



レイヤ4からレイヤ7サービスの展開

- [概要 \(1 ページ\)](#)
- [サービス グラフの展開 \(5 ページ\)](#)

概要

Cisco Cloud APIC を使用すると、レイヤ4からレイヤ7のサービスデバイスをパブリッククラウドに展開できます。この初期リリースは、Amazon Web Services (AWS) でのアプリケーションロードバランサー (ALB) の展開をサポートしています。

アプリケーションロードバランサの概要

アプリケーションロードバランサ (ALB) は、パケットを検査し、HTTP および HTTPS ヘッダーへのアクセスポイントを作成するレイヤ7ロードバランサです。また、負荷を識別し、より高い効率でターゲットに分散します。サービスグラフを使用して ALB を展開します。これにより、トラフィックがネットワークにどのように流入するか、トラフィックが通過するデバイス、およびトラフィックがネットワークを離れる方法を定義できます。これらのアクションを指定するには、1つ以上のリスナーを構成します。

リスナーを使用すると、ALB がトラフィックを受け入れるポートとプロトコル (HTTP または HTTPS) を指定できます。HTTPS を指定する場合は、セキュリティポリシーと SSL 証明書も選択します。



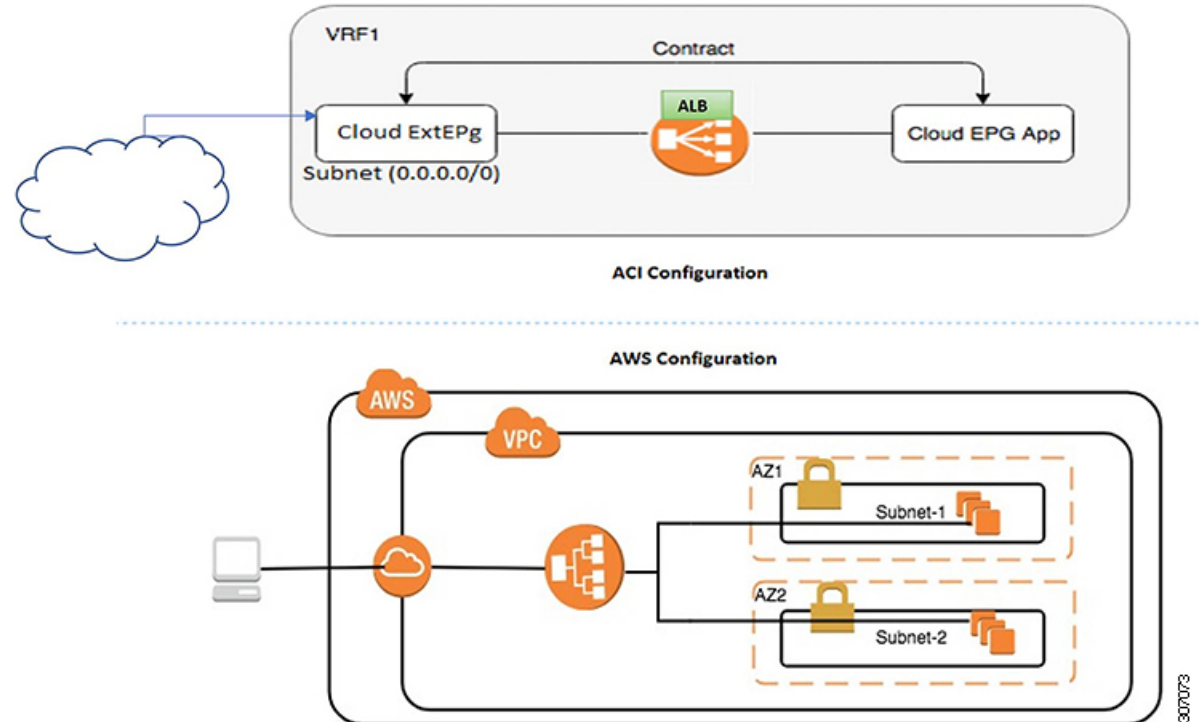
(注) リスナーは複数の証明書をもつことができます。

すべてのリスナーで、少なくとも1つのルール(条件のないデフォルトのルール)を構成する必要があります。ルールを使用すると、条件が満たされたときにロードバランサが実行するアクションを指定できます。たとえば、指定されたホスト名またはパスへの要求が行われたときに、トラフィックを指定された URL にリダイレクトするルールを作成できます。

展開には、インターネット向けと内部向けの2種類があります。インターネットに接続する展開では、コンシューマーの外部 EPG とプロバイダーのクラウド EPG の間にサービスとして

