



Cisco APIC と Cisco ISE の統合

[新機能および変更された機能に関する情報](#) 2

[Cisco APIC-ISE 統合の概要](#) 2

[Cisco APIC と Cisco ISE の統合](#) 3

[ネットワークの可視性のための Cisco APIC の使用](#) 6

[共有サービスのルートリークの構成](#) 11

新機能および変更された機能に関する情報

次の表は、この最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

Cisco APIC のリリース バージョン	特長
6.1(1)	Cisco APIC と Cisco ISE の統合のサポート。 (注) このリリースでは機能に制限があります（ベータ版）。
6.1(2)	EPG間でのルートリークを使用した共有サービスのサポート。

Cisco APIC-ISE 統合の概要

シスコでは、データセンターのアプリケーション ポリシー インフラストラクチャ コントローラ（Application Policy Infrastructure Controller、APIC）や、キャンパスおよびエンタープライズ環境のシスコアイデンティティ サービス エンジン（Cisco Identity Services Engine、ISE）など、さまざまなコントローラを使用してポリシーを管理しています。従来、これらのコントローラは独立して動作し、独立したシステムとして機能していました。Cisco APIC と Cisco ISE はどちらも、ポリシーを適用するためにデバイス、エンドポイント、またはユーザをグループに分類することを容易にします。この分類基準は コンテキストと呼ばれます。

ISE と Cisco ACI を統合すると、Cisco ISE と APIC が Cisco pxGrid（プラットフォーム交換グリッド、Platform Exchange Grid）を使用して通信し、コンテキスト情報を共有できるソリューションが提供されます。この統合により、Cisco APIC と ISE 間のグループ情報の交換が可能になり、共通ポリシー アーキテクチャの一部となり、中央のコンテキスト交換ハブとして ISE に接続されたさまざまなコントローラ間でのグループ コンテキストの共有がサポートされます。

このドキュメントで頻繁に使用される重要な用語：

- エンドポイントグループ（EPG）：同じブリッジドメイン（BD）に属し、同じネットワークとセキュリティポリシーを共有するエンドポイントのグループを含む論理エンティティです。EPG は、1 つのブリッジ ドメインにのみ属することができます。
- エンドポイントセキュリティ グループ（ESG）は、物理または仮想ネットワーク エンドポイントの集まりを含む論理エンティティです。ESG は、単一の VRF インスタンスに関連付けられます。ESG を使用すると、複数のブリッジ ドメインにまたがるセキュリティ ポリシーを定義できます。ESG を使用すると、特定の VRF の下の任意の数の BD にまたがる任意の数のエンドポイントにポリシーをグループ化して適用できます。
- セキュリティ グループ タグ（SGT）は、一意のロールに割り当てられる一意のタグです。送信元ユーザー、デバイス、またはエンティティの権限を表し、Cisco TrustSec ドメインの入力でタグ付けされます。
- Trustsec：ネットワークにアクセス制御ポリシーを適用するために SGT を使用するセキュリティ アーキテクチャです。

- **pxGrid** : クロスプラットフォームのネットワーク コラボレーションを可能にする、オープンでスケーラブルな IETF 承認標準です。プラットフォームは、コンテキストを共有または公開したり、他のプラットフォームからコンテキストを使用またはサブスクライブしたりすることができます。
- **バインディング** : SGT、EPG、および ESG は異なる用語ですが、同じ目的を持っています。これらはすべて、ユーザー、デバイス、またはサービスに関連付けられた IP アドレスを指定されたグループに分類します。IP アドレスとグループの関連付けのことをバインディングと呼びます。
- **インバウンド SGT ドメイン ルール** : SGT バインディングを特定の SGT ドメインにマッピングするために使用されるルールです。
- **アウトバウンド SGT ドメイン ルール** : SGT バインディングを外部 EPG として APIC に割り当てるために使用されるルールです。

