共有サービス

この章は、次の内容で構成されています。

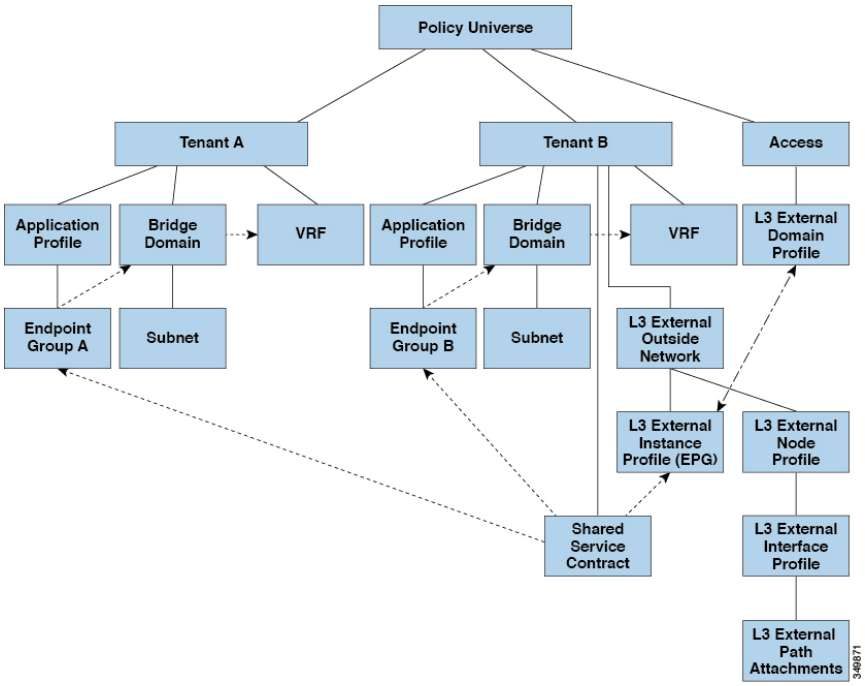
共有レイヤ 3 Out

共有レイヤ 3 アウトサイド ネットワーク(L3extOut)は、外部ネットワークへのルーテッド接続を共有サービスとして提供します。L3extOut プロファイル（l3extInstP)）EPG は、外部ネットワークへのルーテッド接続を提供します。これは、任意のテナント（*user*、common、infra、mgmt.）の共有サービスとしてプロビジョニングできます。リリース 1.2(1x) より前では、この設定は *user* テナントと common テナントでのみサポートされていました。任意のテナントの EPG が、l3extInstP 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その l3extInstP 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 l3extInstP EPG を共有できます。l3extInstP EPG を共有すると、単一の共有 l3extInstP 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。

（注） l3extInstP EPG 共有サービス コントラクトを使用するすべてのスイッチは、APIC 1.2（1x）およびスイッチ 11.2（1x）の各リリース以降で使用可能なハードウェアおよびソフトウェアのサポートを必要とします。詳細については、「*Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*」 とリリース ノート ドキュメントを参照してください。

次の図は、共有 l3extInstP EPG 用に設定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:* 共有レイヤ *3 Out* ポリシー モデル



共有レイヤ3アウトサイドネットワーク設定については、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（*user*、`common`、`infra`、`mgmt`）です。共有 `l3extInstP` EPG が `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 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 にありますが、同じ `l3extInstP` EPG を共有しています。
- サブネットは、*private*、*public*、または *shared* です。`L3extOut` 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、*shared* に設定されている必要があります。`L3extOut` にエクスポートされるサブネットは *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、共有レイヤ 3 アウトサイド ネットワーク サービスを提供する `l3extInstP` 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 L3 Out では禁止コントラクトを使用しないでください。この設定はサポートされません。
- `l3extInstP` は共有サービス プロバイダとしてサポートされますが、l3extInstP 以外のコンシューマのみに限定されます（`L3extOut` EPG = `l3extInstP` である場合）。

- トラフィック中断（フラップ）：l3instP EPG が、l3instP 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*）に設定して外部サブネット 0.0.0.0/0 を使用して設定されると、VRF 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 内のすべての外部トラフィックが中断されます（VRF 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 L3extOut のプレフィックスは一意である必要があります。同じコンテキスト（VRF）の同じプレフィックスを使用した、複数の共有 L3extOut 設定は動作しません。VRF 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 l3instP に属することはできません）。プレフィックス prefix1 を使用した L3extOut 設定（たとえば、L3Out1）と、同様にプレフィックス prefix1 を使用した 2 番目のレイヤ 3 アウトサイド設定（たとえば、L3Out2）が同じ VRF に属すると、動作しません（導入される pcTag は 1 つのみであるため）。L3extOut のさまざまな動作は、同じ VRF の同じリーフ スイッチに設定されている可能性があります。考えられるシナリオは次の 2 つです。

