Risoluzione dei problemi relativi ai criteri di accesso ACI

Sommario

Introduzione

In questo documento viene descritto come comprendere e risolvere i problemi relativi ai criteri di accesso ACI.

Premesse

Il materiale di questo documento è stato estratto dal libro Troubleshooting Cisco Application Centric Infrastructure, Second Edition, in particolare i capitoli **Access Policies - Overview** and **Access Policies - Troubleshooting Workflow**.

Panoramica dei criteri di accesso

In che modo l'amministratore ACI configura una VLAN su una porta della struttura? In che modo l'amministratore ACI inizia a risolvere gli errori relativi alle policy di accesso? In questa sezione viene illustrato come risolvere i problemi relativi ai criteri di accesso all'infrastruttura.

Prima di passare agli scenari di risoluzione dei problemi, è essenziale che il lettore abbia una buona comprensione del funzionamento dei criteri di accesso e delle relative relazioni all'interno del modello a oggetti ACI. A tal fine, il lettore può fare riferimento sia ai documenti "ACI Policy Model" che "APIC Management Information Model Reference" disponibili su Cisco.com (https://developer.cisco.com/site/apic-mim-ref-api/).

La funzione delle policy di accesso è quella di abilitare una configurazione specifica sulle porte di downlink di uno switch foglia. Prima che i criteri tenant vengano definiti per consentire il traffico attraverso una porta ACI fabric, è necessario che siano in vigore i criteri di accesso correlati.

In genere, le policy di accesso vengono definite quando vengono aggiunti nuovi switch foglia alla struttura o quando un dispositivo viene connesso ai collegamenti downlink foglia ACI; tuttavia, a seconda della dinamica dell'ambiente, è possibile modificare i criteri di accesso durante il normale funzionamento del fabric. Ad esempio, per consentire un nuovo set di VLAN o aggiungere un nuovo dominio di routing alle porte di accesso all'infrastruttura.

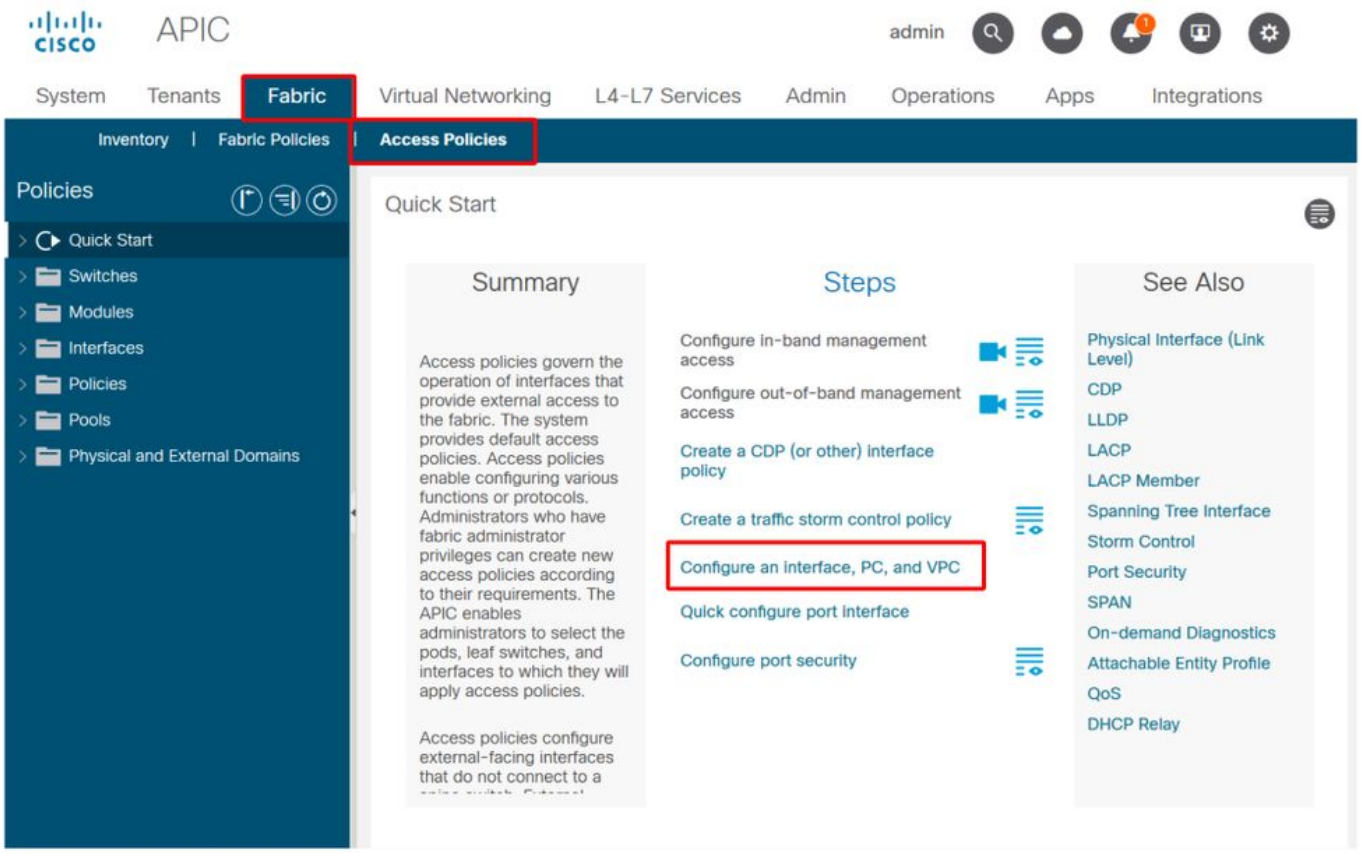
Le policy di accesso ACI, anche se inizialmente un po' intimidatorie, sono estremamente flessibili e sono progettate per semplificare il provisioning della configurazione su una rete SDN su larga scala in continua evoluzione.

Configurazione dei criteri di accesso: Metodologia

Le policy di accesso possono essere configurate in modo indipendente, ad esempio creando tutti gli oggetti necessari in modo indipendente, oppure definite tramite le numerose procedure guidate fornite dall'interfaccia GUI di ACI.

Le procedure guidate sono molto utili in quanto guidano l'utente attraverso il flusso di lavoro e garantiscono che tutti i criteri necessari siano stati implementati.

Criteri di accesso: procedura guidata Avvio rapido

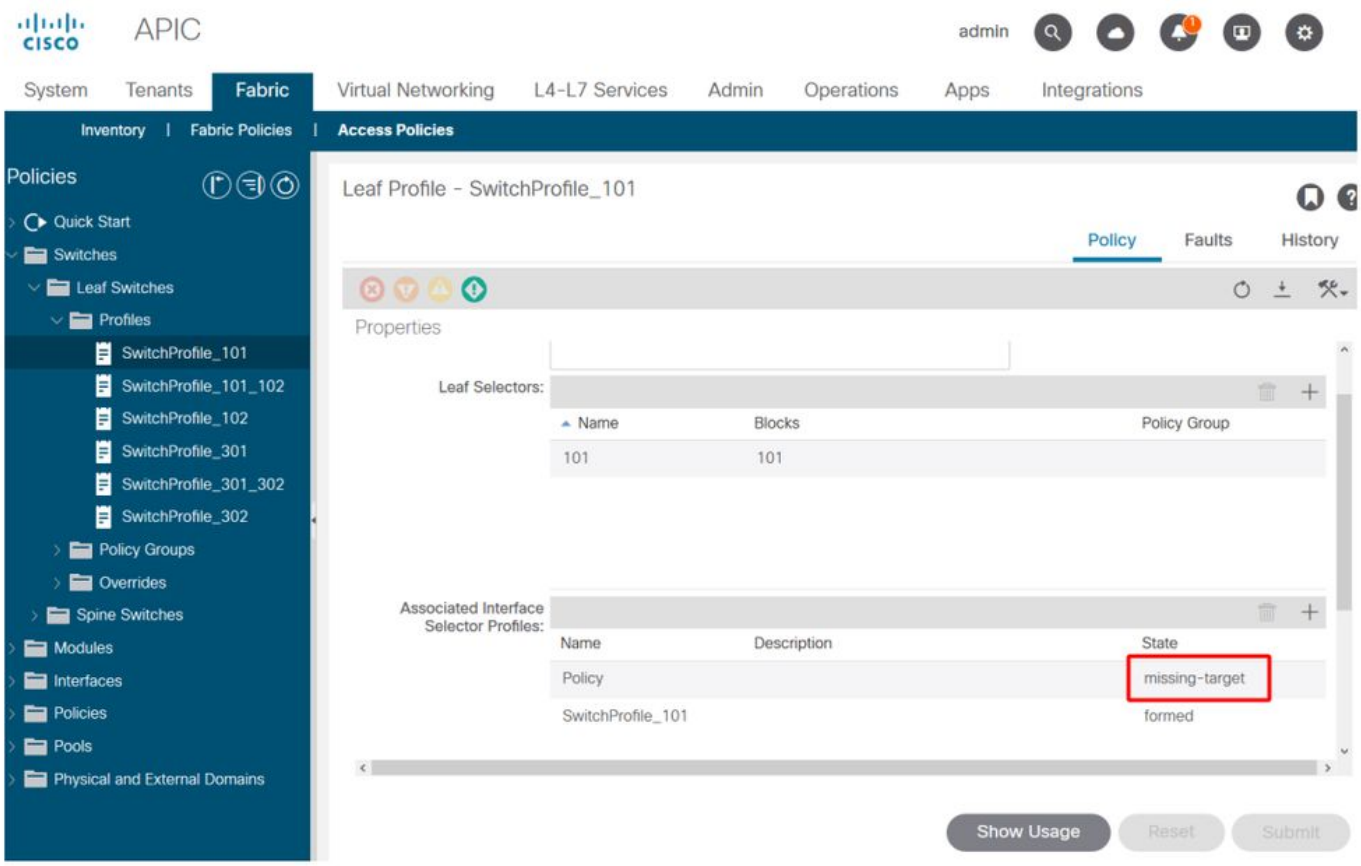


L'immagine precedente mostra la pagina Avvio rapido, in cui è possibile trovare più procedure guidate.

