概要

Google Cloud の概要

次のセクションでは、Cisco Cloud APIC および Nexus Dashboard Orchestrator に関連する Google Cloud の概念の概要を簡単に説明します。Cloud APIC のデプロイと構成の詳細については、[Cloud APIC のドキュメント（Cloud APIC documentation）]を参照してください。

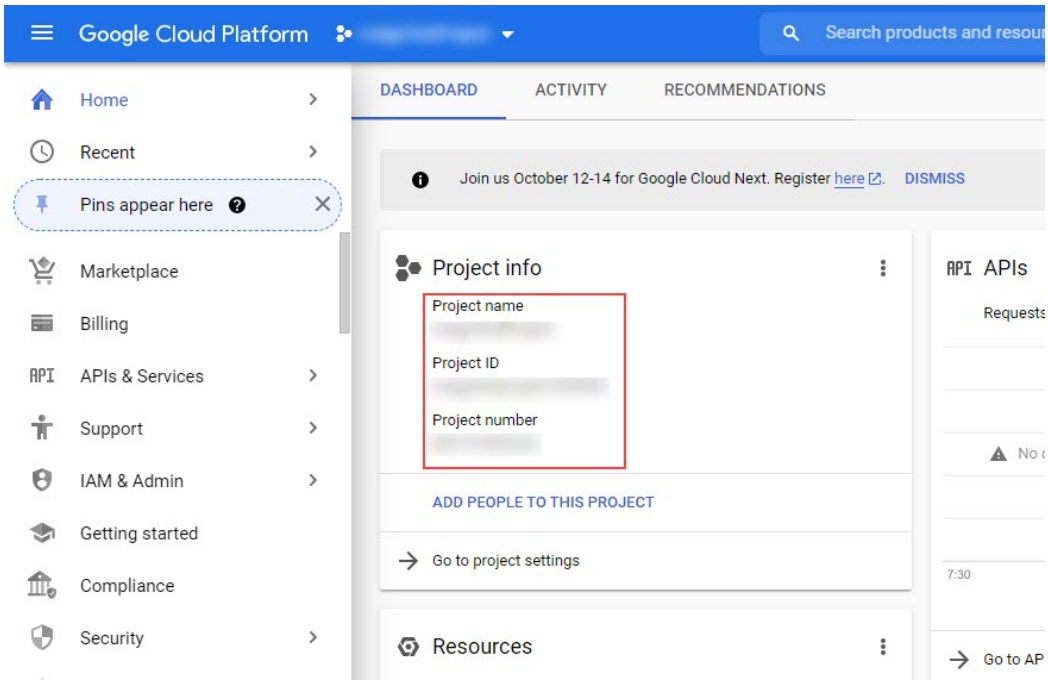
Google Cloud プロジェクトの重要な情報の検索

Google Cloud サイトに新しいテナントを作成する場合は、次の情報が必要です。既存のテナントのみをインポートする予定の場合は、このセクションをスキップできます。

Google Cloud プロジェクトを作成すると、そのプロジェクトには次の 3 つの固有の識別子が割り当てられます。

- プロジェクト名
- プロジェクト ID
- プロジェクト番号

Google Cloud 構成プロセスのさまざまな時点で、Google Cloud プロジェクトにこれら 3 つの識別子が必要になります。これらの Google Cloud プロジェクトIDを含む **[プロジェクト情報（Project Info）]** ペインを見つけるには、Google Cloud アカウントにログインし、**[プロジェクトの選択（Select a Project）]** ウィンドウで特定の Google Cloud プロジェクトを選択します。このプロジェクトの **[ダッシュボード（Dashboard）]** が表示され、[プロジェクト情報（Project Info）] ペインに Google Cloud プロジェクトのこれら3つの一意の識別子が表示されます。



Cloud APIC を使用した Google Cloud の展開について

Google Cloud は、ファイル システムに似た方法でリソースを編成します。

- 最上位の組織は複数のフォルダを持つことができます。
- すべてのフォルダには、他のフォルダを含めることも、すべてのプロジェクトに一意の ID があるプロジェクトを含めることもできます。
- クラウド リソース（VM、VPC、サブネットなど）はプロジェクトに含まれます。

