Google Cloud の統合

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

表 *1:* 機能の履歴

機能名	リリース情報	説明
Google Cloud を使用した Cisco SD-WAN クラウドゲートウェイ	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能により、ブランチサイトは Google Cloud で実行されているワークロードにアクセスできます。また、ブランチサイトは、Google Cloud のグローバルネットワークを介してさまざまなリージョンやサイト間でトラフィックを送受信できます。ソリューションの一環として、クラウドゲートウェイはさまざまなリージョンでインスタンス化されます。クラウドゲートウェイは Cisco Catalyst 8000V インスタンスのペアで構成され、そのインターフェイスは 3 つの異なる VPC にアンカーされます。この機能は、サイトとクラウド間の接続とサイト間の接続をサポートしています。

機能名	リリース情報	説明
Cisco SD-WAN と Google Service Directory の統合と、クラウド状態監査とクラウド リソース インベントリのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	Google Service Directory と Cisco Catalyst SD-WAN ソリューションの統合により、Cisco SD-WAN Manager を使用して Google Cloud 内のアプリケーションを検出できます。検出されたアプリケーションを使用して、Cisco SD-WAN Manager でアプリケーション認識型ルーティングポリシーを定義できます。 Cisco SD-WAN Manager の監査機能が Google Cloud 統合に拡張されました。このオプションを使用して、Google Cloud 内のオブジェクトの状態が Cisco SD-WAN Manager の状態と同期していることを確認します。 Cisco SD-WAN Manager のクラウド リソース インベントリは、クラウドオブジェクト、その識別子、そのようなオブジェクトが作成されたときのタイムスタンプなどの詳細なリストを取得します。
クラウドゲートウェイでの Cisco Catalyst 8000V インスタンスの水平スケーリング	Cisco vManage リリース 20.9.1	この機能により、特定のリージョンのクラウドゲートウェイの一部として 2 ～ 8 つの Cisco Catalyst 8000V インスタンスを展開できます。 以前のリリースでは、クラウドゲートウェイの一部として厳密に 2 つの Cisco Catalyst 8000V インスタンスを展開でき、各インスタンスはリージョンの異なるゾーンに展開されていました。

機能名	リリース情報	説明
クラウドゲートウェイの分離されたサイト間およびサイトとクラウド間の接続設定	Cisco vManage リリース 20.9.1	この機能により、一部のクラウドゲートウェイをサイト間の接続とサイトとクラウド間の接続をサポートするように設定し、他のクラウドゲートウェイをサイトとクラウド間の接続のみをサポートするように設定することができます。この設定の柔軟性は、サイト間接続をまだサポートしていない一部の Google Cloud リージョンで特に役立ちます。 以前のリリースでは、接続タイプはグローバル設定です。すべてのクラウドゲートウェイを、サイト間の接続とサイトとクラウド間の接続をサポートするように設定するか、サイトとクラウドの間の接続のみをサポートするように設定します。

サポートされるプラットフォームとインスタンス

サポートされるプラットフォーム

- Cisco Catalyst 8000V

Google Cloud でサポートされるインスタンス

- N1-standard-8
- N1-standard-4

制限事項と制約事項

- Google Network Connectivity Center の場所のサポートは、Google のサービスによって異なります。サポートされている場所の詳細については、Google Network Connectivity Center の場所に関する Google Cloud のドキュメントを参照してください。
- サービスタイプ（Standard または Premium）の変更は、変更後に作成されたクラウドゲートウェイにのみ適用されます。この変更は、すでに作成されているクラウドゲートウェイには適用されません。
- Google Cloud プロジェクトごとにサポートされるサービスアカウントは 1 つだけです。
- Google リージョンごとにサポートされるクラウドゲートウェイは 1 つだけです。
- 次の処理が進行中の場合は、新しいクラウドゲートウェイを作成できません。
  - クラウドゲートウェイの作成または削除
  - タグの作成またはマッピング
- すでに作成されているクラウドゲートウェイの設定は編集できません。
- 最初のクラウドゲートウェイがすでに作成されている場合、次のクラウドグローバル設定を変更することはできません。
  - IP サブネットプール
  - Cloud Gateway BGP ASN Offset
- ワークロード VPC サブネットに、重複する IP アドレス空間を含めることはできません。
- サイト間接続の場合、VRF と集中管理ポリシーを設定して、ブランチからサイトへのトラフィックが Google Cloud のグローバルネットワークを通過できるようにする必要があります。Google Cloud のグローバル ネットワーク トンネルで障害が発生した場合、トラフィックのドロップが予想されます。

- サイトとクラウド間の接続の場合、1 つのみの VPN を 1 つ以上のタグにマッピングできます。
- VPN が 1 つ以上のタグにマッピングされている場合は、そのようなタグの下にある VPC の合計数が、Google Cloud で指定されている VPC ピアリングの制限を超えないようにしてください。タグ内およびタグ間の接続は VPC ピアリングに依存するため、タグ内およびタグ間のマッピングのために有効になる VPC ピアリング関係の数は、Google Cloud で指定されている VPC ピアリングの制限を超えることはできません。デフォルトの VPC ピアリングの制限は 25 です。この制限を増やすには、Google Cloud サポートにお問い合わせください。Google VPC ピアリングの制限については、Google Cloud のドキュメントを参照してください。
- タグ間のマッピングは常に双方向です。
- サイトとクラウド間の接続のための VPN とタグ間のマッピングの場合、プレフィックスの数は、Google クラウドリージョンによる BGP セッションあたりのカスタム ルート アドバタイズメントの最大数（200）を超えることはできません。
- デフォルトでは、プロジェクトごとに 20 個の Google Cloud Router を使用できます。サイトとクラウド間の接続には、2 つの Google Cloud Router が必要です。サイト間の接続が有効になっている場合は、クラウドゲートウェイごとに 2 つの追加の Google Cloud Router が必要です。そのため、デフォルトの Google Cloud Router のクォータの可用性を使用して、サイト間の機能を無効にしたまま、サイトとクラウド間の接続用に 10 個のクラウドゲートウェイを作成することができます。サイト間の接続も有効にした場合は、最大 5 つのクラウドゲートウェイを作成することができます。より多くのクラウドゲートウェイをインスタンス化するために追加の Google Cloud Router が必要な場合は、Google Cloud ポータルから Google Cloud Router のクォータの増加をリクエストします。
- サイトとクラウド間のトランジット VPC のワークロード VPC から学習されたダイナミックルートは、クラウドゲートウェイの Cisco Catalyst 8000V インスタンスを使用して BGP セッションにアドバタイズされません。そのため、これらのダイナミックルートは Cisco Catalyst SD-WAN エッジデバイスに対して表示されません。
- IPv6 ネットワークアドレスはサポートされていません。
- Network Connectivity Center のトランジット VPC ハブは、Google リージョン内のすべてのクラウドゲートウェイが削除された場合にのみ削除できます。
- トランスポートロケーション（TLOC）の色の **private1** は、サイト間通信にのみ使用されます。そのため、他のインターフェイスには使用しないでください。

