

ACIアクセスポリシーのトラブルシューティング

内容

[概要](#)

[背景説明](#)

[アクセスポリシーの概要](#)

[アクセスポリシーの設定：方法論](#)

[アクセスポリシーの手動基本設定](#)

[スイッチポリシーの設定](#)

[インターフェイスポリシーの設定](#)

[VPCの設定](#)

[VLANプールの設定](#)

[ドメインの設定](#)

[Attachable Access Entity Profile\(AEP\)の設定](#)

[テナント、APP、およびEPGの設定](#)

[EPGスタティックバインディングの設定](#)

[アクセスポリシー設定の要約](#)

[追加サーバの接続](#)

[次のステップ](#)

[トラブルシューティングワークフロー](#)

[「インターフェイス、PC、およびVPCクイックスタートの設定」を使用したトラブルシューティング](#)

[トラブルシューティングのシナリオ](#)

[シナリオ 1：障害F0467:invalid-path、nwissues](#)

[シナリオ 2：EPGスタティックポートまたはL3Out論理インターフェイスプロファイル\(SVI\)に展開するパスとしてVPCを選択できない](#)

[シナリオ 3：障害F0467：別のEPGですでに使用されているファブリックカプセル化](#)

[特記事項](#)

[使用状況の表示](#)

[VLANプールの重複](#)

概要

このドキュメントでは、ACIアクセスポリシーの理解とトラブルシューティングの手順について説明します。

背景説明

このドキュメントの内容は、『[Troubleshooting Cisco Application Centric Infrastructure, Second Edition](#)』に記載されているアクセスポリシー – 概要とアクセスポリシー – トラブルシューティングワークフローの章から抜粋したものです。

アクセスポリシーの概要

ACI管理者は、ファブリック内のポートにVLANをどのように設定しますか。ACI管理者は、アクセスポリシーに関連する障害にどのように対処しますか。このセクションでは、ファブリックアクセスポリシーに関連する問題のトラブルシューティング方法について説明します。

トラブルシューティングのシナリオに入る前に、アクセスポリシーの機能とACIオブジェクトモデル内の関係について十分に理解しておくことが重要です。このため、Cisco.com(<https://developer.cisco.com/site/apic-mim-ref-api/>)で入手可能な「ACIポリシーモデル」と「APIC管理情報モデルリファレンス」の両方のドキュメントを参照できます。

アクセスポリシーの機能は、リーフスイッチのダウンリンクポートで特定の設定を有効にすることです。ACIファブリックポートを通過するトラフィックを許可するようにテナントポリシーを定義する前に、関連するアクセスポリシーを設定する必要があります。

通常、アクセスポリシーは、新しいリーフスイッチがファブリックに追加されたとき、またはデバイスがACIリーフダウンリンクに接続されたときに定義されます。ただし、環境の動的な性質によっては、ファブリックの通常の動作中にアクセスポリシーを変更できます。たとえば、VLANの新しいセットを許可したり、ファブリックアクセスポートに新しいルーテッドドメインを追加したりします。

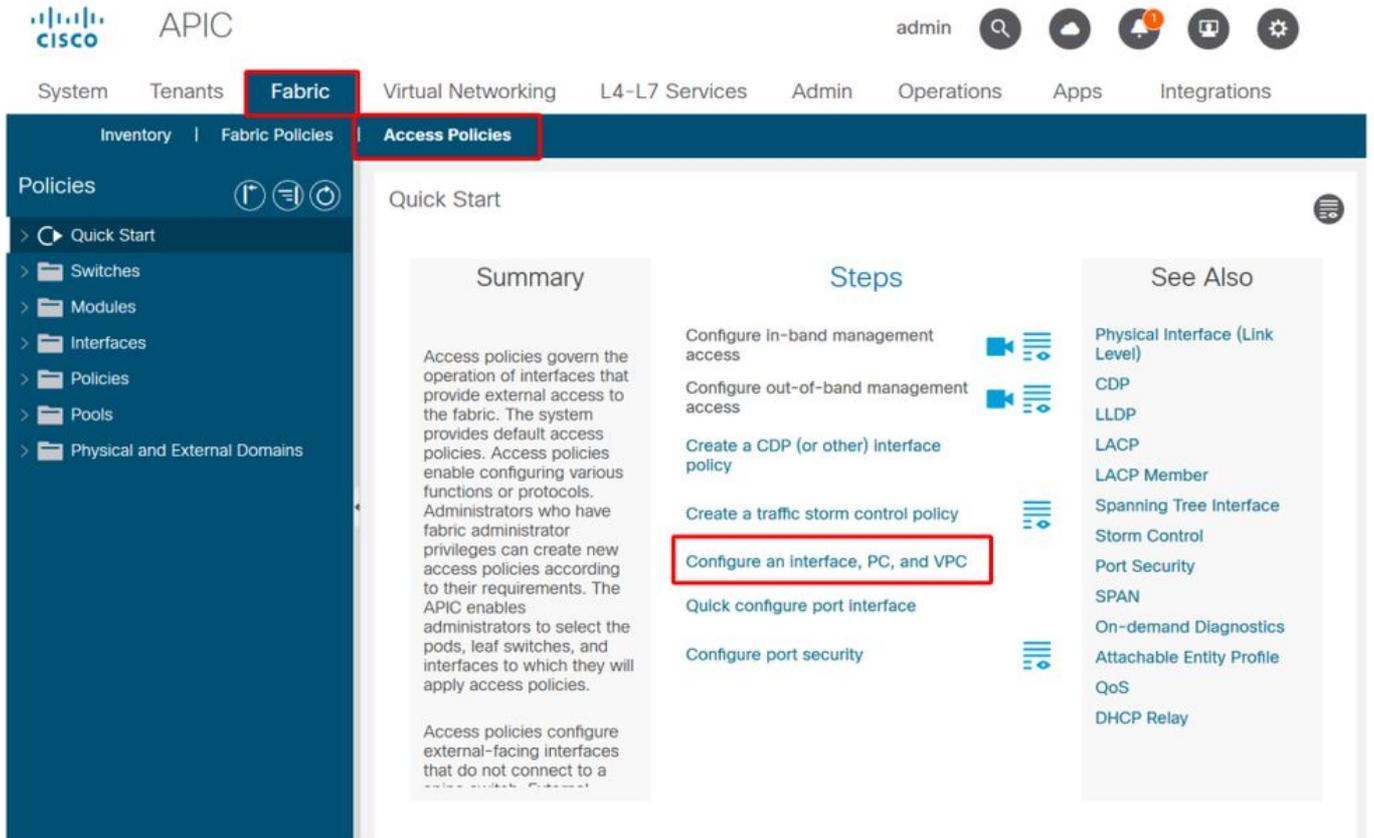
ACIアクセスポリシーは、当初は少し威圧的でしたが、非常に柔軟性が高く、継続的な進化において大規模なSDNネットワークへの設定のプロビジョニングを簡素化するように設計されています。

アクセスポリシーの設定：方法論

アクセスポリシーは個別に設定できます。つまり、必要なすべてのオブジェクトを個別に作成するか、ACI GUIで提供される多数のウィザードを使用して定義できます。

ウィザードは、ユーザーにワークフローをガイドし、必要なポリシーがすべて設定されていることを確認するため、非常に役立ちます。

アクセスポリシー – クイックスタートウィザード



上の図は、複数のウィザードが見つかるクイックスタートページを示しています。

アクセスポリシーを定義した後、一般的な推奨事項は、関連付けられたすべてのオブジェクトに障害が表示されないことを確認して、ポリシーを検証することです。

たとえば、次の図では、スイッチプロファイルによって、存在しないインターフェイスセクタポリシーが割り当てられています。注意深いユーザは、オブジェクトの「missing-target」状態を簡単に特定し、GUIから障害のフラグが設定されたことを確認できます。

リーフプロファイル : SwitchProfile_101

The screenshot shows the Cisco APIC interface for configuring a Leaf Profile. The main view is titled "Leaf Profile - SwitchProfile_101". On the left, a navigation pane shows the hierarchy: Policies > Profiles > SwitchProfile_101. The main content area has tabs for "Policy", "Faults", and "History". Under the "Policy" tab, there are two tables:

- Leaf Selectors:** A table with columns "Name", "Blocks", and "Policy Group". It contains one entry: "101" under "Name" and "101" under "Blocks".
- Associated Interface Selector Profiles:** A table with columns "Name", "Description", and "State". It contains two entries:

Name	Description	State
Policy		missing-target
SwitchProfile_101		formed

 The "missing-target" state is highlighted with a red box.

At the bottom right, there are buttons for "Show Usage", "Reset", and "Submit".

リーフプロファイル - SwitchProfile_101 - エラー

The screenshot shows the "Fault Properties" dialog box in the Cisco APIC interface. The dialog has tabs for "General", "Troubleshooting", and "History". The "General" tab is active, displaying the following information:

- Fault Code:** F1014
- Severity:** warning
- Last Transition:** 2019-10-28T11:23:11.665+00:00
- Lifecycle:** Raised
- Affected Object:** uni/infra/nprof-SwitchProfile_101/rsaccPortP-[uni/infra/accportprof-Policy]
- Description:** Failed to form relation to MO uni/infra/accportprof-Policy of class infraAccPortP
- Type:** Config
- Cause:** resolution-failed
- Change Set:** state (Old: formed, New: missing-target)
- Created:** 2019-10-28T11:23:11.665+00:00
- Code:** F1014
- Number of Occurrences:** 1
- Original Severity:** warning
- Previous Severity:** warning
- Highest Severity:** warning

At the bottom of the dialog, there is a pagination bar showing "Page 1 Of 1", "Objects Per Page: 15", and "Displaying Objects 1 - 1 Of 1".

