# Dépannage des politiques d'accès ACI

## Contenu



## Introduction

Ce document décrit les étapes à suivre pour comprendre et dépanner les politiques d'accès ACI.

## Informations générales

Le contenu de ce document a été extrait du livre Troubleshooting Cisco Application Centric Infrastructure, Second Edition, en particulier les chapitres **Access Policies - Overview** and **Access Policies - Troubleshooting Workflow**.

## Présentation des politiques d'accès

Comment l'administrateur ACI configure-t-il un VLAN sur un port du fabric ? Comment l'administrateur de l'ACI commence-t-il à résoudre les erreurs liées aux politiques d'accès ? Cette section explique comment résoudre les problèmes liés aux politiques d'accès au fabric.

Avant de passer aux scénarios de dépannage, il est impératif que le lecteur comprenne bien le fonctionnement des politiques d'accès et leurs relations au sein du modèle objet ACI. À cette fin, le lecteur peut consulter les documents « ACI Policy Model » et « APIC Management Information Model Reference », disponibles sur le site Cisco.com (https://developer.cisco.com/site/apic-mim-ref-api/).

La fonction des politiques d'accès est d'activer une configuration spécifique sur les ports de liaison descendante d'un commutateur Leaf. Avant de définir une politique de locataire autorisant le trafic via un port de fabric ACI, les politiques d'accès associées doivent être en place.

En général, les politiques d'accès sont définies lorsque de nouveaux commutateurs Leaf sont ajoutés au fabric, ou lorsqu'un périphérique est connecté aux liaisons descendantes Leaf ACI ; mais selon la dynamique d'un environnement, les politiques d'accès peuvent être modifiées pendant le fonctionnement normal du fabric. Par exemple, pour autoriser un nouvel ensemble de VLAN ou ajouter un nouveau domaine routé aux ports d'accès du fabric.

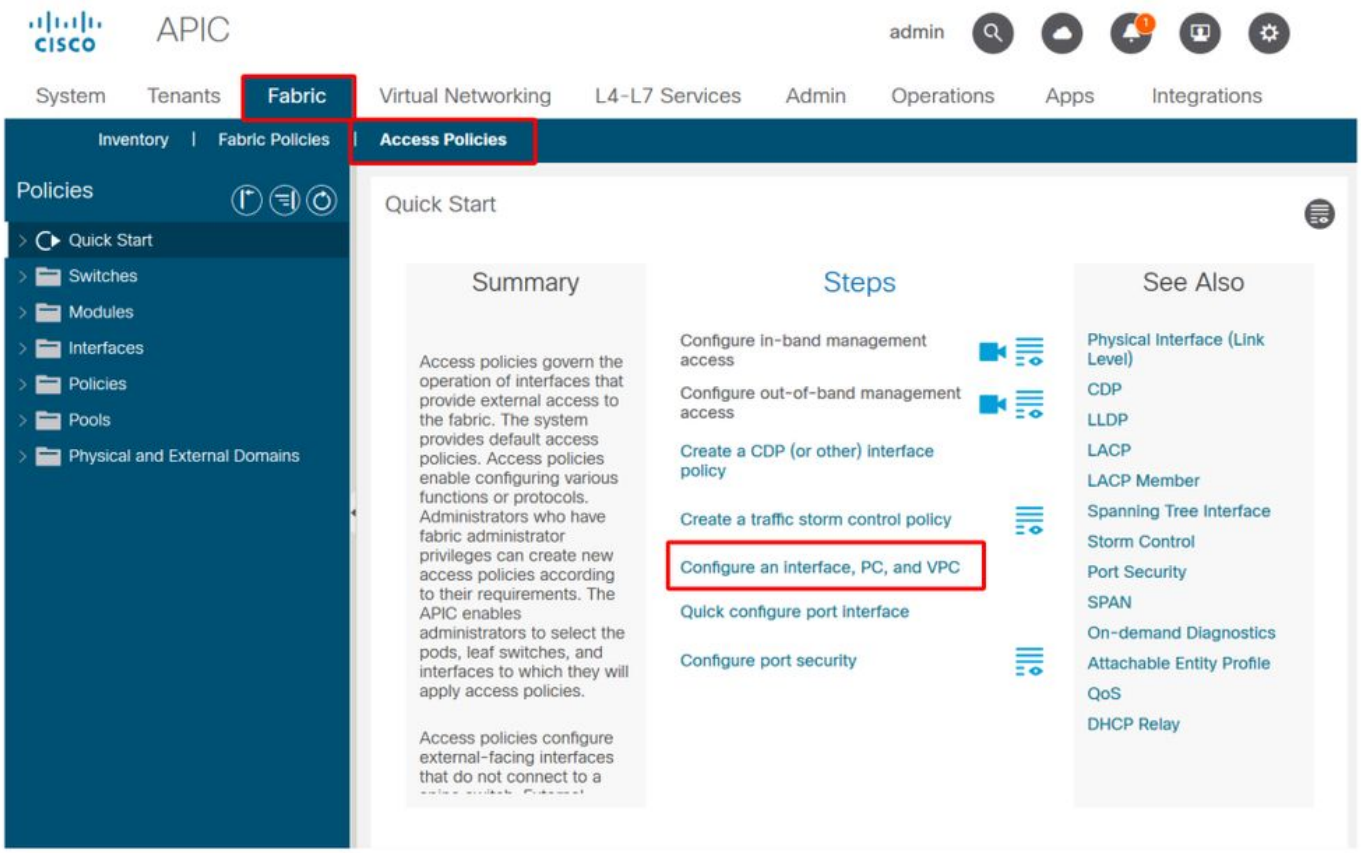
Les politiques d'accès de l'ACI, bien que quelque peu intimidantes au départ, sont extrêmement flexibles et sont conçues pour simplifier le provisionnement de la configuration sur un réseau SDN à grande échelle en évolution constante.

## Configuration de la stratégie d'accès : Méthodologie

Les politiques d'accès peuvent être configurées indépendamment, c'est-à-dire en créant tous les objets requis indépendamment, ou peuvent être définies à l'aide des nombreux assistants fournis par l'interface graphique utilisateur de l'ACI.

Les assistants sont très utiles car ils guident l'utilisateur tout au long du workflow et s'assurent que toutes les stratégies requises sont en place.

### Stratégies d'accès — Assistant Démarrage rapide

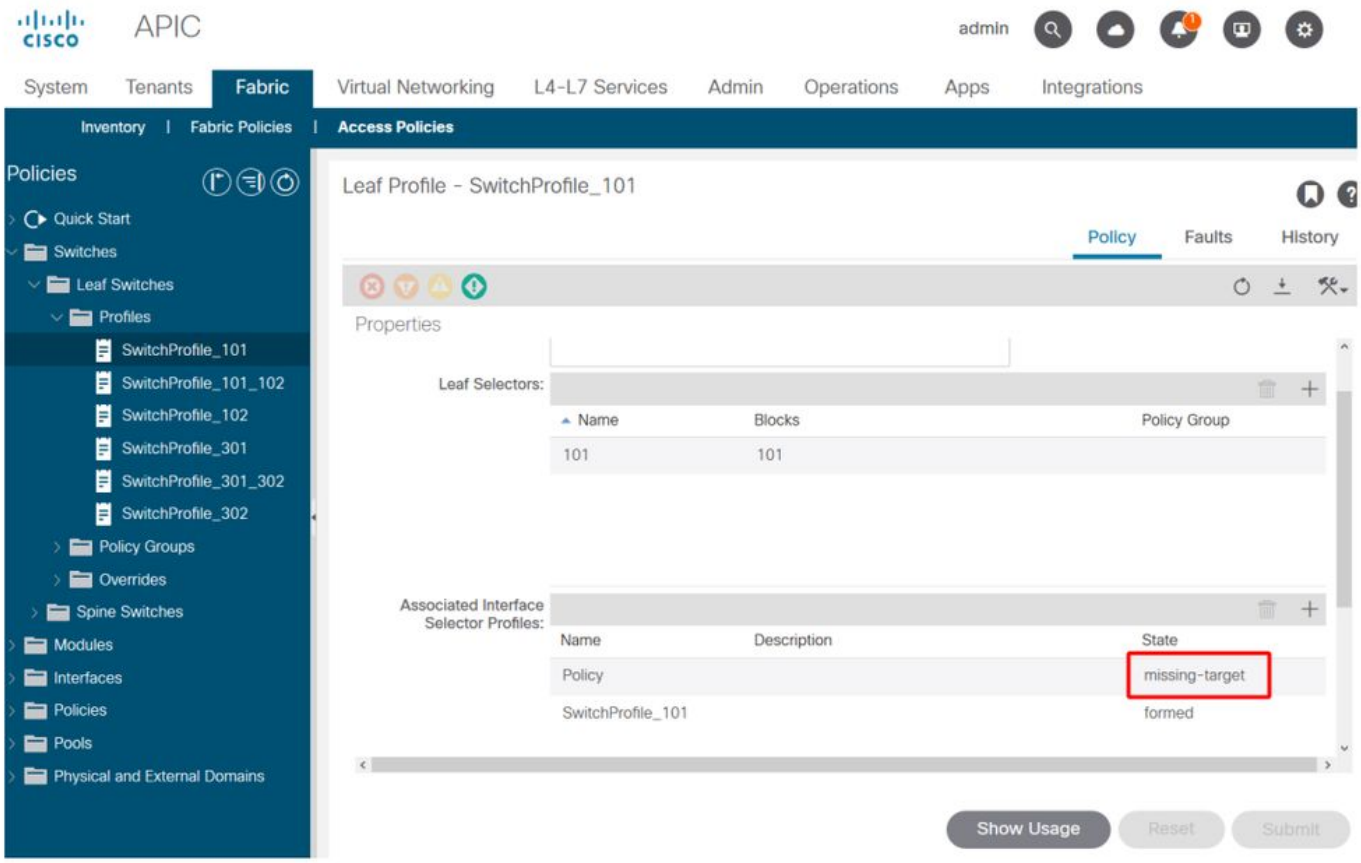



L'image ci-dessus montre la page de démarrage rapide où plusieurs assistants sont disponibles.

