拡張 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

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。

a) [ID] フィールドで、適切な ID を追加します（leaf1 は ID 101、leaf 2 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。

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。
（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。

a) [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。

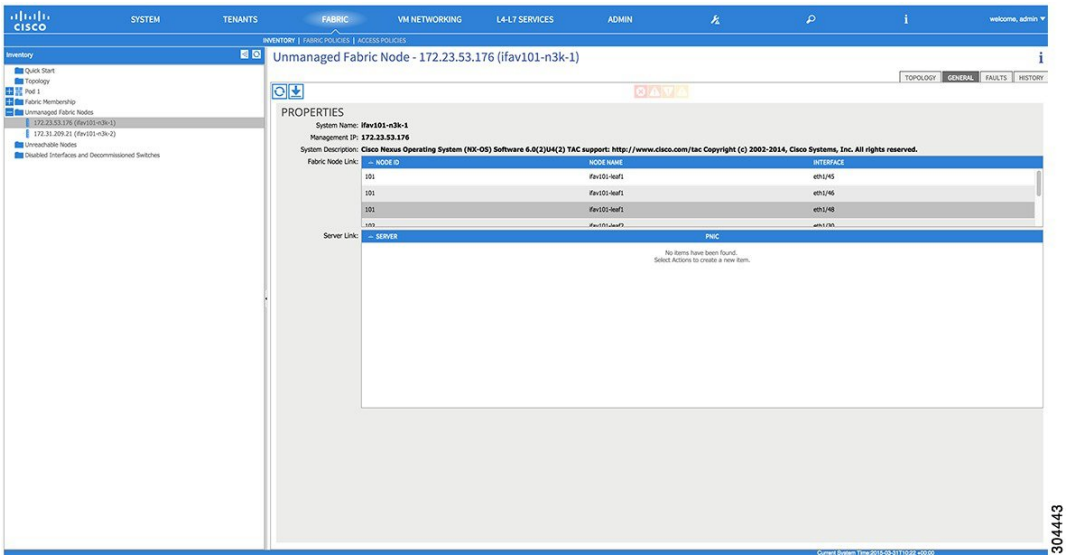
ステップ 5 （任意） トポロジ図を更新するには、[Work] ペインの左上隅にある [Refresh] アイコンをクリックします。

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。

拡張 GUI を使用した NTP の設定

手順

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。

GUI を使用した NTP の動作の確認

手順

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。

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。

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。

a) [Host Name (or IP Address)] フィールドで、ホスト名を追加します。
b) [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。
c) 必要な [Authorization Protocol] オプション ボタンをクリックします。
d) [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。

a) [Name] フィールドに、名前を入力します。
b) [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。
c) [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。

a) [Name] フィールドに、ドメイン名を入力します。
b) [Realm] フィールドのドロップダウン リストで、[RADIUS] レルムを選択します。
c) [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。

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。

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

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、「*Configuring Static Management Access in Cisco APIC*」の KB 記事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、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] > [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。

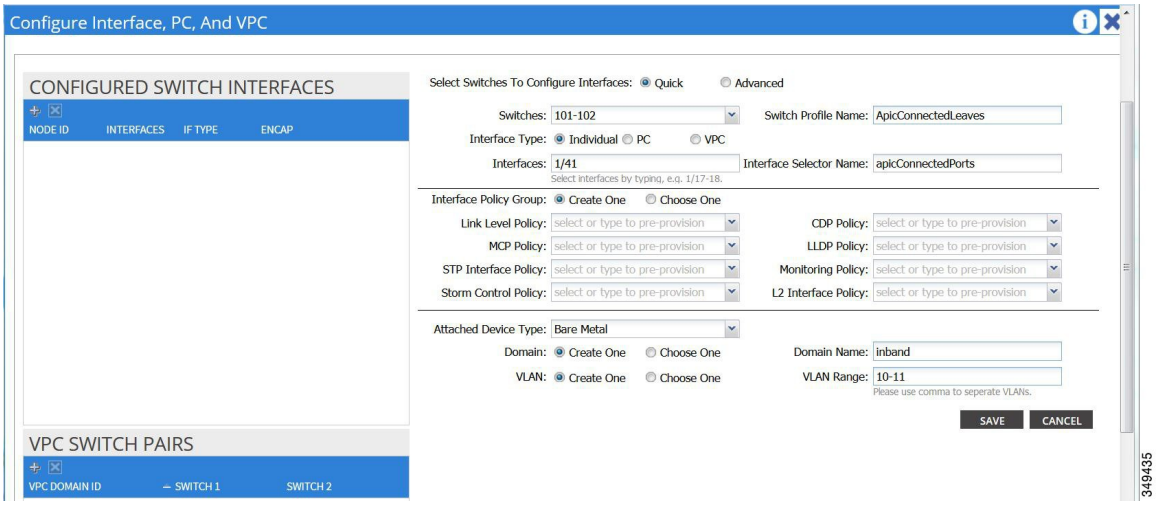
ステップ 3 [Configure Interface, PC, and VPC] ダイアログボックスで、APIC に接続されているスイッチ ポートを設定し、次の操作を実行します。