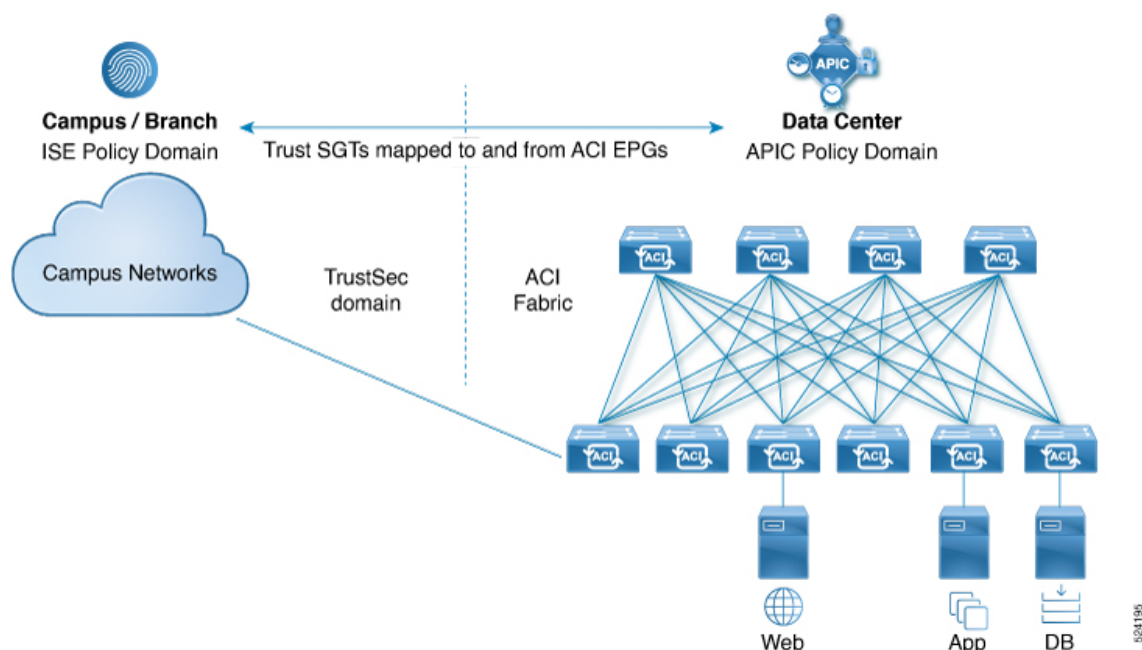
このドキュメントは単独では使用できません。関連する詳細と Cisco ISE を使用して実行される構成が記載されている [Cisco ISE 管理者ガイド、リリース 3.4](#) を参照してください。

Cisco APIC と Cisco ISE の統合

このドキュメントでは、Cisco APIC-ISE 統合の詳細について説明します。この統合では、ISE コントローラがドメイン間のグループ コンテキストの共有を管理します。構成は ISE コントローラから実行されます。Cisco APIC は、統合接続のステータスや、2つのドメイン間で共有されているグループのグループおよびバインディング情報など、Cisco APIC UI からこの統合を可視化します。

ISE 統合は、APIC のマルチポッド、マルチテナント、マルチ VRF、および EPG（または ESG）コンテキストをサポートします。単一ポッドやマルチポッド ファブリックを含む複数の ACI ファブリックへの双方向接続を ISE から直接設定し、SGT/EPG/ESG コンテキストの交換を開始できます。ACI の EPG（または ESG）は正規化され、SGT として ISE に保存されます。これにより、ISE からのコンテキストを消費するすべてのドメイン コントローラが、キャンパス/ブランチのユーザー/デバイスからデータセンターのエンドポイント グループへのトラフィックのポリシーを構成できるようになります。ISE の SGT は正規化され、外部 EPG として ACI に保存されます。

図 1: Cisco APIC と ISE の統合



ISE は、pxGrid チャネルを介して SGT とバインディングを APIC にパブリッシュします。SGT とバインディングは、サブネットバインディングを使用して外部 EPG（EEPG）としてプログラムされ、APIC が ISE のグループメンバーシップに基づいて ACI ファブリックに着信するパケットを分類してポリシーを適用できるようにします。同様に、APIC は EPG および ESG グループとエンドポイント情報を ISE に発行し、そこで SGT とバインディングに変換され、ISE が ACI ファブリックからキャンパス ネットワークに着信するパケットを分類してポリシーを適用できるようにします。

