THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017–2018 Cisco Systems, Inc. All rights reserved.
CONTENTS

PREFACE

Preface vii
  Audience vii
  Document Conventions vii
  Related Documentation ix
  Documentation Feedback x
  Obtaining Documentation and Submitting a Service Request x

CHAPTER 1

New and Changed Information 1
  New and Changed Information 1

CHAPTER 2

Initial Setup 3
  Cisco APIC Documentation Roadmap 3
  Simplified Approach to Configuring in Cisco APIC 4
  Changing the BIOS Default Password 4
  About the APIC 4
  Setting up the Cisco APIC 5
    Setup for Active and Standby APIC 7
    Provisioning IPv6 Management Addresses on APIC Controllers 12
  Accessing the GUI 12
  Accessing the REST API 13
  Accessing the NX-OS Style CLI 14
    Accessing the NX-OS Style CLI from a Terminal 14
    Accessing the NX-OS Style CLI from the GUI 15
  Accessing the Object Model CLI 15

CHAPTER 3

APIC GUI Overview 17
Overview of the GUI  17
Menu Bar and Submenu Bar  18
  Menu Bar Tabs  19
    System Tab  19
    Tenants Tab  19
    Fabric Tab  20
    Virtual Networking Tab  20
    L4-L7 Services Tab  20
    Admin Tab  20
    Operations Tab  21
    Apps Tab  21
  Menu Bar Tools  21
    Search  21
    Alerts  21
    User Profile and Preferences  22
  System Tools  22
Navigation Pane  23
Work Pane  24
  Common Pages in the Work Pane  24
Show Me How  25
Personalizing the Interface  25
  Naming the APIC GUI  25
  Adding a Login Banner to the CLI or GUI  26
Deployment Warning and Policy Usage Information  26
Graphical Configuration of Ports  27
Viewing an API Interchange in the GUI  28
GUI Icons  30
  Fault, Statistics, and Health Level Icons  31

CHAPTER 4

Fabric Initialization and Switch Discovery  33
  Initializing the Fabric  33
  About Fabric Initialization  33
  Example Topology  33
  Example Topology Connections  34
Switch Discovery 35
  About Switch Discovery with the APIC 35
  Switch Registration with the APIC Cluster 35
  Registering the Unregistered Switches Using the GUI 35
  Switch Discovery Validation and Switch Management from the APIC 36
  Validating the Registered Switches Using the GUI 36
  Validating the Fabric Topology 37
  Validating the Fabric Topology Using the GUI 37
  Unmanaged Switch Connectivity in VM Management 37
Graceful Insertion and Removal (GIR) Mode 38
  Graceful Insertion and Removal (GIR) Mode 38
  Removing a Switch to Maintenance Mode Using the GUI 39
  Removing a Switch to Maintenance Mode Using the CLI 39
  Removing a Switch to Maintenance Mode Using the REST API 40
  Inserting a Switch to Operational Mode Using the GUI 40
  Inserting a Switch to Operational Mode Using CLI 40
  Inserting a Switch to Operational Mode Using the REST API 40

CHAPTER 5
Cisco APIC Cluster Management 43
  APIC Cluster Overview 43
  Expanding the Cisco APIC Cluster 43
  Contracting the Cisco APIC Cluster 44
  Cluster Management Guidelines 44
    Expanding the APIC Cluster Size 45
    Reducing the APIC Cluster Size 45
    Replacing Cisco APIC Controllers in the Cluster 46
  Expanding the Cluster Examples 47
    Expanding the APIC Cluster Using the GUI 47
    Expanding the APIC Cluster Using the REST API 48
  Contracting the Cluster Examples 48
    Contracting the APIC Cluster Using the GUI 48
    Contracting the APIC Cluster Using the REST API 49
Commissioning and Decommissioning Cisco APIC Controllers 50
  Commissioning a Cisco APIC Controller in the Cluster Using the GUI 50
Preface

This preface includes the following sections:

- Audience, on page vii
- Document Conventions, on page vii
- Related Documentation, on page ix
- Documentation Feedback, on page x
- Obtaining Documentation and Submitting a Service Request, on page x

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Virtual machine installation and administration
- Server administration
- Switch and network administration
- Cloud administration

Document Conventions

Command descriptions use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>Bold text indicates the commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Italic text indicates arguments for which the user supplies the values.</td>
</tr>
<tr>
<td>[x]</td>
<td>Square brackets enclose an optional element (keyword or argument).</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
<tr>
<td>variable</td>
<td>Indicates a variable for which you supply values, in context where italics cannot be used.</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
</tbody>
</table>

Examples use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>screen font</strong></td>
<td>Terminal sessions and information the switch displays are in screen font.</td>
</tr>
<tr>
<td><strong>boldface screen font</strong></td>
<td>Information you must enter is in boldface screen font.</td>
</tr>
<tr>
<td><strong>italic screen font</strong></td>
<td>Arguments for which you supply values are in italic screen font.</td>
</tr>
<tr>
<td><code>&lt; &gt;</code></td>
<td>Nonprinting characters, such as passwords, are in angle brackets.</td>
</tr>
<tr>
<td><code>[ ]</code></td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td><code>!</code>, <code>#</code></td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

This document uses the following conventions:

Note

Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Caution

Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Warning

**IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS
Related Documentation

Cisco Application Policy Infrastructure Controller (APIC) Documentation

The following companion guides provide documentation for Cisco APIC:

- Cisco APIC Getting Started Guide
- Cisco APIC Basic Configuration Guide
- Cisco ACI Fundamentals
- Cisco APIC Layer 2 Networking Configuration Guide
- Cisco APIC Layer 3 Networking Configuration Guide
- Cisco APIC NX-OS Style Command-Line Interface Configuration Guide
- Cisco APIC REST API Configuration Guide
- Cisco APIC Layer 4 to Layer 7 Services Deployment Guide
- Cisco ACI Virtualization Guide
- Cisco Application Centric Infrastructure Best Practices Guide

All these documents are available at the following URL: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Cisco Application Centric Infrastructure (ACI) Documentation


Cisco Application Centric Infrastructure (ACI) Simulator Documentation


Cisco Nexus 9000 Series Switches Documentation


Cisco Application Virtual Switch Documentation

Cisco ACI Virtual Edge Documentation


Cisco ACI Virtual Pod Documentation


Cisco Application Centric Infrastructure (ACI) Integration with OpenStack Documentation


Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to apic-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.
CHAPTER 1

New and Changed Information

This chapter contains the following sections:

- New and Changed Information, on page 1

New and Changed Information

The following tables provide an overview of the significant changes to this guide up to this current release. The tables do not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

| Table 1: New Features and Changed Information for Cisco APIC Release 3.2(1x) |
|---|---|---|
| Feature | Description | Where Documented |
| APIC GUI Alias | You can add and display a name in the APIC GUI heading. | Naming the APIC GUI, on page 25 |
| Summary Pages | Many folders contain tile-based summaries of contained folders, along with brief health and fault status. | Common Pages in the Work Pane, on page 24 |

| Table 2: New Features and Changed Information for Cisco APIC Release 3.1(2) |
|---|---|---|
| Feature | Description | Where Documented |
| LACP support for Layer 2 and Layer 3 traffic diversion has been added to GIR process to reduce traffic loss | Implementation of graceful removal of vPC port channels using LACP. | Graceful Insertion and Removal (GIR) Mode, on page 38 |
### Table 3: New Features and Changed Information for Cisco APIC Release 3.1(1)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Topology Refactoring</td>
<td>Detailed health, inventory, and link information is available from topology diagram.</td>
<td>Validating the Fabric Topology Using the GUI, on page 37</td>
</tr>
<tr>
<td>Favorites</td>
<td>Favorite menu pages can be bookmarked for quick access from the menu bar.</td>
<td>User Profile and Preferences, on page 22</td>
</tr>
<tr>
<td>Show Me How</td>
<td>A GUI overlay shows you how to perform several common tasks.</td>
<td>Show Me How, on page 25</td>
</tr>
<tr>
<td>QuickStart Configuration Workflows</td>
<td>Guides you through setting up node, remote leaf, or multipod configurations.</td>
<td></td>
</tr>
<tr>
<td>Active Sessions</td>
<td>Allows you to view all user login sessions with the ability to cancel a session.</td>
<td></td>
</tr>
<tr>
<td>Menu restructuring</td>
<td>Several tabs have been restructured to reduce the number of folders. In addition, many global policies were moved to the System tab.</td>
<td></td>
</tr>
<tr>
<td>Basic GUI mode is deprecated</td>
<td>The Cisco APIC Basic mode is no longer available.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 4: New Features and Changed Behavior in Cisco APIC and Document Reorganization for Cisco APIC Release 3.0(1k)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redesign of the APIC GUI</td>
<td>--</td>
<td>Overview of the GUI, on page 17</td>
</tr>
<tr>
<td>Graceful Insertion and Removal (GIR) Mode</td>
<td>The Graceful Insertion and Removal (GIR) mode or maintenance mode allows you to isolate a switch from the network with minimum service disruption.</td>
<td>Graceful Insertion and Removal (GIR) Mode, on page 38</td>
</tr>
<tr>
<td>Last Login</td>
<td>The Last Login feature allows you to view the date and time of your last login.</td>
<td>Overview of the GUI, on page 17</td>
</tr>
<tr>
<td>Type-ahead</td>
<td>For Layer 2 configuration of ports, you can type into the node and path fields to filter ports.</td>
<td>Tenants Tab, on page 19</td>
</tr>
<tr>
<td>Graphical Configuration of Ports</td>
<td>Interface ports can be configured by clicking a port diagram.</td>
<td>Graphical Configuration of Ports, on page 27</td>
</tr>
</tbody>
</table>
CHAPTER 2

Initial Setup

This chapter contains the following sections:

- Cisco APIC Documentation Roadmap, on page 3
- Simplified Approach to Configuring in Cisco APIC, on page 4
- Changing the BIOS Default Password, on page 4
- About the APIC, on page 4
- Setting up the Cisco APIC, on page 5
- Accessing the GUI, on page 12
- Accessing the REST API, on page 13
- Accessing the NX-OS Style CLI, on page 14
- Accessing the Object Model CLI, on page 15

Cisco APIC Documentation Roadmap

This table provides a list of additional documents that are useful references along with the Cisco APIC Getting Started Guide. All Cisco APIC documents are available at the APIC documents landing page.

