

# ACI 액세스 정책 문제 해결

## 목차

[소개](#)

[배경 정보](#)

[액세스 정책 개요](#)

[액세스 정책 구성: 방법론](#)

[액세스 정책 수동 기본 구성](#)

[스위치 정책 구성](#)

[인터페이스 정책 구성](#)

[VPC 구성](#)

[VLAN 풀 구성](#)

[도메인 구성](#)

[AEP\(Attachable Access Entity Profile\) 구성](#)

[테넌트, APP 및 EPG 구성](#)

[EPG 고정 바인딩 구성](#)

[액세스 정책 컨피그레이션 요약](#)

[추가 서버 연결](#)

[다음 단계는?](#)

[문제 해결 워크플로](#)

[문제 해결을 위해 "인터페이스, PC 및 VPC 빠른 시작 구성" 사용](#)

[문제 해결 시나리오](#)

[시나리오 1: 결합 F0467 - 잘못된 경로, nwissues](#)

[시나리오 2: EPG 고정 포트 또는 L3Out SVI\(Logical Interface Profile\)에 배포할 경로로 VPC를 선택할 수 없습니다.](#)

[시나리오 3: 결합 F0467 - 다른 EPG에서 패브릭 캡슐화 기능이 이미 사용됨](#)

[특별 언급](#)

[사용 표시](#)

[중복 VLAN 풀](#)

## 소개

이 문서에서는 ACI 액세스 정책을 이해하고 문제를 해결하는 단계에 대해 설명합니다.

## 배경 정보

이 문서의 자료는 Troubleshooting [Cisco Application Centric Infrastructure, Second Edition](#) 책, 특히 [액세스 정책 - 개요](#) 및 [액세스 정책 - 문제 해결 워크플로](#) 장에서 발췌했습니다.

## 액세스 정책 개요

ACI 관리자는 패브릭의 포트에 VLAN을 어떻게 구성합니까? ACI 관리자는 액세스 정책과 관련된 결합을 어떻게 처리하기 시작합니까? 이 섹션에서는 패브릭 액세스 정책과 관련된 문제를 해결하

는 방법에 대해 설명합니다.

문제 해결 시나리오를 시작하기 전에 먼저 ACI Object Model 내에서 액세스 정책의 작동 방식 및 그 관계를 올바르게 이해해야 합니다. 이를 위해 독자는

Cisco.com(<https://developer.cisco.com/site/apic-mim-ref-api/>)에서 제공되는 "ACI Policy Model" 및 "APIC Management Information Model Reference" 문서를 모두 참조할 수 [있습니다](#).

액세스 정책의 기능은 leaf 스위치의 다운링크 포트에서 특정 컨피그레이션을 활성화하는 것입니다. ACI 패브릭 포트를 통한 트래픽을 허용하도록 테넌트 정책을 정의하려면 먼저 관련 액세스 정책을 마련해야 합니다.

일반적으로 액세스 정책은 새로운 리프 스위치가 패브릭에 추가되거나 디바이스가 ACI 리프 다운링크에 연결될 때 정의됩니다. 그러나 환경이 얼마나 동적인지에 따라 패브릭의 정상 작동 중에 액세스 정책이 수정될 수 있습니다. 예를 들어, 새 VLAN 집합을 허용하거나 패브릭 액세스 포트에 새 라우팅 도메인을 추가합니다.

ACI 액세스 정책은 처음에는 다소 위협적이지만 매우 유연하며 지속적인 진화 과정에서 대규모 SDN 네트워크에 대한 컨피그레이션 프로비저닝을 간소화하도록 설계되었습니다.

## 액세스 정책 구성: 방법론

액세스 정책은 독립적으로 구성할 수 있습니다. 즉, 필요한 모든 객체를 독립적으로 생성할 수도 있고, ACI GUI에서 제공하는 다양한 마법사를 통해 정의할 수도 있습니다.

마법사는 사용자에게 워크플로를 안내하고 필요한 모든 정책이 적용되도록 하기 때문에 매우 유용합니다.

### 액세스 정책 — 빠른 시작 마법사

The screenshot displays the Cisco APIC (Application Policy Infrastructure Controller) web interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'L4-L7 Services', 'Admin', 'Operations', 'Apps', and 'Integrations'. The 'Fabric' tab is active, and the 'Access Policies' sub-tab is selected. The main content area is titled 'Quick Start' and is divided into three columns: 'Summary', 'Steps', and 'See Also'. The 'Steps' column lists several configuration tasks, with 'Configure an interface, PC, and VPC' highlighted by a red box. The 'See Also' column 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'.

위 그림에서는 여러 마법사를 찾을 수 있는 빠른 시작 페이지를 보여 줍니다.

액세스 정책이 정의되면 모든 관련 객체에 결함이 표시되지 않도록 하여 정책을 검증하는 것이 좋습니다.

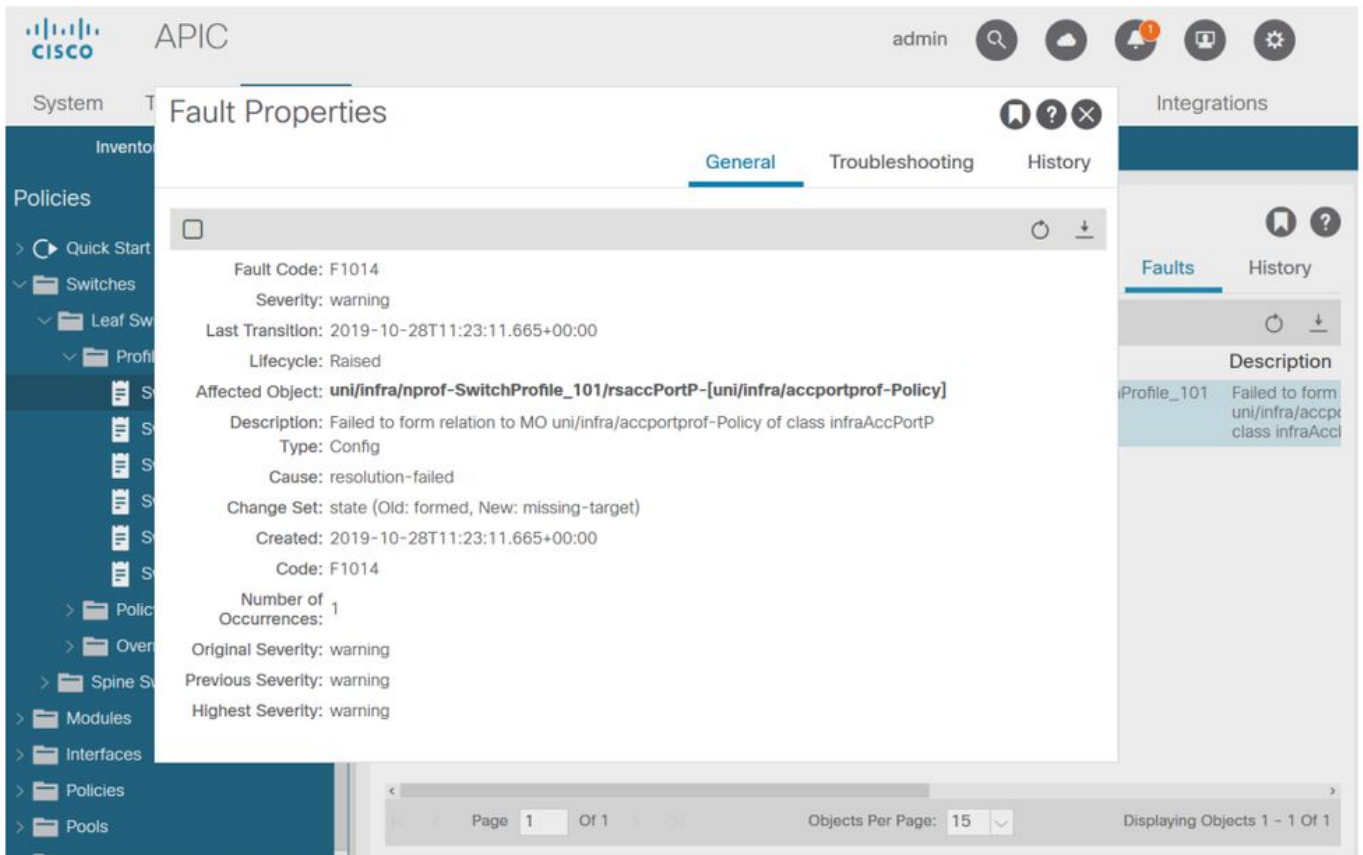
예를 들어, 아래 그림에서 스위치 프로파일에 존재하지 않는 인터페이스 선택기 정책이 할당되었습니다. 주의 깊은 사용자는 손쉽게 객체의 'missing-target' 상태를 확인하고 GUI에서 결함이 플래그되었는지 확인할 수 있습니다.

## 리프 프로파일 — SwitchProfile\_101

The screenshot displays the Cisco APIC interface for configuring a Leaf Profile. The left sidebar shows the navigation tree with 'SwitchProfile\_101' selected. The main content area shows the configuration for 'Leaf Profile - SwitchProfile\_101'. The 'Associated Interface Selector Profiles' table is as follows:

Name	Description	State
Policy		missing-target
SwitchProfile_101		formed

## 리프 프로파일 — SwitchProfile\_101 — 결함



이 경우 결함을 수정하는 것은 'Policy'라는 새로운 인터페이스 선택기 프로필을 생성하는 것만큼 쉽습니다.