この場合、障害の修正は、「Policy」という名前の新しいインターフェイスセクタプロファイルを作成するのと同じくらい簡単です。

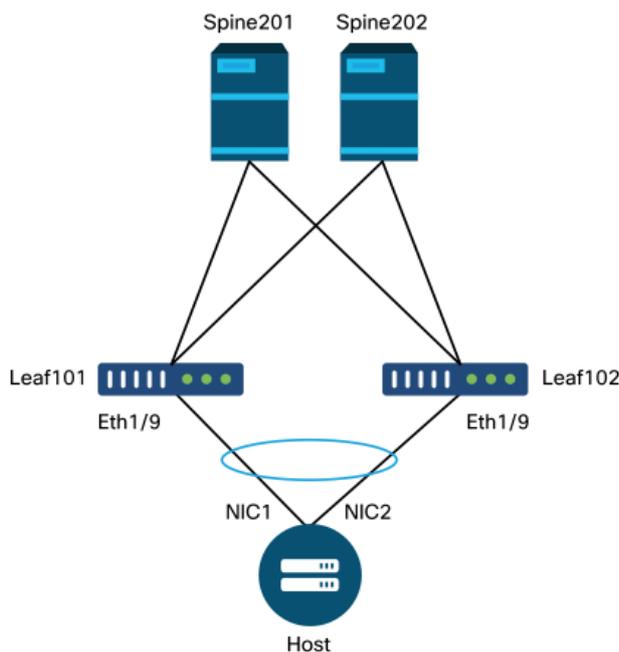
基本的なアクセスポリシーの手動設定については、以降の段落で説明します。

アクセスポリシーの手動基本設定

アクセスポリシーを導入する際、オブジェクトは特定のダウンリンクの使用目的を表すように定義されます。ダウンリンクをプログラムする宣言（EPG静的ポート割り当てなど）は、この表明された意図に依存します。これにより、構成を拡張し、特定の外部デバイスに特に接続されているスイッチやポートなど、同様の使用オブジェクトを論理的にグループ化できます。

この章の残りの部分については、次のトポロジを参照してください。

デュアルホームサーバのアクセスポリシー定義のトポロジ

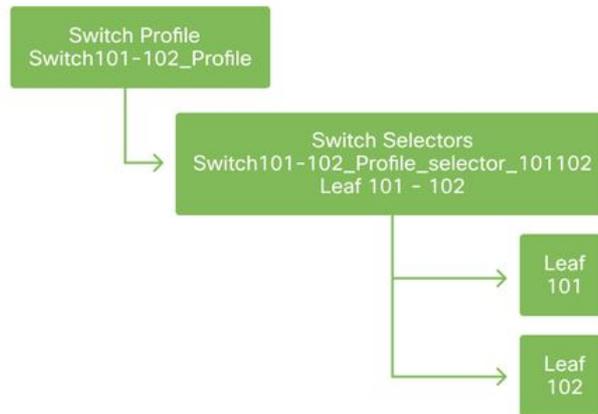


WebサーバはACIファブリックに接続されます。Webサーバには、LACPポートチャネルで設定された2つのネットワークインターフェイスカード(NIC)があります。Webサーバは、リーフスイッチ101および102のポート1/9に接続されています。WebサーバはVLAN-1501に依存し、EPG「EPG-Web」に存在する必要があります。

スイッチポリシーの設定

最初の論理的なステップは、どのリーフスイッチを使用するかを定義することです。「スイッチプロファイル」には、使用するリーフノードIDを定義する「スイッチセレクタ」が含まれます。

スイッチポリシー



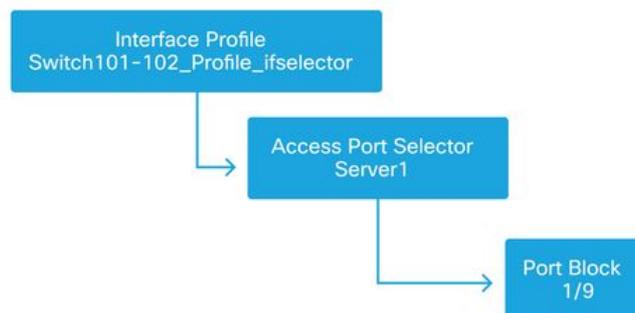
一般的な推奨事項としては、プロファイルの一部であるノードを示す命名方式を使用して、個々のリーフスイッチごとに1つのスイッチプロファイル、およびVPCドメインペアごとに1つのスイッチプロファイルを設定します。

クイックスタートでは、論理的な名前付けスキームを導入して、適用場所を簡単に理解できるようにします。完成した名前は、「Switch<node-id>_Profile」形式に従います。たとえば、「Switch101_Profile」はリーフノード101を含むスイッチプロファイル用に、「Switch101-102_Profile」はVPCドメインの一部であるリーフノード101および102を含むスイッチプロファイル用に設定します。

インターフェイスポリシーの設定

スイッチアクセスポリシーが作成されたら、インターフェイスを定義することが次の論理的なステップになります。これを行うには、「Port Block」定義を含む1つ以上の「Access Port Selectors」で構成される「Interface Profile」を作成します。

インターフェイスポリシー



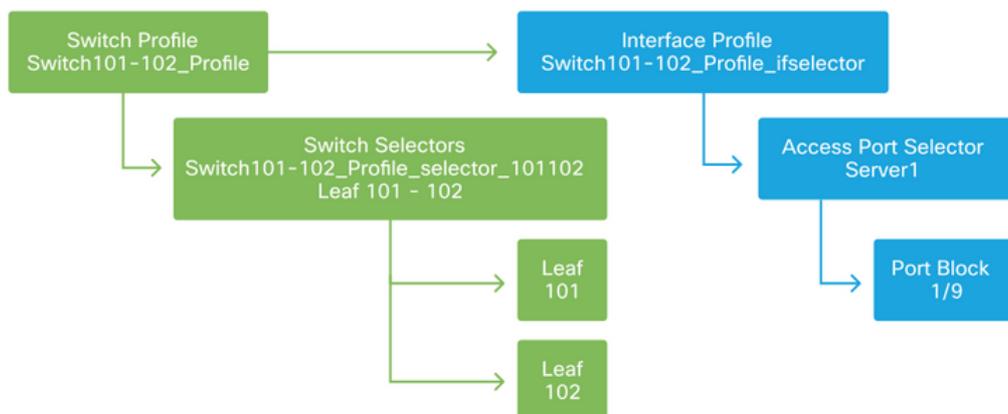
「Interface Profile」と関連するスイッチの関係を形成するには、「Switch Profile」を「Interface Profile」にリンクします。

「インターフェイスプロファイル」はさまざまな方法で定義できます。「スイッチプロファイル」と同様に、物理スイッチごとに1つの「インターフェイスプロファイル」を作成し、VPCドメインごとに「インターフェイスプロファイル」を作成できます。これらのポリシーには、対応するスイッチプロファイルへの1対1のマッピングが必要です。このロジックに従うと、ファブリックアクセスポリシーが大幅に簡素化され、他のユーザが理解しやすくなります。

ここでは、クイックスタートで使用される既定の名前付けスキームも使用できます。インターフェイスの選択にこのプロファイルが使用されることを示すには、「<switch profile

name>_ifselector」の形式に従います。たとえば、「Switch101_Profile_ifselector」のようになります。この例の「Interface Profile」は、リーフスイッチ101に非VPCインターフェイスを設定するために使用され、「Switch101_Profile」アクセスポリシーにのみ関連付けられます。

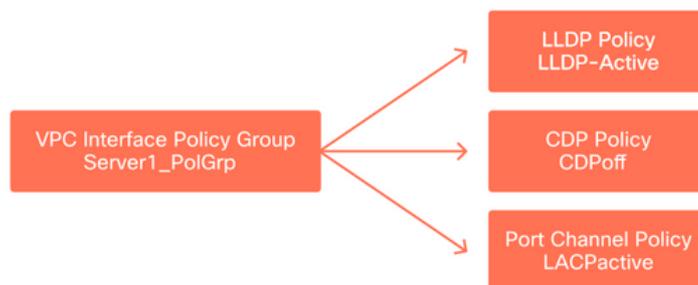
インターフェイスプロファイルに関連付けられたスイッチプロファイル



Eth 1/9を持つ「Interface Profile」は、リーフスイッチ101と102の両方を含む「Switch Profile」に接続されているため、両方のノードでのEth1/9のプロビジョニングが同時に開始されます。