Cisco APIC-ISE 統合の利点

- 各ドメイン内で個別にコンテキストを確立します。その後、コンテキストは正規化され、SGT として保存されるため、異なるドメイン間で共有できます。
- 一貫性のある SGT ベースのポリシーにより、シンプルで統合されたポリシー エクスペリエンスを実現します。
- ユーザー、デバイス、アプリケーション ワークロード間で一貫したアクセスポリシーを適用します。

Cisco APIC-ISE の用語

Cisco APIC	Cisco ISE
エンドポイント グループ（EPG）またはエンドポイントセキュリティ グループ（ESG）	セキュリティ グループ タグ（SGT）
IP-EPG バインディング	IP-SGTバインディング
コントラクト	TrustSecポリシー

Cisco APIC-ISE 統合のガイドラインと制限事項

ガイドライン

- サポートされている ISE バージョンは ISE 3.4P1 です。
- ISE から ACI への接続は、APIC クラスタのコントローラの 1 つで確立されます。ISE-ACI 接続を持つノードがダウンした場合、クラスタの他のノードによるテイクオーバー時間は約 5 分です。
- 共有サービスは、キャンパス SGT から EPG またはキャンパス SGT から SGT 間でサポートされます。

制限事項

- SGT に関連付けられた L3Out を含む VRF は、入力モードまたは出力モードにすることができます。

SGT 外部 EPG を使用した L3Out（このドキュメントではキャンパス SGT L3Out と呼びます）を含む VRF は、入力または出力ポリシー制御の適用方向で設定できます。

入力ポリシー制御の適用方向に関する制限事項：

- サイト間 L3Out。
- 動的 EPG 分類（DEC）は、同じ L3Out の構成と共存できません。
- EPG は、共有サービス契約のプロバイダーである必要があります。
- 純粋な非境界リーフからキャンパス境界リーフへのトラフィックの場合、ポリシーはキャンパス境界リーフノードで適用されます。
- 1 つの SGT が 1 つの ISE-ACI 接続に関連付けられます。1 つの SGT から複数の ISE-ACI 接続への関連付けはサポートされていません。複数の ISE 接続が ACI で SGT をプログラミングすることになるため、同じ L3Out でプログラミングする場合は、各 ISE 接続で一意的な SGT 名を設定する必要があります。
- 最初の SGT（外部 EPG）が ISE によって設定されると、キャンパス SGT L3Out で学習されたプレフィックスについては数秒間のトラフィック損失が発生することがあります。
- 構成ロールバックはサポートされていません。ロールバックを実行しようとする、ISE と ACI の間に設定の不一致が発生する可能性があります。ISE と ACI の同期を維持するために ISE の設定を削除または再適用する必要があります。

Cisco APIC-ISE 統合でサポートされるスケール数

パラメータ	拡張性
ACI サイトまたは ACI クラスタ	75
ACI ファブリックあたりの ISE 接続の最大数	3
ACI ファブリックごとのテナント	10
ACI ファブリックごとの VRF	50

パラメータ	拡張性
ACI ファブリックあたりの最大 L3Out	500
L3Out あたりの最大 SGT	250
1 つの ACI ファブリックから ISE に公開される EPG/ESG の最大数	500
1 つの ACI ファブリックですべての ISE から登録された SGT の最大数	500
最大 SGT : ISE	50000
最大 Trustsec マトリックス	10000
ISE 接続ごと、ACI ファブリックごとの IPv4 および IPv6 バインディングの最大数	32000
ソリューションの最大 IPv4 および IPv6 バインディング	200 万
すべての ISE 接続から 1 つの ACI ファブリックが受信する IPv4 バインディングの最大数	64000
すべての ISE 接続から 1 つの ACI ファブリックが受信する IPv6 バインディングの最大数	64000
すべての ISE 接続から 1 つの ACI ファブリックが受信する IPv4 および IPv6 バインディングの最大数	64000



