ACI強制ドメイン検証について

内容

はじめに

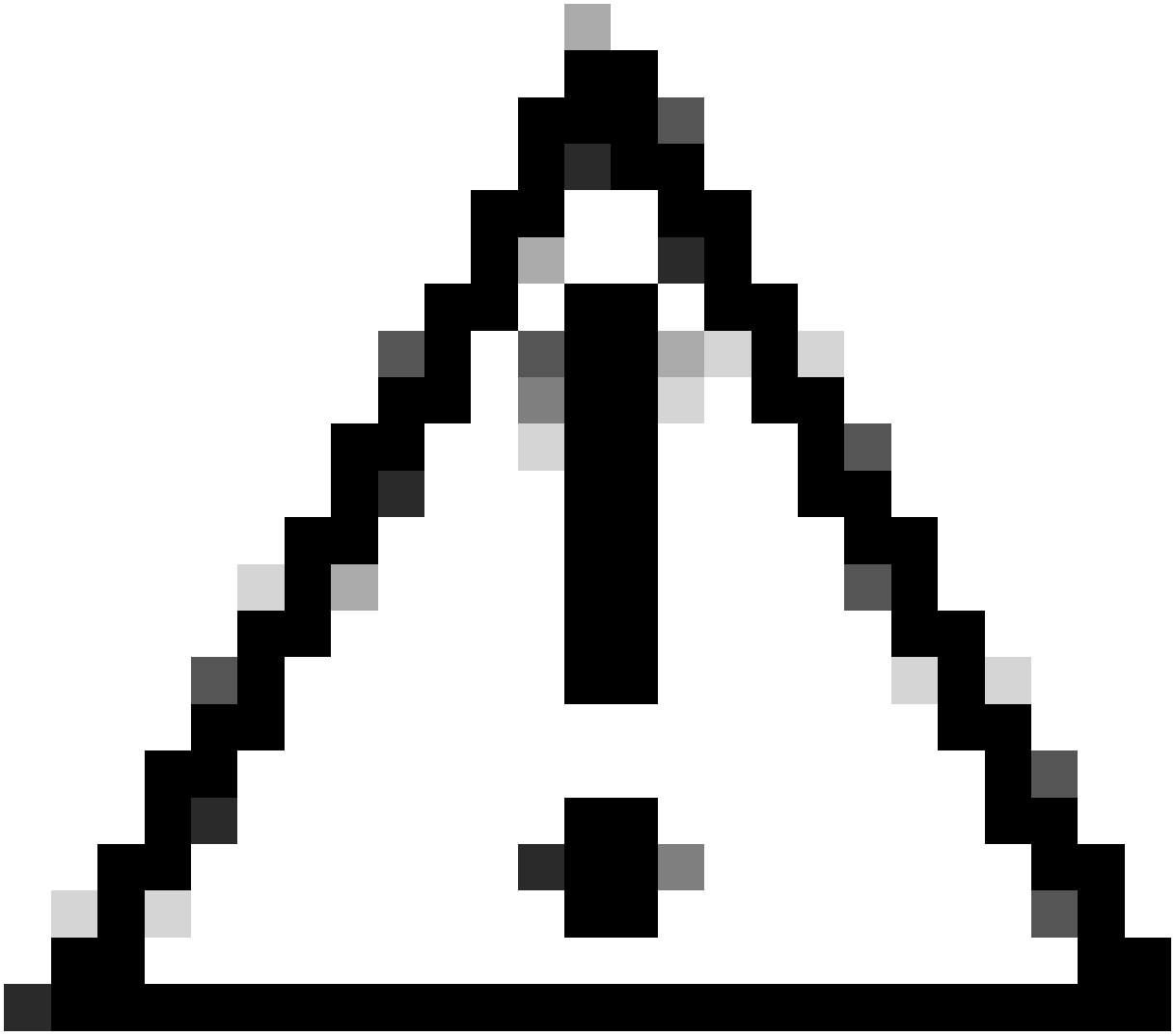
このドキュメントでは、Enforce Domain Validationの設定とその利点について説明します。

ドメイン検証の強制に関する説明

デフォルトでは、Enforce Domain Validationは無効になっています。そのため、このVLANを含むドメインが存在しない静的な{port, VLAN}を使用してEPGが設定されている場合、次のことが発生します。

- アプリケーションセントリックインフラストラクチャ(ACI)でエラーF0467「Configuration failed for <path> due to Invalid path Configuration」が生成されます。
- Vlanはインターフェイスに展開されます。
- トラフィックは特定のインターフェイスで転送されます。

