルータには、ルーティング、高可用性（HA）、インターフェイス、ARP 管理、ACL などに関するサイトローカルの決定を行うためのローカルインテリジェンスがあります。Cisco SD-WAN コントローラ との OMP セッションは、エッジルータの RIB に影響を与え、オーバーレイネットワークの構築に必要なサイトローカルでないルートと到達可能性情報を提供します。

ハードウェアエッジルータには、ルータの秘密キーと公開キー、および署名付き証明書を含む安全な暗号プロセッサであるトラステッドボード ID チップが含まれています。このすべての情報がデバイス認証に使用されます。エッジルータの初回起動時に、エッジルータと Cisco SD-WAN Validator の IP アドレスなどの最小限の設定情報を入力します。エッジルータは、この情報とトラステッドボード ID チップの情報を使用して、ネットワーク上で自身を認証し、ドメイン内の Cisco SD-WAN コントローラ との DTLS 接続を確立し、ドメインに存在する場合は完全な設定を Cisco SD-WAN Manager から受信してアクティブ化します。それ以外の場合は、設定ファイルを手動でダウンロードするか、コンソール接続を介してエッジルータ上で直接設定を作成できます。

Cisco Catalyst SD-WAN 制御接続

以降の項では、Cisco Catalyst SD-WAN 制御接続について説明します。

Cisco Catalyst SD-WAN 制御接続に関する情報

Cisco Catalyst SD-WAN 制御接続は、Cisco Catalyst SD-WAN ネットワークの動作を制御および管理する通信チャンネルを参照します。これらの接続は、Cisco Catalyst SD-WAN 制御コンポーネント（Cisco Catalyst SD-WAN Validator、Cisco Catalyst SD-WAN コントローラ、Cisco SD-WAN Manager）と Cisco IOS XE Catalyst SD-WAN デバイスの間で確立されます。

TLS 1.3 プロトコルのサポート

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a および Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降、Cisco Catalyst SD-WAN の制御接続は Transport Layer Security プロトコルバージョン 1.3 をサポートします。TLS 1.3 バージョンは、TLS 1.2 よりも強力なセキュリティを提供するため、ネットワークのパフォーマンスと効率が向上します。

Cisco Catalyst SD-WAN 制御コンポーネントが Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.13.1 以降を使用しており、デバイスが Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a を使用している場合、それらの間で TLS 1.3 接続が確立されます。TLS 1.3 接続がない場合、これらのコンポーネントは TLS 1.2 を使用して接続をネゴシエートし、確立します。

暗号スイート

制御接続の場合、Cisco Catalyst SD-WAN は次のいずれかの暗号スイートを自動的に選択します。

- TLS-AES-256-GCM-SHA384
- TLS-AES-128-GCM-SHA256
- TLS-AES-128-CCM-8-SHA256
- TLS-AES-128-CCM-SHA256

Cisco Catalyst SD-WAN 制御接続の TLS 1.3 の利点

- TLS 1.3 は、TLS 1.2 よりも強力なセキュリティを提供します。
- TLS 1.3 では、初期接続セットアップ（ハンドシェイク）に必要なラウンドトリップの数が削減されます。これにより、遅延が減少し、セキュアな接続の確立が高速化され、全体的なパフォーマンスが向上します。

Cisco Catalyst SD-WAN 制御接続の確認

次に、TLS バージョンと選択した暗号スイートを含む、接続ステータスを表示する **show sdwan control connections** コマンドの出力例を示します。このコマンドは、Cisco IOS XE Catalyst SD-WAN デバイスのアクティブな制御接続とコントロールプレーン接続に関する情報を表示します。

次のコマンド出力では、プロトコルバージョン（TLS 1.3）と暗号スイートが太字で示されています。

```
Device# show sdwan control connections

LOCAL-COLOR- lte SYSTEM-IP- 12.16.255.19 PEER-PERSONALITY- vsmart

site-id 100
domain-id 1 protocol tls
protocol-version TLS1_3
cipher-name TLS_AES_256_GCM_SHA384 private-ip 10.0.5.19
private-port 23556
public-ip 10.0.5.19
public-port 23556
org-name vIptela Inc Regression
state up [Local Err: NO_ERROR] [Remote Err: NO_ERROR] uptime 0:00:01:24
hello interval 1000
hello tolerance 12000
controller-grp-id 0 shared-region-id-set N/A peer-session-id 0xdba4a2f8
Tx Statistics- hello 86
connects 0
registers 0
register-replies 0
challenge 0
challenge-response 1
challenge-ack 0
teardown 0
teardown-all 0
```

```

vmanage-to-peer 0
register-to-vmanage 0 Rx Statistics-
hello 86
connects 0
registers 0
register-replies 0
challenge 1
challenge-response 0

challenge-ack 1
teardown 0
vmanage-to-peer 0
register-to-vmanage 0

```

このコマンドは、Cisco IOS XE Catalyst SD-WAN デバイス でローカルデバイスによって開始されたコントロールプレーン接続試行に関する情報を表示します。

```
Device# show sdwan control connection-history detail
```

```

LOCAL-COLOR- lte SYSTEM-IP- 0.0.0.0 PEER-PERSONALITY- vbond

site-id 0
domain-id 0 protocol dtls
protocol-version DTLS1_2
cipher-name ECDHE-RSA-AES256-GCM-SHA384
private-ip 10.0.12.26
private-port 12346
public-ip 10.0.12.26
public-port 12346
UUID/chassis-number eb8844be-f58f-4bd3-b8c2-4f8cbc78131c
state tear_down [Local Err: ERR_DISCONNECT_VBOND] [Remote Err: NO_ERROR] downtime
2023-10-13T20:06:44+0000
repeat count 0 previous downtime N/A
Tx Statistics- hello 17
connects 0
registers 2
register-replies 0
challenge 0
challenge-response 1
challenge-ack 0
teardown 1
teardown-all 0
vmanage-to-peer 0
register-to-vmanage 0 Rx Statistics-

hello 17
connects 0
registers 0
register-replies 2
challenge 1
challenge-response 0
challenge-ack 1
teardown 0
vmanage-to-peer 0
register-to-vmanage 0

```

このコマンドは、Cisco IOS XE Catalyst SD-WAN デバイス によって開始された Cisco Catalyst SD-WAN Validator および Cisco Catalyst SD-WAN コントローラ へのコントロールプレーン接続試行に関する情報を表示します。

```
Device# show control connections detail"
```

```
-----
```



```
REMOTE-COLOR- lte SYSTEM-IP- 172.16.255.21 PEER-PERSONALITY- vedge
```

```
-----
site-id          100
domain-id        1
protocol         tls
protocol-version TLS1_2
cipher-name      ECDHE-RSA-AES256-GCM-SHA384
private-ip       10.0.111.1
private-port     46437
public-ip        10.0.111.1
public-port      46437
org-name         vIPtela Inc Regression
state            up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime          0:00:10:02
hello interval   1000
hello tolerance  12000
peer-session-id  0x00656994de
```

Tx Statistics-

```
-----
hello            603
connects         0
registers        0
register-replies  0
challenge        1
challenge-response 0
challenge-ack     1
teardown         0
teardown-all    0
vmanage-to-peer  1
register-to-vmanage 0
create-cert-reply 0
```

Rx Statistics-

```
-----
hello            603
connects         0
registers        0
register-replies  0
challenge        0
challenge-response 1
challenge-ack     0
teardown         0
vmanage-to-peer  0
register-to-vmanage 1
create-cert      0
```

```
-----
REMOTE-COLOR- default SYSTEM-IP- 172.16.255.19 PEER-PERSONALITY- vsmart
```

```
-----
site-id          100
domain-id        1
protocol         tls
protocol-version TLS1_3
cipher-name      TLS_AES_256_GCM_SHA384
private-ip       10.0.5.19
private-port     23456
public-ip        10.0.5.19
public-port      23456
org-name         vIPtela Inc Regression
state            up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime          0:00:09:48
```

```

hello interval      1000
hello tolerance     12000
peer-session-id     0x00b6655c4d

```

Tx Statistics-

```

-----
hello                589
connects             0
registers             0
register-replies      0
challenge             0
challenge-response    1
challenge-ack         0
teardown             0
teardown-all         0
vmanage-to-peer      1
register-to-vmanage   0
create-cert-reply    0

```

Rx Statistics-

```

-----
hello                589
connects             0
registers             0
register-replies      0
challenge             1
challenge-response    0
challenge-ack         1
teardown             0
vmanage-to-peer      0
register-to-vmanage   1
create-cert          0

```

Cisco Catalyst SD-WAN ソリューション

クラウドネットワークングを合理化および最適化するために、Cisco Catalyst SD-WAN はセキュアな仮想 IP ファブリック上で実行される次世代のソフトウェアサービスを提供します。

- Cloud onRamp for SaaS** : Cloud onRamp for SaaS は、サービスとしてのソフトウェア (SaaS) クラウドアプリケーションのパフォーマンスを最適化します。個々のアプリケーションのパフォーマンスを明確に可視化し、それぞれに最適なパスを自動的に選択します。Cloud onRamp は、アプリケーションごとにカスタマイズされた式を使用して、損失と遅延に関するメトリックを計算します。
- Cisco SD-WAN Analytics** : Cisco SD-WAN Analytics は、ソリューションの一部として Cisco Catalyst SD-WAN によってホストされる SaaS サービスです。オーバーレイネットワーク全体のパフォーマンスを経時的にグラフィカルに表示し、特定の時間における単一のキャリア、トンネル、またはアプリケーションの特性にドリルダウンできます。
- Cisco Catalyst SD-WAN ポータル** : Cisco Catalyst SD-WAN ポータル は、Cisco Catalyst SD-WAN に適したクラウドインフラストラクチャ自動化ツールであり、パブリッククラウドプロバイダーで Cisco SD-WAN コントローラ をプロビジョニング、監視、および保守するための迅速な方法を提供します。

Cloud onRamp for SaaS

企業は、Microsoft Office365、Salesforce、Dropbox などのビジネスクリティカルな SaaS アプリケーションを採用しています。企業は、次の 3 つの主要な方法を使用して、ユーザーに SaaS アプリケーションへの接続を提供します。

- 支社からのダイレクト インターネット アクセス（DIA）。
- 地域施設のゲートウェイを介したインターネットアクセス。
- キャリアニュートラルファシリティ（CNF）のゲートウェイを介したクラウドエクスチェンジまたは直接接続。

遅延とパケット損失は、アプリケーションのパフォーマンスとエンドユーザー エクスペリエンスに直接影響しますが、多くの場合、ネットワーク管理者は、エンドユーザーと SaaS アプリケーション間のネットワークのパフォーマンス特性を限定的に認識できる、またはまったく認識できません。パスの障害が発生し、アプリケーションのパフォーマンスが低下した場合、トラフィックをプライマリパスから代替パスに移行するには、通常、ネットワーク管理者が、複雑で時間がかかり、エラーが発生しやすい一連の手順を手作業で実行する必要があります。

Cisco Catalyst SD-WAN Cloud onRamp for SaaS は、ネットワークのパフォーマンス特性の可視性と継続的な監視を提供します。最適なユーザーエクスペリエンスを実現するために、エンドユーザーと SaaS アプリケーションの間で最高のパフォーマンスを発揮するパスを選択することで、リアルタイムの意思決定を行います。劣化したネットワークパスのアプリケーショントラフィックをインテリジェントに再ルーティングして、ネットワークパフォーマンスの変化に自動的に対応します。

Cloud onRamp for SaaS は、DIA、地域施設を介したインターネットアクセス、CNF を介したアクセスなど、クラウドベースの SaaS アプリケーションのすべてのアクセス方法をサポートします。

Cloud onRamp for SaaS は、エンタープライズクラウドアプリケーションの Viptela Quality of Experience (vQoE) と呼ばれるアプリケーションのパフォーマンス値を計算します。vQoE 値は、アプリケーションごとにカスタマイズされた式を使用して、損失と遅延を比較検討します。たとえば、電子メールアプリケーションはビデオアプリケーションよりも遅延の許容度が高く、ビデオアプリケーションは電子メールよりも損失の許容度が高くなります。vQoE 値の範囲は 0 から 10 で、0 が最低品質、10 が最高品質です。

マウスを数回クリックするだけで Cisco SD-WAN Manager で Cloud onRamp for SaaS を有効にできます。その後 Cisco SD-WAN Manager の Cloud onRamp ダッシュボードにアクセスして、個々のアプリケーションのパフォーマンスを継続的に可視化します。

Cisco Catalyst SD-WAN Analytics

Cisco SD-WAN Analytics は、アプリケーションとネットワークのパフォーマンスの経時的な可視性を提供します。Cisco SD-WAN Analytics は、ソリューションの一部として Cisco Catalyst SD-WAN によってホストされる SaaS サービスです。オーバーレイネットワーク全体をグラフィカルに表示し、ドリルダウンして特定の時間における単一のキャリア、トンネル、またはアプリケーションの特性を表示できます。

Cisco SD-WAN Analytics ダッシュボードでネットワークの概要をインタラクティブに確認し、そこからさらに詳しい情報を確認することができます。このダッシュボードにはデフォルトで過去 24 時間に集計された情報が表示されます。ドリルダウンすると、表示するデータセットごとに異なる期間を選択できます。ダッシュボードには、アプリケーションのパフォーマンス、WAN サイトの使用状況、およびキャリアの使用状況に関するデータが表示されます。

Cisco SD-WAN Analytics プラットフォームは、個々のアプリケーション用にカスタマイズされた QoE 値により、アプリケーションのパフォーマンスを計算します。この値の範囲は 0 から 10 で、0 が最低、10 が最高のパフォーマンスです。Cisco SD-WAN Analytics は、遅延、損失、ジッターに基づいて QoE を計算し、アプリケーションごとに計算をカスタマイズします。

Cisco SD-WAN Analytics は長期間にわたってデータを保存し、過去の傾向情報を表示し、将来の計画に使用できる洞察を提供します。

次の構成が可能です。

- アプリケーションの可視性：
 - パフォーマンスが最高および最低のアプリケーション：パフォーマンスが最高および最低のアプリケーションを表示し、サイトレベルで詳細にドリルダウンします。
 - 最も帯域幅を消費するアプリケーション：最も帯域幅を消費するアプリケーションを表示し、サイトとユーザーにドリルダウンします。
- ネットワークの可視性：
 - ネットワークの可用性と回線の可用性：ネットワークの可用性を表示し、ネットワークと回線の可用性を関連付けます。
 - トンネルのパフォーマンス：さまざまな Cisco Catalyst SD-WAN トンネルでの損失、遅延、ジッターなどの主要なパフォーマンス インジケータを表示します。
 - キャリアの使用状況ビュー：プロバイダーとそのネットワーク特性を表示します。

Cisco Catalyst SD-WAN ポータル

Cisco Catalyst SD-WAN ポータル は、Cisco Catalyst SD-WAN に適したクラウドインフラストラクチャ自動化ツールであり、パブリック クラウドプロバイダーで Cisco SD-WAN コントローラ をプロビジョニング、監視、および保守するための迅速な方法を提供します。

Cisco Catalyst SD-WAN ポータル を使用して、次のコントローラをプロビジョニングできます。

- Cisco SD-WAN Manager
- Cisco Catalyst SD-WAN Validator
- Cisco Catalyst SD-WAN コントローラ



- (注) Cisco vManage リリース 20.9.1 以降、Cisco Catalyst SD-WAN ポータルへのリンクが Cisco Catalyst SD-WAN メニューから追加されます。Cisco Catalyst SD-WAN のメニューから [SD-WAN Portal] をクリックして、Cisco SD-WAN コントローラ のプロビジョニング、監視、および保守のために Cisco Catalyst SD-WAN ポータルにアクセスします。

Cisco Catalyst SD-WAN ポータル の詳細については、『[Cisco Catalyst SD-WAN ポータル Configuration Guide](#)』を参照してください。

Cisco SD-AVC

18.4 リリース以降、Cisco Catalyst SD-WAN はシスコのソフトウェア定義型 Application Visibility and Control (SD-AVC) を組み込んで、次のことを提供できます。

- 可視性、分析、アプリケーション認識型ルーティング、およびアプリケーションベースのポリシー（QoS やアプリケーションベースのファイアウォールポリシーなど）のためのネットワーク アプリケーション トラフィックの認識。
- ネットワークレベルでの分析。

Cisco SD-AVC はネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイス で動作し、Cisco SD-AVC ネットワークサービスは Cisco SD-WAN Manager 内のコンテナとして動作します。



- (注) 関連するすべての Cisco SD-AVC 機能は、Cisco SD-WAN Manager インターフェイスを介してアクセスされます。Cisco Catalyst SD-WAN は、個別の SD-AVC インターフェイスの使用をサポートしていません。

Cisco SD-WAN Manager Cluster

Cisco SD-AVC は、単一の Cisco SD-WAN Manager インスタンスのみで動作する必要があります。Cisco SD-WAN Manager クラスタでは、単一の Cisco SD-WAN Manager インスタンスのみで Cisco SD-AVC を有効にします。

Cisco Catalyst SD-WAN との連携

Cisco vEdge デバイスを使用した基本的なオーバーレイネットワークの構築

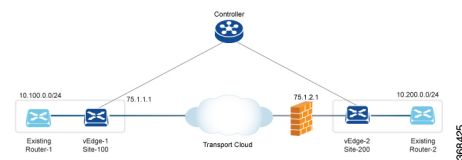
2 つの vEdge ルータと 1 つの Cisco SD-WAN コントローラ を含む単純なネットワーク設計を使用して、正常に機能するオーバーレイネットワークを Cisco vEdge コンポーネントから形成する方法を説明します。このトポロジでは、Cisco SD-WAN Validator ソフトウェアが一方の vEdge

ルータで有効になっています。単純なネットワークを理解できたら、より複雑なトポロジの設計と構築を開始できます。

単純なネットワークトポロジ

次の図に、単純なトポロジを示します。ここには、Site-100 と Site-200 の 2 つのサイトがあります。vEdge-1 は Site-100 のエッジデバイスであり、vEdge-2 は Site-200 のエッジデバイスです。各ローカルサイトで、vEdge ルータは標準のイーサネットインターフェイスを介して既存の従来型ルータに接続します。vEdge-2 は、ファイアウォール機能も備えた NAT デバイスを介してトランスポートネットワークに接続されます。

図 8: 単純なネットワークトポロジ



この設計の目的は、プライベートネットワークを作成して、レイヤ 3 の観点から Router-1 と Router-2 を相互に隣接させ、これらの各ルータに接続されているホストがプライベートネットワークを介して通信できるようにすることです。

基本的なネットワークの構築

次の手順により、上記のトポロジに示されている単純なオーバーレイネットワークを作成できます。

- 手順 1：初期起動および基本構成を実行します。
- 手順 2：ホストまたはサービス側のインターフェイスとルーティングを有効にします。
- 手順 3：OMP を介したオーバーレイルーティングを有効にします。
- 手順 4：IPsec データプレーンの自動セットアップを確認します。
- 手順 5：ポリシーを適用します。

これらの手順について、もう少し詳しく説明します。

手順 1：初期起動および基本構成の実行

ネットワーク管理者の観点では、Cisco vEdge ネットワークコンポーネントの初期起動は、各ネットワークコンポーネントの構成を作成し、いくつかの重要な認証関連ファイルが適切に配置されていることを確認することを含む、簡単で単純なプロセスです。ユーザーの観点では、起動は、vEdge ルータの電源を入れ、ケーブルを差し込んでルータをネットワークに接続するだけです。起動の残りの部分は、ゼロタッチプロビジョニングプロセスによって自動的に実行されます。

ネットワーク管理者は、初期起動の一部として次のタスクを実行します。

1. ネットワーク内のいずれかの vEdge ルータで Cisco SD-WAN Validator 機能を設定します。この例では、これは vEdge-1 です。
2. 必要に応じて、トップレベルの Cisco SD-WAN Validator を ZTP サーバーとして機能するように設定します。この状況では、DNS サーバーがエンタープライズ ネットワークに存在する必要があります。
3. DHCP サーバーがエンタープライズ ネットワークに存在することを確認します。
4. 署名付き証明書を Cisco SD-WAN Manager にインストールし、その証明書を Cisco SD-WAN Manager Orchestrator にダウンロードします。
5. Cisco SD-WAN Manager に vEdge ルータ認定シリアル番号ファイルをインストールし、それを Cisco SD-WAN コントローラ にダウンロードします。
6. Cisco SD-WAN Manager CLI から、オーバーレイネットワークの各 Cisco Catalyst SD-WAN コントローラ および vEdge ルータの構成を作成します。
 1. 従来型ルータのルータ ID アドレスに似たシステム IP アドレスを設定します。この、デバイス上のどのインターフェイスにも依存しないアドレスにより、Cisco vEdge デバイスが識別されます。システム IP アドレスは、事前に割り当てられる必要があります、各 vEdge ルータと Cisco Catalyst SD-WAN コントローラ の全体にわたって一意である必要があります。これらのアドレスは、ネットワーク経路でルーティング可能である必要はありません。
 2. オーバーレイネットワーク内のさまざまなサイトのサイト ID を設定します。この例では、vEdge-1 が Site-100、vEdge-2 が Site-200 にあります。Cisco Catalyst SD-WAN コントローラ は、一つのサイトに併置することも、独自のサイトに配置することもできます。
 3. ドメイン ID を設定します。これは、クラスタを作成するためのオプションの手順です。この例では、ドメイン ID を 1 として設定します。
 4. Cisco SD-WAN Validator サーバーと Cisco Catalyst SD-WAN コントローラ の IP アドレスまたは DNS 名を設定します。
 5. vEdge-1 および vEdge-2 で WAN インターフェイスを設定します。VPN 0 は、WAN トランスポート インターフェイス用に予約された VPN です。IP アドレスは DHCP 経由で自動的に取得できます。また、デフォルトゲートウェイと DNS を明示的に設定することもできます。
 6. デフォルトでは、WAN インターフェイスで DTLS と IPsec が有効になっています。
 7. 設定を保存します。

Cisco SD-WAN コントローラ はネットワークに参加すると Cisco SD-WAN Validator によって認証され、vEdge ルータはネットワークに参加すると Cisco SD-WAN Validator と Cisco SD-WAN コントローラ の両方によって認証されます。その後、これらのデバイスが Cisco SD-WAN Manager に接続し、構成をダウンロードします。

vEdge-1 の構成例 :

```

system
  host-name vEdge-1
  system-ip 1.0.0.1
  domain-id 1
  site-id 100
  vbond 75.1.1.1 local
!
vpn 0
  interface ge 0/0
  ip address 75.1.1.1/24
  tunnel-interface
  color default
  no shutdown
  ip route 0.0.0.0/0 75.1.1.254
!

```

この記事の残りのセクションでは、vEdge ルータおよび Cisco SD-WAN コントローラ で他の一般的な機能を設定する方法について説明します。通常、Cisco SD-WAN Manager で作成する構成において、すべての機能を一度に設定します。この構成は、オーバーレイネットワークに参加するときにデバイスにダウンロードされます。ただし、各種機能を詳しく説明するために、この記事では構成のさまざまな部分を個別に説明します。

手順 2：ホストまたはサービス側のインターフェイスとルーティングの有効化

Cisco SD-WAN Manager から、サービス側のインターフェイスと通常のルーティングを設定することもできます。

1. 既存の従来型ルータに向けて vEdge-1 のインターフェイスを設定します。IP アドレスを割り当て、そのインターフェイスをデフォルト以外の VPN に配置します。この例では、これは VPN 1 です。vEdge-2 で同じ手順を実行します。
2. 既存のルータに向けて vEdge ルータで OSPF または BGP を設定します。
3. コミットします。

ローカルサイトで標準の IP 到達可能性、ルート、およびネクストホップを確認するには、標準の **ping**、**traceroute**、およびさまざまな **show** コマンドを Cisco SD-WAN Manager で、またはデバイスの CLI から（デバイスに直接接続している場合）使用します。

ホストまたはサービス側の VPN の構成例：

```

vpn 1
  router
    ospf
      redistribute omp
      area 0
      interface ge 0/1
      exit
    exit
  !
!
interface ge 0/1
  ip address 10.1.2.12/24
  no shutdown
!

```


手順 3 : OMP を介したオーバーレイルーティングの有効化

すべてのサイトローカルルートは、vEdge ルータに入力されます。これらのルートは他の vEdge ルータに配布されます。これは、Cisco Catalyst SD-WAN コントローラによって、OMP を介して実行されます。

1. BGP を使用しているか OSPF 外部 LSA がある場合は、OMP による BGP ルートの再配布を許可します。
2. OMP ルートを BGP または OSPF に再アドバタイズします。
3. コミットします。

OMP を介したオーバーレイルーティングの構成例 :

```
omp
  advertise ospf external
!
```

この時点で、vEdge-1 は Site-200 からプレフィックスについて学習でき、vEdge-2 は Site-100 からプレフィックスについて学習できます。すべてのプレフィックスが VPN 1 の一部であるため、Site-100 と Site-200 のホストは相互に到達可能です。Cisco Catalyst SD-WAN オーバーレイネットワークの観点では、vEdge-1 が、アドレス 10.100.0.0/24 とデフォルトの TLOC カラーで構成される vRoute（この例では {75.1.1.1, default} と記述）を Cisco Catalyst SD-WAN コントローラにアドバタイズするため、この到達可能性が実現されます。つづいて、Cisco Catalyst SD-WAN コントローラがこの vRoute を vEdge-2 にアドバタイズします。同じプロセスが vEdge-2 でプレフィックス 10.200.0.0/24 によって発生します。

手順 4 : IPsec データプレーンの自動セットアップの確認

vEdge ルータのすべての TLOC について、vEdge ルータが暗号化用の対称キーをアドバタイズします。Cisco Catalyst SD-WAN コントローラは、このキーを自動的に反映し、対称キーを使用して TLOC をアドバタイズします。その結果、双方向の IPsec SA がセットアップされ（つまり、各方向に異なるキーが存在します）、データトラフィックは自動的にこの IPsec トンネルの使用を開始します。トンネルが稼働状態になると、そのトンネルで BFD が自動的に開始されます。これは、トランスポートネットワークで障害が発生した場合にデータプレーン的高速コンバージェンスを確保するために行われます。

IPsec データプレーンのセットアップは自動的に実行されます。コンフィギュレーションは必要ありません。複数の show コマンドを使用して、SA と、IPsec トンネルの状態を確認できます。

手順 5 : ポリシーの適用

オプションの手順として、Cisco Catalyst SD-WAN コントローラでコントロールプレーンポリシーとデータプレーンポリシーを作成し、それらを vEdge ルータにプッシュすることができします。たとえば、ネットワーク管理者が { vEdge-2, prefix 10.200.0.0/24 } 宛てのトラフィックを vEdge-3 などの別のサイトに転送するポリシーを適用する場合は、Cisco Catalyst SD-WAN コントローラでコントロールプレーンポリシーを作成し、それぞれの vEdge ルータにプッシュすることができます。構成自体ではなくポリシーの結果が vEdge ルータにプッシュされます。

ポリシーの構成例：

```

policy
  lists
    site-list site-100
      site-id 100
    !
    prefix-list my-prefixes
      ip-prefix 10.200.0.0/24
    !
    control-policy TE-thru-vedge3
      sequence 10
        match route
          prefix-list my-prefixes
        !
        action accept
          set
            tloc 1.0.0.3 color default
          !
        !
        default action accept
      !
    apply-policy
      site-list site-100
        control-policy TE-thru-vedge3 out
      !
    !
  !

```

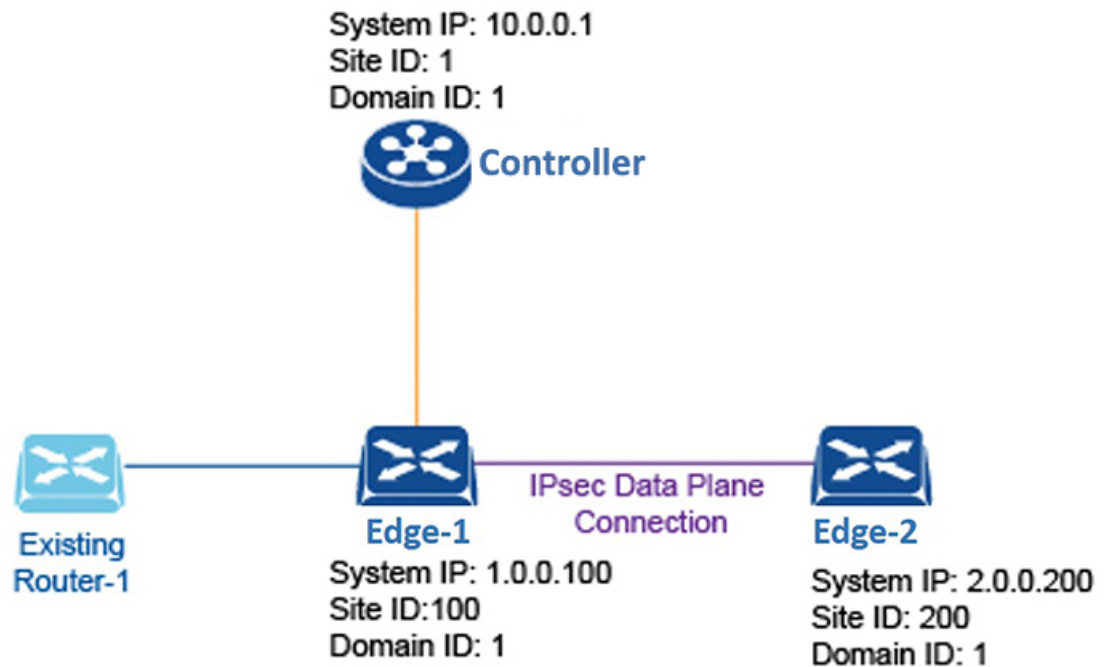
詳細オプション

基本的なルーティング、セキュリティ、およびポリシーを確認したので、ネットワークへの他のさまざまな要素の追加を開始できます。[Software] カテゴリを調べて、高可用性、コンバージェンス、BFD、QoS、ACL、セグメンテーション、高度なポリシーなどの要素を追加することをお勧めします。

Cisco Catalyst SD-WAN に関する用語

次の図は、Cisco Catalyst SD-WAN オーバーレイネットワークの説明に使用される用語をまとめたものです。

図 9: Cisco Catalyst SD-WAN オーバーレイネットワークで使用される用語



ドメイン ID

ドメインは、Cisco SD-WAN コントローラの制御範囲を区切る、エッジルータと Cisco SD-WAN コントローラの論理グループです。各ドメインは、ドメイン ID と呼ばれる一意の整数によって識別されます。現時点では、Cisco Catalyst SD-WAN オーバーレイネットワークで設定できるドメインは 1 つだけです。

ドメイン内では、エッジルータは、独自のドメイン内の Cisco SD-WAN コントローラにのみ接続できます。Cisco SD-WAN Validator は、どの Cisco SD-WAN コントローラがどのドメインにあるのかを認識しているため、新しいエッジルータが起動したときに、Cisco SD-WAN Validator はそれらのルータを適切なドメインの Cisco SD-WAN コントローラに向けることができます。ただし、Cisco SD-WAN Validator はドメインのメンバーにはなりません。

ドメイン内では、Cisco SD-WAN コントローラとエッジルータの間にルーティング情報の完全な同期があり、ルート集約および要約の範囲が存在します。組織は、ネットワークをドメインに分割して、必要なビジネス目的に合致させることができます。たとえば、ドメインを大きな地理的領域またはデータセンターに対応させ、各データセンターとそれが担当する分散拠点が単一のドメインに含まれるようにすることができます。

OMP ルート

Cisco SD-WAN コントローラ およびエッジルータでは、OMP はローカルサイトから学習したルートとサービスを、対応するトランスポート ロケーション マッピング（「トランスポート ロケーション」（TLOC）と呼ばれる）とともにピアにアドバタイズします。これらのルート

は、標準の IP ルートと区別するために「OMP ルート」と呼ばれます。Cisco SD-WAN コントローラは、この OMP ルートを介して、ネットワークトポロジと使用可能なサービスを学習します。

Cisco Catalyst SD-WAN コントロールプレーン アーキテクチャは、次の 3 種類の OMP ルートを使用します。

- **OMP ルート**：OMP 編成のトランスポートネットワークを使用するエンドポイント間の到達可能性を確立するプレフィックス。OMP ルートは、中央データセンターのサービス、ブランチオフィスのサービス、またはオーバーレイネットワークの任意の場所にあるホストやその他のエンドポイントの集合を表すことができます。OMP ルートは、機能転送のために TLOC を必要とし、TLOC に解決されます。BGP と比較すると、OMP ルートは、いずれかの BGP AFI/SAFI フィールドで伝送されるプレフィックスと同等です。
- **TLOC**：OMP ルートを物理ロケーションに関連付ける識別子。TLOC は、基盤となるネットワークから認識できる OMP ルーティングドメインの唯一のエンティティであり、基盤となるネットワークのルーティングを介して到達できる必要があります。TLOC は、物理ネットワークのルーティングテーブル内のエントリを介して直接到達できるか、または NAT デバイスの外部に存在するプレフィックスによって表され、ルーティングテーブルに含まれている必要があります。BGP と比較すると、TLOC は OMP ルートのネクストホップとして機能します。
- **サービスルート**：OMP ルートをネットワーク内のサービスに関連付ける識別子であり、ネットワーク内のサービスの場所を指定します。サービスには、ファイアウォール、侵入検知システム (IDP)、およびロードバランサが含まれます。



(注) サポートされる OMP ルートの最大数は、C1131X_8PW デバイスで 140K です。140K を超える OMP ルートがある場合、メモリ不足の問題によりデバイスがクラッシュします。

サイト ID

サイトは、分散拠点、データセンター、キャンパスなど、Cisco Catalyst SD-WAN オーバーレイネットワーク内にある特定の物理的な場所です。各サイトは、サイト ID と呼ばれる一意の整数によって識別されます。サイトの各 Cisco vEdge デバイスは、同じサイト ID で識別されます。そのため、データセンター内では、すべての Cisco SD-WAN コントローラ およびエッジルータが同じサイト ID で設定されます。通常、分散拠点またはローカルサイトには単一のエッジルータがありますが、冗長性のために 2 つ目のルータが存在する場合は、両方のルータが同じサイト ID で設定されます。

システム IP アドレス

各エッジルータおよび Cisco Catalyst SD-WAN コントローラ にはシステム IP アドレスが割り当てられ、インターフェイスアドレスとは独立して物理システムが識別されます。このアドレスは、通常のルータのルータ ID に似ています。システム IP アドレスは、エッジルータと Cisco SD-WAN コントローラ の永続的なネットワーク オーバーレイ アドレスを提供し、必要に応じ

て、Cisco vEdge デバイス の到達可能性に影響を与えることなく、物理インターフェイスの番号付けを変更することを可能にします。システム IP アドレスは、IPv4 アドレスと同様に、ドットで区切られた 4 つの部分からなる 10 進表記で記述します。

TLOC

TLOC（トランスポートロケーション）は、エッジルータが WAN トランスポートネットワークまたは NAT ゲートウェイに接続する物理インターフェイスを識別します。TLOC はいくつかのプロパティで識別されますが、主要なものは {IP-address, color} タプルとして記述できる IP アドレス/カラーペアです。このタプルでは、IP アドレスはシステム IP アドレスであり、カラーは VPN または VPN 内のトラフィックフローを識別する固定のテキスト文字列です。OMP は TLOC ルートを使用して TLOC をアドバタイズします。

その他の情報

Cisco Catalyst SD-WAN オーバーレイネットワークの要素の説明については、「*Components of the Cisco Catalyst SD-WAN Solution*」を参照してください。Cisco Catalyst SD-WAN ソフトウェアおよびハードウェアを使用してオーバーレイネットワークを構築する方法については、「*Constructing a Basic Network Using Cisco Catalyst SD-WAN Components*」を参照してください。オーバーレイネットワークのコンポーネントの機能例については、「Validated Examples」を参照してください。



第 4 章

ハードウェアとソフトウェアの設置

表 2: 機能の履歴

機能名	リリース情報	説明
CLI を使用した Cisco IOS XE Catalyst SD-WAN デバイスのブートストラップファイルの生成	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a	この機能により、最小限のブートストラップ設定ファイルをデバイス上で直接生成できます。このファイルを使用すると、完全な設定が失われたり削除されたりした場合に、デバイスがコントローラに再接続することができます。

- [サーバー推奨事項 \(40 ページ\)](#)
- [モジュールの追加または削除後の Cisco IOS XE Catalyst SD-WAN デバイスのデバイス設定のリセット \(40 ページ\)](#)
- [Cisco Catalyst SD-WAN デバイスのオンサイト ブートストラッププロセス \(41 ページ\)](#)
- [SHA2 エンタープライズ証明書を使用した Cisco vEdge 5000 のオンサイト ブートストラッププロセス \(44 ページ\)](#)
- [CLI を使用した Cisco IOS XE Catalyst SD-WAN デバイスのブートストラップファイルの生成 \(50 ページ\)](#)
- [ワンタッチプロビジョニング：汎用ブートストラップ構成を使用した Cisco IOS XE Catalyst SD-WAN デバイスのオンボード \(52 ページ\)](#)
- [Cisco SD-AVC のインストール \(Cisco vManage 20.1.1 以前\) \(57 ページ\)](#)
- [Cisco SD-AVC のインストール \(Cisco vManage リリース 20.3.1 以降\) \(60 ページ\)](#)
- [クラウドサービスの有効化 \(73 ページ\)](#)
- [Cisco IOS XE ルータのソフトウェアのインストールとアップグレード \(74 ページ\)](#)
- [デフォルトパスワードの復元 \(85 ページ\)](#)
- [vEdge ルータのソフトウェアのインストールとアップグレード \(85 ページ\)](#)
- [Cisco Catalyst SD-WAN Manager をホストしている仮想マシンでのメモリおよび vCPU リソースのアップグレード \(96 ページ\)](#)

- セカンダリディスクサイズの拡大 (Cisco Catalyst SD-WAN Manager リリース 20.12.x 以前) (98 ページ)
- Cisco IOS XE Catalyst SD-WAN デバイスのソフトウェア メンテナンス アップグレード (99 ページ)

サーバー推奨事項

このトピックは、Cisco SD-WAN Validator サーバー、vEdge Cloud ルータサーバー、Cisco SD-WAN Manager サーバー、および Cisco SD-WAN コントローラ サーバーのハードウェア推奨事項 (『[Cisco Catalyst SD-WAN Controller Compatibility Matrix and Recommended Computing Resources](#)』) に結び付いています。

vEdge Cloud ルータサーバーの推奨事項

[vEdge Cloud のデータシート](#)を参照してください。

モジュールの追加または削除後の Cisco IOS XE Catalyst SD-WAN デバイスのデバイス設定のリセット

前提条件

ルータモジュールのハードウェアの設置に関する基礎知識が必要です。モジュールをプラットフォームに挿入する方法、またはプラットフォームから削除する方法については、それぞれのプラットフォームまたはモジュールのドキュメントを参照してください。

OIR サポート



(注) OIR は Cisco IOS XE Catalyst SD-WAN デバイス ではサポートされていません。

活性挿抜 (OIR) を行うと、システム運用に影響を与えずにシスコデバイスの部品を交換できます。モジュールが挿入されると、モジュールが通電し、モジュール自身が初期化され、動作を開始します。

ホットスワップ機能により、システムは、装置の物理構成に発生した変更の状況を判断し、すべてのインターフェイスが適切に機能するように装置のリソースを再度割り当てることができます。この機能を使用すると、モジュールのインターフェイスを再構成しても、ルータの他のインターフェイスを変更せずに済みます。

ソフトウェアは、モジュールの取り外しと挿入の処理に必要なタスクを実行します。ハードウェア割り込みは、ハードウェアの変更が検出されるとソフトウェアサブシステムに送られ、ソフトウェアがシステムを次のように再構成します。

- モジュールが挿入されると、エンドユーザーが適切に構成できるように分析および初期化されます。OIR 中に使用される初期化ルーチンは、ルータの電源投入時のルーチンと同じです。ソフトウェアによっても処理されるシステムリソースは、新しいインターフェイスに割り当てられます。
- モジュールを取り外すと、空きスロットに関連付けられたリソースは、解放されるか、ステータスの変更を示すために変更される必要があります。

デバイス設定のリセット

モジュールを Cisco IOS XE Catalyst SD-WAN デバイス に挿入または取り外した場合は、CLI を使用してデバイス設定のリセットを実行して、Cisco IOS XE Catalyst SD-WAN デバイス と物理的な変更との同期を保つ必要があります。コントローラモード構成のリセットの詳細については、「[Controller Mode Configuration Reset](#)」を参照してください。

Cisco Catalyst SD-WAN デバイスのオンサイト ブートストラップ プロセス

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 Cisco Catalyst SD-WAN 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。デバイスは起動すると、構成ファイルの情報を使用してネットワークに接続します。

オンサイト ブートストラップ プロセスは、次の一般的なワークフローで構成されます。

- Cisco SD-WAN Manager を使用して構成ファイルを生成する
- 構成ファイルをブート可能な USB ドライブにコピーしてドライブをデバイスに接続するか、構成をデバイスのブートフラッシュにコピーします。
- デバイスを起動します。

挿入された USB ドライブとブートフラッシュの両方に構成ファイルがある場合、ブートフラッシュの構成ファイルが優先されます。

デバイスの要件

オンサイト ブートストラップ プロセスを使用して構成するデバイスは、次の要件を満たしている必要があります。

- サポートされている Cisco Catalyst SD-WAN イメージがデバイスにインストールされている
- デバイスは、構成が追加されていない工場出荷時のデフォルト状態である

オンサイト ブートストラップ プロセスの実行

デバイスのオンサイト ブートストラップ プロセスを実行するには、次の手順に従います。

1. デバイスのシャーシ ID とのシリアル番号を Cisco SD-WAN Manager にアップロードします。
手順については、「vEdge シリアル番号ファイルのアップロード」を参照してください。
2. Cisco SD-WAN Manager メニューから、**[Administration]** > **[Settings]** の順に選択し、組織名と Cisco Catalyst SD-WAN Validator の IP アドレスが正しく設定されていることを確認します。
3. ネットワーク内のデバイス認証に独自のエンタープライズルート認証局（CA）を使用している場合は、Cisco SD-WAN Manager で次の操作を実行します。
 1. Cisco SD-WAN Manager のメニューで、**[Administration]** > **[Settings]** の順に選択します。
 2. **[WAN Edge Cloud Certificate Authorization]** をクリックします。
(Cisco Catalyst SD-WAN Manager リリース 20.12.x 以前を使用している場合は、**[Edit]** をクリックします。)
 3. **[Manual]** をクリックします。
 4. **[Save]** をクリックします。
4. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
5. **[Feature Templates]** をクリックして、デバイスのテンプレートを作成します。



(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。

6. 次の操作を行ってください。
 1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Devices]** の順に選択します。
 2. 目的のデバイスで [...] をクリックし、**[Generate Bootstrap Configuration]** を選択します。
 3. ダイアログボックスで、**[Cloud-init]** を選択し、**[OK]** をクリックします。
Multipurpose Internet Mail Extensions（MIME）ファイルが生成され、内容がポップアップウィンドウに表示されます。このファイルには、デバイスのシステムプロパティ、ルート CA（エンタープライズルート CA を使用している場合）、および作成したテンプレートの構成設定が含まれています。
7. **[MIME file]** ポップアップウィンドウで、**[Download]** をクリックします。

ファイルがローカルシステムにダウンロードされ、ダウンロード用のディレクトリに保存されます。ファイル名は `chassis.cfg` で、`chassis` はステップ 1 でアップロードしたデバイスのシャーシ ID です。



- (注) この手順の代わりに、MIME ファイルの内容をポップアップウィンドウからテキストファイルにコピーし、`ciscosdwan.cfg`（大文字と小文字を区別）という名前で保存してから、ステップ 8 にスキップできます。



- (注) ハードウェアデバイスの場合は、ブートストラップファイル名を `ciscosdwan.cfg` として使用します。このファイルは Cisco SD-WAN Manager によって生成され、UUID が含まれていますが、OTP は含まれていません。ソフトウェアデバイス（CSR および ISRv）、および ASR1002-X などの OTP 認証デバイスの場合、ブートストラップファイル名を `ciscosdwan_cloud_init.cfg` として使用します。このファイルには OTP が含まれていますが、`ciscosdwan_cloud_init.cfg` の UUID 検証は含まれていません。

8. MIME ファイルをダウンロードした場合は、名前を `ciscosdwan.cfg`（大文字と小文字を区別）に変更します。



- (注) これは、オンサイト ブートストラップ プロセスの構成ファイルです。

9. `ciscosdwan.cfg` ファイルをブート可能な USB ドライブまたはデバイスのブートフラッシュにコピーします。



- (注) ファイルには、表示されているとおりに名前を付ける必要があります。そうしないと、デバイスがファイルを読み取れません。

10. USB ドライブを使用している場合は、USB ドライブをデバイスに接続します。
11. デバイスを起動します。

デバイスは、USB ドライブまたはブートフラッシュから構成ファイルを読み取り、構成情報を使用してネットワークに接続します。デバイスでは、ブートフラッシュにある構成ファイルが優先されます。

SHA2 エンタープライズ証明書を使用した Cisco vEdge 5000 のオンサイト ブートストラップ プロセス

表 3: 機能の履歴

機能名	リリース情報	説明
SHA2 エンタープライズ証明書を使用した Cisco vEdge 5000 のオンサイト ブートストラップ プロセス	Cisco SD-WAN リリース 20.3.1 Cisco vManage リリース 20.3.1	デフォルトでは、Cisco vEdge 5000 デバイスは、オーバーレイネットワーク内のコントローラによる認証に SHA1 証明書を使用します。この機能を使用すると、OTP と公開キーを使用してデバイスを認証し、SHA2 エンタープライズ証明書をデバイスにインストールすることができます。OTP と公開キーを使用してデバイスを認証し、SHA2 エンタープライズ証明書をインストールすることにより、SHA1 証明書認証をバイパスし、SHA1 の脆弱性からデバイスを保護することができます。

Cisco vEdge 5000 デバイスは、トラステッドプラットフォームモジュール (TPM 1.2) を装備しており、オーバーレイネットワークへの接続時に認証に SHA1 証明書を使用します。SHA1 証明書を使用したブートストラッププロセスについては、「Cisco Catalyst SD-WAN デバイスのオンサイト ブートストラッププロセス」を参照してください。

Cisco Catalyst SD-WAN リリース 20.3.1 以降では、Cisco vEdge 5000 デバイスのブートストラップおよびそのデバイスのオーバーレイネットワークへの接続時に、ワンタイムパスワード (OTP) と公開キーを使用してデバイスを認証し、そのデバイスに SHA2 エンタープライズ証明書をインストールすることができます。OTP と公開キーを使用してデバイスを認証し、SHA2 エンタープライズ証明書をインストールすることにより、SHA1 証明書認証をバイパスし、SHA1 の脆弱性からデバイスを保護することができます。

OTP と公開キーを使用して Cisco vEdge 5000 を認証する方法

1. **Plug and Play Connect** でデバイスの公開キーを入力し、serial.viptela ファイルを生成します。
2. serial.viptela ファイルを Cisco SD-WAN Manager にアップロードします。

3. Cisco SD-WAN Manager が、デバイスのランダム認証トークンを生成します。Cisco SD-WAN Manager が、デバイスの公開キーを使用して認証トークンを暗号化し、それを OTP として <chassis>.config ファイルに入力します。
4. <chassis>.config ファイルをブート可能 USB ドライブにダウンロードし、工場出荷時設定へのリセットを実行した後に、USB ドライブをデバイスに挿入します。
5. デバイスが、<chassis>.config ファイルを読み取り、暗号化されたダイジェストを [OTP] フィールドから読み取って、デバイスの秘密キーを使用してダイジェストを復号し、認証トークンを取得します。
6. デバイスが、AVNET/TPM1.2 SHA1 証明書認証を無効にします。
7. デバイスが、認証トークンを使用して Cisco SD-WAN Manager でそれ自体を認証し、制御接続を確立します。
8. Cisco SD-WAN Manager が、初期構成をデバイスにプッシュします。
9. Cisco SD-WAN Manager が、デバイスの SHA2 エンタープライズ証明書をプッシュし、証明書をデバイスにインストールします。
10. デバイスが、SHA2 エンタープライズ証明書を使用してそれ自体をコントローラに対して再認証し、コントローラに接続します。

考慮すべき点

- Cisco vEdge 5000 デバイスが OTP を使用して Cisco SD-WAN Validator または Cisco SD-WAN Manager で認証された後、SHA2 エンタープライズ証明書がインストールされて検証されるまで、デバイスを再起動しないでください。エンタープライズ証明書が検証される前にデバイスが再起動した場合は、ブートストラップ手順を再び開始します。
- 署名付き SHA2 エンタープライズ証明書が Cisco vEdge 5000 デバイ스에インストールされ、ブートストラッププロセスが完了した後に、ソフトウェアリセット、構成リセット、または工場出荷時リセットを実行する場合は、デバイスのブートストラップを再実行します。
- Cloud-Init（暗号化 OTP）ブートストラップ構成を生成するたびに、新しい構成ファイルをブート可能 USB ドライブにダウンロードする必要があります。

前提条件

1. エンタープライズ証明書認証が設定されていることを確認します。
 1. Cisco SD-WAN Manager のメニューで、**[Administration] > [Settings]** の順に選択します。
 2. **[Hardware WAN Edge Certificate Authorization]** をクリックします。
(Cisco Catalyst SD-WAN Manager リリース 20.12.x 以前を使用している場合は、**[Edit]** をクリックします。)

3. [Enterprise Certificate (signed by Enterprise CA)] がオンになっていることを確認し、[Save] をクリックします。
2. serial.viptela ファイルを生成する前に、デバイスの公開キーエントリが PNP サーバーで使用できることを確認します。詳細については、「Cisco vEdge 5000 デバイスの公開キーの表示または追加」を参照してください。
3. Cisco vEdge 5000 デバイスが SHA1 証明書を使用してオーバーレイネットワークに接続されている場合は、認証に OTP、公開キー、および SHA2 エンタープライズ証明書を使用するように設定する前に、デバイスを無効にしてオーバーレイネットワークから削除する必要があります。

Cisco vEdge 5000 デバイスの公開キーの表示または追加

1. [Cisco Software Central](#) で、Cisco vEdge 5000 デバイスへのアクセスに必要なスマートアカウントおよびバーチャルアカウントを使用して **Plug and Play Connect** にログインします。
2. [Devices] リストで、Cisco vEdge 5000 デバイスのシリアル番号をクリックします。
[Device Information] が表示されます。
3. [Device Information] ダイアログボックスで、デバイスの**公開キー**が使用可能かどうかを確認します。
4. 公開キーを使用できない場合は、**公開キー**を追加します。
 1. [Devices] リストで、チェックボックスを使用して Cisco vEdge 5000 デバイスを選択します。
 2. [Edit] をクリックします。
[Edit Devices] ページが表示されます。
 3. [Selected Devices] エリアで、[Public Key] 列の [view/edit] をクリックします。
[Public Key] ダイアログボックスが表示されます。
 4. テキストボックスに公開キーを入力するか、[Browse] をクリックして公開キーを含むファイルをアップロードします。
 5. [OK] をクリックして公開キーを保存し、ダイアログボックスを閉じます。
 6. [Edit Devices] ページで、[Submit] をクリックして公開キーを Cisco vEdge 5000 デバイスにアタッチします。

ブートストラップ手順

オンサイトブートストラッププロセスには、ブート可能 USB ドライブから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。Cisco vEdge 5000 デバイスは、起動時に、構成ファイルの情報を使用してオーバーレイネットワークに接続します。

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Devices] > [WAN Edge List]** の順に選択します。
2. **[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 Cisco vEdge 5000 シリアル番号ファイルを選択します。 **[Validate the uploaded vEdge list and send to controllers]** を選択し、**[Upload]** をクリックします。

WAN Edge リストがコントローラにアップロードされます。

Cisco vEdge 5000 デバイスが **WAN Edge** リストに追加されます。
4. デバイスをデバイス構成テンプレートにアタッチします。
 1. Cisco SD-WAN Manager 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。
 3. 目的のテンプレートについて、**[...]** をクリックし、**[Attach Devices]** を選択します。**[Attach Devices]** ダイアログボックスが開きます。
 4. **[Available Devices]** 列で、グループを選択し、検索して Cisco vEdge 5000 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 **[Selected Devices]** 列に移動します。
 6. **[Attach]** をクリックします。

構成テンプレートはデバイス用にスケジュールされています。
5. 新しく追加されたデバイスのブートストラップ構成を生成します。
 1. Cisco SD-WAN Manager 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、Cisco vEdge 5000 デバイスを選択します。
 3. 選択したデバイスについて、**[...]** をクリックし、**[Generate Bootstrap Configuration]** を選択します。
 4. **[Generate Bootstrap Configuration]** ダイアログボックスで、**[Cloud-Init(Encrypted OTP)]** を選択し、**[OK]** をクリックします。
 5. **[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、**<ChassisNumber>.cfg** 形式のファイル名を付けてファイルを保存します。
 6. **<ChassisNumber>.cfg** ファイルをブート可能 USB ドライブにコピーします。



- (注)
- Cisco vEdge 5000 デバイスがドライブを認識して自動マウントするには、USB ドライブが FAT-32 フォーマットである必要があります。
 - <ChassisNumber>.cfg ファイルを USB ドライブのホームディレクトリまたは親ディレクトリにコピーします。

6. Cisco vEdge 5000 シリアル番号ファイルおよび OTP 情報をコントローラに送信します。

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Certificates] > [WAN Edge List]** の順に選択します。
2. **[Send to Controllers]** をクリックして、すべてのコントローラの WAN Edge リストを同期させます。

デバイスシリアル番号ファイルおよび OTP 情報がコントローラに送信されます。

3. (任意) **show orchestrator valid-vedges hardware-installed-serial-number prestaging** コマンドを使用して、コントローラの WAN Edge リストを確認します。

```
vbond# show orchestrator valid-vedges hardware-installed-serial-number prestaging
```

```

HARDWARE

      INSTALLED      SUBJECT
      SERIAL         SERIAL
CHASSIS NUMBER     SERIAL NUMBER                VALIDITY  ORG
      NUMBER         NUMBER

-----
193A0122170001  deaedef5d39919454fdfcc8470eccd8d8  valid      vIPtela Inc
Regression prestaging N/A

```

7. Cisco SD-WAN リリース 20.3.1 以降のデフォルトイメージを使用して、Cisco vEdge 5000 デバイスの工場出荷時設定へのリセットを実行します。
8. Cisco vEdge 5000 デバイスが「稼働中」（LCD ディスプレイにステータスが「System: Up」と表示されます）のときに、<ChassisNumber>.cfg ファイルが保存された USB ドライブを挿入します。

デバイスは、USB ドライブから <ChassisNumber>.cfg ファイルを読み取ります。組織名、Cisco SD-WAN Validator の IP アドレス、OTP トークン、およびエンタープライズ ルート CA は、構成ファイルから取得されます。

1. (任意) デバイスで **show control local-properties** コマンドを発行して、構成ファイルから取得された情報を検証します。
2. (任意) デバイスの WAN インターフェイスに DHCP を介して IP アドレスが割り当てられていない場合、静的 IP アドレスと、コントローラに到達するために必要なルーティング情報を設定します。

デバイスは、OTP を使用した認証後に Cisco SD-WAN Validator および Cisco SD-WAN Manager に接続します。

デバイスは、Cisco SD-WAN Manager 構成テンプレートからシステム IP アドレスとサイト ID を取得します。Cisco SD-WAN Manager でテンプレートが設定されていない場合は、デバイスで必要なシステム構成を設定します。

デバイスが Cisco SD-WAN Manager に接続した後に、Cisco SD-WAN Manager はエンタープライズ証明書署名要求 (CSR) を取得します。Cisco SD-WAN Manager メニューから、**[Configuration] > [Certificates] > [WAN Edge List]** の順に選択すると、デバイス証明書の状態が「CSR」と表示されます。

9. CSR をダウンロードします。
 1. Cisco SD-WAN Manager 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 Cisco vEdge 5000 デバイスを選択します。
 3. 選択したデバイスについて、[...] をクリックし、**[View Enterprise CSR]** を選択します。
 4. CSR をダウンロードするには、**[Download]** をクリックします。
10. 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。
11. 証明書をデバイスにインストールするには、次の手順を実行します。
 1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Certificates] > [Controllers]** の順に選択します。



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、**[Controllers]** タブの名前が **[Control Components]** タブに変更されました。

2. 画面の右上隅にある **[Install Certificate]** ボタンをクリックします。
3. **[Install Certificate]** 画面で、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。

インストールされているデバイスの証明書シリアル番号がコントローラで更新されます。

Cisco SD-WAN Manager メニューから、**[Configuration] > [Certificates] > [WAN Edge List]** の順に選択すると、デバイス証明書の状態が「installed」と表示されます。

12. (任意) コントローラの WAN Edge リストを調べて、デバイスのシリアル番号がインストールされていることを確認します。

```
vbond# show orchestrator valid-vedges hardware-installed-serial-number 12399910
```

				HARDWARE INSTALLED SERIAL NUMBER	SUBJECT SERIAL NUMBER
CHASSIS	NUMBER	SERIAL NUMBER	VALIDITY	ORG	
193A0122170001	18DB5D4F	valid	vIPtela Inc Regression	12399910	N/A

13. USB ドライブをデバイスから取り外します。

結果

- Cisco vEdge 5000 デバイスが、SHA2 エンタープライズ証明書を使用してオーバーレイネットワークに追加され、コントローラに接続されます。
- デバイスは、再起動、ソフトウェアアップグレード、または Cisco SD-WAN リリース 20.3.1 以降のリリースへのソフトウェアダウングレードの後に、インストールされた SHA2 エンタープライズ証明書を使用します。SHA1 証明書の使用は無効になります。

CLI を使用した Cisco IOS XE Catalyst SD-WAN デバイスのブートストラップファイルの生成

Cisco Catalyst SD-WAN コントローラとの接続を確立するには、デバイスに最小限の設定が必要です。ほとんどの場合、この最小限のブートストラップ設定（MBC）は、最初はプラグアンドプレイ（PnP）によって提供できます。ただし、リモートサイトで PnP を使用しないほうがよい場合など、状況によっては、デバイスをコントローラに接続できる保存済みのブートストラップ設定があると便利です。

request platform software sdwan bootstrap-config save コマンドを実行すると、デバイス設定がブートフラッシュに保存されます。このコマンドは設定を保存するためにいつでも使用できますが、その目的は、設定全体が失われたり削除されたりした場合に、デバイスがコントローラに再接続できるようにする最小限のブートストラップ設定（MBC）ファイルを保存することです。

デバイスをセットアップするときに、コントローラに接続するために必要な詳細を設定に追加し、このコマンドを使用して MBC を保存します。ファイルは次の場所に保存されます。

```
bootflash:/ciscosdwan.cfg
```

前提条件

- デバイスを認証するために、コントローラ ルート証明書が Cisco IOS XE Catalyst SD-WAN デバイス にインストールされていること。
- デバイスはそのインターフェイスの 1 つを介して WAN に物理的に接続されていること。

手順

1. Cisco IOS XE Catalyst SD-WAN デバイス で、次のように設定して、Cisco SD-WAN Manager への接続を確立します。

- システム IP アドレス
- ドメイン ID
- サイト ID
- sp-organization-name
- organization-name
- Cisco SD-WAN Validator の IP アドレスおよびポート番号
- GRE または IPSEC として設定されたカプセル化を使用したトンネル

例 :

```
system
system-ip 10.0.0.10
domain-id 1
site-id 200
admin-tech-on-failure
sp-organization-name CiscoISR
organization-name CiscoISR
vbond 10.0.100.1 port 12346
!
interface Tunnel1
no shutdown
ip unnumbered GigabitEthernet0/1/0
tunnel source GigabitEthernet0/1/0
tunnel mode sdwan
exit
sdwan
interface GigabitEthernet0/1/0
tunnel-interface
encapsulation ipsec
exit
exit
commit
```

2. **show sdwan control connections** を使用して Cisco SD-WAN Manager、Cisco SD-WAN コントローラ、および Cisco SD-WAN Validator への接続を確認します。
3. **request platform software sdwan bootstrap-config save** コマンドを使用して、ブートストラップファイルをデバイスのブートフラッシュに保存します。

例 :

```
Device#request platform software sdwan bootstrap-config save
Saving bootstrap file 'bootflash:/ciscosdwan.cfg'...
Done
```

設定ファイルは次の場所に保存されます。

bootflash:/ciscosdwan.cfg

ワンタッチプロビジョニング：汎用ブートストラップ構成を使用した Cisco IOS XE Catalyst SD-WAN デバイスのオンボード

表 4: 機能の履歴

機能名	リリース情報	説明
ワンタッチプロビジョニング：汎用ブートストラップ構成を使用した Cisco IOS XE Catalyst SD-WAN デバイスのオンボード	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	Cisco SD-WAN Manager で汎用ブートストラップ構成を生成し、この構成を使用して複数の Cisco IOS XE Catalyst SD-WAN デバイスをオンボードできます。汎用ブートストラップ構成でデバイスを起動すると、デバイスは要求されていない WAN エッジデバイスとして Cisco SD-WAN Manager にリストされます。オンボーディングを完了するには、Cisco SD-WAN Manager でデバイスを要求し、システムの IP アドレスとサイト ID を設定するデバイステンプレートを添付します。

汎用ブートストラップ構成の概要

Cisco IOS XE Catalyst SD-WAN デバイスを Cisco Catalyst SD-WAN オーバーレイネットワークにオンボードするには、Cisco SD-WAN Manager でブートストラップ構成を生成し、この構成でデバイスを起動します。デバイスが Cisco SD-WAN Manager に接続されたら、Cisco SD-WAN Manager GUI を使用してオンボーディングを完了します。ブートストラップ構成にはデバイス固有の構成設定が含まれているため、オンボードする必要があるデバイスごとにブートストラップ構成を生成する必要があります。Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降、汎用ブートストラップ構成を使用して、複数の Cisco IOS XE Catalyst SD-WAN デバイスをオンボードできます。

汎用ブートストラップ構成では、デバイス固有の詳細（デバイスの UUID など）が省略され、Cisco SD-WAN Validator に接続するために Cisco IOS XE Catalyst SD-WAN デバイスが使用できる設定が提供されます。デバイスが Cisco SD-WAN Validator に接続すると、デバイスは Cisco SD-WAN Manager 上の要求されていない WAN エッジデバイスとして表示されます。オンボーディングを完了するには、Cisco SD-WAN Manager でデバイスを要求し、システム IP とサイト ID を設定するデバイステンプレートを添付する必要があります。Cisco SD-WAN Manager は汎用ブートストラップ構成の一部としてデバイスにインストールされている証明書を使用してデバイスを認証します。

汎用ブートストラップ構成には、次のものが含まれます。

- 組織名
- Cisco IOS XE Catalyst SD-WAN デバイス で有効にする WAN インターフェイス
- Cisco SD-WAN Validator の IP アドレス
- デバイスを認証するための Cisco SD-WAN Manager 署名付き証明書。

汎用ブートストラップ構成を使用してデバイスをオンボードするには、デバイスをインストールするブランチネットワークに Dynamic Host Configuration Protocol (DHCP) サーバーが必要です。汎用ブートストラップ構成では、WAN インターフェイスに IP アドレスを割り当てません。代わりに、WAN インターフェイスで DHCP クライアントを有効にして、インターフェイスがブランチネットワークの DHCP サーバーから IP アドレスを取得できるようにします。

汎用ブートストラップ構成の仕組み

1. Cisco SD-WAN Manager で汎用ブートストラップ構成を生成するときに、Cisco IOS XE Catalyst SD-WAN デバイス で VPN 0 (WAN) インターフェイスとして機能するインターフェイスを選択します。
2. 汎用ブートストラップ構成ファイルをデバイスのブートフラッシュにコピーし、デバイスをリセットします。リセット時に、デバイスは汎用ブートストラップ構成で初期化されます。
3. ブートストラップ構成により、指定された VPN 0 インターフェイスで DHCP クライアントが有効になります。インターフェイスは、ネットワーク内の DHCP サーバーから IP アドレスと関連する詳細を取得します。
4. VPN 0 インターフェイスを介して Cisco SD-WAN Validator に接続するデバイスは、Cisco SD-WAN Validator および Cisco SD-WAN Manager で要求されていない WAN エッジデバイスとしてリストされています。
5. Cisco SD-WAN Manager でデバイスを要求すると、Cisco SD-WAN Manager はブートストラップ構成の一部としてデバイスにインストールされた証明書を使用してデバイスを認証します。認証後、デバイスは Cisco SD-WAN Manager および Cisco SD-WAN Validator の有効な WAN エッジデバイス間にリストされます。
6. システム IP とサイト ID を含むテンプレートを添付して、デバイスにプッシュします。
7. デバイスは Cisco SD-WAN コントローラ への制御接続を確立し、オーバーレイネットワークに追加されます。

汎用ブートストラップ構成を使用した Cisco IOS XE Catalyst SD-WAN デバイス へのオンボード

1. ワンタッチプロビジョニングの有効化：
 1. (Cisco Catalyst SD-WAN Manager リリース 20.12.x 以前) Cisco SD-WAN Manager のメニューで、**[Administration]** > **[Settings]** の順に選択します。
 2. **[One Touch Provisioning]** が **[Enabled]** になっているか確認します。[Enabled] になっている場合は、ステップ 2 に進みます。

3. [One Touch Provisioning] が [Disabled] になっている場合は、[Edit] をクリックします。
4. [Enable Claim WAN Edges] 設定で、[Enabled] を選択して [Save] をクリックします。
2. Cisco SD-WAN Manager メニューから、[Configuration] > [Devices] > [WAN Edge List] の順に選択します。
3. [Export Bootstrap Configuration] をクリックします。
 1. [Export Bootstrap Configuration] ダイアログボックスで、[VPN0 Interface name] を入力します。



(注) VPN 0 インターフェイス名は、Cisco IOS XE Catalyst SD-WAN デバイス 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インターフェイス名を指定します。

2. [Generate Generic Configuration] をクリックします。
4. 汎用ブートストラップ構成ファイルを保存します。
ファイルには <filename>.cfg の形式で名前が付けられます。
5. 汎用ブートストラップ構成ファイルの名前を ciscosdwan.cfg に変更します。
6. ciscosdwan.cfg ファイルをブート可能な USB ドライブまたはデバイスのブートフラッシュにコピーします。
7. USB ドライブを使用している場合は、USB ドライブをデバイスに接続します。
8. CLI で次のコマンドを発行して、デバイスソフトウェア構成をリセットします。

```
Device# request platform software sdwan config reset
```

```
Device# reload
```



(注) 設定リセットを実行すると、新しいタイプ 6 マスターキーが生成されます。したがって、ブートストラップ設定ファイルを保護している現在のパスワードがプレーンテキストであり、タイプ 6 キーが含まれていないことを確認してください。ブートストラップ設定パスワードにタイプ 6 のキーが含まれていると、デバイスのリセットが失敗します。

9. デバイスを再起動します。
 - 再起動中、デバイスは USB ドライブまたはブートフラッシュから構成ファイルを読み取り、構成を適用します。

この構成により、VPN0 インターフェイスが有効になり、インターフェイスで DHCP クライアントが初期化されます。インターフェイスは、ネットワーク内の DHCP サーバーから IP アドレスを取得します。

デバイスが Cisco SD-WAN Validator に接続し、Cisco SD-WAN Validator および Cisco SD-WAN Manager で要求されていない WAN エッジデバイスとしてリストされます。

- Cisco SD-WAN Validator で、**show orchestrator unclaimed-vedges** コマンドを使用して、要求されていない WAN エッジデバイスを表示できます。
- Cisco SD-WAN Manager で、**[Configuration] > [Devices] > [Unclaimed WAN Edges]** を選択して、要求されていない WAN エッジデバイスを表示できます。

デバイスが要求されていない WAN エッジデバイスとしてリストされていない場合は、デバイスが Cisco SD-WAN Validator に接続できるか確認し、接続の問題を修正します。

10. Cisco SD-WAN Manager でデバイスを要求します。

Cisco SD-WAN Manager メニューから、**[Configuration] > [Devices] > [Unclaimed WAN Edges]**の順に選択します。

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

- デバイスは、[Unclaimed WAN Edges] から削除され、[WAN Edge List] にリストされます。
- Cisco SD-WAN Validator で、デバイスが有効な WAN エッジデバイスとして表示されます。**show orchestrator valid-vedges** コマンドを発行すると、有効な WAN エッジデバイスを表示できます。

11. 構成テンプレートをデバイスに添付します。

1. テンプレートにシステム IP アドレスとサイト ID が含まれていることを確認してください。
2. テンプレートをデバイスにプッシュします。

結果

デバイスが Cisco SD-WAN コントローラ に接続し、オーバーレイネットワークに追加されます。

デバイスが制御接続を確立し、オーバーレイネットワークの一部であることを確認するには、Cisco SD-WAN Manager メニューから、**[Monitor] > [Overview]**の順に選択し、[WAN Edges] 領域の番号をクリックします。



- (注) Cisco vManage リリース 20.6.x 以前の場合：デバイスが制御接続を確立し、オーバーレイネットワークの一部であることを確認するには、Cisco SD-WAN Manager メニューから、**[Dashboard] > [Main Dashboard]**の順に選択し、[Summary Pane] ペインで [WAN Edge Devices] をクリックします。

汎用ブートストラップ構成を使用してオンボードされた Cisco IOS XE Catalyst SD-WAN デバイスを削除する

1. テンプレートからデバイスを切り離します。
 1. Cisco SD-WAN Manager 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、デバイスに添付されている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. 選択したテンプレートについて、**[...]** をクリックし、**[Detach Devices]** を選択します。
4. **[Available Devices]** 列で、テンプレートから切り離す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 **[Selected Devices]** 列に移動します。
6. **[Detach]** をクリックします。

2. SSH を使用して、デバイスに接続します。デバイスの SSH ターミナルから、次のコマンドを使用して VPN 0 WAN インターフェイスをシャットダウンします。

```
Device(config)# interface vpn0-interface-name
Device(config-if)# shutdown
```

3. デバイスを無効にします。
 1. Cisco SD-WAN Manager のメニューから **[Configuration] > [Certificates]** の順に選択します。
 2. **[WAN Edge List]** をクリックし、無効にするデバイスを選択します。
 3. **[Validate]** 列で、**[Invalid]** をクリックします。
 4. **[OK]** をクリックして、無効な状態への移行を確認します。
 5. **[Send to Controllers]** をクリックして、無効化されたデバイスのシャシー番号とシリアル番号をネットワーク内のコントローラに送信します。Cisco SD-WAN Manager にプッシュ操作のステータスを示す **[Push WAN Edge List]** 画面が表示されます。
4. WAN エッジデバイスを削除します。
 1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Devices]** の順に選択します。
 2. **[WAN Edge List]** をクリックして、削除するデバイスを選択します。
 3. 選択したデバイスについて、**[...]** をクリックし、**[Delete WAN Edge]** を選択します。
 4. **[OK]** をクリックして、デバイスの削除を確認します。

Cisco SD-AVC のインストール (Cisco vManage 20.1.1 以前)



- (注) Cisco vManage リリース 20.3.1/Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降、Cisco SD-AVC のインストールが変更されました。「[Cisco SD-AVC のインストール \(Cisco vManage リリース 20.3.1 以降\) \(60 ページ\)](#)」を参照してください。

概要

18.4 リリース以降、Cisco Catalyst SD-WAN は任意でシスコのソフトウェア定義型 Application Visibility and Control (SD-AVC) を Cisco IOS XE Catalyst SD-WAN デバイス に組み込むことができます。SD-AVC ネットワークサービスは、Cisco SD-WAN Manager 内部のコンテナとして動作します。

この機能の利点

Cisco SD-AVC は、ネットワーク内のデバイスで動作する Cisco NBAR2 およびその他のコンポーネントを使用して、次の機能を提供します。

- 可視性、分析、アプリケーション認識型ルーティング、およびアプリケーションベースのポリシー (QoS やアプリケーションベースのファイアウォールポリシーなど) のためのネットワーク アプリケーション トラフィックの認識。
- ネットワークレベルでの分析。

Cisco SD-WAN Manager の Cisco SD-AVC インストール要件

次の表に、SD-AVC のインストール要件を示します。

Cisco SD-WAN Manager インストールのシナリオ	要件
クラウドベースサーバー上の Cisco vManage 18.4 (シスコのクラウド運用チームによって完全に設定された状態で提供されます)	SD-AVC パッケージは、シスコのクラウド運用チームによって事前インストールされます。
自己管理型クラウドまたはローカルサーバー上の Cisco vManage 18.4	以下の説明に従って SD-AVC パッケージをインストールします。
以前のバージョンの Cisco SD-WAN Manager から Cisco vManage 18.4 へのアップグレード	以下の説明に従って SD-AVC パッケージをインストールします。

