

Solucionar problemas de políticas de acceso ACI

Contenido

[Introducción](#)

[Antecedentes](#)

[Descripción general de políticas de acceso](#)

[Configuración de la política de acceso: Metodología](#)

[Políticas de acceso configuraciones básicas manuales](#)

[Configuración de la política de switch](#)

[Configuración de la política de interfaz](#)

[Configuración de VPC](#)

[Configurar grupos de VLAN](#)

[Configurar dominios](#)

[Configuración del perfil de entidad de acceso \(AEP\) adjuntable](#)

[Configuración del arrendatario, APP y EPG](#)

[Configuración de los enlaces estáticos de EPG](#)

[Resumen de la configuración de la política de acceso](#)

[Conexión de servidores adicionales](#)

[¿Qué sigue?](#)

[Flujo de resolución de problemas](#)

[Uso de "Configuración de la interfaz, el PC y VPC Quick Start" para la resolución de problemas](#)

[Escenarios de resolución de problemas](#)

[Escenario 1: Fault F0467 — invalid-path, nwissues](#)

[Escenario 2: No se puede seleccionar VPC como ruta para implementar en el puerto estático EPG o en el perfil de interfaz lógica \(SVI\) L3Out](#)

[Escenario 3: Fault F0467: encapsulado de fabric ya utilizado en otro EPG](#)

[Menciones especiales](#)

[Mostrar uso](#)

[Conjuntos de VLAN superpuestos](#)

Introducción

Este documento describe los pasos para comprender y resolver problemas de las políticas de acceso de ACI.

Antecedentes

El material de este documento se extrajo del libro [Troubleshooting Cisco Application Centric Infrastructure, Second Edition](#), específicamente de los capítulos **Access Policies - Overview** y **Access Policies - Troubleshooting Workflow**.

Descripción general de políticas de acceso

¿Cómo configura el administrador de ACI una VLAN en un puerto del fabric? ¿Cómo empieza el administrador de ACI a solucionar los fallos relacionados con las políticas de acceso? En esta sección se explica cómo solucionar problemas relacionados con las políticas de acceso al fabric.

Antes de abordar los escenarios de solución de problemas, es fundamental que el lector conozca bien el funcionamiento de las políticas de acceso y sus relaciones dentro del modelo de objetos de ACI. Para ello, el lector puede consultar los documentos "Modelo de política de ACI" y "Referencia del modelo de información de gestión de APIC" disponibles en Cisco.com (<https://developer.cisco.com/site/apic-mim-ref-api/>).

La función de las políticas de acceso es habilitar la configuración específica en los puertos de enlace descendente de un switch de hoja. Antes de definir la política de arrendatarios para permitir el tráfico a través de un puerto de fabric de ACI, deben aplicarse las políticas de acceso correspondientes.

Normalmente, las políticas de acceso se definen cuando se agregan nuevos switches de hoja al fabric o cuando un dispositivo se conecta a enlaces descendentes de hoja de ACI; pero dependiendo de lo dinámico que sea un entorno, las políticas de acceso se podrían modificar durante el funcionamiento normal del fabric. Por ejemplo, para permitir un nuevo conjunto de VLAN o agregar un nuevo dominio enrutado a los puertos de acceso al fabric.

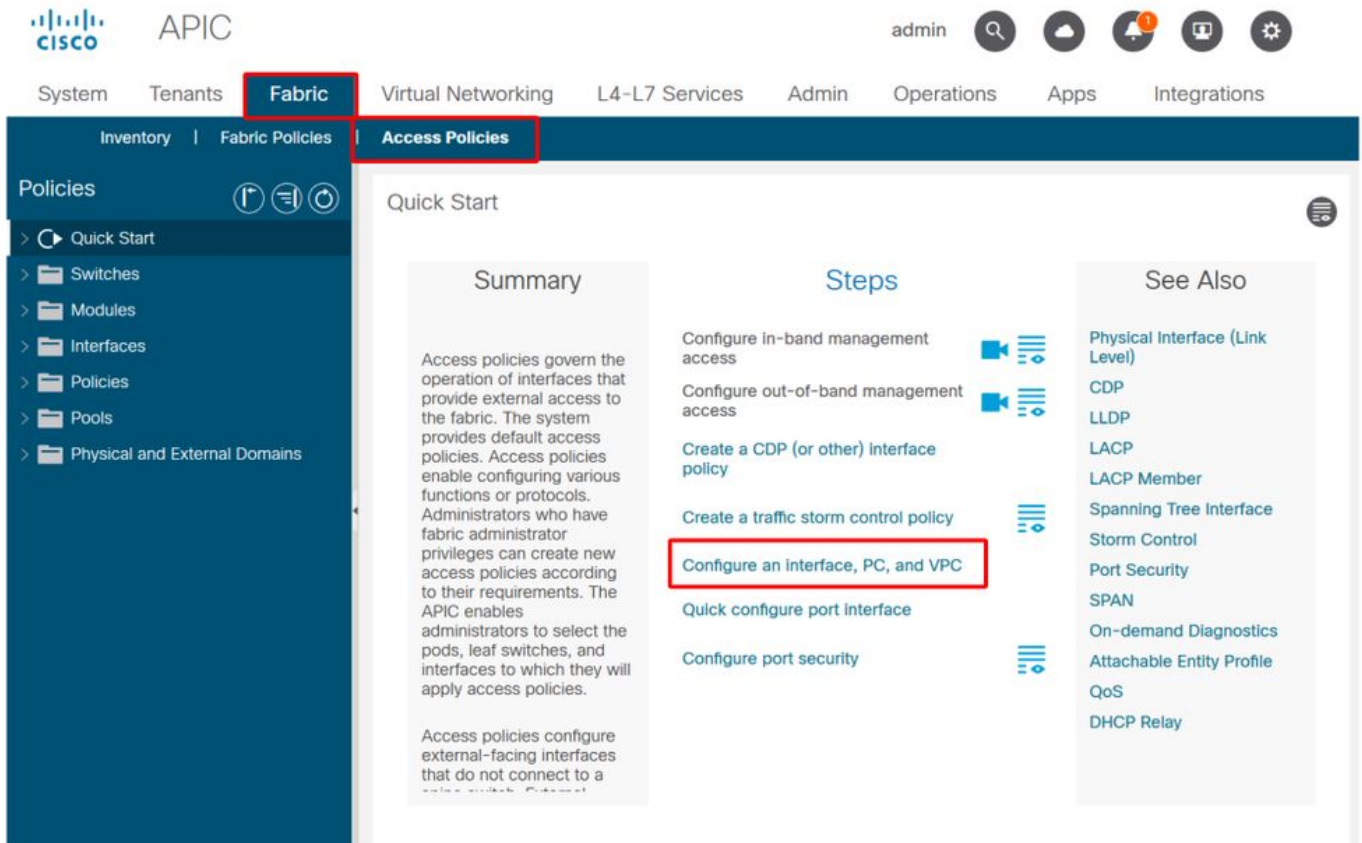
Las políticas de acceso de ACI, aunque inicialmente son un poco intimidantes, son extremadamente flexibles y están diseñadas para simplificar el aprovisionamiento de la configuración a una red SDN a gran escala en continua evolución.

Configuración de la política de acceso: Metodología

Las políticas de acceso se pueden configurar de forma independiente, es decir, creando todos los objetos necesarios de forma independiente, o se pueden definir a través de los numerosos asistentes proporcionados por la GUI de ACI.

Los asistentes son muy útiles porque guían al usuario a través del flujo de trabajo y se aseguran de que todas las políticas necesarias están en su lugar.

Directivas de acceso: Asistente para inicio rápido



La imagen anterior muestra la página Inicio rápido, donde se pueden encontrar varios asistentes.

Una vez definida una directiva de acceso, la recomendación genérica consiste en validar la directiva asegurándose de que todos los objetos asociados no muestran ningún error.

Por ejemplo, en la siguiente figura, un perfil de switch ha asignado una política de selector de interfaz que no existe. Un usuario atento podrá detectar fácilmente el estado **'missing-target'** del objeto y verificar que se ha detectado un fallo desde la GUI:

Perfil de hoja: SwitchProfile_101

The screenshot shows the Cisco APIC interface for configuring a Leaf Profile. The left sidebar shows a navigation tree with 'Policies' expanded. The main content area is titled 'Leaf Profile - SwitchProfile_101' and has tabs for 'Policy', 'Faults', and 'History'. Under the 'Policy' tab, there are sections for 'Leaf Selectors' and 'Associated Interface Selector Profiles'. The 'Associated Interface Selector Profiles' table has the following data:

Name	Description	State
Policy		missing-target
SwitchProfile_101		formed

Buttons at the bottom include 'Show Usage', 'Reset', and 'Submit'.

Perfil de hoja — SwitchProfile_101 — Fault

The screenshot shows the 'Fault Properties' dialog box in the Cisco APIC interface. The dialog has tabs for 'General', 'Troubleshooting', and 'History'. The 'General' tab is active, showing the following details:

- Fault Code: F1014
- Severity: warning
- Last Transition: 2019-10-28T11:23:11.665+00:00
- Lifecycle: Raised
- Affected Object: uni/infra/nprof-SwitchProfile_101/rsaccPortP-[uni/infra/accportprof-Policy]
- Description: Failed to form relation to MO uni/infra/accportprof-Policy of class infraAccPortP
- Type: Config
- Cause: resolution-failed
- Change Set: state (Old: formed, New: missing-target)
- Created: 2019-10-28T11:23:11.665+00:00
- Code: F1014
- Number of Occurrences: 1
- Original Severity: warning
- Previous Severity: warning
- Highest Severity: warning

The background shows the 'Faults' tab in the interface, with a table listing the fault:

Description
Profile_101 Failed to form uni/infra/accportprof-Policy of class infraAccPortP

At the bottom, there is a pagination bar showing 'Page 1 Of 1' and 'Objects Per Page: 15'.

