レイヤ 4 ～ レイヤ 7 のサービスの挿入

この章は、次の内容で構成されています。

レイヤ 4 ～ レイヤ 7 のサービスの挿入

Cisco Application Policy Infrastructure Controller（APIC）は、ネットワーク サービスを管理します。ポリシーは、サービスを挿入するために使用されます。APIC のサービスを統合することでライフサイクルの自動化フレームワークが確立され、サービスがオンラインまたはオフラインになった場合に、システムが動的に対応できるようになります。ファブリック全体で使用可能な共有サービスは、ファブリックの管理者によって管理されます。単一のテナント向けのサービスは、テナントの管理者によって管理されます。

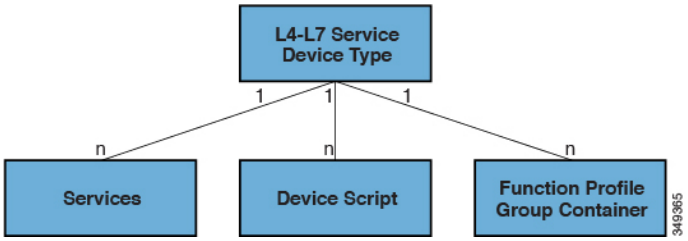
APIC は、ポリシー制御の中心点として機能すると同時に、自動サービス挿入を提供します。APIC ポリシーは、ネットワーク ファブリックとサービス アプライアンスの両方を管理します。APIC は、トラフィックがサービスを通って流れるように、ネットワークを自動的に設定できます。また、APIC はアプリケーション要件に従ってサービスを自動的に構成できます。

このアプローチにより、組織はサービス挿入を自動化し、従来のサービス挿入の複雑なすべてのトラフィック誘導技術の管理に伴う課題を排除できます。

レイヤ 4 ～ レイヤ 7 のポリシー モデル

レイヤ 4 ～ レイヤ 7 のサービス デバイス タイプ ポリシーには、パッケージおよびデバイス スクリプトでサポートされるサービスなどの主要な管理対象オブジェクトが含まれます。次の図は、レイヤ 4 ～ レイヤ 7 のサービス デバイス タイプ ポリシー モデルのオブジェクトを示します。

図 *1*: レイヤ *4* ～ レイヤ *7* のポリシー モデル



レイヤ 4 ～ レイヤ 7 のサービス ポリシーには次のものが含まれます。

- **サービス**：SSL オフロードやロードバランシングなどのデバイスによって提供されるすべての機能のメタデータが含まれます。この MO には、コネクタの名前、VLAN や VXLAN などのカプセル化のタイプ、およびインターフェイス ラベルが含まれます。
- **デバイス スクリプト**：名前、パッケージ名、バージョンなどのスクリプト ハンドラの関連属性に関するメタ情報を含むデバイス スクリプト ハンドラを表します。
- **機能プロファイル グループ コンテナ**：サービス デバイス タイプで使用可能な機能を含むオブジェクト。機能プロファイルには、フォルダに編成されたデバイスでサポートされる構成可能なすべてのパラメータが含まれます。

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重要部分としてサービスを見なします。必要なサービスは、Cisco Application Policy Infrastructure Controller（APIC）からの Cisco ACI ファブリックでインスタンス化されたサービス グラフとして処理されます。ユーザは、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、トランスフォーム（SSL ターミネーション、VPN ゲートウェイ）、フィルタ（ファイアウォール）、または端末（侵入検知システム）など、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。
- 接続：接続によって、ネットワーク経由でトラフィックを転送する方法が決定されます。

グラフが Cisco APIC に設定されると、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 はまた、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が、これによってサービス デバイスでの変更は要求されません。

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。

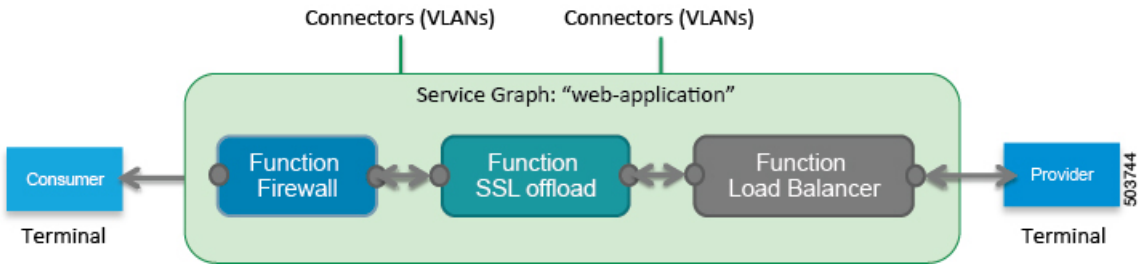
サービス アプライアンス（デバイス）は、グラフ内でサービス機能を実行します。1 つ以上のサービス アプライアンスが、グラフに必要なサービスをレンダリングするために必要になることがあります。1 つ以上のサービス機能が単一のサービス デバイスで実行できます。

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。

- エンドポイント グループで送受信されたトラフィックはポリシーに基づいてフィルタリングでき、トラフィックのサブセットはグラフ内の異なるエッジにリダイレクトできます。
- サービス グラフのエッジには方向性があります。
- タップ（ハードウェア ベースのパケット コピー サービス）は、サービス グラフの異なるポイントに接続できます。
- 論理機能は、ポリシーに基づいて適切な（物理または仮想）デバイスでレンダリングできます。
- 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。
- 論理サービス機能は、要件に応じて、拡張や縮小が可能で、クラスタ モードまたは 1:1 アクティブ/スタンバイ ハイアベイラビリティ モードで展開できます。