Cisco SD-WAN Manager での SD-AVC の有効化

前提条件

- SD-AVC ネットワークサービスの最新のコンテナイメージをダウンロードします。Cisco SD-WAN Manager をホスティングしているサーバー上のアクセス可能な場所にファイルを保存します。このコンテナは手続きに必要です。コンテナをダウンロードするには、[Cisco Software Download] ページを開き、「SD-WAN」と入力します。結果から [Software-Defined WAN (SD-WAN)] を選択し、[SD-WAN] を選択します。ダウンロード可能なソフトウェアパッケージで、[SD-AVC] を選択します。
- SD-WAN トポロジに含まれるネットワーク内のルータに DNS サーバーが設定されていることを確認します。
- Cisco SD-WAN Manager が動作する仮想マシンには、SD-AVC ネットワークサービス専用で利用できる次のリソースが必要です。
 - vCPU: 4
 - RAM : 5 GB
 - ストレージ : 40 GB

手順

1. ダウンロードした SD-WAN イメージがお使いの Cisco SD-WAN Manager バージョンと互換性があることを確認してください。
 1. 次の API を使用して、互換性のあるイメージのチェックサムを表示します。
`https://[vManage-IP-address]/dataservice/sdavic/checksum`
例 : `https://10.0.0.1/dataservice/sdavic/checksum`
 2. ダウンロードしたイメージのチェックサムがこのチェックサムと一致することを確認します。
2. SD-AVC 仮想サービスパッケージを Cisco SD-WAN Manager にアップロードするには、次の手順を実行します。
 1. [Cisco SD-WAN Manager] メニューから、[Maintenance] > [Software Repository] の順に選択します。
 2. [Virtual Images] をクリックし、[Upload Virtual Image] を選択して SD-AVC パッケージをアップロードします。
3. Cisco SD-WAN Manager メニューから、[Administration] > [Cluster Management] ページの順に選択します。
4. 目的のホスト (SD-AVC を有効にする Cisco SD-WAN Manager ポータル) で、[...] をクリックし、[Edit] を選択します。

5. [Edit Cisco SD-WAN Manager] ダイアログボックスで、Cisco SD-WAN Manager ログイン情報を使用してユーザー名とパスワードを入力します。
6. [Enable SD-AVC] のチェックボックスをオンにします。[Update] をクリックします。
7. デバイスを再起動して変更をデバイスに適用する前に、確認を求めるプロンプトが Cisco SD-WAN Manager から表示されます。[OK] をクリックして確定します。
8. 再起動後、Cisco SD-WAN Manager が自動的に起動し、SD-AVC アクティベーションの進行状況が表示されます。アクティベーションが完了するまで待ちます。
9. (オプション) インストールが完了したら、Cisco SD-WAN Manager により SD-AVC 仮想サービスがインストールされ、正しく動作していることを確認できます。
 1. Cisco SD-WAN Manager メニューから、[Administration] > [Cluster Management] の順に選択します。
 2. [Service Configuration] の表の Cisco SD-WAN Manager 行で、SD-AVC に緑色のチェックマークが表示されていることを確認します。

Cisco SD-WAN Manager コマンドの詳細については、『Cisco SD-WAN Manager Command Reference』を参照してください。

Cisco IOS XE Catalyst SD-WAN デバイス での SD-AVC の有効化

Cisco IOS XE Catalyst SD-WAN デバイス で SD-AVC を有効にするには、**アプリの可視性を有効にするローカライズされたポリシー**を作成し、そのポリシーを Cisco IOS XE Catalyst SD-WAN デバイス のテンプレートに適用します。

前提条件

- Cisco IOS XE Catalyst SD-WAN デバイス 用のテンプレートが存在すること（例：Cisco ASR 1001-X、Cisco ISR 4321）。
- TCP ポート 10501 の宛先トラフィックを許可する必要があります。

手順

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Policies] の順に選択します。
2. [Localized Policy] をクリックします。
3. ポリシーを追加してアプリケーションを有効にするには、次の手順に従います。
 1. [ポリシーの追加 (Add Policy)] をクリックします。
 2. [Policy Overview] 画面が表示されるまで、複数の画面 ([Create Groups of Interest]、[Configure Forwarding Classes/QOS]、[Configure Access Control Lists]、[Configure Route Policy]) で [Next] をクリックします。
 3. [Policy Overview] 画面で、ポリシー名とポリシーの説明を入力します。

4. [Application] を選択します。
5. ポリシーを保存します。
4. ローカライズされたポリシーをデバイステンプレートに追加するには、次の手順に従います。
 1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Templates]** の順に選択します。
 2. SD-AVC を有効にする必要があるデバイスで、[...] をクリックし、メニューから **[Edit]** を選択します。
 3. **[Additional Templates]** をクリックします。
 4. この手順の前のステップで作成したローカライズされたポリシーを追加します。
 5. **[Update]** をクリックして次の画面に進み、更新されたテンプレートをデバイスにプッシュします。
5. (オプション) 更新をデバイスにプッシュすると、次のいずれかのコマンドを使用して、デバイスの SD-AVC のステータスを確認できます。

```
show avc sd-service info summary
```

または

```
show avc sd-service info connectivity
```

Cisco SD-AVC のインストール (Cisco vManage リリース 20.3.1 以降)

Cisco vManage リリース 20.3.1 をインストールまたはアップグレードすると、Cisco SD-AVC がコンポーネントとして自動的にインストールされます。

Cisco SD-AVC の詳細については、[Cisco SD-AVC \(29 ページ\)](#) を参照してください。

Cisco SD-AVC、Cisco vManage リリース 20.3.1 以降の有効化

前提条件

Cisco Catalyst SD-WAN トポロジに含まれるネットワーク内のルータに DNS サーバーが設定されていることを確認します。



- (注) Cisco SD-AVC は、単一の Cisco SD-WAN Manager インスタンスのみで動作する必要があります。Cisco SD-WAN Manager クラスターでは、単一の Cisco SD-WAN Manager インスタンスのみで Cisco SD-AVC を有効にします。

Cisco SD-AVC を有効にするには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、[Administration] > [Cluster Management] の順に選択します。
2. 目的のホスト（SD-AVC を有効にするポータル）で、[...] をクリックし、[Edit] を選択します。
3. [Edit Manage] ポップアップウィンドウで、[Enable SD-AVC] のチェックボックスをオンにします。



- (注) [Edit Manage] ポップアップウィンドウには、アプリケーションサーバーを無効にするオプションがあります。アプリケーションサーバーを無効にした後、この方法を使用して後で他のサービスを有効にすることはできません。アプリケーションサーバーを無効にする必要がある場合は、他の機能を有効にするのと同時にアプリケーションサーバーを無効にすることはしないでください。

4. Cisco SD-WAN Manager のログイン情報を使用して、ユーザー名とパスワードを入力します。デバイスを再起動して変更を適用します。
5. 再起動後、Cisco SD-WAN Manager が自動的に起動し、SD-AVC アクティベーションの進行状況が表示されます。アクティベーションが完了するまで待ちます。
6. （オプション）インストールが完了したら、Cisco SD-WAN Manager により SD-AVC 仮想サービスがインストールされ、正しく動作していることを確認できます。
 1. Cisco SD-WAN Manager メニューから、[Administration] > [Cluster Management] の順に選択します。
 2. [Service Configuration] をクリックし、テーブルの [Cisco SD-WAN Manager] 行で、SD-AVC に緑色のチェックマークが表示されていることを確認します。

Cisco IOS XE Catalyst SD-WAN デバイス での SD-AVC の有効化

Cisco IOS XE Catalyst SD-WAN デバイス で SD-AVC を有効にするには、アプリの可視性を有効にするローカライズされたポリシーを作成し、そのポリシーを Cisco IOS XE Catalyst SD-WAN デバイスのテンプレートに適用します。

前提条件

- Cisco IOS XE Catalyst SD-WAN デバイス 用のテンプレートが存在すること（例：Cisco ASR 1001-X、Cisco ISR 4321）。
- TCP ポート 10501 の宛先トラフィックを許可する必要があります。

手順

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Policies]** の順に選択します。
2. **[Localized Policy]** をクリックします。
3. ポリシーを追加してアプリケーションを有効にするには、次の手順に従います。
 1. **[ポリシーの追加 (Add Policy)]** をクリックします。
 2. **[Policy Overview]** 画面が表示されるまで、複数の画面（**[Create Groups of Interest]**、**[Configure Forwarding Classes/QOS]**、**[Configure Access Control Lists]**、**[Configure Route Policy]**）で **[Next]** をクリックします。
 3. **[Policy Overview]** 画面で、ポリシー名とポリシーの説明を入力します。
 4. **[Application]** を選択します。
 5. ポリシーを保存します。
4. ローカライズされたポリシーをデバイステンプレートに追加するには、次の手順に従います。
 1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Templates]** の順に選択します。
 2. SD-AVC を有効にする必要があるデバイスで、**[...]** をクリックし、メニューから **[Edit]** を選択します。
 3. **[Additional Templates]** をクリックします。
 4. この手順の前のステップで作成したローカライズされたポリシーを追加します。
 5. **[Update]** をクリックして次の画面に進み、更新されたテンプレートをデバイスにプッシュします。
5. （オプション）更新をデバイスにプッシュすると、次のいずれかのコマンドを使用して、デバイスの SD-AVC のステータスを確認できます。

```
show avc sd-service info summary
```

または

```
show avc sd-service info connectivity
```

Cisco SD-AVC Cloud Connector、Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降の有効化

表 5: 機能の履歴

機能名	リリース情報	説明
Cisco SD-AVC Cloud Connector を有効にするための新しい手順	Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.14.1	このリリースでは、 [Administration]>[Settings] の [Cloud Services] オプションから Cisco SD-AVC Cloud Connector を有効にするための新しい手順が導入されています。このリリース以降、Cloud Connector を有効にするために、OTP や TAC ケースをオープンする必要はありません。

Cisco Catalyst SD-WAN Manager リリース 20.14.1 より前は、Cloud Connector を有効にするために、クライアント ID、クライアントシークレットのログイン情報、および場合によってはクラウドゲートウェイの URL と OTP が必要でした。Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降、**[Cloud Services]** ページを使用して Cisco SD-AVC Cloud Connector を設定できます。この機能を使用すると、SD-AVC Cloud Connector を有効にするために、OTP を取得したり、TAC ケースを個別に作成したりする必要はありません。

前提条件

Cloud Connector を有効にするには、**[Administration] > [Cluster Management]** で Cisco SD-AVC を有効にします。

クラウドサービスを使用した Cisco SD-AVC Cloud Connector の有効化

1. Cisco SD-WAN Manager メニューから、**[Administration] > [Settings]** の順に選択します。
2. **[Cloud Services]** をクリックします。
3. **[Cloud Services]** タブで **[Cloud Services]** を有効にします。
4. フィールドにスマートアカウントのログイン情報を入力します。
5. (任意) **[Analytics]** を有効にします。



(注) Cisco Catalyst SD-WAN Analytics を展開し、Cisco SD-WAN Manager によって到達可能であることを確認した場合にのみ、このオプションを有効にします。

6. **[SD-AVC Cloud Connector]** を有効化します。



- (注) Cisco SD-WAN Manager がシスコによってクラウドでホストされている場合、このオプションは表示されず、クラウドサービスオプションを有効にした後で、Cloud Connector が自動的に有効になります。

7. [Save] をクリックします。

Cisco Catalyst SD-WAN Manager リリース 20.13.x を使用する Cisco SD-AVC Cloud Connector の有効化

表 6: 機能の履歴

機能名	リリース情報	説明
Cisco SD-AVC Cloud Connector	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	Cloud onRamp for SaaS で Office 365 トラフィックを管理できるようにする場合、Microsoft によって定義された Office 365 トラフィックカテゴリに従って、ベストパスの選択を一部の Office 365 トラフィックのみに適用するか、またはすべての Office 365 トラフィックを含めるように制限できます。 Cisco SD-AVC Cloud Connector では、この機能がサポートされています。
SD-AVC Cloud Connector を有効にするための更新	Cisco vManage リリース 20.10.1	このリリース以降、Cloud Connector を有効にするには、クライアント ID とクライアントシークレットではなく、クラウドゲートウェイの URL とワンタイムパスワード (OTP) が必要です。

はじめる前に

- Cisco vManage リリース 20.10.1 以前は、Cloud Connector を有効にするには、クライアント ID とクライアントシークレットのログイン情報が必要でした。Cisco vManage リリース 20.10.1 以降は、クラウドゲートウェイの URL と OTP が必要です。OTP を使用する利点は、クライアントシークレットとは対照的に、OTP が期限切れにならないことです。さまざまなリリース、アップグレードシナリオ、およびホスティングオプションに必要なログイン情報の詳細については、次の表を参照してください。
- Cisco SD-AVC Cloud Connector は、Cloud onRamp for SaaS が Office 365 トラフィックカテゴリに従って、Office 365 トラフィックを管理するために必要なコンポーネントです。

表 7: SD-AVC Cloud Connector を有効にするための要件

リリース	Cisco SD-WAN Manager ホスティング	Cloud Connector を有効にするための要件
Cisco vManage リリース 20.3.1 から Cisco vManage リリース 20.9.x へ	すべてのホスティングオプション	必要なログイン情報： Client ID クライアントシークレット (手順で説明されているように、ログイン情報をまだ持っていない場合は、Cisco API Console ページを開いて Cloud Connector ログイン情報を作成します。) (注) Cisco SD-WAN Manager 内に SD-AVC ログイン情報の有効期限が近づいていることを示すメッセージが表示されたら、Cisco API コンソールに戻り、新しい Cloud Connector ログイン情報を作成します。 その他の要件： ここで説明されているように、クラスタ管理で SD-AVC を有効にします。

リリース	Cisco SD-WAN Manager ホスティング	Cloud Connector を有効にするための要件
既存のインスタンスを以前のリリースから Cisco vManage リリース 20.10.1 にアップグレード	シスコホステッド	必要なログイン情報： - クラウドゲートウェイの URL： 使用： <code>datamanagement01.sdwan.cisco.com</code> - OTP： Cisco Catalyst SD-WAN Portal を使用して、OTP を取得します。詳細については、『Cisco Catalyst SD-WAN Portal Configuration Guide』を参照してください。 https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/self-serv-por/sdwan-ssp.html その他の要件： ここで説明されているように、クラスタ管理で SD-AVC を有効にします。 注： このシナリオでは、SD-AVC コンポーネントは以前のリリースとは異なる方法で動作します。そのため、Cisco SD-WAN Manager インスタンスで request nms all status コマンドを実行すると、「NMS SDAVC サーバー」コンポーネントが有効になっていないことが示されます。これは予期される動作であり、SD-AVC の問題を示すものではありません。「NMS SDAVC ゲートウェイ」コンポーネントが有効と表示されていることに注意してください。

リリース	Cisco SD-WAN Manager ホス ティング	Cloud Connector を有効にする ための要件
	自己管理型、パブリッククラ ウド、プライベートクラウ ド、またはオンプレミスでホ スト	

リリース	Cisco SD-WAN Manager ホスティング	Cloud Connector を有効にするための要件
		必要なログイン情報： • アップグレード時に Cloud Connector がすでに有効になっている場合、クライアント ID とクライアントシークレットのログイン情報は、クライアントシークレットの期限が切れるまで引き続き機能します。 クライアントシークレットが期限切れになると、期限切れを示すアラームが Cisco SD-WAN Manager に表示されます。この時点で、Cloud Connector を有効にするには、クラウドゲートウェイの URL と OTP が必要です。URL に <code>sdwanmanagementus01sdwancisco.com</code> を使用し、TAC ケースを開いて OTP を取得します。TAC ケースを開く方法については、このセクションの手順を参照してください。 • アップグレード時に Cloud Connector が有効になっていない場合、Cloud Connector を有効にするには、クラウドゲートウェイの URL と OTP が必要です。URL に <code>sdwanmanagementus01sdwancisco.com</code> を使用し、TAC ケースを開いて OTP を取得します。TAC ケースを開く方法については、このセクションの手順を参照してください。

リリース	Cisco SD-WAN Manager ホスティング	Cloud Connector を有効にするための要件
		その他の要件： Cloud Connector を有効にする前に、 ここで説明されている ように、クラスタ管理で SD-AVC を有効にします。

リリース	Cisco SD-WAN Manager ホスティング	Cloud Connector を有効にするための要件
Cisco vManage リリース 20.10.1 以降の新規インストール	シスコホステッド	必要なログイン情報： Cloud Connector はデフォルトで有効になっており、ログイン情報を手動で入力する必要はありません。必要に応じて、Cisco SD-WAN Self-Service Portal を使用して OTP を表示できます。詳細については、『Cisco Catalyst SD-WAN Portal Configuration Guide』を参照してください。 https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/self-serv-por/sdwan-ssp.html その他の要件： ここで説明されているように、クラスタ管理で SD-AVC を有効にします。 注： このシナリオでは、SD-AVC コンポーネントは以前のリリースとは異なる方法で動作します。そのため、Cisco SD-WAN Manager インスタンスで request nms all status コマンドを実行すると、「NMS SDAVC サーバー」コンポーネントが有効になっていないことが示されます。これは予期される動作であり、SD-AVC の問題を示すものではありません。「NMS SDAVC ゲートウェイ」コンポーネントが有効と表示されていることに注意してください。
	自己管理型、パブリッククラウド、プライベートクラウド、またはオンプレミスでホスト	

リリース	Cisco SD-WAN Manager ホスティング	Cloud Connector を有効にするための要件
		必要なログイン情報： - クラウドゲートウェイの URL： <code>sdwanmanagement-us01.sdwancisco.com</code> を使用 - OTP： TAC ケースを開いて OTP を取得します。TAC ケースを開く方法については、このセクションの手順を参照してください。 その他の要件： ここで説明されているように、クラスタ管理で SD-AVC を有効にします。

Cisco SD-AVC Cloud Connector の有効化

1. Cisco SD-WAN Manager メニューから、[Administration] > [Settings] の順に選択します。
2. [SD-AVC] をクリックし、[Cloud Connector] を有効にします。

(Cisco vManage リリース 20.10.x、Cisco vManage リリース 20.11.x、または Cisco Catalyst SD-WAN Manager リリース 20.12.x を使用している場合は、[Edit] をクリックし、[Cloud Connector] を有効にします。)

(Cisco vManage リリース 20.9.x 以前のリリースでは、オプションは [SD-AVC Cloud Connector] と呼ばれています。これらのリリースでは、[Edit] をクリックし、[Cloud Connector] を有効にします。)



- (注) Cisco SD-WAN Manager がシスコによってクラウドでホストされている場合、このオプションは表示されず、Cloud Connector が自動的に有効になります。

3. (この手順は Cisco vManage リリース 20.10.1 以降に適用され、Cisco SD-WAN Manager がシスコホステッドの場合は自動的に処理されます。)

さまざまなシナリオで SD-AVC Cloud Connector を有効にするための要件の詳細については、これらの手順の前にある [Before You Begin] セクションを参照してください。そこに記載されているように、Cloud Connector を有効にする前に、クラスタ管理で SD-AVC を有効にします。

クラウドゲートウェイの URL を入力する必要がある場合は、
datamanagement-us-01.sdwan.cisco.com を使用します

Cisco Catalyst SD-WAN Portal を使用して OTP を取得する必要がある場合は、詳細について
『Cisco Catalyst SD-WAN Portal Configuration Guide』を参照してください。

OTP を受け取るために TAC ケースを開く必要がある場合は、
<https://mycase.cloudapps.cisco.com/case> を開きます。OTP を受け取るためのワークフローには、次のものがが必要です。

- 資格情報。
- スマートアカウント。
- バーチャルアカウント。
- Cisco SD-WAN Manager で設定された組織名。
- Cisco SD-WAN Manager 地理的位置：南北アメリカ、欧州連合 (EU)、またはアジア太平洋 (APAC)。
- テクノロジー：オンプレミスインストールには Cisco Catalyst SD-WAN On-Prem を使用し、シスコがホストするインストールには Cisco Catalyst SD-WAN- Cisco-Hosted を使用します。
- サブテクノロジー：SDWAN クラウドインフラを使用します。

4. (Cisco vManage リリース 20.9.x 以前のリリースの場合) 次のログイン情報を入力します。
 - Client ID



(注) [Client ID] の (i) をクリックし、ブラウザウィンドウで [Cisco API Console] ページを開き、ログイン情報がない場合は Cloud Connector ログイン情報を作成します。 <https://apiconsole.cisco.com/>

- クライアントのシークレット (Client Secret)]
- [Organization Name] : [Cisco API Console] ページの [Name of your application] フィールドに入力したわかりやすい名前を使用します。

5. (Cisco vManage リリース 20.10.1 より以前のリリース) [Affinity] の場合、Cloud Connector データを保存する地理的な場所を選択できます。ヨーロッパに所在する組織の場合、EU 一般データ保護規則 (GDPR) 規則に従って、場所をヨーロッパに変更することを推奨します。
6. [Telemetry] の場合、必要に応じて、テレメトリデータの収集を無効化できます。



- (注) Cisco SD-WAN Manager がシスコによってクラウドでホストされている場合、このオプションは表示されず、テレメトリが自動的に有効になります。

Cisco API コンソールでのログイン情報の作成

次の手順は、Cisco API コンソールでログイン情報を作成する方法を示しています。便宜上、ここに手順が示されていますが、変更される可能性があります。

1. [Cisco API Console] ページで、シスコのログイン情報を使用してサインインします。
2. [My Apps and keys] をクリックします。新規アプリケーションの登録ページが開きます。
3. SD-AVC を登録するには、以下の手順に従います。
 1. アプリケーションの名前：わかりやすい名前を使用してください。後の手順のためにこの名前を保存します。
 2. [Application Type] 領域で、[Service] をクリックします。
 3. [Grant Type] 領域で、[Client Credentials] チェックボックスをオンにします。
 4. [Hello API] チェックボックスをオンにします。
 5. [Terms of Service] セクションで、チェックボックスをオンにして条件に同意します。
 6. [Register] をクリックします。[Cisco API Console] ページには、クライアント ID とクライアントシークレットの詳細が表示されます。このページを開いたままにして、手順を完了します。



- (注) Cisco SD-WAN Manager 内に SD-AVC ログイン情報の有効期限が近づいていることを示すメッセージが表示されたら、Cisco API コンソールに戻り、新しい Cloud Connector ログイン情報を作成します。

クラウドサービスの有効化

手順

- ステップ 1 Cisco SD-WAN Manager メニューから、[Administration] > [Settings] の順に選択します。
- ステップ 2 [Cloud Services] をクリックします。
- ステップ 3 [Cloud Services] タブで [Cloud Services] を有効にします。

ステップ 4 フィールドにスマートアカウントのログイン情報を入力します。

ステップ 5 (任意) [Analytics] を有効にします。

(注)

Cisco SD-WAN Analytics を展開し、Cisco SD-WAN Manager によって到達可能であることを確認した場合にのみ、このオプションを有効にします。

ステップ 6 [Save] をクリックします。

Cisco IOS XE ルータのソフトウェアのインストールとアップグレード

同じルータに最大 2 つの Cisco Catalyst SD-WAN イメージをインストールできます。

サポートされているハードウェア プラットフォームとインターフェイスモジュール

サポートされているハードウェア プラットフォームとインターフェイスモジュールについては、[リリースノート](#)を参照してください。



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a の Cisco IOS XE Catalyst SD-WAN デバイスの場合、PnP または自動インストールプロセス完了後に .bin ファイルを使用してデバイスを起動すると、デバイスは Day-0 構成で起動します。その後、デバイスが自動的にリロードして、インストールモードになります。

サポートされる暗号モジュール

ASR 1000 シリーズのルータには、以下の暗号モジュールが必要です。

- ASR 1001-HX 用 ASR 1001HX-IPSECHW
- ASR 1002-HX 用 ASR 1002HX-IPSECHW

はじめる前に

オーバーレイネットワークに IOS XE ルータを展開する前に、次の点を確認してください。

- コントローラデバイス (Cisco SD-WAN Validator、Cisco SD-WAN Manager インスタンス、および Cisco SD-WAN コントローラ) が Cisco Catalyst SD-WAN ソフトウェアリリース 18.3 を実行していること。
- オーバーレイネットワークに IOS XE ルータと vEdge ルータの両方を展開する場合、vEdge ルータがリリース 17.2.1 以降の Cisco Catalyst SD-WAN ソフトウェアを実行していること。

これらのソフトウェアバージョンでは、vEdge と IOS XE ソフトウェアが相互運用でき、vEdge ルータと IOS XE ルータ間に BFD トンネルを確立できます。

- 同じサイトに IOS XE ルータと vEdge ルータの両方を展開する場合、vEdge ルータが Cisco Catalyst SD-WAN ソフトウェア リリース 18.3 を実行していること。
- ISR 4000 シリーズ ルータに少なくとも 4 GB の DRAM が搭載されていること。ルータには 8 GB の DRAM を搭載することをお勧めします。
- ASR 1000 Cisco SD-WAN Validator シリーズ ルータに少なくとも 8 GB の DRAM が搭載されていること。ASR 1002-HX ルータに少なくとも 16 GB の DRAM が搭載されていること。
- ルータブートフラッシュでは最小 1.5 GB のスペースが XE SD-WAN イメージに使用できます。Cisco IOX SD-WAN リリース 17.10 以降のルータブートフラッシュでは、ディスクスペースの半分以上が XE SD-WAN イメージに使用できます。
- エンタープライズルート証明書を使用してルータを認証する場合、XE SD-WAN ソフトウェアをインストールする前に、証明書がルータのブートフラッシュにコピーされていること。
- XE SD-WAN ソフトウェアをインストールする前に、サポートされていないすべてのモジュールをルータから取り外していること。サポートされるモジュールのリストについては、「サポートされるインターフェイスモジュール」および「サポートされる暗号モジュール」を参照してください。
- RP3 モジュールを搭載した Cisco ASR 1006-X の展開については、[RP3 モジュールを搭載した Cisco ASR 1006-X](#) を参照してください。
- 更新されたデバイスリストが Cisco SD-WAN Manager にアップロードされ、Cisco SD-WAN Validator に送信されていること。次の手順を実行します。
 1. システムプロンプトで **show crypto pki certificates CISCO_IDEVID_SUDI** コマンドを実行して、ルータのシャーシおよびボード ID のシリアル番号を取得します。ASR シリーズ ルータでリリース 16.6.1 以前を実行している場合は、**show sdwan certificate serial** コマンドを実行します。
 2. プラグアンドプレイ (PnP) Connect ポータルでルータのシリアル番号を追加します。詳細については、「IOS XE ルータの PnP ポータルへの追加」セクションを参照してください。
 3. Cisco SD-WAN Manager メニューから、**[Configuration] > [Devices]** を選択します。[Sync Smart Account] をクリックして、更新されたデバイスリストを Cisco SD-WAN Manager にダウンロードし、Cisco SD-WAN Validator に送信します。
- デバイス設定テンプレートは、Cisco SD-WAN Manager の **[Configuration] > [Templates]** を使用して作成され、ルータにアタッチされます。これにより、ルータが起動時に設定を取得し、完全な制御接続を確立できるようになります。

- ルータが 250 Mbps の単方向暗号化帯域幅を超えており、HSECK9 ライセンスがまだインストールされていない場合、ライセンスファイルはルータのブートフラッシュにコピーされ、ライセンスはルータのライセンス インストール ファイル パスにインストールされます。
- ASR 1000 シリーズ、ISR 1000 シリーズ、および ISR 4000 シリーズルータが、次の表に示すように、必要なバージョンの ROM モニタソフトウェア (ROMMON) を実行していること。ルータで実行中の ROMMON のバージョンを確認するには、システムプロンプトで **show rom-monitor** コマンドまたは **show platform** コマンドを実行します。

ハードウェア プラットフォーム	必要な ROM モニタ ソフトウェア バージョン
ASR 1000 シリーズ	16.3 (2r)
ISR1000 シリーズ	16.9 (1r)
ISR4000 シリーズ	16.7 (3r)

- ISRv ルータが、次の表に示すように、CIMC および NFVIS ソフトウェアの必要最小限のバージョンを実行していること。

ハードウェア プラットフォーム	CIMC	NFVIS
ISRv	324	3.8.1

Cisco IOS XE SD-WAN リリース 16.12 以前の Cisco IOS XE Catalyst SD-WAN ソフトウェアのダウンロード

Cisco IOS XE Catalyst SD-WAN ソフトウェアのダウンロード

シスコのサイトから Cisco IOS XE Catalyst SD-WAN ソフトウェアをダウンロードするには、次の手順を実行します。

- <https://www.cisco.com> にアクセスします。
- 左側のメニューから [Support & Downloads] をクリックします。
- [Products and Downloads] ページの [Downloads] 検索ボックスで、[Software-Defined WAN (SD-WAN)] を選択します。
- [Select a Product] ページの右端のペインで、[XE SD-WAN Routers] を選択します。
- 右端のペインから、ルータのモデルを選択します。
- 目的のソフトウェアリリースバージョンをクリックしてダウンロードします。ソフトウェアイメージ名の形式は、router-model-ucmk9.release-number です。

7. ソフトウェアイメージをローカルネットワークの HTTP または FTP ファイルサーバーにコピーします。

Cisco IOS XE SD-WAN リリース 16.12 以前の Cisco IOS XE Catalyst SD-WAN ソフトウェアのインストール

すべての新しい Cisco IOS XE Catalyst SD-WAN デバイスは、Cisco IOS XE Catalyst SD-WAN ソフトウェアがすでにインストールされた状態で出荷されます。

既存の Cisco IOS XE Catalyst SD-WAN デバイスがある場合は、次の手順に従って Cisco IOS XE Catalyst SD-WAN ソフトウェアをインストールします。Cisco IOS XE Catalyst SD-WAN イメージを使用してルータが再起動します。

1. シスコのサイトから Cisco IOS XE Catalyst SD-WAN ソフトウェアイメージをダウンロードします。
2. ファイルサーバーからデバイスのブートフラッシュに Cisco IOS XE Catalyst SD-WAN ソフトウェアイメージをアップロードします。次に FTP の構文例を示します。

```
Device# (config)# ip ftp source-interface interface
Device# copyftp:// username:password@server-IP/file-location bootflash:
TFTP:
Device(config)# ip tftp source-interface interface
Device(config)# ip tftp blocksize 8192
Device(config)# exit
Device#copy tftp: bootflash:
SCP (assumes SSH is enabled):
Device# configure terminal
Device# (config)# ip scp server enable
FileServer$ scp filenameusername@router-IP:/filename
```

3. デバイスが管理コンソールに接続されていることを確認します。
4. デバイスのブートフラッシュに保存できる現在の構成のバックアップを作成します。

```
Device# copy run bootflash:original-xe-config
```

5. 既存の boot ステートメントをすべて削除し、構成を保存します。

```
ISR4K# (config)# no boot system ...
ISR4K# wr mem
```

6. 次の出力で、BOOT 変数が空白であることを確認します。

```
ISR4K# show bootvar
BOOT variable =
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
Standby not ready to show bootvar
```

7. Cisco IOS XE Catalyst SD-WAN イメージを指す BOOT 変数を追加します。

```
Device(config)# boot system flash bootflash:
SDWAN-image
Device(config)# exit
ISR4K# write memory
```

8. BOOT 変数が Cisco IOS XE Catalyst SD-WAN イメージを指していることを確認します。

```
Device# show bootvar
BOOT variable = bootflash:isr4300-ucmk9.16.10.1a.SPA.bin,1;
CONFIG FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
Standby not ready to show bootvar
```

9. ルータから既存の構成をすべて削除します。

```
Device# write erase
```

10. config-register を 0x2102 に設定します。

```
Device# configure terminal
Deovce(config)# config-register 0x2102
Device(config)# end
```

11. config-register が 0x2102 に設定されていることと、それが次の再起動時に 0x2102 に設定されることを確認します。

```
Device# show bootvar
```

12. ルータを再起動します。

```
ISR4K# reload
Proceed with reload? [confirm] Yes
If prompted to save the configuration, enter No. The router reboots with the XE
SD-WAN image.
```

13. 初期構成ダイアログを開始するプロンプトが表示されたら、「No」と入力します。

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [Yes/No]: No
```

14. 自動インストールプロセスの終了を求められたら、「Yes」と入力します。

```
Would you like to terminate auto-install? [Yes/No]: Yes
```

15. ログインプロンプトで、デフォルトのユーザー名およびパスワード (**admin**) を使用してログインします。

デフォルトのパスワードは 1 回使用でき、その後は変更する必要があります。初期構成セッションがタイムアウトになったか、パスワードを変更して保存する前にセッションが中断または終了した場合、以降のログイン試行は失敗します。デバイスへのログインアクセスを復元するには、ROMMON モードのローカルコンソールからパスワードをデフォルト値にリセットする必要があります。その後、初期プロビジョニングプロセスを再開する必要があります。パスワードの復元については、[デフォルトパスワードの復元 \(85 ページ\)](#) を参照してください。

16. PnP を停止し、Cisco IOS XE Catalyst SD-WAN パッケージのインストールを許可します。

```
ISR4K# npa service discovery stop
```

17. **request platform software sdwan software upgarde-confirm** を使用して、Cisco IOS XE Catalyst SD-WAN デバイスのアップグレードを設定します。

```
Router# request platform software sdwan software upgrade-confirm
Router#
*Sep 21 00:26:29.242: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
```

```
install commit PACKAGE
*Sep 21 00:26:30.153: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine:
Completed install commit PACKAGE
Router#
```

18. **show sdwan software** の出力に、ユーザーとして CONFIRMED ステートが表示され、他の値が表示されないことを確認します。

```
Router# sh sdwan software
VERSION          ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
-----
16.12.1b.0.4    true   true     true      user       2019-09-21T00:24:22-00:00

Total Space:388M Used Space:86M Available Space:298M
```

19. **request platform software sdwan software reset** を使用して Cisco IOS XE Catalyst SD-WAN デバイスを設定します。

```
Router# request platform software sdwan software reset

*Sep 21 00:27:20.025: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install activate bootflash:isr4300-ucmk9.16.12.1b.SPA.bin
*Sep 21 00:27:43.105: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
*Sep 21 00:28:47.233: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine:
Completed install activate PACKAGE
*Sep 21 00:28:54.240: %PMAN-5-EXITACTION: R0/0:
pvp: Process manager
```



- (注) このイメージをインストールしたら、必ず、**config-transaction** コマンドを使用して CLI 構成モードを開始してください。**config terminal** コマンドは、Cisco Catalyst SD-WAN ルータではサポートされていません。



- (注) 古いイメージバージョンのフレッシュインストールへのダウングレードはサポートされていません。古いイメージの以前の既存バージョンにのみダウングレードできます。たとえば、Cisco IOS XE Catalyst SD-WAN 16.10.3 を Cisco IOS XE Catalyst SD-WAN デバイスにインストールしたことがなく、Cisco IOS XE Catalyst SD-WAN 16.11.1 リリースから Cisco IOS XE Catalyst SD-WAN 16.10.3 リリースにダウングレードしようとする、この操作はサポートされず、予期しない動作が発生します。ただし、以前に 16.10.3 イメージをインストールしている場合は、**request platform software sdwan activate** コマンドを使用して再アクティブ化できます。



- (注) データは、アップグレード時にのみ既存の Cisco Catalyst SD-WAN イメージから新しい Cisco Catalyst SD-WAN イメージに移行されます。アップグレードが完了すると、Cisco IOS XE Catalyst SD-WAN と Cisco vEdge デバイスの両方について、インストールされているイメージの異なるバージョンの間でデータが移行されることはありません。たとえば、以前に 19.2.4 をインストールしていて、20.3.2 が現在のアクティブイメージである場合、19.2.4 イメージをアクティブにすると、追加の構成が 20.3.2 から 19.2.4 に移行されません。

CLI を使用した IOS XE ルータの設定

Cisco IOS XE Catalyst SD-WAN デバイスが DHCP サーバーに接続されている場合、PnP は自動的に実行され、Cisco SD-WAN Manager は制御接続が稼働するとデバイスを自動的に設定します。制御接続が稼働しており、デバイスが検証されていることを確認するには、システムプロンプトで次のコマンドを入力します。

```
Device# show sdwan control connections
```

IOS XE ルータが DHCP サーバーに接続されていて、PnP を使用していない場合、または IOS XE ルータが WAN 上の DHCP サーバーに接続されていない場合は、次の手順に示すように、CLI を使用してルータを手動で設定します。

また、**system host-name hostname** コマンドを使用してホスト名を設定することもできます。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 SD-WAN Manager 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。このコマンドはデバイス CLI では使用できませんが、CLI デバイステンプレートを使用している場合は使用できます。

1. 管理コンソールを使用してルータに接続します。
2. PnP を停止して、CLI へのアクセスを許可します。

```
Device# pnpa service discovery stop
```

3. コンフィギュレーション モードに入ります。

```
Device# config-transaction
Device(config)#
```

4. システム IP アドレスを設定します。

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

Cisco SD-WAN Manager 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。

5. 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。

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

6. Cisco SD-WAN Validator の IP アドレスか、Cisco SD-WAN Validator を指す DNS 名を設定します。Cisco SD-WAN Validator の IP アドレスは、ルータが Cisco SD-WAN Validator 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。

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

7. 組織名を設定します。組織名は、オーバーレイネットワーク内のすべてのデバイスの証明書に含まれる名前です。組織名は、すべてのデバイスで同じにする必要があります。

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

8. オーバーレイ接続に使用する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 ID が、Cisco SD-WAN Manager によって自動的に割り当てられる他のインターフェイス ID と競合しないようにしてください。これは、構成プレビューで確認できます。


```
Device(config)# interface Tunnel #
Device(config-if)# ip unnumbered wan-physical-interface
Device(config-if)# tunnel source wan-physical-interface
Device(config-if)# tunnel mode sdwan
```



(注)

- 構成に Cisco SD-WAN Manager 機能テンプレートを使用している場合、トンネルインターフェイスは、使用されている WAN インターフェイスに基づいて自動的に割り当てられます。
- CLI モードから Cisco SD-WAN Manager モードに切り替えると、使用する WAN インターフェイスに基づき、トンネルインターフェイス番号が Cisco SD-WAN Manager によって自動的に割り当てられるため、設定したトンネルインターフェイスが変更される場合があります。トンネル番号の変更により、構成がプッシュされたときに、トンネルが停止してから再起動する可能性があります。

9. ルータが DHCP サーバーに接続されていない場合は、WAN インターフェイスの IP アドレスを設定します。

```
Device(config)# interface GigabitEthernet #
Device(config)# ip address ip-address mask
Device(config)# no shut
Device(config)# exit
```

10. トンネルパラメータを設定します。

```
Device(config)# sdwan
Device(config-sdwan)# interface WAN-interface-name
Device(config-interface-interface-name)# tunnel-interface
Device(config-tunnel-interface)# color color/path-name
Device(config-tunnel-interface)# encapsulation ipsec
```

11. ルータで IP アドレスが手動で設定されている場合は、デフォルトルートを設定します。

```
Device(config)# ip route 0.0.0.0 0.0.0.0 next-hop-ip-address
```

12. Cisco SD-WAN Validator アドレスがホスト名として定義されている場合は、DNS を設定します。

```
Device(config)# ip domain lookup
Device(config)# ip name-server dns-server-ip-address
```

13. 変更を保存して、コンフィギュレーション モードを終了します。

```
Device(config)# commit and-quit
Device# exit
```

14. エンタープライズルート CA によって署名された証明書を使用している場合は、その証明書をインストールします。

```
Device# request platform software sdwan root-cert-chain install bootflash:
certificate
```

15. 制御接続が稼働しており、ルータが検証されていることを確認します。

```
Device# show sdwan control connections
```

```
PEER      PEER PEER      SITE  DOMAIN  PEER      PEER PRIV  PEER      PEER
```

PUB TYPE	PORT LOCAL	SYSTEM COLOR	IP	ID	ID	PRIVATE IP	PORT	PUBLIC IP	PORT				
vsmart	dtls	192.168.1.2	10	1		172.1.1.3	12346	172.1.1.3	12346				
	biz-internet												
vbond	dtls	-		0	0	172.1.1.4	12346	172.1.1.4	12346				
	biz-internet												
vmanage	dtls	192.168.1.3	10	0		172.1.1.2	12346	172.1.1.2	12346				
	biz-internet												
				CONTROLLER GROUP									
PROXY	STATE	UPTIME	ID										

up		1:19:51:40	0										
up		1:19:51:45	0										
up		1:19:51:38	0										

これで、Cisco SD-WAN Manager テンプレートを使用して、ルータで SD-WAN 機能を設定できるようになりました。

IOS XE デバイスのプラグアンドプレイポータルへの追加

表 8: 機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN の オンプレミスの ZTP サー バー	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能により、オンプレミスのプ ラグアンドプレイ実装のサポートが Cisco IOS XE Catalyst SD-WAN ルータ に拡張されます。

プラグアンドプレイ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。

- デバイスが PNP ポータルに到達できる場合は、『[Cisco Plug and Play Support Guide for Cisco Catalyst SD-WAN Products](#)』を参照してください。
- デバイスが PNP ポータルにアクセスできない場合は、「[Cisco Catalyst SD-WAN Overlay Network Bring-Up Process](#)」の章の「[Start the Enterprise ZTP Server](#)」および「[Prepare Routers for ZTP](#)」を参照してください。



(注) デバイスが返品許可 (RMA) の期限に達している場合、デバイスの詳細は Cisco PNP にあります。ただし、これらのデバイスを Cisco SD-WAN Manager の RMA リストから削除することはできません。代わりに、Cisco SD-WAN Manager 管理者は、RMA に従って、返品されたデバイスを無効としてマークできます。

Cisco IOS XE リリース 17.2 以降については、「[Install and Upgrade Cisco IOS XE Release 17.2 and Later](#)」を参照してください。

ROMMON のアップグレードまたはダウングレード

ここでは、デバイスで実行されている ROM モニタ (ROMmon) のバージョンをアップグレードまたはダウングレードする方法について説明します。ROMmon のバージョンを、「はじめる前に」に示されている必要なバージョンに変更する必要がある場合は、この手順を実行します。

デバイスで実行されている ROMmon のバージョンを判別するには、次のコマンドを入力します。

```
Device# Show rom-monitor R0
```

ROMmon をアップグレードまたはダウングレードするには、次の手順を実行します。

1. 次のいずれかの操作を実行します。

1. SCP、FTP、TFTP、USB ドライブなどの方法を使用して、ROMmon ファイルをデバイスのブートフラッシュにロードします。
2. ルータへのアウトオブバンド管理アクセスがない場合は、次の例のように、Cisco SD-WAN Manager CLI を使用して ROMmon ファイルを転送します。

```
vManage# request execute vpn 0 scp -P 830 C1100-rommon-16-1r-SPA.pkg  
admin@router-ip-address:/bootflash/vmanage-admin/C1100-rommon-169-1r-SPA.pkg
```

2. 次のいずれかのアクションを実行して、ロードまたは転送した ROMmon ファイルがディレクトリ出力に表示されることを確認します。

1. ROMmon ファイルをデバイスのブートフラッシュにロードした場合は、次のコマンドを入力します。

```
Device# dir bootflash
```

2. Cisco SD-WAN Manager CLI を使用して ROMmon ファイルを転送した場合は、次のコマンドを入力します。

```
vManage# dir bootflash:vmanage-admin
```

3. 次のコマンドを入力して config-register を 0x2102 に設定します。

```
Device# config-register 0x2102
```

4. 次の例のように、upgrade コマンドを使用して、デバイスの ROMmon ファイルをアップグレード (またはダウングレード) します。

- ROMmon ファイルをデバイスのブートフラッシュにロードした場合の upgrade コマンドの例 :

```
Device# upgrade rom-monitor filename bootflash: C1100-rommon-169-1r-SPA.pkg R0
```

- Cisco SD-WAN Manager CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例 :

```
vManage# upgrade rom-monitor filename  
bootflash:vmanage-admin/C1100-rommon-169-1r-SPA.pkg R0
```

- アップグレードに関する一連のメッセージが表示され、ルータのプロンプトが表示されたら、次のコマンドを入力してルータをリロードします。

```
Device# Reload
```

- 次のコマンドを入力して、出力に ROMmon の新しいバージョンが表示されていることを確認します。

```
ISR4K# Show rom-monitor R0
```

工場出荷時の状態へのリセット

このセクションでは、工場出荷時設定へのリセット機能と、この機能を使用してルータを保護状態、または以前の完全に機能する状態に復元する方法について説明します。さまざまなプラットフォームでの工場出荷時設定へのリセット手順については、次を参照してください。

- [Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ](#)
- [Cisco 4000 シリーズ サービス統合型ルータ](#)
- [Cisco Cloud Services Router 1000V シリーズ](#)



- (注) Cisco IOS XE Catalyst SD-WAN ASR 1000 ルータで工場出荷時設定のリセットを実行するには、ルータがサブパッケージモードで起動されていることを確認してください。 **show version** コマンドを実行し、システムイメージファイルの出力を確認して、起動されたイメージを特定します。

```
Device# show version
Cisco IOS XE Software, Version BLD_POLARIS_DEV_LATEST_20200303_002119_V17_X_X_XX
Cisco IOS Software [Amsterdam], ASR1000 Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Tue 03-Mar-20 00:29 by mcpre
```

```
Cisco IOS-XE software, Copyright (c) 2005-2020 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
```

```
ROM: IOS-XE ROMMON
```

```
2KP-CEDGE uptime is 3 minutes
Uptime for this control processor is 5 minutes
System returned to ROM by Reload Command
System image file is "bootflash:packages.conf"
```

デフォルトパスワードの復元

Cisco IOS XE Catalyst SD-WAN デバイス のデフォルトのパスワードは **admin** です。このパスワードを初めて使用した後、管理者は新しいパスワードを作成する必要があります。初期構成セッションがタイムアウトになったか、新しいパスワードが作成される前にセッションが中断または終了した場合、以降のログイン試行は失敗します。この場合、デフォルトパスワードを復元する必要があります。

デバイスのデフォルトパスワードを復元するには、次の手順を実行します。

1. デバイスの電源を切り、入れなおします。
2. デバイスのローカルコンソールで、ROMMON モードを開始します。
3. 次のコマンドを入力して、**config-register** 値を **0x8000** に設定します。

```
rommon 1 > confreg 0x8000
```
4. デバイスの電源を切り、入れなおすことによって、更新を有効にします。
5. ユーザー名とパスワードとして「**admin**」を使用してデバイスにログインします。
6. デバイスのローカルコンソールで、SD-WAN 構成モードを開始します。
7. 次のコマンドを入力して、**config-register** 値を **0x2102** に設定します。

```
Device# confreg 0x2102
```
8. デバイスのローカルコンソールで、特権 EXEC モードを開始します。
9. 次のいずれかの操作を実行します。
 - リリース 16.10.4 以降の Cisco IOS XE SD-WAN 16.10 リリース、またはリリース 16.12.2 以降の Cisco IOS XE SD-WAN 16.12 リリースの場合：

```
Device# request platform software sdwan config reset
```

```
Device# reload
```
 - リリース 16.10.4 より前の Cisco IOS XE SD-WAN 16.10 リリース、または 16.12.2 より前の Cisco IOS XE SD-WAN 16.12 リリースの場合：

```
Device# request platform software sdwan software reset
```
10. デバイスが起動したら、新しい管理者パスワードを設定します。

vEdge ルータのソフトウェアのインストールとアップグレード

この記事では、すべての Cisco vEdge デバイス（Cisco SD-WAN Manager インスタンス、Cisco Catalyst SD-WAN 制御コンポーネント、Cisco SD-WAN Validator、および vEdge ルータ）にソ

ソフトウェアをインストールする方法と、Cisco Catalyst SD-WAN ソフトウェアをすでに実行しているデバイスでソフトウェアをアップグレードする方法について説明します。

ソフトウェアイメージの署名

Cisco Catalyst SD-WAN ソフトウェアイメージはデジタル署名されており、そのイメージが正式な Cisco Catalyst SD-WAN イメージであること、およびイメージが作成および署名されてからコードが変更または破損していないことが保証されます。標準の Cisco Catalyst SD-WAN ソフトウェアイメージはすべて署名されていますが、パッチイメージは署名されていません。標準ソフトウェアイメージは3つの数値フィールド（16.1.0 など）で識別され、パッチソフトウェアイメージは4つの数値フィールド（16.1.0.1 など）で識別されます。

署名されたイメージには失効メカニズムが含まれているため、バグまたはセキュリティ上の欠陥により危険であることが判明したイメージは、Cisco Catalyst SD-WAN が取り消すことができます。既知の脆弱性が存在する以前に署名されたイメージをインストールしようとすると、失効メカニズムにより攻撃から保護されます。

署名されたイメージを Cisco Catalyst SD-WAN デバイスにインストールすると、署名されていないイメージをデバイスにインストールできなくなります。

ソフトウェアイメージの署名は、リリース 16.1 以降で使用できます。

ソフトウェアバージョンの互換性

コントローラデバイス（Cisco SD-WAN Manager インスタンス、Cisco SD-WAN コントローラ、および Cisco SD-WAN Validator）のソフトウェアバージョンを、vEdge ルータを同じバージョンにアップグレードすることなく、アップグレードできます。ただし、コントローラデバイスで実行されているソフトウェアバージョンは、vEdge ルータで実行されているバージョンと互換性がある必要があります。

コントローラと vEdge ルータの互換性のあるバージョンのリストについては、[リリースノート](#)を参照してください。



(注) 同じタイプのすべてのコントローラデバイスは、同じソフトウェアバージョンを実行する必要があります。つまり、すべての Cisco SD-WAN Manager インスタンスで同じソフトウェアバージョンを実行し、すべての Cisco SD-WAN コントローラ で同じソフトウェアバージョンを実行し、すべての Cisco SD-WAN Validator で同じバージョンを実行する必要があります。

ソフトウェアのインストール

開始する前に、Cisco Catalyst SD-WAN サポートサイトからソフトウェアをダウンロードします。

最初にオーバーレイネットワークを起動するときに Cisco Catalyst SD-WAN デバイスにソフトウェアをインストールし、それらのデバイスをネットワークに追加します。

- Cisco SD-WAN Validator にソフトウェアをインストールするには、「ESXi での Cisco SD-WAN Validator VM インスタンスの作成」または「KVM での Cisco Catalyst SD-WAN Validator VM インスタンスの作成」を参照してください。VM の作成プロセス中に、vBond.ova ファイルをインストールします。
- vEdge Cloud ルータにソフトウェアをインストールするには、「AWS での vEdge クラウド VM インスタンスの作成」、「ESXi での vEdge クラウド VM インスタンスの作成」、または「KVM での vEdge クラウド VM インスタンスの作成」を参照してください。VM の作成プロセス中に、vEdge Cloud.ova ファイルをインストールします。
- Cisco SD-WAN Manager にソフトウェアをインストールするには、「ESXi での Cisco SD-WAN Manager VM インスタンスの作成」または「KVM での Cisco SD-WAN Manager インスタンスの作成」を参照してください。VM の作成プロセス中に、vManage.ova ファイルをインストールします。
- Cisco Catalyst SD-WAN コントローラ にソフトウェアをインストールするには、「ESXi での Cisco Catalyst SD-WAN コントローラ VM インスタンスの作成」または「KVM での Cisco Catalyst SD-WAN コントローラ VM インスタンスの作成」を参照してください。VM の作成プロセス中に、vSmart.ova ファイルをインストールします。
- ハードウェア vEdge ルータにソフトウェアをインストールするために必要なものは特にありません。すべての vEdge ハードウェア ルータは、ソフトウェアがすでにインストールされた状態で出荷されます。

ソフトウェアのアップグレード

Cisco SD-WAN Manager からオーバーレイネットワーク内にある Cisco vEdge デバイス で実行中のソフトウェアイメージをアップグレードし、新しいソフトウェアで再起動できます。これは、1つのデバイスに対して行うことも、複数のデバイスに対して同時に行うこともできます。

ソフトウェアをアップグレードするには、Cisco Catalyst SD-WAN からソフトウェアイメージを取得し、新しいソフトウェアイメージを Cisco SD-WAN Manager またはリモートサーバーにあるリポジトリに追加して、新しいソフトウェアイメージをデバイスにインストールします。[Activate and Reboot] チェックボックスをオンにすると、次の再起動がすぐに実行されます。また、次の定期的にスケジュールされているメンテナンス期間まで待つこともできます。アップグレードが失敗し、デバイスが再起動しない場合、Cisco SD-WAN Manager は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自動的に戻します。

Cisco vEdge デバイスのソフトウェアをアップグレードする前に、デバイスで必要なソフトウェアバージョンが実行されていることを確認します。



(注) Cisco Catalyst SD-WAN リリース 18.4.5、19.2.2、および 20.1.1 以降のリリースには、セキュリティロックアウト機能があります。これらのソフトウェアバージョン（または以降のバージョン）がデバイスにインストールされ、アクティブ化されると、デバイスにインストールされている古いイメージを削除するために 30 日間のタイマーが設定されます。タイマーが切れると、古いイメージは削除されます。たとえば、リリース 18.4.5 をインストールしてアクティブ化すると、以前にインストールされたリリース 19.2.1 イメージで 30 日間のタイマーが開始されますが、リリース 19.2.2 では開始されません。同様に、リリース 19.2.2 をインストールしてアクティブ化すると、以前にインストールされたリリース 18.4.4 イメージで 30 日間のタイマーが開始されますが、リリース 18.4.5 では開始されません。

30 日間のタイマーが切れる前は、インストール済みの古いイメージを引き続きアクティブ化できます。30 日間のタイマーが切れる前にデバイスが再起動すると、タイマーはリセットされます。

詳細については、『[Cisco Catalyst SD-WAN Command Reference](#)』ガイドを参照してください。

- **request software secure-boot set** : 30 日間待たずに、古いイメージ* がすぐに削除されます。
- **request software secure-boot status** : インストールされている古いイメージを表示します*。
- **request software secure-boot list** : インストールされているすべての古いイメージ* のリストを出力します。

*古いイメージ = リリース 18.4.5、19.2.2、および 20.1.1 より前のイメージ



(注) Cisco SD-WAN Manager のダウングレードはサポートされていません。Cisco SD-WAN Manager をアップグレードする前に、VM のスナップショットを作成してください。以前の Cisco SD-WAN Manager リリースにロールバックするには、スナップショットに戻します。

ソフトウェアアップグレードに関する追加情報と注意事項については、[リリースノート](#)を参照してください。

ソフトウェアアップグレードのベストプラクティス

- CLI ではなく Cisco SD-WAN Manager から、ソフトウェアをアップグレードします。
- リモート Cisco SD-WAN Manager のソフトウェアイメージをアップグレードする場合は、オーバーレイネットワークがすでに稼働している必要があります。
- オーバーレイネットワーク内のすべてのデバイスをアップグレードする場合は、次の順序でアップグレードを実行する必要があります。
 1. Cisco SD-WAN Manager インスタンスをアップグレードします。
 2. Cisco SD-WAN Validator をアップグレードします。

3. 半分の Cisco SD-WAN コントローラ をアップグレードします。
4. アップグレードされた Cisco SD-WAN コントローラ を少なくとも 1 日 (24 時間) 動作させ、Cisco vEdge デバイス とオーバーレイネットワークが安定して期待どおりに動作していることを確認します。
5. 残りの Cisco SD-WAN コントローラ をアップグレードします。
6. 10% の vEdge ルータをアップグレードします。マルチルータサイトの場合、サイトごとに 1 つのルータのみをアップグレードすることをお勧めします。
7. アップグレードされた vEdge ルータを少なくとも 1 日 (24 時間) 動作させ、Cisco Catalyst SD-WAN デバイスとオーバーレイネットワークが安定して期待どおりに動作していることを確認します。
8. 残りの vEdge ルータをアップグレードします。



(注) Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.13.1 以降、Cisco vEdge デバイス の場合、Datagram Transport Layer Security (DTLS) の制御セッションレートは、アップグレード中のみ 4000 pps に増加し、アップグレードの完了後に元の値にリセットされます。

- 新しいソフトウェアイメージが FTP サーバーにある場合は、FTP サーバーが同時ファイル転送を処理できることを確認してください。
- 新しいソフトウェアイメージが Cisco SD-WAN Manager のイメージリポジトリにある場合は、Cisco SD-WAN Manager が配置されている WAN に同時ファイル転送に十分なキャパシティがあることを確認してください。
- グループのソフトウェアアップグレード処理に Cisco SD-WAN Manager を含めることはできません。Cisco SD-WAN Manager サーバーを単体でアップグレードして再起動する必要があります。
- グループ ソフトウェア アップグレード操作では、最大 40 の Cisco vEdge デバイス または Cisco IOS XE Catalyst SD-WAN デバイス をアップグレードし、最大 100 の Cisco vEdge デバイス または Cisco IOS XE Catalyst SD-WAN デバイス を同時に再起動またはアクティブ化することができます (新しいイメージがローカルで使用可能な場合)。これらの最大数は、Cisco SD-WAN Manager がアイドル状態であり、アップグレードおよび再起動操作のみが実行されていることを前提としています。Cisco SD-WAN Manager で他の管理タスクが同時に発生すると、使用可能なセッションの数が減少します。
- ソフトウェアイメージをデフォルトのソフトウェアイメージに設定する場合は、最初にそれをアクティブにしてから、デフォルトのイメージにします。
- 設定変更を行った後に以前にアクティブ化したイメージを再度アクティブ化すると、設定の相違のために予期しない動作が発生する場合があります。新しいソフトウェアバージョンの新規インストールとアクティブ化を行う必要があります。

Cisco Catalyst SD-WAN からのソフトウェアイメージの取得

オーバーレイネットワークのデバイスで実行されているソフトウェアをアップグレードするには、最初に Cisco Catalyst SD-WAN Web サイトから新しいソフトウェアパッケージを取得する必要があります。パッケージを取得するには、<http://www.cisco.com/go/support> にアクセスし、Cisco Catalyst SD-WAN Support にログインして、新しいリリースのソフトウェアパッケージをダウンロードします。ソフトウェアイメージをネットワーク内の FTP サーバーにダウンロードし、Cisco SD-WAN Manager からリモートホスト上のアップグレードパッケージを指定することもできます。

ソフトウェアの初期インストールの場合、リリース 16.1 以降のソフトウェアパッケージ名は次の形式になります。x.x.x は Cisco Catalyst SD-WAN ソフトウェア リリース バージョンを表します。各パッケージには、仮想マシンと Cisco Catalyst SD-WAN ソフトウェアが含まれています。

- vEdge Cloud ルータ
 - viptela-x.x.x-edge-genericx86-64.ova (ESXi ハイパーバイザ用)
 - viptela-edge-genericx86-64.qcow2 (KVM ハイパーバイザ用)
- Cisco SD-WAN Validator
 - viptela-edge-genericx86-64.ova (ESXi ハイパーバイザ用)
 - viptela-edge-genericx86-64.qcow2 (KVM ハイパーバイザ用)
- Cisco Catalyst SD-WAN コントローラ
 - viptela-smart-genericx86-64.ova (ESXi ハイパーバイザ用)
 - viptela-smart-genericx86-64.qcow2 (KVM ハイパーバイザ用)
- Cisco SD-WAN Manager
 - viptela-vmanage-genericx86-64.ova (ESXi ハイパーバイザ用)
 - viptela-vmanage-genericx86-64.qcow2 (KVM ハイパーバイザ用)

リリース 16.1 以降のソフトウェア アップグレード パッケージ名は次の形式になります。x.x.x はリリースバージョンを表します。文字列 mips64 および x86_64 は、基になるチップアーキテクチャを表します。

- vEdge ルータハードウェア : viptela-x.x.x-mips64.tar.gz
- Cisco SD-WAN Validator、vEdge Cloud ルータ、および Cisco Catalyst SD-WAN コントローラ : viptela-x.x.x-x86_64.tar.gz
- Cisco SD-WAN Manager : vmanage-x.x.x-x86_64.tar.gz

リリース 15.4 以前の場合、ソフトウェア アップグレード パッケージは、拡張子が .tar.bz2 のファイルにあります。vEdge 100 ルータの場合は .tar.gz です。パッケージ名の形式は次のとお

りです。x.x.x はリリースバージョンを表します。文字列 mips64 および x86_64 は、基になるチップアーキテクチャを表します。

- vEdge ルータ : vptela-x.x.x-mips64.tar.bz2
- Cisco SD-WAN Validator および Cisco Catalyst SD-WAN コントローラ : vptela-x.x.x-x86_64.tar.bz2
- Cisco SD-WAN Manager : vmanage-x.x.x-x86_64.tar.bz2

リポジトリへの新しいソフトウェアイメージの追加

Cisco Catalyst SD-WAN Web サイトから新しいソフトウェアパッケージをダウンロードしたら、Cisco SD-WAN Manager リポジトリにアップロードします。ソフトウェアイメージを FTP サーバーにダウンロードした場合は、Cisco SD-WAN Manager からリモートホスト上のアップグレードパッケージを指定します。

1. [Cisco SD-WAN Manager] メニューから、**[Maintenance] > [Software Repository]**の順に選択します。
- 2.
3. [Add New Software] をクリックし、ソフトウェアイメージをダウンロードする場所を選択します。場所は次のとおりです。
 - Cisco SD-WAN Manager : ローカル Cisco SD-WAN Manager に保存するイメージを選択する場合。
 - Remote Server (推奨) : リモートファイルサーバーに保存されているイメージを選択する場合。
 - Remote Server – Cisco SD-WAN Manager : リモート Cisco SD-WAN Manager に保存されているイメージを選択する場合。この場所は、リリース 17.2 以降で使用できます。
4. Cisco SD-WAN Manager を選択すると、[Upload Software to Cisco SD-WAN Manager] ダイアログボックスが開きます。
 1. [Browse] をクリックしてソフトウェアイメージを選択するか、vEdge ルータ、Cisco SD-WAN コントローラ、または Cisco SD-WAN Manager のイメージをドラッグアンドドロップします。
 2. [Upload] をクリックして、イメージを Cisco SD-WAN Manager リポジトリに追加します。
5. [Remote Server] を選択すると、[Location of Software on Remote Server] ダイアログボックスが開きます。
 1. ソフトウェアイメージのバージョン番号を入力します。
 2. イメージが存在する FTP または HTTP サーバーの URL を入力します。
 3. [OK] をクリックして、リモートホスト上のソフトウェアイメージを指定します。

6. [Remote Server – Cisco SD-WAN Manager] を選択すると、[Upload Software to Cisco SD-WAN Manager] ダイアログボックスが開きます。
 1. Cisco SD-WAN Manager サーバーのホスト名を入力します。
 2. [Browse] をクリックしてソフトウェアイメージを選択するか、vEdge ルータ、Cisco SD-WAN コントローラ、または Cisco SD-WAN Manager のソフトウェアイメージをドラッグアンドドロップします。
 3. [Upload] をクリックして、イメージを Cisco SD-WAN Manager リポジトリに追加します。

追加されたソフトウェアイメージは Cisco SD-WAN Manager リポジトリテーブルに一覧表示され、デバイスにインストールできるようになります。テーブルには、イメージの名前とタイプ、更新日時、および URL が表示されます。

リストに追加されたソフトウェアバージョンを削除するには、目的のソフトウェアバージョンで [...] をクリックし、[Delete] を選択します。

ソフトウェアイメージのアップグレード

ソフトウェアイメージが Cisco SD-WAN Manager イメージリポジトリに存在している場合、デバイスにソフトウェアイメージをアップロードできます。

1. Cisco SD-WAN Manager のメニューから **[Maintenance] > [Software Upgrade]** の順に選択します。
2. チェックボックスをクリックして、ソフトウェアイメージをアップグレードする 1 つ以上のデバイスを選択します。デバイスを検索するには、[Device Groups] ドロップダウンや検索ボックスを使用します。
3. [Upgrade] をクリックすると、[Software Upgrade] ダイアログボックスが開きます。
4. [Version] ドロップダウンから、インストールするソフトウェアイメージのバージョンを選択します。Cisco SD-WAN Manager とリモートサーバーがアクティブ化されます。
5. ソフトウェアイメージが Cisco SD-WAN Manager またはリモートサーバー上で使用可能かどうかを選択します。
6. ステップ 5 でリモートサーバーを選択した場合は、Cisco Catalyst SD-WAN コントローラ/Cisco SD-WAN Manager および vEdge に適切な VPN を選択し、ステップ 8 に進みます。
7. ステップ 5 で Cisco SD-WAN Manager を選択した場合は、[Activate and Reboot] チェックボックスをオンにして、新しいソフトウェアイメージを自動的にアクティブ化し、デバイスを再起動できます。([Activate and Reboot] チェックボックスをオンにしない場合でも、新しいソフトウェアイメージはインストールされますが、デバイスでは既存のソフトウェアイメージが引き続き使用されることに注意してください。新しくインストールされたソフトウェアイメージをアクティブ化するには、以下の「新しいソフトウェアイメージのアクティブ化」を参照してください)。

8. [Upgrade] をクリックします。プログレスバーにソフトウェアアップグレードのステータスが表示されます。

アップグレードが 60 分以内に正常に完了しない場合、タイムアウトになります。

Cisco SD-WAN Manager への制御接続が 15 以内に確立されなかった場合、Cisco SD-WAN Manager はデバイスを以前に実行されていたソフトウェアイメージに自動的に戻します。

新しいソフトウェアイメージのアクティブ化

ソフトウェアイメージのアップロード時に [Activate and Reboot] チェックボックスをオンにする場合、[Upgrade] をクリックすると、新しいソフトウェアが自動的にアクティブになり、デバイスが再起動します。

リモートサーバーからソフトウェアイメージをアップロードした場合、または Cisco SD-WAN Manager からのソフトウェアイメージのアップロード時に [Activate and Reboot] チェックボックスをオンにしなかった場合、新しいイメージはデバイスにインストールされますが、デバイスは引き続き既存のソフトウェアイメージを使用します。新しいソフトウェアイメージをアクティブにするには、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. チェックボックスをクリックして、新しいソフトウェアイメージをアクティブにする 1 つ以上のデバイスを選択します。デバイスを検索するには、[Device Groups] ドロップダウンや検索ボックスを使用します。
3. [Activate] をクリックして新しいソフトウェアをアクティブにします。アクティブ化プロセスにより、デバイスが再起動され、新しくインストールされたソフトウェアにアップグレードされます。

デバイスと Cisco SD-WAN Manager の制御接続が 15 分以内に確立されなかった場合、Cisco SD-WAN Manager はデバイスを以前に実行されていたソフトウェアイメージに自動的に戻します。

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

各デバイスのソフトウェアアップグレードのステータスと、関連するアクティビティのログを表示するには、次の手順を実行します。

1. [Active Devices] トグルボタンをクリックします。画面の上部、タイトルバーのすぐ下には、実行されたアップグレードの総数と、成功と失敗の総数が表示されます。ソフトウェアアップグレードの表には、各アップグレード操作のステータスが表示されます。
2. 表の各行の左側にある右山カッコをクリックして、操作の詳細を確認します。詳細を閉じるには、下山カッコをクリックします。

CLI からのソフトウェアイメージのアップグレード

デバイス上でソフトウェアイメージを直接アップグレードする必要がある場合、またはネットワークで Cisco SD-WAN Manager を使用していない場合は、ソフトウェアイメージをアップグレードするために、インストールプロセスを繰り返すか、CLI 内からソフトウェアイメージをインストールできます。

CLI 内から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。

1. ソフトウェアのアップグレードが成功したことを確認するための制限時間を設定します。時間の範囲は 1 ～ 60 分です。

```
Device# system upgrade-confirmminutes
```

2. ソフトウェアをインストールします。

```
vEdge# request software install url  
/viptela- release -mips64.tar.bz2 [reboot] [vpn vpn-id]
```

```
vSmart# request software install url/viptela- release  
-x86_64.tar.bz2 [reboot] [vpn vpn-id]
```

次のいずれかの方法でイメージの場所を指定します。

- イメージファイルがローカルサーバー上にある場合：

/directory-path/

CLI のオートコンプリート機能を使用して、パスとファイル名を完成させることができます。

- イメージファイルが FTP サーバー上にある場合：

ftp://hostname/

- イメージファイルが HTTP サーバー上にある場合：

http://hostname/

- イメージファイルが TFTP サーバー上にある場合：

tftp://hostname/

必要に応じて、サーバーが配置されている VPN の識別子を指定します。

[reboot] オプションは、新しいソフトウェアイメージをアクティブにして、インストールの完了後にデバイスを再起動します。

3. ステップ 2 で [reboot] オプションを含めなかった場合は、新しいソフトウェアイメージをアクティブにして、デバイスを再起動します。

```
Viptela# request software activate
```

4. アップグレード確認のための設定した制限時間内にソフトウェアアップグレードが成功したことを確認します。

```
Viptela# request software upgrade-confirm
```

この制限時間内にこのコマンドを発行しないと、デバイスは自動的に以前のソフトウェアイメージに戻ります。

冗長ソフトウェアイメージ

Cisco vEdge デバイスに複数のソフトウェアイメージをダウンロードして保存できます。

現在インストールされているソフトウェアバージョンを一覧表示し、現在実行されているソフトウェアイメージを確認するには、次のコマンドを使用します。

```
Viptela# show software
VERSION    ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
-----
15.4.3      true   false   false     user       2016-02-04T03:45:13-00:00
15.4.2      false  true    true      user       2015-12-06T14:01:12-00:00
```

ソフトウェアを特定のバージョンにアップグレードするには、次のコマンドを使用します。

```
Viptela# request software activate
```

CiscovEdge デバイスの古いソフトウェアイメージへのダウングレード

CLI を使用して Cisco vEdge デバイス を以前のソフトウェアイメージにダウングレードするには、次の手順を実行します。

1. 必要に応じて、既存のソフトウェアイメージを削除して、新しいソフトウェアイメージをロードするための領域を用意します。

```
vEdge# request software remove previous-installed-build
```

2. ダウングレード用のソフトウェアイメージをダウンロードします。
3. ダウンロードしたイメージをインストールします。

```
vEdge# request software install desired-build
```

インストールする前にイメージをローカルストレージにコピーすることをお勧めしますが、次のいずれかの方法でイメージの場所を指定できます。

- イメージファイルがローカルサーバー上にある場合：

```
/directory-path/
```

CLI のオートコンプリート機能を使用して、パスとファイル名を完成させることができます。

- イメージファイルが FTP サーバー上にある場合：

```
ftp://hostname/
```

- イメージファイルが HTTP サーバー上にある場合：

```
http://hostname/
```

- イメージファイルが TFTP サーバー上にある場合：

```
tftp://hostname/
```

4. インストールしたイメージをデフォルトとして設定します。

```
vEdge# request software set-default desired-build
```

5. リセットを実行します。これにより、デバイスがリセットされ、既存の構成が削除されます。デバイスはゼロデイ構成で起動します。

```
vEdge# request software reset
```

Cisco Catalyst SD-WAN Manager をホストしている仮想マシンでのメモリおよび vCPU リソースのアップグレード

次の手順を実行して、Cisco SD-WAN Manager をホストする仮想マシン（VM）上のメモリと仮想中央処理装置（vCPU）のリソースをアップグレードします。



- (注) メモリまたは vCPU の増加のみが許可されます。メモリまたは vCPU をアップグレードした後にダウングレードすることはできません。

1. コマンド **show system status** を使用して、Cisco SD-WAN Manager の現在の設定を確認します。

```
vManage#show system status
```

```
Viptela (tm) vmanage Operating System Software
Copyright (c) 2013-2021 by Viptela, Inc.
Controller Compatibility:
Version: 20.7.0-185
Build: 185
```

```
System logging to host is disabled
System logging to disk is enabled
```

```
System state:          GREEN. All daemons up
System FIPS state:     Enabled
Testbed mode:         Enabled
Engineering Signed:    True
```

```
Last reboot:          Initiated by user.
CPU-reported reboot:   Not Applicable
Boot loader version:   Not applicable
System uptime:         1 days 02 hrs 44 min 52 sec
Current time:          Sat Oct 23 22:12:10 UTC 2021
```

```
Load average:         1 minute: 14.58, 5 minutes: 12.31, 15 minutes: 10.73
Processes:            5775 total
CPU allocation:        32 total
CPU states:            31.58% user, 4.36% system, 64.06% idle
Memory usage:          65741448K total, 38096172K used, 490324K free
                      4606444K buffers, 22548508K cache
```

```
Disk usage:           Filesystem      Size  Used Avail Use % Mounted on
                      /dev/root        15230M 3496M 10898M 24% /
```



```

vManage storage usage:  Filesystem      Size  Used Avail  Use% Mounted on
                        /dev/sdb        502942M  206906M  270435M   41%  /opt/data

