Probleemoplossing voor ACI-toegangsbeleid

Inhoud

Inleiding

Dit document beschrijft stappen om ACI-toegangsbeleid te begrijpen en problemen op te lossen.

Achtergrondinformatie

Het materiaal van dit document is afgeleid uit het boek Problemen oplossen van Cisco Application Centric Infrastructure, Second Edition, met name het **Access Policies - Overview** and **Access Policies - Troubleshooting Workflow** hoofdstukken.

Overzicht van toegangsbeleid

Hoe vormt de ACI-beheerder een VLAN op een poort in de stof? Hoe begint de ACI-beheerder

fouten in verband met toegangsbeleid aan te pakken? In deze sectie wordt uitgelegd hoe u problemen met betrekking tot beleid voor fabric access kunt oplossen.

Alvorens in het oplossen van problemen scenario's te springen, is het noodzakelijk dat de lezer een goed inzicht in hoe het toegangsbeleid en hun verhoudingen binnen het ACI Objectmodel functioneren heeft. Voor dit doel kan de lezer zowel de "ACI Policy Model" (ACI-beleidsmodel) als de "APIC Management Information Model Reference" (APIC Management Information Model Reference) documenten raadplegen op Cisco.com (https://developer.cisco.com/site/apic-mim-ref-api/).

De functie van toegangsbeleid is specifieke configuratie op de downlink-poorten van een switch toe te laten. Alvorens het huurdersbeleid wordt bepaald om verkeer door een ACI stoffenhaven toe te staan, zou het verwante toegangsbeleid op zijn plaats moeten zijn.

Doorgaans wordt een toegangsbeleid gedefinieerd wanneer er nieuwe switches aan de stof worden toegevoegd of wanneer een apparaat is aangesloten op ACI-bladkoppelingen; maar afhankelijk van hoe dynamisch een omgeving is, kan het toegangsbeleid worden gewijzigd tijdens de normale werking van de stof. Bijvoorbeeld, om een nieuwe reeks VLAN's toe te staan of een nieuw Routed Domain toe te voegen aan fabric access poorten.

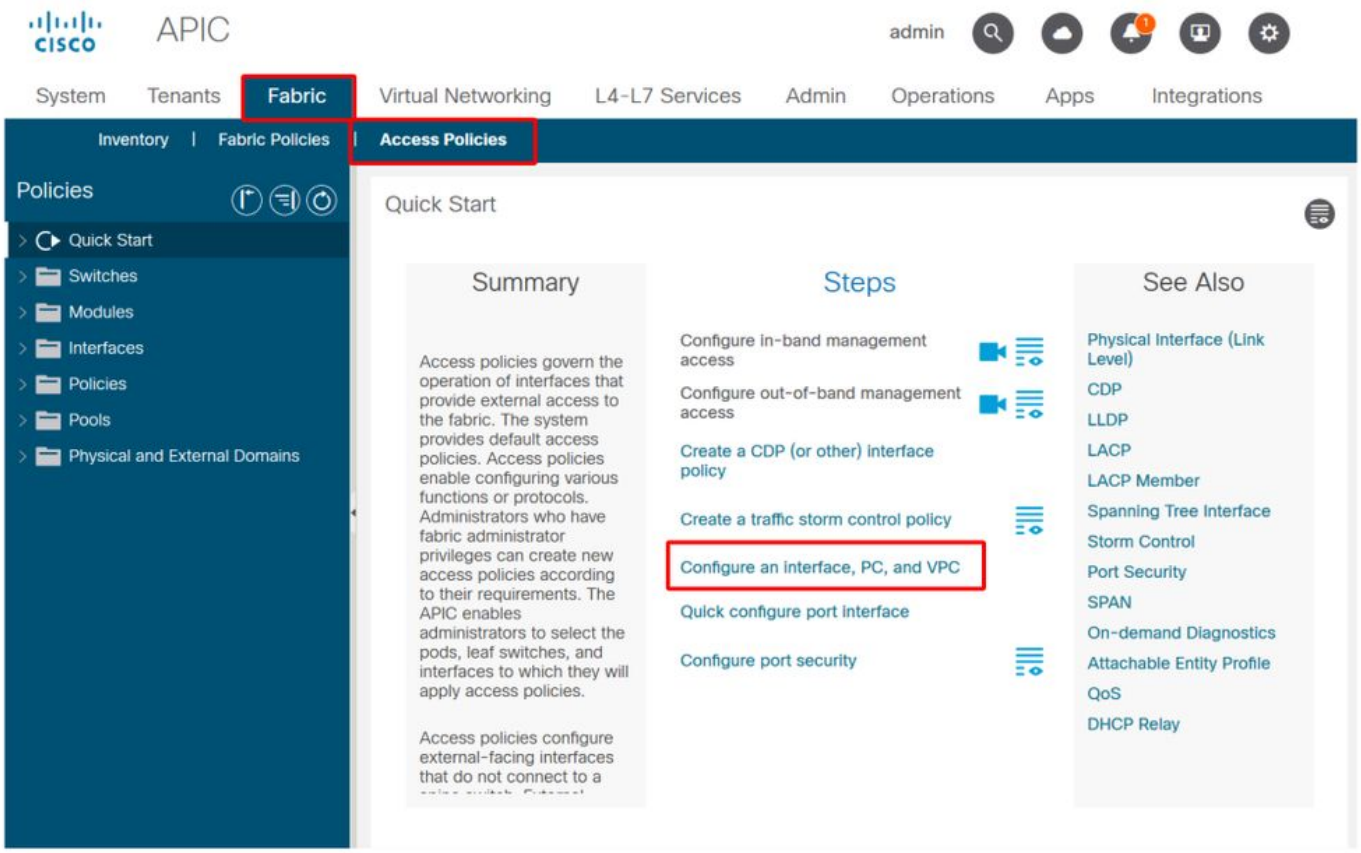
Het ACI-toegangsbeleid is in eerste instantie een beetje intimiderend, maar is uiterst flexibel en is ontworpen om de provisioning van configuratie naar een grootschalig SDN-netwerk in continue evolutie te vereenvoudigen.

Configuratie van toegangsbeleid: Methodologie

Toegangsbeleid kan onafhankelijk van elkaar worden geconfigureerd, d.w.z. door alle benodigde objecten onafhankelijk te maken, of kan worden gedefinieerd via de talrijke wizards die door de ACI GUI worden geleverd.

Wizards zijn zeer behulpzaam omdat ze de gebruiker door de workflow begeleiden en ervoor zorgen dat alle vereiste beleidsregels zijn.

Toegangsbeleid — Snelle start wizard

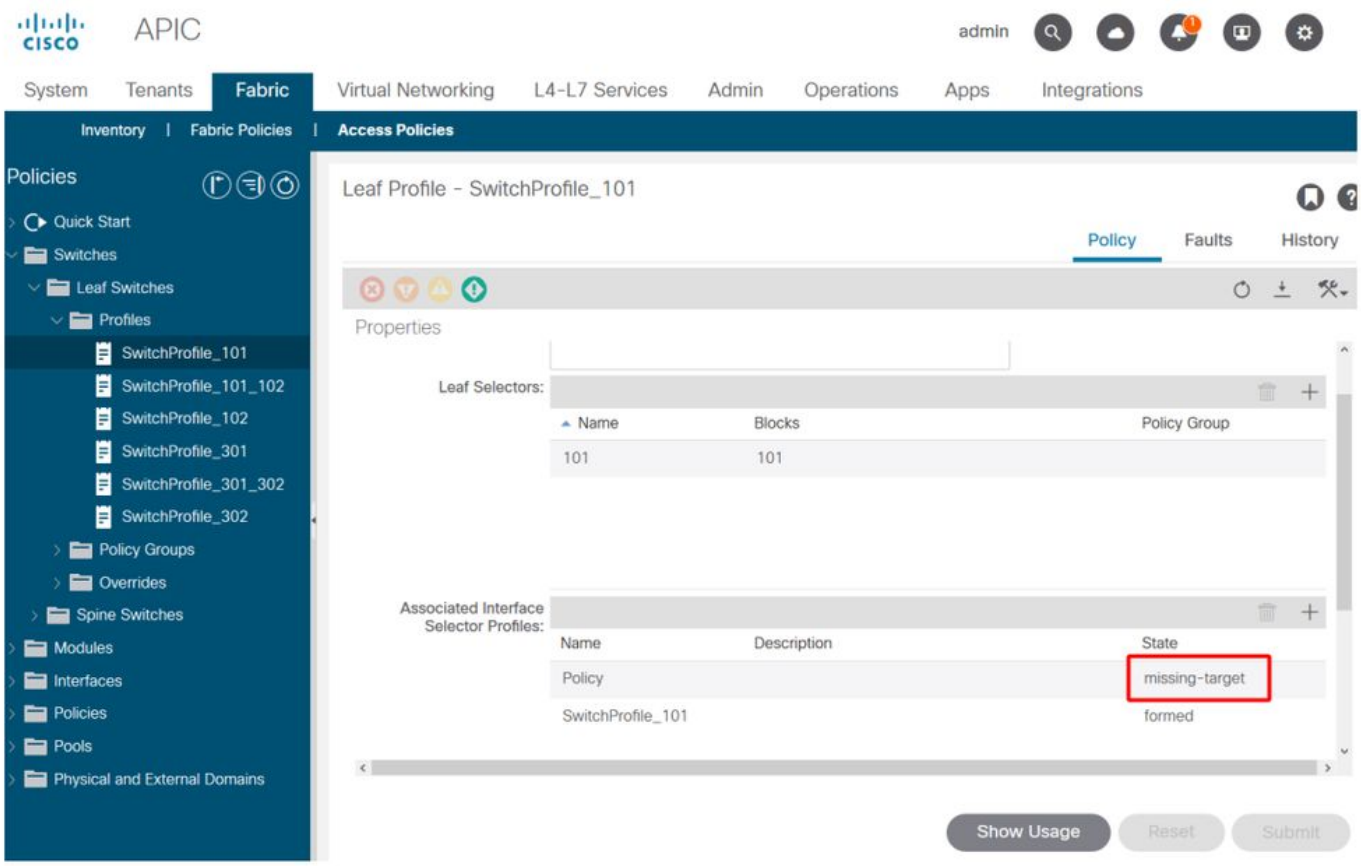


De bovenstaande afbeelding toont de pagina Snel starten, waar u meerdere wizards kunt vinden.

