# 排除ACI訪問策略故障

# 目錄

簡介 背景資訊 訪問策略概述 訪問策略配置:方法 訪問策略手動基本配置 配置交換機策略 配置介面策略 配置VPC 配置<u>VLAN池</u> 配置域 配置可連線訪問實體配置檔案(AEP) <u>配置租戶、APP和EPG</u> <u>配置EPG靜</u>態繫結 訪問策略配置摘要 連線其他伺服器 <u>下一步是</u>什麼? 故障排除工作流 使用「配置介面、PC和VPC快速入門」進行故障排除 故障排除場景 案例 1:故障F0467 — 路徑無效,新問題 案例 2:無法選擇VPC作為在EPG靜態埠或L3Out邏輯介面配置檔案(SVI)上部署的路徑 案例 3:故障F0467 — 已在另一個EPG中使用交換矩陣封裝 特殊提及 顯示使用情況 重疊的VLAN池

# 簡介

本文檔介紹瞭解ACI訪問策略並對其進行故障排除的步驟。

# 背景資訊

本文檔中的資料摘自<u>疑難排解思科以應用為中心的基礎設施,第二版</u>書籍,具體而言是**訪問策略 —** 概述和訪問策略 — 故障排除工作流章節。

# 訪問策略概述

ACI管理員如何在交換矩陣中的埠上配置VLAN?ACI管理員如何開始解決與訪問策略相關的故障?本 節將介紹如何排除與交換矩陣訪問策略相關的問題。 在進入故障排除場景之前,讀者必須很好地瞭解訪問策略在ACI對象模型中的功能及其關係。為此 ,讀者可參閱Cisco.com(<u>https://developer.cisco.com/site/apic-mim-ref-api/</u>)上提供的「ACI策略模 型」和「APIC管理資訊模型參考」文檔。

接入策略的功能是在枝葉交換機的下行鏈路埠上啟用特定配置。在定義租戶策略以允許流量通過 ACI交換矩陣埠之前,應準備好相關訪問策略。

通常,在將新枝葉交換機新增到交換矩陣或將裝置連線到ACI枝葉下行鏈路時定義訪問策略;但是 ,根據環境的動態性,可以在交換矩陣的正常操作期間修改訪問策略。例如,允許一組新的 VLAN或將新的路由域新增到交換矩陣接入埠。

ACI訪問策略(雖然最初有點令人生畏)非常靈活,旨在簡化在持續發展過程中向大規模SDN網路 調配配置的過程。

#### 訪問策略配置:方法

訪問策略可以獨立配置,即通過獨立建立所需的所有對象,也可以通過ACI GUI提供的大量嚮導進 行定義。

嚮導非常有用,因為它們可以指導使用者完成工作流程,並確保所有必要的策略都到位。

#### 訪問策略 — 快速啟動嚮導

cisco	APIC						admin Q	0	<b>()</b> 🖸		Č.
System	Tenants	Fabric	Virtual Networking	L4-L7	7 Services	Admin	Operations	Apps	Integra	ations	
Inv	entory I Fal	bric Policies	Access Policies								
Policies	( Start	00	Quick Start								•
<ul> <li>Switche</li> <li>Module</li> <li>Interfac</li> <li>Policies</li> <li>Pools</li> <li>Physica</li> </ul>	es es al and External [	Domains	Summary Access policies gove operation of interface provide external acce the fabric. The syste provides default acce policies. Access polic enable configuring va functions or protocol Administrators who h fabric administrator privileges can create access policies acco to their requirements APIC enables administrators to sele pods, leaf switches, i interfaces to which ti apply access policies	ern the ess that ess to m sss cies arious s. new roling . The ect the and hey will a. a gure faces to a	Configure i access Configure o access Create a Cl policy Create a tra Configure a Quick confi Configure p	Step n-band manage but-of-band m DP (or other) in affic storm cor an interface, P igure port inter port security	DS gement nanagement nterface ntrol policy C, and VPC rface		See Al Physical Interfact Level) CDP LLDP LACP LACP Member Spanning Tree In Storm Control Port Security SPAN On-demand Diag Attachable Entity QoS DHCP Relay	ISO e (Link nterface gnostics / Profile	

上圖顯示了可以找到多個嚮導的「快速入門」頁。

定義訪問策略後,一般建議是通過確保所有關聯對象不顯示任何錯誤來驗證策略。

例如,在下圖中,交換機配置檔案分配了一個不存在的介面選擇器策略。細心的使用者可以很容易 地發現對象的「missing-target」狀態,並驗證是否已從GUI中標籤錯誤:

# 葉配置檔案 — SwitchProfile\_101

cisco	APIC					admin	٩	0	0		٢
System	Tenants Fabric	Virtual Networking	L4-L7 Services	Admin	Operations	Apps	Integ	rations			
Inve	ntory   Fabric Policies	Access Policies									
Policies	050	Leaf Profile - Switchl	Profile_101								0.6
> C Quick St	tart							Dollay	Eau	lte	History
~ 🚞 Switche	s							Policy	Fau	its	HISTORY
💛 🚞 Leaf	Switches	0 0 0 0								Ó	<u>+</u> **+
💛 🚞 P	rofiles	Properties									
Ē	SwitchProfile_101										^
=	SwitchProfile_101_102	Leaf Selectors	S:							10	+
=	SwitchProfile_102		<ul> <li>Name</li> </ul>	Block	s			P	olicy Gro	up	
-	SwitchProfile_301		101	101							
-	SwitchProfile_301_302										
Ē	SwitchProfile_302	•									
> 🥅 P	olicy Groups										
> 🚞 0	lverrides										
> 🚞 Spin	e Switches	Associated Interfac Selector Profiles	9 S:								+
> 🧮 Modules	5		Name	Desc	ription			S	tate	_	<u> </u>
> 🚞 Interface	es		Policy					n	nissing-ta	arget	
> 🚞 Policies			SwitchProfile_101	1				f	ormed		
> 🚞 Pools											
> 🚞 Physical	l and External Domains	¢									>
						Show	v Usage				

# 枝葉配置檔案 — SwitchProfile\_101 — 故障

cisco	APIC			admin	30	00
System	<sup>T</sup> Fault Prope	rties			000	Integrations
Invent	to		General	Troubleshooting	History	
Policies						0.0
> C Ouick Star	rt				0 ±	
	Fault Code:	F1014				Faults History
- Switches	Severity:	warning				
V Leaf St	Last Transition:	2019-10-28T11:23:11.665+00:0	0			0 +
V 🚞 Pro	Lifecycle:	Raised				Description
	S Affected Object:	uni/infra/nprof-SwitchProfile_10	01/rsaccPortP-[uni/infra/ac	cportprof-Policy]		Profile_101 Failed to form
	S Description: Type:	Failed to form relation to MO uni/ir Config	nfra/accportprof-Policy of cla	ss infraAccPortP		class infraAccl
E	S Cause:	resolution-failed				
E	S Change Set:	state (Old: formed, New: missing-	target)			
8	S Created:	2019-10-28T11:23:11.665+00:0	0			
	S Code:	F1014				
> 🚞 Poli	ic Number of Occurrences:	1				
> 🚞 Ove	en Original Severity:	warning				
> 🧮 Spine :	S Previous Severity:	warning				
> 🚞 Modules	Highest Severity:	warning				
> 🚞 Interfaces						
> 🚞 Policies		ĸ				,
> 🚞 Pools		Page 1 C	of 1	Objects Per Page: 15	~	Displaying Objects 1 - 1 Of 1

在這種情況下,糾正故障與建立名為「Policy」的新介面選擇器配置檔案一樣簡單。

基本訪問策略的手動配置將在以下段落中探討。

## 訪問策略手動基本配置

部署訪問策略時,將定義對象以表示給定下行鏈路的預期用途。對下行鏈路進行程式設計的宣告 (例如EPG靜態埠分配)依賴於此明示意圖。這有助於擴展配置並對相似的使用對象進行邏輯分組 ,例如專門連線到給定外部裝置的交換機或埠。

在本章的其餘部分參考以下拓撲。

#### 雙宿主伺服器訪問策略定義的拓撲



Web伺服器連線到ACI交換矩陣。Web伺服器具有在LACP埠通道中配置的2個網路介面卡(NIC)。 Web伺服器連線到枝葉交換機101和102的埠1/9。Web伺服器依賴於VLAN-1501,應位於EPG「 EPG-Web」中。

#### 配置交換機策略

第一個邏輯步驟是定義將使用的枝葉交換機。「交換機配置檔案」將包含「交換機選擇器」,這些 選擇器定義了要使用的枝葉節點ID。

#### 交換機策略



一般建議是使用指示配置檔案中的節點的命名方案,為每個枝葉交換機配置1個交換機配置檔案,每個VPC域對配置1個交換機配置檔案。

「快速入門」部署了一個邏輯命名方案,可以讓您輕鬆瞭解其應用於何處。完成的名稱採用「 Switch<node-id>\_Profile」格式。例如,「Switch101\_Profile」將用於包含枝葉節點101的交換機配 置檔案,以及包含應成為VPC域一部分的枝葉節點101和102的交換機配置檔案的Switch101-102\_Profile。

