

ACI durchsetzen Domänenvalidierung

Inhalt

[Einleitung](#)

[Domänenvalidierung erzwingen erklärt](#)

[Domänenvalidierung erzwingen: Deaktiviert \(Standardverhalten\)](#)

[Domänenvalidierung durchsetzen: Aktiviert](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

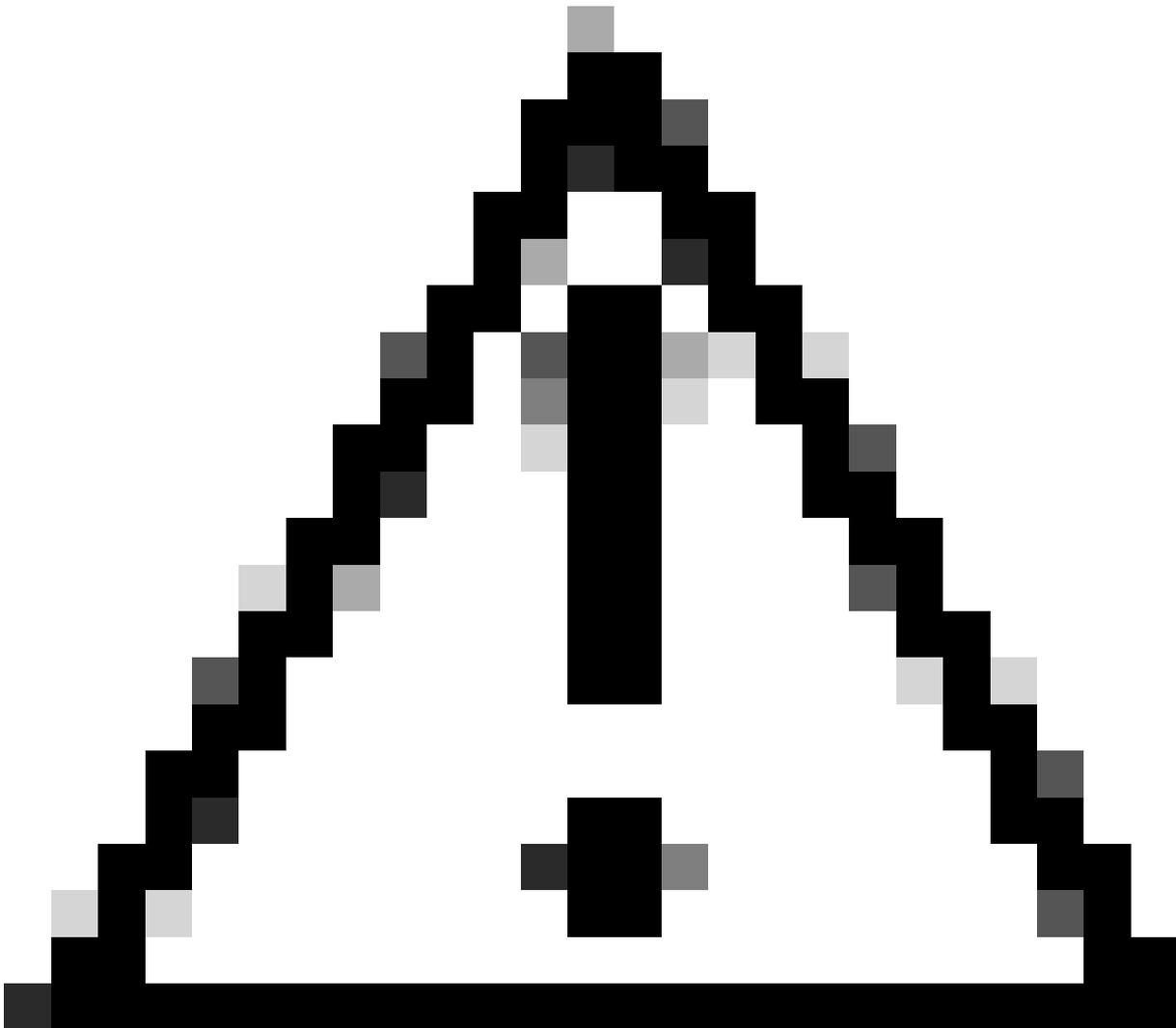
In diesem Dokument werden die Einstellung zur Domänenvalidierung erzwingen und ihre Vorteile beschrieben.

