概要

マルチクラウド向け Cisco Catalyst SD-Routing Cloud OnRamp 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 ルーティングデバイスに統合するのに役立ちます。AWS Transit Gateway（TGW）を使用して、SD ルーティングブランチサイトをサポートします。これらの機能により、ブランチデバイスは、クラウドネットワークとインターフェイスするアプリケーションにアクセスできます。この機能は、Cisco IOS XE 17.13.1a リリース以降でサポートされます。

（注） Cisco IOS XE 17.12.1a 以降、コンポーネントのブランド名が **Cisco vManage** から **Cisco Catalyst SD-WAN Manager** に、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** に変更されました。

- AWS 統合に関する情報 （1 ページ）
- Azure 仮想 WAN ハブと Cisco SD ルーティングの統合 （13 ページ）
- マルチクラウド 向け Cisco SD ルーティング Cloud OnRamp の機能情報 （22 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。

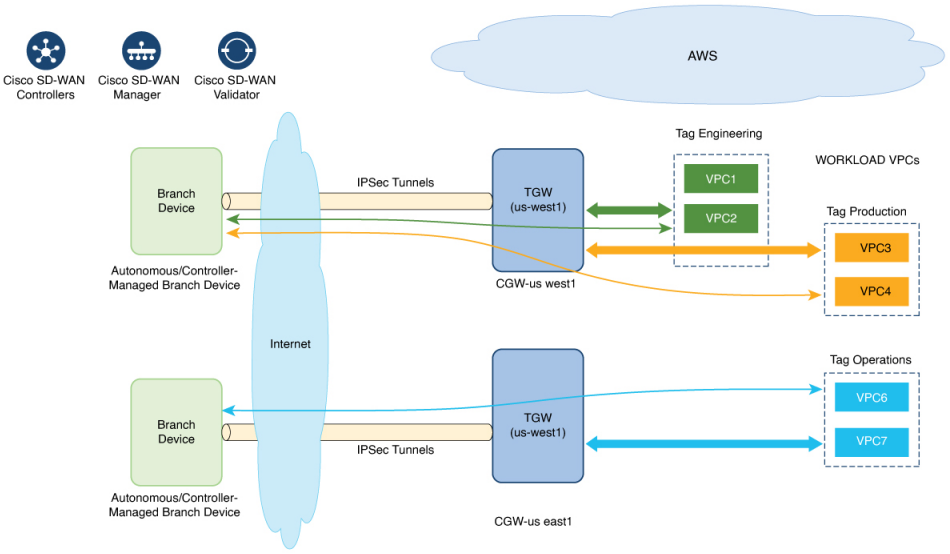
Cisco SD-WAN Manager コントローラを使用して、マルチクラウド環境の Cloud OnRamp を設定および管理できます。Cisco SD-WAN Manager の設定ウィザードは、パブリック クラウド アカウントへのトランジットゲートウェイの起動を自動化し、オーバーレイネットワーク内のブランチで、パブリック クラウド アプリケーションとそれらのアプリケーションのユーザーとの間の接続を自動化します。この機能は、Cisco Cloud ルータ上の AWS 仮想プライベートクラウド（VPC）で動作します。

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。

SD ルーティングデバイスを使用した AWS Branch Connect

SD ルーティングベースのブランチを介して SD-Routing Cloud OnRamp を展開する場合は、SD ルーティングベースの設定グループを介して展開する必要があります。また、Cloud OnRamp 接続中にトンネルベースの設定が機能するように、それぞれの CG デバイス CLI テンプレートを使用してブートアップ ライセンス レベルを手動で設定する必要があります。

エッジ/ブランチデバイスは、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（TGW）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 または VRF 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。



SD ルーティングブランチデバイスには、デフォルトの VRF のみを設定できます。このデフォルト VRF を使用して、SD-Routing Cloud OnRamp ブランチ接続を介してマッピングできます。マッピングに他の VPN/VRF を使用することはできません。SD ルーティングソリューションとともに、SD-WAN ソリューションに複数の VPN マッピングを設定できます。Cisco SD-WAN と Cisco SD-Routing の両方の接続を共存させることができます。