<table>
<thead>
<tr>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Centric Infrastructure Fabric Hardware Installation Guide</td>
</tr>
<tr>
<td>Cisco APIC Management, Installation, Upgrade, and Downgrade Guide</td>
</tr>
<tr>
<td>Cisco APIC Basic Configuration Guide</td>
</tr>
<tr>
<td>Cisco APIC Layer 2 Networking Configuration Guide</td>
</tr>
<tr>
<td>Cisco APIC Layer 3 Networking Configuration Guide</td>
</tr>
<tr>
<td>Cisco ACI Virtualization Guide</td>
</tr>
<tr>
<td>Cisco Application Centric Infrastructure Fundamentals</td>
</tr>
<tr>
<td>Cisco APIC Layer 4 to Layer 7 Services Deployment Guide</td>
</tr>
</tbody>
</table>
Simplified Approach to Configuring in Cisco APIC

Cisco APIC supports a simplified approach to configuring the ACI with an additional NX-OS style CLI interface. The existing methods of configuration using REST API and the GUI are supported as well.

In addition to the simple approach available for network administrators and other users of the NX-OS style CLI, there is intelligence embedded in this approach as compared to the GUI or the REST API. In several instances, the NX-OS style CLI can create the ACI model constructs implicitly for a user's ease of use, and they also provide validations to ensure consistency in configuration. This functionality reduces and prevents faults.

For further details about configurations and tasks, see the *Cisco APIC Basic Configuration Guide* and the *Cisco APIC NX-OS Style Command-Line Interface Configuration Guide*.

Changing the BIOS Default Password

The APIC controller ships with a default BIOS password. The default password is 'password'. When the boot process starts, the boot screen displays the BIOS information on the console server.

To change the default BIOS password perform the following task:

**Procedure**

1. **Step 1** During the BIOS boot process, when the screen displays *Press <F2> Setup*, press F2.
   
   The *Entering Setup* message displays as it accesses the setup menu.

2. **Step 2** At the *Enter Password* dialog box, enter the current password.
   
   **Note** The default is 'password'.

3. **Step 3** In the *Setup Utility*, choose the *Security* tab, and choose *Set Administrator Password*.

4. **Step 4** In the *Enter Current Password* dialog box, enter the current password.

5. **Step 5** In the *Create New Password* dialog box, enter the new password.

6. **Step 6** In the *Confirm New Password* dialog box, re-enter the new password.

7. **Step 7** Choose the *Save & Exit* tab.

8. **Step 8** In the *Save & Exit Setup* dialog box, choose *Yes*.

9. **Step 9** Wait for the reboot process to complete.

The updated BIOS password is effective.

About the APIC

The Cisco Application Centric Infrastructure (ACI) is a distributed, scalable, multi-tenant infrastructure with external end-point connectivity controlled and grouped through application-centric policies. The Application Policy Infrastructure Controller (APIC) is the unified point of automation, management, monitoring, and programmability for the ACI. The APIC supports the deployment, management, and monitoring of any...
application anywhere, with a unified operations model for the physical and virtual components of the
infrastructure. The APIC programmatically automates network provisioning and control that is based on the
application requirements and policies. It is the central control engine for the broader cloud network; it simplifies
management and allows flexibility in how application networks are defined and automated. It also provides
northbound Representational State Transfer (REST) APIs. The APIC is a distributed system that is implemented
as a cluster of many controller instances.

Setting up the Cisco APIC

When the Cisco Application Policy Infrastructure Controller (Cisco APIC) is launched for the first time, the
Cisco APIC console presents a series of initial setup options. For many options, you can press Enter to
choose the default setting that is displayed in brackets. At any point in the setup dialog, you can restart the
dialog from the beginning by pressing Ctrl-C.

Important Notes

- If the UNIX user ID is not explicitly specified in the response from the remote authentication server,
  then some Cisco APIC software releases assign a default ID of 23999 to all users. If the response from
  the remote authentication server fails to specify a UNIX ID, all users will share the same ID of 23999
  and this can result in the users being granted higher or lower privileges than the configured privileges
  through the RBAC policies on the Cisco APIC.

- Cisco recommends that you assign unique UNIX user IDs in the range of 16000 to 23999 for the AV
  Pairs that are assigned to the users when in Bash shell (using SSH, Telnet, or Serial/KVM consoles). If
  a situation arises where the Cisco AV Pair does not provide a UNIX user ID, the user is assigned a user
  ID of 23999 or similar number from the range that also enables the user's home directories, files, and
  processes accessible to the remote users with a UNIX ID of 23999.

To ensure that your remote authentication server does not explicitly assign a UNIX ID in its cisco-av-pair
response, open an SSH session to the Cisco APIC and log in as an administrator (using a remote user
account). Once logged in, run the following commands (replace userid with the username that you logged
in with):

- admin@apic1: remoteuser-userid> cd /mit/uni/userext/remoteuser-userid

- admin@apic1: remoteuser-userid> cat summary

- If you are using a Cisco Integrated Management Controller (CIMC) for your setup, use only the port-side
  utility console port with the breakout cable. Setup the CIMC first, and then access the Cisco APIC through
  the CIMC KVM or continue to access the Cisco APIC locally through the port-side utility console port.
  Do not use the RJ-45 console port, unless access to the port side is restricted. If you choose the CIMC
  KVM access, you will have remote access available later which is required during operations.

- If you are using RJ-45 console port, connect to CIMC using SSH and enable the Serial over LAN port
  using the following parameters:

  - Scope SOL sol
  - Set Enabled to Yes
  - Commit
  - Exit
After enabling, enter the command `connect host` to access the console. If the serial port is connected, either disconnect the serial port or ensure that the connected device has the proper configuration.

- It is recommended not to modify any parameters using CIMC. If there are any issues, ensure that the default setting for CIMC management node is `Dedicated Mode` and not `Shared`. If `Dedicated Mode` is not used, it can prevent the discovery of fabric nodes.

- Do not upgrade software or firmware using the CIMC user interface, XML, or SSH interfaces unless the modified property and software or firmware version are supported with your specific Cisco APIC version.

- Set the NIC mode to Dedicated, when setting up the CIMC, in the CIMC Configuration Utility. After the CIMC is configured, in the CIMC GUI, verify that you have the following parameters set.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP</td>
<td>Disabled on the VIC</td>
</tr>
<tr>
<td>TPM Support</td>
<td>Enabled on the BIOS</td>
</tr>
<tr>
<td>TPM Enabled Status</td>
<td>Enabled</td>
</tr>
<tr>
<td>TPM Ownership</td>
<td>Owned</td>
</tr>
</tbody>
</table>

- Starting with Cisco APIC release 1.2(2x), during the initial setup the system will prompt you to select IPv4, or IPv6, or dual stack configuration. Choosing dual stack will enable accessing the Cisco APIC and Cisco Application Centric Infrastructure (Cisco ACI) fabric out-of-band management interfaces with either IPv4 or IPv6 addresses. While the examples in the table below use IPv4 addresses, you can use whatever IP address configuration options you chose to enable during the initial setup.

- A minimum subnet mask of /19 is recommended.

- Connecting the Cisco APIC to the Cisco ACI fabric requires a 10G interface on the ACI-mode leaf switch. You cannot connect the Cisco APIC directly to the Cisco Nexus 9332PQ, Cisco Nexus 93180LC, or Cisco Nexus 9336C-FX2 ACI-mode leaf switches unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the leaf switches will auto-negotiate to 10G without requiring any manual configuration.

**Note** Starting with Cisco APIC release 2.2(1n), the Cisco Nexus 93180LC leaf switch is supported.

- The fabric ID is set during the Cisco APIC setup and it cannot be changed unless you perform a clean reload of the fabric. To change the fabric ID, perform a clean reload on the Cisco APIC and leaf switches after changing the `sam.config` file. All Cisco APICs in a cluster must have the same fabric ID.

**About Cold Standby for a Cisco APIC Cluster**

The Cold Standby functionality for a Cisco APIC cluster enables you to operate the Cisco APICs in a cluster in an active/standby mode. In a Cisco APIC cluster, the designated active Cisco APICs share the load and the designated standby Cisco APICs can act as an replacement for any of the Cisco APICs in an active cluster.

An admin user can set up the Cold Standby functionality when the Cisco APIC is launched for the first time. We recommend that you have at least 3 active Cisco APICs in a cluster, and one or more standby Cisco APICs.
An admin user must initiate the switch over to replace an active Cisco APIC with a standby Cisco APIC. See the Cisco APIC Management, Installation, Upgrade, and Downgrade Guide for more information.

## Setup for Active and Standby APIC

### Table 5: Setup for Active APIC

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric name</td>
<td>Fabric domain name</td>
<td>ACI Fabric1</td>
</tr>
<tr>
<td>Fabric ID</td>
<td>Fabric ID</td>
<td>1</td>
</tr>
<tr>
<td>Number of active controllers</td>
<td>Cluster size</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>When setting up APIC in an active-standby mode, you must have at least 3 active APICs in a cluster.</td>
</tr>
<tr>
<td>POD ID</td>
<td>POD ID</td>
<td>1</td>
</tr>
<tr>
<td>Standby controller</td>
<td>Setup standby controller</td>
<td>NO</td>
</tr>
<tr>
<td>Controller ID</td>
<td>Unique ID number for the active APIC instance.</td>
<td>Valid range: 1-19</td>
</tr>
<tr>
<td>Controller name</td>
<td>Active controller name</td>
<td>apic1</td>
</tr>
<tr>
<td>IP address pool for tunnel endpoint addresses</td>
<td>Tunnel endpoint address pool</td>
<td>10.0.0.0/16</td>
</tr>
</tbody>
</table>

This value is for the infrastructure virtual routing and forwarding (VRF) only.