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、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。

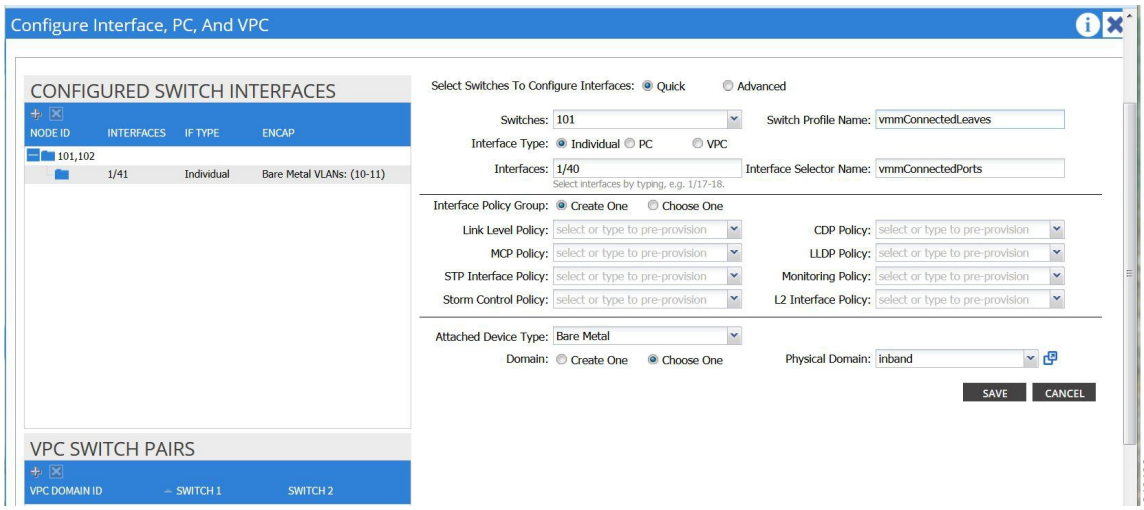
ステップ 5 [Configure Interface, PC, and VPC] ダイアログ ボックスで、次のアクションを実行します。

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、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。

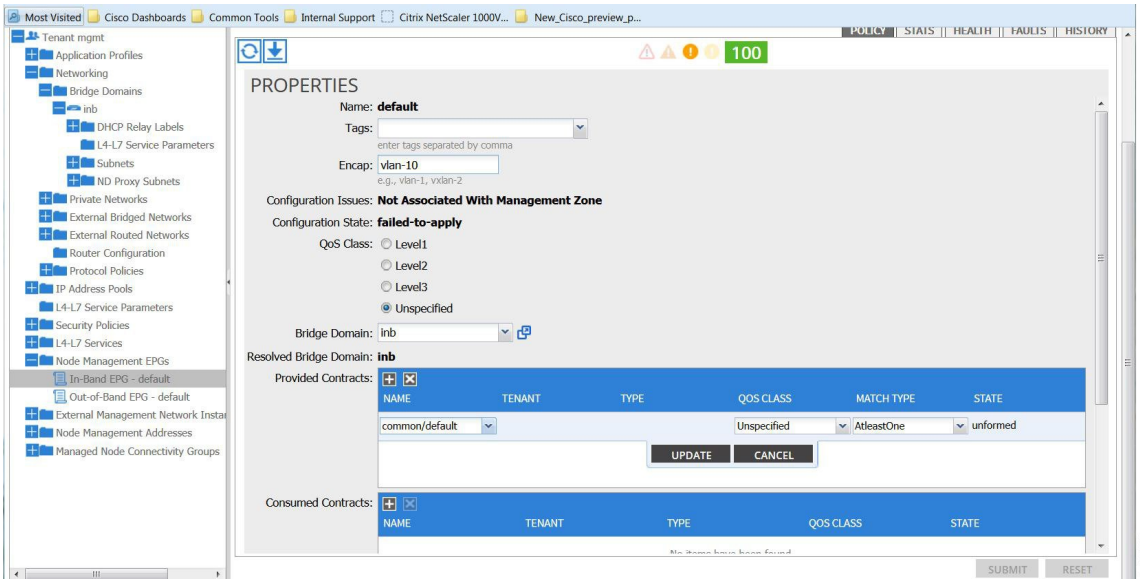
c) [Bridge Domain] ドロップダウン フィールドから、ブリッジ ドメインを選択します。[Submit] をクリックします。

