Cisco ACI/APIC の設定について

Cisco Application Policy Infrastructure Controller の推奨設定

Cisco Application Policy Infrastructure Controller (Cisco APIC) には、次の設定を推奨します。

表 *1 : Cisco APIC* への推奨設定

ナビゲーション パス	プロパティ	値	説明（**Description)**
[システム（System）] > [システム設定（System Settings）] > [ファブリック幅設定（Fabric Wide Setting）]	Enforce Subnet Check	ボックスをオンにします。	この機能は、Cisco Application Centric Infrastructure (Cisco 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、この機能はファブリック全体での設定ポリシーの下では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。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。このオプションをオンにすると、ファブリックは、ブリッジドメインで構成されたもの以外のサブネットからの IP アドレスを学習しなくなります。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。

ナビゲーション パス	プロパティ	値	説明（Description)
[System] > **[System Settings]** > **[Endpoint Controls]**	IP Aging Policy	有効	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。追跡は、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 用に設定されたエンドポイント保持ポリシーを使用して実行されます。IP アドレスから応答を受信しなかった場合、その IP アドレスの寿命は切れます。
[Fabric] > **[External Access Policies]** > **[Policies]** > **[Global]** > **[MCP Instance Policy default]**	Admin State	有効	これはミスケーブリング プロトコル (MCP) を有効にします。
	制御: VLAN 単位で MCP PDU を有効化にします。	ボックスをオンにします。	MCP は、LLDP や STP が発見できない、構成の誤りなどさまざまな問題によって引き起こされた、その他のタイプの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。

ACI/APIC インターフェイスについて

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）アーキテクチャ内での一元管理は、Application Policy Infrastructure Controller（APIC）と呼ばれています。このコントローラによって、すべての設定、管理、モニタリング、ヘルスの機能にアクセスできます。アプリケーションプログラミングインターフェイス（API）を備えた中央集中型コントローラを

使用すると、ファブリックを通じて設定またはアクセスされるすべての機能に次のインターフェイスを介してアクセスできます。

- APIC GUI

  APIC GUI は、REST API メッセージを交換することによって APIC エンジンと内部的に通信する 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。次の 2 つのモードがあります。

  - 以前のアドバンスト モード、現在はシンプルな APIC GUI：大規模な構成、導入環境、運用で使用します。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）などでの詳細なポリシー制御が可能で、大規模なファブリック構成および導入環境の自動化を実現します。

  - 以前の基本モード：リリース 3.1(x) まで導入されており、現在は削除されています。これは、一般的なワークフローを有効にするシンプルなインターフェイスで、GUI 動作モードによりオブジェクト モデルの最低限の知識で、管理者が簡単に ACI を開始できます。シンプル化された GUI を使用すると、高度なポリシーを設定しなくてもリーフ ポートとテナントの設定が可能です。

  APIC GUI の詳細については、『*Cisco APIC Getting Started Guide, Release 3.x*』および『*Cisco APIC* リリース *3.x* 基本設定ガイド』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、APIC の設定、導入、および運用に使用できます。この CLI は、ルートに EXEC モードを持つコマンドモードの階層にまとめられており、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が含まれます。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 を設定する NX-OS スタイル CLI と APIC GUI の両方を使用する際の重要な注意事項については、NX-OS Style CLI および APIC GUI の混合 （5 ページ） 参照してください。

  NX-OS スタイル CLI の詳細については、「*Cisco APIC NX-OS Style Command-Line Interface Configuration Guide*」を参照してください。

- APIC REST API：REST API は構成を許可するとともに、コントローラに管理機能へのアクセスを提供します。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、また、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。

  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。プログラミング言語を使用して、API メソッドまたは MO の説明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 Configuration Guide*』を参照してください。