This subnet should not overlap with any other routed subnets in your network. If this subnet does overlap with another subnet, change this subnet to a different /16 subnet. The minimum supported subnet for a 3 APIC cluster is /23. If you are using Release 2.0(1) the minimum is /22.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID for infrastructure network</td>
<td>Infrastructure VLAN for APIC-to-switch communication including virtual switches&lt;br&gt;&lt;br&gt;&lt;strong&gt;Note&lt;/strong&gt; Reserve this VLAN for APIC use only. The infrastructure VLAN ID must not be used elsewhere in your environment and must not overlap with any other reserved VLANs on other platforms.</td>
<td>--</td>
</tr>
<tr>
<td>IP address pool for bridge domain multicast address (GIPo)</td>
<td>IP addresses used for fabric multicast. For Cisco APIC in a Cisco ACI Multi-Site topology, this GIPo address can be the same across sites.</td>
<td>225.0.0.0/15&lt;br&gt;Valid range: 225.0.0.0/15 to 231.254.0.0/15, prefixlen must be 15 (128k IPs)</td>
</tr>
<tr>
<td>IPv4/IPv6 addresses for the out-of-band management</td>
<td>IP address that you use to access the APIC through the GUI, CLI, or API. This address must be a reserved address from the VRF of a customer</td>
<td>—</td>
</tr>
<tr>
<td>IPv4/IPv6 addresses of the default gateway</td>
<td>Gateway address for communication to external networks using out-of-band management</td>
<td>—</td>
</tr>
<tr>
<td>Management interface speed/duplex mode</td>
<td>Interface speed and duplex mode for the out-of-band management interface</td>
<td>auto&lt;br&gt;&lt;br&gt;Valid values are as follows&lt;br&gt;• auto&lt;br&gt;• 10baseT/Half&lt;br&gt;• 10baseT/Full&lt;br&gt;• 100baseT/Half&lt;br&gt;• 100baseT/Full&lt;br&gt;• 1000baseT/Full</td>
</tr>
</tbody>
</table>
To change the VLAN ID after the initial APIC setup, export your configurations, rebuild the fabric with a new infrastructure VLAN ID and import the configurations so that the fabric does not revert to the old infrastructure VLAN ID. See the KB article about Using Export and Import to Recover Configuration State.

Table 6: Setup for Standby APIC

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric name</td>
<td>Fabric domain name</td>
<td>ACI Fabric1</td>
</tr>
<tr>
<td>Fabric ID</td>
<td>Fabric ID</td>
<td>1</td>
</tr>
<tr>
<td>Number of active controllers</td>
<td>Cluster size</td>
<td>3</td>
</tr>
<tr>
<td>POD ID</td>
<td>ID of the POD</td>
<td>1</td>
</tr>
<tr>
<td>Standby controller</td>
<td>Setup standby controller</td>
<td>Yes</td>
</tr>
<tr>
<td>Standby Controller ID</td>
<td>Unique ID number for the standby APIC instance</td>
<td>Recommended range: &gt;20</td>
</tr>
<tr>
<td>Controller name</td>
<td>Standby controller name</td>
<td>NA</td>
</tr>
<tr>
<td>IP address pool for tunnel endpoint addresses</td>
<td>Tunnel endpoint address pool</td>
<td>10.0.0.0/16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This value is for the infrastructure virtual routing and forwarding (VRF) only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This subnet should not overlap with any other routed subnets in your network. If this subnet does overlap with another subnet, change this subnet to a different /16 subnet. The minimum supported subnet for a 3 APIC cluster is /23. If you are using Release 2.0(1) the minimum is /22.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Default Value</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>VLAN ID for infrastructure network⁴</td>
<td>Infrastructure VLAN for APIC-to-switch communication including virtual switches</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>Note Reserve this VLAN for APIC use only. The infrastructure VLAN ID must not be used elsewhere in your environment and must not overlap with any other reserved VLANs on other platforms.</td>
<td></td>
</tr>
<tr>
<td>IPv4/IPv6 addresses for the out-of-band management</td>
<td>IP address that you use to access the APIC through the GUI, CLI, or API. This address must be a reserved address from the VRF of a customer</td>
<td>—</td>
</tr>
<tr>
<td>IPv4/IPv6 addresses of the default gateway</td>
<td>Gateway address for communication to external networks using out-of-band management</td>
<td>—</td>
</tr>
<tr>
<td>Management interface speed/duplex mode</td>
<td>Interface speed and duplex mode for the out-of-band management interface</td>
<td>auto</td>
</tr>
<tr>
<td>Strong password check</td>
<td>Check for a strong password</td>
<td>[Y]</td>
</tr>
</tbody>
</table>
To change the VLAN ID after the initial APIC setup, export your configurations, rebuild the fabric with a new infrastructure VLAN ID and import the configurations so that the fabric does not revert to the old infrastructure VLAN ID. See the KB article about Using Export and Import to Recover Configuration State.

Example

The following is a sample of the initial setup dialog as displayed on the console:

Cluster configuration ...
Enter the fabric name [ACI Fabric1]:
Enter the fabric ID (1-128) [1]:
Enter the number of active controllers in the fabric (1-9) [3]:
Enter the POD ID (1-9) [1]:
Is this a standby controller? [NO]:
Enter the controller ID (1-3) [1]:
Enter the controller name [apic1]: sec-ifc5
Enter address pool for TEP addresses [10.0.0.0/16]:
Note: The infra VLAN ID should not be used elsewhere in your environment and should not overlap with any other reserved VLANs on other platforms.
Enter the VLAN ID for infra network (2-4094): 3967
Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
Enable IPv6 for Out of Band Mgmt Interface? [N]:
Enter the IPv4 address [192.168.10.1/24]: 172.23.142.29/21
Enter the IPv4 address of the default gateway [None]: 172.23.136.1
Enter the interface speed/duplex mode [auto]:

admin user configuration ...
Enable strong passwords? [Y]:
Enter the password for admin:
Reenter the password for admin:

Cluster configuration ...
Fabric name: ACI Fabric1
Fabric ID: 1
Number of controllers: 3
Controller name: sec-ifc5
POD ID: 1
Controller ID: 1
TEP address pool: 10.0.0.0/16
Infra VLAN ID: 3967
Multicast address pool: 225.0.0.0/15

Out-of-band management configuration ...
Management IP address: 172.23.142.29/21
Default gateway: 172.23.136.1
Interface speed/duplex mode: auto

admin user configuration ...
Strong Passwords: Y
User name: admin
Password: ********

The above configuration will be applied ...

Warning: TEP address pool, Infra VLAN ID and Multicast address pool cannot be changed later, these are permanent until the fabric is wiped.

Would you like to edit the configuration? (y/n) [n]:

Provisioning IPv6 Management Addresses on APIC Controllers

IPv6 management addresses can be provisioned on the APIC controller at setup time or through a policy once the APIC controller is operational. Pure IPv4, Pure IPv6 or dual stack (i.e both IPv6 and IPv4 addresses) are supported. The following snippet is of a typical setup screen that describes how to setup dual stack (IPv6 and IPv4) addresses for out-of-band management interfaces during the setup:

Cluster configuration ...

Enter the fabric name [ACI Fabric1]:
Enter the number of controllers in the fabric (1-9) [3]:
Enter the controller ID (1-3) [1]:
Enter the controller name [apic1]: infraipv6-ifc1
Enter address pool for TEP addresses [10.0.0.0/16]:
Note: The infra VLAN ID should not be used elsewhere in your environment and should not overlap with any other reserved VLANs on other platforms.
Enter the VLAN ID for infra network (1-4094): 3967
Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
Enable IPv6 for Out of Band Mgmt Interface? [N]: Y (Enter Y to Configure IPv6 Address for Out of Band Management Address)
Enter the IPv6 address [0:0:0:0:0:ffff:c0a8:a01/40]: 2001:420:28e:2020:0:ffff:ac1f:88e4/64 (IPv6 Address)
Enable IPv4 also for Out of Band Mgmt Interface? [Y]: (Enter Y to Configure IPv4 Address for Out of Band Management Address)
Enter the IPv4 address [192.168.10.1/24]: 172.31.136.228/21 (IPv4 Address)
Enter the IPv4 address of the default gateway [None]: 172.31.136.1 (IPv4 Gateway)
Enter the interface speed/duplex mode [auto]:

admin user configuration ...
Enable strong passwords? [Y]:
Enter the password for admin:
Reenter the password for admin:

Accessing the GUI

Procedure

Step 1 Open one of the supported browsers:
• Chrome version 59 (at minimum)
- Firefox version 54 (at minimum)
- Internet Explorer version 11 (at minimum)
- Safari version 10 (at minimum)

**Note** A known issue exists with the Safari browser and unsigned certificates. Read the information presented here before accepting an unsigned certificate for use with WebSockets. When you access the HTTPS site, the following message appears:

“Safari can’t verify the identity of the website APIC. The certificate for this website is invalid. You might be connecting to a website that is pretending to be an APIC, which could put your confidential information at risk. Would you like to connect to the website anyway?”

To ensure that WebSockets can connect, you must do the following:

Click **Show Certificate**.

Choose **Always Trust** in the three drop-down lists that appear.

If you do not follow these steps, WebSockets will not be able to connect.

---

**Step 2**

Enter the URL: **https://mgmt_ip-address**

Use the out-of-band management IP address that you configured during the initial setup. For example, https://192.168.10.1.

**Note** Only https is enabled by default. By default, http and http-to-https redirection are disabled.

**Step 3**

When the login screen appears, enter the administrator name and password that you configured during the initial setup.

**Step 4**

In the **Domain** field, from the drop-down list, choose the appropriate domain that is defined.

If multiple login domains are defined, the **Domain** field is displayed. If the user does not choose a domain, the DefaultAuth login domain is used for authentication by default. This may result in login failure if the username is not in the DefaultAuth login domain.

---

**What to do next**

To learn about the features and operation of the Application Centric Infrastructure fabric and the Application Policy Infrastructure Controller, see the available white papers and the *Cisco Application Centric Infrastructure Fundamentals Guide*.

---

**Accessing the REST API**

**Procedure**

By using a script or a browser-based REST client, you can send an API POST or GET message of the form: **https://apic-ip-address/api/api-message-url**

Use the out-of-band management IP address that you configured during the initial setup.
Accessing the NX-OS Style CLI

You can access the NX-OS style CLI either directly from a terminal or through the APIC GUI.

For information about using the NX-OS style CLI commands, see the *Cisco APIC NX-OS Style Command-Line Interface Configuration Guide* and the *Cisco APIC NX-OS Style CLI Command Reference*.

**Guidelines and Restrictions for the NX-OS Style CLI**

- The CLI is supported only for users with administrative login privileges.
- The APIC NX-OS style CLI uses similar syntax and other conventions to the Cisco NX-OS CLI, but the APIC operating system is not a version of Cisco NX-OS software. Do not assume that a Cisco NX-OS CLI command works with or has the same function on the APIC CLI.
- If FIPS is enabled in the Cisco ACI setups, then SHA256 support is mandatory on the SSH Client. Additionally, to have the SHA256 support, the openssh-client must be running version 6.6.1 or higher.
- From Cisco APIC Release 1.0 until Release 1.2, the default CLI was a Bash shell with commands to directly operate on managed objects (MOs) and properties of the Management Information Model. Beginning with Cisco APIC Release 1.2, the default CLI is a NX-OS style CLI. The object model CLI is available by typing the `bash` command at the initial CLI prompt.

