Fehlerbehebung bei ACI-Zugriffsrichtlinien

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Verständnis der ACI-Zugriffsrichtlinien und zur Fehlerbehebung beschrieben.

Hintergrundinformationen

Das Material aus diesem Dokument wurde aus dem Buch Troubleshooting Cisco Application Centric Infrastructure, Second Edition, extrahiert. Dies betrifft insbesondere die Kapitel **Zugriffsrichtlinien - Überblick** und **Zugriffsrichtlinien - Fehlerbehebung für Workflows**.

Übersicht über Zugriffsrichtlinien

Wie konfiguriert der ACI-Administrator ein VLAN auf einem Port in der Fabric? Wie kann der ACI-Administrator mit Fehlern in Bezug auf Zugriffsrichtlinien umgehen? In diesem Abschnitt wird erläutert, wie Sie Probleme mit den Fabric-Zugriffsrichtlinien beheben.

Bevor Sie sich mit den Problembehebungsszenarien befassen, müssen Sie sicherstellen, dass der Leser die Funktionsweise der Zugriffsrichtlinien und ihre Beziehungen innerhalb des ACI-Objektmodells versteht. Zu diesem Zweck kann der Leser auf die Dokumente "ACI Policy Model" (ACI-Richtlinienmodell) und "APIC Management Information Model Reference" (APIC-Management-Informationsmodell-Referenz) zugreifen, die unter Cisco.com verfügbar sind (https://developer.cisco.com/site/apic-mim-ref-api/).

Zugriffsrichtlinien dienen dazu, eine bestimmte Konfiguration auf den Downlink-Ports eines Leaf-Switches zu aktivieren. Bevor die Tenant-Richtlinie definiert wird, um Datenverkehr über einen ACI-Fabric-Port zuzulassen, müssen die entsprechenden Zugriffsrichtlinien festgelegt werden.

In der Regel werden Zugriffsrichtlinien definiert, wenn neue Leaf-Switches zur Fabric hinzugefügt werden oder ein Gerät mit ACI-Leaf-Downlinks verbunden wird. Je nachdem, wie dynamisch eine Umgebung ist, können die Zugriffsrichtlinien jedoch im normalen Betrieb der Fabric geändert werden. So können Sie beispielsweise einen neuen Satz von VLANs zulassen oder Fabric-Access-Ports eine neue geroutete Domäne hinzufügen.

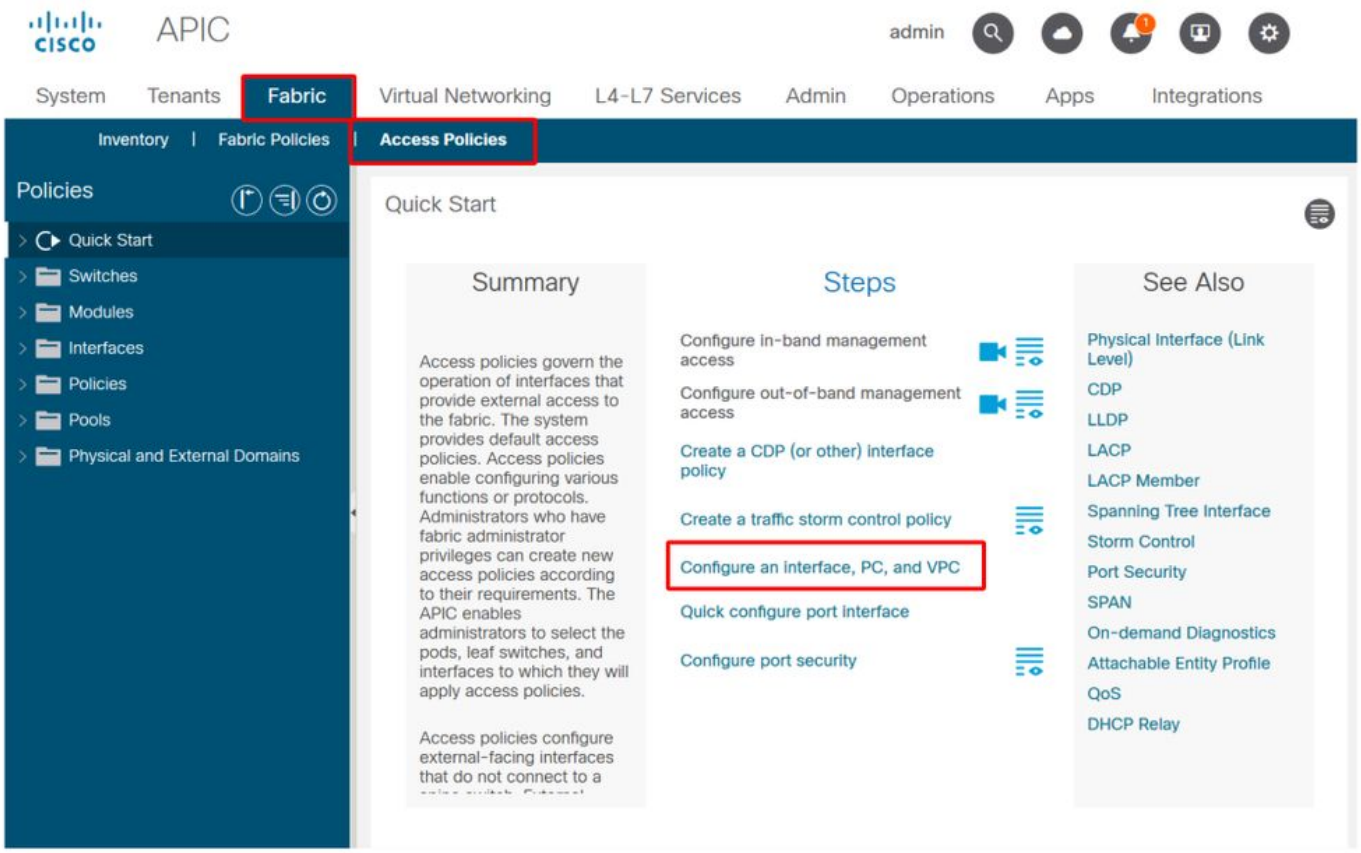
Die Zugriffsrichtlinien der ACI sind anfangs zwar etwas einschüchternd, aber äußerst flexibel und sollen die Bereitstellung von Konfigurationen für ein großes SDN-Netzwerk in kontinuierlicher Weiterentwicklung vereinfachen.

Konfiguration der Zugriffsrichtlinie: Methodik

Zugriffsrichtlinien können unabhängig konfiguriert werden, d. h. durch die Erstellung aller erforderlichen Objekte. Sie können auch mithilfe der zahlreichen Assistenten der ACI-GUI definiert werden.

Assistenten sind sehr hilfreich, da sie den Benutzer durch den Workflow führen und sicherstellen, dass alle erforderlichen Richtlinien vorhanden sind.

Zugriffsrichtlinien: Schnellstart-Assistent

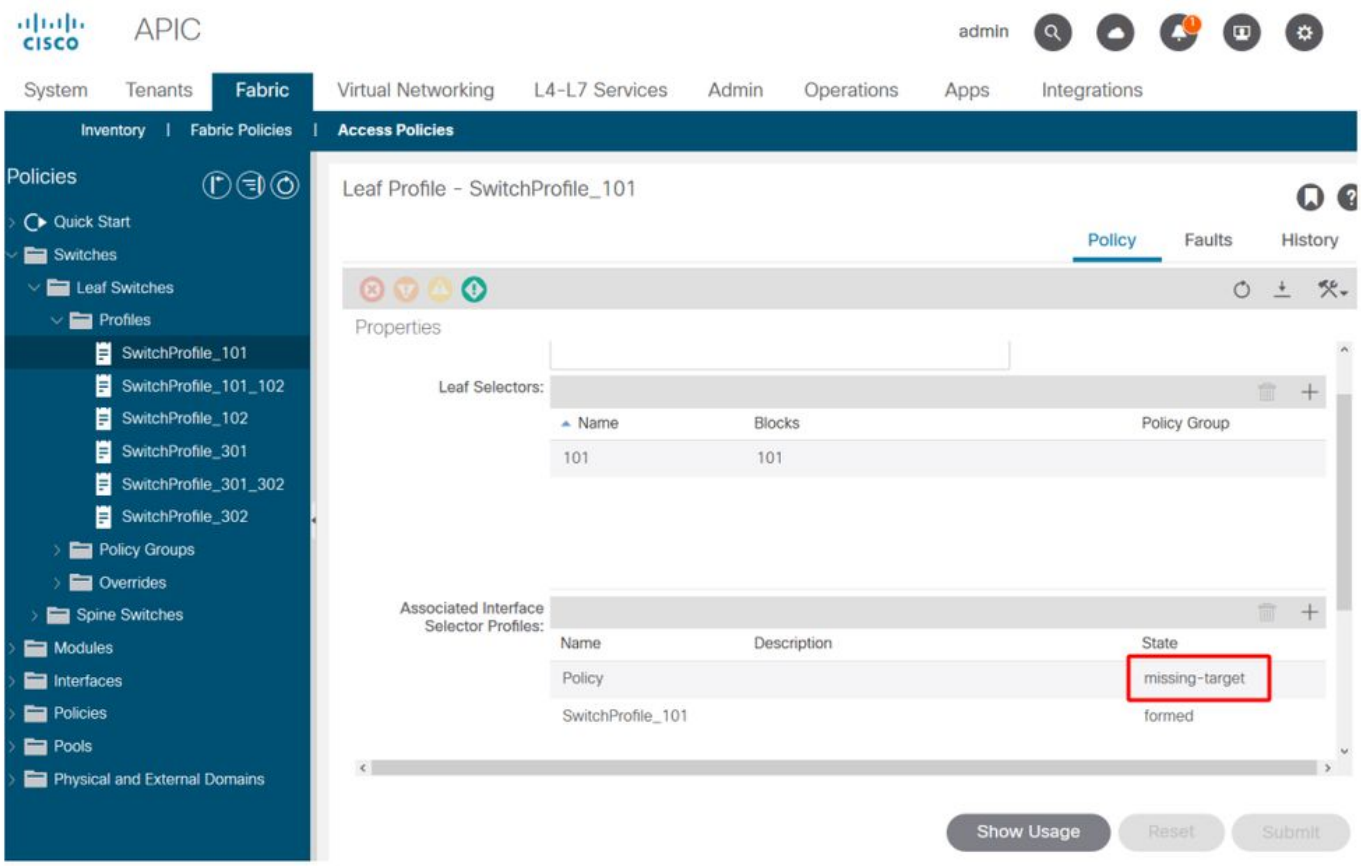


Die Abbildung oben zeigt die Schnellstartseite, auf der mehrere Assistenten zu finden sind.

