# コア ACI ファブリック サービスのプロビジョニング

この章の内容は、次のとおりです。


- 時刻同期と NTP （1 ページ）
- DHCP リレー ポリシーの設定 （12 ページ）
- DNS サービス ポリシーの設定 （16 ページ）
- カスタム証明書の設定 （23 ページ）
- ファブリック全体のシステム設定のプロビジョニング （25 ページ）
- グローバル ファブリック アクセス ポリシーのプロビジョニング （39 ページ）


## 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） 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。
- 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、ファブリックによるNTPサーバへの接続を許可する方法です。

# 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。

# 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。
b) をクリックして **有効になっている** の **認証状態** フィールドおよび展開、 **NTP クライアントの認証キー** テーブルが表示され、重要な情報を入力します。**Update** と **Next** をクリックします。
c) [+] 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。
d) [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。[送信（Submit）] をクリックします。

# NX-OS スタイルの CLI を使用した NTP の設定

ACI ファブリックをアウトオブバンド管理で展開する場合、ファブリックの各ノードは ACI ファブリックの外部から管理されます。アウトオブバンド管理の NTP サーバを設定すると、各ノードは一貫したクロック ソースとして同じNTPサーバに個々に照会することができます。

### 手順

**ステップ 1** **configure**

コンフィギュレーション モードに入ります。

例：

```
apic1# configure
```

**ステップ 2** **template ntp-fabric** *ntp-fabric-template-name*

ファブリックの NTP テンプレート (ポリシー) を指定します。

例：

```
apic1(config)# template ntp-fabric pol1
```

**ステップ 3** **[no] server** *dns-name-or-ipaddress* **[prefer] [use-vrf** {**inband-mgmt** | **oob-default**}] [ **key** *key-value*]

アクティブ NTP ポリシーの NTP サーバを設定します。このサーバをアクティブ NTP ポリシーの優先サーバにするには、**prefer** キーワードを含めます。NTP 認証が有効になっている場合は、参照キー ID を指定します。To specify the in-band or out-of-band management access VRF, include the **use-vrf** keyword with the **inb-default** or **oob-default** keyword.

例：

```
apic1(config-template-ntp-fabric)# server 192.0.20.123 prefer use-vrf oob-mgmt
```

**ステップ 4** **[no] authenticate**

NTP 認証を有効または無効にします。

例：

```
apic1(config-template-ntp-fabric)# no authenticate
```

**ステップ 5** **[no] authentication-key** *key-value*

認証 NTP 認証を設定します。指定できる範囲は 1 ～ 65535 です。

例：

```
apic1(config-template-ntp-fabric)# authentication-key 12345 md5 "key_value"
```

**ステップ 6** **[no] trusted-key** *key-value*

信頼 NTP 認証を設定します。指定できる範囲は 1 ～ 65535 です。

例：

```
apic1(config-template-ntp-fabric)# trusted-key 54321
```

**ステップ 7** **exit**

グローバル コンフィギュレーション モードに戻ります。

例：

```
apic1(config-template-ntp-fabric)# exit
```

**ステップ 8** **template pod-group** *pod-group-template-name*

ポッドグループ テンプレート（ポリシー）を設定します。

例：

```
apic1(config)# template pod-group allPods
```

**ステップ 9** **inherit ntp-fabric** *ntp-fabric-template-name*

事前に設定した NTP ファブリック テンプレート (ポリシー) を使用するように NTP ファブリックのポッドグループを設定します。

例：

```
apic1(config-pod-group)# inherit ntp-fabric pol1
```

**ステップ 10** **exit**

グローバル コンフィギュレーション モードに戻ります。

例：

```
apic1(config-template-pod-group)# exit
```

**ステップ 11** **pod-profile** *pod-profile-name*

ポッド プロファイルを設定します。

例：

```
apic1(config)# pod-profile all
```

**ステップ 12** **pods** {*pod-range-1-255* | **all**}

一連のポッドを設定します。

例：

```
apic1(config-pod-profile)# pods all
```

**ステップ 13** **inherit pod-group** *pod-group-name*

事前に設定したポッド グループにポッドプロファイルを関連付けます。

例：

```
apic1(config-pod-profile-pods)# inherit pod-group allPods
```

**ステップ 14** **end**

EXEC モードに戻ります。

例：

```
apic1(config-pod-profile-pods)# end
```

---

例

次に、優先アウトオブバンド NTP サーバを設定し、その設定および展開を確認する例を示します。

```
apic1# configure t
apic1(config)# template ntp-fabric pol1
apic1(config-template-ntp-fabric)# server 192.0.20.123 use-vrf oob-default
apic1(config-template-ntp-fabric)# no authenticate
apic1(config-template-ntp-fabric)# authentication-key 12345 md5 abcdef1235
apic1(config-template-ntp-fabric)# trusted-key 12345
apic1(config-template-ntp-fabric)# exit
apic1(config)# template pod-group allPods
```

```
apic1(config-pod-group)# inherit ntp-fabric pol1
apic1(config-pod-group)# exit
apic1(config)# pod-profile all
apic1(config-pod-profile)# pods all
apic1(config-pod-profile-pods)# inherit pod-group allPods
apic1(config-pod-profile-pods)# end
apic1#

apic1# show ntpq
 nodeid     remote        refid   st    t   when   poll   reach  delay    offset   jitter

 ------  -  ------------  ------  ----  --  -----  -----  -----  ------   ------   ------

 1       *  192.0.20.123  .GPS.         u   27     64     377    76.427   0.087    0.067

 2       *  192.0.20.123  .GPS.         u   3      64     377    75.932   0.001    0.021

 3       *  192.0.20.123  .GPS.         u   3      64     377    75.932   0.001    0.021
```

# REST API を使用した NTP の設定

**手順**

**ステップ 1** NTP を設定します。

**例**：

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

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

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

**例**：

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

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

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

**例**：

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

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

# 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。

# NX-OSスタイルの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** SSH プロトコルを使用して、ファブリック内の APIC コントローラにログオンします。

**ステップ 2** 次に示すように、ノードに接続して NTP ピアのステータスを確認します。

```
apic1# fabric  node_name show ntp peer-status
```

**ステップ 3** ファブリック内のさまざまなノードに対して、ステップ 2 を繰り返します。

# NTP サーバー

NTP サーバ機能は、クライアントのスイッチも NTPサーバとして動作して、下流のクライアントに NTP の時間情報を提供できるようにします。NTP サーバを有効にすると、スイッチ上の NTP デーモンは、NTP クライアントからのすべてのユニキャスト (IPv4 または IPv6) リクエ

ストに対し、が時間情報によって応答します。NTP サーバの実装は、NTP RFCv3 に準拠しています。NTP RFC に従い、サーバはクライアントに関連する状態情報は維持しません。