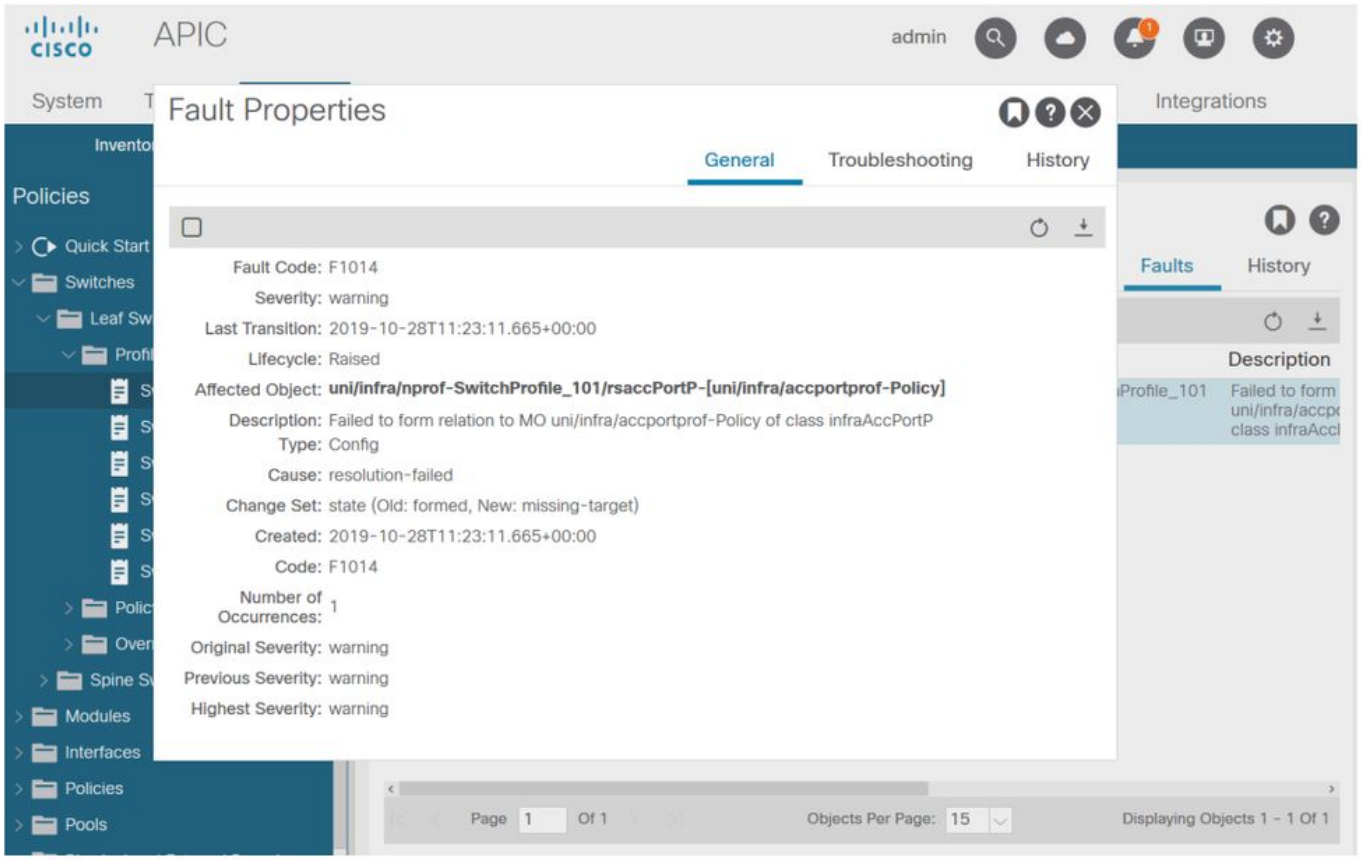
Dopo aver definito un criterio di accesso, è consigliabile convalidarlo verificando che tutti gli oggetti associati non mostrino errori.

Nella figura seguente, ad esempio, a un profilo di switch è stata assegnata una policy di selezione dell'interfaccia che non esiste. Un utente attento sarà facilmente in grado di individuare lo stato '**missing-target**' dell'oggetto e verificare che un errore sia stato contrassegnato dalla GUI:

Profilo foglia — SwitchProfile_101



Profilo foglia — SwitchProfile_101 — Errore



In questo caso, correggere l'errore sarebbe facile come creare un nuovo profilo di selezione interfaccia chiamato "Policy".

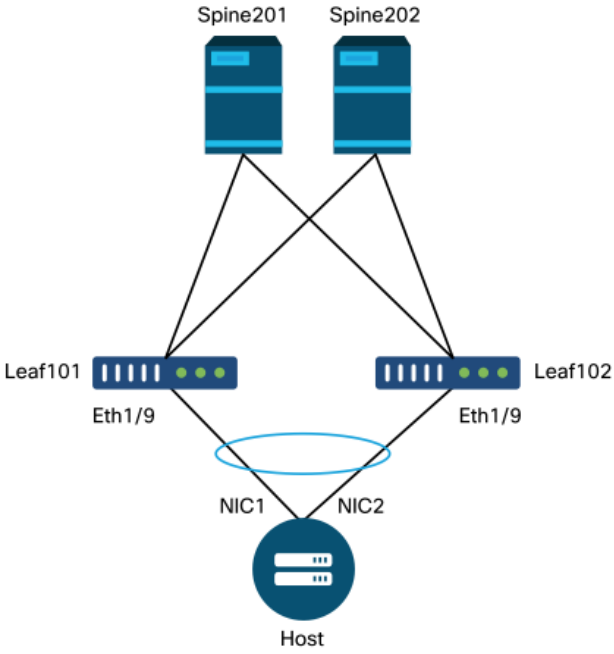
La configurazione manuale dei criteri di accesso di base verrà illustrata nei paragrafi seguenti.

Configurazioni di base manuali dei criteri di accesso

Durante la distribuzione dei criteri di accesso, vengono definiti oggetti per esprimere l'utilizzo previsto dei collegamenti di scelta rapida specificati. La dichiarazione con cui vengono programmati i downlink (ad esempio, l'assegnazione della porta statica EPG) si basa su questo intento espresso. Ciò consente di scalare la configurazione e raggruppare logicamente oggetti simili, quali switch o porte specificamente connessi a una determinata periferica esterna.

Fare riferimento alla topologia riportata di seguito per il resto di questo capitolo.

Topologia della definizione dei criteri di accesso per il server dual-homed

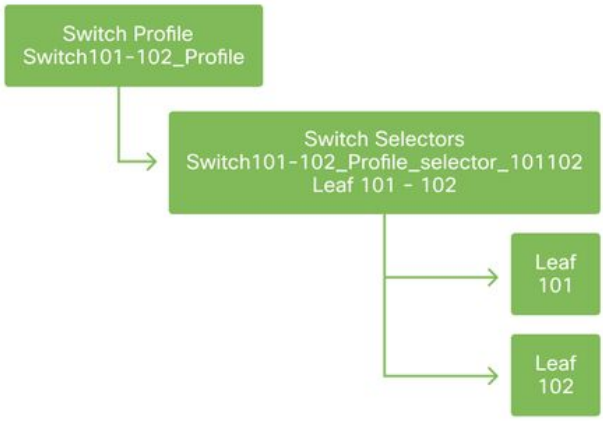


Un server Web è connesso a un'infrastruttura ACI. Il server Web dispone di due schede di interfaccia di rete (NIC, Network Interface Card) configurate in un canale porta LACP. Il server Web è collegato alla porta 1/9 degli switch foglia 101 e 102. Il server Web si basa sulla VLAN-1501 e deve risiedere nell'EPG 'EPG-Web'.

Configurazione del criterio Switch

Il primo passaggio logico consiste nel definire quali switch foglia verranno utilizzati. Il 'Profilo switch' conterrà 'Selettori switch' che definiscono gli ID dei nodi foglia da utilizzare.

Cambia criteri



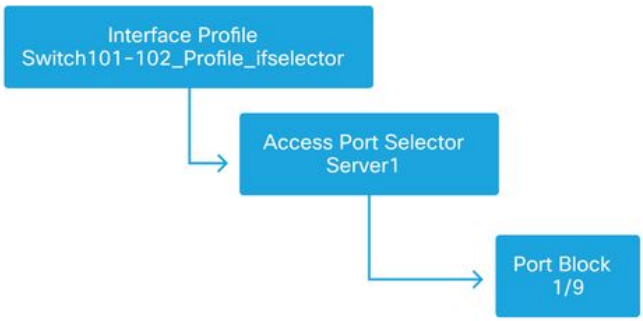
Si consiglia di configurare 1 profilo di switch per ogni switch foglia e 1 profilo di switch per coppia di domini VPC, utilizzando uno schema di denominazione che indichi i nodi che fanno parte del profilo.

La Guida introduttiva consente di distribuire uno schema di denominazione logico che ne facilita l'individuazione. Il nome completo segue il formato 'Switch<node-id>_Profile'. Ad esempio, 'Switch101_Profile' è per un profilo di switch contenente il nodo foglia 101 e lo switch 101-102_Profile per un profilo di switch contenente i nodi foglia 101 e 102 che deve essere parte di un dominio VPC.

Configurazione dei criteri di interfaccia

Dopo aver creato le policy di accesso allo switch, la definizione delle interfacce sarebbe il passaggio logico successivo. A tale scopo, viene creato un 'Profilo interfaccia' costituito da uno o più 'Selettori porte di accesso' contenenti le definizioni 'Blocco porte'.

Criteri di interfaccia



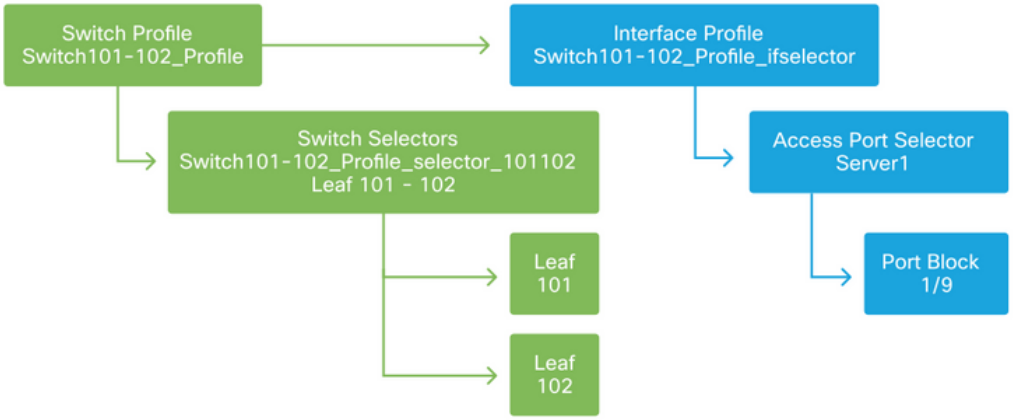
Per definire la relazione tra il 'Profilo interfaccia' e gli switch interessati, collegare il 'Profilo switch' al 'Profilo interfaccia'.

I 'profili di interfaccia' possono essere definiti in molti modi. Analogamente ai 'profili di switch', è possibile creare un singolo 'profilo di interfaccia' per switch fisico insieme a un 'profilo di interfaccia' per dominio VPC. A questo punto, le policy devono avere un mapping uno a uno al profilo di switch corrispondente. Seguendo questa logica, le regole di accesso alla struttura sono notevolmente semplificate e ciò consente agli altri utenti di comprenderle facilmente.

Èpossibile utilizzare anche gli schemi di denominazione predefiniti utilizzati dall'avvio rapido. Segue il formato '<switch profile name>_ifselector' per indicare che questo profilo viene utilizzato

per selezionare le interfacce. Ad esempio, 'Switch101_Profile_ifselector'. Nell'esempio, 'Interface Profile' viene usato per configurare le interfacce non VPC sullo switch foglia 101 e viene associato solo al criterio di accesso 'Switch101_Profile'.

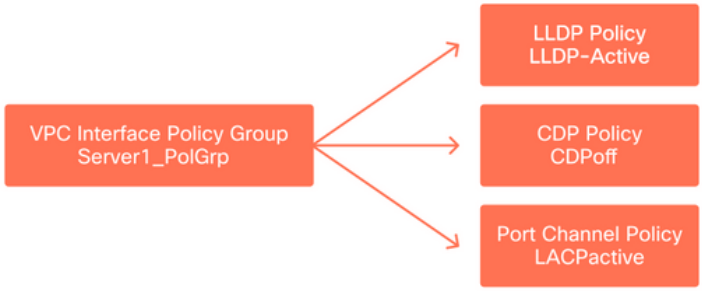
Profilo switch associato al profilo interfaccia



Si noti che, poiché un 'Profilo interfaccia' con Eth 1/9 è collegato a un 'Profilo switch' che include entrambi gli switch foglia 101 e 102, il provisioning di Eth1/9 su entrambi i nodi inizia contemporaneamente.