En este caso, corregir la falla sería tan fácil como crear un nuevo perfil de selector de interfaz llamado 'Policy'.

La configuración manual de las políticas de acceso básicas se examinará en los párrafos

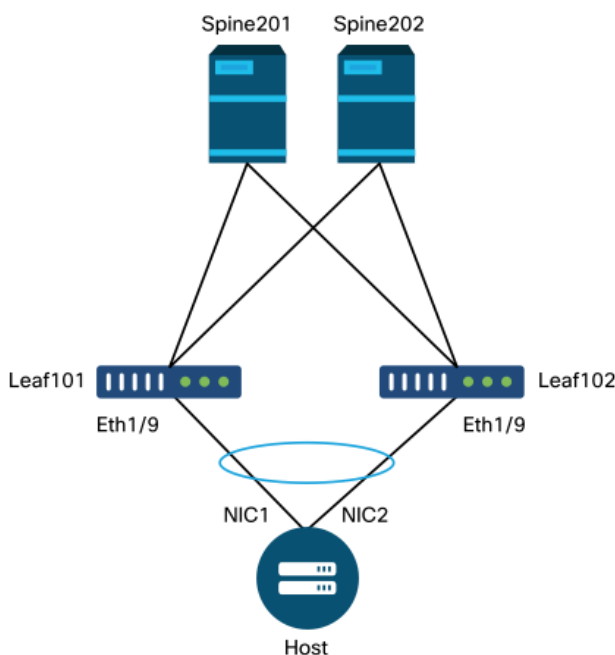
siguientes.

Políticas de acceso configuraciones básicas manuales

Al desplegar directivas de acceso, se definen objetos para expresar el uso esperado de los enlaces descendentes proporcionados. La declaración que programa los enlaces descendentes (por ejemplo, asignación de puerto estático EPG) se basa en esta intención expresada. Esto ayuda a escalar la configuración y agrupar lógicamente objetos de uso similares, como switches o puertos conectados específicamente a un dispositivo externo determinado.

Consulte la siguiente topología para ver el resto de este capítulo.

Topología de la definición de la política de acceso para el servidor de doble conexión

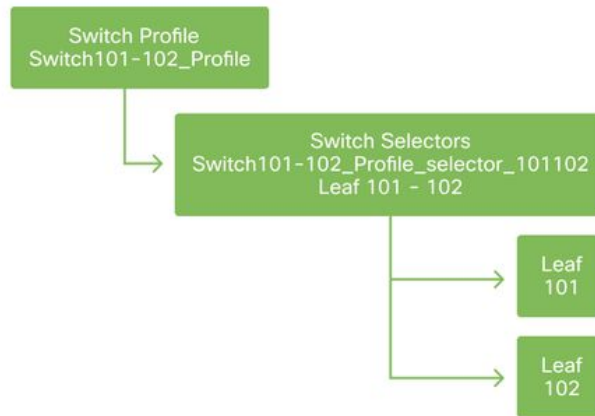


Un servidor web está conectado a un fabric ACI. El servidor web tiene 2 tarjetas de interfaz de red (NIC) configuradas en un canal de puerto LACP. El servidor web está conectado al puerto 1/9 de los switches de hoja 101 y 102. El servidor web depende de VLAN-1501 y debe residir en el EPG 'EPG-Web'.

Configuración de la política de switch

El primer paso lógico es definir qué switches de hoja se utilizarán. El 'perfil de switch' contendrá 'selectores de switch' que definen los ID de nodo de hoja que se utilizarán.

Políticas del switch



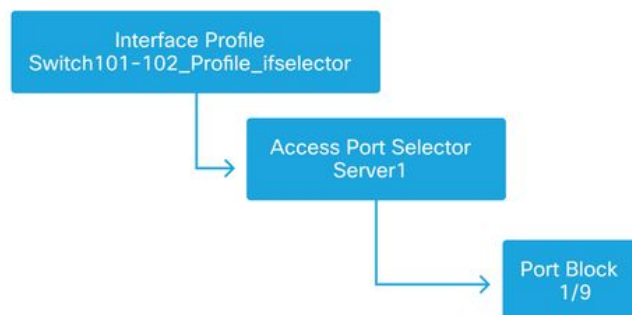
La recomendación general es configurar 1 perfil de switch por switch de hoja individual y 1 perfil de switch por par de dominios VPC, usando un esquema de nomenclatura que indique los nodos que forman parte del perfil.

El Inicio rápido implementa un esquema de nombres lógico que facilita la comprensión de dónde se aplica. El nombre completo sigue el formato 'Switch<node-id>_Profile'. Por ejemplo, 'Switch101_Profile' será para un perfil de switch que contenga el nodo de hoja 101 y Switch101-102_Profile para un perfil de switch que contenga los nodos de hoja 101 y 102 que deberían formar parte de un dominio VPC.

Configuración de la política de interfaz

Una vez creadas las políticas de acceso del switch, definir las interfaces sería el siguiente paso lógico. Esto se realiza mediante la creación de un 'Perfil de interfaz' que consta de 1 o más 'Selectores de puerto de acceso' que contienen las definiciones de 'Bloque de puerto'.

Políticas de interfaz



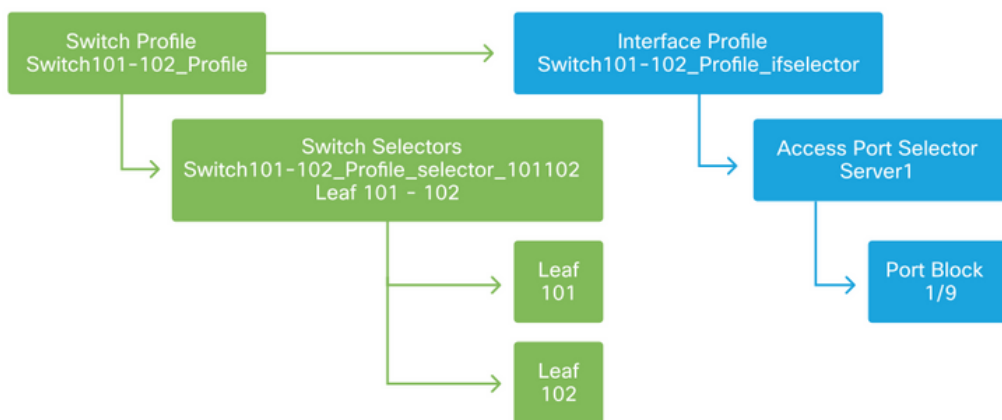
Para formar la relación entre el 'Perfil de interfaz' y los switches involucrados, vincule el 'Perfil de switch' al 'Perfil de interfaz'.

Los 'perfiles de interfaz' se pueden definir de muchas maneras. De forma similar a los 'perfiles de switch', se puede crear un solo 'perfil de interfaz' por switch físico junto con un 'perfil de interfaz' por dominio VPC. Estas políticas deberían tener una asignación 1 a 1 a su perfil de switch correspondiente. Siguiendo esta lógica, las políticas de acceso al fabric se simplifican en gran medida, lo que facilita la comprensión por parte de otros usuarios.

Aquí también se pueden utilizar los esquemas de nomenclatura predeterminados que emplea el Inicio rápido. Sigue el formato '<switch profile name>_ifselector' para indicar que este perfil se

utiliza para seleccionar interfaces. Un ejemplo sería 'Switch101_Profile_ifselector'. Este ejemplo 'Perfil de interfaz' se utilizaría para configurar interfaces no VPC en el switch de hoja 101 y sólo se asociaría a la política de acceso 'Switch101_Profile'.

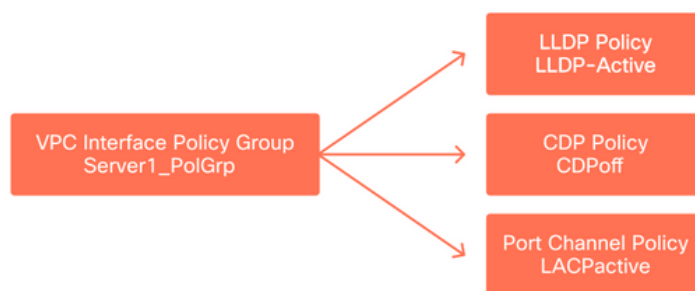
Perfil de switch asociado al perfil de interfaz



Observe que como un 'Perfil de interfaz' con Eth 1/9 está conectado a un 'Perfil de switch' que incluye el switch de hoja 101 y 102, el aprovisionamiento de Eth1/9 en ambos nodos comienza simultáneamente.

