

# 了解ACI实施域验证

## 目录

---

[简介](#)

[实施域验证说明](#)

[强制域验证：禁用（默认行为）](#)

[强制域验证：已启用](#)

[故障排除](#)

[相关信息](#)

---

## 简介

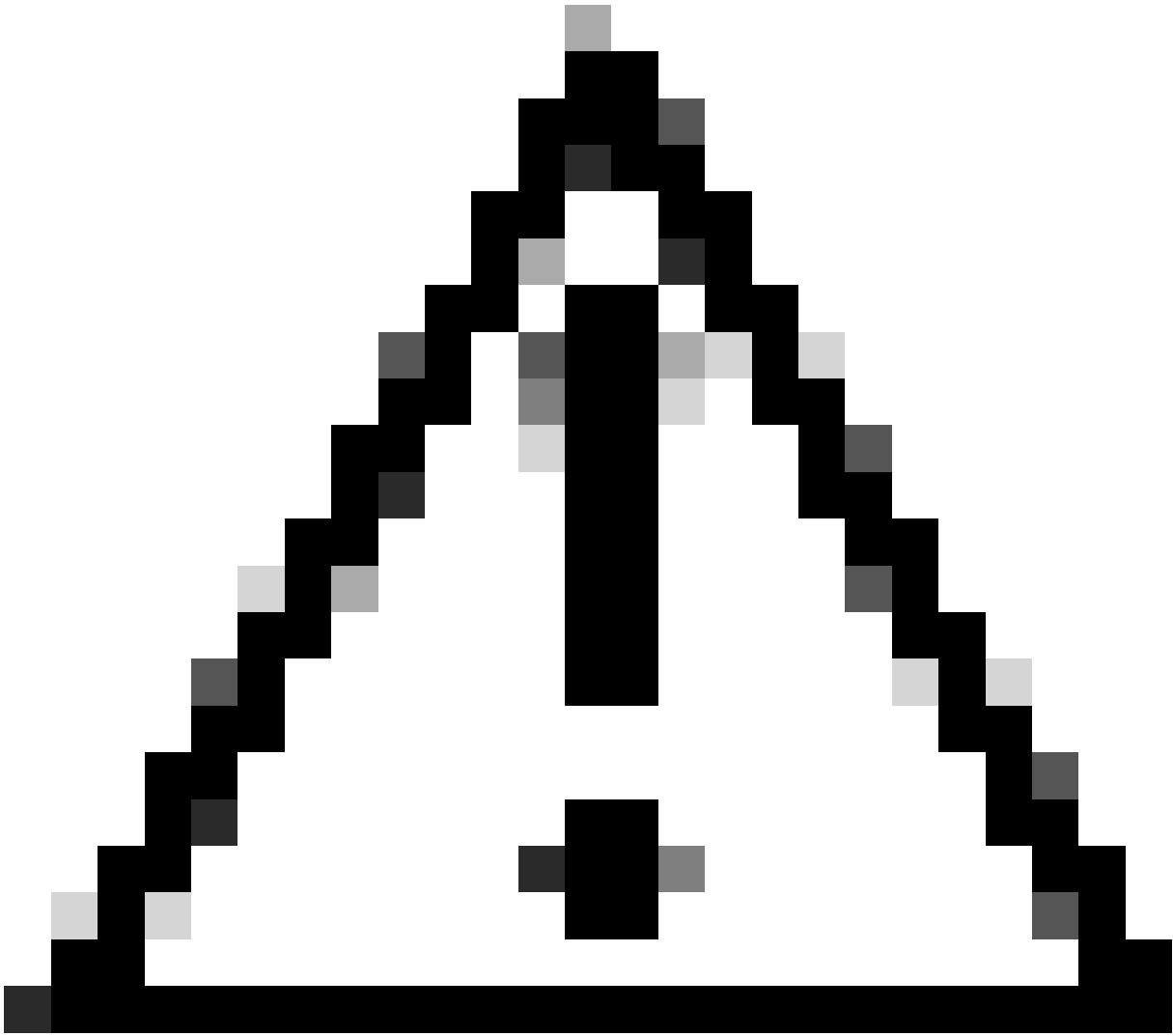
本文档介绍强制域验证设置及其优点。

## 实施域验证说明

默认情况下，Enforce Domain Validation未启用，因此，如果EPG配置了静态{port，VLAN}，但其中不存在包含此VLAN的域，则会发生以下情况：

- 以应用为中心的基础设施(ACI)引发故障F0467“Configuration failed for <path> due to Invalid Path Configuration”。
- Vlan部署在接口上。
- 流量在特定接口上转发。