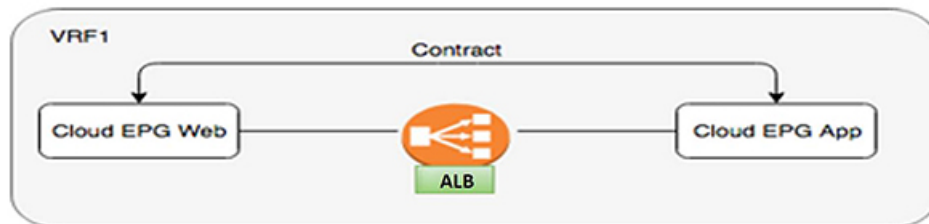
ALB が挿入されます。次の図は、VRF 内のコントラクト構成と、コンシューマーの外部 EPG とプロバイダーのクラウド EPG の間に挿入されるサービスとしての ALB を示しています。

図 1: インターネットに面した展開



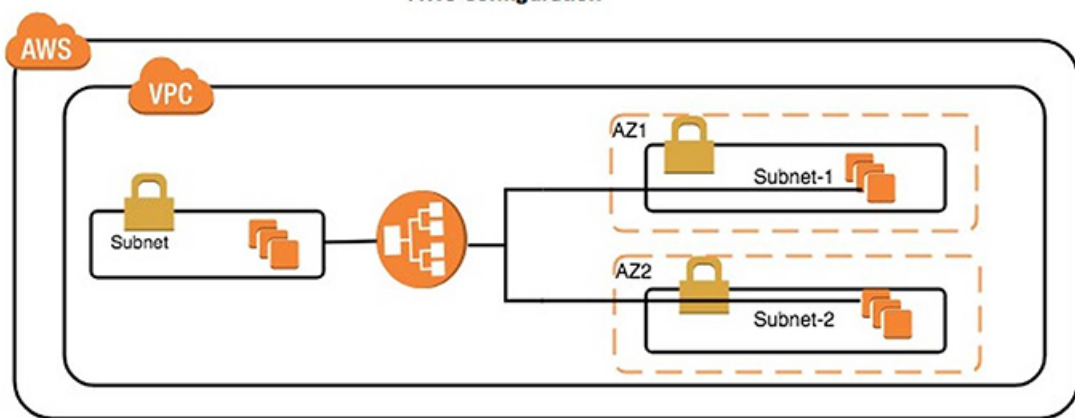
内部向け展開では、コンシューマークラウド EPG とプロバイダークラウド EPG の間にサービスとしての ALB が挿入されます。次の図は、コンシューマクラウド EPG とプロバイダークラウド EPG の間に挿入されるサービスとしての VRF および ALB 内の契約構成を示しています。

図 2: 内部に向けた展開



ACI Configuration

AWS Configuration



(注) ALBの詳細については、AWSのWebサイトのマニュアルを参照してください。

サーバー プールへのダイナミック サーバーのアタッチ

サーバープールまたはターゲットグループ内のサーバーはダイナミックに追加されます。ターゲットのIPアドレスまたはインスタンスIDを指定する必要はありません。リスナールールからプロバイダークラウド EPG への関係は、エンドポイントのダイナミックな選択に使用されます。この関係は、エンドポイントターゲットグループに追加するためにも使用されます。デフォルトでは、エンドポイントはポート番号 80 で登録されています。

ALB で提供されるターゲットグループとセキュリティグループの関連付け、およびエンドポイントの EPG (セキュリティグループ) に基づいて、EC2 インスタンス (サーバー) は、ターゲットグループのデフォルトポートでダイナミックにターゲットグループに関連付けられます。または、ターゲットグループポートで EC2 インスタンスを登録する代わりに、次の表のポートを指定してカスタムポートをアタッチできます。

表 1: カスタム ポートベースのアタッチ

プロバイダー-EPG	ポート
EPGMap:<Epg1DN>	9090
EPGMap:<Epg2DN>	9091、9099

EPGMap:<EpgDN>をタグとして、さらに、コンマで区切られたリストとしてターゲットグループに登録されるポートのリストを指定できます。

サービス グラフについて

Cisco Application Centric Infrastructure (ACI) はアプリケーションの一部としてサービスを見なします。必要とされるすべてのサービスが、Cisco APIC から Cisco ACI ファブリックでインスタンス化されるサービス グラフとして扱われます。ユーザーは、アプリケーションに対してサービスを定義し、サービス グラフはアプリケーションが必要とする一連のネットワークまたはサービス機能を識別します。

