Solucionar problemas de políticas de acesso da ACI

Contents

Introduction

Este documento descreve as etapas para entender e solucionar problemas das políticas de acesso da ACI.

Informações de Apoio

O material deste documento foi extraído do livro Troubleshooting Cisco Application Centric Infrastructure, Second Edition, especificamente os capítulos **Access Policies - Overview** e **Access Policies - Troubleshooting Workflow**.

Visão geral das políticas de acesso

Como o administrador da ACI configura uma VLAN em uma porta na estrutura? Como o administrador da ACI começa a lidar com falhas relacionadas às políticas de acesso? Esta seção explicará como solucionar problemas relacionados às políticas de acesso à estrutura.

Antes de passar para cenários de solução de problemas, é fundamental que o leitor tenha um bom entendimento de como as políticas de acesso funcionam e de suas relações dentro do ACI Object Model. Para essa finalidade, o leitor pode consultar os documentos "ACI Policy Model" (Modelo de política da ACI) e "APIC Management Information Model Reference" (Referência do modelo de informações de gerenciamento do APIC), disponíveis em Cisco.com (https://developer.cisco.com/site/apic-mim-ref-api/).

A função das políticas de acesso é ativar a configuração específica em portas de downlink de um switch leaf. Antes que a política de locatário seja definida para permitir o tráfego através de uma porta de estrutura da ACI, as políticas de acesso relacionadas devem estar em vigor.

Normalmente, as políticas de acesso são definidas quando novos switches leaf são adicionados à estrutura ou um dispositivo é conectado a downlinks leaf da ACI; mas, dependendo do quão dinâmico é um ambiente, as políticas de acesso podem ser modificadas durante a operação normal da malha. Por exemplo, para permitir um novo conjunto de VLANs ou adicionar um novo Domínio Roteado às portas de acesso da malha.

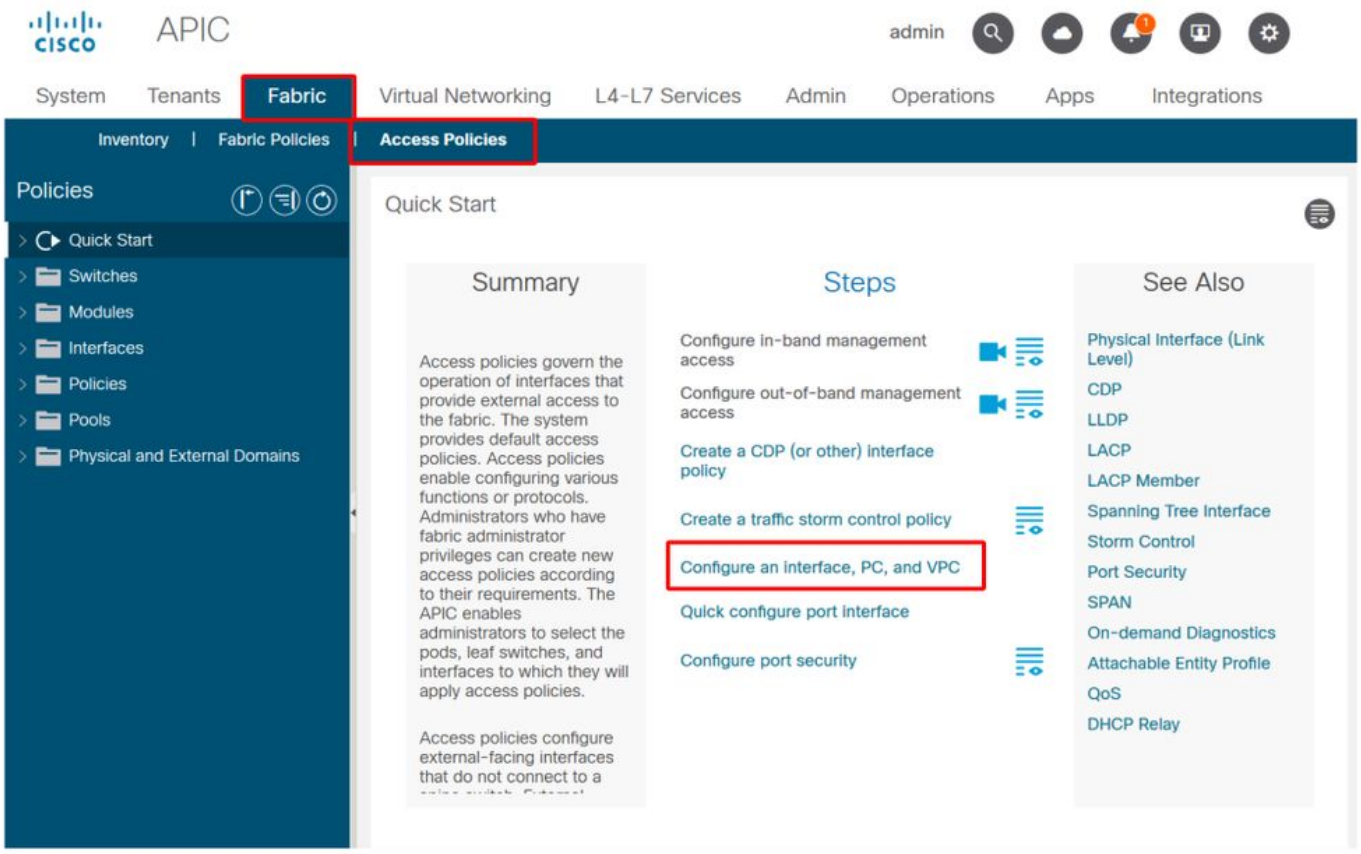
As políticas de acesso da ACI, embora inicialmente um pouco intimidantes, são extremamente flexíveis e foram projetadas para simplificar o provisionamento de configuração para uma rede de SDN de grande escala em evolução contínua.

Configuração da política de acesso: Metodologia

As políticas de acesso podem ser configuradas de forma independente, isto é, criando todos os objetos necessários de forma independente, ou podem ser definidas por meio dos vários assistentes fornecidos pela GUI da ACI.

Os assistentes são muito úteis, pois orientam o usuário no fluxo de trabalho e garantem que todas as políticas necessárias sejam aplicadas.

Políticas de acesso — Assistente de início rápido

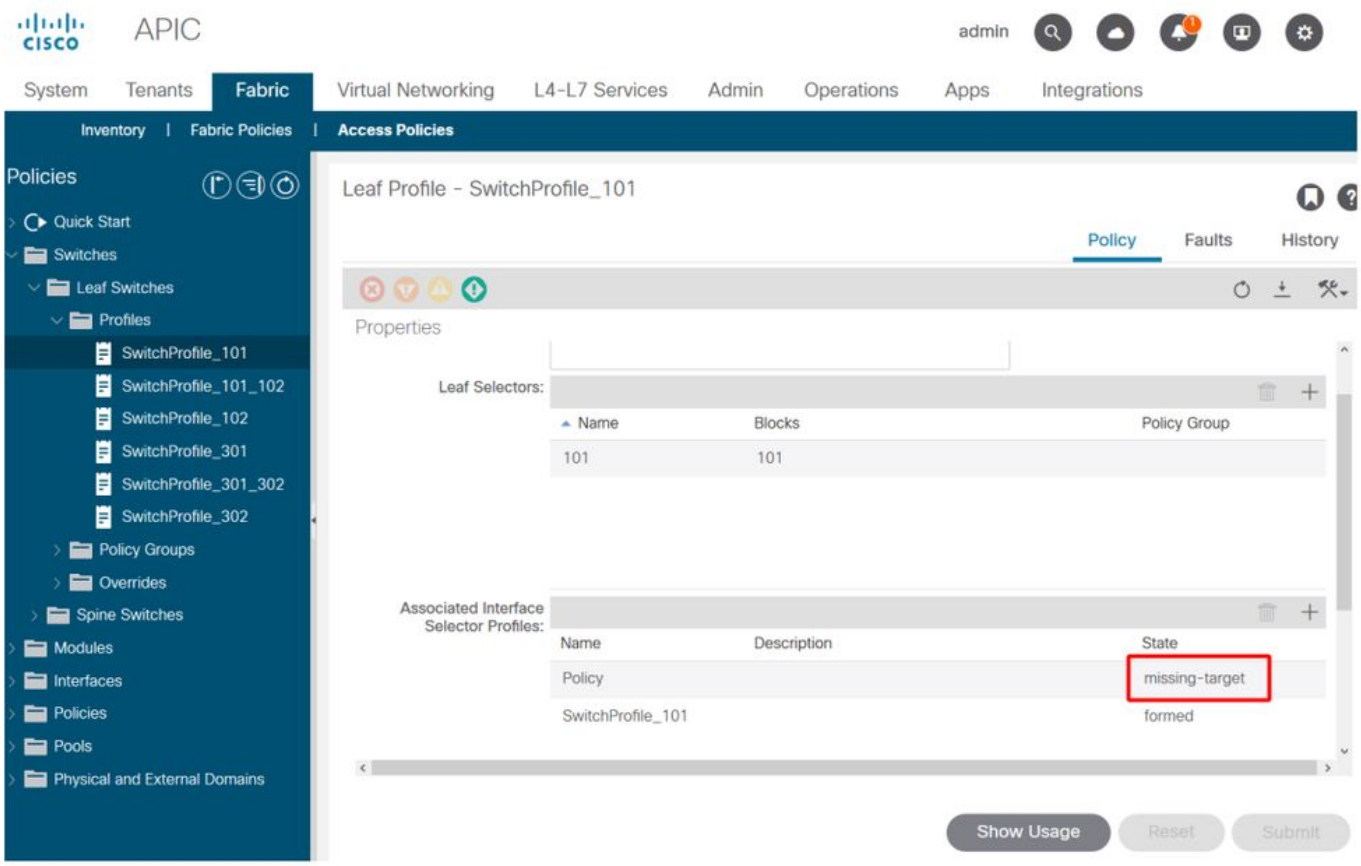


A imagem acima mostra a página Início rápido, onde vários assistentes podem ser encontrados.

