コアACIファブリックサービスのプロビジョニング

この章の内容は、次のとおりです。

時刻同期と NTP

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

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

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

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

インバンドおよびアウトオブバンドの管理 NTP

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

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

拡張 GUI を使用した NTP の設定

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

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

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

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

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

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

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

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

作成するプロバイダーごとに、この手順を繰り返します。

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

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

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

a) ポリシー グループの名前を入力します。

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

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

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

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

REST API を使用した NTP の設定

ステップ 1 NTP を設定します。

例：

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

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

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

例：

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

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

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

例：

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

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

CLI を使用した、各ノードに導入された NTP ポリシーの確認

ステップ 1 ファブリックの APIC に SSH 接続します。

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

例：

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

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

例：

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

ステップ 4 NTP ピアのステータスを表示します。

例：

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

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

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

GUI を使用した NTP の動作の確認

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

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

ステップ 3 [Work] ペインで、サーバの詳細を確認します。

DHCP リレー ポリシーの設定

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

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

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

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

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

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

はじめる前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

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

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

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

a) [Name] フィールドに、DHCP リレー プロファイル名（DhcpRelayP）を入力します。

b) [Providers] を展開します。[Create DHCP Provider] ダイアログボックスの [EPG Type] フィールドで、DHCP サーバがどこで接続されているかによって適切なオプション ボタンをクリックします。

c) [Application EPG] 領域の [Tenant] フィールドで、ドロップダウン リストから、テナントを選択します。（infra）

d) [Application Profile] フィールドで、ドロップダウン リストから、アプリケーションを選択します。（access）

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

f) [DHCP Server Address] フィールドに、インフラ DHCP サーバの IP アドレスを入力します。[Update] をクリックします。

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

g) [Submit] をクリックします。

DHCP リレー ポリシーが作成されます。

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

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

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

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

b) [Name] フィールドで、ドロップダウン リストから、作成した DHCP ポリシーの名前を選択します（DhcpRelayP）。

c) [Submit] をクリックします。

DHCP サーバがブリッジ ドメインに関連付けられます。

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

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

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

はじめる前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

手順の概要

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

手順の詳細

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

例：

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

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

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

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

はじめる前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

手順の概要

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

手順の詳細

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

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

例：

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

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


  <fvTenant name="infra">

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

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

  </fvTenant>
</polUni>
```

DNS サービス ポリシーの設定

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

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

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

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

インバンド DNS サービス ポリシーによる外部宛先の設定

次のように、サービスに対して外部宛先を設定します。

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

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

次に示すのは、外部サーバのリストです。

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

推奨されるガイドラインは次のとおりです。

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

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

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

はじめる前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

手順の概要

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

手順の詳細

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

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

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

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

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

c) [Update] をクリックします。

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

ステップ 4 [DNS Domains] を展開し、次の操作を実行します。

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

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

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

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

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

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

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：
```
admin@apic1:~> cd /aci
```

ステップ 2 DNS サーバ ポリシーを設定します。

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

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

例：

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

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

はじめる前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

手順の概要

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

手順の詳細

ステップ 1 DNS サービス ポリシーを設定します。

例：

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

<dnsProfile name="default">

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

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

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

</dnsProfile>
```

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

例：

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

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

ステップ 1 デフォルトの DNS プロファイルの設定を確認します。

例：

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

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

ステップ 2 DNS ラベルの設定を確認します。

例：

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

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

例：

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

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

例：

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

カスタム証明書の設定のガイドライン

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

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

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

はじめる前に

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

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

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

a) [Public Key Management] を展開します。

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

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

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

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

e) [Submit] をクリックします。

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

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

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

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

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

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

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

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

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

b) [Subject] フィールドに、Cisco APIC コントローラの完全修飾ドメイン名（FQDN）を入力します。

（注） /etc/hosts ファイルに、APIC コントローラの IP アドレスと DNS 名のエントリが必要です。DNS 名は証明書のサブジェクトに一致する必要があります。APIC コントローラごとに、このファイル内のエントリが必要です。

c) 必要に応じて、残りのフィールドに入力します。APIC コントローラと適切な証明書ごとにこの手順（CSR）を繰り返します。

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

d) [Submit] をクリックします。

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

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

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

b) [Submit] をクリックします。

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

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

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

ステップ 7 [Work] ペインの [Admin Key Ring] フィールドで、ドロップダウン メニューを使用して目的のキー リングを選択します。[Submit] をクリックします。

すべての Web サーバが再起動されます。証明書がアクティブになり、デフォルト以外のキー リングが HTTPS アクセスに関連付けられています。

次の作業

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