組織とフォルダのレベルは、Google Cloud の観点から理解するのに有用な領域ですが、プロジェクトレベルは、Cloud APIC の観点から最も関連性があります。

各 Cloud APIC テナントは Google Cloud プロジェクトに 1 対 1 でマッピングされます。

- Cloud APIC テナントは複数の Google Cloud プロジェクトにまたがることはできません
- Google Cloud プロジェクトに複数の Cloud APIC テナントが存在することはできません

Cloud APIC を使用すると、Google Cloud は**[サービス アカウント（Service Accounts）]**を使用してプロジェクトへのアクセスを提供します。これらのアカウントは、Google Cloud サービスにアクセスする必要があるアプリケーション用です。これらを使用して、Google Cloud と他のテナントのポリシーを実行および展開し、プッシュすることができます。Google Cloud 内部で実行されるアプリケーションで使用されるサービスアカウントにはクレデンシャルは必要ありませんが、事前に生成された秘密キーを必要とする Google Cloud の外部で実行されるアプリケーションにはクレデンシャルが必要です。サービス アカウントは1つの Google Cloud プロ

ジェクトに存在しますが、他のプロジェクト（Google Cloud の場合、他のテナント用）のポリシーを管理するためのアクセス権も付与されます。

管理対象クレデンシャルを持つユーザ テナント

このタイプのユーザ テナントには、次の特性があります。

- このテナント アカウントは、Cisco Cloud APIC によって管理されます。
- このタイプのユーザー テナントのテナント設定プロセスの一環として、最初に Nexus Dashboard Orchestrator GUIで **[管理対象アイデンティティ（Managed Identity）]** を選択します。
- Nexus Dashboard Orchestrator で必要なパラメータを構成した後で、Google Cloud でこのテナントに必要な権限を設定する必要があります。クラウド APIC によって作成されたサービス アカウントを、次のルールを使用して IAM ユーザーとして追加します。
  - クラウド機能サービス エージェント
  - 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 ネットワーク管理者
  - コンピューティング セキュリティ管理者
  - 管理者のログイン
  - パブ/サブ管理者
  - ストレージ管理者

管理対象外クレデンシャルを持つユーザ テナント

このタイプのユーザ テナントには、次の特性があります。

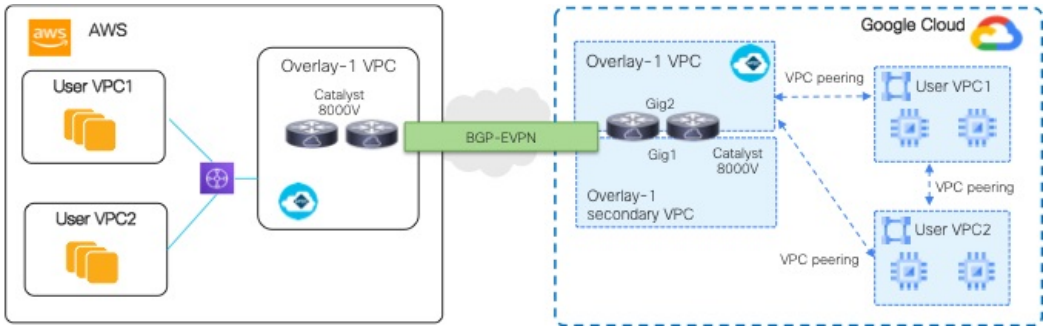
- このテナント アカウントは、Cisco Cloud APIC によって管理されません。
- このタイプのテナントの Cisco Cloud APIC に必要なパラメータを設定する前に、まず、このテナントに関連付けられたサービス アカウントの Google Cloud から必要な秘密キー情報を含む JSON ファイルをダウンロードする必要があります。
- 次に、このタイプのユーザー テナントのテナント設定プロセスの一環として、Nexus Dashboard Orchestrator GUI で **[管理対象外アイデンティティ（Unmanaged Identity）]** を選択します。Nexus Dashboard Orchestrator でこのタイプのテナントの構成プロセスの一環として、ダウンロードした JSON ファイルから次の情報を提供します。
  - キーID
  - RSA プライベート キー
  - クライアントID
  - E メール

BGP-EVPN を使用したサイト間接続

Cloud Network Controller リリース 25.0(5) 以降、次のシナリオでサイト間接続用の BGP-EVPN 接続を構成するためのサポートも利用できます。

