Cisco Cloud APIC の概要

概要

Cisco Application Policy Infrastructure Controller（APIC）リリース 4.1(1) では、クラウドベースの仮想マシン（VM）に展開する Cisco APIC のソフトウェア展開である Cisco Cloud APIC が導入されています。リリース 4.1(1) は Amazon Web サービスをサポートします。リリース 4.2(x) 以降、Azure のサポートが追加されました。

展開した場合の Cisco Cloud APIC：

- Azure パブリッククラウドと対話するための既存の Cisco APIC と同様のインターフェイスを提供します
- クラウド構成の展開と構成を自動化します
- クラウド ルータ コントロール プレーンを設定します
- オンプレミス Cisco ACI ファブリックとクラウドサイト間のデータ パスを設定します
- Cisco ACI ポリシーをクラウド ネイティブ コンストラクトに変換します
- エンドポイントを検出します
- オンプレミスのデータセンターまたはパブリック クラウドの両方またはいずれかに展開されたワークロードに対して一貫したポリシー、セキュリティ、および分析を提供します

（注）
- Cisco Multi-Site は、MP-BGP EVPN 構成をオンプレミスのスパイン スイッチにプッシュします
- オンプレミス VPN ルーターには、IPsec の手動構成が必要です

- オンプレミスのデータセンターとパブリック クラウド間の自動接続を提供し、プロビジョニングとモニタリングを容易にします。
- ポリシーは Cisco Nexus Dashboard Orchestrator によってオンプレミスおよびクラウド サイトにプッシュされ、Cisco Cloud APIC はポリシーをクラウド ネイティブ コンストラクトに変換して、ポリシーをオンプレミス サイトと一致させます。

パブリック クラウドに Cisco ACI を拡張することの詳細については、『*Cisco Cloud APIC Installation Guide*』を参照してください。

Cisco Cloud APIC が稼働している場合は、Cisco Cloud APIC コンポーネントの追加と構成を開始できます。このドキュメントでは、Cisco Cloud APIC ポリシー モデルについて説明し、GUI および REST API を使用して Cisco Cloud APIC コンポーネントを管理 (追加、構成、表示、および削除) する方法について説明します。

overlay-2（セカンダリ）VRF の変更について

リリース 25.0(2) より前では、セカンダリ VRF である overlay-2 VRF は、Cisco Cloud APIC の起動時にインフラ テナントで暗黙的に作成され、overlay-2（セカンダリ）VRF でのみ Azure のサービスを作成する必要がありました。リリース 25.0(2) 以降、その制限は削除され、overlay-2 VRF は Cisco Cloud APIC の起動中にインフラ テナントで暗黙的に作成されなくなりました。

Cloud APIC または Nexus Dashboard Orchestrator（NDO）のいずれかで、この overlay-2（セカンダリ）VRF の特別な処理はありません。任意の名前で任意のセカンダリ VRF を作成し、インフラ VPC で `RsSubnetToCtx` を関連付け、Azure のこれらの任意のセカンダリ VRF にサービスを展開できます。いつでもセカンダリ VRF を作成でき、overlay-2 はリリース 25.0(2) 以降では単なるセカンダリ VRF です。

リリース 25.0(2) へのアップグレード時に、overlay-2 VRF を使用していた場合、それは引き続き存在し、ユーザが作成したセカンダリ VRF と同じように扱われます。引き続き、overlay-2 という名前のインフラまたはユーザ VPC でセカンダリ VRF を作成または削除することを選択できます。

このドキュメント全体で、「overlay-2 VRF」という用語のすべてのインスタンスは、より一般的な「セカンダリ VRF」という用語に変更されました。したがって、「セカンダリ VRF」という用語は、Cloud APIC が実行されているリリースに応じて、このドキュメントでは異なることを意味します。

- リリース 25.0(2) 以降 （3 ページ）

• リリース 25.0(1) 以前 （3 ページ）

リリース 25.0(2) 以降

Cloud APIC がリリース 25.0(2) 以降で実行されている場合、このドキュメントの「セカンダリ VRF」は、ユーザが作成したセカンダリ VRF である VRF を指します。前述のように、リリース 25.0(2) 以降で自動的に作成される一意の overlay-2 VRF はなくなりましたが、overlay-2 という名前のインフラまたはユーザ VPC でセカンダリ VRF を作成または削除することを選択できます。

リリース 25.0(1) 以前

Cloud APIC がリリース 25.0(1) 以前で実行されている場合、このドキュメントの「セカンダリ VRF」は、特に Cisco Cloud APIC の起動中にインフラ テナントで暗黙的に作成された overlay-2 VRF を指します。次の情報は、リリース 25.0(1) 以前用に自動的に作成される overlay-2（セカンダリ）VRF に特に適用されます。

インフラ ハブ サービス VRF（インフラ VNet の overlay-2 VRF）について

リリース 25.0(1) 以前の場合、overlay-2 VRF は、Cisco Cloud APIC の起動中にインフラ テナントに暗黙的に作成されます。クラウド サイトで使用されるインフラ サブネット（CCR およびネットワーク ロードバランサ用）と共有サービス用に展開されたユーザ サブネットの間でネットワーク セグメンテーションをそのまま維持するために、インフラ サブネットとユーザが展開したサブネットには異なる VRF が使用されます。

