

瞭解ACI實施域驗證

目錄

[簡介](#)

[強制域驗證介紹](#)

[強制域驗證：停用（預設行為）](#)

[強制域驗證：已啟用](#)

[疑難排解](#)

[相關資訊](#)

簡介

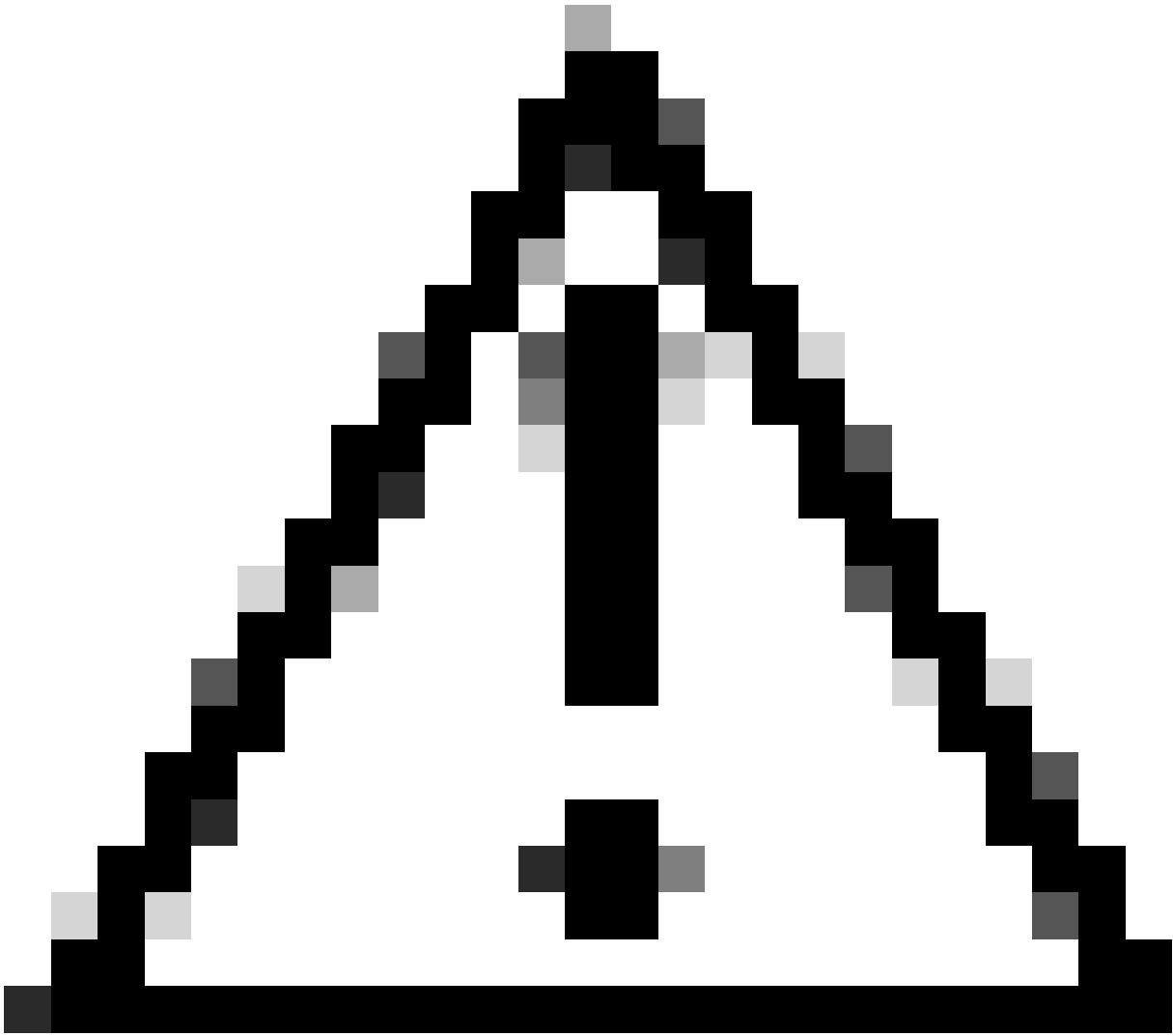
本檔案說明「強制網域驗證」設定及其優點。

強制域驗證介紹

預設情況下，不會啟用強制域驗證，因此，如果為EPG配置的靜態{port, VLAN}中不存在包含此VLAN的域，則會發生以下情況：

- 以應用為中心的基礎設施(ACI)引發F0467故障「Configuration failed for <path> due to Invalid Path Configuration」（由於無效的路徑配置）。
- Vlan部署在介面上。
- 流量在特定介面上轉發。

透過強制域驗證可以防止此配置錯誤。



警告：未經適當盡職調查，請勿在現有交換矩陣上啟用此功能。

此功能一旦啟用就無法停用。即使現有配置不正確，這些配置仍可正常工作。在啟用之前，請確保驗證對EPG和關聯的AEP的域分配。

強制域驗證：停用（預設行為）

APIC CLI實施域驗證驗證。預設狀態指示域驗證已停用。

```
<#root>
```

```
APIC# moquery -c infraSetPol | egrep "domainValidation"  
domainValidation :
```

```
no
```

假設encap vlan 420未繫結到與EPG關聯的域/AEP。Vlan 420仍在預期介面上部署。