Domänenvalidierung erzwingen erklärt

Standardmäßig ist die Domänenvalidierung erzwingen nicht aktiviert. Wenn also eine EPG mit einem statischen {port, VLAN} konfiguriert ist, in dem keine Domäne mit diesem VLAN vorhanden ist, geschieht Folgendes:

- Die Application Centric Infrastructure (ACI) löst den Fehler F0467 aus: "Die Konfiguration für <path> ist aufgrund der ungültigen Pfadkonfiguration fehlgeschlagen."
- VLAN wird auf der Schnittstelle bereitgestellt.
- Der Datenverkehr wird über die spezifische Schnittstelle weitergeleitet.

Diese Fehlkonfiguration kann durch Erzwingen der Domänenvalidierung verhindert werden.



Vorsicht: AKTIVIEREN SIE DIESE FUNKTION NICHT OHNE ANGEMESSENE SORGFALT AUF EINER VORHANDENEN FABRIC.

Diese Funktion kann nicht deaktiviert werden, nachdem sie aktiviert wurde. Bestehende Konfigurationen können funktionsfähig sein, selbst wenn sie falsch waren. Überprüfen Sie vor der Aktivierung die Domänenzuweisung zu den EPGs und den zugehörigen AEPs.

Domänenvalidierung erzwingen: Deaktiviert (Standardverhalten)

APIC CLI erzwingt Überprüfung der Domänenvalidierung. Der Standardstatus gibt an, dass die Domänenvalidierung deaktiviert ist.

```
<#root>
```

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

```
no
```

Angenommen, das encap-VLAN 420 ist nicht an die Domäne/den AEP gebunden, die/der mit der EPG verknüpft ist. VLAN 420 wird weiterhin auf der erwarteten Schnittstelle bereitgestellt.

<#root>

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

420

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

Platform Independent (PI) VLANs (1, 19) für EPG und BD werden bereitgestellt und dürfen an der erwarteten Schnittstelle Trunks senden.

<#root>

```
"
VLAN Name                               Encap          Ports
-----
1
  1c_TN:1c_APP:1c_EPG                   vlan-420      Eth1/13
19
  1c_TN:1c_BD                           vxlan-1641666 Eth1/13
```

VLANs für BD und EPG werden auf der erwarteten Schnittstelle bereitgestellt.