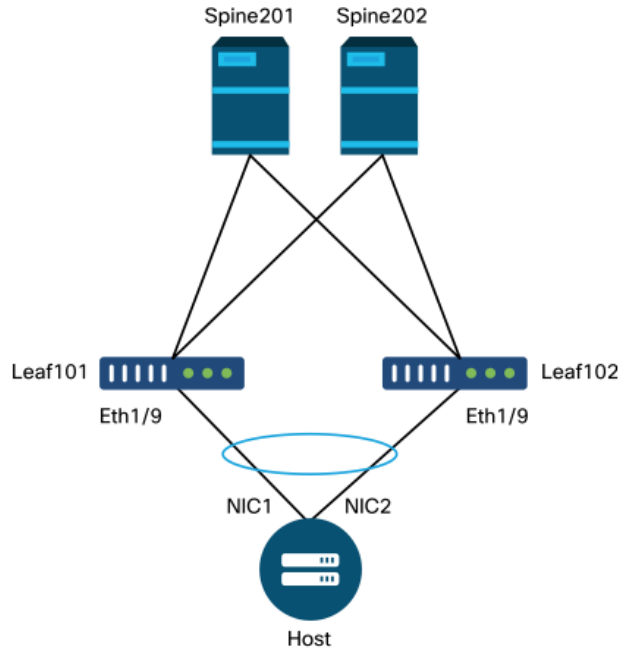
기본 액세스 정책의 수동 컨피그레이션은 다음 단락에서 살펴봅니다.

## 액세스 정책 수동 기본 구성

액세스 정책을 구축할 때, 지정된 다운링크의 용도를 나타내기 위해 객체를 정의하고 있습니다. 다운링크를 프로그래밍하는 선언(예: EPG 정적 포트 할당)은 이러한 명시적 의도에 의존합니다. 이를 통해 구성을 확장하고 특정 외부 디바이스에 특별히 연결된 스위치 또는 포트와 같은 유사한 사용 객체를 논리적으로 그룹화할 수 있습니다.

이 장의 나머지 부분에 대해서는 아래 토폴로지를 참조하십시오.

### 듀얼 홈 서버의 액세스 정책 정의 토폴로지

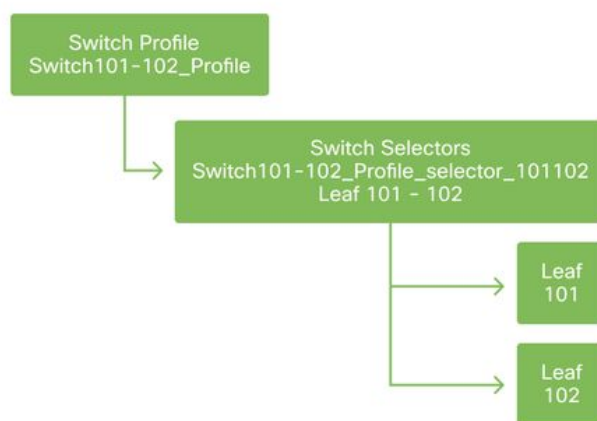


웹 서버가 ACI 패브릭에 연결됩니다. 웹 서버에는 LACP 포트 채널에 구성된 2개의 NIC(Network Interface Card)가 있습니다. 웹 서버가 리프 스위치 101 및 102의 포트 1/9에 연결되어 있습니다. 웹 서버는 VLAN-1501을 사용하며 EPG 'EPG-Web'에 상주해야 합니다.

## 스위치 정책 구성

첫 번째 논리적 단계는 사용할 리프 스위치를 정의하는 것입니다. '스위치 프로필'에는 사용할 리프 노드 ID를 정의하는 '스위치 선택기'가 포함됩니다.

## 스위치 정책



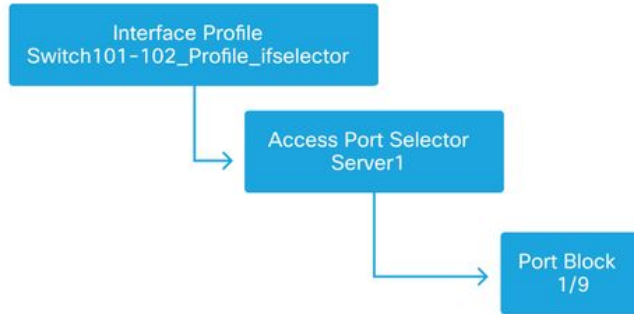
일반적으로 프로파일의 일부인 노드를 나타내는 명명 체계를 사용하여 개별 리프 스위치당 1개의 스위치 프로파일 및 VPC 도메인 쌍당 1개의 스위치 프로파일을 구성하는 것이 좋습니다.

빠른 시작은 논리 명명 체계를 배포하여 적용 위치를 쉽게 이해할 수 있도록 합니다. 완성된 이름은 'Switch<node-id>\_Profile' 형식을 따릅니다. 예를 들어, 'Switch101\_Profile'은 리프 노드 101을 포함하는 스위치 프로파일에 대한 것이고, VPC 도메인의 일부여야 하는 리프 노드 101과 102를 포함하는 스위치 프로파일에 대한 Switch101-102\_Profile일 것입니다.

## 인터페이스 정책 구성

스위치 액세스 정책이 생성되면 인터페이스를 정의하는 것이 다음 논리적 단계가 됩니다. 이는 'Port Block' 정의가 포함된 1개 이상의 'Access Port Selectors'로 구성된 'Interface Profile'을 생성하는 방식으로 수행됩니다.

### 인터페이스 정책

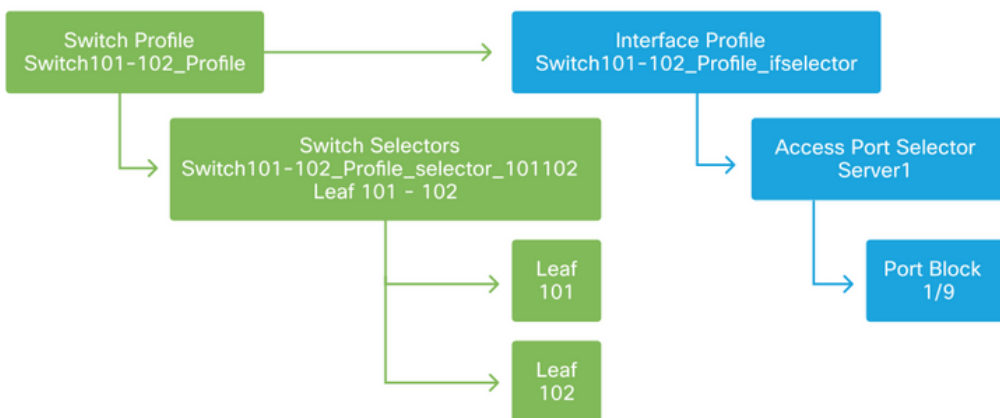


'인터페이스 프로필'과 관련 스위치 간의 관계를 구성하려면 '스위치 프로필'을 '인터페이스 프로필'에 연결합니다.

'인터페이스 프로필'은 여러 가지 방법으로 정의할 수 있습니다. '스위치 프로필'과 유사하게 물리적 스위치당 하나의 '인터페이스 프로필'을 생성할 수 있으며, VPC 도메인당 하나의 '인터페이스 프로필'도 생성할 수 있습니다. 그러면 이러한 정책에 해당 스위치 프로필에 대한 1:1 매핑이 있어야 합니다. 이러한 논리에 따라 패브릭 액세스 정책이 대폭 간소화되어 다른 사용자가 쉽게 이해할 수 있습니다.

빠른 시작에서 사용하는 기본 이름 지정 체계도 여기에서 사용할 수 있습니다. 이 프로파일이 인터페이스 선택에 사용됨을 나타내기 위해 '<switch profile name>\_ifselector' 형식을 따릅니다. 예를 들면 'Switch101\_Profile\_ifselector'가 있습니다. 이 예제 '인터페이스 프로필'은 리프 스위치 101에서 비 VPC 인터페이스를 구성하는 데 사용되며 'Switch101\_Profile' 액세스 정책에만 연결됩니다.

### 인터페이스 프로필에 연결된 스위치 프로필

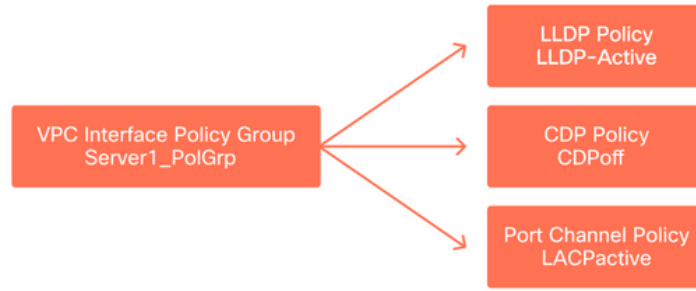


Eth 1/9의 '인터페이스 프로필'이 leaf 스위치 101과 102를 모두 포함하는 '스위치 프로필'에 연결되어 있으므로 두 노드에서 Eth 1/9의 프로비저닝이 동시에 시작됩니다.

