Cisco Catalyst SD-WAN Cloud OnRamp コンフィギュレーションガイド、Cisco IOS XE Catalyst SD-WAN リリース 17.x

最終更新：2024 年 10 月 14 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/

目 次

第 1 章 最初にお読みください 1

第 2 章 Cisco IOS XE（SD-WAN）の新機能 3

第 3 章 Cloud OnRamp for IaaS 5

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS 6

概要 6

サポートされている Cisco Cloud Service プロバイダーとサポートされている Cisco Catalyst SD-WAN クラウドデバイス 8

Cisco Catalyst SD-WAN クラウドデバイスの前提条件 9

Cisco SD-WAN Manager サーバーのプロビジョニング 9

Cisco SD-WAN Manager での Cisco Catalyst SD-WAN クラウドデバイスの有無の確認 10

Cisco Catalyst SD-WAN クラウドデバイスのデバイステンプレートの設定 11

Cisco Catalyst SD-WAN クラウドデバイスへのデバイステンプレートのアタッチ 11

AWS の前提条件 13

AWS での Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定 14

ホストおよびトランジット VPC の管理 20

ホスト VPC の表示 20

トランジット VPC へのホスト VPC のマッピング 21

ホスト VPC のマッピング解除 21

トランジット VPC の表示 22

トランジット VPC の追加 22

デバイスペアの削除 22

トランジット VPC の削除 23

デバイスペアの追加 24
トランジット VPC のデバイスペアの履歴 24
中継 VPC の編集 25
Microsoft Azure の前提条件 25
Microsoft Azure の Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定 29
ホストおよびトランジット VNet の管理 34
ホスト VNet の表示 34
既存のトランジット VNet へのホスト VNet のマッピング 34
ホスト VNet のマッピング解除 35
トランジット VNet の表示 35
トランジット VNet の追加 35
トランジット VNet の削除 36
Cisco Catalyst SD-WAN Cloud OnRamp for IaaS のトラブルシューティング 36
機能テンプレートの設定例 40
デバイステンプレート変数値の例 47
Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の例 47

第 4 章 **Cloud OnRamp for Colocation 51**
Cloud OnRamp for Colocation ソリューションの展開 53
Cloud OnRamp for Colocation デバイスの管理 54
Cloud OnRamp Colocation デバイスの追加 55
Cloud OnRamp for Colocation デバイスの削除 56
クラスタの管理 57
クラスタのプロビジョニングと構成 59
クラスタの作成とアクティブ化 60
クラスタの設定 62
クラスタアクティベーションの進行状況 73
クラスタの表示 76
クラスタの編集 76
CSP デバイスのクラスタへの追加 77
クラスタからの CSP デバイスの削除 79

Cisco Colo Manager がある CSP の削除 80
RMA 後の Cisco CSP デバイスの交換 82
Cisco CSP デバイスの返却 82
Cisco CSP デバイスの RMA プロセス 83
CSP デバイスのバックアップと復元の前提条件と制限事項 84
クラスタの削除 85
クラスタの再アクティブ化 86
サービス グループの管理 87
サービスグループでのサービスチェーンの作成 87
サービスチェーンの QoS 94
サービスグループの複製 96
カスタムサービスチェーンの作成 98
共有 PNF デバイスによるカスタムサービスチェーン 99
共有 VNF デバイスによるカスタムサービスチェーン 103
サービスグループの表示 105
サービスグループの編集 105
クラスタ内のサービスグループの接続または切断 106
VM カタログとリポジトリの管理 107
VNF イメージのアップロード 109
カスタマイズされた VNF イメージの作成 111
VNF イメージの表示 117
VNF イメージの削除 118
Cisco SD-WAN Manager を使用した Cisco NFVIS のアップグレード 118
NFVIS アップグレードイメージのアップロード 119
Cisco NFVIS アップグレードイメージを使用した CSP デバイスのアップグレード 119
サポートされるアップグレードシナリオと推奨される接続 121
Cisco Catalyst SD-WAN Manager からの Cloud OnRamp for Colocation デバイスの動作ステータスのモニター 122
Cisco Colo Manager の正常性の表示 124
VNF に関する情報の表示 125
Cloud OnRamp Colocation クラスタのモニター 127

Cloud OnRamp Colocation クラスタのパケットキャプチャ 131
Cisco Catalyst SD-WAN Cloud OnRamp for Colocation マルチテナント機能 134
コロケーション マルチテナント機能の概要 134
マルチテナント環境での役割と機能 136
マルチテナント環境での推奨仕様 137
コロケーション マルチテナント機能の前提条件と制限事項 138
サービスプロバイダー機能 139
新しいテナントのプロビジョニング 139
コロケーション ユーザー グループからの RBAC ユーザーの削除 141
テナント コロケーション クラスタの管理 142
テナント機能 143
テナントとしてのコロケーションクラスタの管理 143
共同管理されたマルチテナント環境でのコロケーション クラスタ デバイスと Cisco Catalyst SD-WAN デバイスのモニター 144

第 I 部 : **Cloud OnRamp for SaaS** 147

第 5 章 **Cloud OnRamp for SaaS、Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降** 149
Cloud onRamp for SaaS に関する情報 154
Cloud onRamp for SaaS を使用する一般的なシナリオ 154
シナリオ 1：ダイレクト インターネット アクセス リンクを介したクラウドアクセス 154
シナリオ 2：ゲートウェイサイトを介したクラウドアクセス 155
シナリオ 3：ハイブリッドアプローチ 155
Office 365 トラフィックカテゴリの指定 156
ベストパスの決定 156
複数のインターフェイス間でのロードバランシング 157
ゲートウェイサイトの VPN 0 インターフェイスを介した Cloud OnRamp for SaaS のプローブに関する情報 157
Webex の Cloud OnRamp for SaaS のサポートに関する情報 159
SD-AVC Cloud Connector に関する情報 161
Office 365 トラフィックのパススコアの表示に関する情報 162
特定のポリシーのトラフィックカテゴリとサービスエリアの設定に関する情報 162

特定のポリシーのトラフィックカテゴリとサービスエリアの設定の利点 162
特定のサイトの特定のアプリケーションに対する Cloud OnRamp for SaaS の動作の有効化に関する情報 162
特定のサイトの特定のアプリケーションに対する Cloud OnRamp for SaaS の動作の有効化の利点 163
Microsoft 365 SaaS トラフィックの可視性に関する情報 163
Microsoft 365 SaaS トラフィックの可視性の利点 163
Microsoft 365 トラフィックのベストパスの決定での Microsoft テレメトリデータの包含または除外に関する情報 163
ループバック、ダイヤラ、およびサブインターフェイスの Cloud OnRamp for SaaS のサポートに関する情報 165
データプレフィックスの除外に関する情報 165
フェールオーバーの高速化のためのトラッカーの使用に関する情報 165
Cloud onRamp for SaaS の利点 166
ゲートウェイサイトの VPN 0 インターフェイスを介した Cloud OnRamp for SaaS のプローブの利点 166
Webex の Cloud onRamp for SaaS のサポートの利点 166
Cloud onRamp for SaaS でサポートされるデバイス 167
Cloud OnRamp for SaaS の前提条件 167
Cloud OnRamp for SaaS の前提条件、全般 168
ゲートウェイサイトの VPN 0 インターフェイスを介した Cloud OnRamp for SaaS のプローブの前提条件 168
Webex の Cloud OnRamp for SaaS のサポートの前提条件 169
特定のポリシーのトラフィックカテゴリとサービスエリアの設定の前提条件 169
特定のサイトの特定のアプリケーションに対する Cloud OnRamp for SaaS の動作の有効化の前提条件 169
Microsoft 365 SaaS トラフィックの可視性の前提条件 169
Microsoft 365 トラフィックのベストパスの決定での Microsoft テレメトリデータの包含または除外の前提条件 170
Webex サーバー側メトリックの前提条件 170
ループバック、ダイヤラ、およびサブインターフェイスの Cloud OnRamp for SaaS のサポートの前提条件 170

Cloud OnRamp for SaaS アプリケーションのデータプレフィックスリストの除外の前提条件 170
DIA トラッカーを使用した高速フェールオーバーの前提条件 171
Cloud onRamp for SaaS の制約事項 171
Cloud OnRamp for SaaS の制約事項、全般 171
Webex アプリケーションの制約事項 172
トラッカーと DIA およびゲートウェイサイトの関連付けの制約事項 173
Cloud onRamp for SaaS のユースケース 173
ゲートウェイサイトの VPN 0 インターフェイスを介した Cloud OnRamp for SaaS のプローブのユースケース 173
SD-AVC Cloud Connector のユースケース 173
トラフィックカテゴリとサービスエリアの設定のユースケース 174
特定のサイトでの特定のアプリケーションの有効化のユースケース 174
Cloud OnRamp for SaaS の最適化からのデータプレフィックスの除外のユースケース 175
Cloud onRamp for SaaS の設定 175
Cloud OnRamp for SaaS の有効化、Cisco IOS XE Catalyst SD-WAN デバイス 175
Cloud OnRamp for SaaS の有効化 176
Cisco SD-WAN Manager を使用した Cloud OnRamp for SaaS のアプリケーションの設定 176
Cisco SD-WAN Manager を使用した Cloud onRamp for SaaS のサイトの設定 180
クライアントサイトの設定 180
ゲートウェイサイトのインターフェイスの編集 184
ダイレクト インターネット アクセス（DIA）サイトの設定 186
ダイレクト インターネット アクセス（DIA）サイトのインターフェイスの編集 188
Office 365 トラフィックのアプリケーション フィードバック メトリックの有効化 189
Microsoft による Office 365 トラフィックのテレメトリの提供の有効化 190
Cloud OnRamp for SaaS の Webex の有効化 192
Webex サーバー側メトリックの有効化 192
Cloud OnRamp for SaaS の Webex サーバー情報の更新 194
Cisco SD-WAN Manager を使用した特定のポリシーのトラフィックカテゴリとサービスエリアの設定 194
Cisco SD-WAN Manager を使用した特定のサイトの特定のアプリケーションで Cloud OnRamp の動作を有効にするための AAR ポリシーの設定 196

アプリケーションの可視性とフローの可視性の有効化 196
Cisco SD-WAN Manager を使用した Microsoft 365 SaaS トラフィックの可視性の設定 197
アプリケーションの使用状況の表示 197
Cloud onRamp for SaaS の確認 198
アプリケーションが Cloud OnRamp for SaaS に対して有効になっていることの確認 199
Cisco SD-WAN Manager を使用した特定のポリシーのトラフィックカテゴリとサービスエリアの設定に対する変更の確認 199
Cisco SD-WAN Manager を使用した特定のデバイスで有効になっているアプリケーションの確認 200
Cisco SD-WAN Manager を使用した特定のポリシーで有効になっているアプリケーションの確認 200
Cisco SD-WAN Manager を使用した除外されたデータプレフィックスの確認 200
Cloud onRamp for SaaS のモニター 201
モニタリング対象アプリケーションの詳細の表示 201
Cloud OnRamp for SaaS の Webex のステータスのモニター 205
SD-AVC Cloud Connector を使用したサーバー情報の表示 206
Cloud OnRamp for SaaS の除外されたデータプレフィックスリストのモニター 208
Syslog およびコンソールログのログの表示 208
SIG トンネル経由の Cloud onRamp for SaaS 209
SIG トンネル経由の Cloud onRamp for SaaS の前提条件 209
SIG トンネル経由の Cloud OnRamp for SaaS の制約事項 209
SIG トンネル経由の Cloud OnRamp for SaaS に関する情報 210
SIG トンネル経由の Cloud onRamp for SaaS の利点 211
SIG トンネル経由の Cloud onRamp for SaaS のユースケース 211
SIG トンネル経由の Cloud OnRamp for SaaS の設定 215
CLI を使用した SIG トンネル経由の Cloud onRamp for SaaS の設定 216
SIG トンネル経由の Cloud OnRamp for SaaS のモニター 217
CLI を使用した SIG トンネル経由の Cloud onRamp for SaaS のモニター 218
SIG トンネル経由の Cloud onRamp for SaaS の設定例 219
Cloud OnRamp for SaaS のトラブルシューティング 220
Webex アプリケーションのテレメトリを有効にできない 220
各 Webex リージョンのベストパスを特定できない 220

Debug コマンドと Show コマンド 221

第 6 章 アプリケーションリスト 227

SaaS アプリケーションリストに関する情報 228

SaaS アプリケーションリストの利点 229

SaaS アプリケーションリストの前提条件 229

SaaS アプリケーションリストの制約事項 230

SaaS アプリケーションリストのユースケース 230

ワークフロー 231

Cisco SD-WAN Manager を使用したユーザー定義の SaaS アプリケーションリストの作成 232

SaaS アプリケーションリストの表示 233

第 7 章 Cloud OnRamp for SaaS、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 235

概要：Cloud onRamp for SaaS の設定方法 237

Cloud onRamp for SaaS を使用する一般的なシナリオ 238

シナリオ 1：ダイレクト インターネット アクセス リンクを介したクラウドアクセス 239

シナリオ 2：ゲートウェイサイトを介したクラウドアクセス 241

シナリオ 3：ハイブリッドアプローチ 243

プローブ機能テンプレートの作成 245

Cloud onRamp for SaaS のポリシーの作成 248

第 II 部： Cloud OnRamp for Multicloud 253

第 8 章 Cloud OnRamp for Multicloud 255

第 9 章 AWS の統合 257

AWS 統合に関する情報 259

AWS ブランチ接続の概要 262

AWS Cloud WAN 263

Cisco Catalyst SD-WAN Manager リリース 20.12.1 から Cisco Catalyst SD-WAN Manager リリース 20.13.1 へのアップグレードの考慮事項 264

設定グループを使用した AWS 統合のためのデバイスの設定に関する情報 264

AWS 統合の制約事項 264
AWS 統合の設定 266
AWS クラウドアカウントの作成 266
クラウドグローバル設定の構成 269
ホスト プライベート ネットワークの検出 277
クラウドゲートウェイの作成 278
サイトアタッチメントの設定 280
インテント管理 - 接続 282
トランジット ゲートウェイ ピアリング 285
監査管理 286
Cisco SD-WAN Manager を使用した AWS 統合のモニター 287

第 10 章 **Amazon GovCloud（米国）の統合 289**
AWS GovCloud（米国）統合に関する情報 290
AWS GovCloud（米国）統合の利点 291
AWS GovCloud（米国）でサポートされるデバイス 292
AWS GovCloud（米国）統合の前提条件 292
AWS GovCloud（米国）統合の制約事項 293
AWS GovCloud（米国）統合のユースケース 293
AWS GovCloud（米国）の設定 293

第 11 章 **Microsoft Azure Virtual WAN の統合 295**
Azure Virtual WAN 統合に関する情報 297
Azure Virtual WAN ハブと Cisco Catalyst SD-WAN の統合 297
仮想 WAN ハブ統合の仕組み 298
接続モデル 300
セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックフローのルーティング 302
Azure Virtual WAN の監査 302
定期監査に関する情報 303
監査の不一致と解決 303

ネットワーク仮想アプライアンスの SKU スケール値 305
ネットワーク仮想アプライアンスのセキュリティルールの設定 306
NVA への Azure ExpressRoute 接続に関する情報 306
各リージョンの複数の仮想ハブに関する情報 307
Azure Virtual WAN 統合でサポートされるデバイス 307
サポートされている Azure インスタンス 307
Azure Virtual WAN 統合の前提条件 309
セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックのルーティングの前提条件 309
ネットワーク仮想アプライアンスの Azure SKU スケーリング、監査、およびセキュリティルールの前提条件 309
Azure Virtual WAN 統合の制約事項 310
Azure Virtual WAN 統合の制約事項 310
セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックのルーティングの制約事項 310
ネットワーク仮想アプライアンスの Azure SKU スケーリング、監査、およびセキュリティルールの制約事項 311
リージョンごとの複数の仮想ハブの制約事項 311
Azure Virtual WAN 統合のユースケース 311
セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックフローのルーティングのユースケース 311
Azure SKU スケーリングのユースケース 311
Azure 監査のユースケース 312
NVA のセキュリティルールのユースケース 312
Azure Virtual WAN 統合の設定 312
Azure Virtual WAN ハブの設定 312
設定要件 312
Azure クラウドアカウントの統合 313
クラウドゲートウェイの作成と管理 316
ホスト VNet の検出とタグの作成 319
VNet タグとブランチネットワーク VPN のマッピング 320
VNet の再調整 320

Azure ポータルからの Azure Virtual WAN ハブの設定 321
セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックフローのルーティングの設定 325
Azureのセキュリティ保護付き仮想ハブへのローカル発信トラフィックフローのルーティング 325
ローカルブランチルータへの Azure 発信トラフィックフローのルーティング 326
SKU スケール値の設定 327
オンデマンド監査の開始 327
定期監査の有効化 328
NVA のセキュリティルールの設定 328
Azure Virtual WAN 統合の確認 329
クラウドゲートウェイの表示、編集、または削除 329
Azure SKU スケール値の更新の確認 330
ネットワーク仮想アプライアンスのセキュリティルールの確認 330
Cisco SD-WAN Manager を使用した Azure Virtual WAN 統合のモニター 331
Azure Virtual WAN 統合のモニター 331

第 12 章 **米国政府向け Microsoft Azure の統合 333**
米国政府向け Azure 統合に関する情報 334
米国政府向け Azure 統合の利点 335
米国政府向け Azure でサポートされるデバイス 336
米国政府向け Azure 統合の前提条件 336
米国政府向け Azure 統合の制約事項 336
米国政府向け Azure 統合のユースケース 336
米国政府向け Azure の設定 336
米国政府向け Azure 統合のモニター 337

第 13 章 **Google Cloud の統合 339**
サポートされるプラットフォームとインスタンス 343
制限事項と制約事項 343
Google Cloud を使用した Cisco Catalyst SD-WAN クラウドゲートウェイの概要 344

クラウドゲートウェイでの Cisco Catalyst 8000V インスタンスの水平スケーリング 345
Google Service Directory の統合とルックアップ 345
接続モデル 347
クラウドゲートウェイの分離されたサイト間およびサイトとクラウド間の接続設定 349
Google Cloud を使用した Cisco Catalyst SD-WAN クラウドゲートウェイの設定 350
設定要件 350
デバイステンプレートへの Cisco Catalyst 8000V インスタンスのアタッチ 351
Cisco SD-WAN Manager と Google Cloud アカウントの関連付け 351
クラウドグローバル設定の構成 353
ホスト VPC の検出とタグの作成 354
クラウドゲートウェイの作成と管理 355
VPC タグとブランチネットワーク VPN のマッピング 357
Service Directory のルックアップと検出されたアプリケーションによるトラフィックポリシー 359
Service Directory のルックアップの有効化 359
クラウドで検出されたアプリケーションを使用したトラフィックポリシーの作成 361
接続のモニター 362
監査 362
クラウド リソース インベントリの表示 364

第 14 章 マルチクラウドサービスのモニタリングのための Cisco Catalyst SD-WAN Manager のサポート 365
Cisco SD-WAN Manager を使用したマルチクラウドサービスのモニタリングの制約事項 366
Cisco SD-WAN Manager を使用したマルチクラウドサービスのモニタリングに関する情報 366
地理的ビュー 367
クラウドとインターコネクト ダッシュボード 368
クラウドゲートウェイのサマリービュー 369
インターコネクト ゲートウェイのサマリービュー 370

第 III 部： Cloud OnRamp for Multicloud：Cisco Catalyst SD-WAN Cloud Interconnect 371

第 15 章 Cloud OnRamp for Multicloud：Cisco Catalyst SD-WAN Cloud Interconnect 373

第 16 章 Cisco Catalyst SD-WAN Cloud Interconnect with Megaport のライセンス管理 375

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport のライセンス管理に関する情報 377

インターコネクト ゲートウェイ ライセンス 378

インターコネクト接続ライセンス 379

補足ライセンス 382

ライセンスの適用 383

インターコネクト ゲートウェイのライセンスの適用 383

短距離インターコネクト接続のライセンスの適用 384

長距離インターコネクト接続のライセンスの適用 385

AWS ホスト型接続のライセンスの適用 386

従量制ライセンスに関する情報 387

Megaport アカウントに関連付けられたライセンスの表示 388

インターコネクト ゲートウェイに関連付けられたライセンス SKU の確認 390

インターコネクト接続に関連付けられたライセンス SKU の確認 391

第 17 章 Cisco Catalyst SD-WAN Cloud Interconnect with Megaport 393

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport の前提条件 399

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport の制約事項 400

暗号化されたマルチクラウド インターコネクトの制約事項 403

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport の使用上の注意 404

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport に関する情報 407

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport の利点 409

暗号化されたマルチクラウド インターコネクト 409

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport の設定ワークフロー 410

Cisco SD-WAN Cloud Interconnect with Megaport の前提条件の設定 412

Cisco SD-WAN Manager と Megaport アカウントの関連付け 412

インターコネクト ゲートウェイのグローバル設定の構成 413

Cisco Catalyst 8000v インスタンスへの Megaport テンプレートのアタッチ 415

Megaport の場所でのインターコネクト ゲートウェイの作成 416

AWS へのインターコネクトの作成 419

AWS アカウントと Cisco SD-WAN Manager の関連付け 419
ホスト プライベート ネットワークの検出と AWS VPC のタグ付け 420
インターコネクト ゲートウェイから AWS への Direct Connect パブリックホスト型 VIF の作成 423
インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect プライベートホスト型 VIF の作成 425
インターコネクト ゲートウェイから AWS への Direct Connect パブリックホスト型接続の作成 429
インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect プライベートホスト型接続の作成 431
インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect トランジットホスト型接続の作成 435
Google Cloud へのインターコネクトの作成 439
Cisco SD-WAN Manager と Google Cloud アカウントの関連付け 439
インターコネクト ゲートウェイから Google Cloud Router へのインターコネクトの作成 440
Google Cloud 内のクラウドゲートウェイへのインターコネクト接続の作成 446
Microsoft Azure へのインターコネクトの作成 451
Cisco SD-WAN Manager と Microsoft Azure アカウントの関連付け 451
ホスト プライベート ネットワークの検出と Microsoft Azure VNet のタグ付け 452
インターコネクト ゲートウェイから Microsoft Azure ExpressRoute への Microsoft ピアリング接続の作成 455
インターコネクト ゲートウェイから Microsoft Azure ExpressRoute へのプライベートピアリング接続の作成 460
インターコネクト ゲートウェイ間のインターコネクトの作成 470
設定の確認と変更 471
インターコネクト ゲートウェイと接続の概要の表示 471
接続の表示、編集、または削除 472
インターコネクト ゲートウェイの表示、編集、または削除 478
インターコネクトアカウントの表示、編集、または削除 479
監査管理 480
Cisco Catalyst SD-WAN Cloud Interconnect with Megaport のトラブルシューティング 481

第 18 章 Cisco Catalyst SD-WAN Cloud Interconnect with Equinix 485

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の前提条件 487

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の制約事項 488

暗号化されたマルチクラウド インターコネクトの制約事項 490

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の使用上の注意 491

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix に関する情報 494

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の利点 497

暗号化されたマルチクラウド インターコネクト 497

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の設定ワークフロー 498

Cisco SD-WAN Cloud Interconnect with Equinix の前提条件の設定 501

Cisco SD-WAN Manager と Equinix アカウントの関連付け 501

Equinix インターコネクト ゲートウェイのグローバル設定の構成 502

Cisco CSR 1000v または Cisco Catalyst 8000v インスタンスへの Equinix テンプレートのアタッチ 504

Equinix の場所でのインターコネクト ゲートウェイの作成 505

AWS へのインターコネクトの作成 508

AWS アカウントと Cisco SD-WAN Manager の関連付け 508

ホスト プライベート ネットワークの検出と AWS VPC のタグ付け 508

インターコネクト ゲートウェイから AWS への Direct Connect パブリックホスト型接続の作成 510

インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect プライベートホスト型接続の作成 512

インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect トランジットホスト型接続の作成 515

Google Cloud へのインターコネクトの作成 519

Cisco SD-WAN Manager と Google Cloud アカウントの関連付け 519

インターコネクト ゲートウェイから Google Cloud Router へのインターコネクトの作成 519

Google Cloud 内のクラウドゲートウェイへのインターコネクト接続の作成 525

Microsoft Azure へのインターコネクトの作成 529

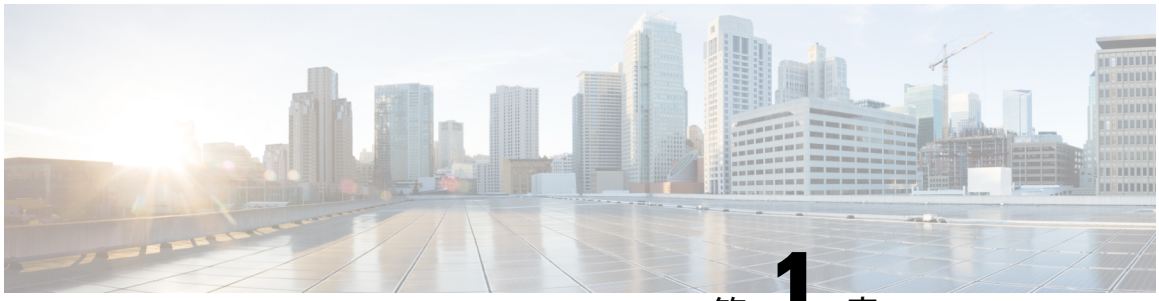
Cisco SD-WAN Manager と Microsoft Azure アカウントの関連付け 529

ホスト プライベート ネットワークの検出と Microsoft Azure VNet のタグ付け 530

インターコネクト ゲートウェイから Microsoft Azure ExpressRoute への Microsoft ピアリング接続の作成 534
インターコネクト ゲートウェイから Microsoft Azure ExpressRoute へのプライベートピアリング接続の作成 539
デバイスリンク 548
デバイスリンクの追加 548
デバイスリンクの削除 549
デバイスリンクの更新 549
インターコネクト ゲートウェイ間のインターコネクトの作成 550
Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の設定の確認と変更 552
インターコネクト ゲートウェイと接続の概要の表示 552
接続の表示、編集、または削除 553
インターコネクト ゲートウェイの表示、編集、または削除 557
インターコネクトアカウントの表示、編集、または削除 558
監査管理 558
Cisco Catalyst SD-WAN Cloud Interconnect with Equinix のトラブルシューティング 560

第 IV 部 : **Cisco Catalyst SD-WAN Cloud OnRamp のトラブルシューティング** 565

第 19 章 **Cisco SD-WAN Cloud OnRamp のトラブルシューティング** 567
概要 567
サポート記事 568
フィードバックのリクエスト 568
免責事項と注意事項 569



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]

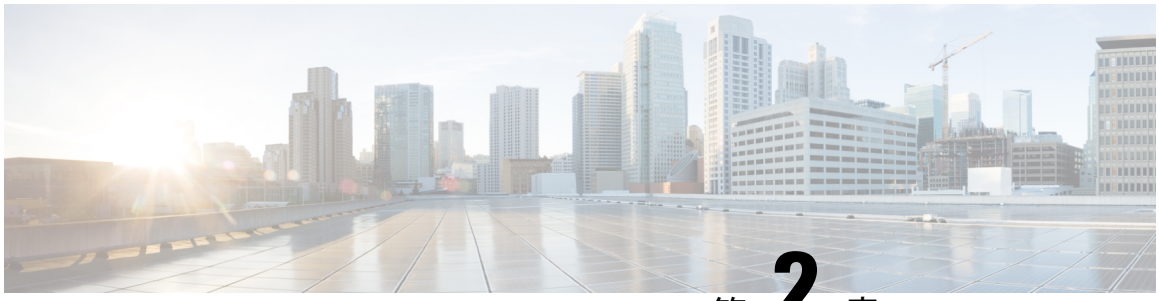
通信、サービス、およびその他の情報

- 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、CiscoDevnet 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ドキュメント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ドキュメント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。



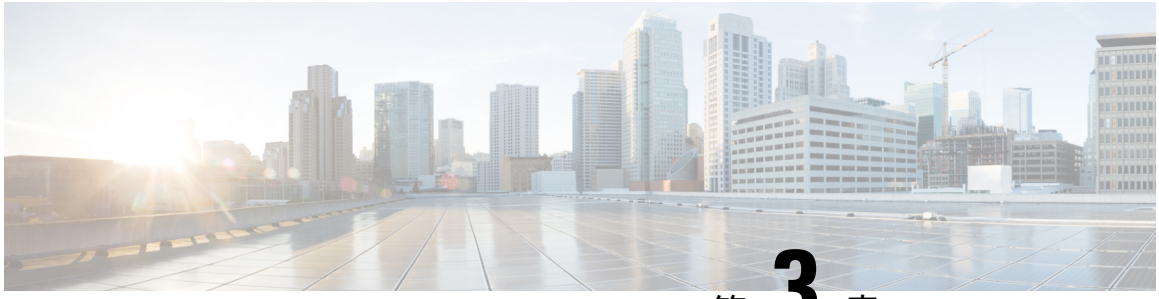
第 2 章

Cisco IOS XE（SD-WAN）の新機能

（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。

（注） 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。次の表に、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新機能と変更された機能を示します。Cisco Catalyst SD-WAN ソリューションに関係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]



第 3 章

Cloud OnRamp for IaaS

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。

- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS （6 ページ）
- 概要 （6 ページ）
- サポートされている Cisco Cloud Service プロバイダーとサポートされている Cisco Catalyst SD-WAN クラウドデバイス （8 ページ）
- Cisco Catalyst SD-WAN クラウドデバイスの前提条件 （9 ページ）
- AWS の前提条件 （13 ページ）
- AWS での Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定 （14 ページ）
- ホストおよびトランジット VPC の管理 （20 ページ）
- Microsoft Azure の前提条件 （25 ページ）
- Microsoft Azure の Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定 （29 ページ）
- ホストおよびトランジット VNet の管理 （34 ページ）
- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS のトラブルシューティング （36 ページ）
- 機能テンプレートの設定例 （40 ページ）
- デバイステンプレート変数値の例 （47 ページ）
- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の例 （47 ページ）

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS

表 *1:* 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイスの Azure Government クラウドのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	この機能により、Microsoft Azure Government クラウドで Cisco Catalyst 8000V デバイスを設定できます。これらのクラウドデバイスが Microsoft Azure Government クラウドでサポートされるようになったことで、Government クラウドのお客様は、Azure パブリッククラウドですでに利用可能なものと同じ高度なルーティングとセキュリティの利点を利用できます。
Cisco IOS XE Catalyst SD-WAN デバイスの AWS Government クラウドのサポート	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、Amazon Web Services（AWS）Government クラウドで Cisco CSR1000V を設定できます。Cisco CSR1000V が AWS Government クラウドでサポートされるようになったことで、Government クラウドのお客様は、ルーティングのすべての利点を利用して、機密性の高いワークロードをクラウドに移動し、データを安全に管理することができます。
	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	このリリース以降では、AWS Government クラウドで Cisco Catalyst 8000V デバイスがサポートされます。

概要

（注） Cisco vManage リリース 20.9.1 以降では、Cloud OnRamp for Multicloud を使用してクラウドインフラストラクチャを設定することを推奨します。Cloud OnRamp for IaaS は、今後のリリースで段階的に廃止されます。

Cisco Catalyst SD-WAN Cloud OnRamp for Infrastructure as a Service（IaaS）は、Cisco Catalyst SD-WAN オーバーレイネットワークのファブリックをパブリック クラウド インスタンスに拡張します。Cisco Catalyst SD-WAN Cloud OnRamp for IaaS を使用すると、Cisco Cloud Services Router 1000V シリーズと Cisco Catalyst 8000V デバイスを備えたブランチがパブリック クラウド アプリケーション プロバイダーに直接接続できます。物理データセンターの必要性を排除することで、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS は SaaS アプリケーションのパフォーマンスを向上させます。

Cisco Catalyst 8000V デバイスの詳細については、『Cisco Catalyst 8000V Edge Software Configuration Guide』を参照してください。

オーバーレイネットワークとパブリック クラウドアプリケーションの間の接続は、1 ～ 4 つのペアの冗長 Cisco Catalyst SD-WAN クラウドデバイスによって提供されます。これらのデバイスは、オーバーレイネットワークとアプリケーションの間のトランジットとして連携して機能します。冗長デバイスを使用してトランジットを形成することで、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS によりパブリッククラウドに対するパスの復元力を得ることができます。さらに、冗長ルータを使用すると電圧低下保護に役立ち、パブリック クラウド アプリケーションの可用性が向上します。2 つのルータが連携することで、電圧低下時に発生する可能性のあるリンクの通信品質の低下を修復できます。これらのデバイスは、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS ワークフローの一環として設定できます。

Amazon Web Services（AWS）および Microsoft Azure Government クラウド（GovCloud）での Cisco Catalyst SD-WAN Cloud OnRamp for IaaS サポートにより、機密データをホストするように Cisco CSR1000V および Cisco Catalyst 8000V デバイスを設定することができます。AWS または Microsoft Azure GovCloud（米国）は、米国政府の機関および取引先が機密性の高いワークロードを政府機関のクラウドに移動できるようにする、分離された AWS または Azure リージョンです。取引先は、ルーティング機能を提供し、強力な暗号スイートによるフルパス暗号化をサポートしているこれらのデバイスを使用できます。Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定中に選択できるリージョンは、AWS または Microsoft Azure GovCloud の仕様に関連しています。GovCloud（米国）アカウントの設定の詳細については、AWS GovCloud のドキュメントおよび Microsoft Azure GovCloud のドキュメントを参照してください。

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS は、AWS Virtual Private Cloud（VPC）および Azure Virtual Network（VNet）と連携して動作します。

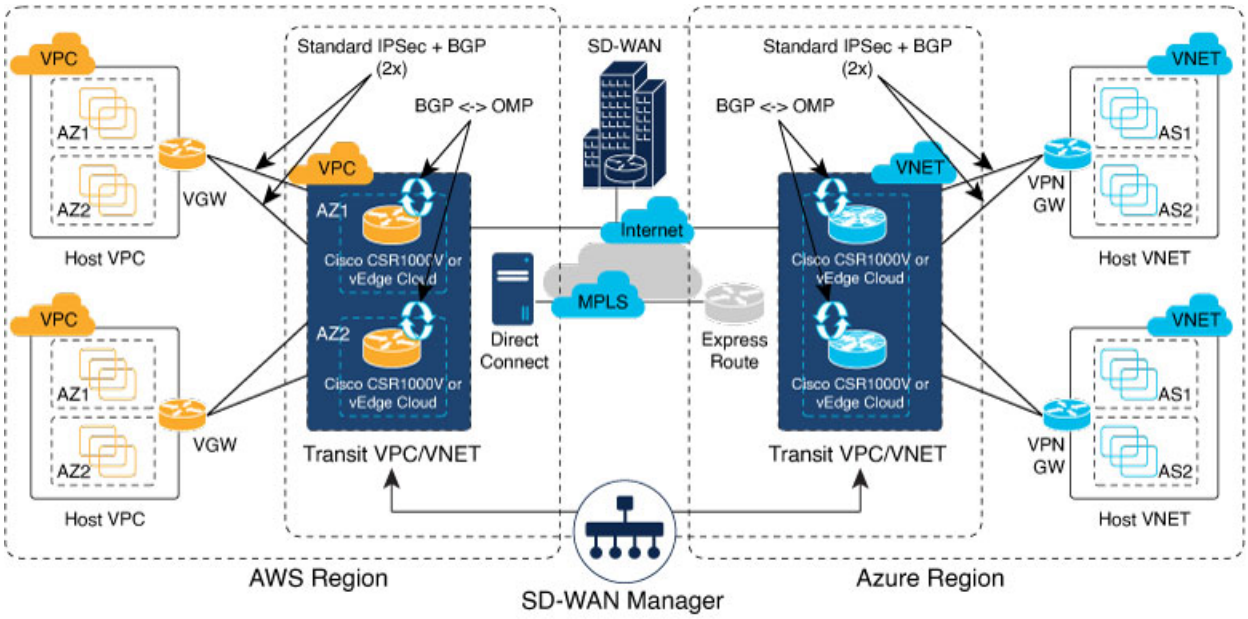
Cisco Catalyst SD-WAN Cloud OnRamp for IaaS ソリューションを展開するための主な手順は次のとおりです。

1. Cisco Catalyst SD-WAN Cloud OnRamp for IaaS に使用できる Cisco SD-WAN Manager 内の未使用の Cisco Catalyst SD-WAN クラウドデバイスのペアを 1 ～ 4 つ特定します。
2. 基本的なデバイステンプレートを設定し、両方の Cisco Catalyst SD-WAN クラウドデバイスにアタッチします。
3. Cisco SD-WAN Manager を使用して設定する場合は、AWS または Azure API のログイン情報（アクセスキーと秘密キー）を入力します。
4. トランジット仮想プライベートクラウド（VPC）またはトランジット仮想ネットワーク（VNet）の設定を追加します。
5. ホスト VPC またはホスト VNet を検出し、トランジット VPC またはトランジット VNet にマッピングします。

次の図は、AWS と Microsoft Azure が統合された Cisco Catalyst SD-WAN Cloud OnRamp for IaaS のトポロジを示しています。オンプレミス上および複数のクラウド上にあるすべての Cisco Catalyst SD-WAN デバイスの単一サーバーとして Cisco SD-WAN Manager を使用して、すべての場所で同じポリシー、セキュリティ、およびその他の Cisco Catalyst SD-WAN のポリシーを適用することができます。AWS と Microsoft Azure のインフラストラクチャは、Cisco Catalyst

SD-WAN ファブリックにシームレスに統合できます。Cisco Catalyst SD-WAN Cloud OnRamp for IaaS ワークフローがすべての手順を自動化し、Cisco SD-WAN Manager サーバーが数分以内にソリューション全体を構築します。

図 *1 : Cisco Catalyst SD-WAN Cloud OnRamp for IaaS* のトポロジ



サポートされている Cisco Cloud Service プロバイダーとサポートされている Cisco Catalyst SD-WAN クラウドデバイス

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS では、次の IaaS パブリック クラウド プロバイダーがサポートされています。

- Amazon AWS
- Microsoft Azure

次のデバイスがサポートされています。

- Cisco Cloud Services Router 1000V シリーズ（Cisco CSR1000V）
- Cisco Catalyst 8000V Edge ソフトウェア（Cisco Catalyst 8000V）

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降では、Cisco Catalyst 8000V は Cisco CSR1000V に置き換わっています。そのため、Azure Government クラウドのサポートは Cisco Catalyst 8000V でのみ使用可能であり、Cisco Catalyst 8000V デバイスを使用することを推奨します。

このドキュメントでは、サポートされているデバイスをまとめて Cisco Catalyst SD-WAN クラウドデバイスと呼びます。

Cisco Catalyst SD-WAN クラウドデバイスの前提条件

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS を設定する前に、次のデバイス要件を満たしていることを確認してください。

- Cisco SD-WAN Manager で、少なくとも 2 つの Cisco CSR1000V または Cisco Catalyst 8000V デバイスに使用可能なトークンまたはライセンスがあることを確認します。Cisco SD-WAN Manager での Cisco Catalyst SD-WAN クラウドデバイスの有無の確認 （10 ページ）を参照してください。
- 設定時に、トランジット VPC または VNet 内で使用する Cisco CSR1000V または Cisco Catalyst 8000V デバイスの機能テンプレートとデバイステンプレートを設定します。Cisco Catalyst SD-WAN クラウドデバイスのデバイステンプレートの設定 （11 ページ）を参照してください。
- トランジット VPC または VNet 内で使用する Cisco CSR1000V または Cisco Catalyst 8000V デバイスを表すソフトウェアトークンに、デバイステンプレートをアタッチします。Cisco Catalyst SD-WAN クラウドデバイスへのデバイステンプレートのアタッチ （11 ページ）を参照してください。

Cisco SD-WAN Manager サーバーのプロビジョニング

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS を設定する前に、Cisco SD-WAN Manager サーバーをプロビジョニングします。

1. Cisco SD-WAN Manager サーバーがインターネットにアクセスできることを確認し、AWS または Microsoft Azure に到達できるように DNS サーバーを設定します。DNS サーバーを設定するには、Cisco SD-WAN Manager VPN 機能設定テンプレートで DNS サーバーの IP アドレスを入力します。次に、Cisco SD-WAN Manager を使用して設定テンプレートを VPN 機能に再アタッチします。
2. Cisco Catalyst SD-WAN Cloud OnRamp for IaaS を起動するには、少なくとも 2 つの Cisco Catalyst SD-WAN クラウドデバイスを Cisco SD-WAN Manager サーバーに追加してください。これら 2 つの Cisco Catalyst SD-WAN クラウドデバイスを適切な設定テンプレートにアタッチします。これらのデバイスの設定に次の属性が含まれていることを確認します。
   - ホストネーム

- Cisco Catalyst SD-WAN Validator の IP アドレス
- サイト ID
- 組織名
- eth1 インターフェイスでのトンネルインターフェイスの設定

  Cisco CSR1000V または Cisco Catalyst 8000V デバイスでは、トンネルインターフェイスは GigabitEthernet2 インターフェイス上にあります。

3. Cisco SD-WAN Manager サーバーを現在の時刻と同期していることを確認します。現在の時刻を確認するには、Cisco SD-WAN Manager 画面の上部バーにある [Help (?)] アイコンをクリックします。[Timestamp] フィールドに現在の時刻が表示されます。時刻が正しくない場合は、Cisco SD-WAN Manager サーバーの時刻が Google NTP サーバーなどの NTP タイムサーバーを指すように設定します。サーバータイムを設定するには、Cisco SD-WAN Manager NTP 機能設定テンプレートで、NTP サーバーのホスト名を入力します。次に、Cisco SD-WAN Manager を使用して設定テンプレートを NTP 機能に再アタッチします。Google NTP サーバーは、time.google.com、time2.google.com、time3.google.com、time4.google.com などです。

Cisco SD-WAN Manager での Cisco Catalyst SD-WAN クラウドデバイスの有無の確認

手順

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

ステップ 2 [Device listing] ページで、まだ使用されていない有効な Cisco CSR1000V または Cisco Catalyst 8000V デバイスが少なくとも 2 つあることを確認します。

以下が、有効な未使用のデバイスです。

- [Validity] 列に "valid" という単語があるデバイス。
- [Assigned Template]、[Device Status]、[Hostname]、[System IP]、および [Site ID] 列が空白のデバイス。

Cisco CSR1000V または Cisco Catalyst 8000V デバイスが不足している場合は、software.cisco.com にアクセスし、Plug and Play Connect ポータルを使用してトークンまたはライセンスを追加します。

Cisco Catalyst SD-WAN クラウドデバイスのデバイステンプレートの設定

Cisco SD-WAN Manager 内で 2 つの Cisco CSR1000V または Cisco Catalyst 8000V デバイスに少なくとも最小限のデバイステンプレートが割り当てられていることを確認します。最小限のデバイステンプレートは、デバイステンプレート内の工場出荷時のデフォルトの機能テンプレートを使用するテンプレートです。デバイステンプレート内で、少なくとも 1 つのサービス VPN と管理（VPN 512）インターフェイスが設定されている必要があります。ただし、カスタム機能テンプレート内の展開に固有の設定を含む、完全に機能するデバイステンプレートを設定することを推奨します。Cisco SD-WAN Manager を使用して個々の機能テンプレートとデバイステンプレートを作成する手順については、「Configure the Cisco SD-WAN Routers」を参照してください。

これらのテンプレートをデバイステンプレートにアタッチし、Cloud onRamp for IaaS を使用して設定した後は、機能テンプレートを変更しないでください。Cloud onRamp for IaaS の設定は、変更されたこれらの機能テンプレートの設定を上書きします。

「機能テンプレートの設定例」トピック内に、デバイステンプレートの例と、デバイステンプレートを構成するさまざまな機能テンプレートがあり、Cisco CSR1000V または Cisco Catalyst 8000V デバイスに使用できます。

Cisco Catalyst SD-WAN クラウドデバイスへのデバイステンプレートのアタッチ

デバイステンプレートを Cisco CSR1000V または Cisco Catalyst 8000V デバイスにアタッチすると、Cisco SD-WAN Manager が機能テンプレートに基づいて設定を作成してから、指定された Cisco CSR1000V または Cisco Catalyst 8000V デバイスに設定を保存します。設定を作成して保存する前に、デバイステンプレートにアタッチされている機能テンプレート内のすべての変数を定義します。

.csv ファイルをアップロードする代わりに、Cisco SD-WAN Manager を使用して変数の値を手動で入力するには、次の手順を実行します。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Templates]** > **[Device Templates]** を選択します。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

ステップ 2 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。

この設定にアタッチできる使用可能なデバイスが一覧表示されるポップアップウィンドウが表示されます。使用可能なデバイスのリストには、次のいずれかが含まれています。

- デバイスのホスト名と IP アドレス（Cisco SD-WAN Manager を使用していて既知の場合）。
- デバイスのシャーシのシリアル番号（ネットワーク上で使用できず、Cisco SD-WAN Manager に認識されていない場合）。

Cisco CSR1000V または Cisco Catalyst 8000V デバイスには物理シャーシはありませんが、シャーシのシリアル番号が割り当てられます。このリストには、デバイステンプレートの作成時に定義されたデバイスモデルのみが含まれています。

ステップ 3 設定テンプレートを適用するには、1 つ以上のデバイスを [Available Devices] から選択し、[Selected Devices] に移動します。

（注） このドキュメントでは、2 つの Cisco Catalyst SD-WAN クラウドデバイスを使用して、設定を適用します。

ステップ 4 [Attach] をクリックします。

表示されたウィンドウに、選択した Cisco Catalyst SD-WAN クラウドデバイスが一覧表示されます。

ステップ 5 最初の Cisco CSR1000V または Cisco Catalyst 8000V デバイスに対して、[…] をクリックし、[Edit Device Template] を選択します。

ポップアップウィンドウが表示され、変数のリストと空のテキストボックスが表示されます。チェックボックスを使用してオンとオフの値を示す変数もあります。すべてのテキストボックスに入力してください。デバイステンプレート変数値の例 （47 ページ）のトピックにあるサンプル情報を使用して、変数値を入力することができます。

ステップ 6 [Update] をクリックします。

ステップ 7 2 番目の Cisco CSR1000V または Cisco Catalyst 8000V デバイスに対してステップ 5 ～ 6 を繰り返します。

将来使用するために、変数値を .csv ファイルにダウンロードすることができます。

ステップ 8 [Next] をクリックします。

ウィンドウに、1 つのデバイステンプレートにアタッチされている 2 つのデバイスに設定アクションが適用されていることが示されます。

左側のペインからデバイスを選択して、Cisco Catalyst SD-WAN クラウドデバイスに保存されている設定を表示することができます。

ステップ 9 [Configure Devices] をクリックします。

ステップ 10 表示されたポップアップウィンドウで、[Confirm configuration changes on 2 devices] をオンにします。

ステップ 11 [OK] をクリックします。

[Task View] ウィンドウが表示されます。

しばらくすると、2 つの Cisco CSR1000V または Cisco Catalyst 8000V デバイスのステータスが [Done – Scheduled] になり、デバイスがオフラインであり、オンラインになるとテンプレートがデバイスにアタッチされることを示すメッセージが表示されます。

次のタスク

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS を使用して、AWS トランジット VPC または Azure トランジット VNet 内に 2 つの Cisco CSR1000V または Cisco Catalyst 8000V デバイスを展開できるようになりました。

AWS の前提条件

手順

ステップ 1 有効な AWS アカウントを用意します。

ステップ 2 GovCloud にアクセスするための有効な AWS Government アカウントを用意します。

ステップ 3 AWS Marketplace 内で、使用しているアカウントで Cisco CSR1000V、Cisco Catalyst 8000V デバイスの Amazon マシンイメージ（AMI）に登録します。AWS Marketplace 内で、使用しているアカウントで Amazon マシンイメージ（AMI）に登録するには、次の手順を実行します。

a) Amazon Web Services Marketplace にログインします。

b) AWS Marketplace で「Cisco CSR1000V または Cisco Catalyst 8000V デバイス」を検索します。

AMI のリストが表示されます。

c) リストから、展開する予定の Cisco CSR1000V または Cisco Catalyst 8000V デバイスのリンクをクリックします。

サブスクリプション画面が表示され、Cisco CSR1000V または Cisco Catalyst 8000V デバイスの AMI に登録できます。

d) **[引き続きサブスクライブする（Continue to Subscribe）]** をクリックして登録します。

e) [条件に同意する（Accept Terms）] をクリックします。

しばらくすると、Cisco CSR1000V または Cisco Catalyst 8000V デバイスの AMI を使用するために登録されたことを示すメッセージが表示されます。

（注） Cisco Catalyst SD-WAN Cloud OnRamp for IaaS はトランジット VPC の作成時に Cisco Catalyst SD-WAN クラウドデバイスを自動的に設定するため、[Continue to Configuration] はクリックしないでください。

f) AWS Marketplace からログアウトします。

AWS での Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定

考慮すべき点

- トランジット VPC は、シスコのオーバーレイネットワークとホスト VPC で実行されているクラウドベースのアプリケーション間の接続を提供します。ブランチからホスト VPC へのトラフィックのトランジットポイントとして機能する専用の各 VPC 内で、冗長 Cisco Catalyst SD-WAN クラウドデバイスのペアを最大 4 つまでプロビジョニングできます。各冗長ペアの個々の Cisco Catalyst SD-WAN デバイスは、トランジット VPC の AWS リージョン内の異なる可用性ゾーン内に展開されます。複数の Cisco Catalyst SD-WAN デバイスは、オーバーレイネットワークとクラウドベースのアプリケーション間の接続に冗長性を提供します。これら 2 つの Cisco Catalyst SD-WAN クラウドデバイスのそれぞれで、トランスポート VPN（VPN 0）はブランチルータに接続し、サービス側 VPN（VPN 0 と VPN 512 を除く VPN）はパブリッククラウド内のアプリケーションおよびアプリケーション プロバイダーに接続します。

- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS ワークフローは、2 番目の WAN インターフェイスのパブリック IP アドレスを使用して、ホスト VPC をトランジット VPC にマッピングするためのカスタマーゲートウェイ（ipsec トンネル）を設定します。WAN インターフェイスのパブリック IP アドレスを追加するには、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS で使用されるデバイスの VPN インターフェイス イーサネット テンプレートを GigabitEthernet2 インターフェイスを使用して設定します。Cisco CSR1000V および Cisco Catalyst 8000V デバイスでは、トンネルインターフェイスは GigabitEthernet2 インターフェイス上にあります。VPN0 インターフェイス機能テンプレート （44 ページ）の VPN インターフェイス イーサネット テンプレートの設定例を参照してください。

- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS は AWS の自動スケールをサポートしています。AWS の自動スケール機能を使用するには、Cisco Catalyst SD-WAN クラウドデバイスの 1 ～ 4 つのペアをトランジット VPC に関連付けていることを確認します。

- ホスト VPC は、クラウドベースのアプリケーションが存在する仮想プライベートクラウドです。トランジット VPC がアプリケーションまたはアプリケーション プロバイダーに接続する場合は、ホスト VPC に接続するだけです。

- すべてのホスト VPC が同じ AWS アカウントに属することも、各ホスト VPC が異なるアカウントに属することもできます。ある AWS アカウントに属するホストを、別のアカウントに属するトランジット VPC にマッピングすることができます。Cloud OnRamp 構成ウィザードを使用して、クラウドインスタンスまたはクラウドアカウントを設定します。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for IaaS]** を選択します。

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS を初めて設定する場合、クラウドインスタンスは画面に表示されません。クラウドインスタンスは、AWS リージョン内で作成された 1 つ以上のトランジット VPC を持つ AWS アカウントに対応しています。

ステップ 2 [Add New Cloud Instance] をクリックします。

ステップ 3 [Amazon Web Services (AWS)] オプションボタンをクリックします。

ステップ 4 次のポップアップウィンドウで、次の手順を実行します。

a) クラウドサーバーにログインするために、[IAM Role] または [Key] をクリックします。[IAM Role] を使用することを推奨します。

b) [IAM Role] をクリックした場合は、Cisco SD-WAN Manager が提供する [External ID] を使用して IAM ロールを作成します。ウィンドウに表示された外部 ID をメモして、IAM ロールの作成時に使用できる [Role ARN] 値を指定します。

Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降では、IAM ロールを作成するには、AWS 管理コンソールを使用して Cisco SD-WAN Manager から提供された外部 ID をポリシーに入力する必要があります。次の手順を実行します。

1. 既存の Cisco SD-WAN Manager EC2 インスタンスに IAM ロールをアタッチします。

   1. ポリシーを作成するには、AWS ドキュメントの IAM ロールの作成（コンソール）のトピックを参照してください。AWS の [Create policy] ウィザードで、[JSON] をクリックし、次の JSON ポリシードキュメントを入力します。

```
{

"Version": "2012-10-17",

  "Statement": [{

    "Sid": "VisualEditor0",

"Effect": "Allow",

    "Action": "sts:AssumeRole",

"Resource": "*"

    }
]

}
```

   2. IAM ロールを作成し、ステップ 1 で作成したポリシーに基づいて Cisco SD-WAN Manager EC2 インスタンスにアタッチする方法については、AWS Security Blog の「Easily Replace or Attach an IAM Role to an Existing EC2 Instance by Using the EC2 Console」ブログを参照してください。

      （注） [Attach permissions policy] ウィンドウで、ステップ 1 で作成した AWS 管理ポリシーを選択します。

2. Cisco Catalyst SD-WAN Cloud OnRamp for IaaS に使用する AWS アカウントで IAM ロールを作成します。

1. AWS ドキュメントの IAM ロールの作成（コンソール）のトピックを参照して、[Require external ID] をオンにし、ステップ 4（b）でメモした外部 ID を貼り付けて、IAM ロールを作成します。
2. ロールを担当できるユーザーを変更するには、AWS ドキュメント のロール信頼ポリシーの変更（コンソール）のトピックを参照してください。

   [IAM Roles] ウィンドウで、下にスクロールして、前の手順で作成したロールをクリックします。

   [Summary] ウィンドウで、[Role ARN] をメモします。

   （注） ステップ 4（b）で IAM ロールを選択した場合は、このロール ARN 値を入力できます。

3. 信頼関係を変更したら、[JSON] をクリックし、次の JSON ドキュメントを入力します。変更内容を保存します。

   （注） 次の JSON ドキュメントのアカウント ID は、Cisco SD-WAN Manager EC2 インスタンスです。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::[Account ID from Part 1]:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "[vManage provided External ID]"
       }
      }
    }
  ]
}
```

c) [Key] オプションボタンをクリックした場合は、次の手順を実行します。

1. [API Key] フィールドに、Amazon API キーを入力します。
2. [Secret Key] フィールドに、API キーに関連付けられたパスワードを入力します。
3. [Environment] ドロップダウンリストから、[commercial] または [govcloud] を選択します。

   デフォルトでは、[commercial] 環境が選択されています。環境の仕様に基づいて地理的なリージョンを選択できます。

ステップ 5 [Login] をクリックして、クラウドサーバーにログインします。

クラウドインスタンス構成ウィザードが表示されます。このウィザードは、リージョンの選択、トランジット VPC の追加、ホスト VPC の検出、およびトランジット VPC へのホスト VPC のマッピングに使用する、3 つの画面で構成されています。各ウィザード画面のグラフィックは、クラウドインスタンスの設定プロセスの手順を示しています。まだ完了していない手順は、明るいグレーで表示されます。現在の手順は、

青いボックス内に強調表示されます。完了した手順は緑色のチェックマークで示され、明るいオレンジで表示されます。

ステップ 6 リージョンを選択します。

[Choose Region] ドロップダウンリストから、トランジット VPC を作成するリージョンを選択します。

ステップ 7 トランジット VPC を追加します。

a) [Transit VPC Name] フィールドに、トランジット VPC 名を入力します。

名前には、128 文字の英数字、ハイフン（–）、および下線（_）を含めることができます。スペースやその他の文字を含めることはできません。

b) [Device Information] で、トランジット VPC に関する情報を入力します。

1. [WAN Edge Version] ドロップダウンリストで、トランジット VPC で実行する Cisco Catalyst SD-WAN クラウドデバイスのソフトウェアバージョンを選択します。
2. [Size of Transit WAN Edge] ドロップダウンリストで、トランジット VPC で実行される各 Cisco Catalyst SD-WAN クラウドデバイスに使用できるメモリと CPU を決定するオプションを選択します。
   - 『Cisco CSR 1000v Series Cloud Services Router Deployment Guide for Amazon Web Services』の Cisco CSR1000V デバイスの「Supported Instance Types」のトピックを参照してください。
   - 「Deploying Cisco Catalyst 8000V on Amazon Web Services」の Cisco Catalyst 8000V の「Supported Instance Types」のトピックを参照してください。

   （注） 次のサイズを選択することを推奨します。

   Cisco CSR1000V および Cisco Catalyst 8000V には、4 つ以上の vCPU を持つ c5 インスタンスタイプを選択します（[c5.xlarge (4 vCPU)] など）。
3. [Max. Host VPCs per Device Pair] フィールドで、トランジット VPC の各デバイスペアにマッピングできるホスト VPC の最大数を選択します。有効な値は 1 ～ 32 です。
4. ダイレクト インターネット アクセス（DIA）用にトランジット VPC デバイスを設定するには、次のいずれかをクリックします。
   - [Disabled]：インターネットアクセスなし。
   - [Enabled via Transport]：デバイスの WAN インターフェイスに対して NAT を設定または有効化します。
   - [Enabled via Umbrella SIG]：デバイスでセキュアな DIA を有効にするように Cisco Umbrella を設定します。
5. [Device Pair 1#] フィールドで、ペアの各デバイスのシリアル番号を選択します。デバイスのシリアル番号を削除するには、フィールドに表示される [X] をクリックします。

   表示されるデバイスのシリアル番号は設定テンプレートに関連付けられていて、ステップ 1 で選択した Cisco Catalyst SD-WAN WAN エッジバージョンをサポートしています。

6. デバイスペアをさらに追加するには、  をクリックします。

   デバイスペアを削除するには、  をクリックします。

   トランジット VPC は、1 ～ 4 つのデバイスペアに関連付けることができます。AWS で自動スケール機能を有効にするには、少なくとも 2 つのデバイスペアをトランジット VPC に関連付けます。

7. より具体的な設定オプションを入力する場合は、[Advanced] をクリックします。

   1. [Transit VPC CIDR] フィールドに、16 ～ 25 の範囲のネットワークマスクを持つカスタム CIDR を入力します。このフィールドを空のままにすると、トランジット VPC はデフォルト CIDR の 10.0.0.0/16 を使用して作成されます。CIDR ブロック内に 6 つのサブネットを作成するために十分なアドレス空間が必要です。

   2. （オプション）[SSH PEM Key] ドロップダウンリストで、インスタンスにログインするための PEM キーペアを選択します。このキーペアはリージョン固有です。キーペアの作成手順については、AWS のドキュメントを参照してください。

8. [Save and Finish] をクリックしてトランジット VPC の設定を完了するか、必要に応じて [Proceed to Discovery and Mapping] をクリックしてウィザードを続行します。

   このクラウドインスタンスでは、2 つの Cisco Catalyst SD-WAN クラウドデバイスがある単一のトランジット VPC が作成されています。単一のクラウドインスタンス（リージョン内の AWS アカウント）内に複数のトランジット VPC を設定できます。クラウドインスタンス内に複数のトランジット VPC が存在する場合は、ホスト VPC をいずれかのトランジット VPC にマッピングすることができます。

9. ホスト VPC を検出します。

   1. [Select an account to discover] フィールドで、ホスト VPC を検出する AWS アカウントを選択します。

      または、ホスト VPC を検出する新しい AWS アカウントを追加するには、[New Account] をクリックします。

   2. [Discover Host VPCs] をクリックします。

      トランジット VPC にマッピングできる VPC を示すテーブルが表示されます。選択した AWS アカウント内の、トランジット VPC と同じ AWS リージョン内のホスト VPC のみが表示されます。

   3. 表示されたテーブルで、トランジット VPC にマッピングする 1 つ以上のホストのチェックボックスをオンにします。

      検索結果をフィルタリングするには、検索バーの [Filter] オプションを使用して、特定の検索条件に一致するホスト VPC のみを表示します。

      [Refresh] アイコンをクリックすると、テーブルが最新の情報で更新されます。

      テーブルに表示される列を指定するには、[Show Table Columns] アイコンをクリックします。

10. ホスト VPC をトランジット VPC にマッピングします。
    1. すべてのホスト VPC のテーブルで、目的のホスト VPC を選択します。
    2. [Map VPCs] をクリックします。[Map Host VPCs] ポップアップが開きます。
    3. [Transit VPC] ドロップダウンリストで、ホスト VPC にマッピングするトランジット VPC を選択します。
    4. [VPN] ドロップダウンリストで、マッピングを配置するオーバーレイネットワーク内のサービス VPN を選択します。
    5. Cisco SD-WAN Manager がホスト VPC ルートテーブルにルートを自動的に伝達する場合は、[Route Propagation] オプションを有効にします。

       デフォルトでは、[Route Propagation] は無効になっています。
    6. [Map VPCs] をクリックします。

数分後に [Task View] 画面が表示されるので、ホスト VPC がトランジット VPC にマッピングされたことを確認します。

（注） トランジット VPC を形成する 2 つの Cisco Catalyst SD-WAN クラウドデバイスの VPN 0 の VPN 機能テンプレートを設定する場合は、トンネルインターフェイスに割り当てる色がプライベートの色ではなくパブリックの色であることを確認します。パブリックの色は次のとおりです。

- **3g**
- **biz-internet**
- **blue**
- **bronze**
- **custom1**
- **custom2**
- **custom3**
- **default**
- **gold**
- **green**
- **lte**
- **metro-ethernet**
- **mpls**
- **public-internet**
- **red**
- **silver**

ホストおよびトランジット VPC の管理

ホスト VPC の表示

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

デフォルトでは、[Mapped Host VPCs] フィールドが選択され、マッピングされたホスト VPC の下のテーブルには、マッピングされたホストとトランジット VPC、トランジット VPC の状態、および VPN ID が一覧表示されます。

ステップ 2 マッピングされていないホスト VPC を一覧表示するには、[Un-Mapped Host VPCs] をクリックします。次に、[Discover Host VPCs] をクリックします。

ステップ 3 トランジット VPC を表示するには、[Transit VPCs] をクリックします。

トランジット VPC へのホスト VPC のマッピング

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

ステップ 2 [Un-Mapped Host VPCs] をクリックします。

ステップ 3 [Select an account to discover] フィールドで、ホスト VPC を検出する AWS アカウントを選択します。

ステップ 4 [Discover Host VPCs] をクリックします。

ステップ 5 検出されたホスト VPC のリストから、目的のホスト VPC を選択します。

ステップ 6 [Map VPCs] をクリックします。[Map Host VPCs] ポップアップが開きます。

ステップ 7 [Transit VPC] ドロップダウンリストから、目的のトランジット VPC を選択します。

ステップ 8 [VPN] ドロップダウンリストで、マッピングを配置するオーバーレイネットワーク内の VPN を選択します。

ステップ 9 [Map VPCs] をクリックします。

ホスト VPC のマッピング解除

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

ステップ 2 [Mapped Host VPCs] をクリックします。

ステップ 3 VPC のリストから、マッピングを解除するホスト VPC を選択します。

ステップ 4 [Un-Map VPCs] をクリックします。

ステップ 5 [OK] をクリックして、マッピングの解除を確定します。

ホスト VPC のマッピングを解除すると、ホスト VPC 内の VPN ゲートウェイへのすべての VPN 接続が削除されてから、VPN ゲートウェイが削除されます。マッピングされたホスト VPC へ

の VPN 接続を追加している場合、その接続はマッピング解除プロセスの一環として終了されます。

トランジット VPC の表示

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

ステップ 2 [Transit VPCs] をクリックします。

トランジット VPC の追加

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

ステップ 2 [Transit VPCs] をクリックします。

ステップ 3 [Add Transit VPC] をクリックします。

トランジット VPC を追加するには、AWS での Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定 （14 ページ）のステップ 7 の手順に従います。

デバイスペアの削除

（注） オンラインデバイスペアの最後のペアを削除するには、トランジット VPC を削除してください。

始める前に

削除するデバイスペアはオフラインである必要があります。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。

ステップ 2 デバイスペア ID をクリックします。

ステップ 3 デバイスペアのステータスがオフラインであることを確認します。

ステップ 4 デバイスペアのスケールを解除するには、[Action]列の下にあるごみ箱アイコンをクリックするか、[Trigger Autoscale] をクリックします。

トランジット VPC の削除

（注） オンラインデバイスペアの最後のペアを削除するには、トランジット VPC を削除する必要があります。

始める前に

トランジット VPC に関連付けられているデバイスペアを削除します。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

ステップ 2 [Host VPCs] をクリックします。

ステップ 3 すべてのホスト VPC を選択し、[Un-Map VPCs] をクリックします。

トランジット VPC にマッピングされていたすべてのホスト VPC のマッピングが解除されたことを確認します。

ステップ 4 [OK] をクリックして、マッピングの解除を確定します。

ステップ 5 [Transit VPCs] をクリックします。

ステップ 6 削除するトランジット VPC のごみ箱アイコンをクリックします。

（注） トランジット VPC の最後のデバイスペアでは、ごみ箱アイコンは使用できません。そのため、最後のデバイスペアを削除するには、[Delete Transit] ドロップダウンリスト項目をクリックします。ごみ箱アイコンは、2 番目以降のデバイスペアでのみ使用できます。

ステップ 7 [OK] をクリックして確定します。

デバイスペアの追加

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

ステップ 2 [Transit VPCs] をクリックします。

トランジット VPC のリストを含むテーブルが表示されます。

ステップ 3 目的のトランジット VPC について、[...] をクリックし、[Add Device Pair] を選択します。

ステップ 4 [Add Device Pairs] ダイアログボックスで、[Add] をクリックしてデバイスペアを追加します。

（注） 追加するデバイスがすでにデバイステンプレートに関連付けられていることを確認します。

トランジット VPC には最大で合計 4 つのデバイスペアを追加できます。

ステップ 5 [Save] をクリックします。

トランジット VPC のデバイスペアの履歴

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

ステップ 2 [Transit VPCs] をクリックします。

トランジット VPC のリストを含むテーブルが表示されます。

ステップ 3 目的のトランジット VPC について、[...] をクリックし、[History for a device pair] を選択します。

これにより、対応するすべてのイベントが含まれている [Transit VPC Connection History] ページが表示されます。

ステップ 4 過去 1 時間に発生したイベントのヒストグラムと、選択したトランジット VPC のすべてのイベントのテーブルが表示されます。このテーブルには、トランジット VPC で生成されたすべてのイベントが一覧表示されます。イベントは次のいずれかです。

- Device Pair Added
- Device Pair Spun Up
- Device Pair Spun Down
- Device Pair Removed

- Host Vpc Mapped
- Host Vpc Unmapped
- Host Vpc Moved
- Transit Vpc Created
- Transit Vpc Removed

中継 VPC の編集

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VPC をクリックします。[Host VPCs/Transit VPCs] ウィンドウが開きます。

ステップ 2 [Transit VPCs] をクリックします。

トランジット VPC のリストを含むテーブルが表示されます。

ステップ 3 目的のトランジット VPC について、[...] をクリックして選択し、[Edit Transit Details] をクリックします。

ステップ 4 DIA 情報を入力するには、AWS での Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定 （14 ページ）のステップ 7（iv）の手順に従います。

この操作により、必要に応じて自動スケールがトリガーされる場合があります。

Microsoft Azure の前提条件

1. 有効な Microsoft Azure アカウントを用意します。
2. GovCloud にアクセスするための有効な Azure Government アカウントを用意します。

（注） Azure Government クラウドのサポートは Cisco Catalyst 8000V でのみ利用できます。

3. Azure Marketplace で、Cisco CSR1000V または Cisco Catalyst 8000V デバイスの利用規約に同意します。

   Cisco Catalyst SD-WAN Cloud OnRamp for IaaS ワークフローの一部として Cisco Catalyst SD-WAN クラウドルータを使用するには、仮想マシン（VM）の使用に関するマーケットプレイスの条件に同意する必要があります。次のいずれかの方法で Azure の利用規約に同意できます。

- ポータルでクラウドデバイスを手動で起動し、オンボーディングウィザードの最終ページの一部の条件に同意します。
- Azure API または Powershell/Cloud Shell スクリプトで、Set-AzureRmMarketplaceTerms コマンドを使用します。

4. Microsoft Azure でアプリケーション登録を作成し、Azure アカウントのログイン情報を取得します。Cisco Catalyst SD-WAN Cloud OnRamp for IaaS で、これらのログイン情報が、Azure で Cisco SD-WAN Manager サーバーを認証し、VNet および仮想マシンインスタンスを起動するために使用されます。

   Azure ログイン情報を作成および取得するには、所有者権限を使用して Azure でアプリケーション登録を作成します。

   1. Microsoft Azure ポータルを開きます。
   2. Azure Active Directory（AD）の権限を確認します。[Azure Active Directory] を選択し、ロールをメモします。Azure AD テナントにアプリケーションを登録できるのは、管理者権限を持つロールのみです。
   3. サブスクリプションの権限を確認します。

      Azure AD に関連付けられているロールと権限を確認したら、Azure サブスクリプション アカウントに、Azure AD アプリケーションにロールを割り当てるための [Microsoft.Authorization/*/Write] のアクセス権があることを確認します。このアクセス権は、所有者ロールまたはユーザーアクセス管理者ロールにのみ関連付けられます。

      1. Azure ポータルで、[Subscriptions] をクリックします。
      2. [Subscriptions] サービスに移動し、行の右側にある [More Actions] アイコンをクリックします。

         [Microsoft Azure Enterprise] ページが表示されます。
      3. [My permissions] を選択します。次に、[Click here to view complete access details for this subscription] をクリックします。
      4. [View my access] をクリックして、割り当てられたロールを表示します。
      5. AD アプリケーションにロールを割り当てるための適切な権限があるかどうかを確認します。ない場合は、[User Access Administrator] ロールを自分に追加するように、Azure サブスクリプション管理者に依頼します。

   4. アプリケーション ID とサービスプリンシパルを作成します。

      1. Azure ポータルの左側のペインで、[Azure Active Directory] をクリックします。
      2. サブメニューから、[App registrations] をクリックします。
      3. [新規登録（New Registration）] をクリックします。[Register an application] 画面が表示されます。
      4. [Name] フィールドに、CloudOnRampApp などのわかりやすい名前を入力します。

5. [Supported account types] で、[Accounts in this organizational directory only (Microsoft only - Single tenant)] を選択します。
6. [Redirect URI] で、作成するアプリケーションのタイプとして [Web] を選択します。
7. 値を設定したら、[Register] をクリックします。

これで、Azure AD アプリケーションとサービスプリンシパルが作成されました。

5. Cloud OnRamp アプリケーションの秘密キーを作成します。
   1. Azure AD の [App registrations] で、使用するアプリケーションをクリックします。
   2. 左側のペインで、[Certificates & secrets] をクリックします。
   3. [Client secrets] の下で、[New client secret] をクリックします。
   4. 秘密キーの説明と、秘密キーの有効期限を入力します。
   5. [Add] をクリックします。

   クライアントシークレットを保存すると、クライアントシークレットの値またはキーの値が表示されます。必要に応じて後でキーを取得することはできないため、この値をメモしてください。作成したアプリケーションにサインインするには、アプリケーション ID とともにキー値を指定する必要があります。
6. サブスクリプション ID を取得します。
   1. Azure ポータルで、[Subscriptions] をクリックします。
   2. [Subscriptions] サービスに移動し、行の右側にある [More Actions] アイコンをクリックします。

      [Microsoft Azure Enterprise] ページが表示されます。
   3. このページの [Subscription ID] をメモします。

      Cisco SD-WAN Manager に Azure サブスクリプションへのプログラムによるアクセスを提供するには、サブスクリプション ID が必要です。

   複数のサブスクリプションがある場合は、CloudOnRampApp の設定に使用する予定のサブスクリプション ID をコピーして保存します。
7. テナント ID を表示します。
   1. Azure ポータルの左側のペインで、[Azure Active Directory] をクリックします。
   2. 左側のペインで、[Properties] をクリックします。テナント ID に相当するディレクトリ ID が表示されます。
8. アプリケーションに所有者ロールを割り当てます。

   このガイドでは、すべてのアクセスと管理が可能な所有者ロールを割り当てる手順を説明しました。

（注） アプリケーションの適切なロールについては、Azure 管理者にお問い合わせください。

1. Azure ポータルの左側のペインで、[Subscriptions] をクリックします。
2. サブスクリプションをクリックして、Cloud OnRamp アプリケーションに割り当てます。
3. サブスクリプションペインで、[Access Control (IAM)] に移動します。
4. [Add a role assignment] をクリックします。[Add role assignment] ポップアップが表示されます。
5. [Role] ドロップダウンリストから、[Owner] を選択します。
6. [Assign Access To] ドロップダウンリストで、デフォルト値の [Azure AD user, group, or service principal] を選択します。
7. [Select] ドロップダウンリストから、ステップ d で作成した Cloud OnRamp アプリケーションを選択します。
8. [Save] をクリックします。

その範囲のロールを持つユーザーのリストに、使用するアプリケーションが表示されます。

これで、作成して保存した Azure ログイン情報を使用して Cloud OnRamp アプリケーションにログインすることができます。

5. Azure ポータルで使用するサブスクリプションに移動して、アカウントに関連付けられている Azure の制限を確認します。[Settings] の下で、[Usage + Quotas] を選択します。
   1. [All Providers] ドロップダウンリストからプロバイダーを選択します。
   2. [Microsoft.Network] を確認します。

      このサブスクリプションで使用可能な可用性セットの量を表示できます。アカウントで次のリソースを作成できるように、可用性セットが十分であることを確認します。

      - トランジット VNet の作成に必要な 1 つの VNet。
      - トランジット VNet での仮想マシンの配布に必要な 1 つの可用性セット。
      - トランジットクラウドルータに関連付けられた 6 つのスタティックパブリック IP アドレス。
      - ホスト VNet ごとに 1 つの Azure Virtual Network トランジットと 2 つのスタティックパブリック IP アドレス
      - 各ホスト VNet をマッピングするための 4 つの VPN 接続

（注） F シリーズの Azure VM（F4 および F8）が、Cisco Catalyst SD-WAN クラウドデバイスでサポートされています。

Microsoft Azure の Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定

設定プロセスでは、1 つ以上のホスト VNet を単一のトランジット VNet にマッピングします。マッピング時に、ブランチユーザーがアクセスできるクラウドベースのアプリケーションを設定します。

マッピングプロセスにより、トランジット VNet と各ホスト VNet の間に IPsec および BGP 接続が確立されます。トランジット VNet とホスト VNet を接続する IPsec トンネルは、接続のセキュリティを提供するために IKE を実行します。Azure の場合、IPsec トンネルは IKE バージョン 2 を使用します。セキュアな IPsec トンネルを介して確立された BGP 接続により、トランジット VNet とホスト VNet はルートを交換できます。その後、BGP 接続または BGP ルートが Cisco Catalyst SD-WAN クラウドデバイス内の OMP に再配布され、これによりドメイン内の Cisco SD-WAN コントローラに OMP ルートがアドバタイズされます。トランジット VNet は、その後、ブランチから適切なホスト VNet および適切なクラウドベースのアプリケーションにトラフィックを転送できます。

マッピングプロセス中に、IPsec トンネルと BGP ピアリングセッションが自動的に設定および確立されます。マッピングを確立した後は、VPN インターフェイスの IPsec および BGP 機能設定テンプレートで IPsec および BGP 設定を表示し、必要に応じて変更することができます。

考慮すべき点：

Azure で Cisco Catalyst SD-WAN Cloud OnRamp for IaaS を設定するには、それぞれがルータのペアで構成される Azure トランジット VNet を作成します。次に、Azure クラウドに存在するトランジット VNet にホスト VNet をマッピングします。すべての VNet は同じリソースグループ内に存在します。

- トランジット VNet は、オーバーレイネットワークとホスト VNet で実行されているクラウドベースのアプリケーション間の接続を提供します。各トランジット VNet は、独自の VNet に存在する 2 つのクラウドデバイスで構成されます。2 つのクラウドデバイスは、オーバーレイネットワークとクラウドベースのアプリケーション間の接続に冗長性を提供します。これら 2 つのクラウドデバイスのそれぞれで、トランスポート VPN（VPN 0）はシミュレートされたブランチデバイスに接続し、サービス側 VPN（VPN 0 と VPN 512 を除く VPN）はパブリッククラウド内のアプリケーションおよびアプリケーション プロバイダーに接続します。
- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS ワークフローは、2 番目の WAN インターフェイスのパブリック IP アドレスを使用して、ホスト VNet をトランジット VNet にマッピングするためのカスタマーゲートウェイ（ipsec トンネル）を設定します。WAN イン

ターフェイスのパブリック IP アドレスを追加するには、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS で使用されるデバイスの VPN インターフェイス イーサネット テンプレートを GigabitEthernet2 インターフェイスを使用して設定します。Cisco CSR1000V および Cisco Catalyst 8000V では、トンネルインターフェイスは GigabitEthernet2 インターフェイス上にあります。VPN0 インターフェイス機能テンプレート （44 ページ）の VPN インターフェイス イーサネット テンプレートの設定例を参照してください。

- ホスト VNet は、クラウドベースのアプリケーションが存在する仮想プライベートクラウドです。トランジット VNet がアプリケーションまたはアプリケーション プロバイダーに接続する場合は、ホスト VNet に接続するだけです。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for IaaS]** を選択します。

ステップ 2 [Add New Cloud Instance] をクリックします

ステップ 3 [Microsoft Azure] オプションボタンをクリックします。

ステップ 4 次のポップアップ画面で、次の手順を実行します。

a) [Subscription ID] フィールドに、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS ワークフローの一環として使用する Microsoft Azure サブスクリプションの ID を入力します。

b) [Client ID] フィールドに既存のアプリケーションの ID を入力するか、新しいアプリケーションを作成します。アプリケーションを作成するには、**[Azure Active Directory]** > **[App Registrations]** > **[New registration]** に移動します。アプリケーションの作成の詳細については、Microsoft Azure のドキュメントを参照してください。

c) [Tenant ID] フィールドに、アカウントの ID を入力します。テナント ID を見つけるには、Microsoft Azure Active Directory に移動し、[Properties] をクリックします。

d) [Secret Key] フィールドに、クライアント ID に関連付けられたパスワードを入力します。

e) [Environment] フィールドで、[commercial] または [GovCloud] を選択します。

デフォルトでは、[commercial] 環境が選択されています。環境の仕様に基づいて地理的な場所を選択できます。

f) [ログイン（Login）] をクリックします。

クラウドインスタンス構成ウィザードが開きます。

このウィザードは、場所の選択、トランジット VNet の追加、ホスト VNet の検出、およびトランジット VNet へのホスト VNet のマッピングに使用する、3 つの画面で構成されています。各ウィザード画面の右側のグラフィックは、クラウドインスタンスの設定プロセスの手順を示しています。まだ完了していない手順は、明るいグレーで表示されます。現在の手順は、青いボックス内に強調表示されます。完了したすべての手順は緑色のチェックマークで示され、明るいオレンジで表示されます。

ステップ 5 [Choose Location] ドロップダウンリストから、トランジット VNet を作成する場所を選択します。

使用可能な場所は、商用クラウドか GovCloud かの選択に基づいています。

ステップ 6 トランジット VNet を追加します。

a) [Transit VNet Name] フィールドに、トランジット VNet の名前を入力します。

名前には、32 文字の英数字、ハイフン（–）、および下線（_）を含めることができます。スペースやその他の文字を含めることはできません。

b) [Device Information] で、トランジット VNet に関する情報を入力します。

1. [WAN Edge Version] ドロップダウンリストで、トランジット VNet で実行するソフトウェアバージョンを選択します。このドロップダウンリストには、Microsoft Azure マーケットプレイスで公開されているデバイスソフトウェアのバージョンが含まれています。
2. [Size of Transit WAN Edge] ドロップダウンリストで、トランジット VNet で実行される各 Cisco Catalyst SD-WAN クラウドデバイスに使用できるメモリと CPU を決定するオプションを選択します。
   - 『Cisco CSR 1000v Deployment Guide for Microsoft Azure』の Cisco CSR1000V の「Supported Instance Types」を参照してください。
   - 「Deploying Cisco Catalyst 8000V on Microsoft Azure」の Cisco Catalyst 8000V の「Supported Instance Types」を参照してください。

   （注） 次のサイズを選択することを推奨します。

   Cisco CSR1000V および Cisco Catalyst 8000V には、4 つ以上の vCPU を持つ DS3 インスタンスタイプを選択します（[Standard DS3 v2 (4vCPU)] など）。
3. ダイレクトインターネットアクセス（DIA）用にトランジット VNet デバイスを設定するには、次のいずれかをクリックします。
   - [Disabled]：インターネットアクセスなし。
   - [Enabled via Transport]：デバイスの WAN インターフェイスに対して NAT を設定または有効化します。
   - [Enabled via Umbrella SIG]：デバイスでセキュアな DIA を有効にするように Cisco Umbrella を設定します。
4. [Device 1] ドロップダウンリストで、最初のデバイスのシリアル番号を選択します。
5. [Device 2] ドロップダウンリストで、デバイスペアの 2 番目のデバイスのシリアル番号を選択します。
6. より具体的な設定オプションを入力する場合は、[Advanced] をクリックします。
7. [Transit VNet CIDR] フィールドに、16 ～ 25 の範囲のネットワークマスクを持つカスタム CIDR を入力します。このフィールドを空のままにすると、トランジット VNet はデフォルト CIDR の 10.0.0.0/16 を使用して作成されます。

c) [Save and Finish] をクリックしてトランジット VNet の設定を完了するか、必要に応じて [Proceed to Discovery and Mapping] をクリックしてウィザードを続行します。

ステップ 7 ホスト VNet をトランジット VNet にマッピングします。

a) [Select an account to discover] ドロップダウンリストで、Azure サブスクリプション ID を選択します。
または、ホスト VNet を検出する新しい Azure アカウントを追加するには、[New Account] をクリックします。

b) [Discover Host VNets] をクリックします。

c) [Select a VNet] ドロップダウンリストで、目的のホスト VNet を選択します。

d) [Next] をクリックします。

e) ホスト VNet のテーブルから、目的のホスト VNet を選択します。

f) [Map VNets] をクリックします。[Map Host VNets] ポップアップが表示されます。

g) [Transit VNet] ドロップダウンリストで、ホスト VNet にマッピングするトランジット VNet を選択します。

h) [VPN] ドロップダウンリストで、マッピングを配置するオーバーレイネットワーク内の VPN を選択します。

i) [IPSec Tunnel CIDR] セクションで、Azure Virtual Network トランジットに到達するように IPSec トンネルを設定するには、Cisco CSR1000V または Cisco Catalyst 8000V デバイスのそれぞれに対して、インターフェイス IP アドレスの 2 つのペアと、ループバック IP アドレスのペアを入力します。IP アドレスが /30 サブネット内のネットワークアドレスであり、オーバーレイネットワーク全体で一意であり、ホスト VNet CIDR の一部ではないことを確認します。ホスト VNet CIDR の一部である場合、トランジット VNet への VPN 接続を作成しようとすると、Microsoft Azure からエラーが返されます。

（注） IP アドレスは、ホスト VNet およびトランジット VPC CIDR の一部ではありません。

Microsoft Azure は、IPSec トンネルを介した単一の仮想プライベートゲートウェイ（VGW）の設定をサポートし、単一のトンネルを介して冗長性を提供します。そのため、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS は冗長性のために 2 つの VGW をサポートしています。VGW の計画的なメンテナンスまたは計画外のイベント中に、VGW からクラウドデバイスへの IPSec トンネルが切断されます。この接続が失われると、クラウドデバイスは IPSec トンネルを介した Cisco SD-WAN Manager との BGP ピアリングを失います。IPSec トンネルの IP アドレスではなくクラウドルータとの BGP ピアリングを有効にするには、各クラウドデバイスにループバックアドレスを指定します。

（注） BGP ピアリングのループバックオプションは、Azure クラウドでの単一および複数の仮想ゲートウェイ、カスタマーゲートウェイ、またはその両方の設定をサポートしています。ループバックオプションは、トランジット VNet にマッピングされた新しいホスト VNet にのみ適用され、既存の VNet には適用されません。

j) [Azure Information] セクションで、次の手順を実行します。

1. [BGP ASN] フィールドに、ホスト VNet 内で起動される Azure Virtual Network ゲートウェイで設定する ASN を入力します。Azure の既存の設定に含まれていない ASN を使用します。許容可能な ASN 値については、Microsoft Azure のドキュメントを参照してください。

2. [Host VNet Gateway Subnet] フィールドに、仮想ネットワークゲートウェイを配置できるホスト VNet サブネットを入力します。/28 以上のサブネットを使用することを推奨します。VNet 内にすでに作成されているサブネットは指定しないでください。

（注） ホスト VNet CIDR 内に未使用の CIDR があることを確認します。

k) [Map VNets] をクリックします。

l) [Save and Complete] をクリックします。

（注） トランジット VNet を形成する 2 つの Cisco Catalyst SD-WAN クラウドデバイスの VPN 0 の VPN 機能テンプレートを設定する場合は、トンネルインターフェイスに割り当てる色がプライベートの色ではなくパブリックの色であることを確認します。パブリックの色は次のとおりです。

- **3g**
- **biz-internet**
- **blue**
- **bronze**
- **custom1**
- **custom2**
- **custom3**
- **default**
- **gold**
- **green**
- **lte**
- **metro-ethernet**
- **mpls**
- **public-internet**
- **red**
- **silver**

[Task View] 画面が表示されるので、ホスト VNet がトランジット VNet に正常にマッピングされたことを確認します。

VNet ゲートウェイの作成には、最大で 45 分かかる場合があります。

ホストおよびトランジット VNet の管理

ホスト VNet の表示

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VNet をクリックします。[Host VNets/Transit VNets] ウィンドウが開きます。

デフォルトでは、[Mapped Host VNets] フィールドが選択され、マッピングされたホスト VNet の下のテーブルには、マッピングされたホストとトランジット VNet、トランジット VNet の状態、および VPN ID が一覧表示されます。

ステップ 2 マッピングされていないホスト VNet を一覧表示するには、[Un-Mapped Host VNets] をクリックします。次に、[Discover Host VNets] をクリックします。

ステップ 3 トランジット VNet を表示するには、[Transit VNets] をクリックします。

既存のトランジット VNet へのホスト VNet のマッピング

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VNet をクリックします。[Host VNets/Transit VNets] ウィンドウが開きます。

ステップ 2 [Un-Mapped Host VNets] をクリックします。

ステップ 3 [Discover Host VNets] をクリックします。

ステップ 4 検出されたホスト VNet のリストから、目的のホスト VNet を選択します。

ステップ 5 [Map VNet] をクリックします。[Map Host VNets] ポップアップが開きます。

ステップ 6 [Transit VNet] ドロップダウンリストから、目的のトランジット VNet を選択します。

ステップ 7 [VPN] ドロップダウンリストで、マッピングを配置するオーバーレイネットワーク内の VPN を選択します。

ステップ 8 [Map VNets] をクリックします。

ホスト VNet のマッピング解除

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VNet をクリックします。[Host VNets/Transit VNets] ウィンドウが開きます。

ステップ 2 [Mapped Host VNets] をクリックします。

ステップ 3 VNet のリストから、目的のホスト VNet を選択します。一度に 1 つの VNet のマッピングを解除することを推奨します。複数の VNet のマッピングを解除する場合は、1 回のマッピング解除操作で 4 つ以上選択しないでください。

ステップ 4 [Un-Map VNets] をクリックします。

ステップ 5 [OK] をクリックして、マッピングの解除を確定します。

トランジット VNet の表示

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VNet をクリックします。[Host VNets/Transit VNets] ウィンドウが開きます。

ステップ 2 [Transit VNets] をクリックします。

テーブルに、すべてのトランジット VNet が一覧表示されます。

トランジット VNet の追加

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VNet をクリックします。[Host VNets/Transit VNets] ウィンドウが開きます。

ステップ 2 [Transit VNets] をクリックします。

ステップ 3 [Add Transit VNet] をクリックします。

トランジット VNet を追加するには、Microsoft Azure の Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定 （29 ページ）のステップ 5 の手順に従います。

トランジット VNet の削除

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。目的の VNet をクリックします。[Host VNets/Transit VNets] ウィンドウが開きます。

ステップ 2 [Mapped Host VNets] をクリックします。

ステップ 3 目的のホスト VNet を選択し、[Un-Map VNets] をクリックします。

削除するトランジット VNet にマッピングされているすべてのホスト VNet のマッピングを解除してください。

ステップ 4 [OK] をクリックして、マッピングの解除を確定します。

ステップ 5 [Transit VNets] をクリックします。

ステップ 6 削除するトランジット VNet のごみ箱アイコンをクリックします。

ステップ 7 [OK] をクリックして確定します。

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS のトラブルシューティング

この項では、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の一般的な問題のトラブルシューティングの方法について説明します。

2 つの Cisco CSR1000V または Cisco Catalyst 8000V デバイスが使用できない

Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。[Add New Cloud Instance] をクリックすると、2 つの Cisco CSR1000V または Cisco Catalyst 8000V デバイスが使用できないことを示すエラーメッセージが表示されます。

問題の解決方法

Cisco SD-WAN Manager サーバーに、ライセンスが有効な Cisco Catalyst SD-WAN ソフトウェアを実行している 2 つの Cisco CSR1000V または Cisco Catalyst 8000V デバイスがありません。オペレーションズチームに連絡して、必要な Cisco CSR1000V または Cisco Catalyst 8000V デバイスを作成できるようにします。

Cisco CSR1000V または Cisco Catalyst 8000V デバイスが存在し、エラーメッセージが引き続き表示される場合は、2 つのデバイスが設定テンプレートにアタッチされていません。Cisco SD-WAN Manager の **[Configuration]** > **[Templates]** [Device] ウィンドウで、これらのテンプレートをアタッチします。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。

必要な API 権限が使用できない

API キーを入力すると、このユーザーに必要な権限がないことを示すエラーメッセージが表示されます。

問題の解決方法

Cisco SD-WAN Manager サーバーがインターネットに到達できることと、AWS または Microsoft Azure に到達できるように DNS サーバーが設定されていることを確認します。DNS サーバーを設定するには、Cisco SD-WAN Manager VPN 機能設定テンプレートで DNS サーバーの IP アドレスを入力し、設定テンプレートを Cisco SD-WAN Manager サーバーに再アタッチします。

AWS の場合は、AWS アカウントに属する API キーを確認します。キーが正しくないと思われる場合は、別のキーのペアを生成します。

AWS で、正しいキーを入力してもエラーメッセージが引き続き表示される場合は、キーに必要な権限がありません。キーに関連付けられているユーザー権限を確認します。VPC と EC2 インスタンスを作成および編集するために必要な権限をユーザーに付与します。

エラーメッセージが引き続き表示される場合は、Cisco SD-WAN Manager サーバーの時刻を確認して、現在の時刻に設定されていることを確認します。そうでない場合は、Cisco SD-WAN Manager のサーバータイムが Google NTP サーバーを示すように設定します。サーバータイムを設定するには、Cisco SD-WAN Manager NTP 機能設定テンプレートで、NTP サーバーのホスト名を入力します。次に、Cisco SD-WAN Manager を使用して設定テンプレートを NTP 機能に再アタッチします。Google NTP サーバーは、time.google.com、time2.google.com、time3.google.com、time4.google.com などです。

AWS の設定時に WAN エッジルータのソフトウェアバージョンがドロップダウンに表示されない

問題に関する説明

トランジット VPC のトランジット VPC パラメータの設定を試みたときに、Cisco CSR1000V および Cisco Catalyst 8000V デバイスのソフトウェアバージョンがドロップダウンリストに表示されません。

問題の解決方法

AWS Marketplace 内で、使用しているアカウントで Cisco CSR1000V または Cisco Catalyst 8000V デバイスの Amazon マシンイメージ（AMI）に登録していることを確認します。

Cisco CSR1000V がソフトウェアリリース 16.12.1b 以降を使用していて、Cisco Catalyst 8000V がソフトウェアリリース 17.4.1a 以降を使用していることを確認します。

設定中に VPN がリストにない

問題に関する説明

マッピングするホスト VPC または VNet を選択した後に、VPN がドロップダウンリストに表示されません。

問題の解決方法

この問題は、Cisco Catalyst SD-WAN クラウドデバイスにアタッチされたデバイス設定テンプレートにサービス側VPNが含まれていない場合に発生します。トランジットおよびホストVPCまたはVNet 用に選択した 2 つの Cisco Catalyst SD-WAN クラウドデバイス間の IPsec 接続を設定するには、サービス側 VPN（VPN 0 および VPN 512 以外の VPN）が必要です。

この問題は、トランジット VPC または VNet 用に選択した 2 つの Cisco Catalyst SD-WAN クラウドデバイスに重複するサービス側 VPN がない場合にも発生する可能性があります。2 つの Cisco Cloud Services Router 1000V または Cisco Catalyst 8000V デバイスがアクティブ-アクティブのペアを形成するため、両方のデバイスで同じサービス側 VPN を設定します。

サービス側 VPN を設定するには、Cisco SD-WAN Manager VPN 機能設定テンプレートで、少なくとも 1 つのサービス側 VPN を設定します。両方のルータで、少なくとも 1 つのサービス側 VPN が同じであることを確認します。次に、設定テンプレートをルータに再アタッチします。

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS タスクが失敗する

問題に関する説明

ホスト VPC からトランジット VPC へのマッピング、またはホスト VNet からトランジット VNet へのマッピングが完了した後に、Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の設定が失敗します。

問題の解決方法

画面に表示されたタスク情報を確認して、タスクが失敗した理由を特定します。エラーがAWSまたはAzureのリソースに関連している場合は、必要なすべてのリソースが配置されていることを確認します。

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS タスクは成功するが、Cisco Catalyst SD-WAN クラウドデバイスがダウンしている

問題に関する説明

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS タスクは成功しましたが、Cisco Catalyst SD-WAN クラウドデバイスが引き続きダウン状態です。

問題の解決方法

設定テンプレートを確認します。

- ポリシーを含む、Cisco Catalyst SD-WAN クラウドデバイス設定のすべての部分が有効で正しいことを確認します。設定が無効な場合、設定はルータに適用されず、ルータは起動しません。
- Cisco Catalyst SD-WAN Validator の設定が正しいことを確認します。Cisco Catalyst SD-WAN Validator で設定された DNS 名または IP アドレスが間違っている場合、Cisco CSR1000V または Cisco Catalyst 8000V デバイスは Cisco Catalyst SD-WAN Validator に到達できないため、オーバーレイネットワークに参加できません。

設定の問題を特定したら、次の手順を実行します。

1. Cisco Catalyst SD-WAN Cloud OnRamp for IaaS コンポーネントを削除します。
    1. ホスト VPC または VNet とトランジット VPC または VNet のマッピングを解除します。
    2. Cisco CSR1000V または Cisco Catalyst 8000V デバイスのトランジット VPC を削除します。
2. 設定テンプレートを編集し、Cisco Catalyst SD-WAN クラウドデバイスに再アタッチします。
3. Cisco Catalyst SD-WAN Cloud OnRamp for IaaS 設定プロセスを繰り返します。

必要なルートが交換されない

問題に関する説明

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS 設定ワークフローが成功し、Cisco CSR1000V または Cisco Catalyst 8000V デバイスが使用可能で実行されていますが、目的のルートが交換されていません。

問題の解決方法

Cisco SD-WAN Manager で、トランジットクラウドルータの BGP 設定を確認します。マッピングプロセス中に Cisco Catalyst SD-WAN Cloud OnRamp for IaaS サービスを設定すると、BGP はネットワークアドレス 0.0.0.0/0 をアドバタイズするように設定されます。サービス側 VPN に、0.0.0.0/0 を指す IP ルートが含まれていることを確認します。必要に応じて、VPN 機能設定テンプレートにスタティックルートを追加し、トランジット VPC または VNet 用に選択した 2 つのクラウドルータに設定を再アタッチします。

AWS で、ホスト VPC に移動し、ルートテーブルを確認します。ルートテーブルで、[Enable route propagation] をクリックして、VPC がルートを受信するようにします。

エンドツーエンドの ping が失敗する

問題に関する説明

ルーティングは正常に機能していますが、エンドツーエンドの ping が機能していません。

問題の解決方法

AWS で、ホスト VPC のセキュリティグループルールを確認します。Azure で、ホスト VNet のネットワーク セキュリティ グループ ルールを確認します。セキュリティグループルールでは、オンプレミスまたはブランチ側のデバイスの送信元 IP アドレス範囲のサブネットで、ブランチからのトラフィックが AWS に到達することが許可されるようにする必要があります。

機能テンプレートの設定例

機能テンプレート

次に、Cisco CSR1000V、Cisco Catalyst 8000V デバイスのさまざまな機能テンプレートの設定例を示します。

システム機能テンプレート

テンプレート：Basic Information/Cisco System

テンプレート名：Cisco_System_cEdge_Template

説明：System Template

表 *2:* システム機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
基本設定	サイト ID	デバイス固定	system_site_id
	システム IP	デバイス固定	system_system_ip
	ホストネーム	デバイス固定	system_host_name
	デバイスグループ	デバイス固定	system_device_groups
	Console Baud Rate	グローバル	115200
GPS	Latitude	デバイス固定	system_latitude
	Longitude	デバイス固定	system_longitude
Advanced	ポートホッピング	デバイス固定	system_port_hop
	ポートオフセット	デバイス固定	system_port_offset

ロギング機能テンプレート

テンプレート：Other Templates/Cisco Logging

テンプレート名：Cisco_Logging_cEdge_Template

説明：Logging Template

表 *3 :* ロギング機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
Server（オプション）	Hostname/IP address	グローバル	10.1.0.68
	VPN ID	デバイス固定	logging_server_vpn

Logging_Template 内のロギングサーバーはオプションです。

BFD 機能テンプレート

テンプレート：Basic Information/Cisco BFD_Template

テンプレート名：BFD_cEdge_Template

説明：BFD Template

表 *4 : BFD* 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
基本設定	Poll Interval	グローバル	120000
Color (Biz Internet)	色	ドロップダウン リスト	Biz Internet
	Hello Interval (milliseconds)	デバイス固定	biz_internet_bfd_hello_interval
	Path MTU	グローバル	オフ

VPN512 機能テンプレート

テンプレート：VPN/Cisco VPN

テンプレート名：Cisco_Transit_VPN512_Template_cEdge_Template

説明：VPN 512 Out-of-Band Management

表 *5 : VPN512* 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
基本設定	VPN	グローバル	512
	Name	グローバル	管理 VPN

VPN512 インターフェイス イーサネット機能テンプレート

テンプレート：VPN / Cisco VPN Interface Ethernet

テンプレート名：Cisco_Transit_VPN512_Interface_Template_cEdge_Template

説明：VPN 512 Management Interface

表 *6 : VPN512* インターフェイス イーサネット機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
基本設定	シャットダウン	グローバル	非対応
	Interface Name	デバイス固定	vpn512_mgmt_int
	説明	グローバル	管理インターフェイス
IPv4 の設定	IPv4 アドレス	オプション ボタン（Radio Button）	Dynamic

NTP 機能テンプレート

テンプレート：Basic Information/Cisco NTP

テンプレート名：Cisco_NTP_cEdge_Template

説明：NTP Template

表 *7 : NTP* 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
サーバー（Server）	Hostname/IP address	グローバル	time.nist.gov

既知の信頼できる NTP サーバーのみを使用するように注意する必要があります。時刻同期の中断は、トランジット VPC またはトランジット VNet 内の Cisco Catalyst SD-WAN クラウドデバイスが Cisco SD-WAN 制御コンポーネントに接続する機能、および他の Cisco Catalyst SD-WAN デバイスへの IPsec 接続を確立する機能に影響を与える可能性があります。

AAA 機能テンプレート

テンプレート：Basic Information/Cisco AAA

テンプレート名：Cisco_AAA_cEdge_Template

説明：AAA Template

表 *8 : Cisco AAA* 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
Local	User/admin/Password	グローバル	<自分の管理者パスワード>
	User/admin/Privilege	グローバル	15
AAA	ServerGroups priority order	グローバル	local

OMP 機能テンプレート

テンプレート：Basic Information/Cisco OMP

テンプレート名：Cisco_OMP_cEdge_Template

説明：OMP Template

表 *9 : Cisco OMP* 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
OMP	Number of Paths Advertised per Prefix	グローバル	Factory_Default_Cisco_OMP__ipv46_Template

セキュリティ機能テンプレート

テンプレート：Basic Information/Cisco Security

テンプレート名：Cisco_Security_cEdge_Template

説明：Security Template

表 *10 :* セキュリティ機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
セキュリティ	Replay window	グローバル/ドロップダウンリスト	Factory_Default_Cisco_Security_Template

VPN0 機能テンプレート

テンプレート：VPN/Cisco VPN

テンプレート名：Cisco_Transit_VPN0_cEdge_Template

説明：VPN0 Transport Template

表 *11 : VPN0* 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
Basic configuration	VPN	グローバル	0
	Name	グローバル	トランスポート VPN

VPN0 インターフェイス機能テンプレート

テンプレート：VPN/Cisco VPN Interface Ethernet

テンプレート名：Cisco_Transit_VPN0_cEdge_gigabit-ethernet2

説明：VPN0 Transport Interface

表 *12 : Cisco VPN0* インターフェイス機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
Basic configuration	シャットダウン	デバイス固定	vpn0_inet_int_shutdown
	Interface Name	ドロップダウンリスト	GigabitEthernet2/
	説明	グローバル	Internet Interface
IPv4 の設定	IPv4 アドレス	オプション ボタン（Radio Button）	Dynamic
	Bandwidth Upstream	デバイス固定	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	デバイス固定	vpn0_inet_int_bandwidth_down

セクション	パラメータ	タイプ	変数/値
Tunnel	トンネル インターフェイス	グローバル	オン
	色	グローバル	biz-internet
	[Allow Service] > [All]	グローバル	オン
[Tunnel] > [Advanced Options] > [Encapsulation]	IPsec Preference	デバイス固定	vpn0_inet_tunnel_ipsec_preference
Advanced	TCP MSS	グローバル	1350

VPN1 機能テンプレート

テンプレート：VPN/Cisco VPN

テンプレート名：Cisco_Transit_VPN1_cEdge_Template

説明：VPN1 Service Template

表 *13 : VPN1* 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
Basic configuration	VPN	グローバル	1
	Name	グローバル	Service VPN 1
	Enhance ECMP Keying	グローバル	オン
OMP のアドバタイズ	BGP (IPv4)	グローバル	オン
	Connected (IPv4)	グローバル	オン

VPN2 機能テンプレート

テンプレート：VPN/Cisco VPN

テンプレート名：Cisco_Transit_VPN2_cEdge_Template

説明：VPN2 Service Template

表 *14 : VPN2* 機能テンプレートの設定

セクション	パラメータ	タイプ	変数/値
Basic configuration	VPN	グローバル	2
	Name	グローバル	Service VPN 2
	Enhance ECMP Keying	グローバル	オン
OMP のアドバタイズ	BGP (IPv4)	グローバル	オン

デバイステンプレート

次の表に、Cisco CSR1000V または Cisco Catalyst 8000V デバイスのデバイステンプレートの概要を示します。

テンプレート名：Cloud_OnRamp_cEdge_Template

表 *15 :* トランジット *VPC* またはトランジット *VNet* デバイステンプレート

[Template Type]	テンプレートのサブタイプ	テンプレート名
Cisco System		Cisco_System_cEdge_Template
	Cisco ロギング	Cisco_Logging_cEdge_Template
	Cisco NTP	Cisco_NTP_cEdge_Template
	Cisco AAA	Cisco_AAA_cEdge_Template
Cisco BFD		BFD_cEdge_Template
Cisco OMP		Cisco_OMP_cEdge_Template
シスコのセキュリティ		Cisco_Security_cEdge_Template
Cisco VPN0		Cisco_Transit_VPN0_cEdge_Template
	Cisco VPN インターフェイス イーサネット	Cisco_Transit_VPN0_cEdge_gigabit-ethernet2

[Template Type]	テンプレートのサブタイプ	テンプレート名
Cisco VPN512		Cisco_Transit_VPN512_Template_cEdge_Template
	Cisco VPN インターフェイス イーサネット	Cisco_Transit_VPN512_Interface_Template_cEdge_Template
Cisco VPN1		Cisco_Transit_VPN1_cEdge_Template
VPN2		Cisco_Transit_VPN2_cEdge_Template

デバイステンプレート変数値の例

次のサンプル情報は、1 番目と 2 番目の Cisco CSR1000V または Cisco Catalyst 8000V デバイスに使用できるデバイステンプレート変数値を示しています。

表 *16 :* 最初のデバイスの *Cisco CSR1000V* または *Cisco Catalyst 8000V* のデバイステンプレート変数値

変数	値
ホスト名 (system_host_name)	CSR_CoR1
システム IP (system_system_ip)	209.165.200.225
サイト ID (system_site_id)	115001

表 *17 : 2* 番目のデバイスの *Cisco CSR1000V* または *Cisco Catalyst 8000V* のデバイステンプレート変数値

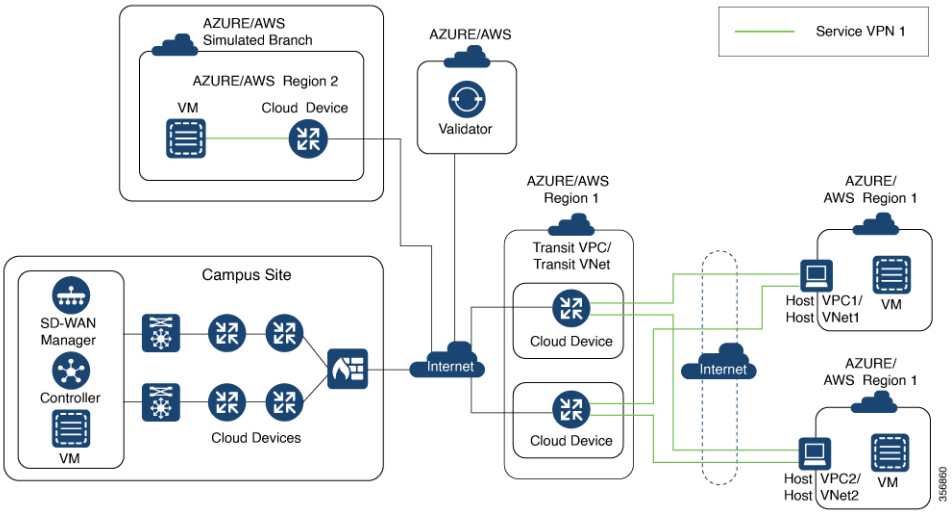
変数	値
ホスト名 (system_host_name)	CSR_CoR2
システム IP (system_system_ip)	209.165.201.1
サイト ID (system_site_id)	115001

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の例

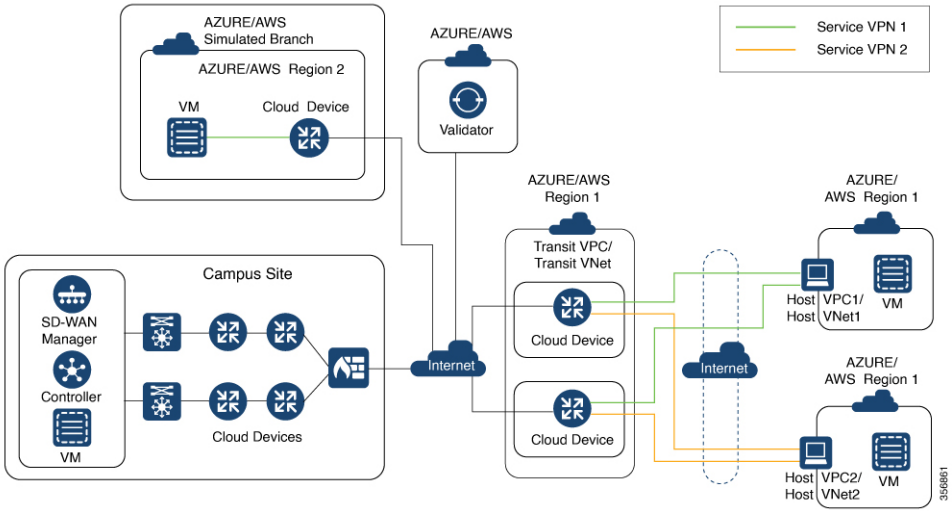
この例では、単一のトランジット VPC または VNet が AWS または Microsoft Azure のリージョン内に作成され、同じリージョン内の 2 つの既存のホスト VPC または VNet をトランジット VPC または VNet にマッピングします。その後、キャンパスおよびシミュレートされたブランチの場所からホスト VPC または VNet にアクセスできます。

Cisco Catalyst SD-WAN 展開では、0 ～ 512 の範囲のさまざまな VPN を使用して接続を実装します。VPN 0 はトランスポート（WAN）ネットワークを表し、VPN 512 は管理ネットワークを表します。残りの VPN（1 ～ 511）をサービス VPN として使用します。Cisco Catalyst SD-WAN Cloud OnRamp for IaaS の展開では次の 2 つのシナリオが考慮されます。

- 完全接続：両方のホスト VPC または VNet を、トランジット VPC または VNet 内のサービス VPN 1 にマッピングします。サービス VPN 1 は、キャンパス内に展開されている Cisco CSR1000V または Cisco Catalyst 8000V デバイス、およびシミュレートされたブランチ内に展開されている Cisco CSR1000V または Cisco Catalyst 8000V デバイスのサービス側で設定できます。この接続により、キャンパスサイトとブランチサイトの両方から、いずれかのホスト VPC 内の AWS Elastic Compute Cloud（EC2）インスタンスへの通信が可能になります。また、この接続により、2 つのホスト VPC 内に展開された AWS または Azure EC2 インスタンス間の通信も可能になります。この展開では、組織内のすべてのエンティティが、組織によって展開されたパブリッククラウドリソースに完全に接続できるシナリオを示しています。次の図は、この最初のシナリオを示しています。



- クラウドプロバイダーに対するセグメンテーション：片方のホスト VPC または VNet をサービス VPN 1 にマッピングし、もう片方のホスト VPC または VNet をトランジット VPC または VNet 内のサービス VPN 2 にマッピングします。このマッピングによりセグメンテーションが提供されるため、2 つのホスト VPC または VNet 間のトラフィックが分離されます。サービス VPN 1 にのみキャンパスを設定し、最初のホスト VPC 内の AWS または Azure EC2 インスタンスと通信できるようにすることができます。サービス VPN 2 のブランチを設定し、2 番目のホスト VPC 内の AWS または Azure EC2 インスタンスと通信できるようにします。この展開では、組織内のさまざまなエンティティが、特定のパブリッククラウドリソースへのアクセスのみを必要とするシナリオを示しています。次の図は、この 2 番目のシナリオを示しています。



同じサービス VPN 内のトランジット VPC または VNet へのホスト VPC または VNet のマッピング

両方のホスト VPC または VNet を、トランジット VPC または VNet 内のサービス VPN 1 にマッピングするには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。マッピングする両方のホスト VPC またはホスト VNet を選択し、[Map VPCs] または [Map VNets] をクリックします。

   [Map Host VPCs] または [Map Host VNets] ポップアップが開きます。

2. [Transit VPC] または [Transit VNet] ドロップダウンリストで、ホスト VPC または VNet にマッピングするトランジット VPC または VNet を選択します。

3. [VPN] ドロップダウンリストで、[1] を選択します。

   ホスト VPC またはホスト VNet を同じサービス VPN にマッピングすると、ホスト VPC または VNet 間の通信が可能になります。

4. AWS 設定の場合は、[Route Propagation] を無効にします。

   ルート伝達を有効にすると、マッピング用に選択されたホスト VPC に BGP ルートが伝達されます。

5. [Map VPCs] または [Map VNets] をクリックします。

   数分後に [Task View] ウィンドウが表示されるので、ホスト VPC または VNet がトランジット VPC または VNet にマッピングされたことを確認します。

これらの手順により、サービス VPN 1 への両方のホスト VPC または VNet のマッピングが完了します。各ホスト VPC または VNet での EC2 インスタンス間の接続を確認するには、それらの間に SSH 接続を確立します。同様に、キャンパスとブランチの両方をサービス VPN 1 にマッピングして、キャンパスとブランチからホスト VPC または VNet 内の EC2 インスタンスへの SSH 接続を確立することで、両方のホスト VPC または VNet への接続を確認できます。

異なるサービス VPN 内のトランジット VPC または VNet への各ホスト VPC または VNet のマッピング

片方のホスト VPC または VNet をサービス VPN 1 にマッピングし、もう片方のホスト VPC または VNet をサービス VPN 2 にマッピングするには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for IaaS]** を選択します。マッピングするホスト VPC または VNet を選択し、[Map VPCs] または [Map VNets] をクリックします。

   [Map Host VPCs] または [Map Host VNets] ポップアップが開きます。

2. [Transit VPC] または [Transit VNet] ドロップダウンリストで、ホスト VPC または VNet にマッピングするトランジット VPC または VNet を選択します。

3. [VPN] ドロップダウンリストで、[1] を選択します。

   これで、最初のホスト VPC または VNet がサービス VPN 1 にマッピングされました。

4. [Map VPCs] または [Map VNets] をクリックします。

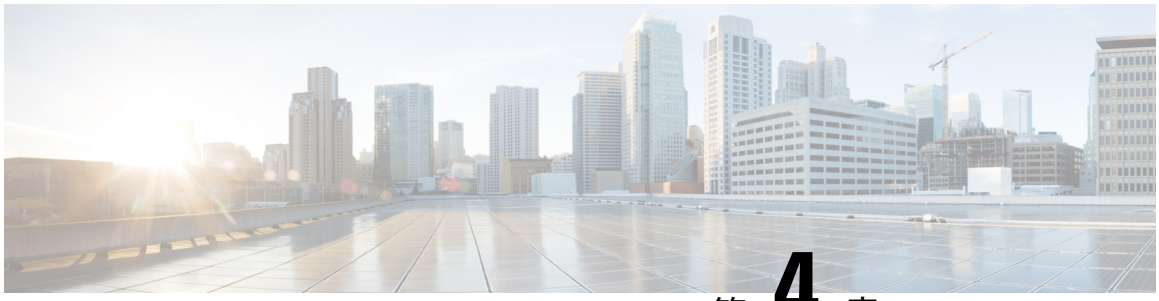
   数分後に [Task View] ウィンドウが表示されるので、ホスト VPC または VNet がトランジット VPC または VNet にマッピングされたことを確認します。

5. 2 番目のホスト VPC または VNet に対してステップ 1 ～ 3 を繰り返します

   VPN 値を選択するときは、ホスト VPC または VNet をサービス VPN 2 にマッピングします。

このプロセスにより、サービス VPN 1 への最初のホスト VPC または VNet のマッピングと、サービス VPN 2 への 2 番目のホスト VPC または VNet のマッピングが完了します。

キャンパスをサービス VPN 1 にマッピングして、キャンパスから最初のホスト VPC または VNet 内の EC2 インスタンスへの SSH 接続を確立することで、最初のホスト VPC または VNet への接続を確認できます。ただし、キャンパスから 2 番目のホスト VPC または VNet 内の EC2 インスタンスへの SSH 接続は確立できません。ブランチをサービス VPN 2 にマッピングして、ブランチから 2 番目のホスト VPC または VNet 内の EC2 インスタンスへの SSH 接続を確立することで、2 番目のホスト VPC または VNet への接続を確認できます。ただし、ブランチから最初のホスト VPC または VNet 内の EC2 インスタンスへの SSH 接続は確立できません。



第 4 章

Cloud OnRamp for Colocation

（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。

クラウドに移行するアプリケーションが増えるにつれて、トラフィックを高価な WAN 回線経由でデータセンターにバックホールする従来型のアプローチはもはや妥当ではなくなってきています。従来の WAN インフラストラクチャは、クラウド内のアプリケーションにアクセスすることを想定して設計されていませんでした。このインフラストラクチャは高額で、エクスペリエンスを低下させる不要な遅延を生みます。

ネットワークアーキテクトは、次のことを達成するために WAN の設計を再評価しています。

- クラウドへの移行をサポート。
- ネットワークコストの削減。
- クラウドトラフィックの可視性と管理性の向上。

ネットワークアーキテクトは、Software-Defined WAN（SD-WAN）ファブリックに変更して安価なブロードバンド インターネット サービスを利用し、リモートブランチから信頼性のある SaaS クラウドバウンド トラフィックをインテリジェントにルーティングします。

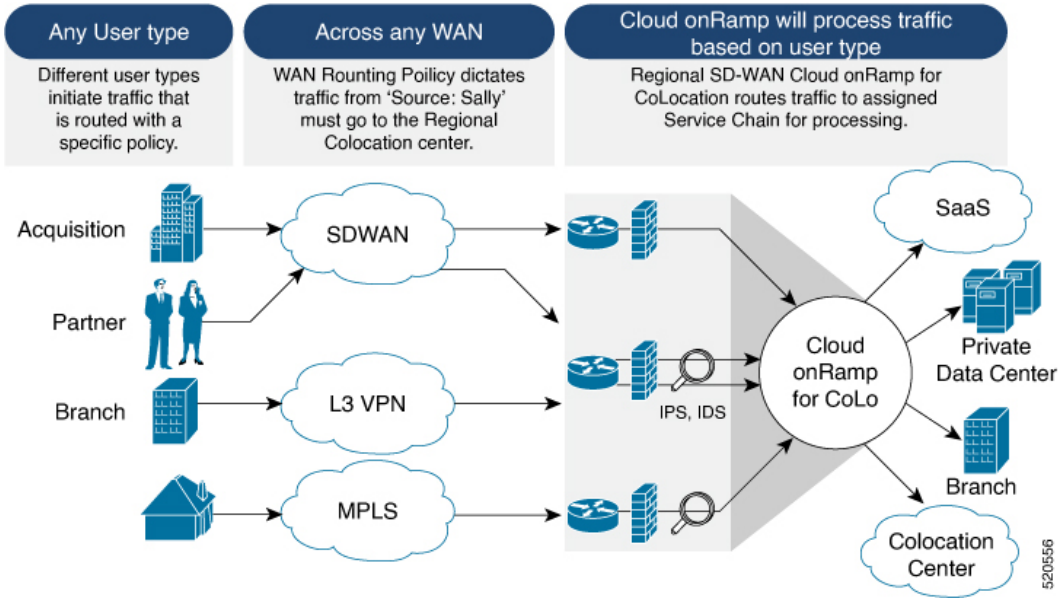
このソリューションでは、コロケーション設備向けに特別に構築された Cisco Catalyst SD-WAN Cloud OnRamp for Colocation ソリューションにより、ブランチおよびリモートワーカーからすべてのアプリケーションがホストされている場所への最適なパスにトラフィックをルーティングします。また、このソリューションにより、分散型企業はブランチで直接インターネットア

クセスが可能になり、Infrastructure-as-a-Service（IaaS）プロバイダーおよびSoftware as a Service（SaaS）プロバイダーへの接続を強化できます。

このソリューションは、大都市の周りに集まっている、または複数の国に分散している複数の分散型ブランチオフィスを持つ企業に、コロケーション設備でルーティングサービスを地域化する機能を提供します。その理由は、これらの設備がブランチに物理的に近く、企業がアクセスする必要があるクラウドリソースをホストできるためです。したがって、基本的に、仮想Cisco Catalyst SD-WAN をコロケーションセンターの地域アーキテクチャに分散させることにより、クラウドエッジに処理能力を与えます。

次の図は、マルチクラウドアプリケーションへのアクセスを複数のブランチから地域のコロケーション設備に集約する方法を示しています。

図 *2 : Cisco Catalyst SD-WAN Cloud OnRamp for Colocation*



このソリューションは、次の 4 つの特定のタイプの企業に対応できます。

- セキュリティ制限とプライバシー規制により、クラウドおよびSaaS プラットフォームへの直接インターネット接続を使用できない多国籍企業。
- Cisco Catalyst SD-WAN を使用していないが、顧客への接続が必要なパートナーおよびベンダー。これらの企業は、自社サイトに Cisco Catalyst SD-WAN ルーティングアプライアンスをインストールすることを望んでいません。
- 高帯域幅、最適なアプリケーションパフォーマンス、きめ細かいセキュリティを必要とする、地理的に分散したブランチオフィスを持つグローバルな組織。
- 安価な直接インターネットリンクを介した企業への安全な VPN 接続を必要とするリモートアクセス。

Cisco Catalyst SD-WAN Cloud OnRamp for Colocation ソリューションは、コロケーション IaaS プロバイダーによって特定のコロケーション設備内でホストできます。必要なコンポーネントを

サポートしている限り、地域ごとにニーズを満たすコロケーションプロバイダーを選択できます。

- Cloud OnRamp for Colocation ソリューションの展開, on page 53
- Cloud OnRamp for Colocation デバイスの管理 （54 ページ）
- クラスタの管理, on page 57
- サービス グループの管理, on page 87
- VM カタログとリポジトリの管理, on page 107
- Cisco Catalyst SD-WAN Manager からの Cloud OnRamp for Colocation デバイスの動作ステータスのモニター （122 ページ）
- Cisco Catalyst SD-WAN Cloud OnRamp for Colocation マルチテナント機能 （134 ページ）

Cloud OnRamp for Colocation ソリューションの展開

このトピックでは、colo デバイスの使用を開始し、Cisco SD-WAN Manager でクラスタを構築する手順の概要を説明します。クラスタを作成して構成したら、クラスタをアクティブ化するために必要な手順を実行できます。サービスグループまたはサービスチェーンを設計し、それらをアクティブ化されたクラスタに接続する方法を理解します。サポートされている Day-N 操作もこのトピックにリストされています。

1. ソリューションの前提条件と要件を満たします。「Prerequisites and Requirements of Cloud OnRamp for Colocation Solution」を参照してください。
   - CSP デバイス（初期 CSP アクセス用の CIMC のセットアップ）および Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチ（コンソールサーバーのセットアップ）と OOB または管理スイッチの配線を完了します。 すべてのデバイスの電源をオンにします。
   - DHCP サーバーをセットアップして構成します。「Provision DHCP Server per Colocation」を参照してください。
2. インストールされている Cisco NFVIS のバージョンを確認し、必要に応じて NFVIS をインストールします。「Install Cisco NFVIS Cloud OnRamp for Colocation on Cisco CSP」を参照してください。
3. クラスタをセットアップまたはプロビジョニングします。クラスタは、CSP デバイスや Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチを含むすべての物理デバイスで構成されます。 「Get Started with Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution」を参照してください。
   - CSP デバイスを起動します。「Bring Up Cloud Services Platform Devices」を参照してください。
   - Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチを起動します。「Bring Up Switch Devices」を参照してください。
   - クラスタをプロビジョニングして構成します。「Provision and Configure Cluster」を参照してください。

クラスタ設定でクラスタを構成します。「Cluster Settings」を参照してください。

4. クラスタをアクティブ化します。『クラスタの作成とアクティブ化, on page 60』を参照してください。
5. サービスグループまたはサービスチェーンを設計します。『サービス グループの管理, on page 87』を参照してください。

Note クラスタを作成する前、またはすべてのVMがリポジトリにアップロードされた後にクラスタをアクティブ化する前に、いつでもサービスチェーンを設計し、サービスグループを作成できます。

6. サービスグループとサービスチェーンをクラスタに接続または切り離します。『クラスタ内のサービスグループの接続または切断, on page 106』を参照してください。

Note クラスタがアクティブになった後、サービスチェーンをクラスタに接続できます。

7. （オプション）すべての Day-N 操作を実行します。
   - サービスグループを切り離して、サービスチェーンを切り離します。『クラスタ内のサービスグループの接続または切断, on page 106』を参照してください。
   - クラスタにCSPデバイスを追加および削除します。Cloud OnRamp Colocation デバイスの追加, on page 55および Cloud OnRamp for Colocation デバイスの削除, on page 56を参照してください。
   - クラスタを非アクティブ化します。『クラスタの削除 , on page 85』を参照してください。
   - クラスタを再アクティブ化します。『クラスタの再アクティブ化, on page 86』を参照してください。
   - より多くのサービスグループまたはサービスチェーンを設計します。サービスグループでのサービスチェーンの作成, on page 87を参照してください。

Cloud OnRamp for Colocation デバイスの管理

Cisco SD-WAN Manager を介して、CSP デバイス、Catalyst 9500-40X デバイス、および VNF を追加できます。

Cloud OnRamp Colocation デバイスの追加

Cisco SD-WAN Manager を使用して、CSP デバイス、スイッチデバイス、および VNF を追加できます。Cisco Catalyst SD-WAN Cloud OnRamp for Colocation ソリューション製品識別子（PID）を注文すると、Cisco SD-WAN Manager からアクセスできるスマートアカウントからデバイス情報を入手できます。

始める前に

セットアップの詳細が次のようになっていることを確認します。

- Cisco SD-WAN Manager IP アドレスとログイン情報、Cisco SD-WAN Validator IP アドレスとログイン情報などの Cisco Catalyst SD-WAN セットアップの詳細
- Cisco CSP デバイスの CIMC IP アドレスとログイン情報、または UCSC CIMC IP アドレスとログイン情報などの NFVIS セットアップの詳細
- 両方のスイッチコンソールにアクセス可能

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Tools]** > **[SSH Terminal]** を選択して、Cisco SD-WAN Manager との SSH セッションを開始します。

ステップ 2 CSP デバイスまたはスイッチデバイスを選択します。

ステップ 3 CSP デバイスまたはスイッチデバイスのユーザー名とパスワードを入力し、[Enter] をクリックします。

ステップ 4 CSP デバイスの PID とシリアル番号（SN）を取得します。

次の出力例は、いずれかの CSP デバイスの PID を示しています。

```
CSP# show pl
platform-detail hardware_info Manufacturer "Cisco Systems Inc"
platform-detail hardware_info PID CSP-5444
platform-detail hardware_info SN WZP224208MB
platform-detail hardware_info hardware-version 74-105773-01
platform-detail hardware_info UUID da39edec-d831-e549-b663-9e407afd5ac6
platform-detail hardware_info Version 4.6.0-15
```

出力には、CSP デバイスの PID とシリアル番号の両方が表示されます。

ステップ 5 両方の Catalyst 9500 スイッチデバイスのシリアル番号を取得します。

次のサンプルは、最初のスイッチのシリアル番号を示しています。

```
Switch1# show version
Cisco IOS XE Software, Version 17.03.03
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.3.3, RELEASE
 SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Fri 26-Feb-21 02:01 by mcpre
Technology Package License Information:

-----------------------------------------------------------------------------
```

```
Technology-package                                          Technology-package
Current                       Type                          Next reboot
------------------------------------------------------------------------------
network-advantage    Smart License                  network-advantage
dna-advantage        Subscription Smart License     dna-advantage
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Advantage


Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco C9500-40X (X86) processor with 1331521K/6147K bytes of memory.
Processor board ID FCW2229A0RK
1 Virtual Ethernet interface
96 Ten Gigabit Ethernet interfaces
4 Forty Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
16777216K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
1638400K bytes of Crash Files at crashinfo-1:.
11264000K bytes of Flash at flash:.
11264000K bytes of Flash at flash-1:.

