

ACI Case Study : Physical Domain Get Disassociated from EPG upon Removal of Last Static Port Binding from NXOS CLI

Contents

[Introduction](#)

[Prerequisites](#)

[Setup and Topology](#)

[Case Study](#)

[Steps Involved](#)

Introduction

This document describes the impact of deleting all static port bindings from APIC CLI for a leaf switch when domain validation feature is enabled on ACI.

Prerequisites

Basic understanding of Application Centric Infrastructure (ACI) configuration and Domain Validation feature.

More information on Domain validation feature in ACI can be found at,

<https://www.cisco.com/c/en/us/support/docs/software/aci-data-center/221206-understand-aci-enforce-domain-validation.html#:~:text=13%201%2C19-.Enforce%20Domain%20Validation%3A%20Enabled,NOT%20programmed%20on%20the%20interface.>

Setup and Topology

In this setup you are going to use two different ways to program Vlan on the ACI Leaf switch interfaces

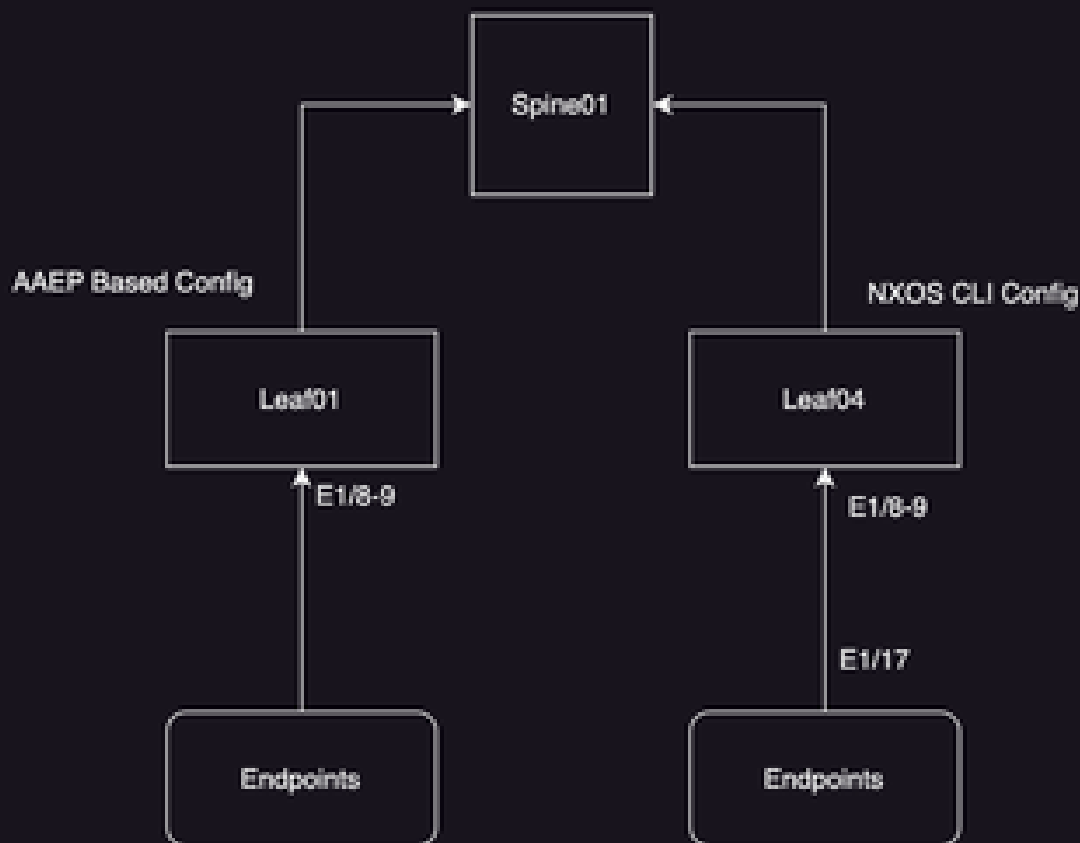
1. **Attachable Access Entity Profile** (AAEP) attached to Leaf01 ports Interface Policy Group (IPG) has been configured with Endpoint Policy Group (EPG) Mapping.
2. AAEP attached to Leaf04 port IPG does not have any EPG mapping however " Static port binding" is performed through CLI to push Vlans.

Two Leaf - 01 and 04 ,

Model: N9K-C93180YC-FX

- Version- 16.0(3e)
- IPG Policy: ipg_1
 - aaep1 (Used for Leaf 01)
 - system-cdp-enabled
 - system-lldp-enabled

- IPG Policy: ipg_2
 - aaep_static (Used for Leaf04)
 - system-cdp-enabled
 - system-lldp-enabled
- Leaf Interface Selector:Leaf_101_interface_profile
 - Port8-9
 - ipg_1
- Leaf Interface Selector:Leaf_104_interface_profile
 - Port8-9
 - ipg_2
- Switch Profile: Leaf_101
 - Leaf101
 - Leaf_101_interface_profile
- Switch Profile: Leaf_104
 - Leaf104
 - Leaf_104_interface_profile
- Tenant: abc-tn , Application Profile: abc-ap, EPG: epg-1, BD: bd-1
- Physical Domain: abc-dom , Vlan Pool: Static : abc-vlan-pool(150-152)
- Domain sample-dom is mapped to EPG epg-1



Case Study

In this lab you are going to observe the Impact of deleting static port bindings from NXOS® CLI. The behaviour in this document is going to show you " When you remove all static port mappings from NXOS® CLI(CLI Only), the APIC is going to remove physical domain from the EPG". As per the current CLI design a clean-up occurs for Physical Domain to EPG association upon removal of the last Static port. This is a for maintaining a optimal configuration and avoiding overlapping vlans in certain scenarios. The same is not relevant to the configurations done via GUI/API.

