

Informazioni su ACI Enforce Domain Validation

Sommario

[Introduzione](#)

[Spiegazione dell'applicazione della convalida del dominio](#)

[Applica convalida dominio: disabilitato \(comportamento predefinito\)](#)

[Applica convalida dominio: abilitata](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

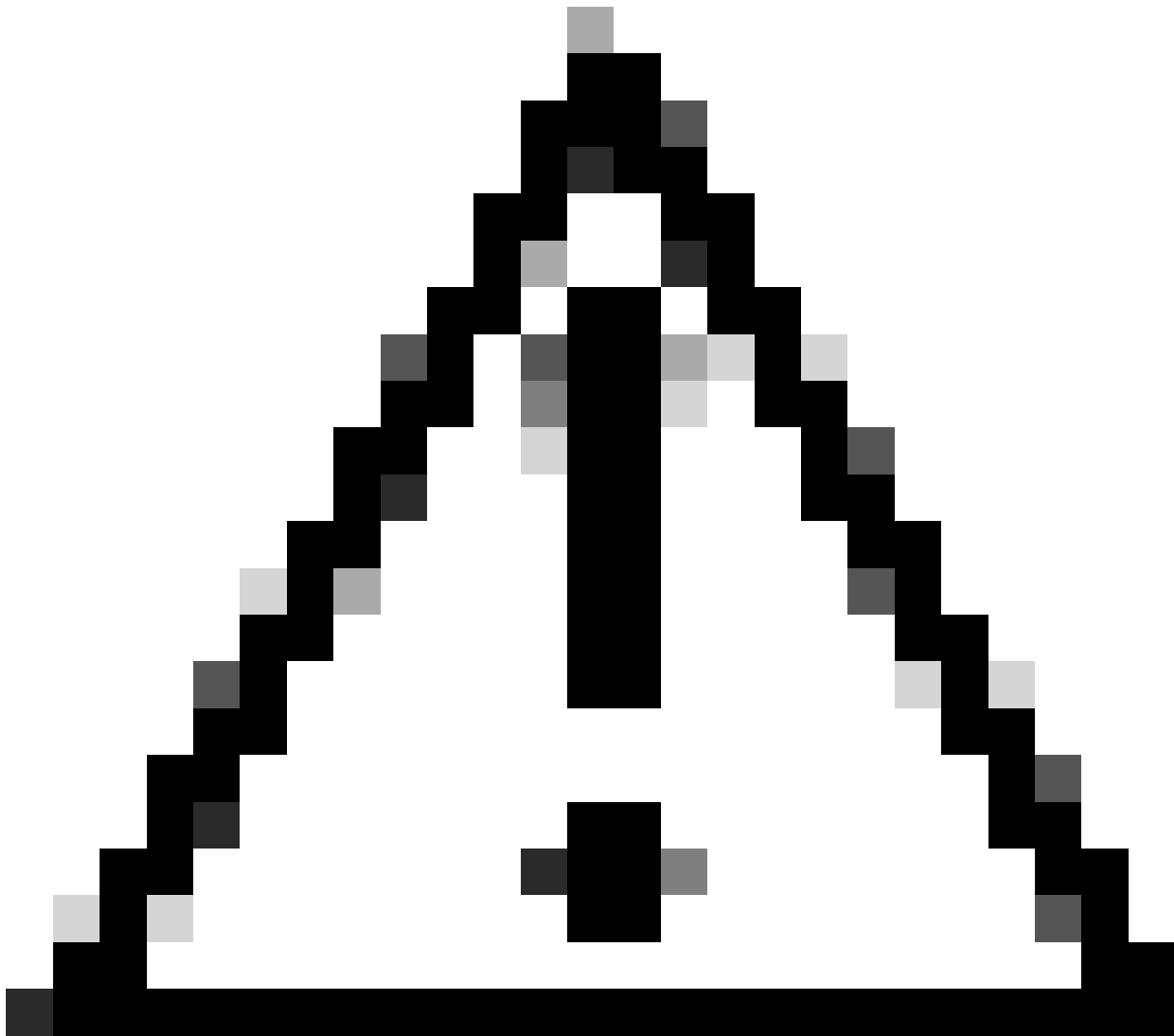
In questo documento viene descritta l'impostazione Applica convalida dominio e i relativi vantaggi.