（注） ブランチサイトには、クラウドに接続する複数のブランチエンドポイントを設定できます。

SD ルーティングデバイス向け Cloud OnRamp の利点

SD-Routing Cloud OnRamp は、SD ルーティングデバイスを使用し、マルチクラウドワークフローを介して AWS または Azure に展開されたクラウドワークロードのセキュアなクラウド接続をサポートします。

Cloud onRamp の前提条件

Cloud onRamp の前提条件は次のとおりです。

- ブランチサイトは到達可能な状態であり、ステータスは同期中（In-Sync）である必要があります。
- ブランチサイトには、次のいずれかのブートレベルライセンスが必要です。
  - network-advantage
  - network-essentials
  - network-premier

  そうしないと、サイトを接続するときに、IPSec トンネル設定が適用されません。
- インターフェイスには、AWS TGW または Azure vHub、あるいはブランチデバイスの NAT から到達可能なパブリック IP アドレスが割り当てられている必要があります。そうしないと、ブランチサイトと AWS TGW または Azure vHub の間にトンネルが形成されません。
- SD ルーティングブランチは、設定グループを使用して展開するか、設定グループに移植する必要があります。
  - Cloud onRamp 機能を使用するための導入準備または互換性のある SD ルーティングデバイスを取得するには、既存のデバイスの導入準備 （4 ページ）および設定グループの自動化されたワークフローを使用した SD ルーティングデバイスの導入準備 （5 ページ）のセクションを参照してください。

制限事項

- Cloud OnRamp は、異なるリージョンの TGW 間のピアリングをサポートしていません。

SD ルーティングデバイスでの AWS 統合の設定

ここでは、SD ルーティングデバイスの機能を導入準備するためのワークフローについて説明します。

- 既存のデバイスの導入準備：
  - 既存の自律型デバイスを SD ルーティングデバイスに変換し、Cloud onRamp 機能を使用する
  - Cloud onRamp 機能を使用するための既存の非設定グループベースの SD ルーティングデバイスの変換
- 設定グループの自動化されたワークフローを使用した SD ルーティングデバイスの導入準備

既存のデバイスの導入準備

既存のデバイスを導入準備するには、次の手順を実行します。

ステップ 1 既存の自律デバイスを SD ルーティングデバイスに手動で展開または変換するには、「デバイスの手動でのオンボーディング」のセクションに記載されている手順に従います。

または

ステップ 2 クイック接続ワークフローを使用して SD ルーティングデバイスを展開するには、「ブートストラップを使用したSDルーティングデバイスのオンボーディング」のセクションに記載されている手順に従います。

前提条件：

ステップ 3 SD ルーティングデバイスを設定グループに移植するには、次の手順を実行します。

（注） 手順 1 と 2 のデバイスでは、次に進む前に次の前提条件を満たしている必要があります。

- ユーザー名とパスワード（admin/admin）を使用してデバイスにログインします。
- コマンドプロンプトで、**license boot level network-advantage addon dna-advantage** コマンドを設定します。
- 設定を保存し、デバイスをリブートします。Cisco SD-WAN Manager の [Configuration Devices] で、デバイスが同期していることを確認します。

a) Cisco IOS XE Catalyst SD-WAN Manager のメニューから、[Configuration] > [Configuration Groups] > [Add CLI based Configuration Group] の順に選択します
b) [Add CLI Group] ポップアップ ダイアログ ボックスで、設定グループ名を入力します。
c) [Solution Type] ドロップダウンリストをクリックし、SD ルーティングデバイスのソリューションタイプとして [sd-routing] を選択します。
d) [Description] フィールドに、説明を入力します。
e) [Create] をクリックします。