- クラウド サイトからクラウド サイトへ：
  - Google Cloud サイトから Google Cloud サイトへ
  - Google Cloud サイトから AWS サイトへ
  - Google Cloud サイトから Azure サイトへ
- Google Cloud サイトから AWS サイトへ

これらの各シナリオでは、BGP-EVPN 接続に Cisco Catalyst 8000V が使用されます。



BGP-EVPN を使用したサイト間接続の特性

GCP の動作に基づいて、VM またはインスタンスの各ネットワーク インターフェイスを異なる VPC に関連付ける必要があります。Cisco Catalyst 8000V も VM であるため、これは、特定の Cisco Catalyst 8000V の各ネットワーク インターフェイスを異なる VPC に関連付ける必要があることを意味します。したがって、Cisco Catalyst 8000V の 2 つのギガビット ネットワーク インターフェイスは、次のように使用されます。

- gig1 インターフェイスは、overlay-1 セカンダリ VPC に関連付けられています。また、gig1 インターフェイスは管理インターフェイスとして使用されます。
- gig2 インターフェイスは、overlay-1 VPC に関連付けられています。また、ルーティング インターフェイスとしてgig2 インターフェイスを使用しています。

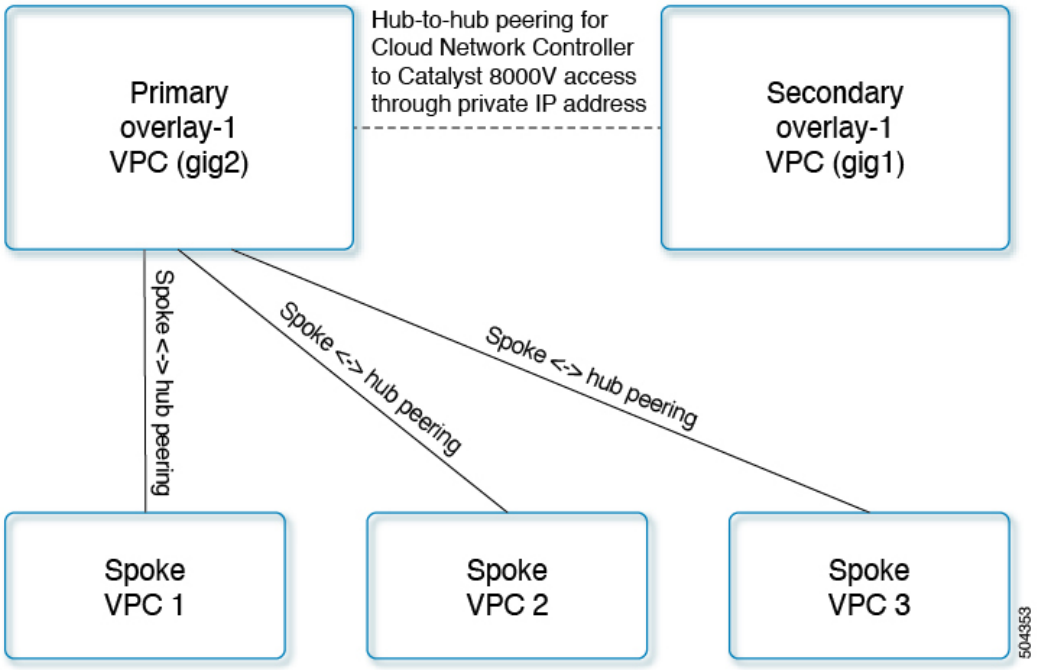
VPC ピアリング

スポーク VPC からオンプレミス ネットワークへの通信を行うには、スポーク VPC でハブ VPC へのピアリングが有効になっている必要があります。ピアリングは、Cisco Cloud Network Controller からの意図によって自動化されます。次の図に示すように、Google Cloud を使用した Cisco Cloud Network Controller の VPC ピアリングは、ハブスポーク トポロジを採用しています。

