Cisco ACI ベーシック コンフィギュレーション ガイド

初版：2015 年 10 月 19 日

最終更新：2015 年 02 月 22 日

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/

Text Part Number:

【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。

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

このガイドは、次の 1 つ以上に責任を持つ、専門知識を備えたデータセンター管理者を主な対象にしています。

- 仮想マシンのインストールと管理
- サーバ管理
- スイッチおよびネットワークの管理

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。

表記法	説明
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告 安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保存しておいてください。

関連資料

アプリケーション セントリック インフラストラクチャのマニュアル セットには、次の URL の Cisco.com から入手可能な次のドキュメントが含まれます。http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Web ベースのマニュアル

- 『*Cisco APIC Management Information Model Reference*』
- 『*Cisco APIC Online Help Reference*』
- 『*Cisco APIC Python SDK Reference*』
- 『*Cisco ACI Compatibility Tool*』
- 『*Cisco ACI MIB Support List*』

ダウンロード可能なドキュメント

- ナレッジ ベースの記事（KB 記事）は、次の URL から入手できます。 http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html
- 『*Cisco Application Centric Infrastructure Controller Release Notes*』
- 『*Cisco Application Centric Infrastructure Fundamentals Guide*』

- 『*Cisco APIC Getting Started Guide*』
- 『*Cisco ACI Basic Configuration Guide*』
- 『*Cisco ACI Virtualization Guide*』
- 『*Cisco APIC REST API User Guide*』
- 『*Cisco APIC Object Model Command Line Interface User Guide*』
- 『*Cisco APIC NX-OS Style Command-Line Interface Configuration Guide*』
- 『*Cisco APIC Faults, Events, and System Messages Management Guide*』
- 『*Cisco ACI System Messages Reference Guide*』
- 『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』
- 『*Cisco APIC Layer 4 to Layer 7 Device Package Development Guide*』
- 『*Cisco APIC Layer 4 to Layer 7 Device Package Test Guide*』
- 『*Cisco ACI Firmware Management Guide*』
- 『*Cisco ACI Troubleshooting Guide*』
- 『*Cisco APIC NX-OS Style CLI Command Reference*』
- 『*Cisco ACI Switch Command Reference, NX-OS Release 11.0*』
- 『*Verified Scalability Guide for Cisco ACI*』
- 『*Cisco ACI MIB Quick Reference*』
- 『*Cisco Nexus CLI to Cisco APIC Mapping Guide*』
- 『*Application Centric Infrastructure Fabric Hardware Installation Guide*』
- 『*Cisco NX-OS Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches*』
- 『*Nexus 9000 Series ACI Mode Licensing Guide*』
- 『*Cisco Nexus 9332PQ ACI-Mode Switch Hardware Installation Guide*』
- 『*Cisco Nexus 9336PQ ACI-Mode Switch Hardware Installation Guide*』
- 『*Cisco Nexus 9372PX and 9372PX-E ACI-Mode Switch Hardware Installation Guide*』
- 『*Cisco Nexus 9372TX ACI-Mode Switch Hardware Installation Guide*』
- 『*Cisco Nexus 9396PX ACI-Mode Switch Hardware Installation Guide*』
- 『*Cisco Nexus 9396TX ACI-Mode Switch Hardware Installation Guide*』
- 『*Cisco Nexus 93128TX ACI-Mode Switch Hardware Installation Guide*』
- 『*Cisco Nexus 9504 NX-OS Mode Switch Hardware Installation Guide*』
- 『*Cisco Nexus 9508 ACI-Mode Switch Hardware Installation Guide*』
- 『*Cisco Nexus 9516 ACI-Mode Switch Hardware Installation Guide*』

シスコ アプリケーション セントリック インフラストラクチャ（ACI）シミュレータのマニュアル

次のシスコ ACI シミュレータのマニュアルは、次の URL から入手できます。http://www.cisco.com/c/en/us/support/cloud-systems-management/application-centric-infrastructure-simulator/tsd-products-support-series-home.html

- 『*Cisco ACI Simulator Release Notes*』
- 『*Cisco ACI Simulator Installation Guide*』
- 『*Cisco ACI Simulator Getting Started Guide*』

Cisco Nexus 9000 シリーズ スイッチのマニュアル

Cisco Nexus 9000 シリーズ スイッチのマニュアルは、次の URL で入手できます。http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html

Cisco Application Virtual Switch のマニュアル

Cisco Application Virtual Switch（AVS）のマニュアルは、次の URL で入手できます。http://www.cisco.com/c/en/us/support/switches/application-virtual-switch/tsd-products-support-series-home.html

シスコ アプリケーション セントリック インフラストラクチャ（ACI）と OpenStack の統合に関するマニュアル

Cisco ACI と OpenStack の統合に関するマニュアルは、次の URL から入手できます。http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、apic-docfeedback@cisco.com までご連絡ください。ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、次から入手できます。 http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、RSS フィードとして購読できます。また、リーダー アプリケーションを使用して、コンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

第 1 章

ユーザ アクセス、認証およびアカウンティング

この章の内容は、次のとおりです。

アクセス権のワークフローの依存関係

Cisco ACI RBAC のルールは、ファブリックの一部または全体へのアクセスを有効にするか、または制限します。たとえば、ベア メタル サーバ アクセス用のリーフ スイッチを設定するには、ログインしている管理者が `infra` ドメインに対する権限を持っている必要があります。デフォルトでは、テナント管理者は `infra` ドメインに対する権限を持っていません。この場合、リーフ スイッチに接続されているベア メタル サーバの使用を計画しているテナント管理者は、そのために必要なすべての手順を実行することはできません。テナント管理者は、`infra` ドメインに対する権限を持っているファブリック管理者と連携する必要があります。ファブリック管理者は、ACI リーフ

ユーザ アクセス、認証およびアカウンティング

スイッチに接続されたベア メタル サーバを使用するアプリケーション ポリシーを導入するためにテナント管理者が使用するスイッチ設定ポリシーをセットアップします。

ユーザ アクセス、認証およびアカウンティング

APIC ポリシーは、Cisco ACI ファブリックのアクセス、認証、およびアカウンティング（AAA）機能を管理します。ユーザ権限、ロールおよびドメインとアクセス権限の継承を組み合わせることにより、管理者は非常に細分化された方法で管理対象オブジェクト レベルで AAA 機能を設定することができます。これらの設定は、REST API、CLI、または GUI を使用して実行できます。

マルチテナントのサポート

コア APIC 内部データ アクセス コントロール システムにより、マルチテナント分離が提供され、テナント間での個人情報の漏洩が防止されます。読み取り/書き込みの制約により、テナントによる他のテナントの設定、統計情報、障害、またはイベント データの参照が防止されます。管理者によって読み取り権限が割り当てられない限り、テナントはファブリックの設定、ポリシー、統計情報、障害、またはイベントの読み取りが制限されます。

ユーザ アクセス：ロール、権限、セキュリティ ドメイン

APIC では、ロールベース アクセス コントロール（RBAC）を介してユーザのロールに従ってアクセスが提供されます。ACI ファブリック ユーザは、次に関連付けられています。

- ロールのセット
- ロールごとの権限タイプ：アクセスなし、読み取り専用、または読み取り/書き込み
- ユーザがアクセスできる管理情報ツリー（MIT）の一部を識別する 1 つ以上のセキュリティ ドメイン タグ

ACI ファブリックは、管理対象オブジェクト（MO）レベルでアクセス権限を管理します。権限は、システム内の特定の機能に対するアクセスを許可または制限する MO です。たとえば、ファブリック機器は権限ビットです。このビットは、物理ファブリックの機器に対応するすべてのオブジェクト上で APIC によって設定されます。

ロールは権限ビットの集合です。たとえば、「管理者」ロールが「ファブリック機器」と「テナント セキュリティ」に対する権限ビットに設定されていると、「管理者」ロールにはファブリックの機器とテナント セキュリティに対応するすべてのオブジェクトへのアクセス権があります。

セキュリティ ドメインは、ACI MIT オブジェクト階層の特定のサブツリーに関連付けられたタグです。たとえば、デフォルトのテナント「common」にはドメイン タグ `common` が付いています。同様に、特殊なドメイン タグ `all` の場合、MIT オブジェクト ツリー全体が含まれます。管理者は、MIT オブジェクト階層にカスタム ドメイン タグを割り当てることができます。たとえば、管理者は「solar」という名前のテナントにドメイン タグ「solar」を割り当てることができます。MIT 内では、特定のオブジェクトだけがセキュリティ ドメインとしてタグ付けできます。たとえば、

テナントはセキュリティ ドメインとしてタグ付けすることができますが、テナント内のオブジェクトはできません。

ユーザを作成してロールを割り当てても、アクセス権は有効になりません。1 つ以上のセキュリティ ドメインにそのユーザを割り当てることも必要です。デフォルトでは、ACI ファブリックには事前作成された以下の 2 つの特殊なドメインが含まれています。

- `All`：MIT 全体へのアクセスを許可
- `Infra`：ファブリック アクセス ポリシーなどの、ファブリック インフラストラクチャのオブジェクトおよびサブツリーへのアクセスを許可

（注） ユーザのクレデンシャルが許可しない管理対象オブジェクトの読み取り操作の場合、「DN/Class Unauthorized to read」ではなく「DN/Class Not Found」というエラーが返されます。ユーザのクレデンシャルが許可しない管理対象オブジェクトへの書き込み操作の場合、「HTTP 401 Unauthorized」というエラーが返されます。GUI では、ユーザのクレデンシャルが許可しないアクションの場合、表示されないか、またはグレー表示されます。

事前に定義された一連の管理対象オブジェクト クラスをドメインに関連付けることができます。これらのクラスがオーバーラップすることはできません。ドメインの関連付けをサポートするクラスの例：

- レイヤ 2 およびレイヤ 3 のネットワークで管理されたオブジェクト
- ネットワーク プロファイル（物理、レイヤ 2、レイヤ 3、管理など）
- Quality of Service（QoS）ポリシー

ドメインに関連付けることができるオブジェクトが作成されると、ユーザは、ユーザのアクセス権の範囲内でオブジェクトにドメインを割り当てる必要があります。ドメインの割り当てはいつでも変更できます。

仮想マシン管理（VMM）ドメインがセキュリティ ドメインとしてタグ付けされている場合、セキュリティ ドメイン内のユーザは、対応するタグ付き VMM ドメインにアクセスできます。たとえば、solar という名前のテナントに sun というセキュリティ ドメインのタグが付いており、VMM ドメインにも sun というセキュリティ ドメインのタグが付いている場合、solar テナント内のユーザは各自のアクセス権限に従って VMM ドメインにアクセスできます。

ローカル ユーザの設定

初期の設定スクリプトで、管理者アカウントが設定され、管理者はシステム起動時の唯一のユーザとなります。APIC は、きめ細かなロールベースのアクセス コントロール システムをサポートしており、そのシステムでは、権限が少ない管理者以外のユーザを含め、ユーザ アカウントをさまざまなロールで作成することができます。

GUI を使用したローカル ユーザの設定

（注） このタスク例のビデオを視聴するには、ビデオを掲載している Web ページ を参照してください。

はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要に応じて、ユーザがアクセスするセキュリティ ドメインが定義されていること。たとえば、新しい使用アカウントがテナントにアクセスすることを制限する場合は、それに従ってテナント ドメインにタグ付けします。
- 以下を行うことができる APIC ユーザ アカウントを使用できること。
  - TACACS+ と TACACS+ プロバイダー グループの作成。
  - ターゲット セキュリティ ドメインでのローカル ユーザ アカウントの作成。ターゲット ドメインが `all` である場合、新しいローカル ユーザの作成に使用するログイン アカウントは、`all` にアクセスできるファブリック全体の管理者である必要があります。ターゲット ドメインがテナントである場合、新しいローカル ユーザの作成に使用するログイン アカウントは、ターゲット テナント ドメインに対する完全な読み取り/書き込みアクセス権を持つテナント管理者である必要があります。

手順の概要

1. メニュー バーで、[ADMIN] > [AAA] を選択します。
2. [Navigation] ペインで、[AAA Authentication] をクリックします。
3. [Work] ペインのデフォルトの [Authentication] フィールドで、[Realm] フィールドが [Local] と表示されていることを確認します。
4. [Navigation] ペインで、[Security Management] > [Local Users] を展開します。
5. [Navigation] ペインで、[Create Local User] を右クリックします。
6. [Security] ダイアログボックスで、ユーザに必要なセキュリティ ドメインを選択し、[Next] をクリックします。
7. [Roles] ダイアログボックスで、ユーザのロールを選択するためのオプション ボタンをクリックし、[Next] をクリックします。
8. [User Identity] ダイアログボックスで、次の操作を実行します。
9. [Navigation] ペインで、作成したユーザの名前をクリックします。[Work] ペインで、[Security Domains] 領域のユーザの横にある [+] 記号を展開します。

手順の詳細

ステップ 1 メニュー バーで、[ADMIN] > [AAA] を選択します。

ステップ 2 [Navigation] ペインで、[AAA Authentication] をクリックします。

ステップ 3 [Work] ペインのデフォルトの [Authentication] フィールドで、[Realm] フィールドが [Local] と表示されていることを確認します。

ステップ 4 [Navigation] ペインで、[Security Management] > [Local Users] を展開します。
管理ユーザはデフォルトで存在しています。

ステップ 5 [Navigation] ペインで、[Create Local User] を右クリックします。

ステップ 6 [Security] ダイアログボックスで、ユーザに必要なセキュリティ ドメインを選択し、[Next] をクリックします。

ステップ 7 [Roles] ダイアログボックスで、ユーザのロールを選択するためのオプション ボタンをクリックし、[Next] をクリックします。
読み取り専用または読み取り/書き込み権限を提供できます。

ステップ 8 [User Identity] ダイアログボックスで、次の操作を実行します。

a) [Login ID] フィールドで、ID を追加します。

b) [Password] フィールドにパスワードを入力します。
ユーザがパスワードを設定する時点で、APIC は以下の基準に対してパスワードを検証します。

- パスワードの最小長は 8 文字です。
- パスワードの最大長は 64 文字です。
- 連続して繰り返される文字は 3 文字未満です。
- 小文字、大文字、数字、記号の文字種のうち少なくとも 3 種類の文字が含まれている必要があります。
- 簡単に推測できるパスワードは使用しません。
- ユーザ名やユーザ名を逆にしたものは使用できません。
- cisco、isco、またはこれらの文字列の並べ替えを変化させたものや、それらの文字の大文字化の変更により取得される変形語であってはなりません。

c) [Confirm Password] フィールドで、パスワードを確認します。

d) [Finish] をクリックします。

ステップ 9 [Navigation] ペインで、作成したユーザの名前をクリックします。[Work] ペインで、[Security Domains] 領域のユーザの横にある [+] 記号を展開します。
ユーザのアクセス権限が表示されます。

リモート ユーザの設定

ローカルユーザを設定する代わりに、APICを一元化された企業クレデンシャルのデータセンターに向けることができます。APIC は、Lightweight Directory Access Protocol（LDAP）、Active Directory、RADIUS、および TACACS+ をサポートしています。

外部認証プロバイダーを通じて認証されたリモート ユーザを設定するには、次の前提条件を満たす必要があります。

- DNS 設定は、RADIUS サーバのホスト名ですでに名前解決されている必要があります。
- 管理サブネットを設定する必要があります。

外部認証サーバの AV ペア

Cisco 属性/値（AV）ペアを既存のユーザ レコードに追加して、ユーザ権限を APIC コントローラに伝播することができます。Cisco AV ペアは、APIC ユーザに対してロールベース アクセス コントロール（RBAC）のロールと権限を指定するために使用する単一の文字列です。オープンRADIUS サーバ（/etc/raddb/users）の設定例は次のとおりです。

```
aaa-network-admin Cleartext-Password := "<password>"
Cisco-avpair = "shell:domains = all/aaa/read-all(16001)"
```

AV ペアを割り当てるためのベスト プラクティス

ベストプラクティスとして、シスコは、bash シェルでユーザに割り当てられる AV ペアには 16000 ～ 23999 の範囲の一意の UNIX ユーザ ID を割り当てることを推奨します（SSH、Telnet または Serial/KVM のコンソールを使用）。Cisco AV ペアが UNIX ユーザ ID を提供しない状況が発生すると、そのユーザにはユーザ ID 23999 または範囲内の類似した番号が割り当てられます。これにより、そのユーザのホーム ディレクトリ、ファイル、およびプロセスに UNIX ID 23999 を持つリモート ユーザがアクセスできるようになってしまいます。

外部認証サーバの AV ペアの設定

属性/値（AV）のペア文字列のカッコ内の数字は、セキュア シェル（SSH）または Telnet を使用してログインしたユーザの UNIX ユーザ ID として使用されます。

手順の概要

1. 外部認証サーバの AV ペアの設定

手順の詳細

外部認証サーバの AV ペアの設定

Cisco AV ペアの定義は次のとおりです（シスコは、UNIX ユーザ ID が指定されているかどうかにかかわらず AV ペアをサポートします）

例：

```
* shell:domains =
domainA/writeRole1|writeRole2|writeRole3/readRole1|readRole2,domainB/writeRole1|writeRole2|writeRole3/readRole1|readRole2
         * shell:domains =
domainA/writeRole1|writeRole2|writeRole3/readRole1|readRole2,domainB/writeRole1|writeRole2|writeRole3/readRole1|readRole2(8101)

These are the boost regexes supported by APIC:
uid_regex("shell:domains\\s*[=:]\\s*((\\S+?/\\S*?/\\S*?),\\S+?/\\S*?/\\S*?){0,31})(\\(\\d+\\))$");
regex("shell:domains\\s*[=:]\\s*((\\S+?/\\S*?/\\S*?),\\S+?/\\S*?/\\S*?){0,31})$");
```

次に、例を示します。

```
shell:domains = coke/tenant-admin/read-all,pepsi//read-all(16001)
```

TACACS+ アクセス用の APIC の設定

はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- TACACS+ サーバのホスト名または IP アドレス、ポート、およびキーを使用できること。
- APIC 管理 EPG を使用できること。
- 以下を行うことができる APIC ユーザ アカウントを使用できること。

◦ TACACS+ プロバイダーと TACACS+ プロバイダー グループの作成。

図 *1*：*TACACS+* プロバイダー

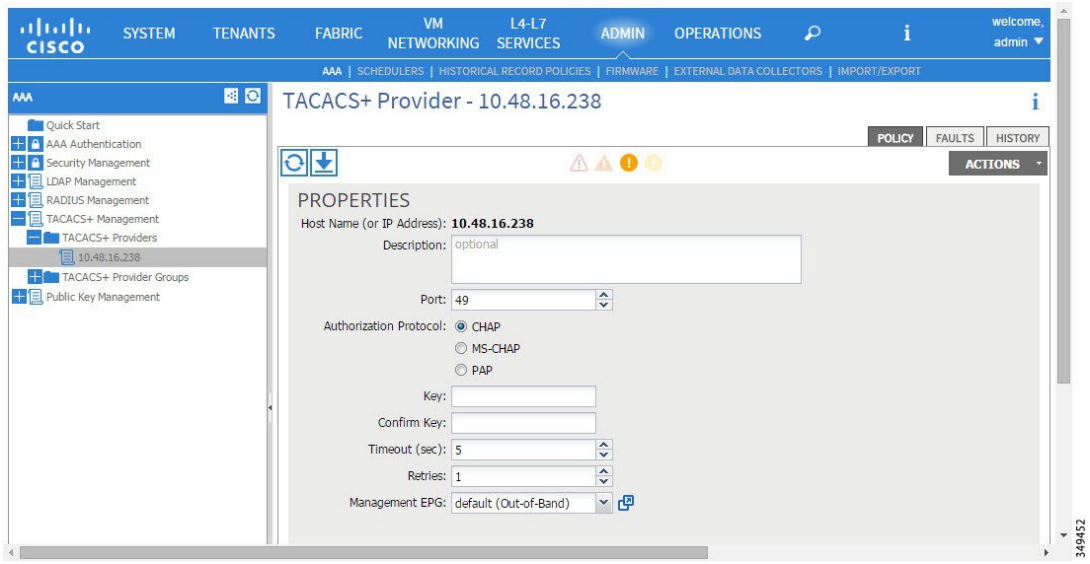
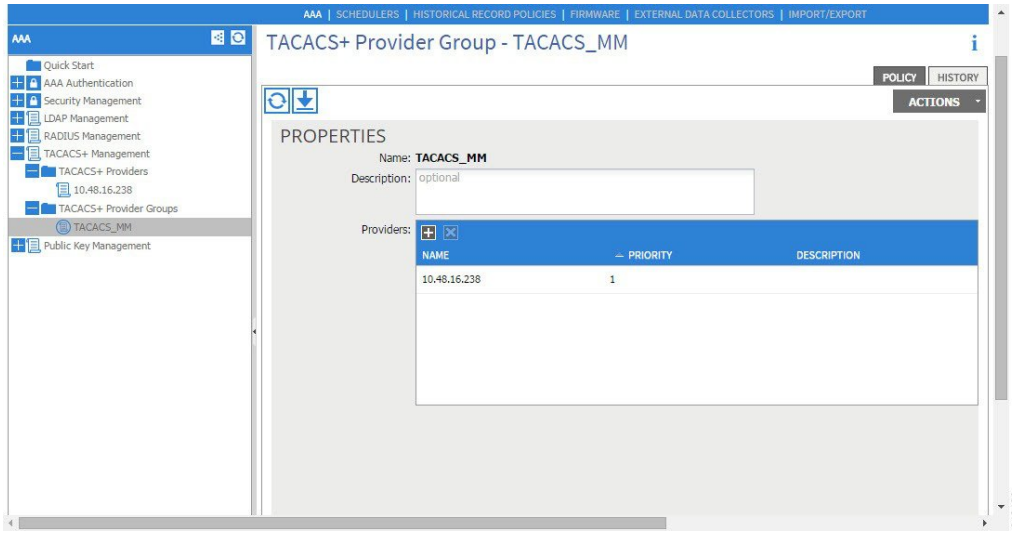
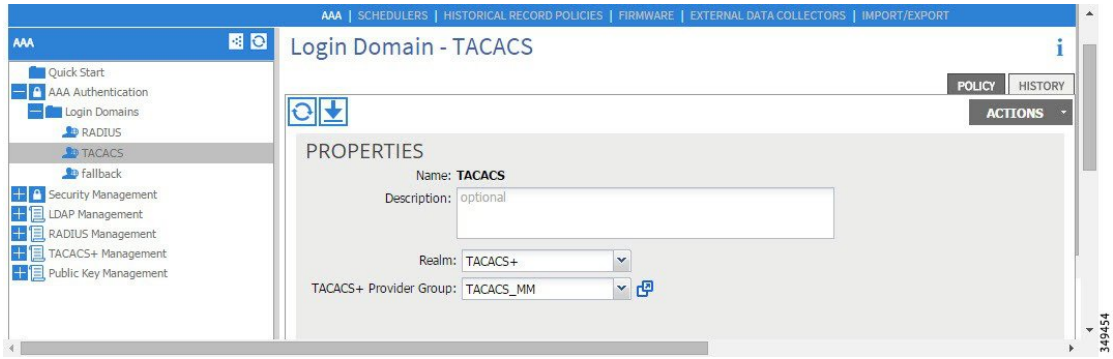


図 *2*：*TACACS+* プロバイダー グループ



- TACACS+ ログイン ドメインの作成。

図 3 : *TACACS+* の *AAA* ログイン ドメイン



ステップ 1 APIC で、[TACACS+ Provider] を作成します。

a) APIC メニュー バーで、[ADMIN] > [AAA] の順にクリックします。

b) [Navigation] ペインで、[+] アイコンをクリックして [TACACS+ Managment] オプションを展開します。

c) [Navigation] ペインで、[TACACS+ Providers] オプションを右クリックし、[Create TACACS+ Provider] を選択します。

d) TACACS+ ホスト名（または IP アドレス）、ポート、認証プロトコル、キー、および管理 EPG を指定します。

（注） APICがインバンド管理接続用に設定されている場合、TACACS+アクセス用にアウトオブバンド管理 EPG を選択しても有効にはなりません。また、インバンド管理 EPG 上のアウトオブバンドで TACACS+ サーバに接続することはできますが、TACACS+ サーバのスタティック ルートの設定が必要です。以下の Cisco ACS の設定手順例では、APIC インバンド IP アドレスを使用します。

ステップ 2 TACACS+ プロバイダー グループを作成します。

a) [Navigation] ペインで、[TACACS+ Provider Groups] オプションを右クリックし、[Create TACACS+ Provider Group] を選択します。

b) 必要に応じて、TACACS+ プロバイダー グループ名、説明、およびプロバイダーを指定します。

ステップ 3 TACACS+ の [Login Domain] を作成します。

a) [Navigation] ペインで、[+] アイコンをクリックして [AAA Authentication] オプションを展開します。

b) [Navigation] ペインで、[Login Domains] オプションを右クリックし、[Create Login Domain] を選択します。

c) 必要に応じて、ログイン ドメイン名、説明、レルム、およびプロバイダー グループを指定します。

次の作業

これで、APIC TACACS+ 設定手順は完了です。次に、RAIDUS サーバも使用する場合は、RADIUS 用の APIC の設定も行います。TACACS+ サーバのみを使用する場合は、次の ACS サーバ設定に関するトピックに進みます。

RADIUS アクセス用の APIC の設定

はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- RADIUS サーバのホスト名または IP アドレス、ポート、認証プロトコル、およびキーを使用できること。
- APIC 管理 EPG を使用できること。
- 以下を行うことができる APIC ユーザ アカウントを使用できること。

- RADIUS プロバイダーと RADIUS プロバイダー グループの作成。

図 *4*：*RADIUS* プロバイダー

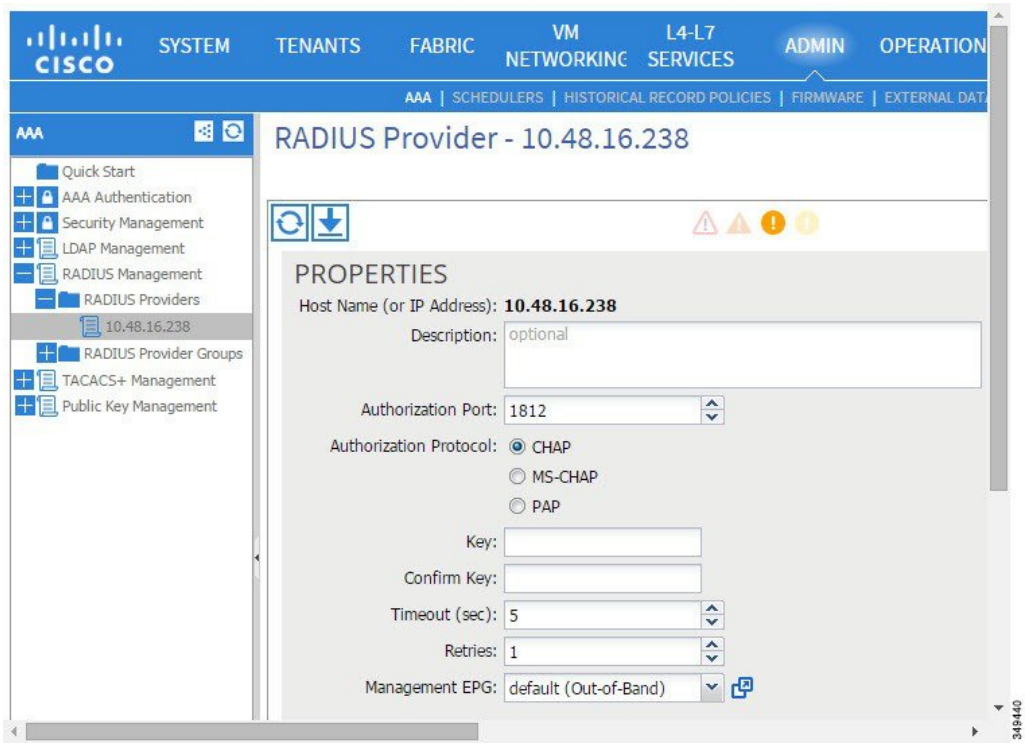
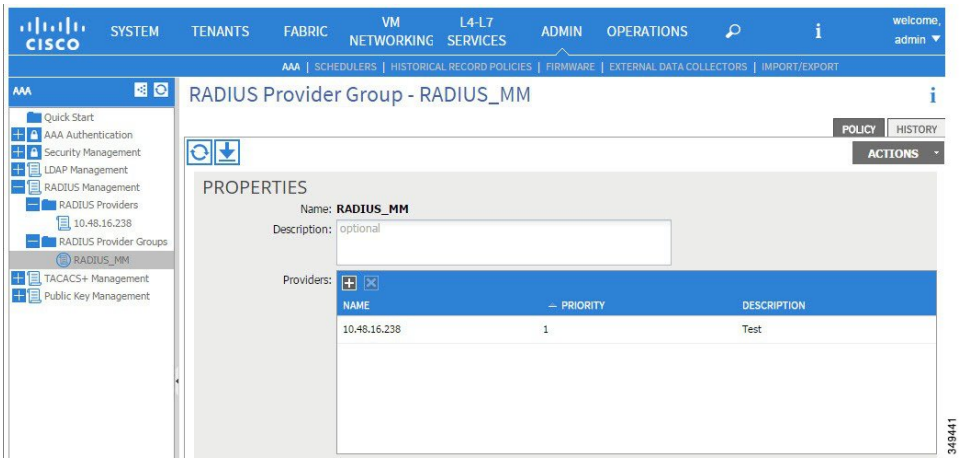
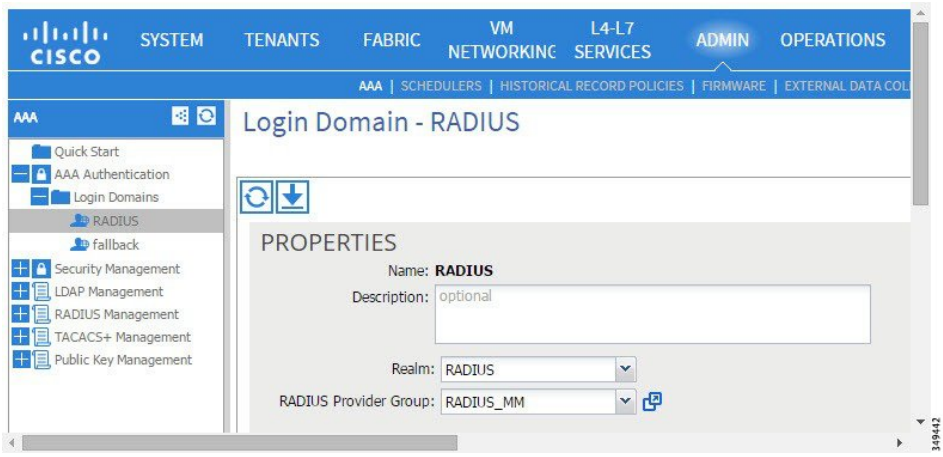


図 *5*：*RADIUS* プロバイダー グループ



- RADIUS ログイン ドメインの作成。

図 *6*： *RADIUS* の *AAA* ログイン ドメイン



ステップ 1 APIC で、[RADIUS Provider] を作成します。

a) APIC メニュー バーで、[ADMIN] > [AAA] の順にクリックします。

b) [Navigation] ペインで、[+] アイコンをクリックして [RADIUS Managment] オプションを展開します。

c) [Navigation] ペインで、[RADIUS Providers] オプションを右クリックし、[Create RADIUS Provider] を選択します。

d) RADIUS ホスト名（または IP アドレス）、ポート、プロトコル、および管理 EPG を指定します。

（注） APIC がインバンド管理接続用に設定されている場合、RADIUS アクセス用にアウトオブバンド管理 EPG を選択しても有効にはなりません。また、インバンド管理 EPG 上のアウトオブバンドで RADIUS サーバに接続することはできますが、RADIUS サーバのスタティック ルートの設定が必要です。以下の Cisco ACS の設定手順例では、APIC インバンド IP アドレスを使用します。

ステップ 2 [RADIUS Provider Group] を作成します。

a) [Navigation] ペインで、[RADIUS Provider Groups] オプションを右クリックし、[Create RADIUS Provider Group] を選択します。

b) 必要に応じて、RADIUS プロバイダー グループ名、説明、およびプロバイダーを指定します。

ステップ 3 RADIUS のログイン ドメインを作成します。

a) [Navigation] ペインで、[+] アイコンをクリックして [AAA Authentication] オプションを展開します。

b) [Navigation] ペインで、[Login Domains] オプションを右クリックし、[Create Login Domain] を選択します。

c) 必要に応じて、ログイン ドメイン名、説明、レルム、およびプロバイダー グループを指定します。

次の作業

これで、APIC RADIUS 設定手順は完了です。次に、RADIUS サーバを設定します。

APIC にアクセスする RADIUS および TACACS+ 用の Cisco Secure Access Control Server の設定

はじめる前に

- Cisco Secure Access Control Server（ACS）バージョン 5.5 がインストールされ、オンラインになっていること。
- APIC インバンド IP アドレスを使用できること。
- APIC の RADIUS キーまたは TACACS+ キーを使用できること（両方を設定する場合は両方のキー）。
- APIC コントローラがインストールされ、オンラインになっていること。APIC クラスタが形成されて正常に動作していること。
- RADIUS または TACACS+ のポート、認証プロトコル、およびキーを使用できること。
- 以下を行うことができる ACS ユーザ アカウントを使用できること。
  - APIC ACS クライアントの作成。

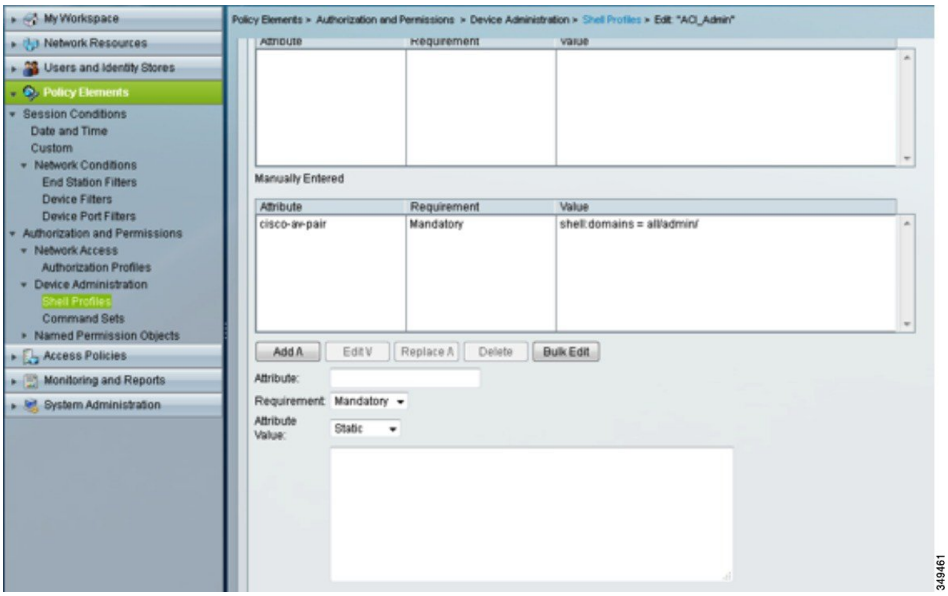
図 *7* : *APIC ACS* クライアント

- ユーザの定義と適切な ID グループへのマッピング。

図 *8*：*ID* グループへのユーザのマッピング

- APIC RBAC ロールを割り当てるための RADIUS ポリシー要素または TACACS+ シェル プロファイルの作成

図 *9*：*TACACS+* シェル プロファイル



ステップ 1　APIC をクライアントとして設定するには、ACS サーバにログインします。

a) [Network Resources] > [Network Devices Groups] > [Network Devices and AAA Clients] に移動します。
b) クライアント名と APIC インバンド IP アドレスを指定し、TACACS+ または RADIUS（または両方）の認証オプションを選択します。

（注） RADIUS または TACACS+ のみの認証が必要な場合は、必要なオプションのみを選択します。

c) 共有秘密（キー）や認証オプションに適したポートなど、認証の詳細を指定します。

（注） [Shared Secret] は APIC [Provider] キーと一致する必要があります。

ステップ 2 ID グループを作成します。

a) [Users and Identity Stores] > [Internal Groups] オプションに移動します。
b) 必要に応じて、[Name] と [Parent Group] を指定します。

ステップ 3 ユーザを ID グループにマッピングします。

a) [Navigation] ペインで、[Users and Identity Stores] > [Internal Identity Stores] > [Users] オプションをクリックします。
b) 必要に応じて、ユーザの [Name] と [Identity Group] を指定します。

ステップ 4 ポリシー要素を作成します。

a) [Policy Elements] オプションに移動します。
b) RADIUS の場合、[Authorization and Permissions] > [Network Access] > [Authorization Profiles Name] を指定します。TACACS+ の場合、必要に応じて、[Authorization and Permissions] > [Device Administration] > [Shell Profile Name] を指定します。
c) RADIUS の場合、必要に応じて、[Attribute] には「`cisco-av-pair`」、[Type] には「string」、[Value] には「shell:domains = <domain>/<role>/,<domain>// role」と指定します。TACACS+ の場合、必要に応じて、[Attribute] には「`cisco-av-pair`」、[Requirement] には「Mandatory」、[Value] には「shell:domains = <domain>/<role>/,<domain>// role」と指定します。
たとえば、*cisco-av-pair* が shell:domains = solar/admin/,common// read-all(16001) である場合、「solar」は ACI テナント、「admin」は solor というテナント内すべてに対する書き込み権限をこのユーザに付与するロール、「common」は ACI テナント common、「read-all(16001)」は ACI テナント common のすべてに対する読み取り権限をこのユーザに付与するロールです。

ステップ 5 サービス選択ルールを作成します。

a) RADIUS の場合、サービス選択ルールを作成して ID グループをポリシー要素に関連付けるには、[Access Policies] > [Default Device Network Access Identity] > [Authorization] に移動し、ルールの [Name]、[Status]、および [Conditions] を指定し、必要に応じて「`Internal Users:UserIdentityGroup in ALL Groups:<identity group name>`」を追加します。
b) TACACS+ の場合、サービス選択ルールを作成して ID グループをシェル プロファイルに関連付けるには、[Access Policies] > [Default Device Admin Identity] > [Authorization] に移動します。ルールの [Name] と [Conditions] を指定し、必要に応じて [Shell Profile] を選択します。

次の作業

新しく作成された RADIUS および TACACS+ のユーザを使用して、APIC にログインします。割り当てられた RBAC ロールと権限に従って正しい APIC セキュリティ ドメインにアクセスできることを確認します。ユーザは、明示的に許可されていない項目にアクセスできてはなりません。読み取り/書き込みアクセス権が、そのユーザに設定されたものと一致している必要があります。

APIC アクセス用の Windows Server 2008 LDAP の設定

はじめる前に

- 最初に LDAP サーバを設定し、次に APIC を LDAP アクセス用に設定します。
- Microsoft Windows Server 2008 がインストールされ、オンラインになっていること。
- Microsoft Windows Server 2008 サーバ マネージャの ADSI Edit ツールがインストールされていること。ADSI Edit をインストールするには、Windows Server 2008 サーバ マネージャのヘルプに記載されている手順に従ってください。
- `AciCiscoAVPair` の属性の指定：Common Name = AciCiscoAVPair、LDAP Display Name = AciCiscoAVPair、Unique X500 Object ID = 1.3.6.1.4.1.9.22.1、Description = AciCiscoAVPair、Syntax = Case Sensitive String。

（注） LDAP 設定のベスト プラクティスは、属性文字列として AciCiscoAVPair を使用することです。これにより、オブジェクト識別子（OID）の重複を許可しない一般的な LDAP サーバの制限に関連した問題が回避されます。つまり、ciscoAVPair OID がすでに使用されている場合です。

- 以下を行うことができる Microsoft Windows Server 2008 ユーザ アカウントを使用できること。
  - ADSI Edit を実行して `AciCiscoAVPair` 属性を Active Directory（AD）スキーマに追加する。
  - `AciCiscoAVPair` 属性に対するアクセス許可を持つように Active Directory LDAP ユーザを設定する。

ステップ 1 ドメイン管理者として Active Directory（AD）サーバにログインします。

ステップ 2 AD スキーマに `AciCiscoAVPair` 属性を追加します。

a) [Start] > [Run] に移動し、「mmc」と入力し、Enter を押します。
Microsoft Management Console（MMC）が開きます。

b) [File] > [Add/Remove Sanp-in] > [Add] に移動します。

c) [Add Standalonee Snap-in] ダイアログボックスで、[Active Directory Schema] を選択し、[Add] をクリックします。
MMC コンソールが開きます。
d) [Attributes] フォルダを右クリックし、[Create Attribute] オプションを選択します。
[Create New Attribute] ダイアログボックスが開きます。
e) [] に「AciCiscoAVPair」、[LDAP Display Name] に「AciCiscoAVPair」、[Unique X500 Object ID] に「1.3.6.1.4.1.9.22.1」と入力し、[Syntax] で「Case Sensitive String」を選択します。
f) [OK] をクリックして、属性を保存します。

ステップ 3 [User Properties] クラスを [CiscoAVPair] 属性が含まれるように更新します。

a) MMC コンソールで、[Classes] フォルダを展開し、[user] クラスを右クリックし、[Properties] を選択します。
[user Properties] ダイアログボックスが開きます。
b) [Attributes] タブをクリックし、[Optional] リストから「CiscoAVPair」を選択し、[Add] をクリックします。
[Select Schema Object] ダイアログボックスが開きます。
c) [Select a schema object:] リストで、「CiscoAVPair」を選択し、[Apply] をクリックします。
d) MMC コンソールで、[Active Directory Schema] を右クリックし、[Reload the Schema] を選択します。

ステップ 4 AciCiscoAVPair 属性のアクセス許可を設定します。
LDAP には AciCiscoAVPair 属性が含まれているため、LDAP ユーザに APICRBAC ロールを割り当てることにより APIC アクセス許可を付与する必要があります。

a) [ADSI Edit] ダイアログ ボックスで、APIC にアクセスする必要があるユーザを見つけます。
b) ユーザ名を右クリックし、[Properties] を選択します。
[<user> Properties] ダイアログボックスが開きます。
c) [Attribute Editor] タブをクリックし、「*AciCiscoAVPair*」属性を選択し、[Value] に「shell:domains = <domain>/<role>/,<domain>// role」と入力します。
たとえば、*AciCiscoAVPair* が shell:domains = solar/admin/,common// read-all(16001) である場合、「solar」は ACI テナント、「admin」は solor というテナント内すべてに対する書き込み権限をこのユーザに付与するロール、「common」は ACI テナント common、「read-all(16001)」は ACI テナント common のすべてに対する読み取り権限をこのユーザに付与するロールです。
d) [OK] をクリックして変更を保存し、[<user> Properties] ダイアログボックスを閉じます。

LDAP サーバは APIC にアクセスするように設定されます。

次の作業

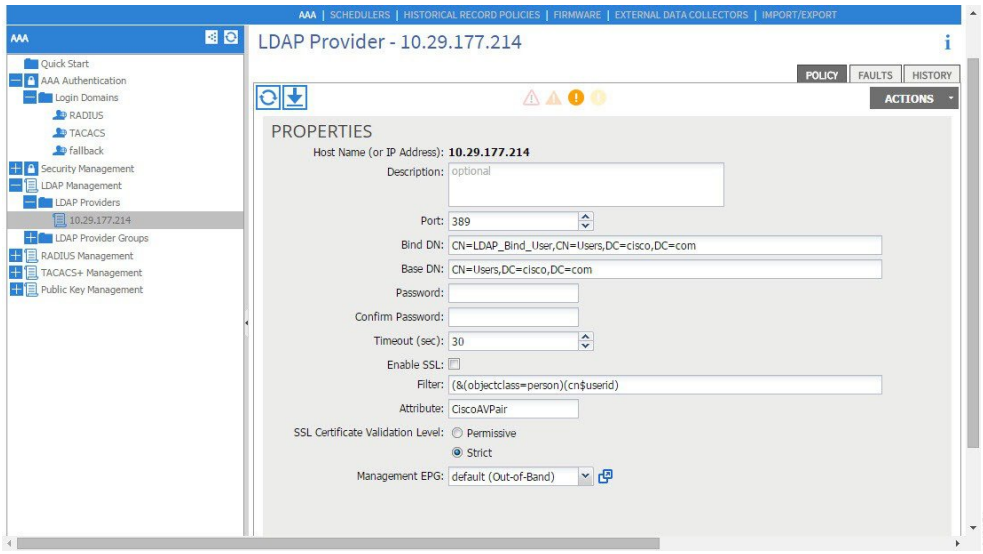
APIC を LDAP アクセス用に設定します。

LDAP アクセス用の APIC の設定

はじめる前に

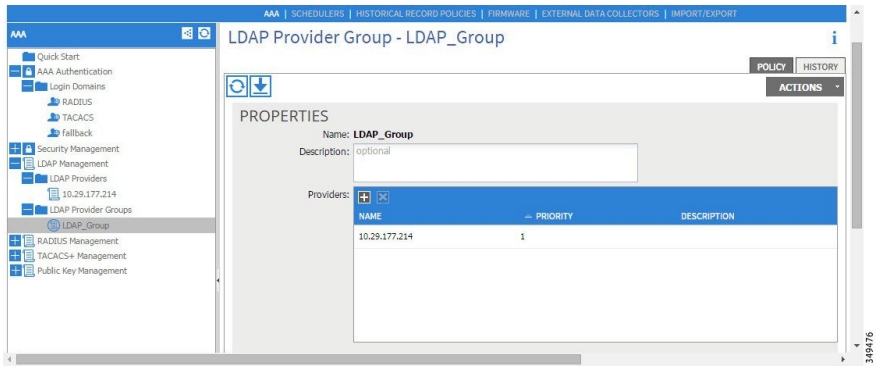
- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- LDAP サーバのホスト名または IP アドレス、ポート、バインド DN、ベース DN、およびパスワードを使用できること。
- APIC 管理 EPG を使用できること。
- 以下を行うことができる APIC ユーザ アカウントを使用できること。
  - LDAP プロバイダーと LDAP プロバイダー グループの作成。

図 *10*： *LDAP* プロバイダー



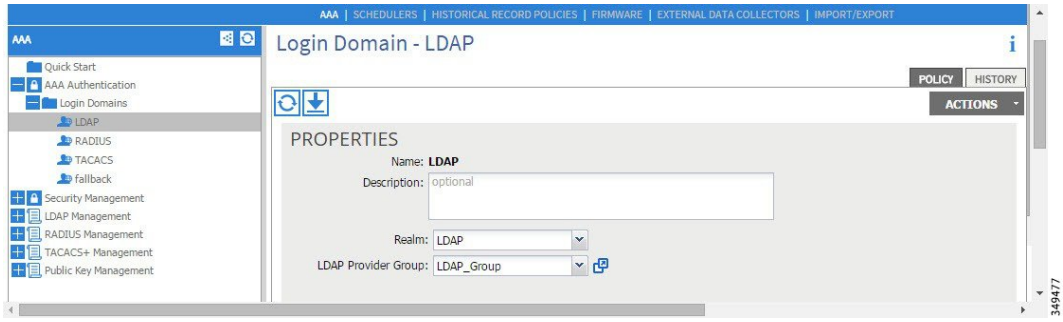
（注） バインド DN は、APIC が LDAP サーバにログインするために使用する文字列です。APICは、ログインしようとするリモートユーザを検証するためにこのアカウントを使用します。ベース DN は LDAP サーバのコンテナの名前とパスであり、そこで APIC がリモート ユーザ アカウントを検索します。これはパスワードが検証される場所です。フィルタを使用して、*cisco-av-pair* に使用することを APIC が 要求している属性を見つけます。これには、APIC で使用するユーザ認証と割り当て済み RBAC ロールが含まれます。APIC は、この属性を LDAP サーバに要求します。

図 *11*： *LDAP* プロバイダー グループ



◦ LDAP ログイン ドメインの作成。

図 *12*： *LDAP* の *AAA* ログイン ドメイン



ステップ 1 APIC で、LDAP プロバイダーを設定します。

a) APIC メニュー バーで、[ADMIN] > [AAA] の順にクリックします。

b) [Navigation] ペインで、[+] アイコンをクリックして [LDAP Managment] オプションを展開します。

c) [Navigation] ペインで、[LDAP Providers] オプションを右クリックし、[Create LDAP Provider] を選択します。

d) LDAP ホスト名（または IP アドレス）、ポート、バインド DN、ベース DN、パスワード、および管理 EPG を指定します。

（注） APIC がインバンド管理接続用に設定されている場合、LDAP アクセス用にアウトオブバンド管理 EPG を選択しても有効にはなりません。また、インバンド管理 EPG 上のアウトオブバンドで LDAP サーバに接続することはできますが、LDAP サーバのスタティック ルートの設定が必要です。本書の設定手順例では、APIC インバンド管理 EPG を使用します。

ステップ 2 APICで、LDAP プロバイダー グループを設定します。

a) [Navigation] ペインで、[LDAP Provider Groups] オプションを右クリックし、[Create LDAP Provider Group] を選択します。

b) 必要に応じて、LDAP プロバイダー グループ名、説明、およびプロバイダーを指定します。

ステップ 3 APIC で、LDAP のログイン ドメインを設定します。

a) [Navigation] ペインで、[+] アイコンをクリックして [AAA Authentication] オプションを展開します。

b) [Navigation] ペインで、[Login Domains] オプションを右クリックし、[Create Login Domain] を選択します。

c) 必要に応じて、ログイン ドメイン名、説明、レルム、およびプロバイダー グループを指定します。

次の作業

これで、APIC LDAP 設定手順は完了です。次に、APIC LDAP ログイン アクセスをテストします。

Cisco AV ペアが欠落しているか不良であるリモート ユーザのデフォルトの動作の変更

ステップ 1 メニュー バーで、[ADMIN] > [AAA] の順にクリックします。

ステップ 2 [Navigation] ペインで、[AAA Authentication] をクリックします。

ステップ 3 [Work] ペインの [Properties] 領域で、[Remote user login policy] ドロップダウン リストから、[Assign Default Role] を選択します。
デフォルト値は [No Login] です。[Assign Default Role] オプションは、Cisco AV ペアが欠落しているか不良であるユーザに最小限の読み取り専用権限を割り当てます。不正な AV ペアは、解析ルール適用時に問題があった AV ペアです。

署名ベースのトランザクションについて

Cisco ACI ファブリックの APIC コントローラは、ユーザを認証するためにさまざまな方法を提供します。

主要な認証方式ではユーザ名とパスワードが使用され、APIC REST API は APIC に対するその後のアクセスに使用できる認証トークンを返します。これは、HTTPS が使用不可であるか有効でない状況では安全でないと見なされます。

提供されている別の認証形式では、トランザクションごとに計算される署名が活用されます。その署名の計算には秘密キーが使用され、そのキーは安全な場所に保管して秘密にしておく必要があります。APIC がトークン以外の署名が付いた要求を受信すると、APIC は X.509 証明書を活用して署名を確認します。署名ベースの認証では、APIC に対するすべてのトランザクションに新しく計算された署名が必要です。これは、ユーザがトランザクションごとに手動で行うタスクではありません。理想的には、この機能は APIC と通信するスクリプトまたはアプリケーションで使用する必要があります。この方法では、攻撃者がユーザ クレデンシャルを偽装またはなりすますためには RSA/DSA キーを解読する必要があるため、最も安全です。

（注） また、リプレイ攻撃を防ぐためには HTTPS を使用する必要があります。

認証に X.509 証明書ベースの署名を使用する前に、次の必須タスクが完了していることを確認します。

1. OpenSSL または同様のツールを使用して X.509 証明書と秘密キーを作成します。
2. APIC のローカル ユーザを作成します（ローカル ユーザがすでに利用可能である場合、このタスクはオプションです）。
3. APIC のローカル ユーザに X.509 証明書を追加します。

注意事項と制約事項

次の注意事項と制約事項に従ってください。

- ローカル ユーザはサポートされます。リモート AAA ユーザはサポートされません。
- APIC GUI は証明書認証方式をサポートしません。
- WebSocket と eventchannel は X.509 要求では動作しません。
- サードパーティにより署名された証明書はサポートされません。自己署名証明書を使用します。

X.509 証明書と秘密キーの生成

ステップ 1 OpenSSL コマンドを入力して、X.509 証明書と秘密キーを生成します。

例：

```
$ openssl req -new -newkey rsa:1024 -days 36500 -nodes -x509 -keyout userabc.key -out userabc.crt
 -subj '/CN=User ABC/O=Cisco Systems/C=US'
```

（注）
- X.509 証明書が生成されると、APIC のユーザプロファイルに追加され、署名の確認に使用されます。秘密キーは、署名を生成するためにクライアントによって使用されます。
- 証明書には公開キーは含まれていますが、秘密キーは含まれていません。公開キーは、計算された署名を確認するために APIC によって使用される主要な情報です。秘密キーが APIC に保存されることはありません。このキーを秘密にしておく必要があります。

ステップ 2 OpenSSL を使用して証明書のフィールドを表示します。

例：

```
$ openssl x509 -text -in userabc.crt
        Certificate:
            Data:
                Version: 3 (0x2)
                Serial Number:
                    c4:27:6c:4d:69:7c:d2:b6
                Signature Algorithm: sha1WithRSAEncryption
                Issuer: CN=User ABC, O=Cisco Systems, C=US
                Validity
                    Not Before: Jan 12 16:36:14 2015 GMT
                    Not After : Dec 19 16:36:14 2114 GMT
                Subject: CN=User ABC, O=Cisco Systems, C=US
                Subject Public Key Info:
                    Public Key Algorithm: rsaEncryption
                    RSA Public Key: (1024 bit)
                        Modulus (1024 bit):
                            00:92:35:12:cd:2b:78:ef:9d:ca:0e:11:77:77:3a:
                            99:d3:25:42:94:b5:3e:8a:32:55:ce:e9:21:2a:ff:
                            e0:e4:22:58:6d:40:98:b1:0d:42:21:db:cd:44:26:
                            50:77:e5:fa:b6:10:57:d1:ec:95:e9:86:d7:3c:99:
                            ce:c4:7f:61:1d:3c:9e:ae:d8:88:be:80:a0:4a:90:
                            d2:22:e9:1b:25:27:cd:7d:f3:a5:8f:cf:16:a8:e1:
                            3a:3f:68:0b:9c:7c:cb:70:b9:c7:3f:e8:db:85:d8:
                            98:f6:e3:70:4e:47:e2:59:03:49:01:83:8e:50:4a:
                            5f:bc:35:d2:b1:07:be:ec:e1
                        Exponent: 65537 (0x10001)
                X509v3 extensions:
                    X509v3 Subject Key Identifier:
                        0B:E4:11:C7:23:46:10:4F:D1:10:4C:C1:58:C2:1E:18:E8:6D:85:34
                    X509v3 Authority Key Identifier:
                        keyid:0B:E4:11:C7:23:46:10:4F:D1:10:4C:C1:58:C2:1E:18:E8:6D:85:34
                        DirName:/CN=User ABC/O=Cisco Systems/C=US
                        serial:C4:27:6C:4D:69:7C:D2:B6

                    X509v3 Basic Constraints:
                        CA:TRUE
            Signature Algorithm: sha1WithRSAEncryption
                8f:c4:9f:84:06:30:59:0c:d2:8a:09:96:a2:69:3d:cf:ef:79:
                91:ea:cd:ae:80:16:df:16:31:3b:69:89:f7:5a:24:1f:fd:9f:
                d1:d9:b2:02:41:01:b9:e9:8d:da:a8:4c:1e:e5:9b:3e:1d:65:
                84:ff:e8:ad:55:3e:90:a0:a2:fb:3e:3e:ef:c2:11:3d:1b:e6:
                f4:5e:d2:92:e8:24:61:43:59:ec:ea:d2:bb:c9:9a:7a:04:91:
```

```
                8e:91:bb:9d:33:d4:28:b5:13:ce:dc:fe:c3:e5:33:97:5d:37:
                cc:5f:ad:af:5a:aa:f4:a3:a8:50:66:7d:f4:fb:78:72:9d:56:
                91:2c
        [snip]
```

ローカル ユーザの設定

GUI を使用したローカル ユーザの作成とユーザ証明書の追加

ステップ 1 メニュー バーで、[ADMIN] > [AAA] を選択します。

ステップ 2 [Navigation] ペインで、[AAA Authentication] をクリックします。

ステップ 3 [Work] ペインのデフォルトの [Authentication] フィールドで、[Realm] フィールドが [Local] と表示されていることを確認します。

ステップ 4 [Navigation] ペインで、[Security Management] > [Local Users] を展開します。
管理ユーザはデフォルトで存在しています。

ステップ 5 [Navigation] ペインで、[Local Users] をクリックし、[Create Local User] をクリックします。

ステップ 6 [Security] ダイアログボックスで、ユーザに必要なセキュリティ ドメインを選択し、[Next] をクリックします。

ステップ 7 [Roles] ダイアログボックスで、ユーザのロールを選択するためのオプション ボタンをクリックし、[Next] をクリックします。
読み取り専用または読み取り/書き込み権限を提供できます。

ステップ 8 [User Identity] ダイアログボックスで、次の操作を実行します。

a) [Login ID] フィールドで、ID を追加します。
b) [Password] フィールドにパスワードを入力します。
c) [Confirm Password] フィールドで、パスワードを確認します。
d) [Finish] をクリックします。

ステップ 9 [Navigation] ペインで、作成したユーザの名前をクリックします。[Work] ペインで、[Security Domains] 領域のユーザの横にある [+] 記号を展開します。
ユーザのアクセス権限が表示されます。

ステップ 10 [Work] ペインの [User Certificates] 領域で、ユーザ証明書の [+] 記号をクリックし、[Create X509 Certificate] 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、証明書の名前を入力します。
b) [Data] フィールドに、ユーザ証明書の詳細を入力します。
c) [Submit] をクリックします。

X509 証明書がローカル ユーザ用に作成されます。

REST API を使用したローカル ユーザの作成とユーザ証明書の追加

ローカル ユーザを作成し、ユーザ証明書を追加します。

例：

```
method: POST
        url: http://apic/api/node/mo/uni/userext/user-userabc.json
        payload:
        {
            "aaaUser": {
                "attributes": {
                    "name": "userabc",
                    "firstName": "Adam",
                    "lastName": "BC",
                    "phone": "408-525-4766",
                    "email": "userabc@cisco.com",
                },
                "children": [{
                    "aaaUserCert": {
                        "attributes": {
                            "name": "userabc.crt",
                         "data": "-----BEGIN CERTIFICATE-----\nMIICjjCCAfegAwIBAgIJAMQnbE <snipped
 content> ==\n-----END CERTIFICATE-----",
                        },
                        "children": []
                    },
                    "aaaUserDomain": {
                        "attributes": {
                            "name": "all",
                        },
                        "children": [{
                            "aaaUserRole": {
                                "attributes": {
                                    "name": "aaa",
                                    "privType": "writePriv",
                                },
                                "children": []
                            }
                        }, {
                            "aaaUserRole": {
                                "attributes": {
                                    "name": "access-admin",
                                    "privType": "writePriv",
                                },
                                "children": []
                            }
                        }, {
                            "aaaUserRole": {
                                "attributes": {
                                    "name": "admin",
                                    "privType": "writePriv",
                                },
                                "children": []
                            }
                        }, {
                            "aaaUserRole": {
                                "attributes": {
                                    "name": "fabric-admin",
                                    "privType": "writePriv",
                                },
                                "children": []
```

```
                    }
                }, {
                    "aaaUserRole": {
                        "attributes": {
                            "name": "nw-svc-admin",
                            "privType": "writePriv",
                        },
                        "children": []
                    }
                }, {
                    "aaaUserRole": {
                        "attributes": {
                            "name": "ops",
                            "privType": "writePriv",
                        },
                        "children": []
                    }
                }, {
                    "aaaUserRole": {
                        "attributes": {
                            "name": "read-all",
                            "privType": "writePriv",
                        },
                        "children": []
                    }
                }, {
                    "aaaUserRole": {
                        "attributes": {
                            "name": "tenant-admin",
                            "privType": "writePriv",
                        },
                        "children": []
                    }
                }, {
                    "aaaUserRole": {
                        "attributes": {
                            "name": "tenant-ext-admin",
                            "privType": "writePriv",
                        },
                        "children": []
                    }
                }, {
                    "aaaUserRole": {
                        "attributes": {
                            "name": "vmm-admin",
                            "privType": "writePriv",
                        },
                        "children": []
                    }
                }]
            }
        }]
    }
}
```