此错误配置可以通过实施域验证来避免。



注意：未经适当的尽职调查，请勿在现有交换矩阵上启用此功能。

---

启用此功能后，无法将其禁用。即使现有配置不正确，它们也可以正常工作。在启用之前，请确保验证到EPG和关联AEP的域分配。

## 强制域验证：禁用（默认行为）

APIC CLI实施域验证验证。默认状态指示域验证已禁用。

```
<#root>
```

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

```
no
```

假设封装vlan 420未绑定到与EPG关联的域/AEP。Vlan 420仍在预期接口上部署。

<#root>

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

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

部署用于EPG和BD的独立于平台(PI)的Vlan (1,19)并允许其在预期接口上中继。

<#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部署在预期接口上。

<#root>

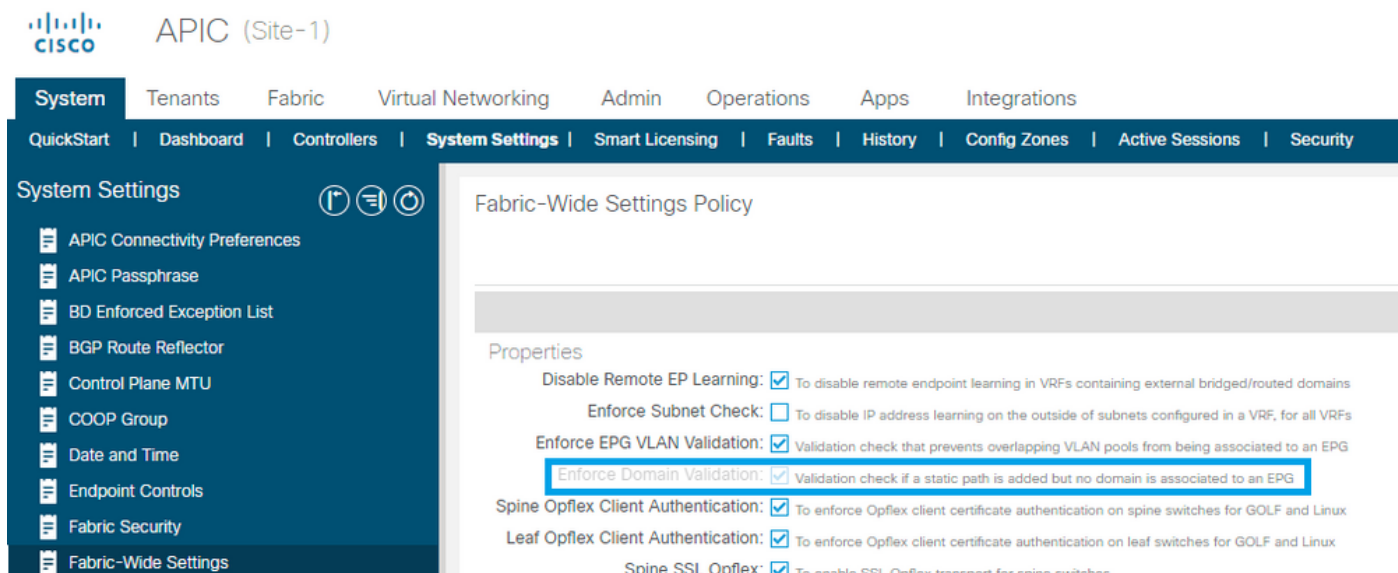
```
leaf# show int eth
```

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

## 强制域验证：已启用

如果启用了Enforce Domain Validation，则可以在EPG上创建静态路径，其VLAN ID不链接到各个访问策略路径。交换矩阵引发故障，并且接口上未对VLAN进行编程。