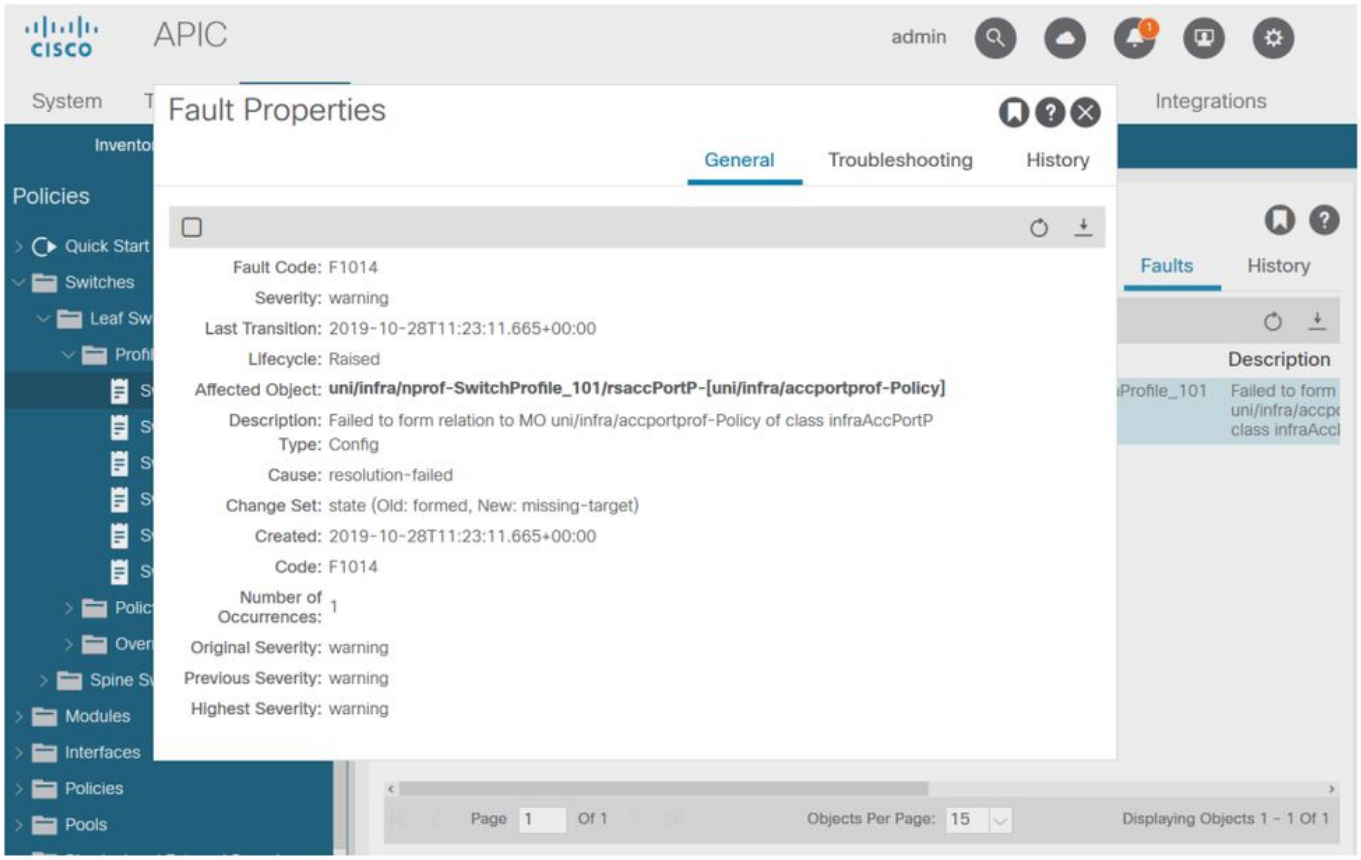
Une fois qu'une stratégie d'accès est définie, la recommandation générique consiste à valider la stratégie en s'assurant que tous les objets associés ne présentent aucune défaillance.

Par exemple, dans la figure ci-dessous, un profil de commutateur a attribué une stratégie de sélection d'interface qui n'existe pas. Un utilisateur attentif pourra facilement repérer l'état "**cible manquante**" de l'objet et vérifier qu'une erreur a été signalée depuis l'interface utilisateur graphique :

**Profil leaf — SwitchProfile_101**




Profil leaf — SwitchProfile_101 — Défaut




Dans ce cas, la correction de la panne serait aussi simple que la création d'un nouveau profil de sélection d'interface appelé « Stratégie ».

La configuration manuelle des politiques d'accès de base sera étudiée dans les paragraphes

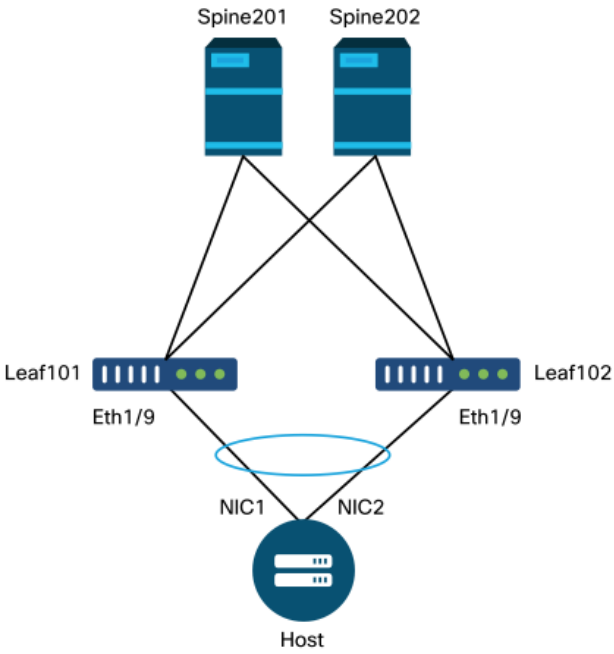
suivants.

## Politiques d'accès configurations de base manuelles

Lors du déploiement des politiques d'accès, des objets sont définis pour exprimer l'utilisation prévue des liaisons descendantes données. La déclaration qui programme les liaisons descendantes (par exemple, l'attribution de port statique EPG) repose sur cette intention exprimée. Cela permet de faire évoluer la configuration et de regrouper logiquement des objets d'utilisation similaires, tels que des commutateurs ou des ports spécifiquement connectés à un périphérique externe donné.

Reportez-vous à la topologie ci-dessous pour la suite de ce chapitre.

### Topologie de la définition de la stratégie d'accès pour le serveur à double résidence

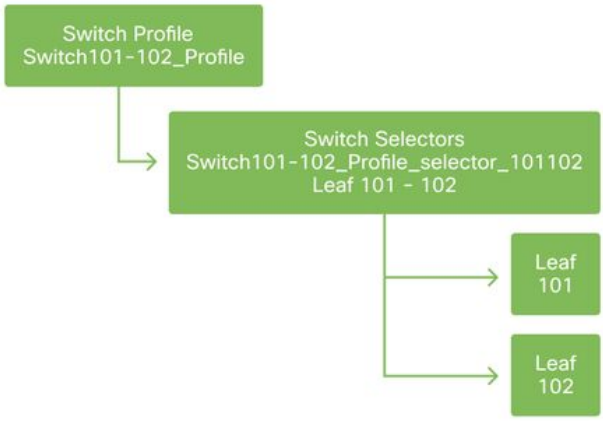



Un serveur Web est connecté à un fabric ACI. Le serveur Web dispose de 2 cartes réseau configurées dans un canal de port LACP. Le serveur Web est connecté au port 1/9 des commutateurs Leaf 101 et 102. Le serveur Web s'appuie sur VLAN-1501 et doit résider dans l'EPG « EPG-Web ».

### Configuration de la politique de commutation

La première étape logique consiste à définir les commutateurs Leaf à utiliser. Le 'Switch Profile' contiendra les 'Switch Selectors' qui définissent les ID de noeud feuille à utiliser.

### Stratégies de commutateur



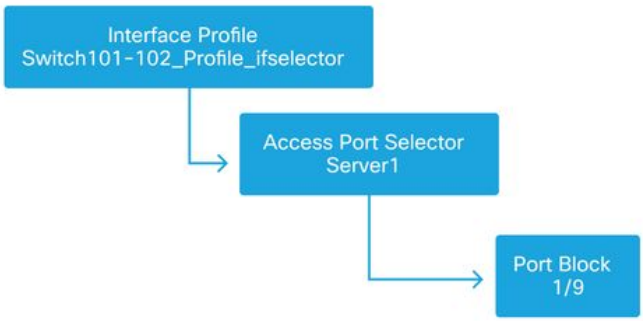

La recommandation générale est de configurer 1 profil de commutateur par commutateur leaf individuel et 1 profil de commutateur par paire de domaines VPC, en utilisant un schéma d'attribution de noms qui indique les noeuds qui font partie du profil.

Le démarrage rapide déploie un système d'attribution de noms logique qui facilite la compréhension de son application. Le nom complet suit le format « Switch<node-id>_Profile ». Par exemple, « Switch101_Profile » sera utilisé pour un profil de commutateur contenant le noeud leaf 101 et Switch101-102_Profile pour un profil de commutateur contenant les noeuds leaf 101 et 102 qui doivent faire partie d'un domaine VPC.

### Configurer la stratégie d'interface

Une fois les politiques d’accès au commutateur créées, la définition des interfaces constitue l’étape logique suivante. Pour ce faire, un « profil d'interface » composé d'au moins un « sélecteur de ports d'accès » contient les définitions de « bloc de ports ».

### Politiques d'interface



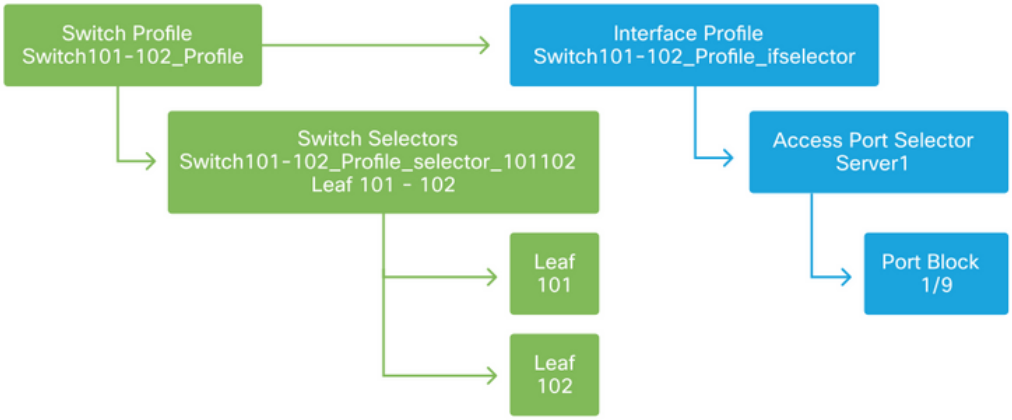

Pour établir la relation entre le « profil d'interface » et les commutateurs concernés, liez le « profil de commutateur » au « profil d'interface ».

Les « profils d'interface » peuvent être définis de plusieurs manières. Comme pour les « profils de commutateur », un seul « profil d'interface » peut être créé par commutateur physique avec un « profil d'interface » par domaine VPC. Ces politiques doivent alors avoir un mappage 1 à 1 vers leur profil de commutateur correspondant. Dans cette logique, les politiques d'accès au fabric sont considérablement simplifiées, ce qui facilite la compréhension des autres utilisateurs.

Les schémas d'attribution de noms par défaut utilisés par le démarrage rapide peuvent également être utilisés ici. Il suit le format '<switch profile name>_ifselector' pour indiquer que ce profil est

utilisé pour sélectionner des interfaces. Par exemple, « Switch101_Profile_ifselector ». Cet exemple « Interface Profile » serait utilisé pour configurer des interfaces non VPC sur le commutateur leaf 101 et il serait associé uniquement à la stratégie d'accès « Switch101_Profile ».

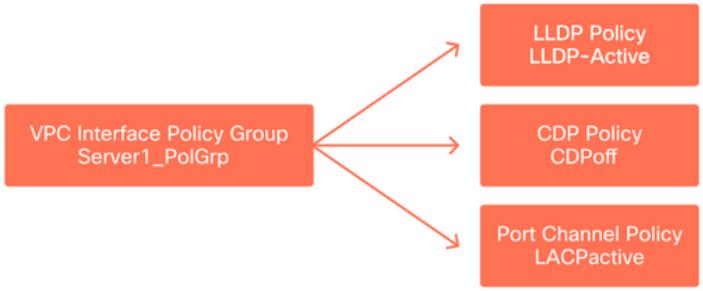
### Profil de commutateur associé au profil d'interface




Notez qu'étant donné qu'un « profil d'interface » avec Eth1/9 est connecté à un « profil de commutateur » qui inclut les deux commutateurs Leaf 101 et 102, l'approvisionnement d'Eth1/9 sur les deux noeuds commence simultanément.