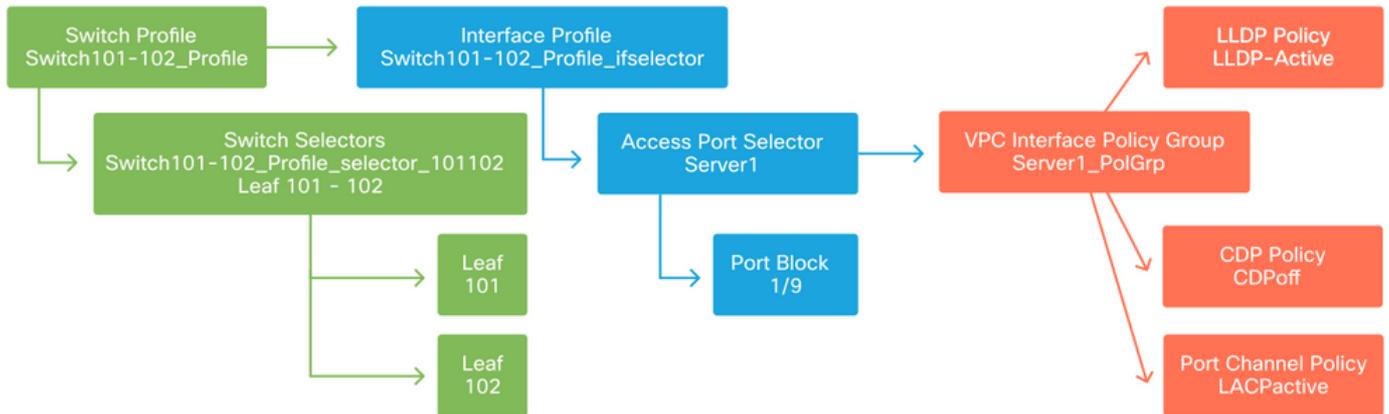
この時点で、リーフスイッチとそのポートが定義されています。次の論理的なステップは、これらのポートの特性を定義することです。「インターフェイスポリシーグループ」では、これらのポートプロパティを定義できます。上記のLACPポートチャネルを許可するために、「VPCインターフェイスポリシーグループ」が作成されます。

ポリシーグループ



「VPCインターフェイスポリシーグループ」は、「アクセスポートセレクタ」から「インターフェイスポリシーグループ」に関連付けられ、リーフスイッチ/インターフェイスからポートプロパティへの関係を形成します。

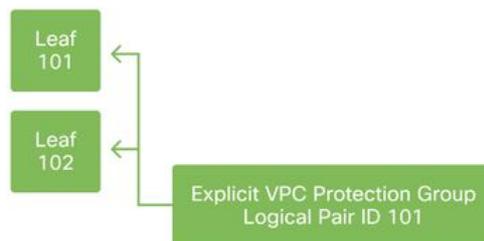
スイッチとインターフェイスのプロファイルの結合



VPCの設定

2つのリーフスイッチ上にLACPポートチャネルを作成するには、リーフスイッチ101と102の間にVPCドメインを定義する必要があります。これを行うには、2つのリーフスイッチ間に「VPC保護グループ」を定義します。

VPC



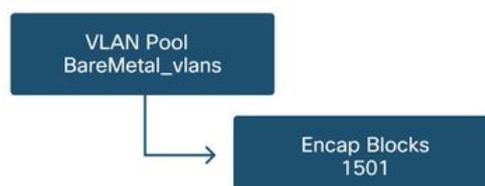
VLANプールの設定

次の論理的な手順は、このポートで使用されるVLAN（この場合はVLAN-1501）を作成することです。「Encap Blocks」を使用した「VLANプール」の定義により、この設定が完了します。

VLANプール範囲のサイズを検討する際には、ほとんどの展開で必要なVLANプールは1つと、VMM統合を使用する場合は1つだけであることを注意してください。レガシーネットワークからACIにVLANを持ち込むには、レガシーVLANの範囲をスタティックVLANプールとして定義します。

たとえば、VLAN 1 ~ 2000がレガシー環境で使用されていると仮定します。VLAN 1 ~ 2000を含むスタティックVLANプールを1つ作成します。これにより、ACIブリッジドメインとEPGをレガシーファブリックにトランキングできます。VMMを展開する場合、空きVLAN IDの範囲を使用して2つ目のダイナミックプールを作成できます。

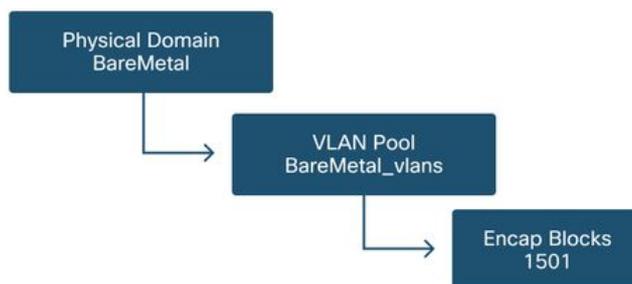
VLANプール



ドメインの設定

次の論理的なステップは、「ドメイン」を作成することです。「ドメイン」は、VLANプールの範囲、つまりプールが適用される場所を定義します。「ドメイン」には、物理、仮想、または外部（ブリッジまたはルーティング）があります。この例では、「物理ドメイン」を使用して、ベアメタルサーバをファブリックに接続します。この「ドメイン」は、必要なVLANを許可するために「VLANプール」に関連付けられます。

物理ドメイン



ほとんどの導入では、ベアメタル導入には1つの「物理ドメイン」で十分で、L3Out導入には1つの「ルーテッドドメイン」で十分です。両方を同じ「VLANプール」にマッピングできます。ファブリックがマルチテナント方式で導入されている場合、または特定のEPGおよびVLANをポートに導入できるユーザを制限するためにより細かい制御が必要な場合は、より戦略的なアクセスポリシー設計を検討する必要があります。

[ドメイン(Domains)]には、ロールベースアクセスコントロール(RBAC)を使用して、[セキュリティドメイン(Security Domains)]を使用してポリシーへのユーザアクセスを制限する機能もあります。

スイッチにVLANを展開する場合、ACIはVLANの取得元のドメインに基づく一意のVXLAN IDでスパニングツリーBPDUをカプセル化します。このため、他のブリッジとのSTP通信を必要とするデバイスを接続するときは、常に同じドメインを使用することが重要です。

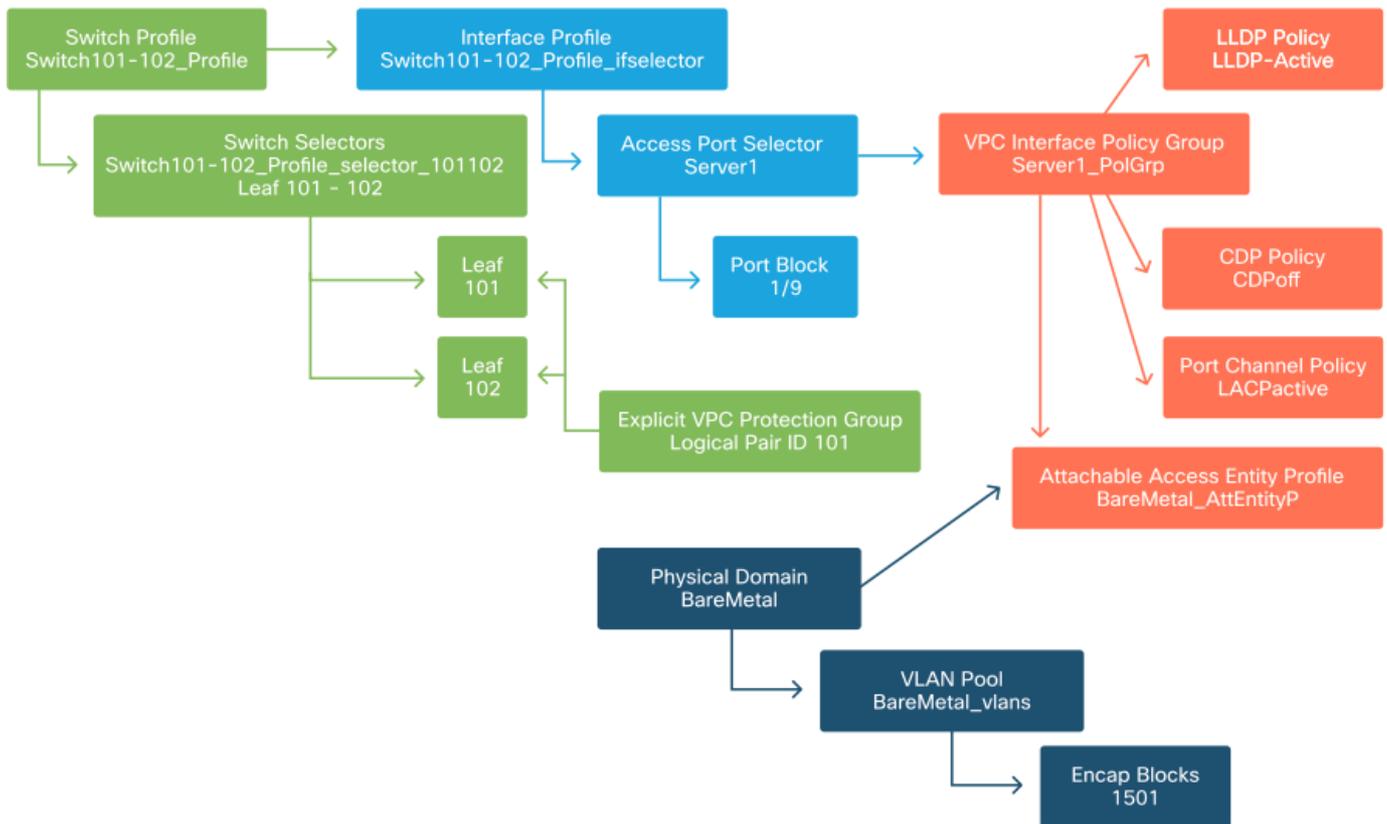
VLAN VXLAN IDは、VPCスイッチがVPCによって学習されたMACアドレスとIPアドレスを同期するためにも使用されます。このため、VLANプールの最も簡単な設計は、静的な展開に単一のプールを使用し、動的な展開に2番目のプールを作成することです。