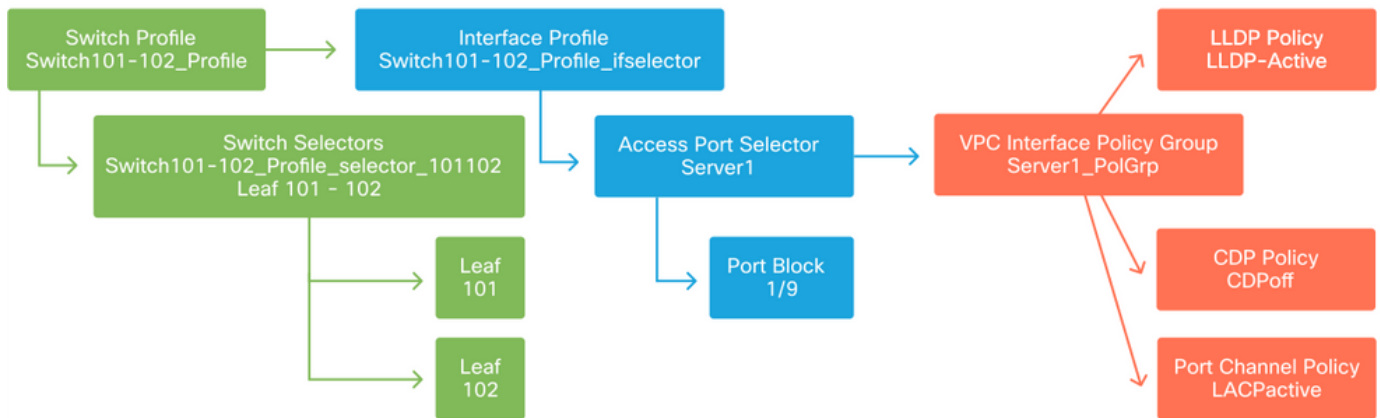
En este punto, se han definido los switches de hoja y sus puertos. El siguiente paso lógico sería definir las características de estos puertos. El 'Grupo de políticas de interfaz' permite la definición de estas propiedades de puerto. Se creará un 'Grupo de políticas de interfaz VPC' para permitir el canal de puerto LACP anterior.

Grupo de políticas



El 'Grupo de políticas de interfaz VPC' se asocia al 'Grupo de políticas de interfaz' desde el 'Selector de puertos de acceso' para formar la relación entre las propiedades del puerto y el switch de hoja y la interfaz.

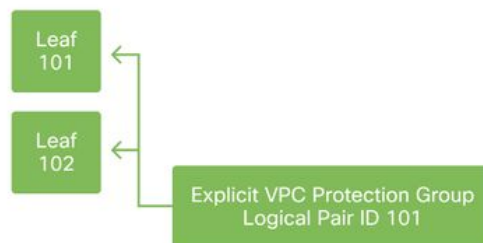
Switch y perfiles de interfaz combinados



Configuración de VPC

Para crear el canal de puerto LACP en 2 switches de hoja, se debe definir un dominio VPC entre el switch de hoja 101 y 102. Esto se hace definiendo un 'Grupo de protección VPC' entre los dos switches de hoja.

VPC



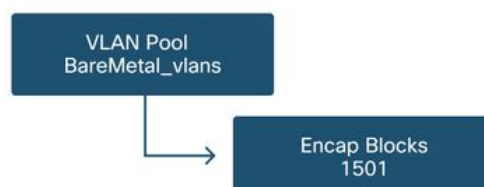
Configurar grupos de VLAN

El siguiente paso lógico será crear las VLAN que se utilizarán en este puerto, en este caso VLAN-1501. La definición de un 'VLAN Pool' con 'Encap Blocks' completa esta configuración.

Al considerar el tamaño de los rangos de grupos de VLAN, tenga en cuenta que la mayoría de las implementaciones solo necesitan un único grupo de VLAN y un grupo adicional si se usa la integración de VMM. Para incorporar VLAN de una red antigua a ACI, defina el rango de VLAN heredadas como un conjunto de VLAN estáticas.

Como ejemplo, supongamos que las VLAN 1-2000 se utilizan en un entorno heredado. Cree un conjunto de VLAN estáticas que contenga las VLAN 1-2000. Esto permitirá vincular los dominios de puente de ACI y los EPG al fabric heredado. Si implementa VMM, se puede crear un segundo grupo dinámico mediante un intervalo de ID de VLAN libres.

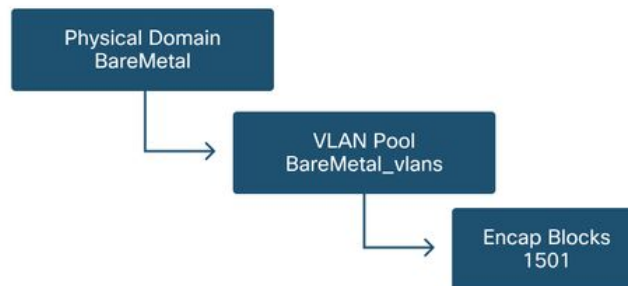
Conjunto VLAN



Configurar dominios

El siguiente paso lógico es crear un 'Dominio'. Un 'Dominio' define el alcance de un conjunto de VLAN, es decir, dónde se aplicará ese conjunto. Un 'dominio' puede ser físico, virtual o externo (puenteado o enrutado). En este ejemplo, se utilizará un 'dominio físico' para conectar un servidor físico al fabric. Este 'dominio' se asocia al 'conjunto de VLAN' para permitir las vlan necesarias.

Dominios físicos



Para la mayoría de las implementaciones, un solo "dominio físico" es suficiente para implementaciones de hardware físico y un solo "dominio enrutado" es suficiente para implementaciones L3Out. Ambos pueden asignarse al mismo 'VLAN Pool'. Si el fabric se implementa de forma de varios arrendatarios o si se requiere un control más granular para restringir los usuarios que pueden implementar EPG y VLAN específicos en un puerto, debe considerarse un diseño de política de acceso más estratégico.

'Dominios' también proporciona la funcionalidad para restringir el acceso del usuario a la política con 'Dominios de seguridad' mediante el control de acceso basado en roles (RBAC).

Al implementar las VLAN en un switch, ACI encapsulará las BPDU del árbol de expansión con un ID de VXLAN único que se basa en el dominio del que proviene la VLAN. Debido a esto, es importante utilizar el mismo dominio siempre que se conecten dispositivos que requieran comunicación STP con otros puentes.

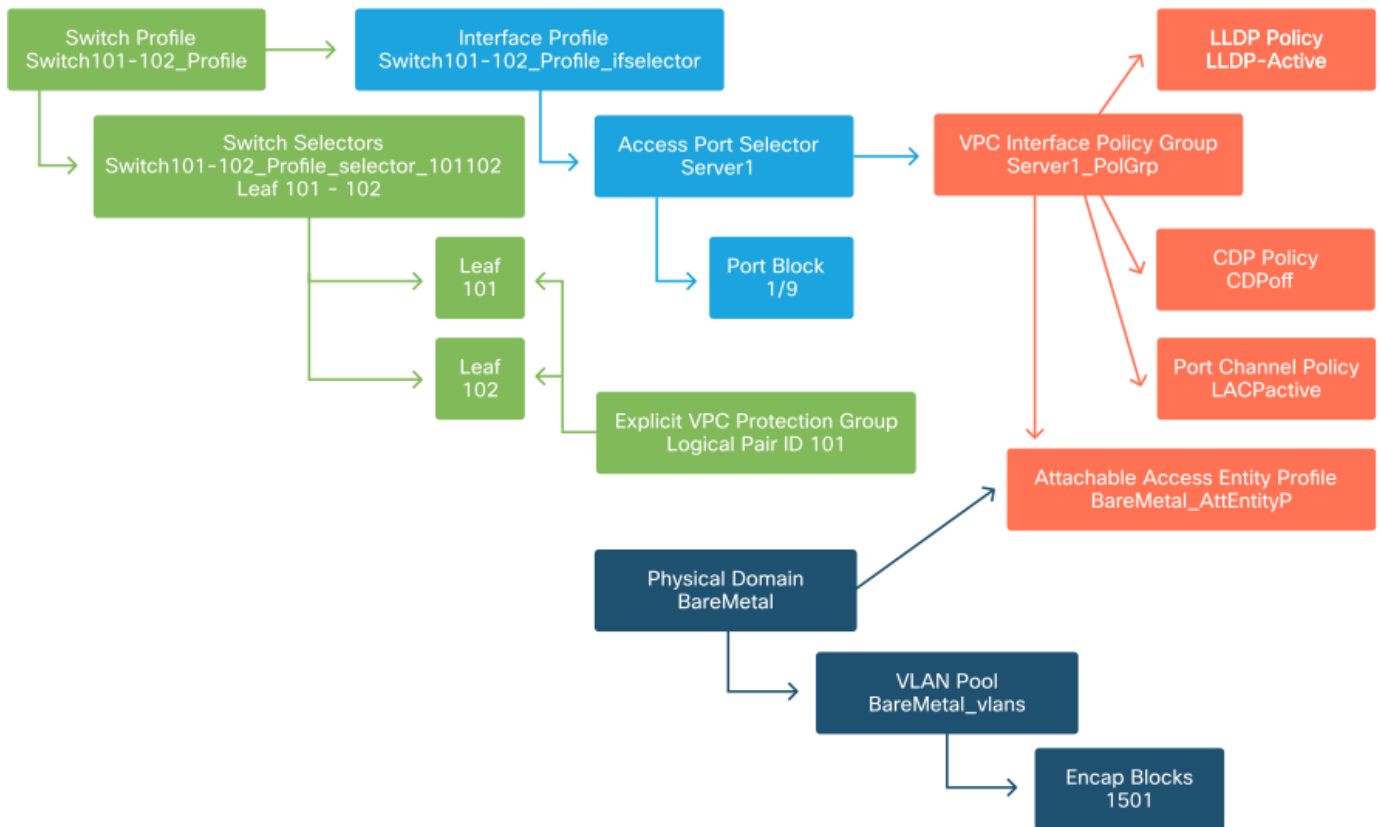
Las ID de VLAN VXLAN también se utilizan para permitir que los switches VPC sincronicen las direcciones MAC e IP adquiridas de VPC. Debido a esto, el diseño más simple para los grupos de VLAN es utilizar un único grupo para las implementaciones estáticas y crear un segundo grupo para las implementaciones dinámicas.