#### 配置介面策略

建立交換機訪問策略後,下一步的邏輯步驟是定義介面。這是通過建立「介面配置檔案」完成的 ,該配置檔案由1個或多個「訪問埠選擇器」組成,這些選擇器包含「埠塊」定義。

#### 介面策略



要建立「Interface Profile」與所涉及的交換機之間的關係,請將「Switch Profile」連結到「 Interface Profile」。

「Interface Profiles」可通過多種方式定義。與「Switch Profiles」類似,每台物理交換機可以建立 單個「Interface Profile」,每個VPC域也可以建立「Interface Profile」。然後,這些策略應有一個 1到1的對映來對映到其相應的交換機配置檔案。按照此邏輯,交換矩陣訪問策略得到極大簡化,讓 其他使用者更容易理解。

此處也可以使用快速入門使用的預設命名方案。它採用「<switch profile name>\_ifselector」格式 ,表示此配置檔案用於選擇介面。例如「Switch101\_Profile\_ifselector」。此示例「Interface Profile」將用於配置枝葉交換機101上的非VPC介面,並且它僅與「Switch101\_Profile」訪問策略相 關聯。

#### 與介面配置檔案關聯的交換機配置檔案



請注意,由於帶有Eth 1/9的「Interface Profile」連線到包含枝葉交換機101和102的「Switch Profile」,因此在兩個節點上同時開始調配Eth1/9。

此時,已定義枝葉交換機及其埠。下一個邏輯步驟是定義這些連線埠的特性。「介面策略組」允許 定義這些埠屬性。將建立「VPC介面策略組」以允許上述LACP埠通道。

#### 策略組



「VPC介面策略組」從「接入埠選擇器」與「介面策略組」相關聯,形成從枝葉交換機/介面到埠屬 性的關係。

#### 交換器與介面設定檔結合使用



#### 配置VPC

要在2台枝葉交換機上建立LACP埠通道,必須在枝葉交換機101和102之間定義VPC域。通過在兩台 枝葉交換機之間定義「VPC保護組」來完成此操作。



#### 配置VLAN池

下一個邏輯步驟是建立將在此連線埠上使用的VLAN(本例中為VLAN-1501)。使用「Encap Blocks」定義「VLAN池」即可完成此配置。

考慮VLAN池範圍大小時,請記住,如果使用VMM整合,大多數部署只需要一個VLAN池和一個附加 池。要將傳統VLAN從傳統網路引入ACI,請將傳統VLAN的範圍定義為靜態VLAN池。

例如,假設VLAN 1-2000用於傳統環境。建立一個包含VLAN 1-2000的靜態VLAN池。這將允許將 ACI網橋域和EPG中繼到傳統交換矩陣。如果部署VMM,可以使用一系列可用VLAN ID建立第二個 動態池。

#### VLAN池



#### 配置域

下一個邏輯步驟是建立「域」。「域」定義VLAN池的範圍,即該池將應用於何處。「域」可以是 物理、虛擬或外部(橋接或路由)。 在本示例中,將使用「物理域」將裸機伺服器連線到交換矩陣 。此「域」與「VLAN池」關聯以允許所需的VLAN。

#### 物理域



對於大多數部署,一個「物理域」就足以部署裸機,而一個「路由域」就足以部署L3Out。兩者都可以對映到相同的「VLAN池」。如果以多租戶方式部署交換矩陣,或者如果需要更精細的控制來限制哪些使用者可以在埠上部署特定EPG和VLAN,則應考慮更具戰略性的訪問策略設計。

「域」還提供使用基於角色的訪問控制(RBAC)通過「安全域」限制使用者訪問策略的功能。

在交換機上部署VLAN時,ACI將使用基於VLAN來源的域的唯一VXLAN ID封裝生成樹BPDU。因此 ,在連線需要與其他網橋進行STP通訊的裝置時,必須使用相同的域。

VLAN VXLAN ID也用於允許VPC交換機同步VPC學習的MAC和IP地址。因此,最簡單的VLAN池設 計是將單個池用於靜態部署並建立第二個池用於動態部署。

#### 配置可連線訪問實體配置檔案(AEP)

兩個主要訪問策略配置塊現已完成;交換機和介面定義以及域/VLAN定義。名為「可連線訪問實體 配置檔案」(Attachable Access Entity Profile)(AEP)的對象將用於將這兩個資料塊連線在一起。