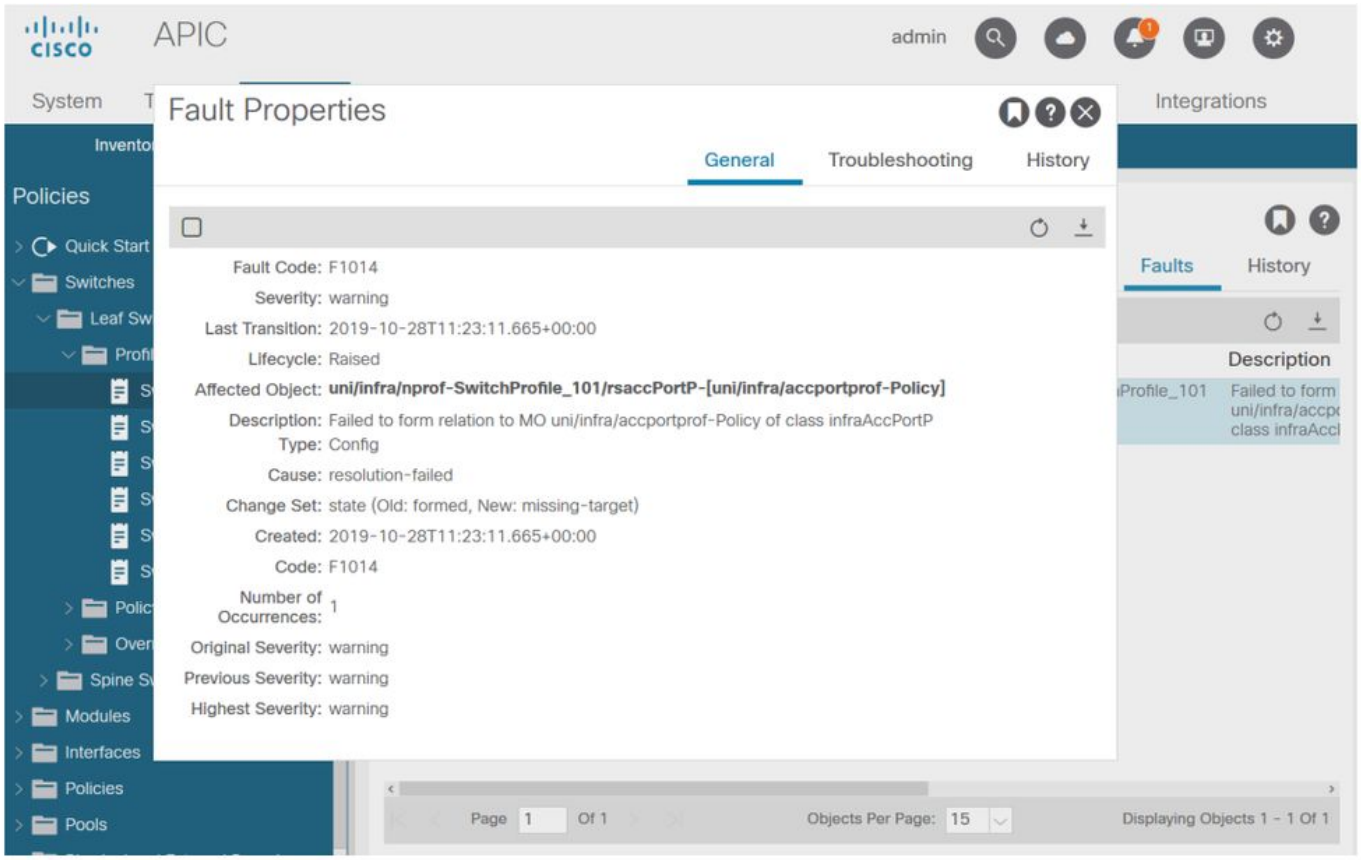
Nach dem Definieren einer Zugriffsrichtlinie wird allgemein empfohlen, die Richtlinie zu validieren, indem sichergestellt wird, dass keine Fehler bei allen verknüpften Objekten auftreten.

In der folgenden Abbildung wurde beispielsweise einem Switch-Profil eine Schnittstellenauswahl-Richtlinie zugewiesen, die nicht existiert. Ein aufmerksamer Benutzer kann leicht den Status "**Missing-Target**" des Objekts erkennen und überprüfen, ob ein Fehler in der GUI angezeigt wurde:

Leaf-Profil — SwitchProfile_101



Leaf-Profil — SwitchProfile_101 — Fehler



In diesem Fall wäre die Korrektur des Fehlers so einfach wie die Erstellung eines neuen Schnittstellenauswahl-Profils namens "Policy".

Die manuelle Konfiguration grundlegender Zugriffsrichtlinien wird in den folgenden Abschnitten

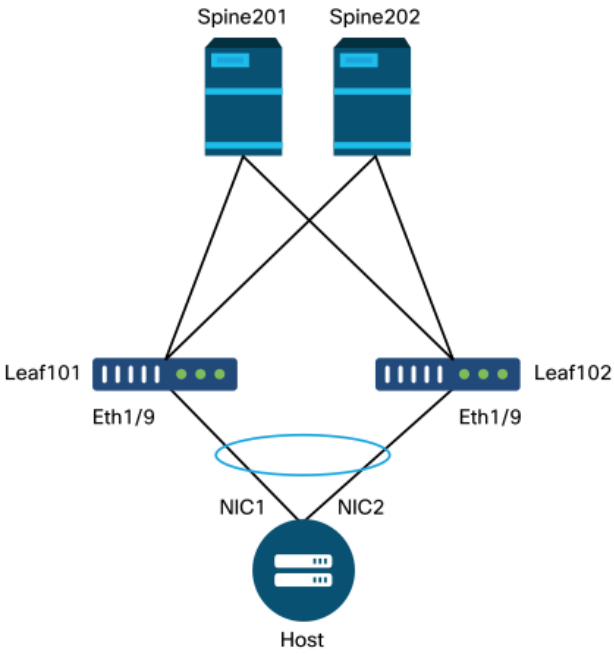
näher erläutert.

Manuelle Basiskonfigurationen für Zugriffsrichtlinien

Bei der Bereitstellung von Zugriffsrichtlinien werden Objekte definiert, die die beabsichtigte Verwendung der angegebenen Downlinks zum Ausdruck bringen. Die Deklaration, die die Downlinks programmiert (z.B. EPG Static Port Assignment), beruht auf dieser ausdrücklichen Absicht. Dies hilft, die Konfiguration zu skalieren und ähnliche Anwendungsobjekte wie Switches oder Ports, die speziell mit einem bestimmten externen Gerät verbunden sind, logisch zu gruppieren.

Verweisen Sie im weiteren Verlauf dieses Kapitels auf die nachfolgende Topologie.

Topologie der Zugriffsrichtliniendefinition für Dual-Homed-Server

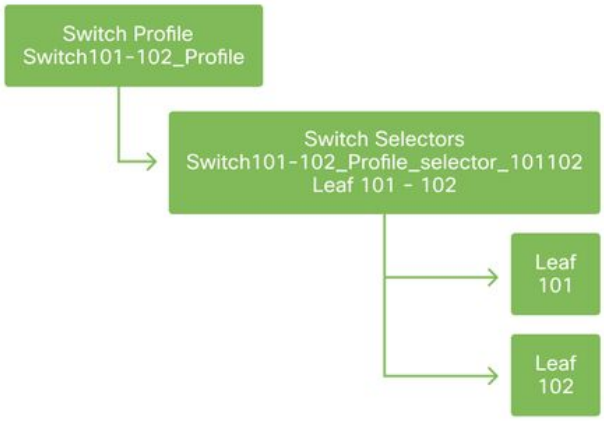


Ein Webserver ist mit einer ACI-Fabric verbunden. Der Webserver verfügt über 2 Netzwerkschnittstellenkarten (NICs), die in einem LACP-Port-Channel konfiguriert sind. Der Webserver ist mit dem Port 1/9 der Leaf-Switches 101 und 102 verbunden. Der Webserver verwendet VLAN-1501 und sollte sich in der EPG "EPG-Web" befinden.

Konfigurieren der Switch-Richtlinie

Der erste logische Schritt besteht in der Definition der zu verwendenden Leaf-Switches. Das 'Switch Profile' enthält 'Switch Selectors', die die zu verwendenden Leaf-Knoten-IDs definieren.

Switch-Richtlinien



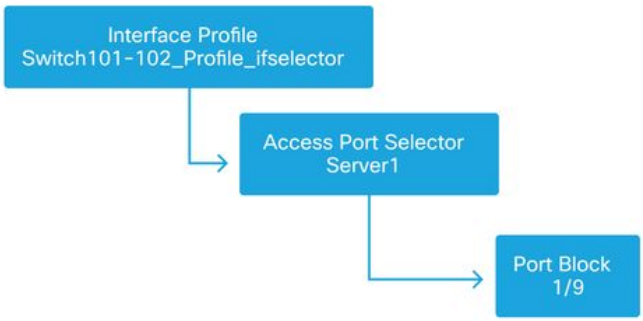
Es wird allgemein empfohlen, ein Switch-Profil pro einzelnem Leaf-Switch und ein Switch-Profil pro VPC-Domänenpaar zu konfigurieren. Dabei wird ein Namensschema verwendet, das die Knoten angibt, die Teil des Profils sind.

Der Schnellstart stellt ein logisches Benennungsschema bereit, das es einfach macht zu verstehen, wo es angewendet wird. Der vollständige Name entspricht dem Format 'Switch<node-id>_Profile'. Als Beispiel gilt "Switch101_Profile" für ein Switch-Profil mit dem Leaf-Knoten 101 und "Switch101-102_Profile" für ein Switch-Profil mit den Leaf-Knoten 101 und 102, das Teil einer vPC-Domäne sein sollte.

Konfigurieren der Schnittstellenrichtlinie

Nach dem Erstellen der Switch-Zugriffsrichtlinien ist die Definition der Schnittstellen der nächste logische Schritt. Dazu wird ein 'Interface Profile' erstellt, das aus mindestens einem 'Access Port Selector' besteht, der die 'Port Block'-Definitionen enthält.

Schnittstellenrichtlinien



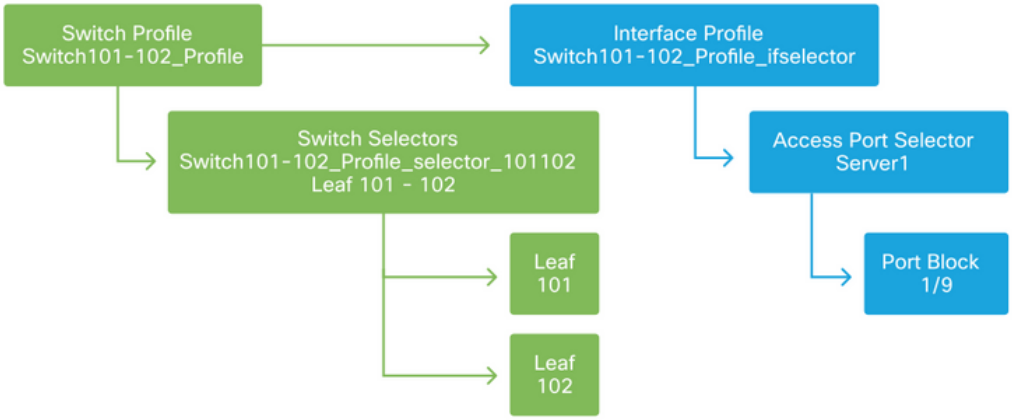
Um die Beziehung zwischen dem 'Interface Profile' und den beteiligten Switches herzustellen, verknüpfen Sie das 'Switch Profile' mit dem 'Interface Profile'.

"Schnittstellenprofile" können auf viele Arten definiert werden. Ähnlich wie bei "Switch Profiles" (Switch-Profilen) kann ein einzelnes "Interface Profile" (Schnittstellenprofil) pro physischem Switch zusammen mit einem "Interface Profile" (Schnittstellenprofil) pro VPC-Domäne erstellt werden. Diese Richtlinien müssen dann dem entsprechenden Switch-Profil 1:1 zugeordnet werden. Entsprechend dieser Logik werden die Fabric-Zugriffsrichtlinien stark vereinfacht, sodass andere Benutzer sie leicht verstehen können.

Auch die Standardbenennungsschemata des Schnellstarts können hier verwendet werden. Es

folgt dem Format "<Name des Switch-Profils>_ifSelector", um anzugeben, dass dieses Profil zum Auswählen von Schnittstellen verwendet wird. Ein Beispiel wäre "Switch101_Profile_ifSelector". In diesem Beispiel wird "Interface Profile" verwendet, um Nicht-VPC-Schnittstellen auf dem Leaf-Switch 101 zu konfigurieren, und es wird nur der Zugriffsrichtlinie "Switch101_Profile" zugeordnet.

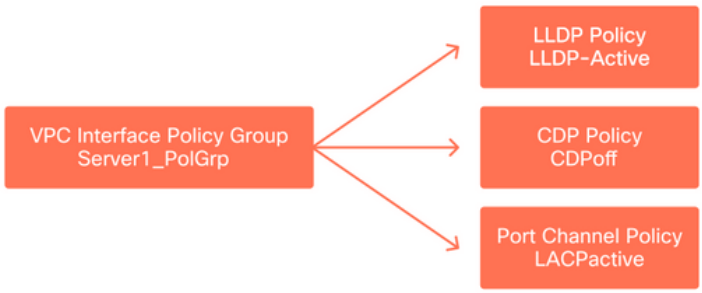
Mit Schnittstellenprofil verbundenes Switch-Profil



Da ein 'Schnittstellenprofil' mit Eth 1/9 mit einem 'Switch-Profil' verbunden ist, das beide Leaf-Switches 101 und 102 enthält, beginnt die Bereitstellung von Eth1/9 auf beiden Knoten gleichzeitig.

