



基本 GUI の使用

この章の内容は、次のとおりです。

- [基本および拡張 GUI モード間の切り替え, 1 ページ](#)
- [APIC の準備の例について, 2 ページ](#)
- [APIC によるスイッチ検出, 2 ページ](#)
- [ネットワーク タイム プロトコルの設定, 6 ページ](#)
- [ユーザアカウントの作成, 9 ページ](#)
- [基本 GUI の 管理アクセスの追加, 14 ページ](#)
- [VMM ドメインの設定, 17 ページ](#)
- [テナント、VRF、およびブリッジ ドメインの作成, 23 ページ](#)
- [サーバまたはサービス ポリシーの設定, 25 ページ](#)
- [テナントの外部接続の設定, 32 ページ](#)
- [アプリケーション ポリシーの展開, 36 ページ](#)

基本および拡張 GUI モード間の切り替え

APIC GUI にログインすると、現在の GUI モードを確認できます。GUI の右上隅に現在のモードが表示されます。次のどちらのモードで動作するかを選択することができます。

注意：シスコでは、コンフィギュレーションモード（拡張または基本）を混在させないことをお勧めします。いずれかのモードで設定を作成し、他方のモードを使用して設定を変更すると、意図しない変更が発生する可能性があります。たとえば、拡張モードを使用して2つのポートにインターフェイス ポリシーを適用し、次に基本モードを使用して1つのポートの設定を変更すると、変更内容が両方のポートに適用される可能性があります。

- 基本モード：基本モードで実行するタスクについては、「[基本 GUI を使用した APIC の開始](#)」の章を参照してください。

- 拡張モード：拡張モードで実行するタスクについては、「拡張 GUI を使用した APIC の開始」の章を参照してください。

次のようにして 1 つの GUI モードから他のモードに変更またはモード間を切り替えることができます。

- 1 GUI で、[welcome, <login_name>] ドロップダウンリストをクリックし、[Toggle GUI Mode] を選択します。
- 2 [Warning] ダイアログボックスで、[Yes] をクリックします。
- 3 アプリケーションがロードを完了し、変更されたモードで GUI が表示されるのを待ちます。

APIC の準備の例について

このマニュアルのいくつかの例の手順には、パラメータ名が含まれています。これらのパラメータ名は、便宜上理解しやすいように例として提供されるもので、それらを使用する必要はありません。

APIC によるスイッチ検出

APIC は、ACI ファブリックの一部であるすべてのスイッチに対する自動プロビジョニングおよび管理の中心となるポイントです。単一のデータセンターには、複数の ACI ファブリックを組み込むことができます。各データセンターは、自身の APIC クラスタとファブリックの一部である Cisco Nexus 9000 シリーズ スイッチを持つことができます。スイッチが単一の APIC クラスタによってのみ管理されるようにするには、各スイッチがファブリックを管理するその特定の APIC クラスタに登録される必要があります。

APIC は、現在管理している任意のスイッチに直接接続されている新規スイッチを検出します。クラスタ内の各 APIC インスタンスは、直接接続されているリーフ スイッチのみを最初に検出します。リーフ スイッチが APIC で登録されると、APIC はリーフ スイッチに直接接続されているすべてのスパイン スイッチを検出します。各スパイン スイッチが登録されると、その APIC はそのスパイン スイッチに接続されているすべてのリーフ スイッチを検出します。このカスケード化された検出により、APIC は簡単なわずかな手順でファブリック トポロジ全体を検出することができます。

APIC クラスタによるスイッチ登録



- (注) スイッチを登録する前に、ファブリック内のすべてのスイッチが物理的に接続され、適切な設定で起動されていることを確認します。シャーシの設置については、<http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/products-installation-guides-list.html> を参照してください。

スイッチが APIC で登録されると、そのスイッチは APIC で管理されるファブリック インベントリの一部となります。アプリケーションセントリック インフラストラクチャファブリック (ACI ファブリック) を使用すると、APIC はインフラストラクチャ内のスイッチのプロビジョニング、管理、およびモニタリングのシングル ポイントとなります。



(注) インフラストラクチャの IP アドレス範囲は、インバンドおよびアウトオブバンドのネットワーク用の ACI ファブリックで使用する他の IP アドレスと重複してはなりません。

GUI を使用した未登録スイッチの登録



(注) インフラストラクチャの IP アドレス範囲は、インバンドおよびアウトオブバンドのネットワーク用の ACI ファブリックで使用する他の IP アドレスと重複してはなりません。



(注) このタスク例のビデオを視聴するには、[Videos Webpage](#) を参照してください。

はじめる前に

ファブリック内のすべてのスイッチが物理的に接続され、起動されていることを確認します。

手順

-
- ステップ 1** メニュー バーで、[FABRIC] > [INVENTORY] を選択します。
- ステップ 2** [Navigation] ペインで、[Fabric Membership] をクリックします。
[Work] ペインの [Fabric Membership] テーブルで、単一のリーフ スイッチが ID 0 として表示されます。それが apic1 に接続されているリーフ スイッチです。
- ステップ 3** リーフ スイッチの行をダブルクリックし、次の操作を実行して、ID を設定します。
- [ID] フィールドで、適切な ID を追加します (leaf1 は ID 101、leaf2 は ID 102)。
ID は、100 より大きい数である必要があります。最初の 100 の ID は APIC アプライアンス ノード用です。
 - [Switch Name] フィールドで、スイッチの名前を追加し、[Update] をクリックします。
(注) ID が割り当てられた後は、更新できません。スイッチ名は、名前をダブルクリックし、[Switch Name] フィールドを更新することによって更新できます。
- IP アドレスがスイッチに割り当てられ、[Navigation] ペインで、スイッチがポッドの下に表示されます。
- ステップ 4** 1 つ以上のスパイン スイッチが表示されるまで [Work] ペインをモニタします。
- ステップ 5** スパイン スイッチの行をダブルクリックし、次の操作を実行して、ID を設定します。
- [ID] フィールドで、適切な ID を追加します (spine1 は ID 203、spine 2 は ID 204)。

(注) リーフノードとスパインノードには異なる数字をつけることをお勧めします。たとえば、スパインの数字を 100 の範囲、リーフの数字を 200 の範囲とします。

b) [Switch Name] フィールドで、スイッチの名前を追加し、[Update] をクリックします。

IP アドレスがスイッチに割り当てられ、[Navigation] ペインで、スイッチがポッドの下に表示されます。次の手順に進む前に、残りのすべてのスイッチが [Node Configurations] テーブルに表示されるまで待機します。