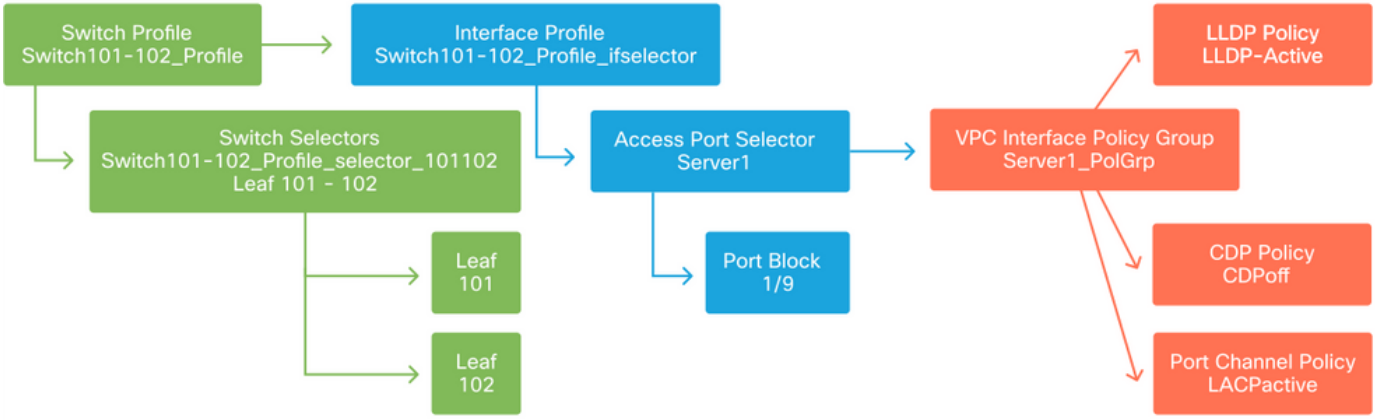
A questo punto, sono stati definiti gli switch foglia e le relative porte. Il passaggio logico successivo consiste nel definire le caratteristiche di queste porte. Il 'Gruppo di criteri di interfaccia' consente la definizione di queste proprietà della porta. Verrà creato un 'gruppo di criteri dell'interfaccia VPC' per consentire il canale della porta LACP sopra indicato.

Gruppo di criteri



Il 'Gruppo di criteri di interfaccia VPC' viene associato al 'Gruppo di criteri di interfaccia' dal 'Selettore porta di accesso' per formare la relazione tra switch/interfaccia foglia e proprietà della porta.

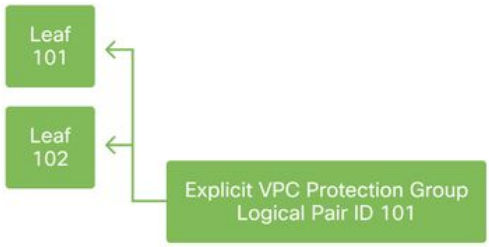
Combinazione di profili di switch e interfaccia



Configurazione del VPC

Per creare il canale della porta LACP su due switch foglia, è necessario definire un dominio VPC tra lo switch foglia 101 e 102. A tale scopo, viene definito un 'gruppo di protezione VPC' tra i due switch foglia.

VPC



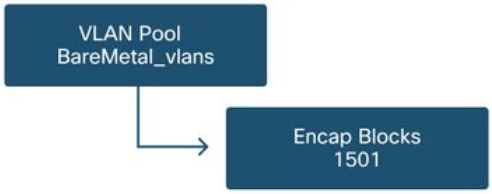
Configurazione dei pool di VLAN

Il passaggio logico successivo è la creazione delle VLAN che verranno utilizzate su questa porta, in questo caso VLAN-1501. La definizione di un 'pool VLAN' con 'blocchi di incapsulamento' completa questa configurazione.

Se si considerano le dimensioni degli intervalli di pool di VLAN, tenere presente che per la maggior parte delle implementazioni sono necessari un solo pool di VLAN e un pool aggiuntivo se si utilizza l'integrazione VMM. Per configurare le VLAN da una rete legacy in ACI, definire l'intervallo di VLAN legacy come pool di VLAN statico.

Ad esempio, si supponga che le VLAN 1-2000 vengano utilizzate in un ambiente legacy. Creare un pool di VLAN statiche contenente le VLAN 1-2000. In questo modo i domini ACI Bridge e gli EPG verranno trunk verso il fabric legacy. Se si distribuisce VMM, è possibile creare un secondo pool dinamico utilizzando un intervallo di ID VLAN liberi.

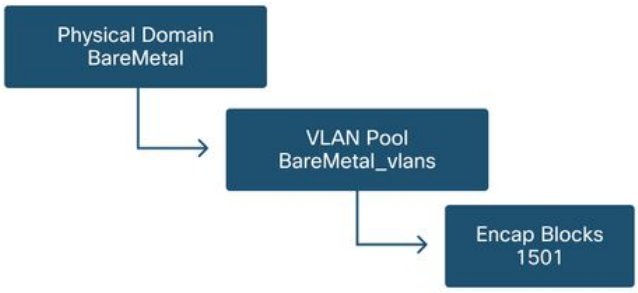
Pool di VLAN



Configura domini

Il passaggio logico successivo consiste nella creazione di un 'Dominio'. Un "dominio" definisce l'ambito di un pool VLAN, ossia il punto in cui verrà applicato. Un 'dominio' può essere fisico, virtuale o esterno (con bridging o routing). In questo esempio, verrà utilizzato un 'dominio fisico' per connettere un server bare metal all'infrastruttura. Questo 'Dominio' viene associato al 'Pool VLAN' per consentire le vlan richieste.

Domini fisici



Per la maggior parte delle distribuzioni, è sufficiente un singolo 'dominio fisico' per le distribuzioni bare metal e un singolo 'dominio di routing' per le distribuzioni L3Out. Entrambi possono eseguire il mapping allo stesso 'pool VLAN'. Se la struttura viene implementata in modalità multi-tenancy, o se è necessario un controllo più granulare per limitare gli utenti che possono implementare EPG e VLAN specifiche su una porta, è opportuno prendere in considerazione una progettazione di policy di accesso più strategica.

'Domini' fornisce inoltre la funzionalità per limitare l'accesso degli utenti ai criteri con 'Domini di sicurezza' che utilizzano il controllo di accesso basato sui ruoli (RBAC).

Quando si distribuiscono le VLAN su uno switch, ACI incapsula le BPDU Spanning-Tree con un ID VXLAN univoco basato sul dominio da cui proviene la VLAN. Per questo motivo, è importante utilizzare lo stesso dominio quando si connettono dispositivi che richiedono la comunicazione STP con altri bridge.

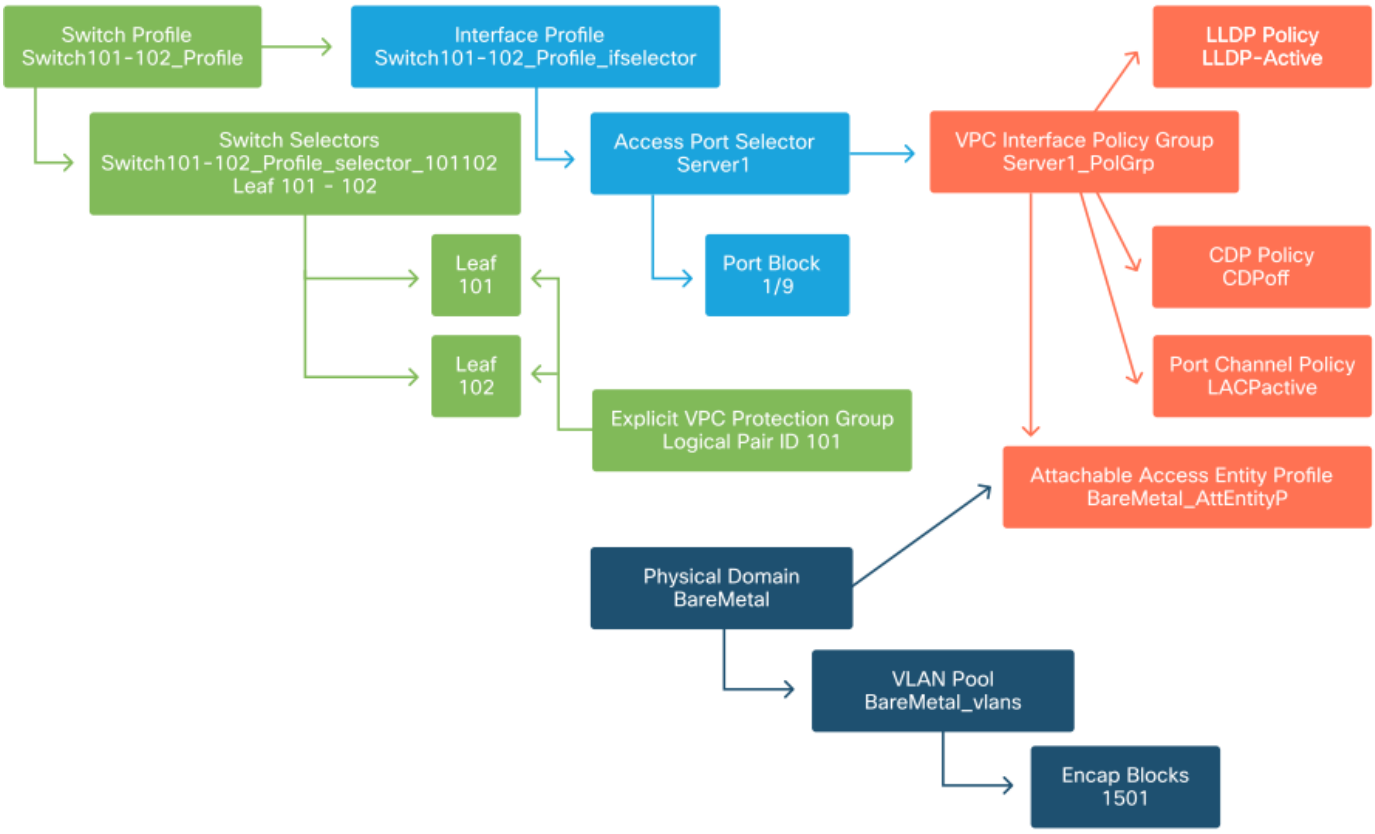
Gli ID VLAN e VXLAN vengono usati anche per consentire agli switch VPC di sincronizzare gli indirizzi MAC e IP appresi dal VPC. Per questo motivo, la progettazione più semplice per i pool VLAN è usare un singolo pool per le distribuzioni statiche e crearne un secondo per le distribuzioni dinamiche.

Configurare il profilo dell'entità di accesso collegabile (AEP)

Sono stati ora completati due grandi blocchi di configurazione delle regole di accesso; le definizioni dello switch e dell'interfaccia e le definizioni del dominio/della VLAN. Un oggetto denominato 'Attachable Access Entity Profile' (AEP) consente di collegare i due blocchi.

Un "gruppo di criteri" è collegato a un AEP in una relazione uno-a-molti che consente all'AEP di raggruppare interfacce e switch che condividono requisiti di criteri simili. Ciò significa che è necessario fare riferimento a un solo AEP quando si rappresenta un gruppo di interfacce su switch specifici.

Profilo entità accesso collegabile



Nella maggior parte delle distribuzioni è consigliabile utilizzare un singolo AEP per i percorsi statici e un AEP aggiuntivo per ogni dominio VMM.

La considerazione più importante è che le VLAN possono essere distribuite sulle interfacce tramite l'AEP. A tale scopo, è possibile eseguire il mapping degli EPG a un AEP direttamente oppure configurare un dominio VMM per il pre-provisioning. Entrambe queste configurazioni rendono l'interfaccia associata una porta trunk (‘switchport mode trunk’ su switch legacy).

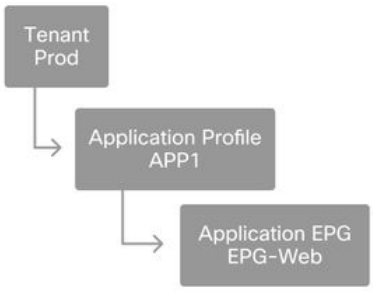
Per questo motivo, è importante creare un AEP separato per L3Out quando si utilizzano porte o sottointerfacce indirizzate. Se nell'uscita L3D vengono utilizzate SVI, non è necessario creare un'ulteriore AEP.

Configurare il tenant, APP ed EPG

ACI utilizza metodi diversi per definire la connettività utilizzando un approccio basato su criteri.