<#root>

```
leaf# show int eth
```

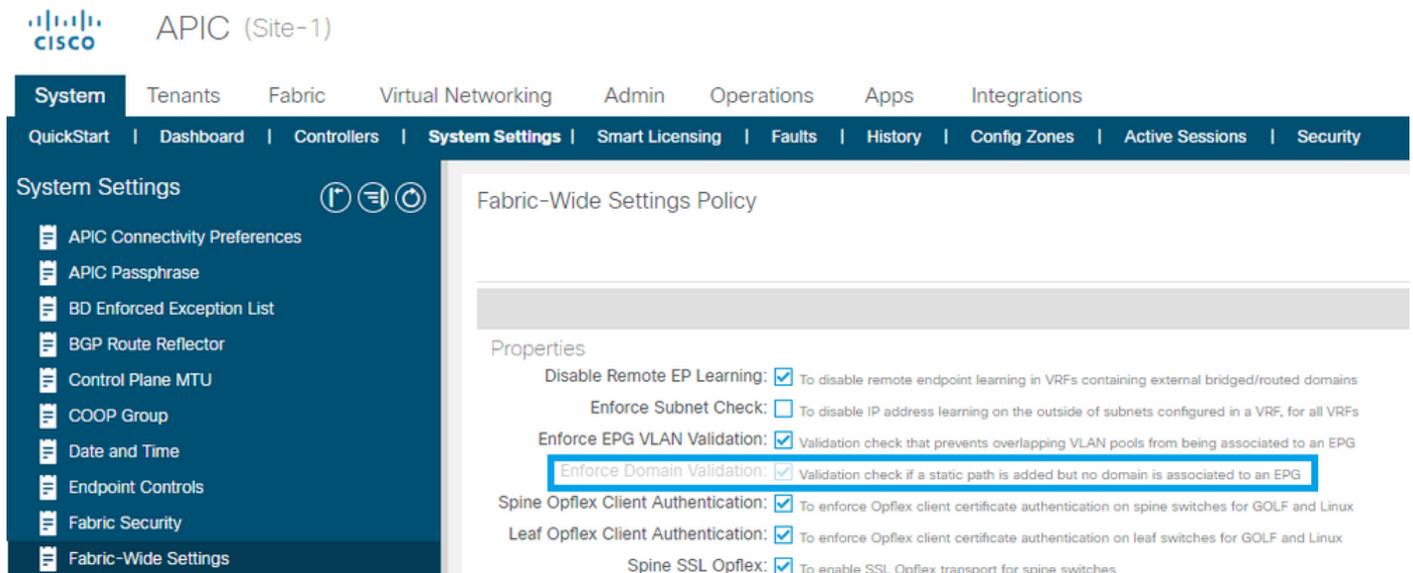
1/13

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

Domänenvalidierung durchsetzen: Aktiviert

Wenn die Domänenvalidierung erzwingen aktiviert ist, können Sie einen statischen Pfad auf einer EPG mit einer VLAN-ID erstellen, die nicht mit dem entsprechenden Zugriffsrichtlinienpfad verknüpft ist. Die Fabric löst einen Fehler aus, und das VLAN ist auf der Schnittstelle NICHT programmiert.

APIC-GUI - Überprüfen der Domänenvalidierung System > Systemeinstellungen > Domänenvalidierung erzwingen.



The screenshot shows the APIC (Site-1) interface. The left sidebar contains the 'System Settings' menu with 'Fabric-Wide Settings' selected. The main content area displays the 'Fabric-Wide Settings Policy' configuration. Under the 'Properties' section, the following settings are visible:

- 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

Domänenvalidierung erzwingen

Bestätigung der Verifizierung

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

Nach der Erzwingung kann die Domänenvalidierung nicht mehr rückgängig gemacht werden.

Wenn die Einstellung aktiviert ist, ist die Option ausgegraut, sodass Sie die Aktion nicht rückgängig machen können.

APIC CLI: Überprüfung der Domänenvalidierung erzwingen

```
<#root>
```

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

```
yes
```

Diese Validierung tritt NUR dann für die bestehende Konfiguration in Kraft, wenn die Richtlinie auf den Switch heruntergeladen werden muss.

In der Regel kann dies bei einem Switch-Upgrade, einem sauberen Neuladen oder einer Snapshot-/Backup-Wiederherstellung der Konfiguration der Fall sein.

Beispiel für einen sauberen Neuladeschritt:

```
<#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

VLAN 420, das ursprünglich bereitgestellt wurde, befindet sich derzeit NICHT auf der erwarteten Schnittstelle.

<#root>

leaf# show int eth

1/13

trunk		grep -A 2 Allowed
Port		Vlans Allowed on Trunk

Eth1/13

none

Die Aktivierung der Domänenvalidierung wird als Best Practice erachtet. Nach der Aktivierung gibt es keine Option zum Zurücksetzen der Änderung.

Eine POSTMAN-API zeigt an, dass der Beitrag zum Ändern der Einstellung nicht erfolgreich ist.

The screenshot shows a REST client interface for a POST request to `https://{{apic}}/api/node/mo/uni/infra/settings.json`. The request body is a JSON object with the following structure:

```
... "infraSetPol": {
  "attributes": {
    "dn": "uni/infra/settings",
    "domainValidation": "no"
  },
  "children": []
}
```

The response is a 400 Bad Request with the following JSON body:

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

A tooltip for the 400 Bad Request status reads: "The request cannot be fulfilled due to bad syntax."

Die Domänenvalidierung ist nur einmal erforderlich. Weitere Änderungen sind nicht zulässig.

Da diese Einstellung in der ersten Version keine Standardeinstellung war, kann jede erzwungene Änderung in der Standardeinstellung dazu führen, dass eine falsche Konfiguration fehlschlägt, was zu Ausfällen führt.

Aus diesem Grund ist die Einstellung vom Benutzer konfigurierbar.

Fehlerbehebung

Der Fehler F0467 wird für betroffene EPGs mit fehlenden Zugriffsrichtlinienzuordnungen ausgelöst.

[Schnellstartisolierung](#) zur Fehlerbehebung in diesem Artikel.

Zugehörige Informationen

- [Adresse ACI-Fehlercode F0467: invalid-vlan, invalid-path, encap-already-in-use](#)
- [Einrichten einer ACI-Fabric: Konfigurationsbeispiel für die Ersteinrichtung > Systemeinstellungen](#)
- [Cisco Application Centric Infrastructure \(ACI\) - Designleitfaden > Validierung von EPG-Domänen](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.