サービス グラフは、次の要素を使ってネットワークを表します。

- 機能ノード：機能ノードは、ロードバランサなどのトラフィックに適用される機能を表します。サービス グラフ内の1つの機能は1つ以上のパラメータを必要とし、1つまたは複数のコネクタを持っている場合があります。
- 端末ノード：端末ノードはサービス グラフからの入出力を有効にします。
- コネクタ：コネクタはノードからの入出力を有効にします。

グラフが設定されると、Cisco APIC はサービス グラフに明記されたサービス機能の要件に従って、サービスを自動的に設定します。Cisco APIC もまた、サービス グラフで指定されるサービス機能のニーズに応じてネットワークを自動的に設定します。これにより、サービスデバイスを変更する必要がなくなります。

サービス グラフは、アプリケーションの複数の階層として表され、適切なサービス機能が階層間に挿入されます。

サービス アプライアンス (デバイス) は、グラフ内でサービス機能を実行します。1つ以上のサービス アプライアンスが、グラフに必要なサービスをレンダリングするために必要になることがあります。1つ以上のサービス機能が単一のサービス デバイスで実行できます。

サービス グラフおよびサービス機能には、次の特性があります。

- 特定のエンドポイントグループから送信されたトラフィックは、ポリシーに基づいてリダイレクトできます。
- サービス グラフのリダイレクトには方向があります。つまり、リダイレクトは両方のトラフィック方向またはいずれか一方のトラフィックに適用できます。
- Logical functions can be rendered on the appropriate device, based on the policy.

- サービスグラフでは、エッジの分割と結合がサポートされ、管理者は線形サービスチェーンに制限されません。
- トラフィックは、サービスアプライアンスが発信した後にネットワーク内で再度分類できます。

サービスグラフを使用すると、サービス、ロードバランサを一度インストールして、異なる論理トポロジで何度も展開できます。グラフを展開するたびに、Cisco ACIは新しい論理トポロジでの転送を行えるように、サービスデバイスで設定の変更を行います。

機能ノードについて

機能ノードは、単一のサービス機能を表します。機能ノードには、サービス機能のネットワーク要件を表す機能ノードコネクタがあります。

サービスグラフ内の関数ノードには、次のパラメーターが必要です。

- テナント
- 2つのアベイラビリティゾーンにサブネットを持つクラウドコンテキストプロファイル

サービスグラフのレンダリング時に関数パラメータを指定できます。たとえば、関数ノードがロードバランサーである場合、リスナーとそのルールは、グラフのレンダリング時に関数ノードに対して指定できます。

端末ノードについて

端末ノードはサービスグラフとコントラクトを接続します。コントラクトに端末ノードを接続することにより、2つのアプリケーションクラウドEPG間のトラフィックにサービスグラフを挿入できます。接続されると、コントラクトのコンシューマクラウドEPGとプロバイダークラウドEPG間のトラフィックはサービスグラフにリダイレクトされます。

サービスグラフの展開

サービスグラフを使用すると、デバイス間のトラフィックフロー、ネットワークへのトラフィックの流入方法、トラフィックが通過するデバイス、およびトラフィックがネットワークから出る方法を定義できます。

Before you can configure a service graph, you must first configure the following:

1. テナント
2. クラウドコンテキストプロファイル
3. サブネット
4. アプリケーションプロファイル
5. コンシューマEPG

6. プロバイダー-EPG

7. コントラクト

Cloud APIC GUI を使用したサービス グラフの展開

Cisco Cloud APIC GUI を使用したロード バランサの作成

このセクションでは、Cisco Cloud APIC GUI を使用したローカル ユーザーの作成方法について説明します。

ステップ1 Click **Application Management** > **Services**.

The **Services** page appears.

ステップ2 Click the **Devices** tab, then click **Actions** > **Create Device**.

The **Create Device** page appears.

ステップ3 次の [デバイスの作成ダイアログボックスのフィールド (*Create Device Dialog Box Fields*)] の表にリストされた各フィールドに該当する値を入力し、続行します。

表 2: デバイスの作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
全般	
名前	ロード バランサーの名前を入力します。
テナント	テナントを選択します。 <ol style="list-style-type: none"> [テナントの選択 (Select Tenant)] をクリックします。[テナントの選択 (Select Tenant)] ダイアログが表示されます。 左側の列から、クリックしてテナントを選択します。 [選択 (Select)] をクリックします。[デバイスの作成 (Create Device)] ダイアログボックスに戻ります。
[設定 (Settings)]	
サービス タイプ	Choose Application Load Balancer .
スキーム	Choose Internal or Internet Facing .