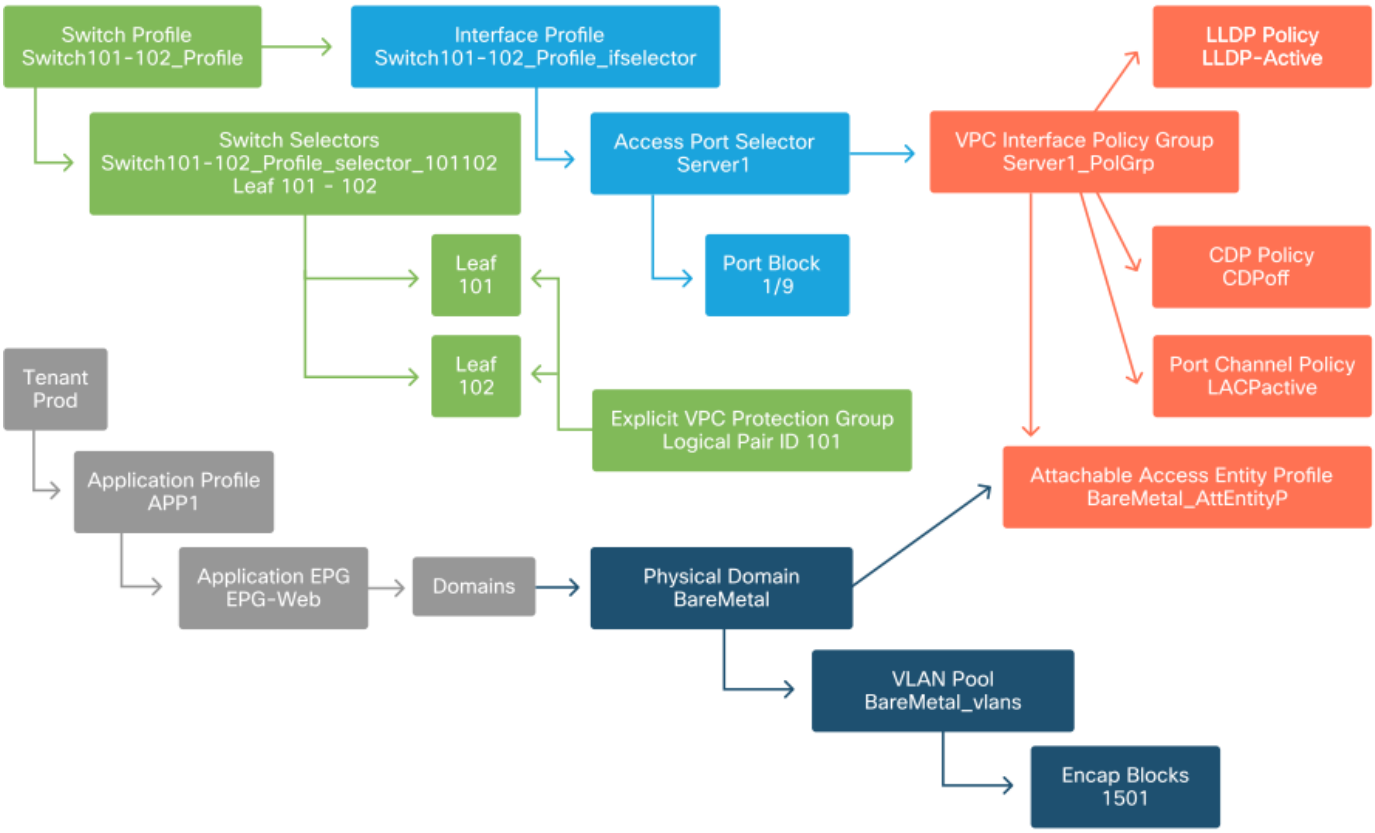
L'oggetto di livello più basso è denominato 'Endpoint Group' (EPG). Il costrutto EPG viene utilizzato per definire un gruppo di VM o server (endpoint) con requisiti di policy simili. I 'profili applicazione', presenti in un tenant, vengono utilizzati per raggruppare logicamente gli EPG.

Tenant, APP e EPG



Il passo successivo consiste nel collegare l'EPG al dominio. In questo modo viene creato il collegamento tra l'oggetto logico che rappresenta il carico di lavoro, l'EPG, e gli switch/interfacce fisiche, le policy di accesso.

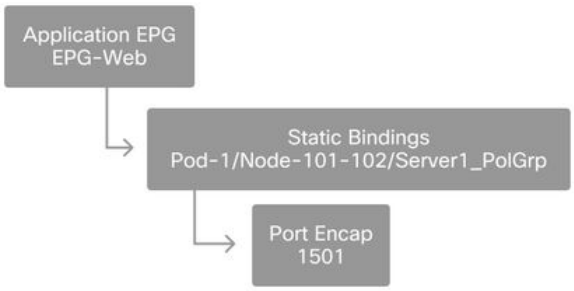
Collegamento da EPG a dominio



Configurare i binding statici EPG

L'ultimo passaggio logico è programmare la VLAN su un'interfaccia di switch per un determinato EPG. Ciò è particolarmente importante se si utilizza un dominio fisico, poiché questo tipo di dominio richiede una dichiarazione esplicita. Ciò consentirà di estendere l'EPG al di fuori del fabric e di classificare il server bare metal nell'EPG.

Associazioni statiche

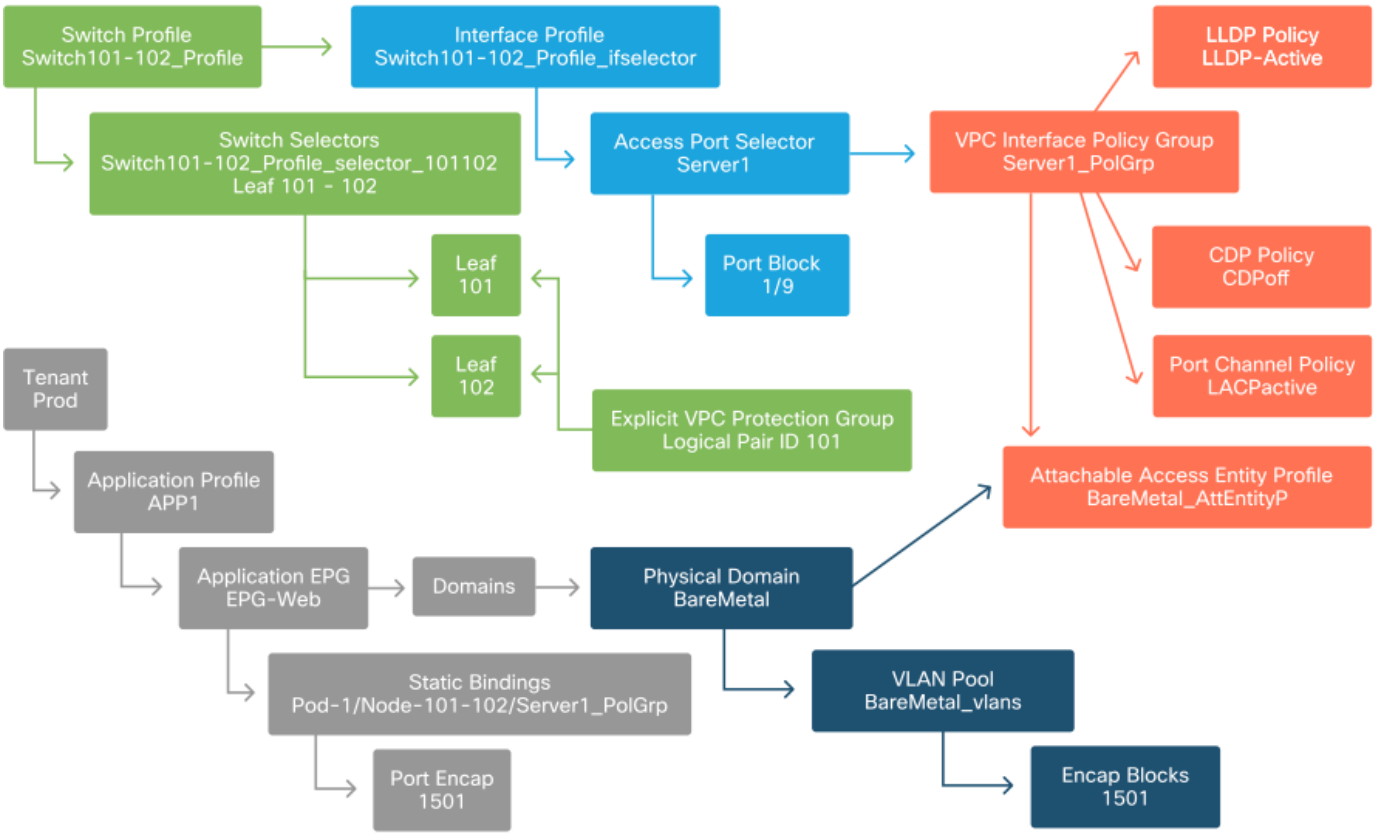


Il parametro 'Port Encap' a cui si fa riferimento deve essere risolvibile sul parametro 'VLAN Pool'. In caso contrario, verrà contrassegnato un errore. Questo argomento viene descritto nella sezione "Flusso di lavoro per la risoluzione dei problemi" di questo capitolo.

Riepilogo della configurazione dei criteri di accesso

Il diagramma seguente riepiloga tutti gli oggetti creati per consentire la connettività dell'host tramite la VLAN-1501, con una connessione VPC allo switch foglia 101 e 102.

Connettività ACI bare-metal



Collegamento di server aggiuntivi

Con tutti i criteri creati in precedenza, cosa significherebbe connettere un altro server sulla porta Eth1/10 sugli switch foglia 101 e 102 con un canale porta?

Facendo riferimento al diagramma "Connettività ACI bare-metal", è necessario creare quanto segue:

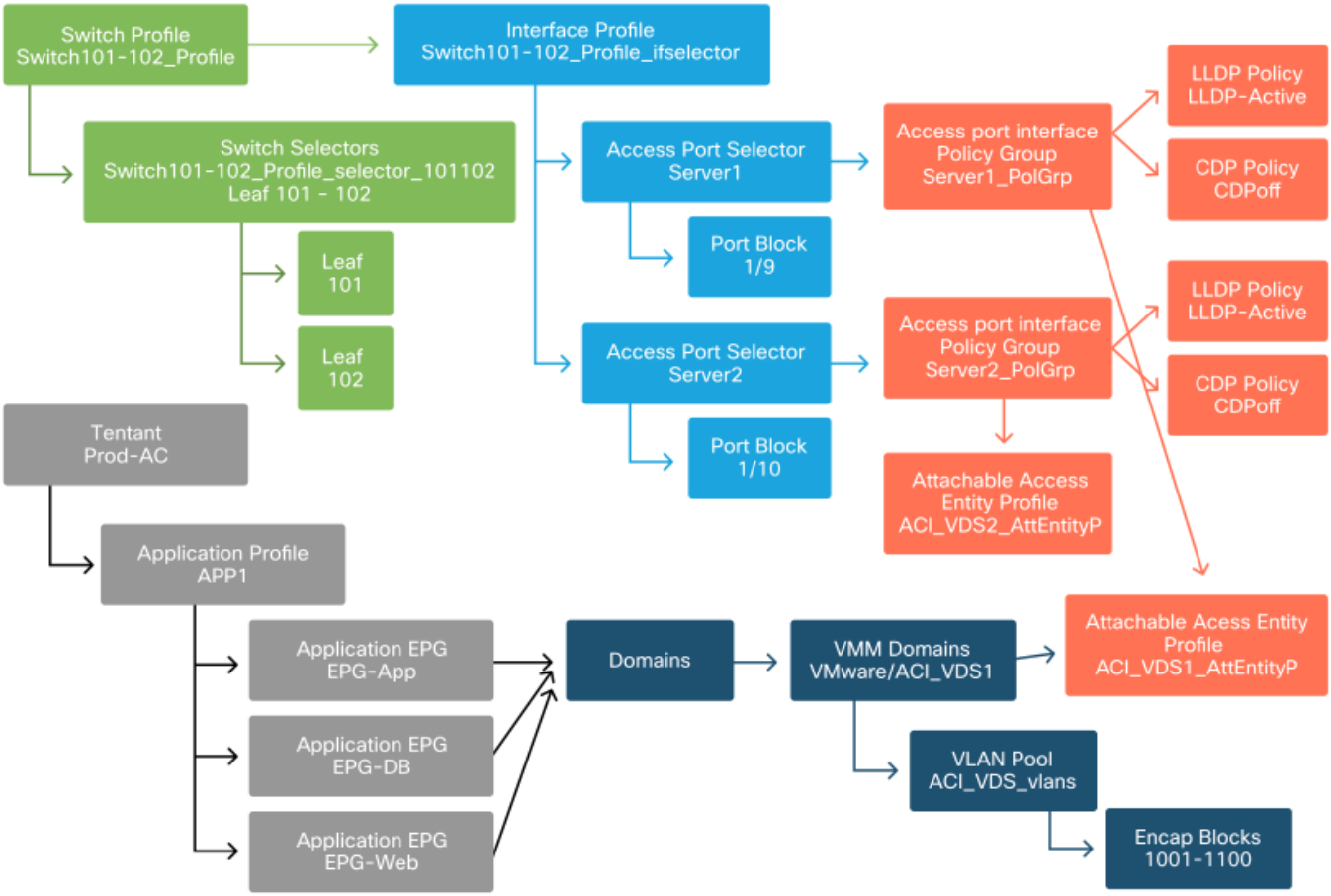
- Un selettore di porta di accesso e un blocco di porta aggiuntivi.
- Gruppo di criteri di interfaccia VPC aggiuntivo.
- Associazione statica aggiuntiva con Port Encap.