- NTP サーバは、NTP クライアント リクエストを処理するスイッチのインバンド/アウトオブバンド管理 IP を有効にします。
- NTP サーでは、既存の NTP クライアント機能のように、インバンド/アウトオブバンド管理 VRF でのみ動作します。
- NTP サーバは、両方の管理 VRF で着信 NTP 要求に応答し、同じ VRF を使用して応答します。
- NTP サーバはIPv4 と IPv6 の両方をポートします。
- スイッチは、IPv4 クライアントとして同期して IPv6 サーバとして動作すること、およびその逆が可能です。
- スイッチは、アウトオブバンド管理 VRF 経由で NTP クライアントとして同期し、インバンド管理 VRF 経由でサーバとして動作すること、およびその逆が可能です。
- 追加契約または IP テーブルの設定は必要ありません。
- スイッチは上流のサーバと同期すると、サーバとして時間情報をストラタム番号とともに送信します。この番号はシステムのピアのストラタム番号から 1 増えたものになります。
- スイッチ クロックが非統制 (アップストリーム サーバに同期されていない) の場合、サーバはストラタム 16 で時間情報を送信します。クライアントはこのサーバには同期できません。

デフォルトでは、NTP サーバ 機能は無効になっています。これはポリシーの設定によって明示的に有効にする必要があります。

（注） クライアントは、リーフのインバンド、アウトオブ バンドの IP を NTP サーバ IP として使用できます。クライアントはまた、NTPサーバ IP の一部である EPG の BD SVI も、NTP サーバ IP として使用できます。

（注） ファブリックのスイッチは、同じファブリックの他のスイッチに同期するべきではありません。ファブリック スイッチは常に、外部の NTP サーバに同期するべきです。

## GUI を使用した NTP サーバの有効化

このセクションでは、APIC GUI で NTP を設定して NTPサーバを有効にする方法について説明します。

手順

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

**ステップ 2** **ナビゲーション** ウィンドウで、**Pod Policies** > **Policies** を選択します。

**Date and Time** オプションが **Navigation** ウィンドウに表示されます。

**ステップ 3** **Navigation** ウィンドウで、、**Date and Time** を右クリックして **Create Date and Time Policy** を選択します。

**Create Date and Time Policy** ダイアログが **Work** ウィンドウに表示されます。

**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。

b) **Server State** オプションで、**enabled** をクリックします。

**Server State** によって、スイッチを NTP サーバとして動作し、下流のクライアントに NTP 時間情報を提供できるようにします。

（注） サーバ機能をサポートする場合、サーバは常にピア設定にすることを推奨します。これにより、サーバはクライアントに対し、一貫した時間を提供できるようになります。

**Server State** を有効にすると、次のことが可能になります:

- NTP サーバは、上流のサーバに同期するスイッチに対し、時刻情報とともにストラタム番号を送信します。この番号はシステムのピアのストラタム番号から 1 つ増えたものになります。
- スイッチのクロックが上流サーバに同期していない場合、サーバは時刻情報とストラタム 16 を送信します。クライアントはこのサーバに同期することはできません。

（注） サーバ機能をサポートする場合、サーバは常にピア設定にすることを推奨します。ピア設定では、クライアントに対し一貫した時間を提供できます。

c) **Master Mode** オプションで、**enabled** をクリックします。

**Master Mode** を使用すれば、指定された NTP サーバが、下流のクライアントに対し、設定されたストラタム番号とともに、調整されていないローカルクロック時刻を提供することが可能になります。たとえば、NTP サーバとして動作しているリーフ スイッチは、クライアントとして動作しているリーフスイッチに対し、調整されていないローカルクロック時刻を提供できます。

（注）
- **Master Mode** が適用できるのは、サーバのクロックが調整されていない場合のみです。
- デフォルトのマスター モードの **Stratum Value** は 8 です。

d) **Stratum Value** フィールドには、NTP クライアントが同期した時刻を取得するときのストラタム番号を指定します。範囲は 1 ～ 14 です。
e) **Next** をクリックします。
f) [+] 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。
g) [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** ウィンドウで、**Pod Policies** を選択し、**Policy Groups** を右クリックします。

**Create Pod Policy Group** ダイアログが表示されます。

**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。

**ステップ 11** [送信（Submit）] をクリックします。

## CLI を使用した NTP サーバの有効化

このセクションでは、CLI コマンドを使用して、NTP サーバ機能を有効にする方法について説明します。

始める前に

手順

**ステップ 1** グローバル設定モードに入ります:

例：

```
apic1#configure t
```

**ステップ 2** アクティブな NTP ポリシーのための NTP サーバを設定します。

例：

```
apic1(config)#template ntp-fabric default
```

**ステップ 3** NTP サーバを指定します。

例：

```
apic1(config-template-ntp-fabric)#server 10.81.254.201 prefer use-vrf oob-default
```

**ステップ 4** NTP サーバとして動作するようにスイッチを有効にします。

例：

```
apic1(config-template-ntp-fabric)#server-mode
```

**ステップ 5** ストラタム値 10 の NTP マスターモードで動作するようにスイッチを有効にします。

例：

```
apic1(config-template-ntp-fabric)#master stratum 10
```

**ステップ 6** グローバル設定モードに戻ります。

例：

```
aic1(config-template-ntp-fabric)#exit
```

## REST API を使用した NTP サーバの有効化

この例では、REST API を使用した NTP サーバの設定方法を示します。

手順

`serverState` および `masterMode` を有効にして、`StratumValue` を指定します (`StratumValue` は 1 ～ 14 から選択できます)。

例：

```
POST url: https://APIC-IP/api/node/mo/uni/fabric/time-test.xml
<datetimePol name="testdatetime" adminSt="enabled" authSt="enabled" serverState="enabled"
 masterMode="enabled" StratumValue="10" >
```

# 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。

# GUI を使用した APIC インフラストラクチャに対する DHCP サーバ ポリシーの設定

- アプリケーション エンドポイント グループ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。ドメインにそれらの関連付けが確立されていない場合、APIC では EPG の展開を続行しますが障害が発生します。
- 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。

### エンドポイント グループの DHCP リレー ポリシーの導入

#### 始める前に

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] フィールドのドロップダウン リストから、作成済みの DHCP ポリシーの名前（DhcpRelayP）を選択するか、[Create DHCP Relay Policy] を選択して新しいリレー ポリシーを作成します。

c) [DHCP Option Policy] で、既存のオプション ポリシーを選択するか、[Create DHCP Option Policy] を選択して新しいオプション ポリシーを作成します。

d) [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。

# NX-OSスタイルCLIを使用したAPICインフラストラクチャのDHCPサーバ ポリシーの設定

- アプリケーション エンドポイント グループ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。ドメインにそ

れらの関連付けが確立されていない場合、APIC では EPG の展開を続行しますが障害が発生します。

- 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。

### 始める前に

DHCP サーバ アドレスに到達するためにレイヤ 2 またはレイヤ 3 接続が設定されていることを確認します。

### 手順

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

例：

**エンドポイント グループの DHCP リレー ポリシー**

```
apic1(config)# tenant infra
apic1(config-tenant)# template dhcp relay policy DhcpRelayP
apic1(config-tenant-template-dhcp-relay)# ip address 10.0.0.1 tenant infra application access epg default
apic1(config-tenant-template-dhcp-relay)# exit
apic1(config-tenant)# interface bridge-domain default
apic1(config-tenant-interface)# dhcp relay policy tenant DhcpRelayP
apic1(config-tenant-interface)# exit
```