Base Ethernet MAC Address          : 00:aa:6e:f3:02:00
Motherboard Assembly Number        : 73-18140-03
Motherboard Serial Number          : FOC22270RF8
Model Revision Number              : D0
Motherboard Revision Number        : B0
Model Number                       : C9500-40X
System Serial Number               : FCW2229A0RK
CLEI Code Number                   :
```

この出力から、Catalyst 9500 スイッチ シリーズとシリアル番号を知ることができます。

ステップ 6 コロケーションクラスタ内のすべての CSP デバイスと Catalyst 9500 スイッチの PID とシリアル番号レコードを含む .CSV ファイルを作成します。

たとえば、ステップ 4 と 5 で得られた情報から、CSV 形式のファイルは次のようになります。

```
C9500-40,FCW2229A0RK CSP-5444,SN WZP224208MB
```

（注） コロケーションクラスタ内のすべてのデバイスに対して 1 つの .CSV ファイルを作成できます。

ステップ 7 Cisco SD-WAN Manager を使用して、すべての CSP とスイッチデバイスをアップロードします。詳細については、「Uploading a device authorized serial number file」を参照してください。

アップロード後、デバイスのテーブルにすべての CSP とスイッチデバイスが表示されます。

Cloud OnRamp for Colocation デバイスの削除

Cisco SD-WAN Manager から CSP デバイスを削除するには、次の手順を実行します。

始める前に

次の点を考慮してください。

- 削除するデバイスにサービスチェーンが接続されている場合は、サービスグループを切り離します。『クラスタ内のサービスグループの接続または切断（106ページ）』を参照してください。

手順

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

ステップ 2 該当するデバイスで [...] をクリックし、[Invalid] を選択します。

ステップ 3 **[Configuration]** > **[Certificates]**ウィンドウで、[Send to Controller] をクリックします。

ステップ 4 **[Configuration]** > **[Devices]**ウィンドウで、目的のデバイスの [...] をクリックし、[Delete WAN Edge] を選択します。

ステップ 5 [OK] をクリックして、デバイスの削除を確認します。

デバイスを削除すると、[WAN edge router serial number] リストからシリアル番号とシャーシ番号が削除され、Cisco SD-WAN Manager からも設定が完全に削除されます。

クラスタの管理

Note 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。

Cloud OnRamp for Colocation 画面を使用して、クラスタで使用できるコロケーションクラスタとサービスグループを構成します。

構成する 3 つの手順は次のとおりです。

- クラスタを作成します。『クラスタの作成とアクティブ化, on page 60』を参照してください。
- サービスグループを作成します。『サービスグループでのサービスチェーンの作成, on page 87』を参照してください。

- クラスタをサービスグループに接続します。『クラスタ内のサービスグループの接続または切断, on page 106』を参照してください。

コロケーションクラスタは、2 ～ 8 台の CSP デバイスと 2 台のスイッチの集合です。サポートされているクラスタテンプレートは次のとおりです。

- 小規模クラスタ：2 Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C +2 CSP
- 中規模クラスタ：2 Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C +4 CSP
- 大規模クラスタ：2 Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C +6 CSP
- 超大規模クラスタ：2 Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C +8 CSP

Note 少なくとも 2 つの CSP デバイスを 1 つずつクラスタに追加してください。3 つ、4 つなど、最大 8 つの CSP デバイスを追加することができます。任意のクラスタの Day-N 構成を編集し、最大 8 つの CSP デバイスまで各サイトに CSP デバイスのペアを追加できます。

クラスタに組み入れるすべてのデバイスのソフトウェアバージョンが同じであることを確認してください。

Note CSP-5444 および CSP-5456 デバイスを同じクラスタで使用することはできません。

クラスタの状態は次のとおりです。

- Incomplete：2 つの CSP デバイスと 2 つのスイッチの最小要件を提供せずに、クラスタが Cisco SD-WAN Manager インターフェイスから作成された場合。また、クラスタのアクティベーションはまだトリガーされていません。
- Inactive：2 つの CSP デバイスと 2 つのスイッチの最小要件を提供した後、Cisco SD-WAN Manager インターフェイスからクラスタが作成され、クラスタのアクティベーションがまだトリガーされていない場合。
- Init：クラスタのアクティベーションが Cisco SD-WAN Manager インターフェイスからトリガーされ、エンドデバイスへの Day-0 構成プッシュが保留中の場合。
- Inprogress：クラスタ内のいずれかの CSP デバイスが制御接続を確立すると、クラスタはこの状態に移行します。
- Pending：Day-0 構成のプッシュが保留中、または VNF のインストールが保留中の場合。
- Active：クラスタが正常にアクティブ化され、NCS が構成をエンドデバイスにプッシュした場合。
- Failure：Cisco Colo Manager が起動していない場合、またはいずれかの CSP デバイスが UP イベントの受信に失敗した場合。

Active 状態または Failure 状態へのクラスタの移行は次のとおりです。

- **[Inactive]** > **[Init]** > **[Inprogress]** > **[Pending]** > **[Active]**— 成功
- **[Inactive]** > **[Init]** > **[Inprogress]** > **[Pending]** > **[Failure]**— 失敗

クラスタのプロビジョニングと構成

このトピックでは、サービスチェーンの展開を可能にするクラスタのアクティブ化について説明します。

クラスタをプロビジョニングして構成するには、次の手順を実行します。

1. 2 ～ 8 個の CSP デバイスと 2 つのスイッチを追加して、コロケーションクラスタを作成します。

   起動する前に CSP デバイスをクラスタに追加し、Cisco SD-WAN Manager を使用して設定できます。AAA、デフォルトのユーザー（admin）パスワード、NTP、syslog などのグローバル機能を使用して、CSP デバイスと Catalyst 9K スイッチを設定できます。

2. サービスチェーン VLAN プール、VNF 管理 IP アドレスプール、管理ゲートウェイ、VNF データプレーン IP プール、システム IP アドレスプールなどの IP アドレスプール入力を含むコロケーション クラスタ パラメータを設定します。

3. サービス グループを設定します。

   サービスグループは、1 つ以上のサービスチェーンで構成されます。

   Note 定義済みまたは検証済みのサービス チェーン テンプレートのいずれかを選択するか、カスタムのサービスチェーンを作成して、サービスチェーンを追加できます。前述のように、サービスチェーンごとに、入力および出力 VLAN ハンドオフとサービスチェーンのスループットまたは帯域幅を設定します。

4. サービステンプレートから各 VNF を選択して、各サービスチェーンを構成します。VNF リポジトリにすでにアップロードされている VNF イメージを選択して、必要なリソース（CPU、メモリ、ディスク）とともに VM を起動します。サービスチェーン内の各 VNF について、次の情報を指定します。

   - HA、共有 VM などの特定の VM インスタンスの動作は、サービスチェーン全体で共有できます。
   - VLAN プール、管理 IP アドレス、またはデータ HA IP アドレスの一部ではなく、トークン化されたキーの Day-0 設定値。ピアリング IP や自律システム値など、最初と最後の VM ハンドオフ関連情報を指定する必要があります。サービスチェーンの内部パラメータは、指定された VLAN、管理、またはデータプレーン IP アドレスプールから Cisco SD-WAN Validator によって自動的に更新されます。

5. サービスグループごとに必要な数のサービスチェーンを追加し、クラスタに必要な数のサービスグループを作成します。
6. クラスタをサイトまたは場所に接続するには、すべての構成が完了した後にクラスタをアクティブ化します。

   [Task View] ウィンドウで、クラスタのステータスが進行中からアクティブまたはエラーに変化するのを確認できます。

クラスタを編集するには、以下を行います。

1. サービスグループまたはサービスチェーンを追加または削除して、アクティブ化されたクラスタを変更します。
2. AAA、システム設定などのグローバル機能設定を変更します。

クラスタを作成する前に、サービスグループとサービスチェーンを事前に設計できます。クラスタがアクティブになった後、サービスグループをクラスタに接続できます。

クラスタの作成とアクティブ化

このトピックでは、CSP デバイス、Cisco Catalyst スイッチを 1 つのユニットとして使用してクラスタを形成し、クラスタ固有の構成でクラスタをプロビジョニングする方法の手順について説明します。

始める前に

- Cisco SD-WAN Manager および CSP デバイスのクロックを同期していることを確認します。CSP デバイスのクロックを同期するには、クラスタ設定に関する情報を入力するときに、CSP デバイスの NTP サーバーを構成します。
- Cisco SD-WAN Manager および Cisco SD-WAN Validator の NTP サーバーが設定されていることを確認します。NTP サーバーを設定するには、『Cisco Catalyst SD-WAN System and Interface Configuration Guide』を参照してください。
- CSP デバイスを起動するように、CSP デバイスの OTP を構成していることを確認します。『Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide』の「Bring Up Cloud Services Platform」を参照してください。
- 両方の Catalyst 9500 スイッチの電源をオンにして、それらが動作していることを確認してください。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、Cisco SD-WAN Manager を選択して、**[Configuration]** > **[Cloud OnRamp for Colocation]** をクリックします。

a) [Configure & Provision Cluster] をクリックします。

b) 次の情報を入力します。

表 *18 :* クラスタ情報

フィールド	説明
Cluster Name	クラスタ名には、128 文字の英数字を含めることができます。
Description	説明には、2048 文字の英数字を含めることができます。
Site ID	オーバーレイ ネットワーク サイト識別子。サイト ID に入力する値が、他の Cisco Catalyst SD-WAN オーバーレイ要素の組織サイト ID 構造と同様であることを確認してください。
Location	場所には、128 文字の英数字を含めることができます。
Cluster Type	複数のテナント間で共有できるようにマルチテナントモードでクラスタを構成するには、[Shared] を選択します。 （注） シングルテナントモードでは、クラスタタイプはデフォルトで [Non Shared] が選択されています。

c) スイッチを構成するには、[Switches] ボックスのスイッチアイコンをクリックします。[Edit Switch] ダイアログボックスで、スイッチ名を入力し、ドロップダウンリストからスイッチのシリアル番号を選択します。[Save] をクリックします。

スイッチ名には、128 文字の英数字を含めることができます。

ドロップダウンリストに表示されるスイッチのシリアル番号は、PnP プロセスを使用して取得され、Cisco SD-WAN Manager と統合されます。これらのシリアル番号は、CCW で Cisco Catalyst SD-WAN Cloud OnRamp for Colocation ソリューション PID を注文し、スイッチデバイスを調達するときに、スイッチに割り当てられます。

（注） スイッチデバイスと CSP デバイスのシリアル番号フィールドを空白のままにして、コロケーションクラスタを設計し、後でクラスタを編集して、デバイスを調達した後でシリアル番号を追加できます。ただし、シリアル番号のない CSP デバイスまたはスイッチデバイスを使用してクラスタをアクティブ化することはできません。

d) 別のスイッチを構成するには、手順 c を繰り返します。

e) CSP デバイスを構成するには、[Appliances] ボックスの CSP アイコンをクリックします。[Edit CSP] ダイアログボックスが表示されます。CSP デバイス名を指定し、ドロップダウンリストから CSP シリアル番号を選択します。[Save] をクリックします。

CSP デバイス名には、128 文字の英数字を含めることができます。

f) CSP デバイスの OTP を構成して、デバイスを起動します。

g) 残りの CSP デバイスを追加するには、手順 e を繰り返します。

h) [Save] をクリックします。
クラスタを作成すると、クラスタ設定画面で、デバイスにシリアル番号が割り当てられていないデバイスの横に、黄色の円で囲まれた省略記号が表示されます。デバイスを編集してシリアル番号を入力できます。

i) CSP デバイス構成を編集するには、CSP アイコンをクリックし、サブステップ e で説明されているプロセスを実行します。

j) クラスタの必須およびオプションのグローバルパラメータを設定するには、クラスタ構成ページで、[Cluster Configuration] のパラメータを入力します。クラスタの設定 （62 ページ）を参照してください。

k) [**保存（Save）**] をクリックします。
作成したクラスタは、クラスタ構成ページの表に表示できます。

ステップ 2 クラスタをアクティブ化するには、次の手順を実行します。

a) クラスタテーブルからクラスタをクリックします。

b) 目的のクラスタの […] をクリックし、[Activate] を選択します。

クラスタをアクティブ化すると、Cisco SD-WAN Manager はクラスタ内の CSP デバイスとの DTLS トンネルを確立し、そこで Cisco Colo Manager を介してスイッチに接続します。DTLS トンネル接続が実行されている場合、クラスタ内の CSP デバイスが Cisco Colo Manager をホストするために選択されます。Cisco Colo Manager が起動し、Cisco SD-WAN Manager がグローバルパラメータ設定を CSP デバイスと Cisco Catalyst 9500 スイッチに送信します。クラスタのアクティブ化の進行状況については、クラスタアクティベーションの進行状況 （73 ページ）を参照してください。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、Cisco Colo Manager（CCM）および CSP デバイス設定タスクは、タスクが作成されてから 30 分後にタイムアウトします。長時間実行されるイメージのインストール操作の場合、これらの構成タスクがタイムアウトして失敗することがありますが、クラスタのアクティブ化状態は引き続き保留中の状態のままになります。

Cisco vManage リリース 20.8.1 以降では、CCM および CSP デバイス設定タスクは、Cisco SD-WAN Manager がターゲットデバイスから受信した最後のハートビートステータスメッセージの 30 分後にタイムアウトします。この変更により、実行時間の長いイメージのインストール操作によって、タスクの作成後に事前定義された時間が経過した後に構成タスクが失敗することがなくなりました。

クラスタの設定

クラスタ設定パラメータを以下に示します。

ログイン クレデンシャル

1. [Cluster Topology] ウィンドウで、[Credentials] の横にある [Add] をクリックします。[Credentials] 設定画面で、次のように入力します。
   - （必須）[Template Name]：テンプレート名には、128 文字の英数字を含めることができます。
   - （オプション）[Description]：説明には、2048 文字の英数字を含めることができます。
2. [New User] をクリックします。
   - [Name] フィールドに、ユーザー名を入力します。
   - [Password] フィールドにパスワードを入力し、[Confirm Password] フィールドでパスワードを確認します。
   - [Role] ドロップダウンリストで、管理者を選択します。
3. [Add] をクリックします。

   新しいユーザーとユーザー名およびパスワード、およびロールとアクションが表示されます。
4. [Save] をクリックします。

   新しいユーザーのログイン情報が追加されます。
5. 構成をキャンセルするには、[Cancel] をクリックします。
6. ユーザーの既存のログイン情報を編集するには、[Edit] をクリックして構成を保存します。

リソースプール

1. [Cluster Topology] ウィンドウで、[Resource Pool] の横にある [Add] をクリックします。[Resource Pool] 設定画面で、次のフィールドに値を入力します。
   - [Name]：IP アドレスプールの名前には、128 文字の英数字を含める必要があります。
   - [Description]：説明には、2048 文字の英数字を含めることができます。
2. [DTLS Tunnel IP] フィールドに、DTLS トンネルに使用する IP アドレスを入力します。複数の IP アドレスを入力するには、アドレスをカンマで区切ります。範囲を入力するには、IP アドレスをハイフンで区切ります（たとえば、172.16.0.180-172.16.255.190）。
3. [Service Chain VLAN Pool] フィールドに、サービスチェーンに使用する VLAN 番号を入力します。複数の番号を入力するには、カンマで区切ります。数値の範囲を入力するには、番号をハイフンで区切ります（たとえば、1021-2021）。

   VLAN 情報を入力するときは、次の点を考慮してください。

   1002 ～ 1005 は予約済みの VLAN 値であり、クラスタ作成 VLAN プールでは使用しないでください。

（注） 有効な VNF VLAN プール：1010 ～ 2000 および 1003 ～ 2000

無効：1002 ～ 1005（使用しないでください）

注意 1002 ～ 1005 は構成に使用できません。許可される VLAN は連続している必要があります。

例：データ VLAN プールを 1006-2006 と入力します。サービスチェーンの作成中に、この VLAN 範囲が入力/出力 VLAN で使用されないようにしてください。

4. [VNF Data Plane IP Pool] フィールドに、VNF インターフェイスでデータプレーンを自動構成するために使用する IP アドレスを入力します。複数の IP アドレスを入力するには、アドレスをカンマで区切ります。範囲を入力するには、IP アドレスをハイフンで区切ります（たとえば、10.0.0.1-10.0.0.100）。

5. [VNF Management IP Pool] フィールドで、VNF に使用する IP アドレスを入力します。複数の IP アドレスを入力するには、アドレスをカンマで区切ります。範囲を入力するには、IP アドレスをハイフンで区切ります（たとえば、192.168.30.99-192.168.30.150）。

（注） これらのアドレスは、セキュアインターフェイスの IP アドレスです。

6. [Management Subnet Gateway] フィールドに、管理ネットワークへのゲートウェイの IP アドレスを入力します。これにより、DNS がクラスタから抜けられるようになります。

7. [Management Mask] フィールドに、フェールオーバークラスタのマスク値を入力します。たとえば、/24 です。255.255.255.0 ではありません

8. [Switch PNP Server IP] フィールドに、スイッチデバイスの IP アドレスを入力します。

（注） スイッチの IP アドレスは、管理プールから自動的に取得され、これが最初の IP アドレスです。スイッチの DHCP サーバーで別の IP アドレスが構成されている場合、これを変更できます。

9. [Save] をクリックします。

ポート接続

表 *19* : 機能の履歴

機能名	リリース情報	説明
フレキシブルトポロジ	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1 Cisco NFVIS リリース 4.2.1	この機能により、NIC カードを柔軟に挿入し、Cloud onRamp for Colocation クラスタ内でデバイス（CSP デバイスおよび Catalyst 9500 スイッチ）を相互接続することができます。どの CSP ポートも、スイッチの任意のポートに接続できます。Stackwise Virtual Switch Link（SVL）ポートは任意のポートに接続でき、同様にアップリンクポートはスイッチの任意のポートに接続できます。
100G インターフェイスでの SVL ポート構成のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1 Cisco NFVIS リリース 4.8.1	この機能を使用すると、Cisco Catalyst 9500-48Y4C スイッチの 100-G イーサネットインターフェイスに SVL ポートを構成できるため、高レベルのパフォーマンスとスループットが保証されます。

SVL およびアップリンクポートを構成するための前提条件

- SVL およびアップリンクポートを構成するときは、Cisco SD-WAN Manager で構成するポート番号が物理的にケーブル接続されたポートと一致していることを確認してください。
- 両方のスイッチにシリアル番号を割り当ててください。「Create and Activate Clusters」を参照してください。

SVL およびアップリンクポートの構成

- [Cluster Topology] ウィンドウで、[Port Connectivity] の横にある [Add] をクリックします。

  [Port Connectivity] 設定画面に、構成された両方のスイッチが表示されます。スイッチポートにカーソルを合わせると、ポート番号とポートタイプが表示されます。

（注） SVL およびアップリンクポートの詳細については、『Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide』の「Wiring Requirements」を参照してください。

デフォルトの SVL およびアップリンクポートの変更

デフォルトのポート番号とポートタイプを変更する前に、Cisco Catalyst 9500-40X および Cisco Catalyst 9500-48Y4C スイッチに関する次の情報に注意してください。

- Cisco vManage リリース 20.8.1 以降では、2 つの Cisco Catalyst 9500-40X スイッチまたは 2 つの Cisco Catalyst 9500-48Y4C スイッチでコロケーションクラスタを作成するときに、2 つの SVL ポートと 1 つのデュアルアクティブ検出（DAD）ポートを構成できます。
- SVL および DAD ポートが Cisco Catalyst 9500-48Y4C スイッチに対して正しく構成されていることを確認するには、次の情報に注意してください。
  - 同じ速度のインターフェイス、つまり 25G インターフェイスまたは 100G インターフェイスのいずれかで SVL ポートを構成します。両方のスイッチで構成が同じであることを確認します。
  - 両方のスイッチの 25G インターフェイスでのみ DAD ポートを構成します。
  - 既存のクラスタの場合、非アクティブな場合にのみ SVL ポートを変更できます。
  - Cisco vManage リリース 20.8.1 以前のリリースで作成されたクラスタは、Cisco vManage リリース 20.8.1 にアップグレード後に 2 つの SVL ポートと 1 つの DAD ポートを自動的に表示します。
- Cisco Catalyst 9500-40X スイッチの場合、両方のスイッチの 10G インターフェイスで SVL および DAD ポートを構成する必要があります。
- Cisco Catalyst 9500 スイッチのデフォルトの SVL、DAD、およびアップリンクポートは次のとおりです。

  Cisco Catalyst 9500-40X

  - SVL ポート：Te1/0/38 ～ Te1/0/39、および Te2/0/38 ～ Te2/0/39

    Cisco vManage リリース 20.7.1 以前のリリースでは、デフォルトの SVL ポートは Te1/0/38 ～ Te1/0/40 および Te2/0/38 ～ Te2/0/40 です。
  - DAD ポート：Te1/0/40 および Te2/0/40
  - アップリンクポート：Te1/0/36、Te2/0/36（入力 VLAN ハンドオフ）、Te1/0/37、および Te2/0/37（出力 VLAN ハンドオフ）

  Cisco Catalyst 9500-48Y4C

  - SVL ポート：Hu1/0/49 ～ Hu1/0/50 および Hu2/0/49 ～ Hu2/0/50

    Cisco vManage リリース 20.7.1 以前のリリースでは、デフォルトの SVL ポートは Twe1/0/46 ～ Twe1/0/48 および Twe2/0/46 ～ Twe2/0/48 です。
  - DAD ポート：Twe1/0/48 および Twe2/0/48
  - アップリンクポート：25G スループット用の Twe1/0/44、Twe2/0/44（入力 VLAN ハンドオフ）、Twe1/0/45、および Twe2/0/45（出力 VLAN ハンドオフ）。

- I、E、および S は、それぞれ入力、出力、および SVL ポートを表します。
- 物理的ケーブル接続がデフォルト構成と同じであることを確認し、[Save] をクリックします。

SVL ポートとアップリンクポートの接続が異なる場合にデフォルトポートを変更するには、次の手順を実行します。

1. 両方のスイッチが同じポートを使用している場合：
   1. 物理的に接続されているポートに対応するスイッチのポートをクリックします。
   2. ポート構成を他のスイッチに追加するには、[Apply change] チェックボックスをオンにします。

   両方のスイッチが同じポートを使用していない場合：
   1. [Switch1] のポートをクリックします。
   2. [Port Type] ドロップダウンリストからポートタイプを選択します。
   3. [Switch2] のポートをクリックし、ポートタイプを選択します。
2. 別のポートを追加するには、手順 1 を繰り返します。
3. [Save] をクリックします。
4. ポート接続情報を編集するには、[Cluster Topology] ウィンドウで、[Port Connectivity] の横にある [Edit] をクリックします。

（注） クラスタがアクティブ化されていない場合は、クラスタの SVL およびアップリンクポートを変更できます。

5. ポートをリセットしてデフォルト設定にするには、[Reset] をクリックします。

Cisco CSP デバイスの残りのポート（SR-IOV および OVS）とスイッチとの接続は、クラスタをアクティブ化するときに、Link Layer Discovery Protocol（LLDP）を使用して自動的に検出されます。これらのポートを設定する必要はありません。

Cisco Colo Manager は、スイッチのネイバーポートを検出し、すべての Niantic ポートと Fortville ポートが接続されているかどうかを識別します。いずれかのポートが接続されていない場合、CCM から Cisco SD-WAN Manager に通知が送信され、タスクビューウィンドウに表示できます。

NTP

必要に応じて、クラスタの NTP サーバーを構成します。

1. [Cluster Topology] ウィンドウで、[NTP] の横にある [Add] をクリックします。[NTP] 設定画面で、次のように入力します。

- [Template Name]：NTP テンプレートの名前は英数字で、最大 128 文字である必要があります。
- [Description]：説明は英数字で、最大 2048 文字にする必要があります。

2. [Preferred server] フィールドに、プライマリ NTP サーバーの IP アドレスを入力します。
3. [Backup server] フィールドに、セカンダリ NTP サーバーの IP アドレスを入力します。
4. [Save] をクリックします。

   NTP サーバーが追加されます。
5. NTP サーバーの構成をキャンセルするには、[Cancel] をクリックします。
6. NTP サーバーの構成の詳細を編集するには、[Edit] をクリックします。

Syslog サーバ

必要に応じて、クラスタの syslog パラメータを構成します。

1. [Cluster Topology] ウィンドウで、[Syslog] の横にある [Add] をクリックします。[Syslog] 設定画面で、次のように入力します。
   - [Template Name]：システムテンプレートの名前は英数字で、最大 128 文字を含めることができます。
   - [Description]：説明の最大長は 2048 文字で、英数字のみを使用できます。
2. [Severity] ドロップダウンリストから、ログ記録する syslog メッセージのシビラティ（重大度）を選択します。
3. 新しい syslog サーバーを追加するには、[New Server] をクリックします。

   syslog サーバーの IP アドレスを入力します。
4. [Save] をクリックします。
5. 構成をキャンセルするには、[Cancel] をクリックします。
6. 既存の syslog サーバー構成を編集するには、[Edit] をクリックして構成を保存します。

TACACS 認証

表 *20 :* 機能の履歴

機能名	リリース情報	説明
TACACS Authentication	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、Cisco CSP および Cisco Catalyst 9500 デバイスにアクセスするユーザーの TACACS 認証を構成できます。TACACS を使用してユーザーを認証すると、Cisco CSP および Cisco Catalyst 9500 デバイスへのアクセスが検証され、保護されます。

TACACS 認証は、クラスタがアクティブになった後に Cisco CSP および Cisco Catalyst 9500 デバイスにアクセスできる有効なユーザーを決定します。

考慮すべき点

- デフォルトでは、ロールベース アクセス コントロール（RBAC）を持つ管理ユーザーは、Cisco CSP および Cisco Catalyst 9500 デバイスへのアクセスを許可されています。
- TACACS と RBAC を使用して構成する場合は、同じユーザーに異なるパスワードを設定しないでください。TACACS と RBAC で同じユーザーに異なるパスワードが設定されている場合、RBAC ユーザーとパスワードの認証が使用されます。デバイスで RBAC を構成する方法については、ログイン クレデンシャル （63 ページ）を参照してください。

ユーザーを認証するには、次の手順を実行します。

1. TACACS サーバー構成を追加するには、[Cluster Topology] ウィンドウで、[TACACS] の横にある**[Other Settings]** > **[Add]** をクリックします。

   TACACS サーバー構成を編集するには、[Cluster Topology] ウィンドウで、[TACACS] の横にある**[Other Settings]** > **[Edit]** をクリックします。

   [TACACS] 設定画面で、次に関する情報を入力します。

   - [Template Name]：TACACS テンプレート名には、128 文字の英数字を含めることができます。
   - （オプション）[Description]：説明には、2048 文字の英数字を含めることができます。

2. 新しい TACACS サーバーを追加するには、[+ New TACACS SERVER] をクリックします。
   - [Server IP Address] に、IPv4 アドレスを入力します。

     TACACS サーバーのホスト名には IPv4 アドレスを使用します。
   - [Secret] にパスワードを入力し、[Confirm Secret] でパスワードを確認します。

3. [Add] をクリックします。

   新しい TACACS サーバーの詳細は、[TACACS] 設定画面にリストされます。

（注） 最大 4 つの TACACS サーバーを追加できます。

4. 別の TACACS サーバーを追加するには、手順 2 から手順 3 を繰り返します。

   ユーザーの認証時に、最初の TACACS サーバーに到達できない場合、4 つのサーバーすべてが検証されるまで、次のサーバーが検証されます。

5. [Save] をクリックします。

6. TACACS サーバーの設定を削除するには、TACACS サーバーの詳細リストから行を選択し、[Action] の下の [Delete] をクリックします。

（注） 既存の TACACS サーバー情報を変更するには、TACACS サーバーを削除してから新しいサーバーを追加してください。

7. Cisco SD-WAN Manager で TACACS サーバーの設定を表示するには、**[Configuration]** > **[Devices]**をクリックします。

   目的の Cisco CSP デバイスまたは Cisco Catalyst 9500 スイッチの [...] をクリックし、[Running Configuration] を選択します。

バックアップサーバー設定

考慮すべき点

- NFS サーバーを使用しない場合、Cisco SD-WAN Manager は、将来の RMA 要件のための CSP デバイスのバックアップコピーを正常に作成できません。
- NFS サーバーのマウント場所と構成は、クラスタ内のすべての CSP デバイスで同じです。
- クラスタ内の既存のデバイスを交換用の CSP デバイスとして考えないでください。

（注） 交換用の CSP デバイスが利用できない場合は、Cisco SD-WAN Manager にデバイスが表示されるまで待ちます。

- クラスタ内の CSP デバイスに障害があることを特定した後は、クラスタにそれ以上サービスチェーンを接続しないでください。
- CSP デバイスでのバックアップ操作により、NFVIS 構成と VM を含むバックアップファイルが作成されます（VM が CSP デバイスでプロビジョニングされている場合）。以下の情報を参考にしてください。
  - 自動バックアップファイルが生成され、次の形式になります。

    serial_number + "_" + time_stamp + ".bkup"

次に例を示します。

```
WZP22180EW2_2020_06_24T18_07_00.bkup
```

- バックアップ操作全体のステータスと各バックアップコンポーネントの内部状態を指定する内部状態モデルが維持されます。
  - NFVIS：xml ファイルとしての CSP デバイスの構成バックアップ、config.xml。
  - VM_Images：個別にリストされている `data/intdatastore/uploads` 内のすべての VNF tar.gz パッケージ。
  - VM_Images_Flavors：img_flvr.img.bkup などの VM イメージ。
  - VNF の個々の tar バックアップ：vmbkp などのファイル。
- backup.manifest ファイルには、バックアップパッケージ内のファイルの情報と、復元操作中に検証するためのチェックサムが含まれています。

クラスタ内のすべての CSP デバイスのバックアップコピーを作成するには、次の手順を実行します。

1. [Cluster Topology] ウィンドウで、[Backup] の横にある [Add] をクリックします。

   バックアップサーバーの設定を編集するには、[Cluster Topology] ウィンドウで、[Backup] の横にある [Edit] をクリックします

   [Backup] 設定画面で、次のフィールドに関する情報を入力します。

   - Mount Name：NFS の場所をマウントした後、NFS マウントの名前を入力します。
   - Storage Space：ディスク容量を GB 単位で入力します。
   - Server IP：NFS サーバーの IP アドレスを入力します。
   - Server Path：`/data/colobackup` など、NFS サーバーのフォルダパスを入力します
   - Backup：[Backup] をクリックして有効にします。
   - Time：バックアップ操作をスケジュールする時間を設定します。
   - Interval：オプションから選択して、定期的なバックアッププロセスをスケジュールします。
     - Daily：最初のバックアップは、バックアップ構成がデバイスに保存されてから 1 日後に作成され、その後は毎日作成されます。
     - Weekly：最初のバックアップは、バックアップ構成がデバイスに保存されてから 7 日後に作成され、その後は毎週作成されます。
     - Once：バックアップコピーは選択した日に作成され、クラスタの存続期間全体にわたって有効です。未来のカレンダーの日付を選択できます。

2. [Save] をクリックします。

3. 過去 5 回のバックアップ操作のステータスを表示するには、**show hostaction backup status** コマンドを使用します。バックアップステータス構成コマンドについては、「Backup and Restore NFVIS and VM Configurations」を参照してください。このコマンドを使用するには、以下の手順を実行します。
   1. Cisco SD-WAN Manager で、**[Tools]** > **[SSH Terminal]** の画面をクリックして、Cisco SD-WAN Manager との SSH セッションを開始します。
   2. CSP デバイスを選択します。
   3. CSP デバイスのユーザー名とパスワードを入力し、[Enter] をクリックして CSP デバイスにログインし、**show hostaction backup status** コマンドを実行します。

CSP デバイスの復元

復元する CSP デバイスで CLI を使用する場合にのみ、復元操作を実行できます。

1. **mount nfs-mount storage** コマンドを使用して NFS をマウントします。

   詳細については、「Network File System Support」を参照してください。

（注） バックアップファイルにアクセスするには、NFS ファイルシステムをマウントするための構成が、障害のあるデバイスと一致している必要があります。NFS マウントの場所と構成はすべての CSP デバイスで同じであるため、他の正常な CSP デバイスからこの情報を表示できます。情報を表示してキャプチャするには、次のいずれかを実行します。

- [Cluster Topology] ウィンドウで、[Backup] の横にある [Add] をクリックします。
- **show running-config** コマンドを使用して、CSP デバイスで実行されているアクティブな構成を表示します。

mount nfs-mount storage { *mount-name* | **server_ip** *server_ip* | **server_path** *server_path* | **storage_space_total_gb** *storage_space_total_gb* | **storage_type** *storage_type* }

例：`mount nfs-mount storage nfsfs/ server_ip 172.19.199.199 server_path /data/colobackup/ storage_space_total_gb 100.0 storagetype nfs`

2. **hostaction restore** コマンドを使用して、交換用 CSP デバイスでバックアップ情報を復元します。

   次に例を示します。

```
hostaction restore except-connectivity file-path
nfs:nfsfs/WZP22180EW2_2020_06_24T18_07_00.bkup
```

（注） ステップ 2 でマウントされた NFS サーバーとの接続を維持するには、except-connectivity パラメータを指定します。

3. **show hostaction backup status** コマンドを使用して、過去 5 つのバックアップイメージのステータスとそれらの動作ステータスを表示します。

   また、Cisco SD-WAN Manager **[Monitor]** > **[Logs]** > **[Events]**ページで利用可能な通知からバックアップイメージを表示することもできます。

（注） Cisco vManage リリース 20.6.1 以前のリリースでは、Cisco SD-WAN Manager の **[Monitor]** > **[Events]** ページで利用可能な通知からバックアップイメージを表示できます。

4. CSP デバイスで **show hostaction restore-status** コマンドを使用して、復元プロセス全体と、システム、イメージとフレーバー、VM などの各コンポーネントのステータスを表示します。

5. ステータスを表示した後でエラーを修正するには、デバイスの工場出荷時のデフォルトへのリセットを実行します。

（注） 工場出荷時のデフォルトにリセットすると、デバイスがデフォルト構成に設定されます。したがって、交換用デバイスで手順 1 ～ 4 の復元操作を実行する前に、復元操作のすべての前提条件が満たされていることを確認してください。

CSP デバイスで復元操作を構成する方法の詳細については、「Backup and Restore NFVIS and VM Configurations」を参照してください。

クラスタアクティベーションの進行状況

表 *21* : 機能の履歴

機能名	リリース情報	説明
クラスタのアクティブ化の進行状況を監視する	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	この機能は、各ステップでクラスタのアクティブ化の進行状況を表示し、プロセス中に発生する可能性のある障害を示します。クラスタをアクティブ化するプロセスには約 30 分以上かかります。Cisco SD-WAN Manager タスクビューウィンドウを使用して進行状況をモニターし、[Monitoring] ページからイベントをモニターできます。

クラスタのアクティブ化後にクラスタのアクティブ化ステータスを確認するには、タスクビューウィンドウで進行状況を表示します。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、Cisco Colo Manager が起動し、アクティブ化の進行状況が CLOUD ONRAMP タスクの一部として報告されます。このタスクは、Cisco Colo Manager の起動およびアクティブ化シーケンスの 7 つのステップを表示し、シーケンスが正常に完了したかどうかを示します。プッシュ機能テンプレート構成タスクは、RBAC 設定構成プッシュのステータスを表示します。

Cisco vManage リリース 20.8.1 では、Cisco SD-WAN Manager がターゲット CSP デバイスから Cisco Colo Manager Healthy を受信すると、CLOUD ONRAMP タスクが完了します。プッシュ機能テンプレート構成タスクは、Cisco Colo Manager の起動およびアクティブ化シーケンスの 7 つのステップを表示し、シーケンスが正常に完了したかどうか、および RBAC 設定構成プッシュのステータスを示します。

図 *3*：クラスタのアクティブ化（*Cisco vManage* リリース *20.7.1* 以前）

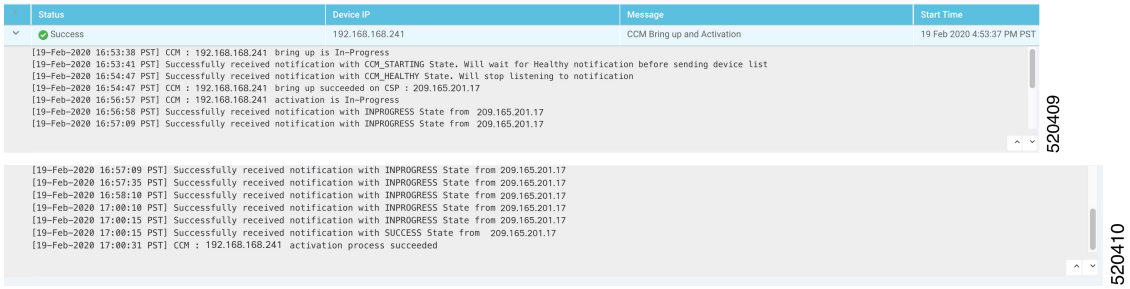


図 *4*：*CLOUD ONRAMP Cisco Colo Manager* タスク（*Cisco vManage* リリース *20.8.1* 以降）

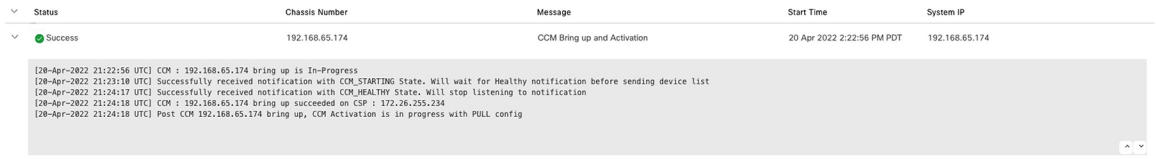
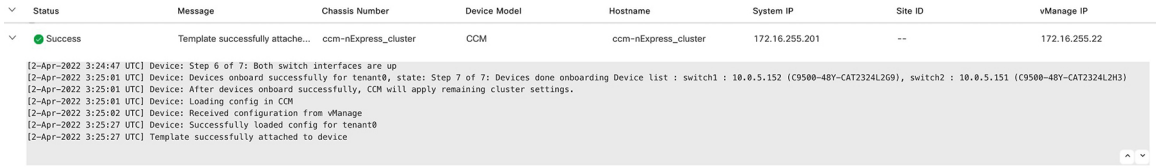


図 *5*：プッシュ機能テンプレート構成タスク（*Cisco vManage* リリース *20.8.1* 以降）



次の検証手順を実行します。

1. クラスタの状態を表示して状態を変更するには、以下の手順を実行します。
    1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]** を選択します。「PENDING」状態になったクラスタについては、[...] をクリックし、[Sync] を選択します。このアクションは、クラスタを「ACTIVE」状態に戻します。

2. クラスタが「ACTIVE」状態に戻ったかどうかを確認するには、クラスタの正常なアクティブ化を表示します。

2. CSP デバイスに存在するサービスグループを表示するには、Cisco SD-WAN Manager メニューから **[Monitor]** > **[Devices]** > **[Colocation Cluster]** を選択します。

   Cisco vManage リリース 20.6.1 以前：CSP デバイスに存在するサービスグループを表示するには、Cisco SD-WAN Manager メニューから **[Monitor]** > **[Network]** > **[Colocation Clusters]** を選択します。

   クラスタを選択してから、CSP デバイスを選択します。他の CSP デバイスを選択して表示できます。

3. クラスタが CSP デバイスからアクティブ化されているかどうかを確認するには、以下の手順を実行します。

   1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Devices]** の順に選択します。
   2. すべての CSP デバイスのデバイスステータスを表示し、それらが Cisco SD-WAN Manager と同期していることを確認します。
   3. CSP デバイスの状態を表示し、証明書が CSP デバイスにインストールされていることを確認します。

（注） OTP による CSP のアクティブ化後、5 分以上 CSP デバイスの状態に「cert installed」と表示されない場合は、 を参照してください。

   クラスタが CSP デバイスからアクティブ化された後、Cisco Colo Manager は、Cisco NFVIS ホストでクラスタアクティブ化タスクを実行します。

4. CSP デバイスで Cisco Colo Manager が有効になっているかどうかを表示するには、以下の手順を実行します。

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

      Cisco vManage リリース 20.6.1 以前：Cisco SD-WAN Manager のメニューから **[モニター（Monitor）]** > **[ネットワーク（Network）]** の順に選択します。

   2. [Colocation Cluster] をクリックします。

      Cisco vManage リリース 20.6.1 以前：[Colocation Clusters] をクリックします。

      特定の CSP デバイスに対して Cisco Colo Manager が有効になっているかどうかを表示します。

5. Cisco Colo Manager の正常性をモニターするには、次の手順を実行します。

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

Cisco vManage リリース 20.6.1 以前：Cisco SD-WAN Manager のメニューから **[モニター（Monitor）]** > **[ネットワーク（Network）]** の順に選択します。

2. [Colocation Cluster] をクリックします。

   Cisco vManage リリース 20.6.1 以前：[Colocation Clusters] をクリックします。

   目的の CSP デバイスで Cisco Colo Manager が有効になっているかどうかを表示します。

3. Cisco Colo Manager が有効な CSP デバイスの場合は、CSP デバイスをクリックします。
4. Cisco Colo Manager の正常性を表示するには、[Colo Manager] をクリックします。

Cisco Colo Manager のステータスが "STARTING" の後に "HEALTHY" に変わらない場合は、『Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide』の「Troubleshoot Cisco Colo Manager Issues」のトピックを参照してください。

Cisco Colo Manager のステータスは "STARTING" の後に "HEALTHY" に変わったが、スイッチの設定がすでに完了した後、Cisco Colo Manager のステータスが 20 分以上にわたって IN-PROGRESS と表示される場合は、『Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide』の「Switch devices are not calling home to PNP or Cisco Colo Manager」のトピックを参照してください。

クラスタの表示

クラスタ構成を表示するには、次の手順を実行します。

手順

ステップ 1 Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]**を選択します。

ステップ 2 目的のクラスタの […] をクリックし、[View] を選択します。

[Cluster] ウィンドウには、クラスタ内のスイッチデバイスと CSP デバイスが表示され、構成されているクラスタ設定が表示されます。

クラスタのグローバルパラメータ、スイッチデバイスおよび CSP デバイスの構成のみを表示できます。

ステップ 3 [Cancel] をクリックし、[Cluster] ウィンドウに戻ります。

クラスタの編集

グローバルパラメータなどの既存のクラスタ構成を変更するには、次の手順を実行します。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]** を選択します

ステップ 2 目的のクラスタの [...] をクリックし、[Edit] を選択します。

[Cluster] ウィンドウには、クラスタ内のスイッチデバイスと CSP デバイスが表示され、構成されているクラスタ設定が表示されます。

ステップ 3 クラスタ設計ウィンドウでは、いくつかのグローバルパラメータを変更できます。クラスタがアクティブ状態か非アクティブ状態かに基づいて、クラスタで次の操作を実行できます。

1. 非アクティブ状態：
   - すべてのグローバルパラメータとリソースプールパラメータを編集します。
   - CSP デバイスをさらに追加します（最大 8 つ）。
   - スイッチまたはCSPデバイスの名前またはシリアル番号を編集することはできません。代わりに、CSP またはスイッチを削除し、別の名前とシリアル番号を持つ別のスイッチまたは CSP を追加します。
   - クラスタ構成全体を削除します。
2. アクティブ状態：
   - リソースプールパラメータを除くすべてのグローバルパラメータを編集します。

     （注） クラスタがアクティブなときは、リソースプールパラメータを変更できません。ただし、リソースプールパラメータを変更する唯一のオプションは、クラスタを削除し、正しいリソースプールパラメータを使用してクラスタを再作成することです。

   - スイッチまたは CSP デバイスの名前またはシリアル番号を編集することはできません。
   - アクティブ状態のクラスタは削除できません。
   - CSP デバイスをさらに追加します（最大 8 つ）。

ステップ 4 [Save Cluster] をクリックします。

CSP デバイスのクラスタへの追加

Cisco SD-WAN Manager を使用して、CSP デバイスを追加および設定できます。

始める前に

使用する Cisco NFVIS バージョンがクラスタ内のすべての CSP デバイスで同じであることを確認してください。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]** を選択します

ステップ 2 目的のクラスタの […] をクリックし、[Add/Delete CSP] を選択します。

ステップ 3 CSP デバイスを追加するには、[+ Add CSP] をクリックします。[Add CSP] ダイアログボックスが表示されます。名前を入力し、CSP デバイスのシリアル番号を選択します。[Save] をクリックします。

ステップ 4 CSP デバイスを構成するには、CSP ボックスの CSP アイコンをクリックします。[Edit CSP] ダイアログボックスが表示されます。名前を入力し、CSP デバイスのシリアル番号を選択します。[Save] をクリックします。

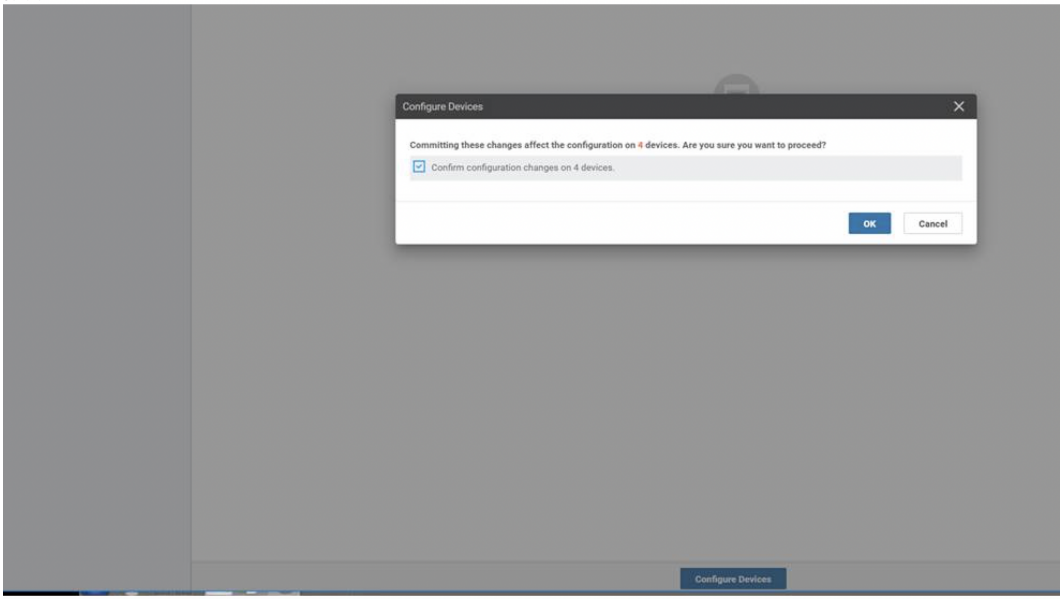
名前には、128 文字の英数字を含めることができます。

（注） CSP デバイスを起動するには、デバイスの OTP を設定してください。

図 *6 : CSP* デバイスの追加

ステップ 5 [Save] をクリックします。

ステップ 6 保存後、次の図に示すように、画面上の構成手順を実行します。



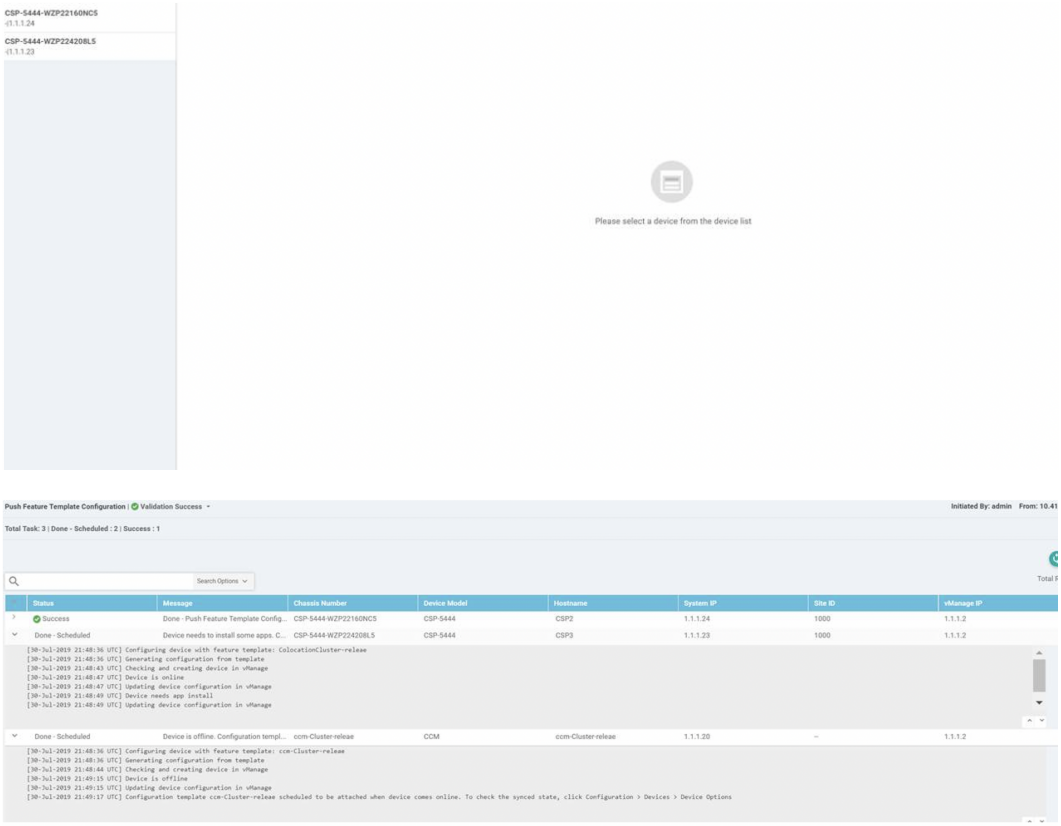
ステップ 7 CSP デバイスが追加されているかどうかを確認するには、実行中のすべてのタスクのリストを表示する [Task View] ウィンドウを使用します。

クラスタからの CSP デバイスの削除

Cisco SD-WAN Manager を使用して CSP デバイスを削除できます。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]** を選択します
ステップ 2 目的のクラスタの […] をクリックし、[Add/Delete CSP] を選択します。
ステップ 3 CSP デバイスを削除するには、[Appliances] ボックスから [CSP] アイコンをクリックします。
ステップ 4 [Delete] をクリックします。
ステップ 5 **[Save]** をクリックします。
ステップ 6 次の図に示すように、画面上の指示に従って削除を続行します。



ステップ 7 CSP 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。

ステップ 8 無効な CSP デバイスをデコミッションするには、Cisco SD-WAN Manager のメニューから **[Configuration]** > **[Devices]** を選択します。

ステップ 9 非アクティブ化されたクラスタにある CSP デバイスについては、[...] をクリックし、[Decommission WAN Edge] を選択します。

このアクションにより、デバイスに新しいトークンが提供されます。

削除された CSP デバイスに HA サービスチェーンが展開されている場合、対応する HA サービスチェーンは、HA インスタンスをホストする CSP デバイスから削除されます。

Cisco Colo Manager がある CSP の削除

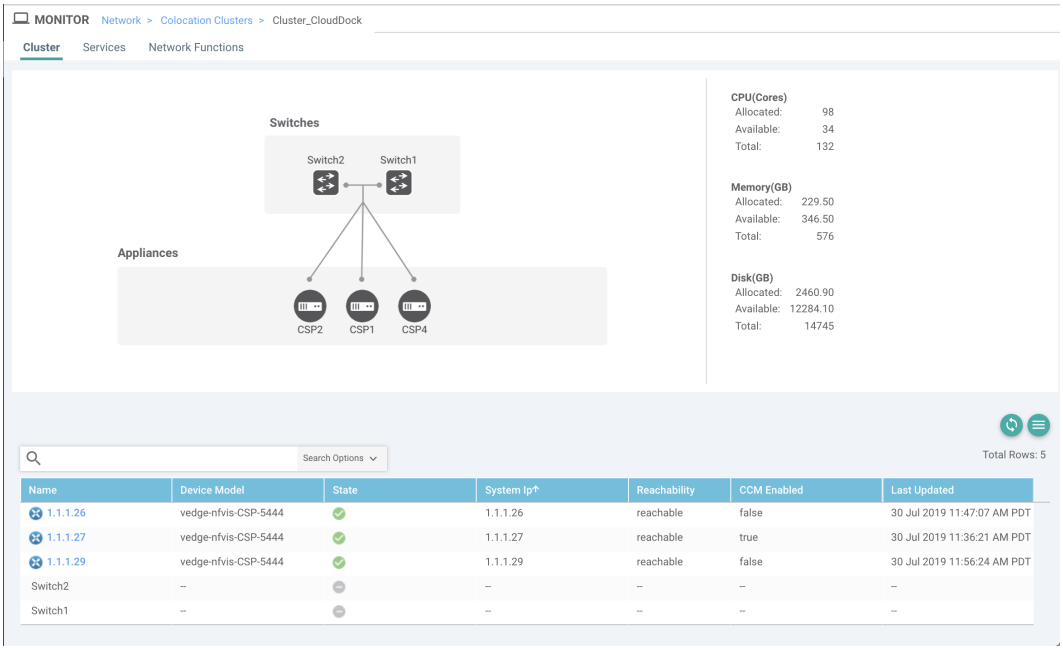
手順

ステップ 1 Cisco Colo Manager をホストする CSP デバイスを特定します。

ステップ 2 CSP デバイスで [CCM Enabled] が true であり、この CSP デバイスを削除することにした場合は、そのデバイスで [...] をクリックし、[Add/Delete CSP] を選択します。

[Monitor] ウィンドウから、Cisco Colo Manager が有効になっているかどうかを確認できます。次の図は、Cisco Colo Manager ステータスを表示できる場所を示しています。

図 *7 : Cisco Colo Manager* を使用する *CSP* デバイス



クラスタから削除することを選択した CSP デバイスでサービスチェーンのモニタリングサービスと Cisco Colo Manager が実行されている場合は、クラスタの [Sync] をクリックしてください。同期ボタンをクリックすると、別の CSP デバイスでサービスチェーンのヘルスモニタリング サービスが開始され、既存のサービスチェーンのヘルスモニタリングが続行されます。

別の CSP デバイスで Cisco Colo Manager インスタンスを起動できるように、Cisco SD-WAN Manager にクラスタのすべての CSP デバイスへの制御接続があることを確認します。

（注） Cisco vManage リリース 20.8.1 以前のリリースでは、Cisco Colo Manager インスタンスをホストしている CSP デバイスを削除した場合、CSP デバイスを追加して、1 つ以上の CSP デバイスで Cisco Colo Manager インスタンスを起動する必要があります。

Cisco Colo Manager がある CSP デバイスを削除すると、Cisco Colo Manager インスタンスはクラスタ上の別の CSP デバイスで開始されます。

（注） サービスチェーンのモニタリングは、残りの CSP デバイスのいずれかで Cisco Colo Manager インスタンスが開始されなくなるまで無効になります。

RMA 後の Cisco CSP デバイスの交換

手順の概要

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]** を選択します
2. 目的のクラスタの […] をクリックし、[RMA] を選択します。
3. [RMA] ダイアログボックスで次の操作を行います。

手順の詳細

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]** を選択します

ステップ 2 目的のクラスタの […] をクリックし、[RMA] を選択します。

ステップ 3 [RMA] ダイアログボックスで次の操作を行います。

a) アプライアンスの選択：交換する CSP デバイスを選択します。

特定のコロケーションクラスタ内のすべての CSP デバイスは、CSP Name-<Serial Number> の形式で表示されます。

b) ドロップダウンリストから新しい CSP デバイスのシリアル番号を選択します。

c) [Save] をクリックします。

保存後、構成を表示できます。

Cisco CSP デバイスの返却

表 *22 :* 機能の履歴

機能名	リリース情報	説明
Cisco CSP デバイスの RMA 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	この機能を使用すると、デバイスのバックアップコピーを作成し、交換用デバイスを交換前の状態に復元することで、障害のある CSP デバイスを交換できます。HA モードで実行されている VM は、デバイスの交換中に中断されることなくトラフィックの継続的なフローで動作します。

バックアップコピーを作成し、NFVIS 構成と VM を復元できるようになりました。

考慮すべき点

- ネットワーク ファイル ストレージ（NFS）サーバーを使用して、CSP デバイスの定期的なバックアップコピーを作成できます。
- バックアップ操作に外部 NFS サーバーを使用している場合は、NFS ディレクトリを定期的に保守およびクリーニングしてください。このメンテナンスにより、NFS サーバーに受信バックアップパッケージ用の十分なスペースが確保されます。
- NFS サーバーを使用しない場合は、Cisco SD-WAN Manager を使用してバックアップサーバー設定を構成しないでください。ただし、バックアップサーバー設定を構成していない場合、交換用デバイスを復元することはできません。CSP の削除を使用して、障害のあるデバイスを削除し、新しい CSP デバイスを追加してから、追加された CSP デバイスへのサービスチェーンのプロビジョニングを開始できます。

Cisco CSP デバイスの RMA プロセス

Return of Materials（RMA）プロセスは、次の順序で実行してください。

1. Cisco SD-WAN Manager を使用して、クラスタ内のすべての CSP デバイスのバックアップコピーを作成します。『バックアップサーバー設定（70ページ）』を参照してください。

（注） CSP デバイスの交換時、Cisco SD-WAN Manager を使用してクラスタを作成するときに NFS サーバーにデバイスのバックアップコピーを作成します。クラスタを起動する場合、または既存のクラスタを編集する場合は、次のいずれかを実行します。

- コロケーションクラスタの起動：クラスタの作成時およびアクティブ化時に、NFS ストレージサーバーとバックアップ間隔に関する情報を指定します。CSP デバイスでバックアップタスクが失敗した場合、デバイスはエラーを返しますが、クラスタのアクティブ化は続行されます。障害に対処した後でクラスタを更新し、クラスタが正常にアクティブ化されるまで待機してください。
- コロケーションクラスタの編集：既存のアクティブクラスタの場合、クラスタを編集し、NFS ストレージサーバーとバックアップ間隔に関する情報を指定します。

2. シスコテクニカルサポートに連絡して、交換用の CSP デバイスを入手してください。CSP デバイスの交換の詳細については、『Cisco Cloud Services Platform 5000 Hardware Installation Guide』を参照してください。
3. 交換用 Cisco CSP デバイスを Cisco Catalyst 9500 スイッチに再配線して、障害のあるデバイスの配線を交換用デバイスに移動します。
4. 交換用デバイスで実行されている Cisco CSP ISO イメージが、障害のあるデバイスで実行されていたものと同じであることを確認します。
5. CLI を使用して交換用デバイスを復元します。

CSP デバイスのバックアップと復元の前提条件と制限事項

前提条件

バックアップ操作

- Cisco SD-WAN Manager を使用してバックアップサーバー設定を構成する前に、CSP デバイスから NFS サーバーへの接続を確立する必要があります。
- NFS サーバー上のバックアップディレクトリには、書き込み権限が必要です。
- 外部 NFS サーバーは、利用可能で、到達可能であり、メンテナンスされている必要があります。外部 NFS サーバーのメンテナンスでは、利用可能なストレージスペースとネットワークの到達可能性を定期的にチェックする必要があります。
- バックアップ操作のスケジュールは、CSPデバイスのローカルの日時と同期する必要があります。

復元操作

- 交換用デバイスには、障害のあるデバイスと同じリソースが必要です。これらのリソースは、障害のあるCSPデバイスとしてのCisco NFVISイメージバージョン、CPU、メモリ、およびストレージです。
- 交換用デバイスとスイッチポート間の接続は、障害のあるデバイスおよびスイッチと同じである必要があります。
- 交換用デバイスの PNIC 配線は、Catalyst 9500 スイッチの障害のあるデバイスと一致する必要があります。

  次に例を示します。

  障害のあるデバイスのスロット 1/ポート 1（eth1-1）がスイッチ 1 およびポート 1/0/1 に接続されている場合は、交換用デバイスのスロット 1/ポート 1（eth1-1）を、スイッチ 1 およびポート 1/0/1 などの同じスイッチポートに接続します。
- 交換用デバイスのオンボーディングは、CSPデバイスのPnPプロセスを使用して完了する必要があります。
- 復元操作中にバックアップアクセスが失われるのを防ぐには、NFSサーバーをマウントしてバックアップパッケージにアクセスするための構成が、障害のあるデバイスの構成と一致している必要があります。

  NFS マウントの場所と構成はすべての CSP デバイスで同じであるため、他の CSP デバイスから構成情報を表示できます。正常な CSP デバイスで実行されているアクティブな構成を表示するには、**show running-config** コマンドを使用します。 復元操作中にマウントポイントを作成するときに、このアクティブな構成情報を使用します。

  次に例を示します。

```
nfvis# show running-config mount
mount nfs-mount storage nfsfs/
storagetype            nfs
```