この誤設定は、Enforce Domain Validationによって防止できます。



注意：適切なデューデリジェンスを行わずに、既存のファブリックでこの機能を有効にしないでください。

この機能は、一度有効にすると無効にできません。 誤りがあっても動作していた既存の設定がある可能性があります。有効にする前に、EPGおよび関連するAEPへのドメイン割り当てを確認してください。

ドメイン検証の強制：無効（既定の動作）

APIC CLIドメイン検証の検証を適用します。デフォルトの状態は、ドメインの検証が無効であることを示します。

<#root>

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

no

encap vlan 420がEPGに関連付けられたドメイン/AEPに関連付けられていないとします。Vlan 420は、想定されるインターフェイス上にまだ展開されています。

<#root>

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

420

```
 extended
 VLAN Name                             Encap            Ports
 ---- -------------------------------- ---------------- -----------------------
```

1

```
    lc_TN:lc_APP:lc_EPG              vlan-420
```

Eth1/13

EPGおよびBD用のプラットフォーム非依存(PI)VLAN(1、19)が導入され、想定されるインターフェイスでトランクが許可されます。

<#root>

```
"
 VLAN Name                             Encap            Ports
 ---- -------------------------------- ---------------- -----------------------
```

1

```
    lc_TN:lc_APP:lc_EPG              vlan-420         Eth1/13
```

19

```
   lc_TN:lc_BD                      vxlan-16416666   Eth1/13
```

BDおよびEPG用のVLANは、想定されるインターフェイス上に展開されます。

<#root>

```
leaf# show int eth
```

1/13

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

Eth1/

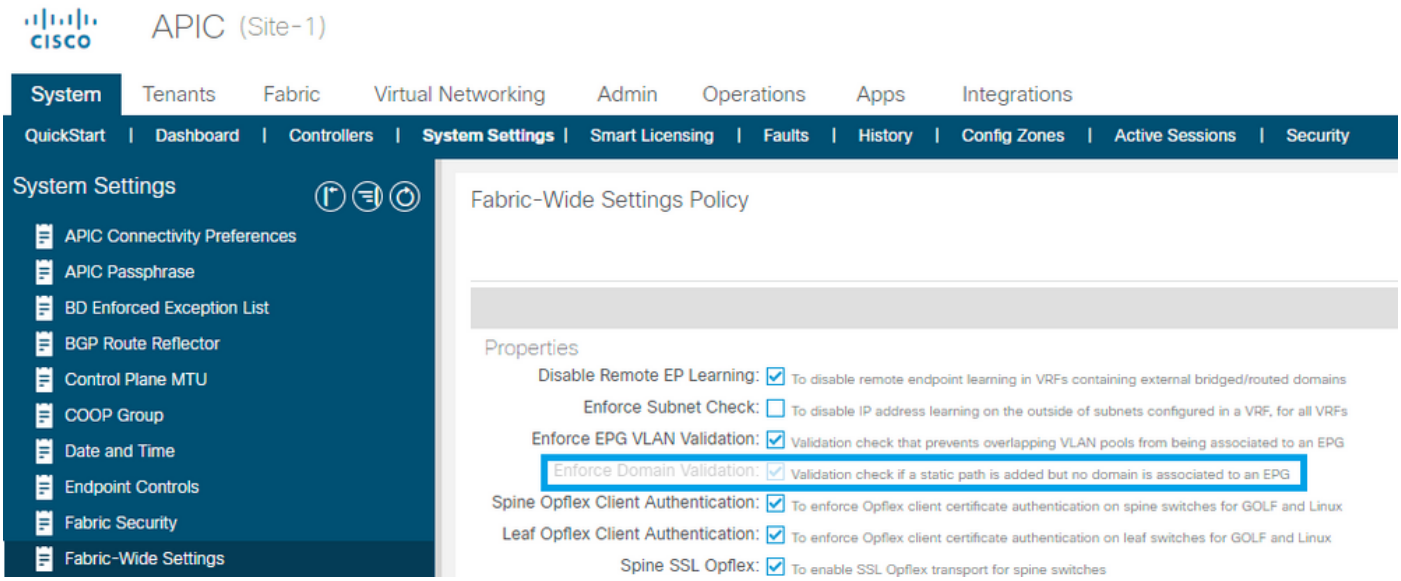
13

```
        1,19
```

ドメイン検証の強制：有効

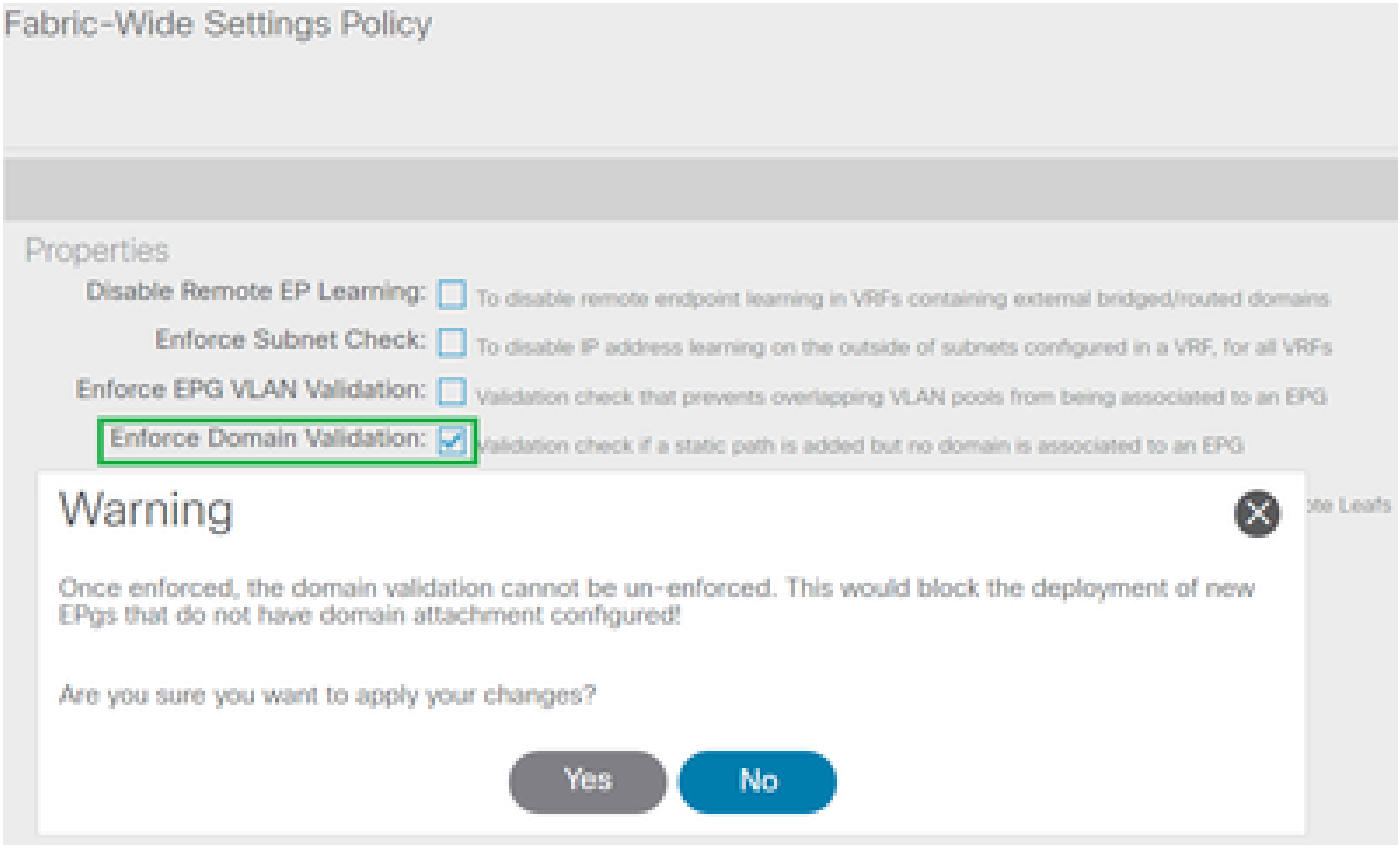
Enforce Domain Validationが有効な場合、各アクセスポリシーパスにリンクされていないVLAN IDを持つEPGにスタティックパスを作成できます。ファブリックで障害が発生し、インターフェイス上でVLANがプログラムされていない。

APIC GUIドメイン検証の適用の検証「システム」 > 「システム設定」 > 「ドメイン検証の適用」。



有効化：ドメイン検証の強制

確認確認の警告



この設定を有効にすると、このオプションはグレー表示され、操作を元に戻すことはできません。

APIC CLI：ドメイン検証の検証の適用

```
<#root>

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

yes
```