(注) SGT バインディングは、外部 EPG のホストプレフィックスとして機能します。

ネットワークの可視性のための Cisco APIC の使用

ISE は APIC への接続を作成し、ISE と APIC の間に pxGRID チャンネルを確立します。ISE で作成された SGT は、APIC で外部 EPG として公開されます。

Cisco ISE で次の前提条件を満たしてください。

- スタンドアロン/展開セットアップで pxGrid および SXP サービスを有効にします。
- ACI が ISE を認識できる、またその逆もできるように、DNS を構成します。
- ACI 接続を作成します。これは APIC のオブジェクトとして示されます。

Cisco APIC で次の前提条件を満たしてください。

- テナント、VRF、L3Out、コントラクトなどの標準 APIC の構成を行います。

- アプリケーション EPG や ESG を構成します。
- ISE pxGrid デバイスの DNS サーバーを構成します。
- DNS サーバーを構成し、ISE FQDN が APIC から到達可能であることを確認します。

APIC GUI には、ISE 構成の詳細を取得できる場所が 2 つあります。

- [\[インテグレーション \(Integrations\)\] タブ](#)
- [\[テナント \(Tenants\)\] タブ](#)

[統合 (Integrations)] タブの詳細

ISE で作成された ACI 接続の詳細を取得するには、次の手順に従います。

始める前に

ISE GUI で、ACI 接続を構成します（例：s1_ACI）。Cisco ISE では複数の Cisco ACI 接続を追加できます。

手順

ステップ 1 Cisco APIC GUI にログインします。

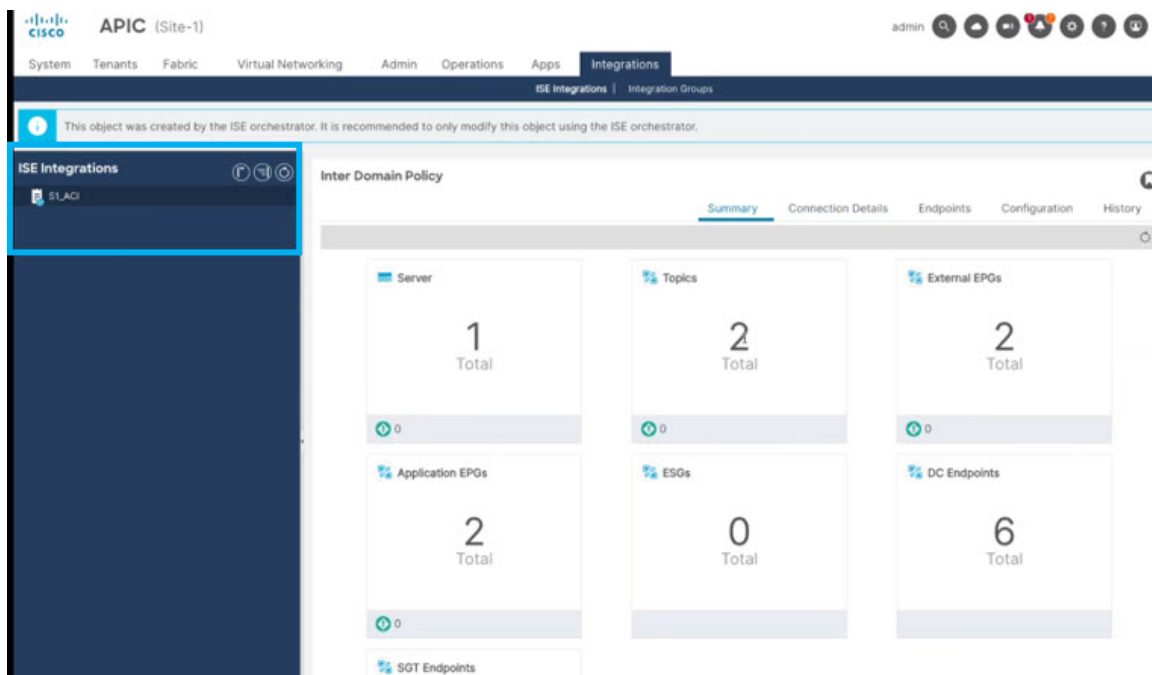
ステップ 2 [\[統合 \(Integrations\)\]](#) > [\[ISE 統合 \(ISE Integrations\)\]](#) に移動します。