Python SDK を使用したローカル ユーザの作成

ローカル ユーザを作成します。

例：

```
#!/usr/bin/env python
from cobra.model.pol import Uni as PolUni
from cobra.model.aaa import UserEp as AaaUserEp
from cobra.model.aaa import User as AaaUser
from cobra.model.aaa import UserCert as AaaUserCert
from cobra.model.aaa import UserDomain as AaaUserDomain
from cobra.model.aaa import UserRole as AaaUserRole
from cobra.mit.access import MoDirectory
from cobra.mit.session import LoginSession
from cobra.internal.codec.jsoncodec import toJSONStr

APIC = 'http://10.10.10.1'
username = 'admin'
password = 'p@$$w0rd'

session = LoginSession(APIC, username, password)
modir = MoDirectory(session)
modir.login()

def readFile(fileName=None, mode="r"):
   if fileName is None:
      return ""
   fileData = ""
   with open(fileName, mode) as aFile:
      fileData = aFile.read()
   return fileData

# Use a dictionary to define the domain and a list of tuples to define
# our aaaUserRoles (roleName, privType)
# This can further be abstracted by doing a query to get the valid
# roles, that is what the GUI does

userRoles = {'all': [
               ('aaa', 'writePriv'),
               ('access-admin', 'writePriv'),
               ('admin', 'writePriv'),
               ('fabric-admin', 'writePriv'),
               ('nw-svc-admin', 'writePriv'),
               ('ops', 'writePriv'),
               ('read-all', 'writePriv'),
               ('tenant-admin', 'writePriv'),
               ('tenant-ext-admin', 'writePriv'),
               ('vmm-admin', 'writePriv'),
           ],
}

uni = PolUni('') # '' is the Dn string for topRoot
aaaUserEp = AaaUserEp(uni)
aaaUser = AaaUser(aaaUserEp, 'userabc', firstName='Adam',
                  email='userabc@cisco.com')

aaaUser.lastName = 'BC'
aaaUser.phone = '555-111-2222'
aaaUserCert = AaaUserCert(aaaUser, 'userabc.crt')
aaaUserCert.data = readFile("/tmp/userabc.crt")
# Now add each aaaUserRole to the aaaUserDomains which are added to the
# aaaUserCert
for domain,roles in userRoles.items():
   aaaUserDomain = AaaUserDomain(aaaUser, domain)
   for roleName, privType in roles:
       aaaUserRole = AaaUserRole(aaaUserDomain, roleName,
                                 privType=privType)
print toJSONStr(aaaUser, prettyPrint=True)

cr = ConfigRequest()
cr.addMo(aaaUser)
modir.commit(cr)
```

```
# End of Script to create a user
```

秘密キーを使用した署名の計算

はじめる前に

次の情報が用意されている必要があります。

- HTTP メソッド：GET、POST、DELETE
- 要求される REST API URI（クエリ オプションを含む）
- POST 要求の場合、APIC に送信される実際のペイロード
- ユーザの X.509 証明書の生成に使用される秘密キー
- APIC のユーザ X.509 証明書の宛先名

ステップ 1 HTTP メソッド、REST API URI、およびペイロードをこの順序で連結し、ファイルに保存します。OpenSSL で署名を計算するには、この連結データをファイルに保存する必要があります。この例では、ファイル名 payload.txt を使用します。秘密キーは userabc.key というファイルにあることに注意してください。

例：
GET の例：
```
GET http://10.10.10.1/api/class/fvTenant.json?rsp-subtree=children
```
POST の例：
```
POST http://10.10.10.1/api/mo/tn-test.json{"fvTenant": {"attributes": {"status": "deleted", "name":
 "test"}}}
```

ステップ 2 OpenSSL を使用して、秘密キーとペイロード ファイルを使用して署名を計算します。

例：
```
openssl dgst -sha256 -sign userabc.key payload.txt > payload_sig.bin
```
生成されたファイルには、複数行に印字された署名があります。

ステップ 3 Bash を使用して、署名から改行文字を取り除きます。

例：
```
$ tr -d '\n' < payload_sig.base64
P+OTqK0CeAZjl7+Gute2RlWw8OGgtzE0wsLlx8fIXXl4V79Zl7
Ou8IdJH9CB4W6CEvdICXqkv3KaQszCIC0+Bn07o3qF//BsIplZmYChD6gCX3f7q
IcjGX+R6HAqGeK7k97cNhXlWEoobFPe/oajtPjOu3tdOjhf/9ujG6Jv6Ro=
```
（注） これは、この特定の要求に関して APIC に送信される署名です。その他の要求では、独自の署名を計算する必要があります。

ステップ 4 署名を文字列内に配置し、APIC が署名をペイロードと照合して確認できるようにします。

この完全な署名が、要求のヘッダー内のクッキーとして APIC に送信されます。

例：

```
APIC-Request-Signature=P+OTqK0CeAZjl7+Gute2R1Ww8OGgtzE0wsLlx8f
IXXl4V79Zl7Ou8IdJH9CB4W6CEvdICXqkv3KaQszCIC0+Bn07o3qF//BsIplZmYChD6gCX3f
7qIcjGX+R6HAqGeK7k97cNhXlWEoobFPe/oajtPjOu3tdOjhf/9ujG6Jv6Ro=;
APIC-Certificate-Algorithm=v1.0; APIC-Certificate-Fingerprint=fingerprint;
APIC-Certificate-DN=uni/userext/user-userabc/usercert-userabc.crt
```

（注） ここで使用される DN が、次のステップの x509 証明書を含むユーザ認定オブジェクトの DN に一致する必要があります。

ステップ 5 署名を使用して APIC と通信するには、Python SDK の CertSession クラスを使用します。
次のスクリプトは、ACI Python SDK の CertSession クラスを使用して、署名を使用して APIC に要求する方法の例です。

例：

```
#!/usr/bin/env python
# It is assumed the user has the X.509 certificate already added to
# their local user configuration on the APIC
from cobra.mit.session import CertSession
from cobra.mit.access import MoDirectory

def readFile(fileName=None, mode="r"):
    if fileName is None:
        return ""
    fileData = ""
    with open(fileName, mode) as aFile:
        fileData = aFile.read()
    return fileData

pkey = readFile("/tmp/userabc.key")
csession = CertSession("https://ApicIPOrHostname/",
                       "uni/userext/user-userabc/usercert-userabc.crt", pkey)

modir = MoDirectory(csession)
resp = modir.lookupByDn('uni/fabric')
pring resp.dn
# End of script
```

（注） 前のステップで使用した DN が、このステップの x509 証明書を含むユーザ認定オブジェクトの DN に一致する必要があります。

アカウンティング

ACI ファブリック アカウンティングは、障害およびイベントと同じメカニズムで処理される以下の 2 つの管理対象オブジェクト（MO）によって処理されます。

- `aaaSessionLR` MO は、APIC およびスイッチでのユーザ アカウントのログイン/ログアウト セッション、およびトークン更新を追跡します。ACI ファブリック セッション アラート機能は、次のような情報を保存します。
  - ユーザ名

- セッションを開始した IP アドレス
- タイプ（telnet、https、REST など）
- セッションの時間と長さ
- トークン更新：ユーザ アカウントのログイン イベントは、ユーザ アカウントが ACI ファブリックの権利を行使するために必要な、有効なアクティブ トークンを生成します。

（注） トークンはログインに関係なく期限切れになります。ユーザはログアウトできますが、トークンは含まれているタイマー値の期間に従って期限切れになります。

- `aaaModLR` MO は、ユーザがオブジェクトに対して行う変更、およびいつ変更が発生したかを追跡します。

`aaaSessionLR` と `aaaModLR` 両方のイベント ログは、APIC シャードに保存されます。データがプリセットされているストレージ割り当てサイズを超えると、先入れ先出し方式でレコードを上書きします。

（注） APIC クラスタ ノードを破壊するディスク クラッシュや出火などの破壊的なイベントが発生した場合、イベント ログは失われ、イベント ログはクラスタ全体で複製されません。

`aaaModLR` MO と `aaaSessionLR` MO は、クラスまたは識別名（DN）でクエリできます。クラスのクエリは、ファブリック全体のすべてのログ レコードを提供します。ファブリック全体のすべての `aaaModLR` レコードは、GUI の [Fabric] -> [Inventory] -> [pod-1] -> [history] -> [audit log] セクションで取得できます。[GUI] => [History] => [Log] オプションを使用すると、GUI コンテキストで識別された特定のオブジェクトのイベント ログを表示できます。

標準の syslog、callhome、REST クエリ、および CLI エクスポート メカニズムは、aaaModLR MO と aaaSessionLR MO のクエリ データで完全にサポートされます。このデータをエクスポートするデフォルト ポリシーはありません。

APIC には、一連のオブジェクトまたはシステム全体のデータの集約を報告する、事前設定されたクエリはありません。ファブリック管理者は、`aaaModLR` および `aaaSessionLR` のクエリ データを定期的に syslog サーバにエクスポートするエクスポート ポリシーを設定できます。エクスポートされたデータを定期的にアーカイブし、システムの一部またはシステム ログ全体のカスタム レポートを生成するために使用できます。

共有サービスとしての外部ネットワークへのルーテッド接続の課金と統計情報

APIC は、共有サービスとしての外部ネットワークへのルーテッド接続用に設定されたポート（`l3extInstP` EPG）からバイト カウントとパケット カウントでの課金統計情報を収集するように設定できます。任意のテナントの任意の EPG が、外部ネットワークへのルーテッド接続用に `l3extInstP` EPG を共有できます。課金統計情報は、共有サービスとして `l3extInstP` EPG を使用する任意のテナント内の EPG ごとに収集できます。`l3extInstP` がプロビジョニングされているリーフ スイッチは課金統計情報を APIC に転送し、そこで課金情報が集約されます。定期的に課金統計情報をサーバにエクスポートするようにアカウンティング ポリシーを設定できます。

第 2 章

管理

この章の内容は、次のとおりです。

管理アクセスの追加

APIC コントローラには、管理ネットワークに到達するルートが 2 つあります。1 つはインバンド管理インターフェイスを使用し、もう 1 つはアウトオブバンド管理インターフェイスを使用します。

- インバンド管理アクセス：APIC および ACI ファブリックへのインバンド管理接続を設定できます。APIC がリーフ スイッチと通信するときに APIC によって使用される VLAN を最初に設定し、次に VMM サーバがリーフ スイッチとの通信に使用する VLAN を設定します。
- アウトオブバンド管理アクセス：APIC および ACI ファブリックへのアウトオブバンド管理接続を設定できます。アウトオブバンドエンドポイント グループ（EPG）に関連付けられるアウトオブバンド契約を設定し、外部ネットワーク プロファイルにその契約を接続します。

（注） APIC アウトオブバンド管理接続のリンクは、1 Gbps である必要があります。

APIC コントローラは、インバンド管理インターフェイスが設定されている場合は、アウトオブバンド管理インターフェイスを通してインバンド管理インターフェイスを常に選択します。アウトオブバンド管理インターフェイスは、インバンド管理インターフェイスが設定されていない場合、または宛先アドレスが APIC のアウトオブバンド管理サブネットと同じサブネットにある場合にのみ使用されます。この動作は、変更または再設定できません。

APIC 管理インターフェイスは IPv6 アドレスをサポートしないため、このインターフェイスを介して外部 IPv6 サーバに接続することはできません。

インバンドまたはアウトオブバンドの管理テナントで外部管理インスタンス プロファイルを設定しても、ファブリック全体の通信ポリシーで設定されているプロトコルには影響しません。外部管理インスタンスプロファイルで指定されているサブネットおよびコントラクトは、HTTP/HTTPS または SSH/Telnet には影響しません。

インバンドおよびアウトオブバンド管理アクセス

管理テナントでは、ファブリック管理機能へのアクセスを設定するための便利な方法が提供されます。APIC を介してファブリック管理機能にアクセスできると同時に、インバンドおよびアウトオブバンドのネットワーク ポリシー経由で直接アクセスすることもできます。

拡張 GUI を使用したインバンド管理アクセスの設定

（注）
- インバンド管理アクセスでは、IPv4 アドレスと IPv6 アドレスがサポートされます。スタティック設定を使用した IPv6 設定がサポートされます（インバンドとアウトバンドの両方）。IPv4 および IPv6 のインバンドおよびアウトオブバンドのデュアル設定は、スタティック設定を使用する場合にのみサポートされます。詳細については、KB 記事、「*Configuring Static Management Access in Cisco APIC*」を参照してください。
- このタスク例のビデオを視聴するには、ビデオを掲載している Web ページ を参照してください。

手順の概要

1. メニュー バーで、[FABRIC] > [Access Policies] を選択します。[Navigation] ペインで、[Interface Policies] を展開します。
2. [Navigation] ペインで、[Switch Policies] を右クリックし、[Configure Interface, PC and VPC] を選択します。
3. [Configure Interface, PC, and VPC] ダイアログボックスで、APIC に接続されているスイッチ ポートを設定し、次の操作を実行します。
4. [Navigation] ペインで、[Switch Policies] を右クリックし、[Configure Interface, PC and VPC] を選択します。
5. [Configure Interface, PC, and VPC] ダイアログ ボックスで、次のアクションを実行します。
6. [Configure Interface, PC, and VPC] ダイアログボックスで、[Submit] をクリックします。
7. メニュー バーで、[TENANTS] > [mgmt] をクリックします。[Navigation] ペインで、[Tenant mgmt] > [Networking] > [Bridge Domains] を展開し、インバンド接続のブリッジ ドメインを設定します。
8. インバンド ブリッジ ドメイン（inb）を展開します。[Subnets] を右クリックします。[Create Subnets] をクリックし、次の操作を実行してインバンド ゲートウェイを設定します。
9. [Navigation] ペインで、[Tenant mgmt] > [Node Management EPGs] の順に展開します。[Node Management EPGs] を右クリックし、[Create In-Band Management EPG] を選択します。APIC と通信するために使用するインバンド EPG の VLAN を設定するには、次の操作を実行します。
10. [Navigation] ペインで、[Node Management Addresses] を右クリックし、[Create Node Management Addresses] をクリックし、次の操作を実行してファブリック内の APIC コントローラに割り当てる IP アドレスを設定します。
11. [Navigation] ペインで、[Node Management Addresses] を右クリックします。[Create Node Management Addresses] をクリックし、次の操作を実行して、ファブリック内のリーフ スイッチおよびスパイン スイッチの IP アドレスを設定します。
12. [Navigation] ペインの [Node Management Addresses] 下で、APIC ポリシー名（apicInb）をクリックして設定を確認します。[Work] ペインに、さまざまなノードに割り当てられた IP アドレスが表示されます。
13. [Navigation] ペインの [Node Management Addresses] 下で、スイッチ ポリシー名（switchInb）をクリックします。[Work] ペインに、スイッチに割り当てられている IP アドレスと使用しているゲートウェイ アドレスが表示されます。

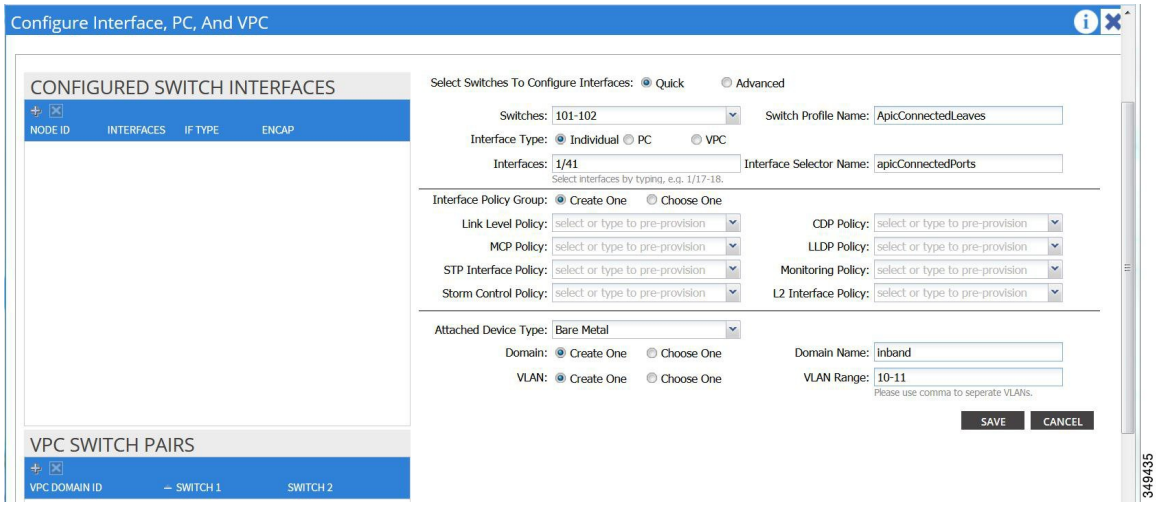
手順の詳細

ステップ 1 メニュー バーで、[FABRIC] > [Access Policies] を選択します。[Navigation] ペインで、[Interface Policies] を展開します。

ステップ 2 [Navigation] ペインで、[Switch Policies] を右クリックし、[Configure Interface, PC and VPC] を選択します。

ステップ 3 [Configure Interface, PC, and VPC] ダイアログボックスで、APIC に接続されているスイッチ ポートを設定し、次の操作を実行します。

a) スイッチ図の横にある大きい [+] アイコンをクリックして、新しいプロファイルを作成して VLAN を APIC 用に設定します。
b) [Switches] フィールドのドロップダウン リストから、APIC が接続されているスイッチのチェックボックスをオンにします。（leaf1 および leaf2）。
c) [Switch Profile Name] フィールドに、プロファイルの名前（apicConnectedLeaves）を入力します。
d) [+] アイコンをクリックして、ポートを設定します。
ユーザがコンテンツを入力できるように、次の画像のようなダイアログボックスが表示されます。



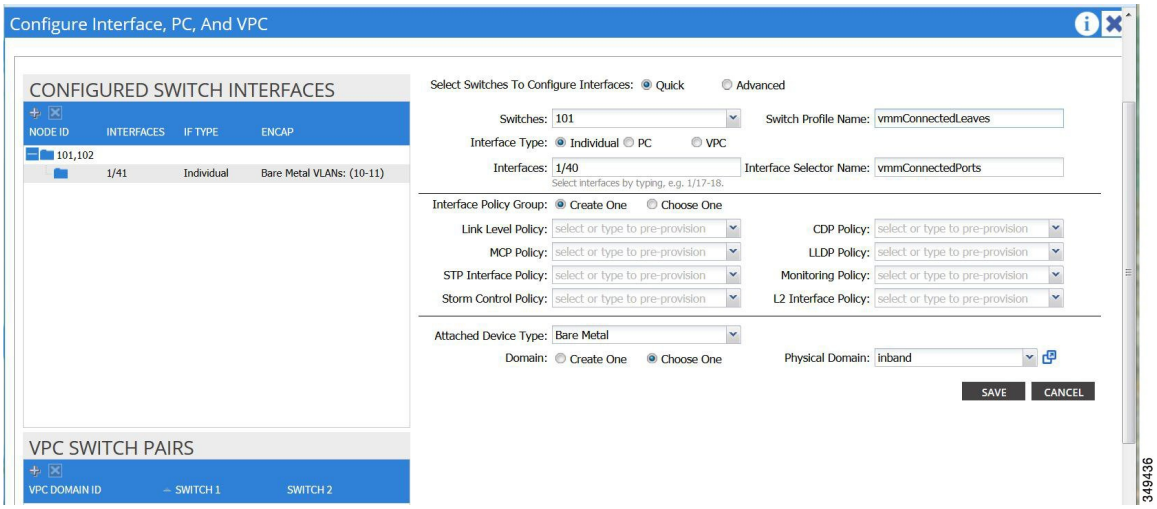
e) [Interface Type] 領域で、[Individual] オプション ボタンが選択されていることを確認します。
f) [Interfaces] フィールドで、APIC が接続されているポートを入力します。
g) [Interface Selector Name] フィールドに、ポート プロファイルの名前（apicConnectedPorts）を入力します。
h) [Interface Policy Group] フィールドで、[Create One] オプション ボタンをクリックします。
i) [Attached Device Type] フィールドで、適切なデバイス タイプを選択してドメイン（ベア メタル）を設定します。
j) [Domain] フィールドで、[Create One] オプション ボタンをクリックします。
k) [Domain Name] フィールドに、ドメイン名を入力します。（[inband]）
l) [VLAN] フィールドで、[Create One] オプション ボタンを選択します。
m) [VLAN Range] フィールドに、VLAN 範囲を入力します。[Save] をクリックし、[Save] をもう一度クリックします。[Submit] をクリックします。

ステップ 4 [Navigation] ペインで、[Switch Policies] を右クリックし、[Configure Interface, PC and VPC] を選択します。

ステップ 5 [Configure Interface, PC, and VPC] ダイアログ ボックスで、次のアクションを実行します。

a) スイッチ図の横にある大きい [+] アイコンをクリックして、新しいプロファイルを作成して VLAN をサーバ用に設定します。
b) [Switches] フィールドのドロップダウン リストから、サーバが接続されているスイッチのチェックボックスをオンにします。（leaf1）。
c) [Switch Profile Name] フィールドに、プロファイルの名前（vmmConnectedLeaves）を入力します。
d) [+] アイコンをクリックして、ポートを設定します。

ユーザがコンテンツを入力できるように、次の画像のようなダイアログボックスが表示されます。



e) [Interface Type] 領域で、[Individual] オプション ボタンが選択されていることを確認します。
f) [Interfaces] フィールドで、サーバが接続されているポートを入力します（1/40）。
g) [Interface Selector Name] フィールドに、ポート プロファイルの名前を入力します。
h) [Interface Policy Group] フィールドで、[Create One] オプション ボタンをクリックします。
i) [Attached Device Type] フィールドで、適切なデバイス タイプを選択してドメイン（ベア メタル）を設定します。
j) [Domain] フィールドのドロップダウン リストから、[Choose One] オプション ボタンをクリックします。
k) [Physical Domain] ドロップダウン リストから、前に作成したドメインを選択します。
l) [Domain Name] フィールドに、ドメイン名を入力します。
m) [Save] をクリックし、[Save] をもう一度クリックします。

ステップ 6 [Configure Interface, PC, and VPC] ダイアログボックスで、[Submit] をクリックします。

ステップ 7 メニュー バーで、[TENANTS] > [mgmt] をクリックします。[Navigation] ペインで、[Tenant mgmt] > [Networking] > [Bridge Domains] を展開し、インバンド接続のブリッジ ドメインを設定します。

ステップ 8 インバンド ブリッジ ドメイン（inb）を展開します。[Subnets] を右クリックします。[Create Subnets] をクリックし、次の操作を実行してインバンド ゲートウェイを設定します。

a) [Create Subnet] ダイアログボックスで、[Gateway IP] フィールドに、インバンド管理ゲートウェイ IP アドレスとマスクを入力します。
b) [Submit] をクリックします。

ステップ 9 [Navigation] ペインで、[Tenant mgmt] > [Node Management EPGs] の順に展開します。[Node Management EPGs] を右クリックし、[Create In-Band Management EPG] を選択します。APIC と通信するために使用するインバンド EPG の VLAN を設定するには、次の操作を実行します。

a) [Name] フィールドに、インバンド管理 EPG 名を入力します。
b) [Encap] フィールドで、VLAN（vlan-10）を入力します。

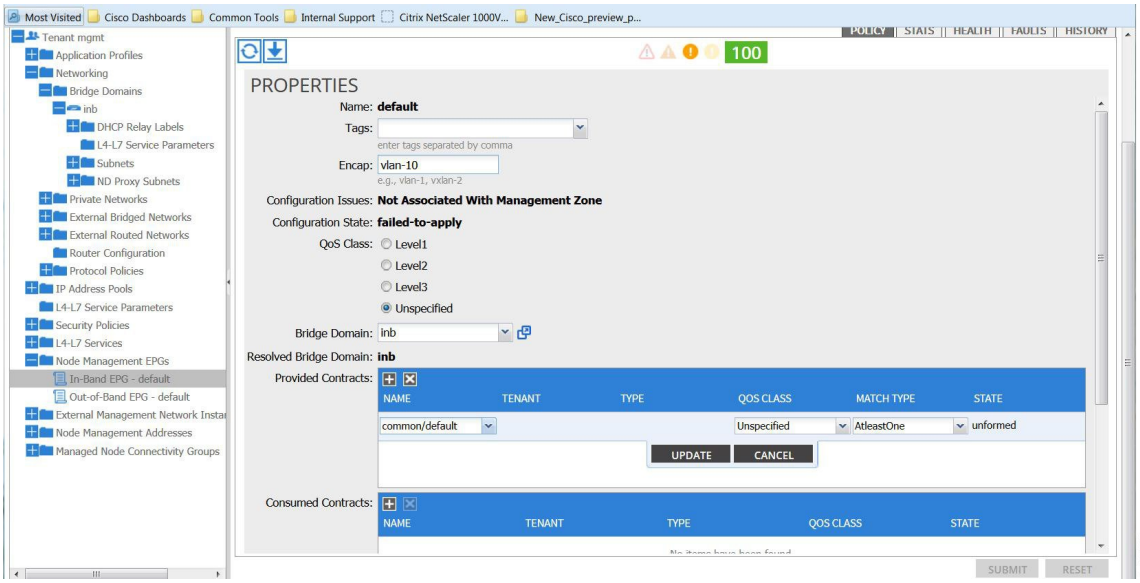
c) [Bridge Domain] ドロップダウン フィールドから、ブリッジ ドメインを選択します。[Submit] をクリックします。

d) [Navigation] ペインで、新しく作成したインバンド EPG を選択します。

e) [Provided Contracts] を展開します。[Name] フィールドで、ドロップダウン リストから、デフォルトのコントラクトを選択し、VMM サーバが存在する EPG で消費されるデフォルトのコントラクトを EPG が提供できるようにします。

f) [Update] をクリックし、[Submit] をクリックします。

次の画像のようなダイアログボックスが表示されます。



ステップ 10 [Navigation] ペインで、[Node Management Addresses] を右クリックし、[Create Node Management Addresses] をクリックし、次の操作を実行してファブリック内の APIC コントローラに割り当てる IP アドレスを設定します。

a) [Create Node Management Addresses] ダイアログボックスで、[Policy Name] フィールドに、ポリシー名（apicInb）を入力します。

b) [Nodes] フィールドの [Select] 列で、このファブリックの一部となるノードのチェックボックスをオンにします（apic1、apic2、apic3）。

c) [Config] フィールドで、[In-Band Addresses] チェックボックスをオンにします。

d) [Node Range] フィールドに、範囲を入力します。

e) [In-Band IP Addresses] 領域の [In-Band Management EPG] フィールドで、ドロップダウン リストから、[default] を選択します。これで、デフォルトのインバンド管理 EPG が関連付けられます。

f) [In-Band IP Addresses] フィールドと [Gateway] フィールドに、必要に応じて IPv4 アドレスまたは IPv6 アドレスを入力します。

g) [Submit] をクリックします。これで、APIC の IP アドレスが設定されました。

ステップ 11 [Navigation] ペインで、[Node Management Addresses] を右クリックします。[Create Node Management Addresses] をクリックし、次の操作を実行して、ファブリック内のリーフ スイッチおよびスパイン スイッチの IP アドレスを設定します。

a) [Create Node Management Addresses] ダイアログボックスで、[Policy Name] フィールドに、ポリシー名（switchInb）を入力します。
b) [Nodes] フィールドの [Select] 列で、このファブリックの一部となるノードの横のチェックボックスをオンにします（leaf1、leaf2、spine1、spine2）。
c) [Config] フィールドで、[In-Band Addresses] チェックボックスをクリックします。
d) [Node Range] フィールドに、範囲を入力します。
e) [In-Band IP Addresses] 領域の [In-Band Management EPG] フィールドで、ドロップダウン リストから、[default] を選択します。デフォルトのインバンド管理 EPG が関連付けられました。
f) [In-Band IP Addresses] フィールドと [Gateway] フィールドに、必要に応じて IPv4 アドレスまたは IPv6 アドレスを入力します。
g) [Submit] をクリックします。[Confirm] ダイアログボックスで、[Yes] をクリックします。リーフおよびスパイン スイッチの IP アドレスが設定されました。

ステップ 12 [Navigation] ペインの [Node Management Addresses] 下で、APIC ポリシー名（apicInb）をクリックして設定を確認します。[Work] ペインに、さまざまなノードに割り当てられた IP アドレスが表示されます。

ステップ 13 [Navigation] ペインの [Node Management Addresses] 下で、スイッチ ポリシー名（switchInb）をクリックします。[Work] ペインに、スイッチに割り当てられている IP アドレスと使用しているゲートウェイ アドレスが表示されます。

CLI を使用したインバンド管理アクセスの設定

手順の概要

1. 管理トラフィック用の VLAN ネームスペースを作成します。
2. 管理トラフィック用の物理ドメインを作成します。
3. インバンド トラフィック用のリーフ セレクタを作成します。
4. インバンド ブリッジ ドメインとエンドポイント グループ（EPG）を設定します。
5. 管理アドレス プールを作成します。
6. ノード管理グループを作成します。

手順の詳細

ステップ 1 管理トラフィック用の VLAN ネームスペースを作成します。

例：

```
admin@apic1:~> cd /aci/fabric/access-policies/pools/vlan/
admin@apic1:vlan> mocreate inband static-allocation
admin@apic1:vlan> moconfig commit
Committing mo 'fabric/access-policies/pools/vlan/inband-static-allocation'

All mos committed successfully.
```

```
admin@apic1:vlan> cd inband-static-allocation/encap-blocks
admin@apic1:encap-blocks> mocreate vlan10 vlan11
admin@apic1:encap-blocks> cd vlan10-vlan11
admin@apic1:vlan10-vlan11> moset name encap
admin@apic1:vlan10-vlan11> moconfig commit
Committing mo 'fabric/access-policies/pools/vlan/inband-static-allocation/encap-blocks/vlan10-vlan11'

All mos committed successfully.
admin@apic1:vlan10-vlan11>
```

ステップ 2 管理トラフィック用の物理ドメインを作成します。

例：

```
admin@apic1:~> cd /aci/fabric/access-policies/physical-and-external-domains/physical-domains/
admin@apic1:physical-domains> mocreate inband
admin@apic1:physical-domains> moconfig commit
Committing mo 'fabric/access-policies/physical-and-external-domains/physical-domains/inband'

All mos committed successfully.
admin@apic1:physical-domains> cd inband
admin@apic1:inband> moset vlan-pools fabric/access-policies/pools/vlan/inband-static-allocation
admin@apic1:inband> moconfig commit
Committing mo 'fabric/access-policies/physical-and-external-domains/physical-domains/inband'

All mos committed successfully.
admin@apic1:inband>
```

ステップ 3 インバンド トラフィック用のリーフ セレクタを作成します。

例：

```
admin@apic1:~> cd /aci/fabric/access-policies/switch-policies/profiles
admin@apic1:profiles> mocreate vmmNodes
admin@apic1:profiles> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/vmmNodes'

All mos committed successfully.
admin@apic1:profiles> cd vmmNodes
admin@apic1:vmmNodes> mocreate leaf-selector leafS range
admin@apic1:vmmNodes> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/vmmNodes/leaf-selector-leafS-range'

All mos committed successfully.
admin@apic1:vmmNodes>
admin@apic1:vmmNodes> cd leaf-selector-leafS-range
admin@apic1:leaf-selector-leafS-range> mocreate single0
admin@apic1:leaf-selector-leafS-range> cd single0
admin@apic1:single0> moset to 101
admin@apic1:single0> moset from 101
admin@apic1:single0> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/vmmNodes/leaf-selector-leafS-range/single0'

All mos committed successfully.
admin@apic1:single0>
admin@apic1:single0> cd ../../associated-interface-selector-profiles
admin@apic1:associated-interface-selector-profiles> mocreate
fabric/access-policies/interface-policies/profiles/interfaces/vmmPorts
admin@apic1:associated-interface-selector-profiles> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/vmmNodes/associated-interface-selector-profiles/[fabric/access-policies
/interface-policies/profiles/interfaces/vmmPorts]'

All mos committed successfully.
admin@apic1:associated-interface-selector-profiles>
admin@apic1:associated-interface-selector-profiles> cd /aci/fabric/access-policies/interface-policies/profiles/interfaces
admin@apic1:interfaces> mocreate vmmPorts
admin@apic1:interfaces> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/vmmPorts'

All mos committed successfully.
admin@apic1:interfaces> cd vmmPorts
admin@apic1:vmmPorts> mocreate portS range
admin@apic1:vmmPorts> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/vmmPorts/portS-range'

All mos committed successfully.
admin@apic1:vmmPorts>
admin@apic1:vmmPorts> cd portS-range
admin@apic1:portS-range> mocreate block1
admin@apic1:portS-range> cd block1
```

```
admin@apic1:block1> moset from-module 1
admin@apic1:block1> moset to-module 1
admin@apic1:block1> moset from-port 40
admin@apic1:block1> moset to-port 40
admin@apic1:block1> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/vmmPorts/portS-range/block1'

All mos committed successfully.
admin@apic1:block1>
admin@apic1:block1> cd ../
admin@apic1:portS-range> moset policy-group
fabric/access-policies/interface-policies/policy-groups/interface/inband
admin@apic1:portS-range> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/vmmPorts/portS-range'

All mos committed successfully.
admin@apic1:portS-range>
admin@apic1:portS-range> cd /aci/fabric/access-policies/switch-policies/profiles
admin@apic1:profiles> mocreate apicConnectedNodes
admin@apic1:profiles> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/apicConnectedNodes'

All mos committed successfully.
admin@apic1:profiles> cd apicConnectedNodes
admin@apic1:apicConnectedNodes> mocreate leaf-selector leafS range
admin@apic1:apicConnectedNodes> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/apicConnectedNodes/leaf-selector-leafS-range'

All mos committed successfully.
admin@apic1:apicConnectedNodes>
admin@apic1:apicConnectedNodes> cd leaf-selector-leafS-range
admin@apic1:leaf-selector-leafS-range> mocreate single0
admin@apic1:leaf-selector-leafS-range> cd single0
admin@apic1:single0> moset to 102
admin@apic1:single0> moset from 101
admin@apic1:single0> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/apicConnectedNodes/leaf-selector-leafS-range/single0'

All mos committed successfully.
admin@apic1:single0>
admin@apic1:single0> cd ../../associated-interface-selector-profiles
admin@apic1:associated-interface-selector-profiles> mocreate
fabric/access-policies/interface-policies/profiles/interfaces
/apicConnectedPorts
admin@apic1:associated-interface-selector-profiles> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/apicConnectedNodes/associated-interface-selector-profiles/[fabric/access-policies
/interface-policies/profiles/interfaces/apicConnectedPorts]'

All mos committed successfully.
admin@apic1:associated-interface-selector-profiles>
admin@apic1:associated-interface-selector-profiles> cd /aci/fabric/access-policies/interface-policies/profiles/interfaces
admin@apic1:interfaces> mocreate apicConnectedPorts
admin@apic1:interfaces> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/apicConnectedPorts'

All mos committed successfully.
admin@apic1:interfaces> cd apicConnectedPorts
admin@apic1:apicConnectedPorts> mocreate portS range
admin@apic1:apicConnectedPorts> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/apicConnectedPorts/portS-range'

All mos committed successfully.
admin@apic1:apicConnectedPorts>
admin@apic1:apicConnectedPorts> cd portS-range
admin@apic1:portS-range> mocreate block1
admin@apic1:portS-range> cd block1
admin@apic1:block1> moset from-module 1
admin@apic1:block1> moset to-module 1
admin@apic1:block1> moset from-port 1
admin@apic1:block1> moset to-port 3
admin@apic1:block1> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/apicConnectedPorts/portS-range/block1'

All mos committed successfully.
admin@apic1:block1> cd ../
admin@apic1:portS-range> moset policy-group
fabric/access-policies/interface-policies/policy-groups/interface/inband
admin@apic1:portS-range> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/apicConnectedPorts/portS-range'

All mos committed successfully.
admin@apic1:portS-range>
admin@apic1:portS-range> cd /aci/fabric/access-policies/interface-policies/policy-groups/interface
admin@apic1:interface> mocreate inband
admin@apic1:interface> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/policy-groups/interface/inband'

All mos committed successfully.
admin@apic1:interface> cd inband
```

```
admin@apic1:inband> moset attached-entity-profile
fabric/access-policies/global-policies/attachable-entity-profile/inband
admin@apic1:inband> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/policy-groups/interface/inband'

All mos committed successfully.
admin@apic1:inband>
admin@apic1:inband> cd /aci/fabric/access-policies/global-policies/attachable-entity-profile
admin@apic1:attachable-entity-profile> mocreate inband
admin@apic1:attachable-entity-profile> moconfig commit
Committing mo 'fabric/access-policies/global-policies/attachable-entity-profile/inband'

All mos committed successfully.
admin@apic1:attachable-entity-profile> cd inband/domains-associated-to-interfaces
admin@apic1:domains-associated-to-interfaces> mocreate
fabric/access-policies/physical-and-external-domains/physical-domains/inband
admin@apic1:domains-associated-to-interfaces> moconfig commit
Committing mo 'fabric/access-policies/global-policies/attachable-entity-profile/inband/domains-associated-to-interfaces/[fabric/access-policies
/physical-and-external-domains/physical-domains/inband]'

All mos committed successfully.
admin@apic1:domains-associated-to-interfaces>
```

ステップ 4 インバンド ブリッジ ドメインとエンドポイント グループ（EPG）を設定します。

例：

```
admin@apic1:~> cd /aci/tenants/mgmt/networking/bridge-domains/inb/subnets
admin@apic1:subnets> mocreate 10.13.1.254/24
admin@apic1:subnets> moconfig commit
Committing mo 'tenants/mgmt/networking/bridge-domains/inb/subnets/10.13.1.254:24'

All mos committed successfully.
admin@apic1:subnets>
admin@apic1:subnets> cd /aci/tenants/mgmt/node-management-epgs/default/in-band/default
admin@apic1:default> moset encap vlan-10
admin@apic1:default> moconfig commit
Committing mo 'tenants/mgmt/node-management-epgs/default/in-band/default'

All mos committed successfully.
admin@apic1:default>
admin@apic1:default> cd provided-contracts
admin@apic1:provided-contracts> mocreate default
admin@apic1:provided-contracts> moconfig commit
Committing mo 'tenants/mgmt/node-management-epgs/default/in-band/default/provided-contracts/default'

All mos committed successfully.
admin@apic1:provided-contracts>
```

ステップ 5 管理アドレス プールを作成します。

例：

```
admin@apic1:provided-contracts> cd /aci/tenants/mgmt/node-management-addresses/address-pools
admin@apic1:address-pools> mocreate switchInb
admin@apic1:address-pools> cd switchInb
admin@apic1:switchInb> moset gateway-address 10.13.1.254/24
admin@apic1:switchInb> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/address-pools/switchInb'

All mos committed successfully.
admin@apic1:switchInb> cd address-blocks
admin@apic1:address-blocks> mocreate 10.13.1.101 10.13.1.120
admin@apic1:address-blocks> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/address-pools/switchInb/address-blocks/10.13.1.101-10.13.1.120'

All mos committed successfully.
admin@apic1:address-blocks>
admin@apic1:address-blocks>
admin@apic1:address-blocks> cd /aci/tenants/mgmt/node-management-addresses/address-pools
admin@apic1:address-pools> mocreate apicInb
admin@apic1:address-pools> cd apicInb
admin@apic1:apicInb> moset gateway-address 10.13.1.254/24
admin@apic1:apicInb> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/address-pools/apicInb'

All mos committed successfully.
admin@apic1:apicInb> cd address-blocks
```

```
admin@apic1:address-blocks> mocreate 10.13.1.1 10.13.1.10
admin@apic1:address-blocks> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/address-pools/apicInb/address-blocks/10.13.1.1-10.13.1.10'

All mos committed successfully.
admin@apic1:address-blocks>
```

ステップ 6 ノード管理グループを作成します。

例：

```
admin@apic1:~> cd aci/tenants/mgmt/node-management-addresses/
admin@apic1:node-management-addresses> mocreate node-management-address apic
admin@apic1:node-management-addresses> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-management-address-apic'

All mos committed successfully.
admin@apic1:node-management-addresses> cd node-management-address-apic/node-blocks/
admin@apic1:node-blocks> mocreate all
admin@apic1:node-blocks> cd all
admin@apic1:all> moset from 1
admin@apic1:all> moset to 3
admin@apic1:all> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-management-address-apic/node-blocks/all'

All mos committed successfully.
admin@apic1:all>
admin@apic1:all> cd ../../
admin@apic1:node-management-address-apic> moset managed-node-connectivity-group
tenants/mgmt/node-management-addresses/connectivity-groups/apic
admin@apic1:node-management-address-apic> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-management-address-apic'

All mos committed successfully.
admin@apic1:node-management-address-apic>
admin@apic1:node-management-address-apic>
admin@apic1:node-management-address-apic> cd ../
admin@apic1:node-management-addresses> mocreate node-management-address switch
admin@apic1:node-management-addresses> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-management-addresses/switch'

All mos committed successfully.
admin@apic1:node-management-addresses>
admin@apic1:node-management-addresses> cd node-management-address-switch/node-blocks/
admin@apic1:node-blocks> mocreate all
admin@apic1:node-blocks> cd all
admin@apic1:all> moset from 101
admin@apic1:all> moset to 104
admin@apic1:all> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-management-address-switch/node-blocks/all'

All mos committed successfully.
admin@apic1:all>
admin@apic1:all> cd ../../
admin@apic1:node-management-address-switch> moset managed-node-connectivity-group
tenants/mgmt/node-management-addresses
/connectivity-groups/switch
admin@apic1:node-management-address-switch> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-management-address-switch'

All mos committed successfully.
admin@apic1:node-management-address-switch>
admin@apic1:node-management-address-switch>
admin@apic1:node-management-address-switch> cd /aci/tenants/mgmt/node-management-addresses/connectivity-groups/
admin@apic1:connectivity-groups> mocreate aci
admin@apic1:connectivity-groups> moconfig commit
Committing mo '/aci/tenants/mgmt/node-management-addresses/connectivity-groups/aci'

All mos committed successfully.
admin@apic1:connectivity-groups>
admin@apic1:connectivity-groups> cd aci/
admin@apic1:aci> mocreate inb-managed-nodes-zone in-band-zone default
admin@apic1:aci> moconfig commit
Committing mo '/aci/tenants/test/node-management-addresses/connectivity-groups/aci/inb-managed-nodes-zone/default'

All mos committed successfully.
admin@apic1:aci>
admin@apic1:aci> cd inb-managed-nodes-zone/
admin@apic1:inb-managed-nodes-zone> moset in-band-ip-address-pool
tenants/mgmt/node-management-addresses/address-pools/apicInb
admin@apic1:inb-managed-nodes-zone> moset in-band-management-epg
```

```
tenants/mgmt/node-management-epgs/default/in-band/default
admin@apic1:inb-managed-nodes-zone> moconfig commit
Committing mo '/tenants/test/node-management-addresses/connectivity-groups/aci/inb-managed-nodes-zone/in-band-ip-address-pool'
Committing mo '/tenants/test/node-management-addresses/connectivity-groups/aci/inb-managed-nodes-zone/in-band-management-epg'

All mos committed successfully.
admin@apic1:inb-managed-nodes-zone>
admin@apic1:inb-managed-nodes-zone> cd ../../
admin@apic1:connectivity-groups> mocreate switch
admin@apic1:connectivity-groups> moconfig commit
Committing mo '/tenants/test/node-management-addresses/connectivity-groups/switch'

All mos committed successfully.

admin@apic1:connectivity-groups>
admin@apic1:connectivity-groups> cd switch/
admin@apic1:switch> mocreate inb-managed-nodes-zone in-band-zone default
admin@apic1:switch> moconfig commit
Committing mo '/tenants/test/node-management-addresses/connectivity-groups/switch/inb-managed-nodes-zone/default

All mos committed successfully.

admin@apic1:switch> cd inb-managed-nodes-zone/
admin@apic1:inb-managed-nodes-zone> moset in-band-ip-address-pool
tenants/mgmt/node-management-addresses/address-pools/switchInb
admin@apic1:inb-managed-nodes-zone> moset in-band-management-epg
tenants/mgmt/node-management-epgs/default/in-band/default
admin@apic1:inb-managed-nodes-zone> moconfig commit
Committing mo '/tenants/mgmt/node-management-addresses/address-pools/switchInb/in-band-ip-address-pool'
Committing mo '/tenants/mgmt/node-management-epgs/default/in-band/default/in-band-management-epg'

All mos committed successfully.

admin@apic1:inb-managed-nodes-zone>
```

REST API を使用したインバンド管理アクセスの設定

インバンド管理アクセスでは、IPv4アドレスとIPv6アドレスがサポートされます。スタティック設定を使用したIPv6設定がサポートされます（インバンドとアウトバンドの両方）。IPv4およびIPv6 のインバンドおよびアウトオブバンドのデュアル設定は、スタティック設定を使用する場合にのみサポートされます。詳細については、KB 記事、「*Configuring Static Management Access in Cisco APIC*」を参照してください。

手順の概要

1. VLAN ネームスペースを作成します。
2. 物理ドメインを作成します。
3. インバンド管理用のセレクタを作成します。
4. インバンド ブリッジ ドメインとエンドポイント グループ（EPG）を設定します。
5. アドレス プールを作成します。
6. 管理グループを作成します。

手順の詳細

ステップ 1　VLAN ネームスペースを作成します。

例：

```
POST
https://APIC-IP/api/mo/uni.xml

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/uni.xml -->
<polUni>
  <infraInfra>
    <!-- Static VLAN range -->
    <fvnsVlanInstP name="inband" allocMode="static">
      <fvnsEncapBlk name="encap" from="vlan-10" to="vlan-11"/>
    </fvnsVlanInstP>
  </infraInfra>
</polUni>
```

ステップ 2 物理ドメインを作成します。

例：

```
POST
https://APIC-IP/api/mo/uni.xml

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/uni.xml -->
<polUni>
  <physDomP name="inband">
    <infraRsVlanNs tDn="uni/infra/vlanns-inband-static"/>
  </physDomP>
</polUni>
```

ステップ 3 インバンド管理用のセレクタを作成します。

例：

```
POST
https://APIC-IP/api/mo/uni.xml

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
  <infraInfra>
    <infraNodeP name="vmmNodes">
      <infraLeafS name="leafS" type="range">
        <infraNodeBlk name="single0" from_="101" to_="101"/>
      </infraLeafS>
      <infraRsAccPortP tDn="uni/infra/accportprof-vmmPorts"/>
    </infraNodeP>

    <!-- Assumption is that VMM host is reachable via eth1/40. -->
    <infraAccPortP name="vmmPorts">
      <infraHPortS name="portS" type="range">
        <infraPortBlk name="block1"
                      fromCard="1" toCard="1"
                      fromPort="40" toPort="40"/>
        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-inband" />
      </infraHPortS>
    </infraAccPortP>


    <infraNodeP name="apicConnectedNodes">
      <infraLeafS name="leafS" type="range">
        <infraNodeBlk name="single0" from_="101" to_="102"/>
      </infraLeafS>
      <infraRsAccPortP tDn="uni/infra/accportprof-apicConnectedPorts"/>
    </infraNodeP>

    <!-- Assumption is that APIC is connected to eth1/1. -->
    <infraAccPortP name="apicConnectedPorts">
```

```
      <infraHPortS name="portS" type="range">
        <infraPortBlk name="block1"
                      fromCard="1" toCard="1"
                      fromPort="1" toPort="3"/>
        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-inband" />
      </infraHPortS>
    </infraAccPortP>

    <infraFuncP>
      <infraAccPortGrp name="inband">
        <infraRsAttEntP tDn="uni/infra/attentp-inband"/>
      </infraAccPortGrp>
    </infraFuncP>

    <infraAttEntityP name="inband">
      <infraRsDomP tDn="uni/phys-inband"/>
    </infraAttEntityP>
  </infraInfra>
</polUni>
```

ステップ 4 インバンド ブリッジ ドメインとエンドポイント グループ（EPG）を設定します。

例：

```
POST
https://APIC-IP/api/mo/uni.xml

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
  <fvTenant name="mgmt">
    <!-- Configure the in-band management gateway address on the
         in-band BD. -->
    <fvBD name="inb">
      <fvSubnet ip="10.13.1.254/24"/>
    </fvBD>

    <mgmtMgmtP name="default">
      <!-- Configure the encap on which APICs will communicate on the
           in-band network. -->
      <mgmtInB name="default" encap="vlan-10">
        <fvRsProv tnVzBrCPName="default"/>
      </mgmtInB>
    </mgmtMgmtP>
  </fvTenant>
</polUni>
```

ステップ 5 アドレス プールを作成します。

例：

```
POST
https://APIC-IP/api/mo/uni.xml

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
  <fvTenant name="mgmt">
    <!-- Adresses for APIC in-band management network -->
    <fvnsAddrInst name="apicInb" addr="10.13.1.254/24">
      <fvnsUcastAddrBlk from="10.13.1.1" to="10.13.1.10"/>
    </fvnsAddrInst>

    <!-- Adresses for switch in-band management network -->
    <fvnsAddrInst name="switchInb" addr="10.13.1.254/24">
      <fvnsUcastAddrBlk from="10.13.1.101" to="10.13.1.120"/>
    </fvnsAddrInst>
  </fvTenant>
</polUni>
```

（注） IPv6 のダイナミック アドレス プールはサポートされていません。

ステップ 6 管理グループを作成します。

例：

```
POST
https://APIC-IP/api/mo/uni.xml

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
  <infraInfra>
    <!-- Management node group for APICs -->
    <mgmtNodeGrp name="apic">
      <infraNodeBlk name="all" from_="1" to_="3"/>
      <mgmtRsGrp tDn="uni/infra/funcprof/grp-apic"/>
    </mgmtNodeGrp>

    <!-- Management node group for switches-->
    <mgmtNodeGrp name="switch">
      <infraNodeBlk name="all" from_="101" to_="104"/>
      <mgmtRsGrp tDn="uni/infra/funcprof/grp-switch"/>
    </mgmtNodeGrp>

    <!-- Functional profile -->
    <infraFuncP>
      <!-- Management group for APICs -->
      <mgmtGrp name="apic">
        <!-- In-band management zone -->
        <mgmtInBZone name="default">
          <mgmtRsInbEpg tDn="uni/tn-mgmt/mgmtp-default/inb-default"/>
          <mgmtRsAddrInst tDn="uni/tn-mgmt/addrinst-apicInb"/>
        </mgmtInBZone>
      </mgmtGrp>

      <!-- Management group for switches -->
      <mgmtGrp name="switch">
        <!-- In-band management zone -->
        <mgmtInBZone name="default">
          <mgmtRsInbEpg tDn="uni/tn-mgmt/mgmtp-default/inb-default"/>
          <mgmtRsAddrInst tDn="uni/tn-mgmt/addrinst-switchInb"/>
        </mgmtInBZone>
      </mgmtGrp>
    </infraFuncP>
  </infraInfra>
</polUni>
```

（注） IPv6 のダイナミック アドレス プールはサポートされていません。

拡張 GUI を使用したアウトオブバンド管理アクセスの設定

（注）
- アウトオブバンド管理アクセスでは、IPv4 アドレスと IPv6 アドレスがサポートされます。
- このタスク例のビデオを視聴するには、ビデオを掲載している Web ページ を参照してください。

はじめる前に

APIC アウトオブバンド管理接続のリンクは、1 Gbps である必要があります。

手順の概要

1. メニュー バーで、[TENANTS] > [mgmt] を選択します。[Navigation] ペインで、[Tenant mgmt] を展開します。
2. [Node Management Addresses] を右クリックし、[Create Node Management Addresses] をクリックします。
3. [Create Node Management Addresses] ダイアログボックスで、次の操作を実行します。
4. [Navigation] ペインで、[Node Management Addresses] を展開し、作成したポリシーをクリックします。
5. [Navigation] ペインで、[Security Policies] > [Out-of-Band Contracts] を展開します。
6. [Out-of-Band Contracts] を右クリックし、[Create Out-of-Band Contract] をクリックします。
7. [Create Out-of-Band Contract] ダイアログボックスで、次のタスクを実行します。
8. [Navigation] ペインで、[Node Management EPGs] > [Out-of-Band EPG - default] を展開します。
9. [Work] ペインで、[Provided Out-of-Band Contracts] を展開します。
10. [OOB Contract] カラムで、ドロップダウン リストから、作成したアウトオブバンド契約（oob-default）を選択します。[Update] をクリックし、[Submit] をクリックします。
11. [Navigation] ペインで、[External Network Instance Profile] を右クリックし、[Create External Management Entity Instance] をクリックします。
12. [Create External Management Entity Instance] ダイアログボックスで、次の操作を実行します。

手順の詳細

ステップ 1 メニュー バーで、[TENANTS] > [mgmt] を選択します。[Navigation] ペインで、[Tenant mgmt] を展開します。

ステップ 2 [Node Management Addresses] を右クリックし、[Create Node Management Addresses] をクリックします。

ステップ 3 [Create Node Management Addresses] ダイアログボックスで、次の操作を実行します。

a) [Policy Name] フィールドに、ポリシー名（switchOob）を入力します。

b) [Nodes] フィールドで、適切なリーフおよびスパイン スイッチ（leaf1、leaf2、spine1）の横にあるチェックボックスをオンにします。

c) [Config] フィールドで、[Out of-Band Addresses] のチェックボックスをオンにします。

（注） [Out-of-Band IP addresses] 領域が表示されます。

d) [Out-of-Band Management EPG] フィールドで、ドロップダウン リストから EPG を選択します（デフォルト）。

e) [Out-of-Band IP Addresses] フィールドおよび [Out-of-Band Gateway] フィールドに、スイッチに割り当てられる希望する IPv4 アドレスまたは IPv6 アドレスを入力します。[OK] をクリックします。

ノード管理 IP アドレスが設定されます。APIC だけではなくリーフ スイッチおよびスパイン スイッチにもアウトオブバンド管理アクセスのアドレスを設定する必要があります。

ステップ 4 [Navigation] ペインで、[Node Management Addresses] を展開し、作成したポリシーをクリックします。
[Work] ペインに、スイッチに対するアウトオブバンド管理アドレスが表示されます。

ステップ 5 [Navigation] ペインで、[Security Policies] > [Out-of-Band Contracts] を展開します。

ステップ 6 [Out-of-Band Contracts] を右クリックし、[Create Out-of-Band Contract] をクリックします。

ステップ 7 [Create Out-of-Band Contract] ダイアログボックスで、次のタスクを実行します。

a) [Name] フィールドに、契約の名前（oob-default）を入力します。

b) [Subjects] を展開します。[Create Contract Subject] ダイアログボックスで、[Name] フィールドに、サブジェクト名（oob-default）を入力します。

c) [Filters] を展開し、[Name] フィールドで、ドロップダウン リストから、フィルタの名前（default）を選択します。[Update] をクリックし、[OK] をクリックします。

d) [Create Out-of-Band Contract] ダイアログボックスで、[Submit] をクリックします。

アウトオブバンド EPG に適用できるアウトオブバンド契約が作成されます。

ステップ 8 [Navigation] ペインで、[Node Management EPGs] > [Out-of-Band EPG - default] を展開します。

ステップ 9 [Work] ペインで、[Provided Out-of-Band Contracts] を展開します。

ステップ 10 [OOB Contract] カラムで、ドロップダウン リストから、作成したアウトオブバンド契約（oob-default）を選択します。[Update] をクリックし、[Submit] をクリックします。
契約がノード管理 EPG に関連付けられます。

ステップ 11 [Navigation] ペインで、[External Network Instance Profile] を右クリックし、[Create External Management Entity Instance] をクリックします。

ステップ 12 [Create External Management Entity Instance] 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、名前（oob-mgmt-ext）を入力します。

b) [Consumed Out-of-Band Contracts] フィールドを展開します。[Out-of-Band Contract] ドロップダウン リストから、作成した契約（oob-default）を選択します。[Update] をクリックします。
アウトオブバンド管理によって提供された同じ契約を選択します。

c) [Subnets] フィールドに、サブネット アドレスを入力します。[Submit] をクリックします。
ここで選択したサブネット アドレスだけがスイッチの管理に使用されます。含まれていないサブネット アドレスはスイッチの管理に使用できません。

ノード管理 EPG は、外部ネットワーク インスタンス プロファイルに接続されます。アウトオブバンド管理接続が設定されます。

CLI を使用したアウトオブバンド管理アクセスの設定

はじめる前に

APIC アウトオブバンド管理接続のリンクは、1 Gbps である必要があります。

手順の概要

1. アウトオブバンド契約を作成します。
2. アウトオブバンド契約をアウトオブバンド EPG に関連付けます。
3. アウトオブバンド契約を外部管理 EPG に関連付けます。
4. 管理アドレス プールを作成します。
5. ノード管理グループを作成します。

手順の詳細

ステップ 1 アウトオブバンド契約を作成します。

例：

```
admin@apic1:~> cd /aci/tenants/mgmt/security-policies
admin@apic1:security-policies> cd out-of-band-contracts
admin@apic1:out-of-band-contracts> moconfig commit
Committing mo 'tenants/mgmt/security-policies/out-of-band-contracts/oob-default'

All mos committed successfully.
admin@apic1:out-of-band-contracts> cd oob-default
admin@apic1:oob-default> cd subjects
admin@apic1:subjects> mocreate oob-default
admin@apic1:subjects> moconfig commit
Committing mo 'tenants/mgmt/security-policies/out-of-band-contracts/oob-default/subjects/oob-default'

All mos committed successfully.
admin@apic1:subjects> cd oob-default
admin@apic1:oob-default> cd filters
admin@apic1:filters> mocreate default
admin@apic1:filters> moconfig commit
Committing mo
'tenants/mgmt/security-policies/out-of-band-contracts/oob-default/subjects/oob-default/filters/default'

All mos committed successfully.
```

ステップ 2 アウトオブバンド契約をアウトオブバンド EPG に関連付けます。

例：

```
admin@apic1:~> cd /aci/tenants/mgmt/node-management-epgs/default
admin@apic1:default> cd out-of-band
```

```
admin@apic1:out-of-band> cd default
admin@apic1:default> cd provided-out-of-band-contracts
admin@apic1:provided-out-of-band-contracts> mocreate oob-default
admin@apic1:provided-out-of-band-contracts> moconfig commit
Committing mo
'tenants/mgmt/node-management-epgs/default/out-of-band/default/provided-out-of-band-contracts/oob-default'

All mos committed successfully.
```

