Cisco APIC の設定

Cisco Application Policy Infrastructure Controller 設定の推薦構成

特定の Cisco Application Policy Infrastructure Controller （APIC）設定を有効にすることをお勧めします。

Enforce Subnet Check

サブネット チェックの適用機能は、Cisco Application Centric Infrastructure（ACI）が IP アドレスをデータ プレーンからエンドポイントとして学習した場合、VRF インスタンス レベルでサブネットのチェックを適用します。サブネット チェックの範囲は VRF インスタンスですが、ファブリック全体での設定ポリシーの下では、この機能をグローバルにのみ有効または無効にすることができます。このオプションを有効にすると、ファブリックはブリッジ ドメインに構成されている 1 つのサブネット以外からは IP アドレスを学習しません。この機能は、このようなシナリオで、ファブリックがエンドポイント情報を学習しないようにします。

サブネット チェックの適用に関する注意事項と制約事項

1 つの VRF インスタンスだけでこのオプションを有効にすることはできません。オプションを有効にすると、すべての VRF インスタンスで有効になります。

サブネット チェックの適用を有効にする

1. **[システム（System）] > [システム設定（System Settings）] > [ファブリック全体での設定（Fabric Wide Setting）]**
2. **[サブネット チェックの適用（Enforce Subnet Check）]** ボックスをオンにします。

IP エージング ポリシー

IP エージング ポリシーは、エンドポイント上の使用されていない IP アドレスを追跡し、その寿命を管理します。Cisco APIC は、ローカルのエンドポイント エージング間隔の 75% で、IPv4 の場合には ARP リクエスト、IPv6 の場合にはネイバー誘導を送信する、ブリッジ ドメイン用に構成されたエンドポイント保持ポリシーを使用して追跡を実行します。Cisco APIC が IP アドレスから応答を受信しなかった場合、その IP アドレスはエージング アウトします。

IP エージング ポリシーを有効にする

1. **[システム（System）] > [システム設定（System Settings）] > [エンドポイント制御（Endpoint Controls）]** に移動します。
2. **[IP エージング（IP Aging）]** タブをクリックします。
3. **[管理状態（Administrative State）]** で **[有効（Enabled）]** を選択します。

ミスケーブル プロトコル

ミスケーブルプロトコル（MCP）は、リンク層検出プロトコル（LLDP）やスパニング ツリー プロトコル（STP）では検出できない、さまざまな問題（構成ミスなど）によって発生する可能性のあるループを検出します。このオプションは、MCP が EPG 単位でパケットを送信できるようにします。

ミスケーブル プロトコルを有効にする

1. **[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] >> [ポリシー（Policies）] > [グローバル（Global）] > [MCP インスタンス ポリシー デフォルト（MCP Instance Policy default）]** に移動します。
2. **[管理状態（Administrative State）]** で **[有効（Enabled）]** を選択します。
3. **[VLAN 単位での MCP PDU を有効にする（Enable MCP PDU per VLAN）]** ボックスをオンにします。

Cisco Application Policy Infrastructure Controller のインターフェイス

次のインターフェイスを使用して、アプリケーション プログラミング インターフェイス（API）を介して Cisco Application Policy Infrastructure Controller（APIC）のすべての機能にアクセスまたは構成できます。

GUI

Cisco APIC GUI は、内部的に REST API メッセージを交換することによって Cisco APIC エンジンと通信する、Cisco APIC へのブラウザベースのグラフィカル インターフェイスです。大規模な構成、展開、および運用には GUI を使用します。GUI を使用すれば、大規模なファブリック構成と展開を自動化するための、インスイッチ プロファイル、インターフェイス プロファ

イル、ポリシー グループ、アクセス エンティティ プロファイル（AEP）などのきめ細かなポリシー制御が可能です。

Cisco APIC GUI の詳細については、「『*Cisco APIC Getting Started Guide*』」および「*Cisco APIC* ベーシック コンフィギュレーション ガイド」を参照してください。

NX-OS スタイルの CLI

NX-OS スタイルのコマンドラインインターフェイス（CLI）は、Cisco APIC の構成、展開、および運用に使用できます。CLI は、EXEC モードをルートとするコマンド モードの階層にまとめられています。グローバル コンフィギュレーション モードで始まるコンフィギュレーション サブモードのツリーとなっています。使用できるコマンドは実行しているモードによって異なります。