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。

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、Videos Webpage 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

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。

GUI を使用した APIC コントローラの IP アドレスの変更

はじめる前に

手順

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、ポリシー名を入力します。

b) [Nodes] フィールドで、IP アドレスを変更する該当するコントローラのチェックボックスをクリックします。

c) [Config] フィールドで、[Out-of-Band Addresses] のチェックボックスをクリックします。
[Out-of-Band Addresses] 領域が展開します。

d) [Out-of-Band Management EPG] フィールドで、ドロップダウン リストから、該当する EPG を選択します。
e) [Out-of-Band Gateway] フィールドで、割り当てる新しい IP アドレスのゲートウェイを入力します。
[Mask] フィールドに自動的に入力されます。
f) [Out-of-Band IP Addresses] 範囲のフィールドで、適切な IP アドレスを入力します。[Submit] をクリックします。
g) [Confirm] ダイアログボックスで、新しい管理 IP アドレスの割り当てに進むかどうかを確認するメッセージが表示されたら、[Yes] をクリックします。
新しい管理 IP アドレスが APIC コントローラに割り当てられます。

次の作業

- APIC コントローラに再接続するには、新しい IP アドレスを使用する必要があります。
- 新しい IP アドレスがコントローラに割り当てられたら、コントローラの古い IP アドレスを削除する必要があります。

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にのみシステム 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。

管理接続モード

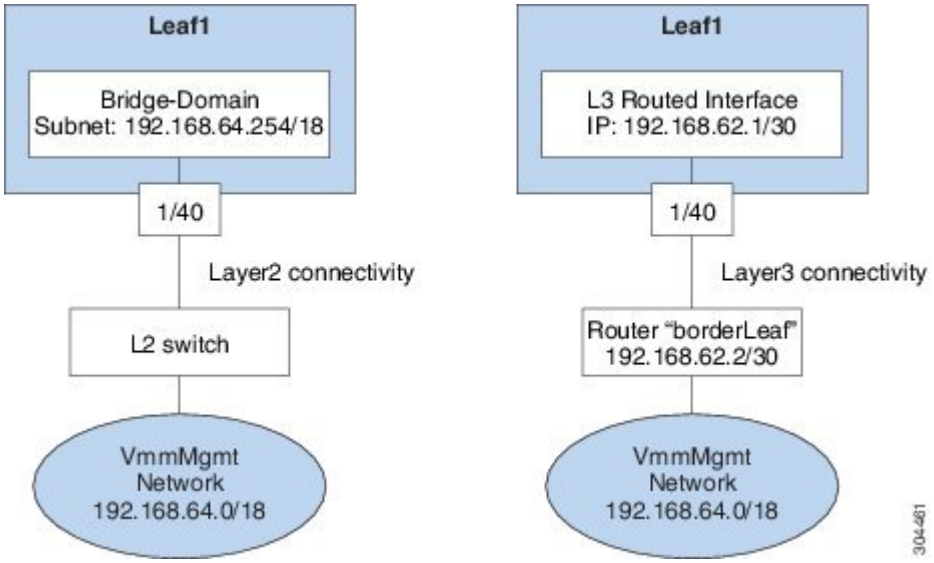
アウトオブバンドとインバンド管理接続が設定されているかどうかに応じて、アウトオブバンドまたはインバンドネットワークを使用する外部エンティティへの接続を確立します。vCenter Server などの外部エンティティへの接続を確立するには次の 2 つのモードを使用できます。

- レイヤ 2 管理接続：外部エンティティがレイヤ 2 を使用してリーフ ノードに接続されている場合は、このモードを使用します。
- レイヤ 3 管理接続：外部エンティティがレイヤ 3 を使用してルータを介してリーフ ノードに接続されている場合は、このモードを使用します。リーフは、外部エンティティに到達可能なルータに接続されます。