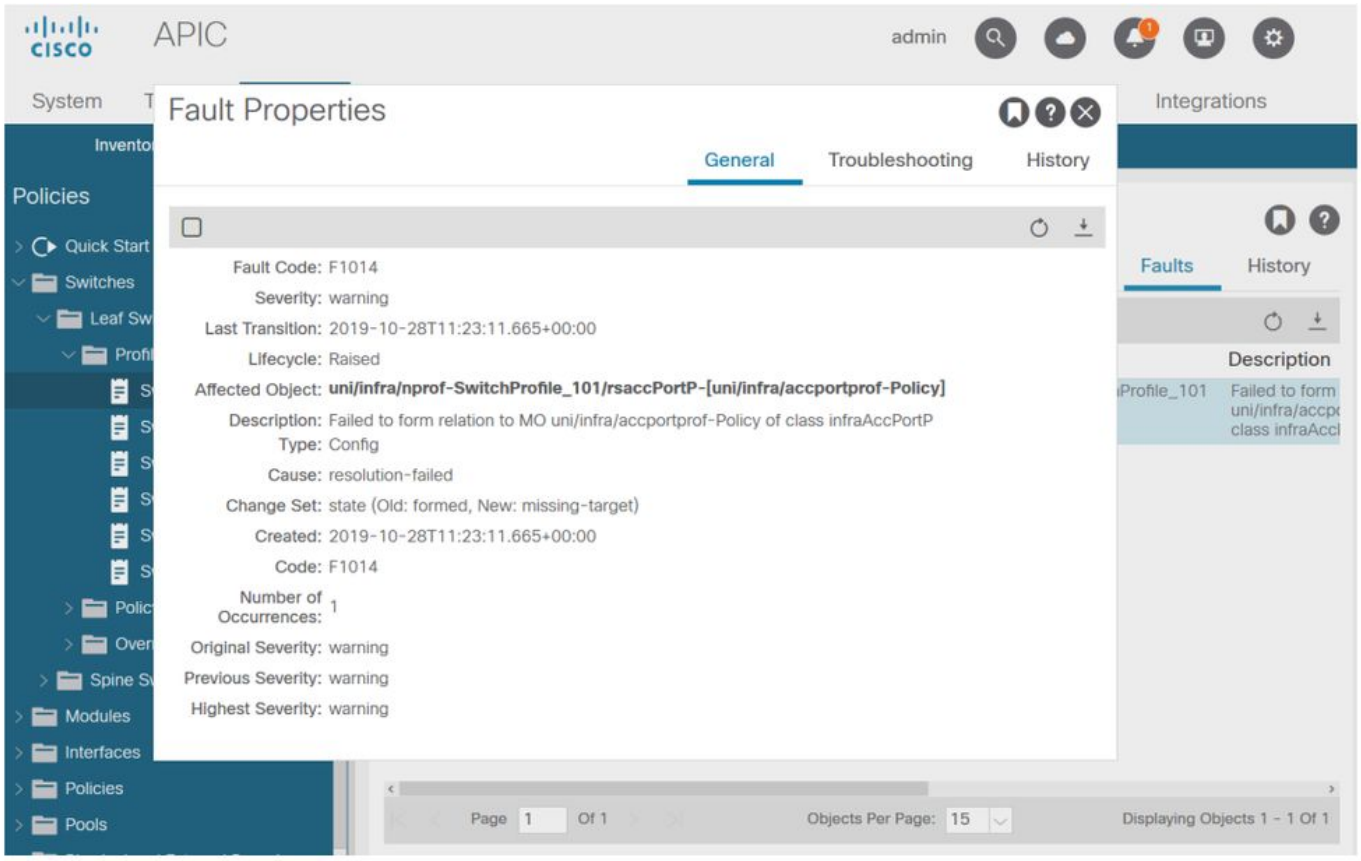
Depois que uma política de acesso é definida, a recomendação genérica é validar a política, certificando-se de que todos os objetos associados não mostram nenhuma falha.

Por exemplo, na figura abaixo, um Perfil de Switch atribuiu uma Política de Seletor de Interface que não existe. Um usuário atencioso poderá facilmente detectar o estado '**missing-target**' do objeto e verificar se uma falha foi sinalizada na GUI:

Perfil Folha — SwitchProfile_101



Perfil Folha — SwitchProfile_101 — Falha



Nesse caso, corrigir a falha seria tão fácil quanto criar um novo Perfil do Seletor de Interface chamado 'Política'.

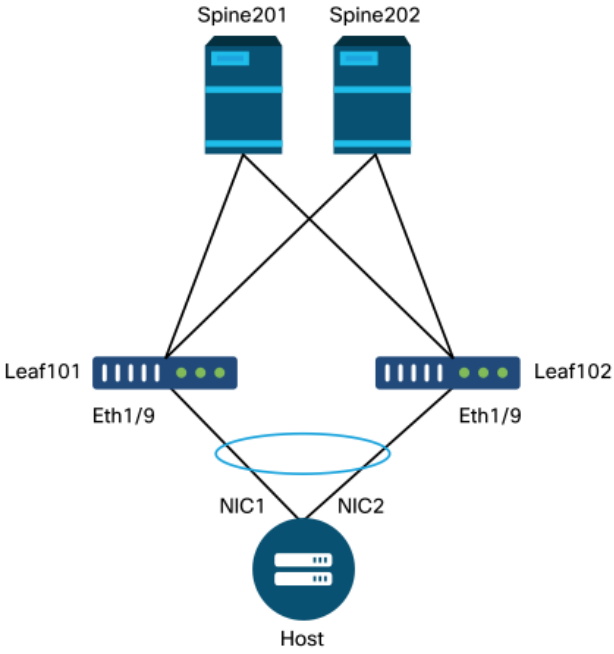
A configuração manual das políticas básicas de acesso será explorada nos parágrafos a seguir.

Configurações básicas manuais das políticas de acesso

Ao implantar políticas de acesso, os objetos estão sendo definidos para expressar o uso pretendido dos downlinks fornecidos. A declaração que programa os downlinks (por exemplo, atribuição de porta estática EPG) se baseia nessa intenção expressa. Isso ajuda a dimensionar a configuração e agrupar logicamente objetos de uso semelhantes, como switches ou portas especificamente conectadas a um determinado dispositivo externo.

Consulte a topologia abaixo para o restante deste capítulo.

Topologia de definição de política de acesso para servidor dual-homed

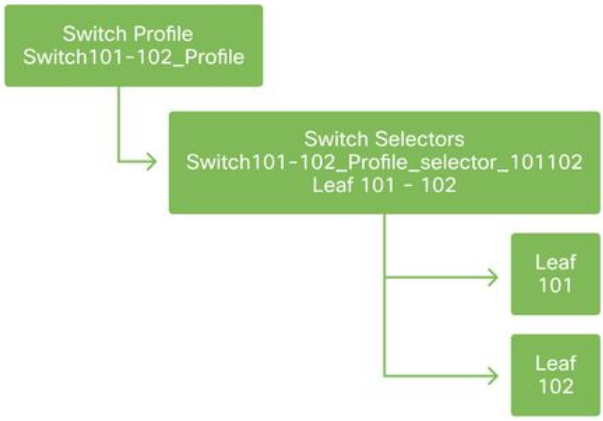


Um servidor da Web está conectado a uma malha da ACI. O servidor Web tem 2 placas de interface de rede (NICs) configuradas em um canal de porta LACP. O servidor Web está conectado à porta 1/9 dos switches leaf 101 e 102. O servidor Web depende da VLAN-1501 e deve residir no EPG 'EPG-Web'.

Configurar a política do switch

A primeira etapa lógica é definir quais switches leaf serão usados. O 'Perfil do Switch' conterá 'Seletores de Switch' que definem as IDs de nó folha a serem usadas.

Políticas de switch



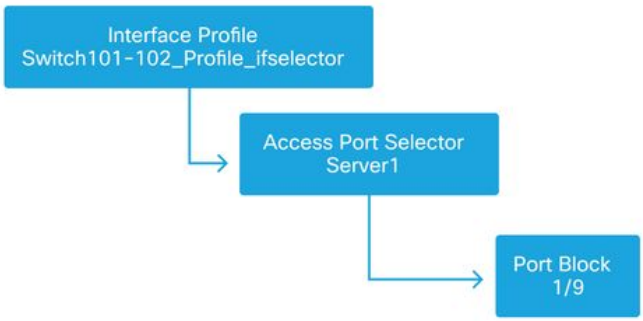
A recomendação geral é configurar 1 Perfil de Switch por switch de folha individual e 1 Perfil de Switch por par de domínios VPC, usando um esquema de nomenclatura que indica os nós que fazem parte do perfil.

O Início rápido implanta um esquema de nomenclatura lógico que facilita a compreensão de onde ele é aplicado. O nome completo segue o formato 'Switch<node-id>_Profile'. Como exemplo, 'Switch101_Profile' será para um perfil de switch contendo o nó folha 101 e Switch101-102_Profile para um Perfil de Switch contendo os nós folha 101 e 102 que devem fazer parte de um domínio VPC.

Configurar a política de interface

Depois que as políticas de acesso do switch forem criadas, definir as interfaces seria a próxima etapa lógica. Isso é feito criando-se um "Perfil de interface" que consiste em um ou mais "Seletores de porta de acesso" que contêm as definições de "Bloco de porta".

Políticas de interface



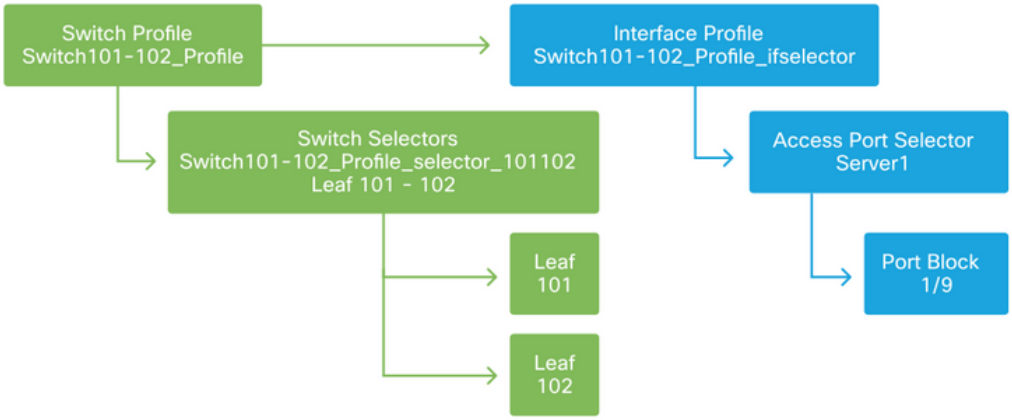
Para formar a relação entre o 'Perfil da interface' e os switches envolvidos, vincule o 'Perfil do switch' ao 'Perfil da interface'.

Os "perfis de interface" podem ser definidos de várias maneiras. Semelhante aos "Perfis de Switch", um único "Perfil de Interface" pode ser criado por switch físico junto com um "Perfil de Interface" por domínio VPC. Essas políticas devem ter um mapeamento 1 para 1 para o perfil de switch correspondente. Seguindo essa lógica, as políticas de acesso à estrutura são bastante simplificadas, o que facilita a compreensão de outros usuários.

Os esquemas de nomenclatura padrão empregados pelo Início rápido também podem ser usados aqui. Ele segue o formato '<switch profile name>_ifselector' para indicar que esse perfil é usado

para selecionar interfaces. Um exemplo seria 'Switch101_Profile_ifselector'. Este exemplo de 'Perfil de Interface' seria usado para configurar interfaces não VPC no switch folha 101 e seria associado somente à política de acesso 'Switch101_Profile'.

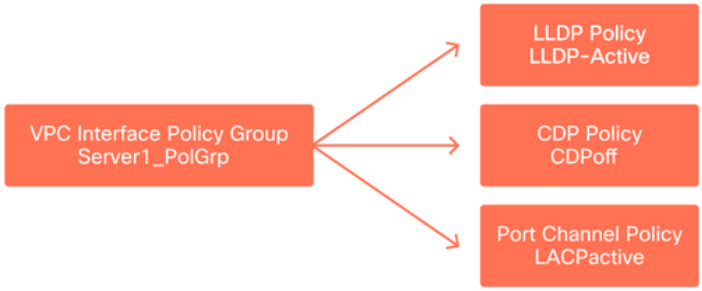
Perfil do Switch associado ao Perfil da Interface



Observe que como um "Perfil de Interface" com Eth 1/9 está conectado a um "Perfil de Switch" que inclui os switches leaf 101 e 102, o provisionamento de Eth1/9 em ambos os nós começa simultaneamente.