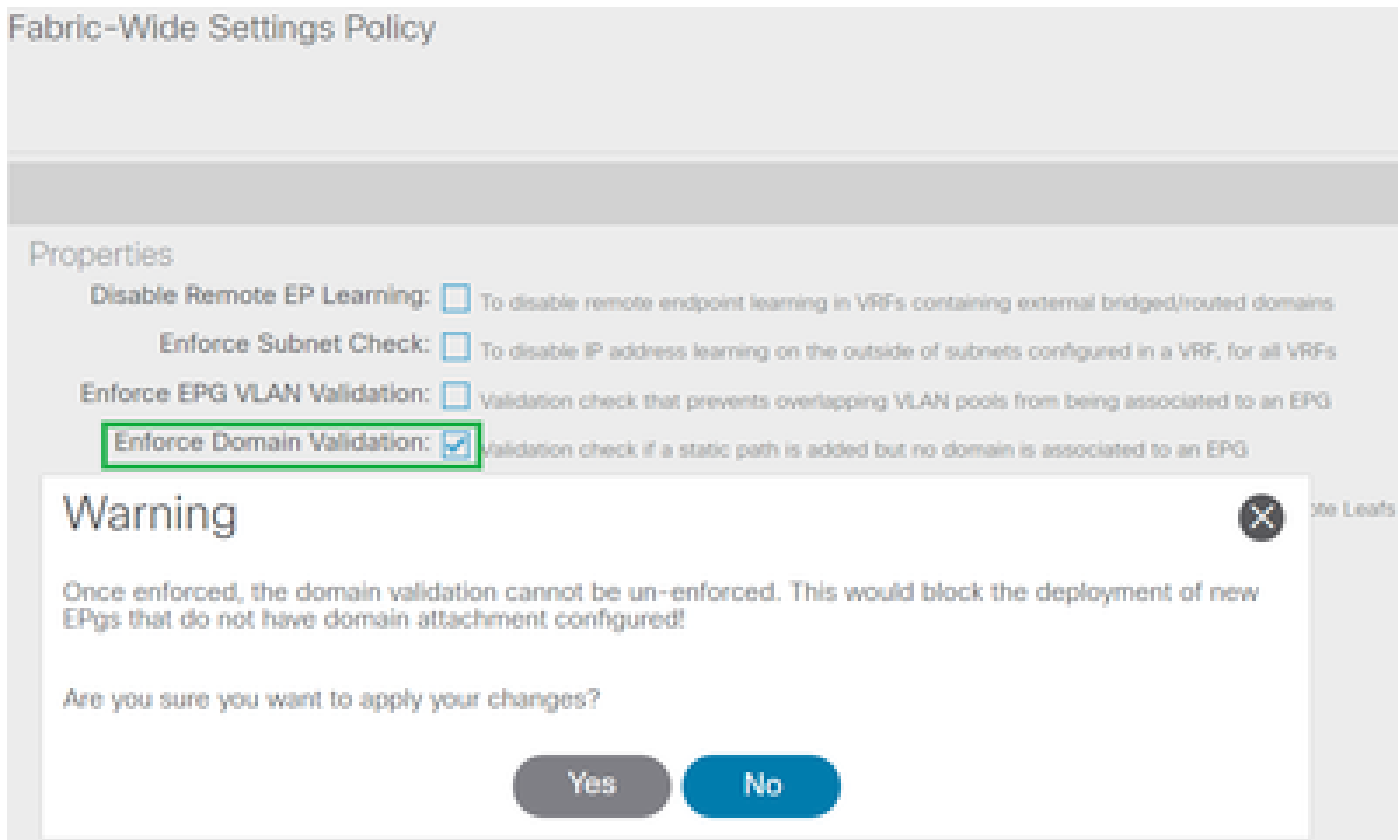
APIC GUI实施域验证验证System > System Settings > Enforce Domain Validation。



The screenshot shows the APIC (Site-1) interface. The left sidebar contains 'System Settings' with a sub-menu 'Fabric-Wide Settings'. The main content area is titled 'Fabric-Wide Settings Policy' and shows a 'Properties' section with several checkboxes. The 'Enforce Domain Validation' checkbox is checked and highlighted with a blue box. Other checkboxes include 'Disable Remote EP Learning', 'Enforce Subnet Check', 'Enforce EPG VLAN Validation', 'Spine Opflex Client Authentication', 'Leaf Opflex Client Authentication', and 'Spine SSL Opflex'.

已启用强制域验证

## 确认验证警告



The screenshot shows the 'Fabric-Wide Settings Policy' page with a 'Warning' dialog box open. The dialog box has a title 'Warning' and a close button. The text inside the dialog reads: 'Once enforced, the domain validation cannot be un-enforced. This would block the deployment of new EPGs that do not have domain attachment configured!' and 'Are you sure you want to apply your changes?'. There are two buttons at the bottom: 'Yes' and 'No'.

实施后，将无法取消实施域验证

启用设置后，该选项将灰显，因此您无法撤消操作。

APIC CLI：实施域验证验证

```
<#root>
```

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

仅当必须将策略下载到交换机时，此验证才会对现有配置生效。

通常，这可能发生在交换机升级、全新重新加载或配置快照/备份恢复期间。

全新重新加载步骤示例：

```
<#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此时不在预期的接口上。