Cisco APIC を構成するために、NX-OS スタイルの CLI と APIC GUI の両方を使用する場合の重要な注意事項については、ユーザー インターフェイスの混在に関する制限 （3 ページ） を参照してください。

REST API

REST API は構成の変更を受け取り、コントローラの管理機能にアクセスできるようにします。このインターフェイスは、GUI や CLI の重要なコンポーネントであり、自動化ツール、プロビジョニング スクリプト、およびサードパーティのモニタリング ツールや管理ツールへのアクセス ポイントにもなっています。

Cisco APIC REST API は、REST アーキテクチャを使用するプログラマチック インターフェイスです。API は JavaScript オブジェクトの表記（JSON）または拡張マークアップ言語（XML）のドキュメントを含む HTTP（デフォルトでは無効）または HTTPS のメッセージを受け入れ、返します。任意のプログラミング言語を使用して、API メソッドまたは管理対象オブジェクトに関する記述を含むメッセージや、JSON または XML ドキュメントを生成できます。

REST API の詳細については、 *Cisco APIC REST API* 設定ガイド を参照してください。

ユーザー インターフェイスの混在に関する制限

Cisco APIC は構成のための複数のユーザー インターフェイス (UI) をサポートしているので、ある UI を使用して構成を作成し、その後別の UI を使用して構成を変更することは可能ですが、予期しない結果になることがあります。たとえば、NX-OS スタイル CLI を使用して実行された構成も、APIC GUI で表示できます。表示はできますが、GUI では編集できないこともあり得ます。同様に、APIC GUI で行われた変更も、NX-OS スタイル CLI で確認はできますが、部分的にしか変更できないことがあります。

インターフェイスごとに構成する場合の NX-OS スタイルの CLI と Cisco APIC GUI の混在による制限

インターフェイスごとに構成する場合、Cisco APIC GUI で実行した構成が、NX-OS スタイルの CLI では部分的にしか扱えない場合があります。

たとえば、GUI の **[テナント（Tenants）] > [tenant-name] > [アプリケーション プロファイル（Application Profiles）] > [application-profile-name] > [アプリケーション EPG（Application EPGs）] > [EPG-name] > [スタティック ポート（Static Ports）] > [PC、VPC、インターフェイス上に静的 EPG を展開（Deploy Static EPG on PC, VPC, or Interface）]** でスイッチ ポートを構成したとします。次に NX-OS スタイルの CLI で **show running-config** コマンドを使用すると、以下のように出力されます。

```
leaf 102
interface ethernet 1/15
switchport trunk allowed vlan 201 tenant t1 application ap1 epg ep1
 exit
 exit
```

NX-OS スタイルの CLI でこれらのコマンドを使用してスタティック ポートを設定すると、次のエラーが発生します。

```
apic1(config)# leaf 102
apic1(config-leaf)# interface ethernet 1/15
apic1(config-leaf-if)# switchport trunk allowed vlan 201 tenant t1 application ap1 epg
ep1
No vlan-domain associated to node 102 interface ethernet1/15 encap vlan-201
```

これは、CLI に APIC GUI では実行されない検証があることが原因です。**show running-config** コマンドによって出力されたコマンドが NX-OS CLI で機能するためには、vlan ドメインが事前に構成されている必要があります。設定の順序は GUI に適用されません。

レイヤ 3 外部接続コンフィギュレーション モードのユーザ インターフェイスの混在に関する制限

ここでは、さらに他のユーザーインターフェイスを使用していた場合、NX-OS スタイルの CLI を使用してレイヤ 3 外部接続を構成するための考慮事項を説明します。

APIC NX-OS スタイルの CLI を使用してレイヤ 3 外部接続を設定する場合、次の 2 つのモードを選択することができます。

- **暗黙モード**：シンプルなモードですが、APIC GUI または REST API と互換性がありません。
- **名前付き（または明示）モード**：APIC GUI および REST API と互換性があります。

いずれの場合も、設定は互換性がない UI では読み取り専用であると考えてください。

レイヤ 3 外部接続コンフィギュレーション モードの違い

どちらのモードでも、構成設定は API の l3extOut クラスのインスタンスである内部コンテナ オブジェクト「Layer 3 Outside」（または「L3Out」）内で定義されます。2 つのモード間の主な違いは、このコンテナ オブジェクト インスタンスの命名にあります。