- **Overlay-1**：CCR、インフラ ネットワーク ロードバランサ、および Cisco Cloud APIC とともに、クラウド インフラのインフラ CIDR に使用されます。
- **Overlay-2**：ユーザ CIDR が共有サービスを展開するために使用され、インフラ VNet（Azure クラウドの overlay-1 VNet）のレイヤ 4 からレイヤ 7 サービス デバイスとともに使用されます。

CIDR が overlay-2（セカンダリ）VRF にマッピングされる方法は、リリースによって異なります。

- リリース 5.0(2) の場合、インフラ テナントでユーザが作成したすべての EPG は、インフラ VNet の overlay-2 VRF にのみマッピングできます。追加の CIDR とサブネットを既存のインフラ VNet（既存のインフラ クラウド コンテキスト プロファイル）に追加できます。これらは、インフラ VNet の overlay-2 VRF に暗黙的にマッピングされ、Azure クラウドの overlay-1 VNet に展開されます。
- 5.0(2) 以降のリリースでは、これは当てはまりません。インフラ テナントで、overlay-2 VRF を含む任意のセカンダリ VRF でクラウド EPG を作成できます。インフラ VNet で新しい CIDR を作成すると、それらの CIDR は overlay-2 VRF に暗黙的にマッピングされないため、新しい CIDR をセカンダリ VRF にマッピングするのはユーザの責任です。

リリース 5.0(2) より前では、特定のクラウド コンテキスト プロファイルは、特定の VNet のクラウド リソースにマップされていました。VNet のすべてのサブネットと関連するルート テーブルには、単一の VRF との 1 対 1 のマッピングがあります。リリース 5.0(2) 以降、インフラ

VNet のクラウド コンテキスト プロファイルは、複数の VRF（インフラ VNet の overlay-1 および overlay-2 VRF）にマッピングできます。

クラウドでは、サブネットのルート テーブルは、ネットワークの分離を実現するための最も詳細なエンティティです。したがって、overlay-1 VRF のすべてのシステム作成クラウドサブネットと、overlay-2 VRF のユーザ作成サブネットは、ネットワーク セグメンテーションを実現するためにクラウド内の個別のルート テーブルにマッピングされます。

（注） Azure クラウドでは、他の VNet とのアクティブなピアリングがある VNet で CIDR を追加または削除することはできません。したがって、インフラ VNet に CIDR を追加する必要がある場合は、最初にその中で VNet ピアリングを無効にする必要があります。これにより、インフラ VNet に関連付けられているすべての VNet ピアリングが削除されます。インフラ VNet に新しい CIDR を追加したら、インフラ VNet で VNet ピアリングを再度有効にする必要があります。

ハブ VNet の既存の CIDR に新しいサブネットを追加する場合は、VNet ピアリングを無効にする必要はありません。

外部ネットワーク接続

リリース 25.0(1) より前は、AWS と Cisco Cloud APIC の外部ネットワーク接続は、インフラ VNet の CCR からの EVPN 接続を使用することによってのみ利用可能でした。

リリース 25.0(1) 以降では、インフラ VNet CCR から IPSec/BGP を使用する任意の外部デバイスへの IPv4 接続もサポートされています。この IPSec/BGP 外部接続により、Cisco Cloud APIC をブランチ オフィスに接続できます。

次の項では、リリース 25.0(1) 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 は、クラウドに存在しない一意の VRF ですが、1 つ以上の外部ネットワークに関連付けられています。VNet をホストするために使用され、クラウド コンテキスト プロファイルに関連付けられている VRF である内部 VRF とは対照的に、外部 VRF は、Cisco Cloud APIC で使用されるどのクラウド コンテキスト プロファイルでも参照されません。

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、外部 VRF にルートをリークしたり、外部 VRF からルートを取得したりできます。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。

非 ACI 外部デバイスへの接続

リリース 25.0(1) では、既存の外部接続モデルが拡張され、AWS CCR から非 ACI 外部デバイスへの接続が提供されます。インフラ VNet CCR からこれらの非 ACI 外部デバイスへの IPv4 セッションが 外部 VRF で作成され、外部 VRF とサイト ローカル VRF の間で VRF 間ルーティングが設定されます。

このタイプの接続に関する注意事項と制限事項を次に示します。

- EVPN と IPv4 IPSec/BGP の両方を使用して、クラウドから同じリモート サイトに接続することはできません。

ガイドラインと制約事項

リリース 25.0(2) 以降、すべてのリージョンを手動で選択する代わりに、外部ネットワーク接続に対して `allRegion` を true に設定する必要があります。

サポートされているルーティングとセキュリティ ポリシーの概要

ルーティングとセキュリティ ポリシーは、Cisco Cloud APIC で実行しているリリースに応じて、異なる方法で処理されます。

ルーティングおよびセキュリティポリシー：リリース 25.0(1) 以前のリリース

リリース 25.0(1) より前のリリースでは、ルーティング ポリシーとセキュリティ ポリシーは緊密に結合されていました。EPG にまたがる 2 つのエンドポイント間の通信を許可するには、コントラクトを構成する必要があります。これらのコントラクトは、次の目的で使用されます。