[Feature Profiles] タブと [Associated Device] タブを含む新しい設定グループページが表示されます。

f) ドロップダウンリストから [Load Running Config from Reachable Device] をクリックし、設定を作成するデバイスのシステム IP を選択します。[Preview] テキストボックスの要件に基づいて設定を編集できます。
g) [Configuration Preview] テキストボックスにロードされた設定をコピーし、テキストファイルとしてシステムに保存します。

ステップ 4 SD ルーティングデバイスに設定グループを追加するには、次の手順を実行します。

a) Cisco SD-WAN Manager のメニューから、[Configuration] > [Configuration Groups] > [Add Configuration Group] > [Create SD-Routing Config] を選択します。
b) [Name] フィールドに、設定グループの名前を入力します。
c) [Description] フィールドに、説明を入力します。
d) [Create SD-Routing Config] をクリックします。

e) [Configuration Group Created] ポップアップ ダイアログ ボックスで、[No, I will Do It Later] オプションをクリックします。
f) [What's Next?] セクションで、[Go to Configuration Group] をクリックします。
g) 設定グループ名の横にある [(…)] をクリックし、[Edit] を選択します。
h) [Feature Profiles] で CLI プロファイルをクリックし、[Unconfigured] を選択します。
i) [Create New] をクリックします。
j) 一意の名前を入力します。テキストファイルとして保存されている設定をコピーして貼り付けます。
k) [Save] をクリックします。

ステップ 5 [Associate Devices] をクリックし、SD ルーティングデバイスのサイト ID を選択して、関連付けを続行します。

ステップ 6 展開ステータスのリンクをクリックし、展開が成功したことを確認します。

ステップ 7 [Configuration] > [Devices] ページで、次の詳細を確認します。

- [Device Status]：デバイスのステータスは [In Sync] である必要があります
- [Managed By]：ステップ 4a で作成したそれぞれの SD ルーティング設定グループ。

ステップ 8 ステータスを確認するには、 **show sd-routing connections summary** コマンドを使用します。

設定グループの自動化されたワークフローを使用した SD ルーティングデバイスの導入準備

設定グループの自動化されたワークフローを使用して新しい SD ルーティングデバイスを導入準備するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Configuration Groups] > [Add Configuration Group] > [Create SD-Routing Config] を選択します。

ステップ 2 [Name] フィールドに、設定グループの名前を入力します。

ステップ 3 [Description] フィールドに、説明を入力します。

ステップ 4 [Create SD-Routing Config] をクリックします。

ステップ 5 [Configuration Group Created] ポップアップ ダイアログ ボックスで、[No, I will Do It Later] オプションをクリックします。

ステップ 6 [What's Next?] セクションで、[Go to Configuration Group] をクリックします。

ステップ 7 設定グループ名の横にある [(…)] をクリックし、[Edit] を選択します。

ステップ 8 [Feature Profiles] で CLI プロファイルをクリックし、[Unconfigured] を選択します。

ステップ 9 [Create New] をクリックします。

ステップ 10 基本設定グループを設定します。

この例は、設定グループの最小 CLI を示しています。

```
Configurations:
==============
sd-routing
organization-name CSRQA20231024
site-id 1
```

```
system-ip 4.7.8.9
vbond ip 44.226.182.48
vbond port 12346
wan-interface GigabitEthernet1
!
interface GigabitEthernet1
no shutdown
negotiation auto
ip address dhcp
exit
interface GigabitEthernet2
no shutdown
negotiation auto
ip address dhcp
exit

ip domain lookup

license boot level network-advantage addon dna-advantage
no logging console
```

ステップ 11 [Save] をクリックします。

ステップ 12 [Associate Devices] > [Associate Devices] の順にクリックします。

ステップ 13 [Unassigned] を選択し、UUID を 1 つ選択します。

ステップ 14 [Save] をクリックします。

ステップ 15 それぞれのシステム IP、サイト ID、およびホスト名を使用してデバイスをプロビジョニングできます。

ステップ 16 [Next] をクリックします。

ステップ 17 [Deploy] をクリックし、

ステップ 18 展開ステータスのリンクをクリックし、展開が成功したことを確認します。

ステップ 19 [Configuration] > [Devices] に移動し、uuid の 3 つのドットに対して「generate bootstrap」をクリックし、WAN インターフェイス名（例：GigabitEthernet1）を入力してブートストラップを生成します。