  - シナリオ 1 には、SVI インターフェイスおよび 2 個のサブネット（10.10.10.0/24 および 0.0.0.0/0）が定義された.L3extOut があります。レイヤ 3 アウトサイド ネットワークの入力トラフィックに一致するプレフィックス 10.10.10.0/24 がある場合、入力トラフィックは外部 EPG pcTag を使用します。レイヤ 3 アウトサイド ネットワーク上の入力トラフィックに一致するデフォルト プレフィックス 0.0.0.0/0 がある場合、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 には、2 個のサブネット（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 routed-sub-interface を使用する L3extOut があります。レイヤ 3 アウトサイド ネットワークの入力トラフィックに一致するプレフィックス 10.10.10.0/24 がある場合、入力トラフィックは外部 EPG pcTag を使用します。レイヤ 3 アウトサイド ネットワーク上の入力トラフィックに一致するデフォルト プレフィックス 0.0.0.0/0 がある場合、入力トラフィックは VRF pcTag を使用します。

  - これらの説明した動作の結果として、SVI インターフェイスを使用して L3extOut-A および L3extOut-B で同じ VRF および同じリーフ スイッチが設定されている場合、次のユース ケースが考えられます。

    ケース 1 は L3extOut -A 用です。この外部ネットワーク EPG には 2 個のサブネットが定義されています。 10.10.10.0/24 & 0.0.0.0/1。L3extOut-A の入力トラフィックに一致するプレフィックス 10.10.10.0/24 がある場合、L3extOut-A に関連付けられている外部 EPG pcTag & コントラクトを使用します。L3extOut-A の出力トラフィックに特定の一致がなく、最大のプレフィックス一致が 0.0.0.0/1 の場合、外部ブリッジ ドメイン（BD）pcTag & コントラクト-A を使用します。

    ケース 2 は L3extOut-B です。 この外部ネットワーク EPG には定義された 1 個のサブネット: 0.0.0.0/0 があります。L3extOut-B の入力トラフィックに一致するプレフィックス 10.10.10.0/24 (L3extOut-A で定義）がある場合、L3extOut-A に関連付けられている L3extOut-A およびコントラクト A の外部 EPG pcTag を使用します。L3extOut-B に関連付けられているコントラクト-B は使用しません。

- 許可されないトラフィック：無効な設定で、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。そのようなトラフィックは、`shared-rtctrl` プレフィックスを shared-security プレフィックスとしても使用するように設定を修正することで、有効にすることができます。
- 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** 設定の詳細：
    - VRF1 を持つレイヤ 3 アウトサイド ネットワーク設定（たとえば、名前付き `L3extOut` -1）は provider1 と呼ばれます。
    - VRF2 を持つ二番目のレイヤ 3 アウトサイド ネットワーク設定（たとえば、名前付き `L3extOut`-2）は provider2 と呼ばれます。
    - `L3extOut` -1 VRF1 は、インターネット 0.0.0.0/0 にデフォルト ルートをアドバタイズし、これは *shared-rtctrl* および *shared-security* の両方を有効にします。
    - `L3extOut`-2 VRF2 は特定のサブネットを DNS および NTP 192.0.0.0/8 にアドバタイズし、*shared-rtctrl* を有効にします。
    - `L3extOut`-2 VRF2 に特定の 192.1.0.0/16 があり、*shared-security* を有効にします。
    - **バリエーション A**：EPG トラフィックが複数の VRF に向かいます。
      - EPG1 と `L3extOut`-1 の間の通信は *allow_all* コントラクトによって制御されます。
      - EPG1 と `L3extOut`-2 の間の通信は *allow_all* コントラクトによって制御されます。

        結果：EPG1 から `L3extOut`-2 へのトラフィックも 192.2.x.x に向かいます。
    - **バリエーション B**：EPG は 2 番目の共有レイヤ 3 アウトサイド ネットワーク の *allow_all* コントラクトに従います。
      - EPG1 と `L3extOut`-1 の間の通信は *allow_all* コントラクトによって制御されます。
      - EPG1 と `L3extOut`-2 の間の通信は *allow_icmp* コントラクトによって制御されます。