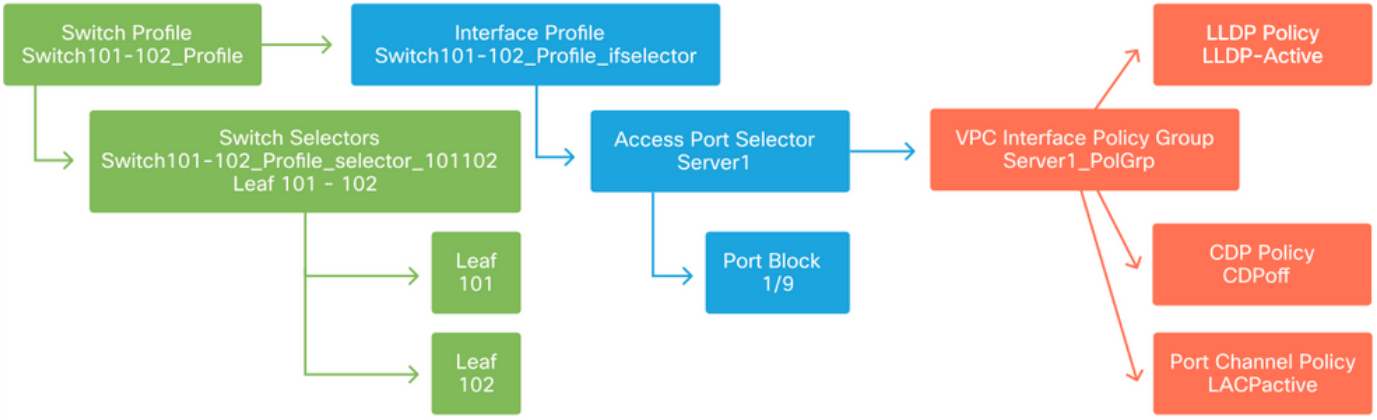
Jetzt wurden Leaf-Switches und ihre Ports definiert. Der nächste logische Schritt wäre die Definition der Merkmale dieser Ports. Die Schnittstellenrichtliniengruppe ermöglicht die Definition dieser Port-Eigenschaften. Es wird eine "vPC Interface Policy Group" (vPC-Schnittstellen-Richtliniengruppe) erstellt, um den oben genannten LACP-Port-Channel zu ermöglichen.

Richtliniengruppe



Die vPC-Schnittstellen-Richtliniengruppe wird mit der Schnittstellenrichtliniengruppe der Zugriffsport-Auswahl verknüpft, um die Beziehung zwischen Leaf-Switch/Schnittstelle und Port-Eigenschaften herzustellen.

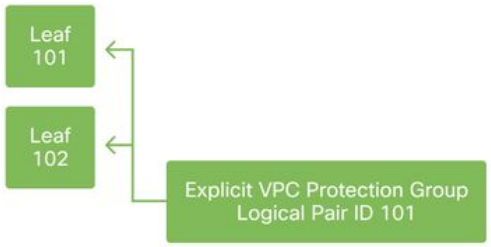
Kombination aus Switch- und Schnittstellenprofilen



Konfigurieren der vPC

Um den LACP-Port-Channel über zwei Leaf-Switches zu erstellen, muss zwischen den Leaf-Switches 101 und 102 eine vPC-Domäne definiert werden. Hierzu wird zwischen den beiden Leaf-Switches eine vPC-Schutzgruppe definiert.

VPC



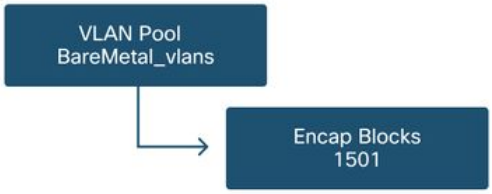
Konfigurieren von VLAN-Pools

Der nächste logische Schritt besteht in der Erstellung der VLANs, die an diesem Port verwendet werden, in diesem Fall VLAN-1501. Die Definition eines "VLAN-Pools" mit "Encap Blocks" vervollständigt diese Konfiguration.

Wenn Sie die Größe der VLAN-Pool-Bereiche berücksichtigen, beachten Sie, dass die meisten Bereitstellungen nur einen einzigen VLAN-Pool und einen zusätzlichen Pool benötigen, wenn Sie VMM-Integration verwenden. Um VLANs aus einem bestehenden Netzwerk in die ACI zu integrieren, definieren Sie den Bereich der vorhandenen VLANs als statischen VLAN-Pool.

Nehmen wir beispielsweise an, die VLANs 1-2000 werden in einer älteren Umgebung verwendet. Erstellen Sie einen statischen VLAN-Pool, der die VLANs 1-2000 enthält. Dadurch können ACI-Bridge-Domänen und EPGs mit der alten Fabric verbunden werden. Bei der Bereitstellung von VMM kann ein zweiter dynamischer Pool mit einer Reihe freier VLAN-IDs erstellt werden.

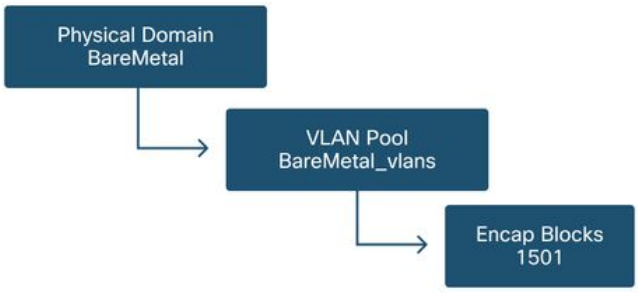
VLAN-Pool



Domänen konfigurieren

Der nächste logische Schritt ist die Erstellung einer 'Domäne'. Eine 'Domäne' definiert den Bereich eines VLAN-Pools, d. h. wo dieser Pool angewendet wird. Eine 'Domäne' kann physisch, virtuell oder extern (überbrückt oder geroutet) sein. In diesem Beispiel wird eine "physische Domäne" verwendet, um einen Bare-Metal-Server mit der Fabric zu verbinden. Diese Domäne wird mit dem VLAN-Pool verknüpft, um die erforderlichen VLANs zuzulassen.

Physische Domänen



Für die meisten Bereitstellungen reicht eine einzige "physische Domäne" für Bare-Metal-Bereitstellungen aus, und eine einzige "Routed Domain" für L3Out-Bereitstellungen. Beide können demselben VLAN-Pool zugeordnet werden. Wenn die Fabric auf Multi-Tenant-Basis bereitgestellt wird oder wenn eine detailliertere Kontrolle erforderlich ist, um einzuschränken, welche Benutzer bestimmte EPGs und VLANs auf einem Port bereitstellen können, sollte ein strategischeres Design der Zugriffsrichtlinien in Betracht gezogen werden.

'Domänen' bieten außerdem die Funktion, den Benutzerzugriff auf Richtlinien mithilfe von 'Sicherheitsdomänen' mithilfe der rollenbasierten Zugriffskontrolle (RBAC) zu beschränken.

Bei der Bereitstellung von VLANs auf einem Switch kapselt die ACI Spanning-Tree-BPDUs mit einer eindeutigen VXLAN-ID, die auf der Domäne basiert, von der das VLAN stammt. Aus diesem Grund ist es wichtig, bei der Verbindung von Geräten, die STP-Kommunikation mit anderen Brücken benötigen, dieselbe Domäne zu verwenden.

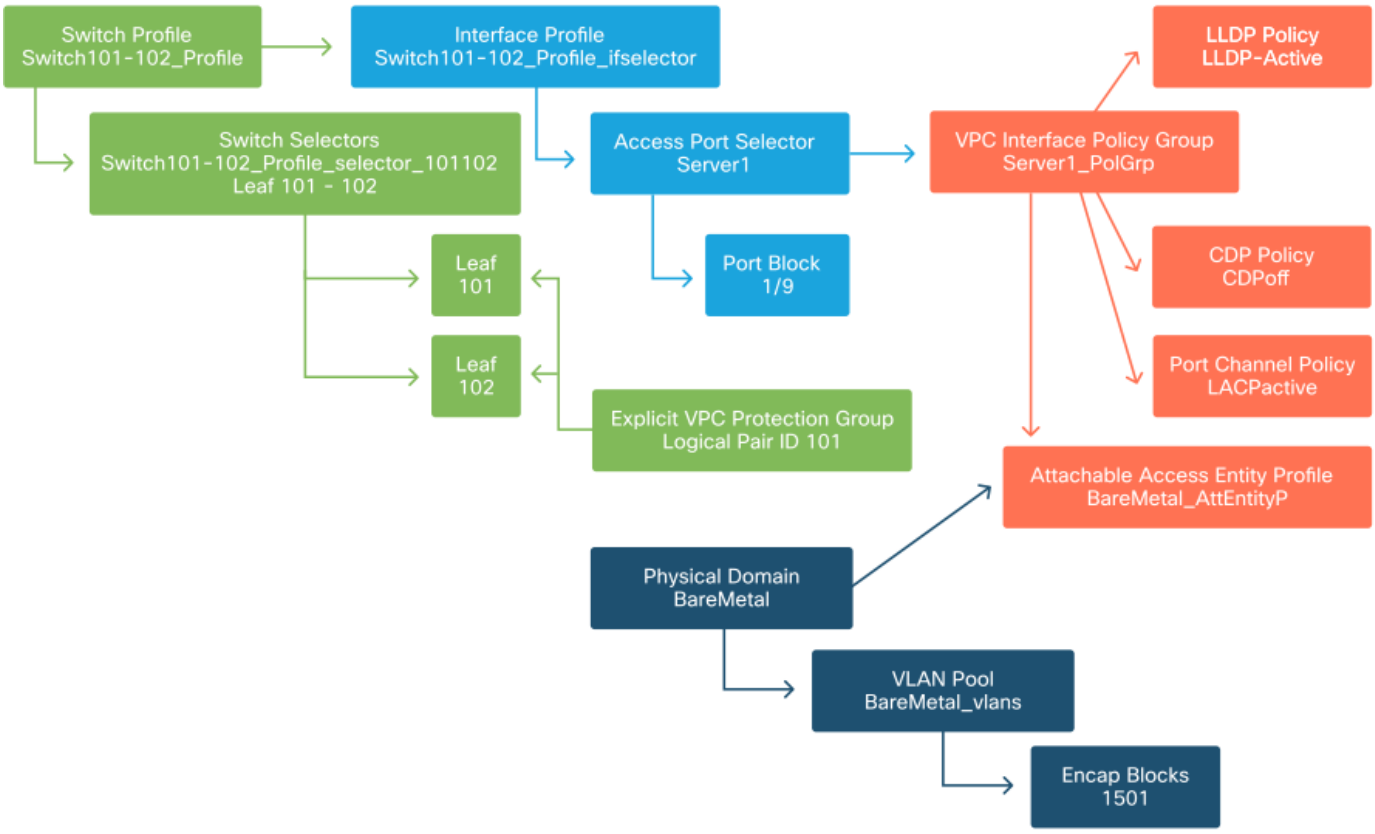
VLAN-VXLAN-IDs werden auch verwendet, damit VPC-Switches die von VPC abgefragten MAC- und IP-Adressen synchronisieren können. Aus diesem Grund besteht das einfachste Design für VLAN-Pools darin, einen einzelnen Pool für statische Bereitstellungen zu verwenden und einen zweiten Pool für dynamische Bereitstellungen zu erstellen.

Konfigurieren des angebundenen Zugriffsentitätsprofils (AEP)

Zwei wichtige Abschnitte der Konfiguration der Zugriffsrichtlinien wurden abgeschlossen: die Switch- und Schnittstellendefinitionen sowie die Domänen-/VLAN-Definitionen. Ein Objekt mit der Bezeichnung "Attachable Access Entity Profile" (AEP) dient dazu, diese beiden Blöcke miteinander zu verknüpfen.

Eine "Richtliniengruppe" ist mit einem AEP in einer 1:n-Beziehung verknüpft, die es dem AEP ermöglicht, Schnittstellen und Switches zusammenzufassen, die ähnliche Richtlinienanforderungen erfüllen. Das bedeutet, dass bei der Darstellung einer Gruppe von Schnittstellen auf bestimmten Switches nur auf einen AEP verwiesen werden muss.

Profil der angebundenen Zugriffseinheit



In den meisten Bereitstellungen sollte ein einzelner AEP für statische Pfade und ein zusätzlicher AEP pro VMM-Domäne verwendet werden.

Der wichtigste Aspekt ist, dass VLANs über den AEP an Schnittstellen bereitgestellt werden können. Dies kann durch direkte Zuordnung von EPGs zu einem AEP oder durch Konfiguration einer VMM-Domäne für die Vorabbereitstellung erfolgen. Beide Konfigurationen machen die zugehörige Schnittstelle zu einem Trunk-Port ("switchport mode trunk" auf Legacy-Switches).

