

# ACI Upgrade Best Practices and Troubleshooting

## Contents

[Introduction](#)

[Before the Upgrade](#)

[Things to Do Before the APIC Upgrade](#)

[Things to Do Before the Switch Upgrade](#)

[Troubleshoot Upgrade Issues](#)

[Scenario : APIC ID 2 or Later Stuck at 75%](#)

[How to Troubleshoot](#)

## Introduction

This document describes the steps to troubleshoot Application Centric Infrastructure (ACI) upgrade issues and the best practices to follow before and during the upgrade process.

An ACI upgrade involves the update of Application Policy Infrastructure Controller (APIC) software and switches (leaf and spine). A switch upgrade is usually very straightforward, however an APIC upgrade might involve some cluster issues. Here are a few prechecks that Cisco recommends to prepare before an upgrade is started.

## Before the Upgrade

Before you start the ACI upgrade, make sure to perform some prechecks in order to avoid any unexpected behaviors.

### Things to Do Before the APIC Upgrade

#### 1. Clear All the Faults

Many faults in ACI fabric state that there are invalid or conflict policies or even disconnected interfaces and so on. Understand the trigger and clear them before you start the upgrade. Be aware, the faults such as `encap already been used` or `Routed port is in L2 mode` could result in an unexpected outage. When you upgrade the switch, it downloads all the policies from APIC from scratch. As a result, the unexpected policies might take over the expected policies which could cause an outage.

#### 2. Clear VLAN Pool Overlap

VLAN pool overlap means the same VLAN ID is part of two or more VLAN pools. If the same VLAN ID is deployed on multiple leaf switches which is part of different VLAN pools, it would have a different VXLAN ID on these switches. Since ACI uses the VXLAN ID for forwarding, traffic destined to a particular VLAN might end up in different VLAN or get dropped. Since the

leaf downloads the configuration from APIC after its upgrade, the order in which VLAN gets deployed has a major role. So, this could result in an outage or intermittent connectivity loss to endpoints in some VLANs.

It is important to check for VLAN ID overlap and correct them before you start the upgrade. It is recommended to have one VLAN ID be part of one VLAN pool only and reuse the VLAN pool where needed.

### 3. Confirm Supported Upgrade Path

The APIC upgrade involves the data conversion from one version to other which is done internally. For the data conversion to succeed, there are some version compatibility issues that need to be taken care of. Always make sure to check if Cisco supports the direct upgrade from your current ACI version to the new target version you are upgrading to. Sometimes you will have to go through multiple hops to reach the target version. If you upgrade to a non-supported version, it could result in cluster issues and configuration issues.

The supported upgrade paths are always listed in the [Cisco ACI Upgrade Guide](#).

### 4. Backup APIC Configuration

Make sure to export a configuration backup to a remote server before you start the upgrade. This exported backup file can be used to get the configuration back on APICs if you lose all configuration or there is a data corruption after the upgrade.

**Note:** If you enable encryption for the backup, make sure to save the encryption key. Otherwise, all the user account passwords including the **admin** password would not be imported properly.

### 5. Confirm APIC CIMC Access

Cisco Integrated Management Controller (CIMC) is the best way to get the remote console access to the APIC. If the APIC does not come back up after a reboot or the processes are stuck, you might not be able to connect to the APIC through out-of-band or inband management of the APIC. At this stage, you can log in to CIMC and connect to the KVM console for the APIC to perform some checks and troubleshoot the issue.

### 6. Check and Confirm the CIMC Version Compatibility

Always make sure to run the Cisco recommended CIMC version compatible with the target ACI version before you start the ACI upgrade. Refer to [Recommended APIC and CIMC Version](#).

### 7. Confirm the APIC Process is not Locked

The process called Appliance Element (AE) which runs in the APIC is responsible to trigger the upgrade in the APIC. There is a known bug in CentOS Intelligent Platform Management Interface (IPMI) which could lock the AE process in APIC. If the AE process is locked, the APIC firmware upgrade will not kick in. This process queries the chassis IPMI every 10 seconds. If the AE process has not queried the chassis IPMI in the last 10 seconds, that

could mean the AE process is locked.

You can check the status of the AE process to know the last IPMI query. From the APIC CLI, enter the command `date` in order to check the current system time. Now enter the command `grep "ipmi" /var/log/dme/log/svc_ifc_ae.bin.log | tail -5` and check the last time when the AE process queried the IPMI. Compare the time against the system time in order to check if the last query was within the 10 second window of the system time.