**Accessing the NX-OS Style CLI from a Terminal**

**Procedure**

**Step 1**

From a secure shell (SSH) client, open an SSH connection to APIC at `username@ip-address`.

Use the administrator login name and the out-of-band management IP address that you configured during the initial setup. For example, `admin@192.168.10.1`.

**Step 2**

When prompted, enter the administrator password.

**What to do next**

When you enter the NX-OS style CLI, the initial command level is the EXEC level. You can stay in EXEC mode or you can type `configure` to enter global configuration mode. In any mode, type `?` to see the available commands.
For information about using the NX-OS style CLI commands, see the Cisco APIC NX-OS Style Command-Line Interface Configuration Guide and the Cisco APIC NX-OS Style CLI Command Reference.

### Accessing the NX-OS Style CLI from the GUI

**Procedure**

1. From the menu bar, choose **System > Controllers**.
2. In the navigation pane, click **Controllers**.
3. Right-click the desired APIC and choose **Launch SSH**.
4. Follow the displayed instructions to open an SSH session to the selected controller.

**What to do next**

When you enter the NX-OS style CLI, the initial command level is the EXEC level. You can stay in EXEC mode or you can type `configure` to enter global configuration mode. In any mode, type `?` to see the available commands.

For information about using the NX-OS style CLI commands, see the Cisco APIC NX-OS Style Command-Line Interface Configuration Guide and the Cisco APIC NX-OS Style CLI Command Reference.

### Accessing the Object Model CLI

**Note**

From Cisco APIC Release 1.0 until Release 1.2, the default CLI was a Bash shell with commands to directly operate on managed objects (MOs) and properties of the Management Information Model. Beginning with Cisco APIC Release 1.2, the default CLI is a NX-OS style CLI. The object model CLI is available by typing the `bash` command at the initial CLI prompt.

**Procedure**

1. From a secure shell (SSH) client, open an SSH connection to `username@ip-address`.
   
   Use the administrator login name and the out-of-band management IP address that you configured during the initial setup. For example, `ssh admin@192.168.10.1`.

2. When prompted, enter the administrator password that you configured during the initial setup.
   
   With Cisco APIC Releases 1.0 and 1.1, you are now in the object model CLI. With Cisco APIC Release 1.2, you are now in the NX-OS style CLI for APIC.

3. With Cisco APIC Release 1.2, type `bash` to enter the object model CLI.
   
   This example shows how to enter the object model CLI and how to return to the NX-OS style CLI:
$ ssh admin@192.168.10.1
Application Policy Infrastructure Controller
admin@192.168.10.1's password: cisco123
apic# <---- NX-OS style CLI prompt
apic# bash
admin@apic1:~> <---- object model CLI prompt
admin@apic1:~> exit
apic#

What to do next

Every user must use the shared directory called /home. This directory gives permissions for a user to create directories and files; files created within /home inherit the default umask permissions and are accessible by the user and by root. We recommend that users create a /home/userid directory to store files, such as /home/jsmith, when logging in for the first time.

For more information about accessing switches using the ACI CLI using modes of operation such as BASH or VSH, see the Cisco APIC Command Line Interface User Guide and the Cisco ACI Switch Command Reference.

For detailed information about configuring the APIC CLI, see the Cisco APIC Object Model Command Line Interface User Guide.
APIC GUI Overview

This chapter contains the following sections:

- Overview of the GUI, on page 17
- Menu Bar and Submenu Bar, on page 18
- Navigation Pane, on page 23
- Work Pane, on page 24
- Show Me How, on page 25
- Personalizing the Interface, on page 25
- Deployment Warning and Policy Usage Information, on page 26
- Graphical Configuration of Ports, on page 27
- Viewing an API Interchange in the GUI, on page 28
- GUI Icons, on page 30

Overview of the GUI

The APIC GUI is a browser-based graphical interface for configuring and monitoring the ACI fabric. The GUI is organized to provide hierarchical navigation to all components, logical and physical, of the overall system. The primary control regions of the GUI are shown in the following figure.
The functions of these regions are described in the following links:

1. **Menu bar and tool icons**—See *Menu Bar and Submenu Bar*, on page 18
2. **Submenu bar**—See *Menu Bar and Submenu Bar*, on page 18
3. **Navigation pane**—See *Navigation Pane*, on page 23
4. **Work pane**—See *Work Pane*, on page 24
5. **Last Login**—Displays the date and time of the last instance of the current user's login.
6. **Show Me How**—(currently inactive)

As you operate the GUI to make configuration changes and retrieve information, the GUI communicates with the underlying operating system by exchanging REST API messages. You can observe these API messages using the API Inspector tool described in *Viewing an API Interchange in the GUI*, on page 28.

---

**Note**

The Basic UI is deprecated in Cisco APIC Release 3.1(1). Cisco does not recommend using the Basic UI for configurations.

---

**Menu Bar and Submenu Bar**

The menu bar is displayed across the top of the APIC GUI. The menu bar provides access to the main configuration tabs, along with access to tools such as search, notifications, and preferences. Immediately below the menu bar is the submenu bar, which presents specific configuration areas for each selected menu bar tab. The submenu bar tabs are different for each menu bar tab and might also differ depending upon your specific configuration or privilege level.
In the APIC GUI configuration instructions, you will see notation such as Fabric > Fabric Policies. In this example, you are asked to click the Fabric tab in the menu bar followed by the Fabric Policies tab in the submenu bar.

At the far right side of the menu bar are the following menu bar tools:

<table>
<thead>
<tr>
<th>Menu Bar Tools</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>The name of the currently logged in local user.</td>
</tr>
<tr>
<td></td>
<td>Search, on page 21</td>
</tr>
<tr>
<td></td>
<td>Alerts, on page 21</td>
</tr>
<tr>
<td></td>
<td>User Profile and Preferences, on page 22</td>
</tr>
<tr>
<td></td>
<td>System Tools, on page 22</td>
</tr>
</tbody>
</table>

The individual menu bar tabs and tools are described in the following sections.

**Menu Bar Tabs**

**System Tab**

Use the System tab to collect and display a summary of the overall system health, its history, and a table of system-level faults.

In addition, the System tab provides the following functions:

- You can configure global system policies in the System Settings submenu.
- You can view your licensing status in the Smart Licensing submenu.
- You can view user sessions in the Active Sessions submenu.

**Tenants Tab**

Use the Tenants tab in the menu bar to perform tenant management. The submenu bar provides a list of all tenants, an Add Tenant link, and links to three built-in tenants plus up to two of the most recently used tenants.

- A tenant contains policies that enable qualified users domain-based access control. Qualified users can access privileges such as tenant administration and networking administration.
- A user requires read/write privileges for accessing and configuring policies in a domain. A tenant user can have specific privileges into one or more domains.
• In a multitenancy environment, a tenant provides group user access privileges so that resources are isolated from one another (such as for endpoint groups and networking). These privileges also enable different users to manage different tenants.

The built-in tenants are:

• The common tenant is preconfigured for defining policies that provide common behavior for all the tenants in the fabric. A policy defined in the common tenant is usable by any tenant.

• The infra tenant is preconfigured for configuration related to the fabric infrastructure

• The mgmt tenant is preconfigured for inband and out-of-band connectivity configurations of hosts and fabric nodes (leafs, spines, and controllers).

---

**Note**

For Layer 2 configuration of ports, you can type into the node and path fields to filter ports.

---

**Fabric Tab**

The Fabric tab contains the following tabs in the submenu bar:

• **Inventory** tab—Displays the individual components of the fabric.

• **Fabric Policies** tab—Displays the monitoring and troubleshooting policies and fabric protocol settings or fabric maximum transmission unit (MTU) settings.

• **External Access Policies** tab—Displays the access policies that apply to the edge ports of the system. These ports are on the leaf switches that communicate externally.

---

**Virtual Networking Tab**

Use the Virtual Networking tab to view and configure the inventory of the various virtual machine (VM) managers. You can configure and create various management domains under which connections to individual management systems (such as VMware vCenters or VMware vShield) can be configured. Use the Inventory tab in the submenu bar to view the hypervisors and VMs that are managed by these VM management systems (also referred to as controllers in API).

---

**L4-L7 Services Tab**

Use the L4-L7 Services tab to perform services such as importing packages that define Layer 4 to Layer 7 devices such as a firewall, SSL offload, load balancer, context switch, SSL termination device, or intrusion prevention system (IPS). In the Inventory submenu tab, you can view existing Layer 4 to Layer 7 devices registered with the controller. The Packages submenu tab allows you to import L4-L7 device packages, which are used to define, configure, and monitor a network service device.

---

**Admin Tab**

Use the Admin tab to perform administrative functions such as authentication, authorization, and accounting functions, scheduling policies, retaining and purging records, upgrading firmware, and controlling features such as syslog, Call Home, and SNMP.
Operations Tab

The Operations tab provides the following built-in tools for planning and monitoring fabric resources.

• **Visibility & Troubleshooting**—Shows the location of specified end points in the fabric and displays the traffic path, including any L4-L7 devices.

• **Capacity Dashboard**—Displays the available capacity of configurable resources such as end points, bridge domains, tenants, and contexts.

• **ACI Optimizer**—Enables you to enter your network requirements to determine how many leaf switches you will need for your network and to learn how to deploy each application and external EPG on each leaf without violating any constraints.

• **EP Tracker**—Enables you to view virtual and bare metal endpoint connections and disconnections to leaf switches and FEXes.

• **Visualization**—Provides visualization of traffic maps.

Apps Tab

The Apps tab displays all the applications installed or uploaded to APIC. The tab allows an APIC administrator to upload, enable, upgrade, install, or uninstall a packaged application in APIC.

Menu Bar Tools

Search

Click the Search icon to display the search field. The search field enables you to locate objects by name or other distinctive fields.

*Figure 2: Search*

In Cisco APIC Release 3.2(1), the search function is improved and allows the use of wildcards (*).