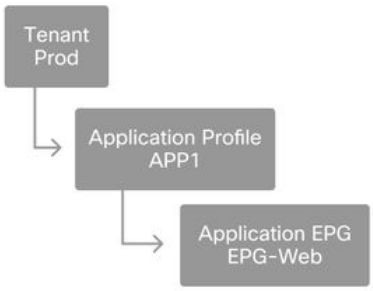
Aus diesem Grund ist es wichtig, einen separaten AEP für L3Out zu erstellen, wenn geroutete Ports oder geroutete Subschnittstellen verwendet werden. Wenn SVIs im L3Out verwendet werden, muss kein zusätzlicher AEP erstellt werden.

Tenant, APP und EPG konfigurieren

Die ACI definiert die Anbindung anders, indem sie einen richtlinienbasierten Ansatz verwendet.

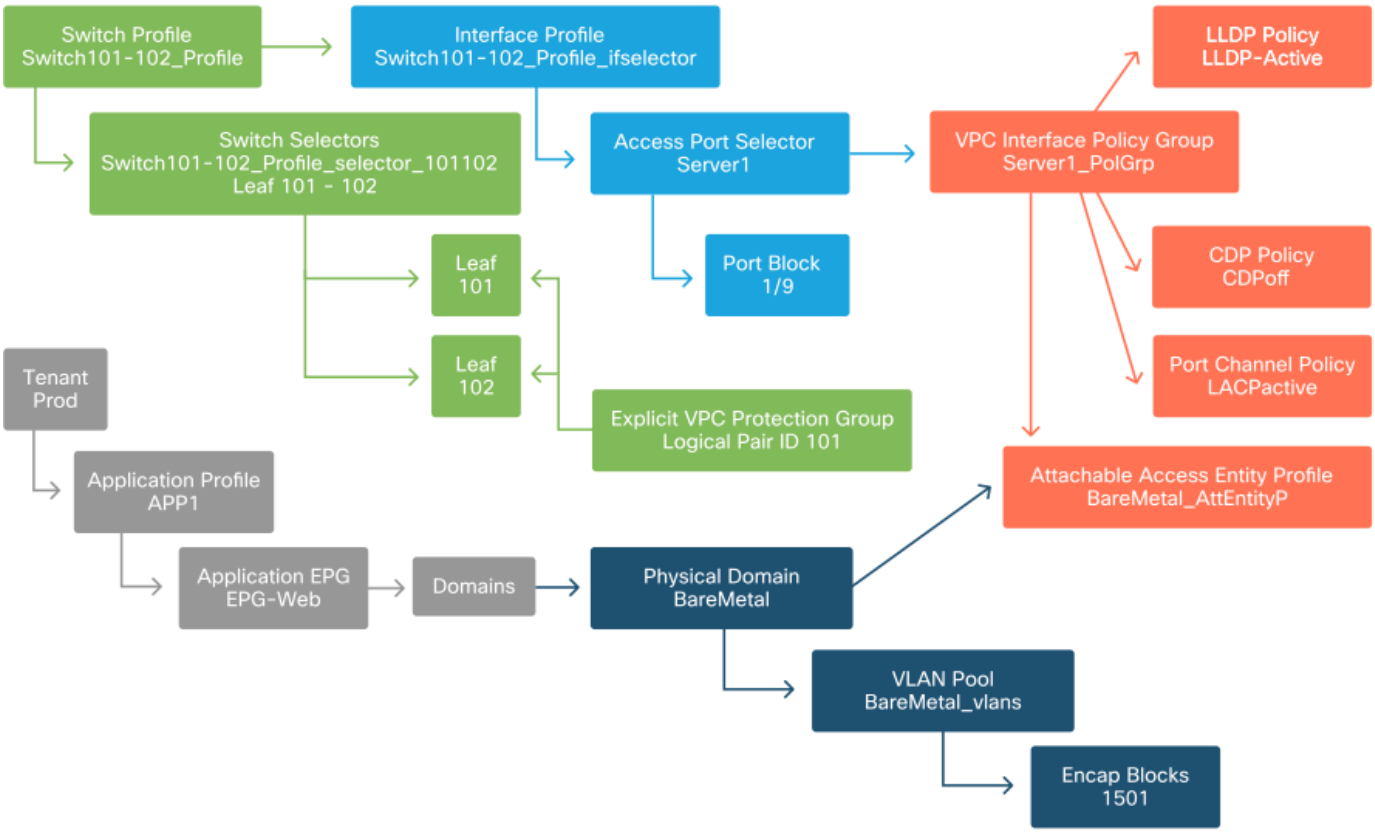
Das Objekt der untersten Ebene wird als Endpunktgruppe (Endpoint Group, EPG) bezeichnet. Mit dem EPG-Konstrukt wird eine Gruppe von VMs oder Servern (Endpunkten) mit ähnlichen Richtlinienanforderungen definiert. 'Anwendungsprofile', die unter einem Tenant vorhanden sind, werden zum logischen Gruppieren von EPGs verwendet.

Tenant, APP und EPG



Der nächste logische Schritt ist die Verknüpfung der EPG mit der Domäne. Dadurch wird eine Verbindung zwischen dem logischen Objekt, das unsere Arbeitslast darstellt, der EPG, und den physischen Switches/Schnittstellen, den Zugriffsrichtlinien, erstellt.

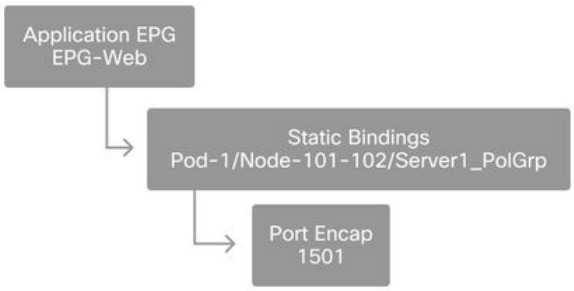
Verbindung zwischen EPG und Domäne



Konfigurieren der statischen EPG-Bindungen

Der letzte logische Schritt besteht darin, das VLAN für eine bestimmte EPG auf einer Switch-Schnittstelle zu programmieren. Dies ist besonders wichtig, wenn eine physische Domäne verwendet wird, da dieser Domänentyp eine explizite Deklaration erfordert. So kann die EPG aus dem Fabric heraus erweitert werden, und der Bare-Metal-Server kann in die EPG klassifiziert werden.

Statische Bindungen

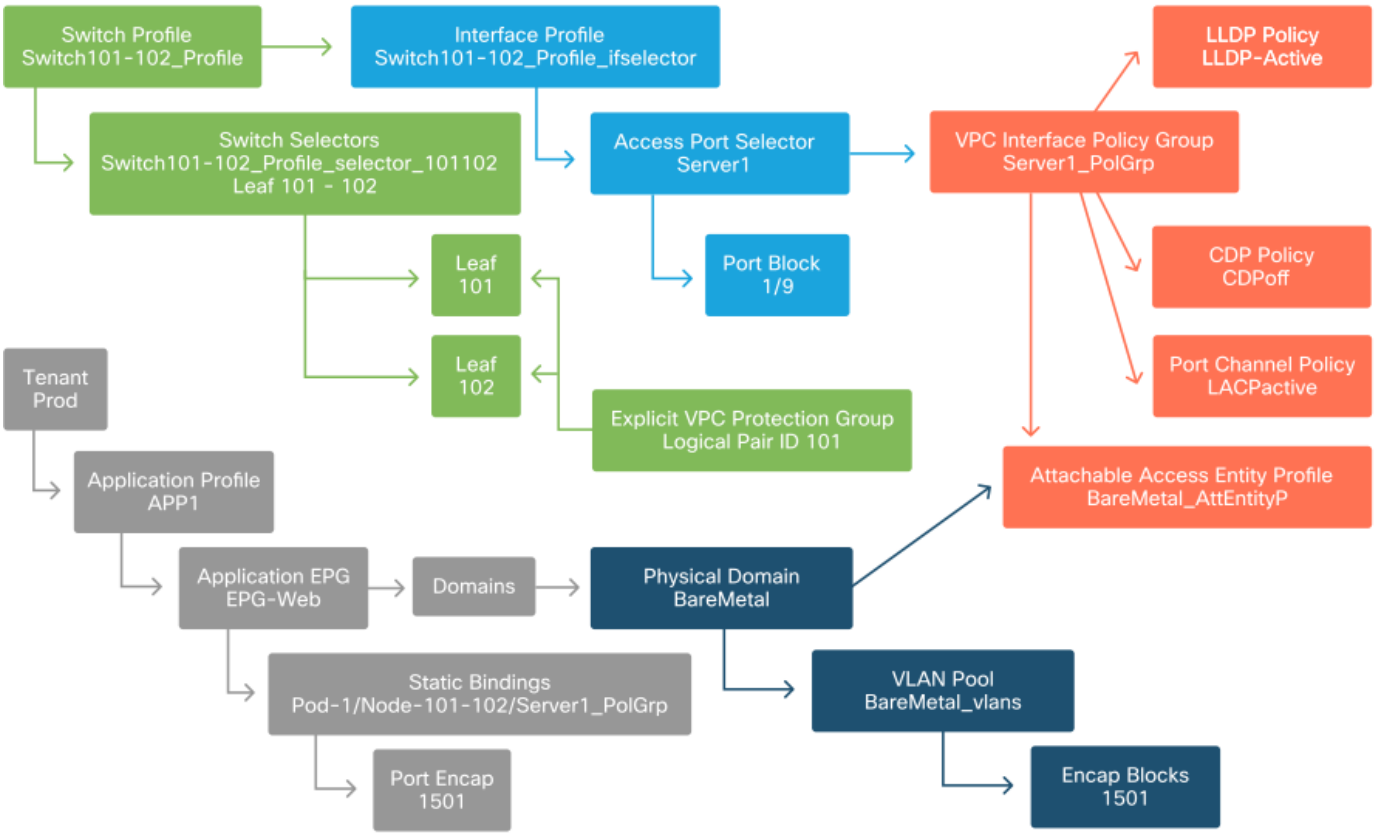


Die referenzierte Port-Encap muss gegenüber dem VLAN-Pool auflösbar sein. Ist dies nicht der Fall, wird ein Fehler markiert. Dies wird im Abschnitt "Problembehebungs-Workflow" dieses Kapitels beschrieben.

Zusammenfassung der Zugriffsrichtlinienkonfiguration

Im folgenden Diagramm werden alle Objekte zusammengefasst, die für die Verbindung des Hosts über VLAN-1501 mithilfe einer VPC-Verbindung mit den Leaf-Switches 101 und 102 erstellt wurden.

Bare-Metal-ACI-Anbindung



Anschließen zusätzlicher Server

Was würde es bedeuten, wenn alle zuvor erstellten Richtlinien einen weiteren Server an Port Eth1/10 der Leaf-Switches 101 und 102 mit einem Port-Channel verbinden würden?