例：

**レイヤ 3 Outside の DHCP リレー ポリシー**

```
ifav28-ifc2(config)# tenant dhcpTn
ifav28-ifc2(config-tenant)# template dhcp relay policy DhcpRelayPol
ifav28-ifc2(config-tenant-template-dhcp-relay)# ip address 11.1.1.11 tenant dhcpTn application ap epg serverEpg
ifav28-ifc2(config-tenant-template-dhcp-relay)# exit
ifav28-ifc2(config-tenant)# exit
ifav28-ifc2(config)# leaf 2001
ifav28-ifc2(config-leaf)# interface ethernet 1/4
ifav28-ifc2(config-leaf-if)# no switchport
ifav28-ifc2(config-leaf-if)# vrf member tenant dhcpTn vrf v1
ifav28-ifc2(config-leaf-if)# dhcp relay policy tenant DhcpRelayPol
ifav28-ifc2(config-leaf-if)# exit
```

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

- このタスクは、vShield ドメイン プロファイルを作成するユーザの前提条件です。
- アプリケーション エンドポイント グループ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。ドメインにそ

れらの関連付けが確立されていない場合、APIC では EPG の展開を続行しますが障害が発生します。

- 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。

### 始める前に

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

---

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

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

例：

**EPG の DHCP リレー ポリシー**

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

POST https://apic-ip-address/api/mo/uni.xml


  <fvTenant name="infra">

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

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

  </fvTenant>
</polUni>
```

例：

**レイヤ 3 Outside の DHCP リレー ポリシー**

（注） **l3extLIfP** で適切な名前とオーナーを使用して DHCP リレー ラベルを指定する必要があります。

```
<polUni>
  <fvTenant name="dhcpTn">
    <l3extOut name="Out1" >
      <l3extLNodeP name="NodeP" >
        <l3extLIfP name="Intf1">
```

```
            <dhcpLbl name="DhcpRelayPol" owner="tenant" />
          </l3extLIfP>
        </l3extLNodeP>
      </l3extOut>
    </fvTenant>
<polUni>

POST https://apic-ip-address/api/mo/uni.xml
```

# 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。

（注） 管理 EPG では、デフォルトの DNS ポリシーのみがサポートされます。

- 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<br>（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<br>（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。

# 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。

# 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
```

# 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

### 始める前に

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。

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

手順

**ステップ 1** NX-OS CLI で、次に示すようにしてコンフィギュレーション モードに入ります。

例：

```
apic1# configure
apic1(config)#
```

**ステップ 2** DNS サーバ ポリシーを設定します。

例：

```
apic1(config)# dns
apic1(config-dns)# address 172.21.157.5 preferred
apic1(config-dns)# address 172.21.157.6
apic1(config-dns)# domain company.local default
apic1(config-dns)# use-vrf oob-default
```

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

例：

```
apic1(config)# tenant mgmt
apic1(config-tenant)# vrf context oob
apic1(config-tenant-vrf)# dns label default
```

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

### 始める前に

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** DNS サービス ポリシーを設定します。

例：

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

<dnsProfile name="default">

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

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

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

</dnsProfile>
```

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

例：

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

# NX-OS スタイル CLI を使用した DNS プロファイルがファブリック コントローラ スイッチに設定および適用されていることの確認

**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**：

```
apic1# show running-config dns

# Command: show running-config dns
# Time: Sat Oct  3 00:23:52 2015
  dns
    address 172.21.157.5 preferred
    address 172.21.157.6
    domain company.local default
    use-vrf oob-default
    exit
```

**ステップ 2** DNS ラベルの設定を確認します。

**例**：

```
apic1# show running-config tenant mgmt vrf context oob

# Command: show running-config tenant mgmt vrf context oob
# Time: Sat Oct  3 00:24:36 2015
  tenant mgmt
    vrf context oob
      dns label default
      exit
    exit
```

**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**：