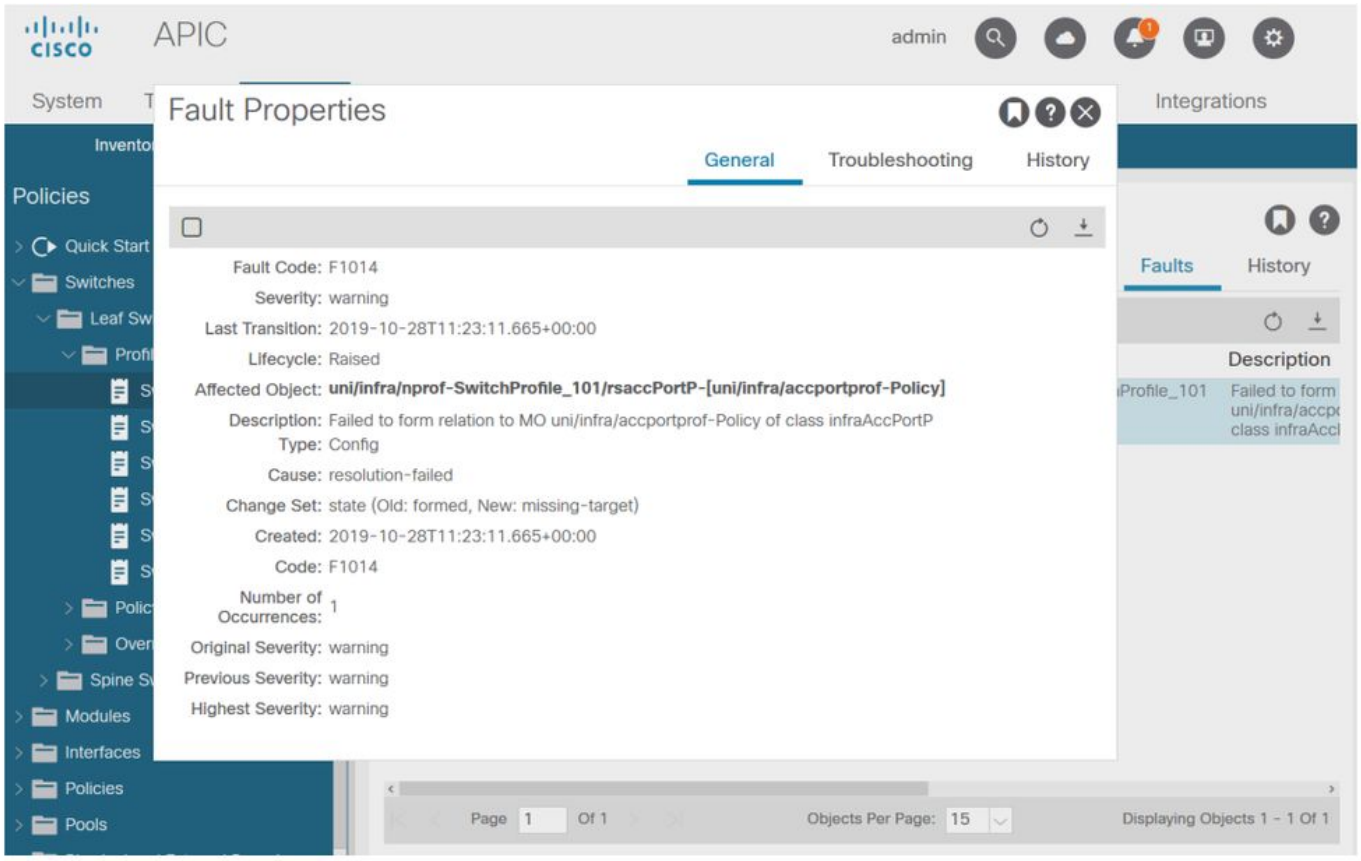
Zodra een toegangsbeleid wordt bepaald, is de generische aanbeveling het beleid te bevestigen door ervoor te zorgen alle bijbehorende voorwerpen geen fout tonen.

In de onderstaande afbeelding heeft een Switch Profile bijvoorbeeld een Interface Selector Policy toegewezen die niet bestaat. Een attente gebruiker kan eenvoudig de '**missing-target**'-status van het object waarnemen en controleren of een fout in de GUI is gemarkeerd:

Bladprofiel — SwitchProfile_101



Bladprofiel — SwitchProfile_101 — Fault



In dit geval zou het corrigeren van de fout net zo eenvoudig zijn als het maken van een nieuw Interface Selector Profile genaamd 'Policy'.

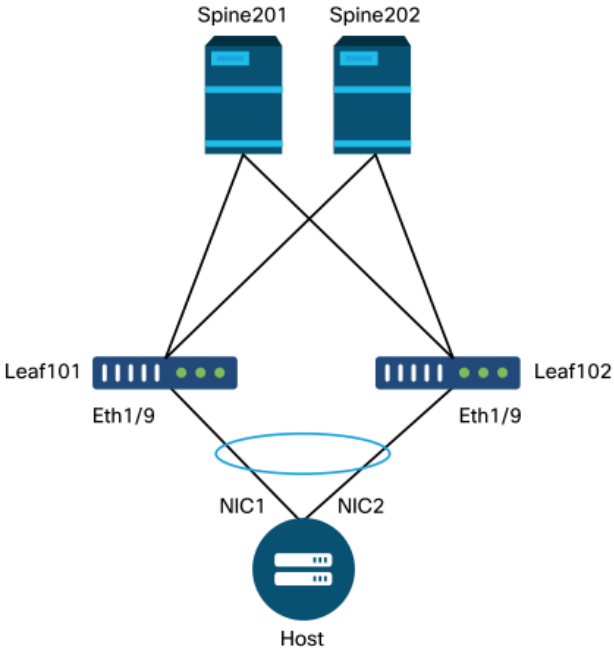
De handmatige configuratie van basistoegangsbeleid wordt in de volgende alinea's besproken.

Toegangsbeleid handmatige basisconfiguraties

Bij het opstellen van toegangsbeleid, worden de voorwerpen bepaald om het voorgenomen gebruik van de bepaalde downlinks uit te drukken. De verklaring die de downlinks programmeert (bv. de statische toewijzing van EPG-poorten), berust op deze uitdrukkelijke bedoeling. Dit helpt om de configuratie te schalen en logischerwijs soortgelijke gebruiksobjecten te groeperen, zoals switches of poorten die specifiek verbonden zijn met een bepaald extern apparaat.

Verwijs naar de topologie hieronder voor de rest van dit hoofdstuk.

Topologie van toegangsbeleid definitie voor dual-homed server

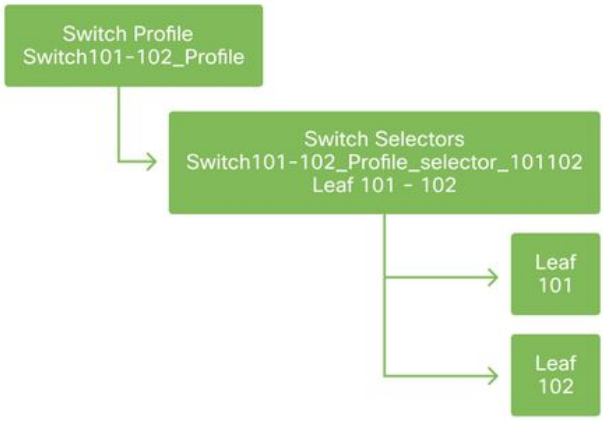


Een webserver is verbonden met een ACI-fabric. De webserver heeft 2 Network Interface Cards (NIC's) die zijn geconfigureerd in een LACP-poortkanaal. De webserver is verbonden met poort 1/9 van bladzijden switches 101 en 102. De webserver is afhankelijk van VLAN-1501 en moet zich bevinden in het EPG 'EPG-Web'.

Het Switch-beleid configureren

De eerste logische stap is om te definiëren welke blad switches zullen worden gebruikt. Het 'Switch Profile' zal 'Switch Selectors' bevatten die de te gebruiken bladknooppunt ID's definiëren.

Switch



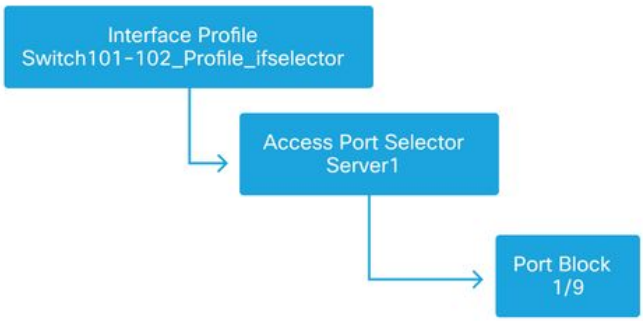
Het is aan te raden om 1 Switch Profile per individuele leaf switch en 1 Switch Profile per VPC domein pair te configureren, met behulp van een naamgevingsschema dat de knooppunten aangeeft die deel uitmaken van het profiel.

De Quick Start implementeert een logische naamgevingsschema die het gemakkelijk te begrijpen maakt waar het wordt toegepast. De voltooide naam volgt de indeling 'Switch<node-id>_Profile'. Als voorbeeld, 'Switch 101_Profile' zal zijn voor een switch profiel dat bladknooppunt 101 en Switch 101-102_Profile bevat voor een Switch Profiel dat bladknooppunten 101 en 102 bevat die deel zouden moeten uitmaken van een VPC-domein.

Het interfacebeleid configureren

Zodra het toegangsbeleid voor de switch is gemaakt, zou het definiëren van de interfaces de volgende logische stap zijn. Dit gebeurt door een 'interfaceprofiel' te maken dat bestaat uit 1 of meer 'Access Port Selectors' die de 'Port Block'-definities bevatten.

Interfacebeleid



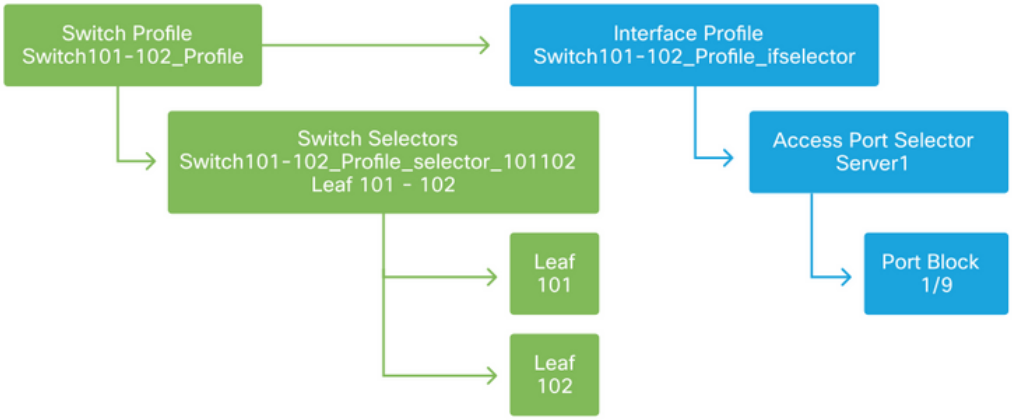
Om de relatie tussen het 'interfaceprofiel' en de betrokken switch Switches te vormen, koppelt u het 'interfaceprofiel' aan het 'interfaceprofiel'.

'Interfaceprofielen' kunnen op vele manieren worden gedefinieerd. Gelijkaardig aan "Switch Profiles", kan één enkel "InterfaceProfiel"per fysische switch samen met een "InterfaceProfiel"per VPC domein worden tot stand gebracht. Dit beleid moet vervolgens een 1-op-1-omzetting naar het corresponderende switch-profiel hebben. Volgens deze logica wordt het beleid voor toegang tot de stof sterk vereenvoudigd, wat het voor andere gebruikers gemakkelijk maakt om te begrijpen.

De standaard naamgevingsschema's van de Quick Start kunnen hier ook gebruikt worden. Het volgt de '<switch profile name>_ifselector' format om aan te geven dat dit profiel gebruikt wordt om

interfaces te selecteren. Een voorbeeld is 'Switch 101_Profile_ifselector'. Dit voorbeeld 'Interfaceprofiel' zou worden gebruikt om niet VPC-interfaces te configureren op bladzijde switch 101 en zou alleen worden gekoppeld aan het 'Switch 101_Profile' toegangsbeleid.

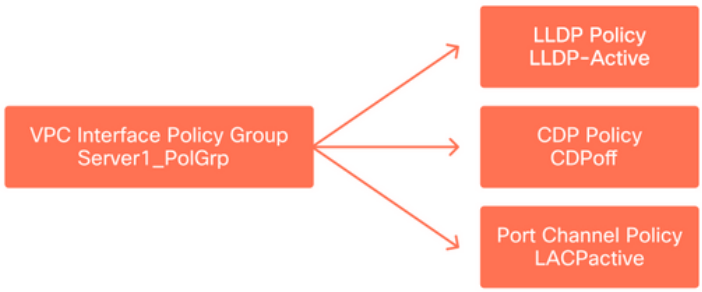
Switch-profiel gekoppeld aan interfaceprofiel



Merk op dat aangezien een 'interfaceprofiel' met Eth 1/9 is verbonden met een 'Switch Profile' dat zowel switch 101 als 102 omvat, de levering Eth1/9 op beide knooppunten gelijktijdig begint.