In Bezug auf das Diagramm für die Bare-Metal-ACI-Anbindung müssen mindestens folgende Werte erstellt werden:

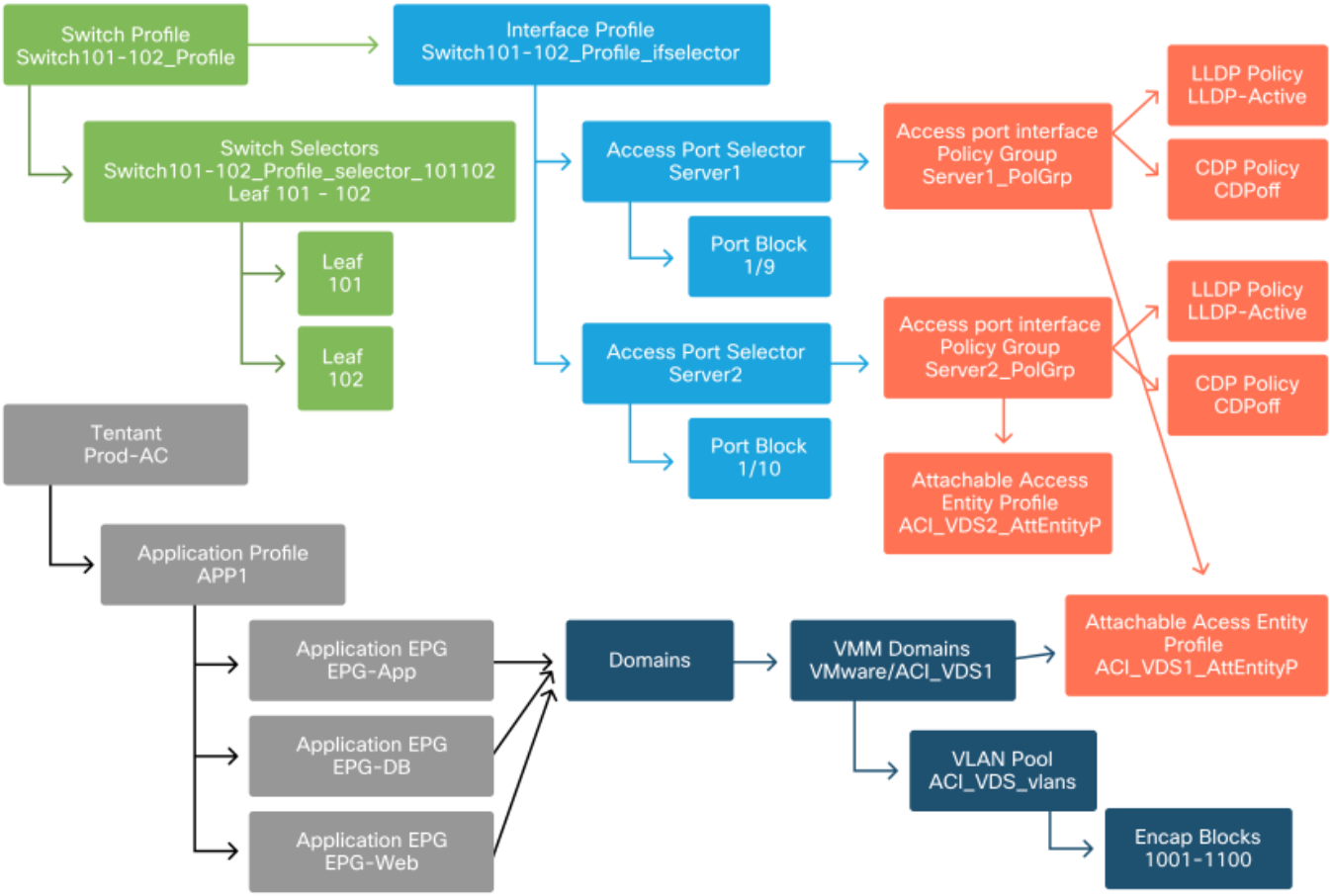
- Eine zusätzliche Auswahl von Access Ports und ein zusätzlicher Port-Block.
- Eine zusätzliche VPC-Schnittstellen-Richtliniengruppe.
- Eine zusätzliche statische Bindung mit Port Encap.

Beachten Sie, dass für LACP-Port-Channels eine dedizierte VPC-Schnittstellen-Richtliniengruppe verwendet werden muss, da diese die VPC-ID definiert.

Bei einzelnen Verbindungen kann die Nicht-VPC-Schnittstellen-Richtliniengruppe für den zusätzlichen Server wiederverwendet werden, wenn für die Verbindung dieselben Port-Eigenschaften erforderlich sind.

Die daraus resultierenden Richtlinien würden wie folgt aussehen:

Verbinden von server2 mit dem Setup



Wie geht es weiter?

Im nächsten Abschnitt werden einige Ausfallszenarien für die Zugriffsrichtlinien behandelt. Beginnen Sie mit der Topologie und dem Anwendungsfall, die in dieser Übersicht behandelt werden.

Problembehebungs-Workflow

Beim Arbeiten mit Zugriffsrichtlinien konnten folgende Fehlerbehebungsszenarien auftreten:

- Eine fehlende Beziehung zwischen zwei oder mehr Einheiten in der Zugriffsrichtlinie, z. B.

eine Zugriffsrichtliniengruppe, die nicht mit einem AEP verknüpft ist.
- Eine fehlende oder unerwartete Richtlinie ist mit einer bestimmten Zugriffsrichtlinie verknüpft, z. B. einer LLDP-Richtlinie mit dem Namen "lldp_enabled", während in der Realität die LLDP rx/tx-Konfiguration deaktiviert ist.
- Ein fehlender oder unerwarteter Wert in der Zugriffsrichtlinie, z. B. das konfigurierte VLAN-ID-Encap, das im konfigurierten VLAN-Pool fehlt.
- Fehlende Beziehung zwischen EPG und Zugriffsrichtlinie, z. B. keine physische oder virtuelle Domänenzuordnung zur EPG.

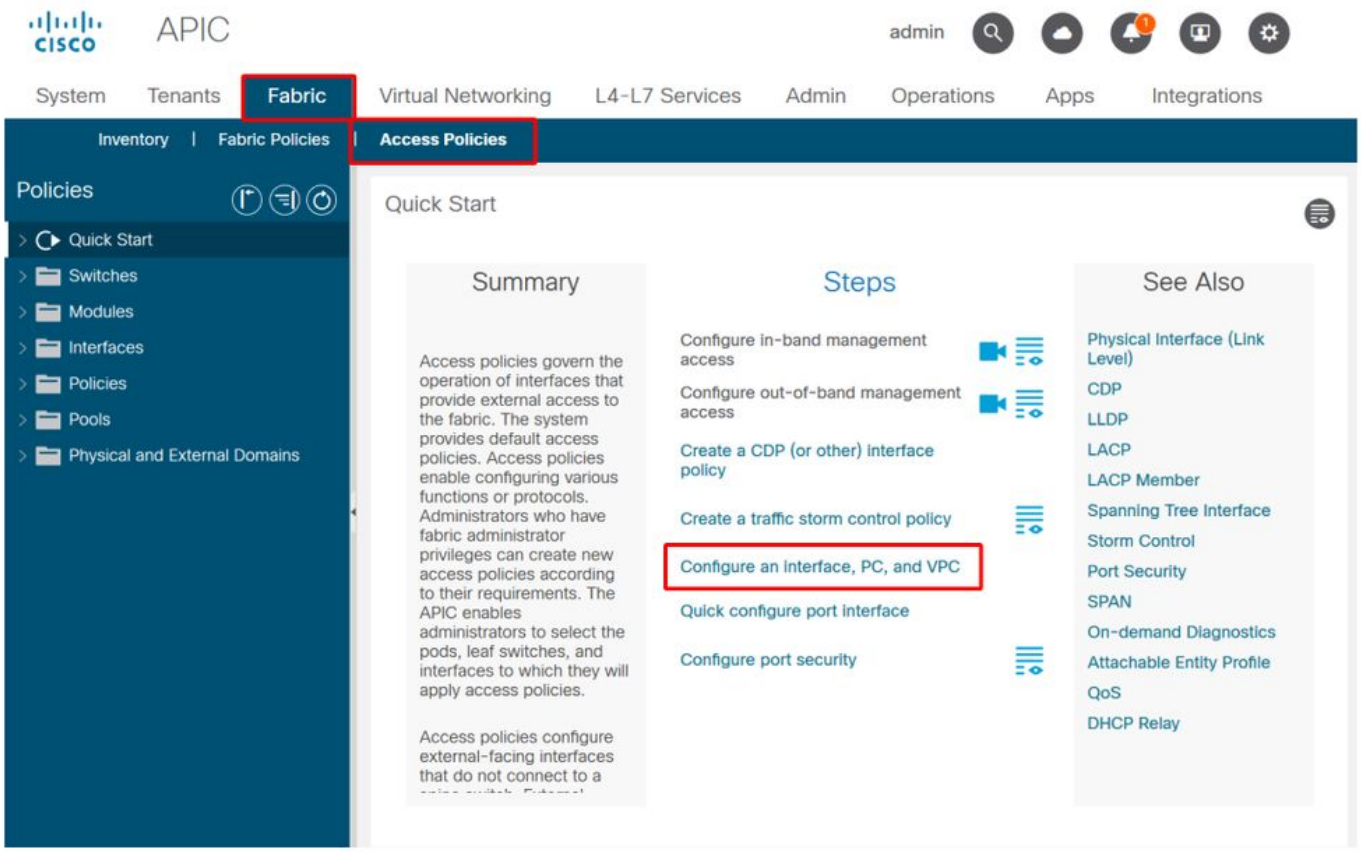
Die meisten der oben genannten Fehlerbehebungsmaßnahmen umfassen eine schrittweise Beschreibung der Beziehungen der Zugriffsrichtlinien, um festzustellen, ob Beziehungen fehlen, welche Richtlinien konfiguriert sind und/oder ob die Konfiguration das gewünschte Verhalten bewirkt.

Verwenden von "Configure interface, PC and VPC Quick Start" (Schnittstelle, PC und VPC Quick Start konfigurieren) zur Fehlerbehebung

Über die APIC-GUI erleichtert der Schnellstart-Assistent zum Konfigurieren von Schnittstellen, PC und VPC die Suche nach Zugriffsrichtlinien, indem er dem Administrator eine aggregierte Ansicht der vorhandenen Zugriffsrichtlinien bereitstellt. Dieser Schnellstart-Assistent ist in der grafischen Benutzeroberfläche unter folgender Adresse zu finden:

"Fabric > Access Policies > Quick Start > Steps > Configure Interface, PC, and VPC" (Fabric > Zugriffsrichtlinien > Schnellstart > Schritte > Schnittstelle konfigurieren, PC und VPC).

Speicherort von "Configure Interface, PC, and VPC" Quick Start



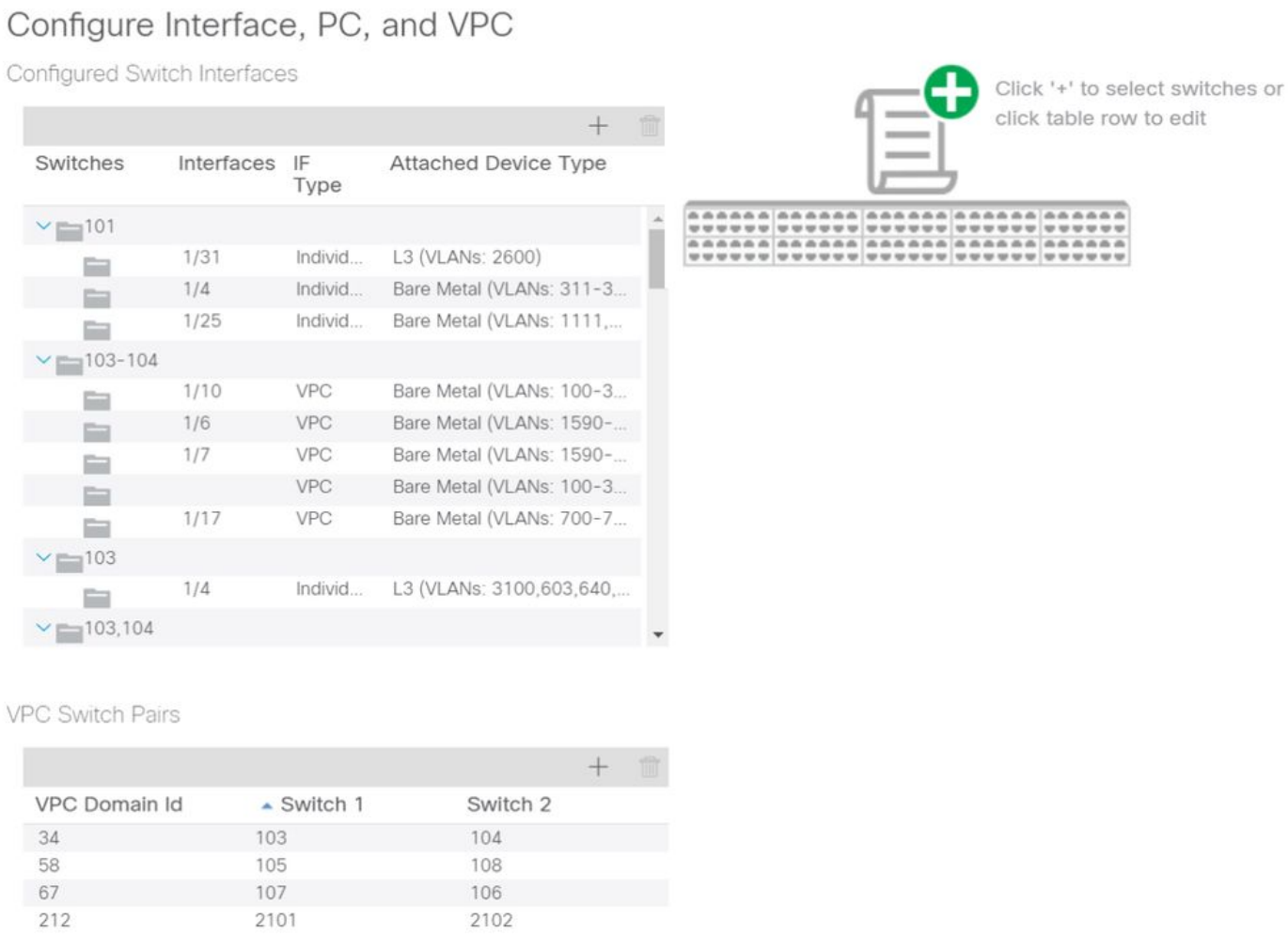
Obwohl der Name des Assistenten "Configure" (Konfigurieren) enthält, ist er besonders praktisch, um eine aggregierte Ansicht der vielen Zugriffsrichtlinien bereitzustellen, die konfiguriert werden

müssen, um Schnittstellen zu programmieren. Diese Aggregation dient als zentrale Ansicht, um zu ermitteln, welche Richtlinien bereits definiert sind, und um die Anzahl der Klicks zu reduzieren, die zum Isolieren von Problemen im Zusammenhang mit Zugriffsrichtlinien erforderlich sind.