「策略組」以一對多關係連結到AEP,這允許AEP將共用相似策略要求的介面和交換機組合在一起 。這意味著在表示特定交換機上的介面組時,只需要引用一個AEP。

#### 可附加訪問實體配置檔案



在大多數部署中,單個AEP應用於靜態路徑,每個VMM域一個額外的AEP。

最重要的考慮事項是可以通過AEP在介面上部署VLAN。這可以通過將EPG直接對映到AEP或配置 VMM域進行預調配來實現。這兩種配置都使關聯的介面成為中繼埠(舊版交換機上的「switchport mode trunk」)。

因此,當使用路由埠或路由子介面時,為L3Out建立單獨的AEP非常重要。如果在L3Out中使用 SVI,則無需建立其他AEP。

配置租戶、APP和EPG

最低級別的對象稱為「終端組」(EPG)。 EPG結構用於定義一組具有相似策略要求的VM或伺服器 (終端)。租戶下存在的「應用配置檔案」用於對EPG進行邏輯分組。

#### 租戶、應用和EPG



下一個邏輯步驟是將EPG連結到域。這樣會在代表我們的工作負載的邏輯對象EPG和物理交換機/介面、訪問策略之間建立鏈路。

#### EPG到域連結



#### 配置EPG靜態繫結

最後一個邏輯步驟是為給定EPG將VLAN程式設計到交換機介面上。如果使用物理域,這一點尤其 重要,因為此類域需要顯式宣告才能執行此操作。這將允許EPG從交換矩陣中擴展,並允許將裸機 伺服器分類到EPG中。

#### 靜態繫結



引用的「埠封裝」需要針對「VLAN池」進行解析。 如果不是,則標籤故障。本章的「故障排除工 作流程」一節對此進行了討論。

#### 訪問策略配置摘要

下圖彙總了建立的所有對象,這些對象用於通過VLAN-1501(使用VPC連線到枝葉交換機101和 102)連線主機。

#### 裸機ACI連線



#### 連線其他伺服器

建立所有先前的策略後,使用埠通道連線枝葉交換機101和102埠Eth1/10上的多台伺服器意味著什 麼?

參考「裸機ACI連線」圖,至少需要建立以下內容:

- •一個額外的接入埠選擇器和埠塊。
- 額外的VPC介面策略組。

•帶有埠封裝的額外靜態繫結。

請注意,對於LACP埠通道,必須使用專用VPC介面策略組,因為此VPC策略組是定義VPC ID的依 據。

在單個鏈路的情況下,如果鏈路要求相同的埠屬性,則可以將非VPC介面策略組重新用於額外的伺 服器。

生成的策略將如下圖所示。

#### 將server2連線到安裝程式



#### 下一步是什麼?

下一節將介紹幾個訪問策略故障場景,從本概述中討論的拓撲和使用案例開始。

# 故障排除工作流

使用訪問策略時可能會遇到以下故障排除場景:

- •訪問策略中兩個或多個實體之間缺少關係,例如未連結到AEP的訪問策略組。
- •缺少或意外的策略與給定的訪問策略(例如名為「lldp\_enabled」的LLDP策略)關聯,而實際 上策略配置已禁用LLDP rx/tx。
- ●訪問策略中缺少或意外的值,例如配置的VLAN池中缺少配置的VLAN ⅠD封裝。
- EPG和訪問策略之間缺少關係,例如沒有與EPG的物理或虛擬域關聯。

上述故障排除大多涉及遍歷訪問策略關係,以瞭解是否缺少任何關係、瞭解配置了哪些策略和/或配

## 使用「配置介面、PC和VPC快速入門」進行故障排除

在APIC GUI中,「配置介面、PC和VPC」快速入門嚮導為管理員提供了現有訪問策略的彙總檢視 ,從而方便了訪問策略查詢。此快速入門嚮導可在GUI中找到,其網址為:

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

#### 「配置介面、PC和VPC」快速入門的位置

cisco	APIC					admin Q	0	C? 🖸	•
System	Tenants	Fabric	Virtual Networking	L4-L7 Service	s Admin	Operations	Apps	Integratio	ons
Inve	entory   Fa	bric Policies	Access Policies						
Policies (F) (=) (O) > () Quick Start			Quick Start						•
<ul> <li>Switche</li> <li>Module</li> <li>Interfac</li> <li>Policies</li> <li>Pools</li> <li>Pools</li> <li>Physica</li> </ul>	es es il and External i	Domains	Summary Access policies gover operation of interfaces provide external acces the fabric. The system provides default acces policies. Access policies administrators who has fabric administrator privileges can create i access policies accom to their requirements. APIC enables administrators to seles pods, leaf switches, a interfaces to which the apply access policies.	n the access s that config access s to access s to config access s Create policy ave Create new Config The Quick ct the nd Config uick access policy ave Create	Step ure in-band manag- ure out-of-band m a CDP (or other) i a traffic storm cor ure an interface, P configure port inte ure port security	DS gement hanagement interface htrol policy PC, and VPC	Physic Leve CDP LLD LAC LAC Spaa Stor Port SPA On- On- Atta QoS DHC	See Also sical Interface ( a)) P P P Member nning Tree Inte m Control Security N demand Diagn ichable Entity P S P Relay	O (Link Inface oostics Profile