[プロパティ (Properties)]	説明
Subnets	<p>アベイラビリティゾーンごとに1つのサブネットのみを指定できます。ロードバランサーの可用性を高めるには、少なくとも2つのアベイラビリティゾーンからサブネットを指定する必要があります。</p> <ol style="list-style-type: none"> 1. Click Add Subnet. The Add Subnet dialog box appears. 2. [サブネットの追加] ダイアログ ボックスで、[クラウド コンテキスト プロファイルの選択] をクリックします。 The Select Cloud Context Profile dialog box appears. 3. [クラウド コンテキスト プロファイルの選択] ダイアログ ボックスで、クラウド コンテキスト プロファイルを選択し、[選択] をクリックします。 You are returned to the Add Subnet dialog box. 4. [サブネットの追加] ダイアログ ボックスで、[サブネットの選択] をクリックします。 [サブネットの選択] ダイアログボックスが表示されます。 5. [サブネットの選択] ダイアログ ボックスでサブネットを選択し、[選択] をクリックします。 You are returned to the Add Subnet dialog box. 6. In the Add Subnet dialog box, click Add. You are returned to the Create Device page.

ステップ4 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUIを使用したサービス グラフ テンプレートの作成

このセクションでは、Cisco Cloud APIC GUI を使用したサービス グラフ テンプレートの作成方法について説明します。

始める前に

デバイスはすでに作成されています。

ステップ1 Click **Application Management > Services**.

The **Services** page appears.

ステップ2 [サービス グラフ] タブをクリックし、[アクション][サービス グラフの作成] をクリックします。 >

The **Create Service Graph** page appears.

ステップ 3 次の [サービス グラフの作成ダイアログ ボックスのフィールド (*Create Service Graph Dialog Box Fields*)] の表に示されているように、各フィールドに適切な値を入力し、続行します。

表 3: サービス グラフの作成ダイアログ ボックスのフィールド

[プロパティ (Properties)]	説明
全般	
名前	サービス グラフ テンプレートの名前を入力します。
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> 1. [テナントの選択 (Select Tenant)] をクリックします。[テナントの選択 (Select Tenant)] ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択 (Select)] をクリックします。[サービス グラフの作成 (Create Service Graph)] ダイアログ ボックスに戻ります。
説明	サービス グラフ テンプレートの説明を入力します。
[設定 (Settings)]	
デバイスを選択	<p>デバイスを選択します。</p> <ol style="list-style-type: none"> 1. Application Load Balancer アイコンをサービス グラフの [デバイスのドロップ] 領域にドラッグアンドドロップします。 The Service Node dialog box appears. 2. Click Select Application Load Balancer. The Select Application Load Balancer dialog appears. 3. 左側の列から、デバイスをクリックして選択します。 4. [選択 (Select)] をクリックします。 You return to the Service Node dialog box. 5. [Add] をクリックします。 You return to the Create Service Graph window.

ステップ4 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したレイヤ4からレイヤ7サービスの展開

このセクションでは、レイヤ4～レイヤ7サービスを展開する方法について説明します。

始める前に

- これでデバイスが構成されました。
- サービス グラフが構成されました。

ステップ1 インテントアイコンをクリックします。[**インテント (Intent)**] メニューが表示されます。

ステップ2 [**インテント (Intent)**] 検索ボックスの下のドロップダウン□をクリックし、[**構成 (Configuration)**] を選択します。

[**インテント (Intent)**] の [**構成 (Configuration)**] オプションのリストが表示されます。

ステップ3 [**インテント (Intent)**] メニューの [**構成 (Configuration)**] リストで、[**EPG Communication**] をクリックします。[**EPG通信 (EPG Communication)**] ダイアログボックスに、**コンシューマ EPG**、**コントラクト**、および**プロバイダー EPG**の情報が表示されます。

ステップ4 コントラクトを選択します。

- a) [**コントラクトの選択 (Select Contract)**] をクリックします。[**コントラクトの選択 (Select Contract)**] ダイアログボックスが表示されます。
- b) [**コントラクトの選択 (Select Contract)**] ダイアログの左側のペインで、契約をクリックして選択し、[**選択 (Select)**] をクリックします。[**コントラクトの選択 (Select Contract)**] ダイアログボックスが閉じます。