Wenn die Schnellstartansicht geladen ist, kann auf die Ansicht "Konfigurierte Switch-Schnittstellen" (linker oberer Bereich) verwiesen werden, um vorhandene Zugriffsrichtlinien zu bestimmen. Der Assistent gruppiert die Einträge unter Ordnern, die einzelne oder mehrere Leaf-Switches darstellen, je nach Konfiguration der Zugriffsrichtlinien.

Um den Wert des Assistenten zu veranschaulichen, werden die folgenden Screenshots des Assistenten präsentiert, da der Leser keine Vorkenntnisse der Fabric-Topologie hat:

Demoansicht von "Configure Interface, PC, and VPC" Quick Start



Im Bereich "Konfigurierte Switch-Schnittstellen" werden Zugriffsrichtlinienzuordnungen angezeigt. Im Bereich "VPC Switch Pairs" werden die vollständigen VPC Protection Group-Definitionen angezeigt.

Die folgende Tabelle zeigt eine Teilmenge abgeschlossener Zugriffsrichtliniendefinitionen, die aus dem obigen Screenshot abgeleitet werden können.

Teilmenge abgeschlossener Zugriffsrichtlinien, die aus der oben stehenden Schnellstartansicht abgeleitet werden können

Switch-	Schnittst	Richtliniengruppen	Domänentyp	VLANs

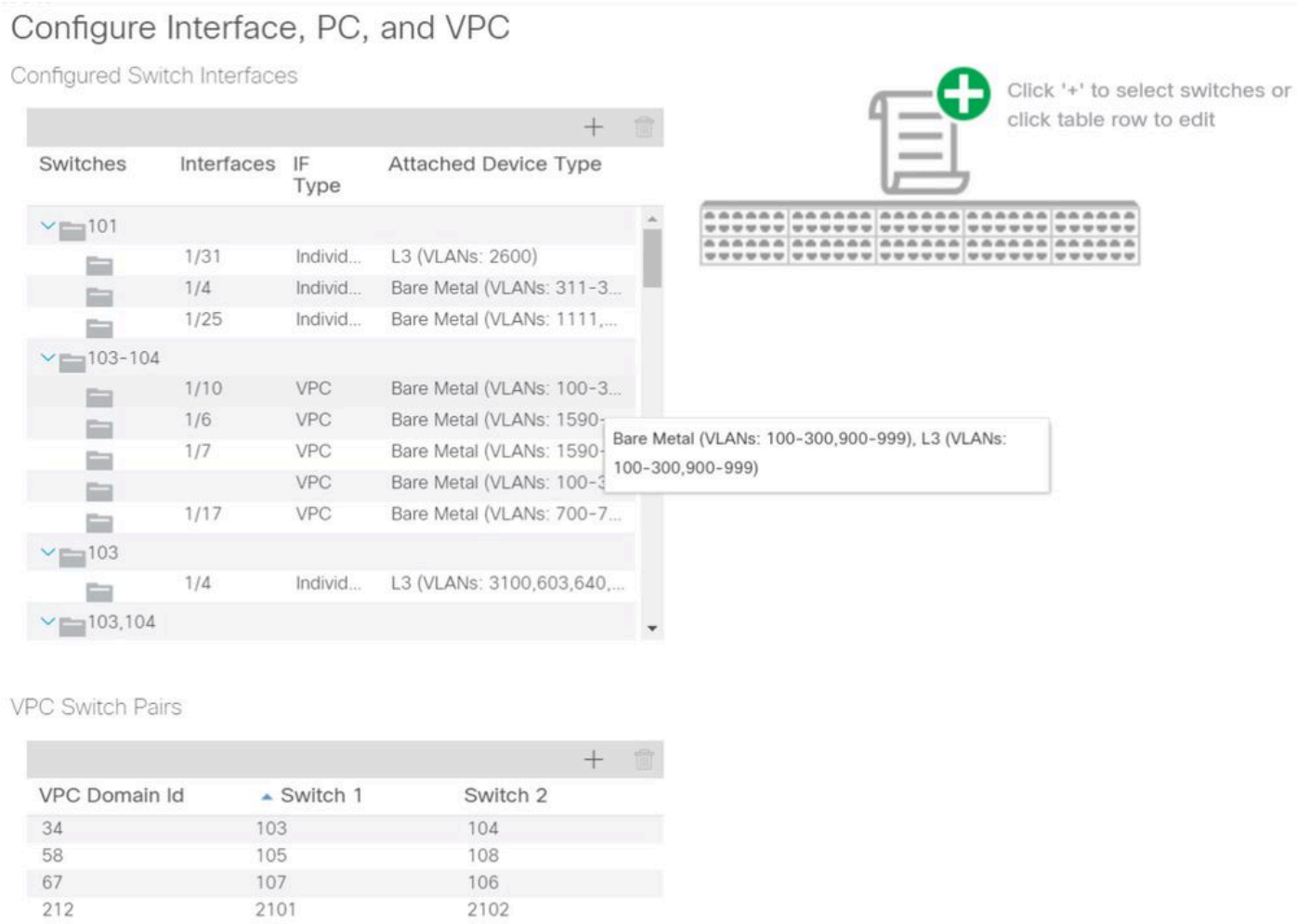
Knoten	elle	-Typ		
101	1/31	Individuell	Geroutet (L3)	2600
101	1/4	Individuell	Phys (Bare-Metal)	311-3?
103-104	1/10	VPC	Phys (Bare-Metal)	100-3?

Die Einträge in der VLAN-Spalte sind in der Standardansicht absichtlich unvollständig.

Ebenso können die vollständigen Richtlinien der VPC-Schutzgruppe aus der Ansicht "VPC-Switch-Paare" (linker unteren Bereich) abgeleitet werden. Ohne "VPC Protection Groups" können keine VPCs bereitgestellt werden, da dies die Richtlinie ist, die die VPC-Domäne zwischen zwei Leaf-Knoten definiert.

Beachten Sie, dass aufgrund der Fenstergröße lange Einträge nicht vollständig sichtbar sind. Bewegen Sie den Mauszeiger auf das entsprechende Feld, um den vollständigen Wert eines Eintrags anzuzeigen.

Mauszeiger bewegt sich über das Feld "Attached Device Type" (Angeschlossener Gerätetyp) für 103-104 in 1/10 VPC-Eintrag:



Wenn Sie den Mauszeiger über das Fenster bewegen, werden die vollständigen Einträge angezeigt.

Teilmenge der abgeschlossenen Zugriffsrichtlinien mit Mauszeigerdetails aktualisiert

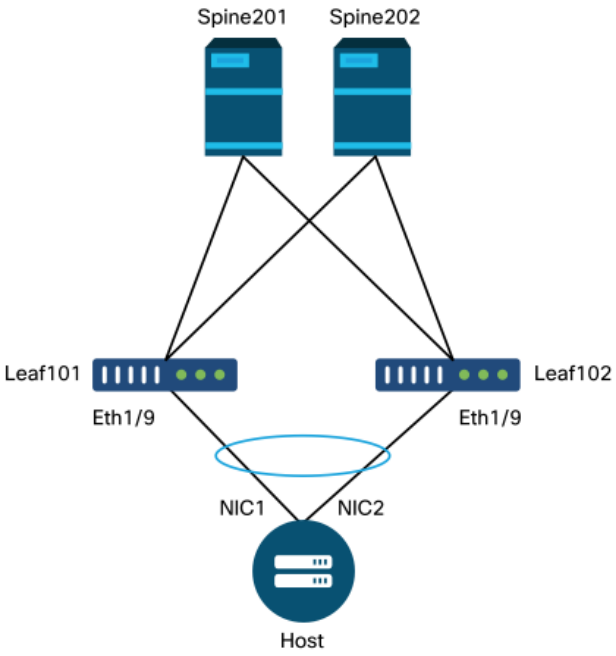
Switch-Knoten	Schnittstelle	Richtliniengruppen-Typ	Domänentyp	VLANs
101	1/31	Individuell	Geroutet (L3)	2600
101	1/4	Individuell	Phys (Bare-Metal)	311-320
103-104	1/10	VPC	Phys (Bare-Metal)	100-300,900-999
103-104	1/10	VPC	Geroutet (L3)	100-300,900-999

Die vollständigen VLAN-Zuordnungen können jetzt beobachtet und für die Fehlerbehebung und Verifizierung verwendet werden.

Fehlerbehebungsszenarien

Verweisen Sie bei den folgenden Fehlerbehebungsszenarien auf die gleiche Topologie wie im vorherigen Kapitel.

Topologie aus dem Abschnitt "Einführung" der Zugriffsrichtlinie



Szenario 1: Fehler F0467 — invalid-path, neue Probleme

Dieser Fehler tritt auf, wenn eine Switch-/Port-/VLAN-Deklaration ohne die entsprechenden Zugriffsrichtlinien erstellt wird, die eine ordnungsgemäße Anwendung der Konfiguration ermöglichen. Je nach Beschreibung dieses Fehlers fehlt möglicherweise ein anderes Element der Zugriffsrichtlinienbeziehung.

Nach der Bereitstellung einer statischen Bindung für die oben genannte VPC-Schnittstelle mit dem Trunked Encap VLAN 1501 ohne die entsprechende Zugriffsrichtlinienbeziehung wird der folgende Fehler in der EPG ausgelöst:

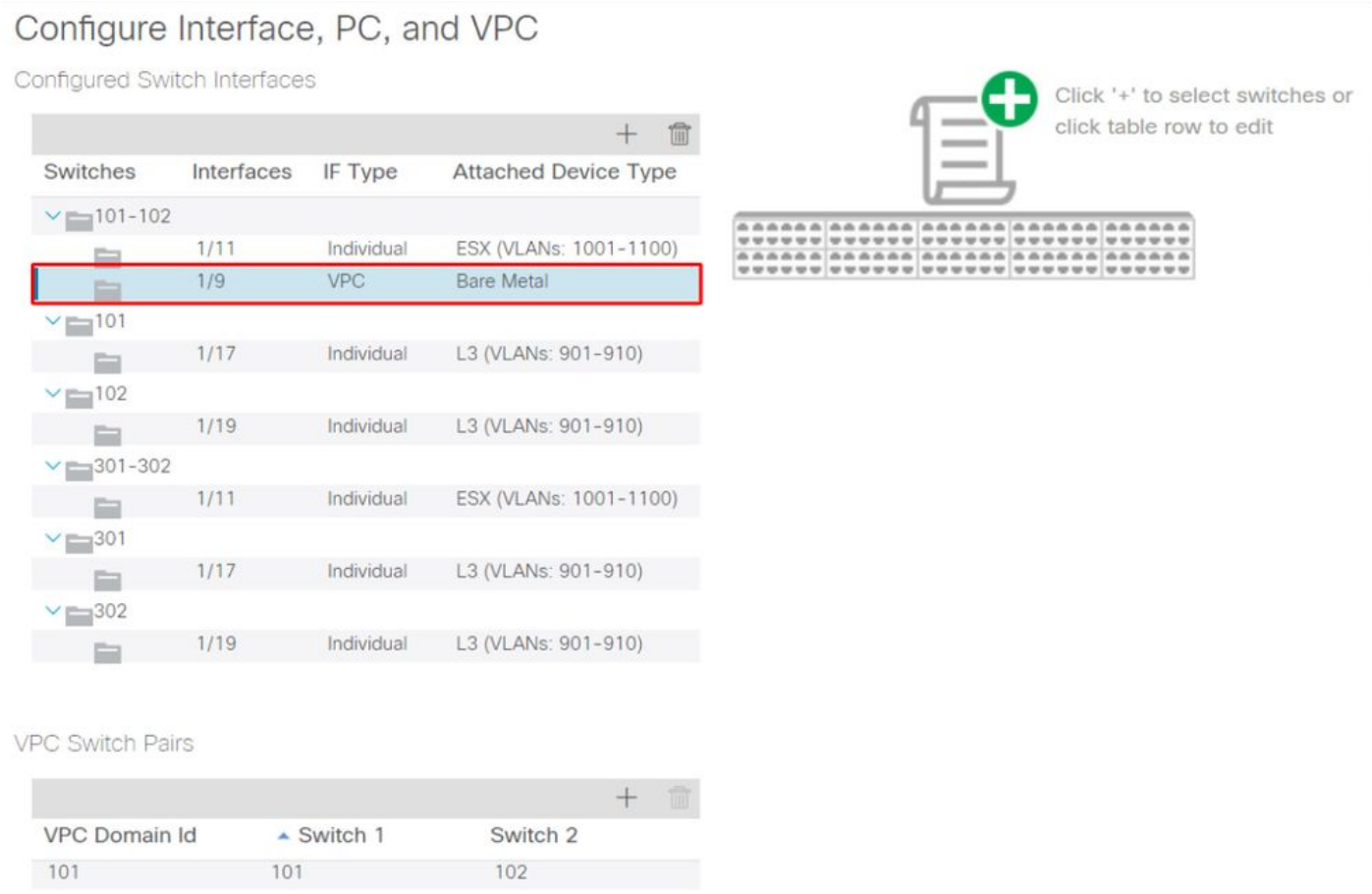
Fehler: F0467

Beschreibung: Fault delegate: Fehler bei der Konfiguration für uni/tn-Prod1/ap-App1/epg-EPG-Web node 101_101_102_eth1_9 aufgrund von ungültiger Pfadkonfiguration, ungültiger VLAN-Konfiguration, Debug-Meldung: Invalid-VLAN: vlan-1501: STP-Segment-ID für Encap nicht vorhanden. Entweder ist die EPG keiner Domäne zugeordnet, oder der Domäne ist dieses VLAN nicht zugewiesen;invalid-path: vlan-1501 : Es gibt keine Domäne, die sowohl der EPG als auch dem Port zugeordnet ist und für die ein VLAN erforderlich ist.

Aus der obigen Fehlerbeschreibung ergeben sich einige eindeutige Hinweise darauf, was die Ursache für die Fehlerauslösung sein könnte. Es wird eine Warnung ausgegeben, um die Beziehungen der Zugriffsrichtlinien und die Domänenzuordnung zur EPG zu überprüfen.

Wenn Sie sich die Schnellstartansicht des oben beschriebenen Szenarios ansehen, fehlt in der Zugriffsrichtlinie eindeutig ein VLAN.

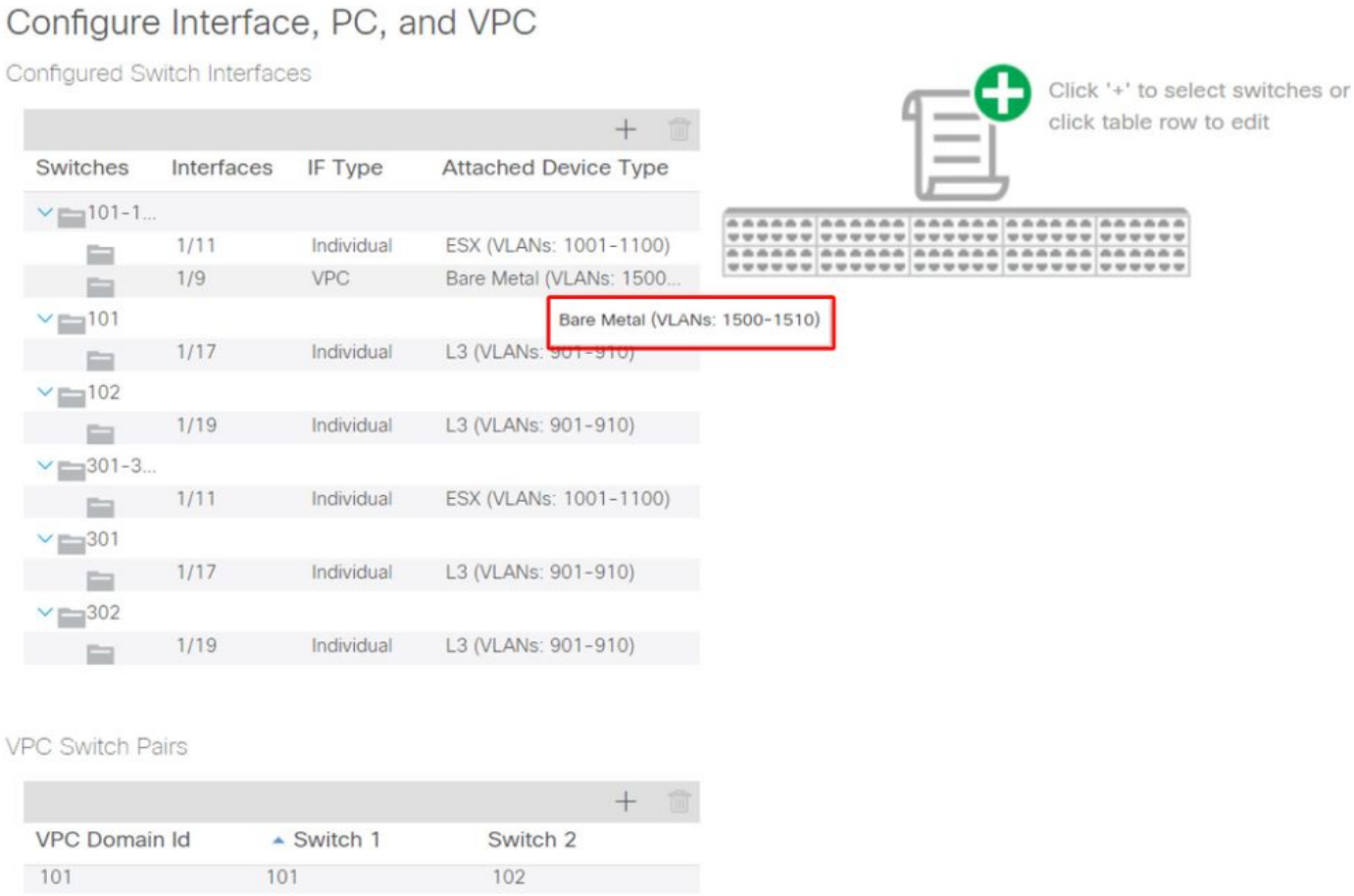
Schnellstartansicht, in der 101-102, Int 1/9 VPC keine VLANs enthält



Beachten Sie, dass dem Eintrag ein Verweis auf VLAN-IDs fehlt.

Nach der Korrektur wird in der Schnellstartansicht "(VLANs 1500-1510)" angezeigt.

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



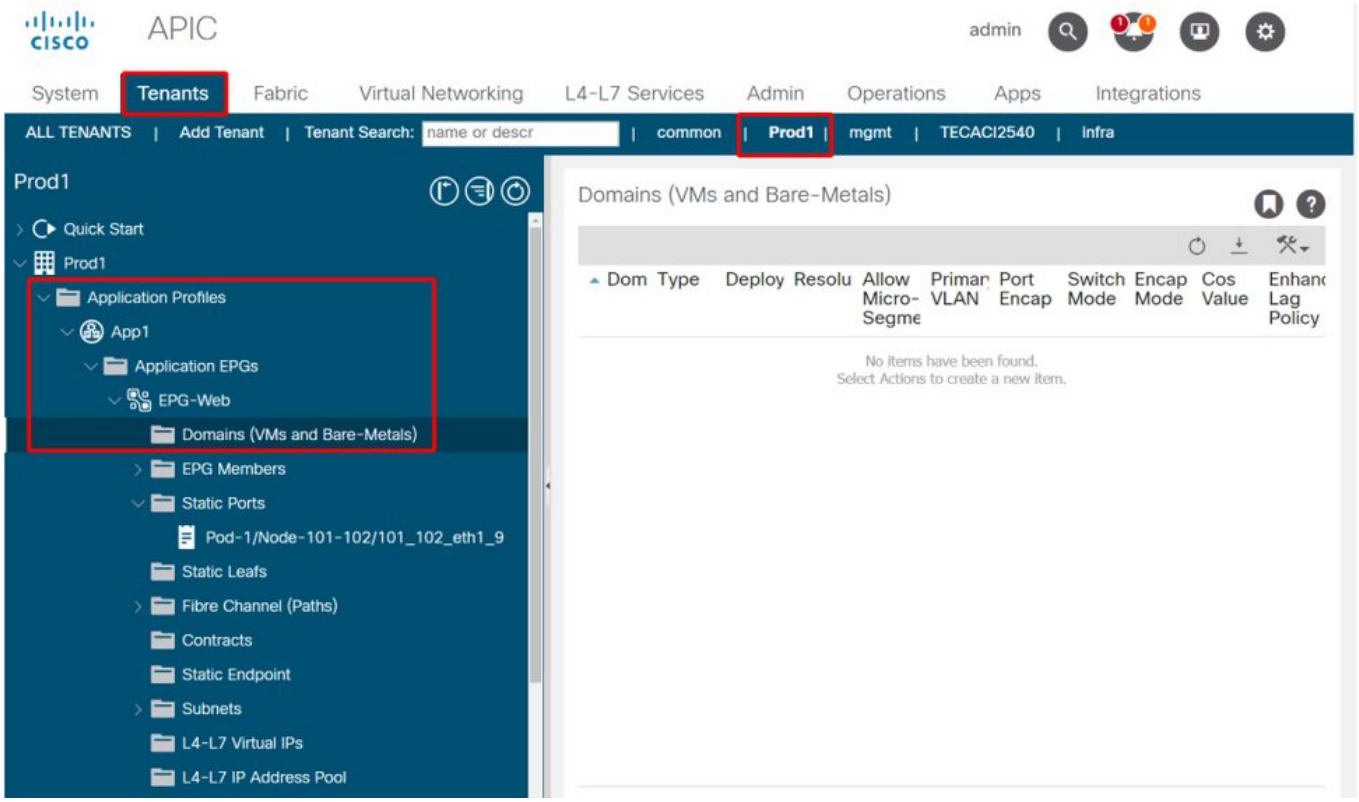
Der EPG-Fehler existiert jedoch weiterhin mit der folgenden aktualisierten Beschreibung für Fehler F0467:

Fehler: F0467

Beschreibung: Fault delegate: Fehler bei der Konfiguration für uni/tn-Prod1/ap-App1/epg-EPG-Web node 101_101_102_eth1_9 aufgrund von ungültiger Pfadkonfiguration, Fehlerbehebungsmeldung: Ungültiger Pfad: VLAN-150: Es gibt keine Domäne, die sowohl der EPG als auch dem Port zugeordnet ist und für die ein VLAN erforderlich ist.

Überprüfen Sie bei dem oben aktualisierten Fehler die EPG-Domänenzuordnungen, um festzustellen, dass keine Domänen mit der EPG verknüpft sind.

EPG-Web hat statische Ports, aber es fehlen Domänenzuordnungen.



Sobald die Domäne, die VLAN 1501 enthält, mit der EPG verknüpft ist, werden keine weiteren Fehler ausgelöst.

Szenario 2: VPC kann nicht als Bereitstellungspfad für den statischen EPG-Port oder das logische L3Out-Schnittstellenprofil (SVI) ausgewählt werden.

Bei dem Versuch, einen VPC als Pfad auf einem EPG Static Port oder L3Out Logical Interface Profile SVI-Eintrag zu konfigurieren, wird der bereitzustellende VPC nicht als verfügbare Option angezeigt.

Beim Versuch, eine statische VPC-Bindung bereitzustellen, sind zwei grundlegende Anforderungen zu beachten:

1. Für das betreffende Leaf-Switch-Paar muss die VPC Explicit Protection Group definiert werden.
2. Die vollständige Zuordnung der Zugriffsrichtlinien muss definiert werden.

Beide Anforderungen können wie oben gezeigt in der Schnellstartansicht überprüft werden. Wenn keines der beiden Kriterien erfüllt ist, wird die vPC-Funktion nicht als verfügbare Option für statische Portbindungen angezeigt.