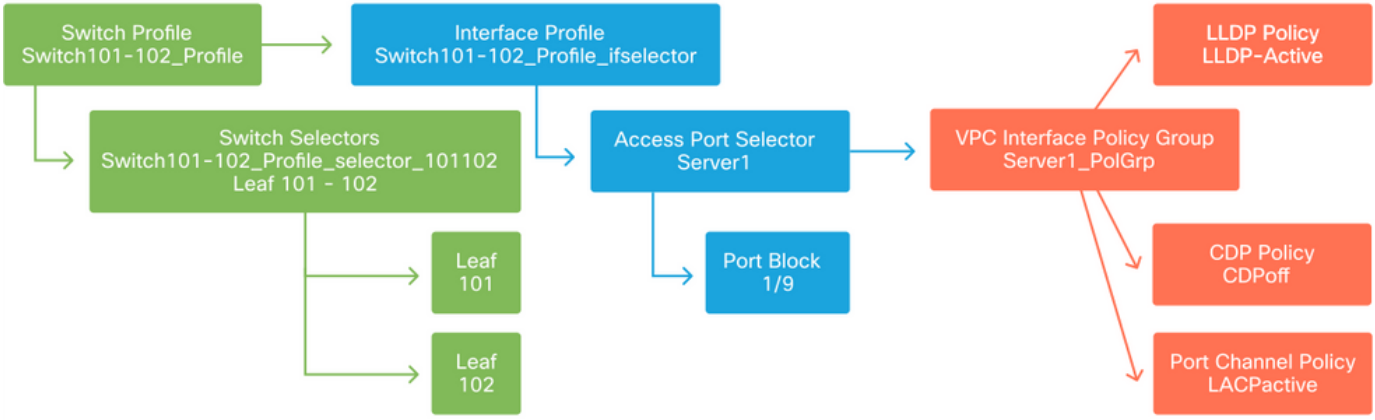
Op dit moment zijn de switches en hun havens gedefinieerd. De volgende logische stap zou zijn de kenmerken van deze havens te definiëren. De 'Interfacebeleidsgroep' maakt het mogelijk deze poorteigenschappen te definiëren. Er zal een 'VPC Interface Policy Group' worden opgericht om de bovengenoemde LACP-poortkanaal mogelijk te maken.

Beleidsgroep



De 'VPC Interface Policy Group' wordt gekoppeld aan de 'Interface Policy Group' van de 'Access Port Selector' om de relatie van bladrelatie/switch tot poorteigenschappen te vormen.

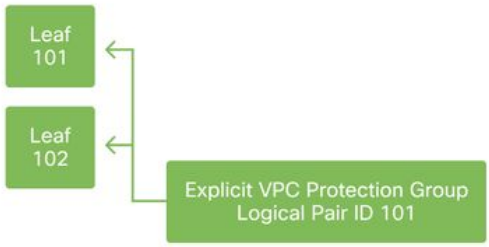
Switch- en interfaceprofielen gecombineerd



De VPC configureren

Om het LACP-poortkanaal over 2 switches te creëren, moet een VPC-domein worden gedefinieerd tussen switch 101 en 102. Dit gebeurt door een "VPC Protection Group" tussen de twee switches te definiëren.

VPC



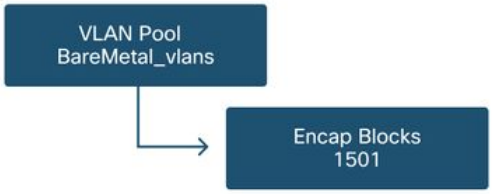
VLAN-pools configureren

De volgende logische stap zal het maken van de VLAN's zijn die op deze poort zullen worden gebruikt, in dit geval VLAN-1501. De definitie van een 'VLAN Pool' met 'Encap Blocks' completeert deze configuratie.

Wanneer u de grootte van VLAN-poolbereiken in overweging neemt, houdt u in gedachten dat de meeste implementaties slechts één VLAN-pool en één extra pool nodig hebben als u VMM-integratie gebruikt. Om VLAN's van een legacy-netwerk naar ACI te brengen, definieert u het bereik van legacy VLAN's als een statische VLAN-pool.

Als voorbeeld, veronderstel VLANs 1-2000 in een erfenismilieu worden gebruikt. Maak één statische VLAN-pool die VLAN's 1-2000 bevat. Hierdoor kunnen ACI Bridge Domains en EPG's naar de legacy-structuur worden gedraaid. Als u VMM implementeert, kan een tweede dynamische pool worden gemaakt met behulp van een reeks gratis VLAN-ID's.

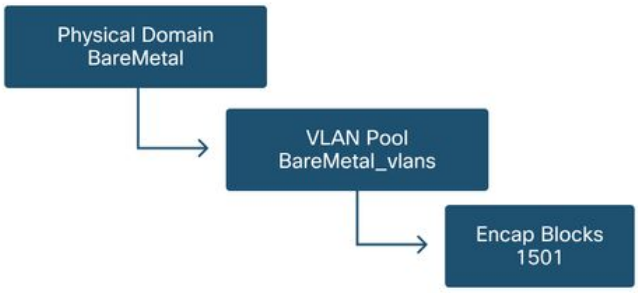
VLAN-pool



Domeinen configureren

De volgende logische stap is het creëren van een 'Domein'. Een 'Domein' definieert het bereik van een VLAN-pool, d.w.z. waar die pool wordt toegepast. Een 'domein' kan fysiek, virtueel of extern zijn (overbrugd of gerouteerd). In dit voorbeeld zal een 'Physical Domain' worden gebruikt om een kale metaalserver met de stof te verbinden. Dit 'domein' wordt gekoppeld aan de 'VLAN-pool' om het vereiste VLAN toe te staan.

Fysieke domeinen



Voor de meeste implementaties is één 'Physical Domain' voldoende voor bare metal implementaties en één 'Routed Domain' is voldoende voor L3Out implementaties. Beide kunnen worden toegewezen aan dezelfde 'VLAN Pool'. Als de stof op een multi-tenancy manier wordt opgesteld, of als meer korrelige controle wordt vereist om te beperken welke gebruikers specifieke EPGs & VLANs op een haven kunnen opstellen, zou een strategischer toegangsbeleidsontwerp moeten worden overwogen.

'Domains' bieden ook de functionaliteit om de toegang van gebruikers tot beleid te beperken met 'Security Domains' met behulp van Roles Based Access Control (RBAC).

Wanneer u VLAN's op een switch implementeert, zal ACI overspanningsbommen inkapselen met een unieke VXLAN-id die is gebaseerd op het domein waar VLAN vandaan kwam. Daarom is het belangrijk om hetzelfde domein te gebruiken wanneer apparaten worden aangesloten die STP-communicatie met andere bruggen vereisen.

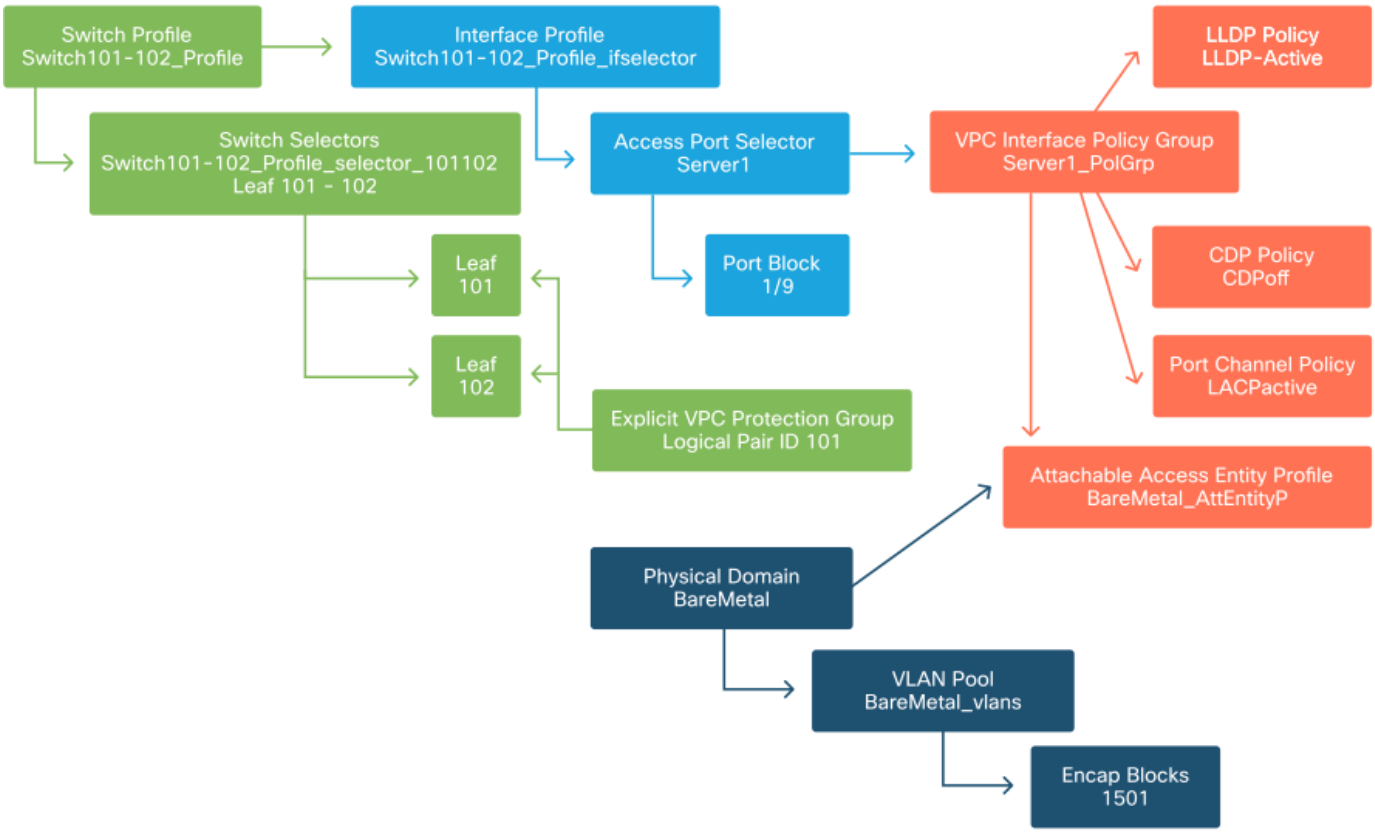
VLAN VXLAN ID's worden ook gebruikt om VPC-switches in staat te stellen VPC-geleerde MAC- en IP-adressen te synchroniseren. Daarom is het eenvoudigste ontwerp voor VLAN-pools om één pool te gebruiken voor statische implementaties en een tweede pool te maken voor dynamische implementaties.

Het Attachable Access Entity Profile (AEP) configureren

Twee belangrijke stukken van de configuratie van het toegangsbeleid zijn nu voltooid; de switch- en interfacedefinities en de domeinen/VLAN's. Een object met de naam 'Attachable Access Entity Profile' (AEP) zal dienen om deze twee blokken aan elkaar te koppelen.

Een "beleidsgroep" is verbonden met een AEP in een één-op-veel-relatie, waardoor de AEP groepsinterfaces en switches kan combineren die vergelijkbare beleidsvereisten delen. Dit betekent dat slechts één AEP moet worden vermeld wanneer een groep interfaces op specifieke switches wordt vertegenwoordigd.

Bijgevoegd profiel van toegangsentiteit



In de meeste implementaties moet één AEP worden gebruikt voor statische paden en één extra AEP per VMM-domein.

De belangrijkste overweging is dat VLAN's op interfaces via het AEP kunnen worden ingezet. Dit kan worden gedaan door EPG's rechtstreeks aan een AEP toe te wijzen of door een VMM-domein te configureren voor preprovisioning. Beide configuraties maken van de bijbehorende interface een trunkpoort ("switchport mode trunk" op legacy switches).

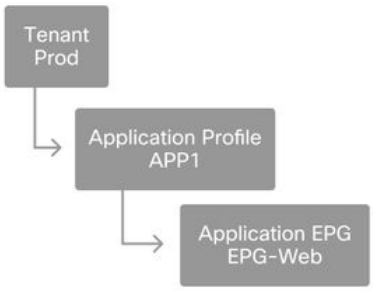
Daarom is het belangrijk om een afzonderlijke AEP voor L3Out te maken wanneer routed-poorten of routed-subinterfaces worden gebruikt. Als in de L3Out SVI's worden gebruikt, is het niet nodig om een extra AEP te creëren.