ステップ 3 アウトオブバンド契約を外部管理 EPG に関連付けます。

例：

```
admin@apic1:~> cd /aci/tenants/mgmt
admin@apic1:mgmt> cd external-network-instance-profiles
admin@apic1:external-network-instance-profiles> cd external-entities-default
admin@apic1:external-entities-default> cd external-management-entity-instances
admin@apic1:external-management-entity-instances> mocreate default
Committing mo
'tenants/mgmt/external-network-instance-profiles/external-entities-default/external-management-entity-instances/default'

All mos committed successfully.
admin@apic1:external-management-entity-instances> cd default
admin@apic1:default> cd consumed-out-of-band-contracts
admin@apic1:consumed-out-of-band-contracts> mocreate oob-default
admin@apic1:consumed-out-of-band-contracts> moconfig commit
Committing mo
'tenants/mgmt/external-network-instance-profiles/external-entities-default/external-management-entity-instances/default
/consumed-out-of-band-contracts/oob-default'

All mos committed successfully.
admin@apic1:consumed-out-of-band-contracts> cd ..
admin@apic1:default> cd subnets
admin@apic1:subnets> mocreate 10.0.0.0/8
admin@apic1:subnets> moconfig commit
Committing mo
'tenants/mgmt/external-network-instance-profiles/external-entities-default/external-management-entity-instances
/default/subnets/10.0.0.0:8'

All mos committed successfully.
```

ステップ 4 管理アドレス プールを作成します。

例：

```
admin@apic1:~> cd /aci/tenants/mgmt
admin@apic1:mgmt> cd node-management-addresses
admin@apic1:node-management-addresses> cd address-pools
admin@apic1:address-pools> mocreate switchOoboobaddr
admin@apic1:address-pools> cd switchOoboobaddr
admin@apic1:switchOoboobaddr> moset gateway-address 172.23.48.1/21
admin@apic1:switchOoboobaddr> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/address-pools/switchOoboobaddr'

All mos committed successfully.
admin@apic1:switchOoboobaddr> cd address-blocks
admin@apic1:address-blocks> mocreate 172.23.49.240 172.23.49.244
admin@apic1:address-blocks> moconfig commit
Committing mo
'tenants/mgmt/node-management-addresses/address-pools/switchOoboobaddr/address-blocks/172.23.49.240-172.23.49.244'

All mos committed successfully.
```

ステップ 5 ノード管理グループを作成します。

例：

```
admin@apic1:~> cd /aci/tenants/mgmt
admin@apic1:mgmt> cd node-management-addresses
```

```
admin@apic1:node-management-addresses> cd node-groups
admin@apic1:node-groups> mocreate switchOob
admin@apic1:node-groups> cd switchOob
admin@apic1:switchOob> moset type range
admin@apic1:switchOob> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-groups/switchOob'

All mos committed successfully.
admin@apic1:switchOob> mocreate connectivity-group uni/infra/funcprof/grp-switchOob
admin@apic1:switchOob> moconfig commit
Committing mo
'tenants/mgmt/node-management-addresses/node-groups/switchOob/connectivity-group-[uni/infra/funcprof/grp-switchOob]'

All mos committed successfully.
admin@apic1:switchOob> cd node-blocks
admin@apic1:node-blocks> mocreate default
admin@apic1:node-blocks> cd default
admin@apic1:default> moset from 101
admin@apic1:default> moset to 103
admin@apic1:default> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-groups/switchOob/node-blocks/default'

All mos committed successfully.
```

REST API を使用したアウトオブバンド管理アクセスの設定

アウトオブバンド管理アクセスでは、IPv4 アドレスと IPv6 アドレスがサポートされます。

はじめる前に

APIC アウトオブバンド管理接続のリンクは、1 Gbps である必要があります。

手順の概要

1. アウトオブバンド契約を作成します。
2. アウトオブバンド契約をアウトオブバンド EPG に関連付けます。
3. アウトオブバンド契約を外部管理 EPG に関連付けます。
4. 管理アドレス プールを作成します。
5. ノード管理グループを作成します。

手順の詳細

ステップ 1 アウトオブバンド契約を作成します。

例：

```
POST
https://APIC-IP/api/mo/uni.xml

<polUni>
    <fvTenant name="mgmt">
        <!-- Contract -->
        <vzOOBBrCP name="oob-default">
```

```
            <vzSubj name="oob-default">
                <vzRsSubjFiltAtt tnVzFilterName="default" />
            </vzSubj>
        </vzOOBBrCP>
    </fvTenant>
</polUni>
```

ステップ 2 アウトオブバンド契約をアウトオブバンド EPG に関連付けます。

例：

```
POST
https://APIC-IP/api/mo/uni.xml

<polUni>
    <fvTenant name="mgmt">
        <mgmtMgmtP name="default">
            <mgmtOoB name="default">
                <mgmtRsOoBProv tnVzOOBBrCPName="oob-default" />
            </mgmtOoB>
        </mgmtMgmtP>
    </fvTenant>
</polUni>
```

ステップ 3 アウトオブバンド契約を外部管理 EPG に関連付けます。

例：

```
POST
https://APIC-IP/api/mo/uni.xml

<polUni>
    <fvTenant name="mgmt">
        <mgmtExtMgmtEntity name="default">
            <mgmtInstP name="oob-mgmt-ext">
                <mgmtRsOoBCons tnVzOOBBrCPName="oob-default" />
                <!-- SUBNET from where switches are managed -->
                <mgmtSubnet ip="10.0.0.0/8" />
            </mgmtInstP>
        </mgmtExtMgmtEntity>
    </fvTenant>
</polUni>
```

ステップ 4 管理アドレス プールを作成します。

例：

```
POST
https://APIC-IP/api/mo/uni.xml

<polUni>
    <fvTenant name="mgmt">
        <fvnsAddrInst name="switchOoboobaddr" addr="172.23.48.1/21">
            <fvnsUcastAddrBlk from="172.23.49.240" to="172.23.49.244"/>
        </fvnsAddrInst>
    </fvTenant>
</polUni>
```

ステップ 5 ノード管理グループを作成します。

例：

```
POST
https://APIC-IP/api/mo/uni.xml

<polUni>
```

```
    <infraInfra>
        <infraFuncP>
            <mgmtGrp name="switchOob">
                <mgmtOoBZone name="default">
                    <mgmtRsAddrInst tDn="uni/tn-mgmt/addrinst-switchOoboobaddr" />
                    <mgmtRsOobEpg tDn="uni/tn-mgmt/mgmtp-default/oob-default" />
                </mgmtOoBZone>
            </mgmtGrp>
        </infraFuncP>
        <mgmtNodeGrp name="switchOob">
            <mgmtRsGrp tDn="uni/infra/funcprof/grp-switchOob" />
            <infraNodeBlk name="default" from_="101" to_="103" />
        </mgmtNodeGrp>
    </infraInfra>
</polUni>
```

テクニカルサポート、統計情報、およびコアファイルのエクスポート

ファイルのエクスポートについて

管理者は、APIC 内で、コア ファイルとデバッグ データを処理するために、統計情報、テクニカル サポートの収集、障害およびイベントをファブリック（APIC およびスイッチ）から外部ホストにエクスポートするようエクスポート ポリシーを設定できます。エクスポートはXML、JSON、Web ソケット、Secure Copy Protocol（SCP）、HTTP などのさまざまな形式にできます。ストリーミング、定期的、またはオンデマンドの各形式でエクスポートを登録できます。

管理者は、転送プロトコル、圧縮アルゴリズム、転送の頻度などポリシーの詳細を設定できます。ポリシーは、AAA を使用して認証されたユーザによって設定できます。実際の転送のセキュリティ メカニズムは、ユーザ名とパスワードに基づいています。内部的に、ポリシー要素はデータのトリガーを処理します。

ファイルのエクスポートに関するガイドラインと制約事項

- HTTPエクスポートとストリーミングAPI形式は、統計情報の場合にのみサポートされます。コア情報と **テクニカル サポート** データはサポートされません。

（注） 特に、APIC、または帯域幅と計算用リソースが不足している外部サーバにエクスポートする場合は、5 つを超えるノードから同時に**テクニカル サポート**をトリガーしないでください。

ファブリック内のすべてのノードから定期的に**テクニカル サポート**を収集するには、複数のポリシーを作成する必要があります。各ポリシーは、ノードのサブセットをカバーする必要があり、時間をずらしてトリガーされるようにスケジュールします（少なくとも 30 分離す）。

ファイル エクスポート用のリモート ロケーションの作成

この手順では、エクスポートされたファイルを受け取るリモート ホストのホスト情報とファイル転送セッティングを設定します。

ステップ 1 メニュー バーで、[Admin] をクリックします。
ステップ 2 サブメニュー バーで、[Import/Export] をクリックします。
ステップ 3 [Navigation] ペインで、[Export Policies] を展開します。
ステップ 4 [Remote Locations] を右クリックし、[Create Remote Path of a File] を選択します。
ステップ 5 [Create Remote Path of a File] 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、リモート ロケーションの名前を入力します。
b) [Host Name/IP] フィールドに、送信先ホストの IP アドレスまたは完全修飾ドメイン名を入力します。
c) [Protocol] フィールドで、必要なファイル転送プロトコルのオプション ボタンをクリックします。
d) [Remote Path] フィールドで、リモート ホストでファイルが保存されるパスを入力します。
e) リモート ホストにログインするためのユーザ名とパスワードを入力し、パスワードを確認します。
f) [Management EPG] ドロップダウン リストから管理 EPG を選択します。
g) [Submit] をクリックします。

オンデマンド テクニカルサポート ファイルの送信

ステップ 1 メニュー バーで、[Admin] をクリックします。
ステップ 2 サブメニュー バーで、[Import/Export] をクリックします。
ステップ 3 [Navigation] ペインで、[Export Policies] を展開します。
ステップ 4 [On-demand TechSupport] を右クリックし、[Create On-demand TechSupport] を選択します。
ステップ 5 [Create On-demand TechSupport] 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、テクニカルサポート ファイルのエクスポート ポリシーの名前を入力します。

b) ファイルをリモート宛先ではなくコントローラにエクスポートする場合は、[Export to Controller] を選択します。
c) [Export Destination] ドロップダウン リストから、テクニカルサポート ファイルを受信する宛先ホストのプロファイルを選択します。
目的の宛先のプロファイルが表示されない場合は、[Create Remote Location] を選択してここで定義します。
d) [Data Container] ドロップダウン リストから、[uni/fabric/tscont] を選択します。
e) 目的の送信元デバイス（リーフまたはスパイン）が [Source Nodes] テーブルに表示されない場合は、[+] アイコンをクリックし、デバイスを選択して、[Update] をクリックします。
f) [Source Nodes] テーブルで送信元名をダブルクリックし、ドロップダウン リストの右にある青のアイコンをクリックして、ソース デバイスの [System Information] ウィンドウを開きます。
ソース デバイスの情報を確認するには、タブを使用します。
g) [State] フィールドで、[triggered] オプション ボタンをクリックして、ファイルを送信できるようにします。
h) [Submit] をクリックして、テクニカルサポート ファイルを送信します。
（注） オンデマンドのテクニカルサポート ファイルは別の APIC に保存し、ストレージと CPU 条件のバランスを取ることができます。場所を確認するには、[Navigation] ペインでオンデマンドのテクニカルサポート ポリシーをクリックし、[Work] ペインで [OPERATIONAL] タブをクリックします。コントローラが [EXPORT LOCATION] フィールドに表示されます。
i) ポリシー名を右クリックし、[Collect Tech Support] を選択します。
j) [Yes] を選択して、テクニカル サポート情報の収集を開始します。

概要

このトピックでは、次の情報を提供します。

- Cisco APIC の設定のインポートとエクスポートを使用して、設定の状態を最新の既知の良好な状態に回復する方法
- Cisco APIC の設定ファイルのセキュア プロパティを暗号化する方法

ユーザ設定のスケジュールバックアップとオンデマンドバックアップの両方を行うことができます。設定の状態を回復すると（「ロールバック」とも呼ばれます）、以前良好であった既知の状態に戻ることができます。そのためのオプションは、アトミック置換と呼ばれます。設定インポート ポリシー（configImportP）は、アトミック＋置換（importMode=atomic、importType=replace）をサポートします。これらの値に設定すると、インポートされる設定が既存の設定を上書きし、インポートされるファイルに存在しない既存の設定があれば削除されます。定期的な設定のバックアップとエクスポートを行うか、または既知の良好な設定のエクスポートを明示的にトリガーする限り、後で以下の CLI、REST API、および GUI 用の手順を使用してこの設定を復元することができます。

Cisco APIC を使用した設定状態の回復に関する詳細な概念情報については、『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

次の項では、設定ファイルのセキュア プロパティの暗号化に関する概念情報を提供します。

設定ファイルの暗号化

リリース 1.1(2) 以降、AES-256 暗号化を有効にすることにより APIC 設定ファイルを暗号化できます。AES 暗号化はグローバル設定オプションです。すべてのセキュア プロパティは AES 構成設定に従っています。テナント設定などの ACI ファブリック設定のサブセットを AES 暗号化を使用してエクスポートするが、ファブリック設定の残りの部分は暗号化しないということはできません。セキュア プロパティのリストについては、『Cisco Application Centric Infrastructure Fundamentals』の「Appendix K: Secure Properties」を参照してください。

APIC は、16 ～ 32 文字のパスフレーズを使用して AES-256 キーを生成します。APIC GUI では、AES パスフレーズのハッシュを表示します。このハッシュを使用して、2 つの ACI ファブリックで同じパスフレーズが使用されているかどうかを確認できます。このハッシュをクライアント コンピュータにコピーして、別の ACI ファブリックのパスフレーズ ハッシュと比較できます。これにより、それらのハッシュが同じパスフレーズを使用して生成されたかどうかを確認できます。ハッシュを使用して、元のパスフレーズまたは AES-256 キーを再構築することはできません。

暗号化された設定ファイルを使用する際は、次のガイドラインに従ってください。

- AES 暗号化設定オプションを使用しているファブリックに古い ACI 設定をインポートするための後方互換性がサポートされています。

  （注） 逆の互換性はサポートされていません。AES 暗号化が有効になっている ACI ファブリックからエクスポートされた設定を古いバージョンの APIC ソフトウェアにインポートすることはできません。

- ファブリック バックアップ設定のエクスポートを実行するときは、必ず AES 暗号化を有効にします。これにより、ファブリックを復元するときに、設定のすべてのセキュア プロパティが正常にインポートされるようになります。

  （注） AES 暗号化を有効にせずにファブリック バックアップ設定がエクスポートされると、どのセキュア プロパティもエクスポートに含まれません。そのような暗号化されていないバックアップにはセキュア プロパティは何も含まれていないため、そのようなファイルをインポートしてシステムを復元すると、ファブリックの管理者およびすべてのユーザがシステムからロックアウトされてしまう可能性があります。

- 暗号化キーを生成する AES パスフレーズは、ACI 管理者やその他のユーザが復元したり読み取ったりすることはできません。AES パスフレーズは保存されません。APIC は、AES パスフレーズを使用して AES キーを生成した後でそのパスフレーズを廃棄します。AES キーは

エクスポートされません。AES キーは、エクスポートされず、REST API を使用して取得できないため、復元できません。

- 同じ AES-256 パスフレーズは、常に同じ AES-256 キーを生成します。設定のエクスポートファイルは、同じ AES パスフレーズを使用する他の ACI ファブリックにインポートできます。
- トラブルシューティングを目的として、セキュアプロパティの暗号化データが含まれていない設定ファイルをエクスポートします。設定のエクスポートを実行する前に一時的に暗号化をオフにすると、エクスポートされた設定からすべてのセキュアプロパティ値が削除されます。すべてのセキュアプロパティが削除されたそのような設定ファイルをインポートするには、インポート マージ モードを使用します。インポート置換モードは使用しません。インポート マージ モードを使用すると、ACI ファブリック内の既存セキュア プロパティが保持されます。
- デフォルトでは、APICは復号できないフィールドが含まれているファイルの設定のインポートを拒否します。この設定をオフにするときは注意してください。このデフォルト設定がオフになっているときに設定のインポートが適切に実行されないと、ファブリックのAES暗号化設定に一致しない設定ファイルのインポート時にACIファブリックのすべてのパスワードが削除される可能性があります。

（注） このガイドラインに従わないと、ファブリック管理者を含むすべてのユーザがシステムからロックアウトされる可能性があります。

GUI を使用したリモート ロケーションの作成

この手順では、APIC GUIを使用してリモートロケーションを作成する方法について説明します。

ステップ 1 メニュー バーで、[ADMIN] タブをクリックします。

ステップ 2 [IMPORT/EXPORT] を選択します。

ステップ 3 [Import/Export] の下で、[Remote Locations] をクリックします。

[CREATE REMOTE LOCATION] ウィンドウが表示されます。

ステップ 4 [Description] フィールドに、説明を入力します（この手順は任意です）。

ステップ 5 [Host Name (or IP Address)] フィールドに、IP アドレスまたはホスト名を入力します。

ステップ 6 [scp]、[ftp]、または [sftp] のボタンを選択して、プロトコルを指定します。

ステップ 7 [Remote Path] フィールドで、パスを指定します。

ステップ 8 [Username] フィールドに、ユーザ名を入力します。

ステップ 9 [Password] フィールドにパスワードを入力し、[Confirm Password] フィールドで確認します。

ステップ 10 [Management EPG] フィールドでは、インバンド オプションまたはアウトオブバンド オプションを指定することも、空白のままにしておくこともできます。

ステップ 11 [Submit] をクリックします。
これで、データをバックアップするためのリモート ロケーションが作成されました。

GUI を使用したエクスポート ポリシーの設定

この手順では、APIC GUI を使用してエクスポート ポリシーを設定する方法について説明します。データのバックアップをトリガーするには、次の手順に従います。

ステップ 1 メニュー バーで、[Admin] タブをクリックします。

ステップ 2 [IMPORT/EXPORT] を選択します。

ステップ 3 [Export Policies] の下で、[Configuration] を選択します。

ステップ 4 [Create Configuration Export Policy] を選択します。
[CREATE CONFIGURATION EXPORT POLICY] ウィンドウが表示されます。

ステップ 5 [Name] フィールドにエクスポート ポリシーの名前を入力します。

ステップ 6 [Description] フィールドに、説明を入力します（この手順は任意です）。

ステップ 7 [Format] の横で、JSON 形式または XML 形式のいずれかに対するボタンを選択します。

ステップ 8 [Start Now] の横で、[No] または [Yes] のボタンを選択し、今すぐトリガーするかスケジュールに基づいてトリガーするかを示します（最も簡単な方法は、ただちにトリガーすることを選択することです）。

ステップ 9 設定全体のバックアップではなく部分バックアップを行う場合は、[Target DN] フィールドに名前を入力します。たとえば、1 つの特定テナントのみをバックアップする場合は、そのテナントの識別名（DN）を入力します。空白のままにすると、すべてがバックアップされます（デフォルト）。

ステップ 10 [Scheduler] フィールドで、事前プロビジョニングを選択または入力します。

ステップ 11 [Export Destination] フィールドで、データのバックアップ先のリモート ロケーションを指定します。

ステップ 12 [Submit] をクリックします。
これで、バックアップが作成されました。[Configuration] タブでこれを確認できます（右側の [Configuration] ペインにバックアップ ファイルが表示されます）。[Operational] タブがあり、そこで、実行中、成功、または失敗のどれであるかを確認できます。まだトリガーしていない場合は、空になっています。バック

アップを作成した場合、ファイルが作成され、作成したバックアップ ファイルの操作ビューに表示されます。そのデータをインポートする場合は、インポート ポリシーを作成する必要があります。

GUI を使用したインポート ポリシーの設定

この手順では、APIC GUI を使用してインポート ポリシーを設定する方法について説明します。バックアップ データをインポートするには、次の手順に従います。

ステップ 1 メニュー バーで、[ADMIN] タブをクリックします。

ステップ 2 [IMPORT/EXPORT] を選択します。

ステップ 3 [Import Policies] の下で、[Configuration] を選択します。

ステップ 4 [Configuration] の下で、[Create Configuration Import Policy] を選択します。
[CREATE CONFIGURATION IMPORT POLICY] ウィンドウが表示されます。

ステップ 5 [Name] フィールドでは、ファイル名は、バックアップされたファイル名と一致する必要があり、かなり固有の形式です。ファイル名は、バックアップを行った担当者が知っています。

ステップ 6 次の 2 つのオプションは、設定の状態の回復に関連しています（「ロールバック」とも呼ばれる）。これらのオプションは、[Input Type] と [Input Mode] です。設定の状態を回復する場合、以前良好であった既知の状態にロールバックします。そのためのオプションは [Atomic Replace] です。
[Replace]、[Merge]、[Best Effort]、[Atomic] などの入力タイプやモードの詳細については、『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

ステップ 7 [Import Source] フィールドで、作成済みのリモート ロケーションと同じ値を指定します。

ステップ 8 設定が完了したら、[Start Now] をクリックします。

ステップ 9 [Submit] をクリックします。

CLI を使用したエクスポート ポリシーの設定

CLI を使用してエクスポート ポリシーを設定するには、次のように入力します。

```
cd /aci/admin/import-export/export-policies/configuration
admin@trunk13-ifc1:configuration> mocreate myExport
admin@trunk13-ifc1:configuration> cd myExport
admin@trunk13-ifc1:myExport> moset export-destination myServer
admin@trunk13-ifc1:myExport> moconfig commit
Committing mo 'admin/import-export/export-policies/configuration/myExport'

All mos committed successfully.
```

CLI を使用したインポート ポリシーの設定

CLI を使用してインポート ポリシーを設定するには、次のように入力します。

```
cd /aci/admin/import-export/import-policies
admin@trunk13-ifc1:import-policies> mocreate myImport
admin@trunk13-ifc1:import-policies> cd myImport
admin@trunk13-ifc1:myImport> moset file-name ce_export-2014-07-03T21-59-14.tar.gz
admin@trunk13-ifc1:myImport> moconfig commit
Committing mo 'admin/import-export/import-policies/myImport'

All mos committed successfully
```

REST API を使用したエクスポート ポリシーの設定

REST API を使用してエクスポート ポリシーを設定するには、次の手順に従います。

```
POST
https://<ip-of-apic>/api/mo/uni/fabric.xml
<fabricInst dn="uni/fabric">
<configExportP name="export" format="xml" adminSt="triggered">
<configRsExportDestination tnFileRemotePathName="backup" />
</configExportP>
<fileRemotePath name="backup" host="10.10.10.1" protocol="scp"
remotePath="/home/user" userName="user" userPasswd="pass" />
</fabricInst>
```

REST API を使用したインポート ポリシーの設定

REST API を使用してインポート ポリシーを設定するには、次の手順に従います。

```
POST
https://<ip-of-apic>/api/mo/uni/fabric.xml
<fabricInst dn="uni/fabric">
<configImportP name="imp" fileName="aa.tar.gz" adminSt="triggered" importType="replace"
importMode="best-effort">
<configRsImportSource tnFileRemotePathName="backup" />
</configImportP>
<fileRemotePath name="backup" host="10.10.10.1" protocol="scp"
remotePath="/home/user" userName="user" userPasswd="pass" />
</fabricInst>
```

GUI を使用した設定ファイルの暗号化

APIC GUI を使用して設定ファイルを暗号化するには、次の手順に従います。

ステップ 1 メニュー バーで、[ADMIN] タブを選択します。

ステップ 2 [ADMIN] タブの下で [AAA] タブを選択します。

ステップ 3 左側のナビゲーション ペインで、[AES Encryption Passphrase and Keys for Config Export (and Import)] を選択します。

右側のペインに、[Global AES Encryption Settings for all Configurations Import and Export] ウィンドウが表示されます。

ステップ 4 パスフレーズを作成します（16 ～ 32 文字の長さ）。使用される文字のタイプに制限はありません。

ステップ 5 [Submit] をクリックします。

（注） パスフレーズを作成して送信すると、バックエンドでキーが生成され、パスフレーズを復元することはできません。したがって、パスフレーズは、キーを自動的に生成した後で削除されるため、誰にも表示されません。バックアップは、パスフレーズを知っている場合にのみ動作します（他のユーザは誰も開くことはできません）。

[Key Configured] フィールドには [yes] と表示されます。[Encrpyted Passphrase] フィールドには暗号化されたハッシュ（実際のパスフレーズではなく、そのハッシュでしかありません）が表示されます。

ステップ 6 パスフレーズを設定して確認したら、[Enable Encryption] の横にあるチェックボックスをクリックして、AES 暗号化機能をオンまたはオフにします。

（注） このチェックボックスにマークが付いておらず（オフ）暗号化が無効になっている場合、エクスポートされるすべての設定（エクスポート）に、セキュア フィールド（パスワードや証明書など）は含まれていません。このボックスにマークを付けると（オン）、すべてのエクスポートでセキュア フィールドが表示されます。

ステップ 7 [ADMIN] タブの下で [IMPORT/EXPORT] を選択します。

ステップ 8 左側のナビゲーション ペインで [Import Policies] を選択します。

ステップ 9 [Import Policies] の下で [Configuration] を選択します。

前に [Enable Encryption] をオンにした場合、左側のナビゲーション ペインの [Configuration] の下に設定インポート ポリシー（またはポリシーのリスト）が表示され、そのプロパティを設定できます。

ステップ 10 [Fail Import if secure fields cannot be decrypted] の横にあるチェックボックスがオンになっている（デフォルトの選択）ことを確認します。

（注） このチェックボックスは、デフォルトでオンになっています。設定をインポートするときにこのチェックボックスをオフにしないことを強くお勧めします。このボックスをオフにすると、システムはすべてのフィールドのインポートを試みますが、暗号化できないフィールドはブランクまたは欠落となります。その結果、管理者のパスワードがブランクまたは欠落しているためにユーザがシステムからロックアウトされてしまう可能性があります（システムからロックアウトされた場合は、『Cisco APIC Troubleshooting Guide』を参照してください）。このボックスをオフにすると、警告メッセージのポップアップ画面が表示されます。このボックスをオンにすると、ロックアウトを予防するためのセキュリティ チェックが行われ、その設定はインポートされません。

ステップ 11 左側のナビゲーション ペインの [Export Policies] タブの下の [Configuration] タブで、設定ファイルをエクスポートするためのプロパティを設定することもできます。

前に説明した設定インポート ポリシーのプロパティの設定と同じ手順に従います。

（注） このセクションではパスフレーズを設定できません。前に設定したパスフレーズは、このボックス内のすべての設定およびすべてのテナントにわたってグローバルになっています。このタブから設定をエクスポートすると（パスフレーズが設定され、暗号化は有効）、完全なバックアップ ファイルが得られます。暗号化が有効になっていない場合、セキュア プロパティが削除されたバックアップ ファイルが得られます。これらのバックアップ ファイルは、TAC サポートエンジニア向けにエクスポートする場合に役立ちます（たとえば、すべてのセキュア フィールドが欠落しているため）。これは、設定内のすべてのセキュアプロパティに該当します。また、暗号化キーをクリアするクリア オプションもあります。

ステップ 12 次の表で、設定インポートの動作と関連する結果のリストに注意してください。

設定インポートの動作シナリオ	結果
以前のリリースからの古い設定	古いリリースの設定のインポートは完全にサポートされ、古い設定に保存されているすべてのセキュア フィールドが正常にインポートされます。
AES 暗号化が設定されていないときの設定インポート	セキュア フィールドがない設定のインポートである場合は、前に説明した動作で正常に行われます。インポートされる設定にセキュア フィールドがある場合は、拒否されます。
AES パスフレーズが一致しないときの設定インポート	セキュア フィールドがない設定のインポートである場合は、前に説明した動作で正常に行われます。インポートされる設定にセキュア フィールドがある場合は、拒否されます。
AES パスフレーズが一致するときの設定インポート	正常にインポートされます。
コピー/ペーストされたフィールドで AES パスフレーズが一致しないときの設定インポート	この特定のケースは、別のパスフレーズを使用してエクスポートされた他の設定からのセキュア フィールドを、ユーザがコピー/ペーストした場合に発生します。最初のパスでインポートされるバックアップ ファイルを解析しているときに、正しく復号できないプロパティがあった場合、インポートはどのシャードもインポートせずに失敗します。したがって、あるシャードですべてのプロパティを復号することができない場合、すべてのシャードが拒否されます。

CLI を使用した設定ファイルの暗号化

CLI を使用して設定ファイルの暗号化を設定するには、次のようにします。
エディタでオブジェクトを開き、passphrase と strongEncryption:yes を設定します。

```
admin@ifav74-ifc1:exportcryptkey> vi /mit/uni/exportcryptkey/mo

# AES Encryption Passphrase and Keys for Config Export (and Import)


# Configurable Properties:
clearEncryptionKey             : no
descr                          : Object was created during upgrade
name                           :
ownerKey                       :
ownerTag                       :
passphrase                     : abcdefghijklmnopqrstuvwxyz
passphraseKeyDerivationVersion : v1
strongEncryptionEnabled        : yes

Save file and

admin@ifav74-ifc1:exportcryptkey> moconfig commit
Committing mo 'uni/exportcryptkey'

All mos committed successfully.
admin@ifav74-ifc1:exportcryptkey>
```

REST API を使用した設定ファイルの暗号化

REST API を使用して設定ファイルを暗号化するには、次のように入力します。

```
POST
https://<ip-of-apic>/api/mo/uni/fabric.xml
<pkiExportEncryptionKey passphrase="abcdefghijklmnopqrstuvwxyz"
strongEncryptionEnabled="true"/>
```

コントローラコンフィギュレーションのバックアップ、復元、およびロールバック

ここでは、コントローラ コンフィギュレーションのバックアップ（スナップショットの作成）、復元、およびロールバックのための一連の機能について説明します。

ワークフロー

この項では、設定ファイルのバックアップ、復元、およびロールバックのワークフローについて説明します。本書で説明されている機能はすべて同じワークフロー パターンに従います。対応するポリシーを設定すると、ジョブをトリガーするために **admintSt** を **triggered** に設定する必要があります。

トリガーされると、タイプ **configJob**（その実行を表す）のオブジェクトがタイプ **configJobCont**（名前付けプロパティ値をポリシー DN に設定）のコンテナ オブジェクトに作成されます。コンテナの **lastJobName** フィールドを使用して、そのポリシーに対してトリガーされた最後のジョブを確認することができます。

（注） 同時に最大 5 つの configJob オブジェクトが単一ジョブ コンテナに保持され、それぞれの新規ジョブがトリガーされます。そのために、最も古いジョブは削除されます。

configJob オブジェクトには、次の情報が含まれています。

- 実行時間
- 処理または生成されるファイルの名前
- 以下のステータス：
  - pending
  - running
  - failed
  - fail-no-data
  - success
  - success-with-warnings
- 詳細の文字列（障害メッセージと警告）
- 進捗率 = 100 * lastStepIndex/totalStepCount
- 最後に行われた内容を示す lastStepDescr フィールド

Remote Path

fileRemotePath オブジェクトは、以下のリモート ロケーション パスのパラメータを保持しています。

- ホスト名または IP
- ポート
- プロトコル：ftp、scp など

- リモート ディレクトリ（ファイル パスではない）
- ユーザ名
- パスワード

（注） パスワードは、変更するたびに再送信する必要があります。

設定例

以下に設定サンプルを示します。

fabricInst（uni/fabric）の下に、次のように入力します。

```
<fileRemotePath name="path-name" host="host name or ip" protocol="scp"
remotePath="path/to/some/folder" userName="user-name" userpasswd="password" />
```

コントローラへの設定のエクスポート

設定のエクスポートでは、クラスタ内の32個のシャードすべてからユーザ設定可能な管理対象オブジェクト（MO）のツリーを抽出して別々のファイルに書き込み、tar gzipに圧縮します。次に、tar gzip を、事前設定されているリモート ロケーション（**fileRemotePath** オブジェクトを指す **configRsRemotePath** を使用して設定）にアップロードするか、またはコントローラ上の**スナップショット**として保存します。

（注） 詳細については、「スナップショット」の項を参照してください。

configExportP ポリシーは次のように設定されます。

- **name**：ポリシー名
- **format**：エクスポートされたアーカイブ内にデータを保存する形式（xml または json）
- **targetDn**：エクスポートする特定のオブジェクトのドメイン名（DN）（空はすべてを意味します）
- **snapshot**：true の場合、ファイルはコントローラ上に保存され、リモート ロケーションの設定は不要です。
- **includeSecureFields**：デフォルトで true に設定され、暗号化されたフィールド（パスワードなど）をエクスポートのアーカイブに含めるかどうかを示します。

（注） このスナップショットに関する情報を保持する **configSnapshot** オブジェクトが作成されます（「スナップショット」の項を参照）。

エクスポートのスケジューリング

エクスポート ポリシーは、事前設定されたスケジュールに基づいて自動的にエクスポートをトリガーするスケジューラーにリンクできます。これは、ポリシーから **trigSchedP** オブジェクトへの **configRsExportScheduler** 関係によって行われます（後の「設定例」の項を参照）。

（注） スケジューラーはオプションです。ポリシーは、adminSt を **triggered** に設定することにより、いつでもトリガーできます。

トラブルシューティング

生成されたアーカイブをリモート ロケーションにアップロードできないことを示すエラー メッセージが表示された場合は、接続の問題に関する項を参照してください。

NX-OS スタイルの CLI を使用した設定例

以下に、NX-OS スタイルの CLI を使用した設定例を示します。

```
apic1(config)# snapshot
 download  Configuration snapshot download setup mode
export    Configuration export setup mode
import    Configuration import setup mode
rollback  Configuration rollback setup mode
upload    Configuration snapshot upload setup mode
apic1(config)# snapshot export policy-name
apic1(config-export)#
 format    Snapshot format: xml or json
no        Negate a command or set its defaults
remote    Set the remote path configuration will get exported to
schedule  Schedule snapshot export
target    Snapshot target

bash      bash shell for unix commands
end       Exit to the exec mode
exit      Exit from current mode
fabric    show fabric related information
show      Show running system information
where     show the current mode
apic1(config-export)# format xml
apic1(config-export)# no remote path             [If no remote path is specified, the file
 is exported locally to a folder in the controller]
apic1(config-export)# target                     [Assigns the target of the export, which
can be fabric, infra, a specific tenant, or none. If no target is specified, all configuration
 information is exported.]
WORD  infra, fabric or tenant-x
apic1(config-export)#
apic1# trigger snapshot export policy-name       [Executes the snapshot export task]
```

GUI を使用した設定例

以下に、GUI を使用した設定例を示します。

1. メニュー バーで、[ADMIN] タブをクリックします。
2. [IMPORT/EXPORT] を選択します。
3. [Export Policies] の下で、[Configuration] を選択します。
4. [Configuration] の下で、ロールバック先の設定をクリックします。たとえば、デフォルトである [defaultOneTime] をクリックできます。

5 [Format] の横で、JSON 形式または XML 形式のいずれかに対するボタンを選択します。
6 [Start Now] の横で、[No] または [Yes] のボタンを選択し、今すぐトリガーするかスケジュールに基づいてトリガーするかを示します（最も簡単な方法は、ただちにトリガーすることを選択することです）。
7 [Target DN] フィールドに、エクスポートするテナント設定の名前を入力します。
8 設定をコントローラ自体に保存する場合は、[Snapshot] オプションをオンにします。リモートロケーションを設定する場合は、このオプションをオフにします。
9 [Scheduler] フィールドでは、オプションで、設定をエクスポートする時間と方法を指示するスケジューラを作成できます。
10 [Encryption] フィールドでは、オプションで、設定ファイルの暗号化を

有効または無効にすることができます。
11 設定が完了したら、[Start Now] をクリックします。
12 [SUBMIT] をクリックして、設定のエクスポートをトリガーします。

REST API を使用した設定例

以下に、REST API を使用した設定例を示します。

```
<configExportP name="policy-name" format="xml" targetDn="/some/dn or empty which means
everything"
snapshot="false" adminSt="triggered">
<configRsRemotePath tnFileRemotePathName="some remote path name" />
<configRsExportScheduler tnTrigSchedPName="some scheduler name" />
</configExportP>
```

（注） リモートロケーションを指定するときに、スナップショットを True に設定すると、バックアップはリモート パスを無視し、ファイルをコントローラに保存します。

コントローラへの設定のインポート

設定のインポートでは、指定されている以前にエクスポートされたアーカイブのダウンロード、抽出、解析、分析、および適用を、一度に 1 つのシャードずつ行います（infra、fabric、tn-common、その他すべて、の順）。fileRemotePath 設定は、エクスポートの場合と同様に実行されます（configRsRemotePath を使用）。スナップショットのインポートもサポートされます。

configImportP ポリシーは次のように設定されます。

- **name**：ポリシー名
- **fileName**：インポートするアーカイブ ファイルの名前（パス ファイルではない）
- **importMode**
  - ベスト エフォート モード：各 MO は個々に適用され、エラーがあっても無効な MO がスキップされるだけです。

（注） オブジェクトがコントローラに存在しない場合、そのオブジェクトの子は設定されません。ベスト エフォート モードでは、オブジェクトの子を設定しようとします。

- アトミック モード：設定はシャード全体で適用されます。1つのエラーがあると、シャード全体が元の状態にロールバックされます。

- **importType**
  - replace：現在のシステム設定は、インポートされる内容またはアーカイブで置換されます（アトミック モードのみをサポート）
  - merge：何も削除されず、アーカイブの内容が既存のシステム設定上に適用されます。

- **snapshot**：true の場合、ファイルはコントローラから取得され、リモート ロケーションの設定は不要です。
- **failOnDecryptErrors**：（デフォルトで true）現在システムに設定されているキーとは異なるキーでアーカイブが暗号化されている場合、ファイルはインポートされません。

トラブルシューティング

以下のシナリオでは、トラブルシューティングが必要な可能性があります。

- 生成されたアーカイブをリモート ロケーションからダウンロードできなかった場合は、接続の問題に関する項を参照してください。
- インポートは正常に終了したが警告が表示された場合は、詳細を確認してください。
- ファイルを解析できなかった場合は、以下のシナリオを参照してください。
  - ファイルが有効な XML または JSON ファイルでない場合は、エクスポートされたアーカイブから取得したファイルが手動で変更されたかどうかを確認してください。
  - オブジェクト プロパティに未知のプロパティまたはプロパティ値がある場合は、以下の原因が考えられます。
    - プロパティが削除されたか、または未知のプロパティ値が手動で入力された
    - モデル タイプの範囲が変更された（後方互換性がないモデル変更）
    - 名前付けプロパティ リストが変更された

- MO を設定できなかった場合は、以下に注意してください。
  - ベスト エフォート モードでは、エラーをログに記録し、その MO をスキップします
  - アトミック モードでは、エラーをログに記録し、シャードをスキップします

NX-OS スタイルの CLI を使用した設定例

以下に、NX-OS スタイルの CLI を使用した設定例を示します。

```
ifav101-apic1# configure
ifav101-apic1(config)# snapshot
 download  Configuration snapshot download setup mode
export    Configuration export setup mode
import    Configuration import setup mode
rollback  Configuration rollback setup mode
upload    Configuration snapshot upload setup mode
ifav101-apic1(config)# snapshot import
 WORD       Import configuration name
default
rest-user
ifav101-apic1(config)# snapshot import policy-name
ifav101-apic1(config-import)#
 action  Snapshot import action merge|replace
file    Snapshot file name
mode    Snapshot import mode atomic|best-effort
no      Negate a command or set its defaults
remote  Set the remote path configuration will get imported from

bash    bash shell for unix commands
end     Exit to the exec mode
exit    Exit from current mode
fabric  show fabric related information
show    Show running system information
where   show the current mode
ifav101-apic1(config-import)# file < from "show snapshot files" >
ifav101-apic1(config-import)# no remote path
ifav101-apic1(config-import)#
ifav101-apic1# trigger snapshot import policy-name      [Executes the snapshot import task]
```

GUI を使用した設定例

以下に、GUI を使用した設定例を示します。

1. メニュー バーで、[ADMIN] タブをクリックします。
2. [IMPORT/EXPORT] を選択します。
3. [Import Policies] の下で、[Configuration] を選択します。
4. [Configuration] の下で、[Create Configuration Import Policy] を選択します。[CREATE CONFIGURATION IMPORT POLICY] ウィンドウが表示されます。
5. [Name] フィールドでは、ファイル名は、バックアップされたファイル名と一致する必要があり、かなり固有の形式です。ファイル名は、バックアップを行った担当者が知っています。
6. 次の2つのオプションは、設定の状態の回復に関連しています（「ロールバック」とも呼ばれる）。これらのオプションは、[Input Type] と [Input Mode] です。設定の状態を回復する場合、以前良好であった既知の状態にロールバックします。そのためのオプションは[Atomic Replace] です。[Replace]、[Merge]、[Best Effort]、[Atomic] などの入力タイプやモードの詳細については、『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。
7. 設定をコントローラ自体に保存する場合は、[Snapshot] オプションをオンにします。リモートロケーションを設定する場合は、このオプションをオフにします。
8. [Import Source] フィールドで、作成済みのリモート ロケーションと同じ値を指定します。
9. [Encryption] フィールドでは、オプションで、設定ファイルの暗号化を

   有効または無効にすることができます。
10. [SUBMIT] をクリックして、設定のインポートをトリガーします。

REST API を使用した設定例

以下に、REST API を使用した設定例を示します。

```
<configImportP name="policy-name" fileName="someexportfile.tgz" importMode="atomic"
importType="replace" snapshot="false" adminSt="triggered">
<configRsRemotePath tnFileRemotePathName="some remote path name" />
</configImportP>
```

スナップショット

スナップショットは設定のバックアップのアーカイブであり、コントローラで管理されているフォルダに保存（および複製）されます。スナップショットを作成するには、**snapshot** プロパティを true に設定してエクスポートを実行します。この場合、リモート パスの設定は不要です。スナップショットをユーザに公開するために、**configSnapshot** タイプのオブジェクトが作成されます。

configSnapshot オブジェクトは以下を提供します。

- ファイル名
- ファイルサイズ
- 作成日
- 何のスナップショットであるかを示すルート DN（ファブリック、インフラ、特定のテナントなど）
- スナップショットを削除する機能（retire フィールドを true に設定）

スナップショットをインポートするには、インポート ポリシーの snapshot プロパティを true に設定し、スナップショット ファイルの名前を指定します（configSnapshot から）。

スナップショット マネージャ ポリシー

configSnapshotManagerP ポリシーを使用すると、リモートで保存したエクスポート アーカイブのスナップショットを作成することができます。ポリシーにリモート パスを付加し、ファイル名（configImportP と同じ）を指定し、モードをダウンロードに設定し、トリガーすることができます。マネージャは、ファイルをダウンロードし、そのファイルを分析してアーカイブが有効であることを確認し、そのファイルをコントローラに保存し、対応する configSnapshot オブジェクトを作成します。スナップショット マネージャを使用すると、リモート ロケーションにスナップショット アーカイブをアップロードすることもできます。この場合、モードをアップロードに設定する必要があります。

トラブルシューティング

トラブルシューティングについては、接続の問題に関する項を参照してください。

NX-OS CLI を使用した、コントローラからリモート パスへのスナップショットのアップロード

```
apic1(config)# snapshot upload policy-name
apic1(config-upload)#
 file    Snapshot file name
```

```
no      Negate a command or set its defaults
remote  Set the remote path configuration will get uploaded to

bash    bash shell for unix commands
end     Exit to the exec mode
exit    Exit from current mode
fabric  show fabric related information
show    Show running system information
where   show the current mode
apic1(config-upload)# file <file name from "show snapshot files">
apic1(config-upload)# remote path remote-path-name
apic1# trigger snapshot upload policy-name       [Executes the snapshot upload task]
```

NX-OS CLI を使用した、コントローラからリモート パスへのスナップショットのダウンロード

```
apic1(config)# snapshot download policy-name
apic1(config-download)#
 file    Snapshot file name
no      Negate a command or set its defaults
remote  Set the remote path configuration will get downloaded from

bash    bash shell for unix commands
end     Exit to the exec mode
exit    Exit from current mode
fabric  show fabric related information
show    Show running system information
where   show the current mode
apic1(config-download)# file < file from remote path>
apic1(config-download)# remote path remote-path-name
apic1# trigger snapshot download policy-name       [Executes the snapshot download task]
```

GUI を使用したスナップショットのアップロードとダウンロード

スナップショットファイルをリモートロケーションにアップロードするには、次の手順に従います。

1. [Config Rollbacks] ペインにリストされているスナップショットを右クリックし、[Upload to Remote Location option] を選択します。[Upload snapshot to remote location] ボックスが表示されます。
2. [Submit] をクリックします。

リモートロケーションからスナップショットファイルをダウンロードするには、次の手順に従います。

1. 画面の右上にあるインポート アイコンをクリックします。[Import remotely stored export archive to snapshot] ボックスが表示されます。
2. [File Name] フィールドにファイル名を入力します。
3. [Import Source] プルダウンからリモート ロケーションを選択するか、または [Or create a new one] の横にあるボックスをオンにして新しいリモート ロケーションを作成します。
4. [Submit] をクリックします。

REST API を使用したスナップショットのアップロードとダウンロード

```
<configSnapshotManagerP name="policy-name" fileName="someexportfile.tgz"
mode="upload|download" adminSt="triggered">
<configRsRemotePath tnFileRemotePathName="some remote path name" />
</configSnapshotManagerP>
```

ロールバック

configRollbackP ポリシーは、2 つのスナップショット間で行われた変更を元に戻すために使用されます。オブジェクトは、次のように処理されます。

- 削除された MO を再作成します
- 作成された MO を削除します
- 変更された MO を元に戻します

（注） ロールバック機能はスナップショットに対してのみ動作します。リモートアーカイブはサポートされません。リモート アーカイブを使用するには、スナップショット マネージャを使用してそこからロールバック用のスナップショットを作成することができます。ポリシーでは、リモート パス設定は不要です。指定されていても、無視されます。

ロールバックのワークフロー

ポリシーの snapshotOneDN フィールドと snapshotTwoDn フィールドを設定する必要があり、最初のスナップショット（S1）がスナップショット 2（S2）より前である必要があります。トリガーされると、スナップショットが抽出および分析され、それらの間の違いが計算され、適用されます。

MO の場所：

- S1 に存在するが、S2 には存在しない：これらの MO は削除され、ロールバックにより再作成されます
- S1 には存在しないが、S2 には存在する：これらの MO は S1 後に作成されており、以下に該当する場合はロールバックにより削除されます。
  - これらの MO は S2 取得後に変更されていない
  - S2 取得後に作成または変更された MO の子孫がない
- S1 と S2 の両方に存在するが、プロパティ値は異なる：S2 取得後にプロパティが別の値に変更されていない限り、これらの MO プロパティは S1 に戻されます。この場合、現状どおりになります。

  ロールバック機能では、これらの計算の結果として生成された設定が含まれている diff ファイルも生成されます。この設定の適用は、ロールバック プロセスの最後のステップです。このファイルの内容は、readiff と呼ばれる特殊な REST API を使用して取得できます。apichost/mqapi2/snapshots.readiff.xml?jobdn=SNAPSHOT_JOB_DN

  ロールバック（予測は困難）にはプレビュー モード（preview を true に設定）もあり、ロールバックにより実際の変更が行われないようにします。diffファイルを計算して生成し、ロールバックを実際に実行したときに何が発生するかを正確にプレビューできます。

Diff ツール

2 つのスナップショット間の diff 機能を提供する別の特殊な REST API を使用できます。
apichost/mqapi2/snapshots.diff.xml?s1dn=SNAPSHOT_ONE_DN&s2dn=SNAPSHOT_TWO_DN

NX-OS スタイルの CLI を使用した設定例

この例では、NX-OS スタイルの CLI を使用してロールバックを設定および実行する方法を示します。

```
apic1# show snapshot files
File    : ce2_DailyAutoBackup-2015-11-21T01-00-17.tar.gz
Created : 2015-11-21T01:00:21.167+00:00
Root    :
Size    : 22926

File    : ce2_DailyAutoBackup-2015-11-21T09-00-21.tar.gz
Created : 2015-11-21T09:00:24.025+00:00
Root    :
Size    : 23588

apic1# configure
apic1(config)# snapshot rollback myRollbackPolicy
apic1(config-rollback)# first-file ce2_DailyAutoBackup-2015-11-21T01-00-17.tar.gz
apic1(config-rollback)# second-file ce2_DailyAutoBackup-2015-11-21T09-00-21.tar.gz
apic1(config-rollback)# preview
apic1(config-rollback)# end
apic1# trigger snapshot rollback myRollbackPolicy
```

GUI を使用した設定例

この例では、GUI を使用してロールバックを設定および実行する方法を示します。

1. メニュー バーで、[Admin] タブをクリックします。
2. [Admin] タブにある [Config Rollbacks] をクリックします。
3. [Config Rollbacks] リスト（左側のペイン）で最初の設定ファイルを選択します。
4. [Configuration for selected snapshot] ペイン（右側のペイン）で 2 番目の設定ファイルを選択します。
5. [Compare with previous snapshot] ドロップダウン メニュー（右側のペインの下部）をクリックし、リストから 2 番目の設定ファイルを選択します。その後、2 つのスナップショット間の違いを比較できるように diff ファイルが生成されます。

（注） ファイルが生成された後、これらの変更を元に戻すことができます。

REST API を使用した設定例

この例では、REST API を使用してロールバックを設定および実行する方法を示します。

```
<configRollbackP name="policy-name" snapshotOneDn="dn/of/snapshot/one"
snapshotOneDn="dn/of/snapshot/two" preview="false" adminSt="triggered" />
```

Syslog の使用

Syslog について

稼働中、シスコ アプリケーション セントリック インフラストラクチャ（ACI）システムでの障害またはイベントは、コンソール、ローカル ファイル、および別のシステム上のロギング サーバへのシステム ログ（syslog）の送信をトリガーできます。システム ログ メッセージには、通常、障害またはイベントに関する情報のサブセットが含まれます。システム ログ メッセージには、監査ログとセッション ログのエントリを含めることもできます。

（注） APIC およびファブリック ノードが生成できる syslog メッセージのリストについては、http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/syslog/guide/aci_syslog/ACI_SysMsg.html を参照してください。

多くのシステム ログ メッセージは、ユーザが実行している処理、あるいはユーザが設定または管理しているオブジェクトに固有のものです。これらのメッセージには次のようなものがあります。

- 情報メッセージ。実行している処理のヘルプおよびヒントを提供します。
- 警告メッセージ。ユーザが設定または管理しているオブジェクト（ユーザ アカウントやサービス プロファイルなど）に関連するシステム エラーの情報を提供します。

システム ログ メッセージを受信してモニタするためには、syslog 宛先（コンソール、ローカル ファイル、または syslog サーバを実行している 1 つ以上のリモート ホスト）を指定する必要があります。また、コンソールに表示されるか、ファイルまたはホストによってキャプチャされるメッセージの重大度の最小値を指定できます。syslog メッセージを受信するローカル ファイルは `/var/log/external/messages` です。

Syslog 送信元は、オブジェクト モニタリング ポリシーを適用できる任意のオブジェクトにすることができます。送信されるメッセージの重大度の最小値、syslog メッセージに含める項目、および syslog の宛先を指定できます。

これらのシステム メッセージを生成する障害またはイベントの詳細については、『*Cisco APIC Faults, Events, and System Messages Management Guide*』で説明されており、システム ログ メッセージは『*Cisco ACI System Messages Reference Guide*』にリストされています。

（注） システム ログ メッセージは、必ずしもシステムに問題があることを示しているとは限りません。単に情報を通知するだけのメッセージもありますし、通信回線、内部ハードウェア、またはシステム ソフトウェアに関する問題点の診断に役立つメッセージもあります。

Syslog の宛先および宛先グループの作成

この手順では、ロギングおよび評価用の syslog データの宛先を設定します。syslog データは、コンソール、ローカル ファイル、または宛先グループ内の 1 つまたは複数の syslog サーバにエクスポートできます。

ステップ 1 メニュー バーで、[Admin] をクリックします。

ステップ 2 サブメニュー バーで、[External Data Collectors] をクリックします。

ステップ 3 [Navigation] ペインで、[Monitoring Destinations] を展開します。

ステップ 4 [Syslog] を右クリックし、[Create Syslog Monitoring Destination Group] を選択します。

ステップ 5 [Create Syslog Monitoring Destination Group] ダイアログボックスで、次の操作を実行します。

a) グループおよびプロファイルの [Name] フィールドに、モニタリングの宛先グループおよびプロファイルの名前を入力します。

b) グループおよびプロファイルの [Admin State] ドロップダウン リストで、[enabled] を選択します。

c) ローカル ファイルへの syslog メッセージの送信を有効にするには、[Local File Destination] の [Admin State] ドロップダウン リストから [enabled] を選択し、[Local File Destination] の [Severity] ドロップダウン リストから重大度の最小値を選択します。
syslog メッセージを受信するローカル ファイルは `/var/log/external/messages` です。

d) コンソールへの syslog メッセージの送信を有効にするには、[Console Destination] の [Admin State] ドロップダウン リストから [enabled] を選択し、[Console Destination] の [Severity] ドロップダウン リストから重大度の最小値を選択します。

e) [Next] をクリックします。

f) [Create Remote Destinations] 領域で、[+] をクリックしてリモート宛先を追加します。

ステップ 6 [Create Syslog Remote Destination] ダイアログボックスで、次の操作を実行します。

a) [Host] フィールドに、送信先ホストの IP アドレスまたは完全修飾ドメイン名を入力します。

b) （任意） [Name] フィールドに、宛先ホストの名前を入力します。

c) [Admin State] フィールドで、[enabled] オプション ボタンをクリックします。

d) （任意） 重大度の最小値 [Severity]、[Port] 番号、および syslog の [Forwarding Facility] を選択します。

e) [Management EPG] ドロップダウン リストから管理エンドポイント グループを選択します。

f) [OK] をクリックします。

ステップ 7 （任意） リモート宛先グループにリモート宛先を追加するには、もう一度 [+] をクリックし、[Create Syslog Remote Destination] ダイアログボックスの手順を繰り返します。

ステップ 8 [Finish] をクリックします。

Syslog 送信元の作成

Syslog 送信元は、オブジェクト モニタリング ポリシーを適用できる任意のオブジェクトにすることができます。

はじめる前に

syslog モニタリング宛先グループを作成します。

ステップ 1 メニュー バーおよびナビゲーション フレームから、関心領域の [Monitoring Policies] メニューに移動します。
テナント、ファブリック、およびアクセスのモニタリング ポリシーを設定できます。

ステップ 2 [Monitoring Policies] を展開し、モニタリング ポリシーを選択して展開します。
[Fabric] > [Fabric Policies] > [Monitoring Policies] > [Common Policy] の下に、基本モニタリング ポリシーがあります。このポリシーは、すべての障害とイベントに適用され、ファブリック内のすべてのノードとコントローラに自動的に導入されます。または、スコープが限定された既存のポリシーを指定することもできます。

ステップ 3 モニタリング ポリシーの下で、[Callhome/SNMP/Syslog] をクリックします。

ステップ 4 [Work] ペインで、[Source Type] ドロップダウン リストから [Syslog] を選択します。

ステップ 5 [Monitoring Object] リストから、モニタ対象の管理対象オブジェクトを選択します。
目的のオブジェクトがリストに表示されない場合は、次の手順に従います。

a) [Monitoring Object] ドロップダウン リストの右側にある [Edit] アイコンをクリックします。
b) [Select Monitoring Package] ドロップダウン リストから、オブジェクト クラス パッケージを選択します。
c) モニタ対象の各オブジェクトのチェックボックスをオンにします。
d) [Submit] をクリックします。

ステップ 6 テナント モニタリング ポリシーでは、[All] ではなく特定のオブジェクトを選択すると、[Scope] 選択が表示されます。
[Scope] フィールドで、オプション ボタンを選択して、このオブジェクトに関して送信するシステム ログ メッセージを指定します。

- all：このオブジェクトに関連するすべてのイベントと障害を送信します。
- specific event：このオブジェクトに関連する指定されたイベントのみを送信します。[Event] ドロップダウン リストからイベント ポリシーを選択します。
- specific fault：このオブジェクトに関連する指定された障害のみを送信します。[Fault] ドロップダウン リストから障害ポリシーを選択します。

ステップ 7 [+] をクリックして syslog 送信元を作成します。

ステップ 8 [Create Syslog Source] 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、syslog 送信元の名前を入力します。
b) [Min Severity] ドロップダウン リストから、送信するシステム ログ メッセージの重大度の最小値を選択します。
c) [Include] フィールドで、送信するメッセージ タイプのチェックボックスをオンにします。
d) [Dest Group] ドロップダウン リストから、システム ログ メッセージの送信先の syslog 宛先グループを選択します。
e) [Submit] をクリックします。

ステップ 9 （任意） syslog 送信元を追加するには、もう一度 [+] をクリックし、[Create Syslog Source] ダイアログボックスの手順を繰り返します。

アウトオブバンド DNS 接続

（注） テクニカル サポートや Cisco Call Home ホームなどのアプリケーションでは、ホスト名を正しく解決するためにリーフ スイッチでインバンドとアウトオブバンドの DNS 接続が必要です。

アトミック カウンタの使用

アトミック カウンタについて

アトミック カウンタは、フロー間のトラフィックに関する統計情報を収集できます。アトミック カウンタを使用すると、ファブリック内のドロップとルーティングミスを検出し、アプリケーション接続に関する問題の迅速なデバッグと分離が可能になります。たとえば、管理者はすべてのリーフ スイッチでアトミック カウンタを有効にして、エンドポイント 1 からエンドポイント 2 のパケットをトレースすることができます。送信元と宛先のリーフ スイッチ以外のリーフ スイッチにゼロ以外のカウンタがある場合、管理者はそれらのリーフにドリル ダウンできます。

従来の設定では、ベア メタル NIC から特定の IP アドレス（エンドポイント）または任意の IP アドレスへのトラフィックの量をモニタすることはほぼ不可能です。アトミック カウンタでは、データ パスに干渉することなく、管理者がベア メタル エンドポイントから受信されたパケットの数を数えることができます。さらに、アトミック カウンタはエンドポイントまたはアプリケーション グループで送受信されるプロトコルごとのトラフィックをモニタリングできます。

リーフ間（TEP 間）のアトミック カウンタは次を提供できます。

- 送信パケット、受信パケット、ドロップ パケット、および超過パケットのカウント
  - 送信パケット：送信数は、送信元 TEP（トンネル エンドポイント）から宛先 TEP に送信されたパケット数を表します。

- 受信パケット：受信数は、宛先TEPが送信元TEPから受信したパケット数を表します。
- ドロップパケット：ドロップ数は、伝送中にドロップされたパケット数を表します。この数値は、送信パケット量と受信パケット量の差です。
- 超過パケット：超過数は、伝送中に受信された超過パケット数を表します。この数値は、転送の不一致または間違った場所へのルーティングミスによって予期せず受信されたパケット量です。

- 最後の 30 秒などの短期間のデータ収集、5 分、15 分、またはそれ以上の長期間のデータ収集
- スパイン トラフィックごとの詳細
- 継続的なモニタリング

（注） リーフ間（TEP間）アトミック カウンタは累積であり、クリアできません。ただし、30 秒のアトミック カウンタは 30 秒間隔でリセットされるため、断続的な問題や、再発する問題の分離に使用できます。アトミック カウンタには、アクティブなファブリック ネットワーク タイム プロトコル（NTP）ポリシーが必要です。

テナントのアトミック カウンタは次を提供できます:

- 送信、受信、ドロップ、および超過パケットを含む、ファブリック全体のトラフィックのアプリケーション固有カウンタ
- モードは次を含みます。
  - EPtoEP（エンドポイント間）
  - EPGtoEPG（エンドポイント グループ間）

    （注） EPGtoEPGの場合、オプションにはipv4のみ、ipv6のみ、ipv4、ipv6が含まれます。ipv6 オプションがある場合は必ず TCAM エントリを 2 回使用します。これは、スケール数が、純粋な ipv4 ポリシーの場合に予期される数より小さい可能性があることを意味します。

  - EPGtoEP（エンドポイント グループ/エンドポイント間）
  - EPtoAny（エンドポイント ツー エニー）
  - AnytoEP（エニー ツー エンドポイント）
  - EPGtoIP（エンドポイント グループ/IP 間、外部 IP アドレスの場合にのみ使用）
  - EPtoExternalIP（エンドポイント/外部 IP アドレス間）