- **暗黙モード**：コンテナの命名は暗黙的であり、CLI コマンドには表示されません。CLI は、これらのオブジェクトを内部的に作成し保持します。
- **名前付きモード**： コンテナの名前を指定します。名前付きモードの CLI コマンドには、追加の l3Out フィールドがあります。名前付き L3Out を正常に構成し、障害を回避するた

めには、ユーザーが外部レイヤ 3 構成用の API オブジェクト モデルを理解する必要があります。

（注） 「名前付きモードを使用したレイヤ3外部接続の構成」セクションの手順を除き、このガイドでは、暗黙モードの手順を説明します。

レイヤ3外部接続コンフィギュレーション モードの注意事項と制約事項

次の注意事項と制約事項は、レイヤ 3 外部接続コンフィギュレーション モードに適用されます。

暗黙モードと名前付きモードの併用

同じ Cisco APIC インスタンスで、両方のモードを一緒に使用してレイヤ 3 外部接続を構成できます。ただし、テナント、VRF インスタンス、およびリーフ スイッチの特定の組み合わせに対するレイヤ 3 外部接続構成は、1 つのモードでのみ実行できます。

レイヤ 3 外部接続用に展開されたテナント VRF インスタンスに 1 つのモードを使用する

特定のテナント VRF インスタンスの場合、外部 EPG を配置できるポリシー ドメインは、名前付きモードまたは暗黙モードのいずれかになります。推奨する構成方式は、特定のテナント VRFインスタンスがレイヤ3外部接続用に展開されるすべてのノード全体で、その特定のテナント VRF インスタンスの組み合わせに対する 1 つのモードだけを使用することです。モードは、異なるテナントまたは異なる VRF インスタンス全体で異なったものにすることができ、制限は適用されません。

構成は不整合に対して検証される可能性がある

場合によっては、Cisco APIC クラスタへの着信設定で不整合が検証されます。外部から確認できる設定（L3Outを通過するノースバウンド トラフィック）も検証の対象です。構成が無効な状況では、構成が無効であるとのエラー メッセージが表示されます。

外部レイヤ 3 機能でサポートされるコンフィギュレーション モード

外部レイヤ3機能は、次の例外を除き、両方のコンフィギュレーションモードでサポートされます。レイヤ 4 ～ レイヤ 7 サービス アプライアンスを使用したルート ピアリングおよびルート ヘルス インジェクション（RHI）は、指定されたモードでのみサポートされます。ルート ピアリングが関係するテナント VRF インスタンスのすべてのボーダー リーフ スイッチでは、名前付きモードを使用する必要があります。

暗黙モード CLI を使用して作成された L3Out は、GUI では読み取り専用になる

暗黙モードCLI手順を使用して作成されたレイヤ3外部ネットワーク オブジェクト（L3Outとも呼ばれる）は、「_ui_」で始まる名前で識別され、GUI で読み取り専用としてマークされます。

暗黙モード CLI を使用して作成された L3Out は、REST API を使用して変更された場合、CLI で変更できなくなる可能性がある

CLI は、インターフェイス、プロトコル、ルートマップ、EPG などの機能で、L3Out を分割します。REST API を使用して L3Out の構成を変更すると、この構造が壊れ、CLI を使用して L3Out を変更できなくなる可能性があります。

変更できない L3Out を削除するには、 *Cisco APIC Troubleshooting Guide* の「不要な _ui_ オブジェクトのトラブルシューティング」セクションを参照してください。

レイヤ 3 外部接続の設定のモードについて

APIC は設定のための複数のユーザ インターフェイス (UI) をサポートしているので、1 つの UI を使用して設定を作成し、その後、別の UI を使用して設定を変更する場合は、予期しないインタラクションが潜んでいます。ここでは、さらに他の APIC のユーザ インターフェイスを使用した可能性がある場合、APIC NX-OS スタイルの CLI を使用してレイヤ 3 外部接続を設定するための考慮事項を説明します。

APIC NX-OS スタイルの CLI を使用してレイヤ 3 外部接続を設定する場合、次の 2 つのモードを選択することができます。

- よりシンプルな暗黙 モードは、APIC GUI または REST API と互換性がありません。
- 名前付き（または明示) モードは、APIC GUI および REST API と互換性があります。