Attachable Access Entity Profile(AEP)の設定

アクセスポリシー設定の2つの主要なチャンクが完了しました。スイッチとインターフェイスの定義、およびドメインとVLANの定義です。「Attachable Access Entity Profile」(AEP)というオブジェクトは、これら2つのチャンクを結び付けるのに役立ちます。

「ポリシーグループ」は、1対多の関係でAEPにリンクされます。これにより、AEPは同様のポリシー要件を共有するインターフェイスとスイッチをグループ化できます。つまり、特定のスイッチ上のインターフェイスグループを表すとき、参照する必要があるAEPは1つだけです。

アタッチ可能なアクセスエンティティプロファイル



ほとんどの展開では、スタティックパスに1つのAEPを使用し、VMMドメインごとに1つの追加AEPを使用する必要があります。

最も重要な考慮事項は、AEPを介してVLANをインターフェイスに展開できることです。これを行うには、EPGをAEPに直接マッピングするか、事前プロビジョニング用にVMMドメインを構成します。これらの設定はどちらも、関連付けられたインターフェイスをトランクポートにします（レガシースイッチでは「switchport mode trunk」）。

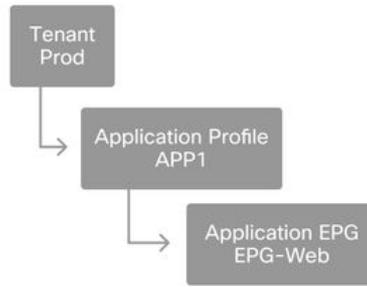
このため、ルーテッドポートまたはルーテッドサブインターフェイスを使用する場合は、L3Out用に別のAEPを作成することが重要です。L3OutでSVIを使用する場合、追加のAEPを作成する必要はありません。

テナント、APP、およびEPGの設定

ACIは、ポリシーベースのアプローチを使用して接続を定義する別の方法を使用します。

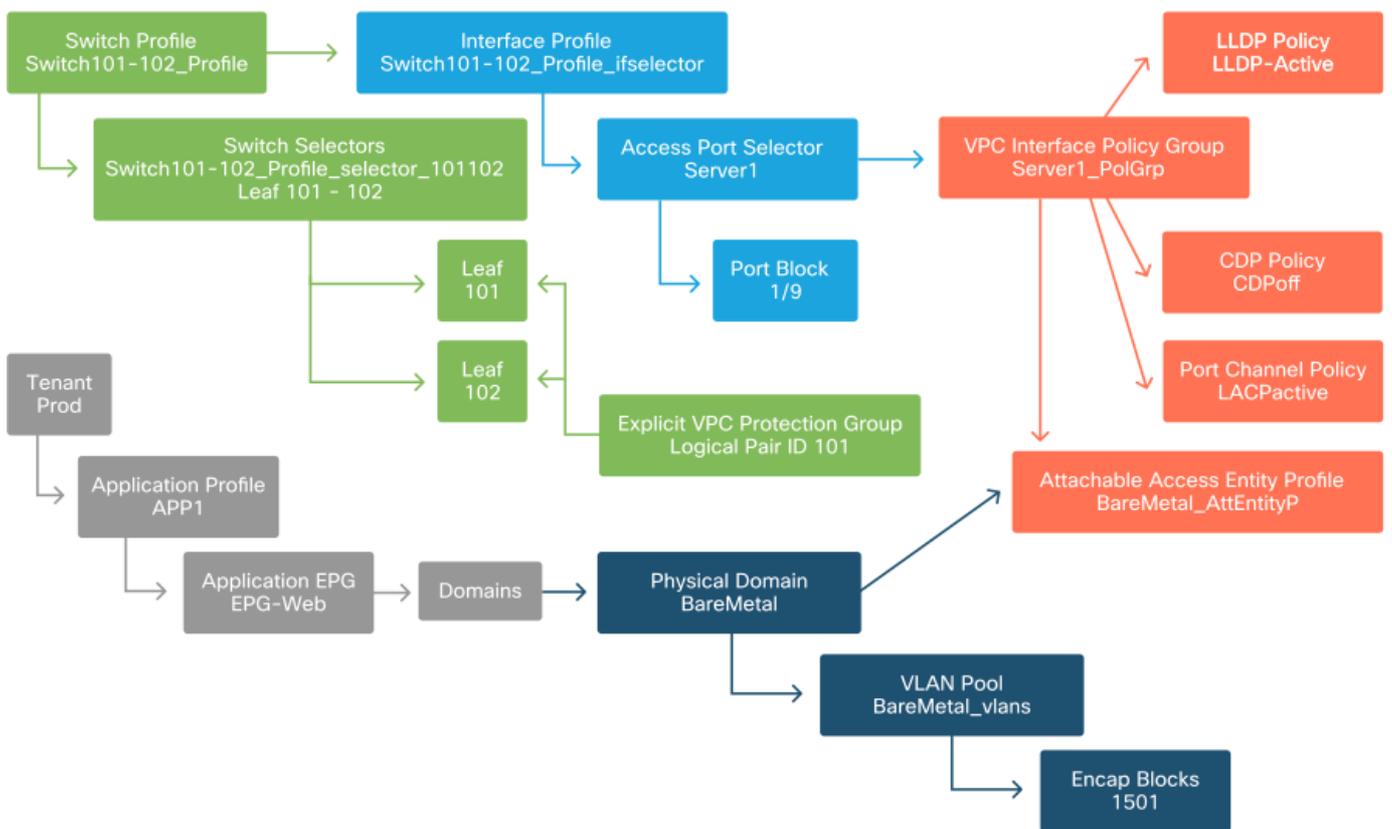
最下位レベルのオブジェクトは、「エンドポイントグループ」(EPG)と呼ばれます。EPG構成は、同様のポリシー要件を持つVMまたはサーバ（エンドポイント）のグループを定義するために使用されます。テナントの下にある「アプリケーションプロファイル」は、EPGを論理的にグループ化するために使用されます。

テナント、APP、EPG



次の論理的なステップは、EPGをドメインにリンクすることです。これにより、作業負荷を表す論理オブジェクト、EPG、および物理スイッチ/インターフェイス、アクセスポリシー間のリンクが作成されます。

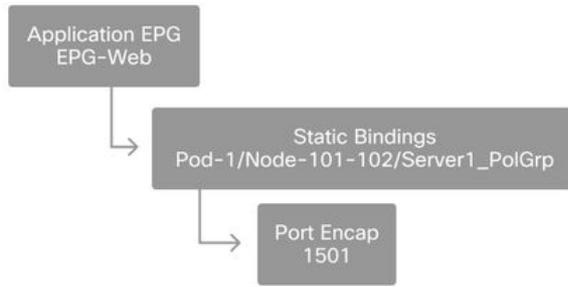
EPGからドメインリンク



EPGスタティックバインディングの設定

最後の論理的なステップは、VLANを特定のEPGのスイッチインターフェイスにプログラムすることです。物理ドメインを使用する場合、このタイプのドメインは明示的な宣言を必要とするため、これは特に重要です。これにより、EPGをファブリックから拡張でき、ベアメタルサーバをEPGに分類できます。