Google Cloud を使用した Cisco Catalyst SD-WAN クラウドゲートウェイの概要

この機能により、Cisco SD-WAN Manager の Cloud OnRamp for Multicloud ワークフローを使用して、Cisco Catalyst SD-WAN クラウドゲートウェイで冗長 Cisco Catalyst 8000V Edge ソフト

ウェア（Cisco Catalyst 8000V）インスタンスのペアを設定できます。冗長ルータを使用してクラウドゲートウェイを形成すると、パブリッククラウドに対するパスの復元力が得られます。Cisco Catalyst SD-WAN ファブリックを使用して、この機能により、ブランチおよびデータセンターのデバイスが Google Cloud のアプリケーションおよびサービスと通信できるようになります。また、Google Cloud のグローバルネットワークを使用してサイト間接続を行うこともできます。

Cisco SD-WAN Manager の Cloud OnRamp for Multicloud ワークフローは、Google Cloud での WAN 仮想プライベートクラウド（VPC）と 2 つのトランジット VPC の起動を自動化します。このワークフローは、地理的な Google Cloud リージョン内の既存の VPC も検出します。その後、Cisco SD-WAN Manager で検出された VPC のタグを作成できます。これらのタグは、サービス VPN をパブリック クラウド インフラストラクチャ内の特定の VPC にマッピングするために使用されます。このマッピングにより、Google Cloud 内のワークロード VPC への接続と、Google Cloud のグローバルネットワークを使用したサイト間接続が可能になります。

クラウドゲートウェイでの Cisco Catalyst 8000V インスタンスの水平スケーリング

最小リリース：Cisco vManage リリース 20.9.1

特定のリージョンのクラウドゲートウェイの一部として、最小 2 つ、最大 8 つの Cisco Catalyst 8000V インスタンスを展開できます。3 つ以上のインスタンスを追加する（つまり、インスタンスの数を水平方向にスケールアップする）ことで、スループットを向上させることができます。必要なスループットに基づいて、最小制限の 2 つから最大制限の 8 つのインスタンスの間で、インスタンス数を水平スケーリングできます。

2 つの Cisco Catalyst 8000V インスタンスのみを使用してクラウドゲートウェイを展開する場合、各インスタンスはリージョンの異なるゾーンに展開され、冗長性が提供されます。3 つ以上のインスタンスを持つクラウドゲートウェイを展開する場合、インスタンスは冗長性のために 2 つ以上のゾーンに展開されます。インスタンスは、ゾーン間で均等に分散されない場合があります。

（注） クラウドゲートウェイの一部であるすべての Cisco Catalyst 8000V インスタンスが、同じインスタンスタイプであることを確認します。

関連トピック

クラウドゲートウェイの作成と管理 （17 ページ）

Google Service Directory の統合とルックアップ

Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降では、Google Service Directory が Cisco Catalyst SD-WAN と統合されます。Google Service Directory は、Google Cloud 内のアプリケーションまたはサービスのカタログです。Cisco SD-WAN Manager で Service Directory のルック

アップを有効にすると、この統合により、Cisco SD-WAN Manager は Google Cloud でホストされているアプリケーションを検出し、クラウドで検出されたアプリケーションとして表示することができます。その後、このようなアプリケーションを使用して、アプリケーション認識型ルーティングポリシーを定義できます。

Google Service Directory の作成、および Google Service Directory への新しいサービスの登録については、Google のドキュメントを参照してください。

Google Service Directory のルックアップの仕組み

1. Google Service Directory のルックアップは、Cisco SD-WAN Manager の [Cloud OnRamp for Multicloud] ワークフローの [Cloud Global Settings] ウィンドウと [Associate Cloud Account] ウィンドウから設定します。

   [Service Directory Lookup Capable] として設定されているアカウントでは、ルックアップ結果が 20 分ごとに Cisco SD-WAN Manager タスクバーに表示されます。

2. Cisco SD-WAN Manager が、アカウントに関連付けられている Google リージョンをルックアップして、Google Service Directory 内のアプリケーションを検出します。

3. Cisco SD-WAN Manager が、アカウントに関連付けられている Google リージョン内の名前空間を検出してから、各名前空間内のサービスまたはアプリケーションのリストを検出します。

4. Cisco SD-WAN Manager が、名前空間で検出された各サービスのエンドポイントリストとメタデータを取得します。メタデータまたはサービス注釈には、トラフィックプロファイルなどの属性が含まれます。

   Cisco SD-WAN Manager が、サービス注釈のリストでキーワードの trafficProfile キーを検索します。次に、このキーに対する値が既知の SLA キーワード（data、voice、video、critical、realtime、best-effort、または default）のいずれかであるかどうかを確認します。値が一致しない場合、サービスのトラフィックプロファイルは default として設定されます。キーワードの trafficProfile が見つからない場合、トラフィックプロファイルは default に設定されます。サービスのトラフィックプロファイルは適切な SLA クラスに自動的に変換され、集中管理型ポリシーの作成時に使用できます。

   ルックアップの一環として、Cisco SD-WAN Manager は現在の Google Cloud のマッピング状態に対してエンドポイントリストを検証します。これにより、サービスが Cisco SD-WAN Manager を介して到達可能かどうかを判断します。

5. Cisco SD-WAN Manager を介して到達可能な検出された各サービスが、クラウドで検出されたアプリケーションとしてカタログ化されます。

   クラウドで検出されたアプリケーションの名前は、Google アカウント名、リージョン名、名前空間の名前、および Google Cloud でのサービスまたはアプリケーションの名前を連結して導出されます。名前のサブフィールドはハイフンで結合されます。クラウドで検出されたアプリケーション名の長さには、59 文字の制限があります。名前がこの文字制限を超えると、アプリケーションを追加する際に Cisco SD-AVC で問題が発生する可能性があります。これにより、ポリシーでアプリケーションが正しく使用されない可能性があります。