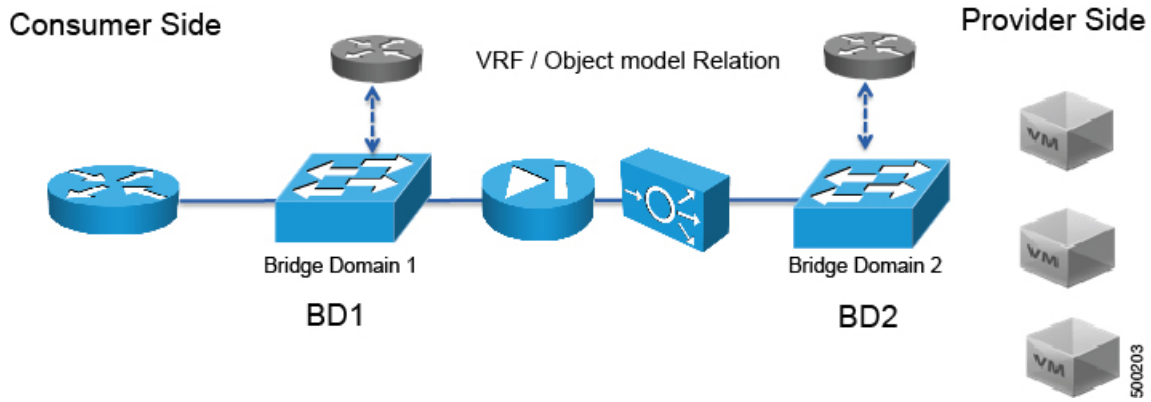
次の図は、サービスグラフの導入の例を示しています:

図 *2:* サービス グラフの展開の例



サービスグラフを展開するには、次の図に示すようにブリッジドメインと VRF インスタンスが必要です。

図 *3:* サービスグラフのブリッジドメインと *VRF* インスタンス



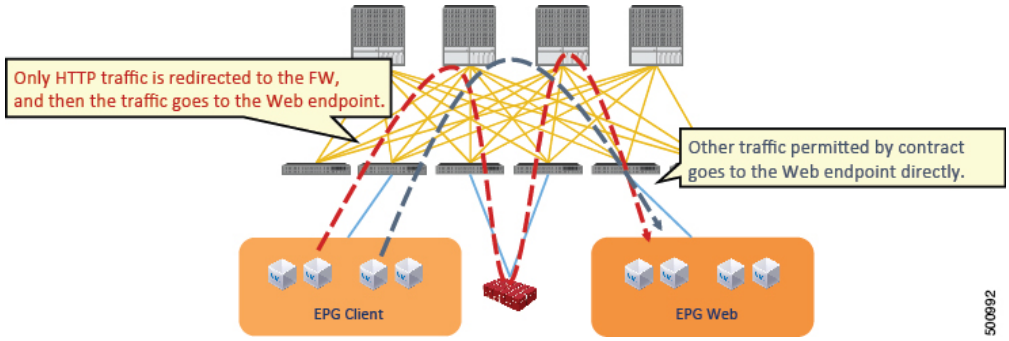
（注） 使用すると、その他のテナント内のエンドポイント グループに関連付けられているサービス グラフの脚の一部があるかどうか、 **グラフ テンプレートの関連のオブジェクトを削除** GUI で、機能、 Cisco APIC 以外のテナントからインポートされた契約は削除されませんサービス グラフが存在します。Cisco APICもサービス グラフよりも異なるテナントにあるエンドポイント グループ契約のクリーニングはありません。手動で異なるテナントではこれらのオブジェクトを削除する必要があります。

ポリシーベースのリダイレクトについて

Cisco Application Centric Infrastructure (ACI) ポリシーベースリダイレクト (PBR) により、ファイアウォールやロードバランサなどのサービスアプライアンスをプロビジョニングできます。一般的な使用例としては、プールしてアプリケーションプロファイルに合わせて調整すること、また容易にスケーリングすることができ、サービス停止の問題が少ないサービスアプライアンスのプロビジョニングがあります。PBRにより、プロビジョニングするコンシューマおよびプロバイダー エンドポイント グループをすべて同じ仮想ルーティングおよび転送（VRF）インスタンスに含めることで、サービス アプライアンスの展開をシンプル化できます。PBR の導入は、ルート リダイレクト ポリシーおよびクラスタのリダイレクト ポリシーの設定と、ルーティングとクラスタ リダイレクト ポリシーを使用するサービス グラフ テンプレートの作成から構成されます。サービス グラフ テンプレートを展開した後は、サービス グラフ プロバイダーのエンドポイント グループを利用するためにエンドポイント グループを有効にすることにより、サービスアプライアンスを使用します。これは、vzAny を使用することにより、さらに簡素化し、自動化できます。パフォーマンスの要件が、専用のサービスアプライアンスをプロビジョニングするかどうかを決定するものとなるのに対し、PBR を使用すれば、仮想サービス アプライアンスの展開も容易になります。

次の図は、ファイアウォールへのトラフィックに固有の、リダイレクトの使用例を示しています:

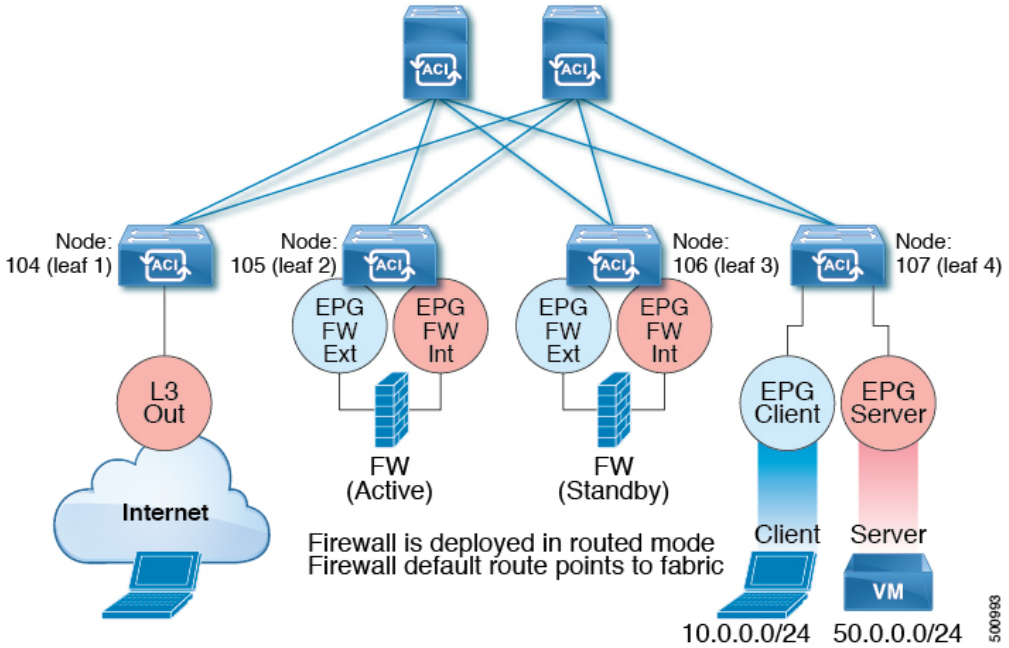
図 *4*:使用例:ファイアウォール特有のトラフィックのリダイレクト



この使用例では、2つの情報カテゴリを作成する必要があります。最初の情報カテゴリはHTTPトラフィックを許可します。その後このトラフィックはファイアウォールにリダイレクトされます。トラフィックはファイアウォールを通過してから、Webエンドポイントに送られます。2 番目の情報カテゴリはすべてのトラフィックを許可します。これは最初の情報カテゴリではリダイレクトされなかったトラフィックをキャプチャします。トラフィックはそのまま Web エンドポイントに送られます。

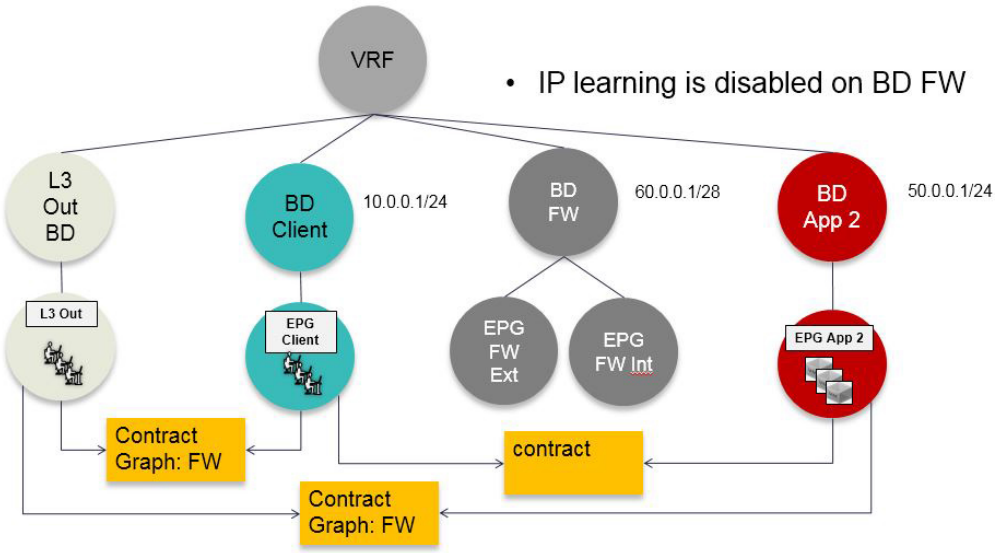
次の図は、ACI PBR 物理トポロジのサンプルを示しています:

図 *5*:サンプルの *ACI PBR* 物理トポロジ



次の図は、ACI PBR 論理トポロジのサンプルを示しています:

図 *6*: サンプルの *ACI PBR* 論理トポロジ



これらの例はシンプルな導入ですが、 ACI PBR は、ファイアウォールやサーバのロード バランサなどのような、複数のサービスのために物理および仮想サービス アプライアンスの両方を混在させたものにスケールアップすることを可能にします。

対称ポリシー ベースのリダイレクトについて

対称ポリシーベースリダイレクト(PBR)構成により、サービスノードのプールをプロビジョニングできるため、ポリシーに基づき、コンシューマーとプロバイダーのエンドポイントグループ間のトラフィックを負荷分散できます。トラフィックは、送信元および宛先 IP 等価コスト マルチパス ルーティング(ECMP)プレフィックス ハッシュに応じて、プール内のサービス ノードの 1 つにリダイレクトされます。

（注） 対称 PBR 構成には、9300-EX 以降のハードウェアが必要です。

対称 PBR REST のサンプルの例を以下に示します。

```
Under fvTenant svcCont

<vnsSvcRedirectPol name="LoadBalancer_pool">
          <vnsRedirectDest name="lb1" ip="1.1.1.1" mac="00:00:11:22:33:44"/>
          <vnsRedirectDest name="lb2" ip="2.2.2.2" mac="00:de:ad:be:ef:01"/>
          <vnsRedirectDest name="lb3" ip="3.3.3.3" mac="00:de:ad:be:ef:02"/>
</vnsSvcRedirectPol>

<vnsLIfCtx name="external">
          <vnsRsSvcRedirectPol tnVnsSvcRedirectPolName="LoadBalancer_pool"/>
          <vnsRsLIfCtxToBD tDn="uni/tn-solar/bd-fwBD">
</vnsLIfCtx>

<vnsAbsNode name="FW" routingMode="redirect">
```