Google Cloud を備えた Cisco Cloud Network Controller は、次の 3 種類の VPC ピアリングを使用します。

- スポーク間 VPC ピアリング：これは、スポーク間のサイト内通信に使用されます。
- ハブツースポーク VPC ピアリング：これは、BGP-EVPN を使用して Cisco Catalyst 8000V ルーターを経由するサイト間通信に使用されます。
- ハブツーハブ VPC ピアリング：これは、overlay-1 VPC の Cisco Cloud Network Controller と overlay-1 セカンダリ VPC の Cisco Catalyst 8000V ルーター管理インターフェイスとの間の通信に使用されます。

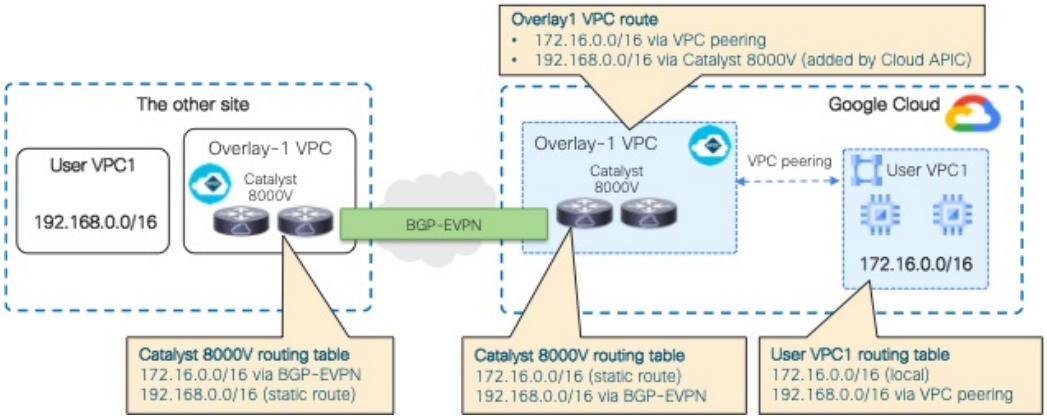
オーバーレイ 1 セカンダリ VPC は、スポーク間またはサイト間トラフィックのデータ パスに関与しないことに注意してください。



Cisco Cloud Network Controller は、次の状況でクラウド サイト間でルートを交換するための構成を自動化します。

- 同じサイト内の接続先へのオーバーレイ 1 VPC：オーバーレイ 1 VPC には、VPC ピアリングを介した同じサイト内のスポーク VPC へのルートがあります。
- 別のサイトの接続先への VPC のスポーク：他のサイトのサブネットのルートは、Cisco Cloud Network Controller によってオーバーレイ 1 VPC に追加され、ルートはスポーク VPC にエクスポートされます。このようにして、スポーク VPC には、他のサイトの接続先サブネットに到達するためのルートがあります。
- 異なるサイトの Cisco Catalyst 8000V 間：スポーク VPC CIDR の静的ルートは、同じサイトの Cisco Catalyst 8000V ルーターに追加されます。静的ルートは、BGP EVPN を介して他のサイトの Catalyst 8000V ルータに再配布されます。このようにして、Catalyst 8000V に

は、次の図に示すように、他のサイトの接続先サブネットに到達するためのルートがあります。



このシナリオでは、リモート CIDR への静的ルートがハブ VPC で、ネクスト ホップが Cisco Catalyst 8000V としてプログラムされています。これらのルートは、ピアリングを使用してスポーク VPC によって学習されます。

外部ネットワーク接続

サポートは、Google Cloudサイトと非 Google Cloud サイトまたは外部デバイス間の外部接続に使用できます。この IPv4 接続を確立するには、Google Cloud ルータと外部デバイス（CSR を含む）の間に VPN 接続を作成します。

次の項では、Cloud APIC リリース 25.0（2）以降で提供される新しい外部ネットワーク接続を可能にするコンポーネントの詳細について説明します。

外部VRF

[外部 VRF（external VRF）] は、クラウド内に存在しない一意の VRF です。このVRFは、Nexus Dashboard Orchestrator によって使用されるクラウド コンテキスト プロファイルでは参照されません。

外部 VRF は、他のクラウド サイトまたはオンプレミス サイトに接続されている外部ネットワークを表します。複数のクラウド VRF は、ルートを外部 VRF にリークしたり、外部 VRF からルートを取得したりする可能性があります。外部 VRF で外部ネットワークが作成されると、VRF 間ルーティングが設定され、外部ネットワークで受信およびアドバタイズされたルートが外部 VRF で受信またはアドバタイズされます。