Alerts

Click the alert menu bar icon to view a list of active alerts. When system alerts are available, a numeric badge will appear on the alert icon indicating the number of active alerts. When critical system notifications are available, the alert icon will blink red. To view the alerts, click the following icon.

*Figure 3: Alerts*

To disable blinking of the alert icon, remove all critical alerts from the alert list. A disabled Close button on a critical alert indicates that you must first resolve the underlying issue before the alert can be cleared.
User Profile and Preferences

To configure settings and preferences for the logged in user, click the following menu bar icon and select an item from the drop-down list.

*Figure 4: User Profile and Preferences*

The following selections are available:

- **Favorites**—Display links to menus bookmarked by the user.
  
  Menus that display the Favorites icon (⭐️) can be bookmarked by clicking the icon. This feature is added in Cisco APIC Release 3.1(1).

- **Change My Password**—Change the password of the currently logged in local user.

- **Change My SSH Keys**—Change the user's public SSH key used for certificate-based login.

- **Change My X.509 Certificate**—Change the user's X.509-format certificate for login.

- **View My Permissions**—Display the user's role-based read and write privileges for domains and accessible objects.

- **Settings**—Change general GUI settings.
  
  - **Remember Tree Selection**—Enable the GUI to keep the navigation tree expanded when returning to a window. For example, if you enable this property and expand the navigation tree in the Tenants tab, click on the Fabric tab, then return to the Tenants tab, the tree will remain expanded.

  - **Preserve Tree Divider Position**—Enable the GUI to keep the position of the tree divider after dragging the tree divider to the desired location.

  - **Disable Notification on Success**—Suppress the success dialog box notification.

  - **Disable Deployment Warning at Login**—Disable the Deployment Warning dialog box when logging in. See Deployment Warning and Policy Usage Information, on page 26.

  - **Default Page Size for Tables**—Set the GUI table size.

  - **Show All UI Sections**—Display hidden UI configuration options.

  - **Show What's New at Login**—Display splash screen at login, showing recent features.

  - **Change Deployment Settings**—Enable and set the scope of the deployment notification. See Deployment Warning and Policy Usage Information, on page 26.

- **Logout**—Exit the APIC configuration GUI.

System Tools

To access the system tools, click the following menu bar icon and select an item from the drop-down list.
The following selections are available:

- **Help**—Display the online help.
- **Documentation**—Display links to API documentation and to the APIC documentation home page.
- **Show API Inspector**—Open the API Inspector, which is a built-in tool of the APIC that allows you to view the internal API messages between the GUI and the APIC operating system to execute tasks. For more information, see Viewing an API Interchange in the GUI, on page 28.
- **Start Remote Logging**—Forward logging information to a remote URL.
- **Object Store Browser**—Open the Managed Object Browser, or Visore, which is a utility built into APIC that provides a graphical view of the managed objects (MOs) using a browser.
- **Show Debug Info**—Open a status bar at the bottom of the GUI to display information such as current managed object (MO) and system time. When the status bar is open, this selection changes to **Hide Debug Info**.
- **About**—Display the APIC version.

**Note**
Global system settings are configured in **System > System Settings**.

---

**Navigation Pane**

Use the **Navigation** pane, which is on the left side of the APIC GUI below the submenu bar, to navigate to all elements of the submenu category.

For each submenu category, the **Navigation** pane is organized as a hierarchical tree of objects, logical and physical, related to that category. These objects typically represent ports, policies, or groupings of other objects. When you select an object in the **Navigation** pane, details of the object display in the **Work** pane.

**Note**
In Cisco APIC Release 3.2(1), the navigation tree was reorganized in several places in order to group items such as switches, interfaces, and policies.

When you right-click an object in the **Navigation** pane, you might be presented with a menu of possible actions related to the object, such as one or more of the following actions:

- **Delete**—Delete the object.
- **Create <type of object>**—Create a new object.
- **Save as...**—Download the object and its properties in JSON or XML format to a local file.
- **Post...**—Export the object and its properties to an existing local file.
• **Share**—Displays the URL of the object. You can copy the URL and send it to others.

• **Open In Object Store Browser**—Open the object in Visore, a built-in utility that displays an object and its properties. This information may be useful in troubleshooting or for developing API tools.

• **Clone**—Create a copy of the object. This action is useful for deriving a new contract or policy based on an existing contract or policy.

---

**Note**

If any container in the *Navigation* pane, for example *Application Profiles* under a *Tenant*, contains more than 40 profiles, you cannot click on a profile and expand it in the *Navigation* pane. You must select the desired profile from the *Work* pane and expand it.

---

### Work Pane

Use the *Work* pane, which is on the right side of the APIC GUI, to display details about the component that you selected in the *Navigation* pane.

The *Work* pane includes the following elements:

• A content area that displays tabs. These tabs enable you to access information that is related to the component that you chose in the *Navigation* pane. The tabs displayed in the content area depend upon the selected component.

• A link to context-sensitive online help that is represented by a question mark icon in the upper right corner.

• For some components, a link to conceptual information related to the component, represented by a list icon in the upper right corner.

• For some pages, a button allowing you to bookmark the page as a Favorite, represented by a star icon in the upper right corner.

Bookmarked links to Favorite pages are accessible from the User Profile icon in the Menu Bar. The Favorites feature is added in Cisco APIC Release 3.1(1).

### Common Pages in the Work Pane

In addition to displaying specific task menus, the Work pane also displays several types of special-purpose menus described in this section.

#### Quick Start Pages

Many APIC menu and submenu tabs open an initial Quick Start page, which summarizes the purpose of the tab, provides links to step-by-step instructions and videos for commonly-used procedures, and provides shortcut links to commonly-used subsections within the tab. An overall Quick Start page at *System > QuickStart* assists you in performing common and basic procedures, providing step-by-step instructions, available concept information, and links to main functional areas in the GUI.
Dashboard Pages

Dashboard pages provide at-a-glance summaries of the status of the ACI system and major system components, including health score trends, components with below-threshold health scores, and fault counts. You can configure health score thresholds to determine when components will appear in the dashboard. The system dashboard page at System > Dashboard summarizes the health of the overall ACI system, while switch dashboard pages at Fabric > Inventory > Pod n > component > Dashboard summarize the health and faults of each spine and leaf switch.

Summary Pages

With Cisco APIC Release 3.2(1), the APIC GUI folder navigation is restructured to reduce the number of folders and to consolidate related configuration areas. As part of the reorganization, many top-level folders in the Navigation pane now display tile-based Summary pages in the Work pane that link to subfolders. Some Summary pages, such as those in Fabric > Inventory, contain tiles summarizing major components along with brief health and fault information for each component. Other Summary pages, such as those in Fabric > Fabric Policies, contain tiles that describe the configuration areas served by the contained folders.

Show Me How

The Show Me How feature provides guided support for many common GUI tasks. Click the Show Me How tab to open a list of tasks with available Show Me How modules. For each task, an active overlay guides you step-by-step through the selected configuration procedure, with an on-screen pointer to the next configuration item and with context-based help information about configuration choices.

Guidelines and Restrictions for Using Show Me How

- If you deviate while in progress of a Show Me How module, you will no longer be able to continue.
- You must have IPv4 enabled to use the Show Me How modules.

Personalizing the Interface

Naming the APIC GUI

An ACI controller cluster comprises three or more APICs. In some cases, it might be helpful to know which APIC you are viewing. In Cisco APIC Release 3.2(1) and later releases, perform the following steps to add a custom name to the heading of the APIC GUI.

Before you begin

Note

This feature is available in Cisco APIC Release 3.2(1) and later releases.
Procedure

Step 1  On the menu bar, choose Admin > AAA.
Step 2  In the Navigation pane, click Security Management.
Step 3  In the User Management - Security Management menu, type the desired APIC name in the GUI Alias box.
Step 4  Click Submit.

The APIC name appears in parentheses at the top left of the GUI.

Adding a Login Banner to the CLI or GUI

You can define banners to be displayed when the user is prompted to log in to the CLI or GUI. The CLI banner is a simple text string to be printed at the terminal before the password prompt. You can define a banner for the APIC CLI and a separate banner for the switch CLI. The GUI banner displays at the APIC URL before user login authentication. The GUI banner is defined as a URL of a site hosting the desired HTML.

Procedure

Step 1  On the menu bar, choose Admin > AAA.
Step 2  In the Navigation pane, click Security Management.
Step 3  In the User Management - Security Management menu, complete the following fields as desired:
   a) To configure an APIC CLI banner, type the banner text into the Controller CLI Banner textbox.
   b) To configure a switch CLI banner, type the banner text into the Switch CLI Banner textbox.
   c) To configure an APIC GUI banner, type the URL of a site hosting the desired HTML into the GUI Banner (URL) textbox.

Note the URL site owner must allow the site to be placed in an iFrame to display the informational banner. If the owner of the site sets the x-frame-option to deny or sameorigin, the site the URL points to will not appear.

Step 4  Click Submit.

Deployment Warning and Policy Usage Information

By configuring Deployment Warning Settings, you can enable the automatic display of policy usage information whenever you modify or delete policies that might affect other resources or policies. The policy usage information allows you to identify which resources and policies are being used by the policy that you are currently modifying or deleting. Tables display the nodes where the given policy is used and other policies that use this policy. By default, usage information is displayed within a dialog box whenever you attempt to modify a policy. Also, at any time, you can click the Show Usage button at the bottom of the screen to view the same information.

The Deployment Warning Settings dialog box allows you to enable and alter the scope of deployment notification that displays policy usage information. You can access this dialog box by selecting Change
Deployment Settings in the menu bar tool User Settings and Preferences drop-down list or through a button on the Policy Usage Information dialog box.

When the Policy tab is selected in the upper right corner of the Deployment Warning Settings dialog box, you can configure the following policy options:

- **(Global) Show Deployment Warning on Delete/Modify**—Enable the Deployment Warning notification for every policy deletion or modification across the APIC.

- **(Local) Show Deployment Warning on Delete/Modify**—Set the rule for the Deployment Warning notification for specific policy configuration.
  - Use Global Settings—Use the setting selected for (Global) Show Deployment Warning on Delete/Modify.
  - Yes—Display the Deployment Warning notification before submitting configuration modifications on any policy change. Valid for this browser session only.
  - No—Do not display the Deployment Warning notification before submitting configuration modifications on any policy change. Valid for this browser session only.

When the History tab is selected in the upper right corner of the Deployment Warning Settings dialog box, you can view tables of Events and Audit Log entries for previous deployment warnings.