Configuración del perfil de entidad de acceso (AEP) adjuntable

Ya se han completado dos partes principales de la configuración de la política de acceso; las definiciones de switch e interfaz, y las definiciones de dominio/VLAN. Un objeto denominado "perfil de entidad de acceso adjuntable" (AEP) servirá para unir estos dos fragmentos.

Un 'grupo de políticas' está vinculado a un AEP en una relación de uno a varios que permite que el AEP agrupe interfaces y switches que comparten requisitos de políticas similares. Esto significa que sólo se necesita hacer referencia a un AEP cuando se representa un grupo de interfaces en switches específicos.

Perfil de entidad de acceso adjuntable



En la mayoría de las implementaciones, se debe utilizar un solo AEP para las rutas estáticas y un AEP adicional por dominio VMM.

La consideración más importante es que las VLAN se pueden implementar en interfaces a través del AEP. Esto se puede hacer asignando EPG a un AEP directamente o configurando un dominio VMM para el preaprovisionamiento. Ambas configuraciones convierten la interfaz asociada en un puerto troncal ('switchport mode trunk' en switches heredados).

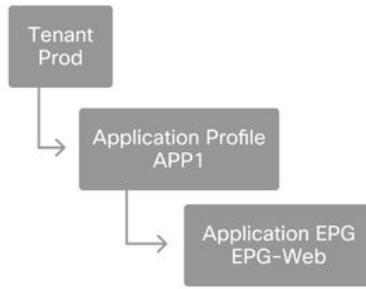
Debido a esto, es importante crear un AEP separado para L3Out cuando se utilizan puertos ruteados o subinterfaces ruteadas. Si se utilizan SVI en L3Out, no es necesario crear un AEP adicional.

Configuración del arrendatario, APP y EPG

ACI utiliza un medio diferente de definir la conectividad mediante un enfoque basado en políticas.

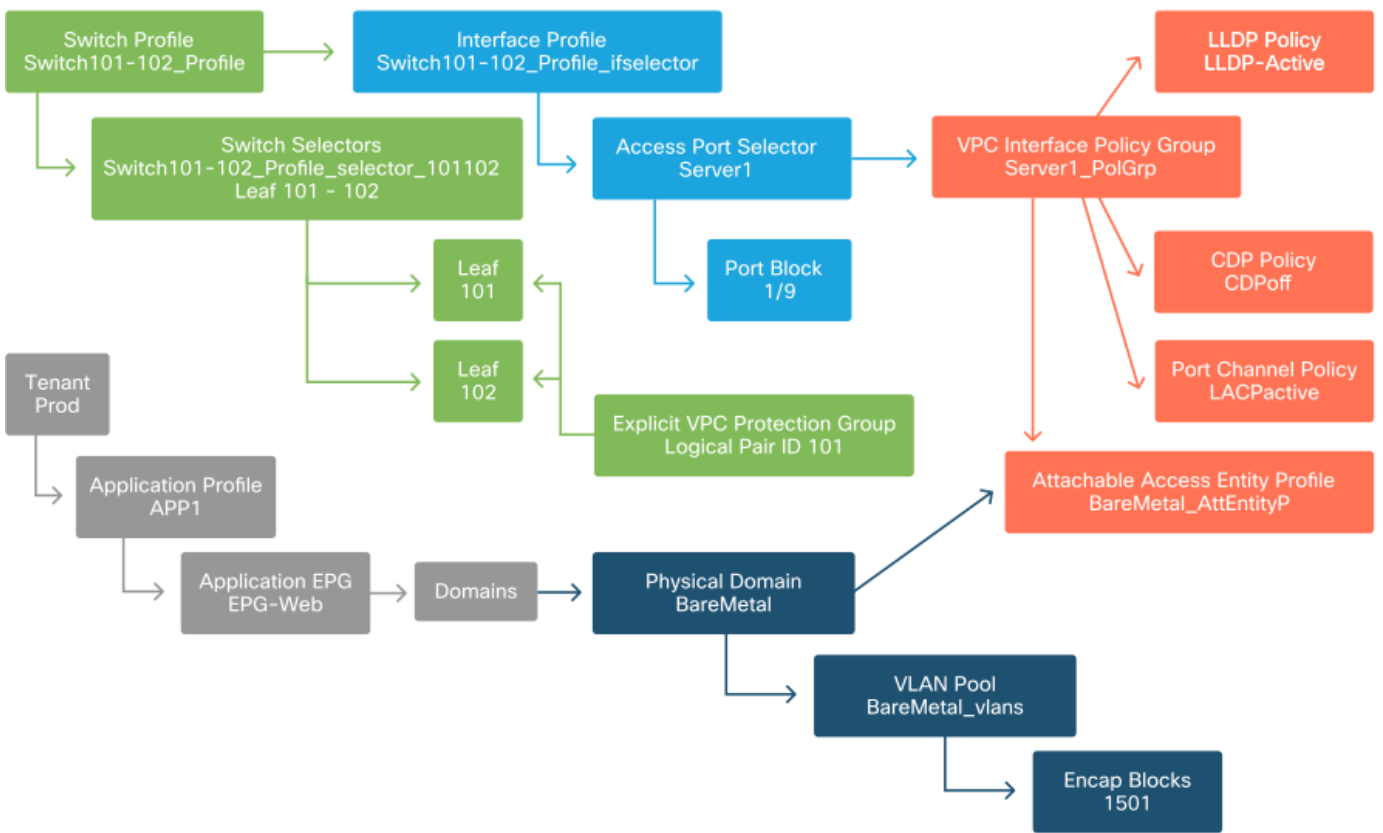
El objeto de nivel más bajo se denomina 'Grupo de terminales' (EPG). La construcción EPG se utiliza para definir un grupo de VM o servidores (terminales) con requisitos de políticas similares. Los 'perfiles de aplicación', que existen bajo un arrendatario, se utilizan para agrupar de forma lógica los EPG.

Arrendatario, APP y EPG



El siguiente paso lógico es vincular el EPG al dominio. Esto crea el enlace entre el objeto lógico que representa nuestra carga de trabajo, el EPG y los switches/interfases físicos, las políticas de acceso.

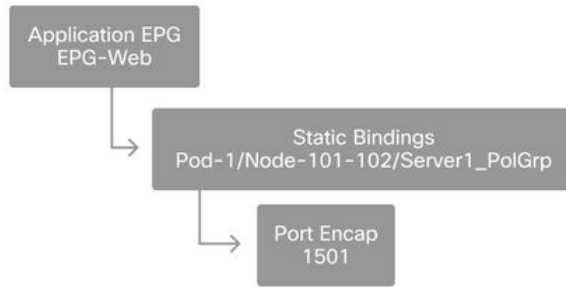
Enlace EPG a dominio



Configuración de los enlaces estáticos de EPG

El último paso lógico es programar la VLAN en una interfaz de switch para un EPG determinado. Esto es especialmente importante si se utiliza un dominio físico, ya que este tipo de dominio requiere una declaración explícita para hacerlo. Esto permitirá que el EPG se extienda fuera del fabric y que el servidor de metal desnudo se clasifique en el EPG.