ステップ 20 UUID 名の横にある [(…)] をクリックし、[Generate bootstrap] をクリックします。

ステップ 21 [WAN Interface] フィールドに、インターフェイス名 GigabitEthernet1 を入力し、ブートストラップを生成します。

ステップ 22 ブートストラップを使用して、AWS コンソールのそれぞれの AMI に対して Cisco 8000v インスタンスを展開し、WAN インターフェイスにパブリック IP を割り当てます。

ステップ 23 展開ステータスのリンクをクリックし、展開が成功したことを確認します。

ステップ 24 [Configuration] > [Devices] ページで、次の詳細を確認します。

- [Device Status]：デバイスのステータスは [In Sync] である必要があります
- [Managed By]：ステップ 1 で作成したそれぞれの SD ルーティング設定グループ。

ステップ 25 ステータスを確認するには、 **show sd-routing connections summary** コマンドを使用します。

AWS クラウドアカウントの作成

AWS クラウドアカウントを作成するには、次の手順に従ってください。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 4 [Cloud Account Name] フィールドにアカウント名を入力します。

ステップ 5 （任意）[Description] フィールドに説明を入力します。

ステップ 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。

ステップ 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、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 が提供する外部 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、手順 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 で「Easily Replace or Attach an IAM Role to an Existing EC2 Instance by Using the EC2 Console」のブログ [英語] 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]"
       }
      }
    }
```