- **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**：セキュリティ グループ ルール、ネットワーク セキュリティ ルールなど、セキュリティ目的で使用されるルール

つまり、コントラクトは本質的に、セキュリティ ポリシーとルーティング ポリシーの両方を構成するという 2 つの目的を果たします。つまり、コントラクトを破棄すると、許可するトラフィックと拒否するトラフィックを管理するセキュリティポリシーが破棄されるだけでなく、そのトラフィックのルーティングに使用されるポリシーも破棄されます。リリース 25.0(1) より前では、セキュリティポリシーを設定せずにルーティングポリシーを設定する方法はなく、その逆も同様です。

ルーティングおよびセキュリティ ポリシー: リリース 25.0(1)

リリース 25.0(1) 以降、セキュリティ ポリシーから独立して、ルーティングを個別に構成するためのサポートが利用できるようになりました。

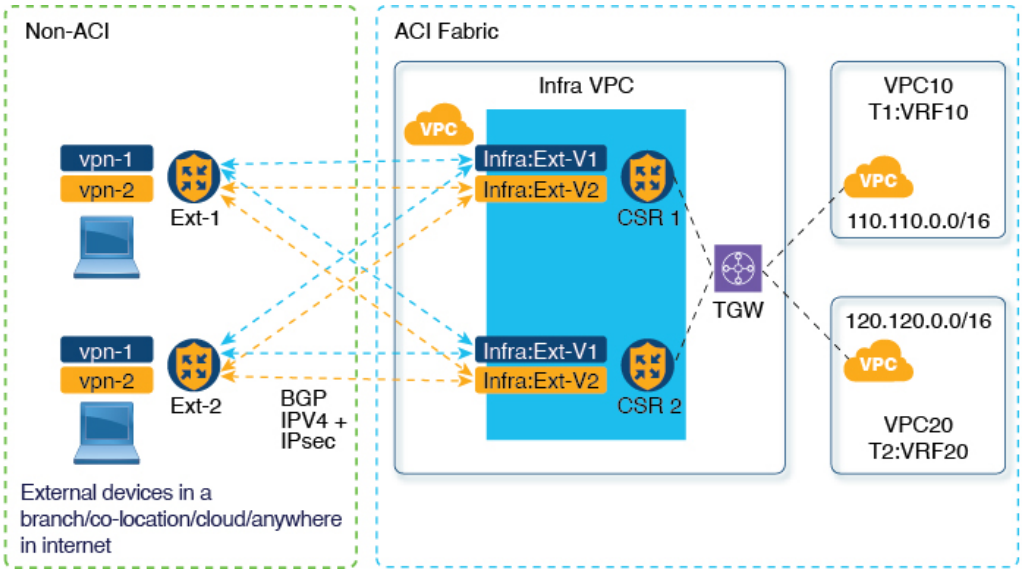
（注） このセクションで説明するルーティング ポリシーは、25.0(1) リリース専用であり、内部と 外部 VRF の間でのみ適用されます。 25.0(2) リリースでのルーティング ポリシーとセキュリティポリシーの変更については、ルーティング ポリシー: リリース 25.0(2) （8 ページ） を参照してください。

ルーティングおよびセキュリティ ポリシーを構成する手順は次のとおりです。

- **ルーティング ポリシー**: リリース 25.0(1) で導入された VRF 間ルーティング機能を使用して、ルーティング ポリシーを個別に設定します。これらの手順については、Cisco Cloud APIC GUI を使用した VRF間 ルート リークの設定 を参照してください。
- **セキュリティ ポリシー** : ルーティング ポリシーを構成した後、セキュリティ ポリシーを個別に構成するために以前に行ったように、引き続きコントラクトを使用します。
  - まず、外部 EPG を作成します。これらの手順については、Cisco Cloud APIC GUI を使用した外部 EPG の作成 を参照してください。
  - 次に、外部 EPG とクラウド EPG の間のコントラクトを作成します。これらの手順については、Cisco Cloud APIC GUI を使用したコントラクトの作成 を参照してください。

VRF 間ルーティングを使用すると、独立したルーティング ポリシーを構成して、次のタイプのサイト間のルーティングを設定するときに、内部のペアと外部 VRF の間でリークするルートを指定できます。

次の図は、この種の構成のトポロジ例を示しています。このトポロジ例は、ACI以外のサイトにある可能性のある外部デバイス (Ext-1) の背後にあるリモート エンドポイント (vpn-1) に接続する方法を示しています。この非ACIサイトは、ブランチ オフィス、同じ場所にあるサイト、クラウド サイト、または BGP IPv4 および IPSec の機能を備えたインターネット上の任意の場所である可能性があります。



この例では、infra:Ext-V1 はインフラ VNet の CCR 上の 外部 VRF にあり、リモート デバイスへの IPSec トンネルを介した BGP IPv4 セッションがあります。リモート エンドポイント ルートは、これらのセッションを介して infra:Ext-V1 VRF で受信され、図の右側に表示されている内部 VRF（たとえば、VNet10 の T1:VRF10）にリークされます。逆リーク ルートも設定されています。