이 시점에서는 리프 스위치와 해당 포트가 정의되었습니다. 다음 논리적 단계는 이러한 포트의 특

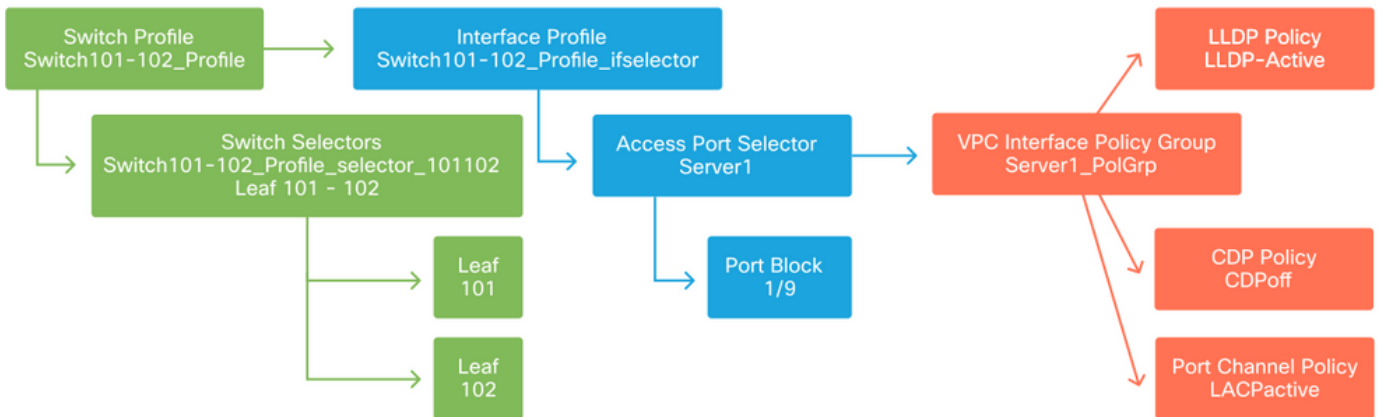
성을 정의하는 것입니다. '인터페이스 정책 그룹'에서는 이러한 포트 속성을 정의할 수 있습니다. 위의 LACP 포트 채널을 허용하기 위한 'VPC 인터페이스 정책 그룹'이 생성됩니다.

### 정책 그룹



'VPC 인터페이스 정책 그룹'은 '액세스 포트 선택기'에서 '인터페이스 정책 그룹'에 연결되어 리프 스위치/인터페이스에서 포트 속성으로의 관계를 형성합니다.

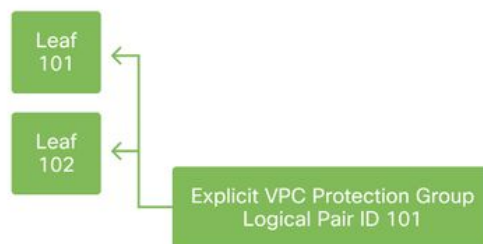
### 스위치 및 인터페이스 프로파일 결합



### VPC 구성

LACP 포트 채널 over 2 리프 스위치를 생성하려면 리프 스위치 101과 102 사이에 VPC 도메인을 정의해야 합니다. 이는 두 리프 스위치 사이에 'VPC 보호 그룹'을 정의하여 수행됩니다.

### VPC



### VLAN 풀 구성

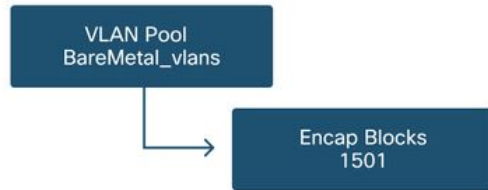
다음 논리적 단계는 이 포트에서 사용될 VLAN(이 경우 VLAN-1501)을 생성하는 것입니다. '캡슐화 블록'이 있는 'VLAN 풀'을 정의하면 이 컨피그레이션이 완료됩니다.



VLAN 풀 범위의 크기를 고려할 때 VMM 통합을 사용하는 경우 대부분의 구축에는 단일 VLAN 풀과 하나의 추가 풀만 필요합니다. 레거시 네트워크의 VLAN을 ACI로 가져오려면 레거시 VLAN의 범위를 정적 VLAN 풀로 정의합니다.

예를 들어 레거시 환경에서 VLAN 1-2000이 사용된다고 가정합니다. VLAN 1-2000을 포함하는 하나의 고정 VLAN 풀을 생성합니다. 그러면 ACI 브리지 도메인 및 EPG를 레거시 패브릭으로 트렁크할 수 있습니다. VMM을 구축할 경우, 사용 가능한 VLAN ID 범위를 사용하여 두 번째 동적 풀을 생성할 수 있습니다.

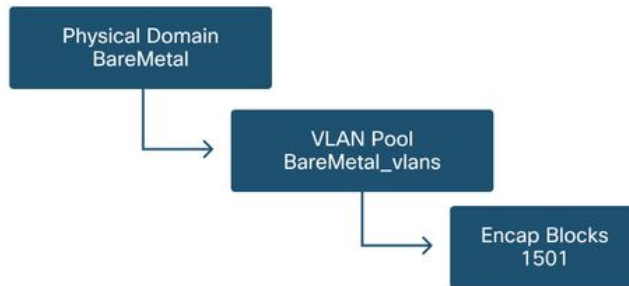
## VLAN 풀



## 도메인 구성

다음 논리적 단계는 '도메인'을 만드는 것입니다. '도메인'은 VLAN 풀의 범위, 즉 해당 풀이 적용되는 위치를 정의합니다. '도메인'은 물리적, 가상 또는 외부(연결 또는 라우팅)일 수 있습니다. 이 예에서는 베어 메탈 서버를 패브릭에 연결하는 데 '물리적 도메인'을 사용합니다. 이 '도메인'은 'VLAN 풀'에 연결되어 필요한 VLAN을 허용합니다.

## 물리적 도메인



대부분의 구축에서 단일 '물리적 도메인'은 베어 메탈 구축에 충분하며 단일 '라우티드 도메인'은 L3Out 구축에 충분합니다. 둘 다 동일한 'VLAN 풀'에 매핑할 수 있습니다. 패브릭이 멀티 테넌시 방식으로 구축되거나 어떤 사용자가 포트에 특정 EPG 및 VLAN을 구축할 수 있는지를 제한하기 위해 더 세부적인 제어가 필요한 경우, 보다 전략적인 액세스 정책 설계를 고려해야 합니다.

'도메인'은 또한 RBAC(역할 기반 액세스 제어)를 사용하여 '보안 도메인'이 있는 정책에 대한 사용자 액세스를 제한하는 기능을 제공합니다.

스위치에 VLAN을 구축할 때 ACI는 스페닝 트리 BPDU를 VLAN이 보낸 도메인을 기반으로 하는 고유한 VXLAN ID로 캡슐화합니다. 따라서 다른 브리지와 STP 통신이 필요한 디바이스를 연결할 때 마다 동일한 도메인을 사용하는 것이 중요합니다.

VLAN VXLAN ID는 VPC 스위치가 VPC에서 학습한 MAC 주소와 IP 주소를 동기화할 수 있도록 하는 데에도 사용됩니다. 따라서 VLAN 풀을 위한 가장 간단한 설계는 정적 구축에 단일 풀을 사용하고 동적 구축에 두 번째 풀을 생성하는 것입니다.

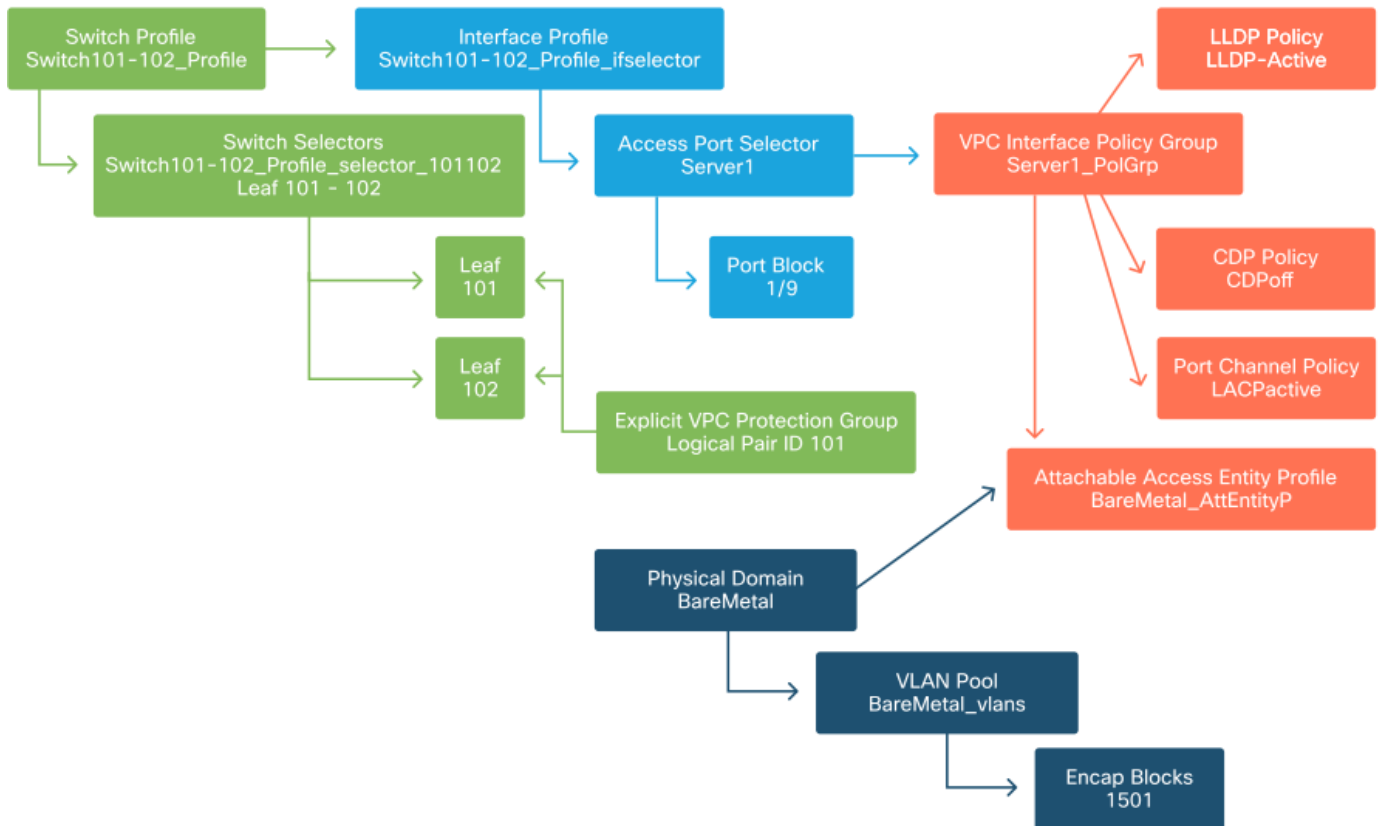


## AEP(Attachable Access Entity Profile) 구성

액세스 정책 컨피그레이션의 두 가지 주요 청크가 완료되었습니다. 스위치 및 인터페이스 정의, 도메인/VLAN 정의 'AEP(Attachable Access Entity Profile)'라는 개체는 이 두 청크를 서로 연결하는 역할을 합니다.