ステップ 6 [Fabric Membership] テーブルにリストされる各スイッチに対し、次の手順を実行します。

a) スイッチをダブルクリックし、ID と名前を入力し、[Update] をクリックします。

b) リストの次のスイッチに対して繰り返し行います。

APIC からのスイッチ検出の検証とスイッチ管理

スイッチが APIC で登録された後、APIC はファブリック トポロジ ディスカバリを自動的に実行し、ネットワーク全体のビューを取得し、ファブリック トポロジ内のすべてのスイッチを管理します。

各スイッチは、個々にアクセスせずに、APIC から設定、モニタ、およびアップグレードできます。

GUI を使用した登録スイッチの検証



(注) このタスク例のビデオを視聴するには、[Videos Webpage](#) を参照してください。

手順

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

ステップ 2 [Navigation] ペインで、[Fabric Membership] を展開します。ファブリック内のスイッチがノード ID とともに表示されます。[Work] ペインに、登録されているすべてのスイッチが割り当てられた IP アドレスとともに表示されます。

ファブリック トポロジの検証

すべてのスイッチが APIC クラスタに登録された後、APIC はファブリック内のすべてのリンクおよび接続を自動的に検出し、その結果トポロジ全体を検出します。

GUI を使用したファブリック トポロジの検証



(注) このタスク例のビデオを視聴するには、[Videos Webpage](#) を参照してください。

手順

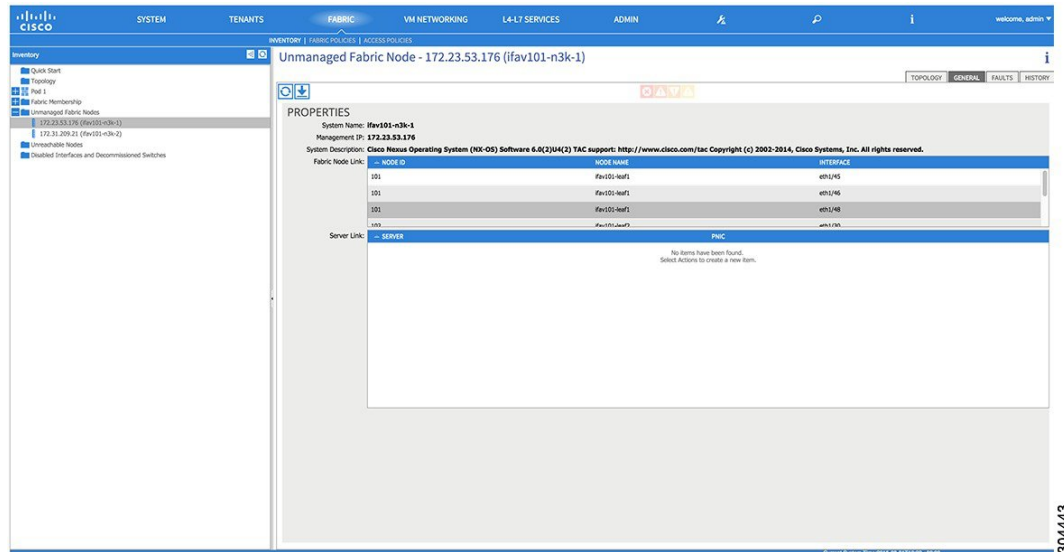
- ステップ 1 メニューバーで、[FABRIC] > [INVENTORY] を選択します。
- ステップ 2 [Navigation] ペインで、表示したいポッドを選択します。
- ステップ 3 [Work] ペインで、[TOPOLOGY] タブをクリックします。
表示された図は、すべての接続されたスイッチ、APIC インスタンスおよびリンクを示します。
- ステップ 4 (任意) リーフスイッチまたはスパインスイッチのポートレベルの接続を表示するには、トポロジ図のアイコンをダブルクリックします。
トポロジ図に戻るには、[Work] ペインの左上隅にある [Previous View] アイコンをクリックします。
- ステップ 5 (任意) トポロジ図を更新するには、[Work] ペインの左上隅にある [Refresh] アイコンをクリックします。

VM 管理でのアンマネージドスイッチの接続

VM コントローラ（たとえば、vCenter）によって管理されているホストは、レイヤ 2 スイッチを介してリーフポートに接続できます。必要な唯一の前提条件は、レイヤ 2 スイッチを管理アドレスで設定することです。この管理アドレスは、スイッチに接続されているポート上で Link Layer Discovery Protocol (LLDP) または Cisco Discovery Protocol (CDP) によってアドバタイズされる必要があります。レイヤ 2 スイッチは、APIC によって自動的に検出され、管理アドレスで識別さ

れます。次の図は、[Fabric]>[Inventory] ビューにアンマネージド スイッチを表示する APIC GUI を示します。

図 1: APIC ファブリック インベントリのアンマネージド レイヤ 2 スイッチ



ネットワーク タイム プロトコルの設定

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ル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、エラーやヘルル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ともに展開する場合、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ともに展開する場合は、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。

NTP over IPv6

NTP over IPv6 アドレスは、ホスト名とピアアドレスでサポートされます。gai.conf も、IPv4 アドレスのプロバイダーまたはピアの IPv6 アドレスが優先されるように設定できます。ユーザは、IP アドレス（インストールまたは優先順位によって IPv4、IPv6、または両方）を提供することによって解決できるホスト名を設定できます。

基本 GUI を使用した NTP の設定

はじめる前に

手順

-
- ステップ 1** メニュー バーで、[System] > [System Settings] の順に選択します。
- ステップ 2** [Navigation] ペインで、[NTP] をクリックします。
- ステップ 3** [Work] ペインに、デフォルトの NTP ポリシー プロパティが表示されます。
- ステップ 4** [NTP Server] フィールドで、[+] 記号を展開して [Create Providers] ダイアログボックスを表示します。
- ステップ 5** [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。
-

CLI を使用した、各ノードに導入された NTP ポリシーの確認

手順

-
- 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。

ユーザ アカウントの作成

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。

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。

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、[Videos Webpage](#) 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