したがって、Google Cloud でアプリケーションの名前を決定する際には、Cisco SD-WAN Manager でクラウドで検出されたアプリケーションの名前を決定するために使用されるロジックを考慮することを推奨します。

（注） 以前に検出されたサービスまたはアプリケーションが Google Cloud で使用できなくなった場合、Cisco SD-WAN Manager はそのアプリケーションを削除します。このようなアプリケーションがポリシーで使用されている場合、アラームが生成され、ポリシーからアプリケーションを手動で削除する必要があります。削除されたサービス向けのパケットは引き続きクラウドに到達できますが、クラウドに到達した後にドロップされる可能性があります。

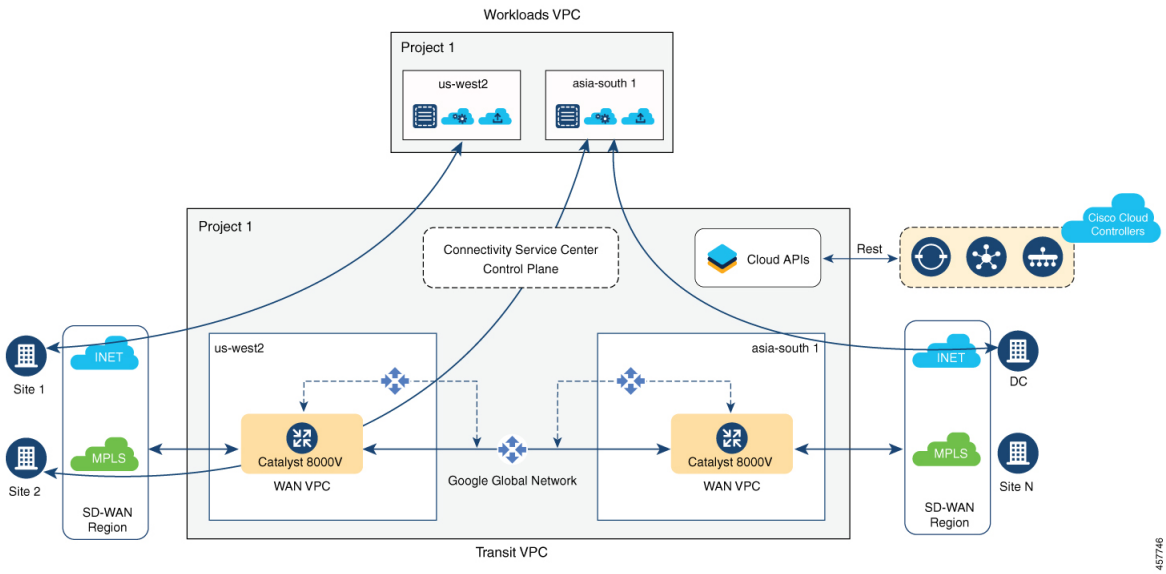
接続モデル

Google Cloud 機能を使用した Cisco Catalyst SD-WAN クラウドゲートウェイでは、次の接続モデルがサポートされています。

サイトから Google Cloud へ

このユースケースは、ブランチサイトが Google Cloud 内の VPC で実行されているアプリケーションにアクセスする必要がある場合に適用されます。このシナリオでは、ブランチサイトは WAN VPC に接続します。WAN VPC は、サイトとクラウド間のトランジット VPC を介してワークロードまたはアプリケーション VPC に接続します。

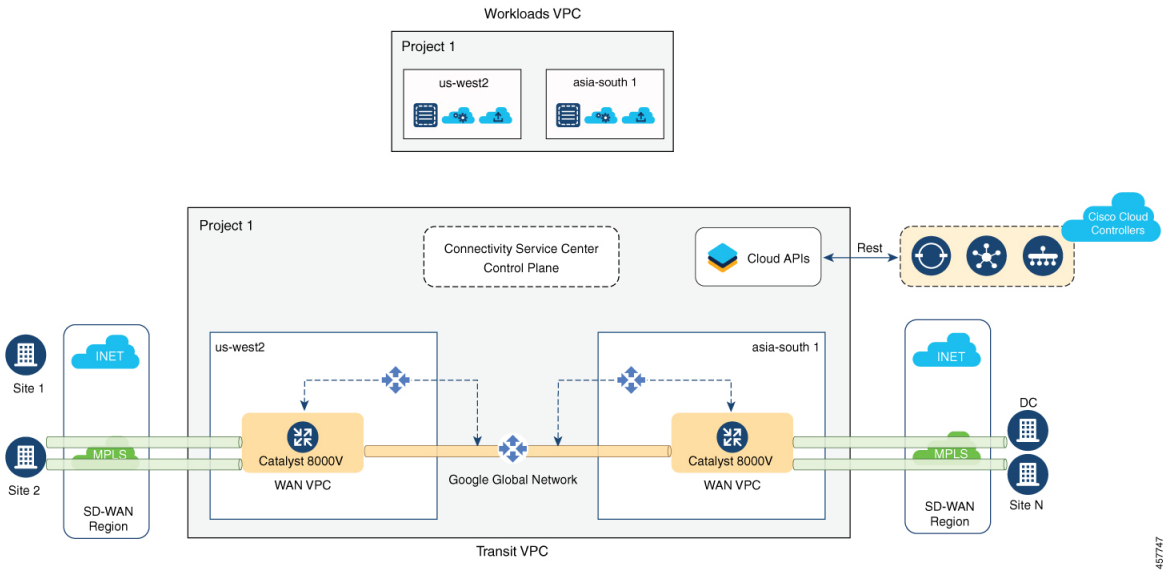
図 *1*：サイトとクラウド間の接続



サイト間

このユースケースは、Google Cloud のグローバルネットワークを使用して、サイト間トランジット VPC を介して異なるリージョンにある 2 つのブランチを接続する場合に適用されます。パブリックインターネットを介してブランチを接続することもできますが、Google Cloud のグローバルネットワークを介して接続することで、トランジットが最適化されます。