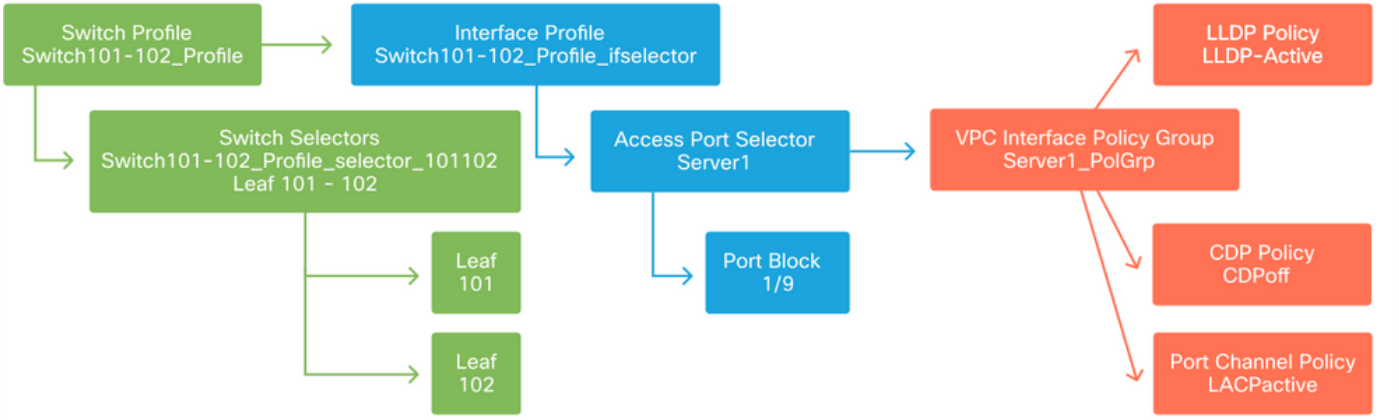
Àce stade, les commutateurs Leaf et leurs ports ont été définis. L'étape logique suivante consiste à définir les caractéristiques de ces ports. Le groupe de politiques d'interface permet de définir ces propriétés de port. Un « groupe de stratégie d'interface VPC » sera créé pour autoriser le Port-Channel LACP ci-dessus.

### groupe de politiques




Le « groupe de stratégie d'interface VPC » est associé au « groupe de stratégie d'interface » à partir du « sélecteur de port d'accès » pour former la relation entre le commutateur/interface leaf et les propriétés de port.

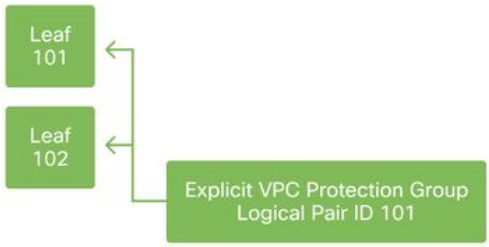
### Profils de commutateur et d'interface combinés




## Configuration du VPC

Pour créer le canal de port LACP sur 2 commutateurs Leaf, un domaine VPC doit être défini entre les commutateurs Leaf 101 et 102. Pour ce faire, définissez un « groupe de protection VPC » entre les deux commutateurs Leaf.

## VPC



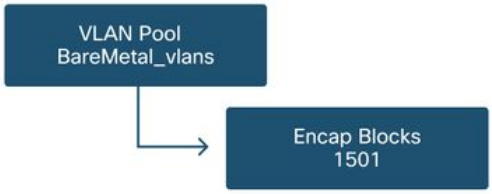

## Configurer les pools VLAN

L'étape logique suivante consiste à créer les VLAN qui seront utilisés sur ce port, dans ce cas VLAN-1501. La définition d'un « pool de VLAN » avec des « blocs d'encapsulation » complète cette configuration.

Lorsque vous examinez la taille des plages de pools de VLAN, gardez à l'esprit que la plupart des déploiements ne nécessitent qu'un seul pool de VLAN et un pool supplémentaire si vous utilisez l'intégration VMM. Pour amener les VLAN d'un réseau existant vers l'ACI, définissez la plage des VLAN existants en tant que pool de VLAN statiques.

Par exemple, supposons que les VLAN 1 à 2000 soient utilisés dans un environnement hérité. Créez un pool de VLAN statiques contenant les VLAN 1 à 2000. Cela permettra d'agréger les domaines de pont ACI et les EPG vers le fabric existant. Lors du déploiement de VMM, un second pool dynamique peut être créé à l'aide d'une plage d'ID de VLAN libres.

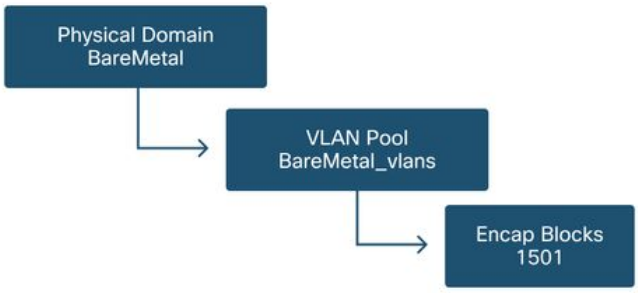
## Pool VLAN




### Configurer les domaines

L'étape logique suivante consiste à créer un « domaine ». Un « domaine » définit l'étendue d'un pool de VLAN, c'est-à-dire l'endroit où ce pool sera appliqué. Un « domaine » peut être physique, virtuel ou externe (ponté ou routé). Dans cet exemple, un « domaine physique » sera utilisé pour connecter un serveur sans système d'exploitation au fabric. Ce « domaine » est associé au « pool de VLAN » pour autoriser les VLAN requis.

### Domaines physiques




Pour la plupart des déploiements, un seul « domaine physique » suffit pour les déploiements sans système d'exploitation et un seul « domaine routé » suffit pour les déploiements L3Out. Les deux peuvent correspondre au même « pool de VLAN ». Si le fabric est déployé de manière multilocataire, ou si un contrôle plus granulaire est nécessaire pour limiter quels utilisateurs peuvent déployer des EPG et des VLAN spécifiques sur un port, une conception de politique d'accès plus stratégique doit être envisagée.

Les 'Domaines' fournissent également la fonctionnalité de restriction de l'accès utilisateur à la stratégie avec 'Domaines de sécurité' à l'aide du contrôle d'accès basé sur les rôles (RBAC).

Lors du déploiement de VLAN sur un commutateur, l'ACI encapsule les BPDU Spanning Tree avec un ID VXLAN unique basé sur le domaine d'origine du VLAN. Pour cette raison, il est important d'utiliser le même domaine chaque fois que vous connectez des périphériques qui nécessitent une communication STP avec d'autres ponts.

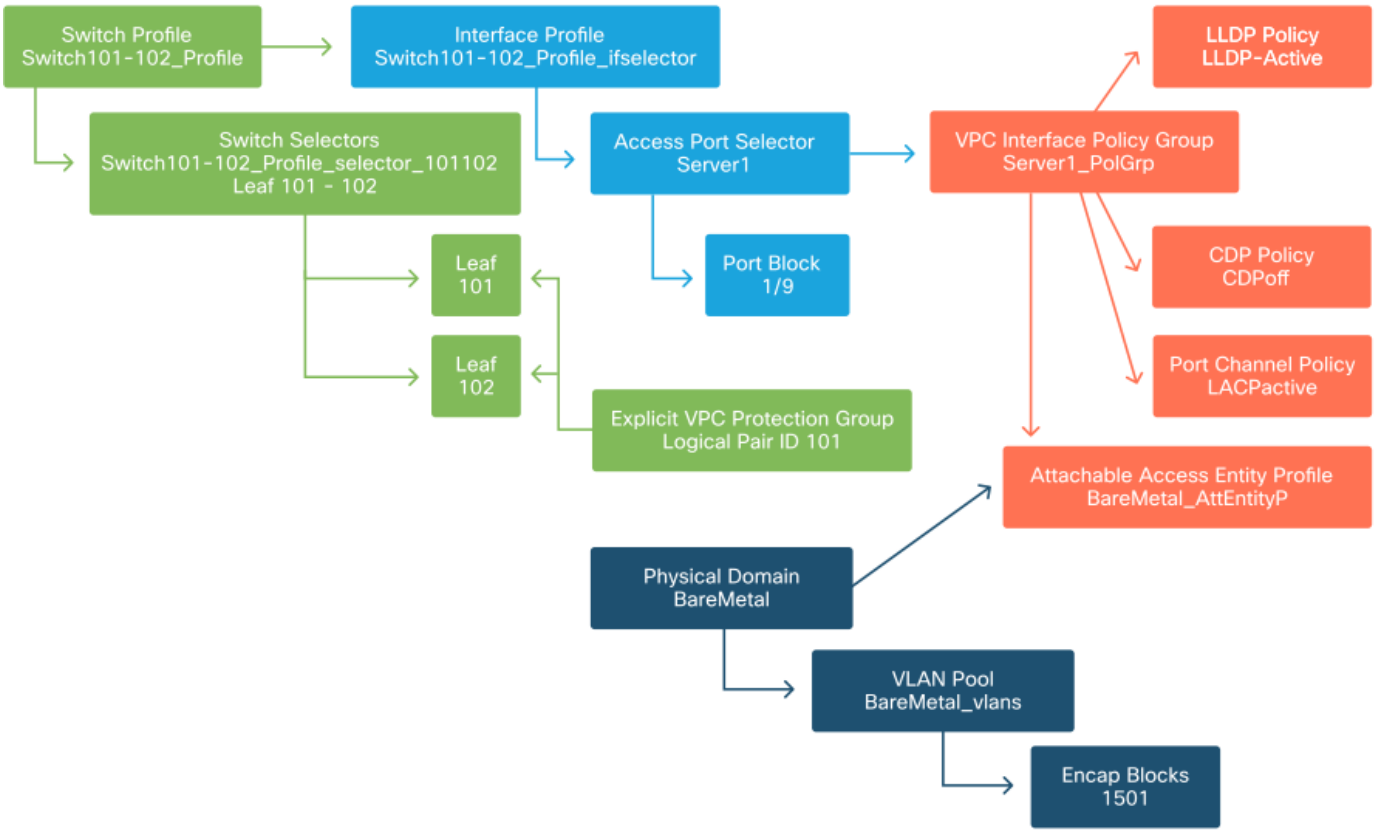
Les ID de VLAN VXLAN sont également utilisés pour permettre aux commutateurs VPC de synchroniser les adresses MAC et IP apprises par VPC. De ce fait, la conception la plus simple pour les pools de VLAN consiste à utiliser un pool unique pour les déploiements statiques et à en créer un second pour les déploiements dynamiques.

### Configurer le profil d'entité d'accès attachable (AEP)

Deux grandes parties de la configuration des politiques d'accès sont maintenant terminées ; les définitions de commutateur et d’interface, ainsi que les définitions de domaine/VLAN. Un objet appelé « Attachable Access Entity Profile » (AEP) servira à lier ces deux segments.

Un « groupe de politiques » est lié à un AEP dans une relation un-à-plusieurs qui permet à l'AEP de regrouper des interfaces et des commutateurs partageant des exigences de politiques similaires. Cela signifie qu'un seul AEP doit être référencé lors de la représentation d'un groupe d'interfaces sur des commutateurs spécifiques.

### Profil d'entité d'accès attachable




Dans la plupart des déploiements, un seul AEP doit être utilisé pour les chemins statiques et un AEP supplémentaire par domaine VMM.

La considération la plus importante est que les VLAN peuvent être déployés sur des interfaces via l'AEP. Pour ce faire, vous pouvez mapper directement des groupes de terminaux sur un AEP ou configurer un domaine VMM pour le pré-provisionnement. Ces deux configurations font de l'interface associée un port agrégé (« switchport mode trunk » sur les commutateurs hérités).

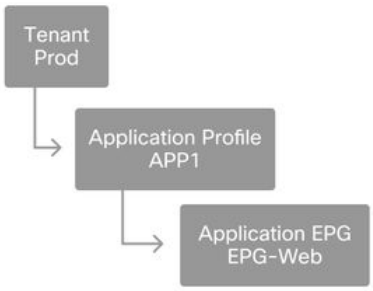
Pour cette raison, il est important de créer un AEP distinct pour L3Out lors de l'utilisation de ports routés ou de sous-interfaces routées. Si des interfaces SVI sont utilisées dans L3Out, il n'est pas nécessaire de créer un AEP supplémentaire.

### Configurer le locataire, l'application et l'EPG

L'ACI utilise un autre moyen de définir la connectivité en utilisant une approche basée sur des politiques.