クラウド ネイティブ ルータ

Google Cloud を使用して Cisco Cloud APIC を構成すると、インフラ VPC は Google Cloud ネイティブ ルータ（クラウド ルータおよびクラウド VPN ゲートウェイ）を使用して、オンプレミス サイト、他のクラウド サイト、または任意のリモート デバイスへの IPsec トンネルと BGP

セッションを作成します。BGP - IPv4 セッションが外部 VRF で作成されているクラウド ネイティブ ルータを使用したこのタイプの接続では、BGP - IPv4 接続のみがサポートされます。

Google Cloud は、スタティック ルートと BGP の両方で VPN 接続をサポートします。BGP との VPN 接続を作成するために、Cisco Cloud APIC はクラウド ルータと VPN ゲートウェイの両方が必要です。VPC は複数のクラウド ルータと VPN ゲートウェイを持つことができます。ただし、Google Cloud には、クラウド ルータと VPN ゲートウェイの両方が同じリージョンおよび同じ VPC に存在する必要があるという制限があります。さらに、Cisco Cloud APIC ではリージョンごとに 1 つのクラウド ルータと 1 つのクラウド VPN ゲートウェイのみがサポートされるという制限があります。

VPN 通信

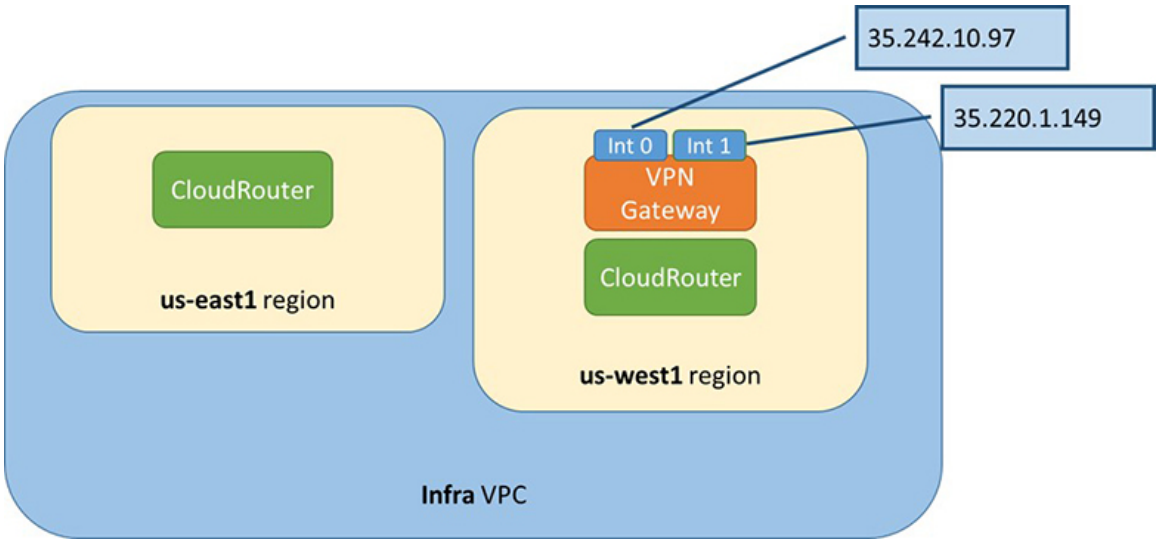
Cisco Cloud APIC を Google Cloud で構成する場合、インフラ VPC を使用して Cisco Cloud APIC をホストし、外部デバイスおよびサイトへの VPN 接続をホストします。ただし、インフラ VPC は、スポーク間通信を実装するための中継として使用されません。代わりに、Cisco Cloud APIC を Google Cloud と使用して構成すると、スポーク間通信はスポーク間 VPC ピアリングによって行われます。

インフラ VPC は、Google Cloud ルータと Google Cloud VPN ゲートウェイを使用して、オンプレミス サイトまたは他のクラウド サイトへの IPsec トンネルと BGP セッションを作成します。スポーク VPC は、インフラ VPC とピアリングして、外部サイトへの VPN 接続を共有します。