（注）
- インバンド IP アドレス範囲は、リーフ ノードからファブリックの外へのレイヤ 3 接続で使用される IP アドレス範囲から分離して異なっている必要があります。
- レイヤ 3 インバンド管理の設計では、トポロジ内のスパイン ファブリック ノードへのインバンド管理アクセスは提供されません。

次の図は、接続の確立に使用可能な 2 つのモードを示します。

図 *2*：レイヤ *2* およびレイヤ *3* 管理接続の例



拡張 GUI を使用したレイヤ 2 管理接続の設定

（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

vCenter ドメインプロファイルを作成する前に、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を確立するための接続を確立する必要があります。

管理接続ポリシーの一部として設定された IP アドレス範囲が ACI ファブリックで使用されるインフラストラクチャの IP アドレス範囲と重複していないことを確認します。

手順

ステップ 1 メニュー バーで、[Tenants] > [mgmt] の順に選択します。

ステップ 2 [Navigation] ペインで、[Tenant mgmt] > [Networking] を展開し、[Bridge Domains] を右クリックし、[Create Bridge Domain] をクリックします。

ステップ 3 [Create Bridge Domain] 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、ブリッジ ドメイン名を入力します。

b) [VRF] フィールドで、ドロップダウン リストから、ネットワーク（mgmt/inb）を選択します。[Next] をクリックします。

c) [L3 Configuration] タブをクリックし、[Subnets] フィールドで、[+] アイコンをクリックしてサブネットを追加します。
必要に応じてゲートウェイ IP アドレスを追加します。

d) [Create Bridge Domain] ダイアログボックスで、[Next] をクリックしてから、[Submit] をクリックします。
ブリッジ ドメインが作成されます。

ステップ 4 [Navigation] ペインで、[Tenant mgmt] > [Application Profiles] の順に展開します。

ステップ 5 [Application Profiles] を右クリックし、[Create Application Profile] をクリックします。

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

a) [EPGs] フィールドで、[+] アイコンをクリックして EPG を追加し、[Name] フィールドに名前を入力します。

b) [BD] ドロップダウン リストから、適切な BD を選択します。

c) [Domain] フィールドのドロップダウン リストから、適切なドメインを選択します。

d) [Static Path] フィールドに、次の例の 101/1/40 と同様の適切な値を入力します。

e) [Static Path VLAN] フィールドに、適切な VLAN を入力します（次の例の vlan-11 と同様の適切な値を入力します）。

f) [Consumed Contract] フィールドで、ドロップダウン リストから、適切な値を選択します。
[Update] と [Submit] をクリックします。

[Navigation] ペインで、[Networking] の下にブリッジ ドメインが作成され、[Application Profiles] の下にアプリケーション プロファイルとアプリケーション EPG が作成されます。 レイヤ 2 管理接続が設定されました。

拡張 GUI を使用したレイヤ 3 管理接続の設定

（注）
- 名前 vmm がこのタスクで文字列の例として使用されます。
- 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

VMM ドメイン プロファイルを作成する前に、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。

管理接続ポリシーの一部として設定された IP アドレス範囲が ACI ファブリックで使用されるインフラストラクチャの IP アドレス範囲と重複していないことを確認します。

手順

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、次の操作を実行します。

a) [Tenant mgmt] > [Networking] > [External Routed Networks] を展開します。

b) [Create Routed Outside] を右クリックします。

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、レイヤ 3 ルーテッド外部ポリシーの名前（vmm）を入力します。
名前には 64 文字以内の英数字を使用できます。この名前は、オブジェクトの保存後には変更できません。

b) [VRF] ドロップダウン リストから、インバンド デフォルト ネットワーク（mgmt/inb）を選択します。

（注） デフォルトのインバンド ネットワークを選択する必要があります。

ステップ 4 [Nodes and Interfaces Protocol Profiles] 領域を展開します。[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、名前を入力します（borderLeaf）。

b) [Nodes] を展開して、[Select Node] ダイアログボックスを表示します。[Node ID] フィールドで、ドロップダウン リストからリーフ スイッチ（leaf1）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) [Static Routes] を展開します。

e) [Create Static Route] ダイアログボックスで、[Prefix] フィールドに、通信する外部管理システム（たとえば、VMware vCenter、Syslog サーバ、AAA サーバ）のスタティック ルート用のサブネット プレフィクスを入力します。