'정책 그룹'은 일대다 관계의 AEP에 연결되며, AEP는 유사한 정책 요구 사항을 공유하는 인터페이스와 스위치를 함께 그룹화할 수 있습니다. 이는 특정 스위치의 인터페이스 그룹을 나타낼 때 하나의 AEP만 참조해야 함을 의미합니다.

### 연결 가능한 액세스 엔티티 프로파일



대부분의 구축에서는 고정 경로에 단일 AEP를 사용하고 VMM 도메인당 추가 AEP를 하나씩 사용해야 합니다.

가장 중요한 고려 사항은 AEP를 통해 인터페이스에 VLAN을 구축할 수 있다는 것입니다. 이는 EPG를 AEP에 직접 매핑하거나 VMM 도메인에서 사전 프로비저닝을 구성하여 수행할 수 있습니다. 이 두 가지 컨피그레이션 모두 연결된 인터페이스를 트렁크 포트('switchport mode trunk' on legacy switches)로 만듭니다.

따라서 라우팅된 포트 또는 라우팅된 하위 인터페이스를 사용할 경우 L3Out에 대해 별도의 AEP를 생성하는 것이 중요합니다. SVI가 L3Out에서 사용되는 경우 추가 AEP를 생성할 필요가 없습니다.

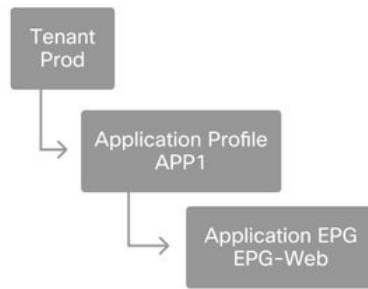
## 테넌트, APP 및 EPG 구성

ACI는 정책 기반 접근 방식을 사용하여 연결을 정의하는 다른 수단을 사용합니다.

최하위 레벨 객체는 '엔드포인트 그룹'(EPG)이라고 합니다. EPG 구성은 유사한 정책 요구 사항이 있는 VM 또는 서버(엔드포인트) 그룹을 정의하는 데 사용됩니다. 테넌트 아래에 있는 '애플리케이션'

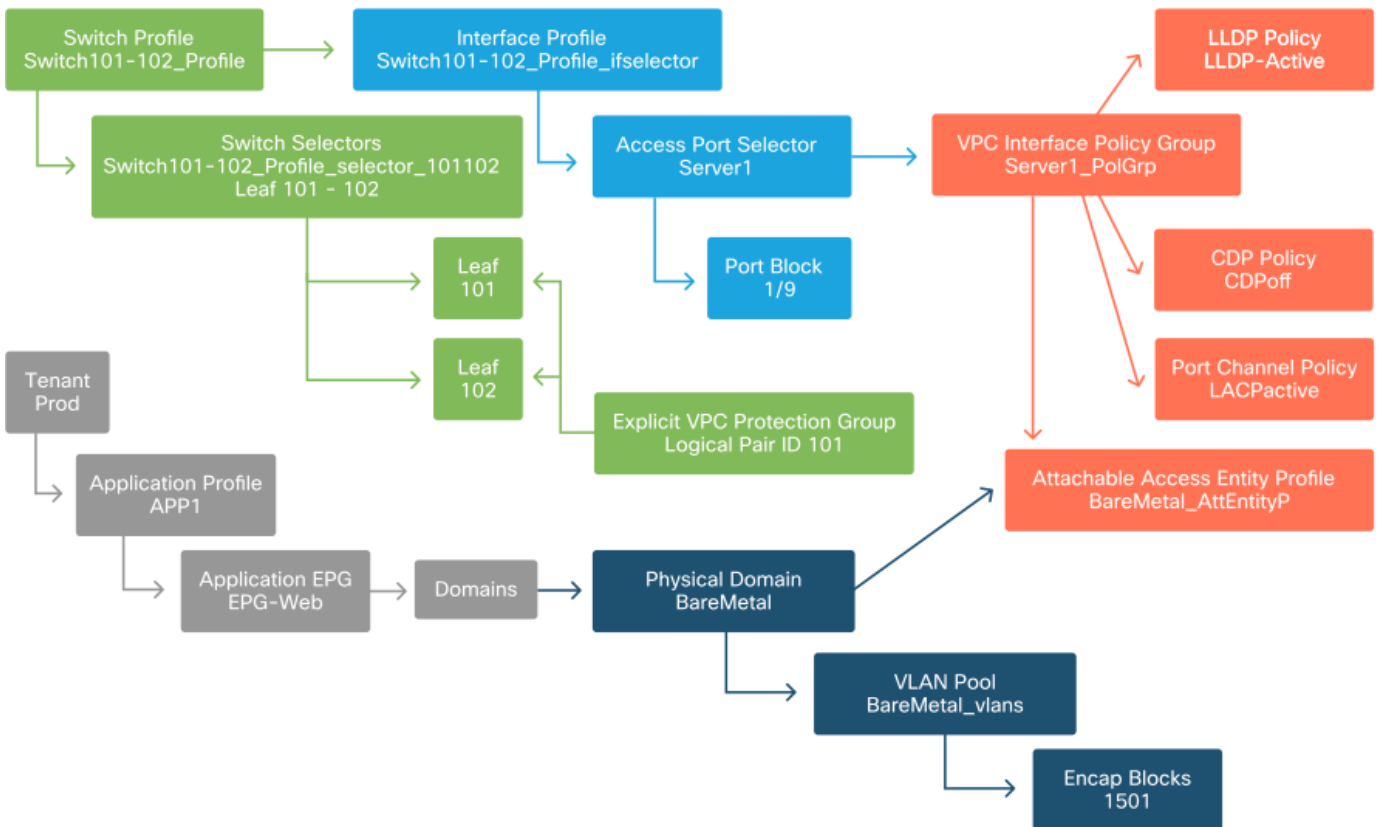
선 프로파일'은 EPG를 논리적으로 그룹화하는 데 사용됩니다.

### 테넌트, 앱 및 EPG



다음 논리적 단계는 EPG를 도메인에 연결하는 것입니다. 그러면 워크로드를 나타내는 논리적 객체, EPG 및 물리적 스위치/인터페이스, 액세스 정책 간에 링크가 생성됩니다.

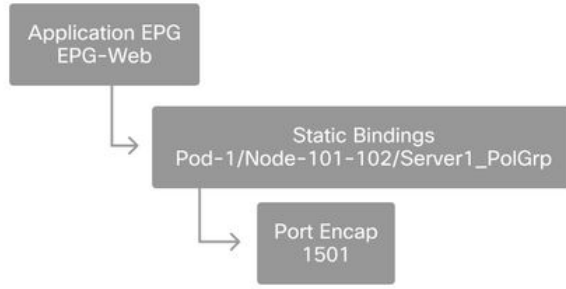
### EPG-도메인 링크



### EPG 고정 바인딩 구성

마지막 논리적 단계는 지정된 EPG의 스위치 인터페이스에 VLAN을 프로그래밍하는 것입니다. 이는 물리적 도메인을 사용하는 경우 특히 중요합니다. 이 유형의 도메인에는 명시적 선언이 필요하기 때문입니다. 이렇게 하면 EPG가 패브릭에서 확장되고 베어 메탈 서버가 EPG로 분류될 수 있습니다.