アトミック カウンタに関する注意事項および制約事項

- アトミック カウンタの使用は、エンドポイントが異なるテナントまたは同じテナント内の異なるコンテキスト（VRF）にある場合はサポートされません。
- IP アドレスが学習されない純粋なレイヤ 2 設定（IP アドレスは 0.0.0.0）では、エンドポイント/EPG 間および EPG/エンドポイント間のアトミック カウンタ ポリシーはサポートされません。この場合、エンドポイント間および EPG 間のポリシーはサポートされます。外部ポリシーは学習された IP アドレスが必要な Virtual Routing and Forwarding（VRF）ベースであり、サポートされます。
- アトミック カウンタの送信元または宛先がエンドポイントである場合、そのエンドポイントはスタティックではなくダイナミックである必要があります。ダイナミック エンドポイント（fv:CEp）とは異なり、スタティック エンドポイント（fv:StCEp）にはアトミック カウンタに必要な子オブジェクト（fv:RsCEpToPathEp）がありません。
- 中継トポロジでは、リーフ スイッチはすべてのスパイン スイッチを使用したフル メッシュにはなく、リーフ間（TEP 間）のカウンタは予期どおりに動作しません。
- リーフ間（TEP 間）アトミック カウンタの場合、トンネル数がハードウェア制限を上回ると、システムはモードをトレール モードからパス モードに変更し、ユーザにはスパインごとのトラフィックは表示されなくなります。
- アトミック カウンタはスパイン プロキシ トラフィックはカウントしません。
- ファブリックに入る前、またはリーフ ポートに転送される前にドロップされたパケット、アトミック カウンタによって無視されます。
- ハイパーバイザで切り替えられるパケット（同じポート グループとホスト）はカウントされません。
- アトミック カウンタには、アクティブなファブリック ネットワーク タイム プロトコル（NTP）ポリシーが必要です。
- 送信元または宛先として fvCEp を使用して設定されたアトミック カウンタ ポリシーでは、fvCEp 管理対象オブジェクト（MO）に存在する MAC アドレスおよび IP アドレスからの、または両者へのトラフィックのみがカウントされます。fvCEp MO の IP アドレス フィールドが空である場合、その MAC アドレスへの/からのすべてのトラフィックが IP アドレスに関係なくカウントされます。APIC が fvCEp について複数の IP アドレスを学習している場合、前述のように、fvCEp MO 自体にある 1 つの IP アドレスのみがカウントされます。特定の IP アドレスへの/からのアトミック カウンタ ポリシーを設定するには、送信元または宛先として fvIp MO を使用します。
- fvCEp の背後に fvIp が存在する場合は、fvCEp ベースのポリシーではなく fvIP ベースのポリシーを追加する必要があります。

アトミック カウンタの構成

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、必要なテナントをクリックします。

ステップ 3 [Navigation] ペインでテナントを拡張し、[Troubleshoot Policies] を拡張します。

ステップ 4 [Troubleshoot Policies] の下で [Atomic Counter Policy] を展開し、トラフィック トポロジを選択します。
エンドポイントの組み合わせ、エンドポイント グループ、外部インターフェイスおよび IP アドレス間のトラフィックを測定できます。

ステップ 5 必要なトポロジを右クリックして、[Add*topology*Policy] を選択し、[Add Policy] ダイアログボックスを開きます。

ステップ 6 [Add Policy] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドにポリシーの名前を入力します。

b) トラフィックの送信元の識別情報を選択するか、入力します。
必要な識別情報のソース（エンドポイント、エンドポイントのグループ、外部インターフェイス、または IP アドレス）によって異なります。

c) トラフィックの宛先の識別情報を選択するか、入力します。

d) （任意） （任意）[Filters] テーブルで + アイコンをクリックし、カウントするトラフィックのフィルタリングを指定します。
表示される [Create Atomic Counter Filter] ダイアログボックスで、IP プロトコル番号（たとえば TCP=6）によるフィルタリング、および送信元と宛先の IP ポート番号によるフィルタリングを指定できます。

e) [Submit] をクリックし、アトミック カウンタ ポリシーを保存します。

ステップ 7 [Navigation] ペインで、選択したトポロジの下の新しいアトミック カウンタ ポリシーを選択します。
ポリシー設定が [Work] ペインに表示されます。

ステップ 8 [Work] ペインで [Operational] タブをクリックし、[Traffic] サブタブをクリックして、アトミック カウンタの統計情報を表示します。

SNMP の使用

SNMP の概要

Cisco Application Centric Infrastructure （ACI）は、管理情報ベース（MIB）と通知（トラップ）を含む広範な SNMPv1、v2、および v3 のサポートを提供します。SNMP 標準では、ACI ファブリックを管理しモニタするさまざまな MIB をサポートするサードパーティ製アプリケーションを使用できます。

SNMPv3 はさらに広範なセキュリティ機能を提供します。各 SNMPv3 デバイスで SNMP サービスを有効または無効にするように選択できます。また、各デバイスで SNMP v1 および v2 要求の処理方法を設定できます。

SNMP の使用方法の詳細については、『*Cisco ACI MIB Quick Reference*』を参照してください。

ACI での SNMP アクセスのサポート

ACI での SNMP のサポートは次のとおりです。

- SNMP 読み取りクエリー（Get、Next、Bulk、Walk）は、リーフおよびスパイン スイッチと APIC によってサポートされます。
- SNMP 書き込みコマンド（Set）は、リーフおよびスパイン スイッチまたは APIC によってサポートされません。
- SNMP トラップ（v1、v2c、および v3）は、リーフおよびスパイン スイッチと APIC によってサポートされます。

（注） ACI は最大 10 個のトラップ レシーバをサポートします。

- SNMPv3 は、リーフおよびスパイン スイッチと APIC によってサポートされます。

表 *1*：*Cisco APIC* リリースでの *SNMP* サポートの変更

リリース	説明
1.2(2)	SNMP トラップの宛先として IPv6 サポートを追加。
1.2(1)	APIC コントローラの SNMP サポートを追加。以前のリリースでは、リーフおよびスパイン スイッチについてのみ SNMP がサポートされています。

ACI でサポートされる MIB の完全なリストについては、http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/mib/list/mib-support.html を参照してください。

SNMP の設定

GUI による SNMP ポリシーの設定

この手順では、ACI スイッチの SNMP ポリシーを設定し、有効にします。

はじめる前に

SNMP 通信を有効にするには、以下の設定が必要です。

- アウトオブバンド コントラクトを設定して SNMP トラフィックを許可します。SNMP トラフィックは、通常、SNMP 要求に UDP ポート 161 を使用します。
- 'mgmt' テナントで APIC アウトオブバンド IP アドレスを設定します。アウトオブバンド アドレスは APIC セットアップ時に設定されますが、アウトオブバンド コントラクトを有効にするには 'mgmt' テナントでアドレスを明示的に設定する必要があります。

ステップ 1 メニュー バーで、[Fabric] をクリックします。

ステップ 2 サブメニュー バーで、[Fabric Policies] をクリックします。

ステップ 3 [Navigation] ペインで、[Pod Policies] を展開します。

ステップ 4 [Pod Policies] の下で [Policies] を展開します。

ステップ 5 [SNMP] を右クリックし、[Create SNMP Policy] を選択します。
新しい SNMP ポリシーを作成する代わりに、次の手順で示されるものと同じ方法で [default] ポリシー フィールドを編集できます。

ステップ 6 SNMP ポリシーの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、SNMP ポリシーの名前を入力します。
b) [Admin State] フィールドで、[Enabled] を選択します。
c) [Community Policies] テーブルで + アイコンをクリックし、名前を入力して、[Update] をクリックします。
d) （任意） [SNMP v3 Users] テーブルで + アイコンをクリックし、名前を入力して、ユーザの認証データを入力し、[Update] をクリックします。
この手順は SNMPv3 アクセスが必要な場合のみ実行します。

ステップ 7 許可された SNMP 管理ステーションを設定するには、SNMP ポリシーのダイアログボックスで、次の操作を実行します。

a) [Client Group Policies] テーブルで + アイコンをクリックし、[Create SNMP Client Group Profile] ダイアログボックスを開きます。
b) [Name] フィールドに、SNMP クライアント グループのプロファイル名を入力します。
c) [Associated Management EPG] ドロップダウン リストから管理 EPG を選択します。
d) [Client Entries] テーブルで + アイコンをクリックします。
e) [Name] フィールドにクライアントの名前を入力し、[Address] のフィールドにクライアントの IP アドレスを入力して、[Update] をクリックします。

ステップ 8 [OK] をクリックします。

ステップ 9 [Submit] をクリックします。

ステップ 10 [Pod Policies] の下で [Policy Groups] を展開して、ポリシー グループを選択するか、または [Policy Groups] を右クリックし、[Create POD Policy Group] を選択します。
新しいポッド ポリシー グループを作成することも、既存のグループを使用することもできます。ポッド ポリシー グループには、SNMP ポリシーに加えて他のポッド ポリシーを含めることができます。

ステップ 11 ポッド ポリシー グループの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、ポッド ポリシー グループの名前を入力します。
b) [SNMP Policy] ドロップダウン リストから、設定した SNMP ポリシーを選択して、[Submit] をクリックします。

ステップ 12 [Pod Policies] の下で [Profiles] を展開し、[default] をクリックします。

ステップ 13 [Work] ペインで、[Fabric Policy Group] ドロップダウン リストから、作成したポッド ポリシー グループを選択します。

ステップ 14 [Submit] をクリックします。

ステップ 15 [OK] をクリックします。

GUI による SNMP トラップ通知先の設定

この手順では、SNMP トラップ通知を受信する SNMP マネージャのホスト情報を設定します。

（注） ACI は最大 10 個のトラップ レシーバをサポートします。10 個より多く設定すると、一部では通知が受信されません。

ステップ 1 メニュー バーで、[Admin] をクリックします。

ステップ 2 サブメニュー バーで、[External Data Collectors] をクリックします。

ステップ 3 [Navigation] ペインで、[Monitoring Destinations] を展開します。

ステップ 4 [SNMP] を右クリックし、[Create SNMP Trap Destination Group] [Create SNMP Monitoring Destination Group] を選択します。

ステップ 5 [Create SNMP Trap Destination Group] [Create SNMP Monitoring Destination Group]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、SNMP 通知先の名前を入力し、[Next] をクリックします。
b) [Create Destinations] テーブルで+アイコンをクリックし、[Create SNMP Trap Destination] ダイアログボックスを開きます。
c) [Host Name/IP] フィールドに、送信先ホストの IP アドレスまたは完全修飾ドメイン名を入力します。
（注） Cisco APIC Release 1.2(2) 以降のリリースは、IPv6 SNMP トラップ宛先をサポートします。
d) 通知先のポート番号と SNMP バージョンを選択します。
e) SNMP v1 または v2c 通知先の場合、[Security Name] として設定したコミュニティ名の 1 つを入力し、[v3 Security Level] として noauth を選択します。
f) SNMP v3 通知先の場合、[Security Name] として設定したユーザ名の 1 つを入力し、必要な [v3 Security Level] を選択します。
g) [Management EPG] ドロップダウン リストから管理 EPG を選択します。
h) [OK] をクリックします。

i) [Finish] をクリックします。

GUI による SNMP トラップ ソースの設定

この手順では、ファブリック内のソース オブジェクトを選択して有効にし、SNMP トラップ通知を生成します。

ステップ 1 メニュー バーで、[Fabric] をクリックします。

ステップ 2 サブメニュー バーで、[Fabric Policies] をクリックします。

ステップ 3 [Navigation] ペインで、[Monitoring Policies] を展開します。
共通ポリシー、デフォルト ポリシーで SNMP ソースを作成することも、または新しいモニタリング ポリシーを作成することもできます。

ステップ 4 必要なモニタリング ポリシーを展開し、[Callhome/SNMP/Syslog] を選択します。
[Common Policy] を選択する場合は、[Common Policy] を右クリックして、[Create SNMP Source] を選択し、そのダイアログボックスで次の手順に従ってください。

ステップ 5 [Work] ペインで、[Monitoring Object] ドロップダウン リストから [ALL] を選択します。

ステップ 6 [Source Type] ドロップダウン リストから、[SNMP] を選択します。

ステップ 7 テーブルで + アイコンをクリックし、[Create SNMP Source] ダイアログボックスを開きます。

ステップ 8 [Create SNMP Source] 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、SNMP ポリシーの名前を入力します。
b) [Include] フィールドで、必要な通知タイプ（イベント、監査ログ、エラー）のチェックボックスをオンにします。
c) [Min Severity] ドロップダウン リストから、通知をトリガーする [Info] 重大度レベルを選択します。
d) [Dest Group] ドロップダウン リストから、通知を送信する既存の通知先を選択するか、または [Create SNMP Trap Destination Group] [Create SNMP Monitoring Destination Group]を選択して新しい通知先を作成します。
SNMP の通知先グループを作成する手順は、別項で説明します。
e) [Submit] をクリックします。

SNMP を使用したシステムのモニタリング

個々のホスト（APIC またはその他のホスト）をリモートでモニタし、特定のノードの状態を確認できます。

SNMP を使用してシステムの CPU とメモリの使用状況をチェックし、CPU のスパイクが発生しているかどうかを確認できます。SNMP（ネットワーク管理システム）は、SNMP クライアントを使用して APIC の情報にアクセスし、情報を取得します。

リモートでシステムにアクセスして、情報がネットワーク管理システムのコンテキストに属するものかどうかを確認し、CPU またはメモリの使用量が多すぎないか、またはシステムやパフォーマンスの問題が発生しているかどうかを調べることができます。問題の原因がわかると、システムの正常性をチェックし、メモリまたは CPU の使用量多すぎないかどうかを確認できます。

詳細については、『*Cisco ACI MIB Quick Reference Manual*』を参照してください。

SPAN の使用

SPAN の概要

スイッチド ポート アナライザ（SPAN）ユーティリティを使って、詳細なトラブルシューティングの実行または特定のアプリケーション ホストからトラフィックのサンプルを取得し、プロアクティブなモニタリングと分析を行うことができます。

SPAN は 1 つ以上のポート、VLAN、またはエンドポイント グループ（EPG）からのトラフィックをコピーし、ネットワーク アナライザによる分析のためにコピーしたトラフィックを 1 つ以上の送信先に送信します。このプロセスはどの接続デバイスも中断せず、ハードウェア内で実施されるので不要な CPU 負荷を防ぎます。

SPANセッションはソースが受信したトラフィック（入力トラフィック）、ソースから送信したトラフィック（出力トラフィック）、またはその両方をモニタリングするように設定できます。デフォルトでは、SPAN はすべてのトラフィックをモニタリングしますが、選択したトラフィックだけをモニタリングするようにフィルタを設定できます。

マルチノード SPAN

APIC トラフィックのモニタリング ポリシーは、各アプリケーション グループのメンバーとそれが接続する場所を追跡するために、適切な場所でポリシーを SPAN することが可能です。いずれかのメンバーが移動した場合、APIC は新しいリーフ スイッチに自動的にポリシーをプッシュします。たとえば、エンドポイントが新しいリーフ スイッチに VMotion すると、SPAN 設定が自動的に調整されます。

SPAN の注意事項と制約事項

- SPAN はトラブルシューティングのために使用します。SPAN トラフィックはスイッチ リソースのユーザ トラフィックと競合します。負荷を最小限にするには、分析対象の特定のトラフィックだけをコピーするように SPAN を設定します。
- SPAN 送信元として l3extLIfP のレイヤ 3 サブインターフェイスを指定することはできません。外部ソースからのトラフィックをモニタリングするためにはポート全体を使用します。

- テナントおよびアクセス SPAN は カプセル化リモート拡張 SPAN（ERSPAN）タイプ I を使用し、ファブリック SPAN は ERSPAN タイプ II を使用します。ERSPAN ヘッダーについては、IETF の Internet Draft（https://tools.ietf.org/html/draft-foschiano-erspan-00）を参照してください。
- アクティブな SPAN セッションの最大数など、SPAN 関連の制限については、『『*Verified Scalability Guide for Cisco ACI*』』という資料 を参照してください。

SPAN セッションの設定

この手順では、リモート トラフィック アナライザにレプリケートされたソース パケットを転送するようにポリシーを設定する方法を示します。

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、送信元エンドポイントを含むテナントをクリックします。

ステップ 3 [Navigation] ペインでテナントを拡張し、[Troubleshooting Policies] を拡張して、[SPAN] を拡張します。

ステップ 4 [SPAN] の下で [SPAN Destination Groups] を右クリックし、[Create SPAN Destination Group] を選択します。

ステップ 5 [Create SPAN Destination Group] 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、SPAN 宛先グループの名前を入力します。
b) [Create Destinations] テーブルで + アイコンをクリックし、[Create SPAN Destination] ダイアログボックスを開きます。
c) [Name] フィールドに、SPAN 宛先の名前を入力します。
d) [Destination EPG] ドロップダウン リストで、宛先テナント、アプリケーション プロファイル、または複製されたパケットの転送先の EPG を選択または入力します。
e) [Destination IP] フィールドで、複製されたパケットを受信するリモート サーバの IP アドレスを入力します。
f) [Source IP Prefix] フィールドに、ソース パケットの IP サブネットの基本 IP アドレスを入力します。
g) （任意） [Flow ID] フィールドで、SPAN パケットのフロー ID 値を増分または減分します。
h) （任意） [TTL] フィールドで、SPAN トラフィックでのパケットの IP 存続可能時間（TTL）値を増分または減分します。
i) （任意） [MTU] フィールドで、パケットの MTU トランケーション サイズを増分または減分します。
j) （任意） [DSCP] フィールドで、SPAN トラフィックでのパケットの IP DSCP 値を増分または減分します。
k) [OK] をクリックして、SPAN 送信先を保存します。
l) [Submit] をクリックして、SPAN 送信先グループを保存します。

ステップ 6 [SPAN] の下で [SPAN Source Groups] を右クリックし、[Create SPAN Source Group] を選択します。

ステップ 7 [Create SPAN Source Group] 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、SPAN 送信元グループの名前を入力します。
b) [Destination Group] ドロップダウン リストから、以前設定した SPAN 送信先グループを選択します。

c) [Create Sources] テーブルで + アイコンをクリックし、[Create ERSPAN Source] ダイアログボックスを開きます。
d) [Name] フィールドに、送信元の名前を入力します。
e) [Direction] フィールドで、送信元に着信するパケット、送信元から発信するパケット、または着信と発信の両方のパケットを複製および転送するかどうかに基づいて、オプション ボタンを選択します。
f) [Source EPG] ドロップダウン リストから、そのパケットが SPAN 送信先に複製および転送される EPG（テナント / アプリケーション プロファイル / EPG によって特定）を選択します。
g) [OK] をクリックして、SPAN 送信元を保存します。
h) [Submit] をクリックして、SPAN 送信元グループを保存します。

次の作業

SPAN 送信先のトラフィック アナライザを使用して、SPAN 送信元 EPGからのデータ パケットを観察し、パケット形式、アドレス、プロトコルおよびその他の情報を確認できます。

トレースルートの使用

トレースルートの概要

トレースルート ツールは、パケットが送信先に移動するときに実際に通るルートを検出するために使用されます。トレースルートでは、ホップごとに使用されるパスが識別され、双方向で各ホップにタイムスタンプが付けられます。トレースルートを使用すると、発信元のデバイスと送信先に最も近いデバイスの間のパスに沿ってポート接続をテストできます。送信先に到達できない場合は、パス検出によってパスが障害ポイントまで追跡されます。

テナントのエンドポイントから開始された traceroute は、入力リーフのスイッチに表示される中間ホップとしてデフォルト ゲートウェイを示します。

traceroute は、エンドポイント間やリーフ間（トンネル エンドポイント、または TEP 間）など、さまざまなモードをサポートしています。トレースルートはファブリック全体のすべてのパスを検出し、外部エンドポイントの出口を検出します。パスが妨げられているかどうかを発見するのに役立ちます。

traceroute の注意事項および制約事項

- traceroute の送信元または宛先が エンドポイントである場合、そのエンドポイントはスタティックではなくダイナミックである必要があります。ダイナミック エンドポイント（fv:CEp）とは異なり、スタティック エンドポイント（fv:StCEp）には traceroute に必要な子オブジェクト（fv:RsCEpToPathEp）がありません。

- traceroute 関連の制限については、『*Verified Scalability Guide for Cisco ACI*』というマニュアルを参照してください。

エンドポイント 間での traceroute の実行

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、送信元エンドポイントを含むテナントをクリックします。

ステップ 3 [Navigation] ペインでテナントを拡張し、[Troubleshoot Policies] を拡張します。

ステップ 4 [Troubleshoot Policies] の下で、[Endpoint-to-Endpoint Traceroute Policies] を右クリックし、[Create Endpoint-to-Endpoint Traceroute Policy] を選択します。

ステップ 5 [Create Endpoint-to-Endpoint Traceroute Policy] 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 traceroute ポリシーの名前を入力します。

b) [Source End Points] テーブルで + アイコンをクリックし、トレースルートの発信元を編集します。

c) [Source MAC] ドロップダウン リストから送信元エンドポイントの MAC アドレスを選択または入力し、[Update] をクリックします。

d) [Destination End Points] テーブルで + アイコンをクリックし、トレースルートの発信先を編集します。

e) [Destination MAC] ドロップダウン リストから、宛先エンドポイントの MAC アドレスを選択または入力し、[Update] をクリックします。

f) [State] フィールドで、[Start] オプション ボタンをクリックします。

g) [Submit] をクリックして、トレースルートを起動します。

ステップ 6 [Navigation] ペインまたは [Traceroute Policies] テーブルで、トレースルート ポリシーをクリックします。トレースルート ポリシーが [Work] ペインに表示されます。

ステップ 7 [Work] ペインで [Operational] タブをクリックし、[Source End Points] タブをクリックして、[Results] タブをクリックします。

ステップ 8 [Traceroute Results] テーブルで、追跡に使用された単数または複数のパスを確認します。

（注） 複数のパスが、送信元ノードから宛先ノードへの移動に使用されている場合があります。

（注） 見やすくするには、[Name] 列などの複数の列の幅を広げます。

第 3 章

コアACIファブリックサービスのプロビジョニング

この章の内容は、次のとおりです。

時刻同期と NTP

シスコ アプリケーション セントリック インフラストラクチャ（ACI）ファブリックにおいて、時刻の同期は、モニタリング、運用、トラブルシューティングなどの多数のタスクが依存している重要な機能です。クロック同期は、トラフィック フローの適切な分析にとって重要であり、複数のファブリック ノード間でデバッグとフォールトのタイム スタンプを関連付けるためにも重要です。

1 つ以上のデバイスでオフセットが生じると、多くの一般的な運用問題を適切に診断して解決する機能がブロックされる可能性があります。また、クロック同期によって、アプリケーションのヘルススコアが依存している ACI の内蔵アトミック カウンタ機能をフル活用できます。時刻同期が存在しない場合や不適切に設定されている場合でも、エラーやヘルススコアの低下が引き起こされるわけではありません。これらの機能を適切に使用できるように、ファブリックやアプリケーションを完全に展開する前に、時刻同期を設定する必要があります。デバイスのクロックを同期させる最も一般的な方法は、ネットワーク タイム プロトコル（NTP）を使用することです。

NTP を 設定する前に、どの管理 IP アドレス スキームを ACI ファブリックに配置するかを検討してください。すべての ACI ノードと Application Policy Infrastructure Controller（APIC）の管理を設定するために、インバンド管理とアウトオブバンド管理の 2 つのオプションがあります。ファブリックに対して選択した管理オプションに応じて、NTP の設定が異なります。時刻同期の展開に

関するもう 1 つの考慮事項は、時刻源の場所です。プライベート内部時刻または外部パブリック時刻の使用を決定する際は、時刻源の信頼性について慎重に検討する必要があります。

インバンドおよびアウトオブバンドの管理 NTP

（注）
- 管理 EPG が NTP サーバ用に設定されていることを確認してください。設定されていない場合、このサーバはスイッチで設定されません。
- インバンド管理アクセスおよびアウトオブバンド管理アクセスについては、本書の「管理アクセスの追加」という項を参照してください。

- アウトオブバンド管理 NTP：ACI ファブリックをアウトオブバンド管理と共に展開する場合、ファブリックの各ノードは、スパイン、リーフ、および APIC クラスタの全メンバーを含めて、ACI ファブリックの外部から管理されます。この IP 到達可能性を活用することで、各ノードは一貫した時刻源として同じ NTP サーバに個々に照会することができます。NTP を設定するには、アウトオブバンド管理のエンドポイント グループを参照する日付時刻ポリシーを作成する必要があります。日付時刻ポリシーは 1 つのポッドに限定され、ACI ファブリック内のプロビジョニングされたすべてのポッドに展開する必要があります。現在は、ACI ファブリックあたり 1 つのポッドのみが許可されます。
- インバンド管理 NTP：ACI ファブリックをインバンド管理と共に展開する場合は、ACI のインバンド管理ネットワーク内から NTP サーバへの到達可能性を検討します。ACI ファブリック内で使用されるインバンド IP アドレッシングには、ファブリックの外部から到達できません。インバンド管理されているファブリックの外部の NTP サーバを使用するには、その通信を可能にするポリシーを作成します。インバンド管理ポリシーの設定に使用される手順は、アウトオブバンド管理ポリシーの確立に使用される手順と同じです。違いは、ファブリックが NTP サーバに接続できるようにする方法です。

拡張 GUI を使用した NTP の設定

ステップ 1 メニュー バーで、[FABRIC] > [Fabric Policies] を選択します。

ステップ 2 [Navigation] ペインで、[Pod Policies] > [Policies] の順に選択します。

ステップ 3 [Work] ペインで、[Actions] > [Create Date and Time Policy] の順に選択します。

ステップ 4 [Create Date and Time Policy] ダイアログボックスで、次の操作を実行します。

a) 環境内のさまざまな NTP 設定を区別するポリシーの名前を入力します。[Next] をクリックします。

b) [+] 記号をクリックし、使用する NTP サーバ情報（プロバイダー）を指定します。

c) [Create Providers] ダイアログボックスで、次のフィールドを含めて、すべての関連情報を入力します。[Name]、[Description]、[Minimum Polling Intervals]、[Maximum Polling Intervals]

- 複数のプロバイダーを作成する場合は、最も信頼できる NTP 時刻源の [Preferred] チェックボックスをオンにします。
- ファブリックのすべてのノードがアウトオブバンド管理によって NTP サーバに到達できる場合は、[Management EPG] ドロップダウン リストで、[Out-of-Band] を選択します。インバンド管理を導入した場合は、インバンド管理 NTP の詳細を参照してください。[OK] をクリックします。

作成するプロバイダーごとに、この手順を繰り返します。

ステップ 5 [Navigation] ペインで、[Pod Policies] > [Policy Groups] の順に選択します。

ステップ 6 [Work] ペインで、[Actions] > [Create Pod Policy Group] の順に選択します。

ステップ 7 [Create Pod Policy Group] ダイアログボックスで、次の操作を実行します。

a) ポリシー グループの名前を入力します。

b) [Date Time Policy] フィールドのドロップダウン リストから、前に作成した NTP ポリシーを選択します。[Submit] をクリックします。
ポッド ポリシー グループが作成されます。または、デフォルトのポッド ポリシー グループを使用することもできます。

ステップ 8 [Navigation] ペインで、[Pod Policies] > [Profiles] の順に選択します。

ステップ 9 [Work] ペインで、目的のポッド セレクタ名をダブルクリックします。

ステップ 10 [Properties] 領域の [Fabric Policy Group] ドロップダウン リストから、作成したポッド ポリシー グループを選択します。[Submit] をクリックします。

REST API を使用した NTP の設定

ステップ 1 NTP を設定します。

例：

```
POST url: https://APIC-IP/api/node/mo/uni/fabric/time-test.xml

<imdata totalCount="1">
    <datetimePol adminSt="enabled" authSt="disabled" descr="" dn="uni/fabric/time-CiscoNTPPol"
name="CiscoNTPPol" ownerKey="" ownerTag="">
        <datetimeNtpProv descr="" keyId="0" maxPoll="6" minPoll="4" name="10.10.10.11"
preferred="yes">
            <datetimeRsNtpProvToEpg tDn="uni/tn-mgmt/mgmtp-default/inb-default"/>
        </datetimeNtpProv>
    </datetimePol>
</imdata>
```

ステップ 2 デフォルトの日付と時刻のポリシーをポッド ポリシー グループに追加します。

例：

```
POST url: https://APIC-IP/api/node/mo/uni/fabric/funcprof/podpgrp-calo1/rsTimePol.xml
```

```
POST payload: <imdata totalCount="1">
<fabricRsTimePol tnDatetimePolName="CiscoNTPPol">
</fabricRsTimePol>
</imdata>
```

ステップ 3 ポッド ポリシー グループをデフォルトのポッド プロファイルに追加します。

例：

```
POST url: https://APIC-IP/api/node/mo/uni/fabric/podprof-default/pods-default-typ-ALL/rspodPGrp.xml

payload: <imdata totalCount="1">
<fabricRsPodPGrp tDn="uni/fabric/funcprof/podpgrp-calo1" status="created">
</fabricRsPodPGrp>
</imdata>
```

CLI を使用した、各ノードに導入された NTP ポリシーの確認

ステップ 1 ファブリックの APIC に SSH 接続します。

ステップ 2 attach コマンドを入力して Tab キーを 2 回押し、使用可能なノードの名前をすべて表示します。

例：

```
admin@apic1:~> attach <Tab> <Tab>
```

ステップ 3 APIC へのアクセスに使用したのと同じパスワードを使用して、ノードのいずれかにログインします。

例：

```
admin@apic1:~> attach node_name
```

ステップ 4 NTP ピアのステータスを表示します。

例：

```
leaf-1# show ntp peer-status
```

到達可能な NTP サーバの IPアドレスの前にはアスタリスク（*）が付き、遅延がゼロ以外の値になります。

ステップ 5 ステップ 3 および 4 を繰り返し、ファブリック内の各ノードを確認します。

GUI を使用した NTP の動作の確認

ステップ 1 メニュー バーで、[FABRIC] > [Fabric Policies] を選択します。

ステップ 2 [Navigation] ペインで、[Pod Policies] > [Policies] > [Date and Time] > *[ntp_policy]* > *[server_name]* の順に選択します。
ntp_policy は前に作成したポリシーです。[Host Name] フィールドまたは [IP address] フィールドでは IPv6 アドレスがサポートされます。入力したホスト名に IPv6 アドレスが設定されている場合、IPv6 アドレスが IPv4 アドレスより優先されるように実装する必要があります。

ステップ 3 [Work] ペインで、サーバの詳細を確認します。

DHCP リレー ポリシーの設定

DHCP リレー ポリシーは、DHCP クライアントとサーバが異なるサブネット上にある場合に使用できます。クライアントが配置された vShield ドメイン プロファイルとともに ESX ハイパーバイザ上にある場合は、DHCP リレー ポリシー設定を使用することが必須です。

vShield コントローラが Virtual Extensible Local Area Network（VXLAN）を展開すると、ハイパーバイザホストはカーネル（vmkN、仮想トンネルエンドポイント（VTEP））インターフェイスを作成します。これらのインターフェイスは、DHCP を使用するインフラストラクチャ テナントで IP アドレスを必要とします。したがって、APIC が DHCP サーバとして動作しこれらの IP アドレスを提供できるように、DHCP リレー ポリシーを設定する必要があります。

ACI fabricは、DHCP リレーとして動作するときに、DHCP オプション 82（DHCP Relay Agent Information Option）を、クライアントの代わりに中継する DHCP 要求に挿入します。応答（DHCP オファー）がオプション 82 なしで DHCP サーバから返された場合、その応答はファブリックによってサイレントにドロップされます。したがって、ACI fabricが DHCP リレーとして動作するときは、ACI fabricに接続されたノードを計算するために IP アドレスを提供している DHCP サーバはオプション 82 をサポートする必要があります。

拡張 GUI を使用した APIC インフラストラクチャの DHCP サーバ ポリシーの設定

- このタスク例のビデオを視聴するには、ビデオを掲載している Web ページ を参照してください。
- アプリケーション EPG で使用されるポートおよびカプセル化は、物理または VM マネージャ（VMM）ドメインに属している必要があります。ドメインとのそのような関連付けが確立されていないと、APIC は EPG の展開を続行しますが、エラーを生成します。

- Cisco APIC は、IPv4 と IPv6 の両方のテナント サブネットで DHCP リレーをサポートします。DHCP サーバ アドレスには IPv4 または IPv6 を使用できます。DHCPv6 リレーは、ファブリック インターフェイスで IPv6 が有効になっており、1 つ以上の DHCPv6 リレー サーバが設定されている場合にのみ、発生します。

はじめる前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

ステップ 1 メニュー バーで、[TENANTS] > [infra] を選択します。[Navigation] ペインの [Tenant infra] 下で、[Networking] > [Protocol Policies] > [DHCP] > [Relay Policies] を展開します。

ステップ 2 [Relay Policies] を右クリックし、[Create DHCP Relay Policy] をクリックします。

ステップ 3 [Create DHCP Relay Policy] 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、DHCP リレー プロファイル名（DhcpRelayP）を入力します。
b) [Providers] を展開します。[Create DHCP Provider] ダイアログボックスの [EPG Type] フィールドで、DHCP サーバがどこで接続されているかによって適切なオプション ボタンをクリックします。
c) [Application EPG] 領域の [Tenant] フィールドで、ドロップダウン リストから、テナントを選択します。（infra）
d) [Application Profile] フィールドで、ドロップダウン リストから、アプリケーションを選択します。（access）
e) [EPG] フィールドで、ドロップダウン リストから、EPG を選択します。（デフォルト）
f) [DHCP Server Address] フィールドに、インフラ DHCP サーバの IP アドレスを入力します。[Update] をクリックします。

（注） インフラ DHCP IP アドレスは、インフラ IP アドレス APIC1 です。vShield コントローラ設定のために展開する場合は、デフォルトの IP アドレス 10.0.0.1 を入力する必要があります。

g) [Submit] をクリックします。

DHCP リレー ポリシーが作成されます。

ステップ 4 [Navigation] ペインで、[Networking] > [Bridge Domains] > [default] > [DHCP Relay Labels] を展開します。

ステップ 5 [DHCP Relay Labels] を右クリックし、[Create DHCP Relay Label] をクリックします。

ステップ 6 [Create DHCP Relay Label] ダイアログボックスで、次の操作を実行します。

a) [Scope] フィールドで、テナントのオプション ボタンをクリックします。
このアクションにより、[Name] フィールドのドロップダウン リストに、以前に作成した DHCP リレー ポリシーが表示されます。
b) [Name] フィールドで、ドロップダウン リストから、作成した DHCP ポリシーの名前を選択します（DhcpRelayP）。
c) [Submit] をクリックします。

DHCP サーバがブリッジ ドメインに関連付けられます。

ステップ 7 [Navigation] ペインで、[Networking] > [Bridge Domains] > [default] > [DHCP Relay Labels] を展開し、作成された DHCP サーバを表示します。

CLI を使用した APIC インフラストラクチャの DHCP サーバ ポリシーの設定

- アプリケーションEPGで使用されるポートおよびカプセル化は、物理またはVMマネージャ（VMM）ドメインに属している必要があります。ドメインとのそのような関連付けが確立されていないと、APIC は EPG の展開を続行しますが、エラーを生成します。
- Cisco APIC は、IPv4 と IPv6 の両方のテナント サブネットで DHCP リレーをサポートします。DHCP サーバ アドレスには IPv4 または IPv6 を使用できます。DHCPv6 リレーは、ファブリック インターフェイスで IPv6 が有効になっており、1 つ以上の DHCPv6 リレー サーバが設定されている場合にのみ、発生します。

はじめる前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

手順の概要

1. APIC インフラストラクチャ トラフィックの DHCP サーバ ポリシー設定を設定します。

手順の詳細

APIC インフラストラクチャ トラフィックの DHCP サーバ ポリシー設定を設定します。

例：

```
admin@apic1:~> cd /aci/tenants/infra/networking/protocol-policies/dhcp/relay-policies/
admin@apic1:relay-policies> mocreate DhcpRelayP
admin@apic1:relay-policies> cd DhcpRelayP/
admin@apic1:DhcpRelayP> moset owner tenant
admin@apic1:DhcpRelayP> cd providers/
admin@apic1:providers> mocreate tenants/infra/application-profiles/access/application-epgs/default
admin@apic1:providers> cd \[tenants--infra--application-profiles--access--application-epgs--default\]/
admin@apic1:[tenants--infra--application-profiles--access--application-epgs--default]> moset dhcp-server-address 10.0.0.1
admin@apic1:[tenants--infra--application-profiles--access--application-epgs--default]> cd
/aci/tenants/infra/networking/bridge-domains/default/
admin@apic1:default> cd dhcp-relay-labels/
admin@apic1:dhcp-relay-labels> mocreate DhcpRelayP
admin@apic1:dhcp-relay-labels> cd DhcpRelayP/
admin@apic1:DhcpRelayP> moset scope tenant
admin@apic1:DhcpRelayP> moconfig commit
```

REST API を使用した APIC インフラストラクチャの DHCP サーバ ポリシーの設定

- このタスクは、vShield ドメイン プロファイルを作成するユーザの前提条件です。

- アプリケーションEPGで使用されるポートおよびカプセル化は、物理またはVMマネージャ（VMM）ドメインに属している必要があります。ドメインとのそのような関連付けが確立されていないと、APIC は EPG の展開を続行しますが、エラーを生成します。
- Cisco APIC は、IPv4 と IPv6 の両方のテナント サブネットで DHCP リレーをサポートします。DHCP サーバ アドレスには IPv4 または IPv6 を使用できます。DHCPv6 リレーは、ファブリック インターフェイスで IPv6 が有効になっており、1 つ以上の DHCPv6 リレー サーバが設定されている場合にのみ、発生します。

はじめる前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

手順の概要

1. インフラストラクチャ テナントの DHCP サーバ ポリシーとして APIC を設定します。

手順の詳細

インフラストラクチャ テナントの DHCP サーバ ポリシーとして APIC を設定します。

（注） このリレー ポリシーは、接続エンティティ プロファイルの設定を使用した接続されたハイパーバイザであるすべてのリーフ ポートにプッシュされます。接続エンティティ プロファイルによる設定の詳細については、VMM ドメイン プロファイルの作成に関連する例を参照してください。

例：

```
<!-- api/policymgr/mo/.xml -->
<polUni>

POST URL:
https://APIC-IP/api/mo/uni.xml


  <fvTenant name="infra">

    <dhcpRelayP name="DhcpRelayP"  owner="tenant">
      <dhcpRsProv tDn="uni/tn-infra/ap-access/epg-default" addr="10.0.0.1" />
    </dhcpRelayP>

    <fvBD name="default">
      <dhcpLbl name="DhcpRelayP" owner="tenant"/>
    </fvBD>

  </fvTenant>
</polUni>
```

DNS サービス ポリシーの設定

DNS ポリシーは、ホスト名で外部サーバ（AAA、RADIUS、vCenter、サービスなど）に接続するために必要です。DNS サービス ポリシーは共有ポリシーであるため、このサービスを使用するす

べてのテナントと VRF を特定の DNS プロファイル ラベルで設定する必要があります。ACI ファブリックの DNS ポリシーを設定するには、次のタスクを完了する必要があります。

- 管理 EPG が DNS ポリシー用に設定されていることを確認してください。設定されていない場合、このポリシーはスイッチで有効になりません。
- DNS プロバイダーと DNS ドメインに関する情報が含まれる DNS プロファイル（デフォルト）を作成します。
- DNS プロファイル（デフォルトまたは別の DNS プロファイル）の名前を必要なテナントで DNS ラベルに関連付けます。

テナントごと、VRF ごとの DNS プロファイル設定を設定することができます。適切な DNS ラベルを使用して、追加の DNS プロファイルを作成して、特定のテナントの特定の VRF に適用できます。たとえば、名前が acme の DNS プロファイルを作成する場合、テナント設定で acme の DNS ラベルを適切な [Networking] > [VRF] ポリシー設定に追加できます。

インバンド DNS サービス ポリシーによる外部宛先の設定

次のように、サービスに対して外部宛先を設定します。

送信元	インバンド管理	アウトオブバンド管理	外部サーバの場所
APIC	IP アドレスまたは完全修飾ドメイン名（FQDN）	IP アドレスまたは FQDN	どこでも
リーフ スイッチ	IP アドレス	IP アドレスまたは FQDN （注） DNS ポリシーは、DNS サーバの到達可能性に対するアウトオブバンド管理 EPG を指定する必要があります。	どこでも

送信元	インバンド管理	アウトオブバンド管理	外部サーバの場所
スパイン スイッチ	IP アドレス	IP アドレスまたは FQDN （注） DNS ポリシーは、DNS サーバの到達可能性に対するアウトオブバンド管理 EPG を指定する必要があります。	リーフ スイッチに直接接続されます

次に示すのは、外部サーバのリストです。

- Call Home SMTP サーバ
- Syslog サーバ
- SNMP トラップの宛先
- 統計情報のエクスポートの宛先
- エクスポートの設定の宛先
- Techsupport のエクスポートの宛先
- コア エクスポートの宛先

推奨されるガイドラインは次のとおりです。

- 外部サーバは、リーフ アクセス ポートに接続する必要があります。
- 管理ポートの追加の配線を避けるために、リーフ スイッチにはインバンド接続を使用します。
- スパイン スイッチにはアウトオブバンド管理接続を使用します。スパイン スイッチとリーフ スイッチが外部サーバの同じセットに到達できるように、スパイン スイッチのこのアウトオブバンド ネットワークをインバンド管理の仮想ルーティングおよび転送（VRF）機能があるリーフ ポートの 1 つに接続します。
- 外部サーバには IP アドレスを使用します。

拡張 GUI を使用した DNS プロバイダーと接続するための DNS サービス ポリシーの設定

（注） このタスク例のビデオを視聴するには、ビデオを掲載している Web ページ を参照してください。

はじめる前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

手順の概要

1. メニュー バーで、[FABRIC] > [Fabric Policies] を選択します。[Navigation] ペインで、[Global Policies] > [DNS Profiles] を展開し、デフォルトの DNS プロファイルをクリックします。
2. [Work] ペインの [Management EPG] フィールドで、ドロップダウン リストから、適切な管理 EPG （デフォルト（Out-of-Band））を選択します。
3. [DNS Providers] を展開し、次の操作を実行します。
4. [DNS Domains] を展開し、次の操作を実行します。
5. [Submit] をクリックします。
6. メニュー バーで、[TENANTS] > [mgmt] をクリックします。
7. [Navigation] ペインで、[Networking] > [VRF] > [oob] の順に展開し、[oob] をクリックします。
8. [Work] ペインの [Properties] 下で、[DNS labels] フィールドに、適切な DNS ラベル（デフォルト）を入力します。[Submit] をクリックします。

手順の詳細

ステップ 1 メニュー バーで、[FABRIC] > [Fabric Policies] を選択します。[Navigation] ペインで、[Global Policies] > [DNS Profiles] を展開し、デフォルトの DNS プロファイルをクリックします。

ステップ 2 [Work] ペインの [Management EPG] フィールドで、ドロップダウン リストから、適切な管理 EPG （デフォルト（Out-of-Band））を選択します。

ステップ 3 [DNS Providers] を展開し、次の操作を実行します。

a) [Address] フィールドに、プロバイダー アドレスを入力します。

b) [Preferred] カラムで、優先するプロバイダーとしてこのアドレスが必要な場合は、チェックボックスをオンにします。
優先するプロバイダーは 1 つだけ持てます。

c) [Update] をクリックします。

d) （任意） セカンダリ DNS プロバイダーを追加するには、[DNS Providers] を展開し、[Address] フィールドで、プロバイダー アドレスを入力します。[Update] をクリックします。

ステップ 4 [DNS Domains] を展開し、次の操作を実行します。

a) [Name] フィールドに、ドメイン名（cisco.com）を入力します。
b) [Default] カラムで、チェックボックスをオンにしてこのドメインをデフォルト ドメインにします。デフォルトとして持てるドメイン名は 1 つだけです。
c) [Update] をクリックします。
d) （任意） セカンダリ DNS ドメインを追加するには、[DNS Domains] を展開します。[Address] フィールドに、セカンダリ ドメイン名を入力します。[Update] をクリックします。

ステップ 5 [Submit] をクリックします。
DNS サーバが設定されます。

ステップ 6 メニュー バーで、[TENANTS] > [mgmt] をクリックします。

ステップ 7 [Navigation] ペインで、[Networking] > [VRF] > [oob] の順に展開し、[oob] をクリックします。

ステップ 8 [Work] ペインの [Properties] 下で、[DNS labels] フィールドに、適切な DNS ラベル（デフォルト）を入力します。[Submit] をクリックします。
DNS プロファイル ラベルがテナントおよび VRF で設定されました。

CLI を使用した DNS プロバイダーと接続するための DNS サービス ポリシーの設定

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：
```
admin@apic1:~> cd /aci
```

ステップ 2 DNS サーバ ポリシーを設定します。

例：
```
admin@apic1:~> cd /aci/fabric/fabric-policies/global-policies/dns-profiles
admin@apic1:~> mocreate default
admin@apic1:~> cd default/
admin@apic1:default> cd dns-providers/
admin@apic1:dns-providers> mocreate 172.21.157.5 preferred yes
admin@apic1:dns-providers> mocreate 172.21.157.6
admin@apic1:dns-providers> cd ../dns-domains/
admin@apic1:dns-domains> mocreate company.local default yes
admin@apic1:dns-domains> cd ../
admin@apic1:default> moset management-epg uni/tn-mgmt/mgmtp-default/oob-default
admin@apic1:default> moconfig commit
```

ステップ 3 DNS プロファイルを使用する任意の VRF 上で DNS プロファイル ラベルを設定します。

例：

```
admin@apic1:default> cd /aci/tenants/mgmt/networking/vrf/oob/dns-profile-labels/
admin@apic1:dns-profile-labels> ls
admin@apic1:dns-profile-labels> mocreate default
admin@apic1:dns-profile-labels> cd default
admin@apic1:default> moset tag yellow-green
admin@apic1:default> moconfig commit
```

REST API を使用した DNS プロバイダーと接続するための DNS サービス ポリシーの設定

はじめる前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

手順の概要

1. DNS サービス ポリシーを設定します。
2. アウトオブバンド管理テナント下で DNS ラベルを設定します。

手順の詳細

ステップ 1 DNS サービス ポリシーを設定します。

例：

```
POST URL :
https://apic-IP/api/node/mo/uni/fabric.xml

<dnsProfile name="default">

    <dnsProv addr="172.21.157.5" preferred="yes"/>
    <dnsProv addr="172.21.157.6"/>

    <dnsDomain name="cisco.com" isDefault="yes"/>

    <dnsRsProfileToEpg tDn="uni/tn-mgmt/mgmtp-default/oob-default"/>

</dnsProfile>
```

ステップ 2 アウトオブバンド管理テナント下で DNS ラベルを設定します。

例：

```
POST URL: https://apic-IP/api/node/mo/uni/tn-mgmt/ctx-oob.xml
<dnsLbl name="default" tag="yellow-green"/>
```

CLIを使用して、DNSプロファイルが設定されファブリックコントローラ スイッチに適用されているかを確認する

ステップ 1 デフォルトの DNS プロファイルの設定を確認します。

例：

```
admin@apic1:~> cd /aci/fabric/fabric-policies/global-policies/dns-profiles/default
admin@apic1:default> cat summary
# dns-profile
name : default
description : added via CLI by tdeleon@cisco.com
ownerkey :
ownertag :

dns-providers:
address preferred
--------------- ---------
10.44.124.122 no
10.70.168.183 no
10.37.87.157 no
10.102.6.247 yes
dns-domains:
name default description
--------- ------- -----------
cisco.com yes
management-epg : tenants/mgmt/node-management-epgs/default/out-of-band/default
```

ステップ 2 DNS ラベルの設定を確認します。

例：

```
admin@apic1:default> cd /aci/tenants/mgmt/networking/private-networks/oob/dns-profile-labels/default
admin@apic1:default> cat summary
# dns-lbl
name : default
description :
ownerkey :
ownertag :
tag : yellow-green
```

ステップ 3 適用された設定がファブリック コントローラで動作していることを確認します。

例：

```
admin@apic1:~> cat /etc/resolv.conf
# Generated by IFC
search cisco.com
nameserver 10.102.6.247
nameserver 10.44.124.122
nameserver 10.37.87.157
nameserver 10.70.168.183
admin@apic1:~> ping www.cisco.com
PING origin-www.cisco.com (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=238 time=35.4 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=238 time=29.0 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=238 time=29.2 ms
```

ステップ 4 適用された設定がリーフおよびスパイン スイッチで動作していることを確認します。

例：

```
leaf1# cat /etc/resolv.conf
search cisco.com
nameserver 10.102.6.247
nameserver 10.70.168.183
nameserver 10.44.124.122
nameserver 10.37.87.157
leaf1# cat /etc/dcos_resolv.conf
# DNS enabled
leaf1# ping www.cisco.com
PING origin-www.cisco.com (72.163.4.161): 56 data bytes
64 bytes from 72.163.4.161: icmp_seq=0 ttl=238 time=29.255 ms
64 bytes from 72.163.4.161: icmp_seq=1 ttl=238 time=29.212 ms
64 bytes from 72.163.4.161: icmp_seq=2 ttl=238 time=29.343 ms
```

カスタム証明書の設定のガイドライン

- ワイルドカード証明書（*.cisco.com など。複数のデバイス間で使用）およびそれに関連する他の場所で生成される秘密キーは、APIC ではサポートされません。これは、APIC に秘密キーまたはパスワードを入力するためのサポートがないためです。
- 証明書署名要求（CSR）を生成する前に、公開中間証明書とルート CA 証明書をダウンロードしてインストールする必要があります。ルート CA 証明書は技術的には CSR を生成するために必要ではありませんが、シスコでは、対象とする CA 機関と CSR への署名に使用される実物の間の不一致を防ぐために、CSR を生成する前にルート CA 証明書が必要です。APIC は、送信された証明書が設定されている CA によって署名されていることを確認します。
- 更新された証明書の生成に同じ公開キーと秘密キーを使用するには、次のガイドラインを満たす必要があります。
  - 元の CSR にはキー リング内の秘密キーとペアになる公開キーが含まれているため、元の CSR を維持する必要があります。
  - APIC で公開キーと秘密キーを再利用する場合は、元の証明書に使用されたものと同じ CSR を、更新された証明書に関して再送信する必要があります。
  - 更新された証明書に同じ公開キーと秘密キーを使用する場合は、元のキー リングを削除しないでください。キー リングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。

GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定

注意：ダウンタイムの可能性があるため、メンテナンス時間中にのみこのタスクを実行してください。この操作中にファブリック内のすべての Web サーバの再起動が予期されます。

はじめる前に

適切な認証局を作成できるように、信頼できる証明書を取得する機関を決定します。

ステップ 1 メニュー バーで、[ADMIN] > [AAA] を選択します。

ステップ 2 [Navigation] ペインで、次の操作を実行して認証局を設定します。

a) [Public Key Management] を展開します。

b) [Certificate Authorities] を右クリックし、[Create Certificate Authority] をクリックします。

c) [Create Certificate Authority] ダイアログボックスの [Name] フィールドに、認証局の名前を入力します。

d) [Certificate Chain] フィールドに、Cisco APIC の証明書署名要求（CSR）に署名する認証局の中間証明書およびルート証明書をコピーします。
証明書は、Base64 エンコード X.509（CER）形式である必要があります。中間証明書はルート CA 証明書の前に配置されます。次の例のようになります。

```
-----BEGIN CERTIFICATE-----
<Intermediate Certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA Certificate>
-----END CERTIFICATE-----
```

e) [Submit] をクリックします。

ステップ 3 [Navigation] ペインで、[Public Key Management] > [Key Rings] の順に展開し、次の操作を実行することによりキー リングを作成します。

a) [Key Rings] を右クリックし、[Create Key Ring] を選択します。

a) [Create Key Ring] ダイアログボックスで、[Name] フィールドに、名前を入力します。

b) [Certificate] フィールドには、コンテンツを追加しないでください。

c) [Modulus] フィールドで、目的のキー強度のラジオボタンをクリックします。

d) [Certificate Authority] フィールドのドロップダウン リストから、前に作成した認証局を選択します。
[Submit] をクリックします。
[Work] ペインの [Key Rings] 領域では、作成したキー リングに対する [Admin State] に [Started] と表示されます。

（注） キー リングは削除しないでください。キー リングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。

ステップ 4 [Navigation] ペインで、作成したキー リングを右クリックし、次の作業を実行して CSR を生成します。

a) [Create Certificate Request] をクリックします。

b) [Subject] フィールドに、Cisco APIC コントローラの完全修飾ドメイン名（FQDN）を入力します。
（注） /etc/hosts ファイルに、APIC コントローラの IP アドレスと DNS 名のエントリが必要です。DNS 名は証明書のサブジェクトに一致する必要があります。APIC コントローラごとに、このファイル内のエントリが必要です。

c) 必要に応じて、残りのフィールドに入力します。APIC コントローラと適切な証明書ごとにこの手順（CSR）を繰り返します。
（注） 使用可能なパラメータの説明については、[Create Certificate Request] ダイアログボックスでオンライン ヘルプ情報を確認してください。

d) [Submit] をクリックします。

[Navigation] ペインでは、前に作成したキー リングの下にオブジェクトが作成され、表示されます。[Navigation] ペインでそのオブジェクトをクリックすると、[Work] ペインの [Properties] 領域の [Request] フィールドにその CSR が表示されます。認証局に送信するコンテンツをフィールドからコピーします。

ステップ 5 [Navigation] ペインで、作成したキー リングをクリックし、次の作業を実行して署名付き証明書をインストールします。

a) [Work] ペインの [Certificate] フィールドに、認証局から受信した署名付き証明書を貼り付けます。

b) [Submit] をクリックします。

（注） CSR がキー リングで示されている認証局によって署名されていない場合、または証明書に MS-DOS 形式の行末が含まれている場合は、エラー メッセージが表示され、証明書は承認されません。MS-DOS 形式の行末を削除します。

キーが確認され、[Work] ペインの [Admin State] は [Completed] に変わり、http ポリシーを使用する準備ができました。

ステップ 6 メニュー バーで、[FABRIC] > [Fabric Policies] を選択します。[Navigation] ペインで、[Pod Policies] > [Policies] > [Communication] > [default] の順に展開します。

ステップ 7 [Work] ペインの [Admin Key Ring] フィールドで、ドロップダウン メニューを使用して目的のキー リングを選択します。[Submit] をクリックします。

すべての Web サーバが再起動されます。証明書がアクティブになり、デフォルト以外のキー リングが HTTPS アクセスに関連付けられています。

次の作業

証明書の失効日には注意しておき、期限切れになる前に対応する必要があります。更新された証明書に対して同じキーペアを維持するには、CSR を維持する必要があります。これは、CSR にはキー リング内の秘密キーとペアになる公開キーが含まれているためです。証明書が期限切れになる前に、同じ CSR を再送信する必要があります。キー リングを削除すると、APIC に内部的に保存されている秘密キーも削除されるため、新しいキー リングの削除または作成は行わないでください。

第 4 章

ACI ファブリックのアクセス レイヤ 2 接続

この章の内容は、次のとおりです。

ネットワーク ドメイン

ファブリック管理者は、ポート、プロトコル、VLAN プール、およびカプセル化を設定するドメイン ポリシーを作成します。これらのポリシーは、単一テナント専用にすることも、共有することもできます。ファブリック管理者が ACI ファブリック内にドメインを設定すると、テナント管理者はテナント エンドポイント グループ（EPG）をドメインに関連付けることができます。

以下のネットワーク ドメイン プロファイルを設定できます。

- VMM ドメイン プロファイル（`vmmDomP`）は、仮想マシンのハイパーバイザ統合のために必要です。
- 物理ドメイン プロファイル（`physDomP`）は、ベア メタル サーバ接続と管理アクセスに使用します。

- ブリッジド外部ネットワーク ドメイン プロファイル（l2extDomP）は通常、ACI ファブリックのリーフ スイッチにブリッジド外部ネットワーク トランク スイッチを接続するために使用されます。
- ルーテッド外部ネットワーク ドメイン プロファイル（l3extDomP）は、ACI ファブリックのリーフ スイッチにルータを接続するために使用されます。

ドメインは VLAN プールに関連付けられるように設定されます。その後、EPG は、ドメインに関連付けられている VLAN を使用するように設定されます。

（注） EPG ポートと VLAN の設定は、EPG が関連付けられているドメイン インフラストラクチャ設定で指定されている設定に一致する必要があります。一致しない場合、APIC でエラーが発生します。そのようなエラーが発生した場合は、ドメインインフラストラクチャ設定が EPG ポートと VLAN の設定に一致していることを確認してください。

接続可能エンティティ プロファイル

ACI ファブリックにより、リーフ ポートを通してベア メタル サーバ、仮想サーバ、ハイパーバイザ、レイヤ 2 スイッチ（たとえば、Cisco UCS ファブリック インターコネクト）、またはレイヤ 3 ルータ（たとえば、Cisco Nexus 7000 シリーズ スイッチ）などのさまざまな外部エンティティに接続する複数の接続ポイントが提供されます。これらの接続ポイントは、リーフ スイッチ上の物理ポート、FEX ポート、ポート チャネル、またはバーチャル ポート チャネル（vPC）にすることができます。

接続可能エンティティ プロファイル（AEP）は、同様のインフラストラクチャ ポリシー要件を持つ外部エンティティのグループを表します。インフラストラクチャ ポリシーは、Cisco Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）、最大伝送単位（MTU）、Link Aggregation Control Protocol（LACP）などのさまざまなプロトコル オプションを設定する物理インターフェイス ポリシーで構成されます。

AEP は、リーフ スイッチで VLAN プールを展開するのに必要です。カプセル化ブロック（および関連 VLAN）は、リーフ スイッチで再利用可能です。AEP は、VLAN プールの範囲を物理インフラストラクチャに暗黙的に提供します。

次の AEP の要件と依存関係は、さまざまな設定シナリオ（ネットワーク接続や VMM ドメインなど）でも考慮する必要があります。

- AEP は許容される VLAN の範囲を定義しますが、それらのプロビジョニングは行いません。EPG がポートに展開されていない限り、トラフィックは流れません。AEP で VLAN プールを定義しないと、EPG がプロビジョニングされても VLAN はリーフ ポートでイネーブルになりません。
- リーフ ポートで静的にバインディングしている EPG イベントに基づいて、または VMware vCenter や Microsoft Azure Service Center Virtual Machine Manager（SCVMM）などの外部コントローラからの VM イベントに基づいて、特定の VLAN がリーフ ポート上でプロビジョニングされるかイネーブルになります。

Virtual Machine Manager（VMM）ドメインは、AEP のインターフェイス ポリシー グループから物理インターフェイス ポリシーを自動的に取得します。

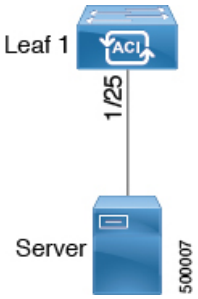
AEP のオーバーライド ポリシーを VMM ドメイン用の別の物理インターフェイス ポリシーを指定するために使用できます。このポリシーは、VM コントローラが中間レイヤ 2 ノードを介してリーフ スイッチに接続され、異なるポリシーがリーフ スイッチおよび VM コントローラの物理ポートで要求される場合に役立ちます。たとえば、リーフ スイッチとレイヤ 2 ノード間で LACP を設定できます。同時に、AEP オーバーライド ポリシーで LACP をディセーブルにすることで、VM コントローラとレイヤ 2 スイッチ間の LACP をディセーブルにできます。

ベア メタル サーバの ACI リーフ スイッチ インターフェイス設定

次の手順では、クイック スタート ウィザードを使用します。

（注） この手順では、ACI リーフ スイッチ インターフェイスにサーバを接続する手順を示します。手順は、ACI リーフ スイッチ インターフェイスに他の種類のデバイスを接続する場合と同じになります。