```
apic1# cat /etc/resolv.conf
# Generated by IFC

nameserver 172.21.157.5
nameserver 172.21.157.6
```

# カスタム証明書の設定

## カスタム証明書の設定のガイドライン

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

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

注意：ダウンタイムの可能性があるため、メンテナンス時間中にのみこのタスクを実行してください。ダウンタイムは外部ユーザまたはシステムからのAPICクラスタおよびスイッチへのアクセスには影響しますが、APICとスイッチの接続には影響しません。スイッチ上のNGINXプロセスも影響を受けますが、外部接続のみでファブリックのデータプレーンには影響ありません。APIC、設定、管理、トラブルシューティングなどへのアクセスは影響を受けることになります。この操作中にファブリック内のすべてのWebサーバの再起動が予期されます。

### 始める前に

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

### 手順

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

**ステップ 2** [Navigation] ペインで、**[Public Key Management]** > **[Certificate Authorities]** の順に選択します。

**ステップ 3** [Work] ペインで、**[Actions]** > **[Create Certificate Authority]** の順に選択します。

**ステップ 4** [Create Certificate Authority] ダイアログボックスの [Name] フィールドに、認証局の名前を入力します。

**ステップ 5** [Certificate Chain] フィールドに、Application Policy Infrastructure Controller（APIC）の証明書署名要求（CSR）に署名する認証局の中間証明書およびルート証明書をコピーします。

証明書は、Base64 エンコード X.509（CER）形式である必要があります。中間証明書はルート CA 証明書の前に配置されます。次の例のようになります。

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

**ステップ 6** [Submit] をクリックします。

**ステップ 7** [Navigation] ペインで、**[Public Key Management]** > **[Key Rings]** の順に選択します。

**ステップ 8** [Work] ペインで、**[Actions]** > **[Create Key Ring]** の順に選択します。

**ステップ 9** [Create Key Ring] ダイアログボックスで、[Name] フィールドに、名前を入力します。

**ステップ 10** [Certificate] フィールドには、コンテンツを追加しないでください。

**ステップ 11** [Modulus] フィールドで、目的のキー強度のラジオボタンをクリックします。

**ステップ 12** [Certificate Authority] フィールドのドロップダウン リストから、前に作成した認証局を選択します。[Submit] をクリックします。

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

[Work] ペインの [Key Rings] 領域では、作成したキー リングに対する [Admin State] に [Started] と表示されます。

**ステップ 13** [Navigation] ペインで、**[Public Key Management]** > **[Key Rings]** > ***[key_ring_name]*** の順に選択します。

**ステップ 14** [Work] ペインで、**[Actions]** > **[Create Certificate Request]** の順に選択します。

**ステップ 15** [Subject] フィールドに、APIC の完全修飾ドメイン名（FQDN）を入力します。

**ステップ 16** 必要に応じて、残りのフィールドに入力します。

（注） 使用可能なパラメータの説明については、[Create Certificate Request] ダイアログボックスでオンライン ヘルプ情報を確認してください。

**ステップ 17** [Submit] をクリックします。

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

**ステップ 18** [Navigation] ペインで、**[Public Key Management]** > **[Key Rings]** > ***[key_ring_name]*** の順に選択します。

**ステップ 19** [Work] ペインの [Certificate] フィールドに、認証局から受信した署名付き証明書を貼り付けます。

**ステップ 20** [Submit] をクリックします。

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

キーが確認されて [Work] ペインの [Admin State] が [Completed] に変わり、HTTP ポリシーを使用できるようになります。

**ステップ 21** メニュー バーで、**[Fabric]** > **[Fabric Policies]** の順に選択します。

**ステップ 22** [Navigation] ペインで、**[Pod Policies]** > **[Policies]** > **[Management Access]** > **[default]** の順に選択します。

**ステップ 23** [Work] ペインの [Admin Key Ring] ドロップダウン リストで目的のキー リングを選択します。

**ステップ 24** [Submit] をクリックします。
すべての Web サーバが再起動されます。証明書がアクティブになり、デフォルト以外のキーリングが HTTPS アクセスに関連付けられています。

### 次のタスク

証明書の失効日には注意しておき、期限切れになる前に対応する必要があります。更新された証明書に対して同じキーペアを維持するには、CSR を維持する必要があります。これは、CSR にはキー リング内の秘密キーとペアになる公開キーが含まれているためです。証明書が期限切れになる前に、同じ CSR を再送信する必要があります。キー リングを削除すると、APIC に内部的に保存されている秘密キーも削除されるため、新しいキー リングの削除または作成は行わないでください。

# ファブリック全体のシステム設定のプロビジョニング

## APICインバンドまたはアウトオブバンド接続設定(preferences)の設定

このトピックでは、APIC サーバ認証サーバまたは ACI ファブリックに外部 SNMP サーバなどのデバイスの管理アクセスのインバンドおよびアウトオブバンド接続の間で切り替える方法について説明します。有効化 **インバンド** ACI ファブリックのリーフ スイッチからの外部デバイ

スに APIC サーバ間のインバンド管理接続を実行します。有効化 **ooband** ACI ファブリックに外部接続の外部デバイスに APIC サーバ間のアウトオブバンド管理接続を実行します。

### 始める前に

インバウンドおよびアウトバウンド管理ネットワークを構成します。詳細については、「管理」(『*Cisco APIC* 基本設定ガイド、リリース *3.x*』) を参照してください。

### 手順

**ステップ 1** メニューバーで、 **System** > **System Settings** の順にクリックします。
**ステップ 2** ナビゲーション バーで、をクリックして **APIC 接続設定 (preferences)** 。
**ステップ 3** ポリシーを有効にするにはクリックして **インバンド** または **ooband** 。
**ステップ 4** [送信（Submit）] をクリックします。

# クォータ管理ポリシーの設定

Application Policy Infrastructure Controller (APIC) リリース 2.3(1) 移行から、テナント管理者が設定できるオブジェクトの数に制限が設けられました。これにより、管理者は、テナントを超えてグローバルに追加される管理対象オブジェクトの数を制限できるようになりました。

この機能は、テナントまたはテナントのグループが、リーフごと、またはファブリックごとの ACI の最大数を超えないようにする点で、または利用可能なリソースの大部分を不当に消費して、同じファブリックの他のテナントに影響を及ぼすことがないようにする点で役立ちます。

### 手順

**ステップ 1** メニュー バーで、**System** > **System Settings** をクリックします。
**ステップ 2** **Quota** を右クリックして、**Create Quota Configuration** を選択します。
**ステップ 3** **Class** フィールドで、クォータによる制限を掛けるオブジェクトのタイプを選択します。
**ステップ 4** **Container Dn** フィールドに、クラスを説明する識別名 (DN) を入力します。
**ステップ 5** **Exceed Action** フィールドで、**Fail Transaction Action** または **Raise Fault Action** を選択します。
**ステップ 6** **Max Number** フィールドで、作成できる管理対象オブジェクトの最大数を入力します。これを超えると、超過アクションが適用されることになります。
**ステップ 7** [送信（Submit）] をクリックします。

# 適用 BD 例外リストの作成

このトピックでは、適用対象のブリッジ ドメインには従わない、サブネットのグローバルな例外リストの作成方法について説明します。適用 BD の機能を設定している場合、対象のエンドポイント グループ (EPG) が ping を送信できるのは、関連付けられたブリッジ ドメイン内のサブネット ゲートウェイだけです。

例外 IP アドレスは、すべての VRF のすべての BD ゲートウェイに ping を送信できます。

L3Out 用に設定されたループバック インターフェイスでは、対象のループバック インターフェイスに合わせて設定された IP アドレスへの到達可能性は適用されません。

EBGP ピアとなる IP アドレスが、L3Out インターフェイスのサブネットとは異なるサブネットに存在している場合には、許容例外サブネットにピア サブネットを追加する必要があります。そうしないと、送信元 IP アドレスが L3Out インターフェイスのサブネットとは異なるサブネットに存在するため、eBGP トラフィックがブロックされます。

### 始める前に

適用対象のブリッジ ドメイン (BD) を作成します。

### 手順

**ステップ 1** メニュー バーで、**System** > **System Settings** を選択します。

**ステップ 2** **BD Enforced Exception List** をクリックします。

**ステップ 3** **Exception List** の [+] をクリックします。

**ステップ 4** 任意のサブネット ゲートウェイに ping を送信できるサブネットの IP アドレスとネットワーク マスクを追加します。

**ステップ 5** これを繰り返して、適用ブリッジ ドメインの例外となるサブネットを追加します。

**ステップ 6** [送信（Submit）] をクリックします。

# BGP ルータ リフレクタ ポリシーとルート リフレクタ ノード エンドポイントの作成

このトピックでは、ACI ファブリック ルート リフレクタを作成する方法について説明します。リフレクタは、ファブリック内で外部ルートを配布するために、マルチ プロトコル BGP (MP-BGP) を使用します。ACI ファブリックでルート リフレクタをイネーブルにするには、ファブリックの管理者がルート リフレクタになるスパイン スイッチを選択して、自律システム（AS）番号を提供する必要があります。ルート リフレクタが ACI ファブリックで有効になれば、管理者は、外部ネットワークへの接続を設定できます。

### 始める前に

**必須項目**：

- ACI ファブリックに外部ルータを接続するには、ファブリック インフラストラクチャの管理者がボーダー ゲートウェイ プロトコル（BGP）のルート リフレクタとしてスパイン ノードを設定するひつようがあります。