### Graphical Configuration of Ports

The APIC GUI provides a graphical method for configuring ports, port channels, and virtual port channels on the leaf switches in the fabric, configure ports for dynamic breakout, and link interfaces to FEX switches. This configuration capability is present in the following GUI locations:

- Fabric > Inventory > Topology
- Fabric > Inventory > Pod
- Fabric > Inventory > Pod > Leaf
- Fabric > Inventory > Pod > Spine

In the Work pane's Interface tab, click on the + button (at the top left), select one or more switches to configure, and click Add Selected. To select multiple switches, use Ctrl+Click or Shift+Click.

The switches are graphically displayed with their ports and links. If you have configured a breakout port, a block containing the sub ports is displayed below the leaf diagram.

**Note**

If you accessed the Interface tab from a leaf switch, the leaf switch is automatically added.

Select the interfaces to configure. When interfaces are selected, the available configuration buttons appear. Depending on the number of selected interfaces and where they are located, you can then click one of the following buttons at the top of the page:

- **L2**—Layer 2. Visible when you click one or more leaf interfaces on the switch diagrams.
- **PC**—Port Channel. Visible when you click one or more leaf interfaces on the switch diagrams.
• **VPC**—Virtual Port Channel. Visible when you click at least one interface on two switch diagrams.
• **FEX**—Fabric Extender. Visible when you click one or more leaf interfaces on the switch diagrams.
• **Breakout**—Breakout mode. Visible when you click one or more leaf interfaces on the switch diagrams.
• **Spine**—Visible when you click one or more leaf interfaces on the switch diagrams.

## Viewing an API Interchange in the GUI

When you perform a task in the APIC graphical user interface (GUI), the GUI creates and sends internal API messages to the operating system to execute the task. By using the API Inspector, which is a built-in tool of the APIC, you can view and copy these API messages. A network administrator can replicate these messages in order to automate key operations, or you can use the messages as examples to develop external applications that will use the API.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Log in to the APIC GUI.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In the upper right corner of the APIC window, click the &quot;welcome, &lt;name&gt;&quot; message to view the drop-down list.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>In the drop-down list, choose the <strong>Show API Inspector</strong>. The <strong>API Inspector</strong> opens in a new browser window.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>In the <strong>Filters</strong> toolbar of the <strong>API Inspector</strong> window, choose the types of API log messages to display. The displayed messages are color-coded according to the selected message types. This table shows the available message types:</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>trace</td>
<td>Displays trace messages.</td>
</tr>
<tr>
<td>debug</td>
<td>Displays debug messages. This type includes most API commands and responses.</td>
</tr>
<tr>
<td>info</td>
<td>Displays informational messages.</td>
</tr>
<tr>
<td>warn</td>
<td>Displays warning messages.</td>
</tr>
<tr>
<td>error</td>
<td>Displays error messages.</td>
</tr>
<tr>
<td>fatal</td>
<td>Displays fatal messages.</td>
</tr>
<tr>
<td>all</td>
<td>Checking this checkbox causes all other checkboxes to become checked. Unchecking any other checkbox causes this checkbox to be unchecked.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>In the <strong>Search</strong> toolbar, you can search the displayed messages for an exact string or by a regular expression. This table shows the search controls:</td>
</tr>
</tbody>
</table>
In the **Options** toolbar, you can arrange the displayed messages.

This table shows the available options:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log</td>
<td>Check this checkbox to enable logging.</td>
</tr>
<tr>
<td>Wrap</td>
<td>Check this checkbox to enable wrapping of lines to avoid horizontal scrolling of the log list.</td>
</tr>
<tr>
<td>Newest at the top</td>
<td>Check this checkbox to display log entries in reverse chronological order.</td>
</tr>
<tr>
<td>Scroll to latest</td>
<td>Check this checkbox to scroll immediately to the latest log entry.</td>
</tr>
<tr>
<td>Clear</td>
<td>Click this button to clear the log list.</td>
</tr>
<tr>
<td>Close</td>
<td>Click this button to close the API Inspector.</td>
</tr>
</tbody>
</table>

### Example

This example shows two debug messages in the API Inspector window:

```
response: {"imdata": [{"infraInfra": {"attributes": {"instanceId": "0:0", "childAction": "", "dn": "uni/infra", "lcOwn": "local", "name": "", "replTs": "never", "status": ""}]}]}
```

```
query-target=subtree&subscription=yes
```
### GUI Icons

#### Table 7: Frequently Displayed Icons in the APIC GUI

<table>
<thead>
<tr>
<th>Icons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Bookmark" /></td>
<td>Bookmark this page</td>
</tr>
<tr>
<td><img src="image" alt="Help" /></td>
<td>Displays online help information for the current menu page</td>
</tr>
<tr>
<td><img src="image" alt="Concept" /></td>
<td>Displays concept information for the current menu page</td>
</tr>
<tr>
<td><img src="image" alt="Quick Start" /></td>
<td>Quick Start</td>
</tr>
<tr>
<td><img src="image" alt="Video" /></td>
<td>Plays a Quick Start video</td>
</tr>
<tr>
<td><img src="image" alt="Quick Procedure" /></td>
<td>Displays a Quick Start procedure</td>
</tr>
<tr>
<td><img src="image" alt="Link" /></td>
<td>Link to related section</td>
</tr>
<tr>
<td><img src="image" alt="Topology" /></td>
<td>Topology</td>
</tr>
<tr>
<td><img src="image" alt="Pod" /></td>
<td>Pod</td>
</tr>
<tr>
<td><img src="image" alt="Collapse" /></td>
<td>Collapse Tree View</td>
</tr>
<tr>
<td><img src="image" alt="Expand" /></td>
<td>Expand Tree View</td>
</tr>
<tr>
<td><img src="image" alt="Nodes" /></td>
<td>Collapse All Nodes</td>
</tr>
</tbody>
</table>
## Fault, Statistics, and Health Level Icons

### Table 8: Severity Levels of Faults Displayed in the APIC GUI

<table>
<thead>
<tr>
<th>Icons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Critical Icon" /></td>
<td>Critical—This icon displays a fault level with critical severity.</td>
</tr>
<tr>
<td><img src="image" alt="Major Icon" /></td>
<td>Major—This icon displays a fault level with major severity.</td>
</tr>
<tr>
<td><img src="image" alt="Minor Icon" /></td>
<td>Minor—This icon displays a fault level with minor severity.</td>
</tr>
<tr>
<td><img src="image" alt="Warning Icon" /></td>
<td>Warning—This icon displays a fault level that requires a warning.</td>
</tr>
</tbody>
</table>
CHAPTER 4

Fabric Initialization and Switch Discovery

This chapter contains the following sections:

- Initializing the Fabric, on page 33
- Switch Discovery, on page 35
- Graceful Insertion and Removal (GIR) Mode, on page 38

Initializing the Fabric

About Fabric Initialization

You can build a fabric by adding switches to be managed by the APIC and then validating the steps using the GUI, the CLI, or the API.

Note

Before you can build a fabric, you must have already created an APIC cluster over the out-of-band network.

Example Topology

An example topology is as follows:

- Two spine switches (spine1, spine2)
- Two leaf switches (leaf1, leaf2)
- Three instances of APIC (apic1, apic2, apic3)

The following figure shows an example of a fabric topology.
Example Topology Connections

An example topology with connection details is as follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>Connection Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>leaf1</td>
<td>eth1/1 = apic1 (eth2/1)</td>
</tr>
<tr>
<td></td>
<td>eth1/2 = apic2 (eth2/1)</td>
</tr>
<tr>
<td></td>
<td>eth1/3 = apic3 (eth2/1)</td>
</tr>
<tr>
<td></td>
<td>eth1/49 = spine1 (eth5/1)</td>
</tr>
<tr>
<td></td>
<td>eth1/50 = spine2 (eth5/2)</td>
</tr>
<tr>
<td>leaf2</td>
<td>eth1/1 = apic1 (eth2/2)</td>
</tr>
<tr>
<td></td>
<td>eth1/2 = apic2 (eth2/2)</td>
</tr>
<tr>
<td></td>
<td>eth1/3 = apic3 (eth2/2)</td>
</tr>
<tr>
<td></td>
<td>eth1/49 = spine2 (eth5/1)</td>
</tr>
<tr>
<td></td>
<td>eth1/50 = spine1 (eth5/2)</td>
</tr>
<tr>
<td>spine1</td>
<td>eth5/1 = leaf1 (eth1/49)</td>
</tr>
<tr>
<td></td>
<td>eth5/2 = leaf2 (eth1/50)</td>
</tr>
<tr>
<td>spine2</td>
<td>eth5/1 = leaf2 (eth1/49)</td>
</tr>
<tr>
<td></td>
<td>eth5/2 = leaf1 (eth1/50)</td>
</tr>
</tbody>
</table>
Switch Discovery

About Switch Discovery with the APIC

The APIC is a central point of automated provisioning and management for all the switches that are part of the ACI fabric. A single data center might include multiple ACI fabrics; each data center might have its own APIC cluster and Cisco Nexus 9000 Series switches that are part of the fabric. To ensure that a switch is managed only by a single APIC cluster, each switch must be registered with that specific APIC cluster that manages the fabric.

The APIC discovers new switches that are directly connected to any switch it currently manages. Each APIC instance in the cluster first discovers only the leaf switch to which it is directly connected. After the leaf switch is registered with the APIC, the APIC discovers all spine switches that are directly connected to the leaf switch. As each spine switch is registered, that APIC discovers all the leaf switches that are connected to that spine switch. This cascaded discovery allows the APIC to discover the entire fabric topology in a few simple steps.

Switch Registration with the APIC Cluster

Before you begin registering a switch, make sure that all switches in the fabric are physically connected and booted in the desired configuration. For information about the installation of the chassis, see http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/products-installation-guides-list.html.

After a switch is registered with the APIC, the switch is part of the APIC-managed fabric inventory. With the Application Centric Infrastructure fabric (ACI fabric), the APIC is the single point of provisioning, management, and monitoring for switches in the infrastructure.

The infrastructure IP address range must not overlap with other IP addresses used in the ACI fabric for in-band and out-of-band networks.

Registering the Unregistered Switches Using the GUI

The infrastructure IP address range must not overlap with other IP addresses used in the ACI fabric for in-band and out-of-band networks.

