

Comprensión de ACI Exigir validación de dominio

Contenido

[Introducción](#)

[Explicación de aplicación de validación de dominio](#)

[Aplicar validación de dominio: deshabilitado \(comportamiento predeterminado\)](#)

[Aplicar validación de dominio: habilitado](#)

[Resolución de problemas](#)

[Información Relacionada](#)

Introducción

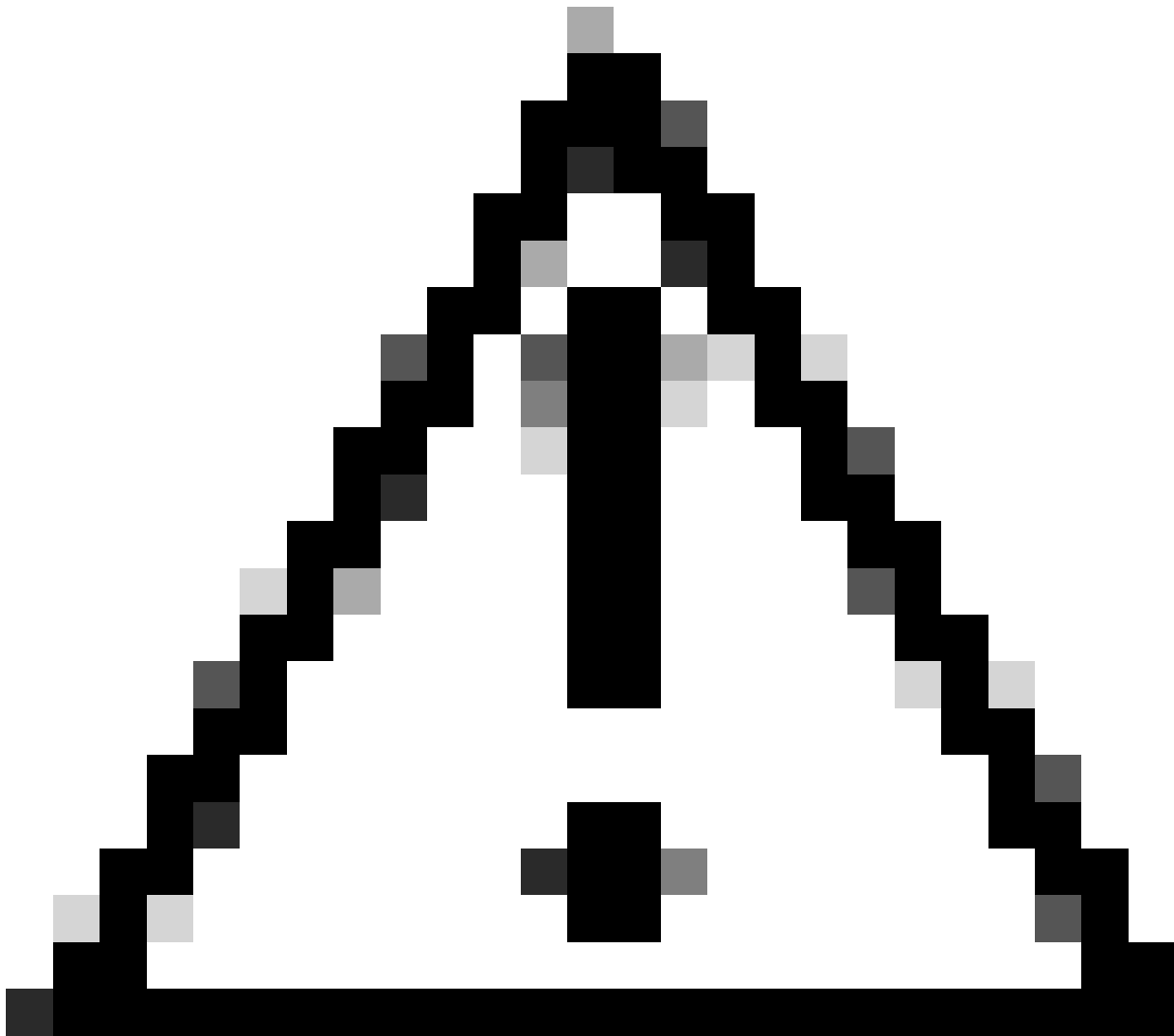
Este documento describe la configuración de Aplicar validación de dominio y sus ventajas.

Explicación de aplicación de validación de dominio

De forma predeterminada, la aplicación de validación de dominio no está habilitada, por lo que si un EPG está configurado con un {port, VLAN} estático en el que no hay un dominio que contenga esta VLAN, sucede lo siguiente:

- Application Centric Infrastructure (ACI) provoca el fallo F0467 "Error de configuración para <path> debido a una configuración de ruta no válida".
- La VLAN se implementa en la interfaz.
- El tráfico se reenvía en la interfaz específica.