図 *13*：ベア メタル サーバのスイッチ インターフェイス設定



はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。

- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。

ステップ 1 APIC メニュー バーで、[Fabric] > [Access Policies] > [Quick Start] に移動し、[Configure an interface, PC, and VPC] をクリックします。

ステップ 2 [Select Switches To Configure Interfaces] 作業領域で、大きい [+] をクリックして、設定するスイッチを選択します。[Switches] セクションで、[Switches] をクリックして、使用可能なスイッチ ID のドロップダウン リストからスイッチ ID を追加し、[Update] をクリックします。

ステップ 3 大きい [+] をクリックして、スイッチ インターフェイスを設定します。
インターフェイス ポリシー グループは、選択したスイッチのインターフェイスに適用するインターフェイス ポリシーのグループを指定する名前付きポリシーです。インターフェイス ポリシーの例は、リンク レベル ポリシー（たとえば、1 gbit ポート速度）、ストーム制御インターフェイス ポリシーなどです。

（注） [Attached Dervice Type] ドメインは、スイッチ プロファイルで指定されているインターフェイスを EPG が使用できるようにするために必要です。

a) 使用するインターフェイス タイプとして [individual] を指定します。
b) 使用するインターフェイス ID を指定します。
c) 使用するインターフェイス ポリシーを指定します。
d) 使用する接続デバイス タイプを指定します。ベア メタル サーバに接続する場合、[Bare Metal] を選択します。ベア メタルでは、phys ドメイン タイプを使用します。
e) [Save] をクリックしてポリシーの詳細を更新し、[Submit] をクリックしてスイッチプロファイルを APIC に送信します。
APIC が、インターフェイス、セレクタ、および接続デバイス タイプの各ポリシーとともに、スイッチ プロファイルを作成します。

確認：スイッチインターフェイスが適切に設定されていることを確認するには、サーバが接続されているスイッチに対して CLI コマンド **show int** を使用します。

次の作業

これで、基本リーフ インターフェイスの設定手順は完了しました。

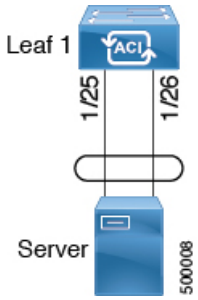
（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

ACI リーフ スイッチ ポート チャネル設定

次の手順では、クイック スタート ウィザードを使用します。

（注） この手順では、ACI リーフ スイッチ インターフェイスにサーバを接続する手順を示します。手順は、ACI リーフ スイッチ インターフェイスに他の種類のデバイスを接続する場合と同じになります。

図 *14*：スイッチ ポート チャネル設定



はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。

ステップ 1 APIC メニュー バーで、[Fabric] > [Access Policies] > [Quick Start] に移動し、[Configure an interface, PC, and VPC] をクリックします。

ステップ 2 [Select Switches To Configure Interfaces] 作業領域で、大きい [+] をクリックして、設定するスイッチを選択します。[Switches] セクションで、[Switches] をクリックして、使用可能なスイッチ ID のドロップダウン リストからスイッチ ID を追加し、[Update] をクリックします。

ステップ 3 大きい [+] をクリックして、スイッチ インターフェイスを設定します。
インターフェイス ポリシー グループは、選択したスイッチのインターフェイスに適用するインターフェイス ポリシーのグループを指定する名前付きポリシーです。インターフェイス ポリシーの例は、リンク レベル ポリシー（たとえば、1 gbit ポート速度）、ストーム制御インターフェイス ポリシーなどです。

（注） [Attached Dervice Type] は、スイッチ プロファイルで指定されているインターフェイスを EPG が使用できるようにするために必要です。

a) 使用するインターフェイス タイプとして [pc] を指定します。
b) 使用するインターフェイス ID を指定します。
c) 使用するインターフェイス ポリシーを指定します。

d) 使用する接続デバイス タイプを指定します。ベア メタル サーバに接続する場合、[Bare Metal] を選択します。ベア メタルでは、phys ドメイン タイプを使用します。

e) [Save] をクリックしてポリシーの詳細を更新し、[Submit] をクリックしてスイッチプロファイルを APIC に送信します。
APIC が、インターフェイス、セレクタ、および接続デバイス タイプの各ポリシーとともに、スイッチ プロファイルを作成します。

確認：スイッチインターフェイスが適切に設定されていることを確認するには、サーバが接続されているスイッチに対して CLI コマンド **show int** を使用します。

次の作業

これで、ポート チャネルの設定手順は完了しました。

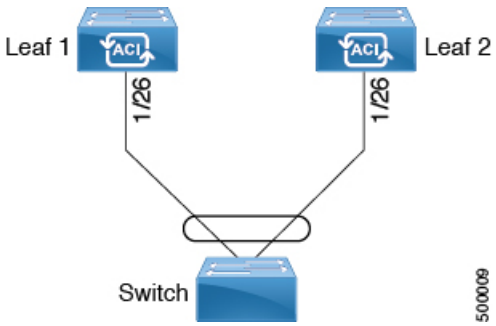
（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

ACI リーフ スイッチ バーチャル ポート チャネル設定

次の手順では、クイック スタート ウィザードを使用します。

（注） この手順では、ACI リーフ スイッチ バーチャル ポート チャネルにトランキング スイッチを接続する手順を示します。手順は、ACI リーフ スイッチ インターフェイスに他の種類のデバイスを接続する場合と同じになります。

図 *15*：スイッチ バーチャル ポート チャネル設定



はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。

ステップ 1 APIC メニュー バーで、[Fabric] > [Access Policies] > [Quick Start] に移動し、[Configure an interface, PC, and VPC] をクリックします。

ステップ 2 [Configure an interface, PC, and VPC] 作業領域で、大きい [+] をクリックして、スイッチを選択します。[Select Switches To Configure Interfaces] 作業領域が表示されます。

ステップ 3 ドロップダウン リストからスイッチ ID を選択し、プロファイルに名前を付け、[Save] をクリックします。保存したポリシーが [Configured Switch Interfaces] リストに表示されます。

ステップ 4 バーチャル ポート チャネルが選択したスイッチに対して使用する [Interface Policy Group] と [Attached Device Type] を設定します。
インターフェイス ポリシー グループは、選択したスイッチのインターフェイスに適用するインターフェイス ポリシーのグループを指定する名前付きポリシーです。インターフェイス ポリシーの例は、リンク レベル ポリシー（たとえば、1 gbit ポート速度）、ストーム制御インターフェイス ポリシーなどです。

（注） [Attached Dervice Type] ドメインは、スイッチ プロファイルで指定されているインターフェイスを EPG が使用できるようにするために必要です。

a) 使用するインターフェイス タイプ（individual、pc、または vpc）として [vpc] を指定します。
b) 使用するインターフェイス ID を指定します。
c) 使用するインターフェイス ポリシーを指定します。
d) 使用する接続デバイス タイプを指定します。スイッチの接続用に [External Bridged Devices] を選択します。
e) [Domain] および [VLAN Range] を指定します。
f) [Save] をクリックしてポリシーの詳細を更新し、[Submit] をクリックしてスイッチ プロファイルを APIC に送信します。
APIC が、インターフェイス、セレクタ、および接続デバイス タイプの各ポリシーとともに、スイッチ プロファイルを作成します。

確認：vpc が適切に設定されていることを確認するには、外部スイッチが接続されているリーフ スイッチに対して CLI コマンド **show int** を使用します。

次の作業

これで、スイッチ バーチャル ポート チャネルの設定手順は完了しました。

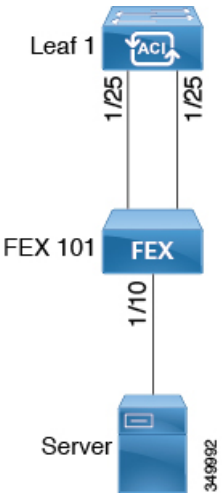
（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

基本的な FEX 設定

次の手順では、FEX導入に必要ないくつかのポリシーを自動的に作成するクイック スタート ウィザードを使用します。主な手順は次のとおりです。

1. 自動生成された FEX プロファイルを含むスイッチ プロファイルを設定します。
2. サーバを単一 FEX ポートに接続できるようにするために、自動生成された FEX プロファイルをカスタマイズします。

図 *16*：基本的な *FEX* 設定



（注） この手順では、FEX にサーバを接続する手順を示します。手順は、ACI が接続された FEX にデバイスを接続する場合と同じになります。

はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。

- ターゲット リーフ スイッチ、インターフェイス、およびプロトコルが設定されており、使用可能であること。
- FEX に電源が入っていて、ターゲット リーフ インターフェイスに接続されていること。

ステップ 1 APIC で、[Fabric] > [Access Policies] > [Quick Start] の [Configure Interface, PC, And VPC] ウィザードを使用して、スイッチ プロファイルを作成します。

a) APIC メニュー バーで、[Fabric] > [Access Policies] > [Quick Start] に移動します。
b) [Quick Start] ページで、[Configure an interface, PC, and VPC] オプションをクリックして [Configure Interface, PC And VPC] ウィンドウを開きます。
c) [Configure an interface, PC, and VPC] 作業領域で、[+] をクリックして、新しいスイッチ プロファイルを追加します。
d) [Select Switches To Configure Interfaces] 作業領域で、[Advanced] オプション ボタンをクリックします。
e) 使用可能なスイッチ ID のドロップダウン リストからスイッチを選択します。

トラブルシューティングのヒント
この手順では、1 つのスイッチがプロファイルに含まれています。複数のスイッチを選択すると、同じプロファイルを複数のスイッチで使用できます。

f) [Switch Profile Name] フィールドで名前を指定します。
g) [Fexes] リストの上にある [+] をクリックして、FEX ID およびスイッチ プロファイルへの接続に使用するスイッチ ポートを追加します。
h) [Save] をクリックして変更を保存します。[Submit] をクリックして、スイッチ プロファイルを APIC に送信します。
APIC が、必要な FEX プロファイル（*<switch policy name>_FexP<FEX ID>*）およびセレクタ（*<switch policy name>_ifselctor*）を自動的に生成します。

確認：FEX がオンラインであることを確認するには、FEX が接続されているスイッチに対して CLI コマンド **show fex** を使用します。

ステップ 2 サーバを単一 FEX ポートに接続できるようにするために、自動生成された FEX プロファイルをカスタマイズします。

a) [Navigation] ペインで、ポリシー リストで作成したスイッチ ポリシーを見つけます。また、自動生成された FEX、*<switch policy name>_FexP<FEX ID>* プロファイルもあります。
b) *<switch policy name>_FexP<FEX ID>* プロファイルの作業ペインで、[+] をクリックして *Interface Selectors For FEX* リストに新しいエントリを追加します。
[Create Access Port Selector] ダイアログが開きます。
c) セレクタの名前を指定します。
d) 使用する FEX インターフェイス ID を指定します。
e) リストから既存のインターフェイス ポリシー グループを選択するか、アクセス ポート ポリシー グループを作成します。
アクセス ポート ポリシー グループは、選択した FEX のインターフェイスに適用するインターフェイス ポリシーのグループを指定する名前付きポリシーです。インターフェイス ポリシーの例は、リンク

レベル ポリシー（たとえば、1 gbit ポート速度）、接続エンティティ プロファイル、ストーム制御インターフェイス ポリシーなどです。

（注） インターフェイス ポリシー グループ内で、FEX ポート セレクタで指定されているインターフェイスを EPG が使用できるようにするために、[Attached Entity Profile] は必須です。

f) [Submit] をクリックして FEX プロファイルを APIC に送信します。
APIC が FEX プロファイルを更新します。

確認：FEXインターフェイスが適切に設定されていることを確認するには、FEXが接続されているスイッチに対して CLI コマンド **show int** を使用します。

次の作業

これで、基本 FEX の設定手順は完了しました。

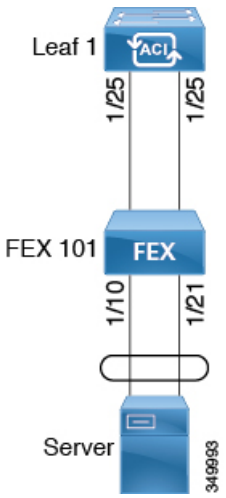
（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

FEX ポート チャネル設定

主な手順は次のとおりです。

1. ポート チャネルの形成に FEX ポートを使用するように FEX プロファイルを設定します。
2. サーバに接続できるようにポート チャネルを設定します。

図 *17*：*FEX* ポート チャネル



（注） この手順では、FEX ポート チャネルにサーバを接続する手順を示します。手順は、ACI が接続された FEX にデバイスを接続する場合と同じになります。

はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチ、インターフェイス、およびプロトコルが設定されており、使用可能であること。
- FEX が設定されており、電源が入っていて、ターゲット リーフ インターフェイスに接続されていること。

ステップ 1 APIC で、FEX プロファイルにポート チャネルを追加します。

a) APIC メニュー バーで、[Fabric] > [Access Policies] > [Switch Policies] > [Profiles] に移動します。

b) [Navigation] ペインで、FEX プロファイルを選択します。
APIC で自動生成された FEX プロファイル名の形式は、*<switch policy name>_FexP<FEX ID>* です。

c) [FEX Profile] 作業領域で、[+] をクリックして、[Interface Selectors For FEX] リストに新しいエントリを追加します。
[Create Access Port Selector] ダイアログが開きます。

ステップ 2 FEX ポート チャネルにサーバを接続できるように、[Create Access Port Selector] をカスタマイズします。

a) セレクタの名前を指定します。

b) 使用する FEX インターフェイス ID を指定します。

c) リストから既存のインターフェイス ポリシー グループを選択するか、PC インターフェイス プロファイル グループを作成します。
ポート チャネル インターフェイス ポリシー グループは、選択した FEX のインターフェイスに適用するポリシーのグループを指定します。インターフェイス ポリシーの例は、リンク レベル ポリシー（たとえば、1 gbit ポート速度）、接続エンティティ プロファイル、ストーム制御インターフェイス ポリシーなどです。

（注） インターフェイス ポリシー グループ内で、FEX ポート セレクタで指定されているインターフェイスを EPG が使用できるようにするために、[Attached Entity Profile] は必須です。

d) [Port Channel Policy] オプションで、設定の要件に従って静的 LDAP または動的 LDAP を選択します。

e) [Submit] をクリックして、更新された FEX プロファイルを APIC に送信します。
APIC が FEX プロファイルを更新します。

確認：ポート チャネルが適切に設定されていることを確認するには、FEX が接続されているスイッチに対して CLI コマンド **show port-channel summary** を使用します。

次の作業

これで、FEX ポート チャネルの設定手順は完了しました。

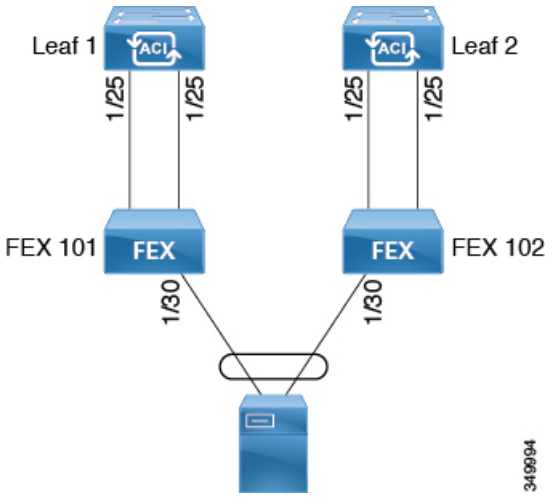
（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

FEX バーチャル ポート チャネル設定

主な手順は次のとおりです。

1. バーチャル ポート チャネルを形成するように、2 つの既存 FEX プロファイルを設定します。
2. FEX ポート チャネルにサーバを接続できるように、バーチャル ポート チャネルを設定します。

図 *18* : *FEX* バーチャル ポート チャネル



（注） この手順では、FEX バーチャル ポート チャネルにサーバを接続する手順を示します。手順は、ACI が接続された FEX にデバイスを接続する場合と同じになります。

はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチ、インターフェイス、およびプロトコルが設定されており、使用可能であること。
- FEX が設定されており、電源が入っていて、ターゲット リーフ インターフェイスに接続されていること。

ステップ 1 APIC で、2 つの FEX プロファイルにバーチャル ポート チャネルを追加します。

a) APIC メニュー バーで、[Fabric] > [Access Policies] > [Switch Policies] > [Profiles] に移動します。

b) [Navigation] ペインで、最初の FEX プロファイルを選択します。
APIC で自動生成された FEX プロファイル名の形式は、<*switch policy name*>_*FexP*<*FEX ID*> です。

c) [FEX Profile] 作業領域で、[+] をクリックして、[Interface Selectors For FEX] リストに新しいエントリを追加します。
[Create Access Port Selector] ダイアログが開きます。

ステップ 2 FEX バーチャル ポート チャネルにサーバを接続できるように、[Create Access Port Selector] をカスタマイズします。

a) セレクタの名前を指定します。

b) 使用する FEX インターフェイス ID を指定します。
通常、各 FEX に同じインターフェイス ID を使用してバーチャル ポート チャネルを形成します。

c) リストから既存のインターフェイス ポリシー グループを選択するか、VPC インターフェイス プロファイル グループを作成します。
バーチャル ポート チャネル インターフェイス ポリシー グループは、選択した FEX のインターフェイスに適用するポリシーのグループを指定します。インターフェイス ポリシーの例は、リンク レベル ポリシー（たとえば、1 gbit ポート速度）、接続エンティティ プロファイル、ストーム制御インターフェイス ポリシーなどです。

（注） インターフェイス ポリシー グループ内で、FEX ポート セレクタで指定されているインターフェイスを EPG が使用できるようにするために、[Attached Entity Profile] は必須です。

d) [Port Channel Policy] オプションで、設定の要件に従って静的 LDAP または動的 LDAP を選択します。

e) [Submit] をクリックして、更新された FEX プロファイルを APIC に送信します。
APIC が FEX プロファイルを更新します。

確認：ポート チャネルが適切に設定されていることを確認するには、FEX が接続されているスイッチに対して CLI コマンド **show port-channel summary** を使用します。

ステップ 3 最初の FEX に指定したものと同じインターフェイス ポリシー グループを使用するように 2 番目の FEX を設定します。

a) 2 番目の FEX プロファイルの [FEX Profile] 作業領域で、[+] をクリックして、[Interface Selectors For FEX] リストに新しいエントリを追加します。
[Create Access Port Selector] ダイアログが開きます。
b) セレクタの名前を指定します。
c) 使用する FEX インターフェイス ID を指定します。
通常、各 FEX に同じインターフェイス ID を使用してバーチャル ポート チャネルを形成します。
d) ドロップダウン リストから、最初の FEX プロファイルで使用したものと同じバーチャル ポート チャネル インターフェイス ポリシー グループを選択します。
バーチャル ポート チャネル インターフェイス ポリシー グループは、選択した FEX のインターフェイスに適用するポリシーのグループを指定します。インターフェイス ポリシーの例は、リンクレベル ポリシー（たとえば、1 gbit ポート速度）、接続エンティティ プロファイル、ストーム制御インターフェイス ポリシーなどです。

（注） インターフェイス ポリシー グループ内で、FEX ポート セレクタで指定されているインターフェイスを EPG が使用できるようにするために、[Attached Entity Profile] は必須です。

e) [Submit] をクリックして、更新された FEX プロファイルを APIC に送信します。
APIC が FEX プロファイルを更新します。

確認：バーチャル ポート チャネルが適切に設定されていることを確認するには、いずれかの FEX が接続されているスイッチに対して CLI コマンド **show vpc extended** を使用します。

次の作業

これで、FEX バーチャル ポート チャネルの設定手順は完了しました。

（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

トラフィック ストーム制御について

トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御ポリシーを使用すると、物理インターフェイス上におけるブロードキャスト、未知のマルチキャスト、または未知のユニキャストのトラフィック ストームによって、レイヤ 2 ポート経由の通信が妨害されるのを防ぐことができます。

デフォルトでは、ストーム制御は ACI ファブリックでは有効になっていません。ACI ブリッジ ドメイン（BD）レイヤ 2 の未知のユニキャストのフラッディングは BD 内でデフォルトで有効になっていますが、管理者が無効にすることができます。その場合、ストーム制御ポリシーはブロードキャストと未知のマルチキャストのトラフィックにのみ適用されます。レイヤ 2 の未知のユニキャストのフラッディングが BD で有効になっている場合、ストーム制御ポリシーは、ブロード

キャストと未知のマルチキャストのトラフィックに加えて、レイヤ 2 の未知のユニキャストのフラッディングに適用されます。

トラフィック ストーム制御（トラフィック抑制ともいいます）を使用すると、着信するブロードキャスト、マルチキャスト、未知のユニキャストのトラフィックのレベルを 1 秒間隔でモニタできます。この間に、トラフィック レベル（ポートで使用可能な合計帯域幅のパーセンテージ、または特定のポートで許可される 1 秒あたりの最大パケット数として表されます）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。管理者は、ストーム制御しきい値を超えたときにエラーを発生させるようにモニタリング ポリシーを設定できます。

ストーム制御のガイドライン

以下のガイドラインと制約事項に従って、トラフィック ストーム制御レベルを設定してください。

- 通常、ファブリック管理者は以下のインターフェイスのファブリック アクセス ポリシーでストーム制御を設定します。
  - 標準トランク インターフェイス。
  - 単一リーフ スイッチ上のダイレクト ポート チャネル。
  - バーチャル ポート チャネル（2 つのリーフ スイッチ上のポート チャネル）。
- ポート チャネルおよびバーチャル ポート チャネルでは、ストーム制御値（1 秒あたりのパケット数またはパーセンテージ）はポート チャネルのすべての個別メンバーに適用されます。ポート チャネルのメンバーであるインターフェイスには、ストーム制御を設定しないでください。
- 使用可能な帯域幅のパーセンテージで設定する場合、値 100 はトラフィック ストーム制御を行わないことを意味し、値 0.01 はすべてのトラフィックを抑制します。
- ハードウェアの制限およびさまざまなサイズのパケットのカウント方式が原因で、レベルのパーセンテージは概数になります。着信トラフィックを構成するフレームのサイズに応じて、実際に適用されるパーセンテージ レベルと設定したパーセンテージ レベルの間には、数パーセントの誤差がある可能性があります。1 秒あたりのパケット数（PPS）の値は、256 バイトに基づいてパーセンテージに変換されます。
- 最大バーストは、通過するトラフィックがないときに許可されるレートの最大累積です。トラフィックが開始されると、最初の間隔では累積レートまでのすべてのトラフィックが許可されます。後続の間隔では、トラフィックは設定されたレートまでのみ許可されます。サポートされる最大数は 65535 KB です。設定されたレートがこの値を超えると、PPS とパーセンテージの両方についてこの値で制限されます。
- 累積可能な最大バーストは 512 MB です。
- 最適化されたマルチキャスト フラッディング（OMF）モードの出力リーフ スイッチでは、トラフィック ストーム制御は適用されません。

- OMF モードではない出力リーフ スイッチでは、トラフィック ストーム制御が適用されます。
- FEX のリーフ スイッチでは、ホスト側インターフェイスにはトラフィック ストーム制御を使用できません。

GUI を使用したトラフィック ストーム制御ポリシーの設定

ステップ 1 メニュー バーで、[Fabric] をクリックします。

ステップ 2 サブメニュー バーで、[Access Policies] をクリックします。

ステップ 3 [Navigation] ペインで、[Interface Policies] を展開します。

ステップ 4 [Policies] を展開します。

ステップ 5 [Storm Control] を右クリックし、[Create Storm Control Interface Policy] を選択します。

ステップ 6 [Create Storm Control Interface Policy] ダイアログボックスで、[Name] フィールドにポリシーの名前を入力します。

ステップ 7 [Specify Policy In] フィールドで、[Percentage] または [Packets Per Second] いずれかのオプション ボタンをクリックします。

ステップ 8 [Percentage] を選択した場合は、次の手順を実行します。

a) [Rate] フィールドに、トラフィック レートのパーセンテージを入力します。
ポートで使用可能な合計帯域幅のパーセンテージを指定する 0 ～ 100 の数値を入力します。1 秒の間隔中に入力トラフィックがこのレベルに達すると、トラフィック ストーム制御により、その間隔の残りのトラフィックはドロップされます。値 100 は、トラフィック ストーム制御を行わないことを意味します。値 0 の場合、すべてのトラフィックが抑制されます。

b) [Max Burst Rate] フィールドに、バースト トラフィック レートのパーセンテージを入力します。
ポートで使用可能な合計帯域幅のパーセンテージを指定する 0 ～ 100 の数値を入力します。入力トラフィックがこのレベルに達すると、ストーム制御がトラフィックをドロップし始めます。

ステップ 9 [Packets Per Second] を選択した場合は、次の手順を実行します。

a) [Rate] フィールドに、トラフィック レートを 1 秒あたりのパケット数で入力します。
この間、トラフィック レベル（1 秒あたりにポートを通過するパケット数として表される）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

b) [Max Burst Rate] フィールドに、バースト トラフィック レートを 1 秒あたりのパケット数で入力します。
この間、トラフィック レベル（1 秒あたりにポートを通過するパケット数として表される）が、設定したバースト トラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

ステップ 10 [Submit] をクリックします。

ステップ 11 ストーム制御インターフェイス ポリシーをインターフェイス ポートに適用します。

a) メニュー バーで、[Fabric] をクリックします。
b) サブメニュー バーで、[Access Policies] をクリックします。
c) [Navigation] ペインで、[Interface Policies] を展開します。
d) [Policy Groups] を展開します。
e) [Policy Group] を選択します。
f) [Work] ペインで、[Storm Control Interface Policy] のドロップダウンをクリックし、作成したトラフィック ストーム制御ポリシーを選択します。
g) [Submit] をクリックします。

REST API を使用したトラフィック ストーム制御ポリシーの設定

トラフィック ストーム制御ポリシーを設定するには、希望するプロパティを使用して `stormctrl:IfPol` オブジェクトを作成します。

MyStormPolicy というポリシーを作成するには、次の HTTP POST メッセージを送信します。

```
POST https://192.0.20.123/api/mo/uni/infra/stormctrlifp-MyStormPolicy.json
```

使用可能な帯域幅のパーセンテージでポリシーを指定するには、POST メッセージの本文に次の JSON ペイロード構造を含めます。

```
{"stormctrlIfPol":
    {"attributes":
        {"dn":"uni/infra/stormctrlifp-MyStormPolicy",
        "name":"MyStormPolicy",
        "rate":"75",
        "burstRate":"85",
        "rn":"stormctrlifp-MyStormPolicy",
        "status":"created"
        },
        "children":[]
    }
}
```

1 秒あたりのパケット数でポリシーを指定するには、POST メッセージの本文に次の JSON ペイロード構造を含めます。

```
{"stormctrlIfPol":
    {"attributes":
        {"dn":"uni/infra/stormctrlifp-MyStormPolicy",
        "name":"MyStormPolicy",
        "ratePps":"12000",
        "burstPps":"15000",
        "rn":"stormctrlifp-MyStormPolicy",
        "status":"created"
        },
        "children":[]
    }
}
```

トラフィック ストーム制御インターフェイス ポリシーをインターフェイス ポートに適用します。

```
POST
http://192.0.20.123/api/node/mo/uni/infra/funcprof/accportgrp-InterfacePolicyGroup/rsstormctrlIfPol.json
```

ポリシーをインターフェイス ポリシー グループに適用するには、POST メッセージの本文に次の JSON ペイロード構造を含めます。

```
{"infraRsStormctrlIfPol":{"attributes":{"tnStormctrlIfPolName":"testStormControl"},"children":[]}}
```

CLI を使用したトラフィック ストーム制御ポリシーの設定

手順の概要

1. CLI で、ディレクトリを /storm-ctrl に変更します。
2. PPS ポリシーを作成するには、次の手順に従います。
3. パーセント ポリシーを作成するには、次の手順に従います。
4. CLI を使用して、トラフィック ストーム制御ポリシーを適用します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	CLI で、ディレクトリを /storm-ctrl に変更します。 例： `cd aci/fabric/access-policies/interface-policies/policies/storm-ctrl/`	

ステップ 2	PPS ポリシーを作成するには、次の手順に従います。
	
	例：
	`> mocreate pps_10k_10k`
	`> cd pps_10k_10k/`
	`> moset rate-in-pps 10000`
	`> moset burst-rate-in-pps 10000`
	`> moconfig commit`	

ステップ 3	パーセント ポリシーを作成するには、次の手順に従います。
	
	例：
	`> cd /home/admin/aci/fabric/access-policies/interface-policies/policies/storm-ctrl`
	`> mocreate percent_50_60`
	`> cd percent_50_60/`
	`> moset rate-in-percentage 50`
	`> moset burst-rate-in-percentage 60`
	`> moconfig commit`	

ステップ 4	CLI を使用して、トラフィック ストーム制御ポリシーを適用します。
	
	例：
	`> cd`
	`/aci/fabric/access-policies/interface-policies/policy-groups/interface/InterfacePolicyGroup`	

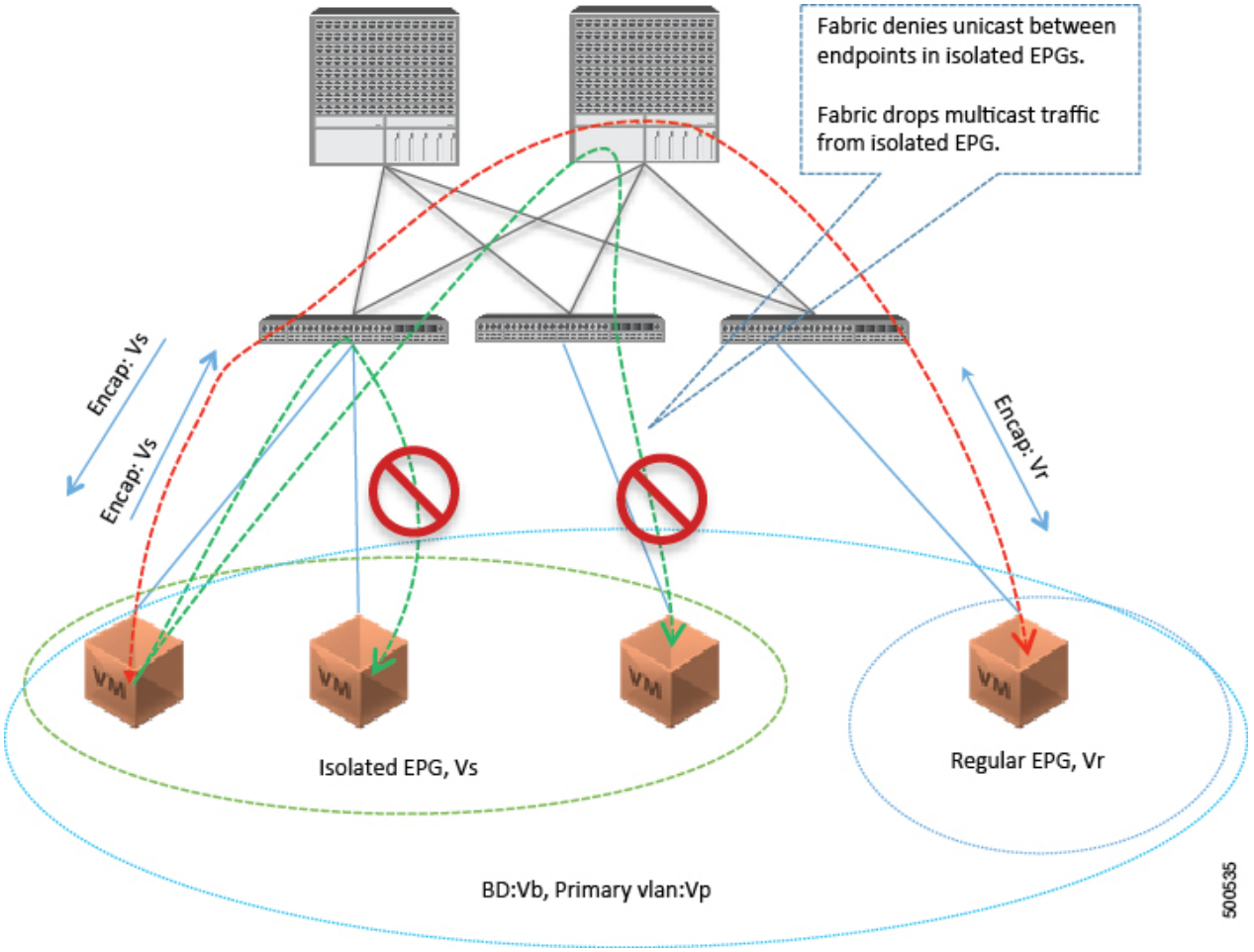
	コマンドまたはアクション	目的
	`> moset storm-control-policy MyStormPolicy` `> moconfig commit "`	

EPG 内拒否エンドポイントの分離

EPG 内拒否ポリシーにより、仮想エンドポイントまたは物理エンドポイントが完全に分離されます。完全分離モードで稼働している EPG 内のエンドポイント間の通信は許可されません。分離モードの EGP では、多くのクライアントが共通サービスにアクセスするときに必要な EPG カプセル化の数が削減されますが、相互通信は許可されません。EPG は、すべての ACI ネットワークドメインで分離されるか、またはどのドメインでも分離されません。ACI ファブリックは接続エ

ンドポイントに直接分離を実装しますが、ファブリックに接続されているスイッチはプライマリ VLAN（PVLAN）タグに従って分離規則を認識します。

図 *19*：ベア メタル

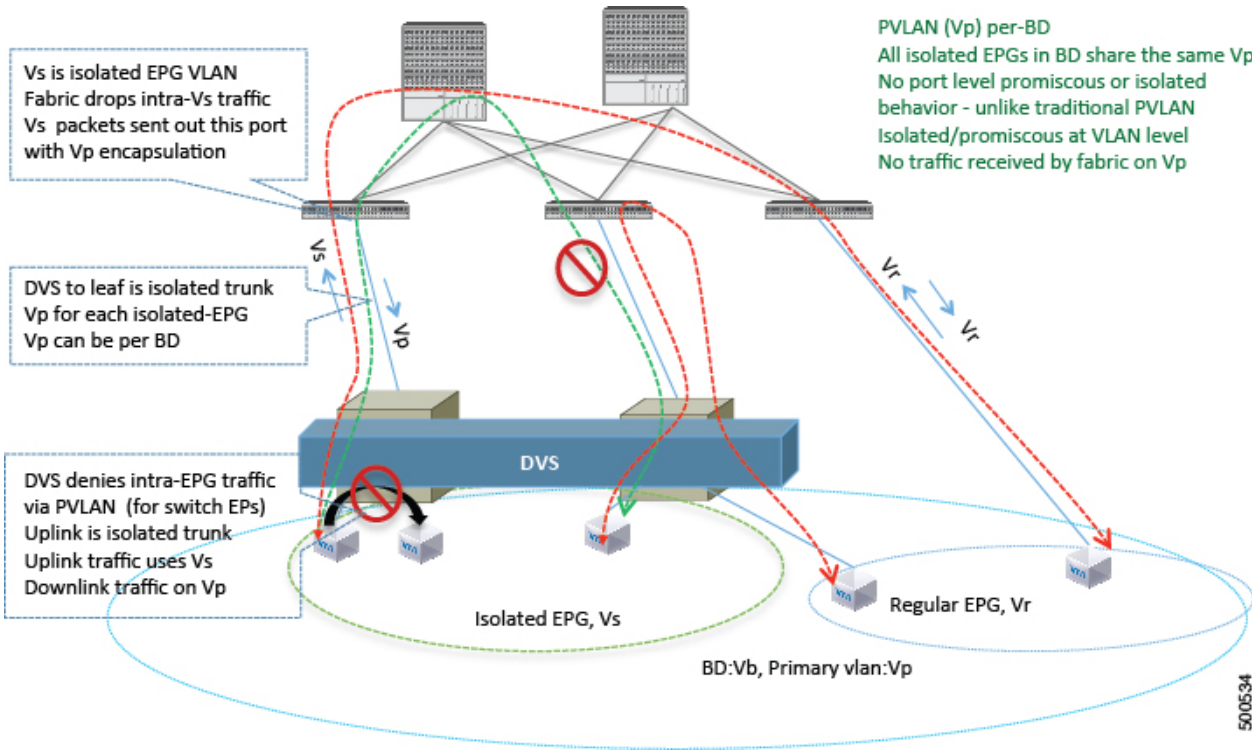


いくつかの使用例を次に示します。

- バックアップ クライアントは、バックアップ サービスにアクセスするための通信要件は同じですが、相互に通信する必要はありません。
- ロードバランサの背後にあるサーバの通信要件は同じですが、それらのサーバを相互に分離すると、不正アクセスや感染のあるサーバに対して保護されます。

EPG 内拒否分離は、PVLAN タグに基づいて VMware Distributed Virtual Switch（DVS）導入環境に適用できます。

図 *20*：*VMware DVS*



ACI Virtual Machine Manager（VMM）ドメインは、EPG 内拒否が有効である EGP ごとに DVS に分離 PVLAN ポート グループを作成します。追加のプライマリ カプセル化を、管理者が提供するか、または EPG/VMM ドメイン間の関連付け時に動的に割り当てる必要があります。VMM は、分離されたセカンダリ（Vs）を持つプライマリ VLAN（Vp）を DVS に作成します。EPG 内拒否 EPG は、タイプを `PVLAN` に設定して Vs を使用します。ファブリックから DVS への通信では Vp が使用されます。DVS とファブリックは Vp/Vs カプセル化を交換します。Vp/Vs ペアは、EPG/ドメイン間の関連付け時に VMM ドメインごとに選択されます。ファブリック管理者が Vp と Vs の値を静的に選択するときに、VMM は、Vp と Vs がドメイン プール内の静的ブロックに含まれていること、およびそのドメイン内の他の EPG との衝突がないことを検証します。

（注） EPG 内エンドポイントの拒否分離を適用して EPG が設定されている場合、さらに 2 つの制限が適用されます。

- 分離された EPG 全体のすべてのレイヤ 2 エンドポイント通信は、ブリッジ ドメイン内にドロップされます。
- 分離された EPG 全体のすべてのレイヤ 3 エンドポイント通信は、同じサブネット内にドロップされます。

GUI を使用した EPG 内拒否 EPG の設定

EPG が使用するポートは、物理ドメイン内のベア メタル サーバ インターフェイスに関連付けられているか、またはいずれかの VM マネージャ（VMM）に属している必要があります。

手順の概要

1. テナントで、[Application Profile] を右クリックし、[Create Application EPG] ダイアログ ボックスを開いて次の操作を実行します。
2. [Domains] ダイアログボックスで、次の操作を実行します。
3. [Leaves/Paths] ダイアログボックスで、次の操作を実行します。

手順の詳細

ステップ 1 テナントで、[Application Profile] を右クリックし、[Create Application EPG] ダイアログ ボックスを開いて次の操作を実行します。

a) [Name] フィールドに、EPG の名前（intra_EPG-deny）を追加します。
b) [Intra EPG Isolation] で、[Enforced] をクリックします。
c) [Bridge Domain] フィールドで、ドロップダウン リストからブリッジ ドメイン（bd1）を選択します。
d) EPG をベア メタル/物理ドメイン インターフェイスまたは VM ドメインに関連付けます。
VM ドメインの場合、[Associate to VM Domain Profiles] チェックボックスをオンにします。

ベア メタルの場合、[Statically Link with Leaves/Paths] チェックボックスをオンにします。

e) [Next] をクリックします。
f) [Step 2 for Specify the VM Domains] 領域で、[Associate VM Domain Profiles] を展開し、ドロップダウン リストから目的の VMM ドメインを選択します。[Update] をクリックし、[OK] をクリックします。

ステップ 2 [Domains] ダイアログボックスで、次の操作を実行します。

a) ベア メタルの場合、[Domain Profile] フィールドで、ドロップダウン リストからドメイン プロファイルを選択します（VMwarePVLAN）。

スタティックの場合、[Port Encap (or Secondary VLAN for Micro-Seg)] フィールドで、セカンダリ VLAN（vlan-2005）を指定し、[Primary VLAN for Micro-Seg] フィールドで、プライマリ VLAN（vlan-2006）を指定します。Encap フィールドを空白のままにすると、値が動的に割り当てられます。

（注） スタティックの場合、スタティック VLAN を VLAN プールで使用できる必要があります。

b) VMware DVS の場合、[Domain Profile] フィールドで、ドロップダウン リストからドメイン プロファイルを選択します（VMwareDVS）。

c) [Next] をクリックします。

ステップ 3 [Leaves/Paths] ダイアログボックスで、次の操作を実行します。

a) ベア メタルの場合、[Path] セクションで、ドロップダウン リストからトランク モードでのパスを選択します（Node-107/eth1/16）。
セカンダリ VLAN の [Port Encap]（vlan-102）を指定します。

プライマリ VLAN の [Primary Encap]（vlan-103）を指定します。

b) VMware DVS の場合、[Path] セクションで、ドロップダウン リストからトランク モードでのパスを選択します（Node-107/eth1/16）。

c) [Update] をクリックします。

d) [Finish] をクリックします。

NX-OS スタイルの CLI を使用した EPG 内拒否 EPG の設定

手順の概要

1. CLI で、EPG 内拒否 EPG を作成します。
2. 設定を確認します。

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	CLI で、EPG 内拒否 EPG を作成します。
	
	例：
	以下に、VMM ケースを示します。
	`ifav19-ifc1(config)# tenant SCVMMTenant`
	`ifav19-ifc1(config-tenant)# application PVLAN`
	`ifav19-ifc1(config-tenant-app)# epg EPG1`
	`ifav19-ifc1(config-tenant-app-epg)# show running-config`
	`# Command: show running-config`
	`tenant SCVMMTenant`
	`  application PVLAN epg EPG1`	

	コマンドまたはアクション	目的

```
  tenant SCVMMTenant
     application PVLAN
      epg EPG1
        bridge-domain member VMM_BD
        contract consumer SCVMM-Ext
        contract consumer default
        contract provider Deny_EPG
        vmware-domain member PVLAN encap vlan-2002 primary-encap vlan-2001 push on-demand <---
Assigns static primary & secondary encap to EPG.
        vmware-domain member mininet  <--- If no static vlan assigned APIC assigns primary &
secondary encap for isolated EPG.
        isolation enforce   <---- This enables EPG into isolation mode.
        exit
    exit
exit
```

例：
スタティック バインディング EPG -> Tenant:Tenant_BareMetal -> Application: PVLAN -> Static を関連付けるには、次のようにします。

```
ifav19-ifc1(config)#
ifav19-ifc1(config)# leaf ifav19-leaf3
ifav19-ifc1(config-leaf)# interface ethernet 1/16
ifav19-ifc1(config-leaf-if)# show running-config
ifav19-ifc1(config-leaf-if)# switchport trunk native vlan 101 tenant SCVMMTenant application
PVLAN epg StaticEPG primary-vlan 100
```

ステップ 2 設定を確認します。

例：

```
 show epg StaticEPG detail
Application EPg Data:
Tenant               : SCVMMTenant
Application          : PVLAN
AEPg                 : StaticEPG
BD                   : VMM_BD
uSeg EPG             : no
Intra EPG Isolation  : enforced
Vlan Domains         : phys
Consumed Contracts   : SCVMM-Ext
Provided Contracts   : default,Deny_EPG
Denied Contracts     :
Qos Class            : unspecified
Tag List             :
VMM Domains:
Domain                Type       Deployment Immediacy  Resolution Immediacy  State
Encap       Primary
Encap
 --------------------  ---------  --------------------  --------------------  --------------
----------  ----------
 DVS1                  VMware     On Demand             immediate             formed
auto        auto

Static Leaves:
 Node        Encap             Deployment Immediacy  Mode                Modification Time

----------  ----------------  --------------------  ------------------
------------------------------

Static Paths:
 Node        Interface                       Encap             Modification Time
 ----------  ------------------------------  ----------------  ------------------------------
```

	コマンドまたはアクション	目的
	1018 eth101/1/1 vlan-100 2016-02-11T18:39:02.337-08:00 1019 eth1/16 vlan-101 2016-02-11T18:39:02.337-08:00 Static Endpoints: Node Interface Encap End Point MAC End Point IP Address Modification Time ---------- ---------- ---------- ---------- ---------- Dynamic Endpoints: Encap: (P):Primary VLAN, (S):Secondary VLAN Node Interface Encap End Point MAC End Point IP Address Modification Time ---------- ---------- ---------- ---------- ---------- 1017 eth1/3 **vlan-943(P)** 00:50:56:B3:64:C4 --- 2016-02-17T18:35:32.224-08:00 **vlan-944(S)**	

REST API を使用した EPG 内拒否 EPG の設定

はじめる前に

EPG が使用するポートは、物理ドメイン内のベア メタル サーバ インターフェイスに関連付けられているか、またはいずれかの VM マネージャ（VMM）に属している必要があります。

手順の概要

1. XML API を使用してアプリケーションを展開するには、次の HTTP POST メッセージを送信します。
2. ベア メタル展開では、POST メッセージの本文にこの XML 構造を含めます。
3. VMM 展開では、POST メッセージの本文にこの XML 構造を含めます。

手順の詳細

ステップ 1 XML API を使用してアプリケーションを展開するには、次の HTTP POST メッセージを送信します。

例：

```
POST
https://192.0.20.123/api/mo/uni/tn-ExampleCorp.xml
```

ステップ 2 ベア メタル展開では、POST メッセージの本文にこの XML 構造を含めます。

例：

```
<fvTenant name="Tenant_BareMetal" >
  <fvAp name="Web">
    <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
          <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
          <fvRsBd tnFvBDName="bd" />
          <fvRsDomAtt tDn="uni/phys-Dom1" />
          <!-- PATH ASSOCIATION -->
          <fvRsPathAtt tDn="topology/pod-1/paths-1017/pathep-[eth1/2]" encap="vlan-51"
primaryEncap="vlan-100" instrImedcy='immediate'/>
    </fvAEPg>
 </fvAp>
</fvTenant>
```

ステップ 3 VMM 展開では、POST メッセージの本文にこの XML 構造を含めます。

例：

```
<fvTenant name="Tenant_VMM" >
  <fvAp name="Web">
    <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
          <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
          <fvRsBd tnFvBDName="bd" />
          <fvRsPathAtt tDn="topology/pod-1/paths-1017/pathep-[eth1/2]" encap="vlan-51"
primaryEncap="vlan-100" instrImedcy='immediate'/>
          <!-- STATIC ENCAP ASSOCIATION TO VMM DOMAIN-->
          <fvRsDomAtt encap="vlan-2001" instrImedcy="lazy" primaryEncap="vlan-2002"
resImedcy="immediate" tDn="uni/vmmp-VMware/dom-DVS1”>
    </fvAEPg>
 </fvAp>
</fvTenant>
```

第 5 章

基本ユーザ テナント設定

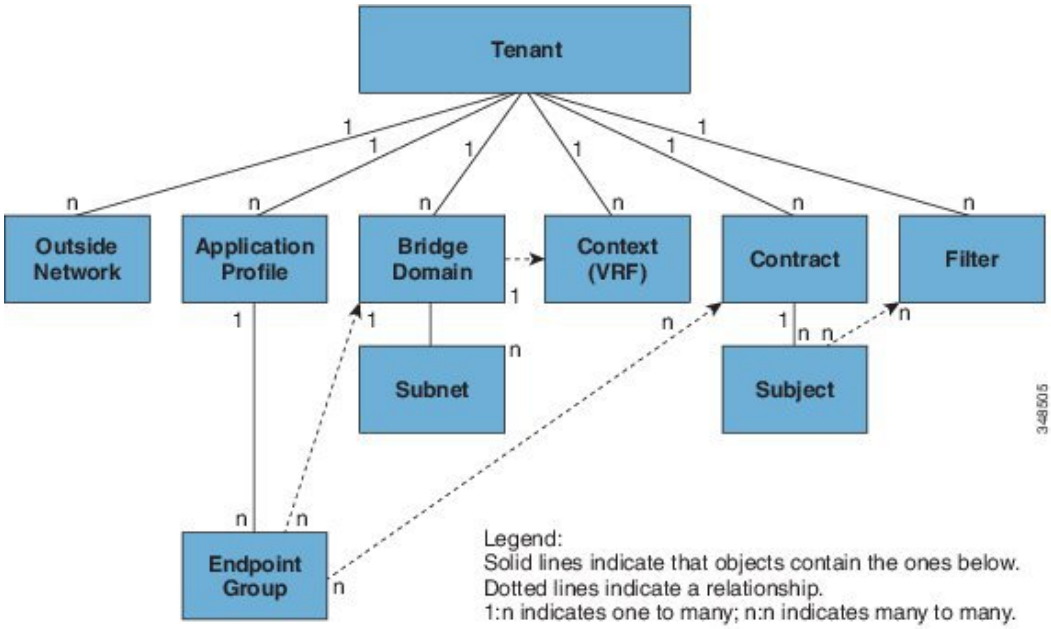
この章の内容は、次のとおりです。

テナント

テナント（`fvTenant`）は、アプリケーション ポリシーの論理コンテナで、管理者はドメインベースのアクセス コントロールを実行できます。テナントはポリシーの観点から分離の単位を表しますが、プライベート ネットワークは表しません。テナントは、サービス プロバイダーの環境では

お客様を、企業の環境では組織またはドメインを、または単にポリシーの便利なグループ化を表すことができます。次の図は、管理情報ツリー（MIT）のテナント部分の概要を示します。

図 *21*：テナント



テナントは相互に分離することも、リソースを共有することもできます。テナントが含む主要な要素は、フィルタ、コントラクト、外部ネットワーク、ブリッジ ドメイン、コンテキスト、およびエンドポイント グループ（EPG）を含むアプリケーション プロファイルです。テナントのエンティティはそのポリシーを継承します。テナントには、1 つ以上の仮想ルーティングおよび転送（VRF）インスタンスまたはコンテキストを含めることができます。各コンテキストは、複数のブリッジ ドメインに関連付けることができます。

（注） テナント ナビゲーション パス の下の APIC GUI では、コンテキスト（VRF）はプライベート ネットワークと呼ばれます。

テナントはアプリケーション ポリシーの論理コンテナです。ファブリックには複数のテナントを含めることができます。レイヤ 4 ～ 7 のサービスを展開する前に、テナントを設定する必要があります。ACI ファブリックは、テナント ネットワークに対して IPv4、IPv6、およびデュアル スタック構成をサポートします。

テナント内のルーティング

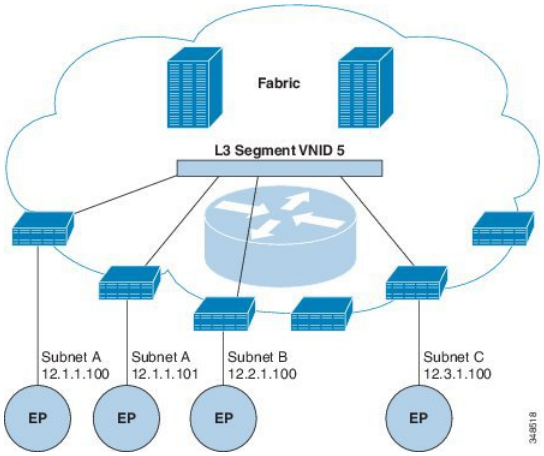
アプリケーション セントリック インフラストラクチャ（ACI）のファブリックでは、テナントのデフォルト ゲートウェイ機能が提供され、ファブリックの Virtual Extensible Local Area（VXLAN）

ネットワーク間のルーティングが行えます。各テナントについて、APIC でサブネットが作成されるたびに、ファブリックは仮想デフォルト ゲートウェイまたはスイッチ仮想インターフェイス（SVI）を提供します。これは、そのテナント サブネットの接続エンドポイントがあるすべてのスイッチにわたります。各入力インターフェイスはデフォルトのゲートウェイ インターフェイスをサポートし、ファブリック全体のすべての入力インターフェイスは任意のテナント サブネットに対する同一のルータの IP アドレスと MAC アドレスを共有します。

Intersubnet のテナント トラフィックを転送するために使用されるレイヤ 3 VNID

ACI モデルでは、ACI ファブリックのデフォルト ゲートウェイに送信されるファブリックのイングレスに到達するトラフィックは、レイヤ 3 VNID として知られる仮想ネットワーク セグメントにルーティングされます。単一のレイヤ 3 VNID が、各テナント コンテキストに割り当てられます。次の図は、テナント内のルーティングがどのように行われるかを示します。

図 *22* : *Intersubnet* のテナント トラフィックを転送するレイヤ *3 VNID*



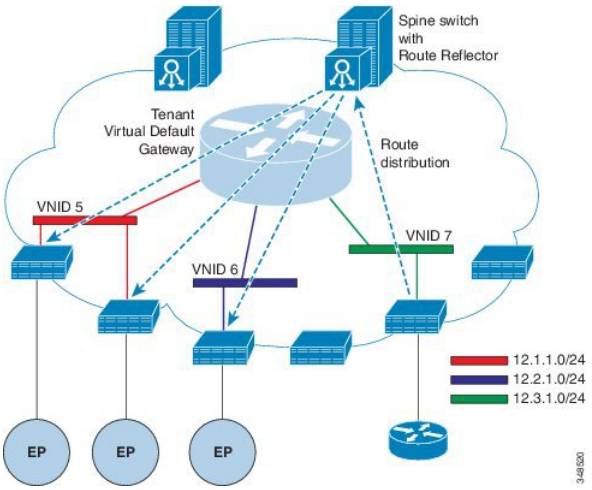
レイヤ 3 VNID は、APIC によって割り当てられます。ファブリックを経由するトラフィックは、レイヤ 3 セグメントの VNID を使用して転送されます。出力リーフ スイッチでは、パケットはレイヤ 3 セグメントの VNID から出力サブネットの VNID にルーティングされます。

ACI モデルでは、テナント内でルーティングされるトラフィックのファブリックで非常に効率的な転送が提供されます。たとえば、同じ物理ホストの同じテナントに属するがサブネットは異なる 2 つの仮想マシン（VM）間のトラフィックでは、（最小パス コストを使用して）正しい宛先にルーティングされる前の移動先は入力スイッチのみです。現在の VM 環境では、トラフィックは正しい宛先にルーティングされる前に、（異なる物理サーバ上にあると思われる）エッジ VM に伝送されます。

ルータ ピアリングおよびルート配布

次の図に示すように、ルーティング ピア モデルを使用すると、リーフ スイッチ インターフェイスが外部ルータのルーティング プロトコルとピアリングするように静的に設定されます。

図 *23*：ルータのピアリング

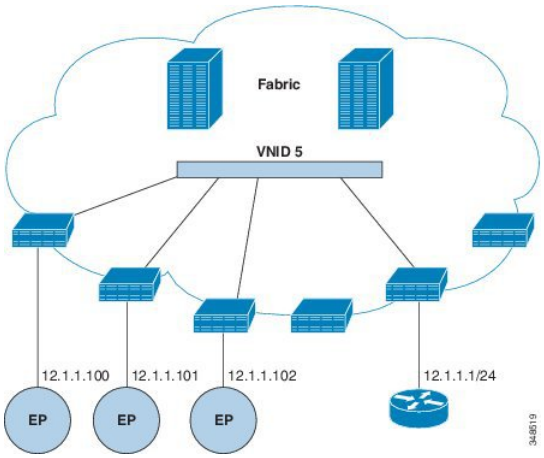


ピアリングによって学習されるルートは、スパイン スイッチに送信されます。スパイン スイッチはルート リフレクタとして動作し、外部ルートを同じテナントに属するインターフェイスを持つすべてのリーフ スイッチに配布します。これらのルートは、最長プレフィクス照合（LPM）により集約されたアドレスで、外部ルータが接続されているリモートのリーフ スイッチの VTEP IP アドレスが含まれるリーフ スイッチの転送テーブルに配置されます。WAN ルートには転送プロキシはありません。WAN ルートがリーフ スイッチの転送テーブルに適合しない場合、トラフィックはドロップされます。外部ルータがデフォルト ゲートウェイではないため、テナントのエンドポイント（EP）からのパケットはACI ファブリックのデフォルト ゲートウェイに送信されます。

外部ルータへのブリッジド インターフェイス

次の図に示すように、リーフ スイッチのインターフェイスがブリッジドインターフェイスとして設定されている場合、テナント VNID のデフォルト ゲートウェイが外部ルータとなります。

図 *24*：ブリッジド外部ルータ



ACI ファブリックは、外部ルータの存在を認識せず、APIC はリーフ スイッチのインターフェイスを EPG に静的に割り当てます。

ルート リフレクタの設定

ACI ファブリックのルート リフレクタは、マルチプロトコル BGP（MP-BGP）を使用してファブリック内に外部ルートを配布します。ACI ファブリックでルート リフレクタをイネーブルにするには、ファブリックの管理者がルートリフレクタになるスパインスイッチを選択して、自律システム（AS）番号を提供する必要があります。ルート リフレクタが ACI ファブリックでイネーブルになると、管理者は次の項で説明するように、外部ネットワークへの接続を設定できます。

ACI ファブリックに外部ルータを接続するには、ファブリック インフラストラクチャの管理者がボーダー ゲートウェイ プロトコル（BGP）のルート リフレクタとしてスパイン ノードを設定します。冗長性のために、複数のスパインがルータ リフレクタ ノードとして設定されます（1 台のプライマリ リフレクタと 1 台のセカンダリ リフレクタ）。

テナントが ACI ファブリックに WAN ルータを接続する必要がある場合は、インフラストラクチャの管理者が WAN ルータが WAN のトップ オブ ラック（ToR）として接続されるリーフ ノードを（以下の通りに）設定し、この WAN ToR を BGP ピアとしてルート リフレクタ ノードの 1 つと組み合わせます。ルート リフレクタが WAN ToR に設定されていると、ファブリックにテナント ルートをアドバタイズできます。

各リーフ ノードには最大 4000 のルートを保存できます。WAN ルータが 4000 を超えるルートをアドバタイズしなければならない場合、複数のリーフ ノードとピアリングする必要があります。

インフラストラクチャの管理者は、ペアになったリーフ ノードそれぞれをアドバタイズできるルート（またはルート プレフィクス）で設定します。

インフラストラクチャの管理者は、次のようにファブリックに接続されている外部 WAN ルータを設定する必要があります。

1. ルート リフレクタとして最大 2 つのスパイン ノードを設定します。冗長性のために、プライマリおよびセカンダリ ルート リフレクタを設定します。
2. WAN ToR で、プライマリおよびセカンダリ ルート リフレクタのノードを設定します。
3. WAN ToR で、ToR がアドバタイズを担当するルートを設定します。これは任意で、テナント ルータが 4000 を超えるルートをアドバタイズすることがわかっている場合にのみ行う必要があります。

テナントの外部接続の設定

スタティック ルートをアプリケーション セントリック インフラストラクチャ（ACI）ファブリック上の他のリーフ スイッチに配布する前に、マルチプロトコル BGP（MP-BGP）プロセスが最初に動作していて、スパイン スイッチが BGP ルート リフレクタとして設定されている必要があります。

ACI ファブリックを外部ルーテッド ネットワークに統合するために、管理テナントのレイヤ 3 接続に対し Open Shortest Path First（OSPF）を設定できます。

拡張 GUI を使用した MP-BGP ルート リフレクタの設定

（注） このタスク例のビデオを視聴するには、ビデオを掲載している Web ページ を参照してください。

ステップ 1 メニュー バーで、[FABRIC] > [Fabric Policies] を選択します。

ステップ 2 [Navigation] ペインで、[Pod Policies] > [Policies] > [BGP Route Reflector default] を展開し、[BGP Route Reflector default] を右クリックし、[Create Route Reflector Node Policy EP] をクリックします。