ルート リークは、ルート マップを使用して内部 VRF と外部 VRF の間で発生します。Cisco Cloud APIC では、ルート マップを使用して、内部 VRF から外部 VRF へ および 外部 VRF から内部 VRF へのセキュリティ ポリシーとは独立したルーティング ポリシーを設定できます。内部 VRF のペア間のルーティングを設定するときに引き続きコントラクトを使用するため、内部 VRF 間のルーティング時に、ルーティング ポリシーとセキュリティ ポリシーが設定プロセスで結び付けられます。

次のリストは、**ルート マップ**を使用してセキュリティ ポリシーから独立してルーティング ポリシーを構成できる状況、およびルーティング ポリシーとセキュリティ ポリシーが結び付けられている**コントラクト**を使用する必要がある状況に関する詳細を示しています。

- コントラクトベースのルーティングを使用するルーティングの状況:
  - サイト内ルーティング（リージョン内およびリージョン間）
  - サイト間ルーティング（EVPN を使用したオンプレミスのクラウドから ACI）
  - クラウド間ルーティング
  - 内部 VRF 間のルート リーク
- ルート マップベースのルーティングを使用するルーティングの状況:
  - L3Out 外部 VRF を使用したクラウドから非 ACI オンプレミス サイトへ (EVPN なし)
  - 内部 VRF から 外部 VRF への特定のルートまたはすべてのルートをリークします。
  - 外部 VRF から内部 VRF への特定のルートまたはすべてのルートをリークする

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、内部 VRF と外部 VRF の間で双方向にリークされます。

  たとえば、内部 VRF (V1) と外部 VRF (Ext-V1) を持つユーザー テナント (t1) があるとします。ルート リークは、これらの VRF の両方に対して双方向に設定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。
- クラウド外部 EPG (cloudExtEpgs) 間の契約は許可されていません。
- 外部 VRF は、クラウド EPG の作成には使用できません。
- 外部 VRF は常にインフラ テナントに属します。
- 外部 VRF 間のリーク ルーティングはサポートされていません。

ルーティング ポリシー: リリース 25.0(2)

（注） このセクションで説明するルーティングおよびセキュリティ ポリシーは、25.0(2) リリース専用です。以前のリリースでのルーティング ポリシーとセキュリティ ポリシーの変更については、ルーティングおよびセキュリティ ポリシー: リリース 25.0(1) （6 ページ）を参照してください。

リリース 25.0(2) では、ルーティング ポリシーとセキュリティ ポリシーは、ルーティングおよびセキュリティ ポリシー: リリース 25.0(1) （6 ページ） で説明されているように引き続き分割されますが、特にルーティング ポリシーに次の変更が追加されています。

- 内部 VRF 間のルート リーク （8 ページ）
- グローバルな Inter-VRF ルート リーク ポリシー （9 ページ）
- ガイドラインと制約事項 （10 ページ）

内部 VRF 間のルート リーク

以前の 25.0(1) リリースでは、内部 VRF と外部 VRF のペア間でリークするルートを指定する独立したルーティング ポリシーを設定できる、VRF 間ルート マップベースのルーティング機能が導入されました。このルート マップ ベースのルーティング機能は、特に内部 VRF と外部 VRF の間に適用されます。内部 VRF のペア間のルーティングを設定する場合、ルーティング

およびセキュリティ ポリシー: リリース 25.0(1) （6 ページ）で説明されているように、その状況ではコントラクトベースのルーティングのみを使用できます。

リリース 25.0(2) 以降、内部 VRF のペア間でのルート マップベースのルート リークがサポートされるようになりました。次のいずれかのオプションを使用して、ルートをリークする方法を指定します。

- 次を使用して、VRF に関連付けられているすべての CIDRS または特定のサブネット IP アドレスをリークします。
  - GUI を介した **Leak All** オプション
  - REST API を介した `leakInternalPrefix` フィールド
- 次を使用して、VRF のペア間でリークします。
  - GUI による **サブネット IP** オプション
  - REST API を介した `leakInternalSubnet` フィールド

グローバルな Inter-VRF ルート リーク ポリシー

内部 VRF のペア間でのルート マップ ベースのルート リークのサポートに加えて、内部 VRF ルート リーク ポリシーでは、コントラクト ベースのルーティングまたは内部 VRF のペア間のルートマップベースのルーティングを使用するかどうかを選択することもできます。これは、初回セットアップで利用可能なグローバル モード構成であり、コントラクトベースまたはルートマップ ベースのモデルを可能にします。このグローバル モードでコントラクト ベース ルーティングを有効にすると、ルートマップがない場合にのみ、コントラクトを使用して内部 VRF のペア間のルートがリークされる可能性があることに注意してください。

このポリシーには、次の特性があります。

- このポリシーは、すべての内部 VRF に関連付けられています。
- これは、Cisco Cloud APIC が作成されたポリシーです。
- コントラクトベースのルーティングは、グリーンフィールドケースに対してデフォルトで無効になっています (オフになっています) (Cisco Cloud APIC に初めて構成する場合)。アップグレードの場合、リリース 25.0(2) より前に設定された Cisco Cloud APIC がある場合、コントラクトベースのルーティングが有効になります (オンになります)。