De huurder, APP en EPG configureren

ACI maakt gebruik van een andere methode om connectiviteit te definiëren aan de hand van een beleidsgebaseerde benadering.

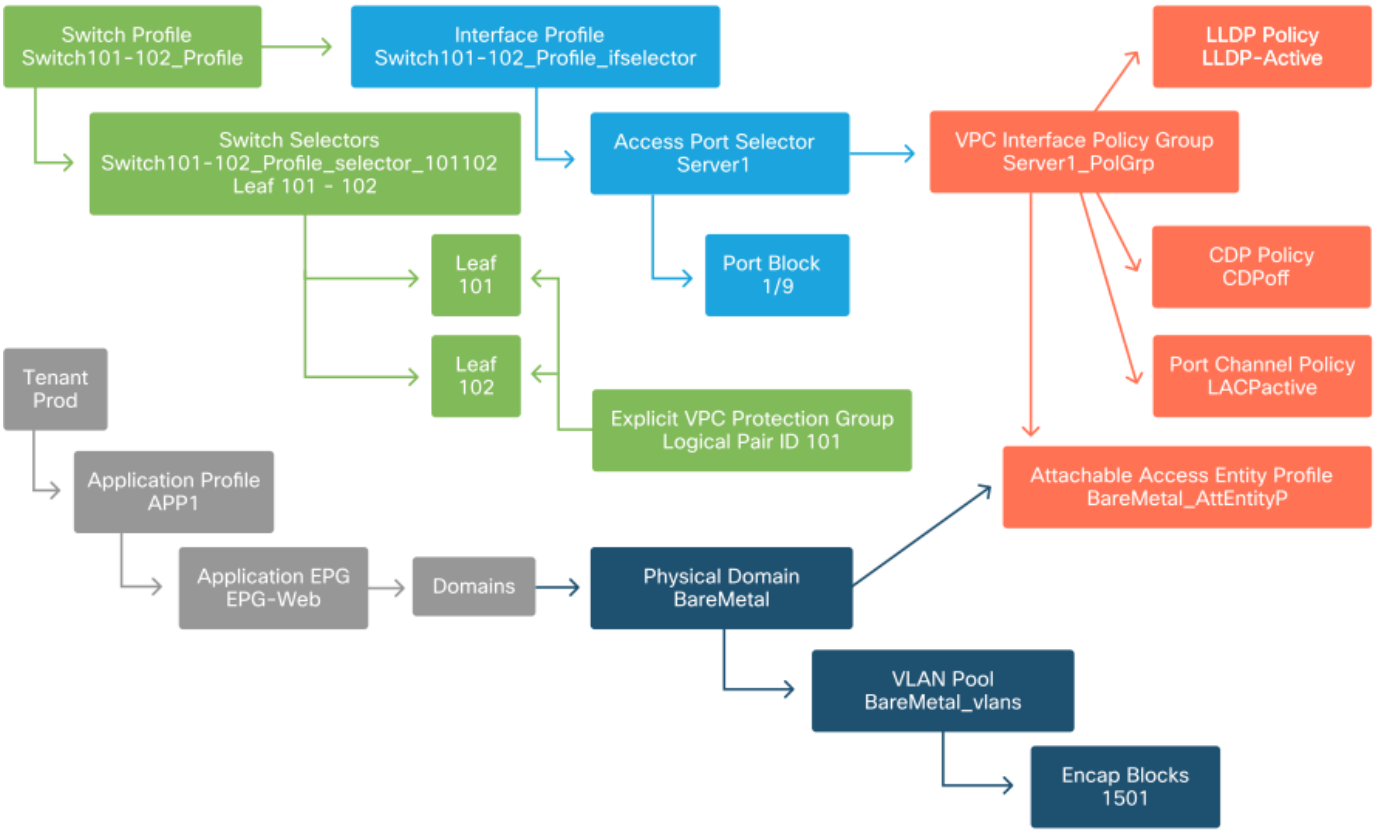
Het object met het laagste niveau wordt een 'Endpoint Group' (EPG) genoemd. De EPG-constructie wordt gebruikt om een groep VM's of servers (endpoints) met soortgelijke beleidsvereisten te definiëren. 'Toepassingsprofielen', die onder een huurder bestaan, worden gebruikt om EPG's logisch samen te voegen.

Huurder, APP en EPG



De volgende logische stap is de EPG te koppelen aan het domein. Dit creëert de koppeling tussen het logische object dat onze werklast vertegenwoordigt, de EPG, en de fysieke switches/interfaces, het toegangsbeleid.

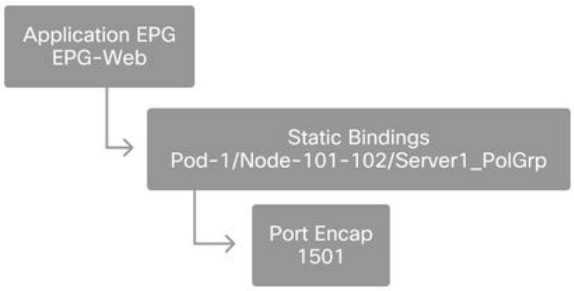
EPG naar domein link



De statische EPG-banden configureren

De laatste logische stap is het VLAN te programmeren op een switch-interface voor een bepaalde EPG. Dit is vooral belangrijk bij het gebruik van een fysiek domein, aangezien dit type domein een expliciete verklaring vereist om dit te doen. Hierdoor kan de EPG uit de stof worden uitgebreid en kan de kale metaalserver in de EPG worden geclassificeerd.

Statische banden

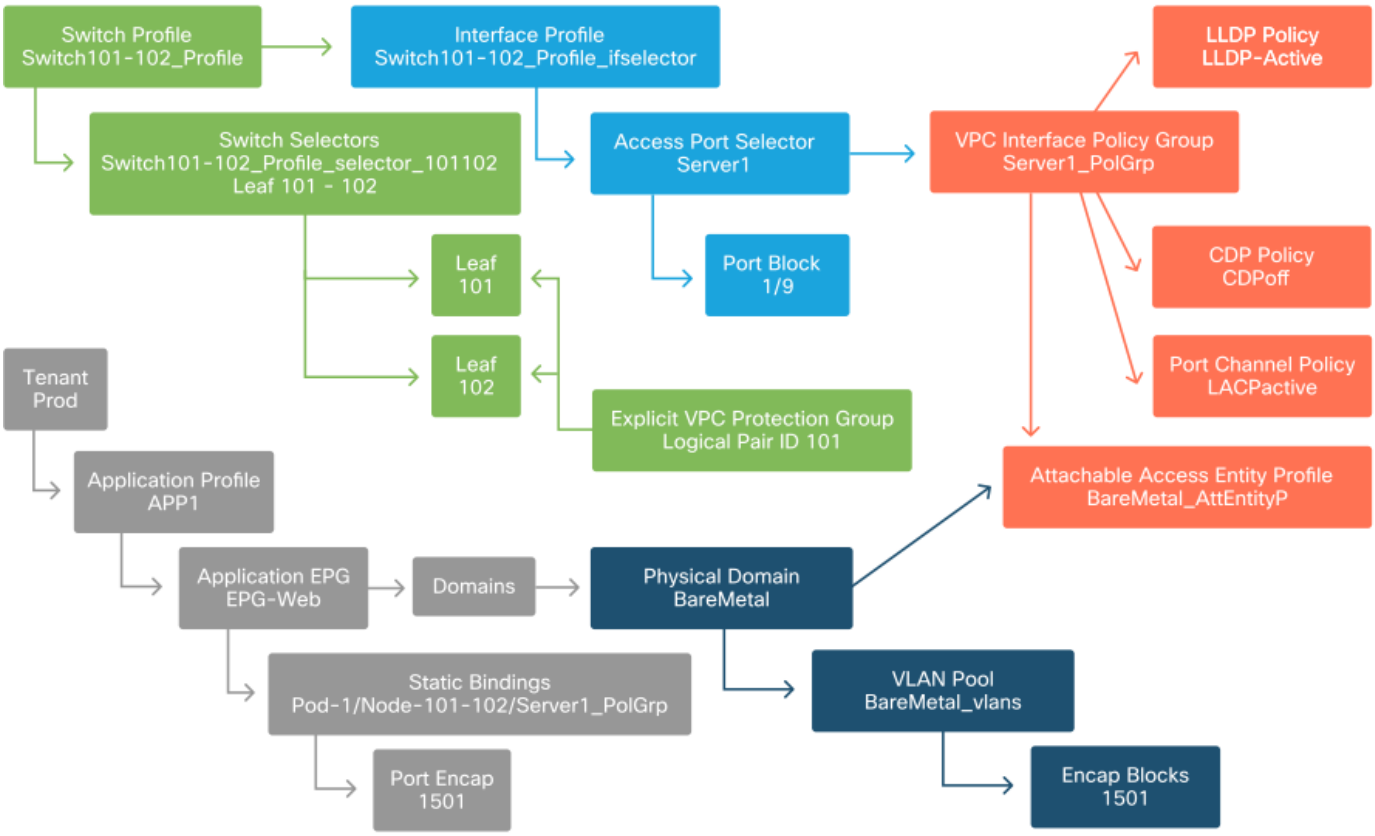


De genoemde 'Port Encap' moet oplosbaar zijn tegen de 'VLAN Pool'. Is dit niet het geval, dan wordt een fout gemarkeerd. Dit wordt besproken in de sectie "Problemen oplossen" van dit hoofdstuk.

Samenvatting van de configuratie van het toegangsbeleid

In het volgende diagram worden alle objecten samengevat die zijn gemaakt om connectiviteit voor de host mogelijk te maken via VLAN-1501, met behulp van een VPC-verbinding met switch 101 en 102.

Bare-metal ACI-connectiviteit



Aanvullende servers aansluiten

Wat zou het betekenen om, nu alle vorige beleidslijnen zijn gecreëerd, één extra server op poort Eth1/10 op switches 101 en 102 te verbinden met een poortkanaal?

Onder verwijzing naar het "Bare-metal ACI connectiviteit"-diagram, moet het volgende minimaal worden gecreëerd:

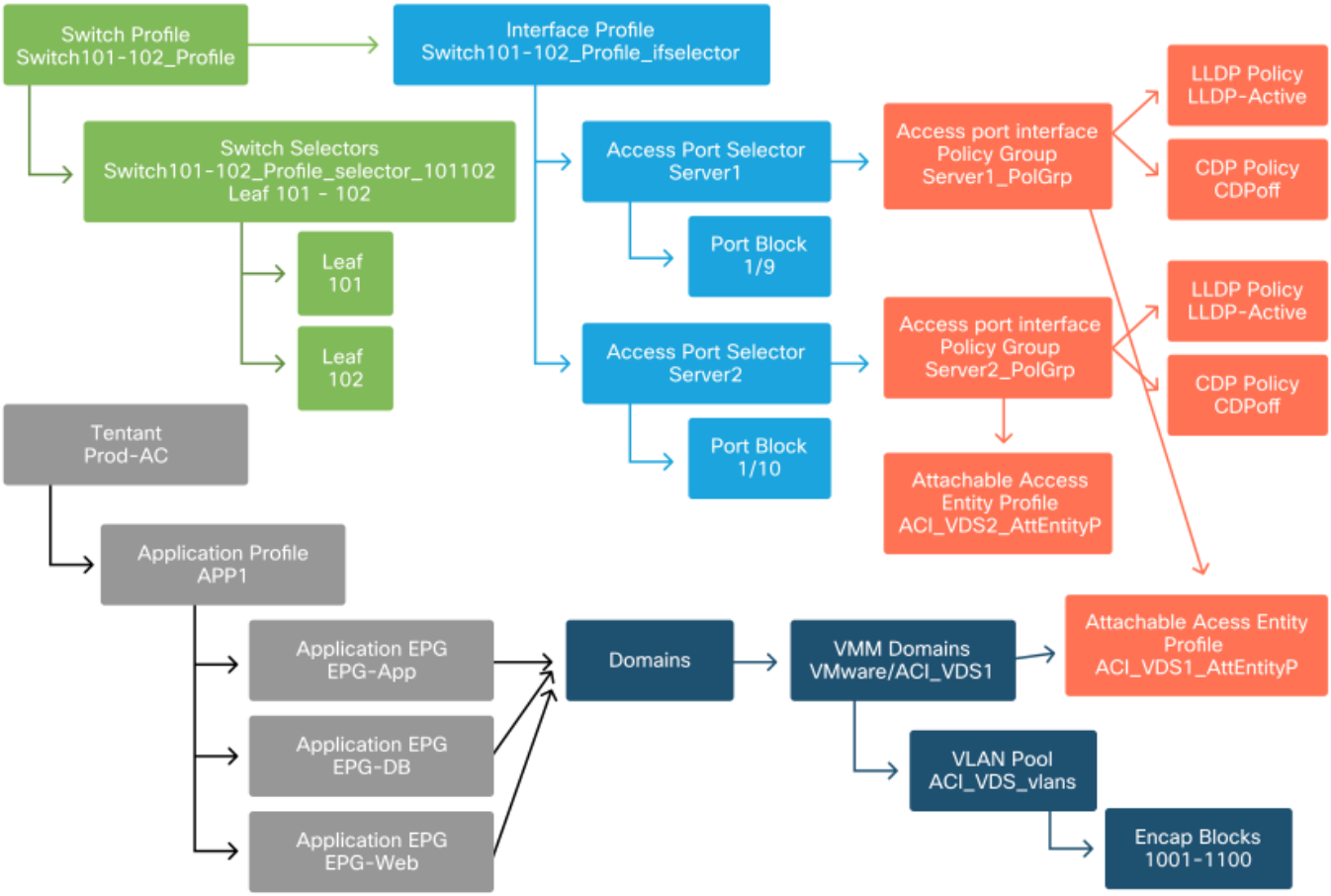
- Een extra Access Port Selector en een poortblok.
- Een extra VPC Interface Policy Group.
- Een extra statische binding met Port Encap.

Voor LACP-poortkanalen moet een speciale VPC Interface Policy Group gebruikt worden, omdat deze VPC Policy Group de definitie van de VPC-id bepaalt.

In het geval van individuele links kan de niet-VPC Interface Policy Group opnieuw worden gebruikt voor de extra server als de link dezelfde poorteigenschappen vereist.

Het resulterende beleid ziet er als volgt uit.

Server2 aansluiten op de setup



Wat nu?

De volgende sectie zal door een paar de mislukkingsscenario's van het toegangsbeleid gaan, om te beginnen met de topologie en de gebruikszaak die in dit overzicht wordt besproken.

Werkstroom voor probleemoplossing

De volgende probleemoplossing kan worden gevonden bij het werken met toegangsbeleid:

- Een ontbrekende relatie tussen twee of meer entiteiten in het toegangsbeleid, zoals toegangsbeleidsgroep die niet aan een AEP is gekoppeld.
- Een ontbrekend of onverwacht beleid is verbonden aan een bepaald toegangsbeleid, zoals

een beleid LLDP genaamd 'lldp_enabled', terwijl in werkelijkheid de beleidsconfiguratie LLDP rx/tx heeft uitgeschakeld.
- Een ontbrekende of onverwachte waarde in het toegangsbeleid, zoals de geconfigureerde VLAN-ID-encoder die ontbreekt in de geconfigureerde VLAN-pool.
- Een ontbrekende relatie tussen de EPG en het toegangsbeleid, zoals geen fysieke of virtuele domeinassociatie met de EPG.

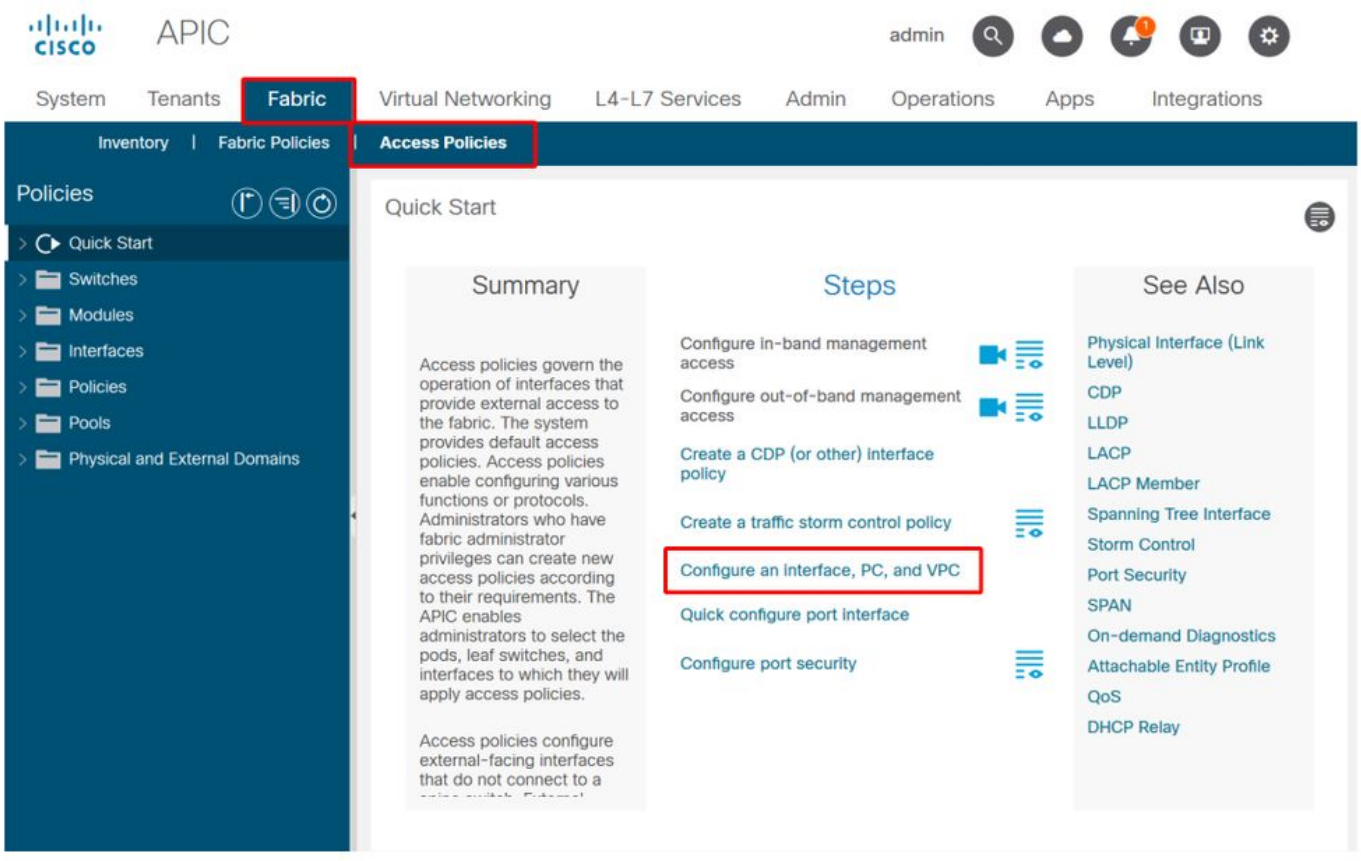
Het grootste deel van de bovenstaande probleemoplossing houdt in dat je door de relatie van het toegangsbeleid moet lopen om te begrijpen of er relaties ontbreken, of om te begrijpen welk beleid is geconfigureerd en/of of de configuratie resulteert in het gewenste gedrag.

Gebruik van de "Interface configureren, pc en VPC Quick Start" voor probleemoplossing

Binnen de APIC GUI, vergemakkelijkt de 'Configure Interface, PC, en VPC' snelle start wizard het opzoeken van toegangsbeleid door de beheerder een geaggregeerde weergave van bestaand toegangsbeleid te bieden. Deze wizard kan snel worden gestart in de GUI op:

'Fabric > Toegangsbeleid > Snel starten > Stappen > Interface, PC en VPC configureren'.

Locatie van 'Configure Interface, PC en VPC' Snel starten



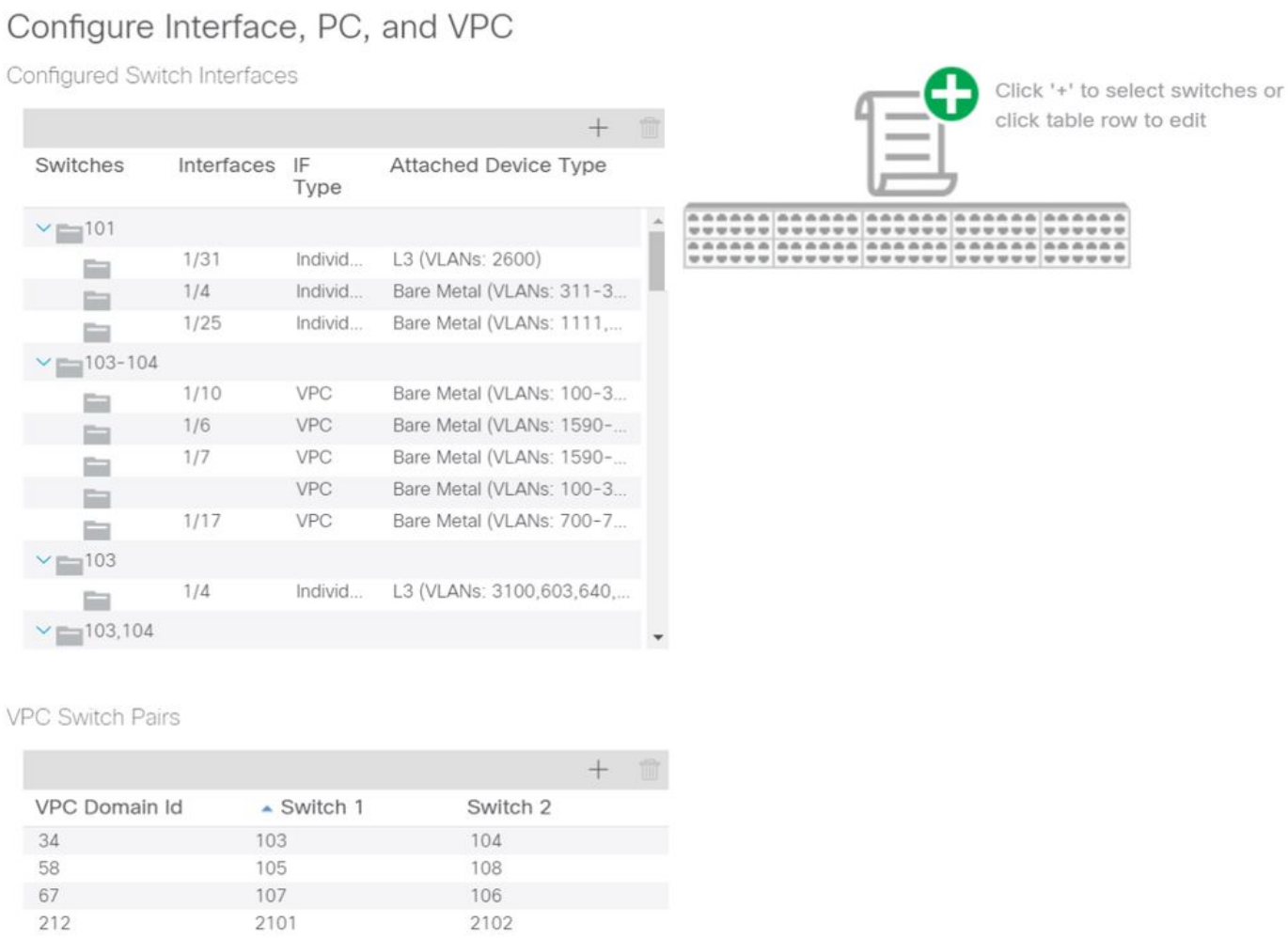
Alhoewel de wizard 'Configure' in de naam heeft, is het uitzonderlijk handig om een geaggregeerde weergave te bieden van de vele toegangsbeleid die moeten worden geconfigureerd om interfaces geprogrammeerd te krijgen. Deze samenvoeging dient als één enkele mening om te begrijpen welk beleid reeds wordt bepaald en vermindert effectief het aantal klikken die worden vereist beginnen met het isoleren van toegangsbeleid gerelateerde kwesties.