Personality:           vmanage
Model name:            vmanage
Services:              None
vManaged:             false
Commit pending:       false
Configuration template: None
Chassis serial number: None

```

2. メモリをアップグレードするには、デバイスの電源を切ります。
3. ホスティング プラットフォームのガイドラインを使用して、VM の CPU とメモリをアップグレードします。次のアップグレードを行うことができます。

リソース	現在	アップグレード
vCPU	16	32
メモリ	32 G	64 G または 128 G
メモリ	64 G	128 G



(注) Cisco Catalyst 8000V および Cisco Catalyst SD-WAN デプロイメントでは、8GB メモリが最小要件です。

4. デバイスの電源を入れ、メモリと CPU を確認します。

```
vManage1# show system status
```

```

Viptela (tm) vmanage Operating System Software
Copyright (c) 2013-2021 by Viptela, Inc.
Controller Compatibility:
Version: 20.7.0-139
Build: 139

```

```

System logging to host  is disabled
System logging to disk is enabled

```

```

System state:           GREEN. All daemons up
System FIPS state:      Enabled
Testbed mode:          Enabled
Engineering Signed:     True

```

```

Last reboot:           Initiated by user - activate 20.7.0-139.
CPU-reported reboot:   Not Applicable
Boot loader version:   Not applicable
System uptime:         16 days 17 hrs 43 min 28 sec
Current time:          Sat Oct 23 22:22:16 UTC 2021

```

```

Load average:          1 minute: 15.86, 5 minutes: 13.02, 15 minutes: 11.45
Processes:             6067 total
CPU allocation:         32 total

```

```

CPU states:          32.13% user,   4.34% system,  63.53% idle
Memory usage:        131703148K total,   88221488K used,   19285636K free
                      7022488K buffers,  17173536K cache

Disk usage:          Filesystem      Size  Used Avail  Use % Mounted on
                      /dev/root      15998M 10702M 4461M   71%  /
vManage storage usage: Filesystem      Size  Used Avail  Use% Mounted on
                      /dev/sdb       10402115M 702212M 9175615M   6%  /opt/data

Personality:         vmanage
Model name:          vmanage
Services:            None
vManaged:           false
Commit pending:      false
Configuration template: None
Chassis serial number: None

```

セカンダリディスクサイズの拡大（Cisco Catalyst SD-WAN Manager リリース 20.12.x 以前）

既知の制限により、この手順は Cisco Catalyst SD-WAN Manager リリース 20.13.x または 20.14.x では無効です。

Cisco SD-WAN Manager インスタンスをホストする仮想マシンのセカンダリディスクのサイズを増やすには、次の手順を実行します。

手順

ステップ 1 Cisco SD-WAN Manager をホストしている仮想マシンをシャットダウンします。

ステップ 2 ハイパーバイザ（ETA、Azure、AWS など）を使用して、Cisco SD-WAN Manager をホストしている仮想マシンのセカンダリディスク用に追加のスペースをプロビジョニングします。

ステップ 3 Cisco SD-WAN Manager をホストしている VM を再起動します。

ステップ 4 Cisco SD-WAN Manager で次のように入力し、Cisco SD-WAN Manager が追加のディスク容量を検出してファイルシステムを拡張しその容量を使用できるようにします。

```
vm# request nms application-server resize-data-partition
```

ステップ 5 次のコマンドを入力して、/opt/data ディスクのサイズが変更されたことを確認します。

```
vm# vshell
vm:~$ df -hk | grep data
```

出力には新しいディスクサイズが表示されます。

Cisco IOS XE Catalyst SD-WAN デバイスのソフトウェアメンテナンスアップグレード

表 9: 機能の履歴

機能名	リリース情報	説明
ソフトウェアメンテナンスアップグレードパッケージのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能により、Cisco IOS XE Catalyst SD-WAN デバイスにインストール可能なソフトウェアメンテナンスアップグレード (SMU) パッケージのサポートが有効になります。SMU パッケージにより、リリース済みの Cisco IOS XE イメージにパッチ修正やセキュリティの解決策が提供されます。デベロッパーは、次のリリースで修正が利用可能になるのを待たずに、報告された問題の修正を提供するこのパッケージをビルドできます。
Cisco ISR1100 および ISR1100X シリーズ ルータの SMU サポート	Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a Cisco vManage リリース 20.11.1	Cisco ISR 1100 および ISR 1100X シリーズ サービス統合型ルータ に対するサポートが追加されました。

ソフトウェアメンテナンスアップグレードについて

ソフトウェアメンテナンスアップグレード (SMU) は、リリースされたソフトウェアの重大なバグに対するポイントフィックスであり、可能な場合、ルータの中断が最小限に抑えられます。SMU は、メンテナンスリリースを置き換えるようには設計されていません。

シスコは、SMU の修正をパッケージファイル (Cisco Catalyst SD-WAN の各リリースと各コンポーネントのファイル) として提供します。パッケージには、パッケージの内容を記述するメタデータ、および報告済みの問題の修正が含まれています。

SMU イメージファイル

ソフトウェアリポジトリの各 SMU イメージファイル名には、基本イメージバージョンと修正に関連する欠陥 ID が含まれています。イメージ名の内容:

- base_image_version は、Cisco IOS XE イメージのバージョンです。
- defect_id は、SMU パッケージに修正がある欠陥の識別子です。

SMU タイプ

SMU タイプは、Cisco IOS XE Catalyst SD-WAN デバイス にインストールされた SMU パッケージの影響を表します。SMU パッケージのタイプは次のとおりです。

- ホット SMU（リロードなし）：SMU イメージのアクティブ化後に、Cisco IOS XE Catalyst SD-WAN デバイス を再起動（リロード）せずに SMU パッケージを有効にします。
- コールド SMU（リロードあり）：Cisco IOS XE Catalyst SD-WAN デバイス の再起動（リロード）後に SMU パッケージを有効にします。

ソフトウェアメンテナンスアップグレードを使用する利点

- ネットワークの問題に迅速に対応でき、テストに必要な時間と範囲も削減できます。Cisco IOS XE Catalyst SD-WAN デバイス では SMU イメージの互換性が内部的に検証されるため、互換性のない SMU パッケージはインストールできません。
- デバイスに一度に 1 つの SMU パッケージのみをインストールまたはアクティブ化して、初期実装プロセスを簡素化できます。
- Cisco SD-WAN Manager を使用してインストールするときに、同時に複数の Cisco IOS XE Catalyst SD-WAN デバイス に SMU パッケージをインストールできます。CLI を使用して複数のデバイスに SMU パッケージをインストールするには、複数のデバイスでインストールプロセスを繰り返します。

ソフトウェアメンテナンスアップグレードでサポートされるデバイス

リリース	サポートされるデバイス数
Cisco IOS XE Catalyst SD-WAN リリース 17.9.x の Cisco IOS XE Catalyst SD-WAN リリース 17.9.5a 以降のリリース Cisco IOS XE Catalyst SD-WAN リリース 17.12.x の Cisco IOS XE Catalyst SD-WAN リ リース 17.12.3a 以降のリリース Cisco IOS XE Catalyst SD-WAN リリース 17.15.1a 以降	• Cisco ISR 1000 シリーズ サービス統合型ルー タ • Cisco IR1101 耐環境性能 サービス統合型 ルータ • Cisco ISR 4000 シリーズ サービス統合型ルー タ • Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ • Cisco Catalyst 8500 シリーズ エッジ プラッ トフォーム • Cisco Catalyst 8500L シリーズ エッジプラッ トフォーム • Cisco Catalyst 8000v シリーズ エッジプラッ トフォーム
Cisco IOS XE Catalyst SD-WAN リリース 17.12.x の Cisco IOS XE Catalyst SD-WAN リ リース 17.12.3a 以降のリリース	• Cisco Catalyst 8300 シリーズ エッジ プラッ トフォーム • Cisco Catalyst 8200L シリーズ エッジプラッ トフォーム
Cisco IOS XE Catalyst SD-WAN リリース 17.12.x の Cisco IOS XE Catalyst SD-WAN リ リース 17.12.3a 以降のリリース	Cisco ISR 1100 および ISR 1100X シリーズ サー ビス統合型ルータ

ソフトウェアメンテナンスアップグレードイメージの管理

SMU イメージの追加、アップグレードとアクティブ化、または非アクティブ化と削除には、Cisco SD-WAN Manager を使用します。



(注) SMU イメージをアクティブ化または非アクティブ化すると、SMU イメージによってはデバイスが再起動する場合があります。非リロード SMU タイプではデバイスの再起動はトリガーされず、リロード SMU タイプではデバイスの再起動がトリガーされます。

SMU イメージの追加、表示、およびアクティブ化

1. Cisco SD-WAN Manager ソフトウェアリポジトリを使用して SMU イメージを追加します。

『Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide』の Cisco SD-WAN Manager 「[Add Software Images to Repository](#)」 手順を参照してください。

2. Cisco SD-WAN Manager ソフトウェアリポジトリを使用して SMU イメージを表示します。

『Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide』の Cisco SD-WAN Manager 「[View Software Images](#)」 手順を参照してください。SMU イメージを表示するときは、次の点に注意してください。

- [Available SMU Versions] 列には、現在の基本イメージバージョン（Cisco IOS XE イメージバージョン）で利用できる SMU イメージの数が表示されます。
- [Available SMU Versions] 列で目的のエントリをクリックして、その SMU イメージに関連付けられている欠陥を表示します。[Available SMU Versions] ダイアログボックスで、欠陥 ID、対応する SMU バージョン、および SMU タイプ（非リロードまたはリロードなど）を確認できます。
- [Available SMU Versions] ダイアログボックスで、SMU バージョンの横にある削除アイコンをクリックして、その SMU バージョンを削除します。

3. [Cisco SD-WAN Manager Software Upgrade] ウィンドウを使用して、デバイスの SMU イメージをアップグレードします。

『Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide』の Cisco SD-WAN Manager 「[Upgrade the Software Image on a Device](#)」 手順を参照してください。アップグレード対象として選択する SMU イメージについて、次の点に注意してください。

- デバイステーブルの [Available SMUs] 列には、現在の基本イメージバージョンで利用可能な SMU イメージの数が表示されます。
- [Available SMUs] 列の下にある目的のエントリをクリックして、利用可能なすべての SMU バージョンとデバイスのアップグレードイメージのリストを表示します。[Available SMUs] ダイアログボックスで、SMU バージョン、SMU タイプ、および SMU バージョンの状態を確認できます。

SMU バージョンの形式は `base_image_version.cdets_id` です。

- [Upgrade] ダイアログボックスで、必要に応じて [Activate and Reboot] をオンにして、SMU イメージをアクティブ化し、Cisco IOS XE Catalyst SD-WAN デバイスを自動的に再起動します。

[Activate and Reboot] チェックボックスをオンにすると、Cisco SD-WAN Manager はデバイスに SMU イメージをインストールしてアクティブ化し、SMU タイプに基づいてリロードをトリガーします。『Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide』の Cisco SD-WAN Manager 「[Activate a Software Image](#)」 手順を参照してください。

SMU イメージのアップグレードが成功すると、Cisco IOS XE Catalyst SD-WAN デバイスは対応する成功メッセージを送信します。

SMU イメージの非アクティブ化または削除

『Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide』の「[Delete a Software Image](#)」手順を使用して、SMU イメージを非アクティブ化し、デバイスからイメージを削除します。

Cisco SD-WAN Manager への ISR1100 のオンボーディング

1. ISR1100 デバイスで Cisco IOS XE Catalyst SD-WAN デバイスのインターフェイスを有効にしないでください。
2. serial.viptela ファイルを Cisco SD-WAN Manager に追加して、デバイスを追加します。
3. Cisco SD-WAN Manager メニューから、**[Configuration] > [Devices] > [Migrate Device]**の順に選択して、viptela オペレーティングシステムから Cisco IOS XE オペレーティングシステムに移行します。
4. Cisco IOS XE Catalyst SD-WAN デバイスのインターフェイスを有効にして、制御接続を確立します。
5. Cisco SD-WAN Manager でデバイスの同期を確認します。

CLI を使用したソフトウェア メンテナンス アップグレード イメージの管理

次の CLI を使用して、SMU イメージのインストール、アップグレードとアクティブ化、または非アクティブ化と削除を行います。



- (注) SMU イメージがアクティブ化および非アクティブ化されると、非リロードまたはリロード SMU タイプに基づいてデバイスの再起動がトリガーされる場合があります。非リロード SMU タイプではデバイスの再起動はトリガーされませんが、リロード SMU タイプではデバイスの再起動がトリガーされます。

CLI を使用した SMU イメージのインストールとアクティブ化

1. ファイルサーバーからデバイスのブートフラッシュに SMU イメージをアップロードします。

copy コマンドを使用して、SMU イメージをアップロードします。copy コマンドの詳細については、「[Cisco IOS XE ソフトウェアのインストール](#)」トピックのステップ 2 を参照してください。

2. SMU イメージのアクティブ化が成功したことを確認するための制限時間を設定します（まだ設定されていない場合）。

制限時間は 1 分から 60 分に設定できます。制限時間は 15 分以上に設定することを推奨します。

```
Device# config-transaction
Device(config)# system
Device(config-system)# upgrade-confirm minutes
```

3. デバイスのブートフラッシュから SMU イメージをインストールし、デバイスと SMU パッケージバージョンの互換性チェックを実行します。

```
Device# request platform software sdwan smu install file-path
```

4. Cisco IOS XE Catalyst SD-WAN デバイス で SMU イメージをアクティブ化します。

```
Device# request platform software sdwan smu activate
build-number.smu-defect-id
```

5. 設定した確認用制限時間内で、SMU イメージのアップグレードを確認します。

```
Device# request platform software sdwan smu upgrade-confirm
```



(注) **upgrade-confirm minutes** コマンドで指定した制限時間内にデバイスでこのコマンドを発行しないと、デバイスは SMU イメージがアクティブ化される前の状態に自動的に戻ります。

CLI を使用した SMU イメージの非アクティブ化および削除

1. SMU イメージの非アクティブ化が成功したことを確認するための制限時間を設定します（まだ設定されていない場合）。

制限時間は 1 分から 60 分に設定できます。制限時間は 15 分以上に設定することを推奨します。

```
Device# config-transaction
Device(config)# system
Device(config-system)# upgrade-confirm minutes
```

2. Cisco IOS XE Catalyst SD-WAN デバイス で SMU イメージを非アクティブ化します。

```
Device# request platform software sdwan smu deactivate
build-number.smu-defect-id
```

3. SMU イメージを非アクティブ化できたことを確認します。

```
Device# request platform software sdwan smu upgrade-confirm
```



(注) **upgrade-confirm minutes** コマンドで指定した制限時間内にデバイスでこのコマンドを発行しないと、イメージの非アクティブ化は失敗し、デバイスは SMU イメージが非アクティブ化される前の状態に自動的に戻ります。

4. Cisco IOS XE Catalyst SD-WAN デバイス から SMU イメージを削除します。

```
Device# request platform software sdwan smu remove  
build-number.smu-defect-id
```

次の例は、SMU イメージ操作を管理するために使用できるコマンドを示しています。

- アップグレードをチェックし、設定を確認します。

```
show sdwan running system
```

- 確認タイマーを追加してアップグレードします。

```
config-transaction  
system  
upgrade-confirm 15  
commit
```

- 実行コマンド：

```
• request platform software sdwan smu install  
  bootflash:c8000v-universalk9.2022-08-17_23.44_mcpres.24042.CSCvq24042.SSA.smu.bin  
  
• request platform software sdwan smu activate 17.09.01a.0.247.CSCvq24042  
  
• request platform software sdwan smu upgrade-confirm  
  
• request platform software sdwan smu deactivate 17.09.01a.0.247.CSCvq24042  
  
• request platform software sdwan smu upgrade-confirm  
  
• request platform software sdwan smu remove 17.09.01a.0.247.CSCvq24042
```

ソフトウェアメンテナンス アップグレードイメージのステータスの検証

Cisco SD-WAN Manager または CLI を使用して、SMU イメージのステータスを監視できます。

Cisco SD-WAN Manager を使用した SMU ステータスの監視

1. Cisco SD-WAN Manager のメニューから、**[Maintenance] > [Software Upgrade]** の順に選択します。
2. 目的の Cisco IOS XE Catalyst SD-WAN デバイス について、**[Available SMUs]** の下にある SMU イメージリンク（ハイパーリンク）をクリックします。

[Available SMUs] ダイアログボックスで、SMU イメージの状態を確認できます。

現在の基本イメージバージョン（Cisco IOS XE イメージバージョン）で使用できる SMU イメージがない場合、SMU イメージリンクは **[Available SMUs]** の下で使用できず、Cisco SD-WAN Manager には 0 と表示されます。

CLI を使用した SMU のステータスの確認

例 1 :

以下は、SMU イメージをインストールし、アクティブにして、アップグレード（コミット）を確認した後の **show install summary** コマンドの出力例です。

```
Device# show install summary[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St  Filename/Version
-----
IMG   C   17.09.01a.0.247
SMU   I   bootflash:c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin

-----
Auto abort timer: inactive
-----
```

この出力は、SMU イメージがブートフラッシュ ファイル システムからインストールされ、アクティブ化されていることを示しています。[Auto abort timer] の値から、SMU イメージのロールバックの残り時間を追跡できます。この値は、自動中止タイマーの期限が切れ、デバイスがロールバックするまでの残り時間を示しています。

例 2 :

次の例は、**request platform software sdwan smu deactivate** コマンドを使用して SMU イメージを非アクティブ化した後の出力を示しています。

```
Device# request platform software sdwan smu deactivate 17.09.01a.0.247.CSCvq24042
smu_deactivate: START Mon Mar 5 21:54:06 PST 2021
smu_deactivate: Deactivating SMU
Executing pre scripts....

Executing pre scripts done.
--- Starting SMU Deactivate operation ---
Performing SMU_DEACTIVATE on all members
  [1] SMU_DEACTIVATE package(s) on switch 1
  [1] Finished SMU_DEACTIVATE on switch 1
Checking status of SMU_DEACTIVATE on [1]
SMU_DEACTIVATE: Passed on [1]
Finished SMU Deactivate operation
SUCCESS: smu_deactivate 17.09.01a.0.247.CSCvq24042
```

この出力には、SMU イメージがデバイスから非アクティブ化されていることが示されています。

以下は、SMU イメージを非アクティブ化した後の **show install summary** コマンドの出力例です。

```
Device# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St  Filename/Version
-----
IMG   C   17.09.01a.0.247
```

```
SMU   D   bootflash:
c8000v-universalk9.2022-08-17_23.44_mcpres.24042.CSCvq24042.SSA.smu.bin
```

```
-----
Auto abort timer: active , time before rollback - 00:04:57
-----
```

次の出力例は、**request platform software sdwan smu upgrade-confirm command** を使用して SMU イメージを非アクティブ化できることを確認した後に SMU イメージを非アクティブ化した出力を示しています。

```
Device# request platform software sdwan smu deactivate 17.09.01a.0.247.CSCvq24042
```

```
install_deactivate: START Thu Aug 25 17:47:10 UTC 2022
install_deactivate: Deactivating SMU
Executing pre scripts....
Executing pre scripts done.
```

```
--- Starting SMU Deactivate operation ---
Performing SMU_DEACTIVATE on Active/Standby
  [1] SMU_DEACTIVATE package(s) on R0
  [1] Finished SMU_DEACTIVATE on R0
Checking status of SMU_DEACTIVATE on [R0]
SMU_DEACTIVATE: Passed on [R0]
Finished SMU Deactivate operation
```

```
CSCvq24042:SUCCESS
SUCCESS: install_deactivate /bootflash/c8kv_hot.bin Thu Aug 25 17:47:33 UTC 2022
```

以下は、SMU イメージを削除化した後の **show install summary** コマンドの出力例です。

```
Device# show install summary[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
```

```
-----
Type  St   Filename/Version
-----
IMG   C    17.09.01a.0.247
```

```
-----
Auto abort timer: inactive
-----
```

例 3 :

以下は、SMU イメージのメタデータ (SMU タイプ、SMU ID、SMU 障害 ID など) を表示する **show install package** コマンドからの出力例です。

```
Device# show install package
bootflash:c8000v-universalk9.2022-08-17_23.44_mcpres.24042.CSCvq24042.SSA.smu.bin
Name: c8000v-universalk9.2022-08-17_23.44_mcpres.24042.CSCvq24042.SSA.smu.bin
Version: 17.09.01a.0.247.1660805065
Platform: C8000V
Package Type: SMU
Defect ID: CSCvq24042
Package State: Inactive
Supersedes List: {}
SMU Fixes List: {}
SMU ID: 24042
SMU Type: non-reload
SMU Compatible with Version: 17.09.01a.0.247
SMUImpact:
```




第 5 章

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のインストールとアップグレード

- Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のインストールおよびアップグレード (110 ページ)
- コントローラモードでサポートされるプラットフォーム (111 ページ)
- Cisco IOS XE イメージの互換性 (112 ページ)
- アップグレードの考慮事項 (112 ページ)
- 機能制限 (114 ページ)
- 自己署名済みトラストポイント (115 ページ)
- 自律モードとコントローラモードの概要 (115 ページ)
- Cisco IOS XE ルータのソフトウェアのインストール (116 ページ)
- Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のリリースでのプラグアンドプレイ (118 ページ)
- PnP 以外のオンボーディング (122 ページ)
- ブートストラップファイルによるモード検出とモード変更 (126 ページ)
- コントローラモード設定のリセット (128 ページ)
- モードスイッチング：追加情報 (130 ページ)
- コントローラモードと自律モードの検証 (130 ページ)
- インストール後のコンソールポートアクセスの変更 (コントローラモード) (132 ページ)
- Cisco IOS XE リリース 17.2.1r 以降へのアップグレード (134 ページ)
- Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のリリースからのダウングレード (138 ページ)
- スマートライセンスとスマートライセンス予約の復元 (140 ページ)
- クラウドサービスによってホストされる Cisco Catalyst 8000V Edge ソフトウェアのオンボード (PAYG ライセンスを使用) (141 ページ)
- Cisco Catalyst 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 (143 ページ)
- トラブルシューティング (145 ページ)

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のインストールおよびアップグレード

表 10: 機能の履歴

機能名	リリース情報	説明
インストールおよびアップグレード	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	この機能により、単一の「universalk9」イメージを使用して、サポートされているすべてのデバイスに Cisco IOS XE Catalyst SD-WAN および Cisco IOS XE 機能を展開できます。この universalk9 イメージは、自律モード（Cisco IOS XE 機能の場合）とコントローラモード（Cisco Catalyst SD-WAN 機能の場合）の 2 つのモードをサポートしています。
Cisco Catalyst 8000V Edge ソフトウェアプラットフォーム	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a	Cisco Catalyst 8000V Edge ソフトウェアプラットフォームのサポートが追加されました。Cisco CSR1000V または Cisco ISRv プラットフォームから Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a へのアップグレードには、プラットフォームタイプから Cisco Catalyst 8000V へのアップグレードが含まれます。

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降、universalk9 イメージを使用して、Cisco IOS XE Catalyst SD-WAN と Cisco IOS XE の両方を Cisco IOS XE Catalyst SD-WAN デバイスに展開できます。

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r を起動すると、UCMK9 イメージは利用できません。

このリリースは Cisco Catalyst SD-WAN と非 Cisco Catalyst SD-WAN の両方の機能と展開のシームレスなアップグレードに役立ちます。

Cisco IOS XE と Cisco IOS XE Catalyst SD-WAN 機能には、それぞれ自律モードとコントローラ実行モードでアクセスします。自律モードはルータのデフォルトモードで、Cisco IOS XE 機能

が含まれています。Cisco IOS XE Catalyst SD-WAN 機能にアクセスするには、コントローラモードに切り替えます。既存のプラグアンドプレイワークフローを使用してデバイスのモードを決定できます。

コントローラモードでサポートされるプラットフォーム

コントローラモードでサポートされるプラットフォーム

- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ
- ASR1000-RP3 モジュールを搭載したモジュラ型 Cisco ASR 1006-X (Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a またはそれ以降、[RP3 モジュールを搭載した Cisco ASR 1006-X](#) を参照)。
- Cisco ISR 1000 シリーズ サービス統合型ルータ
- Cisco ISR 4000 シリーズ サービス統合型ルータ
- Cisco 1101 産業向けサービス統合型ルータ
- Cisco CSR 1000v シリーズ クラウド サービス ルータ
- シスコサービス統合型仮想ルータ (ISRv)
- Cisco Catalyst 8200 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8300 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8500 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8000V Edge ソフトウェア (Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降)

コントローラモードでサポートされていないプラットフォーム

次の ASR 1000 シリーズルータに基づくモジュラ型プラットフォームは、コントローラモードではサポートされていません。

- ASR1000-RP2

コントローラモードでサポートされる暗号モジュール

ASR 1000 シリーズのルータには、以下の暗号モジュールが必要です。

- ASR 1001-HX 用 ASR 1001HX-IPSECHW
- ASR 1002-HX 用 ASR 1002HX-IPSECHW

Cisco IOS XE イメージの互換性

展開イメージのバージョン	Cisco Catalyst SD-WAN	非 Cisco Catalyst SD-WAN
Cisco IOS XE リリース 16.9.x、16.10.x、16.11.x、16.12.x	ucmk9	universalk9
Cisco IOS XE リリース 17.1.x	該当なし	universalk9
Cisco IOS XE リリース 17.2.x 以降	universalk9*	universalk9**

- * Cisco Catalyst SD-WAN のユースケースでは、非 LI および非ペイロードの暗号化イメージタイプはサポートされていません。
- ** 非 Cisco Catalyst SD-WAN のユースケースでは、非 LI および非ペイロードの暗号化イメージタイプがサポートされています（universalk9_noli、universalk9_npe、universalk9_npe_noli）。

アップグレードの考慮事項

次の Cisco IOS XE Catalyst SD-WAN デバイスは、マルチレートインターフェイスをサポートしており、10G インターフェイスポートで 1GE Small Form-factor Pluggable (SFP)（光および CU）モジュールと 10GE SFP+（光および CU）モジュールをサポートしています。

- Cisco ASR 1001-HX ルータ
- Cisco Catalyst 8500-12X4QC
- Cisco Catalyst 8500-12X

これらのデバイスは、1GE SFP（光および CU）モジュールを備えた 10G インターフェイスポートでの自動ネゴシエーションをサポートしています。次の注意事項は、上記の3つのルータモデルのみについて、SD-WAN モードと非 SD-WAN モードの両方での自動ネゴシエーションに適用されます。

- Cisco IOS XE 17.6.1a より前のリリースでは、CLI を使用して自動ネゴシエーションを設定できます。
- Cisco IOS XE 17.6.1a より前のリリースでは、CLI または Cisco Catalyst SD-WAN を使用して、10GE SFP+ モジュールを含む 10G インターフェイスを備えたデバイスを再起動すると、そのインターフェイスは起動しません。この状況では、Cisco Catalyst SD-WAN または CLI を使用して、インターフェイスに「**no negotiation auto**」を設定してから、デバイスを再起動します。
- Cisco IOS XE リリース 17.6.3a 以降では、自動ネゴシエーションの **auto neg** 値は、機能テンプレートを介して、サポートされているデバイスの 10G インターフェイスにプッシュ

されます。機能テンプレートを適切に設定できるように、デバイスのどの 10G インターフェイスにどの SFP モジュールが取り付けられているのかを確認してください。

- Cisco IOS XE リリース 17.6.3a までのソフトウェアリリースでは、10GE SFP+ モジュールが取り付けられている 10G インターフェイスで **negotiation auto** コマンドがサポートされません。
- Cisco IOS XE リリース 17.6.4 以降では、10 GE SFP+ モジュールが取り付けられている 10G インターフェイスで **negotiation auto** コマンドがサポートされます。このシナリオでは、**show interface Tengig x/x/x** の出力において、**negotiation auto/no negotiation auto** の設定に関係なく、リンクタイプは **force-up** になります。設定が Cisco SD-WAN Manager テンプレートを介してプッシュされる場合も同様です。
- Cisco IOS XE リリース 17.6.4 以降では、1GE 光ファイバおよび導線 SFP を含む 10G インターフェイスで **negotiation auto** コマンドがサポートされます。
- Cisco IOS XE リリース 17.6.3a までのソフトウェアリリースでは、デフォルトの「OFF」オプションを指定した **no negotiate auto** コマンドを、機能テンプレートを介して、10GE SFP+ モジュールが取り付けられたすべての 10G インターフェイスに送信する必要があります。そうしないと、テンプレートのプッシュに失敗します。
- Cisco IOS XE リリース 17.6.3a にアップグレードする前に、機能テンプレート、CLI アドオン機能テンプレート、または CLI を使用して、10GE SFP+ モジュールが取り付けられたすべての 10G インターフェイスに **no negotiation auto** を適用します。
- 10GE SFP+ モジュールが取り付けられた 10G インターフェイスで自動ネゴシエーションが有効になっているリリースから Cisco IOS XE リリース 17.6.3a にアップグレードすると、そのインターフェイスは起動しません。この状況では、CLI を使用して、アップグレードの完了後にインターフェイスに **no negotiation auto** を設定します。
- Cisco Catalyst SD-WAN Manager リリース 20.12.1 または Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以降のリリースにアップグレードする前に、Cisco TAC に連絡して、互換性のないインデックスを確認して削除してください。互換性のない古いインデックスは、新しいバージョンへの正常なアップグレードに影響する可能性があります。
- ASR 1001-HX では、ベイ 1 8X10G/1G の最後の 4 ポートでのみマルチレートがサポートされます。

次の注意事項は、ルータの C8300、C8500L-8S4X モデルに適用されます。

- Cisco IOS XE リリース 17.15.1 以降では、10GE SFP+ モジュールが取り付けられている 10G インターフェイスで **negotiation auto** コマンドがサポートされます。
- Cisco IOS XE リリース 17.15.1 以降、10GE SFP+ モジュールを含む 10G インターフェイスでは、**show interface Tengig x/x/x** の出力で、**negotiation auto/no negotiation auto** の設定に関係なく、リンクタイプは常に **force-up** と表示されます。設定が Cisco SD-WAN Manager テンプレートを介してプッシュされる場合も同様です。

表 11: 自動ネゴシエーションの設定

C8500			
SFP	デフォルトの自動ネゴシエーション	デフォルトの速度	デフォルトのデュプレックス
1G 銅線	消灯	1000M	フル
1G 光	消灯	1000M	フル
10G Optical	消灯	10000M	フル
C8300			
1G 銅線	点灯	1000M	フル
1G 光	点灯	1000M	フル
10G Optical	点灯	10000M	フル



(注) ネゴシエーション設定がピアデバイスのインターフェイス設定と一致することを確認します。インターフェイスの設定に不一致があると、インターフェイスがダウンする可能性があります。

機能制限

単一の「universalk9」イメージの制限

- Dual-IOSd は、自律モードでのみサポートされます。
- ペイロード暗号化のないイメージと NO-LI (universalk9_npe、universalk9_noli、universalk9_npe_noli) イメージは、コントローラモードではサポートされていません。universalk9 イメージのみがサポートされています。
- オンボーディングして動作モードを決定後、コントローラモードから自律モードに、またはその逆に変更すると構成が失われます。
- リセットボタン機能は、Cisco ISR 1000 シリーズ サービス統合型ルータのコントローラモードではサポートされていません。コントローラモードのリセットボタンには、ゴールデンイメージや設定を復元する機能はありません。
- 自動インストール (Python と TCL スクリプト) および ZTP : 自動インストールおよび ZTP はコントローラモードではサポートされていません。DHCP がいずれかのプロセスを使用したインストールの試行を検出すると、自律モードへのモード変更がトリガーされます。

- WebUI : コントローラモードでは、WebUIはサポートされておらず、使用されている場合はエラーメッセージが表示されます。

自己署名済みトラストポイント

デバイスの起動時に自己署名トラストポイントが生成され、Cisco IOS XE Catalyst SD-WAN デバイ스에 로드됩니다. このトラストポイントが何らかの理由で削除された場合は、デバイスを再起動することにより、新しいトラストポイントを生成してロードすることができます。新しいキーは、削除されたキーとは異なる場合があります。

自律モードとコントローラモードの概要

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r リリースでは、自律モードとコントローラモードの2つのインストールモードが導入されています。自律モードはCisco IOS XE 非 Cisco Catalyst SD-WAN 展開の機能をサポートしており、コントローラモードは Cisco Catalyst SD-WAN ソリューションをサポートしています。

自律モードとコントローラモードの主な違いは次のとおりです。

表 12:

機能	自律モード	コントローラモード
コンフィギュレーション方式	• コマンドライン インターフェイス (CLI) • NETCONF	YANG ベースの構成 • Cisco SD-WAN Manager • NETCONF
オンボーディングモード	• プラグ アンド プレイ • 設定ウィザード • WebUI • ブートストラップ (USB、ブートフラッシュなど) • 自動インストール (Python スクリプト、TCL スクリプト) • ZTP (DHCP オプション 150 およびオプション 67 を使用)	• プラグ アンド プレイ • ブートストラップ (USB、ブートフラッシュなど)

機能	自律モード	コントローラモード
ライセンス	Cisco Smart Licensing	Cisco High Performance Security (HSEC) ソフトウェアライセンス。デバイスのライセンスはありません。
イメージタイプ	Universalk9	Universalk9
Dual-IOSd 冗長性モデル	サポート対象	未サポート
ハイ アベイラビリティ	サポート対象	未サポート
グローバル コンフィギュレーション モード	configure terminal	config-transaction

Cisco IOS XE ルータのソフトウェアのインストール

Cisco IOS XE リリース 17.2.1r 以降のソフトウェアのダウンロード

`router-model-universalk9.release-number` イメージ（Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のソフトウェア用）をシスコのサイト（<https://software.cisco.com>）からダウンロードします。

Cisco ASR、Cisco ISR および Cisco ENCS プラットフォームでのソフトウェアのインストール

インストール手順については、次のマニュアルを参照してください。

- [Cisco ISR 1000 シリーズ サービス統合型ルータ](#)
- [Cisco ISR 4000 シリーズ サービス統合型ルータ](#)
- [Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ](#)
- [Cisco ENCS 5100 および ENCS 5400 への Cisco Enterprise NFVIS のインストール](#)

Cisco CSR 1000v プラットフォームでのソフトウェアのインストール

CSR 1000v インスタンスを展開しているクラウドに応じて、以下を参照してブートストラップおよび/またはデイレゾ設定を実行します。

- [VM への OVA の展開](#)
- [.iso ファイルを使用した Cisco CSR 1000v VM の手動作成](#)（Citrix XenServer）

- 自己インストール型 .run パッケージを使用した CSR 1000v VM の作成
- .iso ファイルを使用した VM の手動作成 (Microsoft Hyper-V)
- CSR 1000v インスタンスの起動
- カスタムデータを使用した CSR 1000v VM の展開
- Microsoft Azure での Cisco CSR 1000v VM の展開

Cisco Catalyst 8000V Edge ソフトウェア プラットフォームのインストール

表 13: 機能の履歴

機能名	リリース情報	説明
OpenStack Train での Cisco Catalyst 8000V Edge ソフトウェア プラットフォームのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a	この機能では、OpenStack クラウド コンピューティング プラットフォーム「Train」リリースでホストされている Cisco Catalyst 8000V Edge ソフトウェア プラットフォームの管理のサポートが導入されています。

Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降、Cisco Catalyst SD-WAN は Cisco CSR1000V および Cisco ISRv に代わる Cisco Catalyst 8000V 仮想ルータプラットフォームをサポートします。Cisco Catalyst 8000V を Cisco Catalyst SD-WAN 環境にインストールするには、Cisco vManage リリース 20.4.1 以降が必要です。

展開方法に適した Cisco Catalyst 8000V ソフトウェアイメージをダウンロードします。たとえば、ESXi の OVA ファイル、あるいは OpenStack または KVM の QCOW2 イメージをダウンロードします。ISO イメージは選択しないでください。イメージを Cisco SD-WAN Manager ソフトウェア イメージ リポジトリにアップロードできる状態にします。ファイル名は c8000v-universalk9 で始まります。



- (注) Cisco Catalyst SD-WAN で操作するには、デバイスがコントローラモードになっている必要があります。デバイスをコントローラモードで起動する場合は、bootflash:packages.conf ファイルを使用してデバイスを起動します。

KVM、ESXi、および OpenStack 環境でのインストールを含む、プラットフォームの詳細については、[Cisco Catalyst 8000V Edge Software Installation and Configuration Guide \[英語\]](#) を参照してください。Cisco Catalyst 8000V を Cisco Catalyst SD-WAN にオンボードするためのブートスト

ラップファイルの作成については、「[Bootstrap Process for Cisco Catalyst SD-WAN Cloud-Hosted Devices](#)」を参照してください。

クリーンインストール

Cisco Catalyst 8000V のクリーンインストールを推奨します。クリーンインストールにより、すべての機能が確実にサポートされ、最新のライセンスが提供され、デバイスとコントローラの同期が維持されます。アップグレードが必要な場合は、**Cisco IOS XE リリース 17.2.1r 以降へのアップグレードの手順**を参照してください。



(注) Cisco Catalyst 8000V のクリーンインストール後、デバイスを Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以前のリリースにダウングレードすることはできません。

Cisco CSR1000V から Cisco Catalyst 8000V へのアップグレード

Cisco CSR1000V または Cisco ISRV 仮想ルータから Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a へのアップグレードには、Cisco Catalyst 8000V へのアップグレードが含まれます。次の点に注意してください。

- Cisco Catalyst 8000V は、Cisco CSR1000V または Cisco ISRV プラットフォームで使用可能なすべての機能を保持します。
- Cisco SD-WAN Manager でアップグレードを実行すると、アップグレードされるデバイスの設定が保持されます。

OpenStack

Cisco Catalyst 8000V を OpenStack Train リリースにインストールするには、Cisco Catalyst 8000V の Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a 以降のイメージを使用する必要があります。

シスコは、以前のイメージを使用して OpenStack に Cisco Catalyst 8000V をインストールすること、または以前のイメージを使用して OpenStack にインストールしてから Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a にアップグレードすることをサポートしていません。

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のリリースでのプラグアンドプレイ

プラグアンドプレイのオンボーディングワークフロー

1. 顧客のスマートアカウントとバーチャルアカウントの詳細情報を使用して、Cisco Commerce でデバイスを注文します。

2. デバイスのシリアル番号、スマートアカウント、仮想アカウントなど、Cisco Commerce のデバイス情報がプラグアンドプレイポータルに追加されます。
3. 同じスマートアカウントとバーチャルアカウントについて、Cisco SD-WAN Validator コントローラプロファイルをプラグアンドプレイ (PnP) ポータルに追加します。
4. 新しいデバイスを Cisco SD-WAN Validator コントローラプロファイルに手動で関連付けます。
5. PnP は、Cisco SD-WAN Validator の詳細、デバイスのシリアル番号、組織名、ネットワーク ID を含むすべての関連情報をゼロタッチプロビジョニング (ZTP) に送信します。
6. PnP からデバイスのシリアル番号ファイル (プロビジョニングファイル) をダウンロードし、Cisco SD-WAN Manager にアップロードします。Cisco SD-WAN Manager でデバイスが利用可能になりました。Cisco SD-WAN Manager の **Sync Smart Account** オプションを使用して、デバイスを仮想アカウントと同期し、Cisco SD-WAN Manager にデバイスを入力することもできます。



- (注) Cisco vManage リリース 20.3.x でデバイステンプレートを作成およびスケジュールし、ターゲットデバイスをオンボードする前に Cisco SD-WAN Manager を Cisco vManage リリース 20.4.1 以降にアップグレードした場合、PNP または ZTP を使用してデバイスをオンボードすると、テンプレートのプッシュが失敗します。この失敗を回避するには、Cisco SD-WAN Manager ソフトウェアをアップグレードしてからデバイスをオンボードした後にテンプレートを再スケジュールします。



- (注) デバイスのリロードまたは電源の再投入が原因でデバイスの ZTP プロセスが中断された場合、ZTP プロセスは再開されず、デバイスは元の設定にあった Cisco SD-WAN Manager イメージでオンラインになります。この場合、デバイスを目的の Cisco SD-WAN Manager リリースに手動でアップグレードします。



- (注) 詳細については、『[Plug and Play Support Guide](#)』を参照してください。

プラグアンドプレイ オンボーディングによるモードの検出

PnP ベースの検出プロセスは、コントローラの検出に基づいてデバイスが動作するモードを決定し、必要に応じてモード変更を開始します。モードを変更すると、デバイスが再起動します。再起動が完了すると、デバイスは適切な検出プロセスを実行します。

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降にアップグレードすると、Cisco IOS XE または Cisco Catalyst SD-WAN イメージをすでに実行しているシスコデバイスでは、設定されたコントローラに応じて、デバイスは自律モードまたはコントローラモードで起動します。

プラグアンドプレイ (PnP) 導入には、次の検出プロセスシナリオが含まれます。

表 14:

ブートアップ モード	構成モード	オンボーディ ング エージェ ント	Cisco SD-WAN Validator	ディスカバリ プ ロセス	モード変更
自律	Cisco Digital Network Architecture (DNA)	プラグ アンド プレイ	非対応	プラグアンドプレ イ接続の検出また はオンプレミスの プラグアンドプレ イサーバーの検出	モード変更 なし
自律	Cisco SD-WAN Manager	プラグ アンド プレイ	対応	Plug and Play Connect ディスカ バリ	コントロー ラモードへ のモード変 更
コントローラ	Cisco DNA	プラグ アンド プレイ	非対応	プラグアンドプレ イ接続の検出また はオンプレミスの プラグアンドプレ イサーバーの検出	自律モード へのモード 変更
コントローラ	Cisco SD-WAN Manager	プラグ アンド プレイ	対応	Plug and Play Connect ディスカ バリ	モード変更 なし

IP アドレスの自動検出

表 15: 機能の履歴

機能名	リリース情報	説明
ARP を使用したデイゼロ WAN インターフェイスの自動 IP 検 出	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco SD-WAN リリース 20.7.1 Cisco vManage リリース 20.7.1	この機能により、デバイスは、DHCP サーバーを利用できない場合に、利用可能な IP アドレスとデフォルトゲートウェイの情報を自動的に学習できます。デバイスは、その WAN インターフェイスに IP アドレスを割り当て、PnP サーバーに接続して、PnP オンボーディングプロセスを開始します。

通常、Cisco IOS XE Catalyst SD-WAN デバイス または Cisco vEdge デバイス の WAN インターフェイスは DHCP クライアントとして設定されており、このインターフェイスは、プラグアンドプレイ (PnP) オンボーディングプロセスの実行中に DHCP サーバーから IP アドレスとゲートウェイサーバーの情報を受け取ります。

DHCP サーバーが利用できない場合、デバイスは、Address Resolution Protocol (ARP) パケットを使用して、利用可能な IP アドレスとデフォルトゲートウェイの情報を自動的に学習します。デバイスが学習した IP アドレスによって PnP サーバーに正常に接続できる場合、デバイスは PnP オンボーディングプロセスを続行します。



(注) この機能は、デイズロ展開にのみ適用され、デフォルトで有効になります。

自動 IP アドレス検出の前提条件

- ARP をトリガーするには、プロバイダーエッジ (PE) ルータでデバイスの IP アドレスを BGP ネイバーとして設定します。

この PE ルータは、WAN トランスポートネットワーク内に存在するデバイスの最初の接続ポイントです。その後、PE ルータは、この IP アドレスを使用して ARP パケットをデバイスに送信します。デバイスが ARP パケットを受信すると、自動 IP アドレス検出機能が ARP 宛先 IP アドレスをデバイスの WAN インターフェイス IP アドレスとして定義します。

- Cisco IOS XE Catalyst SD-WAN デバイス の場合、この IP アドレスのネットワークマスクは 30 ビットである必要があります。
- オンプレミス ZTP サーバーを介した自動 IP アドレス検出およびリダイレクトの場合、DNS サーバー上の ZTP サーバーの A レコードを `ztp.cisco.com` に設定する必要があります。さらに、DNS サーバーは 8.8.8.8 または 8.8.4.4 の `ip name-server` 値を持つ必要があります。

自動 IP アドレス検出の場合、デバイスは 8.8.8.8 または 8.8.4.4 を DNS サーバーとして使用して `devicehelper.cisco.com` または `ztp.cisco.com` を解決します。その後、PnP プロセスは、オンボーディングを続行するために `devicehelper.cisco.com` または `ztp.cisco.com` への到達を試みます。



(注) デバイスが自動検出する IP アドレスは、PnP オンボーディングが完了する前に発生するデバイスの再起動時に保持されません。このような場合、PE ルータの ARP キャッシュが期限切れになると、IP アドレスが自動的に割り当てられます。

自動 IP アドレス検出の制限事項と制約事項

次の制限事項および制約事項は Cisco IOS XE Catalyst SD-WAN デバイス にのみ適用されます。

- この機能は、Cisco 1000 シリーズ サービス統合型ルータ、Cisco 4000 シリーズ サービス統合型ルータ、および Cisco Catalyst 8200 および 8300 シリーズ エッジプラットフォームでのみサポートされています。これらのデバイスでは、この機能は、ギガビットイーサネット インターフェイス 0/0/0 でのみサポートされています。

- この機能は、コントローラ（SD-WAN 構成）モードのデバイスでのみサポートされます。
<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/install-upgrade-17-2-later.html>を参照してください。
- この機能は、1 つの PE ルータと 1 つのカスタマーエッジルータが同じ VLAN に存在する単純な 30 ビット ネットワーク マスク レイヤ 2 ネットワークでのみサポートされます。
- この機能は、PE ルータの VRRP、HSRP、または GLBP をサポートしていません。
- ARP 宛先 IP アドレスは、デバイスが 150 秒の間隔内に同じ ARP 要求を 8 回受信した後のみ、デバイスの WAN インターフェイス IP アドレスとして使用されます。

PnP 以外のオンボーディング

Cisco Catalyst SD-WAN ブートストラップ設定ファイルの作成

ブートストラップファイルの生成については、「Cisco Catalyst SD-WAN デバイスのオンサイトブートストラッププロセス」および「CLI を使用した Cisco IOS XE Catalyst SD-WAN デバイスのブートストラップファイルの生成」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/hardware-and-software-installation.html#c_On_Site_Bootstrap_Process_for_SD_WAN_Devices_12488.xml
<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/hardware-and-software-installation.html#generate-bootstrap-file-using-cli>

新規インストール：モード変更デバイスのデイレゼロシナリオ

1. デバイスが新しいボックスで 17.2 より前の Universalk9 イメージを実行している場合、または **write erase** および **reload** を実行し、Cisco IOS XE 17.2 以降のイメージをロードした既存のボックスの場合、デバイスはデイレゼロ構成および自律モードで起動します。
2. 新しいデバイスは、ブートストラップファイルに基づいてモードの変更が必要かどうかを判断します。
 - ブートストラップ ロケーションに接続されているブートストラップファイルの `ciscosdwan.cfg` または `ciscosdwan_cloud_init.cfg` の場合、コントローラモードへのモード変更が開始されます。デバイスがコントローラモードで起動すると、構成ファイルに含まれる構成が適用されます。
 - `ciscottr.cfg` ブートストラップファイルまたは `config-wizard` が検出された場合は、モード変更が開始されず、起動は自律モードで続行されます。



- (注)
- ブートストラップファイル (ciscosdwan.cfg) は、Cisco SD-WAN Manager によって生成され、UUID を持ちますが、OTP はありません。
 - ソフトウェアデバイス (Cisco Catalyst 8000V Edge ソフトウェア、Cisco Cloud Services Router 1000V シリーズ、および Cisco ISRv) の場合や OTP 認証デバイス (Cisco ASR1002-X など) の場合は、ciscosdwan_cloud_init.cfg ブートストラップファイルを使用します。このファイルは OTP を持ちますが、UUID 検証はありません。

Cisco CLI を使用したモードの切り替え

コントローラモードと自律モードを切り替えるには、特権 EXEC モードで **controller-mode** コマンドを使用します。

自律モード

controller-mode reset コマンドは、デバイスをデイレート設定に戻します。

```
Device# controller-mode reset
```

controller-mode disable コマンドは、デバイスを自律モードに切り替えます。

```
Device# controller-mode disable
```



- (注) **controller-mode disable** は、デバイスを一時的に自律モードで動作させる場合にのみ使用してください。デバイスが同じイメージを使用してコントローラモードに戻っていることを確認します。

コントローラモード



- (注) デバイスをコントローラモードに切り替えるには、bootflash:/*.bin または bootflash:/packages.conf ファイルを使用してシステムを起動します。



- (注) bootflash:core または harddisk:core にコアファイル (プロセスクラッシュに関する情報を含むファイル) が含まれている場合は、デバイスをコントローラモードに変更する前に、ファイルを別の場所に移動します。これらのファイルが bootflash:core または harddisk:core ディレクトリに残っている場合、Cisco SD-WAN Manager はデバイスのオンボーディング後にアラームを表示します。ファイルは、コアディレクトリ以外のデバイス上の任意のディレクトリに移動できます。

controller-mode enable コマンドは、デバイスをコントローラモードに切り替えます。

Device# **controller-mode enable**

注

注記	説明
バンドル モード	デバイスがバンドルモード（スーパーパッケージ）で起動される場合、再起動後、イメージが自動的に展開されてアクティブ化され、SD-WAN動作のためにルータが準備されます。4GB RAM のデバイスでは、/bootflash のスペースを解放するために追加の再起動が必要になる場合があります。4GB RAM の次のデバイスはリロードする必要があります。 • Cisco ISR 4451 • Cisco ISR 4431 • Cisco ISR 4461 • Cisco ISR 4351 • Cisco ISR 4331 • Cisco ISR 4321
bootflash:/sdwaninstaller ディレクトリの内容の表示	次のいずれかの状況では、Cisco IOS XE Catalyst SD-WAN デバイスの bootflash:/sdwaninstaller ディレクトリの内容を表示できません。 • デバイスがコントローラモードになっている場合。 または • デバイスが自律モードになっていて、Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降を使用している場合。

デバイスのコントローラモードへの変更

自律モードからコントローラモードに変更するには、現在実行中のイメージのソフトウェアパッケージを展開する操作をデバイスで行う必要があります。展開操作にはブートフラッシュ領域が必要です。**controller-mode enable** コマンドを実行してコントローラモードに変更する場合、実行中のイメージのソフトウェアパッケージを展開するのに十分なブートフラッシュ領域がルータにない可能性があります。手順の最初のステップでは、これに対処します。

手順

ステップ 1 デバイスのブートフラッシュで使用可能な領域を確認します。ソフトウェアイメージの .bin ファイルに 100 MB を加えたサイズと等しい領域があることを確認します。

ステップ 2 デバイスで **controller-mode enable** コマンドを使用して、コントローラモードに変更します。

デバイスは、ブートフラッシュにソフトウェアイメージファイルを展開するのに十分な領域があることを確認します。

十分なブートフラッシュ領域がある場合、デバイスはコントローラモードで再起動し、ソフトウェアイメージを展開します。

ブートフラッシュに十分な領域がない場合、コマンドの出力には必要な領域が示され、デバイスはコントローラモードに移行しません。

(注)

次のリリース以降、デバイスはブートフラッシュにソフトウェアイメージファイルを展開するのに十分な領域があることを確認します。

- 17.12.x の Cisco IOS XE Catalyst SD-WAN リリース 17.12.5a 以降のメンテナンスリリース
- 17.12.x の Cisco IOS XE Catalyst SD-WAN リリース 17.15.2 以降のメンテナンスリリース
- Cisco IOS XE Catalyst SD-WAN リリース 17.16.1a 以降のすべてのリリース

以前のリリースでは、**controller-mode enable** コマンドを実行しても、ブートフラッシュにソフトウェアイメージファイルを展開するのに十分なスペースがあるかどうかは最初に確認されません。まずデバイスをコントローラモードに変更し、次にファイルを展開します。デバイスがイメージファイルを展開したことを確認し、展開していなかった場合はトラブルシュートを行うには、[「ブートフラッシュ領域の不足によるソフトウェアイメージの展開失敗のトラブルシュート」](#)を参照してください。

ブートストラップファイルによるモード検出とモード変更



- (注) Cisco IOS XE Catalyst SD-WAN デバイス ですでに古い Cisco Catalyst SD-WAN の構成バージョンまたはファイルが実行されている場合、デバイスを Cisco IOS XE Catalyst SD-WAN リリース 16.x から Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降にアップグレードすると、デバイスはコントローラモードで起動します。デバイスがコントローラモードで起動しないようにするには、デバイスのアップグレードを実行する前に、古い Cisco Catalyst SD-WAN 構成ファイルをブートフラッシュから削除してください。

ブートフラッシュからすべての Cisco Catalyst SD-WAN アーティファクトを削除するための詳細な手順は、次のとおりです。

```
delete /force bootflash:/ciscosdwan*.cfg
delete /force /recursive bootflash:/sdwaninstallerfs
delete /force /recursive bootflash:/sdwaninstaller
delete /force /recursive bootflash:/sdwaninternal
delete /force /recursive bootflash:/sdwan
delete /force /recursive bootflash:/vmanage-admin
delete /force /recursive bootflash:/cdb_backup
delete /force /recursive bootflash:/installer/active
delete /force /recursive bootflash:/installer
```

すでに Cisco Catalyst SD-WAN イメージを実行しているデバイスの場合、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のイメージをアップグレードすると、デバイスがコントローラモードで起動します。



- (注) Cisco Catalyst 8000V を OpenStack にインストールするには、Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a 以降の Cisco Catalyst 8000V イメージを使用する必要があります。

controller-mode enable コマンドを使用して自律モードからコントローラモードに切り替え、**controller-mode disable** コマンドを使用してコントローラモードから自律モードに切り替えます。

CLIを使用してモードを切り替えるには、次の表に示されている適切な構成ファイルが存在することを確認してください。デバイスが起動すると、コンフィギュレーションファイル内の設定が適用されます。デバイスは、構成ファイルを読み取り、構成情報を使用してネットワークに接続します。

表 16: モードを変更するための構成ファイルの前提条件

現在のモード	変更後のモード	プラットフォーム	構成ファイルと場所
コントローラ	自律	サポートされているすべてのプラットフォーム	デバイスで使用可能な任意のファイルシステムの <code>ciscotr.cfg</code>
自律	コントローラ	- シスコ クラウド サービス ルータ (CSR) 1000v - シスコ サービス 統合型仮想ルータ (ISRv) - Cisco Catalyst 8000V - Cisco ASR 1002-X	ブートフラッシュ、USB、CDROM0、または CDROM1 上の <code>ciscosdwan_cloud_init.cfg</code>
自律	コントローラ	- Cisco アグリゲーション サービス ルータ (ASR) 1000 シリーズ - Cisco サービス 統合型ルータ (ISR) 4000 シリーズおよび 1000 シリーズ ルータ	ブートフラッシュまたは USB 上の <code>ciscosdwan.cfg</code>



- (注) Cisco CSR1000v デバイス (Cisco IOS XE リリース 17.2 以降の場合) および Cisco Catalyst 8000V (Cisco IOS XE リリース 17.4 以降の場合) イメージの展開では、デバイスをコントローラモードで起動する場合、Cisco SD-WAN Manager でブートストラップ (ESXi、KVM、および OpenStack)、ユーザーデータ (AWS)、またはカスタムデータ (Azure および GCP) によって生成されたブートストラップファイルをロードします。

`ciscosdwan_cloud_init.cfg` ブートストラップファイルに次のフィールドが存在する必要があります。

- otp
- uuid
- vbond
- org



- (注) デバイスを自律モードからコントローラモードに切り替えると、スタートアップコンフィギュレーションと NVRAM (証明書) の情報が消去されます。このアクションは、**write erase** コマンドを実行したのと同じです。



(注) デバイスをコントローラモードから自律モードに切り替えると、すべての Yang ベースの設定が保持され、元のコントローラモードに切り替えた場合に再利用できます。



(注) デバイスが DayN 構成に含まれており、リロードされた場合、ブートストラップファイルの存在はデバイスの動作モードに影響を与えません。



(注) 次のいずれかの状況では、Cisco IOS XE Catalyst SD-WAN デバイスの bootflash:/sdwaninstaller ディレクトリおよび .sdwaninstallerfs ファイルの内容を表示できません。

- デバイスがコントローラモードになっている場合。
- または
- デバイスが自律モードになっていて、Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降を使用している場合。

コントローラモードでファイルおよびディレクトリが非表示になっている場合、ディレクトリなどのコピーおよび削除操作は実行できません。

コントローラモード設定のリセット

request platform software sdwan config reset または **request platform software sdwan software reset** コマンドを使用してデバイスをコントローラモードのデフォルト設定に戻すと、デバイスは次のいずれかのアクションを実行します。

- モード検出を実行します。モード検出の詳細については、[プラグアンドプレイ オンボーディングによるモードの検出 \(119 ページ\)](#) を参照してください。
- 適切な設定ファイルを使用してブートストラップを実行します。Cisco Catalyst SD-WAN ブートストラップ設定ファイルの詳細については、[Cisco Catalyst SD-WAN ブートストラップ設定ファイルの作成 \(122 ページ\)](#) を参照してください。

現在アクティブなイメージの Cisco Catalyst SD-WAN 設定を消去するには、次の CLI を使用します。

```
Device# request platform software sdwan config reset
%WARNING: Bootstrap file doesn't exist and absence of it can cause loss of connectivity
to the controller.
For saving bootstrap config, use:
request platform software sdwan bootstrap-config save
Proceed to reset anyway? [confirm]
Backup of running config is saved under /bootflash/sdwan/backup.cfg
WARNING: Reload is required for config-reset to become effective.
```




- (注) 上記の設定にリストされている警告は、Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降のイメージでのみ表示されます。

変更を有効にするには、CLI の実行後にルータをリロードする必要があります。この CLI を実行すると、現在インストールされているバージョンの設定が暗号キーとともに消去され、デバイスはリロード後にデイズロワークフローに入ります。

オンボーディングに PnP を使用するようにデバイスが設定されていない場合、デバイスはブートフラッシュ内の設定ファイルを読み取り、設定情報を使用してネットワークに接続します。デバイスが PnP オンボーディングを使用するように設定されている場合、リロード後に PnP 検出が再開されます。



- (注) パブリッククラウドの場合、新規インストールと同様に、追加のブートストラップ設定がプロビジョニングされ、インスタンスにログインできるようになります。



- (注) パブリッククラウドおよびNFVIS環境では、設定のリセット操作の前に、最新のデイズロブートストラップ設定ファイル（Cisco SD-WAN Manager からエクスポート）がサポートされている場所で使用可能であり、標準のファイル命名規則（例：bootflash:/ciscosdwan_cloud_init.cfg ファイル）に従っていることを確認してください。が実行されます。



- 警告** これらの環境でブートストラップファイルを保存しないと、仮想マシンの接続が失われます。

リセットされた構成

設定をリセットすると、デバイスは次の処理を実行します。

- 現在実行中のイメージの設定のみを消去します。
- 証明書を消去します。
- 同じイメージを使用してルータを再起動します。この時点で、デバイスは Day-0 起動を繰り返します。

ソフトウェアリセット

ソフトウェアリセットを実行すると、デバイスは次の処理を実行します。

- 証明書を含む bootflash:/sdwan フォルダに保存されているすべての SD-WAN メタデータを消去します。

- すべてのイメージの設定を消去します（実行中のイメージと以前にアクティブ化されたイメージ）。
- デフォルトとしてマークされているファイルを除き、すべてのイメージファイルを削除します。
- デフォルトバージョンのイメージを使用してルータを再起動します。この時点で、デバイスは Day-0 起動を繰り返します。

モードスイッチング：追加情報

モード切り替え中の設定の永続性

表 17:

現在の構成モード	切り替えた後のモード	動作
自律	コントローラ	NVRAMの内容とスタートアップ構成が消去されます。構成は復元されません。デバイスはデイズロ構成に戻ります。以前の実行構成はブートフラッシュに保存されます。 (注) 自律モードをコントローラモードに切り替えてから、自律モードに戻すと、スタートアップ構成が空であるために、Cisco IOS XE 構成は復元されません。バックアップから構成を手動で復元する必要があります。
コントローラ	自律	CDBの内容は消去され（後続のモードのスイッチで）、Cisco IOS 構成は復元されません（スタートアップ構成が空であるため）。バックアップから構成を手動で復元する必要があります。

コントローラモードと自律モードの検証

コントローラモードのコマンド出力の表示

```
Device# show logging | include OPMODE_LOG
*Dec  8 16:01:17.339: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in CONTROLLER mode

Device# show version | inc operating

Router operating mode: Controller-Managed
```

```

Device# show platform software device-mode
Operating device-mode: Controller

Device-mode bootup status:
-----
Success

Device# show platform software chasfs r0 brief | inc device_managed_mode

/tmp/chassis/local/rp/chasfs/etc/device_managed_mode : [controller]
/tmp/fp/chasfs/etc/device_managed_mode : [controller]

Device# show version | inc Last reload
Last reload reason: Enabling controller-mode

```

自律モードでの show コマンド出力

```

Device# show logging | include OPMODE_LOG
*Dec  8 17:01:17.339: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode

Device# show version | inc operating

Router operating mode: Autonomous

Device# show platform software device-mode

Operating device-mode: Autonomous

Device-mode bootup status:
-----

Device# show platform software chasfs r0 brief | inc device_managed_mode

/tmp/chassis/local/rp/chasfs/etc/device_managed_mode : [autonomous]
/tmp/fp/chasfs/etc/device_managed_mode : [autonomous]

Device# show version | inc Last reload
Last reload reason: Enabling autonomous-mode

```



(注) デバイスがコントローラモードの場合、**show sdwan running-config** コマンドでは次の情報は表示されません。

- tcp-small-servers、udp-small-servers、tcp-keepalives-in、および tcp-keepalives-out を除く /native/service の下のすべてのサービスコマンド
- transport、access-class、および ipv6 access-class を除く VTY 回線の下の設定
- IPv6 ユニキャストルーティングの設定
- /native/enable のコマンド

これらの設定を確認するには、**show running-config** コマンドを使用します。

インストール後のコンソールポートアクセスの変更（コントローラモード）

はじめる前に

この手順を開始する前に、現在設定されているコンソールアクセス方式を介して Cisco CSR1000V または Cisco Catalyst 8000V ルータにアクセスできることを確認してください。

コンソールポートアクセスの変更

この手順では、コンソールに接続して Cisco CSR1000V または Cisco Catalyst 8000V ソフトウェアデバイスにアクセスする方式を変更します。

Cisco CSR1000V または Cisco Catalyst 8000V ソフトウェアの展開に使用されるイメージによって、使用するコンソールアクセスのデフォルトのタイプ（仮想またはシリアル）が決まります。

この手順には、コントローラモードから自律モードに変更し、その後にコントローラモードに戻す（Cisco Catalyst SD-WAN とともに動作するために必要）というモードの変更が含まれます。これらのモード変更により、デバイスがリロードされます。

コンソールポートアクセスを変更するには、次の手順を実行します。

1. EXEC モードで **enable** を入力して特権 EXEC モードを開始します。

```
Router> enable
```

2. コントローラモードを無効にします。次のコマンドを入力し、プロンプトに従ってコマンドを完了します。

```
Device# controller-mode disable
```



(注) これにより、デバイスが自律モードで再起動します。

3. デバイスが再起動したら、**enable** を入力して特権 EXEC モードを開始します。

```
Router> enable
```

4. グローバル コンフィギュレーション モードを開始します。

```
Device# configure terminal
```

5. 次のいずれかのオプションを使用して、アクセスのタイプを設定します。

- **virtual** : このオプションにより、ハイパーバイザの仮想VGA コンソールを介してデバイスにアクセスすることが指定されます。

```
Device(config)# platform console virtual
```

- **serial** : このオプションにより、仮想マシン（VM）のシリアルポートを介してデバイスにアクセスすることが指定されます。



(注)

- このオプションは、ハイパーバイザがシリアルポートコンソールアクセスをサポートしている場合にのみ使用してください。
- デバイス構成が Cisco SD-WAN Manager デバイステEMPLATE として保存され、Cisco SD-WAN Manager を使用してデバイスにアタッチされている場合は、次のコマンドを

```
Device(config)# platform console serial
```

CLI アドオン機能TEMPLATEに入力します。CLI アドオン機能TEMPLATEの詳細については、『[Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide](#)』を参照してください。これは、デバイステEMPLATEがデバイスにアタッチされているときに、Cisco SD-WAN Manager によるシリアルポートの削除を回避するために役立ちます。

```
Device(config)# platform console serial
```

- **auto** : (このオプションは廃止されており、推奨されません) このオプションにより、デバイスコンソールの自動検出が指定されます。これは、初期インストールブートプロセス中のデフォルト設定です。詳細については、「[VM と連動した Cisco CSR 1000v の起動](#)」を参照してください。

6. コンフィギュレーション モードを終了します。

```
Device(config)# end
```

7. 設定を保存します。

```
Device# write memory
```

8. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

```
Device# copy system:running-config nvram:startup-config
```

9. デバイスをコントローラモードに戻します。次のコマンドを入力し、プロンプトに従ってコマンドを完了します。

```
Device# controller-mode enable
```



(注)

この手順により、デバイスがコントローラモードで再起動します。

Cisco IOS XE リリース 17.2.1r 以降へのアップグレード

サポートされるアップグレード

表 18 : Cisco CSR1000V および Cisco ISRv ルータ

可能なアップグレード先...	元のリリース
Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a	Cisco IOS XE SD-WAN 17.3.1a 以降 Cisco IOS XE SD-WAN 17.2.2 以降 Cisco IOS XE SD-WAN 16.12.4a 以降 (注) • Cisco CSR1000V または Cisco ISRv ルータを、ここにリストされていないリリースから Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a にアップグレードするには、最初にこれらのリリースのいずれかにアップグレードする必要があります。 • Cisco CSR1000V または Cisco ISRv ルータから Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a へのアップグレードには、Cisco Catalyst 8000V へのアップグレードが含まれます。
Cisco IOS XE 17.3.x	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r Cisco IOS XE リリース 17.2.1v Cisco IOS XE SD-WAN 16.12.x Cisco IOS XE SD-WAN 16.11.x Cisco IOS XE SD-WAN 16.10.x Cisco IOS XE SD-WAN 16.9.x
Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	Cisco IOS XE SD-WAN 16.12.x Cisco IOS XE SD-WAN 16.11.x Cisco IOS XE SD-WAN 16.10.x Cisco IOS XE SD-WAN 16.9.x

表 19: Cisco Catalyst SD-WAN のサポート対象のすべてのルータ（Cisco CSR1000V、Cisco ISRv、および Cisco Catalyst 8000V を除く）

可能なアップグレード先...	元のリリース
Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a	Cisco IOS XE SD-WAN 17.3.1a 以降 Cisco IOS XE SD-WAN 17.2.1 以降 Cisco IOS XE SD-WAN 16.12.4a 以降
Cisco IOS XE 17.3.x	
Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	Cisco IOS XE SD-WAN 16.12.x Cisco IOS XE SD-WAN 16.11.x Cisco IOS XE SD-WAN 16.10.x Cisco IOS XE SD-WAN 16.9.x

デバイスを Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のイメージにアップグレードするには、次の手順を使用します。



(注) ロールバックオプションを確保するため、既存のイメージは削除しないでください。



(注) アップグレードが失敗した場合は、新しいソフトウェアイメージを再アクティブ化しないでください。代わりに、新しいソフトウェアイメージを削除し、失敗の原因となった可能性のある構成設定を特定して修正し、アップグレード手順を再試行します。問題が解決しない場合は、シスコにお問い合わせください。



(注) Cisco IOS XE リリース 17.3.1a 以前から Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a にアップグレードする場合、機能テンプレートが切り離されている間は、CLI を使用してデバイス設定を変更しないことをお勧めします。Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降、Cisco Catalyst SD-WAN は支援型アップグレードを使用します。このアップグレード手順では、Cisco Catalyst SD-WAN はアップグレード前にデバイス設定を保存します。CLI を使用して変更されたデバイスの設定が Cisco Catalyst SD-WAN の設定と同じでない場合、アップグレード後のデバイスの設定に矛盾が生じます。

たとえば、CLI を使用してデバイスの BGP AS 番号を別の値に設定した場合、デバイスの設定に一貫性がなくなり、アップグレードが失敗します。デバイスが CLI モードのときにアップグレードを実行する場合は、BGP AS 番号を元の値に戻してから、デバイスをアップグレードする必要があります。そのため、Cisco Catalyst SD-WAN を使用してデバイスをアップグレードすることをお勧めします。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降、プライマリ トンネル インターフェイスがセルラーインターフェイスで、バックアップ トンネル インターフェイスがギガビットインターフェイスであるデバイスのファームウェアをアップグレードする場合、ファームウェアアップグレードのプライマリインターフェイスとしてギガビットインターフェイスを使用します。

トンネルインターフェイスの優先順位の設定については、『Cisco Catalyst SD-WAN Command Reference』の `vmanage-connection-preference` コマンドを参照してください。優先度の値が高く設定されたインターフェイスは、優先度が高くなります。

Cisco Catalyst SD-WAN を使用したアップグレード

Cisco SD-WAN Manager を使用してアップグレードすることを推奨します。アップグレードすると、デバイスとコントローラの同期が維持されます。

- 『Cisco Catalyst SD-WAN Monitor and Maintain』ガイドで説明されている「Cisco SD-WAN Manager [upgrade and activate](#)」の手順を使用します。

CLI を使用したアップグレード

Cisco SD-WAN Manager を使用してアップグレードすることを推奨します。アップグレードすると、デバイスとコントローラの同期が維持されます。CLIを使用してアップグレードする必要がある場合は、次の手順を使用します。

構成ファイルのバックアップ

手動アップグレードプロセスを実行する前に、次の手順を使用して構成ファイルのコピーを作成します。この手順を実行しないと、アップグレード中にルータの設定が失われます。



- (注) 展開環境が Amazon Web Services (AWS) などのパブリッククラウドサービスにある場合、手動でアップグレードする前に設定を保存しないと、デバイスとの接続が失われ回復できない可能性があります。ハードウェアデバイスとは対照的に、仮想ルータへのコンソールアクセスを取得する方法がない場合があります。

- 次のコマンドを使用して、Cisco IOS XE Catalyst SD-WAN の設定のバックアップコピーを作成します。

```
show running-config | redirect bootflash:/sdwan/ios.cli
```

- 次のコマンドを使用して、Cisco Catalyst SD-WAN の実行コンフィギュレーションのバックアップコピーを作成します。

```
show sdwan running-config | redirect bootflash:/sdwan/sdwan.cli
```


アップグレード手順

1. <https://software.cisco.com> からデバイスの Cisco IOS XE リリース 17.2 イメージをダウンロードします。

2. からデバイスの Cisco IOS XE リリース 17.2 イメージをダウンロードします。

3. 新しいソフトウェアをインストールします。例：

```
Device# request platform software sdwan software install
bootflash:/isr4300-universalk9.17.2.1.SPA.bin
```

4. ソフトウェアをアクティブ化します。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。例：

```
Device# request platform software sdwan software activate 17.2.01r.9.3
```

5. ソフトウェアがアクティブ化されていることを確認します。

```
Device# show sdwan software
```

VERSION	ACTIVE	DEFAULT	PREVIOUS	CONFIRMED	TIMESTAMP
16.12.1d.0.48	false	true	true	auto	2020-03-04T10:43:45-00:00
17.2.01r.9.3	true	false	false	user	2020-03-04T11:15:20-00:00

```
Total Space:388M Used Space:100M Available Space:285M
```

6. (オプション) ソフトウェアのリセットが必要な場合に新しいバージョンが保持されるようにするには、次のコマンドを使用します。例：

```
Device# request platform software sdwan software set-default 17.2.01r.9.3
```

7. **request platform software sdwan software upgrade-confirm** を使用してアップグレードを検証します。

```
Device# request platform software sdwan software upgrade-confirm
```



- (注) 17.6.1 リリース以降、アップグレード確認機能が既存の操作に対して保留中の場合、イメージまたはソフトウェアメンテナンスアップデート (SMU) に対する別のインストール、アクティブ化または非アクティブ化操作は実行できません。



- (注) コントローラモードで **config-transaction** コマンドを使用して、グローバル コンフィギュレーションモードを開始します。**configuration terminal** コマンドは、コントローラモードではサポートされていません。

表 20: アップグレードシナリオでの設定の永続性

既存のインストール（イメージ）	アップグレード先（イメージ）	動作
Cisco IOS XE SD-WAN リリース 16.12 以前（ucmk9）	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r（universalk9）	デバイスはコントローラモードで起動し、設定は保持されます。
Cisco IOS XE リリース 16.12 以前（universalk9）	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r（universalk9）	デバイスは自律モードで起動し、設定は（スタートアップコンフィギュレーションを介して）保持されます。

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のリリースからのダウングレード

Cisco IOS XE Catalyst SD-WAN デバイスの以前にインストールされたソフトウェアイメージへのダウングレード

CLI を使用して、Cisco IOS XE Catalyst SD-WAN デバイスをデバイスに現在インストールされている以前のソフトウェアイメージにダウングレードするには、次の手順を実行します。

1. 現在インストールされているイメージを表示します。