### 정적 바인딩

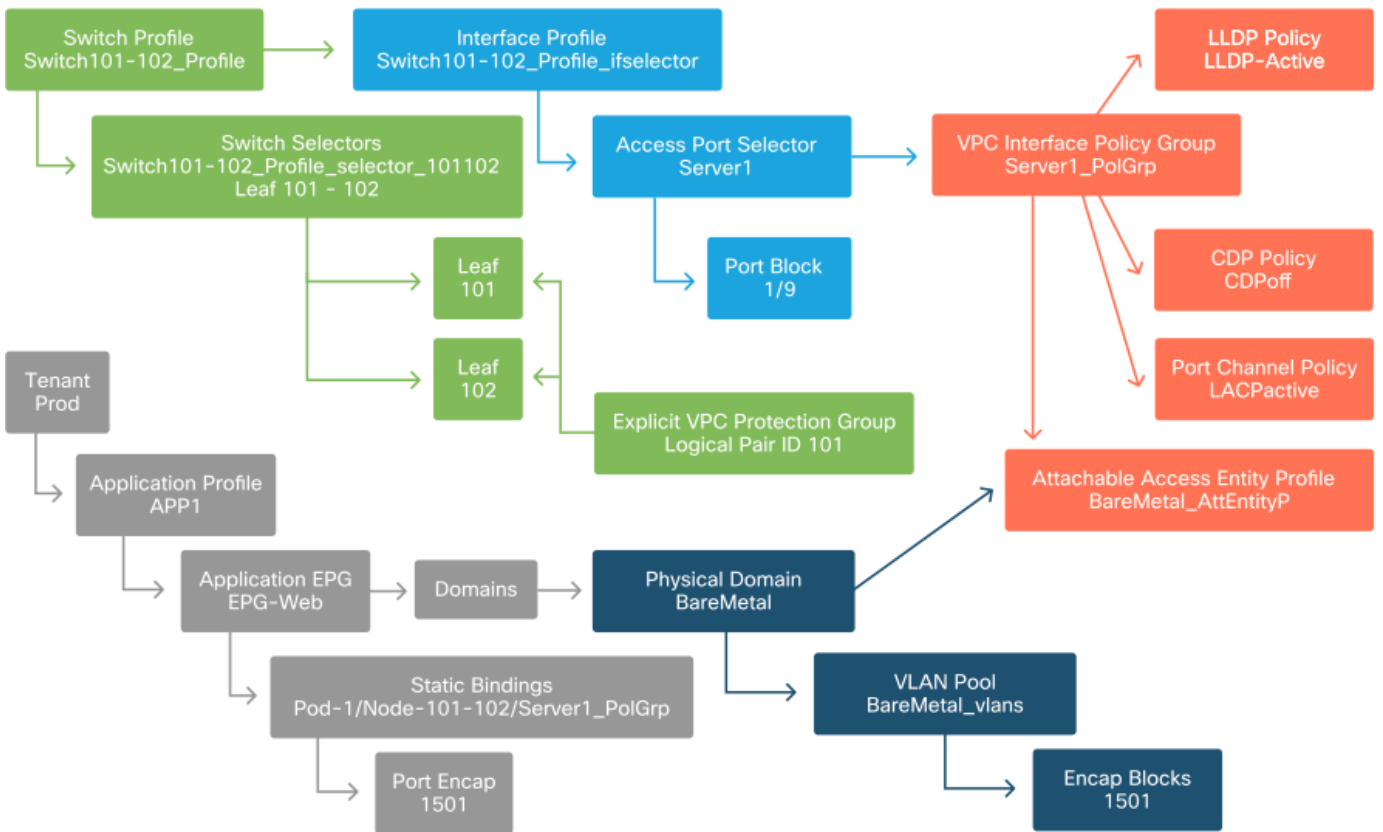


참조된 '포트 캡슐화'를 'VLAN 풀'에 대해 확인할 수 있어야 합니다. 그렇지 않으면 결함이 플래그됩니다. 이에 대해서는 이 장의 "문제 해결 워크플로" 섹션에서 설명합니다.

### 액세스 정책 컨피그레이션 요약

다음 다이어그램에는 리프 스위치 101 및 102에 대한 VPC 연결을 사용하여 VLAN-1501을 통한 호스트 연결을 허용하도록 생성된 모든 객체가 요약되어 있습니다.

### 베어 메탈 ACI 연결



### 추가 서버 연결

이전의 모든 정책이 생성되었으므로 리프 스위치 101 및 102의 포트 Eth1/10에 있는 서버를 포트 채널과 연결한다는 것은 무엇을 의미합니까?

'베어 메탈 ACI 연결' 다이어그램을 참조하여 최소 다음 항목을 만들어야 합니다.

- 추가 액세스 포트 선택기 및 포트 블록
- 추가 VPC 인터페이스 정책 그룹.

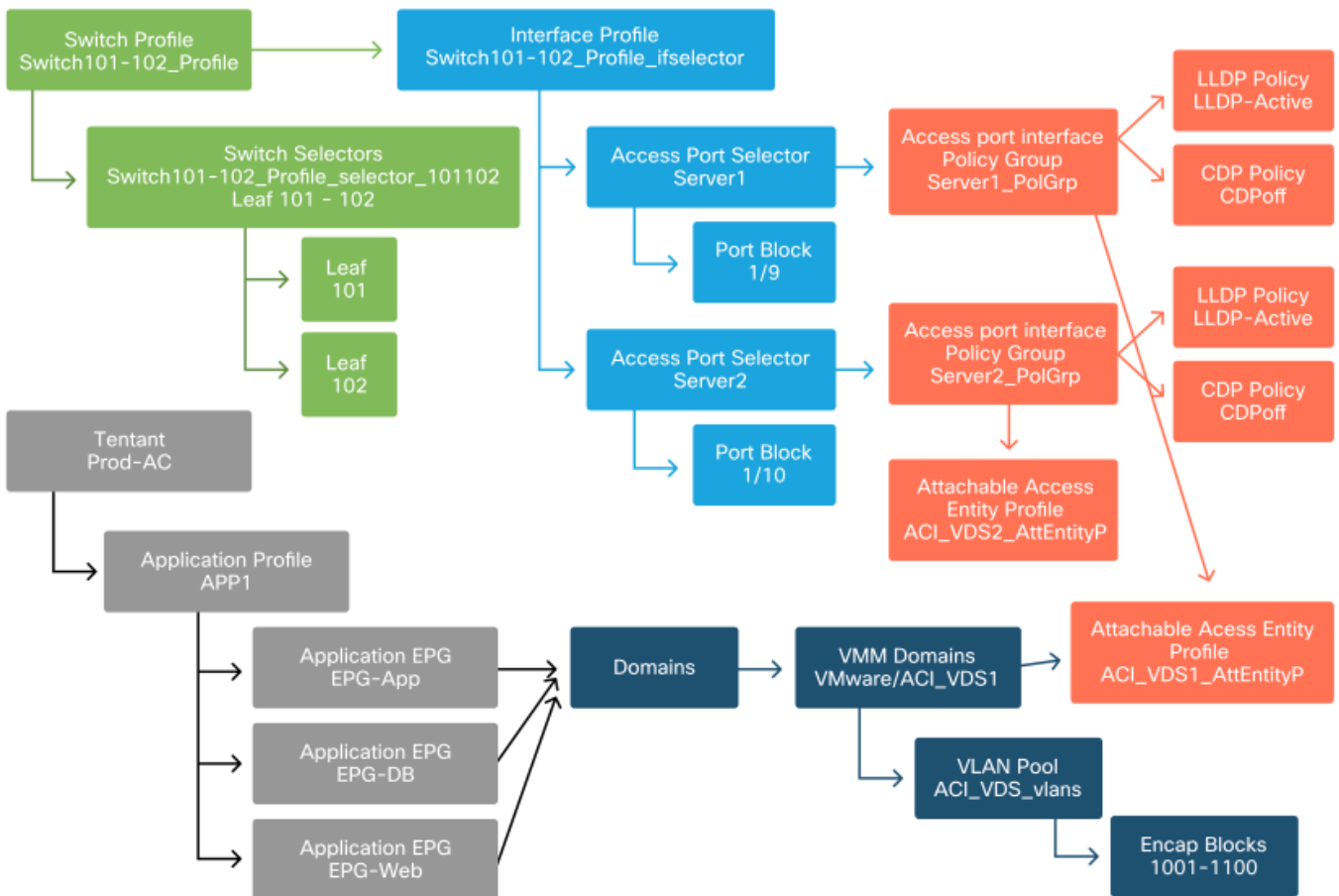
- 포트 캡슐화 기능이 있는 추가 정적 바인딩.

LACP 포트 채널의 경우 전용 VPC 인터페이스 정책 그룹을 사용해야 합니다. 이 VPC 정책 그룹은 VPC ID를 정의하는 그룹입니다.

개별 링크의 경우, 링크에 동일한 포트 속성이 필요한 경우 비 VPC 인터페이스 정책 그룹을 추가 서버에 다시 사용할 수 있습니다.

결과 정책은 다음 이미지와 같습니다.

### 서버 2를 설정에 연결하는 중



### 다음 단계는?

다음 섹션에서는 이 개요에서 설명하는 토폴로지 및 활용 사례부터 시작하여 몇 가지 액세스 정책 실패 시나리오를 살펴봅니다.

## 문제 해결 워크플로

액세스 정책으로 작업할 때 다음과 같은 문제 해결 시나리오가 발생할 수 있습니다.

- AEP에 연결되지 않은 액세스 정책 그룹과 같은 액세스 정책에서 둘 이상의 엔터티 간의 누락된 관계입니다.
- 누락되거나 예기치 않은 정책은 지정된 액세스 정책(예: 'lldp\_enabled'라는 LLDP 정책에 연결되어 있지만, 실제로는 정책 컨피그레이션에 LLDP rx/tx가 비활성화되어 있습니다).
- 구성된 VLAN ID 캡슐화가 구성된 VLAN 풀에서 누락된 것과 같이 액세스 정책에 없거나 예기

치 않은 값입니다.

- EPG와 액세스 정책 간의 누락된 관계(예: EPG에 대한 물리적 또는 가상 도메인 연결 없음).