Wanneer de weergave Snel starten is geladen, kan de weergave 'Geconfigureerde Switch-

interfaces' (linksboven deelvenster) worden gebruikt om het bestaande toegangsbeleid te bepalen. Switch De wizard groepeert de items onder de mappen die een individuele of meerdere bladmappen vertegenwoordigen, afhankelijk van de configuratie van het toegangsbeleid.

Als demonstratie van de waarde van de wizard worden de volgende screenshots van de wizard getoond, wetende dat de lezer nog geen kennis heeft van de topologie van de stof:

Demo weergave van 'Configure Interface, PC, en VPC' Snel starten



Het venster 'Geconfigureerde Switch-interfaces' toont toewijzingen van toegangsbeleid. Het 'VPC Switch Paren'-venster toont de afgeronde definities van de VPC Protection Group.

De onderstaande tabel toont een subset van voltooide definities van toegangsbeleid die kunnen worden afgeleid uit de bovenstaande screenshot.

Subset van voltooid toegangsbeleid dat kan worden afgeleid uit de bovenstaande Quick Start-weergave

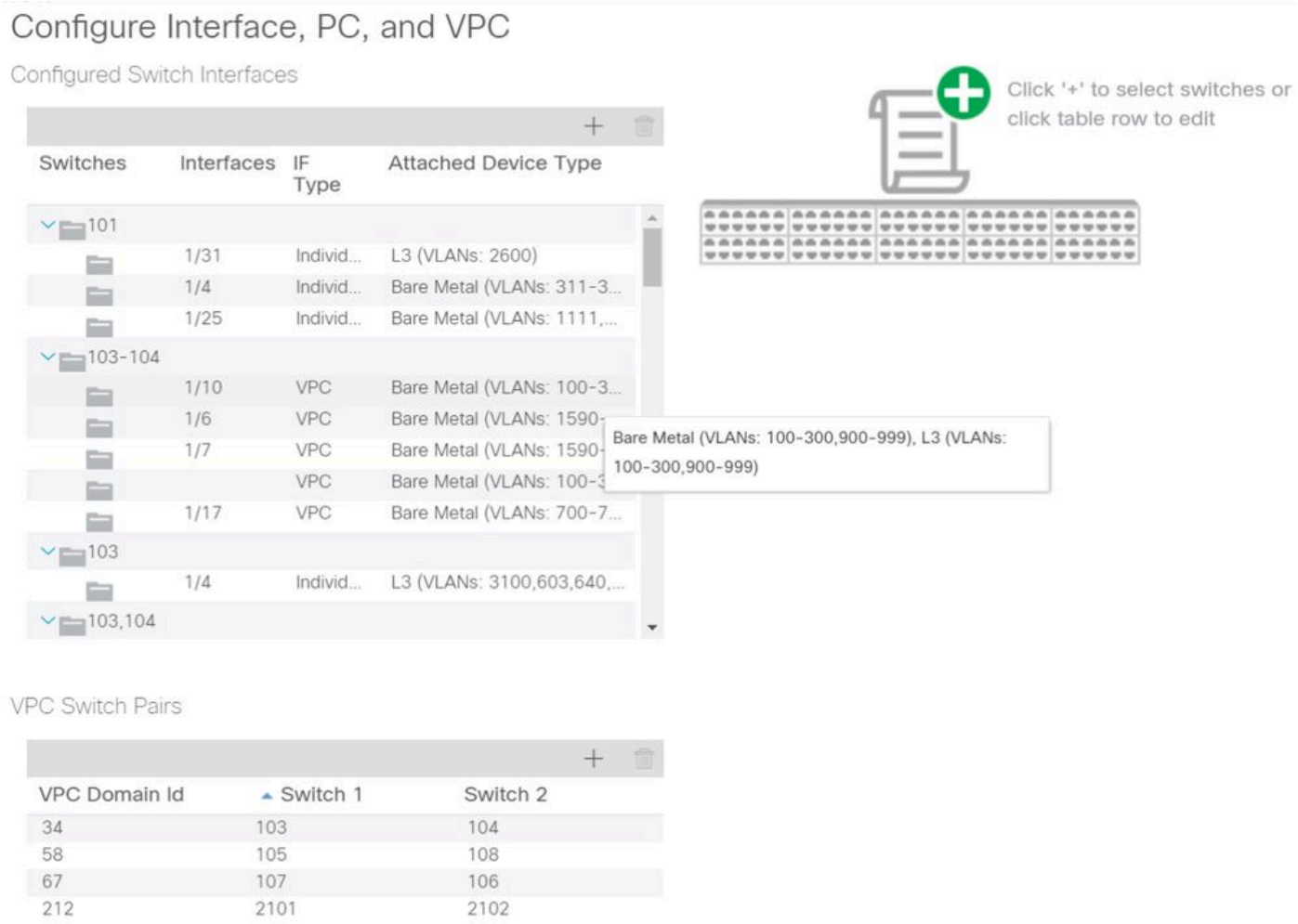
Switch-knooppunt	Interface	Type beleidsgroep	Domeintype	VLAN's
101	1/31	individueel	Routed (L3)	2600
101	1/4	individueel	Phys (schuimmetaal)	311-3...?
103-104	1/10	VPC	Phys (schuimmetaal)	100-3...?

De VLAN-kolomvermeldingen zijn opzettelijk onvolledig gezien de standaardweergave.

Op dezelfde manier kan het voltooide beleid van de 'VPC Protection Group' worden afgeleid uit de 'VPC Switch Paren' weergave (linksonder deelvenster). Zonder 'VPC-beschermingsgroepen' kunnen VPC's niet worden ingezet, aangezien dit het beleid is dat het VPC-domein tussen twee bladknooppunten definieert.

Houd er rekening mee dat vanwege de venstergrootte lange vermeldingen niet volledig zichtbaar zijn. Om de volledige waarde van een ingang te bekijken, hang de muiswijzer op het gebied van belang.

De muisaanwijzer zweeft over het veld 'Attached Device Type' voor 103-104, 1/10 VPC-ingang:



Door de muis over het deelvenster te bewegen, worden de volledige items zichtbaar.

Bijgewerkt subset van voltooid toegangsbeleid met behulp van muis-over-details

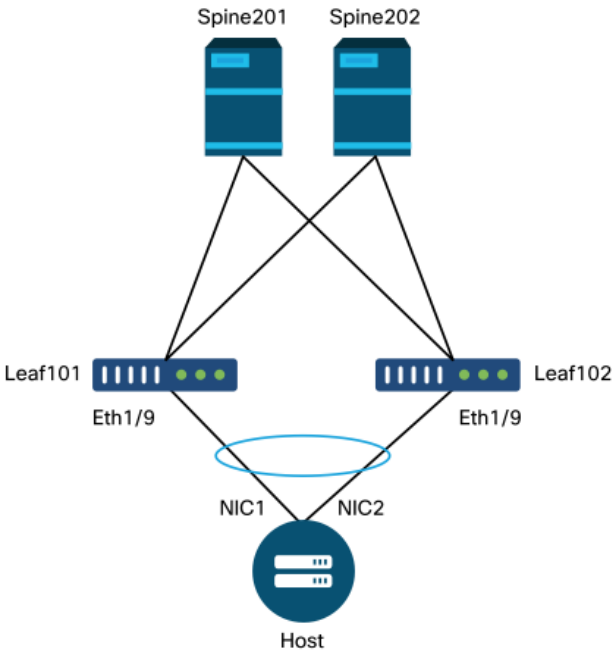
Switch-knooppunt	Interface	Type beleidsgroep	Domeintype	VLAN's
101	1/31	individueel	Routed (L3)	2600
101	1/4	individueel	Phys (schuimmetaal)	311-320
103-104	1/10	VPC	Phys (schuimmetaal)	100-300,900-999
103-104	1/10	VPC	Routed (L3)	100-300,900-999

De volledige verenigingen van VLAN kunnen nu voor het oplossen van problemen en controle worden waargenomen en worden begrepen.

Scenario's voor probleemoplossing

Voor de volgende het oplossen van probleemscenario's, verwijzing de zelfde topologie van het vorige hoofdstuk.

Topologie uit het toegangsbeleid "Inleiding" sectie



Scenario 1: Fout F0467 — ongeldig pad, onregelmatigheden

Deze fout wordt veroorzaakt wanneer een switch/poort/VLAN-aangifte wordt gedaan zonder het corresponderende toegangsbeleid om de juiste toepassing van die configuratie mogelijk te maken. Afhankelijk van de beschrijving van deze fout, kan een ander element van de toegangsbeleidsrelatie ontbreken.

Na het implementeren van een statische band voor de bovenstaande VPC-interface met trunked encap VLAN 1501 zonder de corresponderende toegangsbeleidsrelatie op zijn plaats, wordt de volgende fout op de EPG veroorzaakt:

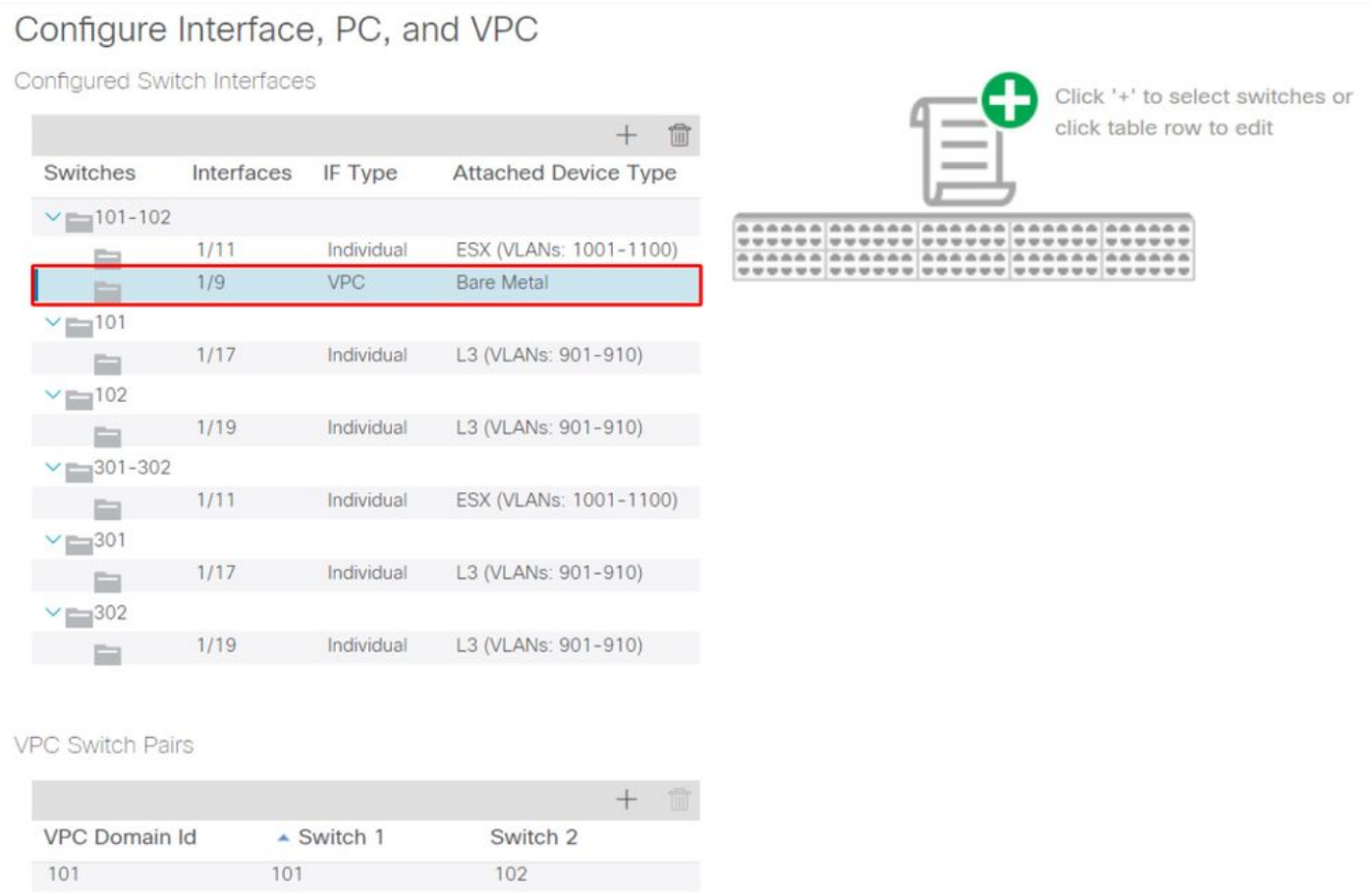
Fout: F0467

Beschrijving: Fault delegate: Configuratie mislukt voor uni/tn-Prod1/ap-App1/epg-EPG-Web knooppunt 101 101_102_eth1_9 vanwege ongeldige padconfiguratie, ongeldige VLAN-configuratie, debug bericht: ongeldig-VLAN: vlan-1501: STP-segment-id niet aanwezig voor Encap. Ofwel de EPG is niet gekoppeld aan een domein of het domein heeft dit VLAN niet toegewezen;ongeldige-pad: vlan-1501: er is geen domein, gekoppeld aan EPG en poort, dat VLAN vereist heeft;