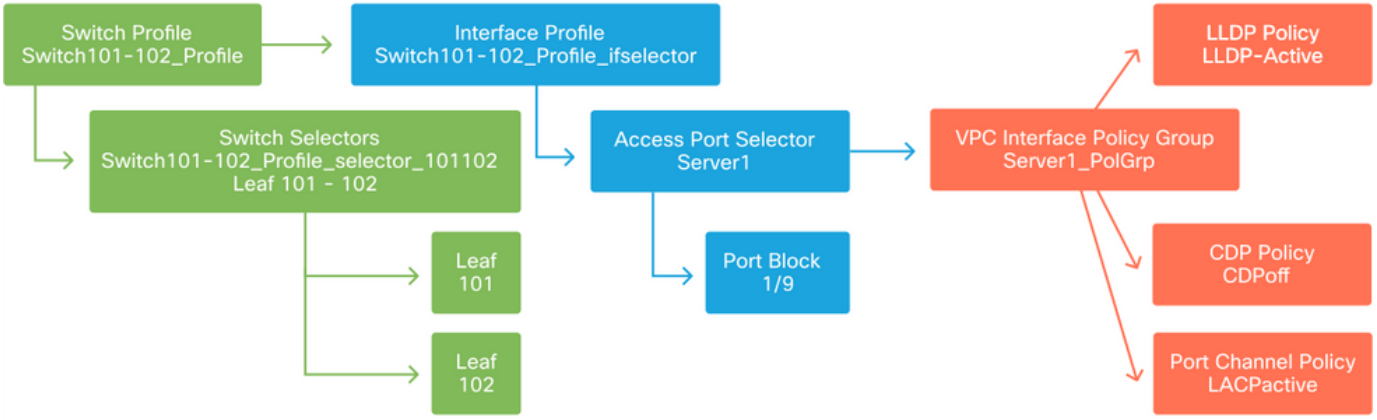
Neste ponto, foram definidos switches leaf e suas portas. A próxima etapa lógica seria definir as características dessas portas. O 'Grupo de política de interface' permite a definição dessas propriedades de porta. Um 'Grupo de Política de Interface VPC' será criado para permitir o Canal de Porta LACP acima.

Grupo de Políticas



O 'Grupo de Política de Interface VPC' é associado ao 'Grupo de Política de Interface' do 'Seletor de Porta de Acesso' para formar a relação do switch/Interface folha com as propriedades da porta.

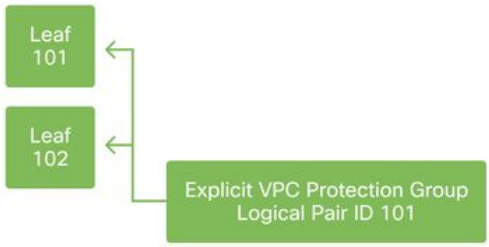
Perfis de switch e interface combinados



Configurar o VPC

Para criar o canal de porta do LACP sobre switches de 2 folhas, um domínio do VPC deve ser definido entre os switches de folha 101 e 102. Isso é feito definindo-se um 'Grupo de Proteção do VPC' entre os dois switches de folha.

VPC



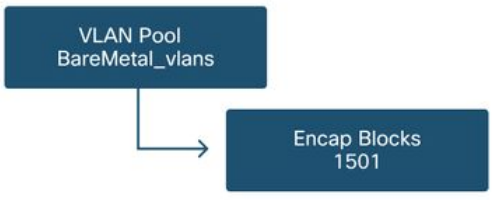
Configurar pools de VLANs

A próxima etapa lógica será criar as VLANs que serão usadas nessa porta, nesse caso, VLAN-1501. A definição de um "Pool de VLANs" com "Blocos de Encap" conclui esta configuração.

Ao considerar o tamanho dos intervalos de pool de VLANs, lembre-se de que a maioria das implantações só precisa de um único pool de VLANs e um pool adicional se estiver usando integração de VMM. Para trazer VLANs de uma rede antiga para a ACI, defina o intervalo de VLANs antigas como um pool de VLANs estáticas.

Por exemplo, suponha que as VLANs 1 a 2000 sejam usadas em um ambiente herdado. Crie um pool de VLANs estáticas que contenha VLANs 1-2000. Isso permitirá o entroncamento de EPGs e domínios de bridge da ACI em direção à malha antiga. Se estiver implantando o VMM, um segundo pool dinâmico pode ser criado usando um intervalo de IDs de VLAN livres.

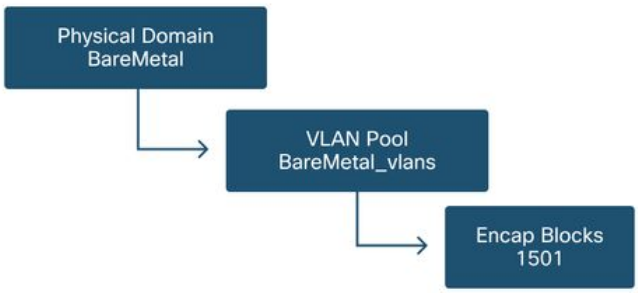
Pool de VLANs



Configurar domínios

A próxima etapa lógica é criar um 'Domínio'. Um 'Domínio' define o escopo de um pool de VLANs, isto é, onde esse pool será aplicado. Um 'Domínio' pode ser físico, virtual ou externo (ligado ou roteado). Neste exemplo, um 'Domínio físico' será usado para conectar um servidor bare-metal à estrutura. Este 'Domínio' é associado ao 'Pool de VLANs' para permitir a(s) vlan(s) necessária(s).

Domínios físicos



Para a maioria das implantações, um único 'Domínio Físico' é suficiente para implantações bare-metal e um único 'Domínio Roteado' é suficiente para implantações L3Out. Ambos podem mapear para o mesmo "Pool de VLANs". Se a estrutura for implantada de forma multilocatária ou se for necessário um controle mais granular para restringir quais usuários podem implantar EPGs e VLANs específicos em uma porta, um projeto de política de acesso mais estratégico deve ser considerado.

Os 'Domínios' também fornecem a funcionalidade para restringir o acesso do usuário à política com 'Domínios de Segurança' usando o RBAC (Controle de Acesso Baseado em Funções).

Ao implantar VLANs em um switch, a ACI encapsulará BPDUs de spanning-tree com um ID de VXLAN exclusivo baseado no domínio de origem da VLAN. Por isso, é importante usar o mesmo domínio sempre que conectar dispositivos que exigem comunicação STP com outras pontes.

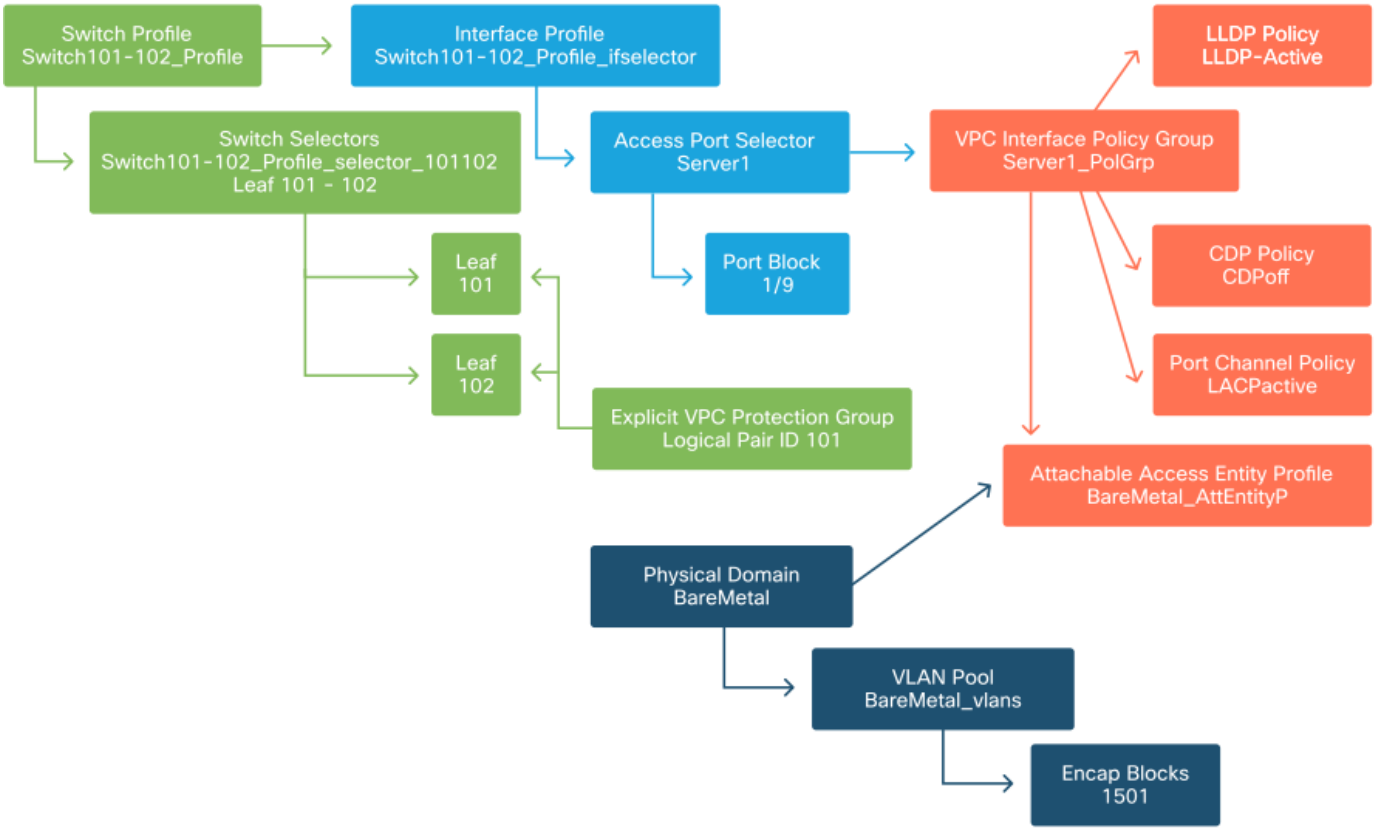
As VLAN VXLAN IDs também são usadas para permitir que os switches VPC sincronizem os endereços MAC e IP aprendidos pelo VPC. Devido a isso, o design mais simples para pools de VLAN é usar um único pool para implantações estáticas e criar um segundo para implantações dinâmicas.

Configurar o AEP (Attachable Access Entity Profile)

Duas partes principais da configuração da política de acesso foram concluídas; as definições de switch e interface e as definições de domínio/VLAN(s). Um objeto chamado 'Perfil de entidade de acesso anexável' (AEP) servirá para unir esses dois blocos.

Um "grupo de políticas" está ligado a um AEP em uma relação um-para-muitos que permite que o AEP agrupe interfaces e switches que compartilham requisitos de política semelhantes. Isso significa que somente um AEP precisa ser referenciado ao representar um grupo de interfaces em switches específicos.

Perfil de Entidade de Acesso Anexável



Na maioria das implantações, um único AEP deve ser usado para caminhos estáticos e um AEP adicional por domínio VMM.

A consideração mais importante é que as VLANs podem ser implantadas nas interfaces através do AEP. Isso pode ser feito mapeando EPGs para um AEP diretamente ou configurando um domínio do VMM para pré-provisionamento. Ambas as configurações fazem da interface associada uma porta de tronco ("switchport mode trunk" em switches herdados).

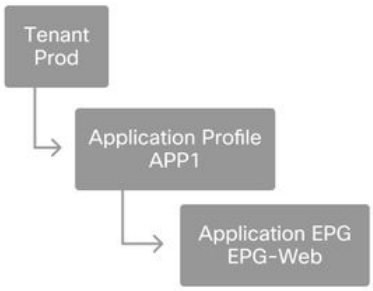
Por isso, é importante criar um AEP separado para L3Out ao usar portas roteadas ou subinterfaces roteadas. Se as SVIs forem usadas na L3Out, não será necessário criar uma AEP adicional.