[ドメイン間ポリシー (Inter Domain Policy)] ペインが表示されます。右側の 5 つのタブは、[\[概要 \(Summary\)\]](#)、[\[接続の詳細 \(Connection Details\)\]](#)、[\[エンドポイント \(Endpoints\)\]](#)、[\[構成 \(Configuration\)\]](#)、[\[履歴 \(History\)\]](#) です。

[\[ISE 統合 \(ISE Integrations\)\]](#) ペインの左側に、ISE で作成された接続 s1_ACI が表示されます。

ステップ 3 これらの各タブをクリックして、関連する詳細を取得します。

図 2: [インテグレーション (*Integrations*)] タブ



[概要 (Summary)] タブに表示される詳細：

- [サーバー (Server)]：ISE サーバーの数。
- [トピック (Topics)]：通常は2つのトピック。1つは公開された SGT 用、もう1つはサブスクライブされた EPG 用です。
- [外部 EPG (External EPGs)]：ISE によって公開された SGT の数。APIC で外部 EPG として示されます。
- [アプリケーション EPG (Application EPGs)]：APIC によって ISE に公開された EPG。
- [ESG (ESGs)]：ISE に対して APIC によって公開された ESG。
- [DC エンドポイント (DC endpoints)]：APIC によって ISE に公開されたバインディング。
- [SGT エンドポイント (SGT endpoints)]：ISE によって APIC に公開されたバインディング。

[接続 (Connections)] タブに表示される詳細：

- [名前 (Name)]：ISE で作成された接続。
- [説明します (Description)]：接続の説明を入力します。
- [管理状態 (Admin state)]：オプションは次のとおりです。
 - [publish-and-listen]：ISE に向けて EPG/ESG バインディングを公開し、SGT バインディング更新の ISE/pxgrid 更新をリッスンします。
 - [listen]：SGT バインディング更新の ISE/pxgrid 更新をリッスンします (ISE への公開なし)。

- [接続モード (Connection mode)] : ACI 接続 (インバンドまたはアウトオブバンド) で構成された APIC IP アドレスに基づいて、ISE によって自動的に検出されます。
- [接続タイプ (Connections)] : pxGrid 接続。
- [ユーザー名 (Username)] : 接続の作成に使用されるユーザー名。
- [サーバー (Servers)] : ドメイン名を含む ISE サーバーの IP アドレス。
- [トピック (Topics)] : オプションは次のとおりです。
 - [パブリッシャー ロール (Publisher role)] : APIC によって ISE にパブリッシュされた EPG/ESG。
 - [サブスクライバ ロール (Subscriber role)] : ISE から APIC によってサブスクライブされた SGT。

[エンドポイント (Endpoints)] タブに表示される詳細 :

- [SGT エンドポイント (SGT Endpoints)] サブタブ : ISE からのバインディングと SGT 番号。[バインディングの詳細 (Binding details)] の行をクリックします。関連付けられた外部 EPG の詳細を含む新しいウィンドウが表示されます。
- [DC] サブタブ : テナント、EPG/ESG、VRF、および IP アドレスの詳細を含む、ISE に対して公開されたバインディング。

[設定 (Configuration)] タブに表示される詳細 :

- [公開済み EPG/ESG (Published EPGs/ESGs)] サブタブ : ISE ユーザーが ACI から ISE の対応する IP バインディングを学習するために選択した EPG/ESG。EPG/ESG ごとに、テナント、アプリケーション プロファイル、EPG/ESG 名が表示されます。
テナントの詳細を含む行をクリックして、関連するコントラクトを取得します。
- [サブスクライブ済み SGT (Subscribed SGTs)] サブタブ : ISE ユーザーが ISE から ACI に対応する IP バインディングを公開するために選択する SGT。SGT ごとに、テナント、L3Out、および外部 EPG の名前が表示されます。