ステップ5 コンシューマ EPG を追加するには、次の手順を実行します。

- a) [**コンシューマ EPG の追加 (Add Consumer EPGs)**] をクリックします。[**コンシューマー EPG の選択 (Select Consumer EPGs)**] ダイアログが表示されます。
- b) [**コンシューマ EPG の選択**] ダイアログの左側のペインで、チェックボックスをクリックしてチェックボックスをオンにして、クラウド EPG (内部向けロードバランサの場合) またはクラウド外部 EPG (インターネット向けロードバランサの場合) を選択します。[**選択**] をクリックします。[**コンシューマ EPG の選択 (Select Consumer EPGs)**] ダイアログボックスが閉じます。

ステップ6 プロバイダー EPG を追加するには、次の手順を実行します。

- a) [**プロバイダー EPG の追加 (Add Provider EPGs)**] をクリックします。[**プロバイダー EPG の選択 (Select Provider EPGs)**] ダイアログが表示されます。
- b) [**プロバイダー EPG の選択 (Select Provider EPGs)**] ダイアログの左側のペインで、チェックボックスをオンにしてプロバイダー EPG を選択し、[**選択**] をクリックします。[**プロバイダー EPG の選択 (Select Provider EPGs)**] ダイアログボックスが閉じます。

ステップ7 サービス グラフを選択するには:

- a) **[EPF 通信の構成 (EPG Communication Configuration)]** ダイアログで、**[サービス グラフの選択 (Select Service Graph)]** をクリックします。**[サービス グラフの選択 (Select Service Graph)]** ダイアログボックスが表示されます。
- b) **[サービス グラフの選択 (Select Service Graph)]** ダイアログの左側のペインで、サービス グラフをクリックして選択し、**[選択 (Select)]** をクリックします。**[サービス グラフの選択 (Select Service Graph)]** ダイアログボックスが閉じます。

ステップ 8 **[サービス グラフのプレビュー (Service Graph Preview)]** で、**[クラウド ロード バランサ リスナーの追加 (Add Cloud Load Balancer Listener)]** をクリックします。**[クラウド ロード バランサ リスナーの追加 (Add Cloud Load Balancer Listener)]** ダイアログが表示され、リスナーを追加できます。

リスナーは、デバイスが動作するポートとプロトコルです。

ステップ 9 次の**[クラウドロードバランサリスナーの追加ダイアログボックスのフィールド (Add Cloud Load Balancer Listener Dialog Box Fields)]** テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 4:クラウドロードバランサリスナーの追加ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
名前 (Name)	リスナーの名前を入力します。
Port	デバイスがトラフィックを受け入れるポートを入力します。
[プロトコル (Protocol)]	HTTP または HTTPS を選択します。
Security Policy	ドロップダウンリストをクリックし、セキュリティポリシーを選択します (HTTPS が選択されている場合にのみ選択可能)。

[プロパティ (Properties)]	説明
SSL 証明書	<p>SSL 証明書を選択するには (HTTPS が選択されている場合にのみ選択可能):</p> <ol style="list-style-type: none"> 1. [SSL 証明書の追加] をクリックします。 2. クリックして、追加する証明書のチェックボックスをオンにします。 3. キーリングを選択してください: <ol style="list-style-type: none"> 1. [キーリングの選択] をクリックします。 [キーリングの選択 (Select Key Ring)] ダイアログが表示されます。 2. [キーリングの選択 (Select Key Ring)] ダイアログで、左側の列のキーリングをクリックして選択し、[選択 (Select)] をクリックします。[キーリングの選択 (Select Key Ring)] ダイアログボックスが閉じます。 4. [証明書ストア] ドロップダウンリストをクリックして、証明書を選択します。 <p>(注) リスナーは複数の証明書を持つことができます。</p>
ルールの追加	<p>ルール設定をデバイスリスナーに追加するには、[ルールの追加] をクリックします。[ルール] リストに新しい行が表示され、[ルール設定] フィールドが有効になります。</p>

[プロパティ (Properties)]	説明
ルール設定	

[プロパティ (Properties)]	説明
	<p>[ルール設定 (Rule Settings)] ペインで、次のオプションを設定します。</p> <ul style="list-style-type: none"> • 名前 : 規則の名前を入力します。 • ホスト : ホスト名を入力して、ホストベースの条件を作成します。このホスト名に対して要求が行われると、指定したアクションが実行されます。 • パス : パスを入力して、パスベースの条件を作成します。このパスに対して要求が行われると、指定したアクションが実行されます。 • タイプ : アクションタイプは、実行するアクションをデバイスに通知します。アクションタイプのオプション: <ul style="list-style-type: none"> • 固定応答を返す : 次のオプションを使用して応答を返します。 <ul style="list-style-type: none"> • 固定応答本文 : 応答メッセージを入力します。 • 固定応答コード : 応答コードを入力します。 • 固定の応答コンテンツタイプ : コンテンツタイプを選択します。 • 転送 : 次のオプションを使用してトラフィックを転送します。 <ul style="list-style-type: none"> • ポート : デバイスがトラフィックを受け入れるポートを入力します。 • プロトコル : [HTTP] または [HTTPS] を選択します。 • プロバイダー EPG : トラフィックを処理する Web サーバーを持つ EPG。 • EPG : EPG を選択するには: <ol style="list-style-type: none"> 1. [EPGの選択] をクリックします。 [EPGの選択] ダイアログボックスが表示されます。 2. [EPGの選択] ダイアログで、左側の列の EPG をクリックして選択

