共有サービス

この章で説明する内容は、次のとおりです：

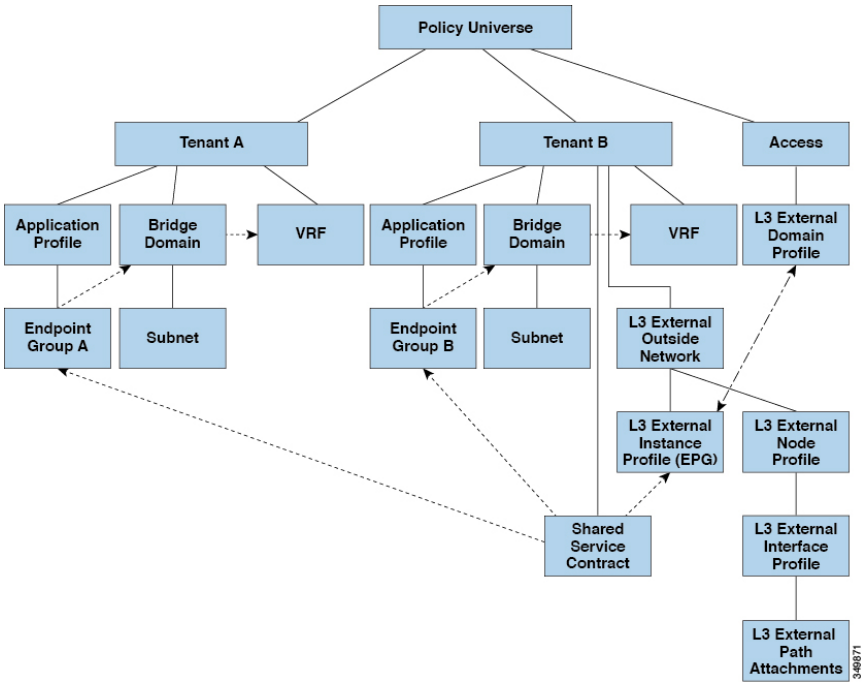
共有レイヤ 3 Out

共有レイヤ 3 アウトサイド（L3Out または `l3extOut`）構成は、外部ネットワークへのルーテッド接続を、VRF インスタンス間またはテナント間の共有サービスとして提供します。L3Out の外部 EPG インスタンス プロファイル（外部 EPG または `l3extInstP`）は、ルーティングの観点とコントラクトの観点の両方から共有できるルートを制御するための構成を提供します。外部 EPG 下のコントラクトは、これらのルートをリークする必要がある VRF インスタンスまたはテナントを決定します。

L3Out は、任意のテナント（*[*ユーザー（*user*）*]*、`[共通（common）]`、`[インフラ（Infra）]`、または `[管理（mgmt）]`）の共有サービスとしてプロビジョニングできます。任意のテナントの EPG は、外部 EPG がファブリック内のどこにプロビジョニングされているかには関係なく、共有サービス コントラクトを使用して、外部 EPG に接続できます。これにより、外部ネットワークへのルーテッド接続のプロビジョニングが簡単になります。複数のテナントが、外部ネットワークへのルーテッド接続用に単一の外部 EPG を共有できます。外部 EPG を共有すると、単一の共有外部 EPG を使用する EPG の数には関係なくスイッチ上で使用されるセッションは 1 つのみであるため、より効率的になります。