図 *2:* サイト間の接続



（注） 特定のクラウドゲートウェイまたは Google Cloud リージョン間でサイト間接続を有効にすることはできません。すべてのクラウドゲートウェイ間で、グローバルにのみ有効にできます。

Cisco vManage リリース 20.9.1 以降では、すべてのクラウドゲートウェイに対してサイト間接続をグローバルに有効にした後に、サイト間通信に参加しないように一部のクラウドゲートウェイを設定することができます（クラウドゲートウェイの分離されたサイト間およびサイトとクラウド間の接続設定 （11 ページ）を参照）。

（注） サイト間接続のユースケースでは、要件に基づいてトラフィックをインテリジェントにステアリングするための制御ポリシーを定義できます。たとえば、重要でないトラフィックフローと重要なトラフィックフローの交換のために、パブリックインターネットと Google Cloud のグローバルネットワークをそれぞれ使用することができます。詳細については、「Centralized Policies」を参照してください。

クラウドゲートウェイの分離されたサイト間およびサイトとクラウド間の接続設定

最小リリース：Cisco vManage リリース 20.9.1

Cisco vManage リリース 20.8.1 以前のリリース：グローバル設定フィールドの [Site-to-site Communication] を使用して、展開内のすべてのクラウドゲートウェイのサイト間接続を有効または無効にします。

- グローバル設定でサイト間接続を無効にした場合は、サイトとクラウド間の接続をサポートしているリージョンでのみクラウドゲートウェイを作成できます。これらのクラウドゲートウェイは、サイトとクラウド間の通信にのみ参加できます。
- グローバル設定でサイト間接続を有効にした場合は、サイト間接続をサポートしているリージョンでのみクラウドゲートウェイを作成できます。これらのクラウドゲートウェイは、サイト間通信とサイトとクラウド間の通信の両方に参加できます。ただし、サイト間接続をサポートしているリージョンは、サイトとクラウド間の接続のみをサポートしているリージョンよりも少なくなります。そのため、サイトとクラウド間の接続を利用するための選択肢は少なくなります。

Cisco vManage 20.9.1 以降：グローバル設定フィールドの [Site-to-site Communication] を使用して、展開内のすべてのクラウドゲートウェイのサイト間接続を有効または無効にします。

- グローバル設定でサイト間接続を有効にした場合、クラウドゲートウェイの作成時に [Involved in Site-to-site communication] フィールドを使用して、クラウドゲートウェイをサイト間通信に参加させるかどうかを選択することができます。
  - クラウドゲートウェイをサイト間通信に参加させない場合は、サイトとクラウド間の接続のみをサポートしている任意のリージョンにゲートウェイを作成することができます。
  - クラウドゲートウェイをサイト間通信に参加させる場合は、サイト間接続をサポートしている任意のリージョンにゲートウェイを作成することができます。クラウドゲートウェイは、サポートされているリージョン内のサイト間通信とサイトとクラウド間の通信の両方に参加できます。

  そのため、サイト間通信とサイトとクラウド間の通信に参加するクラウドゲートウェイと、サイトとクラウド間の通信のみに参加するクラウドゲートウェイを作成することができます。
- グローバル設定でサイト間接続を無効にした場合は、サイトとクラウド間の接続をサポートしているリージョンでのみクラウドゲートウェイを作成できます。サイト間接続がグローバルに無効になっている場合、特定のクラウドゲートウェイでこのタイプの接続を有効にすることはできません。

関連トピック

クラウドグローバル設定の構成 （15 ページ）
クラウドゲートウェイの作成と管理 （17 ページ）

Google Cloud を使用した Cisco Catalyst SD-WAN クラウドゲートウェイの設定

この項では、Cisco SD-WAN Manager を使用して Google Cloud 機能で Cisco Catalyst SD-WAN クラウドゲートウェイを設定する方法について説明します。この項では、この機能を設定するために満たす必要がある前提条件も示します。

設定要件

- Google Cloud のサブスクリプションが必要です。アカウントを Cisco SD-WAN Manager に関連付けるには、Google Cloud アカウントの詳細が必要です。
- Cisco SD-WAN Manager で Google Cloud サービスアカウントを登録できるようにするには、Google Cloud アカウントに少なくとも次のロールが設定されていることを確認してください。
  - サービスアカウントユーザー
  - コンピューティング インスタンス管理（v1）
  - コンピューティング ネットワーク管理
  - コンピューティング パブリック IP 管理
  - コンピューティング セキュリティ管理
  - ハブ & スポーク管理
  - スポーク管理
- 関連するプロジェクトで次の Google Cloud API が有効になっていることを確認します。
  - Compute API
  - Billing API
  - Network Connectivity Center Alpha API
- Cisco SD-WAN Manager がインターネットに接続されていて、Google Cloud と通信してアカウントを認証できることを確認します。
- Cisco SD-WAN Manager に、WAN VPC の作成に自由に使用できる 2 つの Cisco Catalyst 8000V インスタンスがあることを確認します。250 Mbps を超えるスループット要件の場合は、Cisco Catalyst 8000V ライセンスが必要です。
- すべての Cisco SD-WAN 制御コンポーネント（Cisco SD-WAN Manager、Cisco SD-WAN コントローラ、および Cisco SD-WAN Validator）が Cisco SD-WAN リリース 20.5.1 以降を実行し、Cisco Catalyst 8000V インスタンスが Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降を実行していることを確認します。

- 2 つの Cisco Catalyst 8000V インスタンスがデバイステンプレートにアタッチされていることを確認します。詳細については、「Attach Device to a Device Template」を参照してください。

（注） Cisco Catalyst 8000V を Google Cloud 用の工場出荷時のデフォルトテンプレート（Default_GCP_C8000V_Template_V01）にアタッチしていることを確認します。

- Cisco Catalyst SD-WAN の TCP ポートと UDP ポートが開いていることを確認します。詳細については、「Firewall Ports for Cisco SD-WAN Deployments」を参照してください。

デバイステンプレートへの Cisco Catalyst 8000V インスタンスのアタッチ

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
2. [Device Template] をクリックします。

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

3. [Template Type] ドロップダウンリストから [Default] を選択します。

   デフォルトテンプレートのリストが表示されます。
4. Google Cloud 用の工場出荷時のデフォルトテンプレート（Default_GCP C8000V_Template_V01）を選択します。
5. 自由に使用できる 2 つの Cisco Catalyst 8000V インスタンスをデバイステンプレートにアタッチします。詳細については、「Attach Device to a Device Template」を参照してください。