f) [Next Hop Addresses] を展開して、[Next Hop IP] フィールドに、リーフ スイッチに接続されるルータの IP アドレスを入力します。[Preference] フィールドで、優先順位を選択します。[Update] をクリックします。

g) [OK] をクリックします。[Select Node] ダイアログボックスで、[OK] をクリックします。

ステップ 5 [Interface Profiles] を展開します。[Create Interface 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、名前を入力します（portProfile1）。

b) [Routed Interfaces] を展開します。[Select Routed Interface] 領域の [Path] フィールドで、ドロップダウン リストから、leaf1 に関連付けるパスを選択します。

c) [IPv4 Primary/IPv6 Preferred Address] フィールドに、リーフのルーテッド インターフェイスの IP アドレスとサブネット マスクを入力します。[OK] をクリックします。

d) [Create Interface Profile] ダイアログボックスで、[OK] をクリックします。[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 6 [Create Routed Outside] ダイアログボックスで、[Next] をクリックし、[External EPG Networks] を展開します。

ステップ 7 [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、名前（vmmMgmt）を入力します。
b) [Subnet] の [+] アイコンを展開します。
c) [Create Subnet] ダイアログボックスで、[IP address] フィールドに、サブネット アドレスを入力します。
d) [OK] を 2 回クリックし、[Finish] をクリックします。

L3 管理接続が設定されます。

管理接続の検証

この検証プロセスは、レイヤ 2 とレイヤ 3 の両方のモードに適用され、APIC GUI、REST API、または CLI を使用して確立される接続を確認するために使用できます。

管理接続を確立するための手順を完了したら、APIC コンソールにログインします。到達可能な vCenter Server の IP アドレス（たとえば、192.168.81.2）に ping を送り、その ping が機能することを確認します。この操作は、ポリシーが正常に適用されたことを示します。

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、同様のネットワーキング 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。

接続可能エンティティ プロファイルについて

接続エンティティ プロファイル

ACI ファブリックにより、リーフ ポートを通じて baremetal 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）、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、ポート チャネル、または仮想ポート 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、物理インターフェイス ポリシーで構成され、たとえば Cisco Discovery Protocol（CDP）、Link Layer Discovery

Protocol（LLDP）、最大伝送単位（MTU）、Link Aggregation Control Protocol（LACP）などがあります。

VM マネージャ（VMM）ドメインは、AEP に関連付けられたインターフェイス 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 でオーバーライド 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、ハイパーバイザが中間レイヤ 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 スイッチおよびハイパーバイザ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、ハイパーバイザとレイヤ 2 スイッチ間の LACP をディセーブルにできます。

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。異なるリーフ スイッチ間でカプセル化プール（たとえば VLAN）を再利用することができます。AEP は、（ドメインに関連付けられた）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。

（注）

- AEP は、リーフ上で VLAN プール（および関連 VLAN）をプロビジョニングします。VLAN はポートでは実際にイネーブルになっていません。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 を使用して VLAN プールを展開しないと、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 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。
  - EPG で VMM カプセル化を静的に設定する場合は、スタティック プールを使用する必要があります。静的割り当てと動的割り当てを組み合わせる場合は、ダイナミック プールを作成し、スタティック モードでそのプール内にブロックを追加します。
- 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 プールをドメインを介して関連付けられる同一の AEP に関連付けることはできません。

LLDP および CDP の設定の詳細については、本ガイドのブレード サーバとの連携に関する章を参照してください。

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。

拡張 GUI を使用した vCenter ドメイン プロファイルの作成

vCenter ドメインの作成時に行う作業の概要は次のとおりです（詳細は下のステップで説明します）。

- スイッチ プロファイルの作成/選択
- インターフェイス プロファイルの作成/選択
- インターフェイス ポリシー グループの作成/選択
- VLAN プールの作成/選択
- vCenter ドメインの作成
- vCenter クレデンシャルの作成