```
Device# show sdwan software
```

Example:

VERSION	ACTIVE	DEFAULT	PREVIOUS	CONFIRMED	TIMESTAMP
16.10.400.0.0	false	true	true	auto	2019-11-20T04:40:05-00:00
17.3.1.0.102822	true	false	false	auto	2020-07-31T11:01:22-00:00

2. イメージをアクティブにします。これにより、デバイスがリセットされ、既存の構成が削除されます。デバイスはゼロデイ構成で起動します。

```
Device# request platform software software activate desired-build
```

例：

```
Device# request platform software software activate 16.10.400.0.0
```

Cisco IOS XE Catalyst SD-WAN デバイスの古いソフトウェアイメージへのダウングレード

以前のソフトウェアイメージをダウンロードし、CLIを使用して Cisco IOS XE Catalyst SD-WAN デバイスを以前のソフトウェアイメージにダウングレードするには、次の手順を実行します。

1. 現在インストールされているイメージを表示します。

```
Device# show sdwan software
```

Example:

VERSION	ACTIVE	DEFAULT	PREVIOUS	CONFIRMED	TIMESTAMP
16.10.400.0.0	false	true	true	auto	2019-11-20T04:40:05-00:00
17.3.1.0.102822	true	false	false	auto	2020-07-31T11:01:22-00:00

2. 必要に応じて、既存のソフトウェアイメージを削除して、新しいソフトウェアイメージをロードするための領域を用意します。

```
Device# request platform software sdwan software remove previous-installed-build
```

例:

```
Device# request platform software sdwan software remove 16.10.400.0.0
```

3. ダウングレード用のソフトウェアイメージをダウンロードし、デバイスのブートフラッシュにコピーします。
4. ダウンロードしたイメージをインストールします。

```
Device# request platform software sdwan software install bootflash:/desired-build
```

例:

```
Device# request platform software sdwan software install
bootflash:/isr1100be-universalk9.17.02.01a.SPA.bin
```

5. 現在インストールされているイメージを表示します。これには、新しいイメージが含まれています。

```
Device# show sdwan software
```

VERSION	ACTIVE	DEFAULT	PREVIOUS	CONFIRMED	TIMESTAMP
17.02.01a.0.211	false	true	true	auto	2020-03-30T09:34:04-00:00

6. 新しいイメージをアクティブにします。これにより、デバイスがリセットされ、既存の構成が削除されます。デバイスはゼロデイ構成で起動します。

```
Device# request platform software sdwan software activate desired-build clean
```

例:

```
Device# request platform software sdwan software 17.02.01a.0.211 clean
```

Cisco IOS XE リリース 17.2.x のダウングレードシナリオ

表 21: ダウングレードシナリオでの設定の永続性

既存のインストール（イメージ）	ダウングレード先（イメージ）	動作
コントローラモードの Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r (universalk9)	Cisco IOS XE SD-WAN リリース 16.12 以前 (ucmk9)	デバイスは ucmk9 イメージで起動し、ucmk9 イメージがデバイスにインストールされていた場合、設定が復元されます。 古いイメージバージョンのフレッシュインストールにダウングレードすると、デバイスは Day 0 構成になります。続行するには、アクティベーション時に clean オプションを使用します。
自律モードの Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r (universalk9)	Cisco IOS XE リリース 17.1.1 以前 (universalk9)	デバイスが universalk9 イメージで起動し、設定が復元されます。



(注)

- コントローラモードから Cisco IOS XE Amsterdam リリース 17.1.x や以前のリリースの universalk9、またはその他の非 Cisco Catalyst SD-WAN イメージへの直接ダウングレードはサポートされていません。コントローラモードから以前の IOS XE イメージにダウングレードするには、自律モードに切り替えて、ダウングレードプロセスを実行します。
- 自律モードから Cisco IOS XE SD-WAN 16.12 以前の ucmk9 SD-WAN イメージへの直接ダウングレードはサポートされていません。自律モードから以前の Cisco IOS XE Catalyst SD-WAN イメージにダウングレードするには、コントローラモードに切り替えて、ダウングレードプロセスを実行します。

スマートライセンスとスマートライセンス予約の復元

デバイスが自律モードからコントローラモードに切り替わり、再び自律モードに戻ると、スマートライセンス認証は失われます。

スマートライセンスの詳細については、『[Smart Licensing Guide for Access and Edge Routers](#)』を参照してください。

スマートライセンスの復元

1. Cisco Smart Software Manager (CSSM) に到達するようにデバイスを再設定します。
2. 特権 EXEC モードで **license smart register idtoken token force** コマンドを使用してデバイスを登録します。
3. **platform hardware throughput crypto crypto-value** を使用して、必要な暗号化スループットを設定します。
4. 特権 EXEC モードで **write memory** を使用して設定を保存します。
5. デバイスをリロードし、**show platform hardware throughput crypto** コマンドを使用して新しい暗号化スループット値が適用されていることを確認します。

スマートライセンス予約の復元

1. グローバル コンフィギュレーション モードで **license smart reservation** コマンドを使用して、予約モードを有効にします。
2. **platform hardware throughput crypto crypto-value** を使用して、必要な暗号化スループットを設定します。
3. **write memory** を使用して設定を保存します。
4. デバイスをリロードし、**show platform hardware throughput crypto** コマンドを使用して新しい暗号化スループット値が適用されていることを確認します。

クラウドサービスによってホストされる Cisco Catalyst 8000V Edge ソフトウェアのオンボード（PAYG ライセンスを使用）

ペイアズユーゴー（PAYG）ライセンスを使用して、クラウドサービスによってホストされる Cisco Catalyst 8000V プラットフォームをオンボードするには、次の手順を実行します。

また、Cisco Cloud onRamp for Multi-Cloud を使用して、PAYG ライセンスで Cisco Catalyst 8000V プラットフォームをオンボードすることもできます。パブリック クラウドインフラストラクチャを Cisco Catalyst SD-WAN ファブリックに統合する方法については、『[Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.x](#)』を参照してください。



- (注) この手順は、Amazon Web Services (AWS) によってホストされている Cisco Catalyst 8000V に適用されます。

1. Cisco SD-WAN Manager メニューから **[Configuration] > [Devices]** の順に選択し、**[Add PAYG WAN Edges]** をクリックします。
 2. **[Add PAYG WAN Edges]** ダイアログボックスで、Cisco Catalyst SD-WAN にオンボードする PAYG デバイスの数を入力し、**[Validate]** チェックボックスをオンにして、**[Add]** をクリックします。
- [Task View]** ページが開き、Cisco SD-WAN Manager による論理デバイス作成の進行状況が表示されます。



(注) 検証により、Cisco SD-WAN Manager がデバイスのリストをネットワーク内の Cisco Catalyst SD-WAN Validator および Cisco Catalyst SD-WAN コントローラ コントローラにパブリッシュします。

3. **[Task View]** ページに論理デバイスが正常に作成されたことが表示されたら、**[Configuration] > [Devices]** の順に選択し、**[Devices]** ページに新しい論理デバイスを表示します。



(注) **[Chassis Number]** 列には、各論理デバイスの一意の識別子が表示されます。

4. 作成された論理デバイスについて、**[...]** をクリックし、**[Generate Bootstrap Configuration]** を選択します。
5. (任意) 作成された論理デバイスにデバイステンプレートをアタッチします。
6. **[Generate Bootstrap Configuration]** ダイアログボックスで、**[Cloud-Init]** をクリックし、**[OK]** をクリックします。

[Generate Bootstrap Configuration] ダイアログボックスに論理デバイスの UUID を含むブートストラップ構成の内容が表示されます。デバイステンプレートがアタッチされている場合は、そのテンプレートによって提供される構成の詳細も含まれます。



(注) UUID は、**[Devices]** テーブルの **[Chassis Number]** 列の識別子に対応します。

7. クラウドサービスの C8000V インスタンスにブートストラップ構成をロードする方法は複数存在します。使用する方法は、クラウドサービスによって異なります。**[Generate Bootstrap Configuration]** ダイアログボックスで **[Download]** をクリックしてブートストラップ構成のコピーを保存することをお勧めします。
8. クラウドサービスポータルで Cisco Catalyst 8000V の PAYG 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 SD-WAN Manager で作成したブートストラップ構成を使用します。Cisco Catalyst SD-WAN のブートストラップ構成をインスタンスにロードする方法の詳細は、クラウド サービス プロバイダーに固有です。



- (注) AWS では、インスタンスを起動するためのワークフローに、ブートストラップ構成のロードを可能にするユーザーデータ手順が含まれます。

9. クラウドサービスプラットフォームで、前の手順のブートストラップ構成を使用して Cisco Catalyst 8000V インスタンスを起動します。

Cisco Catalyst 8000V インスタンスは、起動すると、Cisco Catalyst SD-WAN オーバーレイに自動的に参加します。Cisco SD-WAN Manager の [Devices] ページでは、この Cisco Catalyst 8000V インスタンスの [State] 列に緑色のメダルのアイコンが表示され、[Device Status] 列に「In Sync」と表示されます。



- (注) [Devices] ページでは、Cisco Catalyst SD-WAN オーバーレイに参加していない論理デバイスの場合、[State] 列に点線の円のアイコンが表示されます。

Cisco Catalyst 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

はじめる前に

デバイステンプレートは、Cisco SD-WAN Manager へのデバイスの接続を可能にする構成の詳細情報を提供します。

論理デバイスを作成し、最初にデバイステンプレートをアタッチすることなくブートストラップ構成を生成すると、生成されるファイルには最小限の構成が含まれます。ブートストラップ構成を生成する前にデバイステンプレートを論理デバイスにアタッチすると、生成されるファイルにはより完全な構成が含まれ、デバイスを Cisco Catalyst SD-WAN オーバーレイに接続できるようにするために役立ちます。ブートストラップ構成を作成する前にデバイステンプレートを論理デバイスにアタッチすることをお勧めします。

この手順は、Cisco Catalyst 8000V などのソフトウェアデバイスを KVM、ESXi、OpenStack などのプライベートクラウドにオンボードする場合に役立ちます。

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

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Devices] の順に選択します。
2. クラウドでホストされる新しいインスタンスに使用している論理デバイス（UUIDを含む）について、[...] をクリックし、[Generate Bootstrap Configuration] を選択します。
3. [Generate Bootstrap Configuration] ダイアログボックスで、[Cloud-Init] を選択し、[OK] をクリックします。[Generate Bootstrap Configuration] ダイアログボックスに、ライセンスの OTP

トークン、Cisco SD-WAN Validator アドレス、UUID、および組織情報を含むブートストラップ構成が表示されます。



(注) UUID は、[Devices] テーブルの [Chassis Number] 列の識別子に対応します。



(注) ブートストラップ構成に含まれるインターフェイスの数が、クラウド環境で仮想デバイスインスタンスが持つインターフェイスよりも多くないことを確認します。

4. クラウドサービスのデバイスインスタンスにブートストラップ構成をロードする方法は複数存在します。使用する方法は、クラウドサービスによって異なります。[Generate Bootstrap Configuration] ダイアログボックスで [Download] をクリックしてブートストラップ構成のコピーを保存することをお勧めします。

クラウドサービスでデバイスインスタンスをセットアップするときに、ブートストラップ構成を使用できます。この構成により、デバイスインスタンスが Cisco Catalyst SD-WAN に接続できるようになります。

プライベートクラウドへの Cisco Catalyst 8000V のオンボーディングについては、次を参照してください。

- 『Cisco Catalyst 8000V Edge Software Installation And Configuration Guide』の「Installing in KVM Environments」
- 『Cisco Catalyst 8000V Edge Software Installation And Configuration Guide』の「Installing in VMware ESXi Environment」
- 『Cisco Catalyst 8000V Edge Software Installation And Configuration Guide』の「Installing in OpenStack」

Cisco Catalyst 8000V のブートストラップ構成ファイルの例については、『Cisco Catalyst 8000V Cloud Initialization Files』を参照してください。

トラブルシューティング

ソフトウェアインストールのトラブルシューティング

ブート後にルータが以前のソフトウェアバージョンをロードする

ブート後にルータが以前のソフトウェアバージョンをロードする

問題

ルータは、以前にインストールされたソフトウェアバージョンを使用して起動します。

条件

Cisco IOS XE を使用するルータに、2 つ以上のソフトウェアバージョンがインストールされている。

考えられる原因

ルータがブートアップを開始していて、ブートアップ中に電源を再投入すると、以前にインストールされたソフトウェアバージョンを使用して再起動する場合があります。



(注) Cisco IOS XE デバイスには、以前にインストールされたソフトウェアバージョンを保持するメカニズムがあります。破損したソフトウェアイメージでブートアップ中にスタックすることを防ぐため、デバイスは以前にインストールされたソフトウェアバージョンにフォールバックできます。このフォールバックは、ブートアップ中にデバイスの電源の再投入が発生した場合にも発生する可能性があります。この場合（ブートアップ中に電源を再投入）、デバイスを再起動して最新のソフトウェアをロードできます。

対処方法

1. 次のいずれかの手順を使用して、デバイスのアクティブおよび非アクティブなシステムソフトウェアバージョンを確認します。
 - Cisco SD-WAN Manager の手順：
 1. Cisco SD-WAN Manager のメニューから **[Monitor] > [Devices]** の順に選択します。
 2. [Hostname] 列のデバイス名をクリックします。
 3. 左ペインで **[Real Time]** をクリックします。
 4. [Device Options] フィールドに、[Software Versions] と入力します。

ブート後にルータが以前のソフトウェアバージョンをロードする

テーブルに、インストールされているソフトウェアのバージョンが表示され、どのバージョンがアクティブであるかが示されます。

• CLI 手順：

1. **show sdwan software** コマンドを特権 EXEC モードで実行して、現在アクティブなソフトウェアバージョンと以前のバージョンを表示します。
2. デバイス上で、**show version** コマンドを特権 EXEC モードで実行します。

デバイスがインストールされている最新のソフトウェアバージョンを使用している場合、コマンド出力には `bootflash:packages.conf` と表示されます。

デバイスが以前のソフトウェアバージョンを使用している場合、コマンド出力には `bootflash:prev_packages.conf` と表示されます。

2. デバイスを再起動し、ロードされているシステムソフトウェアを再度確認します。
3. デバイスが以前のソフトウェアバージョン (`bootflash:prev_packages.conf`) で再度起動する場合は、Cisco TAC にお問い合わせください。



第 6 章

Cisco Catalyst SD-WAN オーバーレイネットワークの起動プロセス

- ネットワークオーバーレイの起動 (147 ページ)
- Cisco SD-WAN Manager ペルソナおよびストレージデバイス (148 ページ)
- 稼働イベントシーケンス (149 ページ)
- ソフトウェアのダウンロード (185 ページ)
- Cisco SD-WAN Manager の導入 (186 ページ)
- Cisco Catalyst SD-WAN Validator の導入 (197 ページ)
- vContainer ホスト (215 ページ)
- Cisco Catalyst SD-WAN コントローラ の導入 (215 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 (231 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 (232 ページ)
- Alibaba Cloud への Cisco Catalyst 8000V Edge ソフトウェア の展開 (232 ページ)
- vEdge クラウドルータ の展開 (234 ページ)

ネットワークオーバーレイの起動

表 22: 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN 制御コンポーネントをホストしている仮想マシンのオンプレミス ESXi でのディスク暗号化	Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.14.1	この機能を使用すると、Cisco UCS プラットフォームでホストされている VMWare ESXi ハイパーバイザを使用して、オンプレミスのインストールで Cisco SD-WAN 制御コンポーネントをホストする場合に、仮想ディスクにディスク暗号化を適用できます。

Cisco SD-WAN Manager ペルソナおよびストレージデバイス

Cisco SD-WAN Manager を展開すると、Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager ペルソナ

Cisco vManage リリース 20.6.1 以降、各 Cisco SD-WAN Manager 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 SD-WAN Manager クラスタ内でサーバーが持つ役割を定義します。Cisco SD-WAN Manager ペルソナの関連情報については、「Cisco SD-WAN Manager クラスタ」を参照してください。

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

Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager クラスタの一部である必要があります。

Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager ストレージデバイス

各 Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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も尋ねられます。

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 SD-WAN Manager 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 Catalyst 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 SD-WAN Validator と Cisco SD-WAN 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 SD-WAN Manager からダウンロードする必要があり、その後、これらの Cisco SD-WAN コントローラ と Cisco SD-WAN Validator が Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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。

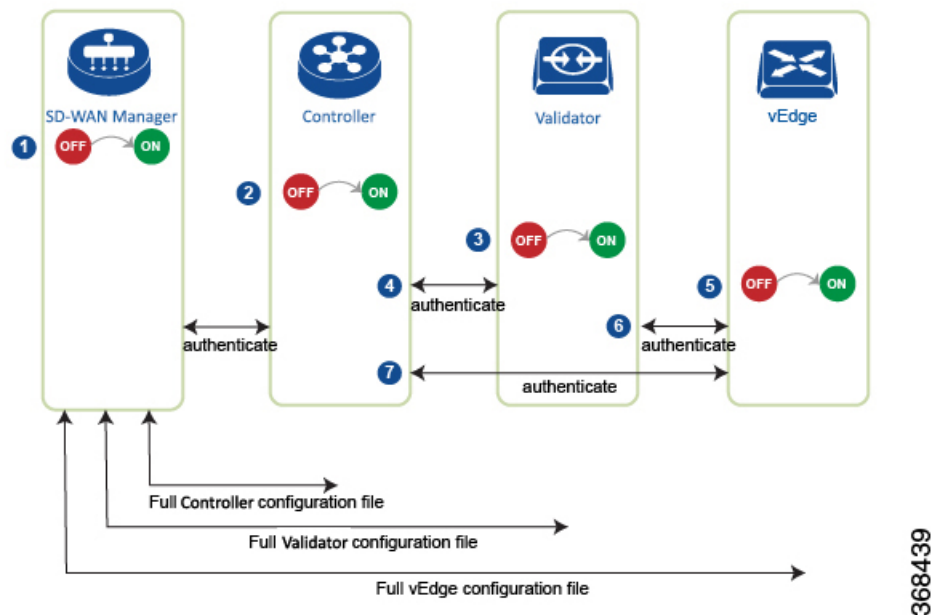
この2つの部分からなるプロセスの最終結果は、運用可能なオーバーレイネットワークです。

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 10: 稼働イベントシーケンス



1. Cisco SD-WAN Manager 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 SD-WAN Validator が、DMZ 内のサーバーで起動します。
3. Cisco SD-WAN 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 SD-WAN Manager と Cisco SD-WAN Validator が相互に認証し、Cisco SD-WAN Manager と Cisco SD-WAN コントローラ が相互に認証し、Cisco SD-WAN コントローラ と Cisco SD-WAN Validator が相互にセキュアに認証します。

5. Cisco SD-WAN Manager が、Cisco SD-WAN コントローラ と Cisco SD-WAN Validator 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 SD-WAN Validator で認証します。
8. ルータが、それ自体を Cisco SD-WAN Manager で認証します。
9. ルータが、それ自体を Cisco SD-WAN コントローラ で認証します。
10. Cisco SD-WAN Manager 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 Catalyst 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 SD-WAN 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 Catalyst 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 Catalyst 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 Catalyst 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。



- (注) Cisco vManage リリース 20.3.1 以降では、172.17.0.0/16 サブネットで Cisco SD-WAN Manager VPN0 IP アドレスを割り当てる場合、エッジデバイス（IOS XE SD-WAN および SD ルーティング）への制御接続を形成できません。

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 SD-WAN Manager 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 23:

起動タスク	ステップごとの手順
ステップ 1: Cisco SD-WAN Manager を起動します。	1. ハイパーバイザで、VM インスタンスを作成します。 2. Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Validator を起動 します。	1. ハイパーバイザで、VM インスタンスを作成します。 2. Cisco SD-WAN Validator サーバーを起動し、VM を起動します。 3. Cisco SD-WAN Manager メニューから、[Configuration] > [Devices] > [Controllers]の順に選択し、Cisco SD-WAN Validator を追加して CSR を生成します。 (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。 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 SD-WAN Manager 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 SD-WAN Manager メニューから、[Configuration] > [Templates]の順に選択します。 1. Cisco SD-WAN Validator の構成テンプレートを作成します。 2. テンプレートを Cisco SD-WAN Validator に添付します。 8. Cisco SD-WAN Manager メニューから、[Monitor] > [Overview]の順に選択し、Cisco SD-WAN Validator 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 SD-WAN Manager メニューから、[Dashboard] > [Main Dashboard]の順に選択し、Cisco SD-WAN Validator 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 Catalyst SD-WAN コントローラ を起動します。	1. ハイパーバイザで、VM インスタンスを作成します。 2. Cisco SD-WAN コントローラ サーバーを起動し、VM を起動します。 3. Cisco SD-WAN Manager メニューから、[Configuration] > [Devices] > [Controller]の順に選択し、Cisco Catalyst SD-WAN コントローラ を追加して CSR を生成します。 (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。 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 SD-WAN Manager 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 SD-WAN Manager メニューから、[Configuration] > [Templates]の順に選択します。 1. Cisco Catalyst SD-WAN 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 Catalyst SD-WAN コントローラ に添付します。 8. Cisco SD-WAN Manager メニューから、[Monitor] > [Overview]の順に選択し、Cisco Catalyst SD-WAN 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 SD-WAN Manager メニューから、[Dashboard] > [Main Dashboard]の順に選択し、Cisco Catalyst SD-WAN 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。	1. Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager メニューから、[Configuration] > [Templates]の順に選択します。 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。	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 SD-WAN Manager 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 SD-WAN Manager 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

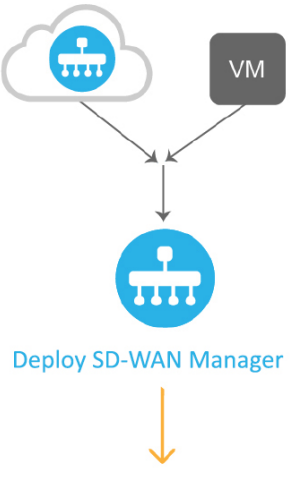
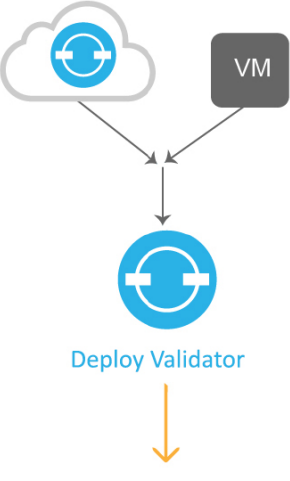
一般に、Cisco Catalyst SD-WAN オーバーレイネットワークを起動するために実行する作業は、ネットワークを起動するための作業です。ネットワークを計画し、デバイス構成を作成してから、ネットワークハードウェアおよびソフトウェアコンポーネントを展開します。展開するコンポーネントには、すべての Cisco vEdge デバイス、オーバーレイネットワークに参加するすべての従来のルータ、およびオーバーレイネットワーク全体で共有サービス（ファイアウォール、ロードバランサ、IDP システムなど）を提供するすべてのネットワークデバイスが含まれます。

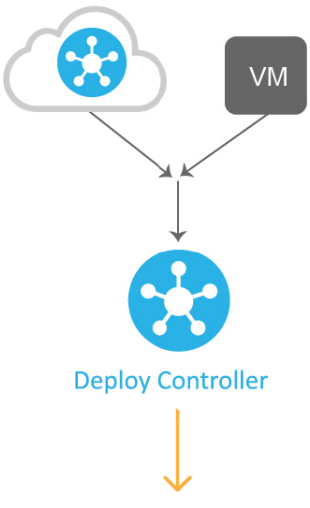
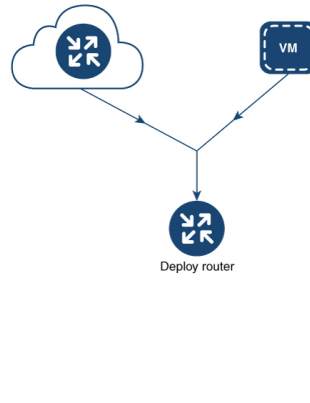
次の表に、Cisco Catalyst SD-WAN オーバーレイネットワークの稼働シーケンスのユーザー部分における手順の概要を示します。各手順の詳細については、「手順」列に示されている手順のリンク先を参照してください。Cisco vEdge デバイスは任意の順序で起動できますが、以下に記載されている順序で展開することを推奨します。これは、デバイスがデバイス自体を検証および認証する機能的な順序です。

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 Catalyst 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 24:

	ワークフロー	手順
1	 Plan Network  368182	オーバーレイネットワークを計画します。「Cisco Catalyst 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  368183	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。

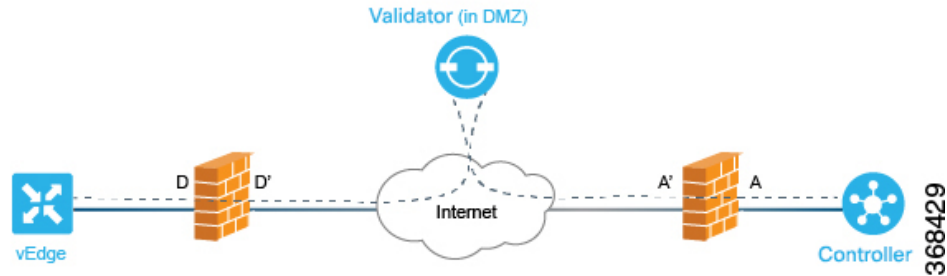
	ワークフロー	手順
3	 368184	ソフトウェアイメージをダウンロードします。
4	 368185	データセンターに Cisco SD-WAN Manager を展開します。 1. ESXi または KVM ハイパーバイザのいずれかで Cisco SD-WAN Manager VM インスタンスを作成します。 2. Cisco SD-WAN Manager サーバーごとに最小構成または完全な構成を作成します。 3. 証明書の設定を設定し、Cisco SD-WAN Manager の証明書を生成します。 4. Cisco SD-WAN Manager クラスタを作成します。
5	 368186	Cisco SD-WAN Validator を導入します。 1. ESXi または KVM ハイパーバイザのいずれかで Cisco SD-WAN Validator VM インスタンスを作成します。 2. Cisco SD-WAN Validator の最小構成を作成します。 3. Cisco SD-WAN Validator 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 SD-WAN Validator の証明書を生成します。 4. Cisco SD-WAN Validator の完全な構成を作成します。

ワークフロー	手順
6  368187	データセンターに Cisco SD-WAN コントローラ を展開します。 1. ESXi または KVM ハイパーバイザのいずれかで Cisco SD-WAN コントローラ VM インスタンスを作成します。 2. Cisco SD-WAN コントローラ の最小構成を作成します。 3. Cisco SD-WAN 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 SD-WAN コントローラ の証明書を作成します。 4. Cisco SD-WAN コントローラ の完全な構成を作成します。
7  368188	オーバーレイネットワークに Cisco vEdge ルータ を展開します。 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. 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 SD-WAN Manager 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 SD-WAN コントローラ および Cisco SD-WAN Validator 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 SD-WAN Validator によって導かれます。次の図を参照してください。Cisco SD-WAN Validator 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 SD-WAN Manager 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 SD-WAN Manager は例外です。各 Cisco SD-WAN Manager サーバー自体を手動で構成する必要があります）。

図 11: Cisco SD-WAN Validator の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 Catalyst 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 Catalyst 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 SD-WAN コントローラ と Cisco SD-WAN Validator 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 SD-WAN Validator および Cisco SD-WAN 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 コントローラ 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 SD-WAN コントローラ および Cisco SD-WAN Validator 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。

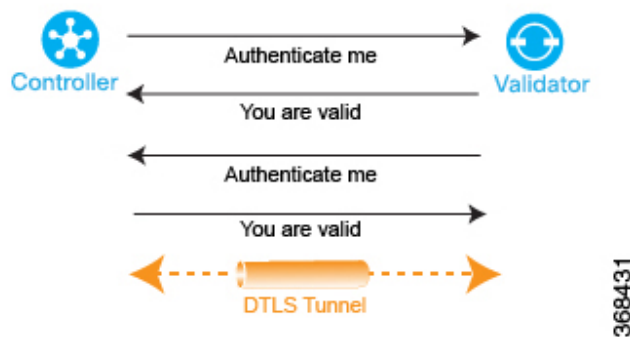
- **Cisco SD-WAN コントローラ 認定シリアル番号**：Cisco SD-WAN Manager は、CSR を作成して署名付き証明書をインストールするときに、ネットワーク内に存在することが許可されているすべての Cisco SD-WAN コントローラ のシリアル番号を学習します。これらのシリアル番号を Cisco SD-WAN Validator にダウンロードすると、Cisco SD-WAN Validator は、それらを自動認証プロセス中に Cisco Catalyst SD-WAN コントローラ にプッシュします。
- **vEdge 認定シリアル番号ファイル**：このファイルには、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 SD-WAN Validator および Cisco SD-WAN 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 SD-WAN Manager 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 Catalyst 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 Catalyst SD-WAN コントローラ と Cisco Catalyst SD-WAN Validator 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 Catalyst 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 SD-WAN コントローラ と Cisco SD-WAN Validator です。このプロセスは、Cisco SD-WAN コントローラ によって開始されます。

図 12: Cisco SD-WAN コントローラ と Cisco SD-WAN Validator の認証



Cisco SD-WAN コントローラ は、起動すると、Cisco SD-WAN Validator への接続を開始します。それにより、Cisco SD-WAN Validator が Cisco SD-WAN 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 SD-WAN コントローラ はそれ自体を、Cisco SD-WAN Validator はそれ自体を Cisco SD-WAN Validator 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 SD-WAN コントローラ デバイスと Cisco SD-WAN Validator 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 SD-WAN Validator の IP アドレスまたは DNS 名であるため、Cisco SD-WAN コントローラ は Cisco SD-WAN Validator に到達する方法を認識しています。次の理由から、Cisco SD-WAN Validator は、Cisco SD-WAN Validator 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 SD-WAN Validator 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。

- Cisco SD-WAN コントローラ 認定シリアル番号を Cisco SD-WAN Manager から Cisco SD-WAN Validator にダウンロードしています。

Cisco SD-WAN コントローラ が認証プロセスを開始するときに、Cisco SD-WAN Validator がまだ起動していない場合、Cisco SD-WAN 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。

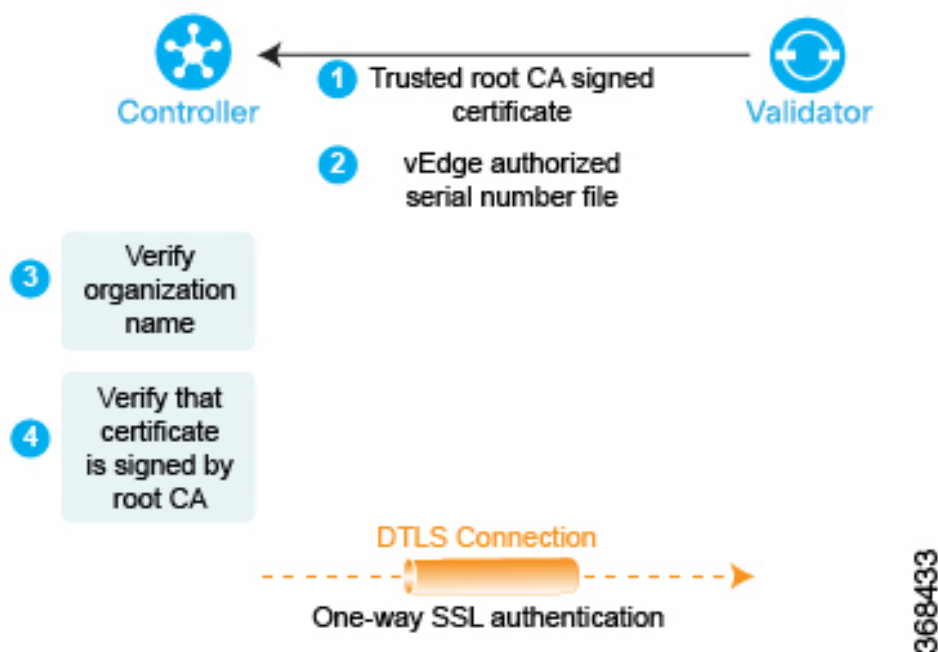
以下では、Cisco SD-WAN コントローラ と Cisco SD-WAN Validator の間で自動認証がどのように行われるかについて、詳しくステップバイステップで説明します。

Cisco SD-WAN コントローラ と Cisco SD-WAN Validator の間でセッションを開始するために、Cisco SD-WAN コントローラ が Cisco SD-WAN Validator 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ネルを介して、Cisco SD-WAN コントローラ と Cisco SD-WAN Validator 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 SD-WAN Validator の Cisco SD-WAN コントローラ 認証から説明します。

1. Cisco SD-WAN Validator は信頼できるルート CA 署名付き証明書を Cisco SD-WAN コントローラ に送信します。
2. Cisco SD-WAN Validator は vEdge 認定シリアル番号ファイルを Cisco SD-WAN コントローラ に送信します。
3. Cisco SD-WAN 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 SD-WAN 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 SD-WAN コントローラ は、Cisco SD-WAN Validator 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 Catalyst SD-WAN コントローラ は DTLS 接続を切断します。
4. Cisco Catalyst SD-WAN 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 Catalyst SD-WAN 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 Catalyst SD-WAN コントローラ は DTLS 接続を切断します。

図 13: Cisco SD-WAN コントローラ による Cisco SD-WAN Validator の認証

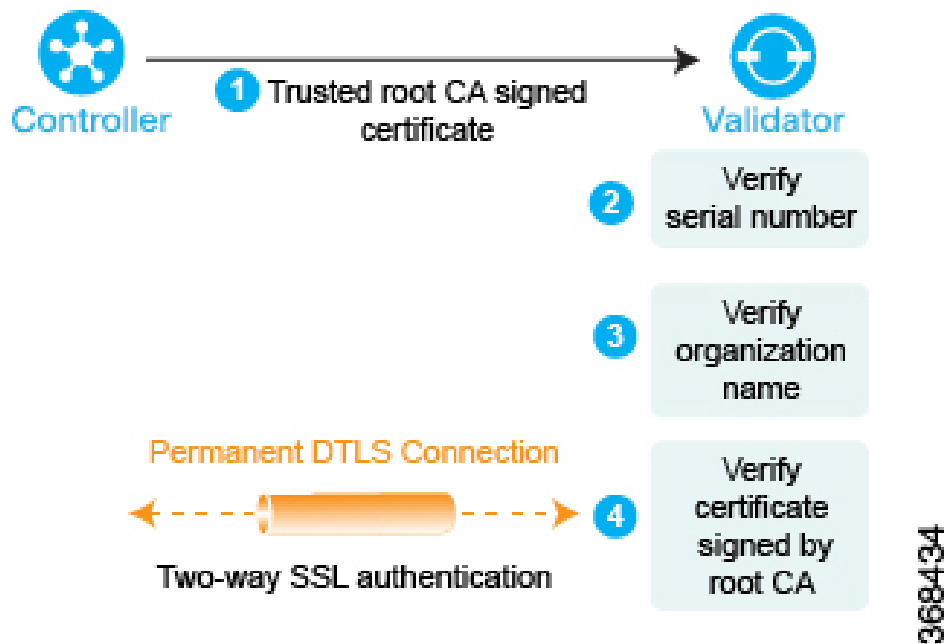


この2つのチェックを実行すると、Cisco SD-WAN Validator の Cisco SD-WAN コントローラ 認証が完了します。

反対方向では、Cisco SD-WAN Validator が Cisco SD-WAN コントローラ を認証します。

1. Cisco SD-WAN 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 SD-WAN Validator に送信します。
2. Cisco SD-WAN Validator は、信頼のチェーンを使用して証明書から Cisco SD-WAN 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、Cisco SD-WAN コントローラ 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 SD-WAN Validator は DTLS 接続を切断します。
3. Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator は、Cisco SD-WAN 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 SD-WAN Validator は DTLS 接続を切断します。
4. Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator は DTLS 接続を切断します。

図 14: Cisco SD-WAN Validator による Cisco SD-WAN コントローラ の認証



この3つのチェックを実行すると、Cisco SD-WAN Validator の Cisco SD-WAN Validator 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 SD-WAN Validator と Cisco SD-WAN 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 SD-WAN コントローラ があるドメインでは、このプロセスが Cisco SD-WAN コントローラ デバイスと Cisco SD-WAN Validator デバイスの各ペア間で繰り返されます。Cisco SD-WAN コントローラ は、Cisco SD-WAN Validator 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 Cisco SD-WAN 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 SD-WAN Validator には、ネットワークトポロジ内の Cisco SD-WAN 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 SD-WAN コントローラ が Cisco SD-WAN Validator に登録されると、Cisco SD-WAN Validator および Cisco SD-WAN コントローラ は Cisco Catalyst 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 Catalyst SD-WAN コントローラ 間の認証

複数の Cisco SD-WAN 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 SD-WAN コントローラ は Cisco SD-WAN Validator から相手の Cisco SD-WAN コントローラ の IP アドレスを学習します。

Cisco SD-WAN コントローラ は、Cisco SD-WAN Validator との認証ハンドシェイク中に、Cisco SD-WAN コントローラ 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 SD-WAN 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 SD-WAN 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 SD-WAN コントローラ が Cisco SD-WAN Validator で認証されると、Cisco SD-WAN Validator は Cisco SD-WAN コントローラ に認証されている他の Cisco SD-WAN コントローラの IP アドレスを送信します。Cisco SD-WAN Validator は後で別の Cisco SD-WAN 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 SD-WAN コントローラ に送信します。

次に、Cisco SD-WAN 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. Cisco SD-WAN コントローラ 1 (vSmart1) は、Cisco SD-WAN コントローラ 2 (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 Cisco SD-WAN コントローラ 2 に送信します。
2. Cisco SD-WAN コントローラ 2 は、その信頼チェーンを使用して Cisco SD-WAN コントローラ 1 のシリアル番号を抽出します。シリアル番号は、Cisco SD-WAN コントローラ 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、Cisco SD-WAN コントローラ 2 は DTLS 接続を切断します。
3. Cisco SD-WAN コントローラ 2 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、Cisco SD-WAN コントローラ 2 は、Cisco SD-WAN コントローラ 1 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 SD-WAN コントローラ 2 は DTLS 接続を切断します。
4. Cisco SD-WAN コントローラ 2 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 SD-WAN コントローラ 2 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 SD-WAN コントローラ 2 は DTLS 接続を切断します。

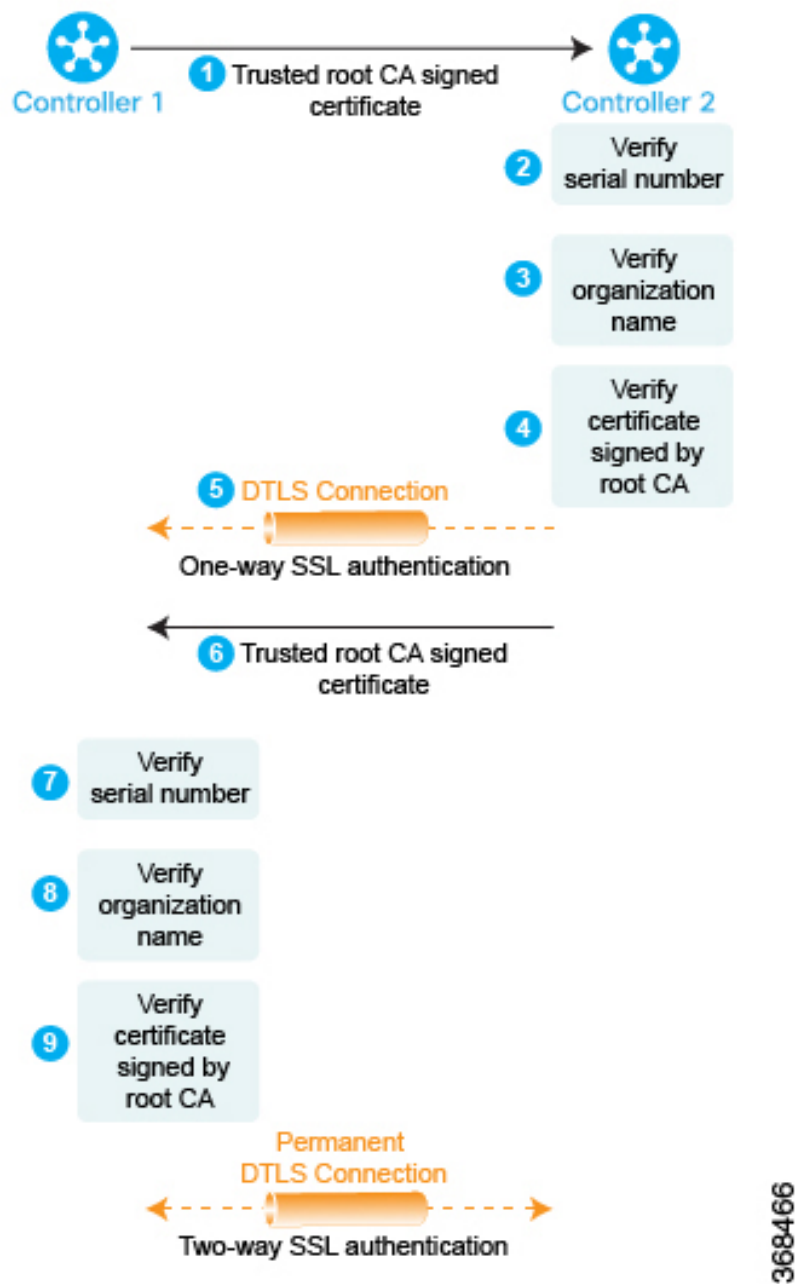
この 3 つのチェックを実行すると、Cisco SD-WAN コントローラ 1 の Cisco SD-WAN コントローラ 2 認証が完了します。

これで、Cisco SD-WAN コントローラ 1 は Cisco SD-WAN コントローラ 2 を認証するので、前述の同じ手順を実行します。

1. まず、Cisco SD-WAN コントローラ 2 は、その信頼できるルート CA 署名付き証明書を Cisco SD-WAN コントローラ 1 に送信します。
2. Cisco SD-WAN コントローラ 1 は、その信頼チェーンを使用して Cisco SD-WAN コントローラ 2 のシリアル番号を抽出します。シリアル番号は、Cisco SD-WAN コントローラ 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、Cisco SD-WAN コントローラ 1 は DTLS 接続を切断します。

3. Cisco SD-WAN コントローラ 1 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、Cisco SD-WAN コントローラ 2 は、Cisco SD-WAN コントローラ 2 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 SD-WAN コントローラ 1 は DTLS 接続を切断します。
4. Cisco SD-WAN コントローラ 1 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 SD-WAN コントローラ 2 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 SD-WAN コントローラ 1 は DTLS 接続を切断します。

図 15: Cisco SD-WAN コントローラ の認証



この3つのチェックを実行すると、Cisco SD-WAN コントローラ 2 の Cisco SD-WAN コントローラ 1 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 SD-WAN コントローラ が登録されると、Cisco SD-WAN Validator および Cisco SD-WAN コントローラ は Cisco Catalyst 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。

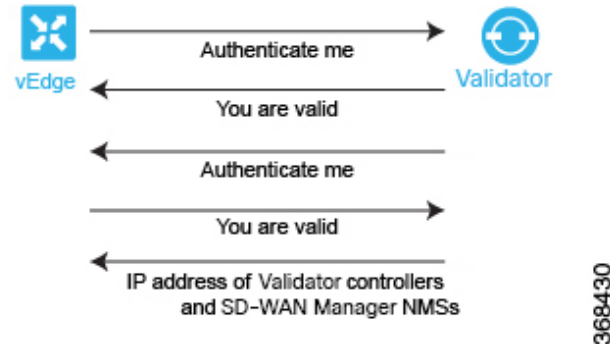
Cisco Catalyst SD-WAN Validator と Cisco vEdge ルータの間の認証

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 つのを行う必要があります。

- Cisco SD-WAN Manager 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 Catalyst SD-WAN コントローラ とのセキュアな接続を確立して、Cisco Catalyst 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 SD-WAN Manager と Cisco Catalyst SD-WAN コントローラ を自動検出し、接続を確立します。その際、Cisco SD-WAN Validator の助けを借ります。Cisco vEdge ルータの初期構成には、Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator は、Cisco vEdge ルータに Cisco SD-WAN Manager と Cisco Catalyst SD-WAN 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 SD-WAN Validator 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 16: Cisco vEdge ルータと Cisco SD-WAN Validator 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 SD-WAN Validator の検索が自動的に開始されます。Cisco SD-WAN Validator と Cisco SD-WAN 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 SD-WAN Validator 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 SD-WAN Validator に到達します。次の理由により、Cisco SD-WAN Validator 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 Cisco SD-WAN Validator 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ことであると認識しています。

- 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 SD-WAN Validator 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 SD-WAN Validator 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。

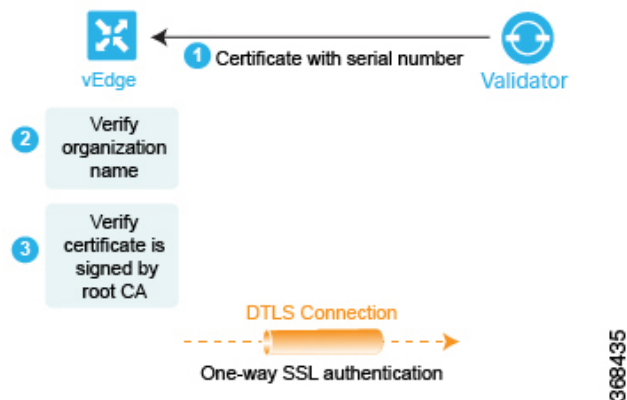
以下では、Cisco SD-WAN Validator と Cisco vEdge ルータの間で自動認証がどのように行われるかについて、詳しくステップバイステップで説明します。

まず、Cisco vEdge ルータは、Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator の相互認証は並行して処理されます。Cisco vEdge ルータが Cisco SD-WAN Validator をどのように認証するかの説明から議論を開始します。

1. Cisco SD-WAN Validator 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 SD-WAN Validator 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 17: Cisco vEdge ルータによる Cisco SD-WAN Validator の認証

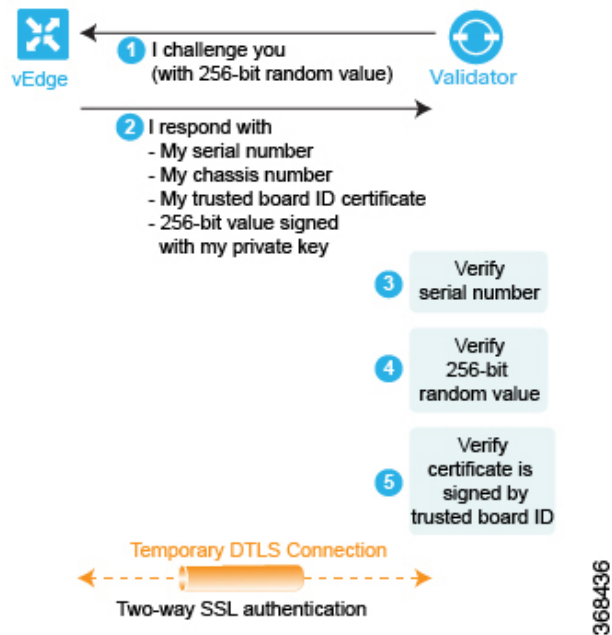


これらの 2 つのチェックを実行した後、Cisco vEdge ルータは Cisco SD-WAN Validator が有効であることを認識し、Cisco SD-WAN Validator の認証が完了します。

反対方向では、Cisco SD-WAN Validator が Cisco vEdge ルータを認証します。

1. Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator は DTLS 接続を切断します。
4. Cisco SD-WAN Validator 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 SD-WAN Validator は DTLS 接続を切断します。
5. Cisco SD-WAN Validator 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 SD-WAN Validator は DTLS 接続を切断します。

図 18 : Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator 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 Catalyst SD-WAN コントローラ に同時に送信します。Cisco vEdge ルータに Cisco SD-WAN Validator 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 SD-WAN 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 SD-WAN Validator は、Cisco vEdge ルータが Cisco Catalyst SD-WAN 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 SD-WAN コントローラ のシリアル番号。

Cisco Catalyst SD-WAN コントローラ に Cisco SD-WAN Validator 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 SD-WAN Validator は、Cisco Catalyst SD-WAN 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 SD-WAN Validator との DTLS 接続を切断します。

Cisco vEdge ルータと Cisco SD-WAN Manager 間の認証

Cisco vEdge ルータと Cisco SD-WAN Validator の相互認証の後、Cisco vEdge ルータは、Cisco SD-WAN Manager 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 SD-WAN Manager との DTLS 接続を確立します。
2. Cisco SD-WAN Manager 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 SD-WAN 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 SD-WAN Manager 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。

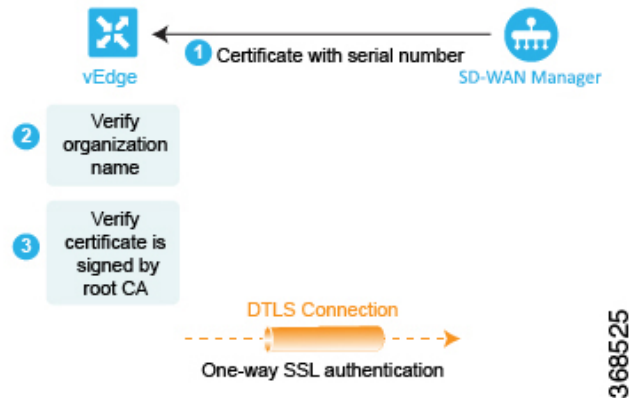
以下では、Cisco vEdge ルータと Cisco SD-WAN Manager の間で自動認証がどのように行われるかについて、詳しくステップバイステップで説明します。

まず、Cisco vEdge ルータは、Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager の相互認証は並行して処理されます。Cisco vEdge ルータが Cisco SD-WAN Manager をどのように認証するかの説明から議論を開始します。

1. Cisco SD-WAN Manager 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 SD-WAN Manager 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 19: Cisco vEdge ルータによる Cisco SD-WAN Manager の認証

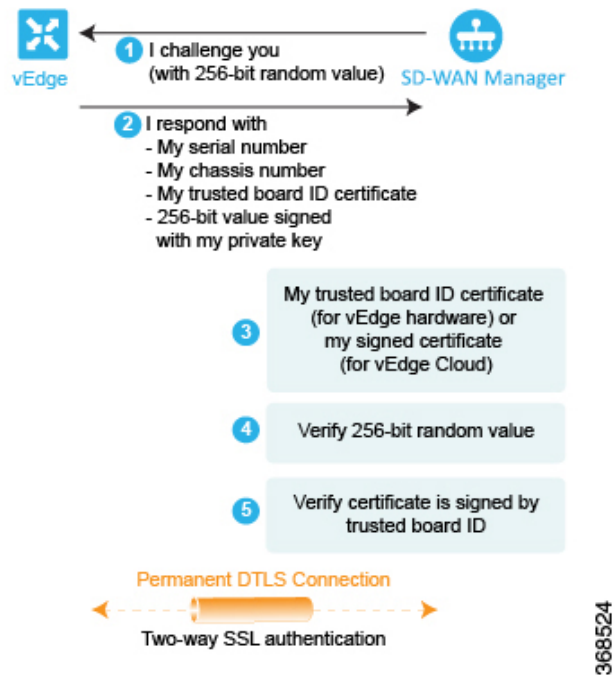


これらの2つのチェックを実行した後、Cisco vEdge ルータは Cisco SD-WAN Manager が有効であることを認識し、Cisco SD-WAN Manager の認証が完了します。

反対方向では、Cisco SD-WAN Manager が Cisco vEdge ルータを認証します。

1. Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager Cisco SD-WAN Manager NMS は DTLS 接続を切断します。
4. Cisco SD-WAN Manager 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 SD-WAN Manager は DTLS 接続を切断します。
5. Cisco SD-WAN Manager 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 SD-WAN Manager は DTLS 接続を切断します。

図 20 : Cisco SD-WAN Manager による Cisco vEdge ルータの認証



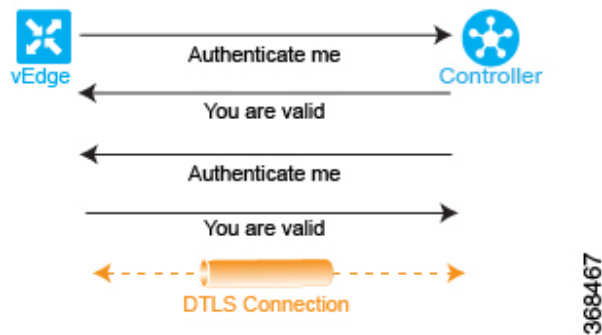
これらの3つのチェックを実行した後、Cisco SD-WAN Manager は Cisco vEdge ルータが有効であることを認識し、ルータの認証が完了します。

双方向認証が成功すると、Cisco SD-WAN Manager 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 SD-WAN 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 Catalyst SD-WAN 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 SD-WAN 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 SD-WAN 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 SD-WAN 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 SD-WAN 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 Catalyst 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 21 : Cisco SD-WAN コントローラ と Cisco vEdge ルータの認証



ここでは、Cisco SD-WAN コントローラ 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。

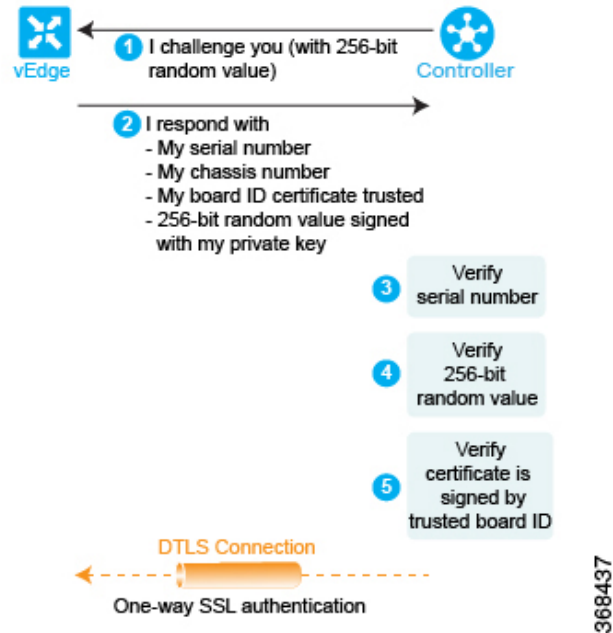
Cisco SD-WAN コントローラ と Cisco vEdge ルータの間にセッションを開始するために、2つのデバイスの一方が他方への暗号化された DTLS 接続を開始します。暗号化は RSA によって提供されます。各デバイスは、起動時に RSA の秘密キーと公開キーのペアを自動生成します。

Cisco SD-WAN 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 SD-WAN 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 SD-WAN 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 SD-WAN 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 SD-WAN コントローラ は DTLS 接続を切断します。
4. Cisco SD-WAN 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 SD-WAN コントローラ は DTLS 接続を切断します。
5. Cisco SD-WAN 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 SD-WAN コントローラ は DTLS 接続を切断します。

6. Cisco SD-WAN コントローラ は、応答を元のチャレンジと比較します。Cisco SD-WAN Validator 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 SD-WAN コントローラ が DTLS 接続を切断します。

図 22: Cisco SD-WAN コントローラによる Cisco vEdge ルータの認証

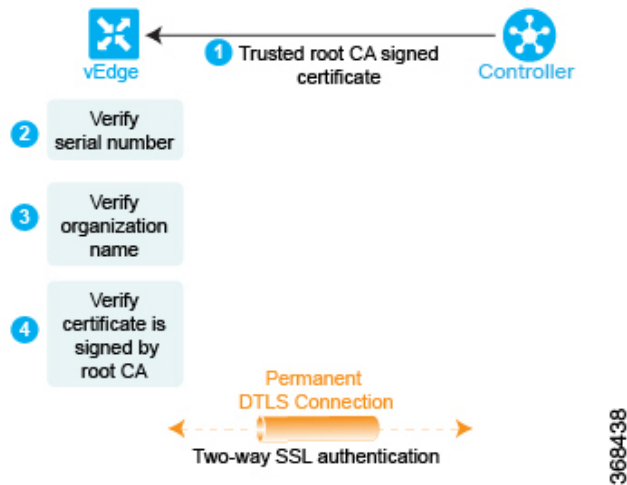


これらの3つのチェックを実行した後、Cisco SD-WAN コントローラ は Cisco vEdge ルータが有効であることを認識し、ルータの認証が完了します。

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

1. Cisco SD-WAN 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 SD-WAN 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、Cisco SD-WAN コントローラ 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 SD-WAN 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 23 : Cisco vEdge ルータによる Cisco SD-WAN コントローラの認証



この3つのチェックを実行すると、Cisco SD-WAN 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 SD-WAN 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 SD-WAN 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 SD-WAN 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 SD-WAN 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 SD-WAN 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 SD-WAN コントローラ にリレーして、Cisco SD-WAN 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 SD-WAN コントローラ の間で DTLS 接続が確立されると、OMP は TLOC を Cisco SD-WAN 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 SD-WAN 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 Catalyst 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 SD-WAN 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 SD-WAN 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 Catalyst SD-WAN 展開のためのファイアウォールポート

この記事では、Cisco Catalyst 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 Catalyst 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 Catalyst 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。



- (注) NAT ゲートウェイがアンダーレイに存在し、元のポートを保持せずに送信元ポート変換を実行する場合、特定の条件下でランダムな送信元ポートを割り当てる場合があります。これは、複数のデバイスが同じ送信元ポートを使用している同じ NAT 後の IP アドレスの背後にある場合、またはポートがすでに既存のセッションによって占有されている場合に発生する可能性があります。結果として、割り当てられた送信元ポートが、指定された UDP ポートの範囲 (12346+n、12366+n、12386+n、12406+n、および 12426+n、n の範囲は 0～19 で、設定されたオフセットを表す) とは異なる場合があります。リモートルータ側でインバウンドファイアウォールルールを設定する場合は、このことを考慮することが重要です。

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 Catalyst 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 SD-WAN Manager、Cisco SD-WAN Validator、および Cisco SD-WAN 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できます。

Cisco SD-WAN コントローラ および Cisco SD-WAN Manager 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 SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator に接続するか、2 つの Cisco SD-WAN Validator 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>
```

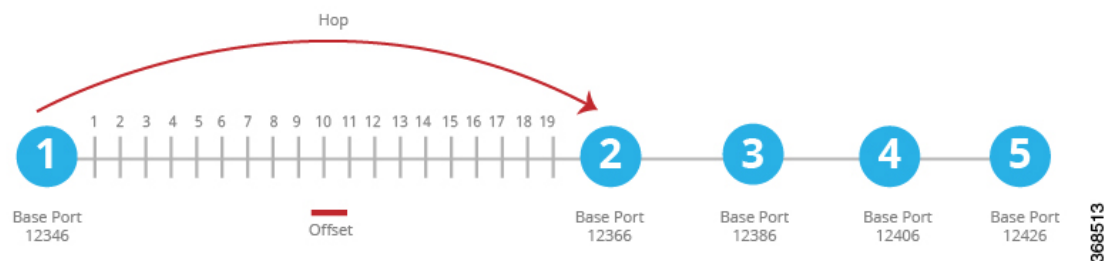


- (注) ポートホッピングを設定しないように選択した場合は、次のコマンドを使用します。

```
system
no port-hop
```

システム IP の変更、TLOC の追加中の TLOC の色の変更などの外部トリガーは、ポートホップが設定されていなくても、ポートホップをトリガーできます。

図 24: 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 SD-WAN Validator、Cisco SD-WAN Manager、または Cisco SD-WAN 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 SD-WAN Validator がクラッシュすると、Cisco SD-WAN Manager 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 SD-WAN Validator がクラッシュすると、Cisco SD-WAN Manager 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 SD-WAN Manager が、ポートホッピングを実行して、別のポートでの Cisco SD-WAN コントローラへの接続確立を試みます。Cisco SD-WAN Manager 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その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 SD-WAN 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 SD-WAN 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 SD-WAN 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 SD-WAN 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 SD-WAN コントローラの **graceful-restart timers** は、冗長 Cisco SD-WAN コントローラピアリングで変更するか（一度に 1 つの Cisco SD-WAN 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 SD-WAN Validator、Cisco SD-WAN Manager、および Cisco Catalyst SD-WAN 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 SD-WAN Validator から Cisco Catalyst SD-WAN コントローラの場所を学習し、その構成を Cisco SD-WAN Manager から受信して、そのポリシーとポリシーの更新を Cisco Catalyst SD-WAN 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 Catalyst 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 SD-WAN コントローラ および Cisco SD-WAN Manager では必要ありません。

Cisco Catalyst 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、「[Firewall Port Considerations](#)」を参照してください

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 Catalyst SD-WAN デバイスで使用するポート

Cisco SD-WAN 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 SD-WAN Manager 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 SD-WAN Validator は複数のコアをサポートしていません。Cisco SD-WAN Validator 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 SD-WAN Manager 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 SD-WAN Manager によって使用される管理ポート

Cisco SD-WAN Manager 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
HTTPS	着信	TCP	443
SNMP クエリー	着信	UDP	161
SSH	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、 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 SD-WAN Manager 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
TACACS	発信	TCP	49

Cisco SD-WAN Manager 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。

Cisco SD-WAN Manager サービス	トラフィックの方向	プロトコル	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	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

Cisco SD-WAN Manager サービス	トラフィックの方向	プロトコル	ポート番号
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

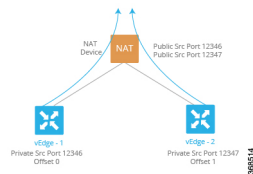
2 つ以上の Cisco vEdge デバイス が同じフルコーン NAT デバイスの背後にある場合、1 つのデバイスはデフォルトのポートオフセットを使用できますが、残りのデバイスではポートオフセットを設定する必要があります。

```
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 25: 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 Catalyst 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 Catalyst 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 Catalyst 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。



(注) Cisco vManage リリース 20.9.1 以降、vEdge クラウドルータ はサポートされていません。

コンポーネント	注
Cisco SD-WAN Validator	Cisco SD-WAN Validator が Cisco vEdge 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 クラウドルータ として表示されます。
Cisco SD-WAN Manager	ダウンロードページに Cisco SD-WAN コントローラ ソフトウェアとして表示されます
Cisco Catalyst SD-WAN コントローラ	ダウンロードページに Cisco SD-WAN コントローラ ソフトウェアとして表示されます

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.14.1 以降のファイル名

Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降、ソフトウェアイメージの名前が viptela-edge から viptela-bond に変更され、Cisco SD-WAN コントローラ (vSmart) および Cisco SD-WAN Validator (vBond) に統合ソフトウェアイメージが使用されます。両方のコントローラの初期デフォルトホスト名は vsmart です。ホスト名を更新することをお勧めします。

ソフトウェアイメージ	Cisco Catalyst SD-WAN Manager リリース 20.14.1 以前	Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降
.qcow2 (名前の変更)	viptela-edge-genericx86-64.qcow2 viptela-image-generic86-64.qcow2	viptela-bond-genericx86-64.qcow2
.vhd (名前の変更)	viptela-edge-genericx86-64_vhd.tar.gz viptela-image-generic86-64_vhd.tar.gz	viptela-bond-genericx86-64_vhd.tar.gz
.ova (名前の変更)	viptela-edge-genericx86-64.ova viptela-image-generic86-64.ova	viptela-bond-genericx86-64.ova
.tar.gz (変更なし)	viptela-20.14.1-x86_64.tar.gz	viptela-20.14.1-x86_64.tar.gz

Cisco SD-WAN Manager の導入

Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager で管理することも、少なくとも 3 つの Cisco SD-WAN Manager 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、Cisco SD-WAN Manager クラスターで構築することをお勧めします。Cisco SD-WAN Manager 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。



(注) ゼロ以外のプレフィックスを持つデフォルトルートは、vEdge ルータではサポートされていません。

Cisco SD-WAN Manager 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 Cisco SD-WAN Manager VM インスタンスを作成します。
2. Cisco SD-WAN Manager 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。ESXi コンソールを使用して Cisco SD-WAN Manager 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 SD-WAN Manager を手動で設定することもできます。
3. 証明書の設定を設定し、Cisco SD-WAN Manager の証明書を生成します。
4. Cisco SD-WAN Manager クラスターを作成します。

Cisco SD-WAN Manager Web サーバー暗号

リリース 16.3.0 以降、Cisco SD-WAN Manager 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、Cisco SD-WAN Manager 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 Cisco Catalyst SD-WAN Manager VM インスタンスの作成

はじめる前に

Cisco SD-WAN Manager 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。

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.14.1から、ハイパーバイザでディスク暗号化を有効にできます。

Cisco Catalyst SD-WAN Manager VM インスタンスの作成

1. vSphere Client を起動し、Cisco SD-WAN Manager VM インスタンスを作成します。
2. Cisco SD-WAN Manager 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 SD-WAN Manager VM インスタンスの起動と Cisco SD-WAN Manager コンソールへの接続
5. Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 Cisco Catalyst SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager – 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 SD-WAN Manager – 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 SD-WAN Manager 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 Catalyst SD-WAN Manager コンソール への Cisco Catalyst SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 仮想マシンの電源が入ります。
2. [Console] タブを選択して、Cisco SD-WAN Manager コンソールに接続します。Cisco SD-WAN Manager コンソールが表示されます。Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager インスタンスに接続するために、Cisco SD-WAN Manager インスタンスの IP アドレスを設定します。
 1. Cisco SD-WAN Manager 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 SD-WAN Manager 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。



(注) Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco SD-WAN Manager を使用して制御管理デバイスを再起動する前に設定をコミットできます。

KVM での Cisco Catalyst SD-WAN Manager VM インスタンスの作成

Cisco SD-WAN Manager 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 Catalyst SD-WAN Manager VM インスタンスの作成

KVM ハイパーバイザで Cisco SD-WAN Manager 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 SD-WAN Manager 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 Catalyst SD-WAN は VMXNET3 vNIC のみをサポートします。

8. [Cisco SD-WAN Manager Virtual Machine] ウィンドウで、[Add Hardware] をクリックして、Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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] (Cisco SD-WAN Manager 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 SD-WAN Manager インスタンスが表示されます。
18. Cisco SD-WAN Manager クラスタを作成するには、手順 1 ～ 17 を繰り返して、Cisco SD-WAN Manager インスタンスごとに VM を作成します。

Cisco Catalyst SD-WAN Manager インスタンスへの接続

Web ブラウザを使用して Cisco SD-WAN Manager インスタンスに接続するために、Cisco SD-WAN Manager 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. Cisco SD-WAN Manager 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 Catalyst SD-WAN Manager の設定

デバイステンプレートを使用して Cisco SD-WAN Manager を設定できます。しかし、デバイステンプレートを使用する代わりに、CLI モードを使用して Cisco SD-WAN Manager を設定することを推奨します。

Cisco SD-WAN Manager 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、CLI モードまたは ESXi コンソールを使用し、Cisco SD-WAN Manager サーバー自体から直接各 Cisco SD-WAN Manager インスタンスを設定して、Cisco SD-WAN Manager 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 SD-WAN Validator の IP アドレス、デバイスのシステム IP アドレス、および VPN0 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 SD-WAN Validator、Cisco SD-WAN Manager、および Cisco SD-WAN 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 SD-WAN Manager 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。

- VPN0 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。VPN0 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 Catalyst 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) Cisco SD-WAN Manager クラスタの場合は、クラスタ内の各 Cisco SD-WAN Manager インスタンスを、その Cisco SD-WAN Manager サーバー自体から、CLI モードまたは ESXi コンソールを使用して、個別に設定する必要があります。

Cisco Catalyst SD-WAN Manager の設定

Cisco SD-WAN Manager 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 SD-WAN Validator のアドレスを設定します。
 1. Cisco SD-WAN Manager メニューから、**[Administration] > [Settings]** の順に選択します。
 2. **[Validator]** をクリックします。(Cisco Catalyst SD-WAN Manager リリース 20.12.1 以前を使用している場合は、**[Edit]** をクリックします)。
 3. **[Validator DNS/IP Address: Port]** フィールドに、Cisco SD-WAN Validator を指す DNS 名または Cisco SD-WAN Validator 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. CLI を使用した Cisco SD-WAN Manager の設定

CLI モードを使用して Cisco SD-WAN Manager を設定します。CLI にアクセスするには、別の SSH クライアントを使用して ESXi コンソールを使用するか、Cisco SD-WAN Manager グラフィカル ユーザー インターフェイス (GUI) を使用して SSH セッションを確立します。

デバイスへの SSH セッションを確立するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューで、[Tools] > [SSH Terminal] を選択します。
2. 左側のペインで、デバイスをクリックして選択します。
3. 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。
4. コンフィギュレーション モードに入ります。

```
Device# config
```

```
Device(config)#
```

CLI コマンドを発行して、Cisco SD-WAN Manager を設定できるようになりました。

Cisco SD-WAN Manager の動作には、次の機能が必須です。これらの機能は CLI モードで設定します。

- 認証、許可、アカウントिंग (AAA)
- セキュリティ
- システム全体のパラメータ
- トランスポート VPN (VPN 0)
- 管理 VPN (アウトオブバンド管理トラフィック用)

CLI 構成例

このセクションでは、CLI を使用して Cisco SD-WAN Manager を設定するためのサンプル CLI 設定について説明します。

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
!
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 SD-WAN Manager インスタンス、Cisco SD-WAN Validator、および Cisco SD-WAN 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 SD-WAN Manager 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、「[Certificates](#)」を参照してください。

Cisco Catalyst SD-WAN Manager 証明書の生成

Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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。

Cisco Catalyst SD-WAN Manager クラスタの作成

Cisco SD-WAN Manager クラスタは、Cisco Catalyst 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 SD-WAN Manager 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 Cisco SD-WAN Manager 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 SD-WAN Manager インスタンスを管理者が設定します。

Cisco SD-WAN Manager クラスタの作成の詳細については、「[Cluster Management](#)」を参照してください。

Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager メニューから、**[Administration] > [Settings]**を選択します。
2. **[User Sessions]** をクリックします。**[Client Session Timeout]** オプションで、**[Session Timeout]** を有効にします。（Cisco Catalyst SD-WAN Manager リリース 20.12.1 以前を使用している場合は、**[Edit]** をクリックします。）
3. 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 SD-WAN Manager クラスタ内のすべての Cisco SD-WAN Manager サーバーに適用されます。

Cisco Catalyst SD-WAN Validator の導入

Cisco SD-WAN Validator は、オーバーレイネットワーク内の Cisco SD-WAN 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 SD-WAN Validator 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 SD-WAN 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 SD-WAN Validator はネットワークサーバー上で VM として実行されます。

Cisco Catalyst SD-WAN オーバーレイネットワークには、1つ以上の Cisco SD-WAN Validator を含めることができます。

Cisco SD-WAN Validator 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 Cisco SD-WAN Validator VM インスタンスを作成します。
2. Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator をオーバーレイネットワークに追加して、Cisco SD-WAN Manager が認識できるようにします。

4. Cisco Catalyst SD-WAN ゼロタッチプロビジョニング (ZTP) Cisco SD-WAN Validator 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 SD-WAN Validator を 1 つ設定します。
5. Cisco SD-WAN Validator 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 SD-WAN Validator への CLI セッションを開きます。次に、Cisco SD-WAN Manager で構成テンプレートを作成し、テンプレートを Cisco SD-WAN Validator 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 SD-WAN Validator 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 Cisco Catalyst SD-WAN Validator VM インスタンスの作成

はじめる前に

Cisco SD-WAN Validator 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。

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.14.1 から、ハイパーバイザでディスク暗号化を有効にできます。

Cisco Catalyst SD-WAN Validator VM インスタンスの作成

1. vSphere Client を起動し、Cisco SD-WAN Validator 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. Cisco SD-WAN Validator 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 Cisco SD-WAN Validator 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 クライアントの起動および Cisco Catalyst SD-WAN Validator 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、Cisco SD-WAN Validator 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、Cisco SD-WAN Validator 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 Cisco SD-WAN Validator 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。

Cisco Catalyst SD-WAN Validator 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 Cisco SD-WAN Validator 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。Cisco SD-WAN Validator 仮想マシンの電源が入ります。
2. [Console] を選択して、Cisco SD-WAN Validator 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 Catalyst SD-WAN Validator の設定」を参照してください。

KVM での Cisco Catalyst SD-WAN Validator VM インスタンスの作成

Cisco SD-WAN Validator 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 Cisco SD-WAN Validator 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、Cisco SD-WAN Validator 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 Cisco SD-WAN Validator ソフトウェアイメージを検索します。
 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. [Cisco SD-WAN Validator 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、Cisco SD-WAN Validator 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 Catalyst SD-WAN Validator の設定」を参照してください。

Cisco Catalyst SD-WAN Validator の設定

オーバーレイネットワークで Cisco SD-WAN Validator の仮想マシン (VM) をセットアップして起動すると、Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator への CLI セッションを開きます。

初期構成を作成したら、Cisco SD-WAN Manager で構成テンプレートを作成し、そのテンプレートを Cisco SD-WAN Validator 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 SD-WAN Validator 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 Catalyst SD-WAN Validator の初期構成の作成

CLI セッションを使用して Cisco SD-WAN Validator 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。

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.14.x 以降のリリースの場合：

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

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.14.x より前のリリースの場合：

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

4. ホスト名を設定します。

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.14.x 以降のリリースの場合：

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

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.14.x より前のリリースの場合：