静的バインディング

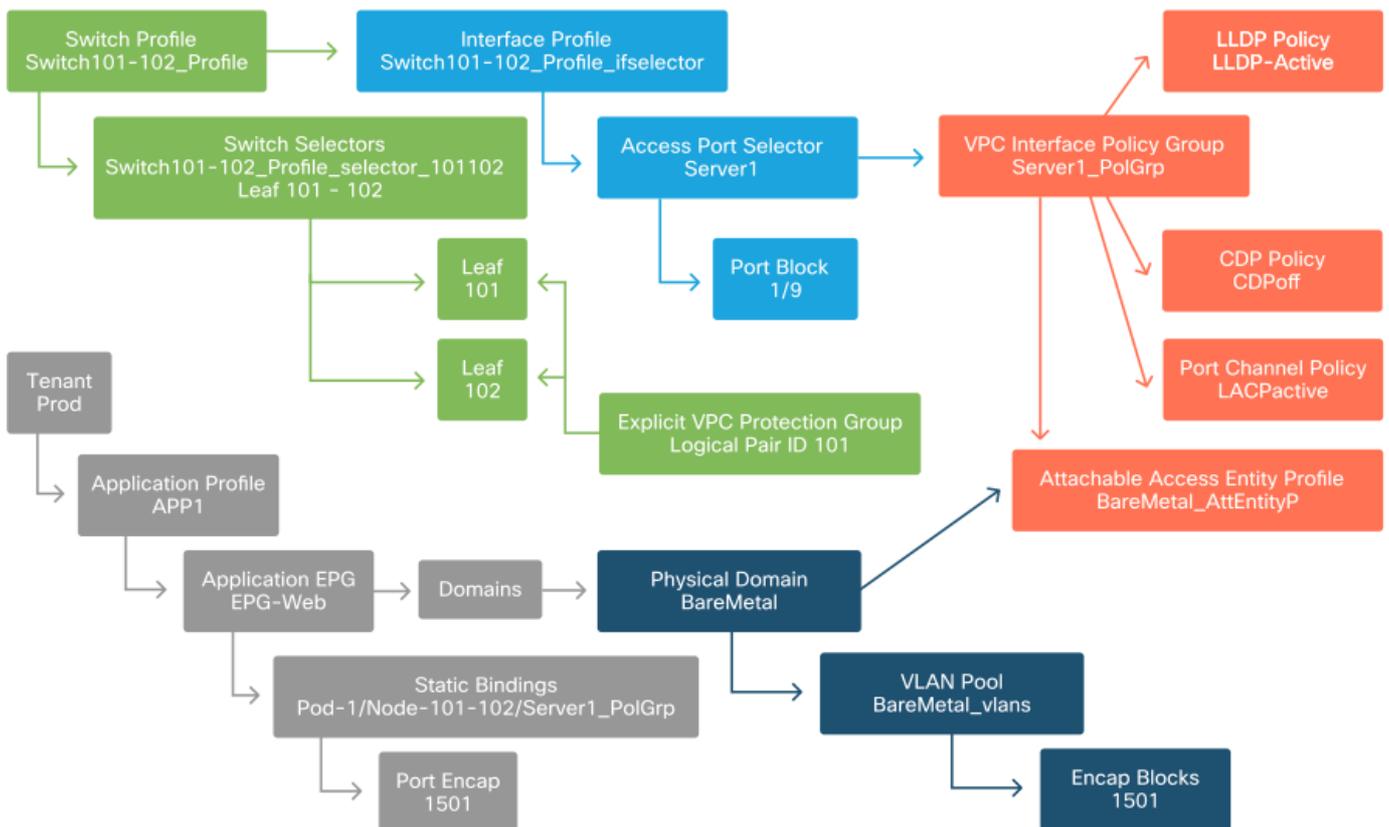


参照される「ポートカプセル化」は、「VLANプール」に対して解決可能である必要があります。そうでない場合、障害にフラグが付けられます。これについては、この章の「トラブルシューティングワークフロー」セクションで説明します。

アクセスポリシー設定の要約

次の図は、リーフスイッチ101および102へのVPC接続を使用してVLAN-1501経由でホストに接続できるようにするために作成されたすべてのオブジェクトを示しています。

ベアメタルACI接続



追加サーバの接続

以前のすべてのポリシーが作成された状態で、リーフスイッチ101および102のポートEth1/10上の1台のサーバをポートチャンネルで接続するとどうなりますか。

「ベアメタルACI接続」の図を参照して、最低限次のものを作成する必要があります。

- 追加のアクセスポートセレクタとポートブロック。

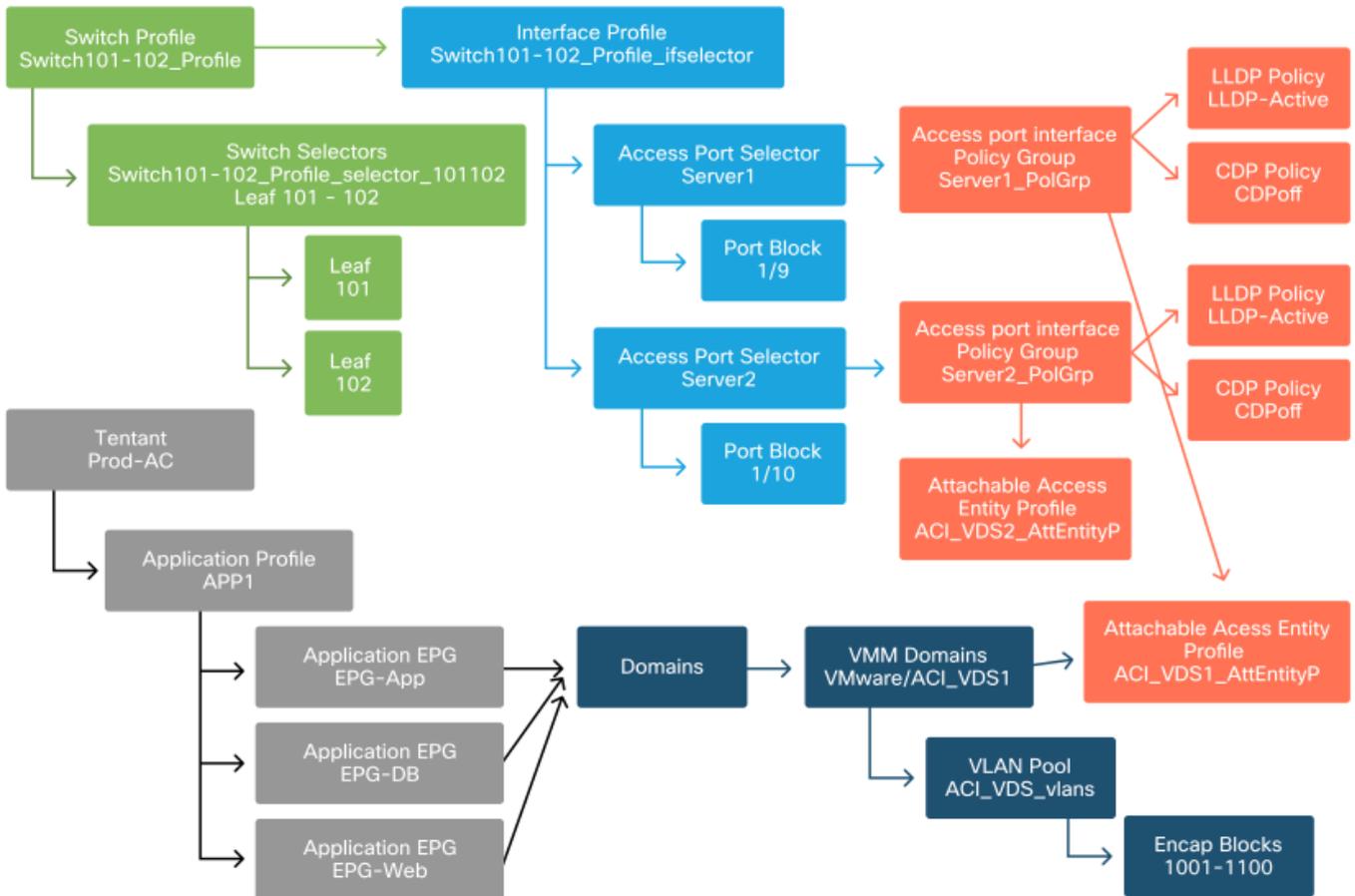
- 追加のVPCインターフェイスポリシーグループ。
- ポートカプセルによる追加のスタティックバインディング。

LACPポートチャネルの場合は、専用のVPCインターフェイスポリシーグループを使用する必要があります。これは、このVPCポリシーグループがVPC IDを定義するためです。

個々のリンクの場合、リンクに同じポートプロパティが必要な場合は、非VPCインターフェイスポリシーグループを余分なサーバに再利用できます。

ポリシーは次の図のようになります。

セットアップにserver2を接続しています



次のステップ

次のセクションでは、この概要で説明したトポロジと使用例から始めて、いくつかのアクセスポリシーの障害シナリオを説明します。

トラブルシューティングワークフロー

アクセスポリシーを操作する際に、次のトラブルシューティングシナリオが発生する可能性があります。

- AEPにリンクされていないアクセスポリシーグループなど、アクセスポリシー内の2つ以上のエンティティ間の関係が欠落している。
- 欠落したポリシーや予期しないポリシーは、「lldp_enabled」という名前のLLDPポリシーな

どの特定のアクセスポリシーに関連付けられますが、実際にはポリシー設定でLLDP rx/txが無効になっています。

- 設定されたVLAN IDのカプセル化が設定されたVLANプールから欠落しているなど、アクセスポリシー内で欠落している、または予期しない値。
- EPGとアクセスポリシー間の関係が欠落している（EPGへの物理または仮想ドメインの関連付けがないなど）。

上記のトラブルシューティングの大部分では、アクセスポリシーの関係を調べて、関係が欠落しているかどうかを理解したり、設定されているポリシーを理解したり、設定によって望ましい動作が引き起こされるかどうかを理解します。

「インターフェイス、PC、およびVPCクイックスタートの設定」を使用したトラブルシューティング

APIC GUIでは、[Configure Interface, PC, and VPC]クイックスタートウィザードを使用して、既存のアクセスポリシーを集約したビューを管理者に提供し、アクセスポリシーの検索を容易にします。このクイックスタートウィザードは、次のGUIで参照できます。

[Fabric] > [Access Policies] > [Quick Start] > [Steps] > [Configure Interface, PC, and VPC]

「インターフェイス、PC、およびVPCの設定」クイックスタートの場所

The screenshot displays the APIC GUI interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'L4-L7 Services', 'Admin', 'Operations', 'Apps', and 'Integrations'. The 'Fabric' tab is selected, and the 'Access Policies' sub-tab is active. The left sidebar shows a tree view with 'Policies' expanded, and 'Quick Start' is highlighted. The main content area is titled 'Quick Start' and is divided into three sections: 'Summary', 'Steps', and 'See Also'. The 'Steps' section lists several configuration tasks, with 'Configure an Interface, PC, and VPC' highlighted by a red box. The 'See Also' section lists related configuration topics such as 'Physical Interface (Link Level)', 'CDP', 'LLDP', 'LACP', 'LACP Member', 'Spanning Tree Interface', 'Storm Control', 'Port Security', 'SPAN', 'On-demand Diagnostics', 'Attachable Entity Profile', 'QoS', and 'DHCP Relay'.