Uit de bovenstaande foutbeschrijving blijkt duidelijk wat de oorzaak van de fout kan zijn. Er is een waarschuwing om de relaties met het toegangsbeleid te controleren, evenals om de domeinassociatie met de EPG te controleren.

Bij het bekijken van de weergave Snel starten in het hierboven beschreven scenario ontbreekt duidelijk het toegangsbeleid VLAN's.

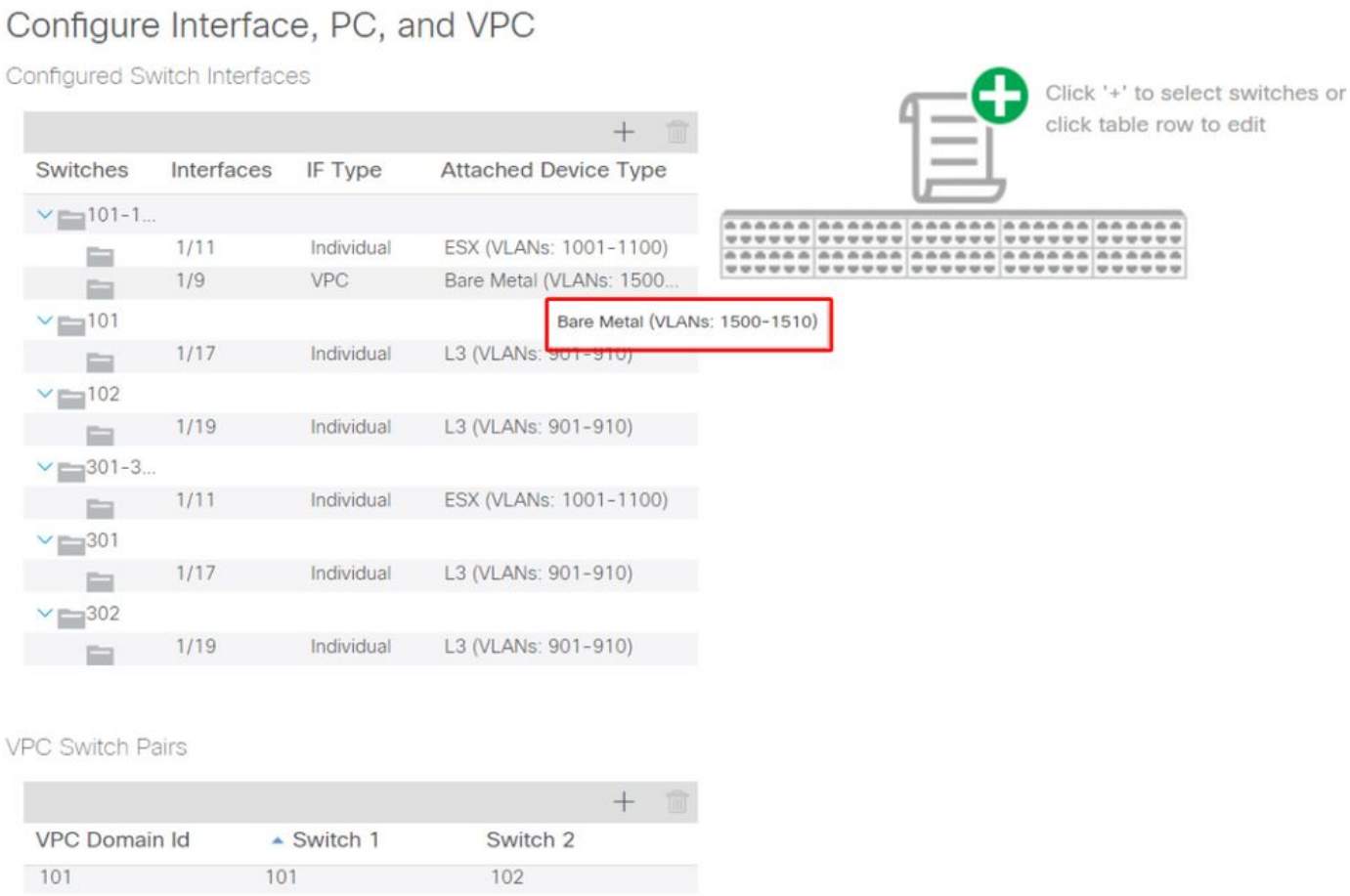
Quick Start view waar 101-102, Int 1/9 VPC ontbreekt VLAN's



Merk op dat de ingang een verwijzing naar om het even welke VLAN IDs mist.

Na correctie wordt in de weergave Snel starten weergegeven '(VLAN's 1500-1510)'.

101-102, Intel 1/9 VPC toont nu Bare Metal (VLAN's: 1500-1510)



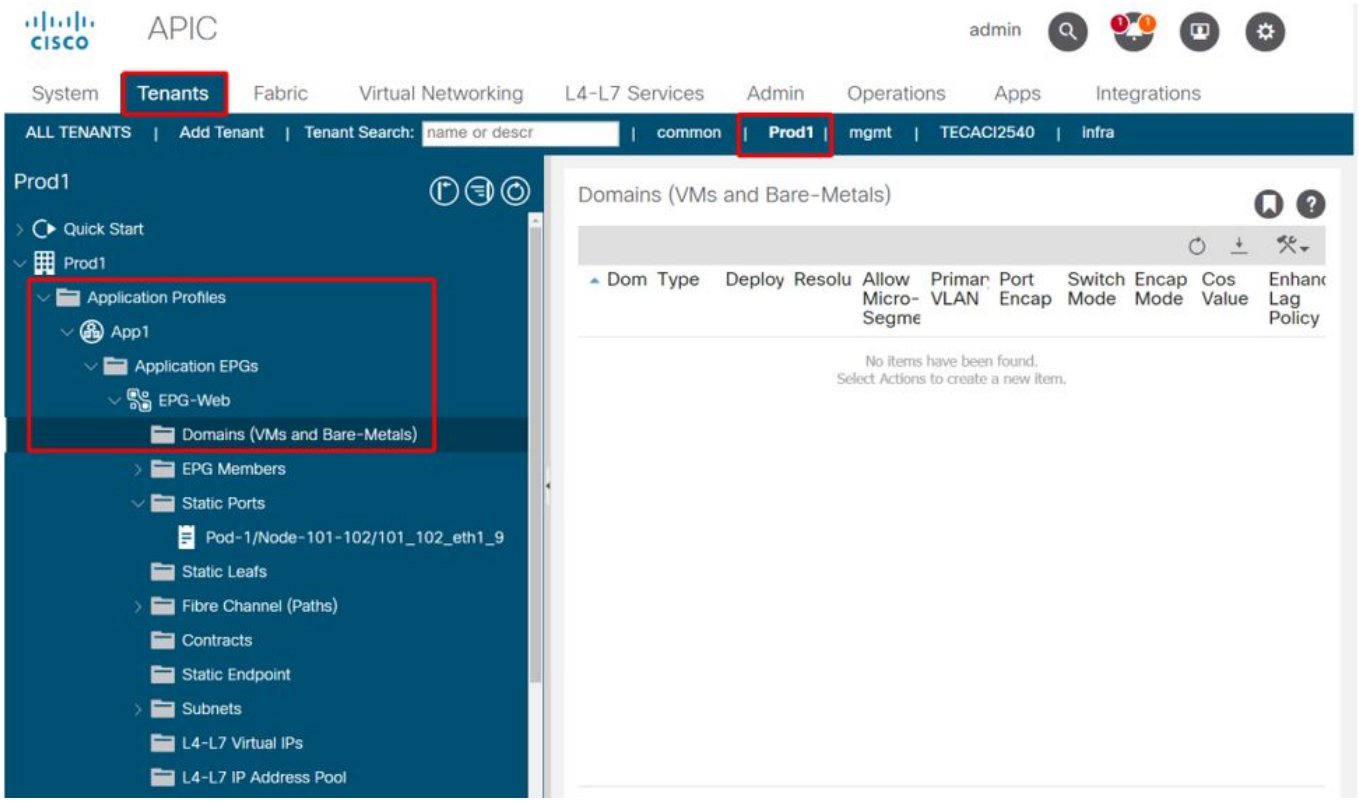
De EPG-fout bestaat echter nog steeds met de volgende bijgewerkte beschrijving van fout F0467:

Fout: F0467

Beschrijving: Fault delegate: Configuratie mislukt voor uni/tn-Prod1/ap-App1/epg-EPG-Web knooppunt 101 101_102_eth1_9 vanwege ongeldige padconfiguratie, debug bericht: ongeldig pad: VLAN 150: Er is geen domein, gekoppeld aan zowel EPG als Port, dat VLAN heeft vereist.

Met de hierboven geüpdatete fout, controleer de EPG domeinassociaties om te zien dat er geen domeinen verbonden zijn met de EPG.

EPG-Web heeft Statische Poorten vereniging, maar ontbreekt domeinverenigingen



Zodra het domein dat VLAN 1501 bevat aan EPG wordt geassocieerd, worden geen verdere fouten verhoogd.

Scenario 2: Kan VPC niet selecteren als pad voor implementatie op EPG Statische poort of L3Out Logical Interface Profile (SVI)

Tijdens het configureren van een VPC als pad op een statische EPG-poort of L3Out Logical Interface Profile SVI-ingang, wordt de specifieke te implementeren VPC niet weergegeven als een beschikbare optie.

Wanneer u probeert een VPC statische binding te implementeren, zijn er twee harde vereisten:

1. De VPC Explicit Protection Group moet worden gedefinieerd voor het betrokken paar switches.
2. Er moet een overzicht van het volledige toegangsbeleid worden opgesteld.

Beide vereisten kunnen worden gecontroleerd vanuit de Snelle weergave Start zoals hierboven wordt getoond. Als geen van beide volledig is, zal VPC eenvoudig niet als beschikbare optie voor Statische Poortbanden verschijnen.