儘管嚮導的名稱中包含「Configure」,但它非常方便您提供許多訪問策略的聚合檢視,這些策略必 須配置為使介面程式化。此聚合作為一個單一檢視,用於瞭解已定義哪些策略,並有效地減少開始 隔離與訪問策略相關的問題所需的點選次數。

載入快速入門檢視時,可參考「已配置的交換機介面」檢視(左上窗格)來確定現有訪問策略。嚮 導根據訪問策略配置,對代表單個或多個枝葉交換機的資料夾下的條目進行分組。

為了演示嚮導的價值,提供了以下嚮導螢幕截圖,因為讀者事先並不瞭解交換矩陣拓撲:

「配置介面、PC和VPC」快速入門的演示檢視

## Configure Interface, PC, and VPC

Configured Switch Interfaces

Configured Swi	itch Interface	es			Click '+' to select switches of
			+	Ŵ	click table row to edit
Switches	Interfaces	IF Type	Attached Device Type		
<b>v m</b> 101					
-	1/31	Individ	L3 (VLANs: 2600)	1	
-	1/4	Individ	Bare Metal (VLANs: 311-3		
1	1/25	Individ	Bare Metal (VLANs: 1111,		
× 103-104					
-	1/10	VPC	Bare Metal (VLANs: 100-3		
-	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		
<b>×</b> 103					
-	1/4	Individ	L3 (VLANs: 3100,603,640,		
► 103,104					

VPC Switch Pairs

			+	
VPC Domain Id	<ul> <li>Switch 1</li> </ul>	Switch 2		
34	103	104		
58	105	108		
67	107	106		
212	2101	2102		

Configured Switch Interfaces窗格顯示訪問策略對映。「VPC交換機對」窗格顯示已完成的VPC保 護組定義。

下表顯示可從上述螢幕截圖匯出的已完成訪問策略定義的子集。

#### 可從上述「快速入門」檢視匯出的已完成訪問策略的子集

交換節點	介面	策略組型別	域型別	VLAN
101	1/31	個人	路由(L3)	2600
101	1/4	個人	Phys(裸機)	311-3
103-104	1/10	VPC	Phys(裸機)	100- 3?

在預設檢視下,VLAN列條目故意不完整。

同樣,已完成的「VPC保護組」策略也可從「VPC交換機對」檢視(左下窗格)中派生。 如果沒有 「VPC保護組」,則無法部署VPC,因為這是在兩個枝葉節點之間定義VPC域的策略。

考慮到由於調整了窗格大小,長條目並非完全可見。要檢視任何條目的完整值,請將滑鼠指標懸停 在感興趣的欄位上。

滑鼠指標懸停在103-104, int 1/10 VPC條目的「Attached Device Type」欄位上:

## Configure Interface, PC, and VPC

Configured Switch Interfaces

ningarea own			1		Click '+' to select switches o click table row to edit
Switches	Interfaces	IF Type	+ Attached Device Type		
<b>v</b> 101					·
-	1/31	Individ	L3 (VLANs: 2600)		
	1/4	Individ	Bare Metal (VLANs: 311-3	J	
	1/25	Individ	Bare Metal (VLANs: 1111,		
<b>~1</b> 03-104					
-	1/10	VPC	Bare Metal (VLANs: 100-3	J	
-	1/6	VPC	Bare Metal (VLANs: 1590-		
-	1/7	VPC	Bare Metal (VLANs: 1590-	Ban	Metal (VLANs: 100-300,900-999), L3 (VLANs:
-		VPC	Bare Metal (VLANs: 100-3	100	-300,400-333)
-	1/17	VPC	Bare Metal (VLANs: 700-7		
<b>v m</b> 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

## 將滑鼠懸停在窗格上,即可看到完整的條目。

#### 使用滑鼠懸停詳細資訊更新已完成訪問策略的子集

交換節點	介面	策略組型別	域型別	VLAN
101	1/31	個人	路由(L3)	2600
101	1/4	個人	Phys(裸機)	311-320
103-104	1/10	VPC	Phys(裸機)	100-300,900- 999
103-104	1/10	VPC	路由(L3)	100-300,900- 999