Si noti che per i canali della porta LACP è necessario utilizzare un gruppo di criteri dell'interfaccia VPC dedicato, in quanto tale gruppo definisce l'ID VPC.

Nel caso di singoli collegamenti, il gruppo di criteri dell'interfaccia non VPC può essere riutilizzato per il server aggiuntivo se il collegamento richiede le stesse proprietà della porta.

I criteri risultanti saranno simili a quelli illustrati nella figura seguente.

Collegamento di server2 al programma di installazione



Quali saranno le prossime fasi?

Nella sezione successiva verranno illustrati alcuni scenari di errore dei criteri di accesso, a partire dalla topologia e dallo Use Case descritti in questa panoramica.

Flusso di lavoro di risoluzione dei problemi

Durante l'utilizzo dei criteri di accesso è possibile verificare gli scenari di risoluzione dei problemi seguenti:

- Relazione mancante tra due o più entità nei criteri di accesso, ad esempio un gruppo di criteri di accesso non collegato a un'istanza di Access Point.

- Un criterio mancante o imprevisto è associato a un determinato criterio di accesso, ad esempio un criterio LLDP denominato 'lldp_enabled', mentre in realtà la configurazione del criterio ha LLDP rx/tx disabilitato.
- Valore mancante o imprevisto nei criteri di accesso, ad esempio l'ID VLAN configurato non presente nel pool di VLAN configurato.
- Relazione mancante tra EPG e i criteri di accesso, ad esempio nessuna associazione di dominio fisico o virtuale all'EPG.

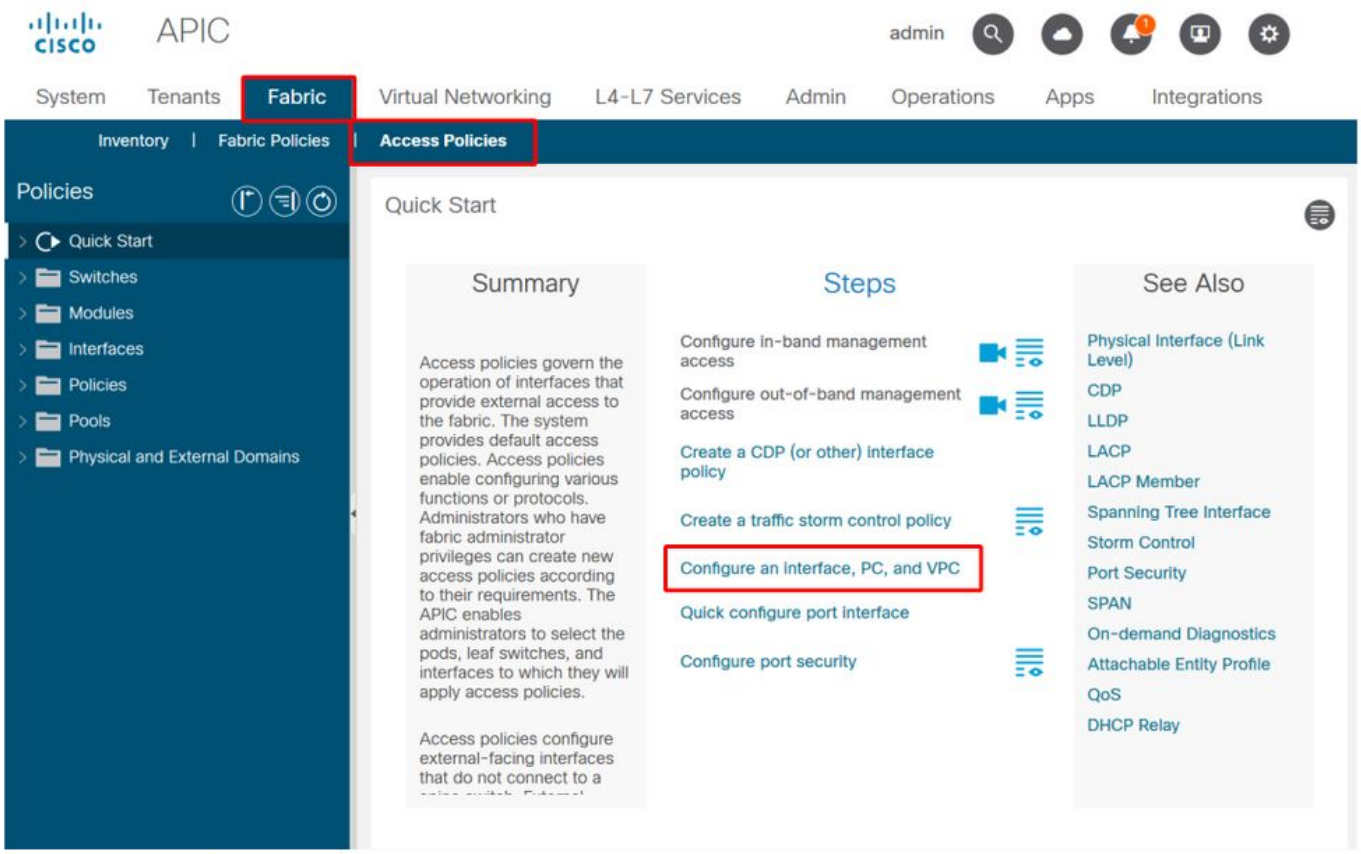
La maggior parte delle procedure di risoluzione dei problemi descritte in precedenza prevede l'analisi delle relazioni dei criteri di accesso per comprendere se mancano relazioni o per capire quali criteri sono configurati e/o se la configurazione determina il comportamento desiderato.

Utilizzo dell'avvio rapido di "Configurazione interfaccia, PC e VPC" per la risoluzione dei problemi

Nell'interfaccia GUI di APIC, la procedura guidata di avvio rapido 'Configura interfaccia, PC e VPC' facilita la ricerca dei criteri di accesso fornendo all'amministratore una vista aggregata dei criteri di accesso esistenti. Questa procedura guidata di avvio rapido è disponibile nella GUI all'indirizzo:

'Fabric > Access Policies > Quick Start > Steps > Configure Interface, PC, and VPC' (Infrastruttura > Criteri di accesso > Avvio rapido > Passi > Configura interfaccia, PC e VPC).

Posizione della Guida introduttiva alla configurazione di interfaccia, PC e VPC

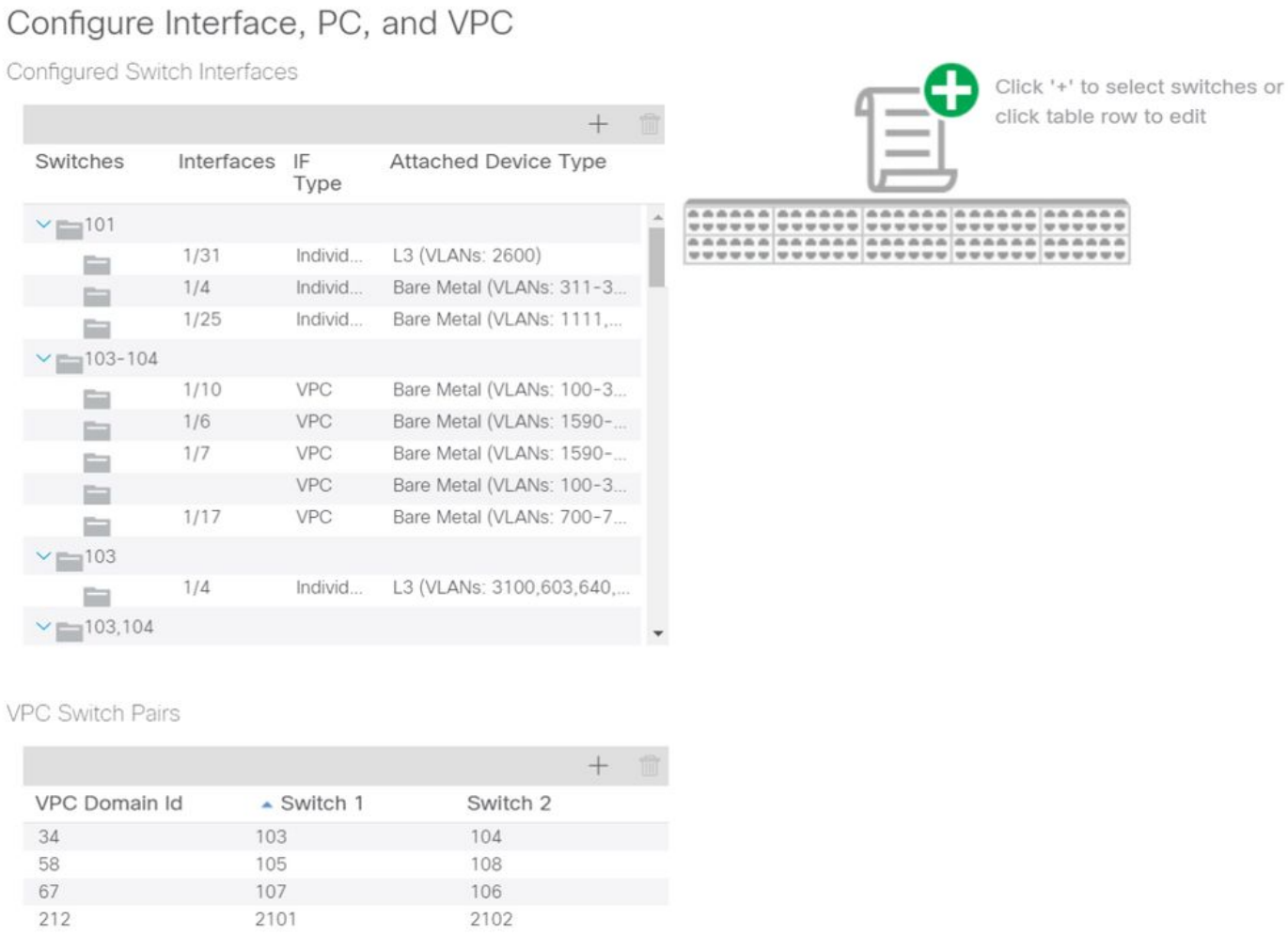


Sebbene il nome della procedura guidata contenga 'Configura', questa funzionalità risulta particolarmente utile per fornire una visualizzazione aggregata dei numerosi criteri di accesso che devono essere configurati per ottenere le interfacce programmate. Questa aggregazione consente di individuare le policy già definite e di ridurre efficacemente il numero di clic necessari per iniziare a isolare i problemi relativi alle policy di accesso.