<#root>

```
leaf# show vlan encap-id
```

```
420

extended
VLAN Name                               Encap          Ports
-----
1
  1c_TN:1c_APP:1c_EPG                   vlan-420
Eth1/13
```

部署用於EPG和BD的平台獨立(PI) Vlan (1,19) , 並允許它們在預期介面上建立中繼。

<#root>

```
"
VLAN Name                               Encap          Ports
-----
1
  1c_TN:1c_APP:1c_EPG                   vlan-420      Eth1/13
19
  1c_TN:1c_BD                           vxlan-16416666 Eth1/13
```

BD和EPG的VLAN部署在預期介面上。

<#root>

```
leaf# show int eth
```

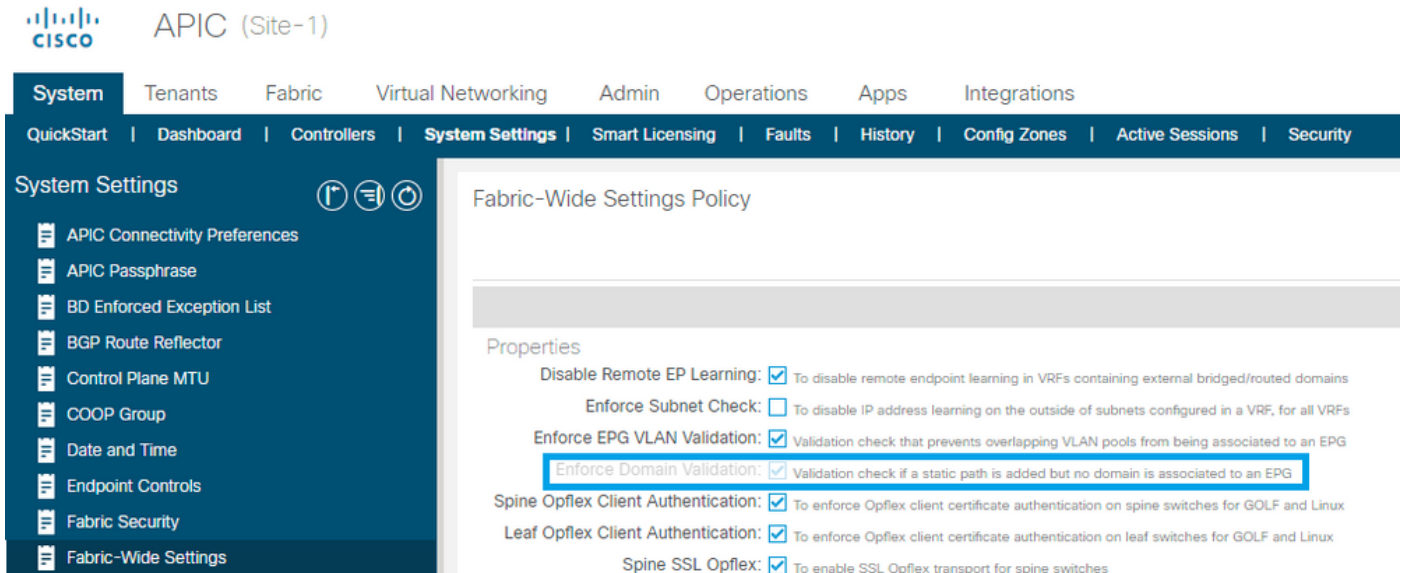
```
1/13

trunk | grep -A Allowed
Port          Vlans Allowed on Trunk
-----
Eth1/
13
  1,19
```