現在可以觀察和瞭解完整的VLAN關聯,以便進行故障排除和驗證。

# 故障排除場景

對於以下故障排除方案,請參考上一章中的相同拓撲。

訪問策略「簡介」部分的拓撲



## 案例 1:故障F0467 — 路徑無效,新問題

在沒有相應的訪問策略允許正確應用配置的情況下進行交換機/埠/VLAN宣告時,將引發此故障。根 據此故障的描述,可能會缺少訪問策略關係的另一個元素。

為具有中繼封裝的VLAN 1501的上述VPC介面部署靜態繫結後,如果沒有相應的訪問策略關係 ,EPG上會出現以下故障:

**故障**:F0467

**描述:錯**誤委託:uni/tn-Prod1/ap-App1/epg-EPG-Web節點101 101\_102\_eth1\_9配置失敗,因為路 徑配置無效、VLAN配置無效、調試消息:invalid-vlan:vlan-1501:封裝沒有STP段ID。EPG未與域 關聯,或者域未分配此VLAN;invalid-path:vlan-1501:沒有與EPG和埠關聯的域具有所需的VLAN;

從上述故障描述中,對於什麼原因可能導致故障被觸發,有一些明確的指示。系統會發出警告來檢 查訪問策略關係,以及檢查與EPG的域關聯。

檢視上述場景中的「快速入門」檢視,可以清楚地看到訪問策略缺少VLAN。

快速入門檢視,其中101-102, Int 1/9 VPC缺少VLAN

# Configure Interface, PC, and VPC

Configured Switch Interfaces

			+ 🗊
Switches	Interfaces	IF Type	Attached Device Type
V 101-10	2		
-	1/11	Individual	ESX (VLANs: 1001-1100)
	1/9	VPC	Bare Metal
<b>∼</b> ∎101			
	1/17	Individual	L3 (VLANs: 901-910)
✓ ■ 102			
	1/19	Individual	L3 (VLANs: 901-910)
×=301-30	2		
-	1/11	Individual	ESX (VLANs: 1001-1100)
<b>∽</b> 301			
	1/17	Individual	L3 (VLANs: 901-910)
✓ ■ 302			
	1/19	Individual	L3 (VLANs: 901-910)



	-	-	-					_		
	D	1.2	51	٨ï	εŤ.	$\sim$	h.	$\cup$	31	re
v	1	~	$\sim r$	W.	15	$\sim$	1.1		G1	10

			+	
VPC Domain Id	<ul> <li>Switch 1</li> </ul>	Switch 2		
101	101	102		

請注意,該條目缺少對任何VLAN ID的引用。

更正後,快速入門檢視將顯示「(VLAN 1500-1510)」。

101-102, Int 1/9 VPC現在顯示裸機(VLAN:1500-1510)

# Configure Interface, PC, and VPC

Configured Switch Interfaces

				Click '+' to select switches
			+ 🏦	click table row to edit
Switches	Interfaces	IF Type	Attached Device Type	
101-1				
-	1/11	Individual	ESX (VLANs: 1001-1100)	0000000         0000000         0000000         0000000         0000000         0000000           0000000         0000000         0000000         0000000         0000000         0000000
-	1/9	VPC	Bare Metal (VLANs: 1500	<b>A A A A A A A A A A</b>
101			Bare Metal (VLA)	Ns: 1500-1510)
-	1/17	Individual	L3 (VLANs: 901-910)	
102				
-	1/19	Individual	L3 (VLANs: 901-910)	
<b>~ 3</b> 01-3				
-	1/11	Individual	ESX (VLANs: 1001-1100)	
301				
-	1/17	Individual	L3 (VLANs: 901-910)	
<b>~</b> =302				
-	1/19	Individual	L3 (VLANs: 901-910)	
_				
C Switch Pa	airs			
			+ 🗊	
/PC Domair	n Id 🔺	Switch 1	Switch 2	
101	10	)1	102	

但是,EPG故障仍存在, 並以下更新了故障F0467的說明:

**故障**:F0467

**描述:錯**誤委託:由於路徑配置無效,uni/tn-Prod1/ap-App1/epg-EPG-Web節點101 101\_102\_eth1\_9的配置失敗,調試消息:invalid-path:vlan-150:沒有與EPG和埠關聯的域具有所需 的VLAN。