```
storage_space_total_gb 123.0
server_ip              172.19.199.199
server_path            /data/colobackup/
!
```

- 交換デバイスの復元後に、OTP プロセスを使用した Cisco SD-WAN 制御コンポーネントによる交換デバイスの認証を完了する必要があります。

（注） **request activate chassis-number** *chassis-serial-number* **token** *token-number* コマンドを使用して、Cisco NFVIS にログインしてデバイスを認証します。

- 交換用デバイスには、障害のあるデバイスの構成以外の構成を含めないでください。

制約事項

バックアップ操作

- CSP デバイスのアップグレード中に、定期的なバックアップ操作は開始されません。
- NFS フォルダパスが NFS サーバーで使用できない場合、バックアップ操作は開始されません。
- 特定の時間に実行できるバックアップ操作は 1 つだけです。
- NFS サーバーで使用可能なディスク容量が VM エクスポートサイズと tar.gz VM パッケージの合計サイズより小さい場合、バックアップ操作は失敗します。
- バックアップデバイス情報は、交換用の CSP デバイスでのみ復元でき、すでにクラスタの一部である既存のデバイスでは復元できません。
- NFS マウント構成は、CSP デバイス用に構成した後は更新できません。更新するには、NFS 構成を削除し、更新された構成を NFS サーバーに再適用して、バックアップスケジュールを再構成します。バックアップ操作が進行中でないときに、この更新を実行します。

復元操作

- 特定の時間に実行できる復元操作は 1 つだけです。
- バックアップファイルが NFS サーバーに存在しない場合、復元操作は開始されません。
- クラスタをシングルテナントモードからマルチテナントモードに変換する場合、およびその逆の場合、復元操作はサポートされません。

クラスタの削除

Cisco SD-WAN Manager からクラスタ全体をデコミッションするには、次の手順を実行します。

手順

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

ステップ 2 削除する CSP デバイスの [Validate] 列を確認し、[Invalid] をクリックします。

ステップ 3 無効なデバイスについては、[Send to Controllers] をクリックします。

ステップ 4 Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]**を選択します。

ステップ 5 無効な CSP デバイスがあるクラスタの場合は、[...] をクリックし、[Deactivate] を選択します。

クラスタが 1 つ以上のサービスグループに接続されている場合、CSP デバイスで実行されている VM をホストしているサービスチェーンと、クラスタの削除を続行できるかどうかを示すメッセージが表示されます。ただし、クラスタの削除を確認しても、この CSP デバイスでホストされているサービスグループを切り離さずにクラスタを削除することはできません。クラスタがどのサービスグループにも関連付けられていない場合は、クラスタの削除に関する確認を求めるメッセージが表示されます。

（注） 必要に応じて、クラスタを削除するか、非アクティブ状態のままにすることができます。

ステップ 6 クラスタを削除するには、[Delete] を選択します。

ステップ 7 クラスタを削除しない場合は、[Cancel] をクリックします。

ステップ 8 無効なデバイスをデコミッションするには、Cisco SD-WAN Manager のメニューから **[Configuration]** > **[Devices]** を選択します。

ステップ 9 非アクティブ化されたクラスタにあるデバイスについては、[...] をクリックし、[Decommission WAN Edge] を選択します。

このアクションにより、デバイスに新しいトークンが提供されます。

ステップ 10 次のコマンドを使用して、デバイスを工場出荷時のデフォルトにリセットします。

factory-default-reset all

ステップ 11 ログイン名として **admin** を使用し、デフォルトのパスワードとして **Admin123#** を使用して、Cisco NFVIS にログインします。

ステップ 12 スイッチ構成をリセットし、スイッチをリブートします。『Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide』の「Troubleshooting」の章を参照してください。

クラスタの再アクティブ化

新しい CSP デバイスを追加する場合、または CSP デバイスが RMA プロセスの対象となる場合は、次の手順を実行します。

手順

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

ステップ 2 非アクティブ化されたクラスタにあるデバイスを見つけます。

ステップ 3 デバイス用に Cisco SD-WAN Manager から新しいトークンを取得します。

ステップ 4 ログイン名として **admin** を使用し、デフォルトのパスワードとして **Admin123#** を使用して、Cisco NFVIS にログインします。

ステップ 5 **request activate chassis-number** *chassis-serial-number* **token** *token-number* コマンドを使用します。

ステップ 6 Cisco SD-WAN Manager を使用して、コロケーションデバイスを設定し、クラスタをアクティブ化します。『クラスタの作成とアクティブ化 （60 ページ）』を参照してください。

クラスタを削除した場合は、再作成してからアクティブ化します。

ステップ 7 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Certificates]** の順に選択します。コロケーションデバイスのステータスを見つけて確認します。

ステップ 8 有効にする必要がある目的のデバイスの [Valid] をクリックします。

ステップ 9 有効なデバイスについては、[Send to Controllers] をクリックします。

サービス グループの管理

サービスグループは、1 つ以上のサービスチェーンで構成されます。Cisco SD-WAN Manager を使用してサービスグループを設定できます。サービスチェーンはネットワークサービスの構造であり、リンクされたネットワーク機能のセットで構成されます。

サービスグループでのサービスチェーンの作成

サービスグループは、1 つ以上のサービスチェーンで構成されます。

表 *23 :* 機能の履歴

機能名	リリース情報	機能説明
サービスチェーンの正常性の監視	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b	この機能により、サービスチェーンデータパスの定期的なチェックを設定し、全体的なステータスをレポートできます。サービスチェーンのヘルスモニタリングを有効にするには、クラスタ内のすべての CSP デバイスに NFVIS バージョン 3.12.1 以降をインストールする必要があります。

手順

Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]** を選択します

a) [Service Group] をクリックし、[Create Service Group] をクリックします。サービスグループの名前、説明、およびコロケーショングループを入力します。

サービスグループ名には、128 文字の英数字を含めることができます。

サービスグループの説明には、2048 文字の英数字を含めることができます。

マルチテナントクラスタの場合、ドロップダウンリストからコロケーショングループまたはテナントを選択します。シングルテナントクラスタの場合、コロケーショングループ [admin] がデフォルトで選択されます。

b) [Add Service Chain] をクリックします。

c) [Add Service Chain] ダイアログボックスで、次の情報を入力します。

表 *24 :* サービスチェーン情報の追加

フィールド	説明
Name	サービスチェーン名には、128 文字の英数字を含めることができます。
Description	サービスチェーンの説明には、2048 文字の英数字を含めることができます。
Bandwidth	サービスチェーンの帯域幅は Mbps 単位です。デフォルトの帯域幅は 10 Mbps で、5 Gbps の最大帯域幅を設定できます。
Input Handoff VLANS and Output Handoff VLANS	入力 VLAN ハンドオフおよび出力 VLAN ハンドオフは、カンマ区切りの値（10、20）、または 10 ～ 20 の範囲にすることができます。

フィールド	説明
Monitoring	サービスチェーンのヘルスモニタリングを有効または無効にできるトグルボタン。サービスチェーンのヘルスモニタリングは、サービスチェーンデータパスの正常性をチェックし、サービスチェーン全体の正常性ステータスを報告する定期的なモニタリングサービスです。デフォルトでは、モニタリングサービスは無効になっています。 SCHM（サービスチェーンヘルスモニタリングサービス）などのサブインターフェイスを持つサービスチェーンは、サブインターフェイス VLAN リストの最初の VLAN を含むサービスチェーンのみをモニタリングできます。 サービスチェーンのモニタリングは、エンドツーエンドの接続に基づいてステータスを報告します。したがって、より良い結果を得るために、Cisco Catalyst SD-WAN サービスチェーンに注意しながら、ルーティングとリターントラフィックパスを処理するようにしてください。 （注） • 入力および出力ハンドオフサブネットからの入力および出力モニタリング IP アドレスが指定されていることを確認します。ただし、最初と最後の VNF デバイスが VPN で終端されている場合、入力および出力モニタリング IP アドレスを指定する必要はありません。 たとえば、ネットワーク機能が VPN 終端されていない場合、入力モニタリング IP はインバウンドサブネット 192.0.2.0/24 からの 192.0.2.1/24 である可能性があります。インバウンドサブネットは最初のネットワーク機能に接続し、出力モニタリング IP はアウトバウンドサブネットからの 203.0.113.11/24、サービスチェーンの最後のネットワーク機能の 203.0.113.0/24 にすることができます。 • サービスチェーンの最初または最後の VNF ファイアウォールがトランスペアレントモードの場合、これらのサービスチェーンをモニタリングすることはできません。
Service Chain	サービスチェーンのドロップダウンリストから選択するトポロジです。サービスチェーントポロジの場合、ルータ - ファイアウォール - ルータ、ファイアウォール、ファイアウォール - ルータなど、検証済みのサービスチェーンのいずれかを選択できます。『Cisco Catalyst SD-WAN Cloud OnRamp Colocation Solution Guide』の「Validated Service Chains」のトピックを参照してください。カスタマイズされたサービスチェーンを作成することもできます。カスタムサービスチェーンの作成 （98 ページ）を参照してください。

d) [Add Service Chain] ダイアログボックスで、[Add] をクリックします。

サービスチェーンの構成情報に基づいて、すべてのサービスチェーンと VNF を含むサービスグループのグラフィック表現が、デザインビューウィンドウに自動的に表示されます。VNF または PNF は、仮想および物理ネットワーク機能の周囲に「V」または「P」が付いて表示されます。各サービスグループ内に構成されているすべてのサービスチェーンが表示されます。サービスチェーンの横にあるチェックマークは、サービスチェーンの構成が完了していることを示します。

クラスタをアクティブ化したら、CCM が実行されている CSP デバイスを起動するときに、クラスタをサービスグループに接続し、サービスチェーンのモニタリングサービスを有効にします。Cisco SD-WAN Manager は、モニタリングサービスを開始するために同じ CSP デバイスを選択します。モニタリングサービスは、モニタリング間隔を 30 分に設定することにより、すべてのサービスチェーンをラウンドロビン方式で定期的にモニタリングします。『Cloud OnRamp Colocation クラスタのモニター （127 ページ）』を参照してください。

e) デザインビューウィンドウで、VNF を構成するには、サービスチェーン内の VNF をクリックします。[Configure VNF] ダイアログボックスが表示されます。

f) 次の情報を使用して VNF を構成し、必要に応じてアクションを実行します。

（注） Cisco vManage リリース 20.7.1 以降では次のフィールドを使用できます。

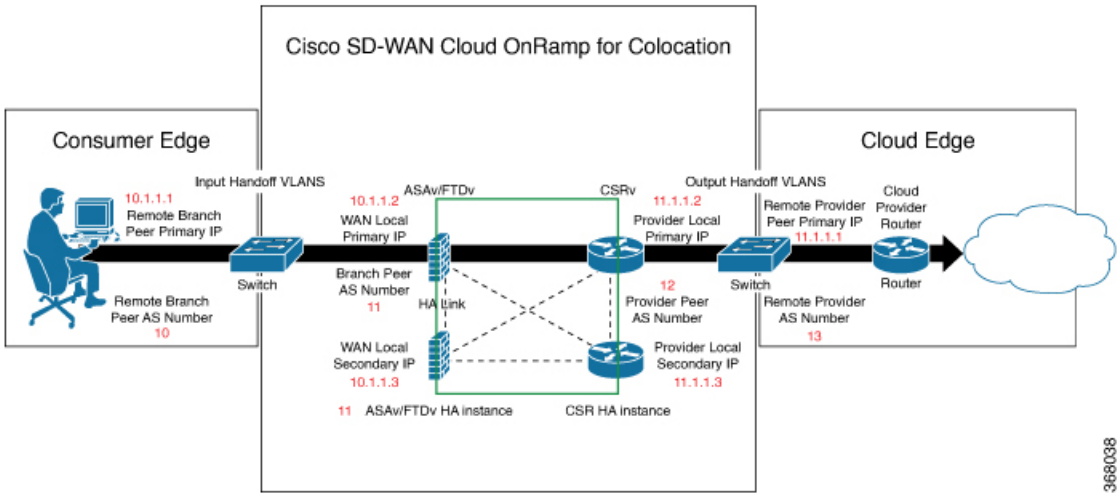
- Disk Image/Image Package (Select File)
- Disk Image/Image Package (Filter by Tag, Name and Version)
- Scaffold File (Select File)
- Scaffold File (Filter by Tag, Name and Version)

表 *25 :* ルータとファイアウォールの *VNF* プロパティ

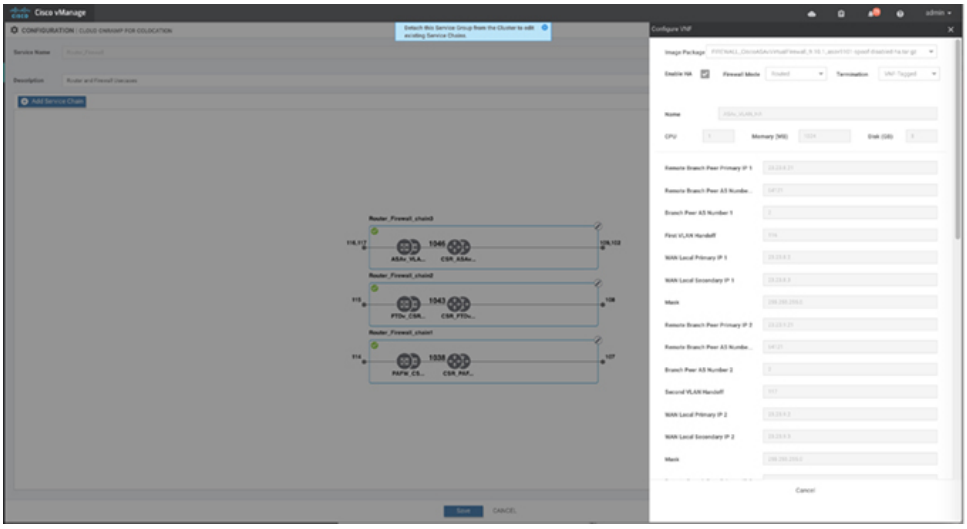
フィールド	説明
Image Package	ルータ、ファイアウォールパッケージを選択します。
Disk Image/Image Package (Select File)	tar.gz パッケージまたは qcow2 イメージファイルを選択します。
Disk Image/Image Package (Filter by Tag, Name and Version)	（オプション）VNF イメージのアップロード時に指定した名前、バージョン、タグに基づいて、イメージまたはパッケージファイルをフィルタリングします。

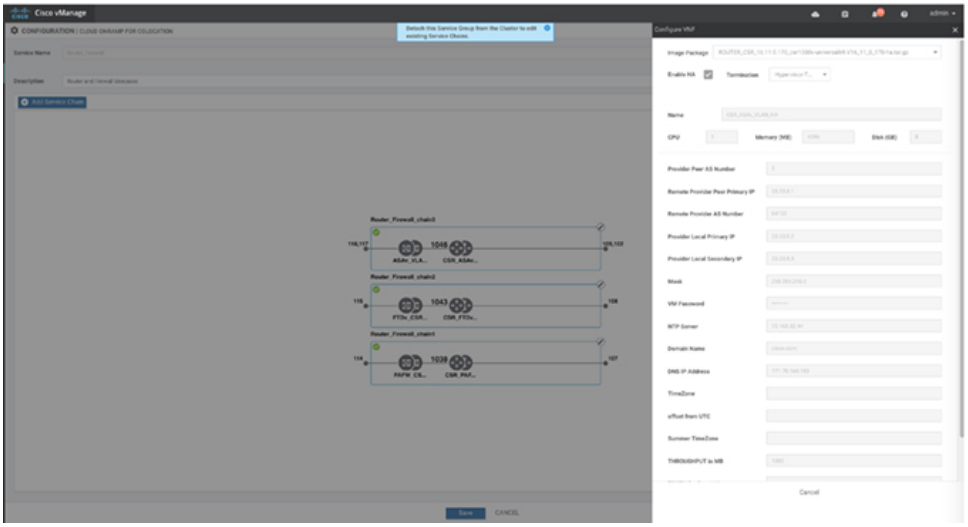
フィールド	説明
Scaffold File (Select File)	スキャフォールドファイルを選択します。 （注） • qcow2 イメージファイルが選択されている場合、このフィールドは必須です。tar.gzパッケージが選択されている場合はオプションです。 • tar.gz パッケージとスキャフォールドファイルの両方を選択した場合、スキャフォールドファイルのすべてのイメージプロパティとシステムプロパティは、tar.gzパッケージで指定されたDay-0 構成ファイルを含むイメージプロパティとシステムプロパティをオーバーライドします。
Scaffold File (Filter by Tag, Name and Version)	（オプション）VNFイメージのアップロード時に指定した名前、バージョン、タグに基づいて、スキャフォールドファイルをフィルタリングします。
[Fetch VNF Properties] をクリックします。イメージの利用可能な情報は、[Configure VNF] ダイアログボックスに表示されます。	
Name	VNF イメージ名
CPU	（オプション）VNF に必要な仮想 CPU の数を指定します。デフォルト値は 1 vCPU です。
Memory	（オプション）VNF が使用できる最大プライマリメモリを MB 単位で指定します。デフォルト値は 1024 MB です。
Disk	（オプション）VM に必要なディスクを GB 単位で指定します。デフォルト値は 8 GB です。
入力が必要な、Day-0 からのカスタムトークン化変数を含むダイアログボックスが表示されます。値を指定します。	

次の図で、緑色のボックス内のすべての IP アドレス、VLAN、および自律システムは、VLAN から生成されたシステム固有の情報、クラスタに提供される IP プールです。この情報は、VM の Day-0 構成に自動的に追加されます。



次の図は、Cisco SD-WAN Manager での VNF IP アドレスと自律システム番号の設定例です。





マルチテナントクラスタと共同管理シナリオを使用している場合は、サービスチェーン設計の必要に応じて、次のフィールドと残りのフィールドに値を入力して、Cisco Catalyst SD-WAN VM を設定します。

（注） テナント オーバーレイ ネットワークに参加するには、プロバイダーは次のフィールドに正しい値を指定する必要があります。

フィールド	説明
Serial Number	Cisco Catalyst SD-WAN デバイスの承認済みシリアル番号。サービスプロバイダーは、サービスチェーンを作成する前に、テナントからデバイスのシリアル番号を取得できます。
OTP	Cisco SD-WAN 制御コンポーネントで認証された後に使用できる Cisco Catalyst SD-WANデバイスのOTP。サービスプロバイダーは、サービスチェーンを作成する前に、テナントから対応するシリアル番号の OTP を取得できます。
Site Id	ブランチ、キャンパス、データセンターなど、Cisco Catalyst SD-WAN デバイスが存在するテナント Cisco Catalyst SD-WAN オーバーレイ ネットワーク ドメイン内のサイトの識別子。サービスプロバイダーは、サービスチェーンを作成する前に、テナントからサイト ID を取得できます。
Tenant ORG Name	証明書署名要求（CSR）に含まれるテナント組織名。サービスプロバイダーは、サービスチェーンを作成する前に、テナントから組織名を取得できます。
System IP connect to Tenant	テナント オーバーレイ ネットワークに接続するための IP アドレス。サービスプロバイダーは、サービスチェーンを作成する前にテナントからIPアドレスを取得できます。
Tenant vBond IP	テナント Cisco SD-WAN Validator の IP アドレス。サービスプロバイダーは、サービスチェーンを作成する前にテナントから Cisco SD-WAN Validator IP アドレスを取得できます。

サービスチェーンの最初と最後の VM などのエッジ VM の場合、ブランチルータおよびプロバイダールータとピアリングするときに、次のアドレスを指定する必要があります。

表 *26*：サービスチェーンの最初の *VM* の *VNF* オプション

フィールド	必須または任意	説明
Firewall Mode	必須	ルーテッドモードまたはトランスペアレントモードを選択します。 （注） ファイアウォールモードは、ファイアウォールVMにのみ適用されます。
Enable HA	オプション	VNF の HA モードを有効にします。

フィールド	必須または任意	説明

Termination	必須	次のいずれかのモードを選択します。
		• トランクモードのサブインターフェイスでの L3 モードの選択
		`<type>selection</type> <val help="L3 Mode With Sub-interfaces(Trunked)" display="VNF-Tagged">vlan</val>`
		• コンシューマ側からの IPSEC 終端を使用し、プロバイダーゲートウェイに再ルーティングされる L3 モード
		`<val help="L3 Mode With IPSEC Termination From Consumer and Routed to Provider GW" display="Tunneled">vpn</val>`
		• アクセスモードでの L3 モード（非トランクモード）
		`<val help="L3 Mode In Access Mode (Non-Trunked)" display="Hypervisor-Tagged">routed</val>`

g) [Configure] をクリックします。サービスチェーンは VNF 構成で構成されます。
h) 別のサービスチェーンを追加するには、手順 b ～ g を繰り返します。
i) [Save] をクリックします。

[Service Group] の下のテーブルに新しいサービスグループが表示されます。モニタリングされているサービスチェーンのステータスを表示するには、[Task View] ウィンドウを使用します。このウィンドウには、実行中のすべてのタスクのリストと、成功と失敗の合計数が表示されます。サービスチェーンの正常性ステータスを確認するには、サービスチェーンのヘルスモニタリングが有効になっている CSP デバイスで **show system:system status** コマンドを使用します。

サービスチェーンの QoS

表 *27 :* 機能の履歴

機能名	リリース情報	説明
サービスチェーンの QoS	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	この機能は、レイヤ 2 仮想ローカルエリアネットワーク（VLAN）識別番号に基づいてネットワークトラフィックを分類します。QoS ポリシーを使用すると、双方向トラフィックにトラフィックポリシングを適用することにより、各サービスチェーンで使用可能な帯域幅を制限できます。双方向トラフィックは、Cisco Catalyst 9500-40X スイッチをコンシューマに接続する入力側とプロバイダーに接続する出力側です。

前提条件

• 共有 VNF および PNF デバイスを持たないサービスチェーンで、サービス品質（QoS）トラフィックポリシングを使用していることを確認します。

（注） 複数のサービスチェーンで入力 VLAN と出力 VLAN が同じである共有 VNF デバイスを持つサービスチェーンに QoS ポリシーを適用することはできません。

- QoS トラフィックポリシングに次のバージョンのソフトウェアを使用していることを確認してください。

ソフトウェア	リリース
Cisco NFVIS Cloud OnRamp for Colocation	4.1.1 以降
Catalyst 9500-40X	16.12.1 以降

QoS ポリシングポリシーは、次のワークフローに基づいてネットワークトラフィックに適用されます。

1. Cisco SD-WAN Manager は、帯域幅、入力、または出力 VLAN 情報を VNF および PNF デバイスに保存します。帯域幅と VLAN 情報を提供するには、サービスグループでのサービスチェーンの作成 （87 ページ）を参照してください。
2. CCM は、帯域幅、入力、または出力 VLAN 値の情報を Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチに保存します。
3. CCM は、VLAN 一致基準に基づいて、Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチに対応するクラスマップおよびポリシーマップを作成します。
4. CCM は、入力ポートと出力ポートに入力サービスポリシーを適用します。

（注） Cisco vManage リリース 20.7.1 以降、サービスチェーンの QoS トラフィックポリシーは、Cisco Catalyst 9500 スイッチではサポートされていません。

- アクティブクラスタが Cisco vManage リリース 20.7.1 および CSP 4.7.1 にアップグレードされ、アップグレード前にプロビジョニングされたサービスチェーンがある場合、アップグレード中に QoS 設定がスイッチから自動的に削除されます。
- Cisco vManage リリース 20.7.1 で新しいサービスチェーンがプロビジョニングされると、QoS ポリシーはスイッチに設定されません。
- 同様に、Cisco vManage リリース 20.7.1 で作成された新しいクラスタは、スイッチのサービスチェーンの QoS 設定を構成しません。

サービスグループの複製

表 *28 :* 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN Manager のサービスグループの複製	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能を使用すると、同じ設定情報を何度も入力することなく、さまざまな RBAC ユーザーのサービスグループのコピーを作成できます。サービスグループを複製すると、保存されているサービスチェーンテンプレートを利用してサービスチェーンを簡単に作成できます。

サービスチェーンのコピーを複製または作成するときは、次の点に注意してください。

- Cisco SD-WAN Manager は、複製されたサービスグループがクラスタに接続されているかどうかに関係なく、サービスグループのすべての構成情報を複製されたサービスグループにコピーします。
- CSV ファイルを確認し、CSV ファイルのアップロード中に構成情報に一致するサービスグループ名があることを確認します。これを行わないと、サービスグループ名が一致しない場合に CSV ファイルのアップロード中にエラーメッセージが表示される可能性があります。
- サービスグループの設定値の更新されたリストを取得するには、常にサービスグループのデザインビューからサービスグループの構成プロパティをダウンロードします。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]** を選択します

ステップ 2 [Service Group] をクリックします。
サービスグループの構成ページが表示され、すべてのサービスグループが表示されます。

ステップ 3 目的のサービスグループの […] をクリックし、[Clone Service Group] を選択します。

元のサービスグループのクローンがサービスグループのデザインビューに表示されます。次の点に注意してください。

- デフォルトでは、複製されたサービスグループ名と VM 名には、一意の文字列がサフィックスとして付けられます。
- VM 構成を表示するには、サービスチェーン内の VM をクリックします。
- Cisco SD-WAN Manager は、構成が必要なサービスチェーンを、サービスチェーンの編集ボタンの横に [Unconfigured] としてマークします。

ステップ 4 必要に応じてサービスグループ名を変更します。サービスグループの説明を入力します。

ステップ 5 サービスチェーンを構成するには、次のいずれかの方法を使用します。

- サービスチェーンの編集ボタンをクリックし、値を入力して、[Save] をクリックします。
- CSV ファイルから設定値をダウンロードし、値を変更してファイルをアップロードし、[Save] をクリックします。CSV ファイルをダウンロード、変更、およびアップロードする方法については、ステップ 6、7、8 を参照してください。

複製されたサービスグループは、サービスグループの構成ページに表示されます。更新されたサービスグループの設定値をダウンロードできるようになりました。

ステップ 6 複製されたサービスグループの設定値をダウンロードするには、次のいずれかを実行します。

（注） CSV ファイルのダウンロードとアップロードは、クラスタに接続されていないサービスグループの作成、編集、および複製のためにサポートされています。

- サービスグループの構成ページで、複製されたサービスグループをクリックし、サービスグループの右側にある [More Actions] をクリックして、[Download Properties (CSV)] を選択します。
- サービスグループのデザインビューで、画面の右上隅にある [Download CSV] をクリックします。

Cisco SD-WAN Manager は、サービスグループのすべての設定値を CSV 形式の Excel ファイルにダウンロードします。CSV ファイルは複数のサービスグループで構成でき、各行は 1 つのサービスグループの設定値を表します。CSV ファイルに行を追加するには、既存の CSV ファイルからサービスグループの設定値をコピーして、このファイルに貼り付けます。

たとえば、各サービスチェーンに 1 つの VM を持つ 2 つのサービスチェーンがある ServiceGroup1_Clone1 は、1 つの行で表されます。

（注） Excel ファイルのサービス チェーン デザイン ビューでのヘッダーとその表現は次のとおりです。

- sc1/name は、最初のサービスチェーンの名前を表します。
- sc1/vm1/name は、最初のサービスチェーンの最初の VNF の名前を表します。
- sc2/name は、2 番目のサービスチェーンの名前を表します。
- sc2/vm2/name は、2 番目のサービスチェーンの 2 番目の VNF の名前を表します。

ステップ 7 サービスグループの設定値を変更するには、次のいずれかを実行します。

- デザインビューでサービスグループ構成を変更するには、サービスグループ構成ページで複製されたサービスグループをクリックします。

  サービスチェーン内の任意の VM をクリックして設定値を変更し、[Save] をクリックします。

- ダウンロードした Excel ファイルを使用してサービスグループ構成を変更するには、Excel ファイルに設定値を手動で入力します。Excel ファイルを CSV 形式で保存します。

ステップ 8 サービスグループのすべての設定値を含む CSV ファイルをアップロードするには、サービスグループ構成ページでサービスグループをクリックし、画面の右隅にある [Upload CSV] をクリックします。

[Browse] をクリックして CSV ファイルを選択し、[Upload] をクリックします。

サービスグループ構成に表示される更新された値を表示できます。

（注） 同じCSVファイルを使用して、複数のサービスグループの設定値を追加できます。ただし、Cisco SD-WAN Manager を使用して CSV ファイルをアップロードする場合、特定のサービスグループの設定値のみを更新できます。

ステップ 9 CSV ファイルおよび Cisco SD-WAN Manager デザインビューでのサービスグループ構成プロパティの表現を確認するには、サービスグループ構成ページでサービスグループをクリックします。

[Show Mapping Names] をクリックします。

サービスチェーン内のすべての VM の横にテキストが表示されます。Cisco SD-WAN Manager は、このテキストを CSV ファイルの構成プロパティにマッピングした後に表示します。

カスタムサービスチェーンの作成

次の方法でサービスチェーンをカスタマイズできます。

- 追加の VNF を含めるか、他の VNF タイプを追加すること。
- 事前定義されたサービスチェーンの一部ではない新しいVNFシーケンスを作成すること。

手順

ステップ 1 サービスグループとサービスグループ内のサービスチェーンを作成します。『サービスグループでのサービスチェーンの作成 （87 ページ）』を参照してください。

ステップ 2 [Add Service Chain] ダイアログボックスで、サービスチェーン名、説明、帯域幅、入力 VLAN ハンドオフ、出力 VLAN ハンドオフ、サービスチェーンの正常性情報の監視、およびサービスチェーン構成を入力します。[Add] をクリックします。

サービスチェーン構成では、ドロップダウンから [Create Custom] を選択します。デザインビューウィンドウに空のサービスチェーンが表示されます。

ステップ 3 ルータ、ロードバランサ、ファイアウォールなどの VNF を追加するには、VNF アイコンをクリックし、アイコンをサービスグループボックス内の適切な場所にドラッグします。必要なすべての VNF を追加し、VNF サービスチェーンを形成したら、各 VNF を構成します。サービスグループボックスで VNF をクリックします。[Configure VNF] ダイアログボックスが表示されます。次のパラメータを入力します。

a) [Disk Image/Image Package]（[Select File]）ドロップダウンリストから、ロードするソフトウェアイメージを選択します。

（注） Cisco vManage リリース 20.7.1 から qcow2 イメージファイルを選択できます。

b) qcow2 イメージファイルを選択した場合は、[Scaffold File]（[Select File]）ドロップダウンリストからスキャフォールドファイルを選択します。

（注） このオプションは、Cisco vManage リリース 20.7.1 から入手できます。

c) 必要に応じて、VNF イメージのアップロード時に指定した名前、バージョン、およびタグに基づいて、イメージ、パッケージファイル、またはスキャフォールドファイルをフィルタリングします。

（注） このオプションは、Cisco vManage リリース 20.7.1 から入手できます。

d) [Fetch VNF Properties] をクリックします。
e) [Name] フィールドに、VNF の名前を入力します。
f) [CPU] フィールドに、VNF に必要な仮想 CPU の数を入力します。
g) [Memory] フィールドに、VNF に割り当てるメモリの量をメガバイト単位で入力します。
h) [Disk] フィールドに、VNF に割り当てるストレージのメモリ量をギガバイト単位で入力します。
i) 必要に応じて、VNF 固有のパラメータを入力します。

（注） これらの VNF の詳細は、VNF の Day-0 オペレーションに必要なカスタム変数です。

j) [Configure] をクリックします。
k) VNF を削除するか、VNF 構成をキャンセルするには、それぞれ [Delete] または [Cancel] をクリックします。

カスタマイズされたサービスチェーンがサービスグループに追加されます。

（注） サービスチェーンで最大 4 つの VNF のみを使用して VNF シーケンスをカスタマイズできます。

共有 PNF デバイスによるカスタムサービスチェーン

サポートされている PNF デバイスを追加して、サービスチェーンをカスタマイズできます。

注意 コロケーションクラスタ間で PNF デバイスを共有しないようにしてください。PNF デバイスは、サービスチェーン間またはサービスグループ間で共有できます。ただし、PNF デバイスは、単一のクラスタ間でのみ共有できるようになりました。

表 *29 :* 機能の履歴

機能名	リリース情報	機能説明
サービスチェーンでの PNF デバイスの管理	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b	この機能を使用すると、仮想ネットワーク機能（VNF）デバイスに加えて、物理ネットワーク機能（PNF）デバイスをネットワークに追加できます。これらの PNF デバイスは、サービスチェーンに追加して、サービスチェーン、サービスグループ、およびクラスタ全体で共有できます。サービスチェーンに PNF デバイスを含めると、サービスチェーンで VNF デバイスのみを使用することによって引き起こされるパフォーマンスとスケーリングの問題を解決できます。

始める前に

検証済みの物理ネットワーク機能の詳細については、『Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide』の「Validated Physical Network Functions」のトピックを参照してください。

ルータまたはファイアウォールを既存のサービスチェーンに追加してカスタマイズされたサービスチェーンを作成するには、次の点に注意してください。

- PNF デバイスを Cisco SD-WAN Manager で管理する必要がある場合は、シリアル番号が Cisco SD-WAN Manager ですでに利用可能であることを確認してください。これにより、PNF 設定時に選択できるようになります。
- FTD デバイスは、サービスチェーンの任意の位置に配置できます。
- ASR 1000 シリーズアグリゲーション サービス ルータは、サービスチェーンの最初と最後の位置にのみ配置できます。
- PNF デバイスは、サービスチェーンおよびサービスグループ全体に追加できます。
- PNF デバイスは、サービスグループ間で共有できます。同じシリアル番号を入力することで、サービスグループ間で共有できます。
- PNF デバイスは、単一のコロケーションクラスタ間で共有できますが、複数のコロケーションクラスタ間で共有することはできません。

手順

ステップ 1 サービスグループとサービスグループ内のサービスチェーンを作成します。『サービスグループでのサービスチェーンの作成 （87 ページ）』を参照してください。

ステップ 2 [Add Service Chain] ダイアログボックスで、サービスチェーン名、説明、帯域幅、入力 VLAN ハンドオフ、出力 VLAN ハンドオフ、サービスチェーンの正常性情報の監視、およびサービスチェーン構成を入力します。[Add] をクリックします。

サービスチェーン構成では、ドロップダウンリストから [Create Custom] を選択します。デザインビューウィンドウに空のサービスチェーンが表示されます。左側に、サービスチェーンに追加できる VNF デバイスと PNF デバイスのセットが表示されます。VNF デバイスの周囲の「V」は VNF を表し、PNF デバイスの周囲の「P」は PNF を表します。

（注） PNF デバイスを共有してサービスチェーンを作成するには、必ず [Create Custom] オプションを選択してください。

ステップ 3 サービスチェーンで物理ルータ、物理ファイアウォールなどの PNF を追加するには、必要な PNF アイコンをクリックし、アイコンをサービスチェーンボックス内の適切な場所にドラッグします。

必要なすべての PNF デバイスを追加したら、それぞれを設定します。

a) サービスチェーンボックスで PNF デバイスをクリックします。

[Configure PNF] ダイアログボックスが表示されます。PNF を設定するには、次のパラメータを入力します。

b) PNF デバイスで HA が有効になっている場合は、[HA Enabled] をチェックします。

c) PNF で HA が有効になっている場合は、HA シリアル番号を [HA Serial] に追加してください。

PNF デバイスが FTD の場合は、次の情報を入力します。

1. [Name] フィールドに、PNF の名前を入力します。
2. [Firewall Mode] として [Routed] または [Transparent] を選択します。
3. [PNF Serial] フィールドに、PNF デバイスのシリアル番号を入力します。

PNF デバイスが ASR 1000 シリーズ アグリゲーション サービス ルータの場合は、次の情報を入力します。

1. デバイスが Cisco SD-WAN Manager によって管理されている場合は、[vManaged] チェックボックスをオンにします。
2. [Fetch Properties] をクリックします。
3. [Name] フィールドに、PNF の名前を入力します。
4. [PNF Serial] フィールドに、PNF デバイスのシリアル番号を入力します。

d) [Configure] をクリックします。

ステップ 4 サービスチェーンを追加して PNF デバイスを共有するには、ステップ 2 から繰り返します。

ステップ 5 既存の PNF 構成を編集するには、PNF をクリックします。

ステップ 6 [Share NF To] ドロップダウンリストで、PNF を共有するサービスチェーンを選択します。

PNF の共有後、PNF にカーソルを合わせると、それぞれの共有 PNF デバイスが青色で強調表示されます。ただし、異なるサービスグループの PNF は青色で強調表示されません。共有する NF を選択すると、青色の縁が表示されます。同じ PNF が複数のサービスチェーンで共有されている場合は、PNF アイコンをドラッグして特定の位置に配置することで、さまざまな位置で使用できます。

図 *8 :* サービスチェーン内の単一の *PNF*

次の図は、単一のPNF、Ftd_Pnf（他のサービスチェーンと共有されない）で構成されるサービスチェーンを示しています。

図 *9 :* サービスチェーン内の *2* つの *PNF* デバイス

次の図は、サービスチェーン 1（SC1）とサービスチェーン 2（SC2）で共有される FTdv_PNF と ASR_PNF（非共有）の 2 つの PNF で構成されるサービスチェーンを示しています。

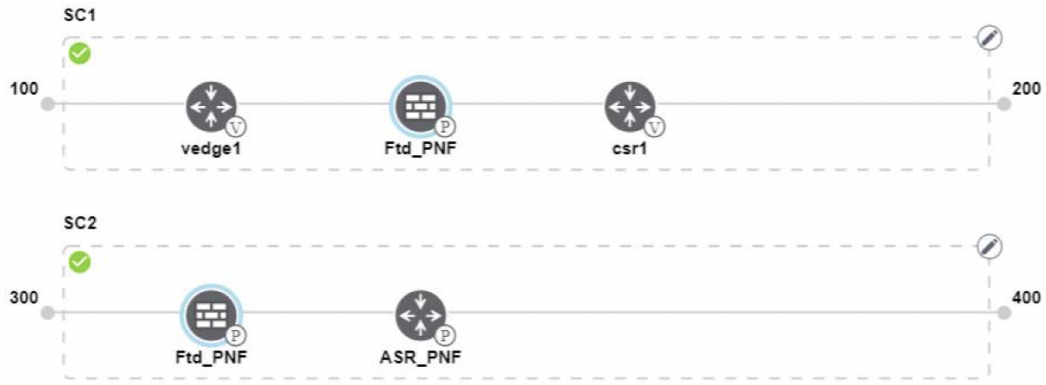
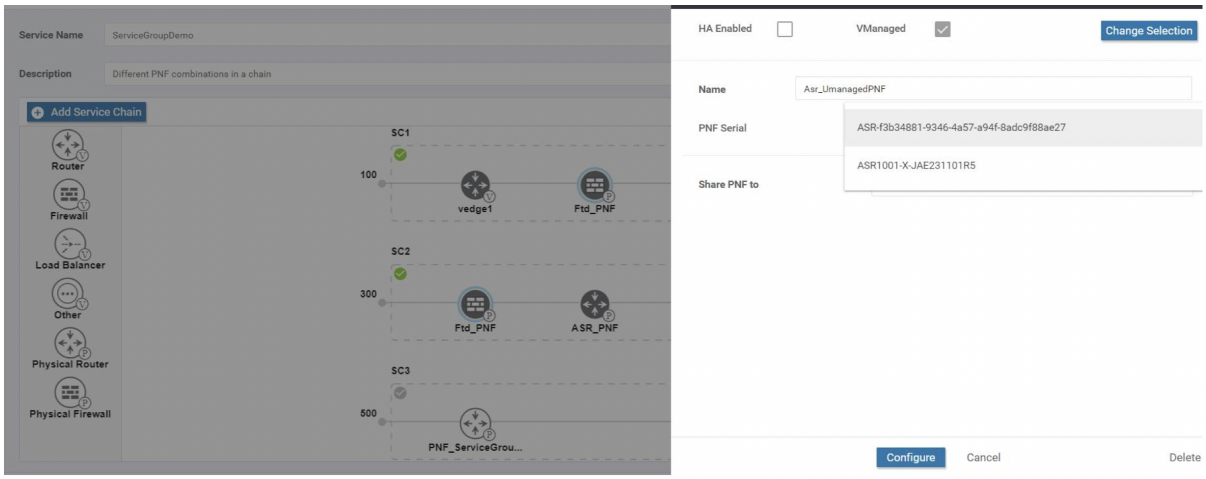


図 *10 :* サービスチェーン内の *3* つの *PNF* デバイス

次の図は、2 つの異なる位置にある 3 つの PNF デバイスで構成されるサービスチェーンと、Cisco SD-WAN Manager 設定を示しています。



ステップ 7 ネットワーク機能構成を削除またはキャンセルするには、それぞれ [Delete] または [Cancel] をクリックします。

サービスグループをコロケーションクラスタに接続する必要があります。PNFデバイスを含むサービスグループを接続した後、VNF デバイスとは異なり、PNF 構成は PNF デバイスに自動的にプッシュされません。代わりに、[Monitor] ウィンドウで生成された構成に注意して、PNF デバイスを手動で構成する必要があります。Cloud OnRamp Colocation クラスタのモニター（127 ページ）VLAN は、Cisco Catalyst 9500-40X スイッチデバイスでも構成する必要があります。特定の PNF 構成の詳細については、『ASR 1000 Series Aggregation Services Routers Configuration Guides』および『Cisco Firepower Threat Defense Configuration Guides』を参照してください。

共有 VNF デバイスによるカスタムサービスチェーン

サポートされている VNF デバイスを含めることで、サービスチェーンをカスタマイズできます。

表 *30* : 機能の履歴

機能名	リリース情報	機能説明
サービスチェーン全体で VNF デバイスを共有する	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b	この機能により、サービスチェーン全体で仮想ネットワーク機能（VNF）デバイスを共有して、リソースの使用率を向上させ、リソースの断片化を減らすことができます。

始める前に

VNF デバイスの共有について、次の点に注意してください。

- サービスチェーンの最初、最後、または最初と最後の両方の VNF デバイスのみを共有できます。

- VNF は、少なくとも 1 つ以上のサービスチェーン、最大 5 つまでのサービスチェーンと共有できます。
- 各サービスチェーンには、サービスチェーン内に最大 4 つの VNF デバイスを含めることができます。
- 同じサービスグループ内でのみ VNF デバイスを共有できます。

手順

ステップ 1 サービスグループとサービスグループ内のサービスチェーンを作成します。『サービスグループでのサービスチェーンの作成 （87 ページ）』を参照してください。

ステップ 2 [Add Service Chain] ダイアログボックスで、サービスチェーン名、説明、帯域幅、入力 VLAN ハンドオフ、出力 VLAN ハンドオフ、サービスチェーンの正常性情報の監視、およびサービスチェーン構成を入力します。[Add] をクリックします。

サービスチェーン構成では、ドロップダウンリストから [Create Custom] を選択します。デザインビューウィンドウに空のサービスチェーンが表示されます。左側に、サービスチェーンに追加できる VNF デバイスと PNF デバイスのセットが表示されます。VNF デバイスの周囲の「V」は VNF を表し、PNF デバイスの周囲の「P」は PNF を表します。

（注） 共有 VNF パッケージを作成するには、必ず [Create Custom] オプションを選択してください。

ステップ 3 ルータ、ロードバランサ、ファイアウォールなどの VNF を追加するには、左側のパネルから VNF アイコンをクリックし、アイコンをサービスチェーンボックス内の適切な場所にドラッグします。

必要なすべての VNF デバイスを追加したら、それぞれを構成します。

a) サービスチェーンボックスで VNF をクリックします。

[Configure VNF] ダイアログボックスが表示されます。VNF を構成するには、次のパラメータを入力します。

b) [Image Package] ドロップダウンリストから、ロードするソフトウェアイメージを選択します。

Cisco SD-WAN Manager でカスタマイズされた VNF パッケージを作成するには、カスタマイズされた VNF イメージの作成 （111 ページ）を参照してください。

c) [Fetch VNF Properties] をクリックします。
d) [Name] フィールドに、VNF の名前を入力します。
e) [CPU] フィールドに、VNF に必要な仮想 CPU の数を入力します。
f) [Memory] フィールドに、VNF に割り当てるメモリの量をメガバイト単位で入力します。
g) [Disk] フィールドに、VNF に割り当てるストレージのメモリ量をギガバイト単位で入力します。
h) 必要に応じて、VNF 固有のパラメータを入力します。VNF 固有のプロパティの詳細については、サービスグループでのサービスチェーンの作成 （87 ページ）を参照してください。

これらの VNF 固有のパラメータは、VNF の Day-0 操作に必要なカスタムユーザー変数です。

さまざまな位置にある場合のさまざまな VNF タイプのユーザー変数およびシステム変数のリストに関する完全な情報については、を参照してください。

（注） ユーザー変数が必須として定義されている場合は、必ずユーザー変数の値を入力してください。システム変数は Cisco SD-WAN Manager によって自動的に設定されます。

i) [Configure] をクリックします。

ステップ 4 VNF デバイスを共有するには、ステップ 2 から繰り返します。

ステップ 5 既存の VNF 構成を編集するには、VNF をクリックします。

ステップ 6 VNF 構成を下にスクロールして、[Share NF To] フィールドを見つけます。[Share NF To] ドロップダウンリストから、VNF を共有するサービスチェーンを選択します。

VNF が共有された後、VNF にカーソルを合わせると、特定の共有 VNF デバイスが青色で強調表示されます。共有する NF を選択すると、青い縁が表示されます。

ステップ 7 VNF を削除するか、VNF 構成をキャンセルするには、それぞれ [Delete] または [Cancel] をクリックします。

サービスグループをクラスタに接続する必要があります。

サービスグループの表示

サービスグループを表示するには、次の手順を実行します。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]** を選択します

ステップ 2 [Service Group] をクリックします。

ステップ 3 目的のサービスグループの […] をクリックし、[View] を選択します。

設計ウィンドウでサービスチェーンを表示できます。

サービスグループの編集

サービスグループをクラスタに接続する前に、すべてのパラメータを編集できます。サービスグループをクラスタに接続した後は、モニタリング構成パラメータのみを編集できます。また、サービスグループを接続した後、新しいサービスチェーンを追加することはできますが、サービスチェーンを編集または接続することはできません。したがって、既存のサービスチェーンを編集する前に、クラスタからサービスグループを切断してください。サービスグループを編集および削除するには、次の手順を実行します。

手順

ステップ 1 Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]**を選択します。

ステップ 2 [Service Group] をクリックします。

ステップ 3 目的のサービスグループの […] をクリックし、[Edit] を選択します。

ステップ 4 サービスチェーン構成を変更するか、VNF 構成を変更するには、ルータまたはファイアウォールの VNF アイコンをクリックします。

ステップ 5 新しいサービスチェーンを追加するには、[Add Service Chain] をクリックします。

クラスタ内のサービスグループの接続または切断

Cisco Catalyst SD-WAN Cloud OnRamp for Colocation 構成を完了するには、サービスグループをクラスタに接続する必要があります。サービスグループをクラスタに接続またはクラスタから切り離すには、次の手順を実行します。

手順

ステップ 1 Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]**を選択します。

ステップ 2 対応するクラスタの隣にある [...] をクリックし、[Attach Service Groups] を選択します。

ステップ 3 [Attach Service Groups] ダイアログボックスで、[Available Service Groups] で 1 つ以上のサービスグループを選択し、[Add] をクリックして、選択したグループを [Selected Service Groups] に移動します。

ステップ 4 [Attach] をクリックします。

ステップ 5 サービスグループをクラスタから切り離すには、対応するクラスタの隣にある [...] をクリックし、[Detach Service Groups] を選択します。

サービスグループ内の 1 つのサービスチェーンを接続または切り離すことはできません。

ステップ 6 表示される [Config Preview] ウィンドウで、[Cancel] をクリックして、接続または切り離しタスクをキャンセルします。

（注）

ステップ 7 サービスグループがアタッチまたはデタッチされているかどうかを確認するには、Cisco SD-WAN Manager を使用してステータスを表示します。次の点に注意してください。

- [Task View] ウィンドウのタスクのステータスが長時間にわたって [FAILURE] または [PENDING] と表示される場合は、Cisco Catalyst SD-WAN Cloud OnRamp for Colocation ソリューションガイドの「Troubleshoot Service Chain Issues」のトピックを参照してください。
- Cisco Colo Manager タスクが失敗した場合は、『Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide』の「Troubleshoot Cisco Colo Manager Issues」のトピックを参照してください。

コロケーションクラスタが [PENDING] 状態に移行した場合は、クラスタの [...] をクリックし、[Sync] を選択します。このアクションにより、クラスタは [ACTIVE] 状態に戻ります。[Sync] オプションは、Cisco SD-WAN Manager とコロケーションデバイスの同期を維持します。

VM カタログとリポジトリの管理

Note 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。

Table 31: **機能の履歴**

機能名	リリース情報	説明
qcow2 形式での Cisco VM イメージアップロードのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能を使用すると、仮想マシンイメージを qcow2 形式で Cisco SD-WAN Manager にアップロードできます。以前は、事前にパッケージ化された tar.gz 形式のイメージファイルのみをアップロードできました。

Cisco SD-WAN Manager は、事前にパッケージ化された Cisco 仮想マシンイメージ、tar.gz または、qcow2 形式のイメージのアップロードをサポートします。qcow2 イメージファイルを選択した場合は、スキャフォールドファイルをアップロードする必要があります。同様に、サービスチェーンの作成中に仮想ネットワーク機能（VNF）を構成するときに、イメージパッケージファイル、またはスキャフォールドファイルを含む qcow2 イメージファイルを選択できるようになりました。

スキャフォールドファイルには、次のコンポーネントが含まれています。

- VNF メタデータ（image_properties.xml）

- サービスチェーン用のクラスタリソースプールからのシステム生成変数（system_generated_propeties.xml）
- トークン化された Day-0 構成ファイル
- パッケージ マニフェスト ファイル（package.mf）

また、サポートされている形式（qcow2）でルートディスクイメージを提供することで、VM イメージをパッケージ化することもできます。Linux のコマンドライン NFVIS VM パッケージ ツール **nfvpt.py** を使用して qcow2 をパッケージ化するか、または Cisco SD-WAN Manager を使用してカスタマイズされた VM イメージを作成します。『カスタマイズされた VNF イメージの作成, on page 111』を参照してください。

VM が SR-IOV 対応であることは、vm パッケージ *.tar.gz の image_properties.xml で sriov_supported が true に設定されていることを意味します。また、サービス チェーン ネットワークは自動的に SR-IOV ネットワークに接続されます。sriov_supported が false に設定されている場合、データポートチャネル上に OVS ネットワークが作成されます。OVS ネットワークを使用して、サービスチェーンのために VM VNIC に接続されます。 Cloud OnRamp for Colocation ソリューションの場合、VM はサービスチェーンで同種タイプのネットワークを使用します。このタイプのネットワークは、SR-IOV と OVS の組み合わせではなく、OVS または SR-IOV のいずれかであることを意味します。

どの VM にも 2 つのデータ VNIC のみが接続されています。1 つはインバウンドトラフィック用で、もう 1 つはアウトバウンドトラフィック用です。3 つ以上のデータインターフェイスが必要な場合は、VM 内のサブインターフェイス構成を使用します。VM パッケージは VM カタログに保存されます。

Note ファイアウォールなどの各 VM タイプには、同じまたは異なるベンダーから Cisco SD-WAN Manager にアップロードされ、カタログに追加される複数の VM イメージを含めることができます。また、同じ VM のリリースに基づく異なるバージョンをカタログに追加できます。ただし、VM 名が一意であることを確認してください。

Cisco VM イメージ形式は *.tar.gz としてバンドルでき、次のものを含めることができます。

- VM を起動するルートディスクイメージ。
- パッケージ内のファイルリストのチェックサム検証用のパッケージマニフェスト。
- VM メタデータをリストする XML 形式のイメージプロパティファイル。
- （オプション）0 日目設定、VM のブートストラップに必要なその他のファイル。
- （オプション）VM がステートフル HA をサポートする場合の HA Day-0 構成。
- VM システムプロパティをリストする XML 形式のシステム生成プロパティファイル。

VM イメージは、Cisco SD-WAN Manager がホストする HTTP サーバーローカルリポジトリまたはリモートサーバーの両方でホストできます。

VM が tar.gz などの Cisco NFVIS でサポートされる VM パッケージ形式である場合、Cisco SD-WAN Manager はすべての処理を実行し、VNF プロビジョニング中に変数キーと値を指定できます。

Note Cisco SD-WAN Manager は Cisco VNF を管理します。VNF 内の Day-1 および Day-N 設定は他の VNF ではサポートされません。VM パッケージの形式と内容、および image_properties.xml とマニフェスト（package.mf）のサンプルの詳細については、『Cisco NFVIS Configuration Guide』の「VM Image Packaging」を参照してください。

同じ VM、同じバージョン、Communication Manager（CM）タイプの複数のパッケージをアップロードするには、3 つの値（名前、バージョン、VNF タイプ）のいずれかが異なることを確認します。その後、アップロードする VM *.tar.gz を再パッケージ化できます。

VNF イメージのアップロード

VNF イメージは Cisco SD-WAN Manager ソフトウェアリポジトリに保存されます。これらの VNF イメージは、サービスチェーンの展開中に参照され、サービスチェーンの接続中に Cisco NFVIS にプッシュされます。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Maintenance]** > **[Software Repository]**を選択します。

ステップ 2 事前にパッケージ化された VNF イメージを追加するには、[Virtual Images] をクリックしてから、[Upload Virtual Image] をクリックします。

ステップ 3 仮想イメージを保存する場所を選択します。

- 仮想イメージをローカルの Cisco SD-WAN Manager サーバーに保存し、コントロールプレーン接続を介して CSP デバイスにダウンロードするには、[Manager] をクリックします。[Upload VNF's Package to Manager] ダイアログボックスが表示されます。

  1. 仮想イメージファイルまたは qcow2 イメージファイルをダイアログボックスにドラッグアンドドロップするか、[Browse] をクリックしてローカルの Cisco SD-WAN Manager サーバーから仮想イメージを選択します （例：CSR.tar.gz、ASAv.tar.gz、ABC.qcow2）。
  2. ファイルをアップロードする場合は、アップロードするファイルのタイプ（[Image Package] または [Scaffold]）を指定します。必要に応じてファイルの説明を指定し、カスタムタグをファイルに追加します。サービスチェーンを作成する際、このタグを使用してイメージとスキャフォールドファイルをフィルタリングできます。
  3. qcow2 イメージファイルをアップロードする場合は、サービスまたは VNF タイプ（[FIREWALL] または [ROUTER]）を指定します。必要に応じて、以下を指定します。
     - イメージの説明
     - イメージのバージョン番号

- チェックサム
- ハッシュアルゴリズム

また、サービス チェーンの作成時に、イメージやスキャフォールドファイルのフィルタ処理で使用できるカスタムタグをファイルに追加することもできます。

（注）
- qcow2 イメージファイルを選択した場合は、スキャフォールドファイルをアップロードする必要があります。
- qcow2 イメージファイルを選択するオプションは、Cisco vManage リリース 20.7.1 以降で利用できます。Cisco vManage リリース 20.6.1 以前では、tar.gz ファイルのみを選択できます。

4. [Upload] をクリックして、イメージを仮想イメージリポジトリに追加します。仮想イメージリポジトリテーブルには、追加された仮想イメージが表示され、CSP デバイスにインストールできます。

- イメージをリモートの Cisco SD-WAN Manager サーバーに保存してから CSP デバイスにダウンロードするには、[Remote Server - Manager] をクリックします。[Upload VNF's Package to Remote Server-Manager] ダイアログボックスが表示されます。

1. [Manager Hostname/IP Address] フィールドに、管理 VPN（通常は VPN 512）にある Cisco SD-WAN Manager サーバー上のインターフェイスの IP アドレスを入力します。
2. 仮想イメージファイルまたは qcow2 イメージファイルをダイアログボックスにドラッグアンドドロップするか、[Browse] をクリックしてローカルの Cisco SD-WAN Manager サーバーから仮想イメージを選択します。
3. ファイルをアップロードする場合は、アップロードするファイルのタイプ（[Image Package] または [Scaffold]）を指定します。必要に応じてファイルの説明を指定し、カスタムタグをファイルに追加します。サービスチェーンを作成する際、このタグを使用してイメージとスキャフォールドファイルをフィルタリングできます。
4. qcow2 イメージファイルをアップロードする場合は、サービスまたは VNF タイプ（[FIREWALL] または [ROUTER]）を指定します。必要に応じて、以下を指定します。
   - イメージの説明
   - イメージのバージョン番号
   - チェックサム
   - ハッシュアルゴリズム

   また、サービス チェーンの作成時に、イメージやスキャフォールドファイルのフィルタ処理で使用できるカスタムタグをファイルに追加することもできます。

（注）
- qcow2 イメージファイルを選択した場合は、スキャフォールドファイルをアップロードする必要があります。
- qcow2 イメージファイルを選択するオプションは、Cisco vManage リリース 20.7.1 以降で利用できます。Cisco vManage リリース 20.6.1 以前では、tar.gz ファイルのみを選択できます。

5. [Upload] をクリックして、イメージを仮想イメージリポジトリに追加します。仮想イメージリポジトリテーブルには、追加された仮想イメージが表示され、CSP デバイスにインストールできます。

同じベンダーまたは異なるベンダーのファイアウォールなど、複数の VNF エントリを設定できます。また、同じ VNF のリリースに基づく異なるバージョンの VNF を追加することもできます。ただし、VNF 名が一意であることを確認してください。

カスタマイズされた VNF イメージの作成

始める前に

ルートディスクイメージに加えて、1 つ以上の qcow2 イメージを入力ファイルとして VM 固有のプロパティ、ブートストラップ構成ファイル（存在する場合）と共にアップロードし、圧縮 TAR ファイルを生成できます。カスタムパッケージを使用すると、次のことができます。

- イメージプロパティとブートストラップファイル（必要な場合）と共にカスタム VM パッケージを TAR アーカイブファイルに作成します。
- カスタム変数をトークン化し、ブートストラップ構成ファイルで渡されるシステム変数を適用します。

次のカスタムパッケージの要件が満たされていることを確認します。

- VNF のルートディスクイメージ：qcow2
- Day-0 構成ファイル：システム変数とトークン化されたカスタム変数
- VM 構成：CPU、メモリ、ディスク、NIC
- HA モード：VNF が HA をサポートしている場合は、Day-0 のプライマリファイルとセカンダリファイル、HA リンクの NIC を指定します。
- 追加のストレージ：より多くのストレージが必要な場合は、事前定義されたディスク（qcow2）、ストレージボリューム（NFVIS レイヤー）を指定します。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Maintenance]** > **[Software Repository]** を選択します。

ステップ 2 **[Virtual Images]** > [Add Custom VNF Package] をクリックします。

ステップ 3 次の VNF パッケージプロパティを使用して VNF を構成し、[Save] をクリックします。

表 *32 : VNF* パッケージのプロパティ

フィールド	必須または任意	説明
Package Name	必須	ターゲット VNF パッケージのファイル名。これは、.tar または .gz 拡張子が付いた Cisco NFVIS イメージ名です。
App Vendor	必須	Cisco VNF またはサードパーティの VNF。
Name	必須	VNF イメージの名前。
Version	任意	プログラムのバージョン番号。
Type	必須	選択する VNF のタイプ。 サポートされている VNF タイプは、ルータ、ファイアウォール、ロードバランサなどです。

ステップ 4 VM qcow2 イメージをパッケージ化するには、[File Upload] をクリックし、qcow2 イメージファイルを参照して選択します。

ステップ 5 VNF のブートストラップ構成ファイルを選択するには、[Day 0 Configuration]、[File Upload] の順にクリックし、ファイルを参照して選択します。

次の Day-0 構成プロパティを含めます。

表 *33 : Day-0* 構成

フィールド	必須または任意	説明
Mount	必須	ブートストラップファイルがマウントされるパス。
Parseable	必須	Day-0 構成ファイルを解析できるかどうか。 オプションは、[Enable] または [Disable] です。デフォルトでは、[Enable] が選択されています。

フィールド	必須または任意	説明
High Availability	必須	選択する Day-0 構成ファイルのハイアベイラビリティ。 指定できる値は、[Standalone]、[HA Primary]、[HA Secondary] です。

（注） VNF にブートストラップ構成が必要な場合は、*bootstrap-config* または *day0-config* ファイルを作成します。

ステップ 6 Day-0 構成を追加するには、[Add]、[Save] の順にクリックします。Day-0 構成が [Day 0 Config File] テーブルに表示されます。システム変数とカスタム変数を使用して、ブートストラップ構成の変数をトークン化できます。Day-0 構成ファイルの変数をトークン化するには、目的の Day-0 構成ファイルの横にある [View Configuration File] をクリックします。[Day 0 configuration file] ダイアログボックスでは、次のタスクを実行します。

（注） ブートストラップ構成ファイルは XML またはテキスト形式で、VNF と環境に固有のプロパティが含まれています。共有 VNF については、『Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide』のトピックとその他の関連資料を参照してください。さまざまな VNF タイプに追加する必要があるシステム変数のリストが記載されています。.

a) システム変数を追加するには、[CLI configuration] ダイアログボックスで、テキストフィールドからプロパティを選択して強調表示します。[System Variable] をクリックします。[Create System Variable] ダイアログボックスが表示されます。

b) [Variable Name] ドロップダウンリストからシステム変数を選択し、[Done] をクリックします。強調表示されたプロパティは、システム変数名に置き換えられます。

c) カスタム変数を追加するには、[CLI configuration] ダイアログボックスで、テキストフィールドからカスタム変数属性を選択して強調表示します。[Custom Variable] をクリックします。[Create Custom Variable] ダイアログボックスが表示されます。

d) カスタム変数名を入力し、[Type] ドロップダウンリストからタイプを選択します。

e) カスタム変数属性を設定するには、次の手順を実行します。

- サービスチェーンの作成時にカスタム変数が必須になるようにするには、[Mandatory] の横にある [Type] をクリックします。
- VNF にプライマリとセカンダリの Day-0 ファイルの両方が含まれるようにするには、[Common] の横にある [Type] をクリックします。

f) [Done] をクリックしてから、[Save] をクリックします。強調表示されたカスタム変数属性は、カスタム変数名に置き換えられます。

ステップ 7 追加の VM イメージをアップロードするには、[Advance Options] を展開し、[Upload Image] をクリックします。次に、追加の qcow2 イメージファイルを参照して選択します。ルートディスク、エフェメラルディスク 1、またはエフェメラルディスク 2 を選択し、[Add] をクリックします。新しく追加された VM イメージが [Upload Image] テーブルに表示されます。

（注） 追加の VM イメージをアップロードするときは、エフェメラルディスクとストレージボリュームを組み合わせないようにしてください。

ステップ 8 ストレージ情報を追加するには、[Add Storage] を展開し、[Add volume] をクリックします。次のストレージ情報を入力し、[Add] をクリックします。追加されたストレージの詳細が [Add Storage] テーブルに表示されます。

表 *34*：ストレージのプロパティ

フィールド	必須または任意	説明
Size	必須	VM 操作に必要なディスクサイズ。サイズ単位が GiB の場合、最大ディスクサイズは 256 GiB です。
Size Unit	必須	サイズ単位を選択します。 サポートされる単位は、MIB、GiB、TiB です。
Device Type	任意	ディスクまたは CD-ROM を選択します。デフォルトでは、ディスクが選択されています。
Location	任意	ディスクまたは CD-ROM の場所。デフォルトでは、ローカルです。
Format	任意	ディスクイメージ形式を選択します。 サポートされている形式は、qcow2、raw、および vmdk です。デフォルトでは、raw です。
Bus	任意	ドロップダウンリストから値を選択します。 バスでサポートされる値は、virtio、scsi、および ide です。デフォルトでは、virtio です。

ステップ 9 VNF イメージのプロパティを追加するには、[Image Properties] を展開し、次のイメージ情報を入力します。

表 *35 : VNF* イメージのプロパティ

フィールド	必須または任意	説明
SR-IOV Mode	必須	SR-IOV サポートを有効または無効にします。デフォルトでは有効になっています。
Monitored	必須	ブートストラップできる VM の正常性モニタリング。 オプションは enable または disable です。デフォルトでは有効になっています。
Bootup Time	必須	モニタリング対象 VM のモニタリングタイムアウト期間。デフォルトは 600 秒です。
Serial Console	任意	サポートされている、またはされていないシリアルコンソール。 オプションは enable または disable です。デフォルトでは無効になっています。
Privileged Mode	任意	プロミスキャスモードやスヌーピングなどの特別な機能を許可します。 オプションは enable または disable です。デフォルトでは無効になっています。
Dedicate Cores	必須	VM の低遅延（ルータやファイアウォールなど）を補う専用リソース（CPU）の割り当てを容易にします。それ以外の場合は、共有リソースが使用されます。 オプションは enable または disable です。デフォルトでは有効になっています。

ステップ 10 VM リソース要件を追加するには、[Resource Requirements] を展開し、次の情報を入力します。

表 *36 : VM* リソース要件

フィールド	必須または任意	説明
Default CPU	必須	VM でサポートされる CPU。サポートされる CPU の最大数は 8 です。
Default RAM	必須	VM でサポートされる RAM。指定できる RAM の範囲は 2 ～ 32 です。
Disk Size	必須	VM でサポートされるディスクサイズ（GB）。指定できるディスクサイズの範囲は 4 ～ 256 です。
Max number of VNICs	任意	VM に許可される VNIC の最大数。VNIC の数は 8 ～ 32 の範囲で指定でき、デフォルト値は 8 です。
Management VNIC ID	必須	管理インターフェイスに対応する管理 VNIC ID。有効な範囲は、0 から VNIC の最大数までです。
Number of Management VNICs ID	必須	vNIC の数。
High Availability VNIC ID	必須	ハイアベイラビリティが有効になっている VNIC ID。有効な範囲は、0 から VNIC の最大数までです。管理 VNIC ID と競合してはいけません。デフォルトでは、値は 1 になっています。
Number of High Availability VNICs ID	必須	ハイアベイラビリティが有効になっている VNIC ID の最大数。有効な範囲は 0 ～（VNIC の最大数 - 管理 VNIC の数 - 2）で、デフォルトの値は 1 です。

ステップ 11 Day-0 構成ドライブオプションを追加するには、[Day 0 Configuration Drive options] を展開し、次の情報を入力します。

表 *37 : Day-0* 構成ドライブオプション

フィールド	必須または任意	説明
Volume Label	必須	Day-0 構成ドライブのボリュームラベル。 オプションは、V1 または V2 です。デフォルトでは、オプションは V2 です。V2 は、構成ドライブラベル config-2 です。V1 は、構成ドライブラベル cidata です。
Init Drive	任意	マウント時のディスクとしての Day-0 構成ファイル。デフォルトのドライブは CD-ROM です。
Init Bus	任意	初期バスを選択します。 バスでサポートされる値は、virtio、scsi、および ide です。デフォルトでは ide です。

ソフトウェア リポジトリ テーブルにはカスタマイズされた VNF イメージが表示されます。カスタムサービスチェーンを作成するときにイメージを選択できます。

VNF イメージの表示

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Maintenance]** > **[Software Repository]**を選択します。

ステップ 2 [Virtual Images] をクリックします。

ステップ 3 検索結果をフィルタリングするには、検索バーのフィルタオプションを使用します。

[Software Version] 列には、ソフトウェアイメージのバージョンが表示されます。

[Software Location] 列は、ソフトウェアイメージが保存されている場所を示します。ソフトウェアイメージは、Cisco SD-WAN Manager サーバー上のリポジトリまたはリモートロケーションのリポジトリに格納できます。

[Version Type Name] 列には、ファイアウォールのタイプが表示されます。

[Available Files] 列には、VNF イメージファイル名が表示されます。

[Update On] 列は、ソフトウェアイメージがリポジトリに追加された場合に表示されます。

ステップ 4 目的のイメージで [...] をクリックし、[Show Info] を選択します。

VNF イメージの削除

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Maintenance]** > **[Software Repository]**を選択します。
ステップ 2 [Virtual Images] をクリックします。リポジトリ内のイメージが表に表示されます。
ステップ 3 目的のイメージの [...] をクリックし、[Delete] を選択します。

（注） VNFイメージをデバイスにダウンロードしている場合、ダウンロードプロセスが完了するまで VNF イメージを削除することはできません。

（注） また、サービスチェーンによって参照されている VNF イメージは削除できません。

Cisco SD-WAN Manager を使用した Cisco NFVIS のアップグレード

Cisco NFVIS をアップロードしてアップグレードするには、アップグレードイメージが、Cisco SD-WAN Manager を使用して Cisco SD-WAN Manager リポジトリにアップロードできるアーカイブファイルとして利用できる必要があります。Cisco NFVIS イメージをアップロードした後、Cisco SD-WAN Manager の [Software Upgrade] ウィンドウを使用して、アップグレードされたイメージを CSP デバイスに適用できます。Cisco SD-WAN Manager を使用して Cisco NFVIS ソフトウェアをアップグレードする場合、次のタスクを実行できます。

- Cisco NFVIS アップグレードイメージをアップロードします。『NFVIS アップグレードイメージのアップロード, on page 119』を参照してください。
- アップロードされたイメージで CSP デバイスをアップグレードします。『Cisco NFVIS アップグレードイメージを使用した CSP デバイスのアップグレード, on page 119』を参照してください。
- Cisco SD-WAN Manager ツールバーにある [Tasks] アイコンをクリックして、CSP デバイスのアップグレードステータスを表示します。

NFVIS アップグレードイメージのアップロード

手順

ステップ 1 所定の場所からローカルシステムに Cisco NFVIS アップグレードイメ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することもできます。

ステップ 2 Cisco SD-WAN Manager のメニューから、**[Maintenance]** > **[Software Repository]** を選択します。

ステップ 3 **[Add New Software]** > **[Remote Server/Remote Server - Manager]** をクリックします。

ソフトウェアイメージは、リモートファイルサーバー、リモート Cisco SD-WAN Manager サーバー、または Cisco SD-WAN Manager サーバーに保存できます。

Cisco SD-WAN Manager サーバー：ソフトウェアイメージをローカルの Cisco SD-WAN Manager サーバーに保存します。

リモートサーバー：ソフトウェアイメージの場所を指す URL を保存し、FTP または HTTP URL を使用してアクセスできます。

リモート Cisco SD-WAN Manager サーバー：ソフトウェアイメージをリモート Cisco SD-WAN Manager サーバーに保存し、リモート Cisco SD-WAN Manager サーバーの場所はローカル Cisco SD-WAN Manager サーバーに保存されます。

ステップ 4 イメージをソフトウェアリポジトリに追加するには、ステップ 1 でダウンロードした Cisco NFVIS アップグレードイメージを参照して選択します。

ステップ 5 [Add|Upload] をクリックします。

ソフトウェア リポジトリ テーブルには、追加された NFVIS アップグレードイメージが表示され、CSP デバイスにインストールできます。『Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide』の「Manage Software Upgrade and Repository」のトピックを参照してください。

Cisco NFVIS アップグレードイメージを使用した CSP デバイスのアップグレード

始める前に

Cisco NFVIS ソフトウェアバージョンが、`.nfvispkg` 拡張子を持つファイルであることを確認します。

手順

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

ステップ 2 選択するデバイスの 1 つ以上の CSP デバイスチェックボックスをオンにします。

ステップ 3 [Upgrade] をクリックします。[Software Upgrade] ダイアログボックスが表示されます。

ステップ 4 CSP デバイスにインストールする Cisco NFVIS ソフトウェアバージョンを選択します。ソフトウェアがリモートサーバーにある場合は、適切なリモートバージョンを選択します。

ステップ 5 新しい Cisco NFVIS ソフトウェアバージョンで自動的にアップグレードおよびアクティブ化し、CSP デバイスを再起動するには、[Activate and Reboot] チェックボックスをオンにします。

[Activate and Reboot] チェックボックスをオンにしない場合、CSP デバイスはソフトウェアイメージをダウンロードして検証します。ただし、CSP デバイスでは引き続き古いバージョンまたは現在のバージョンのソフトウェアイメージが実行されます。CSP デバイスで新しいソフトウェアイメージを実行できるようにするには、デバイスを再度選択し、[Software Upgrade] ウィンドウで [Activate] ボタンをクリックして、新しい Cisco NFVIS ソフトウェアバージョンを手動でアクティブ化する必要があります。

ステップ 6 [Upgrade] をクリックします。

[Task View] ウィンドウには、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。ウィンドウは定期的に更新され、アップグレードの進行状況またはステータスを示すメッセージが表示されます。Cisco SD-WAN Manager のツールバーにある [Task View] アイコンをクリックすると、ソフトウェア アップグレード ステータス ウィンドウに簡単にアクセスできます。

（注） 同じクラスタに属する 2 つ以上の CSP デバイスがアップグレードされる場合、CSP デバイスのソフトウェアアップグレードは順番に実行されます。

（注） [Set the Default Software Version] オプションは、Cisco NFVIS イメージでは使用できません。

CSP デバイスが再起動し、新しい NFVIS バージョンがデバイスでアクティブ化されます。この再起動は、**アクティブ化**のフェーズ中に発生します。[Activate and Reboot] チェックボックスをオンにした場合、または CSP デバイスを再度選択した後に手動で [Activate] をクリックすると、アクティブ化はアップグレードの直後に行われます。

CSP デバイスが再起動して実行されているかどうかを確認するには、タスクビューウィンドウを使用します。Cisco SD-WAN Manager は、ネットワーク全体を 90 秒ごとに最大 30 回ポーリングし、タスクビューウィンドウにステータスを表示します。

（注） イメージバージョンがデバイスで実行されているアクティブなバージョンでない場合は、CSP デバイスから Cisco NFVIS ソフトウェアイメージを削除できます。

サポートされるアップグレードシナリオと推奨される接続

規範的接続またはフレキシブルな接続の使用を決定するさまざまなアップグレードシナリオとクラスタの状態を以下に示します。

表 *38* : サポートされる接続

Cisco SD-WAN Manager	Cisco NFVIS	クラスタの状態	サポートされる接続
リリース 19.3 または 20.1.1.1 からリリース 20.3.1 へのアップグレード	リリース 3.12 または 4.1 からリリース 4.1.1 または 4.2.1 へのアップグレード	リリース 19.3 または 20.1.1.1 で作成され、アクティブなクラスタ	規範的接続を使用する
最新のリリース 20.3.1 を使用する	最新のリリース 4.2.1 を使用する	Cisco vManage リリース 20.3.1 で作成され、アクティブなクラスタ	規範的接続またはフレキシブルな接続を使用できる
リリース 20.1.1.1 からリリース 20.3.1 へのアップグレード	リリース 4.1 からリリース 4.1.1 または 4.2.1 へのアップグレード	リリース 20.1.1.1 で作成され、アクティブなクラスタ	規範的接続を使用する
リリース 20.1.1.1 からリリース 20.3.1 へのアップグレード	リリース 4.1 からリリース 4.1.1 または 4.2.1 へのアップグレード	リリース 20.1.1.1 で作成され、アクティブなクラスタ。 アップグレード後に新しい Cisco CSP デバイスを追加するには、「Cisco SD-WAN Manager および Cisco NFVIS のアップグレード後のクラスタへの Cisco CSP デバイスの追加」を参照してください。	規範的接続を使用する
リリース 20.1.1.1 からリリース 20.3.1 へのアップグレード	リリース 4.1 からリリース 4.1.1 または 4.2.1 へのアップグレード	Cisco vManage リリース 20.3.1 で作成され、アクティブなクラスタ	規範的接続またはフレキシブルな接続を使用できる

Cisco SD-WAN Manager および Cisco NFVIS のアップグレード後のクラスタへの Cisco CSP デバイスの追加

Cisco SD-WAN Manager をリリース 20.3.1 にアップグレードする前にクラスタが作成された場合に、Cisco CSP デバイスをクラスタに追加するには、次の手順を実行します。

1. 規範的接続に従って、新しく追加された Cisco CSP デバイスのケーブルを接続します。
2. Cisco NFVIS をリリース 4.2.1 にアップグレードする
3. Cisco NFVIS にログインして、新しく追加された Cisco CSP デバイスで次のコマンドを使用します。
   - **request csp-prescriptive-mode**

     新しく追加された Cisco CSP デバイスを規範モードで実行するように要求します。
   - **request activate chassis-number** *chassis number* **token** *serial number*

     Cisco CSP デバイスをアクティブ化する

     例

     ```
     request activate chassis-number 71591a3b-7d52-24d4-234b-58e5f4ad0646
     token e0b6f073220d85ad32445e30de88a739
     ```

クラスタを更新する前の推奨事項

- Cisco Catalyst SD-WAN Cloud OnRamp for Colocation ソリューションの最新リリースにアップグレードするときにすでにアクティブなクラスタを使用するには、Cisco SD-WAN Manager および Cisco NFVIS を最新リリースにアップグレードしてください。
- Cisco Catalyst SD-WAN Cloud OnRamp for Colocation ソリューションの最新リリースにアップグレードするときに新しいクラスタを作成するには、フレキシブルな接続のために Cisco SD-WAN Manager および Cisco NFVIS を最新リリースにアップグレードしてください。

Cisco Catalyst SD-WAN Manager からの Cloud OnRamp for Colocation デバイスの動作ステータスのモニター

（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。

コロケーションデバイスのモニタリングは、クラウド サービス プラットフォーム（CSP）デバイスや Cisco Colo Manager などのデバイスの正常性、インベントリ、可用性、およびその他

の運用関連プロセスを確認および分析するプロセスです。CPU、メモリ、ファン、温度など、CSP デバイスのコンポーネントを監視することもできます。Cisco SD-WAN Manager モニタリング画面の詳細については、『Cisco Catalyst SD-WAN Configuration Guides』を参照してください。

すべての通知は、Cisco SD-WAN Manager 通知ストリームに送信されます。通知ストリームコマンドを使用するには、『Cisco Catalyst SD-WAN Command Reference』を参照してください。

手順

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

Cisco SD-WAN リリース 20.6.x 以前：Cisco SD-WAN Manager のメニューから **[モニター（Monitor）]** > **[ネットワーク（Network）]** の順に選択します。

Cisco SD-WAN Manager が CSP デバイスに到達できず、Cisco Colo Manager がスイッチに到達できない場合、CSP デバイスと Cisco Colo Manager は到達不能として表示されます。

ステップ 2 ホスト名をクリックして、リストから CSP デバイスまたはスイッチをクリックします。

デフォルトでは、VNF ステータスウィンドウが表示されます。

ステップ 3 [Select Device] をクリックし、デバイスの検索結果をフィルタリングするには、検索バーの [Filter] オプションを使用します。

表示されるデバイスに関する情報のカテゴリは次のとおりです。

- VNF ステータス：各 VNF のパフォーマンス仕様、必要なリソース、およびコンポーネントネットワーク機能を表示します。VNF に関する情報の表示 （125 ページ）を参照してください。
- インターフェイス：インターフェイスのステータスと統計情報を表示します。『Cisco Catalyst SD-WAN Configuration Guides』の「View Interfaces」を参照してください。
- 制御接続：制御接続のステータスと統計を表示します。『Cisco Catalyst SD-WAN Configuration Guides』の「View Control Connections」のトピックを参照してください。
- システムステータス：リブートとクラッシュの情報、ハードウェアコンポーネントのステータス、CPU とメモリの使用状況を表示します。『Cisco Catalyst SD-WAN Configuration Guides』の「View Control Connections」のトピックを参照してください。
- Cisco Colo Manager：Cisco Colo Manager の正常性ステータスを表示します。Cisco Colo Manager の正常性の表示 （124 ページ）を参照してください。
- イベント：最新のシステムログ（syslog）イベントを表示します。『Cisco Catalyst SD-WAN Configuration Guides』の「View Events」のトピックを参照してください。
- トラブルシューティング：ping および traceroute トラフィック接続ツールに関する情報を表示します。『Cisco Catalyst SD-WAN Configuration Guides』の「Troubleshoot a Device」のトピックを参照してください。

- リアルタイム：機能固有の操作コマンドのリアルタイムデバイス情報を表示します。『Cisco Catalyst SD-WAN Configuration Guides』の「View Real-Time Data」のトピックを参照してください。

ステップ 4 コロケーションクラスタを監視するには、Cisco SD-WAN Manager メニューから**[Monitor]** > **[Devices]**を選択し、[Colocation Cluster] をクリックします。

Cisco vManage リリース 20.6.1 以前：コロケーションクラスタをモニターするには、Cisco SD-WAN Manager メニューから **[Monitor]** > **[Network]** を選択し、[Colocation Clusters] をクリックします。

ステップ 5 目的のクラスタ名をクリックします。詳細については、「Cloud OnRamp Colocation クラスタのモニター（127 ページ）」を参照してください。

Cisco Colo Manager の正常性の表示

デバイス、CCM ホストシステム IP、CCM IP、および CCM 状態に関する Cisco Colo Manager（CCM）の正常性を表示できます。この情報を確認すると、ネットワーク サービスチェーンの設計時に使用する VNF を決定するのに役立ちます。VNF に関する情報を表示するには、次の手順を実行します。

手順

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

Cisco SD-WAN Manager リリース 20.6.x 以前：Cisco SD-WAN Manager のメニューから **[Monitor]** > **[Network]** の順に選択します。

すべてのデバイスの情報が表形式で表示されます。

ステップ 2 表から CSP デバイスをクリックします。

ステップ 3 左ペインで、[Colo Manager] をクリックします。

右ペインには、Cisco Colo Manager のメモリ使用率、CPU 使用率、稼働時間などに関する情報が表示されます。

VNF に関する情報の表示

表 *39* : 機能の履歴

機能名	リリース情報	説明
VNF の状態とカラーコード	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	この機能を使用すると、展開された VM の状態を、**[Monitor]** > **[Devices]** ページで表示できるカラーコードを使用して判断できます。これらのカラーコードは、VM の状態に基づいてサービスチェーンの作成を決定するのに役立ちます。

表 *40* : 機能の履歴

機能名	リリース情報	説明
SR-IOV 対応の NIC および OVS スイッチのネットワーク使用率チャート	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	この機能により、SR-IOV 対応の NIC と OVS スイッチの両方に接続された VM VNIC のネットワーク使用率チャートを表示できます。これらのチャートは、VM の使用率がサービスチェーンの作成に最適かどうかを判断するのに役立ちます。

各 VNF のパフォーマンス仕様と必要なリソースを表示できます。この情報を確認すると、ネットワークサービスの設計時に使用する VNF を決定するのに役立ちます。VNF に関する情報を表示するには、次の手順を実行します。

手順

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

Cisco vManage リリース 20.6.x 以前：Cisco SD-WAN Manager のメニューから**[Monitor]** > **[Network]** の順に選択します。

Cisco SD-WAN Manager は、VNF 情報を表形式で表示します。この表には、CPU 使用率、メモリ消費量、ディスク、およびネットワークサービスのパフォーマンスを決定するその他の主要パラメータなどの情報が表示されます。

ステップ 2 表から CSP デバイスをクリックします。

ステップ 3 左側のペインで、[VNF Status] をクリックします。

ステップ 4 表から、VNF 名をクリックします。Cisco SD-WAN Manager が特定の VNF に関する情報を表示します。ネットワーク使用率、CPU 使用率、メモリ使用率、およびディスク使用率をクリックして、VNF リソースの使用率を監視できます。

次の VNF 情報が表示されます。

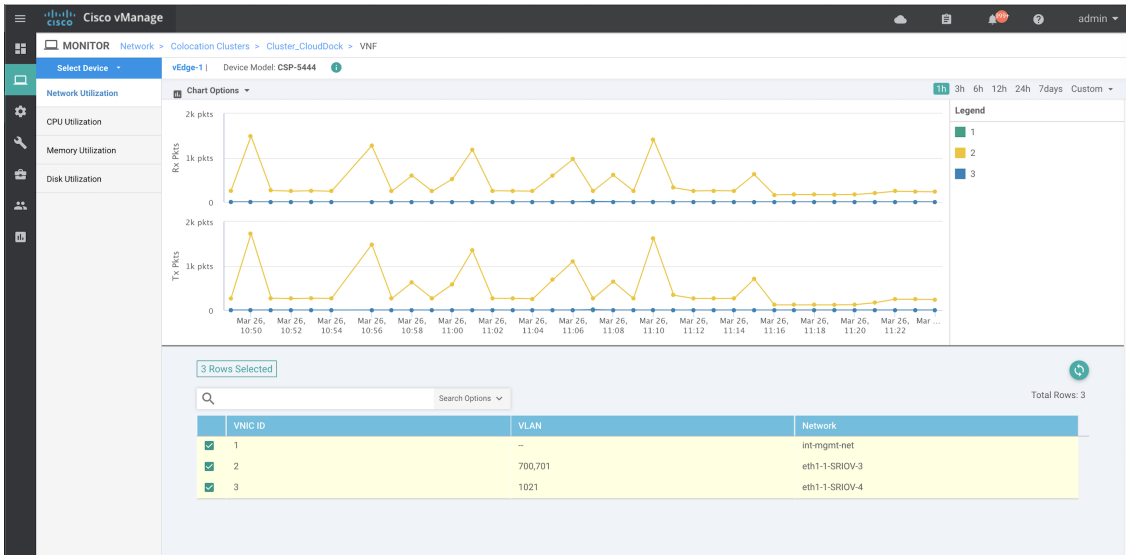
表 *41 : VNF* 情報

チャートオプションバー	グラフ形式の VNF 情報	色分けされた形式の VNF 情報
• [Chart Options] ドロップダウン：[Chart Options] ドロップダウンリストをクリックして、表示するデータのタイプを選択します。 • 期間：データを表示する事前定義された期間またはカスタム期間をクリックします。	[Select Device] ドロップダウンリストから VNF を選択して、VNF の情報を表示します。	VNF は、VNF ライフサイクルの次の運用ステータスに基づいて特定の色で表示されます。 • 緑：VNF は正常に展開され、正常に起動されています。 • 赤：VNF の展開またはその他の操作が失敗するか、VNF が停止しています。 • 黄色：VNF はある状態から別の状態に移行中です。

右側のペインには、以下が表示されます。

- フィルタ基準
- すべての VNF または VM に関する情報を一覧表示する VNF テーブル。デフォルトでは、最初の 6 つの VNF が選択されています。SR-IOV が有効な NIC および OVS スイッチに接続された VNIC のネットワーク使用率チャートが表示されます。

図 *11 : VNF* 情報



チェックボックスをオンにすると選択した VNF の情報がグラフィック表示にプロットされます。

- 左側のチェックボックスをクリックして、VNF を選択または選択解除します。一度に最大 6 つの VNF の情報を選択して表示できます。

• 列のソート順を変更するには、列のタイトルをクリックします。

Cloud OnRamp Colocation クラスタのモニター

表 *42 :* 機能の履歴

機能名	リリース情報	説明
ネットワークアシュアランス – VNF：停止/開始/再起動	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、[Colocation Cluster] タブから Cisco CSP デバイスの VNF を停止、開始、または再起動できます。Cisco SD-WAN Manager を使用して VNF の操作を簡単に実行できます。

クラスタ情報とその正常性状態を表示できます。この情報を確認すると、サービスチェーン内の各 VNF をホストする Cisco CSP デバイスを判断するのに役立ちます。クラスタに関する情報を表示するには、次の手順を実行します。

手順

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

Cisco vManage リリース 20.6.1 以前：Cisco SD-WAN Manager のメニューから **[モニター（Monitor）]** > **[ネットワーク（Network）]** の順に選択します。

ステップ 2 クラスタを監視するには、[Colocation Cluster] をクリックします。

Cisco vManage リリース 20.6.1 以前：[Colocation Clusters] をクリックします。

関連する情報を保有するすべてのクラスタが表形式で表示されます。クラスタ名をクリックします。[Config. View] および [Port Level View] をクリックすると、クラスタを監視できます。

- [Config. View]：ウィンドウの主要部分に、クラスタを形成する CSP デバイスとスイッチデバイスが表示されます。右側のペインでは、コロケーションサイズに基づいて、使用可能な CPU リソースと合計 CPU リソース、使用可能メモリと割り当て済みメモリなどのクラスタ情報を表示できます。

  ウィンドウの詳細部分には以下が含まれます。

  - 検索：検索結果をフィルタリングするには、検索バーの [Filter] オプションを使用します。
  - クラスタ内のすべてのデバイス（Cisco CSP デバイス、PNF、およびスイッチ）に関する情報を一覧表示する表。

    Cisco CSP デバイスをクリックします。VNF 情報が表形式で表示されます。この表には、VNF 名、サービスチェーン、CPU の数、メモリ消費量、およびネットワーク サービス チェーンのパフォー

マンスを定義するその他のコアパラメータなどの情報が含まれています。VNF に関する情報の表示 （125 ページ）を参照してください。

VNF を開始、停止、またはリブートするには、目的の VNF の [...] をクリックし、次のいずれかの操作を選択します。

- [Start]
- [Stop]
- [Restart]

（注） サービスチェーンのいずれかの VNF で開始、停止、再開の操作を実行する前に、サービスチェーンのプロビジョニングが完了し、VM が展開されていることを確認します。

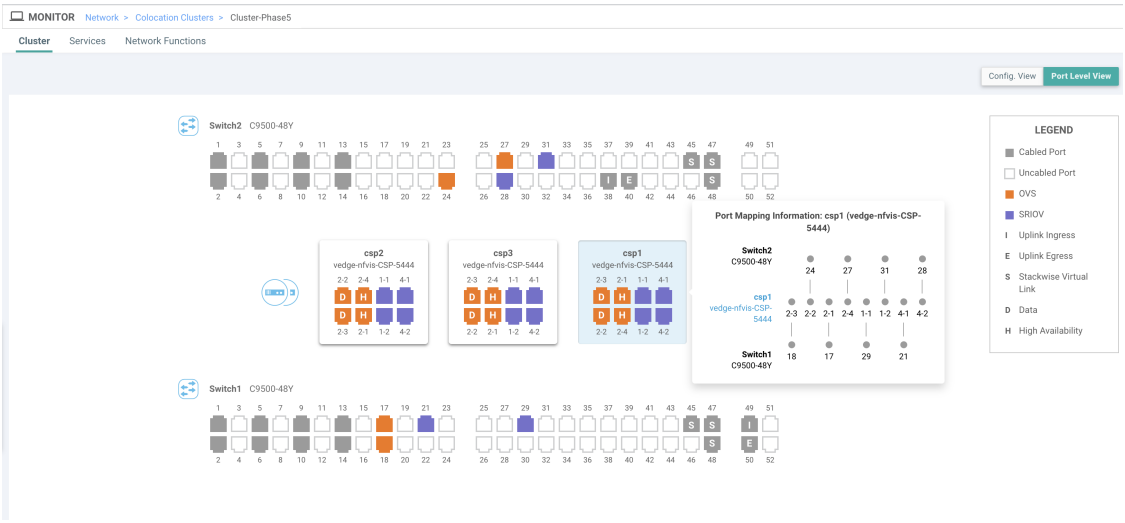
VNF で操作を選択したら、操作が完了するまで待ってから、別の操作を実行します。[Task View] ウィンドウから操作の進行状況を表示できます。

- [Port Level View]：クラスタをアクティブ化した後、ポート接続の詳細を表示するには、[Port Level View] をクリックします。

  スイッチと CSP デバイスの詳細なポート接続情報を、SR-IOV および OVS モードに基づいて色分けされた形式で表示できます。

  Catalyst 9500 スイッチと CSP デバイス間のポートのマッピングを表示するには、CSP デバイスをクリックするか、カーソルを合わせます。

図 *12*：クラスタのポート接続の詳細の監視



ステップ 3 [Services] をクリックします。

ここでは、次の情報を表示できます。

- サービスチェーンの完全な情報。最初の 2 列には、サービスグループ内のサービスチェーンの名前と説明が表示され、残りの列には、VNF、PNF ステータス、モニタリングサービスイネーブルメント、およびサービスチェーンの全体的な正常性が表示されます。サービスチェーンに関連付けられたコロ

ケーションユーザーグループを表示することもできます。さまざまな正常性ステータスとその表現は次のとおりです。

- Healthy：緑の上向き矢印。すべての VNF、PNF デバイスが実行されていて、正常な状態の場合、サービスチェーンは「Healthy」状態になります。ルーティングとポリシーが正しく構成されていることを確認してください。
- Unhealthy：赤の下向き矢印。VNF または PNF の 1 つが異常な状態にある場合、サービスチェーンは「Unhealthy」状態であると報告されます。たとえば、サービスチェーンを展開した後、ネットワーク機能の IP アドレスの 1 つが WAN または LAN 側で変更された場合、またはファイアウォールポリシーがトラフィックを通過させるように構成されていない場合、異常な状態が報告されます。これは、ネットワーク機能またはサービスチェーン全体が異常であるか、両方が異常な状態にあるためです。
- Undetermined：黄色の下向き矢印。この状態は、サービスチェーンの正常性を判断できない場合に報告されます。この状態は、一定期間にわたって監視対象のサービスチェーンで正常または異常などの使用可能なステータスがない場合にも報告されます。ステータスが未確定のサービスチェーンをクエリまたは検索することはできません。

  サービスチェーンが 1 つの PNF で構成されていて、PNF が Cisco SD-WAN Manager の到達可能範囲外にある場合は、モニターできません。サービスチェーンが単一のネットワーク機能で構成されている場合、ファイアウォールの両側に VPN 終端があり、監視できない場合は、Undetermined として報告されます。

  （注） サービスチェーンのステータスが未確定の場合、サービスチェーンを選択して詳細な監視情報を表示することはできません。

- 監視フィールドを有効にしてサービスチェーンを構成した場合は、Healthy または Unhealthy 状態のサービスグループをクリックします。サービスチェーンの監視ウィンドウの主要な部分には、次の要素が含まれています。

  サービスチェーン、VNF、PNF の遅延情報をプロットするグラフィック表示。

  サービスチェーンの監視ウィンドウの詳細部分には、以下が含まれます。

  - 検索：検索結果をフィルタリングするには、検索バーの [Filter] オプションを使用します。
  - すべてのサービスチェーン、VNF、PNF、それらの正常性ステータス、およびタイプに関する情報を一覧表示する表。
    - 選択するサービスチェーン、VNF、PNF のサービスチェーン、VNF、PNF チェックボックスをオンにします。
    - 列のソート順を変更するには、列のタイトルをクリックします。

  ステータスの詳細列は、監視対象のデータパスを示し、ホップごとの分析を提供します。

- [Diagram] をクリックして、サービスグループおよびすべてのサービスチェーンと VNF をデザインビューウィンドウに表示します。

- VNF をクリックすると、VNF に割り当てられた CPU、メモリ、およびディスクがダイアログボックスに表示されます。
- [Service Group] ドロップダウンリストからサービスグループを選択します。デザインビューには、選択したサービスグループと一緒にすべてのサービスチェーンと VNF が表示されます。

ステップ 4 [Network Functions] をクリックします。

ここでは、次の情報を表示できます。

- 表形式のすべての仮想または物理ネットワーク機能。[Show] ボタンを使用して、VNF または PNF を選択して表示します。

  VNF 情報が表形式で表示されます。この表には、VNF 名、サービスチェーン、コロケーション ユーザー グループ、CPU 使用率、メモリ消費量などの情報、およびネットワークサービスのパフォーマンスを明確に示すその他の主要パラメータが記載されています。VNF の詳細を表示するには、VNF 名をクリックします。VNF に関する情報の表示 （125 ページ）を参照してください。

- PNF 情報が表形式で表示されます。この表には、シリアル番号や PNF タイプなどの情報が含まれています。特定の PNF の構成を表示してメモするには、目的の PNF シリアル番号をクリックします。PNF のすべての構成を手動でメモしてから、PNF デバイスを構成するようにしてください。たとえば、サービスチェーンのさまざまな場所に PNF を配置する PNF 構成の一部を次に示します。PNF を手動で設定するには、「ASR 1000 Series Aggregation Services Routers Configuration Guides」および「Cisco Firepower Threat Defense Configuration Guides」を参照してください。

図 *13*：サービスチェーン側のパラメータを持つ最初の位置にある *PNF*

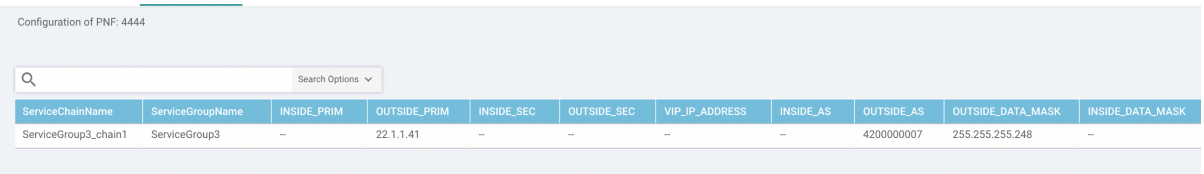


図 *14*：外部ネイバー情報を持つ最初の位置にある *PNF*

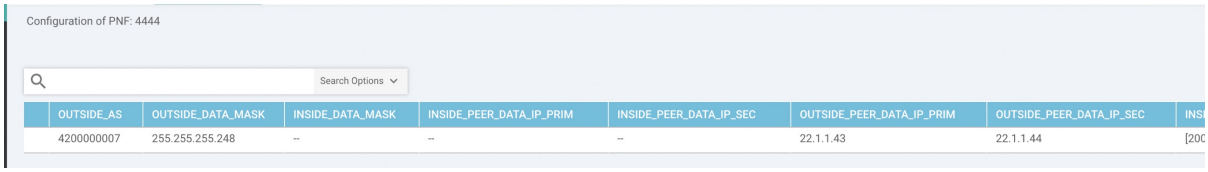


図 *15*：*2* つのサービスチェーンで共有される *PNF*

ServiceGroup2_chain3 は PNF のみのサービスチェーンであるため、構成は生成されません。PNF は ServiceGroup2_chain1 の最後の位置にあるため、INSIDE 変数のみが生成されます。

図 *16 :* 外部ネイバー情報を持つ *2* つのサービスチェーン間で共有される *PNF*

Cloud OnRamp Colocation クラスタのパケットキャプチャ

表 *43 :* 機能の履歴

機能名	リリース情報	説明
Cloud OnRamp Colocation クラスタのパケットキャプチャ	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能を使用すると、コロケーションクラスタの Cloud Services Platform（CSP）デバイスで、物理ネットワーク インターフェイス カード（PNIC）レベルまたは仮想ネットワーク インターフェイス カード（VNIC）レベルでパケットをキャプチャできます。同じデバイスの 1 つ以上の PNIC または VNIC でパケットをキャプチャすることも、異なるブラウザを使用する異なるデバイスで同時にパケットをキャプチャすることもできます。この機能により、パケットの形式に関する情報を収集し、アプリケーションの分析、セキュリティ、トラブルシューティングに役立てることができます。

コロケーションクラスタの CSP デバイスとの間で送受信されるパケットをキャプチャできます。CSP デバイスの PNIC または VNIC レベルでパケットをキャプチャできます。

Cloud OnRamp Colocation クラスタのパケットキャプチャでサポートされるポート

パケットキャプチャは、次のポートでサポートされています。

表 *44* : パケットキャプチャでサポートされるポート

モード	VNIC レベル	PNIC レベル
シングルテナント	OVS-DPDK、HA-OVS-DPDK、SR-IOV、OVS-MGMT	SR-IOV、MGMT
マルチテナント（ロールベース アクセス コントロール）	OVS-DPDK、HA-OVS-DPDK、OVS-MGMT	MGMT

Cisco SD-WAN Manager でパケットキャプチャを有効にする

コロケーションクラスタの CSP デバイスで PNIC または VNIC レベルでパケットをキャプチャする前に、Cisco SD-WAN Manager でパケットキャプチャ機能を有効にします。

1. Cisco SD-WAN Manager のメニューで、**[Administration]** > **[Settings]** を選択します。
2. [Data Stream] で、[Enabled] を選択します。

   Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、トグルボタンをクリックしてデータストリームを有効にします。

PNIC レベルでパケットをキャプチャする

1. Cisco SD-WAN Manager メニューから**[Monitor]** > **[Devices]**の順に選択します。
2. [Colocation Cluster] をクリックし、クラスタを選択します。
3. 表示されるデバイスのリストから、CSP デバイス名をクリックします。
4. 左側のペインで、[Packet Capture] をクリックします。
5. [PNIC ID] ドロップダウンリストから、PNIC を選択します。
6. （オプション）[Traffic Filter] をクリックして、キャプチャするパケットを IP ヘッダーの値に基づいてフィルタ処理します。

   表 *45* : パケットキャプチャフィルタ

フィールド	説明
Source IP	パケットの送信元 IP アドレス。
Source Port	パケットの送信元ポート番号。

フィールド	説明
Protocol	パケットのプロトコル ID。 サポートされているプロトコルは、ICMP、IGMP、TCP、UDP、ESP、AH、ICMP バージョン 6（ICMPv6）、IGRP、PIM、および VRRP です。
Destination IP	パケットの宛先 IP アドレス。
Destination Port	パケットの宛先ポート番号。

7. [Start] をクリックします。

   パケットキャプチャが開始され、その進行状況が表示されます。

   - Preparing file to download：ファイルサイズが 20 MB に達した後、またはパケットキャプチャを開始してから 5 分後、または [Stop] をクリックすると、パケットキャプチャが停止します。
   - Preparing file to download：Cisco SD-WAN Manager は libpcap 形式のファイル（.pcap ファイル）を作成します。
   - 「File ready, click to download the file」：ダウンロードアイコンをクリックして、生成されたファイルをダウンロードします。

VNIC レベルでパケットをキャプチャする

1. Cisco SD-WAN Manager メニューから**[Monitor]** > **[Devices]**の順に選択します。
2. [Colocation Cluster] をクリックし、クラスタを選択します。
3. 表示されるデバイスのリストから、CSP デバイス名をクリックします。
4. VNF を選択し、左側のペインで [Packet Capture] をクリックします。
5. または、**[Monitor]** > **[Devices]** > **[Colocation Cluster]**を選択します。 次に、クラスタを選択して [Network Functions] をクリックし、VNF を選択してから、左側のペインで [Packet Capture] をクリックします。
6. [VNIC ID] ドロップダウンリストから、VNIC を選択します。
7. （オプション）[Traffic Filter] をクリックして、IP ヘッダーの値に基づいてキャプチャするパケットをフィルタ処理します。これらのフィルタの詳細については、上記のセクションを参照してください。
8. [Start] をクリックします。パケットキャプチャが開始され、進行状況が表示されます。

Cisco Catalyst SD-WAN Cloud OnRamp for Colocation マルチテナント機能

（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。

表 *46* : 機能の履歴

機能名	リリース情報	説明
ロールベースのアクセス制御を使用したコロケーション マルチテナント機能	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能により、サービスプロバイダーは複数のコロケーションクラスタを管理し、複数のコロケーショングループを使用してこれらのクラスタをテナント間で共有できます。マルチテナント設定では、サービスプロバイダーはテナントごとに一意のコロケーションクラスタを展開する必要はありません。代わりに、コロケーションクラスタのハードウェアリソースは複数のテナント間で共有されます。マルチテナント機能では、サービスプロバイダーは、個々のテナントユーザーの役割に基づいてアクセスを制限することにより、テナントが自分のデータのみを表示できるようにします。

コロケーション マルチテナント機能の概要

Cisco Catalyst SD-WAN Cloud OnRamp for Colocation マルチテナント機能では、サービスプロバイダーはシングルテナントモードで Cisco SD-WAN Manager を使用して複数のコロケーションクラスタを管理できます。サービスプロバイダーは、シングルテナントモードでクラスタを起動するのと同じ方法でマルチテナントクラスタを起動できます。マルチテナントクラスタは、複数のテナント間で共有できます。「Create and Activate Clusters」を参照してください。

テナントは、コロケーションクラスタの Cisco Cloud Services Platform（CSP）デバイスや Cisco Catalyst 9500 デバイスなどのハードウェアリソースを共有します。この機能の重要なポイントは次のとおりです。

- サービスプロバイダーは、有効な証明書を使用して Cisco SD-WAN 制御コンポーネント（Cisco SD-WAN Manager、Cisco Catalyst SD-WAN Validator、および Cisco Catalyst SD-WAN コントローラ）を展開および設定します。
- サービスプロバイダーは、Cisco CSP デバイスと Cisco Catalyst 9500 スイッチをオンボードした後、コロケーションクラスタをセットアップします。
- Cisco Catalyst SD-WAN はシングルテナントモードで動作し、Cisco SD-WAN Manager はシングルテナントモードで表示されます。
- コロケーションマルチテナント展開では、サービスプロバイダーは、ロールを作成することにより、テナントがサービスチェーンのみを参照できるようにします。サービスプロバイダーは、コロケーショングループ内の各テナントのロールを作成します。これらのテナントは、ロールに基づいてサービスチェーンにアクセスして監視することが許可されています。ただし、サービスチェーンを構成したり、システムレベルの設定を変更したりすることはできません。ロールにより、テナントは表示が許可されている情報のみにアクセスできるようになります。
- 各テナントトラフィックは、コンピューティングデバイス全体で VXLAN を使用してセグメント化され、Cisco Catalyst スイッチファブリック全体で VLAN を使用してセグメント化されます。
- サービスプロバイダーは、特定のクラスタにサービスチェーンをプロビジョニングできます。

コロケーション マルチテナント セットアップの 2 つのシナリオを以下に示します。

- サービスプロバイダーが所有する Cisco Catalyst SD-WAN デバイス：このシナリオでは、サービスチェーンで使用される Cisco Catalyst SD-WAN デバイスは、対応するサービスプロバイダーに属します。CSP デバイスと Catalyst 9500 スイッチは、サービスプロバイダーが所有、監視、保守します。仮想マシン（VM）パッケージは、サービスプロバイダーが所有、アップロード、および保守します。『共同管理されたマルチテナント環境でのコロケーション クラスタ デバイスと Cisco Catalyst SD-WAN デバイスのモニター （144 ページ）』を参照してください。
- 共同管理された Cisco Catalyst SD-WAN デバイス：このシナリオでは、サービスチェーンで使用される Cisco Catalyst SD-WAN デバイスはテナント オーバーレイ ネットワークに属します。コロケーションクラスタ デバイスはサービスプロバイダーが所有しますが、サービスチェーンの Cisco Catalyst SD-WAN はテナントの Cisco SD-WAN 制御コンポーネント（Cisco SD-WAN Manager、Cisco Catalyst SD-WAN Validator、および Cisco Catalyst SD-WAN コントローラ）によって制御されます。CSP デバイスと Catalyst 9500 スイッチは、サービスプロバイダーが所有、監視、保守します。VM パッケージは、サービスプロバイダーが所有、アップロード、および保守します。共同管理されたマルチテナント環境でのコロケーション クラスタ デバイスと Cisco Catalyst SD-WAN デバイスのモニター （144 ページ）を参照してください。

マルチテナント環境での役割と機能

マルチテナント環境には、サービスプロバイダーと複数のテナントが含まれます。各ロールには、明確な責任と関連する機能があります。

サービス プロバイダ

サービスプロバイダーは、すべてのハードウェアインフラストラクチャを所有し、クラスタを管理します。また、サービスプロバイダーは、ロールを作成してテナントをオンボーディングし、テナントのサービスチェーンをプロビジョニングし、すべてのテナントのすべてのサービスチェーンを表示できます。

サービスプロバイダーは、**管理**ユーザーまたは管理ユーザー権限の書き込み権限を持つユーザーとしてCisco SD-WAN Managerにログインします。サービスプロバイダーは、Cisco SD-WAN Managerサーバーからユーザーおよびユーザーグループを追加、編集、または削除でき、通常は次のアクティビティを担当します。

- テナントのクラスタを作成および管理します。
- 事前にパッケージ化されたVMイメージパッケージとCisco Enterprise NFVインフラストラクチャ ソフトウェア（NFVIS）ソフトウェアイメージをCSPデバイスにアップロードします。
- カスタムのコロケーショングループとロールベースのアクセス制御（RBAC）ユーザーを作成します。
- サービスグループを作成し、コロケーショングループを複数のサービスグループに関連付けます。
- CSPデバイスとCatalyst 9500スイッチをアップグレードします。
- すべてのテナントのサービスチェーンとVMを監視します。
- テナントの仮想ネットワーク機能（VNF）のいずれかで操作を開始、停止、または再開します。
- Cisco SD-WAN Managerを管理し、Cisco Catalyst SD-WANデバイスのシステム全体のログを記録します。

テナント

テナントは、自分自身に属するサービスチェーンのVNFで操作を開始できますが、別のテナントに属するサービスチェーンのVNFで表示、アクセス、または操作を開始することはできません。テナントは、以下のアクティビティを担当します。

- すべてのサービスグループと、テナントに属するサービスチェーンの正常性ステータスを監視します。
- テナントに属するサービスチェーンの一部であるVNFのイベントまたはアラームを監視します。
- テナントに属するサービスチェーンの一部であるVNFで、開始、停止、または再起動の操作を開始します。

- クラスタ、サービスチェーン、または VNF に問題がある場合は、対応するサービスプロバイダーと協力します。

マルチテナント環境での推奨仕様

サービスプロバイダーは、次の情報を使用して、テナント、クラスタ、テナントごとのサービスチェーン、およびさまざまなコロケーションサイズの VLAN 数を決定することをお勧めします。

表 *47*：マルチテナント環境の仕様

テナント	クラスタ（CPU）	テナントあたりのサービスチェーン（CPU）	VLAN
150	2（608）	1（4）：小	～ 300
75 ～ 150	2（608）	2 ～ 3（4 ～ 8）：中	300 ～ 450
25 ～ 50	2（608）	4 ～ 6（12 ～ 24）：大	～ 400
300	4（1216）	小	～ 600
150 ～ 300	4（1216）	中	600 ～ 900
50 ～ 100	4（1216）	大	～ 800
600	8（2432）	小	～ 1200
300 ～ 600	8（2432）	中	900 ～ 1200
100 ～ 200	8（2432）	大	～ 1050
750	10（3040）	小	～ 1500
375 ～ 750	10（3040）	中	600 ～ 1500
125 ～ 230	10（3040）	大	～ 1250

たとえば、サービスプロバイダーが、1 つの VM で構成されるサービスチェーンのテナントごとに 4 つの vCPU をプロビジョニングする場合、サービスプロバイダーは、8 つの CSP デバイスを備えた 2 つのクラスタで約 150 のテナントをオンボードできます。これらの各テナントまたはサービスチェーンには、サービスチェーンごとに 300 のハンドオフ VLAN、1 つの入力 VLAN、および 1 つの出力 VLAN が必要です。

コロケーション マルチテナント機能の前提条件と制限事項

次のセクションでは、コロケーションマルチテナント環境での前提条件と制限事項について詳しく説明します。

前提条件

- Cisco CSP デバイスと Cisco Catalyst 9500 スイッチ間の配線は、規範的接続またはフレキシブルなトポロジに従って完了します。複数のクラスタを起動するには、クラスタの CSP デバイスと Catalyst 9500 スイッチ間の配線が単一のクラスタと同じであることを確認してください。配線の詳細については、「Wiring Requirements」を参照してください。
- 各 Cisco CSP デバイスには、アウトオブバンド（OOB）管理スイッチへのポートチャネルとして手動で構成された 2 つの 1 GB 管理ポートがあります。
- テナントは、所有するサービスチェーンの一部である VNF の [Monitor] ウィンドウからイベントまたはアラームを監視のみできます。テナント監視ウィンドウには、テナントがサービスチェーンを表示しているときに、対応するコロケーショングループが表示されます。

（注） 共同管理されたマルチテナントセットアップでは、サービスプロバイダーはテナントから必要な情報を収集することにより、テナントのサービスチェーンをプロビジョニングします。たとえば、テナントは、テナント組織名、テナント Cisco SD-WAN Validator IP アドレス、テナントサイト ID、システム IP アドレスなどをアウトオブバンドで提供します。サービスグループでのサービスチェーンの作成 （87 ページ）を参照してください。

制約事項

- シングルテナントモードからマルチテナントモードへのコロケーションクラスタの変更、およびその逆の変更はサポートされていません。
- 複数のテナント間での VNF デバイスの共有はサポートされていません。
- サービスプロバイダーは、テナントに対して複数のサービスグループをプロビジョニングできます。ただし、同じサービスグループを複数のテナントにプロビジョニングすることはできません。
- シングルテナントモードの Cisco Catalyst SD-WAN Cloud OnRamp for Colocation リリース 20.4.1 から、マルチテナントモードのリリース 20.5.1 以降へのアップグレードはサポートされていません。この制限は、シングルテナントモードからマルチテナントモードにアップグレードできないことを意味します。
- シングルルート IO 仮想化対応（SR-IOV 対応）の物理ネットワーク インターフェイス カード（PNIC）のマルチテナント機能はサポートされていません。VNF VNIC のオープン仮想

スイッチ（OVS）のみがサポートされています。現在の SR-IOV ドライバは VXLAN をサポートしていないため、CSP デバイスのすべての PNIC は OVS モードです。VNF VNIC は OVS ネットワークに接続されていて、必要な速度でトラフィックを転送する機能が低下する可能性があります。

- テナントが使用するリソースの課金とサブスクリプションの管理はサポートされていません。
- 共同管理されたマルチテナントセットアップでは、テナントは、テナントが所有する VNF デバイスのみを監視できます。

サービスプロバイダー機能

新しいテナントのプロビジョニング

サービスプロバイダーは、コロケーショングループを作成して新しいテナントをプロビジョニングし、コロケーショングループに関連付けられたユーザーグループの RBAC ユーザーを作成してテナントへのアクセスを提供できます。RBAC ユーザーは、独自のテナント環境内で制限付きの管理業務を実行できます。

始める前に

サービスプロバイダーは、CSP デバイスとの制御接続を確立し、クラスタをアクティブ化することにより、クラスタを共有モードで起動する必要があります。サービスプロバイダーは複数のクラスタを作成でき、これらの各クラスタには 2 ～ 8 台の CSP デバイスと 2 台の Catalyst 9500 スイッチを含めることができます。クラスタ作成操作では、クラスタがマルチテナント展開またはシングルテナント展開のどちらであるかを選択するオプションがサポートされています。「Create and Activate Clusters」を参照してください。

手順

ステップ 1 テナントをオンボーディングするには、コロケーショングループを作成します。詳細については、「Create Colocation Group」を参照してください。このグループは、テナントのサービスグループと VM を監視するためのアクセスをテナントに提供します。

ステップ 2 RBAC ユーザーを追加し、ステップ 1 で作成したコロケーショングループに関連付けます。詳細については、「Create an RBAC User and Associate to Colocation Group」を参照してください。

（注） Cisco SD-WAN Manager の代わりに TACACS サーバーを使用してユーザーを認証している場合は、RBAC ユーザーを追加しないでください。TACACS サーバーを使用してユーザーを認証している場合は、ユーザーをステップ 1 で作成したコロケーショングループに関連付けます。

ステップ 3 サービスグループを作成し、それをコロケーショングループに関連付け、サービスグループを特定のクラスタに接続します。「Create Service Chain in a Service Group」を参照してください。

テナントが新しいサービスチェーンを必要とする場合は、テナントに固有のハンドオフ VLAN を使用します。

コロケーショングループの作成

シングルテナント Cisco SD-WAN Manager では、コロケーショングループを使用して、複数のテナント間でコロケーションクラスタを共有できます。コロケーショングループは、サービスチェーンを特定のテナントに関連付けるメカニズムです。テナント用に作成された RBAC ユーザーは、コロケーショングループと呼ばれます。これらのユーザーは、ログイン情報を使用して Cisco SD-WAN Manager にログインし、テナント固有のサービスチェーンと VNF 情報のみを表示できます。サービスプロバイダーがテナントにサービスグループを使用することを選択した場合、コロケーショングループをサービスグループに関連付けることができるように、サービスグループを作成する前にコロケーショングループを作成する必要があります。

手順

ステップ 1 Cisco SD-WAN Manager のメニューで、**[Administration]** > **[Colo Groups]** を選択します。

ステップ 2 [Add Colo Group] をクリックします。

ステップ 3 コロケーショングループ名、コロケーショングループを関連付ける必要があるユーザーグループの名前、および説明を入力します。

（注） ここで指定するコロケーショングループ名は、マルチテナント設定のサービスグループを作成するときに表示されます。

ステップ 4 [Add] をクリックします。

ユーザーグループの権限の表示

手順

ステップ 1 Cisco SD-WAN Manager メニューから **[Administration]** > **[Manage Users]** を選択します。

ステップ 2 **[User Groups]**をクリックします。

ステップ 3 ユーザーグループの権限を表示するには、[Group Name] リストで、作成したユーザーグループの名前をクリックします。

（注） ユーザーグループとその権限が表示されます。マルチテナント環境でのユーザーグループの権限のリストについては、『Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide』の「Manage Users」のトピックを参照してください。

RBAC ユーザーの作成とコロケーショングループへの関連付け

手順

ステップ 1 Cisco SD-WAN Manager メニューから **[Administration]** > **[Manage Users]** を選択します。

ステップ 2 [Add User] をクリックします。

ステップ 3 [Add User] ダイアログボックスに、ユーザーのフルネーム、ユーザー名、パスワードを入力します。

（注） ユーザー名に大文字を入力することはできません。

ステップ 4 [User Groups] ドロップダウンリストから、ユーザーが属する必要のあるグループを追加します。たとえば、コロケーション機能用に作成したユーザーグループなど、グループを 1 つずつ選択します。デフォルトでは、リソースグループ [global] が選択されています。

ステップ 5 [Add] をクリックします。

Cisco SD-WAN Manager では [Users] テーブルにあるユーザーが一覧表示されるようになりました。

（注） テナントまたはコロケーショングループ用に作成された RBAC ユーザーは、ログイン情報を使用して Cisco SD-WAN Manager にログインできます。これらのユーザーは、テナントに関連付けられたサービスグループがクラスタにアタッチされた後、テナント固有のサービスチェーンと VNF 情報を表示できます。

コロケーション ユーザー グループからの RBAC ユーザーの削除

RBAC ユーザーを削除するには、ユーザーが Cisco SD-WAN Manager を使用して設定されている場合、コロケーショングループから RBAC ユーザーを削除します。ユーザーが TACACS サーバーを使用して認証されている場合は、TACACS サーバーのユーザーグループからユーザーの関連付けを解除します。

RBAC ユーザーが削除されると、そのユーザーはクラスタのデバイスにアクセスしたり、デバイスを監視したりできなくなります。RBAC ユーザーが Cisco SD-WAN Manager にログインしている場合、ユーザーを削除しても RBAC ユーザーはログアウトされません。

手順

ステップ 1 Cisco SD-WAN Manager メニューから **[Administration]** > **[Manage Users]** を選択します。

ステップ 2 削除する RBAC ユーザーをクリックします。

ステップ 3 削除する RBAC ユーザーの [...] をクリックし、[Delete] を選択します。

ステップ 4 [OK] をクリックして RBAC ユーザーの削除を確認します。

テナントの削除

テナントを削除するには、テナントに関連付けられているサービスグループを削除してから、テナントのコロケーショングループを削除します。

手順

ステップ 1 削除するテナントに関連付けられているサービスグループのリストを見つけます。「View Service Groups」を参照してください。

（注） テナントは、同じコロケーショングループに関連付けられた1つ以上のRBACユーザーを持つコロケーショングループです。サービスグループの構成ページでは、テナントのコロケーショングループを表示できます。

ステップ 2 削除したいテナントのクラスタからサービスグループを切り離します。『クラスタ内のサービスグループの接続または切断 （106 ページ）』を参照してください。

（注） サービスグループを別のテナントに再利用する場合は、サービスグループに関連付けられているコロケーショングループを変更します。サービスグループを削除した場合は、再作成する必要があります。

ステップ 3 テナントのコロケーショングループを削除します。『Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide』の「Manage a User Group」トピックを参照してください。

テナント コロケーション クラスタの管理

サービスプロバイダーは、次の管理タスクを実行できます。

- クラスタのアクティブ化：サービスプロバイダーは、デバイス、リソースプール、システム設定を構成し、マルチテナントモードまたは共有モードでクラスタをアクティブ化できます。「Create and Activate Clusters」を参照してください。
- サービスグループを作成し、RBAC ユーザーをコロケーショングループに関連付ける：サービスプロバイダーは、コロケーショングループを作成し、RBACユーザーをコロケーショングループに関連付け、サービスグループを作成し、サービスグループをマルチテナントモードのコロケーショングループに関連付け、サービスグループを特定のクラスタに接続できます。「Create Service Chain in a Service Group」を参照してください。

（注） サービスプロバイダーは、テナントごとに特定のサービスグループを関連付ける必要があります。

- VMパッケージの作成：サービスプロバイダーは、VMパッケージを作成してCisco SD-WAN Managerリポジトリにアップロードできます。同じパッケージを使用して、複数のテナントのサービスチェーンに VNF をプロビジョニングできます。

（注） サービスグループがコロケーショングループに関連付けられている場合、VNF の構成に使用される VM パッケージ作成の SR-IOV オプションは無視されます。マルチテナントモードでは、VNF パッケージは VXLAN を使用した OVS-DPDK のみをサポートします。

- サービスチェーンとテナントの VNF を監視する：サービスプロバイダーは、すべてのテナントサービスチェーンを監視し、これらのサービスチェーンに関連付けられているテナントとともに、正常でないサービスチェーンを特定できます。サービスプロバイダーは、Cisco SD-WAN Manager または CSP デバイスからログを収集し、テナントに通知することもできます。
- Cisco CSP デバイスの追加と削除：サービスプロバイダーは、コロケーションクラスタを管理するために、CSP デバイスを追加または削除できます。

テナント機能

テナントとしてのコロケーションクラスタの管理

すべてのテナントは、サービスチェーンとサービスチェーンに関連付けられている VM を監視し、サービスチェーンで正常性の問題が発生した場合はサービスプロバイダーと協力する必要があります。テナントは、テナントに属するサービスチェーンの一部である VNF のイベントまたはアラームのみを監視できます。

テナントには管理者権限がなく、サービスプロバイダーが作成するサービスチェーンのみを表示できます。テナント監視ウィンドウには、テナントがサービスチェーンを表示しているときに、対応するコロケーショングループが表示されます。テナントは、次のタスクを実行できます。

1. RBAC ユーザー名とパスワードを入力してテナントとして Cisco SD-WAN Manager にログインします。
2. VNF の正常性とともに、テナントサービスチェーンの正常性を表示および監視します。さまざまなサービスチェーンの正常性ステータスの詳細については、Cloud OnRamp Colocation クラスタのモニター （127 ページ）を参照してください。

   [Monitor.Network] ウィンドウで、サービスチェーンの [Diagram] をクリックして、すべてのテナントサービスグループとサービスチェーンと VNF をデザインビューに表示します。
3. テナントの VNF 正常性を表示します。
   1. [Monitor] ウィンドウで、[Network Functions] をクリックします。
   2. [Virtual NF] テーブルから VNF 名をクリックします。

左側のペインで、[CPU Utilization]、[Memory Utilization]、および [Disk Utilization] をクリックして、VNF のリソース使用率を監視します。

左ペインから VM 固有のアラームとイベントを表示することもできます。

4. VNF を開始、停止、またはリブートします。
   1. [Monitor] ウィンドウで、[Virtual NF] テーブルから VNF 名をクリックします。
   2. クリックした VNF 名について、[...] をクリックし、次のいずれかの操作を選択します。
      - [Start]
      - [Stop]
      - [Restart]

共同管理されたマルチテナント環境でのコロケーション クラスタ デバイスと Cisco Catalyst SD-WAN デバイスのモニター

始める前に

- サービスプロバイダー Cisco SD-WAN Manager を使用してサービスチェーンを作成する場合、サービスプロバイダーは、サービスチェーン内の Cisco Catalyst SD-WAN VM の正しい UUID とデバイス OTP が入力されていることを確認する必要があります。サービスプロバイダーはテナントオーバーレイにアクセスできないため、テナントはこの情報を提供する必要があります。
- サービスプロバイダーがサービスグループをコロケーションクラスタから切り離す場合、サービスプロバイダーは、テナント Cisco SD-WAN Manager を使用して対応する VM デバイスをデコミッションする必要があることをテナントに通知する必要があります。
- サービスプロバイダーがサービスグループをコロケーションクラスタに再アタッチする必要がある場合は、Cisco Catalyst SD-WAN VM の新しい OTP を入力する必要があります。この OTP はテナントによって提供されます。サービスプロバイダー Cisco SD-WAN Manager のサービスグループを編集して、Cisco SD-WAN VM の新しい OTP を保存する必要があります。

手順

ステップ 1 サービスチェーンを作成するときに、テナントの Cisco Catalyst SD-WAN デバイスをサービスプロバイダーのサービスグループに関連付けます。「Create Service Chain in a Service Group」を参照してください。

ステップ 2 サービスプロバイダー Cisco SD-WAN Manager からの VNF を監視します。「Monitor Cloud OnRamp Colocation Clusters」を参照してください。

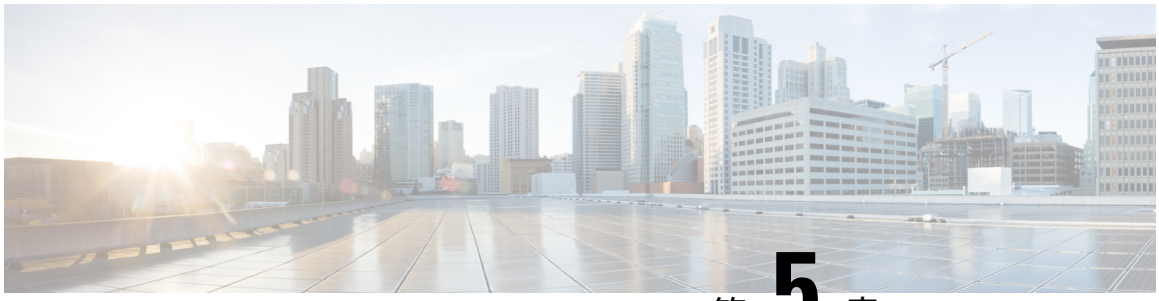
ステップ 3 テナント Cisco SD-WAN Manager からの VNF の Cisco Catalyst SD-WAN デバイスに関する情報をモニターします。

（注） サービスプロバイダーは、VNF の Cisco Catalyst SD-WAN デバイスに関する情報をサービスプロバイダーの **[Configuration]** > **[Devices]** ウィンドウの [WAN Edge List] から表示できません。これらのデバイスはテナントによって制御されているためです。

第 部

Cloud OnRamp for SaaS

- Cloud OnRamp for SaaS、Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降 （149 ページ）
- アプリケーションリスト （227 ページ）
- Cloud OnRamp for SaaS、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r （235 ページ）



第 5 章

Cloud OnRamp for SaaS、Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降

（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。

表 *48 :* 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイスでの Cloud OnRamp for SaaS 用の Office 365 トラフィックカテゴリの指定のサポート	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、Cisco IOS XE Catalyst SD-WAN デバイスの既存の Cloud OnRamp for SaaS 設定ワークフローを更新します。この機能により、Microsoft が定義した Office 365 トラフィックカテゴリに従って、ベストパス選択の使用を一部またはすべての Office 365 トラフィックに制限することができます。

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイスでの Office 365 ベストパス選択用のアプリケーション フィードバック メトリック	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	この機能は、Office 365 トラフィックのベストパス選択アルゴリズムへの入力として、新しいメトリックを追加します。この新しい入力には、Microsoft Cloud Services からのベストパスメトリックが含まれます。この機能により、ベストパスアルゴリズムで使用される入力データの詳細なログを表示するための新しいページも提供されます。
複数のインターフェイス間でのロードバランシング	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能により、複数の DIA インターフェイス間でクラウドアプリケーションのトラフィックを分散する機能が追加されます。
ゲートウェイサイトの VPN 0 インターフェイスを介した Cloud OnRamp for SaaS のプローブのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	Cloud OnRamp for SaaS は、（プローブ）ルーティングパスのパフォーマンスをテストして、特定のクラウドアプリケーションのトラフィックに最適なルーティングパスを見つけます。クラウドアプリケーションのトラフィックに最適なルーティングパスを使用すると、アプリケーションのパフォーマンスが最適化されます。 この機能により、Cloud OnRamp for SaaS は、指定されたクラウドアプリケーションのトラフィックに使用するベストパスの決定の一環として、ゲートウェイサイトの VPN 0 インターフェイスを介してプローブできます。これにより、ベストパスのプローブが拡張され、インターネットに接続されている使用可能なインターフェイスがさらに多く含まれるようになります。 この機能により、Cloud OnRamp for SaaS は、サービス VPN（VPN 1、VPN 2 など）またはトランスポート VPN（VPN 0）のどちらが使用されているかにかかわらず、ゲートウェイサイトのインターフェイスをプローブできます。これは、VPN 0 インターフェイスを使用してインターネットに接続するゲートウェイサイトを介して、ブランチサイトが排他的または部分的にインターネットに接続する場合に役立ちます。

機能名	リリース情報	説明
Webex の Cloud OnRamp for SaaS のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能により、Cloud OnRamp for SaaS でサポートされるクラウドアプリケーションのリストに Webex が追加されます。Cloud OnRamp for SaaS が、Webex クラウドサーバーへの最適なネットワークパスを決定できます。Cisco SD-WAN Manager が、地理的リージョン別に整理された Webex サーバーのリストを定期的にダウンロードします。Cloud OnRamp for SaaS は、このサーバーリストを使用して、さまざまなリージョンの Webex トラフィックに最適なネットワークパスを計算するために役立てます。
Microsoft 365 SharePoint および Teams のトラフィックに対する Microsoft テレメトリメトリックの使用のサポート。	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco SD-WAN リリース 20.7.1	この機能により、Microsoft 365 SharePoint および Teams の Microsoft テレメトリメトリックを使用するためのサポートが追加されます。Cloud OnRamp for SaaS が、Office 365 トラフィックのベストパスを決定するときにメトリックデータを使用します。
Microsoft テレメトリの詳細の表示と Office 365 トラフィックのアプリケーションサーバー情報の表示	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1	この機能により、Microsoft テレメトリの使用を選択した場合に、Cloud OnRamp for SaaS が Microsoft Office 365 トラフィックのベストパスを決定する方法の可視性が向上します。 拡張機能の 1 つに、Microsoft がさまざまなインターフェイスの接続品質を、特に Office 365 トラフィックのさまざまなタイプ（サービスエリアと呼ばれる）に対してどのように評価しているかを示すチャートがあります。これは、Office 365 のパフォーマンスの問題のトラブルシューティングに役立ちます。 他には、[SD-AVC Cloud Connector] ページが追加されます。このページでは、Cisco Catalyst SD-WAN が Microsoft Cloud から受信する Microsoft URL および IP エンドポイントとカテゴリのリストが表示されます。
特定のポリシーのトラフィックカテゴリとサービスエリアの設定	Cisco vManage リリース 20.9.1 Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a	AAR ポリシーを個別に編集して、特定の AAR ポリシーの指定された Microsoft 365 トラフィックカテゴリとサービスエリアを変更することができます。

機能名	リリース情報	説明
特定のサイトの特定のアプリケーションに対する Cloud OnRamp for SaaS の動作の有効化	Cisco vManage リリース 20.9.1 Cisco IOS XE リリース 17.2.1	この機能により、AAR ポリシーシーケンスを選択的に削除して、特定のサイトの特定のアプリケーションでの Cloud OnRamp for SaaS の動作を除外することができます。
Microsoft 365 トラフィックの可視性の向上	Cisco vManage リリース 20.9.1 Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a	この機能により可視性が向上し、Cloud OnRamp for SaaS によって処理される Microsoft 365 トラフィックの詳細をモニターできます。
Microsoft 365 トラフィックのベストパスの決定での Microsoft テレメトリデータの包含または除外のためのオプション	Cisco vManage リリース 20.9.1	この機能により、Cloud OnRamp for SaaS がベストパスの決定で Microsoft テレメトリデータを考慮するかどうかを選択することができます。このオプションを無効にしても、Cisco SD-WAN Analytics ダッシュボードで Microsoft テレメトリデータを表示することはできますが、ベストパスの決定には影響しません。
Webex トラフィックの可視性と制御の向上	Cisco vManage リリース 20.10.1 Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a	この機能により、Webex トラフィックの可視性と制御に関していくつかの改善が行われます。これには、以下が含まれます。 • Cisco SD-AVC を使用した Webex トラフィックのディープ パケット インスペクション（DPI）の管理 • Webex トラフィックのパフォーマンスに関する詳細情報を提供するための、サーバー側 Webex メトリックの受信 • Webex トラフィックに対して Cloud OnRamp for SaaS を有効にするための、アプリケーション認識型ルーティング（AAR）ポリシーへの単一シーケンスのみの追加
ループバック、ダイヤラ、およびサブインターフェイスの Cloud OnRamp for SaaS のサポートの追加	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	この機能により、Cloud OnRamp for SaaS のサポートが、ループバック、ダイヤラ、およびサブインターフェイスを含む SD-WAN 対応 WAN インターフェイスに拡張されます。また、ループバック、ダイヤラ、およびサブインターフェイスでの TLOC 拡張と SIG のサポートも追加されます。

機能名	リリース情報	説明
Cloud OnRamp for SaaS の最適化からのデータプレフィックスの除外のためのオプション	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	Cloud OnRamp for SaaS の最適化から除外する IP プレフィックスのリストを定義できます。これは、SaaS アプリケーションがオンプレミスまたはプライベートクラウドでホストされている場合に役立ちます。
DIA トラッカーと Cloud OnRamp for SaaS の関連付けによる高速フェールオーバーの有効化	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	失敗したルートからのフェールオーバーを高速化するために、トラッカーを DIA またはゲートウェイサイトに関連付けることができます。トラッカーは、Cloud OnRamp for SaaS のプローブよりも高速にインターフェイスでのインターネット接続障害を検出します。

多くの組織は、ビジネスに不可欠な機能を Software-as-a-Service（SaaS）アプリケーションに依存しています。これらのクラウドベースのサービスには、Amazon AWS、Box、Dropbox、Google Apps、Office 365 などの、多くのサービスがあります。クラウドベースのサービスとして、これらの SaaS アプリケーションは、インターネット接続を介して使用可能な独自のリモートサーバーと通信する必要があります。

リモートサイトでは、SaaS アプリケーションによって次のような特別な課題が発生する可能性があります。

- **パフォーマンス**：ブランチオフィスなどのリモートサイトが、データセンターなどの一元化された場所を介して SaaS トラフィックをルーティングすると、パフォーマンスが低下し、遅延が発生してユーザー体験に影響を与えます。
- **ルーティングを最適化できない**：ネットワーク管理者が、これらの SaaS アプリケーションのパフォーマンスを可視化できない場合や、SaaS トラフィックのルーティングをより効率的なパスに変更できない場合があります。

Cloud OnRamp for SaaS（旧称 CloudExpress サービス）は、これらの課題に対処します。これにより、特定の SaaS アプリケーションおよびインターフェイスを選択し、Cisco Catalyst SD-WAN が指定されたインターフェイスを使用して各 SaaS アプリケーションのパフォーマンスが最も高いパスを決定できるようになります。たとえば、以下を有効にすることができます。

- ブランチサイトでのダイレクト インターネット アクセス（DIA）接続を介したルーティング（使用可能な場合）
- 地域のデータセンターなどの、ゲートウェイの場所を介したルーティング

クラウドトラフィックのベストパスを確保することは重要です。SD-WAN は各 SaaS アプリケーションの使用可能な各パスを継続的にモニターするため、1 つのパスで問題が発生した場合は、SaaS トラフィックを動的に調整して、より適切なパスに移動させることができます。

• Cloud onRamp for SaaS に関する情報 （154 ページ）
• Cloud onRamp for SaaS でサポートされるデバイス （167 ページ）
• Cloud OnRamp for SaaS の前提条件 （167 ページ）
• Cloud onRamp for SaaS の制約事項 （171 ページ）
• Cloud onRamp for SaaS のユースケース （173 ページ）
• Cloud onRamp for SaaS の設定 （175 ページ）
• Cloud onRamp for SaaS の確認 （198 ページ）
• Cloud onRamp for SaaS のモニター （201 ページ）
• SIG トンネル経由の Cloud onRamp for SaaS （209 ページ）
• Cloud OnRamp for SaaS のトラブルシューティング （220 ページ）

Cloud onRamp for SaaS に関する情報

Cloud onRamp for SaaS を使用する一般的なシナリオ

SD-WAN を使用している組織の場合、通常、ブランチサイトはデフォルトで SaaS アプリケーション トラフィックを SD-WAN オーバーレイ リンク経由でデータセンターにルーティングします。データセンターから、SaaS トラフィックは SaaS サーバーに到達します。

たとえば、中央データセンターとブランチサイトがある大規模な組織で、従業員がブランチサイトで Office 365 を使用する場合があります。デフォルトでは、ブランチサイトの Office 365 トラフィックは、SD-WAN オーバーレイ リンクを介して中央データセンターにルーティングされ、そこから Office 365 クラウドサーバーにルーティングされます。

シナリオ 1：ブランチサイトにダイレクト インターネット アクセス（DIA）接続がある場合は、データセンターをバイパスしてその直接ルートを介して SaaS トラフィックをルーティングすることで、パフォーマンスを向上させることができます。

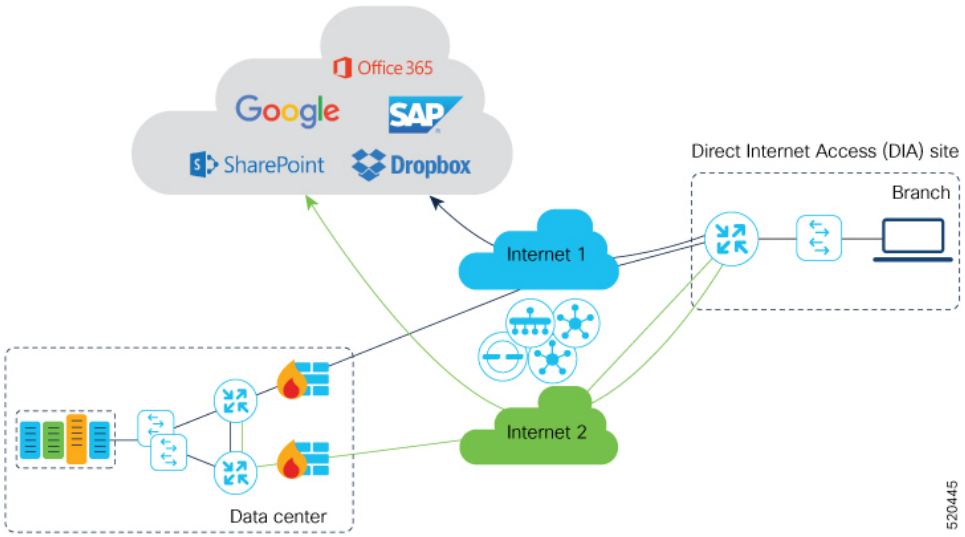
シナリオ 2：DIA リンクがあるゲートウェイサイトにブランチサイトが接続する場合、SaaS トラフィックがゲートウェイサイトの DIA を使用できるようにすることができます。

シナリオ 3：ハイブリッド方式。

シナリオ 1：ダイレクト インターネット アクセス リンクを介したクラウドアクセス

このシナリオでは、次の図に示すように、ブランチサイトに 1 つ以上のダイレクト インターネット アクセス（DIA）リンクがあります。

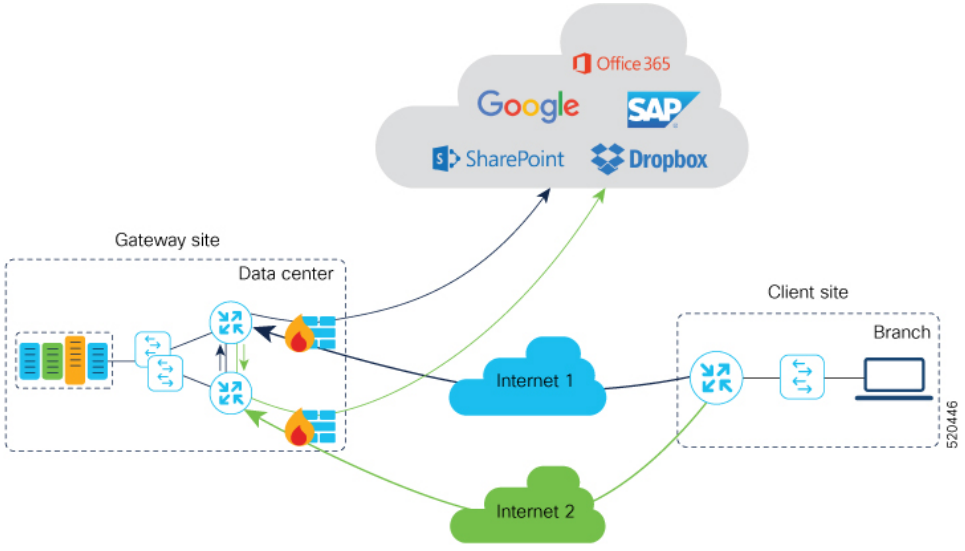
Cloud onRamp for SaaS を使用すると、SD-WAN は、DIA リンクまたは SD-WAN オーバーレイ リンクを介して、各 SaaS アプリケーションに最適な接続を選択できます。最適な接続は、SaaS アプリケーションによって異なる場合があることに注意してください。たとえば、Office365 のトラフィックはある 1 つのリンクを介すると高速になり、Dropbox のトラフィックは別のリンクを介すると高速になる可能性があります。



シナリオ 2：ゲートウェイサイトを介したクラウドアクセス

このシナリオでは、ブランチサイトにゲートウェイサイトへの直接接続が 1 つ以上あり、ゲートウェイサイトにインターネットへのリンクがあります。

Cloud OnRamp for SaaS を使用すると、Cisco Catalyst SD-WAN は、ゲートウェイサイトを介して、各 SaaS アプリケーションに最適な接続を選択できます。ブランチサイトが複数のゲートウェイサイトに接続している場合、異なるゲートウェイサイトを通過する場合でも、SD-WAN は各 SaaS アプリケーションについて SaaS トラフィックがベストパスを使用するようにします。



シナリオ 3：ハイブリッドアプローチ

このシナリオでは、ブランチサイトには、ダイレクトインターネットアクセス（DIA）リンクと、インターネットへのリンクもあるゲートウェイサイトへのリンクの両方があります。

Cloud OnRamp for SaaS を使用すると、Cisco Catalyst SD-WAN は、DIA リンクまたはゲートウェイサイトを介して、各 SaaS アプリケーションに最適な接続を選択できます。

Office 365 トラフィックカテゴリの指定

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は、次のオプションを使用して、Cloud onRamp for SaaS のパス選択を一部またはすべての Office 365 トラフィックに適用するように制限できます。

- **Optimize** トラフィック
- **Optimize** および **Allow** トラフィック
- すべての Office 365 トラフィック

これらのオプションは、Microsoft が次のように定義している Office 365 トラフィックの 3 つのカテゴリに対応しています。

- Optimize：ネットワークパフォーマンス、遅延、および可用性の影響を最も受けやすいトラフィック。
- Allow：ネットワークパフォーマンス、遅延、および可用性の影響を受けづらいトラフィック。
- Default：ネットワークパフォーマンスの影響を受けないトラフィック。

Office 365 カテゴリでトラフィックを指定するには、[Administration] > [Settings] で Cisco SD-AVC Cloud Connector コンポーネントを有効にする必要があります。

ベストパスの決定

Cloud OnRamp for SaaS は、次のソースから入力を取得するアルゴリズムを使用して、各アプリケーションのベストパスを選択します。

	入力	すべてのクラウド アプリケーション トラフィック	Office 365 トラフィック
1	パスプローブに基づく Cloud OnRamp for SaaS のメトリック	対応	対応
2	アプリケーション応答時間（ART）のメトリック	非対応	対応（有効な場合）
3	Microsoft テレメトリのメトリック	非対応	対応（有効な場合）

Office 365 トラフィックでは、ベストパスの決定で考慮されるメトリックのログを表示できます。このメトリックは、この情報のみを表示するように特別に設計された Cisco SD-WAN Analytics のページに表示され、Cisco SD-WAN Manager から直接使用できます。

複数のインターフェイス間でのロードバランシング

Cloud onRamp for SaaS は、クラウドトラフィックのタイプごとに最適なネットワークパスを決定できます。ただし、ブランチサイトにある WAN エッジデバイスの複数のダイレクト インターネット アクセス（DIA）インターフェイスがクラウドアプリケーションに対して許容可能なパフォーマンスを提供している場合、Cloud onRamp for SaaS は最大 3 つのインターフェイス間でロードバランシングを使用して、パフォーマンスをさらに向上させることができます。

WAN エッジデバイスの複数のインターフェイス間でのロードバランシングを有効にすると、Cloud onRamp for SaaS によって管理されるすべてのクラウドアプリケーションに対してロードバランシングが有効になります。クラウドアプリケーションのベストパスインターフェイスを決定した後、Cloud onRamp は他のインターフェイスのパフォーマンス統計を比較します。ロードバランシング用に別のインターフェイスを使用するには、次の条件を満たす必要があります。

- インターフェイスのパケット損失値は、ベストパスインターフェイスのパケット損失値から設定値（%）を超えて変動することはできません。ベストパスインターフェイスのパケット損失値を小さく設定して、その値に非常に近いインターフェイスにのみロードバランシングを制限するか、または値を大きく設定して、パケット損失がそれよりも大きいことが予想されるインターフェイスを広く含めることができます。
- インターフェイスの遅延値は、ベストパスインターフェイスの遅延値から設定値（ミリ秒）を超えて変動することはできません。ベストパスインターフェイスの遅延値を小さく設定して、その値に非常に近いインターフェイスにのみロードバランシングを制限するか、または値を大きく設定して、遅延がそれよりも大きいことが予想されるインターフェイスを広く含めることができます。

必要に応じて、単一のホストからのすべてのトラフィックが単一のインターフェイスを使用するようにするオプションを選択できます。たとえば、DNS とアプリケーションのトラフィックが同じパスを使用するようにします。

ゲートウェイサイトの VPN 0 インターフェイスを介した Cloud OnRamp for SaaS のプローブに関する情報

ブランチサイトは、ブランチサイト自体での 1 つ以上のダイレクト インターネット アクセス（DIA）インターフェイスを介してインターネットに接続することも、インターネットに接続するためにサービス VPN または VPN 0 を使用できるゲートウェイサイトを介してインターネットに接続することもできます。

ブランチサイトの DIA インターフェイスのプローブに加えて、Cloud OnRamp for SaaS は、指定されたクラウドアプリケーションのトラフィックに使用するベストパスを決定する際に、インターフェイスがサービス VPN（VPN 1、VPN 2 など）またはトランスポート VPN（VPN 0）を使用しているかどうかにかかわらず、ゲートウェイサイトのインターフェイスをプローブすることができます。これは、ブランチサイトがゲートウェイサイトを介してインターネットに接続する場合に役立ちます。

ゲートウェイサイトを使用するように Cloud OnRamp for SaaS を設定する場合は、次の図に示すように、ゲートウェイサイトがサービス VPN または VPN 0 を使用してインターネットに接続するかどうかを指定します。

図 *17*: サービス *VPN* を使用してインターネットに接続するゲートウェイサイトに接続するブランチサイト

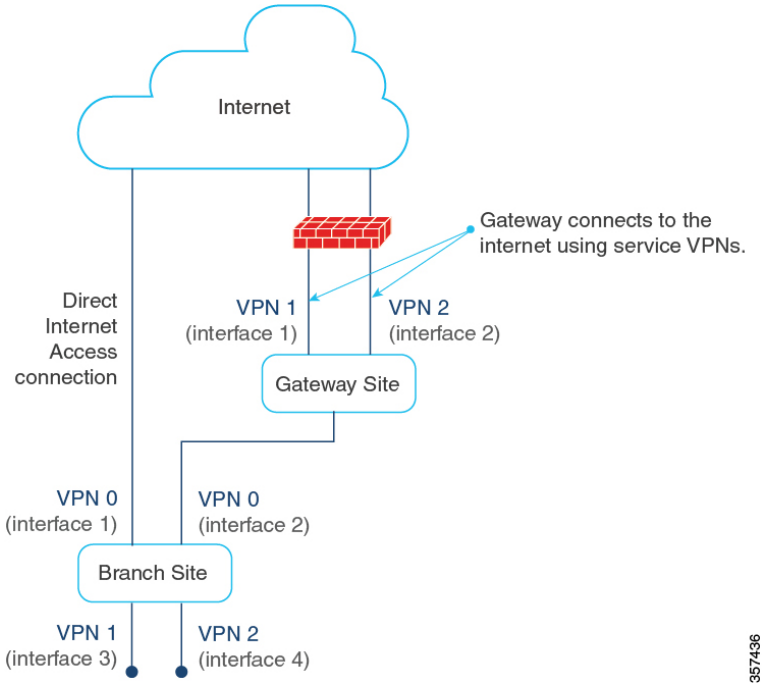
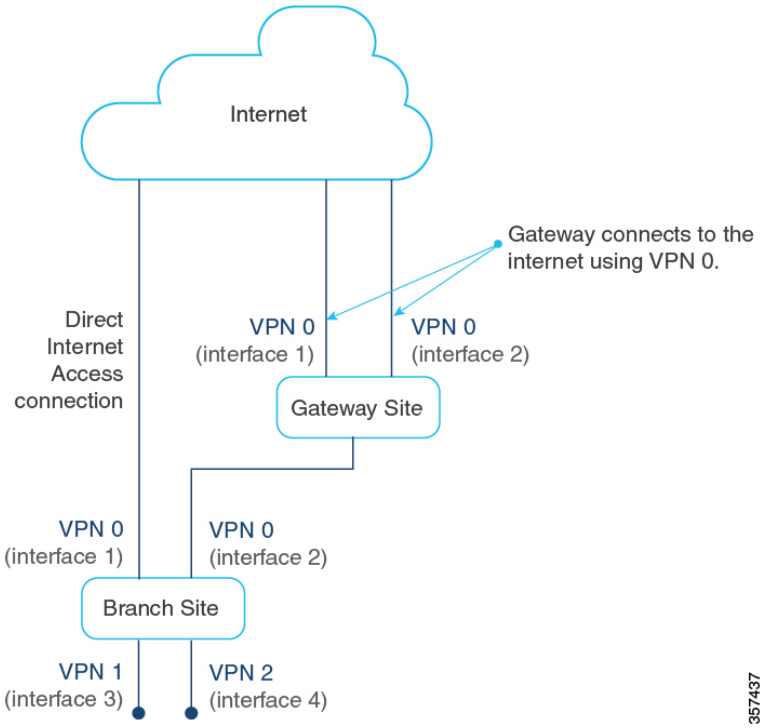


図 *18 : VPN 0* を使用してインターネットに接続するゲートウェイサイトに接続するブランチサイト



Webex の Cloud OnRamp for SaaS のサポートに関する情報

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco vManage リリース 20.7.1

アプリケーションの Cloud OnRamp for SaaS によるベストパス決定を有効にすると、Cisco SD-WAN Manager は、アプリケーションの Cloud OnRamp for SaaS 機能をサポートするために、アクティブな集中管理型ポリシー内のアプリケーション認識型ポリシーの一致条件を更新します。ほとんどのアプリケーションでは、一致条件を後から更新する必要はありません。

Webex の場合、Cloud OnRamp for SaaS は他のほとんどのアプリケーションよりも複雑な方法を使用します。Cloud OnRamp for SaaS は、世界中の Webex サーバーのリストを維持しています。Webex の Cloud OnRamp for SaaS によるベストパス決定を有効にすると、Cloud OnRamp for SaaS は世界中の各 Webex サーバーのベストパスを決定します。それぞれのリージョンの Webex サーバーに対応するために、アプリケーション認識型ポリシーに一致条件が追加されます。これにより、接続する必要が生じる可能性のある世界中の Webex サーバーへのベストパスが、Webex アプリケーションに提供されます。

表 *49 :* 他のアプリケーションの方法と比較した、*Webex* のベストパス決定方法

アプリケーション	Cloud OnRamp for SaaS の方法
ほとんどのクラウドアプリケーション	Cloud OnRamp for SaaS は、デバイスに設定された DNS サーバーを使用して、DNS 応答によって決定された、クラウドアプリケーションに最も関連性の高いサーバーへのベストパスを決定します。
Webex	Cloud OnRamp for SaaS は、世界中の Webex サーバーのリストを維持し、使用可能なすべての Webex サーバーのベストパスを決定します。

Webex サーバーの最新リストの維持

Webex サーバーの最新リストを維持するために、Cisco SD-WAN Manager は定期的に最新のサーバー情報を取得し、情報に変更があるかどうかを判断します。Cisco SD-WAN Manager が Webex サーバー情報に変更があることを検出すると、Cloud OnRamp for SaaS のダッシュボードに通知が表示され、Webex サーバー情報を同期するように求められます。この通知は、Cloud OnRamp for SaaS のダッシュボードページに表示されるダイアログボックスと、ダッシュボードに表示される Webex アプリケーションペインのメッセージに表示されます。

SD-AVC を使用したトラフィックの分類

Cisco vManage リリース 20.10.1 および Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a 以降、Cloud OnRamp for SaaS は Cisco SD-AVC を使用して Webex トラフィックのディープ パケット インスペクション（DPI）を管理し、トラフィックの最初のパケットの分類を可能にしています。これを行うには、**[Administration]** > **[Settings]** で SD-AVC を有効にする必要があります。

最初のパケットから Webex トラフィックフローを分類することで、Cloud OnRamp for SaaS 制御ポリシーは、ルータによって処理されるより多くの Webex トラフィックに対して機能することができます。

DPI に SD-AVC を使用する利点の 1 つは、一部の Webex トラフィックがクラウドサーバーへの最適ではないパスを使用する可能性があるという既知の問題を解決できることです。このシナリオでは、ある地理的リージョンの Webex サーバーが、別のリージョンの Webex サーバーと同じ IP アドレスの一部を使用する場合があります。以前のリリースでは、この IP の重複により、ある地理的リージョン宛ての Webex トラフィックが、別のリージョンへのトラフィックに最適なエッジ デバイス インターフェイスを使用する可能性がありました。トラフィックフローは正しく動作し、正しい宛先に到達しましたが、トラフィックは最適ではないパスを使用しました。Cisco vManage リリース 20.10.1 では、これは解決済みです。

シンプルなアプリケーション認識型ルーティングポリシー

Cisco vManage リリース 20.10.1 および Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a 以降では、Cloud OnRamp for SaaS を有効にして Webex トラフィックに対して動作させると、Cisco SD-WAN Manager は以前のリリースのような一連のシーケンスではなく、単一のシーケンスのみをアプリケーション認識型ルーティング（AAR）ポリシーに追加します。Cisco Catalyst

SD-WAN は、より多くのシーケンスステートメントを使用して Webex の Cloud OnRamp for SaaS を有効にする、既存のレガシー AAR ポリシーを引き続きサポートしています。

（多数のシーケンスを使用して Webex トラフィックの Cloud OnRamp for SaaS を有効にする）レガシー AAR ポリシーを使用している場合、Cloud OnRamp for SaaS で Webex を無効にすると、Webex トラフィックに対応する一連のシーケンスが AAR ポリシーから削除されます。Webex を再度有効にすると、Cloud OnRamp for SaaS は、AAR ポリシーに単一のシーケンスのみを追加する、新しいより効率的な方法を使用します。

新しいポリシーモデルに関連する制約事項の詳細については、Webex アプリケーションの制約事項 （172 ページ）を参照してください。

Webex サーバー側メトリック

Cisco vManage リリース 20.10.1 および Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a 以降では、Webex サーバーは、音声やビデオなどの Webex トラフィックのさまざまな側面のパフォーマンスを示すメトリックを Cisco SD-WAN Analytics に提供できます。このメトリックは、Cloud OnRamp for SaaS が損失や遅延などのメトリックを決定するためにパスプローブを使用して収集するトラフィックメトリックを拡張します。Webex サーバーとプローブからの集約情報は、ネットワーク内の Webex トラフィックのパフォーマンスを理解するための有用なツールとなります。集約されたメトリックの表示については、モニタリング対象アプリケーションの詳細の表示 （201 ページ）を参照してください。

Cloud OnRamp for SaaS は、Webex トラフィックのベストパスを決定するときはメトリックデータを使用しません。Webex サーバー側メトリックの前提条件 （170 ページ）と、「Webex サーバー側メトリックの有効化」を参照してください。

SD-AVC Cloud Connector に関する情報

サポート対象の最小リリース：Cisco vManage リリース 20.8.1

Cisco Catalyst SD-WAN は、SD-AVC Cloud Connector と呼ばれるコンポーネントを使用して、Office 365 トラフィックを処理する Microsoft アプリケーションサーバーに関する情報を Microsoft Cloud から収集します。この情報には、トラフィックのトランスポートプロトコルと、トラフィックを管理するアプリケーションサーバーのドメイン名、IP アドレス、およびポートが含まれます。このサーバー情報により、ネットワークトラフィックの識別プロセスが改善されます。たとえば、最初のパケットからトラフィックを識別できるようになります。ポリシーは多くの場合、最初のパケットからすべてのトラフィックを照合できるため、トラフィック識別を改善すると、アプリケーション認識型ルーティングポリシーの有効性が向上します。

[SD-AVC Cloud Connector] ページでは、Office 365 トラフィックに使用されるアプリケーションサーバーが可視化されます。このページには、Cisco Catalyst SD-WAN が Office 365 トラフィック用に収集したサーバー情報のテーブルがあります。このテーブルでは、たとえば、*-admin.sharepoint.com で表されるドメインが SharePoint トラフィックに対応していることが示されている場合があります。この場合、connect-admin.sharepoint.com などの、それらのドメインに含まれる宛先ドメインを持つトラフィックフローは、フローの最初のパケットから SharePoint トラフィックとして識別できます。

Office 365 トラフィックのパススコアの表示に関する情報

サポート対象の最小リリース：Cisco vManage リリース 20.8.1

Office 365 トラフィックに対して、Exchange、SharePoint、Skype などの各 Microsoft サービスエリアについて Microsoft テレメトリによって提供されたパススコア（[OK]、[NOT-OK]、または [INIT]）が表示されるチャートを表示することができます。このチャートには、使用可能な各インターフェイスの時間の経過に伴うパススコアが表示されます。

パス スコア履歴の表示は、Office 365 トラフィックのネットワークパフォーマンスの問題をトラブルシューティングする場合に役立ちます。たとえば、Skype トラフィックなどの一部のタイプのトラフィックについて、Microsoft が特定のインターフェイスを一貫して [NOT-OK] と評価するかどうかを判断する場合などです。その場合は、インターフェイスが一貫して低いパススコアを受け取っている理由を調査できます。

特定のポリシーのトラフィックカテゴリとサービスエリアの設定に関する情報

最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a

[Applications and Policy] ページで Microsoft 365 を有効にして、トラフィックカテゴリを選択すると、Cloud OnRamp for SaaS は選択したトラフィックカテゴリに従って Microsoft 365 トラフィックに対する Cloud OnRamp for SaaS の動作を有効にするためのシーケンスをすべてのアプリケーション認識型ルーティング（AAR）ポリシーに追加します。これらのシーケンスを AAR ポリシーに追加することで、選択したトラフィックカテゴリを使用して、このトラフィックに対する Cloud OnRamp for SaaS の動作が有効になります。

Cisco vManage リリース 20.9.1 以降では、AAR ポリシーのシーケンスを個別に編集して、特定の AAR ポリシーの指定された Microsoft 365 トラフィックカテゴリとサービスエリアを変更することができます。

（注） この機能は、Microsoft 365 アプリケーションでのみ使用できます。

特定のポリシーのトラフィックカテゴリとサービスエリアの設定の利点

個々の AAR ポリシーを編集することで、さまざまなポリシーでさまざまな Microsoft 365 のサービスエリアとトラフィックカテゴリに対して Cloud OnRamp for SaaS を有効にして動作させることができます。

特定のサイトの特定のアプリケーションに対するCloudOnRampforSaaSの動作の有効化に関する情報

最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE リリース 17.2.1

Cisco vManage リリース 20.9.1 以降では、Cloud OnRamp for SaaS を選択的に有効にして、他のサイトを除外しながら、特定のサイトの特定のアプリケーションに対して動作させることができます。[Applications and Policy] ページでアプリケーションを有効にすると、Cloud OnRamp for SaaS は選択したアプリケーションのトラフィックに一致する AAR ポリシーシーケンスを追加し、Cloud OnRamp for SaaS のベストパス計算に従ってトラフィックを転送します。これにより、すべてのサイトで Cloud OnRamp for SaaS の動作が有効になります。

特定のサイトのアプリケーションに対する Cloud OnRamp for SaaS の動作を除外するには、AAR ポリシーを編集し、AAR ポリシー内の特定のアプリケーションを削除します。これにより、AAR ポリシーを使用するサイトで、そのアプリケーションに対する Cloud OnRamp for SaaS のアクティビティが無効になります。

Microsoft 365 トラフィックでのみ機能する特定のポリシーのトラフィックカテゴリまたはサービスエリアの編集（「特定のポリシーのトラフィックカテゴリとサービスエリアの設定に関する情報」を参照）とは異なり、この機能を使用して任意の SaaS アプリケーションの有効化または除外ができます。

特定のサイトの特定のアプリケーションに対する Cloud OnRamp for SaaS の動作の有効化の利点

この機能により、ネットワーク内の各サイトで Cloud OnRamp for SaaS が動作するアプリケーションをサイトレベルできめ細かく制御できます。

Microsoft 365 SaaS トラフィックの可視性に関する情報

最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a

Cisco vManage リリース 20.9.1 では、アプリケーションの可視性が改善され、Cloud OnRamp for SaaS によって処理される Microsoft 365 トラフィックをより詳細にモニターできます。時間の経過に伴う Microsoft 365 トラフィックの量を、ダイレクト インターネット アクセス（DIA）リンクを使用したトラフィックの量と、ゲートウェイサイトを介してルーティングされた量の詳細とともに、グラフまたは表形式で表示することができます。モニタリングページには、Cloud OnRamp for SaaS の影響を受けないトラフィックの量も表示されます。

Microsoft 365 SaaS トラフィックの可視性の利点

Cloud OnRamp for SaaS がトラフィックをルーティングする方法の詳細の可視性は、トラフィックルーティングの問題をトラブルシューティングするときに役立ちます。

Microsoft 365 トラフィックのベストパスの決定での Microsoft テレメトリデータの包含または除外に関する情報

最小リリース：Cisco vManage リリース 20.9.1

Cisco vManage リリース 20.9.1 以降では、Cloud OnRamp for SaaS のベストパスの決定に、Microsoft 365 トラフィックの要因として Microsoft テレメトリデータを含めるかどうかを制御できます。

Microsoft 365（Office 365）トラフィックのテレメトリを有効にすると、[Application Feedback] ダイアログボックスに [Traffic Steering] チェックボックスが表示されます。ベストパスの決定での Microsoft テレメトリデータの使用を有効にするには、このチェックボックスをオンにします。詳細については、「Enable Application Feedback Metrics for Office 365 Traffic」を参照してください。

ベストパスの決定で Microsoft テレメトリデータを使用しないことを選択した場合でも、テレメトリデータを表示できます。Cisco vAnalytics を使用して、Microsoft 365 アプリケーションに関連するテレメトリデータと、デバイスで行われたベストパスの決定に関する詳細情報を表示できます。Cisco SD-WAN Analytics の詳細については、「Cisco vAnalytics」を参照してください。

Microsoft が Microsoft 365 トラフィックのテレメトリを提供できるようにする方法の詳細については、「Enable Microsoft to Provide Telemetry for Office 365 Traffic」を参照してください。

Cisco SD-WAN Manager のアップグレード後

Cisco SD-WAN Manager の以前のリリースで Microsoft テレメトリを有効にしていて、Cisco vManage リリース 20.9.1 にアップグレードした場合、Cloud OnRamp for SaaS ではベストパスの決定での Microsoft テレメトリデータの使用は自動的には有効になりません。デバイスがベストパスの決定に Microsoft テレメトリを使用するようにするには、そのオプションを設定している場合は、次のいずれかを実行します。

- Microsoft 365 トラフィックの Microsoft テレメトリを無効にしてから有効にします。「Enable Application Feedback Metrics for Office 365 Traffic」を参照してください
- Microsoft 365 トラフィックのモニタリングを無効にしてから有効にします。「Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager」を参照してください
- 次の手順を実行します。

1. サイトとゲートウェイをデタッチしてからアタッチします。「クライアントサイトの設定」を参照してください。
2. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for SaaS]** を選択します。
3. [Manage Cloud OnRamp for SaaS] ドロップダウンリストで、[Applications and Policy] を選択します。[Applications and Policy] ページには、すべての SaaS アプリケーションが表示されます。
4. [Save Applications and Next] をクリックします。これにより、各サイトのデバイスにトラフィックステアリング値が送信されます。

（注） Cisco vManage リリース 20.9.1 以降では、Microsoft ポータルでエッジデバイスのパブリックシステム IP を入力できます。詳細については、「Enable Microsoft to Provide Telemetry for Office 365 Traffic」のステップ 2-c を参照してください。

ループバック、ダイヤラ、およびサブインターフェイスの Cloud OnRamp for SaaS のサポートに関する情報

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a

Cloud OnRamp for SaaS は、ループバック、ダイヤラ、およびサブインターフェイスをサポートしています。これらのインターフェイスで TLOC 拡張と SIG を設定できます。

要件に応じて、Cisco IOS XE Catalyst SD-WAN デバイス上でさまざまなインターフェイスを設定できます。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。

ループバック インターフェイスおよびダイヤラインターフェイスでサポートされるネットワークアドレス変換（NAT）設定の詳細については、「Configure NAT」を参照してください。

データプレフィックスの除外に関する情報

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 17.9.1a、Cisco Catalyst SD-WAN Manager リリース 20.13.1

Cloud OnRamp for SaaS の最適化から除外する宛先 IP プレフィックスのリストを定義できます。データプレフィックスの除外リストは、すべての SaaS アプリケーションに適用することも、特定のアプリケーションに個別に適用することもできます。

一般的な用途は、オンプレミス SaaS アプリケーションサーバーまたはプライベートクラウドでホストされる SaaS アプリケーションサーバーのプレフィックスを除外することです。たとえば、ローカルのオンプレミス SharePoint サーバーがあり、SharePoint トラフィックを最適化するように Cloud OnRamp for SaaS を設定する場合、Cloud OnRamp for SaaS の最適化からローカル SharePoint サーバーのプレフィックスを除外することができます。これにより、SharePoint トラフィックを内部でルーティングでき、Cloud OnRamp for SaaS の影響を受けなくなります。

フェールオーバーの高速化のためのトラッカーの使用に関する情報

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 17.13.1a、Cisco Catalyst SD-WAN Manager リリース 20.13.1

Cloud OnRamp for SaaS は、使用可能なすべてのインターフェイスでプローブを使用してベストパスの決定を実行します。インターフェイスでのインターネット接続に障害が発生すると、Cloud OnRamp for SaaS は別のパスに再ルーティングします。これをフェールオーバーと呼びます。障害の検出には時間がかかる場合があります。プローブを使用する場合、インターフェイスでのインターネット接続障害を検出するために 2 ～ 4 分かかります。

フェールオーバーを高速化するために、DIA トラッカーを設定し、Cloud OnRamp for SaaS 用に設定された DIA またはゲートウェイサイトに関連付けることができます。トラッカーにより、定期的にトランスポートインターフェイスをプローブして、インターネットまたは外部ネットワークが使用できなくなったかどうかを判断できます。トラッカーを Cloud OnRamp for SaaS

に関連付けると、アプリケーションのプライマリリンクが使用できない場合に代替パスにすばやく切り替えることができます。

トラッカーまたはトラッカーグループの速度は、しきい値、間隔、乗数などのパラメータの設定によって異なります。DIA トラッカーの詳細については、「NAT DIA Tracker」を参照してください。

SIG トンネル経由の Cloud OnRamp for SaaS を使用する場合の高速フェールオーバーの以前のサポートについては、SIG トンネル経由の Cloud OnRamp for SaaS に関する情報 （210 ページ）を参照してください。

Cloud onRamp for SaaS の利点

ゲートウェイサイトの VPN 0 インターフェイスを介した Cloud OnRamp for SaaS のプローブの利点

一部のネットワークシナリオでは、VPN 0 インターフェイスを使用してインターネットに接続するゲートウェイサイトを介して、サイトの全体または一部がインターネットに接続されます。これは、サービス VPN（VPN 1、VPN 2 など）の使用とは対照的です。

ゲートウェイサイトが VPN 0 を使用してインターネットに接続する場合、クラウドアプリケーションサーバーへのベストパスが VPN 0 インターフェイスを経由する可能性があります。Cloud onRamp for SaaS は、指定されたクラウドアプリケーションのトラフィックのベストパスをプローブする場合、ゲートウェイサイトの VPN 0 インターフェイスを介してプローブできます。これにより、ベストパスのオプションが拡張され、インターネットに接続されている使用可能なインターフェイスがさらに多く含まれるようになります。

（注） ゲートウェイサイトを介してインターネットに接続するブランチサイトは、ブランチサイト自体での 1 つ以上の DIA インターフェイスを介してインターネットに接続することもできます。

Webex の Cloud onRamp for SaaS のサポートの利点

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco vManage リリース 20.7.1

世界中の Webex サーバーのリストを管理し、使用可能なすべての Webex サーバーのベストパスを決定することで、Cloud onRamp for SaaS は Webex トラフィックの高度なパス最適化を行うことができます。Webex アプリケーションが遠隔地のクラウドサーバーに接続する場合や、異なる時間に異なるサーバーに接続する場合でも、Cloud onRamp for SaaS は常に世界中の Webex サーバーへのベストパスを提供します。

Cloud onRamp for SaaS でサポートされるデバイス

Cisco IOS XE Catalyst SD-WAN デバイスおよび Cisco vEdge デバイスは Cloud onRamp for SaaS をサポートしています。

次の表では、特定の Cloud onRamp for SaaS 機能のデバイスのサポートについて説明します。

表 *50* : デバイス機能のサポート

機能	Cisco IOS XE Catalyst SD-WAN デバイス サポート	Cisco vEdge デバイス サポート
基本的な Cloud onRamp for SaaS の機能	対応	対応
ゲートウェイサイトの VPN 0 インターフェイスを介した Cloud OnRamp for SaaS のプローブ	対応	対応
Webex アプリケーションのサポート	対応	非対応
Office 365 トラフィックのアプリケーション フィードバック メトリック	対応	非対応
Microsoft による Office 365 トラフィックのトラフィックメトリックの提供	対応	非対応
SD-AVC Cloud Connector	対応	非対応
Office 365 トラフィックのパススコアの表示	対応	非対応
SIG トンネル経由の Cloud onRamp for SaaS	対応	対応
SaaS アプリケーションリスト	対応	非対応
Webex サーバー側メトリック	対応	非対応

Cisco vEdge デバイスでサポートされている機能の詳細については、「Cloud onRamp for SaaS, Cisco SD-WAN Release 20.3.1 and Later」を参照してください。

Cloud OnRamp for SaaS の前提条件

以下の項では、Cloud OnRamp for SaaS 機能の前提条件について説明します。

Cloud OnRamp for SaaS の前提条件、全般

Cloud OnRamp for SaaS を使用するための前提条件は、Cisco vEdge デバイスと Cisco IOS XE Catalyst SD-WAN デバイスで異なります。Cisco vEdge デバイスで Cloud OnRamp for SaaS を使用する方法については、『Cloud OnRamp Configuration Guide for vEdge Routers, Cisco SD-WAN Release 20』を参照してください。

Cisco IOS XE Catalyst SD-WAN デバイスの場合、要件は次のとおりです。

- デバイスは Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降を実行している必要があります。
- デバイスは Manager モードである必要があります。
- すべての Cisco Catalyst SD-WAN コントローラ インスタンスは Manager モードである必要があります。
- アプリケーション認識型ポリシーを含む集中管理型ポリシーをアクティブにする必要があります。Cisco SD-WAN Manager では複数の集中管理型ポリシーを設定できますが、アクティブにできるのは 1 つだけです。

（注） これは、この要件がない Cisco vEdge デバイスで Cloud OnRamp for SaaS を使用する場合との重要な違いです。

- Cloud OnRamp for SaaS が有効になっている（[Administration] > [Settings]）。

  Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、Cloud OnRamp for SaaS がデフォルトで有効になっています。（**[Administration]** > **[Settings]**）

Office 365 トラフィックカテゴリによってトラフィックを指定するには、次の手順も必要です。

- Cisco SD-AVC が有効になっている（[Administration] > [Cluster Management]）。
- SD-AVC Cloud Connector が有効になっている（[Administration] > [Settings]）。Cloud Connector が有効になっていない場合、Office 365 トラフィックを指定するポリシーは Office 365 トラフィックを照合できません。トラフィックは、Cloud OnRamp for SaaS によって選択されたベストパスではなく、デフォルトパスを使用します。

ゲートウェイサイトの VPN 0 インターフェイスを介した Cloud OnRamp for SaaS のプローブの前提条件

ゲートウェイサイトの VPN 0 インターフェイスを介した Cloud onRamp for SaaS のプローブは、ブランチサイトがゲートウェイサイトを介してインターネットに接続し、ゲートウェイサイトが VPN 0 インターフェイスを使用してインターネットに接続することを前提としています。ブランチサイトは、1 つ以上の DIA 接続を介してインターネットに接続する場合としない場合があります。

Webex の Cloud OnRamp for SaaS のサポートの前提条件

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco vManage リリース 20.7.1

- 「Information About Cloud onRamp for SaaS Support for Webex」の「Maintaining an Up-to-Date List of Webex Servers」で説明されているように、Webex サーバーに関する最新情報をダウンロードするには、Cisco SD-WAN Manager にインターネットへのアクセスが必要です。
- Cloud OnRamp for SaaS を有効にして Webex トラフィックを最適化する場合は、各ルータに対して、サービス VPN にデフォルトルートが設定されていることを確認します。このデフォルトルートは、Cloud OnRamp for SaaS によって最適化されない Webex トラフィックのコンポーネントである Webex DNS および制御トラフィックに必要です。

特定のポリシーのトラフィックカテゴリとサービスエリアの設定の前提条件

最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a

- 複数のアクティブな AAR ポリシーが必要です。
- サービスエリアとトラフィックカテゴリを編集するには、Microsoft 365 アプリケーションの [Monitoring] と [Policy/Cloud SLA] を有効にする必要があります。詳細については、「Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager」を参照してください。

特定のサイトの特定のアプリケーションに対するCloudOnRampforSaaSの動作の有効化の前提条件

最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE リリース 17.2.1

異なるサイトのセットに関連付けられる複数の AAR ポリシーの可用性。

Microsoft 365 SaaS トラフィックの可視性の前提条件

最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a

- アプリケーションの可視性とフローの可視性を有効にします。詳細については、アプリケーションの可視性とフローの可視性の有効化 （196 ページ）を参照してください。
- グラフィカルに可視化したトラフィックを表示し、ログを表示するには、オンデマンドトラブルシューティングを有効にします。詳細については、『Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide』の「On Demand Troubleshooting」を参照してください。

Microsoft 365 トラフィックのベストパスの決定での Microsoft テレメトリデータの包含または除外の前提条件

最小リリース：Cisco vManage リリース 20.9.1

Microsoft トラフィックメトリックを有効にします。

「Enable Microsoft to Provide Traffic Metrics for Office 365 Traffic」を参照してください。

Webex サーバー側メトリックの前提条件

最小リリース：Cisco vManage リリース 20.10.1、Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a

- **[Administration]** > **[Settings]** で SD-AVC を有効にします。
- **[Administration]** > **[Settings]** でクラウドサービスを有効にします。
- Webex アカウント（これは通常、組織用のアカウントです）。
- サーバー側メトリックを有効にします。Webex サーバー側メトリックの有効化 （192 ページ）を参照してください。

ループバック、ダイヤラ、およびサブインターフェイスの Cloud OnRamp for SaaS のサポートの前提条件

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a

Cloud OnRamp for SaaS のダイヤラインターフェイスを使用するには、DIA インターフェイスに関連付けられている Point-to-Point Protocol（PPP）モデルが NAT DIA をサポートしている必要があります。

Cloud OnRamp for SaaS アプリケーションのデータプレフィックスリストの除外の前提条件

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 17.13.1a、Cisco Catalyst SD-WAN Manager リリース 20.13.1

Cloud OnRamp for SaaS アプリケーションの宛先データプレフィックスリストを使用または作成する前に、特定のプレフィックスを除外するアプリケーションについて、[Applications and Policy] ページで次の手順を実行します。

- アプリケーションのモニタリングを有効にします。
- アプリケーションのポリシー/クラウド SLA を有効にします。

DIA トラッカーを使用した高速フェールオーバーの前提条件

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 17.13.1a、Cisco Catalyst SD-WAN Manager リリース 20.13.1

- Cloud OnRamp for SaaS が有効になっている DIA またはゲートウェイサイトで、エンドポイントの DNS 名または IP アドレスを使用してトラッカーを設定します。
  - Cisco System 機能テンプレートを使用して DIA トラッカーを設定するには、「Configure NAT DIA Tracker on IPv4 Interfaces Using Feature Templates in Cisco SD-WAN Manager」を参照してください。
  - サイトのデバイスに、トラッカーまたはトラッカーグループが関連付けられている必要があります。
  - CLI テンプレートを使用して ICMP トラッカーを設定することができます。ICMP トラッカーの設定の詳細については、「Information About NAT DIA Tracking」を参照してください。
- トラッカーを関連付ける前に、Cloud OnRamp for SaaS 用に DIA インターフェイスが設定されていることを確認します。

Cloud onRamp for SaaS の制約事項

以下の項では、Cloud OnRamp for SaaS 機能に適用される制約事項について説明します。

Cloud OnRamp for SaaS の制約事項、全般

制約事項	説明
ループバック インターフェイス TLOC	サイトでトランスポートロケータ（TLOC）インターフェイスとしてループバックを使用するときに、Cloud OnRamp for SaaS を設定することはサポートされていません。 Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降では、Cloud OnRamp for SaaS は TLOC インターフェイスとしてのループバックの使用をサポートしています。
ダイヤラインターフェイス TLOC	Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降では、Cloud OnRamp for SaaS は TLOC インターフェイスとしてのダイヤラの使用をサポートしています。 ダイヤラインターフェイスに関連する制約事項については、「Restrictions for Using a Dialer Interface with NAT DIA」を参照してください。

制約事項	説明
VLANインターフェイスTLOC	サイトでTLOCインターフェイスとしてVLANを使用するときに、Cloud OnRamp for SaaSを設定することはサポートされていません。
セルラーインターフェイスTLOC	サイトでTLOCインターフェイスとしてセルラーを使用するときに、Cloud OnRamp for SaaSを設定することはサポートされていません。
アプリケーション認識型ポリシー	Cisco IOS XE Catalyst SD-WANデバイス デバイスでのCloud OnRamp for SaaSの設定は、一致条件 "cloud-saas-app-list" とアクション "cloud-saas" を使用した一元化されたアプリケーション認識型ポリシーを介してのみ行われます。Cisco vEdgeデバイスとCisco IOS XE Catalyst SD-WANデバイスを含む混在展開の場合は、Cisco vEdgeデバイスとCisco IOS XE Catalyst SD-WANデバイスに対して異なるアプリケーション認識型ポリシーを用意することを推奨します。
ICMP トラフィック	Cisco IOS XE Catalyst SD-WANリリース17.8.1aおよびCisco SD-WANリリース20.8.1以降では、Cloud OnRamp for SaaSはICMPトラフィックをサポートしません。これによる、Cisco IOS XE Catalyst SD-WANリリース17.7.1aおよびCisco SD-WANリリース20.7.1と比較したWebexトラフィックカウンタへの影響は軽微です。
設定グループ	Cloud onRamp for SaaSの設定 （175ページ）の項で説明されている方法を使用して、Cloud OnRamp for SaaSを設定できます。Cloud OnRamp for SaaSは、設定グループを使用した設定をサポートしていません。
NAT プール	DIAインターフェイスでのNATプールマッピングを使用したCloud OnRamp for SaaSの設定はサポートされていません。

Webex アプリケーションの制約事項

Cisco vManageリリース20.10.1およびCisco IOS XE Catalyst SD-WANリリース17.10.1a以降では、Webexトラフィックでの Cloud OnRamp for SaaSの動作を有効にすると、Cisco SD-WAN Managerはより効率的なポリシーモデルを使用しながら、Webexに対して Cloud OnRamp for SaaSを有効にする既存のレガシー制御ポリシーも引き続きサポートします。Cloud OnRamp for SaaSで Webexアプリケーションを無効にしてから Webexアプリケーションを再度有効にした場合、Cisco SD-WAN Managerは新しいポリシーモデルのみを使用することができます。Webexアプリケーションを無効にしてから再度有効にする前に、ネットワーク内のデバイスが Cisco IOS XE Catalyst SD-WANリリース17.10.1a以降を使用していることと、（**[Administration]** > **[Settings]** で）SD-AVCが有効になっていることを確認します。

トラッカーと DIA およびゲートウェイサイトの関連付けの制約事項

サポート対象の最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.13.1

ゲートウェイサイトへの接続がサービス VPN ではなく VPN 0 を使用する場合にのみ、トラッカーをゲートウェイサイトに関連付けることができます。

Cloud onRamp for SaaS のユースケース

ゲートウェイサイトの VPN 0 インターフェイスを介した Cloud OnRamp for SaaS のプローブのユースケース

次の条件が当てはまる場合は、VPN 0 インターフェイスを介したゲートウェイプローブを有効にします。

- ブランチサイトがゲートウェイサイトを介してインターネットに接続する。ブランチサイトは、1 つ以上の DIA インターフェイスを介してインターネットに接続する場合としない場合があります。
- ゲートウェイサイトに、1 つ以上のインターフェイスを介してトランスポート VPN（VPN 0）を使用するインターネット出口がある。

SD-AVC Cloud Connector のユースケース

サポート対象の最小リリース：Cisco vManage リリース 20.8.1

サーバー情報の可視性は、トラブルシューティングの際に役立ちます。たとえば、Sharepoint サービスエリア内の Office 365 トラフィックにのみ Cloud onRamp for SaaS を適用するポリシーを作成した後に、Cisco Catalyst SD-WAN が、Sharepoint トラフィックの最初のいくつかのフローを Cloud OnRamp for SaaS によって決定されたベストパスでルーティングしておらず、Sharepoint のパフォーマンスが期待を下回っていることが判明したとします。

トラブルシューティングを行うには、次の手順を実行します。

1. Sharepoint トラフィックが使用しているサーバーを特定します。
2. SD-AVC Cloud Connector のページを開き、“sharepoint” という用語でフィルタリングします。
3. 最初の手順で見つけた Sharepoint サーバーを探します。そのサーバーがリストに表示されない場合は、Cloud OnRamp for SaaS がそのサーバーへのトラフィックを Sharepoint トラフィックとして分類していないことを意味します。Sharepoint トラフィックとして分類されていない場合は、最初のいくつかのフローに対して、Cloud OnRamp for SaaS によって決定されたベストパスが使用されません。

トラフィックカテゴリとサービスエリアの設定のユースケース

最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a

ある組織が、オフィスアプリケーションについてMicrosoft 365に大きく依存していて、本社と各ブランチオフィスでMicrosoft 365 トラフィックを最適化するようにCloud OnRamp for SaaSを設定しています。さらに、データセンターでオンプレミスのOutlookサーバーを使用して会社の電子メールを処理しています。

Microsoftは、次のサービスエリアを使用して、さまざまなタイプのMicrosoft 365 トラフィックを区別します。

- Common：Microsoft 365 ProPlus、ブラウザ内のOffice、Azure Active Directory（AD）、およびその他のCommonネットワークエンドポイント
- Exchange：Exchange Online および Exchange Online Protection
- SharePoint：SharePoint Online および OneDrive for Business
- Skype：Skype for Business および Microsoft Teams

組織はオンプレミスのOutlookサーバーを使用しているため、ネットワーク管理者は、Cloud OnRamp for SaaSによるMicrosoft 365 トラフィックの最適化からOutlookトラフィックを除外することを選択します。AARポリシーを変更して、Cloud OnRamp for SaaSが機能するMicrosoft 365 トラフィックからExchangeサービスエリア（Outlook用）を除外することで、オンプレミスのOutlookサーバーを使用した電子メールトラフィックのパフォーマンスを最適化します。

特定のサイトでの特定のアプリケーションの有効化のユースケース

最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r

ある組織のネットワークが、多数のサイトにまたがっています。ほとんどのサイトでBox.comクラウドストレージアプリケーションを使用していますが、一部のサイトではBox.comを使用していません。

まず、ネットワーク管理者はBox.comを使用していない一部のサイトで機能するAARポリシーを作成します。次に、ネットワーク管理者はBox.comトラフィックに対してCloud OnRamp for SaaSを有効にします。これにより、ネットワーク内のすべてのサイトでCloud OnRamp for SaaSの動作が有効になります。

Box.comを使用しない一部のサイトを除外するために、ネットワーク管理者はその一部のサイトのAARポリシーを編集して、Box.comトラフィックに対するCloud OnRamp for SaaSの動作を無効にします。これにより、その一部のサイトでのみ、Box.comトラフィックに対するCloud OnRamp for SaaSの動作が無効になります。

Cloud OnRamp for SaaS の最適化からのデータプレフィックスの除外のユースケース

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 17.13.1a、Cisco Catalyst SD-WAN Manager リリース 20.13.1

一部の組織では、組織の内部ネットワークを介してのみ到達可能なプライベートデータセンターで SaaS アプリケーションをホストしています。Cloud OnRamp for SaaS を有効にしてこれらの SaaS アプリケーションのいずれかのトラフィックを最適化すると、Cloud OnRamp for SaaS が組織の内部ネットワーク外のサーバーに SaaS トラフィックをルーティングしようとする可能性があります。これにより、プライベートデータセンターへの SaaS トラフィックが意図せずに到達できなくなります。

たとえば、ある組織が内部 SharePoint トラフィック用にプライベートのオンプレミス SharePoint サーバーをホストしているとします。同時に、この組織は、SharePoint を含むいくつかの SaaS アプリケーションに対して Cloud OnRamp for SaaS による最適化を有効にしました。これにより、SharePoint トラフィックが意図せず干渉される可能性があります。

内部 SharePoint トラフィックが Cloud OnRamp for SaaS によって最適化されないようにするには、ネットワーク管理者は、内部 SharePoint サーバーの IP プレフィックスを除外するように Cloud OnRamp for SaaS を設定します。これにより、内部 SharePoint トラフィックが、プライベートデータセンターのオンプレミス SharePoint サーバーへと正しく流れるようになります。

Cloud onRamp for SaaS の設定

以下の項では、Cloud OnRamp for SaaS 機能の設定手順について説明します。

Cloud OnRamp for SaaS の有効化、Cisco IOS XE Catalyst SD-WAN デバイス

ダイレクト インターネット アクセス（DIA）を使用するサイトおよびインターネットにアクセスする DIA サイトで Cisco Catalyst SD-WAN オーバーレイネットワークの Cloud OnRamp for SaaS を有効にできます。ゲートウェイサイトと呼ばれるオーバーレイネットワーク内の別のサイトを介してインターネットにアクセスするクライアントサイトでも、Cloud OnRamp for SaaS を有効にできます。ゲートウェイサイトには、地域のデータセンターまたはキャリアニュートラルな施設を含めることができます。ゲートウェイを介してインターネットにアクセスするクライアントサイトで Cloud OnRamp for SaaS を有効にする場合は、ゲートウェイサイトでも Cloud OnRamp for SaaS を有効にします。

（注） Cloud OnRamp for SaaS 機能は、このドキュメントで説明されている Cisco SD-WAN Manager の手順を使用してのみ有効にできます。CLI テンプレートを使用した Cloud OnRamp for SaaS の設定はサポートされていません。CLIテンプレートを使用してデバイスの他の機能を設定する場合でも、Cisco SD-WAN Manager を使用して Cloud OnRamp for SaaS 機能を設定する必要があります。

Cloud OnRamp for SaaS の有効化

はじめる前に

Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、Cloud OnRamp for SaaS がデフォルトで有効になっています。

Cloud OnRamp for SaaS 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 OnRamp for SaaS] の横にある [Edit] をクリックします。
3. [Cloud OnRamp for SaaS] フィールドで、[Enabled] をクリックします。
4. [Save] をクリックします。

Cisco SD-WAN Manager を使用した Cloud OnRamp for SaaS のアプリケーションの設定

1. Cloud OnRamp for SaaS を開きます。
   - Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for SaaS] を選択します。

     または

   - Cisco SD-WAN Manager で、右上付近にあるクラウドアイコンをクリックし、[Cloud OnRamp for SaaS] を選択します。
2. [Manage Cloud OnRamp for SaaS] ドロップダウンリストで、[Applications and Policy] を選択します。

   [Applications and Policy] ウィンドウには、すべての SaaS アプリケーションが表示されます。
3. 必要に応じて、[App Type] フィールドのオプションをクリックして、アプリケーションのリストをフィルタリングすることができます。
   - [Standard]：Cloud OnRamp for SaaS にデフォルトで含まれているアプリケーション。

- [Custom]：ユーザー定義の SaaS アプリケーションリスト（「Information About SaaS Application Lists」を参照）。

4. （オプション）（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）すべての SaaS アプリケーションの特定のデータプレフィックスを除外するには、[Exclude Destination Data Prefix] をクリックします。

   ドロップダウンリストで、既存のデータプレフィックスリストを選択するか、[New Data Prefix List] をクリックして新しいデータプレフィックスリストを定義します。

   データプレフィックスの設定の詳細については、『Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x』の「Centralized Policy」の「Configure Data Prefix」の項を参照してください。

（注） 特定の SaaS アプリケーションのデータプレフィックスを除外するには、この手順内の後のステップを参照してください。

   データプレフィックスの除外については、データプレフィックスの除外に関する情報（165 ページ）を参照してください。

5. アプリケーションを有効にして設定します。

カラム	説明
アプリケーション	Cloud OnRamp for SaaS で使用できるアプリケーション。 **Office 365** アプリケーションを有効にした場合、[Enable Application Feedback] リンクをクリックして、Cloud OnRamp for SaaS が Microsoft からサーバー側のメトリックを受信できるようにすることができます。詳細については、「Enable Application Feedback Metrics for Office 365 Traffic」を参照してください。 **Webex** アプリケーションを有効にした場合は、[Enable Application Telemetry] リンクをクリックして、Cloud OnRamp for SaaS が Webex からサーバー側のメトリックを受信できるようにすることができます。詳細については、Webex サーバー側メトリックの有効化 （192 ページ）を参照してください。
モニタリング	[Enabled]：Cloud OnRamp for SaaS が、ベストパスを見つけるための Quality of Experience プローブを開始できるようにします。 [Disabled]：Cloud OnRamp for SaaS は、このアプリケーションに対する Quality of Experience プローブを停止します。
VPN	（Cisco vEdge デバイス）1 つ以上の VPN を指定します。

カラム	説明
Policy/Cloud SLA	（Cisco IOS XE Catalyst SD-WAN デバイス）[Enable] を選択して、Cloud OnRamp for SaaS がこのアプリケーションにベストパスを使用できるようにします。 （注） [Enable] を選択できるのは、アクティブ化されたアプリケーション認識型ポリシーを含む集中管理型ポリシーがある場合だけです。
	（Cisco IOS XE Catalyst SD-WAN デバイス）Microsoft 365（M365）の場合、次のいずれかを選択して、ベストパスを決定するためにどの M365 トラフィックのタイプを含めるのかを指定します。 • [Optimize]：Microsoft によって「最適化」として分類された M365 トラフィック、すなわち、ネットワークパフォーマンス、遅延、および可用性の影響を最も受けやすいトラフィックのみを含めます。 • [Optimize and Allow]：Microsoft によって「最適化」または「許可」として分類された M365 トラフィックのみを含めます。トラフィックの「許可」カテゴリは、「最適化」カテゴリほどネットワークパフォーマンスと遅延の影響を受けません。 • [All]：すべての M365 トラフィックを含めます。
	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降では、M365 アプリケーションが属するサービスエリアを選択できます。これにより、指定したサービスエリア内のアプリケーションに対してのみポリシーを適用できます。 Microsoft では、次のサービスエリアオプションを許可しています。 • [Common]：M365 Pro Plus、ブラウザ内の Office、Azure AD、およびその他の Common ネットワークエンドポイント。 • [Exchange]：Exchange Online および Exchange Online Protection。 • [SharePoint]：SharePoint Online および OneDrive for Business。 • [Skype]：Skype for Business および Microsoft Teams。 サービスエリアの更新については、Microsoft のドキュメントを参照してください。

カラム	説明
Exclude Destination Data Prefix	（オプション）Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、特定の SaaS アプリケーションのデータプレフィックスリストを除外できます。 1. [Select Destination Data Prefix] をクリックします。 2. ドロップダウンリストで、データプレフィックスリストを選択するか、[New Data Prefix List] をクリックして新しいリストを定義します。 3. [Save] をクリックします。 （注） すべての SaaS アプリケーションのデータプレフィックスを除外するには、この手順内の前のステップを参照してください。 データプレフィックスの除外については、データプレフィックスの除外に関する情報 （165 ページ）を参照してください。

6. [Save Applications and Next] をクリックします。

   [Application Aware Routing Policy] ウィンドウが表れ、現在アクティブな集中管理型ポリシーに対するアプリケーション認識型ポリシーが表示されます。

   - アプリケーション認識型ポリシーを選択したら、[Review and Edit] をクリックしてポリシーの詳細を確認できます。ポリシーの一致条件には、モニタリングが有効になっている SaaS アプリケーションが表示されます。
   - 既存のポリシーの場合、サイトリストまたは VPN リストを編集することはできません。
   - 既存の集中管理型ポリシーに含まれていないサイトであれば、新しいポリシーを作成できます。新しいポリシーを作成する場合は、そのポリシーの VPN リストを追加する必要があります。
   - SaaS アプリケーション用に新しく追加された 1 つ以上のシーケンスを削除したり、その順序を変更したりできます。

7. [Save Policy and Next] をクリックします。これにより、ポリシーが Cisco Catalyst SD-WAN コントローラに保存されます。
8. 変更したポリシーをアクティブ化するには、[Activate] をクリックします。

Cisco SD-WAN Manager を使用した Cloud onRamp for SaaS のサイトの設定

次の 2 種類のサイトを設定します。

- クライアントサイト
- ダイレクト インターネット アクセス（DIA）サイト

クライアントサイトの設定

ゲートウェイ経由でインターネットにアクセスするクライアントサイトで Cloud OnRamp for SaaS を設定するには、クライアントサイトとゲートウェイサイトの両方で Cloud OnRamp for SaaS を設定します。

（注） ゲートウェイサイトではポイント ツー ポイント プロトコル（PPP）インターフェイスを使用して Cloud OnRamp for SaaS を設定できません。

Cloud OnRamp サービスを利用しているクライアントサイトの場合は、インターネットへのアクセスに使用するアプリケーションごとに最適なゲートウェイサイトを選択します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for SaaS]** を選択します。**Cloud OnRamp for SaaS** のダッシュボードが表示されます。
2. [Manage Cloud OnRamp for SaaS] をクリックし、[Client Sites] を選択します。このページには、次の要素が表示されます。
   - [Attach Sites]：Cloud OnRamp for SaaS サービスにクライアントサイトを追加します。
   - [Detach Sites]：Cloud OnRamp for SaaS サービスからクライアントサイトを削除します。
   - [Client sites] テーブル：Cloud OnRamp for SaaS サービス用に設定されたクライアントサイトが表示されます。
3. **[Cloud OnRamp for SaaS]** > **[Manage Sites]** ウィンドウで、[Attach Sites] をクリックします。[Attach Sites] ダイアログボックスに、使用可能なサイトが強調された状態で、オーバーレイネットワーク内のサイトがすべて表示されます。サイトを使用可能にするには、そのサイトのすべてのデバイスが Manager のモードで実行されている必要があります。
4. [Available Sites] からクライアントサイトを 1 つ以上選択し、それらを [Selected Sites] に移します。
5. [Attach] をクリックします。Cisco SD-WAN Manager によって、機能テンプレートの設定がデバイスに保存されます。[Task View] ウィンドウには、検証成功のメッセージが表示されます。

6. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for SaaS]** を選択して、Cloud OnRamp for SaaS のダッシュボード画面に戻ります。
7. [Manage Cloud OnRamp for SaaS] をクリックし、[Gateways] を選択します。このページには、次の要素が表示されます。
   - [Attach Gateways]：ゲートウェイサイトをアタッチします。
   - [Detach Gateways]：Cloud OnRamp サービスからゲートウェイサイトを削除します。
   - [Edit Gateways]：ゲートウェイサイトのインターフェイスを編集します。
   - [Gateways] テーブル：Cloud OnRamp サービス用に設定されたゲートウェイサイトが表示されます。
8. [Manage Gateways] ウィンドウで、[Attach Gateways] をクリックします。[Attach Gateways] ダイアログボックスに、使用可能なサイトが強調された状態で、オーバーレイネットワーク内のサイトがすべて表示されます。サイトを使用可能にするには、そのサイトのすべてのデバイスが Manager のモードで実行されている必要があります。
9. [Device Class] フィールドで、次のオペレーティングシステムのいずれかを選択します。
   - [Cisco OS]：Cisco IOS XE Catalyst SD-WAN デバイス
   - [Viptela OS (vEdge)]：Cisco vEdge デバイス
10. [Available Sites] からゲートウェイサイトを 1 つ以上選択し、それらを [Selected Sites] に移します。
11. （Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a より前のリリースの Cisco vEdge デバイス）使用する Cloud OnRamp for SaaS の GRE インターフェイスを指定するには、ステップ 11a ～ 11d のアクションを実行します。

    （Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a 以降のリリースの Cisco vEdge デバイス）使用する Cloud OnRamp for SaaS のゲートウェイサイトの VPN 0 インターフェイスまたはサービス VPN インターフェイスを指定するには、ステップ 11a ～ 11d のアクションを実行します。

（注） Cloud OnRamp for SaaS が使用するインターフェイスを指定しない場合、システムによって、VPN 0 から NAT 対応の物理インターフェイスが選択されます。

    1. [Attach Gateways] ウィンドウの右下隅にある、選択したサイトに対する [Add interfaces] をクリックします（オプション）。
    2. [Select Interfaces] をクリックします。
    3. 使用可能なインターフェイスから、追加する GRE インターフェイス（Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a より前のリリースの場合）、または、追加する

VPN 0 インターフェイスまたはサービス VPN インターフェイス（Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a 以降のリリースの場合）を選択します。

4. [Save Changes] をクリックします。

12. （Cisco IOS XE Catalyst SD-WAN デバイス）ゲートウェイサイトのルータを設定するには、次の手順を実行します。

（注） Cloud OnRamp for SaaS のインターフェイスを指定しない場合、インターフェイスが VPN 0 ではないことを示すエラーメッセージが表示されます。

1. [Add interfaces to selected sites] をクリックします。
2. [Attach Gateways] ウィンドウに、ゲートウェイサイトの各 WAN エッジルータが表示されます。

   Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降では、ゲートウェイが Cisco IOS XE Catalyst SD-WAN デバイスを使用する場合は、サービス VPN または VPN 0 を選択できます。

   - ゲートウェイサイトのルータがサービス VPN 接続（VPN 1、VPN 2 など）でインターネットに接続する場合は、[Service VPN] を選択します。
   - ゲートウェイサイトのルータが VPN 0 でインターネットに接続する場合は、[VPN 0] を選択します。

（注）
- [Service VPN] または [VPN 0] を正しく選択する際には、ゲートウェイサイトからインターネットへ接続する方法についての情報が必要です。
- ゲートウェイサイトで WAN エッジルータを使用してインターネットにアクセスする場合は、必ずサービス VPN または VPN 0 接続のいずれかを使用してください。Cloud OnRamp for SaaS では、両方の使用をサポートしていません。

3. 次のいずれかを実行します。
   - [Service VPN] を選択した場合は、WAN エッジルータごとに、インターネット接続に使用するインターフェイスを選択します。
   - [VPN 0] を選択した場合は、[All DIA TLOC] を選択するか、または [TLOC list] を選択して、TLOC リストに含める色を指定します。
4. Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、[All DIA TLOC] を選択するか、または [TLOC list] を選択して TLOC リストに含める色を指定した場合は、[Enable Tracker Association] チェックボックスをオンにして、ゲートウェイサイトのトラッカーまたはトラッカーグループを関連付けることができます。

トラッカーの設定の詳細については、DIA トラッカーを使用した高速フェールオーバーの前提条件 （171 ページ）を参照してください。

5. WAN エッジデバイスの複数のインターフェイス間でクラウド アプリケーション トラフィックのロードバランシングを有効にするには、[Enable Load Balancing] チェックボックスをオンにします（「Load Balancing Across Multiple Interfaces」を参照してください）。

6. ロード バランシング オプションを設定します。

オプション	説明
Loss (%)	クラウドアプリケーションのベストパスインターフェイスを決定した後、Cloud OnRamp は他のインターフェイスのパフォーマンス統計を比較します。ロードバランシングに別のインターフェイスを使用する上で、インターフェイスのパケット損失値は、ベストパスインターフェイスのパケット損失値からこの設定値を超えて変動することはできません。 ベストパスインターフェイスのパケット損失値を小さく設定して、その値に非常に近いインターフェイスにのみロードバランシングを制限するか、または値を大きく設定して、パケット損失がそれよりも大きいことが予想されるインターフェイスを広く含めることができます。 たとえば、ベストパスインターフェイスのパケット損失値が 2% で、[Loss] 値が 10 に設定されている場合、パケット損失値が 12% を超えない場合に限り、別のインターフェイスをロードバランシングに使用できます。 範囲：0 ～ 100 デフォルト：10

オプション	説明
Latency (milliseconds)	ロードバランシングに別のインターフェイスを使用する上で、インターフェイスの遅延値は、ベストパスインターフェイスの遅延からこのミリ秒の数値を超えて変動することはできません。 ベストパスインターフェイスの遅延値を小さく設定して、その値に非常に近いインターフェイスにのみロードバランシングを制限するか、または値を大きく設定して、遅延がそれよりも大きいことが予想されるインターフェイスを広く含めることができます。 たとえば、ベストパスインターフェイスの遅延が 5 ミリ秒で、[Latency] 値が 50 に設定されている場合、遅延時間が 55 ミリ秒を超えない場合に限り、別のインターフェイスをロードバランシングに使用できます。 範囲：1 ～ 1000 デフォルト：50
Source IP based Load Balancing	単一のホストからのすべてのトラフィックが単一のインターフェイスを使用するようにするには、このオプションを有効にします。 たとえば、DNS とアプリケーショントラフィックが同じパスを使用するようにするには、このオプションを有効にします。

7. [Save Changes] をクリックします。

13. [Attach] をクリックします。Cisco SD-WAN Manager によって、機能テンプレートの設定がデバイスに保存されます。[Task View] ウィンドウには、検証成功のメッセージが表示されます。

14. Cloud OnRamp for SaaS のダッシュボードに戻るには、Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for SaaS]** を選択します。

ゲートウェイサイトのインターフェイスの編集

1. 編集するサイトを選択して、[Edit Gateways] をクリックします。
2. [Edit Interfaces of Selected Sites] ウィンドウで、編集するサイトを選択します。
   - ゲートウェイサイトがインターネットに接続する方法に基づいて、[Service VPN] または [VPN 0] を選択します。
   - 次のいずれかを実行します。

- [Service VPN] を選択した場合は、WAN エッジルータごとに、インターネット接続に使用するインターフェイスを選択します。
- [VPN 0] を選択した場合は、[All DIA TLOC] を選択するか、または [TLOC list] を選択して、TLOC リストに含める色を指定します。

- Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、[VPN 0] を選択した場合、[Enable Tracker Association] チェックボックスをオンにすることで、トラッカーをゲートウェイサイトに関連付けることができます。

  トラッカーの設定の詳細については、DIA トラッカーを使用した高速フェールオーバーの前提条件 （171 ページ）を参照してください。

- インターフェイスを追加するには、[Interfaces] フィールドをクリックして使用可能なインターフェイスを選択します。
- インターフェイスを削除するには、名前の横にある [X] をクリックします。
- WAN エッジデバイスの複数のインターフェイス間でクラウド アプリケーション トラフィックのロードバランシングを有効にするには、[Enable Load Balancing] チェックボックスをオンにして、ロード バランシング オプションを設定します（複数のインターフェイス間でのロードバランシング （157 ページ） を参照）。

オプション	説明
Loss (%)	クラウドアプリケーションのベストパスインターフェイスを決定した後、Cloud OnRamp は他のインターフェイスのパフォーマンス統計を比較します。ロードバランシングに別のインターフェイスを使用する上で、インターフェイスのパケット損失値は、ベストパスインターフェイスのパケット損失値からこの設定値を超えて変動することはできません。 ベストパスインターフェイスのパケット損失値を小さく設定して、その値に非常に近いインターフェイスにのみロードバランシングを制限するか、または値を大きく設定して、パケット損失がそれよりも大きいことが予想されるインターフェイスを広く含めることができます。 たとえば、ベストパスインターフェイスのパケット損失値が 2% で、[Loss] 値が 10 に設定されている場合、パケット損失値が 12% を超えない場合に限り、別のインターフェイスをロードバランシングに使用できます。 範囲：0 ～ 100 デフォルト：10

オプション	説明
Latency (milliseconds)	ロードバランシングに別のインターフェイスを使用する上で、インターフェイスの遅延値は、ベストパスインターフェイスの遅延からこのミリ秒の数値を超えて変動することはできません。 ベストパスインターフェイスの遅延値を小さく設定して、その値に非常に近いインターフェイスにのみロードバランシングを制限するか、または値を大きく設定して、遅延がそれよりも大きいことが予想されるインターフェイスを広く含めることができます。 たとえば、ベストパスインターフェイスの遅延が 5 ミリ秒で、[Latency] 値が 50 に設定されている場合、遅延時間が 55 ミリ秒を超えない場合に限り、別のインターフェイスをロードバランシングに使用できます。 範囲：1 ～ 1000 デフォルト：50
Source IP based Load Balancing	単一のホストからのすべてのトラフィックが単一のインターフェイスを使用するようにするには、このオプションを有効にします。 たとえば、DNS とアプリケーション トラフィックが同じパスを使用するようにするには、このオプションを有効にします。

3. [Save Changes] をクリックして、テンプレートをデバイスにプッシュします。

ダイレクト インターネット アクセス（DIA）サイトの設定

（注） Cloud OnRamp for SaaS では、インターフェイスを介した SaaS プローブを有効にするために、各物理インターフェイスに SD-WAN トンネルが必要となります。DIA しか設定されていない物理インターフェイスの場合、SD-WAN ファブリックに向かう SD-WAN トンネルがないので、Cloud OnRamp for SaaS の使用を有効にするために、デフォルトまたはダミーの色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と色が設定されていない DIA のみの物理インターフェイスでは、SaaS プローブは実行されません。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for SaaS]** を選択します。
2. タイトルバーの右側にある [Manage Cloud OnRamp for SaaS] ドロップダウンリストから、[Direct Internet Access (DIA) Sites] を選択します。

[Manage DIA] ウィンドウには、DIA サイトのアタッチ、デタッチ、または編集のオプションがあり、Cloud OnRamp サービス用に設定されたサイトのテーブルが表示されます。

3. [Attach DIA Sites] をクリックします。[Attach DIA Sites] ダイアログボックスに、使用可能なサイトが強調された状態で、オーバーレイネットワーク内のすべてのサイトが表示されます。サイトを使用可能にするには、そのサイトのすべてのデバイスが Manager のモードで実行されている必要があります。
4. [Device Class] フィールドで、次のいずれかを選択します。
   - [Cisco OS]：Cisco IOS XE Catalyst SD-WAN デバイス
   - [Viptela OS (vEdge)]：Cisco vEdge デバイス
5. [Available Sites] から DIA サイトを 1 つ以上選択し、それらを [Selected Sites] に移します。
6. （Cisco vEdge デバイスのみ）Cloud OnRamp for SaaS が使用するインターフェイスを指定しない場合、デフォルトでは、システムによって VPN 0 からすべての NAT 対応の物理インターフェイスが選択されます。次の手順を使用して、Cloud OnRamp for SaaS 用の特定のインターフェイスを指定します。

（注） ループバック インターフェイスは選択できません。

   1. ウィンドウの右下隅にあるリンクの [Add interfaces to selected sites]（オプション）をクリックします。
   2. [Select Interfaces] ドロップダウンリストで、追加するインターフェイスを選択します。
   3. [Save Changes] をクリックします。
7. （Cisco IOS XE Catalyst SD-WAN デバイスの場合、オプション）サイトの TLOC を指定します。

（注） TLOC インターフェイスとしてループバックを使用するときに、Cloud OnRamp for SaaS を設定することはサポートされていません。

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降では、Cloud OnRamp for SaaS は TLOC インターフェイスとしてのループバックの使用をサポートしています。

（注） TLOC を指定しない場合、[All DIA TLOC] オプションがデフォルトで使用されます。

   1. [Attach DIA Sites] ダイアログボックスの右下隅にある [Add TLOC to selected sites] リンクをクリックします。

2. [Edit Interfaces of Selected Sites] ダイアログボックスで、[All DIA TLOC] または [TLOC List] を選択し、TLOC リストを指定します。
3. Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、[All DIA TLOC] を選択するか、または [TLOC list] を選択して TLOC リストに含める色を指定した場合は、[Enable Tracker Association] チェックボックスをオンにして、DIA サイトのトラッカーまたはトラッカーグループを関連付けることができます。

   トラッカーの設定の詳細については、DIA トラッカーを使用した高速フェールオーバーの前提条件 （171 ページ）を参照してください。
4. [Save Changes] をクリックします。

8. [Attach] をクリックします。Cisco SD-WAN Manager NMS によって、機能テンプレートの設定がデバイスに保存されます。[Task View] ウィンドウには、検証成功のメッセージが表示されます。
9. Cloud OnRamp for SaaS のダッシュボードに戻るには、Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for SaaS]** を選択します。

ダイレクト インターネット アクセス（DIA）サイトのインターフェイスの編集

1. 編集するサイトを選択して、[Edit DIA Sites] をクリックします。
2. （Cisco vEdge デバイス）[Edit Interfaces of Selected Sites] 画面で、編集するサイトを選択します。
   - インターフェイスを追加するには、[Interfaces] フィールドをクリックして使用可能なインターフェイスを選択します。
   - インターフェイスを削除するには、名前の横にある [X] をクリックします。
3. （Cisco IOS XE Catalyst SD-WAN デバイス）[Edit Interfaces of Selected Sites] ダイアログボックスで、次の手順を実行します。
   1. [All DIA TLOC] をクリックしてすべての TLOC を含めるか、[TLOC List] をクリックして特定の TLOC を選択します。
   2. Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、[Enable Tracker Association] チェックボックスをオンにすることで、トラッカーを DIA サイトに関連付けることができます。

      トラッカーの設定の詳細については、DIA トラッカーを使用した高速フェールオーバーの前提条件 （171 ページ）を参照してください。
4. [Save Changes] をクリックして、新しいテンプレートをデバイスにプッシュします。

Cloud OnRamp for SaaS のダッシュボードに戻るには、**[Configuration]** > **[Cloud OnRamp for SaaS]** を選択します。

Office 365 トラフィックのアプリケーション フィードバック メトリックの有効化

Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降では、追加のソースからの次のタイプのアプリケーション フィードバックを有効にできます。Cloud OnRamp for SaaS は、これらのメトリックを使用して、Office 365 トラフィックのベストパスの決定に役立てることができます。ベストパスの決定 （156 ページ）を参照してください。

- Microsoft Exchange クラウドサーバーでテレメトリを有効にします。これにより、特別に設定されたインターフェイスで Office 365 トラフィックのベストパスのメトリックを提供できます。これには、Microsoft 365 の情報に基づくネットワークルーティングと呼ばれる Microsoft サービスの使用が必要です。この機能の理解を深めるには、「Microsoft 365 informed network routing」のドキュメントで入手可能な情報を参照してください。
- アプリケーション応答時間（ART）メトリックを有効にします。これにより、ART メトリックを報告するようにネットワークデバイスが設定されます。

はじめる前に

- Office 365 トラフィックのモニタリングを有効にします。

  Cisco SD-WAN Manager を使用した Cloud OnRamp for SaaS のアプリケーションの設定 （176 ページ）を参照してください。

- Cisco IOS XE SD-WAN デバイスの Office 365 のポリシーを設定します。

  Cisco SD-WAN Manager を使用した Cloud OnRamp for SaaS のアプリケーションの設定 （176 ページ）の [Policy/Cloud SLA] のオプションを参照してください。

- NetFlow メトリックを有効にするには、クラウドサービスを有効にします。

  （Cisco SD-WAN Manager のメニューから、[Administration] > [Settings] > [Cloud Services] を選択します）

- ネットワーク内のデバイスの NetFlow メトリックを有効にするには、各デバイスのローカライズされたポリシーで [NetFlow] オプションと [Application] オプションを有効にします。

  （Cisco SD-WAN Manager のメニューから、[Configuration] > [Policies] > [Localized Policy] > [Policy template]、[Policy Settings] セクションを選択します）

- Cisco SD-WAN Analytics をイネーブルにします。Cisco vAnalytics のインサイトを参照してください。

Office 365 トラフィックのアプリケーション フィードバック メトリックの有効化

1. Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for SaaS] を選択します。
2. [Manage Cloud OnRamp for SaaS] ドロップダウンリストで、[Applications and Policy] を選択します。

3. [Office 365] の行で、[Enable Application Feedback for Path Selection] リンクをクリックします。

   [Application Feedback] ダイアログボックスが開きます。

4. [Application Feedback] ダイアログボックスで、トラフィックメトリックを有効にします。

   - [Telemetry]：Microsoft Exchange クラウドサーバーでテレメトリを有効にして、特定の設定済みインターフェイスを介して Office 365 トラフィックのトラフィックメトリックを受信します。これらのメトリックのインターフェイスの設定については、Microsoft による Office 365 トラフィックのテレメトリの提供の有効化 （190 ページ）を参照してください。

     このオプションが無効になっていて、Microsoft アカウントへのサインインを要求するメッセージがダイアログボックスに表示されている場合は、メッセージに記載されているコードをコピーし、サインインするためのリンクをクリックします。表示された Microsoft のページでコードを入力し、プロンプトが表示されたら、Microsoft テナントアカウントのログイン情報を使用してログインします。サインインすると、ダイアログボックスの [Telemetry] オプションが有効になります。

     Microsoft による Office 365 トラフィックのテレメトリの提供の有効化 （190 ページ）を参照してください。

   - [Traffic Steering]：Cisco vManage リリース 20.9.1 以降では、このチェックボックスをオンにすると、Cloud OnRamp for SaaS がベストパスの決定で Microsoft テレメトリデータを考慮できるようになります。これを無効にしても、Cisco SD-WAN Analytics ダッシュボードで Microsoft テレメトリデータを表示することはできますが、このテレメトリはベストパスの決定には影響しません。

   - （オプション）[Application Response Time (ART)]：ART メトリックを有効にします。

（注） ART を有効にすると、ART メトリックを報告するようにデバイスが自動的に設定されます。

5. [Save] をクリックします。

Microsoft による Office 365 トラフィックのテレメトリの提供の有効化

Cisco Catalyst SD-WAN オーバーレイの特定のインターフェイスから着信する Microsoft Exchange トラフィックのトラフィックメトリックを計算するために、Microsoft Exchange クラウドサーバーを有効にすることができます。Microsoft Azure ポータルを使用して、パブリック IP アドレスでインターフェイスを示し、含めるインターフェイスを指定します。これは、インターフェイスのオプトインと呼ばれます。

指定されたインターフェイスについて、Microsoft はパケット送信元 ID によって Office 365 トラフィックを識別し、Office 365 トラフィックのベストパスを決定するために Cloud OnRamp for SaaS が使用できるメトリックを提供します。

はじめる前に

- Cloud OnRamp for SaaS の有効化

  （[Administration] > [Settings] > [Cloud OnRamp for SaaS]）

  Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、Cloud OnRamp for SaaS がデフォルトで有効になっています。

- SD-AVC Cloud Connector の有効化

  （[Administration] > [Settings] > [SD-AVC Cloud Connector]）

  サポート対象の最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.13.1

  [Administration] > [Settings] > [SD-AVC]

  「Enable Cisco SD-AVC Cloud Connector」を参照してください。

- クラウドサービスの有効化

  （[Administration] > [Settings] > [Cloud Services]）

- 統計の収集間隔を 5 分に設定します。

  （[Administration] > [Settings] > [Statistics Configuration]）

- Office 365 トラフィックの Microsoft テレメトリを有効にします。Office 365 トラフィックのアプリケーション フィードバック メトリックの有効化 （189 ページ）を参照してください。

- Microsoft 365 テナントアカウントの Microsoft 365 の情報に基づくネットワーク ルーティング サービスをアクティブにします。

- **ip visibility**

  テレメトリの動作を有効にするには、次のように、ネットワーク内の各 Cisco IOS XE Catalyst SD-WAN デバイスで **ip visibility** を設定します。