対称 PBR NX-OS スタイルの CLI コマンドの例を次に示します。

テナント スコープの下の次のコマンドは、サービス リダイレクト ポリシーを作成します。

```
apic1(config-tenant)# svcredir-pol fw-external
apic1(svcredir-pol)# redir-dest 2.2.2.2 00:11:22:33:44:56
```

次のコマンドは PBR を有効にします。

```
apic1(config-tenant)# l4l7 graph FWOnly contract default
apic1(config-graph)# service FW svcredir enable
```

次のコマンドは、デバイス選択ポリシー コネクタの下にリダイレクト ポリシーを設定します。

```
apic1(config-service)# connector external
apic1(config-connector)# svcredir-pol tenant solar name fw-external
```

自動サービス挿入

VLANおよび仮想ルーティングおよび転送（VRF）スイッチングは、従来のサービス挿入モデルによってサポートされますが、Application Policy Infrastructure Controller（APIC）はポリシー制御の中心点として機能する一方で、サービス挿入とセキュアソケットレイヤ（SSL）オフロード、サーバ ロード バランシング（SLB）、Web アプリケーション ファイアウォール（WAF）およびファイアウォールなどのネットワーク サービスのプロビジョニングを自動化できます。ネットワーク サービスは通常、Application Delivery Controller（ADC）やファイアウォールなどのサービス アプライアンスによってレンダリングされます。APIC ポリシーは、ネットワーク ファブリックとサービス アプライアンスの両方を管理します。APIC は、トラフィックがサービスを通って流れるように、ネットワークを自動的に設定できます。APICは、アプリケーション要件に従ってサービスを自動的に設定することもでき、それにより組織はサービス挿入を自動化し、従来のサービス挿入の複雑な技術の管理に伴う課題を排除できます。

デバイス パッケージについて

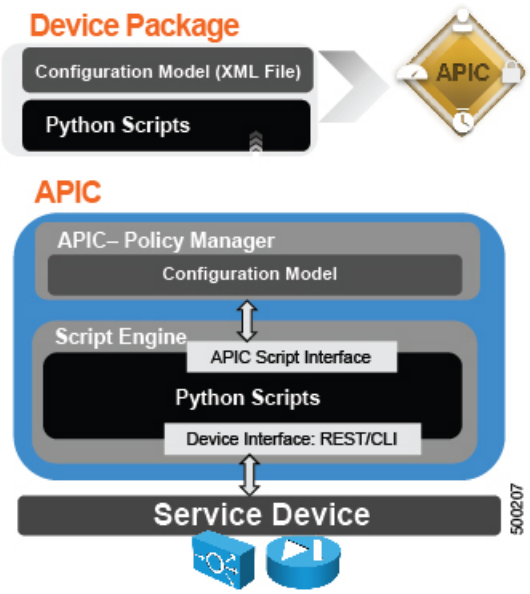
Application Policy Infrastructure Controller（APIC）は、サービス デバイスの設定およびモニタリングにデバイス パッケージを必要とします。Cisco APIC にサービスの機能を追加するには、デバイス パッケージを使用します。デバイス パッケージは、単一クラスのサービス デバイスを管理し、デバイスとその機能に関する情報を Cisco APIC に提供します。デバイス パッケージは次の項目を含む `zip` ファイルです。

デバイス仕様	次を定義する XML ファイル： • デバイス プロパティ： • **[Model]**：デバイスのモデル。 • **[Vendor]**：デバイスのベンダー。 • **[Version]**：デバイスのソフトウェア バージョン。 • ロード バランシング、コンテンツ切り替え、および SSL 終端などの、デバイスによって提供される機能。 • 各機能のインターフェイスおよびネットワーク接続情報。 • デバイス設定パラメータ。 • 各機能の設定パラメータ。
デバイス スクリプト	Cisco APIC とデバイスのやりとりに使用される Python スクリプト。Cisco APIC イベントは、デバイス スクリプトで定義した機能呼び出しにマッピングされます。デバイス パッケージには、複数のデバイス スクリプトを含めることができます。デバイス スクリプトは、REST、SSH、または、同様のメカニズムを使用して、デバイスと連携できます。
機能プロファイル	ベンダーによって指定されたデフォルト値を持つ機能パラメータ。これらのデフォルト値を使用するように機能を設定できます。
デバイス レベル設定パラメータ	デバイスに必要なパラメータを指定するコンフィギュレーション ファイル。この設定は、デバイスを使用している 1 つ以上のグラフで共有できます。

デバイス パッケージを作成できます。または、デバイス ベンダーか Cisco によって提供されるものを使用できます。

次の図では、デバイス パッケージと Cisco APIC の関係について説明します:

図 *7:* デバイス パッケージと、*Cisco APIC*

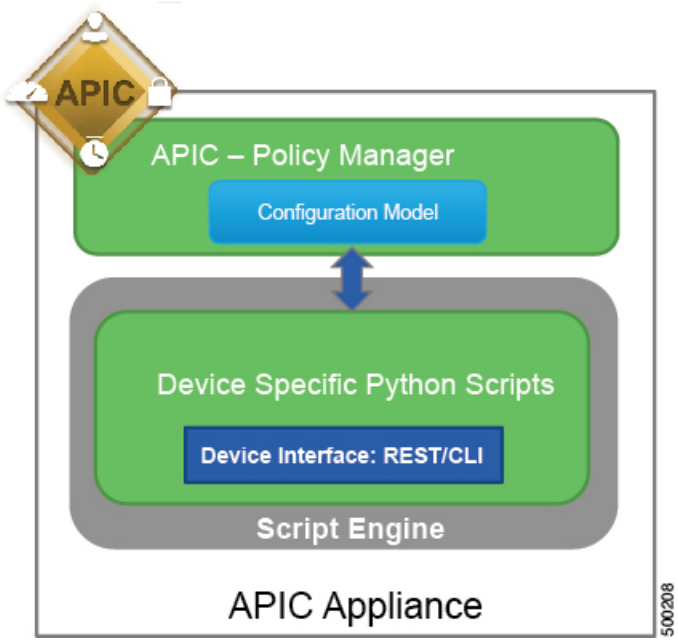


デバイスのスクリプトでの機能は、次のカテゴリに分類されます。

- デバイス/インフラストラクチャ：デバイス レベルの設定とモニタリングを行うため
- サービス イベント：デバイス上でサーバのロード バランサまたはセキュア ソケット レイヤなどの機能を設定するため
- エンドポイント/ネットワーク イベント：エンドポイントとネットワークの接続/接続解除イベントを処理するため

Cisco APIC は、デバイス パッケージで提供されたデバイス構成モデルを使用して、デバイス スクリプトに適切な構成を渡します。デバイス スクリプト ハンドラは、REST または CLI インターフェイスを使用してデバイスと連解します。

図 *8*: デバイス スクリプトがサービス デバイスと連携する方法



デバイス パッケージにより、管理者は次のサービスの管理を自動化することができます。

- デバイスの接続と切断
- エンドポイントの接続と切断
- サービス グラフのレンダリング
- ヘルス モニタリング
- アラーム、通知、ロギング
- カウンタ

デバイス パッケージとデバイス パッケージを作成する方法の詳細については、『*Cisco APIC Layer 4 to Layer 7 Device Package Development Guide*』を参照してください。

デバイス クラスタについて

デバイス クラスタ（別名論理デバイス）は、単一のデバイスとして機能する 1 つ以上の具象デバイスです。デバイス クラスタには、そのデバイス クラスタのインターフェイス情報を説明するクラスタ（論理）インターフェイスがあります。サービス グラフ テンプレートのレンダリング時に、機能ノード コネクタはクラスタ（論理）インターフェイスに関連付けられます。Application Policy Infrastructure Controller（APIC）は、サービス グラフ テンプレートのインスタンス化およびレンダリング時に機能ノード コネクタにネットワーク リソース（VLAN）を割り当て、クラスタ（論理）インターフェイスにネットワーク リソースをプログラミングします。

Cisco APIC では、グラフのインスタンス化時にサービスグラフに対してネットワークリソースのみを割り当てて、ファブリック側のみをプログラミングできます。この動作は、既存のオーケストレータまたはデバイスクラスタ内のデバイスをプログラムする dev-op ツールがすでにある環境では有効です。

Cisco APIC はデバイス クラスタおよびデバイスのトポロジ情報 （論理インターフェイスと具象インターフェイス） を把握する必要があります。この情報により、Cisco APIC はリーフスイッチの適切なポートをプログラミングできます。また、Cisco APIC ではこの情報をトラブルシューティング ウィザードの目的で使用できます。さらに、Cisco APIC はカプセル化の割り当てに使用する `DomP` との関係も把握する必要があります。

デバイス クラスタまたは論理デバイスは、物理デバイスまたは仮想デバイスのいずれかです。デバイス クラスタは、そのクラスタの一部である仮想マシンが、VMM ドメインを使用して Cisco APIC と統合されたハイパーバイザ上に存在する場合、仮想と見なされます。これらの仮想マシンが VMM ドメインの一部ではない場合、仮想マシン インスタンスであっても物理デバイスとして扱われます。

（注） 論理デバイスには、VMware VMM ドメインまたは SCVMM VMM ドメインのみを使用できます。

次の設定が必要です。

- 論理デバイス（`vnsLDevViP`）およびデバイス（`CDev`）の接続情報
- サポートする機能タイプ（go-through、go-to、L1、L2）に関する情報