-
- 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。

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)"
```

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

手順

- ステップ 1** メニューバーで、[ADMIN] > [AAA] の順をクリックします。
- 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。

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

外部認証サーバの AV ペアを設定します。

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)
```

GUI を使用したリモート ユーザの設定



(注) このタスク例のビデオを視聴するには、[Videos Webpage](#) を参照してください。

はじめる前に

- DNS 設定は、ファブリック コントローラがサーバに到達できるように、RADIUS サーバ ホスト名を解決している必要があります。
- APIC には、RADIUS サーバに到達できるように、外部管理サブネット ポリシーを設定しておく必要があります。

手順

-
- ステップ 1** メニューバーで、[ADMIN]>[AAA] を選択します。[Navigation] ペインで、[RADIUS Management] を展開します。
- ステップ 2** [RADIUS Providers] を右クリックし、[Create RADIUS Provider] をクリックします。
- ステップ 3** [Create RADIUS Provider] ダイアログボックスで、次の操作を実行します。
- [Host Name (or IP Address)] フィールドで、ホスト名を追加します。
 - [Authorization Port] フィールドで、認証に必要なポート番号を追加します。
この番号は、設定されている RADIUS サーバによって異なります。
 - 必要な [Authorization Protocol] オプション ボタンをクリックします。
 - [Key] および [Confirm Key] フィールドに、事前共有キーを入力します。
このキーは、RADIUS サーバで設定されたサーバ キーと共有されるものと同一の情報です。
- ステップ 4** [Navigation] ペインの [RADIUS Providers] 下で、作成した RADIUS プロバイダーをクリックします。
RADIUS プロバイダーの設定の詳細は、[Work] ペインに表示されます。
- ステップ 5** [Navigation] ペインで、[RADIUS Provider Groups] を右クリックし、[Create RADIUS Provider Group] をクリックします。
- ステップ 6** [Create RADIUS Provider Group] ダイアログボックスで、次の操作を実行します。
- [Name] フィールドに、名前を入力します。
 - [Providers] フィールドを展開し、[Name] フィールドのドロップダウン リストから、先ほど作成したプロバイダーを選択します。
 - [Priority] フィールドで、プライオリティを割り当てます。[Update] をクリックし、[Submit] をクリックします。
RADIUS プロバイダー グループが作成されます。
- ステップ 7** [Navigation] ペインで、[AAA Authentication] を展開し、[Login Domain] を右クリックして [Create Login Domain] をクリックします。
- ステップ 8** [Create Login Domain] ダイアログボックスで、次の操作を実行します。
- [Name] フィールドに、ドメイン名を入力します。
 - [Realm] フィールドのドロップダウン リストで、[RADIUS] レalm を選択します。
 - [RADIUS Provider Group] フィールドのドロップダウン リストから、前に作成したプロバイダー グループを選択します。[Submit] をクリックします。
- ログイン ドメインが作成され、リモート ユーザ ログインおよび設定に使用可能になりました。
-

基本 GUI の 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。

インバンド管理ネットワークは、ACI ファブリックを使用して APIC がリーフ スイッチや外部と通信することを可能にし、ファブリック自体を使用して外部管理デバイスが APIC またはリーフ スイッチおよびスパイン スイッチと通信することを可能にします。

アウトオブバンド管理ネットワークの設定は、コントローラ、リーフ スイッチ、およびスパイン スイッチの管理ポートの設定を定義します。

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。

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。

IPv4/IPv6 アドレスおよびインバンド ポリシー

インバンド管理アドレスは、ポリシーによってのみ (Postman REST API、NX-OS スタイル CLI、または GUI) APIC コントローラにプロビジョニングできます。また、インバンド管理アドレスは、各ノードに静的に設定する必要があります。

アウトオブバンド ポリシーの IPv4/IPv6 アドレス

アウトオブバンド管理アドレスは、ブートストラップ時に、またはポリシーを使用して (Postman REST API、NX-OS スタイル CLI、GUI) APIC コントローラにプロビジョニングできます。また、アウトオブバンド管理アドレスは、各ノードに静的にまたはクラスタ全体にアドレスの範囲 (IPv4/IPv6) を指定することによって設定する必要があります。IP アドレスは、範囲からクラスタ内のノードにランダムに割り当てられます。

管理アクセスの設定

基本 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、「*Configuring Static Management Access in Cisco APIC*」のKB記事を参照してください。

手順

- ステップ 1** APIC GUI の [Basic Mode] にログインし、メニューバーで、[System] > [In Band & Out Of Band] の順にクリックします。
- ステップ 2** [Navigation] ペインで、[InBand Management Configuration] を選択します。
- ステップ 3** (任意) [Encap] フィールドで、必要に応じてインバンド管理に使用するデフォルト VLAN を変更するために新しい値を入力します。
- ステップ 4** [Nodes] を展開し、次のアクションを実行します。
- [Nodes] フィールドで、適切なノードを選択してインバンドアドレスを関連付けます。
 - [IP Address] フィールドに目的の IPv4 または IPv6 アドレスを入力します。
 - [Gateway] フィールドに目的の IPv4 または IPv6 ゲートウェイアドレスを入力します。[Submit] をクリックします。
(注) デフォルトゲートウェイの IP アドレスは、インバンド管理用の VRF の ACI ファブリックの拡散型ゲートウェイになります。
- ステップ 5** [L2 Connectivity] タブをクリックし、[Ports] を展開して、次のアクションを実行します。
- [Path] フィールドで、ドロップダウンリストから、管理用サーバまたは外部に接続されているポートを選択します。
 - [Encap] フィールドで、このポートで使用する VLAN を指定します。
- ステップ 6** [Gateway IP Address for External Connectivity] を展開し、[IP address] フィールドに外部接続用の目的のゲートウェイ IPv4 および IPv6 アドレスが一覧表示されます。
- ステップ 7** [ACL] を展開し、インバンド管理ネットワークに接続する目的のポートを追加します。[Submit] をクリックします。