```
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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Validator の IP アドレスを設定します。Cisco SD-WAN Validator 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 SD-WAN Validator 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。Cisco SD-WAN Manager 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 SD-WAN Validator であることを指定します。Cisco SD-WAN Validator 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 SD-WAN Manager 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)#tunnel-interface
vBond(config-tunnel-interface)# encapsulation ipsec
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 SD-WAN Validator 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 Cisco SD-WAN Validator 構成テンプレートを Cisco SD-WAN Manager で作成します。次の Cisco SD-WAN Manager 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 Cisco SD-WAN Validator 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 SD-WAN Manager メニューから、**[Administration] > [Settings]** の順に選択し、組織名を設定します。
- Cisco SD-WAN Manager 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 SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator 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 Catalyst SD-WAN Validator の構成テンプレートの作成

ここでは、Cisco SD-WAN Manager によって管理されている Cisco SD-WAN Validator の設定方法について説明します。これらのデバイスは、Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Validator を設定する前に、Cisco SD-WAN Validator 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 SD-WAN Manager 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 SD-WAN コントローラ、および Cisco SD-WAN Validator) 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 Catalyst SD-WAN Validator の機能テンプレート

次の機能は Cisco SD-WAN Validator 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 SD-WAN Validator の完全な構成の構成要素です。Cisco SD-WAN Validator で有効にできる機能ごとに、Cisco SD-WAN Manager 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 SD-WAN Validator 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。

Cisco SD-WAN Validator 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 SD-WAN Manager のメニューから、**[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 [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す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 SD-WAN Validator には関係ありません。[Advanced Options] 領域にある [Cisco SD-WAN Validator Only] と [Local Cisco SD-WAN Validator] 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 SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator 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 つのイーサネット インターフェイス テンプレートを作成します。Cisco SD-WAN Validator 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 SD-WAN Manager 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 SD-WAN Validator を設定するときに使用できます。

機能テンプレートから Cisco SD-WAN Validator 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 SD-WAN Manager のメニューから、**[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 SD-WAN Validator 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 SD-WAN Validator では BFD または OMP テンプレートを選択しないでください。
 2. 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。
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 SD-WAN Manager 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 SD-WAN Manager のメニューから、**[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、[CLI Template] を選択します。
4. テンプレート名と説明を入力します。
5. [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。
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。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 Catalyst SD-WAN Validator へのデバイステンプレートのアタッチ

Cisco SD-WAN Validator 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 SD-WAN Validator に同時にアタッチできます。

Cisco SD-WAN Validator 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。

1. Cisco SD-WAN Manager のメニューから、[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 SD-WAN Validator 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 Catalyst SD-WAN Validator の追加

Cisco SD-WAN Validator の最小限の構成を作成したら、Cisco SD-WAN Manager に Cisco SD-WAN Validator 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 SD-WAN Validator 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 Catalyst SD-WAN Validator の追加と証明書の生成

Cisco SD-WAN Validator 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 SD-WAN Manager メニューから、**[Configuration] > [Devices]**の順に選択します。
2. **[Control Components]** をクリックし、**[Add Validator]** をクリックします。
3. **[Add Validator]** ウィンドウで、次の手順を実行します。
 1. VPN 0 の 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 SD-WAN Validator 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 SD-WAN Manager は CSR を生成し、生成した証明書を取得して、Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Manager 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 Catalyst SD-WAN ゼロタッチプロビジョニング (ZTP) 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 SD-WAN Validator を 1 つ設定する必要があります。この Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator と考えることができます。

Cisco Catalyst 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 SD-WAN Validator を設定する必要はありません。

このセクションでは、Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator 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上の Cisco SD-WAN Validator 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 SD-WAN Validator 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（^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 SD-WAN Validator の IP アドレス
 - Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator の IP アドレス
 - Cisco SD-WAN Validator 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 SD-WAN Manager、Cisco SD-WAN コントローラ、および Cisco SD-WAN Validator 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: O = 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 SD-WAN Validator 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 SD-WAN Validator 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 Cisco SD-WAN コントローラおよび Cisco vEdge デバイス が Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator 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 Catalyst 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 Catalyst SD-WAN のクロックを確認します。

14. ルータシャーン情報を含む 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 SD-WAN Validator 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 SD-WAN Validator 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

「Deploy the Cisco Catalyst SD-WAN コントローラ」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 Catalyst SD-WAN コントローラの導入

Cisco SD-WAN コントローラ は、Cisco Catalyst 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 SD-WAN 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す。Cisco SD-WAN 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 Catalyst SD-WAN オーバーレイネットワークには、1 つ以上の Cisco SD-WAN コントローラ を含めることができます。Cisco SD-WAN 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 SD-WAN コントローラ を含めることをお勧めします。単一の Cisco SD-WAN 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 SD-WAN Manager または Cisco SD-WAN Manager クラスタは、オーバーレイネットワーク内の最大 20 の Cisco SD-WAN コントローラ をサポートできます。

Cisco SD-WAN 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 Cisco SD-WAN コントローラ VM インスタンスを作成します。
2. Cisco SD-WAN 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 SD-WAN 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 SD-WAN 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 SD-WAN Manager が認識できるようにします。
4. Cisco SD-WAN 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 SD-WAN コントローラの Cisco SD-WAN Manager 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。Cisco SD-WAN Manager テンプレートのアタッチすると、初期の最小限の構成が上書きされます。

ESXi での Cisco Catalyst SD-WAN コントローラ VM インスタンスの作成

はじめる前に

Cisco SD-WAN 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。

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.14.1 から、ハイパーバイザでディスク暗号化を有効にできます。

Cisco Catalyst SD-WAN コントローラ VM インスタンスの作成

1. vSphere Client を起動し、Cisco SD-WAN コントローラ 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. Cisco SD-WAN コントローラ 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 Cisco SD-WAN コントローラ 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 クライアントの起動および Cisco Catalyst SD-WAN コントローラ 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、Cisco SD-WAN コントローラ 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、Cisco SD-WAN コントローラ 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 Cisco SD-WAN Manager 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 SD-WAN Manager– 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. [Cisco SD-WAN Manager– 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。

Cisco Catalyst SD-WAN コントローラ 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。Cisco SD-WAN コントローラ 仮想マシンの電源が入ります。
2. [Console] を選択して、Cisco SD-WAN コントローラ 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 Catalyst SD-WAN コントローラ の設定」を参照してください。

KVM での Cisco Catalyst SD-WAN コントローラ VM インスタンスの作成

Cisco SD-WAN 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、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 Cisco SD-WAN コントローラ 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、Cisco SD-WAN コントローラ 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] をクリックして Cisco SD-WAN コントローラ ソフトウェアイメージを検索します。
 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. [Cisco SD-WAN コントローラ 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. [Cisco SD-WAN コントローラ 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、Cisco SD-WAN コントローラ 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 Catalyst SD-WAN コントローラ の設定」を参照してください。

Cisco Catalyst SD-WAN コントローラ の設定

オーバーレイネットワークで Cisco SD-WAN 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 Cisco SD-WAN Validator 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 (Cisco SD-WAN Validator、Cisco SD-WAN Manager、および Cisco SD-WAN 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 VPN0 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、Cisco SD-WAN 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 Catalyst 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。

SSH を使用して初期構成を作成し、Cisco SD-WAN コントローラ への CLI セッションを開きます。

初期設定を作成したら、Cisco SD-WAN Manager NMS で構成テンプレートを作成し、Cisco SD-WAN コントローラ 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 SD-WAN コントローラ にアタッチすると、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。

この初期構成では、システム IP アドレスを Cisco SD-WAN 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。Cisco SD-WAN コントローラ と vEdge ルータ間、および Cisco SD-WAN コントローラ と Cisco SD-WAN Validator 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 Cisco SD-WAN 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。

Cisco Catalyst SD-WAN コントローラ の初期設定の作成

CLI セッションから Cisco SD-WAN コントローラ で初期設定を作成するには、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 SD-WAN Manager 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 Catalyst SD-WAN 制御コンポーネントリリース 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す。

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

Cisco SD-WAN Manager 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 Catalyst SD-WAN Validator の IP アドレスか、Cisco Catalyst SD-WAN Validator を指す DNS 名を設定します。Cisco Catalyst SD-WAN Validator 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 SD-WAN Manager 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 SD-WAN 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 Cisco SD-WAN コントローラ 構成テンプレートを Cisco SD-WAN Manager で作成します。次の Cisco SD-WAN Manager 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 Cisco SD-WAN Validator 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 SD-WAN Manager メニューから、**[Administration]** > **[Settings]**の順に選択し、組織名を設定します。
- Cisco SD-WAN Manager 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。
- ロギング機能構成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、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、Cisco SD-WAN コントローラ 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。

```
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

「Cisco SD-WAN コントローラ 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 Catalyst SD-WAN コントローラ の構成テンプレートの作成

Cisco SD-WAN Manager によって管理されている Cisco SD-WAN コントローラ の場合は、Cisco SD-WAN Manager から設定する必要があります。Cisco Catalyst SD-WAN コントローラ で CLI から直接設定すると、Cisco SD-WAN Manager により Cisco SD-WAN Manager 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 SD-WAN コントローラ を設定する前に、Cisco SD-WAN 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 SD-WAN Manager 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 SD-WAN コントローラ、および Cisco SD-WAN Validator）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 Catalyst SD-WAN コントローラ の機能テンプレート

次の機能は Cisco SD-WAN 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、アカウントティング (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 SD-WAN コントローラ の完全な構成の構成要素です。Cisco Catalyst SD-WAN コントローラ で有効にできる機能ごとに、Cisco SD-WAN Manager 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 SD-WAN 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。

Cisco SD-WAN コントローラ 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 SD-WAN Manager 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 **[Controller]** を選択します。Cisco SD-WAN 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 SD-WAN 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。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- 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 SD-WAN 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 SD-WAN Manager 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 SD-WAN 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 Cisco SD-WAN コントローラ 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 SD-WAN Manager はエラーメッセージを返します。Cisco SD-WAN 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 SD-WAN Manager 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] ドロップダウンリストから [Controller] を選択します。
5. Cisco SD-WAN コントローラ 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 SD-WAN Manager 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 SD-WAN Manager 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、[Controller] 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 SD-WAN コントローラ へのデバイステンプレートのアタッチ

Cisco SD-WAN 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 SD-WAN 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 SD-WAN 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 SD-WAN Manager 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 SD-WAN 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 SD-WAN 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 SD-WAN 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 Catalyst SD-WAN コントローラの追加

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

Cisco Catalyst SD-WAN コントローラ の追加と証明書の生成

Cisco SD-WAN 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 SD-WAN Manager 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。



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、**[Controllers]** タブの名前が **[Control Components]** タブに変更されました。

3. **[Add Controller]** ウィンドウで、次の手順を実行します。
 1. Cisco SD-WAN 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 SD-WAN 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 SD-WAN Manager は CSR を自動的に生成し、生成した証明書を取得して、Cisco SD-WAN 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 SD-WAN 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 SD-WAN Manager 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 SD-WAN コントローラ と Cisco SD-WAN Validator 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 SD-WAN Manager に表示されません。Cisco SD-WAN コントローラ と Cisco SD-WAN Validator 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 25: 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 Catalyst SD-WAN 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 Catalyst SD-WAN 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。

- [Deploying Cisco Catalyst 8000V Edge ソフトウェア on Amazon Web Services](#)
- [Deploying Cisco Catalyst 8000V Edge ソフトウェア on Microsoft Azure](#)
- [Deploying Cisco Catalyst 8000V Edge ソフトウェア on Google Cloud Platform](#)
- [Cisco Catalyst 8000V Edge Software Deployment Guide for Alibaba Cloud](#)

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 Catalyst 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。

- [Cisco CSR 1000v Series Cloud Services Router Deployment Guide for Amazon Web Services](#)
- [Cisco CSR 1000v Deployment Guide for Microsoft Azure](#)

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 Catalyst 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、[Cisco Catalyst 8000V Edge Software Deployment Guide for Alibaba Cloud](#) [英語] を参照してください。

機能

Cisco Catalyst 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 26: 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 Catalyst SD-WAN Cloud onRamp の統合	Cisco Catalyst SD-WAN 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 (233 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 Catalyst 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 Catalyst 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 Catalyst 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 Catalyst 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 Catalyst SD-WAN インスタンスを作成するときは、Cisco SD-WAN Manager 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 Catalyst 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 SD-WAN Validator および Cisco SD-WAN Manager コントローラに接続します。

Cisco Catalyst SD-WAN 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 SD-WAN Manager 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 Catalyst 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 SD-WAN Manager 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 SD-WAN Manager 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。Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN コントローラ および Cisco SD-WAN Validator 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 SD-WAN Validator の Cisco SD-WAN Manager テンプレートを作成して、オーケストレータにアタッチします。Cisco SD-WAN Manager テンプレートのアタッチすると、初期の最小限の構成が上書きされます。
5. Cisco Catalyst 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 SD-WAN Validator、Cisco SD-WAN Manager、および Cisco SD-WAN 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

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 SD-WAN Validator と Cisco SD-WAN Manager 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



(注) Cisco vManage リリース 20.9.1 以降、vEdge クラウドルータ はサポートされていません。

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 Cisco Catalyst 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 Catalyst 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 Catalyst SD-WAN AMI はプライベートです。共有できる Cisco Catalyst SD-WAN の営業担当者にお問い合わせください。
2. Cisco Catalyst 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 27: 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
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/inedited
  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$9ac6af765f1cd0c0$jm/rCPsQ56JlUJ/1s9H7zhksy/FZht37zD1kz4Mh/IU/FsrltBuLw3AVI5KnfX9WingP8CsGk.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す。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 バイトのパケット）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**

				IF	IF						
				TCP	ADMIN	OPER	ENCAP				
				MSS		RX					
VPN	INTERFACE	AF	IP ADDRESS		STATUS	STATUS	TYPE	PORT	TYPE	MTU	HWADDR
		SPEED	DUPLEX	ADJUST	UPTIME		PACKETS	PACKETS			
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**

				IF	IF						
				TCP							
				AF	ADMIN	OPER	ENCAP				
				SPEED		RX	TX				
VPN	INTERFACE	TYPE	IP ADDRESS	MSS	STATUS	STATUS	TYPE	PORT	TYPE	MTU	HWADDR
				DUPLEX	UPTIME	PACKETS	PACKETS				
0	ge0/0	ipv4	10.66.15.15/24		Up	Up	null	service		1500	
00:0c:29:db:f0:62	1000	full	1420		0:14:05:30	546018	545562				
0	ge0/1	ipv4	10.1.17.15/24		Up	Up	null	service		1500	
00:0c:29:db:f0:6c	1000	full	1420		0:14:21:42	0	10				
0	ge0/2	ipv4	-		Down	Up	null	service		1500	
00:0c:29:db:f0:76	1000	full	1420		0:14:22:10	0	0				
0	ge0/3	ipv4	10.0.20.15/24		Up	Up	null	service		2000	
00:0c:29:db:f0:80	1000	full	1920		0:14:21:42	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		0:14:21:42	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		0:14:21:42	773	708				
0	system	ipv4	172.16.255.15/32		Up	Up	null	loopback		1500	
00:00:00:00:00:00	0	full	1420		0:14:21:54	0	0				
0	loopback3	ipv4	10.1.15.15/24		Up	Up	null	transport		2000	
00:00:00:00:00:00	10	full	1920		0:14:21:46	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		0:14:21:38	52038	52079				
1	ge0/5	ipv4	172.16.1.15/24		Up	Up	null	service		1500	


```

00:0c:29:db:f0:94 1000 full 1420 0:14:21:38 0 8
512 eth0 ipv4 10.0.1.15/24 Up Up null service 1500
00:50:56:00:01:05 0 full 0 0:14:21:39 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、H11、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 Catalyst 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 Catalyst 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

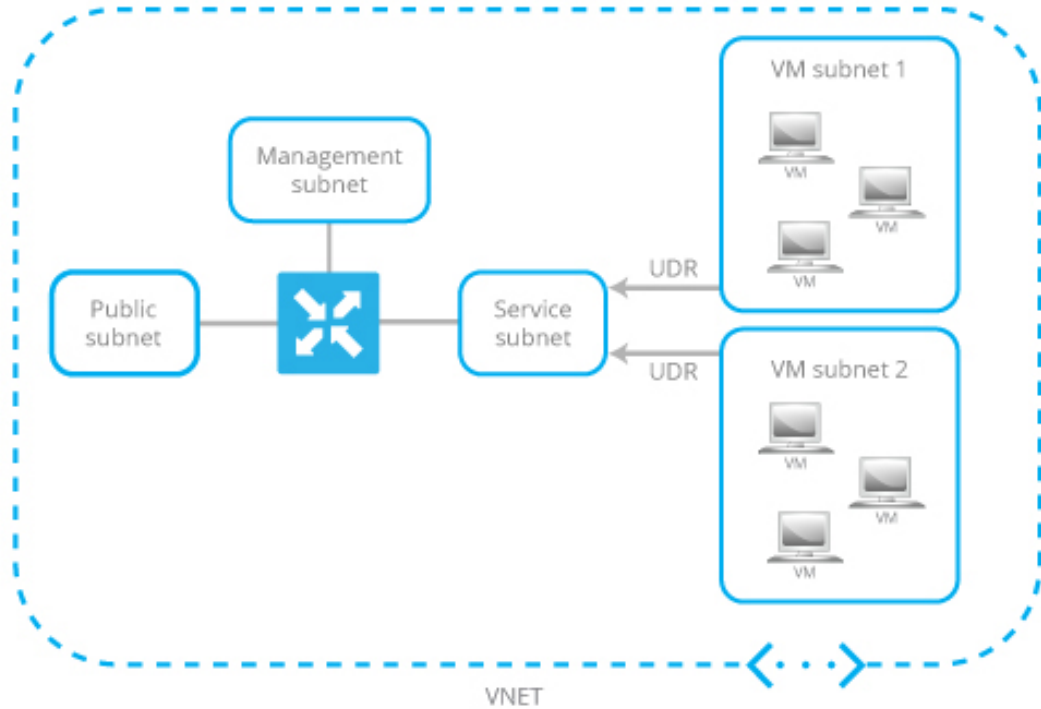
1. Azure Marketplace アプリケーションを起動します。
 1. 左側のペインで、[New] をクリックして、新しい vEdge クラウドルータ VM インスタンスを作成します。
 2. [Search] ボックスで、「Cisco」を検索します。
2. 右側のペインで、[Cisco vEdge クラウドルータ (3 NICs) (Staged)] を選択します。
3. [Cisco vEdge クラウドルータ (3 NICs) (Staged)] 画面で、左側のペインの [Basic] をクリックして、vEdge クラウドルータ VM の基本設定を指定します。
 1. [VM Name] 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/azure/active-directory/active-directory-ssh-key-pairs> 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する必要があります。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 26: 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 Catalyst 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 Catalyst 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 Catalyst 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 Catalyst 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 Catalyst 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 28:

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 宛てのトラフィックは 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、vEdgeCloud 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 Catalyst 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 SD-WAN Manager 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 SD-WAN Manager 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）を送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 Catalyst 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 Catalyst 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 Catalyst 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 29:

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

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 SD-WAN Manager メニューから、**[Administration] > [Settings]**の順に選択します。
2. **[Hardware WAN Edge Certificate Authorization]** をクリックします。（Cisco Catalyst SD-WAN Manager リリース 20.12.1 以前を使用している場合は、**[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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager はトークンを Cisco SD-WAN Validator および Cisco SD-WAN 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、ルータのシャース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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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、ルータのシャシー番号として使用されます。
- トークン。これは、ルータが Cisco SD-WAN Manager と Cisco SD-WAN Validator 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。
- Cisco SD-WAN Validator の IP アドレスまたは DNS 名。
- 組織名。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降、ブートストラップ設定ファイルの [Organization Name] フィールドにカンマを含めることはできません。

- デバイス構成テンプレートをすでに作成し、vEdgeCloud 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 Catalyst SD-WAN Validator 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、Cisco SD-WAN Validator 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 SD-WAN Manager メニューから、**[Administration] > [Settings]** の順に選択します。
2. **[Validator]** をクリックします。 (**[Edit]** をクリックします。)
3. **[DNS/IP Address: Port]** フィールドに Cisco SD-WAN Validator 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. 組織名を確認します。この名前は、Cisco SD-WAN Validator で設定されたものと同じである必要があります。(Cisco Catalyst SD-WAN Manager リリース 20.12.1 以前を使用している場合、**[Organization Name]** を確認するには、**[View]** をクリックします。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、システムの組織名にカンマを含めることはできません。デバイスの設定中に、カンマを使用することはできません。

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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager メニューから、**[Administration] > [Settings]** の順に選択します。
2. **[WAN Edge Cloud Certificate Authorization]** をクリックし、**[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



- (注) Cisco SD-WAN リリース 20.5.1 では、Cisco vEdge クラウドルータ用に生成した cloud-init ブートストラップ構成を Cisco vEdge クラウドルータ 20.5.1 の展開に使用できません。ただし、ブートストラップ構成を使用して Cisco vEdge クラウドルータ 20.4.1 以前のバージョンを展開できます。

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 SD-WAN Manager 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、Cisco SD-WAN Validator 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。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、システムの組織名にカンマを含めることはできません。デバイスの設定中に、カンマを使用することはできません。

- 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、Cisco SD-WAN Validator 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 Catalyst 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager が CSR を生成します。
2. CSR をダウンロードします。
 1. Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager から収集し、ブートストラップ構成を作成した後に、Cisco SD-WAN Manager 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 Cisco SD-WAN Validator の DNS 名または IP アドレスと組織名を追加します。
2. ルータのシャード番号とトークン番号を Cisco SD-WAN Manager に送信します。
3. Cisco SD-WAN Manager 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 SD-WAN Manager 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. Cisco SD-WAN Validator の IP アドレスか、Cisco SD-WAN Validator を指す DNS 名を設定します。Cisco SD-WAN Validator 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 ルータのシャード番号とトークン番号を Cisco SD-WAN Manager 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ド番号を確認します。
 1. Cisco SD-WAN Manager 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 SD-WAN Manager 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、Cisco SD-WAN Validator 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager がシャーン番号とトークン番号を受け取ると、Cisco SD-WAN Manager が CSR を生成します。

2. CSR をダウンロードします。

1. Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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://catmanag<wb>websecuritysymantec.com<wb>mcopenroll/index?jur_hash=<wb>#22d7cb508a24e32a7db478b7<wb>#8
```

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 Catalyst 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、Cisco SD-WAN Validator 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 30: 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 Catalyst SD-WAN 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 SD-WAN Manager 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 SD-WAN Manager、Cisco SD-WAN コントローラ、および Cisco SD-WAN Validator 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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。



(注) Cisco vManage リリース 20.10.1 以前の Cisco Catalyst SD-WAN Manager にルータのシリアル番号ファイルを正常に送信するには、ファイルが /home/admin または /home/vmanage-admin にインストールされていることを確認します。admin または vmanage-admin 以外のログイン情報を使用してルータのシリアル番号ファイルを送信すると、エラーが発生します。

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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager メニューから、**[Administration]** > **[Settings]** の順に選択します。
2. **[Smart Account Credentials]** をクリックします。(Cisco Catalyst SD-WAN Manager リリース 20.12.1 以前を使用している場合は、**[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]** をクリックします。(Cisco Catalyst SD-WAN Manager リリース 20.12.1 以前を使用している場合は、**[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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 Catalyst 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 SD-WAN Manager 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 Catalyst 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 SD-WAN Manager 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。

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す。

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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 Cisco SD-WAN Manager にアップロードするには、**[Upload]** をクリックします。

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 SD-WAN Manager 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

ルータが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 SD-WAN Manager 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 SD-WAN Manager 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れば、**[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 Catalyst 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 SD-WAN Validator、Cisco SD-WAN Manager、および Cisco SD-WAN 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 Catalyst 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 Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Manager 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 Cisco SD-WAN Validator 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 SD-WAN コントローラ と vEdge ルータ間、および Cisco SD-WAN コントローラ と Cisco SD-WAN Validator 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。

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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager のメニューから、**[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. タイムゾーン
 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 Cisco SD-WAN Manager 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 SD-WAN Manager のメニューから、**[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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 Catalyst 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 Cisco SD-WAN Manager 設定テンプレートを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 SD-WAN Manager 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 SD-WAN Manager によって管理されるようになった場合、Cisco SD-WAN Manager がルータを検出すると、ルータの設定が Cisco SD-WAN Manager 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。

vEdgeCloud 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Validator の IP アドレスか、Cisco SD-WAN Validator を指す DNS 名を設定します。Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager で作成します。次の Cisco SD-WAN Manager 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 Cisco SD-WAN Validator 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 SD-WAN Manager メニューから、**[Administration] > [Settings]**の順に選択し、組織名を設定します。
- Cisco SD-WAN Manager 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。
 - ログ機能設定テンプレートの場合、ロ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 Catalyst SD-WAN ネットワークで VPN 512 を設定する必要もあります。

1. Cisco SD-WAN Manager メニューから、**[Administration]** > **[Settings]**の順に選択します。
2. **[Data Stream]** をクリックします。（Cisco Catalyst SD-WAN Manager リリース 20.12.1 以前を使用している場合は、**[Edit]** をクリックします。）
3. **[Data Stream]** を有効化します。
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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 Catalyst 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。

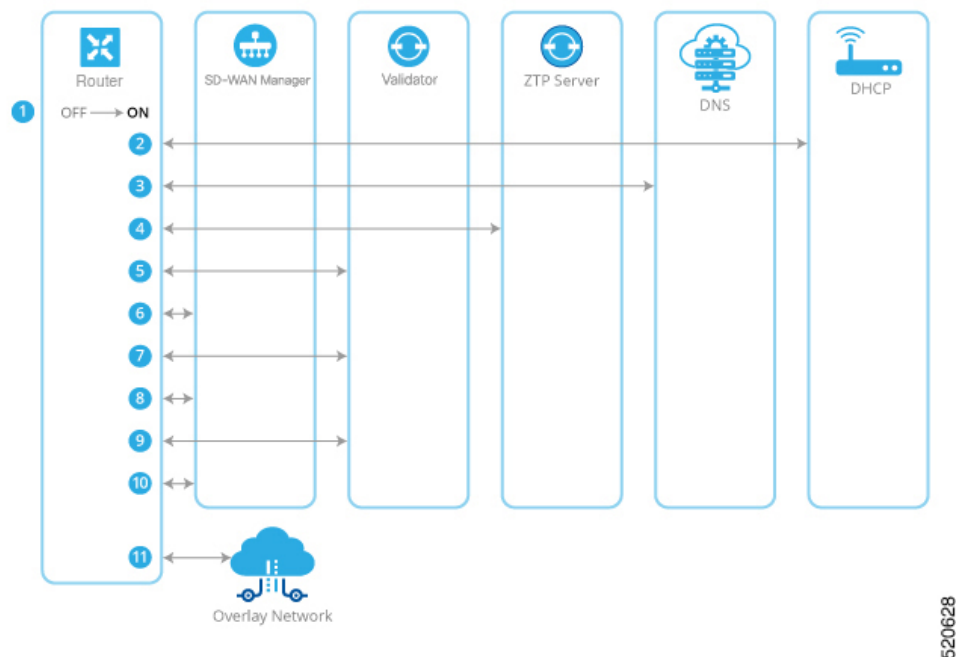
ZTP プロセスが機能するには:

- 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 Catalyst 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 Catalyst 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 27: 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。
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 Catalyst SD-WAN リリース 17.7.1a の Cisco IOS XE Catalyst 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 Catalyst SD-WAN リリース 17.7.1a 以前の Cisco IOS XE Catalyst 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 Catalyst SD-WAN デバイス）を解決し、Cisco Catalyst 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 SD-WAN Validator の IP アドレスを送信します。この Cisco SD-WAN Validator の組織名は、vEdge ルータと同じです。
5. ルータは Cisco SD-WAN Validator 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 SD-WAN Validator 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 SD-WAN Validator はルータに Cisco SD-WAN Manager の IP アドレスを送信します。
6. ルータは Cisco SD-WAN Manager への接続を確立し、vManage によってルータが検証されます。Cisco SD-WAN Manager 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 SD-WAN Validator 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Validator への接続を再確立し、オーケストレータはルータを再度検証します。
10. ルータは Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Validator を Cisco Catalyst 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 SD-WAN Manager 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 SD-WAN Validator を Cisco Catalyst 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 SD-WAN Manager 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 を使用するときには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 SD-WAN Manager 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 SD-WAN Manager 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。



第 7 章

Quick Connect ワークフロー

- [Quick Connect ワークフロー \(282 ページ\)](#)
- [Quick Connect ワークフローを使用するための前提条件 \(282 ページ\)](#)
- [Quick Connect ワークフローの制約事項 \(283 ページ\)](#)
- [Quick Connect について \(284 ページ\)](#)
- [Quick Connect ワークフローへのアクセス \(287 ページ\)](#)

Quick Connect ワークフロー

表 31: 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイス をオンボードするための Quick Connect ワークフロー	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能は、サポートされている WAN Edge デバイスを Cisco Catalyst SD-WAN オーバーレイネットワークにオンボードするための Cisco SD-WAN Manager におけるガイド付きの代替手法を提供します。Quick Connect ワークフローの一部として、基本的なデイズロ構成プロファイルが作成されます。これは、デバイスモデルやデバイスファミリーに関係なく、すべての Cisco Catalyst SD-WAN (IOS XE) デバイスに適用されます。このワークフローにより、WAN トランスポートにエッジデバイスが追加され、データプレーンとコントロールプレーンの接続が確立されます。 この機能は、Cisco IOS XE Catalyst SD-WAN デバイスでのみサポートされています。
デバイス展開時のリージョンとサブリージョンの指定	Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.13.1	デバイスを展開するときに、リージョンとサブリージョンの両方を指定できます。

Quick Connect ワークフローを使用するための前提条件

- 組織名を設定する必要があります。
- Cisco SD-WAN Validator および Cisco SD-WAN コントローラ の証明書認証を設定する必要があります。

- コントローラ（Cisco SD-WAN Manager、Cisco SD-WAN Validator、および Cisco SD-WAN コントローラ）をインストールして設定する必要があります。



(注) これらのコントローラを設定していない場合は、Quick Connect ワークフローから Cisco SD-WAN Manager の **[Administration]** > **[Settings]** ウィンドウに移動し、前提条件の設定を完了します。

Quick Connect ワークフローの制約事項

WAN 設定

Quick Connect ワークフローは、WAN 設定（VPN 0）の指定に限定されています。Cisco Catalyst SD-WAN オーバーレイの起動プロセスを完了できるようにするには、サービス側 VPN テンプレートも構成する必要があります。

ネットワーク インターフェイスの設定の詳細については、「[Configure Network Interfaces](#)」を参照してください。

プラットフォーム サポート

Quick Connect ワークフローは、Cisco Catalyst SD-WAN Device（IOS XE）デバイスでのみサポートされています。

1 つの進行中のワークフロー

どの時点でも、同時に複数のワークフローを進行させることはできません。

Quick Connect ワークフローのデバイスの最大数

Quick Connect ワークフローは、以下の例外を除き、一度に最大 500 台のデバイスのデイレロ構成の作成をサポートしています。

- Cisco Catalyst SD-WAN Manager リリース 20.14.1 および 20.16.x：一度に最大 25 台のデバイス
- Cisco Catalyst SD-WAN Manager リリース 20.15.1：一度に最大 25 台のデバイス。20.15.x の今後のリリースでは 500 台をサポートします。

最大数を超えるデバイスがある場合は、ワークフローを複数回実行します。

Quick Connect について

Quick Connect ワークフローの概要

Cisco SD-WAN Manager の Quick Connect ワークフローでは、デバイスのファミリーおよびモデルに関係なく、すべての Cisco IOS XE SD-WAN デバイスに適用できる基本的なゼロ構成プロファイルが作成されます。このワークフローにより、WAN でコントロールプレーンとデータプレーンへのアクセスが確立されます。

Quick Connect ワークフローの動作は、デバイスを Cisco SD-WAN Manager にアップロードする方法によって異なります。次のいずれかの方法で、Quick Connect ワークフローの一部として、または個別に、デバイスをアップロードできます。

- 自動同期オプションを使用：スマートアカウントが Cisco SD-WAN Manager と同期されます。このオプションでは、Cisco SD-WAN Manager が Cisco Plug n Play (PnP) ポータルに接続する必要があります
- 手動アップロード手法を使用：デバイスの認定シリアル番号ファイルを Cisco PnP ポータルからダウンロードし、Cisco SD-WAN Manager にアップロードします

オンボードデバイスの IP アドレス

Quick Connect ワークフローでは、新たにオンボードされたデバイスに IP アドレスが次のように割り当てられます。

- 次の場合、アドレスはシステム IP プールから割り当てられます。
 - システム IP プールが定義済みである（「[システム IP プールの作成](#)」を参照）場合
 - システム IP の選択が Quick Connect ワークフローで [Auto] に設定されている場合
- それ以外の場合は、ワークフローのいずれかのステップで手動で入力した IP アドレスを使用します。

自動同期を使用したデバイスのアップロード

デバイスを Cisco SD-WAN Manager にアップロードする自動同期方式は、クラウドコントローラを含む展開とオンプレミスコントローラを含む展開のどちらも使用できますが、Cisco SD-WAN Manager がプラグアンドプレイ (PnP) ポータルに接続できることが条件です。

自動同期オプションが Cisco PnP で機能する仕組み

シスコチームが Cisco SD-WAN コントローラを設定して展開すると、注文に関連付けられた Cisco SD-WAN Manager 情報を含む電子メールが送信されます。このような場合にデバイスをオーバーレイネットワークに追加するには、次の手順に従います。

1. デフォルトのログイン情報（admin/admin）を使用して Cisco SD-WAN Manager にログインします。
2. Cisco PnP ポータルから Cisco SD-WAN Manager にデバイス情報を転送するには、Cisco SD-WAN Manager でスマートアカウントまたは仮想アカウントを同期します。この手順には、バーチャルアカウント管理者ロールのシスコクレデンシャルが必要です。WAN エッジルータのシリアル番号のアップロードの詳細については、[Upload WAN Edge Router Serial Numbers from Cisco Smart Account \[英語\]](#) を参照してください。



- (注) PnP ポータルに新しいデバイスを追加するたびに、Cisco SD-WAN Manager をスマートアカウントまたは仮想アカウントと再同期して、新しいデバイスが Cisco SD-WAN Manager に表示されるようにする必要があります。

デバイス情報が Cisco SD-WAN Manager に転送されたら、Cisco SD-WAN Manager オーバーレイを設定できます。



- (注) Cisco PnP ポータルと、Cisco SD-WAN Manager のオンボーディングデバイスにおけるその役割の詳細については、次の参考ドキュメントを参照してください。

- [Cisco Plug and Play Support Guide for Cisco SD-WAN Products](#)
- [Plug n Play Onboarding Workflow](#)

自動同期オプションが ZTP で機能する仕組み

サポートされている WAN エッジデバイスが Cisco ゼロタッチプロビジョニング（ZTP）に登録されている場合、デバイスのオンボーディングは自動化され、デバイスは Cisco SD-WAN Validatorによって認証されます。

ZTP を使用する場合、デバイスを箱から出した後、その WAN ポートをネットワークに接続し、DHCP からの IP 設定が構成されていることを確認します。これには、IP アドレス、マスク、ゲートウェイ、および DNS の設定が含まれます。次にデバイスは Cisco PnP ポータルのインベントリを認識している ZTP サーバーを探します。次に ZTP サーバーはデバイスを認証し、さらなる認証のために Cisco SD-WAN Validator にリダイレクトします。



- (注) vEdge ルータをオーバーレイネットワークに自動的に参加するように設定する方法については、「[Prepare Routers for ZTP](#)」を参照してください。

自動同期オプションを使用してオンボードされたデバイスの表示方法

自動同期オプションのいずれかを使用して（Cisco ZTP または Cisco PnP を介して）デバイスを Cisco SD-WAN Manager にアップロードすると、Quick Connect ワークフローの最後に、

[Monitor] > [Overview]からアクセス可能な Cisco SD-WAN Manager ダッシュボードにデバイスが表示されます。

Cisco vManage リリース 20.6.x 以前：自動同期オプションのいずれかを使用して（Cisco ZTP または Cisco PnP を介して）デバイスを Cisco SD-WAN Manager にアップロードすると、Quick Connect ワークフローの最後に、[Dashboard] > [Main Dashboard]からアクセス可能な Cisco SD-WAN Manager ダッシュボードにデバイスが表示されます。

デバイスの手動アップロード

次の場合、デバイスを Cisco SD-WAN Manager に手動でアップロードすることを選択できます。

- スマートアカウントを Cisco SD-WAN Manager と同期する必要がある自動同期オプションを使用したくない
- Cisco SD-WAN Manager インスタンスが Cisco PnP ポータルに接続できない

デバイスの手動アップロードの方法

デバイスを Cisco SD-WAN Manager に手動でアップロードするには、次の手順を実行します。

1. Cisco PnP ポータルから認定シリアル番号ファイルまたはプロビジョニングファイルをダウンロードします。このファイルは、PnP ポータルで入手できます（[Controllers] > [Provisioning File]）。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

2. 認定シリアル番号ファイルを Cisco SD-WAN Manager に手動でアップロードすることにより、デバイス情報を Cisco SD-WAN Manager に転送します。WAN Edge ルータシリアル番号の手動アップロードの詳細については、『[Upload WAN Edge Router Authorized Serial Number File](#)』を参照してください。

デバイスを手動アップロードするときの Quick Connect の動作

手動の手法でデバイスを Cisco SD-WAN Manager にアップロードする場合、Quick Connect ワークフローによって生成される CLI ブートストラップ構成を使用してデバイスを展開するまで、それらは Cisco SD-WAN Manager ダッシュボードに表示されません。

ブートストラップ方式では、工場出荷時の WAN Edge デバイスを、安全に展開して Cisco Catalyst SD-WAN ネットワークに参加させるために必要な構成でオンボードできます。



- (注) CLI ブートストラップ設定を使用して Cisco Catalyst SD-WAN デバイス (IOS XE) を展開する完全な手順については、『[On-Site Bootstrap Process for Cisco SD-WAN Devices](#)』を参照してください。

Quick Connect ワークフローへのアクセス

1. Cisco SD-WAN Manager のメニューから、[Workflows] を選択します。
2. 新しい **Quick Connect** ワークフローを開始：[Library] 領域で、[Quick Connect] を選択します。

または

進行中の Quick Connect ワークフローを再開：進行中の領域で、[Quick Connect] をクリックします。



- (注) 手動アップロード方式でデバイスを Cisco SD-WAN Manager にアップロードする場合は、Quick Connect ワークフローが生成する CLI ブートストラップ設定を使用してデバイスを展開するという追加の手順を完了する必要があります。デバイスにロードするブートストラップ設定ファイルの生成の詳細については、[On-Site Bootstrap Process for Cisco SD-WAN Devices](#) を参照してください。



第 8 章

クラスタの管理

表 32: 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN Manager ペルソナベースのクラスタ構成	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco SD-WAN リリース 20.6.1 Cisco vManage リリース 20.6.1	ペルソナに基づいてサーバーを識別することにより、クラスタへの Cisco SD-WAN Manager サーバーの追加を簡素化します。ペルソナは、サーバーで実行されるサービスを定義します。

- [クラスタ管理に関する情報 \(289 ページ\)](#)
- [Cisco Catalyst SD-WAN Manager クラスタのガイドライン \(290 ページ\)](#)
- [利用可能なクラスタサービスの表示 \(292 ページ\)](#)
- [Cisco Catalyst SD-WAN Manager サーバーのクラスタ IP アドレスの設定 \(292 ページ\)](#)
- [Cisco Catalyst SD-WAN Manager サーバーのクラスタへの追加 \(294 ページ\)](#)
- [Cisco Catalyst SD-WAN Manager サービスの詳細の表示 \(298 ページ\)](#)
- [Cisco Catalyst SD-WAN Manager パラメータの編集 \(299 ページ\)](#)
- [設定データベースのログイン情報の更新 \(299 ページ\)](#)
- [Cisco Catalyst SD-WAN Manager のダウングレード \(301 ページ\)](#)
- [Cisco SD-WAN Manager クラスタのアップグレード \(301 ページ\)](#)
- [Cisco Catalyst SD-WAN Manager プロセスの手動再起動 \(306 ページ\)](#)
- [クラスタからの Cisco Catalyst SD-WAN Manager ノードの削除 \(308 ページ\)](#)

クラスタ管理に関する情報

Cisco SD-WAN Manager クラスタは、少なくとも 3 つの Cisco SD-WAN Manager サーバーで構成されます。これらのサーバーは、ネットワーク内の Cisco Catalyst SD-WAN エッジデバイスを管理します。クラスタ内の Cisco SD-WAN Manager サーバーは、サーバーで実行されているサービスに基づいて特定の機能を実行します。このようにして、クラスタは Cisco SD-WAN Manager サーバー間で情報を共有しながら、サーバー間でワークロードを分散します。拡張性

の推奨事項については、『[Cisco Catalyst SD-WAN Controller Compatibility Matrix and Server Recommendations](#)』で、ご使用のリリースの「Server Recommendations」を参照してください。

[Administration] > [Cluster Management] ウィンドウを使用して、Cisco SD-WAN Manager クラスタを作成し、関連するタスクを実行します。

Cisco vManage リリース 20.6.1 以降、各 Cisco SD-WAN Manager サーバーにはペルソナがあります。ペルソナは、Cisco SD-WAN Manager のインストール後、Cisco SD-WAN Manager サーバーが最初に起動したときに決まり、サーバーで実行されるサービスが定義されます。サーバーのペルソナは、サーバーの存続期間中持続し、変更できません。サーバーは、クラスタに追加する前にペルソナを持っている必要があります。ペルソナの詳細については、「[Cisco Catalyst SD-WAN Manager Persona and Storage Device](#)」を参照してください。

クラスタ内でのサーバーの役割は、そのペルソナによって異なります。Cisco SD-WAN Manager サーバーは、次のいずれかのペルソナを持つことができます。

- コンピューティングとデータ：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 SD-WAN Manager に必要なすべてのサービスが含まれます
- コンピューティング：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。
- データ：アプリケーションと統計に使用されるサービスが含まれます。

暗号化 (Encryption)

Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a から、すべてのサービスのクラスタトラフィックが暗号化されます。

予約済み IP アドレス

Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a から、Cisco SD-WAN Manager クラスタ内の WAN エッジデバイスまたは Cisco SD-WAN 制御コンポーネントは、172.30.0.0/16 プレフィックスで IP アドレスを予約します。これらの予約済み IP アドレスは、WAN エッジデバイスまたは Cisco SD-WAN 制御コンポーネントでシステム IP アドレスとして使用することはできません。予約済み IP アドレスが WAN エッジデバイスまたは Cisco SD-WAN 制御コンポーネントですでに使用されている場合は、TAC ケースを開いて IP アドレスを置き換えます。

Cisco Catalyst SD-WAN Manager クラスタのガイドライン

次のガイドラインは Cisco SD-WAN Manager クラスタに適用されます。

- Cisco SD-WAN Manager クラスタのすべてのメンバーを同じデータセンターに配置することをお勧めします。
- Cisco SD-WAN Manager クラスタのすべてのメンバーの IP アドレスが同じサブネットに存在することをお勧めします。



(注)

- マルチノード Cisco SD-WAN Manager クラスタでは、SD-WAN Manager system-ip は SD-WAN Manager クラスタ自身が指定したシステム IP であり、個々のデバイスのシステム IP とは異なる場合があります。
 - デバイスの system-ip が各デバイスの一意的識別子である一方で、SD-WAN Manager system-ip は制御接続を管理するクラスタノードを表します。
-
- Cisco SD-WAN Manager クラスタインターフェイスは、トランスポート インターフェイスと同じにしないことをお勧めします。Cisco vManage リリース 20.9.1 以降、これは強制的になります。この設定を行おうとすると、Cisco SD-WAN Manager にエラーメッセージが表示されます。
 - クラスタインターフェイスは外部からアクセスできないようにする必要があります。
 - Cisco SD-WAN Manager クラスタ IP アドレスへのアクセスは、同じクラスタ内の Cisco SD-WAN Manager インスタンスに制限されます。
 - Cisco SD-WAN Manager クラスタのメンバーは、タイムスタンプに依存してデータを同期し、デバイスの稼働時間を追跡します。この時間依存データの正確さを保つため、クラスタ内の Cisco SD-WAN Manager サーバーの時刻を変更する必要がある場合は、クラスタ内のすべての Cisco SD-WAN Manager サーバーで同じ変更を行います。
 - 3 ノードクラスタ展開では、系統的な障害が発生できるのは 1 つのノードのみです。1 つのノードに障害が発生しても、残り 2 つのノードの Cisco SD-WAN Manager グラフィカル ユーザーインターフェイス (GUI) は到達可能であり、SSH を介して残りのノードと通信できます。2 つのノードに障害が発生した場合、ユーザーがすでにログインしているアクティブノードの GUI では読み取り専用操作が許可されますが、GUI への新しいログインは許可されません。
 - 工場出荷時のデフォルトのログイン情報がゲストノードに設定されている場合に、ホストノードがそれをクラスタに追加しようとする、クラスタ管理が失敗します。新しいノードのパスワードは、クラスタ内の他のノードと同じように変更する必要があります。
 - netadmin 権限を持つシングルサインオン (SSO) ユーザーを使用してログインすると、ユーザーは SSO ユーザーを使用してクラスタまたはディザスタリカバリ操作を実行できません。ノードの追加、削除、SD-AVC の有効化などのクラスタ操作の場合、Cisco SD-WAN Manager は net-admin グループのローカルユーザー名とパスワードの一部を想定しています。マルチテナンシーの場合、管理者ユーザーのみが SD-AVC を更新できます。netadmin 権限を持っていても、他のユーザーは SD-AVC を更新できません。
 - 専用の mgmt-intf を持たないデバイスでは、VPN 512 は VRF mgmt-intf ではなく、カスタムの VRF 512 にマッピングされます。バックエンドでは、この VRF は他のプラットフォームと同じ名前空間にマッピングされません。プラットフォームが異なるため、そのイメージはダウンロードできません。

利用可能なクラスタサービスの表示

Cisco SD-WAN Manager クラスタ内のすべてのメンバーで使用可能なサービスと到達可能なサービスを表示するには、**[Administration] > [Cluster Management] > [Service Reachability]** を選択します。

Cisco Catalyst SD-WAN Manager サーバーのクラスタ IP アドレスの設定

初めて Cisco SD-WAN Manager を起動すると、Cisco SD-WAN Manager サーバーのデフォルト IP アドレスが `localhost` と表示されます。新しい Cisco SD-WAN Manager サーバーをクラスタに追加する前に、プライマリ Cisco SD-WAN Manager サーバーの `localhost` アドレスをアウトオブバンド IP アドレスに変更する必要があります（Cisco vManage リリース 20.6.1 以降、プライマリ Cisco SD-WAN Manager サーバーにはコンピューティング+データペルソナがあります）。クラスタ内のサーバーは、このアウトオブバンド IP アドレスを使用して相互に通信します。

今後、アウトオブバンド IP アドレスを変更する必要がある場合は、シスコのサポート担当者にお問い合わせください。

Cisco SD-WAN Manager サーバー間のクラスタ相互接続では、各サーバーに静的 IP アドレスを割り当てる必要があります。クラスタの一部となる Cisco SD-WAN Manager サーバーに IP アドレスを割り当てる場合、DHCP を使用しないことをお勧めします。VPN 0 の非トンネルインターフェイスで IP アドレスを設定します。

Cisco SD-WAN Manager サーバーのクラスタ IP アドレスを設定する前に、そのサーバーインターフェイスについて、VPN0 でアウトオブバンド IP アドレスが設定されていることを確認してください。この構成は、通常、サーバーのプロビジョニング時に行われます。アウトオブバンド IP アドレスのポートタイプは、その IP アドレスを Cisco SD-WAN Manager サーバーへの割り当てに使用できるように、「`service`」である必要があります。



(注) Cisco vManage リリース 20.11.1 以降、一部のアラームでは、`system-ip/hostname` が Cisco SD-WAN Manager で構成されていないため、初めてクラスタセットアップ中にホスト名が **localhost** と表示されます。`system-ip/hostname` が構成されている場合、アラームは正しいホスト名を表示します。

Cisco vManage リリース 20.6.1 より前のリリースでの IP アドレスの設定

サーバーをクラスタに追加する前に、Cisco SD-WAN Manager サーバーの IP アドレスを設定します。Cisco vManage リリース 20.6.1 より前のリリースでこれを実行するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Administration] > [Cluster Management]** の順に選択し、**[Service Configuration]** をクリックします。
2. **[Add vManage]** をクリックします。
[Edit vManage] ダイアログボックスが開きます。
3. **[vManage IP Address]** ドロップダウンリストから、Cisco SD-WAN Manager サーバーに割り当てる IP アドレスを選択します。
4. Cisco SD-WAN Manager サーバーにログインするためのユーザー名とパスワードを入力します。
5. **[Update]** をクリックします。

Cisco SD-WAN Manager サーバーが再起動し、**[Cluster Management]** ウィンドウが表示されます。

Cisco vManage リリース 20.6.1 以降のリリースでの IP アドレスの設定

サーバーをクラスタに追加する前に、Cisco SD-WAN Manager サーバーの IP アドレスを設定します。Cisco vManage リリース 20.6.1 以降でこれを実行するには、次の手順を実行します。

この手順は、プライマリ Cisco SD-WAN Manager サーバー（コンピューティング + データペルソナを持つ）で実行します。

1. Cisco SD-WAN Manager メニューから、**[Administration] > [Cluster Management]** の順に選択します。
[Cluster Management] ウィンドウが表示されます。このウィンドウのテーブルには、クラスタ内にある Cisco SD-WAN Manager サーバーがリストされます。
2. 設定する Cisco SD-WAN Manager サーバーの横にある [...] をクリックし、**[Edit]** をクリックします。
[Edit vManage] ダイアログボックスが表示されます。
3. **[Edit vManage]** ダイアログボックスで、次のアクションを実行します。



(注) サーバーのペルソナは変更できません。そのため、**[Node Persona]** オプションは無効になっています。

1. **[vManage IP Address]** ドロップダウンリストから、サーバーに割り当てる静的アウトオブバンド IP アドレスを選択します。
2. **[Username]** フィールドに、サーバーにログインするためのユーザー名を入力します。
3. **[Password]** フィールドに、サーバーにログインするためのパスワードを入力します。
4. （任意）シスコのソフトウェア定義型 Application Visibility and Control (SD-AVC) をサーバーで実行する場合は、**[Enable SD-AVC]** をクリックします。

Cisco SD-AVC は Cisco Application Visibility and Control (AVC) のコンポーネントです。これは、1 つの Cisco SD-WAN Manager サーバーでのみ有効にできます。これを有効にするサーバーは、コンピューティング + データペルソナまたはコンピューティングペルソナを持つ必要があります。Cisco SD-AVC は、データペルソナを持つサーバーでは有効にできません。



(注) Cisco SD-WAN Manager がクラスタとしてセットアップされており、再起動またはアップグレードの結果としてクラスタがクラッシュする場合、エッジデバイスへの接続がリセットされ、カスタムアプリケーションが機能しなくなります。

これを解決して動作を再開させるには、カスタムアプリケーション名を新しい一意の名前で再定義します。カスタムアプリケーションの定義の詳細については、『Cisco Catalyst SD-WAN Policies Configuration Guide』の「[Define Custom Applications Using Cisco Catalyst SD-WAN Manager](#)」の章を参照してください。

5. [Update] をクリックします。

サーバーが再起動し、[Cluster Management] ウィンドウが表示されます。

Cisco Catalyst SD-WAN Manager サーバーのクラスタへの追加

表 33: 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN Manager ペルソナベースのクラスタ構成	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco SD-WAN リリース 20.6.1 Cisco vManage リリース 20.6.1	ペルソナに基づいてサーバーを識別することにより、クラスタへの Cisco SD-WAN Manager サーバーの追加を簡素化します。ペルソナは、サーバーで実行されるサービスを定義します。

ここでは、さまざまな Cisco SD-WAN Manager リリースでのクラスタへの Cisco SD-WAN Manager サーバーの追加に関する情報を提供します。

Cisco vManage リリース 20.6.1 より前のリリースでの Cisco SD-WAN Manager サーバーのクラスタへの追加

Cisco vManage リリース 20.6.1 より前のリリースでクラスタに新しい Cisco SD-WAN Manager サーバーを追加するには、プライマリ Cisco SD-WAN Manager サーバーで次の手順を実行します。

はじめる前に、[Cisco Catalyst SD-WAN Manager サーバーのクラスタ IP アドレスの設定 \(292 ページ\)](#) で説明されているように、Cisco SD-WAN Manager サーバーのデフォルト IP アドレスがアウトオブバンド IP アドレスに変更されていることを確認してください。

1. Cisco SD-WAN Manager メニューから、**[Administration] > [Cluster Management]** の順に選択し、**[Service Configuration]** をクリックします。
2. **[マネージャの追加 (Add Manager)]** をクリックします。
[Edit Manager] ウィンドウが開きます。
3. **[Manager IP Address]** フィールドで、Cisco SD-WAN Manager サーバーに割り当てる IP アドレスを選択します。
4. Cisco SD-WAN Manager サーバーにログインするためのユーザー名とパスワードを入力します。
5. クラスタに追加する Cisco SD-WAN Manager サーバーの IP アドレスを入力します。
6. 新しい Cisco SD-WAN Manager サーバーのユーザー名とパスワードを指定します。
7. Cisco SD-WAN Manager サーバーで動作するサービスを選択します。次のリストからサービスを選択できます。**[Application Server]** フィールドは編集できないことに注意してください。Cisco SD-WAN Manager アプリケーションサーバーは、ローカルの Cisco SD-WAN Manager HTTP Web サーバーです。
 - 統計データベース：ネットワーク内のすべての Cisco Catalyst SD-WAN デバイスからの統計を保存します。
 - 構成データベース：ネットワーク内のすべての Cisco Catalyst SD-WAN デバイスについて、すべてのデバイスおよび機能テンプレートと構成を保存します。
 - メッセージングサーバー：メッセージを配信し、すべての Cisco SD-WAN Manager クラスタメンバー間で状態を共有します。
8. **[Add]** をクリックします。
追加した Cisco SD-WAN Manager サーバーは、クラスタに参加する前に再起動します。



- (注)
- クラスタでは、各サービスのインスタンスを少なくとも 3 つ実行することをお勧めします。
 - 最初の 2 つのコンピューティングノードまたはコンピューティング+データノードをクラスタに追加すると、ホストノードのアプリケーションサーバーは使用できなくなります。アプリケーションサーバーがホストノードでシャットダウンする前に、次のメッセージがホストノードの GUI に表示されます。
`\Node added to the cluster. The operation may take up to 30 minutes and may cause application-server to restart in between. Once the application server is back online, the post cluster operation progress can be viewed under tasks pop-up\`
 - Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以降、クラスタにノードを追加する前に、Cisco SD-WAN Manager 設定で [HTTP/HTTPS Proxy] オプションを無効にしてください。

Cisco vManage リリース 20.6.1 以降のリリースでの Cisco SD-WAN Manager サーバーのクラスタへの追加

Cisco vManage リリース 20.6.1 以降、クラスタは、次のどのノード展開もサポートします。

- 3 つの Compute+Data ノード
- 3 つの Compute+Data ノードと 3 つの Data ノード



- (注) データノードは、構成+データを持つ 3 ノードクラスタが追加された後にのみ追加する必要があります。

- 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 リリース 20.6.1 以降で Cisco SD-WAN Manager サーバーをクラスタに追加するには、次の手順を実行します。

この手順は、コンピューティング+データノードまたはコンピューティングノードで実行します。データノードは追加に必要なすべてのサービスを実行しないため、データノードでこの手順を実行することはサポートされません。

過去にクラスタのメンバーになり、その後クラスタから削除されたサーバーは追加しないでください。そのサーバーをクラスタに追加する必要がある場合は、そのサーバーで新しい VM を起動して、追加するノードとして使用します。

はじめる前に、[Cisco Catalyst SD-WAN Manager サーバーのクラスタ IP アドレスの設定 \(292 ページ\)](#) で説明されているように、Cisco SD-WAN Manager サーバーのデフォルト IP アドレスがアウトオブバンド IP アドレスに変更されていることを確認してください。この操作は、Cisco

SD-WAN Manager サーバーで 1 回だけ実行する必要があります。その後、同じ操作を使用して他のサーバーを追加してクラスタを形成します。

1. Cisco SD-WAN Manager メニューから、**[Administration] > [Cluster Management]** の順に選択します。

[Cluster Management page] ウィンドウが表示されます。このウィンドウのテーブルには、クラスタ内にある Cisco SD-WAN Manager サーバーが表示されます。

2. [マネージャの追加 (Add Manager)] をクリックします。

[Add Manager] ダイアログボックスが開きます。



- (注) [Edit Manager] ダイアログボックスが開いたら、[Cisco Catalyst SD-WAN Manager サーバーのクラスタ IP アドレスの設定 \(292 ページ\)](#) の説明に従ってサーバーのアウトオブバンド IP アドレスを設定し、サーバーを追加するためにこの手順を繰り返します。

3. [Add Manager] ダイアログボックスで、次のアクションを実行します。

1. サーバー用に設定されたペルソナに対応する [Node Persona] オプション ([Compute+Data]、[Compute]、または [Data]) をクリックします。

サーバーにログインし、**[Administration] > [Cluster Management]** ウィンドウのペルソナ表示を調べることで、サーバーのペルソナを判別できます。誤ったペルソナを選択すると、選択する必要があるペルソナがメッセージに表示されます。

2. [Manager IP Address] ドロップダウンリストから、クラスタに追加するサーバーの IP アドレスを選択します。

3. [Username] フィールドに、サーバーにログインするためのユーザー名を入力します。

4. [Password] フィールドに、サーバーにログインするためのパスワードを入力します。

5. (任意) シスコのソフトウェア定義型 Application Visibility and Control (SD-AVC) をサーバーで実行する場合は、[Enable SD-AVC] をクリックします。

Cisco SD-AVC は Cisco Application Visibility and Control (AVC) のコンポーネントです。これは、1 つの Cisco SD-WAN Manager サーバーで有効にできます。これを有効にするサーバーは、コンピューティング + データペルソナまたはコンピューティングペルソナを持つ必要があります。Cisco SD-AVC は、データペルソナを持つサーバーでは有効にできません。

サーバーの IP アドレスを変更したときにそのサーバーの Cisco SD-AVC を有効にした場合は、[Enable SD-AVC] チェックボックスがデフォルトでオンになります。

6. [Add] をクリックします。

7. 確定するには、[OK] をクリックします。

このダイアログボックスは、サービスが再開されることと、サーバーがクラスタに参加するときに不要な既存のメタデータおよびその他の情報がサーバーから削除されることを示しています。

[OK] をクリックすると、サーバー追加操作が開始されます。[Cluster Management] ウィンドウに、サーバーを追加するときにシステムが実行するタスクが表示されます。

この操作の一環として、システムは、追加するサーバーの互換性をチェックします。このチェックにより、サーバーに十分なディスク領域があることと、指定したペルソナがノードのペルソナと一致することが確認されます。

サーバーが追加されると、システムは、クラスタ同期操作を実行します。これにより、クラスタ内のサービスが再調整されます。その後、クラスタ内の Cisco SD-WAN Manager サーバーが再起動します。

Cisco Catalyst SD-WAN Manager サービスの詳細の表示

次のセクションでは、Cisco SD-WAN Manager サーバーで実行されているサービスに関する詳細情報を表示する方法と、Cisco SD-WAN Manager に接続されているデバイスを表示する方法について説明します。

サービスに関する詳細情報の表示

Cisco SD-WAN Manager サーバーで実行されているサービスに関する詳細情報を表示するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Administration] > [Cluster Management]** を選択し、**[Service Configuration]** をクリックします。
2. Cisco SD-WAN Manager サーバーのホスト名をクリックします。

[vManage Details] ウィンドウが開き、Cisco SD-WAN Manager で有効になっているすべての Cisco SD-WAN Manager サービスのプロセス ID が表示されます。

3. タイトルバーのトピックパス（パンくずリスト）で **[Cluster Management]** をクリックして、**[Cluster Management]** ウィンドウに戻ります。

Cisco SD-WAN Manager に接続されているデバイスの表示

Cisco SD-WAN Manager に接続されているデバイスのリストを表示するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Administration] > [Cluster Management]** を選択し、**[Service Configuration]** をクリックします。
2. Cisco SD-WAN Manager サーバーのホスト名をクリックします。
3. **[Managed Device]** をクリックします。

または、下記の手順も実行できます。

1. Cisco SD-WAN Manager メニューから、**[Administration]** > **[Cluster Management]** を選択し、**[Service Configuration]** をクリックします。
2. Cisco SD-WAN Manager サーバーの隣にある [...] をクリックし、**[Device Connected]** を選択します。
3. デバイスがクラスタから Cisco SD-WAN Manager に接続されている場合は、データストリームのホスト名を Cisco SD-WAN Manager のシステム IP アドレスに設定しないでください。ただし、VPN 512 の管理 IP アドレスまたは VPN 0 のインターネットパブリック IP アドレスは設定できます。データストリームのトラブルシューティングツールについては、[Data Stream Troubleshooting Tools FAQ](#) [英語] を参照してください。

Cisco Catalyst SD-WAN Manager パラメータの編集

クラスタに追加された Cisco SD-WAN Manager サーバーのさまざまなパラメータを編集できます。これを行うには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Administration]** > **[Cluster Management]** の順に選択し、**[Service Configuration]** をクリックします。
2. 編集する Cisco SD-WAN Manager サーバーの横にある [...] をクリックし、**[Edit]** をクリックします。
[Edit vManage] ウィンドウが開きます。
3. 編集する IP アドレスを選択します。
4. ユーザー名とパスワードを入力し、選択した Cisco SD-WAN Manager サーバーのパラメータを編集します。
 - Cisco vManage リリース 20.6.1 より前のリリースでは、クラスタサービスを編集できません。
 - Cisco vManage リリース 20.6.1 から、IP アドレスを [vManage IP Address] ドロップダウンリストに表示される別の IP アドレスに変更したり、Cisco SD-AVC 設定を変更したり、サーバーログイン情報が変更された場合にユーザー名とパスワードを変更することができます。
5. **[Update]** をクリックします。

設定データベースのログイン情報の更新

設定データベースのデフォルトのユーザー名は **neo4j**、デフォルトのパスワードは **password** です。設定データベースのデフォルトのログイン資格情報を更新するには、端末を使用して Cisco SD-WAN Manager にアクセスし、次のコマンドを実行します。これらのコマンドを実行するた

めに Cisco SD-WAN Manager で SSH 端末オプションを使用しないでください。これを行うと、Cisco SD-WAN Manager にアクセスできなくなります。

1. configuration-db が有効かどうかにかかわらず、**request nms application-server stop** を使用してすべての Cisco SD-WAN Manager サーバーでアプリケーションサーバーを停止します。
2. 次のいずれかのコマンドを使用して、すべての Cisco SD-WAN Manager サーバーの設定データベースのユーザー名とパスワードをリセットします。

- Cisco SD-WAN リリース 20.1.1 以前の場合：

```
request nms configuration-db update-admin-user username username password password  
newusername newadminuser newpassword newpassword
```

- Cisco SD-WAN リリース 20.1.2 以降のリリースの場合：

```
request nms configuration-db update-admin-user
```

プロンプトが表示されたら、現在のユーザー名とパスワード、および新しいユーザー名とパスワードを入力します。

これらのコマンドのいずれかを実行すると、Cisco SD-WAN Manager がアプリケーションサーバーを再起動します。



(注)

- 設定データベースのデフォルトの資格情報がわからない場合は、シスコのサポート担当者に連絡して資格情報を取得してください。
- 以前のユーザー名は使用できません。
- パスワードには、A～Z の文字（大文字または小文字）、0～9 の数字、@、#、および * の特殊文字の組み合わせのみを使用できます。

例

- Cisco SD-WAN リリース 20.1.1 以前の場合：

```
request nms configuration-db update-admin-user username neo4j  
password ***** newusername myusername newpassword mypassword
```

- Cisco SD-WAN リリース 20.1.2 以降のリリースの場合：

```
request nms configuration-db update-admin-user
```

```
Enter current user name: neo4j
```

```
Enter current user password: password
```

```
Enter new user name: myusername
```

```
Enter new user password: mypassword
```



- (注) 設定データベースの管理者ユーザーの更新後、特定の Cisco SD-WAN Manager インスタンスを表示できない場合は、**request nms application-server restart** コマンドを使用して、その Cisco SD-WAN Manager インスタンスでアプリケーションサーバーを再起動します。



- (注) Cisco SD-WAN リリース 20.6.1 以降では、**request nms configuration-db update-admin-user** コマンドを使用して管理者ユーザークレデンシャルを更新するときに、Cisco SD-WAN Manager クラスタ内のすべてのノードで同じ入力（古いユーザー名、パスワード、および新しいユーザー名、パスワード）を指定します。一度に 1 ノードずつ **request nms configuration-db update-admin-user** コマンドを実行する必要があります。新しい設定を有効にするために NMS サービスが再起動されるため、CLI をすべてのノードに同時にプッシュしないことをお勧めします。

Cisco Catalyst SD-WAN Manager のダウングレード

Cisco SD-WAN Manager から、または CLI コマンドを使用して Cisco SD-WAN Manager をダウングレードする（現在のバージョンよりも古いバージョンの Cisco SD-WAN Manager をインストールする）ことはできません。



- (注) この制限は、単一の Cisco SD-WAN Manager インスタンスと Cisco SD-WAN Manager クラスタに適用されます。この制限は、ネットワークデバイスでのソフトウェアのアップグレードまたはダウングレードには関係ありません。

Cisco SD-WAN Manager のバージョンをダウングレードするには、シスコのサポート担当者に連絡してください。

Cisco SD-WAN Manager クラスタのアップグレード

表 34: 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN Manager クラスタのアップグレード	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a	この機能は、クラスタ内の Cisco SD-WAN Manager サーバーのアップグレード手順の概要を示しています。
	Cisco SD-WAN リリース 20.3.1	
	Cisco vManage リリース 20.3.1	

機能名	リリース情報	説明
データベーススキーマ違反の確認	Cisco Catalyst SD-WAN Manager リリース 20.13.1	構成データベースにスキーマ違反があるかどうかを示すように、 request nms application-server status コマンドを更新しました。クラスタをアップグレードする前に違反を確認できます。
Cisco SD-WAN Manager クラスタのアップグレード互換性チェック	Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a Cisco Catalyst SD-WAN Manager リリース 20.14.1	この機能は、Cisco SD-WAN Manager クラスタのアップグレードに役立ち、アップグレード前のソフトウェア互換性チェックとアップグレード後のチェックを実行して、アップグレードが正常に行われるようにします。この機能は、アップグレードが正常に行われることを支援し、アップグレードが失敗した場合の問題のトラブルシューティングに役立ちます。

クラスタのアップグレードに関する情報

ここでは、クラスタ内の Cisco SD-WAN Manager をアップグレードする方法について説明します。

Cisco vManage 20.3.1 以降のリリースから Cisco vManage リリース 20.6.1 に直接アップグレードできます。それ以前のリリースからアップグレードするには、最初に Cisco vManage 20.4.2 または Cisco vManage リリース 20.5.1 にアップグレードしてください。

Cisco SD-WAN Manager クラスタ展開を Cisco vManage リリース 20.3.1 以降から Cisco vManage リリース 20.5.1 以降にアップグレードする場合は、CLI を使用して行う必要があります。

6 ノード Cisco SD-WAN Manager クラスタ展開（すべてのノードですべてのサービスが実行されているわけではない）から Cisco vManage リリース 20.6.1 以降のリリースにアップグレードする場合は、アップグレードを実行する前に、シスコのサポート担当者に連絡してください。

アップグレード前のソフトウェア互換性の確認

（サポート対象の最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.14.1）

クラスタ展開では、設定データベース、調整サービス、メッセージングサービスなどの Cisco SD-WAN Manager サービスはクラスタモードで動作します。

CLI 方式ではなく、Cisco SD-WAN Manager を使用してクラスタのアップグレードを実行することをお勧めします。Cisco SD-WAN Manager は、アップグレードを続行する前に、重要なアップグレード前チェックを実行します。アップグレード前のチェックには、証明書の有効期限、設定データベース、CPU、ディスク、メモリ、および調整サービスやメッセージングサービスなどのサービスのステータスなどの項目が含まれます。クラスタのアップグレードの準備ができていない場合は、Cisco SD-WAN Manager から通知されます。

アップグレード後、Cisco SD-WAN Manager はアップグレード後チェックを実行します。これには、アップグレードが成功したことを確認するためのサービスの機能のチェックが含まれます。アップグレードが失敗した場合は、Cisco SD-WAN Manager を使用してトラブルシューティングを行い、アップグレードを再度実行できます。

クラスタのアップグレードの進行中、特定の時点で、クラスタ内の一部のノードは古いソフトウェアリリースを実行し続け、他のノードは新しいリリースにアップグレードされます。その結果、アップグレード中に、古いリリースと新しいリリースのサービス間に非互換性が存在し、正常に機能しなくなる可能性があります。

Cisco SD-WAN Manager を使用して Cisco SD-WAN Manager クラスタをアップグレードする方法については、『Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide』の「[Software Upgrade](#)」セクションを参照してください。

暗号化 (Encryption)

サポート対象の最小リリース : Cisco Catalyst SD-WAN Manager リリース 20.14.1

Cisco SD-WAN Manager を使用した Cisco Catalyst SD-WAN Manager リリース 20.13.1 から Cisco Catalyst SD-WAN Manager リリース 20.14.1 へのマルチテナントクラスタのアップグレードでは、暗号化キーが原因でアップグレードコーディネータが失敗することがあります。アップグレード コーディネータ サービスは、暗号化キーを使用してサービスクレデンシャルを暗号化します。

サービスクレデンシャルを再暗号化するには、Cisco SD-WAN Manager を再起動し、ソフトウェアのアクティベーションをトリガーします。

クラスタのアップグレードの前提条件

Cisco SD-WAN Manager ノードを Cisco vManage リリース 20.6.1 以降のリリースにアップグレードする前に、次のことを確認してください。

- アップグレードするサーバーの内部ユーザーアカウント `vmanage-admin` がロックされていないことを確認します。

サーバーに接続されているデバイスにテンプレートをプッシュすることで、この管理者アカウントのステータスを確認できます。アカウントがロックされている場合、プッシュは失敗します。このようなシナリオでは、`request aaa unlock-user vmanage-admin` コマンドを使用してアカウントのロックを解除できます。

- アップグレードするサーバー間で PKI キーが交換されていることを確認します。

これを行うには、サーバー上で制御接続が UP 状態であることを確認し、アプリケーションサーバーを再起動します。

- 各サーバーの帯域外 IP アドレスに到達できることを確認します。
- クラスタ内のすべてのサーバーで Cisco SD-WAN Manager にアクセスできることを確認します。
- DCA がクラスタ内のすべてのサーバーで実行されていることを確認します。

これを行うには、**request nms data-collection-agent status** コマンドを使用して、各ノードのステータス値が **running** と表示されていることを確認します。

DCA を起動するには、必要に応じて **request nms data-collection-agent start** コマンドを使用します。

- (サポートされる最小リリース : Cisco Catalyst SD-WAN Manager リリース 20.13.1) **request nms application-server status** コマンドを使用して、構成データベースにスキーマ違反がないことを確認します。コマンドの出力に違反が示されている場合は、シスコカスタマーサポートに連絡して問題を解決してください。
- Cisco Catalyst SD-WAN Manager リリース 20.12.3 以降、コンピューティングとデータのチェックは、ディザスタリカバリ (DR) のレプリケーションが機能するための前提条件です。DR レプリケーション用に 3 つのコンピューティングノードと 3 つのデータノードを実行している場合、DR はサポートされません。

これらの前提条件が満たされていない場合、またはアップグレード中に別のエラーが発生した場合、イメージのアクティブ化は失敗し、**upgrade-context.json** という名前のファイルがクラスタ内の各ノードの **/opt/data/extra-packages/ image-version** フォルダに作成されます。このファイルをシスコの担当者に提供して、問題の解決に役立てることができます。

CLI を使用したクラスタのアップグレード

1. すべての Cisco SD-WAN Manager サーバーのスナップショットを作成します。次のコマンドを使用して設定データベースのバックアップを取り、Cisco SD-WAN Manager サーバーの外部の場所に保存します。

request nms configuration-db backup path_and_filename

2. Cisco vManage リリース 18.3 以降がインストールされていることを確認します。
3. Cisco vManage リリース 20.3.1 以降からのアップグレードの場合は、現在のイメージをクラスタ内の各 Cisco SD-WAN Manager サーバーにコピーし、次のコマンドを使用して各 Cisco SD-WAN Manager サーバーにイメージをインストールします。この時点ではイメージをアクティブにしないでください。

request software install path



- (注) Cisco SD-WAN Manager へのコピーは、VPN 512 インターフェイスを使用して CLI で SCP を使用して実行できます。

4. Cisco vManage リリース 20.3.1 以降からのアップグレードの場合は、次のコマンドを使用して、各 Cisco SD-WAN Manager サーバーで現在のイメージをアクティブ化します。すべてのサーバーが同時に再起動します。

request software activate version

5. 次のいずれかからアップグレードする場合は、設定データベースをアップグレードする必要があります。
 - Cisco vManage リリース 18.4.x または 19.2.x から Cisco vManage 20.3.x または 20.4.x
 - Cisco vManage リリース 20.3.x または 20.4.x から Cisco vManage リリース 20.5.x または 20.6.x
 - Cisco SD-WAN Manager リリースから Cisco vManage リリース 20.10.1 以降



- (注) • Cisco vManage リリース 20.1.1 以降では、設定データベースをアップグレードする前に、データベースのサイズを確認してください。データベースのサイズは 5 GB 以下にすることを推奨します。データベースのサイズを確認するには、次の診断コマンドを使用します。

request nms configuration-db diagnostics

- 設定データベースをアップグレードするときは、前の手順で説明したように、クラスタ内の各 Cisco SD-WAN Manager サーバーで現在のイメージをアクティブ化したことを確認してください。さらに、各サーバーで **request nms all status** コマンドを入力して、アプリケーションサーバーと設定データベースサービスを除くすべてのサービスがこれらのサーバーで実行されていることを確認します。

設定データベースをアップグレードするには、次の手順を実行します。

1. アップグレードするノードを決定するには、各ノードで **request nms configuration-db status** コマンドを入力します。出力で次を探します。