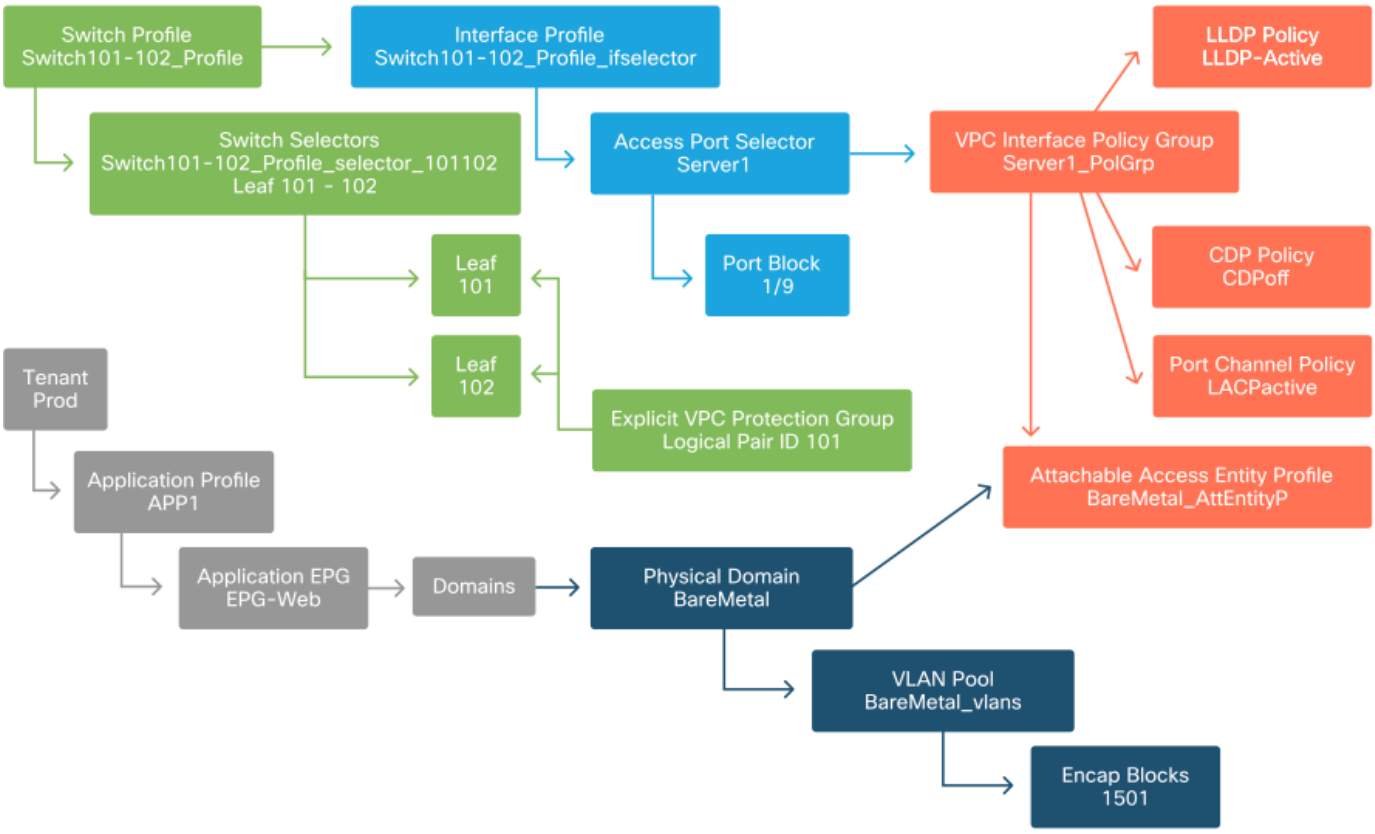
L'objet de plus bas niveau est appelé « groupe de terminaux » (EPG). La conception EPG permet de définir un groupe de machines virtuelles ou de serveurs (terminaux) avec des exigences de stratégie similaires. Les « profils d'application », qui existent sous un locataire, sont utilisés pour regrouper logiquement les groupes de terminaux.

### Locataire, APP et EPG




L'étape logique suivante consiste à relier le groupe de terminaux au domaine. Ceci crée le lien entre l'objet logique représentant notre charge de travail, l'EPG, et les commutateurs/interfaces physiques, les politiques d'accès.

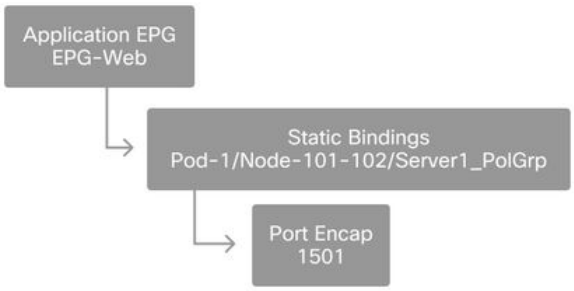
### Liaison EPG vers domaine




### Configuration des liaisons statiques EPG

La dernière étape logique consiste à programmer le VLAN sur une interface de commutateur pour un EPG donné. Ceci est particulièrement important si vous utilisez un domaine physique, car ce type de domaine nécessite une déclaration explicite pour le faire. Cela permettra à l'EPG d'être étendu hors du fabric et au serveur sans système d'exploitation d'être classé dans l'EPG.

### Liaisons statiques

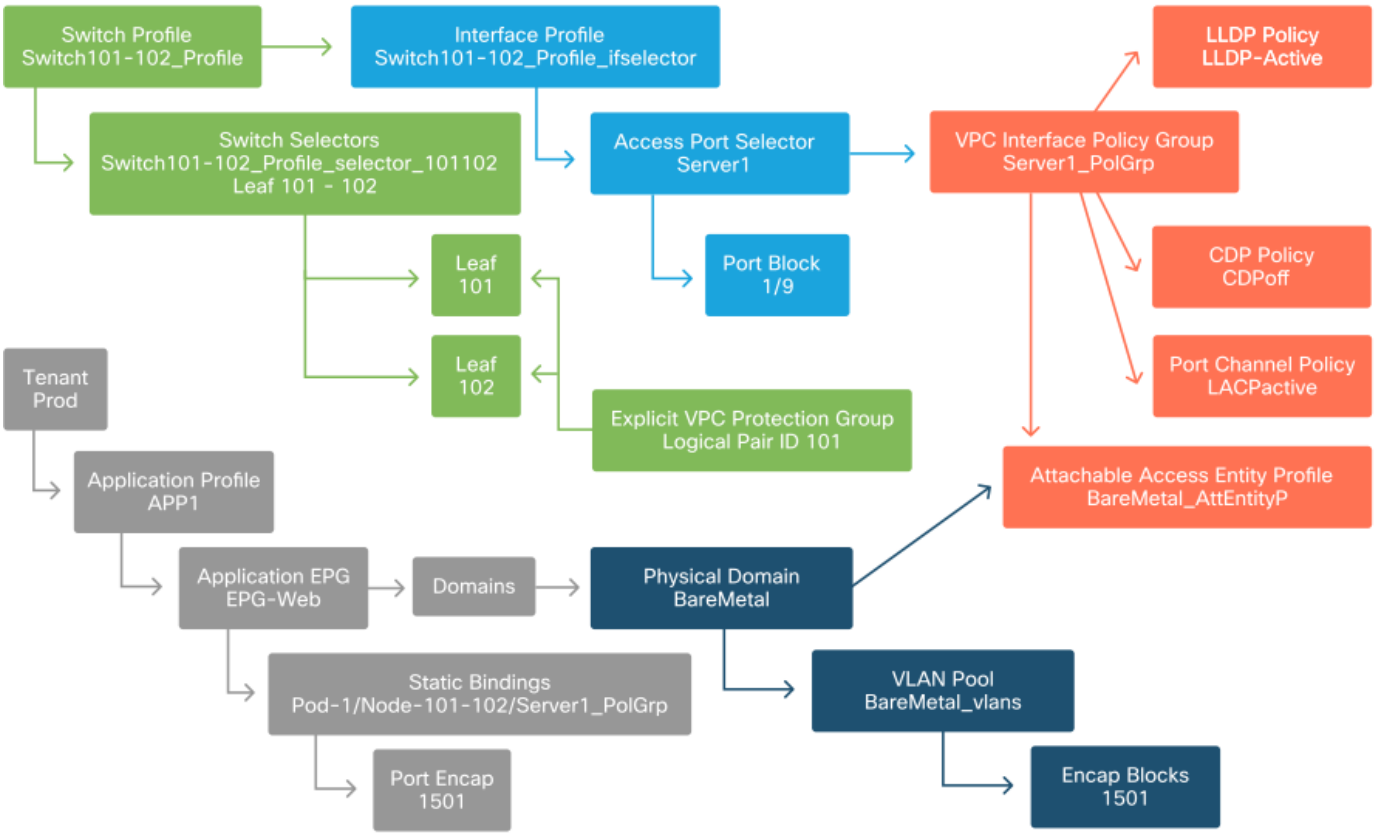



Le « Port Encap » référencé doit pouvoir être résolu par rapport au « VLAN Pool ». Si ce n'est pas le cas, un défaut sera signalé. Ceci est traité dans la section « Dépannage du workflow » de ce chapitre.

### Résumé de la configuration de la stratégie d'accès

Le schéma suivant résume tous les objets créés pour permettre la connectivité de l'hôte via VLAN-1501, en utilisant une connexion VPC aux commutateurs Leaf 101 et 102.

### Connectivité ACI sans système d'exploitation




### Connexion de serveurs supplémentaires

Avec toutes les stratégies précédentes créées, que signifie connecter un serveur supplémentaire sur le port Eth1/10 sur les commutateurs Leaf 101 et 102 avec un port-channel ?

En vous reportant au schéma de connectivité ACI sans système d'exploitation, vous devez créer au minimum les éléments suivants :