ステップ 3 [Create Route Reflector Node Policy EP] ダイアログボックスで、[Spine Node] ドロップダウン リストから、適切なスパイン ノードを選択します。[Submit] をクリックします。

（注） 必要に応じてスパイン ノードを追加するには、上記の手順を繰り返してください。

スパイン スイッチがルート リフレクタ ノードとしてマークされます。

ステップ 4 [BGP Route Reflector default] プロパティ領域で、[Autonomous System Number] フィールドで、適切な番号を選択します。[Submit] をクリックします。

（注） 自律システム番号は、Border Gateway Protocol（BGP）がルータに設定されている場合は、リーフが接続されたルータ設定に一致する必要があります。スタティックまたは Open Shortest Path First（OSPF）を使用して学習されたルートを使用している場合は、自律システム番号値を任意の有効な値にできます。

ステップ 5 [Navigation] ペインで、[Policy Groups] を展開して右クリックし、[Create POD Policy Group] をクリックします。

ステップ 6 [Create POD Policy Group] ダイアログボックスで、[Name] フィールドに、ポッド ポリシー グループの名前を入力します。

ステップ 7 [BGP Route Reflector Policy] ドロップダウン リストで、適切なポリシー（デフォルト）を選択します。[Submit] をクリックします。
BGP ルート リフレクタのポリシーは、ルート リフレクタのポッド ポリシー グループに関連付けられ、BGP プロセスはリーフ スイッチでイネーブルになります。

ステップ 8 [Navigation] ペインで、[Pod Policies] > [Profiles] > [default] の順に選択します。[Work] ペインで、[Fabric Policy Group] ドロップダウン リストから、前に作成されたポッド ポリシーを選択します。[Submit] をクリックします。
ポッド ポリシー グループが、ファブリック ポリシー グループに適用されました。

拡張 GUI を使用した管理テナントの OSPF 外部ルーテッド ネットワークの作成

- ルータ ID と論理インターフェイス プロファイルの IP アドレスが異なっていて重複していないことを確認します。
- 次の手順は、管理テナントの OSPF 外部ルーテッド ネットワークを作成するためのものです。テナントの OSPF 外部ルーテッド ネットワークを作成するには、テナントを選択し、テナント用の VRF を作成する必要があります。
- 詳細については、トランジット ルーティングに関する KB 記事も参照してください。

（注） このタスク例のビデオを視聴するには、ビデオを掲載している Web ページ を参照してください。

ステップ 1 メニュー バーで、[TENANTS] > [mgmt] を選択します。

ステップ 2 [Navigation] ペインで、[Networking] > [External Routed Networks] を展開します。

ステップ 3 [External Routed Networks] を右クリックし、[Create Routed Outside] をクリックします。

ステップ 4 [Create Routed Outside] 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、名前（RtdOut）を入力します。

b) [OSPF] チェックボックスをオンにします。

c) [OSPF Area ID] フィールドに、エリア ID を入力します。
d) [OSPF Area Control] フィールドで、適切なチェックボックスをオンにします。
e) [OSPF Area Type] フィールドで、適切なエリア タイプを選択します。
f) [OSPF Area Cost] フィールドで、適切な値を選択します。
g) [VRF] フィールドのドロップダウン リストから、VRF（inb）を選択します。
（注） このステップでは、ルーテッド Outside をインバンド VRF に関連付けます。
h) [External Routed Domain] ドロップダウン リストから、適切なドメインを選択します。
i) [Nodes and Interfaces Protocol Profiles] 領域の [+] アイコンをクリックします。

ステップ 5 [Create Node Profile] 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、ノード プロファイルの名前を入力します（borderLeaf）。
b) [Nodes] フィールドで、[+] アイコンをクリックして [Select Node] ダイアログボックスを表示します。
c) [Node ID] フィールドで、ドロップダウン リストから、最初のノードを選択します（leaf1）。
d) [Router ID] フィールドに、一意のルータ ID を入力します。
e) [Use Router ID as Loopback Address] フィールドをオフにします。
（注） デフォルトでは、ルータ ID がループバック アドレスとして使用されます。これらが異なるようにする場合は、[Use Router ID as Loopback Address] チェックボックスをオフにします。
f) [Loopback Addresses] を展開し、[IP] フィールドに IP アドレスを入力します。[Update] をクリックし、[OK] をクリックします。
希望する IPv4 または IPv6 の IP アドレスを入力します。
g) [Nodes] フィールドで、[+] アイコンを展開して [Select Node] ダイアログボックスを表示します。
（注） 2 つ目のノード ID を追加します。
h) [Node ID] フィールドで、ドロップダウン リストから、次のノードを選択します（leaf2）。
i) [Router ID] フィールドに、一意のルータ ID を入力します。
j) [Use Router ID as Loopback Address] フィールドをオフにします。
（注） デフォルトでは、ルータ ID がループバック アドレスとして使用されます。これらが異なるようにする場合は、[Use Router ID as Loopback Address] チェックボックスをオフにします。
k) [Loopback Addresses] を展開し、[IP] フィールドに IP アドレスを入力します。[Update] をクリックし、[OK] をクリックします。[OK] をクリックします。
希望する IPv4 または IPv6 の IP アドレスを入力します。

ステップ 6 [Create Node Profile] ダイアログボックスで、[OSPF Interface Profiles] 領域の [+] アイコンをクリックします。

ステップ 7 [Create Interface Profile] ダイアログボックスで、次のタスクを実行します。

a) [Name] フィールドに、プロファイルの名前（portProf）を入力します。
b) [Interfaces] 領域で、[Routed Interfaces] タブをクリックし、[+] アイコンをクリックします。
c) [Select Routed Interfaces] ダイアログボックスの [Path] フィールドで、ドロップダウン リストから、最初のポート（leaf1、ポート 1/40）を選択します。
d) [IP Address] フィールドに、IP アドレスとマスクを入力します。[OK] をクリックします。

e) [Interfaces] 領域で、[Routed Interfaces] タブをクリックし、[+] アイコンをクリックします。
f) [Select Routed Interfaces] ダイアログボックスの [Path] フィールドで、ドロップダウン リストから、2 つ目のポート（leaf2、ポート 1/40）を選択します。
g) [IP Address] フィールドに、IP アドレスとマスクを入力します。[OK] をクリックします。
（注） この IP アドレスは、前に leaf1 に入力した IP アドレスと異なっている必要があります。
h) [Create Interface Profile] ダイアログボックスで、[OK] をクリックします。

インターフェイスが OSPF インターフェイスとともに設定されます。

ステップ 8 [Create Node Profile] ダイアログボックスで、[OK] をクリックします。

ステップ 9 [Create Routed Outside] ダイアログボックスで、[Next] をクリックします。
[Step 2 External EPG Networks] 領域が表示されます。

ステップ 10 [External EPG Networks] 領域で、[+] アイコンをクリックします。

ステップ 11 [Create External Network] 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、外部ネットワークの名前（extMgmt）を入力します。
b) [Subnet] を展開し、[Create Subnet] ダイアログボックスの [IP address] フィールドに、サブネットの IP アドレスとマスクを入力します。
c) [Scope] フィールドで、目的のチェックボックスをオンにします。[OK] をクリックします。
d) [Create External Network] ダイアログボックスで、[OK] をクリックします。
e) [Create Routed Outside] ダイアログボックスで、[Finish] をクリックします。
（注） [Work] ペインで、[External Routed Networks] 領域に、外部ルーテッド ネットワークのアイコン（RtdOut）が表示されるようになりました。

REST API を使用した MP-BGP ルート リフレクタの設定

ステップ 1 スパイン スイッチをルート リフレクタとしてマークします。

例：

```
POST URL: https://apic-ip/api/policymgr/mo/uni/fabric.xml

<bgpInstPol name="default">
  <bgpAsP asn="1" />
  <bgpRRP>
     <bgpRRNodePEp id="<spine_id1>"/>
     <bgpRRNodePEp id="<spine_id2>"/>
  </bgpRRP>
</bgpInstPol>
```

ステップ 2 次のポストを使用してポッド セレクタをセットアップします。

例：

FuncP セットアップの場合：

```
POST URL:
https://APIC-IP/api/policymgr/mo/uni.xml

<fabricFuncP>
  <fabricPodPGrp name="bgpRRPodGrp”>
    <fabricRsPodPGrpBGPRRP tnBgpInstPolName="default" />
  </fabricPodPGrp>
</fabricFuncP>
```

例：
PodP セットアップの場合：

```
POST URL:
https://APIC-IP/api/policymgr/mo/uni.xml

<fabricPodP name="default">
  <fabricPodS name="default" type="ALL">
    <fabricRsPodPGrp tDn="uni/fabric/funcprof/podpgrp-bgpRRPodGrp"/>
  </fabricPodS>
</fabricPodP>
```

MP-BGP ルート リフレクタ設定の確認

ステップ 1 次の操作を実行して、設定を確認します。

a) セキュア シェル（SSH）を使用して、必要に応じて各リーフ スイッチへの管理者としてログインします。

b) **show processes | grep bgp** コマンドを入力して、状態が S であることを確認します。
状態が NR（実行していない）である場合は、設定が正常に行われませんでした。

ステップ 2 次の操作を実行して、自律システム番号がスパイン スイッチで設定されていることを確認します。

a) SSH を使用して、必要に応じて各スパイン スイッチへの管理者としてログインします。

b) シェル ウィンドウから次のコマンドを実行します。

例：
cd /mit/sys/bgp/inst

例：
grep asn summary

設定した自律システム番号が表示される必要があります。自律システム番号の値が 0 と表示される場合は、設定が正常に行われませんでした。

テナント、VRF、およびブリッジ ドメインの作成

テナントの概要

- テナントには、承認されたユーザのドメインベースのアクセス コントロールをイネーブルにするポリシーが含まれます。承認されたユーザは、テナント管理やネットワーキング管理などの権限にアクセスできます。
- ユーザは、ドメイン内のポリシーにアクセスしたりポリシーを設定するには読み取り/書き込み権限が必要です。テナント ユーザは、1 つ以上のドメインに特定の権限を持つことができます。
- マルチテナント環境では、リソースがそれぞれ分離されるように、テナントによりグループ ユーザのアクセス権限が提供されます（エンドポイント グループやネットワーキングなどのため）。これらの権限では、異なるユーザが異なるテナントを管理することもできます。

テナントの作成

テナントには、最初にテナントを作成した後に作成できるフィルタ、契約、ブリッジ ドメイン、およびアプリケーション プロファイルなどのプライマリ要素が含まれます。

VRF およびブリッジ ドメイン

テナントの VRF およびブリッジ ドメインを作成および指定できます。定義されたブリッジ ドメイン要素のサブネットは、対応するレイヤ 3 コンテキストを参照します。

IPv6 ネイバー探索の有効化の詳細については、関連 KB 記事、「*KB: Creating a Tenant, VRF, and Bridge Domain with IPv6 Neighbor Discovery*」を参照してください。

拡張 GUI を使用したテナント、VRF、およびブリッジ ドメインの作成

- このタスク例のビデオを視聴するには、ビデオを掲載している Web ページ を参照してください。
- 外部ルーテッドを設定するときにパブリック サブネットがある場合は、ブリッジ ドメインを外部設定と関連付ける必要があります。

手順の概要

1. メニュー バーで、[TENANT] > [Add Tenant] の順にクリックします。
2. [Create Tenant] ダイアログボックスで、次のタスクを実行します。
3. [Navigation] ペインで、[Tenant-name] > [Networking] の順に展開し、[Work] ペインで、[VRF] アイコンをキャンバスにドラッグして [Create VRF] ダイアログボックスを開き、次のタスクを実行します。
4. [Networking] ペインで、[BD] アイコンを [VRF] アイコンにつなげながらキャンバスにドラッグします。[Create Bridge Domain] ダイアログボックスが表示されたら、次のタスクを実行します。
5. [Networks] ペインで、[L3] アイコンを [VRF] アイコンにつなげながらキャンバスにドラッグします。[Create Routed Outside] ダイアログボックスが表示されたら、次のタスクを実行します。

手順の詳細

ステップ 1 メニュー バーで、[TENANT] > [Add Tenant] の順にクリックします。

ステップ 2 [Create Tenant] ダイアログボックスで、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。
b) [Security Domains +] アイコンをクリックして [Create Security Domain] ダイアログボックスを開きます。
c) [Name] フィールドに、セキュリティ ドメインの名前を入力します。[Submit] をクリックします。
d) [Create Tenant] ダイアログボックスで、作成したセキュリティ ドメインのチェックボックスをオンにし、[Submit] をクリックします。

ステップ 3 [Navigation] ペインで、[Tenant-name] > [Networking] の順に展開し、[Work] ペインで、[VRF] アイコンをキャンバスにドラッグして [Create VRF] ダイアログボックスを開き、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。
b) [Submit] をクリックして VRF の設定を完了します。

ステップ 4 [Networking] ペインで、[BD] アイコンを [VRF] アイコンにつなげながらキャンバスにドラッグします。[Create Bridge Domain] ダイアログボックスが表示されたら、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。
b) [L3 Configurations] タブをクリックします。
c) [Subnets] を展開して [Create Subnet] ダイアログボックスを開き、[Gateway IP] フィールドにサブネット マスクを入力し、[OK] をクリックします。
d) [Submit] をクリックしてブリッジ ドメインの設定を完了します。

ステップ 5 [Networks] ペインで、[L3] アイコンを [VRF] アイコンにつなげながらキャンバスにドラッグします。[Create Routed Outside] ダイアログボックスが表示されたら、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。
b) [Nodes And Interfaces Protocol Profiles] を展開して [Create Node Profile] ダイアログボックスを開きます。
c) [Name] フィールドに、名前を入力します。
d) [Nodes] を展開して [Select Node] ダイアログボックスを開きます。

e) [Node ID] フィールドで、ドロップダウン リストからノードを選択します。
f) [Router ID] フィールドに、ルータ ID を入力します。
g) [Static Routes] を展開して [Create Static Route] ダイアログボックスを開きます。
h) [Prefix] フィールドに、IPv4 アドレスまたは IPv6 アドレスを入力します。
i) [Next Hop Addresses] を展開し、[Next Hop IP] フィールドに IPv4 アドレスまたは IPv6 アドレスを入力します。
j) [Preference] フィールドに数値を入力し、[UPDATE] をクリックしてから [OK] をクリックします。
k) [Select Node] ダイアログボックスで、[OK] をクリックします。
l) [Create Node Profile] ダイアログボックスで、[OK] をクリックします。
m) 必要に応じてチェックボックス [BGP]、[OSPF]、または [EIGRP] をオンにし、[NEXT] をクリックします。[OK] をクリックしてレイヤ 3 の設定を完了します。

L3 設定を確認するには、[Navigation] ペインで、[Networking] > [VRFs] の順に展開します。

アプリケーション ポリシーの展開

セキュリティ ポリシーの適用

トラフィックは前面パネルのインターフェイスからリーフ スイッチに入り、パケットは送信元 EPG の EPG でマーキングされます。リーフ スイッチはその後、テナント エリア内のパケットの宛先IPアドレスでフォワーディングルックアップを実行します。ヒットすると、次のシナリオのいずれかが発生する可能性があります。

1. ユニキャスト（/32）ヒットでは、宛先エンドポイントの EPG と宛先エンドポイントが存在するローカル インターフェイスまたはリモート リーフ スイッチの VTEP IP アドレスが提供されます。
2. サブネット プレフィクス（/32 以外）のユニキャスト ヒットでは、宛先サブネット プレフィクスの EPG と宛先サブネット プレフィクスが存在するローカル インターフェイスまたはリモート リーフ スイッチの VTEP IP アドレスが提供されます。
3. マルチキャスト ヒットでは、ファブリック全体の VXLAN カプセル化とマルチキャスト グループの EPG で使用するローカル レシーバのローカル インターフェイスと外側の宛先 IP アドレスが提供されます。

（注） マルチキャストと外部ルータのサブネットは、入力リーフ スイッチでのヒットを常にもたらします。セキュリティ ポリシーの適用は、宛先 EPG が入力リーフ スイッチによって認識されるとすぐに発生します。

転送テーブルの誤りにより、パケットがスパイン スイッチの転送プロキシに送信されます。転送プロキシはその後、転送テーブル検索を実行します。これが誤りである場合、パケットはドロップされます。これがヒットの場合、パケットは宛先エンドポイントを含む出力リーフ スイッチに送信されます。出力リーフ スイッチが宛先の EPG を認識するため、セキュリティ ポリシーの適用が実行されます。出力リーフ スイッチは、パケット送信元の EPG を認識する必要があります。ファブリック ヘッダーは、入力リーフ スイッチから出力リーフ スイッチに EPG を伝送するため、このプロセスをイネーブルにします。スパイン スイッチは、転送プロキシ機能を実行するときに、パケット内の元の EPG を保存します。

出力リーフ スイッチでは、送信元 IP アドレス、送信元 VTEP、および送信元 EPG 情報は、学習によってローカルの転送テーブルに保存されます。ほとんどのフローが双方向であるため、応答パケットがフローの両側で転送テーブルに入力し、トラフィックが両方向で入力フィルタリングされます。

セキュリティ ポリシー仕様を含むコントラクト

ACI セキュリティ モデルでは、コントラクトに EPG 間の通信を管理するポリシーが含まれます。コントラクトは通信内容を指定し、EPG は通信の送信元と宛先を指定します。コントラクトは次のように EPG をリンクします。

EPG 1 ---------- コントラクト ---------- EPG 2

コントラクトで許可されていれば、EPG 1 のエンドポイントは EPG 2 のエンドポイントと通信でき、またその逆も可能です。このポリシーの構造には非常に柔軟性があります。たとえば、EPG 1 と EPG 2 間には多くのコントラクトが存在でき、1 つのコントラクトを使用する EPG が 3 つ以上存在でき、コントラクトは複数の EPG のセットで再利用できます。

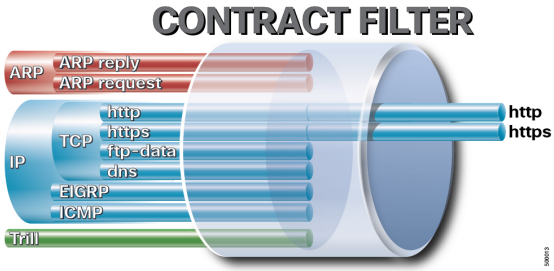
また EPG とコントラクトの関係には方向性があります。EPG はコントラクトを提供または消費できます。コントラクトを提供する EPG は通常、一連のクライアントデバイスにサービスを提供する一連のエンドポイントです。そのサービスによって使用されるプロトコルはコントラクトで定義されます。コントラクトを消費する EPG は通常、そのサービスのクライアントである一連のエンドポイントです。クライアントエンドポイント（コンシューマ）がサーバエンドポイント（プロバイダー）に接続しようとすると、コントラクトはその接続が許可されるかどうかを確認します。特に指定のない限り、そのコントラクトは、サーバがクライアントへの接続を開始することを許可しません。ただし、EPG 間の別のコントラクトが、その方向の接続を簡単に許可する場合があります。

この提供/消費の関係は通常、EPG とコントラクト間を矢印を使って図で表されます。次に示す矢印の方向に注目してください。

EPG 1 <------- 消費 -------- コントラクト <------- 提供 -------- EPG 2

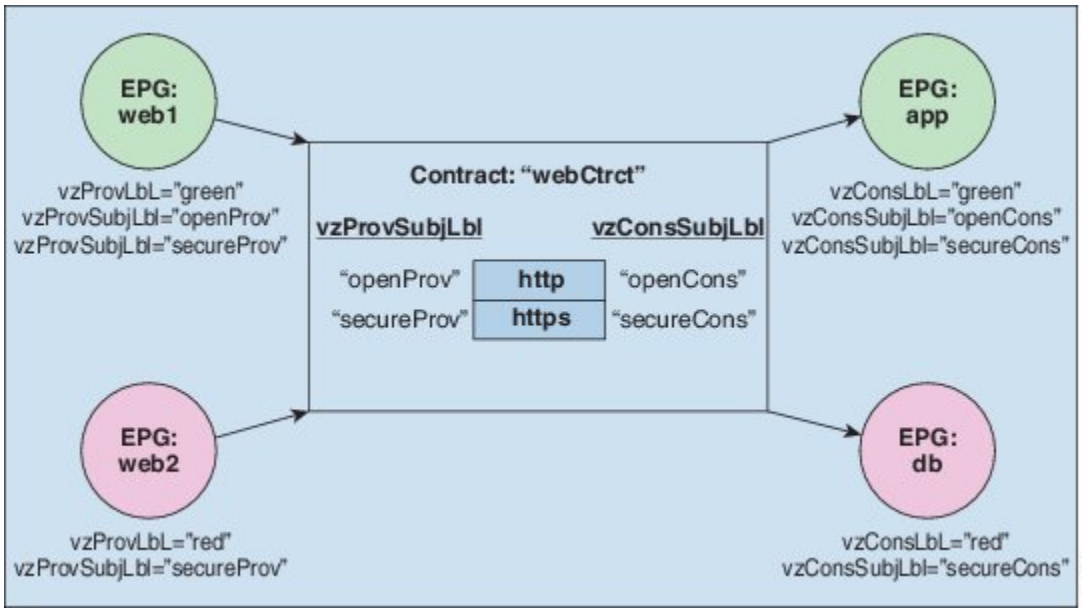
コントラクトは階層的に構築されます。1 つ以上のサブジェクトで構成され、各サブジェクトには 1 つ以上のフィルタが含まれ、各フィルタは 1 つ以上のプロトコルを定義できます。

図 *25*：コントラクト フィルタ



次の図は、コントラクトが EPG の通信をどのように管理するかを示します。

図 *26*： *EPG/EPG* 通信を決定するコントラクト



たとえば、TCP ポート 80 とポート 8080 を指定する HTTP と呼ばれるフィルタと、TCP ポート 443 を指定する HTTPS と呼ばれる別のフィルタを定義できます。その後、2 セットのサブジェクトを持つ webCtrct と呼ばれるコントラクトを作成できます。openProv と openCons are は HTTP フィルタが含まれるサブジェクトです。secureProv と secureCons は HTTPS フィルタが含まれるサブジェクトです。この webCtrct コントラクトは、Web サービスを提供する EPG とそのサービスを消費するエンドポイントを含む EPG 間のセキュアな Web トラフィックと非セキュアな Web トラフィックの両方を可能にするために使用できます。

これらの同じ構造は、仮想マシンのハイパーバイザを管理するポリシーにも適用されます。EPG が Virtual Machine Manager（VMM）のドメイン内に配置されると、APIC は EPG に関連付けられたすべてのポリシーを VMM ドメインに接続するインターフェイスを持つリーフ スイッチにダウ

ンロードします。VMM ドメインの完全な説明については、『ACI の基本』マニュアルの「Virtual Machine Manager のドメイン」の章を参照してください。このポリシーが作成されると、APIC は EPG のエンドポイントへの接続を可能にするスイッチを指定する VMM ドメインにそれをプッシュ（あらかじめ入力）します。VMM ドメインは、EPG 内のエンドポイントが接続できるスイッチとポートのセットを定義します。エンドポイントがオンラインになると、適切な EPG に関連付けられます。パケットが送信されると、送信元 EPG および宛先 EPG がパケットから取得され、対応するコントラクトで定義されたポリシーでパケットが許可されたかどうかが確認されます。許可された場合は、パケットが転送されます。許可されない場合は、パケットはドロップされます。

コントラクトは、許可や拒否よりも複雑なアクションも許可します。コントラクトは、所定のサブジェクトに一致するトラフィックをサービスにリダイレクトしたり、コピーしたり、その QoS レベルを変更したりできることを指定可能です。具象モデルでアクセス ポリシーをあらかじめ入力すると、APIC がオフラインまたはアクセスできない場合でも、エンドポイントは移動でき、新しいエンドポイントをオンラインにでき、通信を行うことができます。APIC は、ネットワークの単一の障害発生時点から除外されます。ACI ファブリックにパケットが入力されると同時に、セキュリティ ポリシーがスイッチで実行している具象モデルによって適用されます。

Three-Tier アプリケーションの展開

フィルタは、フィルタを含む契約により許可または拒否されるデータ プロトコルを指定します。契約には、複数のサブジェクトを含めることができます。サブジェクトは、単方向または双方向のフィルタを実現するために使用できます。単方向フィルタは、コンシューマからプロバイダー（IN）のフィルタまたはプロバイダーからコンシューマ（OUT）のフィルタのどちらか一方向に使用されるフィルタです。双方向フィルタは、両方の方向で使用される同一フィルタです。これは、再帰的ではありません。

契約は、エンドポイント グループ間（EPG 間）の通信をイネーブルにするポリシーです。これらのポリシーは、アプリケーション層間の通信を指定するルールです。契約が EPG に付属していない場合、EPG 間の通信はデフォルトでディセーブルになります。EPG 内の通信は常に許可されているので、EPG 内の通信には契約は必要ありません。

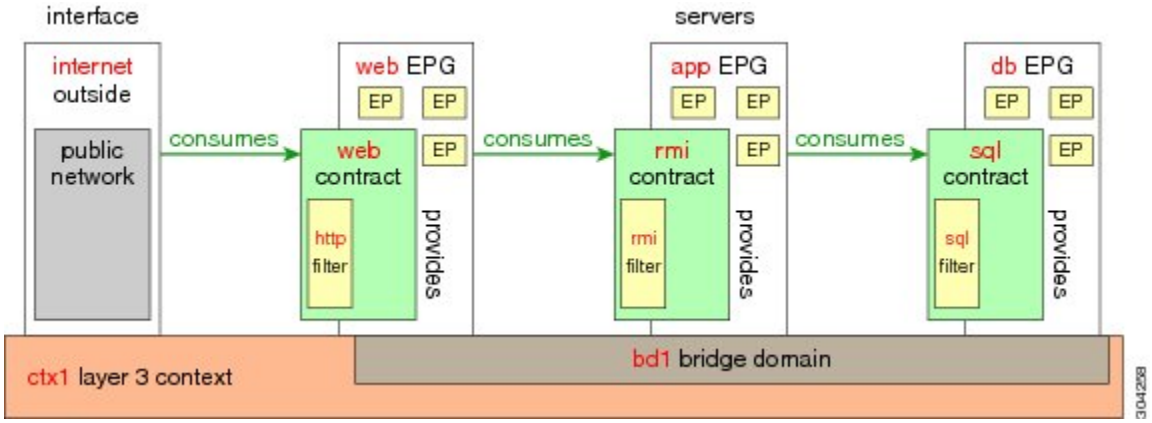
アプリケーション プロファイルでは、APIC がその後ネットワークおよびデータセンターのインフラストラクチャで自動的にレンダリングするアプリケーション要件をモデル化することができます。アプリケーション プロファイルでは、管理者がインフラストラクチャの構成要素ではなくアプリケーションの観点から、リソース プールにアプローチすることができます。アプリケーション プロファイルは、互いに論理的に関連する EPG を保持するコンテナです。EPG は同じアプリケーション プロファイル内の他の EPG および他のアプリケーション プロファイル内の EPG と通信できます。

アプリケーションポリシーを展開するには、必要なアプリケーションプロファイル、フィルタ、および契約を作成する必要があります。通常、APIC ファブリックは、テナント ネットワーク内の Three-Tier アプリケーションをホストします。この例では、アプリケーションは 3 台のサーバ（Web サーバ、アプリケーション サーバ、およびデータベース サーバ）を使用して実行されます。Three-Tier アプリケーションの例については、次の図を参照してください。

Web サーバには HTTP フィルタがあり、アプリケーション サーバには Remote Method Invocation（RMI）フィルタがあり、データベース サーバには Structured Query Language（SQL）フィルタが

あります。アプリケーション サーバは、SQL 契約を消費してデータベース サーバと通信します。Web サーバは、RMI 契約を消費して、アプリケーション サーバと通信します。トラフィックは Web サーバから入り、アプリケーション サーバと通信します。アプリケーション サーバはその後、データベース サーバと通信し、トラフィックは外部に通信することもできます。

図 *27*：*Three-Tier* アプリケーションの図



http 用のフィルタを作成するパラメータ

この例での http 用のフィルタを作成するパラメータは次のとおりです。

パラメータ名	http のフィルタ
名前	http
エントリの数	2
エントリ名	Dport-80 Dport-443
Ethertype	IP
プロトコル	tcp tcp
宛先ポート	http https

rmi および sql 用のフィルタを作成するパラメータ

この例での rmi および sql 用のフィルタを作成するパラメータは次のとおりです。

パラメータ名	rmi のフィルタ	sql のフィルタ
名前	rmi	sql
エントリの数	1	1
エントリ名	Dport-1099	Dport-1521
Ethertype	IP	IP
プロトコル	tcp	tcp
宛先ポート	1099	1521

アプリケーション プロファイル データベースの例

この例のアプリケーション プロファイル データベースは次のとおりです。

EPG	提供される契約	消費される契約
Web	Web	rmi
app	rmi	sql
db	sql	--

GUI を使用したアプリケーション ポリシーの展開

GUI を使用したフィルタの作成

3 つの個別のフィルタを作成します。この例では、HTTP、RMI、SQL です。このタスクでは、HTTP フィルタを作成する方法を示します。このタスクは、他のフィルタを作成するタスクと同じです。

はじめる前に

テナント、ネットワーク、およびブリッジ ドメインが作成されていることを確認します。

手順の概要

1. メニュー バーで、[TENANTS] を選択します。[Navigation] ペインで、[tenant] > [Security Policies] を展開し、[Filters] を右クリックして、[Create Filter] をクリックします。
2. [Create Filter] ダイアログボックスで、次の操作を実行します。
3. [Name] フィールドの [Entries] を展開します。同じプロセスを実行して、別のエントリを宛先ポートとして HTTPS で追加し、[Update] をクリックします。
4. さらに 2 つのフィルタ（rmi および sql）を作成し、rmi および sql 用のフィルタを作成するパラメータ，（150 ページ）に示すパラメータを使用するには、上記手順の同じプロセスを実行します。

手順の詳細

ステップ 1 メニュー バーで、[TENANTS] を選択します。[Navigation] ペインで、[tenant] > [Security Policies] を展開し、[Filters] を右クリックして、[Create Filter] をクリックします。

（注） [Navigation] ペインで、フィルタを追加するテナントを展開します。

ステップ 2 [Create Filter] 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、フィルタ名（http）を入力します。
b) [Entries] を展開し、[Name] フィールドに、名前（Dport-80）を入力します。
c) [EtherType] ドロップダウン リストから、EtherType（IP）を選択します。
d) [IP Protocol] ドロップダウン リストから、プロトコル（tcp）を選択します。
e) [Destination Port/Range] ドロップダウン リストから、[From] フィールドと [To] フィールドで、[http] を選択します。（http）
f) [Update] をクリックし、[Submit] をクリックします。
新しく追加されたフィルタが、[Navigation] ペインと [Work] ペインに表示されます。

ステップ 3 [Name] フィールドの [Entries] を展開します。同じプロセスを実行して、別のエントリを宛先ポートとして HTTPS で追加し、[Update] をクリックします。
この新しいフィルタ ルールが追加されます。

ステップ 4 さらに 2 つのフィルタ（rmi および sql）を作成し、rmi および sql 用のフィルタを作成するパラメータ，（150 ページ）に示すパラメータを使用するには、上記手順の同じプロセスを実行します。

GUI を使用した契約の作成

手順の概要

1. メニュー バーで、[TENANTS] と実行するテナント名を選択します。[Navigation] ペインで、[tenant] > [Security Policies] を展開します。
2. [Contracts] > [Create Contract] を右クリックします。
3. [Create Contract] ダイアログボックスで、次のタスクを実行します。
4. [Create Contract Subject] ダイアログボックスで、[OK] をクリックします。
5. この手順と同じステップに従って、rmi と sql 用の契約をさらに 2 つ作成します。rmi 契約の場合は rmi サブジェクトを選択し、sql の場合は sql サブジェクトを選択します。

手順の詳細

ステップ 1 メニュー バーで、[TENANTS] と実行するテナント名を選択します。[Navigation] ペインで、[tenant] > [Security Policies] を展開します。

ステップ 2 [Contracts] > [Create Contract] を右クリックします。

ステップ 3 [Create Contract] ダイアログボックスで、次のタスクを実行します。

a) [Name] フィールドに、契約名（web）を入力します。

b) [Subjects] の横の [+] 記号をクリックし、新しいサブジェクトを追加します。

c) [Create Contract Subject] ダイアログボックスで、[Name] フィールドにサブジェクト名を入力します。（web）

d) （注） この手順では、契約のサブジェクトで前に作成されたフィルタを関連付けます。

[Filter Chain] 領域で、[Filters] の横の [+] 記号をクリックします。

e) ダイアログボックスで、ドロップダウンメニューから、フィルタ名（http）を選択し、[Update] をクリックします。

ステップ 4 [Create Contract Subject] ダイアログボックスで、[OK] をクリックします。

ステップ 5 この手順と同じステップに従って、rmi と sql 用の契約をさらに 2 つ作成します。rmi 契約の場合は rmi サブジェクトを選択し、sql の場合は sql サブジェクトを選択します。

GUI を使用したアプリケーション プロファイルの作成

手順の概要

1. メニュー バーで、[TENANTS] を選択します。[Navigation] ペインで、テナントを展開し、[Application Profiles] を右クリックし、[Create Application Profile] をクリックします。
2. [Create Application Profile] ダイアログボックスで、[Name] フィールドに、アプリケーション プロファイル名（OnlineStore）を追加します。

手順の詳細

ステップ 1 メニュー バーで、[TENANTS] を選択します。[Navigation] ペインで、テナントを展開し、[Application Profiles] を右クリックし、[Create Application Profile] をクリックします。

ステップ 2 [Create Application Profile] ダイアログボックスで、[Name] フィールドに、アプリケーション プロファイル名（OnlineStore）を追加します。

GUI を使用した EPG の作成

EPG が使用するポートは、VM マネージャ（VMM）ドメインまたは EPG に関連付けられた物理ドメインのいずれか 1 つに属している必要があります。

手順の概要

1. [EPGs] を展開します。[Create Application EPG] ダイアログボックスで、次の操作を実行します。
2. [Create Application Profile] ダイアログボックスで、EPG をさらに 2 つ作成します。3 つの EPG は、同じブリッジ ドメインおよびデータセンター内の db、app、および web である必要があります。

手順の詳細

ステップ 1 [EPGs] を展開します。[Create Application EPG] 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、EPG の名前（db）を追加します。
b) [Bridge Domain] フィールドで、ドロップダウン リストからブリッジ ドメイン（bd1）を選択します。
c) [Associate to VM Domain Profiles] チェックボックスをオンにします。[Next] をクリックします。

d) [Step 2 for Specify the VM Domains] 領域で、[Associate VM Domain Profiles] を展開し、ドロップダウン リストから目的の VMM ドメインを選択します。[Update] をクリックし、[OK] をクリックします。

ステップ 2 [Create Application Profile] ダイアログボックスで、EPG をさらに 2 つ作成します。3 つの EPG は、同じブリッジ ドメインおよびデータセンター内の db、app、および web である必要があります。

GUI を使用した契約の消費と提供

EPG 間のポリシー関係を作成するために、前に作成した契約を関連付けることができます。

提供するコントラクトと使用するコントラクトに名前を付けるときは、提供するコントラクトと使用するコントラクトの両方に同じ名前を付けてください。

手順の概要

1. APIC GUI ウィンドウをクリックして db EPG から app EPG にドラッグします。
2. [Name] フィールドで、ドロップダウン リストから、sql 契約を選択します。[OK] をクリックします。
3. APIC GUI 画面 をクリックして、app ePG から web EPG にドラッグします。
4. [Name] フィールドで、ドロップダウン リストから、rmi 契約を選択します。[OK] をクリックします。
5. web EPG のアイコンをクリックし、[Provided Contracts] 領域の [+] 記号をクリックします。
6. [Name] フィールドで、ドロップダウン リストから、web 契約を選択します。[OK] をクリックします。[Submit] をクリックします。
7. 確認するには、[Navigation] ペインで、[Application Profiles] 下の [OnlineStore] に移動してクリックします。
8. [Work] ペインで、[Operational] > [Contracts] を選択します。

手順の詳細

ステップ 1 （注） db、app、および web EPG は、アイコンで表示されます。
APIC GUI ウィンドウをクリックして db EPG から app EPG にドラッグします。
[Add Consumed Contract] ダイアログボックスが表示されます。

ステップ 2 [Name] フィールドで、ドロップダウン リストから、sql 契約を選択します。[OK] をクリックします。
この手順により、db EPG は sql 契約を提供でき、app EPG は sql 契約を消費することができます。

ステップ 3 APIC GUI 画面 をクリックして、app ePG から web EPG にドラッグします。
[Add Consumed Contract] ダイアログボックスが表示されます。

ステップ 4 [Name] フィールドで、ドロップダウン リストから、rmi 契約を選択します。[OK] をクリックします。

この手順により、app EPG は rmi 契約を提供でき、web EPG は rmi 契約を消費することができます。

ステップ 5 web EPG のアイコンをクリックし、[Provided Contracts] 領域の [+] 記号をクリックします。
[Add Provided Contract] ダイアログボックスが表示されます。

ステップ 6 [Name] フィールドで、ドロップダウン リストから、web 契約を選択します。[OK] をクリックします。
[Submit] をクリックします。
OnlineStore と呼ばれる 3 層アプリケーション プロファイルが作成されました。

ステップ 7 確認するには、[Navigation] ペインで、[Application Profiles] 下の [OnlineStore] に移動してクリックします。
[Work] ペインで、3 つの EPG app、db および web が表示されていることを確認できます。

ステップ 8 [Work] ペインで、[Operational] > [Contracts] を選択します。
消費/提供される順番で表示された EPG と契約を確認できます。

特定のポートへの EPG の静的な導入

このトピックでは、Cisco APIC を使用しているときに特定のポートに EPG を静的に導入する方法の典型的な例を示します。

GUI を使用した APIC の特定のポートへの EPG の導入

はじめる前に

EPG を導入するテナントがすでに作成されていること。

ステップ 1 メニュー バーで、[TENANTS] をクリックします。

ステップ 2 [with APIC] ペインで、*[Tenant_name]* > [Application Profiles] の順に適切に展開します。

ステップ 3 [Application Profiles] を右クリックし、[Create Application Profile] をクリックします。

ステップ 4 [Create Application Profile] 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、アプリケーション プロファイルの名前を入力します。

b) [EPGs] を展開します。

c) [Create Application EPG] ダイアログボックスで、[Name] フィールドに、EPG 名を入力します。

d) [Statically Link with Leaves/Paths] フィールドで、[Statically Link with Leaves/Paths] のチェックボックスをオンにします（これは、EPG を導入する必要があるポートを指定するために選択します）。[Next] をクリックします。

e) [Leaves/Paths] 領域で、[Paths] を展開します。
この例では、EPGをノードのポートに導入します。または、EPGをノードに導入することもできます。

f) [Path] ドロップダウン リストから、適切なノードおよびポートを選択します。

g) [Encap] フィールドに、導入先の VLAN を入力します。

h) [Deployment Immediacy] フィールドのドロップダウン リストで、希望する導入時間を選択します。
i) [Mode] フィールドで、適切なモードを選択します。
j) [OK] をクリックし、[Submit] をクリックします。

ステップ 5 [Navigation] ペインで、[Application Profiles] を展開して、新しいアプリケーション プロファイルを表示します。

ステップ 6 [Application EPGs] を展開して、新しい EPG を表示します。

ステップ 7 EPG を展開して [Static Bindings (Paths)] をクリックし、[Work] ペインで、確立されたスタティック バインディング パスの詳細を表示します。

REST API を使用した APIC の特定のポートへの EPG の導入

はじめる前に

EPG を導入するテナントが作成されていること。

特定のポート上に EPG を導入します。

例：

```
<fvTenant name="<tenant_name>" dn="uni/tn-test1" >
    <fvCtx name="<network_name>" pcEnfPref="enforced" knwMcastAct="permit"/>
    <fvBD name="<bridge_domain_name>" unkMcastAct="flood" >
        <fvRsCtx tnFvCtxName="<network_name>"/>
    </fvBD>
    <fvAp name="<application_profile>" >
        <fvAEPg name="<epg_name>" >
            <fvRsPathAtt tDn="topology/pod-1/paths-1017/pathep-[eth1/13]" mode="regular"
instrImedcy="immediate" encap="vlan-20"/>
        </fvAEPg>
    </fvAp>
</fvTenant>
```

CLI を使用した APIC の特定のポートへの EPG の導入

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：

```
admin@apic1:~> cd /aci
```

ステップ 2 テナントを作成します。

例：

```
# tenant
admin@apic1:~> cd '/aci/tenants'
admin@apic1:tenants> mocreate 'test1'
admin@apic1:tenants> moconfig commit
```

ステップ 3 ブリッジ ドメインを作成します。

例：

```
# bridge-domain
admin@apic1:tenants> cd '/aci/tenants/test1/networking/bridge-domains'
admin@apic1:bridge-domains> mocreate 'bd1'
admin@apic1:bridge-domains> cd 'bd1'
admin@apic1:bd1> moset network 'ctx1'
admin@apic1:bd1> moconfig commit
```

ステップ 4 プライベート ネットワークを作成します。

例：

```
# private-network
admin@apic1:bd1> cd '/aci/tenants/test1/networking/private-networks'
admin@apic1:private-networks> mocreate 'ctx1'
admin@apic1:private-networks> moconfig commit
```

ステップ 5 アプリケーション プロファイルを作成します。

例：

```
# application-profile
admin@apic1:private-networks> cd '/aci/tenants/test1/application-profiles'
admin@apic1:application-profiles> mocreate 'AP1'
admin@apic1:application-profiles> moconfig commit
```

ステップ 6 アプリケーション EPG を作成します。

例：

```
# application-epg
admin@apic1:application-profiles> cd '/aci/tenants/test1/application-profiles/AP1/application-epgs'
admin@apic1:application-epgs> mocreate 'EPG1'
admin@apic1:application-epgs> moconfig commit
```

ステップ 7 EPG を特定のポートに関連付けます。

例：

```
# fv-rspathatt
admin@apic1:application-epgs> cd
'/aci/tenants/test1/application-profiles/AP1/application-epgs/EPG1/static-bindings-paths'
admin@apic1:static-bindings-paths> mocreate 'topology/pod-1/paths-1017/pathep-[eth1/13]'
admin@apic1:static-bindings-paths> cd '[topology--pod-1--paths-1017--pathep-[eth1--13]]'
admin@apic1:[topology--pod-1--paths-1017--pathep-[eth1--13]]> moset encap 'vlan-20'
admin@apic1:[topology--pod-1--paths-1017--pathep-[eth1--13]]> moset deployment-immediacy 'immediate'
admin@apic1:[topology--pod-1--paths-1017--pathep-[eth1--13]]> moconfig commit
```

特定のポートに EPG を導入するためのドメイン、接続エンティティ プロファイル、および VLAN の作成

このトピックでは、特定のポートに EPG を導入する場合に必須である物理ドメイン、接続エンティティ プロファイル（AEP）、および VLAN を作成する方法の典型的な例を示します。

（注） すべてのエンドポイント グループ（EPG）にドメインが必要です。また、インターフェイス ポリシー グループを接続エンティティ プロファイル（AEP）に関連付ける必要があり、AEP と EPG が同じドメインに存在する必要がある場合は、AEP をドメインに関連付ける必要があります。EPG とドメイン、およびインターフェイス ポリシー グループとドメインの関連付けに基づいて、EPG が使用するポートと VLAN が検証されます。以下のドメイン タイプが EPG に関連付けられます。

- アプリケーション EPG
- レイヤ 3 Outside 外部ネットワーク インスタンス EPG
- レイヤ 2 Outside 外部ネットワーク インスタンス EPG
- アウトオブバンドおよびインバンド アクセスの管理 EPG

GUI を使用した、EPG を特定のポートに導入するためのドメインおよび VLAN の作成

はじめる前に

- EPG を導入するテナントがすでに作成されていること。
- EPG は特定のポートに静的に導入されます。

ステップ 1 メニュー バーで、[FABRIC] > [Access Policies] をクリックします。

ステップ 2 [Navigation] ペインで、[Quick Start] をクリックします。

ステップ 3 [Work] ペインで、[Configure an interface, PC, and vPC] をクリックします。

ステップ 4 [Configure Interface, PC, and vPC] ダイアログボックスで、[+] アイコンをクリックしてスイッチを選択し、次の操作を実行します。

a) [Switches] ドロップダウン リストで、目的のスイッチのチェックボックスをオンにします。

b) [Switch Profile Name] フィールドに、スイッチ名が自動的に入力されます。

（注） 任意で、変更した名前を入力することができます。

c) スイッチ インターフェイスを設定するために [+] アイコンをクリックします。
d) [Interface Type] フィールドで、[Individual] オプション ボタンをクリックします。
e) [Interfaces] フィールドに、目的のインターフェイスの範囲を入力します。
f) [Interface Selector Name] フィールドに、インターフェイス名が自動的に入力されます。
（注） 任意で、変更した名前を入力することができます。
g) [Interface Policy Group] フィールドで、[Create One] オプション ボタンを選択します。
h) [Link Level Policy] ドロップダウン リストで、適切なリンク レベル ポリシーを選択します。
（注） 必要に応じて追加のポリシーを作成します。または、デフォルトのポリシー設定を使用できます。
i) [Attached Device Type] フィールドから、適切なデバイス タイプを選択します。
j) [Domain] フィールドで、[Create One] オプション ボタンをクリックします。
k) [Domain Name] フィールドに、ドメイン名を入力します。
l) [VLAN] フィールドで、[Create One] オプション ボタンをクリックします。
m) [VLAN Range] フィールドに、目的の VLAN 範囲を入力します。[Save] をクリックし、[Save] をもう一度クリックします。
n) [Submit] をクリックします。

ステップ 5 メニュー バーで、[TENANTS] をクリックします。[Navigation] ペインで、*[Tenant_name]* > [Application Profiles] > [Domains (VMs and Bare-Metals)] > *[EPG_name]* の順に適切に展開し、次の操作を実行します。

a) [Domains (VMs and Bare-Metals)] を右クリックし、[Add Physical Domain Association] をクリックします。
b) [Add Physical Domain Association] ダイアログボックスで、[Physical Domain Profile] ドロップダウン リストから、適切なドメインを選択します。
c) [Deploy Immediacy] フィールドで、目的のオプション ボタンをクリックします。
d) [Resolution Immediacy] フィールドで、目的のオプション ボタンをクリックします。[Submit] をクリックします。
AEP は、ノード上の特定のポート、およびドメインに関連付けられます。物理ドメインは VLAN プールに関連付けられ、テナントはこの物理ドメインに関連付けられます。

スイッチ プロファイルとインターフェイス プロファイルが作成されます。インターフェイス プロファイルのポート ブロックにポリシー グループが作成されます。AEP が自動的に作成され、ポート ブロックおよびドメインに関連付けられます。ドメインはVLANプールに関連付けられ、テナントはドメインに関連付けられます。

REST API を使用した、EPG を特定のポートに導入するための AEP、ドメイン、および VLAN の作成

はじめる前に

- EPG を導入するテナントがすでに作成されていること。

- EPG は特定のポートに静的に導入されます。

ステップ 1 インターフェイスプロファイル、スイッチプロファイル、および接続エンティティプロファイル（AEP）を作成します。

例：

```
   <infraInfra>

      <infraNodeP  name="<switch_profile_name>" dn="uni/infra/nprof-<switch_profile_name>" >
           <infraLeafS  name="SwitchSeletor" descr="" type="range">
                <infraNodeBlk name="nodeBlk1" descr="" to_="1019" from_="1019"/>
           </infraLeafS>
          <infraRsAccPortP tDn="uni/infra/accportprof-<interface_profile_name>"/>
      </infraNodeP>

      <infraAccPortP name="<interface_profile_name>"
dn="uni/infra/accportprof-<interface_profile_name>" >
           <infraHPortS  name="portSelector"  type="range">
              <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-<port_group_name>" fexId="101"/>

                <infraPortBlk name="block2"  toPort="13" toCard="1" fromPort="11" fromCard="1"/>
          </infraHPortS>
     </infraAccPortP>

   <infraAccPortGrp  name="<port_group_name>" dn="uni/infra/funcprof/accportgrp-<port_group_name>"
 >
          <infraRsAttEntP tDn="uni/infra/attentp-<attach_entity_profile_name>"/>
          <infraRsHIfPol tnFabricHIfPolName="1GHifPol"/>
    </infraAccPortGrp>

    <infraAttEntityP  name="<attach_entity_profile_name>"
dn="uni/infra/attentp-<attach_entity_profile_name>" >
         <infraRsDomP tDn="uni/phys-<physical_domain_name>"/>
    </infraAttEntityP>

<infraInfra>
```

ステップ 2 ドメインを作成する。

例：

```
<physDomP  name="<physical_domain_name>" dn="uni/phys-<physical_domain_name>">
    <infraRsVlanNs tDn="uni/infra/vlanns-[<vlan_pool_name>]-static"/>
</physDomP>
```

ステップ 3 VLAN 範囲を作成します。

例：

```
<fvnsVlanInstP  name="<vlan_pool_name>" dn="uni/infra/vlanns-[<vlan_pool_name>]-static"
allocMode="static">
    <fvnsEncapBlk name="" descr="" to="vlan-25" from="vlan-10"/>
</fvnsVlanInstP>
```

ステップ 4 ドメインに EPG を関連付けます。

例：

```
<fvTenant  name="<tenant_name>" dn="uni/tn-" >
    <fvAEPg prio="unspecified" name="<epg_name>" matchT="AtleastOne"
dn="uni/tn-test1/ap-AP1/epg-<epg_name>" descr="">
        <fvRsDomAtt tDn="uni/phys-<physical_domain_name>" instrImedcy="immediate"
resImedcy="immediate"/>
```

```
    </fvAEPg>
</fvTenant>
```

CLI を使用した、EPG を特定のポートに導入するための AEP、ドメイン、および VLAN の作成

はじめる前に

- EPG を導入するテナントがすでに作成されていること。
- EPG は特定のポートに静的に導入されます。

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：

```
admin@apic1:~> cd /aci
```

ステップ 2 インターフェイス プロファイルを作成します。

例：

```
# interface-profile
admin@apic1:~> cd '/aci/fabric/access-policies/interface-policies/profiles/interfaces'
admin@apic1:interfaces> mocreate 'InterfaceProfile1'
admin@apic1:interfaces> moconfig commit

# access-port-selector
admin@apic1:interfaces> cd
'/aci/fabric/access-policies/interface-policies/profiles/interfaces/InterfaceProfile1'
admin@apic1:InterfaceProfile1> mocreate 'portSelector' 'range'
admin@apic1:InterfaceProfile1> cd 'portSelector-range'
admin@apic1:portSelector-range> moset policy-group
'fabric/access-policies/interface-policies/policy-groups/interface/PortGroup'
admin@apic1:portSelector-range> moconfig commit

# access-port-block
admin@apic1:portSelector-range> cd
'/aci/fabric/access-policies/interface-policies/profiles/interfaces/InterfaceProfile1/portSelector-range'
admin@apic1:portSelector-range> mocreate 'block2'
admin@apic1:portSelector-range> cd 'block2'
admin@apic1:block2> moset from-port '11'
admin@apic1:block2> moset to-port '13'
admin@apic1:block2> moconfig commit

# access-port-policy-group
admin@apic1:block2> cd '/aci/fabric/access-policies/interface-policies/policy-groups/interface'
admin@apic1:interface> mocreate 'PortGroup'
admin@apic1:PortGroup> cd 'PortGroup'
admin@apic1:PortGroup> moset link-level-policy '1GHifPol'
admin@apic1:PortGroup> moset attached-entity-profile
'fabric/access-policies/global-policies/attachable-entity-profile/IntfAttEntityP'
admin@apic1:PortGroup> moconfig commit
```

ステップ 3 スイッチ プロファイルを作成します。

例：

```
# switch-profile
admin@apic1:PortGroup> cd '/aci/fabric/access-policies/switch-policies/profiles'
admin@apic1:profiles> mocreate 'SwitchProfile-1019'
admin@apic1:profiles> moconfig commit

# infra-rsaccportp
admin@apic1:profiles> cd
'/aci/fabric/access-policies/switch-policies/profiles/SwitchProfile-1019/associated-interface-selector-profiles'
admin@apic1:associated-interface-selector-profiles> mocreate
'fabric/access-policies/interface-policies/profiles/interfaces/InterfaceProfile1'
admin@apic1:associated-interface-selector-profiles> moconfig commit

# leaf-selector
admin@apic1:associated-interface-selector-profiles> cd
'/aci/fabric/access-policies/switch-policies/profiles/SwitchProfile-1019/switch-selectors'
admin@apic1:switch-selectors> mocreate 'SwitchSeletor' 'range'
admin@apic1:switch-selectors> moconfig commit

# node-block
admin@apic1:switch-selectors> cd
'/aci/fabric/access-policies/switch-policies/profiles/SwitchProfile-1019/switch-selectors/SwitchSeletor-range'
admin@apic1:SwitchSeletor-range> mocreate 'eeac466a56b66898'
admin@apic1:SwitchSeletor-range> cd 'eeac466a56b66898'
admin@apic1:eeac466a56b66898> moset from '1019'
admin@apic1:eeac466a56b66898> moset to '1019'
admin@apic1:eeac466a56b66898> moconfig commit
```

ステップ 4 接続エンティティ プロファイル（AEP）を作成します。

例：

```
# attachable-access-entity-profile
admin@apic1:~> cd '/aci/fabric/access-policies/global-policies/attachable-entity-profile'
admin@apic1:attachable-entity-profile> mocreate 'IntfAttEntityP'
admin@apic1:attachable-entity-profile> moconfig commit

# infra-rsdomp
admin@apic1:attachable-entity-profile> cd
'/aci/fabric/access-policies/global-policies/attachable-entity-profile/IntfAttEntityP/domains-associated-to-interfaces'
admin@apic1:domains-associated-to-interfaces> mocreate
'fabric/access-policies/physical-and-external-domains/physical-domains/domP'
admin@apic1:domains-associated-to-interfaces> moconfig commit
```

ステップ 5 ドメインを作成します。

例：

```
# physical-domain
admin@apic1:~> cd '/aci/fabric/access-policies/physical-and-external-domains/physical-domains'
admin@apic1:physical-domains> mocreate 'domP'
admin@apic1:physical-domains> cd 'domP'
admin@apic1:domP> moset vlan-pools 'fabric/access-policies/pools/vlan/vlanPool1-static-allocation'
admin@apic1:domP> moconfig commit
```

ステップ 6 VLAN プールを作成します。

例：

```
# vlan-pool
admin@apic1:~> cd '/aci/fabric/access-policies/pools/vlan'
admin@apic1:vlan> mocreate 'vlanPool1' 'static-allocation'
admin@apic1:vlan> moconfig commit

# fvns-encapblk
admin@apic1:vlan> cd '/aci/fabric/access-policies/pools/vlan/vlanPool1-static-allocation/encap-blocks'
```

```
admin@apic1:encap-blocks> mocreate 'vlan-10' 'vlan-25'
admin@apic1:encap-blocks> moconfig commit
```

ステップ 7 ドメインに EPG を関連付けます。

例：

```
admin@apic1:~> cd
'/aci/tenants/test1/application-profiles/AP1/application-epgs/EPG1/domains-vms-and-bare-metals'
admin@apic1:domains-vms-and-bare-metals> mocreate
'fabric/access-policies/physical-and-external-domains/physical-domains/domP'
admin@apic1:domains-vms-and-bare-metals> cd
'[fabric--access-policies--physical-and-external-domains--physical-domains--domP]'
admin@apic1:[fabric--access-policies--physical-and-external-domains--physical-domains--domP]> moset
 deployment-immediacy 'immediate'
admin@apic1:[fabric--access-policies--physical-and-external-domains--physical-domains--domP]> moset
 resolution-immediacy 'immediate'
admin@apic1:[fabric--access-policies--physical-and-external-domains--physical-domains--domP]> moset
 name 'domP'
admin@apic1:[fabric--access-policies--physical-and-external-domains--physical-domains--domP]>
moconfig commit
```

第 6 章

ACI ファブリックのレイヤ 3 Outside 接続

この章の内容は、次のとおりです。

BGP レイヤ 3 外部ネットワーク接続設定のガイドライン

BGP 外部ルーテッド ネットワークを設定するときは、以下のガイドラインに従ってください。

- リーフ スイッチにルータ ID を作成すると、必ず内部ループバック アドレスが作成されます。リーフ スイッチに BGP 接続をセットアップする場合、ルート ID をインターフェイスの IP アドレスと同じにすることはできません。これは、その設定が ACI リーフ スイッチではサポートされていないためです。ルータ ID は、別のサブネット内の別のアドレスである必要があります。外部レイヤ 3 デバイスでは、ルータ ID はループバック アドレスまたはインターフェイス アドレスです。スタティック ルートまたは OSPF 設定のいずれかを使用して、レイヤ 3 デバイスのルーティング テーブルにリーフ ルータ ID へのルートが存在することを確認してください。また、レイヤ 3 デバイスに BGP ネイバーをセットアップする場合、使用するピア IP アドレスはリーフ スイッチのルータ ID である必要があります。

- BGP を使用する 2 つの外部レイヤ 3 ネットワークを同じノードに設定する際、ループバック アドレスを明示的に定義する必要があります。このガイドラインに従わないと、BGP を確立できない可能性があります。
- 定義上、ルータ ID はループバック インターフェイスです。ルータ ID を変更してループバックに別のアドレスを割り当てるには、ループバック インターフェイス ポリシーを作成する必要があります（ループバック ポリシーは、アドレス ファミリ、IPv4、および IPv6 ごとに 1 つずつ設定できます）。ループバック ポリシーを作成しない場合は、ルータ ID ループバック（デフォルトで有効）を有効にすることができます。ルータ ID ループバックが無効である場合、導入先の特定のレイヤ 3 Outside に対するループバックは作成されません。
- この設定作業は iBGP および eBGP に適用されます。BGP 設定がループバック アドレスに対するものである場合、iBGP セッションまたはマルチホップ eBGP セッションです。ピア IP アドレスが BGP ピアが定義されている物理インターフェイスに対するものである場合、物理インターフェイスが使用されます。
- IPv6 を使用したループバックを介したピアリングを有効にするには、ユーザが IPv6 アドレスを設定する必要があります。
- 自律システム機能は eBGP ピアでしか使用できません。この機能では、ルータが実際の AS に加えて、2 番めの自律システム（AS）のメンバであるように見せることができます。ローカル AS を使用すると、ピアリングの調整を変更せずに 2 つの ISP をマージできます。マージされた ISP 内のルータは、新しい自律システムのメンバになりますが、使用者に対しては古い自律システム番号を使用し続けます。
- リリース 1.2（1x）以降、BGP `l3extOut` 接続のテナント ネットワーキング プロトコル ポリシーは、最大プレフィックス制限を使用して設定できます。これにより、ピアから受信されるルートプレフィックスの数をモニタし、制限することができます。最大プレフィックス制限を超えると、ログエントリの記録、それ以降のプレフィックスの拒否、固定期間中にカウントがしきい値未満になった場合の接続の再起動、または接続のシャットダウンを行うことができます。一度に 1 つのオプションだけを使用できます。デフォルト設定では 20,000 プレフィックスに制限され、その後は新しいプレフィックスは拒否されます。拒否オプションが導入されると、BGP は設定されている制限よりも 1 つ多くプレフィックスを受け入れ、APIC でエラーが発生します。

BGP 接続タイプおよびループバックのガイドライン

BGP 接続タイプおよびループバックの設定要件については、以下のガイドラインに従ってください。

- ノードのルータ ID が作成されると、ルータ ID と同じ IP アドレスでループバック インターフェイスも作成されます。これはデフォルトの動作ですが、ルータ ID を設定するときにオーバーライドできます。
- ルータ ID に対して設定される IP アドレスは、そのノードで設定されているその他すべての IP アドレスと異なるサブネットの異なるアドレスである必要があります。