Enlaces estáticos

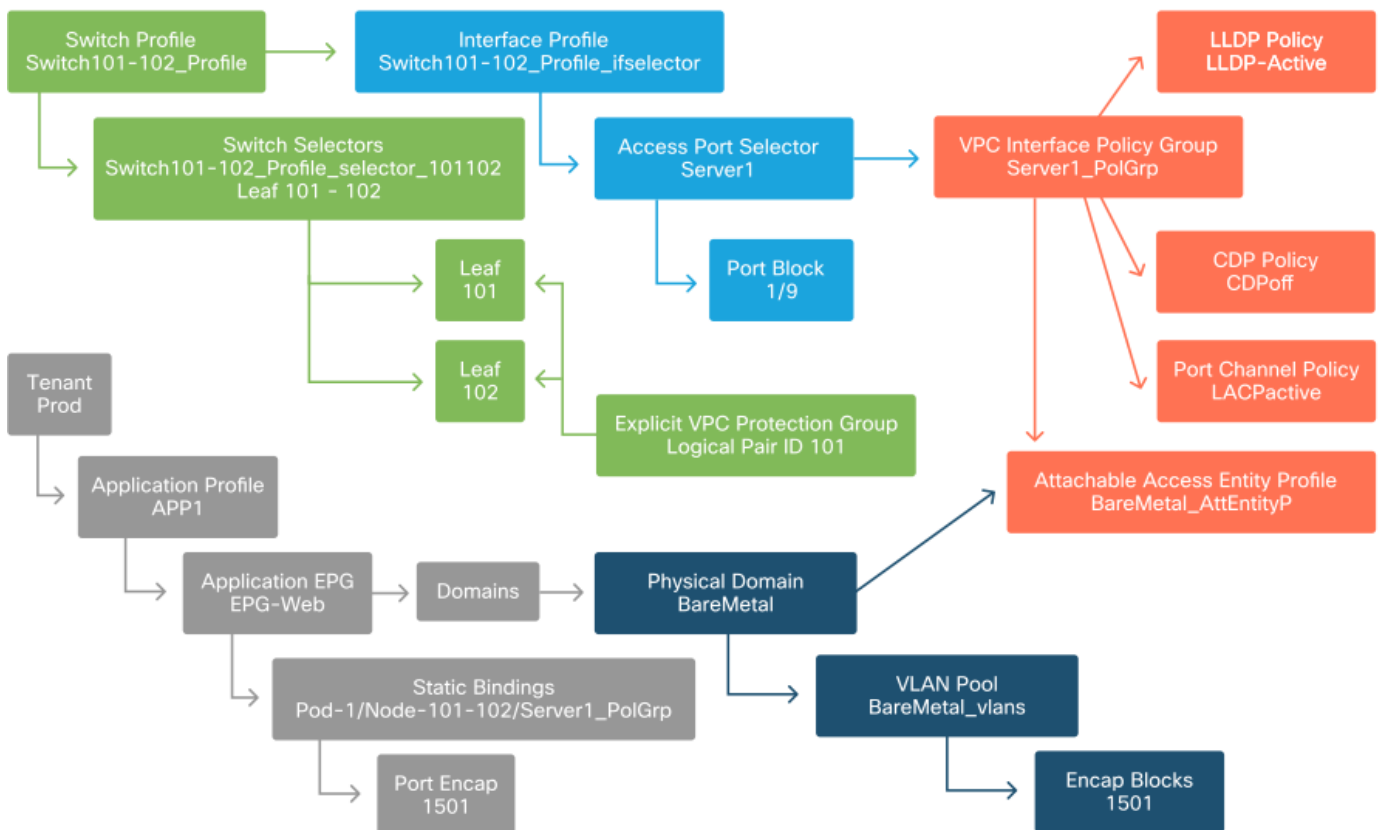


El 'Port Encap' al que se hace referencia debe poder resolverse contra el 'VLAN Pool'. Si no es así, se marcará un fallo. Esto se trata en la sección "Flujo de trabajo de solución de problemas" de este capítulo.

Resumen de la configuración de la política de acceso

El siguiente diagrama resume todos los objetos creados para permitir la conectividad para el host a través de VLAN-1501, utilizando una conexión VPC con el switch de hoja 101 y 102.

Conectividad ACI sin software específico



Conexión de servidores adicionales

Con todas las políticas anteriores creadas, ¿qué significaría conectar un servidor más en el puerto Eth1/10 en los switches de hoja 101 y 102 con un canal de puerto?

En relación con el diagrama "Conectividad ACI sin software específico", deberá crearse lo siguiente como mínimo:

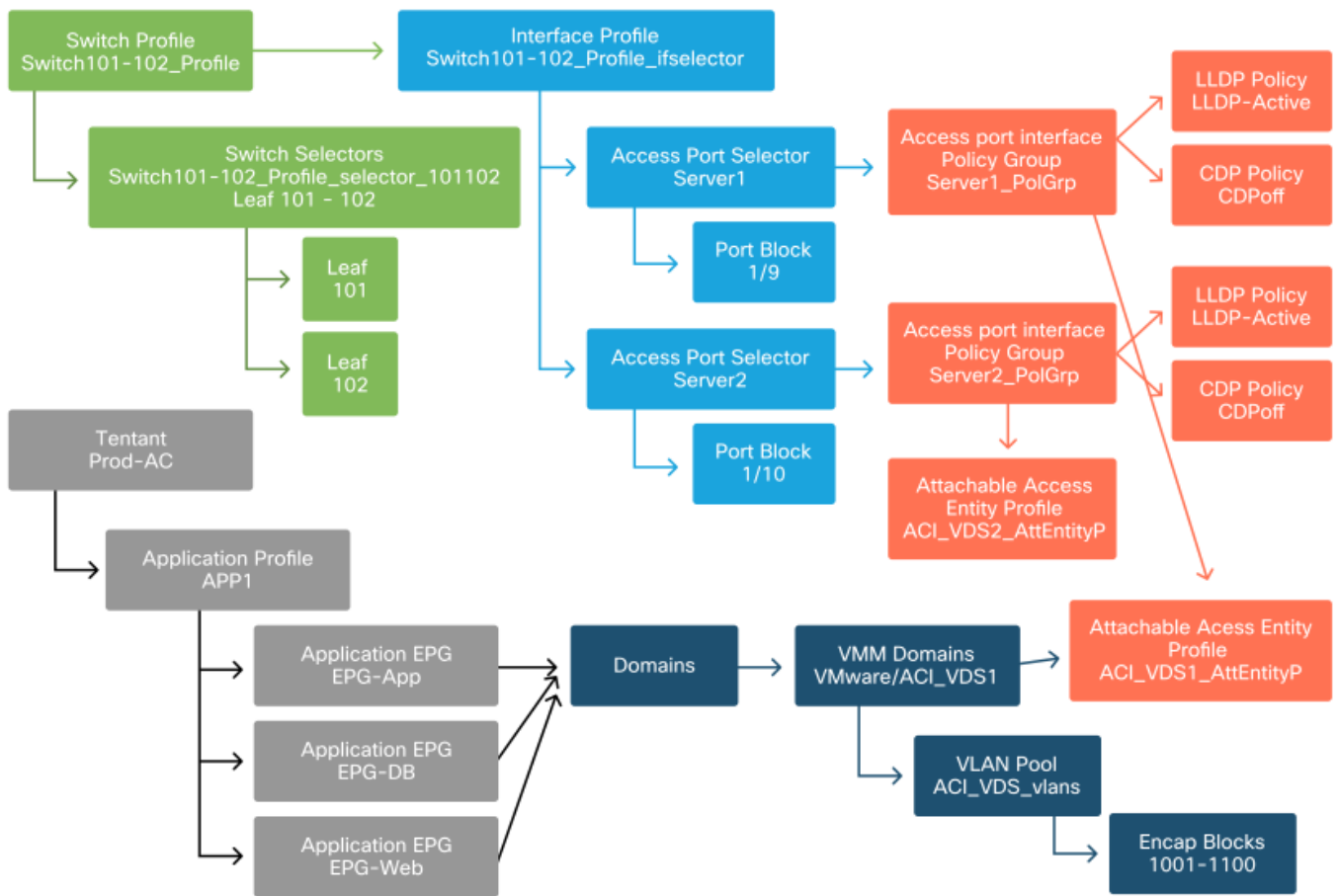
- Un selector de puerto de acceso y bloque de puertos adicionales.
- Un grupo de políticas de interfaz VPC adicional.
- Un enlace estático adicional con Port Encap.

Tenga en cuenta que para los canales de puerto LACP, se debe utilizar un grupo de políticas de interfaz VPC dedicado, ya que este grupo de políticas VPC es lo que define la ID de VPC.

En el caso de links individuales, el grupo de políticas de interfaz no VPC podría reutilizarse para el servidor adicional si el link requiere las mismas propiedades de puerto.

Las políticas resultantes se parecerían a la siguiente imagen.

Conexión del servidor 2 a la configuración



¿Qué sigue?

En la siguiente sección se abordarán algunos escenarios de fallos de políticas de acceso, empezando por la topología y el caso práctico que se describe en esta descripción general.

Flujo de resolución de problemas

Al trabajar con directivas de acceso, se pueden encontrar los siguientes escenarios de solución de problemas:

- Falta una relación entre dos o más entidades de la política de acceso, como un grupo de políticas de acceso no vinculado a un AEP.

- Una política inesperada o que falta está vinculada a una política de acceso determinada, como una política LLDP denominada 'lldp_enabled', mientras que en realidad la configuración de la política tiene LLDP rx/tx deshabilitado.
- Un valor ausente o inesperado en la política de acceso, como la encapsulación de ID de VLAN configurada que falta en el conjunto de VLAN configurado.
- Falta una relación entre el EPG y la política de acceso, como la ausencia de asociación de dominio físico o virtual con el EPG.

La mayor parte de la solución de problemas anterior implica recorrer las relaciones de las políticas de acceso para comprender si faltan relaciones, o para comprender qué políticas se configuran y/o si la configuración está dando como resultado el comportamiento deseado.

Uso de "Configuración de la interfaz, el PC y VPC Quick Start" para la resolución de problemas

En la GUI de APIC, el asistente de inicio rápido "Configurar interfaz, PC y VPC" facilita la búsqueda de políticas de acceso al proporcionar al administrador una vista agregada de las políticas de acceso existentes. Este asistente de inicio rápido se encuentra en la GUI en:

'Fabric > Políticas de acceso > Inicio rápido > Pasos > Configurar interfaz, PC y VPC'.

Inicio rápido de la ubicación de 'Configurar interfaz, PC y VPC'

The screenshot shows the APIC GUI interface. At the top, the 'Fabric' tab is selected in the navigation bar. Below it, the 'Access Policies' section is active. On the left, a sidebar menu lists various policy categories, with 'Quick Start' highlighted. The main content area displays a 'Quick Start' guide for 'Configure an interface, PC, and VPC'. The guide is divided into three columns: 'Summary', 'Steps', and 'See Also'. The 'Steps' column lists several tasks, with 'Configure an interface, PC, and VPC' highlighted by a red box. The 'See Also' column lists related configuration topics like 'Physical Interface (Link Level)', 'CDP', 'LLDP', 'LACP', 'LACP Member', 'Spanning Tree Interface', 'Storm Control', 'Port Security', 'SPAN', 'On-demand Diagnostics', 'Attachable Entity Profile', 'QoS', and 'DHCP Relay'.

