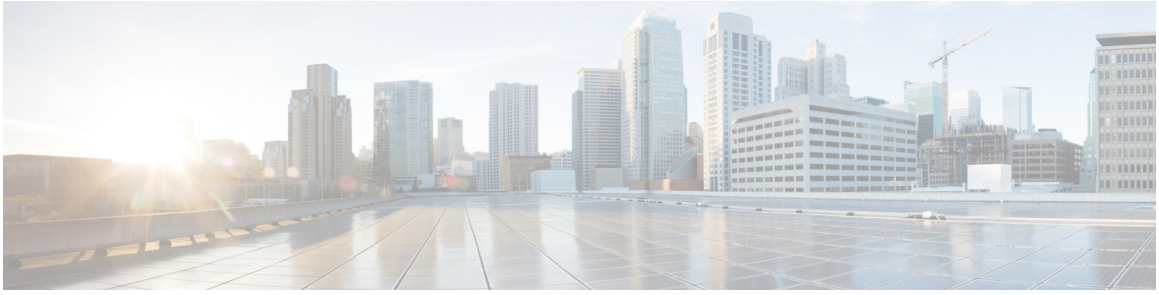
SD-Routing デバイス上のクラウド インフラストラクチャ

First Published: 2024-03-28

Last Modified: 2024-04-04

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

Full Cisco Trademarks with Software License ?

PREFACE

はじめに vii

ここに参照前文マップ vii

CHAPTER 1

概要 1

AWS 統合に関する情報 1

SD-Routing デバイスを使用した AWS Branch Connect 2

SD-Routing デバイス向け Cloud OnRamp の利点 2

Cloud onRamp の前提条件 3

制限事項 3

SD-Routing デバイスでの AWS 統合の設定 3

Azure 仮想 WAN ハブと Cisco SD-Routing の統合 14

仮想 WAN ハブ統合の仕組み 14

Azure 仮想 WAN 統合ワークフローのコンポーネント 15

Azure の前提条件 16

Azure SD-Routing Cloud OnRamp の制限事項 16

SD-Routing 用の Azure 仮想 WAN ハブの構成 16

アカウントと Cisco SD-WAN Manager の関連付け 17

グローバルクラウド設定の追加と管理 17

クラウドゲートウェイの作成と管理 18

サイトの接続 19

サイトの切断 20

ホスト VNet の検出とタグの作成 21
VNet タグとブランチネットワーク VRF のマッピング 21
VNet の再調整 22
Cisco SD-Routing Cloud OnRamp for Multicloud の機能情報 22

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

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

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

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

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

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

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

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

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

© Cisco Systems, Inc. All rights reserved.

はじめに

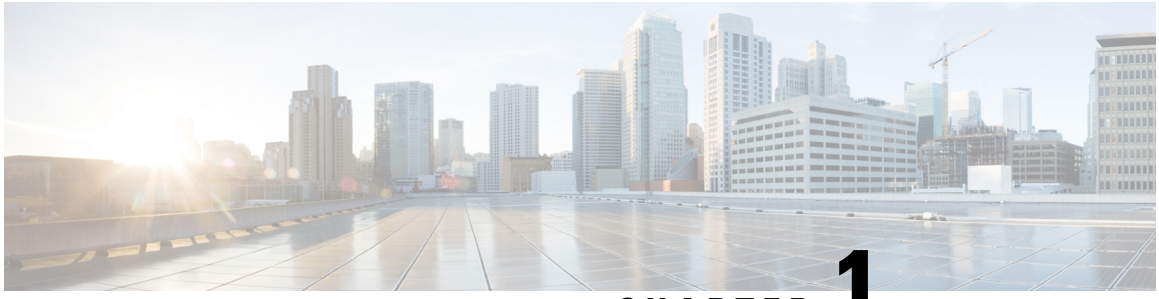
ここでは、このマニュアルの対象読者、構成、および表記法について説明します。また、他のマニュアルの入手方法についても説明します。

この前書きは、次の項で構成されています。

- ここに参照前文マップ, on page vii

ここに参照前文マップ

はじめに



CHAPTER 1

概要

Cisco Catalyst 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-Routing 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-Routing 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。

Note Cisco IOS XE 17.12.1a 以降、**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** へ、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** へのコンポーネントのブランド変更が行われました。

- AWS 統合に関する情報, on page 1
- Azure 仮想 WAN ハブと Cisco SD-Routing の統合, on page 14
- Cisco SD-Routing Cloud OnRamp for Multicloud の機能情報 , on page 22