内部 VRF ルート リーク ポリシーは、インフラ テナントの First Time Setup 画面で設定されるグローバル ポリシーです。ここでは、ブール フラグを使用して、ルート マップがない場合にコントラクトがルートを駆動できるかどうかを示します。

- **オフ**: デフォルト設定。ルートはコントラクトに基づいて漏洩するのではなく、ルートマップに基づいて漏洩します。
- **オン**: ルート マップが存在しない場合、コントラクトに基づいてルートが漏洩します。有効に設定されている場合、ルートマップが構成されていないときに、ドライブ回送を契約します。ルート マップが存在するときに、ルート マップは常にドライブ回送です。

この Boolen フラグを前後に切り替えることができます。次に、このグローバル VRF ルート リーク ポリシーを切り替えるための一般的な推奨手順を示します。詳細な手順は、Cisco Cloud APIC GUI を使用した内部 VRF のリーク ルートの構成 で提供されています。

- EVPN を使用したマルチクラウドおよびハイブリッド クラウドの展開では、Cisco Cloud APICでコントラクトベースのルーティングを有効にする必要があります。
- EVPN を使用しないマルチクラウドおよびハイブリッドクラウドの展開の場合、ルーティングは、コントラクトではなくルート マップのみを介して実行されます。
- コントラクト ベースのルーティングからルート マップ ベースのルーティングに切り替える (**オフ**設定に切り替える) ことによってコントラクト ベースのルーティングを無効にする場合、**オフ**に設定する前にルートマップベースのルーティングが構成されていないと、このアクションは混乱を招く可能性があります。

  ルートマップベースのルーティングに切り替える前に、次の設定変更を行う必要があります。

  1. 既存のコントラクトを持つ VRF のすべてのペア間でルート マップ ベースのルート リークを有効にします。
  2. グローバル ポリシーでコントラクトベースのルーティング ポリシーを無効にします。

  その時点で、ルーティング ポリシーをルート マップ ベースのルーティングに変更できます。その後、新しいルート マップ ベースのルーティングで必要な粒度を反映するようにルーティングを変更できます。
- ルートマップベースのルーティングからコントラクトベースのルーティングに切り替える (**オン**設定に切り替える) ことでコントラクトベースのルーティングを有効にする場合は、コントラクトベースのルーティングに切り替える前に構成を変更する必要はありません。これは、この設定が追加操作であるためです。つまり、コントラクトベースとルートマップベースの両方のルーティングを、VRFのペア間で有効にすることができます。ルーティングを有効にする場合、ルート マップはコントラクトよりも優先されます。ルート マップベースのルーティングを有効にすると、コントラクトベースのルーティングの追加は中断がないようにしなければなりません。

ガイドラインと制約事項

次の注意事項および制約事項は、リリース 25.0(2) に適用されます。

- 外部 VRF と内部 VRF 間のルーティングでは、引き続きルート マップ ベースのルーティングのみが使用されます。
- レイヤ 4 からレイヤ 7 へのサービス挿入は引き続きコントラクトを介して行われるため、このような状況では、グローバル レベルでコントラクト ベースのルーティングを有効にする必要があります。
- Azureエキスプレス ルートとの外部接続では、引き続きコントラクトベースのルーティングが使用されます。

- leakExternalPrefix は、SSH を実行する外部 EPG 用に構成された外部エンドポイント セレクタと重複しないようにしてください。そうしないと、SSH が壊れます。この場合、プレフィックスは、Azure のインターネットへのデフォルトルートではなく、ネットワーク ロードバランサを指します。
- インターネット トラフィックをリモートサイトにリダイレクトする必要がない限り、leakInternalPrefix（Leak All、または 0.0.0.0/0）は使用しないでください。そうしないと、SSH が破損します。この場合、インターネットへのデフォルトルートは、ネットワーク ロードバランサを指す新しい UDR によって上書きされます。

トンネルのソース インターフェイスの選択

リリース 25.0(2) より前は、同じ宛先への IPsec トンネルは許可されていませんでした。リリース 25.0(2) 以降、異なる外部ネットワーク間で同じ宛先への複数のトンネルを持つことができます。これは、GUI でさまざまなソース インターフェイス (2、3、または 4) を使用するか、cloudtemplateIpseTunnlSourceInterface を使用して REST API を介して実行されます。

次の例は、インターフェイス 3 だけが発信元インターフェイスとして使用される状況を示しています。

```
<cloudtemplateIpSecTunnel peeraddr="173.36.19.2" preSharedKey="def" poolname="pool1">
    <cloudtemplateIpSecTunnelSourceInterface sourceInterfaceId=”3″ />
 </cloudtemplateIpSecTunnel>
```

次の例は、インターフェイス 2 と 3 の両方が発信元インターフェイスとして使用されている状況を示しています。

```
<cloudtemplateIpSecTunnel peeraddr="173.36.19.2" preSharedKey="def" poolname="pool1">
    <cloudtemplateIpSecTunnelSourceInterface sourceInterfaceId=”2″ />
    <cloudtemplateIpSecTunnelSourceInterface sourceInterfaceId=”3″ />
</cloudtemplateIpSecTunnel>
```

ガイドラインと制約事項

- インターフェイスの数を増やすと、トンネルの内部ローカル IP アドレスの需要が増加します。
- IPsec トンネル ソース インターフェイスの機能は、IKEv2 構成でのみサポートされます。