- 冗長性のために、複数のスパインがルータ リフレクタ ノードとして設定されます（1 台のプライマリ リフレクタと 1 台のセカンダリ リフレクタ）。

### 手順

**ステップ 1** BGP ルート リフレクタ ポリシーを作成するには、次の手順を実行します:

a) メニュー バーで、**System** > **System Settings** をックリックします。
b) **BGP Route Reflector** をクリックします。
c) 入力自律システム番号を入力します。
d) **Route Reflector Nodes** で [+] をクリックします。
e) スパイン ルート リフレクタ ノードの ID エンドポイントを入力し、**Submit** をクリックします。

**ステップ 2** 外部ルート リフレクタ ノードのエンドポイントを作成するには、次の手順に従います:

a) **External Route Reflector Nodes** で [+] をクリックします。
b) 外部ルート リフレクタ ノードのエンドポイントとして機能するスパインを選択します。
c) これがマルチサイトによって管理されるサイトである場合には、インターサイト スパイン ルート リフレクタも指定できます。
d) [送信（Submit）] をクリックします。

# ファブリック全体のコントロール プレーンの MTU ポリシーを設定する

このトピックでは、ファブリック全体のコントロール プレーン (CP) の MTU ポリシーを作成する方法について説明します。これは、ファブリックのノード (APIC とスイッチ) から送信されたコントロール プレーン パケットのグローバル MTU サイズを設定します。

マルチポッド トポロジでは、ファブリック外部ポートの MTU 設定は、CP MTU の値セット以上である必要があります。そうしないと、ファブリックの外部ポートが CP MTU パケットをドロップする可能性があります。

（注） MTU を IPN から継承する L3Out インターフェイス プロファイルを設定するには 9150 にします。IPN 全体で使用される MTU を 2916 に設定する必要がある場合には、L3Out インターフェイス プロファイル内で明示的に設定する必要があります ( **Tenants** > ***tenant-name*** > **Networking** > **External Routed Networks** > **Create Routed Outside** > **Nodes and Interface Protocol Profiles** > **Create Node Profile** > **Create Interface Profile** で設定します)。

IPN または CP MTU を変更する場合、Cisco では CP MTU 値を変更し、次にリモート ポッドのスパイン上の MTU 値を変更することをお勧めします。これで、MTU の不一致によりポッド間の接続が失われるリスクが減少します。

**手順**

**ステップ 1** メニュー バーで、**System** > **System Settings** をックリックします。

**ステップ 2** **Control Plane MTU** をクリックします。

**ステップ 3** ファブリック ポートの MTU を入力します。

**ステップ 4** [送信（Submit）] をクリックします。

# COOP グループ ポリシーの作成

このトピックでは、スパイン プロキシを (ロケーションと id) のマッピング情報を通信するために使用される協議会の Oracle プロトコル (COOP) グループ ポリシーを作成する方法について説明します。リーフ スイッチは、Zero Message Queue（ZMQ）を使用して、エンドポイント アドレス情報をスパイン スイッチ「Oracle」に転送します。スパイン ノードで実行している COOP によって、すべてのスパイン ノードが一貫性のあるエンドポイント アドレスとロケーション情報のコピーを維持することができ、さらに、ロケーション マッピング データベースに対するエンドポイント ID の分散ハッシュ テーブル（DHT）レポジトリを維持することができます。

**手順**

**ステップ 1** メニューバーで、 **System** > **System Settings** の順にクリックします。

**ステップ 2** **COOP Group** をクリックします。

**ステップ 3** ポリシー プロパティ タイプを選択します。タイプは、 **互換性のある型** または **厳密な型** 。

Oracle ノードでは、システムによって自動的に入力されて、fabric 背表紙です。

**ステップ 4** [Submit] をクリックします。

# エンドポイント ループ保護の設定

エンドポイントのループ保護ポリシーでは、頻繁な MAC の移動を処理することによる、ループ検出の方法を指定します。EP ループ保護を設定するには、次の手順を実行します:

**手順**

**ステップ 1** メニュー バーで、**System** > **System Settings** を選択します。

**ステップ 2** をクリックして **エンドポイント コントロール** 。

**ステップ 3** **Ep Loop Protection** タブをクリックします。

**ステップ 4** ポリシーを有効にするには、**Enabled** をクリックします (**Administrative State** フィールドにあります)。

**ステップ 5** オプション。ループを検出の間隔を設定します。これはループを検出するための時間を指定します。指定できる範囲は 30～ 300 秒です。デフォルトの設定は 60 秒です。

**ステップ 6** ループ検出乗算係数を設定します。これは、ループ検出間隔内で単一の EP がポート間を移動した回数です。範囲は 1 ～ 255 です。デフォルトは 4 です。

**ステップ 7** ループを検出したときに実行するアクションを選択します。

アクションとしては、次のものがあります:

- **BD Learn Disable**
- **Port Disable**

デフォルトは **Port Disable** です。

**ステップ 8** [送信（Submit）] をクリックします。

# 不正なエンドポイントの制御ポリシーについて

別の ToR ポートで頻繁かつ急速にパケットを挿入し、802.1 q を変更することで (したがってエンドポイントのエミュレートが移動します)、不正なエンドポイントはラック上部 (ToR) のスイッチに攻撃して、学習クラスと EPG ポートが変更されることになります。誤設定により頻繁に IP アドレスと MAC アドレスが変更 (移動する) されることになります。

ファブリックの急速な移動などで、大きなネットワークの不安定状態、高い CPU 使用率、まれなケースでは、大量かつ長期のメッセージおよびトランザクション サービス (MTS) バッファ消費のため、エンドポイント マッパー (EPM) および EPM クライアント (EPMC) がクラッシュすることになります。また、このような頻繁な移動により、EPM および EPMC ログが非常にすばやくロール オーバーされ、無関係なエンドポイントのデバッグを妨害する可能性があります。

不正なエンドポイントの制御機能は脆弱性にすばやく対処します。

- このような急速 MAC および IP エンドポイントの移動の特定

- 一時的に移動を停止することで、エンドポイントを静的にします (したがって、エンドポイントを隔離します)
- **不正 EP 検出間隔** の静的エンドポイントを保持し、不正なエンドポイントとの間のトラフィックをドロップします。この時間が経過すると、認可されていない MAC または IP アドレスが削除されます
- ホスト トラッキング パケットを生成することで、影響を受ける MAC または IP アドレスを再学習するようシステムを有効にします
- 障害が発生すると是正措置が有効になります

不正なエンドポイント制御ポリシーはグローバルに設定されており、他のループ防止方法とは異なり、個々のエンドポイント レベルの機能です (IP および MAC アドレス)。ローカルまたはリモートの移動を区別していません。いかなる種類のインターフェイスの変更も、エンドポイントを隔離する必要があるかどうかを決定する際に移動と見なされます。

不正なエンドポイント制御機能は、デフォルトで無効になっています。

## 不正エンドポイント制御ポリシーの制限事項

不正エンドポイント制御ポリシーを使用する際には、次の制限が適用されます:

- 不正エンドポイント制御ポリシーのパラメータを変更しても、既存の不正エンドポイントには影響しません。
- 不正エンドポイントが有効になっていても、ループ検出とブリッジドメイン移動頻度は有効になりません。
- 不正エンドポイント機能を無効にすると、すべての不正エンドポイントがクリアされます。
- Cisco Application Policy Infrastructure Controller (Cisco APIC) をアップグレードまたはダウングレードする前には、不正エンドポイント機能を無効にする必要があります。
- エンドポイント マッパー (EPM) の値は、不正エンドポイントのパラメータに制限を課します。この範囲外のパラメータ値を設定すると、Cisco APIC 適切でないパラメータごとにエラーが発生します。
- 不正エンドポイント機能は、リモートのリーフ スイッチまたは Cisco ACI マルチサイトではサポートされていません。

## GUI を使用した不正なエンドポイントの制御ポリシーの構成

Cisco Application Policy Infrastructure Controller (Cisco APIC) GUIを使用して、不正なエンドポイントを検出および削除するために、ファブリックの **Rogue EP Control** ポリシーを設定できます。このトピックには、TOR スイッチの不正なエンドポイントをアドホックにクリアする手順も含まれています。

ポリシー オプションには、次の有効な値とサポートされている値があります。

- **Rogue EP Detection Interval**—不正なエンドポイント検出のインターバルを設定します。これは、不正なエンドポイントを検出する時間を指定します。有効な値は 0 ～ 65535 秒です。デフォルトは 60 です。
- **Hold Interval (sec)**—エンドポイントが不正であると宣言された後の時間 (秒単位)。静的に保持されますので、学習が防止され、不正エンドポイントとの間のトラフィックがドロップされます。このインターバルの後、エンドポイントは削除されます。有効値は 1800 ～ 3600 です。デフォルト値は 1800 です。
- **Rogue EP Detection Multiplication Factor**—エンドポイントが許可されていないかどうかを判断するための不正なエンドポイント検出倍率を設定します。エンドポイントがこの数よりも多く移動する場合、EP 検出間隔内で、エンドポイントは不正と宣言されます。有効値は 2 ～ 10 です。デフォルト値は 6 です。

**手順**

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

**ステップ 2** ナビゲーション バーの **[Endpoint Controls]** をクリックし、**[Rogue EP Control]** タブをクリックします。

**ステップ 3** **[Administrative State]** を **[Enabled]** に設定します。

**ステップ 4** オプション。**[Rogue EP Detection Interval (sec)]**、**[Rogue EP Detection Multiplication Factor]**、または **[Hold Interval (sec)]** をリセットします。

**ステップ 5** （任意） TOR スイッチで不正なエンドポイントをクリアするには、次の手順を実行します。

a) Cisco APICメニュー バーで、**[Fabric]** > **[Inventory]** の順にクリックします。
b) ナビゲーションバーで、[Pod]を展開し、不正なエンドポイントをクリアするリーフ スイッチをクリックします。
c) リーフ スイッチ サマリが作業ウィンドウに表示されたら、ナビゲーション バーのリーフ スイッチ名を右クリックし、**[Clear Rogue Endpoints]** を選択します。
d) **[Yes]** をクリックします。

## NX-OS スタイル CLI を使用した エンドポイント の設定

**不正 EP 制御** ポリシーをファブリックに設定して、NX-OS スタイル CLI を使用して認証されていないエンドポイントを検出および削除できます。

**手順**

**ステップ 1** **configure**

グローバル コンフィギュレーション モードを開始します。

**例**：