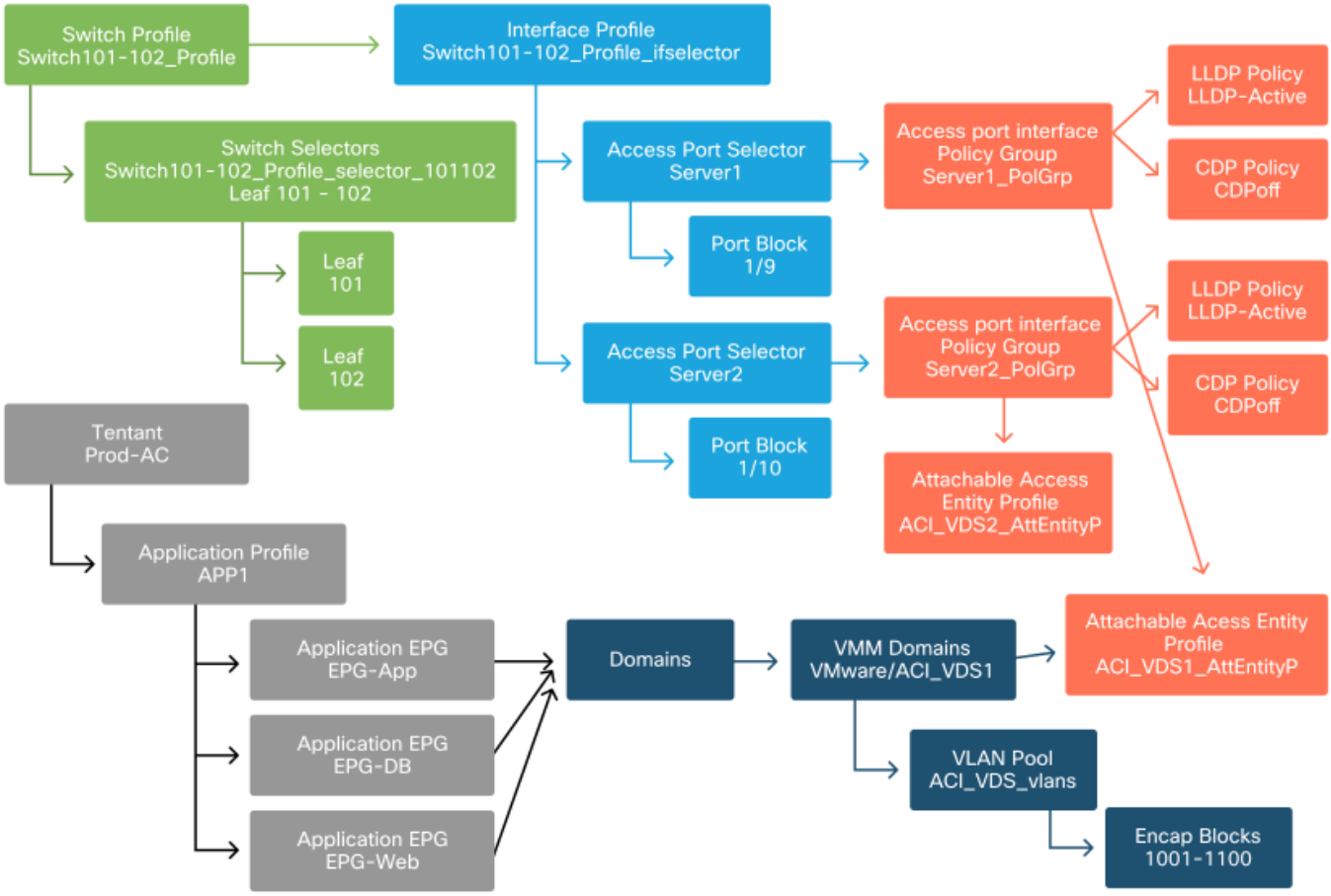
- Un sélecteur de port d'accès et un bloc de ports supplémentaires.
- Un groupe de stratégie d'interface VPC supplémentaire.
- Une liaison statique supplémentaire avec encapsulation de port.

Notez que pour les canaux de port LACP, un groupe de stratégie d'interface VPC dédié doit être utilisé car ce groupe de stratégie VPC est ce qui définit l'ID VPC.

Dans le cas de liaisons individuelles, le groupe de stratégie d'interface non-VPC peut être réutilisé pour le serveur supplémentaire si la liaison nécessite les mêmes propriétés de port.

Les politiques qui en résulteraient ressembleraient à l'image suivante.

### Connexion de server2 à la configuration




### Opérations suivantes

La section suivante présente quelques scénarios d'échec de la politique d'accès, en commençant par la topologie et l'exemple d'utilisation abordés dans cette présentation.

## Workflow de dépannage

Les scénarios de dépannage suivants peuvent être rencontrés lors de l'utilisation de stratégies d'accès :

- Relation manquante entre deux ou plusieurs entités de la stratégie d'accès, comme un groupe de stratégies d'accès non lié à un AEP.

- Une stratégie manquante ou inattendue est liée à une stratégie d'accès donnée, telle qu'une stratégie LLDP nommée « lldp_enabled », alors qu'en réalité la configuration de la stratégie a LLDP rx/tx désactivé.
- Une valeur manquante ou inattendue dans la stratégie d'accès, telle que l'encapsulation d'ID de VLAN configurée manquante dans le pool de VLAN configuré.
- Une relation manquante entre l'EPG et la politique d'accès, telle qu'aucune association de domaine physique ou virtuel à l'EPG.

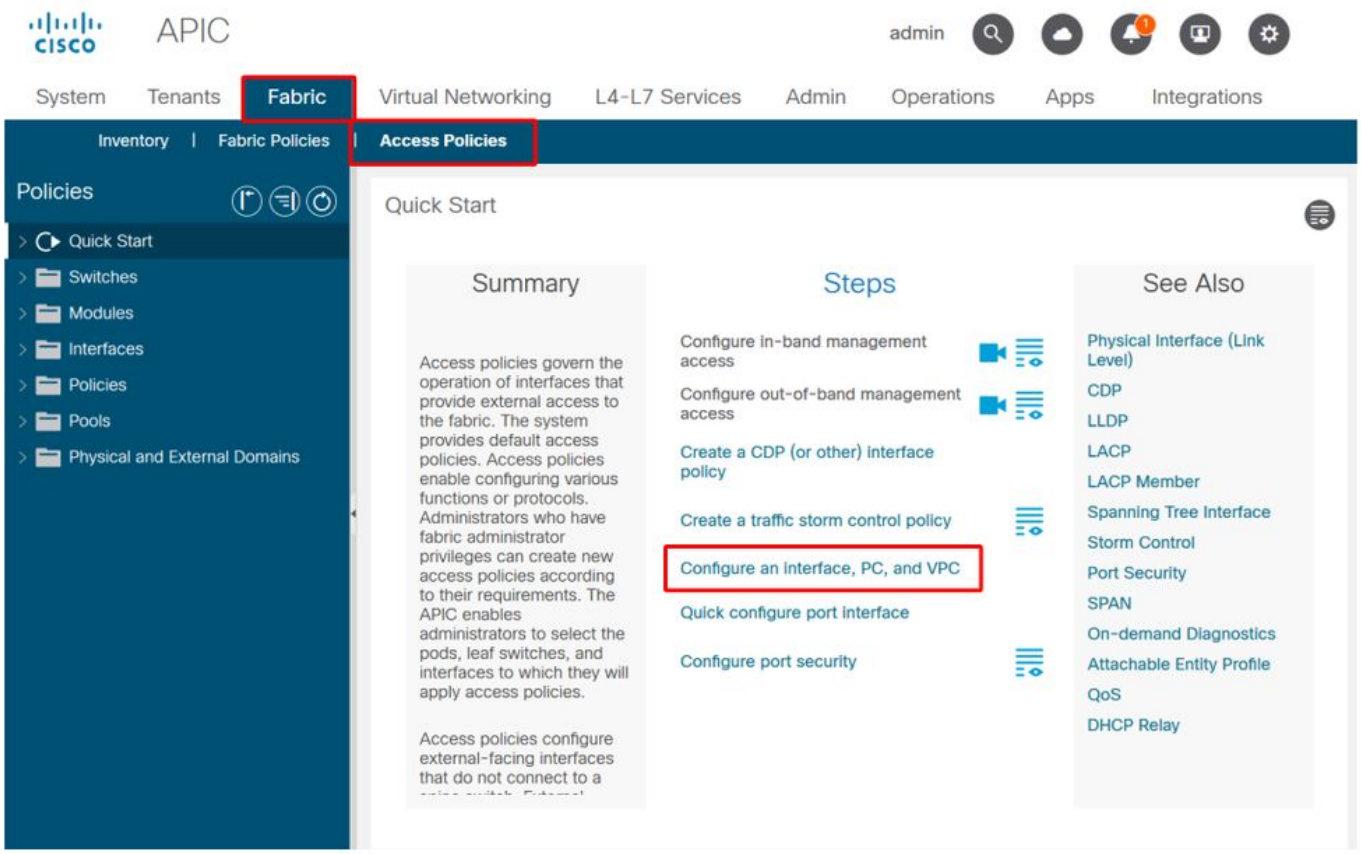
La plupart des opérations de dépannage ci-dessus consistent à parcourir les relations de stratégie d'accès pour déterminer si des relations sont manquantes, ou pour identifier les stratégies configurées et/ou si la configuration entraîne le comportement souhaité.

## Utilisation de la section « Configuration de l'interface, du PC et du démarrage rapide du VPC » pour le dépannage

Dans l'interface graphique du contrôleur APIC, l'assistant de démarrage rapide « Configurer l'interface, le PC et le VPC » facilite la recherche des politiques d'accès en fournissant à l'administrateur une vue agrégée des politiques d'accès existantes. Cet assistant de démarrage rapide se trouve dans l'interface utilisateur graphique à l'adresse :

'Fabric > Access Policies > Quick Start > Steps > Configure Interface, PC, and VPC'.

**Emplacement du démarrage rapide « Configurer l'interface, le PC et le VPC »**

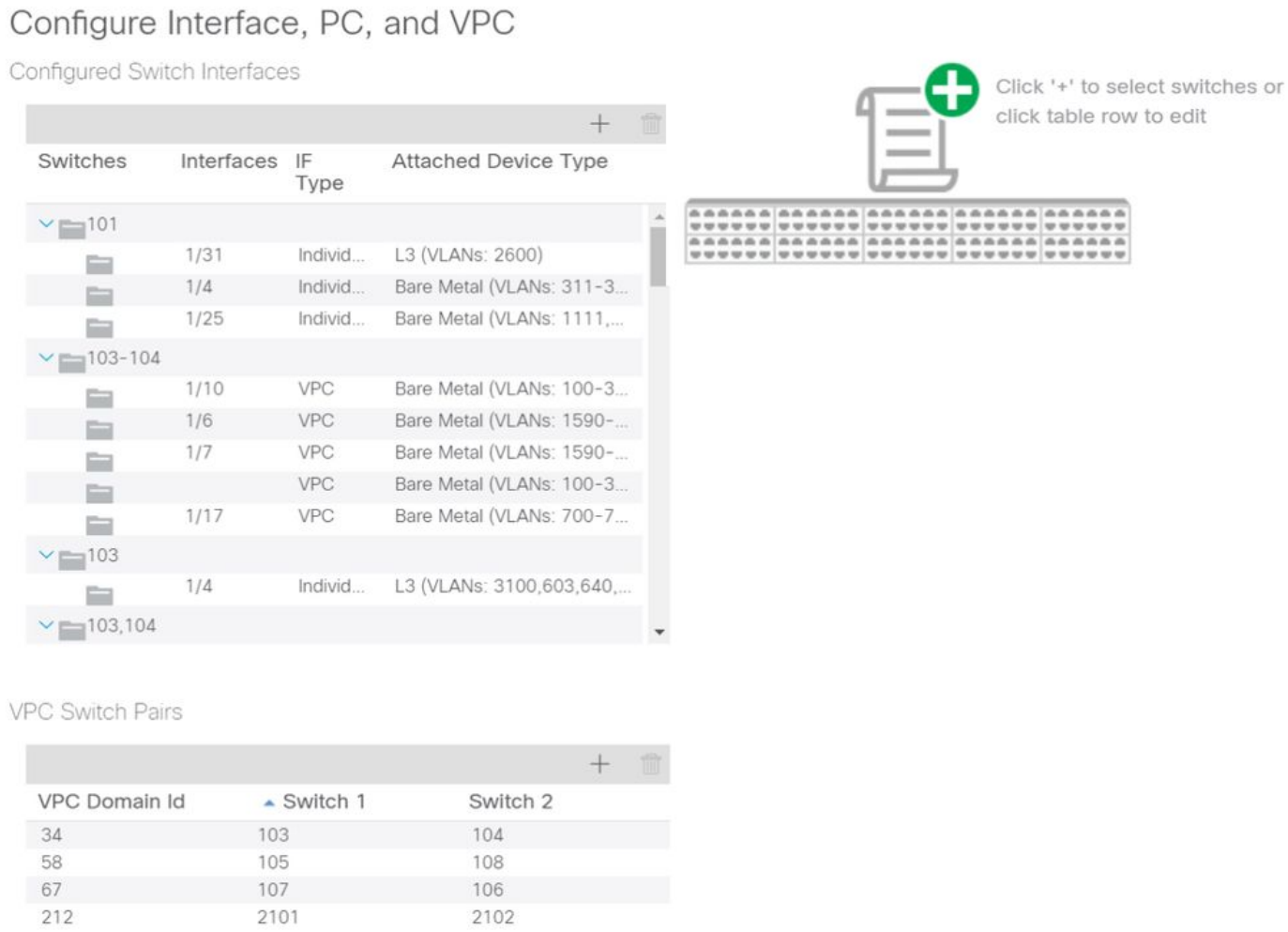



Bien que le nom de l'assistant contienne « Configure », il est particulièrement pratique pour fournir une vue agrégée des nombreuses stratégies d'accès qui doivent être configurées pour que les interfaces soient programmées. Cette agrégation sert de vue unique pour comprendre quelles politiques sont déjà définies et réduit efficacement le nombre de clics requis pour commencer à isoler les problèmes liés aux politiques d'accès.