[プロパティ (Properties)]	説明
	<p>し、[選択 (Select)]をクリックします。[EPGの選択]ダイアログボックスが閉じます。</p> <ul style="list-style-type: none"> • リダイレクト : 次のオプションを使用して、リクエストを別の場所にリダイレクトします。 <ul style="list-style-type: none"> • リダイレクト コード : [リダイレクト コード] ドロップダウン リストをクリックして、コードを選択します。 • リダイレクト ホスト名 : リダイレクトのホスト名を入力します。 • リダイレクト パス : リダイレクトパスを入力します。 • リダイレクト ポート : デバイスがトラフィックを受け入れるポートを入力します。 • リダイレクト プロトコル : [リダイレクト プロトコル (Redirect Protocol)] ドロップダウン リストをクリックして、[HTTP]、[HTTPS]、または[継承 (Inherit)]を選択します。 • リダイレクト クエリ : リダイレクトクエリを入力します。 <p>完了したら、[ルールの追加] をクリックします。</p>

ステップ 10 終了したら、[Add] をクリックします。
サービス グラフが展開されます。

REST API を使用したサービス グラフの展開

REST API を使用したインターネット向けロード バランサの作成

この例では、REST API を使用して内部向けのロード バランサを作成する方法を示します。

内部向けのロードバランサを作成するには:

例:

```
<polUni>
  <fvTenant name="t2" status="">
    <cloudLB name="ALB1" type="application" scheme="internal" status="">
      <cloudRsLDevToCloudSubnet tDn="uni/tn-t2/ctxprofile-c1/cidr-[10.33.0.0/16]/subnet-[10.33.7.0/24]"
status=""/>
      <cloudRsLDevToCloudSubnet tDn="uni/tn-t2/ctxprofile-c1/cidr-[10.33.0.0/16]/subnet-[10.33.8.0/24]"
status=""/>
    </cloudLB>
  </fvTenant>
</polUni>
```

REST API を使用したインターネット向けロードバランサの構成

この例では、REST API を使用してインターネット向けのロードバランサを作成する方法を示します。

インターネット向けのロードバランサを作成するには:

例:

```
<polUni>
  <fvTenant name="t2" status="">
    <cloudLB name="ALB1" type="application" scheme="internet" status="">
      <cloudRsLDevToCloudSubnet tDn="uni/tn-t2/ctxprofile-c1/cidr-[10.33.0.0/16]/subnet-[10.33.5.0/24]"
status=""/>
      <cloudRsLDevToCloudSubnet tDn="uni/tn-t2/ctxprofile-c1/cidr-[10.33.0.0/16]/subnet-[10.33.6.0/24]"
status=""/>
    </cloudLB>
  </fvTenant>
</polUni>
```

REST API を使用したサービスグラフの作成

この例では、REST API を使用してサービスグラフを作成する方法を示します。

サービスグラフを作成するには:

```
<polUni>
  <fvTenant name="t2">
    <vnsAbsGraph name="CloudGraph" type="cloud" status="">
      <vnsAbsTermNodeProv name="Input1">
        <vnsAbsTermConn name="C1"/>
      </vnsAbsTermNodeProv>
      <vnsAbsTermNodeCon name="Output1">
        <vnsAbsTermConn name="C2"/>
      </vnsAbsTermNodeCon>
    </vnsAbsGraph>
  </fvTenant>
</polUni>
```

```

</vnsAbsTermNodeCon>
<vnsAbsNode funcType="GoTo" name="N1" managed="yes">
  <vnsRsNodeToCloudLDev tDn="uni/tn-t2/clb-ALB1" status=""/>
  <vnsAbsFuncConn name="provider"/>
  <vnsAbsFuncConn name="consumer"/>
</vnsAbsNode>
<vnsAbsConnection connDir="consumer" connType="external" name="CON2">
  <vnsRsAbsConnectionConns tDn="uni/tn-t2/AbsGraph-CloudGraph/AbsTermNodeCon-Output1/AbsTConn"/>

  <vnsRsAbsConnectionConns tDn="uni/tn-t2/AbsGraph-CloudGraph/AbsNode-N1/AbsFConn-consumer"/>

</vnsAbsConnection>
<vnsAbsConnection connDir="provider" connType="internal" name="CON1">
  <vnsRsAbsConnectionConns tDn="uni/tn-t2/AbsGraph-CloudGraph/AbsTermNodeProv-Input1/AbsTConn"/>

  <vnsRsAbsConnectionConns tDn="uni/tn-t2/AbsGraph-CloudGraph/AbsNode-N1/AbsFConn-provider"/>

</vnsAbsConnection>
</vnsAbsGraph>
</fvTenant>
</polUni>