（注） インスタンスをアタッチした後に、**private1** をトランスポートロケーション（TLOC）の色として指定しないでください。**private1** はサイト間通信にのみ使用されるためです。

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

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

2. [Setup] で、[Associate Cloud Account] をクリックします。
3. [Cloud Provider] フィールドで、ドロップダウンリストから [Google Cloud] を選択します。
4. 必要な情報を入力します。

フィールド	説明
Cloud Account Name	Google Cloud アカウントの名前を入力します。
[説明（Description）]（任意）	アカウントの説明を入力します。
Use for Cloud Gateway	[Yes] を選択すると、アカウントにクラウドゲートウェイが作成されます。デフォルトでは [No] が選択されています。
[課金 ID（Billing ID）]	（オプション）Google Cloud サービスアカウントに関連付けられている課金 ID を入力します。 （注） 最初のアカウントの関連付けの後にのみ、課金 ID を入力します。 課金 ID を指定すると、自動検証プロセスが実行されます。 （注） このフィールドは、[Use for Cloud Gateway] フィールドで [Yes] オプションを選択した場合にのみ表示されます。
Service Directory Lookup （注） このフィールドは、Cisco vManage リリース 20.6.1 以降でのみ使用できます。	[Enabled] を選択して、Cisco SD-WAN Manager がクラウドアカウントに関連付けられた Google Service Directory 内のサービスまたはアプリケーションを検出できるようにします。デフォルトでは、[Disabled] が選択されています。

フィールド	説明
Private Key ID	[Upload Credential File] をクリックします。このファイルは、Google Cloud コンソールにログインして生成する必要があります。秘密キー ID は、JSON または REST API 形式の場合があります。形式は、キーの生成方法によって異なります。詳細については、Google Cloud のドキュメントを参照してください。 （注） Google Cloud からダウンロードした JSON ファイルに、**universe_domain** という名前のエントリがないことを確認します。

5. [Add] をクリックします。

クラウドグローバル設定の構成

クラウドプロバイダーのクラウドグローバル設定は、[Create Cloud Gateway] ページで設定をカスタマイズしない限り、プロバイダーのクラウドゲートウェイに適用されます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。[Cloud OnRamp for Multicloud] ウィンドウで、[Setup] エリアの [Cloud Global Settings] をクリックします。

（注） [Enable Configuration Group] オプションは、将来の使用のために予約されています。

2. [Cloud Provider] フィールドで、ドロップダウンリストから [Google Cloud] を選択します。
3. グローバル設定を追加するには、[Add] をクリックします。クラウドグローバル設定がすでに構成されている場合は、[Edit] をクリックして変更します。
4. [Software Image] フィールドで、WAN VPC の WAN エッジデバイスのソフトウェアイメージを選択します。これは、プリインストールされた Cisco Catalyst 8000V インスタンスである必要があります。
5. [Instance Size] フィールドで、ドロップダウンリストから、要件に基づいてインスタンスを選択します。
6. [IP Subnet Pool] フィールドで、Google Cloud 内の SD-WAN クラウドゲートウェイの IP サブネットプールを指定します。このサブネットプールには、/16 ～ /21 の範囲内のプレフィックスが必要です。

7. [Cloud Gateway BGP ASN Offset] フィールドで、BGP ピアリング用クラウドゲートウェイの自律システム番号（ASN）を指定します。これは、クラウドゲートウェイと Google Cloud Router の ASN 割り当ての開始オフセットです。オフセットから開始して、10 個の ASN 値がクラウドゲートウェイへの割り当て用に予約されています。

注目　このオフセット値は、クラウドゲートウェイの作成後に変更できません。

8. [Intra Tag Communication] に対して、[Enabled] を選択します。これにより、同じタグを持つ VPC が相互に通信できるようになります。

9. Google グローバルネットワークを使用したサイト間トランジット接続では、[Site-to-Site Communication] に対して [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。

10. [Site-to-Site Tunnel Encapsulation Type] フィールドで、ドロップダウンリストからカプセル化を選択します。

11. Cisco SD-WAN Manager がこの Google アカウントに関連付けられた Google Service Directory 内のアプリケーションを検出できるようにするには、[Service Directory Lookup Capable] に対して [Enabled] を選択します。 デフォルトでは [Disabled] が選択されています。

（注）　このフィールドは、Cisco vManage リリース 20.6.1 以降でのみ使用できます。

12. [Service Directory Poll Timer Value] フィールドの値は、デフォルトでは 20 分に設定されています。

    このフィールドは、Cisco vManage リリース 20.6.1 以降でのみ使用できます。

13. [Network Service Tier] フィールドで、いずれかの Google Cloud サービスパッケージを選択します。

    - [PREMIUM]：Google グローバルネットワークを使用して、高パフォーマンスのネットワーク エクスペリエンスを提供します。
    - [STANDARD]：ネットワークコストを制御できます。

14. [Save] または [Update] をクリックします。

ホスト VPC の検出とタグの作成

Google Cloud アカウントを Cisco SD-WAN Manager に関連付けると、Google Cloud アカウントに関連付けられたリージョンでホスト VPC を検出できます。このワークフローでは、VPC レベルでのクラウド インフラストラクチャが示されます。検出された VPC の新しいタグを作成したり、既存のタグを変更または削除したりすることができます。タグは、VPC と Cisco Catalyst SD-WAN ブランチ VPN 間の接続を管理するために使用されます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Discover] ワークフローで、[Host Private Networks] をクリックします。
3. [Cloud Provider] フィールドで、[Google Cloud] を選択します。

   検出されたホスト VPC のリストが、[Cloud Region]、[Account Name]、[Host VPC Name]、[Host VPC Tag]、[Account ID]、および [Host VPC ID] 列があるテーブルに表示されます。
4. [Tag Actions] ドロップダウンリストをクリックして、次のいずれかを実行します。
   - [Add Tag]：VPC または VPC のグループのタグを作成します。
   - [Edit Tag]：選択した VPC の既存のタグを変更します。
   - [Delete Tag]：選択した VPC のタグを削除します。