Este error de configuración se puede evitar mediante la aplicación de la validación de dominio.



Precaución: NO HABILITE ESTA FUNCIÓN EN UN FABRIC EXISTENTE SIN LA DILIGENCIA DEBIDA.

Esta función no se puede desactivar una vez que la haya activado. Puede tener configuraciones existentes que funcionaban aunque fueran incorrectas. Antes de habilitarlo, asegúrese de verificar la asignación de dominio a los EPG y los AEP asociados.

Aplicar validación de dominio: deshabilitado (comportamiento predeterminado)

APIC CLI Exige la verificación de validación de dominio. El estado predeterminado indica que la validación del dominio está deshabilitada.

<#root>

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

```
domainValidation      :
```

```
no
```

Suponga que encap vlan 420 no está vinculado al dominio/AEP asociado al EPG. Vlan 420 todavía está implementado en la interfaz esperada.

```
<#root>
```

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

```
420
```

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

Las VLAN independientes de la plataforma (PI) (1,19) para EPG y BD se implementan y se les permite establecer enlaces troncales en la interfaz esperada.

```
<#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
```

Las VLAN para BD y EPG se implementan en la interfaz esperada.

```
<#root>
```

```
leaf# show int eth
```

```
1/13
```

```
trunk | grep -A Allowed
Port          Vlans Allowed on Trunk
-----
Eth1/
```

Aplicar validación de dominio: habilitado

Si se habilita la aplicación de validación de dominio, puede crear una ruta estática en un EPG con un ID de VLAN que no esté vinculado a la ruta de la política de acceso correspondiente. El entramado genera un fallo y la VLAN NO está programada en la interfaz.

GUI de APIC Aplicación de validación de dominio System > System Settings > Enforce Domain Validation.

The screenshot shows the APIC (Site-1) GUI. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'Admin', 'Operations', 'Apps', and 'Integrations'. Below this is a secondary navigation bar with 'QuickStart', 'Dashboard', 'Controllers', 'System Settings', 'Smart Licensing', 'Faults', 'History', 'Config Zones', 'Active Sessions', and 'Security'. The left sidebar is titled 'System Settings' and lists various configuration options, with 'Fabric-Wide Settings' selected. The main content area is titled 'Fabric-Wide Settings Policy' and shows a 'Properties' section with several settings:

- Disable Remote EP Learning: To disable remote endpoint learning in VRFs containing external bridged/routed domains
- Enforce Subnet Check: To disable IP address learning on the outside of subnets configured in a VRF, for all VRFs
- Enforce EPG VLAN Validation: Validation check that prevents overlapping VLAN pools from being associated to an EPG
- Enforce Domain Validation: Validation check if a static path is added but no domain is associated to an EPG**
- Spine Opflex Client Authentication: To enforce Opflex client certificate authentication on spine switches for GOLF and Linux
- Leaf Opflex Client Authentication: To enforce Opflex client certificate authentication on leaf switches for GOLF and Linux
- Spine SSL Opflex: To enable SSL Opflex transport for spine switches

Habilitado Aplicar validación de dominio

Advertencia de verificación de confirmación

Fabric-Wide Settings Policy

Properties

Disable Remote EP Learning: To disable remote endpoint learning in VRFs containing external bridged/routed domains

Enforce Subnet Check: To disable IP address learning on the outside of subnets configured in a VRF, for all VRFs

Enforce EPG VLAN Validation: Validation check that prevents overlapping VLAN pools from being associated to an EPG

Enforce Domain Validation: Validation check if a static path is added but no domain is associated to an EPG

Warning

Once enforced, the domain validation cannot be un-enforced. This would block the deployment of new EPGs that do not have domain attachment configured!

Are you sure you want to apply your changes?

Yes

No

Una vez aplicada, la validación de dominio no se puede anular

Una vez habilitada la configuración, la opción aparece atenuada para que no pueda deshacer la acción.

APIC CLI: aplicación de la verificación de validación de dominio

```
<#root>
```

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

```
yes
```

Esta validación se inicia para la configuración existente SOLAMENTE cuando la política tiene que ser descargada al switch.

Normalmente, esto puede ocurrir durante una actualización de switch, una recarga limpia o una restauración de instantánea/copia de seguridad de la configuración.