Configurar o espaço, o APP e o EPG

A ACI usa um meio diferente de definir a conectividade usando uma abordagem baseada em políticas.

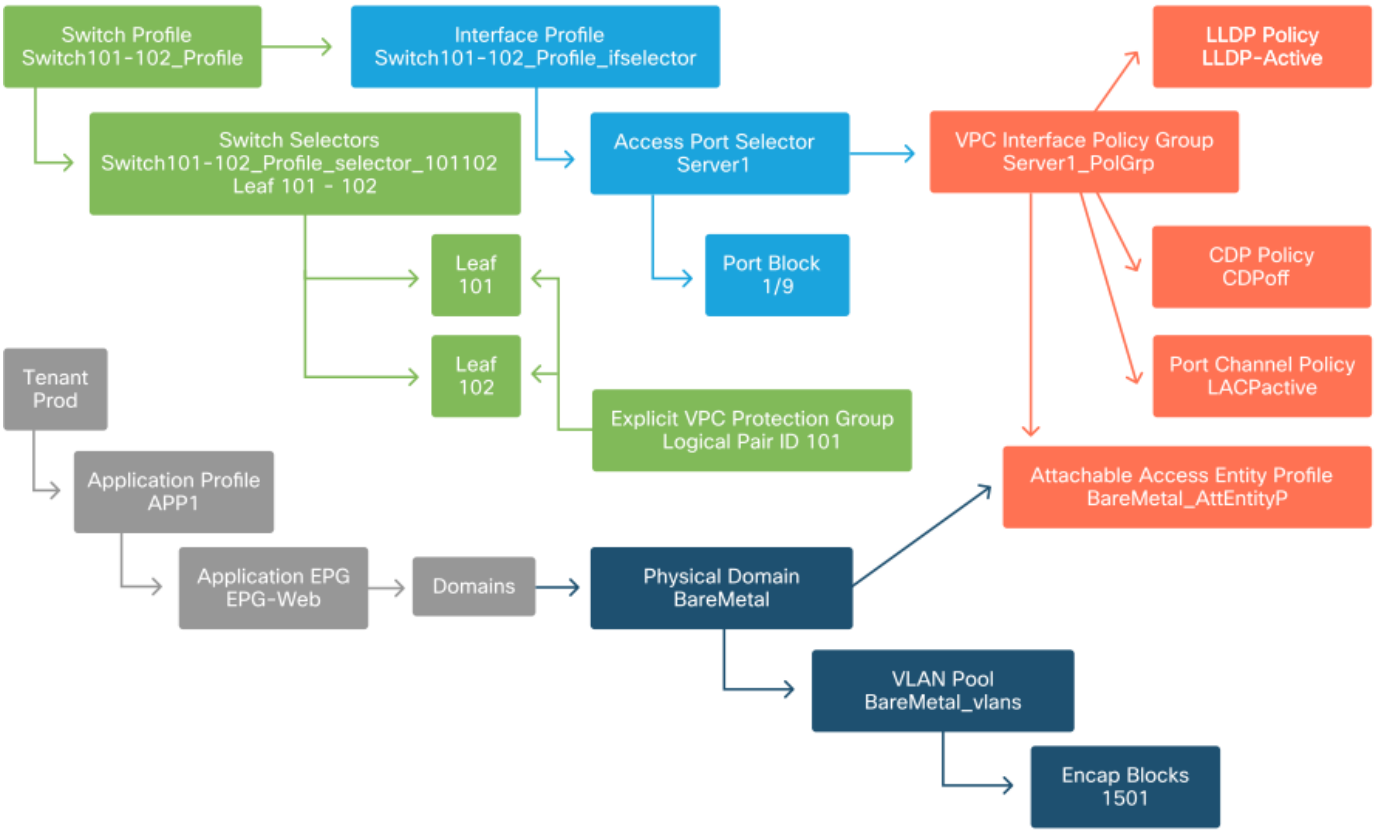
O objeto de nível mais baixo é chamado de 'Endpoint Group' (EPG). A construção do EPG é usada para definir um grupo de VMs ou servidores (endpoints) com requisitos de política semelhantes. Os 'Perfis de aplicativo', que existem em um espaço, são usados para agrupar EPGs logicamente.

Locatário, APP e EPG



A próxima etapa lógica é vincular o EPG ao domínio. Isso cria o link entre o objeto lógico que representa nossa carga de trabalho, o EPG e os switches/interfaces físicos, as políticas de acesso.

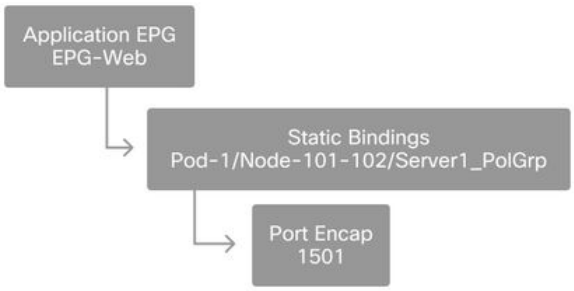
EPG para link de domínio



Configurar as vinculações estáticas do EPG

A última etapa lógica é programar a VLAN em uma interface de switch para um determinado EPG. Isso é especialmente importante se for usado um domínio físico, pois esse tipo de domínio exige uma declaração explícita para fazer isso. Isso permitirá que o EPG seja estendido para fora da estrutura e que o servidor bare-metal seja classificado no EPG.

Ligações estáticas

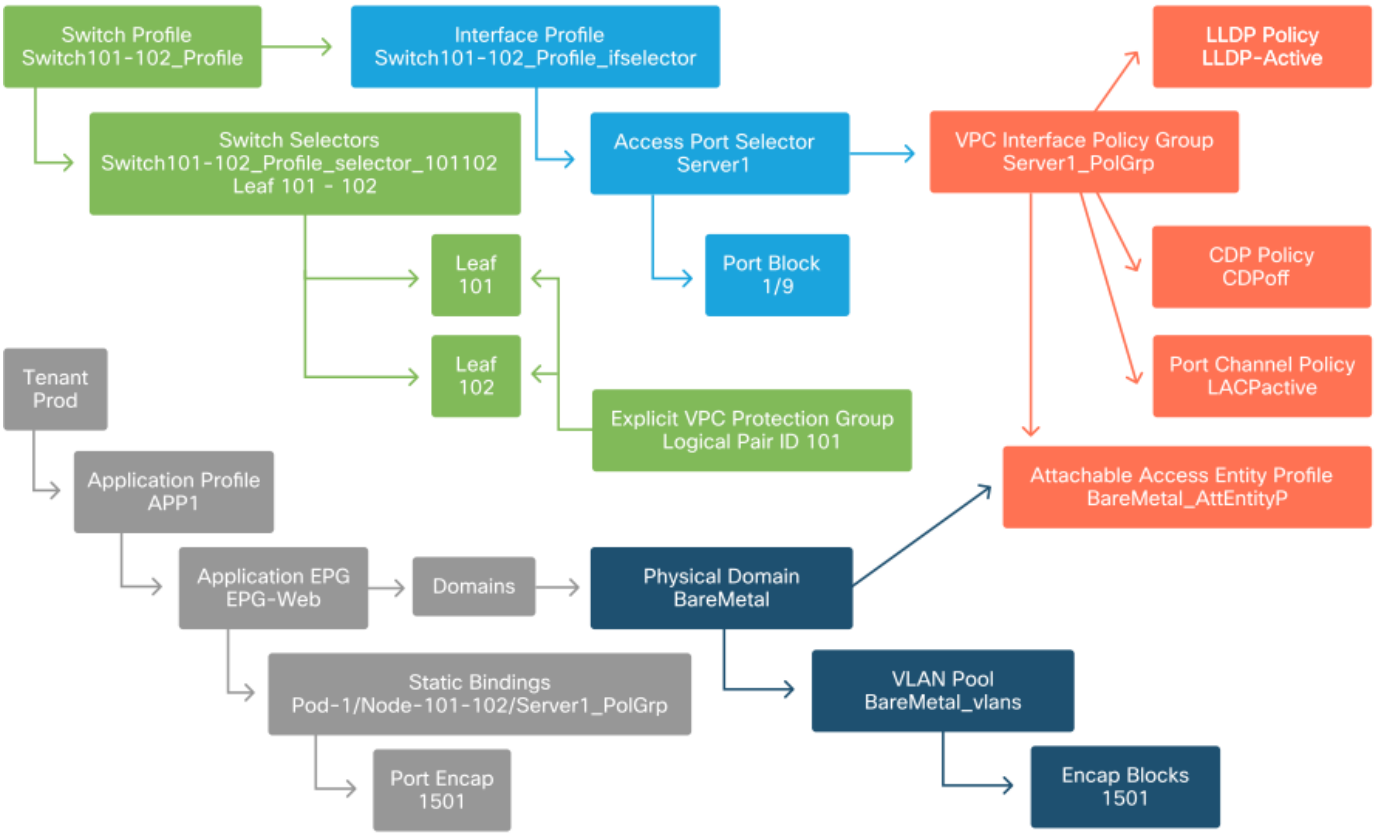


O 'Port Encap' referenciado precisa ser resolvível em relação ao 'VLAN Pool'. Se não for, uma falha será sinalizada. Isso é discutido na seção "Troubleshooting de fluxo de trabalho" deste capítulo.

Resumo da configuração da política de acesso

O diagrama a seguir resume todos os objetos criados para permitir a conectividade para o host através da VLAN-1501, usando uma conexão VPC com os switches leaf 101 e 102.

Conectividade de ACI bare-metal



Conexão de servidores adicionais

Com todas as políticas anteriores criadas, o que significaria conectar mais um servidor na porta Eth1/10 nos switches leaf 101 e 102 com um canal de porta?