クラウドゲートウェイの作成と管理

最初のクラウドゲートウェイが作成されると、WAN トランジット VPC、サイト間のトランジット VPC、およびサイトとクラウド間のトランジット VPC の、3 つの予約済み VPC がインスタンス化されます。クラウドゲートウェイの一部としてインスタンス化される Cisco Catalyst 8000V インスタンスが、VPC にアンカーされます。

この手順では、Google Cloud で Cisco Catalyst SD-WAN クラウドゲートウェイを作成する方法について説明します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Manage] で、[Create Cloud Gateway] をクリックします。
3. [Cloud Provider] フィールドで、ドロップダウンリストから [Google Cloud] を選択します。
4. [Cloud Gateway Name] フィールドに、クラウドゲートウェイの名前を入力します。

（注） 名前が小文字であることを確認してください。リソースの名の指定およびリソース名の表記規則については、Google Cloud のドキュメントを参照してください。

5. （任意）[Description] に説明を入力します。
6. [Account Name] フィールドで、ドロップダウンリストから Google Cloud アカウント名を選択します。
7. [Region] フィールドで、ドロップダウンリストから Google リージョンを選択します。

8. （最小リリース：Cisco vManage リリース 20.9.1）[Involved in Site-to-site communication]：クラウドゲートウェイがサイト間通信に参加する場合は、[Yes] をクリックします。クラウドゲートウェイがサイト間通信に参加しない場合は、[No] をクリックします。

（注） このフィールドは、グローバル設定で [Site-to-site Communication] が有効になっている場合にのみ、設定に対して有効になります。グローバル設定で [Site-to-site Communication] が無効になっている場合、このフィールドはグレー表示されます。

9. （最小リリース：Cisco vManage リリース 20.10.1）[Site Name] ドロップダウンリストから、クラウドゲートウェイを作成するサイトを選択します。

10. （オプション）[Settings] セクションで、必要な情報を入力します。

（注） 以下のフィールドを使用して、クラウドのグローバル設定または個々のクラウドゲートウェイの設定のカスタマイズを使用することができます。

1. [Software Image] フィールドで、サイトを Google Cloud に接続するために WAN VPC でインスタンス化する WAN エッジデバイスのソフトウェアイメージを選択します。
2. [Instance Size] フィールドで、要件に基づいて Cisco Catalyst 8000V のインスタンスサイズを選択します。
3. [IP Subnet Pool] フィールドで、Google Cloud WAN VPC に使用する IP サブネットプールを指定します。このサブネットプールには、/16 ～ /21 の範囲内のプレフィックスが必要です。

（注） IP サブネットプールは、[Cloud Global Settings] で指定した IP サブネットプールと重複することはできません。

4. [Network Service Tier] フィールドで、ドロップダウンリストからいずれかの Google Cloud ネットワーク サービス パッケージを選択します。
   - [PREMIUM]：Google Cloud グローバルネットワークを使用して、高パフォーマンスのネットワーク エクスペリエンスを提供します。
   - [STANDARD]：ネットワークコストを制御できます。

11. [UUID (specify 2)]：

Cisco vManage リリース 20.8.1 以前：ドロップダウンリストから 2 つの Cisco Catalyst 8000V ライセンスを選択します。

Cisco vManage リリース 20.9.1 以降：ドロップダウンリストから最小で 2 つ、最大で 8 つの Cisco Catalyst 8000V ライセンスを選択します。

（注）
- クラウドゲートウェイ内のすべての Cisco Catalyst 8000v インスタンスは、同じインスタンスタイプである必要があります。垂直スケーリングはサポートされていません。
- Cisco vManage リリース 20.10.1 以降では、[Site Name] ドロップダウンリストからサイトを選択すると、UUID が自動的に入力されます。

デフォルトの Google Cloud テンプレートにアタッチした UUID を選択します。

12. （最小リリース：Cisco vManage リリース 20.10.1）[Multi-Region Fabric Settings] エリアの [MRF Role] で、[Border] または [Edge] を選択します。

このオプションは、マルチリージョンファブリックが有効になっている場合にのみ使用できます。

13. [Add] をクリックします。

VPC タグとブランチネットワーク VPN のマッピング

VPC から VPN へのマッピングを有効にするには、1 つまたは複数の Google リージョンで一連の VPC を検出し、タグを作成します。次に、同じタグを使用して VPC をマッピングするサービス VPN を選択します。

マッピングと接続の仕組み

- 明示的に接続を作成する必要はありません。VPC タグに基づいて、クラウドゲートウェイが特定のリージョンでインスタンス化されたとき、またはタグ付け操作が行われたときに、接続が自動的に確立されます。
- タグ間およびタグ内マッピングの接続インテントは、さまざまなクラウドリージョンでのクラウドゲートウェイの存在に関係なく定義できます。インテントは保持され、新しいクラウドゲートウェイまたはマッピングの変更が検出されたときにマッピングが実現されます。
- クラウドゲートウェイが異なるリージョンでインスタンス化されると、マッピングインテントがそれらのリージョンで自動的に実現されます。
- タグ間およびタグ内マッピングは VPC ピアリングに基づいていて、双方向接続のみを自動的に有効にします。
- 1 つのサービス VPN のみを、1 つ以上のタグにマッピングできます。
- 一度に実行できるクラウド操作（タグ付け、マッピング、クラウドゲートウェイの作成または削除など）は 1 つだけです。1 つの操作が実行されていると、他の操作はロックされます。

- すべてのクラウド操作には時間制限があります。たとえば、マッピング操作は 60 分後にタイムアウトします。タイムアウト時に、操作は失敗として宣言されます。タイムアウト値は設定できません。
- 新しいマッピングインテントの実現中は、[Intent Management] ページは自動更新されません。

正常にマッピングするための前提条件

- （タグの一部として）マッピングに関係する VPC には、少なくとも 1 つのサブネットが必要です。
- マッピングは VPC ピアリングに依存しています。ピアリング VPC のサブネットは、RFC1918 に準拠している必要があります。
- VPC では Classless Interdomain Routing（CIDR）アドレスは重複できません。CIDR アドレスが重複していると、マッピングが失敗します。

接続の表示または編集

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Intent Management] で、[Cloud Connectivity] をクリックします。
3. [Cloud Provider] フィールドで、ドロップダウンリストから [Google Cloud] を選択します。