Spiegazione dell'applicazione della convalida del dominio

Per impostazione predefinita, l'opzione Imponi convalida dominio non è abilitata, quindi se un EPG è configurato con una {port, VLAN} statica in cui non è presente un dominio contenente questa VLAN, si verifica quanto segue:

- ACI (Application Centric Infrastructure) genera l'errore F0467 "Configurazione non riuscita per <percorso> a causa di una configurazione del percorso non valida".
- La VLAN è distribuita sull'interfaccia.
- Il traffico viene inoltrato sull'interfaccia specifica.

È possibile impedire questa configurazione errata applicando la convalida del dominio.



ATTENZIONE: NON ABILITARE QUESTA FUNZIONE SU UN FABRIC ESISTENTE SENZA LA DOVUTA DILIGENZA.

Una volta attivata, la funzionalità non può essere disattivata. È possibile che le configurazioni esistenti funzionino anche se non sono corrette. Prima di abilitarla, verificare l'assegnazione del dominio agli EPG e agli AEP associati.

Applica convalida dominio: disabilitato (comportamento predefinito)

APIC CLI Applica la verifica della convalida del dominio. Lo stato predefinito indica che la convalida del dominio è disattivata.

<#root>

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

```
domainValidation      :
no
```

Si supponga che la vlan 420 dell'encap non sia collegata al dominio/AEP associato all'EPG. La VLAN 420 è ancora implementata sull'interfaccia prevista.

```
<#root>
```

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

```
420
```

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

Le Vlan IP (Platform Independent) (1,19) per EPG e BD vengono distribuite e possono essere trunk sull'interfaccia prevista.

```
<#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
```

Le Vlan per BD ed EPG sono installate sull'interfaccia prevista.

```
<#root>
```

```
leaf# show int eth
```

```
1/13
```

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

Applica convalida dominio: abilitata

Se l'opzione Applica convalida dominio è abilitata, è possibile creare un percorso statico su un EPG con un ID VLAN non collegato al rispettivo percorso dei criteri di accesso. La struttura genera un errore e la VLAN NON è programmata sull'interfaccia.

GUI APIC applicazione della convalida del dominio verifica System > System Settings > Enforce Domain Validation.

The screenshot shows the APIC (Site-1) interface. 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 checkboxes:

- 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

Abilitato Applica convalida dominio

Avviso verifica conferma

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 volta applicata, la convalida del dominio non può essere annullata

Una volta attivata l'impostazione, l'opzione è disattivata e non è possibile annullare l'operazione.

CLI APIC: Applica verifica convalida dominio

```
<#root>
```

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

```
yes
```

Questa convalida attiva la configurazione esistente SOLO quando il criterio deve essere scaricato sullo switch.

In genere, ciò può verificarsi durante un aggiornamento dello switch, un ricaricamento pulito o un ripristino della configurazione tramite snapshot/backup.

Esempio di un passo di ricaricamento:

```
<#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, originariamente implementata, NON è al momento sull'interfaccia prevista.