インバンド管理アクセスが確立されました。

基本 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。

手順

- ステップ 1 APIC GUI の [Basic Mode] にログインし、メニューバーで、[System] > [In Band & Out Of Band] の順に選択します。
- ステップ 2 [Navigation] ペインで、[Out-of-Band EPG - default] をクリックします。
- ステップ 3 [Work] ペインで、[Properties] の下の [Nodes] を展開し、適切なノードを IPv4 または IPv6 アドレスおよびデフォルト ゲートウェイと関連付けます。[Update] をクリックします。
- ステップ 4 [Access Restrictions] を展開し、ACI ファブリック ノードのアウトオブバンド管理アドレスと通信する目的の外部サブネットのリストを追加します。
- ステップ 5 外部サブネットの [ACL] を展開し、ACI ファブリック ノードの管理を許可する L4 ポートの適切な情報を入力します。
アウトオブバンド管理アクセスが設定されました。

既存の IP tables 機能をミラーリングする IPv6 の変更

すべての IPv6 は、ネットワーク アドレス変換 (NAT) を除いて、既存の IP tables 機能をミラーリングします。

既存の IP tables

- 1 以前は、IPv6 テーブルのすべてのルールが一度に1つずつ実行され、すべてのルールの追加または削除に対してシステム コールが行われていました。
- 2 新しいポリシーが追加されるたびに、ルールが既存の IP tables ファイルに追加され、ファイルへの追加変更は行われませんでした。
- 3 新しい送信元ポートがアウトオブバンドポリシーで設定されると、同じポート番号で送信元と宛先のルールを追加しました。

IP tables への変更

- 1 IP tables が作成されると、はじめにハッシュマップに書き込まれ、次に中間ファイル IP tables-new に書き込まれてこれが復元されます。保存すると、新しい IP tables ファイルが /etc/sysconfig/ フォルダに作成されます。これら両方のファイルは同じ場所にあります。すべてのルールにシステム コールを行う代わりに、ファイルを復元および保存している時のみシステム コールを行う必要があります。

- 2 ルールを追加する代わりに新しいポリシーがファイルに追加されると、hashmaps にデフォルトポリシーをロードし、新しいポリシーを確認し、hashmaps に追加することによって、IP テーブルがゼロから作成されます。その後、中間ファイル (/etc/sysconfig/iptables-new) に書き込まれて保存されます。
- 3 アウトオブバンドポリシーのルールの送信元ポートだけを設定することはできません。宛先ポートまたは送信元ポートいずれかを宛先ポートとともにルールに追加できます。
- 4 新しいポリシーが追加されると、新しいルールが IP tables ファイルに追加されます。このルールは、IP tables デフォルトルールのアクセス フローを変更します。

```
-A INPUT -s <OOB Address Ipv4/Ipv6> -j apic-default
```
- 5 新しいルールが追加された場合、これは IP tables-new ファイルに存在して IP tables ファイルには存在せず、IP tables-new ファイルにエラーがあることを意味します。復元が正常な場合に限り、ファイルが保存され、新しいルールを IP tables ファイルで確認できます。



(注)

- IPv4 のみ有効な場合、IPv6 ポリシーを設定しないでください。
- IPv6 のみ有効な場合、IPv4 ポリシーを設定しないでください。
- IPv4 と IPv6 の両方が有効な場合にポリシーが追加されると、両方のバージョンに設定されます。したがって、IPv4 サブネットを追加すると IP tables に追加され、同様に IPv6 サブネットは IPv6 tables に追加されます。

VMM ドメインの設定

仮想マシン ネットワーキング ポリシーの設定

APIC は、サードパーティの VM マネージャ (VMM) (VMware vCenter および SCVMM など) と統合し、ACI の利点を仮想化されたインフラストラクチャに拡張します。APIC によって、VMM システム内の ACI ポリシーをその管理者が使用できるようになります。

ここでは、VMware vCenter および vShield を使用する VMM 統合の例を示します。シスコ ACI と VMM 統合の異なるモードに関する詳細については、『*ACI Virtualization Guide*』を参照してください。

VM マネージャについて



(注)

vCenter との統合のために必要な APIC の設定に関する情報を次に示します。VMware コンポーネントの設定手順については、VMware のマニュアルを参照してください。

次は、VM マネージャの用語の詳細情報です。

- VM コントローラは、VMware vCenter や VMware vShield などの、外部仮想マシン管理エンティティです。APIC は、コントローラと通信し、仮想ワークロードに適用されるネットワークポリシーを公開します。VM コントローラの管理者は、APIC 管理者に VM コントローラの認証クレデンシャルを提供します。同じタイプの複数のコントローラが同じクレデンシャルを使用できます。
- クレデンシャルは、VM コントローラと通信するための認証クレデンシャルを表します。複数のコントローラが同じクレデンシャルを使用できます。
- 仮想マシンのモビリティドメイン (vCenter のモビリティドメイン) は、同様のネットワークポリシー要件を持つ VM コントローラのグループです。この必須コンテナは、VLAN プールなどのためのポリシー、サーバ/ネットワーク MTU ポリシー、またはサーバ/ネットワークアクセス LACP ポリシーとともに 1 つ以上の VM コントローラを保持します。エンドポイントグループが vCenter ドメインに関連付けられると、ネットワークポリシーが vCenter ドメイン内のすべての VM コントローラにプッシュされます。
- プールは、トラフィックのカプセル化 ID の範囲を表します (たとえば、VLAN ID、VNID、マルチキャストアドレスなど)。プールは共有リソースで、VMM などの複数のドメインおよびレイヤ 4 ~ レイヤ 7 のサービスで消費できます。リーフスイッチは、重複した VLAN プールをサポートしていません。異なる重複した VLAN プールを VMM ドメインと関連付けることはできません。VLAN ベースのポートには、次の 2 種類があります。
 - ダイナミックプール: APIC によって内部的に管理され、エンドポイントグループ (EPG) の VLAN を割り当てます。vCenter ドメインはダイナミックプールのみに関連付けることができます。
 - スタティックプール: EPG にはドメインとの関係があり、ドメインにはプールとの関係があります。プールには、さまざまなカプセル化された VLAN および VXLAN が含まれます。スタティック EPG 導入環境の場合、ユーザはインターフェイスとカプセル化を定義します。カプセル化は、EPG が関連付けられているドメインに関連付けられたプールの範囲内である必要があります。
- 導入する VMware vCenter では、VLAN モードまたは VXLAN モードで動作する必要があります。VMM ドメインは VLAN プールに関連付け、vShield は vCenter に関連付ける必要があります。