- VPN 接続で受信したルートがスポーク VPC にリークされる
- スポーク VPC ルートが VPN 接続でアドバタイズされる

VRF 間ルーティングを使用すると、VPN 接続の外部 VRF とクラウド ローカル スポーク VRF 間でルートがリークされます。

VPN ゲートウェイには 2 つのインターフェイスがあり、Google Cloud は各インターフェイスにパブリック IP アドレスを割り当てます。Google Cloud VPN ゲートウェイは 1 つまたは 2 つのインターフェイスを持つことができますが、ハイアベイラビリティを実現するには 2 つのインターフェイスが必要であるため、Cisco Cloud APIC は 2 つのインターフェイスを持つ VPN ゲートウェイのみをサポートします。



ルーティングポリシーとセキュリティポリシーの個別の構成

異なるVRFの2つのエンドポイント間の通信を許可するには、ルーティングポリシーとセキュリティ ポリシーを別々に確立する必要があります。

- **ルーティング ポリシー**：トラフィック フローを確立するルートを定義するために使用されるポリシー
- **セキュリティ ポリシー**：ゾーン分割ルール、セキュリティ グループ ルール、ACL など、セキュリティ目的で使用されるルール

Google Cloudの場合、ルーティングはセキュリティとは無関係に構成する必要があります。つまり、Google Cloudの場合、「契約」はセキュリティのためだけに使用されます。ルーティングを構成するには、VRF ルート リークを構成する必要があります。

ルーティング ポリシーの設定

VRF 間ルーティングを使用すると、独立したルーティング ポリシーを設定して、VRF のペア間でリークするルートを指定できます。ルーティングを確立するには、VRFのペア間にルートマップを設定する必要があります。

ルート マップを使用して、VRF のペア間でリークするルートを設定できる状況では、VRF 間ルーティングに次のタイプの VRF が使用されます。

- **[外部 VRF（External VRF）]** は、1 つ以上の外部ネットワークに関連付けられている VRF です。

- **内部 VRF** は、1 つ以上のクラウド コンテキスト プロファイルまたはクラウド サブネットが関連付けられているVRFです。

次のタイプの VRF で VRF 間ルーティングを設定する場合：

- 内部 VRF のペア間では、常にすべてのルートをリークする必要があります。
- 内部 VRF から外部 VRF へ、特定のルートまたはすべてのルートをリークできます。
- 外部 VRF から内部 VRF に、すべてのルートをリークする必要があります。

注意事項および制約事項

VRF 間ルーティングを使用してルートマップを使用して VRF ペア間のルートをリークする場合は、次の注意事項が適用されます。

- ルートは常に 2 つの VRF 間で双方向にリークされます。あるテナント/VRF から別のテナント/VRF へのルート リーク エントリごとに、対応するルート リーク エントリが反対方向に存在する必要があります。

  たとえば、2 つのテナント（`t1`と`t2`）と 2 つの対応する VRF（`v1` と`v2`）があるとします。VRF `t2:v2` のすべてのルート リーク エントリ `t1:v1` に対して、VRF `t1:v1` の対応するルート リーク エントリ `t2:v2` が必要です。

- 外部 VRF を外部ネットワークに関連付けた後、外部 VRF を変更する場合は、外部ネットワークを削除してから、新しい外部 VRF で外部ネットワークを再作成する必要があります。
- 「より大きな」プレフィックスがすでにリークされている間に、「より小さな」プレフィックスをリークするように設定することはできません。たとえば、10.10.0.0/16 プレフィックスがすでにリークされるように設定されている場合、10.10.10.0/24 プレフィックスの設定は拒否されます。同様に、0.0.0.0/0（すべてリーク）プレフィックスを設定した場合、他のプレフィックスは設定できません。

セキュリティ ポリシーの設定

Cisco Cloud APIC の EPG は AWS と Azure のセキュリティ グループに対応しますが、EPGに対する Google Cloud の対応コンポーネントはありません。Google Cloud で最も近いものは、ファイアウォール ルールとネットワーク タグの組み合わせです。

Google Cloudのファイアウォール技術情報は、プロジェクト（テナント）に対してグローバルです。ファイアウォール ルールは単一の VPC に関連付けられ、その範囲は VPC 全体にグローバルに適用されます。ファイアウォール ルールの範囲は、Target パラメータによってさらに定義されます。つまり、ルールが適用されるインスタンスのセットは、次の 1 つ以上のターゲット タイプによって選択できます。