Quando si carica la visualizzazione Avvio rapido, è possibile fare riferimento alla visualizzazione 'Interfacce di switching configurate' (riquadro in alto a sinistra) per determinare le policy di accesso esistenti. La procedura guidata raggruppa le voci sotto le cartelle che rappresentano uno o più switch foglia, a seconda della configurazione dei criteri di accesso.

A dimostrazione del valore della procedura guidata, vengono presentati i seguenti screenshot della procedura guidata, sapendo che il lettore non ha alcuna conoscenza precedente della topologia della struttura:

Visualizzazione demo dell'avvio rapido di 'Configura interfaccia, PC e VPC'



Nel riquadro 'Interfacce switch configurate' vengono visualizzati i mapping dei criteri di accesso. Nel riquadro 'Coppie di switch VPC' sono visualizzate le definizioni completate del gruppo protezione dati VPC.

La tabella seguente mostra un sottoinsieme di definizioni di criteri di accesso completate che possono essere derivate dallo screenshot precedente.

Sottoinsieme di criteri di accesso completati che è possibile derivare dalla visualizzazione Avvio rapido precedente

Cambia nodo	Interfaccia	Tipo di gruppo di criteri	Tipo di dominio	VLAN
101	1/31	Individuale	Routed (L3)	2600
101	1/4	Individuale	Phys (Bare	311-

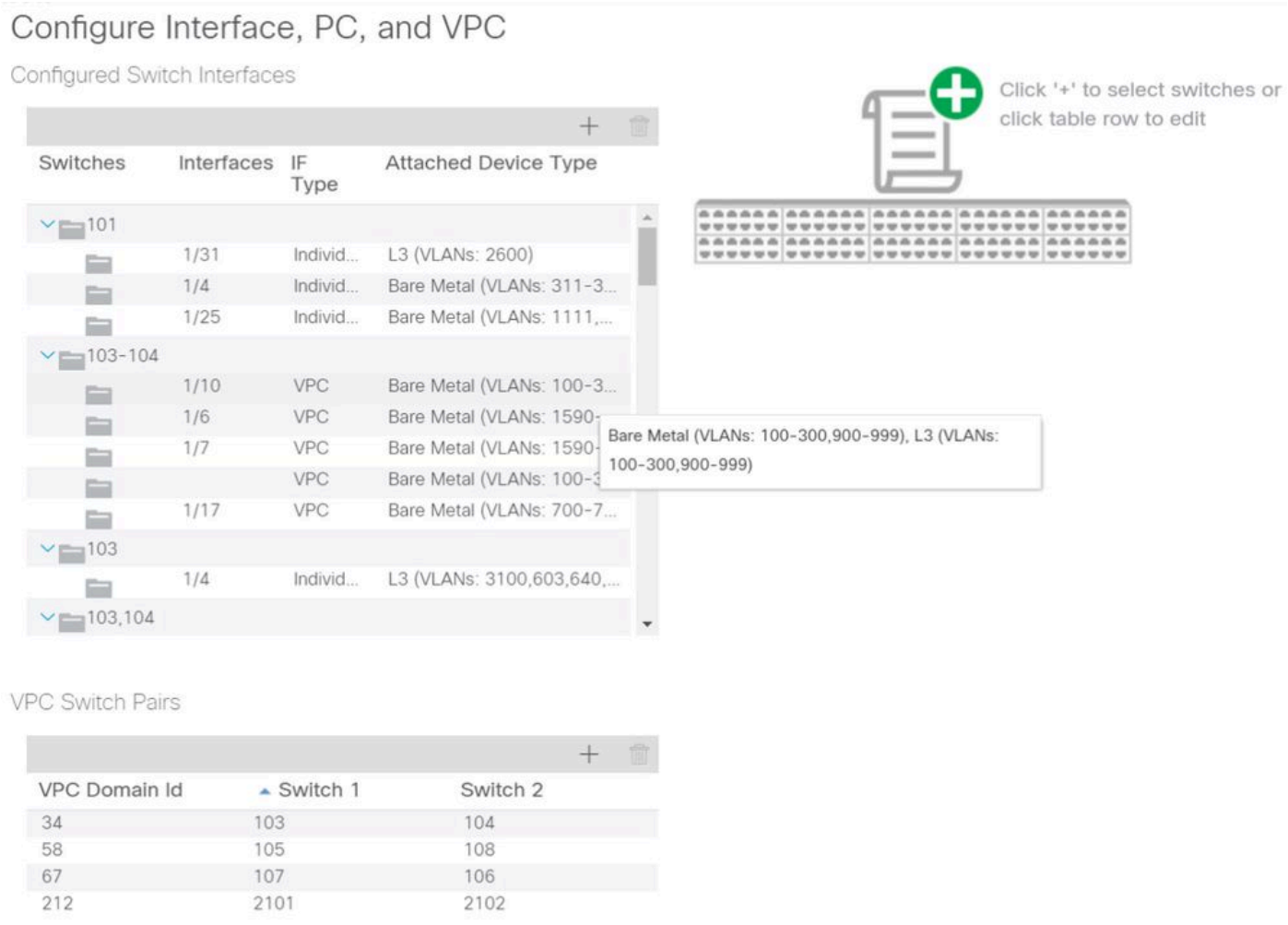
			Metal)	3...?
103-104	1/10	VPC	Phys (Bare Metal)	100-3...?

Le voci della colonna VLAN sono intenzionalmente incomplete nella vista predefinita.

Analogamente, i criteri 'VPC Protection Group' completati possono essere derivati dalla visualizzazione 'VPC Switch Pairs' (riquadro inferiore sinistro). Senza 'Gruppi di protezione VPC', non è possibile distribuire le VPC poiché si tratta del criterio che definisce il dominio VPC tra due nodi foglia.

Tenere presente che a causa delle dimensioni dei riquadri, le voci lunghe non sono completamente visibili. Per visualizzare il valore completo di una voce, posizionare il puntatore del mouse sul campo desiderato.

Il puntatore del mouse è posizionato sul campo 'Tipo di dispositivo collegato' per 103-104, int 1/10 VPC voce:



Passando il mouse sul riquadro, vengono visualizzate le voci complete.

Sottoinsieme aggiornato di criteri di accesso completato utilizzando i dettagli del mouse

Cambia nodo	Interfaccia	Tipo di gruppo di criteri	Tipo di dominio	VLAN
101	1/31	Individuale	Routed (L3)	2600
101	1/4	Individuale	Phys (Bare	311-320

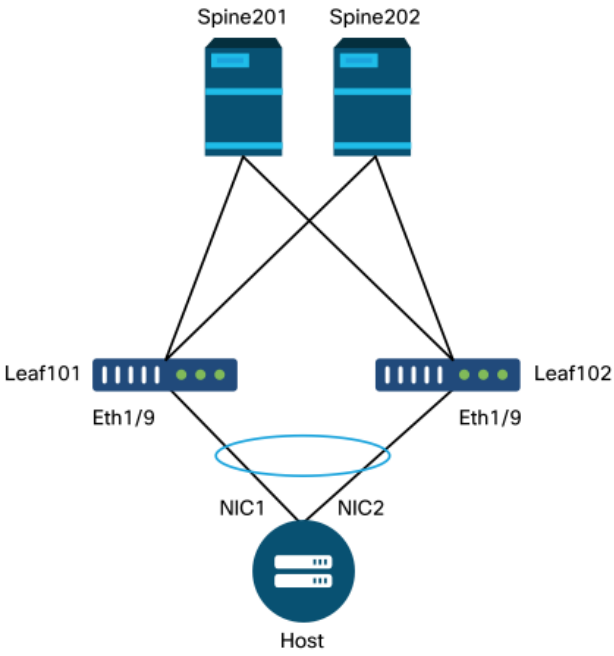
103-104	1/10	VPC	Metal) Phys (Bare Metal)	100-300,900-999
103-104	1/10	VPC	Routed (L3)	100-300,900-999

Èora possibile osservare e comprendere le associazioni di VLAN complete per la risoluzione dei problemi e la verifica.

Risoluzione dei problemi

Per gli scenari di risoluzione dei problemi seguenti, fare riferimento alla stessa topologia del capitolo precedente.

Topologia della sezione 'Introduzione' dei criteri di accesso



Scenario 1: Errore F0467 — percorso non valido, problemi

Questo errore viene generato quando si esegue una dichiarazione di switch, porta o VLAN senza le policy di accesso corrispondenti in uso per consentire la corretta applicazione della configurazione. A seconda della descrizione dell'errore, è possibile che manchi un elemento diverso della relazione tra i criteri di accesso.

Dopo aver implementato un binding statico per l'interfaccia VPC di cui sopra con l'encap trunked VLAN 1501 senza la relazione di policy di accesso corrispondente, viene generato il seguente errore sull'EPG:

Errore: F0467

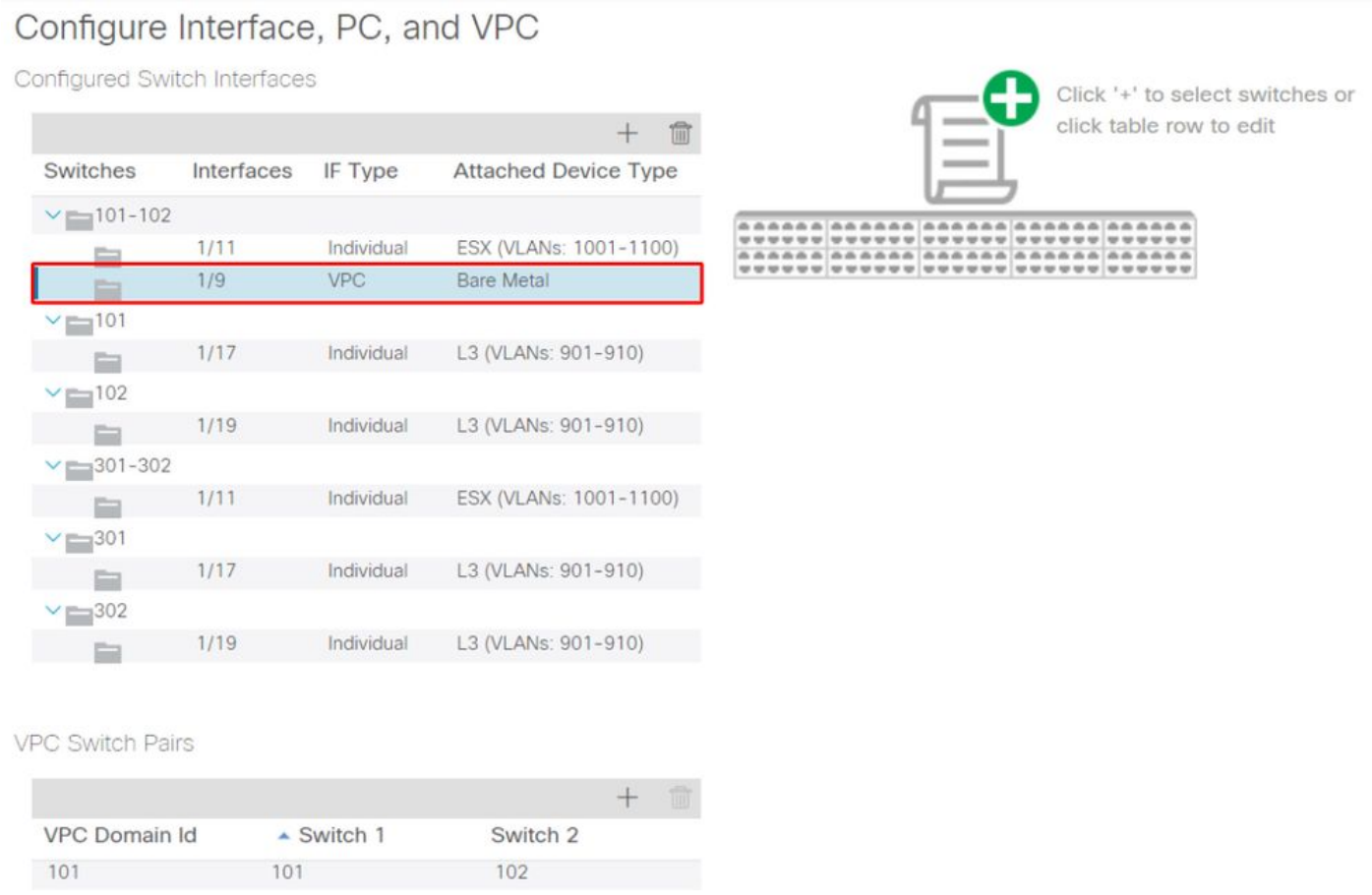
Descrizione: Delegato errore: Configurazione non riuscita per uni/tn-Prod1/ap-App1/epg-EPG-Web node 101/101_102_eth1_9 a causa di configurazione del percorso non valida, configurazione