VMM ドメイン プロファイルを作成するための前提条件

VMM ドメイン プロファイルを設定するには、次の前提条件を満たす必要があります。

- すべてのファブリック ノードが検出され、設定されている。
- インバンド (inb) またはアウトオブバンド (oob) 管理が APIC 上で設定されている。
- Virtual Machine Manager (VMM) がインストールされ、設定されて、inb/oob 管理ネットワーク (たとえば、vCenter) 経由で到達可能である。

- VMM の管理者とルートのクレデンシャルがある (vCenter など)。



(注) vCenter の管理者とルートのクレデンシャルを使用しない場合は、必要な最小アクセス許可を持つカスタム ユーザ アカウントを作成できます。必要なユーザ権限のリストについては、[最小 VMware vCenter 権限を持つカスタム ユーザ アカウント](#)、(19 ページ) を参照してください。

- IP アドレスではなくホスト名で VMM を参照する予定がある場合は、APIC の DNS ポリシーを設定する必要があります。
- VMware vShield のドメイン プロファイルを作成している場合は、DHCP サーバとリレー ポリシーを設定する必要があります。

最小 VMware vCenter 権限を持つカスタム ユーザ アカウント

Cisco APIC から vCenter を設定するには、vCenter で次の最小権限セットが許可されるクレデンシャルである必要があります。

- アラーム
- 分散スイッチ
- dvPort グループ
- フォルダ
- ホスト
 - 詳細設定
 - ローカル操作.再構成済み仮想マシン
 - ネットワーク設定
- ネットワーク
- 仮想マシン
 - 仮想マシン.構成.デバイス設定の変更
 - 仮想マシン.構成.設定

これにより、APIC は vCenter に VMware API コマンドを送信して、DVS/AVS の作成、VMK インターフェイス (AVS) の作成、ポート グループの発行および必要なすべてのアラートのリレーを行うことができます。

VMM ドメイン プロファイルの作成

この項では、VMM ドメインの例は、vCenter ドメインまたは vCenter および vShield ドメインです。

基本 GUI を使用した vCenter ドメイン プロファイルの作成

はじめる前に

VMM ドメイン プロファイルを作成する前に、APIC 上でインバンド管理ネットワークを使用して外部ネットワークへの接続を確立する必要があります。

手順

-
- ステップ 1** (注) APIC GUI の [Basic Mode] にログインします。
- メニュー バーで、[VM NETWORKING] > [Inventory] の順に選択します。
- ステップ 2** [Navigation] ペインで、[VMware] を右クリックし、[Create vCenter Domain] をクリックします。
- ステップ 3** [Create vCenter Domain] ダイアログボックスで、[Name] を入力します。
- ステップ 4** [Virtual Switch] フィールドで、[VMware vSphere Distributed Switch] が選択されていることを確認します。
- ステップ 5** (注) このステップでは、このサーバ下に作成されるすべてのポート グループおよび EPG に対する VLAN の範囲が提供されます。
- [VLAN Pool] ドロップダウン リストで、[Create VLAN Pool] を選択します。[Create VLAN Pool] ダイアログボックスで、次の操作を実行します。
- [Name] を入力します。
 - [Allocation Mode] フィールドで、[Dynamic Allocation] が選択されていることを確認します。
 - [Encap Blocks] を展開して、VLAN ブロックを追加します。[Create Ranges] ダイアログボックスで、VLAN の範囲を入力します。
(注) 少なくとも 200 の VLAN 番号の範囲を使用することを推奨します。
 - [OK] をクリックし、[Submit] をクリックします。
- ステップ 6** [vCenter/vShield] を展開し、次のタスクを実行します。
- [Create vCenter/vShield Controller] ダイアログボックスの [Type] フィールドで、[vCenter] オプション ボタンをクリックします。
 - vCenter Controller の [Host Name (or IP Address)] フィールドに、vCenter の名前または IP アドレスを入力します。
 - [Datacenter] フィールドで、必要に応じてデータセンターを入力します。
 - [Username] フィールドにユーザ名を入力します。

ユーザ名は、vCenter の管理者としてログインするためのクレデンシャルである必要があります。

- e) [Password] フィールドにパスワードを入力し、[Confirm Password] フィールドにパスワードをもう一度入力します。[OK] をクリックし、[Submit] をクリックします。
パスワードは、vCenter の管理者としてログインするためのクレデンシャルである必要があります。

ステップ 7 メニュー バーで、[FABRIC] > [Inventory] を選択します。

ステップ 8 [Navigation] ペインで、[Pod] を展開し、[Configure] タブをクリックし、次の操作を実行します。

- a) [Configure] ペインで、[Add Switches] をクリックし、設定するスイッチを選択します。[Add Selected] をクリックします。
(注) 複数のスイッチを選択するには、[Command] ボタンを使用します。
- b) ポート番号をクリックしてこれらを VMware に関連付けし、[Configure Interface] をクリックします。
- c) [Configure Interface] ペインで、[VLAN] タブをクリックします。
- d) [VLAN] ペインで、[ESX And SCVMM] を展開します。
- e) [Name] フィールドで、ドロップダウンリストから作成した VMware を選択します。[Update] および [Apply Changes] をクリックし、VMware の設定を完了します。

ステップ 9 次の手順に従って、新しいドメインとプロファイルを確認します。

(注) ポリシーが送信された後にコントローラを確実に動作させるには、vCenter の管理者は分散スイッチにホストを追加する必要があります。

- a) メニュー バーで、[VM Networking] > [Inventory] を選択します。
- b) [Navigation] ペインで、[VMware] を展開し、vCenter ドメイン名を展開します。
- c) [Navigation] ペインで、コントローラ名をクリックし、コントローラがオンラインであることを確認します。
[Work] ペインに、プロパティが動作ステータスとともに表示されます。表示される情報によって、APIC コントローラからサーバへの接続が確立され、インベントリが使用できることを確認します。

基本 GUI を使用した vCenter および vShield ドメイン プロファイルを作成する

手順

- ステップ 1** (注) APIC GUI の [Basic Mode] にログインします。

メニュー バーで、[VM NETWORKING] > [Inventory] の順に選択します。

ステップ 2 [Navigation] ペインで、[VMware] を右クリックし、[Create vCenter Domain] をクリックします。

ステップ 3 [Create vCenter Domain] ダイアログボックスで、[Name] を入力します。

ステップ 4 [Virtual Switch] フィールドで、[VMware vSphere Distributed Switch] が選択されていることを確認します。