```

REST API を使用してサービス グラフを添付する

この例では、REST API を使用してサービス グラフを作成する方法を示します。

サービス グラフを添付するには:

```

<polUni>
  <fvTenant name="t2">
    <vzBrCP name="httpFamily">
      <vzSubj name="default" revFltPorts="yes" targetDscp="unspecified">
        <vzRsSubjGraphAtt tnVnsAbsGraphName="CloudGraph"/>
      </vzSubj>
    </vzBrCP>
  </fvTenant>
</polUni>

```

REST API を使用した HTTPS サービス ポリシーの構成

この例では、REST API を使用して HTTP サービス ポリシーを作成する方法を示します。

HTTP サービス ポリシーを作成するには:

```

<polUni>
  <fvTenant name="t2">
    <vnsAbsGraph name="CloudGraph" type="cloud" status="">
      <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
        <cloudSvcPolicy tenantName="t2" contractName="httpFamily" subjectName="consubj">
          <cloudListener name="http_listener1" port="80" protocol="http" status="">
            <cloudListenerRule name="rule1" priority="10" default="yes" status="">
              <cloudRuleAction type="forward" port="80" protocol="http"

```



```

epgdn="uni/tn-t2/cloudapp-ap/cloudepg-provEPG"/>
  </cloudListenerRule>
  <cloudListenerRule name="redirectRule" priority="20">
    <cloudRuleCondition type="path" value="/img/*"/>
    <cloudRuleAction type="redirect" RedirectPort="8080"/>
  </cloudListenerRule>
  <cloudListenerRule name="FixedRspRule" priority="30">
    <cloudRuleCondition type="host" value="example.com"/>
    <cloudRuleAction type="fixedResponse" FixedResponseCode="200"/>
  </cloudListenerRule>
  <cloudListenerRule name="redirectHPRule" priority="40" status="">
    <cloudRuleCondition type="host" value="example.com"/>
    <cloudRuleCondition type="path" value="/img/*"/>
    <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-t2/cloudapp-ap/cloudepg-provEPG"/>
  </cloudListenerRule>
</cloudListener>
</cloudSvcPolicy>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>

```

REST API を使用したキー リングの設定

この例では、REST API を使用したキー リングのリーク ルートを構成する方法を示します。キー リング構成の詳細については、*Cisco APIC 基本構成ガイド*を参照してください。