Consultando o diagrama 'Conectividade de ACI bare-metal', será necessário criar pelo menos o seguinte:

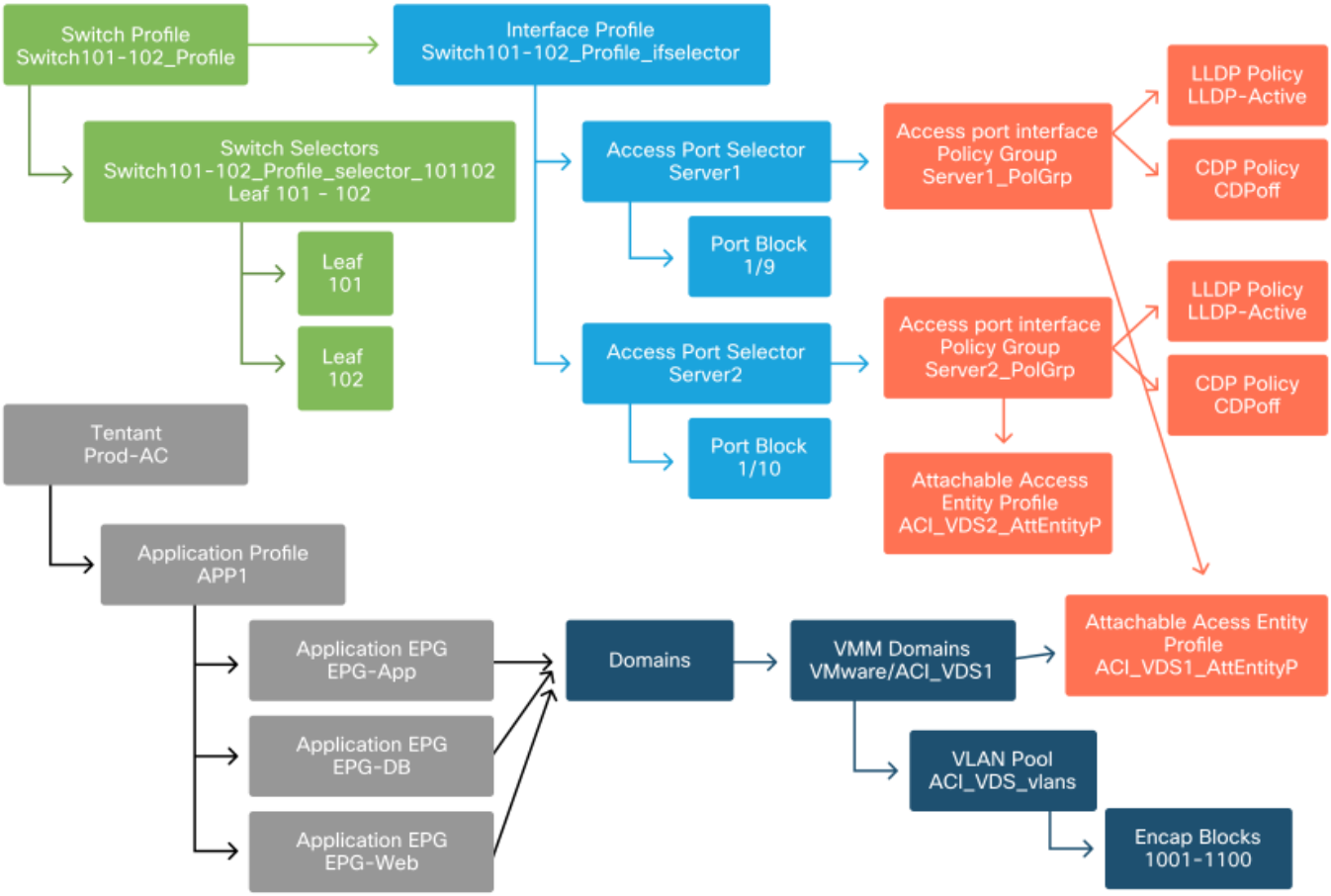
- Um seletor de porta de acesso e um bloco de porta extras.
- Um grupo de política de interface VPC extra.
- Uma vinculação estática extra com Port Encap.

Observe que para canais de porta LACP, um grupo de política de interface VPC dedicado deve ser usado, pois esse grupo de política VPC é o que define a ID do VPC.

No caso de links individuais, o grupo de política de interface não-VPC pode ser reutilizado para o servidor extra se o link exigir as mesmas propriedades de porta.

As políticas resultantes se pareceriam com a imagem a seguir.

Conectando server2 à configuração



O que vem a seguir?

A próxima seção passará por alguns cenários de falha de política de acesso, começando com a topologia e o caso de uso discutidos nesta visão geral.

Troubleshooting de fluxo de trabalho

Os seguintes cenários de solução de problemas podem ser encontrados ao trabalhar com políticas de acesso:

- Relacionamento ausente entre duas ou mais entidades na política de acesso, como grupo de política de acesso não vinculado a um AEP.

- Uma política ausente ou inesperada está ligada a uma determinada política de acesso, como uma política LLDP chamada 'lldp_enabled', enquanto na realidade a configuração da política tem LLDP rx/tx desabilitado.
- Um valor ausente ou inesperado na política de acesso, como o encapsulamento de ID de VLAN configurado, está ausente no Pool de VLANs configurado.
- Relacionamento ausente entre o EPG e a política de acesso, como nenhuma associação de domínio físico ou virtual com o EPG.

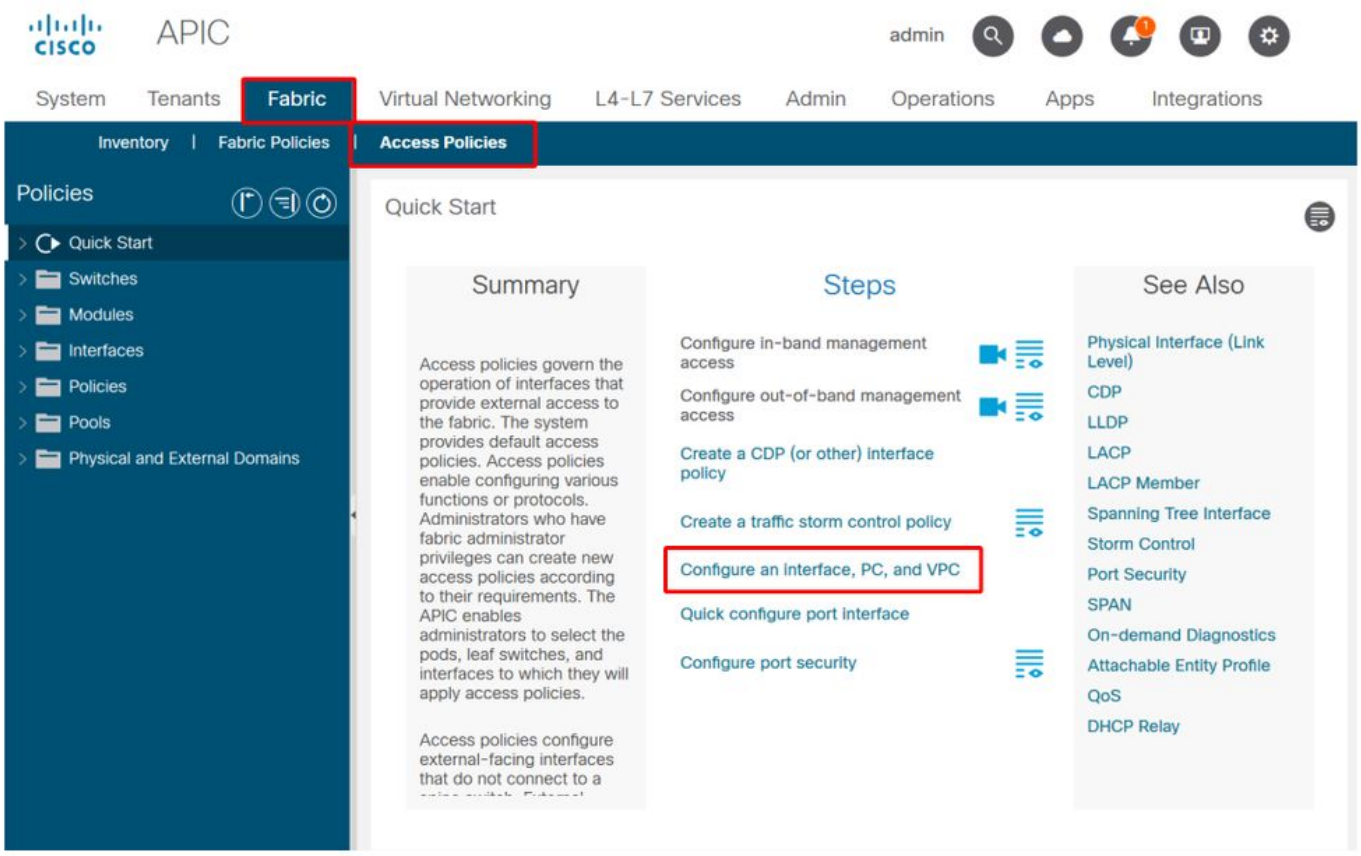
A maior parte da solução de problemas acima envolve percorrer as relações da política de acesso para entender se alguma relação está faltando ou para entender quais políticas estão configuradas e/ou se a configuração está resultando no comportamento desejado.

Usando o "Configure interface, PC, and VPC Quick Start" para Troubleshooting

Na GUI do APIC, o assistente de início rápido 'Configurar interface, PC e VPC' facilita a pesquisa da política de acesso, fornecendo ao administrador uma visualização agregada das políticas de acesso existentes. Este assistente de início rápido pode ser encontrado na GUI em:

'Estrutura > Políticas de acesso > Início rápido > Etapas > Configurar interface, PC e VPC'.

Localização do Início Rápido 'Configurar Interface, PC e VPC'



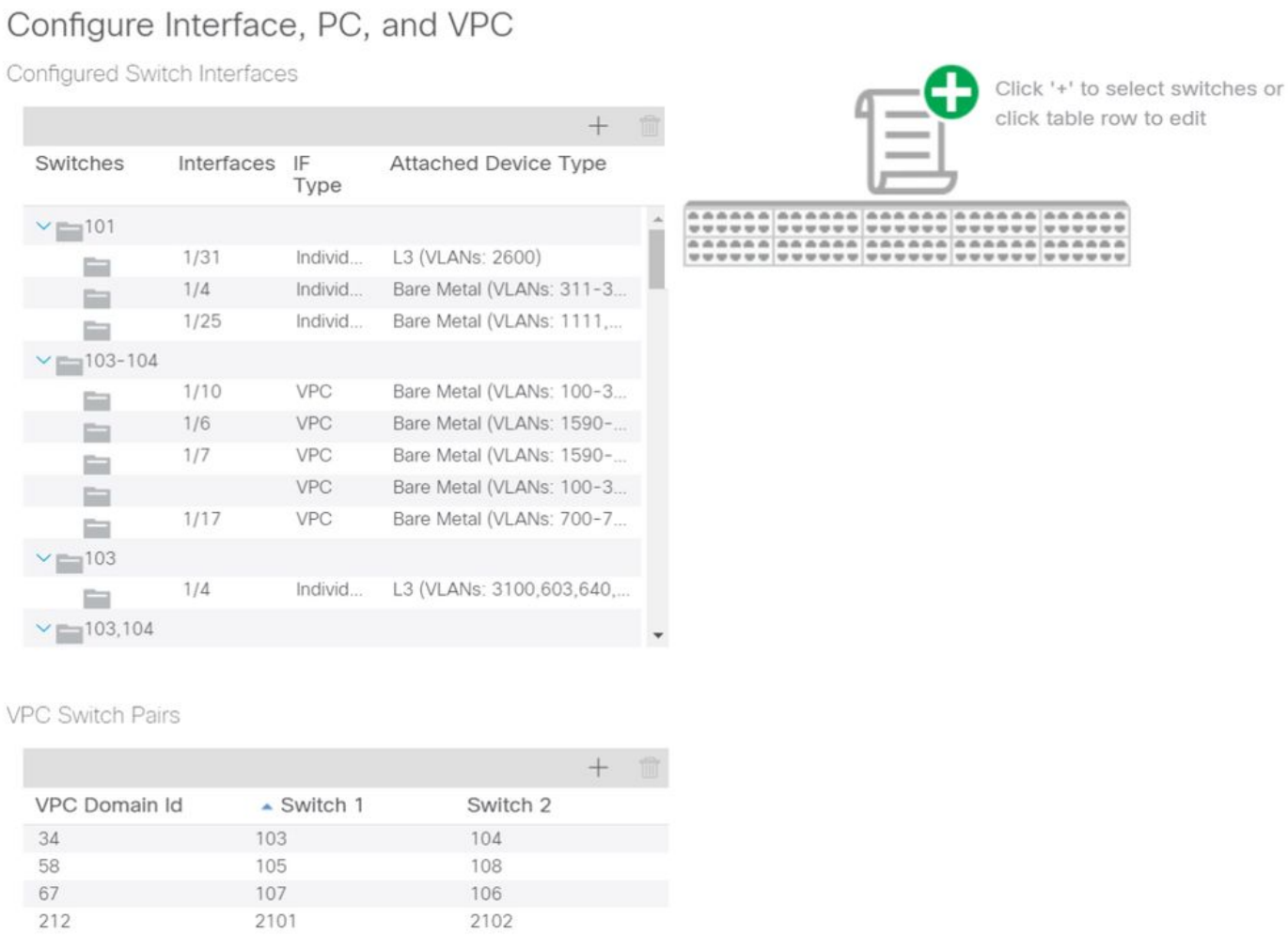
Embora o assistente tenha 'Configurar' no nome, é excepcionalmente útil para fornecer uma exibição agregada das várias políticas de acesso que devem ser configuradas para programar as interfaces. Essa agregação serve como uma exibição única para entender quais políticas já estão definidas e reduz efetivamente o número de cliques necessários para começar a isolar problemas relacionados à política de acesso.