ステップ 5 (注) このステップでは、このサーバ下に作成されるすべてのポート グループおよび EPG に対する VLAN の範囲が提供されます。

[VLAN Pool] ドロップダウン リストで、[Create VLAN Pool] を選択します。[Create VLAN Pool] ダイアログボックスで、次の操作を実行します。

a) [Name] を入力します。

b) [Allocation Mode] フィールドで、[Dynamic Allocation] が選択されていることを確認します。

c) [Encap Blocks] を展開して、VLAN ブロックを追加します。[Create Ranges] ダイアログボックスで、VLAN の範囲を入力します。

(注) 少なくとも 200 の VLAN 番号の範囲を使用することを推奨します。

d) [OK] をクリックし、[Submit] をクリックします。

ステップ 6 [vCenter/vShield] を展開し、次のタスクを実行します。

a) [Create vCenter/vShield Controller] ダイアログボックスの [Type] フィールドで、[vCenter+vShield] オプション ボタンをクリックします。

b) vCenter Controller の [Host Name (or IP Address)] フィールドに、vCenter の名前または IP アドレスを入力します。

c) [Datacenter] フィールドで、必要に応じてデータセンターを入力します。

d) [Username] フィールドにユーザ名を入力します。

ユーザ名は、vCenter の管理者としてログインするためのクレデンシャルである必要があります。

e) [Password] フィールドにパスワードを入力し、[Confirm Password] フィールドにパスワードをもう一度入力します。

パスワードは、vCenter の管理者としてログインするためのクレデンシャルである必要があります。

f) vShield Controller の [Host Name (or IP Address)] フィールドに、vShield の名前または IP アドレスを入力します。

g) [Datacenter] フィールドで、必要に応じてデータセンターを入力します。

h) [Username] フィールドにユーザ名を入力します。

ユーザ名は、vShield の管理者としてログインするためのクレデンシャルである必要があります。

i) [Password] フィールドにパスワードを入力し、[Confirm Password] フィールドにパスワードをもう一度入力します。[OK] をクリックし、[Submit] をクリックします。

パスワードは、vShield の管理者としてログインするためのクレデンシャルである必要があります。

ステップ 7 メニュー バーで、[FABRIC] > [Inventory] を選択します。

ステップ 8 [Navigation] ペインで、[Pod] を展開し、[Configure] タブをクリックし、次の操作を実行します。

- a) [Configure] ペインで、[Add Switches] をクリックし、設定するスイッチを選択します。[Add Selected] をクリックします。
(注) 複数のスイッチを選択するには、[Command] ボタンを使用します。
- b) ポート番号をクリックしてこれらを VMware に関連付けし、[Configure Interface] をクリックします。
- c) [Configure Interface] ペインで、[VLAN] タブをクリックします。
- d) [VLAN] ペインで、[ESX And SCVMM] を展開します。
- e) [Name] フィールドで、ドロップダウンリストから作成した VMware を選択します。[Update] および [Apply Changes] をクリックし、VMware の設定を完了します。

ステップ 9

次の手順に従って、新しいドメインとプロファイルを確認します。

(注) ポリシーの発行後にコントローラが機能していることを確認するには、vCenter と vShield の管理者は分散スイッチにホストを追加する必要があります。

- a) メニューバーで、[VM Networking] > [Inventory] を選択します。
- b) [Navigation] ペインで、[VMware] を展開し、vCenter ドメイン名を展開します。VMware の [Work] ペインに vCenter と vShield の両方が表示されている必要があります。
- c) [Navigation] ペインで、コントローラ名をクリックし、コントローラがオンラインであることを確認します。
[Work] ペインに、プロパティが動作ステータスとともに表示されます。表示される情報によって、APIC コントローラからサーバへの接続が確立され、インベントリが使用できることを確認します。

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ク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クなどのため）。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。

基本 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

手順

-
- ステップ 1** APIC GUI の [Basic Mode] にログインし、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。
- [Name] フィールドに、名前を入力します。
 - [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。
 - [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。
 - [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、[VRF] アイコンを Canvas 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。
- [Name] フィールドに、名前を入力します。
 - [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。
- [Name] フィールドに、名前を入力します。
 - [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。
 - [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** [Networking] ペインで、[VRF] アイコンに接続しながら、Canvas に [L3] アイコンをドラッグします。[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) [Node ID] フィールドに、ノード ID を入力します。
 - b) [Router ID] フィールドに、ルータ ID を入力します。
 - c) [Static Routes] を展開し、[IP Address] および [Next Hop IP] フィールドに IPv4 または IPv6 アドレスを入力し、[Update] をクリックします。
(注) ゲートウェイ IPv6 アドレスは、グローバルユニキャスト IPv6 アドレスである必要があります。
 - d) 必要に応じて [Protocols] ボックスをクリックし、設定する [BGP]、[OSPF]、[EIGRP] を選択します。
 - e) [OK] をクリックしてから [Submit] をクリックし、レイヤ 3 の設定を完了します。
- L3 の設定を確認するには、[Navigation] ペインで、[VRFs] > [VRF name] > [Deployed VRFs] の順に展開します。

サーバまたはサービス ポリシーの設定

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。

基本 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



- (注) DHCP サーバポリシーの設定は、[Advanced Mode] モードでのみ使用できます。このタスクを実行するには、APIC GUI で [Advanced Mode] に切り替えます。

- 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

-
- 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。
- [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。
 - [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。
 - [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)
 - [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)
 - [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)
 - [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。
 - [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。
- [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。

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。

ソース	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	Anywhere

ソース	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
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。	Anywhere
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せん。

- 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。

DNS プロファイルの IPv4 または IPv6 の優先順位のポリシー

DNS プロファイルは、IPv4 と IPv6 のバージョン優先順位の選択をサポートします。ユーザ インターフェイスを使用して、優先順位を有効にすることができます。IPv4 がデフォルトです。

次の例は、Postman REST API を使用したポリシーベースの設定を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/fabric/dnsp-default.xml -->
<dnsProfile dn="uni/fabric/dnsp-default" IPVerPreference="IPv6" childAction="" descr="" >
</dnsProfile>
```

gai.conf の設定は、宛先アドレス選択を制御します。ファイルには、ラベル テーブル、優先順位 テーブル、IPv4 範囲テーブルが含まれます。IPv4 または IPv6 をもう一方よりも優先付けする変更は、優先順位 テーブルのエントリに含める必要があります。Linux システムで多数のフレーバーに使用されている標準ファイルの内容例を下に示します。ファイルの precedence ラベルの一行でデフォルト設定を上書きします。

次の例は、IPv4 を IPv6 よりも優先させるための gai.conf です。