```
policy
app-visibility
ip visibility features
  cxp        enable
  probe-saas enable
```

Microsoft による Office 365 トラフィックのテレメトリの提供の有効化

（注） Microsoft Azure ポータルの機能は、今後変更される可能性があります（そのため、このドキュメントの説明範囲外です）。これらの大まかな手順でガイダンスを提供しますが、詳細については Microsoft 365 のドキュメントを参照してください。

次の手順の詳細については、Microsoft 365 ドキュメントの「Microsoft 365 informed network routing」のトピックを参照してください。

1. Microsoft Azure ポータルにログインします（Microsoft Azure テナントアカウントの作成方法については、Microsoft Azure のドキュメントを参照してください）。
2. Microsoft Azure ポータルを使用して、トラフィックメトリックを追跡する Cisco Catalyst SD-WAN オーバーレイ ネットワーク インターフェイスを指定します。
    1. Azure ポータルで、Microsoft 365 管理センターにアクセスします。
    2. [Locations] ページで、必要に応じて SD-WAN オーバーレイネットワークの各場所について場所のエントリを追加します。
    3. 場所のエントリ内で、次のいずれかを実行します。
        - Cisco IOS XE リリース 17.9.1a 以降で動作するエッジルータを使用している場所の場合、[Add an office location] ページ（または同等のページ）で、SD-WAN ソリューションが LAN サブネットと出力アドレス範囲を自動的に設定できるようにするオプションを有効にします。次に、場所のエッジデバイスのシステム IP アドレスを入力します。
        - Cisco IOS XE リリース 17.8.x 以前で動作するエッジルータを使用している場所の場合は、目的のインターフェイスのパブリック IP アドレスを使用して、出力 IP アドレスを追加します。

Cloud OnRamp for SaaS の Webex の有効化

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco vManage リリース 20.7.1

Cloud onRamp for SaaS を有効にして Webex トラフィックのベストパスを決定するには、他のアプリケーションと同じ方法で Webex アプリケーションを有効にします。「Enable Cloud OnRamp for SaaS, Cisco IOS XE SD-WAN Devices」を参照してください。

Webex サーバー側メトリックの有効化

最小リリース：Cisco vManage リリース 20.10.1、Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a

はじめる前に

テレメトリの動作を有効にするには、次のように、ネットワーク内の各 Cisco IOS XE Catalyst SD-WAN デバイスで **ip visibility** を設定します。

```
policy
app-visibility
ip visibility features
  cxp        enable
  probe-saas enable
```

Webex サーバー側メトリックの有効化

Webex 統合により、Cisco SD-WAN Manager などのアプリケーションは、アプリケーション プログラミングインターフェイス（API）を使用して Webex サーバーからの情報をリクエストできます。

1. Webex アカウントを使用して、Cisco SD-WAN Manager の統合を作成します。統合の作成の詳細については、Webex for Developers ドキュメントの「Integrations & Authorization」を参照してください。

   Webex 統合を作成するには、Cisco SD-WAN Manager サーバーの IP アドレスを次の形式で含むリダイレクト URI が必要です。

   https://*vManage-ip-address*:*port*/dataservice/webex/redirect

   Webex 統合を作成するプロセスの最後に、Webex for Developers サイトからクライアント ID とクライアントシークレットが提供されます。

（注） Webex for Developers サイトでの統合アプリケーションの作成の詳細は、このドキュメントの範囲外です。

2. Webex in Cloud OnRamp for SaaS を有効にするときに、前の手順で受け取ったクライアント ID とクライアントシークレットを使用して、Cisco SD-WAN Manager で Webex 統合を使用できるようにします。

   1. Cloud OnRamp for SaaS を開きます。

      - Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for SaaS]** を選択します。

        または

      - Cisco SD-WAN Manager で、右上付近にあるクラウドアイコンをクリックし、[Cloud OnRamp for SaaS] を選択します。

   2. [Manage Cloud OnRamp for SaaS] ドロップダウンリストで、[Applications and Policy] を選択します。

      [Applications and Policy] ページには、Cloud OnRamp アプリケーションが表示されます。

   3. [Webex] の横にある [Enable vAnalytics Webex Telemetry] をクリックします。

4. ポップアップウィンドウで、[Enable Webex Telemetry] チェックボックスをオンにします。
5. Webex 統合のクライアント ID とクライアントシークレットを入力し、[Save] をクリックします。
6. 要求されたら、**Webex** アカウントのログイン情報を入力します。

（注） 前の手順で使用した Webex 統合に関連付けられている Webex アカウントのログイン情報を使用する必要があります。これにより、その Webex アカウントの Webex テレメトリが有効になります。

7. Cisco SD-WAN Manager で [Save Applications and Next] をクリックして Webex テレメトリ設定を保存し、更新をエッジデバイスと Cisco SD-WAN Analytics にプッシュします。

Cloud OnRamp for SaaS の Webex サーバー情報の更新

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco vManage リリース 20.7.1

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for SaaS]** を選択して、Cloud OnRamp for SaaS のダッシュボードを表示します。
2. （この手順は、Cisco vManage リリース 20.10.1 より前のリリースにのみ適用されます）。ダッシュボードに Webex サーバー情報を同期するように求めるダイアログボックスが表示された場合は、ダイアログボックスで [Yes] をクリックします。

   Cisco SD-WAN Manager に [Application Aware Routing Policy] ページが表示され、ポリシーを確認することができます。ポリシーには、最新の Webex サーバー情報を使用する更新された一致条件が含まれています。
3. [Save Policy] をクリックします。

   Cloud OnRamp for SaaS は、必要に応じて以下を更新し、世界中の Webex サーバーの更新情報を反映します。

   - アプリケーション認識型ポリシーの一致条件
   - クラウドアプリケーションをプローブするための設定

Cisco SD-WAN Manager を使用した特定のポリシーのトラフィックカテゴリとサービスエリアの設定

最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a

はじめる前に

サービスエリアとトラフィックカテゴリを編集するには、少なくとも1つのサービスエリアでMicrosoft 365アプリケーションの[Monitoring]と[Policy/Cloud SLA]を有効にする必要があります。詳細については、「Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager」を参照してください。

トラフィックカテゴリとサービスエリアの設定

1. Cloud OnRamp for SaaSを開きます。
   - Cisco SD-WAN Managerのメニューから、**[Configuration]** > **[Cloud OnRamp for SaaS]**を選択します。

     または

   - Cisco SD-WAN Managerで、右上付近にあるクラウドアイコンをクリックし、[Cloud OnRamp for SaaS]を選択します。
2. [Manage Cloud OnRamp for SaaS]ドロップダウンリストで、[Applications and Policy]を選択します。

   [Applications and Policy]ページには、すべてのCloud OnRamp for SaaSアプリケーションが表示されます。
3. Microsoft 365アプリケーションの[Policy/Cloud SLA]列の編集アイコンをクリックします。

   [Policy/Cloud SLA Settings]ポップアップウィンドウが開きます。
4. [Policy/Cloud SLA Settings]ポップアップウィンドウで、次のいずれかを実行します。
   - **[はい（Yes）]**をクリックします。少なくとも1つのサービスエリアとトラフィックカテゴリを選択します。
   - サービスエリアとトラフィックカテゴリをすでに選択している場合は、[No]をクリックして、Microsoft 365のカテゴリまたはサービスエリアを編集します。
5. [Save Applications and Next]をクリックします。

   [Application Aware Routing Policy]ページが開きます。現在アクティブな集中管理型ポリシーのAARポリシーのリストが表示されます。
6. 編集するAARポリシーを選択し、[Review and Edit]をクリックします。

   [Review Policy]ページが開きます。
7. 編集するMicrosoft 365シーケンスを選択して、サービスエリアまたはトラフィックカテゴリを変更し、編集アイコンをクリックします。
8. サービスエリアとトラフィックカテゴリを編集し、[Save Match And Actions]をクリックします。
9. [Save Policy and Next]をクリックします。これにより、ポリシーが保存されます。

Cisco SD-WAN Manager を使用した特定のサイトの特定のアプリケーションで Cloud OnRamp の動作を有効にするための AAR ポリシーの設定

最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r

1. Cloud OnRamp for SaaS を開きます。
   - Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for SaaS]** を選択します。

     または

   - Cisco SD-WAN Manager のメニューで、右上付近にあるクラウドアイコンをクリックし、[Cloud OnRamp for SaaS] を選択します。
2. [Manage Cloud OnRamp for SaaS] ドロップダウンリストで、[Applications and Policy] を選択します。

   [Applications and Policy] ページには、すべての Cloud OnRamp for SaaS アプリケーションが表示されます。
3. [Save Applications and Next] をクリックします。

   [Application Aware Routing Policy] ページが開き、現在アクティブな集中管理型ポリシーのアプリケーション認識型ポリシーが表示されます。
4. 編集するポリシーを選択し、[Review and Edit] をクリックしてポリシーの詳細を表示します。
5. 特定のアプリケーションに対して Cloud OnRamp for SaaS によって追加された 1 つ以上のシーケンスを削除したり、シーケンスの順序を変更したりできるようになりました。
6. [Save Policy and Next] をクリックします。これにより、更新されたポリシーが Cisco SD-WAN コントローラにプッシュされます。

（注） 注：[Applications and Policy] ページでアプリケーションを有効にすると、デフォルトでは、現在アクティブな集中管理型ポリシーの一部であるすべての AAR ポリシーに対して Cloud OnRamp for SaaS が有効になります。

アプリケーションの可視性とフローの可視性の有効化

最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a

Cisco SD-WAN Manager を使用した可視性とフローの可視性の有効化

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. [Add Policy] をクリックします。
4. [Policy Settings] ページが表示されるまで、[Next] をクリックし続けます。
5. [Netflow and Applications] チェックボックスをオンにします。
6. [Save Policy] をクリックします。

   アプリケーションの可視性とフローの可視性が有効になりました。

CLI テンプレートを使用したアプリケーションの可視性とフローの可視性の有効化

CLI テンプレートの使用の詳細については、CLI アドオン機能テンプレートおよび CLI テンプレートを参照してください。

Cisco SD-WAN Manager を使用した Microsoft 365 SaaS トラフィックの可視性の設定

最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a

Microsoft 365 トラフィックの可視化用にデータを提供するためのデバイスの有効化

1. Cisco SD-WAN Manager のメニューから**[Tools]** > **[On Demand Troubleshooting]**の順で選択します。[On Demand Troubleshooting] ページが開きます。
2. [Select Device] ドロップダウンリストをクリックして、デバイスを選択します。
3. [Select Data Type] ドロップダウンリストをクリックして、データ型に [DPI] を選択します。
4. [Data Backfill Time Period] から時間範囲を選択します。
5. [Add] をクリックして、処理のためにデバイスをキューに入れます。
6. [Status] 列に [Completed] が表示されるまで待ちます。

アプリケーションの使用状況の表示

最小リリース（Microsoft 365 トラフィックの場合）：Cisco vManage リリース 20.9.1、Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a

最小リリース（Webex トラフィックの場合）：Cisco vManage リリース 20.10.1、Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a

1. Cloud OnRamp for SaaS を開きます。

- Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for SaaS]** を選択します。

  または

- Cisco SD-WAN Manager で、右上付近にあるクラウドアイコンをクリックし、[Cloud OnRamp for SaaS] を選択します。

2. [Manage Cloud OnRamp for SaaS] をクリックします。
3. [Microsoft 365] アプリケーションまたは [Webex] アプリケーションをクリックします。DIA またはゲートウェイにアタッチされているデバイスのリストが表示されます。
4. デバイスの [Application Usage] 列で、[View Usage] をクリックします。

   Webex アプリケーションの場合、Webex のリージョンに応じて使用状況情報が表示されます。
5. [CoR SaaS Application Usage] ページには、トラフィックのタイプごとの情報が表示されます。表示されるトラフィック情報を制限するには、[Search] フィールドをクリックし、[All CoR SaaS Traffic]、[DIA]、[Gateway]、または [Non CoR SaaS] を選択します。

（注）

- 上記のグラフまたはログに表示される情報は、個々のデバイスに関するものです。一度に 1 つのデバイスに関連する情報のみを表示できます。グラフまたはログは、オンデマンドのトラブルシューティングが有効になっているデバイスについてのみ表示されます。オンデマンドのトラブルシューティングの詳細については、「On-Demand Troubleshooting」を参照してください。
- IP 可視性機能コマンドは、CLI またはアドオン CLI テンプレートを介してのみサポートされます。
- 特定の Cisco IOS XE Catalyst SD-WAN デバイスのトラフィックタイプごとにアプリケーションの使用状況が表示されない場合は、CLI アドオン機能テンプレートを使用して次の設定をデバイスに追加します。

```
policy
 app-visibility
 ip visibility features
  cxp        enable
  probe-saas enable
```

Cloud onRamp for SaaS の確認

以下の項では、Cloud OnRamp for SaaS 機能の確認手順について説明します。

アプリケーションが Cloud OnRamp for SaaS に対して有効になっていることの確認

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for SaaS]** を選択します。
2. [Manage Cloud OnRamp for SaaS] をクリックし、[Applications and Policy] を選択します。

   [Applications and Policy] ウィンドウには、すべての SaaS アプリケーションが表示されます。
3. 確認するアプリケーションの行で、[Monitoring] 列と [Policy/Cloud SLA] 列の両方に [Enabled] と表示されていることを確認します。

Cisco SD-WAN Manager を使用した特定のポリシーのトラフィックカテゴリとサービスエリアの設定に対する変更の確認

最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Devices]**を選択します。
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。

   デバイスのリストが表示されます。
3. 確認するデバイスについて、[…] をクリックし、[Running Configuration] をクリックします。[Running Configuration] ウィンドウが開き、実行コンフィギュレーションが表示されます。
4. AAR ポリシーに加えた変更が実行コンフィギュレーションに反映されていることを確認します。

または

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

   [Policies] ページにポリシーが表示されます。
2. 確認するポリシーについて、[…] をクリックし、[Preview] をクリックします。

   [Policy Configuration Preview] ポップアップウィンドウが表示され、実行コンフィギュレーションのプレビューが表示されます。

3. AARポリシーに加えた変更がポリシーのプレビューに反映されていることを確認します。

Cisco SD-WAN Managerを使用した特定のデバイスで有効になっているアプリケーションの確認

最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE リリース 17.2.1

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Devices]**を選択します。
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。

デバイスのリストが表示されます。

3. 確認するデバイスについて、[…] をクリックし、[Running Configuration] をクリックします。[Running Configuration] ウィンドウが開き、実行コンフィギュレーションが表示されます。
4. AARポリシーに加えた変更が実行コンフィギュレーションに反映されていることを確認します。

Cisco SD-WAN Managerを使用した特定のポリシーで有効になっているアプリケーションの確認

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

   [Policies] ウィンドウにポリシーが表示されます。
2. 確認するポリシーについて、[…] をクリックし、[Preview] をクリックします。

   [Policy Configuration Preview] ページが表示され、実行コンフィギュレーションのプレビューが表示されます。
3. AAR ポリシーに加えた変更がポリシーに反映されていることを確認します。

Cisco SD-WAN Managerを使用した除外されたデータプレフィックスの確認

サポート対象の最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.13.1

はじめる前に

Cloud OnRamp for SaaS の最適化から特定のデータプレフィックスを除外できます。詳細については、データプレフィックスの除外に関する情報（165 ページ）を参照してください。除外されたデータプレフィックスは、アプリケーション認識型ルーティングポリシーに表示されます。この手順では、アプリケーション認識型ルーティングポリシーを表示し、除外されたデータプレフィックスを確認できるようにします。

除外されたプレフィックスの確認

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for SaaS]** を選択します。
2. [Manage Cloud OnRamp for SaaS] をクリックし、[Applications and Policy] を選択します。

   [Applications and Policy] ページには、すべての SaaS アプリケーションが表示されます。
3. [Save Applications and Next] をクリックします。

   [Application Aware Routing Policy] ページが表れ、アクティブな集中管理型ポリシーに対するアプリケーション認識型ポリシーが表示されます。
4. アプリケーション認識型ポリシーを選択し、[Review and Edit] をクリックしてポリシーの詳細を表示します。
5. [Preview] をクリックします。
6. [Config Diff] をクリックします。
7. 除外するデータプレフィックスを表示します。

Cloud onRamp for SaaS のモニター

以下の項では、Cloud OnRamp for SaaS 機能のモニタリング手順について説明します。

モニタリング対象アプリケーションの詳細の表示

1. Cloud OnRamp for SaaS を開きます。
   - Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for SaaS] を選択します。

     または
   - Cisco SD-WAN Manager で、右上にあるクラウドアイコンをクリックし、[Cloud OnRamp for SaaS] をクリックします。

   このページには、モニター対象アプリケーションごとに、次の情報を含むタイルが含まれています。

- Cloud OnRamp for SaaS で動作しているサイトの数。
- 各サイトで動作しているデバイスでのアプリケーションの Quality of Experience（vQoE）スコアの色分けされた評価（緑＝良いスコア、黄色＝中程度のスコア、赤＝低いスコア）。

2. 必要に応じて、タイルをクリックして、次のようなアプリケーションの Cloud OnRamp for SaaS アクティビティの詳細を表示できます。

フィールド	説明
vQoE Status	緑色のチェックマークは、ベストパスの vQoE スコアが許容可能な接続の基準を満たしていることを示します。vQoE は、平均損失と平均遅延に基づいて計算されます。Office 365 トラフィックの場合、他の接続メトリックも vQoE スコアで考慮されます。

フィールド	説明
vQoE Score	各サイトの、クラウドアプリケーション トラフィックに使用可能なベストパスの vQoE スコアです。 vQoE スコアは、Cloud OnRamp for SaaS のプローブによって決定されます。サイトのルータのタイプに応じて、次のように [vQoE Score] の詳細を表示できます。 • Cisco IOS XE Catalyst SD-WAN デバイスを展開するには、次の操作を行います。 使用可能な各インターフェイスの vQoE スコア履歴のチャートを表示するには、チャートアイコンをクリックします。このチャートでは、各インターフェイスの vQoE スコア履歴が色付きの線で表示されます。実線は、Cloud OnRamp for SaaS が、チャート上の特定の時点でのクラウドアプリケーションのベストパスとしてインターフェイスを指定したことを示しています。 チャート上の特定の時点で線にカーソルを合わせると、その時点でのインターフェイスの vQoE スコアの詳細を表示できます。 Cisco vManage リリース 20.8.1 以降では、Office 365 アプリケーションのチャートには、Exchange、SharePoint、Skype などの特定のサービスエリアの vQoE スコア履歴を表示するオプションが含まれています。各サービスエリアについて、チャート内の実線は、特定の時点でのベストパスとして選択されたインターフェイスを示しています。Cloud OnRamp for SaaS で Office 365 トラフィックに Microsoft トラフィックメトリックを使用できるようにしている場合は、ベストパスの選択で Microsoft トラフィックメトリックが考慮されます。 • Cisco vEdge デバイスを展開するには、次の操作を行います。 vQoE スコア履歴のチャートを表示するには、チャートアイコンをクリックします。このチャートには、Cloud OnRamp for SaaS によって選択されたベストパスの vQoE スコアが表示されます。
DIA Status	ローカル（サイトから）やゲートウェイサイト経由などの、インターネットへの接続のタイプ。

フィールド	説明
Selected Interface	クラウドアプリケーションにベストパスを提供するインターフェイス。 （注） DIA ステータスが [Gateway] の場合、このフィールドには [N/A] と表示されます。 Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、ベストパスがループバック インターフェイスの場合、このフィールドにはループバックへのインターフェイスバインドが表示されます。
Activated Gateway	ゲートウェイサイトを介してインターネットに接続するサイトの場合、これはゲートウェイサイトの IP アドレスを示します。 （注） DIA ステータスが [Local] の場合、このフィールドには [N/A] と表示されます。
Local Color	ゲートウェイサイトを介してインターネットに接続するサイトの場合、これはゲートウェイサイトへの接続に使用されるトンネルのローカルカラー識別子です。 （注） DIA ステータスが [Local] の場合、このフィールドには [N/A] と表示されます。
Remote Color	ゲートウェイサイトを介してインターネットに接続するサイトの場合、これはゲートウェイサイトへの接続に使用されるトンネルのリモート（ゲートウェイサイト）カラー識別子です。 （注） DIA ステータスが [Local] の場合、このフィールドには [N/A] と表示されます。

フィールド	説明
SDWAN Computed Score	このフィールドは、サイトが Cisco IOS XE Catalyst SD-WAN デバイスを使用している場合にのみ適用されます。Cisco vEdge デバイスには適用されません。 Cisco vManage リリース 20.8.1 以降では、Microsoft Office 365 アプリケーションに対して、Exchange、SharePoint、Skype などの各 Microsoft サービスエリアについて Microsoft テレメトリによって提供されたパススコア（[OK]、[NOT-OK]、または [INIT]）のチャートを表示するためのリンクが [SDWAN Computed Score] 列で提供されます。このチャートには、使用可能な各インターフェイスの時間の経過に伴うスコアが表示されます。スコアは次のように定義されています。 • [OK]：許容できるパス • [NOT-OK]：許容できないパス • [INIT]：データが不十分 これらのチャートは、Cloud OnRamp for SaaS が Microsoft Office 365 トラフィックのタイプごとにベストパスを選択する方法を可視化します。 パススコア履歴を表示するユースケースとして、Skype トラフィックなどの一部のタイプのトラフィックについて、Microsoft が特定のインターフェイスを一貫して [NOT-OK] と評価するかどうかを判断する場合があります。

Cloud OnRamp for SaaS の Webex のステータスのモニター

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco vManage リリース 20.7.1

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for SaaS]** を選択します。

   このページには、モニター対象の各アプリケーション、関連サイト、およびそれぞれに関する情報が表示されます。

2. 必要に応じて、サイトをクリックして、アプリケーショントラフィックに使用可能なさまざまなパスのスコアのチャートと、ベストパス（実線）を表示することができます。

3. Cisco vManage リリース 20.10.1 以降では、各サイトとリージョンについて、Webex トラフィックが使用しているインターフェイスに関する情報を表示できます。詳細については、アプリケーションの使用状況の表示 （197 ページ）を参照してください。

SD-AVC Cloud Connector を使用したサーバー情報の表示

はじめる前に

- SD-AVC を有効にします（**[Administration]** > **[Cluster Management]**、[…] をクリックして [Edit] を選択し、[Enable SD-AVC] を選択）。
- SD-AVC Cloud Connector を有効化します。『Cisco Catalyst SD-WAN Getting Started Guide』の「Enable Cisco SD-AVC Cloud Connector」を参照してください。

サーバー情報の表示

1. Cisco SD-WAN Manager のメニューから、**[Monitor]** > **[SD-AVC Cloud Connector]** を選択します。
2. [Application] フィールドで、アプリケーションを選択します。
   - Office 365 アプリケーションの場合、[SD-AVC Cloud Connector] ページには、Office 365 トラフィックを処理する Microsoft アプリケーションサーバーに関して Microsoft Cloud から収集された次の情報が表示されます。

フィールド	説明
[Domain] タブ	
アプリケーション	トラフィックを生成しているアプリケーションの名前。Cisco IOS XE のコンポーネントである Network-Based Application Recognition（NBAR）がアプリケーション名を提供します。
ドメイン	トラフィックの宛先ドメイン。これは、クラウド アプリケーション トラフィックを処理するアプリケーションサーバーです。
サービス エリア	Microsoft によって決定された、サービスエリアの分類（[exchange]、[sharepoint]、[skype]、[common] など）。
カテゴリ	Microsoft によるトラフィックの分類（[optimize]、[allow]、または [default]）。このフィールドのダッシュは、トラフィックに定義済みのカテゴリがないことを示しています。
Service Instance	Microsoft によって定義された、サーバーのサービスインスタンス情報。サービスインスタンスの例として、China、Germany、USGovGCCHigh、および USGovDoD があります。
[IP Address] タブ	
IP	トラフィックの宛先 IP。これは、クラウド アプリケーション トラフィックを処理するアプリケーションサーバーの IP アドレスです。

フィールド	説明
Port	トラフィックの宛先ポート。
L4 Protocol	トラフィックのトランスポートプロトコル（TCP や UDP など）。
アプリケーション	トラフィックを生成しているアプリケーションの名前。Cisco IOS XE のコンポーネントである NBAR がアプリケーション名を提供します。
カテゴリ	Microsoft によるトラフィックの分類（[optimize]、[allow]、または [default]）。このフィールドのダッシュは、トラフィックに定義済みのカテゴリがないことを示しています。
サービス エリア	Microsoft によって決定された、サービスエリアの分類（[exchange]、[sharepoint]、[skype]、[common] など）。
Service Instance	Microsoft によって定義された、サーバーのサービスインスタンス情報。サービスインスタンスの例として、China、Germany、USGovGCCHigh、および USGovDoD があります。

- （最小リリース：Cisco vManage リリース 20.10.1）Webex アプリケーションの場合、[SD-AVC Cloud Connector] ページには Webex クラウドサーバーから収集された次の情報が表示されます。

フィールド	説明
[IP Address] タブ	
アプリケーション	トラフィックを生成しているアプリケーションの名前。
サービス エリア	Webex トラフィックのタイプ：meeting、calling、または teams。
IP アドレス	トラフィックの宛先 IP アドレス。これは、クラウドアプリケーション トラフィックを処理するアプリケーションサーバーの IP アドレスです。
Port	トラフィックの宛先ポート。
L4 Protocol	トラフィックのトランスポートプロトコル（TCP や UDP など）。
Quality of Service	Webex によって定義された、Webex トラフィックの QoS 分類（default や optimizemedia など）。
Primary or Fallback	Webex トラフィックのカテゴリ。
[地域（Region）]	Webex サーバーデータセンターのリージョン（ap-south-1、ap-northeast-1、ap-southeast-1 など）。

3. 必要に応じて、検索フィールドを使用してテーブル内の情報をフィルタリングできます。たとえば、アプリケーション名またはドメイン名でフィルタリングできます。

Cloud OnRamp for SaaS の除外されたデータプレフィックスリストのモニター

サポート対象の最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.13.1

1. Cisco SD-WAN Manager のメニューから**[Monitor]** > **[Devices]** の順に選択します。
2. デバイスをクリックして選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] ドロップドロップリストをクリックし、[Policy App Route Filter] を選択します。

テーブルに、アプリケーションのデータプレフィックスリストを表すパケットカウンタ名などの、リアルタイムの統計が表示されます。

Syslog およびコンソールログのログの表示

Cisco Cloud OnRamp for SaaS の通知とアラームは syslog に入力されます。これらの通知とアラームは、コンソールログには入力されません。Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以降では、Cisco Cloud OnRamp for SaaS の通知とアラームは syslog とコンソールログの両方に表示されます。ただし、syslog とコンソールログの両方での通知とアラームのフラッディングを回避するために、Cisco SD-WAN Manager はデフォルトで NETCONF を生成します（syslog はオンデマンド、コンソールログは CLI テンプレートの追加時）。CLI テンプレートの使用の詳細については、「CLI Add-on Feature Templates」および「CLI Templates」を参照してください。

1. Cloud Express のスコア変更通知を syslog とコンソールログの両方に出力するには、CLI テンプレートを使用して **system** *alarms alarm cloud-express-score change syslog* コマンドを使用します。
2. Cloud Express のアプリケーション変更通知を syslog とコンソールログの両方に出力するには、CLI テンプレートを使用して **system** *alarms alarm cloud-express-application-change syslog* コマンドを使用します。

SIG トンネル経由の Cloud onRamp for SaaS

表 *51* : 機能の履歴

機能名	リリース情報	説明
SIG トンネル経由の Cloud onRamp for SaaS	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能により、SIG トンネルを使用して Cloud onRamp for SaaS に接続できます。 SIG トンネル経由の Cloud onRamp for SaaS 機能は、SaaS アプリケーションへのセキュアなアクセスと、SaaS アプリケーションへのアクセスに最適な SIG トンネルを自動的に選択する機能を提供します。

SIG トンネル経由の Cloud onRamp for SaaS の前提条件

- セキュアインターネットゲートウェイ（SIG）テンプレートを使用して作成された SIG トンネルには、有効なトラッカー送信元 IP アドレスが必要です。Cloud onRamp for SaaS は、プローブ目的で SIG テンプレートのトラッカー送信元 IP アドレスを使用します。
- SIG トンネルを介して到達できる IP アドレスを持つインターネットベースの DNS サーバーを使用するようにデバイスを設定します。

SIG トンネル経由の Cloud OnRamp for SaaS の制約事項

- アプリケーション識別子：

  Cloud OnRamp for SaaS により、ブランチと Cloud OnRamp for SaaS の間でエッジルータを通過するフローの最初のパケットから、アプリケーションが識別される必要があります。フローの最初のパケットでアプリケーションを識別できない場合、Cloud OnRamp によって選択されたベストパスを、そのフローの後続のパケットに導入できません。アプリケーションが分類されると、後続のトラフィックフローは、Cloud OnRamp for SaaS によって選択されたベストパスを通過します。

- ゲートウェイ出口と DIA：

  ゲートウェイ出口とダイレクトインターネットアクセス（DIA）出口間の Cloud OnRamp for SaaS の比較ロジックでは、リモートゲートウェイの Cloud OnRamp for SaaS がアンダーレイ インターフェイスまたは SIG インターフェイスを使用して計算を実行しているかどうかを判断できません。

- IPv6 のサポート：

  Cloud OnRamp for SaaS では、IPv6 はサポートされていません。

- テレメトリのサポート：

  - SIG トンネル経由の Cloud OnRamp for SaaS を使用するサイトでは、Microsoft 365 テレメトリまたは Webex サーバー側メトリックを有効にできません。

  - Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降では、（a）SIG トンネル経由の Cloud OnRamp for SaaS を使用するサイトと、（b）SIG トンネルを使用せずに Cloud OnRamp for SaaS を使用するサイトを含むシナリオで、SIG トンネルを使用しないサイトでのみ、Microsoft 365 テレメトリと Webex サーバー側メトリックがサポートされます。

    Microsoft 365 テレメトリまたは Webex サーバー側メトリックをグローバルに有効にすると、SIG トンネル経由の Cloud OnRamp for SaaS を使用しないサイトでのみそれらがアクティブになります。

  - Cisco vManage リリース 20.6.1 から Cisco Catalyst SD-WAN Manager リリース 20.13.x では、（a）SIG トンネル経由の Cloud OnRamp for SaaS を使用するサイトと、（b）SIG トンネルを使用せずに Cloud OnRamp for SaaS を使用するサイトを含むシナリオで、Microsoft 365 テレメトリと Webex サーバー側メトリックは、ネットワーク内のどのサイトでもサポートされません。

    このシナリオで Microsoft 365 テレメトリまたは Webex サーバー側メトリックを有効にしようとすると、プッシュ機能テンプレート設定タスクに関連付けられたエラーがタスクリストに表示されます。

SIG トンネル経由の Cloud OnRamp for SaaS に関する情報

Cloud OnRamp for SaaS を使用すると、サイトは次の方法で SaaS アプリケーションに接続できます。

- 最もパフォーマンスの高い SIG トンネル経由
- ゲートウェイサイト経由。ブランチからゲートウェイに最もパフォーマンスの高いオーバーレイトンネルを介してトラフィックが送信されてから、ゲートウェイサイトから最もパフォーマンスの高い SIG トンネルを介してトラフィックが送信されます。

SIG トンネル経由で接続するサイトの Cloud OnRamp for SaaS を設定すると、インターネット経由で SaaS アプリケーションにセキュアにアクセスすることができます。

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.6.1 および Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降では、SIG トンネルがレイヤ 7 正常性チェックを使用して設定されている場合、Cloud OnRamp for SaaS はデフォルトで SIG トンネルでの高速フェールオーバーをサポートしています。レイヤ 7 正常性チェックの設定の詳細については、「Support for Layer 7 Health Check」を参照してください。

SIG トンネル経由の Cloud onRamp for SaaS の利点

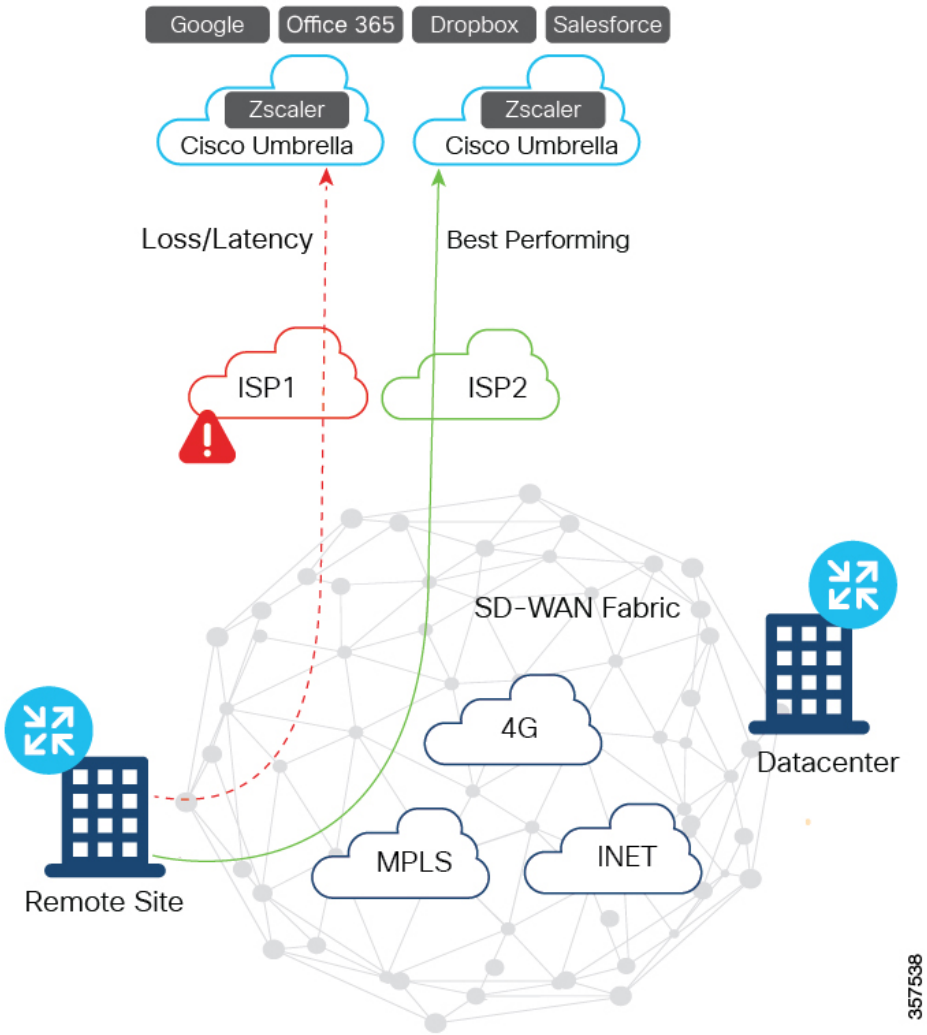
SIG トンネル経由の Cloud OnRamp for SaaS への接続には、次の利点があります。

- SIG トンネル経由で SaaS アプリケーションに安全にアクセスできます。
- SIG トンネル経由の Cloud onRamp for SaaS はベストパスパフォーマンスを提供し、最良のパフォーマンスを発揮するトンネルを介した SaaS アプリケーションへのアクセスが有効になります。

SIG トンネル経由の Cloud onRamp for SaaS のユースケース

SIG トンネル経由で SaaS アプリケーションにアクセスするには、さまざまな方法があります。

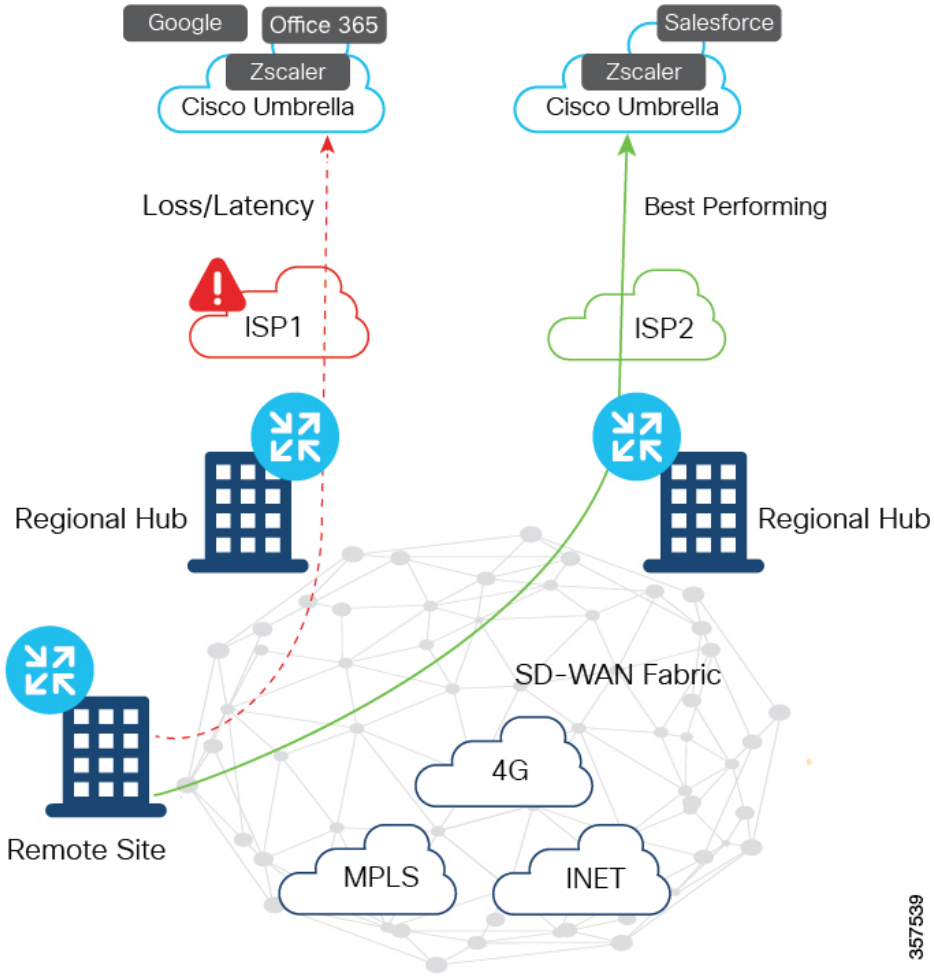
DIA を使用したブランチからの複数の SIG トンネルによる SaaS アプリケーションへのダイレクトアクセス



このシナリオでは、次のようになります。

- GRE または IPSec を介した複数の VPN0 トンネルが、ブランチから Zscaler および Cisco Umbrella に設定されています。
- ブランチからのトラフィックは、特定の SaaS アプリケーションのために最もパフォーマンスの高いトンネルを介して転送され、セキュリティ検査のために Zscaler と Cisco Umbrella で終端されます。
- トラフィックは SIG からインターネットに転送されます。

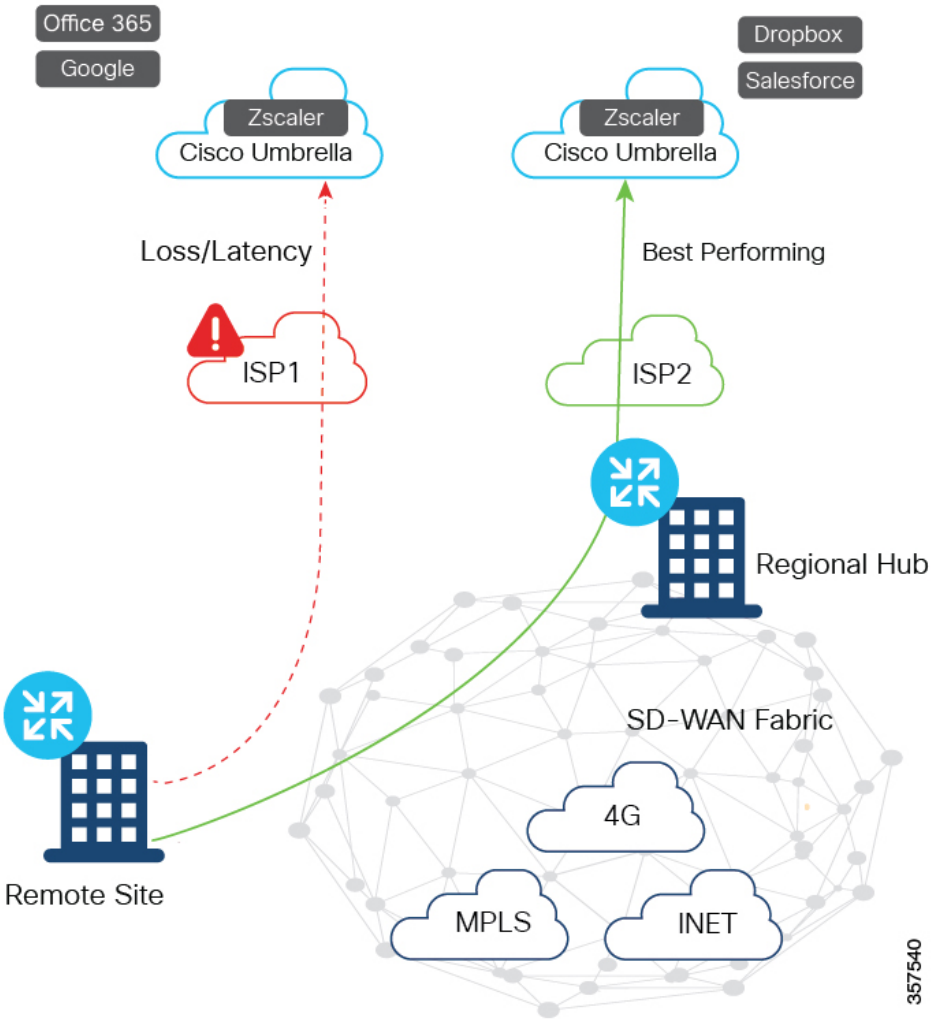
ゲートウェイを使用したブランチからの複数の SIG トンネルによる SaaS アプリケーションへのアクセス



このシナリオでは、次のようになります。

- GRE または IPSec を介した複数の VPN0 トンネルが、1 つ以上の地域ハブから Zscaler および Cisco Umbrella に設定されています。
- ブランチからのトラフィックは、特定の SaaS アプリケーションのために最もパフォーマンスの高い地域ハブに転送され、セキュリティ検査のために Zscaler と Cisco Umbrella で終端されます。
- トラフィックは SIG からインターネットに転送されます。

DIA とゲートウェイを使用したブランチからの複数の SIG トンネルによる SaaS アプリケーションへのアクセス



このシナリオでは、次のようになります。

- GRE または IPSec を介した複数の VPN0 トンネルが、ブランチ、地域ハブ、またはその両方から Zscaler および Cisco Umbrella に設定されています。
- ブランチ、地域ハブ、またはその両方からのトラフィックは、特定の SaaS アプリケーションのために最もパフォーマンスの高いトンネルを介して転送され、セキュリティ検査のために Zscaler と Cisco Umbrella で終端されます。
- トラフィックは SIG からインターネットに転送されます。

SIG トンネル経由の Cloud OnRamp for SaaS の設定

DIA を使用した SIG トンネル経由の Cloud OnRamp for SaaS の設定

1. Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for SaaS] を選択します。
2. [Manage Cloud OnRamp for SaaS] ドロップダウンリストから、[Direct Internet Access (DIA) Sites] を選択します。
3. [Attach DIA Sites] をクリックします。

   [Attach DIA Sites] ダイアログボックスに、使用可能なサイトが強調された状態で、オーバーレイネットワーク内のすべてのサイトが表示されます。
4. [Device Class] で、次を選択します。

   Cisco OS (cEdge)
5. [Available Sites] ペインで、アタッチするサイトを選択し、右矢印をクリックします。サイトを削除するには、[Selected Sites] ペインでサイトをクリックし、左矢印をクリックします。
6. [Add TLOC to selected sites] をクリックします。
7. [Secure Internet Gateway (SIG) Interfaces] をクリックします。
8. [Attach DIA Sites] ウィンドウから [All Auto SIG Interfaces] または [SIG Interface List] をクリックし、シスコ セキュア インターネット ゲートウェイ テンプレートによって設定されたトンネルのリストから選択します。

（注） [SIG Interface List] フィールドの Tunnel1000X エントリは、インターフェイス名を参照します。これは、SIG テンプレートの設定時に入力した IPSec インターフェイス名に相当します。

9. [Save Changes] をクリックします。
10. [Attach] をクリックします。

    Cisco SD-WAN Manager が機能テンプレート設定をデバイスにプッシュし、[Task View] ウィンドウに「Validation Success」というメッセージが表示されます。

ゲートウェイを使用した SIG トンネル経由の Cloud OnRamp for SaaS の設定

ゲートウェイを使用した SIG トンネル経由の Cloud OnRamp for SaaS を設定するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for SaaS] を選択します。
2. [Manage Cloud OnRamp for SaaS] ドロップダウンリストから、[Gateways] を選択します。

3. [Attach Gateways] をクリックします。

   [Attach Gateways] ポップアップウィンドウに、使用可能なサイトが強調された状態で、オーバーレイネットワーク内のすべてのサイトが表示されます。

4. [Device Class] で、次を選択します。

   Cisco OS (cEdge)

5. [Available Sites] ペインで、アタッチするサイトを選択し、右矢印をクリックします。サイトを削除するには、[Selected Sites] ペインでサイトをクリックし、左矢印をクリックします

6. [Add interfaces to selected sites] をクリックします。

7. [VPN 0] をクリックします。

8. [Secure Internet Gateway (SIG) Interfaces] をクリックします。

9. [Attach Gateways] ウィンドウから [All Auto SIG Interfaces] または [SIG Interface List] をクリックし、シスコ セキュア インターネット ゲートウェイ テンプレートによって設定されたトンネルのリストから選択します。

（注） [SIG Interface List] フィールドの Tunnel1000X エントリは、インターフェイス名を参照します。これは、SIG テンプレートの設定時に入力した IPSec インターフェイス名に相当します。

10. [Save Changes] をクリックします。

11. [Attach] をクリックします。Cisco SD-WAN Manager が機能テンプレート設定をデバイスにプッシュし、[Task View] ウィンドウに「Validation Success」というメッセージが表示されます。

CLI を使用した SIG トンネル経由の Cloud onRamp for SaaS の設定

この項では、SIG トンネル経由の Cloud onRamp for SaaS の CLI 設定例を示します。

DIA およびゲートウェイサイトの SIG トンネル経由の Cloud OnRamp for SaaS の設定

```
Device# config-transaction
Device(config)# probe-path {branch|gateway}
{all-auto-sig-tunnels|sig-tunnel-list} list of SIG tunnels
Device(config)# ip sdwan route vrf vrf ip address service sig
```

ゲートウェイサイトの SIG トンネル経由の Cloud OnRamp for SaaS の NBAR プロトコル検出の有効化

```
Device# config-transaction
```

```
Device(config)# probe-path gateway {all-auto-sig-tunnels|sig-tunnel-list}
list of SIG tunnels
Device(config)# ip sdwan route vrf vrf ip address service sig
Device(config)# interface tunnel-id
Device(config-if)# ip nbar protocol-discovery
```

例

次の例では、ゲートウェイサイトの SIG トンネル経由の Cloud onRamp for SaaS を設定し、トンネルインターフェイス Tunnel100001 および Tunnel100002 で NBAR プロトコル検出を有効にします。

```
Device# config-transaction
Device(config)# probe-path gateway all-auto-sig-tunnels
Device(config)# ip sdwan route vrf 1 192.168.0.1 service sig
Device(config)# interface Tunnel101
Device(config-if)# ip nbar protocol-discovery
Device(config-if)# interface Tunnel102
Device(config-if)# ip nbar protocol-discovery
```

ループバック インターフェイスでの VPN の設定

```
Device# config-transaction
Device(config)# vrf definition vrf
Device(config-vrf)# address-family ipv4
Device(config-vrf)# exit-address-family

Device(config)# interface  Loopback interface_number
Device(config-if)# no shutdown
Device(config-vrf)# vrf forwarding vrf_number
Device(config-vrf)# ip address ip address mask
Device(config-vrf)# exit
```

SIG トンネル経由の Cloud OnRamp for SaaS のモニター

SIG トンネル経由の Cloud OnRamp for SaaS をモニターするには、次の手順を実行します。

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

   Cisco vManage リリース 20.6.x 以前：Cisco SD-WAN Manager のメニューから**[Monitor]** > **[Network]**の順に選択します。

2. 表示されるデバイスのリストから、デバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] ドロップダウンリストをクリックし、次のコマンドのいずれかを選択します。

デバイスオプション	説明
CloudExpress Applications	Cloud OnRamp for SaaS で設定されたアプリケーションのベストパスを表示します。ベストパスは、DIA のあるローカルインターフェイス、またはリモートゲートウェイへのパスです。
CloudExpress Gateway Exits	Cloud OnRamp for SaaS で設定されたアプリケーションの各ゲートウェイ出口での損失と遅延を表示します。
CloudExpress Local Exits	Cloud OnRamp for SaaS が有効になっている各DIAインターフェイスでのアプリケーションの損失と遅延を表示します。

5. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud onRamp for SaaS]** を選択してダッシュボードにアクセスし、Cloud OnRamp for SaaS で使用可能なアプリケーションを表示することができます。

CLI を使用した SIG トンネル経由の Cloud onRamp for SaaS のモニター

例 1

次に、Cisco IOS XE Catalyst SD-WAN デバイスでの **show sdwan cloudexpress local-exits** コマンドの出力例を示します。この例では、Cloud OnRamp for SaaS が有効になっている各 DIA インターフェイスでのアプリケーションの損失と遅延を表示します。

```
Device# show sdwan cloudexpress local-exits

VPN APPLICATION INTERFACE LATENCY LOSS
------------------------------------------------------------------------
1 office365 Tunnel100015 10 0
1 office365 Tunnel100016 3 0
1 amazon_aws Tunnel100015 10 0
1 amazon_aws Tunnel100016 3 0
```

例 2

次に、Cisco IOS XE Catalyst SD-WAN デバイスでの **show sdwan cloudexpress gateway-exits** コマンドの出力例を示します。この例では、Cloud OnRamp for SaaS で設定されたアプリケーションの各ゲートウェイ出口での損失と遅延を表示します。

```
Device# show sdwan cloudexpress gateway-exits

                                                                    LOCAL   REMOTE
VPN  APPLICATION             GATEWAY IP              LATENCY  LOSS  COLOR   COLOR
-------------------------------------------------------------------------------------
1    salesforce              172.16.255.14           72       2     lte     lte
1    google_apps             172.16.255.14           16       0     lte     lte
```

例 3

次に、Cisco IOS XE Catalyst SD-WAN デバイスでの **show sdwan cloudexpress applications** コマンドの出力例を示します。この例では、Cloud OnRamp for SaaS で設定されたアプリケーションのベストパスを表示します。ベストパスは、DIA のあるローカルインターフェイス、またはリモートゲートウェイへのパスです。

```
Device# show sdwan cloudexpress applications

                                EXIT     GATEWAY
   LOCAL  REMOTE
VPN  APPLICATION              TYPE     SYSTEM IP      INTERFACE  LATENCY  LOSS
  COLOR  COLOR
-----------------------------------------------------------------------------------
1    salesforce               gateway  172.16.255.14  -          103      1
   lte    lte
1    google_apps              gateway  172.16.255.14  -          47       0
   lte    lte
```

例 4

次に、Cisco IOS XE Catalyst SD-WAN デバイスでの **show ip route vrf** コマンドの出力例を示します。この例では、特定の VPN ルーティングおよび転送（VRF）インスタンスに関連付けられている IP ルーティングテーブルを表示します。

```
Device# show ip route vrf vrf1

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route

Gateway of last resort is not set

B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C    10.0.0.0/8 is directly connected, Ethernet1/3
B    10.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20
```

例 5

次に、Cisco IOS XE Catalyst SD-WAN デバイスでの **show sdwan run probe-path** コマンドの出力例を示します。この例では、SIG トンネルのプローブパスを表示します。

```
Device# show sdwan run probe-path
probe-path branch sig-tunnel-list Tunnel100015 Tunnel100016
```

SIG トンネル経由の Cloud onRamp for SaaS の設定例

次の例は、SIG トンネル経由の Cloud on Ramp for SaaS の設定を示しています。

例