次の図は、共有外部 EPG 用に構成された主なポリシー モデル オブジェクトを示しています。

図 *1*: 共有 *L3Out* ポリシー モデル



共有 L3Out ネットワーク構成については、以下の注意事項と制限事項に注意してください：

- テナント制限なし：テナント A と B は、任意の種類のテナント（*[*ユーザー（*user*）*]*、[共通（common）]、[インフラ（Infra）]、[管理（mgmt）]）です。共有外部 EPG が [共通（common）] テナントにある必要はありません。
- EPG の柔軟な配置：上の図の EPG A と EPG B は異なるテナントにあります。EPG A と EPG B で同じブリッジ ドメインと VRF インスタンスを使用することはできますが、それは必須ではありません。EPG A と EPG B は異なるブリッジ ドメインおよび異なる VRF インスタンスにありますが、同じ外部 EPG を共有しています。
- サブネットは *[*プライベート（*private*）*]*、*[*パブリック（*public*）*]*、または *[*共有（*shared*）*]* である可能性があります。L3Out のコンシューマまたはプロバイダ EPG にアドバタイズされるサブネットは、*[*共有（*shared*）*]* に設定されている必要があります。L3Out にエクスポートされるサブネットは *[*パブリック（*public*）*]* に設定される必要があります。
- 共有サービス コントラクトは、共有 L3Out ネットワーク サービスを提供する外部 EPG が含まれているテナントからエクスポートされます。共有サービス コントラクトは、共有サービスを使用する EPG が含まれているテナントにインポートされます。
- 共有 L3Out では禁止コントラクトを使用しないでください。この構成はサポートされません。
- 外部 EPG は、共有サービス プロバイダーとしてサポートされますが、非外部 EPG コンシューマと組み合わせる場合に限られます（L3Out EPG が外部 EPG と同じ）。

- トラフィック中断（フラップ）：外部 EPG を、外部サブネット 0.0.0.0/0 を使用して構成し、外部 EPG サブセットのスコープ プロパティを共有ルート制御（*shared-rctrl*）または共有セキュリティ（*shared-security*）に設定すると、VRF インスタンスはグローバル pcTag を使用して再配置されます。これにより、その VRF インスタンス内のすべての外部トラフィックが中断されます（VRF インスタンスがグローバル pcTagを使用して再配置されるため）。
- 共有レイヤ L3Out のプレフィックスは一意である必要があります。同じ VRF インスタンスの同じプレフィックスを使用した、複数の共有 L3Out 構成は動作しません。VRF インスタンスにアドバタイズする外部サブネット（外部プレフィックス）が一意であることを確認してください（同じ外部サブネットが複数の外部EPGに属することはできません）。prefix1 付きの L3Out 構成（たとえば、 L3Out1と呼ばれます) と同じ VRF インスタンスに属する prefix1 付きの 2 番目の L3Out 構成（たとえば、 L3Out2と呼ばれます）は、機能しません。（導入される pcTag が 1 つだけであるため）。
- L3Out の異なる動作が、同じ VRF インスタンスの同じリーフ スイッチ上に構成される場合があります。考えられるシナリオは次の 2 つです：
  - シナリオ 1 は、SVI インターフェイスおよび 2 つのサブネット（10.10.10.0/24 および 0.0.0.0/0）が定義された L3Out がある場合です。L3Out ネットワーク上の入力トラフィックが、マッチング プレフィックス 10.10.10.0/24 を持っていると、入力トラフィックは外部 EPG pcTag を使用します。L3Out ネットワーク上の入力トラフィックが、マッチング デフォルト プレフィックス 0.0.0.0/0 を持っていると、入力トラフィックは外部ブリッジ pcTag を使用します。
  - シナリオ 2 は、2 つのサブネット（10.10.10.0/24 および 0.0.0.0/0）が定義されたルーテッドまたはルーテッドサブインターフェイスを使用する L3Out がある場合です。L3Out ネットワーク上の入力トラフィックが、マッチング プレフィックス 10.10.10.0/24 を持っていると、入力トラフィックは外部 EPG pcTag を使用します。L3Out ネットワーク上の入力トラフィックが、マッチング デフォルト プレフィックス 0.0.0.0/0 を持っていると、入力トラフィックは VRF インスタンス pcTag を使用します。
  - ここまでで説明した動作の結果として、同じ VRF インスタンスおよび同じリーフ スイッチに、SVI インターフェイスを使用する L3Out-A および L3Out-B が構成されている場合、次のユース ケースが考えられます：