手順

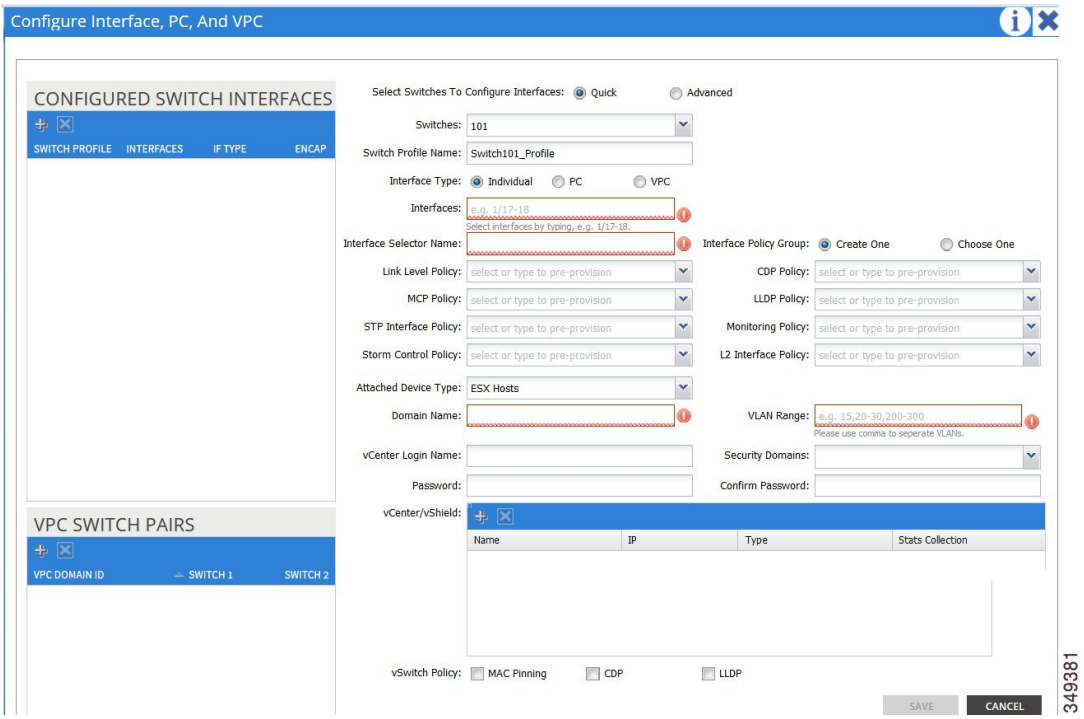
ステップ 1 メニュー バーで、[FABRIC] > [Access Policies] をクリックします。

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

ステップ 3 [Switch Policies] を右クリックし、[Configured Interfaces, PC, and VPC] をクリックします。

ステップ 4 [Work] ペインの [Configured Switch Interfaces] 領域で [Switch Profile] を展開し、次の操作を実行します。

図 3：***[Configure Interface, PC, and VPC]*** ダイアログボックスの典型的なスクリーンショット



a) [Select Switches to Configure Interfaces] フィールドで、[Quick] オプション ボタンが自動的にオンになります。

b) [Switches] フィールドのドロップダウン リストから、適切なリーフ ID を選択します。

c) [Switch Profile Name] フィールドに、スイッチ プロファイル名が自動的に入力されます。

d) 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。

e) [Interface Type] フィールドで、適切なオプション ボタンをオンにします。

f) [Interfaces] フィールドに、目的のインターフェイス範囲を入力します。

g) [Interface Selector Name] フィールドに、ESX ポートを接続するセレクタ名を入力します。

h) [Link Level Policy] ドロップダウン リストから、目的のリンク レベル ポリシーを選択します。

i) [CDP Policy] ドロップダウン リストから、目的の CDP ポリシーを選択します。

（注） 同様に、利用可能なポリシー フィールドから目的のインターフェイス ポリシーを選択します。

j) [Attached Device Type] フィールドで、[ESX Hosts] を選択します。
k) [Domain Name] フィールドに、ドメイン名を入力します。
l) [VLAN Range] フィールドに、必要に応じて VLAN の範囲を入力します。
（注） 少なくとも 200 の VLAN 番号の範囲を推奨します。インフラストラクチャ ネットワーク用に予約された VLAN は内部使用が目的のため、この VLAN ID を含む範囲を定義しないでください。
m) [vCenter Login Name] フィールドに、ログイン名を入力します。
n) （任意） [Security Domains] ドロップダウン リストから、適切なセキュリティ ドメインを選択します。
o) [Password] フィールドに、パスワードを入力します。
p) [Confirm Password] フィールドにパスワードを再入力します。
q) [vCenter/vShield] を展開します。

ステップ 5 [Create vCenter/vShield Controller] ダイアログボックスに、適切な情報を入力し、[Save] をクリックします。

ステップ 6 [Configure Interface, PC, And VPC] ダイアログボックスの [vSwitch Policy] フィールドで、目的のチェックボックスをオンにして、CDP または LLDP を有効にします。[Save] をクリックし、[Submit] をクリックします。