Aunque el asistente tiene 'Configurar' en el nombre, es excepcionalmente útil para proporcionar una vista agregada de las muchas políticas de acceso que se deben configurar para obtener interfaces programadas. Esta agregación sirve como una vista única para comprender qué políticas ya están definidas y reduce de forma eficaz el número de clics necesarios para comenzar a aislar los problemas relacionados con las políticas de acceso.

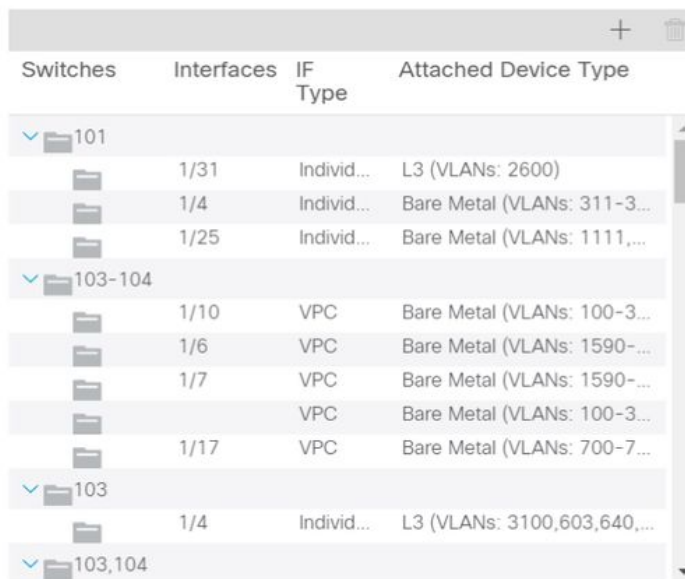
Cuando se carga la vista Inicio rápido, se puede hacer referencia a la vista 'Interfaces de switch configuradas' (panel superior izquierdo) para determinar las directivas de acceso existentes. El asistente agrupa las entradas debajo de las carpetas que representan switches de hoja individuales o múltiples, según la configuración de las políticas de acceso.

Como demostración del valor del asistente, se presentan las siguientes capturas de pantalla del asistente, sabiendo que el lector no tiene conocimientos previos de la topología del fabric:

Vista de demostración del Inicio rápido "Configurar interfaz, PC y VPC"

Configure Interface, PC, and VPC

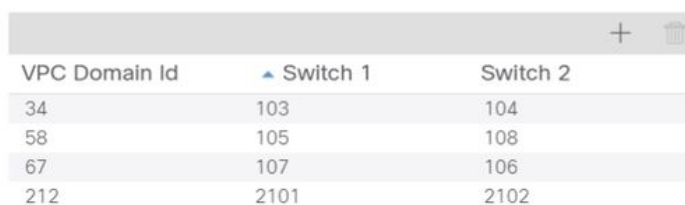
Configured Switch Interfaces



Switches	Interfaces	IF Type	Attached Device Type
101	1/31	Individ...	L3 (VLANs: 2600)
101	1/4	Individ...	Bare Metal (VLANs: 311-3...)
101	1/25	Individ...	Bare Metal (VLANs: 1111,...
103-104	1/10	VPC	Bare Metal (VLANs: 100-3...)
103-104	1/6	VPC	Bare Metal (VLANs: 1590-...)
103-104	1/7	VPC	Bare Metal (VLANs: 1590-...)
103-104		VPC	Bare Metal (VLANs: 100-3...)
103-104	1/17	VPC	Bare Metal (VLANs: 700-7...)
103	1/4	Individ...	L3 (VLANs: 3100,603,640,...
103,104			



VPC Switch Pairs



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

El panel 'Interfaces de switch configuradas' muestra las asignaciones de políticas de acceso. El panel "Pares de switches VPC" muestra las definiciones de grupos de protección VPC completados.

La siguiente tabla muestra un subconjunto de definiciones de políticas de acceso completadas que se pueden derivar de la captura de pantalla anterior.

Subconjunto de directivas de acceso completadas que se pueden derivar de la vista Inicio rápido anterior

Nodo de switch	Interfaz	Tipo de grupo de políticas	Tipo de dominio	VLAN
101	1/31	Individual	Enrutado (L3)	2600
101	1/4	Individual	Phys (metal desnudo)	¿311-3...?

103-104	1/10	VPC	Phys (metal desnudo)	¿100-3...?
---------	------	-----	----------------------	------------

Las entradas de la columna VLAN están intencionalmente incompletas dada la vista predeterminada.

Del mismo modo, las políticas de 'Grupo de protección VPC' completadas se pueden obtener de la vista 'Pares de switches VPC' (panel inferior izquierdo). Sin los "grupos de protección VPC", no se pueden implementar VPC, ya que esta es la política que define el dominio VPC entre dos nodos de hoja.

Tenga en cuenta que debido al tamaño del panel, las entradas largas no son completamente visibles. Para ver el valor total de cualquier entrada, coloque el puntero del ratón sobre el campo de interés.

El puntero del ratón está pasando el ratón sobre el campo 'Tipo de dispositivo conectado' para la entrada 103-104, int 1/10 VPC:

Configure Interface, PC, and VPC

Configured Switch Interfaces

Switches	Interfaces	IF Type	Attached Device Type
101	1/31	Individ...	L3 (VLANs: 2600)
	1/4	Individ...	Bare Metal (VLANs: 311-3...
	1/25	Individ...	Bare Metal (VLANs: 1111,...
103-104	1/10	VPC	Bare Metal (VLANs: 100-300,900-999), L3 (VLANs: 100-300,900-999)
	1/6	VPC	Bare Metal (VLANs: 1590-...
	1/7	VPC	Bare Metal (VLANs: 1590-...
		VPC	Bare Metal (VLANs: 100-3...
	1/17	VPC	Bare Metal (VLANs: 700-7...
103	1/4	Individ...	L3 (VLANs: 3100,603,640,...
103,104			

VPC Switch Pairs

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

Al pasar el ratón sobre el panel, se pueden ver todas las entradas.

Subconjunto actualizado de directivas de acceso completadas mediante los detalles del mouse (ratón)

Nodo de switch	Interfaz	Tipo de grupo de políticas	Tipo de dominio	VLAN
101	1/31	Individual	Enrutado (L3)	2600

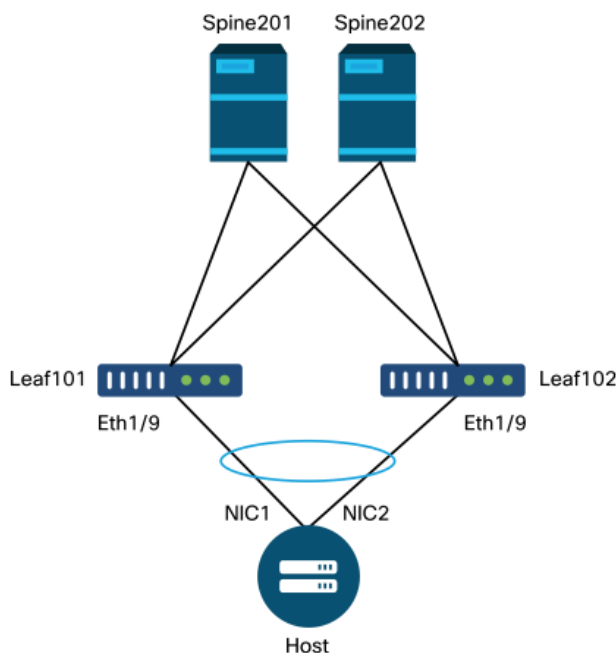
101	1/4	Individual	Phys (metal desnudo)	311-320
103-104	1/10	VPC	Phys (metal desnudo)	100-300,900-999
103-104	1/10	VPC	Enrutado (L3)	100-300,900-999

Ahora se pueden observar y comprender las asociaciones VLAN completas para la resolución de problemas y la verificación.

Escenarios de resolución de problemas

Para los siguientes escenarios de troubleshooting, consulte la misma topología del capítulo anterior.

Topología de la sección "Introducción" de la política de acceso



Escenario 1: Fault F0467 — invalid-path, nwissues

Este fallo se produce cuando se realiza una declaración de switch/puerto/VLAN sin las políticas de acceso correspondientes en vigor para permitir que esa configuración se aplique correctamente. Dependiendo de la descripción de este fallo, puede que falte un elemento diferente de la relación de política de acceso.

Después de implementar un enlace estático para la interfaz VPC anterior con VLAN 1501 de encapsulación troncal sin la relación de política de acceso correspondiente en su lugar, se genera el siguiente error en el EPG:

Error: F0467

Descripción: Delegado de errores: Error de configuración para uni/tn-Prod1/ap-App1/epg-EPG-

Web node 101 101_102_eth1_9 debido a una configuración de ruta no válida, configuración de VLAN no válida, mensaje de depuración: invalid-vlan: vlan-1501 :La ID de segmento STP no está presente para Encap. El EPG no está asociado con un dominio o el dominio no tiene esta vlan asignada;invalid-path: vlan-1501: No hay ningún dominio, asociado tanto con EPG como con Port, que haya requerido VLAN;

A partir de la descripción de la falla anterior, hay algunas indicaciones claras en cuanto a lo que podría estar causando que se active la falla. Hay una advertencia para verificar las relaciones de política de acceso, así como para verificar la asociación de dominio al EPG.