    ケース 1 は L3Out-A用です：この外部ネットワーク EPG には、10.10.10.0/24 および 0.0.0.0/1 という 2 つのサブネットが定義されています。 L3Out-A 上の入力トラフィックは、マッチング プレフィックス 10.10.10.0/24 を持つ場合、これは、外部 EPG pcTag と contract-Aを使用します。これは、 L3Out-Aと関連付けられています。 L3Out-A の出力トラフィックで特定のマッチが見つからない場合でも、0.0.0.0/1 との最大プレフィックス マッチがあるので、外部ブリッジ ドメイン pcTag と contract-Aを使用します。

    ケース 2は L3Out-B用です：この外部 EPG では、1 つのサブネット 0.0.0.0/0 が定義されています。 L3Out-B の入力通信が一致するプレフィックス 10.10.10.0/24（ L3Out-A で定義されています）を持つ場合、これは、 L3Out-A および contract-Aの外部 EPG pcTag を使用します。これは、 L3Out-Aと関連付けられています。 contract-Bを使用しません。これは、 L3Out-Bと関連付けられています。

- 許可されないトラフィック：無効な構成で、共有ルート制御（shared-rtctrl）に対する外部サブネットのスコープが、共有セキュリティ（shared-security）に設定されているサブネットのサブセットとして設定されている場合、トラフィックは許可されません。たとえば、以下の設定は許可されません：
  - *shared rtctrl*：10.1.1.0/24、10.1.2.0/24
  - *shared security*: 10.1.0.0/16

  この場合、10.1.1.0/24 および 10.1.2.0/24 の各プレフィックスがドロップ ルールを使用してインストールされているため、宛先 IP 10.1.1.1 を使用して非境界リーフの入力トラフィックはドロップされます。トラフィックは許可されません。このようなトラフィックは、`shared-rtctrl` プレフィックスを共有セキュリティ プレフィックスとしても使用するように構成を修正することで有効にできます。
- 不注意によるトラフィック フロー：次の設定シナリオを避けることで、不注意によるトラフィック フローを予防します：
  - **ケース 1** 構成の詳細
    - VRF1 との L3Out ネットワーク構成（たとえば、 `L3Out-1`と名付けられた) は、`provider1`と呼ばれます。
    - VRF2 を使用する 2 番目の L3Out ネットワーク構成（例えば `L3Out-2`と名付けられた）は `provider2`と呼ばれます。
    - `L3Out-1` の VRF1 は、デフォルト ルート、0.0.0.0/0 をインターネットにアドバタイズします。これは *shared-rtctrl* および *shared-security*の両方を有効にします。
    - `L3Out-2` の VRF2 は特定のサブネット、192.0.0.0/8 を DNS および NTP にアドバタイズし、 *shared-rtctrl*を有効にします。
    - `L3Out-2` の VRF2 には特定のサブネット、192.1.0.0/16 があります。これは *shared-security*を有効にします。
    - **[バリエーション A（Variation A）]**：EPG トラフィックは複数の VRF インスタンスに向かいます。
      - EPG1 と `L3Out-1` の間の通信は、 *allow_all* 契約によって規制されています。
      - EPG1 と `L3Out-2` の間の通信は、 *allow_all* 契約によって規制されています。

      [結果（Result）]：EPG1 から `L3Out-2` へのトラフィックも 192.2.xx に移動します
    - **[バリエーション B（Variation B）]**：EPG は 2 番目の共有 L3Out ネットワークの *allow_all* に準拠します。
      - EPG1 と `L3Out-1` の間の通信は、 *allow_all* 契約によって規制されています。
      - EPG1 と `L3Out-2` の間の通信は、 *allow_icmp* 契約によって規制されています。

[結果（Result）]：EPG1 から `L3Out-2` へそして192.2.xx へのトラフィックは、*allow_all* 契約に準拠します。

- **ケース 2** 構成の詳細：
  - 外部 EPG は、1 つの共有プレフィックスと、その他の非共有プレフィックスを持っています。
  - `src = non-shared` 付きの着信トラフィックは、EPG にアクセスできます。
    - **[バリエーション A（Variation A）]**：意図しないトラフィックが EPG を通過します。