對於上述已更新的故障,請檢查EPG域關聯以發現沒有域與EPG關聯。

#### EPG-Web具有靜態埠關聯,但缺少域關聯

cisco	APIC									ad	min	۹ و	9		•
System	Tenants	Fabric	Virtual Ne	tworking	L4-	L7 Service	s	Admin	Operatio	ons	Apps	Inte	gration	S	
ALL TENANTS	6   Add Ten	ant   Tenar	t Search: na	me or descr		com	non	Prod1	mgmt	TECAC	12540	infra			
Prod1			C	000	Do	omains (VI	VIs an	d Bare-N	letals)						00
> C Quick St	art												(	<u>+</u> C	***
	cation Profiles				^	Dom Type	e De	ploy Resc	Micro- Segme	Primar VLAN	Port Encap	Switch Mode	Encap Mode	Cos Value	Enhand Lag Policy
~ <b></b>	Application EP	Gs							No items Select Action	have beer s to create	n found. a new iten	n.			
~	EPG-Web	(Me and Bar	a-Mataie)												
	> EPG Mer	mbers	e-metais/												
	V 📰 Static Po	orts			•										
	F Pod-	1/Node-101-	102/101_102_	_eth1_9											
	E Static Le	afs													
	> 🚞 Fibre Ch	annel (Paths)													
	Contract	s													
	E Static En	ndpoint													
	> E Subnets														
	L4-L7 V	irtual IPs													
	🔚 L4-L7 IP	Address Pool													

一旦包含VLAN 1501的域與EPG關聯,則不會引發進一步的故障。

# 案例 2:無法選擇VPC作為在EPG靜態埠或L3Out邏輯介面配置檔案(SVI)上部署的路徑

嘗試將VPC配置為EPG靜態埠或L3Out邏輯介面配置檔案SVI條目的路徑時,要部署的特定VPC不會 顯示為可用選項。

嘗試部署VPC靜態繫結時,有兩個硬性要求:

1. 必須為相關的一對枝葉交換機定義VPC顯式保護組。

2. 必須定義完全訪問策略對映。

可從「快速入門」檢視中檢查這兩個要求,如上所示。如果兩者均未完成,VPC將不會顯示為靜態 埠繫結的可用選項。

#### 案例 3:故障F0467 — 已在另一個EPG中使用交換矩陣封裝

預設情況下,VLAN具有全域性範圍。這意味著給定的VLAN ID只能用於給定枝葉交換機上的單個 EPG。在給定枝葉交換機內的多個EPG上重複使用同一VLAN的任何嘗試都會導致以下故障:

故障: F0467

**描述:錯**誤委託:由於封裝已在另一個EPG中使用,調試消息:encap-already-in-use:Prod1:App1:EPG-Web已在使用封裝;

除了選擇不同的VLAN外,使此配置有效的另一個選項是考慮使用「本地埠」VLAN範圍。此範圍允 許基於每個介面對映VLAN,這意味著VLAN-1501可能用於同一枝葉上的多個介面上的不同EPG。

雖然「Port Local」範圍基於策略組進行關聯(具體是通過L2策略),但是它在枝葉級別應用。

## 在APIC GUI中更改「VLAN範圍」設定的位置

cisco APIC	admin 🔇 😍 😰 😆
System Tenants Fabric	Virtual Networking L4-L7 Services Admin Operations Apps Integrations
Inventory   Fabric Policies	Access Policies
Policies	Create L2 Interface Policy
	Description: optional
<ul> <li>Priority Flow Control</li> <li>Fibre Channel Interface</li> </ul>	QinQ: CorePort disabled doubleQtagPort edgePort
PoE     DP Interface	Reflective Relay (802.1Qbg): disabled enabled
> 🚞 LLDP Interface	VLAN Scope: Global scope Port Local scope
<ul> <li>Port Channel</li> <li>Port Channel Member</li> </ul>	
> Spanning Tree Interface > Storm Control	
Data Plane Policing     MCP Interface	Cancel Submit
> CoPP Interface	
e default	Page 1 Of 1 Objects Per Page: 15 🗸 Displaying Objects 1 - 1 Of 1

在實施「本地埠」VLAN範圍配置之前,請檢視Cisco.com上的「思科APIC第2層網路配置指南」 ,以確保其限制和設計限制對於期望的使用案例和設計是可接受的。

#### 特殊提及

#### 顯示使用情況

雖然不是訪問策略的特定按鈕,但是在GUI中標籤為「顯示使用情況」的大多數對象上都有一個按 鈕。 此按鈕執行基於選定對象的策略查詢,以確定哪些枝葉節點/介面與其有直接關係。這對於常規 查詢方案以及瞭解特定對象或策略是否在使用中都有用。