Before you begin

Make sure that all switches in the fabric are physically connected and booted.
**Procedure**

**Step 1** On the menu bar, choose FABRIC > INVENTORY.

**Step 2** In the Navigation pane, click Fabric Membership.
In the Work pane, in the Fabric Membership table, a single leaf switch is displayed with an ID of 0. It is the leaf switch that is connected to apic1.

**Step 3** Configure the ID by double-clicking the leaf switch row, and performing the following actions:

a) In the ID field, add the appropriate ID (leaf1 is ID 101, and leaf 2 is ID 102).
   The ID must be a number that is greater than 100 because the first 100 IDs are for APIC appliance nodes.

b) In the Switch Name field, add the name of the switch, and click Update.

   **Note** After an ID is assigned, it cannot be updated. The switch name can be updated by double-clicking the name and updating the Switch Name field.

An IP address gets assigned to the switch, and in the Navigation pane, the switch is displayed under the pod.

**Step 4** Monitor the Work pane until one or more spine switches appear.

**Step 5** Configure the ID by double-clicking the spine switch row, and perform the following actions:

a) In the ID field, add the appropriate ID (spine1 is ID 203 and spine 2 is ID 204).

   **Note** It is recommended that leaf nodes and spine nodes be numbered differently. For example, number spines in the 200 range and number leaves in the 100 range.

b) In the Switch Name field, add the name of the switch, and click Update.

An IP address gets assigned to the switch, and in the Navigation pane, the switch is displayed under the pod. Wait until all remaining switches appear in the Node Configurations table before you go to the next step.

**Step 6** For each switch listed in the Fabric Membership table, perform the following steps:

a) Double-click the switch, enter an ID and a Name, and click Update.

b) Repeat for the next switch in the list.

---

**Switch Discovery Validation and Switch Management from the APIC**

After the switches are registered with the APIC, the APIC performs fabric topology discovery automatically to gain a view of the entire network and to manage all the switches in the fabric topology.

Each switch can be configured, monitored, and upgraded from the APIC without having to access the individual switches.

**Validating the Registered Switches Using the GUI**

**Procedure**

**Step 1** On the menu bar, choose FABRIC > INVENTORY.

**Step 2** In the Navigation pane, expand Fabric Membership.
The switches in the fabric are displayed with their node IDs. In the Work pane, all the registered switches are displayed with the IP addresses that are assigned to them.

### Validating the Fabric Topology

After all the switches are registered with the APIC cluster, the APIC automatically discovers all the links and connectivity in the fabric and discovers the entire topology as a result.

### Validating the Fabric Topology Using the GUI

**Procedure**

**Step 1**  
On the menu bar, choose FABRIC > INVENTORY.

**Step 2**  
In the Navigation pane, click TOPOLOGY.  
The displayed summary shows the quantity and health of all pods, switches, APIC instances, and EPGs.

**Step 3**  
In the Work pane, click the TOPOLOGY tab.  
If an Inter-Pod Network block diagram is displayed, click View Pod in the desired pod.  
The displayed diagram shows all attached switches, APIC instances, and links.

**Step 4**  
(Optional) Hover over any component to view its health, status, and inventory information.

**Step 5**  
(Optional) To view the port-level connectivity of a leaf switch or spine switch, double-click its icon in the topology diagram.

**Step 6**  
(Optional) To refresh the topology diagram, click the icon in the upper right corner of the Work pane.

### Unmanaged Switch Connectivity in VM Management

The hosts that are managed by the VM controller (for example, a vCenter), can be connected to the leaf port through a Layer 2 switch. The only prerequisite required is that the Layer 2 switch must be configured with a management address, and this management address must be advertised by Link Layer Discovery Protocol (LLDP) or Cisco Discovery Protocol (CDP) on the ports that are connected to the switches. Layer 2 switches are automatically discovered by the APIC, and they are identified by the management address. The following figure shows the APIC GUI displaying unmanaged switches in the Fabric > Inventory view.
Graceful Insertion and Removal (GIR) Mode

Graceful Insertion and Removal (GIR) Mode

The Graceful Insertion and Removal (GIR) mode, or maintenance mode, allows you to isolate a switch from the network with minimum service disruption. In the GIR mode you can perform real-time debugging without affecting traffic.

You can use graceful insertion and removal to gracefully remove a switch and isolate it from the network in order to perform debugging operations. The switch is removed from the regular forwarding path with minimal traffic disruption. When you are finished performing the debugging operations, you can use graceful insertion to return the switch to its fully operational (normal) mode. In graceful removal, all external protocols are gracefully brought down except the fabric protocol (IS-IS) and the switch is isolated from the network. During maintenance mode, the maximum metric is advertised in IS-IS within the Cisco Application Centric Infrastructure (Cisco ACI) fabric and therefore the maintenance mode TOR does not attract traffic from the spine switches. In addition, all the front-panel interfaces are shutdown on the switch except the fabric interfaces. In graceful insertion, the switch is automatically decommissioned, rebooted, and recommissioned. When recommissioning is completed, all external protocols are restored and maximum metric in IS-IS is reset after 10 minutes.

The following protocols are supported:

- Border Gateway Protocol (BGP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Intermediate System-to-Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)
- Link Aggregation Control Protocol (LACP)
Important Notes

• Upgrading or downgrading a switch in maintenance mode is not supported.

• While the switch is in maintenance mode, the Ethernet port module stops propagating the interface related notifications. As a result, if the remote switch is rebooted or the fabric link is flapped during this time, the fabric link will not come up afterward unless the switch is manually rebooted (using the `acidiag touch clean` command), decommissioned, and recommissioned.

• For multi-pod, **IS-IS metric for redistributed routes** should be set to less than 63. To set the **IS-IS metric for redistributed routes**, choose Fabric > Fabric Policies > Pod Policies > IS-IS Policy.

• Existing GIR supports all Layer 3 traffic diversion. With LACP, all the Layer 2 traffic is also diverted to the redundant node. Once a node goes into maintenance mode, LACP running on the node immediately informs neighbors that it can no longer be aggregated as part of port-channel. All traffic is then diverted to the vPC peer node.

• For a GIR upgrade, Cisco Application Policy Infrastructure Controller (Cisco APIC)-connected leaf switches must be put into different maintenance groups such that the Cisco APIC-connected leaf switches get upgraded one at a time.

Removing a Switch to Maintenance Mode Using the GUI

Use this procedure to remove a switch to maintenance mode using the GUI. During the removal of a switch to maintenance mode, the out-of-band management interfaces will remain up and accessible.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>On the menu bar, choose Fabric &gt; Inventory.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>In the navigation pane, click Fabric Membership.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>In the work pane, click Actions &gt; Maintenance (GIR)</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

The gracefully removed switch displays Debug Mode in the Status column.

Removing a Switch to Maintenance Mode Using the CLI

Use this procedure to remove a switch to maintenance mode using the CLI.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no]debug-switch node_id or node_name</td>
<td>Removes the switch to maintenance mode.</td>
</tr>
</tbody>
</table>
Removing a Switch to Maintenance Mode Using the REST API

Use this procedure to remove a switch to maintenance mode using the REST API.

Procedure

Remove a switch to maintenance mode.

Example:

```
POST
https://<IP address>/api/node/mo/uni/fabric/outofsvc
<fabricOOServicePol descr="" dn="" name="default" nameAlias="" ownerKey="" ownerTag="">
   <fabricRsDecommissionNode debug="yes" dn="">
      removeFromController="no" tDn="topology/pod-1/node-102"/>
</fabricOOServicePol>
```

Inserting a Switch to Operational Mode Using the GUI

Use this procedure to insert a switch to operational mode using the GUI.

Procedure

- **Step 1**: On the menu bar, choose Fabric > Inventory.
- **Step 2**: In the navigation pane, click Fabric Membership.
- **Step 3**: In the work pane, click Actions > Commission.
- **Step 4**: Click OK.

Inserting a Switch to Operation Mode Using CLI

Use this procedure to insert a switch to operational mode using the CLI.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no]no debug-switch node_id or node_name</td>
<td>Inserts the switch to operational mode.</td>
</tr>
</tbody>
</table>

Inserting a Switch to Operational Mode Using the REST API

Use this procedure to insert a switch to operational mode using the REST API.
Procedure

Insert a switch to operational mode.

Example:

POST
https://1<IP address>/api/node/mo/uni/fabric/outofsvc.xml

<fabricOOServicePol descr="" dn="" name="default" nameAlias="" ownerKey="" ownerTag="">
  <fabricRsDecommissionNode debug="yes" dn="" removeFromController="no" tDn="topology/pod-1/node-102" status="deleted"/>
</fabricOOServicePol>
Inserting a Switch to Operational Mode Using the REST API
APIC Cluster Overview

The Cisco Application Policy Infrastructure Controller (APIC) appliance is deployed in a cluster. A minimum of three controllers are configured in a cluster to provide control of the Cisco ACI fabric. The ultimate size of the controller cluster is directly proportionate to the size of the ACI deployment and is based on transaction-rate requirements. Any controller in the cluster can service any user for any operation, and a controller can be transparently added to or removed from the cluster.

This section provides guidelines and examples related to expanding, contracting, and recovering the APIC cluster.

Expanding the Cisco APIC Cluster

Expanding the Cisco APIC cluster is the operation to increase any size mismatches, from a cluster size of N to size N+1, within legal boundaries. The operator sets the administrative cluster size and connects the APICs with the appropriate cluster IDs, and the cluster performs the expansion.

During cluster expansion, regardless of in which order you physically connect the APIC controllers, the discovery and expansion takes place sequentially based on the APIC ID numbers. For example, APIC2 is discovered after APIC1, and APIC3 is discovered after APIC2 and so on until you add all the desired APICs to the cluster. As each sequential APIC is discovered, a single data path or multiple data paths are established, and all the switches along the path join the fabric. The expansion process continues until the operational cluster size reaches the equivalent of the administrative cluster size.
Contracting the Cisco APIC Cluster

Contracting the Cisco APIC cluster is the operation to decrease any size mismatches, from a cluster size of N to size N - 1, within legal boundaries. As the contraction results in increased computational and memory load for the remaining APICs in the cluster, the decommissioned APIC cluster slot becomes unavailable by operator input only.

During cluster contraction, you must begin decommissioning the last APIC in the cluster first and work your way sequentially in reverse order. For example, APIC 4 must be decommissioned before APIC 3, and APIC 3 must be decommissioned before APIC 2.