      外部 EPG トラフィックは、次のプレフィックスを持つ L3Out を通過します。

      Unordered List bullet 5 `192.0.0.0/8 = import-security, shared-rtctrl`

      Unordered List bullet 5 `192.1.0.0/16 = shared-security`

      Unordered List bullet 5 EPG は、 `1.1.0.0/16 = shared`を持ちます。

      [結果（Result）]：192.2.x.x からのトラフィックも EPG に向かいます。

    - **[バリエーション B（Variation B）]**：意図しないトラフィックが EPG を通過します。共有 L3Out に到達したトラフィックは EPG を通過できます。

      Unordered List bullet 5 共有 L3Out VRF インスタンスは、 `pcTag = prov vrf` 付きの EPG を持ち、契約は、 *allow_all*に設定されています。

      Unordered List bullet 5 EPG `<subnet> = shared`です。

      [結果（Result）]：レイヤ 3 Out に到達するトラフィックは EPG を通過することができます。

レイヤ 3 アウトからレイヤ 3 アウト内部 VRF への漏洩

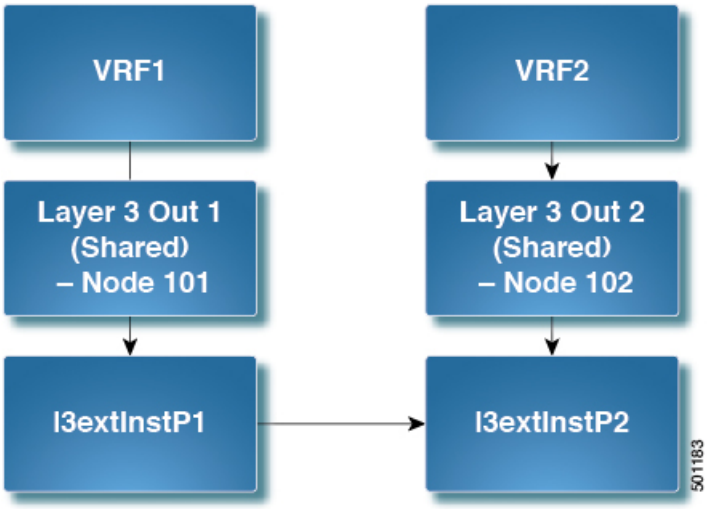
Cisco APIC リリース 2.2（2e）から、2 つの異なる VRF に 2 個のレイヤ 3 アウトがある場合、VRF 内部の漏洩がサポートされています。

この機能を稼働するには、次の条件を満たす必要があります。

- 2 個のレイヤ 3 アウト間にはコントラクトが必要です。
- レイヤ3アウトの接続したり移行したりするサブネットのルートは、コントラクトを適用し（L3Out-L3Outおよび L3Out-EPG）、VRF 間の動的または静的ルートを漏洩させることなく漏洩します。
- 動的または静的ルートは、コントラクトを適用し（L3Out-L3Out および L3Out-EPG）、VRF 間で直接接続したり移行したりするルートをアドバタイズすることなく漏洩します。
- 異なる VRF の共有のレイヤ 3 アウトは相互に通信できます。
- ブリッジ ドメインに必要な関連付けられた L3Out はありません。VRF 間共有 L3Out を使用する場合は、テナント 共通の L3Out にユーザー テナント ブリッジ ドメインを関連付ける必要はありません。テナント固有の L3Out がある場合、それぞれのテナントのブリッジ ドメインに関連付けられます。
- 2 個のレイヤ 3 アウトは異なる 2 個の VRF に存在し、正常にルートを交換できます。
- この強化は、アプリケーション EPG およびレイヤ 3 アウト内部 VRF 間の通信と同じです。唯一の違いは、アプリケーション EPG ではなく別のレイヤ 3 アウトが存在します。したがってこの状況では、コントラクトは 2 個のレイヤ 3 アウト間で記録されます。