```
<#root>
```

```
leaf# show int eth
```

```
1/13
```

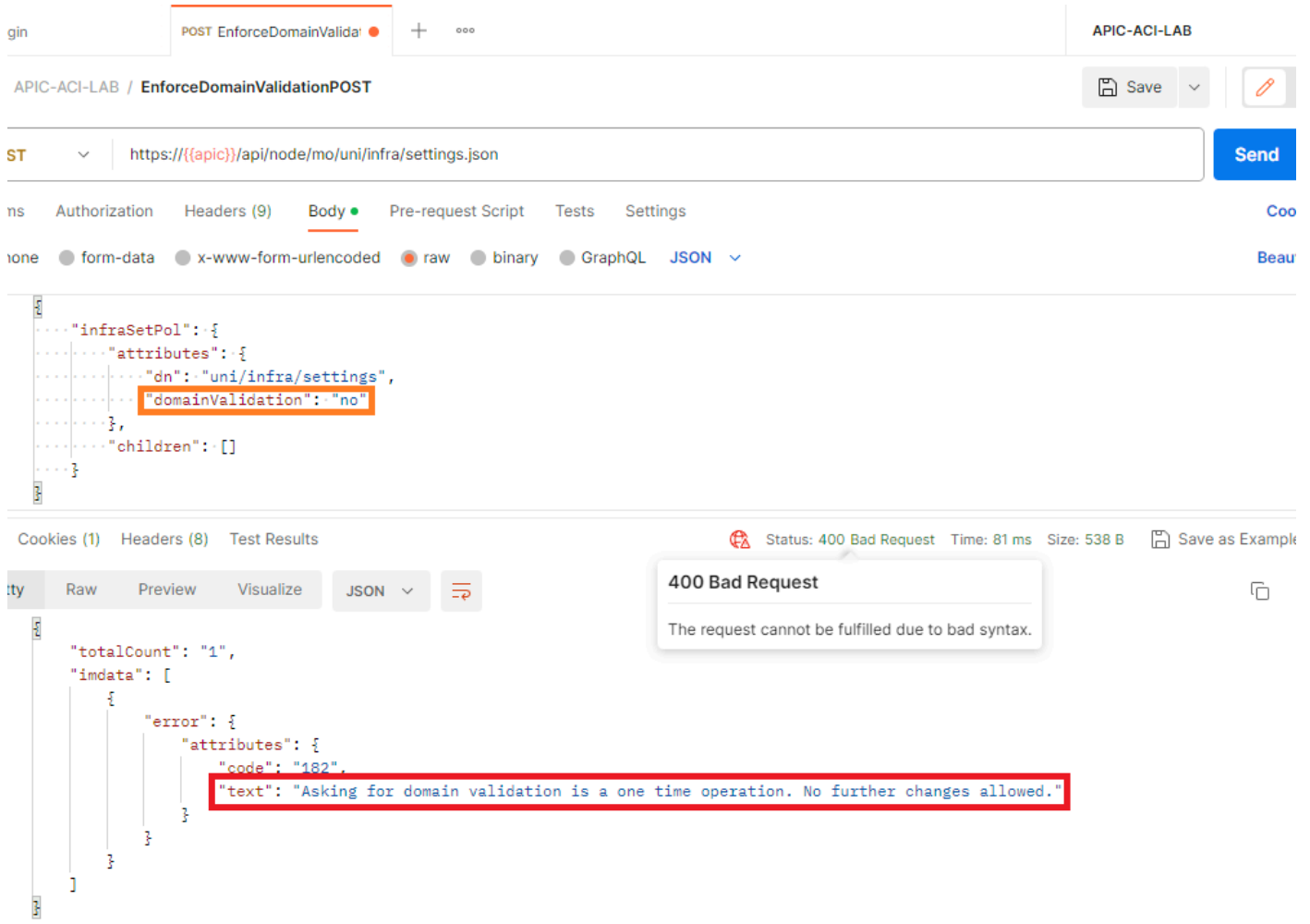
```
trunk | grep -A 2 Allowed  
Port          Vlans Allowed on Trunk
```

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

```
none
```

启用域验证被视为最佳实践，因此启用该功能后，将无法恢复更改。

POSTMAN API显示post以更改设置不成功。



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

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

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

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

请求域验证是一次性操作。不允许进一步更改。

由于此设置不是初始版本期间的默认设置，因此将来在默认设置中执行的任何更改都可能导致不正确的配置失败，从而导致中断。

因此，此设置可由用户配置。

## 故障排除

如果受影响的EPG缺少访问策略关联，则会引发故障F0467。

有关如何进行故障排除，请参阅本文的[快速入门隔离](#)。

## 相关信息

- [地址ACI故障代码F0467：invalid-vlan、invalid-path、encap-already-in-use](#)
- [设置ACI交换矩阵：初始设置配置示例>系统设置](#)
- [思科以应用为中心的基础设施\(ACI\)设计指南> EPG域验证](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。