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。

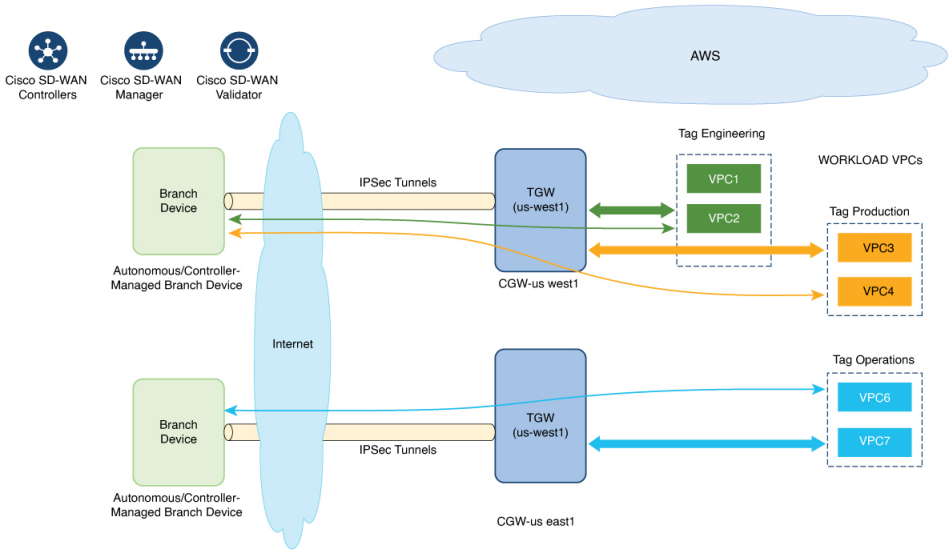
Cisco SD-WAN Manager コントローラを使用して、マルチクラウド環境の Cloud OnRamp を設定および管理できます。Cisco SD-WAN Manager の設定ウィザードは、パブリック クラウド アカウントへのトランジットゲートウェイの起動を自動化し、オーバーレイネットワーク内のブランチで、パブリッククラウドアプリケーションとそれらのアプリケーションのユーザーとの間の接続を自動化します。この機能は、Cisco Cloud ルータ上の AWS 仮想プライベートクラウド（VPC）で動作します。

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-Routing デバイスを使用した AWS Branch Connect

SD-Routing 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-Routing 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-Routing 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-Routing 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。

Note 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-Routing デバイス向け Cloud OnRamp の利点

SD-Routing Cloud OnRamp は、マルチクラウドワークフローを通じて SD-Routing デバイスを使用して 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

  ライセンスがないと、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。割り当てられていないと、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-Routing 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-Routing デバイスを取得するには、既存のデバイスの導入準備 , on page 3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新しい SD-Routing デバイスの導入準備, on page 5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-Routing デバイスでの AWS 統合の設定

ここでは、SD-Routing 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の SD-Routing デバイスへの変換、および Cloud onRamp 機能の使用
  - 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-Routing 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新しい SD-Routing 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。

Procedure

Step 1 既存の自律デバイスを SD-Routing デバイスに手動で展開または変換するには、「Onboarding the Devices Manually」のセクションに記載されている手順に従います。

または

Step 2 クイック接続ワークフローを使用して SD-Routing デバイスを展開するには、「Onboarding the SD-Routing Devices Using Bootstrap」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：

Step 3 SD-Routing 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。

Note
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-Routing 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。

Step 4 SD-Routing 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。

Step 5 [Associate Devices] をクリックし、SD-Routing デバイスのサイト ID を選択して、関連付けを続行します。

Step 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。

Step 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-Routing 設定グループ。

Step 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新しい SD-Routing 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-Routing デバイスを導入準備するには、次の手順を実行します。

Procedure

Step 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。

Step 2 [Name] フィールドに、設定グループの名前を入力します。

Step 3 [Description] フィールドに、説明を入力します。

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

Step 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。

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

Step 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。

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

Step 9 [Create New] をクリックします。

Step 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
```

Step 11 [Save] をクリックします。

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

Step 13 [Unassigned] を選択し、UUID を 1 つ選択します。

Step 14 [Save] をクリックします。

Step 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。

Step 16 [Next] をクリックします。

Step 17 [Deploy] をクリックし、

Step 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。

Step 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

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

Step 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。

Step 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。

Step 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。

Step 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-Routing 設定グループ。

Step 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。

Procedure

Step 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。

Step 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。

Step 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。

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

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

Step 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。

Step 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 Role**

[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。

a. 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 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。

   Note
   [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。

   Note
   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」を参照してください。

b. 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。

   Note
   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。

   Note
   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]"
             }
            }
          }
        ]
      }
```