結果：EPG1 ～ `L3extOut`-2 から 192.2.x.x へのトラフィックは *allow_all* コントラクトに従います。

- **ケース 2** 設定の詳細：
  - `L3extOut` プロファイル（l3instP）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` で到達するトラフィックは、EPG に向かうことが許可されます。
    - **バリエーション A**：意図しないトラフィックが EPG を通過します。

      `L3extOut`（l3instP）EPG のトラフィックがこれらのプレフィックスを持つ `L3extOut` に向かいます。

      - `192.0.0.0/8 = import-security, shared-rtctrl`

      - `192.1.0.0/16 = shared-security`

      - EPG には `1.1.0.0/16 = shared` があります

      結果：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**：意図しないトラフィックが EPG を通過します。共有 `L3extOut` に到達したトラフィックは EPG を通過できます。

      -共有 `L3extOut` VRF には、`pcTag = prov vrf` を持つ EPG と *allow_all* に設定されているコントラクトがあります。

      - EPG は `<subnet> = shared` となっています。

      結果：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。

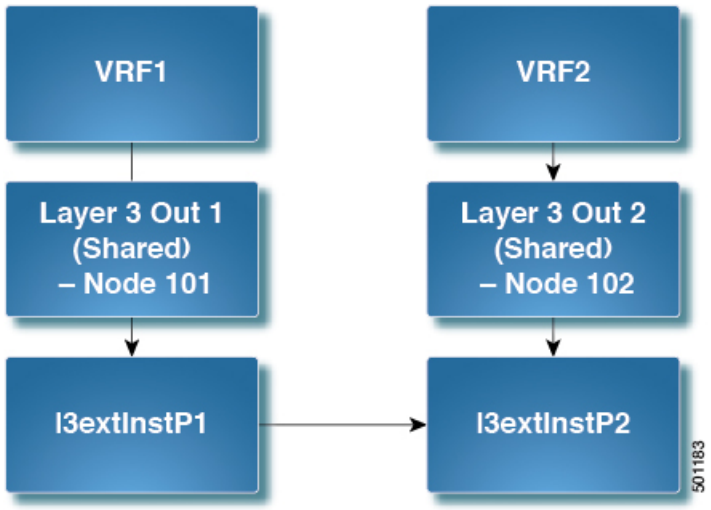
この機能を稼働するには、次の条件を満たす必要があります。

- 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 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 **Tenants** > **Add Tenant** を選択します。

ステップ 2 **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、[**L3Outs**] に移動します。

ステップ 5 [**L3Outs**] を右クリックし、[**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 [**VRF の作成（Create VRF**）] ダイアログ ボックスで、次の操作を実行します。

a) **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。

[識別（Identity）] ウィンドウで選択したプロトコルに応じて、[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。[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) **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) [サブネットの作成（Create Subnet）] ウィンドウにアクセスするには、[+] をクリックします。
d) [**サブネットの作成（Create Subnet**）] ダイアログ ボックスの [**IP アドレス（IP Address**）] フィールドに、マッチングを行う IP アドレスを入力します。**OK** をクリックします。
e) [L3Out の作成（Create L3Out）] ウィザードで [完了（Finish）] をクリックします。

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 **Work** ウィンドウの、外部ネットワークの **Properties** の下で、**Resolved VRF** フィールドに解決された VRF が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 **Scope** フィールドで、必要なチェック ボックスをオンにして、**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**
- **共有セキュリティインポートサブネット**

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

ステップ 14 [**プロバイダ 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。**Submit** をクリックします。

ステップ 15 メニュー バーで、 **Tenants** > **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 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、コンシューマの [**L3Outs**] に移動します。

ステップ 19 [**L3Outs**] を右クリックし、[**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 [**VRF の作成（Create VRF**）] ダイアログ ボックスで、次の操作を実行します。

a) **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) **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。

[識別（Identity）] ウィンドウで選択したプロトコルに応じて、[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。[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 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) **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) [サブネットの作成（Create Subnet）] ウィンドウにアクセスするには、[+] をクリックします。
d) [**サブネットの作成（Create Subnet**）] ダイアログ ボックスの [**IP アドレス（IP Address**）] フィールドに、マッチングを行う IP アドレスを入力します。**OK** をクリックします。
e) **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。

このシナリオでは、**Shared Route Control Subnet** と **Shared Security Import Subnet** のチェック ボックスをオンにします。

f) [L3Out の作成（Create L3Out）] ウィザードで [完了（Finish）] をクリックします。

これで、共有レイヤ 3 Out VRF 間リーキングの設定は完了です。

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。