Quando a visualização Início rápido é carregada, a visualização 'Interfaces de switch

configuradas' (painel superior esquerdo) pode ser consultada para determinar as políticas de acesso existentes. O assistente agrupa as entradas sob pastas que representam switches individuais ou vários switches leaf, dependendo da configuração das políticas de acesso.

Como uma demonstração do valor do assistente, as seguintes capturas de tela do assistente são apresentadas, sabendo que o leitor não tem um entendimento anterior da topologia de estrutura:

Exibição da demonstração do Início rápido 'Configurar interface, PC e VPC'



O painel 'Interfaces de switch configuradas' mostra mapeamentos de política de acesso. O painel 'Pares de Comutadores VPC' mostra as definições do Grupo de Proteção VPC concluídas.

A tabela abaixo mostra um subconjunto de definições de política de acesso concluídas que podem ser derivadas da captura de tela acima.

Subconjunto de políticas de acesso concluídas que podem ser derivadas da exibição Início rápido acima

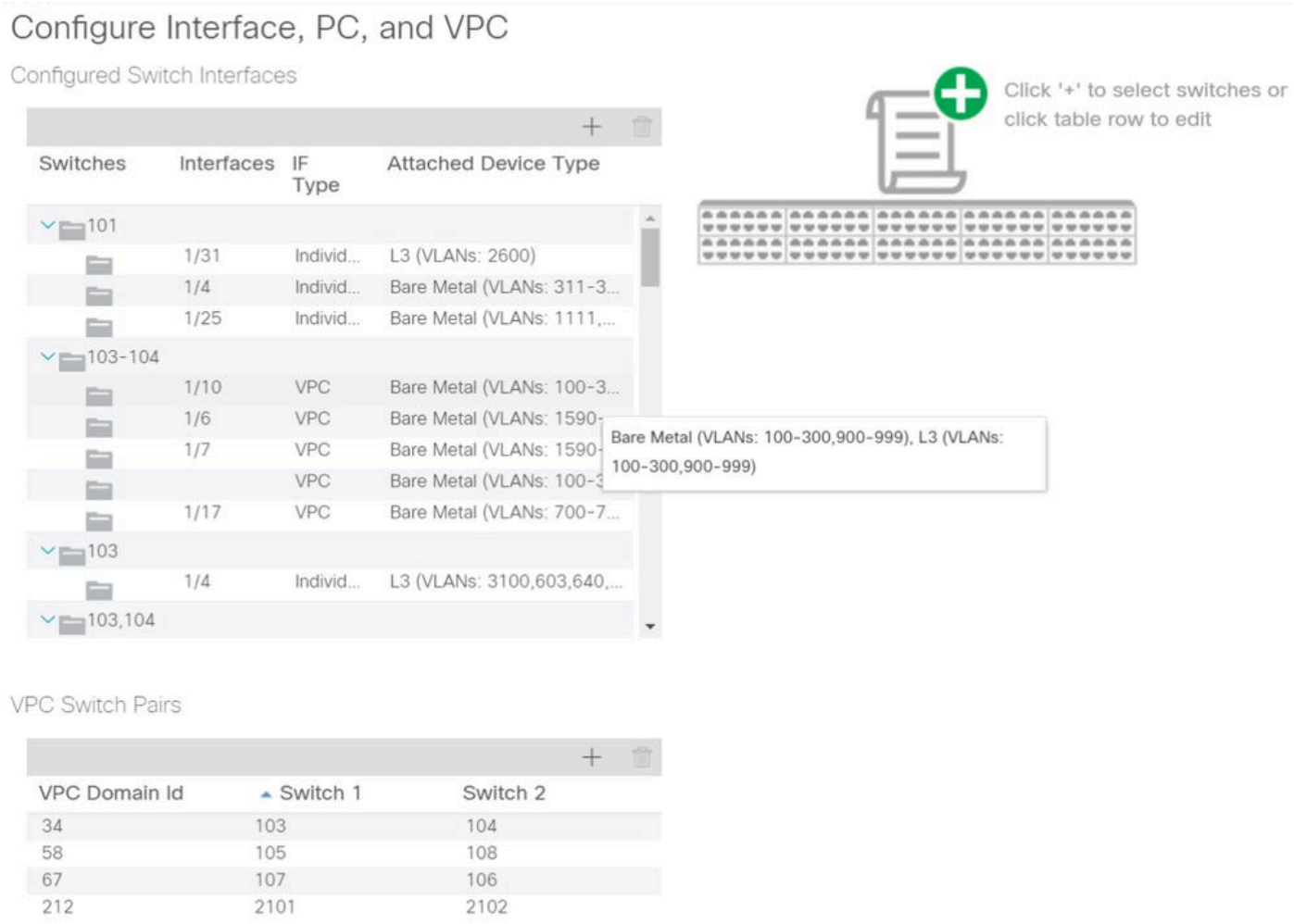
Nó do Switch	Interface	Tipo de Grupo de Política	Tipo de domínio	VLANs
101	1/31	Individual	Roteado (L3)	2600
101	1/4	Individual	Phys (bare metal)	311-3..?
103-104	1/10	VPC	Phys (bare metal)	100-3..?

As entradas da coluna VLAN são intencionalmente incompletas, dada a visualização padrão.

Da mesma forma, as políticas de 'Grupo de proteção VPC' concluídas podem ser derivadas da exibição 'Pares de switches VPC' (painel inferior esquerdo). Sem os 'Grupos de Proteção VPC', os VPCs não podem ser implantados, pois essa é a política que define o Domínio VPC entre dois nós de folha.

Leve em consideração que, devido ao tamanho do painel, as entradas longas não ficam completamente visíveis. Para visualizar o valor completo de qualquer entrada, passe o ponteiro do mouse sobre o campo de interesse.

O ponteiro do mouse está passando o mouse sobre o campo 'Tipo de dispositivo conectado' para a entrada 103-104, int 1/10 VPC:



Ao passar o mouse sobre o painel, as entradas completas ficam visíveis.

Subconjunto atualizado de políticas de acesso concluídas usando detalhes do mouse

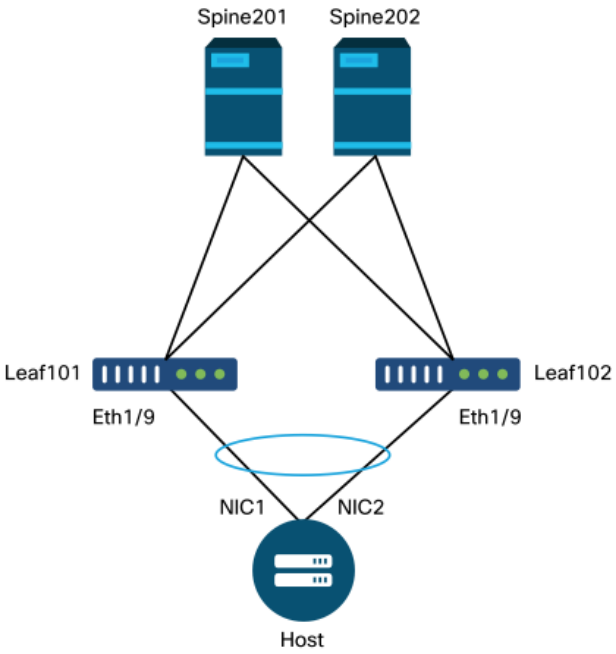
Nó do Switch	Interface	Tipo de Grupo de Política	Tipo de domínio	VLANs
101	1/31	Individual	Roteado (L3)	2600
101	1/4	Individual	Phys (bare metal)	311-320
103-104	1/10	VPC	Phys (bare metal)	100-300,900-999
103-104	1/10	VPC	Roteado (L3)	100-300,900-

As associações VLAN completas podem agora ser observadas e compreendidas para solução de problemas e verificação.

Cenários de Troubleshooting

Para os cenários de Troubleshooting a seguir, consulte a mesma topologia do capítulo anterior.

Topologia da seção 'Introdução' da política de acesso



Cenário 1: Falha F0467 — caminho inválido, nwissues

Essa falha é gerada quando uma declaração de switch/porta/VLAN é feita sem as políticas de acesso correspondentes em vigor para permitir que essa configuração seja aplicada corretamente. Dependendo da descrição dessa falha, um elemento diferente da relação da política de acesso pode estar ausente.

Depois de implantar uma ligação estática para a interface VPC acima com a VLAN 1501 de encapsulamento em tronco sem a relação de política de acesso correspondente em vigor, a seguinte falha é gerada no EPG:

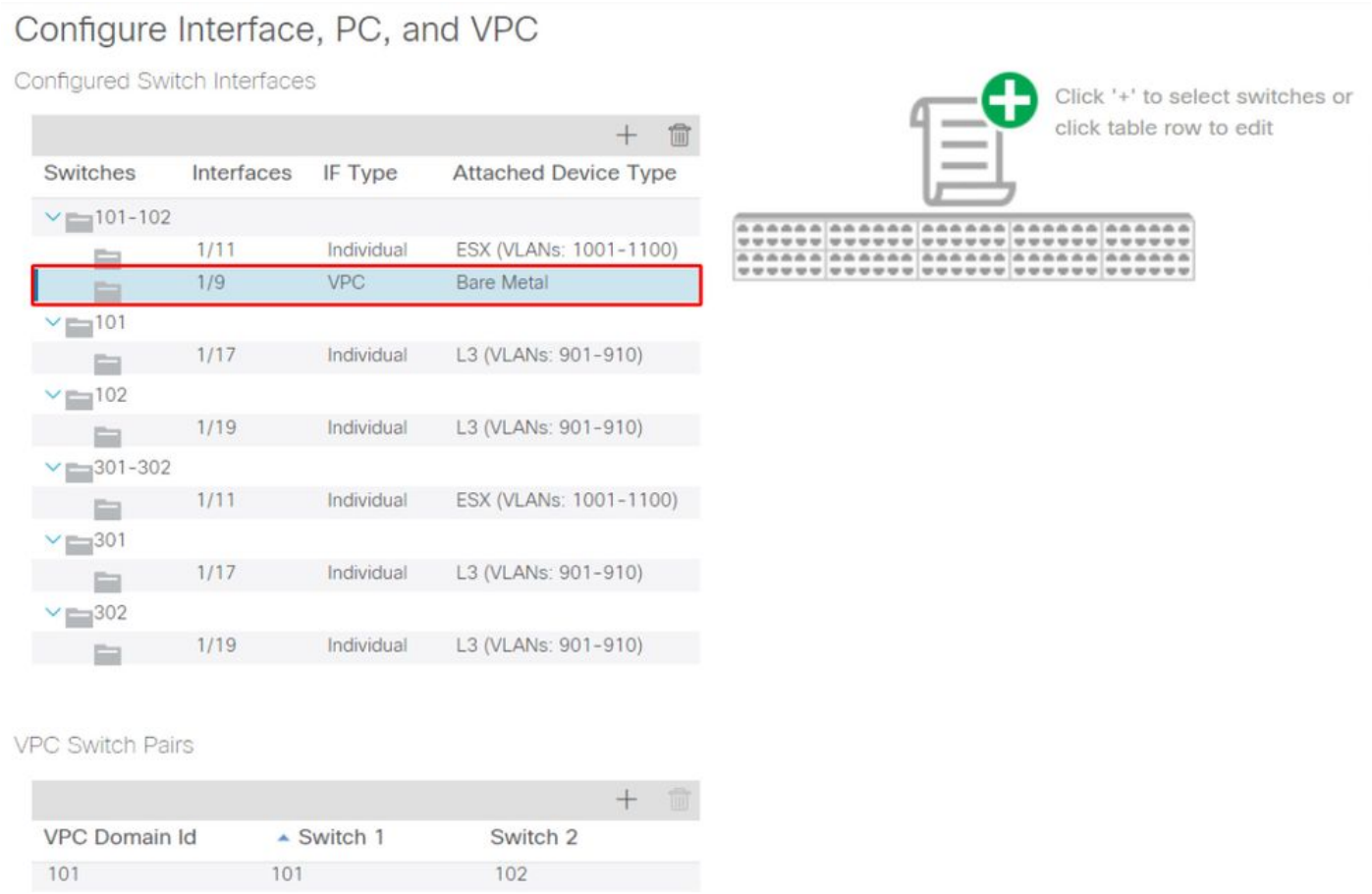
Falha: F0467

Descrição: Delegado de falha: Falha na configuração para o nó uni/tn-Prod1/ap-App1/epg-EPG-Web 101_101_102_eth1_9 devido à configuração de caminho inválido, configuração de VLAN inválida, mensagem de depuração: vlan inválida: vlan-1501 :a ID do segmento STP não está presente para Encap. O EPG não está associado a um domínio ou o domínio não tem essa vlan atribuída a ele;caminho inválido: vlan-1501 :Não há domínio, associado ao EPG e à Porta, que tenha exigido VLAN;

A partir da descrição de falha acima, há algumas indicações claras sobre o que poderia estar causando o disparo da falha. Há um aviso para verificar os relacionamentos da política de acesso, bem como para verificar a associação do domínio ao EPG.

Ao analisar a visualização Início rápido no cenário descrito acima, a política de acesso claramente não tem VLANs.

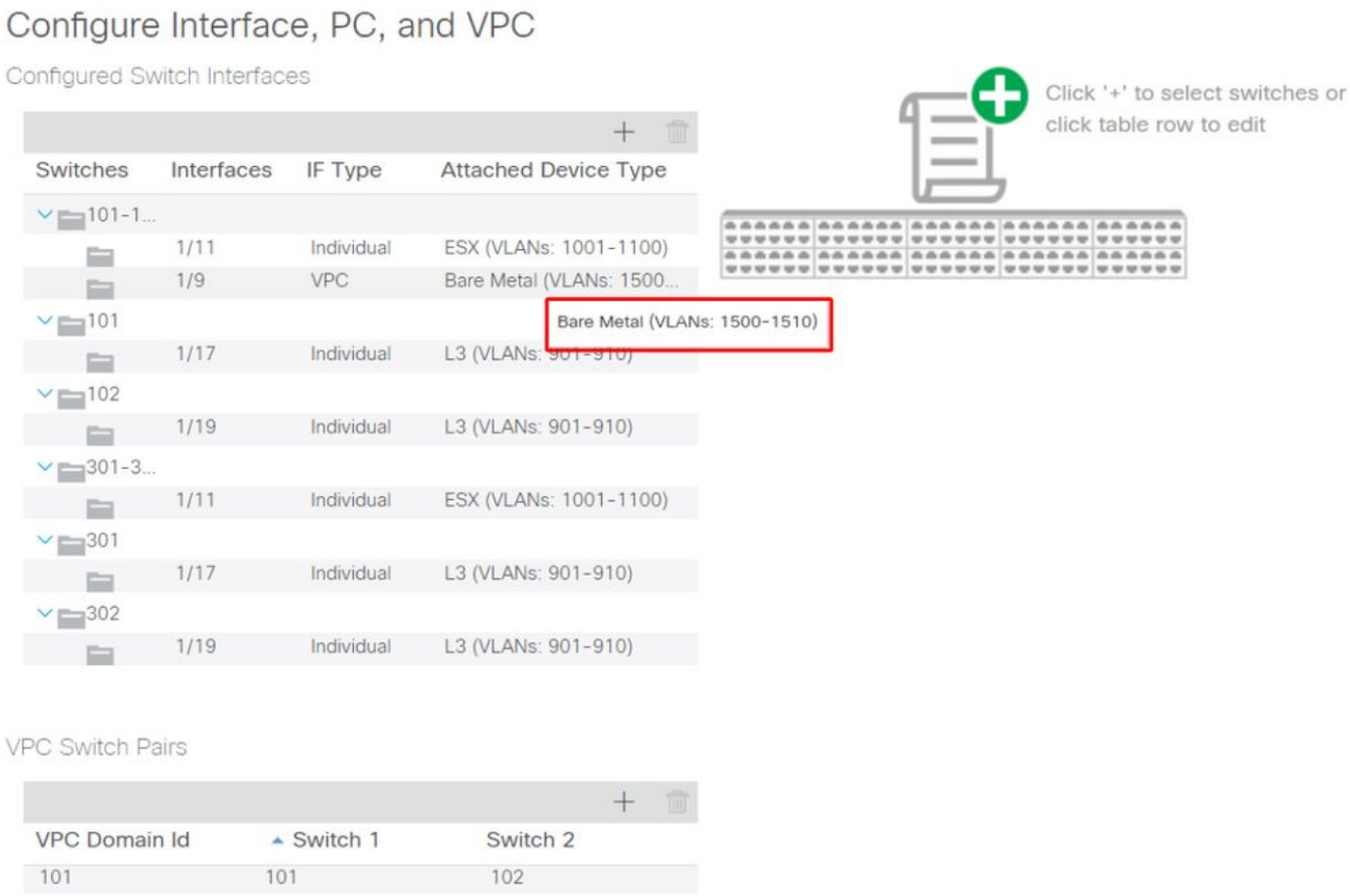
Visualização Início rápido onde 101-102, Int 1/9 VPC está sem VLANs



Observe que a entrada não tem uma referência a nenhum ID de VLAN.

Depois de corrigida, a visualização Início rápido exibirá '(VLANs 1500-1510)'.

101-102, Int 1/9 VPC agora mostra Bare Metal (VLANs: 1500-1510)



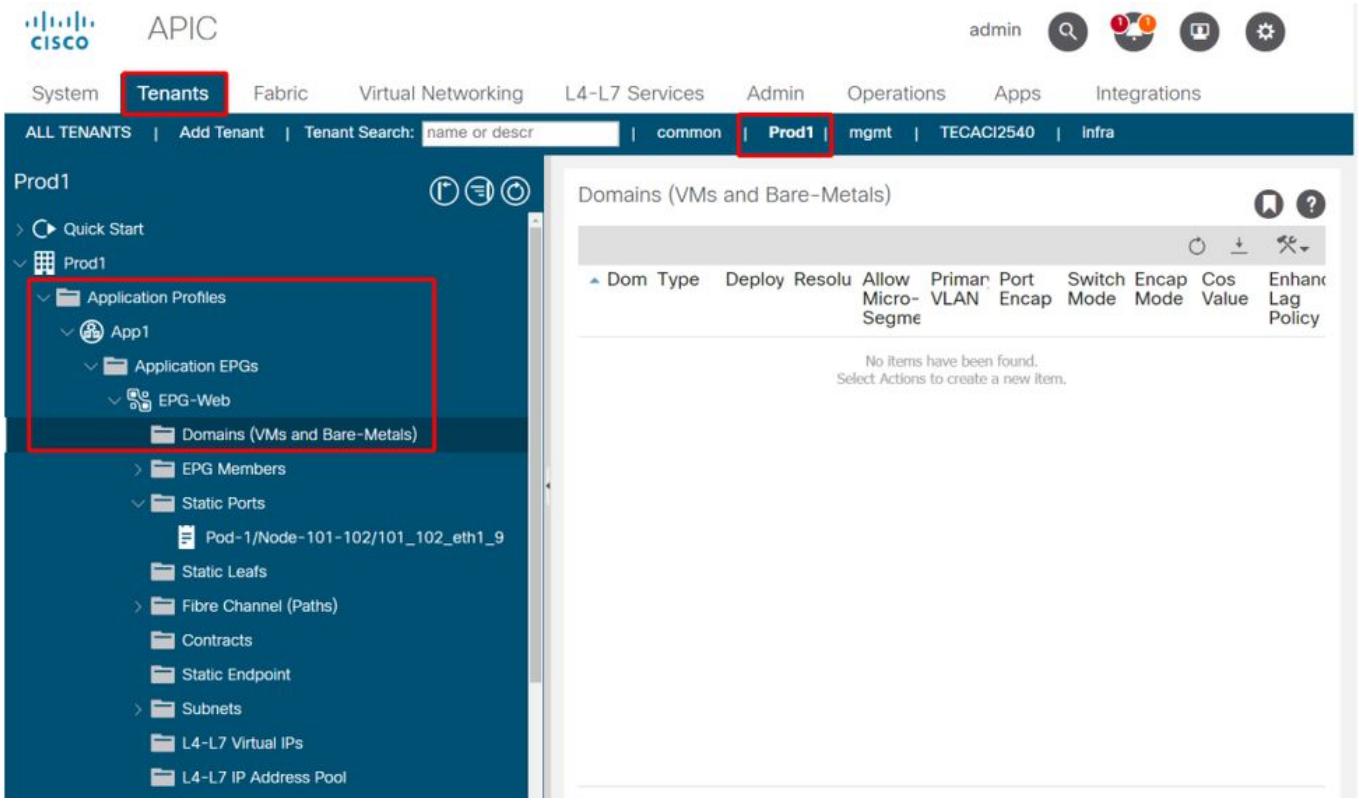
No entanto, a falha de EPG ainda existe com a seguinte descrição atualizada da falha F0467:

Falha: F0467

Descrição: Delegate Fault: Falha na configuração para uni/tn-Prod1/ap-App1/epg-EPG-Web node 101_101_102_eth1_9 devido à configuração de caminho inválido, mensagem de depuração: caminho inválido: vlan-150: Não há domínio, associado ao EPG e à porta, que tenha exigido VLAN.

Com a falha atualizada acima, verifique as associações de domínio EPG para descobrir que não há domínios vinculados ao EPG.

EPG-Web tem associação de portas estáticas, mas não tem associações de domínio



Quando o domínio que contém a VLAN 1501 estiver associado ao EPG, nenhuma outra falha será gerada.

Cenário 2: Não é possível selecionar o VPC como um caminho para implantação na porta estática EPG ou no L3Out Logical Interface Profile (SVI)

Ao tentar configurar um VPC como um caminho em uma entrada de SVI de porta estática EPG ou L3Out Logical Interface Profile, o VPC específico a ser implantado não é exibido como uma opção disponível.

Ao tentar implantar uma vinculação estática VPC, há dois requisitos rígidos:

1. O Grupo de Proteção Explícita do VPC deve ser definido para o par de switches leaf em questão.
2. O mapeamento completo da política de acesso deve ser definido.