- **[ネットワーク タグ**：ネットワークタグは、Google Cloud の VM のファイアウォールとルーティング構成を制御するキー文字列です。インスタンス（VM など）は、一意の文字列でタグ付けできます。ファイアウォール ルールは、等しいタグを持つすべてのインスタンス

に適用されます。複数のタグ値は論理「or」演算子として機能し、少なくとも 1 つのタグが一致する限りファイアウォール ルールが適用されます。

- **ネットワーク内のすべてのインスタンス**：ファイアウォールルールは VPC 内のすべてのインスタンスに適用されます。

ファイアウォール ルールは、トラフィックの送信元と宛先も識別します。ルールが入力トラフィック（VM に向かう）または出力トラフィック（VM を離れる）のどちらであるかによって、送信元フィールドと宛先フィールドの値は異なります。次のリストに、これらの値の詳細を示します。

- **入力ルール**：
  - **ソース**：次を使用して識別できます。
    - ネットワーク タグ
    - IP アドレス
    - 論理「or」演算子を使用した IP アドレスとネットワーク タグの組み合わせ
  - **宛先**：Target パラメータは、宛先インスタンスを識別します。
- **出力ルール**：
  - **送信元**：Target パラメータは、送信元インスタンスを識別します。
  - **宛先**：IP アドレスのみを使用して識別できます（ネットワーク タグは使用できません）。

Cisco Cloud APIC が Google Cloud でファイアウォール ルールを実装する方法

次のリストは、Cisco Cloud APIC の Google Cloud を使用したファイアウォールルールの実装方法を示しています：

- **グローバル 技術情報（Global resources）**：Google Cloud の VPC とファイアウォールはグローバル リソースであるため、Cisco Cloud APIC は複数のリージョンにまたがるエンドポイントのファイアウォールルールをプログラムする必要はありません。エンドポイントが存在するすべてのリージョンに同じファイアウォール ルールが適用されます。
- **ファイアウォール出力ルールとネットワーク タグ**：ファイアウォール出力ルールは、宛先フィールドとしてネットワーク タグをサポートしていないため、エンドポイントの個々の IP アドレスをリストする必要があります。
- **ファイアウォール入力ルールおよびエイリアス IP 範囲の送信元タグ**：ファイアウォール入力ルールには、送信元フィールドで使用されるネットワークタグに一致する VM のエイリアス IP 範囲は含まれません。
- **ファイアウォール ルールの優先度フィールド（Priority fields in firewall rules）**：Google Cloud は優先度の値に従ってファイアウォール ルールを評価します。

Google Cloud ファイアウォール ルールが優先順位リストの後に続く場合、Cisco Cloud APIC は VPC の作成時に、低プライオリティの deny-all 入力ルールと出力ルールのペアを構成します。その後、Cisco Cloud APIC は EPG の優先度の高い契約に従ってトラフィックを開くルールを構成します。したがって、EPGコントラクトの結果として特定のトラフィックを許可する明示的なルールがない場合は、優先順位の低いルールが一致し、デフォルトの動作はdeny-allになります。

エンドポイントおよびエンドポイント セレクタ

Cisco Cloud APIC では、クラウド EPG は、同じセキュリティ ポリシーを共有するエンドポイントの集合です。クラウド EPG は、1 つまたは複数のサブネット内にエンドポイントを持つことができ、VRF に関連付けられます。

Cisco Cloud APIC には、エンドポイントをクラウド EPG に割り当てるために使用される、エンドポイント セレクタと呼ばれる機能があります。エンドポイント セレクタは、基本的に言って、Cisco ACI によって管理される Google Cloud VPC に割り当てられたクラウド インスタンスに対して実行される一連のルールです。エンドポイント インスタンスに一致するエンドポイント セレクタ ルールは、そのエンドポイントをクラウド EPG に割り当てます。エンドポイント セレクタは、 Cisco ACI で使用可能な属性ベースのマイクロ セグメンテーションに似ています。