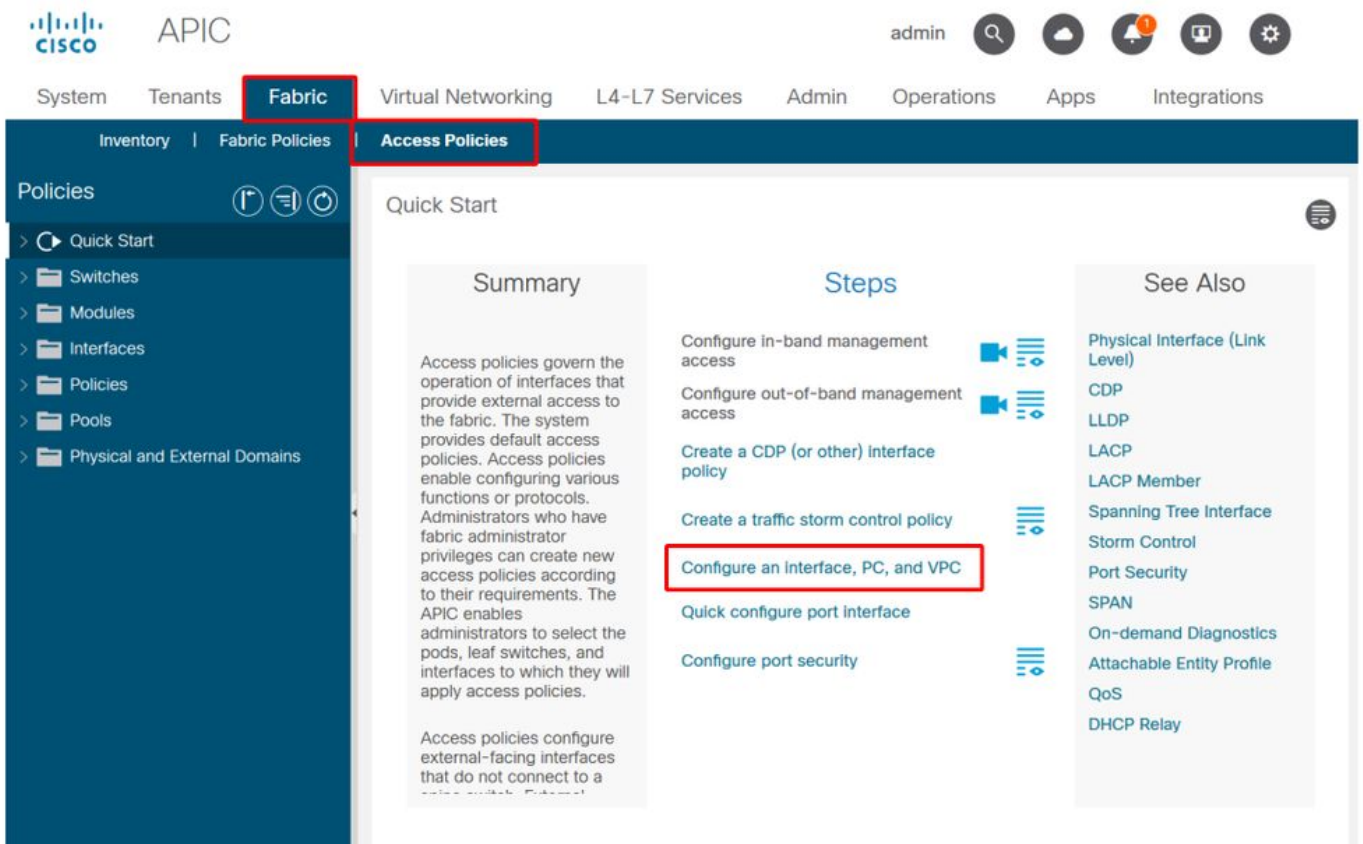
위의 트러블슈팅의 대부분은 액세스 정책 관계를 통해 누락된 관계가 있는지 확인하거나, 구성된 정책 및/또는 컨피그레이션에서 원하는 동작이 발생하는지 파악하는 것입니다.

## 문제 해결을 위해 "인터페이스, PC 및 VPC 빠른 시작 구성" 사용

APIC GUI에서 'Configure Interface, PC, and VPC' 빠른 시작 마법사는 관리자에게 기존 액세스 정책의 집계 보기를 제공하여 액세스 정책 조회를 용이하게 합니다. 이 빠른 시작 마법사는 GUI에서 찾을 수 있습니다.

'패브릭 > 액세스 정책 > 빠른 시작 > 단계 > 인터페이스, PC 및 VPC 구성'

### '인터페이스, PC 및 VPC 구성' 빠른 시작 위치



마법사에 이름에 'Configure'가 있더라도 인터페이스가 프로그래밍되도록 구성해야 하는 여러 액세스 정책의 집계 보기를 제공하는 것이 매우 편리합니다. 이러한 집계는 이미 정의된 정책을 파악하는 단일 보기 역할을 하며 액세스 정책 관련 문제의 격리를 시작하는 데 필요한 클릭 수를 효과적으로 줄여줍니다.

빠른 시작 보기를 로드할 때 '구성된 스위치 인터페이스' 보기(왼쪽 위 창)를 참조하여 기존 액세스 정책을 확인할 수 있습니다. 마법사는 액세스 정책 컨피그레이션에 따라 개별 또는 다중 리프 스위치를 나타내는 폴더 아래의 항목을 그룹화합니다.

이 마법사의 값을 보여 주는 다음 마법사 스크린샷은 독자가 패브릭 토폴로지에 대해 전혀 알지 못한다는 점을 알려줍니다.

### '인터페이스, PC 및 VPC 구성' 빠른 시작 데모 보기

# 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			



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



## VPC Switch Pairs

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

'구성된 스위치 인터페이스' 창에는 액세스 정책 매핑이 표시됩니다. 'VPC 스위치 쌍' 창에는 완료된 VPC 보호 그룹 정의가 표시됩니다.

아래 표에는 위 스크린샷에서 파생될 수 있는 완료된 액세스 정책 정의의 하위 집합이 나와 있습니다.

### 위의 빠른 시작 보기에서 파생될 수 있는 완료된 액세스 정책의 하위 집합

스위치 노드	인터페이스	정책 그룹 유형	도메인 유형	VLAN
101	1/31	개별	라우팅됨(L3)	2600
101	1/4	개별	Phys(베어 메탈)	311-3
103-104	1/10	VPC	Phys(베어 메탈)	100-3

기본 보기에서 VLAN 열 엔트리는 의도적으로 불완전합니다.

마찬가지로, 완료된 'VPC 보호 그룹' 정책은 'VPC 스위치 쌍' 보기(왼쪽 아래 창)에서 파생될 수 있습니다. 'VPC 보호 그룹'이 없으면 두 리프 노드 간에 VPC 도메인을 정의하는 정책이므로 VPC를 배포할 수 없습니다.

창 크기 조정으로 인해 긴 항목이 완전히 표시되지 않는다는 점을 고려하십시오. 모든 항목의 전체 값을 보려면 마우스 포인터를 관련 필드에 올려놓습니다.

마우스 포인터가 103-104, int 1/10 VPC 항목의 '연결된 장치 유형' 필드 위에 마우스 포인터를 올리 고 있습니다.

## 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	1/17	VPC	Bare Metal (VLANs: 100-3...
103	1/4	Individ...	L3 (VLANs: 3100,603,640,...
103,104			



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



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

창 위에 마우스를 올려 놓으면 전체 항목이 표시됩니다.

마우스 오버 세부 정보를 사용하여 완료된 액세스 정책의 하위 집합 업데이트

스위치 노드	인터페이스	정책 그룹 유형	도메인 유형	VLAN
101	1/31	개별	라우팅됨(L3)	2600
101	1/4	개별	Phys(베어 메탈)	311-320
103-104	1/10	VPC	Phys(베어 메탈)	100-300,900-999
103-104	1/10	VPC	라우팅됨(L3)	100-300,900-999

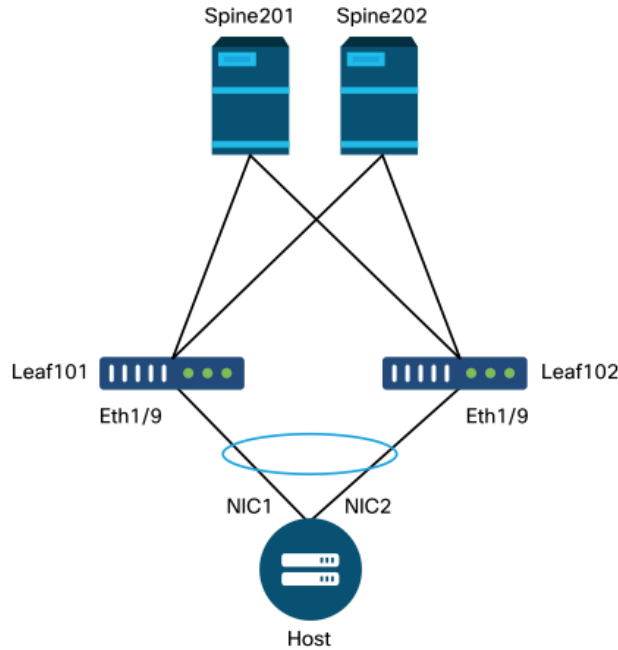
이제 문제 해결 및 확인을 위해 전체 VLAN 연결을 확인하고 이해할 수 있습니다.

## 문제 해결 시나리오

다음 트러블슈팅 시나리오의 경우 이전 장에서 동일한 토폴로지를 참조하십시오.

액세스 정책 '소개' 섹션의 토폴로지





## 시나리오 1: 결함 F0467 - 잘못된 경로, nwissues

이 결함은 스위치/포트/VLAN 선언이 해당 컨피그레이션이 제대로 적용될 수 있도록 해당 액세스 정책 없이 이루어질 때 제기됩니다. 이 결함의 설명에 따라 액세스 정책 관계의 다른 요소가 누락될 수 있습니다.

해당 액세스 정책 관계가 없는 트렁크 엔드캡 VLAN 1501을 사용하여 위 VPC 인터페이스에 대한 정적 바인딩을 배포한 후 EPG에서 다음 결함이 제기됩니다.