ウィザードの名前に「Configure」が含まれていても、インターフェイスをプログラムするために設定する必要がある多くのアクセスポリシーを集約して表示するには非常に便利です。この集約は、どのポリシーがすでに定義されているかを把握するための単一のビューとして機能し、アクセスポリシー関連の問題を切り分けるために必要なクリック数を効果的に削減します。

[Quick Start]ビューがロードされると、[Configured Switch Interfaces]ビュー（左上のペイン）を参照して、既存のアクセスポリシーを確認できます。ウィザードでは、アクセスポリシーの設定

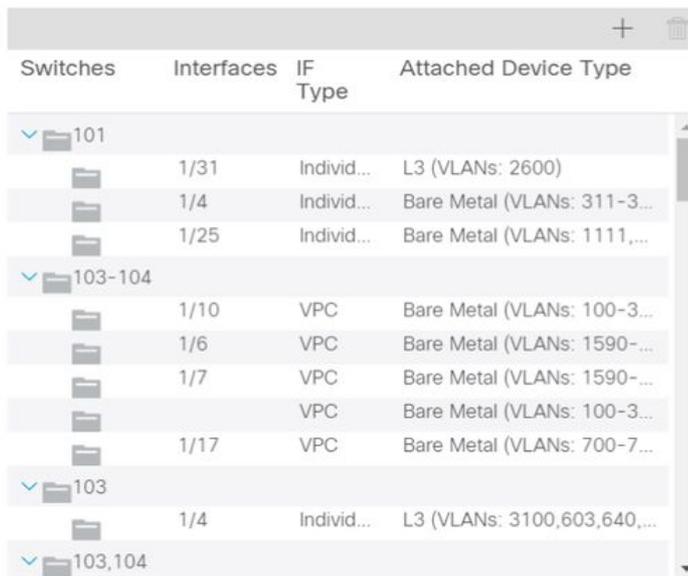
に応じて、個々のリーフスイッチまたは複数のリーフスイッチを表すフォルダの下にエントリがグループ化されます。

ウィザードの価値を示すために、次のウィザードのスクリーンショットが表示されます。これは、読者がファブリックトポロジについて以前に理解していないためです。

「インターフェイス、PC、およびVPCの設定」クイックスタートのデモビュー

Configure Interface, PC, and VPC

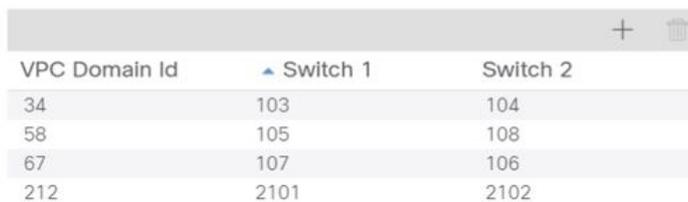
Configured Switch Interfaces



Switches	Interfaces	IF Type	Attached Device Type
101	1/31	Individ...	L3 (VLANs: 2600)
	1/4	Individ...	Bare Metal (VLANs: 311-3...)
	1/25	Individ...	Bare Metal (VLANs: 1111,...)
103-104	1/10	VPC	Bare Metal (VLANs: 100-3...)
	1/6	VPC	Bare Metal (VLANs: 1590-...)
	1/7	VPC	Bare Metal (VLANs: 1590-...)
		VPC	Bare Metal (VLANs: 100-3...)
	1/17	VPC	Bare Metal (VLANs: 700-7...)
103	1/4	Individ...	L3 (VLANs: 3100,603,640,...)
103,104			



VPC Switch Pairs



VPC Domain Id	Switch 1	Switch 2
34	103	104
58	105	108
67	107	106
212	2101	2102

[Configured Switch Interfaces]ペインにアクセスポリシーマッピングが表示されます。[VPCスイッチペア(VPC Switch Pairs)]ペインに、完成したVPC保護グループ定義が表示されます。

次の表に、上のスクリーンショットから取得できる、完成したアクセスポリシー定義のサブセットを示します。

上記のクイックスタートビューから取得できる、完了したアクセスポリシーのサブセット

スイッチノード	インターフェイス	ポリシーグループタイプ	ドメインタイプ	VLAN
101	1/31	個別	ルーテッド(L3)	2600
101	1/4	個別	物理 (ベアメタル)	311-3..?
103-104	1/10	VPC	物理 (ベアメタル)	100-3..?

デフォルトのビューでは、VLAN列のエントリは意図的に不完全です。

同様に、完成した「VPC保護グループ」ポリシーは、「VPCスイッチペア」ビュー（左下のペイン）から取得できます。「VPC保護グループ」がないと、VPCを導入できません。これは、2つのリーフノード間でVPCドメインを定義するポリシーです。

ペインのサイズ設定により、長いエントリが完全には表示されないことを考慮してください。エントリの値をすべて表示するには、目的のフィールドにマウスポインタを合わせます。

マウスポインタが103-104、int 1/10 VPCエントリの[Attached Device Type]フィールドの上に置かれています。

Configure Interface, PC, and VPC

Configured Switch Interfaces

Switches	Interfaces	IF Type	Attached Device Type
101	1/31	Individ...	L3 (VLANs: 2600)
101	1/4	Individ...	Bare Metal (VLANs: 311-3...
101	1/25	Individ...	Bare Metal (VLANs: 1111,...
103-104	1/10	VPC	Bare Metal (VLANs: 100-3...
103-104	1/6	VPC	Bare Metal (VLANs: 1590-
103-104	1/7	VPC	Bare Metal (VLANs: 1590-
103-104		VPC	Bare Metal (VLANs: 100-3...
103-104	1/17	VPC	Bare Metal (VLANs: 700-7...
103	1/4	Individ...	L3 (VLANs: 3100,603,640,...
103,104			



Bare Metal (VLANs: 100-300,900-999), L3 (VLANs: 100-300,900-999)

VPC Switch Pairs

VPC Domain Id	Switch 1	Switch 2
34	103	104
58	105	108
67	107	106
212	2101	2102

ペインの上にマウスを置くと、すべてのエントリが表示されます。

マウスオーバーの詳細を使用して、完了したアクセスポリシーのサブセットを更新

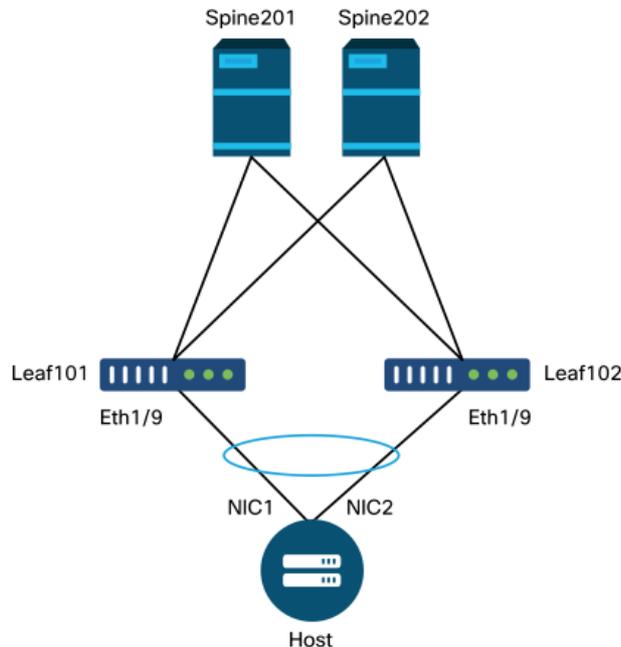
スイッチノード	インターフェイス	ポリシーグループタイプ	ドメインタイプ	VLAN
101	1/31	個別	ルーテッド(L3)	2600
101	1/4	個別	物理 (ベアメタル)	311-320
103-104	1/10	VPC	物理 (ベアメタル)	100-300,900-999
103-104	1/10	VPC	ルーテッド(L3)	100-300,900-999

VLANの完全な関連付けを確認し、理解して、トラブルシューティングと検証を行うことができます。

トラブルシューティングのシナリオ

次のトラブルシューティングシナリオについては、前の章と同じトポロジを参照してください。

アクセスポリシーの[Introduction]セクションからのトポロジ



シナリオ 1 : 障害F0467:invalid-path、nwissues

この障害は、設定を適切に適用するために、対応するアクセスポリシーが設定されていない状態でスイッチ/ポート/VLANが宣言されると発生します。この障害の説明によっては、アクセスポリシー関係の別の要素が欠落している場合があります。

トランキングされたカプセル化VLAN 1501を使用して、対応するアクセスポリシー関係を確認せずに上記のVPCインターフェイスのスタティックバインディングを展開すると、EPGで次のエラーが発生します。

障害:F0467

説明 : 障害委任 : uni/tn-Prod1/ap-App1/epg-EPG-Webノード101 101_102_eth1_9の設定が失敗しました。原因は無効なパス設定、無効なVLAN設定、デバッグメッセージです。invalid-vlan:vlan-1501:STPセグメントIDがカプセル化に存在しません。EPGがドメインに関連付けられていないか、ドメインにこのVLANが割り当てられていません。invalid-path:vlan-1501:EPGとポートの両方に関連付けられた、必要なVLANを持つドメインはありません。

上記の障害の説明から、障害がトリガーされる原因に関する明確な兆候がいくつかあります。アクセスポリシーの関係を確認し、EPGへのドメインの関連付けを確認する警告があります。