VLAN non valida, messaggio di debug: invalid-vlan: vlan-1501: ID segmento STP non presente per Encap. L'EPG non è associato a un dominio o al dominio non è stata assegnata questa vlan;percorso-non valido: vlan-1501: non vi è alcun dominio, associato sia a EPG che a Port, che abbia richiesto la VLAN;

Dalla descrizione del guasto di cui sopra, vi sono alcune indicazioni chiare su quali possano essere le cause del guasto. Viene visualizzato un avviso per controllare le relazioni dei criteri di accesso e l'associazione del dominio all'EPG.

Se si esamina la vista Quick Start nello scenario descritto in precedenza, è chiaro che nella policy di accesso non sono presenti VLAN.

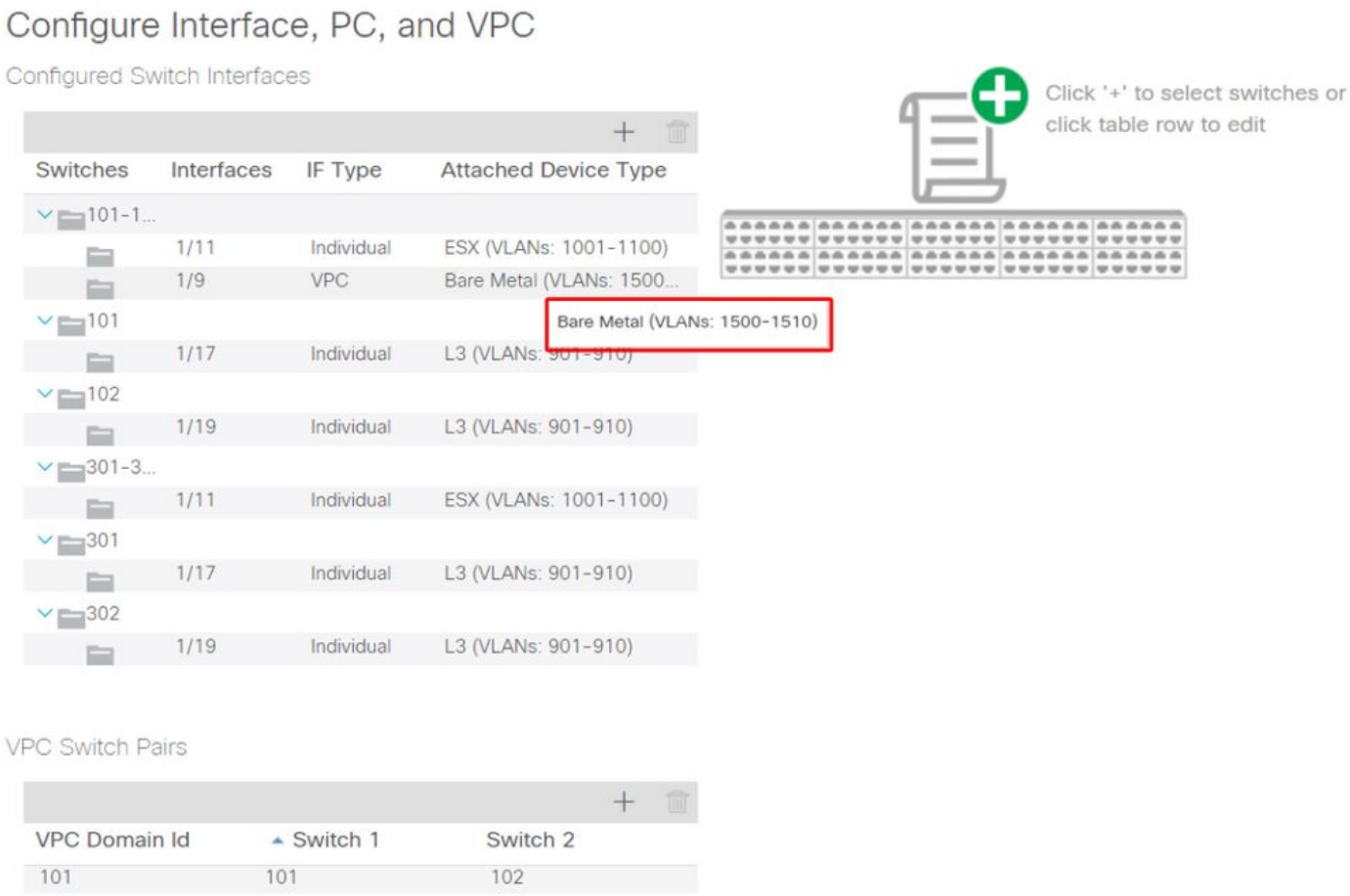
Vista introduttiva in cui 101-102 VPC 1/9 interni non dispongono di VLAN



Nella voce manca un riferimento a qualsiasi ID VLAN.

Una volta eseguita la correzione, nella schermata di avvio rapido verrà visualizzato il messaggio "(VLAN 1500-1510)".

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



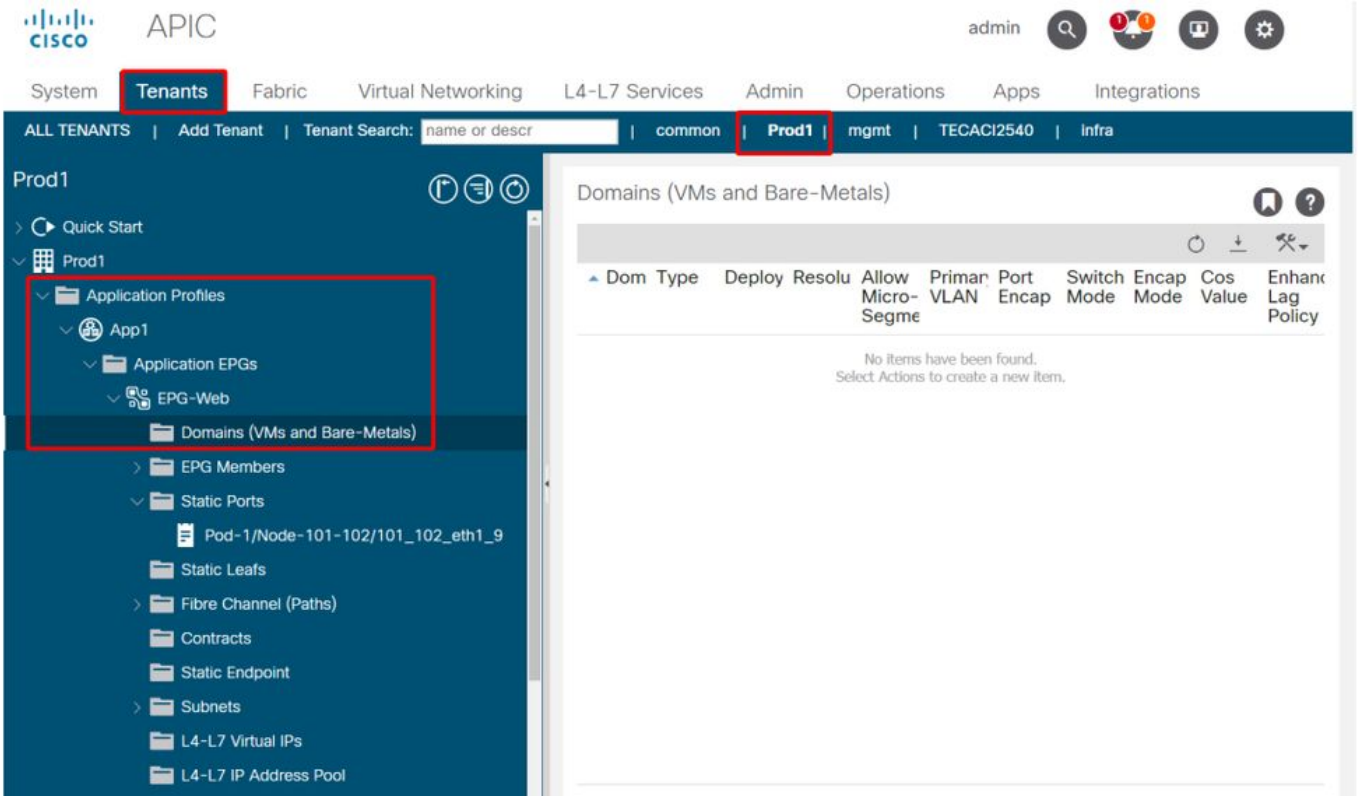
Tuttavia, il guasto EPG è ancora presente con la seguente descrizione aggiornata del guasto F0467:

Errore: F0467

Descrizione: delegato errore: Configurazione non riuscita per uni/tn-Prod1/ap-App1/epg-EPG-Web node 101/101_102_eth1_9 a causa di configurazione del percorso non valida. Messaggio di debug: percorso non valido: vlan-150: Nessun dominio, associato sia a EPG che a Port, ha richiesto una VLAN.

Con l'errore aggiornato sopra, controllare le associazioni di dominio EPG per verificare che non vi siano domini collegati a EPG.

EPG-Web è associato a porte statiche, ma non dispone di associazioni di dominio



Dopo aver associato all'EPG il dominio che contiene la VLAN 1501, non vengono più generati errori.

Scenario 2: Impossibile selezionare VPC come percorso da distribuire sulla porta statica EPG o sul profilo di interfaccia logica L3Out (SVI)

Durante il tentativo di configurare un VPC come percorso su una voce SVI EPG Static Port o L3Out Logical Interface Profile, il VPC specifico da implementare non viene visualizzato come opzione disponibile.

Quando si tenta di distribuire un'associazione statica VPC, esistono due requisiti hardware:

1. Ènecessario definire il gruppo VPC Explicit Protection per la coppia di switch foglia in questione.
2. Ènecessario definire il mapping dei criteri di accesso completo.

Entrambi i requisiti possono essere controllati dalla vista di avvio rapido come illustrato sopra. Se nessuna delle due è completa, il VPC non verrà visualizzato come opzione disponibile per i binding delle porte statiche.