```
Enabled: true
Status: not running
```



- (注) Cisco SD-WAN Manager ホストサーバーで新しいイメージをアクティブ化すると、サーバーが再起動します。再起動後の約 30 分間、NMS サービスがコンテナ化された形式に移行している間は、設定データベースが有効になっているノードでも、**request nms configuration-db status** コマンドの出力が **Enabled: false** と表示されます。

2. 前の手順で決定したアップグレード対象のノードで、次のように入力します。

```
request nms configuration-db upgrade
```



- (注)
- このコマンドは1つのノードでのみ入力してください。
 - Cisco vManage Release 20.5.x から Cisco vManage リリース 20.6.1 以降にアップグレードする場合は、このコマンドを入力しないでください。

6. プロンプトが表示されたらログインクレデンシャルを入力します。ログインクレデンシャルが求められるのは、Cisco vManage リリース 20.3.1 よりも前のリリースですべての Cisco SD-WAN Manager サーバーが相互に制御接続を確立する場合です。アップグレードが成功すると、すべての設定データベースのサービスがクラスタ全体で稼働状態となり、アプリケーションサーバーが起動します。

データベース アップグレード ログは `vmanage-server :/var/log/nms/neo4j-upgrade.log` で確認できます。

Cisco Catalyst SD-WAN Manager プロセスの手動再起動

クラスタが誤動作しており、再起動が必要な場合は、Cisco SD-WAN Manager プロセスを手動で再起動できます。次のいずれかを実行します。

- (Cisco vManage リリース 20.6.1 以降) `request nms all restart` コマンドを使用して、すべてのプロセスを再起動します。
- (Cisco vManage リリース 20.6.1 より前のリリース) 次の手順を使用して、一度に1つずつ順番にプロセスを再開します。手動再起動の順序は、クラスタ内の Cisco SD-WAN Manager インスタンスで実行しているサービスに応じて、クラスタによって異なる場合があります。次の順序は、3つの Cisco SD-WAN Manager デバイスを持つ基本的なクラスタに基づいています。

1. 各 Cisco SD-WAN Manager デバイスで、すべての NMS サービスを停止します。

```
request nms all stop
```

2. すべてのサービスが停止したことを確認します。**request nms all stop** コマンドの場合、通常、時間がかかりすぎるとサービスの停止に失敗したことを示すメッセージを表示されるため、次のコマンドを使用して、次に進む前にすべてのサービスが停止していることを確認します。

```
request nms all status
```

3. 統計データベースを実行するように設定された各デバイスで統計データベースを開始します。毎回サービスが開始されるのを待ってから、次の Cisco SD-WAN Manager デバイスに進みます。

```
request nms statistics-db start
```

4. 次の Cisco SD-WAN Manager でサービスを開始する前に、そのサービスが開始されていることを確認します。サービスが開始したら、手順 3 を実行して、次の Cisco SD-WAN Manager デバイスで統計データベースを開始します。すべての Cisco SD-WAN Manager デバイスで統計データベースが実行されたら、次の手順に進みます。

```
request nms statistics-db status
```

5. 構成データベースを実行するように設定されている各デバイスで構成データベースを開始します。毎回サービスが開始されるのを待ってから、次の Cisco SD-WAN Manager デバイスに進みます。

```
request nms configuration-db start
```

6. Cisco vManage リリース 20.3.1 より前のリリースの場合、次の Cisco SD-WAN Manager デバイスで開始する前に、そのサービスが開始されていることを確認してください。vshell に移動し、ログファイルを追跡して、データベースがオンラインであるというメッセージを探します。確認後、手順 5 に進み、次の Cisco SD-WAN Manager デバイスで構成データベースを開始します。すべての Cisco SD-WAN Manager デバイスで構成データベースが実行されたら、次の手順に進みます。

```
tail -f -n 100 /var/log/nms/vmanage-neo4j-out.log
```

7. 各デバイスで調整サーバーを起動します。毎回サービスが開始されるのを待ってから、次の Cisco SD-WAN Manager デバイスに進みます。

```
request nms coordination-server start
```

8. 次の Cisco SD-WAN Manager デバイスでサービスを開始する前に、そのサービスが開始されていることを確認します。確認後、手順 7 に進み、次の Cisco SD-WAN Manager デバイスで調整サーバーを起動します。すべての Cisco SD-WAN Manager デバイスで調整サーバーが実行されたら、次の手順に進みます。

```
request nms coordination-server status
```

9. 各デバイスでメッセージングサーバーを起動します。毎回サービスが開始されるのを待ってから、次の Cisco SD-WAN Manager デバイスに進みます。

```
request nms messaging-server start
```

10. 次の Cisco SD-WAN Manager デバイスでサービスを開始する前に、そのサービスが開始されていることを確認します。確認したら、手順 9 に進み、次の Cisco SD-WAN Manager デバイスでメッセージングサーバーを起動します。すべての Cisco SD-WAN Manager デバイスでメッセージングサーバーが実行されたら、次の手順に進みます。

```
request nms messaging-server status
```

11. 各デバイスでアプリケーションサーバーを起動します。毎回サービスが開始されるのを待ってから、次の Cisco SD-WAN Manager デバイスに進みます。

```
request nms application-server start
```

12. Cisco vManage リリース 20.3.1 以降のリリースでは、各 Cisco SD-WAN Manager デバイスでサーバープロキシサービスを開始します。

```
request nms server-proxy start
```

サービスが完全に開始されたことを確認するには、その Cisco SD-WAN Manager デバイスの GUI を開きます。GUI が完全にロードされ、ログイン可能になったら、次の Cisco SD-WAN Manager デバイスでサーバープロキシサービスを開始します。

13. 各デバイスで NMS クラウドサービスを再起動します。毎回サービスが開始されるのを待ってから、次の Cisco SD-WAN Manager デバイスに進みます。

次のコマンドを入力して、クラウドサービスが実行されていることを確認できます。

```
request nms cloud-agent status
request nms cloud-agent-v2 status
```

次の Cisco SD-WAN Manager デバイスでサービスを開始する前に、そのサービスが開始されていることを確認します。確認後、次の Cisco SD-WAN Manager デバイスでクラウドサービスを開始します。すべての Cisco SD-WAN Manager デバイスでクラウドサービスが実行されたら、次の手順に進みます。

14. エラーがなく、すべてが正常にロードされたことを確認するには、ログファイルを追跡します。

Cisco vManage リリース 20.6.1 以降にアップグレードするときに問題が発生した場合は、シスコのサポート担当者に連絡して支援を受けてください。



- (注) Cisco SD-WAN Manager デバイスを再起動する必要がある場合、またはアップグレード後は、常にこのセクションの説明に従い、サービスを手動で起動することを検討してください。

Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a から、[device-data-collector] サービスコンテナが追加されます。以下は、コマンド [request nms device-data-collector] の出力例です。

```
Device# request nms device-data-collector
Possible completions:
diagnostics    Run diagnostics on NMS component
jcmd           Run jcmd on NMS component
restart        Restart NMS component
start          Start NMS component
status         Status of NMS component
stop           Stop NMS component
```

クラスタからの Cisco Catalyst SD-WAN Manager ノードの削除

必要に応じて、クラスタから Cisco SD-WAN Manager ノードを削除できます。

Cisco vManage リリース 20.6.1 より前のリリースでは、n の Cisco SD-WAN Manager ノードのクラスタからは n-2 のノードしか削除できません。クラスタ内に少なくとも 2 つの Cisco SD-WAN Manager ノードを保持する必要があります。

Cisco vManage リリース 20.6.1 以降では、コンピューティング機能を含む少なくとも 2 つの Cisco SD-WAN Manager ノードと、データ機能を含む少なくとも 1 つのノードを保持する必要があります。つまり、クラスタは次のいずれかを保持する必要があります。

- コンピューティング + データペルソナを含む少なくとも 2 つの Cisco SD-WAN Manager ノード
- コンピューティング + データペルソナを含む少なくとも 1 つの Cisco SD-WAN Manager ノードとコンピューティングペルソナを含む 1 つの Cisco SD-WAN Manager ノード
- コンピューティングペルソナを含む少なくとも 2 つの Cisco SD-WAN Manager ノードとデータペルソナを含む 1 つの Cisco SD-WAN Manager ノード

Cisco vManage リリース 20.6.1 以降では、Cisco SD-WAN Manager ノードをクラスタから削除したときにそのノードが到達可能である場合、Cisco SD-WAN Manager は、削除されたノードで工場出荷時設定へのリセット操作を自動的に実行するため、ノードが再びクラスタに参加することはありません。Cisco SD-WAN Manager ノードをクラスタから削除したときにそのノードが到達可能ではない場合、そのノードでは工場出荷時設定へのリセット操作は実行されません。この場合、そのノードは、到達可能になると、自動的にクラスタに戻されます。ノードがクラスタに再び戻されないようにするには、ノードがクラスタから削除された後に、そのノードの CLI から **request software reset** コマンドを入力します。

クラスタから Cisco SD-WAN Manager ノードを削除するには、次の手順を実行します。

1. Cisco SD-WAN Manager から、**[Administration] > [Cluster Management]** の順に選択し、**[Service Configuration]** をクリックします。
2. 削除する Cisco SD-WAN Manager インスタンスの横にある [...] をクリックし、**[Remove]** をクリックします。

[Remove Manager] ダイアログボックスが開きます。
3. ユーザー名とパスワードを入力して、ネットワークからデバイスを削除することを確認します。
4. **[Remove]** をクリックします。

Cisco SD-WAN Manager インスタンスがクラスタから削除され、その Cisco SD-WAN Manager の証明書が削除されて、Cisco SD-WAN Manager が工場出荷時設定にリセットされます。



第 9 章

証明書管理

- Cisco Catalyst SD-WAN Manager での証明書の管理 (311 ページ)
- Cisco SD-WAN Manager を使用した Cisco IOS XE Catalyst SD-WAN デバイス へのサードパーティ CA 証明書の設定 (322 ページ)
- Cisco SD-WAN Manager を使用した CA 証明書の設定に関する情報 (322 ページ)
- CA 証明書のアップロードでサポートされるデバイス (323 ページ)
- CA 証明書を設定するための前提条件 (323 ページ)
- CA 証明書のアップロードの制約事項 (323 ページ)
- CA 証明書のアップロード (323 ページ)
- Cisco SD-WAN Manager を使用した CA 証明書の設定 (324 ページ)
- CA 証明書と PKI トラストポイントの監視 (326 ページ)
- CRLベースの検疫 (327 ページ)
- Cisco Catalyst SD-WAN Manager でのルート認証局証明書の管理 (329 ページ)
- エンタープライズ証明書 (330 ページ)
- Cisco PKI コントローラの証明書 (340 ページ)
- Cisco SD-WAN Manager の Web サーバー証明書 (348 ページ)

Cisco Catalyst SD-WAN Manager での証明書の管理

[Configuration] > [Certificates] ページで Cisco SD-WAN Manager の証明書操作を実行します。

- トップバー：左側には、Cisco SD-WAN Manager メニューを展開および折りたたむためのメニューアイコン、および Cisco SD-WAN Manager 製品名が表示されます。右側には、多くのアイコンとユーザープロファイルのドロップダウンがあります。
- タイトルバー：画面のタイトルである証明書を含みます。
- [WAN Edge List] タブ：オーバーレイネットワークのコントローラにルータ認定シリアル番号ファイルをインストールし、ファイル内のシリアル番号を管理します。[Certificates] 画面を最初に開いたときには、[WAN Edge List] タブが選択されています。
 - [Send to Controllers]：WAN エッジルータシャーシ番号とシリアル番号をネットワーク内のコントローラに送信します。

- [Table of WAN edge routers in the overlay network] : 列を再配置するには、列のタイトルを目的の位置にドラッグします。
- [Controllers] タブ : 証明書をインストールし、デバイスのシリアル番号を Cisco SD-WAN Validator にダウンロードします。



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

- [Send to Cisco SD-WAN Validator] : コントローラのシリアル番号を Cisco SD-WAN Validator に送信します。
- [Install Certificate] : コントローラデバイスに署名付き証明書をインストールします。このボタンは、[Administration] > [Settings] > [Certificate Signing by Symantec] で [Manual] を選択した場合のみ使用できます。
- [Export Root Certificate] : ファイルにダウンロードできるコントローラデバイスのルート証明書のコピーを表示します。
- [Table of controller devices in the overlay network] : 列を再配置するには、列のタイトルを目的の位置にドラッグします。
- [Certificate] ステータスバー : このバーは画面の下部にあり、[Administration] > [Settings] > [Certificate Authorization] で [Server Automated] を選択した場合のみ表示されます。証明書のインストールプロセスの状態が表示されます。
 - Device Added
 - CSR の作成
 - 証明書を待機中
 - コントローラに送信

緑色のチェックマークは、ステップが完了したことを示します。灰色のチェックマークは、ステップがまだ実行されていないことを示します。

- 検索ボックス : [Contains] または [Match] 文字列の [Search Options] ドロップダウンが含まれています。
- [Refresh] アイコン : クリックすると、デバイステーブルのデータが最新のデータで更新されます。
- [Export] アイコン : クリックして、すべてのデータを CSV 形式でファイルにダウンロードします。

- [Show Table Fields] アイコン：アイコンをクリックして、デバイステーブルの列を表示または非表示にします。デフォルトでは、すべての列が表示されます。

WAN Edge ルータ証明書ステータスの確認

[WAN Edge List] タブで、[Validate] 列を確認します。ステータスは、次のいずれかになります。

- [Valid]（緑色で表示）：ルータの証明書は有効です。
- [Staging]（黄色で表示）：ルータはステージング状態です。
- [Invalid]（赤色で表示）：ルータの証明書は無効です。

WAN Edge ルータの検証

[Configuration] > [Devices] 画面を使用して Cisco vEdge デバイス と WAN ルータをネットワークに追加する際、[Validate the uploaded WAN Edge List and send to controllers] チェックボックスをクリックすることにより、ルータを自動的に検証し、そのシャシ番号とシリアル番号をコントローラデバイスに送信することができます。このオプションをオンにしない場合は、各ルータを個別に検証し、そのシャシ番号とシリアル番号をコントローラデバイスに送信する必要があります。次の手順を実行します。

1. [WAN Edge List] タブで、検証するルータを選択します。
2. [Validate] 列で、[Valid] をクリックします。
3. [OK] をクリックして、有効な状態への移行を確認します。
4. 検証するルータごとに上記の手順を繰り返します。
5. 画面の左上隅にある [Send to Controllers] ボタンをクリックして、検証済みルータのシャシ番号とシリアル番号をネットワーク内のコントローラデバイスに送信します。Cisco SD-WAN Manager NMS は、プッシュ操作のステータスを示す [Push WAN Edge List] 画面を表示します。

WAN エッジルータのステージング

WAN エッジルータを最初に起動して設定する場合、Cisco SD-WAN Manager インスタンスを使用してステージング状態にできます。ルータがステージングの状態の場合、ルータを設定し、ルータが Cisco SD-WAN コントローラ および Cisco SD-WAN Manager インスタンスとの動作可能な接続を確立できることをテストできます。

ルータを実稼働サイトに物理的に配置した後、ルータの状態をステージングから有効に変更します。ルータが実稼働ネットワークに参加するのは、この時点でのみです。ルータをステージングするには、次の手順を実行します。

1. [WAN Edge List] タブで、ステージングするルータを選択します。

2. [Validate] 列で、[Staging] をクリックします。
3. [OK] をクリックして、ステージング状態への移行を確認します。
4. 画面の左上隅にある [Send to Controllers] をクリックして、WAN エッジ認証シリアル番号ファイルをコントローラと同期します。Cisco SD-WAN Manager NMS は、プッシュ操作のステータスを示す [Push WAN Edge List] 画面を表示します。
5. ステージングを解除するには、WAN エッジルータを検証します。

WAN エッジルータの無効化

1. [WAN Edge List] タブで、無効にするルータを選択します。
2. [Validate] 列で、[Invalid] をクリックします。
3. [OK] をクリックして、無効な状態への移行を確認します。
4. 無効にするルータごとに上記の手順を繰り返します。
5. 画面の左上隅にある [Send to Controllers] ボタンをクリックして、検証済みルータのシャーシとシリアル番号をネットワーク内のコントローラデバイスに送信します。Cisco SD-WAN Manager インスタンスは、プッシュ操作のステータスを示す [Push WAN Edge List] 画面を表示します。

コントローラのシリアル番号を Cisco Catalyst SD-WAN Validator に送信する

Cisco SD-WAN Validator は、オーバーレイネットワーク内の有効なコントローラを判別するために、コントローラのシリアル番号のリストを保持しています。Cisco SD-WAN Manager インスタンスは、証明書生成プロセス中にこれらのシリアル番号を学習します。

コントローラのシリアル番号を Cisco SD-WAN Validator に送信するには、次の手順を実行します。

1. [Controllers] タブで、画面の下部にある証明書ステータスバーを確認します。[Send to Controllers] チェックマークが緑色の場合、すべてのシリアル番号はすでに Cisco SD-WAN Validator に送信されています。灰色の場合は、1 つ以上のシリアル番号を Cisco SD-WAN Validator に送信できます。



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

2. [Controllers] タブの [Send to Validator] ボタンをクリックします。コントローラのシリアル番号と検証済みルータの UUID が Cisco SD-WAN Validator に送信されます。すべてのシリ

アル番号が送信済みの場合、[Send to Validator] をクリックすると、エラーメッセージが表示されます。コントローラのシリアル番号を再送信するには、最初にデバイスを選択してから、[Validity] 列で [Invalid] を選択する必要があります。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.14.x 以前では、[Controllers] タブで [Send to Validator] ボタンをクリックすると、コントローラのシリアル番号のみが Cisco SD-WAN Validator に 1 回送信されます。

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

シリアル番号が送信されたら、Cisco SD-WAN Manager ツールバーの [Tasks] アイコンをクリックして、ファイルのダウンロードおよびその他の最近のアクティビティのログを表示します。

署名付き証明書のインストール

[Administration] > [Settings] > [Certificate Signing by Symantec] で、証明書生成プロセスに [Manual] オプションを選択した場合は、[Install Certificate] ボタンを使用して、コントローラデバイスに証明書を手動でインストールします。

Symantec またはエンタープライズルート CA は、証明書に署名すると、個別の署名済み証明書を含むファイルを返します。それらをローカルネットワーク内のサーバーに配置します。その後、それらを各コントローラにインストールします。

1. [Controllers] タブの [Install Certificate] をクリックします。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

2. [Install Certificate] ウィンドウで、ファイルを選択するか、証明書のテキストをコピーして貼り付けます。
3. [Install] をクリックしてデバイスに証明書をインストールします。証明書にはコントローラを識別する情報が含まれているため、証明書をインストールするデバイスを選択する必要はありません。
4. 上記の手順を繰り返して、追加の証明書をインストールします。

ルート証明書のエクスポート

1. [Controllers] タブで、[Export Root Certificate] ボタンをクリックします。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。
2. [Export Root Certificate] ウィンドウで、[Download] をクリックしてルート証明書をファイルにエクスポートします。
 3. [閉じる (Close)] をクリックします。

証明書署名要求の表示

1. [WAN Edge List] または [Controllers] タブで、デバイスを選択します。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。
2. 行の右側にある [More Actions] アイコンをクリックし、[View CSR] をクリックして証明書署名要求 (CSR) を表示します。

デバイス証明書署名要求の表示

1. [WAN Edge List] または [Controllers] タブで、Cisco IOS XE Catalyst SD-WAN デバイス を選択します。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。
2. 行の右側にある [More Actions] アイコンをクリックし、[View Device CSR] をクリックして証明書署名要求 (CSR) を表示します。
 トラストポイントが設定されている Cisco IOS XE Catalyst SD-WAN デバイス の場合は、[More Actions] アイコンをクリックすると、次の 3 つのオプションを表示できます。
 - [View Device CSR]
 - [Generate Feature CSR]
 - [View Feature CSR]



- (注) Cisco SD-WAN Manager は、デバイス証明書が Cisco SD-WAN Manager を介してインストールされている場合にのみアラームを生成します。証明書を手動でインストールした場合、Cisco SD-WAN Manager は証明書の期限切れのアラームを生成しません。

証明書の表示

1. [Controllers] タブで、デバイスを選択します。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。
2. 行の右側にある [More Actions] アイコンをクリックし、[View Certificate] をクリックします。

証明書署名要求の生成

以下の手順では、CSR の生成プロセスについて説明します。

コントローラ証明書署名要求の生成

1. Cisco SD-WAN Manager メニューから **[Configuration] > [Certificates]** の順に選択します。
2. [Controllers] をクリックします。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。
3. 目的のコントローラについて、[...] をクリックし、[Generate CSR] を選択します。
[Generate CSR] ウィンドウが表示されます。
 4. [Generate CSR] ウィンドウで、[Download] をクリックしてファイルをローカル PC（つまり、Cisco SD-WAN Manager NMS への接続に使用している PC）にダウンロードします。
 5. 上記の手順を繰り返して、別のコントローラの CSR を生成します。

機能証明書署名要求の生成

1. Cisco SD-WAN Manager のメニューから **[Configuration] > [Certificates]** の順に選択します。

2. [WAN Edge List] をクリックします。
3. 目的のデバイスで [...] をクリックし、[Generate Feature CSR] を選択します。
[Generate Feature CSR] ウィンドウが表示されます。
4. [Generate Feature CSR] ウィンドウで、[OK] をクリックして、機能 CSR の生成を続行します。この手順では、設定されているデバイスのトラストポイントを認証し、デバイスから CSR を抽出します。
5. CSR を生成するデバイスごとに、上記の手順を繰り返します。

WAN エッジデバイス証明書署名要求の生成

1. Cisco SD-WAN Manager のメニューから[Configuration] > [Certificates]の順に選択します。
2. [WAN Edge List] をクリックします。
3. 目的のデバイスで [...] をクリックし、[Renew Device CSR] を選択します。
[Renew Device CSR] ウィンドウが表示されます。
4. [Renew Device CSR] ウィンドウで、[OK] をクリックして新しいCSRの生成を続行します。



(注) Cisco vManage リリース 20.9.1 以降のリリース：[Renew Device CSR] をクリックすると、RSA 秘密キーと公開キーがリセットされ、新しいキーペアを使用する CSR が生成されます。また、Cisco SD-WAN Manager は Cisco vManage リリース 20.6.4 および以降の Cisco vManage 20.6.x リリースで新しい CSR を生成する前に、RSA 秘密キーと公開キーをリセットします。

前述のリリース以外の Cisco SD-WAN Manager リリース：[Renew Device CSR] をクリックすると、既存のキーペアを使用して CSR が生成されます。

RSA キーペアのリセット

1. [Controllers] タブで、デバイスを選択します。



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

2. 行の右側にある [More Actions] アイコンをクリックし、[Reset RSA] をクリックします。
3. [OK] をクリックしてデバイスの RSA キーのリセットを確認し、新しい公開キーまたは秘密キーで新しい CSR を生成します。

制御コンポーネントの無効化

ファブリック内の最後に残っている Cisco SD-WAN Validator または Cisco SD-WAN コントローラ を無効にすると、Cisco SD-WAN Manager はコンポーネントを無効にするメンテナンス期間を設定するように求めます。現在時刻から 5 分以上の時間を設定します。

手順

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Certificates] > [Control Components]** の順に選択します。
2. **[Control Components]** タブで、Cisco SD-WAN 制御コンポーネント インスタンスを選択します。

Cisco Catalyst SD-WAN Manager リリース 20.13.1 より前のリリースでは、このタブは**コントローラ**と呼ばれています。

3. Cisco SD-WAN 制御コンポーネント インスタンスの隣の **[...]** をクリックし、**[Invalidate]** を選択します。

認定アクティビティログの表示

証明書関連のアクティビティのステータスを表示するには、次の手順を実行します。

1. Cisco SD-WAN Manager ツールバーにある **[Task]** アイコンをクリックします。Cisco SD-WAN Manager NMS には、すべての実行中タスクのリストと、成功と失敗の合計数が表示されます。
2. 行をクリックして、タスクの詳細情報を表示します。Cisco SD-WAN Manager NMS 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。

署名付き証明書の表示

署名付き証明書は、オーバーレイネットワーク内の Cisco SD-WAN デバイスの認証に使用されます。Cisco SD-WAN Manager を使用して署名付き証明書の内容を表示するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから **[Configuration] > [Certificates]** の順に選択します。
2. **[Controllers]** をクリックします。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、**[Controllers]** タブの名前が **[Control Components]** タブに変更されました。

3. 目的のデバイスの[...]をクリックし、[View Certificate]を選択して、インストールされている証明書を表示します。

証明書の失効

表 35: 機能の履歴

機能名	リリース情報	機能説明
証明書の失効	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco SD-WAN リリース 20.7.1 Cisco vManage リリース 20.7.1	この機能は、Cisco SD-WAN Manager がルート認証局から取得した証明書失効リストに基づいて、デバイスからエンタープライズ証明書を失効させます。

証明書の失効に関する情報

Cisco Catalyst SD-WAN でエンタープライズ証明書を使用している場合は、必要に応じて、Cisco SD-WAN Manager が指定された証明書をデバイスから取り消せるようにすることができます。たとえば、サイトでセキュリティの問題が発生した場合、証明書を取り消す必要がある場合があります。



(注) 証明書の失効機能は、デフォルトで無効になっています。

Cisco SD-WAN Manager は、Cisco SD-WAN Manager がルート認証局（CA）から取得した証明書失効リスト（CRL）に含まれている証明書を失効させます。

証明書失効機能を有効にして、CRL の URL を Cisco SD-WAN Manager に提供すると、Cisco SD-WAN Manager は設定された間隔でルート CA をポーリングし、CRL を取得して、CRL をオーバーレイネットワークの Cisco IOS XE Catalyst SD-WAN デバイス、Cisco vEdge デバイス、Cisco SD-WAN Validator、および Cisco SD-WAN コントローラ にプッシュします。CRL に含まれる証明書は、デバイスから取り消されます。

証明書が取り消されると、無効としてマークされます。デバイス制御接続は、次の制御接続フラップが発生するまで稼働し続け、その発生時点でデバイス制御接続はダウンします。デバイス制御接続を再び稼働させるには、デバイスに証明書を再インストールし、デバイスをオンボードします。

Cisco SD-WAN Manager がデバイスから証明書を取り消しても、デバイスがオーバーレイネットワークから削除されることはありませんが、オーバーレイネットワーク内の他のデバイスとは通信できなくなります。ピアデバイスは、証明書が CRL にあるデバイスからの接続試行を拒否します。

証明書の失効に関する制約事項

- デフォルトでは、証明書失効機能は無効になっています。証明書失効機能を初めて有効にするときは、ネットワークフラップ内のすべてのデバイスへの接続を制御します。サービスの中断を避けるために、最初はこの機能をメンテナンス時間中に有効にすることをお勧めします。

証明書失効機能が無効にするときは、ネットワークフラップ内のすべてのデバイスへの接続を制御します。サービスの中断を避けるために、この機能をメンテナンス時間中に無効にすることをお勧めします。

- エンタープライズ CA を使用してハードウェア WAN エッジ証明書承認、コントローラ証明書承認、または WAN エッジクラウド証明書承認の証明書に署名している場合にのみ、証明書失効機能を使用できます。
- Cisco SD-WAN Manager は、VPN 0 インターフェイスを介してのみサーバーに接続して CRL を取得できます。



(注) Cisco vManage リリース 20.11.1 以降、VPN 512 を介した接続がサポートされます。

証明書の失効の設定

はじめる前に

ルート CA CRL の URL を書き留めます。

手順

- Cisco SD-WAN Manager のメニューで、**[Administration] > [Settings]** の順に選択します。
- [Administration Settings] ウィンドウで、[Certificate Revocation List] の横にある [Edit] をクリックします。
証明書失効オプションが表示されます。
- [Enabled] をクリックします。
- [CRL Server URL] フィールドに、セキュアサーバーで作成した CRL の URL を入力します。
- [Retrieval Interval] フィールドに、Cisco SD-WAN Manager がセキュアサーバーから CRL を取得し、CRL が指定する証明書を失効させる間隔を時間単位で入力します。
1 ～ 24 の値を入力します。デフォルトの取得間隔は 1 時間です。
- [Save] をクリックします。

Cisco SD-WAN Manager はすぐに CRL を取得し、CRL が指定する証明書を取り消します。これ以降、Cisco SD-WAN Manager は指定した取得間隔の期間に従って CRL を取得します。

Cisco SD-WAN Manager を使用した Cisco IOS XE Catalyst SD-WAN デバイス へのサードパーティ CA 証明書の設定

表 36: 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN Manager を使用した Cisco IOS XE Catalyst SD-WAN デバイス へのサードパーティ CA 証明書の設定	Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a Cisco Catalyst SD-WAN Manager リリース 20.13.1	Cisco SD-WAN Manager を使用すると、一般的なサードパーティ CA 証明書をトラストポイント名とともに Cisco IOS XE Catalyst SD-WAN デバイス にアップロードしてプッシュできます。プロビジョニングは設定グループパーセルを介して実行され、ステータスはモニタリングですぐに確認できます。

Cisco SD-WAN Manager を使用した CA 証明書の設定に関する情報

Cisco SD-WAN Manager は現在、Cisco Catalyst SD-WAN ファブリックとの統合中にデバイスへのサードパーティ証明書のアップロードを許可していますが、この機能は制御接続の確立と初期デバイスのセットアップ中にのみ使用できます。

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、この機能により、UI を使用した証明書のアップロードが可能になります。Cisco SD-WAN Manager は、デバイスのセットアップ後でも CA 証明書のアップロードをサポートします。

CA 証明書はサーバー ID を認証し、不正アクセスを防止します。Cisco IOS XE Catalyst SD-WAN デバイスは、CA 証明書を使用して、ネットワーク内のさまざまなサーバーとのセキュアな接続を確立および管理します。Cisco SD-WAN Manager に CA 証明書をアップロードすると、Cisco IOS XE Catalyst SD-WAN デバイスは設定グループパーセルからのこの証明書情報を使用して、ネットワーク全体のサーバーと確立する接続を検証および認証します。これにより、ネットワークトラフィックの全体的なセキュリティと整合性が向上します。



(注) CA 証明書は、ルータの信頼できるルートを使用した SSL ベースのアクセスには適していません。

CA 証明書のアップロードでサポートされるデバイス

Cisco IOS XE Catalyst SD-WAN デバイス

CA 証明書を設定するための前提条件

- CA 証明書をアップロードするには、Cisco SD-WAN Manager で Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降のリリースを実行する必要があります。
- CA 証明書をアップロードするには、Cisco IOS XE Catalyst SD-WAN デバイス で Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降のリリースを実行する必要があります。

CA 証明書のアップロードの制約事項

- PEM でエンコードされた証明書ファイルのみをサポートします。
- 証明書の最大ファイルサイズは 10 MB です。
- Cisco Catalyst SD-WAN マルチテナンシーを使用している場合、CA 証明書をアップロードして管理するには、テナントである必要があります。詳細については、「[Tenant Role](#)」を参照してください。



(注) プロバイダーとして Cisco SD-WAN Manager にログインすると、CA 証明書をアップロードして管理することはできません。

CA 証明書のアップロード

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Certificates]** の順に選択します。
2. **[CA Cert]** タブをクリックします。
3. **[Add CA Certificate]** をクリックします。
4. **[Add CA Certificate]** ペインで、**[Certificate Name]** を入力します。
5. ファイルを選択するか、ドラッグアンドドロップして CA 証明書をアップロードします。
6. **[Paste]** タブをクリックし、証明書の詳細を貼り付けます。
7. **[Save]** をクリックします。

[Certificate Authority] ページで、[Device Group] テーブルにリストされている CA 証明書を見つけます。



- (注) [Device Group] テーブルで CA 証明書の [Expiration Date] を見つけ、[...] をクリックしてさらに [Actions] を実行します。

CA 証明書の削除

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Certificates]** の順に選択します。
2. [CA Cert] タブをクリックします。
3. [Device Group] テーブルで、削除する CA 証明書を選択します。
4. [Delete] をクリックします。



- (注) CA 証明書を削除する別の方法 : [Actions] 列の [...] アイコンをクリックし、[Delete] をクリックします。

Cisco SD-WAN Manager を使用した CA 証明書の設定

1. Cisco SD-WAN Manager のメニューから、[Configuration] > [Configuration Groups] を選択します。
設定グループの作成の詳細については、「[設定グループワークフロー](#)」を参照してください。
2. 設定グループに機能を追加します。
機能の追加の詳細については、「[Feature Management](#)」を参照してください。
3. [System Profile] で、[Add Feature] をクリックします。
4. [Add Feature] ペインで、[CA Certificate] を選択します。
5. [CA Certificates] セクションを設定します。

表 37: CA 証明書

フィールド	説明
Type	ドロップダウンリストから [CA Certificates] を選択します。
Name	証明書の名前を入力します。

フィールド	説明
Description	(任意) 証明書の説明を入力します。
Add CA Certificate	[Add CA Certificate] をクリックして、CA 証明書を追加します。
TrustPoint Name	トラストポイント名を入力します。
Certificate Name	ドロップダウンリストから CA 証明書を選択します。

6. [Save] をクリックします。
7. 設定グループに関連付けられているデバイスを展開します。詳細については、「[Deploy Devices](#)」を参照してください。



(注) [Device Group] テーブルから証明書を変更すると、変更はデバイスにミラーリングされません。これは、証明書とトラストポイントの関連付けによるものです。証明書を更新するには、証明書情報を含む既存のトラストポイントを削除する必要があります。その後、新しいトラストポイントを作成し、証明書を追加します。最後に、証明書を有効にするために変更をデバイスに展開します。

[Certificates] タブから証明書を削除しても、関連付けられているトラストポイントは自動的に削除されません。トラストポイントを削除するには、トラストポイントへの変更を手動で削除してから保存する必要があります。

CA 証明書の取り消し

CA 証明書を取り消すには、次の手順を使用します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration] > [Configuration Groups]** を選択します。
2. 設定グループ名の横にある [...] をクリックし、[Edit] を選択します。
3. 目的のシステムプロファイルをクリックします。
4. CA 証明書の横にある [...] をクリックし、[Delete Feature] を選択します。
5. 変更をデバイスに展開します。

CA 証明書の更新

CA 証明書を更新するには、次の手順を使用します。

1. 更新する CA 証明書を Cisco SD-WAN Manager にアップロードします。
2. Cisco SD-WAN Manager のメニューから、**[Configuration] > [Configuration Groups]** を選択します。
3. 設定グループ名の横にある [...] をクリックし、[Edit] を選択します。
4. 目的のシステムプロファイルをクリックします。
5. CA 証明書の横にある [...] をクリックし、[Delete Feature] を選択します。
6. [Configuration Groups] を使用して、設定グループに機能を追加し、「CA 証明書の設定」トピックのステップ 3 からステップ 7 の手順に従います。

CA 証明書と PKI トラストポイントの監視

CA 証明書の追跡

Cisco SD-WAN Manager に記載されている **[Issuer Name]**、**[Certificate Serial No.]** および **[Expiration Date]** を使用して CA 証明書を追跡します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration] > [Certificates]** の順に選択します。
2. [CA Cert] タブをクリックします。
3. Cisco SD-WAN Manager に追加された CA 証明書が [Device Group] テーブルに表示されます。

CA 証明書のインストールの監視

CA 証明書のインストールが完了すると、Cisco IOS XE Catalyst SD-WAN デバイスはイベントログを Cisco Catalyst SD-WAN Manager に送信します。

Cisco SD-WAN Manager のメニューから **[Monitor] > [Logs] > [Events]** の順に選択します。

CA 証明書のインストールはイベントとしてリストされ、[Events] テーブルに表示されます。

PKI トラストポイントの監視

リアルタイムコマンド **PKI Trustpoint** を使用して、PKI トラストポイントを監視します。詳細については、「View PKI Trustpoint information」を参照してください。

CRLベースの検疫

表 38: 機能の履歴

機能名	リリース情報	機能説明
CRLベースの検疫	Cisco vManage リリース 20.11.1	この機能を使用すると、認証局から Cisco SD-WAN Manager が取得した証明書失効リストに基づいて SD-WAN エッジデバイスを検疫できます。

CRL ベースの検疫に関する情報

Cisco Catalyst SD-WAN でエンタープライズ証明書を使用すると、Cisco SD-WAN Manager を使用して、侵害され、証明書が取り消された SD-WAN エッジデバイスを検疫できます。



(注) 証明書失効リスト (CRL) ベースの検疫機能は、デフォルトで無効になっています。

- Cisco SD-WAN Manager は、証明書失効リスト (CRL) に含まれている証明書を失効させます。Cisco SD-WAN Manager は、認証局 (CA) からこのリストを取得します。
- Cisco SD-WAN Manager は、定義された間隔で、最新の CRL について CRL サーバーをポーリングします。リストを受信すると、Cisco SD-WAN Manager はそれを分析して、隔離する SD-WAN エッジデバイスを決定します。
- Cisco SD-WAN Manager は、ネットワーク内の有効な各 SD-WAN エッジデバイスの証明書のシリアル番号が CRL 内の証明書のシリアル番号と一致するかどうかを確認します。一致が見つかった場合、SD-WAN エッジデバイス上の証明書は削除されないため、SD-WAN エッジデバイスは Cisco SD-WAN Manager への制御接続を保持できます。

SD-WAN エッジデバイスの検疫プロセスは次のとおりです。

- 検疫された各 SD-WAN エッジデバイスについて：
 - Cisco SD-WAN Manager は SD-WAN エッジデバイスをステージングモードに移行します。ステージングモードでは、Cisco SD-WAN Manager への制御接続を維持しながらデータトラフィックをシャットダウンします。
 - Cisco SD-WAN Manager は隔離されている SD-WAN エッジデバイスの通知を生成します。

隔離されたそれぞれの Cisco SD-WAN コントローラ について、Cisco SD-WAN Manager はコントローラへの通知を生成します。



(注) CRL サーバーは、VPN 0 または VPN 512 を介して Cisco SD-WAN Manager に接続します。

CRL ベースの検疫の制限

- CRL ベースの検疫機能を使用できるのは、ハードウェア WAN エッジ証明書承認、コントローラ証明書承認、または WAN エッジクラウド証明書承認の証明書に署名するエンタープライズ CA（認証局）がある場合のみです。
- CRL を無効にして、証明書の失効から検疫、または検疫から証明書の失効に切り替えます。証明書の失効と CRL ベースの検疫オプションを同時に有効にすることはできません。

CRL ベースの検疫の構成

はじめる前に

- Cisco SD-WAN Manager のメニューから **[Administration]** > **[Settings]** の順に選択します。次のいずれかのオプションをクリックし、エンタープライズモードを選択して CRL（証明書失効リスト）を有効にします。
 - **[Controller Certificate Authorization]** フィールドで、**[Enterprise Root Certificate]** または
 - **[Hardware WAN Edge Certificate Authorization]** フィールドで、**[Enterprise Certificate (signed by Enterprise CA)]** または
 - **[WAN Edge Cloud Certificate Authorization]** フィールドで、**[Manual (Enterprise CA - 推奨)]** を選択します。
- CA CRL の URL をメモします。



(注) デフォルトでは、CRL ベースの検疫機能は無効になっています。

CRL ベースの検疫を構成するには：

1. Cisco SD-WAN Manager のメニューから **[Administration]** > **[Settings]** の順に選択します。
2. **[Administration Settings]** ページで、**[Certificate Revocation List]** の横にある **[Edit]** をクリックします。
[Certificate Revocation] オプションと **[CRL-Based Quarantine]** オプションが表示されます。
3. **[CRL-Based Quarantine]** をクリックします。
4. **[CRL Server URL]** フィールドに、セキュアサーバーで作成した CRL の URL を入力します。

5. [Retrieval Interval] フィールドに、間隔を時間単位で入力します。Cisco SD-WAN Manager は証明書失効リスト（CRL）を使用して、SD-WAN エッジデバイスを検疫します。
1 ～ 24 の値を入力します。デフォルトの取得間隔は 24 時間です。
6. [VPN 0] または [VPN 512] をクリックします。Cisco SD-WAN Manager ではサーバーに接続し、VPN 0 または VPN 512 インターフェイスを介して CRL を取得します。
7. [Save] をクリックします。

Cisco SD-WAN Manager は定期的に CRL サーバーをポーリングして最新の CRL を取得します。このリストを分析して、隔離する SD-WAN エッジデバイスを決定します。



(注) 以前のリリースで CRL が無効になっている場合、Cisco vManage リリース 20.11.1 にアップグレードした後も CRL は無効のままです。Cisco vManage リリース 20.11.1 より前のリリースで CRL が有効になっていた場合、Cisco vManage リリース 20.11.1 にアップグレードした後、VPN0 をデフォルトとして証明書失効オプションが有効になります。

Cisco Catalyst SD-WAN Manager でのルート認証局証明書の管理

機能名	リリース情報	説明
Cisco SD-WAN Manager でのルート CA 証明書の管理のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco SD-WAN リリース 20.4.1 Cisco vManage リリース 20.4.1	この機能により、ルート認証局（CA）証明書を追加および管理できます。

ルート証明機関証明書の追加

1. Cisco SD-WAN Manager で、[Administration] > [Root CA Management] を選択します。
2. [Modify Root CA] をクリックします。
3. [Root Certificate] フィールドに証明書のテキストを貼り付けるか、[Select a File] をクリックしてファイルから証明書をロードします。
4. [Add] をクリックします。証明書テーブルで新しい証明書が表示されます。[Recent Status] 列は、証明書がまだインストールされていないことを示しています。
5. [Next] をクリックして、インストールされていない証明書の詳細を確認します。

6. [Save] をクリックして証明書をインストールします。証明書テーブルで新しい証明書が表示されます。

ルート認証局証明書の表示

1. Cisco SD-WAN Manager で、[Administration] > [Root CA Management] を選択します。
2. (オプション) [検索] フィールドにテキストを入力して、証明書ビューをフィルタ処理します。証明書のテキストまたは属性値 (シリアル番号など) でフィルタ処理できます。
3. 証明書のテーブルで、[More Actions(...)] をクリックし、[View] を選択します。ポップアップウィンドウが開き、証明書と詳細が表示されます。

ルート証明書の削除

この手順を使用して、ルート認証局 (CA) 証明書を削除します。

1. Cisco SD-WAN Manager で、[Administration] > [Root CA Management] を選択します。
2. [Modify Root CA] をクリックします。
3. テーブルにあるルート証明書を 1 つ以上選択し、[Action] 列のごみ箱アイコンをクリックします。削除対象としてマークされた証明書がテーブルに表示されます。
4. [Next] をクリックして、削除対象としてマークされている証明書の詳細を確認します。
5. [Save] をクリックして証明書を削除します。

エンタープライズ証明書

機能名	リリース情報	説明
Cisco SD-WAN Manager での RSA キーの長さの増加	Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.15.2 Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.16.1	エンタープライズ証明書の証明書署名要求 (CSR) に対して 4096 ビット RSA キーのサポートが追加されました。

Cisco IOS XE SD-WAN リリース 16.11.1 および Cisco SD-WAN リリース 19.1 でエンタープライズ証明書が導入されました。エンタープライズ証明書は、以前に使用されていたコントローラ証明書の承認に置き換わるものです。証明書管理の目的では、「コントローラ」という用語は、Cisco SD-WAN Manager、Cisco Catalyst SD-WAN コントローラ、および Cisco Catalyst SD-WAN Validator をまとめて指すために使用されます。

RSA キーの長さ

Cisco SD-WAN コントローラ にエンタープライズ証明書を使用する場合は、少なくとも 2048 ビットの RSA キーでルート証明書を使用してください。

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.16.1 および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.15.2 以降、Cisco SD-WAN 制御コンポーネント は 2048 ～ 4096 ビットの RSA キーサイズをサポートします。

ダウングレードに関する制限

4096 ビットの RSA キーを使用するエンタープライズ証明書を使用している場合は、Cisco SD-WAN 制御コンポーネントを Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.16.1 Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.15.2 より前のリリースにダウングレードする前に、2048 ビットの RSA キーを使用するようにエンタープライズ証明書を変更します。



- (注) エンタープライズ証明書に関するさらなる詳細については、『[Cisco Catalyst SD-WAN Controller Certificates and Authorized Serial Number File Prescriptive Deployment Guide](#)』を参照してください。

[Certificates] ページを使用して、証明書を管理し、オーバーレイネットワーク内の WAN エッジデバイスおよびコントローラデバイスを認証します。

Cisco Catalyst SD-WAN ソリューションの 2 つのコンポーネントで、デバイス認証が実行されます。

- 署名付き証明書は、オーバーレイネットワーク内のデバイスの認証に使用されます。認証されたデバイスは、相互にセキュアなセッションを確立できます。これらの証明書を生成し、それらをコントローラデバイス（Cisco SD-WAN Manager、Cisco SD-WAN Validator、および Cisco SD-WAN コントローラ）にインストールするのは Cisco SD-WAN Manager からです。
- WAN Edge 認定シリアル番号ファイルには、ネットワーク内のすべての有効な vEdge ルータと WAN ルータのシリアル番号が含まれています。Cisco Catalyst SD-WAN からこのファイルを受信し、各ルータを有効または無効としてマークし、Cisco SD-WAN Manager からネットワーク内のコントローラデバイスにファイルを送信します。

Cisco Catalyst SD-WAN オーバーレイ ネットワーク コンポーネントが相互に検証および認証できるようにするには、証明書と WAN Edge 認定シリアル番号ファイルをコントローラデバイスにインストールします。インストールすると、オーバーレイネットワークが動作可能になります。

Cisco SD-WAN コントローラ のエンタープライズ証明書の設定

機能名	リリース情報	説明
セカンダリ組織単位をサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r Cisco SD-WAN リリース 20.1.1	このオプション機能を使用すると、証明書を設定するときにセカンダリ組織単位を設定できます。指定した場合、この設定はすべてのコントローラとエッジデバイスに適用されます。
サブジェクト代替名 (SAN) のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco SD-WAN リリース 20.4.1 Cisco vManage リリース 20.4.1	この機能により、サブジェクト代替名 (SAN) DNS 名または Uniform Resource Identifier (URI) を設定でき、複数のホスト名と URI で同じ SSL 証明書を使用できるようになります。
WAN エッジクラウドデバイス エンタープライズ証明書の全組織の指定に関するサポート	Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.11.1	WAN エッジクラウドデバイスでエンタープライズ証明書のコントローラ証明書認証を構成する場合、[Organization] フィールドで任意の組織を指定できます。[Viptela LLC]、[vIPtela Inc]、[Cisco Systems] などの名前に限定されません。これにより、組織の認証局名またはサードパーティの認証局名を使用できます。
組織単位フィールドのない証明書のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.12.1	デバイスにインストールするエンタープライズ証明書では、組織単位 (OU) フィールドを定義する必要はありません。以前は、このフィールドはデバイスの認証の一部として使用されていました。

エンタープライズ証明書に関する情報

エンタープライズ証明書を使用すると、組織は、公的証明書署名機関に依存することなく、独自のプライベート証明書署名機関を使用できます。[Set CSR Properties] フィールドを使用して、カスタム証明書プロパティを適用することもできます。



- (注) 16.11/19.1 リリースでは、エンタープライズ証明書が導入されました。エンタープライズ証明書は、以前に使用されていたコントローラ証明書の承認に置き換わるものです。独立した組織がエンタープライズ証明書の署名を実施します。

[Configuration] > [Certificates] ページを使用して、証明書を管理し、オーバーレイネットワーク内の WAN エッジデバイスおよびコントローラデバイスを認証します。

Cisco Catalyst SD-WAN ソリューションの 2 つのコンポーネントで、デバイス認証が実行されます。

- 署名付き証明書は、オーバーレイネットワーク内のデバイスの認証に使用されます。認証されたデバイスは、相互にセキュアなセッションを確立できます。これらの証明書を生成し、それらをコントローラデバイス（Cisco SD-WAN Manager インスタンス、Cisco SD-WAN Validator、および Cisco SD-WAN コントローラ）にインストールするのは Cisco SD-WAN Manager からです。
- WAN エッジ認証シリアル番号ファイルには、ネットワーク内のすべての有効な vEdge ルータと WAN ルータのシリアル番号が含まれています。Cisco プラグアンドプレイ（PnP）からこのファイルを受信し、各ルータを有効または無効としてマークし、Cisco SD-WAN Manager からネットワーク内のコントローラデバイスにファイルを送信します。

Cisco Catalyst SD-WAN オーバーレイ ネットワーク コンポーネントが相互に検証および認証できるようにするには、証明書と WAN Edge 認定シリアル番号ファイルをコントローラデバイスにインストールする必要があります。インストールすると、オーバーレイネットワークが動作可能になります。



- (注) 証明書管理の目的で、コントローラという用語は、Cisco SD-WAN Manager、Cisco SD-WAN コントローラ、および Cisco SD-WAN Validator をまとめて指します。

WAN エッジデバイスをリセットしたら、エンタープライズルート証明書を手動でデバイスにインストールする必要があります。アップグレードを実行しても、証明書は保持されます。



- (注) Cisco SD-WAN Manager は、Base 64 でエンコードされた証明書のみをサポートします。エンコードされた他の形式（DER など）はサポートされていません。

たとえば、PEM 拡張機能は、**--BEGIN...** 行のプレフィックスが付いた ASCII（Base64）装甲データを含むさまざまなタイプの X.509v3 ファイルに使用されます。

エンタープライズ証明書の OU フィールドへの依存関係

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.12.1 以降、デバイスのオンボーディング時に、Cisco Catalyst SD-WAN では、関連付けられたエンタープライズ証明書に OU フィールド

ドが定義されている必要はありません。ただし、少なくとも1つのOUフィールドが定義されている場合、Cisco Catalyst SD-WAN では、OU フィールドの1つがファブリックの組織名と一致する必要があります。

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.12.2 から、デバイスのオンボーディング時に、関連付けられたエンタープライズ証明書に1つ以上のOUフィールドが定義されている場合、OU フィールドはファブリックの組織名と一致する必要はありません。

エンタープライズ証明書をサポートするデバイス

デバイス	エンタープライズ証明書サポート
Cisco SD-WAN Manager	対応
Cisco SD-WAN Validator	対応
Cisco SD-WAN コントローラ	対応
エッジルータ	すべてのハードウェア WAN エッジルータ ASR1002-X、ISRv、CSR1000v を除く vEdge/IOS-XE-SD-WAN

エンタープライズ証明書の設定

1. Cisco SD-WAN Manager メニューから、**[Administration] > [Settings] > [Hardware WAN Edge Certificate Authorization]** の順に選択します。
2. **[Enterprise Certificate]** (エンタープライズ CA によって署名済み) をクリックします。
[On Box Certificate (TPM/SUDI Certificate)] はデフォルトのオプションです。
3. カスタム証明書プロパティを指定する場合は、**[Set CSR Properties]** をクリックし、次のプロパティを設定します。

プロパティ	説明
Domain Name	ネットワークドメイン名。 17 文字以下にする必要があります。

プロパティ	説明
Organizational Unit	このフィールドは編集できません。組織単位は、Cisco SD-WAN Manager で使用されている組織名と同じである必要があります。 (注) Cisco IOS XE Catalyst SD-WAN リリース 17.9.3a、または Cisco IOS XE Release 17.9.x 以降、あるいは Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以降を使用するデバイスの場合、デバイスにインストールする証明書では、組織単位フィールドを定義する必要はありません。ただし、署名付き証明書に組織単位フィールドが含まれている場合、フィールドはデバイスで構成されている組織名と一致する必要があります。これは、2022 年 9 月の時点で、認証局ブラウザフォーラム (CA/ブラウザフォーラム) のポリシーに対応し、署名付き証明書に組織単位を含めることを停止します。CA/ブラウザフォーラムのポリシーが変更されたにもかかわらず、一部の認証局では、署名付き証明書に組織単位が含まれている場合があります。
Secondary Organization Unit	このオプションのフィールドは Cisco IOS XE SD-WAN リリース 17.2 または Cisco SD-WAN リリース 20.1.x から入手できます。このオプションのフィールドを指定すると、すべてのコントローラとエッジデバイスに適用されます。 (注) 署名付き証明書に [Organizational Unit] フィールドまたは [Secondary Organization Unit] フィールドが含まれている場合、これらのフィールドのいずれかが、デバイスに設定されている組織名と一致する必要があります。これは、2022 年 9 月の時点で、認証局ブラウザフォーラム (CA/ブラウザフォーラム) のポリシーに対応し、署名付き証明書に組織単位を含めることを停止します。CA/ブラウザフォーラムのポリシーが変更されたにもかかわらず、一部の認証局では、署名付き証明書に組織単位が含まれている場合があります。
Organization	組織名。
City	市区町村郡の名前。
State	都道府県の名前。
Email	電子メール アドレス。
2-Letter Country Code	国コード。

プロパティ	説明
Subject Alternative Name (SAN) DNS Names	任意で、複数のホスト名で同じ SSL 証明書を使用するように設定できます。 たとえば、cisco.com と cisco2.com を入力します。
Subject Alternative Name (SAN) URIs	任意で、複数の Uniform Resource Identifier (URI) で同じ SSL 証明書を使用するように設定できます。 たとえば、cisco.com と support.cisco.com を入力します。

4. **[Select a file]** を選択して、ルート認証局ファイルをアップロードします。
アップロードされたルート認証局がテキストボックスに表示されます。
5. **[Save]** をクリックします。
6. Cisco SD-WAN Manager メニューから、**[Configuration] > [Devices]**の順に選択します。
7. **[Upload WAN Edge List]** タブを選択します。
8. Cisco IOS XE Catalyst SD-WAN デバイス および Cisco vEdge デバイス リストの場所を参照し、**[Upload]** をクリックします。
9. **[Configuration] > [Certificates]** ページで **[...]** をクリックし、アクションを選択します。
 - **[View Enterprise CSR]** (証明書署名要求) : CSR をコピーし、エンタープライズルート証明書を使用して署名し、証明書のインストール操作を使用して Cisco SD-WAN Manager に署名済み証明書をアップロードします。Cisco SD-WAN Manager は、証明書をインストールする必要があるハードウェアエッジを自動的に検出します。
 - **[View Enterprise Certificate]** : 証明書をインストールすると、インストールされた証明書を表示してダウンロードできます。
 - **[Renew Enterprise CSR]** : ハードウェアデバイスに新しい証明書をインストールする必要がある場合は、**[Renew Enterprise CSR]** オプションを使用できます。**[Renew Enterprise CSR]** オプションは CSR を生成します。次に、証明書を表示し (**[View Enterprise CSR]** オプション)、証明書をインストールします (**[Install Certificate]** オプション)。この手順により、制御接続が新しいシリアル番号としてフラップされます。新しいシリアル番号と有効期限のデータは、**[Configuration] > [Certificates]** ページで確認できます。



- (注) Cisco Catalyst SD-WAN オーバーレイ内のデバイスにインストールする証明書では、組織単位フィールドを定義する必要はありません。ただし、署名付き証明書に組織単位フィールドが含まれている場合、フィールドはデバイスで構成されている組織名と一致する必要があります。

- **[Revoke Enterprise Certificate]** : このオプションは、デバイスからエンタープライズ証明書を削除し、プレステージングに戻します。デバイスでは、Cisco SD-WAN Validator と Cisco SD-WAN Manager のコントロールのみが動作しています。

Cisco IOS XE Catalyst SD-WAN デバイス の場合は、[...] をクリックしてアクションを選択します。

- **[View Feature CSR]** :

- Cisco IOS XE Catalyst SD-WAN デバイス から入手可能な CSR をコピーします。
- 証明機関からのエンタープライズルート証明書を使用して証明書に署名します。
- **[Install Feature Certificate]** 操作を使用して、署名付き証明書を Cisco SD-WAN Manager にアップロードします。

Cisco SD-WAN Manager は、証明書をインストールする必要があるハードウェアエッジを自動的に検出します。機能証明書をインストールすると、**[View Feature Certificate]** オプションが使用可能になります。

- **[View Feature Certificate]** : 機能証明書をインストールすると、機能証明書を表示してダウンロードできます。
- **[Revoke Feature Certificate]** : このオプションは、機能証明書またはトラストポイント情報を Cisco IOS XE Catalyst SD-WAN デバイス から削除します。証明書を取り消すと、デバイスに対するすべてのアクションが使用できなくなります。デバイスのすべてのアクションを表示するには、デバイスのログ情報を、認証タイプをサーバーとして Transport Layer Security (TLS) プロファイルに設定してから、相互に設定し直します。また、アクションを表示するには、Cisco IOS XE Catalyst SD-WAN デバイスを工場出荷時のデフォルト設定にリセットします。

デバイスを工場出荷時のデフォルトにリセットするには、次の手順を実行します。

- Cisco SD-WAN Manager メニューから、**[Configuration] > [Templates]** を選択します。
- 工場出荷時のデフォルトテンプレートを使用してデバイステンプレートを作成します。

工場出荷時のデフォルトテンプレートは、Factory_Default_feature-name_Template です。機能テンプレートを使用してデバイステンプレートを作成する方法については、[Create a Device Template from Feature Templates \[英語\]](#) を参照してください。

10. **[Install Certificate]** または **[Install Feature Certificate]** をクリックして、署名付き証明書をアップロードします。

証明書は、署名付き証明書である必要があります。最初の状態は「CSR Generated」です。

正常にインストールされると、状態が「Certificate Installed」に変わります。

11. Cisco SD-WAN Manager のメニューから **[Configuration]** > **[Certificates]** の順に選択します。デバイスタイプ、シャーシID、エンタープライズシリアル番号、エンタープライズ証明書の日付など、エンタープライズ証明書の列を確認できます。

デバイス証明書の無効化

WAN エッジデバイスを削除する前に、デバイスを無効にします。

1. Cisco SD-WAN Manager のメニューから **[Configuration]** > **[Certificates]** の順に選択します。
2. デバイスが表示されている行で、**[Invalid]** をクリックしてデバイスを無効にします。

エンタープライズルート証明書のコントローラ証明書の承認

1. Cisco SD-WAN Manager のメニューから **[Administration]** > **[Settings]** の順に選択します。
2. **[Controller Certificate Authorization]** 領域で、**[Edit]** をクリックします。
3. **[Enterprise Root Certificate]** をクリックします。警告が表示されたら、**[Proceed]** をクリックして続行します。
4. 必要に応じて、**[Set CSR Properties]** をクリックして、証明書署名要求（CSR）の詳細を手動で構成します。



- (注) マルチテナントシナリオで、CSR プロパティを手動で構成し、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.11.1 以降を使用している場合は、ネットワーク内のデバイスが Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a 以降を使用していることを確認してください。シングルテナントのシナリオでは、これは必要ありません。

マルチテナントシナリオで、CSR プロパティを手動で構成する場合、テナントデバイスの CSR を生成する準備ができたなら、以下で説明する **[Secondary Organizational Unit]** フィールドにテナントの組織名を入力します。マルチテナントシナリオで、サービスプロバイダー デバイスの CSR を生成する場合、これは必要ありません。

次のプロパティが表示されます。

- **[Domain Name]** : ネットワークドメイン名。最大 17 文字を入力できます。
- **Organizational Unit**



- (注) **[Organizational Unit]** フィールドは編集できません。このフィールドには、**[Administration]** > **[Settings]** > **[Organization Name]** の Cisco SD-WAN Manager に対して構成した組織名が自動的に入力されます。

- [Secondary Organizational Unit] : このオプションのフィールドは Cisco IOS XE SD-WAN リリース 17.2 または Cisco SD-WAN リリース 20.1.x 以降でのみ使用できます。このオプションのフィールドを指定すると、すべてのコントローラとエッジデバイスに適用されることに注意してください。
 - [Organization] : Cisco vManage リリース 20.11.1 以降では、WAN エッジクラウドデバイスでエンタープライズ証明書のコントローラ証明書認証を構成するときに、このフィールドで任意の組織を指定できます。[Viptela LLC]、[Viptela Inc]、[Cisco Systems] などの名前に限定されません。これにより、組織の認証局名またはサードパーティの認証局名を使用できます。最大長は 64 文字で、スペースと特殊文字を含めることができます。名前を入力すると、Cisco SD-WAN Manager により、名前が検証されます。
 - 市区町村郡 (City)
 - 都道府県 (State)
 - 電子メール (Email)
 - 2 文字の国コード (2-Letter Country Code)
 - [Subject Alternative Name (SAN) DNS Names] : (オプション) 同じ SSL 証明書を使用するように複数のホスト名を設定できます。例 : cisco.com および cisco2.com
 - [Subject Alternative Name (SAN) URIs] : (オプション) 複数の Uniform Resource Identifier (URI) を設定して、同じ SSL 証明書を使用できます。例 : cisco.com および support.cisco.com
5. SSL 証明書を [Certificate] フィールドに貼り付けるか、[Select a file] をクリックして SSL 証明書ファイルに移動します。
6. (任意) [Subject Alternative Name (SAN) DNS Names] フィールドに複数のホスト名を入力して同じ SSL 証明書を使用することができます。
たとえば、cisco.com と cisco2.com を入力します。
7. (任意) [Subject Alternative Name (SAN) URIs] フィールドに複数の URI を入力して同じ SSL 証明書を使用することができます。
たとえば、cisco.com と support.cisco.com を入力します。
- これは、組織の異なる部分に異なるサブドメインを使用せず、ホスト名に単一の証明書を使用する組織に役立ちます。

ブートストラップ構成の生成

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-WAN 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。デバイスは起動すると、構成ファイルの情報を使用してネットワークに接続します。



(注) ブートストラップ構成を生成する必要がある場合は、**[Configuration] > [Devices]** ページを使用して [...] をクリックし、**[Generate Bootstrap Configuration]** を選択します。



(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 Catalyst 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。

Cisco PKI コントローラの証明書

ソフトウェアリリース 19.x 以降では、Cisco Catalyst SD-WAN コントローラ証明書の Symantec/DigiCert の代わりに、Cisco を認証局 (CA) として使用するオプションがあります。

このセクションでは、展開タイプ、および Cisco Public Key Infrastructure (PKI) を使用してコントローラ証明書を管理、インストール、およびトラブルシューティングするシナリオについて説明します。Cisco PKI を使用すると、IP セキュリティ (IPSec)、セキュアシェル (SSH)、セキュアソケットレイヤ (SSL) などのセキュリティプロトコルをサポートする証明書管理を実現できます。

Symantec/DigiCert 証明書と Cisco PKI 証明書の主な違いは、Cisco PKI 証明書がプラグアンドプレイ (PnP) のスマートアカウント (SA) およびバーチャルアカウント (VA) にリンクされており、DigiCert などのポータルを使用した手動の承認が不要な点です。各 VA には 100 の証明書の制限、つまり、各オーバーレイには 100 の証明書の制限があり、証明書署名要求 (CSR) が生成された後、Cisco SD-WAN Manager 設定が正しく設定されていれば、承認とインストールが自動的に行われます。

デバイスが追加され、証明書が Cisco PKI サーバーから自動的にインストールされます。証明書を承認するための操作は不要です。

Cisco PKI 証明書のサポート対象デバイス

Cisco PKI 証明書を使用するためにサポートされているデバイスは次のとおりです。

デバイス	サポート
Cisco SD-WAN Manager	対応

デバイス	サポート
Cisco Catalyst SD-WAN Validator	対応
Cisco Catalyst SD-WAN コントローラ	対応
Cisco vEdge デバイス	対応
Cisco IOS XE Catalyst SD-WAN デバイス	対応

Cisco PKI コントローラ証明書のユースケース

- 使用例：ソフトウェアバージョン 19.x 以降によるシスコがホストするクラウドのオーバーレイ (341 ページ)
- ユースケース：証明書更新時の DigiCert 証明書から Cisco PKI コントローラ証明書へのアクティブな既存オーバーレイの移行 (343 ページ)
- 使用例：オンプレミスコントローラでの CSR の送信と証明書のダウンロード (347 ページ)

使用例：ソフトウェアバージョン 19.x 以降によるシスコがホストするクラウドのオーバーレイ

前提条件

Cisco SD-WAN Manager およびコントローラはすべて同じソフトウェアバージョンを実行している必要があります。

[Configuration] > [Devices] > [Controllers] ページで、すべてのコントローラの OOB IP アドレスとログイン情報が更新されていることを確認します。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

SSH を使用した制御接続を設定せずに、新規または期限切れのオーバーレイのソフトウェアバージョンを確認できます。

1. 各コントローラに SSH で接続すると、SSH プロセス中にバージョンが表示されます。
2. 実際にログイン情報を機能させる必要がないため、ログイン情報が機能しないコントローラでこの操作を実行できます。

オーバーレイ内のすべてのコントローラに対してこのプロセスを繰り返して確認します。

3. 次のいずれかの方法を使用して、お客様のスマートアカウントのログイン情報を準備する必要があります。

1. PnP トリガー通知からお客様の連絡先に個別に電子メールを送信し、スマートアカウントのログイン情報を提供するように依頼します。

または

2. お客様の連絡先に電子メールを送信し、お客様自身で Cisco SD-WAN Manager にログインして自身を追加するように依頼します。また、お客様の IP を許可リストに追加するように依頼します。

お客様にお客様の連絡先のログイン情報の入力を求める場合は、お客様が Cisco SD-WAN Manager GUI にアクセスしてログインし、スマートアカウントのログイン情報を入力できるように、IP を許可リストに追加するようにお客様に求めてから、この手順を実行するようにしてください。

スマートアカウントのログイン情報を表示するには、Cisco SD-WAN Manager メニューから、**[Administration] > [Settings] > [Smart Account Credentials]**の順に選択します。

ユーザ名およびパスワードを入力し、**[Save]** をクリックします。

Cisco PKI 証明書を要求してインストールするための Runbook

1. 前提条件を満たしていること、およびスマートアカウントのログイン情報を追加したことを確認します。
2. Cisco SD-WAN Manager メニューから、**[Administration] > [Settings] > [Controller Certificate Authorization]**の順に選択し、**[Edit]** をクリックします。
3. **[Cisco (Recommended)]** をクリックします。



- (注) スマートアカウントのログイン情報が追加されていない場合、Cisco SD-WAN Manager にエラーが表示されます。前提条件を確認します。

4. ドロップダウンで、有効期間を POC の場合は 1 年、生産オーバーレイの場合は 2 年に設定します。
5. **[Certificate Retrieve Interval]** を 1 分に設定し、**[Save]** を押します。



- (注) CSR リクエストが完了するとすぐに証明書が自動承認されるため、現在、承認についてお客様に通知するための電子メールフィールドはありません。

6. このステップ以降のプロセスは、Cisco SD-WAN Manager GUI の Symantec/DigiCert コントローラの場合と同じです。

Cisco SD-WAN Manager メニューから、**[Configuration] > [Certificates]**の順に選択し、**[Controllers]** をクリックします。[...] をクリックし、**[Generate CSR]** を選択します。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、**[Controllers]** タブの名前が **[Control Components]** タブに変更されました。

操作ステータスには、署名のために送信された CSR、人手による処理を必要とせずに自動的に署名およびインストールされた証明書が表示されます。

7. 証明書は自動的にインストールされます。成功すると、**[Configuration] > [Certificates] > [Controllers]** ページに次の内容が表示されます。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、**[Controllers]** タブの名前が **[Control Components]** タブに変更されました。

- 各コントローラの証明書の期限日
- **[Operation Status]** 列：
 - Cisco SD-WAN Validator : **[Installed]**
 - Cisco SD-WAN Manager および Cisco Catalyst SD-WAN コントローラ : "Cisco SD-WAN Validator Updated"
- **[Certificate Serial]** 列：証明書のシリアル番号

8. 制御接続が起動し、Cisco SD-WAN Manager ダッシュボードのコントローラに接続されていることを確認します。

ユースケース：証明書更新時の DigiCert 証明書から Cisco PKI コントローラ証明書へのアクティブな既存オーバーレイの移行

前提条件

Cisco SD-WAN Manager、コントローラ、および vEdge はすべて、制御接続が稼働している必要があります。

[Configuration] > [Devices] > [Controllers] で OOB IP アドレスとログイン情報が更新されていることを確認します。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

コントローラごとに [...] をクリックして更新を確認します。

DigiCert 証明書から Cisco PKI コントローラ証明書へのアクティブな既存オーバーレイの移行

1. Cisco SD-WAN Manager で、コントローラおよび Cisco vEdge デバイス への制御接続が稼働していることを確認します。

制御接続が稼働していない場合、DigiCert から Cisco PKI への移行は続行できません。

制御接続が部分的にのみ稼働している場合、つまり、一部の Cisco vEdge デバイス の制御がダウンしている場合、証明書を Cisco PKI に移行した後に制御が確立されても、それらの Cisco vEdge デバイス はコントローラに自動的に再接続できません。

証明書が期限切れで制御接続がダウンしている場合は、まず DigiCert で証明書を更新し、制御接続を起動してから Cisco PKI コントローラ証明書に移行する必要があります。

2. コントローラのソフトウェアバージョンが 19.x 以降であることを確認します。

Cisco SD-WAN Manager を使用して、アクティブな既存オーバーレイのソフトウェアバージョンを確認する方法（コントローラへの有効な制御接続あり）

1. Cisco SD-WAN Manager のメニューから **[Maintenance] > [Software Upgrade]** の順に選択します。
2. **[Manager]** をクリックして、**[Current Version]** 列を確認します。バージョンが 19.x 以降であることを確認します。

制御接続が稼働しており、Cisco SD-WAN Manager とコントローラのバージョンが 19.x 以降でない場合は、Cisco PKI への移行を実行する前に、まずそれらをアップグレードします（Cisco vEdge デバイス のアップグレードは不要）。



- (注) 19.x にアップグレードしたコントローラでは、アップグレードの一環として Cisco PKI を使用して証明書をすぐに更新する必要があります。既存のシマンテック証明書が有効なままであっても、それらの証明書を使用して実行することはできません。

3. 前提条件を確認したら、Cisco PKI ルート CA がすべてのコントローラと Cisco vEdge デバイスに伝播されていることを確認します。これには、コントローラへの SSH アクセスが必要です。

1. Cisco SD-WAN Manager およびコントローラに SSH で接続し、**show certificate root-ca-cert | include Cisco** コマンドを実行します。

出力が空白の場合、または結果が表示されない場合は、クラウドインフラ管理チームにエスカレーションします。

4. 次のいずれかの方法で、お客様のスマートアカウントのログイン情報を準備する必要があります。

1. PnP トリガー通知からお客様の連絡先に個別に電子メールを送信し、スマートアカウントのログイン情報を提供するように依頼します。

または

2. お客様の連絡先に電子メールを送信し、お客様自身で Cisco SD-WAN Manager にログオンしてご自身を追加するように依頼します。また、お客様の IP を許可リストに追加するように依頼します。

お客様に情報の入力を求める場合は、お客様が Cisco SD-WAN Manager GUI にアクセスしてログオンし、スマートアカウントのログイン情報を入力できるように、IP を許可リストに追加するようにお客様に求めてから、この手順を実行するようにしてください。

スマートアカウントのログイン情報を表示するには、Cisco SD-WAN Manager メニューから、**[Administration] > [Settings]**の順に選択し、**[Smart Account Credentials]** セクションを表示します。

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。

すべての前提条件が満たしたら、「**Cisco PKI 証明書を要求してインストールするための Runbook**」の手順に従って CSR を要求し、Cisco 証明書をインストールします。コントローラと Cisco vEdge デバイスへのすべての制御接続が復旧したことを確認します。復旧していない場合は、クラウドインフラ管理チームにエスカレーションします。

Cisco PKI 証明書を要求してインストールするための Runbook

1. 前提条件を満たしていること、およびスマートアカウントのログイン情報を追加したことを確認します。
2. Cisco SD-WAN Manager メニューから、**[Administration] > [Settings]**の順に選択し、**[Controller Certificate Authorization]** セクションで **[Edit]** をクリックします。
3. **[Cisco (Recommended)]** をクリックします。



(注) スマートアカウントのログイン情報が追加されていない場合、Cisco SD-WAN Manager にエラーが表示されます。前提条件を確認します。

4. ドロップダウンで、有効期間を POC の場合は 1 年、生産オーバーレイの場合は 2 年に設定します。

5. [Certificate Retrieve Interval] を 1 分に設定し、[Save] を押します。



(注) CSR リクエストが完了するとすぐに証明書が自動承認されるため、現在、承認についてお客様に通知するための電子メールフィールドはありません。

6. このステップ以降のプロセスは、Cisco SD-WAN Manager GUI の Symantec/DigiCert コントローラの場合と同じです。

Cisco SD-WAN Manager メニューから、**[Configuration] > [Certificates]**の順に選択し、**[Controllers]** をクリックします。[...] をクリックし、**[Generate CSR]** を選択します。



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、**[Controllers]** タブの名前が **[Control Components]** タブに変更されました。

操作ステータスには、署名のために送信された CSR、ユーザーの操作を必要とせずに自動的に署名およびインストールされた証明書が表示されます。

7. 証明書は自動的にインストールされます。成功すると、**[Configuration] > [Certificates] > [Controllers]** ページに次の内容が表示されます。



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、**[Controllers]** タブの名前が **[Control Components]** タブに変更されました。

- 各コントローラの証明書の期限日
- [Operation Status] 列：
 - Cisco SD-WAN Validator : [Installed]
 - Cisco SD-WAN Manager および Cisco SD-WAN コントローラ : "Cisco SD-WAN Validator Updated"
- [Certificate Serial] 列：証明書のシリアル番号

8. 制御接続が起動し、Cisco SD-WAN Manager ダッシュボードのコントローラに接続されていることを確認します。
9. [Certificate Retrieve Interval] を 1 分に設定します。
10. [Sync Root Certificate] をクリックして、Cisco SD-WAN Manager の Cisco vEdge デバイスまたは Cisco IOS XE Catalyst SD-WAN デバイスを Cisco PKI に移行します。このサポートは、19.2.1 バージョン以降から利用できます。

11. [Save] をクリックします。

使用例：オンプレミスコントローラでの CSR の送信と証明書のダウンロード

次の手順では、PnP および対象の SA/VA にアクセスできる必要があります。お客様は、独自の SA/VA にアクセスできます。

前提条件

証明書のインストールに手動の手法を使用することを除き、前提条件は上記の場合と同じです。

ランブック

1. Cisco SD-WAN Manager のメニューで、**[Administration] > [Settings]** の順に選択します。
[Controller Certificate Authorization] セクションで、[Manual] に設定されていることを確認します。
2. コントローラの CSR を生成します。

Cisco SD-WAN Manager メニューから、**[Configuration] > [Certificates]** の順に選択し、**[Controllers]** をクリックします。



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

[...] をクリックし、**[Generate CSR]** を選択します。

各 CSR をファイル名の拡張子が .csr のファイルにダウンロードし、署名付き証明書を取得するためにそれを PnP ポータルに送信できるように準備します。

3. 必要な SA/VA の PnP ポータルにログオンし、**[Certificates]** タブを選択します。
4. **[Generate Certificate]** をクリックし、手順に従って証明書ファイルの名前を指定してから、CSR を貼り付けて、署名付き証明書をダウンロードします。

これで、完成した証明書をダウンロードできます。CSR ごとにこのプロセスを繰り返して、必要なすべての証明書をダウンロードします。
5. ダウンロードした証明書をインストールするには、Cisco SD-WAN Manager メニューから、**[Configuration] > [Certificates]** の順に選択し、**[Controllers]** をクリックします。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

[Install Certificate] をクリックします。

インストール後、制御接続が稼働していることを確認します。

デバッグおよびログ情報

1. PnP の VA で Cisco Catalyst SD-WAN Validator プロファイルを調べて、正しい組織名が存在することを確認します。
2. 証明書プロセス全体のログについて、Cisco SD-WAN Manager で `/var/log/nms/vmanage-server.log` を確認します。
3. Cisco SD-WAN Manager に、Cisco PKI サーバーに到達するためのインターネット接続があることを確認します。

Cisco SD-WAN Manager の Web サーバー証明書

認証証明書を使用して Web ブラウザと Cisco SD-WAN Manager サーバー間のセキュアな接続を確立するには、CSR を生成して証明書を作成し、ルート CA による署名を得てから、インストールする必要があります。サーバーごとに次の手順を実行して、クラスタ内の各 Cisco SD-WAN Manager サーバーに個別の証明書をインストールする必要があります。

1. Cisco SD-WAN Manager のメニューで、**[Administration] > [Settings]** の順に選択します。
2. [Web Server Certificate] 領域で、[CSR] をクリックします。
3. [Common Name] フィールドに、Cisco SD-WAN Manager サーバードメイン名または IP アドレスを入力します。たとえば、Cisco SD-WAN Manager の完全修飾ドメイン名は `vmanage.org.local` になります。
4. [Organizational Unit] フィールドに、組織内の単位名を入力します（例：Network Engineering）。
5. [Organization] フィールドに、ルート CA によって指定された組織の正確な名前を入力します（例：Viptela Inc.）。
6. [City] フィールドに、組織がある都市の名前（例：川崎）を入力します。
7. [State] フィールドに、ユーザーの市がある都道府県を入力します（例：神奈川県）。
8. [2-Letter Country Code] フィールドに、ユーザーの都道府県がある国の 2 文字のコードを入力します。たとえば、米国の 2 文字の国コードは US です。

9. [Validity] をクリックして、証明書の有効期間を選択します。
10. 必要に応じて、[Subject Alternative Name (SAN) DNS Names] フィールドに、証明書の信頼を拡張する必要がある DNS サーバーの名前を入力します。複数の DNS サーバー名を入力する場合は、各名前をスペースまたはコンマで区切ります。



(注) Cisco Catalyst SD-WAN は、Cisco IOS XE SD-WAN リリース 16.11 および Cisco SD-WAN リリース 19.1 以降の SAN DNS 名をサポートしています。

11. 必要に応じて、[Subject Alternative Name (SAN) URIs] フィールドに、証明書の信頼を拡張する必要があるリソースの URI を入力します。複数の URI を入力する場合は、各 URI をスペースまたはコンマで区切ります。

各 URI を `schema:value` 形式で入力します。ここで、`schema` はリソースにアクセスするためのプロトコルで、`value` はリソースです。例：`https://example.example.com` または `scp://example.example.com`。



(注) Cisco Catalyst SD-WAN は、Cisco IOS XE SD-WAN リリース 16.11 および Cisco SD-WAN リリース 19.1 以降の SAN URI をサポートしています。

12. [Generate (生成)] をクリックして CSR を生成します。
13. CSR を CA サーバーに送信して、署名してもらいます。
14. 署名付き証明書を受け取ったら、[Web Server Certificate] バーの近くにある [Certificate] をクリックして、新しい証明書をインストールします。[View] ボックスに、Cisco SD-WAN Manager サーバー上の現在の証明書が表示されます。
15. 新しい証明書をコピーしてボックスに貼り付けます。または、[Import and Select a File] をクリックして、新しい証明書ファイルをダウンロードします。
16. アプリケーションサーバーを再起動して、Cisco SD-WAN Manager にログインします。

Web サーバー証明書期限日の表示

認証証明書を使用して Web ブラウザと Cisco SD-WAN Manager サーバー間のセキュアな接続を確立する場合は、証明書の有効期間を設定します（前のセクションのステップ 8）。この期間が終了すると、証明書が期限切れになります。[Web Server Certificate] バーに、期限の日時が表示されます。

証明書の有効期限が切れる 60 日前から、証明書の有効期限が近づいていることを示す通知が Cisco SD-WAN Manager ダッシュボードに表示されます。この通知は、期限日の 30 日前、15 日前、および 7 日前に再表示され、その後は毎日表示されます。



第 10 章

期限切れのエンタープライズ証明書の表示と検疫

- [期限切れの証明書の表示と検疫（351 ページ）](#)
- [期限切れの証明書の表示と検疫について（352 ページ）](#)
- [証明書が期限切れのデバイスの検疫の有効化（353 ページ）](#)
- [期限切れ証明書の検疫におけるデバイスの表示と修復（353 ページ）](#)

期限切れの証明書の表示と検疫

表 39: 機能の履歴

機能名	リリース情報	機能説明
期限切れの証明書の表示と検疫	Cisco IOS XE Catalyst SD-WAN リリース 17.16.1a Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.16.1	Cisco SD-WAN Manager は、デバイスまたは Cisco Catalyst SD-WAN 制御コンポーネントの証明書がいつ期限切れになったかを示します。 また、証明書が期限切れになったすべてのエッジデバイスを検疫できます。検疫により、デバイスはステージングステータスになります。検疫対象のデバイスは Cisco Catalyst SD-WAN 制御コンポーネントへの制御接続は維持しますが、データプレーントラフィックは処理しません。

期限切れの証明書の表示と検疫について

期限切れの証明書の表示

デジタル証明書は、オーバーレイネットワーク内のデバイスの認証に使用されます。認証後、デバイスと Cisco Catalyst SD-WAN 制御コンポーネント は相互にセキュアなセッションを確立できます。証明書は認証局（CA）によって発行され、有効期限があります。

Cisco SD-WAN Manager は数分ごとに、ネットワーク内のデバイスと Cisco Catalyst SD-WAN 制御コンポーネントに期限切れの証明書がないかチェックします。期限切れの証明書が検出された場合、Cisco SD-WAN Manager には、**[Configuration] > [Certificates] > [WAN Edges]** ページまたは **[Configuration] > [Certificates] > [Control Components]** ページへのリンク付きのバナーが表示され、証明書の更新が必要なデバイスまたはコンポーネントの詳細が示されます。

デバイス検疫

検疫とは、デバイスをステージング状態にすることを指します。検疫対象のデバイスは Cisco Catalyst SD-WAN 制御コンポーネントへの制御接続は維持しますが、データプレーントラフィックは処理しません。

証明書の期限が切れているデバイスを検疫できます。「[証明書が期限切れのデバイスの検疫の有効化（353 ページ）](#)」を参照してください。

証明書の期限が切れているデバイスを検疫すると、期限切れの証明書の更新が要求されます。組織のネットワークセキュリティ要件に準拠するために、証明書の期限が切れているネットワーク要素の削除が必要となる場合があります。

この表は、検疫機能が有効になっている場合に、自動検疫の対象となるデバイスを示しています。

表 40: 期限切れ証明書の自動検疫

デバイスまたは制御コンポーネント	検疫が有効な場合の自動検疫
証明書を使用するハードウェアデバイス	対応
オンボックスのトラステッドプラットフォーム モジュール（TPM）のセキュアな固有デバイス識別子（SUDI）証明書を使用するハードウェアデバイス	非対応
ソフトウェアデバイス	対応
Cisco Catalyst SD-WAN 制御コンポーネント	非対応

マルチテナント機能

マルチテナントのシナリオでは、期限切れ証明書の検疫の有効化はプロバイダーレベルでのみ可能であり、すべてのテナントに適用されます。

証明書が期限切れのデバイスの検疫の有効化

手順

ステップ 1 Cisco SD-WAN Manager のメニューで、**[Administration] > [Settings]** の順に選択します。

ステップ 2 **[Device Quarantine]** をクリックします。

ステップ 3 デバイス検疫を有効にします。

期限切れ証明書の検疫におけるデバイスの表示と修復

Cisco SD-WAN Manager は、証明書が期限切れのデバイスを検疫できます。「[期限切れの証明書の表示と検疫について（352 ページ）](#)」を参照してください。Cisco SD-WAN 制御コンポーネントは検疫しません。

始める前に

期限切れ証明書の検疫を有効にします。「[証明書が期限切れのデバイスの検疫の有効化（353 ページ）](#)」を参照してください。

手順

ステップ 1 **[Configuration] > [Certificates] > [WAN Edges]** ページを開き、証明書の更新が必要なデバイスはどれかの詳細を含むテーブルを表示します。

Cisco SD-WAN Manager に証明書の期限切れによって 1 つ以上のデバイスが検疫されていることを示すバナーメッセージが表示されている場合は、バナーメッセージ内のリンクをクリックしてページを開きます。

テーブルで、感嘆符アイコンはデバイスの問題を示しています。アイコンにカーソルを合わせると、証明書の期限切れなどの問題の詳細が表示されます。デバイスが検疫されている場合、そのデバイスの **[Validate]** 列に **[staging]** と表示されます。

ステップ 2 検疫からデバイスを削除するには、その証明書を更新します。「[WAN Edge デバイス証明書署名要求の生成](#)」を参照してください。



第 11 章

リバースプロキシ

- [リバースプロキシ \(355 ページ\)](#)
- [リバースプロキシについて \(355 ページ\)](#)
- [リバースプロキシに関する制約事項 \(358 ページ\)](#)
- [リバースプロキシでの証明書のプロビジョニング \(359 ページ\)](#)
- [Cisco SD-WAN Manager を使用したリバースプロキシの設定 \(360 ページ\)](#)
- [CLI を使用したリバースプロキシの監視 \(362 ページ\)](#)
- [CLI を使用したリバースプロキシの監視 \(366 ページ\)](#)

リバースプロキシ

表 41: 機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN および Cisco Catalyst SD-WAN のマルチテナント機能を使用したリバースプロキシのサポート	Cisco IOS XE リリース 17.6.1a Cisco SD-WAN リリース 20.6.1 Cisco vManage リリース 20.6.1	この機能を使用すると、Cisco IOS XE Catalyst SD-WAN デバイス と Cisco SD-WAN Manager と Cisco SD-WAN コントローラ の間のオーバーレイネットワークにリバースプロキシを展開できます。また、この機能を使用すると、Cisco vEdge デバイス または Cisco IOS XE Catalyst SD-WAN デバイス を含むシングルテナント展開とマルチテナント展開の両方にリバースプロキシを展開できます。マルチテナント展開では、サービスプロバイダーがリバースプロキシおよび関連する設定を管理します。

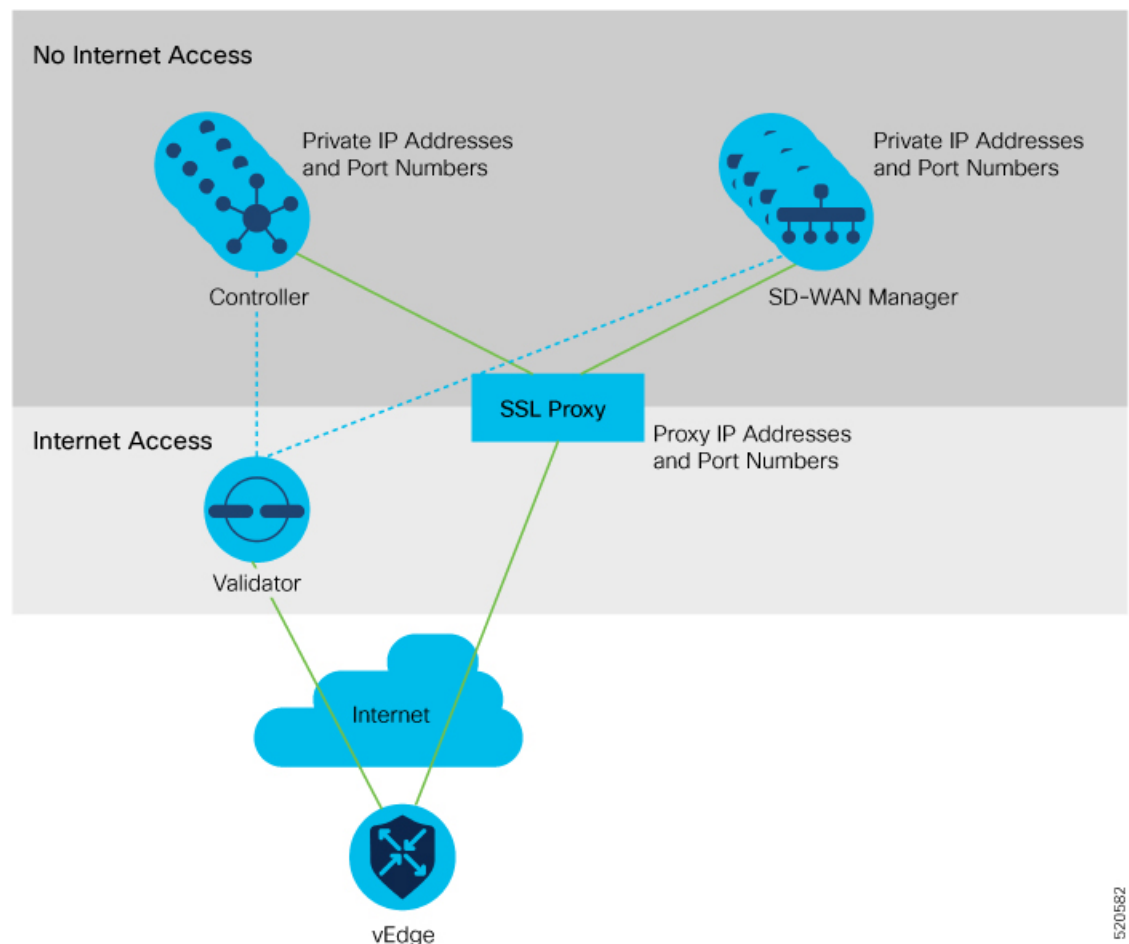
リバースプロキシについて

標準のオーバーレイネットワークでは、Cisco Catalyst SD-WAN エッジデバイスが Cisco SD-WAN 制御コンポーネント（Cisco SD-WAN Manager および Cisco SD-WAN コントローラ）への直接

接続を開始し、これらの接続を介してコントロールプレーン情報を交換します。WAN エッジデバイスは通常、ブランチサイトに配置され、インターネット経由で Cisco SD-WAN コントローラに接続します。その結果、Cisco SD-WAN Manager および Cisco SD-WAN コントローラもインターネットに直接接続されます。

セキュリティまたはその他の理由から、Cisco SD-WAN コントローラに直接インターネット接続をさせたくない場合があります。このようなシナリオでは、Cisco SD-WAN コントローラと WAN エッジデバイスの間にリバースプロキシを展開できます。リバースプロキシは、Cisco SD-WAN コントローラと WAN エッジデバイスの間で制御トラフィックを渡す仲介役として機能します。WAN エッジデバイスは、Cisco SD-WAN Manager および Cisco SD-WAN コントローラと直接通信するのではなくリバースプロキシと通信し、リバースプロキシは Cisco SD-WAN Manager および Cisco SD-WAN コントローラとの間のトラフィックをリレーします。

次の図は、WAN エッジデバイスと Cisco SD-WAN Manager および Cisco SD-WAN コントローラとの間に展開されたリバースプロキシを示しています。



Cisco Catalyst SD-WAN のシングルテナント展開とマルチテナント展開の両方でリバースプロキシを展開できます。TLOC は、パブリックまたはプライベート TLOC に関係なく、パブリック IP アドレスとポートでリバースプロキシと通信します。

プライベートネットワークとパブリックインターネット接続の両方によるデバイスのサポート

次の複数の TLOC を持つデバイスを含む Cisco Catalyst SD-WAN ネットワークでは、リバースプロキシを使用できます。

- インターネットアクセスなしで内部のプライベートネットワークに接続する TLOC、および
- パブリックインターネットに接続する TLOC

このシナリオには、各 Cisco SD-WAN コントローラ の TLOC カラーを設定するための特定の要件があります。次の表では、この特殊なケースについて説明します。比較のために、TLOC が1つのみのデバイスと、プライベートネットワーク用とパブリックインターネット用に個別の TLOC があるデバイスの例を示しています。

表 42: TLOC カラーの要件

デバイス	TLOC	TLOC 接続	この TLOC カラーの設定	この Cisco SD-WAN Validator へのデバイスの接続	接続先 : Cisco SD-WAN コントローラ、および Cisco SD-WAN Manager	特定の TLOC カラー要件
A	1	内部プライベートネットワーク	プライベートの色 例 : private1	プライベートネットワークを介して到達可能な Cisco SD-WAN Validator	プライベートネットワークを介した直接接続	なし
B	1	パブリックインターネット	パブリックの色 例 : custom1	パブリックインターネットを介して到達可能な Cisco SD-WAN Validator	リバースプロキシを介した接続	なし

デバイス	TLOC	TLOC 接続	この TLOC カラーの設定	この Cisco SD-WAN Validator へのデバイスの接続	接続先 : Cisco SD-WAN コントローラ、および Cisco SD-WAN Manager	特定の TLOC カラー要件
C	1	内部プライベートネットワーク	プライベートネットワークの色 例 : private1	プライベートネットワークを介して到達可能な Cisco SD-WAN Validator	プライベートネットワークを介した直接接続	ここに示すように複数の TLOC を持つデバイスを含むネットワークには、次の特定の要件があります。 プライベートネットワークに使用しているプライベートの色を使用して、各 Cisco SD-WAN コントローラの TLOC を設定する。TLOC カラーをデフォルトのままにしない。 Cisco SD-WAN コントローラの TLOC カラーをデフォルトの色のままにすると次の問題が発生します : デバイス C などの内部プライベートネットワークに接続する TLOC を持つデバイスが Cisco SD-WAN コントローラに接続できない。
	2	パブリックインターネット	パブリックの色 例 : custom1	パブリックインターネットを介して到達可能な Cisco SD-WAN Validator	リバースプロキシを介した接続	

リバースプロキシに関する制約事項

• マルチテナントのシナリオ

マルチテナント Cisco Catalyst SD-WAN オーバーレイネットワークでは、3 ノード Cisco SD-WAN Manager クラスタのみでリバースプロキシデバイスを展開できます。

- TLS ベースのコントロールプレーン

リバースプロキシの展開は、Cisco SD-WAN Manager および Cisco SD-WAN コントローラの TLS ベースのコントロールプレーンでのみサポートされます。

- Cisco vEdge 5000 ルータの制限

Cisco vEdge 5000 ルータではリバースプロキシを展開できません。

- IPv6

IPv6 制御接続ではリバースプロキシを展開できません。

- プライベート WAN 用の TLOC を備えたデバイス

次の制限は、(a) 1 つ以上のデバイスがプライベート WAN に接続するための TLOC を持ち、(b) 1 つ以上の Cisco SD-WAN Validator がリバースプロキシに到達できないシナリオで、エッジデバイスに適用されます。

このシナリオでは、ゼロタッチプロビジョニング (ZTP) オンボーディングは、デフォルトの TLOC カラーを使用した TLOC での Cisco IOS XE Catalyst SD-WAN デバイスのオンボーディングをサポートしていません。デフォルト以外の TLOC カラーを設定する最小限の設定でデバイスをブートストラップします。

リバースプロキシでの証明書のプロビジョニング

トラフィックを交換する前に、リバースプロキシと WAN エッジデバイスの相互認証が必要です。

リバースプロキシでは、Cisco SD-WAN コントローラの証明書に署名した CA によって署名された証明書をプロビジョニングする必要があります。この証明書は、WAN エッジデバイスを検証するためにリバースプロキシによって使用されます。

リバースプロキシの証明書署名要求 (CSR) を生成し、シスコが署名するようにするには、次の手順を実行します。

1. リバースプロキシで次のコマンドを実行します。