[履歴 (History)] タブに表示される詳細 :

標準イベントおよび監査ログが表示されます。

[テナント (Tenants)] タブの詳細

ISE が SGT を APIC に公開すると、SGT はテナント L3Out の下で外部 EPG として構成されます。

ISE によって公開された SGT に基づいて、APIC で作成された外部 EPG (EEPG) の詳細を取得するには、次の手順に従います。図 3 と 4 は、APIC で EEPG として使用可能な ISE で作成された SGT を示しています。ISE で作成された SGT (sgt_epg102_EPG) に APIC で対応する EEPG は、ISE_SGT_1016 です。

図 3: ISE GUI で構成されたアウトバウンド SGT ドメインルール

Outbound Rule Details

ifav82_ifc2_ise3 X

Destinations
ifav82_ifc2_ise3

L3 Outs
l3_2 (t39) X

RULE CONFIGURATION

AND

SGP Domains Equals default

SGT Name Equals sgt_epg102_EPG

+ Add AND/OR Statement + Add Condition

CONTRACT CONFIGURATION

SGT Name

sgt_epg102_EPG

Connection/ Tenant/ L3out
ifav82_ifc2_ise3/ t39/ l3_2

Consumed Contract

Provided Contract
common CONTRACT - default X

図 4: ISE の SGT から APIC の EEPG へのマッピング

APIC (ifav82-ifc2-s2)

System Tenants Fabric Virtual Networking Admin Operations Apps Integrations

ALL TENANTS | Add Tenant | Tenant Search: name or descr | common | t39 | mgmt | infra

This object was created by the ISE orchestrator. It is recommended to only modify this object using the ISE orchestrator.

t39

External EPG - ISE_SGT_1016

Summary Policy Operational Health Faults History

Contracts SGT Endpoints

Bindings

103.2.2.2/32

SGT Name Campus SGT

sgt_epg102_EPG 1016

External EPG - ISE_SGT_1016

手順

ステップ 1 Cisco APIC GUI にログインします。

ステップ 2 [テナント (Tenants)] > [Web アプリ (Web-App)] > [ネットワーキング (Networking)] > [L3Outs] > [外部 EPG (External EPGs)] に移動します。

ISE で作成されたアウトバウンド SGT は、外部 EPG としてここ (APIC GUI) に表示されます。

ステップ 3 EEPG の下に表示される SGT をクリックすると、画面の右側に詳細が表示されます。

画面の上部に、オブジェクトが ISE を使用して作成されたことを示すバナーが表示されます。ISE オークストレータを使用してのみオブジェクトを変更できます。

ステップ 4 選択した SGT に接続されているバインディングを確認するには、右側のペインで、[操作 (Operational)]、[SGT エンドポイント (SGT Endpoints)] の順にクリックします。

(注)

サブネット情報は、[ポリシー (Policy)] > [全般 (General)] では使用できません。バインディング情報を確認するには、上記のようにパスを確認します。