上記のシナリオのクイックスタートビューを確認すると、アクセスポリシーにVLANがないことは明らかです。

101-102、Int 1/9 VPCにVLANがない場合のクイックスタートビュー

Configure Interface, PC, and VPC

Configured Switch Interfaces

Switches	Interfaces	IF Type	Attached Device Type
101-102	1/11	Individual	ESX (VLANs: 1001-1100)
101-102	1/9	VPC	Bare Metal
101	1/17	Individual	L3 (VLANs: 901-910)
102	1/19	Individual	L3 (VLANs: 901-910)
301-302	1/11	Individual	ESX (VLANs: 1001-1100)
301	1/17	Individual	L3 (VLANs: 901-910)
302	1/19	Individual	L3 (VLANs: 901-910)



Click '+' to select switches or click table row to edit



VPC Switch Pairs

VPC Domain Id	Switch 1	Switch 2
101	101	102

エントリにVLAN IDへの参照がないことに注意してください。

修正すると、クイックスタートビューに「(VLAN 1500-1510)」と表示されます。

101-102、Int 1/9 VPCにペアメタル(VLAN:1500-1510)

Configure Interface, PC, and VPC

Configured Switch Interfaces

Switches	Interfaces	IF Type	Attached Device Type
101-1...			
	1/11	Individual	ESX (VLANs: 1001-1100)
	1/9	VPC	Bare Metal (VLANs: 1500...
101			Bare Metal (VLANs: 1500-1510)
	1/17	Individual	L3 (VLANs: 901-910)
102			
	1/19	Individual	L3 (VLANs: 901-910)
301-3...			
	1/11	Individual	ESX (VLANs: 1001-1100)
301			
	1/17	Individual	L3 (VLANs: 901-910)
302			
	1/19	Individual	L3 (VLANs: 901-910)



Click '+' to select switches or click table row to edit



VPC Switch Pairs

VPC Domain Id	Switch 1	Switch 2
101	101	102

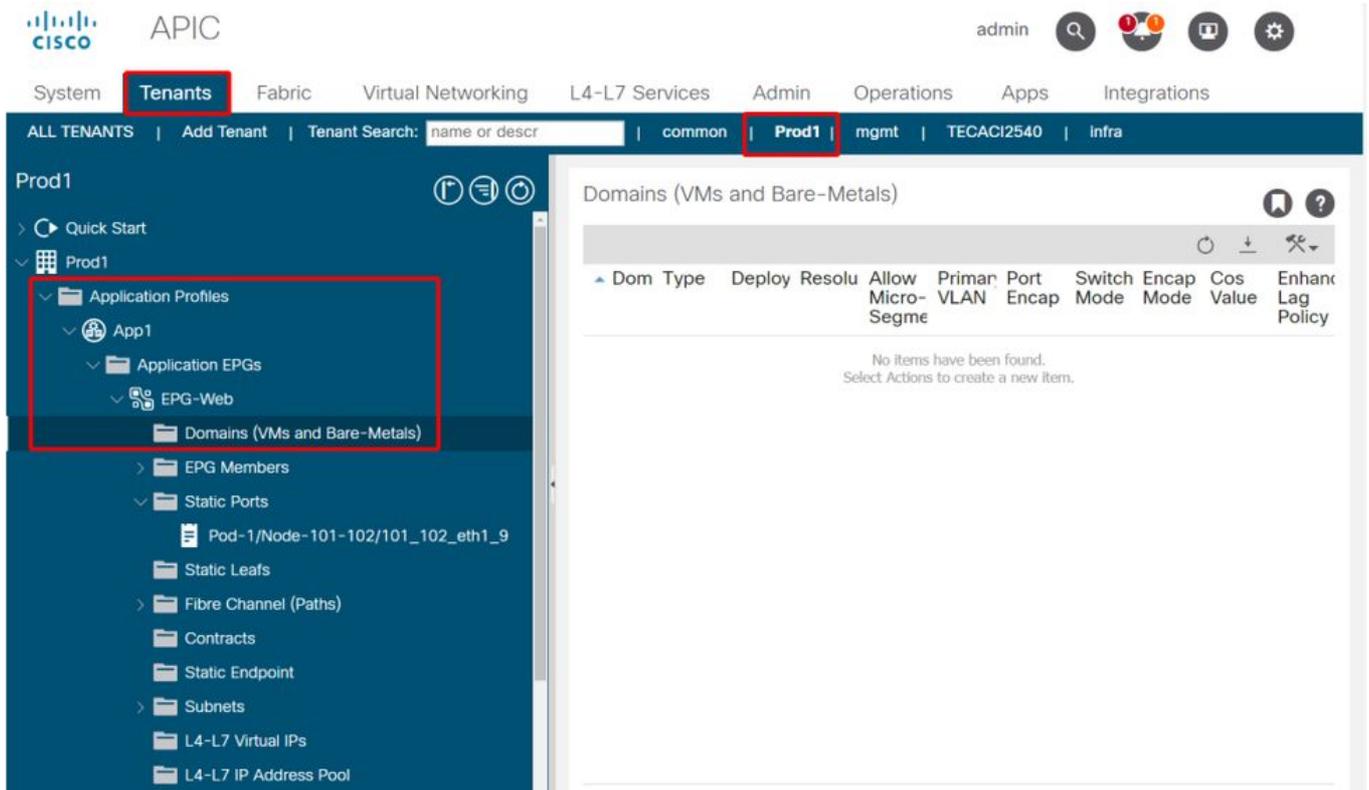
ただし、EPG障害は引き続き存在し、障害F0467に関する次の説明が更新されています。

障害 : F0467

説明 : Fault delegate:uni/tn-Prod1/ap-App1/epg-EPG-Webノード101 101_102_eth1_9の設定が失敗しました。原因は無効なパス設定です。デバッグメッセージ : invalid-path:vlan-150:EPGとポートの両方に関連付けられた、必要なVLANを持つドメインはありません。

上記の更新された障害で、EPGドメインの関連付けをチェックして、EPGに関連付けられたドメインがないことを確認します。

EPG-Webに静的ポートの関連付けがありますが、ドメインの関連付けがありません



VLAN 1501を含むドメインがEPGに関連付けられると、それ以上の障害は発生しません。

シナリオ 2 : EPGスタティックポートまたはL3Out論理インターフェイスプロファイル(SVI)に展開するパスとしてVPCを選択できない

EPGスタティックポートまたはL3Out論理インターフェイスプロファイルSVIエントリ上のパスとしてVPCを設定しようとする、展開する特定のVPCが使用可能なオプションとして表示されません。

VPCスタティックバインディングを導入する際には、次の2つの厳しい要件があります。

1. VPC明示的保護グループは、対象のリーフスイッチのペアに対して定義する必要があります。
2. 完全なアクセスポリシーマッピングを定義する必要があります。

両方の要件は、上記のようにクイックスタートビューから確認できます。どちらも完了しない場合、VPCは単にスタティックポートバインディングの使用可能なオプションとして表示されません。

シナリオ 3 : 障害F0467 : 別のEPGですでに使用されているファブリックカプセル化

デフォルトでは、VLANにはグローバルスコープがあります。つまり、特定のVLAN IDは、特定のリーフスイッチ上の1つのEPGに対してのみ使用できます。特定のリーフスイッチ内の複数のEPGで同じVLANを再利用しようとする、次の障害が発生します。