**결함:** F0467

**설명:** 결함 대리인: 잘못된 경로 구성, 잘못된 VLAN 구성, 디버그 메시지로 인해 uni/tn-Prod1/ap-App1/epg-EPG-Web 노드 101 101\_102\_eth1\_9에 대한 구성이 실패했습니다. 잘못된 vlan: vlan-1501: 캡슐화 대상 STP 세그먼트 ID가 없습니다. EPG가 도메인과 연결되지 않았거나 도메인에 이 VLAN이 할당되지 않았습니다. 잘못된 경로: vlan-1501: EPG 및 포트 둘 다와 연결된 필수 VLAN이 있는 도메인이 없습니다.

위의 fault 설명에서 fault의 원인이 될 수 있는 몇 가지 명확한 징후가 있습니다. 액세스 정책 관계를 확인하고 EPG에 대한 도메인 연결을 확인하라는 경고가 있습니다.

위에서 설명한 시나리오에서 빠른 시작 보기를 검토하면 액세스 정책에 VLAN이 누락되어 있는 것이 분명합니다.

**101-102, Int 1/9 VPC에 VLAN이 없는 빠른 시작 보기**

# Configure Interface, PC, and VPC

## Configured Switch Interfaces

Switches	Interfaces	IF Type	Attached Device Type
101-102			
	1/11	Individual	ESX (VLANs: 1001-1100)
	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

항목에 VLAN ID에 대한 참조가 없습니다.

수정하면 빠른 시작 보기에 '(VLAN 1500-1510)'이 표시됩니다.

**101-102, Int 1/9 VPC에 베어 메탈(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

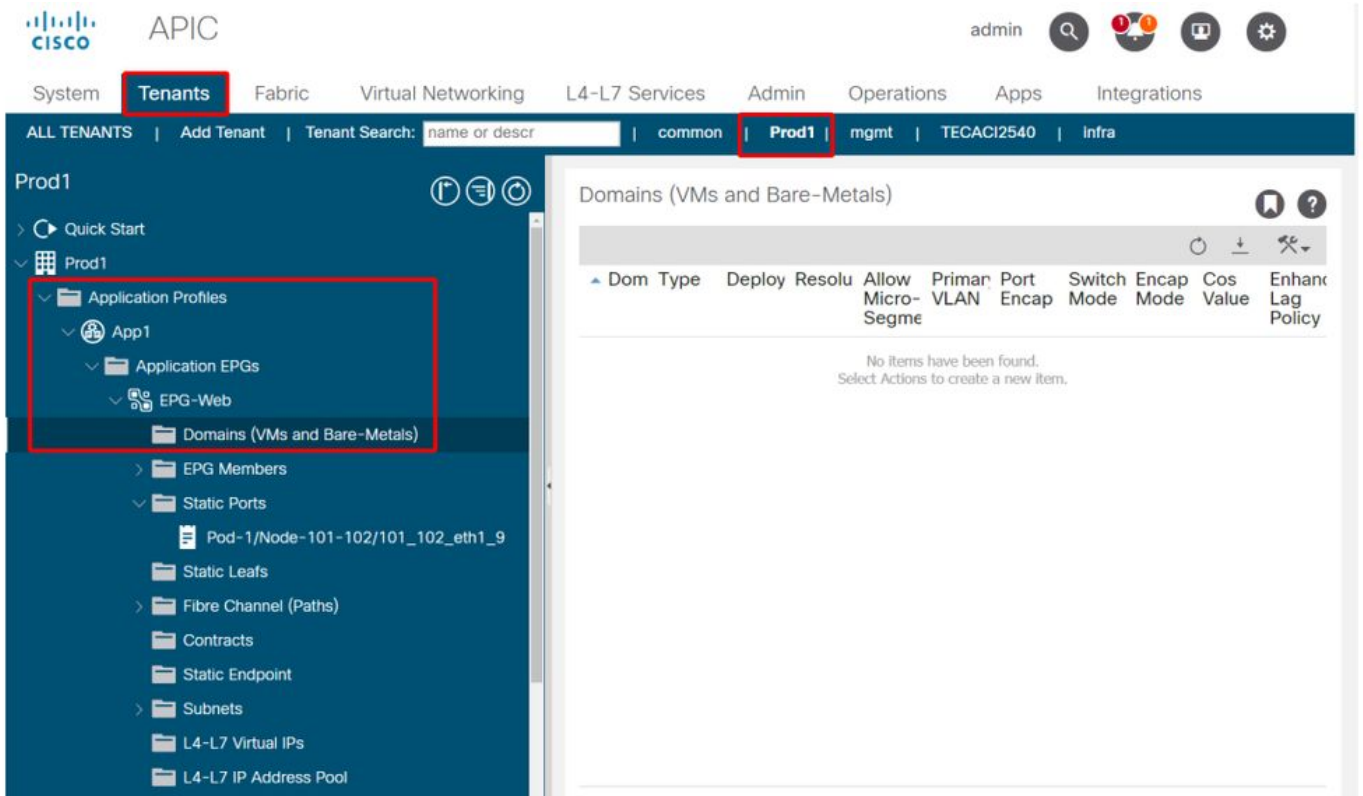
그러나 EPG 결함은 결함 F0467에 대해 업데이트된 다음 설명과 함께 여전히 존재합니다.

#### 결함: F0467

**설명:** 결함 대리인: 잘못된 경로 구성으로 인해 uni/tn-Prod1/ap-App1/epg-EPG-Web node 101 101\_102\_eth1\_9에 대한 컨피그레이션이 실패했습니다. 디버그 메시지: 잘못된 경로: vlan-150: EPG 및 포트 모두에 연결된, 필요한 VLAN이 있는 도메인은 없습니다.

위의 업데이트된 fault에서 EPG 도메인 연결을 확인하여 EPG에 연결된 도메인이 없음을 확인합니다.

EPG-Web에 정적 포트 연결이 있지만 도메인 연결이 없습니다.



VLAN 1501을 포함하는 도메인이 EPG에 연결되면 더 이상 오류가 발생하지 않습니다.

## 시나리오 2: EPG 고정 포트 또는 L3Out SVI(Logical Interface Profile)에 배포할 경로로 VPC를 선택할 수 없습니다.

VPC를 EPG 고정 포트 또는 L3Out 논리 인터페이스 프로파일 SVI 항목의 경로로 구성하려고 시도하는 동안에는 구축할 특정 VPC가 사용 가능한 옵션으로 표시되지 않습니다.

VPC 정적 바인딩을 구축하려고 시도할 때 두 가지 하드 요구 사항이 있습니다.

1. 문제의 리프 스위치 쌍에 대해 VPC 명시적 보호 그룹을 정의해야 합니다.
2. 전체 액세스 정책 매핑을 정의해야 합니다.

위의 그림과 같이 빠른 시작 보기에서 두 요구 사항을 모두 확인할 수 있습니다. 둘 다 완전하지 않으면 VPC는 정적 포트 바인딩에 사용 가능한 옵션으로 표시되지 않습니다.

## 시나리오 3: 결합 F0467 - 다른 EPG에서 패브릭 캡슐화 기능이 이미 사용됨

기본적으로 VLAN에는 전역 범위가 있습니다. 즉, 지정된 VLAN ID는 지정된 리프 스위치의 단일 EPG에만 사용할 수 있습니다. 지정된 리프 스위치 내의 여러 EPG에서 동일한 VLAN을 재사용하려는 경우 다음 오류가 발생합니다.

**결함:** F0467

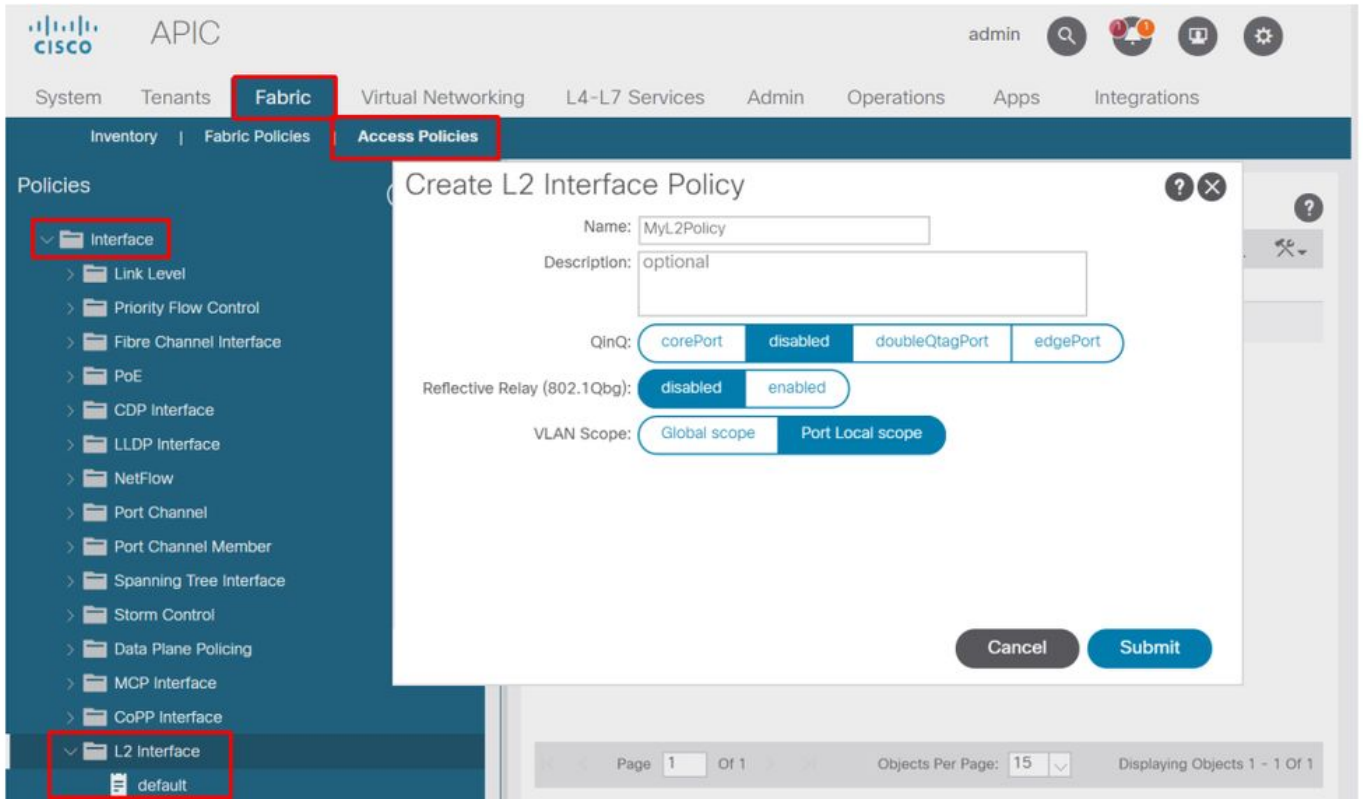
**설명:** 결함 대리인: 다른 EPG에서 이미 사용된 캡슐화 때문에 uni/tn-Prod1/ap-App1/epg-EPG-BusinessApp 노드 102 101\_102\_eth1\_8에 대한 컨피그레이션이 실패했습니다. 디버그 메시지: encap-already-in-use: Encap은 Prod1:App1:EPG-Web에서 이미 사용 중입니다.