共有サービスのルートリークの構成

IP プレフィックスはキャンパス SGT L3Out を介して学習されます。VRF 間で共有するには、次の手順を使用します。

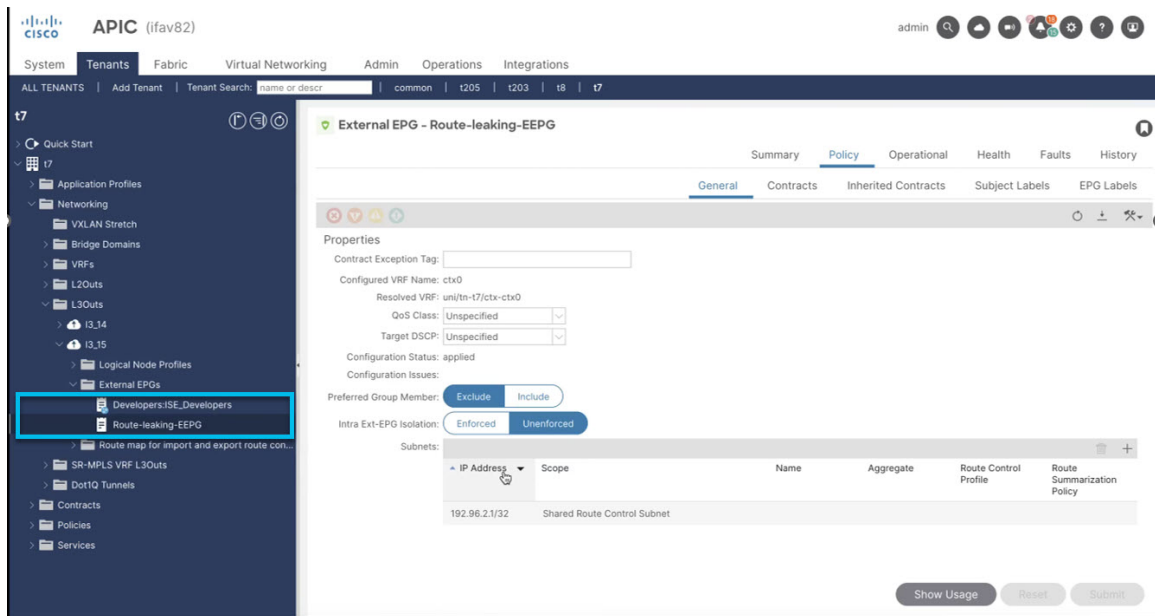
始める前に

SGT と外部 EPG (または AEPg) 間の共有サービス、または SGT と SGT 間の共有サービスをサポートするには、ルートリークサブネットを構成して、APIC の VRF 間でルートリークを設定する必要があります。ポリシープレーン構成は ISE によって促されます。

ルートリークの場合、同じ共有コントラクトを持つ 2 つの外部 EPG が必要です：

- APIC での外部 EPG の構成：共有ルート制御フラグを有効にして、APIC で外部 EPG (ルートリーク EEPG など) を設定します。この外部 EPG に共有コントラクトをアタッチして、VRF 全体でのプレフィックスリークを促進します。
- ISE と SGT の統合：ISE で SGT (ISE_Developers など) を構成します。同じ共有コントラクトがアタッチされた ISE からこの SGT を展開し (ISE からの SGT は APIC で外部 EPG として表示されます)、ポリシー プレーンが定義されたポリシーに基づいてトラフィックを許可または拒否できるようにします。

図 5: APIC の外部 EPG



(注) 集約サブネットまたはデフォルトサブネット (0.0.0.0/0) を持つ集約共有制御フラグを使用しても、ルートリーク外部 EPG を設定できます。

手順

ステップ 1 Cisco APIC GUI で、[テナント (Tenants)] タブをクリックします。

ステップ 2 [ネットワーキング (Networking)] > [L3Outs] > [L3_out_name] > [外部 EPG (External EPGs)] に移動します。右クリックし、[外部 EPG の作成 (Create External EPG)] を選択します。