Ambos os requisitos podem ser verificados na visualização Início rápido, como mostrado acima. Se nenhum estiver completo, o VPC simplesmente não aparecerá como uma opção disponível para Ligações de porta estáticas.

Cenário 3: Falha F0467 — encapsulamento de estrutura já usado em outro EPG

Por padrão, as VLANs têm um escopo global. Isso significa que um determinado ID de VLAN pode ser usado apenas para um único EPG em um determinado switch leaf. Qualquer tentativa de reutilizar a mesma VLAN em vários EPGs dentro de um determinado switch leaf resultará na seguinte falha:

Falha: F0467

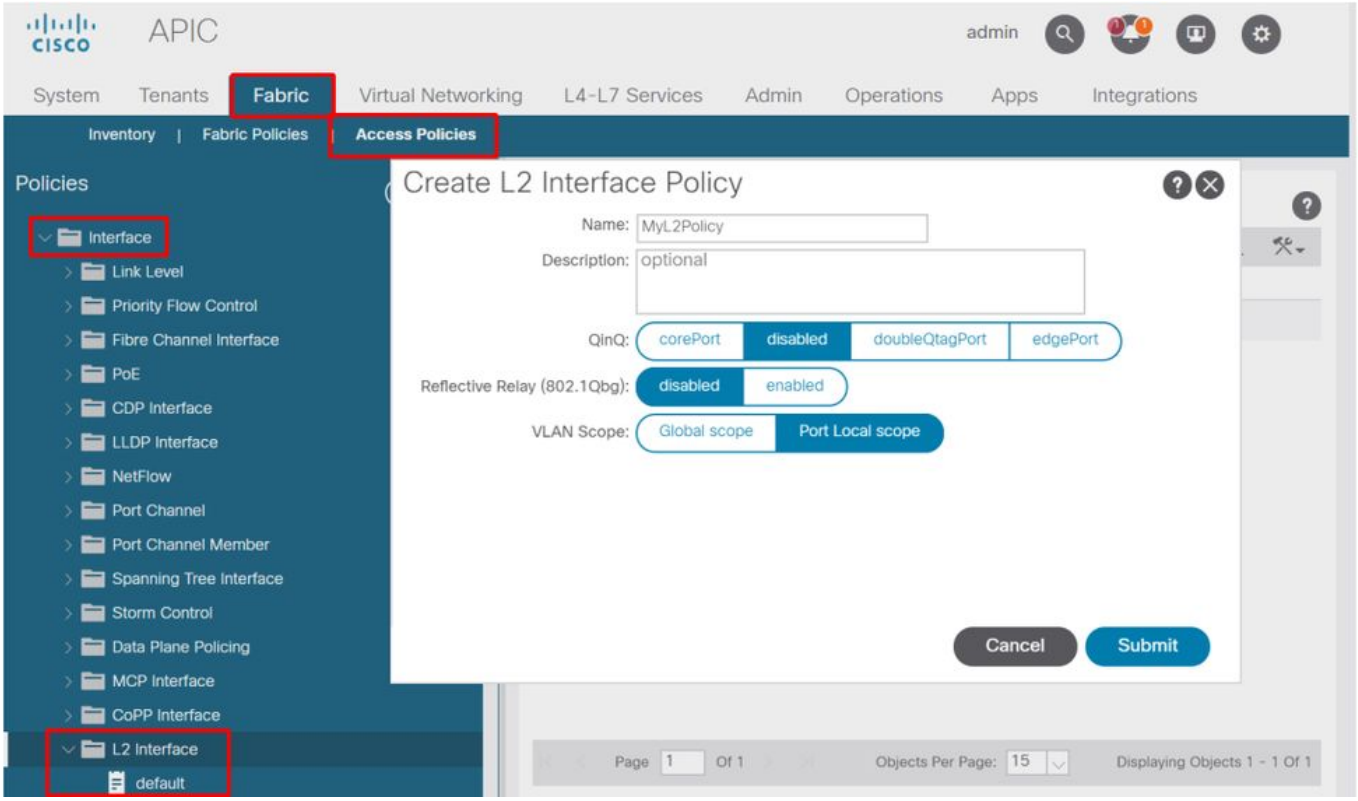
Descrição: Delegate Fault: Falha na configuração para uni/tn-Prod1/ap-App1/epg-EPG-BusinessApp node 102 101_102_eth1_8 devido a Encap já usado em outro EPG, mensagem de

depuração: encapsulamento já em uso: Encap já está em uso por Prod1:App1:EPG-Web;

Além de selecionar uma VLAN diferente, outra opção para fazer essa configuração funcionar é considerar o uso do Escopo de VLAN 'Port Local'. Esse escopo permite que as VLANs sejam mapeadas em uma base por interface, o que significa que a VLAN-1501 poderia ser potencialmente usada para diferentes EPGs, em várias interfaces, na mesma folha.

Embora o escopo 'Porta Local' seja associado em uma base de Grupo de Políticas (especificamente através de uma política L2), ele é aplicado no nível de folha.

Local para alterar a configuração de 'Escopo de VLAN' na GUI do APIC



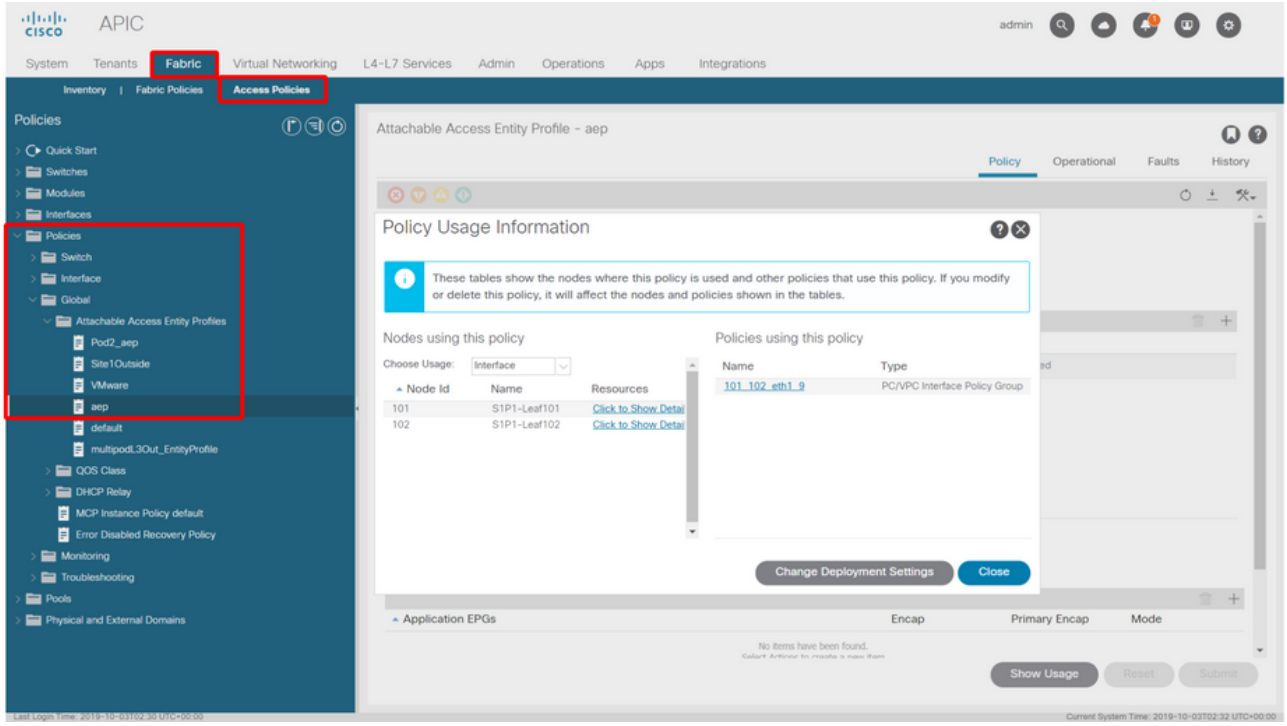
Antes de implementar a configuração de escopo da VLAN 'Port Local', consulte o "Guia de configuração de rede da camada 2 do Cisco APIC" em Cisco.com para garantir que suas limitações e restrições de projeto sejam aceitáveis para os casos de uso e projetos desejados.

Menções especiais

Mostrar Uso

Embora não seja específico para políticas de acesso, um botão está disponível na maioria dos objetos na GUI rotulada como 'Mostrar uso'. Esse botão executa uma pesquisa de política com raiz no objeto selecionado para determinar quais nós/interfaces folha têm uma relação direta com ele. Isso pode ser útil tanto para o cenário de pesquisa geral quanto para compreender se um objeto ou política específica está mesmo em uso.

Na captura de tela abaixo, o AEP selecionado está sendo usado por duas interfaces diferentes. Isso implica que fazer uma modificação no AEP terá um impacto direto nas interfaces associadas.



Sobreposição de pools de VLAN

Embora a função das políticas de acesso seja permitir que uma VLAN específica seja implantada em uma interface, há um uso adicional que deve ser considerado durante a fase de projeto. Especificamente, o domínio é usado no cálculo do ID de VXLAN (chamado Fabric Encap) ligado ao encapsulamento externo. Embora essa funcionalidade geralmente não tenha nenhuma influência importante no tráfego de dataplane, tais IDs são especialmente relevantes para um subconjunto de protocolos que inundam a estrutura, incluindo BPDUs de árvore de abrangência. Se for esperado que as BPDUs de VLAN-<id> que entram no leaf1 saiam da Folha 2 (por exemplo, tendo switches legados que convergem spanning-tree através da ACI), VLAN-<id> deve ter o mesmo encapsulamento de estrutura em ambos os nós de folha. Se o valor de encapsulamento da estrutura for diferente para as mesmas VLANS de acesso, as BPDUs não atravessarão a estrutura.

Como mencionado na seção anterior, evite a configuração das mesmas VLANs em vários domínios (VMM vs Físico, por exemplo), a menos que seja tomado cuidado especial para garantir que cada domínio seja aplicado apenas a um conjunto exclusivo de switches leaf. No momento em que ambos os domínios podem ser resolvidos no mesmo switch leaf para uma determinada VLAN, há uma chance de que a VXLAN subjacente possa ser alterada após uma atualização (ou recarga limpa) que pode levar, por exemplo, a problemas de convergência de STP. O comportamento é o resultado de cada domínio ter um valor numérico exclusivo (o atributo 'base') que é usado na seguinte equação para determinar o ID de VXLAN:

VXLAN VNID = Base + (encap — from_encap)

Para validar quais domínios são enviados para uma determinada folha, um moquery pode ser executado na classe 'stpAllocEncapBlkDef':

```
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
```

A partir dessa saída, discerne as seguintes definições de política de acesso:

- Há um pool de VLAN programado com um bloco de VLANs que define explicitamente as VLANs 1500-1510.
- Esse bloco de VLANs está ligado a um domínio chamado 'physvlans'.
- O valor base usado no cálculo de VXLAN é 8492.
- O cálculo resultante de VXLAN para VLAN-1501 seria 8492 + (1501-1500) = 8493 como o encapsulamento de estrutura.

O ID de VXLAN resultante (neste exemplo, 8493) pode ser verificado com o seguinte comando:

```
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
```

Se houver qualquer outro pool de VLAN contendo VLAN-1501 que seja empurrado para a mesma folha, uma atualização ou recarga limpa poderia potencialmente capturar um valor base exclusivo (e subsequentemente um Fabric Encap diferente), o que fará com que as BPDUs parem de fazê-lo para outra folha que se espera receber BPDUs na VLAN-1501.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.