強制域驗證：已啟用

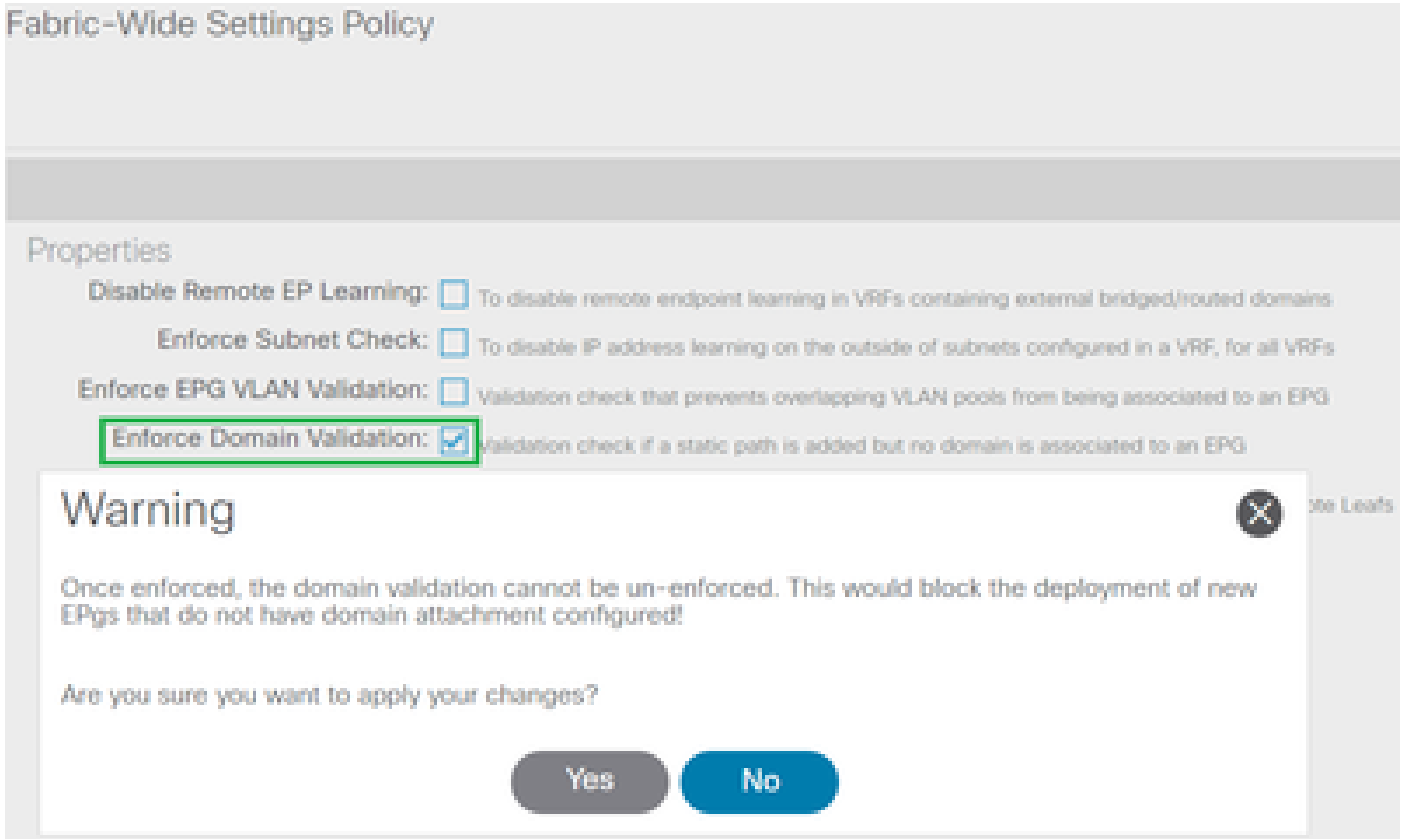
如果啟用了Enforce Domain Validation，則可以在EPG上建立靜態路徑，其VLAN ID未連結到各個訪問策略路徑。交換矩陣引發故障，並且介面上未對VLAN進行程式設計。