Step 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。

Procedure

Step 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。

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

Step 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-Routing 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。

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

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

Step 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。

Step 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。

Step 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。

Step 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。

Procedure

Step 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。

Step 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。

Step 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。

Procedure

Step 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。

Step 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。

Step 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。

Step 4 （任意）[Description] に説明を入力します。

Step 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。

Step 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。

Step 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。

Procedure

Step 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。

Step 2 目的のクラウドゲートウェイで、[(…)] をクリックし、[Cloud Gateway] を選択します。

Step 3 [Attach SD-Routing] をクリックします。

Step 4 [Attach Sites] をクリックします。

Step 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。

Step 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。

Step 7 [Next] をクリックします。

Step 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。

Step 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。

Step 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。

Step 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。

Step 12 [Next] をクリックします。

Step 13 [Save and Exit] をクリックします。設定が成功すると、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。

Step 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。

Step 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。

Procedure

Step 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。

Step 2 目的のクラウドゲートウェイで、[…] をクリックし、[Cloud Gateway] を選択します。

Step 3 [Attach SD-Routing] をクリックします。

Step 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。

Step 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。

Step 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。

Procedure

Step 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。

Step 2 目的のクラウドゲートウェイで、[…] をクリックし、[Cloud Gateway] を選択します。

Step 3 [Edit Site Details] をクリックします。

Step 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。

Step 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。

Step 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。

Step 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。

Note SD-Routing 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-Routing 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。

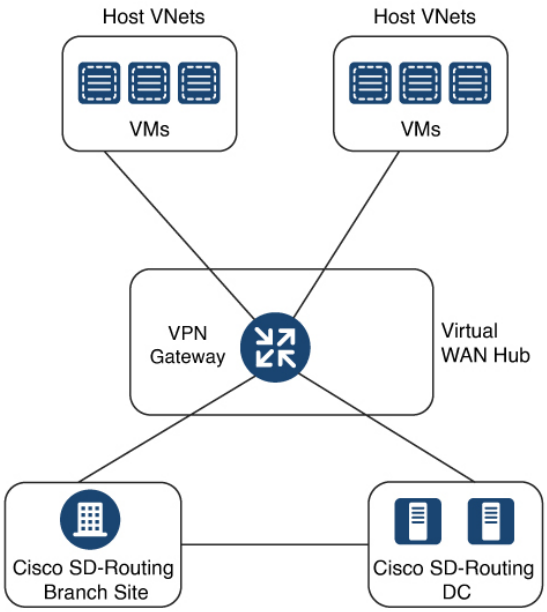
- 必要に応じて、接続の変更を表示します。

- 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-Routing 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-Routing 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、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。



仮想 WAN ハブ統合の仕組み

SD-Routing 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-Routing 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-Routing 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-Routing 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-Routing 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-Routing 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 ハブを作成することです。

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-Routing 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-Routing 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。

アカウントと Cisco SD-WAN Manager の関連付け

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。

Procedure

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

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

Step 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。

Step 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。
Use for Cloud Gateway	[Yes] を選択して、アカウントにクラウドゲートウェイを作成します。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。

Step 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。

Procedure

Step 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。

Step 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。

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

Step 4 グローバル設定を追加するには、[Add] をクリックします。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Procedure

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

Step 2 [Manage] で、[Create Cloud Gateway] をクリックします

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Note
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。

Step 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。

Note
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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Procedure

Step 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。

Step 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。

Step 3 [Attach SD-Routing] をクリックします。

Step 4 [Attach Sites] をクリックします。

Step 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。

Step 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。

Step 7 [Next] をクリックします。

Step 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。

Step 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。

Step 10 [Next] をクリックします。

Step 11 [Save and Exit] をクリックします。設定が成功すると、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。

Step 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。

Step 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。

Procedure

Step 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。

Step 2 目的のクラウドゲートウェイで、[…] をクリックし、[Cloud Gateway] を選択します。

Step 3 [Attach SD-Routing] をクリックします。

Step 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。

Step 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。

Step 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。

Procedure

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

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

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

Step 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。

Before you begin

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。

Procedure

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

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

Step 3 インテントを定義するには、[Edit] をクリックします。

Step 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。再調整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。

Procedure

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

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

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

Step 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。

Note
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。

Step 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。

Step 6 [Rebalance] をクリックします。

Cisco SD-Routing Cloud OnRamp for Multicloud 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。

Table 1: Cisco SD-Routing Cloud OnRamp for Multicloud の機能情報

機能名	リリース	機能情報
Cisco SD-Routing Cloud OnRamp for Multicloud	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-Routing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。