   ウィンドウに、送信元 VPN とその宛先を示す接続マトリックスが表示されます。次の凡例で、インテントのステータスに関する情報が提供されます。

   - 青：インテント定義済み
   - 緑：インテント実現済み
   - 赤：インテント実現済み（エラーあり）

   マトリックス内のいずれかのセルをクリックすると、より詳細なステータス情報が表示されます。
4. [Edit] をクリックして、新しいインテントを定義または記録します。
5. VPN、およびそれに関連付けられている VPC タグに対応するセルを選択し、[Save] をクリックします。

Service Directory のルックアップと検出されたアプリケーションによるトラフィックポリシー

Cisco SD-WAN Manager のトラフィックポリシーで Google Cloud アカウントのサービスまたはアプリケーションを使用するには、まず Cisco SD-WAN Manager で Service Directory のルックアップを有効にしてから、このルックアップによって検出されたアプリケーションを使用してトラフィックポリシーを作成する必要があります。

Service Directory のルックアップの有効化

Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降では、Google Service Directory が Cisco Catalyst SD-WAN ソリューションに統合されました。この統合により、Cisco SD-WAN Manager は、Cisco SD-WAN Manager に関連付けられている Google Cloud アカウントの一部である Google Service Directory のルックアップを実行できます。Cisco SD-WAN Manager は、ルーティングポリシーの定義に使用できるカスタムアプリケーションとして、Service Directory 内のアプリケーションまたはサービスを表示します。

Cisco SD-WAN Manager で Google Service Directory を検索できるようにするには、Cisco SD-WAN Manager で Service Directory のルックアップを有効にする必要があります。

クラウドで検出されたカスタムアプリケーションの命名

Service Directory のルックアップは、Google Cloud で定義したサービスを Google Cloud にクエリします。Cisco SD-WAN Manager により、このサービス用に Cisco Catalyst SD-WAN 内にカスタムアプリケーションが自動的に作成されます。カスタムアプリケーションの名前を作成するために、Cisco SD-WAN Manager は Google Cloud で定義されているフィールド（Google Cloud のアカウント名、Google Cloud のリージョン名、サービス名、および名前空間）の組み合わせを使用します。クラウドで検出されたカスタムアプリケーションの名前の最大長は、SD-AVC コンポーネントの制限により、59 文字です。

Cisco SD-WAN Manager で、カスタムアプリケーションが表示されるアプリケーション リストページを表示できます。Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Policies]** を選択してから、[Custom Options] をクリックし、[Lists] を選択します。Cloud OnRamp for Multicloud によって検出されたサービスから Cisco SD-WAN Manager が生成したカスタムアプリケーションを表示するには、[Cloud Discovered] をクリックします。

- Cisco SD-WAN Manager 20.6.x は、59 文字の制限を次のように処理します。Cisco SD-WAN Manager が上記の 4 つのフィールドを使用してカスタムアプリケーションの名前を作成する場合、名前が 59 文字を超えると、名前が切り捨てられます。名前が切り捨てられると、名前の競合が発生する可能性があります。

  アカウント名とリージョン名の長さは可変であるため、59 文字の制限内でサービス名と名前空間に使用できる残りの文字数を予測することは困難です。

  文字数制限を超えないように、Google Cloud でサービスを定義する際は、サービス名と名前空間名に短い名前を使用することを推奨します。これらの名前で使用可能な長さは、

Google Cloud のアカウント名と Google Cloud のリージョン名を組み合わせた長さによって異なります。

- 次の例では、アカウント名とリージョン名が長いため、短いサービス名と名前空間名が必要です。

  アカウント名：gcp-organization-sw-dev
  リージョン名：australia-southeast1
  サービス名：serv1
  名前空間名：nspace1

- 次の例では、アカウント名とリージョン名が短いため、長いサービス名と名前空間名を使用できます。

  アカウント名：cisco
  リージョン名：us-west
  サービス名：service-xyz
  名前空間名：dev-team

- Cisco SD-WAN Manager 20.7.x 以降では、Google Cloud で定義されたサービスの名前空間とサービス名のフィールドに、より長くわかりやすい名前を使用できます。必要に応じて、最大 59 文字の制限を満たすために、Cisco SD-WAN Manager はサービス名の一部を切り捨てることがあります。

  Cisco SD-WAN Manager は、Google Cloud のアカウント名に 12 文字の制限、Google Cloud のリージョン名に 23 文字の制限、名前空間に 8 文字の制限を適用します。カスタムアプリケーション名では、区切り文字（-）に 3 文字が使用されます。サービス名が切り捨てられずに 59 文字の制限内に収まるようにするには、Google Cloud でサービスのサービス名を指定するときに、最大 13 文字を使用します。より長い名前を使用し、これらのフィールドの組み合わせが 59 文字を超える場合、Cisco SD-WAN Manager は名前を切り捨てます。名前の切り捨てによって、以前に定義されたカスタムアプリケーションとの名前の競合が発生した場合、Cisco SD-WAN Manager はアプリケーション リスト ページにアラームを表示します（アプリケーション リスト ページを開くための手順は上に示されています）。

はじめる前に

Cisco SD-WAN Manager で SD-AVC が有効になっていることを確認します。

- Cisco SD-WAN Manager で SD-AVC を有効にします。

  1. Cisco SD-WAN Manager のメニューから、**[Administration]** > **[Cluster Management]** の順に選択します。
  2. 目的の Cisco SD-WAN Manager インスタンスについて、[...] をクリックし、[Edit] を選択して、[Enable SD-AVC] チェックボックスをオンにします。

- Google Cloud アカウントで Service Directory API が有効になっていることを確認します。

Service Directory のルックアップの有効化

1. **Cloud OnRamp for Multicloud** ワークフローの [Associate Cloud Account] ウィンドウから [Service Directory Lookup] を有効にします。

   詳細については、この章の「Cisco SD-WAN Manager と Google Cloud アカウントの関連付け」のトピックを参照してください。

2. [Cloud Global Settings] で、Cisco SD-WAN Manager に関連付けられている Google アカウントを [Service Directory Lookup Capable] として有効にして、[Service Directory Poll Timer Value] を設定します。

   詳細については、「クラウドグローバル設定の構成」を参照してください。

クラウドで検出されたアプリケーションを使用したトラフィックポリシーの作成

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [カスタムオプション（Custom Options）] をクリックします。
3. [Centralized Policy] で、[Lists] をクリックします。