APIC GUI實施域驗證 System > System Settings > Enforce Domain Validation。



啟用強制域驗證

確認驗證警告



強制執行後，無法取消執行域驗證

啟用設定後，選項會變成灰色，因此您無法復原動作。

APIC CLI：實施域驗證驗證

```
<#root>
```

```
APIC# moquery -c infraSetPol | egrep "domainValidation"  
domainValidation      :  
  
yes
```

僅當必須將策略下載到交換機時，才會針對現有配置啟動此驗證。

通常，這種情況會在交換機升級、全新重新載入或快照/備份恢復配置時發生。

全新重新載入步驟範例：

```
<#root>
```

```
leaf#
```

```
acidiag touch clean
```

```
This command can wipe out this device, Proceed? [y/N] y  
leaf# reload
```

```
This command can reload the chassis, Proceed (y/n)? [n]: y
```

最初部署的VLAN 420此時不在預期介面上。

```
<#root>
```

```
leaf# show int eth
```

```
1/13
```

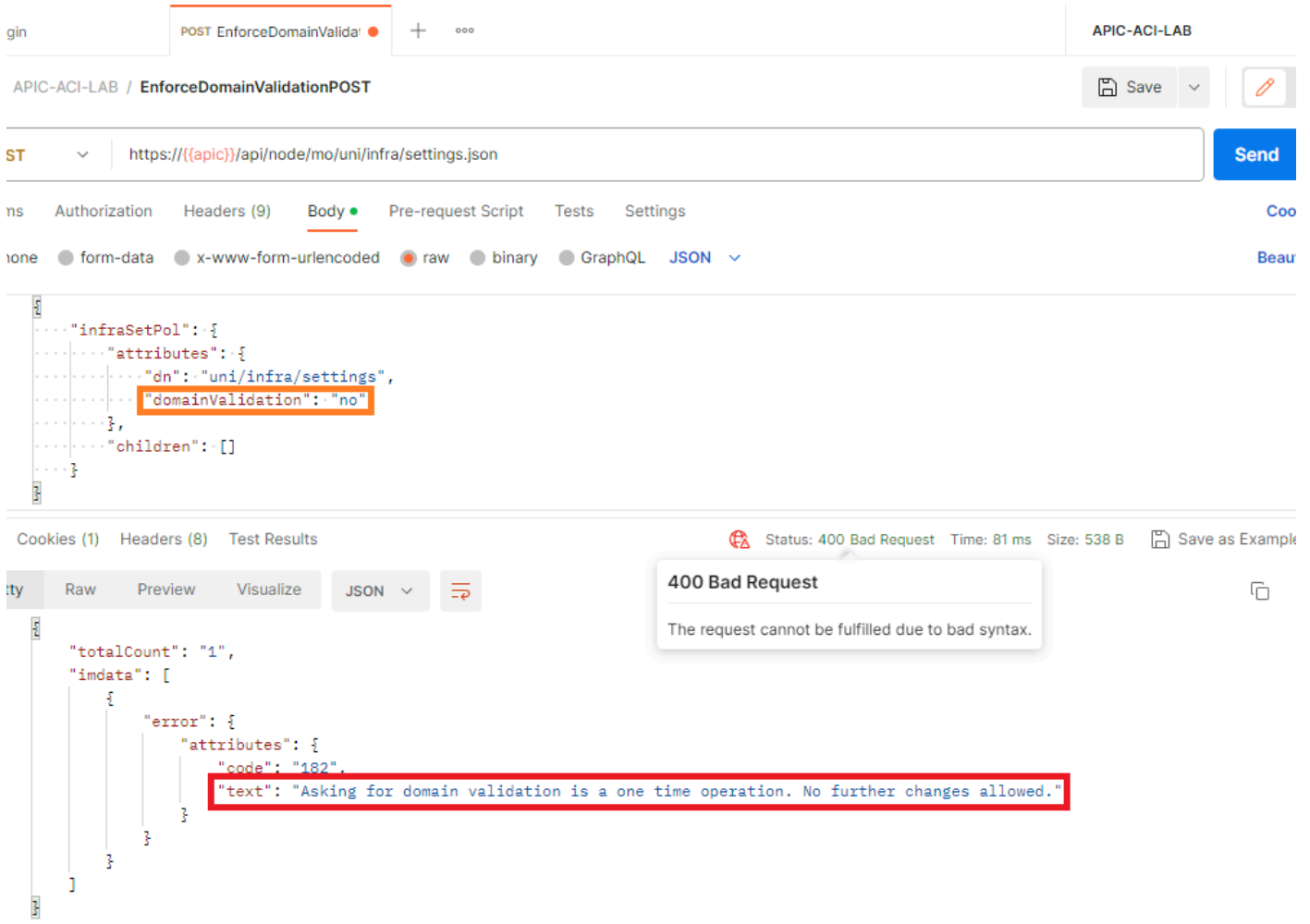
```
trunk | grep -A 2 Allowed  
Port      Vlans Allowed on Trunk
```

```
-----  
Eth1/13
```

```
none
```

啟用領域驗證被視為最佳實務，因此啟用之後，便沒有選項可還原變更。

POSTMAN API顯示更改設定的帖子不成功。



The screenshot shows a REST client interface with the following details:

- URL: `https://{{apic}}/api/node/mo/uni/infra/settings.json`
- Method: `POST`
- Request Body (JSON):

```
{  "infraSetPol": {    "attributes": {      "dn": "uni/infra/settings",      "domainValidation": "no"    },    "children": []  }}
```
- Status: `400 Bad Request` (Time: 81 ms, Size: 538 B)
- Response Body (JSON):

```
{  "totalCount": "1",  "imdata": [    {      "error": {        "attributes": {          "code": "182",          "text": "Asking for domain validation is a one time operation. No further changes allowed."        }      }    }  ]}
```

要求域驗證是一次性的操作。不允許進一步更改。

由於在初始發行期間，此設定不是預設設定，因此將來對預設設定的任何強制更改都會導致不正確的配置失敗，從而導致中斷。

由於這個原因，使用者可設定該設定。

疑難排解

對於缺少訪問策略關聯的受影響EPG，將引發F0467故障。

有關如何進行故障排除，請參閱本文的[快速入門隔離](#)。

相關資訊

- [地址ACI故障代碼F0467：invalid-vlan、invalid-path、encap-already-in-use](#)
- [設定ACI交換矩陣：初始設定配置示例>系統設定](#)
- [思科以應用為中心的基礎設施\(ACI\)設計手冊> EPG域驗證](#)

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）。