다른 VLAN을 선택하는 것 외에도 이 컨피그레이션을 작동하게 하는 또 다른 옵션은 '포트 로컬' VLAN 범위의 사용을 고려하는 것입니다. 이 범위를 사용하면 VLAN을 인터페이스별로 매핑할 수 있습니다. 즉, VLAN-1501을 동일한 리프에 있는 여러 인터페이스에서 서로 다른 EPG에 사용할 수

있습니다.

'포트 로컬' 범위는 정책 그룹 단위로(특히 L2 정책을 통해) 연결되지만 리프 레벨에서 적용됩니다.

## APIC GUI 내에서 'VLAN 범위' 설정을 변경할 위치



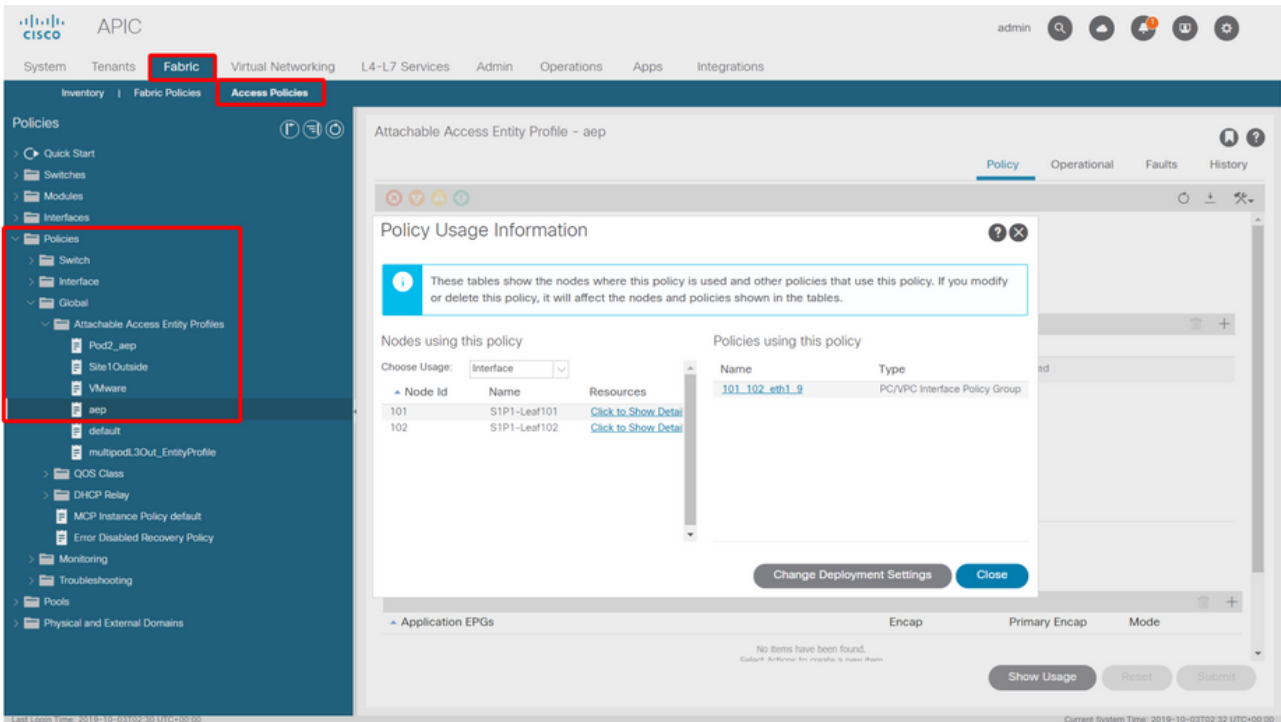
'포트 로컬' VLAN 범위 컨피그레이션을 구현하기 전에 Cisco.com의 "Cisco APIC Layer 2 네트워킹 컨피그레이션 가이드"를 검토하여 제한 사항과 설계 제한이 원하는 사용 사례 및 설계에 적합한지 확인합니다.

## 특별 언급

### 사용 표시

액세스 정책에 특정하지는 않지만 GUI에서 'Show Usage'(사용량 표시)라는 레이블이 지정된 대부분의 객체에서 버튼을 사용할 수 있습니다. 이 단추는 선택한 개체에 루트가 있는 정책 조회를 수행하여 어떤 리프 노드/인터페이스가 직접적인 관계를 가지는지 확인합니다. 이는 일반적인 조회 시나리오뿐만 아니라 특정 객체 또는 정책이 사용 중인지 여부를 파악하는 데 유용합니다.

아래 스크린샷에서는 선택한 AEP가 서로 다른 두 인터페이스에서 사용되고 있습니다. 이는 AEP를 수정하면 연결된 인터페이스에 직접적인 영향을 미칠 것임을 의미합니다.



## 중복 VLAN 풀

액세스 정책의 기능은 특정 VLAN을 인터페이스에 구축할 수 있도록 하는 것이지만, 설계 단계에서 반드시 고려해야 할 추가 사용법이 있습니다. 특히 도메인은 외부 캡슐화에 연결된 VXLAN ID(Fabric Encap이라고 함)를 계산하는 데 사용됩니다. 이 기능은 일반적으로 데이터 플레인 트래픽과 큰 관련이 없지만, 이러한 ID는 스페닝 트리 BPDU를 포함하여 패브릭을 통해 플러딩되는 프로토콜의 하위 집합과 특히 관련이 있습니다. leaf1에서 인그레스하는 VLAN-<id> BPDU가 leaf 2를 이그레스(egress)할 것으로 예상되는 경우(예: ACI를 통해 스페닝 트리를 수렴하는 레거시 스위치가 있는 경우), VLAN-<id>은(는) 두 leaf 노드에서 동일한 패브릭 캡슐화를 가져야 합니다. 동일한 액세스 VLAN에 대해 패브릭 캡슐화 값이 다르면 BPDU가 패브릭을 통과하지 않습니다.

이전 섹션에서 언급한 것처럼, 각 도메인이 고유한 리프 스위치 집합에만 적용되도록 특별히 주의하지 않는 한 여러 도메인(예: VMM 대 물리적)에서 동일한 VLAN을 구성하지 마십시오. 지정된 VLAN에 대해 동일한 리프 스위치에서 두 도메인을 확인할 수 있는 순간, 업그레이드(또는 정상 다시 로드) 후 기본 VXLAN을 변경할 수 있습니다. 그러면 STP 컨버전스 문제가 발생할 수 있습니다. 이 동작은 VXLAN ID를 결정하기 위해 다음 수식에서 사용되는 고유한 숫자 값('base' 특성)을 갖는 각 도메인의 결과입니다.

**VXLAN VNID = 기본 + (encap — from\_encap)**

지정된 leaf에 푸시되는 도메인을 확인하려면 'stpAllocEncapBlkDef' 클래스에 대해 moquery를 실행할 수 있습니다.

```
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
```

이 출력에서 다음 액세스 정책 정의를 식별합니다.

- VLAN 1500-1510을 명시적으로 정의하는 VLAN 블록이 포함된 프로그래밍된 VLAN 풀이 있습니다.
- 이 VLAN 블록은 'physvlans'라는 도메인에 연결됩니다.
- VXLAN 계산에 사용되는 기본 값은 8492입니다.
- VLAN-1501에 대한 결과 VXLAN 계산은 패브릭 캡슐화로서  $8492 + (1501-1500) = 8493$ 이 됩니다.

결과 VXLAN ID(이 예에서는 8493)는 다음 명령으로 확인할 수 있습니다.

```
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

동일한 leaf에 푸시되는 VLAN-1501이 포함된 다른 VLAN 풀이 있는 경우, 업그레이드 또는 클린 다시 로드하면 고유한 기본 값(및 이후에 다른 Fabric Encap)이 확보될 수 있으며, 이로 인해 BPDU가 VLAN-1501에서 BPDU를 수신할 다른 leaf로 만들지 못하게 됩니다.



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.