この検証は、ポリシーをスイッチにダウンロードする必要がある場合にのみ、既存の設定に対して開始されます。

通常、これはスイッチのアップグレード、クリーンリロード、または設定のスナップショット/バックアップ復元中に発生する可能性があります。

クリーンリロードステップの例：

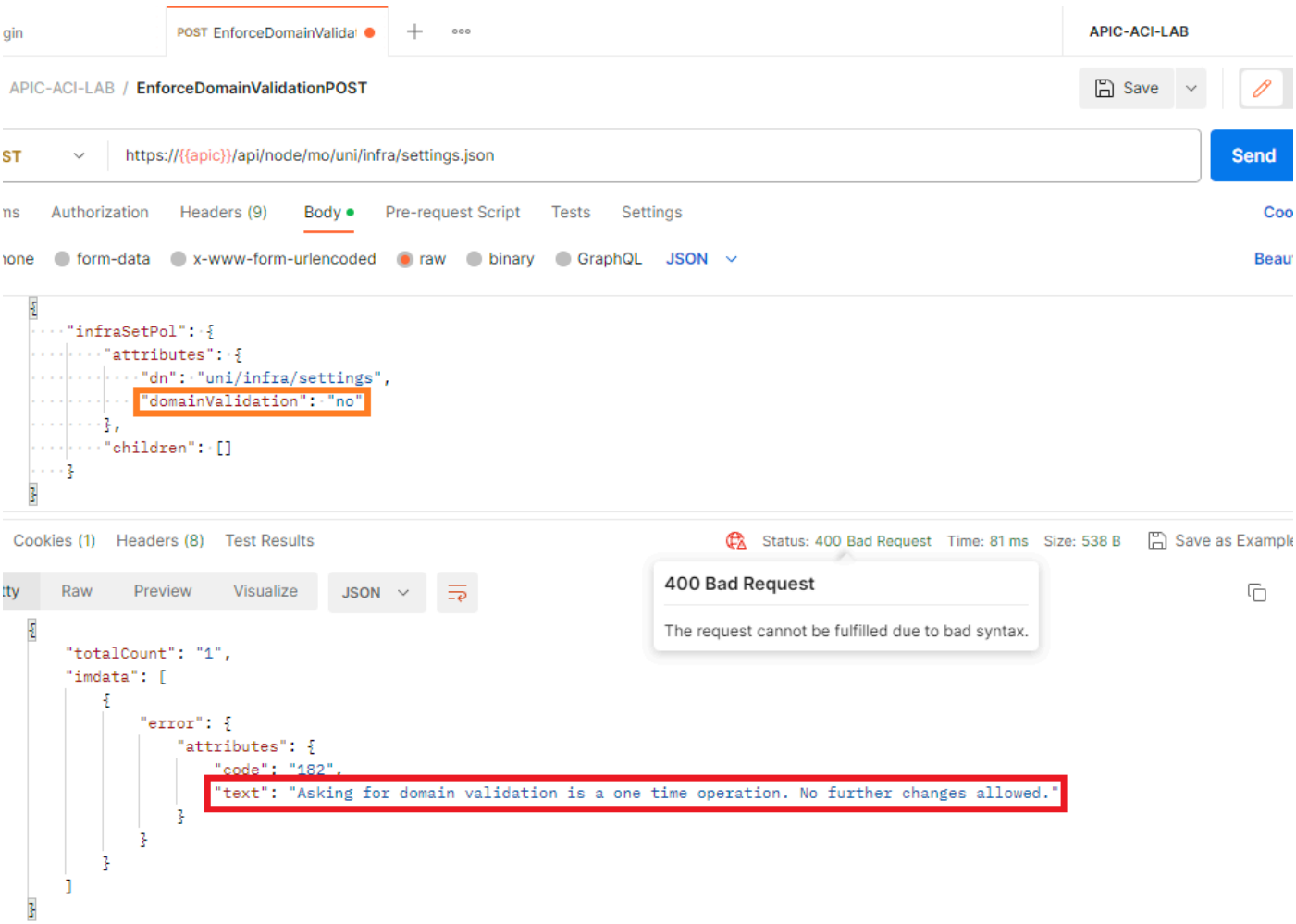
```
<#root>

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
```

最初に導入されたVLAN 420は、現時点で想定されているインターフェイス上にありません。

```
<#root>

leaf# show int eth

1/13

 trunk | grep -A 2 Allowed
 Port           Vlans Allowed on Trunk
--------------------------------------------------------------------------------
 Eth1/13

none
```

ドメイン検証を有効にすることはベストプラクティスと考えられるため、一度有効にすると変更を元に戻すオプションはありません。

POSTMAN APIは、設定を変更するpostが失敗したことを示します。



ドメイン検証の要求は、1回限りの操作です。これ以上の変更はできません。

この設定は初期リリースではデフォルトではなかったため、今後デフォルト設定を変更すると、誤った設定が失敗してサービスが停止する可能性があります。

この理由から、この設定はユーザが設定できます。

トラブルシューティング

アクセスポリシーの関連付けが欠落している影響を受けるEPGに対して、障害F0467が発生します。

障害のトラブルシューティング方法については、この記事の「クイックスタートの切り分け」を参照してください。

関連情報

- アドレスACI障害コードF0467:invalid-vlan、invalid-path、encap-already-in-use

- ACIファブリックのセットアップ：初期セットアップの設定例>システム設定
- Cisco Application Centric Infrastructure(ACI)設計ガイド> EPGドメイン検証

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。