Lorsque la vue Démarrage rapide est chargée, la vue « Interfaces de commutateur configurées » (volet supérieur gauche) peut être référencée pour déterminer les stratégies d'accès existantes. L'Assistant regroupe les entrées sous les dossiers qui représentent des commutateurs Leaf individuels ou multiples, selon la configuration des stratégies d'accès.

Comme démonstration de la valeur de l'assistant, les captures d'écran suivantes sont présentées, sachant que le lecteur n'a aucune connaissance préalable de la topologie du fabric :

**Vue de démonstration du démarrage rapide « Configurer l'interface, le PC et le VPC »**




Le volet « Interfaces de commutateur configurées » affiche les mappages de stratégie d'accès. Le volet « Paires de commutateurs VPC » affiche les définitions de groupe de protection VPC terminées.

Le tableau ci-dessous présente un sous-ensemble de définitions de politique d'accès qui peuvent être déduites de la capture d'écran ci-dessus.

**Sous-ensemble de politiques d'accès terminées pouvant être dérivées de la vue Démarrage rapide ci-dessus**

| Noeud de commutateur | Interface | Type de groupe de stratégies | Type de domaine | Réseaux locaux virtuels (VLAN) |
|---|---|---|---|---|
| 101 | 1/31 | Individu | Routé (L3) | 2600 |

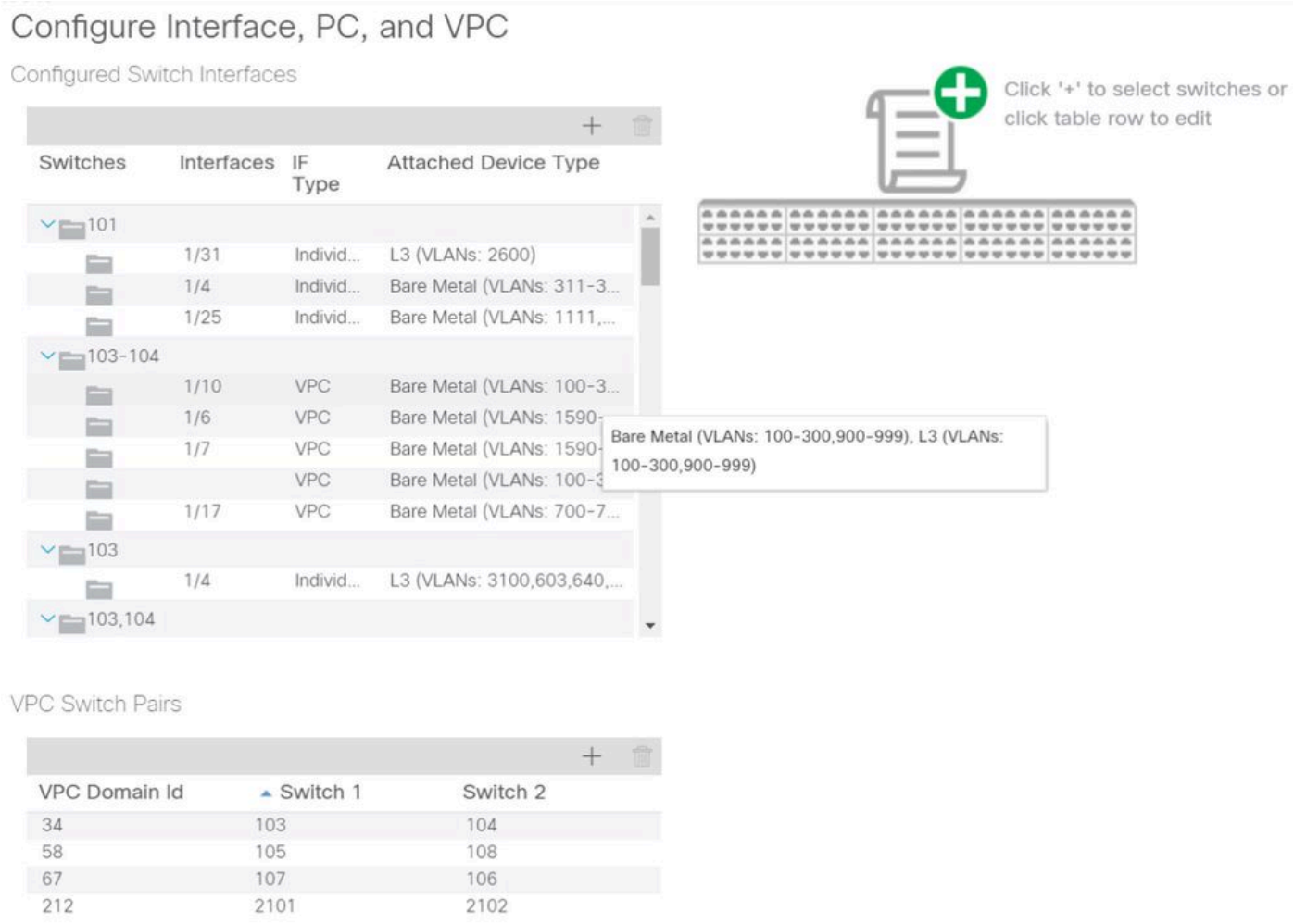
| | | | | |
|---|---|---|---|---|
| 101 | 1/4 | Individu | Phys (sans système d'exploitation) | 311-3.. ? |
| 103-104 | 1/10 | VPC | Phys (sans système d'exploitation) | 100-3.. ? |

Les entrées de la colonne VLAN sont intentionnellement incomplètes, compte tenu de la vue par défaut.

De même, les stratégies « Groupe de protection VPC » terminées peuvent être dérivées de la vue « Paires de commutateurs VPC » (volet inférieur gauche). Sans « groupes de protection VPC », les VPC ne peuvent pas être déployés car il s'agit de la stratégie qui définit le domaine VPC entre deux noeuds leaf.

Tenez compte du fait qu'en raison du dimensionnement du volet, les entrées longues ne sont pas complètement visibles. Pour afficher la valeur complète d'une entrée, placez le pointeur de la souris sur le champ concerné.

**Le pointeur de la souris survole le champ « Attached Device Type » pour l'entrée 103-104, int 1/10 VPC :**




En faisant passer la souris sur le volet, les entrées complètes sont visibles.

**Sous-ensemble mis à jour des politiques d'accès à l'aide de la souris**

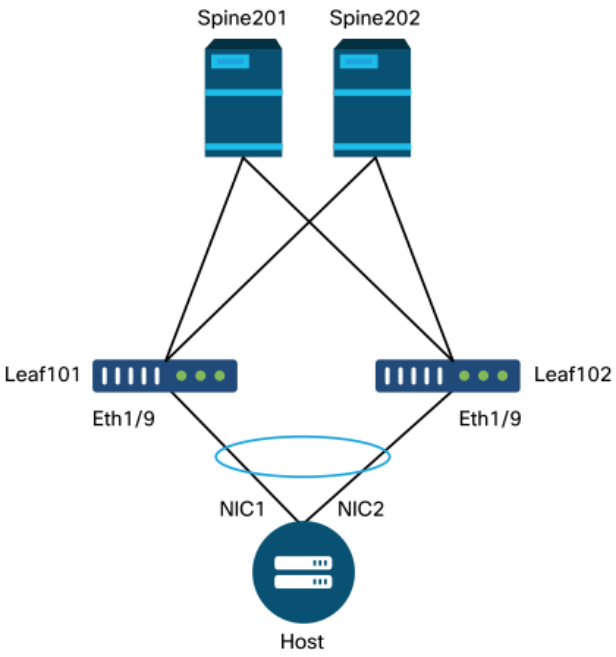
| Noeud de commutateur | Interface | Type de groupe de stratégies | Type de domaine | Réseaux locaux virtuels (VLAN) |
|---|---|---|---|---|
| 101 | 1/31 | Individu | Routé (L3) | 2600 |
| 101 | 1/4 | Individu | Phys (sans système d'exploitation) | 311-320 |
| 103-104 | 1/10 | VPC | Phys (sans système d'exploitation) | 100-300,900-999 |
| 103-104 | 1/10 | VPC | Routé (L3) | 100-300,900-999 |

Les associations VLAN complètes peuvent désormais être observées et comprises à des fins de dépannage et de vérification.

# Scénarios de dépannage

Pour les scénarios de dépannage suivants, reportez-vous à la même topologie du chapitre précédent.

**Topologie de la section « Introduction » de la stratégie d'accès**




## Scénario 1 : Fault F0467 — invalid-path, nouveaux problèmes

Cette erreur est déclenchée lorsqu'une déclaration de commutateur/port/VLAN est effectuée sans les politiques d'accès correspondantes en place pour permettre l'application correcte de cette configuration. Selon la description de cette erreur, un élément différent de la relation de stratégie d'accès peut être manquant.

Après le déploiement d'une liaison statique pour l'interface VPC ci-dessus avec le VLAN 1501

d'encapsulation agrégé sans la relation de stratégie d'accès correspondante en place, la défaillance suivante est soulevée sur l'EPG :