If the AE process has failed to query the IPMI in the last 10 seconds of the system time, you can reboot the APIC to recover the AE process before starting the upgrade.

**Note:** Do not reboot two or more APICs at the same time to avoid any cluster issues.

## 8. Check and Confirm the NTP Availability

From each APIC, ping and confirm the reachability to the NTP server in order to avoid known issues due to the APIC time mismatch. More details on this can be found in the troubleshooting section of this article.

## 9. Check the APIC Health State

Check and confirm the health status of the APIC in the cluster before you start the upgrade. The health score of 255 means the APIC is healthy. Enter the command `acidiag avread | grep id= | cut -d ' ' -f 9,10,20,26,46` from any APIC CLI in order to check the APIC health status. If the health score is not 255 for any APIC, do not start the upgrade.

## 10. Evaluate the Impact of a New Version

Before you start the upgrade, review the [Release Notes](#) for your target ACI version and understand any behavioral changes that are applicable to your fabric configuration in order to avoid any unexpected results after the upgrade.

## 11. Stage the Upgrade in the Lab

Cisco recommends to try the upgrade in a lab or test fabric before the actual production fabric to familiarize yourself with the upgrade and behaviors in the new version. This also helps to evaluate any possible issues you could run in to after the upgrade.

# Things to Do Before the Switch Upgrade

## 1. Place Virtual Port Channel (vPC) and Redundant Leaf Pairs in Different Maintenance Groups

ACI APIC has a mechanism to check and defer the upgrade of vPC pair leaf nodes from a certain version and later. However, it is best practice to put vPC pair switches in different maintenance groups to avoid both the vPC switches reboot at the same time.

In case of non-vPC switches which are redundant, such as border leaf, make sure to put

them in different port groups in order to avoid any outages.

## Troubleshoot Upgrade Issues

Always start to troubleshoot APIC1 if the upgrade gets stuck or fails. If the APIC1 upgrade is not finished yet, do not do anything in APIC2 and APIC3. The APIC upgrade process is incremental and hence APIC2 will upgrade only after APIC1 completes the upgrade and notifies APIC2 about it and so on. So, violation of this might put the cluster into a broken state with corrupt database and you might be required to rebuild the cluster.

### Scenario : APIC ID 2 or Later Stuck at 75%

In this scenario, you would see that APIC1 is upgraded successfully, but APIC2 is still stuck at 75%. This problem happens if the APIC1 upgrade version information is not propagated to APIC2 or later. Be aware that the `svc_ifc_appliance_director` process is in charge of the version sync between APICs.

### How to Troubleshoot

**Step 1:** Make sure that APIC1 could ping the rest of the APICs with their Tunnel End Point (TEP) IP address as this will determine whether you need to troubleshoot from the leaf switch or continue from the APIC itself. If APIC1 cannot ping APIC2, you might want to call the Technical Assistance Center (TAC) to troubleshoot the switch. If APIC1 could ping APIC2, then continue to the second step.

**Step 2:** Since APICs can ping each other, APIC1 version information should have been replicated to the peer, but somehow was not accepted by the peer. The version information is identified by a version timestamp. You can confirm the version timestamp of APIC1 from the CLI and APIC2 CLI which is waiting at 75%.

On APIC1

```
apic1# acidiag avread | grep id=1 | cut -d ' ' -f20-21
version=2.0(2f) 1m(t):1(2018-07-25T18:01:04.907+11:00)
```

On APIC2

```
apic2# acidiag avread | grep id=1 | cut -d ' ' -f20-21
version=2.0(1m) 1m(t):1(2018-07-25T18:20:04.907+11:00)
```

As you see, the version timestamp of APIC2 (18:20:04) which runs Version 2.0(1m) in this example is higher than the version timestamp of APIC1(18:01:04) that runs Version 2.0(2f). So, the APIC2 installer process thinks the APIC1 upgrade is not complete yet and waits at 75%. The APIC2 upgrade will kick off when the version timestamp of APIC1 goes above the version timestamp of APIC2. However, this could be a lot of waiting based on the time difference. In order to recover the fabric from this state, you can open a TAC case to get assistance to troubleshoot and fix the issue from APIC1.