```
# Generated by APIC
label ::1/128 0
label ::/0 1
label 2002::/16 2
label ::/96 3
label ::ffff:0:0/96 4
precedence ::1/128 50
precedence ::/0 40
precedence 2002::/16 30
precedence ::/96 20
# For APICs preferring IPv4 connections, change the value to 100.
precedence ::ffff:0:0/96 10
```

デュアルスタック IPv4 および IPv6 DNS サーバ

DNS サーバには、A レコード (IPv4) または AAAA レコード (IPv6) のプライマリ DNS レコードがあります。A および AAAA レコードは、ドメイン名を特定の IP アドレス (IPv4 または IPv6) と関連付けます。

ACI ファブリックは、IPv4 で実行する信頼できるパブリック DNS サーバを使用するように設定できます。これらのサーバは、A レコード (IPv4) または AAAA レコード (IPv6) で解決および応答できます。

純粋な IPv6 環境では、システム管理者は IPv6 DNS サーバを使用する必要があります。IPv6 DNS サーバは、/etc/resolv.conf に追加することによって有効化されます。

より一般的な環境では、デュアルスタック IPv4 および IPv6 DNS サーバを使用します。デュアルスタックの場合、IPv4 と IPv6 の両方が /etc/resolv.conf にリストされます。ただし、デュアルスタック環境で、単純に IPv6 DNS サーバをリストに追加すると、DNS 解決の大きな遅延を引き起

こす可能性があります。これは、デフォルトで IPv6 プロトコルが優先されるため、IPv4 DNS サーバに接続できないためです (/etc/resolv.conf で最初にリストされている場合)。この解決法は、IPv4 DNS サーバの前に IPv6 DNS サーバをリストすることです。また、IPv4 と IPv6 両方のルックアップで同一ソケットを使用できるようにするために、「options single-request-reopen」を追加します。

IPv6 DNS サーバが最初にリストされているデュアルスタック IPv4 および IPv6 DNS サーバの resolv.conf の例を次に示します。「single-request-reopen」オプションにも注意してください。

```
options single-request-reopen
nameserver 2001:4860:4680::8888
nameserver 2001:4860:4680::8844
nameserver 8.8.8.8
nameserver 8.8.4.4
```

デュアルスタック IPv4 および IPv6 環境

ACI ファブリックの管理ネットワークが IPv4 と IPv6 の両方をサポートする場合、Linux システムアプリケーション (glibc) では、getaddrinfo() が IPv6 を最初に返すため、IPv6 ネットワークをデフォルトで使用します。

ただし、特定の条件下では IPv4 アドレスが IPv6 アドレスよりも推奨されることがあります。Linux IPv6 スタックには、IPv6 にマッピングされた IPv4 アドレス (::ffff/96) を使用して、IPv6 アドレスとしてマッピングされた IPv4 アドレスを有効にする機能があります。これは、IPv6 対応アプリケーションが IPv4 と IPv6 両方を受け入れまたは接続するためにシングルソケットのみ使用できるようにします。これは /etc/gai.conf の getaddrinfo() の glibc IPv6 選択項目によって制御されます。

/etc/hosts を使用する場合は glibc が複数のアドレスを返すようにするために、/etc/hosts ファイルに「multi on」を追加する必要があります。追加しないと、最初に一致したものだけを返す場合があります。

アプリケーションが IPv4 と IPv6 の両方が存在するかどうかを認識していない場合、異なるアドレスファミリを使用するフォールバック試行が実行されないことがあります。このようなアプリケーションでは、フォールバックの実装が必要な場合があります。

基本 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

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

-
- ステップ 1 メニューバーで、[System] > [System Settings] の順に選択します。[Navigation] ペインで、[System Settings] > [DNS] の順に展開し、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 つだけ指定できます。
- 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。
デフォルトとして指定できるドメイン名は 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] > [VRFs] > [oob] の順に展開します。

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

手順

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

```

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。

基本 GUI を使用した MP-BGP ルート リフレクタの設定

手順

-
- ステップ 1** メニュー バーで、[System] > [System Settings] の順に選択します。
- ステップ 2** [Navigation] ペインで、[System Settings] > [BGP Route Reflector] の順に展開し、[BGP Route Reflector] を右クリックして、[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** [Autonomous System Number] フィールドで、適切な数量を選択します。[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。
-

MP-BGP ルート リフレクタ設定の確認

手順

-
- ステップ 1** 次の操作を実行して、設定を確認します。
- 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。
 - 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。
- 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。
 - 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。

基本 GUI を使用した管理テナントの OSPF 外部ルーテッド ネットワークを作成する

はじめる前に

- 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。

手順

- ステップ 1** メニューバーで、[Fabric] > [Inventory] の順にクリックします。[Navigation] ペインで、VRF を導入するリーフスイッチをクリックします。
- ステップ 2** [Configure VRF] を右クリックしてクリックします。
- ステップ 3** [Configure VRF] ダイアログボックスで、次の操作を実行します。
 - a) [Tenant] フィールドのドロップダウンリストから、テナントを選択します。この場合は mgmt テナントです。
 - b) [VRF] フィールドのドロップダウンリストから、VRF を選択します。
 - c) [Router ID] フィールドに、ルータ ID を入力します。
 - d) [Protocols] 領域で、OSPF のチェックボックスをオンにします。
 - e) 表示される [Route Maps] 領域で、[+] 記号をクリックします。
 - f) [Create Route Map] ダイアログボックスで、[Name] フィールドに、ルートマップの名前を入力します。
- ステップ 4** [Prefix List] 領域を展開します。

- a) [Create Prefix List] ダイアログボックスで、[Prefix Name] フィールドに、エリア ID を入力します。
- b) [IP Prefixes] フィールドに、少なくとも 1 つのプレフィックスを入力します。
- c) 必要に応じてダイアログボックスに詳細を入力します。
- d) [Prefix List] ダイアログボックスで、[OK] をクリックします。