注意事項と制約事項

ここでは、Cisco Cloud APIC の注意事項と制限事項について説明します。

- クラウド CCR（クラウド ルータ）で VRF 間ルート リークを使用しているときに、オンプレミスとクラウドの間で複数の VRF をストレッチすることはできません。たとえば、EPG1 を持つ VRF1 が拡張され、EPG2 を持つ VRF2 も拡張される状況では、EPG1 は EPG2 とコ

ントラクトできません。ただし、クラウド内に複数のVRFを設定して、1つのオンプレミス VRF と 1 つ以上のコントラクトを共有することができます。

- クラウド上の CSR にアドバタイズするために、外部でアドバタイズされたオンプレミス サイトのブリッジ ドメイン サブネットを設定します。
- テナントのオブジェクトを設定する前に、古いクラウド リソース オブジェクトを確認します。アカウントを管理していた以前の Cisco Cloud APIC 仮想マシンから適切に消去されなかった場合、古い設定が存在する可能性があります。Cisco Cloud APIC は古いクラウド オブジェクトを表示できますが、削除することはできません。クラウドアカウントにログインし、手動で削除する必要があります。

（注） テナント サブスクリプション ID を追加した後、Cisco Cloud APIC が古いクラウド リソースを検出するには時間がかかります。

Azure では、1 つのテナントが所有する Azure アカウントを複数のテナントが共有できます。アカウントが複数のテナントで共有されている場合、所有者テナントのみが他のテナントの古いオブジェクトを表示できます。

古いクラウド リソースを確認するには、次の手順を実行します。

1. Cisco Cloud APIC GUI から、**[ナビゲーション（Navigation）] メニュー > [アプリケーション管理（Application Management）] > [テナント（Tenants）]**の順にクリックします。**[テナント（Tenants）]** サマリー テーブルは、テナントのリストとともに、サマリー テーブルの行として作業ペインに表示されます。
2. オブジェクトを作成するテナントをダブルクリックします。[概要（Overview）]、[クラウド リソース（Cloud Resources）]、[アプリケーション管理（Application Management）]、[統計（Statistics）]、および[イベント分析（Event Analytics）] タブが表示されます。
3. **[クラウド リソース（Cloud Resources）] > [アクション（Actions）] > [古いクラウド リソース（View Stale Cloud Objects）]** の順にクリックします。**[古いクラウド オブジェクト（Stale Cloud Objects）]** ダイアログボックスが表示されます。

- Cisco Cloud APIC は、作成した Azure リソースの管理を試みます。既存のリソースをインベントリとしてリストするのではなく、他のアプリケーションによって作成されたリソースの管理を試みません。同時に、Azure インフラ テナント サブスクリプションの Azure IAM ユーザ、および他のテナント アカウントが、Cisco Cloud APIC が作成するリソースを妨害しないことも期待されます。このため、Cisco Cloud APIC が Azure 上で作成するすべてのリソースには、次の 2 つのタグの少なくとも 1 つがあります。
  - AciDnTag
  - AciOwnerTag

Cisco Cloud APIC は VM、またはその他のリソースを作成、削除、または更新する権限を持つ Azure IAM ユーザが Cisco Cloud APIC によって作成および管理されるリソースへアクセスすることや変更することを防止する必要があります。このような制限は、インフラとその他のユーザのテナント サブスクリプションの両方に適用する必要があります。Azure サブスクリプション管理者は、上記の2つのタグを使用して、意図しないアクセスや変更を防ぐ必要があります。たとえば、次のようなアクセス ポリシーがある場合、Cloud APIC によって管理されているリソースへのアクセスを防止することができます。

```
{
  "properties": {
    "level": "CanNotDelete",
    "notes": "Optional text notes."
  }
}
```

- 共有 L3Out を構成する場合:
  - オンプレミスの L3Out とクラウド EPG をテナント共通にすることはできません。
  - オンプレミスの L3Out とクラウド EPG が異なるテナントにある場合は、テナント共通でコントラクトを定義します。オンプレミス サイトまたはクラウド テナントでコントラクトすることはできません。
  - オンプレミスの L3Out 外部 EPG（l3extInstP）でクラウド EPG の CIDR を指定します。
  - オンプレミスの L3Out が別の VRF のクラウド EPG とコントラクトしている場合、クラウド EPG が存在する VRF をオンプレミス サイトに拡張することはできず、オンプレミス サイトの他の VRF とコントラクトすることはできません。 。
  - オンプレミスの外部 EPG で外部サブネットを構成する場合:
    - 外部サブネットをゼロ以外のサブネットとして指定します。
    - 外部サブネットは、別の外部サブネットと重複できません。
    - クラウド EPG とコントラクトするには、共有ルート制御フラグを使用して外部サブネットをマークします。
  - オンプレミスの外部 EPG でマークされている外部サブネットは、L3Out のルーティング プロトコルを介して学習されているか、静的ルートとして作成されている必要があります。
- サポートされているスケールの合計については、次のサポートされているスケールの表を参照してください。