```
apic1# configure
```

**ステップ 2** **endpoint rogue-detect enable**

グローバル不正エンドポイント制御ポリシーを有効にします。

**例**：

```
apic1(config)# endpoint rogue-detect enable
```

**ステップ 3** **endpoint rogue-detect hold-interval** *hold_interval*

エンドポイントの不正が発見された後に保留間隔を秒単位で設定することで、ラーニングが防止されるように静的を維持し、不正なエンドポイントによるトラフィックがドロップします。このインターバルが経過すると、エンドポイントは削除されます。有効な値は 1800 ～ 3600 秒です。デフォルト値は 1800 です。

**例**：

```
apic1(config)# endpoint rogue-detect hold-interval 1800
```

**ステップ 4** **endpoint rogue-detect interval** *interval*

不正なエンドポイントを検出するまでの時間を指定する不正の検出間隔を秒で設定します。有効な値は 0 ～ 65535 秒です。デフォルトは 60 です。

**例**：

```
apic1(config)# endpoint rogue-detect interval 60
```

**ステップ 5** **endpoint rogue-detect factor** *factor*

エンドポイントが承認されたかどうかを確認する際に、乗算係数を指定します。エンドポイントは、複数の時間間隔の間に移動した場合、EP は不正を宣言します。有効値は 2 ～ 10 です。デフォルト値は 6 です。

**例**：

```
apic1# endpoint rogue-detect factor 6
```

**ステップ 6** この例では、悪意のあるエンドポイント コントロール ポリシーを設定します。

**例**：

```
apic1# cconfigure
apic1(config)# endpoint rogue-detect enable
apic1(config)# endpoint rogue-detect hold-interval 1800
apic1(config)# endpoint rogue-detect interval 60
apic1(config)# endpoint rogue-detect factor 6
```

## REST API を使用した不正エンドポイント制御ポリシーの設定

ファブリックに **[不正 EP 制御]** ポリシーを設定し、REST API を使用して認証されていないエンドポイントを検出して削除します。

### 手順

不正 EP 制御ポリシーを設定するには、次のように XML で post を送信します。

**例：**