```
    ]
}
```

ステップ 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。

クラウドグローバル設定の構成

AWS のクラウドグローバル設定を構成するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、**[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。

ステップ 2 [Cloud Provider] フィールドで、[Amazon Web Services] を選択します。

ステップ 3 [Cloud Gateway Solution] ドロップダウンリストをクリックして、[Transit Gateway – Branch-connect] を選択します。

- [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 SD ルーティング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。

ステップ 4 [Cloud Gateway BGP ASN Offset] フィールドに、値を入力します。

ステップ 5 [Intra Tag Communication] を選択します。オプションは、[Enabled] または [Disabled] です

ステップ 6 [Program Default Route in VPCs into TGW/Core] を選択します。オプションは、[Enabled] または [Disabled] です。

ステップ 7 [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します。

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。

ステップ 8 [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します。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。

ステップ 9 [Add] または [Update] 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

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。

ホスト プライベート ネットワークを検出するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、**[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
- 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。

ステップ 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。

ステップ 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。

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）と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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 4 （任意）[Description] に説明を入力します。

ステップ 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。

ステップ 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。

ステップ 7 [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。

サイトの接続

クラウドゲートウェイにサイトを接続するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択し、[Manage] の下の [Gateway Management] を選択します。[Cloud Gateway] 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。

ステップ 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。

ステップ 3 [Attach SD-Routing] をクリックします。

ステップ 4 [Attach Sites] をクリックします。

ステップ 5 [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 WAN インターフェイスを持つサイトが表示されます。

ステップ 6 [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。

ステップ 7 [Next] をクリックします。

ステップ 8 [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。

ステップ 9 [Attach Sites - Select Interface] ウィンドウで、インターフェイスの詳細を入力します。このインターフェイスは、TGW へのトンネルを形成するために使用されます。

ステップ 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。

ステップ 11 [Use selected interface as Preferred Path] オプションで、[Enabled] または [Disabled] を選択します。マルチクラウドワークフローは、選択した WAN インターフェイスをデフォルトパスとして設定します。

ステップ 12 [Next] をクリックします。

ステップ 13 [Save and Exit] をクリックします。設定が完了すると、ブランチデバイスが正常に接続されたことを示すメッセージが表示されます。

ステップ 14 デバイスのステータスを確認するには、**show running config** コマンドを使用します。

ステップ 15 設定のステータスを表示するには、Cisco SD-WAN Manager のメニューから、[Configuration] > [Configuration Groups] > [Feature Profile] を選択し、[View Details] をクリックします。

サイトの切断

クラウドゲートウェイからサイトを切り離すには、次の手順を実行します。

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

ステップ 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。

ステップ 3 [Attach SD-Routing] をクリックします。

ステップ 4 [Available Sites] から 1 つ以上のサイトを選択し、[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。

ステップ 5 [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。

ステップ 6 設定のステータスを表示するには、Cisco SD-WAN Manager のメニューから、[Configuration] > [Configuration Groups] > [Feature Profile] を選択し、[View Details] をクリックします。

サイトの編集

サイトを編集するには、次の手順を実行します。

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

ステップ 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。

ステップ 3 [Edit Site Details] をクリックします。

ステップ 4 [Edit Site Details] ダイアログボックスで、トンネル数を入力します。

ステップ 5 [Accelerated VPN] フィールドを有効または無効にします。デフォルトでは、このフィールドは [Enabled] になっています。

ステップ 6 [Use Select Interface as Preferred path] フィールドを有効または無効にします。デフォルトでは、このフィールドは [Enabled] になっています。

ステップ 7 [Submit] をクリックします。

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-Routing 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） SD ルーティング ブランチ デバイスには、デフォルト VRF のみを設定できます。このデフォルト VRF を使用して、SD-Routing Cloud OnRamp ブランチ接続を介してマッピングできます。マッピングに他の VPN/VRF を使用することはできません。SD ルーティングソリューションとともに、SD-WAN ソリューションに複数の VPN マッピングを設定できます。Cisco SD-WAN と Cisco SD-Routing の両方の接続を共存させることができます。