```
proxy$ openssl req -new -days 365 -newkey rsa:2048 -nodes -keyout Proxy.key -out Proxy.csr
```

プロンプトが表示されたら、次の表に示されている値を入力します。

プロパティ	説明
Country Name (2 letter code)	任意の国コード。 例：US
State or Province Name	任意の州または都道府県。 例：CA

プロパティ	説明
Locality Name	任意の地域。 例：San Jose
Organization Name	「vIPTela Inc」または「Viptela LLC」のいずれかを使用してください。 Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a から、エンタープライズ証明書の組織名として「Cisco Systems」文字列を使用できます。 Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降、ブートストラップ設定ファイルの [Organization Name] フィールドにカンマを含めることはできません。 例：Viptela LLC
Organizational Unit Name	オーバーレイで設定した「組織」の名前を使用します。 例：cisco-sdwan-12345
Common Name	「.viptela.com」で終わるホスト名。 例：proxy.viptela.com
Email Address	任意の有効な電子メールアドレスを使用します。 例：someone@example.com

2. CSR がシスコによって署名されます。

- Cisco SD-WAN コントローラの CA として Symantec/Digicert を使用する場合は、Cisco TAC で CSR の署名のためのケースを開きます。
- Cisco SD-WAN コントローラの CA として Cisco Public Key Infrastructure (PKI) を使用する場合は、Cisco ネットワーク プラグ アンド プレイ (PnP) アプリケーションで CSR を送信し、署名付き証明書を取得します。

Cisco SD-WAN Manager を使用したリバースプロキシの設定

リバースプロキシの設定

1. Cisco SD-WAN Manager のメニューで、**[Administration] > [Settings]** の順に選択します。
2. **[Reverse Proxy]** 設定で、**[Edit]** をクリックします。

3. [Enable Reverse Proxy] で、[Enabled] をクリックします。
4. [Save] をクリックします。

Cisco SD-WAN コントローラでのリバースプロキシの設定

1. Cisco SD-WAN Manager のメニューから、[Configure] > [Devices] の順に選択します。
2. [Controllers] をクリックします。



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

3. 目的の Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ で [...] をクリックして、[Add Reverse Proxy] をクリックします。

[Add Reverse Proxy] ダイアログボックスが表示されます。

4. プライベート IP アドレスとポート番号をプロキシ IP アドレスとポート番号にマッピングするには、次の手順を実行します。
 1. [Add Reverse Proxy] をクリックします。
 2. 次の詳細を入力します。

プライベート IP	プライベート IP アドレスは、VPN0 のトランスポートインターフェイスの IP アドレスです。
プライベートポート	これは、オーバーレイネットワークでトラフィックの制御と処理を行う接続を確立するために使用されるポートです。デフォルトポート番号は、12346 です。
プロキシ IP	プライベート IP アドレスをマップする必要があるプロキシ IP アドレス。
プロキシポート	プライベートポートをマップする必要があるプロキシポート。

3. Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ に複数のコアがある場合は、コアごとに手順 4a と手順 4b を繰り返します。
5. プライベート IP アドレスとポート番号からプロキシ IP アドレスとポート番号へのマッピングを削除するには、マッピングを探してごみ箱アイコンをクリックします。
6. リバースプロキシ設定を保存するには、[Add] をクリックします。
設定を破棄するには、[Cancel] をクリックします。

7. Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ にアタッチされたセキュリティ機能テンプレートで、トランスポートプロトコルとして TLS を選択します。

Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ でリバースプロキシを設定すると、オーバーレイネットワーク内の WAN エッジデバイスは、リバースプロキシでの認証用の証明書を使用してプロビジョニングされます。

1. リバースプロキシが展開されると、Cisco SD-WAN Validator はリバースプロキシの詳細を WAN エッジデバイスと共有します。
2. リバースプロキシについて学習した WAN エッジデバイスは、Cisco SD-WAN Manager から署名付き証明書のインストールを開始します。
3. 証明書がインストールされると、WAN エッジデバイスはその証明書を使用してリバースプロキシを認証し、リバースプロキシに接続します。

リバースプロキシの無効化



(注) リバースプロキシを無効にする前に、Cisco SD-WAN Manager インスタンスおよび Cisco SD-WAN コントローラ に対して設定したプライベート IP アドレスとポート番号からプロキシ IP アドレスとポート番号へのマッピングを削除します。マッピングの削除については、「Configure Reverse Proxy Settings on Cisco Catalyst SD-WAN Controllers」を参照してください。

1. Cisco SD-WAN Manager のメニューで、[Administration] > [Settings] の順に選択します。
2. [Reverse Proxy] 設定で、[Edit] をクリックします。
3. [Enable Reverse Proxy] で、[Disabled] をクリックします。
4. [Save] をクリックします。

CLI を使用したリバースプロキシの監視

Cisco SD-WAN コントローラでの WAN エッジデバイスのプライベートおよびプロキシ IP アドレスとポート番号の監視

次に、Cisco SD-WAN コントローラ での **show control connections** コマンドの出力例を示します。WAN エッジデバイスの場合、コマンド出力の [PEER PRIVATE IP] および [PEER PRIVATE PORT] 列のエントリは、設定された TLOC IP アドレスと WAN エッジインターフェイスのポート番号です。[PEER PUBLIC IP] および [PEER PUBLIC PORT] 列のエントリは、リバースプロキシインターフェイスの対応する IP アドレスとポート番号です。同じコマンドを Cisco SD-WAN Manager インスタンスで実行した場合も、同様の出力が得られます。

```
vsmart1# show control connections
```

								PEER	
PEER	PEER	PEER	PEER	SITE	DOMAIN	PEER	PRIV	PEER	
PUB	TYPE	PROT	SYSTEM	IP	ID	ID	PRIVATE	IP	
INDEX	ORGANIZATION		REMOTE	COLOR	STATE	UPTIME	PORT	PUBLIC	
PORT								IP	
0	vbond	dtls	172.16.1.2	0		0	10.1.1.2	12346	
12346	EXAMPLE-ORG	default		up	53:08:18:50			10.1.1.2	
0	vmanage	tls	172.16.1.6	1		0	10.2.100.6	45689	
45689	EXAMPLE-ORG	default		up	53:08:18:32			10.2.100.6	
1	vedge	tls	1.1.100.1	100		1	10.3.1.2	57853	
53624	EXAMPLE-ORG	biz-internet		up	53:08:18:44			10.2.100.1	
1	vedge	tls	1.1.101.1	101		1	10.4.1.2	55411	
53622	EXAMPLE-ORG	biz-internet		up	53:08:18:48			10.2.100.1	
1	vbond	dtls	172.16.1.2	0		0	10.1.1.2	12346	
12346	EXAMPLE-ORG	default		up	53:08:18:51			10.1.1.2	

SD-WAN コントローラのプライベート IP アドレスとポート番号から Cisco SD-WAN Validator のプロキシ IP アドレスとポート番号へのマッピングの表示

次に、Cisco SD-WAN Validator での **show orchestrator reverse-proxy-mapping** コマンドの出力例を示します。コマンド出力の [PROXY IP] 列と [PROXY PORT] 列のエントリは、プロキシの IP アドレスとポート番号です。[PRIVATE IP] 列と [PRIVATE PORT] 列のエントリは、VPN 0 のトランスポートインターフェイスのプライベート IP アドレスとポート番号です。

```
vbond# show orchestrator reverse-proxy-mapping
```

	PRIVATE			PROXY
UUID	PRIVATE IP	PORT	PROXY IP	PORT

14c35ae4-69e3-41c5-a62f-725c839d25df	10.2.100.4	23456	10.2.1.10	23458
14c35ae4-69e3-41c5-a62f-725c839d25df	10.2.100.4	23556	10.2.1.10	23558
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23456	10.2.1.10	23457
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23556	10.2.1.10	23557
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23656	10.2.1.10	23657
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23756	10.2.1.10	23757
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23856	10.2.1.10	23857
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23956	10.2.1.10	23957
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	24056	10.2.1.10	24057
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	24156	10.2.1.10	24157
vbond#				

例：SD-WAN コントローラのプライベート IP アドレスとポート番号から WAN エッジデバイス
のプロキシ IP アドレスとポート番号へのマッピングを表示する

次に、Cisco IOS XE Catalyst SD-WAN デバイス での **show sdwan control connections**
コマンドの出力例を示します。コマンド出力で、Cisco SD-WAN Manager インスタンスまたは
Cisco SD-WAN コントローラ の [PROXY] 列のエントリを確認します。エントリが [Yes] の場
合、[PEER PUBLIC IP] および [PEER PUBLIC PORT] のエントリはプロキシ IP アドレスとポ
ート番号です。

Device# **show sdwan control connections**

				CONTROLLER		PEER		PEER	
PEER	PEER	PEER		SITE	DOMAIN	PEER	PRIV	PEER	PUB
				GROUP					
TYPE	PROT	SYSTEM IP	ID	ID	PRIVATE IP	PORT	PUBLIC IP	PORT	
ORGANIZATION		LOCAL COLOR	PROXY	STATE	UPTIME	ID			
vsmart	tls	172.16.1.4	1	1	10.2.100.4	23558	10.2.1.10	23558	
EXAMPLE-ORG		biz-internet	Yes	up	52:08:44:25 0				
vbond	dtls	0.0.0.0	0	0	10.1.1.2	12346	10.1.1.2	12346	
EXAMPLE-ORG		biz-internet	-	up	52:08:50:47 0				
vmanage	tls	172.16.1.6	1	0	10.2.100.6	23957	10.2.1.10	23957	
EXAMPLE-ORG		biz-internet	Yes	up	66:03:04:50 0				

Device#

Cisco vEdge デバイス では、**show control connections** コマンドを実行して同様の出力を取得で
きます。

リバースプロキシとの認証のために WAN エッジデバイスにインストールされた署名付き証明
書の表示

次に、Cisco IOS XE Catalyst SD-WAN デバイス での **show sdwan certificate reverse-proxy** コマ
ンドの出力例を示します。

Device# **show sdwan certificate reverse-proxy**

Reverse proxy certificate

Certificate:

Data:

Version: 1 (0x0)

```
Serial Number: 1 (0x1)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = US, CN = 6c63e80a-8175-47de-a455-53a127ee70bd, O = Viptela

Validity

    Not Before: Jun  2 19:31:08 2021 GMT

    Not After : May 27 19:31:08 2051 GMT

Subject: C = US, ST = California, CN = C8K-9AE4A5A8-4EB0-E6C1-1761-6E54E4985F78,
O = ViptelaClient
Subject Public Key Info:

    Public Key Algorithm: rsaEncryption

        RSA Public-Key: (2048 bit)

        Modulus:

            00:e2:45:49:53:3a:56:d4:b8:70:59:90:01:fb:b1:
            44:e3:73:17:97:a3:e9:b7:55:44:d4:2d:dd:13:4a:
            a8:ef:78:14:9d:bd:b5:69:de:c9:31:29:bd:8e:57:
            09:f2:02:f8:3d:1d:1e:cb:a3:2e:94:c7:2e:61:ea:
            e9:94:3b:28:8d:f7:06:12:56:f3:24:56:8c:4a:e7:
            01:b1:2b:1b:cd:85:4f:8d:34:78:78:a1:26:17:2b:
            a5:1b:2a:b6:dd:50:51:f8:2b:13:93:cd:a6:fd:f8:
            71:95:c4:db:fc:a7:83:05:23:68:61:15:05:cc:aa:
            60:af:09:ef:3e:ce:70:4d:dd:50:84:3c:9a:57:ce:
            cb:15:84:3e:cd:b2:b6:30:ab:86:68:17:94:fa:9c:
            1a:ab:28:96:68:8c:ef:c8:f7:00:8a:7a:01:ca:58:
            84:b0:87:af:9a:f6:13:0f:aa:42:db:8b:cc:6e:ba:
            c8:c1:48:d2:f4:d8:08:b1:b5:15:ca:36:80:98:47:
            32:3a:df:54:35:fe:75:32:23:9f:b5:ed:65:41:99:
            50:b9:0f:7a:a2:10:59:12:d8:3e:45:78:cb:dc:2a:
            95:f2:72:02:1a:a6:75:06:87:52:4d:01:17:f2:62:
            8c:40:ad:29:e4:75:17:04:65:a9:b9:6a:dd:30:95:
            34:9b

        Exponent: 65537 (0x10001)

Signature Algorithm: sha256WithRSAEncryption

99:40:af:23:bb:cf:7d:59:e9:a5:83:78:37:02:76:83:79:02:
```

```

b3:5c:56:e8:c3:aa:fc:78:ef:07:23:f8:14:19:9c:a4:5d:88:

07:4d:6e:b8:0d:b5:af:fa:5c:f9:55:d0:60:94:d9:24:99:5e:
33:06:83:03:c3:73:c1:38:48:45:ba:6a:35:e6:e1:51:0e:92:

c3:a2:4a:a2:e1:2b:da:cd:0c:c3:17:ef:35:52:e1:6a:23:20:

af:99:95:a2:cb:99:a7:94:03:f3:78:99:bc:76:a3:0f:de:04:

7d:35:e1:dc:4d:47:79:f4:c8:4c:19:df:80:4c:4f:15:ab:f1:

61:a2:78:7a:2b:6e:98:f6:7b:8f:d6:55:44:16:79:e3:cd:51:

0e:27:fc:e6:4c:ff:bb:8f:2d:b0:ee:ed:98:63:e9:c9:cf:5f:

d7:b1:dd:7b:19:32:22:94:77:d5:bc:51:85:65:f3:e0:93:c7:

3c:79:fc:34:c7:9f:40:dc:b1:fc:6c:e5:3d:af:2d:77:b7:c3:

88:b3:89:7c:a6:1f:56:35:3b:35:66:0c:c8:05:b5:28:0b:98:

19:c7:b0:8e:dc:b7:3f:9d:c1:bb:69:f0:7d:20:95:b5:d1:f0:

06:35:b7:c4:64:ba:c4:95:31:4a:97:03:0f:04:54:6d:cb:50:

2f:31:02:59

```

Device#

Cisco vEdge デバイス では、**show certificate reverse-proxy** コマンドを実行して同様の出力を取得できます。

CLI を使用したリバースプロキシの監視

Cisco SD-WAN コントローラでの WAN エッジデバイスのプライベートおよびプロキシ IP アドレスとポート番号の監視

次に、Cisco SD-WAN コントローラ での **show control connections** コマンドの出力例を示します。WAN エッジデバイスの場合、コマンド出力の [PEER PRIVATE IP] および [PEER PRIV PORT] 列のエントリは、設定された TLOC IP アドレスと WAN エッジインターフェイスのポート番号です。[PEER PUBLIC IP] および [PEER PUB PORT] 列のエントリは、リバース プロキシ インターフェイスの対応する IP アドレスとポート番号です。同じコマンドを Cisco SD-WAN Manager インスタンスで実行した場合も、同様の出力が得られます。

vsmart1# **show control connections**

										PEER	
										PRIV	PEER
PUB	PEER	PEER	PEER		SITE	DOMAIN	PEER				
INDEX	TYPE	PROT	SYSTEM	IP	ID	ID	PRIVATE	IP	PORT	PUBLIC	IP
PORT	ORGANIZATION		REMOTE	COLOR	STATE	UPTIME					
0	vbond	dtls	172.16.1.2		0	0	10.1.1.2		12346	10.1.1.2	
12346	EXAMPLE-ORG		default		up	53:08:18:50					

```

0      vmanage tls 172.16.1.6      1      0      10.2.100.6 45689 10.2.100.6
45689  EXAMPLE-ORG default      up      53:08:18:32
1      vedge  tls 1.1.100.1      100    1      10.3.1.2 57853 10.2.100.1
53624  EXAMPLE-ORG biz-internet up      53:08:18:44
1      vedge  tls 1.1.101.1      101    1      10.4.1.2 55411 10.2.100.1
53622  EXAMPLE-ORG biz-internet up      53:08:18:48
1      vbond  dtls 172.16.1.2      0      0      10.1.1.2 12346 10.1.1.2
12346  EXAMPLE-ORG default      up      53:08:18:51

vsmart1#

```

SD-WAN コントローラのプライベート IP アドレスとポート番号から Cisco SD-WAN Validator のプロキシ IP アドレスとポート番号へのマッピングの表示

次に、Cisco SD-WAN Validator での **show orchestrator reverse-proxy-mapping** コマンドの出力例を示します。コマンド出力の [PROXY IP] 列と [PROXY PORT] 列のエントリは、プロキシの IP アドレスとポート番号です。[PRIVATE IP] 列と [PRIVATE PORT] 列のエントリは、VPN 0 のトランスポート インターフェイスのプライベート IP アドレスとポート番号です。

```
vbond# show orchestrator reverse-proxy-mapping
```

	PRIVATE		PROXY	
UUID	PRIVATE IP	PORT	PROXY IP	PORT

14c35ae4-69e3-41c5-a62f-725c839d25df	10.2.100.4	23456	10.2.1.10	23458
14c35ae4-69e3-41c5-a62f-725c839d25df	10.2.100.4	23556	10.2.1.10	23558
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23456	10.2.1.10	23457
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23556	10.2.1.10	23557
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23656	10.2.1.10	23657
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23756	10.2.1.10	23757
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23856	10.2.1.10	23857
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23956	10.2.1.10	23957
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	24056	10.2.1.10	24057
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	24156	10.2.1.10	24157

```
vbond#
```

例：SD-WAN コントローラのプライベート IP アドレスとポート番号から WAN エッジデバイスのプロキシ IP アドレスとポート番号へのマッピングを表示する

次に、Cisco IOS XE Catalyst SD-WAN デバイス での **show sdwan control connections** コマンドの出力例を示します。コマンド出力で、Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ の [PROXY] 列のエントリを確認します。エントリが [Yes] の場

合、[PEER PUBLIC IP] および [PEER PUBLIC PORT] のエントリはプロキシ IP アドレスとポート番号です。

Device# **show sdwan control connections**

				CONTROLLER		PEER		PEER	
PEER	PEER	PEER		SITE	DOMAIN	PEER	PRIV	PEER	PUB
				GROUP					
TYPE	PROT	SYSTEM	IP	ID	ID	PRIVATE	IP	PORT	PUBLIC
ORGANIZATION		LOCAL	COLOR	PROXY	STATE	UPTIME	ID		IP
									PORT
vsmart	tls	172.16.1.4		1	1	10.2.100.4		23558	10.2.1.10
EXAMPLE-ORG		biz-internet		Yes	up	52:08:44:25	0		23558
vbond	dtls	0.0.0.0		0	0	10.1.1.2		12346	10.1.1.2
EXAMPLE-ORG		biz-internet		-	up	52:08:50:47	0		12346
vmanage	tls	172.16.1.6		1	0	10.2.100.6		23957	10.2.1.10
EXAMPLE-ORG		biz-internet		Yes	up	66:03:04:50	0		23957

Device#

Cisco vEdge デバイス では、**show control connections** コマンドを実行して同様の出力を取得できます。

リバースプロキシとの認証のために **WAN** エッジデバイスにインストールされた署名付き証明書の表示

次に、Cisco IOS XE Catalyst SD-WAN デバイス での **show sdwan certificate reverse-proxy** コマンドの出力例を示します。

Device# **show sdwan certificate reverse-proxy**

Reverse proxy certificate

Certificate:

Data:

Version: 1 (0x0)

Serial Number: 1 (0x1)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = US, CN = 6c63e80a-8175-47de-a455-53a127ee70bd, O = Viptela

Validity


```
Not Before: Jun  2 19:31:08 2021 GMT
Not After  : May 27 19:31:08 2051 GMT

Subject: C = US, ST = California, CN = C8K-9AE4A5A8-4EB0-E6C1-1761-6E54E4985F78,
O = ViptelaClient
Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

    00:e2:45:49:53:3a:56:d4:b8:70:59:90:01:fb:b1:
    44:e3:73:17:97:a3:e9:b7:55:44:d4:2d:dd:13:4a:
    a8:ef:78:14:9d:bd:b5:69:de:c9:31:29:bd:8e:57:
    09:f2:02:f8:3d:1d:1e:cb:a3:2e:94:c7:2e:61:ea:
    e9:94:3b:28:8d:f7:06:12:56:f3:24:56:8c:4a:e7:
    01:b1:2b:1b:cd:85:4f:8d:34:78:78:a1:26:17:2b:
    a5:1b:2a:b6:dd:50:51:f8:2b:13:93:cd:a6:fd:f8:
    71:95:c4:db:fc:a7:83:05:23:68:61:15:05:cc:aa:
    60:af:09:ef:3e:ce:70:4d:dd:50:84:3c:9a:57:ce:
    cb:15:84:3e:cd:b2:b6:30:ab:86:68:17:94:fa:9c:
    1a:ab:28:96:68:8c:ef:c8:f7:00:8a:7a:01:ca:58:
    84:b0:87:af:9a:f6:13:0f:aa:42:db:8b:cc:6e:ba:
    c8:c1:48:d2:f4:d8:08:b1:b5:15:ca:36:80:98:47:
    32:3a:df:54:35:fe:75:32:23:9f:b5:ed:65:41:99:
    50:b9:0f:7a:a2:10:59:12:d8:3e:45:78:cb:dc:2a:
    95:f2:72:02:1a:a6:75:06:87:52:4d:01:17:f2:62:
    8c:40:ad:29:e4:75:17:04:65:a9:b9:6a:dd:30:95:
    34:9b

Exponent: 65537 (0x10001)

Signature Algorithm: sha256WithRSAEncryption

    99:40:af:23:bb:cf:7d:59:e9:a5:83:78:37:02:76:83:79:02:
    b3:5c:56:e8:c3:aa:fc:78:ef:07:23:f8:14:19:9c:a4:5d:88:
    07:4d:6e:b8:0d:b5:af:fa:5c:f9:55:d0:60:94:d9:24:99:5e:
    33:06:83:03:c3:73:c1:38:48:45:ba:6a:35:e6:e1:51:0e:92:
    c3:a2:4a:a2:e1:2b:da:cd:0c:c3:17:ef:35:52:e1:6a:23:20:
```

```
af:99:95:a2:cb:99:a7:94:03:f3:78:99:bc:76:a3:0f:de:04:
7d:35:e1:dc:4d:47:79:f4:c8:4c:19:df:80:4c:4f:15:ab:f1:
61:a2:78:7a:2b:6e:98:f6:7b:8f:d6:55:44:16:79:e3:cd:51:
0e:27:fc:e6:4c:ff:bb:8f:2d:b0:ee:ed:98:63:e9:c9:cf:5f:
d7:b1:dd:7b:19:32:22:94:77:d5:bc:51:85:65:f3:e0:93:c7:
3c:79:fc:34:c7:9f:40:dc:b1:fc:6c:e5:3d:af:2d:77:b7:c3:
88:b3:89:7c:a6:1f:56:35:3b:35:66:0c:c8:05:b5:28:0b:98:
19:c7:b0:8e:dc:b7:3f:9d:c1:bb:69:f0:7d:20:95:b5:d1:f0:
06:35:b7:c4:64:ba:c4:95:31:4a:97:03:0f:04:54:6d:cb:50:
2f:31:02:59
```

Device#

Cisco vEdge デバイス では、**show certificate reverse-proxy** コマンドを実行して同様の出力を取得できます。



第 12 章

モジュラ型 Cisco ASR 1000 シリーズインターフェイスのオンボーディング

- [Cisco ASR 1006-X と RP3 モジュール \(371 ページ\)](#)
- [RP3 モジュールを搭載した Cisco ASR 1006-X に関する情報 \(371 ページ\)](#)
- [Cisco ASR 1006-X シャーシの RMA 交換 \(374 ページ\)](#)
- [Cisco RP3 モジュールの RMA 交換 \(378 ページ\)](#)

Cisco ASR 1006-X と RP3 モジュール

表 43: 機能の履歴

機能名	リリース情報	説明
RP3 モジュールを搭載した Cisco ASR 1006-X プラットフォームの Cisco Catalyst SD-WAN サポート	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	このリリース以降、Cisco Catalyst SD-WAN は、Cisco ASR 1000 シリーズルートプロセッサ 3 モジュールを搭載した Cisco ASR 1006-X プラットフォームをサポートします。

RP3 モジュールを搭載した Cisco ASR 1006-X に関する情報

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a、Cisco vManage リリース 20.5.1

サポートされている最新リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.12.x、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.12.x

Cisco Catalyst SD-WAN は、Cisco ASR 1000 シリーズルートプロセッサ 3 (Cisco ASR1000-RP3) モジュールを搭載した Cisco ASR 1006-X プラットフォームをサポートしています。



(注) Cisco Catalyst SD-WAN は、Cisco ASR 1006-X および RP3 モジュールが Cisco Catalyst SD-WAN で動作するユニットとして注文された場合にのみ、この構成をサポートします。

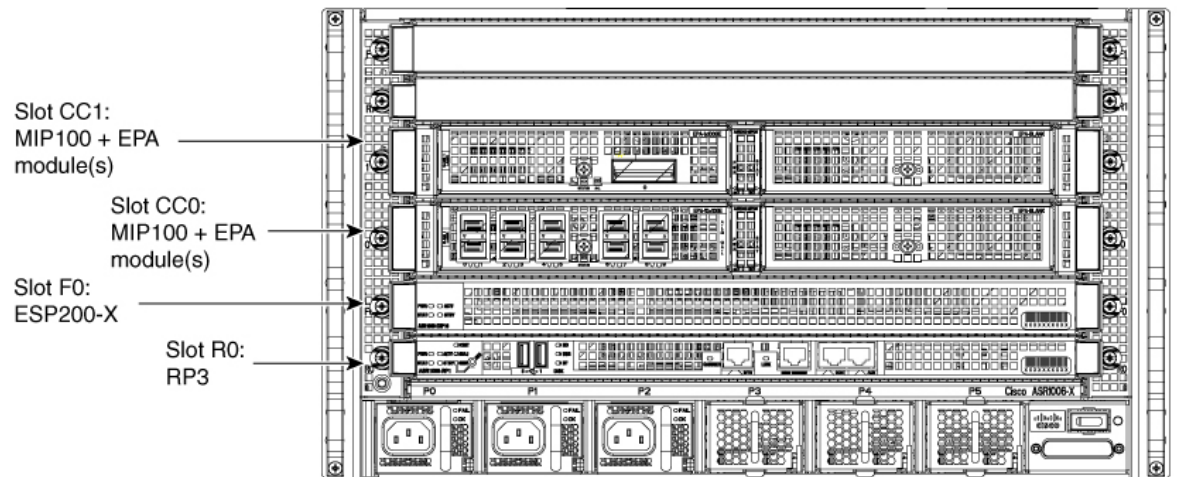
ハードウェア構成

Cisco ASR 1006-X は、次の構成で Cisco Catalyst SD-WAN とともに動作します。

表 44: ハードウェア構成

ASR 1006-X スロット	内容
R0	Cisco ASR 1000 シリーズ ルートプロセッサ 3 (Cisco ASR1000-RP3) モジュール
F0	Cisco ASR 1000 シリーズ 200 Gbps エンベデッド サービス プロセッサ (ASR1000-ESP200-X)
CC0	Cisco ASR1000-MIP100 キャリアカード+キャリアのサブスロットに 1 枚または 2 枚の EPA カード (注) サポートされている EPA カードについては、以下を参照してください。 キャリアで EPA カードを 1 枚だけ使用する場合は、EPA カードをいずれかのサブスロットに配置できます。
CC1	Cisco ASR1000-MIP100 キャリアカード+キャリアのサブスロットに 1 枚または 2 枚の EPA カード (注) サポートされている EPA カードについては、以下を参照してください。 キャリアで EPA カードを 1 枚だけ使用する場合は、EPA カードをいずれかのサブスロットに配置できます。
R1	このスロットは空にする必要があります。
F1	このスロットは空にする必要があります。

図 28 : Cisco ASR 1006-X スロットおよびモジュール



ASR1000-MIP100 キャリアカードおよび EPA カードの取り付けについては、『[Cisco ASR 1000 Series Modular Interface Processor Hardware Installation Guide](#)』を参照してください。

サポートされているカードおよびモジュール

次のイーサネットポートアダプタ（EPA）カードがサポートされています。各 ASR1000-MIP100 キャリアカードは 2 枚の EPA カードをサポートし、合計で最大 4 枚の EPA カードを取り付けることができます。

- 10 ポート 10 ギガビットイーサネット（10x10G） :
EPA-10X10GE
- 2 ポート 40 ギガビットイーサネット（2x40G） :
EPA-2X40GE
- 1 ポート 100 ギガビットイーサネット（1x100G） :
EPA-QSFP-1X100GE

注意事項と制限事項

• ハードウェア冗長性

上記のハードウェア構成の表に示されているように、1 つの ASR1000-RP3 と 1 つの ASR1000-ESP200-X のみを使用します。この Cisco Catalyst SD-WAN の使用例における Cisco ASR 1006-X については、デュアル RP モジュールまたはデュアル ESP ハードウェアの冗長性はサポートされません。

• ISSU および OIR

これらのモジュールおよびカードは、In-Service Software Upgrade（ISSU）または活性挿抜（OIR）をサポートしていません。

ROM モニタ ソフトウェア バージョン

- Cisco ASR 1006-X プラットフォームの場合、特定の ROM モニタ（ROMmon）のバージョン要件はありません。
- RP3 モジュールには、ROM モニタ（ROMmon）ソフトウェアバージョン 16.9(5r) 以降が必要です。

オンボーディング ワークフロー

1. Cisco ASR 1006-X が、「[Hardware Configuration](#)」および「[ROM Monitor Software Version](#)」で説明されている要件を満たしていることを確認します。
2. 「[Cisco Plug and Play Support Guide for Cisco SD-WAN Products](#)」で説明されているプラグアンドプレイ オンボード手順に従います。
3. 「[Plug and Play Onboarding Workflow](#)」で説明されている Cisco Catalyst SD-WAN オンボーディング手順に従います。

Cisco ASR 1006-X シャーシの RMA 交換

返品許可（RMA）プロセスの一部として、Cisco ASR 1006-X シャーシを交換する必要がある場合は、この手順を使用します。この手順では、Cisco ASR 1006-X シャーシを置き換えますが、現在のカード（RP3 モジュール、ESP200 モジュール、MIP100 キャリアカード、EPA カード）は維持されます。

はじめる前に

- RP3 モジュールを搭載した Cisco ASR 1006-X（現在は故障中）が Cisco SD-WAN Manager に完全にオンボードされている。
- 次のシリアル番号を書き留めている。
 - 交換用 Cisco ASR 1006-X シャーシのシリアル番号
 - RP3 モジュールの証明書シリアル番号
 - RP3 モジュールの SUDI シリアル番号

Cisco ASR 1006-X シャーシの交換

Cisco ASR 1006-X シャーシを交換するには、次の手順を実行します。



(注) Cisco SD-WAN Manager のデバイスの一覧表では、Cisco ASR 1006-X シャーシとそのシャーシに取り付けられている RP3 モジュールが区別されません。表の単一の行に、両方の情報を組み合わせたものが表示されます。

1. (この手順は、機能テンプレートを現在のデバイス（現在は故障中）に適用しており、既存の構成を保存して交換用デバイスで使用する場合にのみ実行してください)
RP3 モジュールのデバイス設定ファイルを保存します。
 1. Cisco SD-WAN Manager のメニューから、**[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. RP3 モジュールを含む Cisco ASR 1006-X にアタッチされているテンプレートの [...] をクリックし、**[Export CSV]** を選択してデバイス設定の CSV ファイルをダウンロードします。
2. Cisco Plug and Play (PnP) Connect Web ポータルで、現在の Cisco ASR 1006-X シャーシを削除します。



(注) PnP Connect Web ポータルは、Cisco Commerce Workspace (CCW) とリンクされており、購入したデバイスのシリアル番号と PID を PnP Connect Web ポータルに自動登録できるようになっています。詳細については、『[Cisco Plug and Play Support Guide for Cisco SD-WAN Products](#)』と、『[Cisco Network Plug and Play Connect Capability Overview](#)』の RMA に関するトピックを参照してください。



(注) PnP Connect Web ポータルの機能は、今後変更される可能性があります（このドキュメントの説明範囲外です）。詳細については、PnP Connect Web ポータルのドキュメントを参照してください。

- PnP Connect Web ポータルで、**[Devices] > [Delete Selected Device]**（または同等のもの）を使用して、現在の Cisco ASR 1006-X シャーシを削除します。
3. Cisco Plug and Play (PnP) Connect Web ポータルで、交換用 Cisco ASR 1006-X シャーシを追加します。

1. PnP Connect Web ポータルで、**[Devices] > [Add Device]**（または同等のもの）を選択し、新しいデバイスの詳細情報を入力するオプションを選択します。
2. 交換用 Cisco ASR 1006-X シャーシのシリアル番号を入力します。



(注) Cisco ASR 1006-X ルータで **show pnp version** コマンドを使用すると、シリアル番号を表示できます。

3. RP3 モジュールの SUDI シリアル番号および証明書シリアル番号を追加します。



(注) RP3 モジュールが動作中のシャーシに取り付けられている場合は、**show sdwan certificate serial** コマンドを使用してそれらのシリアル番号を表示できます。

4. 更新内容を保存します。

4. Cisco SD-WAN Manager で、現在の Cisco ASR 1006-X シャーシのエントリを削除します。

1. Cisco SD-WAN Manager で、現在のデバイステンプレートを現在の Cisco ASR 1006-X シャーシから切り離します。
2. Cisco SD-WAN Manager メニューから **[Configuration] > [Certificates]** の順に選択します。
3. 現在の Cisco ASR 1006-X の行で、[Validate] 列の [Invalid] をクリックし、[OK] をクリックします。
タスクビューには、プロセスがいつ完了するのかが示されます。
4. [Send to Controllers] をクリックします。
5. Cisco SD-WAN Manager メニューから、**[Configuration] > [Devices]** の順に選択します。
6. 現在の Cisco ASR 1006-X の行で、[More Options] ([...]) をクリックし、[Delete WAN Edge] を選択します。

5. Cisco SD-WAN Manager メニューから **[Configuration] > [Devices]** の順に選択し、[Sync Smart Account] をクリックします。

Cisco SD-WAN Manager は、スマートアカウントから交換用 Cisco ASR 1006-X シャーシの詳細情報をロードします。

6. 前の手順で CSV ファイルを保存した場合は、そのファイルを編集して交換用シャーシのデバイス ID で更新します。
 1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Devices] > [WAN Edge List]** の順に選択します。

2. デバイスリストの [Chassis Number] 列から新しいシャーシのデバイス ID をコピーします。
 3. テキストエディタまたはスプレッドシート アプリケーションで CSV ファイルを開き、最初の列の csv-deviceId 値を編集して、新しいシャーシのデバイス ID を使用するように更新します。
7. デバイステEMPLATEを交換用 Cisco ASR 1006-X にアタッチします。以前のシャーシに使用していたものと同じデバイステEMPLATEを使用してください。以前の手順で CSV ファイルを保存した場合は、以降のサブ手順でそれを使用してください。
1. Cisco SD-WAN Manager のメニューから、**[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. 現在のシャーシに以前にアタッチされていたテンプレートの行で、**[More Actions]** ([...]) をクリックし、**[Attach Devices]** を選択します。
 4. **[Available Devices]** ペインで、交換用シャーシを選択し、それを **[Selected Devices]** ペインに移動させます。
 5. **[Attach]** をクリックします。**[Configuration Templates]** ページが開きます。
 6. 前の手順で CSV ファイルを保存した場合は、**上矢印** ボタンをクリックして CSV ファイルをアップロードします。
 7. 前の手順で CSV ファイルを保存した場合は、**[Upload CSV File]** ポップアップウィンドウで、前の手順で編集した CSV ファイルを選択し、**[Upload]** をクリックします。CSV ファイルに保存されている値がデバイステEMPLATEにコピーされます。
 8. **[Next]** をクリックします。
 9. **[Configure Devices]** をクリックしてデバイステEMPLATEを交換用 Cisco ASR 1006-X シャーシにプッシュします。交換用デバイスにはまだ到達できないため、タスクステータスには、このタスクが「**Scheduled**」（スケジュール済み）と表示されます。
8. デバイス構成ファイルを保存します。
1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Devices] > [WAN Edge List]** の順に選択します。
 2. Cisco ASR 1006-X の行で、**[More Options]** ([...]) をクリックし、**[Generate Bootstrap Configuration]** を選択します。
 3. ポップアップウィンドウで、**[Cloud-Init]** オプションボタンをクリックします。

4. [Download] をクリックして構成ファイルをダウンロードします。
 5. ダウンロードしたファイルの名前を `ciscosdwan.cfg` に変更します。
 9. 前の手順で作成したブートストラップファイル (`ciscosdwan.cfg`) を USB フラッシュドライブにコピーし、それを現在の RP3 モジュールに接続します。
 10. 現在の Cisco ASR 1006-X シャーシがまだ動作している場合は、電源を切ります。
 11. 現在の Cisco ASR 1006-X シャーシからモジュールとカード (RP3 モジュール、ESP200 モジュール、MIP100 キャリアカード、EPA カード) を取り外します。
 12. 前の手順で構成ファイルを保存した USB フラッシュドライブを RP3 モジュールに接続します。
 13. モジュールとカードを新しい Cisco ASR 1006-X シャーシに取り付けます。
RP3 モジュールの取り付けについては、『[Cisco ASR 1000 Route Processor 3 Installation and Configuration Guide](#)』を参照してください。
MIP100 および EPA の取り付けについては、『[Cisco ASR 1000 MIP and EPA Hardware Installation Guide](#)』を参照してください。
 14. 交換用 Cisco ASR 1006-X ルータの電源を入れます。
 15. ルータの電源を入れたら、ルータで **controller-mode reset** コマンドを実行して RP3 モジュールをリセットします。
- RP3 モジュールが起動すると、次のことが発生します。
- RP3 モジュールが USB フラッシュドライブの `ciscosdwan.cfg` ファイルから構成をロードします。
 - RP3 モジュールがコントローラモードで起動します。



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a では、コントローラモードはサポートされていません。

- コントローラへの接続が確立されると、コントローラが「Scheduled」状態のデバイステンプレートを RP3 モジュールにプッシュします。

Cisco RP3 モジュールの RMA 交換

返品許可 (RMA) プロセスの一部として、Cisco ASR 1006-X で使用されている RP3 モジュールを交換する必要がある場合は、この手順を使用します。

前提条件

- RP3 モジュール（現在は故障中）を搭載した Cisco ASR 1006-X が Cisco SD-WAN Manager にオンボードされている。
- 次のシリアル番号を書き留めている。
 - Cisco ASR 1006-X シャーシのシリアル番号
 - 交換用 RP3 モジュールの証明書シリアル番号
 - 交換用 RP3 モジュールの SUDI シリアル番号

Cisco RP3 モジュールの交換

Cisco RP3 モジュールを交換するには、次の手順を実行します。



- (注) Cisco SD-WAN Manager のデバイスの一覧表では、Cisco ASR 1006-X シャーシとそのシャーシに取り付けられている RP3 モジュールが区別されません。表の単一の行に、両方の情報を組み合わせたものが表示されます。

1. （この手順は、機能テンプレートを現在のデバイス（現在は故障中）に適用しており、既存の構成を保存して交換用デバイスで使用する場合にのみ実行してください）

RP3 モジュールのデバイス設定ファイルを保存します。

1. Cisco SD-WAN Manager のメニューから、**[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. RP3 モジュールを含む Cisco ASR 1006-X にアタッチされているテンプレートの **[More Options] ([...])** をクリックし、**[Export CSV]** を選択してデバイス設定の CSV ファイルをダウンロードします。
2. RP3 モジュールのデバイス構成ファイルを保存します。
 1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Devices] > [WAN Edge List]** の順に選択します。
 2. RP3 モジュールを含む Cisco ASR 1006-X の行で、**[More Options] ([...])** をクリックし、**[Generate Bootstrap Configuration]** を選択します。
 3. ポップアップウィンドウで、**[Cloud-Init]** オプションボタンをクリックします。

4. [Download] をクリックして構成ファイルをダウンロードします。
 5. ダウンロードしたファイルの名前を ciscosdwan.cfg に変更します。
3. 交換用 RP3 モジュールのシリアル番号を使用するために、Cisco Plug and Play (PnP) Connect Web ポータルで、Cisco ASR 1006-X エントリ内の SUDI シリアル番号および証明書シリアル番号を更新します。



- (注) PnP Connect Web ポータルは、Cisco Commerce Workspace (CCW) とリンクされており、購入したデバイスのシリアル番号と PID を PnP Connect Web ポータルに自動登録できるようになっています。詳細については、『[Cisco Plug and Play Support Guide for Cisco Catalyst SD-WAN Products](#)』と、『[Cisco Network Plug and Play Connect Capability Overview](#)』の RMA に関するトピックを参照してください。



- (注) PnP Connect Web ポータルの機能は、今後変更される可能性があります（このドキュメントの説明範囲外です）。詳細については、PnP Connect Web ポータルのドキュメントを参照してください。

1. PnP Connect Web ポータルで、[Devices] > [Edit Device] の順に選択し、交換する RP3 モジュールを含むデバイスの Cisco ASR 1006-X エントリを選択します。
 2. Cisco ASR 1006-X エントリで、既存の RP3 モジュールエントリ（複数存在する場合があります）の SUDI シリアル番号および証明書シリアル番号を削除します。
 3. 交換用 RP3 モジュールの SUDI シリアル番号および証明書シリアル番号を追加します。
 4. 更新内容を保存します。
4. Cisco SD-WAN Manager で、現在の RP3 モジュールを取り外し、交換用 RP3 モジュールを追加します。
 1. Cisco SD-WAN Manager メニューから [Configuration] > [Certificates] の順に選択します。
 2. RP3 モジュールを含む Cisco ASR 1006-X デバイスの行で、[Validate] 列の [Invalid] をクリックし、[OK] をクリックします。
タスクビューには、プロセスがいつ完了するのかが示されます。
 3. [Send to Controllers] をクリックします。
 4. Cisco SD-WAN Manager メニューから、[Configuration] > [Devices] の順に選択します。
 5. RP3 モジュールを含む Cisco ASR 1006-X デバイスの行で、[More Options] ([...]) をクリックし、[Delete WAN Edge] を選択します。

6. Cisco SD-WAN Manager メニューから **[Configuration] > [Devices]** の順に選択し、[Sync Smart Account] をクリックします。

Cisco SD-WAN Manager は、交換用 RP3 モジュールの詳細情報をロードします。この時点で（RP3 モジュールを物理的に交換する前に）、デバイステーブルの Cisco ASR 1006-X デバイスの行には次のように表示されます。

- デバイスモデル：ASR1006-X
- シャーシ番号：シャーシ番号は変更されません
- シリアル番号/トークン：スマートアカウントからロードされた交換用 RP3 モジュールのシリアル番号を表示するように更新されています

5. デバイステンプレートを交換用 Cisco ASR 1006-X にアタッチします。以前のシャーシに使用していたものと同じデバイステンプレートを使用してください。以前の手順で CSV ファイルを保存した場合は、以降のサブ手順でそれを使用してください。

1. Cisco SD-WAN Manager のメニューから、**[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. 現在のシャーシに以前にアタッチされていたテンプレートの行で、**[More Actions]** ([...]) をクリックし、**[Attach Devices]** を選択します。
 4. **[Available Devices]** ペインで、交換用シャーシを選択し、それを **[Selected Devices]** ペインに移動させます。
 5. **[Attach]** をクリックします。**[Configuration Templates]** ページが開きます。
 6. 前の手順で CSV ファイルを保存した場合は、**上矢印** ボタンをクリックして CSV ファイルをアップロードします。
 7. 前の手順で CSV ファイルを保存した場合は、**[Upload CSV File]** ポップアップウィンドウで CSV ファイルを選択し、**[Upload]** をクリックします。CSV ファイルに保存されている値がデバイステンプレートにコピーされます。
 8. **[Next]** をクリックします。
 9. **[Configure Devices]** をクリックしてデバイステンプレートを交換用 Cisco ASR 1006-X シャーシにプッシュします。交換用デバイスにはまだ到達できないため、タスクステータスには、このタスクが「**Scheduled**」（スケジュール済み）と表示されます。
6. 前の手順で作成したブートストラップファイル（ciscosdwan.cfg）を USB フラッシュドライブにコピーし、それを交換用 RP3 モジュールに接続します。

7. Cisco ASR 1006-X シャーシから既存の RP3 モジュールを取り外し、交換用 RP3 モジュールを取り付けます。

RP3 モジュールの取り付けについては、『[Cisco ASR 1000 Route Processor 3 Installation and Configuration Guide](#)』を参照してください。

RP3 モジュールが起動すると、次のことが発生します。

- RP3 モジュールが USB フラッシュドライブの `ciscosdwan.cfg` ファイルから構成をロードします。
- RP3 モジュールがコントローラモードで起動します。



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a では、コントローラモードはサポートされていません。

- コントローラへの接続が確立されると、コントローラが「Scheduled」状態のデバイステンプレートを RP3 モジュールにプッシュします。



第 13 章

API クロスサイト リクエスト フォーजेリの防止

表 45: 機能の履歴

機能名	リリース情報	説明
API クロスサイト リクエスト フォーजेリの防止	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b Cisco Catalyst SD-WAN リリース 19.2.1	この機能により、Cisco Catalyst SD-WAN REST API の使用時に発生するクロスサイト リクエスト フォーजेリ (CSRF) に対する保護が追加されます。この保護は、API リクエストに CSRF トークンを含めることによって提供されます。リクエストを許可リストに含めて、必要に応じて保護を不要にできます。

- [Cisco Catalyst SD-WAN REST API トークンベース認証 \(383 ページ\)](#)
- [トークンの使用 \(384 ページ\)](#)
- [API ドキュメント \(384 ページ\)](#)
- [サードパーティ製アプリケーションのユーザー \(384 ページ\)](#)

Cisco Catalyst SD-WAN REST API トークンベース認証

Cisco Catalyst SD-WAN リリース 19.2 では、Cisco Catalyst SD-WAN REST API を使用する場合にトークンベースの認証が提供されます。この保護は、トークンを API リクエストに含めるよう要求することによって提供されます。各 API セッションは、セッション全体で有効な一意のトークンを使用します。API リクエストにこのトークンが含まれていない場合、エンドポイントが許可リストに含まれていない限り、Cisco SD-WAN Manager はリクエストを拒否します (エンドポイントを許可リストに追加する方法に関するお問い合わせは、Cisco TAC またはエスカレーション サポート チームでケースを開いてください)。



(注) ただし、許可リストに含まれていない Cisco SD-WAN Manager の一部の GET API およびすべての POST API では、クロスサイトリクエストフォージェリ (CSRF) トークン認証が必要です。

トークンの使用

次のセクションでは、API ドキュメントまたはサードパーティアプリケーションを使用するときに、トークンが API でどのように使用されるかについて説明します。

API ドキュメント

Cisco SD-WAN Manager はトークンを自動的に生成し、[Cisco SD-WAN Manager API Docs] ページから送信するすべてのリクエストにトークンを追加します。このプロセスではユーザーのアクションは不要です。また、[API Docs] ページの操作方法は、以前のリリースと同じです。

このトークンベースの認証から除外する API リクエストがある場合は、Cisco TAC またはエスカレーション サポート チームにケースをオープンして、それらの API エンドポイントを許可リストに含めるように要求できます。

サードパーティ製アプリケーションのユーザー

Cisco SD-WAN Manager API リクエストにスクリプトまたはサードパーティ アプリケーション (Postman、LiveAction、SolarWinds、SevOne など) を使用する場合は、API が許可リストに含まれていないかぎり、各リクエストにトークンを含める必要があります。API リクエストにトークンが含まれておらず、許可リストにも含まれていない場合、Cisco SD-WAN Manager は、リクエストを拒否し、応答コード 403 (禁止) と「SessionTokenFilter: Token provided via HTTP Header does not match the token generated by the server.」というメッセージを返します。

特定の API エンドポイントを許可リストに含めるように要求するには、Cisco TAC またはエスカレーション サポート チームとのケースをオープンします。

サードパーティ API リクエストにトークンを含めるには、次の手順を実行します。

方法 1

最初の方法では、作成するセッションが cookies.txt ファイルに保存されます。ファイルに含まれる jsessionid を使用して、以降のすべてのリクエストに同じセッションを使用できます。これは推奨される方法です。

1. Cisco SD-WAN Manager にログインするには、次のコマンド例を使用し、目的の IP アドレスに従って URL を変更します。