```
<#root>
```

```
leaf# show int eth
```

```
1/13
```

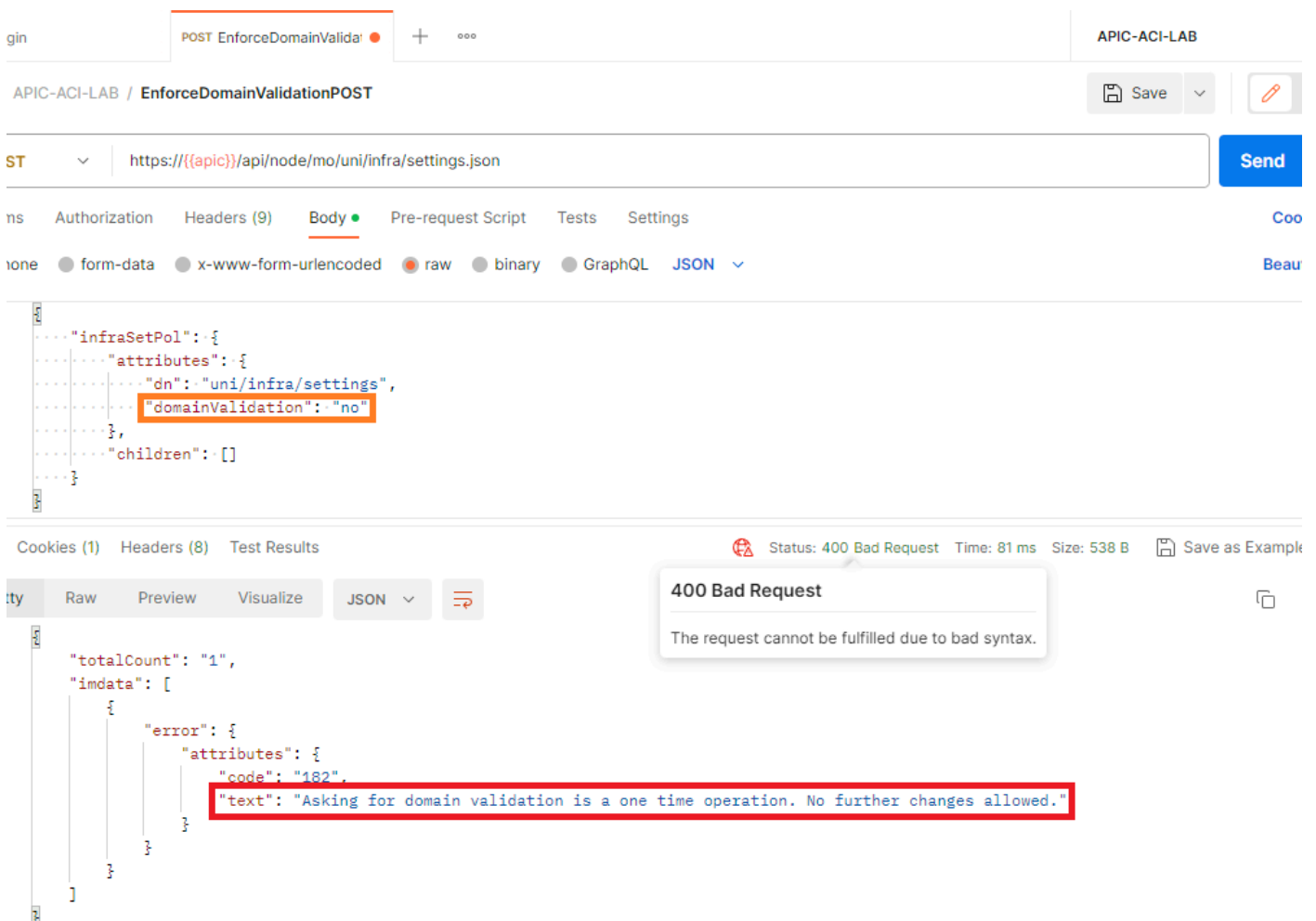
```
trunk | grep -A 2 Allowed
Port          Vlans Allowed on Trunk
```

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

```
none
```

L'abilitazione della convalida del dominio è considerata una procedura consigliata, pertanto una volta abilitata, non è possibile annullare la modifica.

Un'API POSTMAN indica che il post per la modifica dell'impostazione non è riuscito.



The screenshot shows a Postman interface for a REST client. The request is a POST 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 `"domainValidation": "no"` field is highlighted with a red box. The response status is `400 Bad Request` with a time of 81 ms and a size of 538 B. The response body is a JSON object with the following structure:

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

The `"text": "Asking for domain validation is a one time operation. No further changes allowed."` field is highlighted with a red box. A tooltip for the `400 Bad Request` status indicates: "The request cannot be fulfilled due to bad syntax."

La richiesta di convalida del dominio è un'operazione singola. Non Sono Consentite Ulteriori Modifiche.

Poiché questa impostazione non era un'impostazione predefinita durante la release iniziale, qualsiasi modifica applicata in futuro nell'impostazione predefinita può causare errori di configurazione errata, con conseguenti interruzioni.

Per questo motivo, l'impostazione è configurabile dall'utente.

Risoluzione dei problemi

L'errore F0467 viene generato per gli EPG interessati con associazioni di criteri di accesso mancanti.

Fare riferimento a questo articolo [Quick Start Isolation](#) su come risolvere il problema.

Informazioni correlate

- [Codice errore ACI indirizzo F0467: vlan non valida, percorso non valido, crittografia già in uso](#)
- [Impostazione di un'infrastruttura ACI: esempio di configurazione iniziale > Impostazioni di sistema](#)
- [Guida alla progettazione di Cisco Application Centric Infrastructure \(ACI\) > Convalida dominio EPG](#)

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).