```
<polUni>
    <infraInfra>
        <epControlP name="default" adminSt="enabled"  holdIntvl="1800"
rogueEpDetectIntvl="60" rogueEpDetectMult="6"/>
    </infraInfra>
</polUni>
```

# IP エージングの設定

このトピックでは、IP エージング ポリシーを有効にする方法について説明します。有効な場合、IP エージング ポリシーは、エンドポイント上の未使用の Ip 5 します。

管理状態が有効になっているときに、IP エージング ポリシーは、エンドポイントの ip アドレスを追跡する (IPv4) の ARP 要求と (IPv6) のネイバー要請を送信します。応答が指定されていない場合、ポリシーは、未使用の IPs 5 します。

### 手順

**ステップ 1** メニュー バーで、**System** > **System Settings** を選択します。

**ステップ 2** をクリックして **エンドポイント コントロール** 。

**ステップ 3** **Ip Aging** タブをクリックします。

**ステップ 4** ポリシーを有効にするにはクリックして **Enabled** で、 **Administrative State** フィールド。

### 次のタスク

、、エンドポイント上の ip アドレスを追跡するために使用されるタイマーを指定する必要があるエンドポイント保持ポリシーを作成します。移動 **テナント** > **テナント名** > > **ポリシー** > **プロトコル** > **エンドポイント保持** 。

# リモート エンドポイントの学習を無効にする

このトピックでは、有効化または IP エンドポイント ラーニングを無効にする方法について説明します。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

Cisco Nexus 9000 シリーズのスイッチで 93128 を含むファブリックでは、このポリシーを有効にする必要がありますが正常に APIC リリース 2.2(2x) にアップグレードされた以降のすべてのノードが表示された後の N9K M12PQ アップリンク モジュール、TX、9396 PX または 9396 TX がスイッチします。

次の設定の変更のいずれか後に、、手動で以前に学習された IP エンドポイントをフラッシュする必要があります。

- リモート IP エンドポイント ラーニングが無効になっています
- 入力ポリシーの適用、VRF が設定されています。
- VRF に少なくとも 1 つのレイヤ 3 インターフェイスが存在します

以前に学習された IP エンドポイントを手動でフラッシュ、VPC ピアの両方で、次のコマンドを入力します: `vsh-c"システム内部 epm エンドポイントの vrf をクリア<vrf-name>リモート「 </vrf-name>`
。

IP エンドポイントの学習を有効または無効にするには、次の手順を実行します:

**手順**

**ステップ 1** メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。
**ステップ 2** **[Fabric Wide Setting]** をクリックします。
**ステップ 3** チェック ボックスをクリックして **リモート EP 学習の無効化** 。
**ステップ 4** [送信（Submit）] をクリックします。

# サブネット チェックのグローバルな適用

このトピックでは、サブネットチェックを有効また無効にする方法について説明します。有効にすると、ある VRF で設定されたサブネットの外、つまり他のすべての VRF では、IP 学習が無効になります。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

**手順**

**ステップ 1** メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。
**ステップ 2** **[Fabric Wide Setting]** をクリックします。
**ステップ 3** **Enforce Subnet Check** チェック ボックスをオンにします。
**ステップ 4** [送信（Submit）] をクリックします。

# GIPo の再割り当て

このトピックでは、拡大 BDs 確保するために非拡大 BDs で再配置 GIPos を有効にする方法について説明します。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

### 手順

**ステップ 1** メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。
**ステップ 2** **[Fabric Wide Setting]** をクリックします。
**ステップ 3** [Reallocate Gipo] のチェック ボックスをオンにします。
**ステップ 4** [送信（Submit）] をクリックします。

# ドメインの検証のグローバルな適用

このトピックでは、ドメインの検証を適用する方法について説明します。有効な場合、静的なパスを追加すると、EPGに関連付けられたドメインがないかどうか判断するために、検証チェックが実行されます。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

### 手順

**ステップ 1** メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。
**ステップ 2** **[Fabric Wide Setting]** をクリックします。
**ステップ 3** **Enforce Domain Validation** チェック ボックスをオンにします。
**ステップ 4** [送信（Submit）] をクリックします。

# OpFlex クライアント認証を有効にする

このトピックでは、GOLF およびLinux 用の OpFlex クライアント認証を有効にする方法について説明します。

クライアントの ID がネットワークによって保証されない環境で GOLF または Linux Opflex クライアントをデプロイするには、クライアント証明書に基づいてクライアントの ID を動的に検証できます。

（注） 証明書の適用を有効にすると、クライアント認証をサポートしていない GOLF または Linux Opflex クライアントとの接続が無効になります。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

**手順**

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

**ステップ 2** **[Fabric Wide Setting]** をクリックします。

**ステップ 3** **OpFlex Client Authentication** のチェック ボックスをクリックして、GOLF および Linux Opflex クライアントのクライアント証明書認証を有効または無効にします。

**ステップ 4** [送信（Submit）] をクリックします。

# ロード バランシング ポリシーの作成

このトピックでは、デフォルトのロードバランサーポリシーを構成する方法について説明します。

ロード バランシング ポリシー オプションは、利用可能なアップリンク ポート間でトラフィックのバランスをとります。スタティック ハッシュ ロード バランシングは、各フローが 5 タプルのハッシュに基づいてアップリンクに割り当てられるネットワークで使用される従来のロード バランシング機構です。このロード バランシングにより、使用可能なリンクにほぼ均等な流量が分配されます。通常、流量が多いと、流量の均等な分配により帯域幅も均等に分配されます。ただし、いくつかのフローが残りよりも多いと、スタティック ロード バランシングにより完全に最適ではない結果がもたらされる場合があります。

**手順**

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

**ステップ 2** **[Load Balancer]** をクリックします。

**ステップ 3** **[Dynamic Load Balancing Mode]** を選択します。

ダイナミック ロード バランシング (DLB) モードは、輻輳レベルに応じてトラフィックの割り当てを調整します。DLB では、使用可能なパス間の輻輳が測定され、輻輳状態が最も少ないパスにフローが配置されるので、データが最適またはほぼ最適に配置されます。DLB は、フローまたはフローレットの粒度を使用して使用可能なアップリンクにトラフィックを配置するように設定できます。フローレットは、間隔で区切られたフローからのパケットのバーストです。モードは **[Aggressive]**, **[Conservative]**, または **[Off]** (デフォルト)。

**ステップ 4** **[On]** または **[Off]**を選択して、**Dynamic Packet Prioritization**をイネーブルはディスエーブルにします (デフォルト。

Dynamic Packet Prioritization (DPP) は、長いフローよりも短いフローを優先します。短いフローは約 15 です。短いフローは、長いフローより遅延に敏感です。DPP により、アプリケーション全体のパフォーマンスが向上します。

**ステップ 5** [Load Balancing Mode] を選択します。モードは、**Link Failure** または **Traditional** (デフォルト) です。

ロードバランサーの管理状態。スタティックまたはダイナミックのロードバランシングのすべてのモードでは、トラフィックは、Equal Cost Multipath (ECMP) の基準を満たすアップリンクまたはパス上でのみ送信され、これらのパスはルーティングの観点から同等で最もコストがかかりません。

**ステップ 6** [送信（Submit）] をクリックします。

# 時間精度ポリシーの有効化

このトピックでは、ネットワーク上の分散ノードの時間同期プロトコルである Precision Time Protocol (PTP) を有効にする方法について説明します。そのハードウェアのタイムスタンプ機能は、ネットワーク タイム プロトコル（NTP）などの他の時刻同期プロトコルより高い精度を実現します。

PTPは、システムのリアルタイムPTPクロックが相互に同期する方法を指定する分散プロトコルです。これらのクロックは、グランドマスタークロック（階層の最上部にあるクロック）を持つマスター/メンバー同期階層に編成され、システム全体の時間基準を決定します。同期は、タイミング情報を使用して階層のマスターの時刻にクロックを調整するメンバーと、PTPタイミング メッセージを交換することによって実現されます。PTPは、PTP ドメインと呼ばれる論理範囲内で動作します。

### 手順

**ステップ 1** メニュー バーで、**System** > **System Settings** を選択します。

**ステップ 2** **Precision Time Protocol** をクリックします。

**ステップ 3** **Enabled** または **Disabled** を選択します。

PTPを無効にするように選択した場合は、NTPの時間がファブリックを同期するために使用されます。PTPを有効にすると、サイト全体を同期するためのマスターとしてあるスパインが自動的に選択されます。

**ステップ 4** [送信（Submit）] をクリックします。

## グローバル システム GIPo ポリシーの有効化

このトピックでは、インフラ テナント GIPo をシステム GIPo として使用する方法について説明します。