Scenario 3: Fault F0467 — l'encap fabric è già utilizzata in un altro EPG

Per impostazione predefinita, le VLAN hanno un ambito globale. Ciò significa che un determinato ID VLAN può essere utilizzato solo per un singolo EPG su un determinato switch foglia. Ogni tentativo di riutilizzare la stessa VLAN su più EPG all'interno di uno switch foglia specifico avrà il seguente errore:

Errore: F0467

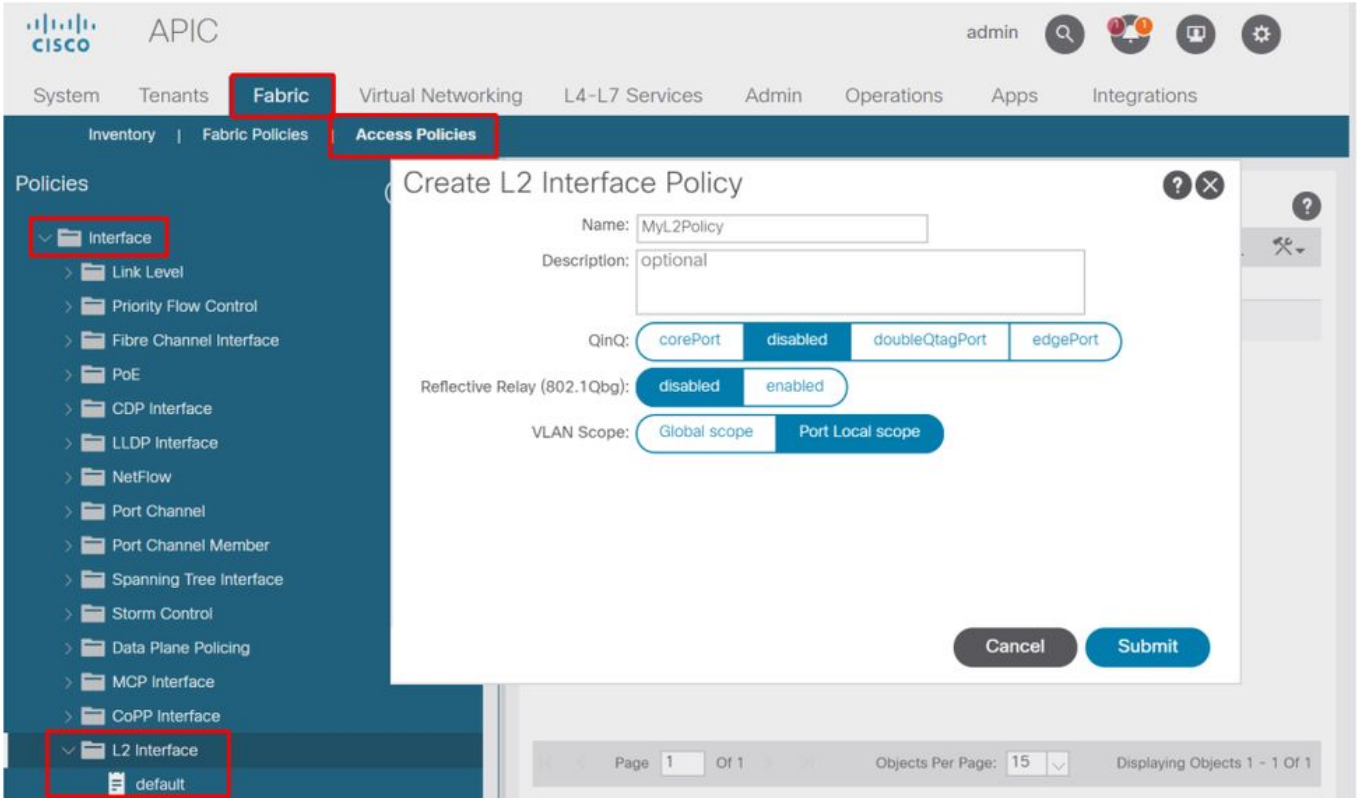
Descrizione: delegato errore: Configurazione non riuscita per il nodo uni/tn-Prod1/ap-App1/epg-EPG-BusinessApp 102/101_102_eth1_8 a causa dell'incapsulamento già utilizzato in un altro

messaggio di debug EPG: encap già in uso: L'incapsulamento è già in uso da Prod1:App1:EPG-Web;

Oltre a selezionare una VLAN diversa, per configurare correttamente la VLAN, è possibile usare l'ambito VLAN 'Port Local'. Questo ambito consente di mappare le VLAN per singola interfaccia, il che significa che la VLAN-1501 potrebbe potenzialmente essere utilizzata per diversi EPG, su più interfacce, sulla stessa foglia.

Sebbene l'ambito 'Port Local' venga associato a un gruppo di criteri (in particolare tramite un criterio L2), viene applicato al livello foglia.

Percorso per modificare l'impostazione 'VLAN Scope' nell'interfaccia grafica di APIC



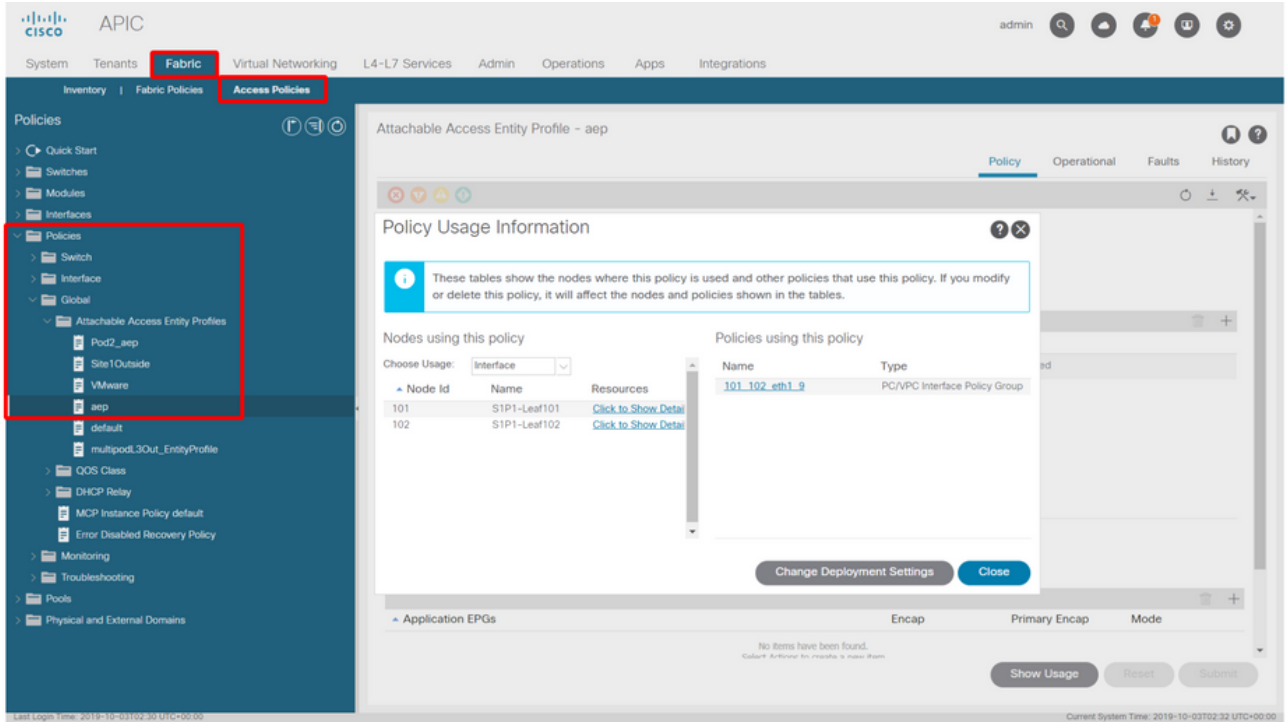
Prima di implementare la configurazione dell'ambito VLAN 'Port Local', consultare la "Cisco APIC Layer 2 Networking Configuration Guide" su Cisco.com per verificare che le limitazioni e le restrizioni di progettazione siano accettabili per gli scenari di utilizzo e le progettazioni desiderate.

Menzioni speciali

Mostra utilizzo

Sebbene non sia specifico dei criteri di accesso, sulla maggior parte degli oggetti della GUI è disponibile un pulsante con l'etichetta 'Mostra utilizzo'. Questo pulsante consente di eseguire una ricerca di criteri basata sull'oggetto selezionato per determinare quali nodi o interfacce foglia hanno una relazione diretta con esso. Ciò può essere utile sia per lo scenario di ricerca generale sia per comprendere se un determinato oggetto o criterio è in uso.

Nell'immagine seguente, l'AEP selezionato è utilizzato da due diverse interfacce. Ciò implica che apportare una modifica all'AEP avrà un impatto diretto sulle interfacce associate.



Pool di VLAN sovrapposti

Le policy di accesso hanno la funzione di consentire l'implementazione di una VLAN specifica su un'interfaccia, ma durante la fase di progettazione è necessario considerare altri utilizzi. In particolare, il dominio viene usato nel calcolo dell'ID VXLAN (chiamato Fabric Encapsulation) associato all'incapsulamento esterno. Anche se questa funzionalità in genere non ha alcuna influenza rilevante sul traffico del dataplane, tali ID sono particolarmente rilevanti per un sottoinsieme di protocolli che passano attraverso il fabric, incluse le BPDU Spanning Tree. Se si prevede che le VLAN-<id> BPDU in entrata su foglia1 escano da foglia 2 (ad esempio, con switch legacy che convergono in spanning-tree tramite ACI), la VLAN-<id> deve avere lo stesso fabric encap su entrambi i nodi foglia. Se il valore dell'encap dell'infrastruttura differisce per le stesse VLAN di accesso, i BPDU non attraversano l'infrastruttura.

Come accennato nella sezione precedente, evitare di configurare le stesse VLAN in più domini (ad esempio, VMM vs Physical), a meno che non si presti particolare attenzione a garantire che ciascun dominio venga applicato solo a un unico insieme di switch foglia. Nel momento in cui entrambi i domini possono essere risolti sullo stesso switch foglia per una determinata VLAN, è possibile modificare la VXLAN sottostante dopo un aggiornamento (o ricaricamento) che può causare, ad esempio, problemi di convergenza STP. Il comportamento è il risultato della presenza di un valore numerico univoco (l'attributo "base") in ciascun dominio, utilizzato nella seguente equazione per determinare l'ID VXLAN:

VXLAN VNID = Base + (encap — from_encap)

Per convalidare i domini di cui viene eseguito il push in una determinata foglia, è possibile eseguire una moquery sulla classe 'stpAllocEncapBlkDef':

```
leaf# moquery -c stpAllocEncapBlkDef

# stp.AllocEncapBlkDef
encapBlk     : uni/infra/vlanns-[physvlans]-dynamic/from-[vlan-1500]-to-[vlan-1510]
base         : 8492
dn           : allocencap-[uni/infra]/encapnsdef-[uni/infra/vlanns-[physvlans]-
```

```
dynamic]/allocencapblkdef-[uni/infra/vlanns-[physvlans]-dynamic/from-[vlan-1500]-to-[vlan-1510]]
from         : vlan-1500
to           : vlan-1510
```

Da questo output, tenere presenti le seguenti definizioni dei criteri di accesso:

- Esiste un pool di VLAN programmato con un blocco di VLAN che definisce in modo esplicito le VLAN 1500-1510.
- Questo blocco di VLAN è associato a un dominio denominato 'physvlans'.
- Il valore di base utilizzato nel calcolo VXLAN è 8492.
- Il calcolo VXLAN risultante per la VLAN-1501 sarebbe 8492 + (1501-1500) = 8493 come incapsulamento della struttura.

L'ID VXLAN risultante (nell'esempio, 8493) può essere verificato con il seguente comando:

```
leaf# show system internal epm vlan all
+----------+---------+-----------------+----------+------+----------+-----------
 VLAN ID    Type      Access Encap     Fabric    H/W id  BD VLAN    Endpoint
                      (Type Value)     Encap                          Count
+----------+---------+-----------------+----------+------+----------+-----------
13          Tenant BD NONE             0 16121790   18     13         0
14            FD vlan 802.1Q       1501 8493       19     13         0
```

Se vi sono altri pool di VLAN contenenti la VLAN-1501 che vengono spinti sulla stessa foglia, un aggiornamento o un ricaricamento pulito potrebbe potenzialmente acquisire un valore di base univoco (e quindi un incapsulamento diverso del fabric), causando la disattivazione delle BPDU su un'altra foglia che dovrebbe ricevere le BPDU sulla VLAN-1501.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).