サービス グラフ テンプレートは、管理者が定義するデバイス選択ポリシー（論理デバイス コンテキストと呼ばれます）に基づく特定のデバイスを使用します。

管理者は、アクティブ/スタンバイ モードで最大2つの具象デバイスをセットアップできます。

デバイス クラスタをセットアップするには、次のタスクを実行する必要があります。

1. ファブリックに具象デバイスを接続します。
2. Cisco APIC を使用してデバイス クラスタを構成します。

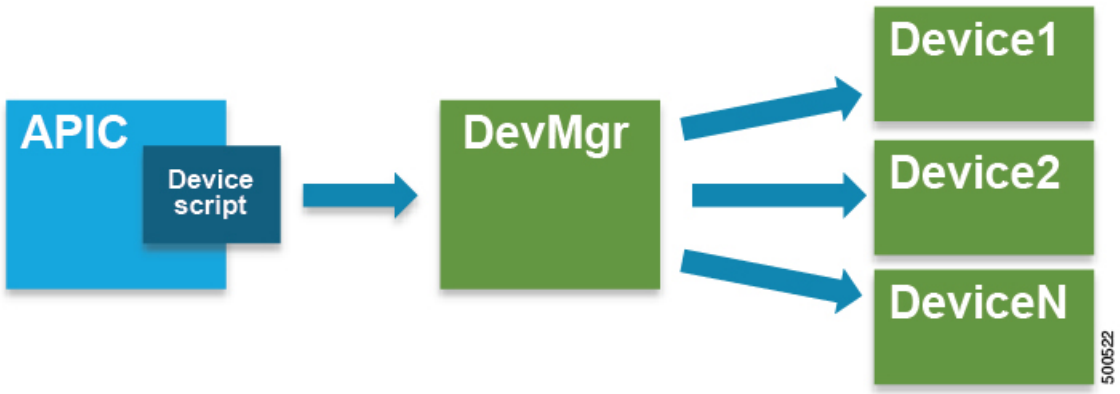
（注） Cisco APIC は、2 つのデバイスのクラスタに IP アドレスが重複して割り当てられているかどうかを検証しません。Cisco APIC は、2 つのデバイスのクラスタが同じ管理 IP アドレスを持っている場合、不適切なデバイスのクラスタをプロビジョニングすることがあります。デバイス クラスタで IP アドレスが重複している場合には、いずれかのデバイスの IP アドレスの設定を削除し、管理 IP アドレスの設定のためにプロビジョニングされた IP アドレスが重複していないことを確認してください。

デバイス マネージャとシャーシ マネージャについて

デバイス マネージャのみで、Cisco Application Centric Infrastructure（ACI）ファブリック内の一連のクラスタを設定できます。管理状態または動作状態はデバイスのネイティブの GUI に表示されます。デバイス マネージャが個々のデバイスの設定を処理するため、Application Policy Infrastructure Controller（APIC）での設定をシンプル化できます。デバイス マネージャにテンプレートを作成してから、APIC のインスタンス固有の値をデバイス マネージャに入力しますが、必要な値はごくわずかです。

次の図に、クラスタ内で複数のデバイスを制御するデバイス マネージャを示します。

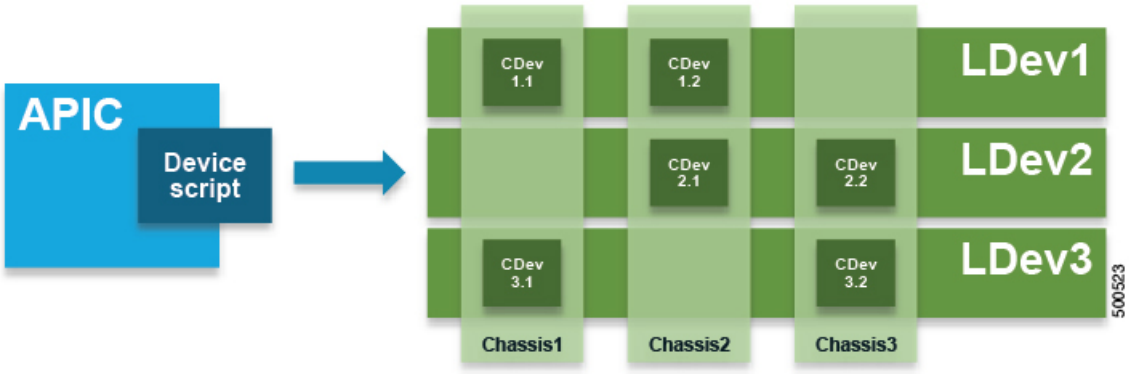
図 *9*: デバイス マネージャでのデバイスの制御



シャーシ マネージャは、処理リソースの物理または仮想「コンテナ」です。シャーシ マネージャは CDev オブジェクトとして表される、いくつかの仮想サービス デバイスをサポートします。シャーシマネージャがネットワーキングを処理し、CDev がプロセスを処理します。シャーシマネージャによって、仮想処理ノードのオンデマンド作成が可能になります。仮想デバイスでは、サービス（特に VLAN）の一部を、仮想マシンではなく、シャーシに適用する必要があります。これを実現するには、シャーシ管理 IP アドレスとクレデンシャルをコールアウトに含める必要があります。