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。

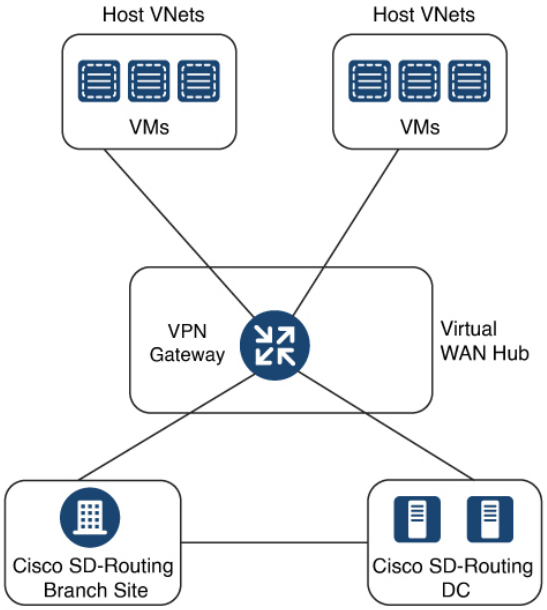
- 必要に応じて、接続の変更を表示します。
- フィルタ処理とソート。
- さまざまなリージョンのクラウドゲートウェイに依存しない接続を定義します。
- クラウドゲートウェイが存在するすべてのリージョンで接続を実現します。

Azure 仮想 WAN ハブと Cisco SD ルーティングの統合

Cisco Catalyst SD-Routing ソリューションと Azure 仮想 WAN の統合により、マルチクラウド展開の Cloud OnRamp が強化され、Cisco VPN ゲートウェイを Azure 仮想 WAN ハブのネットワーク仮想アプライアンス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 仮想 WAN は、Microsoft Azure を介して最適化および自動化さ

れたブランチからクラウドへ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 SD ルーティング 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 VPN ゲートウェイを構成すると、より高速で広い帯域幅が提供されるため、トランジット VNet を使用する際の速度と帯域幅の制限を克服できます。



仮想 WAN ハブ統合の仕組み

SD ルーティングブランチとパブリック クラウド アプリケーション間の接続は、Azure のマルチクラウド SD ルーティングワークフローの Cloud OnRamp の一部として Azure 仮想 WAN ハブ内で設定された Azure VPN ゲートウェイによって提供されます。

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 ルーティングネットワークを簡単に統合できます。

Cisco SD-WAN Manager の設定ウィザードは、パブリック クラウド アカウントに接続するための Azure 仮想 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-Routing Manager では、タグを使用して、ブランチ内のサービスのデフォルト VRF 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 ルーティングのデフォルト VRF（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。SD ルーティングと SD-WAN 接続マッピングの両方を有効にできます。SD-WAN VPN

を有効にすると、SD ルーティング VRF がデフォルトで有効になります。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。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。

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、Azure 仮想ハブ VPN ゲートウェイ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 仮想 WAN、Azure VPN ゲートウェイ、および Azure 仮想 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 仮想 WAN ハブは、デフォルトの VRF サイトと VPN ゲートウェイおよび VNet 間のコア接続を管理します。仮想ハブが作成されると、VPN ゲートウェイを Azure ネットワーキングサービスに統合できます。

Azure の前提条件

- サポートされる最小リリース：Cisco IOS XE Catalyst SD-Routing リリース 17.13.1。
- 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。

Azure SD ルーティング Cloud OnRamp の制限事項

- リージョンごとに作成できる VPN ゲートウェイは 1 つだけです。ただし、1 つのリージョンに複数の NVA ベースのクラウドゲートウェイを作成できます。
- 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。
- 同じリージョンに VPN ゲートウェイと NVA ベースのクラウドゲートウェイを組み合わせることはできません。
- VPN ゲートウェイしかない場合は、監査を実行できません。監査は、少なくとも 1 つの NVA ベースのクラウドゲートウェイがある場合にのみ実行できます。

SD ルーティング用の Azure 仮想 WAN ハブの構成

Cisco SD-WAN Manager の Cloud OnRamp for Multicloud ワークフローを使用して、Azure 仮想 WAN ハブを作成し、Cisco Catalyst SD-Routing ブランチサイト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 仮想 WAN ハブを設定するには、次のタスクを実行します。

アカウントを Cisco SD-WAN マネージャに関連付ける

アカウントを Cisco SD-WAN Manager に関連付けるには、次の手順を実行します。

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

ステップ 2 [Setup] で、[Associate Cloud Account] をクリックします。

ステップ 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。

ステップ 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。
Description (optional)	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。

フィールド	説明
クラウドゲートウェイで使用	[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。
Tenant 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。
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。

ステップ 5 [Add] をクリックします。

グローバルクラウド設定の追加と管理

グローバルクラウド設定を追加および管理するには、次の手順を実行します。

ステップ 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。

ステップ 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。

ステップ 3 グローバル設定を編集するには、[Edit] をクリックします。

ステップ 4 グローバル設定を追加するには、[Add] をクリックします。

ステップ 5 [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。

ステップ 6 [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。

ステップ 7 [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。

ステップ 8 [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。

ステップ 9 [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。

ステップ 10 [Advertise Default route to Azure Virtual Hub] フィールドを有効または無効にします。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。

ステップ 11 [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します。

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。

ステップ 12 [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します。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。

ステップ 13 [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 仮想 WAN ハブとハブ内の 2 つの Cisco VPN ゲートウェイのインスタンス化または検出が含まれます。

クラウドゲートウェイを作成および管理するには、次の手順を実行します。