次の図では、共有サブネットによる 2 個のレイヤ 3 アウトが存在します。両方の VRF でレイヤ 3 外部インスタンス プロファイル（l3extInstP）間のコントラクトがあります。この場合、VRF 1 の共有レイヤ 3 アウト は VRF 2 の共有レイヤ 3 と通信できます。

図 *2 : 2* 個の *VRF* 間で通信する共有レイヤ *3* アウト



拡張 GUI を使用した共有レイヤ 3 Out VRF 間リーキングの設定

始める前に

コンシューマとプロバイダーによって使用される契約ラベルがすでに作成されています。

手順

ステップ 1 メニューバーで、**[テナント（Tenants）]** > **[テナントの追加（Add Tenant）]**を選択します。

ステップ 2 **[テナントの作成（Create Tenant）]** ダイアログボックスに、プロバイダーのテナント名を入力します。

ステップ 3 **[VRF名（VRF Name）]** フィールドに、プロバイダーのVRF名を入力し、**[送信（Submit）]** をクリックしてテナントを作成します。

ステップ 4 **[ナビゲーション（Navigation）]** ペインの新しいテナント名の下で **[L3Out（L3Outs）]**に移動します。

ステップ 5 **[L3Out（L3Outs）]** を右クリックして、**[L3Outの作成（Create L3Out）]**を選択します。

[L3Outの作成（Create L3Out）] ウィザードが表示されます。

ステップ 6 **[L3Outの作成（Create L3Out）]** ダイアログボックスで、次の操作を実行します：

a) **[名前（Name）]** フィールドに L3Out の名前を入力します。

b) **[VRF]** フィールドで、前に作成した VRF を選択します。

c) **[L3ドメイン（L3 Domain）]** フィールドで、L3 ドメインを選択します。

d) プロトコルに適切な選択を行い、**[次へ（Next）]**をクリックします。

ステップ 7 **[外部 EPG（External EPG）]** ウィンドウが表示されるまで、次のウィンドウで必要な選択を行います。

[ノードとインターフェイス（Nodes and Interfaces）] ウィンドウと **[プロトコル（Protocols）]** ウィンドウが表示される場合があります。これは、**[識別（Identity）]** ウィンドウで選択したプロトコルによって

いずれかが表示されます。 **[L3Outの作成（Create L3Out）]** ウィザードの最後のウィンドウは、 **[外部 EPG（External EPG）]** ウィンドウです。

ステップ 8 **[外部 EPG（External EPG）]** ウィンドウで次のアクションを実行します：

a) **[名前（Name）]** フィールドに、外部ネットワーク名を入力します。

b) **[すべての外部ネットワークのデフォルト EPG（Default EPG for all external network）]** チェック ボックスをオフにします。

[サブネット（Subnets）] フィールドが表示されます。

c) **[+]** をクリックして **[サブネットの作成（Create Subnet）]** ウィンドウにアクセスします。

d) **[サブネットの作成（Create Subnet）]** ダイアログ ボックスで **[IP アドレス（IP Address）]** フィールドに、一致する IP アドレスを入力します。 **[OK]**をクリックします。

e) **[終了（Finish）]** をクリックします。これは、 **[L3Outの作成（Create L3Out）]** ウィザードにあります。

ステップ 9 **[ナビゲーション（Navigation）]** ペインで、作成した ***[L3Out_name]*** > **[外部 EPG（External EPGs）]** > ***[ExternalEPG_name]*** に移動します。

ステップ 10 **[作業（Work）]** ペイン（外部ネットワークの **[プロパティ（Properties）]** の下）で、解決された VRF が **[解決された VRF（Resolved VRF）]** フィールドに表示されていることを確認します。

ステップ 11 外部サブネットの IP アドレスをダブルクリックして、 **[サブネット（Subnet）]** ダイアログ ボックスを開きます。

ステップ 12 **[範囲（Scope）]** フィールドで、必要なチェック ボックスをオンにして、OK をクリックします。 **[送信（Submit）]**をクリックします。