Scenario 3: Foutmelding F0467 — reeds in een andere EPG gebruikte stofkap

Standaard hebben VLAN's een wereldwijde scope. Dit betekent dat een gegeven VLAN-id alleen kan worden gebruikt voor één EPG op een bepaalde switch. Elke poging om hetzelfde VLAN te hergebruiken op meerdere EPG's binnen een bepaalde switch zal resulteren in de volgende fout:

Fout: F0467

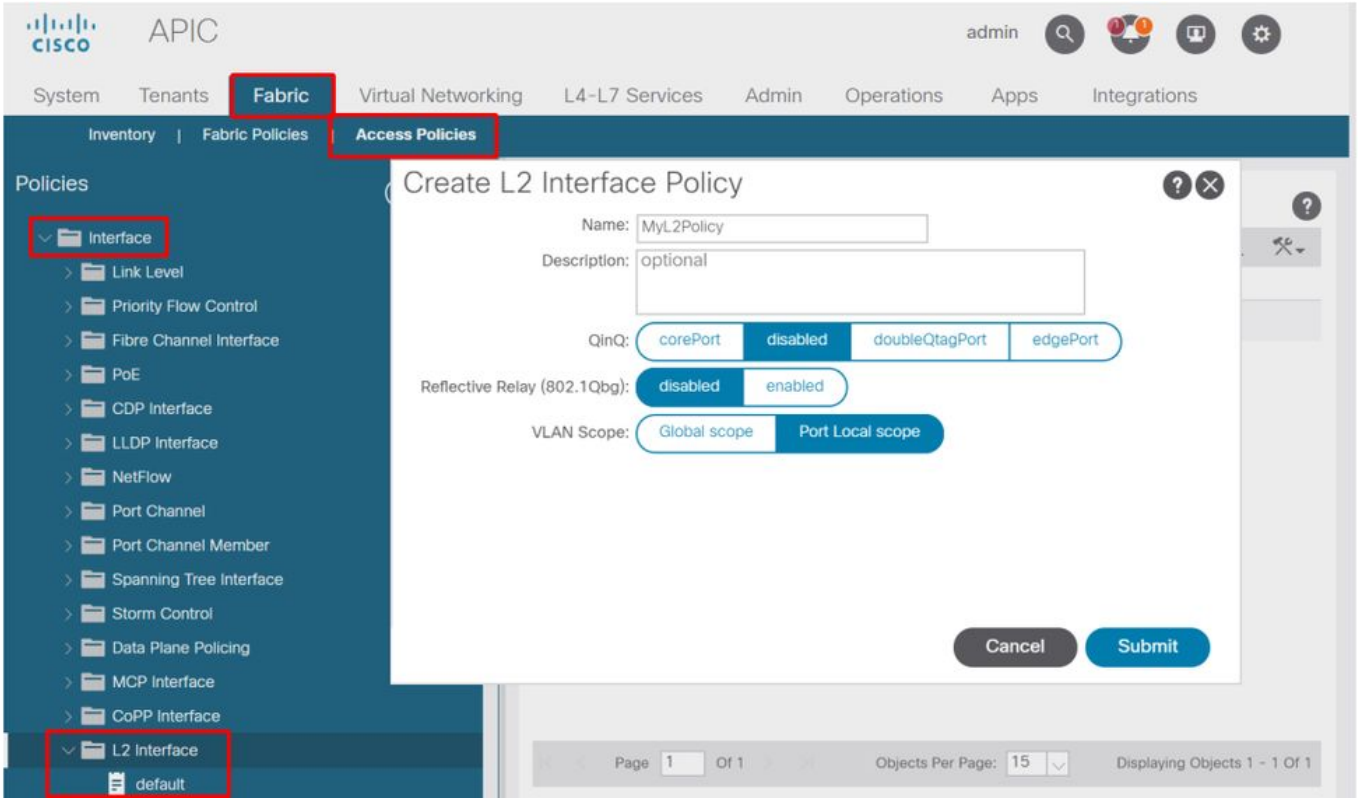
Beschrijving: Fault delegate: Configuratie mislukt voor uni/tn-Prod1/ap-App1/epg-EPG-BusinessApp knooppunt 102 101_102_eth1_8 vanwege Encap reeds gebruikt in een andere EPG, debug bericht: reeds in gebruik zijnde encap: Encap is reeds in gebruik door Prod1:App1:EPG-

Web;

Afgezien van het selecteren van een ander VLAN, een andere optie om deze configuratie te maken werk is om het gebruik van 'Port Local' VLAN Scope te overwegen. Dit werkingsgebied staat voor VLANs toe om op een per-interfacebasis worden in kaart gebracht wat betekent dat VLAN-1501 potentieel voor verschillende EPGs, over meerdere interfaces, op het zelfde blad kon worden gebruikt.

Hoewel het bereik van 'Port Local' op basis van een beleidsgroep wordt geassocieerd (met name via een L2-beleid), wordt het toegepast op bladniveau.

Locatie om 'VLAN scope'-instelling binnen APIC GUI te wijzigen



Alvorens de 'Port Local' VLAN-toepassingsconfiguratie te implementeren, raadpleegt u de 'Cisco APIC Layer 2 Networking Configuration Guide' op Cisco.com om ervoor te zorgen dat de beperkingen en ontwerpbeperkingen aanvaardbaar zijn voor de gewenste gebruikscases en ontwerpen.

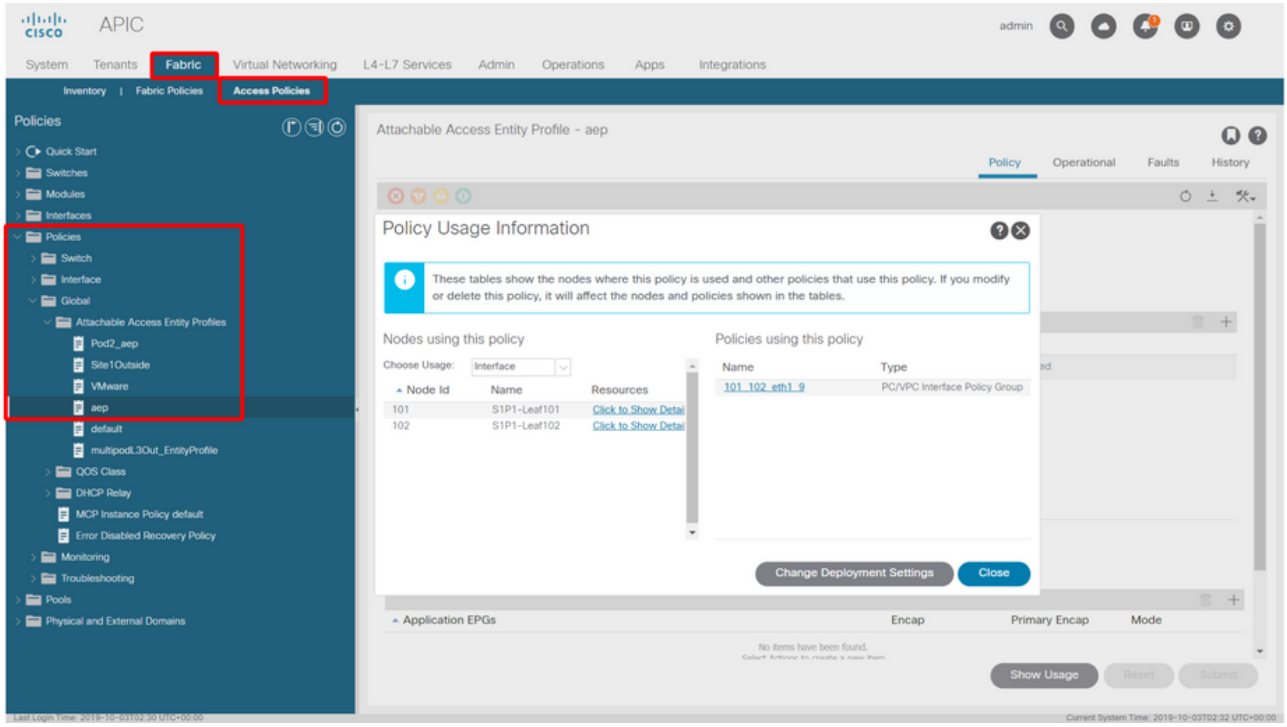
Speciale vermeldingen

Gebruik weergeven

Hoewel dit niet specifiek is voor toegangsbeleid, is er op de meeste objecten in de GUI een knop beschikbaar met het label 'Gebruik tonen'. Deze knop voert een beleidsraadpleging uit op het geselecteerde object om te bepalen welke bladknooppunten/interfaces er een directe relatie mee hebben. Dit kan nuttig zijn voor zowel het algemene lookup scenario als om een begrip te verkrijgen van of een specifiek object of beleid zelfs in gebruik is.

In de screenshot hieronder wordt de geselecteerde AEP gebruikt door twee verschillende interfaces. Dit betekent dat het wijzigen van de AEP een directe impact zal hebben op de

bijbehorende interfaces.



Overlappende VLAN-pools

Terwijl de functie van toegangsbeleid is specifiek VLAN toe te staan om op een interface worden opgesteld, is er extra gebruik dat tijdens de ontwerpfase moet worden overwogen. Met name wordt het domein gebruikt in de berekening van de VXLAN-id (Fabric Encap genoemd) die is gekoppeld aan de externe inkapseling. Terwijl deze functionaliteit over het algemeen geen belangrijke invloed op dataplane verkeer heeft, zijn dergelijke IDs vooral relevant voor een ondergroep van protocollen die door de stof, met inbegrip van het Overspannen - boom BPDUs overstromen. Als van VLAN<id> BPDU's die op leaf1 ingrijpen, wordt verwacht dat ze Leaf 2 verlaten (bijv. omdat ze bestaande switches hebben die Spanning-Tree convergen via ACI), moet VLAN-<id> dezelfde fabric-encryptie hebben op beide bladknooppunten. Als de waarde van de fabric-insluiting verschilt voor dezelfde VLAN's voor toegang, worden de BPDU's niet door de stof getransporteerd.

Zoals in de vorige sectie is vermeld, vermijd de configuratie van dezelfde VLAN's in meerdere domeinen (VMM vs Physical, bijvoorbeeld) tenzij er bijzondere zorg voor wordt besteed dat elk domein alleen ooit wordt toegepast op een unieke set van switches. Het moment dat beide domeinen kunnen worden opgelost op dezelfde bladzijde switch voor een bepaald VLAN, is er een kans dat onderliggende VXLAN kan worden gewijzigd na een upgrade (of schoon reload) die bijvoorbeeld kan leiden tot STP convergentie problemen. Het gedrag is een resultaat van elk domein met een unieke numerieke waarde (het 'base'-kenmerk) dat in de volgende vergelijking wordt gebruikt om VXLAN-id te bepalen:

VXLAN VNID = Base + (encap — from_encap)

Om te bevestigen welke domeinen op een bepaald blad worden gedrukt, kan een moquery tegen de klasse 'stpAllocEncapBlkDef' worden uitgevoerd:

```
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
```

Van deze output, onderken de volgende definities van het toegangsbeleid:

- Er is een geprogrammeerde VLAN-pool met een blok VLAN's dat expliciet VLAN's 1500-1510 definieert.
- Dit blok VLAN's is gekoppeld aan een domein met de naam 'physvlans'.
- De basiswaarde die wordt gebruikt bij de berekening van VXLAN is 8492.
- De resulterende VXLAN-berekening voor VLAN-1501 zou 8492 + (1501-1500) = 8493 zijn als de insluiting van het weefsel.

De resulterende VXLAN-id (in dit voorbeeld 8493) kan met de volgende opdracht worden geverifieerd:

```
leaf# show system internal epm vlan all
+----------+---------+-----------------+----------+------+----------+-----------
 VLAN ID    Type      Access Encap     Fabric    H/W id  BD VLAN    Endpoint
                      (Type Value)     Encap                         Count
+----------+---------+-----------------+----------+------+----------+-----------
13           Tenant BD NONE             0 16121790   18     13          0
14             FD vlan 802.1Q       1501 8493       19     13          0
```

Als er een andere VLAN-pool is die VLAN-1501 bevat die op hetzelfde blad wordt geduwd, kan een upgrade of schoon herladen mogelijk unieke basiswaarde (en vervolgens een andere Fabric Encap) invoegen die ervoor zal zorgen dat BPDU's niet meer een ander blad aanmaakt dat naar verwachting BPDU's op VLAN-1501 zal ontvangen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.