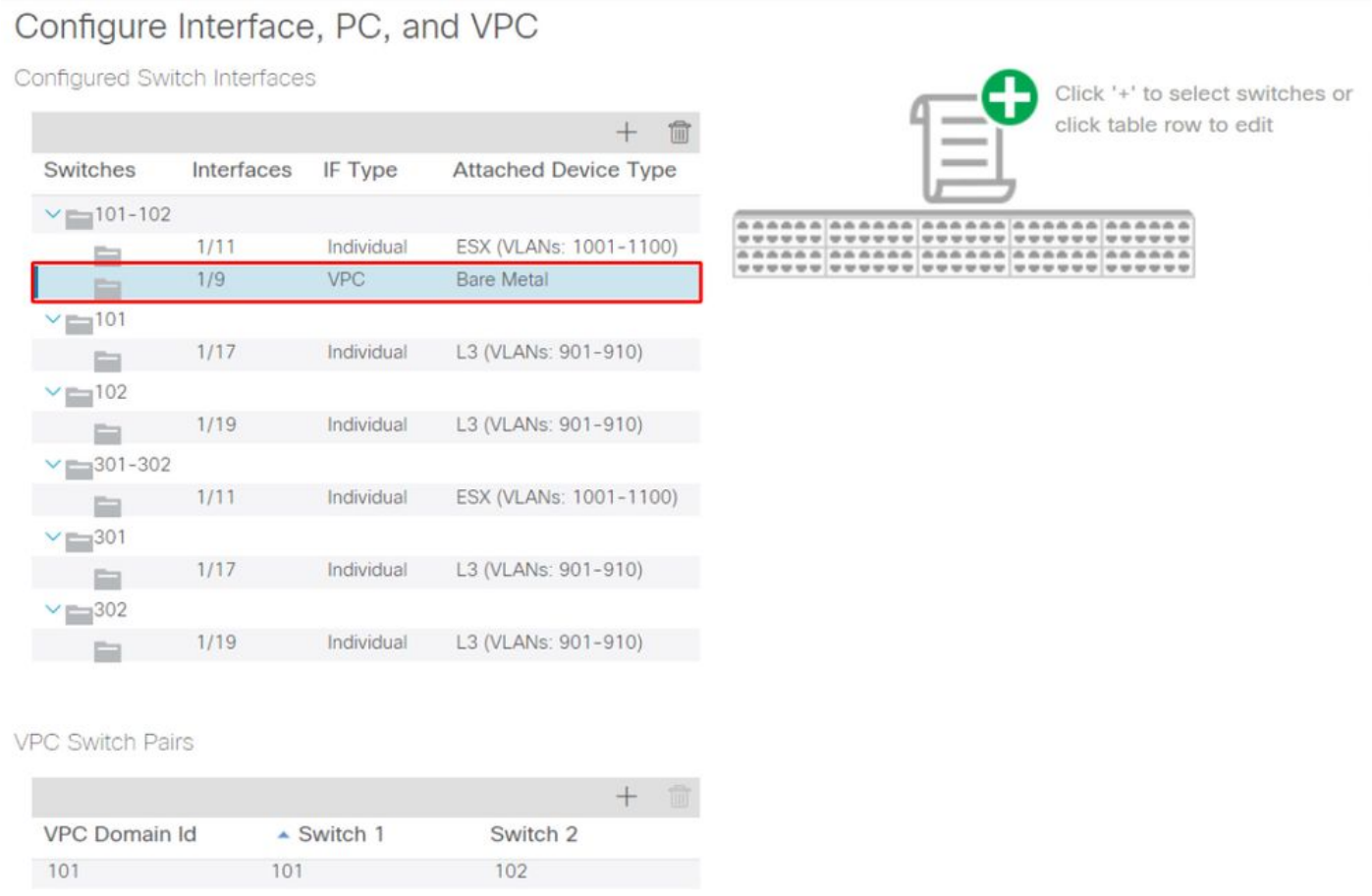
**Défaillance :** F0467

**Description :** Délégué par défaut : Échec de la configuration du noeud uni/tn-Prod1/ap-App1/epg-EPG-Web 101 101_102_eth1_9 en raison d'une configuration de chemin non valide, d'une configuration de VLAN non valide, d'un message de débogage : invalid-vlan : vlan-1501 : ID de segment STP absent pour Encap. Soit l'EPG n'est pas associé à un domaine, soit ce VLAN n'est pas attribué au domaine ; chemin-non-valide : vlan-1501 : aucun domaine, associé à la fois à l'EPG et au port, n'a besoin de VLAN ;

La description de la panne ci-dessus fournit des indications claires sur ce qui pourrait provoquer le déclenchement de la panne. Un avertissement s'affiche pour vérifier les relations de stratégie d'accès, ainsi que l'association du domaine à l'EPG.

En examinant la vue Démarrage rapide dans le scénario décrit ci-dessus, il apparaît clairement que la politique d'accès ne dispose pas de VLAN.

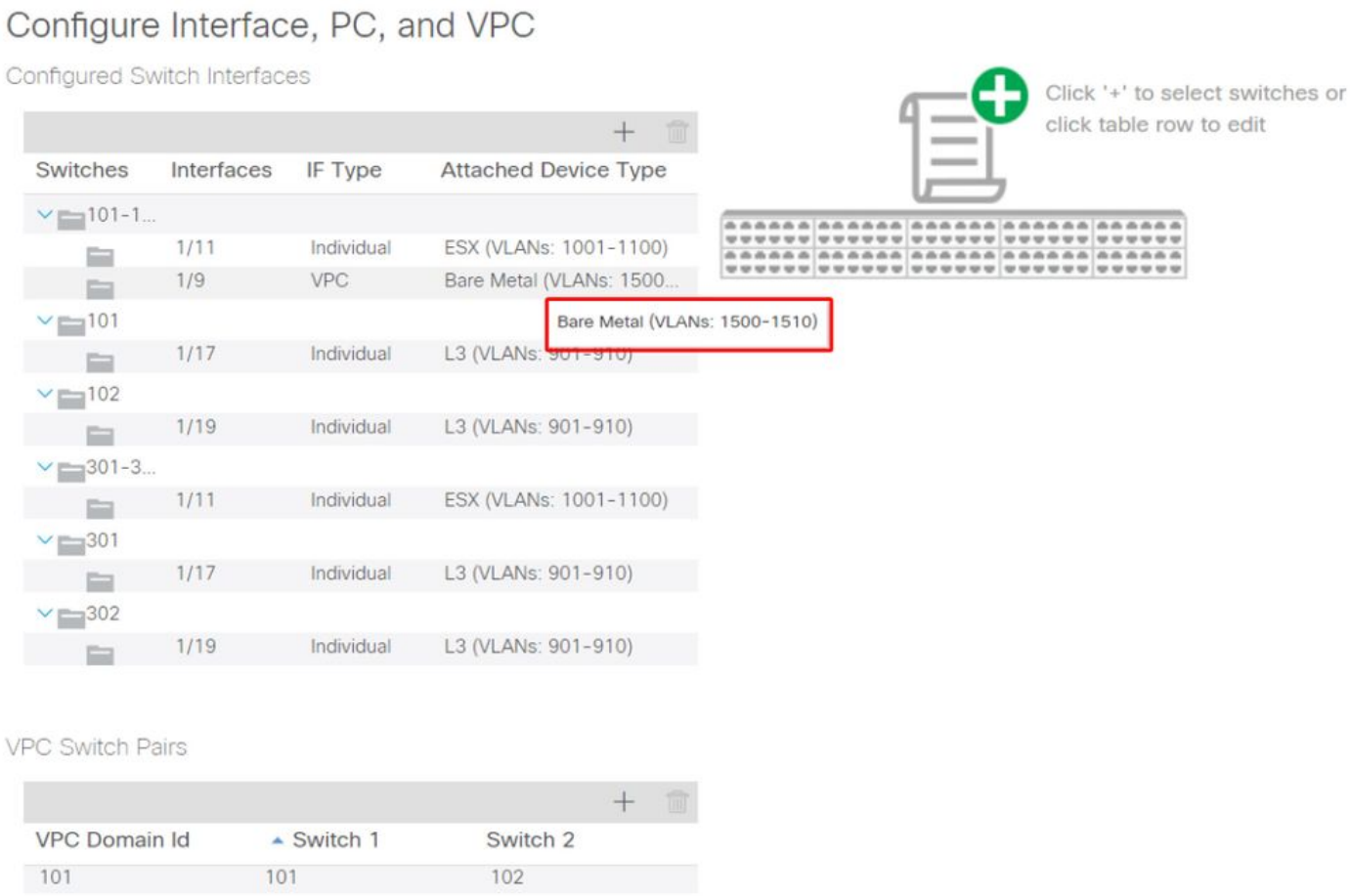
**Vue de démarrage rapide où 101-102, Int 1/9 VPC manque de VLAN**




Notez qu'il manque une référence aux ID de VLAN dans l'entrée.

Une fois la correction effectuée, la vue Démarrage rapide affiche « (VLAN 1500-1510) ».

**101-102, Int 1/9 VPC affiche désormais les VLAN sans système d'exploitation (Bare Metal) : 1500-1510)**



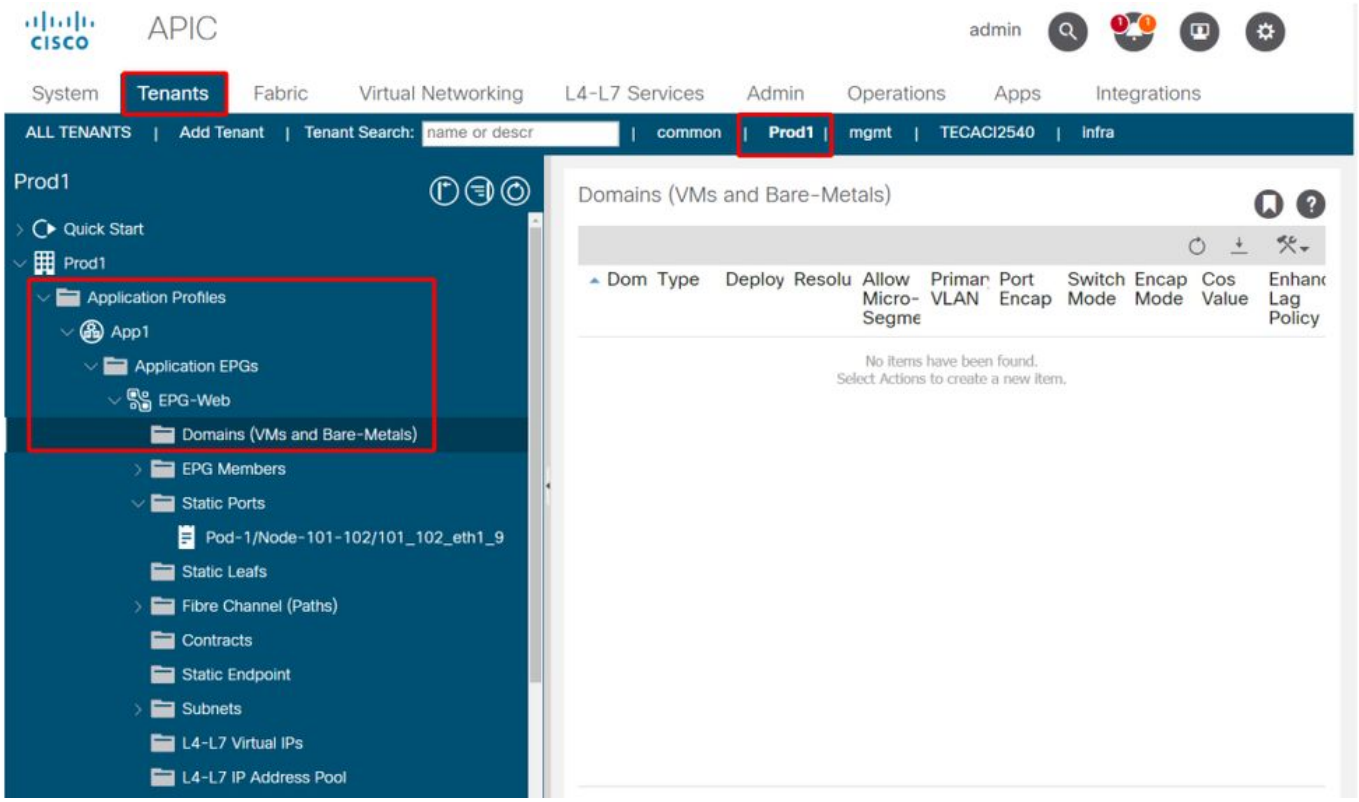

Cependant, la panne EPG existe toujours avec la description mise à jour suivante pour la panne F0467 :

**Erreur :** F0467

**Description :** Délégué par défaut : Échec de la configuration du noeud uni/tn-Prod1/ap-App1/epg-EPG-Web 101 101_102_eth1_9 en raison d'une configuration de chemin non valide. Message de débogage : invalid-path : vlan-150 : Aucun domaine, associé à la fois à l'EPG et au port, n'a besoin de VLAN.

Une fois l'erreur mise à jour ci-dessus, vérifiez les associations de domaines EPG pour vous assurer qu'aucun domaine n'est lié à l'EPG.

**EPG-Web a une association de ports statiques, mais il manque des associations de domaines**




Une fois que le domaine qui contient VLAN 1501 est associé à l'EPG, aucune autre erreur n'est générée.

## Scénario 2 : Impossible de sélectionner VPC comme chemin à déployer sur le port statique EPG ou le profil d'interface logique L3Out (SVI)

Lors de la configuration d'un VPC comme chemin sur un port statique EPG ou une entrée SVI de profil d'interface logique L3Out, le VPC spécifique à déployer n'est pas affiché comme option disponible.

Lors d'une tentative de déploiement d'une liaison statique VPC, deux conditions sont requises :

1. Le groupe de protection explicite VPC doit être défini pour la paire de commutateurs Leaf en question.
2. Le mappage de stratégie d'accès complet doit être défini.

Les deux conditions peuvent être vérifiées à partir de l'affichage Démarrage rapide comme indiqué ci-dessus. Si aucun des deux n'est terminé, le VPC n'apparaît tout simplement pas comme une option disponible pour les liaisons de ports statiques.