（注） サポートされているスケール表で指定されているスケールにより、合計 4 つの管理リージョンのみ所持できます。

表 *1:* サポートされるスケール

コンポーネント	サポートされている数
テナント	20
アプリケーション プロファイル	500
EPG	500
クラウド エンドポイント	1000
VRF	20
クラウド コンテキスト プロファイル	40
コントラクト	1000
サービスグラフ	200
サービス デバイス	100

Cisco Cloud APIC GUI の概要

Cisco Cloud APIC GUI は、関連するウィンドウのグループに分類されます。各ウィンドウでは、特定のコンポーネントにアクセスして管理できます。GUIの左側にある **[ナビゲーション（Navigation）]** メニューを使用して、ウィンドウ間を移動します。メニューのいずれかの部分にマウスを移動すると、**[ダッシュボード（Dashboard）]**、**[アプリケーション管理（Application Management）]**、**[クラウド リソース（Cloud Resources）]**、**[操作（Operations）]**、**[インフラストラクチャ（Infrastructure）]**、および**[管理（Administrative）]** タブのリストが表示されます。

各タブには異なるサブタブのリストが含まれており、各サブタブから異なるコンポーネント固有のウィンドウにアクセスできます。たとえば、EPG固有のウィンドウを表示するには、マウスを**[ナビゲーション（Navigation）]** メニューに合わせ、**[アプリケーション管理（Application Management）]** > **[EPGs]** をクリックします。そこから、**[ナビゲーション（Navigation）]** メニューを使用して別のコンポーネントの詳細を表示できます。たとえば、**[運用（Operations）]**> **[アクティブ セッション（Active Sessions）]** をクリックして、**EPG**から**[アクティブ セッション（Active Sessions）]** ウィンドウに移動できます。

[インテント（Intent）] メニュー バー アイコンを使用すると、GUI の任意の場所からコンポーネントを作成できます。たとえば、**[ルータ（Routers）]** ウィンドウの表示中にテナントを作成するには、**[インテント（Intent）]** アイコンをクリックします。検索ボックスとドロップダウン リストを含むダイアログが表示されます。ドロップダウン リストをクリックして**[アプリケーション管理（Application Management）]** を選択すると、**[テナント（Tenant）]** オプションを含むオプションのリストが表示されます。**[テナント（Tenant）]** オプションをクリックすると、テナントの作成に必要なフィールドのグループを示す**[テナントの作成（Create Tenant）]** ダイアログが表示されます。

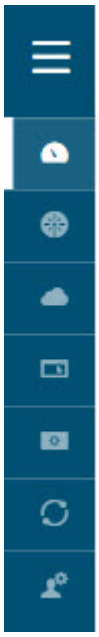
GUI アイコンの詳細については、Cisco Cloud APIC GUI アイコンについて （15 ページ） を参照してください。

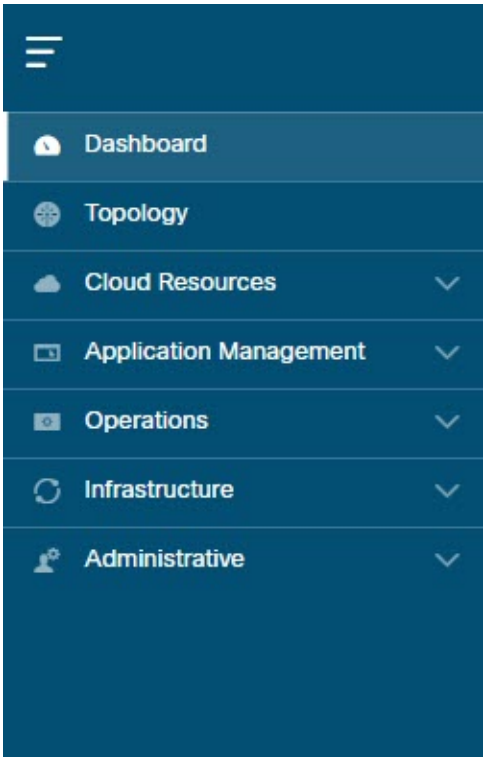
Cisco Cloud APIC コンポーネントの構成の詳細については、Cisco Cloud APIC コンポーネントの設定 を参照してください。

Cisco Cloud APIC GUI アイコンについて

ここでは、Cisco Cloud APIC GUI で一般的に使用されるアイコンの概要について説明します。

表 *2 : Cisco Cloud APIC GUI* アイコン

アイコン	説明
図 *1 :* ナビゲーション ペイン（折りたたみ） 	GUI の左側には **ナビゲーション** ウィンドウがあり、折りたたんだり展開したりします。ペインを展開するには、マウスアイコンをマウスオーバーするか、上部のメニューアイコンをクリックします。メニュー アイコンをクリックすると、**ナビゲーション** ペインが開いた位置でロックされます。折りたたむには、メニュー アイコンをもう一度クリックします。メニュー アイコンの上にマウスのアイコンを重ねて**ナビゲーション** ウィンドウを展開すると、**ナビゲーション** ウィンドウはマウス アイコンから移動して折りたたまれます。 展開すると、**ナビゲーション** ウィンドウにタブのリストが表示されます。各タブをクリックすると、Cisco Cloud APIC コンポーネント ウィンドウ間を移動できる一連のサブタブが表示されます。