This behaviour can only impact the ACI Fabric's where the configuration design involves deployment of both Static port attachments and EPG to AEP association mixed under the same EPG, which is uncommon.

If physical domain is removed from EPG and domain validation feature is enabled in the fabric, APIC is going to remove all the vlans from the EPG interfaces.

This issue has already been addressed in Cisco bug ID [CSCwj74262](#) Changes to the current expected behaviour regarding config clean-up under the CLI config)

Steps Involved

Step1. Ensure Domain validation is enabled.

```
<#root>
```

```
apic1#
```

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

```
domainValidation          : yes
```

If domain validation has been disabled in the scenario, no impact is seen as removing physical domain association from EPG and this is not going for an VLAN removal from Leaf Interfaces.

Step2. Vlans are programmed on Leaf 101 due to AAEP to EPG mapping.

```
<#root>
```

```
apic1#
```

```
fabric 101 show vlan encap-id 151
```

```
-----  
  
Node 101 (bgl-aci07-leaf01)  
  
-----
```

VLAN	Name	Status	Ports

14	abc-tn:abc-ap:epg-1	active	Eth1/8, Eth1/9
VLAN	Type	Vlan-mode	

14	enet	CE	

Step3. Vlans not programmed for Leaf 104 as no static mapping is done.

```

apic1# fabric 104 show vlan encap-id 151

-----

Node 104 (leaf04)

-----

++ No vlan programmed

```

VLAN Name	Status	Ports

VLAN Type	Vlan-mode	

Step3. NXOS® style config on Leaf 104 from APIC CLI

```

apic1(config)# leaf 104

apic1(config-leaf)# interface eth 1/8-9

apic1(config-leaf-if)# switchport trunk allowed vlan 151 tenant abc-tn application abc-ap epg epg-1 <=>

```

Step4. Validate on APIC fvIfConn MO is created

```

apic1# moquery -c fvIfConn | grep dn | grep abc

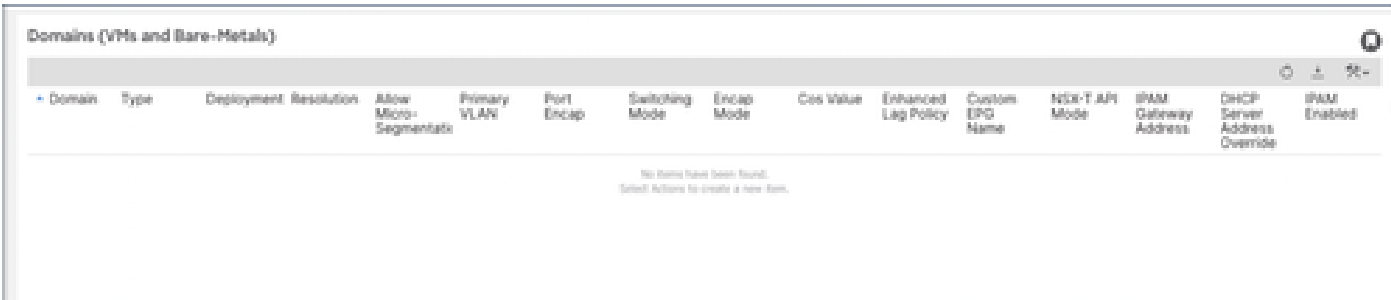
```

```
dn      : uni/epp/fv-[uni/tn-abc-tn/ap-abc-ap/epg-epg-1]/node-101/attEntitypathatt-[abc-aaep
dn      : uni/epp/fv-[uni/tn-abc-tn/ap-abc-ap/epg-epg-1]/node-104/stpathatt-[eth1/8]/conndef
dn      : uni/epp/fv-[uni/tn-abc-tn/ap-abc-ap/epg-epg-1]/node-104/stpathatt-[eth1/9]/conndef
```

Step5. Deleted config from node 104

```
apic1(config-leaf)# interface eth 1/8-9
apic1(config-leaf-if)# no switchport trunk allowed vlan 151 tenant abc-tn application abc-ap epg epg-1
apic1(config-leaf-if)#
```

Step6. Domain got removed due to clean-up script triggered at the backend when config is removed through CLI.



Step7. Vlan programming removed due to Enforce validation feature (As domain is not associated to EPG, vlans are not going to get programmed)

```
apic1# fabric 101 show vlan encap-id 151
-----
Node 101 (leaf01)
-----
```

VLAN Name	Status	Ports
-----	-----	-----

++ vlan got removed

VLAN Type Vlan-mode