```
sampleuser$ TOKEN=$(curl "https://209.165.200.254/dataservice/client/token" -X GET
-b cookies.txt -s -insecure)
```

ログインを確認するには、`cookies.txt` ファイルを参照してください。

2. Cisco SD-WAN Manager にログインした後、リクエストを送信してトークンを取得します。ここで、`vManage_IP` は、Cisco SD-WAN Manager サーバーの IP アドレスです。トークンは、文字列形式または JSON 形式で取得できます。

文字列形式でトークンを取得するには、次の URL を使用します。

```
https://vManage_IP/dataservice/client/token
```

JSON 形式でトークンを取得するには（Cisco IOS XE SD-WAN リリース 16.12 および Cisco SD-WAN リリース 19.2 以降）、次の URL を使用します。

```
https://vManage_IP/dataservice/client/token?json=true
```

これらのコールが返すトークンは、現在のセッションの残りの期間有効です。次の例は、トークンを取得するためのリクエストを示しています。

文字列形式でトークンを取得するコマンド：

```
sampleuser$ TOKEN=$(curl "https://vManage_IP/dataservice/client/token" -X GET -b
cookies.txt -s -insecure)
```

文字列形式の出力：

```
FC5B19BB3521EE20CFBDCD3CEDCC48F50CB1095C9654407936029E9C0EF99FEAE50440B60E49F7CD4A0BAB5307C2855F2E0C
```

JSON 形式でトークンを取得するためのコマンド：

```
TOKEN=$(curl "https://vManage_IP/dataservice/client/token?json=true" -X GET -b
cookies.txt -s -insecure)
```

JSON 形式の出力：

```
sampleuser$ echo $TOKEN
```

```
{"token":"56CF324A8F67993B6FCCF57302068B0756DA8703BE712EFA18D4D9055B11312843F9D30B48A3902320FFAA8659AD01202A63"}
```



(注) `curl` コマンドでは JSON 形式はサポートされていません。

3. 現在のセッションにおける後続の各 API リクエストのヘッダーに、生成したトークンで構成される値を使用した `X-XSRF-TOKEN` キーを含めます。

次の例は、生成されたトークンがヘッダーに含まれている GET リクエストと POST リクエストを示しています。

コマンド：

```
sampleuser$ curl "https://vManage_IP/dataservice/server/info" -b cookies.txt -silent
-insecure -H "X-XSRF-TOKEN: $TOKEN"
```

出力：

```
{"Achitecture":"amd64","Available processors":2}
```

コマンド

```
sampleuser$ curl
"https://vManage_IP/dataservice/settings/configuration/emailNotificationSettings" -X
POST -b cookies.txt -silent -insecure -H "X-XSRF-TOKEN: $TOKEN" -d
'{"enabled":true,"from_address":"test@mydomain.com","protocol":"smtp","smtp_server":"a.com",
"smtp_port":25,"reply_to_address":"test@test.com","notification_use_smtp_authentication":false}='
```

出力:

```
{"data":[{"enabled":true,"notification_use_email_setting_authentication":false,"notification_use_smtp_authentication":false}]}
```

4. Cisco SD-WAN リリース 19.2.1 以降では、メモリリークを防ぐために、トークンを含む各 API コールの後にログアウトする必要があります。

次の例は、ログアウトする方法を示しています。

コマンド:

```
sampleuser$ curl "https://vManage_IP/logout" -b cookies.txt -insecure -H
"X-XSRF-TOKEN:$TOKEN"
```

出力:

```
Replaced cookie JSESSIONID="DcOke5mqix_15qCpWA1blIJVAMnVg3lDMU4ABRgVinvalid" for
domain 209.165.200.254, path /, expire 0
< set-cookie: JSESSIONID=DcOke5mqix_15qCpWA1blIJVAMnVg3lDMU4ABRgVinvalid
```



- (注) セッションからログアウトしたことを確認するには、jsessionidをチェックし、それが「invalid」で終わっていることを確認します。

方法 2

2 つ目の方法では、作成するセッションは保存されず、リクエストごとに新しいセッションを作成する必要があります。

1. Cisco SD-WAN Manager にログインした後、リクエストを送信してトークンを取得します。ここで、vManage_IP は、Cisco SD-WAN Manager サーバーの IP アドレスです。トークンは、文字列形式または JSON 形式で取得できます。

文字列形式でトークンを取得するには、次の URL を使用します。

```
https://vManage_IP/dataservice/client/token
```

JSON 形式でトークンを取得するには（Cisco IOS XE SD-WAN リリース 16.12 および Cisco SD-WAN リリース 19.2 以降）、次の URL を使用します。

```
https://vManage_IP/dataservice/client/token?json=true
```

これらのコールが返すトークンは、現在のセッションの残りの期間有効です。次の例は、トークンを取得するためのリクエストを示しています。

文字列形式でトークンを取得するコマンド:

```
sampleuser$ curl --user admin:admin https://vManage_IP/dataservice/client/token
--insecure
```

文字列形式の出力：

```
FC5B19BB3521EE20CFBDCD3CEDCC48F50CB1095C9654407936029E9C0EF99FEAE50440B60E49F7CD4A0BAB5307C2855F2E0C
```

JSON 形式でトークンを取得するためのコマンド：

```
sampleuser$ curl --user admin:admin
https://vManage_IP/dataservice/client/token?json=true --insecure
{"token":"F1E047E444DB2CA4237B0246DFE133345584B788C6E8776F04749A371B73F300C683043F1CDBB5E01EBBDA7D6C35F58EA37A"}
```

JSON 形式の出力：

```
FC5B19BB3521EE20CFBDCD3CEDCC48F50CB1095C9654407936029E9C0EF99FEAE50440B60E49F7CD4A0BAB5307C2855F2E0C
```

2. 現在のセッションにおける後続の各 API リクエストのヘッダーに、生成したトークンで構成される値を使用した X-XSRF-TOKEN キーを含めます。

次の例は、生成されたトークンがヘッダーに含まれている GET リクエストと POST リクエストを示しています。

コマンド：

```
sampleuser$ curl "https://vManage_IP/dataservice/server/info" -H "Cookie:
JSESSIONID=pSwrx3AEWokiD01TkFiOjgSehp-ITNdfn7Xj9PsL.c331d01e-91d7-41cc-ab90-b629c2ae6d97"
--insecure -H "X-XSRF-TOKEN=
FC5B19BB3521EE20CFBDCD3CEDCC48F50CB1095C9654407936029E9C0EF99FEAE50440B60E49F7CD4A0BAB5307C2855F2E0C"
```

出力：

```
{"Achitecture":"amd64","Available processors":2}
```

コマンド

```
sampleuser$
"https://vManage_IP/dataservice/settings/configuration/emailNotificationSettings" -H
"Cookie:
JSESSIONID=pSwrx3AEWokiD01TkFiOjgSehp-ITNdfn7Xj9PsL.c331d01e-91d7-41cc-ab90-b629c2ae6d97"
--insecure -H "X-XSRF-TOKEN=
FC5B19BB3521EE20CFBDCD3CEDCC48F50CB1095C9654407936029E9C0EF99FEAE50440B60E49F7CD4A0BAB5307C2855F2E0C"
-X POST --insecure -d
'{"enabled":true,"from_address":"test@mydomain.com","protocol":"smtp","smtp_server":"a.com",
"smtp_port":25,"reply_to_address":"test@test.com","notification_use_smtp_authentication":false}='
```

出力：

```
{"data":[{"enabled":true,"protocol":"smtp","smtp_server":"a.com","from_address":"test@mydomain.com",
"smtp_port":25,"notification_use_smtp_authentication":false,"reply_to_address":"test@test.com"}]}
```

3. Cisco SD-WAN リリース 19.2.1 以降では、メモリアリークを防ぐために、トークンを含む各 API コールの後にログアウトする必要があります。

次の例は、ログアウトする方法を示しています。

コマンド：

```
sampleuser$ curl "https://vManage_IP/logout" -b cookies.txt --insecure -H
"X-XSRF-TOKEN:$TOKEN"
```

出力：

```
Replaced cookie JSESSIONID="DcOke5mqix_15qCpWA1b1IJVAMnVg31DMU4ABRgVinvalid" for
domain 209.165.200.254, path /, expire 0
< set-cookie: JSESSIONID=DcOke5mqix_15qCpWA1b1IJVAMnVg31DMU4ABRgVinvalid
```



(注) セッションからログアウトしたことを確認するには、`jsessionid`をチェックし、それが「invalid」で終わっていることを確認します。



第 14 章

Microsoft Azure への Cisco SD-WAN コントローラの展開

表 46: 機能の履歴

機能名	リリース情報	説明
Azure への Cisco SD-WAN コントローラの展開	Cisco vManage リリース 20.6.1	この機能により、Microsoft Azure 環境に Cisco SD-WAN コントローラ（Cisco SD-WAN Manager、Cisco SD-WAN コントローラ、および Cisco Catalyst SD-WAN Validator）を展開できます。

- [Azure での Cisco SD-WAN コントローラの展開に関する情報（389 ページ）](#)
- [Azure で Cisco SD-WAN コントローラを展開するための前提条件（390 ページ）](#)
- [Azure に Cisco SD-WAN コントローラを展開するユースケース（391 ページ）](#)
- [Azure での Cisco SD-WAN コントローラの展開：タスク（391 ページ）](#)
- [Azure での Cisco SD-WAN コントローラの展開の確認（397 ページ）](#)
- [Azure での Cisco SD-WAN コントローラの展開の監視（398 ページ）](#)

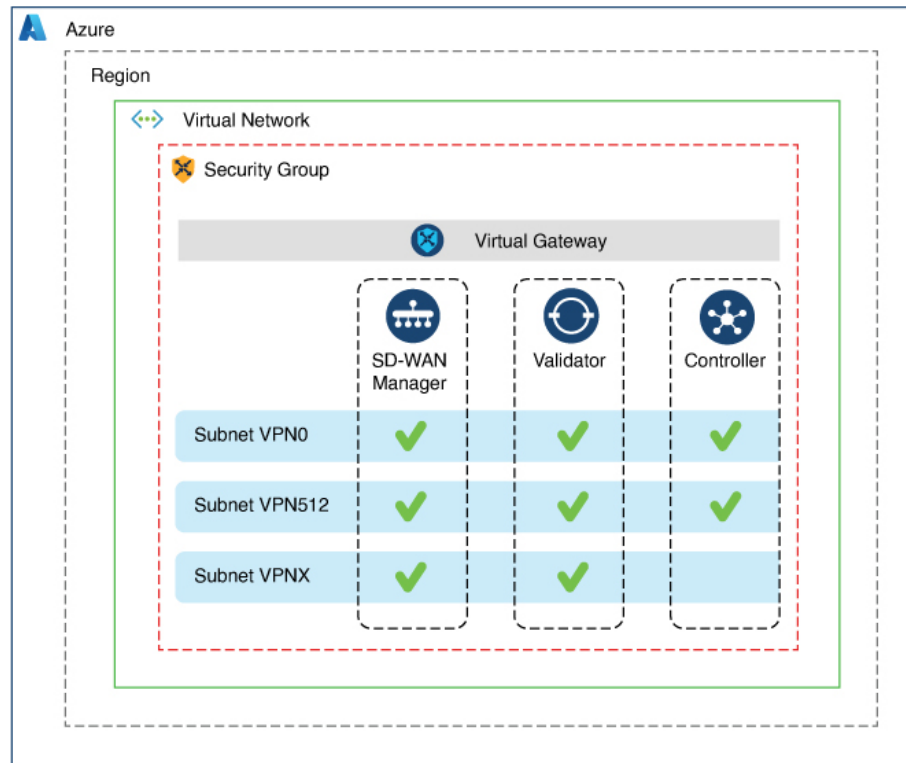
Azure での Cisco SD-WAN コントローラの展開に関する情報

サポートされる最小限のコントローライメージ：Cisco vManage リリース 20.6.1、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.6.1、および Cisco SD-WAN Validator リリース 20.6.1

Azure 環境には、次の Cisco SD-WAN コントローラを展開できます。Cisco SD-WAN Manager、Cisco SD-WAN コントローラ、Cisco SD-WAN Validator。

次の図は、Azure リージョン、仮想ネットワーク、セキュリティグループなどのアーキテクチャを示しており、アーキテクチャ内で Cisco SD-WAN コントローラが機能する場所を示しています。

図 29: Azure での Cisco SD-WAN コントローラ



357661

Cisco SD-WAN コントローラを Azure に展開する利点

- セットアップコスト：追加のデータセンターインフラストラクチャを購入する必要がないため、オンプレミスホスティングと比較して初期セットアップコストが低い。
- 展開：クラウドベースの展開の容易さ。
- 管理：世界中のデバイスを管理する機能。
- 安定性：Azure ホスティングは、その信頼性により、Cisco SD-WAN コントローラ に安定した環境を提供。
- セキュリティ：Azure は、セキュアなホスティング環境を提供。
- 拡張性：Azure は、Cisco Catalyst SD-WAN ネットワークの規模を拡大する容易な方法を提供。

Azure で Cisco SD-WAN コントローラ を展開するための前提条件

有効（かつアクティブ）な Microsoft Azure サブスクリプションが必要です。

Azure に Cisco SD-WAN コントローラ を展開するユースケース

すでに Azure を使用している Cisco Catalyst SD-WAN 展開（Cisco Catalyst 8000V Edge ソフトウェアなど）の場合、Azure で Cisco SD-WAN コントローラ をホストすることは、すべてのサービスの整合性を保つための論理的かつ効率的な選択です。

Azure での Cisco SD-WAN コントローラ の展開：タスク



- (注) ここで説明する手順は、3つのタイプの Cisco SD-WAN コントローラ（Cisco SD-WAN Manager、Cisco SD-WAN コントローラ、および Cisco SD-WAN Validator）に適用されます。特定のコントローラについて指示が異なる場合は、その旨を示します。



- (注) DHCP 設定では、IPv6 ユニークローカルアドレス（ULA）がインターフェイスに割り当てられる場合があります。Cisco SD-WAN Validator は、送信元または宛先が ULA アドレスであるパケットをドロップするように設計されています。Azure セットアップで、デバイスでこれらのアドレスを持つパケットを許可するには、**enable-ipv6-unique-local-address** コマンドを設定して、これらのアドレスを有効または無効にします。

タスク 1：Azure でのコントローライメージの作成

はじめる前に

シスコの「[Software Download](#)」ページで、Cisco SD-WAN 制御コンポーネント（Cisco SD-WAN Manager、Cisco SD-WAN コントローラ、および Cisco SD-WAN Validator）のイメージをダウンロードします。ダウンロードしたファイル（.tar 形式）を圧縮解除します。各コントローラのイメージファイルは、仮想ハードディスク（VHD）形式です。

Azure でのコントローライメージの作成



- (注) Azure のタスクの詳細については、Azure のドキュメントを参照してください。

Azure ポータルで次の手順を実行します。

1. Azure のストレージアカウントをまだ持っていない場合は、今すぐ作成します。
 - ストレージアカウントの名前、場所などを指定します。

- ネットワーク接続については、接続方式、ルーティング設定、データ保護、およびセキュアな転送に関するデフォルトオプションを使用します。
- 必要に応じて、タグを入力してストレージアカウントを分類できます。

2. ストレージアカウントに新しいプライベートコンテナを作成します。コントローラを展開する予定のリージョンでストレージアカウントを選択します。



(注) 各コントローラには個別のコンテナが必要です。

3. コントローラの VHD ファイルをコンテナにアップロードします。
アップロード手順の実行中に、Blob タイプとして [Page Blob] を選択します。



(注) Blob タイプの選択については、Azure のドキュメントを参照してください。

4. 前の手順でアップロードした VHD ファイルを選択して、新しいイメージを作成します。
イメージを作成するときは、次のアクションを実行してください。
 - 有効なサブスクリプションを選択します。
 - 既存のリソースグループを選択するか、新しいリソースグループを作成します。
 - イメージの名前とリージョンを入力します。
 - OS については、[Linux] を選択します。
 - VM の世代については、[Gen 1] を選択します。
 - アカウントタイプについては、[Premium SSD] を選択します。
 - ホストキャッシングについては、[read/write] を選択します。
 - 暗号化については、デフォルト設定を選択します。
 - 必要に応じて、タグを入力してイメージを分類できます。

タスク 2 : Azure での仮想ネットワーク、サブネット、およびネットワーク セキュリティ グループの作成



(注) Azure のタスクの詳細については、Azure のドキュメントを参照してください。

Azure ポータルで次の手順を実行します。

1. 仮想ネットワークを作成するためのワークフローを開始します。

仮想ネットワークを作成するときは、次のアクションを実行してください。

- 有効なサブスクリプションを選択します。
- 既存のリソースグループを選択するか、新しいリソースグループを作成します。



(注) リソースグループは、リージョン全体に展開したすべてのリソースを含む Azure の論理構造です。Cisco Catalyst SD-WAN オーバーレイごとに 1 つのリソースグループを定義することをお勧めします。

- 仮想ネットワークの名前とリージョンを入力します。
- 仮想ネットワークのアドレス空間を入力します。

例 : 10.0.0.0/16

- 少なくとも 2 つのサブネットを仮想ネットワークに追加し、Cisco SD-WAN Manager クラスタを使用している場合は追加のサブネットを追加します。サブネットごとに、サブネットの名前とアドレス空間を指定します。後の手順で、追加したサブネットを VM ネットワーク インターフェイスに関連付けます。

例 :

10.0.1.0/24

10.0.2.0/24

10.0.3.0/24

- 必要に応じて、タグを入力して仮想ネットワークを分類できます。

2. ネットワーク セキュリティ グループ (NSG) を作成するためのワークフローを開始します。

ネットワーク セキュリティ グループを作成するときは、次のアクションを実行してください。

- 有効なサブスクリプションを選択します。
- 仮想ネットワークを作成するワークフローの一部として、前の手順で作成したリソースグループを選択します。
- NSG の名前とリージョンを入力します。
- 必要に応じて、タグを入力して NSG を分類できます。

3. 新たに作成した NSG を、前の手順で作成したサブネットに関連付けます。

タスク 3: コントローラの仮想マシンの作成



(注) Azure のタスクの詳細については、Azure のドキュメントを参照してください。

Azure ポータルで次の手順を実行します。

1. 仮想マシン (VM) を作成するためのワークフローを開始します。

VM を作成するときは、次のアクションを実行してください。

- タスク 2 で作成した仮想ネットワークに VM を展開します。
- 仮想ネットワークを作成するワークフローの間に、前のタスクで作成したリソースグループを選択します。
- VM の名前とリージョンを入力します。
- イメージには、アップロードされたコントローライメージを選択します。



(注) カスタムイメージを見つける方法については、Azure のドキュメントを参照してください。

- VM サイズについては、コントローラに使用する CPU とメモリの数を含むオプションを選択します。

Cisco SD-WAN コントローラデバイスの互換性とサーバー要件については、「[Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations](#)」[英語]を参照してください。

- 認証タイプ (SSH 公開キーやパスワードなど) を選択し、必要に応じてログイン情報を入力します。
 - ディスクリソースについては、次のいずれかを実行します。
 - Cisco Catalyst SD-WAN コントローラ または Cisco Catalyst SD-WAN Validator を展開する場合、デフォルト以外の追加のディスクリソースは必要ありません。
 - Cisco SD-WAN Manager コントローラを展開する場合は、ディスクを 1 つ選択します。
 - Premium SSD オプションとデフォルトの暗号化を選択します。
 - 1 TiB (Azure では P30 と呼ばれます) 以上のディスクサイズを選択します。
- Azure のコントローラに関連するサーバーの推奨事項については、「[Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations](#)」[英語]を参照してください。
- ディスクホストキャッシュを読み取り/書き込みとして設定します。

- ネットワークの詳細については、前の手順で作成した仮想ネットワーク、サブネット、および NSG を選択します。
- パブリック IP アドレスについては、次のオプションを選択します。
 - SKU : [Basic]
 - 割り当て : [static]



(注) Cisco Catalyst SD-WAN にはコントローラの静的 IP アドレスが必要です。

- 必要に応じて、高度なブート診断（管理オプション）を有効にして、診断ログを格納するための追加のストレージアカウントをリソースグループに作成できます。
- （コントローラリリース 20.6.1 以降）必要に応じて、カスタムデータ機能（詳細オプション）を使用して、再起動時に VM が実行するコマンドを入力できます。
- 必要に応じて、コントローラを分類するタグを追加できます。

2. VM を作成したら、VM 用に追加のネットワークインターフェイス（NIC）を作成します。
前のタスクで作成したリソースグループにネットワークインターフェイスを作成します。

- Cisco SD-WAN コントローラ または Cisco SD-WAN Validator を展開している場合は、追加のネットワーク インターフェイスを 1 つ作成します。
- Cisco SD-WAN Manager コントローラを展開する場合は、2 つの追加のネットワーク インターフェイスを作成します。
- クラスタに Cisco SD-WAN Manager コントローラを展開している場合は、Cisco SD-WAN Manager アウトオブバンドインターフェイスの詳細について、「[クラスタの管理](#)」と「[Cisco Catalyst SD-WAN Manager の展開](#)」を参照してください。

ネットワークインターフェイスを作成するときは、次のアクションを実行してください。

- 前のタスクで作成した仮想ネットワーク、サブネット、および NSG を指定します。
- NIC 1 をサブネット 1 に関連付けます。

Cisco SD-WAN Manager コントローラを展開している場合は、NIC 2 をサブネット 2 に関連付けます。

Cisco SD-WAN Manager クラスタを使用している場合は、NIC 3 をサブネット 3 に関連付けます。



(注) NIC をサブネットに関連付けると、VM がサブネットに接続できるようになります。

- NIC ごとに、展開するコントローラに使用するタグを入力します。

3. 使用するすべてのコントローラに静的パブリック IP を作成し、そのパブリック IP を NIC 1 に関連付けます。



(注) Azure の IP 構成オプションを使用して、パブリック IP を作成します。

パブリック IP を作成するときは、次のアクションを実行してください。

- 割り当てには、[static] を選択します。
- NIC 1 を指定する場合は、関連付けオプションを使用します。

4. VM を停止し、停止したことを確認します。

5. 新たに作成した NIC を VM に接続します。

- Cisco SD-WAN コントローラ または Cisco SD-WAN Validator を展開している場合は、NIC を VM に接続します。
- Cisco SD-WAN Manager を展開している場合は、新たに作成した両方の NIC を VM に接続します。

6. VM を再起動します。

VM が再起動したことを Azure ポータルで確認します。

タスク 4: ネットワーク セキュリティ グループの設定

はじめる前に

NSG は、ファイアウォールポリシーに機能的に関連しています。NSG を設定するときは、Cisco Catalyst SD-WAN のファイアウォールポートの構成を把握していると便利です。ファイアウォールポートの詳細については、『[Firewall Ports for Cisco SD-WAN Deployments](#)』を参照してください。

ネットワーク セキュリティ グループの設定



(注) Azure のタスクの詳細については、Azure のドキュメントを参照してください。

1. Azure ポータルを使用し、前のタスクで作成した NSG にインバウンドセキュリティルールを追加して、以下のために必要な IP 範囲からのインバウンドトラフィックを許可します。

- 各 Cisco SD-WAN コントローラ 間の制御接続の確立。コントローラが相互に接続されていない場合、コントロールプレーンとデータプレーンは動作できません。
- HTTPS または SSH プロトコルを使用したコントローラへのアクセス。

NSG については、インバウンドセキュリティルールを追加するオプションを使用します。ルールを使用して、コントローラの VM の IP アドレスをすべて許可し、Cisco SD-WAN コントローラ 間で必要な接続を有効にします。

新しいインバウンドセキュリティルールを作成するときは、次のアクションを実行してください。

- IP 範囲、プロトコルなどを指定します。
 - ルールのアクションについては、トラフィックを許可するオプションを選択します。
2. 接続を確認するには、Cisco SD-WAN Manager の NIC 0 パブリック IP を使用して VM にログインします。

Azure での Cisco SD-WAN コントローラの展開の確認

- インフラストラクチャ :

Azure の仮想マシン内の Cisco SD-WAN コントローラの展開を確認するには、Azure ポータルを使用して、各コントローラをホストする VM がアクティブであることを確認します。

- サービス :

コントローラの展開後に Cisco Catalyst SD-WAN サービスが動作していることを確認するには、次の手順を使用します。

1. Cisco SD-WAN Manager をホストする VM への ping が成功することを確認します。
2. Cisco SD-WAN Manager にログインします。
3. SSH を使用して Cisco SD-WAN Manager に接続し、**request nms all status** コマンドを使用します。出力には、すべての Cisco SD-WAN Manager サービスのステータスが表示されます。アプリケーションサーバーがアクティブになっていることを確認します。

次の **request nms all status** コマンド出力の抜粋は、アプリケーションサーバーがアクティブであることを示しています。

```
vmanage# request nms all status
NMS service proxy
    Enabled: true
    Status: running PID:2881 for 9479s
NMS service proxy rate limit
    Enabled: true
    Status: running PID:4359 for 9521s
NMS application server
    Enabled: true
```

```
Status:  running PID:6131 for 9419s
...
```

4. コントローラをインストール後、「[Cisco SD-WAN Overlay Network Bring-Up Process](#)」の手順に従って、コントローラの制御接続を確立し、各コントローラが動作していることを確認します。

Azure での Cisco SD-WAN コントローラ の展開の監視

インフラストラクチャのステータス（CPU 使用率やディスク使用率など）を監視するには、Azure ポータルの監視ツールを使用します。

Cisco Catalyst SD-WAN サービスのステータスのモニタリングについては、[Cisco SD-WAN Monitor and Maintain guide](#) [英語] を参照してください。



第 15 章

AWS クラウドでの Cisco SD-WAN コントローラの展開

表 47: 機能の履歴

機能名	リリース情報	説明
AWS での Cisco SD-WAN コントローラの展開	Cisco vManage リリース 20.6.1	この機能により、Amazon AWS 環境に Cisco SD-WAN コントローラ（Cisco SD-WAN Manager、Cisco Catalyst SD-WAN コントローラ、および Cisco SD-WAN Validator）を展開できます。

- [AWS での Cisco SD-WAN コントローラの展開について（399 ページ）](#)
- [AWS で Cisco SD-WAN コントローラを展開するための前提条件（401 ページ）](#)
- [AWS に Cisco SD-WAN コントローラを展開するユースケース（401 ページ）](#)
- [AWS での Cisco SD-WAN コントローラの展開：タスク（402 ページ）](#)
- [AWS での Cisco SD-WAN コントローラの展開の確認（407 ページ）](#)
- [AWS での Cisco Catalyst SD-WAN コントローラの展開の監視（408 ページ）](#)

AWS での Cisco SD-WAN コントローラの展開について

サポートされる最小のコントローライメージ：Cisco vManage リリース 20.6.1、Cisco vSmart コントローラリリース 20.6.1、および Cisco vBond Orchestrator リリース 20.6.1。

Amazon Machine Images（AMI）を使用して、Amazon Web Services（AWS）環境に次の Cisco SD-WAN コントローラを展開できます。Cisco SD-WAN Manager、Cisco SD-WAN コントローラ、および Cisco SD-WAN Validator。

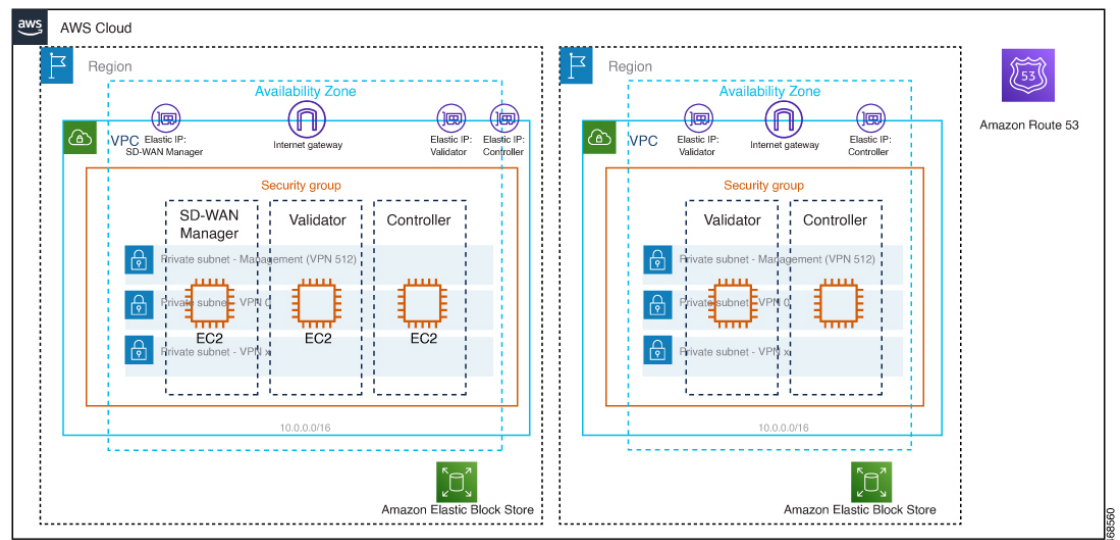
シスコが提供する AMI イメージは対象のユーザー専用です。他の人と共有しないでください。次を実行できます。

- 注文数量に応じた数のコントローラを展開できます。たとえば、50 個の Cisco SD-WAN Manager コントローラ PID を注文した場合、AWS アカウント内に展開できる Cisco SD-WAN Manager コントローラは 50 個のみです。

- 注文した PID の数を超えなければ、リージョン間および独自の AWS アカウント間で AMI をコピーできます。
- コントローラの初期展開後は、アップグレードまたはダウングレードをユーザーが実行する必要があります。

次の図は、AWS リージョン、仮想プライベートクラウド（VPC）、セキュリティグループなどのアーキテクチャを示しており、アーキテクチャ内で Cisco SD-WAN コントローラが機能する場所を示しています。

図 30: AWS での Cisco SD-WAN コントローラ



AWS に Cisco SD-WAN コントローラをインストールする前の考慮事項

- Cisco Catalyst SD-WAN コントローラ AMI は、Cisco Software Download サイトや AWS マーケットプレイスでは入手できません。AMI は、AWS クラウドアカウントで Cisco SD-WAN コントローラをセットアップするための有効なビジネスケースとともにリクエストした場合にのみ提供されます。
- AWS で使用する Cisco SD-WAN コントローラの注文については、シスコアカウントチームまたはシスコパートナーにお問い合わせください。
- シスコは、コントローラのプロビジョニングまたはインストール中にクラウドインフラストラクチャで発生する問題のサポートを提供していません。
- トラブルシューティング：
 - 機能の問題：機能の問題については、Cisco TAC ケースを開いてください。
 - インフラストラクチャの問題：インフラストラクチャの管理、監視、およびトラブルシューティングはお客様が行う必要があります。コントローラがプロビジョニングされ、クラウドアカウントで実行されると、シスコはクラウドインフラストラクチャ関連の問題のサポートを提供しません。

- ソフトウェアのアップグレード：コントローラソフトウェアのアップグレードに AMI イメージは不要です。『Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide』の「[Manage Software Upgrade and Repository](#)」の章の説明に従って、Cisco Software Download サイトからコントローライメージをダウンロードし、コントローラソフトウェアをアップグレードできます。

AWS で Cisco SD-WAN コントローラ を展開する利点

- セットアップコスト：追加のデータセンターインフラストラクチャを購入する必要がないため、オンプレミスホスティングと比較して初期セットアップコストが低い。
- 展開：クラウドベースの展開の容易さ。
- 管理：世界中のデバイスを管理する機能。
- 安定性：AWS ホスティングは、その信頼性により、Cisco SD-WAN コントローラに安定した環境を提供。
- セキュリティ：AWS は、セキュアなホスティング環境を提供。
- 拡張性：AWS は、Cisco Catalyst SD-WAN ネットワークの規模を拡大する容易な方法を提供。

AWS で Cisco SD-WAN コントローラ を展開するための前提条件

- 有効（かつアクティブ）な AWS およびシスコアカウントが必要です。
- クラウドの導入に適したコントローラ PID を注文するための PID 情報については、シスコアカウントチームにお問い合わせください。

AWS に Cisco SD-WAN コントローラ を展開するユースケース

- ユースケース 1：独自のパブリッククラウドアカウントを使用して、コントローラのプロビジョニング、管理、監視、および拡張性を完全に制御します。
- ユースケース 2：特定のアーキテクチャまたはセキュリティ態勢の要件。

AWS での Cisco SD-WAN コントローラ の展開 : タスク



(注) ここで説明する手順は、3つのタイプの Cisco SD-WAN コントローラ（Cisco SD-WAN Manager、Cisco SD-WAN コントローラ、および Cisco SD-WAN Validator）に適用されます。特定のコントローラについて指示が異なる場合は、その旨を示します。

タスク 1 : AWS AMI イメージのリクエスト

AMI イメージを使用して AWS アカウントに Cisco SD-WAN コントローラを展開できます。

1. \$0 のカスタマー管理 Cisco Catalyst SD-WAN コントローラ SKU を注文する必要があります。詳細については、『[Cisco Catalyst SD-WAN Controller Ordering Guide](#)』のセクション 2.3 「SKU Table」を参照してください。
2. SKU を購入すると、Cisco CloudOps チームが注文情報を検証し、次のような追加の詳細をお客様に尋ねます。
 1. AWS アカウント番号。
 2. AMI のソフトウェアバージョンの要件。
3. Cisco CloudOps チームは情報を確認し、要求された AMI を US-WEST-2 リージョンの AMI インベントリと共有します。



(注) CloudOps チームが提供する AMI イメージは対象のユーザー専用です。他の人と共有しないでください。イメージが他の人と共有された場合、シスコはイメージを削除し、イメージが共有されないようにするために必要な措置を講じる権利を留保します。

タスク 2 : AWS で VPC、サブネット、およびセキュリティグループを作成する



(注) AWS のタスクの詳細については、AWS のドキュメントを参照してください。

AWS ポータルで次の手順を実行します。

1. 仮想プライベートクラウド（VPC）を作成し、VPC の作成中に次のアクションを実行してください。
 - VPC の名前とリージョンを入力します。

- VPC のアドレス空間を入力します。例 : 10.0.0.0/16
- 少なくとも 2 つのサブネットを VPC に追加し、Cisco SD-WAN Manager クラスタを作成する予定の場合は追加のサブネットを追加します。サブネットごとに、サブネットの名前とアドレス空間を指定します。後の手順で、追加したサブネットを仮想マシンのネットワーク インターフェイスに関連付けます。

例 :

- サブネット 0 をアドレス 10.0.1.0/24 で追加します。これは、コントローラのプライマリインターフェイスとして使用される VPN 512 になります。
 - サブネット 1 をアドレス 10.0.2.0/24 で追加します。これは、VPN 0 のコントローラのトランスポートまたはトンネルインターフェイスとして使用されます。
 - サブネット 2 をアドレス 10.0.3.0/24 で追加します。これは Cisco SD-WAN Manager クラスタリングに使用されます (Cisco SD-WAN Manager クラスタの展開が必要な場合のみ)。
- (オプション) VPC を分類するタグを入力します。
2. VPC に必要なリソースを作成して、コントローラインスタンスを実行するための環境を形成します。
- セキュリティグループには、次のものが含まれている必要があります。
 - 管理目的でコントローラにアクセスするためのユーザー NOC センターの送信元パブリック IP アドレス。
 - すべてのエッジがコントローラに参加するための TLS/DTLS に対するすべての TCP/UDP ポートのアドレス 0.0.0.0/0。
 - 各コントローラが他のコントローラに到達するためのパブリック IP を有効にします。
 - セキュリティグループの名前とリージョンを入力します。
 - (オプション) セキュリティグループを分類するタグを入力します。
3. 新たに作成したセキュリティグループを、手順 1 で作成したサブネットに関連付けます。
4. インターネットゲートウェイを作成し、VPC に関連付けます。
5. ルーティングテーブルを作成し、VPC に関連付けます。インターネットゲートウェイを指すデフォルトルートエントリを追加します。

タスク 3 : コントローラの仮想マシンの作成



(注) AWS のタスクの詳細については、AWS のドキュメントを参照してください。

AWS ポータルで次の手順を実行します。

1. 仮想マシンを作成するためのワークフローを開始します。仮想マシンを作成するときは、次のアクションを実行してください。
 - タスク 2 で作成した仮想プライベートクラウド (VPC) に仮想マシンを展開します。
 - 仮想マシンの名前とリージョンを入力します。
 - イメージの場合は、Cisco SD-WAN Manager、Cisco SD-WAN Validator、または Cisco SD-WAN コントローラ に対して適切な共有コントローラ AMI を選択します。



(注) カスタムイメージを見つける方法については、AWS のドキュメントを参照してください。

- 仮想マシンのサイズについては、コントローラに使用する CPU とメモリの数を含むオプションを選択します。Cisco SD-WAN コントローラデバイスの互換性と Cisco SD-WAN コントローラ サーバー要件については、「[Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations](#)」を参照してください。
 - 認証タイプ (SSH 公開キーやパスワードなど) を選択し、必要に応じてログイン情報を入力します。
 - ディスクリソースについては、次のいずれかを実行します。
 - Cisco SD-WAN コントローラ または Cisco SD-WAN Validator を展開する場合、デフォルト以外の追加のディスクリソースは必要ありません。
 - Cisco SD-WAN Manager コントローラを展開する場合は、ディスクを 1 つ選択します。
 - Premium SSD オプションとデフォルトの暗号化を選択します。
 - 1 TB (汎用 SSD gp2) 以上のディスクサイズを選択します。
- AWS のコントローラに関連するサーバーの推奨事項については、「[Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations](#)」を参照してください。
- ディスクホストキャッシュを読み取り/書き込みとして設定します。
-
- ネットワークの詳細については、前の手順で作成した VPC、サブネット、およびセキュリティグループを選択します。各仮想マシンには 2 つのネットワーク イン

ターフェイスが必要です。1 つは VPN 512 管理サブネット用、もう 1 つは VPN 0 トンネルサブネット用です。

- Elastic IP アドレスを各コントローラの VPN 0 および VPN 512 ネットワーク インターフェイスに割り当てます。
- (オプション) 高度なブート診断 (管理オプション) を有効にして、診断ログを格納するための追加のストレージアカウントをリソースグループに作成します。
- Cisco SD-WAN コントローラリリース 20.6.1 以降では、必要に応じてカスタムデータ機能を使用して、再起動時に仮想マシンが実行するコマンドを入力できます。
- (オプション) タグを追加してコントローラを分類します。

2. 仮想マシンを作成したら、仮想マシン用に追加のネットワーク インターフェイス (NIC) を作成します。前のタスクで作成したリソースグループにネットワーク インターフェイスを作成します。

- Cisco SD-WAN コントローラ または Cisco SD-WAN Validator を展開している場合は、追加のネットワーク インターフェイスを 1 つ作成します。
- Cisco SD-WAN Manager コントローラを展開する場合は、2 つの追加のネットワーク インターフェイスを作成します。
- クラスタに Cisco SD-WAN Manager コントローラを展開している場合は、Cisco SD-WAN Manager アウトオブバンドインターフェイスの詳細について、「[Cluster Management](#)」と「[Deploy Cisco SD-WAN Manager](#)」を参照してください。

3. ネットワーク インターフェイスを作成するときは、次のアクションを実行してください。

- タスク 2 で作成した VPC、サブネット、およびセキュリティグループを指定します。
- NIC をサブネットに関連付けます。

例: NIC 1 をサブネット 1 に関連付けます。

- Cisco SD-WAN Manager コントローラを展開している場合は、NIC 2 をサブネット 2 に関連付けます。
- Cisco SD-WAN Manager クラスタを使用している場合は、NIC 3 をサブネット 3 に関連付けます。



(注) NIC をサブネットに関連付けると、仮想マシンがサブネットに接続できるようになります。

- NIC ごとに、展開するコントローラに使用するタグを入力します。

4. 使用するすべてのコントローラの静的パブリック IP を作成し、このパブリック IP を NIC 1 に関連付けます。



(注) AWS の IP 構成オプションを使用して、パブリック IP を作成します。

5. パブリック IP を作成するときは、次のアクションを実行してください。
 - 割り当てには、[static] を選択します。
 - NIC 1 を指定する場合は、関連付けオプションを使用します。
6. 仮想マシンを停止し、停止したことを確認します。
7. 新たに作成した NIC を仮想マシンに接続します。
 - Cisco SD-WAN コントローラ または Cisco SD-WAN Validator を展開している場合は、NIC を仮想マシンに接続します。
 - Cisco SD-WAN Manager を展開している場合は、新たに作成した両方の NIC を仮想マシンに接続します。
8. 仮想マシンを再起動します。AWS ポータルで、仮想マシンが再起動したことを確認します。

タスク 4：セキュリティグループの設定

はじめる前に

セキュリティグループは、ファイアウォールポリシーに機能的に関連しています。セキュリティグループを設定するときは、Cisco Catalyst SD-WAN のファイアウォールポートの設定を把握していると便利です。[Firewall Ports for Cisco SD-WAN Deployments](#)を参照してください。



(注) AWS のタスクの詳細については、AWS のドキュメントを参照してください。

セキュリティグループの設定

1. AWS ポータルを使用し、前のタスクで作成したセキュリティグループにインバウンドセキュリティルールを追加して、以下のために必要な IP 範囲からのインバウンドトラフィックを許可します。
 - 各 Cisco SD-WAN コントローラ 間の制御接続の確立。コントローラが相互に接続されていない場合、コントロールプレーンとデータプレーンは動作できません。
 - HTTPS または SSH プロトコルを使用したコントローラへのアクセス。

2. セキュリティグループについては、インバウンドセキュリティルールを追加するオプションを使用します。ルールを使用して、すべてのコントローラの仮想マシンの IP アドレスを許可し、Cisco SD-WAN コントローラ 間で必要な接続を有効にします。

新しいインバウンドセキュリティルールを作成するときは、次のアクションを実行してください。

- IP 範囲、プロトコルなどを指定します。
 - ルールのアクションについては、トラフィックを許可するオプションを選択します。
3. 接続を確認するには、Cisco SD-WAN Manager の NIC 0 パブリック IP を使用して仮想マシンにログインします。

AWS での Cisco SD-WAN コントローラの展開の確認

- インフラストラクチャ：AWS の仮想マシン内の Cisco SD-WAN コントローラの展開を確認するには、AWS ポータルを使用して、各コントローラをホストする仮想マシンがアクティブかどうかを確認します。
 - サービス：コントローラの展開後に Cisco Catalyst SD-WAN サービスが動作していることを確認するには、次の手順を使用します。
1. Cisco SD-WAN Manager をホストする仮想マシンへの ping が成功することを確認します。
 2. AWS コンソールを使用して、admin ユーザーとしてコントローラインスタンスにログインします。新しいパスワードの設定を求められる場合があります。設定したら、コントローラのパブリック IP への SSH 経由のログインを確認します。
 3. SSH を使用して Cisco SD-WAN Manager に接続し、**request nms all status** コマンドを使用します。出力には、すべての Cisco SD-WAN Manager サービスのステータスが表示されます。アプリケーションサーバーがアクティブになっていることを確認します。

次の **request nms all status** コマンド出力の抜粋は、アプリケーションサーバーがアクティブであることを示しています。

```
vmanage# request nms all status
NMS service proxy
  Enabled: true
  Status: running PID:2881 for 9479s
NMS service proxy rate limit
  Enabled: true
  Status: running PID:4359 for 9521s
NMS application server
  Enabled: true
  Status: running PID:6131 for 9419s
...
```

4. コントローラをインストール後、「[Cisco SD-WAN Overlay Network Bring-Up Process](#)」の手順に従って、コントローラの制御接続を確立し、各コントローラが動作していることを確認します。

AWS での Cisco Catalyst SD-WAN コントローラ の展開の監視

インフラストラクチャのステータス（CPU 使用率やディスク使用率など）を監視するには、AWS ポータルの監視ツールを使用します。

Cisco Catalyst SD-WAN サービスのステータスのモニタリングについては、『[Cisco Catalyst SD-WAN Monitor and Maintain guide](#)』を参照してください。



第 16 章

Cisco Catalyst SD-WAN ソリューションのトラブルシューティング

- 概要 (409 ページ)
- サポート記事 (409 ページ)
- フィードバックのリクエスト (412 ページ)
- 免責事項と注意事項 (412 ページ)

概要

この章では、シスコの主題専門家（SME）が作成したドキュメントへのリンクを提供します。サポートチケットを必要とせずに技術的な問題を解決できるようにすることを目的としています。これらのドキュメントで問題を解決できない場合は、該当する[シスココミュニティ](#)にアクセスすることをお勧めします。この問題をすでに経験し、解決策を提供している可能性のある他のシスコのお客様からは、豊富な情報とアドバイスを入手できます。コミュニティで解決策が見つからない場合は、[シスコサポート](#)でサポートチケットを提出するのが最善の方法です。サポートチケットを発行する必要がある場合、これらのドキュメントは、収集してサポートチケットに追加する必要があるデータに関するガイダンスを提供します。参照したサポートドキュメントを指定すると、TAC はドキュメントの所有者と改善要求を作成できます。

サポート記事

このセクションのドキュメントは、各記事の「使用するコンポーネント」セクションにリストされている特定のソフトウェアとハードウェアを使用して作成されています。ただし、これは、それらが使用されるコンポーネントにリストされているものに限定されるという意味ではなく、通常、ソフトウェアおよびハードウェアの新しいバージョンに関連し続けます。ソフトウェアまたはハードウェアに変更があり、コマンドが動作しなくなったり、構文が変更されたり、GUI や CLI がリリースごとに異なって見える可能性があることに注意してください。

このテクノロジーに関連するサポート記事は次のとおりです。

マニュアル	説明
Activate Debugs in vManage	このビデオでは、Cisco Catalyst SD-WAN Manager でデバッグをアクティブ化する手順について説明します。
Cisco Catalyst SD-WAN Control Traffic Overhead User Guide	このドキュメントでは、SD-WAN オーバーレイ展開で制御トラフィックのオーバーヘッドを計算する方法について説明します。
Collect an Admin-Tech in SDWAN Environment and Upload to TAC Case	このドキュメントでは、Cisco Catalyst SD-WAN 環境で admin-tech を開始する方法について説明します。
Configure Basic Parameters to Form Control Connections on cEdge	このドキュメントでは、cEdge を Software-Defined Wide Area Network (SD-WAN) オーバーレイにオンボードするための基本設定と正しいコミット順序について説明します。
Configure HSECK9 License on cEdge SD-WAN XE	このドキュメントでは、SD-WAN XE cEdge に HSECK9 ライセンスをインストールしてトラブルシューティングする方法について説明します。
Configure SD-AVC on Cisco Catalyst SD-WAN	このドキュメントでは、Software-Defined Wide Area Network (SD-WAN) で Software Defined-Application Visibility and Control (SD-AVC) を構成する方法について説明します。
Deploy a CSR1000v/C8000v on Google Cloud Platform	このドキュメントでは、Google Cloud Platform (GCP) に Cisco Cloud Services Router 1000v (CSR1000v) および Catalyst 8000v (C800v) Edge Router を展開および構成する手順について説明します。
How To Generate Self-Signed Web Certificate For Cisco Catalyst SD-WAN Manager	このドキュメントでは、オンプレミスの Cisco SD-WAN Manager で既存の証明書が期限切れになった場合に、自己署名 Web 証明書を生成してインストールする方法について説明します。シスコは、そのような展開の Web 証明書に署名しません。お客様は、独自の認証局 (CA) またはサードパーティの CA によって署名する必要があります。
HSEC License FAQs for Cisco Catalyst SD-WAN	このドキュメントでは、自律モードと SD-WAN モードの HSEC ライセンスに関するいくつかのクエリについて説明します。
Manual Certificate Renewal on SD-WAN Controller	このビデオでは、コントローラの証明書を更新する手順について説明します。

マニュアル	説明
Modifying "Statistics Configuration > Collection Interval" in a vManage Cluster	このドキュメントでは、vManage クラスタで [Statistics Configuration] > [Collection Interval] を変更するプロセスについて説明します。
Quick Start Guide - Data Collection for Various Cisco Catalyst SD-WAN Issues	このドキュメントでは、トラブルシューティングや問題解決の速度を向上させるために、TAC ケースを開く前に事前に収集する必要がある関連データに沿って、いくつかの SD-WAN の問題について説明します。このドキュメントは、Cisco SD-WAN Manager とエッジルータという 2 つの主要な技術セクションに分かれています。該当するデバイスに応じて、関連する出力とコマンド構文が提供されます。
Replace a cEdge RMA Router	このドキュメントでは、障害が発生した cEdge ユニットの別のユニットと交換する方法について説明します。これは、障害が発生したルータから交換用ルータへの設定のコピー、この cEdge の削除、およびネットワークへの新しいルータの追加で構成されます。このプロセスは vEdge 交換に似ていますが、cEdge の Cisco SD-WAN Manager ではコピーオプションがありません。
Transfer Files between a cEdge and Cisco Catalyst SD-WAN Manager	このドキュメントでは、CLI を介してリモート cEdge とローカル Cisco SD-WAN Manager の間でファイルを転送する方法について説明します。
Transfer Files between a vEdge and Cisco Catalyst SD-WAN Manager	このドキュメントでは、CLI を介してリモート vEdge とローカル Cisco SD-WAN Manager の間でファイルを転送する方法について説明します。
Troubleshoot software image expansion failure due to lack of bootflash space	このドキュメントでは、自律モードからコントローラモードに変更したときに、デバイスがソフトウェアイメージファイルを正常に展開したことを確認する方法について説明します。展開が成功しなかった場合のトラブルシューティング方法を示します。
Understand the Web Certificate For Cisco Catalyst SD-WAN Manager	このドキュメントでは、Cisco Catalyst SD-WAN ソリューションでの Web 証明書とコントローラ証明書の違いについて説明します。このドキュメントでは、Web 証明書についても詳しく説明し、これら 2 種類の証明書間の使用を明確にします。

マニュアル	説明
Upgrade Cisco Catalyst SD-WAN cEdge Router with the Use of CLI or Cisco Catalyst SD-WAN Manager	このドキュメントでは、コマンドライン（CLI）および Cisco SD-WAN Manager からコントローラモードで SD-WAN cEdge（Cisco Edge）ルータをアップグレードまたはダウングレードするプロセスについて説明します。
Verify APIs Used by vManage to Gather Statistics	このドキュメントでは、Cisco Catalyst SD-WAN Manager がオーバーレイから統計情報を収集するために使用する特定の API コールを取得する方法について説明します。

フィードバックのリクエスト

ユーザー入力役立ちます。これらのサポートドキュメントを改善するための重要な側面は、お客様からのフィードバックです。これらのドキュメントは、シスコ内の複数のチームによって所有および管理されていることに注意してください。ドキュメントに固有の問題（不明瞭、混乱、情報不足など）を見つけた場合：

- 対応する記事の右側のパネルにある [Feedback] ボタンを使用して、フィードバックを提供します。ドキュメントの所有者に通知され、記事が更新されるか、削除のフラグが付けられます。
- ドキュメントのセクション、領域、または問題に関する情報と、改善できる点を含めてください。できるだけ詳細に記述してください。

免責事項と注意事項

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このマニュアルで使用されるデバイスはすべて、初期設定（デフォルト）の状態から作業が開始されています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。



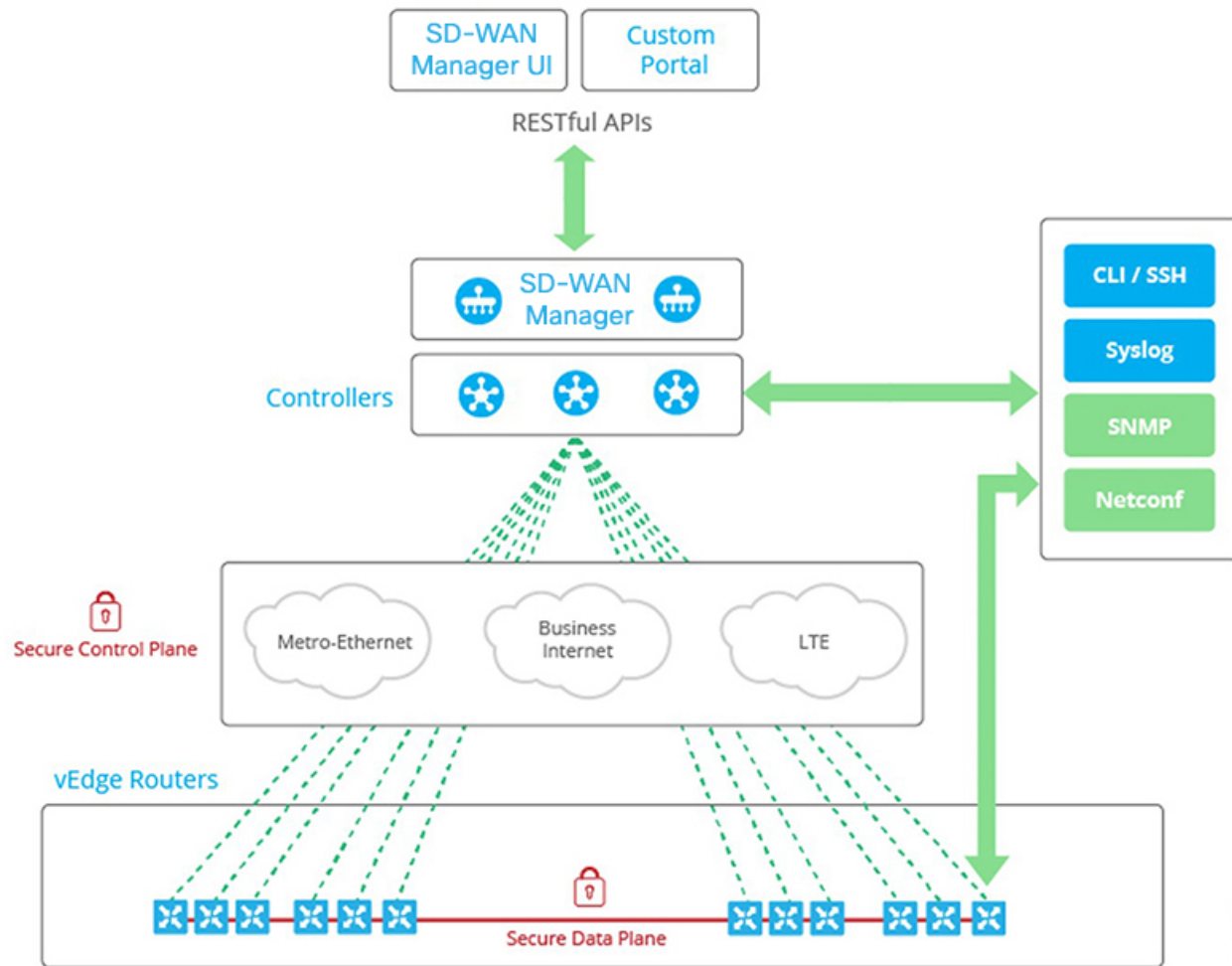
第 17 章

付録：Cisco Catalyst SD-WAN Manager How-To マニュアル

- [Cisco Catalyst SD-WAN Manager の RESTful API](#) (413 ページ)
- [vEdge ルータの交換](#) (416 ページ)
- [Cisco IOS XE Catalyst SD-WAN デバイス の交換](#) (418 ページ)
- [異なるサーバーでの Cisco Catalyst SD-WAN Manager の使用](#) (421 ページ)
- [Cisco Catalyst SD-WAN Manager Web アプリケーションサーバーへのログイン](#) (422 ページ)

Cisco Catalyst SD-WAN Manager の RESTful API

Cisco SD-WAN Manager は RESTful (Representational State Transfer) API をサポートしており、Cisco Catalyst SD-WAN オーバーレイネットワークとネットワーク内のデバイスに関するリアルタイムの静的情報を取得したり、デバイス構成テンプレートやその他の構成関連情報をアップロードしたりするための呼び出しを実行できます。RESTful API を使用して、Cisco SD-WAN Manager と対話するためのカスタムポータルを設計できます。



Cisco SD-WAN Manager API ドキュメントは、Cisco SD-WAN Manager ソフトウェアの一部として、URL：<https://vmanage-ip-address/apidocs> で提供されます。（より正確には、完全な URL には Cisco SD-WAN Manager のポート番号 <https://vmanage-ip-address:8443/apidocs> が含まれます）
vmanage-ip-address は、Cisco SD-WAN Manager サーバーの IP アドレスです。

API 呼び出しは、次のカテゴリの操作に対して提供されます。

- 証明書の管理
- 設定
- デバイスとデバイスインベントリ
- モニターリング
- リアルタイム モニターリング
- トラブルシューティング ツール

REST API を使用した NAT 構成はサポートされていません。



(注) Cisco SD-WAN リリース 20.6.1 以降、Cisco SD-WAN Manager では以下の API 制限がサポートされます。

- API レート制限：100/秒
- Bulk API レート制限：48/分

API のリアルタイム監視では CPU が集中的に使用されるため、トラブルシューティングの目的でのみ使用してください。デバイスのアクティブな監視のために継続的に使用しないでください。

API 呼び出しのグループごとに、[Show/Hide] をクリックして、個々の呼び出しと各呼び出しの URL を一覧表示します。各呼び出しには、その応答クラス、必要なパラメータ、および応答メッセージ（ステータスコード）が表示されます。

[Try It Out] をクリックして、各 API 呼び出しのリクエスト URL と応答本文の形式を表示します。リクエスト URL は、Cisco SD-WAN Manager の URL とそれに続く /dataservice で構成されます。例：https://10.0.1.32:8443/dataservice/device/interface/statistics/ge0/0?deviceId=172.16.255.11

以下に、API 呼び出しに使用する URL の例を示します。

表 48:

要求された情報	API コール
すべてのネットワークデバイスのリスト	dataservice/device
CPU、メモリ、ファン、電源などのハードウェア デバイス コンポーネントの正常性ステータス	dataservice/device/hardware/environment?deviceId=system-ip-address
デバイスのトランスポートインターフェイスのステータス	dataservice/device/interface?deviceId=system-ip-address&port-type=transport
インターフェイスの統計、エラー、およびパケットドロップ	dataservice/device/interface?deviceId=system-ip-address
DTLS/TLS 制御接続ステータス	dataservice/device/control/connections?deviceId=system-ip-address
OMP ピアリング	dataservice/device/omp/peers?deviceId=system-ip-address

要求された情報	API コール
サービス側の BGP ピアリング	<code>dataservice/device/bgp/neighbors?deviceId=system-ip-address</code>

vEdge ルータの交換

ここでは、特定の場所で vEdge ルータを交換する方法について説明します。これは、vEdge ルータが完全に故障した場合や、ルータのコンポーネント（いずれかの電源装置など）が故障した場合に、ルータ全体を交換するために実行できます。

大まかに言うと、vEdge ルータを交換する手順は、削除するルータから新しいルータに構成をコピーし、その新しいルータをネットワークに配置するだけです。

Cisco SD-WAN Manager の vEdge ルータを交換する前に、Cisco SD-WAN Manager が交換用 vEdge ルータのシャーシ番号とシリアル番号を学習しておく必要があります。

- 交換用 vEdge ルータが、以前に受け取ったルータ（スペアインベントリに含まれるルータなど）である場合は、以前にシリアル番号ファイルを Cisco SD-WAN Manager にアップロードしたときに、Cisco SD-WAN Manager がルータのシャーシ番号とシリアル番号をすでに学習しています。
- RMA プロセスを開始して、交換用の新しいルータを受け取った場合は、更新されたバージョンの vEdge 認定シリアル番号ファイルを Cisco SD-WAN Manager にアップロードする必要があります。

故障したルータを、Cisco SD-WAN Manager を使用して交換するには、次の手順を実行します。

1. 故障したルータから交換用ルータに構成をコピーします。
2. 故障したルータを無効にします。ルータを無効にすると、その証明書が非アクティブ化され、ルータがオーバーレイネットワークから削除されます。
3. 交換用ルータを検証して、その証明書をアクティブにします。

新しいルータは、故障したルータの完全な代替品となり、その構成は故障したルータと同じになります（ただし、各ルータは証明書に一意のシャーシ番号と一意のシリアル番号を持つことに注意してください）。故障したルータから交換用ルータに構成をコピーすると、両方のルータの構成は、IP アドレスを含めて同じになります。同じ IP アドレスを持つ 2 つのルータがネットワーク内に同時に存在することはできません。Cisco SD-WAN Manager で一方のルータが有効状態である場合はもう一方のルータが無効状態である必要があり、そうでなければ両方のルータが無効状態である必要があります。

はじめる前に

認定シリアル番号ファイルが Cisco SD-WAN Manager にアップロードされていることを確認してください。

故障したルータから交換用ルータへの構成のコピー

Cisco SD-WAN Manager で、故障した vEdge ルータから交換用ルータに構成をコピーします。

構成のコピー元の vEdge ルータとしては、オーバーレイネットワークでアクティブなデバイス（つまり、有効状態のデバイス）でも非アクティブなデバイス（つまり、無効状態のデバイス）でも使用できます。たとえば、2 つの電源装置の一方が故障したルータを交換する場合、そのルータはネットワーク内でまだアクティブである可能性があります。完全に故障したルータを交換する場合は、そのルータをネットワークから削除するために、すでに無効としてマークされている可能性があります。

構成のコピー先の vEdge ルータは無効状態である必要があります。

vEdge ルータの状態を確認したり有効/無効状態を変更するには、「Validate or Invalidate a vEdge Router」を参照してください。

故障したルータから交換用ルータに構成をコピーするには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Devices]** の順に選択します。
2. 故障したルータについて、[...] をクリックし、**[Copy Configuration]** を選択します。
3. **[Copy Configuration]** ウィンドウで、交換用ルータを選択します。
4. **[Update]** をクリックします。

故障したルータを削除します

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Certificates]** の順に選択します。
2. 故障したルータについて、**[Validate]** 列で、**[Invalid]** をクリックします。
3. **[OK]** をクリックして、デバイスの無効化を確認します。
4. **[Send to Controllers]** をクリックします。

交換用ルータの追加

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Certificates]** の順に選択します。
2. 交換用ルータについて、**[Validate]** 列で、**[Valid]** をクリックします。
3. **[OK]** をクリックして、デバイスの有効化を確認します。
4. **[Send to Controllers]** をクリックします。

ネットワーク内の別のルータと同じ IP アドレスを持つルータを検証しようとする、エラーメッセージが表示され、検証プロセスが終了します。

リリース情報

リリース 15.4 で Cisco SD-WAN Manager に導入されました。

Cisco IOS XE Catalyst SD-WAN デバイスの交換

デバイスが完全に故障した場合、またはデバイスのコンポーネント（電源装置の1つなど）が故障した場合は、Cisco IOS XE Catalyst SD-WAN デバイスを交換することがあります。

一般に、Cisco IOS XE Catalyst SD-WAN デバイスを別のデバイスと交換するには、取り外すデバイスから新しいデバイスに構成をコピーしてから、新しいデバイスをネットワークに追加します。

A. 交換するデバイスの構成をコピーする

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Devices]**の順に選択します。
2. デバイスのリストで、交換するデバイスを見つけます。デバイスの行で[...]をクリックし、**[Running Configuration]**を選択します。



(注) Cisco SD-WAN Manager がデバイスに到達できない場合は、手順 4 にスキップして、デバイスに直接ログインして構成情報をコピーする手順を実行します。

3. 構成のテキストをコピーして、テキストエディタに貼り付けます。

構成情報は、新しい交換用デバイスのオンボーディングに手動展開方式を選択した場合に特に役立ちます。

4. Cisco SD-WAN Manager がデバイスに到達できない場合は、デバイスに直接ログインし、デバイスで次のコマンドを使用して構成情報を表示します。出力から構成情報をコピーします。

- 実行コンフィギュレーションを表示し、出力をテキストファイルに保存します。

```
show running-config | redirect bootflash:sdwan/ios.cli
```

- SD-WAN の実行コンフィギュレーションを表示し、出力をテキストファイルに保存します。

```
show sdwan running-config | redirect bootflash:sdwan/sdwan.cli
```

B. オーバーレイネットワークからデバイスを削除する

1. Cisco SD-WAN Manager のメニューから**[Configuration] > [Certificates]**の順に選択します。
2. デバイスのリストで、交換するデバイスを見つけます。デバイスの行の **[Validate]** 列で、**[Invalid]**、**[OK]** の順にクリックします。



(注) この手順により、デバイスの制御接続がすべて失われます。

3. [Send to Controllers] をクリックします。
4. Cisco SD-WAN Manager メニューから、[Configuration] > [Devices]の順に選択します。
5. デバイスのリストで、交換するデバイスを見つけます。デバイスの行で [...] をクリックし、[Delete WAN Edge] を選択します。

C. 交換用デバイスを Cisco SD-WAN Manager インベントリに追加する

1. 交換用デバイスのシャーシ番号とシリアル番号を取得します。



(注) デバイスで **show sdwan certificate serial** コマンドを使用して、各番号を表示できます。

2. 『Cisco Catalyst SD-WAN Getting Started Guide』で説明されているいずれかの方法を使用して、新しいデバイスをインベントリに追加します。



(注) 新しいデバイスをインベントリに追加する方法は、一般的にデバイスのオンボーディングに関連した方法です。それらは、デバイスの交換に固有の方法ではありません。

D. 交換されるデバイスに適用されたテンプレートと同じデバイステンプレートを使用して、新しいデバイスにデバイステンプレートを適用する

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] の順に選択します。
2. 交換するデバイスに使用されていたテンプレートの行で、[...] をクリックし、[Export CSV] を選択します。CSV ファイルには、テンプレートが添付されている各デバイスのパラメータが表示されます。
3. エクスポートされた CSV ファイルを確認します。
 - 新しいデバイスが交換されるデバイスと同一である場合、CSV ファイルのパラメータを更新する必要はありません。
 - 新しいデバイスが交換されるデバイスと同一でない場合、必要に応じて、新しいデバイスに一致するように CSV ファイルのパラメータ値を更新できます。たとえば、交換用デバイスで、交換されるデバイスとは異なるインターフェイスの番号付けが使用されている場合は、インターフェイスの番号付けを指定するパラメータを更新できます。
4. テンプレートを交換用デバイスに添付するには、次の手順を実行します。
 1. Cisco SD-WAN Manager のメニューから、[Configuration] > [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. 交換されるデバイスに使用されていたテンプレートの行で、[...]をクリックし、[Attach Devices] を選択します。
4. [Attach Devices] ウィンドウで、交換用デバイスを [Selected Devices] ペインに移動し、[Attach] をクリックします。
5. 必要に応じて、次のいずれかの方法を使用して、テンプレートをデバイスに適用する前にテンプレートのパラメータを更新できます。
 - 交換用デバイスの行で [...] をクリックし、[Edit Device Template] を選択します。必要に応じてパラメータを編集します。
 - ダウンロードして編集した CSV ファイルをアップロードして、交換用デバイスのパラメータを更新します。CSV ファイルをアップロードするには、[Upload] (上矢印ボタン) をクリックして、CSV ファイルに移動します。

E. 新しいデバイスをオンボードする

次のいずれかの方法を使用して、新しいデバイスをオンボードします。



(注) 新しいデバイスをインベントリにオンボーディングする方法は、一般的にデバイスのオンボーディングに関連した方法です。それらは、デバイスの交換に固有の方法ではありません。

• プラグアンドプレイ (PnP)

詳細については、『[Cisco Catalyst SD-WAN Getting Started Guide](#)』の「[Plug and Play Onboarding Workflow](#)」セクションと、『[Cisco Catalyst SD-WAN: WAN Edge Onboarding](#)』ガイドを参照してください。

• Bootstrap

詳細については、『[Cisco Catalyst SD-WAN Getting Started Guide](#)』の「[Non-PnP Onboarding](#)」セクションと、『[Cisco Catalyst SD-WAN: WAN Edge Onboarding](#)』を参照してください。

• 手動展開



(注) 新しいデバイスを構成するには、前述のパート A で保存した構成ファイルを使用できます。



- (注) 手動展開方法では、新しいデバイス用のルート認証局（CA）をインストールする必要があります。

詳細については、『[Cisco Catalyst SD-WAN: WAN Edge Onboarding](#)』を参照してください。
ルート CA のインストールについては、『[Cisco Catalyst SD-WAN Getting Started Guide](#)』の「[Enterprise Certificates](#)」セクションを参照してください。

異なるサーバーでの Cisco Catalyst SD-WAN Manager の使用

1 つ以上の Cisco SD-WAN Manager サーバーから次の操作を並行して実行できます。

- Cisco SD-WAN Manager メニューから **[Maintenance]** > **[Software Upgrade]** の順に選択して、次の操作を行います。
 - デバイスのソフトウェアイメージをアップグレードします。
 - デバイスのソフトウェアイメージをアクティブ化します。
 - デバイスからソフトウェアイメージを削除します。
 - ソフトウェアイメージをデバイスのデフォルトイメージに設定します。
- Cisco SD-WAN Manager メニューから **[Maintenance]** > **[Device Reboot]** の順に選択して、デバイスを再起動します。
- Cisco SD-WAN Manager メニューから **[Configuration]** > **[Templates]** の順に選択して、テンプレートを管理します。
 - デバイスをデバイステンプレートにアタッチします。
 - デバイステンプレートからデバイスをデタッチします。
 - デバイスがアタッチされているデバイステンプレートの変数値を変更します。

テンプレート操作には、次のルールが適用されます。

- デバイステンプレートがデバイスに既にアタッチされている場合は、その機能テンプレートの 1 つを変更できます。**[Update]** > **[Configure Devices]** をクリックすると、他のすべてのテンプレート操作（デバイスのアタッチ、デバイスのデタッチ、デバイス値の編集など）は、更新操作が完了するまで、すべての Cisco SD-WAN Manager サーバーでロックされます。つまり、更新が完了するまで、別の Cisco SD-WAN Manager サーバー上のユーザーはテンプレート操作を実行できません。

- 1 つまたは複数の Cisco SD-WAN Manager サーバーから、さまざまなデバイスでデバイステンプレートのアタッチおよびデタッチ操作を同時に実行できます。ただし、これらの操作のいずれかが 1 つの Cisco SD-WAN Manager サーバーで進行中の場合、アタッチまたはデタッチ操作が完了するまで、どのサーバーの機能テンプレートも編集できません。

Cisco Catalyst SD-WAN Manager Web アプリケーションサーバーへのログイン

Cisco SD-WAN Manager は、実行中の Cisco SD-WAN Manager にログインするための Web アプリケーションサーバーとして実行されます。

Cisco SD-WAN Manager が 1 つあるオーバーレイネットワークでは、サーバーにログインするには、HTTPS を使用し、サーバーの IP アドレスを指定します。URL を `https://ip-address:8443` の形式で入力します。8443 は Cisco SD-WAN Manager で使用されるポート番号です。[login] ページで、有効なユーザー名とパスワードを入力して、[Log In] をクリックします。正しいパスワードの入力を 5 回試行できます。間違ったパスワードを 5 回入力すると、ユーザーはデバイスからロックアウトされ、15 分間待ってから、再度ログインを試行する必要があります。

一群の Cisco SD-WAN Manager があるオーバーレイネットワークでは、クラスタにより、Web アプリケーションサーバーの役割で動作している Cisco SD-WAN Manager の 1 つにログインできます。HTTPS を使用します（いずれかの Cisco SD-WAN Manager の IP アドレスを `https://ip-address:8443` の形式で指定）。クラスタソフトウェアは、Web アプリケーションサーバーとして動作する個々の Cisco SD-WAN Manager の間でログインセッションを負荷分散します。ログインする Cisco SD-WAN Manager は制御できません。

Cisco SD-WAN Manager クラスタでは、無効なログイン情報を入力すると、無効なログインエラーメッセージが表示されるまでに時間がかかる場合があります。クラスタのサイズが大きくなるにつれて時間が長くなります。この遅延は、各 Cisco SD-WAN Manager がログイン情報の検証を順番に試行するために発生します。いずれの Cisco SD-WAN Manager サーバーでも認証されない場合にのみ、ユーザーに無効なログインエラーメッセージが表示されます。

ログインしている Cisco SD-WAN Manager を確認するには、画面の上部にある Cisco SD-WAN Manager ツールバーを調べます。この特定の Cisco SD-WAN Manager サーバーに関する詳細情報を表示するには、[Monitor] > [Devices] の検索フィルタにサーバーの名前を入力します。

Cisco vManage リリース 20.6.x 以前：ログインしている Cisco SD-WAN Manager を確認するには、画面の上部にある Cisco SD-WAN Manager ツールバーを調べます。この特定の Cisco SD-WAN Manager サーバーに関する詳細情報を表示するには、[Monitor] > [Network] の検索フィルタにサーバーの名前を入力します。

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。