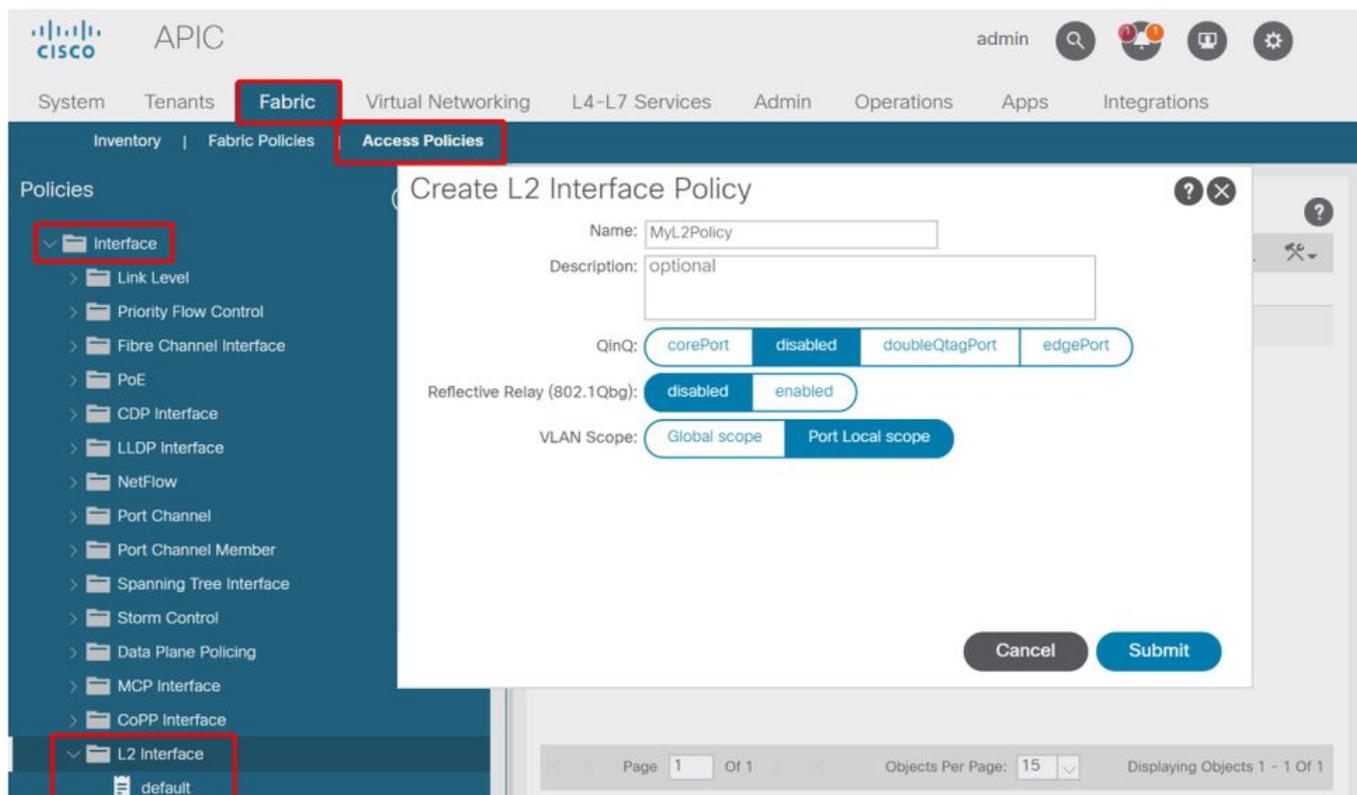
障害:F0467

説明 : Fault delegate:Encap Already Used in Another EPG, debug message:encap-already-in-use:EncapはすでにProd1:App1:EPG-Webで使用されています。

別のVLANを選択する以外に、この設定を機能させるもう1つのオプションは、「ポートローカル」VLANスコープの使用を検討することです。このスコープでは、VLANをインターフェイス単位でマッピングできます。つまり、VLAN-1501を同じリーフ上の複数のインターフェイス間で異なるEPGに使用できます。

「ポートローカル」スコープはポリシーグループ単位（特にL2ポリシーを介して）で関連付けられますが、リーフレベルで適用されます。

APIC GUI内で「VLAN Scope」設定を変更する場所



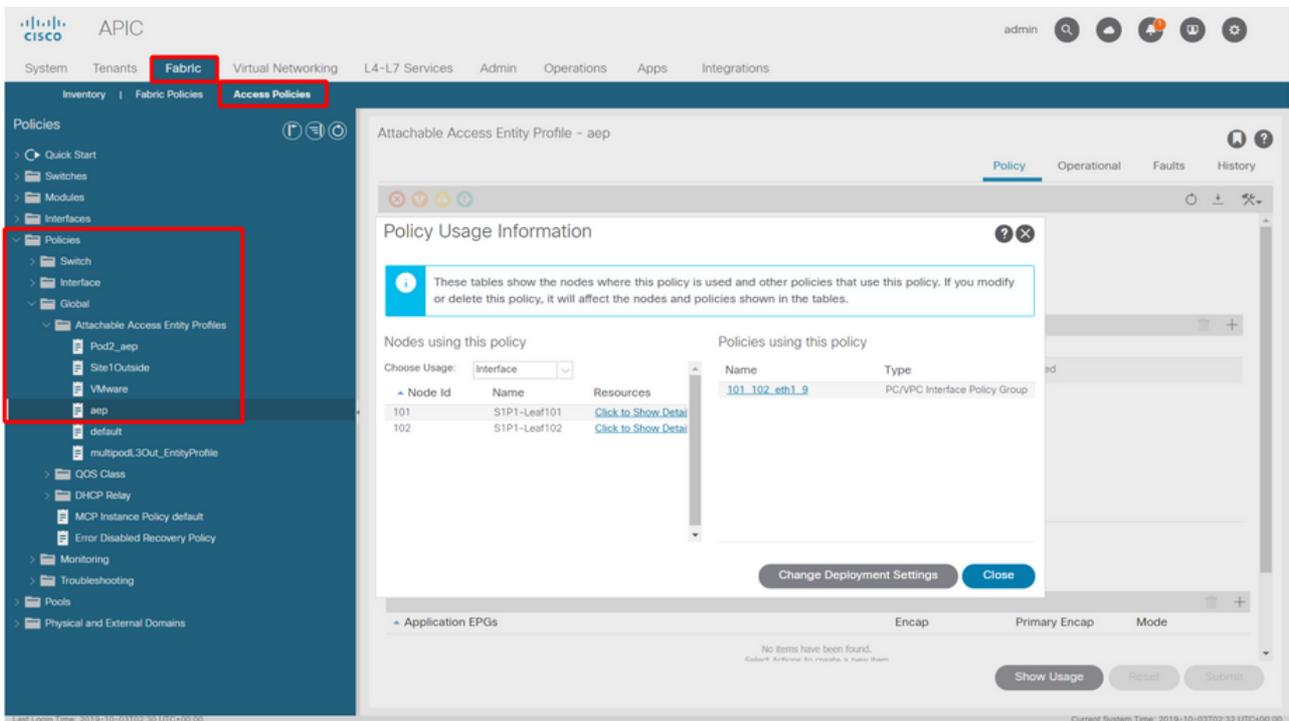
「ポートローカル」VLANスコープ設定を実装する前に、Cisco.comの『Cisco APICレイヤ2ネットワーク設定ガイド』を参照して、目的のユースケースおよび設計に対してその制限および設計上の制限が受け入れられることを確認します。

特記事項

使用状況の表示

アクセスポリシーに固有のものではありませんが、GUIのほとんどのオブジェクトで「Show Usage」というラベルの付いたボタンを使用できます。このボタンは、選択したオブジェクトをルートとするポリシー検索を実行し、どのリーフノードまたはインターフェイスがそのオブジェクトと直接関係しているかを判断します。これは、一般的な検索シナリオと、特定のオブジェクトまたはポリシーが使用中であるかどうかを理解するのに役立ちます。

次のスクリーンショットでは、選択したAEPが2つの異なるインターフェイスによって使用されています。つまり、AEPに変更を加えると、関連付けられたインターフェイスに直接影響します。



VLANプールの重複

アクセスポリシーの機能は、特定のVLANをインターフェイスに導入できるようにすることですが、設計段階で考慮する必要がある追加の用途もあります。具体的には、ドメインは外部カプセル化に関連付けられたVXLAN ID (ファブリックカプセル化と呼ばれます) の計算に使用されます。通常、この機能はデータプレーントラフィックに大きな影響を与えることはありませんが、このようなIDは、スパニングツリーBPDUを含むファブリックをフラッディングするプロトコルのサブセットに特に関連しています。leaf1に入力するVLAN-<id> BPDUがリーフ2から出力されることが予想される場合 (たとえば、ACIを介してスパニングツリーを統合するレガシースイッチがある場合)、VLAN-<id>は両方のリーフノードで同じファブリックカプセル化を持つ必要があります。同じアクセスVLANでファブリックカプセル化値が異なる場合、BPDUはファブリックを通過しません。

前のセクションで説明したように、各ドメインがリーフスイッチの固有のセットにのみ適用されるように特に注意する必要がある場合を除き、複数のドメインで同じVLANを設定することは避けてください (たとえば、VMMと物理)。両方のドメインを同じVLANの同じリーフスイッチに解決できる瞬間に、アップグレード (またはクリーンなリロード) 後に基盤となるVXLANを変更できる可能性があります。この場合、たとえばSTPコンバージェンスの問題が発生する可能性があります。この動作は、各ドメインが一意的な数値 (「base」属性) を持つことの結果であり、次の式でVXLAN IDを決定するために使用されます。

$$\text{VXLAN VNID} = \text{Base} + (\text{encap} - \text{from_encap})$$

どのドメインが特定のリーフにプッシュされるかを検証するには、「stpAllocEncapBlkDef」クラスに対してmoqueryを実行します。

```
leaf# moquery -c stpAllocEncapBlkDef
```

```
# stp.AllocEncapBlkDef
encapBlk      : uni/infra/vlanns-[physvlans]-dynamic/from-[vlan-1500]-to-[vlan-1510]
base         : 8492
dn           : allocencap-[uni/infra]/encapnsdef-[uni/infra/vlanns-[physvlans]-dynamic]/allocencapblkdef-[uni/infra/vlanns-[physvlans]-dynamic/from-[vlan-1500]-to-[vlan-1510]]
```

```
from      : vlan-1500
to        : vlan-1510
```

この出力から、次のアクセスポリシー定義を確認します。

- VLAN 1500 ~ 1510を明示的に定義したVLANのブロックを持つプログラムされたVLANプールがあります。
- このVLANブロックは、「physvlan」という名前のドメインに関連付けられています。
- VXLAN計算で使用される基準値は8492です。
- VLAN-1501に対するVXLANの計算結果は、ファブリックカプセル化として $8492 + (1501 - 1500) = 8493$ になります。

結果のVXLAN ID (この例では8493) は、次のコマンドで確認できます。

```
leaf# show system internal epm vlan all
```

VLAN ID	Type	Access Encap (Type Value)	Fabric Encap	H/W id	BD VLAN	Endpoint Count
13	Tenant BD	NONE	0 16121790	18	13	0
14	FD vlan	802.1Q	1501 8493	19	13	0

同じリーフにプッシュされるVLAN-1501を含む他のVLANプールがある場合、アップグレードまたはクリーンなリロードによって一意のベース値 (およびその後の別のファブリックカプセル化) が取得される可能性があり、その結果、BPDUはVLAN-1501でBPDUを受信すると予想される別のリーフに到達できなくなります。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。