キー リングを設定するには:

```

<polUni>
  <fvTenant name="t2">
    <cloudCertStore>
      <pkiKeyRing status="" name="lbCert" tp="lbTP" key="-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAA4DGxaK+RHv/nToHLnmDBq2BfLimgX/zNJQC9bGuzr8Mj7dm0
XuHfQYGv0h1PtL4Pdx5f5qjB0NbhjAVB1Gw8cDiErEgAXy9Km27ySo2foKryNqCRE
Ginn/CgF75QPied568eScNDZPt/eMeHAuRX/PykKUatWWncGanJvHqc+SOLPF6TD
gQ5nwOHFvYm2DY8bfdYWrWmGs07JqZzbPmptA2QWblILsSoIrdkIIgf6ZfYy/EN
bH+nYN2rJT81zYsxx0YmR0oRQHTiN2NiDY/ZV63yxCXfLg9qpNZCuD8K0fdCZPEq
8takiWBxiR5/HRPscWAdWQsoiKgG1k4NEbFA9QIDAQBAoIBAQQDQQA9IslYrdtqN
q6mZ3s2BNfF/4kgb7gn0Dws+9EJLJCJNZVhFEo2ZxxyfPp6HRnjYS50W83/E1and
+GD1bSucTuxqFWIQVh7r1ebYZIWk+NYSjr5yNVxux8U2hCNNV8WWVqKjKcUqICB
Bm47FKj53LV46zE0gyCaibFrYxZJ9+farGneyBdnoV+3thmez7534KCi0t3J3Eri
lgSY3ql6hPXB2ZXAP4jdAoLgWDU4IIM6OqOiWopZM/QYIE/WtPYyJ0QzNCXObtc5
FboDcvedsgd4x5G1fv2A4xTBQMCTZUZJ9fYAcFogTZXD+UVqxorh47tf/mz+1fjq
f1XphEDlAoGBAPVlvKfGW46qqRnYovfryxxx4OM1sVSGcJpQTQtBQi2koJ8OwEZJ
2s+CX0r+oDqWP23go/QEVYVkcic9RGkJBNge1+dm/bTjzgmQYtqSCNtecTsZD5JN
y1jkciizznDkjCjReS22kh3dGXIBRiYk7ezp2z7EKfDrHe5x5ouGMGcnaoGBAOnh
buDEohv8KJaB+DiUfhftoa3aKNPBO+zWPCHP0HFGjPXshJcIYZc1GycmuDKVnDd
MxhE/yOnQHowi4T9FMLpz5yh5zuCUVqOBgB1P6MzbC5t5MtLrEYr/AqFN11CqyXQ
cVcT6iCWlOAFJRw3c/OiESwLMzchs18RnbwOi6kDAoGBANV1zmPb07zB3eGTCU0t
KGiqwFLncUkVadZZRFZYPPnwiRkoe73j9brkNbgCqxW+Nlp5UjoeFry0N6y106q/
ZA4I7FnXryLBw2HYuw41Vixl+XOZ/He03RmFN1z717dGmaGbv43aKIB9x+X5n8wF
6z1ntBhmBk7yNwomlIRag1sbAoGAX0p4cJ/tJNXSe7AswHDQCL68uimJdDfZ5nKG
k83nE+Qc0qQozDJAmCiSfmuSNRnSep3FiafjBFXK0X4h+mdbJCC7bagRnI92Mh0X
mOwsp4P2GdywkZwdbuHQ6UBp1Ferf9aztzTn+as6xKOUATEezy9DK9zMWzQhhtay
m9yZTp0CgYEA1UtcpWjAzQbXODJGmxGdAAakPpeiKw/Da3MccrTdgJt88ezM1Oej
Pdoab0G2PcFgJZoTSGk7N4XArVKeq7pgz0kwcYash06A2Hal+D1z/bGoZP+kmD/x
-----"
    </pkiKeyRing>
  </cloudCertStore>
</fvTenant>
</polUni>

```


REST API を使用した HTTPS サービス ポリシーの作成

このセクションでは、REST API を使用して HTTPS サービス ポリシーを作成する方法を示します。



- (注) リスナーは複数の証明書をもつことができます。証明書のオプションは次のとおりです。
- ELBSecurityPolicy-2016-08-セキュリティポリシーが選択されていない場合のデフォルト。
 - ELBSecurityPolicy-FS-2018-06
 - ELBSecurityPolicy-TLS-1-2-2017-01
 - ELBSecurityPolicy-TLS-1-2-Ext-2018-06
 - ELBSecurityPolicy-TLS-1-1-2017-01
 - ELBSecurityPolicy-2015-05
 - ELBSecurityPolicy-TLS-1-0-2015-04

複数の証明書を使用する場合は、デフォルトの証明書を指定する必要があります。デフォルトは、**cloudRsListenerToCert** の **defaultCert** プロパティを使用して指定されます。

始める前に

キーリング証明書は既に構成されています。

HTTPS サービス ポリシーを作成するには:

```
<polUni>
  <fvTenant name="t2">
    <vnsAbsGraph name="CloudGraph" type="cloud" status="">
      <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
        <cloudSvcPolicy tenantName="t2" contractName="httpFamily" subjectName="consubj">
          <cloudListener name="https_listener" port="443" protocol="https"
secPolicy="eLBSecurityPolicy-2016-08" status="">
            <cloudRsListenerToCert defaultCert="yes" certStore="iam"
tDn="uni/tn-t2/certstore/keyring-lbCert" status=""/>
            <cloudListenerRule name="defaultRule" default="yes" priority="100" status="">
              <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-t1/cloudapp-ap/cloudepg-ep1">
                </cloudRuleAction>
              </cloudListenerRule>
            </cloudListener>
          </cloudSvcPolicy>
        </vnsAbsNode>
      </vnsAbsGraph>
    </fvTenant>
  </polUni>
```