```
Device(config)# probe-path branch sig-tunnel-list Tunnel100015 Tunnel100016
Device(config)# probe-path branch all-auto-sig-tunnels
```

Cloud OnRamp for SaaS のトラブルシューティング

以下の項では、問題のシナリオとトラブルシューティング情報について説明します。

Webex アプリケーションのテレメトリを有効にできない

問題

Cloud OnRamp for SaaS で Webex アプリケーションのテレメトリを有効にできません。

対処方法

次の各手順のコンテキストについては、Webex サーバー側メトリックの有効化 （192 ページ）を参照してください。

1. Webex デベロッパーサイトを使用して、アプリケーション統合を作成したことを確認します。
2. 以下の形式で正しいリダイレクト URL を入力したことを確認します。

   https://*vManage-ip-address*:*port*/dataservice/webex/redirect
3. Cloud OnRamp for SaaS で Webex を有効にする場合は、正しいクライアント ID とクライアントシークレットを入力したことを確認します。

各 Webex リージョンのベストパスを特定できない

問題

Cloud OnRamp for SaaS が、各 Webex リージョンのベストパスを特定できません。

対処方法

1. デバイスがベストパスの特定に失敗した場合は、デバイスで **show avc sd-service info connectivity** コマンドを実行して、Cisco SD-AVC が有効になっていることを確認します。
2. Cisco SD-WAN Manager のメニューから、**[Monitor]** > **[SD-AVC Cloud Connector]** を選択します。[Webex] アプリケーションを選択し、リージョンフィールドが入力されていることを確認します。
3. Cloud OnRamp for SaaS 設定のコンテキスト外で、DNS と NAT が正しく動作していることを確認します。Cloud OnRamp for SaaS 機能は、これらが正しく設定されているかどうかに依存します。

4. リージョンのレスポンダサーバーが動作可能であり、デバイスから到達可能であることを確認します。これを行うには、デバイスからサーバーに ping を実行し、サーバーが ping に応答することを確認します。

   リージョンのレスポンダサーバー名の形式は次のとおりです。

   pinger.*region-name*.infnet.webex.com

   次に、us-west リージョンの例を示します。

   ```
   Device#ping pinger.us-west-1.infnet.webex.com
   ```

Debug コマンドと Show コマンド

（注） 次の debug コマンドと show コマンドは、Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a 以降を実行している Cisco IOS XE Catalyst SD-WAN デバイスに適用されます。

表 *52*：

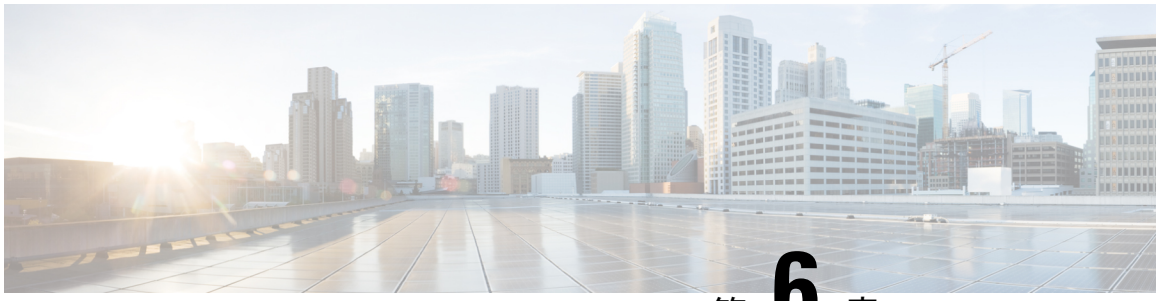
説明	コマンド
CXP と Cisco SD-WAN Analytics のインタラクションシナリオをデバッグする	コマンド **set platform software trace** *cxpd RP active cxpd-analytics* **debug** を使用します
CXP と Cisco SD-WAN Analytics のインタラクションシナリオの詳細レベルのデバッグトレースを分析する	コマンド **set platform software trace** *cxpd RP active cxpd-analytics* **verbose** を使用します
set platform software trace cxpd RP active cxpd-analytics notice を使用して、CXP と Cisco SD-WAN Analytics のインタラクションシナリオの通知レベルのデバッグトレースにデバッグレベルを設定する（これにより、通知よりも高いすべてのトレースレベルが無効になります）	コマンド **set platform software trace** *cxpd RP active cxpd-analytics* **notice** を使用します
デバッグトレースを有効にして、CXP アプリケーションのベストパス選択ロジック処理を分析する	コマンド **set platform software trace** *cxpd RP active cxpd-app* **debug** を使用します
詳細レベルのデバッグトレースを有効にして、CXPアプリケーションのベストパス選択ロジック処理を分析する	コマンド **set platform software trace** *cxpd RP active cxpd-app* **verbose** を使用します

説明	コマンド
デバッグレベルを通知レベルに設定し、CXP アプリケーションのベストパス選択ロジック処理のデバッグを無効にする（これにより、通知よりも高いすべてのトレースレベルが無効になります）	コマンド **set platform software trace** *cxpd RP active cxpd-app* **notice** を使用します
デバッグトレースを有効にして、CXP 設定の解析処理を分析する	コマンド **set platform software trace** *cxpd RP active cxpd-config* **debug** を使用します
デバッグトレースを有効にして、詳細レベルの CXP 設定の解析処理を分析する	コマンド **set platform software trace** *cxpd RP active cxpd-config* **verbose** を使用します
デバッグレベルを通知レベルに設定し、CXP 設定の解析処理のデバッグを無効にする（これにより、通知よりも高いすべてのトレースレベルが無効になります）	コマンド **set platform software trace** *cxpd RP active cxpd-config* **notice** を使用します
デバッグトレースを有効にして、CXP と DPI モジュールのインタラクションシナリオを分析する	コマンド **set platform software trace** *cxpd RP active cxpd-dpi* **debug** を使用します
詳細レベルのデバッグトレースを有効にして、CXP と DPI モジュールのインタラクションシナリオを分析する	コマンド **set platform software trace** *cxpd RP active cxpd-dpi* **verbose** を使用します
デバッグレベルを通知レベルに設定し、CXP と DPI モジュールのインタラクションシナリオのデバッグを無効にする（これにより、通知よりも高いすべてのトレースレベルが無効になります）	コマンド **set platform software trace** *cxpd RP active cxpd-dpi* **notice** を使用します
トレースをデバッグして、CXP と FTM モジュールのインタラクションシナリオを分析する	コマンド **set platform software trace** *cxpd RP active cxpd-ftm* **debug** を使用します このトレースを有効にすると、CXPからのデータプレーンのプログラミングの問題を分析できます。 Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降では、このコマンドの *cxpd-ftm* キーワードは廃止されています

説明	コマンド
トレースをデバッグして、CXP と FMANRP モジュールのインタラクションシナリオを分析する	Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降では、コマンド **set platform software trace** *cxpd RP active cxpd-fmanrp* **debug** を使用します このトレースを有効にすると、CXPからのデータプレーンのプログラミングの問題を分析できます。
詳細レベルのデバッグトレースを有効にして、CXP と FTM モジュールのインタラクションシナリオを分析する	コマンド **set platform software trace** *cxpd RP active cxpd-ftm* **verbose** を使用します Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降では、このコマンドの *cxpd-ftm* キーワードは廃止されています。
詳細レベルのデバッグトレースを有効にして、CXP と FMANRP モジュールのインタラクションシナリオを分析する	Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降では、コマンド **set platform software trace** *cxpd RP active cxpd-fmanrp* **verbose** を使用します
デバッグレベルを通知レベルに設定し、有効になっている CXP と FTM モジュールのインタラクションシナリオのデバッグを無効にする（これにより、通知よりも高いすべてのトレースレベルが無効になります）	コマンド **set platform software trace** *cxpd RP active cxpd-ftm* **notice** を使用します Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降では、このコマンドの *cxpd-ftm* キーワードは廃止されています。
デバッグレベルを通知レベルに設定し、有効になっている CXP と FMANRP モジュールのインタラクションシナリオのデバッグを無効にする（これにより、通知よりも高いすべてのトレースレベルが無効になります）	Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降では、コマンド **set platform software trace** *cxpd RP active cxpd-fmanrp* **notice** を使用します
デバッグトレースを有効にして、CXP と OMP モジュールのインタラクションシナリオを分析する	コマンド **set platform software trace** *cxpd RP active cxpd-omp* **debug** を使用します このトレースを有効にすると、CXPゲートウェイのメトリック処理の問題を分析できます
詳細レベルのデバッグトレースを有効にして、CXP と OMP モジュールのインタラクションシナリオを分析する	コマンド **set platform software trace** *cxpd RP active cxpd-omp* **verbose** を使用します

説明	コマンド
デバッグレベルを通知レベルに設定し、CXP と OMP モジュールのインタラクションシナリオのデバッグを無効にする（これにより、通知よりも高いすべてのトレースレベルが無効になります）	コマンド **set platform software trace** *cxpd RP active cxpd-omp* **notice** を使用します
デバッグトレースを有効にして、CXP 操作コマンドの処理を分析する	コマンド **set platform software trace** *cxpd RP active cxpd-oper* **debug** を使用します
詳細レベルのデバッグトレースを有効にして、CXP 操作コマンドの処理を分析する	コマンド **set platform software trace** *cxpd RP active cxpd-oper* **verbose** を使用します
デバッグレベルを通知レベルに設定し、CXP 操作の解析処理のデバッグを無効にする（これにより、通知よりも高いすべてのトレースレベルが無効になります）	コマンド **set platform software trace** *cxpd RP active cxpd-oper* **notice** を使用します
デバッグトレースを有効にして、CXP と IOS のインタラクションシナリオを分析する	コマンド **set platform software trace** *cxpd RP active cxpd-rtm* **debug** を使用します
詳細レベルのデバッグトレースを有効にして、CXP と IOS モジュールのインタラクションシナリオを分析する	コマンド **set platform software trace** *cxpd RP active cxpd-rtm* **verbose** を使用します
デバッグレベルを通知レベルに設定し、CXP プローブのメトリックのデバッグを無効にする（これにより、通知よりも高いすべてのトレースレベルが無効になります）	コマンド **set platform software trace** *cxpd RP active cxpd-rtm* **notice** を使用します
デバッグトレースを有効にして、CXP プローブのメトリック処理の問題を分析する	コマンド **set platform software trace** *cxpd RP active cxpd-telemetry* **debug** を使用します
詳細レベルのデバッグトレースを有効にして、CXP プローブのメトリック処理の問題を分析する	コマンド **set platform software trace** *cxpd RP active cxpd-telemetry* **verbose** を使用します
デバッグレベルを通知レベルに設定し、CXP プローブのメトリックのデバッグを無効にする（これにより、通知よりも高いすべてのトレースレベルが無効になります）	コマンド **set platform software trace** *cxpd RP active cxpd-telemetry* **notice** level を使用します
デバッグトレースを有効にして、CXP と TTM モジュールのインタラクションシナリオを分析する	コマンド **set platform software trace** *cxpd RP active cxpd-ttm* **debug** を使用します

説明	コマンド
詳細レベルのデバッグトレースを有効にして、CXP と TTM モジュールのインタラクションシナリオを分析する	コマンド **set platform software trace** *cxpd RP active cxpd-ttm* **verbose** を使用します
デバッグレベルを通知レベルに設定し、CXP と TTM モジュールのインタラクションシナリオのデバッグを無効にする（これにより、通知よりも高いすべてのトレースレベルが無効になります）	コマンド **set platform software trace** *cxpd RP active cxpd-ttm* **notice** を使用します
デバッグトレースを有効にして、CXP モジュールレベルの問題を分析する（主にブートアップシナリオ中）	コマンド **set platform software trace** *cxpd RP active cxpd-misc* **debug** を使用します
デバッグトレースを有効にして、詳細な CXP モジュールレベルの問題を分析する（主にブートアップシナリオ中）	コマンド **set platform software trace** *cxpd RP active cxpd-misc* **verbose** を使用します
デバッグレベルを通知レベルに設定し、CXP モジュールレベルのデバッグを無効にする（これにより、通知よりも高いすべてのトレースレベルが無効になります）	コマンド **set platform software trace** *cxpd RP active cxpd-misc* **notice** を使用します
有効になっているさまざまな CXPD トレースのトレースレベルを確認する	コマンド **show platform software trace** *level cxpd* **RP active** を使用します
syslog とコンソールログを表示する	コマンド **show** *sdwan notification stream viptela* を使用します



第 6 章

アプリケーションリスト

（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。

表 *53* : 機能の履歴

機能名	リリース情報	説明
ユーザー定義の SaaS アプリケーションリスト	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1	この機能により、Cloud OnRamp for SaaS がモニターでき、最適なネットワークパスを決定できる SaaS アプリケーションの範囲が拡張されます。この機能により、1 つ以上の SaaS アプリケーションのリストと、それらの SaaS アプリケーションに関連するアプリケーションサーバーを定義できます。これらのリストについては、モニタリング可能な SaaS アプリケーションの定義済みセットを処理するのと同じ方法で処理します。 ユーザー定義リストを有効にすると、アプリケーションサーバーへのベストパスをプローブし、ベストパスを使用するように、リストにあるアプリケーションのアプリケーショントラフィックをルーティングします。

- SaaS アプリケーションリストに関する情報 （228 ページ）
- SaaS アプリケーションリストの前提条件 （229 ページ）

• SaaS アプリケーションリストの制約事項 （230 ページ）
• SaaS アプリケーションリストのユースケース （230 ページ）
• ワークフロー （231 ページ）
• Cisco SD-WAN Manager を使用したユーザー定義の SaaS アプリケーションリストの作成 （232 ページ）
• SaaS アプリケーションリストの表示 （233 ページ）

SaaS アプリケーションリストに関する情報

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 17.8.1a、Cisco vManage リリース 20.8.1

SaaS アプリケーションリスト

Cisco SD-WAN Manager では、Amazon AWS、Box などのクラウドアプリケーションにとってベストパスのトラフィックを決定できるようにするために、Cloud onRamp for SaaS によるモニタリング可能なクラウドアプリケーションを記載したプリセットリストを提供しています。Cisco SD-WAN Manager ではこうしたクラウドアプリケーションはそれぞれ単一のものとして表示されますが、実は密接に関連するアプリケーションがセットとして含まれている可能性のあるリストとなっています。ただし、詳細については Cisco SD-WAN Manager に表示されません。たとえば、Amazon AWS オプションで表示されるリストには、Amazon AWS 機能のアプリケーショントラフィックに絡むアプリケーションが複数記載されたリストがあります。こうしたリストは、SaaS アプリケーションリストと呼ばれています。

Cloud onRamp for SaaS は、SaaS アプリケーションリストごとに、プローブエンドポイントと呼ばれる単一のアプリケーションサーバーをプローブして、リストにあるアプリケーションのネットワークトラフィックにとってのベストパスを決定します。

NBAR

SaaS アプリケーションリスト内の各クラウドアプリケーションは、シスコ ネットワークベース アプリケーション認識（NBAR）によって定義されたアプリケーションになっています。NBAR とは、トラフィックを生成したネットワーク アプリケーションに従ってネットワークトラフィックを識別するテクノロジーのことです。インストールされたプロトコルパックに基づき、NBAR は、識別できるアプリケーションの標準セットに合わせて動作します（「Protocol Pack」を参照）。アプリケーションは標準セットの他に、カスタムアプリケーションを定義して（「Define Custom Applications」を参照）、NBAR が識別できるアプリケーションの範囲を拡張することも可能です。

ユーザー定義の SaaS アプリケーションリスト

ユーザー定義の SaaS アプリケーションリストは、関連アプリケーションを 1 つ以上含めて作成できます。アプリケーションは、インストールされたプロトコルパックを使用して NBAR が識別する標準アプリケーション、またはカスタムアプリケーションとなります。

SaaSアプリケーションリストごとに、アプリケーションサーバーをプローブエンドポイントとして指定します。Cloud onRamp for SaaS は、このサーバーをプローブして、SaaS アプリケーションリスト内のアプリケーションによって生成されるトラフィックに使用するベストパスを決定します。

ユーザー定義の SaaS アプリケーションリストについては、モニタリング可能な SaaS アプリケーションの定義済みセットを処理するのと同じ方法で処理します。ユーザー定義リストを有効にすると、アプリケーションサーバーへのベストパスをプローブし、ベストパスを使用するように、リストにあるアプリケーションのアプリケーショントラフィックをルーティングします。

（注） ユーザー定義のカスタムアプリケーションとは対照的に、ユーザー定義のSaaSアプリケーションリストは、ポリシー作成時に一致するオプションとして表示されません。（『Cisco SD-WAN Policies Configuration Guide』を参照）。

SaaS アプリケーションリストの利点

ユーザー定義の SaaS アプリケーションリストにより、Cloud onRamp for SaaS の範囲が拡張され、追加のクラウドアプリケーションが含まれるようになります。アプリケーションリストは、Cloud onRamp for SaaS の利点を、組織にとって特に関心のあるクラウドアプリケーションに拡張します。

SaaS アプリケーションリストの前提条件

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 17.8.1a、Cisco vManage リリース 20.8.1

- SD-AVC が有効である。
- 集中管理型ポリシーが定義され、アクティブである。

  集中管理型ポリシーの定義については、『Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x』を参照してください。
- ゲートウェイサイトがダイレクト インターネット アクセス（DIA）接続として SIG トンネルを使用する場合は、トンネルの設定で NBAR プロトコル検出を有効にします。

  NBAR プロトコル検出の有効化については、CLI を使用した SIG トンネル経由の Cloud onRamp for SaaS の設定 （216 ページ）を参照してください。

SaaS アプリケーションリストの制約事項

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 17.8.1a、Cisco vManage リリース 20.8.1

SaaS アプリケーションリストには、最大で 8 つのアプリケーションのみを含めることができます。

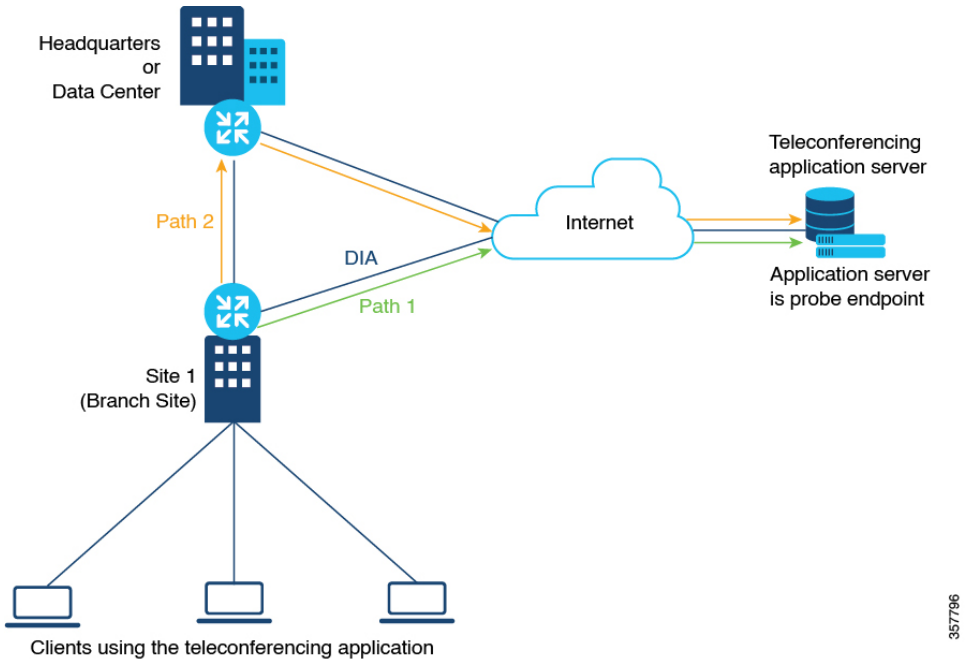
SaaS アプリケーションリストのユースケース

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 17.8.1a、Cisco vManage リリース 20.8.1

シナリオ

組織が、NBAR で認識されていない一般的でない電話会議システムを使用しています。この電話会議システムは、3 つの異なるネットワーク アプリケーションを使用して、音声、ビデオ、およびその他のメディアのトラフィックを管理します。3 つすべてのアプリケーションが、組織内の teleconf-internal.example.com ドメインにあるフロントエンドアプリケーション サーバーに接続します

図 *19 :* 使用例



カスタム アプリケーション

電話会議システムによって生成されたネットワークトラフィックを追跡するために、ネットワーク管理者は、上記のサーバー名または L3/L4 トラフィック属性（「Define Custom Applications」を参照）を使用して 3 つのカスタムアプリケーションを定義し、3 つのアプリケーションからのトラフィックを次のように識別します。

- teleconf-system-audio
- teleconf-system-video
- teleconf-system-media

これらのカスタムアプリケーションを定義すると、NBAR は 3 つそれぞれのアプリケーションからのトラフィックを識別できます。

SaaS アプリケーションリスト

3 つの電話会議関連のネットワーク アプリケーション セットのベストパスを最適化するために、ネットワーク管理者は teleconf-system という SaaS アプリケーションリストを作成し、3 つの関連するカスタムアプリケーションのそれぞれをこのアプリケーションリストに追加します。

SaaS アプリケーションリスト：teleconf-system
リスト内のアプリケーション：teleconf-system-audio、teleconf-system-video、teleconf-system-media

SaaS アプリケーションリストのプローブエンドポイントに対して、ネットワーク管理者は上記のフロントエンドサーバー（teleconf-internal.example.com）を指定します。これにより、3 つのアプリケーションのトラフィックが処理されます。

その結果、3 つのアプリケーションを含むアプリケーションリスト（teleconf-system）になります。ネットワーク管理者が Cloud onRamp for SaaS で teleconf-system アプリケーションリストを有効にすると、Cloud onRamp for SaaS がフロントエンドサーバーへのベストパスのプローブを開始します。Cloud onRamp for SaaS は、これら 3 つのアプリケーションのトラフィックをフロントエンドサーバーのベストパスにルーティングします。

ワークフロー

1. カスタムアプリケーション（プロトコルパックに含まれていないアプリケーション用）をアプリケーションリストに含める場合は、「Define Custom Applications」で説明されている手順を使用してカスタムアプリケーションを定義します。
2. アプリケーションリストは、アプリケーションを 1 つ以上含めて作成します。

   Cisco SD-WAN Manager を使用したユーザー定義の SaaS アプリケーションリストの作成（232 ページ）を参照してください。
3. Cloud OnRamp for SaaS でアプリケーションリストを有効にします。

「Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager」を参照してください。

Cisco SD-WAN Manager を使用したユーザー定義の SaaS アプリケーションリストの作成

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 17.8.1a、Cisco vManage リリース 20.8.1

1. 次のいずれかの方法を使用して、[Cloud OnRamp for SaaS] ページを開きます。
   - Cisco SD-WAN Manager のメインメニューから、**[Configuration]** > **[Cloud OnRamp for SaaS]** を選択します。

     または

   - Cisco SD-WAN Manager のメニューから、右上付近にあるクラウドアイコンをクリックし、[Cloud OnRamp for SaaS] を選択します。
2. [Manage Cloud OnRamp for SaaS] ドロップダウンリストで、[SaaS Application Lists] を選択します。
3. [New Custom Application List] をクリックします。
4. リストの名前を入力します。
5. アプリケーションをリストに追加するには、[Search] フィールドをクリックしてアプリケーションを選択します。このリストには、標準アプリケーションと、定義したカスタムアプリケーションがあります。

   必要に応じて、[Search] フィールドにテキストを入力して、特定のアプリケーションをフィルタリングできます。

   選択したアプリケーションは、[Application] フィールドというリスト内の各アプリケーションを表示する場所に追加されます。
6. 必要に応じて、このワークフロー内に新しいカスタムアプリケーションを作成するには、[Search] フィールドをクリックし、[New Custom Application] をクリックします。このページでカスタムアプリケーションを作成することは、「Define Custom Applications」で説明されているように、集中管理型ポリシーワークフローでカスタムアプリケーションを定義することと同じです。カスタムアプリケーションの定義に必要な情報、ワイルドカード文字の使用、入力した属性とトラフィックを照合するときに適用されるロジックなどの詳細については、「Define Custom Applications Using Cisco SD-WAN Manager」を参照してください。
7. [SaaS Probe Endpoint Type] エリアで、プローブエンドポイントを定義します。このエンドポイントこそ、SaaS アプリケーションリストのトラフィックにとってのベストパスを決定するために、Cloud OnRamp for SaaS がプローブするサーバーです。

- 次のオプションからエンドポイントのタイプを選択します。
  - [IP Address]：IP アドレスを入力します。Cloud OnRamp for SaaS は、ポート 80 を使用してサーバーをプローブします。
  - [FQDN]：完全修飾ドメイン名を入力します。
  - [URL]：HTTP または HTTPS を使用して URL を入力します。Cloud OnRamp for SaaS は、提供された URL によって、ポート 80 またはポート 443 を使用してサーバーをプローブします。
- 選択するエンドポイントのタイプに基づいて、エンドポイント値を入力します。

  例：192.168.0.1、https://www.example.com

8. [Add] をクリックします。アプリケーションリストの表に新しい SaaS アプリケーションリストが表示されます。

SaaS アプリケーションリストの表示

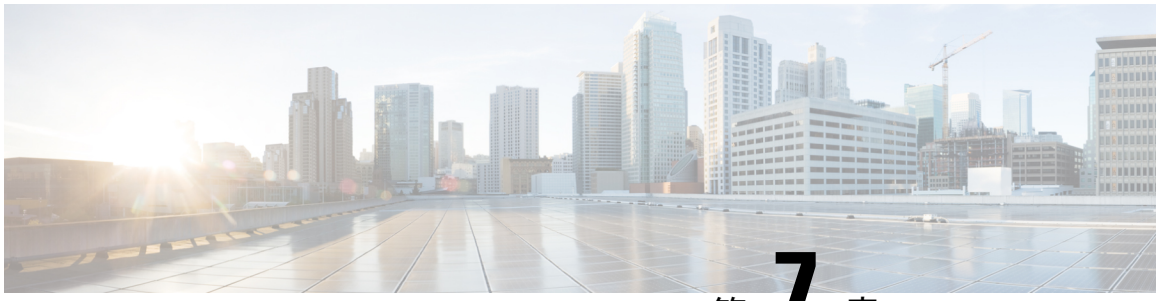
サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a、Cisco vManage リリース 20.8.1

1. 次のいずれかの方法を使用して、[Cloud onRamp for SaaS] ページを開きます。
   - Cisco SD-WAN Manager のメインメニューから、**[Configuration]** > **[Cloud onRamp for SaaS]** を選択します。

     または

   - Cisco SD-WAN Manager のメニューから、右上付近にあるクラウドアイコンをクリックし、[Cloud onRamp for SaaS] を選択します。
2. [Manage Cloud onRamp for SaaS] ドロップダウンリストで、[SaaS Application Lists] を選択します。

   各 SaaS アプリケーションリストの詳細がテーブルに表示されます。必要に応じて、[Action] 列のアイコンをクリックして、リストを編集または削除できます。



第 7 章

Cloud OnRamp for SaaS、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r

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。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r を使用しているデバイスにのみ、この項で説明されているワークフローを使用します。以降のリリースについては、「Cloud OnRamp for SaaS, Cisco IOS XE Release 17.3.1a and Later」を参照してください。

この機能は、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r で完全に機能するベータ版としてリリースされ、プロビジョニング ワークフローが将来のリリースで変更される可能性がありました。このワークフローは Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a で廃止され、Cisco IOS XE Catalyst SD-WAN デバイスおよび Cisco vEdge デバイスに対応する統合ワークフローに置き換えられました。

表 *54* : 機能の履歴

機能名	リリース情報	説明
Cloud OnRamp for SaaS、Cisco IOS XE Catalyst SD-WAN デバイス	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	Cloud OnRamp for SaaS は Cisco IOS XE Catalyst SD-WAN デバイスで使用できますが、設定ワークフローは Cisco vEdge デバイスに適用されるワークフローとはまったく異なります。 この機能は、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r で完全に機能するベータ版としてリリースされています。プロビジョニング ワークフローは、将来のリリースで変更される可能性があります。

多くの組織は、ビジネスに不可欠な機能を Software-as-a-Service（SaaS）アプリケーションに依存しています。これらのクラウドベースのサービスには、Office365、Salesforce、Box などの、多くのサービスがあります。クラウドベースのサービスとして、これらの SaaS アプリケーションは、インターネット接続を介して使用可能な独自のリモートサーバーと通信する必要があります。

リモートサイトでは、SaaS アプリケーションによって次のような特別な課題が発生する可能性があります。

- **パフォーマンス**：ブランチオフィスなどのリモートサイトが、データセンターなどの一元化された場所を介して SaaS トラフィックをルーティングすると、パフォーマンスが低下し、遅延が発生してユーザー体験に影響を与えます。
- **ルーティングを最適化できない**：ネットワーク管理者が、これらの SaaS アプリケーションのパフォーマンスを可視化できない場合や、SaaS トラフィックのルーティングをより効率的なパスに変更できない場合があります。

Cloud OnRamp for SaaS（旧称 CloudExpress サービス）は、これらの課題に対処します。これにより、特定の SaaS アプリケーションおよびインターフェイスを選択し、SD-WAN が指定されたインターフェイスを使用して各 SaaS アプリケーションのパフォーマンスが最も高いパスを決定できるようになります。たとえば、以下を有効にすることができます。

- ブランチサイトでのダイレクト インターネット アクセス（DIA）接続を介したルーティング（使用可能な場合）
- 地域のデータセンターなどの、ゲートウェイの場所を介したルーティング

SD-WAN は各 SaaS アプリケーションの使用可能な各パスを継続的にモニターするため、1 つのパスで問題が発生した場合は、SaaS トラフィックを動的に調整して、より適切なパスに移動させることができます。

詳細については、『SD-WAN: Cloud OnRamp for SaaS Deployment Guide』を参照してください。

- 概要：Cloud onRamp for SaaS の設定方法 （237 ページ）
- Cloud onRamp for SaaS を使用する一般的なシナリオ （238 ページ）
- プローブ機能テンプレートの作成 （245 ページ）

• Cloud onRamp for SaaS のポリシーの作成 （248 ページ）

概要：Cloud onRamp for SaaS の設定方法

vEdge デバイスで Cloud onRamp for SaaS を使用するのとは異なり、Cisco XE SD-WAN デバイスの機能を設定するには、次の 2 つの手順を実行します。

- ベストパスの決定（機能テンプレートによって設定）
- ベストパスの使用（ポリシーによって設定）

次に、タスクの概要を示します。

	タスク	コンポーネント	まとめ
1	SaaS アプリケーションのベストパスの決定	機能テンプレート	特定の SaaS アプリケーションサーバーのパスをプローブするように Cloud onRamp for SaaS を設定する機能テンプレートを作成して、それぞれのベストパスを決定し、これらのパスに基づいてテーブルを作成します。 SD-WAN は定期的にプローブし、ベストパスに関する最新情報でテーブルを更新します。 トポロジにゲートウェイサイトとブランチサイトが含まれている場合は、ブランチサイトとゲートウェイサイトに個別の機能テンプレートが必要です。 「プローブ機能テンプレートの作成」を参照してください。 （注） プローブ機能テンプレートは、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のリリースではサポートされていません。

	タスク	コンポーネント	まとめ
2	SaaS アプリケーションのベストパスの使用	ポリシー	前の手順で決定されたベストパスを使用するように特定の SaaS アプリケーションに指示するポリシーを作成します。 (注) このポリシーでは、機能テンプレートに含まれている SaaS アプリケーションのみを指定します。機能テンプレートに含まれていない SaaS アプリケーションがこのポリシーで指定されている場合、そのアプリケーションのトラフィックは、Cloud onRamp for SaaS が有効になっていない場合と同様にデフォルトのパスを使用します。 「Cloud onRamp for SaaS のポリシーの作成」を参照してください。

Cloud onRamp for SaaS を使用する一般的なシナリオ

SD-WAN を使用している組織の場合、通常、ブランチサイトはデフォルトで SaaS アプリケーション トラフィックを SD-WAN オーバーレイリンク経由でデータセンターにルーティングします。データセンターから、SaaS トラフィックは SaaS サーバーに到達します。

たとえば、中央データセンターとブランチサイトがある大規模な組織で、従業員がブランチサイトで Office 365 を使用する場合があります。デフォルトでは、ブランチサイトの Office 365 トラフィックは、SD-WAN オーバーレイリンクを介して中央データセンターにルーティングされ、そこから Office 365 クラウドサーバーにルーティングされます。

シナリオ 1：ブランチサイトにダイレクト インターネット アクセス（DIA）接続がある場合は、データセンターをバイパスしてその直接ルートを介して SaaS トラフィックをルーティングすることで、パフォーマンスを向上させることができます。

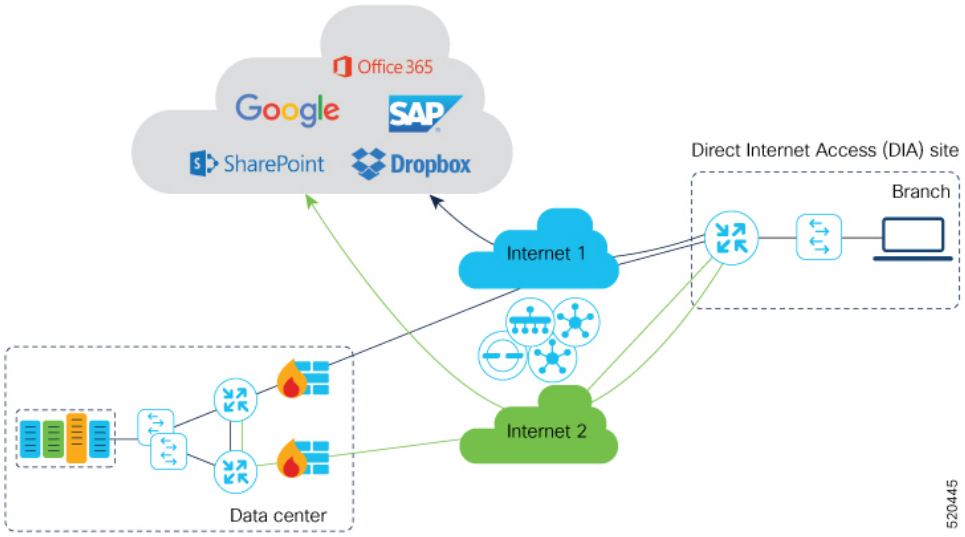
シナリオ 2：DIA リンクがあるゲートウェイサイトにブランチサイトが接続する場合、SaaS トラフィックがゲートウェイサイトの DIA を使用できるようにすることができます。

シナリオ 3：ハイブリッド方式。

シナリオ1：ダイレクトインターネットアクセスリンクを介したクラウドアクセス

このシナリオでは、次の図に示すように、ブランチサイトに 1 つ以上のダイレクト インターネット アクセス（DIA）リンクがあります。

Cloud onRamp for SaaS を使用すると、SD-WAN は、DIA リンクまたは SD-WAN オーバーレイ リンクを介して、各 SaaS アプリケーションに最適な接続を選択できます。最適な接続は、SaaS アプリケーションによって異なる場合があることに注意してください。たとえば、Office365 のトラフィックはある 1 つのリンクを介すると高速になり、Dropbox のトラフィックは別のリンクを介すると高速になる可能性があります。



設定ワークフロー

ブランチサイト専用のプローブ機能テンプレートを作成し、Cloud onRamp for SaaS を使用するためのポリシーを設定します。

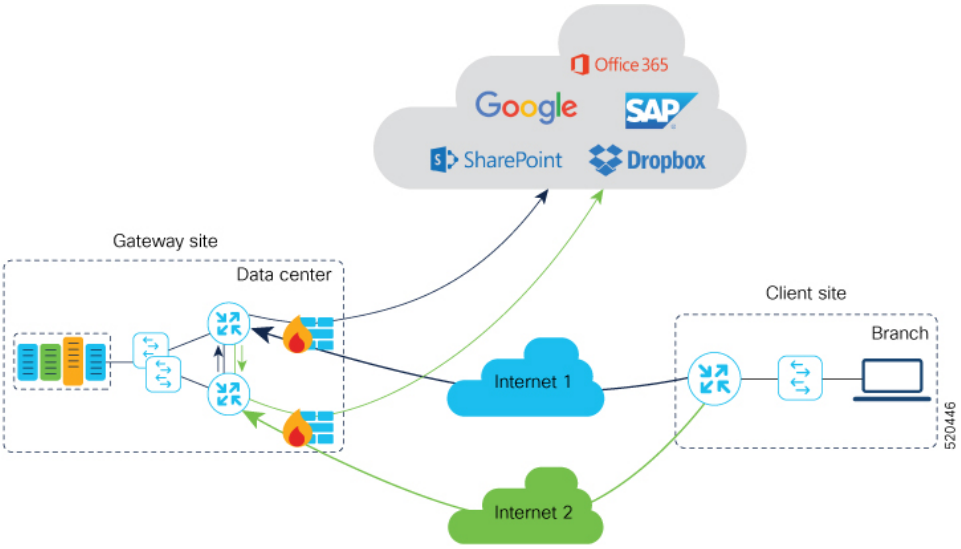
	タスク	詳細
ブランチ サイト		

	タスク	詳細
1	ブランチサイトのプローブ機能テンプレートを作成します。	プローブ機能テンプレートで、次のようにパラメータを設定します。 • [SaaS Mode]：[SaaS Branch] • [TLOCS]：[All DIA TLOC] または [TLOC List] を選択して、ドロップダウンメニューでTLOCの色を選択します。 • [All DIA TLOC]：ブランチのすべてのTLOC に対して DIA が有効になっている場合は、このオプションを選択します。 • [TLOC List]：サイトの一部の TLOC でのみ DIA が有効になっている場合は、このオプションを選択してから、DIA が有効になっている TLOC に対応する色を選択できます。 • [SaaS applications]：Cloud onRamp for SaaS のアプリケーションを指定します。 「プローブ機能テンプレートの作成」を参照してください。
2	ブランチサイトのデバイステンプレートで機能テンプレートを使用します。	デバイステンプレートの [Additional Templates] セクションの [Probes] フィールドで、前の手順で作成した機能テンプレートを選択します。
3	デバイステンプレートをブランチサイトに適用します。	
ポリシー		
4	ポリシーを作成します。	アプリケーションルートポリシーの一致条件で、クラウドSaaSアプリケーションを選択し、機能テンプレートの作成時に指定したものと同じアプリケーションを指定します。アクションとして [Cloud SLA] を選択します。 「Cloud onRamp for SaaS のポリシーの作成」を参照してください。
5	ポリシーをアクティブにします	以前に作成した機能テンプレートが適用されたブランチサイトにポリシーを適用します。

シナリオ 2：ゲートウェイサイトを介したクラウドアクセス

このシナリオでは、ブランチサイトにゲートウェイサイトへの直接接続が 1 つ以上あり、ゲートウェイサイトにインターネットへのリンクがあります。

Cloud onRamp for SaaS を使用すると、SD-WAN は、ゲートウェイサイトを介して、各 SaaS アプリケーションに最適な接続を選択できます。ブランチサイトが複数のゲートウェイサイトに接続している場合、異なるゲートウェイサイトを通過する場合でも、SD-WAN は各 SaaS アプリケーションについて SaaS トラフィックがベストパスを使用するようにします。



設定ワークフロー

ブランチサイトとゲートウェイサイトのプローブ機能テンプレートを作成し、Cloud onRamp for SaaS を使用するためのポリシーを設定します。

	タスク	詳細
ブランチ サイト		

	タスク	詳細
1	ブランチサイトのプローブ機能テンプレートを作成します。	プローブ機能テンプレートで、次のようにパラメータを設定します。 • [SaaS Mode]：[SaaS Branch] • [TLOCS]：[All DIA TLOC] • [SaaS applications]：アプリケーションを指定しません。 （注） シナリオ 1（ダイレクト インターネット アクセス リンクを介したクラウドアクセス）と比較して、このワークフローの違いに注意してください。このワークフローでは、ゲートウェイサイト設定でアプリケーションを指定します（以下を参照）。 「プローブ機能テンプレートの作成」を参照してください。
2	ブランチサイトのデバイステンプレートで機能テンプレートを使用します。	デバイステンプレートの [Additional Templates] セクションの [Probes] フィールドで、前の手順で作成した機能テンプレートを選択します。
3	デバイステンプレートをブランチサイトに適用します。	
ゲートウェイサイト		
4	ゲートウェイサイトのプローブ機能テンプレートを作成します。	• ゲートウェイサイトが同一のルータとインターフェイスを使用していない限り、各ゲートウェイサイトには個別の機能テンプレートが必要です。 • [SaaS Mode]：[SaaS Gateway] [SaaS Gateway] を選択した後に、プローブを開始するインターフェイス名を指定します。このインターフェイスは、ゼロ以外の VPN にバインドする必要があります。 • [SaaS applications]：Cloud onRamp for SaaS のアプリケーションを指定します。 「プローブ機能テンプレートの作成」を参照してください。

	タスク	詳細
5	ゲートウェイサイトのデバイステンプレートで、前の手順で作成した機能テンプレートを使用します。	デバイステンプレートの [Additional Templates] セクションの [Probes] フィールドで、前の手順で作成した機能テンプレートを選択します。
6	デバイステンプレートをゲートウェイサイトに適用します。	
ポリシー		
7	ポリシーを作成します。	上記のタスク 4 の機能テンプレートと同じアプリケーションを指定します。 「Cloud onRamp for SaaS のポリシーの作成」を参照してください。
8	ポリシーをアクティブにします。	以前に作成した機能テンプレートが適用されたブランチサイトおよびゲートウェイサイトにポリシーを適用します。

シナリオ 3：ハイブリッドアプローチ

このシナリオでは、ブランチサイトには、ダイレクトインターネットアクセス（DIA）リンクと、インターネットへのリンクもあるゲートウェイサイトへのリンクの両方があります。

Cloud onRamp for SaaS を使用すると、SD-WAN は、DIA リンクまたはゲートウェイサイトを介して、各 SaaS アプリケーションに最適な接続を選択できます。

設定ワークフロー

ブランチサイトとゲートウェイサイトのプローブ機能テンプレートを作成し、Cloud onRamp for SaaS を使用するためのポリシーを設定します。

	タスク	詳細
ブランチ サイト		

	タスク	詳細
1	ブランチサイトのプローブ機能テンプレートを作成します。	プローブ機能テンプレートで、次のようにパラメータを設定します。 • [SaaS Mode]：[SaaS Branch] • [TLOCS]：[All DIA TLOC] または [TLOC List] を選択して、ドロップダウンメニューでTLOCの色を選択します。 • [All DIA TLOC]：ブランチのすべてのTLOC に対して DIA が有効になっている場合は、このオプションを選択できます。 • [TLOC List]：サイトの一部の TLOC でのみ DIA が有効になっている場合は、このオプションを選択してから、DIA が有効になっている TLOC に対応する色を選択できます。 • [SaaS applications]：アプリケーションを指定します。 「プローブ機能テンプレートの作成」を参照してください。
2	ブランチサイトのデバイステンプレートで機能テンプレートを使用します。	デバイステンプレートの [Additional Templates] セクションの [Probes] フィールドで、前の手順で作成した機能テンプレートを選択します。
3	デバイステンプレートをブランチサイトに適用します。	
ゲートウェイサイト		

	タスク	詳細
4	ゲートウェイサイトのプローブ機能テンプレートを作成します。	• ゲートウェイサイトが同一のルータおよびインターフェイスを使用していない限り、各ゲートウェイサイトには個別の機能テンプレートが必要です。 • [SaaS Mode]：[SaaS Gateway] [SaaS Gateway] を選択した後に、プローブを開始するインターフェイス名を指定します。このインターフェイスは、ゼロ以外の VPN にバインドする必要があります。 • [SaaS applications]：Cloud onRamp for SaaS のアプリケーションを指定します。 「プローブ機能テンプレートの作成」を参照してください。
5	ゲートウェイサイトのデバイステンプレートで、前の手順で作成した機能テンプレートを使用します。	デバイステンプレートの [Additional Templates] セクションの [Probes] フィールドで、前の手順で作成した機能テンプレートを選択します。
6	デバイステンプレートをゲートウェイサイトに適用します。	
ポリシー		
7	ポリシーを作成します。	上記のタスク 4 の機能テンプレートと同じアプリケーションを指定します。 「Cloud onRamp for SaaS のポリシーの作成」を参照してください。
8	ポリシーをアクティブにします。	以前に作成した機能テンプレートが適用されたブランチサイトおよびゲートウェイサイトにポリシーを適用します。

プローブ機能テンプレートの作成

（注） プローブ機能テンプレートは、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のリリースではサポートされていません。

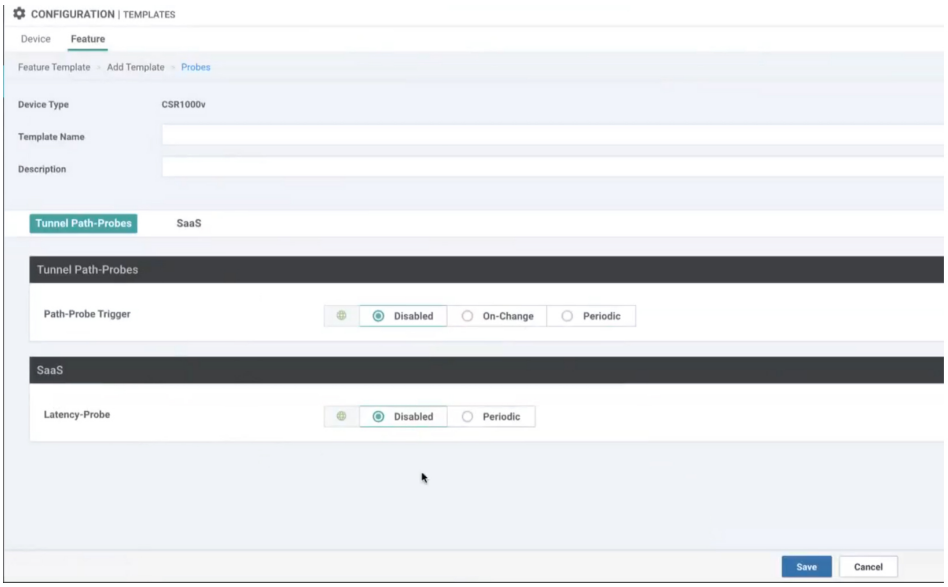
Cisco XE SD-WAN デバイスで Cloud OnRamp for SaaS を使用するためのプローブテンプレートを作成するには、次の手順を実行します。

ブランチサイトまたはゲートウェイサイトに適用する機能テンプレートを作成します。テンプレートの [SaaS Mode] オプションで、ブランチサイトとゲートウェイサイトのどちらでテンプレートを使用するかを決定します。

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 20.7.1 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Add template] をクリックします。
4. デバイスモデルを選択します。
5. [Other Templates] で [Probes] をクリックして、Cloud OnRamp for SaaS のプローブテンプレートを作成します。



6. 必要に応じて、次のフィールドを設定します。一部のオプションを選択すると、他のフィールドで使用できるオプションが変更されます。

フィールド	説明
Tunnel Path-Probes	
Path-Probe Trigger	[Disabled] に設定する必要があります。 （注） 本リリースではサポートされていません。

フィールド	説明
Latency-Probe	[Disabled]：この機能テンプレートで Cloud OnRamp for SaaS が無効になります。 [Periodic]：Cloud OnRamp for SaaS が有効になります。
Latency-Probe Frequency	サイトと SaaS アプリケーション クラウド サーバー間のリンクをプローブする頻度（秒）。プローブは、利用可能な各パスの遅延を判断します。 範囲：0 ～ 65535 デフォルト：30 （注） 推奨：デフォルト値の 30
SaaS Mode	この機能テンプレートのサイトのタイプを選択します。 [SaaS Branch]：ブランチサイトに適用される機能テンプレートの場合。 [SaaS Gateway]：ゲートウェイサイトに適用される機能テンプレートの場合。
TLOCS	（[SaaS Mode] の [SaaS Branch] オプションで利用可能） [All DIA TLOC]：有効な色が割り当てられている、サイトのすべてのダイレクト インターネット アクセス（DIA）インターフェイスを含めます。 [TLOC List]：1 つ以上の色を指定して、含めるインターフェイスを示します。これらのインターフェイスは、SaaS トラフィックで見込まれるルーティングパスを判断します。
TLOCS List Color	（[TLOCS] の [TLOC List] オプションで利用可能） ドロップダウンリストを使用して色を選択します。複数の色を選択できます。
Interface [x]	（[SaaS Mode] の [SaaS Gateway] オプションで利用可能） ゲートウェイサイトの 1 つ以上のインターフェイス名を指定します。機能テンプレートは、これらのインターフェイスのみに適用されます。 例：gig2/0
Path-Probe	[Disabled] に設定する必要があります。 （注） 本リリースではサポートされていません。

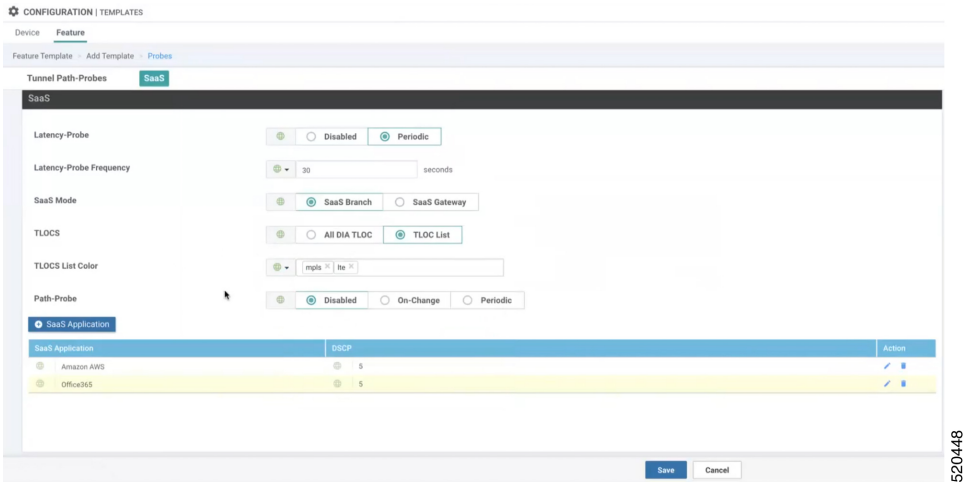
7. [SaaS Application] をクリックして、次のフィールドを表示します。これらのフィールドを使用して、SaaS アプリケーションを指定します。このプロセスを繰り返して、さらにアプリケーションを追加します。

アプリケーションを指定すると、このウィンドウの SaaS アプリケーションテーブルに表示されます。このテーブルには、リスト内のアプリケーションを編集または削除するオプションを備えたアクション列が含まれています。

フィールド	説明
SaaS App	ドロップダウンメニューを使用してアプリケーションを選択します。
DSCP	（注） Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降では、Cisco SD-WAN Manager CoR SaaS ワークフローはこのオプションをプッシュしません。指定された DSCP 値は、この設定オプションを有効にした場合でも使用されません。 Differentiated Services Code Point（DSCP）の整数値を入力します。値を入力する必要がありますが、システムでは使用されません。異なるアプリケーションに同じ DSCP 値を割り当てることができます。 範囲：0 ～ 63

8. [保存（Save）] をクリックして、テンプレートを保存します。

   例：以下の例は、mpls および lte インターフェイスを含むブランチサイト用に設定されたプローブ機能テンプレートを示しています。これにより、Amazon AWS および Office365 SaaS アプリケーションのベストパスを決定します。



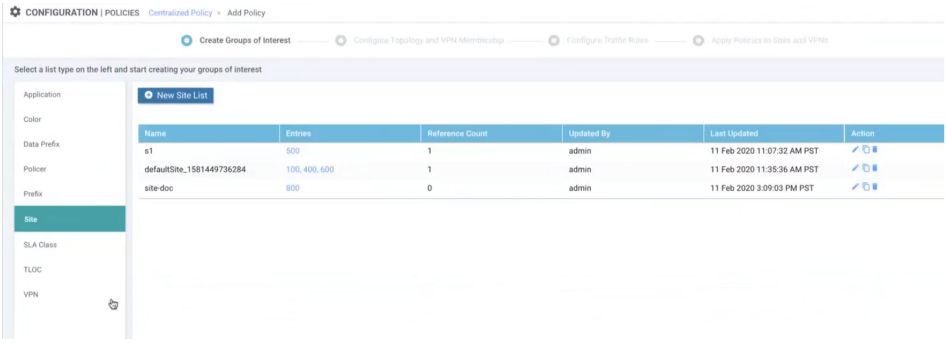
9. デバイステンプレートで機能テンプレートを使用するには、次の手順を実行します。

   デバイステンプレートの [Additional Templates] の [Probes] フィールドで、前述の手順で作成した機能テンプレートを選択します。

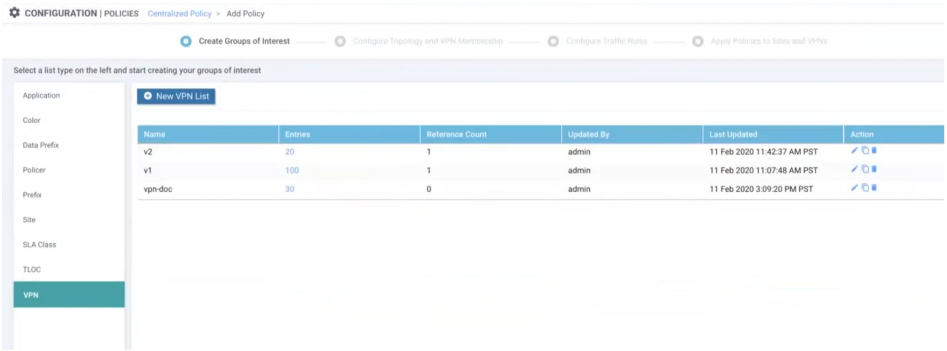
Cloud onRamp for SaaS のポリシーの作成

1. [Configuration] > [Policy] を選択します。

2. [Centralized Policy] タブをクリックします。
3. [Add Policy] をクリックします。
4. 左側のペインで、[Site] をクリックします。
5. ポリシーを適用するサイトのリストを作成します。このリストは後の手順で使用します。
   1. [新しいサイトリスト（New Site List）] をクリックします。
   2. [Site List Name] フィールドに、サイトリスト名を入力します。
   3. [Add Site] フィールドに、1 つ以上のサイト番号を入力します。
   4. [Add] をクリックします。
      サイトがサイトのテーブルに追加されます。

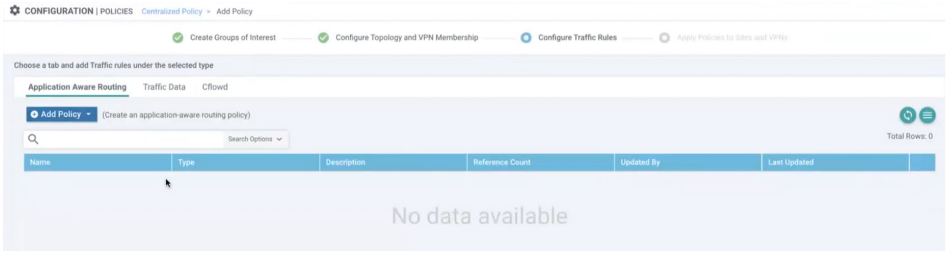


6. 左側のペインで、[VPN] を選択します。
7. ポリシーを適用する VPN のリストを作成します。このリストは後の手順で使用します。
   1. [新しいVPNリスト（New VPN List）] をクリックします。
   2. [VPN List Name] フィールドに、VPN リストの名前を入力します。
   3. [Add VPN] フィールドに、1 つ以上の番号を入力します。
   4. [Add] をクリックします。
      VPN が VPN のテーブルに追加されます。



8. [Next] を 2 回クリックして、[Configure Traffic Rules] ステップを表示します。

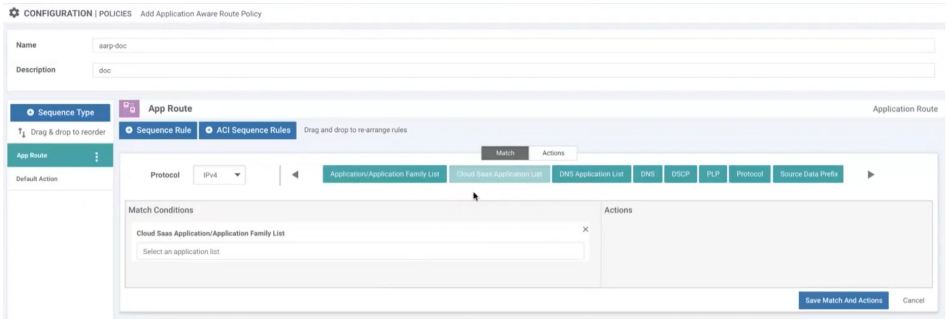
   [Application Aware Routing] タブがデフォルトで選択されています。



9. [Add Policy] をクリックし、[Create New] を選択します。

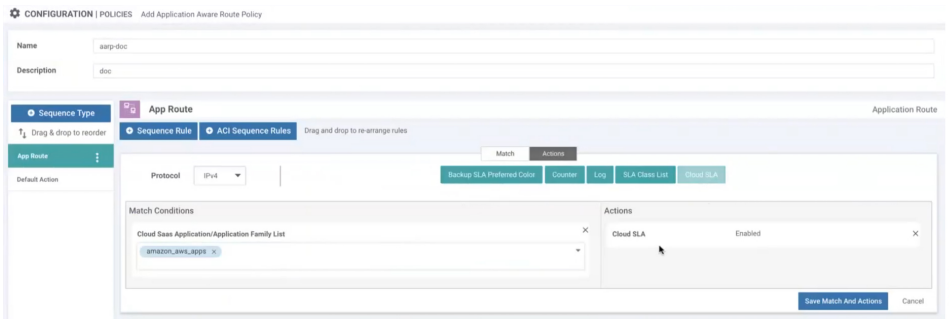
10. ポリシーを作成します。

    1. ポリシーの名前と説明を入力します。
    2. [シーケンスタイプ（Sequence Type）] をクリックします。
    3. [Sequence Rule] をクリックします。
    4. デフォルトの [Match] が選択されている状態で、[Cloud SaaS Application List] をクリックします。



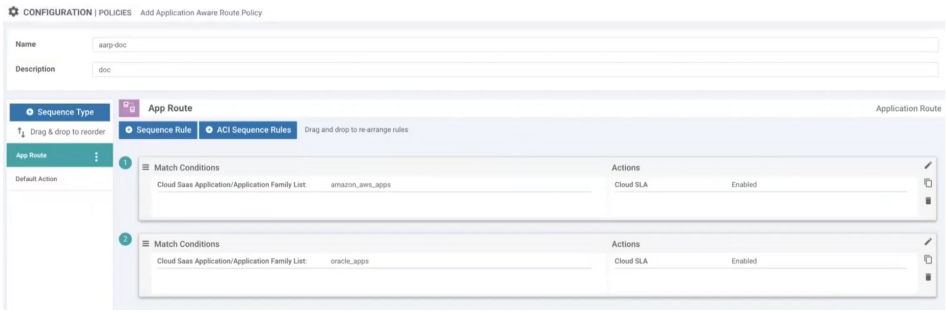
    5. [Match Conditions] セクションで、SaaS アプリケーションを指定します。この SaaS アプリケーションで、Cloud onRamp for SaaS が有効になります。
    6. [アクション（Actions）] をクリックします。
    7. [クラウドSLA（Cloud SLA）] をクリックします。

       [Actions] セクションに、[Cloud SLA Enabled] と表示されます。



8. [一致とアクションの保存（Save Match and Actions）] をクリックします。
9. このポリシーに別の SaaS アプリケーションを追加するには、[Sequence Rule] を再度クリックし、10c の手順に従います。

   次の例は、一致条件とアクションを含む2つのシーケンスルールを示しています。各ルールは単一の SaaS アプリケーションを指定しています。



520454

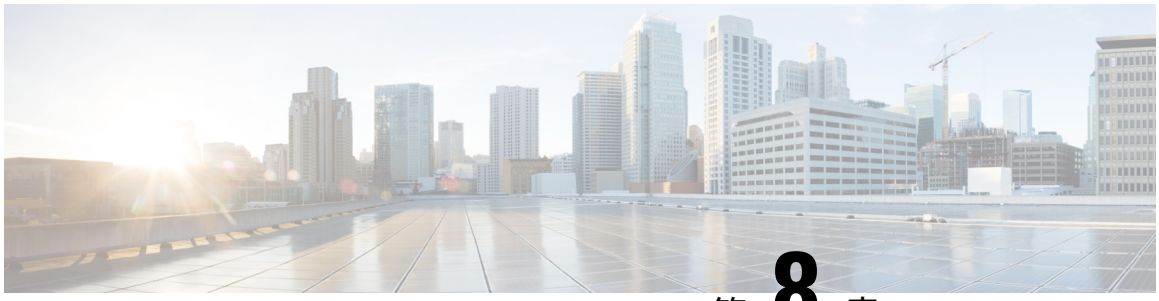
10. [アプリケーション認識型ルーティングポリシーの保存（Save Application Aware Routing Policy）] をクリックします。
11. [Next] をクリックして、[Apply Policies to Sites and VPNs] ステップを表示します。
12. [Application-Aware Routing] タブをクリックします。
13. ポリシーを選択します。
14. [New Site List and VPN List] をクリックします。この手順で前に作成したサイトリストと VPN リストを選択します。
15. [Add] をクリックします。
16. [Save Policy] をクリックします。

11. ポリシーをアクティブにします。
    1. [Configuration] > [Policies] を選択します。
    2. ポリシーのリストで、アクティブ化するポリシーを見つけます。[more actions]（...）ボタンをクリックし、[Activate] を選択して、サイト ID によってポリシーで指定されたデバイスにポリシーをプッシュします。

第 II 部

Cloud OnRamp for Multicloud

- Cloud OnRamp for Multicloud （255 ページ）
- AWS の統合 （257 ページ）
- Amazon GovCloud（米国）の統合 （289 ページ）
- Microsoft Azure Virtual WAN の統合 （295 ページ）
- 米国政府向け Microsoft Azure の統合 （333 ページ）
- Google Cloud の統合 （339 ページ）
- マルチクラウドサービスのモニタリングのための Cisco Catalyst SD-WAN Manager のサポート （365 ページ）



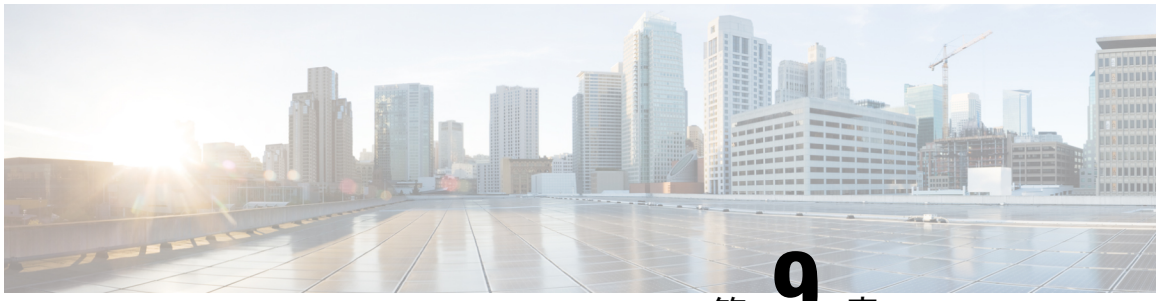
第 8 章

Cloud OnRamp for Multicloud

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。

Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud は、エンタープライズ WAN をパブリック クラウドに拡張します。このマルチクラウド ソリューションは、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のに役立ちます。

- AWS の統合 （257 ページ）
- Microsoft Azure Virtual WAN の統合 （295 ページ）
- Google Cloud の統合 （339 ページ）
- マルチクラウドサービスのモニタリングのための Cisco Catalyst SD-WAN Manager のサポート （365 ページ）



第 9 章

AWS の統合

（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。

表 *55* : 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイスを使用した AWS ブランチの統合	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	Cisco Catalyst SD-WAN Cloud OnRamp for Infrastructure as a Service（IaaS）は、エンタープライズ WAN をパブリッククラウドに拡張します。このマルチクラウド ソリューションは、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のに役立ちます。この機能は、標準の Cloud OnRamp ソリューションでは不十分な場合にトランジットゲートウェイを有効にします。たとえば、1 つのホスト VPC がインターネットゲートウェイを使用して Cisco Catalyst SD-WAN エッジルータに接続されているとします。インターネットゲートウェイの帯域幅制限が小さい場合は、トランジットゲートウェイが SD-WAN 統合に使用されます。これにより、VPC と VPN を相互接続する方法が提供されます。

機能名	リリース情報	説明
Cisco Catalyst 8000V Edge ソフトウェアインスタンスの従量制ライセンスのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	Amazon Web Services（AWS）で新しいクラウドゲートウェイを作成するときに、これまでサポートされていた所有ライセンス持ち込み（BYOL）モデルに加えて、従量制（PAYG）ライセンスで Cisco Catalyst 8000V Edge ソフトウェアインスタンスを使用することができます。
Cisco IOS XE Catalyst SD-WAN デバイスと AWS Transit Gateway Connect 機能を使用した Cisco Catalyst SD-WAN ブランチと AWS の統合	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	このリリースでは、AWS Transit Gateway Connect 機能を使用して、クラウドゲートウェイを AWS Transit Gateway に接続することができます。この GRE ベースの接続タイプは、IPSec VPN トンネル接続を使用する場合と比較して、帯域幅、スケーリング、およびセキュリティが向上します。
AWS ブランチ接続ソリューション	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能は、AWS Transit Gateway のサポートを利用して、ブランチデバイスをクラウドに接続します。 ブランチデバイスは、IPSec トンネルベースのセキュアチャネルを使用してトランジットゲートウェイに接続し、クラウドでホストされているアプリケーションにアクセスします。この機能は、Cisco SD-WAN Manager で AWS Transit Gateway をインスタンス化、管理、および制御するシナリオをサポートしています。
AWS Cloud WAN の統合	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN Manager リリース 20.12.1	この機能により、AWS Cloud WAN を使用して、AWS グローバルネットワークを介してリモートサイト、リージョン、およびクラウドアプリケーションからのトラフィックを簡単に接続およびルーティングすることができます。この機能は、サイト間通信にスタティックルーティングを使用します。
AWS Cloud WAN とダイナミックルーティングの統合	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、ダイナミックルーティングを使用したサイト間通信をサポートするための AWS Cloud WAN 統合の拡張機能です。

機能名	リリース情報	説明
設定グループを使用した AWS 統合のためのデバイスの設定	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	この機能により、Cisco SD-WAN Manager の設定グループを使って、AWS 統合のために自動化を使用してデバイスを設定することができます。

- AWS 統合に関する情報 （259 ページ）
- AWS 統合の制約事項 （264 ページ）
- AWS 統合の設定 （266 ページ）
- インテント管理 - 接続 （282 ページ）
- トランジット ゲートウェイ ピアリング （285 ページ）
- 監査管理 （286 ページ）
- Cisco SD-WAN Manager を使用した AWS 統合のモニター （287 ページ）

AWS 統合に関する情報

トランジットゲートウェイは、VPC とオンプレミスネットワークを相互接続するために使用できるネットワーク トランジット ハブです。VPC または VPN 接続をトランジットゲートウェイに接続できます。VPC と VPN 接続の間を流れるトラフィックの仮想ルータとして機能します。

Cisco SD-WAN Manager コントローラを使用して、Cloud OnRamp for Multicloud を設定および管理できます。Cisco SD-WAN Manager の構成ウィザードは、パブリック クラウド アカウントへのトランジットゲートウェイの起動、トランジットゲートウェイと Cisco Catalyst 8000V Edge を含むクラウドゲートウェイの作成、オーバーレイネットワーク内のブランチでのパブリッククラウドアプリケーションとそれらのアプリケーションのユーザーとの間の接続を自動化します。この機能は、Cisco Cloud ルータ上の AWS 仮想プライベートクラウド（VPC）で動作します。

Cloud OnRamp for Multicloud は、複数の AWS アカウントとの統合をサポートしています。詳細については、「Limitations for AWS Integration」を参照してください。

サポートされるプラットフォーム

AWS での Cloud OnRamp for Multicloud では、次のプラットフォームがサポートされています。

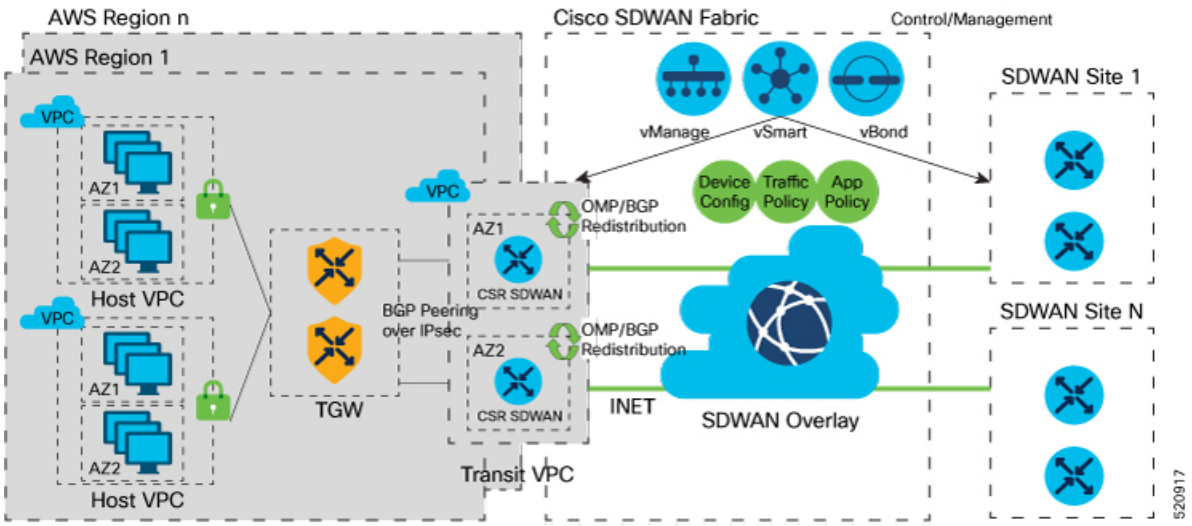
- Cisco Cloud Services Router 1000V シリーズ（Cisco CSR1000V）

（注） このプラットフォームは、Cisco SD-WAN Manager リリース 20.3.x でサポートされています。

- Cisco Catalyst 8000V Edge ソフトウェア

（注） このプラットフォームは、Cisco SD-WAN Manager リリース 20.4.x 以降でサポートされています。

アーキテクチャ



マルチクラウド ダッシュボード

Cisco SD-WAN Manager のマルチクラウド ダッシュボードは、次のワークフローで構成されています。

- 設定
- 検出
- 管理
- インテント管理

設定

AWS 自動化のために、Cisco SD-WAN Manager でクラウドアカウントを作成および管理し、グローバル設定を構成することができます。複数のアカウントを作成して、トランジットゲートウェイ用に特定のアカウントを選択し、トランジット VPC 自動化用に 1 つ以上のアカウントをマークし、ホスト VPC の検出および接続用に他のアカウントを使用することができます。

マルチクラウド ダッシュボードは、認証のために **AWS キー**と **IAM ロール** のモデルをサポートしています。IAM ロールは、特別な AWS AssumeRole 関数が必要なため、AWS クラウド導入型の Cisco SD-WAN Manager でのみ機能します。AssumeRole は、クロスアカウントアクセスに使用されます。

グローバル設定

グローバル設定を使用すると、1 回設定することでリージョン全体でその設定を繰り返し、リソース管理をグローバルに（クラウドごとに）処理することができます。指定されたソフトウェアイメージとインスタンスサイズが、クラウドゲートウェイの一部として、クラウドでの CSR のインスタンス化に使用されます。

次に、グローバル設定を示します。

- [Software image]：クラウドゲートウェイの作成に使用される CSR ソフトウェアイメージ。
- [AWS Instance Size]：帯域幅要件に応じて使用される CSR インスタンスサイズ。
- [Cloud Gateway Solution]：AWS クラウドに使用されるゲートウェイソリューション。たとえば、トランジット VPC を使用するトランジットゲートウェイなどです。
- [IP subnet pool]：リージョン全体でトランジット VPC の作成に使用される IP サブネットプール。サブネットプールは、必要に応じて、カスタム設定オプションを使用してクラウドゲートウェイごとにカスタマイズできます。
- [Intra-Tag Communication]：同じタグの下の VPC 間の通信を許可または拒否します。
- [Default Route in Host VPCs]：デフォルトルートが、トランジットゲートウェイを指す VPC のメインルートテーブルに自動的に追加されます。
- [Full Mesh of Transit VPCs]：さまざまなリージョンのクラウドゲートウェイの TVPC 間にフルメッシュ接続を設定し、パブリッククラウドバックボーン経由でサイト間トラフィックを（CSR を介して）伝送します。

（注） AWS 展開の Cisco Catalyst 8000V のグローバル設定でトランジット VPC のフルメッシュが有効になっている場合、GigabitEthernet3 インターフェイスがこの設定に自動的に使用されます。このインターフェイスを他の目的に使用したり、インターフェイスの設定を変更したりすることはできません。

（注） グローバル設定で一度選択したイメージとインスタンスサイズは、すべてのリージョンに適用されるわけではありません。イメージ検出に使用されるアカウントは異なる場合があり、選択したイメージまたはインスタンスサイズがすべてのリージョンでサポートされているとは限りません。AWS インスタンスサイズとソフトウェアイメージのパラメータは、設定の更新後に作成された新しいクラウドゲートウェイに対してのみ変更できます。

サイト間通信の場合は、追加のインターフェイスが設定されます。グローバル設定でサイト間通信が有効または無効になると、必要な設定が自動的にプッシュまたは削除されます。

VPC の検出

リージョン全体で提供されるすべてのアカウントのすべての VPC を検出できます。これらの VPC をタグ付けおよびタグ解除し、将来の接続に使用することができます。Cisco SD-WAN Manager ではキー **Cisco-SDWAN-key** を使用してタグが作成され、同じタグ内のすべての VPC のタグ値をカスタマイズすることができます。グローバル設定で [Intra-Tag communication] が有効になっている場合、同じタグを使用して VPC をマッピングする（つまり、VPC 間の接続を確立する）ことができます。タグを編集し、VPCに関連付けられたタグのメンバーシップを変更することができます。

（注） インターコネクトゲートウェイに関連付けられているタグを追加する場合、[Intent Management] で AWS クラウドゲートウェイにマッピングすることはできません。

クラウドゲートウェイ

クラウドゲートウェイは、トランジットVPC、2つのCSRデバイス、およびトランジットゲートウェイで構成されます。クラウドゲートウェイをインスタンス化するアカウントとリージョンを選択すると、Cisco SD-WAN Managerがすべてのコンポーネントを作成します。PnP スマートアカウントから同期された未使用の利用可能な CSR 汎用一意識別子（UUID）に適切なデバイステンプレートをアタッチできます。

グローバル設定をカスタム設定でオーバーライドして、特定の展開用に別のイメージ、インスタンスサイズ、およびサブネットプールを選択することができます。リージョンごとに1つのクラウド ゲートウェイ インスタンスのみがサポートされます。

（注） AWS Marketplace で、クラウドゲートウェイに必要なイメージに登録していることを確認します。登録していない場合、クラウドゲートウェイの作成は失敗します。

AWS ブランチ接続の概要

エッジデバイスは、セキュアなポイント ツー ポイント トンネルを介してクラウド内のホスト VPC に接続します。エッジデバイスと AWS Transit Gateway の間に IPSec トンネルが設定されます。これらのトンネルは、ブランチ VPN トラフィックと BGP ルーティングトラフィックを伝送します。BGP を使用して、デバイスとトランジットゲートウェイがルーティング情報を交換し、ルーティングテーブルを構築します。

ブランチデバイスには、ホスト VPC への接続を必要とする VPN をいくつでも設定できます。これらの VPN はそれぞれ、トランジットゲートウェイへの VPN アタッチメントとして表されます。VPN アタッチメントの一部として、AWS カスタマーゲートウェイおよび VPN ゲートウェイ クラウド オブジェクトが作成され、ブランチデバイスからトランジットゲートウェイへの VPN 接続が可能になります。特定のサイトのトランジットゲートウェイとブランチデバイスは、異なるBGP ASN内にあります。タグ（ホストVPC）へのVPNのマッピング情報は、グローバルマッピングから取得されます。このマッピングがクラウドで実現されます。

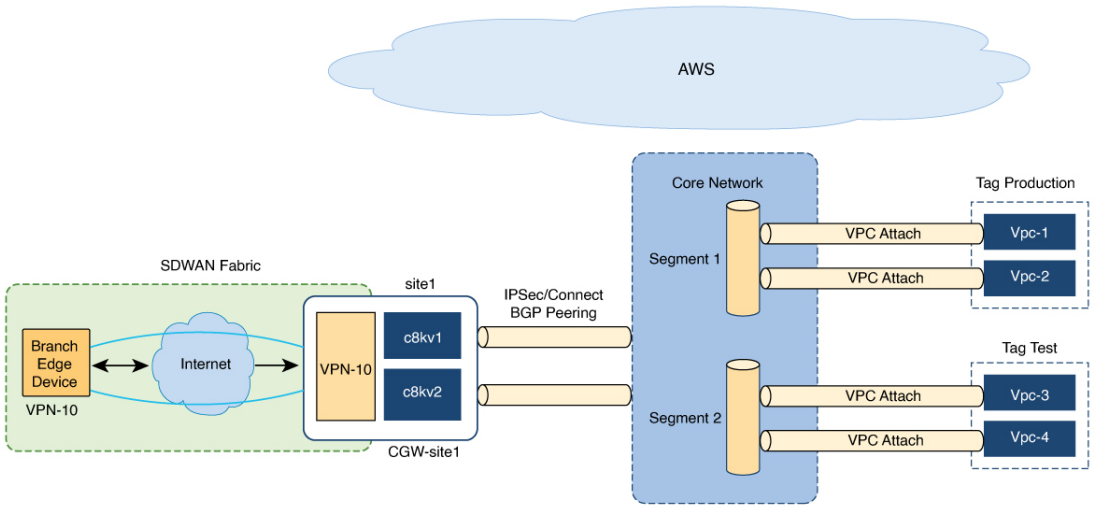
ブランチデバイステンプレートで新しいサービス VPN を設定すると、更新イベントが生成され、接続マトリックスに基づいてマッピングがトリガーされます。同様に、デバイステンプレートからサービス VPN を削除すると、別の更新イベントが生成され、マッピングの解除がトリガーされます。

（注） ブランチエッジ WAN インターフェイスの数は、ブランチエッジデバイスが接続する必要があるリージョンの数に比例する必要があります。たとえば、ブランチが 2 つの AWS リージョン内のホストに接続する必要がある場合は、そのリージョンの各クラウドゲートウェイに 1 つの WAN インターフェイスをアタッチする必要があります。ブランチ内の WAN インターフェイスを同じ色にすることはできません。

AWS Cloud WAN

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 17.12.1a、Cisco Catalyst SD-WAN Manager リリース 20.12.1

図 *20 : AWS Cloud WAN*



AWS Cloud WAN は、統合グローバルネットワークの構築、管理、およびモニターに使用できるマネージド WAN サービスです。AWS グローバルネットワークを介して、さまざまなサイトやリージョンからのトラフィックを簡単に接続してルーティングすることができます。

AWS Cloud WAN を使用すると、シンプルなネットワークポリシーを使用してネットワークを設定および保護することができます。Cisco SD-WAN Manager ワークフローを使用して AWS 統合を設定すると、バックエンドでネットワークポリシーが定義されて入力されます。

AWS 統合ワークフローを使用すると、グローバル AWS クラウド WAN ネットワークを作成し、さまざまなセグメントを定義し、さまざまなリージョンのさまざまな VPC をこれらのセグメントにアタッチすることができます。

（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 17.13.1a および Cisco Catalyst SD-WAN Manager リリース 20.13.1）AWS Cloud WAN 統合は、スタティックルートを使用する代わりに、BGP ベースのダイナミックルーティングを使用して、さまざまなサイトやリージョンからのトラフィックをルーティングします。AWS 統合ワークフローでは、クラウドゲートウェイには、IPSec ベースの接続を可能にするセグメントとの BGP ピアリングがあります。これにより、ワークフローに柔軟性と冗長性が追加されています。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 から Cisco Catalyst SD-WAN Manager リリース 20.13.1 へのアップグレードの考慮事項

- Cisco Catalyst SD-WAN Manager リリース 20.13.1 にアップグレードする前に、Cisco SD-WAN Manager で AWS のサイト間通信を無効にします（グローバル設定内）。アップグレードが完了したら、グローバル設定でサイト間通信を有効にできます。

設定グループを使用した AWS 統合のためのデバイスの設定に関する情報

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a および Cisco Catalyst SD-WAN Manager リリース 20.14.1

Cisco SD-WAN Manager 内の設定グループを使用して、AWS 統合ワークフローでデバイスを設定できます。2 つのクラウドゲートウェイ間で同じ設定グループを使用することはサポートされていません。

グローバル設定の設定グループを使用して、デバイスの設定を有効にすることができます。グローバル設定で設定グループを使用した設定を有効にしていた場合は、クラウドゲートウェイを作成するときに、既存の設定グループを選択するか、新しい設定グループを作成することができます。設定グループの詳細については、『Cisco Catalyst SD-WAN Configuration Groups』を参照してください。

（注） グローバル設定で設定グループを使用したデバイスの設定を有効にすると、テンプレートと設定グループの両方を使用してデバイスを設定することができます。

AWS 統合の制約事項

- AWS Government クラウド（AWS GovCloud）はサポートされていません。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 以降では、AWS GovCloud（米国）がサポートされています。

- IPv6 での AWS 統合はサポートされていません。
- CIDR が重複しているホスト VPC に関連付けられているタグは、相互にマッピングできません。
- 1 つのホスト VPC にマッピングされた異なる VPN での IP アドレスの重複はサポートされていません。
- AWS には、VPN 接続ごとに 1,000 ルートの制限があります。VPN ごとにより多くのルートがある場合は、BGP で集約アドレスまたはネットワークを使用してテンプレートをプロビジョニングする必要があります。
- AWS Transit Gateway には、デフォルトでは 20 個のルートテーブルのみがあります。
- AWS コンソールを介したクラウドゲートウェイの自動修正削除は設定されていません。
- リージョンごとに 1 つのクラウドゲートウェイのみを作成できます。
- Cisco Cloud ルータの 1 つのペアのみがインスタンス化されます。
- 選択した CSR イメージのバージョンが、16.12.02r 以降である必要があります。
- Cisco SD-WAN Manager は、CSR 1000 デバイスごとに 1 つの VPN トンネルを設定します。これにより、ソリューションの帯域幅は 2.5 GBPS（各トンネルのスループットは 1.25 GBPS）に制限されます。
- Cisco IOS XE リリース 17.6.2 以降では、Cloud OnRamp for Multicloud は 10 個の AWS アカウントとの統合をサポートしています。
- マルチクラウド AWS ブランチ接続ソリューションは、機能テンプレートを使用して展開された Cisco SD-WAN ブランチまたはデバイスでのみ機能します。設定グループを使用したブランチまたはデバイスはサポートされていません。
- AWS リージョンでローカルゾーンが有効になっている CGW 展開はサポートされていません。

AWS Cloud WAN の制約事項

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 17.12.1a、Cisco Catalyst SD-WAN Manager リリース 20.12.1

- 同じ AWS アカウントからのみクラウドゲートウェイを作成できます。
- AWS Government クラウド（AWS GovCloud）はサポートされていません。
- AWS Cloud WAN は、コアネットワークごとに最大 20 個のセグメントのみをサポートしています。
- コアネットワークごとにサポートされるピアリングの最大数は 50 です。
- AWS Cloud WAN をサポートしていないリージョンでは、クラウドゲートウェイを作成できません。現在サポートされているリージョンについては、AWS のドキュメントを参照してください。

- トンネルの BGP セッションのステータスを取得するための API のサポートは、AWS では使用できません。そのため、Cisco SD-WAN Manager で、クラウドゲートウェイの電源がオフになっている場合でも AWS Cloud WAN ネットワークへのトンネルが到達可能として表示される場合があります。

AWS 統合の設定

AWS 設定の前提条件

Cisco SD-WAN Manager を使用して AWS 統合を設定するには、以下が必要です。

- AWS クラウドアカウントの詳細
- AWS Marketplace へのサブスクリプション
- Cisco SD-WAN Manager には、新しいアカウントを作成するために自由に使用できる 2 つのクラウドルータライセンスが必要です

AWS クラウドアカウントの作成

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。Cloud OnRamp for Multicloud ダッシュボードが表示されます。
2. [Setup] ペインで [Associate Cloud Account] をクリックします。[Associate Cloud Account] ページの外部 ID をメモします。
3. [Cloud Provider] フィールドで、ドロップダウンリストから [Amazon Web Services] を選択します。
4. [Account Name] フィールドにアカウント名を入力します。
5. （任意）[Description] フィールドに説明を入力します。
6. [Use for Cloud Gateway] で、アカウントにクラウドゲートウェイを作成する場合は [Yes] を選択し、しない場合は [No] を選択します。
7. [Login in to AWS With]フィールドで、使用する認証モデルを選択します。
   - **Key**
   - **IAM 役割**

   [Key] モデルを選択した場合は、[API Key] および [Secret Key] フィールドで、それぞれのキーを指定します。

   または

[IAM Role] モデルを選択した場合は、Cisco SD-WAN Manager が提供する [External ID] を使用して IAM ロールを作成します。ウィンドウに表示された外部 ID をメモして、IAM ロールの作成時に使用できる [Role ARN] 値を指定します。

Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降では、IAM ロールを作成するには、AWS 管理コンソールを使用して Cisco SD-WAN Manager から提供された外部 ID をポリシーに入力する必要があります。次の手順を実行します。

1. 既存の Cisco SD-WAN Manager EC2 インスタンスに IAM ロールをアタッチします。
    1. ポリシーを作成するには、AWS ドキュメントの IAM ロールの作成（コンソール）のトピックを参照してください。AWS の [Create policy] ウィザードで、[JSON] をクリックし、次の JSON ポリシードキュメントを入力します。

```
{

"Version": "2012-10-17",

  "Statement": [{

    "Sid": "VisualEditor0",

"Effect": "Allow",

    "Action": "sts:AssumeRole",

"Resource": "*"

    }
]

}
```

    2. IAM ロールを作成し、ステップ 1 で作成したポリシーに基づいて Cisco SD-WAN Manager EC2 インスタンスにアタッチする方法については、AWS Security Blog の「Easily Replace or Attach an IAM Role to an Existing EC2 Instance by Using the EC2 Console」ブログを参照してください。

（注） [Attach permissions policy] ウィンドウで、手順 1 で作成した AWS 管理ポリシーを選択します。

（注） 次の権限セットが許可されます。

- AmazonEC2FullAccess
- IAMReadOnlyAccess
- AWSNetworkManagerFullAccess
- AWSResourceAccessManagerFullAccess

AWS IAM ロールの作成の詳細については、「Creating an AWS IAM Role」[英語] を参照してください。

2. マルチクラウド環境に使用する AWS アカウントで IAM ロールを作成します。
   1. AWS ドキュメントの IAM ロールの作成（コンソール）のトピックを参照して、[Require external ID] をオンにし、手順 2 でメモした外部 ID を貼り付けて、IAM ロールを作成します。
   2. ロールを担当できるユーザーを変更するには、AWS ドキュメントのロール信頼ポリシーの変更（コンソール）のトピックを参照してください。

      [IAM Roles] ウィンドウで、下にスクロールして、前の手順で作成したロールをクリックします。

      [Summary] ウィンドウで、上部に表示される [Role ARN] をメモします。

（注） 手順 7 で IAM ロールとして認証モデルを選択した場合は、このロール ARN 値を入力できます。

3. 信頼関係を変更したら、[JSON] をクリックし、次の JSON ドキュメントを入力します。変更内容を保存します。

（注） 次の JSON ドキュメントのアカウント ID は、Cisco SD-WAN Manager EC2 インスタンスに属しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::[Account ID from Part 1]:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "[vManage provided External ID]"
```

```
            }
          }
        }
      ]
    }
```

8. [Add] をクリックします。

クラウドアカウントの詳細を表示または更新するには、[Cloud Account Management] ページで [...] をクリックします。

また、関連付けられたホスト VPC タグまたはクラウドゲートウェイがない場合は、クラウドアカウントを削除することもできます。

（注） マルチクラウドリソースのクリーンアッププロセス中に、Cisco SD-WAN Managerは現在のデータベースを、組織名とアカウントの詳細タグを使用してアカウント内の実行中のリソースと比較します。タグには一致するが、現在のデータベースにないリソースがある場合は、削除されます。したがって、組織名および関連するAWSアカウントの詳細が同じ場合、Cisco SD-WAN Manager の AWS マルチクラウドリソースは別の Cisco SD-WAN Manager によって削除される可能性があります。複数の異なる Cisco SD-WAN Manager オーバーレイで同じ AWS アカウントを使用している場合は、Cisco SD-WAN Manager ごとに異なる組織名とオーバーレイ名を使用することをお勧めします。

クラウドグローバル設定の構成

クラウド トランジット ゲートウェイのグローバル設定を構成するには、次の手順を実行します。

1. Cisco SD-WAN Managerのメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。[Setup] ペインで [Cloud Global Settings] をクリックします。[Cloud Global Settings] ウィンドウが表示されます。
2. （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）

   設定グループを使用してデバイスを設定するには、[Enable Configuration Group] オプションを有効にします。
3. [Cloud Provider] フィールドで、[Amazon Web Services] を選択します。
4. [Cloud Gateway Solution] ドロップダウンリストをクリックして、[AWS Transit Gateway and CSR in Transit VPC] を選択します。または、Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降では、次のいずれかのオプションを選択します。

   Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降では、オプションの組み合わせはサポートされていません。たとえば、VPN接続を使用して作成されたクラウドゲートウェイがある場合、AWS Transit Gateway Connect接続を作成する前に、これらのクラウドゲートウェイを削除する必要があります。

- [Transit Gateway–VPN based (using TVPC)]：AWS クラウドでインスタンス化されたトランジットゲートウェイを介して、クラウドゲートウェイをクラウド内の VPC に接続できるようにします。クラウドゲートウェイは、トランジット VPC 内でインスタンス化される 1 組のクラウドサービスルータで構成されます。このオプションでは、AWS VPN 接続（IPSec）アプローチを使用します。
- [Transit Gateway–Connect based (using TVPC)]：AWS クラウドでインスタンス化されたトランジットゲートウェイを介して、クラウドゲートウェイをクラウド内の VPC に接続できるようにします。クラウドゲートウェイは、トランジット VPC 内でインスタンス化される 1 組のクラウドサービスルータで構成されます。このオプションでは、AWS TGW Connect（GRE トンネル）アプローチを使用します。
- [Transit Gateway–Branch-connect]：AWS クラウドでインスタンス化されたトランジットゲートウェイを介して、さまざまな Cisco Catalyst SD-WAN エッジデバイスをクラウド内の VPC に接続できるようにします。このオプションでは、AWS VPN 接続（IPSec）アプローチを使用します。
- （サポートされている最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.12.1）

  [Cloud WAN–VPN based (using TVPC)]：AWS Cloud Wan を介して、クラウドゲートウェイをクラウド内の VPC に接続できるようにします。クラウドゲートウェイは、トランジット VPC 内でインスタンス化される 1 組のクラウドサービスルータで構成されます。このオプションでは、AWS VPN 接続（IPSec）アプローチを使用します。
- （サポートされている最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.12.1）

  [Cloud WAN–Connect based (using TVPC)]：AWS Cloud Wan を介して、クラウドゲートウェイをクラウド内の VPC に接続できるようにします。クラウドゲートウェイは、トランジット VPC 内でインスタンス化される 1 組のクラウドサービスルータで構成されます。このオプションでは、AWS Connect アタッチメント（GRE トンネルのサポート）アプローチを使用します。

5. Cisco vManage リリース 20.8.1 以降では、次のフィールドを使用できます。
   - [Reference Account Name] ドロップダウンリストをクリックして、参照アカウント名を選択します。Cisco SD-WAN Manager は、この参照アカウント名を使用してソフトウェアイメージとインスタンスサイズを検出します。

（注） 必要に応じて、クラウドゲートウェイの作成時に別のアカウントを選択することもできます。

   - [Reference Region] ドロップダウンリストをクリックして、参照リージョンを選択します。Cisco SD-WAN Manager は、参照されたアカウント名の下で、この参照リージョン内のソフトウェアイメージとインスタンスサイズを検出します。

6. [Software Image] フィールドで、次の手順を実行します。
   1. [BYOL] をクリックして所有ライセンス持ち込みソフトウェアイメージを使用するか、[PAYG] をクリックして従量制課金ソフトウェアイメージを使用します。
   2. ドロップダウンリストから、ソフトウェアイメージを選択します。
7. [Instance Size] ドロップダウンリストをクリックして、必要なサイズを選択します。
8. [IP Subnet Pool] を入力します。
9. [Cloud Gateway BGP ASN Offset] を入力します。
10. [Intra Tag Communication] を選択します。オプションは、[Enabled] または [Disabled] です。
11. [Default Route] を選択します。オプションは、[Enabled] または [Disabled] です。
12. [Update] をクリックします。

パラメータ	説明
ソフトウェア イメージ	アカウントの事前インストール済みまたは登録済みソフトウェアイメージを指定します。

パラメータ	説明
Instance Size	

パラメータ	説明
	インスタンスサイズを指定します。次のオプションがあります。 • t2.medium • t3.medium • c4.2xlarge • c4.4xlarge • c4.8xlarge • c4.xlarge • c5.2xlarge • c5.4xlarge • c5.9xlarge • c5.large • c5.xlarge • c5n.2xlarge • c5n.4xlarge • c5n.9xlarge • c5n.large • c5n.xlarge （注） Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降では、次のインスタンスタイプがサポートされています。 • t3.medium • c5.2xlarge • c5.4xlarge （注） Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a 以降では、c5.4xlarge はサポートされていません。 • c5.9xlarge • c5.large • c5.xlarge • c5n.2xlarge

パラメータ	説明
	• c5n.4xlarge • c5n.9xlarge • c5n.large • c5n.xlarge Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a 以降では、次のインスタンスがサポートされています。 • c5n.18xlarge (注) c3.2xlarge の Cisco SD-WAN Manager リリース 19.2.1 で実行されている Cisco Catalyst SD-WAN クラウドデバイスを、次の順序で Cisco SD-WAN Manager リリース 20.4.1 以降にアップグレードします。 1. c3.2xlarge から c5.4xlarge へのサイズ変更 2. ソフトウェアを Cisco SD-WAN Manager リリース 20.4.1 以降にアップグレードします。 (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降では、次のインスタンスタイプがサポートされています。 • t3.medium • c5.large • c5.xlarge • c5.2xlarge • c5.9xlarge • c5n.4xlarge • c5n.18xlarge • c6in.large • c6in.xlarge • c6in.2xlarge • c6in.8xlarge

パラメータ	説明
Cloud Gateway Solution	クラウドゲートウェイ ソリューションの組み合わせを指定します。たとえば、[AWS Transit Gateway and CSR in Transit VPC] などです。
IP Subnet Pool	IP サブネットのリストをカンマで区切って CIDR 形式で指定します。複数のサブネットを指定できます。 単一の /24 サブネットプールは、1 つのクラウドゲートウェイのみをサポートできます。 いくつかのクラウドゲートウェイがすでにプールを使用している場合、プールを変更することはできません。 サブネットの重複は許可されていません。
Cloud Gateway BGP ASN Offset	トランジットゲートウェイ BGP ASN の割り当てのオフセットを指定します。これは、あるトランジットゲートウェイ（eBGP）から別のトランジットゲートウェイへの、学習したルートをブロックするために使用されます。 30 個の一連の ASN が、トランジットゲートウェイ ASN 用に予約されています。開始オフセットに 30 を加えたものが、組織側の BGP ASN になります。たとえば、オフセットが 64,830 の場合、組織 BGP ASN は 64,860 になります。 開始オフセットの許容範囲は 64,520 ～ 65,500 です。10 の倍数である必要があります。

パラメータ	説明
Tunnel Count	このフィールドは、[Cloud Gateway Solution] ドロップダウンリストから [Transit Gateway–Connect based (using TVPC)] を選択した場合に表示されます。 VPN 接続のトンネル数を入力します。 VPN 接続ごとに最大 4 つのトンネルを構成できます。各トンネルは、最大 5 Gbps のトラフィックをサポートします。 (注) このパラメータの値を変更しても、既存のクラウドゲートウェイには影響しません。既存のクラウドゲートウェイのトンネル数を更新するには、**[Configuration]** > **[Cloud OnRamp For Multicloud]** > **[Cloud Gateway]** ページからクラウドゲートウェイを編集します。
Intra Tag Communication	同じタグのホスト VPC 間の通信を有効にするか無効にするかを指定します。タグ付けされた VPC がすでに存在し、クラウドゲートウェイがそれらのリージョンに存在する場合、このフラグは変更できません。
Program Default Route in VPCs towards TGW	デフォルトルートでプログラムされるホスト VPC のメインルートテーブルを有効にするか無効にするかを指定します。
Full Mesh of Transit VPCs	サイト間トラフィックを（CSR 経由で）伝送するための、異なるリージョンのクラウドゲートウェイの TVPC 間のフルメッシュ接続を指定します。

表 *56 :* グローバル設定の予期される動作

アイテム	クラウドゲートウェイの作成後に変更可能（対応/非対応）	デフォルト（有効/無効）
ソフトウェア イメージ	対応	該当なし
Instance Size	対応	該当なし
IP Subnet Pool	以下の説明を参照してください	該当なし
Cloud Gateway BGP ASN Offset	非対応	該当なし

アイテム	クラウドゲートウェイの作成後に変更可能（対応/非対応）	デフォルト（有効/無効）
Intra Tag Communication	クラウドゲートウェイとタグ付きホスト VPC の両方がいずれかのリージョンに存在する場合は変更できません	API レベルで有効
Program Default Route in VPCs towards TGW	非対応	API レベルで有効
Full Mesh of Transit VPCs	対応	ディセーブル

[Global IP Subnet Pool]：グローバルサブネットプールを使用しているクラウドゲートウェイがない場合にのみ更新できます。クラウドゲートウェイは、カスタム設定の有無にかかわらず、グローバルサブネットプールを使用します。サブネットプールの値は、グローバル設定の値と似ています（CIDR のリストをカンマで区切った後に比較できます。たとえば、10.0.0.0/8, 10.255.255.254/8 と 10.255.255.254/8, 10.0.0.0/8 は似ています）。

グローバルサブネットプールを使用しているクラウドゲートウェイがない場合、グローバル設定内の更新されたサブネットプールは、既存のカスタムサブネットプールと重複しないようにする必要があります。

[Custom IP Subnet Pool]：カスタム設定を作成する場合、そのサブネットプールは既存のカスタムサブネットプールと重複しないようにする必要があります。設定されたグローバルサブネットプールと部分的に重複することはできません。

ホスト プライベート ネットワークの検出

利用可能なアカウントの各リージョンすべてにわたって、すべてのアカウントのホスト VPC を検出できます。ホスト VPC 検出が呼び出されると、VPC の検出はキャッシュなしで実行されます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。[Discover] の下の [Host Private Networks] をクリックします。[Discover Host Private Networks] ウィンドウに、使用可能な VPC のリストが表示されます。

   [host VPC] テーブルには次の列があります。

   - クラウド リージョン
   - アカウント名
   - ホスト VPC 名
   - ホスト VPC タグ
   - アカウント ID（Account ID）
   - ホスト VPC ID

必要に応じて、列をクリックして VPC を並べ替えます。

2. [Region] ドロップダウンリストをクリックして、特定のリージョンに基づいて VPC を選択します。
3. [Tag Actions] をクリックして、次のアクションを実行します。
   - [Add Tag]：選択した VPC をグループ化し、これらの VPC に同時にタグ付けします。
   - [Edit Tag]：選択した VPC をあるタグから別のタグに移行します。
   - [Delete Tag]：選択した VPC のタグを削除します。

   複数のホスト VPC をタグの下にグループ化できます。同じタグの下のすべての VPC は、単一のユニットと見なされます。タグは接続を確実にし、**インテント管理**で VPC を表示するために不可欠です。

クラウドゲートウェイの作成

クラウドゲートウェイは、クラウド内のトランジット VPC（TVPC）、TVPC 内の CSR、およびトランジットゲートウェイをインスタンス化したものです。クラウドゲートウェイを作成するには、次の手順を実行します。

（注） この手順を開始する前に、同じタイプのライセンス（BYOL または PAYG）を持つ、テンプレートがアタッチされた 2 つのデバイスがあることを確認します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。[Manage] の下にある [Create Cloud Gateway] をクリックします。[Manage Cloud Gateway - Create] ウィンドウが表示されます。
2. [Cloud Provider] フィールドで、ドロップダウンリストから [Amazon Web Services] を選択します。
3. [Cloud Gateway Name] フィールドに、クラウドゲートウェイ名を入力します。
4. （任意）[Description] に説明を入力します。
5. [Account Name] ドロップダウンリストからアカウント名を選択します。
6. [Region] ドロップダウンリストからリージョンを選択します。
7. （オプション）ドロップダウンリストから SSH キーを選択します。
8. （最小リリース：Cisco vManage リリース 20.10.1）[Site Name] ドロップダウンリストから、クラウドゲートウェイを作成するサイトを選択します。
9. [Software Image] フィールドで、次の手順を実行します。

1. ライセンスオプションを選択します。所有ライセンス持ち込みの場合は[BYOL]、従量課金の場合は [PAYG] を選択します。
2. ドロップダウンメニューで、ソフトウェアイメージを選択します。

（注） ソフトウェアイメージのオプションは、[BYOL] と [PAYG] のどちらを選択するかによって決まります。

（注） Cisco Cloud OnRamp for Multicloud を使用せずに Cisco Catalyst 8000V をオンボーディングする方法については、『Cisco SD-WAN Getting Started Guide』を参照してください。

10. [Instance Size] ドロップダウンリストをクリックして、必要なサイズを選択します。キャパシティのニーズに基づいて、WAN エッジのサイズを選択します。
11. [IP Subnet Pool] を入力します。サブネットプールはトランジット VPC の作成に使用され、/16 ～ /24 の範囲内にある必要があります。システムにより、トランジット VPC の 8 サブネットごとに /27 が割り当てられます。
12. （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）

    クラウドゲートウェイを作成したとき、または AWS のグローバル設定を構成したときに [Enable Configuration Group] オプションを有効にした場合は、[Configuration Group] ドロップダウンリストから次のいずれかのアクションを実行します。

    - 構成グループを選択します。
    - 新しい設定グループを作成して使用するには、[Create New] を選択します。[Create Configuration Group] ダイアログボックスで、新しい設定グループの名前を入力し、[Done] をクリックします。ドロップダウンリストから新しい設定グループを選択します。選択した設定グループは、マルチクラウドワークフローでデバイスを設定するために使用されます。

（注） ここで設定グループを有効にすると、すべてのクラウドプロバイダーに対して設定グループが有効になります。たとえば、ここでこのオプションを有効にすると、他のすべてのマルチクラウドおよびインターコネクト プロバイダーの設定グループも有効になります。

1. [Chassis number] を選択して、シャーシのペアを設定グループに関連付けます。
2. [Configure Device Parameters] をクリックし、以下を入力します。
    1. **システム IP**
    2. **ホスト名（Hostname）**

3. TLOC Color
4. **Username**
5. **[User Password]**

3. [Create Gateway] をクリックします。

13. このオプションは、デバイステンプレートを使用した設定にのみ適用されます。

    [UUID (specify 2)] ドロップダウンリストで UUID の詳細を選択します。

（注）
- テンプレートがアタッチされた論理デバイス（UUID）のみがリストに表示されます。
- Cisco vManage リリース 20.10.1 以降では、[Site Name] ドロップダウンリストからサイトを選択すると、UUID が自動的に入力されます。

14. （最小リリース：Cisco vManage リリース 20.10.1）[Multi-Region Fabric Settings] エリアの [MRF Role] で、[Border] または [Edge] を選択します。

    このオプションは、マルチリージョンファブリックが有効になっている場合にのみ使用できます。

15. [Add] をクリックして、新しいクラウドゲートウェイを作成します。

（注）
AWS Cloud WAN のクラウドゲートウェイの作成には、展開されているリソースに応じて 1 時間以上かかる場合があります。AWS がこのリージョンのリソースを確認および検証している場合は、リージョンでの最初の展開が失敗する可能性があります。

AWS Cloud WAN をサポートしていないリージョンでは、クラウドゲートウェイを作成できません。現在サポートされているリージョンについては、AWS のドキュメントを参照してください。

サイトアタッチメントの設定

次の手順を実行して、クラウドゲートウェイにサイトをアタッチします。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。[Manage] の下の [Gateway Management] をクリックします。[Cloud Gateways] ウィンドウが表示されます。テーブルには、クラウドアカウント名、ID、クラウドタイプ、トランジットゲートウェイとともにクラウドゲートウェイのリストが表示されます。

   クラウドゲートウェイごとに、サイトを表示、削除、またはさらに接続できます。

2. 目的のクラウドゲートウェイについて、[…] をクリックし、[Cloud Gateway] を選択します。

3. [Attachment] をクリックします。
4. [Attach Sites] をクリックします。
5. [Circuit Color] ドロップダウンリストで、回線の色を選択します。回線の色により、クラウドゲートウェイに接続するサイトの検索条件が定義されます。
6. [Next] をクリックします。[Attach Sites - Select Sites] ウィンドウが表示されます。テーブルには、選択した回線の色を持つサイトが表示されます。
7. [Available Sites] からサイトを 1 つ以上選択し、それらを [Selected Sites] に移します。
8. [Next] をクリックします。
9. [Attach Sites - Site Configuration] ウィンドウで、[Tunnel Count] を入力します。トンネル数の範囲は 1 ～ 8 です。各トンネルは 2.5 Gbps の帯域幅を提供します。
10. [Accelerated VPN] オプションで、[Enabled] または [Disabled] を選択します。AWS Global Accelerator は、クラウドへの接続を最適化するのに役立ちます。
11. [Next] をクリックします。[Attach Sites - Configuration Override] ウィンドウが表示されます。必要に応じて、前の手順で実行した設定を上書きすることができます。トンネル数と高速 VPN ステータスの値を変更できます。
12. [Next] をクリックします。[Next Steps] ウィンドウが表示され、追加したアタッチメントを保存してフローを終了することができます。
13. [Save and Exit] をクリックします。設定が成功すると、ブランチエンドポイントが正常にアタッチされたことを示すメッセージが表示されます。

（注） トンネルのステータスを表示するには、[Cloud OnRamp for Multicloud] ダッシュボードまたは [Site Details] ウィンドウに移動します。

サイトのデタッチ

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。[Manage] の下の [Gateway Management] をクリックします。[Cloud Gateways] ウィンドウが表示されます。テーブルには、クラウドアカウント名、ID、クラウドタイプ、トランジットゲートウェイとともにクラウドゲートウェイのリストが表示されます。
2. 目的のクラウドゲートウェイについて、[…] をクリックし、[Cloud Gateway] を選択します。次に、[Attachment] をクリックします。[Attachments - Cloud Gateway Name] ウィンドウが表示されます。このウィンドウに、クラウドゲートウェイにアタッチされているサイトのリストが表示されます。
3. [Detach Sites] をクリックします。[Are you sure you want to detach sites from cloud gateway?] というメッセージがウィンドウに表示されます。

4. [OK] をクリックします。クラウドゲートウェイに接続されているサイトは切り離されます。サイトのマッピング解除が行われ、VPN 設定がデバイスから削除されます。

クラウドゲートウェイの削除

[Cloud Gateways] ウィンドウの目的のクラウドゲートウェイで、[...] をクリックし、[Delete] を選択します。クラウドゲートウェイの削除を試みる前に、クラウドゲートウェイからすべてのサイトをデタッチする必要があります。

Cisco SD-WAN Manager の各クラウドゲートウェイのクラウドリソース インベントリでクラウドリソースを表示できます。

インテント管理 - 接続

Cisco SD-WAN Manager のマッピングワークフローにより、Cisco Catalyst SD-WAN VPN（セグメント）と VPC 間の接続、および VPC から VPC への接続が可能になります。VPC はタグに基づいて表されます。

（注） 進行中のマッピングタスクでは新しいインテントのマッピングが無効になっています。イントラタグが有効になっていて、同じリージョン内の VPC が同じタグに追加されている場合、マッピングはタグ付けの一部として行われます。

システムが接続のインテントを記録すると、クラウドゲートウェイが存在するリージョンのクラウドでマッピングが実現されます。クラウドゲートウェイが異なるリージョンに存在しなくても、マッピングインテントを入力できます。ユーザー マッピング インテントは保持され、新しいクラウドゲートウェイまたはマッピングの変更が検出されたときに実現されます。クラウドゲートウェイが異なるリージョンでインスタンス化されると、マッピングインテントがそれらのリージョンで実現されます。同様に、タグ付け操作はさまざまなリージョンのマッピングにも影響を与える可能性があり、タグごとのマッピングはクラウドで実現されます。

Cloud OnRamp for Multicloud ダッシュボードで、[Management] の下の [Connectivity] をクリックします。[Intent Management - Connectivity] ウィンドウが表示されます。ウィンドウには、接続ステータスと次の凡例が表示されます。

- 空白：編集可能
- グレー：システム定義済み
- 青：インテント定義済み
- 緑：インテント実現済み
- 赤：インテント実現済み（エラーあり）

[Connectivity] ウィンドウでは、次のことができます。

- 必要に応じて、接続の変更を表示します。

- フィルタ処理とソート。
- さまざまなリージョンのクラウドゲートウェイに依存しない接続を定義します。
- クラウドゲートウェイが存在するすべてのリージョンで接続を実現します。

クラウドゲートウェイが同じリージョンに存在する場合、またはタグ付け操作が行われる場合、マッピングは自動的に実現されます。

接続情報またはインテントは、VPN、送信元としてのタグ、宛先としてのタグを使用してマトリックス形式で入力されます。各セルをクリックすると、マッピング済み、マッピング解除、および未処理のマッピングに関する詳細情報が表示されます。

（タグの一部として）マッピングに関係する VPC には、少なくとも 1 つのサブネットが必要です。CIDR が重複している VPC は、マッピングに失敗します。

Cisco IOS XE Catalyst SD-WAN リリース 17.3.2 以降では、マッピングはリージョンに依存せず、特定のリージョンに限定されずに複数のリージョンにまたがることができます。複数のマッピングリクエストではなく、複数のリージョンに関係する単一のマッピングリクエストが、クラウドエージェントにディスパッチされます。リージョン全体のすべての VPC、VPN、および接続要素の情報が、同じマッピングリクエストにまとめられます。マッピングステータスが拡張され、すべてのリージョンのネットワーク全体の接続情報と現在のアタッチメント仕様を取得できるようになりました。

マッピングに応じて、複数のリージョンを同時にロックできます。リージョン間マッピングは、ローカルからリージョンへのマッピングを、必要に応じてリージョン間のマッピングに変更します。マッピングが複数のリージョン間で行われる場合、リージョンはロックされます。監査は本質的にグローバルであるため、監査がオンになっている間はすべてのリージョンがロックされます。

（注） AWS クラウドの動作では、インテント管理のマッピングが完了するまでに最大 40 ～ 60 分かかることがあります。

（注） 複数の WAN インターフェイスを使用しているときに、ブランチのサービスと AWS Transit Gateway の間にトンネルが作成されるように、IP の外部にあるトランジット ゲートウェイ エンドポイントに特定のルートを追加する必要があります。ブランチ接続マッピングでは、トランジット ゲートウェイ エンドポイントへの必要な IPsec トンネル設定のみが構成されます。

（注） コアネットワークごとにサポートされるピアリングの最大数は 50 です。VPN 接続の数がこの制限を超えると、マッピングは失敗します。

（注） マッピング中に、マルチクラウドワークフローはVPCメインルートテーブルにデフォルトルートを追加します。ただし、メインルートテーブルにすでにデフォルトルートがある場合は追加されません。マッピングが適用される前に、VPC メインルートテーブルに既存のデフォルトルートが存在しないようにする必要があります。

脆弱な暗号による IPsec トンネルのダウン

マルチクラウド AWS VPN 接続またはブランチ接続がある Cisco SD-WAN Manager を Cisco vManage リリース 20.11.1 にアップグレードし、Cisco Catalyst 8000V Edge ソフトウェアを以前の 17.x リリースから Cisco IOS XE Catalyst SD-WAN リリース 17.11.x にアップグレードすると、Cisco Catalyst SD-WAN デバイスの TGW（トランジットゲートウェイ）とクラウドゲートウェイ内の Cisco Catalyst SD-WAN デバイス間の IPsec トンネルがダウンします。

トンネルを起動するには、次のいずれかを実行します。

- 古い暗号設定を引き続き使用する場合は、クラウドゲートウェイの Cisco Catalyst SD-WAN デバイスで **crypto engine compliance shield disable** コマンドを使用し、デバイスをリロードしてトンネルを起動します。トンネルは、脆弱な暗号を使用して起動します。クラウド接続に不整合が発生すると、監査がトリガーされます。監査がトリガーされると、グループ 2 のすべてのトンネルがグループ 15 の暗号に変更され、トンネルはダウンしたままになります。監査後にこの問題を解決するには、Cisco SD-WAN Manager の [Intent Management Cloud Connectivity] ページを使用して、接続のマッピングを解除してからマッピングします。
- マルチクラウド AWS VPN 接続またはブランチ接続がある Cisco SD-WAN Manager を Cisco vManage リリース 20.11.1 にアップグレードし、Cisco Catalyst 8000V Edge ソフトウェアを以前の 17.x リリースから 17.11 にアップグレードした場合、CLI コマンドを使用する代わりに Cisco SD-WAN Manager の [Intent Management Cloud Connectivity] ページを使用して、接続のマッピングを直接解除してからマッピングすることができます。トンネルは、グループ 15 暗号を使用して起動します。

（注） SDCI の AWS CGWExtn をアップグレードするときは、上記の手順を使用して、より強力な暗号を使用してトンネルを起動します。ソフトウェア定義型のクラウドインターコネクト（SDCI）には、SDCI から展開される AWS CGWExtn というソリューションがあります。Cisco SD-WAN Manager で SDCI を使用するクラウドゲートウェイを作成した場合、AWS が展開されるとトンネルがダウンします。Cisco SD-WAN Manager の [Intent Management Cloud Connectivity] ページからゲートウェイにアクセスできます。

トランジット ゲートウェイ ピアリング

表 *57 :* 機能の履歴

機能名	リリース情報	説明
トランジット ゲートウェイ ピアリング	Cisco IOS XE リリース 17.3.2 Cisco vManage リリース 20.3.2	この機能により、異なる AWS リージョンのトランジットゲートウェイ間でピア接続を確立できます。この機能により、単一のゲートウェイを使用してさまざまなトランジット仮想プライベートクラウド（TVPC）とオンプレミスネットワークに接続することができます。異なる AWS リージョン間でトランジットゲートウェイをピアリングする機能により、接続を拡張し、他の複数のリージョンにまたがるグローバルネットワークを構築することができます。リージョン間接続をサポートするために、マッピングおよび監査機能が拡張されています。

マルチクラウド ネットワーキングのリージョン間接続により、多数のリージョンにまたがる VPC 間の通信が可能になります。次の接続オプションがサポートされています。

- 複数のリージョンにまたがる単一のタグを使用した VPC 内のタグ内通信。
- 多数のリージョンにまたがる VPC 内での VPC によるタグ間接続。

VPC および VPN アタッチメントは、トランジットゲートウェイ内のさまざまなルーティングテーブルに関連付けられ、伝達されます。目的の接続に応じて、トランジット ゲートウェイ ルートテーブル内に、それぞれのトランジットゲートウェイのピアリングされたアタッチメントを指す他のリージョンの VPC および TVPC Classless Inter-Domain Routing（CIDR）へのルートがあります。これにより、ある TVPC リージョン内の VPC およびクラウドサービスルータは、他のリージョン内の他の TVPC 内の VPC およびクラウドサービスルータと通信できます。TVPC はメッシュで接続されますが、ホスト VPC の接続は定義された接続またはインテントマトリックスに従います。

VPN とタグ間の接続は、そのリージョン内の VPN と VPC 間の接続（タグ内の VPC）に制限されます。VPN 接続は、トランジットゲートウェイのピアリングされたアタッチメントを通過しません。

監査機能はグローバルレベルで設定され、破損したトランジットゲートウェイのピアリングされたアタッチメントを復元するように拡張され、CSR 間の接続が確保されます。監査の詳細については、「監査管理」を参照してください。

監査管理

Cloud OnRamp for Multicloud ダッシュボードでは、監査画面でクラウドの状態を Cisco SD-WAN Manager の状態と同期させることができます。タグ付けの不一致またはホスト VPC の欠落が原因でマッピングが失敗した場合、監査は、回復可能なエラーとタグ付けの不一致の問題についてマッピングを修正するのに役立ちます。

[Cloud OnRamp for Multicloud] ウィンドウで、目的のクラウドタイプに対して、[...] をクリックして [Audit] を選択します。目的のクラウドタイプの監査レポートが表示されます。

監査は、Cisco SD-WAN Manager インテントとクラウドで実現された内容の間の乖離または不一致を特定するのに役立ちます。この乖離は、クラウドリソース、そのマッピング、接続、および状態に関して発生します。このような乖離が検出されると、Cisco SD-WAN Manager はそのような乖離にフラグを立て、回復アクションを実行して、クラウドの状態を設定済みインテントと同期させます。たとえば、あるタグでタグ付けされたアカウントまたはリージョンのすべてのホスト VPC を特定のトランジットゲートウェイにマッピングするインテントがあり、同じタグでタグ付けされた新しいホスト VPC がトランジットゲートウェイと切断されていることがわかった場合、Cisco SD-WAN Manager は新しいホスト VPC をトランジットゲートウェイに接続します。

エラーのタイプ：

- 回復可能なエラー
  - クラウドにホスト VPC がない
  - タグ付けの不一致
  - マッピングの異常：アタッチメント関連の問題、トランジット ゲートウェイ ルートテーブル関連の問題
- 回復不能なエラー（ユーザーの介入が必要）
  - クラウド内のクラウドゲートウェイまたはそのコンポーネント（トランジットゲートウェイ、TVPC、およびクラウドルータ）の削除
  - CIDR が重複している VPC

監査のタイプ：

- オンデマンド
  - ユーザーによって呼び出されます。
  - レポートが同期していない場合は、修正オプション付きの監査を開始して問題を修正できます。
- 定期的：システムによって自動的に、2 時間ごとに定期的に呼び出されます。最初の定期監査は、システムの起動から 15 分後に開始されます。

監査機能はグローバルレベルで設定され、破損したトランジットゲートウェイのピアリングされたアタッチメントを復元するように拡張され、CSR 間の接続が確保されます。

（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 17.12.1a および Cisco Catalyst SD-WAN Manager リリース 20.12.1）AWS Cloud WAN の場合、Cisco SD-WAN Manager のポリシードキュメントと、各クラウドゲートウェイのクラウド リソース インベントリの使用可能なコアネットワークポリシーを表示および比較できます。これらのポリシードキュメントの不一致を特定し、それに応じてトラブルシューティングを行うことができます。

AWS 統合の詳細については、以下を参照してください。

- Amazon Virtual Private Cloud Getting Started Guide
- Amazon Virtual Private Cloud Network Administrator Guide
- Transit gateway VPN Attachment

Cisco SD-WAN Manager を使用した AWS 統合のモニター

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 17.13.1a、Cisco Catalyst SD-WAN Manager リリース 20.13.1

マルチクラウドの展開

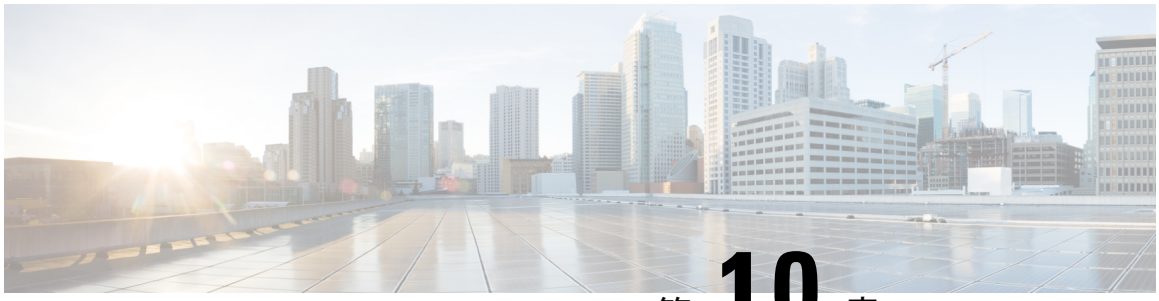
Cisco SD-WAN Manager の **[Monitor]** > **[Multicloud]** から、マルチクラウドの展開に関する次の情報を表示できます。

- クラウドタイプごとに次の情報。
  - クラウドゲートウェイの数と、各ゲートウェイの正常性。
  - WAN エッジデバイスの数と、その正常性。
  - クラウドゲートウェイに接続されているサイトの数。
  - クラウドゲートウェイを通過する VPN 接続トンネルの数。
  - 接続されたタグの数。
  - マッピングされたホスト VPC または vNET の数。
  - VPN 接続の数。
- AWS Cloud WAN ソリューションの場合、AWS クラウドの運用可能な AWS Cloud WAN コアネットワークポリシーを表示できます。

マルチクラウド ダッシュボード

Cisco SD-WAN Manager の **[Configuration]** > **[Cloud OnRamp for Multicloud]** からマルチクラウド ダッシュボードを表示できます。マルチクラウド ダッシュボードでは、ネットワーク全体のスナップショットが要約され、各クラウドゲートウェイに関する情報を表示できます。

ダッシュボードの [Additional Details] セクションで、AWS Cloud WAN を介したサイト間通信の各 WAN エッジデバイスからの BGP セッションの状態を表示できます。



第 10 章

Amazon GovCloud（米国）の統合

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。

表 *58 :* 機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud での AWS GovCloud（米国）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	Amazon Web Services（AWS）GovCloud（US）と Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud を統合することで、米国政府とその取引先の Federal Risk and Authorization Management Program（FedRAMP）の要件を満たす分離されたクラウドに、非常に機密性の高いワークロードを保存することができます。 Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud との AWS 統合で使用できる機能と同じ機能が、Amazon GovCloud（米国）でも使用できます。AWS Transit Gateway を使用して、ブランチデバイスを AWS GovCloud（米国）に接続します。

- AWS GovCloud（米国）統合に関する情報 （290 ページ）
- AWS GovCloud（米国）でサポートされるデバイス （292 ページ）
- AWS GovCloud（米国）統合の前提条件 （292 ページ）
- AWS GovCloud（米国）統合の制約事項 （293 ページ）
- AWS GovCloud（米国）統合のユースケース （293 ページ）
- AWS GovCloud（米国）の設定 （293 ページ）

AWS GovCloud（米国）統合に関する情報

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 17.9.1a、Cisco vManage リリース 20.9.1

Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud は、AWS GovCloud（米国）のサポートを拡張し、非常に機密性の高いワークロードを AWS GovCloud（米国）で保存および管理できるようにします。

次に、AWS GovCloud（米国）に保存できる非常に機密性の高いワークロードの例を示します。

- コントローラの未分類情報（CUI）

- 個人識別情報（PII）
- 機密性の高い患者の医療記録
- 財務データ
- 法執行データ
- データのエクスポート

Transit Gateway Network Manager（TGNM）のサポートを除き、AWS 統合で使用できるのと同じ機能とワークフローを AWS GovCloud（米国）統合でも使用できます。

（注） TGNM は AWS でサポートされていますが、TGNM は AWS GovCloud（米国）ではサポートされていません。

トランジットゲートウェイは、仮想プライベートクラウド（VPC）とオンプレミスネットワークを相互接続するために使用できるネットワーク トランジット ハブです。VPC または VPN 接続をトランジットゲートウェイに接続できます。トランジットゲートウェイは、VPC および VPN 接続の間を流れるトラフィックの仮想ルータとして機能します。トランジットゲートウェイは、VPC と VPN を相互接続する方法を提供します。

Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud は、AWS Transit Gateway を使用して、ブランチデバイスを AWS GovCloud（米国）に接続します。Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud の構成ウィザードは、AWS GovCloud（米国）アカウントへのトランジットゲートウェイの起動を自動化し、オーバーレイネットワーク内で、AWS GovCloud（米国）アプリケーションとブランチのユーザーとの間の接続を自動化します。

AWS GovCloud の詳細については、AWS GovCloud（米国）のドキュメントを参照してください。

Cisco SD-WAN Manager を使用して AWS GovCloud（米国）での Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud を設定します。

AWS GovCloud（米国）統合の利点

- 米国政府とその取引先の FedRAMP 要件を満たす、AWS GovCloud（米国）の機密データワークロードを移動および保存できます
- AWS 統合と同じ機能とワークフローをサポートしています
- データセンターからクラウドへのセキュアな Cisco Catalyst SD-WAN トンネルを使用した高度なルーティング機能とパス選択をサポートしています
- データセンターと AWS GovCloud（米国）間のテレメトリデータの交換をサポートしています

AWS GovCloud（米国）でサポートされるデバイス

サポートされるプラットフォーム

AWS GovCloud（米国）でサポートされるプラットフォームの詳細については、「Overview of AWS Integration」を参照してください。

AWS GovCloud（米国）でサポートされるインスタンス

- c5.large
- c5.xlarge
- c5.2xlarge
- c5.9xlarge
- c5n.large
- c5n.xlarge
- c5n.2xlarge
- c5n.4xlarge
- c5n.9xlarge
- c5n.18xlarge
- t3.medium

（注） AWS と AWS GovCloud（米国）のインスタンスサイズは同じです。

AWS GovCloud（米国）統合の前提条件

- AWS GovCloud（米国）クラウドアカウントが必要です。

（注） AWS GovCloud（米国）アカウントは、AWS アカウントとは異なります。

- AWS GovCloud（米国）マーケットプレイスのサブスクリプションが必要です。
- 新しいアカウントを作成するために自由に使用できる 2 つの Cisco SD-WAN Manager クラウドルータライセンスが必要です。

AWS GovCloud（米国）統合の制約事項

- AWS GovCloud（米国）の TGNM はサポートされていません。

AWS GovCloud（米国）統合のユースケース

Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud と AWS GovCloud（米国）を使用すると、米国政府とその取引先の FedRAMP 要件を満たす分離されたクラウドにコンプライアンス ワークロードを移動および保存できます。

次に、AWS GovCloud（米国）に保存できる機密データの例を示します。

- コントローラの未分類情報（CUI）
- 個人識別情報（PII）
- 機密性の高い患者の医療記録
- 財務データ
- 法執行データ
- データのエクスポート

AWS GovCloud（米国）の設定

AWS GovCloud（米国）を設定するためのワークフローは、AWS を使用した Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud を設定するためのワークフローと同じです。

1. AWS GovCloud（米国）クラウドアカウントを作成します。

   AWS GovCloud（米国）アカウントの作成の詳細については、「Create AWS Cloud Account」を参照してください。

2. クラウド トランジット ゲートウェイのグローバル設定を構成します。

   クラウドトランジットゲートウェイのグローバル設定の構成の詳細については、「Configure Cloud Global Settings」を参照してください。

3. AWS GovCloud（米国）リージョン全体のすべてのアカウントのホスト仮想プライベートクラウド（VPC）を検出します。

   AWS のホスト VPN の検出の詳細については、「Discover Host Private Networks」を参照してください。

4. クラウドゲートウェイを作成します。

クラウドゲートウェイの作成の詳細については、「Create Cloud Gateway」を参照してください。

5. クラウドゲートウェイにサイトをアタッチします。

   クラウドゲートウェイへのサイトのアタッチの詳細については、「Configure Site Attachment」を参照してください。

6. Cisco Catalyst SD-WAN VPN と VPC 間の接続を有効にします。

   Cisco Catalyst SD-WAN VPN と VPC 間の接続の有効化の詳細については、「Intent Management - Connectivity」を参照してください。

7. 異なる AWS GovCloud（米国）リージョンのトランジットゲートウェイ間のピア接続を有効にします。

   異なる AWS GovCloud（米国）リージョン内のトランジットゲートウェイ間のピア接続の有効化の詳細については、「Transit Gateway Peering」を参照してください。

8. 監査を実施し、Cisco SD-WAN Manager インテントとクラウドで実現された内容の間の乖離または不一致を特定します。

   監査管理レビューの実施の詳細については、「Audit Management」を参照してください。

第 11 章

Microsoft Azure Virtual WAN の統合

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。

表 *59* : 機能の履歴

機能名	リリース情報	説明
Azure Virtual WAN と Cisco Catalyst SD-WAN の自動統合	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	この機能は、Cisco Catalyst 8000V Edge ソフトウェア（Cisco Catalyst 8000V）をトランジット VNet 内に展開するのではなく、Azure Virtual WAN ハブ内に展開できるようにすることで、Cloud OnRamp と Microsoft Azure の統合を強化します。また、Cisco Catalyst 8000V を介した Azure Virtual WAN ハブへの Cisco Catalyst SD-WAN ファブリック接続を自動化します。リージョン間の Azure Virtual WAN ハブ間の接続もサポートされます。 さらに、Cisco SD-WAN Manager を使用して作成された Azure Virtual WAN ハブを、内部に Azure ファイアウォールを展開することで、セキュリティ保護付きハブに変換することができます。ただし、セキュリティ保護付き仮想ハブは、Microsoft Azure ポータルを使用してのみ設定できます。

機能名	リリース情報	説明
Azure ポータルを使用した Cisco Catalyst SD-WAN と Azure Virtual WAN ハブの統合	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	Cisco Catalyst SD-WAN と Azure Virtual WAN の統合の一環として、Azure ポータルを使用して、Cisco Catalyst 8000V インスタンスのブートストラップ構成ファイルをアップロードすることもできます。これらのインスタンスは、その後、Azure ポータルを使用して仮想 WAN ハブを作成する際に使用できます。
仮想ハブファイアウォールまたはローカルファイアウォールへのトラフィックフローのルーティング	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能により、Microsoft Azure Virtual WAN ハブのトラフィックをローカルブランチルータのファイアウォールにルーティングしたり、ローカルブランチのトラフィックを Azure のセキュリティ保護付き仮想ハブに転送したりして、Azure Firewall Manager のセキュリティポリシーの対象にすることができます。
ネットワーク仮想アプライアンスの Azure スケーリング、監査、およびセキュリティ	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能により、SKU スケール値を編集し、ネットワーク仮想アプライアンス（NVA）のセキュリティを強化することができます。監査サービスは、Cisco SD-WAN Manager と Azure クラウドデータベースからの情報を比較し、不一致を特定します。
定期的な監査、Azure のスケーリングと監査の強化、および ExpressRoute 接続。	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1	Cisco SD-WAN Manager は、2 時間ごとのオプションの定期監査を提供しています。この自動監査はバックグラウンドで実行され、不一致のレポートが生成されます。自動修正オプションを有効にすると、Cisco SD-WAN Manager は定期監査中に検出された回復可能な問題を自動的に解決します。 オンデマンド監査の開始後に生成された個々の不一致を修正できます。 Cisco SD-WAN Manager は、Cisco Catalyst SD-WAN トンネルを介したブランチオフィスから NVA への ExpressRoute 接続をサポートしています。ExpressRoute 接続は、データ転送のための、信頼性が高く、遅延が少なく、接続が高速なプライベートネットワークです。

機能名	リリース情報	説明
各リージョンの複数の仮想ハブのサポート	Cisco vManage リリース 20.11.1 Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a	1 つの Azure リージョンに複数の仮想ハブを作成できます。
Azure インスタンスタイプの追加	Cisco Catalyst SD-WAN Manager リリース 20.12.1 Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a	Azure の米国中西部およびオーストラリア東部リージョン用に、Standard_D16_v5 Azure インスタンスタイプが追加されました。これには、16 個の CPU コアと 64 GB のメモリが含まれています。このタイプのインスタンスは、20、40、60、および 80 の SKU スケール値で展開できます。

- Azure Virtual WAN 統合に関する情報 （297 ページ）
- Azure Virtual WAN 統合でサポートされるデバイス （307 ページ）
- Azure Virtual WAN 統合の前提条件 （309 ページ）
- Azure Virtual WAN 統合の制約事項 （310 ページ）
- Azure Virtual WAN 統合のユースケース （311 ページ）
- Azure Virtual WAN 統合の設定 （312 ページ）
- Azure Virtual WAN 統合の確認 （329 ページ）
- Cisco SD-WAN Manager を使用した Azure Virtual WAN 統合のモニター （331 ページ）

Azure Virtual WAN 統合に関する情報

Azure Virtual WAN ハブと Cisco Catalyst SD-WAN の統合

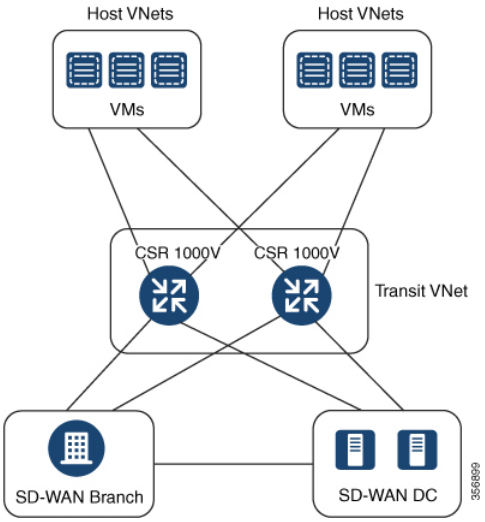
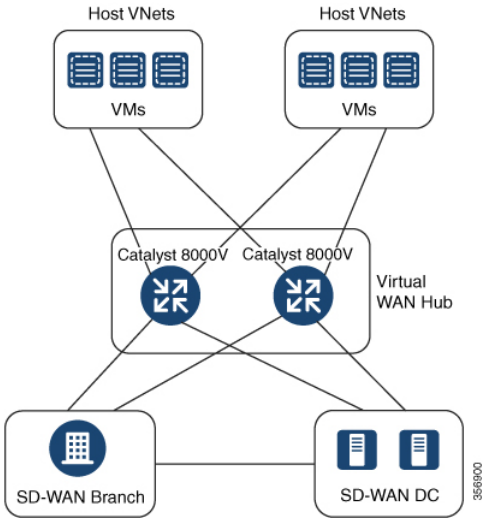
サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a、Cisco vManage リリース 20.4.1

Cisco Catalyst SD-WAN ソリューションと Azure Virtual WAN の統合により、Cloud OnRamp for Multicloud 展開が強化され、Cisco Catalyst 8000V Edge ソフトウェア（Cisco Catalyst 8000V）を Azure Virtual WAN ハブのネットワーク仮想アプライアンス（NVA）として設定できます。

この統合により、トランジット仮想ネットワーク（VNet）を作成する必要がなくなり、Azure 仮想 WAN ハブを介してホスト VNet 接続を直接制御できるため、クラウドサービスの消費モデルが簡素化されます。Azure Virtual WAN は、Microsoft Azure を介して最適化および自動化されたブランチ間の接続を提供するネットワーキングサービスです。Azure と通信できるブランチデバイスを接続して設定できます。Azure 仮想ハブ内に Cisco Catalyst 8000V インスタンスを設定すると、より高速で広い帯域幅が提供され、トランジット VNet を使用する場合の速度と帯域幅の制限が克服されます。

Cloud OnRamp for IaaS と Cloud OnRamp for Multicloud の比較

この表では、Microsoft Azure 統合のコンテキストでの Cloud OnRamp for IaaS と Cloud OnRamp for Multicloud の違いを示しています。

Azure 用の Cloud OnRamp for IaaS	Azure 用の Cloud OnRamp for Multicloud
	
Cisco SD-WAN Manager での Cloud OnRamp for IaaS ワークフローを介したトランジット VNet の自動プロビジョニングを可能にします	Cisco SD-WAN Manager での Cloud OnRamp for Multicloud ワークフローを介した Azure 仮想ハブの自動プロビジョニングを可能にします
Cisco SD-WAN Manager がトランジット VNet 内の 2 つの Cisco Cloud Services Router 1000V シリーズ（Cisco CSR1000V）デバイスを自動的にプロビジョニングします	Cisco SD-WAN Manager が Azure 仮想ハブ内の 2 つの Cisco Catalyst 8000V インスタンスを自動的にプロビジョニングします

Azure を使用した Cloud OnRamp for IaaS に関する情報と、トランジット VNet の設定方法については、「Configure Cloud OnRamp for IaaS for Azure」を参照してください。

仮想 WAN ハブ統合の仕組み

オーバーレイネットワークとパブリック クラウド アプリケーション間の接続は、Azure 用の Cloud OnRamp for Multicloud ワークフローの一環として Azure Virtual WAN ハブ内で設定された冗長 Cisco Catalyst 8000V インスタンスのペアによって提供されます。冗長ルータを使用してトランジットを形成すると、パブリッククラウドに対するパスの復元力が得られます。

Cisco SD-WAN Manager の Cloud OnRamp for Multicloud フローは、地理的なクラウドリージョン内の既存の VNet を検出し、選択した VNet をオーバーレイネットワークに接続できるようにします。このようなシナリオでは、Cloud OnRamp for Multicloud を使用すると、レガシーパブリッククラウド接続と Cisco Catalyst SD-WAN オーバーレイネットワークを簡単に統合できます。

Cisco SD-WAN Manager の構成ウィザードは、パブリック クラウド アカウントに接続するための Azure Virtual WAN ハブの起動を自動化します。また、このウィザードは、パブリック クラウドアプリケーションと、オーバーレイ ネットワーク内のブランチにいるそれらのアプリケーションのユーザーとの間の接続を自動化します。Cisco SD-WAN Manager では、タグを使用して、ブランチ内のサービス VPN をパブリック クラウドインフラストラクチャ内の特定の VNet にマッピングできます。

VNet から VPN へのマッピング

Cisco SD-WAN Manager のインテント管理ワークフローは、Cisco SD-WAN VPN（ブランチネットワーク）と VNet 間の接続、および VNet から VNet への接続を可能にします。VNet は、Cloud OnRamp for Multicloud の Discover ワークフローで作成されたタグで表されます。VNet が仮想 WAN ハブに接続するようにマッピングされると、デフォルトルートが割り当てられ、デフォルトラベルに伝達されます。Azure リージョン内で VNet タグを作成すると、同じタグを共有する他の VNet および VPN に基づいてマッピングが自動的に作成されます。

Cisco SD-WAN Manager が接続のインテントを記録すると、クラウドゲートウェイが存在するリージョンのクラウドでマッピングが実現されます。クラウドゲートウェイが異なるリージョンに存在しなくても、マッピングインテントを入力できます。マッピングインテントは、新しいクラウドゲートウェイまたはマッピングの変更が検出されたときに保持され、実現されます。クラウドゲートウェイが異なるリージョンでインスタンス化または検出されると、マッピングインテントがそれらのリージョンで実現されます。同様に、タグ付け操作はさまざまなリージョンのマッピングにも影響を与える可能性があり、タグごとのマッピングはクラウドで実現されます。

（注） VNet タグにマッピングされるように選択した VPN は、重複する IP アドレスを持つことはできません。これは、Microsoft Azure Virtual WAN ではセグメンテーションがサポートされていないためです。

リージョン間の Azure ハブ間接続は、VNet タグを作成し、それらを VPN サイトにマッピングすることで有効になります。リージョン間のハブ間接続を有効にするために、追加の設定は必要ありません。VNet は、それぞれのリージョンの仮想 WAN ハブに関連付けられます。異なる Azure リージョン内の VNet が同じ VNet タグを共有している場合、そのような VNet 間の接続は自動的に確立され、VNet が接続されているそれぞれの仮想 WAN ハブを介して実行されます。

Azure 仮想 WAN 統合ワークフローのコンポーネント

ブランチとデータセンターをパブリック クラウド インフラストラクチャに接続するためのクラウドゲートウェイは、Cisco Catalyst 8000V インスタンスをホストする論理オブジェクトです。Azure リソースグループ、Azure Virtual WAN、および Azure Virtual WAN ハブで構成されます。

リソース グループ

すべての Azure ネットワーキングリソースはリソースグループに属し、リソースグループは Azure サブスクリプションの下に作成されます。Azure クラウドゲートウェイの場合、Azure 仮想 WAN と Azure 仮想 WAN ハブはリソースグループの下に作成されます。

したがって、Azure クラウドゲートウェイを作成する最初の手順は、リソースグループを作成することです。

リソースグループを作成したら、Azure 仮想 WAN を構成できます。

Azure 仮想 WAN

Azure 仮想 WAN は、Azure ネットワーキングサービスのバックボーンです。既存の Azure リソースグループの下に作成されます。Azure 仮想 WAN には、各仮想ハブが異なる Azure リージョンに属している限り、複数の Azure 仮想ハブを含めることができます。Azure リージョンごとに 1 つの仮想ハブのみがサポートされます。

リージョン内のリソースグループで仮想 WAN を定義したら、次のステップは Azure 仮想 WAN ハブの作成です。

Azure 仮想 WAN ハブ

Azure Virtual WAN ハブは、VPN サイトと NVA および VNet 間のコア接続を管理します。仮想ハブが作成されると、Cisco Catalyst 8000V インスタンスを Azure ネットワーキングサービスに統合できます。

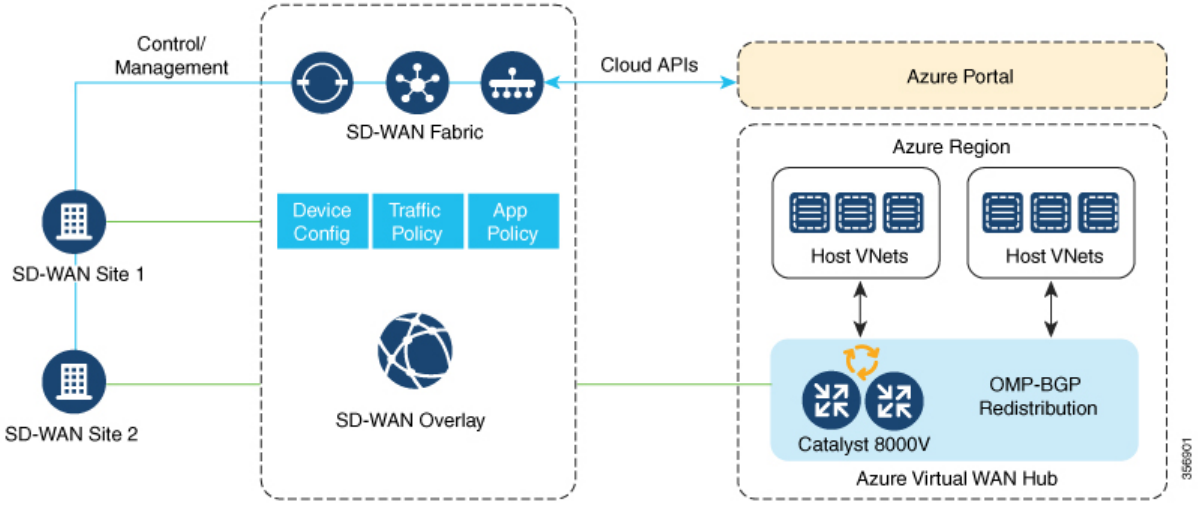
接続モデル

Azure Virtual WAN と Cisco Catalyst SD-WAN ソリューションの統合では、次の接続モデルがサポートされています。

- Cisco Catalyst SD-WAN ブランチから同じ Azure リージョン内の Azure ホスト VNet へ
- リージョン間の Azure 仮想ハブから仮想ハブへの接続

Cisco Catalyst SD-WAN ブランチから Azure ホスト VNet へ（単一リージョン）

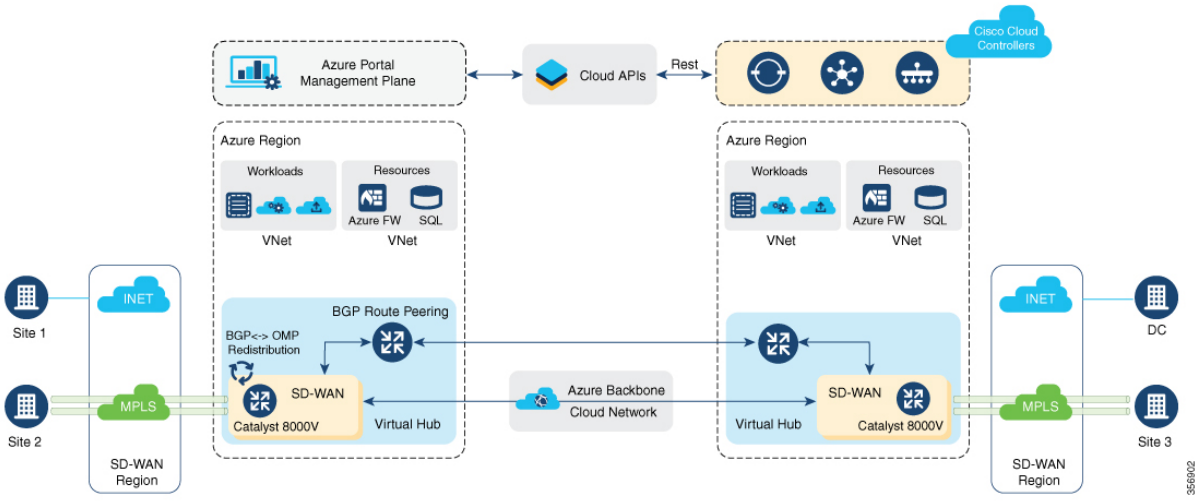
図 *21* : 同じ *Azure* リージョン内の *VNet* から *VNet* へのマッピング



このシナリオでは、仮想ハブはスタンドアロンであり、他の Azure リージョンの仮想ハブには接続されていません。このような場合、VNet は仮想ハブと同じリージョンに属し、Cisco SD-WAN Manager で定義されている VNet タグを使用してブランチ VPN に接続されます。

仮想 WAN ハブから仮想 WAN ハブへ（リージョン間）

図 *22* : 仮想ハブを介したリージョン間の *VNet-VNet* マッピング



この画像は、Azure バックボーンでのハブ間接続を表しています。この接続を個別に設定する必要はありません。異なる Azure リージョンの VNet が同じ VNet タグを共有している場合、この接続は自動的に実現されます。

セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックフローのルーティング

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 17.6.1a、Cisco vManage リリース 20.6.1

Microsoft Azure 環境には、Azure Virtual Network（VNet）ワークロードとローカルブランチデバイス間の接続を可能にする仮想ハブが含まれています。Cisco Catalyst SD-WAN と Azure 環境の統合により、次のファイアウォールオプションが有効になります。

- Azure Virtual WAN ハブの発信インターネットトラフィックを、ローカルブランチルータのファイアウォールにルーティングする
- ローカルブランチルータからの発信インターネットトラフィックを Azure のセキュリティ保護付き仮想ハブにルーティングし、Azure Firewall Manager のセキュリティポリシーを適用する。

（注） Azure のセキュリティ保護付き仮想ハブは、Azure Firewall Manager によって管理されるセキュリティおよびルーティングポリシーを持つ Azure Virtual WAN ハブです。

どちらの場合も、リターントラフィックは発信インターネットトラフィックと同じパスをたどるため、同じファイアウォールポリシーが両方向のトラフィックに適用されます。

Azure Virtual WAN の監査

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 17.7.1a、Cisco vManage リリース 20.7.1

マルチクラウド監査サービスは、Cisco SD-WAN Manager データベースの情報を Azure クラウドデータベースの情報と比較します。この情報には、Azure Virtual WAN、仮想ハブ、ネットワーク仮想アプライアンス、仮想ネットワーク、および VPN から仮想ネットワークへのマッピングが含まれます。その後、Cloud OnRamp for Multicloud は結果を比較して不一致を特定し、エラーの有無にかかわらず Microsoft Azure オブジェクトのリストを表示します。

Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 以降では、監査機能には次の拡張機能が組み込まれています。

- オンデマンド監査を開始すると、Cloud OnRamp for Multicloud の監査サービスが、Cisco SD-WAN Manager データベース内の情報と Azure クラウド内の情報の不一致を特定して一覧表示します。すべての不一致をまとめて修正するか、不一致を選択して個別に修正することができます。個々の不一致の横にあるチェックボックスをオンにすると、問題の簡単な説明が不一致の下に表示されます。

  監査の不一致と解決の詳細については、「Audit Discrepancies and Resolutions」を参照してください。

- 定期監査を有効または無効にできるようになりました。詳細については、「Enable Periodic Audit」を参照してください。

定期監査に関する情報

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 17.8.1a、Cisco vManage リリース 20.8.1

Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 以降では、Cisco SD-WAN Manager は 2 時間間隔のオプションの定期監査を提供しています。この自動監査はバックグラウンドで実行され、不一致のレポートが生成されます。自動修正オプションを有効にすると、Cisco SD-WAN Manager は定期監査中に検出された回復可能な問題を自動的に解決します（存在する場合）。定期監査とその解決の詳細については、「Audit Discrepancies and Resolutions」を参照してください。

（注） Cisco SD-WAN Manager バージョンをアップグレードした場合、定期監査と自動修正のオプションはデフォルトで無効になっています。[Cloud Global Settings] ウィンドウから有効にできます。詳細については、「Add and Manage Global Cloud Settings」を参照してください。

監査の不一致と解決

次の表に、監査の不一致と解決の詳細を示します。

表 *60*：監査の不一致の例

不一致	説明	対処法	
		オンデマンド監査の [Fix Sync Issues] ボタン	**定期監査と自動修正**
タグ内の VNet が使用できない	Cisco SD-WAN Manager データベースでは VNet がタグ付けされているが、Azure ポータルでは使用できない場合。	Cisco SD-WAN Manager データベースから VNet を削除するには、[Fix Sync Issues] をクリックします。	Cisco SD-WAN Manager データベースから VNet を削除します。 注 2 を参照してください。
	Azure ポータルから VNet タグが削除された場合、または Cisco SD-WAN Manager と Azure ポータルの間で VNet タグの不一致がある場合。	Cisco SD-WAN Manager データベースから Azure ポータルに VNet タグを適用するには、[Fix Sync Issues] をクリックします。	Cisco SD-WAN Manager データベースから Azure ポータルに VNet タグを追加します。

不一致	説明	対処法	
		オンデマンド監査の[Fix Sync Issues] ボタン	定期監査と自動修正
ストレージアカウント（NVAの設定の保存）が使用できない	Azure ポータルではストレージアカウントが使用できないが、Cisco SD-WAN Manager データベースでは使用できる場合。	Cisco SD-WAN Manager データベースからストレージアカウントを削除するには、[Fix Sync Issues] をクリックします。	Cisco SD-WAN Manager データベースからストレージアカウントを削除します。 注2を参照してください。
仮想 WAN、vHub、および NVA が使用できない	Azure ポータルで仮想 WAN、vHub、または NVA が使用できない場合。	（注）クラウドゲートウェイを手動で削除しないでください。クラウドゲートウェイを削除すると、クラウドプロバイダー間で不一致が発生し、さらにプロビジョニングする機能に影響を与えたり、他の CoR 操作に影響を与えたりする可能性があります。	注2を参照してください。
Azure ポータルでマッピングが使用できない 注 1 を参照してください。	Cisco SD-WAN Manager データベースにはマッピングがありますが、Azure ポータルにはありません。	マッピングを Azure ポータルに再度追加するには、[Fix Sync Issues] をクリックします。	マッピングを Azure ポータルに再度追加します。

不一致	説明	対処法	
		オンデマンド監査の [Fix Sync Issues] ボタン	定期監査と自動修正
Cisco SD-WAN Manager データベースでマッピングを使用できない （注） この不一致は Cisco vManage リリース 20.8.1 でのみ表示および修正できます 。	Azure ポータルにはマッピングがありますが、Cisco SD-WAN Manager データベースにはありません。	マッピングを Cisco SD-WAN Manager データベースに再度追加するには、Cisco SD-WAN Manager ワークフローを使用して VNet を手動でタグ付けし、マッピングする必要があります。 （注） [Fix Sync Issues] をクリックしても、この問題は解決されません。	マッピングを Cisco SD-WAN Manager データベースに再度追加するには、Cisco SD-WAN Manager ワークフローを使用して VNet を手動でタグ付けし、マッピングする必要があります。 （注） 定期監査では、この問題は解決されません。

（注） **1.**Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 以降では、この不一致を表示して修正することができます。

（注） **2.**Cisco vManage リリース 20.9.x 以降では、自動修正オプションは使用できません。代わりに、次のようにクラウドサービス監査を表示します。Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択して、[Intent Management] ペインで [Audit] をクリックします。クラウドプロバイダーを選択します。Cisco SD-WAN Manager が監査レポートを表示します。

ネットワーク仮想アプライアンスの SKU スケール値

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 17.7.1a、Cisco vManage リリース 20.7.1

Azure で Cisco Catalyst 8000V Edge インスタンスの SKU スケール値を編集できます。Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco vManage リリース 20.7.1 より前のリリースでは、SKU スケール値は編集できません。SKU スケール値を変更する場合は、クラウドゲートウェイを削除してから、新しい SKU スケール値を使用して再作成する必要があります。

より高い SKU スケール値を選択してパフォーマンスを向上させることや、より低い値を選択してコスト効率を高めることができます。

SKU スケール値を更新する方法の詳細については、「Configure SKU Scale Value」を参照してください。

（注） SKU スケール値を編集した後は、3 ー 4 分のネットワークダウンタイムが予想されます。

サポートされる SKU スケールの詳細については、「Supported Azure Instances for Azure Virtual WAN Integration」を参照してください。

ネットワーク仮想アプライアンスのセキュリティルールの設定

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 17.7.1a、Cisco vManage リリース 20.7.1

Microsoft Azure には、ネットワーク仮想アプライアンス（NVA）のセキュリティルールを編集するオプションがあります。Cisco SD-WAN Manager は、NVA のこれらのセキュリティルールの設定をサポートしています。

クラウドゲートウェイの作成中に起動される Cisco Catalyst 8000V NVA は、Cisco Catalyst SD-WAN 関連のポートを除くすべてのインバウンドポートの使用を禁止します。NVA 機能のセキュリティルール設定を使用すると、デバッグ目的などで、必要に応じて特定のポートを有効にすることができます。新しい NVA ルールを追加してポートを有効にすると、そのポートは 2 時間だけアクティブのままになります。同時に、別の NVA ルールを追加するとタイマーが再起動し、すべての有効なポートが 2 時間アクティブのままになります。

（注）
- クラウドゲートウェイの操作が進行中の場合、NVA のセキュリティルールは設定できません。
- Azure の送信元 IP アドレスには、サフィックスとして /30、/31、または /32 のみを使用できます。Azure の送信元 IP アドレスの例には、192.0.2.0/30、192.0.2.0/31、192.0.2.0/32 などがあります。

NVA への Azure ExpressRoute 接続に関する情報

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 17.8.1a、Cisco vManage リリース 20.8.1

Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 以降では、Cisco SD-WAN Manager は、SD-WAN トンネルを介したブランチオフィスから NVA への ExpressRoute 接続をサポートしています。ExpressRoute 接続は、データ転送のための、信頼性が高く、遅延が少なく、接続が高速なプライベートネットワークです。

NVA への Azure ExpressRoute 接続の詳細については、「Alternative Azure Designs」を参照してください。

各リージョンの複数の仮想ハブに関する情報

サポート対象の最小リリース：Cisco vManage リリース 20.11.1

（注） この機能は、Azure クラウドと Azure Government クラウドの両方でサポートされています。

単一のリージョンで Azure に接続されている数千のサイトを持つ組織の場合、Microsoft は複数のクラウドゲートウェイの作成と、単一のリージョンで最大 8 つの仮想ハブの作成をサポートしています。

Cisco vManage リリース 20.10.1 以前のリリースでは、Azure Virtual WAN ソリューションは、1 つのリージョンで単一の仮想ハブのみをサポートしています。Cisco vManage リリース 20.11.1 以降では、このソリューションは各リージョンで複数の仮想ハブをサポートしています。

仮想ネットワークへのクラウド ゲートウェイ アタッチメントは、ロード バランシング アルゴリズムに基づいています。クラウド ゲートウェイ アタッチメントにタグを追加する場合は、[Auto] を選択し、これによって、ロード バランシング アルゴリズムに基づいて VNet を配布することができます。新しいクラウドゲートウェイを作成したときは、VNet を再配布して、すべてのクラウドゲートウェイ間で既存の VNet をロードバランスすることができます。[Auto] の VNet タグを選択した場合にのみ、クラウドゲートウェイ間で VNet を再割り当てできます。クラウドゲートウェイにアタッチされている専用 VNet タグを再割り当てすることはできません。

Azure Virtual WAN 統合でサポートされるデバイス

サポートされている Azure インスタンス

Azure Virtual WAN 統合は、次の Cisco Catalyst 8000V インスタンスをサポートしています。

表 *61 : SKU* スケール値と *Azure* インスタンスタイプ

SKU スケール値	Azure インスタンスタイプ	インスタンスリソース	インスタンス数	サポート開始
2	Standard_D2_v2	2 個の CPU コアと 7 GB のメモリ	2	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a

SKU スケール値	Azure インスタンスタイプ	インスタンスリソース	インスタンス数	サポート開始
4	Standard_D3_v2	4 個の CPU コアと 14 GB のメモリ	2	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a
10	Standard_D4_v2	8 個の CPU コアと 28 GB のメモリ	2	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a
20 （Azure の米国中西部およびオーストラリア東部のリージョンでサポートされています）	Standard_D16_v5	16 個の CPU コアと 64 GB のメモリ	2	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a
40 （Azure の米国中西部およびオーストラリア東部のリージョンでサポートされています）	Standard_D16_v5	16 個の CPU コアと 64 GB のメモリ	3	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a
60 （Azure の米国中西部およびオーストラリア東部のリージョンでサポートされています）	Standard_D16_v5	16 個の CPU コアと 64 GB のメモリ	4	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a
80 （Azure の米国中西部およびオーストラリア東部のリージョンでサポートされています）	Standard_D16_v5	16 個の CPU コアと 64 GB のメモリ	5	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a

Azure Virtual WAN 統合の前提条件

セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックのルーティングの前提条件

（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。

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 17.6.1a、Cisco vManage リリース 20.6.1

Cisco Cloud OnRamp for Multicloud は、Microsoft Azure 環境と連携して動作するように設定されています。「Microsoft Azure Virtual WAN Integration」を参照してください。

ネットワーク仮想アプライアンスの Azure SKU スケーリング、監査、およびセキュリティルールの前提条件

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 17.7.1a、Cisco vManage リリース 20.7.1

- Cisco Cloud OnRamp for Multicloud は、Microsoft Azure 環境と連携して動作するように設定する必要があります。「Microsoft Azure Virtual WAN Integration」を参照してください。
- Azure クラウドアカウントの詳細。
- Azure マーケットプレイスへのサブスクリプション。
- Cisco SD-WAN Manager はインターネットに接続されている必要があり、Azure アカウントを認証するために Microsoft Azure と通信できる必要があります。
- クラウドゲートウェイが動作している必要があります。

Azure Virtual WAN 統合の制約事項

Azure Virtual WAN 統合の制約事項

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 17.4.1a、Cisco vManage リリース 20.4.1

- Azure Virtual WAN ハブアーキテクチャは、セグメンテーションをサポートしていません。
- VNet へのマッピング用に選択する VPN には、IP アドレス空間が重複しないようにする必要があります。
- VNet のタグ付けにより、すべての VPN と VNet が他のすべての VPN と VNet で表示されます。
- 各 Azure リージョンおよび各リソースグループに設定できる仮想ハブは 1 つだけです。
- Cisco SD-WAN Manager では、1 つのリソースグループのみが許可されます。
- リージョン間のハブ間接続の場合、すべての仮想ハブが同じ Azure Virtual WAN の一部である必要があります。
- IPv6 はサポートされていません。
- Azure Virtual WAN ハブはトレースルートをサポートしていません。
- 仮想 WAN ハブに接続されているブランチは、仮想 WAN ハブのデフォルトルートテーブルにのみ割り当てることができます。
- Cisco SD-WAN Manager を介して Azure リージョンで仮想 WAN ハブが作成または検出されない場合、そのリージョンの VNet は VNet タグを使用してマッピングされません。
- Azure WAN ハブに Cisco Catalyst 8000V ネットワーク仮想アプライアンス（NVA）を展開する場合、1 つのリソースグループと仮想 WAN でサポートされます。異なるリソースグループに Cisco Catalyst 8000V を展開することはできません。Cisco Catalyst 8000V NVA を展開すると、デフォルトでは、後続の展開のためにそのリソースグループと仮想 WAN に関連付けられます。

セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックのルーティングの制約事項

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 17.6.1a、Cisco vManage リリース 20.6.1

Azure Firewall Manager で動作する Azure のセキュリティ保護付き仮想ハブへのローカルトラフィックのルーティングには、Azure 環境の追加の運用料金がかかる場合があります。Azure サービスの条件を確認してください。

ネットワーク仮想アプライアンスの Azure SKU スケーリング、監査、およびセキュリティルールの制約事項

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 17.7.1a、Cisco vManage リリース 20.7.1

- クラウドゲートウェイの作成、編集、または削除中は、マルチクラウド監査サービスを実行できません。
- SKU スケール値と監査機能を変更する機能、およびポートを開く機能が、マルチクラウドを使用して Cisco SD-WAN Manager で作成されたクラウドゲートウェイにのみ一時的に適用されます。これらの機能は、Azure ポータルで直接作成されたネットワーク仮想アプライアンスには適用されません。