ステップ 7 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。

a) メニュー バーで、[VM Networking] > [Inventory] を選択します。
b) [Navigation] ペインで、[VMware] > *[Domain_name]* > [vCenter_name] の順に展開します。

[Work] ペインの [Properties] に VMM ドメイン名を表示して、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、vCenter の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 vCenter Server 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。

拡張 GUI を使用した vCenter および vShield ドメイン プロファイルの作成

vCenter および vShield ドメインの作成時に行う作業の概要は次のとおりです（詳細は下のステップで説明します）。

- スイッチ プロファイルの作成/選択
- インターフェイス プロファイルの作成/選択
- インターフェイス ポリシー グループの作成/選択
- VLAN プールの作成/選択
- vCenter および vShield ドメインの作成
- vCenter および vShield クレデンシャルの作成

手順

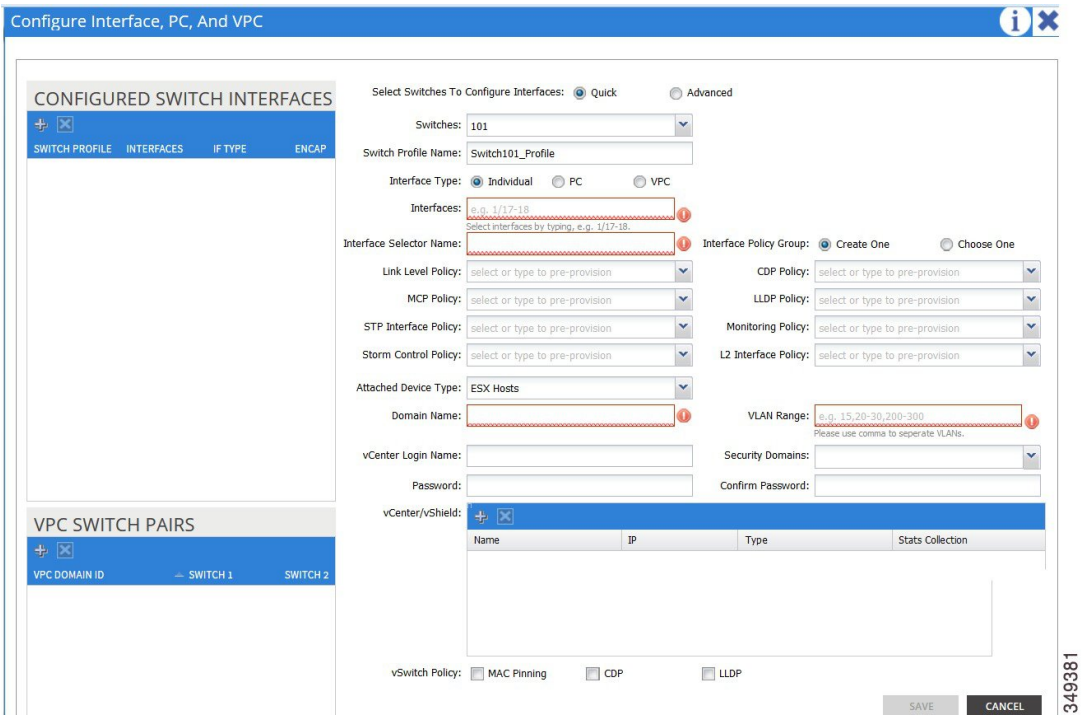
ステップ 1 メニュー バーで、[FABRIC] > [Access Policies] をクリックします。

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

ステップ 3 [Switch Policies] を右クリックし、[Configured Interfaces, PC, and VPC] をクリックします。

ステップ 4 [Work] ペインの [Configured Switch Interfaces] 領域で [Switch Profile] を展開し、次の操作を実行します。