ステップ 3 表示される [外部 EPG の作成 (Create External EPG)] ウィンドウで、必要な詳細を入力します。

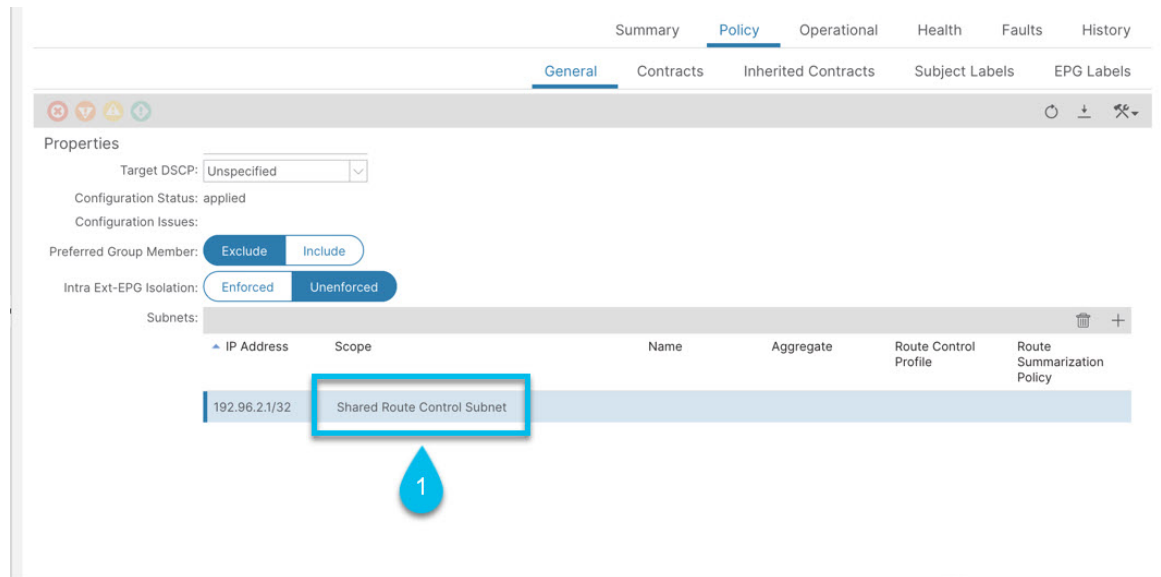
ステップ 4 [サブネット (Subnets)] ペインで、(+) をクリックします。

ステップ 5 表示される [サブネットの作成 (Create Subnet)] ウィンドウで、IP アドレスを入力し、[共有ルート制御サブネット (Shared Route Control Subnet)] チェックボックスをオンにします。

ここでのサブネットは、キャンパス SGT L3Out を介して学習された IP プレフィックスです。

ステップ 6 [OK] をクリックし、[送信 (Submit)] をクリックします ([外部 EPG (External EPG)] ウィンドウ)。

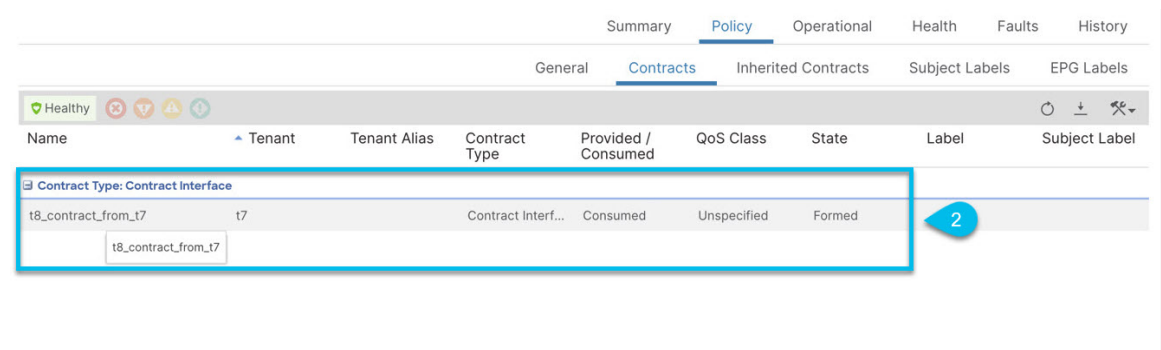
図 6: 選択したスコープのサブネット



ステップ7 作成した外部 EPG をクリックし、[ポリシー (Policy)]>[コントラクト (Contracts)] タブを選択します。

ステップ8 [アクション (Actions)] アイコンをクリックし、ドロップダウンリストからコントラクトを選択します。

図 7: コントラクトのタイプ



ステップ9 (ISE GUI で) ISE からの IP プレフィックスとコントラクトを使用して ISE SGT を展開します。APIC の外部 EPG に定義されたものと同じ共有コントラクトを選択していることを確認します。

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

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。