- ノードあたりの外部 BGP ピアが 1 つのみである場合、ルータ ID IP アドレスを持つループバック インターフェイスを外部ルータとのピアリングに使用できます。同じノードにある複数の BGP ピアでピアリングする場合、ルート ID ループバック アドレスは使用できません。BGP ごとに明示的なループバック インターフェイス ポリシーを使用する必要があります。
- ループバック インターフェイス ポリシーは、直接接続されたネットワークの外部ルータとピアリングするときは必要ではありません。
- ループバック インターフェイス（iBGP または eBGP マルチホップ）を使用して外部ルータとピアリングする場合、リモート ピアのループバック アドレスに到達するためにスタティック ルートまたは OSPF ルートが必要です。
- BGP では、ループバックの作成がデフォルトで選択されています。これが選択されると、BGPセッションを確立するために、送信元インターフェイスとしてループバックが使用されます。ただし、物理インターフェイスを介してeBGPを確立するために、管理者がループバックを作成してはなりません。

表 *2* :

BGP 接続タイプ	ループバックが必要	ルータ ID と同じループバック	スタティック ルートまたは OSPF ルートが必要
直接 iBGP	いいえ	N/A	いいえ
iBGP ループバック ピアリング	はい（BGP ピアごとに個別のループバック）	いいえ（同じノードに複数のレイヤ 3 Out がある場合）	はい
直接 eBGP	いいえ	N/A	いいえ
eBGP ループバック ピアリング（マルチホップ）	はい（BGP ピアごとに個別のループバック）	いいえ（同じノードに複数のレイヤ 3 Out がある場合）	はい

GUI を使用した BGP 外部ルーテッド ネットワークの設定

はじめる前に

外部ルーテッド ネットワークを設定するテナント、VRF、およびブリッジ ドメインがすでに作成されていること。

ステップ 1 [Navigation] ペインで、[Tenant_name] > [Networking] > [External Routed Networks] を展開します。

ステップ 2 右クリックし、[Create Routed Outside] をクリックします。

ステップ 3 [Create Routed Outside] 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、外部ルーテッド ネットワーク ポリシーの名前を入力します。

b) [BGP] チェックボックスをクリックします。

（注） 次の 2 つの方法のいずれかで、BGP ピアの到達可能性を使用できるようになっている必要があります。スタティック ルートを設定するか、または OSPF を有効にする必要があります。

c) （任意） [Route Control Enforcement] フィールドで、[mport] チェックボックスをオンにします。

（注） BGP でインポート制御を適用する場合は、このチェックボックスをオンにします。

d) [VRF] フィールドのドロップダウン リストから、目的の VRF を選択します。

e) [Route Control for Dampening] フィールドを展開し、目的のアドレス ファミリ タイプとルート ダンプニング ポリシーを選択します。[Update] をクリックします。
このステップでは、ポリシーはステップ 4 で作成することができます。または、ポリシー名が選択されているドロップダウン リストでルート プロファイルを作成するオプションがあります。

f) [Nodes and Interfaces Protocol Policies] を展開します。

g) [Create Node Profile] ダイアログボックスに、ノード プロファイルの名前を入力します。

h) [Nodes] を展開します。

i) [Select Node] ダイアログボックスの [Node ID] フィールドのドロップダウン リストから、ノードを選択します。

j) [Router ID] フィールドに、ルータ ID を入力します。

k) [Loopback Address] を展開し、[IP] フィールドに IP アドレスを入力します。[Update] をクリックします。

（注） IPv6 アドレスを入力します。前のステップでルータ ID を追加しなかった場合は、[IP] フィールドに IPv4 アドレスを追加できます。

l) [OK] をクリックします。

ステップ 4 [Navigation] ペインで、[Tenant_name] > [Networking] > [Route Profiles] の順に展開します。[Route Profiles] を右クリックし、[Create Route Profile] をクリックします。[Create Route Profile] 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、ルート制御 VRF の名前を入力します。

b) [Create Route Control Context] ダイアログボックスを展開します。

c) [Name] フィールドに、ルート制御 VRF の名前を入力します。

d) [Set Attribute] ドロップダウン リストから、[Create Action Rule Profile] を選択します。
アクション ルールを作成するときに、必要に応じてルート ダンプニング属性を設定します。

ステップ 5 [Create Interface Profiles] 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、インターフェイス プロファイル名を入力します。
b) [Interfaces] 領域で、目的のインターフェイス タブを選択し、インターフェイスを展開します。

ステップ 6 [Select Routed Interface] ダイアログボックスで、次の操作を実行します。

a) [Path] ドロップダウン リストから、ノードおよびインターフェイスを選択します。
b) [IP Address] フィールドに、IP アドレスを入力します。
（注） 必要に応じて、IPv6 アドレスまたは IPv4 アドレスを追加できます。
c) （任意） 前のステップで IPv6 アドレスを入力した場合は、[Link-local Address] フィールドに IPv6 アドレスを入力します。
d) [BGP Peer Connectivity Profile] フィールドを展開します。

ステップ 7 [Create Peer Connectivity Profile] ダイアログボックスで、次の操作を実行します。

a) [Peer Address] フィールドでは、ダイナミック ネイバー機能を使用できます。必要に応じて、指定されたサブネット内のすべてのピアが BGP と通信またはルートを交換できます。
手順内の前のステップで入力した IPv4 または IPv6 のアドレスに対応する IPv4 または IPv6 のアドレスを入力します。
b) [BGP Controls] フィールドで、目的の制御をオンにします。
c) [Autonomous System Number] フィールドで、目的の値を選択します。
d) （任意） [Weight for routes from this neighbor] フィールドで、目的の値を選択します。
e) （任意） [Private AS Control] フィールドで、[Remove AS] のチェックボックスをオンにします。
f) （任意） [Local Autonomous System Number Config] フィールドで、目的の値を選択します。
eBGP ピアのローカル自律システム機能の場合にオプションで必要です。
g) （任意） [Local Autonomous System Number] フィールドで、目的の値を選択します。
eBGP ピアのローカル自律システム機能の場合にオプションで必要です。
（注） このフィールドの値は、[Autonomous System Number] フィールドの値と同じであってはなりません。
h) [OK] をクリックします。

ステップ 8 次のアクションを実行します。

a) [Select Routed Interface] ダイアログボックスで、[OK] をクリックします。
b) [Create Interface Profile] ダイアログボックスで、[OK] をクリックします。
c) [Create Node Profile] ダイアログボックスで、[OK] をクリックします。
[External EPG Networks] 領域が表示されます。
d) [Create Routed Outside] ダイアログボックスで、前に作成したノード プロファイルを選択し、[Next] をクリックします。

ステップ 9 [External EPG Networks] を展開し、[Create External Network] 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、外部ネットワークの名前を入力します。
b) [Subnet] を展開します。
c) [Create Subnet] ダイアログボックスの [IP address] フィールドに、必要に応じてサブネット アドレスを入力します。

（注） 前のステップで入力した内容に応じて、IPv4 または IPv6 のアドレスを入力します。

外部サブネットを作成するときに、プレフィックス EPG の BGP ループバックの両方を設定するか、またはどちらも設定しない必要があります。BGP ループバックを 1 つのみ設定すると、BGP ネイバーシップは確立されません。

d) [Scope] フィールドで、[Export Route Control Subnet] 、[Import Route Control Subnet] 、および [Security Import Subnet] のチェックボックスをオンにします。[OK] をクリックします。

（注） BGP でインポート制御を適用する場合は、[Import Route Control Subnet] チェックボックスをオンにします。

ステップ 10 [Create External Network] ダイアログボックスで、[OK] をクリックします。

ステップ 11 [Create Routed Outside] ダイアログボックスで、[Finish] をクリックします。
eBGP は外部接続用に設定されています。

REST API を使用した BGP 外部ルーテッド ネットワークの設定

はじめる前に

外部ルーテッド ネットワークを設定するテナントがすでに作成されていること。

ここでは、REST API を使用して BGP 外部ルーテッド ネットワークを設定する方法を示します。

例：

```
<l3extOut descr="" dn="uni/tn-t1/out-l3out-bgp" enforceRtctrl="export" name="l3out-bgp" ownerKey=""
 ownerTag="" targetDscp="unspecified">
<l3extRsEctx tnFvCtxName="ctx3"/>
<l3extLNodeP configIssues="" descr="" name="l3extLNodeP_1" ownerKey="" ownerTag="" tag="yellow-green"
 targetDscp="unspecified">
<l3extRsNodeL3OutAtt rtrId="1.1.1.1" rtrIdLoopBack="no" tDn="topology/pod-1/node-101"/>
<l3extLIfP descr="" name="l3extLIfP_2" ownerKey="" ownerTag="" tag="yellow-green">
<l3extRsNdIfPol tnNdIfPolName=""/>
<l3extRsIngressQosDppPol tnQosDppPolName=""/>
<l3extRsEgressQosDppPol tnQosDppPolName=""/>
<l3extRsPathL3OutAtt addr="3001::31:0:1:2/120" descr="" encap="vlan-3001" encapScope="local"
ifInstT="sub-interface" llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-1/paths-101/pathep-[eth1/8]" targetDscp="unspecified">
<bgpPeerP addr="3001::31:0:1:0/120" allowedSelfAsCnt="3" ctrl="send-com,send-ext-com" descr=""
name="" peerCtrl="bfd" privateASctrl="remove-all,remove-exclusive,replace-as" ttl="1" weight="1000">
<bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
<bgpAsP asn="3001" descr="" name=""/>
</bgpPeerP>
</l3extRsPathL3OutAtt>
</l3extLIfP>
<l3extLIfP descr="" name="l3extLIfP_1" ownerKey="" ownerTag="" tag="yellow-green">
```

```
<l3extRsNdIfPol tnNdIfPolName=""/>
<l3extRsIngressQosDppPol tnQosDppPolName=""/>
<l3extRsEgressQosDppPol tnQosDppPolName=""/>
<l3extRsPathL3OutAtt addr="31.0.1.2/24" descr="" encap="vlan-3001" encapScope="local"
ifInstT="sub-interface" llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-1/paths-101/pathep-[eth1/8]" targetDscp="unspecified">
<bgpPeerP addr="31.0.1.0/24" allowedSelfAsCnt="3" ctrl="send-com,send-ext-com" descr="" name=""
peerCtrl="" privateASctrl="remove-all,remove-exclusive,replace-as" ttl="1" weight="100">
<bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
<bgpLocalAsnP asnPropagate="none" descr="" localAsn="200" name=""/>
<bgpAsP asn="3001" descr="" name=""/>
</bgpPeerP>
</l3extRsPathL3OutAtt>
</l3extLIfP>
</l3extLNodeP>
<l3extRsL3DomAtt tDn="uni/l3dom-l3-dom"/>
<l3extRsDampeningPol af="ipv6-ucast" tnRtctrlProfileName="damp_rp"/>
<l3extRsDampeningPol af="ipv4-ucast" tnRtctrlProfileName="damp_rp"/>
<l3extInstP descr="" matchT="AtleastOne" name="l3extInstP_1" prio="unspecified"
targetDscp="unspecified">
<l3extSubnet aggregate="" descr="" ip="130.130.130.0/24" name="" scope="import-rtctrl">
</l3extSubnet>
<l3extSubnet aggregate="" descr="" ip="130.130.131.0/24" name="" scope="import-rtctrl"/>
<l3extSubnet aggregate="" descr="" ip="120.120.120.120/32" name=""
scope="export-rtctrl,import-security"/>
<l3extSubnet aggregate="" descr="" ip="3001::130:130:130:100/120" name="" scope="import-rtctrl"/>
</l3extInstP>
<bgpExtP descr=""/>
</l3extOut>
<rtctrlProfile descr="" dn="uni/tn-t1/prof-damp_rp" name="damp_rp" ownerKey="" ownerTag=""
type="combinable">
 <rtctrlCtxP descr="" name="ipv4_rpc" order="0">
  <rtctrlScope descr="" name="">
   <rtctrlRsScopeToAttrP tnRtctrlAttrPName="act_rule"/>
  </rtctrlScope>
 </rtctrlCtxP>
</rtctrlProfile>
<rtctrlAttrP descr="" dn="uni/tn-t1/attr-act_rule" name="act_rule">
  <rtctrlSetDamp descr="" halfLife="15" maxSuppressTime="60" name="" reuse="750" suppress="2000"
type="dampening-pol"/>
</rtctrlAttrP>
```

オブジェクト モデル CLI を使用した BGP 外部ルーテッド ネットワークの設定

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：

```
admin@apic1:~> cd /aci
```

ステップ 2 テナントのスコープと外部ルーテッド ネットワークのスコープを入力します。

例：

```
admin@apic1:tenants> ls common infra  mgmt  tn1
admin@apic1:tenants> cd tn1/
admin@apic1:tn1> cd networking/external-routed-networks/
```

ステップ 3 レイヤ 3 Outside を作成します。

例：

```
admin@apic1:external-routed-networks> mocreate l3-outside bgp-ext-out
admin@apic1:external-routed-networks> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out'
All mos committed successfully.
```

ステップ 4 レイヤ 3 Outside スコープで BGP を有効にします。論理ノード プロファイル、ノード プロファイルのノードを作成し、ルータ ID とルータ ループバックを設定します。

例：

```
admin@apic1:external-routed-networks> cd l3-outside-bgp-ext-out/
admin@apic1:l3-outside-bgp-ext-out> mocreate bgp-ext-profile
admin@apic1:l3-outside-bgp-ext-out> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/bgp-ext-profile'
All mos committed successfully.

admin@apic1:l3-outside-bgp-ext-out> moset private-network default
admin@apic1:l3-outside-bgp-ext-out> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out'
All mos committed successfully.

admin@apic1:l3-outside-bgp-ext-out> cd logical-node-profiles
admin@apic1:logical-node-profiles> mocreate
 <name>  logical node profile name

admin@apic1:logical-node-profiles> mocreate np1
admin@apic1:logical-node-profiles> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/logical-node-profiles/np1'
All mos committed successfully.

admin@apic1:logical-node-profiles> cd np1/
admin@apic1:np1> cd nodes/
admin@apic1:nodes> mocreate fabric/inventory/pod-1/node-101
admin@apic1:nodes> ls
[fabric--inventory--pod-1--node-101]  summary
admin@apic1:nodes> cd \[fabric--inventory--pod-1--node-101\]/
admin@apic1:[fabric--inventory--pod-1--node-101]> moset router-id 1.1.1.2
admin@apic1:[fabric--inventory--pod-1--node-101]> moset rtridloopback yes
admin@apic1:[fabric--inventory--pod-1--node-101]> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out
/logical-node-profiles/np1/nodes/[fabric/inventory/pod-1/node-101]'
All mos committed successfully.

admin@apic1:[fabric--inventory--pod-1--node-101]>
admin@apic1:[fabric--inventory--pod-1--node-101]> cd ..
admin@apic1:nodes> cd ..
```

ステップ 5 インターフェイス プロファイルを作成します。

例：

```
admin@apic1:np1> cd logical-interface-profiles/
admin@apic1:logical-interface-profiles> mocreate intfp1
admin@apic1:logical-interface-profiles> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out
```

```
/logical-node-profiles/np1/logical-interface-profiles/intfp1'
All mos committed successfully.
```

ステップ 6 ルータ インターフェイスを設定します。

例：

```
admin@apic1:logical-interface-profiles> cd intfp1/
admin@apic1:intfp1> cd routed-interfaces/
admin@apic1:routed-interfaces> mocreate topology/pod-1/paths-102/pathep-[eth9/3] ip-address
100.1.1.2/24
admin@apic1:routed-interfaces> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out
/logical-node-profiles/np1/logical-interface-profiles/intfp1/routed-interfaces
/[topology/pod-1/paths-102/pathep-[eth9/3]]'
All mos committed successfully.
```

ステップ 7 BGP ピア設定を作成します。

例：

```
admin@apic1:logical-interface-profiles> cd ../bgp-peer-connectivity/

admin@apic1:bgp-peer-connectivity>  mocreate 100.1.1.3/24 bgp-controls send-community add
autonomous-system-number 33
admin@apic1:bgp-peer-connectivity> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out
/logical-node-profiles/np1/bgp-peer-connectivity/100.1.1.3/24'
All mos committed successfully.
```

ステップ 8 外部 EPG を作成します。

例：

```
admin@apic1:l3-outside-bgp-ext-out> cd networks/
admin@apic1:networks> mocreate extepg
admin@apic1:networks> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/networks/extepg'
All mos committed successfully.
```

ステップ 9 サブネットを作成し、サブネットのスコープを設定します。

例：

```
admin@apic1:networks> cd extepg/
admin@apic1:extepg> cd subnets/
admin@apic1:subnets> mocreate 1.1.1.2
admin@apic1:subnets> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/networks/extepg/subnets/1.1.1.2'
All mos committed successfully.

admin@apic1:subnets> cd 1.1.1.2/

admin@apic1:1.1.1.2> moset scope-of-the-external-subnet import-route-control-subnet
admin@apic1:1.1.1.2> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/networks/extepg/subnets/1.1.1.2'

All mos committed successfully.
admin@apic1:1.1.1.2>

The external BGP Outside is now configured successfully.
```

テナントのレイヤ3 Outside ネットワーク接続の設定の概要

このトピックでは、APIC 使用時にテナント ネットワークに対してレイヤ 3 Outside を設定する方法の典型的な例を示します。

GUI を使用したテナント ネットワークのレイヤ 3 Outside の設定

この例で設定されている外部ルーテッド ネットワークを、IPv4 をサポートするように拡張することもできます。IPv4 と IPv6 両方のルートを外部ルーテッド ネットワークにアドバタイズし、外部ルーテッド ネットワークから学習することができます。

はじめる前に

- テナント、VRF、およびブリッジ ドメインが作成されていること。
- 外部ルーテッド ドメインが作成されていること。

ステップ 1 メニュー バーで、[TENANTS] をクリックします。

ステップ 2 [Navigation] ペインで、*[Tenant_name]* > [Networking] > [External Routed Networks] の順に展開し、次の操作を実行します。

a) [External Routed Networks] を右クリックし、[Create Routed Outside] をクリックします。
b) [Create Routed Outside] ダイアログボックスの [Name] フィールドに、ルーテッド Outside の名前を入力します。
c) ルーテッド プロトコルのチェックボックスがある領域で、目的のプロトコルをオンにします。
使用可能なオプションは、BGP、OSPF、EIGRP です。これにより、後のステップで [Create External Network] ダイアログボックスのルート集約ポリシーが有効になります。
d) [VRF] フィールドのドロップダウン リストから、適切な VRF を選択します。
e) [External Routed Domain] ドロップダウン リストから、適切な外部ルーテッド ドメインを選択します。
f) 目的のプロトコルのチェックボックスをオンにします。
選択するプロトコルに応じて、プロパティを設定する必要があります。
g) [Nodes and Interfaces Protocol Profile] を展開します。
h) [Create Node Profile] ダイアログボックスで、[Name] フィールドに、名前を入力します。
i) [Nodes] を展開します。
j) [Select Node] ダイアログボックスで、[Node ID] ドロップダウン メニューから適切なノード ID を選択します。
k) [Router ID] フィールドに、ルータ ID を入力します。
l) [Loopback Addresses] を展開し、[IP] フィールドに IP アドレスを入力します。[Update] をクリックします。

（注） [Loopback Addresses] フィールドで、必要に応じて IPv4 または IPv6 のループバックを作成します。

m) [OK] をクリックします。

ステップ 3 [Interface Profiles] を展開し、次の操作を実行します。

a) [Create Interface Profile] ダイアログボックスの [Name] フィールドに、プロファイルの名前を入力します。

b) [Routed Interfaces] を展開します。

c) [Select Routed Interface] ダイアログボックスの [Path] ドロップダウン リストから、インターフェイス パスを選択します。

d) [IP Address] フィールドに、IP アドレスを入力します。

（注） IPv6 を設定するには、ダイアログボックスの [Link-local Address] フィールドにリンクローカル アドレスを入力する必要があります。

e) [OK] をクリックします。
[Create Interface Profile] ダイアログボックスに、ルーテッド インターフェイスの詳細が表示されます。

f) [OK] をクリックします。

ステップ 4 [Create Node Profile] ダイアログボックスで、[OK] をクリックします。

ステップ 5 [Create Routed Outside] ダイアログボックスで、[Next] をクリックします。

ステップ 6 [External EPG Networks] 領域で、[External EPG Networks] を展開します。

ステップ 7 [Create External Networks] ダイアログボックスの [Name] フィールドに、外部ネットワークの名前を入力します。

ステップ 8 [Subnet] を展開します。

ステップ 9 [Create Subnet] ダイアログボックスで、次の操作を実行します。

a) [IP Address] フィールドに、IP アドレスを入力します。

b) [Scope] フィールドで、適切なチェックボックスをオンにします。[OK] をクリックします。

ステップ 10 [Create External Network] ダイアログボックスで、次の操作を実行します。

a) 別のサブネットを追加するために、[Subnet] を展開します。

b) [Create Subnet] ダイアログボックスの [IP Address] フィールドに、IP アドレスを入力します。

c) [Scope] フィールドで、適切なチェックボックスをオンにします。[OK] をクリックします。

（注）
- インポート制御ポリシーはデフォルトで有効になっていませんが、ユーザが有効にすることができます。インポート制御ポリシーは BGP ではサポートされますが、EIGRP および OSPF ではサポートされません。ユーザがサポートされていないプロトコルのインポート制御ポリシーを有効にしても、自動的に無視されます。
- エクスポート制御ポリシーは、BGP、EIGRP、および OSPF でサポートされます。
- ルート集約もサポートされ、ユーザは希望するエクスポートまたはインポートの方向でルート集約を任意で選択できます。この機能は、0.0.0.0/0 およびセキュリティ オプションの場合に使用できます。インポート制御ポリシーが有効になっていない場合、オンにすべきチェックボックスの例は、[Export Subnet]、[Security Import Subnet]、および [Aggregate Export] です。ユーザは、ルート マップおよびセキュリティ オプションを選択する必要があります。
- レイヤ 3 Outside に対して明示的なルート制御ポリシーが設定されている場合、特定のレイヤ 3 Outside ポリシーのみがサポートされます。集約ルートでは、明示的なルート制御ポリシーはサポートされません。

d) （任意） [Route Summarization Policy] フィールドで、必要に応じてドロップダウン リストから既存のルート集約ポリシーを選択するか、または新しいルート集約ポリシーを作成します。また、チェックボックス [Export Route Control Subnet] をオンにする必要があります。

e) [Create External Network] ダイアログボックスで、[OK] をクリックします。

ステップ 11 [Create Routed Outside] ダイアログボックスで、[Finish] をクリックします。

ステップ 12 [Navigation] ペインの *[Tenant_name]* > [Networking] > [Bridge Domains] で、[Bridge_Domain_name] を選択します。

ステップ 13 [Work] ペインの [Properties] の下の [L3 Out for Route Profile] のドロップダウン リストで、目的のレイヤ 3 Outside を関連付けます。[Submit] をクリックします。
これにより、テナント ネットワークに対してレイヤ 3 Outside が設定されます。

ステップ 14 （注） 受信するすべてのルートについて BGP、OSPF、または EIGRP の通信の属性を設定するには、default-import ルート制御プロファイルを作成し、適切な set アクションおよび no match アクションを作成します。

[Navigation] ペインで、[Route Profiles] をクリックし、[Create Route Profiles] を右クリックし、[Create Route Profiles] 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、名前を入力します。

b) [Type] フィールドで、[Use Routing Policy Only] をクリックする必要があります。[Submit] をクリックします。

REST API を使用したテナント ネットワークのレイヤ 3 Outside の設定

この例で設定されている外部ルーテッド ネットワークを、IPv4 をサポートするように拡張することもできます。IPv4 と IPv6 両方のルートを外部ルーテッド ネットワークにアドバタイズし、外部ルーテッド ネットワークから学習することができます。

はじめる前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。
- 外部ルーテッド ドメインが作成されていること。

テナント ネットワークの L3 Outside を設定し、ブリッジ ドメインを Layer3 Outside に関連付けます。

例：

```
<l3extOut name="L3Out1" enforceRtctrl="import,export">
            <l3extRsL3DomAtt tDn="uni/l3dom-l3DomP"/>
        <l3extLNodeP name="LNodeP1" >
            <l3extRsNodeL3OutAtt rtrId="1.2.3.4" tDn="topology/pod-1/node-101">
                <l3extLoopBackIfP addr="10.10.11.1" />
                <l3extLoopBackIfP addr="2000::3" />
            </l3extRsNodeL3OutAtt>
            <l3extLIfP  name="IFP1" >
                <l3extRsPathL3OutAtt addr="10.11.12.10/24"  ifInstT="l3-port"
tDn="topology/pod-1/paths-103/pathep-[eth1/17]" />
            </l3extLIfP>
            <l3extLIfP  name="IFP2" >
                <l3extRsPathL3OutAtt addr="2001::3/64"  ifInstT="l3-port"
tDn="topology/pod-1/paths-103/pathep-[eth1/17]" />
            </l3extLIfP>
        </l3extLNodeP>
        <l3extRsEctx tnFvCtxName="VRF1"/>
        <l3extInstP name="InstP1" >
            <l3extSubnet ip="192.168.1.0/24" scope="import-security" aggregate=""/>
            <l3extSubnet ip="0.0.0.0/0" scope="export-rtctrl,import-rtctrl,import-security"
aggregate="export-rtctrl,import-rtctrl"/>
            <l3extSubnet ip="192.168.2.0/24" scope="export-rtctrl" aggregate=""/>
           <l3extSubnet ip="::/0" scope="import-rtctrl,import-security" aggregate="import-rtctrl"/>

            <l3extSubnet ip="2001:17a::/64" scope="export-rtctrl" aggregate=""/>
        </l3extInstP>
    </l3extOut>
```

（注） OSPF および EIGRP では、"enforceRtctrl=import" は適用できません。

オブジェクト モデル CLI を使用したテナント ネットワークのレイヤ 3 Outside の設定

この例で設定されている外部ルーテッド ネットワークを、IPv4 をサポートするように拡張することもできます。IPv4 と IPv6 両方のルートを外部ルーテッド ネットワークにアドバタイズし、外部ルーテッド ネットワークから学習することができます。

はじめる前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。

- 外部ルーテッド ドメインが設定されていること。

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：

```
admin@apic1:~> cd /aci
```

ステップ 2 テナントと外部ルータ ネットワークのスコープを入力します。

例：

```
admin@apic1:tenants> ls common infra  mgmt  tn1
admin@apic1:tenants> cd tn1/
admin@apic1:tn1> cd networking/external-routed-networks/
```

ステップ 3 レイヤ 3 Outside スコープで目的のプロトコルを有効にします。論理ノード プロファイル、ノード プロファイルのノードを作成し、ルータ ID とルータ ループバックを設定します。

例：

```
admin@apic1:external-routed-networks> mocreate l3-outside tenant-ext-out
admin@apic1:external-routed-networks> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out'
All mos committed successfully.

admin@apic1:external-routed-networks> cd l3-outside-tenant-ext-out/
admin@apic1:l3-outside-tenant-ext-out> mocreate bgp-ext-profile
admin@apic1:l3-outside-tenant-ext-out> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out/bgp-ext-profile'
All mos committed successfully.

admin@apic1:l3-outside-tenant-ext-out> moset private-network default
admin@apic1:l3-outside-tenant-ext-out> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out'
All mos committed successfully.

admin@apic1:l3-outside-tenant-ext-out> moset  external-routed-domain fabric
/access-policies/physical-and-external-domains/external-routed-domains/dom1
admin@apic1:l3-outside-tenant-ext-out> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out'

admin@apic1:l3-outside-tenant-ext-out> cd logical-node-profiles
admin@apic1:logical-node-profiles> mocreate np1
admin@apic1:logical-node-profiles> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out
/logical-node-profiles/np1'
All mos committed successfully.

admin@apic1:logical-node-profiles> cd np1/
admin@apic1:np1> cd nodes/
admin@apic1:nodes> mocreate fabric/inventory/pod-1/node-101
admin@apic1:nodes> ls [fabric--inventory--pod-1--node-101]  summary
admin@apic1:nodes> cd \[fabric--inventory--pod-1--node-101\]/
admin@apic1:[fabric--inventory--pod-1--node-101]> moset router-id 1.1.1.1

admin@apic1:[fabric--inventory--pod-1--node-101]> moset rtridloopback yes
admin@apic1:[fabric--inventory--pod-1--node-101]> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out
/logical-node-profiles/np1/nodes/[fabric/inventory/pod-1/node-101]'
All mos committed successfully.

admin@apic1:[fabric--inventory--pod-1--node-101]>
```

```
admin@apic1:[fabric--inventory--pod-1--node-101]> cd ..
admin@apic1:nodes> cd ..
```

ステップ 4 インターフェイス プロファイルを作成します。

例：

```
admin@apic1:np1> cd logical-interface-profiles/
admin@apic1:logical-interface-profiles> mocreate intfp1
admin@apic1:logical-interface-profiles> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out
/logical-node-profiles/np1/logical-interface-profiles/intfp1'
All mos committed successfully.
```

ステップ 5 ルータ インターフェイスを設定します。

例：

```
admin@apic1:logical-interface-profiles> cd intfp1/
admin@apic1:intfp1> cd routed-interfaces/
admin@apic1:routed-interfaces> mocreate topology/pod-1/paths-102/pathep-[eth9/3] ip-address
100.1.1.2/24
admin@apic1:routed-interfaces> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out
/logical-node-profiles/np1/logical-interface-profiles/intfp1/routed-interfaces/[topology/pod-1
/paths-102/pathep-[eth9/3]]'
All mos committed successfully.
```

ステップ 6 外部 EPG を作成します。

例：

```
admin@apic1:l3-outside-tenant-ext-out> cd networks/
admin@apic1:networks> mocreate extepg
admin@apic1:networks> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out
/networks/extepg'
All mos committed successfully.
```

ステップ 7 サブネットを作成します。

例：

```
admin@apic1:networks> cd extepg/
admin@apic1:extepg> cd subnets/
admin@apic1:subnets> mocreate 0.0.0.0
admin@apic1:subnets> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out
/networks/extepg/subnets/0.0.0.0'
All mos committed successfully.

admin@apic1:subnets> cd 0.0.0.0/

admin@apic1:1.1.1.1> moset scope-of-the-external-subnet import-route-control-subnet
admin@apic1:1.1.1.1> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out
/networks/extepg/subnets/0.0.0.0'

All mos committed successfully.
admin@apic1:0.0.0.0>
```

ステップ 8 レイヤ 3 Out をブリッジ ドメインに関連付けます。

例：

```
admin@apic1:1.1.1.1> cd /aci/tenants/tn1/networking/bridge-domains
admin@apic1:bridge-domains> mocreate bd1
admin@apic1:bridge-domains> moconfig commit
All mos committed successfully.
```

```
admin@apic1:1.1.1.1>

admin@apic1:bridge-domains> cd bd1/
admin@apic1:bd1> ls associated-l3-outs  dhcp-relay-labels l4-l7-service-parameters mo rasubnets
subnets summary tags
admin@apic1:bd1> cd associated-l3-outs/
admin@apic1:associated-l3-outs> mocreate tenant-ext-out
admin@apic1:1.1.1.1> moconfig commit
```

これで、レイヤ 3 テナント Outside が正常に設定されました。

共有サービス コントラクトの使用

共有サービスを使用すると、テナントの分離とセキュリティ ポリシーを維持したままテナント間で通信できます。外部ネットワークへのルーテッド接続は、複数のテナントが使用する共有サービスの例です。

共有サービス コントラクトの設定時は、次のガイドラインに従ってください。

- さまざまなコンテキスト（VRF）にサブネットをエクスポートする共有サービスでは、EPG にサブネットを定義し、スコープを *advertised externally* および *shared between VRFs* に設定する必要があります。
- プライベート ネットワークを適用しない場合、ブリッジ間ドメインのトラフィックにコントラクトは不要です。
- コンテキスト（VRF）が適用されていない場合でも、共有サービスのコンテキスト（VRF）間トラフィックにはコントラクトが必要です。
- 共有サービスを提供している間は、プロバイダー EPG のコンテキスト（VRF）は非強制モードにできません。
- 共有サービスは、重複しないサブネットのみでサポートされます。共有サービスのサブネットを設定するときは、以下のガイドラインに従ってください。
  - 共有サービス プロバイダーのサブネットは、ブリッジ ドメイン下ではなく EPG 下で設定します。
  - 同じコンテキストを共有する EPG で設定されたサブネットは、統合および重複してはなりません。
  - あるコンテキストから他のコンテキストへ漏れたサブネットは統合および重複してはなりません。
  - 複数のコンシューマ ネットワークからあるコンテキストへ漏れたサブネットまたはその逆で漏れたサブネットは統合および重複してはなりません。

（注） 2 人のコンシューマが誤って同じサブネットに設定されている場合は、両方のサブネットの設定を削除してこの状態からリカバリし、その後サブネットを正しく再設定します。

- プロバイダー コンテキストで共有サービスを `AnyToProv` に設定しないでください。APIC はこの設定を拒否し、エラーが発生します。
- インバンド EPG とアウトオブバンド EPG の間でコントラクトが設定される場合、以下の制限が適用されます。
  - 両方の EPG は同じコンテキスト（VRF）にする必要があります。
  - フィルタは、着信方向のみに適用されます。
  - レイヤ 2 フィルタはサポートされません。
  - QoS は、インバンド レイヤ 4 ～ レイヤ 7 のサービスには適用されません。
  - 管理統計情報は利用できません。
  - CPU 宛てトラフィックの共有サービスはサポートされません。

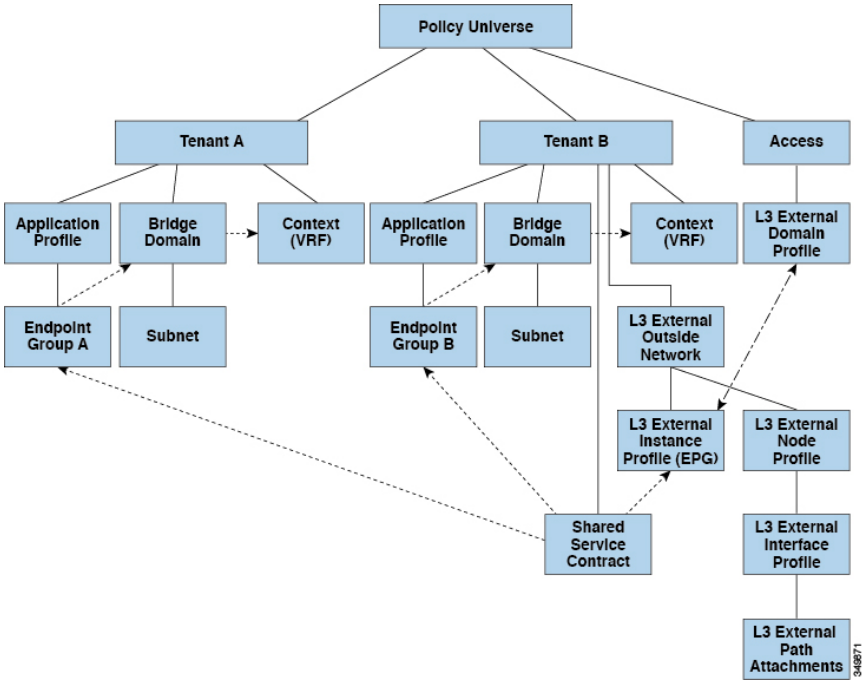
共有レイヤ 3 Out

共有レイヤ 3 Out 設定は、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。`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、または 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、『Firmware Management Guide and Release Notes』というマニュアル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 *28*：共有レイヤ *3 Out* ポリシー モデル



共有レイヤ 3 Out 設定について、以下のガイドライン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 がテナント common 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 ドメインとコンテキスト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コンテキストにありますが、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。レイヤ 3 Outside 外部ネットワークのコンシューマ EPG またはプロバイダー EPG は *shared* に設定されている必要があります。レイヤ 3 Outside 外部ネットワークにエクスポートされるサブネットは、*public* に設定されている必要があります。
- 共有サービス コントラクトは、共有レイヤ 3 Out 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。

- vzAny およびレイヤ 3 Out EPG プロバイダの背後にある `l3extInstP` EPG は、共有サービスの場合はサポートされません。また、コンシューマ `l3extInstP` EPG が vzAny の背後にあり、レイヤ 3 Out EPG がダイレクト コントラクトのプロバイダーである場合、共有レイヤ 3 Out ではトランジット ルーティングはサポートされません。
- トラフィック 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、コンテキスト（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フラップされます（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 3 Out 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、複数の共有レイヤ 3 Out 設定は動作しません。VRF にリーク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 を使用したレイヤ 3 Outside 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 Outside 設定（たとえば、L3Out2）が同じコンテキスト（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）。
- 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に到達する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：
    - コンテキスト（VRF）1 を使用したレイヤ 3 Outside 設定（たとえば L3Out1）は provider1 と呼ばれます。
    - コンテキスト（VRF）2 を使用した 2 番目のレイヤ 3 Outside 設定（たとえば L3Out2）は provider2 と呼ばれます。
    - L3Out1 VRF1 はデフォルト ルートをインターネットにアドバタイズします = 0.0.0.0/0 = *shared-rtctrl*、*shared-security*。
    - L3Out2 VRF2 は特定のサブネットを DNS および NTP にアドバタイズします = 192.0.0.0/8 = *shared-rtctrl*。

- L3Out2 VRF2 には特定のサブネット 192.1.0.0/16 があります = *shared-security*。
- **バリエーション A**：EPG トラフィックが複数のコンテキスト（VRF）に向かいます。
  - EPG1 と L3Out1 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 L3Out2 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 L3Out2 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 Out の *allow_all* コントラクトに従います。
  - EPG1 と L3Out1 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 L3Out2 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 -> L3Out2 -> 192.2.x.x 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：
  - レイヤ 3 Out インスタンス 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。
      - レイヤ 3 Out（l3instP）EPG トラフィックは、以下のプレフィックスを持っているレイヤ 3 Out を通過します。
        - `192.0.0.0/8 = import-security、shared-rtctrl`
        - `192.1.0.0/16 = shared-security`
        - EPG は `1.1.0.0/16 = shared` となっています。

          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。共有レイヤ 3 Out に到達するトラフィックは、コンテキスト（VRF）に応じて通過できます。
      - 共有レイヤ 3 Out のコンテキスト（VRF）は、`pcTag = prov vrf` の EPG と *allow_all* のコントラクトを持っています。
      - 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。

ネイバー探索

IPv6 ネイバー探索（ND）は、ノードのアドレスの自動設定、リンク上の他のノードの探索、他のノードのリンク層アドレスの判別、重複アドレスの検出、使用可能なルータと DNS サーバの検出、アドレスプレフィックスの探索、および他のアクティブなネイバーノードへのパスに関する到達可能性情報の維持を担当します。

ND 固有のネイバー要求/ネイバー アドバタイズメント（NS/NA）およびルータ要求/ルータ アドバタイズメント（RS/RA）パケット タイプは、物理、L3 Sub-if、および SVI（外部およびパーベイシブ）を含むすべての ACI ファブリックのレイヤ 3 インターフェイスでサポートされます。RS/RA パケットはすべての L3 インターフェイスの自動設定に使用されますが、パーベイシブ SVI の場合にのみ設定できます。ACI のブリッジ ドメイン ND は常にフラッド モードで動作します。ユニキャスト モードはサポートされません。

ACI ファブリック ND サポートに含まれるもの：

- インターフェイス ポリシー（`nd:IfPol`）は、NS/NA メッセージに関する ND タイマーと動作を制御します。
- ND プレフィックス ポリシー（`nd:PfxPol`）は、RA メッセージを制御します。
- ND の IPv6 サブネット（fv:Subnet）の設定。
- 外部ネットワークの ND インターフェイス ポリシー。
- 外部ネットワークの設定可能 ND サブネットおよびパーベイシブ ブリッジ ドメインの任意サブネット設定はサポートされません。

設定可能なオプションは次のとおりです。

- 隣接関係
  - 設定可能な静的隣接関係：（<vrf、L3Iface、ipv6 アドレス> --> MAC アドレス）
  - 動的隣接関係：NS/NA パケットの交換によって学習
- インターフェイス単位
  - ND パケットの制御（NS/NA）
    - ネイバー要求間隔
    - ネイバー要求再試行回数
  - RA パケットの制御
    - RA の抑制
    - RA MTU の抑制
    - RA 間隔、RA 最小間隔、再送信時間

- プレフィックス単位（RA でアドバタイズ）の制御
  - ライフタイム、優先ライフタイム
  - プレフィックス制御（自動設定、リンク対象）

拡張 GUI を使用した IPv6 ネイバー探索対応のテナント、VRF、およびブリッジ ドメインの作成

このタスクでは、テナント、VRF、およびブリッジドメイン（BD）を作成し、それらの中に2つの異なるタイプのネイバー探索（ND）ポリシーを作成する方法を示します。これらは ND インターフェイス ポリシーと ND プレフィックス ポリシーです。ND インターフェイス ポリシーは BD に導入されますが、ND プレフィックス ポリシーは個々のサブネットに導入されます。各 BD に独自の ND インターフェイス ポリシーを適用することができます。ND インターフェイス ポリシーは、デフォルトですべての IPv6 インターフェイスに導入されます。Cisco APIC には、使用可能なデフォルトの ND インターフェイス ポリシーがすでに存在します。必要に応じて、代わりに使用するカスタム ND インターフェイス ポリシーを作成できます。ND プレフィックス ポリシーはサブネット レベルにあります。すべての BD が複数のサブネットを持つことができ、各サブネットが異なる ND プレフィックスを持つことができます。

ステップ 1 メニュー バーで、[TENANT] > [Add Tenant] の順にクリックします。

ステップ 2 [Create Tenant] ダイアログボックスで、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。
b) [Security Domains +] アイコンをクリックして [Create Security Domain] ダイアログボックスを開きます。
c) [Name] フィールドに、セキュリティ ドメインの名前を入力します。[Submit] をクリックします。
d) [Create Tenant] ダイアログボックスで、作成したセキュリティ ドメインのチェックボックスをオンにし、[Submit] をクリックします。

ステップ 3 [Navigation] ペインで、[Tenant-name] > [Networking] の順に展開します。[Work] ペインで、[VRF] アイコンをキャンバスにドラッグして [Create VRF] ダイアログボックスを開き、次の操作を実行します。

a) [Name] フィールドに、名前を入力します。
b) [Submit] をクリックして VRF の設定を完了します。

ステップ 4 [Networking] 領域で、[BD] アイコンを [VRF] アイコンにつなげながらキャンバスにドラッグします。[Create Bridge Domain] ダイアログボックスが表示されたら、次の操作を実行します。

a) [Name] フィールドに、名前を入力します。
b) [L3 Configurations] タブをクリックし、[Subnets] を展開して [Create Subnet] ダイアログボックスを開き、[Gateway IP] フィールドにサブネット マスクを入力します。

ステップ 5 [Subnet Control] フィールドで、[ND RA Prefix] チェックボックスがオンになっていることを確認します。

ステップ 6 [ND Prefix policy] フィールドのドロップダウン リストで、[Create ND RA Prefix Policy] をクリックします。

（注） すべての IPv6 インターフェイスに導入される使用可能なデフォルト ポリシーがすでに存在しています。または、この例で示されているように、使用する ND プレフィックス ポリシーを作成できます。デフォルトでは、IPv6 ゲートウェイのサブネットは ND RA メッセージの ND プレフィックスとしてアドバタイズされます。ユーザは、[ND RA prefix] チェックボックスをオフにして、ND RA メッセージでサブネットをアドバタイズしないことを選択できます。

ステップ 7 [Create ND RA Prefix Policy] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドにプレフィックス ポリシーの名前を入力します。
（注） 特定のサブネットに対して存在できるプレフィックス ポリシーは 1 つのみです。サブネットは共通プレフィックス ポリシーを使用できますが、各サブネットに異なるプレフィックス ポリシーを適用することが可能です。

b) [Controller State] フィールドで、目的のチェックボックスをオンにします。

c) [Valid Prefix Lifetime] フィールドで、プレフィックスを有効にする期間について目的の値を選択します。

d) [Preferred Prefix Lifetime] フィールドで、目的の値を選択します。[OK] をクリックします。
（注） ND プレフィックス ポリシーが作成され、特定のサブネットに接続されます。

ステップ 8 [ND policy] フィールドのドロップダウン リストで、[Create ND Interface Policy] をクリックし、次のタスクを実行します。

a) [Name] フィールドにポリシーの名前を入力します。

b) [Submit] をクリックします。

ステップ 9 [OK] をクリックしてブリッジ ドメインの設定を完了します。
同様に、さまざまなプレフィックス ポリシーが適用された追加のサブネットを必要に応じて作成できます。

IPv6 アドレスのサブネットが BD に作成され、ND プレフィックス ポリシーが関連付けられています。

REST API を使用した IPv6 ネイバー探索対応のテナント、VRF、およびブリッジ ドメインの作成

ネイバー探索インターフェイス ポリシーとネイバー探索プレフィックス ポリシーが適用された、テナント、VRF、ブリッジ ドメインを作成します。

例：

```
<fvTenant descr="" dn="uni/tn-ExampleCorp" name="ExampleCorp" ownerKey="" ownerTag="">
    <ndIfPol name="NDPol001" ctrl="managed-cfg”  descr="" hopLimit="64" mtu="1500" nsIntvl="1000"
 nsRetries="3" ownerKey="" ownerTag="" raIntvl="600" raLifetime="1800" reachableTime="0"
retransTimer="0"/>
    <fvCtx descr="" knwMcastAct="permit" name="pvn1" ownerKey="" ownerTag="" pcEnfPref="enforced">

    </fvCtx>
```

```
    <fvBD arpFlood="no" descr="" mac="00:22:BD:F8:19:FF" multiDstPktAct="bd-flood" name="bd1"
ownerKey="" ownerTag="" unicastRoute="yes" unkMacUcastAct="proxy" unkMcastAct="flood">
        <fvRsBDToNdP tnNdIfPolName="NDPol001"/>
        <fvRsCtx tnFvCtxName="pvn1"/>
        <fvSubnet ctrl="nd" descr="" ip="34::1/64" name="" preferred="no" scope="private">
            <fvRsNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
        </fvSubnet>
        <fvSubnet ctrl="nd" descr="" ip="33::1/64" name="" preferred="no" scope="private">
            <fvRsNdPfxPol tnNdPfxPolName="NDPfxPol002"/>
        </fvSubnet>
    </fvBD>
    <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="1000" name="NDPfxPol001" ownerKey=""
ownerTag="" prefLifetime="1000"/>
   <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="4294967295" name="NDPfxPol002" ownerKey=""
 ownerTag="" prefLifetime="4294967295"/>
</fvTenant>
```

（注） 外部ルーテッドを設定するときにパブリック サブネットがある場合は、ブリッジ ドメインを外部設定と関連付ける必要があります。

CLI を使用した IPv6 ネイバー探索対応のテナント、VRF、およびブリッジ ドメインの設定

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：

```
admin@apic1:~> cd /aci
```

ステップ 2 ネイバー探索インターフェイス ポリシーを設定します。

例：

```
admin@apic1:aci> cd tenants/
admin@apic1:tenants> mocreate ExampleCorp
admin@apic1:tenants> moconfig commit
admin@apic1:tenants> cd ExampleCorp/
admin@apic1:ExampleCorp> cd networking/protocol-policies/nd/
admin@apic1:nd> mocreate interface-policy NDPol001
admin@apic1:nd> moconfig commit
admin@apic1:nd> cd interface-policy-NDPol001/
admin@apic1:interface-policy-NDPol001> moset mtu 1500
admin@apic1:interface-policy-NDPol001> moconfig commit
admin@apic1:interface-policy-NDPol001>
admin@apic1:interface-policy-NDPol001> cd ../../../private-networks/
admin@apic1:private-networks> mocreate pvn1
admin@apic1:private-networks> moconfig commit
admin@apic1:pvn1> cd ../../bridge-domains/
admin@apic1:bridge-domains> mocreate bd1
admin@apic1:bridge-domains> cd bd1
admin@apic1:bd1> moset custom-mac-address 00:22:BD:F8:19:FF
admin@apic1:bd1> moset nd-interface-policy NDPol001
admin@apic1:bd1> moconfig commit
```

ステップ 3 ネイバー探索プレフィックス ポリシーを設定します。

例：

```
admin@apic1:bd1> cd ../../protocol-policies/nd/
admin@apic1:nd> mocreate prefix-policy NDPfxPol001
admin@apic1:nd> cd prefix-policy-NDPfxPol001/
admin@apic1:prefix-policy-NDPfxPol001> moset valid-lifetime 1000
admin@apic1:prefix-policy-NDPfxPol001> moset preferred-lifetime 1000
admin@apic1:prefix-policy-NDPfxPol001> moconfig commit
admin@apic1:prefix-policy-NDPfxPol001> cd ../
admin@apic1:nd> mocreate prefix-policy NDPfxPol002
admin@apic1:nd> cd prefix-policy-NDPfxPol002/
admin@apic1:prefix-policy-NDPfxPol002> moset valid-lifetime 4294967295
admin@apic1:prefix-policy-NDPfxPol002> moset preferred-lifetime 4294967295
admin@apic1:prefix-policy-NDPfxPol002> moconfig commit
admin@apic1:prefix-policy-NDPfxPol002> cd ../../../bridge-domains/bd1/subnets/
admin@apic1:subnets> mocreate 34::1/64
admin@apic1:subnets> cd 34::1_64/
admin@apic1:34::1_64> moset nd-prefix-policy NDPfxPol001
admin@apic1:34::1_64> moconfig commit
admin@apic1:34::1_64> cd ../
admin@apic1:subnets> mocreate 33::1/64
admin@apic1:subnets> cd 33::1_64/
admin@apic1:33::1_64> moset nd-prefix-policy NDPfxPol002
admin@apic1:33::1_64> moconfig commit
```

インポート制御とエクスポート制御を使用するルーティング制御プロトコルの設定

このトピックでは、Cisco APIC 使用時にインポート制御とエクスポート制御を使用するルーティング制御プロトコルを設定する方法の典型的な例を示します。

GUI を使用した、インポート制御とエクスポート制御を使用するルート制御プロトコルの設定

このタスクでは、インポートポリシーとエクスポートポリシーの作成手順を示します。デフォルトでは、インポート制御は適用されていないため、インポート制御を手動で割り当てる必要があります。

はじめる前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。

- テナント ネットワークのレイヤ 3 Outside が作成されていること。

ステップ 1 メニュー バーで、[TENANTS] > *[Tenant_name]* > [Networking] > [External Routed Networks] > *[Layer3_Outside_name]* の順にクリックします。

ステップ 2 [Layer3_Outside_name] を右クリックし、[Create Route Profile] をクリックします。

ステップ 3 [Create Route Profile] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドのドロップダウン リストから、適切なルート プロファイルを選択します。
選択内容に応じて、特定の Outside でアドバタイズされている内容が自動的に使用されます。

b) [Type] フィールドで、[Combining Subnets with Routing Policy] を選択します。

c) [Order] を展開します。

ステップ 4 [Create Route Control Context] ダイアログボックスで、次の操作を実行します。

a) [Order] フィールドで、目的の順序の番号を選択します。

b) [Name] フィールドに、ルート制御プライベート ネットワークの名前を入力します。

c) [Match Rule] フィールドのドロップダウン リストで、[Create Match Rule] をクリックします。

d) [Create Match Rule] ダイアログボックスで、[Name] フィールドに、ルート一致ルール名を入力します。
[Submit] をクリックします。
必要に応じて、正規表現による一致コミュニティ条件および一致コミュニティ条件を指定します。一致コミュニティファクタでは、名前、コミュニティ、およびスコープを指定する必要があります。

e) [Set Attribute] ドロップダウン リストから、[Create Action Rule Profile] を選択します。

f) [Create Action Rule Profile] ダイアログボックスの [Name] フィールドに、ルールの名前を入力します。

g) 設定するルールのチェックボックスをオンにし、選択肢として表示されている適切な値を選択します。
[Submit] をクリックします。
ポリシーが作成され、アクション ルールに関連付けられました。

h) [OK] をクリックします。

i) [Create Route Profile] ダイアログボックスで、[Submit] をクリックします。

ステップ 5 [Navigation] ペインで、[Route Profile] > *[route_profile_name]* > *[route_control_private_network_name]* の順に選択します。
[Work] ペインの [Properties] に、ルート プロファイル ポリシーと関連アクション ルール名が表示されます。

ステップ 6 [Navigation] ペインで、[Layer3_Outside_name] をクリックします。
[Work] ペインに、プロパティが表示されます。

ステップ 7 （任意） [Route Control Enforcement] フィールドをクリックし、「Import Control」と入力してインポート ポリシーを有効にします。
インポート制御ポリシーはデフォルトで有効になっていませんが、ユーザが有効にすることができます。インポート制御ポリシーはBGP ではサポートされますが、EIGRP およびOSPF ではサポートされません。ユーザがサポートされていないプロトコルのインポート制御ポリシーを有効にしても、自動的に無視されます。エクスポート制御ポリシーは、BGP、EIGRP、および OSPF でサポートされます。

ステップ 8 カスタマイズされたエクスポート ポリシーを作成するには、[Route Profiles] を右クリックし、[Create Route Profiles] をクリックし、次の操作を実行します。

a) [Create Route Profile] ダイアログボックスで、[Name] フィールドのドロップダウン リストから、エクスポート ポリシーの名前を選択します。
b) ダイアログ ボックスの [+] 記号を展開します。
c) [Create Route Control Context] ダイアログボックスの [Order] フィールドで、値を選択します。
d) [Name] フィールドに、ルート制御プライベート ネットワークの名前を入力します。
e) （任意） [Match Rule] フィールドのドロップダウン リストから、[Create Route Control Context] を選択し、必要に応じて一致ルール ポリシーを作成して付加します。
f) [Set Attribute] フィールドのドロップダウン リストから、[Create Action Rule Profile] を選択します。
または、必要に応じて既存の set アクションを選択し、[Submit] をクリックすることもできます。
g) [Create Action Rule Profile] ダイアログボックスで、[Name] フィールドに、名前を入力します。
h) 設定するルールのチェックボックスをオンにし、選択肢として表示されている適切な値を選択します。[Submit] をクリックします。
[Create Route Control Context] ダイアログ ボックスでは、ポリシーが作成されてアクション ルールに関連付けられています。
i) [OK] をクリックします。
j) [Create Route Profile] ダイアログボックスで、[Submit] をクリックします。

[Work] ペインに、エクスポート ポリシーが表示されます。

（注） エクスポート ポリシーを有効にするには、最初に適用する必要があります。この例では、このポリシーはネットワークのすべてのサブネットに適用されます。

ステップ 9 [Navigation] ペインで、[External Routed Networks] > *[External_Routed_Network_name]* > [Networks] > *[Network_name]* の順に展開し、次の操作を実行します。

a) [Name] フィールドのドロップダウン リストから、前に作成したポリシーを選択します。
b) [Direction] フィールドのドロップダウン リストから、[Route Control Profile] を選択します。[Update] をクリックします。

ステップ 10 [Submit] をクリックします。

REST API を使用した、インポート制御とエクスポート制御を使用するルート制御プロトコルの設定

はじめる前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。
- レイヤ 3 Outside テナント ネットワークが設定されていること。

インポート制御とエクスポート制御を使用するルート制御プロトコルを設定します。

例：

```
<l3extOut descr="" dn="uni/tn-Ten_ND/out-L3Out1" enforceRtctrl="export" name="L3Out1" ownerKey=""
 ownerTag="" targetDscp="unspecified">
        <l3extLNodeP descr="" name="LNodeP1" ownerKey="" ownerTag="" tag="yellow-green"
targetDscp="unspecified">
           <l3extRsNodeL3OutAtt rtrId="1.2.3.4" rtrIdLoopBack="yes" tDn="topology/pod-1/node-101">

               <l3extLoopBackIfP addr="2000::3" descr="" name=""/>
            </l3extRsNodeL3OutAtt>
            <l3extLIfP descr="" name="IFP1" ownerKey="" ownerTag="" tag="yellow-green">
               <ospfIfP authKeyId="1" authType="none" descr="" name="">
                   <ospfRsIfPol tnOspfIfPolName=""/>
               </ospfIfP>
               <l3extRsNdIfPol tnNdIfPolName=""/>
              <l3extRsPathL3OutAtt addr="10.11.12.10/24" descr="" encap="unknown" ifInstT="l3-port"

llAddr="::" mac="00:22:BD:F8:19:FF" mtu="1500" tDn="topology/pod-1/paths-101/pathep-[eth1/17]"
targetDscp="unspecified"/>
            </l3extLIfP>
        </l3extLNodeP>
        <l3extRsEctx tnFvCtxName="PVN1"/>
        <l3extInstP descr="" matchT="AtleastOne" name="InstP1" prio="unspecified"
targetDscp="unspecified">
            <fvRsCustQosPol tnQosCustomPolName=""/>
            <l3extSubnet aggregate="" descr="" ip="192.168.1.0/24" name="" scope=""/>
        </l3extInstP>
        <ospfExtP areaCost="1" areaCtrl="redistribute,summary" areaId="0.0.0.1" areaType="nssa"
descr=""/>
        <rtctrlProfile descr="" name="default-export" ownerKey="" ownerTag="">
            <rtctrlCtxP descr="" name="routecontrolpvtnw" order="3">
                <rtctrlScope descr="" name="">
                    <rtctrlRsScopeToAttrP tnRtctrlAttrPName="actionruleprofile2"/>
                </rtctrlScope>
            </rtctrlCtxP>
        </rtctrlProfile>
    </l3extOut>
```

オブジェクト モデル CLI を使用した、インポート制御とエクスポート制御を使用するルート制御プロトコルの設定

はじめる前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。
- レイヤ 3 Outside テナント ネットワークが設定されていること。

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：

```
admin@apic1:~> cd /aci
```

ステップ 2 ルート プロファイル スコープを入力します。

例：

```
admin@apic1:l3-outside-bgp-ext-out> cd route-profiles/
```

ステップ 3 ルート プロファイルを作成します。

例：

```
admin@apic1:route-profiles> mocreate test-rp
admin@apic1:route-profiles> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/route-profiles/test-rp'
All mos committed successfully.
```

ステップ 4 ルート制御プロファイルのコンテキストを作成し、順序とアクション ルール プロファイルを設定します。

例：

```
admin@apic1:route-profiles> cd test-rp/
admin@apic1:test-rp> cd contexts/
admin@apic1:contexts> mocreate rcctx
admin@apic1:contexts> cd rcctx/
admin@apic1:rcctx> moset order 1

admin@apic1:rcctx> moset action a1
admin@apic1:rcctx> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/route-profiles/test-rp/contexts/rcctx'
All mos committed successfully.
```

ステップ 5 ルート制御適用をエクスポートに設定します。
インポートのルート制御適用は BGP の場合にのみ使用できます。

例：

```
admin@apic1:rcctx> cd ../../../../
admin@apic1:l3-outside-bgp-ext-out> moset enforce-route-control export-control
```

ステップ 6 エクスポート ルート プロファイルを作成し、アクションを設定します。

例：

```
admin@apic1:l3-outside-bgp-ext-out> cd route-profiles
admin@apic1:route-profiles> mocreate export-rp
admin@apic1:route-profiles> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/route-profiles/export-rp'
All mos committed successfully.
admin@apic1:route-profiles> cd export-rp/
admin@apic1:export-rp> cd contexts/
admin@apic1:contexts> mocreate exp-ctx
admin@apic1:contexts> cd exp-ctx/
admin@apic1:exp-ctx> moset action a3
admin@apic1:exp-ctx> moconfig commit

Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/route-profiles/export-rp/contexts/exp-ctx'
All mos committed successfully.
```