Al revisar la vista Inicio rápido en el escenario descrito anteriormente, está claro que a la política de acceso le faltan VLAN.

Vista de inicio rápido donde 101-102, VPC Int 1/9 carece de VLAN

Configure Interface, PC, and VPC

Configured Switch Interfaces

Switches	Interfaces	IF Type	Attached Device Type
101-102	1/11	Individual	ESX (VLANs: 1001-1100)
101-102	1/9	VPC	Bare Metal
101	1/17	Individual	L3 (VLANs: 901-910)
102	1/19	Individual	L3 (VLANs: 901-910)
301-302	1/11	Individual	ESX (VLANs: 1001-1100)
301	1/17	Individual	L3 (VLANs: 901-910)
302	1/19	Individual	L3 (VLANs: 901-910)



VPC Switch Pairs

VPC Domain Id	Switch 1	Switch 2
101	101	102

Observe que a la entrada le falta una referencia a cualquier ID de VLAN.

Una vez corregida, la vista Inicio rápido mostrará '(VLAN 1500-1510)'.

101-102, VPC Int 1/9 ahora muestra metal desnudo (VLAN: 1500-1510)

Configure Interface, PC, and VPC

Configured Switch Interfaces

Switches	Interfaces	IF Type	Attached Device Type
101-1...	1/11	Individual	ESX (VLANs: 1001-1100)
	1/9	VPC	Bare Metal (VLANs: 1500...
101	1/17	Individual	L3 (VLANs: 901-910)
102	1/19	Individual	L3 (VLANs: 901-910)
301-3...	1/11	Individual	ESX (VLANs: 1001-1100)
301	1/17	Individual	L3 (VLANs: 901-910)
302	1/19	Individual	L3 (VLANs: 901-910)



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



Bare Metal (VLANs: 1500-1510)

VPC Switch Pairs

VPC Domain Id	Switch 1	Switch 2
101	101	102

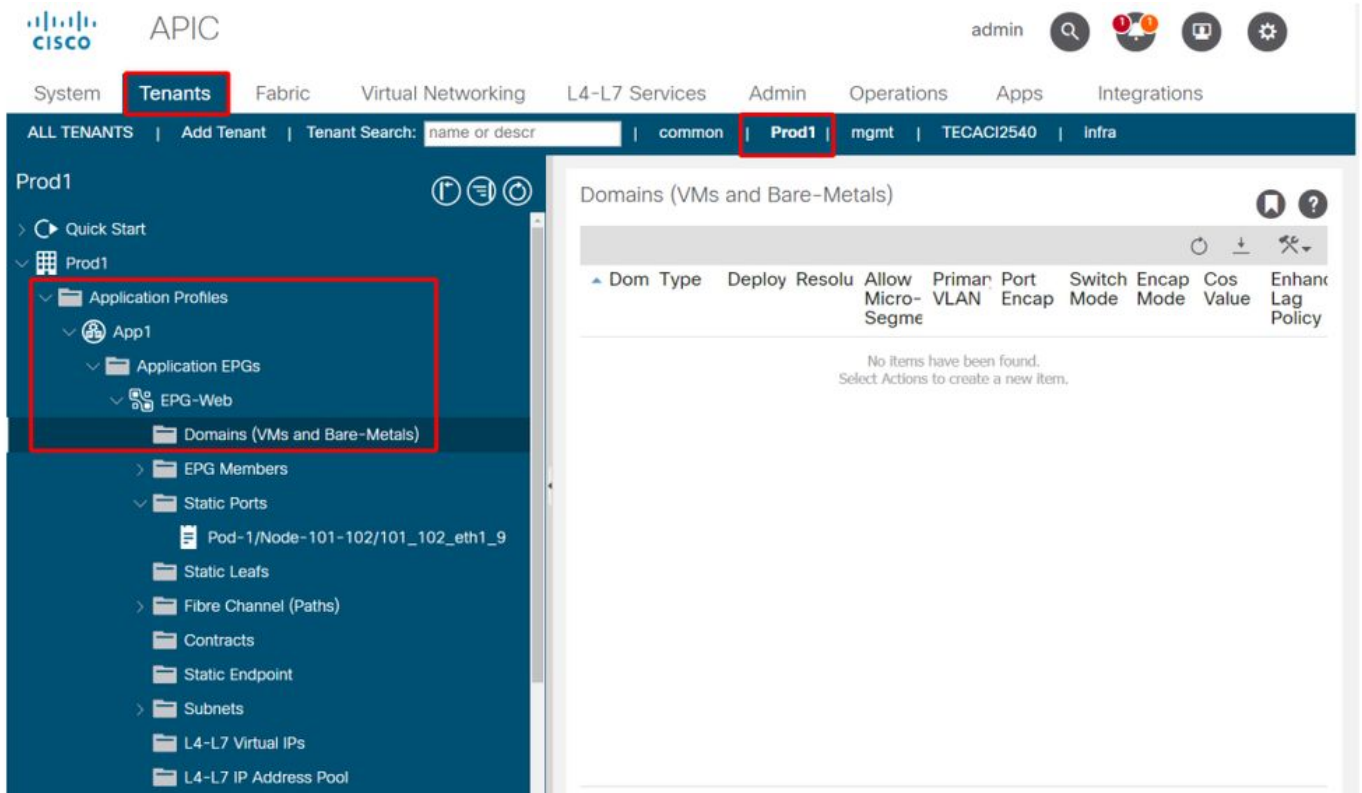
Sin embargo, el error de EPG aún existe con la siguiente descripción actualizada del error F0467:

Error: F0467

Descripción: Delegado de fallas: Error de configuración para uni/tn-Prod1/ap-App1/epg-EPG-Web node 101 101_102_eth1_9 debido a una configuración de ruta no válida, mensaje de depuración: invalid-path: vlan-150: No hay ningún dominio, asociado tanto con EPG como con el puerto, que haya requerido VLAN.

Con el error actualizado anterior, verifique las asociaciones de dominio EPG para encontrar que no hay dominios vinculados al EPG.

EPG-Web tiene una asociación de puertos estáticos, pero le faltan asociaciones de dominio



Una vez que el dominio que contiene la VLAN 1501 se asocia al EPG, no se generan más fallas.

Escenario 2: No se puede seleccionar VPC como ruta para implementar en el puerto estático EPG o en el perfil de interfaz lógica (SVI) L3Out

Mientras se intenta configurar un VPC como ruta en una entrada SVI de puerto estático EPG o perfil de interfaz lógica L3Out, el VPC específico que se va a implementar no se muestra como opción disponible.

Al intentar implementar un enlace estático VPC, hay dos requisitos de hardware:

1. El grupo de protección explícita de VPC debe definirse para el par de switches de hoja en cuestión.
2. Se debe definir la asignación de política de acceso completa.

Ambos requisitos se pueden comprobar en la vista Inicio rápido, como se muestra anteriormente. Si ninguno de los dos está completo, el VPC simplemente no aparecerá como una opción disponible para las vinculaciones de puertos estáticos.

Escenario 3: Fault F0467: encapsulado de fabric ya utilizado en otro EPG

De forma predeterminada, las VLAN tienen un alcance global. Esto significa que un ID de VLAN determinado solo se puede utilizar para un EPG único en un switch de hoja determinado. Cualquier intento de reutilizar la misma VLAN en varios EPG dentro de un switch de hoja dado resultará en el siguiente error:

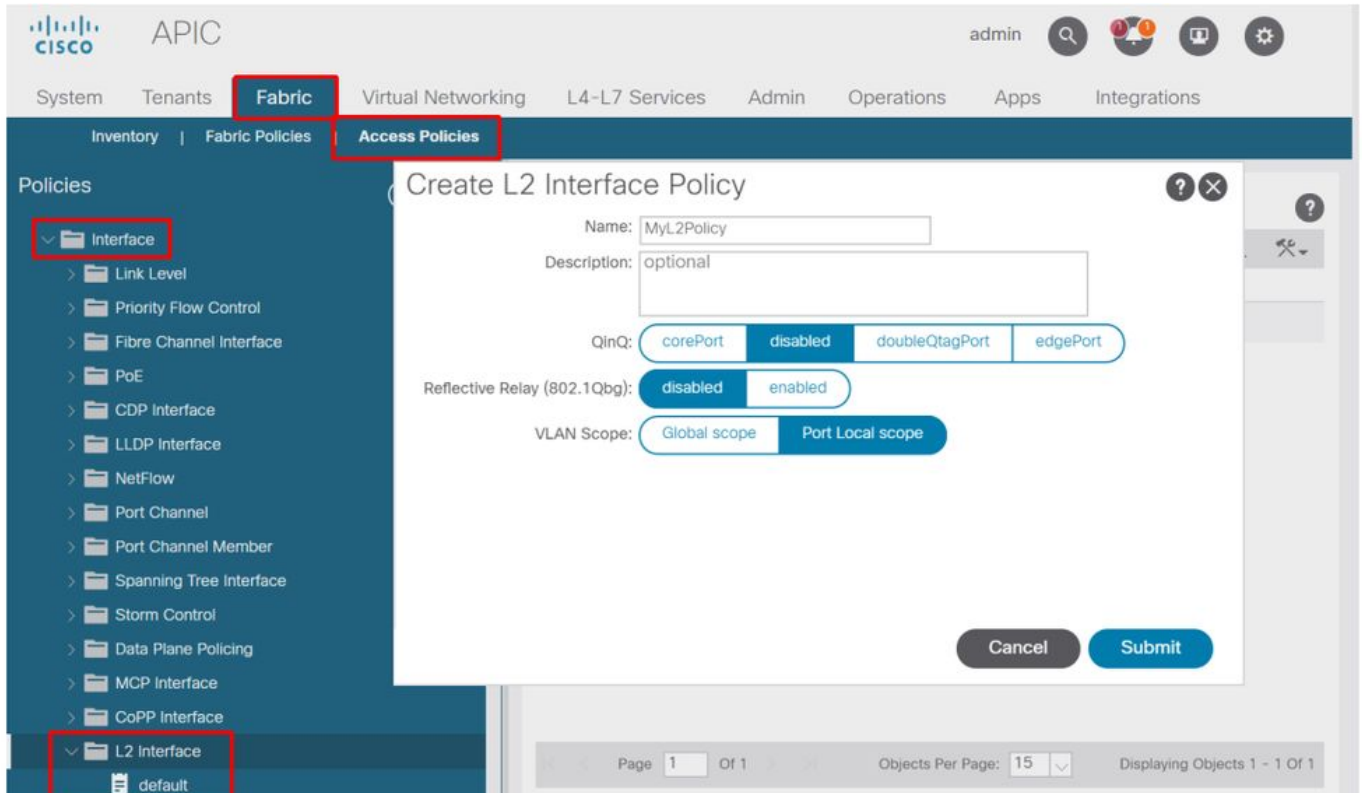
Error: F0467

Descripción: Delegado de fallas: Error de configuración para uni/tn-Prod1/ap-App1/epg-EPG-BusinessApp nodo 102 101_102_eth1_8 debido a Encap ya utilizado en otro EPG, mensaje de depuración: encap-already-in-use: Encap ya está en uso por Prod1:App1:EPG-Web;

Además de seleccionar una VLAN diferente, otra opción para hacer que esta configuración funcione es considerar el uso del alcance de VLAN 'Port Local'. Este alcance permite que las VLAN se mapeen por interfaz, lo que significa que VLAN-1501 podría utilizarse potencialmente para diferentes EPG, a través de múltiples interfaces, en la misma hoja.

Aunque el ámbito 'Port Local' se asocia en función del grupo de políticas (específicamente a través de una política L2), se aplica en el nivel de hoja.

Ubicación para cambiar la configuración de "alcance de VLAN" en la GUI de APIC



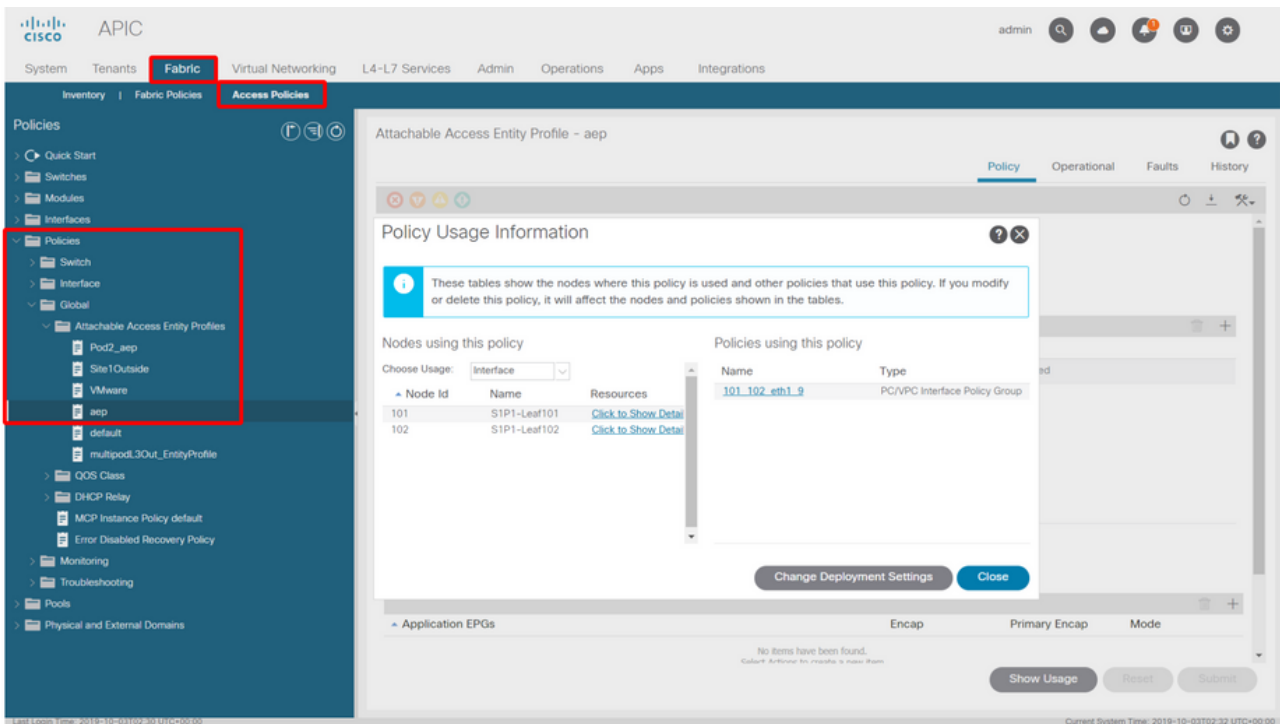
Antes de implementar la configuración de alcance de VLAN 'Port Local', consulte la "Guía de configuración de redes de capa 2 de Cisco APIC" en Cisco.com para asegurarse de que sus limitaciones y restricciones de diseño son aceptables para los diseños y casos prácticos deseados.

Menciones especiales

Mostrar uso

Aunque no es específico de las políticas de acceso, hay un botón disponible en la mayoría de los objetos de la GUI con la etiqueta 'Mostrar uso'. Este botón realiza una búsqueda de políticas basada en el objeto seleccionado para determinar qué nodos de hoja/interfaces tienen una relación directa con él. Esto puede ser útil tanto para el escenario de búsqueda general como para comprender si un objeto o una directiva específicos están siquiera en uso.

En la captura de pantalla siguiente, el AEP seleccionado está siendo utilizado por dos interfaces diferentes. Esto implica que realizar una modificación en el AEP tendrá un impacto directo en las interfaces asociadas.



Conjuntos de VLAN superpuestos

Aunque la función de las políticas de acceso es permitir que una VLAN específica se implemente en una interfaz, hay un uso adicional que debe considerarse durante la fase de diseño. Específicamente, el dominio se utiliza en el cálculo del ID de VXLAN (llamado Fabric Encap) vinculado a la encapsulación externa. Aunque esta funcionalidad generalmente no tiene ninguna relación importante con el tráfico del plano de datos, estos ID son especialmente relevantes para un subconjunto de protocolos que se inundan a través del fabric, incluidas las BPDUs del árbol de extensión. Si se espera que las VLAN-*<id>* BPDUs que ingresan en la hoja 1 salgan de la hoja 2 (por ejemplo, si hay switches heredados que convergen del árbol de expansión a través de ACI), la VLAN-*<id>* debe tener el mismo fabric encap en ambos nodos de hoja. Si el valor de encapsulamiento de la estructura difiere para las mismas VLAN de acceso, las BPDUs no atravesarán la estructura.

Como se mencionó en la sección anterior, evite la configuración de las mismas VLAN en varios dominios (VMM frente a físico, por ejemplo) a menos que se tenga especial cuidado para garantizar que cada dominio se aplique solamente a un conjunto único de switches de hoja. En el momento en que ambos dominios se pueden resolver en el mismo switch de hoja para una VLAN determinada, existe la posibilidad de que la VXLAN subyacente se pueda cambiar después de una actualización (o recarga limpia) lo que puede llevar, por ejemplo, a problemas de convergencia STP. El comportamiento es el resultado de que cada dominio tiene un valor numérico único (el atributo 'base') que se utiliza en la siguiente ecuación para determinar la ID de VXLAN:

$$\text{VXLAN VNID} = \text{Base} + (\text{encap} - \text{from_encap})$$

Para validar los dominios que se insertan en una hoja determinada, se puede ejecutar una query en la clase '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 de este resultado, distinga las siguientes definiciones de políticas de acceso:

- Hay un conjunto de VLAN programadas con un bloque de VLAN que definen explícitamente las VLAN 1500-1510.
- Este bloque de VLAN está vinculado a un dominio denominado 'physvlans'.
- El valor base utilizado en el cálculo de VXLAN es 8492.
- El cálculo de VXLAN resultante para VLAN-1501 sería $8492 + (1501-1500) = 8493$ como encapsulación de fabric.

El ID de VXLAN resultante (en este ejemplo, 8493) se puede verificar con el siguiente comando:

```
leaf# show system internal epm vlan all
```

VLAN ID	Type	Access Encap (Type Value)	Fabric Encap	H/W id	BD VLAN	Endpoint Count
13	Tenant BD	NONE	0 16121790	18	13	0
14	FD vlan	802.1Q	1501 8493	19	13	0

Si hay cualquier otro conjunto de VLAN que contenga VLAN-1501 que se inserte en la misma hoja, una actualización o recarga limpia podría potencialmente tomar un valor base único (y, posteriormente, un Fabric Encap diferente) que hará que las BPDU dejen de llegar a otra hoja que se espera reciba BPDU en VLAN-1501.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).