リージョンごとの複数の仮想ハブの制約事項

サポート対象の最小リリース：Cisco vManage リリース 20.11.1

リージョンごとに最大 8 つの仮想ハブを作成できます。

Azure Virtual WAN 統合のユースケース

セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックフローのルーティングのユースケース

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 17.6.1a、Cisco vManage リリース 20.6.1

- セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックのルーティングは、Azure ベースのファイアウォールまたはローカルファイアウォールのいずれかを使用して、すべての Azure ベースおよびローカルのインターネットトラフィックに同じファイアウォールポリシーを適用することが望ましい場合に役立つ可能性があります。
- ローカルブランチデバイスでファイアウォールを設定しない場合は、ローカルトラフィックをセキュリティ保護付き仮想ハブにルーティングすることが役立つ可能性があります。
- Azure 環境でファイアウォールを設定しない場合は、Azure トラフィックをローカルファイアウォールにルーティングすることが役立つ可能性があります。

Azure SKU スケーリングのユースケース

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 17.7.1a、Cisco vManage リリース 20.7.1

クラウドゲートウェイサービスのパフォーマンスまたはコスト効率を向上させるために、SKU スケール値を設定できます。CPU 負荷が 75% を超える場合はより高い SKU スケール値を設定でき、CPU 負荷が 25% を下回る場合はより低い SKU スケール値を設定できます。

Azure 監査のユースケース

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 17.7.1a、Cisco vManage リリース 20.7.1

接続またはネットワークの問題に直面している場合は、監査を開始します。Azure 監査によって提供される情報は、ネットワークの問題のトラブルシューティングに役立ちます。

NVA のセキュリティルールのユースケース

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 17.7.1a、Cisco vManage リリース 20.7.1

NVA のセキュリティルールを設定すると、特定のポートを有効にできます。

Azure Virtual WAN 統合の設定

Azure Virtual WAN ハブの設定

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 17.4.1a、Cisco vManage リリース 20.4.1

Cisco SD-WAN Manager の Cloud OnRamp for Multicloud ワークフローを使用して、Azure Virtual WAN ハブを作成し、Cisco Catalyst SD-WAN ブランチをプライベートネットワークまたはホスト VNet のアプリケーションに接続します。Azure Virtual WAN ハブを設定するには、次のタスクを指定された順序で実行します。

設定要件

Cisco SD-WAN Manager を使用して Azure Virtual WAN ハブを設定するには、以下が必要です。

- Azure クラウドアカウントの詳細。
- Azure マーケットプレイスへのサブスクリプション。
- Cisco SD-WAN Manager には、Azure クラウドゲートウェイを作成するために自由に使用できる 2 つの Cisco Catalyst 8000V ライセンスが必要です。
- Cisco SD-WAN Manager はインターネットに接続されている必要があり、Azure アカウントを認証するために Microsoft Azure と通信できる必要があります。

Azure クラウドアカウントの統合

Cisco SD-WAN Manager とアカウントの関連付け

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Setup] で、[Associate Cloud Account] をクリックします。
3. [Cloud Provider] フィールドで、ドロップダウンリストから [Microsoft Azure] を選択します。
4. 必要な情報を入力します。

フィールド	説明
Cloud Account Name	Azure サブスクリプションの名前を入力します。
[説明（Description）]（任意）	アカウントの説明を入力します。このフィールドは任意です。
Use for Cloud Gateway	[Yes] を選択すると、アカウントにクラウドゲートウェイが作成されます。デフォルトでは [No] が選択されています。
テナント ID	Azure Active Directory（AD）の ID を入力します。テナント ID を見つけるには、Azure Active Directory に移動し、[Properties] をクリックします。
Subscription ID	このワークフローの一部として使用する Azure サブスクリプションの ID を入力します。
Client ID	既存の Azure アプリケーション ID を入力します。Azure AD にアプリケーションを登録する方法、クライアント ID と秘密キーを取得する方法などの詳細については、Azure のドキュメントを参照してください。
秘密キー（Secret Key）	クライアント ID に関連付けられたパスワードを入力します。

5. [Add] をクリックします。

（注） 複数の Azure サブスクリプションを使用して VNet を検出したり、クラウドゲートウェイを作成したりする場合は、**[Cloud OnRamp for Multicloud Set up]** > **[Associate Cloud Account]** で、異なる Azure アカウントとして同じテナントの下にあるすべてのサブスクリプションを追加する必要があります。

グローバルクラウド設定の追加と管理

1. [Cloud OnRamp for Multicloud] ウィンドウで、[Setup] エリアの [Cloud Global Settings] をクリックします。
2. [Cloud Provider] フィールドで、ドロップダウンリストから [Microsoft Azure] を選択します。
3. グローバル設定を編集するには、[Edit] をクリックします。
4. グローバル設定を追加するには、[Add] をクリックします。
5. Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、[Enable Configuration Group] オプションを有効にして、設定グループを使用してマルチクラウドワークフローでデバイスを設定します。
6. [Software Image] フィールドで、Azure Virtual Hub で使用する WAN エッジデバイスのソフトウェアイメージを選択します。これは、プリインストールされた Cisco Catalyst 8000V イメージである必要があります。

（注） Cisco SD-WAN Manager リリースに基づいて、Cisco Catalyst 8000V イメージを選択します。Cisco SD-WAN Manager リリース 20.n の場合は、Cisco IOS XE リリース 17.n 以前の Cisco Catalyst 8000V イメージを選択します。たとえば、Cisco SD-WAN Manager リリース 20.5 の場合、Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a または Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a に対応するイメージを選択できます。Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降に対応するソフトウェアイメージがプリインストールされたイメージから使用可能な場合、Cisco SD-WAN Manager リリースと互換性がないため、そのようなイメージを選択しないでください。

7. [SKU Scale] フィールドで、容量要件に基づいて、ドロップダウンリストからスケールを選択します。
8. [IP Subnet Pool] フィールドで、Azure Virtual WAN ハブに使用する IP サブネットプールを指定します。サブネットプールには、/16 ～ /24 の範囲内のプレフィックスが必要です。

   単一の /24 サブネットプールは、1 つのクラウドゲートウェイのみをサポートできます。他のクラウドゲートウェイがすでにプールを使用している場合、プールを変更することはできません。サブネットの重複は許可されていません。

IP サブネットプールは、Azure Virtual WAN 内のすべての Azure Virtual WAN ハブを対象としていて、Virtual WAN ハブごとに 1 つの /24 プレフィックスがあります。Virtual WAN 内に作成する予定のすべての Virtual WAN ハブに、十分な /24 サブネットを割り当てていることを確認してください。Virtual WAN ハブが Microsoft Azure ですでに作成されている場合は、Cisco SD-WAN Manager を介してそれを検出し、検出されたハブに既存のサブネットプールを使用できます。

9. [Autonomous System Number] フィールドで、仮想ハブとの eBGP ピアリングのためにクラウドゲートウェイが使用する ASN を指定します。

注目 この値は、クラウドゲートウェイの作成後に変更することはできません。

10. [Push Monitoring Metrics to Azure] フィールドで、[Enabled] または [Disabled] を選択します。[Enabled] を選択すると、Azure サブスクリプションに関連付けられたクラウド ゲートウェイ メトリックが Microsoft Azure Monitoring Service ポータルに定期的に送信されます。これらのメトリックは、すべての NVA ベンダーに対して Microsoft Azure によって規定された形式で送信されます。

重要

- Cisco SD-WAN Manager を介して送信されるデータを処理およびモニタリングするための Azure Monitor サービスの使用に関連するコストが別途発生します。課金と使用条件については、Microsoft Azure のドキュメントを参照してください。
- テレメトリデータの収集と処理に関して、エンドユーザーに通知してエンドユーザーから必要な法的権利と許可を取得することは、マネージドサービスプロバイダーの責任です。

11. Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 以降では、[Advertise Default route to Azure Virtual Hub] フィールドを有効または無効にできます。デフォルトでは、このフィールドは [Disabled] になっています。[Enabled] をクリックすると、仮想ネットワークからのインターネットトラフィックが Cisco Catalyst SD-WAN ブランチ経由でリダイレクトされます。

12. Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 以降では、[Enabled] または [Disabled] をクリックして、[Enable Periodic Audit] フィールドを有効または無効にできます。

    定期監査を有効にすると、Cisco SD-WAN Manager は 2 時間ごとに自動監査をトリガーします。この自動監査はバックグラウンドで実行され、不一致レポートが生成されます。

13. Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 以降では、[Enabled] または [Disabled] をクリックして、[Enable Auto Correct] フィールドを有効または無効にできます。自動修正オプションを有効にすると、定期的な監査がトリガーされるたびに、検出されたすべての回復可能な問題が自動修正されます。

14. [Add] または [Update] をクリックします。

クラウドゲートウェイの作成と管理

クラウドゲートウェイの作成には、Azure Virtual WAN ハブとハブ内の 2 つの Cisco Catalyst 8000V インスタンスのインスタンス化または検出が含まれます。

（注） Azure ポータルを使用して Cisco Catalyst 8000V インスタンスをプロビジョニングしていて、Azure ポータルを使用して Azure Virtual WAN と Azure Virtual WAN ハブを作成した場合は、以下の手順を使用してそれらを検出することもできます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Manage] で、[Create Cloud Gateway] をクリックします。
3. [Cloud Provider] フィールドで、ドロップダウンリストから [Microsoft Azure] を選択します。
4. [Cloud Gateway Name] フィールドに、クラウドゲートウェイの名前を入力します。

（注） Azure ポータルを使用して Azure Virtual WAN ハブを作成した場合は、このフィールドに正確な仮想ハブ名を入力してください。これにより、ハブに関連付けられたリソースが確実に検出されます。関連付けられた Azure Virtual WAN と Azure Virtual WAN ハブは、[Virtual WAN] および [Virtual Hub] フィールドから選択できるようになります。関連付けられた NVA も、[UUID] フィールドに自動入力されます。

5. （任意）[Description] フィールドに、クラウドゲートウェイの説明を入力します。
6. [Account Name] フィールドで、ドロップダウンリストから Azure アカウント名を選択します。
7. [Region] フィールドで、ドロップダウンリストから [Azure] リージョンを選択します。
8. （Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降、クラウドゲートウェイを作成したとき、または Azure クラウドゲートウェイのグローバル設定を構成したときに [Enable Configuration Group] オプションを有効にした場合にのみ適用）[Configuration Group] ドロップダウンリストから次のいずれかのアクションを実行します。
   - 構成グループを選択します。
   - 新しい設定グループを作成して使用するには、[Create New] を選択します。[Create Configuration Group] ダイアログボックスで、新しい設定グループの名前を入力し、[Done] をクリックします。ドロップダウンリストから新しい設定グループを選択します。

   選択した設定グループは、マルチクラウドワークフローでデバイスを設定するために使用されます。

（注） [Configuration Group] ドロップダウンリストには、この手順の説明に従って作成した設定グループのみが含まれています。Cisco Catalyst SD-WAN で作成された他の設定グループは含まれません。このドロップダウンリストの設定グループには、このプロバイダーに必要なオプションが含まれています。

設定グループの詳細については、『Cisco Catalyst SD-WAN Configuration Groups』を参照してください。

9. [Resource Group] フィールドで、ドロップダウンリストからリソースグループを選択するか、[Create New] を選択します。

（注） 新しいリソースグループの作成を選択した場合は、次の 2 つのフィールドで新しい Azure Virtual WAN と Azure Virtual WAN ハブも作成する必要があります。

10. [Virtual WAN] フィールドで、ドロップダウンリストから Azure Virtual WAN を選択します。または、[Create New] をクリックして、新しい Azure 仮想 WAN を作成します。

11. [Virtual HUB] フィールドで、ドロップダウンリストから Azure 仮想 WAN ハブを選択します。または、[Create New] をクリックして、新しい Azure 仮想 WAN ハブを作成します。

（サポート対象の最小リリース：Cisco vManage リリース 20.11.1）[Region]、[Resource Group]、および [Virtual WAN] を選択すると、[Azure Virtual WAN Hub] フィールドに [Create a new vHub using Cloud Gateway Name] と表示されます。ドロップダウンリストから、検出された仮想ハブを選択します。

仮想ハブは、Cisco SD-WAN Manager で次の 2 つの方法で検出されます。

- Azure ポータルで作成された、ネットワーク仮想アプライアンス（NVA）を備えた仮想ハブ。
- Azure ポータルで作成され、Cisco SD-WAN Manager によって検出された仮想ハブ。その後、Cisco SD-WAN Manager で仮想ハブに NVA を追加できます。

12. （最小リリース：Cisco vManage リリース 20.10.1）[Site Name] ドロップダウンリストから、クラウドゲートウェイを作成するサイトを選択します。

13. [Settings] フィールドで、次のいずれかを選択します。

- [Default]：IP サブネットプール、イメージバージョン、および SKU スケールサイズのデフォルト値が、グローバル設定から取得されます。
- [Customized]：このオプションを使用してグローバル設定を上書きできます。このオプションは、新しく作成されたクラウドゲートウェイにのみ適用されます。

（サポート対象の最小リリース：Cisco vManage リリース 20.10.1）

Azure ポータルで作成された Cisco Catalyst 8000V を使用した仮想ハブを Cisco SD-WAN Manager にオンボードした場合にのみ、[Instance Setting] エリアの次のフィールドにグローバル設定の設定が自動入力されます。

- ソフトウェア イメージ
- SKU Scale
- IP Subnet Pool
- UUID (specify 2)

（注） Cisco SD-WAN Manager でクラウドゲートウェイがオンボードされると、NVA なしで、[IP Subnet Pool] フィールドと [UUID (specify 2)] フィールドが自動入力されます。

ドロップダウンリストでオプションを選択することで、グローバル設定を上書きできます。

14. Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降、クラウドゲートウェイを作成したとき、またはAzure クラウドゲートウェイのグローバル設定を構成したときに [Enable Configuration Group] オプションを有効にした場合にのみ適用）[Configuration Group] で、クラウドゲートウェイの作成に使用される設定グループの名前を選択するか、新しい設定グループを作成します。

(

15. [UUID (specify 2)] フィールドで、ドロップダウンリストから 2 つの Cisco Catalyst 8000V ライセンスを選択します。

（注） Cisco vManage リリース 20.10.1 以降では、[Site Name] ドロップダウンリストからサイトを選択すると、UUID が自動的に入力されます。

16. （最小リリース：Cisco vManage リリース 20.10.1）[Multi-Region Fabric Settings] エリアの [MRF Role] で、[Border] または [Edge] を選択します。

このオプションは、マルチリージョン ファブリックが有効になっている場合にのみ使用できます。

17. [Add] をクリックします。

（注） Azure Virtual WAN ハブが作成され、Cisco Catalyst 8000V インスタンスが仮想ハブ内にプロビジョニングされるまでに、最大 40 分かかることがあります。

（注） Azure Virtual WAN ハブの作成が完了したら、それをセキュリティで保護された Azure Virtual WAN ハブに変換するオプションを使用できます。ただし、この設定は Microsoft Azure ポータルからのみ実行できます。詳細については、Microsoft Azure のドキュメントを参照してください。

（注） 異なるリージョンに Azure クラウドゲートウェイを同時に作成できます。

- 異なるリージョンに複数のクラウドゲートウェイを作成する前に、最初のクラウドゲートウェイのリソースグループ、仮想 WAN、およびストレージアカウントを作成します。
- 同じリージョンに複数のクラウドゲートウェイを作成する前に、リージョン内の最初のクラウドゲートウェイの仮想ハブを作成します。
- Cloud OnRamp for Multicloud 用に Azure でストレージアカウントを作成するには、BLOB アクセスが必要です。Cisco Catalyst 8000V デバイスでクラウドゲートウェイを作成する際、およびスケール操作を変更する際には、BLOB アクセスが必要です。

（注） Cloud OnRamp for Multicloud ワークフローは、各 Azure リージョンで最大 8 つの仮想ハブをサポートしています。各仮想ハブに 2 つのクラウド ゲートウェイ ネットワーク仮想アプライアンス（NVA）を展開できます。

ホスト VNet の検出とタグの作成

Azure 仮想ハブを作成したら、仮想ハブのリージョンでホスト VNet を検出できます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Discover] ワークフローで、[Host Private Networks] をクリックします。
3. [Cloud Provider] フィールドで、[Microsoft Azure] を選択します。

   ホスト VNet のリストがテーブルに表示され、[Cloud Region]、[Account Name]、[VNET Tag]、[Cloud Gateway Attachment]、[Account ID]、[Resource Group]、および [VNet Name] 列が表示されます。
4. [Tag Actions] ドロップダウンリストをクリックして、次のいずれかを選択します。
   - [Add Tag]：VNet または VNet のグループのタグを作成します。

     （サポート対象の最小リリース：Cisco vManage リリース 20.11.1）[Cloud Gateway Attachment] に [Auto] を選択するか、既存のクラウドゲートウェイにマッピングすることができます。

- [Edit Tag]：選択した VNet の既存のタグを変更します。

  （サポート対象の最小リリース：Cisco vManage リリース 20.11.1）[Edit Tag] から [Cloud Gateway Attachment] を選択できます。選択しない場合、またはクラウドゲートウェイがそのリージョンでまだ作成されていない場合は、[Auto] オプションが自動的に選択されます。[Auto] オプションは、ロード バランシング アルゴリズムに基づいています。[Auto] オプションが選択された VNet では、クラウド ゲートウェイ アタッチメントは、タグの作成時ではなく、マッピング時に選択されます。

- [Delete Tag]：選択した VNet のタグを削除します。

VNet タグとブランチネットワーク VPN のマッピング

VNet から VPN へのマッピングを有効にするには、1 つまたは複数の Azure リージョンで VNet のセットを選択し、タグを定義します。次に、同じタグを使用して VNet をマッピングするサービス VPN を選択します。1 セットのブランチオフィスには 1 セットの VNet のみをマッピングできます。選択したすべての VNet は、選択したすべての VPN に対して表示され、その逆も同様です。1 つのサービス VPN は、1 つまたは複数のタグにマッピングできます。複数の VNet が同じタグを持つことができます。クラウドゲートウェイが同じリージョンに存在する場合、またはタグ付け操作が行われる場合、マッピングは自動的に実現されます。

（注） VNet タグにマッピングされるように選択した VPN は、重複する IP アドレスを持つことはできません。これは、Microsoft Azure Virtual WAN ではセグメンテーションがサポートされていないためです。

Cisco Catalyst SD-WAN ネットワークの VNet-VPN マッピングを編集するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Intent Management] で、[Connectivity] をクリックします。
3. インテントを定義するには、[Edit] をクリックします。
4. VPN、およびそれに関連付けられている VNet タグに対応するセルを選択し、[Save] をクリックします。

[Intent Management - Connectivity] ウィンドウには、ブランチ VPN とそれらがマッピングされている VNet タグ間の接続ステータスが表示されます。画面の上部には、さまざまなステータスを理解するのに役立つ凡例が表示されます。表示されたマトリックス内のセルのいずれかをクリックすると、[Mapped]、[Unmapped]、[Outstanding] マッピングなど、詳細なステータス情報が表示されます。

VNet の再調整

サポート対象の最小リリース：Cisco vManage リリース 20.11.1

VNet を再配布して、特定のタグのリージョン内のすべてのクラウドゲートウェイ間で既存の VNet をいつでもロードバランスすることができます。クラウドゲートウェイ全体で [Auto] オプションが選択されている VNet のみを再割り当てできます。VNet の割り当ては、ロード バランシング アルゴリズムに基づいています。再バランシングにはクラウドゲートウェイへの VNET のデタッチと再アタッチが含まれるため、トラフィックの中断が発生する可能性があります。VNet の再バランシング後、[tagging] ページで、VNET からクラウドゲートウェイへの修正済みマッピングを表示できます。

（注） 次の場合は、VNet を再バランシングできません。

- クラウドゲートウェイの作成、編集、または削除が進行中の場合。
- VNet のマッピングが進行中の場合。
- 監査が進行中の場合。

1. Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択します。
2. [Intent Management] ワークフローで、[Rebalance VNETS (Azure/GovCloud)] をクリックします
3. [Cloud Provider] フィールドで、[Microsoft Azure] を選択します。
4. [Region] フィールドで、ドロップダウンリストから [Azure] リージョンを選択します。
5. [Tag Name] フィールドで、ドロップダウンリストからタグを選択します。
6. [再調整（Rebalance）] をクリックします。

Azure ポータルからの Azure Virtual WAN ハブの設定

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 17.4.1a、Cisco vManage リリース 20.4.1

（注） Azure Virtual WAN ハブのエンドツーエンド設定は、Cisco SD-WAN Manager を使用して行うことができます。または、Azure ポータルを使用してリソースグループ、仮想 WAN、および仮想 WAN ハブを作成してから、Cisco SD-WAN Manager に戻って Azure ポータルを使用して作成したインフラストラクチャを検出し、VNet タグを作成してそれらをサービス VPN にマッピングすることもできます。

設定ワークフロー

タスク	説明
タスク 1	Cisco SD-WAN Manager のメニューから、Azure Virtual WAN ハブに自由に使用できる 2 つの Cisco Catalyst 8000V インスタンスを選択します。次に、これらのインスタンス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。
タスク 2	Azure ポータルで、仮想 WAN ハブを作成し、作成した仮想 WAN ハブに Cisco Catalyst 8000V インスタンスを関連付けます。
タスク 3	Azure ポータルで、Cisco SD-WAN Manager で生成されたブートストラップ構成ファイルを使用して、Cisco Catalyst 8000V の NVA を作成します。
タスク 4	Cisco SD-WAN Manager で、Azure ポータルで作成したインフラストラクチャを検出します。 この検出の一環として、Azure Virtual WAN ハブで作成された NVA が起動します。
タスク 5	Cisco SD-WAN Manager で、VNet タグをマッピングして、ホスト VNet とサービス VPN 間の接続を設定します。

（注） Azure ポータルを使用して行う設定は、このドキュメントの範囲外です。ただし、Azure ポータルを使用して設定を完了するために役立つ Azure ドキュメントへのリンクが用意されています。

タスク 1.Cisco Catalyst 8000V のブートストラップ設定の生成

前提条件：次の手順に進む前に、2 つの Cisco Catalyst 8000V インスタンスの Cisco SD-WAN Manager で使用可能なライセンスが必要です。

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 20.7.1 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Template Type] ドロップダウンリストから [Default] を選択します。

   デフォルトテンプレートのリストが表示されます。

4. [Default_Azure_vWAN_C8000V_Template_V01] の目的の行について、[...] をクリックし、[Attach Devices] を選択します。
5. [Available Devices] のリストから 2 つの Cisco Catalyst 8000V インスタンスを選択し、[Attach] をクリックします。

   次の画面に、デバイステンプレートにアタッチしたデバイスが表示されます。
6. [Device Templates] 画面で、デバイスの行ごとに [...] をクリックし、[Update Device Template] を選択します。
7. デバイスごとに、要求された情報（ホスト名、システム IP、およびサイト ID）を入力します。**Update** をクリックします。
8. [Next] をクリックします。[Configure Devices] ダイアログボックスで、チェックボックスをオンにして [OK] をクリックします。

   [Task View] 画面が開きます。デバイス情報が更新されるまで数分かかります。ステータス列にステータスが [Done - Complete] と表示されている場合は、デバイス情報が更新されたことを示しています。
9. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Devices]** の順に選択します。
10. 更新したデバイスを見つけて、デバイスごとに [...] をクリックします。オプションから [Generate Bootstrap Configuration] を選択します。
11. [Generate Bootstrap Configuration] ダイアログボックスで、[Include Default Root Certificate] の選択を解除し、[OK] をクリックします。
12. ダイアログボックスで、[Download] をクリックします。

タスク 2. Azure Virtual WAN ハブの作成

この項の手順は、Azure ポータルで実行します。これらの手順を実行するための Azure ドキュメントへのリンクが用意されています。この項の手順を実行するには、Azure のサブスクリプションとログイン情報が必要です。

Azure ポータルで、次の手順を実行します。

1. リソースグループを作成します。
2. 仮想 WAN を作成します。
3. 仮想 WAN ハブを作成します。

次のステップ：仮想ハブで、Cisco Catalyst 8000V インスタンスのネットワーク仮想アプライアンス（NVA）を作成します。NVA を作成する手順は、NVA パートナーによって異なる場合があります。そのため、次の項では Cisco Catalyst 8000V に固有の情報を提供しています。

タスク 3.Cisco Catalyst 8000V の NVA の作成

1. Azure ポータルの検索ボックスで **Cisco Cloud vWAN Application** を検索し、[Marketplace] の下にある結果をクリックします。
2. [Cisco Cloud vWAN Application] ページが開きます。[Create] をクリックします。

   必要な詳細を入力し、[Next: Cisco SD-WAN Cloud Gateway] をクリックします。
3. 要求された詳細を入力します。この画面で入力する詳細は、Cisco SD-WAN Manager の [Cloud Global Settings] 画面に似ています。
   1. [Virtual WAN]：ドロップダウンリストから作成した仮想 WAN を選択します。
   2. [Virtual WAN Hubs]：仮想 WAN を選択すると、その WAN 内のすべての仮想ハブがこのドロップダウンリストに表示されます。この手順で使用する仮想 WAN ハブを選択します。
   3. [Scale Unit]：
   4. [Cisco Version]：Cisco Catalyst 8000V インスタンスのソフトウェアバージョンを入力します。
   5. [BGP ASN to peer with Azure Router Service]：これは、NVA が使用する番号です。
   6. [Cisco SDWAN Cloud Gateway Name]：クラウドゲートウェイの名前を入力します。
   7. [Upload the Bootstrap configuration File that was generated]：このフィールドを使用して、Cisco Catalyst 8000V から Cisco SD-WAN Manager 用にダウンロードしたブートストラップ構成ファイルに移動します。

（注） この手順では、必ず両方のブートストラップ構成ファイルを選択してください。

4. [Next] をクリックし、デフォルト値を維持します。
5. チェックボックスをオンにして利用規約に同意します。[Create] をクリックします。

   展開が完了すると、2 つの Cisco Catalyst 8000V インスタンスが仮想ハブ内にプロビジョニングされます。これらが起動すると、Cisco SD-WAN Manager にも接続されます。

Cisco SD-WAN Manager のメインダッシュボードで、[Devices] の横にある上向き矢印をクリックします。Azure ポータルを介した展開が成功すると、2 つの Cisco Catalyst 8000V インスタンスが到達可能として表示されます。

タスク 4.Cisco SD-WAN Manager での NVA の検出

前提条件：Cisco SD-WAN Manager で NVA を検出するには、Cisco SD-WAN Manager に Azure アカウントを追加する必要があります。Azure アカウントを Cisco SD-WAN Manager にまだ関連付けていない場合は、Azure クラウドアカウントの統合 （313 ページ）を参照してください。

Azure ポータルを使用して設定した NVA または Cisco Catalyst 8000V を検出するには、クラウドゲートウェイの作成と管理 （316 ページ）に記載されている手順に従います。

タスク 5. VNet と VPN 間の接続の設定

VNet から VPN へのタグ付けを設定するには、まず ホスト プライベート ネットワークの検出してから、VNet タグとブランチネットワーク VPN のマッピングして VNet とブランチネットワークまたは VPN を接続する必要があります。

セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックフローのルーティングの設定

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 17.6.1a、Cisco vManage リリース 20.6.1

Azureのセキュリティ保護付き仮想ハブへのローカル発信トラフィックフローのルーティング

はじめる前に

- Cisco Catalyst SD-WAN を使用して Azure Virtual WAN ハブの統合を設定します。詳細については、「Azure Virtual WAN Hub Integration with Cisco SD-WAN」を参照してください。
- Azure環境でファイアウォールを設定します（必要なファイアウォールポリシーを含む）。

Azure のセキュリティ保護付き仮想ハブへのローカル発信トラフィックフローのルーティング

発信インターネットトラフィックをAzureのセキュリティ保護付き仮想ハブにルーティングするようにブランチルータを設定するには、次の手順を実行します。

1. ローカルブランチルータで、ブランチルータに、ブランチからのダイレクトインターネットアクセス（DIA）用に設定されたスタティックデフォルトルートがないことを確認します。

   ローカルブランチルータで、**show ip route vrf** *vrf-number* コマンドを使用して、スタティック デフォルト ルートがサービス側 VPN に設定されていないことを確認します。

2. ローカルブランチルータで、**show ip route vrf** *vrf-number* コマンドを使用して、ローカルブランチルータとAzure間の通信用に設定したVRFを使用して、ローカルブランチルータからのインターネットトラフィックが Azure ファイアウォールにルーティングされていることを確認します。コマンド出力で、0.0.0.0 と表されるデフォルトルートに関連付けられている IP アドレスを探します。この IP アドレスが、Azure ファイアウォールが有効になっている Azure ハブで動作しているクラウドゲートウェイに対応している必要があります。

   次の例では、VRF 100 を使用しています。この例では、コマンド出力の一部のみが表示されています。Azure ハブで動作しているクラウドゲートウェイに対応する IP アドレスは、209.165.201.1 と 209.165.201.2 です。

```
Device# show ip route vrf 100

...
m*    0.0.0.0/0 [251/0] via 209.165.201.1, 21:06:00, Sdwan-system-intf
                [251/0] via 209.165.201.2, 21:06:00, Sdwan-system-intf
...
```

3. Azure環境で、Azureファイアウォールを介してルーティングされるようにインターネットトラフィックを設定します。

ローカルブランチルータへの Azure 発信トラフィックフローのルーティング

はじめる前に

- Cisco Catalyst SD-WAN を使用して Azure Virtual WAN ハブの統合を設定します。詳細については、「Azure Virtual WAN Hub Integration with Cisco SD-WAN」を参照してください。
- ローカルブランチルータでファイアウォールを設定します（必要なファイアウォールポリシーを含む）。

ローカルブランチルータへの Azure 発信トラフィックフローのルーティング

発信インターネットトラフィックをローカルブランチルータのファイアウォールにルーティングするように Azure を設定するには、次の手順を実行します。

1. Cisco SD-WAN Manager で、ローカルブランチルータの CLI テンプレートを使用して、次のコマンドを設定に追加します。これにより、ローカルルータが Azure 環境のデフォルトルートとしてアドバタイズされ、Azure Virtual Network が発信インターネットトラフィックをブランチルータにルーティングするようになります。0.0.0.0 はデフォルトルートを表すことに注意してください。

```
address-family ipv4 vrf branch-router-vpn-id
   advertise connected
   advertise static
   advertise network 0.0.0.0/0
```

   指定された VPN 内のトラフィックのみがブランチルータに転送されます。VPN が Cisco Catalyst SD-WAN と Azure の間の接続をマッピングする方法については、「How Virtual WAN Hub Integration Works」を参照してください。

   次の例では、VPN 100 の Azure トラフィックをブランチルータに転送しています。

```
address-family ipv4 vrf 100
   advertise connected
   advertise static
   advertise network 0.0.0.0/0
```

2. Azure 環境で、トラフィックがローカルブランチルータにルーティングされていることを確認します。ルーティングテーブルを表示し、次のように表示されていることを確認します。

   プレフィックス：0.0.0.0/0
   ネクストホップタイプ：VPN_S2S_GATEWAY

SKU スケール値の設定

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 17.7.1a、Cisco vManage リリース 20.7.1

SKU スケール値を設定するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Manage] の下の [Gateway Management] をクリックします。

   [Cloud Gateways] と、クラウドアカウント名、ID、クラウドタイプ、およびその他の情報を含むクラウドゲートウェイのリストを表示するテーブルが表示されます。
3. 対応するクラウドゲートウェイの隣にある [...] をクリックし、[Edit] を選択します。
4. [SKU Scale] ドロップダウンリストから値を選択します。

（注） [2]、[4]、および [10] の SKU スケール値のみがサポートされています。

5. [Update] をクリックします。

オンデマンド監査の開始

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 17.7.1a、Cisco vManage リリース 20.7.1

これは、ユーザーが起動する監査です。オンデマンド監査を開始するには、次の手順に従います。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Intent Management] の下の [Audit] をクリックします。
3. [Cloud Provider] ドロップダウンリストで、[Microsoft Azure] を選択します。

   このウィンドウには、さまざまな Microsoft Azure オブジェクトのステータスが表示されます。いずれかのオブジェクトのステータスが [In Sync] の場合は、そのオブジェクトにエラーがないことを意味します。オブジェクトのステータスが [Out of Sync] の場合は、Cisco SD-WAN Manager で利用できるオブジェクトの詳細と Azure データベースで利用できる詳細との間に不一致があることを意味します。
4. いずれかのオブジェクトのステータスが [Out of Sync] の場合は、[Fix Sync issues] をクリックします。このオプションにより、回復可能なエラーがあればそれが解決され、ステータス アクティビティ ログを表示するウィンドウが開きます。

オブジェクトのステータスが引き続き [Out of Sync] と表示される場合は、手動による介入が必要なエラーであることを意味します。

（注） マルチクラウド監査サービスは、他のクラウド操作の進行中は実行されません。

定期監査の有効化

次の手順では、定期監査を有効にする手順について説明します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Setup] エリアで、[Cloud Global Settings] をクリックします。
3. [Enable Periodic Audit] フィールドを有効または無効にするには、[Enabled] または [Disabled] をクリックします。

   [Enabled] をクリックすると、Cisco SD-WAN Manager は 2 時間ごとに自動監査をトリガーします。この自動監査はバックグラウンドで実行され、不一致レポートが生成されます。

   監査の不一致と解決の例については、「監査の不一致の例」を参照してください。
4. [Update] をクリックします。

NVA のセキュリティルールの設定

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 17.7.1a、Cisco vManage リリース 20.7.1

NVA のセキュリティルールを設定するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Manage] の下の [Gateway Management] をクリックします。

   [Create Cloud Gateways] ウィンドウと、クラウドアカウント名、ID、クラウドタイプ、およびその他の情報を含むクラウドゲートウェイのリストを表示するテーブルが表示されます。
3. 対応するクラウドゲートウェイの隣にある [...] をクリックし、[Add/Edit Security Rules] を選択します。

   [Add/Edit Security Rules] ウィンドウが表示されます。

   1. 新しいセキュリティルールを追加するには、[Add Security Rule] をクリックし、次の詳細を入力します。

表 *62 :* パラメータの表

パラメータ	説明
ポート番号	ポート範囲を指定します。
IPv4 送信元アドレス	IP アドレスを指定します。

2. [Add] をクリックします。
3. （オプション）セキュリティルールを編集するには、鉛筆アイコンをクリックします。
4. （オプション）セキュリティルールを削除するには、削除アイコンをクリックします。

4. [Update] をクリックします。

（注） セキュリティルールはすべて 2 時間のみアクティブになります。

Azure Virtual WAN 統合の確認

クラウドゲートウェイの表示、編集、または削除

1. Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択します。
2. [Cloud] をクリックします。
3. [Manage] の下の [Gateway Management] をクリックします。

   既存のクラウドゲートウェイの詳細がテーブルにまとめられています。
4. このテーブルで、目的のクラウドゲートウェイの […] をクリックします。
   - クラウドゲートウェイの詳細を表示するには、[View] をクリックします。
   - クラウドゲートウェイの説明を編集するには、[Edit] をクリックします。
   - クラウドゲートウェイを削除するには、[Delete] をクリックして、ゲートウェイを削除することを確定します。

     （サポート対象の最小リリース：Cisco vManage リリース 20.11.1）クラウドゲートウェイを削除すると、アタッチされた VNet はロードバランシング アルゴリズムに基づいて同じリージョン内の他の選択されたクラウドゲートウェイに移動し、VNet は [Auto] としてマークされます。

Azure SKU スケール値の更新の確認

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 17.7.1a、Cisco vManage リリース 20.7.1

Azure SKU スケール値の更新を確認するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Manage] の下の [Gateway Management] をクリックします。

   [Create Cloud Gateways] ウィンドウが表示されます。テーブルには、クラウドアカウント名、ID、クラウドタイプ、およびその他の情報とともにクラウドゲートウェイのリストが表示されます。
3. 対応するクラウドゲートウェイの隣にある [...] をクリックし、[View] を選択します。

   変更された SKU 値が [View Cloud Gateway] ウィンドウに表示されます。

ネットワーク仮想アプライアンスのセキュリティルールの確認

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 17.7.1a、Cisco vManage リリース 20.7.1

NVA 用に作成されたセキュリティルールを確認するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Manage] の下の [Gateway Management] をクリックします。

   [Create Cloud Gateways] ウィンドウと、クラウドアカウント名、ID、クラウドタイプ、およびその他の情報を含むクラウドゲートウェイのリストを表示するテーブルが表示されます。
3. 目的のクラウドゲートウェイで、[...] をクリックし、[Add/Edit Security Rules] を選択します。

   [Add/Edit Security Rules] ウィンドウが表示され、更新されたセキュリティの次のいずれかのステータスが示されます。

   - [Successful]
   - [In-progress: Check the status after sometime.]
   - [Failed: Recreate the security rule.]

Cisco SD-WAN Manager を使用した Azure Virtual WAN 統合のモニター

Azure Virtual WAN 統合のモニター

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 17.4.1a、Cisco vManage リリース 20.4.1

NVA 接続

新しいクラウドゲートウェイを作成するときに、Azure Virtual WAN ハブ内でプロビジョニングされた Cisco Catalyst 8000V インスタンスの作成と到達可能性を確認できます。これらのインスタンスが正常に設定されていて到達可能かどうかを表示するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから**[Monitor]** > **[Overview]** の順に選択します。

   Cisco SD-WAN Manager リリース 20.6.x 以前：Cisco SD-WAN Manager のメニューから、**[Dashboard]** > **[Main Dashboard]** を選択します。

2. [WAN Edge] で、表示された数字の横にある上向き矢印をクリックします。この数字は、使用可能な WAN エッジデバイスを表しています。

3. ポップアップウィンドウに表示されたテーブルで、クラウドゲートウェイの作成時に選択した Cisco Catalyst 8000V インスタンスを探します。クラウドゲートウェイの設定が成功すると、インスタンスがテーブルに表示され、到達可能として表示されます。

Microsoft Azure Monitor サービスを使用した NVA データのモニター

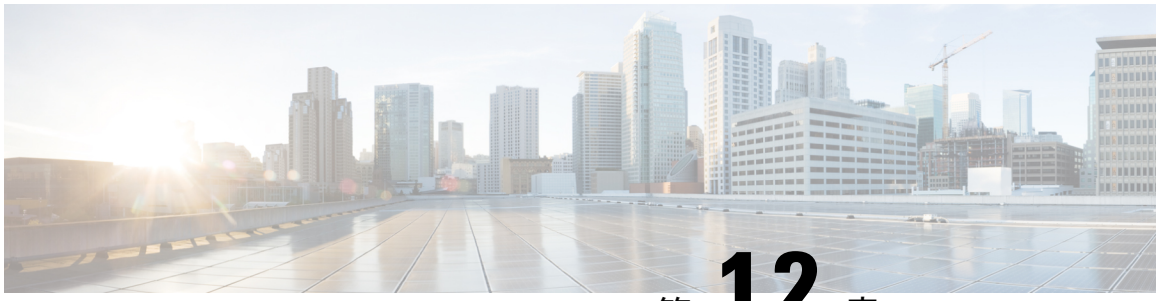
Cisco SD-WAN Manager では、**[Cloud OnRamp for Multicloud]** > **[Cloud Global Settings]** ウィンドウを使用して、Azure ポータルへのメトリックの送信を有効にできます。

[Push Monitoring Metrics to Azure] オプションを有効にすると、Cisco SD-WAN Manager と統合した Azure アカウントに関連付けられているすべてのクラウドゲートウェイに関するデータが Azure Monitor サービスに送信されます。

Azure Monitoring サービスの詳細については、Azure のドキュメントを参照してください。

重要

- Cisco SD-WAN Manager を介して送信されるデータを処理およびモニタリングするための Azure Monitor サービスの使用に関連するコストが別途発生します。課金と使用条件については、Microsoft Azure のドキュメントを参照してください。
- テレメトリデータの収集と処理に関して、エンドユーザーに通知してエンドユーザーから必要な法的権利と許可を取得することは、マネージドサービスプロバイダーの責任です。



第 12 章

米国政府向け Microsoft Azure の統合

（注） p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。

表 *63 :* 機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud での米国政府向け Azure クラウドのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	米国政府向け Azure クラウドと Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud を統合することで、米国政府とその取引先の Federal Risk and Authorization Management Program（FedRAMP）の要件を満たす分離されたクラウドに、非常に機密性の高いワークロードを移動および保存することができます。 仮想 WAN を使用した Azure 統合で使用できる機能と同じすべての機能が、米国政府向け Azure クラウドでも使用できます。
設定グループを使用した米国政府向け Azure のためのデバイスの設定	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	この機能により、Cisco SD-WAN Manager の設定グループを使用して、米国政府向け Azure のために自動化を使用してデバイスを設定することができます。

- 米国政府向け Azure 統合に関する情報 （334 ページ）
- 米国政府向け Azure でサポートされるデバイス （336 ページ）
- 米国政府向け Azure 統合の前提条件 （336 ページ）
- 米国政府向け Azure 統合の制約事項 （336 ページ）
- 米国政府向け Azure 統合のユースケース （336 ページ）
- 米国政府向け Azure の設定 （336 ページ）
- 米国政府向け Azure 統合のモニター （337 ページ）

米国政府向け Azure 統合に関する情報

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 17.9.1a、Cisco vManage リリース 20.9.1

この機能により、米国政府向け Azure クラウドが Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud に追加され、非常に機密性の高いワークロードを米国政府向け Azure クラウドに移動して保存することができるようになります。

次に、米国政府向け Azure クラウドに保存できる非常に機密性の高いワークロードの例を示します。

- コントローラの未分類情報（CUI）
- 個人識別情報（PII）
- 機密性の高い患者の医療記録
- 財務データ
- 法執行データ
- データのエクスポート

Azure Virtual WAN 統合で使用できる機能と同じ機能が、米国政府向け Azure 統合でも使用できます。Azure Virtual WAN は、Azure を介して最適化および自動化されたブランチ間の接続を提供するネットワーキングサービスです。

米国政府向け Azure クラウドの詳細については、米国政府向け Azure のドキュメントを参照してください。

Cisco SD-WAN Manager で Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud の一部として米国政府向け Azure を設定します。

米国政府向け Azure 統合の利点

- Cisco SD-WAN Manager の Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud の一部として、米国政府向け Azure クラウドに非常に機密性の高いワークロードを保存できます
- Cisco SD-WAN Manager での Azure Virtual WAN 統合と同じ機能とワークフローをサポートします
- 米国政府のワークロード専用のデータを保存するための、Azure の独立したインスタンスを提供します
- 米国内のデータセンターとネットワークによりセキュリティを強化します
- 機密データへの潜在的なアクセスを、スクリーニングされた米国の担当者のみに制限します
- 地理的冗長ストレージを提供するための、リージョンペアリングのサポートが含まれています

  リージョンペアリングの詳細については、Microsoft Azure のマニュアルを参照してください。

米国政府向け Azure でサポートされるデバイス

米国政府向け Azure でサポートされているデバイスの詳細については、「Supported Azure Instances」を参照してください。

米国政府向け Azure 統合の前提条件

米国政府向け Azure 統合の前提条件の詳細については、「Prerequisites for Azure Virtual WAN Integration」を参照してください。

米国政府向け Azure 統合の制約事項

- Azure ポータルからのネットワーク仮想アプライアンス（NVA）の作成はサポートされていません。
- 米国政府向け Azure のテレメトリはサポートされていません。

米国政府向け Azure 統合のユースケース

Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud と米国政府向け Azure クラウドを使用すると、機密データを米国政府向け Azure クラウドに安全に移動して保存することができるようになります。米国政府向け Azure クラウドは、米国政府とその取引先のワークロード専用の分離されたクラウドです。

次に、米国政府向け Azure クラウドに保存できる機密データの例を示します。

- コントローラの未分類情報（CUI）
- 個人識別情報（PII）
- 機密性の高い患者の医療記録
- 財務データ
- 法執行データ
- データのエクスポート

米国政府向け Azure の設定

米国政府向け Azure 統合を設定するためのワークフローは、Azure Virtual WAN 統合のためのワークフローと同じです。

1. 米国政府向け Azure アカウントを Cisco SD-WAN Manager に関連付けます。

   米国政府向け Azure アカウントの関連付けの詳細については、「Integrate Your Azure Cloud Account」を参照してください。

2. クラウドグローバル設定を追加および管理します。

   米国政府向け Azure のクラウドグローバル設定の構成の詳細については、「Integrate Your Azure Cloud Account」を参照してください。

3. クラウドゲートウェイを作成および管理します。

   クラウドゲートウェイの作成と管理の詳細については、「Create and Manage Cloud Gateways」を参照してください。

4. ホスト仮想ネットワーク（VNet）を検出し、タグを作成します。

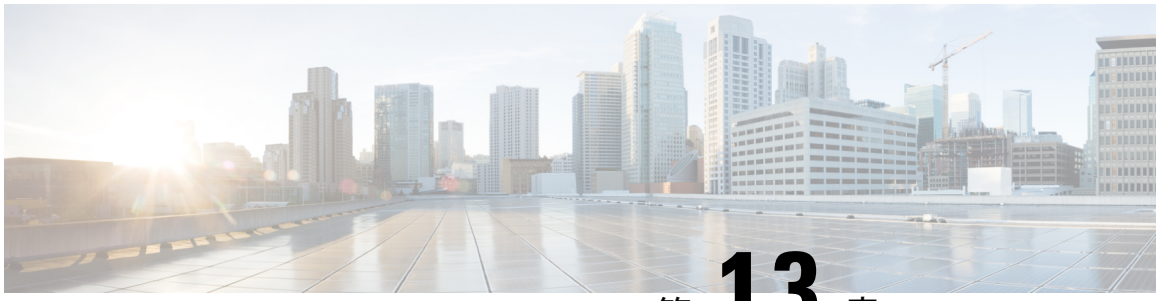
   ホスト VNet の検出とタグの作成の詳細については、「Discover Host VNets and Create Tags」を参照してください。

5. VNet タグとブランチネットワーク VPN をマッピングします。

   VNet とブランチネットワーク VPN のマッピングの詳細については、「Map VNet Tags and Branch Network VPNs」を参照してください。

米国政府向け Azure 統合のモニター

米国政府向け Azure 統合のモニタリングの詳細については、「Monitor Azure Virtual WAN Integration」を参照してください。



第 13 章

Google Cloud の統合

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。

表 *64 :* 機能の履歴

機能名	リリース情報	説明
Google Cloud を使用した Cisco SD-WAN クラウドゲートウェイ	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能により、ブランチサイトは Google Cloud で実行されているワークロードにアクセスできます。また、ブランチサイトは、Google Cloud のグローバルネットワークを介してさまざまなリージョンやサイト間でトラフィックを送受信できます。ソリューションの一環として、クラウドゲートウェイはさまざまなリージョンでインスタンス化されます。クラウドゲートウェイは Cisco Catalyst 8000V インスタンスのペアで構成され、そのインターフェイスは 3 つの異なる VPC にアンカーされます。この機能は、サイトとクラウド間の接続とサイト間の接続をサポートしています。

機能名	リリース情報	説明
Cisco SD-WAN と Google Service Directory の統合と、クラウド状態監査とクラウド リソース インベントリのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	Google Service Directory と Cisco Catalyst SD-WAN ソリューションの統合により、Cisco SD-WAN Manager を使用して Google Cloud 内のアプリケーションを検出できます。検出されたアプリケーションを使用して、Cisco SD-WAN Manager でアプリケーション認識型ルーティングポリシーを定義できます。 Cisco SD-WAN Manager の監査機能が Google Cloud 統合に拡張されました。このオプションを使用して、Google Cloud 内のオブジェクトの状態が Cisco SD-WAN Manager の状態と同期していることを確認します。 Cisco SD-WAN Manager のクラウド リソース インベントリは、クラウドオブジェクト、その識別子、そのようなオブジェクトが作成されたときのタイムスタンプなどの詳細なリストを取得します。
クラウドゲートウェイでの Cisco Catalyst 8000V インスタンスの水平スケーリング	Cisco vManage リリース 20.9.1	この機能により、特定のリージョンのクラウドゲートウェイの一部として 2 ～ 8 つの Cisco Catalyst 8000V インスタンスを展開できます。 以前のリリースでは、クラウドゲートウェイの一部として厳密に 2 つの Cisco Catalyst 8000V インスタンスを展開でき、各インスタンスはリージョンの異なるゾーンに展開されていました。

機能名	リリース情報	説明
クラウドゲートウェイの分離されたサイト間およびサイトとクラウド間の接続設定	Cisco vManage リリース 20.9.1	この機能により、一部のクラウドゲートウェイをサイト間の接続とサイトとクラウド間の接続をサポートするように設定し、他のクラウドゲートウェイをサイトとクラウド間の接続のみをサポートするように設定することができます。この設定の柔軟性は、サイト間接続をまだサポートしていない一部の Google Cloud リージョンで特に役立ちます。 以前のリリースでは、接続タイプはグローバル設定です。すべてのクラウドゲートウェイを、サイト間の接続とサイトとクラウド間の接続をサポートするように設定するか、サイトとクラウドの間の接続のみをサポートするように設定します。

- サポートされるプラットフォームとインスタンス （343 ページ）
- 制限事項と制約事項 （343 ページ）
- Google Cloud を使用した Cisco Catalyst SD-WAN クラウドゲートウェイの概要 （344 ページ）
- Google Service Directory の統合とルックアップ （345 ページ）
- 接続モデル （347 ページ）
- Google Cloud を使用した Cisco Catalyst SD-WAN クラウドゲートウェイの設定 （350 ページ）
- Service Directory のルックアップと検出されたアプリケーションによるトラフィックポリシー （359 ページ）
- 接続のモニター （362 ページ）
- 監査 （362 ページ）
- クラウド リソース インベントリの表示 （364 ページ）

サポートされるプラットフォームとインスタンス

サポートされるプラットフォーム

- Cisco Catalyst 8000V

Google Cloud でサポートされるインスタンス

- N1-standard-8
- N1-standard-4

制限事項と制約事項

- Google Network Connectivity Center の場所のサポートは、Google のサービスによって異なります。サポートされている場所の詳細については、Google Network Connectivity Center の場所に関する Google Cloud のドキュメントを参照してください。
- サービスタイプ（Standard または Premium）の変更は、変更後に作成されたクラウドゲートウェイにのみ適用されます。この変更は、すでに作成されているクラウドゲートウェイには適用されません。
- Google Cloud プロジェクトごとにサポートされるサービスアカウントは 1 つだけです。
- Google リージョンごとにサポートされるクラウドゲートウェイは 1 つだけです。
- 次の処理が進行中の場合は、新しいクラウドゲートウェイを作成できません。
  - クラウドゲートウェイの作成または削除
  - タグの作成またはマッピング
- すでに作成されているクラウドゲートウェイの設定は編集できません。
- 最初のクラウドゲートウェイがすでに作成されている場合、次のクラウドグローバル設定を変更することはできません。
  - IP サブネットプール
  - Cloud Gateway BGP ASN Offset
- ワークロード VPC サブネットに、重複する IP アドレス空間を含めることはできません。
- サイト間接続の場合、VRF と集中管理ポリシーを設定して、ブランチからサイトへのトラフィックが Google Cloud のグローバルネットワークを通過できるようにする必要があります。Google Cloud のグローバル ネットワーク トンネルで障害が発生した場合、トラフィックのドロップが予想されます。

- サイトとクラウド間の接続の場合、1 つのみの VPN を 1 つ以上のタグにマッピングできます。
- VPN が 1 つ以上のタグにマッピングされている場合は、そのようなタグの下にある VPC の合計数が、Google Cloud で指定されている VPC ピアリングの制限を超えないようにしてください。タグ内およびタグ間の接続は VPC ピアリングに依存するため、タグ内およびタグ間のマッピングのために有効になる VPC ピアリング関係の数は、Google Cloud で指定されている VPC ピアリングの制限を超えることはできません。デフォルトの VPC ピアリングの制限は 25 です。この制限を増やすには、Google Cloud サポートにお問い合わせください。Google VPC ピアリングの制限については、Google Cloud のドキュメントを参照してください。
- タグ間のマッピングは常に双方向です。
- サイトとクラウド間の接続のための VPN とタグ間のマッピングの場合、プレフィックスの数は、Google クラウドリージョンによる BGP セッションあたりのカスタム ルート アドバタイズメントの最大数（200）を超えることはできません。
- デフォルトでは、プロジェクトごとに 20 個の Google Cloud Router を使用できます。サイトとクラウド間の接続には、2 つの Google Cloud Router が必要です。サイト間の接続が有効になっている場合は、クラウドゲートウェイごとに 2 つの追加の Google Cloud Router が必要です。そのため、デフォルトの Google Cloud Router のクォータの可用性を使用して、サイト間の機能を無効にしたまま、サイトとクラウド間の接続用に 10 個のクラウドゲートウェイを作成することができます。サイト間の接続も有効にした場合は、最大 5 つのクラウドゲートウェイを作成することができます。より多くのクラウドゲートウェイをインスタンス化するために追加の Google Cloud Router が必要な場合は、Google Cloud ポータルから Google Cloud Router のクォータの増加をリクエストします。
- サイトとクラウド間のトランジット VPC のワークロード VPC から学習されたダイナミックルートは、クラウドゲートウェイの Cisco Catalyst 8000V インスタンスを使用して BGP セッションにアドバタイズされません。そのため、これらのダイナミックルートは Cisco Catalyst SD-WAN エッジデバイスに対して表示されません。
- IPv6 ネットワークアドレスはサポートされていません。
- Network Connectivity Center のトランジット VPC ハブは、Google リージョン内のすべてのクラウドゲートウェイが削除された場合にのみ削除できます。
- トランスポートロケーション（TLOC）の色の **private1** は、サイト間通信にのみ使用されます。そのため、他のインターフェイスには使用しないでください。

Google Cloud を使用した Cisco Catalyst SD-WAN クラウドゲートウェイの概要

この機能により、Cisco SD-WAN Manager の Cloud OnRamp for Multicloud ワークフローを使用して、Cisco Catalyst SD-WAN クラウドゲートウェイで冗長 Cisco Catalyst 8000V Edge ソフト

ウェア（Cisco Catalyst 8000V）インスタンスのペアを設定できます。冗長ルータを使用してクラウドゲートウェイを形成すると、パブリッククラウドに対するパスの復元力が得られます。Cisco Catalyst SD-WAN ファブリックを使用して、この機能により、ブランチおよびデータセンターのデバイスが Google Cloud のアプリケーションおよびサービスと通信できるようになります。また、Google Cloud のグローバルネットワークを使用してサイト間接続を行うこともできます。

Cisco SD-WAN Manager の Cloud OnRamp for Multicloud ワークフローは、Google Cloud での WAN 仮想プライベートクラウド（VPC）と 2 つのトランジット VPC の起動を自動化します。このワークフローは、地理的な Google Cloud リージョン内の既存の VPC も検出します。その後、Cisco SD-WAN Manager で検出された VPC のタグを作成できます。これらのタグは、サービス VPN をパブリック クラウド インフラストラクチャ内の特定の VPC にマッピングするために使用されます。このマッピングにより、Google Cloud 内のワークロード VPC への接続と、Google Cloud のグローバルネットワークを使用したサイト間接続が可能になります。

クラウドゲートウェイでの Cisco Catalyst 8000V インスタンスの水平スケーリング

最小リリース：Cisco vManage リリース 20.9.1

特定のリージョンのクラウドゲートウェイの一部として、最小 2 つ、最大 8 つの Cisco Catalyst 8000V インスタンスを展開できます。3 つ以上のインスタンスを追加する（つまり、インスタンスの数を水平方向にスケールアップする）ことで、スループットを向上させることができます。必要なスループットに基づいて、最小制限の 2 つから最大制限の 8 つのインスタンスの間で、インスタンス数を水平スケーリングできます。

2 つの Cisco Catalyst 8000V インスタンスのみを使用してクラウドゲートウェイを展開する場合、各インスタンスはリージョンの異なるゾーンに展開され、冗長性が提供されます。3 つ以上のインスタンスを持つクラウドゲートウェイを展開する場合、インスタンスは冗長性のために 2 つ以上のゾーンに展開されます。インスタンスは、ゾーン間で均等に分散されない場合があります。

（注） クラウドゲートウェイの一部であるすべての Cisco Catalyst 8000V インスタンスが、同じインスタンスタイプであることを確認します。

関連トピック

クラウドゲートウェイの作成と管理 （355 ページ）

Google Service Directory の統合とルックアップ

Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降では、Google Service Directory が Cisco Catalyst SD-WAN と統合されます。Google Service Directory は、Google Cloud 内のアプリケーションまたはサービスのカタログです。Cisco SD-WAN Manager で Service Directory のルック

アップを有効にすると、この統合により、Cisco SD-WAN Manager は Google Cloud でホストされているアプリケーションを検出し、クラウドで検出されたアプリケーションとして表示することができます。その後、このようなアプリケーションを使用して、アプリケーション認識型ルーティングポリシーを定義できます。

Google Service Directory の作成、および Google Service Directory への新しいサービスの登録については、Google のドキュメントを参照してください。

Google Service Directory のルックアップの仕組み

1. Google Service Directory のルックアップは、Cisco SD-WAN Manager の [Cloud OnRamp for Multicloud] ワークフローの [Cloud Global Settings] ウィンドウと [Associate Cloud Account] ウィンドウから設定します。

   [Service Directory Lookup Capable] として設定されているアカウントでは、ルックアップ結果が 20 分ごとに Cisco SD-WAN Manager タスクバーに表示されます。

2. Cisco SD-WAN Manager が、アカウントに関連付けられている Google リージョンをルックアップして、Google Service Directory 内のアプリケーションを検出します。

3. Cisco SD-WAN Manager が、アカウントに関連付けられている Google リージョン内の名前空間を検出してから、各名前空間内のサービスまたはアプリケーションのリストを検出します。

4. Cisco SD-WAN Manager が、名前空間で検出された各サービスのエンドポイントリストとメタデータを取得します。メタデータまたはサービス注釈には、トラフィックプロファイルなどの属性が含まれます。

   Cisco SD-WAN Manager が、サービス注釈のリストでキーワードの trafficProfile キーを検索します。次に、このキーに対する値が既知の SLA キーワード（data、voice、video、critical、realtime、best-effort、または default）のいずれかであるかどうかを確認します。値が一致しない場合、サービスのトラフィックプロファイルは default として設定されます。キーワードの trafficProfile が見つからない場合、トラフィックプロファイルは default に設定されます。サービスのトラフィックプロファイルは適切な SLA クラスに自動的に変換され、集中管理型ポリシーの作成時に使用できます。

   ルックアップの一環として、Cisco SD-WAN Manager は現在の Google Cloud のマッピング状態に対してエンドポイントリストを検証します。これにより、サービスが Cisco SD-WAN Manager を介して到達可能かどうかを判断します。

5. Cisco SD-WAN Manager を介して到達可能な検出された各サービスが、クラウドで検出されたアプリケーションとしてカタログ化されます。

   クラウドで検出されたアプリケーションの名前は、Google アカウント名、リージョン名、名前空間の名前、および Google Cloud でのサービスまたはアプリケーションの名前を連結して導出されます。名前のサブフィールドはハイフンで結合されます。クラウドで検出されたアプリケーション名の長さには、59 文字の制限があります。名前がこの文字制限を超えると、アプリケーションを追加する際に Cisco SD-AVC で問題が発生する可能性があります。これにより、ポリシーでアプリケーションが正しく使用されない可能性があります。

したがって、Google Cloud でアプリケーションの名前を決定する際には、Cisco SD-WAN Manager でクラウドで検出されたアプリケーションの名前を決定するために使用されるロジックを考慮することを推奨します。

（注） 以前に検出されたサービスまたはアプリケーションが Google Cloud で使用できなくなった場合、Cisco SD-WAN Manager はそのアプリケーションを削除します。このようなアプリケーションがポリシーで使用されている場合、アラームが生成され、ポリシーからアプリケーションを手動で削除する必要があります。削除されたサービス向けのパケットは引き続きクラウドに到達できますが、クラウドに到達した後にドロップされる可能性があります。

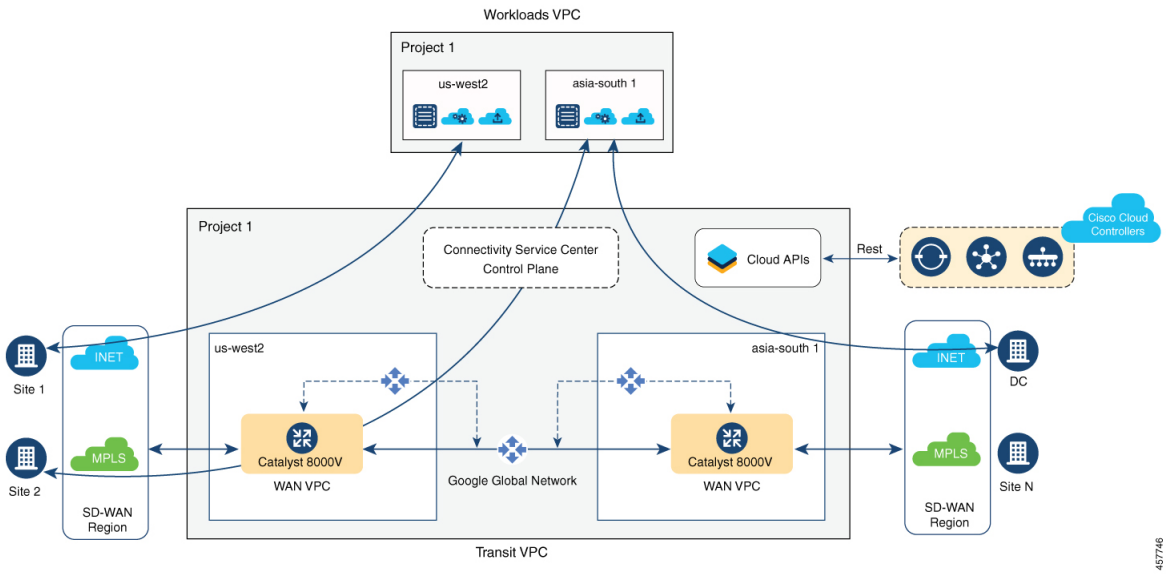
接続モデル

Google Cloud 機能を使用した Cisco Catalyst SD-WAN クラウドゲートウェイでは、次の接続モデルがサポートされています。

サイトから Google Cloud へ

このユースケースは、ブランチサイトが Google Cloud 内の VPC で実行されているアプリケーションにアクセスする必要がある場合に適用されます。このシナリオでは、ブランチサイトは WAN VPC に接続します。WAN VPC は、サイトとクラウド間のトランジット VPC を介してワークロードまたはアプリケーション VPC に接続します。

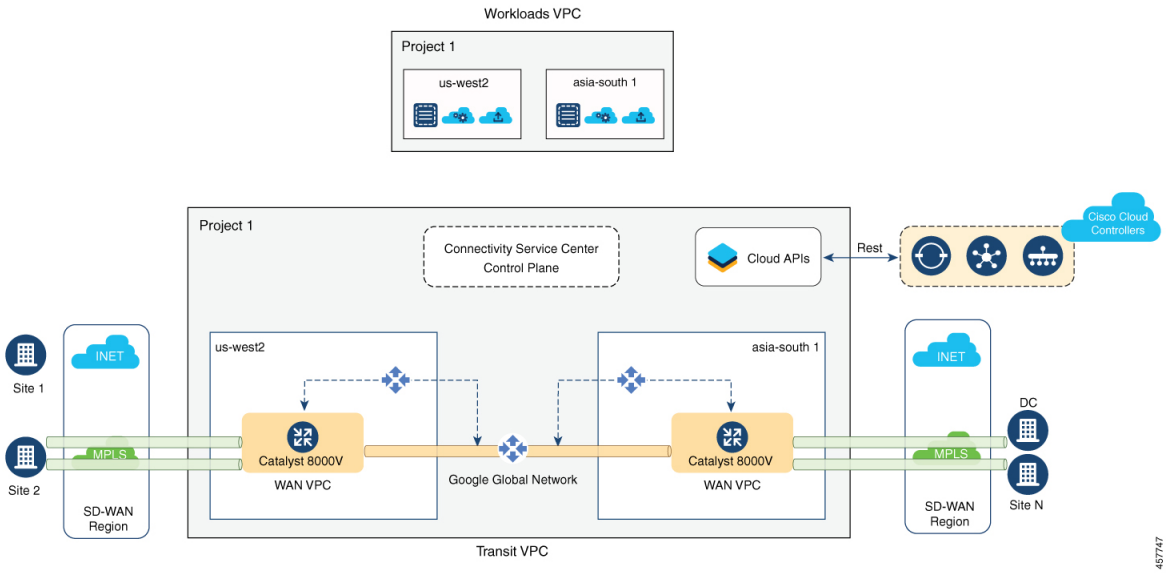
図 *23*：サイトとクラウド間の接続



サイト間

このユースケースは、Google Cloud のグローバルネットワークを使用して、サイト間トランジット VPC を介して異なるリージョンにある 2 つのブランチを接続する場合に適用されます。パブリックインターネットを介してブランチを接続することもできますが、Google Cloud のグローバルネットワークを介して接続することで、トランジットが最適化されます。

図 *24* : サイト間の接続



（注） 特定のクラウドゲートウェイまたは Google Cloud リージョン間でサイト間接続を有効にすることはできません。すべてのクラウドゲートウェイ間で、グローバルにのみ有効にできます。

Cisco vManage リリース 20.9.1 以降では、すべてのクラウドゲートウェイに対してサイト間接続をグローバルに有効にした後に、サイト間通信に参加しないように一部のクラウドゲートウェイを設定することができます（クラウドゲートウェイの分離されたサイト間およびサイトとクラウド間の接続設定 （349 ページ）を参照）。

（注） サイト間接続のユースケースでは、要件に基づいてトラフィックをインテリジェントにステアリングするための制御ポリシーを定義できます。たとえば、重要でないトラフィックフローと重要なトラフィックフローの交換のために、パブリックインターネットと Google Cloud のグローバルネットワークをそれぞれ使用することができます。詳細については、「Centralized Policies」を参照してください。

クラウドゲートウェイの分離されたサイト間およびサイトとクラウド間の接続設定

最小リリース：Cisco vManage リリース 20.9.1

Cisco vManage リリース 20.8.1 以前のリリース：グローバル設定フィールドの [Site-to-site Communication] を使用して、展開内のすべてのクラウドゲートウェイのサイト間接続を有効または無効にします。

- グローバル設定でサイト間接続を無効にした場合は、サイトとクラウド間の接続をサポートしているリージョンでのみクラウドゲートウェイを作成できます。これらのクラウドゲートウェイは、サイトとクラウド間の通信にのみ参加できます。
- グローバル設定でサイト間接続を有効にした場合は、サイト間接続をサポートしているリージョンでのみクラウドゲートウェイを作成できます。これらのクラウドゲートウェイは、サイト間通信とサイトとクラウド間の通信の両方に参加できます。ただし、サイト間接続をサポートしているリージョンは、サイトとクラウド間の接続のみをサポートしているリージョンよりも少なくなります。そのため、サイトとクラウド間の接続を利用するための選択肢は少なくなります。

Cisco vManage 20.9.1 以降：グローバル設定フィールドの [Site-to-site Communication] を使用して、展開内のすべてのクラウドゲートウェイのサイト間接続を有効または無効にします。

- グローバル設定でサイト間接続を有効にした場合、クラウドゲートウェイの作成時に [Involved in Site-to-site communication] フィールドを使用して、クラウドゲートウェイをサイト間通信に参加させるかどうかを選択することができます。
  - クラウドゲートウェイをサイト間通信に参加させない場合は、サイトとクラウド間の接続のみをサポートしている任意のリージョンにゲートウェイを作成することができます。
  - クラウドゲートウェイをサイト間通信に参加させる場合は、サイト間接続をサポートしている任意のリージョンにゲートウェイを作成することができます。クラウドゲートウェイは、サポートされているリージョン内のサイト間通信とサイトとクラウド間の通信の両方に参加できます。

  そのため、サイト間通信とサイトとクラウド間の通信に参加するクラウドゲートウェイと、サイトとクラウド間の通信のみに参加するクラウドゲートウェイを作成することができます。
- グローバル設定でサイト間接続を無効にした場合は、サイトとクラウド間の接続をサポートしているリージョンでのみクラウドゲートウェイを作成できます。サイト間接続がグローバルに無効になっている場合、特定のクラウドゲートウェイでこのタイプの接続を有効にすることはできません。

関連トピック

クラウドグローバル設定の構成 （353 ページ）
クラウドゲートウェイの作成と管理 （355 ページ）

Google Cloud を使用した Cisco Catalyst SD-WAN クラウドゲートウェイの設定

この項では、Cisco SD-WAN Manager を使用して Google Cloud 機能で Cisco Catalyst SD-WAN クラウドゲートウェイを設定する方法について説明します。この項では、この機能を設定するために満たす必要がある前提条件も示します。

設定要件

- Google Cloud のサブスクリプションが必要です。アカウントを Cisco SD-WAN Manager に関連付けるには、Google Cloud アカウントの詳細が必要です。
- Cisco SD-WAN Manager で Google Cloud サービスアカウントを登録できるようにするには、Google Cloud アカウントに少なくとも次のロールが設定されていることを確認してください。
  - サービスアカウントユーザー
  - コンピューティング インスタンス管理（v1）
  - コンピューティング ネットワーク管理
  - コンピューティング パブリック IP 管理
  - コンピューティング セキュリティ管理
  - ハブ & スポーク管理
  - スポーク管理
- 関連するプロジェクトで次の Google Cloud API が有効になっていることを確認します。
  - Compute API
  - Billing API
  - Network Connectivity Center Alpha API
- Cisco SD-WAN Manager がインターネットに接続されていて、Google Cloud と通信してアカウントを認証できることを確認します。
- Cisco SD-WAN Manager に、WAN VPC の作成に自由に使用できる 2 つの Cisco Catalyst 8000V インスタンスがあることを確認します。250 Mbps を超えるスループット要件の場合は、Cisco Catalyst 8000V ライセンスが必要です。
- すべての 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）が Cisco SD-WAN リリース 20.5.1 以降を実行し、Cisco Catalyst 8000V インスタンスが Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降を実行していることを確認します。

- 2 つの Cisco Catalyst 8000V インスタンスがデバイステンプレートにアタッチされていることを確認します。詳細については、「Attach Device to a Device Template」を参照してください。

（注） Cisco Catalyst 8000V を Google Cloud 用の工場出荷時のデフォルトテンプレート（Default_GCP_C8000V_Template_V01）にアタッチしていることを確認します。

- Cisco Catalyst SD-WAN の TCP ポートと UDP ポートが開いていることを確認します。詳細については、「Firewall Ports for Cisco SD-WAN Deployments」を参照してください。

デバイステンプレートへの Cisco Catalyst 8000V インスタンスのアタッチ

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 20.7.1 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Template Type] ドロップダウンリストから [Default] を選択します。

   デフォルトテンプレートのリストが表示されます。
4. Google Cloud 用の工場出荷時のデフォルトテンプレート（Default_GCP C8000V_Template_V01）を選択します。
5. 自由に使用できる 2 つの Cisco Catalyst 8000V インスタンスをデバイステンプレートにアタッチします。詳細については、「Attach Device to a Device Template」を参照してください。

（注） インスタンスをアタッチした後に、**private1** をトランスポートロケーション（TLOC）の色として指定しないでください。**private1** はサイト間通信にのみ使用されるためです。

Cisco SD-WAN Manager と Google Cloud アカウントの関連付け

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。

2. [Setup] で、[Associate Cloud Account] をクリックします。
3. [Cloud Provider] フィールドで、ドロップダウンリストから [Google Cloud] を選択します。
4. 必要な情報を入力します。

フィールド	説明
Cloud Account Name	Google Cloud アカウントの名前を入力します。
[説明（Description）]（任意）	アカウントの説明を入力します。
Use for Cloud Gateway	[Yes] を選択すると、アカウントにクラウドゲートウェイが作成されます。デフォルトでは [No] が選択されています。
[課金 ID（Billing ID）]	（オプション）Google Cloud サービスアカウントに関連付けられている課金 ID を入力します。 （注） 最初のアカウントの関連付けの後にのみ、課金 ID を入力します。 課金 ID を指定すると、自動検証プロセスが実行されます。 （注） このフィールドは、[Use for Cloud Gateway] フィールドで [Yes] オプションを選択した場合にのみ表示されます。
Service Directory Lookup （注） このフィールドは、Cisco vManage リリース 20.6.1 以降でのみ使用できます。	[Enabled] を選択して、Cisco SD-WAN Manager がクラウドアカウントに関連付けられた Google Service Directory 内のサービスまたはアプリケーションを検出できるようにします。デフォルトでは、[Disabled] が選択されています。

フィールド	説明
Private Key ID	[Upload Credential File] をクリックします。このファイルは、Google Cloud コンソールにログインして生成する必要があります。秘密キー ID は、JSON または REST API 形式の場合があります。形式は、キーの生成方法によって異なります。詳細については、Google Cloud のドキュメントを参照してください。 （注） Google Cloud からダウンロードした JSON ファイルに、**universe_domain** という名前のエントリがないことを確認します。

5. [Add] をクリックします。

クラウドグローバル設定の構成

クラウドプロバイダーのクラウドグローバル設定は、[Create Cloud Gateway] ページで設定をカスタマイズしない限り、プロバイダーのクラウドゲートウェイに適用されます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。[Cloud OnRamp for Multicloud] ウィンドウで、[Setup] エリアの [Cloud Global Settings] をクリックします。

（注） [Enable Configuration Group] オプションは、将来の使用のために予約されています。

2. [Cloud Provider] フィールドで、ドロップダウンリストから [Google Cloud] を選択します。
3. グローバル設定を追加するには、[Add] をクリックします。クラウドグローバル設定がすでに構成されている場合は、[Edit] をクリックして変更します。
4. [Software Image] フィールドで、WAN VPC の WAN エッジデバイスのソフトウェアイメージを選択します。これは、プリインストールされた Cisco Catalyst 8000V インスタンスである必要があります。
5. [Instance Size] フィールドで、ドロップダウンリストから、要件に基づいてインスタンスを選択します。
6. [IP Subnet Pool] フィールドで、Google Cloud 内の SD-WAN クラウドゲートウェイの IP サブネットプールを指定します。このサブネットプールには、/16 ～ /21 の範囲内のプレフィックスが必要です。

7. [Cloud Gateway BGP ASN Offset] フィールドで、BGP ピアリング用クラウドゲートウェイの自律システム番号（ASN）を指定します。これは、クラウドゲートウェイと Google Cloud Router の ASN 割り当ての開始オフセットです。オフセットから開始して、10 個の ASN 値がクラウドゲートウェイへの割り当て用に予約されています。

注目　このオフセット値は、クラウドゲートウェイの作成後に変更できません。

8. [Intra Tag Communication] に対して、[Enabled] を選択します。これにより、同じタグを持つ VPC が相互に通信できるようになります。

9. Google グローバルネットワークを使用したサイト間トランジット接続では、[Site-to-Site Communication] に対して [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。

10. [Site-to-Site Tunnel Encapsulation Type] フィールドで、ドロップダウンリストからカプセル化を選択します。

11. Cisco SD-WAN Manager がこの Google アカウントに関連付けられた Google Service Directory 内のアプリケーションを検出できるようにするには、[Service Directory Lookup Capable] に対して [Enabled] を選択します。 デフォルトでは [Disabled] が選択されています。

（注）　このフィールドは、Cisco vManage リリース 20.6.1 以降でのみ使用できます。

12. [Service Directory Poll Timer Value] フィールドの値は、デフォルトでは 20 分に設定されています。

    このフィールドは、Cisco vManage リリース 20.6.1 以降でのみ使用できます。

13. [Network Service Tier] フィールドで、いずれかの Google Cloud サービスパッケージを選択します。

    - [PREMIUM]：Google グローバルネットワークを使用して、高パフォーマンスのネットワーク エクスペリエンスを提供します。
    - [STANDARD]：ネットワークコストを制御できます。

14. [Save] または [Update] をクリックします。

ホスト VPC の検出とタグの作成

Google Cloud アカウントを Cisco SD-WAN Manager に関連付けると、Google Cloud アカウントに関連付けられたリージョンでホスト VPC を検出できます。このワークフローでは、VPC レベルでのクラウド インフラストラクチャが示されます。検出された VPC の新しいタグを作成したり、既存のタグを変更または削除したりすることができます。タグは、VPC と Cisco Catalyst SD-WAN ブランチ VPN 間の接続を管理するために使用されます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Discover] ワークフローで、[Host Private Networks] をクリックします。
3. [Cloud Provider] フィールドで、[Google Cloud] を選択します。

   検出されたホスト VPC のリストが、[Cloud Region]、[Account Name]、[Host VPC Name]、[Host VPC Tag]、[Account ID]、および [Host VPC ID] 列があるテーブルに表示されます。
4. [Tag Actions] ドロップダウンリストをクリックして、次のいずれかを実行します。
   - [Add Tag]：VPC または VPC のグループのタグを作成します。
   - [Edit Tag]：選択した VPC の既存のタグを変更します。
   - [Delete Tag]：選択した VPC のタグを削除します。

クラウドゲートウェイの作成と管理

最初のクラウドゲートウェイが作成されると、WAN トランジット VPC、サイト間のトランジット VPC、およびサイトとクラウド間のトランジット VPC の、3 つの予約済み VPC がインスタンス化されます。クラウドゲートウェイの一部としてインスタンス化される Cisco Catalyst 8000V インスタンスが、VPC にアンカーされます。

この手順では、Google Cloud で Cisco Catalyst SD-WAN クラウドゲートウェイを作成する方法について説明します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Manage] で、[Create Cloud Gateway] をクリックします。
3. [Cloud Provider] フィールドで、ドロップダウンリストから [Google Cloud] を選択します。
4. [Cloud Gateway Name] フィールドに、クラウドゲートウェイの名前を入力します。

（注） 名前が小文字であることを確認してください。リソースの名の指定およびリソース名の表記規則については、Google Cloud のドキュメントを参照してください。

5. （任意）[Description] に説明を入力します。
6. [Account Name] フィールドで、ドロップダウンリストから Google Cloud アカウント名を選択します。
7. [Region] フィールドで、ドロップダウンリストから Google リージョンを選択します。

8. （最小リリース：Cisco vManage リリース 20.9.1）[Involved in Site-to-site communication]：クラウドゲートウェイがサイト間通信に参加する場合は、[Yes] をクリックします。クラウドゲートウェイがサイト間通信に参加しない場合は、[No] をクリックします。

（注） このフィールドは、グローバル設定で [Site-to-site Communication] が有効になっている場合にのみ、設定に対して有効になります。グローバル設定で [Site-to-site Communication] が無効になっている場合、このフィールドはグレー表示されます。

9. （最小リリース：Cisco vManage リリース 20.10.1）[Site Name] ドロップダウンリストから、クラウドゲートウェイを作成するサイトを選択します。

10. （オプション）[Settings] セクションで、必要な情報を入力します。

（注） 以下のフィールドを使用して、クラウドのグローバル設定または個々のクラウドゲートウェイの設定のカスタマイズを使用することができます。

1. [Software Image] フィールドで、サイトを Google Cloud に接続するために WAN VPC でインスタンス化する WAN エッジデバイスのソフトウェアイメージを選択します。
2. [Instance Size] フィールドで、要件に基づいて Cisco Catalyst 8000V のインスタンスサイズを選択します。
3. [IP Subnet Pool] フィールドで、Google Cloud WAN VPC に使用する IP サブネットプールを指定します。このサブネットプールには、/16 ～ /21 の範囲内のプレフィックスが必要です。

（注） IP サブネットプールは、[Cloud Global Settings] で指定した IP サブネットプールと重複することはできません。

4. [Network Service Tier] フィールドで、ドロップダウンリストからいずれかの Google Cloud ネットワーク サービス パッケージを選択します。
   - [PREMIUM]：Google Cloud グローバルネットワークを使用して、高パフォーマンスのネットワーク エクスペリエンスを提供します。
   - [STANDARD]：ネットワークコストを制御できます。

11. [UUID (specify 2)]：

Cisco vManage リリース 20.8.1 以前：ドロップダウンリストから 2 つの Cisco Catalyst 8000V ライセンスを選択します。

Cisco vManage リリース 20.9.1 以降：ドロップダウンリストから最小で 2 つ、最大で 8 つの Cisco Catalyst 8000V ライセンスを選択します。

（注）
- クラウドゲートウェイ内のすべての Cisco Catalyst 8000v インスタンスは、同じインスタンスタイプである必要があります。垂直スケーリングはサポートされていません。
- Cisco vManage リリース 20.10.1 以降では、[Site Name] ドロップダウンリストからサイトを選択すると、UUID が自動的に入力されます。

デフォルトの Google Cloud テンプレートにアタッチした UUID を選択します。

12. （最小リリース：Cisco vManage リリース 20.10.1）[Multi-Region Fabric Settings] エリアの [MRF Role] で、[Border] または [Edge] を選択します。

このオプションは、マルチリージョンファブリックが有効になっている場合にのみ使用できます。

13. [Add] をクリックします。

VPC タグとブランチネットワーク VPN のマッピング

VPC から VPN へのマッピングを有効にするには、1 つまたは複数の Google リージョンで一連の VPC を検出し、タグを作成します。次に、同じタグを使用して VPC をマッピングするサービス VPN を選択します。

マッピングと接続の仕組み

- 明示的に接続を作成する必要はありません。VPC タグに基づいて、クラウドゲートウェイが特定のリージョンでインスタンス化されたとき、またはタグ付け操作が行われたときに、接続が自動的に確立されます。
- タグ間およびタグ内マッピングの接続インテントは、さまざまなクラウドリージョンでのクラウドゲートウェイの存在に関係なく定義できます。インテントは保持され、新しいクラウドゲートウェイまたはマッピングの変更が検出されたときにマッピングが実現されます。
- クラウドゲートウェイが異なるリージョンでインスタンス化されると、マッピングインテントがそれらのリージョンで自動的に実現されます。
- タグ間およびタグ内マッピングは VPC ピアリングに基づいていて、双方向接続のみを自動的に有効にします。
- 1 つのサービス VPN のみを、1 つ以上のタグにマッピングできます。
- 一度に実行できるクラウド操作（タグ付け、マッピング、クラウドゲートウェイの作成または削除など）は 1 つだけです。1 つの操作が実行されていると、他の操作はロックされます。

- すべてのクラウド操作には時間制限があります。たとえば、マッピング操作は 60 分後にタイムアウトします。タイムアウト時に、操作は失敗として宣言されます。タイムアウト値は設定できません。
- 新しいマッピングインテントの実現中は、[Intent Management] ページは自動更新されません。

正常にマッピングするための前提条件

- （タグの一部として）マッピングに関係する VPC には、少なくとも 1 つのサブネットが必要です。
- マッピングは VPC ピアリングに依存しています。ピアリング VPC のサブネットは、RFC1918 に準拠している必要があります。
- VPC では Classless Interdomain Routing（CIDR）アドレスは重複できません。CIDR アドレスが重複していると、マッピングが失敗します。

接続の表示または編集

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Intent Management] で、[Cloud Connectivity] をクリックします。
3. [Cloud Provider] フィールドで、ドロップダウンリストから [Google Cloud] を選択します。

   ウィンドウに、送信元 VPN とその宛先を示す接続マトリックスが表示されます。次の凡例で、インテントのステータスに関する情報が提供されます。

   - 青：インテント定義済み
   - 緑：インテント実現済み
   - 赤：インテント実現済み（エラーあり）

   マトリックス内のいずれかのセルをクリックすると、より詳細なステータス情報が表示されます。
4. [Edit] をクリックして、新しいインテントを定義または記録します。
5. VPN、およびそれに関連付けられている VPC タグに対応するセルを選択し、[Save] をクリックします。

Service Directory のルックアップと検出されたアプリケーションによるトラフィックポリシー

Cisco SD-WAN Manager のトラフィックポリシーで Google Cloud アカウントのサービスまたはアプリケーションを使用するには、まず Cisco SD-WAN Manager で Service Directory のルックアップを有効にしてから、このルックアップによって検出されたアプリケーションを使用してトラフィックポリシーを作成する必要があります。

Service Directory のルックアップの有効化

Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降では、Google Service Directory が Cisco Catalyst SD-WAN ソリューションに統合されました。この統合により、Cisco SD-WAN Manager は、Cisco SD-WAN Manager に関連付けられている Google Cloud アカウントの一部である Google Service Directory のルックアップを実行できます。Cisco SD-WAN Manager は、ルーティングポリシーの定義に使用できるカスタムアプリケーションとして、Service Directory 内のアプリケーションまたはサービスを表示します。

Cisco SD-WAN Manager で Google Service Directory を検索できるようにするには、Cisco SD-WAN Manager で Service Directory のルックアップを有効にする必要があります。

クラウドで検出されたカスタムアプリケーションの命名

Service Directory のルックアップは、Google Cloud で定義したサービスを Google Cloud にクエリします。Cisco SD-WAN Manager により、このサービス用に Cisco Catalyst SD-WAN 内にカスタムアプリケーションが自動的に作成されます。カスタムアプリケーションの名前を作成するために、Cisco SD-WAN Manager は Google Cloud で定義されているフィールド（Google Cloud のアカウント名、Google Cloud のリージョン名、サービス名、および名前空間）の組み合わせを使用します。クラウドで検出されたカスタムアプリケーションの名前の最大長は、SD-AVC コンポーネントの制限により、59 文字です。

Cisco SD-WAN Manager で、カスタムアプリケーションが表示されるアプリケーション リストページを表示できます。Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Policies]** を選択してから、[Custom Options] をクリックし、[Lists] を選択します。Cloud OnRamp for Multicloud によって検出されたサービスから Cisco SD-WAN Manager が生成したカスタムアプリケーションを表示するには、[Cloud Discovered] をクリックします。

- Cisco SD-WAN Manager 20.6.x は、59 文字の制限を次のように処理します。Cisco SD-WAN Manager が上記の 4 つのフィールドを使用してカスタムアプリケーションの名前を作成する場合、名前が 59 文字を超えると、名前が切り捨てられます。名前が切り捨てられると、名前の競合が発生する可能性があります。

  アカウント名とリージョン名の長さは可変であるため、59 文字の制限内でサービス名と名前空間に使用できる残りの文字数を予測することは困難です。

  文字数制限を超えないように、Google Cloud でサービスを定義する際は、サービス名と名前空間名に短い名前を使用することを推奨します。これらの名前で使用可能な長さは、

Google Cloud のアカウント名と Google Cloud のリージョン名を組み合わせた長さによって異なります。

- 次の例では、アカウント名とリージョン名が長いため、短いサービス名と名前空間名が必要です。

  アカウント名：gcp-organization-sw-dev
  リージョン名：australia-southeast1
  サービス名：serv1
  名前空間名：nspace1

- 次の例では、アカウント名とリージョン名が短いため、長いサービス名と名前空間名を使用できます。

  アカウント名：cisco
  リージョン名：us-west
  サービス名：service-xyz
  名前空間名：dev-team

- Cisco SD-WAN Manager 20.7.x 以降では、Google Cloud で定義されたサービスの名前空間とサービス名のフィールドに、より長くわかりやすい名前を使用できます。必要に応じて、最大 59 文字の制限を満たすために、Cisco SD-WAN Manager はサービス名の一部を切り捨てることがあります。

  Cisco SD-WAN Manager は、Google Cloud のアカウント名に 12 文字の制限、Google Cloud のリージョン名に 23 文字の制限、名前空間に 8 文字の制限を適用します。カスタムアプリケーション名では、区切り文字（-）に 3 文字が使用されます。サービス名が切り捨てられずに 59 文字の制限内に収まるようにするには、Google Cloud でサービスのサービス名を指定するときに、最大 13 文字を使用します。より長い名前を使用し、これらのフィールドの組み合わせが 59 文字を超える場合、Cisco SD-WAN Manager は名前を切り捨てます。名前の切り捨てによって、以前に定義されたカスタムアプリケーションとの名前の競合が発生した場合、Cisco SD-WAN Manager はアプリケーション リスト ページにアラームを表示します（アプリケーション リスト ページを開くための手順は上に示されています）。

はじめる前に

Cisco SD-WAN Manager で SD-AVC が有効になっていることを確認します。

- Cisco SD-WAN Manager で SD-AVC を有効にします。

  1. Cisco SD-WAN Manager のメニューから、**[Administration]** > **[Cluster Management]** の順に選択します。
  2. 目的の Cisco SD-WAN Manager インスタンスについて、[...] をクリックし、[Edit] を選択して、[Enable SD-AVC] チェックボックスをオンにします。

- Google Cloud アカウントで Service Directory API が有効になっていることを確認します。

Service Directory のルックアップの有効化

1. **Cloud OnRamp for Multicloud** ワークフローの [Associate Cloud Account] ウィンドウから [Service Directory Lookup] を有効にします。

   詳細については、この章の「Cisco SD-WAN Manager と Google Cloud アカウントの関連付け」のトピックを参照してください。

2. [Cloud Global Settings] で、Cisco SD-WAN Manager に関連付けられている Google アカウントを [Service Directory Lookup Capable] として有効にして、[Service Directory Poll Timer Value] を設定します。

   詳細については、「クラウドグローバル設定の構成」を参照してください。

クラウドで検出されたアプリケーションを使用したトラフィックポリシーの作成

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [カスタムオプション（Custom Options）] をクリックします。
3. [Centralized Policy] で、[Lists] をクリックします。

   [Policies] の下の [Application] セクションにリダイレクトされます。
4. [Cloud Discovered] をクリックします。

   Google Service Directory のルックアップによって検出されたアプリケーションのリストが表示されます。
5. [Map Traffic Profiles] をクリックします。表示されるダイアログボックスで、検出されたサービスのトラフィックプロファイルを設定または変更できます。
6. トラフィックプロファイルごとに、[vManage SLA Classes] をクリックし、アプリケーションをマッピングする SLA クラスを選択します。
7. [Save] をクリックします。
8. 次に、クラウドで検出されたアプリケーションを含むアプリケーションリストを作成します。詳細については、「Configure Application List」を参照してください。
9. 検出されたアプリケーションを使用してトラフィックポリシーを作成するには、**[Custom Options]** > **[Traffic Policy]** をクリックしてから、[Add Policy] をクリックします。

   クラウドで検出されたアプリケーションのアプリケーションリストでトラフィックルールを設定するには、「Application-Aware Routing」の「Configure Traffic Rules」を参照してください。

接続のモニター

新しいクラウドゲートウェイを作成するときに、クラウドゲートウェイ内でプロビジョニングされた Cisco Catalyst 8000V インスタンスの起動と到達可能性を確認できます。

オプション 1

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Cloud] の下の [Network Snapshot] では、さまざまなクラウドプロバイダーのクラウドゲートウェイ、ホスト VPC、および WAN エッジデバイスの概要が表示されます。

   WANエッジデバイスの横にある上向きの矢印は、稼働しているデバイスの数を示します。矢印をクリックして、デバイスの詳細を表示します。

オプション 2

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Workflows] セクションで、[Intent Management] の下の [Cloud Connectivity] をクリックします。
3. [Cloud Provider] フィールドで、ドロップダウンリストから [Google Cloud] を選択します。
4. ページ上の任意のセルをクリックすると、VPN と VPC タグの接続ステータスが表示されます。

監査

Cisco vManage リリース 20.6.1 以降では、[Cloud OnRamp for Multicloud] ワークフローの [Audit] オプションが Google Cloud に対して有効になっています。このオプションを使用して、Google Cloud の状態が Cisco SD-WAN Manager の状態と同期しているかどうかを確認します。監査の一環として、クラウドの状態が Cisco SD-WAN Manager の状態と同期していないと識別された場合、Cisco SD-WAN Manager は自動的に問題の解決を試行し、状態を同等にしようとします。

監査メカニズムの一部として、クラウドオブジェクトの存在、それらの相互関係、およびそれらの状態はすべて、Cisco SD-WAN Manager で定義された接続インテントに照らして検証されます。不一致が特定された場合は、Cisco SD-WAN Manager が修正処置を行います。

監査オプションによって識別されるエラーのタイプ

回復可能なエラー

これらは、Cisco SD-WAN Manager がアクションを実行して解決できるエラーです。Cisco SD-WAN Manager は、Cisco SD-WAN Manager によって作成されたオブジェクトのエラーを解

決できます。監査オプションでは、次のシナリオで不足しているリソースを再作成することにより、次のエラーを自動的に検出して解決しようとします。

- ハブまたはスポークの削除
- Google Cloud Router の削除（プライマリ、セカンダリ、またはその両方）
- Cisco SD-WAN Manager の VPN にマッピングされた VPC のサイトとクラウド間のピアリングの削除
- Cisco SD-WAN Manager の他の VPC にマッピングされた VPC の VPC ピアリングの削除
- カスタムルートの欠落
- BGP セッションの欠落
- 古い BGP セッション

回復不能なエラー

これらは、Cisco SD-WAN Manager では解決できないエラーであり、手動による介入が必要です。

- クラウドゲートウェイまたはそのコンポーネントのいずれかの削除
- CIDR が重複しているホスト VPC の問題
- サイト間の VPC の問題
- サイトとクラウド間の VPC の問題
- WAN VPC の問題

定期監査

Cisco SD-WAN Manager は、2 時間ごとに自動監査をトリガーします。この自動監査はバックグラウンドで実行され、回復可能な問題を解決します。

Cisco SD-WAN Manager にはこの監査の結果が表示されませんが、定期的な監査に関連するイベントが記録されます。

オンデマンド監査

これは、ユーザーが起動する監査です。オンデマンド監査を開始するには、次の手順に従います。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Intent Management] エリアで、[Audit] をクリックします。
3. [Cloud Provider] フィールドで、[Google Cloud] を選択します。

このウィンドウには、さまざまな Google Cloud オブジェクトのステータスが表示されます。

4. いずれかのオブジェクトのステータスが [Out of Sync] と表示されている場合は、[Fix Sync issues] をクリックします。このオプションにより、回復可能なエラーが解決されます。

（注） [Fix Sync Issues] をクリックして、問題を修正できない場合は、同じ状態を示すタスクの更新が表示されます。回復不能なエラーには、手動による介入が必要です。

クラウド リソース インベントリの表示

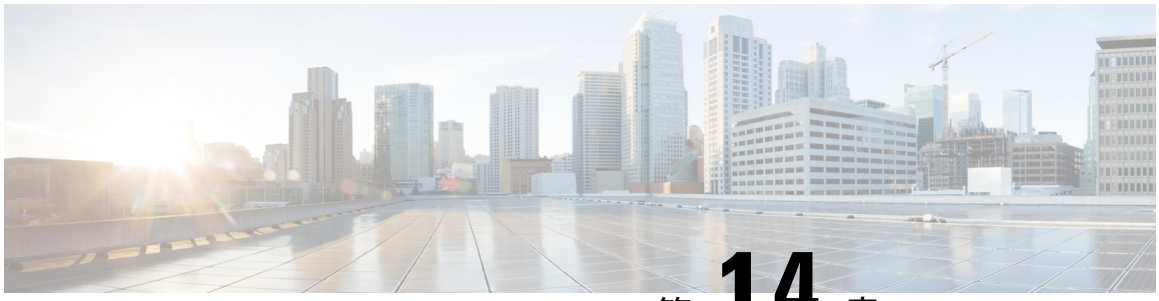
Cisco vManage リリース 20.6.1 以降では、Google Cloud 用に有効にされた Cisco SD-WAN Manager で [Cloud Resource Inventory] オプションを使用できます。Cisco SD-WAN Manager に関連付けられている Google Cloud アカウントのクラウドオブジェクトとその識別子の詳細を表示するには、このオプションを使用します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Manage] の下の [Gateway Management] をクリックします。

   既存のクラウドゲートウェイが表示されます。
3. 目的のクラウドゲートウェイで、[…] をクリックし、[Cloud Resource Inventory] を選択します。

[Cloud Resource Inventory] オプションを使用すると、選択したクラウドゲートウェイの次の情報を取得します。

- VPC：WAN、サイト間、およびサイトとクラウド間の VPC。
- VPC サブネット：Google Cloud アカウントに関連付けられている各 Google Cloud リージョンの WAN、サイト間、およびサイトとクラウド間。
- VM：各 Google Cloud リージョン内の Cisco Catalyst 8000V インスタンスのペア。
- Google Cloud Router：各リージョンのそれぞれのサイトとクラウド間およびサイト間の Google Cloud Router のペア。
- ハブ：それぞれのサイト間およびサイトとクラウド間の Google グローバルネットワークハブのインスタンス。
- スポーク：サイト間およびサイトとクラウド間のハブに接続されている各リージョンからのスポークのペア。



第 14 章

マルチクラウドサービスのモニタリングのための Cisco Catalyst SD-WAN Manager のサポート

（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。

表 *65 :* 機能の履歴（表）

機能名	リリース情報	リリース情報
マルチクラウドサービスのモニタリングのための Cisco SD-WAN Manager のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能により、Cisco SD-WAN Manager UI を使用してマルチクラウドネットワークをモニターできます。

機能名	リリース情報	リリース情報
Cisco SD-WAN Manager でのリアルタイムデータのマルチクラウドサービスのモニタリング	Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a Cisco vManage リリース 20.10.1	この機能により、すべてのクラウドおよびインターコネクト接続のモニタリングダッシュボードが拡張されます。また、この機能により、好みに合わせて表示するダッシュレットを自由に指定したり、並べ替えたりできます。

- Cisco SD-WAN Manager を使用したマルチクラウドサービスのモニタリングの制約事項（366 ページ）
- Cisco SD-WAN Manager を使用したマルチクラウドサービスのモニタリングに関する情報（366 ページ）
- 地理的ビュー （367 ページ）
- クラウドとインターコネクト ダッシュボード （368 ページ）
- クラウドゲートウェイのサマリービュー （369 ページ）
- インターコネクト ゲートウェイのサマリービュー （370 ページ）

Cisco SD-WAN Manager を使用したマルチクラウドサービスのモニタリングの制約事項

- この機能は、Cisco vManage リリース 20.7.1 以降でマルチテナント モードの動作をサポートしています。Cisco vManage リリース 20.6.x では、この機能はマルチテナントモードの動作をサポートしていません。
- この機能は、Cisco vManage リリース 20.7.1 以降でインターコネクトタイプ Equinix をサポートしています。Cisco vManage リリース 20.6.x では、この機能はインターコネクトタイプ Equinix をサポートしていません。
- ソリューションがブランチ接続 AWS の場合、地理的位置とトラフィック統計は利用できません。

Cisco SD-WAN Manager を使用したマルチクラウドサービスのモニタリングに関する情報

この機能により、Cisco SD-WAN Manager を使用して、さまざまなクラウドリソースへの Cisco SD-WAN の接続をモニターすることができます。この機能により、UI に次のビューが導入されます。これらのビューを使用して、エッジデバイスのおおよその地理的位置、クラウドタイ

プ、およびさまざまなクラウドプロバイダーのクラウドサイトとアカウントに関する情報を視覚的にモニターすることができます。

- 地理的ビュー
- クラウドとインターコネクト ダッシュボード
- クラウドゲートウェイのサマリービュー
- インターコネクト ゲートウェイのサマリービュー

デフォルトでは、[Monitor Overview] ダッシュボードには、Cisco SD-WAN オーバーレイネットワークのさまざまなコンポーネントとサービスをモニタリングする際に役立つすべてのダッシュレットが表示されます。カスタマイズ可能なダッシュボード機能を使用すると、次のことができます。

- ダッシュレットの追加
- ダッシュレットの削除
- ダッシュレットの再配置
- デフォルト設定の復元

（注） Cisco vManage リリース 20.10.1 以降では、クラウドまたはインターコネクトのプロバイダーアカウントが Cisco SD-WAN Manager に関連付けられるとすぐに、[Monitor Overview] ダッシュボードのマルチクラウド ダッシュレットが表示されます。

地理的ビュー

地理的ビューには、マルチクラウド展開における Cisco Catalyst 8000V インスタンスのおおよその地理的位置が表示されます。おおよその位置は、クラウドおよびインターコネクトタイプから公開されている情報に基づきます。位置は、Google Cloud、AWS、Azure クラウドプラットフォームに加え、ソフトウェア定義型のクラウドインターコネクトに提供されます。

マルチクラウド Cisco Catalyst 8000V インスタンスの地理的位置を表示するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから**[Monitor]** > **[Geography]**の順に選択します。
2. マップで、Cisco Catalyst 8000V インスタンスをクリックして、そのインスタンスのクラウドまたはインターコネクトのタイプ、サイト ID、およびシステム IP を表示します。

クラウドとインターコネクト ダッシュボード

クラウドとインターコネクトダッシュボードには、クラウドインスタンスおよびソフトウェア定義型のクラウドインターコネクトごとに個別のパネルが表示されます。円グラフは、クラウドまたはソフトウェア定義型のクラウドインターコネクトに接続されているサイトとその到達可能性を示します。サイトは、クラウドへの BFD セッションまたはインターコネクト Cisco Catalyst 8000V を持つ特定のサイト ID の Cisco Catalyst SD-WAN デバイスです。各クラウドまたはインターコネクトのパネルには、次の情報も表示されます。

- Cisco Catalyst SD-WAN エッジデバイスの数
- 登録済みのマルチクラウドアカウント
- ゲートウェイ
- タグ
- ホスト VPC
- トンネル
- VPN 接続

クラウドとインターコネクトダッシュボードで情報を表示するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Monitor]** > **[Multicloud]** を選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco SD-WAN Manager のメニューから、**[Dashboard]** > **[Multicloud]** を選択します。

2. Cisco Catalyst SD-WAN エッジデバイスに関する情報を表示するには、**WAN エッジ**の数をクリックして、Cisco Catalyst SD-WAN エッジデバイスに関する情報を表示します。表示されるウィンドウには、正常性（CPU、メモリ、ハードウェアの状態の集計）、BFD ステータス、設定ステータス、到達可能性、ホスト名、システム IP、シャーシ番号、クラウドまたはインターコネクト ゲートウェイ名、デバイスモデルおよびデバイスのバージョンが表示されます。

   - **[Monitor]** > **[Multicloud]** で、クラウドまたはインターコネクトエッジデバイスのゼロ以外の数をクリックすると、**[Monitor]** > **[Devices]** ページが開きます。[Devices] ウィンドウの左側のペインにある [Filter] 条件では、使用可能なオプションから表示するフィールドを選択できます。
   - クラウドまたはソフトウェア定義型のクラウド インターコネクト ゲートウェイ名、リージョン、アカウント名、正常性、およびクラウドタイプに固有のすべてのゲートウェイの説明を表示するには、クラウドまたはインターコネクト**ゲートウェイ**のゼロ以外の数をクリックします。
   - クラウドまたはインターコネクト エッジ デバイスの詳細を表示するには、クラウドまたはインターコネクト**エッジ**のゼロ以外の数をクリックします。

- 接続されたサイトの正常性、BFD ステータス、およびサイト ID を表示するには、**接続されたサイト**のゼロ以外の数をクリックします。

クラウドゲートウェイのサマリービュー

（注） ソリューションがブランチ接続 AWS の場合、地理的位置とトラフィック統計は利用できません。

クラウドゲートウェイのサマリービューには、次の情報が表示されます。

- クラウドタイプ
- アカウント名
- リージョン
- クラウド ゲートウェイ デバイス
- 関連するブランチデバイス：クラウド ゲートウェイ デバイスとの BFD セッションが設定されているブランチデバイス。
- 関連付けられた VPC および vNET：クラウドゲートウェイと同じリージョンに属する VPN にマッピングされている VPC および vNET。
- トラフィック統計：クラウド ゲートウェイ デバイスからワークロード VPC へのトンネル統計。デバイスを選択すると、次のトラフィック統計と、リストする期間の表示を選択できます。
  - Kbps
  - パケット
  - Octets
  - Errors
  - Drops
  - Pps

  デバイスが選択されていない場合は、クラウドゲートウェイ内のすべてのデバイスの統計の集計が表示されます。

クラウドゲートウェイのサマリービューに移動するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Cloud] を選択します。

3. クラウドゲートウェイのサマリーテーブルで、詳細を表示するクラウドゲートウェイの名前をクリックします。このページでは、接続されたサイトに関する詳細を表示することもできます。

インターコネクト ゲートウェイのサマリービュー

インターコネクト ゲートウェイのサマリービューには、次の情報が表示されます。

- Cisco Catalyst SD-WAN エッジデバイスのタイプ
- アカウント名
- リージョン
- インターコネクト ゲートウェイ デバイス
- 関連するブランチデバイス
- インターコネクト接続

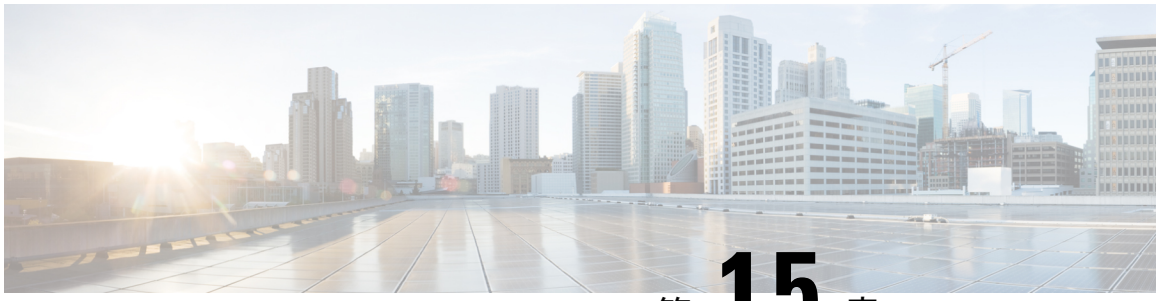
インターコネクト ゲートウェイのサマリービューに移動するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] を選択します。
3. 詳細を表示するインターコネクト ゲートウェイ名をクリックします。

第 III 部

Cloud OnRamp for Multicloud：Cisco Catalyst SD-WAN Cloud Interconnect

- Cloud OnRamp for Multicloud：Cisco Catalyst SD-WAN Cloud Interconnect （373 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Megaport のライセンス管理 （375 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Megaport （393 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix （485 ページ）



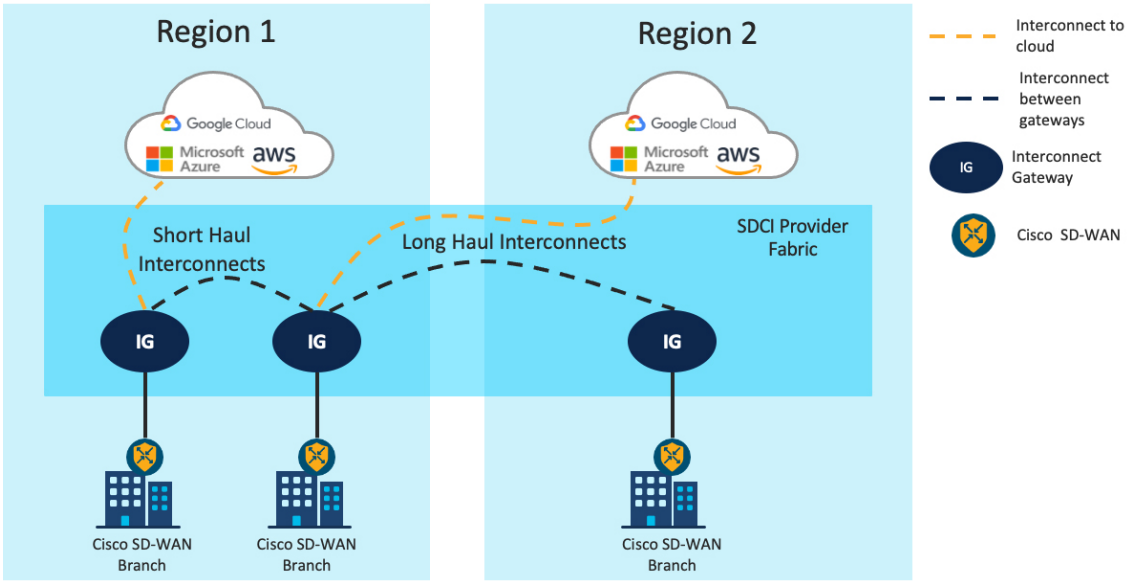
第 15 章

Cloud OnRamp for Multicloud：Cisco Catalyst SD-WAN Cloud Interconnect

（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。

Cisco IOS XE リリース 17.5 および Cisco vManage リリース 20.5 以降では、ソフトウェア定義型のクラウドインターコネクト（SDCI）プロバイダーのファブリック内で Cisco Catalyst SD-WAN エッジデバイスをインスタンス化し、SD-WAN ファブリックを介してこのエッジデバイスにブランチの場所を接続することができます。このエッジデバイスから、SDCI プロバイダーファブリック内の他の Cisco Catalyst SD-WAN エッジデバイスや、パブリッククラウドまたはプライベートクラウドへのソフトウェア定義型のインターコネクトを作成することができます。そのため、SDCI プロバイダーファブリック内のエッジデバイスは、インターコネクト ゲートウェイとして機能します。

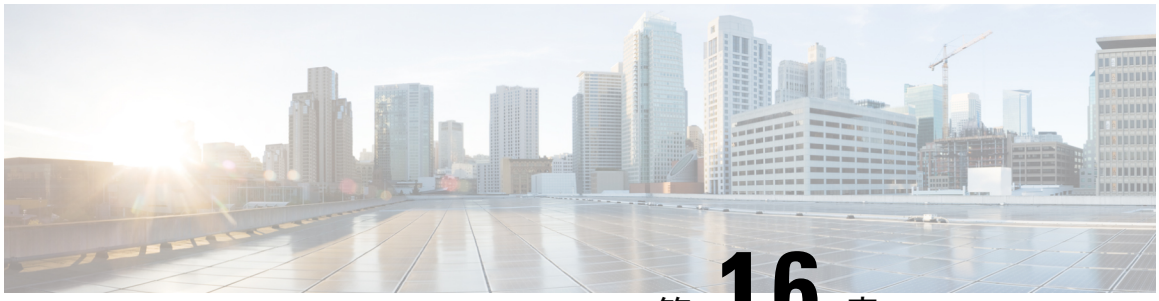
図 *25 : SD-WAN* ブランチ間と *SD-WAN* ブランチとクラウド間をリンクする *Cisco Catalyst SD-WAN Cloud Interconnect*



ソフトウェア定義型のインターコネクトは、ブランチの場所間をリンクするか、ブランチの場所とクラウド サービス プロバイダー間をリンクします。インターコネクトは、SLA によって定められたパフォーマンス帯域幅と 99.999% の可用性を備えた、専用のプライベートレイヤ 2 接続を提供します。短距離インターコネクトは、同じリージョン内のブランチの場所間、またはブランチの場所と Cloud onRamp 間をリンクします。長距離インターコネクトは、異なるリージョンのブランチの場所間、またはあるリージョンのブランチの場所と別のリージョンの Cloud onRamp 間をリンクします。

Cisco SD-WAN Manager は、SDCI ファブリックでエッジデバイスをインスタンス化し、ソフトウェア定義型のインターコネクトを作成できる単一の UI ポータルを提供します。

- Cisco Catalyst SD-WAN Cloud Interconnect with Megaport
- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix



第 16 章

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport のライセンス管理

（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。

表 *66 :* 機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN Cloud Interconnect with Megaport のライセンス管理	Cisco vManage リリース 20.9.1	Megaport ファブリックでインターコネクト ゲートウェイとインターコネクト接続を作成するには、Cisco Commerce Workspace で必要なライセンスを購入する必要があります。 この機能により、Cisco SD-WAN Manager は Megaport と連携してライセンスをモニターできるようになります。また、インターコネクト ゲートウェイまたはインターコネクト接続の作成時に、シスコと Megaport が共同でライセンス要件を適用します。
Megaport の従量制課金および IP トランジットライセンスの管理	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	この機能により、Megaport サービスの従量制課金（PAYG）ライセンスタイプのサポートが導入されます。PAYG モデルは、使用量に基づいて支払うことができる使用量ベースのモデルです。たとえば、クラウド ストレージ サービス プロバイダーは、使用されたストレージの量に基づいて請求することができます。

- Cisco Catalyst SD-WAN Cloud Interconnect with Megaport のライセンス管理に関する情報 （377 ページ）
- Megaport アカウントに関連付けられたライセンスの表示 （388 ページ）
- インターコネクト ゲートウェイに関連付けられたライセンス SKU の確認 （390 ページ）
- インターコネクト接続に関連付けられたライセンス SKU の確認 （391 ページ）

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport のライセンス管理に関する情報

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport ソリューションでは、Cisco SD-WAN Manager を使用して、Cisco Catalyst SD-WAN オーバーレイと Megaport ファブリックにまたがるサイトとクラウド間およびサイト間の接続を作成することができます。サイトとクラウド間のユースケースでは、Megaport ファブリックを使用して Cisco Catalyst SD-WAN ブランチサイトをパブリッククラウドサービスに接続することができます。サイト間のユースケースでは、Megaport ファブリックを使用して Cisco Catalyst SD-WAN ブランチサイトを別のブランチサイトに接続することができます。

Cisco SD-WAN Manager を使用してサイトとクラウド間の接続を作成するワークフローは、次のとおりです。

- Megaport Point of Presence（PoP）で Cisco Catalyst 8000V インスタンスをインターコネクト ゲートウェイとして展開します。
- Megaport ファブリックのインターコネクト ゲートウェイとクラウド サービス プロバイダー間にインターコネクト接続を作成します。
- Cisco Catalyst SD-WAN オーバーレイを介してブランチの WAN エッジデバイスからインターコネクト ゲートウェイにトラフィックをルーティングし、ブランチをクラウド サービス プロバイダーに接続します。

Cisco SD-WAN Manager を使用してサイト間の接続を作成するワークフローは、次のとおりです。

- Megaport Point of Presence（PoP）で 2 つの Cisco Catalyst 8000V インスタンスをインターコネクト ゲートウェイとして展開します。
- Megaport ファブリックのインターコネクト ゲートウェイ間にインターコネクト接続を作成します。
- Cisco Catalyst SD-WAN オーバーレイを介して、ブランチの 1 つにある WAN エッジデバイスからインターコネクト ゲートウェイの 1 つにトラフィックをルーティングします。
- Cisco Catalyst SD-WAN オーバーレイを介して、もう 1 つのブランチの WAN エッジデバイスからもう 1 つのインターコネクト ゲートウェイにトラフィックをルーティングします。

Megaport ファブリックでインターコネクト ゲートウェイとインターコネクト接続を作成する前に、Cisco Commerce Workspace で最小在庫管理単位（SKU）として利用可能な必要なライセンスを購入する必要があります。ライセンスは、次の 3 つのカテゴリに属しています。

- インターコネクト ゲートウェイ ライセンス
- インターコネクト接続ライセンス
- 補足ライセンス

これらのライセンスは、必要な Cisco Catalyst 8000V ライセンスと、必要に応じて HSEC ライセンスとともに購入する必要があります。必要なライセンスがない場合、インターコネクト ゲートウェイまたはインターコネクト接続の作成は失敗し、Megaport が提供する適切なエラーメッセージが Cisco SD-WAN Manager に表示されます。

インターコネクト ゲートウェイ ライセンス

インターコネクト ゲートウェイ ライセンスを使用すると、Megaport ファブリック内の特定のリージョンのメトロにインターコネクト ゲートウェイを展開することができます。

インターコネクト ゲートウェイ ライセンスを選択する際は、次の点を考慮してください。

- 展開リージョン：そのリージョン内のブランチに最も近い Megaport PoP にインターコネクト ゲートウェイを展開します。
- フォームファクタ：ゲートウェイに接続する予定のすべてのブランチからの着信トラフィックの最大累積帯域幅に基づいて、インターコネクト ゲートウェイのフォームファクタを選択します。

SKU は `MVE-<region-code>-<form-factor-code>-C` という形式で命名されます

- Megaport の用語では、インターコネクト ゲートウェイは Megaport Virtual Edge（MVE）と呼ばれます。
- region-code で、1 つ以上のメトロを含むリージョンを識別します。次に、各メトロには冗長性のために複数のデータセンターがあります。次の表に、使用可能なリージョン、リージョンコード、および各リージョン内のメトロを示します。

リージョン	リージョンコード	メトロ
北米	該当なし	アッシュバーン、アトランタ、ベイエリア、シカゴ、ダラス、デンバー、ロサンゼルス、マイアミ、ニューヨーク、フェニックス、シアトル、トロント
欧州	EU	アムステルダム、フランクフルト、パリ
アジア	ASIA	香港、シンガポール、大阪、東京
オーストラリア	AU	メルボルン、パース、シドニー
ニュージーランド	NZ	オークランド
英国	英国	ロンドン

（注）
- サポートされるリージョン内のメトロおよびサポートされるリージョンは、新しいメトロおよびリージョンへのMegaportの拡張に基づいて変更される可能性があります。サポートされるメトロとリージョンの最新リストについては、Cisco Commerce Workspaceを確認してください。
- インターコネクトゲートウェイの展開でメトロを使用できるかどうかは、メトロで使用可能なコンピューティングキャパシティによって異なります。

- フォームファクタは次のいずれかです。

フォーム ファクタ	フォームファクタコード	説明
小	SML	2コアのCisco Catalyst 8000vインスタンスが、500 Mbpsの最大インバウンド帯域幅をサポートします
中	MED	4コアのCisco Catalyst 8000vインスタンスが、1 Gbpsの最大インバウンド帯域幅をサポートします
大	LRG	8コアのCisco Catalyst 8000vインスタンスが、5 Gbpsの最大インバウンド帯域幅をサポートします

- SKU名の末尾にある-Cは、プリペイドライセンスであることを示しています。

インターコネクト ゲートウェイへの IP トランジット

インターコネクト ゲートウェイ ライセンスに加えて、Cisco Commerce Workspaceで適切なIPトランジットライセンスも購入する必要があります。IPトランジットライセンスは、Megaport PoPでのインターネット接続用です。ブランチのWANエッジデバイスは、このインターネット接続を介してインターコネクト ゲートウェイに接続します。Cisco Commerce Workspaceでインターコネクト ゲートウェイ ライセンスを選択すると、適切なIPトランジットライセンスが自動的に購入対象に含まれます。

IP トランジット SKU は `IPT-<region-code>-<form-factor-code>-C` という形式で命名されます

リージョンコードとフォームファクタコードの値は、インターコネクト ゲートウェイ SKU と同じです。SKU名の末尾にある-Cは、プリペイドライセンスであることを示しています。

関連トピック

インターコネクト ゲートウェイのライセンスの適用 （383 ページ）

インターコネクト接続ライセンス

次の2種類のインターコネクト接続を作成できます。

- Megaportリージョンのメトロ内：メトロ内のインターコネクト接続は、短距離接続です。
- メトロ間：メトロ間のインターコネクト接続は、長距離接続です。

Cisco Commerce Workspaceで、短距離接続と長距離接続の両方に適切なライセンスを購入します。

短距離インターコネクト接続ライセンス

インターコネクト ゲートウェイから、Cloud onRampインスタンスまたは同じメトロ内の別のインターコネクト ゲートウェイへの短距離インターコネクト接続を作成できます。短距離インターコネクト接続は、メトロ内のクラウド サービス プロバイダーへのプライベート接続として機能します。短距離インターコネクト接続の帯域幅は1 Gbpsまたは10 Gbpsです。短距離インターコネクト接続は、メトロ内（IM）インターコネクト接続とも呼ばれます。

短距離インターコネクト接続SKUは、`VXC-IM-<bandwidth>-<region-code>-C`という形式で命名されます

- Megaportの用語では、インターコネクト接続は仮想クロスコネクト（VXC）と呼ばれます。IMはIn-Metro（メトロ内）を示しています。
- region-codeで、1つ以上のメトロを含むリージョンを識別します。次に、各メトロには冗長性のために複数のデータセンターがあります。次の表に、使用可能なリージョン、リージョンコード、および各リージョン内のメトロを示します。

リージョン	リージョンコード	メトロ
北米	該当なし	アッシュバーン、アトランタ、ベイエリア、シカゴ、ダラス、デンバー、ロサンゼルス、マイアミ、ニューヨーク、フェニックス、シアトル、トロント
欧州	EU	アムステルダム、フランクフルト、パリ
アジア	ASIA	香港、シンガポール、大阪、東京
オーストラリア	AU	メルボルン、パース、シドニー
ニュージーランド	NZ	オークランド
英国	英国	ロンドン

（注） サポートされるリージョン内のメトロおよびサポートされるリージョンは、新しいメトロおよびリージョンへのMegaportの拡張に基づいて変更される可能性があります。サポートされるメトロとリージョンの最新リストについては、Cisco Commerce Workspaceを確認してください。

リージョンの短距離インターコネクト接続 SKU を使用すると、リージョン内の任意のメトロでインターコネクト接続を作成できます。

- 帯域幅は、1G（1 Gbps を表す）または 10 G（10 Gbps を表す）です。
- SKU 名の末尾にある -C は、プリペイドライセンスであることを示しています。

長距離インターコネクト接続ライセンス

長距離インターコネクト接続は、次の場合に作成できます。

- インターコネクトゲートウェイから、同じリージョンの別のメトロ内または別のリージョン内にある Cloud onRamp インスタンスへ。インターコネクト接続は、メトロまたはリージョンにまたがるクラウド サービス プロバイダーへのプライベート接続として機能します。
- インターコネクトゲートウェイから、同じリージョンの別のメトロ内または別のリージョン内にある別のインターコネクトゲートウェイへ。インターコネクト接続は、メトロまたはリージョンにまたがるインターコネクト ゲートウェイを接続します。

長距離インターコネクト接続の帯域幅は、50 Mbps、100 Mbps、200 Mbps、300 Mbps、400 Mbps、500 Mbps、1 Gbps、2 Gbps、5 Gbps、および 10 Gbps のいずれかです。

長距離インターコネクト接続は、リージョン間/内インターコネクト接続とも呼ばれます。

長距離インターコネクト接続 SKU は、`VXC-II-<region1-code>-<region2-code>-C` という形式で命名されます

- Megaport の用語では、インターコネクト接続は仮想クロスコネクト（VXC）と呼ばれます。II は Inter/Intra-Region（リージョン内/間）を示しています。
- region-code で、1 つ以上のメトロを含むリージョンを識別します。次に、各メトロには冗長性のために複数のデータセンターがあります。次の表に、使用可能なリージョン、リージョンコード、および各リージョン内のメトロを示します。

リージョン	リージョンコード	メトロ
北米	該当なし	アッシュバーン、アトランタ、ベイエリア、シカゴ、ダラス、デンバー、ロサンゼルス、マイアミ、ニューヨーク、フェニックス、シアトル、トロント
欧州	EU	アムステルダム、フランクフルト、パリ
アジア	ASIA	香港、シンガポール、大阪、東京
オーストラリア	AU	メルボルン、パース、シドニー
ニュージーランド	NZ	オークランド
英国	英国	ロンドン

（注） サポートされるリージョン内のメトロおよびサポートされるリージョンは、新しいメトロおよびリージョンへの Megaport の拡張に基づいて変更される可能性があります。サポートされるメトロとリージョンの最新リストについては、Cisco Commerce Workspace を確認してください。

リージョンの長距離インターコネクト接続 SKU を使用すると、リージョン内の任意のメトロでインターコネクト接続を作成できます。

- SKU 名の末尾にある -C は、プリペイドライセンスであることを示しています。

関連トピック

短距離インターコネクト接続のライセンスの適用 （384 ページ）
長距離インターコネクト接続のライセンスの適用 （385 ページ）

補足ライセンス

AWS ホスト型接続を作成するには、短距離または長距離のインターコネクト接続ライセンスに加えて、Cisco Commerce Workspace で AWS ホスト型接続ライセンスを購入する必要があります。