ステップ 7 外部 EPG を作成し、目的のルート制御プロファイルを選択します。

例：

```
admin@apic1:networks> mocreate extepg
admin@apic1:networks> cd extepg/
admin@apic1:extepg> ls consumed-contracts  mo provided-contracts  route-control-profiles  subnets
  summary  tags
admin@apic1:extepg> cd route-control-profiles/

admin@apic1:route-control-profiles> mocreate export-rp route-export-policy
admin@apic1:route-control-profiles> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/networks/extepg/route-control-profiles/rp1-route-export-policy'

All mos committed successfully.
```

ACI トランジット ルーティング

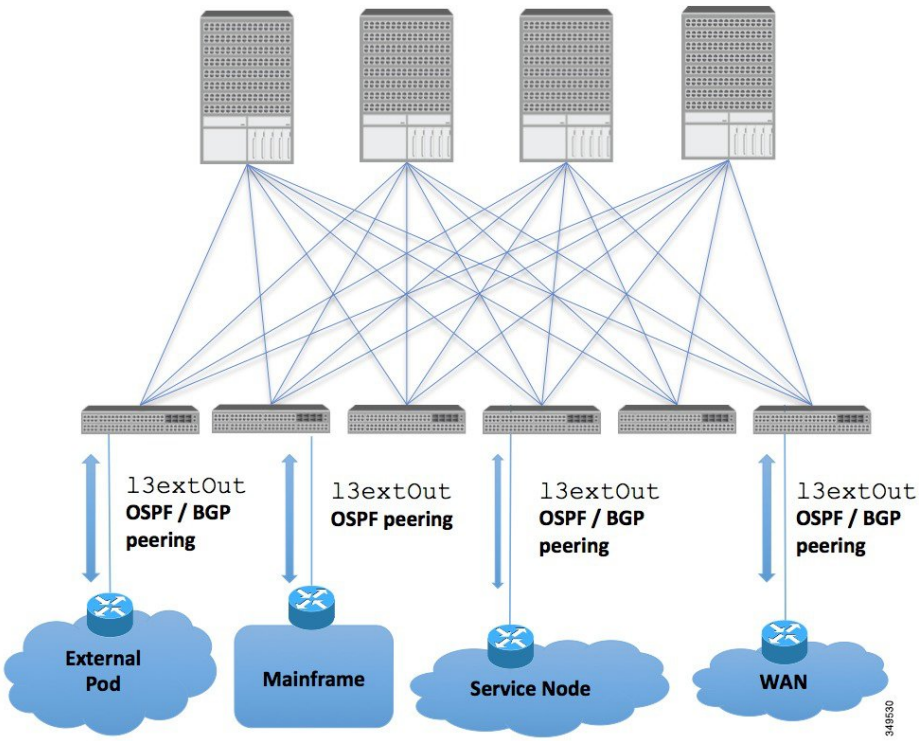
ACI ファブリックは、境界ルータが他のドメインとの双方向再配布を実行できるようにする、トランジット ルーティングをサポートします。トランジット再配布をブロックする ACI ファブリックの以前のリリースのスタブ ルーティング ドメインとは異なり、双方向再配布では、1 つのルーティング ドメインから別のルーティング ドメインにルーティング情報を渡します。そのような再配布により、ACI ファブリックはさまざまなルーティング ドメイン間の完全な IP 接続を提供します。これにより、ルーティング ドメイン間のバックアップ パスを有効にすることで冗長接続を提供することもできます。

最適でないルーティングや、ルーティング ループというさらに重大な問題を回避するように、トランジット再配布ポリシーを設計してください。通常、トランジット再配布は、元のトポロジとリンク状態情報を維持せず、ディスタンス ベクター方式で外部ルートを再配布します（リンクステート プロトコルの場合でもルートはベクター プレフィックスと関連距離としてアドバタイズされます）。このような状況では、ルータが想定外のルーティング ループを形成して、パケットを宛先に配信できなくなる可能性があります。

トランジット ルーティングの使用例

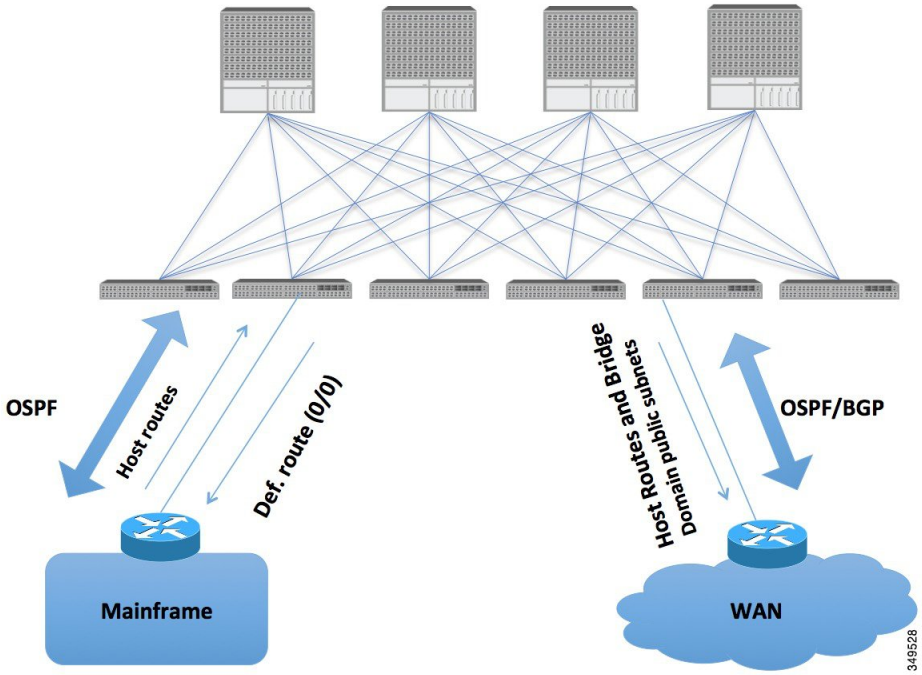
外部ポッド、メインフレーム、サービス ノード、WAN ルータなどの複数のレイヤ 3 ドメインが ACI ファブリックとピアリングして、それらの間のトランジット機能を提供することができます。

図 *29*：レイヤ *3* ドメイン間のトランジット ルーティング



メインフレームは、論理パーティション（LPAR）および仮想 IP アドレッシング（VIPA）の要件に対応する標準 IP ルーティング プロトコルを実行する IP サーバとして機能します。

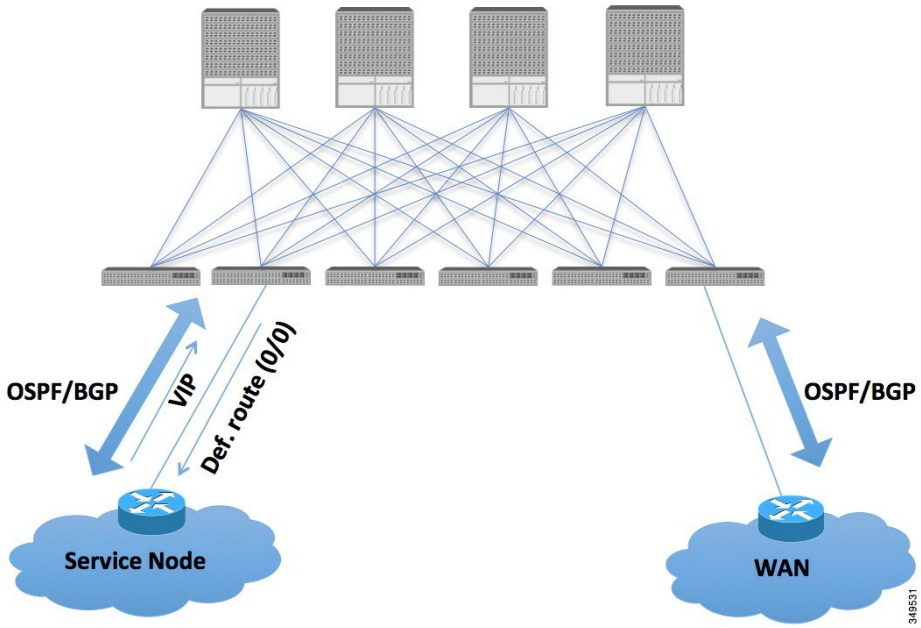
図 *30*：メインフレームのトランジット接続



メインフレームでは、ACI ファブリックが WAN ルータを介した外部ドメインおよびファブリック内の East-West トラフィックのトランジット ドメインである必要がありますが、ホスト ルートがファブリックにプッシュされ、それらのルートがファブリック内および外部インターフェイスに配布されます。

サービス ノードは ACI ファブリックとピアリングし、外部 WAN インターフェイスに再配布される仮想 IP（VIP）ルートをアドバタイズすることができます。

図 *31*：サービス ノードのトランジット接続

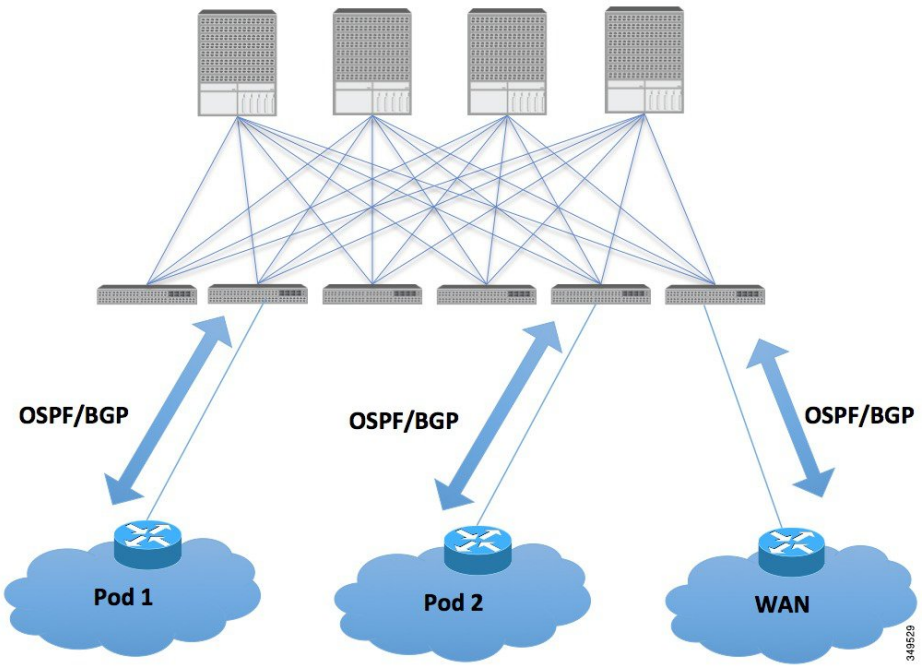


VIP は、特定のサイトやサービスの外部向けの IP アドレスです。VIP は、サービス ノードの背後にある 1 つ以上のサーバまたはノードに関連付けられています。

ACI ファブリックは、外部接続および POD（ポッド）間の相互接続のトランジットとして機能します。クラウドのプロバイダーは、顧客データ センター内に管理対象リソース POD を導入でき

ます。責任分界点は、OSPF および BGP とファブリックとのピアリングが行われている L3Out にすることができます。

図 *32*：複数ポッドのトランジット接続



このようなシナリオでは、ポリシーは責任分界点で管理され、ACI ポリシーを設定する必要はありません。

L4-L7 ルート ピアリングは、ファブリックをトランジットとして使用する特殊なケースであり、ACI ファブリックは他の POD（ポッド）に対する OSPF および BGP のトランジット ドメインの役目を果たします。ルート ピアリングは、L4-L7 サービス デバイスで OSPF および BGP のピアリングを設定し、接続先の ACI リーフ ノードとルートを交換できるようにするために使用されます。ルート ピアリングの一般的な使用例として、SLB VIP が OSPF および iBGP を介して ACI ファブリック外のクライアントにアドバタイズされるルートヘルスインジェクションがあります。このシナリオの設定のウォークスルーについては、付録 H を参照してください。

トランジット ルーティングの概要

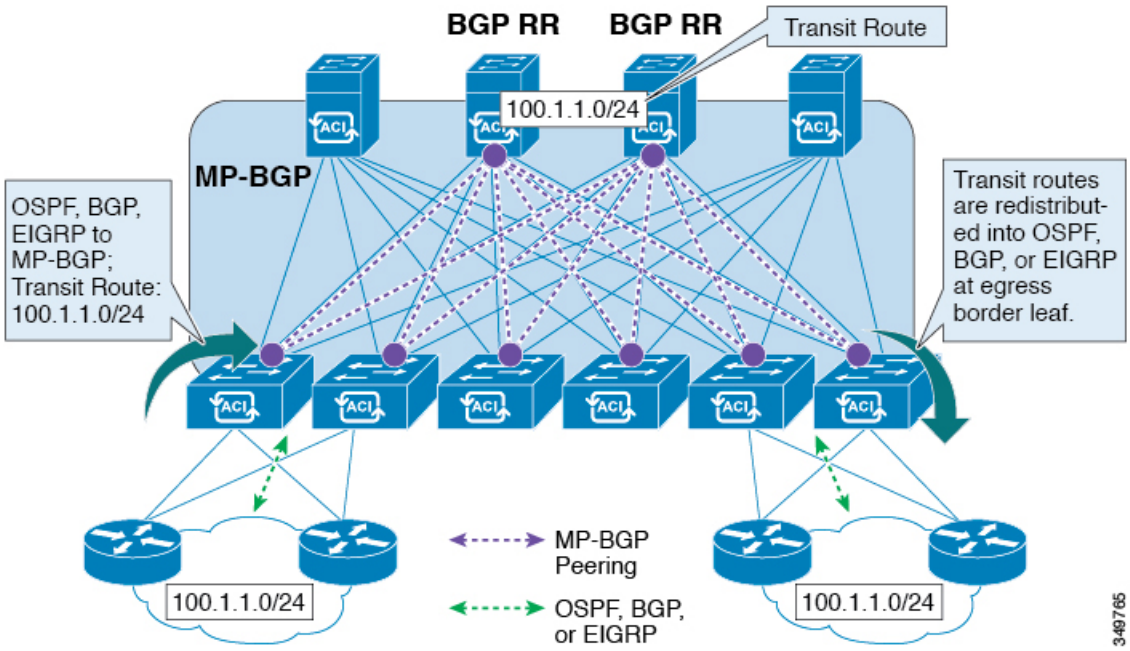
この記事では、Cisco APIC を使用したレイヤ 3 中継ルーティングの概要を示します。

ACI ソフトウェアは、OSPF（NSSA）および iBGP を使用した外部レイヤ 3 接続をサポートします。ACI ファブリックは、外部レイヤ 3 Outside 接続の外部ルータにテナント ブリッジ ドメインのサブネットをアドバタイズします。外部ルータから学習されたルートは、他の外部ルータにアドバタイズされません。ACI ファブリックはスタブ ネットワークと同じように動作し、外部レイヤ 3 ドメイン間のトラフィックの伝送に使用できます。

ACI ソフトウェアでは、トランジット ルーティングのサポートが追加されています。1 つのテナント/コンテキスト（VRF）内で複数の外部レイヤ 3 Outside 接続がサポートされ、ACI ファブリックは 1 つの外部レイヤ 3 Outside 接続から学習されたルートを別の外部レイヤ 3 Outside 接続にアドバタイズすることができます。外部レイヤ 3 ドメインは、リーフ スイッチ（境界リーフ）の ACI ファブリックとピアリングします。ファブリックはピア間の Multiprotocol-Border Gateway Protocol（MP-BGP）中継ドメインです。

外部レイヤ 3 Outside 接続用の ACI ファブリック設定は、テナントおよび VRF レベルで行われます。外部ピアから学習したルートは、VRF ごとに入力リーフの MP-BGP にインポートされます。外部レイヤ 3 Outside 接続から学習したプレフィックスは、テナント VRF が存在するリーフ スイッチにのみエクスポートされます。

図 *33*：トランジット ルーティングの概要を示す図



ACI ファブリック内のルート配布

ACI は以下のルーティング メカニズムをサポートします。

- スタティック ルート
- OSPFv2（IPv4）
- OSPFv3（IPv6）
- iBGP
- eBGP（IPv4 および IPv6）
- EIGRP（IPv4）プロトコル

ACI は、外部ルータに接続する際に VRF-Lite の実装をサポートします。サブインターフェイスを使用して、境界リーフは 1 つの物理インターフェイスを持つ複数のテナントへのレイヤ 3 Outside 接続を提供できます。VRF-Lite の実装では、テナントごとに 1 つのプロトコル セッションが必要です。

ACI ファブリック内の外部ルートを伝播するために、ACI ファブリック内のリーフ スイッチとスパイン スイッチの間に Multiprotocol BGP（MP-BGP）が実装されています。単一ファブリック内で多数のリーフ スイッチをサポートするために、BGP ルート リフレクタ テクノロジーが導入されています。リーフ スイッチとスパイン スイッチはすべて 1 つの BGP 自律システム（AS）内にあります。境界リーフが外部ルートを学習すると、MP-BGP アドレス ファミリ VPN バージョン 4 または VPN バージョン 6 に特定の VRF の外部ルートを再配布できます。アドレス ファミリ VPN バージョン 4 を使用して、MP-BGP は VRF ごとに別の BGP ルーティング テーブルを維持します。MP-BGP 内で、境界リーフは BGP ルート リフレクタであるスパイン スイッチにルートをアドバタイズします。その後、ルートは VRF（APIC GUI の用語ではプライベート ネットワーク）がインスタンス化されているすべてのリーフに伝播されます。

外部レイヤ 3 Outside 接続タイプ

ACI は、以下の外部レイヤ 3 Outside 接続オプションをサポートします。

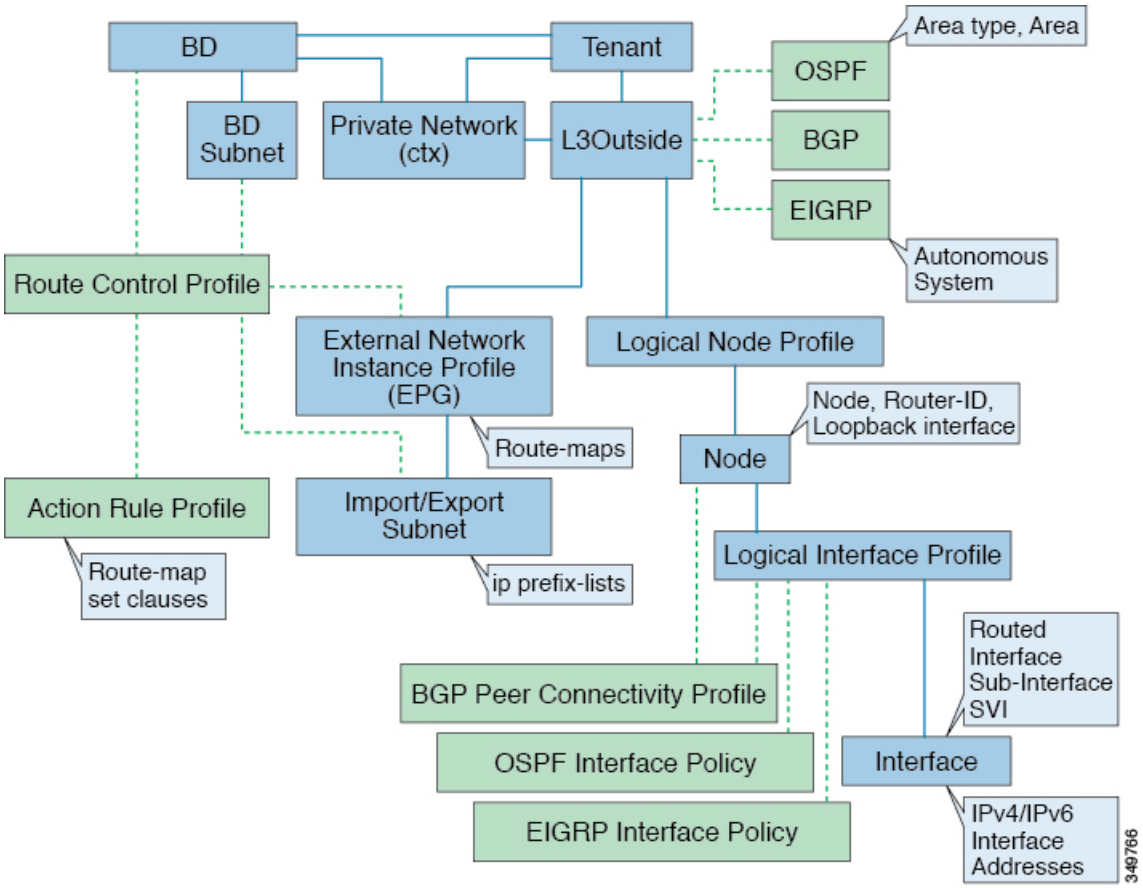
- スタティック ルーティング（IPv4 および IPv6 でサポート）
- 標準および NSSA エリアの OSPFv2（IPv4）
- 標準および NSSA エリアの OSPFv3（IPv6）
- iBGP（IPv4 および IPv6）
- eBGP（IPv4 および IPv6）
- EIGRP（IPv4 のみ）

外部レイヤ 3 Outside 接続は、以下のインターフェイスでサポートされます。

- レイヤ 3 ルーテッド インターフェイス
- 802.1Q タギング対応のサブインターフェイス：サブインターフェイスを使用すると、複数のプライベート ネットワークに対するレイヤ 2 外部接続を提供できます。

- スイッチ仮想インターフェイス（SVI）：SVI インターフェイスを使用すると、レイヤ 2 とレイヤ 3 をサポートする同じ物理インターフェイスをレイヤ 2 外部接続とレイヤ 3 外部接続に使用できます。

図 *34*：*ACI* レイヤ *3* 管理対象オブジェクト



L3Outside 接続に使用される管理対象オブジェクトは、次のとおりです。

- 外部レイヤ 3 Outside（L3ext）：ルーティング プロトコル オプション（OSPF エリア タイプ、エリア、EIGRP AS、BGP）、プライベート ネットワーク、外部物理ドメイン。
- 論理ノード プロファイル：外部レイヤ 3 Outside 接続に対して 1 つ以上のノードが定義されたプロファイル。ルータ ID とループバック インターフェイス設定はプロファイルで定義されます。

（注） 複数の外部レイヤ 3 Outside 接続間の同じノードには同じルータ ID を使用してください。

- 論理インターフェイス プロファイル：IPv4 および IPv6 インターフェイスの IP インターフェイス設定。これは、ルート インターフェイス、ルーテッド サブインターフェイス、および

SVI でサポートされます。SVI は、物理ポート、ポート チャネルまたは VPC で設定できます。

- OSPF インターフェイス ポリシー：OSPF ネットワーク タイプ、優先度など。
- EIGRP インターフェイス ポリシー：タイマー、スプリット ホライズン設定など。
- BGP ピア接続プロファイル：ほとんどの BGP ピア設定、リモート AS、ローカル AS、および BGP ピア接続オプションが設定されるプロファイル。BGP ピア接続プロファイルは、ノードプロファイルの下の論理インターフェイスプロファイルまたはループバック インターフェイスに関連付けることができます。これは、BGP ピアリング セッションの update-source 設定を決定します。
- 外部ネットワーク インスタンス プロファイル（EPG）（l3extInstP）：外部 EPG はプレフィックス ベースの EPG または InstP とも呼ばれます。インポートおよびエクスポートのルート制御ポリシー、セキュリティ インポート ポリシー、およびコントラクトの関連付けは、このプロファイルで定義されます。単一 L3Out に複数の外部 EPG を設定できます。単一外部レイヤ 3 Outside 接続で別のルートまたはセキュリティ ポリシーが定義されている場合、複数の外部 EPG を使用できます。1 つの外部 EPG または複数の外部 EGP がルート マップにまとめられます。外部 EPG で定義されるインポート/エクスポート サブネットは、ルート マップの IP プレフィックス リストの match 句と関連しています。外部 EPG は、インポート セキュリティ サブネットとコントラクトが関連付けられる場所でもあります。これは、この L3out のトラフィックの許可またはドロップに使用されます。
- アクション ルール プロファイル：アクション ルール プロファイルは、L3Out のルート マップの set 句を定義するために使用されます。サポートされる set 句は、BGP communities（standard および extended）、Tags、Preference、Metric、および Metric type です。
- ルート制御プロファイル：ルート制御プロファイルは、アクション ルール プロファイルを参照するために使用されます。これは、アクション ルール プロファイルの順序付きプロファイルにすることができます。ルート制御プロファイルは、テナント BD、BD サブネット、外部 EPG、または外部 EPG サブネットで参照できます。

BGP、OSPF、および EIGRP L3Out 用の追加のプロトコル設定が存在します。これらの設定は、GUI の [ACI Protocol Policies] セクションでテナントごとに設定されます。

サポートされるトランジットの組み合わせのマトリックス

レイヤ 3 Outside 接続タイプ	OSPF	iBGP			eBGP		EIGRP	スタティック ルート
		OSPF 上の iBGP	スタティック ルート上の iBGP	直接接続上の iBGP	OSPF 上の eBGP	直接接続上の eBGP		
OSPF	○	○*	○	×	○	○	○	○

レイヤ 3 Outside 接続タイプ		OSPF	iBGP			eBGP		EIGRP	スタティック ルート
			OSPF 上の iBGP	スタティック ルート上の iBGP	直接接続上の iBGP	OSPF 上の eBGP	直接接続上の eBGP		
iBGP	OSPF 上の iBGP	○*	×	×	×	×	○	×	○
	スタティック ルート上の iBGP	○	×	×	×	×	○	×	○
	直接接続上の iBGP	○	×	×	×	×	○	×	○
eBGP	OSPF 上の eBGP	○	×	×	○	○	×	×	×
	直接接続上の eBGP	○	○	×	○	×	○	×	○
EIGRP		○	×	×	×	×	×	×	
スタティック ルート		○	○	○	○	×	○		○

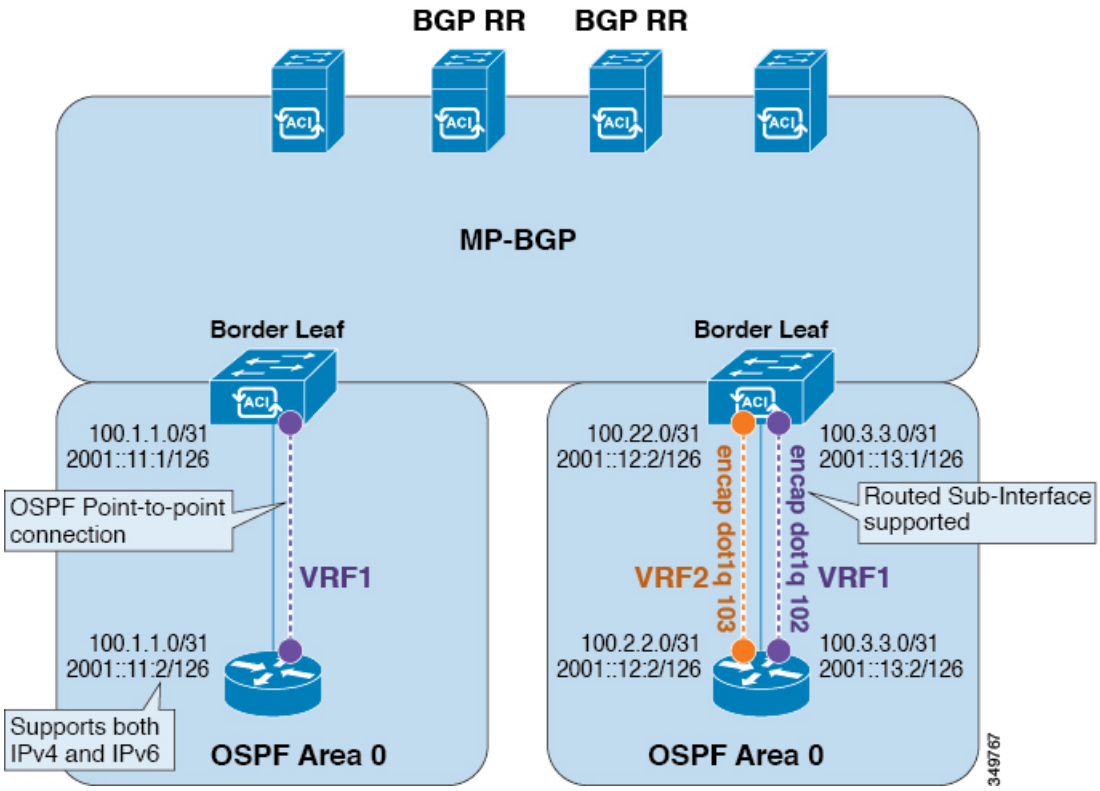
- * = 同じリーフ スイッチではサポートされません
- × = サポートされていないかテストされていない組み合わせ
- **太字 = このリリースでサポートされます**

OSPF レイヤ 3 Outside 接続

OSPF レイヤ 3 Outside 接続は、標準または NSSA エリアです。バックボーン（エリア 0）エリアも、OSPF レイヤ 3 Outside 接続エリアとしてサポートされます。ACI は、IPv4 の OSPFv2 と IPv6 の OSPFv3 の両方をサポートします。OSPF レイヤ 3 Outside を作成するときに、OSPF バージョンを設定する必要はありません。インターフェイス プロファイル設定（IPv4 または IPv6 アドレッシング）に基づいて、正しい OSPF プロセスが自動的に作成されます。IPv4 と IPv6 の両方のプロトコルが同じインターフェイス（デュアルスタック）でサポートされますが、2つの個別インターフェイス プロファイルを作成する必要があります。

レイヤ 3 Outside 接続は、ルーテッド インターフェイス、ルーテッド サブインターフェイス、および SVI でサポートされます。SVI は、L2 と L3 両方のトラフィックで物理接続を共有する必要がある場合に使用されます。SVI は、ポート、ポート チャネル、VPC ポート チャネルでサポートされます。

図 *35*：*OSPF* レイヤ *3 Out* 接続



SVI がレイヤ 3 Outside 接続に使用されると、外部ブリッジ ドメインが境界リーフ スイッチに作成されます。外部ブリッジ ドメインは、ACI ファブリック上の 2 つの VPC スイッチ間の接続を可能にします。これにより、両方の VPC スイッチが、相互の、および外部 OSPF デバイスとの OSPF 隣接関係を確立できます。

ブロードキャスト ネットワークで OSPF を実行する場合、障害が発生したネイバーを検出する時間は dead 間隔（デフォルトは 40 秒）です。障害が発生した後でネイバー隣接関係を再確立する場合にも、代表ルータ（DR）の選定が原因で時間がかかる可能性があります。

（注） 1 つの VPC ノードへのリンクまたはポート チャネルに障害が発生しても、OSPF 隣接関係がダウンすることはありません。OSPF 隣接関係は、その他の VPC ノードを介してアクセスできる外部 BD によりアップ状態を維持することができます。

EIGRP レイヤ 3 Outside 接続

EIGRP レイヤ 3 Outside 接続は、OSPF と同じインターフェイス タイプでサポートされますが、EIGRP では IPv6 はサポートされません。

（注） EIGRP の VPC/SVI 設定は OSPF と同じです。

外部 BGP スピーカーに対する BGP プロトコル ピアリング

ACI は、iBGP と eBGP を使用して境界リーフと外部 BGP スピーカーの間のピアリングをサポートします。ACI は、BGP ピアリングで以下の接続をサポートします。

- OSPF 上の iBGP ピアリング
- OSPF 上の eBGP ピアリング
- 直接接続上の iBGP ピアリング
- 直接接続上の eBGP ピアリング
- スタティック ルート上の iBGP ピアリング

（注） BGP ピアリングで OSPF が使用される場合、OSPF は BGP ピアリング アドレスへのルートの学習とアドバタイズのみに使用されます。レイヤ 3 Outside ネットワーク（EPG）に適用されるすべてのルート制御が BGP プロトコル レベルで適用されます。

ACI は、外部ピアへの iBGP および eBGP 接続用に多数の機能をサポートします。BGP 機能は、[BGP Peer Connectivity Profile] で設定されます。

BGP ピアの接続プロファイル機能について、次の表で説明します。

表 *3*：*BGP* ピアの接続プロファイル機能

BGP 機能	機能の説明	NX-OS での同等のコマンド
Allow Self-AS	Allowed AS Number Count 設定と併用されます。	**allowas-in**
Disable peer AS check	アドバタイズ時のピア AS 番号のチェックを無効にします。	**disable-peer-as-check**
Next-hop self	常にローカル ピア アドレスにネクスト ホップ属性を設定します。	**next-hop-self**

BGP 機能	機能の説明	NX-OS での同等のコマンド
Send community	ネイバーにコミュニティ属性を送信します。	**send-community**
Send community extended	ネイバーに拡張コミュニティ属性を送信します。	**send-community extended**
Password	BGP MD5 認証。	**password**
Allowed AS Number Count	Allow Self-AS 機能と併用されます。	**allowas-in**
Disable connected check	直接接続された EBGP ネイバーの接続チェックを無効にします（EBGP ネイバーがループバックからピアリングすることを許可）。	
TTL	EBGP マルチホップ接続の TTL 値を設定します。これは EBGP でのみ有効です。	**ebgp-multihop <TTL>**
Autonomous System Number	ピアのリモート自律システム番号。	**neighbor <x.x.x.x> remote-as**
Local Autonomous System Number Configuration	ローカル AS 機能を使用するときのオプション（No Prepend+replace-AS+dual-AS など）。	
Local Autonomous System Number	ファブリック MP-BGP ルート リフレクタ プロファイルに割り当てられている AS とは異なる AS 番号をアドバタイズするために使用されるローカル AS 機能。これは EBGP ネイバーの場合にのみサポートされ、ローカル AS 番号がルート リフレクタ ポリシー AS と異なっている必要があります。	**local-as xxx <no-prepend> <replace-as> <dual-as>**

中継ルート制御

ACI ファブリックは、ダイナミック ルーティング プロトコル（OSPF、EIGRP、および BGP）を実行しているテナントおよび VRF ごとに複数の外部レイヤ 3 接続を持つことができます。外部レイヤ 3 Outside 接続から学習したルートまたはスタティック ルートとして設定したルートの配布を制御するために、ACI ファブリックにはルート制御ポリシーが実装されています。ACI はインポート ルート制御とエクスポート ルート制御をサポートします。インポート ルート制御とエクスポート ルート制御は、ルート マップと IP プレフィックス リストを使用して、ACI ファブリックに入ることを許可するプレフィックスおよび ACI ファブリックから外部にアドバタイズされるプレフィックスのインポートとエクスポートを制御します。

インポート ルート制御のデフォルト設定では、すべてのプレフィックスが許可されます。ACI ファブリック内のすべてのリーフ スイッチが、その VRF が導入されているすべての外部プレフィックスを学習します。エクスポート ルート制御のデフォルト設定では、すべてのプレフィックスが拒否されます。インポート ルート制御を有効にすることはできますが、BGP の場合にのみサポートされます。OSPF および EIGRP で学習されたすべてのルートは、レイヤ 3 Outside 接続が導入されている境界リーフ上のそれぞれのプロトコルで許可されます。これらのプレフィックスは、テナントおよび VRF ごとに、入力境界リーフで MP-BGP に再配布（インポート）されます。

インポート ルート制御

- 入力リーフのルーティング テーブルへのプレフィックスのインポートを制御します。
- デフォルトでは、ディセーブルです。
- BGP でのみサポートされます。
- 外部 BGP ネイバーに関連付けられている入力ルート マップを使用して実装されます。

エクスポート ルート制御

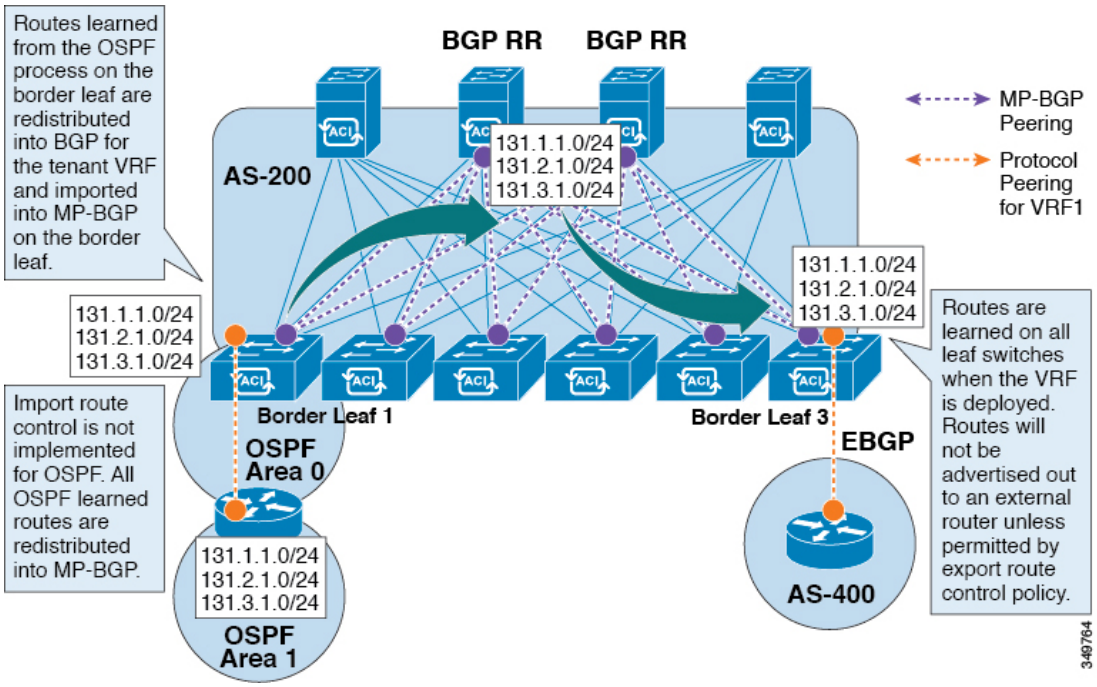
- ACI ファブリックの外部にアドバタイズされる中継プレフィックスのエクスポートを制御します（レイヤ 3 Outside 接続を使用）。
- すべてのレイヤ 3 Outside 接続タイプでサポートされます。
- 常にイネーブルです。
- デフォルト設定ではすべてのプレフィックスが拒否されます。
- 再配布ルート マップ（OSPF および EIGRP）およびネイバー ルート マップ（BGP）を使用して実装されます。
- テナント サブネットまたは元のデフォルト ルートのエクスポートの制御には使用されません。

インポートとエクスポートのルート制御は外部ネットワーク インスタンス プロファイル（l3extInstP）で設定されます。

（注） インポートとエクスポートのルート制御は、中継ルート プレフィックス（外部レイヤ 3 デバイスから学習したルート）およびスタティック ルートのインポートとエクスポートを制御するために使用されます。インポートとエクスポートのルート制御は、テナント サブネット（テナント ブリッジ ドメインに設定されているサブネット）の場合、および発生元がデフォルト ルートである場合は使用されません。

ACI のルート再配布

図 *36*：*ACI* のルート再配布



- 境界リーフの OSPF プロセスで学習されたルートは、テナント VRF 用に BGP に再配布され、それらは境界リーフの MP-BGP にインポートされます。
- インポート ルート制御は OSPF では実装されていません。OSPF で学習されたすべてのルートが MP-BGP に再配布されます。
- ルートは、VRF が導入されている境界リーフで学習されます。ルートは、エクスポート ルート制御で許可されていない限り、外部レイヤ 3 Outside 接続にアドバタイズされません。

レイヤ3Outsideネットワーク インスタンス プロファイルで設定されているサブネットで有効な制御

レイヤ 3 Outside ネットワーク インスタンス プロファイルで設定されているサブネットに対して以下の制御を有効にすることができます。

表 *4*：ルート制御オプション

ルート制御設定	使用目的	オプション
エクスポート ルート制御	外部ピアにアドバタイズされるプレフィックスを許可します。IP プレフィックス リストで実装されます。	特定の一致（プレフィックスとプレフィックス長）。
インポート ルート制御	外部 BGP ピアから受信するプレフィックスを許可します。IP プレフィックス リストで実装されます。	特定の一致（プレフィックスとプレフィックス長）。
セキュリティ インポート サブネット	2つのプレフィックス ベースの EPG 間のパケットを許可します。ACL で実装されます。	ACL のプレフィックスおよびワイルドカードによる一致ルールを使用します。
集約エクスポート	すべてのプレフィックスが外部ピアにアドバタイズされるようにします。0.0.0.0/ le 32 IP プレフィックス リストで実装されます。	0.0.0.0/0 サブネット（すべてのプレフィックス）の場合にのみサポートされます。
集約インポート	外部 BGP ピアから受信するすべてのプレフィックスを許可します。0.0.0.0/0 le 32 IP プレフィックス リストで実装されます。	0.0.0.0/0 サブネット（すべてのプレフィックス）の場合にのみサポートされます。

多くの場合、レイヤ 3 Outside 接続にすべての中継ルートをアドバタイズすることが優先されます。この場合、集約エクスポート オプションがプレフィックス 0.0.0.0/0 で使用されます。これにより、エクスポート ルート マップの match 句として設定された IP プレフィックス リスト エントリ（permit 0.0.0.0/0 le 30）が作成されます。出力を表示するには、**show route-map <outbound route-map>** コマンドと **show ip prefix-list <match-clause>** を使用します。

ファブリック外へのテナント BD サブネットのアドバタイズ

インポートおよびエクスポートのルート制御ポリシーは、中継ルート（他の外部ピアから学習したルート）およびスタティック ルートのみに適用されます。テナント BD サブネット上に設定されているファブリック内部のサブネットは、エクスポートポリシーサブネットを使用して外部にアドバタイズされません。IP プレフィックス リストおよびルート マップを使用すると IP テナントサブネットは許可されますが、これらは別の設定手順を使用して実装されます。テナントサブネットをファブリックの外部にアドバタイズする場合は、次の設定手順を参照してください。

ステップ 1 [subnet properties] ウィンドウで、テナント サブネットのスコープを [Public Subnet] として設定します。

ステップ 2 （任意） [subnet properties] ウィンドウで、[Subnet Control] を [ND RA Prefix] として設定します。

ステップ 3 テナント ブリッジ ドメイン（BD）を外部レイヤ 3 Outside に関連付けます。

ステップ 4 テナント EPG と外部 EPG 間のコントラクト（プロバイダー/コンシューマ）の関連付けを作成します。BD サブネットをスコープ [Public] に設定し、BD をレイヤ 3 Outside に関連付けると、BD サブネット プレフィックスの境界リーフに IP プレフィックスおよびルート マップの連続エントリが作成されます。

テナント EPG からレイヤ 3 Outside へのコントラクト

テナント EPG では、コントラクトのプロバイダーおよびコンシューマをレイヤ 3 Outside 接続に関連付ける必要があります。この関連付けにより、境界リーフにサブネットのルート エントリが作成され（テナント BD がまだリーフに導入されていない場合）、データ プレーンでのトラフィックを許可するためにも使用されます。

状況によっては、コントラクトを設定していなくてもテナント サブネットを外部ピアにアドバタイズできます。テナント サブネットは、次のいずれかの条件に該当すると外部にアドバタイズされます。

- テナント EPG および BD がすでに境界リーフに導入されている。
- テナント EPG および BD に、境界リーフに導入されているテナントおよび EPG とのコントラクトがある。

これら 2 つの条件に該当するとテナント サブネットのルーティング テーブルにエントリが作成され、パブリック スコープとレイヤ 3 Outside の関連付けによりサブネットを外部にアドバタイズできますが、コントラクトがないとデータ プレーン トラフィックは許可されません。

（注） このエントリは、Policy Control Enforcement を enforced に設定してテナント プライベート ネットワーク（コンテキスト）が設定されている場合にのみ有効です。Policy Control Enforcement が unenforced に設定されている場合、テナント プレフィックスはコントラクトなしで境界リーフに存在します。

デフォルト ルートのアドバタイズ

デフォルト ルートのみを必要とするファブリックへの外部接続の場合、OSPF、EIGRP、および BGP のレイヤ 3 Outside 接続をデフォルト ルートの起点とすることがサポートされます。外部ピアからデフォルトルートが受信されると、この文書で説明されている中継エクスポートルート制御に従って、このルートを別のピアに再配布できます。

デフォルト ルートは、デフォルト ルート リーク ポリシーを使用してアドバタイズすることもできます。このポリシーは、デフォルトルートがルーティングテーブル内にあるか、または常にデフォルトルートをアドバタイズすることがサポートされている場合、デフォルトルートのアドバタイズをサポートします。デフォルト ルート リーク ポリシーは、レイヤ 3 Outside 接続で設定されます。

デフォルト ルート リーク ポリシーを作成するときは、以下のガイドラインに従います。

- BGP の場合、[Always] プロパティは適用されません。
- BGP の場合、[Scope] プロパティを選択するときに [Outside] を選択する必要があります。
- OSPF の場合、[Scope] 値 [Context] はタイプ 5 LSA を作成しますが、[Scope] 値 [Outside] はタイプ 7 LSA を作成します。この選択は、そのレイヤ 3 Outside で使用されているエリア タイプによって異なります。したがって、エリア タイプが [regular] である場合はスコープを [Context] に設定し、エリア タイプが [NSSA] である場合はスコープを [Outside] に設定します。

ルート制御プロファイル ポリシー

ACI ファブリックは、ファブリックの内部と外部にアドバタイズされるルート用に、ルート マップの set 句もサポートします。ルート マップの set ルールは、ルート制御プロファイル ポリシーとアクション ルール プロファイルで設定されます。

ACI は以下の set オプションをサポートします。

表 *5*：アクション ルール プロファイルのプロパティ（ルートマップの *set* 句）

プロパティ	OSPF	EIGRP	BGP	注
Set Community			○	標準コミュニティと拡張コミュニティをサポートします。
Route Tag	○	○		BD のサブネットのみでサポートされます。中継プレフィックスには、常にタグ 4294967295 が割り当てられます。
Preference			○	BGP ローカル プリファレンスを設定します。
メトリック	○		○	BGP の MED を設定します。EIGRP のメトリックを変更しますが、EIGRP 複合メトリックは指定できません。
Metric Type	○			OSPF タイプ 1 と OSPF タイプ 2。

ルートプロファイルポリシーは、レイヤ3Outside接続の下に作成されます。ルート制御ポリシーは、以下のオブジェクトで参照できます。

- テナント BD サブネット
- テナント BD
- 外部 EPG
- 外部 EPG のインポート/エクスポート サブネット

以下に、BGP のインポート ルート制御を使用し、2 つの異なるレイヤ 2 Outside から学習した外部ルートのローカル プリファレンスを設定する例を示します。AS300 への外部接続用のレイヤ 3 Outside接続は、インポートルート制御を適用して設定されています。アクションルールプロファ

イルの設定では、[Local Preference] ウィンドウの [Action Rule Profile] でローカル プリファレンスが 200 に設定されています。

レイヤ 3 Outside 接続の外部 EPG は、0.0.0.0/0 インポート集約ポリシーを使用してすべてのルートを許可するように設定されています。これは、インポート ルート制御が適用されていますが、どのプレフィックスもブロックされてはならないためです。ローカル プリファレンスの設定を許可するために、インポート ルート制御が適用されています。また、[Route Control Profile] ウィンドウの [External EPG] で [Action Rule Profile] を参照するルート プロファイルを使用して、別のインポート サブネット 151.0.1.0/24 が追加されています。

MP-BGP テーブルを表示するには、**show ip bgp vrf overlay-1** コマンドを使用します。スパインの MP-BGP テーブルには、プレフィックス 151.0.1.0/24 とローカルプリファレンス 200、および BGP 300 レイヤ 3 Outside 接続の境界リーフの次のホップが表示されます。

default-import と default-export という、2 つの特殊なルート制御プロファイルがあります。名前 default-import および default-export を使用して設定すると、ルート制御プロファイルはインポートとエクスポート両方のレイヤ 3 Outside レベルで自動的に適用されます。default-import および default-export のルート制御プロファイルは、0.0.0.0/0 集約を使用して設定することはできません。

ルート制御プロファイルは、次の順序でファブリック ルートに適用されます。

1. テナント BD サブネット
2. テナント BD
3. レイヤ 3 Outside

ルート制御プロファイルは、次の順序で中継ルートに適用されます。

1. 外部 EPG プレフィックス
2. 外部 EPG
3. レイヤ 3 Outside

セキュリティ インポート ポリシー

本書で説明されているポリシーでは、ACI ファブリックの内外へのルーティング情報の交換、およびルートの制御とタグ付けに使用する方法を取り扱ってきました。ACI ファブリックはホワイトリスト モデルで動作します。この場合のデフォルトの動作では、ポリシーで明示的に許可されない限り、エンドポイント グループ間のすべてのデータ プレーン トラフィックがドロップされます。このホワイトリスト モデルは外部 EPG とテナント EPG に適用されます。

中継トラフィックの場合、テナント トラフィックと比較すると、セキュリティ ポリシーの設定方法と実装方法が少し異なります。

中継セキュリティ ポリシー

- プレフィックス フィルタリングを使用します。
- Ethertype、プロトコル、L4 ポート、および TCP フラグ フィルタはサポートしません。
- セキュリティ インポート サブネット（プレフィックス）と外部 EPG で設定されたコントラクトを使用して実装されます。

テナント EPG セキュリティ ポリシー

- プレフィックス フィルタリングを使用しません。
- Ethertype、プロトコル、L4 ポート、および TCP フラグ フィルタをサポートします。
- テナント EPG←→EPG およびテナント EPG←→外部 EPG でサポートされます。

外部プレフィックスベースの EPG 間にコントラクトがなければ、トラフィックはドロップされます。2 つの外部 EPG 間のトラフィックを許可するには、コントラクトとセキュリティ プレフィックスを設定する必要があります。プレフィックス フィルタリングのみがサポートされるため、デフォルト フィルタを使用できます。

外部レイヤ 3 Outside 接続のコントラクト

レイヤ 3 Outside 接続が導入されているすべてのリーフ ノードで、各レイヤ 3 Outside 接続のプレフィックスの結合がプログラムされます。3 つ以上のレイヤ 3 Outside 接続が導入されている場合、キャッチオール ルール 0.0.0.0/0 を使用すると、コントラクトを持たないレイヤ 3 Outside 接続間のトラフィックが許可されます。

プロバイダー/コンシューマのコントラクト関連付けとセキュリティ インポート サブネットの設定は、外部レイヤ 3 Outside 接続のインスタンス プロファイル（instP）で行われます。

セキュリティ インポート サブネットが設定されており、キャッチオール ルール 0.0.0.0/0 がサポートされている場合、セキュリティ インポート サブネットは ACL タイプのルールに従います。セキュリティ インポート サブネットのルール 10.0.0.0/8 は 10.0.0.0～10.255.255.255 の範囲のすべてのアドレスに一致します。ルート制御サブネットで許可されているプレフィックスに対して正確なプレフィックス照合を設定する必要はありません。

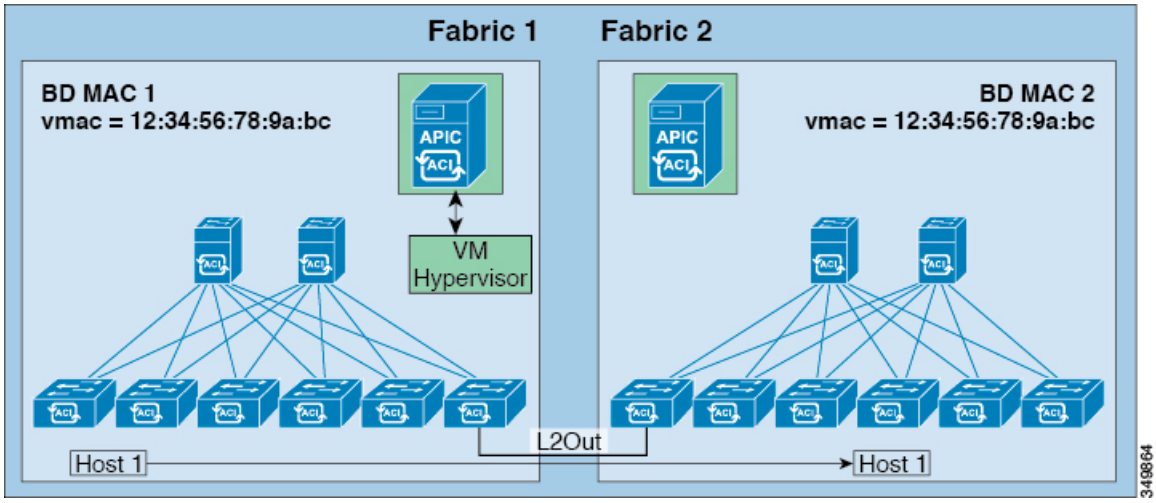
3 つ以上のレイヤ 3 Outside 接続が同じ VRF 内に設定されている場合は、ルールの結合を理由として、セキュリティ インポート サブネットを設定するときに注意する必要があります。

共通パーベイシブ ゲートウェイ

ブリッジ ドメインごとに IPv4 共通ゲートウェイを使用して複数の ACI ファブリックを設定できます。これにより、1 つ以上の仮想マシン（VM）または従来のホストを、ホストがその IP アドレスを保持したままファブリック間で移動できます。ファブリック間の VM ホストの移動は、VM ハイパーバイザによって自動的に行うことができます。ACI ファブリックは、同じ場所に配置することも、複数のサイト間でプロビジョニングすることもできます。ACI ファブリック間のレイ

ヤ 2 接続は、ローカル リンクか、ルーテッド WAN リンクになります。次の図は、基本的な共通パーベイシブ ゲートウェイ トポロジを示しています。

図 *37* : *ACI* 複数ファブリック共通パーベイシブ ゲートウェイ



ブリッジ ドメインごとの共通パーベイシブ ゲートウェイの設定要件は、次のとおりです。

- 各ファブリックのブリッジ ドメイン MAC（*mac*）値は一意である必要があります。

（注） デフォルトのブリッジ ドメイン MAC（*MAC*）アドレス値はすべての ACI ファブリックで同じです。共通パーベイシブ ゲートウェイでは、管理者は、ブリッジ ドメイン MAC（*mac*）値が各 ACI ファブリックで一意になるように設定する必要があります。

- ブリッジ ドメインの仮想 MAC（*vmac*）アドレスとサブネットの仮想 IP アドレスは、ブリッジ ドメインのすべての ACI ファブリックで同じにする必要があります。複数のブリッジ ドメインを、接続されている ACI ファブリック間で通信するように設定できます。仮想 MAC アドレスと仮想 IP アドレスは、ブリッジ ドメイン間で共有できます。

GUI を使用した共通パーベイシブ ゲートウェイの設定

はじめる前に

- テナントおよび VRF が作成されていること。
- ブリッジ ドメインの仮想 MAC アドレスとサブネットの仮想 IP アドレスは、ブリッジ ドメインのすべての ACI ファブリックで同じにする必要があります。複数のブリッジ ドメインを、接続されている ACI ファブリック間で通信するように設定できます。仮想 MAC アドレスと仮想 IP アドレスは、ブリッジ ドメイン間で共有できます。

- ACI ファブリック間で通信するように設定されているブリッジ ドメインは、フラッドモードである必要があります。
- ブリッジ ドメインの 1 つの EPG のみを（BD に複数の EPG がある場合）、2 つ目のファブリックに接続されているポートの境界リーフ上に設定する必要があります。
- 2 つの ACI ファブリック間のパーベイシブ共通ゲートウェイを有効にする相互接続されたレイヤ 2 ネットワークには、ホストを直接接続しないでください。

ステップ 1 メニュー バーで、[TENANTS] をクリックします。

ステップ 2 [Navigation] ペインで、*[Tenant_name]* > [Networking] > [Bridge Domains] の順に展開します。

ステップ 3 [Bridge Domains] を右クリックし、[Create Bridge Domain] をクリックします。

ステップ 4 [Create Bridge Domain] ダイアログボックスで、次の操作を実行し、適切な属性を選択します。

a) [Name] フィールドに、ブリッジ ドメインの名前を入力します。

b) [Subnets] を展開し、[Create Subnets] ダイアログボックスの [Gateway IP] フィールドに IP アドレスを入力します。[Treat as virtual IP address] フィールドで、チェックボックスをオンにします。[Ok] をクリックし、[Finish] をクリックします。

c) もう一度 [Subnets] を展開し、仮想 IP アドレスとして設定されているものと同じサブネットを使用して、[Create Subnets] ダイアログボックスの [Gateway IP] フィールドで物理 IP アドレスを作成します。

（注） 物理 IP アドレスは ACI ファブリック全体で一意である必要があります

ステップ 5 [Work] ペインで作成した物理ドメインをダブルクリックし、次の操作を実行します。

a) [Virtual MAC Address] フィールドをクリックし、[not-applicable] を適切な値に変更します。[Submit] をクリックします。

（注） デフォルト BD の MAC アドレス値はすべての ACI ファブリックで同じです。この設定では、ブリッジ ドメイン MAC 値が各 ACI ファブリックで一意である必要があります。

各ファブリックのブリッジ ドメイン MAC（pmac）値が一意であることを確認してください。

ステップ 6 BD をその他のファブリックに拡張するために、L2out EPG を作成します。これを行うには、[External Bridged Networks] を右クリックして [Create Bridged Outside] ダイアログを開き、次の操作を実行します。

a) [Name] フィールドに、ブリッジされる Outside の名前を入力します。

b) [Bridge Domain] フィールドで、すでに作成されているブリッジ ドメインを選択します。

c) [Encap] フィールドに、その他のファブリック l2out カプセル化に一致する VLAN カプセル化を入力します。

d) [Path Type] フィールドで、[Port]、[PC]、または [VPC] を選択して EPG を導入し、[Next] をクリックします。

e) 外部 EPG ネットワークを作成するには、[Name] フィールドをクリックしてネットワークの名前を入力し（QoS クラスの指定も可能）、[Finish] をクリックして共通パーベイシブ設定を完了します。

REST API を使用した共通パーベイシブ ゲートウェイの設定

はじめる前に

- テナント、VRF、およびブリッジ ドメインが作成されていること。

共通パーベイシブ ゲートウェイを設定します。

例：

```
<!-Things that are bolded only matters-->
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
  <fvTenant name="test">
    <fvCtx name="test"/>

    <fvBD name="test" vmac="12:34:56:78:9a:bc">
      <fvRsCtx tnFvCtxName="test"/>
      <!-- Primary address -->
      <fvSubnet ip="192.168.15.254/24" preferred="yes"/>
      <!-- Virtual address -->
      <fvSubnet ip="192.168.15.1/24" virtual="yes"/>
    </fvBD>

    <fvAp name="test">
      <fvAEPg name="web">
        <fvRsBd tnFvBDName="test"/>
        <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/3]" encap="vlan-1002"/>
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>
```

CLI を使用した共通パーベイシブ ゲートウェイの設定

はじめる前に

- テナント、VRF、およびブリッジ ドメインが作成されていること。

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：

```
admin@apic1:~> cd /aci
```

ステップ 2 共通パーベイシブ ゲートウェイを設定します。

例：

```
apic1#configure
apic1(config)#tenant demo
apic1(config-tenant)#bridge-domain test
apic1(config-tenant-bd)#l2-unknown-unicast flood
apic1(config-tenant-bd)#arp flooding
apic1(config-tenant-bd)#exit

apic1(config-tenant)#interface bridge-domain test
apic1(config-tenant-interface)#multi-site-mac-address 12:34:56:78:9a:bc
apic1(config-tenant-interface)#mac-address 00:CC:CC:CC:C1:01 (Should be unique for each ACI fabric)
apic1(config-tenant-interface)#ip address 192.168.10.1/24 multi-site
apic1(config-tenant-interface)#ip address 192.168.10.254/24 (Should be unique for each ACI fabric)
```

索 引

え

こ

て

と

ふ

へ

り

ろ