ステップ 5 [Configure VRF with Leaf] ダイアログボックスで、[OSPF Configuration] 領域を展開します。

- a) [Configure OSPF] ダイアログボックスで、[Area ID] フィールドに、エリア ID を入力します。
- b) [Area Type] フィールドで、目的のタイプを選択します。
- c) [Route Map] フィールドのドロップダウンリストから、適切なルート マップを選択します。
[OK] をクリックします。
- d) [Configure VRF] ダイアログボックスで、[Submit] をクリックします。

VRF の下の[Navigation] ペインに、VRF が導入されます。

ステップ 6 [Navigation] ペインで、[Interfaces] > [Physical Interfaces] の順に展開します。

ステップ 7 レイヤ 3 を設定する目的のインターフェイスを選択し、次の操作を実行します。

- a) [Convert to L3] ボタンをクリックします。[L2 configuration will be deleted. Do you want to continue?] の [Warning] ダイアログボックスが表示されたら、[Yes] をクリックします。
- b) [Subinterface] フィールドで、[Off] ボタンをクリックします。
- c) [Tenant] フィールドのドロップダウンリストから、適切なテナント (mgmt) を選択します。
- 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) [IPv4 Address] フィールドに、インターフェイスの IP アドレスを入力します。
- f) [Protocols] フィールドで、OSPF のチェックボックスをオンにします。
ダイアログボックスの右上隅に、[OSPF] タブが表示されます。
- g) [OSPF] タブをクリックします。
- h) [Work] ペインの [IP V4 OSPF Area ID] フィールドで、ドロップダウンリストから目的のエリア ID を選択します。
- i) [Policy Name] フィールドで、デフォルトのポリシーを選択します。
またはこのエリアから、認証タイプ、認証キー、ポリシー名を選択します。[Submit] をクリックします。

(注) これにより、管理インターフェイスが作成されます。OSPF が VRF に導入されます。

- j) [Navigation] ペインで、VRF に導入された OSPF をクリックすると、[Work] ペインに統計が表示されます。

管理テナントの OSPF 外部ルーテッドネットワークが作成されます。

アプリケーション ポリシーの展開

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。

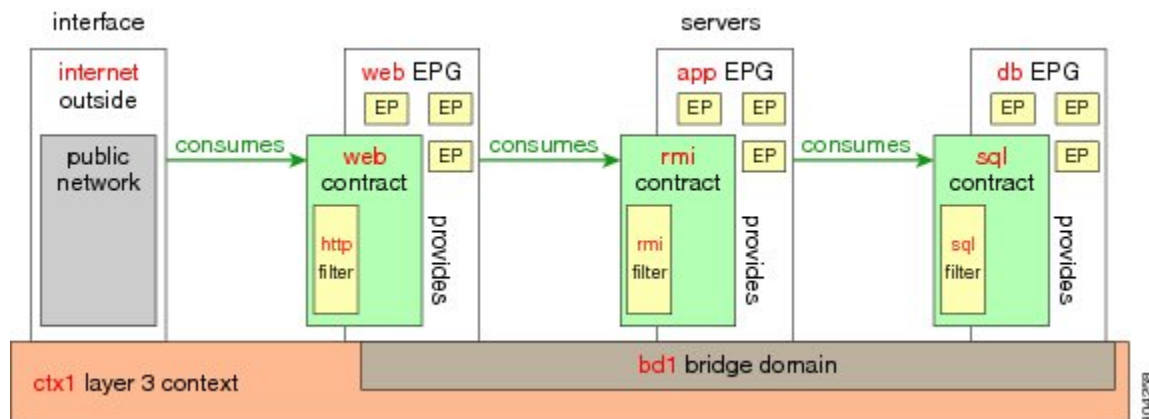
アプリケーション プロファイルでは、APIC がその後ネットワークおよびデータセンターのインフラストラクチャで自動的にレンダリングするアプリケーション要件をモデル化することができます。アプリケーション プロファイルでは、管理者がインフラストラクチャの構成要素ではなくアプリケーションの観点から、リソース プールにアプローチすることができます。アプリケーション プロファイルは、互いに論理的に関連する EPG を保持するコンテナです。EPG は同じアプリケーション プロファイル内の他の EPG および他のアプリケーション プロファイル内の EPG と通信できます。

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 2: *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	--

基本 GUI を使用したアプリケーション ポリシーの展開

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

-
- ステップ 1** (注) APIC GUI の [Basic Mode] にログインします。

- メニューバーで、[Tenants] > [Tenant-name] の順にクリックします。
- ステップ 2** [Navigation] ペインで、[Application Profiles] を右クリックし、[Create Application Profile] をクリックします。
- ステップ 3** [Create Application Profile] ダイアログボックスに、プロファイルの名前を入力します。[Submit] をクリックします。
- ステップ 4** [Navigation] ペインで、新しいアプリケーションプロファイルをクリックして選択します。
- ステップ 5** [Work] ペインの [Drag and drop to configure toolbar] から最初の [EPG] をドラッグし、下の空白の画面にドロップします。
- ステップ 6** 表示される [Create Application EPG] ダイアログボックスで、次の操作を実行します。
- アプリケーション EPG の名前を入力します。
 - [Bridge Domain] フィールドで、ドロップダウンリストから、目的のブリッジドメインを選択します。[OK] をクリックします。
- 異なるブリッジドメインが必要な場合はこの手順を繰り返して追加の EPG を作成します。
- ステップ 7** [Drag and drop to configure toolbar] から、[Contract] をドラッグアンドドロップします。ユーザの必要に応じてドラッグするとプロバイダー EPG としてコンシューマ EPG を自動接続します。関係が矢印で表示されます。
- [Config Contract With L4-L7 Service Graph] ダイアログボックスが表示され、選択した詳細、および関連するプロバイダーとコンシューマの契約が自動的に読み込まれます。
- [Contract Name] フィールドに、契約名を入力します。[OK] をクリックします。
 - [No Filter] フィールドのチェックボックスをオフにして、カスタマイズフィルタを作成します。
(注) チェックボックスをオフにしない場合は、デフォルトのフィルタが自動作成されます。
 - (任意) カスタマイズフィルタを作成するには、必要に応じて [Filter Entries] フィールドに適切な情報を入力します。[OK] をクリックします。
- ステップ 8** [Application Profile] 作業ウィンドウで、[Submit] をクリックします。
これで、アプリケーションプロファイルを導入する手順が完了しました。
-