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

ステップ 2 [Manage] で、[Create Cloud Gateway] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

（注） 保持できる Azure アカウントは 1 つだけです。

ステップ 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。

（注） リージョン内の VPN ゲートウェイは 1 つだけです。リージョンに VPN ゲートウェイがある場合、同じリージョンに NVA ゲートウェイを配置することはできません。

ステップ 8 [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を作成する場合は、既存のすべてのクラウドゲートウェイを削除する必要があります。また、次の 2 つのフィールドで新しい Azure 仮想 WAN と Azure 仮想 WAN ハブを作成する必要があります。

ステップ 9 [Virtual WAN] フィールドで、ドロップダウンリストから Azure 仮想 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。

ステップ 10 [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。

ステップ 11 [Solution Type] フィールドで、ドロップダウンリストから Cisco vHub と VPN を選択します。

ステップ 12 [SKU Scale Unit Size] フィールドで、ドロップダウンリストから SKU スケールユニットサイズを選択します。

ステップ 13 [Add] をクリックして VPN ゲートウェイを展開します。

サイトの接続

クラウドゲートウェイにサイトを接続するには、次の手順を実行します。

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

ステップ 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。

ステップ 3 [Attach SD-Routing] をクリックします。

ステップ 4 [Attach Sites] をクリックします。

ステップ 5 [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 WAN インターフェイスを持つサイトが表示されます。

ステップ 6 [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。

ステップ 7 [Next] をクリックします。

ステップ 8 [Attach Sites - Site Configuration] ウィンドウで、[Tunnel Count] を入力します。トンネル数は 1 で、帯域幅は 2.5 Gbps です。

ステップ 9 [Use selected interface as Preferred Path] オプションで、[Enabled] または [Disabled] を選択します。マルチクラウドワークフローは、選択した WAN インターフェイスをデフォルトパスとして設定します。

ステップ 10 [Next] をクリックします。

ステップ 11 [Save and Exit] をクリックします。設定が完了すると、ブランチデバイスが正常に接続されたことを示すメッセージが表示されます。

ステップ 12 デバイスのステータスを確認するには、**show running cofig** コマンドを使用します。

ステップ 13 設定のステータスを表示するには、Cisco SD-WAN Manager のメニューから、[Configuration] > [Configuration Groups] > [Feature Profile] を選択し、[View Details] をクリックします。

サイトの切断

クラウドゲートウェイからサイトを切り離すには、次の手順を実行します。

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

ステップ 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。

ステップ 3 [Attach SD-Routing] をクリックします。

ステップ 4 [Available Sites] から 1 つ以上のサイトを選択し、[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。

ステップ 5 [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。

ステップ 6 設定のステータスを表示するには、Cisco SD-WAN Manager のメニューから、[Configuration] > [Configuration Groups] > [Feature Profile] を選択し、[View Details] をクリックします。

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。ホスト VNet を検出してタグを作成するには、次の手順を実行します。

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

ステップ 2 [Discover] ワークフローで、[Host Private Networks] をクリックします。

ステップ 3 [Cloud Provider] フィールドで、[Microsoft Azure] を選択します。

ステップ 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。

ul

- [Add Tag]：VNet または VNet のグループのタグを作成します。
- [Edit Tag]：選択した VNet の既存のタグを変更します。
- [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 VRF のマッピング

Cisco Catalyst SD-Routing ネットワークの VNet-VRF マッピングを編集するには、次の手順を実行します。

始める前に

VNet から VRF 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 をマッピングするデフォルトの VRF 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。

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

ステップ 2 [Intent Management] で、[Connectivity] をクリックします。

ステップ 3 インテントを定義するには、[Edit] をクリックします。

ステップ 4 VRF、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 VRF 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

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。

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

ステップ 2 [Intent Management] ワークフローで、[Rebalance VNETS (Azure)] をクリックします。

ステップ 3 [Cloud Provider] フィールドで、[Microsoft Azure] を選択します。

ステップ 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。

（注） Cisco 17.13.1a リリースでは、1 つのリージョンに設定できる VPN ゲートウェイは 1 つだけです。

ステップ 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。

ステップ 6 [再調整（Rebalance）] をクリックします。

マルチクラウド向け Cisco SD ルーティング Cloud OnRamp の機能情報

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

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

表 *1*：マルチクラウド向け *Cisco SD* ルーティング *Cloud OnRamp* の機能情報

機能名	リリース	機能情報
マルチクラウド向け Cisco SD ルーティング Cloud OnRamp	Cisco IOS XE リリース 17.13.1a	Cisco SD-Routing 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 ルーティングデバイスに統合するのに役立ちます。これらの機能により、デバイスは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できます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。