Szenario 3: Fehler F0467 - Fabric Encap bereits in einer anderen EPG verwendet

Standardmäßig haben VLANs einen globalen Umfang. Das bedeutet, dass eine bestimmte VLAN-ID nur für eine einzelne EPG auf einem bestimmten Leaf-Switch verwendet werden kann. Jeder Versuch, dasselbe VLAN auf mehreren EPGs innerhalb eines Leaf-Switches wiederzuverwenden, hat folgenden Fehler zur Folge:

Fehler: F0467

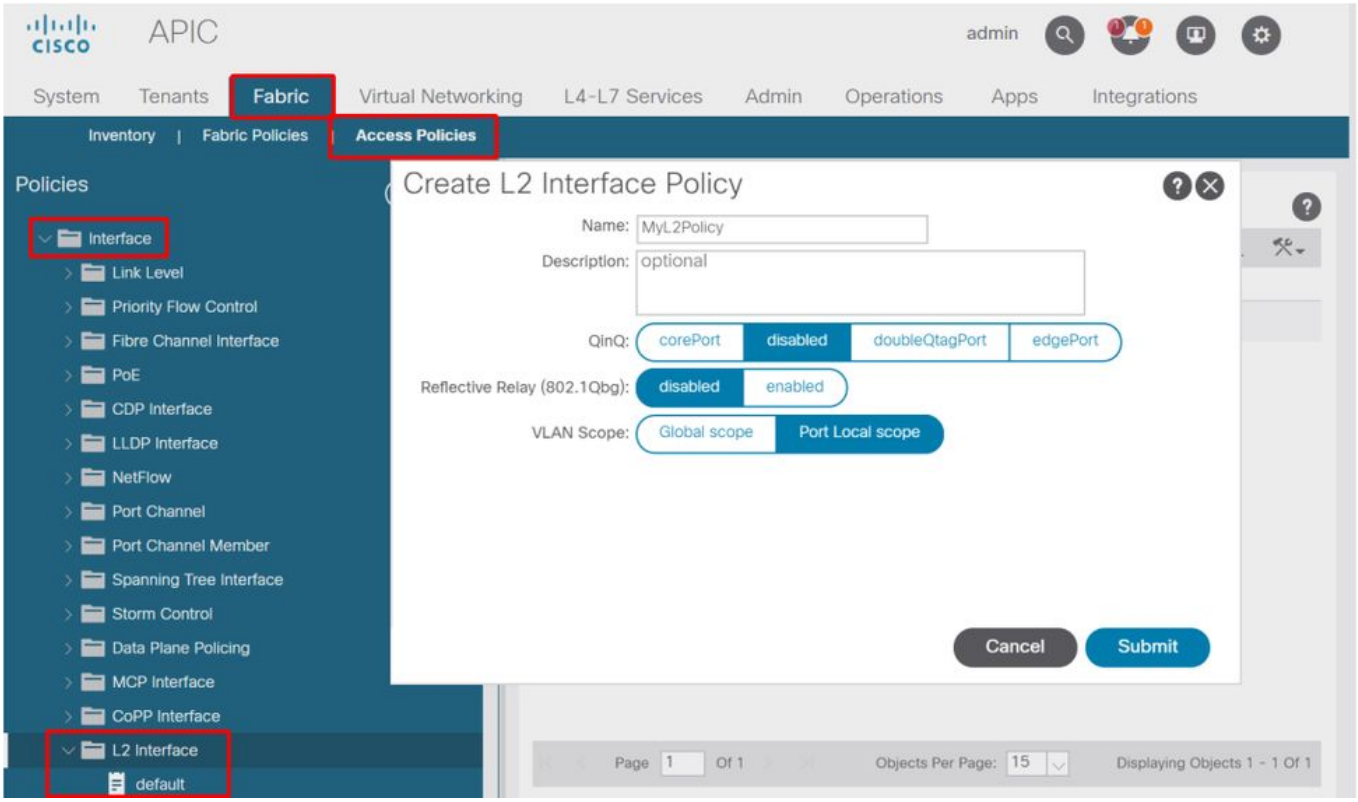
Beschreibung: Fault delegate: Fehler bei der Konfiguration für den uni/tn-Prod1/ap-App1/epg-

EPG-BusinessApp-Knoten 102 101_102_eth1_8. Ursache: Encap Already Used in Another EPG, Debug-Meldung: bereits benutztes encap: Encap wird bereits von Prod1:App1:EPG-Web verwendet.

Neben der Auswahl eines anderen VLAN besteht eine weitere Option, damit diese Konfiguration funktioniert, darin, die Verwendung des VLAN-Bereichs "Port Local" zu berücksichtigen. Dieser Bereich ermöglicht die Zuordnung von VLANs auf Schnittstellenbasis, sodass VLAN-1501 potenziell für verschiedene EPGs über mehrere Schnittstellen hinweg auf demselben Leaf verwendet werden kann.

Der Bereich "Port Local" wird zwar auf Richtliniengruppen-Basis (insbesondere über eine L2-Richtlinie) zugeordnet, aber auf Leaf-Ebene angewendet.

Speicherort zum Ändern der Einstellung für den VLAN-Bereich in der APIC-GUI



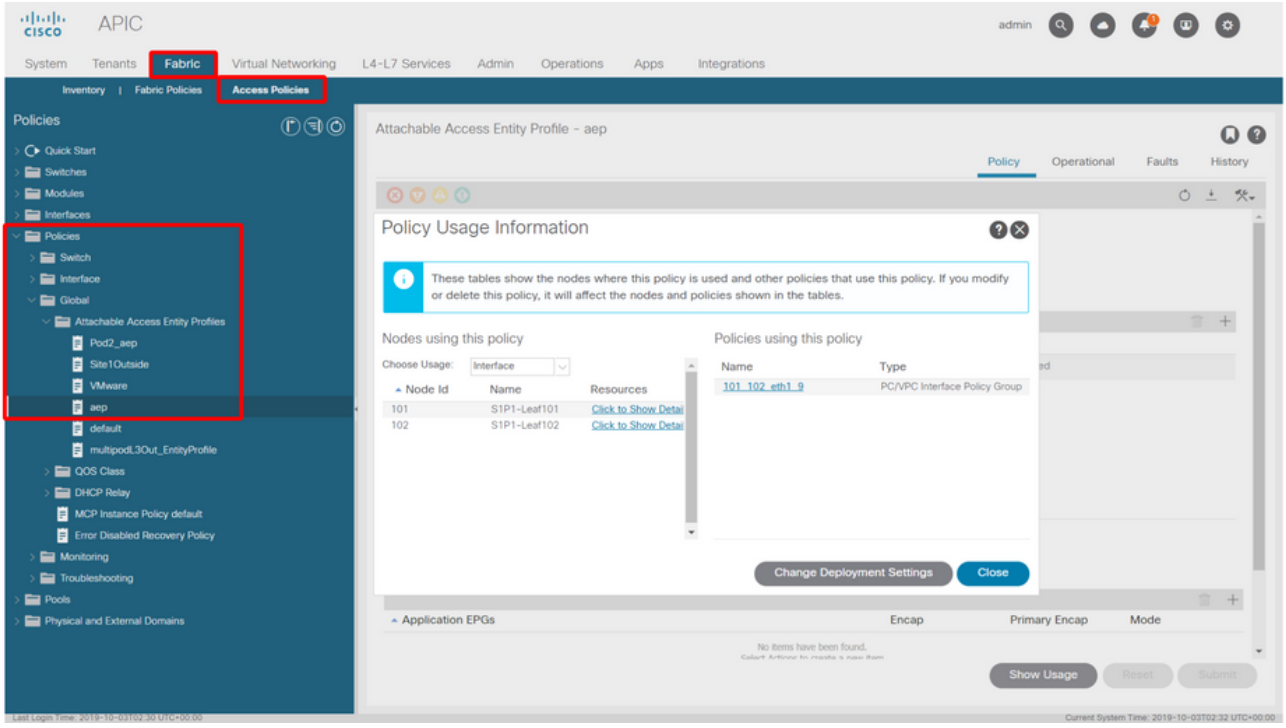
Vor der Implementierung der VLAN-Bereichskonfiguration für "Port Local" sollten Sie den "Cisco APIC Layer 2 Networking Configuration Guide" unter Cisco.com lesen, um sicherzustellen, dass die Einschränkungen und Designbeschränkungen für die gewünschten Anwendungsfälle und Designs akzeptabel sind.

Besondere Erwähnungen

Verwendung anzeigen

Obgleich nicht spezifisch für Zugriffsrichtlinien, steht für die meisten Objekte in der GUI eine Schaltfläche mit der Bezeichnung "Show Usage" (Nutzung anzeigen) zur Verfügung. Diese Schaltfläche führt eine Richtliniensuche mit dem ausgewählten Objekt durch, um zu ermitteln, welche Endknoten/Schnittstellen eine direkte Beziehung zu diesem Objekt haben. Dies kann sowohl für das allgemeine Suchszenario als auch zum Erlangen eines Verständnisses dafür nützlich sein, ob ein bestimmtes Objekt oder eine Richtlinie überhaupt verwendet wird.

Im folgenden Screenshot wird der ausgewählte AEP von zwei verschiedenen Schnittstellen verwendet. Dies bedeutet, dass eine Änderung des AEP direkte Auswirkungen auf die zugehörigen Schnittstellen haben wird.



Überlappende VLAN-Pools

Während die Zugriffsrichtlinien die Bereitstellung eines bestimmten VLAN auf einer Schnittstelle zulassen, muss in der Entwurfsphase eine zusätzliche Nutzung in Betracht gezogen werden. Insbesondere wird die Domäne bei der Berechnung der mit der externen Kapselung verknüpften VXLAN-ID (Fabric Encap) verwendet. Diese Funktion hat im Allgemeinen keine größeren Auswirkungen auf den Datenverkehr von Datenflugzeugen, aber solche IDs sind besonders relevant für eine Untergruppe von Protokollen, die das Fabric durchfluten, einschließlich Spanning Tree-BPDUs. Wenn auf Leaf1 eingehende VLAN-<id> BPDUs Leaf 2 ausgehen sollen (z. B. wenn Legacy-Switches Spanning Tree über die ACI konvergieren), muss VLAN-<id> auf beiden Leaf-Knoten dasselbe Fabric-Encap aufweisen. Wenn sich der Fabric-Encap-Wert für dieselben Zugriffs-VLANS unterscheidet, werden die BPDUs nicht über das Fabric übertragen.

Vermeiden Sie, wie im vorherigen Abschnitt erwähnt, die Konfiguration derselben VLANs in mehreren Domänen (z. B. VMM und Physical), es sei denn, es wird besonders darauf geachtet, dass jede Domäne nur auf einen eindeutigen Satz von Leaf-Switches angewendet wird. Sobald beide Domänen für ein bestimmtes VLAN auf demselben Leaf-Switch aufgelöst werden können, besteht die Möglichkeit, dass das zugrunde liegende VXLAN nach einem Upgrade (oder einem erneuten Laden) geändert werden kann, was beispielsweise zu STP-Konvergenzproblemen führen kann. Das Verhalten ist das Ergebnis jeder Domäne mit einem eindeutigen numerischen Wert (dem "base"-Attribut), der in der folgenden Gleichung zur Bestimmung der VXLAN-ID verwendet wird:

VXLAN VNID = Base + (encap — from_encap)

Um zu überprüfen, welche Domänen auf ein bestimmtes Leaf verschoben werden, kann eine moquery für die 'stpAllocEncapBlkDef'-Klasse ausgeführt werden:

```
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
```

Ermitteln Sie in dieser Ausgabe die folgenden Zugriffsrichtliniendefinitionen:

- Es gibt einen programmierten VLAN-Pool mit einem VLAN-Block, der die VLANS 1500-1510 explizit definiert.
- Dieser VLAN-Baustein ist mit der Domäne "physvlans" verknüpft.
- Der bei der VXLAN-Berechnung verwendete Basiswert ist 8492.
- Die resultierende VXLAN-Berechnung für VLAN-1501 würde 8492 + (1501-1500) = 8493 als Fabric-Kapselung lauten.

Die resultierende VXLAN-ID (in diesem Beispiel 8493) kann mit dem folgenden Befehl überprüft werden:

```
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
```

Wenn es einen anderen VLAN-Pool mit VLAN-1501 gibt, der auf dasselbe Leaf übertragen wird, kann ein Upgrade oder ein Neuladen möglicherweise einen eindeutigen Basiswert (und in der Folge ein anderes Fabric Encap) erfassen. Dies führt dazu, dass BPDUs nicht mehr auf ein anderes Leaf übertragen werden, das BPDUs auf VLAN-1501 empfangen soll.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.