図 4 : *[Configure Interface, PC, and VPC]* ダイアログボックスの典型的なスクリーンショット



a) [Select Switches to Configure Interfaces] フィールドで、[Quick] オプション ボタンが自動的にオンになります。

b) [Switches] フィールドのドロップダウン リストから、適切なリーフ ID を選択します。

c) [Switch Profile Name] フィールドに、スイッチ プロファイル名が自動的に入力されます。

d) 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。

e) [Interface Type] フィールドで、適切なオプション ボタンをオンにします。

f) [Interfaces] フィールドに、目的のインターフェイス範囲を入力します。

g) [Interface Selector Name] フィールドに、ESX ポートを接続するセレクタ名を入力します。

h) [Link Level Policy] ドロップダウン リストから、目的のリンク レベル ポリシーを選択します。

i) [CDP Policy] ドロップダウン リストから、目的の CDP ポリシーを選択します。

（注） 同様に、利用可能なポリシー フィールドから目的のインターフェイス ポリシーを選択します。

j) [Attached Device Type] ドロップダウン リストから、適切なデバイス タイプを選択します。
k) [Domain Name] フィールドに、ドメイン名を入力します。
l) [VLAN Range] フィールドに、必要に応じて VLAN の範囲を入力します。
（注） 少なくとも 200 の VLAN 番号の範囲を推奨します。インフラストラクチャ ネットワーク用に予約された VLAN は内部使用が目的のため、この VLAN ID を含む範囲を定義しないでください。
m) [vCenter Login Name] フィールドに、ログイン名を入力します。
n) [Password] フィールドに、パスワードを入力します。
o) [Confirm Password] フィールドにパスワードを再入力します。
p) [vCenter/vShield] を展開します。

ステップ 5 [Create vCenter/vShield Controller] ダイアログボックスに、適切な情報を入力します。

ステップ 6 [vSwitch Policy] フィールドで、目的の vSwitch ポリシーのチェック ボックスをオンにします。[Save] をクリックします。

ステップ 7 [Configure Interface, PC, and vPC] ダイアログボックスの [vSwitch Policy] フィールドで、目的のチェックボックスをオンにして、CDP または LLDP を有効にします。[Save] をクリックし、[Submit] をクリックします。

ステップ 8 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。

a) メニュー バーで、[VM Networking] > [Inventory] を選択します。
b) [Navigation] ペインで、[VMware] > *[Domain_name]* > [vCenter_name] の順に展開し、クリックします。

[Work] ペインの [Properties] に VMM ドメイン名を表示して、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、vCenter の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 vCenter Server 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、Videos Webpage 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

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。

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。

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、Videos Webpage 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。

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。

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。

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
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。

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 prefering 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。

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、Videos Webpage 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

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] > [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。

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、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] > [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。

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。

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。

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

- 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、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、[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。

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。

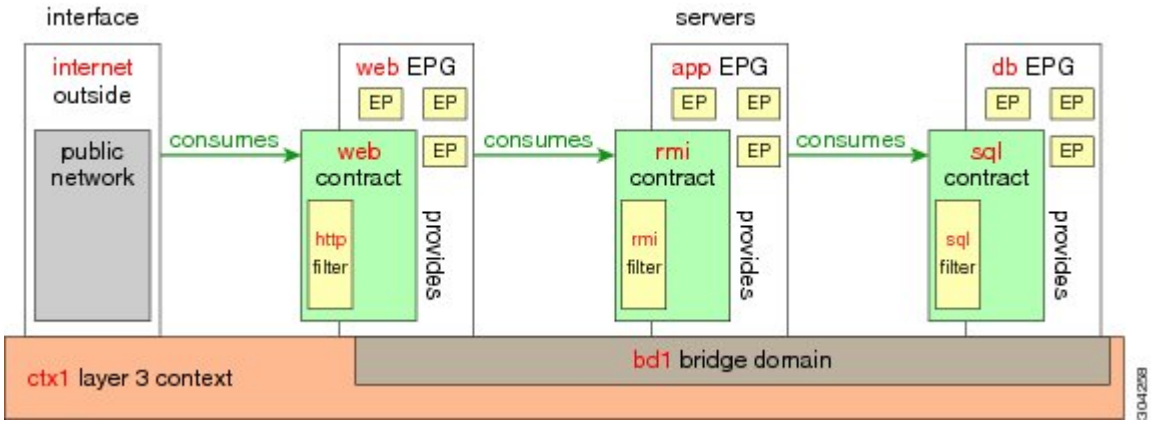
契約は、エンドポイント グループ間（EPG 間）の通信をイネーブルにするポリシーです。これらのポリシーは、アプリケーション層間の通信を指定するルールです。契約が EPG に付属していない場合、EPG 間の通信はデフォルトでディセーブルになります。EPG 内の通信は常に許可されているので、EPG 内の通信には契約は必要ありません。

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 *5*：*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

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

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

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

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

ステップ 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。
[Add Consumed Contract] ダイアログボックスが表示されます。

（注） db、app、および web EPG は、アイコンで表示されます。

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。