次の図に、処理リソースのコンテナとして機能するシャーシ マネージャを示します。

図 *10* : デバイス マネージャでのデバイスの制御

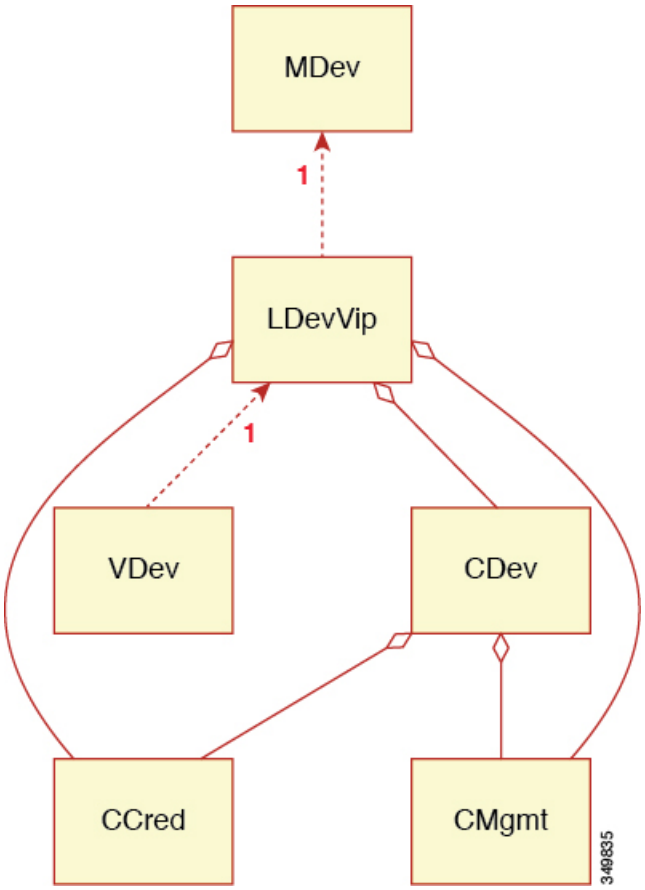


デバイス マネージャまたはシャーシ マネージャを使用せず、サービス デバイスのモデルに次の主要な管理対象オブジェクトを含めます。

- `MDev`：デバイス タイプ（ベンダー、モデル、バージョン）を表します。
- `LDevVIP`：クラスタ、つまりCold Standbyを実現するために同一に設定された一連のデバイスを表します。デバイスにアクセスするための `CMgmt` と `CCred` が含まれます。
- `CDev`：物理または仮想のいずれかのクラスタのメンバーを表します。デバイスにアクセスするための `CMgmt` と `CCred` が含まれます。
- `VDev`：サーバ上の仮想マシンと同様のクラスタのコンテキストを表します。

次の図に、`CMgmt`（管理接続）と `CCred`（クレデンシャル）が含まれた、主要な管理対象オブジェクトのモデルを示します。

図 *11* : デバイス マネージャまたはシャーシ マネージャを含まない管理対象オブジェクト モデル



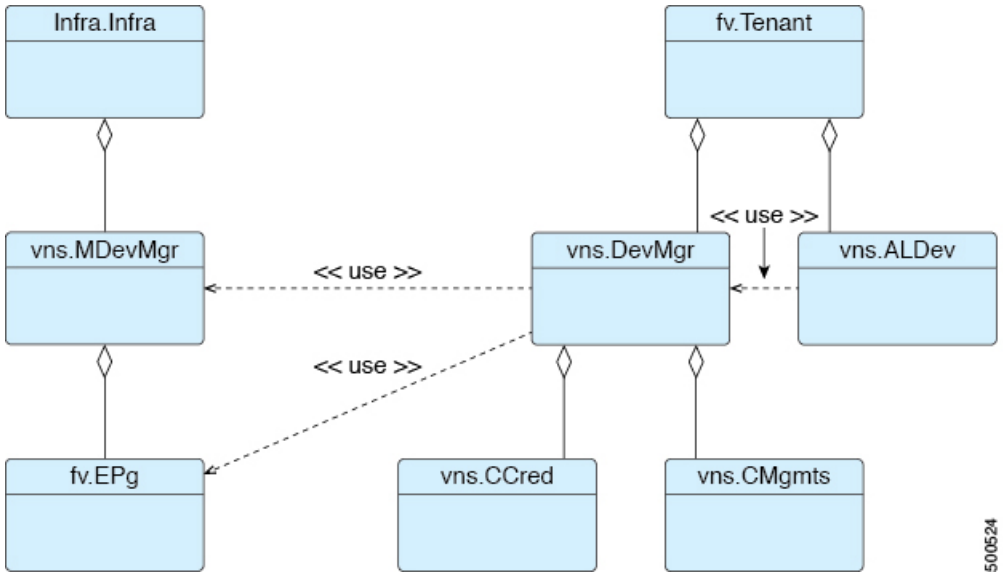
CMgmt（ホスト＋ポート）と CCred（ユーザ名＋パスワード）により、スクリプトでデバイスとクラスタにアクセスできます。

デバイス マネージャとシャーシ マネージャは、集中管理ステーションからのクラスタとデバイスの設定を制御できるようにします。シャーシは並列階層を MDev オブジェクトと ALDev オブジェクトに追加し、特定のシャーシに属しているというタグを CDev オブジェクトに付けることができます。次の管理対象オブジェクトがモデルに追加され、デバイスおよびシャーシマネージャの概念をサポートします。

- MDevMgr：デバイス マネージャのタイプを表します。MDevMgr は、同じベンダーの通常は異なる製品である一連の異なる MDev を管理できます。
- DevMgr：デバイス マネージャを表します。マネージャにアクセスするには、含まれている CMgmt と CCred の管理対象オブジェクトを使用します。各クラスタは 1 つの DevMgr のみと関連付けることができます。
- MChassis：シャーシのタイプを表します。通常、この管理対象デバイスはパッケージに含まれています。
- Chassis：シャーシ インスタンスを表します。これには、CMgmt と CCred[Secret] の管理対象オブジェクトが含まれており、シャーシへの接続を提供します。