## Scénario 3 : Fault F0467 — encapsulation de fabric déjà utilisée dans un autre EPG

Par défaut, les VLAN ont une étendue globale. Cela signifie qu'un ID de VLAN donné ne peut être utilisé que pour un seul EPG sur un commutateur leaf donné. Toute tentative de réutilisation du même VLAN sur plusieurs EPG au sein d'un commutateur leaf donné entraînera l'erreur suivante :

**Défaillance :** F0467

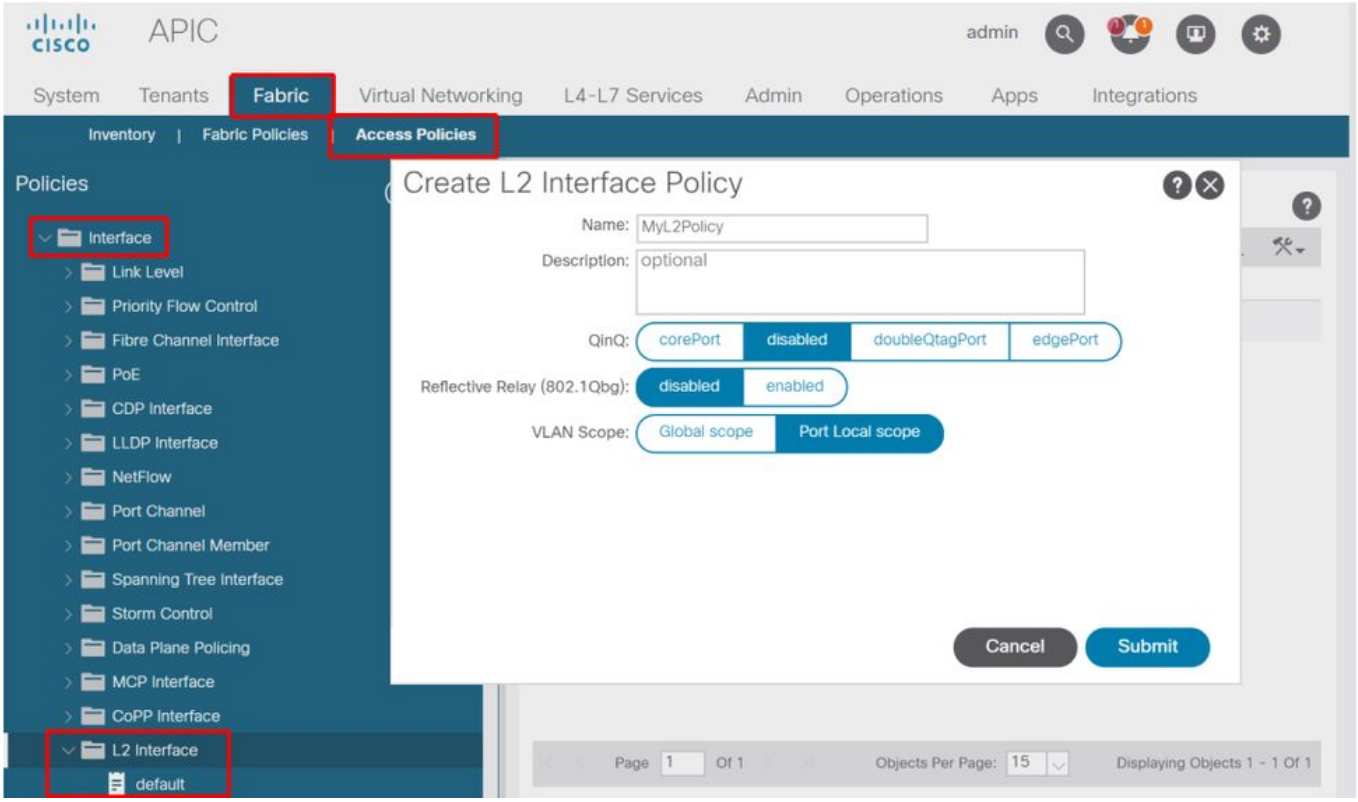
**Description :** Délégué par défaut : Échec de la configuration du noeud uni/tn-Prod1/ap-App1/epg-EPG-BusinessApp 102 101_102_eth1_8 en raison de l'encapsulation déjà utilisée dans un autre EPG, message de débogage : encap-déjà-utilisé : Encap est déjà utilisé par Prod1:App1:EPG-

Web;

Outre la sélection d'un autre VLAN, une autre option pour que cette configuration fonctionne est d'envisager l'utilisation de l'étendue VLAN « Port Local ». Cette portée permet aux VLAN d'être mappés sur une base par interface, ce qui signifie que VLAN-1501 pourrait potentiellement être utilisé pour différents EPG, sur plusieurs interfaces, sur le même leaf.

Bien que la portée « Port Local » soit associée sur une base de groupe de stratégies (en particulier via une stratégie L2), elle est appliquée au niveau leaf.

**Emplacement permettant de modifier le paramètre « VLAN Scope » dans l'interface utilisateur graphique APIC**




Avant d'implémenter la configuration de l'étendue VLAN « Port Local », consultez le « Guide de configuration réseau de couche 2 Cisco APIC » sur Cisco.com pour vous assurer que ses limitations et restrictions de conception sont acceptables pour les cas d'utilisation et les conceptions souhaités.

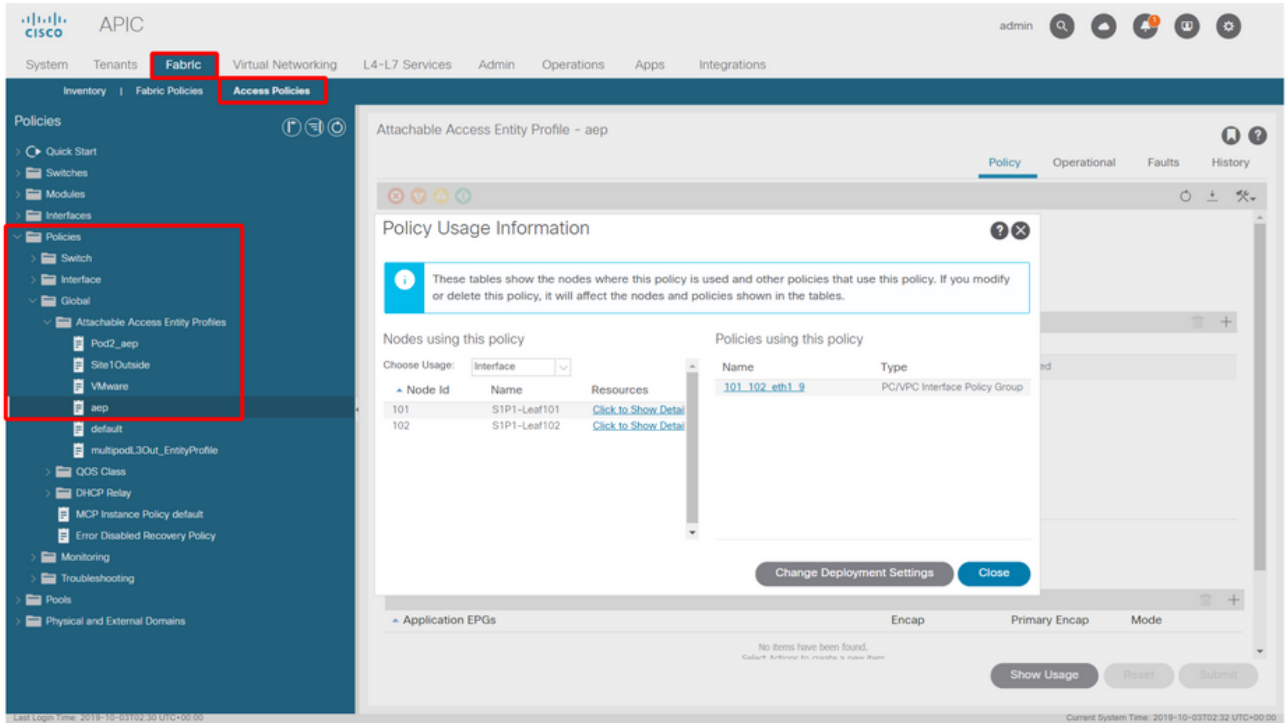
## Mentions spéciales

### Afficher l'utilisation

Bien qu'il ne soit pas spécifique aux stratégies d'accès, un bouton est disponible sur la plupart des objets de l'interface graphique utilisateur, intitulé « Afficher l'utilisation ». Ce bouton effectue une recherche de stratégie basée sur l'objet sélectionné pour déterminer quels noeuds/interfaces leaf ont une relation directe avec lui. Cela peut s'avérer utile pour le scénario de recherche général et pour déterminer si un objet ou une stratégie spécifique est en cours d'utilisation.

Dans la capture d'écran ci-dessous, l'AEP sélectionné est utilisé par deux interfaces différentes. Cela implique que la modification du protocole AEP aura un impact direct sur les interfaces

associées.




## Pools VLAN chevauchants

Bien que la fonction des politiques d'accès soit de permettre le déploiement d'un VLAN spécifique sur une interface, il faut tenir compte d'une utilisation supplémentaire au cours de la phase de conception. Plus précisément, le domaine est utilisé dans le calcul de l'ID VXLAN (appelé encapsulation de fabric) lié à l'encapsulation externe. Bien que cette fonctionnalité n'ait généralement aucune incidence majeure sur le trafic du plan de données, ces ID sont particulièrement pertinents pour un sous-ensemble de protocoles qui inondent le fabric, y compris les unités BPDU Spanning Tree. Si les BPDU VLAN-<id> entrant sur leaf1 sont censées sortir de leaf2 (par exemple, si les commutateurs existants convergent vers le Spanning Tree via l'ACI), VLAN-<id> doit avoir le même encapsulage de fabric sur les deux noeuds leaf. Si la valeur d'encapsulation de fabric diffère pour les mêmes VLAN d'accès, les unités BPDU ne traversent pas le fabric.

Comme mentionné dans la section précédente, évitez de configurer les mêmes VLAN dans plusieurs domaines (VMM vs Physical, par exemple) à moins que des précautions particulières ne soient prises pour s'assurer que chaque domaine n'est jamais appliqué qu'à un ensemble unique de commutateurs Leaf. À partir du moment où les deux domaines peuvent être résolus sur le même commutateur leaf pour un VLAN donné, il y a une chance que le VXLAN sous-jacent puisse être modifié après une mise à niveau (ou un rechargement propre) qui peut conduire par exemple à des problèmes de convergence STP. Le comportement résulte du fait que chaque domaine possède une valeur numérique unique (l'attribut « base ») qui est utilisée dans l'équation suivante pour déterminer l'ID VXLAN :

**VNID VXLAN = Base + (encap — from_encap)**

Pour valider les domaines qui sont poussés sur un leaf donné, une moquery peut être exécutée sur la 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
```

Àpartir de ce résultat, identifiez les définitions de stratégie d'accès suivantes :

- Il existe un pool de VLAN programmé avec un bloc de VLAN définissant explicitement les VLAN 1500-1510.
- Ce bloc de VLAN est lié à un domaine nommé « physvlan ».
- La valeur de base utilisée dans le calcul VXLAN est 8492.
- Le calcul VXLAN résultant pour VLAN-1501 serait 8492 + (1501-1500) = 8493 comme encapsulation de fabric.

L'ID VXLAN résultant (dans cet exemple, 8493) peut être vérifié à l'aide de la commande suivante :

```
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
```

S'il y a un autre pool de VLAN contenant VLAN-1501 qui est poussé sur le même noeud leaf, une mise à niveau ou un rechargement propre pourrait potentiellement saisir une valeur de base unique (et par la suite une encapsulation de fabric différente), ce qui provoquera l'arrêt des BPDU vers un autre noeud leaf qui est censé recevoir des BPDU sur VLAN-1501.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.