長距離インターコネクト接続を AWS ホスト型接続として使用するには、`AWS-HC-IIVXC-C` という形式の SKU を購入します

- AWS-HC は、AWS ホスト型接続を示しています。
- IIVXC は、リージョン間/リージョン内 VXC または長距離インターコネクト接続を示しています。
- 接続の許容帯域幅は、長距離インターコネクト接続ライセンスに関連付けられた帯域幅によって決まります。
- SKU 名の末尾にある -C は、プリペイドライセンスであることを示しています。

短距離インターコネクト接続を AWS ホスト型接続として使用するには、`AWS-HC-IMVXC-<bandwidth>-C` という形式の SKU を購入します

- AWS-HC は、AWS ホスト型接続を示しています。
- IMVXC は、メトロ内 VXC または短距離インターコネクト接続を示しています。
- 帯域幅は、1G（1 Gbps を表す）または 10 G（10 Gbps を表す）です。AWS ホスト型接続ライセンスの帯域幅は、短距離インターコネクト接続ライセンスの帯域幅と一致している必要があります。
- SKU 名の末尾にある -C は、プリペイドライセンスであることを示しています。

関連トピック

AWS ホスト型接続のライセンスの適用 （386 ページ）

ライセンスの適用

シスコと Megaport は、Cisco Commerce Workspace を通じて購入したライセンスの資格を共同で適用します。

- Cisco Commerce Workspace でライセンス SKU を購入すると、Megaport に購入が通知され、ライセンスが Megaport アカウントに追加されます。また、Cisco SD-WAN Manager の [Account Licenses] ページでライセンス情報を表示することもできます。
- Cisco SD-WAN Manager でインターコネクト ゲートウェイ、インターコネクト接続、または AWS ホスト型接続を作成する場合、Megaport ファブリックにリソースを作成する前に、Megaport が必要なライセンスがあるかどうかを確認します。
- 必要なライセンスがある場合、Megaportはライセンスステータスを使用中に変更し、リクエストされたリソースを作成します。Cisco SD-WAN Manager でもライセンスステータスが更新されます。
- 必要なライセンスがない場合、Megaport はリクエストされたリソースを作成せず、Cisco SD-WAN Manager に必要なライセンスがないことを示すエラーメッセージが表示されます。Cisco Commerce Workspace で必要なライセンスを購入し、リソースを作成します。
- Cisco SD-WAN Manager は、ライセンスの有効期限が切れる 90 日前にアラームを発生させます。また、Cisco SD-WAN Manager はライセンスの有効期限が切れたとき、または Cisco Commerce Workspace で更新されたときにもアラームを発生させます。
- Megaportは、ライセンスの有効期限とライセンスの有効期限が近づいていることを、電子メールで通知します。

関連トピック

Megaport アカウントに関連付けられたライセンスの表示 （388 ページ）

インターコネクト ゲートウェイのライセンスの適用

Cisco SD-WAN Manager でインターコネクト ゲートウェイを作成すると、Cisco SD-WAN Manager はリクエストを Megaport に送信します。リクエストを承認する前に、Megaport はアカウントに必要なライセンスがあるかどうかを確認します。

インターコネクト ゲートウェイを作成するには、次の基準に一致するインターコネクト ゲートウェイ ライセンスが必要です。

- ライセンスの有効期限が切れていたり、使用中だったりしてはなりません。
- ライセンスは、インターコネクト ゲートウェイを作成するリージョンに適用する必要があります。
- ライセンスは、作成するインターコネクト ゲートウェイのフォームファクタと一致している必要があります。

- 使用されていない、リクエストされたリージョンとフォームファクタをサポートしている複数のライセンスがある場合は、有効期限が最も早いライセンスが選択されます。

必要な基準に一致するライセンスがある場合、Megaportはライセンスを使用中とマークし、インターコネクト ゲートウェイを作成するためのリクエストを承認します。

必要な基準を満たすライセンスがない場合、インターコネクトゲートウェイの作成は失敗し、Cisco SD-WAN Managerに「`No license for <ICGWName> MVE`」などの該当するエラーメッセージが表示されます

Cisco Commerce Workspaceで必要なライセンスを購入するか、使用中のライセンスを使用可能にして、インターコネクトゲートウェイの作成を再試行します。インターコネクトゲートウェイを削除すると、関連するライセンスのステータスが使用可能に変化します。

ライセンスの有効期限

Cisco SD-WAN Managerは次のシナリオでアラームを発生させます。

- インターコネクト ゲートウェイ ライセンスの有効期限が切れる90日前
- インターコネクト ゲートウェイ ライセンスの有効期限が切れた場合
- インターコネクト ゲートウェイ ライセンスが更新された場合

ライセンスの有効期限が切れても、Megaportはインターコネクト ゲートウェイを停止しません。有効期限が切れる前にライセンスを更新するか、ライセンスの有効期限が切れてから14日以内にインターコネクト ゲートウェイを停止してください。14日間の猶予期間内にライセンスを更新しない場合は、Megaportがグローバルサービス契約に基づいてユーザーに直接請求することができます。

関連トピック

インターコネクト ゲートウェイ ライセンス （378ページ）

短距離インターコネクト接続のライセンスの適用

Cisco SD-WAN Managerで短距離インターコネクト接続を作成すると、Cisco SD-WAN ManagerはリクエストをMegaportに送信します。リクエストを承認する前に、Megaportはアカウントに必要なライセンスがあるかどうかを確認します。

短距離インターコネクト接続を作成するには、次の基準に一致する短距離インターコネクト接続ライセンスが必要です。

- ライセンスの有効期限が切れていたり、使用中だったりしてはなりません。
- ライセンスは、ターゲットのメトロがあるリージョンに適用する必要があります。
- ライセンスが、作成するインターコネクト接続の帯域幅と一致しているか、より大きな帯域幅をサポートしている必要があります。
- 使用されていない、リージョンと帯域幅が一致する複数のライセンスがある場合は、有効期限が最も早いライセンスが選択されます。

帯域幅に一致するライセンス、またはより高い帯域幅の最も近いライセンスが必要なリージョンと可用性の基準を満たしている場合、Megaportはライセンスを使用中としてマークし、短距離インターコネクト接続を作成するためのリクエストを承認します。

必要な基準を満たすライセンスがない場合、短距離インターコネクト接続の作成は失敗し、Cisco SD-WAN Managerに「`Unable to find valid matching license for the Interconnect connection`」などの該当するエラーメッセージが表示されます

Cisco Commerce Workspaceで必要なライセンスを購入するか、使用中のライセンスを使用可能にして、短距離インターコネクト接続の作成を再試行します。短距離インターコネクト接続を削除すると、関連するライセンスのステータスが使用可能に変化します。

ライセンスの有効期限

Cisco SD-WAN Managerは次のシナリオでアラームを発生させます。

- 短距離インターコネクト接続ライセンスの有効期限が切れる90日前
- 短距離インターコネクト接続ライセンスの有効期限が切れた場合
- 短距離インターコネクト接続ライセンスが更新された場合

ライセンスの有効期限が切れても、Megaportは短距離インターコネクト接続を停止しません。有効期限が切れる前にライセンスを更新するか、ライセンスの有効期限が切れてから14日以内に短距離インターコネクト接続を停止してください。14日間の猶予期間内にライセンスを更新しない場合は、Megaportがグローバルサービス契約に基づいてユーザーに直接請求することができます。

関連トピック

インターコネクト接続ライセンス （379ページ）

長距離インターコネクト接続のライセンスの適用

Cisco SD-WAN Managerで長距離インターコネクト接続を作成すると、Cisco SD-WAN ManagerはリクエストをMegaportに送信します。リクエストを承認する前に、Megaportはアカウントに必要なライセンスがあるかどうかを確認します。

長距離インターコネクト接続を作成するには、次の基準に一致する長距離インターコネクト接続ライセンスが必要です。

- ライセンスの有効期限が切れていたり、使用中だったりしてはなりません。
- ライセンスは、ソースとターゲットのメトロがあるリージョンに適用する必要があります。

（注） 英国はEUリージョンに属していません。英国内に発信元または終端がある接続をプロビジョニングするには、適切な英国ライセンスがあることを確認します。

- ライセンスが、作成するインターコネクト接続の帯域幅と一致しているか、より大きな帯域幅をサポートしている必要があります。
- 使用されていない、リージョンと帯域幅が一致する複数のライセンスがある場合は、有効期限が最も早いライセンスが選択されます。

帯域幅に一致するライセンス、またはより高い帯域幅の最も近いライセンスが必要なリージョンと可用性の基準を満たしている場合、Megaportはライセンスを使用中としてマークし、長距離インターコネクト接続を作成するためのリクエストを承認します。

必要な基準を満たすライセンスがない場合、長距離インターコネクト接続の作成は失敗し、Cisco SD-WAN Manager に「`Unable to find valid matching license for the Interconnect connection`」などの該当するエラーメッセージが表示されます

Cisco Commerce Workspace で必要なライセンスを購入するか、使用中のライセンスを使用可能にして、長距離インターコネクト接続の作成を再試行します。長距離インターコネクト接続を削除すると、関連するライセンスのステータスが使用可能に変化します。

ライセンスの有効期限

Cisco SD-WAN Manager は次のシナリオでアラームを発生させます。

- 長距離インターコネクト接続ライセンスの有効期限が切れる 90 日前
- 長距離インターコネクト接続ライセンスの有効期限が切れた場合
- 長距離インターコネクト接続ライセンスが更新された場合

ライセンスの有効期限が切れても、Megaportは長距離インターコネクト接続を停止しません。有効期限が切れる前にライセンスを更新するか、ライセンスの有効期限が切れてから 14 日以内に長距離インターコネクト接続を停止してください。14 日間の猶予期間内にライセンスを更新しない場合は、Megaportがグローバルサービス契約に基づいてユーザーに直接請求することができます。

関連トピック

インターコネクト接続ライセンス （379 ページ）

AWS ホスト型接続のライセンスの適用

短距離または長距離のインターコネクト接続 Cisco SD-WAN Manager を作成し、それを AWS ホスト型接続として使用する場合、Cisco SD-WAN Manager はリクエストを Megaport に送信します。Megaportはリクエストを承認する前に、必要な短距離または長距離のインターコネクト接続ライセンスと、AWS ホスト型接続の補足ライセンスがあるかどうかを確認します。

- 短距離インターコネクト接続ライセンスは、このドキュメントの短距離インターコネクト接続のライセンスの適用 （384 ページ）のセクションに記載されている要件を満たしている必要があります。
- 長距離インターコネクト接続ライセンスは、このドキュメントの長距離インターコネクト接続のライセンスの適用 （385 ページ）のセクションに記載されている要件を満たしている必要があります。

- AWS ホスト型接続ライセンスの有効期限が切れていたり、使用中だったりしてはなりません。

帯域幅に一致するインターコネクト接続ライセンス、またはより高い帯域幅の最も近いライセンスが必要なリージョンと可用性の基準を満たしていて、AWS ホスト型接続の補足ライセンスが使用可能な場合、Megaportはライセンスを使用中としてマークし、長距離インターコネクト接続を作成するためのリクエストを承認します。

必要なライセンスがない場合、接続の作成は失敗し、Cisco SD-WAN Manager に「`Unable to find valid matching license for the Interconnect connection`」などの該当するエラーメッセージが表示されます

Cisco Commerce Workspace で必要なライセンスを購入するか、使用中のライセンスを使用可能にして、AWS ホスト型接続の作成を再試行します。AWS ホスト型接続として使用されているインターコネクト接続を削除すると、関連付けられたライセンスを使用して新しい AWS ホスト型接続を作成できるようになります。

ライセンスの有効期限

Cisco SD-WAN Manager は次のシナリオでアラームを発生させます。

- 補足ライセンスの有効期限が切れる 90 日前
- 補足ライセンスの有効期限が切れたとき
- 補足ライセンスが更新されたとき

ライセンスの有効期限が切れても、Megaport は AWS ホスト型接続を停止しません。有効期限が切れる前にライセンスを更新するか、ライセンスの有効期限が切れてから 14 日以内に接続を停止してください。14 日間の猶予期間内にライセンスを更新しない場合は、Megaport がグローバルサービス契約に基づいてユーザーに直接請求することができます。

関連トピック

補足ライセンス （382 ページ）

従量制ライセンスに関する情報

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 17.14.1a、Cisco Catalyst SD-WAN Manager リリース 20.14.1

Megaport サービスの PAYG ライセンスでは、使用するインフラストラクチャ リソースに対してのみ料金を支払うことができます。PAYG ライセンスメカニズムでは、Cisco Commerce Workspace（CCW）から PAYG SKU を調達する必要があります。これらの PAYG ライセンス SKU は、期間契約を必要とせずに Megaport サービスを起動します。日々の帯域幅要件に基づいてネットワークを動的に拡張または縮小でき、月末に請求されます。

Megaport の場所で PAYG ライセンスを使用してインターコネクト ゲートウェイを作成する方法については、「Create Interconnect Gateway at a Megaport Location」を参照してください。

Megaportアカウントに関連付けられたライセンスの表示

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [SETUP] の [WORKFLOWS] で、[Account Licenses] をクリックします。
4. [Provider]：ドロップダウンリストから、[Megaport] を選択します。
5. [Account Name]：ドロップダウンリストから、Megaport のアカウント名を選択します。
6. インターコネクト ゲートウェイ ライセンスを表示するには、[INTERCONNECT GATEWAY LICENSES] をクリックします。

   Cisco SD-WAN Manager では、アカウントに関連付けられたインターコネクト ゲートウェイ ライセンス SKU が表示され、各 SKU の次の詳細が提供されます。

表 *67*：インターコネクト ゲートウェイ ライセンス *SKU* の詳細

カラム	説明
SKU 名	ライセンス SKU の名前
SKU UUID	ライセンスが属する Megaport アカウント内のライセンス SKU の一意の ID
Gateway Size	インターコネクト ゲートウェイ インスタンスのサイズまたはフォームファクタ（SML、MED、または LRG）
状態	ライセンスの現在の状態（IN_USE、IN_USE, EXPIRED、AVAILABLE、または EXPIRED）
License End Date	開始日と有効期間から導出されたライセンスの終了日（有効期限）
開始日（Start Date）	Cisco Commerce Workspace で SKU を注文したときに指定されたライセンスの開始日
Smart Account ID	ライセンスが属するスマートアカウント
Virtual Account ID	ライセンスが属するバーチャルアカウント
Subscription ID	ライセンスに関連付けられたサブスクリプション ID
Web Order ID	ライセンスの一意の Web 注文 ID

7. インターコネクト接続ライセンスを表示するには、[INTERCONNECT CONNECTION LICENSES] をクリックします。

   Cisco SD-WAN Manager では、アカウントに関連付けられたインターコネクト接続ライセンス SKU が表示され、各 SKU の次の詳細が提供されます。

表 *68：*インターコネクト接続ライセンス *SKU* の詳細

カラム	説明
SKU 名	ライセンス SKU の名前
SKU UUID	ライセンスが属する Megaport アカウント内のライセンス SKU の一意の ID
状態	ライセンスの現在の状態（IN_USE、IN_USE, EXPIRED、AVAILABLE、または EXPIRED）
License End Date	開始日と有効期間から導出されたライセンスの終了日（有効期限）
開始日（Start Date）	Cisco Commerce Workspace で SKU を注文したときに指定されたライセンスの開始日
VXC Bandwidth	インターコネクト接続の設定済み帯域幅（Mbps）
Smart Account ID	ライセンスが属するスマートアカウント
Virtual Account ID	ライセンスが属するバーチャルアカウント
Subscription ID	ライセンスに関連付けられたサブスクリプション ID
Web Order ID	ライセンスの一意の Web 注文 ID

8. 補足ライセンスを表示するには、[SUPPLEMENTAL LICENSES] をクリックします。

   Cisco SD-WAN Manager では、アカウントに関連付けられた補足ライセンス SKU が表示され、各 SKU の次の詳細が提供されます。

表 *69：*補足ライセンス *SKU* の詳細

カラム	説明
SKU 名	ライセンス SKU の名前
SKU UUID	ライセンスが属する Megaport アカウント内のライセンス SKU の一意の ID
状態	ライセンスの現在の状態（IN_USE、IN_USE, EXPIRED、AVAILABLE、または EXPIRED）

カラム	説明
License End Date	開始日と有効期間から導出されたライセンスの終了日（有効期限）
開始日（Start Date）	Cisco Commerce Workspace で SKU を注文したときに指定されたライセンスの開始日
帯域幅	AWS ホスト型接続の設定済み帯域幅（Mbps）
Smart Account ID	ライセンスが属するスマートアカウント
Virtual Account ID	ライセンスが属するバーチャルアカウント
Subscription ID	ライセンスに関連付けられたサブスクリプション ID
Web Order ID	ライセンスの一意の Web 注文 ID

インターコネクトゲートウェイに関連付けられたライセンス SKU の確認

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [WORKFLOWS] の下の [MANAGE] から、[Gateway Management] をクリックします。

   Cisco SD-WAN Manager が、展開されたすべてのインターコネクト ゲートウェイをテーブルに表示します。
4. 目的のインターコネクト ゲートウェイを見つけます。

ヒント 設定時に指定した名前を使用して、インターコネクト ゲートウェイを検索します。

5. 右にスクロールして、[License SKU UUID] 列を表示します。

   [Account Licenses] ページで、この SKU UUID を使用してライセンス SKU に関する詳細情報を表示します。

   [License End Date] 列には、インターコネクト ゲートウェイ ライセンスの有効期限が表示されます。

関連トピック

Megaport アカウントに関連付けられたライセンスの表示 （388 ページ）

インターコネクト接続に関連付けられたライセンス SKU の確認

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [WORKFLOWS] の [INTENT MANAGEMENT] から、[Interconnect Connectivity] をクリックします。

   Cisco SD-WAN Manager が、設定済みのすべてのインターコネクト接続をテーブルに表示します。
4. 目的のインターコネクト接続を見つけます。

ヒント　設定時に入力した名前を使用して、インターコネクト接続を検索します。

5. 右にスクロールして、[Connection License SKU UUID] 列を表示します。[Account Licenses] ページで、この SKU UUID を使用してライセンス SKU に関する詳細情報を表示します。

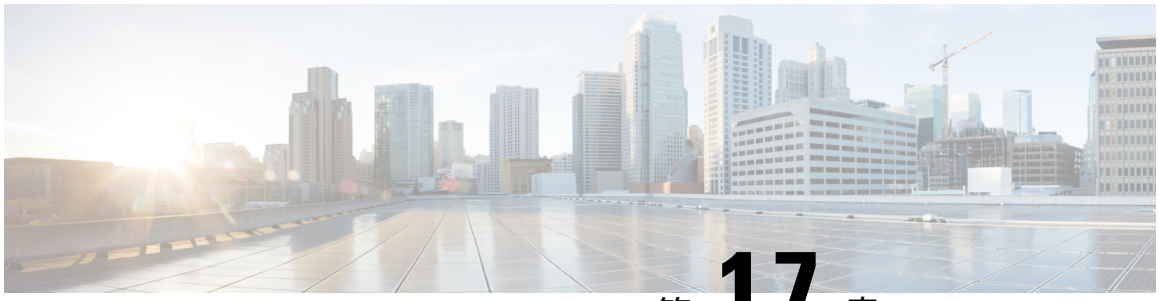
   [License End Date] 列には、インターコネクト接続ライセンスの有効期限が表示されます。

   AWS ホスト型接続の場合、Cisco SD-WAN Manager には次の詳細が表示されます。

   - [AWSHC License UUID] 列には、AWS ホスト型接続の補足ライセンスの SKU UUID が表示されます。[Account Licenses] ページで、この SKU UUID を使用してライセンス SKU に関する詳細情報を表示します。
   - [AWSHC License End Date] 列には、AWS ホスト型接続の補足ライセンスの有効期限が表示されます。

関連トピック

Megaport アカウントに関連付けられたライセンスの表示 （388 ページ）



第 17 章

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

（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。

表 *70*：機能の履歴

機能名	リリース情報	説明
Megaport のソフトウェア定義型インターコネクト	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	Cisco Catalyst 8000v Edge ソフトウェア（Cisco Catalyst 8000V）インスタンスを Megaport ファブリックのインターコネクト ゲートウェイとして展開し、Cisco Catalyst SD-WAN ブランチの場所をインターコネクト ゲートウェイに接続することができます。インターコネクト ゲートウェイから、AWS Cloud OnRamp または Megaport ファブリック内の別のインターコネクト ゲートウェイへのソフトウェア定義型インターコネクトを作成することができます。
Cisco Catalyst SD-WAN Cloud Interconnect with Megaport：Google Cloud および Microsoft Azure へのインターコネクト	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	Cisco Catalyst 8000v Edge ソフトウェア（Cisco Catalyst 8000V）インスタンスを Megaport ファブリックのインターコネクト ゲートウェイとして展開し、Cisco Catalyst SD-WAN ブランチの場所をインターコネクト ゲートウェイに接続することができます。インターコネクト ゲートウェイから、Google Cloud VPC、Microsoft Azure VNet または Virtual WAN へのソフトウェア定義型インターコネクトを作成し、Megaport ファブリックを介してブランチの場所をクラウドリソースにリンクすることができます。

機能名	リリース情報	説明
Megaport との暗号化されたマルチクラウド インターコネクト	Cisco vManage リリース 20.9.1	Cisco Catalyst SD-WAN ファブリックを、Megaport のインターコネクト ゲートウェイから AWS、Google Cloud、および Microsoft Azure クラウド サービス プロバイダーに拡張できます。Cisco SD-WAN Manager の Cloud OnRamp ワークフローを使用して、インターコネクト ゲートウェイとクラウド サービス プロバイダー間のセキュアなプライベート Cisco Catalyst SD-WAN 接続をプロビジョニングすることができます。

機能名	リリース情報	説明
AWS および Microsoft Azure へのインターコネクト接続の追加プロパティの変更	Cisco vManage リリース 20.10.1	

機能名	リリース情報	説明
		AWS へのインターコネクト接続： • Cisco vManage リリース 20.9.x 以前：ホスト型 VIF 接続の作成後は、その帯域幅のみを編集できます。ホスト型接続のプロパティは、接続の作成後に編集できません。 この機能により、接続の作成後に、ホスト型 VIF 接続とホスト型接続の両方の追加プロパティを編集できます。編集可能なプロパティの完全なリストについては、表 73 : AWS へのインターコネクト接続の編集可能なプロパティ（473 ページ）を参照してください。 • Cisco vManage リリース 20.9.x 以前：接続に関連付けられている VPC タグを編集することはできません。 この機能を使用して、プライベートホスト型VIF、プライベートホスト型接続、またはトランジットホスト型接続の VPC のアタッチまたはデタッチや、VPC を追加または削除するための接続に関連付けられている VPC タグの編集を行います。 Microsoft Azure へのインターコネクト接続： • Cisco vManage リリース 20.9.x 以前：接続の作成後は、その帯域幅のみを編

機能名	リリース情報	説明
		集できます。接続の他のプロパティは編集できません。 この機能を使用して、Microsoft のピアリング接続とプライベートピアリング接続の両方の追加プロパティを編集します。編集可能なプロパティの完全なリストについては、表 75 : Microsoft Azure へのインターコネクト接続の編集可能なプロパティ（475ページ）を参照してください。 • Cisco vManage リリース 20.9.x 以前：接続に関連付けられている VNet タグを編集することはできません。 この機能を使用して、プライベートピアリング接続の VNet のアタッチまたはデタッチや、VNet を追加または削除するための接続に関連付けられている VNet タグの編集を行います。

機能名	リリース情報	説明
監査管理	Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a Cisco vManage リリース 20.11.1	監査管理機能は、インターコネクトクラウドとプロバイダーの接続状態が、Cisco SD-WAN Manager の接続状態と同期しているかどうかを把握するのに役立ちます。この状態とは、Cisco Catalyst SD-WAN がクラウドサービスおよびプロバイダーと確立するさまざまな接続ステータスのことを指します。監査は、Cisco SD-WAN Manager インテントとクラウドで実現された内容の間の乖離または不一致を特定するのに役立ちます。

- Cisco Catalyst SD-WAN Cloud Interconnect with Megaport の前提条件 （399 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Megaport の制約事項 （400 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Megaport に関する情報 （407 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Megaport の設定ワークフロー （410 ページ）
- Cisco SD-WAN Cloud Interconnect with Megaport の前提条件の設定 （412 ページ）
- AWS へのインターコネクトの作成 （419 ページ）
- Google Cloud へのインターコネクトの作成 （439 ページ）
- Microsoft Azure へのインターコネクトの作成 （451 ページ）
- インターコネクト ゲートウェイ間のインターコネクトの作成 （470 ページ）
- 設定の確認と変更 （471 ページ）
- 監査管理 （480 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Megaport のトラブルシューティング （481 ページ）

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport の前提条件

- Megaport アカウントを作成します。

  Cisco Commerce Workspace での発注プロセスの一環として、アカウントの作成に関する電子メールを Megaport から受信します。詳細については、この電子メールを参照してください。

- インターコネクトゲートウェイとクラウドプロバイダー間のパブリックピアリングを必要とする接続の場合は、パブリック BGP ASN とパブリック BGP ピアリング IP アドレスを

指定します。接続を作成する前に、パブリック BGP ASN とパブリック BGP ピアリング IP アドレスの使用が組織で許可されていることを確認してください。

- インターコネクト ゲートウェイとして展開する Cisco Catalyst 8000v インスタンスの UUID が必要な数あることを確認します。
- Cisco SD-WAN Manager がインターネットに接続できることを確認します。

  設定ワークフローの一環として、Cisco SD-WAN Manager はインターネットを介して Megaport ポータルに接続します。

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport の制約事項

一般的な制約事項

- 各場所では、一度に 1 つのインターコネクト操作（インターコネクト ゲートウェイの展開や、接続の作成または削除など）のみを実行できます。
- すべてのインターコネクトとクラウドの操作には時間制限があります。操作がタイムアウトした場合は、Cisco SD-WAN Manager が失敗を報告します。現在、このタイムアウト値は設定できません。
- グローバル設定を変更すると、変更後に作成された新しいゲートウェイまたは接続に変更が適用されます。変更前に作成されたゲートウェイまたは接続には、変更は影響しません。
- クラウド サービス プロバイダーの割り当ては、Cisco SD-WAN Manager から作成されるすべてのインターコネクトクラウド接続に適用されます。
- Cisco vManage リリース 20.9.2 および Cisco vManage リリース 20.10.1 以降では、AWS リージョンのトランジットホスト型接続で、1 つのトランジットゲートウェイのみを Direct Connect ゲートウェイに関連付けることができます。

  Cisco SD-WAN Manager は Cisco vManage リリース 20.9.2 および Cisco vManage リリース 20.10.1 以降でこの制限を適用しますが、Cisco vManage リリース 20.9.1 以前のリリースでは、AWS リージョンの Direct Connect ゲートウェイに、1 つのトランジットゲートウェイのみを関連付けることを推奨します。
- Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a 以降では、Cisco Catalyst SD-WAN Cloud Interconnect with Megaport は、バージョン Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降でのみサポートされます。
- Cisco Catalyst SD-WAN Manager リリース 20.12.2 以降では、マルチクラウドワークフローの一環として作成されたトランジットゲートウェイは、SDCI ワークフローのトランジット接続の下にリストされません。

AWS へのインターコネクト

- AWS クラウドリソースへの接続を作成する際は、AWS のクォータと制限に準拠してください。Cisco SD-WAN Manager は、すべての AWS のクォータと制限を適用するわけではありません。
- 異なる AWS アカウントに属するクラウドリソースを、単一の接続の一部として使用することはできません。
- プライベート VIF またはトランジット VIF を Direct Connect ゲートウェイにアタッチします。プライベート VIF とトランジット VIF の組み合わせを、同じ Direct Connect ゲートウェイにアタッチすることはできません。
- Cisco vManage リリース 20.9.2 以降では、AWS リージョンのトランジットホスト型接続で、1 つのトランジットゲートウェイのみを Direct Connect ゲートウェイに関連付けることができます。

  Cisco SD-WAN Manager は Cisco vManage リリース 20.9.2 以降でこの制限を適用しますが、Cisco vManage リリース 20.9.1 以前のリリースでは、AWS リージョンの Direct Connect ゲートウェイに、1 つのトランジットゲートウェイのみを関連付けることを推奨します。
- 特定の VPC へのすべての接続は、以下を満たしている必要があります
  - 同じ Direct Connect ゲートウェイとピアリングしている
  - 同じトランジットゲートウェイまたは仮想プライベートゲートウェイのアタッチメントがある
- トランジット VIF の場合、トランジットゲートウェイと Direct Connect ゲートウェイは、異なる BGP ASN を使用する必要があります。
- Cisco vManage リリース 20.5.1 では、作成後は接続を編集できません。

  Cisco vManage リリース 20.6.1 以降では、以前に作成したホスト型 VIF 接続の帯域幅を変更できます。ただし、ホスト型接続の帯域幅は、作成後に変更できません。
- ホスト VPC タグの作成時に、AWS マルチクラウドワークフローまたはインターコネクト接続ワークフローのいずれかを使用して、タグを使用することを選択します。この選択は、タグの作成後は変更できず、タグが削除されるまで維持されます。
- Cisco vManage リリース 20.9.x 以前：インターコネクト接続用に選択されたホスト VPC タグは、タグの使用中は編集できません。

  Cisco vManage リリース 20.10.1 以降：インターコネクト接続用に選択されたホスト VPC タグは、タグの使用中に編集してホスト VPC を追加または削除することができます。
- Cisco vManage リリース 20.9.x 以前：ホスト VPC がタグに関連付けられていて、そのタグがインターコネクト接続の設定で使用されている場合、タグからホスト VPC の関連付けを解除して別のタグに関連付けることはできません。

Cisco vManage リリース 20.10.1 以降：ホスト VPC がタグに関連付けられていて、そのタグがインターコネクト接続の設定で使用されている場合、次の条件のいずれかまたは両方が満たされている場合は、タグからホスト VPC の関連付けを解除することができます。

- その他のホスト VPC がタグに関連付けられている
- その他の VPC タグがインターコネクト接続の設定で使用されている

タグからホスト VPC の関連付けが解除された後に、別のタグにホスト VPC を関連付けることができます。

インターコネクト接続の設定で VPC タグが使用されている場合、追加するホスト VPC がすでにタグに関連付けられているホスト VPC と同じリージョンに属していれば、追加のホスト VPC をタグに関連付けることができます。

- インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect プライベートホスト型 VIF、Direct Connect プライベートホスト型接続、または Direct Connect トランジットホスト型接続を作成するときに、BGP ピアリング用のカスタム IP アドレスを指定するか、内部に予約されたプールからの IP アドレスを Cisco SD-WAN Manager に選択させることができます。

  Cisco vManage リリース 20.5.1 では、IP アドレスはサブネット 192.168.0.0/16 から選択されます。Cisco vManage リリース 20.6.1 以降では、IP アドレスはサブネット 198.18.0.0/16 から選択されます。Cisco SD-WAN Manager をリリース 20.5.x から 20.6.1 以降にアップグレードする前に、Cisco vManage リリース 20.6.1 以降で内部に予約されているサブネット 198.18.0.0/16 からのカスタム BGP ピアリング IP アドレスを使用するように AWS への接続が設定されているかどうかを確認します。該当する場合は、その接続を削除し、198.18.0.0/16 と重複しないカスタム IP アドレスを使用して接続を再作成します。

- インターコネクト トランジット接続の編集時に、同じリージョン内の VPC タグのない新しいトランジットゲートウェイが選択された場合、接続の編集は破棄されます。

Microsoft Azure へのインターコネクト

- ホスト VNet タグの作成時に、Microsoft Azure マルチクラウドワークフローまたはインターコネクト接続ワークフローのいずれかを使用して、タグを使用することを選択します。この選択は、タグの作成後は変更できず、タグが削除されるまで維持されます。

- Cisco vManage リリース 20.9.x 以前：インターコネクト接続用に選択されたホスト VNet タグは、作成後は編集できません。

  Cisco vManage リリース 20.10.1 以降：インターコネクト接続用に選択されたホスト VNet タグは、タグの使用中に編集してホスト VNet を追加または削除することができます。

- Cisco vManage リリース 20.9.x 以前：ホスト VNet がタグに関連付けられていて、そのタグがインターコネクト接続の設定で使用されている場合、使用中のタグからホスト VNet の関連付けを解除して別のタグに関連付けることはできません。

Cisco vManage リリース 20.10.1 以降：ホスト VNet がタグに関連付けられていて、そのタグがインターコネクト接続の設定で使用されている場合、次の条件のいずれかまたは両方が満たされている場合は、タグからホスト VNet の関連付けを解除することができます。

- その他のホスト VNet がタグに関連付けられている
- その他の VNet タグがインターコネクト接続で使用されている

タグからホスト VNet の関連付けが解除された後に、別のタグにホスト VNet を関連付けることができます。

インターコネクト接続の設定で VNet タグが使用されている場合、追加するホスト VNet がすでにタグに関連付けられているホスト VNet と同じリージョンに属していれば、追加のホスト VNet をタグに関連付けることができます。

- インターコネクト ゲートウェイから Microsoft Azure ExpressRoute へのプライベートピアリング接続を作成するときは、ExpressRoute 回線と同じリソースグループに属する VNet、仮想 WAN、および仮想ハブのみを接続にアタッチできます。別のリソースグループからの VNet、仮想 WAN、および仮想ハブのアタッチは、サポートされていない設定です。

Google Cloud へのインターコネクト

- 各クラウドルータは、すべての BGP セッションに同じ ASN を使用します。

暗号化されたマルチクラウド インターコネクトの制約事項

サポート対象の最小リリース：Cisco vManage リリース 20.9.1

AWS へのインターコネクト

- AWS の要件に従って、
  - クラウドゲートウェイの最小インスタンスタイプは x-large である必要があります。
  - 1 つのインターコネクト接続に最大 10 個のクラウドゲートウェイをアタッチできます。
  - 1 つのクラウドゲートウェイは、30 個のインターコネクト接続に接続できます。

Microsoft Azure へのインターコネクト

- 1 つのクラウドゲートウェイを 8 つの異なるクラウドインターコネクト接続にアタッチでき、1 つのインターコネクト接続を 5 つの異なるクラウドゲートウェイに接続できます。
- 異なるリージョンのクラウドゲートウェイに接続するには、ExpressRoute 回線が Premium タイプである必要があります。
- Microsoft Azure 展開では、クラウドゲートウェイの WAN インターフェイスで Cisco Catalyst SD-WAN トンネルの色は自動的に設定されないため、WAN インターフェイスの色を手動

で更新する必要があります。テンプレートの色がブランチルータ、インターコネクト ゲートウェイ、およびクラウドゲートウェイの色と一致していることを確認します。

Google Cloud へのインターコネクト

- Google Cloud ゲートウェイへのクラウドインターコネクト接続は、冗長性が有効になっている場合にのみサポートされます。
- 1 つの接続にアタッチできる Google Cloud ゲートウェイは 1 つだけです。
- 既存の Google Cloud ゲートウェイは、クラウドインターコネクトではサポートされません。
- リージョンとネットワークの組み合わせに対して、最大 5 つの Google Cloud Router を作成できます。

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport の使用上の注意

表 *71 :* 接続設定の制限

説明	カウント
インターコネクト ゲートウェイ	
インターコネクト ゲートウェイあたりの最大接続数（VXC）	15 **注**：集約 VXC 帯域幅がインターコネクト ゲートウェイの帯域幅容量を超えることはできません。
AWS へのインターコネクト	
プライベート VIF の AWS への接続あたりの VPC の最大数	10
トランジット VIF の AWS への接続あたりの VPC の数	デフォルト：15 最大：15,000
トランジット VIF の AWS への接続あたりのトランジットゲートウェイの最大数	3
接続あたりの Direct Connect ゲートウェイの最大数	1
AWS Direct Connect ゲートウェイあたりの VIF（プライベートまたはトランジット）の最大数	デフォルト：30 制限はリクエストに応じて増やすことができます。

説明	カウント
AWS Direct Connect ホスト型接続あたりのプライベート、パブリック、またはトランジット VIF の最大数	1
トランジット VIF のブランチの場所から AWS へのプレフィックスの最大数	100
Microsoft Azure へのインターコネクト	
ExpressRoute に接続できるインターコネクト ゲートウェイの最大数	2
ExpressRoute が接続できる VNet の最大数	10
VNet に接続できる ExpressRoute の最大数	4
仮想ハブに接続できる ExpressRoute の最大数	ピアリングの場所あたり 8
仮想 WAN ExpressRoute ゲートウェイあたりの最大総スループット	20 Gbps
仮想ハブに接続できる VNet の最大数	500 ～（仮想 WAN 内の仮想ハブの合計数）

AWS へのインターコネクト

- AWS への接続を削除すると、Cisco SD-WAN Manager は、接続の確立中に作成された VIF、仮想プライベートゲートウェイ、およびルートテーブルを削除します。
- 接続を削除すると、Cisco SD-WAN Manager は、接続の確立中に作成された Direct Connect ゲートウェイ、トランジットゲートウェイ、または仮想プライベートゲートウェイへのアタッチメントと関連付けを削除します。
- AWS への接続の作成中に、Cisco SD-WAN Manager から Direct Connect ゲートウェイまたはトランジットゲートウェイを作成した場合、接続を削除してもゲートウェイは削除されません。必要に応じて、これらの AWS リソースを管理します。
- 接続を作成すると、新しいルートテーブルが作成され、接続にアタッチされたホスト VPC のメインルートテーブルとして設定されます。

  Cisco vManage リリース 20.5.1 では、仮想プライベートゲートウェイまたはトランジットゲートウェイへのデフォルトルートがメインルートテーブルに作成され、ルート伝達が有効になっています。必要に応じてルートと伝達を編集します。

  Cisco vManage リリース 20.5.1 以降では、インターコネクトによってアクセスする必要があるスタティックルートとサブネットの関連付けを、Cisco SD-WAN Manager によって新しく作成されたメインルートテーブルに移動する必要があります。

Cisco vManage リリース 20.6.1 以降では、トランジットゲートウェイのみへのデフォルトルートがメインルートテーブルに作成され、ルート伝達が有効になります。必要に応じてルートと伝達を編集します。

- グローバル設定を変更すると、変更後に作成された新しいゲートウェイまたは接続に変更が適用されます。変更前に作成されたゲートウェイまたは接続には、変更は影響しません。

Google Cloud へのインターコネクト

- 非冗長接続の場合は、各ネットワークリージョンに Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成する必要があります。Megaport ファブリックでは、インターコネクト ゲートウェイから各 Google Cloud Router へのインターコネクトが作成されます。
- 冗長接続の場合は、各ネットワークリージョンに 2 つの Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成する必要があります。Megaport ファブリックでは、インターコネクト ゲートウェイのペアのそれぞれから各 Google Cloud Router へのインターコネクトが作成されます。
- インターコネクト アタッチメントで使用するには、Google Cloud Router の Google ASN を 16550 に設定する必要があります。

Microsoft Azure へのインターコネクト

- ExpressRoute にアタッチされた VNet への HA 接続を提供するために特定の ExpressRoute に接続できるインターコネクト ゲートウェイのペアは、1 つだけです。

  インターコネクト ゲートウェイの 2 番目のペアを同じ vNet に接続するには、別の ExpressRoute を作成し、vNet を ExpressRoute にアタッチして、インターコネクト ゲートウェイを ExpressRoute に接続します

  VNet に接続するこのような ExpressRoute を最大 4 つ用意して、各 ExpressRoute をインターコネクト ゲートウェイのペアに接続することができます。

- ExpressRoute は最大 10 個の VNet に接続できます。インターコネクト ゲートウェイから ExpressRoute への接続を作成するときに、VNet を ExpressRoute にアタッチすることができます。VNet は、接続用に選択した VNet タグに基づいてアタッチされます。

  10 個を超える VNet に適用される VNet タグを選択した場合、または選択される VNet の総数が 10 個を超えるような VNet タグの組み合わせを選択した場合、インターコネクトの作成は失敗します。

（注） インターコネクト ゲートウェイからの接続を作成するときに ExpressRoute にアタッチできる VNet の数の決定では、Azure ポータルから ExpressRoute にアタッチした可能性のある VNet も考慮されます。

- VNet は、VNet ゲートウェイまたは ExpressRoute ゲートウェイに接続できます。そのため、VNet ゲートウェイを介した VNet へのプライベートピアリングを作成した場合、ExpressRoute ゲートウェイを介した同じ VNet へのプライベートピアリングを作成することはできません。その逆も同様です。
- VNet が仮想 WAN の仮想ハブに接続されている場合、同じ VNet を別の仮想 WAN に接続することはできません。
- 仮想 WAN の各リージョンには、仮想ハブが 1 つだけ存在する必要があります。
- リージョン内のすべての VNet は、同じリージョン内の単一の仮想ハブに接続する必要があります。
- デフォルトは冗長接続であり、この設定のみがサポートされています。Megaport ファブリック内のインターコネクト ゲートウェイのペアから Microsoft Azure への接続を作成する必要があります。

  Microsoft Azure ExpressRoute へのプライマリ接続とセカンダリ接続を作成するインターコネクト ゲートウェイのペアを選択するときは、インターコネクト ゲートウェイが BGP ピアリングに同じ BGP ASN を使用するように設定されていることを確認します。

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport に関する情報

SDCI プロバイダーである Megaport のファブリックに Cisco Catalyst 8000v Edge ソフトウェア（Cisco Catalyst 8000V）インスタンスを展開できます。さらに、Cisco Catalyst SD-WAN ファブリックを使用して、ブランチの場所を Cisco Catalyst 8000v インスタンスにリンクすることができます。ブランチの場所に最も近い Megaport の場所に Cisco Catalyst 8000v インスタンスを展開することをお勧めします。

Cisco Catalyst 8000v インスタンスは、Cisco Catalyst SD-WAN ファブリックではエッジデバイスとして機能し、Megaport ファブリックではインターコネクト ゲートウェイとして機能します。インターコネクト ゲートウェイから、Megaport ファブリック内の Cloud OnRamp または別のインターコネクト ゲートウェイへの直接レイヤ 2 接続（インターコネクト）を作成することができます。インターコネクトは、Megaport ファブリックを介してブランチの場所間をリンクするか、ブランチの場所とクラウド サービス プロバイダー間をリンクします。

（注） Megaport の用語では、インターコネクト ゲートウェイは Megaport Virtual Edge（MVE）とも呼ばれます。インターコネクト ゲートウェイから Cloud OnRamp または別のインターコネクト ゲートウェイへの直接レイヤ 2 接続は、仮想クロスコネクト（VXC）と呼ばれます。

このセットアップでは、Cisco Catalyst SD-WAN ファブリックがオーバーレイネットワークとして機能し、Megaport ファブリックがアンダーレイネットワークとして機能します。Megaport

ファブリックは、データセンターに依存しない、効率的な、高速、低遅延、高帯域幅の接続を、世界 700 ヵ所のデータセンター間で提供します。

インターコネクト ゲートウェイからの次のタイプの接続を作成できます。

表 *72*：接続のタイプ

接続先	接続のタイプ	開始リリース
Amazon Web Services	• Direct Connect：パブリックホスト型仮想インターフェイス（VIF） • Direct Connect：プライベートホスト型 VIF • Direct Connect：パブリックホスト型接続 • Direct Connect：プライベートホスト型接続 • Direct Connect：トランジットホスト型接続	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1
Google クラウド	Google Cloud Router へのパートナーインターコネクト アタッチメント	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1
Microsoft Azure	• パートナー ExpressRoute 回線：Microsoft ピアリング • パートナー ExpressRoute 回線：プライベートピアリング	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1
インターコネクト ゲートウェイ	インターコネクト ゲートウェイに接続された Cisco Catalyst SD-WAN のブランチの場所間のリンク	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1

Cisco SD-WAN Manager では、以下を行うことができます

- Megaport の場所での Cisco Catalyst 8000v インスタンスの設定と展開
- パブリッククラウドまたはプライベートクラウドへのソフトウェア定義型のクラウドインターコネクトの作成
- Megaport ファブリック全体で Cisco Catalyst SD-WAN のブランチの場所をリンクするためのインターコネクトの作成

このソリューションとともにサポートが提供されます。このソリューションに関するご質問や問題については、シスコサポートにお問い合わせください。

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport の利点

1. ブランチの場所が、Cisco Catalyst SD-WAN ファブリックを介して Megaport ファブリックにシームレスに接続します。
2. SLA が保証されたパブリッククラウドまたはプライベートクラウドへのインターコネクト。
3. Cisco Catalyst SD-WAN ファブリックを介したエンドツーエンドのトラフィックのセキュリティ、セグメンテーション、およびポリシー。
4. シスコが、請求、プロビジョニング、およびサポートの単一の連絡窓口となります。
5. Cisco SD-WAN Manager が、クラウドへの接続を管理するための単一のペインを提供します。
6. Cisco Catalyst SD-WAN ファブリックと Megaport SDN 全体のエンドツーエンドの可視性。
7. Cisco Catalyst SD-WAN のブランチの場所間、および Cisco Catalyst SD-WAN のブランチの場所とパブリッククラウドまたはプライベートクラウド間の、データセンターに依存しないリンク。

暗号化されたマルチクラウド インターコネクト

サポート対象の最小リリース：Cisco vManage リリース 20.9.1

Cisco SD-WAN Manager の Cloud OnRamp ワークフローを使用して、インターコネクト ゲートウェイとクラウド サービス プロバイダー間のセキュアなプライベート Cisco Catalyst SD-WAN 接続をプロビジョニングすることができます。クラウド インターコネクト プロバイダーのインターコネクト ゲートウェイから、マルチクラウドワークフローの一環として作成された既存のクラウドゲートウェイへの仮想クロスコネクトを終了できます。詳細については、「Cloud OnRamp for Multicloud （255 ページ）」を参照してください。この機能により、VPC および VNET ワークロードにアクセスするためのインターネットパスとプライベートパスの両方がサポートされます。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、暗号化されたマルチクラウド インターコネクトは、クラウド WAN ソリューションを使用した AWS クラウドゲートウェイをサポートしています。

利点

- クラウド インターコネクト プロバイダー バックボーンを介して、ブランチサイトからクラウドゲートウェイまでのエンドツーエンドの暗号化を提供します。
- 単一の仮想クロスコネクトで複数の VPN セグメントをサポートしています。

- 接続の作成前後の VPC および VNET タグの変更をサポートしています。VPN から VPC または VNET タグへのマッピングは、[Multicloud Intent Management] 画面を使用して実行できます。
- クラウド サービス プロバイダーによって課されるプレフィックス アドバタイズメントの制限を解消するために、ルートアドバタイズメントがインターコネクト ゲートウェイとクラウドゲートウェイによって制御されます。

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport の設定ワークフロー

前提条件の設定

1. Megaport アカウントを作成します。

   Cisco Commerce Workspace（CCW）での発注プロセスの一環として、アカウントの作成に関する電子メールを Megaport から受信します。詳細については、この電子メールを参照してください。

2. Megaport アカウントを Cisco SD-WAN Manager に関連付けます。
3. インターコネクト ゲートウェイのグローバル設定を構成します。
4. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
5. インターコネクト ゲートウェイとして展開する Cisco Catalyst 8000v インスタンスの UUID が必要な数あることを確認します。
6. Cisco Catalyst 8000v インスタンスに Megaport テンプレートをアタッチします。
7. Cisco Catalyst SD-WAN のブランチの場所に最も近い Megaport の場所でインターコネクト ゲートウェイを作成します。

   AWS への接続のために、Megaport の場所でインターコネクト ゲートウェイを作成します。

   Google Cloud への冗長接続のために、Megaport ファブリックでインターコネクト ゲートウェイのペアを作成します。非冗長接続の場合は、Megaport の場所にインターコネクト ゲートウェイを展開します。

   Microsoft Azure に接続するために、Megaport ファブリックにインターコネクト ゲートウェイのペアを作成します。デフォルトは冗長接続であり、この設定のみがサポートされています。

   Cisco Catalyst SD-WAN のブランチの場所間の接続のために、ブランチの場所ごとに、最も近い Megaport の場所でインターコネクト ゲートウェイを作成します。

AWS へのインターコネクトを作成するためのワークフロー

次の設定手順を実行する前に、前提条件が満たされ、前提条件の設定が適用されていることを確認してください。

1. AWS アカウントを Cisco SD-WAN Manager に関連付けます。
2. AWS 仮想プライベートクラウド（VPC）に接続するためのホストプライベートネットワークを検出します。
3. 次のいずれかのタイプの接続を作成します。

接続タイプ	ヒント
Direct Connect：パブリックホスト型仮想インターフェイス（VIF）	この接続は、パブリック AWS リソースへのリンクに使用します。リンクの帯域幅は 50 Mbps ～ 1 Gbps です。
Direct Connect：プライベートホスト型 VIF	この接続は、AWS VPC への専用リンクに使用します。リンクの帯域幅は 50 Mbps ～ 1 Gbps です。 **注**：接続の帯域幅は、購入した権限付与を超えることはできません。
Direct Connect：パブリックホスト型接続	この接続は、パブリック AWS リソースへのリンクに使用します。リンクの固定帯域幅は 1 Gbps 超です。
Direct Connect：プライベートホスト型接続	この接続は、AWS VPC への専用リンクに使用します。リンクの帯域幅は 1 Gbps 超です。
Direct Connect：トランジットホスト型接続	この接続は、トランジットゲートウェイを介した最大5,000の AWS VPC への専用リンクに使用します。リンクの帯域幅は 1 Gbps 超です。最大 3 つのトランジットゲートウェイを Direct Connect ゲートウェイにアタッチし、最大 15,000 の VPC に接続することができます。

Cisco Catalyst SD-WAN のブランチの場所をリンクするためのワークフロー

次の設定手順を実行する前に、前提条件が満たされ、前提条件の設定が適用されていることを確認してください。

- インターコネクト ゲートウェイ間のインターコネクトを作成します。

Google Cloud へのインターコネクトを作成するためのワークフロー

次の設定手順を実行する前に、前提条件が満たされ、前提条件の設定が適用されていることを確認してください。

1. Google Cloud ポータルを使用して、必要な VPC ネットワークを作成します。
2. 接続するネットワークリージョンに Google Cloud Router を展開します。

非冗長接続の場合は、Google Cloud ポータルを使用して、接続する各ネットワークリージョンに Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成します。

冗長接続の場合は、Google Cloud ポータルを使用して、接続する各ネットワークリージョンに 2 つの Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成します。

3. Google Cloud アカウントを Cisco SD-WAN Manager に関連付けます。
4. インターコネクト ゲートウェイから Google Cloud Router へのインターコネクトを作成します

Microsoft Azure へのインターコネクトを作成するためのワークフロー

次の設定手順を実行する前に、前提条件が満たされ、前提条件の設定が適用されていることを確認してください。

1. Microsoft Azure アカウントを Cisco SD-WAN Manager に関連付けます。
2. 必要な Azure ExpressRoute 回線を作成します。
3. Azure Virtual Network（VNet）に接続するためのホスト プライベート ネットワークを検出します。
4. 次のいずれかのタイプの接続を作成します。
   - Azure ExpressRoute へのパブリック ピアリング接続
   - Azure ExpressRoute へのプライベート ピアリング接続

Cisco SD-WAN Cloud Interconnect with Megaport の前提条件の設定

Cisco SD-WAN Manager と Megaport アカウントの関連付け

前提条件

Megaport アカウントを作成します。Cisco Commerce Workspace（CCW）での発注プロセスの一環として、アカウントの作成に関する電子メールを Megaport から受信します。詳細については、この電子メールを参照してください。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。

2. [Interconnect] をクリックします。
3. [Associate Interconnect Account] をクリックします。
4. 次を設定します。

Interconnect Provider	[Megaport] を選択します。
アカウント名	任意の名前を入力します。この名前は、クラウドまたはサイト間インターコネクトを定義するワークフローでMegaportアカウントを識別するために使用されます。 （注） Cisco vManage リリース 20.6.1 以降では、アカウント名にスペースを使用することはできません。Cisco SD-WAN Manager を Cisco vManage リリース 20.5.1 から Cisco vManage リリース 20.6.1 にアップグレードする場合は、アカウント名のスペースを削除するか、スペースを'_'に置き換えてください。
[説明（Description）]（任意）	説明を入力します。
ユーザー名	Megaport アカウントのユーザー名を入力します。
[パスワード（Password）]	Megaport アカウントのパスワードを入力します。

5. [Add] をクリックします。

Cisco SD-WAN Manager はアカウントを認証し、アカウントの詳細をデータベースに保存します。

インターコネクト ゲートウェイのグローバル設定の構成

前提条件

1. Megaport アカウントを作成します。Cisco Commerce Workspace（CCW）での発注プロセスの一環として、アカウントの作成に関する電子メールをMegaportから受信します。詳細については、この電子メールを参照してください。
2. Megaport アカウントを Cisco SD-WAN Manager に関連付けます。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。

3. [Interconnect Global Settings] をクリックします。
   1. グローバル設定を追加するには、[Add] をクリックします。
   2. グローバル設定を変更するには、[Edit] をクリックします。
4. 次を設定します。

設定グループの有効化	Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、このオプションを有効にして、設定グループを使用してマルチクラウドワークフローでデバイスを設定します。 このオプションは、デフォルトで無効です。 （注） ここで設定グループを有効にすると、すべてのクラウドプロバイダーに対して設定グループが有効になります。たとえば、ここでこのオプションを有効にすると、他のすべてのマルチクラウドおよびインターコネクト プロバイダーの設定グループも有効になります。
Interconnect Provider	[Megaport] を選択します。
ソフトウェア イメージ	Catalyst 8000v イメージを選択します。
Instance Size	インスタンスのサイズは、各 Cisco Catalyst 8000v インスタンスのコンピューティング フットプリントとスループットを決定します。次のいずれかを選択します。 • [Small]：2vCPU、8GB DRAM、500 Mbps • [Medium]：4vCPU、16GB DRAM、1 Gbps • [Large]：8vCPU、32GB DRAM、5 Gbps
Interconnect Transit Color	インターコネクト ゲートウェイ間の接続に割り当てる色を選択します。 この色は、ブランチの場所間を直接ピアリングしないように制限されています。同じ色を Cisco Catalyst SD-WAN ファブリック内の別の接続に割り当てないでください。 （注） プライベートの色を使用することをお勧めします。デフォルトの色は使用しないでください。
BGP ASN	インターコネクト ゲートウェイとクラウドプロバイダー間のピアリングに使用される BGP ASN を入力します。 任意の ASN を入力するか、組織で使用されている既存の ASN を再利用できます。

Interconnect CGW SDWAN Color	サポート対象の最小リリース：Cisco vManage リリース 20.9.1 インターコネクト ゲートウェイがクラウドゲートウェイに接続する際のインターフェイスに使用する色を選択します。 （注）インターフェイスに割り当てられる色は、インターコネクト ゲートウェイ デバイスに対して一意であり、クラウドインターコネクト プロバイダー間では共通である必要があります。 Microsoft Azure 展開では、クラウドゲートウェイの WAN インターフェイスで Cisco Catalyst SD-WAN トンネルの色は自動的に設定されないため、WANインターフェイスの色を手動で更新する必要があります。テンプレートの色がブランチルータ、インターコネクト ゲートウェイ、およびクラウドゲートウェイの色と一致していることを確認します。

5. 新しく追加したグローバル設定を保存するには、[Save] をクリックします。

   変更したグローバル設定を保存するには、[Update] をクリックします。

Cisco Catalyst 8000v インスタンスへの Megaport テンプレートのアタッチ

（注） 設定グループを有効にした場合、この手順は必要ありません。この場合は、「Create Interconnect Gateway at a Megaport Location」に進みます。

Megaport の場所で Cisco Catalyst 8000v インスタンスをインターコネクト ゲートウェイとして展開する前に、Megaport のデフォルトテンプレートをデバイスにアタッチする必要があります。Default_MEGAPORT_ICGW_C8000V_Template_V01 という名前のテンプレートをアタッチすることを推奨します。

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 20.7.1 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Template Type] として [Default] を選択し、Default_MEGAPORT_ICGW_C8000V_Template_V01 という名前のテンプレートを見つけます。

4. このテンプレートについて、[...] をクリックし、[Attach Devices] をクリックします。
5. [Available Devices] から Cisco Catalyst 8000v インスタンスを選択し、[Selected Devices] に移動します。[Attach] をクリックします。
6. 以下を設定し、[Next] をクリックします。
   - 色
   - ホストネーム
   - システム IP
   - サイト ID
7. [Configure Devices] をクリックします。

Megaport の場所でのインターコネクト ゲートウェイの作成

目的の Megaport の場所に、インターコネクト ゲートウェイとして Cisco Catalyst 8000v インスタンスを展開します。ブランチの場所に最も近い Megaport の場所に Cisco Catalyst 8000v インスタンスを展開することをお勧めします。

はじめる前に

1. Megaport アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 設定グループを有効にしない場合は、Cisco Catalyst 8000v インスタンスに Megaport テンプレートをアタッチします。
4. 設定グループを有効にする場合は、設定グループに関連付けられているデバイスのデバイスパラメータを設定していることを確認します。
5. Cisco vManage リリース 20.9.1 以降では、インターコネクト ゲートウェイを作成するために必要なライセンスがあることを確認します。必要なライセンスがないと、インターコネクト ゲートウェイの作成は失敗します。詳細については、「License Management for Cisco SD-WAN Cloud Interconnect with Megaport」を参照してください。

Megaport の場所でのインターコネクト ゲートウェイの作成

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Create Interconnect Gateway] をクリックします。
4. 次を設定します。

Interconnect Provider	[Megaport] を選択します。
ゲートウェイ名	ゲートウェイを一意に識別する名前を入力します。
Description（オプション）	説明を入力します。
Account Name	Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Megaport アカウントを選択します。 （最小リリース：Cisco vManage リリース 20.9.1）アカウントに関連付けられているインターコネクト ゲートウェイ ライセンスを表示するには、[Check available licenses] をクリックします。
Location	1. [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 2. Cisco 8000v インスタンスを展開する必要がある Megaport の場所を選択します。
Provider License Type	（最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.14.1）次のいずれかを選択します。 • [Prepaid]：インターコネクト ゲートウェイを作成するために、プリペイドライセンスタイプを選択します。Cisco Catalyst SD-WAN Manager リリース 20.14.1 より前では、デフォルトではプリペイドライセンスタイプのみが使用可能でした。 • [PayG]：インターコネクト ゲートウェイを作成するために、従量制課金（PAYG）ライセンスタイプを選択します。
IP トランジット	（最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.14.1）IP トランジット帯域幅の値を選択します。
NHM Region	（最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.14.1）ドロップダウンリストから、インターコネクト ゲートウェイを作成するネットワークの正常性のモニタリング（NHM）のリージョンを選択します。
サイト名	（最小リリース：Cisco vManage リリース 20.10.1）ドロップダウンリストから、インターコネクト ゲートウェイを作成するサイトを選択します。

設定グループ	Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、クラウドゲートウェイを作成したとき、またはインターコネクト ゲートウェイのグローバル設定を構成したときに [Enable Configuration Group] オプションを有効にした場合は、次のいずれかのアクションを実行します。 • 構成グループを選択します。 • 新しい設定グループを作成して使用するには、[Create New] を選択します。[Create Configuration Group] ダイアログボックスで、新しい設定グループの名前を入力し、[Done] をクリックします。ドロップダウンリストから新しい設定グループを選択します。 選択した設定グループは、マルチクラウドワークフローでデバイスを設定するために使用されます。 設定グループの詳細については、『Cisco Catalyst SD-WAN Configuration Groups』を参照してください。 （注） [Configuration Group] ドロップダウンリストには、このドロップダウンリストから作成した設定グループのみが含まれています。Cisco Catalyst SD-WAN で作成された他の設定グループは含まれません。このドロップダウンリストの設定グループには、このプロバイダーに必要なオプションが含まれています。
[Chassis Number]	Megaport のデフォルトテンプレートがアタッチされている Cisco Catalyst 8000v インスタンスのシャーシ番号を選択します。 （注） Cisco vManage リリース 20.10.1 以降では、[Site Name] ドロップダウンリストからサイトを選択すると、シャーシ番号が自動的に入力されます。
Instance Settings	次のいずれかを選択します。 • [Default]：インターコネクトのグローバル設定で定義されたインスタンスサイズとソフトウェアイメージを使用します。 • [Custom]：このゲートウェイの特定のインスタンスサイズとソフトウェアイメージを選択します。

MRF Role	（最小リリース：Cisco vManage リリース 20.10.1）[Border] または [Edge] のルータロールを選択します。 このオプションは、マルチリージョン ファブリックが有効になっている場合にのみ使用できます。
トランスポートゲートウェイ（**Transport Gateway**）	（最小リリース：Cisco vManage リリース 20.10.1）[Enabled] または [Disabled] を選択します。 このオプションは、マルチリージョン ファブリックが有効になっている場合にのみ使用できます。

5. [Add] をクリックします。

設定タスクが成功すると、インターコネクト ゲートウェイが [Gateway Management] ページにリストされます。

インターコネクト ゲートウェイからの接続のライセンスタイプは、ゲートウェイのライセンスタイプと同じです。たとえば、ゲートウェイがプリペイドライセンスタイプで展開されている場合、そのゲートウェイからの接続もプリペイドライセンスを消費します。

AWS へのインターコネクトの作成

AWS アカウントと Cisco SD-WAN Manager の関連付け

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Cloud] をクリックします。
3. [Associate Cloud Account] をクリックします。
4. 次を設定します。

Cloud Provider	[Amazon Web Services] を選択します。
Cloud Account Name	任意の名前を入力します。
[説明（Description）]（任意）	説明を入力します。
Use for Cloud Gateway	[No] を選択します。
Log in to AWS with	[Key] または [IAM Role] を選択します。
Role ARN	API/秘密キーまたはロール ARN を入力します。

5. [Add] をクリックします。

Cisco SD-WAN Manager は、AWS への接続を作成するための API ワークフローの一環として、API/秘密キーまたはロール ARN を使用して AWS でユーザーアカウントを認証します。

ホスト プライベート ネットワークの検出と AWS VPC のタグ付け

複数のホスト VPC を、タグを使用してグループ化できます。同じタグの下の VPC は、単一のユニットと見なされます。インターコネクト ゲートウェイからのソフトウェア定義型のクラウドインターコネクトを作成する AWS VPC にタグを付けます。

前提条件

AWS アカウントを Cisco SD-WAN Manager に関連付けます。

タグの追加

VPC をグループ化し、まとめてタグ付けします。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Host Private Networks] をクリックします。
4. [Cloud Provider]：[Amazon Web Services] を選択します。

   使用可能なホスト VPC が検出され、表に一覧表示されます。
5. 左端の列のチェックボックスを使用して、タグ付けする VPC を選択します。
6. [Tag Actions] をクリックします。
7. [Add Tag] をクリックして、以下を設定します。

フィールド	説明
[Tag Name]	選択した VPC をリンクするタグの名前を入力します。
[地域（Region）]	選択した VPC に対応するリージョンのリスト。タグからリージョンおよび関連する VPC を除外するには、[X] をクリックします。
Selected VPCs	選択したホスト VPC の VPC ID のリスト。タグから VPC を除外するには、[X] をクリックします。

フィールド	説明
（Cisco vManage リリース 20.9.1 以降）[Enable for SDCI partner Interconnect Connections] （Cisco vManage リリース 20.8.1 以前）[Enable for Interconnect Connectivity]	AWS へのクラウドインターコネクト接続を作成するときに VPC タグを使用するには、このチェックボックスをオンにします。 有効にすると、タグはクラウドインターコネクト接続にのみ使用でき、マルチクラウドゲートウェイ インテントマッピングには使用できません。 このチェックボックスをオンにしない場合、VPC タグを使用してクラウドインターコネクト接続を作成することはできません。 （注） クラウドゲートウェイを使用して VPC ワークロードを接続する場合、この設定を有効にしないでください。タグが接続で使用されている場合は、この設定を編集できません。

8. [Add] をクリックします。

[Discover Host Private Networks] ページで、選択した VPC にタグが付けられ、タグ名が [Host VPC Tag] 列に表示されます。ソフトウェア定義型のクラウドインターコネクトに VPC タグを使用することを選択した場合、[Interconnect Enabled] 列に [Yes] と表示されます。

タグの編集

既存のタグに VPC を追加するか、既存のタグから VPC を削除します。

Cisco vManage リリース 20.10.1 以降では、次の条件に従ってインターコネクト接続に関連付けられた VPC タグを編集します。

- 1 つの VPC のみが VPC タグに関連付けられている場合、タグから VPC を削除することはできません。タグから VPC を削除するには、インターコネクト接続を削除してからタグを編集します。
- トランジットホスト型接続の場合、タグに関連付ける VPC は、そのタグにすでに関連付けられている VPC と同じリージョンからのものである必要があります。

  新しいリージョンの VPC をトランジットホスト型接続にアタッチするには、次の手順を実行します。

  1. リージョンの新しいタグを作成し、必要な VPC を関連付けます。
  2. トランジットホスト型接続を編集し、VPC タグを接続にアタッチします。

- プライベート VIF またはプライベートホスト型接続の場合、タグの編集中に新しいリージョンからの VPC を関連付けることができます。

（注） Cisco vManage リリース 20.9.1 以前のリリースでは、インターコネクト接続に関連付けられている VPC タグを編集することはできません。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Host Private Networks] をクリックします。
4. [Cloud Provider]：[Amazon Web Services] を選択します。

   使用可能なホスト VPC が検出され、表に一覧表示されます。
5. [Tag Actions] をクリックします。
6. [Edit Tag] をクリックし、必要に応じて以下を変更します。

フィールド	説明
[Tag Name]	ドロップダウンリストからタグ名を選択します。
[地域（Region）]	このフィールドには、タグに関連付けられた VPC に対応するリージョンのリストが表示されます。 • ドロップダウンリストから追加のリージョンを選択します。 • タグからリージョンおよび関連する VPC を除外するには、[X] をクリックします。
Selected VPCs	このフィールドには、タグに関連付けられている VPC のリストが表示されます。 • ドロップダウンリストから追加の VPC を選択します。 • タグから VPC を除外するには、[X] をクリックします。
（Cisco vManage リリース 20.9.1 以降）[Enable for SDCI partner Interconnect Connections] （Cisco vManage リリース 20.8.1 以前）[Enable for Interconnect Connectivity]	（読み取り専用）VPC をインターコネクト接続の設定中に使用するように設定されているか、またはマルチクラウドゲートウェイのインテントマッピングに使用するように設定されているかを示します。

7. [更新（Update）]をクリックします。

タグの削除

VPC をグループ化しているタグを削除します。

（注） VPC タグがインターコネクト接続に関連付けられている間は、タグを削除できません。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Host Private Networks] をクリックします。
4. [Cloud Provider]：[Amazon Web Services] を選択します。

   使用可能なホスト VPC が検出され、表に一覧表示されます。
5. [Tag Actions] をクリックします。
6. [タグを削除（Delete Tag）]をクリックします。
7. [Tag Name]：ドロップダウンリストからタグ名を選択します。
8. [Delete] をクリックします。

インターコネクト ゲートウェイから AWS への Direct Connect パブリックホスト型 VIF の作成

前提条件

1. Megaport アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. AWS アカウントを Cisco SD-WAN Manager に関連付けます。
5. Cisco Catalyst 8000v インスタンスに Megaport テンプレートをアタッチします。
6. Megaport の場所でインターコネクト ゲートウェイを作成します。
7. Cisco vManage リリース 20.9.1 以降では、接続を作成するために必要なライセンスがあることを確認します。必要なライセンスがないと、接続の作成は失敗します。詳細については、「Cisco Catalyst SD-WAN Cloud Interconnect with Megaport のライセンス管理」を参照してください。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[MEGAPORT] を選択します。

（注） このフィールドは Cisco vManage リリース 20.6.1 で導入されました。

5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Megaport アカウントを選択します。
6. [Choose Interconnect Gateway]：Direct Connect 接続を作成する元となるインターコネクトゲートウェイを選択します。
7. （最小リリース：Cisco vManage リリース 20.9.1）Megaport アカウントに関連付けられている利用可能なインターコネクトライセンスを表示するには、[Check available licenses] をクリックします。
8. [Add Connection] をクリックします。
9. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービスプロバイダー	[AWS] を選択します。
Connection Name	接続の一意の名前を入力します。
接続タイプ	[Hosted VIF] を選択します。
AWS Account	Cisco SD-WAN Manager で AWS アカウントの詳細を関連付ける際に入力したアカウント名で AWS アカウントを選択します。

10. 以下を設定し、[Next] をクリックします。

VIF Type	[Public] を選択します。
参照先	1. [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 2. AWS Direct Connect の場所を選択します。
帯域幅	接続帯域幅を指定します。 単位：Mbps。

Interconnect IP Address	インターコネクト ゲートウェイの BGP ピア ID として使用するパブリック IP アドレス（CIDR）を入力します。
Amazon IP Address	AWS BGP ピア ID として使用するパブリック IP アドレス（CIDR）を入力します。
Prefixes	AWS にアドバタイズするサマリーアドレスとプレフィックスを入力します。
Segment	この接続のセグメント ID を選択します。

11. 接続の概要を確認します。
    - 接続を作成するには、[Save] をクリックします。
    - 接続設定を変更するには、[Back] をクリックします。

設定タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect プライベートホスト型 VIF の作成

前提条件

1. Megaport アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. AWS アカウントを Cisco SD-WAN Manager に関連付けます。
5. ホスト プライベート ネットワークを検出して AWS VPC にタグ付けします。
6. Cisco Catalyst 8000v インスタンスに Megaport テンプレートをアタッチします。
7. Megaport の場所でインターコネクト ゲートウェイを作成します。
8. Cisco vManage リリース 20.9.1 以降では、接続を作成するために必要なライセンスがあることを確認します。必要なライセンスがないと、接続の作成は失敗します。詳細については、「License Management for Cisco SD-WAN Cloud Interconnect with Megaport」を参照してください。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。

3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[MEGAPORT] を選択します。

（注） このフィールドは Cisco vManage リリース 20.6.1 で導入されました。

5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Megaport アカウントを選択します。
6. [Choose Interconnect Gateway]：Direct Connect 接続を作成する元となるインターコネクトゲートウェイを選択します。
7. （最小リリース：Cisco vManage リリース 20.9.1）Megaport アカウントに関連付けられている利用可能なインターコネクトライセンスを表示するには、[Check available licenses] をクリックします。
8. [Add Connection] をクリックします。
9. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウド サービス プロバイダー	[AWS] を選択します。
Connection Name	接続の一意の名前を入力します。
接続タイプ	[Hosted VIF] を選択します。
AWS Account	Cisco SD-WAN Manager で AWS アカウントの詳細を関連付ける際に入力したアカウント名で AWS アカウントを選択します。

10. 以下を設定し、[Next] をクリックします。

VIF Type	[Private] を選択します。
参照先	1. [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 2. AWS Direct Connect の場所を選択します。 （注） AWS GovCloud 以外のアカウントには、AWS GovCloud の場所を使用しないことを推奨します。
帯域幅	接続帯域幅を指定します。 単位：Mbps。

Direct Connect Gateway	**1.** [Refresh] ボタンをクリックして、選択した AWS アカウントに関連付けられている Direct Connect ゲートウェイを取得します。 **2.** Direct Connect 接続を作成する必要がある先の Direct Connect ゲートウェイを選択します。 または、[Add New Direct Connect Gateway] をクリックして、新しい Direct Connect ゲートウェイを作成します。 **1.** [Gateway Name] を入力します。 **2.** ゲートウェイの [BGP ASN] を入力します。 **3.** [Save] をクリックします。

設定	次のいずれかを選択します。 • [Global]： • BGP ピアリング IP アドレスは、内部で予約済みの /16 サブネットから選択されます。 Cisco vManage リリース 20.5.1 では、IP アドレスはサブネット 192.168.0.0/16 から選択されます。Cisco vManage リリース 20.6.1 以降では、IP アドレスはサブネット 198.18.0.0/16 から選択されます。 • BGP ASN は、グローバル設定から選択されます。 • [Custom]： • BGP ピアリングのカスタム /30 CIDR IP アドレスを入力します。 • ピアリング用のカスタム BGP ASN を入力します。 • Cisco vManage リリース 20.8.1 以降： • カスタムサブネットの IP アドレスは、10.0.0.0/8、172.16.0.0/12、192.168.0.0/16 の範囲にある必要があります。 • カスタムサブネットは /30 として指定する必要があります。 • カスタムサブネットは、172.31.251.0/21 と競合しないようにする必要があります。 • カスタムサブネットは、他の接続に使用されるサブネットと競合することはできません。 （注） インターコネクト ゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN を指定できます。インターコネクト ゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。
Segment	この接続のセグメント ID を選択します。

添付ファイル	Cisco vManage リリース 20.8.1 以前の場合： [VPC] を選択します。 [VPC Tags]：VPC タグを選択して、この接続を介してトラフィックをルーティングする必要がある VPC を識別します。
	Cisco vManage リリース 20.9.1 以降の場合： 次のいずれかを選択します。 • **VPC** [Segment]：この接続のセグメント ID を選択します。 [VPC Tags]：VPC タグを選択して、この接続を介してトラフィックをルーティングする必要がある VPC を識別します。 • Cloud Gateway [Cloud Gateways]：この接続にアタッチするクラウドゲートウェイを選択します。ドロップダウンが空の場合は、最初にマルチクラウドワークフローを使用してクラウドゲートウェイを作成する必要があります。単一接続の場合、AWS は最大 10 個のクラウドゲートウェイをサポートします。各クラウドゲートウェイは、30 個のインターコネクト接続に接続できます。

11. 接続の概要を確認します。
    - 接続を作成するには、[Save] をクリックします。
    - 接続設定を変更するには、[Back] をクリックします。

設定タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

インターコネクト ゲートウェイから AWS への Direct Connect パブリックホスト型接続の作成

前提条件

1. Megaport アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. AWS アカウントを Cisco SD-WAN Manager に関連付けます。

5. Cisco Catalyst 8000v インスタンスに Megaport テンプレートをアタッチします。
6. Megaport の場所でインターコネクト ゲートウェイを作成します。
7. Cisco vManage リリース 20.9.1 以降では、接続を作成するために必要なライセンスがあることを確認します。必要なライセンスがないと、接続の作成は失敗します。詳細については、「Cisco Catalyst SD-WAN Cloud Interconnect with Megaport のライセンス管理」を参照してください。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[MEGAPORT] を選択します。

（注） このフィールドは Cisco vManage リリース 20.6.1 で導入されました。

5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Megaport アカウントを選択します。
6. [Choose Interconnect Gateway]：Direct Connect 接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. （最小リリース：Cisco vManage リリース 20.9.1）Megaport アカウントに関連付けられている利用可能なインターコネクトライセンスを表示するには、[Check available licenses] をクリックします。
8. [Add Connection] をクリックします。
9. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウド サービス プロバイダー	[AWS] を選択します。
Connection Name	接続の一意の名前を入力します。
接続タイプ	[Hosted Connection] を選択します。
AWS Account	Cisco vManage で AWS アカウントの詳細を関連付ける際に入力したアカウント名で AWS アカウントを選択します。

10. 以下を設定し、[Next] をクリックします。

Connection VIF Type	[Public] を選択します。
参照先	1. [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 2. AWS Direct Connect の場所を選択します。
帯域幅	接続帯域幅を指定します。 単位：Mbps。
Interconnect IP Address	インターコネクト ゲートウェイの BGP ピア ID として使用するパブリック IP アドレス（CIDR）を入力します。
Amazon IP Address	AWS BGP ピア ID として使用するパブリック IP アドレス（CIDR）を入力します。
Prefixes	ブランチの場所にアドバタイズするサマリー AWS アドレスとプレフィックスを入力します。
Segment	この接続のセグメント ID を選択します。

11. 接続の概要を確認します。
    - 接続を作成するには、[Save] をクリックします。
    - 接続設定を変更するには、[Back] をクリックします。

設定タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect プライベートホスト型接続の作成

前提条件

1. Megaport アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. AWS アカウントを Cisco SD-WAN Manager に関連付けます。
5. ホスト プライベート ネットワークを検出して AWS VPC にタグ付けします。
6. Cisco Catalyst 8000v インスタンスに Megaport テンプレートをアタッチします。
7. Megaport の場所でインターコネクト ゲートウェイを作成します。

8. Cisco vManage リリース 20.9.1 以降では、接続を作成するために必要なライセンスがあることを確認します。必要なライセンスがないと、接続の作成は失敗します。詳細については、「License Management for Cisco SD-WAN Cloud Interconnect with Megaport」を参照してください。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[MEGAPORT] を選択します。

（注） このフィールドは Cisco vManage リリース 20.6.1 で導入されました。

5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Megaport アカウントを選択します。
6. [Choose Interconnect Gateway]：Direct Connect 接続を作成する元となるインターコネクトゲートウェイを選択します。
7. （最小リリース：Cisco vManage リリース 20.9.1）Megaport アカウントに関連付けられている利用可能なインターコネクトライセンスを表示するには、[Check available licenses] をクリックします。
8. [Add Connection] をクリックします。
9. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウド サービス プロバイダー	[AWS] を選択します。
Connection Name	接続の一意の名前を入力します。
接続タイプ	[Hosted Connection] を選択します。
AWS Account	Cisco SD-WAN Manager で AWS アカウントの詳細を関連付ける際に入力したアカウント名で AWS アカウントを選択します。

10. 以下を設定し、[Next] をクリックします。

Connection VIF Type	[Private] を選択します。

参照先	**1.** [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 **2.** AWS Direct Connect の場所を選択します。 （注） AWS GovCloud 以外のアカウントには、AWS GovCloud の場所を使用しないことを推奨します。
帯域幅	接続帯域幅を指定します。 単位：Mbps。
Direct Connect Gateway	**1.** [Refresh] ボタンをクリックして、選択した AWS アカウントに関連付けられている Direct Connect ゲートウェイを取得します。 **2.** Direct Connect 接続を作成する必要がある先の Direct Connect ゲートウェイを選択します。 または、[Add New Direct Connect Gateway] をクリックして、新しい Direct Connect ゲートウェイを作成します。 **1.** [Gateway Name] を入力します。 **2.** ゲートウェイの [BGP ASN] を入力します。 **3.** [Save] をクリックします。

設定	次のいずれかを選択します。 • [Global]： • BGP ピアリング IP アドレスは、内部で予約済みの /16 サブネットから選択されます。 Cisco vManage リリース 20.5.1 では、IP アドレスはサブネット 192.168.0.0/16 から選択されます。Cisco vManage リリース 20.6.1 以降では、IP アドレスはサブネット 198.18.0.0/16 から選択されます。 • BGP ASN は、グローバル設定から選択されます。 • [Custom]： • BGP ピアリングのカスタム /30 CIDR IP アドレスを入力します。 • ピアリング用のカスタム BGP ASN を入力します。 • Cisco vManage リリース 20.8.1 以降： • カスタムサブネットの IP アドレスは、10.0.0.0/8、172.16.0.0/12、192.168.0.0/16 の範囲にある必要があります。 • カスタムサブネットは /30 として指定する必要があります。 • カスタムサブネットは、172.31.251.0/21 と競合しないようにする必要があります。 • カスタムサブネットは、他の接続に使用されるサブネットと競合することはできません。 （注） インターコネクト ゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN を指定できます。インターコネクト ゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。
Segment	この接続のセグメント ID を選択します。

添付ファイル	Cisco vManage リリース 20.8.1 以前の場合： [VPC] を選択します。 [VPC Tags]：VPC タグを選択して、この接続を介してトラフィックをルーティングする必要がある VPC を識別します。
	Cisco vManage リリース 20.9.1 以降の場合： 次のいずれかを選択します。 • **VPC** [Segment]：この接続のセグメント ID を選択します。 [VPC Tags]：VPC タグを選択して、この接続を介してトラフィックをルーティングする必要がある VPC を識別します。 • Cloud Gateway [Cloud Gateways]：この接続にアタッチするクラウドゲートウェイを選択します。ドロップダウンが空の場合は、最初にマルチクラウドワークフローを使用してクラウドゲートウェイを作成する必要があります。単一接続の場合、AWS は最大 10 個のクラウドゲートウェイをサポートします。各クラウドゲートウェイは、30 個のインターコネクト接続に接続できます。

11. 接続の概要を確認します。
    - 接続を作成するには、[Save] をクリックします。
    - 接続設定を変更するには、[Back] をクリックします。

設定タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect トランジットホスト型接続の作成

前提条件

1. Megaport アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。

4. AWS アカウントを Cisco SD-WAN Manager に関連付けます。
5. ホスト プライベート ネットワークを検出して AWS VPC にタグ付けします。
6. Cisco Catalyst 8000v インスタンスに Megaport テンプレートをアタッチします。
7. Megaport の場所でインターコネクト ゲートウェイを作成します。
8. Cisco vManage リリース 20.9.1 以降では、接続を作成するために必要なライセンスがあることを確認します。必要なライセンスがないと、接続の作成は失敗します。詳細については、「License Management for Cisco SD-WAN Cloud Interconnect with Megaport」を参照してください。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[MEGAPORT] を選択します。

（注） このフィールドは Cisco vManage リリース 20.6.1 で導入されました。

5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Megaport アカウントを選択します。
6. [Choose Interconnect Gateway]：Direct Connect 接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. （最小リリース：Cisco vManage リリース 20.9.1）Megaport アカウントに関連付けられている利用可能なインターコネクトライセンスを表示するには、[Check available licenses] をクリックします。
8. [Add Connection] をクリックします。
9. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウド サービス プロバイダー	[AWS] を選択します。
Connection Name	接続の一意の名前を入力します。
接続タイプ	[Hosted Connection] を選択します。

AWS Account	Cisco SD-WAN Manager で AWS アカウントの詳細を関連付ける際に入力したアカウント名で AWS アカウントを選択します。

10. 以下を設定し、[Next] をクリックします。

Connection VIF Type	[Transit] を選択します。
参照先	**1.** [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 **2.** AWS Direct Connect の場所を選択します。 （注） AWS GovCloud 以外のアカウントには、AWS GovCloud の場所を使用しないことを推奨します。
帯域幅	接続帯域幅を指定します。 単位：Mbps。
Direct Connect Gateway	**1.** [Refresh] ボタンをクリックして、選択した AWS アカウントに関連付けられている Direct Connect ゲートウェイを取得します。 **2.** Direct Connect 接続を作成する必要がある先の Direct Connect ゲートウェイを選択します。 または、[Add New Direct Connect Gateway] をクリックして、新しい Direct Connect ゲートウェイを作成します。 **1.** [Gateway Name] を入力します。 **2.** ゲートウェイの [BGP ASN] を入力します。 **3.** [Save] をクリックします。

設定	次のいずれかを選択します。 • [Global]： • BGP ピアリング IP アドレスは、内部で予約済みの /16 サブネットから選択されます。 Cisco vManage リリース 20.5.1 では、IP アドレスはサブネット 192.168.0.0/16 から選択されます。Cisco vManage リリース 20.6.1 以降では、IP アドレスはサブネット 198.18.0.0/16 から選択されます。 • BGP ASN は、グローバル設定から選択されます。 • [Custom]： • BGP ピアリングのカスタム /30 CIDR IP アドレスを入力します。 • ピアリング用のカスタム BGP ASN を入力します。 • Cisco vManage リリース 20.8.1 以降： • カスタムサブネットの IP アドレスは、10.0.0.0/8、172.16.0.0/12、192.168.0.0/16 の範囲にある必要があります。 • カスタムサブネットは /30 として指定する必要があります。 • カスタムサブネットは、172.31.251.0/21 と競合しないようにする必要があります。 • カスタムサブネットは、他の接続に使用されるサブネットと競合することはできません。 （注） インターコネクト ゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN を指定できます。インターコネクト ゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。
Segment	この接続のセグメント ID を選択します。

添付ファイル	[Transit Gateway] を選択します。 [Transit Gateway]： **1.** [Refresh] ボタンをクリックして、選択した AWS アカウントに関連付けられているトランジットゲートウェイを取得します。 **2.** Direct Connect 接続を作成する必要があるトランジットゲートウェイを選択します。 または、[Add New Transit Gateway] をクリックして、新しいトランジットゲートウェイを作成します。 **1.** [Gateway Name] を入力します。 **2.** ゲートウェイの [BGP ASN] を入力します。 **3.** [AWS Region] を選択します。 **4.** [Save] をクリックします。 [VPC Tags]：VPC タグを選択して、この接続を介してトラフィックをルーティングする必要がある VPC を識別します。 [Add Prefixes] をクリックします。 選択した VPC の IPv4 CIDR プレフィックスを入力します。AWS VPC ダッシュボードから IPv4 CIDR アドレスを見つけることができます。

11. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。
- 接続設定を変更するには、[Back] をクリックします。

設定タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

Google Cloud へのインターコネクトの作成

Cisco SD-WAN Manager と Google Cloud アカウントの関連付け

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。

2. [Cloud] をクリックします。

3. [Associate Cloud Account] をクリックします。
4. 次を設定します。

Cloud Provider	[Google Cloud] を選択します。
Cloud Account Name	任意の名前を入力します。
[説明（Description）]（任意）	説明を入力します。
Use for Cloud Gateway	[No] を選択します。
Private Key ID	[Upload Credential File] をクリックします。 このファイルは、Google Cloud コンソールにログインして生成する必要があります。秘密キー ID は、JSON または REST API 形式の場合があります。形式は、キーの生成方法によって異なります。詳細については、Google Cloud のドキュメントを参照してください。

5. [Add] をクリックします。

Cisco SD-WAN Manager は、Google Cloud への接続を作成するためのワークフローの一環として、この秘密キー ID を使用して Google Cloud でユーザーアカウントを認証します。

インターコネクト ゲートウェイから Google Cloud Router へのインターコネクトの作成

前提条件

1. Google Cloud コンソールを使用して、必要な VPC ネットワークを作成します。
2. 接続するネットワークリージョンに Google Cloud Router を展開します。

   非冗長接続の場合は、Google Cloud コンソールで、接続する各ネットワークリージョンに Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成します。

   冗長接続の場合は、Google Cloud コンソールで、接続する各ネットワークリージョンに 2 つの Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成します。

（注） インターコネクト アタッチメントで使用するには、Google Cloud Router の Google ASN を 16550 に設定する必要があります。

3. Megaport アカウントを Cisco SD-WAN Manager に関連付けます。

4. インターコネクト ゲートウェイのグローバル設定を構成します。
5. Cisco Catalyst 8000v インスタンスに Megaport テンプレートをアタッチします。
6. Cisco Catalyst SD-WAN のブランチの場所に最も近い Megaport の場所でインターコネクト ゲートウェイを作成します。

   Google Cloud への冗長接続のために、Megaport ファブリックでインターコネクト ゲートウェイのペアを作成します。非冗長接続の場合は、Megaport の場所にインターコネクト ゲートウェイを展開します。
7. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
8. Google Cloud アカウントを Cisco SD-WAN Manager に関連付けます。
9. Cisco vManage リリース 20.9.1 以降では、接続を作成するために必要なライセンスがあることを確認します。必要なライセンスがないと、接続の作成は失敗します。詳細については、「License Management for Cisco SD-WAN Cloud Interconnect with Megaport」を参照してください。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[MEGAPORT] を選択します。
5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Megaport アカウントを選択します。
6. [Choose Interconnect Gateway]：接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. （最小リリース：Cisco vManage リリース 20.9.1）Megaport アカウントに関連付けられている利用可能なインターコネクトライセンスを表示するには、[Check available licenses] をクリックします。
8. [Add Connection] をクリックします。
9. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービス プロバイダー	[Google Cloud] を選択します。
Google Account	Google アカウントの詳細を Cisco SD-WAN Manager に関連付ける際に入力したアカウント名で Google アカウントを選択します。

添付ファイル	サポート対象の最小リリース：Cisco vManage リリース 20.9.1 [Shared VPC] を選択して、Google Cloud Router と Google Cloud インターコネクトを接続にアタッチします。
リージョン	サポートされている最小リリース：Cisco vManage リリース 20.9.1 Google Cloud リージョンを選択します。
VPC Network	サポートされている最小リリース：Cisco vManage リリース 20.9.1 この接続を展開する VPC ネットワークを選択します。

冗長性	Cisco vManage リリース 20.8.1 以前の場合： 冗長性のある接続を作成する場合は、[Enable] を選択します。 [Primary Google Cloud Interconnect Attachment]： • [Primary Google Cloud Interconnect Attachment] ドロップダウンリストの横にある更新マークをクリックします。 • 目的のインターコネクト アタッチメントを選択します。インターコネクト アタッチメント名の形式は、<region-name>::<cloud-router-name>::<interconnect-attachment-name> です。 [Secondary Google Cloud Interconnect Attachment]： • 目的のインターコネクト アタッチメントを選択します。インターコネクト アタッチメント名の形式は、<region-name>::<cloud-router-name>::<interconnect-attachment-name> です。 セカンダリ インターコネクト アタッチメント オプションは、プライマリ インターコネクト アタッチメントが属するリージョンとネットワークに基づいて決定されます。プライマリ インターコネクト アタッチメントと同じリージョンおよびネットワークに未使用のインターコネクト アタッチメントがない場合、このドロップダウンリストは空になり、Google Cloud ポータルで冗長インターコネクト アタッチメントを作成する必要があることが示されます。 冗長性のない接続を作成する場合は、[Disable] を選択します。 [Google Cloud Interconnect Attachment]： • [Google Cloud Interconnect Attachment] ドロップダウンリストの横にある更新マークをクリックします。 • 目的のインターコネクト アタッチメントを選択します。インターコネクト アタッチメント名の形式は、<region-name>::<cloud-router-name>::<interconnect-attachment-name> です。

Cisco vManage リリース 20.9.1 以降の場合：

[Google Cloud Router]：

- [Google Cloud Router] ドロップダウンリストの横にある更新マークをクリックします。
- Google Cloud Router を選択するか、[Add New Google Cloud Router] をクリックします。

[Add New Google Cloud Router] をクリックした場合は、[Add Google Cloud Router] スライドインペインでルータ設定を構成します。

以下を設定し、[Save] をクリックします。

- [Region]：Google Cloud Router のリージョンを選択します。
- [VPC Network]：Google Cloud Router ネットワークを選択します。
- [Cloud Router Name]：固有の Google Cloud Router 名を入力します。

（注） Google Cloud Router は常に、BGP ASN が 16,550、MTU が 1,500、デフォルトルーティング有効で作成されます。

[Google Cloud Interconnect Attachment]：

- [Google Cloud Interconnect Attachment] ドロップダウンリストの横にある更新マークをクリックします。
- 必要なインターコネクトアタッチメントを選択するか、[Add New Google Cloud Interconnect Attachment] をクリックします。

[Add New Google Cloud Interconnect Attachment] をクリックした場合は、[Add Google Cloud Interconnect Attachment] スライドインペインでルータ設定を構成します。

以下を設定し、[Save] をクリックします。

- [Region]：Google Cloud インターコネクト アタッチメントのリージョンを選択します。
- [VPC Network]：インターコネクトアタッチメント用の Google Cloud ネットワークを選択します。
- [Cloud Router Name]：インターコネクト アタッチメント用に、選択したリージョンと VPC ネットワークに展開された Google Cloud Router を選択します。
- [IC Attachment Name]：インターコネクト アタッチメントの一意の名前を入力します。

	• [Secondary Zone]：このアタッチメントをセカンダリゾーンに展開する場合は、このチェックボックスをオンにします。

10. プライマリ仮想クロス コネクト アタッチメントに次の設定を構成し、[Next] をクリックします。

Peering Location	**1.** [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 **2.** Google Cloud Router とプライマリ インターコネクト アタッチメントを作成した Google Cloud リージョンに最も近い Megaport の場所を選択します。
Connection Name	プライマリ接続の一意の名前を入力します。
Bandwidth (Mbps)	接続帯域幅（Mbps）を選択します。許可された帯域幅の値のリストは、選択したピアリングの場所に基づいて作成されます。

11. ステップ 8 で冗長性を有効にした場合は、セカンダリ仮想クロスコネクト アタッチメントに次の設定を構成し、[Next] をクリックします。

Peering Location	**1.** [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 **2.** Google Cloud Router とセカンダリ インターコネクト アタッチメントを作成した Google Cloud リージョンに最も近い Megaport の場所を選択します。 **ヒント** 冗長性を確保するために、プライマリ インターコネクト アタッチメントに関連付けられているピアリングの場所以外の場所を選択します。
Connection Name	セカンダリ接続の一意の名前を入力します。
Bandwidth (Mbps)	セカンダリ接続の帯域幅は、プライマリ接続の帯域幅と同じ値に設定されます。
Source Gateway	セカンダリ インターコネクト アタッチメントへの接続を確立する必要があるインターコネクト ゲートウェイを選択します。

12. 以下を設定し、[Next] をクリックします。

設定	[Auto-generated] または [Custom] を選択します。 • [Auto-generated]：インターコネクト BGP ASN はシステムによって選択されます • [Custom]：インターコネクト仮想クロス コネクト アタッチメントとのピアリング用に、任意のインターコネクト BGP ASN を指定します。 （注） インターコネクト ゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN を指定できます。インターコネクト ゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。 Google Cloud Router へのインターコネクトの BGP ピアリング IP アドレスは、サブネット（169.254.0.0/16）から Google によって自動割り当てされます。Cisco SD-WAN Manager から IP アドレスを設定することはできません。
Segment	この接続のセグメント ID を選択します。

13. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。
- 接続設定を変更するには、[Back] をクリックします。

接続設定を保存すると、設定タスクが起動し、インターコネクト ゲートウェイと Google Cloud Router のインターコネクト アタッチメントの間にインターコネクトが作成されます。

タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。Google Cloud コンソールで接続の詳細を表示することもできます。

次の作業：Google Cloud コンソールで、BGP を介して Google Cloud Router からインターコネクト ゲートウェイにアドバタイズされるルートを管理します。

Google Cloud 内のクラウドゲートウェイへのインターコネクト接続の作成

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 17.9.1a、Cisco vManage リリース 20.9.1

前提条件

1. Google Cloud コンソールを使用して、必要な VPC ネットワークを作成します。

2. Megaport アカウントを Cisco SD-WAN Manager に関連付けます。
3. インターコネクト ゲートウェイのグローバル設定を構成します。
4. Cisco Catalyst 8000v インスタンスに Megaport テンプレートをアタッチします。
5. Cisco Catalyst SD-WAN のブランチの場所に最も近い Megaport の場所でインターコネクト ゲートウェイを作成します。

   Google Cloud では冗長接続のみがサポートされています。Megaport ファブリックにインターコネクト ゲートウェイのペアを作成する必要があります。
6. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
7. Google Cloud アカウントを Cisco SD-WAN Manager に関連付けます。
8. マルチクラウドワークフローを使用して Google Cloud ゲートウェイを作成します。
9. 接続を作成するために必要なライセンスがあることを確認します。必要なライセンスがないと、接続の作成は失敗します。詳細については、「License Management for Cisco SD-WAN Cloud Interconnect with Megaport」を参照してください。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[MEGAPORT] を選択します。
5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Megaport アカウントを選択します。
6. [Choose Interconnect Gateway]：接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. Megaport アカウントに関連付けられている利用可能なインターコネクトライセンスを表示するには、[Check available licenses] をクリックします。
8. [Add Connection] をクリックします。
9. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービスプロバイダー	[Google Cloud] を選択します。
Google Account	Google アカウントの詳細を Cisco SD-WAN Manager に関連付ける際に入力したアカウント名で Google アカウントを選択します。

添付ファイル	クラウドゲートウェイに接続するには、[Cloud Gateway] を選択します。 [Cloud Gateways]：ドロップダウンリストからクラウドゲートウェイを 1 つだけ選択できます。

10. 以下を設定し、[Next] をクリックします。

プライマリ	
Google Cloud Router	プライマリ Google Cloud Router は、選択したクラウドゲートウェイに基づいて自動入力されます。
Google Cloud Interconnect Attachment	必要なインターコネクトアタッチメントを選択するか、[Add New Google Cloud Interconnect Attachment] をクリックします。 [Add New Google Cloud Interconnect Attachment] をクリックした場合は、[Add Google Cloud Interconnect Attachment] スライドインペインでルータ設定を構成します。 以下を設定し、[Save] をクリックします。 • [Region]：Google Cloud インターコネクト アタッチメントのリージョンを選択します。 • [VPC Network]：インターコネクト アタッチメント用に関連付けられたネットワークを選択します。 • [Cloud Router Name]：選択したリージョンと VPC ネットワークに展開された Google Cloud Router を選択します。 • [IC Attachment Name]：一意のアタッチメント名を入力します。 • [Secondary Zone]：このアタッチメントをセカンダリゾーンに展開する場合は、このチェックボックスをオンにします。
セカンダリ	
Google Cloud Router	セカンダリ Google Cloud Router は、選択したクラウドゲートウェイに基づいて自動入力されます。

Google Cloud Interconnect Attachment	必要なインターコネクトアタッチメントを選択するか、[Add New Google Cloud Interconnect Attachment] をクリックします。 [Add New Google Cloud Interconnect Attachment] をクリックした場合は、[Add Google Cloud Interconnect Attachment] スライドインペインでインターコネクト設定を構成します。 以下を設定し、[Save] をクリックします。 • [Region]：Google Cloud インターコネクト アタッチメントのリージョンを選択します。 • [VPC Network]：インターコネクト アタッチメント用に関連付けられたネットワークを選択します。 • [Cloud Router Name]：選択したリージョンと VPC ネットワークに展開された Google Cloud Router を選択します。 • [IC Attachment Name]：一意のアタッチメント名を入力します。 • [Secondary Zone]：このアタッチメントをセカンダリゾーンに展開する場合は、このチェックボックスをオンにします。

11. プライマリ仮想クロス コネクト アタッチメントに次の設定を構成し、[Next] をクリックします。

Peering Location	**1.** [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 **2.** Google Cloud Router とプライマリ インターコネクト アタッチメントを作成した Google Cloud リージョンに最も近い Megaport の場所を選択します。
Connection Name	プライマリ接続の一意の名前を入力します。
Bandwidth (Mbps)	接続帯域幅（Mbps）を選択します。許可された帯域幅の値のリストは、選択したピアリングの場所に基づいて作成されます。

12. セカンダリ仮想クロス コネクト アタッチメントに次の設定を構成し、[Next] をクリックします。

Peering Location	**1.** [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 **2.** Google Cloud Router とセカンダリ インターコネクト アタッチメントを作成した Google Cloud リージョンに最も近い Megaport の場所を選択します。 **ヒント** 冗長性を確保するために、プライマリ インターコネクト アタッチメントに関連付けられているピアリングの場所以外の場所を選択します。
Connection Name	セカンダリ接続の一意の名前を入力します。
Bandwidth (Mbps)	セカンダリ接続の帯域幅は、プライマリ接続の帯域幅と同じ値に設定されます。
Source Gateway	セカンダリ インターコネクト アタッチメントへの接続を確立する必要があるインターコネクト ゲートウェイを選択します。

13. 以下を設定し、[Next] をクリックします。

設定	[Auto-generated] または [Custom] を選択します。 • [Auto-generated]：インターコネクト BGP ASN はシステムによって選択されます • [Custom]：インターコネクト仮想クロス コネクト アタッチメントとのピアリング用に、任意のインターコネクト BGP ASN を指定します。 **（注）** インターコネクト ゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN を指定できます。インターコネクト ゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。 Google Cloud Router へのインターコネクトの BGP ピアリング IP アドレスは、サブネット（169.254.0.0/16）から Google によって自動割り当てされます。Cisco SD-WAN Manager から IP アドレスを設定することはできません。
Segment	この接続のセグメント ID を選択します。

14. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。
- 接続設定を変更するには、[Back] をクリックします。

接続設定を保存すると、設定タスクが起動し、インターコネクトゲートウェイと Google Cloud Router のインターコネクト アタッチメントの間にインターコネクトが作成されます。

タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。Google Cloud コンソールで接続の詳細を表示することもできます。

次の作業：Google Cloud コンソールで、BGP を介して Google Cloud Router からインターコネクト ゲートウェイにアドバタイズされるルートを管理します。

Microsoft Azure へのインターコネクトの作成

Cisco SD-WAN Manager と Microsoft Azure アカウントの関連付け

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Cloud] をクリックします。
3. [Associate Cloud Account] をクリックします。
4. 次を設定します。

Cloud Provider	[Microsoft Azure] を選択します。
Cloud Account Name	任意の名前を入力します。
[説明（Description）]（任意）	説明を入力します。
Use for Cloud Gateway	[No] を選択します。
テナント ID	Azure Active Directory（AD）の ID を入力します。 **ヒント** テナント ID を見つけるには、Azure Active Directory に移動し、[Properties] をクリックします。
サブスクリプション ID	使用する Azure サブスクリプションの ID を入力します。
Client ID	既存の Azure アプリケーション ID を入力します。Azure AD にアプリケーションを登録する方法、クライアント ID と秘密キーを取得する方法などの詳細については、Azureのドキュメントを参照してください。
Secret Key	クライアントIDに関連付けられたパスワードを入力します。

5. [Add] をクリックします。

ホスト プライベート ネットワークの検出と Microsoft Azure VNet のタグ付け

インターコネクト ゲートウェイからのソフトウェア定義型のクラウドインターコネクトを作成する Microsoft Azure VNet にタグを付けます。同じ VNet タグを使用してグループ化された Azure VNet は、単一のユニットと見なされます。

前提条件

Microsoft Azure アカウントを Cisco SD-WAN Manager に関連付けます。

タグの追加

VNet をグループ化し、まとめてタグ付けします。

（注） 異なるリソースグループに属する VNet を一緒に使用することはできません。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Host Private Networks] をクリックします。
4. [Cloud Provider]：[Microsoft Azure] を選択します。

   使用可能なホスト VNet が検出され、表に一覧表示されます。
5. 対応するチェックボックスをオンにして、タグ付けする Azure VNet を選択します。
6. [Tag Actions] をクリックします。
7. [Add Tag] をクリックして、以下を設定します。

フィールド	説明
[Tag Name]	タグの名前を入力します。
[地域（Region）]	[Add Tag] をクリックする前に VNet を選択した場合、このフィールドには、選択した VNet に対応するリージョンのリストが表示されます。 • [Add Tag] をクリックする前に VNet を選択しなかった場合、またはリージョンをさらに選択する場合は、ドロップダウンリストからリージョンを選択します。 • リージョンおよび関連する VNet をタグから除外するには、[X] をクリックします。

フィールド	説明
Selected VNets	[Add Tag] をクリックする前に VNet を選択した場合、このフィールドには、選択したホスト VNet の VNet ID のリストが表示されます。 • [Add Tag] をクリックする前に VNet を選択しなかった場合、または VNet をさらに選択する場合は、ドロップダウンリストから VNet を選択します。 • タグから VNet を除外するには、[X] をクリックします。
（Cisco vManage リリース 20.9.1 以降）[Enable for SDCI partner Interconnect Connections] （Cisco vManage リリース 20.8.1 以前）[Enable for Interconnect Connectivity]	Microsoft Azure へのインターコネクト接続を作成するときに VNet タグを使用するには、このチェックボックスをオンにします。 インターコネクト接続に対して有効になっている場合、タグは Microsoft Azure マルチクラウドワークフローで使用することはできません。 インターコネクト接続に対して有効になっていない場合、タグは Microsoft Azure マルチクラウドワークフローでのみ使用できます。 （注） クラウドゲートウェイを使用して VNet ワークロードに接続する場合、この設定を有効にしないでください。

8. [Add] をクリックします。

[Host Private Networks] ページで、先ほど選択した Azure vNet にタグが付けられ、タグ名が [VNET Tag] 列に表示されます。クラウドインターコネクトに vNet タグを使用することを選択した場合、[Interconnect Enabled] 列に [Yes] と表示されます。

タグの編集

既存のタグに VNet を追加するか、既存のタグから VNet を削除します。

Cisco vManage リリース 20.10.1 以降では、次の条件に従ってインターコネクト接続に関連付けられた VNet タグを編集します。

- 1 つの VNet のみが VNet タグに関連付けられている場合、タグから VNet を削除することはできません。タグから VNet を削除するには、インターコネクト接続を削除してからタグを編集します。
- 仮想 WAN アタッチメントを使用したプライベートピアリング接続の場合、タグに関連付ける VNet は、タグにすでに関連付けられている VNet と同じリージョンのものである必要があります。

新しいリージョンの VNet をプライベートピアリング接続にアタッチするには、次の手順を実行します。

1. リージョンの新しいタグを作成し、必要な VNet を関連付けます。
2. プライベートピアリング接続を編集し、VNet タグを接続にアタッチします。

- VNet アタッチメントを使用したプライベートピアリング接続の場合、タグの編集中に、新しいリージョンの VNet をタグに関連付けることができます。

（注） Cisco vManage リリース 20.9.1 以前のリリースでは、インターコネクト接続に関連付けられている VNet タグを編集することはできません。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Host Private Networks] をクリックします。
4. [Cloud Provider]：[Microsoft Azure] を選択します。

   使用可能なホスト VNet が検出され、表に一覧表示されます。
5. [Tag Actions] をクリックします。
6. [Edit Tag] をクリックし、必要に応じて以下を変更します。

フィールド	説明
[Tag Name]	ドロップダウンリストからタグ名を選択します。
[地域（Region）]	このフィールドには、タグに関連付けられた VNet に対応するリージョンのリストが表示されます。 • ドロップダウンリストから追加のリージョンを選択します。 • リージョンおよび関連する VNet をタグから除外するには、[X] をクリックします。
Selected VNets	このフィールドには、タグに関連付けられている VNet のリストが表示されます。 • ドロップダウンリストから追加の VNet を選択します。 • タグから VNet を除外するには、[X] をクリックします。

フィールド	説明
（Cisco vManage リリース 20.9.1 以降）[Enable for SDCI partner Interconnect Connections] （Cisco vManage リリース 20.8.1 以前）[Enable for Interconnect Connectivity]	（読み取り専用）VNet をインターコネクト接続の設定中に使用するように設定されているか、またはマルチクラウドゲートウェイのインテントマッピングに使用するように設定されているかを示します。

7. [Update] をクリックします。

タグの削除

VNet をグループ化しているタグを削除します。

（注） VNet タグがインターコネクト接続に関連付けられている間は、タグを削除できません。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Host Private Networks] をクリックします。
4. [Cloud Provider]：[Microsoft Azure] を選択します。

   使用可能なホスト VNet が検出され、表に一覧表示されます。
5. [Tag Actions] をクリックします。
6. [タグを削除（Delete Tag）]をクリックします。
7. [Tag Name]：ドロップダウンリストからタグ名を選択します。
8. [Delete] をクリックします。

インターコネクト ゲートウェイから Microsoft Azure ExpressRoute への Microsoft ピアリング接続の作成

前提条件

1. Megaport アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。

3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. Microsoft Azure アカウントを Cisco SD-WAN Manager に関連付けます。
5. Cisco Catalyst 8000v インスタンスに Megaport テンプレートをアタッチします。
6. Megaport の場所でインターコネクト ゲートウェイを作成します。

   Microsoft Azure に接続するために、Megaport ファブリックにインターコネクト ゲートウェイのペアを作成します。デフォルトは冗長接続であり、この設定のみがサポートされています。
7. Cisco vManage リリース 20.9.1 以降では、接続を作成するために必要なライセンスがあることを確認します。必要なライセンスがないと、接続の作成は失敗します。詳細については、「License Management for Cisco SD-WAN Cloud Interconnect with Megaport」を参照してください。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** に移動します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[MEGAPORT] を選択します。
5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Megaport アカウントを選択します。
6. [Choose Interconnect Gateway]：接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. （最小リリース：Cisco vManage リリース 20.9.1）Megaport アカウントに関連付けられている利用可能なインターコネクトライセンスを表示するには、[Check available licenses] をクリックします。
8. [Add Connection] をクリックします。
9. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウド サービス プロバイダー	[Microsoft Azure] を選択します。
Azure Account	Microsoft Azure アカウントの詳細を Cisco SD-WAN Manager に関連付ける際に入力したアカウント名で Microsoft Azure アカウントを選択します。

ExpressRoute	

1. [Refresh] ボタンをクリックして、使用可能な ExpressRoute のリストを更新します
2. ExpressRoute を選択するか、[Add New ExpressRoute] をクリックします。

（注）
- Cisco vManage リリース 20.8.1 以降では、Equinix ExpressRoute を使用できます。

  Equinix ExpressRoute は、Cisco vManage リリース 20.6.1 および Cisco vManage リリース 20.7.1 ではサポートされていません。
- Cisco vManage リリース 20.8.1 以降では、使用可能な ExpressRoute のリストのドロップダウンに表示される、それぞれのインターコネクト プロバイダー用に作成されたすべての ExpressRoute は、プロビジョニングのステータスに応じて色分けされます。色とその意味のリストを示します。
  - 黒：プロビジョニングされていません。
  - グレー：プロビジョニング済み。
  - 赤：失敗。
- 選択した Azure アカウントのプロビジョニングされていない ExpressRoute のみを選択できます。ExpressRoute の状態は、Microsoft Azure ポータルで確認できます。

[Add New ExpressRoute] をクリックした場合は、[Create New ExpressRoute] スライドインペインで ExpressRoute 設定を構成します。

次の項目を設定して、[保存（Save）] をクリックします。

- [Resource Group]：Microsoft Azure アカウントに関連付けられているリソースグループを選択します。
- [Region]：Azure リージョンを選択します。
- [Instance Name]：ExpressRoute インスタンスの名前を入力します。
- [Provider]：[Megaport] を選択します。
- [Peering Location]：[Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。ExpressRoute の場所を選択します。
- [Bandwidth]：ExpressRoute 回線の帯域幅を選択します。

	• [SKU]：[Premium] または [Standard] SKU を選択します。 • [Billing Model]：[Metered] 課金または [Unlimited] を選択します。

10. ExpressRoute へのプライマリ接続について次の設定を構成し、[Next] をクリックします。

Peer Location	場所は、前に選択した ExpressRoute に基づいて自動的に選択されます。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	接続帯域幅（Mbps）を選択します。許可された帯域幅の値のリストは、選択した ExpressRoute の場所に基づいて作成されます。

11. ExpressRoute へのセカンダリ接続について次の設定を構成し、[Next] をクリックします。

Peer Location	場所は、前に選択した ExpressRoute に基づいて自動的に選択されます。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	セカンダリ接続の帯域幅は、プライマリ接続の帯域幅と同じ値に設定されます。
Source Gateway	セカンダリ接続を確立する必要があるインターコネクト ゲートウェイを選択します。

12. 以下を設定し、[Next] をクリックします。

展開タイプ	[Public] を選択します。
Primary IPv4 Subnet	プライマリ インターコネクト ゲートウェイからの BGP ピアリングの /30 CIDR パブリック IP アドレスを入力します。 接続を作成する前に、パブリック IPv4 アドレスの使用が組織で許可されていることを確認してください。
Secondary IPv4 Subnet	セカンダリ インターコネクト ゲートウェイからの BGP ピアリングの /30 CIDR パブリック IP アドレスを入力します。 接続を作成する前に、パブリック IPv4 アドレスの使用が組織で許可されていることを確認してください。
BGP Advertise Prefix	インターコネクト ゲートウェイにアドバタイズするサマリーアドレスとプレフィックスを入力します。
Segment	この接続のセグメント ID を選択します。

13. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。

- 接続設定を変更するには、[Back] をクリックします。

接続設定を保存すると、設定タスクが起動します。このタスクでは、次のリソースが作成されます。

- インターコネクト ゲートウェイと ExpressRoute 間の Megaport ファブリック内の仮想クロスコネクト
- ExpressRoute 回線の Microsoft Azure パブリック/プライベートピアリング
- vNet ゲートウェイ（vNet 用の vNet ゲートウェイが存在しない場合）
- ExpressRoute と vNet ゲートウェイ間の接続

タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

Microsoft Azure ポータルで接続の詳細を表示することもできます。

インターコネクト ゲートウェイから Microsoft Azure ExpressRoute へのプライベートピアリング接続の作成

前提条件

1. Megaport アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. Microsoft Azure アカウントを Cisco SD-WAN Manager に関連付けます。
5. ホスト プライベート ネットワークを検出して Microsoft Azure VNet をタグ付けします。
6. Cisco Catalyst 8000v インスタンスに Megaport テンプレートをアタッチします。
7. Megaport の場所でインターコネクト ゲートウェイを作成します。

   Microsoft Azure に接続するために、Megaport ファブリックにインターコネクト ゲートウェイのペアを作成します。デフォルトは冗長接続であり、この設定のみがサポートされています。

8. Cisco vManage リリース 20.9.1 以降では、接続を作成するために必要なライセンスがあることを確認します。必要なライセンスがないと、接続の作成は失敗します。詳細については、「License Management for Cisco SD-WAN Cloud Interconnect with Megaport」を参照してください。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** に移動します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[MEGAPORT] を選択します。
5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Megaport アカウントを選択します。
6. [Choose Interconnect Gateway]：Direct Connect 接続を作成する元となるインターコネクトゲートウェイを選択します。
7. （最小リリース：Cisco vManage リリース 20.9.1）Megaport アカウントに関連付けられている利用可能なインターコネクトライセンスを表示するには、[Check available licenses] をクリックします。
8. [Add Connection] をクリックします。
9. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービス プロバイダー	[Microsoft Azure] を選択します。
Azure Account	Microsoft Azure アカウントの詳細を Cisco SD-WAN Manager に関連付ける際に入力したアカウント名で Microsoft Azure アカウントを選択します。

ExpressRoute	

1. [Refresh] ボタンをクリックして、使用可能な ExpressRoute のリストを更新します
2. ExpressRoute を選択するか、[Add New ExpressRoute] をクリックします。

（注）
- Cisco vManage リリース 20.8.1 以降では、Equinix ExpressRoute を使用できます。

  Equinix ExpressRoute は、Cisco vManage リリース 20.6.1 および Cisco vManage リリース 20.7.1 ではサポートされていません。

- Cisco vManage リリース 20.8.1 以降では、使用可能な ExpressRoute のリストのドロップダウンに表示される、それぞれのインターコネクト プロバイダー用に作成されたすべての ExpressRoute は、プロビジョニングのステータスに応じて色分けされます。色とその意味のリストを示します。
  - 黒：プロビジョニングされていません。
  - グレー：プロビジョニング済み。
  - 赤：失敗。
- 選択した Azure アカウントのプロビジョニングされていない ExpressRoute のみを選択できます。ExpressRoute の状態は、Microsoft Azure ポータルで確認できます。

[Add New ExpressRoute] をクリックした場合は、[Create New ExpressRoute] スライドインペインで ExpressRoute 設定を構成します。

次の項目を設定して、[保存（Save）] をクリックします。

- [Resource Group]：Microsoft Azure アカウントに関連付けられているリソースグループを選択します。
- [Region]：Azure リージョンを選択します。
- [Instance Name]：ExpressRoute インスタンスの名前を入力します。
- [Provider]：[Megaport] を選択します。
- [Peering Location]：[Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。ExpressRoute の場所を選択します。
- [Bandwidth]：ExpressRoute 回線の帯域幅を選択します。

	• [SKU]：[Premium] または [Standard] SKU を選択します。 • [Billing Model]：[Metered] 課金または [Unlimited] を選択します。

10. ExpressRoute へのプライマリ接続について次の設定を構成し、[Next] をクリックします。

Peer Location	場所は、前に選択した ExpressRoute に基づいて自動的に選択されます。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	接続帯域幅（Mbps）を選択します。許可された帯域幅の値のリストは、選択した ExpressRoute の場所に基づいて作成されます。

11. ExpressRoute へのセカンダリ接続について次の設定を構成し、[Next] をクリックします。

Peer Location	場所は、前に選択した ExpressRoute に基づいて自動的に選択されます。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	セカンダリ接続の帯域幅は、プライマリ接続の帯域幅と同じ値に設定されます。
Source Gateway	セカンダリ接続を確立する必要があるインターコネクト ゲートウェイを選択します。

12. 以下を設定し、[Next] をクリックします。

展開タイプ	[Private] を選択します。

BGP-Peering Settings	[Auto-generated] または [Custom] を選択します。 [Auto-generated]：インターコネクト BGP ASN、およびプライマリおよびセカンダリ IPv4 サブネットがシステムによって選択されます。IPv4 サブネットは、内部で予約された /16 サブネット（198.18.0.0/16）から選択されます。 [Custom]： （注） インターコネクト ゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN とカスタム IPv4 サブネットを指定できます。インターコネクト ゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。 • [BGP ASN]：ExpressRoute とのプライマリおよびセカンダリピアリングに選択した ASN を指定します。 • [Primary IPv4 Subnet]：プライマリ インターコネクト ゲートウェイとの BGP ピアリングの /30 CIDR IP アドレスを入力します。 • [Secondary IPv4 Subnet]：セカンダリ インターコネクト ゲートウェイとの BGP ピアリングの /30 CIDR IP アドレスを入力します。 • Cisco vManage リリース 20.8.1 以降： • カスタムサブネットの IP アドレスは、10.0.0.0/8、172.16.0.0/12、192.168.0.0/16 の範囲にある必要があります。 • カスタムサブネットは/30 として指定する必要があります。 • カスタムサブネットは、172.31.251.0/21 と競合しないようにする必要があります。 • カスタムサブネットは、他の接続に使用されるサブネットと競合することはできません。

添付ファイル	次のいずれかを選択します。 • [vNet]：VNet タグを使用して VNet を接続にアタッチします。 • [vWAN]：仮想 WAN を接続にアタッチし、VNet タグを使用して仮想 WAN のリージョンから VNet を選択します。 • サポート対象の最小リリース：Cisco vManage リリース 20.9.1 [Cloud Gateway]：クラウドゲートウェイを接続にアタッチします。接続ごとに最大 5 つのクラウドゲートウェイを選択できます。
VNet Settings	[VNet Tags]：VNet タグを選択して、この接続を介してトラフィックをルーティングする必要がある VNet を識別します。

virtual WAN Settings	

[vWAN]：新しい仮想 WAN を選択または追加します。

（注） インターコネクト ゲートウェイから Microsoft Azure への最初の接続にのみアタッチする仮想 WAN を選択できます。同じ仮想 WAN が、仮想 WAN をアタッチするように選択した後続の接続にアタッチされます。

Cisco vManage リリース 20.8.1 以降では、Cisco SD-WAN Manager は、Microsoft Azure アカウントごとに、各 Microsoft Azure リソースグループに対して 1 つの vWAN をサポートします。その vWAN が選択され、vWAN 接続の一部として使用されると、同じ Microsoft Azure リソースグループへの後続の vWAN 接続には同じ vWAN が使用されます。

接続に ExpressRoute 回線が選択されると、接続用に Microsoft Azure リソースグループが決定されます。接続に属する他のすべての Microsoft Azure リソースは、選択した ExpressRoute 回線と同じ Microsoft Azure リソースグループに含まれている必要があります。

[vNet]：VNet タグを選択して、この接続を介してトラフィックをルーティングする必要がある VNet を識別します。

Cisco SD-WAN Manager は、選択された VNet タグに基づいて VNet を検索し、VNet が属するリージョンを識別します。選択された仮想 WAN と特定されたリージョンについて、Cisco SD-WAN Manager は、検証に使用できる仮想ハブを見つけて一覧表示します。仮想ハブが存在しないリージョンの場合、名前とアドレスプレフィックスを指定して仮想ハブを追加する必要があります。

[vHub Settings]：

（注） Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、リージョンに複数の Azure Virtual WAN ハブがある場合は、そのリージョンの特定の Azure Virtual WAN ハブを選択できます。Azure Virtual WAN ハブを選択すると、Azure Virtual WAN 用に作成される後続のすべての接続で同じ Azure Virtual WAN ハブが使用されます。

1. [Add Settings] をクリックします。設定を変更する場合は、[Edit Settings] をクリックします。
2. 該当するリージョンの仮想ハブ名とアドレスプレフィックスを確認します。リージョンに仮想ハブが存在しない場合は、リージョンに使用する仮想ハブの名前とアドレスプレフィックスを入力します。

（注） 入力する仮想ハブのアドレスプレフィックスが、

	どの VNet のアドレスプレフィックスとも重複していないことを確認してください。 **3.** 変更を適用するには、[Save] をクリックします。変更を破棄するには、[Cancel] をクリックします。
Segment	この接続のセグメント ID を選択します。

13. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。
- 接続設定を変更するには、[Back] をクリックします。

接続設定を保存すると、設定タスクが起動します。

VNet アタッチメントの場合は、設定タスクにより次のリソースが作成されます。

- インターコネクト ゲートウェイと ExpressRoute 間の Megaport ファブリック内の仮想クロスコネクト
- ExpressRoute 回線の Microsoft Azure パブリック/プライベートピアリング
- vNet ゲートウェイ（vNet 用の vNet ゲートウェイが存在しない場合）
- ExpressRoute と vNet ゲートウェイ間の接続

仮想 WAN アタッチメントの場合は、設定タスクにより次のリソースが作成されます。

- インターコネクト ゲートウェイと ExpressRoute 間の Megaport ファブリック内の仮想クロスコネクト
- ExpressRoute 回線の Microsoft Azure パブリック/プライベートピアリング
- 必要な仮想ハブ
- vNet と仮想ハブ間の接続
- 各仮想ハブの ExpressRoute ゲートウェイ（必要な場合）
- ExpressRoute ゲートウェイと ExpressRoute 回線間の接続

タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

Microsoft Azure ポータルで接続の詳細を表示することもできます。

インターコネクトゲートウェイ間のインターコネクトの作成

Cisco SD-WAN Manager で、2 つ以上の Megaport の場所にあるインターコネクト ゲートウェイ間のインターコネクトを作成できます。これにより、Megaport ファブリックを介してこれらのインターコネクト ゲートウェイに接続されている Cisco Catalyst SD-WAN ブランチの場所をリンクできます。

前提条件

Megaport ファブリックを介して接続される Cisco Catalyst SD-WAN ブランチの場所ごとに、

1. Megaport アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. 最も近い Megaport の場所を特定します。
5. ブランチの場所に最も近い Megaport の場所にインターコネクト ゲートウェイを作成します。

（注） 2 つのブランチの場所で定義された VRF があり、インターコネクト ゲートウェイ間の接続を介して VRF にアタッチされたトラフィックを交換する場合は、インターコネクト ゲートウェイで VRF と適切な集中管理型ポリシーを設定して、インターコネクト ゲートウェイ間の接続を介してブランチのトラフィックをルーティングする必要があります。

6. Cisco vManage リリース 20.9.1 以降では、接続を作成するために必要なライセンスがあることを確認します。必要なライセンスがないと、接続の作成は失敗します。詳細については、「License Management for Cisco SD-WAN Cloud Interconnect with Megaport」を参照してください。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[MEGAPORT] を選択します。

（注） このフィールドは Cisco vManage リリース 20.6.1 で導入されました。

5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Megaport アカウントを選択します。
6. [Choose Interconnect Gateway]：送信元インターコネクト ゲートウェイを選択します。
7. （最小リリース：Cisco vManage リリース 20.9.1）Megaport アカウントに関連付けられている利用可能なインターコネクトライセンスを表示するには、[Check available licenses] をクリックします。
8. [Add Connection] をクリックします。
9. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Edge] を選択します。
プロバイダー	[Megaport] を選択します。 （注） Cisco vManage リリース 20.6.1 以降では、このフィールドは使用できません。
Connection Name	接続の一意の名前を入力します。
Interconnect Gateway	宛先インターコネクト ゲートウェイを選択します。
帯域幅	接続帯域幅を指定します。 単位：Mbps。

10. 接続の概要を確認します。
    - 接続を作成するには、[Save] をクリックします。
    - 接続設定を変更するには、[Back] をクリックします。