Ejemplo de un paso de recarga limpia:

```
<#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

La VLAN 420, que se implementó originalmente, NO se encuentra en la interfaz esperada en este momento.

<#root>

leaf# show int eth

1/13

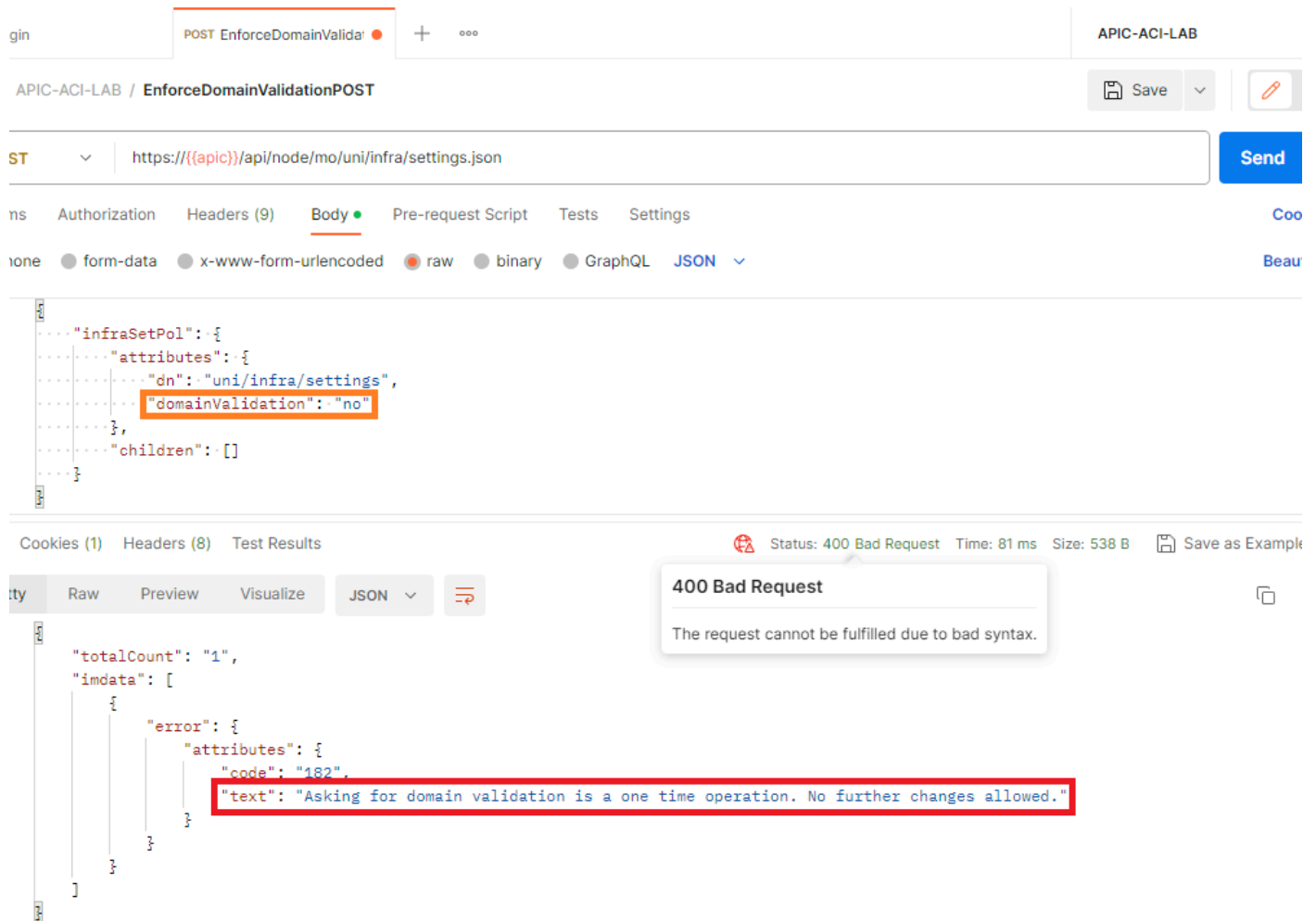
```
trunk | grep -A 2 Allowed
Port      Vlans Allowed on Trunk
```

Eth1/13

none

La habilitación de la validación de dominio se considera una práctica recomendada, por lo que una vez habilitada, no existe la opción de revertir el cambio.

Una API POSTMAN muestra que la publicación para cambiar la configuración no se ha realizado correctamente.



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."        }      }    }  ]}
```

Solicitar la validación de dominio es una operación única. No Se Permiten Más Cambios.

Debido a que esta configuración no era predeterminada durante la versión inicial, cualquier cambio futuro que se exija en la configuración predeterminada puede hacer que falle una configuración incorrecta, lo que provoca interrupciones.

Por este motivo, el usuario puede configurar el parámetro.

Resolución de problemas

El error F0467 se genera para los EPG afectados con asociaciones de políticas de acceso faltantes.

Consulte este artículo [Quick Start Isolation](#) sobre cómo solucionar el problema.

Información Relacionada

- [Dirección Código de error de ACI F0467: invalid-vlan, invalid-path, encap-already-in-use](#)
- [Configuración de un fabric de ACI: Ejemplo de configuración inicial > Configuración del sistema](#)
- [Guía de diseño de Cisco Application Centric Infrastructure \(ACI\) > Validación de dominios EPG](#)

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).