アイコン	説明
図 *2:* ナビゲーション ウィンドウ（展開） 	Cisco Cloud APIC コンポーネント ウィンドウは、**ナビゲーション** ウィンドウで次のように構成されています。 • **[ダッシュボード（Dashboard）]** タブ：Cisco Cloud APIC コンポーネントに関する概要情報を表示します。 • **[トポロジ（Topology）]** タブ：Cisco Cloud APIC に関するトポロジ情報を表示します。 • **[クラウド リソース（Cloud Resources）]** タブ： リージョン、VNET、ルータ、セキュリティ グループ（アプリケーション セキュリティ グループ/ネットワーク グループ）、エンドポイント、インスタンス、クラウド サービス（およびターゲット グループ）に関する情報を表示します。 • **[アプリケーション管理（Application Management）]** タブ：テナント、アプリケーション プロファイル、EPG、コントラクト、フィルタ、VRF、サービス グラフ、デバイス、およびクラウド コンテキスト プロファイルに関する情報を表示します。 • **[操作（Operations）]** タブ：イベント分析、アクティブ セッション、バックアップおよび復元ポリシー、テクニカル サポート ポリシー、ファームウェア管理、スケジューラ、およびリモート ロケーションに関する情報が表示されます。 • **[インフラストラクチャ（Infrastructure）]** タブ： システム設定、リージョン間接続、およびオンプレミス接続に関する情報が表示されます。、 • **[管理（Administrative）]** タブ：認証、イベント分析、セキュリティ、ローカルおよびリモート ユーザー、およびスマート ライセンスに関する情報が表示されます。 （注） これらのタブの内容の詳細については、システムの詳細の表示 を参照してください。
図 *3:* 検索メニュー バー アイコン 	**[検索（Search）]** メニュー バー アイコンは、検索フィールドを表示します。このフィールドを使用すると、名前またはその他の特徴的なフィールドでオブジェクトを検索できます。

アイコン	説明
図 *4*：インテント メニュー バー アイコン 	メニュー アイコンの **検索** アイコンと**フィードバック**アイコンの間に、**[インテント（Intent）]**アイコンが表示されます。 クリックすると、**[インテント（Intent）]** ダイアログが表示されます（以下を参照）。**[インテント（Intent）]** ダイアログでは、Cisco Cloud APIC GUI の任意のウィンドウからコンポーネントを作成できます。コンポーネントを作成または表示すると、ダイアログボックスが開き、**[インテント（Intent）]** アイコンが非表示になります。**[インテント（Intent）]** アイコンに再度アクセスするには、ダイアログボックスを閉じます。 コンポーネントの作成の詳細については、Cisco Cloud APIC コンポーネントの設定 を参照してください。
図 *5*：*[インテント（Intent）]*ダイアログボックス 	**[インテント（Intent）]**（何をしたいか？）ダイアログ ボックスには、検索ボックスとドロップダウン リストがあります。ドロップダウン リストを使用すると、特定のオプションを表示するためのフィルタを適用できます。検索ボックスでは、フィルタリングされたリストを検索するためのテキストを入力できます。
図 *6*：フィードバック アイコン 	**フィードバック** アイコンは、メニューバーの**インテント** アイコンと**ブックマーク** アイコンの間に表示されます。 クリックすると、**フィードバック**パネルが表示されます。
図 *7*：ブックマーク アイコン 	**ブックマーク** アイコンは、**フィードバック**と**システム ツール** アイコンの間にあるメニュー バーに表示されます。 クリックすると、現在のページがシステム上でブックマークされます。
図 *8*：システム ツール メニュー バー アイコン 	**システム ツール**のメニュー バー アイコンには、次のオプションがあります。 • **概要（About）**：Cisco Cloud APIC のバージョンを表示します。 • **オブジェクト ストア ブラウザ**—管理対象オブジェクト ブラウザ (バイザー) を開きます。これは Cisco Cloud APIC に組み込まれているユーティリティで、管理対象オブジェクトを (MO) をブラウザによりグラフィカルに表示します。

アイコン	説明
図 *9 :* ヘルプ メニュー バー アイコン 	**[ヘルプ（Help）]** メニュー バー アイコンには、**[クラウド APIC について（About Cloud APIC）]** メニュー オプションが表示され、クラウド APIC のバージョン情報が提供されます。**[ヘルプ（Help）]** メニュー バー アイコンには、**[ヘルプ センター（Help Center）]**および **[ようこそ画面（Welcome Screen）]** メニュー オプションも表示されます。
図 *10 : [*ユーザー プロファイル（***User Profile***）*]*メニュー バー アイコン 	**ユーザー プロファイル** のメニュー バー アイコンには、次のオプションがあります。 • **[ユーザー設定（User Preferences）]** : 時刻形式（ローカルまたは UTC）を設定し、ログイン時にウェルカム画面を有効または無効にすることができます。 • **[パスワードの変更（Change Password）]** : パスワードを変更できます。 • **[SSH キーの変更（Change SSH Key）]** : SSH キーを変更できます。 • **[ユーザー証明書の変更（Change User Certificate）]** : ユーザー証明書を変更できます。 • **[ログアウト（Logout）]** : GUI からログアウトできます。

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。