設定タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

設定の確認と変更

インターコネクト ゲートウェイと接続の概要の表示

[Interconnect] ページでは、作成したインターコネクト ゲートウェイと接続の概要を確認できます。インターコネクト ゲートウェイを作成していない場合、このページにはインターコネクト ゲートウェイと接続を作成および管理するためのワークフローの概要が表示されます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。

   次の情報が表示されます。

Interconnect Gateways	• インターコネクト ゲートウェイの総数 • 到達可能な（アップ状態の）インターコネクト ゲートウェイの数 • 到達不能な（ダウン状態の）インターコネクト ゲートウェイの数
接続	• 接続の合計数 • アップ状態の接続の数 • ダウン状態の接続の数
Summary Table	すべてのインターコネクト ゲートウェイとゲートウェイからの接続の要約リスト。

接続の表示、編集、または削除

接続プロパティの表示

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。

   既存の接続の概要がテーブルに示されます。
4. 接続に関する詳細を表示するには、目的の接続の [...] をクリックし、[View] をクリックします。

接続設定の編集

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。

   既存の接続の概要がテーブルに示されます。

4. 接続設定を変更するには、目的の接続の [...] をクリックし、[Edit] をクリックします。

   次の表は、接続先と接続タイプ（ある場合）に基づいて、編集可能なパラメータを説明しています。必要に応じてパラメータを設定します。

   Cisco SD-WAN Manager では、これらの編集可能なパラメータに加えて、接続に関する読み取り専用のプロパティも表示されます。

（注） アクティブな接続のプロパティのみを変更できます。

表 *73 : AWS* へのインターコネクト接続の編集可能なプロパティ

フィールド	説明	適用される接続タイプ
帯域幅	接続帯域幅を変更します。 単位：Mbps。	プライベートおよびパブリックホスト型 VIF
Segment	サポート対象の最小リリース：Cisco vManage リリース 20.10.1 この接続の別のセグメント ID を選択します。	AWS へのすべての接続

フィールド	説明	適用される接続タイプ
Transit Gateway	サポート対象の最小リリース：Cisco vManage リリース 20.10.1 **1.** [Refresh] ボタンをクリックして、選択した AWS アカウントに関連付けられているトランジットゲートウェイを取得します。 **2.** Direct Connect 接続を作成する必要があるトランジットゲートウェイを選択します。 （注） • 次の条件下で、トランジットゲートウェイを削除できます。 • 削除するトランジットゲートウェイは、この接続に関連付けられている唯一のトランジットゲートウェイではない。 • 同じ編集操作で、トランジットゲートウェイが提供するリージョンに対応する VPC タグを削除する。 • あるリージョンの既存のトランジットゲートウェイを、同じリージョンの別のトランジットゲートウェイに置き換えることはできません。	トランジットホスト型接続
VPC Tags	サポート対象の最小リリース：Cisco vManage リリース 20.10.1 VPC タグを選択して、この接続を介してトラフィックをルーティングする必要がある VPC を識別します。	• VPC アタッチメントを使用したプライベートホスト型 VIF およびプライベートホスト型接続 • トランジットホスト型接続

フィールド	説明	適用される接続タイプ
許可プレフィックス（**Allowed Prefixes**）	サポート対象の最小リリース：Cisco vManage リリース 20.10.1 [Edit Prefixes] をクリックします。 選択した VPC の IPv4 CIDR プレフィックスを入力します。AWS VPC ダッシュボードから IPv4 CIDR アドレスを見つけることができます。 （注） プレフィックスの追加のみ行うことができます。既存のプレフィックスを削除することはできません。	トランジットホスト型接続

表 *74 : Google Cloud* へのインターコネクト接続の編集可能なプロパティ

フィールド	説明
接続速度	[Connectivity Speed] ドロップダウンリストから必要な帯域幅を選択します。 冗長接続の場合は、プライマリ接続またはセカンダリ接続のいずれかの接続速度を変更します。ピア接続は、同じ接続速度を使用するように更新されます。 接続の帯域幅オプションは、関連付けられたピアリングの場所によって異なる場合があります。

（注） プライマリ接続またはセカンダリ接続のいずれかのプロパティを変更します。ピア接続は、同じ設定を使用するように更新されます。

表 *75 : Microsoft Azure* へのインターコネクト接続の編集可能なプロパティ

フィールド	説明	適用される接続タイプ
帯域幅	接続帯域幅を変更します。 単位：Mbps。 （注） Microsoft Azure への接続の帯域幅のみを増やすことができます。Microsoft Azure への接続の場合、Cisco SD-WAN Manager で接続帯域幅を増やす前に、Azure ポータルで ExpressRoute の帯域幅を増やす必要があります。	プライベートおよびパブリック（Microsoft）ピアリング接続

フィールド	説明	適用される接続タイプ
Segment	サポート対象の最小リリース：Cisco vManage リリース 20.10.1 この接続の別のセグメント ID を選択します。	プライベートおよびパブリック（Microsoft）ピアリング接続
BGP Advertise Prefix	サポート対象の最小リリース：Cisco vManage リリース 20.10.1 インターコネクト ゲートウェイにアドバタイズするサマリーアドレスとプレフィックスを入力します。 （注） Microsoft Azure のデフォルトでは、BGP アドバタイズプレフィックスが正しく表示されないリソースまたはネットワークオブジェクトを表示するために、ポータルで古いバージョンの API が使用されます。Microsoft Azure ポータルから BGP アドバタイズプレフィックスを確認するには、2020-05-01 以降の API バージョンを選択します。	パブリック（Microsoft）ピアリング接続
vNet Settings		
vNet	サポート対象の最小リリース：Cisco vManage リリース 20.10.1 VNet タグを選択して、この接続を介してトラフィックをルーティングする必要がある VNet を識別します。	プライベートピアリング接続

フィールド	説明	適用される接続タイプ
vHub Settings	サポート対象の最小リリース：Cisco vManage リリース 20.10.1 **1.** [Edit Settings] をクリックします。 **2.** 該当するリージョンの仮想ハブ名とアドレスプレフィックスを確認します。リージョンに仮想ハブが存在しない場合は、リージョンに使用する仮想ハブの名前とアドレスプレフィックスを入力します。 （注） 入力する仮想ハブのアドレスプレフィックスが、どの VNet のアドレスプレフィックスとも重複していないことを確認してください。 **3.** 変更を適用するには、[Save] をクリックします。変更を破棄するには、[Cancel] をクリックします。	プライベートピアリング接続

表 *76 :* エッジデバイス間のインターコネクト接続の編集可能なプロパティ

フィールド	説明
帯域幅	接続帯域幅を変更します。 単位：Mbps。

5. 変更を適用するには、[Update] または [Save] をクリックします。

接続の削除

（注）
- AWS への接続を削除すると、Cisco SD-WAN Manager は、接続の確立中に作成された VIF、仮想プライベートゲートウェイ、およびルートテーブルのみを削除します。
- AWS への接続の作成中に Direct Connect ゲートウェイまたはトランジットゲートウェイを作成した場合、Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、オプションで Direct Connect ゲートウェイとトランジットゲートウェイを削除できます。
- Microsoft Azure への接続を削除すると、Cisco SD-WAN Manager は、これらの要素が他の接続で使用されていない場合のみ、接続用に作成された ExpressRoute、VNet ゲートウェイ、ExpressRoute ゲートウェイ、および仮想ハブを削除します。

  Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、必要に応じて、接続の削除時に Express-Route と Virtual Wan を削除するか、これらの Azure リソースを管理するかを選択できます。GCP 接続を削除する場合、必要に応じて、Google Cloud Router を削除するか、これらのリソースを管理するかを選択できます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。

   既存の接続の概要がテーブルに示されます。
4. 接続を削除するには、目的の接続の [...] をクリックし、[Delete] をクリックします。接続を削除することを確定します。

インターコネクト ゲートウェイの表示、編集、または削除

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Gateway Management] をクリックします。

   既存のインターコネクト ゲートウェイの詳細がテーブルにまとめられています。
4. このテーブルで、目的のインターコネクト ゲートウェイの […] をクリックします。
   - インターコネクト ゲートウェイの詳細を表示するには、[View] をクリックします。
   - インターコネクト ゲートウェイの説明を編集するには、[Edit Interconnect Gateway] をクリックします。

- インターコネクトゲートウェイを削除するには、[Delete]をクリックして、ゲートウェイを削除することを確定します。

（注） インターコネクトゲートウェイは、関連付けられている接続がない場合のみ削除できます。

インターコネクトゲートウェイを削除すると、Megaportファブリックからブランチの場所の接続が切断されます。

インターコネクトアカウントの表示、編集、または削除

1. Cisco SD-WAN Managerのメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]**を選択します。
2. [Interconnect]をクリックします。
3. [Account Management]をクリックします。

   使用可能なインターコネクトアカウントがテーブルに表示されます。
4. このテーブルで、目的のインターコネクトアカウントの[...]をクリックします。

- インターコネクトアカウントの詳細を表示するには、[View]をクリックします。
- インターコネクトアカウントの詳細を変更するには、[Edit Account Information]をクリックします。

  [Account Name]と[Description]を変更できます。
- インターコネクトアカウントのログイン情報を変更するには、[Edit Account Credentials]をクリックします。

  アカウントの[User Name]と[Password]を変更できます。

（注） Cisco SD-WAN Managerでログイン情報を変更しても、インターコネクトプロバイダーのログイン情報は変更されません。この設定オプションは、インターコネクトプロバイダーの関連ポータルで実行した、アカウントログイン情報の変更内容を複製する場合にのみ使用してください。

- インターコネクトアカウントを削除するには、[Remove]をクリックして、アカウントの削除を確定します。

監査管理

SDCI プロバイダーのファブリックである Megaport には、Cisco SD-WAN Manager の状態とのクラウド接続状態の同期の確認を支援する、監査管理のサポートが組み込まれています。監査プロセスでは、プロバイダーリソース、インターコネクトゲートウェイ、およびクラウドへの接続をスキャンします。[Audit] 画面で、エラーがある場合はエラーが表示され、エラーがない場合はステータスに [In Sync] と表示されます。

（注） Cisco vManage リリース 20.11.1 では、監査管理機能は Megaport ファブリックでのみサポートされます。

監査レポートへのアクセス

1. [Cloud OnRamp for Multicloud] で、[Interconnect] タブに移動します。
2. [Intent Management] ペインで、[Audit] をクリックします。
3. [Intent Management- Audit] の [Interconnect Gateways] で、ドロップダウンリストから [Interconnect Provider] を選択します。
4. 目的の監査レポートを表示するには、[Destination Type] を選択し、宛先タイプが [cloud] の場合はドロップダウンリストから [Cloud Provider] を選択します。

（注） 要件に応じて、[Destination Type] に [cloud] または [edge] を選択します。

（注） 次に、監査レポートによってスキャンおよび報告されるさまざまな接続を示します。

- [Edge Gateway] では、Cisco SD-WAN Manager ワークフローを使用して作成されたエッジゲートウェイがあることと、それぞれの詳細が示されます。
- [Edge Connections] では、Cisco SD-WAN Manager ワークフローを使用して作成されたエッジ接続があることと、それぞれの詳細が示されます。
- [Unknown Edge Gateways] では、Cisco SD-WAN Manager が特定のエッジゲートウェイを認識できないことが示されます。
- [Unknown Edge Connections] では、Cisco SD-WAN Manager が特定のエッジ接続を認識できないことが示されます。

監査レポートに表示されるステータスは次のとおりです。

- In Sync
- Out of Sync
- AUDIT_INFO

監査の利点

監査は、Cisco SD-WAN Manager インテントとクラウドで実現された内容の間の乖離または不一致を特定するのに役立ちます。この乖離は、クラウドリソース、接続、および状態に関して発生します。このような乖離が検出されると、Cisco SD-WAN Manager によりその乖離にフラグが付けられ、修正アクションの実行に役立てることができます。

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport のトラブルシューティング

シナリオ	対処法
インターコネクトアカウントを追加できない	• Cisco SD-WAN Manager に関連付けられているアカウントのログイン情報が正しいことを確認します。 • インターコネクトプロバイダーでログイン情報を更新した場合は、Cisco SD-WAN Manager でアカウントのログイン情報を更新します。
インターコネクト ゲートウェイの作成を試みている際に、デバイスリストが空になる	デバイスにテンプレートが割り当てられていることを確認します（推奨テンプレート：Default_MEGAPORT_ICGW_C8000V_Template_V01）。

シナリオ	対処法
インターコネクト ゲートウェイの作成を試みている際に、目的の場所が見つからない	[Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。
インターコネクト ゲートウェイの作成に失敗した	**1.** Cisco SD-WAN Manager で設定タスクの進行状況を確認し、エラーメッセージがないか確認します。 **2.** インターコネクトグローバル設定を使用している場合は、選択したソフトウェアイメージがインターコネクト プロバイダーの場所で使用可能かどうかを確認します。 **3.** VM インスタンスが展開されていない場合、または IP プールが使い果たされている場合は、インターコネクト プロバイダーに確認してください。
Direct Connect 接続の作成中に、Direct Connect ゲートウェイまたはトランジット ゲートウェイ リストが空になる	**1.** AWS ポータルで、目的の Direct Connect ゲートウェイまたはトランジットゲートウェイが使用可能であることを確認します。 **2.** [Refresh] ボタンをクリックして、AWS からゲートウェイのリストを取得します。 **3.** ゲートウェイが AWS で使用できない場合は、Cisco SD-WAN Manager からゲートウェイを作成します。
Direct Connect 接続の作成中に、ホスト VPC タグがリストに表示されない	ホスト VPC タグが使用可能であり、インターコネクト接続に対して有効になっていることを確認します。
Direct Connect 接続の作成に失敗した	**1.** Cisco SD-WAN Manager で設定タスクの進行状況を確認し、エラーメッセージがないか確認します。 **2.** インターコネクトグローバル設定を使用している場合は、内部 IP アドレスプールが使い果たされているかどうかを確認します。該当する場合は、一部の接続を削除して再試行します。 **3.** カスタム設定を使用している場合は、ピアリングに重複する CIDR サブネットを入力していないことを確認します。 **4.** 接続制限に達しているかどうかを確認します。「Cisco Catalyst SD-WAN Cloud Interconnect with Megaport の使用上の注意」を参照してください。 **5.** インターコネクト プロバイダー アカウントと AWS アカウントの権限を確認します。

シナリオ	対処法
トラフィックフローの問題	**1.** インバウンドおよびアウトバウンドトラフィックに必要なセキュリティルールがホスト VPC に設定されていることを確認します。 **2.** 仮想インターフェイスが作成され、Direct Connect ゲートウェイにアタッチされているかどうかを確認します。 **3.** AWS で、仮想インターフェイスの BGP ピアリングステータスが UP 状態かどうかを確認します。 **4.** 正しいルートテーブルがホスト VPC のメインルーティングテーブルとして使用されているかどうかと、必要なルートが仮想プライベートゲートウェイまたはトランジットゲートウェイに伝達されているかどうかを確認します。 **5.** 仮想プライベートゲートウェイまたはトランジットゲートウェイが、Direct Connect ゲートウェイにアタッチされているかどうかを確認します。
遅延の問題	**1.** インターコネクト ゲートウェイの場所が、接続の作成時に選択した Direct Connect の場所と近いかどうかを確認します。 **2.** 接続に適切な帯域幅が設定されていることを確認します。
クラウドゲートウェイがドロップダウンリストに表示されない	必要なクラウドゲートウェイがマルチクラウドワークフローを使用して作成され、このドキュメントに記載されている最小要件が満たされていることを確認します。
クラウドゲートウェイへのインターコネクト接続を作成した後も、VPC または VNET ワークロードへのトラフィックがインターネット経由で送信される	Cisco Catalyst SD-WAN のブランチがインターネットを介してクラウドゲートウェイに接続されていて、同じ VPC または VNET ワークロードにアクセスするためにインターコネクト ゲートウェイからのインターコネクト接続を介して接続されている場合、デフォルトでは、ブランチからのトラフィックはインターネットを介して送信されます。 インターコネクト ゲートウェイを介したプライベートパスを優先パスにするには、ブランチの WAN エッジデバイス、インターコネクト ゲートウェイ、およびクラウドゲートウェイに適切な制御ポリシーとデータポリシーを適用します。

第 18 章

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

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。

表 *77* : 機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN Cloud Interconnect with Equinix	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	Cisco Cloud Services Router 1000v（Cisco CSR 1000v）インスタンスを Equinix ファブリックのインターコネクト ゲートウェイとして展開し、Cisco Catalyst SD-WAN ブランチの場所をインターコネクト ゲートウェイに接続することができます。インターコネクト ゲートウェイから、AWS Cloud OnRamp または Equinix ファブリック内の別のインターコネクト ゲートウェイへのソフトウェア定義型インターコネクトを作成することができます。

機能名	リリース情報	説明
Cisco Catalyst SD-WAN Cloud Interconnect with Equinix：Google Cloud および Microsoft Azure	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1	Google Cloud VPC、Microsoft Azure VNet または Virtual WAN へのソフトウェア定義型インターコネクトを作成し、Equinix ファブリックを介してブランチの場所をクラウドリソースにリンクすることができます。Equinix ファブリックのインターコネクト ゲートウェイからデバイスリンクを作成、更新、および削除することもできます。
Equinix との暗号化されたマルチクラウド インターコネクト	Cisco vManage リリース 20.9.1	Cisco Catalyst SD-WAN ファブリックを、Equinix のインターコネクト ゲートウェイから AWS、Google Cloud、および Microsoft Azure クラウド サービス プロバイダーに拡張できます。Cisco SD-WAN Manager の Cloud OnRamp ワークフローを使用して、インターコネクト ゲートウェイとクラウド サービス プロバイダー間のセキュアなプライベート Cisco Catalyst SD-WAN 接続をプロビジョニングすることができます。
Cisco Catalyst 8000V Edge ソフトウェアのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN Manager リリース 20.12.1	Cisco Catalyst 8000v Edge ソフトウェアを Equinix ファブリックのインターコネクト ゲートウェイとして展開し、Cisco Catalyst SD-WAN ブランチの場所をインターコネクト ゲートウェイに接続することができます。
SDCI 接続への VPC および VNet タグの追加	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN Manager リリース 20.12.1	SDCI 接続に関連付けられている VPC および VNet タグと、その他のプロパティを変更できます

機能名	リリース情報	説明
Equinix での監査の管理	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN Manager リリース 20.12.1	監査管理は、インターコネクトクラウドとプロバイダーの状態が、Cisco Catalyst SD-WAN Manager の状態と同期しているかどうかを把握するために役立ちます。監査プロセスには、プロバイダーリソース、インターコネクトゲートウェイ、およびクラウドへの接続のスキャンが含まれています。詳細については、「Audit Management」を参照してください。

- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の前提条件 （487 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の制約事項 （488 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix に関する情報 （494 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の設定ワークフロー （498 ページ）
- Cisco SD-WAN Cloud Interconnect with Equinix の前提条件の設定 （501 ページ）
- AWS へのインターコネクトの作成 （508 ページ）
- Google Cloud へのインターコネクトの作成 （519 ページ）
- Microsoft Azure へのインターコネクトの作成 （529 ページ）
- デバイスリンク （548 ページ）
- インターコネクト ゲートウェイ間のインターコネクトの作成 （550 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の設定の確認と変更 （552 ページ）
- 監査管理 （558 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix のトラブルシューティング （560 ページ）

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の前提条件

1. Equinix ポータルでアカウントを作成します。Equinix の「New User Equinix Fabric Portal Access」のドキュメントを参照してください。

   アカウントを作成したら、アカウントのクライアント ID（コンシューマキー）とクライアント シークレット キー（コンシューマシークレット）を生成します。Equinix Developer Platform Knowledge Center の「Generating Client ID and Client Secret Key」のドキュメントを参照してください。

このアカウントを使用してインターコネクト ゲートウェイを展開する各リージョンの請求アカウントを作成します。Equinix の「Billing Account Management」のドキュメントを参照してください。

2. インターコネクト ゲートウェイとクラウドプロバイダー間のパブリック ピアリングを必要とする接続の場合は、パブリック BGP ピアリング IP アドレスを指定します。接続を作成する前に、パブリック IP アドレスの使用が組織で許可されていることを確認してください。または、Equinix ポータルから BGP ピアリングのパブリック IP アドレスを割り当てることもできます。

3. インターコネクト ゲートウェイとして展開する Cisco CSR 1000v インスタンスの UUID が必要な数あることを確認します。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを展開できます。

4. Cisco SD-WAN Manager がインターネットに接続できることを確認します。

   設定ワークフローの一環として、Cisco SD-WAN Manager はインターネットを介して Equinix ポータルに接続します。

5. Cisco SD-WAN Manager が Equinix と対話できるようにするために、Cisco SD-WAN Manager 証明書がルート CA として Cisco（自動）PKI または Symantec によって署名されている必要があります。Cisco（自動）PKI 証明書の使用を推奨します。エンタープライズ CA 証明書は、Cisco vManage リリース 20.9.1 以降でサポートされています。

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の制約事項

一般

- Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、接続を作成および編集できます。

  Cisco Catalyst SD-WAN Manager リリース 20.12.1 より前では、接続は編集できません。接続を削除し、必要な設定を使用して新しい接続を作成することができます。

- 同じ場所のインターコネクト ゲートウェイを同時に作成または削除することはできません。

- すべてのインターコネクトとクラウドの操作には時間制限があります。操作がタイムアウトした場合は、Cisco SD-WAN Manager が失敗を報告します。現在、このタイムアウト値は設定できません。

- グローバル設定を変更すると、変更後に作成された新しいゲートウェイまたは接続に変更が適用されます。変更前に作成されたゲートウェイまたは接続には、変更は影響しません。

- Cisco Catalyst SD-WAN Manager リリース 20.12.1 より前の Cisco SD-WAN Manager を介して、Cisco IOS XE Catalyst SD-WAN リリース 17.3.3 で Equinix インターコネクト ゲートウェイを展開していた場合は、Cisco SD-WAN Manager を Cisco Catalyst SD-WAN Manager リリース 20.12.1 にアップグレードする前に、Equinix インターコネクト ゲートウェイを Cisco IOS XE Catalyst SD-WAN リリース 17.9.x にアップグレードする必要があります。
- Cisco vManage リリース 20.6.1 を使用して Equinix の場所にインターコネクト ゲートウェイを作成した後に、Cisco SD-WAN Manager ソフトウェアを新しいリリースにアップグレードすると、インターコネクト ゲートウェイのポート 443 が無効になります。この制限事項に対応するには、次のいずれかを実行します。
  - ポート 443 を手動で有効にします。
  - Cisco SD-WAN Manager ソフトウェアのアップグレード後に、既存のインターコネクト ゲートウェイを削除し、新しいインターコネクト ゲートウェイを作成します。
- Cisco Catalyst SD-WAN Manager リリース 20.12.2 以降では、マルチクラウドワークフローの一環として作成されたトランジットゲートウェイは、SDCI ワークフローのトランジット接続の下にリストされません。
- Cisco vManage リリース 20.9.5 以降では、Equinix ファブリックで Cisco Catalyst 8000v Edge ソフトウェアをインターコネクト ゲートウェイとして展開できます。

AWS へのインターコネクト

- AWS クラウドリソースへの接続を作成する際は、AWS のクォータと制限に注意してください。Cisco SD-WAN Manager は、すべての AWS のクォータと制限を適用するわけではありません。
- 異なる AWS アカウントに属するクラウドリソースを、単一の接続の一部として使用することはできません。
- Equinix は、ホスト型接続を介したパブリック、プライベート、およびトランジット VIF のみをサポートしています。ホスト型 VIF はサポートされていません。
- プライベート VIF またはトランジット VIF を Direct Connect ゲートウェイにアタッチします。プライベート VIF とトランジット VIF の組み合わせを、同じ Direct Connect ゲートウェイにアタッチすることはできません。
- Cisco vManage リリース 20.9.2 および Cisco vManage リリース 20.10.1 以降では、AWS リージョンのトランジットホスト型接続で、1 つのトランジットゲートウェイのみを Direct Connect ゲートウェイに関連付けることができます。

  Cisco vManage リリース 20.9.1 以前のリリースでは、AWS リージョンの Direct Connect ゲートウェイに、1 つのトランジットゲートウェイのみを関連付けることを推奨します。
- インターコネクト トランジット接続の編集時に、同じリージョン内の VPC タグのない新しいトランジットゲートウェイが選択された場合、接続の更新は破棄されます。
- 特定の VPC へのすべての接続は、以下を満たしている必要があります

- 同じ Direct Connect ゲートウェイとピアリングしている
- 同じトランジットゲートウェイまたは仮想プライベートゲートウェイのアタッチメントがある

- トランジット VIF の場合、トランジットゲートウェイと Direct Connect ゲートウェイは、異なる BGP ASN を使用する必要があります。
- ホスト VPC タグの作成時に、AWS マルチクラウドワークフローまたはインターコネクト接続ワークフローのいずれかを使用して、タグを使用することを選択します。この選択は、タグの作成後は変更できず、タグが削除されるまで維持されます。
- インターコネクト接続用に選択されたホスト VPC タグは、作成後は編集できません。

  Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、ホスト VPC タグを作成および編集できます。

Microsoft Azure へのインターコネクト

- ホスト VNet タグの作成時に、Microsoft Azure マルチクラウドワークフローまたはインターコネクト接続ワークフローのいずれかを使用して、タグを使用することを選択します。この選択は、タグの作成後は変更できず、タグが削除されるまで維持されます。
- インターコネクト接続用に選択されたホスト VNet タグは、作成後は編集できません。

  Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、ホスト VNet タグを作成および編集できます。
- インターコネクト ゲートウェイから Microsoft Azure ExpressRoute へのプライベートピアリング接続を作成するときは、ExpressRoute 回線と同じリソースグループに属する VNet、仮想 WAN、および仮想ハブのみを接続にアタッチできます。別のリソースグループからの VNet、仮想 WAN、および仮想ハブのアタッチは、サポートされていない設定です。

Google Cloud へのインターコネクト

- 各クラウドルータは、すべての BGP セッションに同じ ASN を使用する必要があります。

デバイスリンク

- デバイスグループ内のすべてのリンクの固定帯域幅には、50 Mbps ～ 10 Gbps の範囲を使用できます。
- 特定のメトロのすべてのリンクの累積帯域幅は、10 Gbps を超えることはできません。

暗号化されたマルチクラウド インターコネクトの制約事項

サポート対象の最小リリース：Cisco vManage リリース 20.9.1

AWS へのインターコネクト

- AWS の要件に従って、
  - クラウドゲートウェイの最小インスタンスタイプは x-large である必要があります。
  - 1 つのインターコネクト接続に最大 10 個のクラウドゲートウェイをアタッチできます。
  - 1 つのクラウドゲートウェイは、30 個のインターコネクト接続に接続できます。

Microsoft Azure へのインターコネクト

- 1 つのクラウドゲートウェイを 8 つの異なるクラウドインターコネクト接続にアタッチでき、1 つのインターコネクト接続を 5 つの異なるクラウドゲートウェイに接続できます。
- 異なるリージョンのクラウドゲートウェイに接続するには、ExpressRoute 回線が Premium タイプである必要があります。
- Microsoft Azure 展開では、クラウドゲートウェイの WAN インターフェイスで Cisco Catalyst SD-WAN トンネルの色は自動的に設定されないため、WAN インターフェイスの色を手動で更新する必要があります。テンプレートの色がブランチルータ、インターコネクトゲートウェイ、およびクラウドゲートウェイの色と一致していることを確認します。

Google Cloud へのインターコネクト

- Google Cloud ゲートウェイへのクラウドインターコネクト接続は、冗長性が有効になっている場合にのみサポートされます。
- 1 つの接続にアタッチできる Google Cloud ゲートウェイは 1 つだけです。
- 既存の Google Cloud ゲートウェイは、クラウドインターコネクトではサポートされません。
- リージョンとネットワークの組み合わせに対して、最大 5 つの Google Cloud Router を作成できます。

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の使用上の注意

表 *78* : 接続設定の制限

説明	カウント
インターコネクト ゲートウェイ	
インターコネクトゲートウェイあたりの最大接続数（VXC）	20 **注**：集約 VXC 帯域幅がインターコネクト ゲートウェイの帯域幅容量を超えることはできません。

説明	カウント
AWS へのインターコネクト	
プライベート VIF の AWS への接続あたりの VPC の最大数	10
トランジット VIF の AWS への接続あたりの VPC の数	デフォルト：15 最大：15,000
トランジット VIF の AWS への接続あたりのトランジットゲートウェイの最大数	3
接続あたりの Direct Connect ゲートウェイの最大数	1
AWS Direct Connect ゲートウェイあたりの VIF（プライベートまたはトランジット）の最大数	デフォルト：30 制限はリクエストに応じて増やすことができます。
AWS Direct Connect ホスト型接続あたりのプライベート、パブリック、またはトランジット VIF の最大数	1
トランジット VIF のブランチの場所から AWS へのプレフィックスの最大数	100
トランジット VIF の AWS からブランチの場所への AWS Transit Gateway あたりのプレフィックスの最大数	20
Microsoft Azure へのインターコネクト	
ExpressRoute に接続できるインターコネクト ゲートウェイの最大数	2
ExpressRoute が接続できる VNet の最大数	10
VNet に接続できる ExpressRoute の最大数	4
仮想ハブに接続できる ExpressRoute の最大数	ピアリングの場所あたり 8
仮想 WAN ExpressRoute ゲートウェイあたりの最大総スループット	20 Gbps
仮想ハブに接続できる VNet の最大数	500 ～（仮想 WAN 内の仮想ハブの合計数）

AWS へのインターコネクト

- AWS へのプライベート VIF 接続を削除すると、Cisco SD-WAN Manager は、接続の確立中に作成された VIF、仮想プライベートゲートウェイ、およびルートテーブルを削除します。
- トランジット VIF 接続を削除すると、Cisco SD-WAN Manager は、接続の確立中に作成された Direct Connect ゲートウェイ、トランジットゲートウェイ、または仮想プライベートゲートウェイへのアタッチメントと関連付けを削除します。
- AWS への接続の作成中に、Cisco SD-WAN Manager から Direct Connect ゲートウェイまたはトランジットゲートウェイを作成した場合、接続を削除してもゲートウェイは削除されません。必要に応じて、これらの AWS リソースを管理する必要があります。

  Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、接続の削除中に Direct Connect ゲートウェイまたはトランジットゲートウェイを削除するオプションがあります。
- 接続を作成すると、新しいルートテーブルが作成され、接続にアタッチされたホスト VPC のメインルートテーブルとして設定されます。トランジットゲートウェイへのデフォルトルートがメインルートテーブルに作成され、ルート伝達が有効になります。必要に応じてルートと伝達を編集します。

  Cisco vManage リリース 20.5.1 以降では、インターコネクトによってアクセスする必要があるスタティックルートとサブネットの関連付けを、Cisco SD-WAN Manager によって新しく作成されたメインルートテーブルに移動する必要があります。

Google Cloud へのインターコネクト

- 非冗長接続の場合は、各ネットワークリージョンに Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成する必要があります。
- 冗長接続の場合は、各ネットワークリージョンに 2 つの Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成する必要があります。
- インターコネクト アタッチメントで使用するには、Google Cloud Router の Google ASN を 16550 に設定する必要があります。

Microsoft Azure へのインターコネクト

- ExpressRoute にアタッチされた VNet への HA 接続を提供するために特定の ExpressRoute に接続できるインターコネクト ゲートウェイのペアは、1 つだけです。

  インターコネクト ゲートウェイの 2 番目のペアを同じ vNet に接続するには、別の ExpressRoute を作成し、vNet を ExpressRoute にアタッチして、インターコネクト ゲートウェイを ExpressRoute に接続します

  VNet に接続するこのような ExpressRoute を最大 4 つ用意して、各 ExpressRoute をインターコネクト ゲートウェイのペアに接続することができます。

- ExpressRoute は最大 10 個の VNet に接続できます。インターコネクト ゲートウェイから ExpressRoute への接続を作成するときに、VNet を ExpressRoute にアタッチすることができます。VNet は、接続用に選択した VNet タグに基づいてアタッチされます。

  10 個を超える VNet に適用される VNet タグを選択した場合、または選択される VNet の総数が 10 個を超えるような VNet タグの組み合わせを選択した場合、インターコネクトの作成は失敗します。

（注） インターコネクト ゲートウェイからの接続を作成するときに ExpressRoute にアタッチできる VNet の数の決定では、Azure ポータルから ExpressRoute にアタッチした可能性のある VNet も考慮されます。

- VNet は、VNet ゲートウェイまたは ExpressRoute ゲートウェイに接続できます。そのため、VNet ゲートウェイを介した VNet へのプライベートピアリングを作成した場合、ExpressRoute ゲートウェイを介した同じ VNet へのプライベートピアリングを作成することはできません。その逆も同様です。
- VNet が仮想 WAN の仮想ハブに接続されている場合、同じ VNet を別の仮想 WAN に接続することはできません。
- リージョン内のすべての VNet は、同じリージョン内の単一の仮想ハブに接続する必要があります。
- デフォルトは冗長接続であり、この設定のみがサポートされています。Equinix ファブリック内のインターコネクト ゲートウェイのペアから Microsoft Azure への接続を作成する必要があります。

  Microsoft Azure ExpressRoute へのプライマリ接続とセカンダリ接続を作成するインターコネクト ゲートウェイのペアを選択するときは、インターコネクト ゲートウェイが BGP ピアリングに同じ BGP ASN を使用するように設定されていることを確認します。

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix に関する情報

Cisco SD-WAN Manager から、Cisco Cloud Services Router 1000v（Cisco CSR 1000v）インスタンスを SDCI プロバイダーである Equinix のファブリックに展開し、そのインスタンスを WAN エッジデバイスとして Cisco SD-WAN ファブリックに追加することができます。WAN エッジデバイスとして、Cisco CSR 1000v インスタンスはブランチの場所を Equinix ファブリックにリンクします。Equinix ファブリックでは、Cisco CSR 1000v インスタンスはインターコネクト ゲートウェイとして機能します。インターコネクト ゲートウェイから、Equinix ファブリック内の Cloud OnRamp または別のインターコネクト ゲートウェイへの直接レイヤ 2 接続（インターコネクト）を作成することができます。インターコネクトは、Equinix ファブリックのイ

ンターコネクト ゲートウェイを介してブランチの場所間をリンクするか、ブランチの場所とクラウド サービス プロバイダー間をリンクします。

このセットアップでは、Cisco SD-WAN ファブリックがオーバーレイネットワークとして機能し、Equinix ファブリックがアンダーレイネットワークとして機能します。Equinix ファブリックは、世界全体の複数の場所にあるクラウドリソースへの、効率的で、高速、低遅延、高帯域幅な接続を提供します。ブランチの場所に最も近い Equinix の場所に Cisco CSR 1000v インスタンスを展開することをお勧めします。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを展開できます。

インターコネクト ゲートウェイからの次のタイプの接続を作成できます。

表 *79*：接続のタイプ

接続先	接続のタイプ	サポート対象ソフトウェアリリース
Amazon Web Services	• インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect プライベートホスト型接続 • インターコネクト ゲートウェイから AWS への Direct Connect パブリックホスト型接続 • インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect トランジットホスト型接続	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a と Cisco Catalyst SD-WAN Manager リリース 20.12.1 を備えた Cisco Catalyst 8000v Cisco IOS XE Catalyst SD-WAN リリース 17.3.3 を備えた Cisco CSR 1000v
Microsoft Azure	• パートナー ExpressRoute 回線：Microsoft ピアリング • パートナー ExpressRoute 回線：プライベートピアリング	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a と Cisco Catalyst SD-WAN Manager リリース 20.12.1 を備えた Cisco Catalyst 8000v Cisco IOS XE Catalyst SD-WAN リリース 17.3.3 を備えた Cisco CSR 1000v

接続先	接続のタイプ	サポート対象ソフトウェアリリース
Google クラウド	Google Cloud Router へのパートナーインターコネクト アタッチメント	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a と Cisco Catalyst SD-WAN Manager リリース 20.12.1 を備えた Cisco Catalyst 8000v Cisco IOS XE リリース 17.3.3 を備えた Cisco CSR 1000v
インターコネクト ゲートウェイ	インターコネクト ゲートウェイに接続された Cisco Catalyst SD-WAN のブランチの場所間のリンク	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a と Cisco Catalyst SD-WAN Manager リリース 20.12.1 を備えた Cisco Catalyst 8000v Cisco IOS XE Catalyst SD-WAN リリース 17.3.3 を備えた Cisco CSR 1000v。

Cisco Catalyst SD-WAN Manager は統合管理ポータルとして機能し、次のタスクを実行できます。

- Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスの設定。

  Cisco Catalyst SD-WAN Manager リリース 20.12.1 より前では、Equinix の場所での Cisco CSR 1000v インスタンスの設定および展開。

- パブリッククラウドリソースへのクラウドインターコネクトの作成。
- Equinix ファブリックを介して Cisco Catalyst SD-WAN のブランチの場所をリンクするためのインターコネクトの作成。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを Equinix ファブリックのインターコネクト ゲートウェイとして展開し、Cisco Catalyst SD-WAN ブランチの場所をインターコネクト ゲートウェイに接続することができます。既存の Cisco CSR1000V 展開を使用して接続を作成することができます。

考慮すべき点

以前の Cisco Catalyst SD-WAN Manager のバージョンから Cisco Catalyst SD-WAN Manager リリース 20.12.1 にアップグレードする場合は、Cisco Catalyst 8000v を有効にするために、次の手順を実行します。

- [Edit Account Credentials] を使用して既存の Equinix アカウントを再認証し、カスタマーキーとカスタマーシークレットを入力します。以前のバージョンで使用していたものと同じキーとシークレットを使用できます。Cisco Catalyst 8000v で使用可能な請求アカウントと場所が内部で更新されます。アカウントの詳細の編集については、「View, Edit, or Delete an Interconnect Account」を参照してください。
- アカウントが再認証されたら、インターコネクト ゲートウェイの**グローバル設定**を更新して、新しいゲートウェイの Cisco Catalyst 8000v ソフトウェアバージョンとその他のパラメータを選択する必要があります。グローバル設定の更新については、「Configure Global Settings for Equinix Interconnect Gateways」を参照してください。
- Cisco Catalyst SD-WAN Manager リリース 20.12.1 より前の Cisco SD-WAN Manager を介して Cisco IOS XE Catalyst SD-WAN リリース 17.3.3 を使用して Equinix インターコネクト ゲートウェイを展開していた場合は、Cisco Catalyst SD-WAN Manager リリース 20.12.1 にアップグレードする前に、Equinix インターコネクト ゲートウェイを Cisco IOS XE Catalyst SD-WAN リリース 17.3.3 から Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a または Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a にアップグレードする必要があります。

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の利点

1. ブランチの場所が、Cisco Catalyst SD-WAN ファブリックを介して Equinix ファブリックにシームレスに接続します。
2. SLA が保証されたパブリッククラウドへのインターコネクト。
3. Cisco Catalyst SD-WAN ファブリックを介したエンドツーエンドのトラフィックのセキュリティ、セグメンテーション、およびポリシー。
4. Cisco SD-WAN Manager が、クラウドへの接続を管理するための単一のペインを提供します。
5. Cisco Catalyst SD-WAN と Equinix ファブリック全体のエンドツーエンドの可視性。
6. Cisco Catalyst SD-WAN のブランチの場所間、および Cisco Catalyst SD-WAN のブランチの場所とパブリッククラウド間のリンク。

暗号化されたマルチクラウド インターコネクト

サポート対象の最小リリース：Cisco vManage リリース 20.9.1

Cisco SD-WAN Manager の Cloud OnRamp ワークフローを使用して、インターコネクト ゲートウェイとクラウド サービス プロバイダー間のセキュアなプライベート Cisco Catalyst SD-WAN 接続をプロビジョニングすることができます。クラウド インターコネクト プロバイダーのインターコネクト ゲートウェイから、マルチクラウドワークフローの一環として作成された既存のクラウドゲートウェイへの仮想クロスコネクトを終了できます。詳細については、「Cloud OnRamp for Multicloud （255 ページ）」を参照してください。この機能により、VPC および

VNETワークロードにアクセスするためのインターネットパスとプライベートパスの両方がサポートされます。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、暗号化されたマルチクラウドインターコネクトは、クラウド WAN ソリューションを使用した AWS クラウドゲートウェイをサポートしています。

利点

- クラウド インターコネクト プロバイダー バックボーンを介して、ブランチサイトからクラウドゲートウェイまでのエンドツーエンドの暗号化を提供します。
- 単一の仮想クロスコネクトで複数の VPN セグメントをサポートしています。
- 接続の作成前後の VPC および VNET タグの変更をサポートしています。VPN から VPC または VNET タグへのマッピングは、[Multicloud Intent Management] 画面を使用して実行できます。
- クラウド サービス プロバイダーによって課されるプレフィックス アドバタイズメントの制限を解消するために、ルートアドバタイズメントがインターコネクト ゲートウェイとクラウドゲートウェイによって制御されます。

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の設定ワークフロー

前提条件の設定

1. Equinix ポータルでアカウントを作成します。Equinix の「New User Equinix Fabric Portal Access」のドキュメントを参照してください。

   アカウントを作成したら、アカウントのクライアントID（コンシューマキー）とクライアント シークレット キー（コンシューマシークレット）を生成します。Equinix Developer Platform Knowledge Center の「Generating Client ID and Client Secret Key」のドキュメントを参照してください。

   また、このアカウントを使用してインターコネクト ゲートウェイを展開する各リージョンの請求アカウントを作成します。Equinix の「Billing Account Management」のドキュメントを参照してください。

2. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
3. インターコネクト ゲートウェイのグローバル設定を構成します。
4. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
5. インターコネクト ゲートウェイとして展開する Cisco CSR 1000v インスタンスの UUID が必要な数あることを確認します。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを展開します。

6. Equinix テンプレートを Cisco CSR 1000v インスタンスにアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスをアタッチできます。

7. Cisco Catalyst SD-WAN のブランチの場所に最も近い Equinix の場所でインターコネクト ゲートウェイを作成します。

   クラウドプロバイダーへの接続のために、Equinix の場所でインターコネクト ゲートウェイを作成します。

   Cisco Catalyst SD-WAN のブランチの場所間の接続のために、ブランチの場所ごとに、最も近い Equinix の場所でインターコネクト ゲートウェイを作成します。

AWS へのインターコネクトを作成するためのワークフロー

次の設定手順を実行する前に、前提条件が満たされ、前提条件の設定が適用されていることを確認してください。

1. AWS アカウントを Cisco SD-WAN Manager に関連付けます。
2. AWS 仮想プライベートクラウド（VPC）に接続するためのホストプライベートネットワークを検出します。
3. 次のいずれかのタイプの接続を作成します。

接続タイプ	ヒント
Direct Connect：パブリックホスト型接続	この接続は、パブリック AWS リソースへのリンクに使用します。リンクの固定帯域幅は最大 10 Gbps です。
Direct Connect：プライベートホスト型接続	この接続は、AWS VPC への専用リンクに使用します。リンクの帯域幅は最大 10 Gbps です。
Direct Connect：トランジットホスト型接続	この接続は、トランジットゲートウェイを介した最大 5,000 の AWS VPC への専用リンクに使用します。リンクの帯域幅は最大 10 Gbps です。最大 3 つのトランジットゲートウェイを Direct Connect ゲートウェイにアタッチし、最大 15,000 の VPC に接続することができます。

Cisco Catalyst SD-WAN のブランチの場所をリンクするためのワークフロー

次の設定手順を実行する前に、前提条件が満たされ、前提条件の設定が適用されていることを確認してください。

- インターコネクト ゲートウェイ間のインターコネクトを作成します。

Google Cloud へのインターコネクトを作成するためのワークフロー

次の設定手順を実行する前に、前提条件が満たされ、前提条件の設定が適用されていることを確認してください。

1. Google Cloud ポータルを使用して、必要な VPC ネットワークを作成します。
2. 接続するネットワークリージョンに Google Cloud Router を展開します。

   非冗長接続の場合は、Google Cloud ポータルを使用して、接続する各ネットワークリージョンに Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成します。

   冗長接続の場合は、Google Cloud ポータルを使用して、接続する各ネットワークリージョンに 2 つの Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成します。

   Cisco vManage リリース 20.9.1 以降では、Cisco SD-WAN Manager のインターコネクト ワークフローを介して Google Cloud Router と VLAN アタッチメントを展開できます。
3. Google Cloud アカウントを Cisco SD-WAN Manager に関連付けます。
4. インターコネクト ゲートウェイから Google Cloud Router へのインターコネクトを作成します。

Microsoft Azure へのインターコネクトを作成するためのワークフロー

次の設定手順を実行する前に、前提条件が満たされ、前提条件の設定が適用されていることを確認してください。

1. Microsoft Azure アカウントを Cisco SD-WAN Manager に関連付けます。
2. Azure Virtual Network（VNet）に接続するためのホスト プライベート ネットワークを検出します。
3. 次のいずれかのタイプの接続を作成します。
   - Azure ExpressRoute へのパブリック ピアリング接続
   - Azure ExpressRoute へのプライベート ピアリング接続

Cisco SD-WAN Cloud Interconnect with Equinix の前提条件の設定

Cisco SD-WAN Manager と Equinix アカウントの関連付け

前提条件

1. Equinix ポータルでアカウントを作成します。Equinix の「New User Equinix Fabric Portal Access」のドキュメントを参照してください。
2. アカウントを作成したら、アカウントのクライアント ID（コンシューマキー）とクライアント シークレット キー（コンシューマシークレット）を生成します。Equinix Developer Platform Knowledge Center の「Generating Client ID and Client Secret Key」の情報を参照してください。
3. このアカウントを使用してインターコネクト ゲートウェイを展開する各リージョンの請求アカウントを作成します。Equinix の「Billing Account Management」のドキュメントを参照してください。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Associate Interconnect Account] をクリックします。
4. 次を設定します。

Interconnect Provider	[EQUINIX] を選択します。
アカウント名	任意の名前を入力します。この名前は、クラウドまたはサイト間インターコネクトを定義するワークフローで Equinix アカウントを識別するために使用されます。
[説明（Description）]（任意）	説明を入力します。
Customer Key	クライアント ID（コンシューマキー）を入力します。
Customer Secret	クライアント シークレット キー（コンシューマシークレット）を入力します。

5. [Add] をクリックします。

Cisco SD-WAN Manager はアカウントを認証し、アカウントの詳細をデータベースに保存します。

Equinix インターコネクト ゲートウェイのグローバル設定の構成

前提条件

1. Equinix ポータルでアカウントを作成します。Equinix の「New User Equinix Fabric Portal Access」のドキュメントを参照してください。
2. アカウントを作成したら、アカウントのクライアント ID（コンシューマキー）とクライアント シークレット キー（コンシューマシークレット）を生成します。Equinix Developer Platform Knowledge Center の「Generating Client ID and Client Secret Key」の情報を参照してください。
3. このアカウントを使用してインターコネクト ゲートウェイを展開する各リージョンの請求アカウントを作成します。Equinix の「Billing Account Management」のドキュメントを参照してください。
4. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Global Settings] をクリックします。
   - グローバル設定を追加するには、[Add] をクリックします。
   - グローバル設定を変更するには、[Edit] をクリックします。
4. 次を設定します。

設定グループの有効化	Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、このオプションを有効にして、設定グループを使用してマルチクラウド ワークフローでデバイスを設定します。 このオプションは、デフォルトで無効です。 （注） ここで設定グループを有効にすると、すべてのクラウド プロバイダーに対して設定グループが有効になります。たとえば、ここでこのオプションを有効にすると、他のすべてのマルチクラウドおよびインターコネクト プロバイダーの設定グループも有効になります。
Interconnect Provider	[EQUINIX] を選択します。

ソフトウェア イメージ	Cisco CSR 1000v イメージを選択します。 Cisco Catalyst SD-WAN Manager リリース 20.12.1 の場合は、Cisco Catalyst 8000v イメージを選択します。
Instance Size	インスタンスのサイズは、各 Cisco CSR 1000v インスタンスのコンピューティング フットプリントとスループットを決定します。次のいずれかを選択します。 • [Small]：2vCPU、4 GB DRAM、最大 1 Gbps • [Medium]：4vCPU、4 GB DRAM、最大 2.5 Gbps • [Large]：6vCPU、4 GB DRAM、最大 2.5 Gbps Cisco Catalyst SD-WAN Manager リリース 20.12.1 の場合、インスタンスサイズは次のとおりです。 • [Small]：2vCPU、8 GB DRAM、最大 1 Gbps • [Medium]：4vCPU、8 GB DRAM、最大 2.5 Gbps • [Large]：6vCPU、16 GB DRAM、最大 2.5 Gbps • [xLarge]：8vCPU、16 GB DRAM、最大 2.5 Gbps
Interconnect Transit Color	インターコネクト ゲートウェイ間の接続に割り当てる色を選択します。 この色は、ブランチの場所間を直接ピアリングしないように制限されています。同じ色を Cisco Catalyst SD-WAN ファブリック内の別の接続に割り当てないでください。 （注） プライベートの色を使用することをお勧めします。デフォルトの色は使用しないでください。
BGP ASN	インターコネクト ゲートウェイとクラウドプロバイダー間のピアリングに使用される BGP ASN を入力します。 任意の ASN を入力するか、組織で使用されている既存の ASN を再利用できます。

Interconnect CGW SDWAN Color	サポート対象の最小リリース：Cisco vManage リリース 20.9.1 インターコネクト ゲートウェイがクラウドゲートウェイに接続する際のインターフェイスに使用する色を選択します。 （注） インターフェイスに割り当てられる色は、インターコネクト ゲートウェイ デバイスに対して一意であり、クラウドインターコネクト プロバイダー間では共通である必要があります。 Microsoft Azure 展開では、クラウドゲートウェイの WAN インターフェイスで Cisco Catalyst SD-WAN トンネルの色は自動的に設定されないため、WAN インターフェイスの色を手動で更新する必要があります。テンプレートの色がブランチルータ、インターコネクト ゲートウェイ、およびクラウドゲートウェイの色と一致していることを確認します。

5. 新しく追加したグローバル設定を保存するには、[Save] をクリックします。

   変更したグローバル設定を保存するには、[Update] をクリックします。

Cisco CSR 1000v または Cisco Catalyst 8000v インスタンスへの Equinix テンプレートのアタッチ

（注） 設定グループを有効にした場合、この手順は必要ありません。この場合は、「Create Interconnect Gateway at an Equinix Location」に進みます。

Equinix の場所で Cisco CSR 1000v インスタンスをインターコネクト ゲートウェイとして展開する前に、Equinix のデフォルトテンプレートをデバイスにアタッチする必要があります。Default_EQUINIX_DHCP_DNS_ICGW_CSR1000V_Template_V02 という名前のテンプレートをアタッチすることを推奨します。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 の場合、Cisco Catalyst 8000v のデフォルトテンプレートは Default_EQUINIX_ICGW_C8000V_Template_V01 です。

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 20.7.1 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Template Type] として [Default] を選択し、Default_EQUINIX_DHCP_DNS_ICGW_CSR1000V_Template_V02 という名前のテンプレートを見つけます。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 の場合、デフォルトの Default_EQUINIX_ICGW_C8000V_Template_V01 を選択します。

4. [...] をクリックして、[Attach Devices] をクリックします。
5. [Available Devices] のリストから目的の Cisco CSR 1000v インスタンスの UUID を選択し、そのインスタンスを [Selected Devices] のリストに移動します。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを選択します。

6. [Attach] をクリックします。
7. テンプレートには変数が含まれています。テンプレートの変数の値を入力するには、[…] をクリックし、[Edit Device Template] をクリックします。
8. 次の変数の値を入力し、[Update] をクリックします。
   - DNS アドレス（vpn_dns_primary）
   - DNS アドレス（vpn_dns_secondary）
   - 色（vpn_if_tunnel_color_value）
   - システム IP（system-ip）
   - サイト ID（site-id）
   - ホスト名（host-name）
9. [Next] をクリックします。
10. [Configure Devices] をクリックします。

Equinix の場所でのインターコネクト ゲートウェイの作成

目的の Equinix の場所に、インターコネクト ゲートウェイとして Cisco CSR 1000v インスタンスを展開します。ブランチの場所に最も近い Equinix の場所に Cisco CSR 1000v インスタンスを展開することをお勧めします。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを展開できます。

前提条件

1. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。

3. 設定グループを有効にしなかった場合は、Equinix テンプレートを Cisco CSR 1000v インスタンスにアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、テンプレートを Cisco Catalyst 8000v インスタンスにアタッチします。

4. 設定グループを有効にした場合は、設定グループに関連付けられているデバイスのデバイスパラメータが設定されていることを確認します。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Create Interconnect Gateway] をクリックします。
4. 次を設定します。

Interconnect Provider	[EQUINIX] を選択します。
ゲートウェイ名	ゲートウェイを一意に識別する名前を入力します。
[説明（Description）]（任意）	説明を入力します。
アカウント名	Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Equinix アカウントを選択します。
参照先	1. [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 2. Cisco CSR 1000v インスタンスを展開する必要がある Equinix の場所を選択します。 Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを選択します。
Billing Account ID	場所に適した請求アカウントを選択します。
サイト名	サイトを選択します。 Cisco vManage リリース 20.10.1 以降では、[Site Name] フィールドを使用できます。

設定グループ	Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、クラウドゲートウェイを作成したとき、またはインターコネクト ゲートウェイのグローバル設定を構成したときに [Enable Configuration Group] オプションを有効にした場合は、次のいずれかのアクションを実行します。 • 構成グループを選択します。 • 新しい設定グループを作成して使用するには、[Create New] を選択します。[Create Configuration Group] ダイアログボックスで、新しい設定グループの名前を入力し、[Done] をクリックします。ドロップダウンリストから新しい設定グループを選択します。 選択した設定グループは、マルチクラウドワークフローでデバイスを設定するために使用されます。 設定グループの詳細については、『Cisco Catalyst SD-WAN Configuration Groups』を参照してください。 （注） • [Configuration Group] ドロップダウンリストには、このドロップダウンリストから作成した設定グループのみが含まれています。Cisco Catalyst SD-WAN で作成された他の設定グループは含まれません。このドロップダウンリストの設定グループには、このプロバイダーに必要なオプションが含まれています。 • 設定グループを使用して Equinix インターコネクト ゲートウェイを作成する場合、Cisco SD-WAN Manager からの SSH の使用は、インターコネクト ゲートウェイが Cisco Catalyst 8000v 17.13 以降の場合にのみ機能します。
UUID	Equinix のデフォルトテンプレートがアタッチされている Cisco CSR 1000v インスタンスの UUID を選択します。 （注） サイト名を選択すると、サイト名に関連付けられた UUID が [UUID] フィールドに自動的に入力されます。 Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを選択します。
設定	次のいずれかを選択します。 • [Default]：インターコネクトのグローバル設定で定義されたインスタンスサイズとソフトウェアイメージを使用します。 • [Custom]：このゲートウェイの特定のインスタンスサイズとソフトウェアイメージを選択します。

5. [Add] をクリックします。

設定タスクが成功すると、インターコネクト ゲートウェイが [Gateway Management] ページにリストされます。

（注） 先に進む前に、インターコネクト ゲートウェイの [Device Status] 列に [In Sync] と表示され、証明書が正常にインストールされていることを確認します。

AWS へのインターコネクトの作成

AWS アカウントと Cisco SD-WAN Manager の関連付け

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Cloud] をクリックします。
3. [Associate Cloud Account] をクリックします。
4. 次を設定します。

Cloud Provider	[Amazon Web Services] を選択します。
Cloud Account Name	任意の名前を入力します。
[説明（Description）]（任意）	説明を入力します。
Use for Cloud Gateway	[No] を選択します。
Log in to AWS with	[Key] または [IAM Role] を選択します。
Role ARN	API/秘密キーまたはロール ARN を入力します。

5. [Add] をクリックします。

Cisco SD-WAN Manager は、AWS への接続を作成するための API ワークフローの一環として、API/秘密キーまたはロール ARN を使用して AWS でユーザーアカウントを認証します。

ホスト プライベート ネットワークの検出と AWS VPC のタグ付け

複数のホスト VPC を、タグを使用してグループ化できます。同じタグの下の VPC は、単一のユニットと見なされます。インターコネクト ゲートウェイからのソフトウェア定義型のクラウドインターコネクトを作成する AWS VPC にタグを付けます。

前提条件

AWS アカウントを Cisco SD-WAN Manager に関連付けます。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Host Private Networks] をクリックします。
4. [Cloud Provider]：[Amazon Web Services] を選択します。

   使用可能なホスト VPC が検出され、表に一覧表示されます。

   [host VPC] テーブルには次の列があります。

   - クラウド リージョン
   - アカウント名
   - ホスト VPC 名
   - ホスト VPC タグ
   - Interconnect Enabled
   - アカウント ID（Account ID）
   - ホスト VPC ID

5. 左端の列のチェックボックスを使用して、タグ付けする VPC を選択します。
6. [Tag Actions] をクリックします。

   次の操作を実行できます。

   - [Add Tag]：選択した VPC をグループ化し、これらの VPC に同時にタグ付けします。
   - [Edit Tag]：選択した VPC をあるタグから別のタグに移行します。
   - [Delete Tag]：選択した VPC のタグを削除します。

7. [Add Tag] をクリックして、以下を設定します。

[Tag Name]	選択した VPC をリンクするタグの名前を入力します。
リージョン	選択した VPC に対応するリージョンのリスト。タグからリージョンおよび関連する VPC を除外するには、[X] をクリックします。
Selected VPCs	選択したホスト VPC の VPC ID のリスト。タグから VPC を除外するには、[X] をクリックします。

（Cisco vManage リリース 20.8.1 以前） Enable for Interconnect Connectivity （Cisco vManage リリース 20.9.1 以降） Enable for SDCI partner Interconnect Connections	AWS へのクラウドインターコネクト接続を作成するときに VPC タグを使用するには、このチェックボックスをオンにします。 有効にすると、タグはクラウドインターコネクト接続にのみ使用でき、マルチクラウドゲートウェイ インテントマッピングには使用できません。 このチェックボックスをオンにしない場合、VPC タグを使用してクラウドインターコネクト接続を作成することはできません。 （注） クラウドゲートウェイを使用して VPC ワークロードを接続する場合、この設定を有効にしないでください。タグが接続で使用されている場合は、この設定を編集できません。

8. [Add] をクリックします。

[Discover Host Private Networks] ページで、先ほど選択した VPC にタグが付けられ、タグ名が [Host VPC Tag] 列に表示されます。ソフトウェア定義型のクラウドインターコネクトに VPC タグを使用することを選択した場合、[Interconnect Enabled] 列に [Yes] と表示されます。

インターコネクト ゲートウェイから AWS への Direct Connect パブリックホスト型接続の作成

前提条件

1. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. AWS アカウントを Cisco SD-WAN Manager に関連付けます。
5. Equinix テンプレートを Cisco CSR 1000v インスタンスにアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスをアタッチします。
6. Equinix の場所でインターコネクト ゲートウェイを作成します。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。

2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[EQUINIX] を選択します。
5. [Choose Interconnect Account]：アカウント名で Equinix アカウントを選択します。このアカウント名は、Cisco SD-WAN Manager でアカウントを関連付ける際に入力した名前です。
6. [Choose Interconnect Gateway]：Direct Connect 接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービスプロバイダー	[AWS] を選択します。
Connection Name	接続の一意の名前を入力します。
AWS Account	Cisco SD-WAN Manager で AWS アカウントの詳細を関連付ける際に入力したアカウント名で AWS アカウントを選択します。

9. 以下を設定し、[Next] をクリックします。

Equinix Hosted Connection VIF Type	[Public] を選択します。
参照先	1. [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 2. AWS Direct Connect の場所を選択します。
帯域幅	接続帯域幅を選択します。 単位：Mbps。
Interconnect IP Address	インターコネクト ゲートウェイの BGP ピア ID として使用するパブリック IP アドレス（CIDR）を入力します。
Amazon IP Address	AWS BGP ピア ID として使用するパブリック IP アドレス（CIDR）を入力します。
Prefixes	ブランチの場所にアドバタイズするサマリー AWS アドレスとプレフィックスを入力します。
Segment	この接続のセグメント ID を選択します。

10. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。
- 接続設定を変更するには、[Back] をクリックします。

設定タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect プライベートホスト型接続の作成

前提条件

1. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. AWS アカウントを Cisco SD-WAN Manager に関連付けます。
5. ホスト プライベート ネットワークを検出して AWS VPC にタグ付けします。
6. Equinix テンプレートを Cisco CSR1000v インスタンスにアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスをアタッチします。
7. Equinix の場所でインターコネクト ゲートウェイを作成します。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[EQUINIX] を選択します。
5. [Choose Interconnect Account]：アカウント名で Equinix アカウントを選択します。このアカウント名は、Cisco SD-WAN Manager でアカウントを関連付ける際に入力した名前です。
6. [Choose Interconnect Gateway]：Direct Connect 接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービスプロバイダー	[AWS] を選択します。
Connection Name	接続の一意の名前を入力します。
AWS Account	Cisco SD-WAN Manager で AWS アカウントの詳細を関連付ける際に入力したアカウント名で AWS アカウントを選択します。

9. 以下を設定し、[Next] をクリックします。

Equinix Hosted Connection VIF Type	[Private] を選択します。
参照先	**1.** [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 **2.** AWS Direct Connect の場所を選択します。
帯域幅	接続帯域幅を選択します。 単位：Mbps。
Direct Connect Gateway	**1.** [Refresh] ボタンをクリックして、選択した AWS アカウントに関連付けられている Direct Connect ゲートウェイを取得します。 **2.** Direct Connect 接続を作成する必要がある先の Direct Connect ゲートウェイを選択します。 または、[Add New Direct Connect Gateway] をクリックして、新しい Direct Connect ゲートウェイを作成します。 **1.** [Gateway Name] を入力します。 **2.** ゲートウェイの [BGP ASN] を入力します。 **3.** [Save] をクリックします。

設定	次のいずれかを選択します。 • [Global]： • BGP ピアリング IP アドレスは、内部で予約済みの /16 サブネットから選択されます（198.18.0.0/16）。 • BGP ASN は、グローバル設定から選択されます。 • [Custom]： • BGP ピアリングのカスタム /30 CIDR IP アドレスを入力します。 • ピアリング用のカスタム BGP ASN を入力します。 （注） インターコネクト ゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN を指定できます。インターコネクト ゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。

添付ファイル	Cisco vManage リリース 20.8.1 以前の場合： [VPC] を選択します。 [Segment]：この接続のセグメント ID を選択します。 [VPC Tags]：VPC タグを選択して、この接続を介してトラフィックをルーティングする必要がある VPC を識別します。
	Cisco vManage リリース 20.9.1 以降の場合： 次のいずれかを選択します。 • **VPC** [Segment]：この接続のセグメント ID を選択します。 [VPC Tags]：VPC タグを選択して、この接続を介してトラフィックをルーティングする必要がある VPC を識別します。 • Cloud Gateway [Cloud Gateways]：この接続にアタッチするクラウドゲートウェイを選択します。ドロップダウンが空の場合は、最初にマルチクラウドワークフローを使用してクラウドゲートウェイを作成する必要があります。単一接続の場合、AWS は最大 10 個のクラウドゲートウェイをサポートします。各クラウドゲートウェイは、30 個のインターコネクト接続に接続できます。

10. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。
- 接続設定を変更するには、[Back] をクリックします。

設定タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect トランジットホスト型接続の作成

前提条件

1. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。

2. インターコネクト ゲートウェイのグローバル設定を構成します。

3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. AWS アカウントを Cisco SD-WAN Manager に関連付けます。
5. ホスト プライベート ネットワークを検出して AWS VPC にタグ付けします。
6. Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスをアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 より前のバージョンの場合は、Equinix テンプレートを Cisco CSR 1000v インスタンスにアタッチします。
7. Equinix の場所でインターコネクト ゲートウェイを作成します。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[EQUINIX] を選択します。
5. [Choose Interconnect Account]：アカウント名で Equinix アカウントを選択します。このアカウント名は、Cisco SD-WAN Manager でアカウントを関連付ける際に入力した名前です。
6. [Choose Interconnect Gateway]：Direct Connect 接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービス プロバイダー	[AWS] を選択します。
Connection Name	接続の一意の名前を入力します。
AWS Account	Cisco SD-WAN Manager で AWS アカウントの詳細を関連付ける際に入力したアカウント名で AWS アカウントを選択します。

9. 以下を設定し、[Next] をクリックします。

Equinix Hosted Connection VIF Type	[Transit] を選択します。

参照先	**1.** [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 **2.** AWS Direct Connect の場所を選択します。
帯域幅	接続帯域幅を選択します。 単位：Mbps。
Direct Connect Gateway	**1.** [Refresh] ボタンをクリックして、選択した AWS アカウントに関連付けられている Direct Connect ゲートウェイを取得します。 **2.** Direct Connect 接続を作成する必要がある先の Direct Connect ゲートウェイを選択します。 または、[Add New Direct Connect Gateway] をクリックして、新しい Direct Connect ゲートウェイを作成します。 **1.** [Gateway Name] を入力します。 **2.** ゲートウェイの [BGP ASN] を入力します。 **3.** [Save] をクリックします。
設定	次のいずれかを選択します。 • [Global]： • BGP ピアリング IP アドレスは、内部で予約済みの /16 サブネットから選択されます（198.18.0.0/16）。 • BGP ASN は、グローバル設定から選択されます。 • [Custom]： **1.** BGP ピアリングのカスタム /30 CIDR IP アドレスを入力します。 **2.** ピアリング用のカスタム BGP ASN を入力します。 （注） インターコネクトゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN を指定できます。インターコネクトゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。

Segment	この接続のセグメント ID を選択します。
添付ファイル	[Transit Gateway] を選択します。 [Transit Gateway]： **1.** [Refresh] ボタンをクリックして、選択した AWS アカウントに関連付けられているトランジットゲートウェイを取得します。 **2.** Direct Connect 接続を作成する必要があるトランジットゲートウェイを選択します。 または、[Add New Transit Gateway] をクリックして、新しいトランジットゲートウェイを作成します。 **1.** [Gateway Name] を入力します。 **2.** ゲートウェイの [BGP ASN] を入力します。 **3.** [AWS Region] を選択します。 **4.** [Save] をクリックします。 [VPC Tags]：VPC タグを選択して、この接続を介してトラフィックをルーティングする必要がある VPC を識別します。 [Allowed Prefixes]： **1.** [Add Prefixes] をクリックします。 **2.** 選択した VPC の IPv4 CIDR プレフィックスを入力します。 AWS VPC ダッシュボードから IPv4 CIDR アドレスを見つけることができます。

10. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。
- 接続設定を変更するには、[Back] をクリックします。

設定タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

Google Cloud へのインターコネクトの作成

Cisco SD-WAN Manager と Google Cloud アカウントの関連付け

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Cloud] をクリックします。
3. [Associate Cloud Account] をクリックします。
4. 次を設定します。

Cloud Provider	[Google Cloud] を選択します。
Cloud Account Name	任意の名前を入力します。
[説明（Description）]（任意）	説明を入力します。
Use for Cloud Gateway	[No] を選択します。
Private Key ID	[Upload Credential File] をクリックします。 このファイルは、Google Cloud コンソールにログインして生成する必要があります。秘密キー ID は、JSON または REST API 形式の場合があります。形式は、キーの生成方法によって異なります。詳細については、Google Cloud のドキュメントを参照してください。

5. [Add] をクリックします。

Cisco SD-WAN Manager は、Google Cloud への接続を作成するためのワークフローの一環として、この秘密キー ID を使用して Google Cloud でユーザーアカウントを認証します。

インターコネクト ゲートウェイから Google Cloud Router へのインターコネクトの作成

前提条件

1. Google Cloud コンソールを使用して、必要な VPC ネットワークを作成します。
2. 接続するネットワークリージョンに Google Cloud Router を展開します。

   非冗長接続の場合は、Google Cloud コンソールで、接続する各ネットワークリージョンに Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成します。

冗長接続の場合は、Google Cloud コンソールで、接続する各ネットワークリージョンに 2 つの Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成します。

Cisco vManage リリース 20.9.1 以降では、接続の作成時に Cisco SD-WAN Manager から Google Cloud Router と VLAN アタッチメントを作成できます。

（注） インターコネクトアタッチメントで使用するには、Google Cloud Router の Google ASN を 16550 に設定する必要があります。

3. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
4. インターコネクト ゲートウェイのグローバル設定を構成します。
5. Equinix テンプレートを Cisco Catalyst 1000v インスタンスにアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスをアタッチします。
6. Cisco Catalyst SD-WAN のブランチの場所に最も近い Equinix の場所でインターコネクト ゲートウェイを作成します。

   Google Cloud への冗長接続のために、Equinix ファブリックでインターコネクト ゲートウェイのペアを作成します。非冗長接続の場合は、Equinix の場所にインターコネクト ゲートウェイを展開します。
7. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
8. Google Cloud アカウントを Cisco SD-WAN Manager に関連付けます。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[Equinix] を選択します。
5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Equinix アカウントを選択します。
6. [Choose Interconnect Gateway]：接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービスプロバイダー	[Google Cloud] を選択します。
Google Account	Google アカウントの詳細を Cisco SD-WAN Manager に関連付ける際に入力したアカウント名で Google アカウントを選択します。
添付ファイル	サポート対象の最小リリース：Cisco vManage リリース 20.9.1 [Shared VPC] を選択して、Google Cloud Router と Google Cloud インターコネクトを接続にアタッチします。
リージョン	サポート対象の最小リリース：Cisco vManage リリース 20.9.1 Google Cloud リージョンを選択します。
VPC Network	サポート対象の最小リリース：Cisco vManage リリース 20.9.1 この接続を展開する VPC ネットワークを選択します。

冗長性	Cisco vManage リリース 20.8.1 以前の場合： 冗長性のある接続を作成する場合は、[Enable] を選択します。 [Primary Google Cloud Interconnect Attachment]： • [Primary Google Cloud Interconnect Attachment] ドロップダウンリストの横にある更新マークをクリックします。 • 目的のインターコネクト アタッチメントを選択します。インターコネクト アタッチメント名の形式は、<region-name>::<cloud-router-name>::<interconnect-attachment-name> です。 [Secondary Google Cloud Interconnect Attachment]： • 目的のインターコネクト アタッチメントを選択します。インターコネクト アタッチメント名の形式は、<region-name>::<cloud-router-name>::<interconnect-attachment-name> です。 セカンダリ インターコネクト アタッチメント オプションは、プライマリ インターコネクト アタッチメントが属するリージョンとネットワークに基づいて決定されます。プライマリ インターコネクト アタッチメントと同じリージョンおよびネットワークに未使用のインターコネクト アタッチメントがない場合、このドロップダウンリストは空になり、Google Cloud ポータルで冗長インターコネクト アタッチメントを作成する必要があることが示されます。 冗長性のない接続を作成する場合は、[Disable] を選択します。 [Google Cloud Interconnect Attachment]： • [Google Cloud Interconnect Attachment] ドロップダウンリストの横にある更新マークをクリックします。 • 目的のインターコネクト アタッチメントを選択します。インターコネクト アタッチメント名の形式は、<region-name>::<cloud-router-name>::<interconnect-attachment-name> です。

Cisco vManage リリース 20.9.1 以降の場合：

[Google Cloud Router]：

- [Google Cloud Router] ドロップダウンリストの横にある更新マークをクリックします。
- Google Cloud Router を選択するか、[Add New Google Cloud Router] をクリックします。

[Add New Google Cloud Router] をクリックした場合は、[Add Google Cloud Router] スライドインペインでルータ設定を構成します。

以下を設定し、[Save] をクリックします。

- [Region]：Google Cloud Router のリージョンを選択します。
- [VPC Network]：Google Cloud Router ネットワークを選択します。
- [Cloud Router Name]：固有の Google Cloud Router 名を入力します。

（注） Google Cloud Router は常に、BGP ASN が 16,550、MTU が 1,500、デフォルトルーティング有効で作成されます。

[Google Cloud Interconnect Attachment]：

- [Google Cloud Interconnect Attachment] ドロップダウンリストの横にある更新マークをクリックします。
- 必要なインターコネクトアタッチメントを選択するか、[Add New Google Cloud Interconnect Attachment] をクリックします。

[Add New Google Cloud Interconnect Attachment] をクリックした場合は、[Add Google Cloud Interconnect Attachment] スライドインペインでルータ設定を構成します。

以下を設定し、[Save] をクリックします。

- [Region]：Google Cloud インターコネクト アタッチメントのリージョンを選択します。
- [VPC Network]：インターコネクトアタッチメント用の Google Cloud ネットワークを選択します。
- [Cloud Router Name]：インターコネクト アタッチメント用に、選択したリージョンと VPC ネットワークに展開された Google Cloud Router を選択します。
- [IC Attachment Name]：インターコネクト アタッチメントの一意の名前を入力します。

	• [Secondary Zone]：このアタッチメントをセカンダリゾーンに展開する場合は、このチェックボックスをオンにします。

9. プライマリ VLAN アタッチメントに次の設定を構成し、[Next] をクリックします。

Peering Location	**1.** [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 **2.** Google Cloud Router とプライマリ VLAN アタッチメントを作成した GCP リージョンに最も近い Equinix の場所を選択します。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	接続帯域幅（Mbps）を選択します。許可された帯域幅の値のリストは、選択したピアリングの場所に基づいて作成されます。

10. ステップ 8 で冗長性を有効にした場合は、セカンダリ VLAN アタッチメントに次の設定を構成し、[Next] をクリックします。

Peering Location	**1.** [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 **2.** Google Cloud Router とセカンダリ VLAN アタッチメントを作成した GCP リージョンに最も近い Equinix の場所を選択します。 **ヒント** 冗長性を確保するために、プライマリ VLAN アタッチメントに関連付けられているピアリングの場所以外の場所を選択します。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	セカンダリ接続の帯域幅は、プライマリ接続の帯域幅と同じ値に設定されます。
Source Gateway	セカンダリ VLAN アタッチメントへの接続を確立する必要があるインターコネクト ゲートウェイを選択します。

11. 以下を設定し、[Next] をクリックします。

設定	[Auto-generated] または [Custom] を選択します。 • [Auto-generated]：インターコネクト BGP ASN はシステムによって選択されます • [Custom]：インターコネクト VLAN アタッチメントとのピアリング用に、任意のインターコネクト BGP ASN を指定します。 （注） インターコネクト ゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN を指定できます。インターコネクト ゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。 Google Cloud Router へのインターコネクトの BGP ピアリング IP アドレスは、サブネット（169.254.0.0/16）から Google によって自動割り当てされます。Cisco SD-WAN Manager から IP アドレスを設定することはできません。
Segment	この接続のセグメント ID を選択します。

12. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。
- 接続設定を変更するには、[Back] をクリックします。

接続設定を保存すると、設定タスクが起動し、インターコネクト ゲートウェイと Google Cloud Router のインターコネクト アタッチメントの間にインターコネクトが作成されます。

タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。Google Cloud コンソールで接続の詳細を表示することもできます。

次の作業：Google Cloud コンソールで、BGP を介して Google Cloud Router からインターコネクト ゲートウェイにアドバタイズされるルートを管理します。

Google Cloud 内のクラウドゲートウェイへのインターコネクト接続の作成

前提条件

1. Google Cloud コンソールを使用して、必要な VPC ネットワークを作成します。
2. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
3. インターコネクト ゲートウェイのグローバル設定を構成します。
4. Equinix テンプレートを Cisco Catalyst 1000v インスタンスにアタッチします。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを選択します。

5. Cisco Catalyst SD-WAN のブランチの場所に最も近い Equinix の場所でインターコネクト ゲートウェイを作成します。

   Google Cloud への冗長接続のために、Equinix ファブリックでインターコネクト ゲートウェイのペアを作成します。非冗長接続の場合は、Equinix の場所にインターコネクト ゲートウェイを展開します。

6. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。

7. Google Cloud アカウントを Cisco SD-WAN Manager に関連付けます。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[Equinix] を選択します。
5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Equinix アカウントを選択します。
6. [Choose Interconnect Gateway]：接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービス プロバイダー	[Google Cloud] を選択します。
Google Account	Google アカウントの詳細を Cisco SD-WAN Manager に関連付ける際に入力したアカウント名で Google アカウントを選択します。
添付ファイル	クラウドゲートウェイに接続するには、[Cloud Gateway] を選択します。 [Cloud Gateways]：ドロップダウンリストからクラウドゲートウェイを 1 つだけ選択できます。

9. 以下を設定し、[Next] をクリックします。

プライマリ

Google Cloud Router	Google Cloud Router を選択します。
Google Cloud Interconnect Attachment	必要なインターコネクトアタッチメントを選択するか、[Add New Google Cloud Interconnect Attachment] をクリックします。 [Add New Google Cloud Interconnect Attachment] をクリックした場合は、[Add Google Cloud Interconnect Attachment] スライドインペインでルータ設定を構成します。 以下を設定し、[Save] をクリックします。 • [Region]：Google Cloud インターコネクト アタッチメントのリージョンを選択します。 • [VPC Network]：アタッチメントに対して関連付けられたネットワークを選択します。 • [Cloud Router Name]：選択したリージョンと VPC ネットワークに展開された Google Cloud Router を選択します。 • [ID Attachment Name]：一意のアタッチメント名を入力します。 • [Secondary Zone]：このアタッチメントをセカンダリゾーンに展開する場合は、このチェックボックスをオンにします。
セカンダリ	
Google Cloud Router	Google Cloud Router を選択します。
Google Cloud Interconnect Attachment	必要なインターコネクトアタッチメントを選択するか、[Add New Google Cloud Interconnect Attachment] をクリックします。 [Add New Google Cloud Interconnect Attachment] をクリックした場合は、[Add Google Cloud Interconnect Attachment] スライドインペインでルータ設定を構成します。 以下を設定し、[Save] をクリックします。 • [Region]：Google Cloud インターコネクト アタッチメントのリージョンを選択します。 • [VPC Network]：アタッチメントに対して関連付けられたネットワークを選択します。 • [Cloud Router Name]：選択したリージョンと VPC ネットワークに展開された Google Cloud Router を選択します。 • [ID Attachment Name]：一意のアタッチメント名を入力します。 • [Secondary Zone]：このアタッチメントをセカンダリゾーンに展開する場合は、このチェックボックスをオンにします。

10. プライマリ VLAN アタッチメントに次の設定を構成し、[Next] をクリックします。

Peering Location	1. [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 2. Google Cloud Router とプライマリ VLAN アタッチメントを作成した GCP リージョンに最も近い Equinix の場所を選択します。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	接続帯域幅（Mbps）を選択します。許可された帯域幅の値のリストは、選択したピアリングの場所に基づいて作成されます。

11. ステップ 8 で冗長性を有効にした場合は、セカンダリ VLAN アタッチメントに次の設定を構成し、[Next] をクリックします。

Peering Location	1. [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 2. Google Cloud Router とセカンダリ VLAN アタッチメントを作成した GCP リージョンに最も近い Equinix の場所を選択します。 ヒント　冗長性を確保するために、プライマリ VLAN アタッチメントに関連付けられているピアリングの場所以外の場所を選択します。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	セカンダリ接続の帯域幅は、プライマリ接続の帯域幅と同じ値に設定されます。
Source Gateway	セカンダリ VLAN アタッチメントへの接続を確立する必要があるインターコネクト ゲートウェイを選択します。

12. 以下を設定し、[Next] をクリックします。

設定	[Auto-generated] または [Custom] を選択します。 • [Auto-generated]：インターコネクト BGP ASN はシステムによって選択されます • [Custom]：インターコネクト VLAN アタッチメントとのピアリング用に、任意のインターコネクト BGP ASN を指定します。 （注） インターコネクト ゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN を指定できます。インターコネクト ゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。 Google Cloud Router へのインターコネクトの BGP ピアリング IP アドレスは、サブネット（169.254.0.0/16）から Google によって自動割り当てされます。Cisco SD-WAN Manager から IP アドレスを設定することはできません。
Segment	この接続のセグメント ID を選択します。

13. 接続の概要を確認します。
    - 接続を作成するには、[Save] をクリックします。
    - 接続設定を変更するには、[Back] をクリックします。

    接続設定を保存すると、設定タスクが起動し、インターコネクト ゲートウェイと Google Cloud Router のインターコネクト アタッチメントの間にインターコネクトが作成されます。

    タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。Google Cloud コンソールで接続の詳細を表示することもできます。

次の作業：Google Cloud コンソールで、BGP を介して Google Cloud Router からインターコネクト ゲートウェイにアドバタイズされるルートを管理します。

Microsoft Azure へのインターコネクトの作成

Cisco SD-WAN Manager と Microsoft Azure アカウントの関連付け

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Cloud] をクリックします。
3. [Associate Cloud Account] をクリックします。

4. 次を設定します。

Cloud Provider	[Microsoft Azure] を選択します。
Cloud Account Name	任意の名前を入力します。
[説明（Description）]（任意）	説明を入力します。
Use for Cloud Gateway	[No] を選択します。
テナント ID	Azure Active Directory（AD）の ID を入力します。 **ヒント** テナント ID を見つけるには、Azure Active Directory に移動し、[Properties] をクリックします。
サブスクリプション ID	使用する Azure サブスクリプションの ID を入力します。
Client ID	既存の Azure アプリケーション ID を入力します。Azure AD にアプリケーションを登録する方法、クライアント ID と秘密キーを取得する方法などの詳細については、Azure のドキュメントを参照してください。
Secret Key	クライアント ID に関連付けられたパスワードを入力します。

5. [Add] をクリックします。

ホスト プライベート ネットワークの検出と Microsoft Azure VNet のタグ付け

インターコネクト ゲートウェイからのソフトウェア定義型のクラウドインターコネクトを作成する Microsoft Azure VNet にタグを付けます。同じ VNet タグを使用してグループ化された Azure VNet は、単一のユニットと見なされます。

前提条件

Microsoft Azure アカウントを Cisco SD-WAN Manager に関連付けます。

タグの追加

VNet をグループ化し、まとめてタグ付けします。

（注） 異なるリソースグループに属する VNet を一緒に使用することはできません。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。

2. [Interconnect] をクリックします。
3. [Host Private Networks] をクリックします。
4. [Cloud Provider]：[Microsoft Azure] を選択します。

   使用可能なホスト VNet が検出され、表に一覧表示されます。
5. 対応するチェックボックスをオンにして、タグ付けする Azure VNet を選択します。
6. [Tag Actions] をクリックします。
7. [Add Tag] をクリックして、以下を設定します。

フィールド	説明
[Tag Name]	タグの名前を入力します。
[地域（Region）]	[Add Tag] をクリックする前に VNet を選択した場合、このフィールドには、選択した VNet に対応するリージョンのリストが表示されます。 • [Add Tag] をクリックする前に VNet を選択しなかった場合、またはリージョンをさらに選択する場合は、ドロップダウンリストからリージョンを選択します。 • リージョンおよび関連する VNet をタグから除外するには、[X] をクリックします。
Selected VNets	[Add Tag] をクリックする前に VNet を選択した場合、このフィールドには、選択したホスト VNet の VNet ID のリストが表示されます。 • [Add Tag] をクリックする前に VNet を選択しなかった場合、または VNet をさらに選択する場合は、ドロップダウンリストから VNet を選択します。 • タグから VNet を除外するには、[X] をクリックします。

フィールド	説明
（Cisco vManage リリース 20.9.1 以降）[Enable for SDCI partner Interconnect Connections] （Cisco vManage リリース 20.8.1 以前）[Enable for Interconnect Connectivity]	Microsoft Azure へのインターコネクト接続を作成するときに VNet タグを使用するには、このチェックボックスをオンにします。 インターコネクト接続に対して有効になっている場合、タグは Microsoft Azure マルチクラウドワークフローで使用することはできません。 インターコネクト接続に対して有効になっていない場合、タグは Microsoft Azure マルチクラウドワークフローでのみ使用できます。 （注） クラウドゲートウェイを使用して VNet ワークロードに接続する場合、この設定を有効にしないでください。

8. [Add] をクリックします。

[Host Private Networks] ページで、先ほど選択した Azure vNet にタグが付けられ、タグ名が [VNET Tag] 列に表示されます。クラウドインターコネクトに vNet タグを使用することを選択した場合、[Interconnect Enabled] 列に [Yes] と表示されます。

タグの編集

既存のタグに VNet を追加するか、既存のタグから VNet を削除します。

Cisco vManage リリース 20.10.1 以降では、次の条件に従ってインターコネクト接続に関連付けられた VNet タグを編集します。

- 1 つの VNet のみが VNet タグに関連付けられている場合、タグから VNet を削除することはできません。タグから VNet を削除するには、インターコネクト接続を削除してからタグを編集します。
- 仮想 WAN アタッチメントを使用したプライベートピアリング接続の場合、タグに関連付ける VNet は、タグにすでに関連付けられている VNet と同じリージョンのものである必要があります。

  新しいリージョンの VNet をプライベートピアリング接続にアタッチするには、次の手順を実行します。

  1. リージョンの新しいタグを作成し、必要な VNet を関連付けます。
  2. プライベートピアリング接続を編集し、VNet タグを接続にアタッチします。

- VNet アタッチメントを使用したプライベートピアリング接続の場合、タグの編集中に、新しいリージョンの VNet をタグに関連付けることができます。

（注） Cisco vManage リリース 20.9.1 以前のリリースでは、インターコネクト接続に関連付けられている VNet タグを編集することはできません。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Host Private Networks] をクリックします。
4. [Cloud Provider]：[Microsoft Azure] を選択します。

   使用可能なホスト VNet が検出され、表に一覧表示されます。
5. [Tag Actions] をクリックします。
6. [Edit Tag] をクリックし、必要に応じて以下を変更します。

フィールド	説明
[Tag Name]	ドロップダウンリストからタグ名を選択します。
[地域（Region）]	このフィールドには、タグに関連付けられた VNet に対応するリージョンのリストが表示されます。 • ドロップダウンリストから追加のリージョンを選択します。 • リージョンおよび関連する VNet をタグから除外するには、[X] をクリックします。
Selected VNets	このフィールドには、タグに関連付けられている VNet のリストが表示されます。 • ドロップダウンリストから追加の VNet を選択します。 • タグから VNet を除外するには、[X] をクリックします。
（Cisco vManage リリース 20.9.1 以降）[Enable for SDCI partner Interconnect Connections] （Cisco vManage リリース 20.8.1 以前）[Enable for Interconnect Connectivity]	（読み取り専用）VNet をインターコネクト接続の設定中に使用するように設定されているか、またはマルチクラウドゲートウェイのインテントマッピングに使用するように設定されているかを示します。

7. [Update] をクリックします。

タグの削除

VNet をグループ化しているタグを削除します。

（注） VNet タグがインターコネクト接続に関連付けられている間は、タグを削除できません。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Host Private Networks] をクリックします。
4. [Cloud Provider]：[Microsoft Azure] を選択します。

   使用可能なホスト VNet が検出され、表に一覧表示されます。
5. [Tag Actions] をクリックします。
6. [タグを削除（Delete Tag）]をクリックします。
7. [Tag Name]：ドロップダウンリストからタグ名を選択します。
8. [Delete] をクリックします。

インターコネクト ゲートウェイから Microsoft Azure ExpressRoute への Microsoft ピアリング接続の作成

前提条件

1. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. Microsoft Azure アカウントを Cisco SD-WAN Manager に関連付けます。
5. Equinix テンプレートを Cisco Catalyst 1000v インスタンスにアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスをアタッチします。
6. Equinix の場所でインターコネクト ゲートウェイを作成します。

   Microsoft Azure に接続するために、Equinix ファブリックにインターコネクト ゲートウェイのペアを作成します。デフォルトは冗長接続であり、この設定のみがサポートされています。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** に移動します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[Equinix] を選択します。
5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Equinix アカウントを選択します。
6. [Choose Interconnect Gateway]：接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウド サービス プロバイダー	[Microsoft Azure] を選択します。
Azure Account	Microsoft Azure アカウントの詳細を Cisco SD-WAN Manager に関連付ける際に入力したアカウント名で Microsoft Azure アカウントを選択します。

ExpressRoute	

1. [Refresh] ボタンをクリックして、使用可能な ExpressRoute のリストを更新します
2. ExpressRoute を選択するか、[Add New ExpressRoute] をクリックします。

（注）
- Cisco vManage リリース 20.8.1 以降では、Equinix ExpressRoute を使用できます。
- Cisco vManage リリース 20.8.1 以降では、使用可能な ExpressRoute のリストのドロップダウンに表示される、それぞれのインターコネクト プロバイダー用に作成されたすべての ExpressRoute は、プロビジョニングのステータスに応じて色分けされます。色とその意味のリストを示します。
  - 黒：プロビジョニングされていません。
  - グレー：プロビジョニング済み。
  - 赤：失敗。
- 選択した Azure アカウントのプロビジョニングされていない ExpressRoute のみを選択できます。ExpressRoute の状態は、Microsoft Azure ポータルで確認できます。

[Add New ExpressRoute] をクリックした場合は、[Create New ExpressRoute] スライドインペインで ExpressRoute 設定を構成します。

次の項目を設定して、[保存（Save）] をクリックします。

- [Resource Group]：Microsoft Azure アカウントに関連付けられているリソースグループを選択します。
- [Region]：Azure リージョンを選択します。
- [Instance Name]：ExpressRoute インスタンスの名前を入力します。
- [Provider]：[Equinix] を選択します。
- [Peering Location]：[Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。ExpressRoute の場所を選択します。
- [Bandwidth]：ExpressRoute 回線の帯域幅を選択します。
- [SKU]：[Premium] または [Standard] SKU を選択します。
- [Billing Model]：[Metered] 課金または [Unlimited] を選択

	します。

9. ExpressRoute へのプライマリ接続について次の設定を構成し、[Next] をクリックします。

Peer Location	場所は、前に選択した ExpressRoute に基づいて自動的に選択されます。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	接続帯域幅（Mbps）を選択します。許可された帯域幅の値のリストは、選択した ExpressRoute の場所に基づいて作成されます。

10. ExpressRoute へのセカンダリ接続について次の設定を構成し、[Next] をクリックします。

Peer Location	場所は、前に選択した ExpressRoute に基づいて自動的に選択されます。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	セカンダリ接続の帯域幅は、プライマリ接続の帯域幅と同じ値に設定されます。
Source Gateway	セカンダリ接続を確立する必要があるインターコネクト ゲートウェイを選択します。

11. 以下を設定し、[Next] をクリックします。

展開タイプ	[Public] を選択します。
Primary IPv4 Subnet	プライマリ インターコネクト ゲートウェイからの BGP ピアリングの /30 CIDR パブリック IP アドレスを入力します。 接続を作成する前に、パブリック IPv4 アドレスの使用が組織で許可されていることを確認してください。
Secondary IPv4 Subnet	セカンダリ インターコネクト ゲートウェイからの BGP ピアリングの /30 CIDR パブリック IP アドレスを入力します。 接続を作成する前に、パブリック IPv4 アドレスの使用が組織で許可されていることを確認してください。
BGP Advertise Prefix	インターコネクト ゲートウェイにアドバタイズするサマリーアドレスとプレフィックスを入力します。
Segment	この接続のセグメント ID を選択します。

12. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。
- 接続設定を変更するには、[Back] をクリックします。

接続設定を保存すると、設定タスクが起動します。このタスクでは、次のリソースが作成されます。

- インターコネクト ゲートウェイと ExpressRoute 間の Equinix ファブリック内の仮想クロスコネクト
- ExpressRoute 回線の Microsoft Azure パブリック/プライベートピアリング
- vNet ゲートウェイ（vNet 用の vNet ゲートウェイが存在しない場合）
- ExpressRoute と vNet ゲートウェイ間の接続

タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

Microsoft Azure ポータルで接続の詳細を表示することもできます。

インターコネクト ゲートウェイから Microsoft Azure ExpressRoute へのプライベートピアリング接続の作成

前提条件

1. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. Microsoft Azure アカウントを Cisco SD-WAN Manager に関連付けます。
5. ホスト プライベート ネットワークを検出して Microsoft Azure VNet をタグ付けします。
6. Equinix テンプレートを Cisco Catalyst 1000v インスタンスにアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスをアタッチします。
7. Equinix の場所でインターコネクト ゲートウェイを作成します。

   Microsoft Azure に接続するために、Equinix ファブリックにインターコネクト ゲートウェイのペアを作成します。デフォルトは冗長接続であり、この設定のみがサポートされています。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** に移動します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。

4. [Choose Interconnect Provider]：[Equinix] を選択します。
5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Equinix アカウントを選択します。
6. [Choose Interconnect Gateway]：Direct Connect 接続を作成する元となるインターコネクトゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービス プロバイダー	[Microsoft Azure] を選択します。
Azure Account	Microsoft Azure アカウントの詳細を Cisco SD-WAN Manager に関連付ける際に入力したアカウント名で Microsoft Azure アカウントを選択します。

ExpressRoute	

1. [Refresh] ボタンをクリックして、使用可能な ExpressRoute のリストを更新します
2. ExpressRoute を選択するか、[Add New ExpressRoute] をクリックします。

   （注）
   - Cisco vManage リリース 20.8.1 以降では、Equinix ExpressRoute を使用できます。
   - Cisco vManage リリース 20.8.1 以降では、使用可能な ExpressRoute のリストのドロップダウンに表示される、それぞれのインターコネクト プロバイダー用に作成されたすべての ExpressRoute は、プロビジョニングのステータスに応じて色分けされます。色とその意味のリストを示します。
     - 黒：プロビジョニングされていません。
     - グレー：プロビジョニング済み。
     - 赤：失敗。
   - 選択した Azure アカウントのプロビジョニングされていない ExpressRoute のみを選択できます。ExpressRoute の状態は、Microsoft Azure ポータルで確認できます。

   [Add New ExpressRoute] をクリックした場合は、[Create New ExpressRoute] スライドインペインで ExpressRoute 設定を構成します。

   次の項目を設定して、[保存（Save）] をクリックします。

   - [Resource Group]：Microsoft Azure アカウントに関連付けられているリソースグループを選択します。
   - [Region]：Azure リージョンを選択します。
   - [Instance Name]：ExpressRoute インスタンスの名前を入力します。
   - [Provider]：[Equinix] を選択します。
   - [Peering Location]：[Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。ExpressRoute の場所を選択します。
   - [Bandwidth]：ExpressRoute 回線の帯域幅を選択します。
   - [SKU]：[Premium] または [Standard] SKU を選択します。
   - [Billing Model]：[Metered] 課金または [Unlimited] を選択

	します。

9. ExpressRoute へのプライマリ接続について次の設定を構成し、[Next] をクリックします。

Peer Location	場所は、前に選択した ExpressRoute に基づいて自動的に選択されます。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	接続帯域幅（Mbps）を選択します。許可された帯域幅の値のリストは、選択した ExpressRoute の場所に基づいて作成されます。

10. ExpressRoute へのセカンダリ接続について次の設定を構成し、[Next] をクリックします。

Peer Location	場所は、前に選択した ExpressRoute に基づいて自動的に選択されます。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	セカンダリ接続の帯域幅は、プライマリ接続の帯域幅と同じ値に設定されます。
Source Gateway	セカンダリ接続を確立する必要があるインターコネクト ゲートウェイを選択します。

11. 以下を設定し、[Next] をクリックします。

展開タイプ	[Private] を選択します。

BGP-Peering Settings	[Auto-generated] または [Custom] を選択します。 [Auto-generated]：インターコネクト BGP ASN、およびプライマリおよびセカンダリ IPv4 サブネットがシステムによって選択されます。IPv4 サブネットは、内部で予約された /16 サブネット（198.18.0.0/16）から選択されます。 [Custom]： （注） インターコネクト ゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN とカスタム IPv4 サブネットを指定できます。インターコネクト ゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。 • [BGP ASN]：ExpressRoute とのプライマリおよびセカンダリピアリングに選択した ASN を指定します。 • [Primary IPv4 Subnet]：プライマリ インターコネクト ゲートウェイとの BGP ピアリングの /30 CIDR IP アドレスを入力します。 • [Secondary IPv4 Subnet]：セカンダリ インターコネクト ゲートウェイとの BGP ピアリングの /30 CIDR IP アドレスを入力します。
添付ファイル	次のいずれかを選択します。 • [vNet]：VNet タグを使用して VNet を接続にアタッチします。 • [vWAN]：仮想 WAN を接続にアタッチし、VNet タグを使用して仮想 WAN のリージョンから VNet を選択します。 • サポート対象の最小リリース：Cisco vManage リリース 20.9.1 [Cloud Gateway]：クラウドゲートウェイを接続にアタッチします。接続ごとに最大 5 つのクラウドゲートウェイを選択できます。
VNet Settings	[VNet Tags]：VNet タグを選択して、この接続を介してトラフィックをルーティングする必要がある VNet を識別します。

virtual WAN Settings	

[vWAN]：新しい仮想 WAN を選択または追加します。

（注） ExpressRoute 回線の選択されたリソースグループに対して、インターコネクト ゲートウェイから Microsoft Azure への最初の接続にのみアタッチする仮想 WAN を選択できます。同じ仮想 WAN が、仮想 WAN をアタッチするように選択した同じリソースグループ内の後続の接続にアタッチされます。

Cisco vManage リリース 20.8.1 以降では、Cisco SD-WAN Manager は、Microsoft Azure アカウントごとに、各 Microsoft Azure リソースグループに対して 1 つの仮想 WAN をサポートします。その vWAN が選択され、仮想 WAN 接続の一部として使用されると、同じ Microsoft Azure リソースグループへの後続の仮想 WAN 接続には同じ仮想 WAN が使用されます。

接続に ExpressRoute 回線が選択されると、接続用に Microsoft Azure リソースグループが決定されます。接続に属する他のすべての Microsoft Azure リソースは、選択した ExpressRoute 回線と同じ Microsoft Azure リソースグループに含まれている必要があります。

[vNet]：VNet タグを選択して、この接続を介してトラフィックをルーティングする必要がある VNet を識別します。

Cisco SD-WAN Manager は、選択された VNet タグに基づいて VNet を検索し、VNet が属するリージョンを識別します。選択された仮想 WAN と特定されたリージョンについて、Cisco SD-WAN Manager は、検証に使用できる仮想ハブを見つけて一覧表示します。仮想ハブが存在しないリージョンの場合、名前とアドレスプレフィックスを指定して仮想ハブを追加する必要があります。

[vHub Settings]：

（注） Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、リージョンに複数の Azure Virtual WAN ハブがある場合は、そのリージョンの特定の Azure Virtual WAN ハブを選択できます。Azure Virtual WAN ハブを選択すると、Azure Virtual WAN 用に作成される後続のすべての接続で同じ Azure Virtual WAN ハブが使用されます。

1. [Add Settings] をクリックします。設定を変更する場合は、[Edit Settings] をクリックします。
2. 該当するリージョンの仮想ハブ名とアドレスプレフィックスを確認します。リージョンに仮想ハブが存在しない場合は、リージョンに使用する仮想ハブの名前とアドレスプレフィッ

	クスを入力します。 （注） 入力する仮想ハブのアドレスプレフィックスが、どの VNet のアドレスプレフィックスとも重複していないことを確認してください。 3. 変更を適用するには、[Save] をクリックします。変更を破棄するには、[Cancel] をクリックします。
Segment	この接続のセグメント ID を選択します。

12. 接続の概要を確認します。
    - 接続を作成するには、[Save] をクリックします。
    - 接続設定を変更するには、[Back] をクリックします。

接続設定を保存すると、設定タスクが起動します。

VNet アタッチメントの場合は、設定タスクにより次のリソースが作成されます。

- インターコネクト ゲートウェイと ExpressRoute 間の Equinix ファブリック内の仮想クロスコネクト
- ExpressRoute 回線の Microsoft Azure パブリック/プライベートピアリング
- vNet ゲートウェイ（vNet 用の vNet ゲートウェイが存在しない場合）
- ExpressRoute と vNet ゲートウェイ間の接続

仮想 WAN アタッチメントの場合は、設定タスクにより次のリソースが作成されます。

- インターコネクト ゲートウェイと ExpressRoute 間の Equinix ファブリック内の仮想クロスコネクト
- ExpressRoute 回線の Microsoft Azure パブリック/プライベートピアリング
- 必要な仮想ハブ
- vNet と仮想ハブ間の接続
- 各仮想ハブの ExpressRoute ゲートウェイ（必要な場合）
- ExpressRoute ゲートウェイと ExpressRoute 回線間の接続

タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

Microsoft Azure ポータルで接続の詳細を表示することもできます。

デバイスリンク

デバイスリンクグループは、2 つ以上のエッジデバイス間にフルメッシュネットワークを作成します。デバイスリンクは、グループの一部であるすべてのエッジデバイスを接続して WAN を作成します。メッシュ内のすべてのデバイスリンクは、エッジデバイス間で同じ帯域幅を共有します。

（注）
- Equinix アカウントごとにサポートされるデバイスリンクは 1 つだけです。
- デバイスリンクグループに属するインターコネクト ゲートウェイ間でポイントツーポイント接続を形成することはできません。
- Cisco vManage リリース 20.9.2 および Cisco vManage リリース 20.10.1 にアップグレードする場合は、いくつかのデバイスを追加または削除して新しい設定をデバイスにプッシュすることで、デバイスリンクを変更する必要があります。これを行わないと、サイト間およびデバイスリンクが同じインターコネクト ゲートウェイ上に存在する場合、サイト間接続の BFD セッションがダウンします。

デバイスリンクの追加

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** に移動します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Device Links] をクリックします。
5. [Add Device Links] をクリックします。
6. ドロップダウンメニューから [Account name] を選択します。これは、アカウントの関連付けを通じて Cisco SD-WAN Manager に関連付けられている Equinix アカウントです。
7. [Device link name] を入力します。
8. ドロップダウンメニューから [Bandwidth] を選択します。

（注） Equinix でサポートされる最大帯域幅は、メトロあたり 10,000 Mbps です。

9. （オプション）

   [Subnet] を入力します。

（注）
- インターコネクト ゲートウェイのデバイス リンク インターフェイスに IP サブネットを指定します。
- サブネットは、10.0.0.0/8、172.16.0.0/12、および 192.168.0.0/16 の範囲にある必要があります。
- サブネットは、172.31.251.0/21 と競合しないようにする必要があります。
- サブネットは、他の接続と競合しないようにする必要があります。
- サブネットを入力しない場合、デフォルトで 198.19.0.0/16 が使用されます。

10. ドロップダウンメニューから [Gateway Name] を選択します。少なくとも 2 つのゲートウェイ名を選択してください。
11. [Save] をクリックします。

デバイスリンクの削除

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** に移動します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Device Links] をクリックします。

   既存のデバイスリンクの概要がテーブルに示されます。
5. このテーブルで、目的のリンクを見つけて [...] をクリックします。
6. デバイスリンクを削除するには、[Delete] をクリックし、デバイスリンクを削除することを確定します。

デバイスリンクの更新

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** に移動します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Device Links] をクリックします。

   既存のデバイスリンクの概要がテーブルに示されます。

5. このテーブルで、目的のリンクを見つけて [...] をクリックします。
6. デバイスリンクを編集するには、[Edit] をクリックします。
7. [Edit Device Link] ページで、[Bandwidth] および [Gateway Name] のみを更新して、ゲートウェイを追加または削除することができます。

（注） 編集できるパラメータは、[Bandwidth] と [Gateway Name] の 2 つだけです。

デバイスを追加または削除するときは、デバイスリンクに少なくとも2つのデバイスが存在している必要があります。

Equinix でサポートされる最大帯域幅は、メトロあたり 10,000 Mbps です。

8. [Save] をクリックします。

インターコネクトゲートウェイ間のインターコネクトの作成

Cisco SD-WAN Manager から、2 つ以上の Equinix の場所にあるインターコネクト ゲートウェイ間のインターコネクトを作成できます。これにより、Equinix ファブリックを介してこれらのインターコネクト ゲートウェイに接続されている SD-WAN ブランチの場所をリンクできます。

前提条件

Equinix ファブリックを介して接続する SD-WAN ブランチの場所ごとに、次の設定の前提条件を満たします。

1. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. 最も近い Equinix の場所を特定します。
5. ブランチの場所に最も近い Equinix の場所にインターコネクト ゲートウェイを作成します。

（注） 2 つのブランチの場所で定義された VRF があり、インターコネクト ゲートウェイ間の接続を介して VRF にアタッチされたトラフィックを交換する場合は、インターコネクト ゲートウェイで VRF と適切な集中管理型ポリシーを設定して、インターコネクト ゲートウェイ間の接続を介してブランチのトラフィックをルーティングする必要があります。

手順

1. Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[EQUINIX] を選択します。
5. [Choose Interconnect Account]：アカウント名で Equinix アカウントを選択します。このアカウント名は、Cisco SD-WAN Manager でアカウントを関連付ける際に入力した名前です。
6. [Choose Interconnect Gateway]：送信元インターコネクト ゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Edge] を選択します。
Connection Name	接続の一意の名前を入力します。
Interconnect Gateway	宛先インターコネクト ゲートウェイを選択します。
帯域幅	接続帯域幅を選択します。 単位：Mbps。

（注） デバイスリンクグループに属するインターコネクト ゲートウェイを使用してポイントツーポイント接続を形成することはできません。

9. 接続の概要を確認します。
   - 接続を作成するには、[Save] をクリックします。
   - 接続設定を変更するには、[Back] をクリックします。

設定タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の設定の確認と変更

インターコネクト ゲートウェイと接続の概要の表示

Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** > **[Interconnect]** を選択します。このページでは、作成したインターコネクト ゲートウェイと接続の概要を表示できます。インターコネクト ゲートウェイを作成していない場合、このページにはインターコネクト ゲートウェイと接続を作成および管理するためのワークフローの概要が表示されます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。

   次の情報が表示されます。

Interconnect Gateways	• インターコネクト ゲートウェイの総数 • 到達可能な（アップ状態の）インターコネクト ゲートウェイの数 • 到達不能な（ダウン状態の）インターコネクト ゲートウェイの数
接続	• 接続の合計数 • アップ状態の接続の数 • ダウン状態の接続の数
Summary Table	すべてのインターコネクト ゲートウェイとゲートウェイからの接続の要約リスト。
Device Link	• デバイスリンクの総数 • アップ状態のデバイスリンクの数 • ダウン状態のデバイスリンクの数

接続の表示、編集、または削除

（注）
- AWS への接続を削除すると、Cisco SD-WAN Manager は、接続の確立中に作成された VIF、仮想プライベートゲートウェイ、およびルートテーブルのみを削除します。
- AWS への接続の作成中に、Cisco SD-WAN Manager から Direct Connect ゲートウェイまたはトランジットゲートウェイを作成した場合、接続を削除してもゲートウェイは削除されません。必要に応じて、これらの AWS リソースを管理する必要があります。

  Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、接続の削除中に Direct Connect ゲートウェイまたはトランジットゲートウェイを削除するオプションがあります。
- AWS への接続を削除する場合、AWS および Equinix によってリソースが破棄される順序には一般的ではないタイミングの問題があるため、Cisco SD-WAN Manager は、サービスプロバイダーによって返される 400 エラーとともに、接続の削除に失敗したことを示すエラーを返す可能性があります。Cisco SD-WAN Manager は、そのデータベースから接続を完全にクリアし、関連するすべてのデバイスの設定をクリアします。Equinix ポータルにログインし、インターフェイスの設定と関連付けが Equinix データベースからも削除されていることを確認することをお勧めします。これにより、同じインターフェイスを後で別の接続に再利用できます。

  Equinix ポータルでインターフェイスのステータスを確認しないと、同じデバイスに新しい接続を作成する際にエラーが発生する可能性があります。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。

   既存の接続の概要がテーブルに示されます。
4. このテーブルで、目的の接続を見つけて [...] をクリックします。
   - 接続の詳細を表示するには、[View] をクリックします。
   - 接続を削除するには、[Delete] をクリックして、接続を削除することを確認します。

接続設定の編集

サポート対象の最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.12.1 および Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。

3. [Interconnect Connectivity] をクリックします。

   既存の接続の概要がテーブルに示されます。

4. 接続設定を変更するには、目的の接続の [...] をクリックし、[Edit] をクリックします。

   次の表は、接続先と接続タイプ（ある場合）に基づいて、編集可能なパラメータを説明しています。必要に応じてパラメータを設定します。

   Cisco Catalyst SD-WAN Manager では、これらの編集可能なパラメータに加えて、接続に関する読み取り専用のプロパティも表示されます。

（注） アクティブな接続のプロパティのみを変更できます。

表 *80 : AWS* へのインターコネクト接続の編集可能なプロパティ

フィールド	説明	適用される接続タイプ
Segment	この接続の別のセグメント ID を選択します。	AWS へのすべての接続
Transit Gateway	1. [Refresh] ボタンをクリックして、選択した AWS アカウントに関連付けられているトランジットゲートウェイを取得します。 2. Direct Connect 接続を作成する必要があるトランジットゲートウェイを選択します。 （注） • 削除するトランジットゲートウェイは、この接続に関連付けられている唯一のトランジットゲートウェイではない。 • 同じ編集操作で、トランジットゲートウェイが提供するリージョンに対応する VPC タグを削除できる。 （注） あるリージョンの既存のトランジットゲートウェイを、同じリージョンの別のトランジットゲートウェイに置き換えることはできません。	トランジットホスト型接続

フィールド	説明	適用される接続タイプ
VPC Tags	VPC タグを選択して、この接続を介してトラフィックをルーティングする必要がある VPC を識別します。	• VPC アタッチメントを使用したプライベートホスト型接続 • トランジットホスト型接続
許可プレフィックス（**Allowed Prefixes**）	[Edit Prefixes] をクリックします。 選択した VPC の IPv4 Classless Inter-Domain Routing（CIDR）プレフィックスを入力します。AWS VPC ダッシュボードから IPv4 CIDR アドレスを見つけることができます。 （注） さらにプレフィックスを追加できます。既存のプレフィックスを削除することはできません。	トランジットホスト型接続

表 *81 : Google Cloud* へのインターコネクト接続の編集可能なプロパティ

フィールド	説明
接続速度	[Connectivity Speed] ドロップダウンリストから必要な帯域幅を選択します。 冗長接続の場合は、プライマリ接続またはセカンダリ接続のいずれかの接続速度を変更します。ピア接続は、同じ接続速度を使用するように更新されます。 接続の帯域幅オプションは、関連付けられたピアリングの場所によって異なる場合があります。

（注） プライマリ接続またはセカンダリ接続のいずれかのプロパティを変更します。ピア接続は、同じ設定を使用するように更新されます。

表 *82 : Microsoft Azure* へのインターコネクト接続の編集可能なプロパティ

フィールド	説明	適用される接続タイプ
帯域幅	接続帯域幅を変更します。 単位：Mbps。 （注） Microsoft Azure への接続の帯域幅のみを増やすことができます。Microsoft Azure への接続の場合、Cisco SD-WAN Manager で接続帯域幅を増やす前に、Azure ポータルで ExpressRoute の帯域幅を増やす必要があります。	プライベートおよびパブリック（Microsoft）ピアリング接続
Segment	この接続の別のセグメント ID を選択します。	プライベートおよびパブリック（Microsoft）ピアリング接続
BGP Advertise Prefix	インターコネクト ゲートウェイにアドバタイズするサマリーアドレスとプレフィックスを入力します。 （注） Microsoft Azure のデフォルトでは、BGP アドバタイズプレフィックスが正しく表示されないリソースまたはネットワークオブジェクトを表示するために、ポータルで古いバージョンの API が使用されます。Microsoft Azure ポータルから BGP アドバタイズプレフィックスを確認するには、2020-05-01 以降の API バージョンを選択します。	パブリック（Microsoft）ピアリング接続
VNet Settings		
VNet	VNet タグを選択して、この接続を介してトラフィックをルーティングする必要がある VNet を識別します。	プライベートピアリング接続

フィールド	説明	適用される接続タイプ
vHub Settings	**1.** [Edit Settings] をクリックします。 **2.** 該当するリージョンの仮想ハブ名とアドレスプレフィックスを確認します。リージョンに仮想ハブが存在しない場合は、リージョンに使用する仮想ハブの名前とアドレスプレフィックスを入力します。 （注） 入力する仮想ハブのアドレスプレフィックスが、どの VNet のアドレスプレフィックスとも重複していないことを確認してください。 **3.** 変更を適用するには、[Save] をクリックします。変更を破棄するには、[Cancel] をクリックします。	プライベートピアリング接続

表 *83 :* エッジデバイス間のインターコネクト接続の編集可能なプロパティ

フィールド	説明
帯域幅	接続帯域幅を変更します。 単位：Mbps。

5. 変更を適用するには、[Update] または [Save] をクリックします。

インターコネクト ゲートウェイの表示、編集、または削除

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。

2. [Interconnect] をクリックします。

3. [Gateway Management] をクリックします。

既存のインターコネクト ゲートウェイの詳細がテーブルにまとめられています。

4. このテーブルで、目的のインターコネクト ゲートウェイを見つけて [...] をクリックします。

- インターコネクト ゲートウェイの詳細を表示するには、[View] をクリックします。
- インターコネクト ゲートウェイの説明を編集するには、[Edit Interconnect Gateway] をクリックします。

- インターコネクトゲートウェイを削除するには、[Delete]をクリックして、ゲートウェイを削除することを確定します。

  インターコネクト ゲートウェイを削除すると、Equinix ファブリックからブランチの場所の接続が切断されます。

インターコネクトアカウントの表示、編集、または削除

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Account Management] をクリックします。

   使用可能なインターコネクトアカウントがテーブルに表示されます。
4. 目的のインターコネクトアカウントに対して、[...]をクリックし、次の手順を実行します。
   - インターコネクトアカウントの詳細を表示するには、[View] をクリックします。
   - インターコネクトアカウントの詳細を変更するには、[Edit Account Information] をクリックします。

     [Account Name] と [Description] を変更できます。
   - インターコネクトアカウントのログイン情報を変更するには、[Edit Account Credentials] をクリックします。

     アカウントの [Customer Key] と [Customer Secret] を変更できます。

（注） Cisco SD-WAN Manager でログイン情報を変更しても、インターコネクトプロバイダーのログイン情報は変更されません。この設定オプションは、インターコネクトプロバイダーの関連ポータルで実行した、アカウントログイン情報の変更内容を複製する場合にのみ使用してください。

   - インターコネクトアカウントを削除するには、[Remove]をクリックして、アカウントの削除を確定します。

監査管理

サポート対象の最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.12.1

SDCIプロバイダーEquinixのファブリックに追加された監査管理のサポートは、クラウドの状態が Cisco SD-WAN Manager の状態と同期しているかどうかを確認するために役立ちます。監

査プロセスには、プロバイダーリソース、インターコネクトゲートウェイ、およびクラウドへの接続のスキャンが含まれています。エラーがある場合はエラーが表示され、エラーがない場合はステータスに [In Sync] と表示されます。

監査レポートへのアクセス

1. [Cloud onRamp for Multicloud] ページで、[Interconnect] タブに移動します。
2. [Intent Management] ペインで、[Audit] をクリックします。
3. [Intent Management- Audit] 画面の [Interconnect Gateways] で、ドロップダウンリストから [Interconnect Provider] を選択します。
4. [Interconnect Connections] を選択します。
5. 目的の監査レポートを表示するには、[Destination Type] を選択し、宛先タイプが [cloud] の場合はドロップダウンリストから [Cloud Provider] を選択します。
6. [Device Links] オプションを選択します。

パラメータ名	説明
Interconnect Provider	ドロップダウンからインターコネクト プロバイダー タイプを選択します。次のオプションがあります。 • Megaport • Equinix
Interconnect Connections	インターコネクト接続を有効または無効にします。
Destination Type	ドロップダウンリストから宛先タイプを選択します。次のオプションがあります。 • **クラウド** • **Edge**
クラウドプロバイダー	ドロップダウンリストからクラウドプロバイダーを選択します。次のオプションがあります。 • Amazon Web Services • **Microsoft Azure** • **Google Cloud**
Device Links	インターコネクト プロバイダーのデバイスリンクを選択します。

（注） 監査が完了すると、次のレポートが生成されます。

- [Edge Gateway]：設定されたエッジゲートウェイに関する情報を提供します。
- [Edge Connections]：設定されたエッジ接続に関する情報を提供します。
- [Unknown Edge Gateways]：不明なエッジゲートウェイに関する情報を提供します。
- [Unknown Edge Connections]：不明なエッジ接続に関する情報を提供します。

監査レポートに詳細とともに表示されるステータスは次のとおりです。

- In Sync
- Out of Sync
- AUDIT_INFO

監査の利点

監査は、Cisco SD-WAN Manager インテントとクラウドで実現された内容の間の乖離または不一致を特定するのに役立ちます。この乖離は、クラウドリソース、接続、および状態に関して発生します。このような乖離が検出されると、Cisco SD-WAN Manager によりその乖離にフラグが付けられ、修正アクションの実行に役立てることができます。

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix のトラブルシューティング

シナリオ	対処法
インターコネクトアカウントを追加できない	• Cisco SD-WAN Manager に関連付けられているアカウントのログイン情報が正しいことを確認します。 • インターコネクトプロバイダーでログイン情報を更新した場合は、Cisco SD-WAN Manager でアカウントのログイン情報を更新します。
インターコネクト ゲートウェイの作成を試みている際に、デバイスリストが空になる	Equinix テンプレートがデバイスにアタッチされていることを確認します。（推奨テンプレート：Default_EQUINIX_DHCP_DNS_ICGW_CSR1000V_Template_V02）
インターコネクト ゲートウェイの作成を試みている際に、目的の場所が見つからない	[Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。

シナリオ	対処法
インターコネクト ゲートウェイの作成に失敗した	**1.** Cisco SD-WAN Manager で設定タスクの進行状況を確認し、エラーメッセージがないか確認します。 **2.** インターコネクトグローバル設定を使用している場合は、選択したソフトウェアイメージがインターコネクト プロバイダーの場所で使用可能かどうかを確認します。 **3.** VM インスタンスが展開されていない場合、または IP プールが使い果たされている場合は、インターコネクト プロバイダーに確認してください。
インターコネクト ゲートウェイの証明書が正常にインストールされない	Cisco SD-WAN Manager のメニューから、**[Maintenance]** > **[Device Reboot]** をクリックします。[Device Reboot] ページで、インターコネクト ゲートウェイを再起動します。
Direct Connect 接続の作成中に、Direct Connect ゲートウェイまたはトランジット ゲートウェイ リストが空になる	**1.** AWS ポータルで、目的の Direct Connect ゲートウェイまたはトランジットゲートウェイが使用可能であることを確認します。 **2.** [Refresh] ボタンをクリックして、AWS からゲートウェイのリストを取得します。 **3.** ゲートウェイが AWS で使用できない場合は、Cisco SD-WAN Manager からゲートウェイを作成します。
Direct Connect 接続の作成中に、ホスト VPC タグがリストに表示されない	ホスト VPC タグが使用可能であり、インターコネクト接続に対して有効になっていることを確認します。

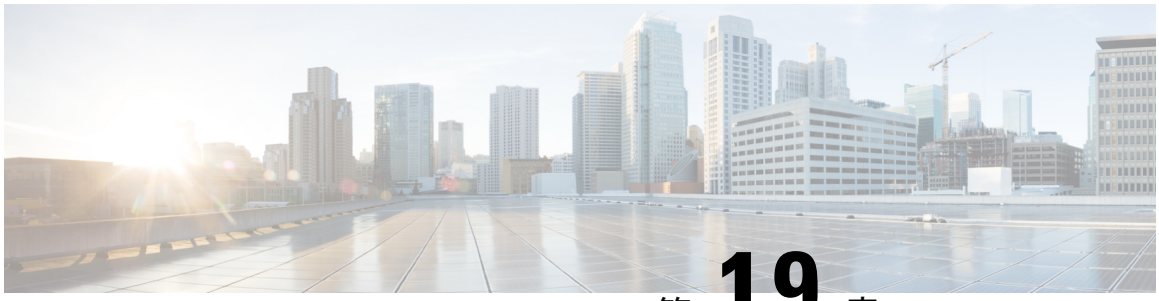
シナリオ	対処法
Direct Connect 接続の作成に失敗した	1. Cisco SD-WAN Manager で設定タスクの進行状況を確認し、エラーメッセージがないか確認します。 2. インターコネクトグローバル設定を使用している場合は、内部 IP アドレスプールが使い果たされているかどうかを確認します。該当する場合は、一部の接続を削除して再試行します。 3. カスタム設定を使用している場合は、ピアリングに重複する CIDR サブネットを入力していないことを確認します。 4. 接続制限に達しているかどうかを確認します。「Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の使用上の注意」を参照してください。 5. インターコネクト プロバイダー アカウントと AWS アカウントの権限を確認します。
トラフィックフローの問題	1. インバウンドおよびアウトバウンドトラフィックに必要なセキュリティルールがホスト VPC に設定されていることを確認します。 2. 仮想インターフェイスが作成され、Direct Connect ゲートウェイにアタッチされているかどうかを確認します。 3. AWS で、仮想インターフェイスの BGP ピアリングステータスが UP 状態かどうかを確認します。 4. 正しいルートテーブルがホスト VPC のメインルーティングテーブルとして使用されているかどうかと、必要なルートが仮想プライベートゲートウェイまたはトランジットゲートウェイに伝達されているかどうかを確認します。 5. 仮想プライベートゲートウェイまたはトランジットゲートウェイが、Direct Connect ゲートウェイにアタッチされているかどうかを確認します。
遅延の問題	1. インターコネクト ゲートウェイの場所が、接続の作成時に選択した Direct Connect の場所と近いかどうかを確認します。 2. 接続に適切な帯域幅が設定されていることを確認します。

シナリオ	対処法
クラウドゲートウェイがドロップダウンリストに表示されない	必要なクラウドゲートウェイがマルチクラウドワークフローを使用して作成され、このドキュメントに記載されている最小要件が満たされていることを確認します。
クラウドゲートウェイへのインターコネクト接続を作成した後も、VPC または VNET ワークロードへのトラフィックがインターネット経由で送信される	Cisco Catalyst SD-WAN のブランチがインターネットを介してクラウドゲートウェイに接続されていて、同じ VPC または VNET ワークロードにアクセスするためにインターコネクト ゲートウェイからのインターコネクト接続を介して接続されている場合、デフォルトでは、ブランチからのトラフィックはインターネットを介して送信されます。 インターコネクト ゲートウェイを介したプライベートパスを優先パスにするには、ブランチの WAN エッジデバイス、インターコネクト ゲートウェイ、およびクラウドゲートウェイに適切な制御ポリシーとデータポリシーを適用します。

第 IV 部

Cisco Catalyst SD-WAN Cloud OnRamp のトラブルシューティング

• Cisco SD-WAN Cloud OnRamp のトラブルシューティング （567 ページ）



第 19 章

Cisco SD-WAN Cloud OnRamp のトラブルシューティング

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。

- 概要 （567 ページ）
- サポート記事 （568 ページ）
- フィードバックのリクエスト （568 ページ）
- 免責事項と注意事項 （569 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
Configure Azure Express Route as Transport with SD-WAN in a Click	このドキュメントでは、ExpressRoute を、VHUB 内の SD-WAN トランスポートとして、マルチクラウド Azure ソリューションの Cloud OnRamp と統合する方法について説明します。
Configure Google Cloud Interconnect as a Transport with Cisco SD-WAN in a Click	このドキュメントでは、Google Cloud Interconnect をソフトウェア定義型ワイドエリアネットワーク（SD-WAN）トランスポートとして使用する方法について説明します。
Configure SD-WAN Cloud OnRamp for SaaS	このドキュメントでは、ブランチのローカル出口を使用した Cloud OnRamp for Software as a Service（SaaS）の設定について説明します。

フィードバックのリクエスト

ユーザー入力が役立ちます。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。

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。