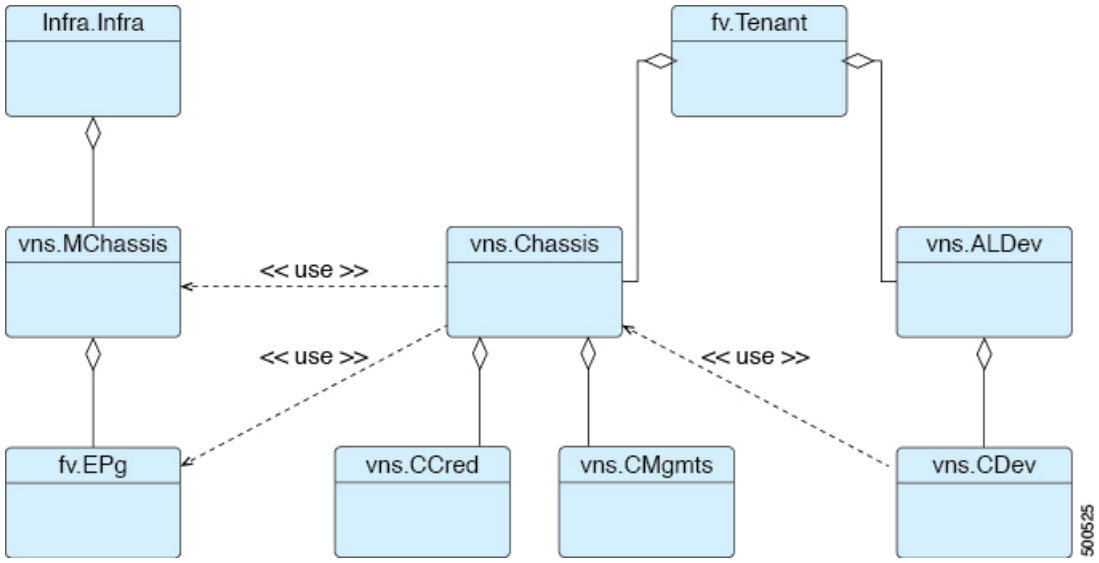
次の図に、デバイス マネージャのオブジェクト モデルを示します。

図 *12 :* デバイス マネージャのオブジェクト モデル



次の図に、シャーシ マネージャのオブジェクト モデルを示します。

図 *13 :* シャーシ マネージャのオブジェクト モデル



具象デバイスについて

具象デバイスとしては、物理デバイスと仮想デバイスがあり得ます。デバイスが仮想デバイスの場合は、コントローラ（vCenter または SCVMM コントローラ）と仮想マシン名を選択する必要があります。具象デバイスには、具象インターフェイスがあります。具象デバイスが論理

デバイスに追加されると、具象インターフェイスが論理インターフェイスにマッピングされます。サービス グラフ テンプレートのインスタンス化時に、VLAN および VXLAN は、論理インターフェイスとの関連付けに基づいた具象インターフェイス上でプログラミングされます。

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。

Cisco Application Policy Infrastructure Controller (APIC) は、ネットワークリソースを割り当てて、ファブリック側で VLAN/VXLAN のプログラミングのみを実行します。

次の設定は必要ありません。

- `MFunc` の関係
- サポートされる機能タイプ（go-through、go-to）に関する情報

Cisco APIC は、機能ノードのネットワーク情報（LIF、CIF）を把握する必要があります。この情報は、Cisco APIC がリーフスイッチでネットワークを適切にプログラムするためと、Cisco APIC がこの情報をトラブルシューティング ウィザードの目的で使用するために必要です。

さらに、次の設定が必要です。

- グラフ インスタンス化時に `LDevVip` の選択を可能にする `LDevCtx`
- グラフ インスタンス化時に `LIf` の選択を可能にする `LIfCtx`
- `LIfCtx` 内のブリッジ ドメイン
- `LIfCtx` でのルート ピアリング
- `LIfCtx` 内のサブネット

（注） Cisco ACI マルチサイト 構成の場合、サービスグラフに最大 2 つのノードを展開できます。非 Cisco ACI マルチサイト 構成の場合、サービスグラフに最大 5 つのノードを展開できます。

機能ノード コネクタについて

機能ノード コネクタは、サービス グラフに機能ノードを接続し、グラフのコネクタ サブネットに基づいて適切なブリッジ ドメインと接続と関連付けられます。各コネクタは、VLAN または Virtual Extensible LAN（VXLAN）に関連付けられます。コネクタの両側がエンドポイント グループ（EPG）として扱われ、ホワイトリストがスイッチにダウンロードされ、2 つの機能ノード間の通信がイネーブルになります。

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台のアプリケーション エンドポイント グループ（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 EPG とプロバイダー 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。

権限について

管理者は、（APIC）でロールに権限を付与できます。権限は、ロールが実行できるタスクを決定します。管理者は、管理者のロールに次の権限を付与できます。

特権	説明
nw-svc-connectivity	• 管理 EPG の作成 • 他のオブジェクトに管理接続を作成
nw-svc-policy	• サービス グラフの作成 • アプリケーション EPG およびコントラクトへのサービス グラフのアタッチ • サービス グラフのモニタ
nw-svc-device	• デバイス クラスタの作成 • 具象デバイスの作成 • デバイス コンテキストの作成

（注） インフラストラクチャの管理者だけがデバイス パッケージを APIC にアップロードできます。

サービスの自動化と構成管理

Cisco APIC は、サービス デバイスの構成管理と自動化のポイントとして任意に動作でき、ネットワーク自動化とのサービス デバイスの調整を行うことができます。Cisco APIC は、さまざまなイベントで Python スクリプトを使用してサービス デバイスと連動し、デバイス固有の Python スクリプト機能を呼び出します。

デバイス スクリプトとサービス デバイスでサポートされる機能を定義するデバイスの仕様は、デバイス パッケージとしてまとめられ、Cisco APIC にインストールされます。デバイス スクリプト ハンドラは、デバイス構成モデルに基づいてその REST インターフェイス（推奨）または CLI を使用してデバイスとやりとりします。

サービス リソースのプーリング

Cisco ACI ファブリックは、多数の接続先間で非ステートフル負荷分散を実行できます。この機能により、組織は物理および仮想サービス デバイスをサービス リソース プールにグループ化でき、機能や場所によってさらにグループ化できます。これらのプールは、標準の高可用性メカニズムを使用することで高可用性を提供するか、または障害が発生した場合に、他のメンバーに負荷が再分散された状態で簡易なステートフル サービス エンジンとして使用できます。どちらのオプションでも、等コスト マルチパス（ECMP）、ポートチャネル機能および共有状態を必要とするサービス アプライアンスのクラスタリングの現在の制限をはるかに超える横方向の拡張性が提供されます。

サービス デバイスがファブリックとやりとりする必要がない場合、Cisco ACI はサービス デバイスを使用して簡易バージョンのリソース プーリングを実行できます。また、ファブリックとサービス デバイス間の調整を伴うより高度なプーリングも実行できます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。