ACI マルチポッドを導入するには、239.255.255.240 のシステム グローバル IP アウトサイド (GIPo) を、インターポッド ネットワーク (IPN) 上で、PIM BIDIR の範囲として設定する必要があります。この、IPN デバイス上での 239.255.255.240 PIM BIDIR 範囲の設定は、インフラ GIPo をシステム GIPo として使用することによって回避できます。

### 始める前に

リーフ スイッチおよびスパイン スイッチを含む、ACI ファブリックのすべてのスイッチを、最新の APIC リリースにアップグレードします。

### 手順

**ステップ 1** メニューバーで、 **System** > **System Settings** の順にクリックします。

**ステップ 2** **Enabled** または **Disabled** (デフォルト) を、**Use Infra GIPo as System GIPo** で選択します。

**ステップ 3** [送信（Submit）] をクリックします。

# グローバルファブリックアクセスポリシーのプロビジョニング

## グローバル接続可能アクセス エンティティ プロファイルの作成

接続可能エンティティ プロファイル（AEP）は、同様のインフラストラクチャ ポリシー要件を持つ外部エンティティのグループを表します。インフラストラクチャ ポリシーは、Cisco Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）、Link Aggregation Control Protocol（LACP）などのさまざまなプロトコル オプションを設定する物理インターフェイス ポリシーで構成されます。

AEP は、リーフ スイッチで VLAN プールを展開するのに必要です。カプセル化ブロック（および関連 VLAN）は、リーフ スイッチで再利用可能です。AEP は、VLAN プールの範囲を物理インフラストラクチャに暗黙的に提供します。

次の AEP の要件と依存関係は、さまざまな設定シナリオ（ネットワーク接続、VMM ドメイン、マルチポッド設定など）でも考慮する必要があります。

- AEP は許容される VLAN の範囲を定義しますが、それらのプロビジョニングは行いません。EPG がポートに展開されていない限り、トラフィックは流れません。AEP で VLAN

プールを定義しないと、EPGがプロビジョニングされてもVLANはリーフ ポートでイネーブルになりません。

- リーフ ポートで静的にバインディングしているEPGイベントに基づいて、またはVMware vCenter や Microsoft Azure Service Center Virtual Machine Manager（SCVMM）などの外部コントローラからのVMイベントに基づいて、特定のVLANがリーフ ポート上でプロビジョニングされるかイネーブルになります。
- 添付されているエンティティ プロファイルに関連付けられているすべてのポートに関連付けられているアプリケーションEpgを導入するアプリケーションEpgに直接と関連付けることができますプロファイルのエンティティが添付されています。AEP では、アタッチ可能なエンティティ プロファイルに関連付けられているセレクタの一部であるすべてのインターフェイスで導入されている EPG (infraRsFuncToEpg) との関係が含まれている設定可能な一般的な機能 (infraGeneric) があります。

Virtual Machine Manager（VMM）ドメインは、AEP のインターフェイス ポリシー グループから物理インターフェイス ポリシーを自動的に取得します。

### 始める前に

接続されているエンティティ プロファイルに関連付けられるテナント、VRF、アプリケーション プロファイルおよび EPG を作成します。

### 手順

**ステップ 1** メニュー バーで、**Fabric** > **External Access Policies** をクリックします。

**ステップ 2** ナビゲーション バーで、**Policies** と **Global** を展開します。

**ステップ 3** **[接続可能なアクセス エンティティ プロファイル]** を右クリックして、**[接続可能なアクセス エンティティ プロファイルの作成]** を選択します。

**ステップ 4** ポリシーの名前を入力します。

**ステップ 5** **[ドメイン]** テーブル上の [+] アイコンをクリックします。

**ステップ 6** 物理ドメイン、以前に作成した物理、レイヤ2、レイヤ3、ファイバ チャネル ドメインを入力するか、新規作成します。

**ステップ 7** ドメインのカプセル化を入力して、**[更新]** をクリックします。

**ステップ 8** **[EPG 展開]** テーブルの [+] アイコンをクリックします。

**ステップ 9** テナント、アプリケーション プロファイル、EPG カプセル化（vlan-1 など）、プライマリ カプセル化（プライマリ カプセル化番号）、インターフェイス モードを入力します（トランク、802.1P またはアクセス（タグなし）。

**ステップ 10** **Update** をクリックします。

**ステップ 11** [Next] をクリックします。

**ステップ 12** 接続可能なエンティティ プロファイルに関連付けるインターフェイスを選択します。

**ステップ 13** [Finish] をクリックします。

# QoS クラスのグローバル ポリシーを設定します。

グローバル QoS クラス ポリシーを使用できます。

- CoS を保持する、CoS 値を保証するために、優先度レベル 802.1 P のパケット数を入力し、ACI ファブリックを通過するが保持されます。802.1 P CoS の保持は単一のポッドおよび multipod トポロジでサポートされます。Multipod トポロジは、CoS の保持を使用できますポッド 1 を入力して、ポッド 2 外からの 802.1 P トラフィックの優先順位の QoS の設定を保持したいですが、CoS の保持を行わない/interpod の DSCP 設定のネットワーク (IPN) トラフィックポッド間。CoS を保持するために multipod トラフィックが通信中、IPN の DSCP 設定を使用して、DSCP ポリシー/(で設定されている **テナント** > **インフラ** > > **ポリシー** > **プロトコル** > **DSCP クラス-cos L3 トラフィックのポリシーの変換**)
- 次のように、デフォルトの QoS クラス レベルのプロパティをリセットします **MTU** 、**キュー制限** 、または **スケジューリング アルゴリズム** 。

**手順**

**ステップ 1** メニュー バーで、**Fabric** > **External Access Policies** をクリックします。
**ステップ 2** ナビゲーション バーで、**Policies** と **Global** を展開します。
**ステップ 3** **QOS Class** をクリックします。
**ステップ 4** CoS 802.1 P の有効化にして、をクリックして、 **保持 COS** チェック ボックス。
**ステップ 5** QoS クラスのデフォルト設定を変更するには、それをダブルクリックします。新しい設定を入力し、**Submit** をクリックします。

# グローバル DHCP リレー ポリシーの作成

グローバル DHCP リレー ポリシーは、ファブリックの DHCP サーバを識別します。

**手順**

**ステップ 1** メニュー バーで、**Fabric** > **External Access Policies** をクリックします。
**ステップ 2** ナビゲーション バーで、**Policies** と **Global** を展開します。
**ステップ 3** **DHCP Relay** を右クリックし、**Create DHCP Relay Policy** を選択します。
**ステップ 4** ポリシーの名前を入力します。
**ステップ 5** **Providers** の [+] アイコンをクリックします。
**ステップ 6** EPG のタイプを選択します。アプリケーション EPG の場合には、テナント、アプリケーション プロファイルおよび EPG プロバイダーを選択します。
**ステップ 7** **DHCP Server Address** フィールドに、サーバの IP アドレスを入力します。

**ステップ 8** [OK] をクリックします。

# グローバル MCP インスタンス ポリシーの有効化にします。

グローバル Mis-Cabling プロトコル (MCP) インスタンス ポリシーを有効にします。現在の実装では、システムで MCP の 1 つだけのインスタンスが実行されます。

### 手順

**ステップ 1** メニュー バーで、**Fabric** > **External Access Policies** をクリックします。
**ステップ 2** ナビゲーション バーで、**Policies** と **Global** を展開します。
**ステップ 3** をクリックして **MCP インスタンス ポリシーのデフォルト** 。
**ステップ 4** **Admin State** を **Enabled** に変更します。
**ステップ 5** 必要に応じて、ファブリックの他のプロパティを設定します。
**ステップ 6** [送信（Submit）] をクリックします。

### 次のタスク

# 作成エラーには、回復ポリシーが無効になっています

エラーディセーブル回復ポリシーは、1つ以上の事前定義されたエラー状態が無効になっていたポートを再度有効にするポリシーを指定します。

### 手順

**ステップ 1** メニュー バーで、**Fabric** > **External Access Policies** をクリックします。
**ステップ 2** ナビゲーション バーで、**Policies** と **Global** を展開します。
**ステップ 3** をクリックして **エラーには、回復ポリシーが無効になっている** .
**ステップ 4** 回復ポリシーを有効にするイベントをダブルクリックします。
**ステップ 5** チェック ボックスをクリックし、をクリックして **更新** 。
**ステップ 6** オプション。その他のイベントについて、ステップ 4 と 5 を繰り返します。
**ステップ 7** オプション。リセット、 **エラー復旧間隔 (秒) の無効化** 。
**ステップ 8** [Submit] をクリックします。

# グローバル ポート トラッキング ポリシーの設定

アップリンク障害検出は、ファブリック アクセス グローバル ポート トラッキング ポリシーで有効化できます。ポート トラッキング ポリシーは、リーフ スイッチとスパイン スイッチ間のリンクの状態を監視します。有効なポート トラッキング ポリシーがトリガーされると、リーフ スイッチは、EPG によって導入されたスイッチ上のすべてのアクセス インターフェイスをダウンさせます。

### 手順

**ステップ 1** メニュー バーで、**Fabric** > **External Access Policies** をクリックします。
**ステップ 2** ナビゲーション バーで、**Policies** と **Global** を展開します。
**ステップ 3** **Port Tracking** をクリックします。
**ステップ 4** **Port tracking state** を **on** に設定して、ポート トラッキングを有効にします。
**ステップ 5** オプション。**Daily restore timer** を変更します。
**ステップ 6** **Number of active spine links that triggers port tracking** を入力します。
**ステップ 7** **Submit** をクリックします。