NX-OS Style CLI および APIC GUI の混合

基本的なモードは、Cisco APIC リリース 3.0 (1) 以降推奨されません。そのリリースにおいて GUI は 1 つだけです。

⚠

注意 NX-OS スタイル CLI を使用して実行された設定は、APIC GUI に表示されます。これらを表示できますが、時折 GUI で編集できない可能性があります。APIC GUI で行われた変更は、NX-OS スタイル CLI で表示できる可能性がありますが、部分的にのみ動作する可能性があります。次の例を参照してください。

- APIC でインターフェイスごとの設定を行う際に、GUI と CLI を混在させないでください。GUI で行われた設定が、NX-OS CLI では部分的にしか機能しない可能性があります。

  たとえば、GUI の **[Tenants]** > ***[tenant-name]*** > **[Application Profiles]** > ***[application-profile-name]*** > **[Application EPGs]** > ***[EPG-name]*** > **[Static Ports]** > **[Deploy Static EPG on PC, VPC, or Interface]** でスイッチ ポートを設定したと仮定します。

  次に NX-OS スタイルの CLI で show running-config コマンドを使用すると、以下のような出力を受信します。

```
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 ドメインが事前に設定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。

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。

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

管理者がで設定を入力すると、 Cisco Application Policy Infrastructure Controller (Cisco APIC)、Cisco APIC チェックを実行して、設定が有効である、検証と呼ばれるはすることを確認します。設定は受け入れられますが、競合する他の以前の構成と Cisco APIC リーフ スイッチは、障害を発生させる可能性がありますか。によって実行されるチェックの量、 Cisco APIC の設定は、リリースによって異なります同意する前にします。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。

追加の検証に関して最も多くの変更が加えられたのは、Cisco APIC リリース 2.3 です。Cisco APIC リリース 3.0 では、VRF インスタンス レベルでの検証がさらに強化されています。例としてで Cisco APIC 2.3 のリリースでは、同じ:VRF インスタンスと同じ L3Out では、別の IP アドレスを持つ同じ SVI (encap) の複数のスイッチ仮想インターフェイス (SVI) 論理インターフェイス プロファイルを定義することができます。パス ノード 1 の IP アドレス 10.10.10.1/24 を定義したり、ポート 1/41、VLAN (encap) 10、およびパス ノード 1 の IP アドレス 10.10.10.2/24 ポート 1/43、VLAN 10 ([encap)。

この結果 SVI 10 の複数の IP アドレスを設定すると、によっては、どの IP アドレスは、ネクストホップとしてを使用ルーティングまたはIGP設定があるかどうかにかかわらずリーフ スイッチで使用されている IP アドレスを 1 つだけにするには、設定があります。正常に機能します。

始まる Cisco APIC リリース 3.0、上記の設定はありませんが受け入れられ、ために場合であっても、 Cisco Application Centric Infrastructure (Cisco ACI) オブジェクト モデル、SVI がパス (論理インターフェイス プロファイル) ごとに定義されている、特定のリーフ スイッチで特定の VRF インスタンスは、SVI の 1 つの IP アドレスを持つのみことができますセカンダリの IP アドレス可能性があります。他のいくつかの検証がで導入されたも Cisco APIC リリース 3.0。

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。

これらの改善の結果として、正しいではありませんが、2.3 のリリースでは、有効と見なされますが、設定をポストするかどうかこの POST は発生しません転記中の設定、および Cisco APIC エラーメッセージが返されます。

可能性がありますがすでにある Cisco APIC は正常に機能する前のバージョンを展開 Cisco APIC リリース 2.3 にもかかわらず、設定が有効なにしない可能性があります。2.3 リリースにアップ

グレードまたはそれ以降、した後でこのようなシナリオでは、ファームウェアのアップグレードの影響を軽減する、 Cisco APIC の既存の設定の検証を緩和できます。

Cisco APICまた、「原子」モードではなく、「ベスト エフォート」モードで既存設定をインポートするオプションを提供します。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設定の無効な部分をプッシュし、検証を一貫性のあるではない部分は無視されます。不整合の部分を Cisco APIC 問題を次のコマンドを使用するときに表示されているエラーメッセージ:

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。