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 *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 （3 ページ）
- AWS 統合の制約事項 （8 ページ）
- AWS 統合の設定 （10 ページ）
- インテント管理 - 接続 （26 ページ）
- トランジット ゲートウェイ ピアリング （29 ページ）
- 監査管理 （30 ページ）
- Cisco SD-WAN Manager を使用した AWS 統合のモニター （31 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。

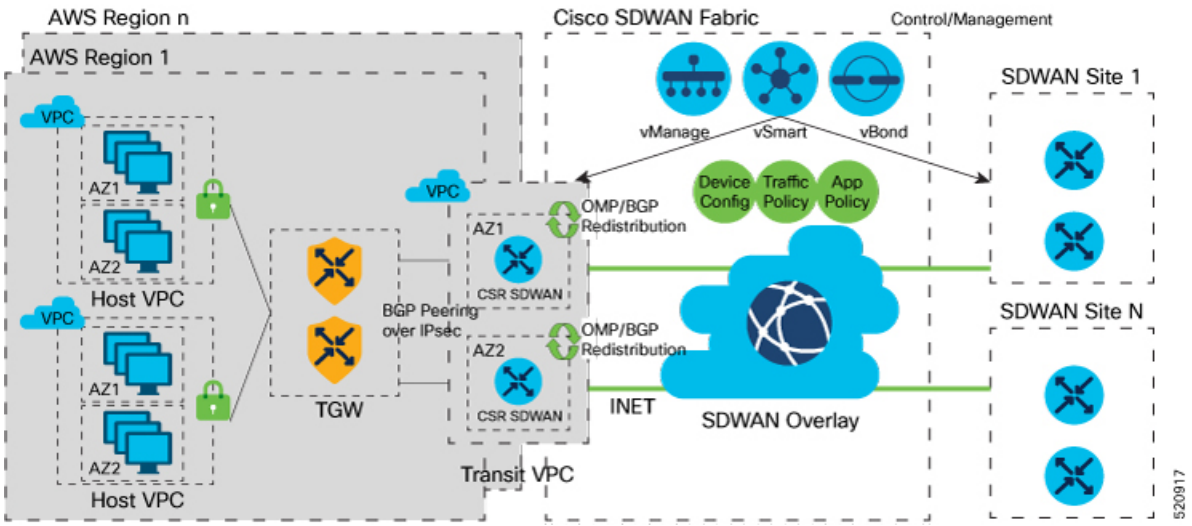
- Cisco Cloud Services Router 1000V シリーズ（Cisco CSR1000V）

（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。

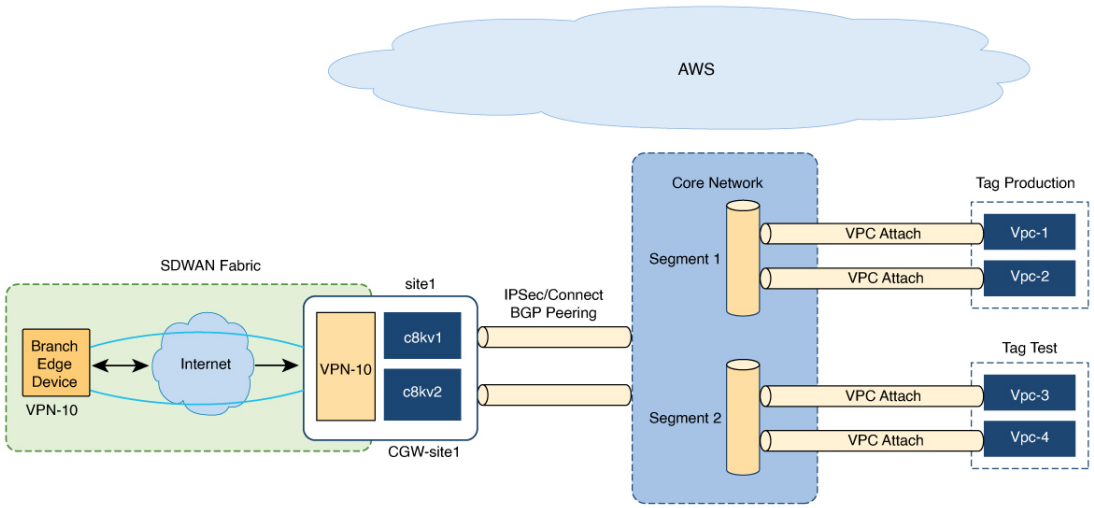
ブランチデバイステンプレートで新しいサービス VPN を設定すると、更新イベントが生成され、接続マトリックスに基づいてマッピングがトリガーされます。同様に、デバイステンプレートからサービス VPN を削除すると、別の更新イベントが生成され、マッピングの解除がトリガーされます。

（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 *1 : 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 *2:* 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 *3*：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。

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。