   [Policies] の下の [Application] セクションにリダイレクトされます。
4. [Cloud Discovered] をクリックします。

   Google Service Directory のルックアップによって検出されたアプリケーションのリストが表示されます。
5. [Map Traffic Profiles] をクリックします。表示されるダイアログボックスで、検出されたサービスのトラフィックプロファイルを設定または変更できます。
6. トラフィックプロファイルごとに、[vManage SLA Classes] をクリックし、アプリケーションをマッピングする SLA クラスを選択します。
7. [Save] をクリックします。
8. 次に、クラウドで検出されたアプリケーションを含むアプリケーションリストを作成します。詳細については、「Configure Application List」を参照してください。
9. 検出されたアプリケーションを使用してトラフィックポリシーを作成するには、**[Custom Options]** > **[Traffic Policy]** をクリックしてから、[Add Policy] をクリックします。

   クラウドで検出されたアプリケーションのアプリケーションリストでトラフィックルールを設定するには、「Application-Aware Routing」の「Configure Traffic Rules」を参照してください。

接続のモニター

新しいクラウドゲートウェイを作成するときに、クラウドゲートウェイ内でプロビジョニングされた Cisco Catalyst 8000V インスタンスの起動と到達可能性を確認できます。

オプション 1

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Cloud] の下の [Network Snapshot] では、さまざまなクラウドプロバイダーのクラウドゲートウェイ、ホスト VPC、および WAN エッジデバイスの概要が表示されます。

   WANエッジデバイスの横にある上向きの矢印は、稼働しているデバイスの数を示します。矢印をクリックして、デバイスの詳細を表示します。

オプション 2

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Workflows] セクションで、[Intent Management] の下の [Cloud Connectivity] をクリックします。
3. [Cloud Provider] フィールドで、ドロップダウンリストから [Google Cloud] を選択します。
4. ページ上の任意のセルをクリックすると、VPN と VPC タグの接続ステータスが表示されます。

監査

Cisco vManage リリース 20.6.1 以降では、[Cloud OnRamp for Multicloud] ワークフローの [Audit] オプションが Google Cloud に対して有効になっています。このオプションを使用して、Google Cloud の状態が Cisco SD-WAN Manager の状態と同期しているかどうかを確認します。監査の一環として、クラウドの状態が Cisco SD-WAN Manager の状態と同期していないと識別された場合、Cisco SD-WAN Manager は自動的に問題の解決を試行し、状態を同等にしようとします。

監査メカニズムの一部として、クラウドオブジェクトの存在、それらの相互関係、およびそれらの状態はすべて、Cisco SD-WAN Manager で定義された接続インテントに照らして検証されます。不一致が特定された場合は、Cisco SD-WAN Manager が修正処置を行います。

監査オプションによって識別されるエラーのタイプ

回復可能なエラー

これらは、Cisco SD-WAN Manager がアクションを実行して解決できるエラーです。Cisco SD-WAN Manager は、Cisco SD-WAN Manager によって作成されたオブジェクトのエラーを解

決できます。監査オプションでは、次のシナリオで不足しているリソースを再作成することにより、次のエラーを自動的に検出して解決しようとします。

- ハブまたはスポークの削除
- Google Cloud Router の削除（プライマリ、セカンダリ、またはその両方）
- Cisco SD-WAN Manager の VPN にマッピングされた VPC のサイトとクラウド間のピアリングの削除
- Cisco SD-WAN Manager の他の VPC にマッピングされた VPC の VPC ピアリングの削除
- カスタムルートの欠落
- BGP セッションの欠落
- 古い BGP セッション

回復不能なエラー

これらは、Cisco SD-WAN Manager では解決できないエラーであり、手動による介入が必要です。

- クラウドゲートウェイまたはそのコンポーネントのいずれかの削除
- CIDR が重複しているホスト VPC の問題
- サイト間の VPC の問題
- サイトとクラウド間の VPC の問題
- WAN VPC の問題

定期監査

Cisco SD-WAN Manager は、2 時間ごとに自動監査をトリガーします。この自動監査はバックグラウンドで実行され、回復可能な問題を解決します。

Cisco SD-WAN Manager にはこの監査の結果が表示されませんが、定期的な監査に関連するイベントが記録されます。

オンデマンド監査

これは、ユーザーが起動する監査です。オンデマンド監査を開始するには、次の手順に従います。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Intent Management] エリアで、[Audit] をクリックします。
3. [Cloud Provider] フィールドで、[Google Cloud] を選択します。

このウィンドウには、さまざまな Google Cloud オブジェクトのステータスが表示されます。

4. いずれかのオブジェクトのステータスが [Out of Sync] と表示されている場合は、[Fix Sync issues] をクリックします。このオプションにより、回復可能なエラーが解決されます。

（注） [Fix Sync Issues] をクリックして、問題を修正できない場合は、同じ状態を示すタスクの更新が表示されます。回復不能なエラーには、手動による介入が必要です。

クラウド リソース インベントリの表示

Cisco vManage リリース 20.6.1 以降では、Google Cloud 用に有効にされた Cisco SD-WAN Manager で [Cloud Resource Inventory] オプションを使用できます。Cisco SD-WAN Manager に関連付けられている Google Cloud アカウントのクラウドオブジェクトとその識別子の詳細を表示するには、このオプションを使用します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Manage] の下の [Gateway Management] をクリックします。

   既存のクラウドゲートウェイが表示されます。
3. 目的のクラウドゲートウェイで、[…] をクリックし、[Cloud Resource Inventory] を選択します。

[Cloud Resource Inventory] オプションを使用すると、選択したクラウドゲートウェイの次の情報を取得します。

- VPC：WAN、サイト間、およびサイトとクラウド間の VPC。
- VPC サブネット：Google Cloud アカウントに関連付けられている各 Google Cloud リージョンの WAN、サイト間、およびサイトとクラウド間。
- VM：各 Google Cloud リージョン内の Cisco Catalyst 8000V インスタンスのペア。
- Google Cloud Router：各リージョンのそれぞれのサイトとクラウド間およびサイト間の Google Cloud Router のペア。
- ハブ：それぞれのサイト間およびサイトとクラウド間の Google グローバルネットワークハブのインスタンス。
- スポーク：サイト間およびサイトとクラウド間のハブに接続されている各リージョンからのスポークのペア。

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。