いずれの場合も、設定は互換性がない UI では読み取り専用であると考えてください。

モードの違いについて

どちらのモードでも、構成設定は API の **l3extOut** クラスのインスタンスである内部コンテナ オブジェクト「L3 Outside」（または「L3Out」）内で定義されます。2 つのモード間の主な違いは、このコンテナ オブジェクト インスタンスの命名にあります。

- 暗黙モード：コンテナのネーミングは潜在的であり、CLI コマンドには表示されません。CLI は、これらのオブジェクトを内部的に作成し保持します。
- 名前付きモード：名前はユーザーが決定します。名前付きモードの CLI コマンドには、追加の **l3Out** フィールドがあります。名前付き L3Out がを正常に設定され障害を回避するためには、ユーザーが外部レイヤ 3 用の API オブジェクト モデルを理解する必要があります。

（注） 「名前付きモードセクションを使用したレイヤ *3* 外部接続の設定」セクションの手順を除き、このガイドでは、暗黙モードの手順を説明します。

注意事項および制約事項

- 同じ APIC インターフェイスでは、両方のモードを、次の制限でレイヤ 3 外部接続を設定するために一緒に使用することができます。テナント VRF、およびリーフの特定の組み合わせのレイヤ 3 外部接続設定は、1 つのモードを介してのみ実行できます。

- 特定のテナント VRF の場合、外部 L3 EPG を配置できるポリシー ドメインは、名前付きモードまたは暗黙モードのいずれかになります。推奨する設定方式は、特定のテナント VRF が、レイヤ 3 外部接続用に展開されたすべてのノード全体で、特定のテナント VRF の組み合わせに対して 1 つのモードだけを使用することです。モードは、異なるテナントまたは異なる VRF 全体で変えることができ、制限は適用されません。
- 場合によっては、Cisco APIC クラスタへの着信設定で不整合が検証されます。外部から確認できる設定（L3Out を通過するノースバウンド トラフィック）も検証の対象です。設定が無効な場合は、「Invalid Configuration」エラー メッセージが表示されます。
- 外部レイヤ 3 機能は、次の例外を除いて、両方の設定モードでサポートされます
  - L4 ～ L7 サービス アプライアンスを使用したルーティング ピアリングとルート ヘルス インジェクション (RHI) は、名前付きモードでのみをサポートされます。名前付きモードは、ルーティング ピアリングが含まれるテナント VRF のすべての境界リーフ スイッチ全体で使用する必要があります。
- 暗黙モード CLI 手順を使用して作成されたレイヤ 3 外部ネットワーク オブジェクト（l3extOut）は、「__ui_」で始まる名前で識別され、GUI で読み取り専用としてマークされます。CLI は、インターフェイス、プロトコル、ルートマップ、EPG などの機能で、これらの外部 L3 ネットワークを分割します。REST API を介して実行される設定変更は、この構造を破棄することができ、CLI を介してさらなる変更を防ぐことができます。

このようなオブジェクトを削除する手順については、『*APIC Troubleshooting Guide*』の「*Troubleshooting Unwanted _ui_ Objects*」を参照してください。

コンフィギュレーションの検証

管理者が Cisco Application Policy Infrastructure Controller（APIC）で構成を入力すると、Cisco APIC はチェックを実行して、構成が有効であるかどうかを確認します。これは検証と呼ばれます。Cisco APIC が構成を受け入れても、その設定が既存の構成と競合する場合、Cisco APIC またはリーフ スイッチで障害が発生する可能性があります。構成を受け入れる前に Cisco APIC が実行するチェックの量は、リリースによって異なります。新しいリリースは、非同期的に障害が発生だけではなく、設定が受け入れられる前に、複数のチェックを実行する拡張されています。

これらの検証の目的を減らすか、設定を受け入れると、非同期的に障害を発生させるではなく設定時に、エラーのユーザを知らせるによって設定エラーを排除します。

また、Cisco APIC は、「アトミック」モードではなく「ベスト エフォート」モードで既存の構成をインポートするオプションも提供しています。このオプションは、無効な部分がある場合も、設定を承認する機能を提供します。Cisco APIC は、構成の有効な部分はプッシュし、検証と不整合な部分は無視します。不整合だった部分については、次のコマンドを実行すると、Cisco APIC はエラー メッセージを表示します。

show snapshot jobs *import_job*

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。