次に、2 種類のクラウド EPG で使用可能なエンドポイント セレクタのタイプを示します。

- **アプリケーション EPG**：
  - **IP**): IP アドレスまたはサブネットによって選択するために使用されます。
  - **リージョン**: エンドポイントのリージョンで選択するために使用されます。
  - **カスタム**：カスタム タグまたはラベルで選択するために使用されます。たとえば、Google Cloud のロケーション タグを追加する場合、Google Cloud で以前に追加したロケーション タグと一致するこのフィールドにカスタム タグのロケーションを作成できます。
- **外部 EPG**：

  サブネット：サブネット セレクタはエンドポイント セレクタのタイプで、一致表現ではサブネットの IP アドレスが使用されるため、サブネット全体が EPG の一部として割り当てられます。基本的に、サブネット セレクタをエンドポイント セレクタとして使用する場合、そのサブネット内のすべてのエンドポイントは関連付けられたEPGに属します。

Google Cloud で Cisco Cloud APIC エンドポイント セレクタを使用する場合、Google Cloud の一致する VM に EPG を関連付けるネットワーク タグが適用されます。ネットワーク タグが VM で設定されると、Google Cloud は VM のトラフィックにファイアウォール ルールが適用されます。

Google Cloud 上の VM もラベルをサポートします。ラベルは、組織的なツールとなるキーと値のペアです。Cisco Cloud APIC のカスタムエンドポイントセレクタは、 Google Cloud の VM に割り当てられたラベルを認識します。

Cisco Cloud APIC は、EPG ごとに一意のネットワーク タグ文字列を予約します。Google Cloud では、この値が EPG 用に作成されたファイアウォール ルールのターゲット フィールドとして使用されます。新しい VM が EPG のエンドポイント セレクタに一致すると、Cisco Cloud APIC はこの値を既存の VM のネットワーク タグに追加します。さらに、EPG のネットワークタグは、Google Cloud ファイアウォール ルールの送信元フィールドで使用されます。

次の設定の VPC に 3 つのエンドポイントがあると仮定すると、Cisco Cloud APIC は次のネットワーク タグを構成します。Cisco Cloud APIC-configured ネットワーク タグは次のフォーマットです。

`capic-<app-profile-name>-<epg-name>`

エンドポイント	アプリケーション プロファイル	EPG	Primary IP	ラベル	クラウド APIC で設定されたネットワーク タグ
EP1	最初のアプリケーション プロファイル（app01）	最初の EPG（epg01）	10.0.0.1	server:web	capic-app01-epg01
EP2	2 番目のアプリケーション プロファイル（app02）	2 番目の EPG（epg02）	20.0.0.1	server:backend	capic-app02-epg02
EP3	2 番目のアプリケーション プロファイル（app02）	3 番目の EPG（epg03）	30.0.0.1	server:database	capic-app02-epg03

Cisco Cloud APIC がネットワーク タグを設定するには、VMに対する管理者権限が必要です。この権限は、コンピューティング インスタンス管理者ロールによって付与されます。

Cisco Cloud APIC にこの権限がなく、VM のタグを管理できない場合があります。これらのシナリオでは、最初にVMでネットワークタグを設定し、その後で Cisco Cloud APIC に適切なエンドポイント セレクタ設定を指定できます。

ファイアウォール ルールを確認するには：

- **Google Cloud の場合**： Google Cloud アカウントで、**[VPC ネットワーク（VPC Network）]** > **[ファイアウォール（Firewall）]**に移動します。
  - VM が EPG の一部である場合は、ファイアウォール ルールを展開し、**[フィルタ（Filters）]** 列に表示される複数のエントリを表示することで、エンドポイントを検索できます。
  - **[タイプ（Type）]** 列のエントリを使用して、特定のファイアウォール ルールが入力ファイアウォール ルールか出力ファイアウォール ルールかを判別します。

- ファイアウォールルールが入力タイプの場合、トラフィックはこれらのエンドポイントに送信されます。
- ファイアウォールルールが出力タイプの場合、これらのエントリはトラフィックを受信できる場所を示します。

- **Cisco Cloud APIC の場合**：ファイアウォール ルールは VPC に関連付けられているため、**[クラウド リソース（Cloud Resources）]** > **[VPC]**に移動し、VPC をダブルクリックして詳細画面を表示します。次に、**[クラウド リソース（Cloud Resources）]** タブをクリックします。入力ルールと出力ルールが表示されます。

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。