在下面的螢幕截圖中,所選的AEP正被兩個不同的介面使用。這意味著,對AEP進行修改將直接影響關聯的介面。

cisco APIC								admin	٩	0	0		•
System Tenants Fabric	Virtual Networking	L4-L7 Services	Admin C	Operations	Apps	Integrations							
Inventory   Fabric Policies	Access Policies												
Policies	$(\mathbf{\bar{D}})$	Attachable Acc	ess Entity Pro	ofile - aep									0.0
> 🕞 Quick Start > 🧮 Switches								Policy	Opera	ational	Faults	н	story
> E Modules		8 7 4 6									Ċ	) <u>*</u>	**-
Policies     Policies		Policy Usa	ige Inform	nation				<b>?</b> &					Î
> 🔤 Switch > 🔁 Interface > 🔁 Global		i These or dela	tables show th ete this policy, i	e nodes when it will affect th	e this policy e nodes and	is used and other policies that policies shown in the tables.	t use this policy. If you m	odify					
Attachable Access Entity Profiles												g .	E I
Pod2_aep		Nodes using t	his policy			Policies using this pol	icy						
Site1Outside		Choose Usage:	Interface			<ul> <li>Name</li> </ul>	Туре		bd				
VMware		A Node Id	Name	Reso	urces	101_102_eth1_9	PC/VPC Interface Polic	cy Group					
e dep		101	S1P1-Leaf1 S1P1-Leaf1	101 <u>Click</u> 102 <u>Click</u>	to Show Detail to Show Detail								
multipodL3Out_EntityProfile													
> 🚍 QOS Class													
> E DHCP Relay													
MCP Instance Policy default													
Error Disabled Recovery Policy						•							
Traubleshooting						Change Depl	oyment Settings	Close					
> E Pools								_					+
> Physical and External Domains		<ul> <li>Application</li> </ul>	EPGs				Encap	Prima	ary Enca	р	Mode		
						No items have been fr Calart Artinue In masta a	ound. naw itam	Show	Usage				•
Last Login Time: 2019-10-03T02:30 UTC+00:00									Curr	ent System	Time: 2019-10	-03T02:3	2 UTC+00:00

#### 重疊的VLAN池

雖然訪問策略的功能是允許將特定VLAN部署到介面上,但在設計階段還必須考慮其他用途。具體 而言,域用於計算與外部封裝繫結的VXLAN ID(稱為交換矩陣封裝)。雖然此功能通常對資料平面 流量沒有主要影響,但此類ID與泛洪通過交換矩陣的協定子集(包括生成樹BPDU)特別相關。如 果leaf1上的VLAN-<id>BPDU入口應輸出枝葉2(例如,讓舊式交換機通過ACI收斂生成樹),則 VLAN-<id>必須在兩個枝葉節點上具有相同的交換矩陣封裝。如果同一接入VLAN的交換矩陣封裝值 不同,則BPDU不會在交換矩陣中傳輸。

如上一節所述,避免在多個域(例如VMM與物理)中配置相同的VLAN,除非特別注意確保每個域 只應用於一組唯一的枝葉交換機。當兩個網域都能夠解析到給定VLAN的同一枝葉交換器時,基礎 VXLAN就有可能在升級(或重新全新載入)後發生變更,例如,這可能導致STP收斂問題。此行為 是每個域具有唯一數值(「base」屬性)的結果,該值用於以下公式以確定VXLAN ID:

VXLAN VNID =基本+(encap — from\_encap)

要驗證將哪些域推入到給定枝葉上,可以對「stpAllocEncapBlkDef」類運行moquery:

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

從此輸出中,可識別以下訪問策略定義:

- 有一個已程式設計的VLAN池,其中包含明確定義VLAN 1500-1510的VLAN塊。
- 此VLAN塊與名為「physvlan」的域關聯。
- VXLAN計算中使用的基值為8492。
- •作為交換矩陣封裝,VLAN-1501的結果的VXLAN計算值為8492 +(1501-1500)= 8493。

### 產生的VXLAN ID(在本例中為8493)可以通過以下命令進行驗證:

leaf# <b>show</b>	system into	ernal epm vlar	n all	+	+	_+	+
VLAN ID	Туре	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
加果有仟何	包全\/I AN	-1501的其他\	/I AN	l池被推入	到同一本	支産┣	升级戓全新重新載入了

如果有任何包含VLAN-1501的其他VLAN池被推入到同一枝葉上,升級或全新重新載入可能會獲取 唯一的基本值(以及隨後的另一個交換矩陣封裝),這將導致BPDU停止進入另一個枝葉上,而後 者預計會接收VLAN-1501上的BPDU。

#### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。