このシナリオで、次のチェック ボックスをオンにします：

- **[外部 EPG の外部サブネット（External Subnets for the External EPG）]**
- **[共有ルート コントロール サブネット（Shared Route Control Subnet）]**
- **[共有セキュリティ インポート サブネット（Shared Route Control Subnet）]**

ステップ 13 事前に作成した **[L3 外部（L3 Outside）]** に移動します。

ステップ 14 **[プロバイダー ラベル（Provider Label）]** フィールドに、このタスクを開始するための前提条件として作成したプロバイダ名を入力します。 **[送信（Submit）]**をクリックします。

ステップ 15 メニュー バーで、 **[テナント（Tenants）]** > **[テナントの追加（Add Tenant）]**をクリックします。

ステップ 16 **[テナントの作成（Create Tenant）]** ダイアログ ボックスで、L3 コンシューマのためのテナント名を入力します。

ステップ 17 **[VRF 名（VRF name）]** フィールドに、コンシューマの VRF 名を入力します。

ステップ 18 **[ナビゲーション（Navigation）]** ペインの新しいテナント名の下で、コンシューマ向けの **[L3Out（L3Outs）]** に移動します。

ステップ 19 **[L3Out（L3Outs）]** を右クリックして、 **[L3Outの作成（Create L3Out）]**を選択します。

[L3Outの作成（Create L3Out）] ウィザードが表示されます。

ステップ 20 **[L3Outの作成（Create L3Out）]** ダイアログボックスで、次の操作を実行します：

a) **[名前（Name）]** フィールドに L3Out の名前を入力します。
b) **[VRF]** フィールドで、ドロップダウン メニューから、コンシューマのために作成された VRF を選択します。
c) **[コンシューマ ラベル（Consumer Label）]** フィールドに、コンシューマ ラベルの名前を入力します。
d) **[L3 ドメイン（L3 Domain）]** フィールドで、L3 ドメインを選択します。
e) プロトコルに適切な選択を行い、 **[次へ（Next）]**をクリックします。

ステップ 21 **[外部 EPG（External EPG）]** ウィンドウが表示されるまで、次のウィンドウで必要な選択を行います。

[ノードとインターフェイス（Nodes and Interfaces）] ウィンドウと **[プロトコル（Protocols）]** ウィンドウが表示される場合があります。これは、**[識別（Identity）]** ウィンドウで選択したプロトコルによっていずれかが表示されます。 **[L3Outの作成（Create L3Out）]** ウィザードでの最後のウィンドウは、 **[外部 EPG（External EPG）]** ウィンドウです。

ステップ 22 **[外部 EPG（External EPG）]** ウィンドウで次のアクションを実行します：

a) **[名前（Name）]** フィールドに、外部ネットワーク名を入力します。
b) **[すべての外部ネットワークのデフォルト EPG（Default EPG for all external network）]** チェックボックスをオフにします。

[サブネット（Subnets）] フィールドが表示されます。

c) **[+]** をクリックして **[サブネットの作成（Create Subnet）]** ウィンドウにアクセスします。
d) **[サブネットの作成（Create Subnet）]** ダイアログ ボックスで **[IP アドレス（IP Address）]** フィールドに、一致する IP アドレスを入力します。 **[OK]**をクリックします。
e) **[範囲（Scope）]** フィールドで、必要なチェック ボックスをオンにして、 **[OK]**をクリックします。

このシナリオで、**[共有ルート コントロール サブネット（Shared Route Control Subnet）]** および **[共有セキュリティ インポート サブネット（Shared Route Control Subnet）]**のチェックボックスをオンにします。

f) **[終了（Finish）]** をクリックします。これは、 **[L3Outの作成（Create L3Out）]** ウィザードにあります。

これで、共有レイヤ 3 Out VRF 間リーキングの構成は完了です。

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。