Cluster Management Guidelines

The APIC cluster is comprised of multiple APIC controllers that provide operators a unified real time monitoring, diagnostic, and configuration management capability for the ACI fabric. To assure optimal system performance, follow the guidelines below for making changes to the APIC cluster.

Prior to initiating a change to the cluster, always verify its health. When performing planned changes to the cluster, all controllers in the cluster should be healthy. If one or more of the APIC controllers' health status in the cluster is not "fully fit", remedy that situation before proceeding. Also, assure that cluster controllers added to the APIC are running the same version of firmware as the other controllers in the APIC cluster.

Follow these general guidelines when managing clusters:

- Cisco recommends that you have at least 3 active APICs in a cluster, along with additional standby APICs. A cluster size of 3, 5, or 7 APICs is recommended. A cluster size of 4 or 6 APICs is not recommended.

- Disregard cluster information from APICs that are not currently in the cluster; they do not provide accurate cluster information.

- Cluster slots contain an APIC ChassisID. Once you configure a slot, it remains unavailable until you decommission the APIC with the assigned ChassisID.

- If an APIC firmware upgrade is in progress, wait for it to complete and the cluster to be fully fit before proceeding with any other changes to the cluster.

- When moving an APIC, first ensure that you have a healthy cluster. After verifying the health of the APIC Cluster, choose the APIC you intend to shut down. After the APIC has shutdown, move the APIC, re-connect it, and then turn it back on. From the GUI, verify that all controllers in the cluster return to a fully fit state.

- Only move one APIC at a time.

- When an APIC cluster is split into two or more groups, the ID of a node is changed and the changes are not synchronized across all APICs. This can cause inconsistency in the node IDs between APICs and also the affected leaf nodes may not appear in the inventory in the APIC GUI. When you split an APIC
cluster, decommission the affected leaf nodes from APIC and register them again, so that the inconsistency in the node IDs is resolved and the health status of the APICs in a cluster are in a fully fit state.

• Before configuring the APIC cluster, ensure that all the APICs are running the same firmware version. Initial clustering of APICs running differing versions is an unsupported operation and may cause problems within the cluster.

This section contains the following topics:

Expanding the APIC Cluster Size

Follow these guidelines to expand the APIC cluster size:

• Schedule the cluster expansion at a time when the demands of the fabric workload will not be impacted by the cluster expansion.

• If one or more of the APIC controllers’ health status in the cluster is not "fully fit", remedy that situation before proceeding.

• Stage the new APIC controller(s) according to the instructions in their hardware installation guide. Verify in-band connectivity with a PING test.

• Increase the cluster target size to be equal to the existing cluster size controller count plus the new controller count. For example, if the existing cluster size controller count is 3 and you are adding 3 controllers, set the new cluster target size to 6. The cluster proceeds to sequentially increase its size one controller at a time until all new the controllers are included in the cluster.

Note
Cluster expansion stops if an existing APIC controller becomes unavailable. Resolve this issue before attempting to proceed with the cluster expansion.

• Depending on the amount of data the APIC must synchronize upon the addition of each appliance, the time required to complete the expansion could be more than 10 minutes per appliance. Upon successful expansion of the cluster, the APIC operational size and the target size will be equal.

Note
Allow the APIC to complete the cluster expansion before making additional changes to the cluster.

Reducing the APIC Cluster Size

Follow these guidelines to reduce the APIC cluster size and decommission the APIC controllers that are removed from the cluster:

Note
Failure to follow an orderly process to decommission and power down APIC controllers from a reduced cluster can lead to unpredictable outcomes. Do not allow unrecognized APIC controllers to remain connected to the fabric.
Reducing the cluster size increases the load on the remaining APIC controllers. Schedule the APIC controller size reduction at a time when the demands of the fabric workload will not be impacted by the cluster synchronization.

If one or more of the APIC controllers' health status in the cluster is not "fully fit", remedy that situation before proceeding.

Reduce the cluster target size to the new lower value. For example if the existing cluster size is 6 and you will remove 3 controllers, reduce the cluster target size to 3.

Starting with the highest numbered controller ID in the existing cluster, decommission, power down, and disconnect the APIC controller one by one until the cluster reaches the new lower target size.

Upon the decommissioning and removal of each controller, the APIC synchronizes the cluster.

After decommissioning an APIC controller from the cluster, power it down and disconnect it from fabric. Before returning it to service, do a wiped clean back to factory reset.

Cluster synchronization stops if an existing APIC controller becomes unavailable. Resolve this issue before attempting to proceed with the cluster synchronization.

Depending on the amount of data the APIC must synchronize upon the removal of a controller, the time required to decommission and complete cluster synchronization for each controller could be more than 10 minutes per controller.

Complete the entire necessary decommissioning steps, allowing the APIC to complete the cluster synchronization accordingly before making additional changes to the cluster.

Replacing Cisco APIC Controllers in the Cluster

Follow these guidelines to replace Cisco APIC controllers:

- If the health status of any Cisco APIC controller in the cluster is not Fully Fit, remedy the situation before proceeding.

- Schedule the Cisco APIC controller replacement at a time when the demands of the fabric workload will not be impacted by the cluster synchronization.

- Make note of the initial provisioning parameters and image used on the Cisco APIC controller that will be replaced. The same parameters and image must be used with the replacement controller. The Cisco APIC proceeds to synchronize the replacement controller with the cluster.

Cluster synchronization stops if an existing Cisco APIC controller becomes unavailable. Resolve this issue before attempting to proceed with the cluster synchronization.
• You must choose a Cisco APIC controller that is within the cluster and not the controller that is being decommissioned. For example: Log in to Cisco APIC1 or APIC2 to invoke the shutdown of APIC3 and decommission APIC3.

• Perform the replacement procedure in the following order:

  1. Make note of the configuration parameters and image of the APIC being replaced.

  2. Decommission the APIC you want to replace (see Decommissioning a Cisco APIC Controller in the Cluster Using the GUI, on page 50)

  3. Commission the replacement APIC using the same configuration and image of the APIC being replaced (see Commissioning a Cisco APIC Controller in the Cluster Using the GUI, on page 50)

• Stage the replacement Cisco APIC controller according to the instructions in its hardware installation guide. Verify in-band connectivity with a PING test.

  └── Note

  Failure to decommission Cisco APIC controllers before attempting their replacement will preclude the cluster from absorbing the replacement controllers. Also, before returning a decommissioned Cisco APIC controller to service, do a wiped clean back to factory reset.

• Depending on the amount of data the Cisco APIC must synchronize upon the replacement of a controller, the time required to complete the replacement could be more than 10 minutes per replacement controller. Upon successful synchronization of the replacement controller with the cluster, the Cisco APIC operational size and the target size will remain unchanged.

  └── Note

  Allow the Cisco APIC to complete the cluster synchronization before making additional changes to the cluster.

• The UUID and fabric domain name persist in a Cisco APIC controller across reboots. However, a clean back-to-factory reboot removes this information. If a Cisco APIC controller is to be moved from one fabric to another, a clean back-to-factory reboot must be done before attempting to add such an controller to a different Cisco ACI fabric.

Expanding the Cluster Examples

Expanding the APIC Cluster Using the GUI

Procedure

Step 1

On the menu bar, choose SYSTEM > Controllers. In the Navigation pane, expand Controllers > apic_controller_name > Cluster.

You must choose an apic_controller_name that is within the cluster that you wish to expand.
In the Work pane, the cluster details are displayed. This includes the current cluster target and current sizes, the administrative, operational, and health states of each controller in the cluster.

Step 2 Verify that the health state of the cluster is Fully Fit before you proceed with contracting the cluster.

Step 3 In the Work pane, click Actions > Change Cluster Size.

Step 4 In the Change Cluster Size dialog box, in the Target Cluster Administrative Size field, choose the target number to which you want to expand the cluster. Click Submit.

Note It is not acceptable to have a cluster size of two APIC controllers. A cluster of one, three, or more APIC controllers is acceptable.

Step 5 In the Confirmation dialog box, click Yes.

In the Work pane, under Properties, the Target Size field must display your target cluster size.

Step 6 Physically connect all the APIC controllers that are being added to the cluster.

In the Work pane, in the Cluster > Controllers area, the APIC controllers are added one by one and displayed in the sequential order starting with N + 1 and continuing until the target cluster size is achieved.

Step 7 Verify that the APIC controllers are in operational state, and the health state of each controller is Fully Fit.

---

**Expanding the APIC Cluster Using the REST API**

The cluster drives its actual size to the target size. If the target size is higher than the actual size, the cluster size expands.

**Procedure**

**Step 1** Set the target cluster size to expand the APIC cluster size.

**Example:**

```plaintext
POST https://<IP address>/api/node/mo/uni/controller.xml
<infraClusterPol name='default' size=3/>
```

**Step 2** Physically connect the APIC controllers that you want to add to the cluster.

---

**Contracting the Cluster Examples**

**Contracting the APIC Cluster Using the GUI**

**Procedure**

**Step 1** On the menu bar, choose SYSTEM > Controllers. In the Navigation pane, expand Controllers > apic_controller_name > Cluster.
You must choose an `apic_controller_name` that is within the cluster and not the controller that is being decommissioned.

In the **Work** pane, the cluster details are displayed. This includes the current cluster target and current sizes, the administrative, operational, and health states of each controller in the cluster.

**Step 2** Verify that the health state of the cluster is **Fully Fit** before you proceed with contracting the cluster.

**Step 3** In the **Work** pane, click **Actions > Change Cluster Size**.

**Step 4** In the Change Cluster Size dialog box, in the **Target Cluster Administrative Size** field, choose the target number to which you want to contract the cluster. Click **Submit**.

**Note** It is not acceptable to have a cluster size of two APIC controllers. A cluster of one, three, or more APIC controllers is acceptable.

**Step 5** In the **Work** pane, in the **Controllers** area, choose the APIC that is last in the cluster.

**Example:**
In a cluster of three, the last in the cluster is three as identified by the controller ID.

**Step 6** Click **Actions > Decommission**. The **Confirmation** dialog box displays. Click **Yes**.
The decommissioned controller displays **Unregistered** in the **Operational State** column. The controller is then taken out of service and not visible in the **Work** pane any longer.

**Step 7** Repeat the earlier step to decommission the controllers one by one for all the APICs in the cluster in the appropriate order of highest controller ID number to the lowest.

**Note** The operation cluster size shrinks only after the last appliance is decommissioned, and not after the administrative size is changed. Verify after each controller is decommissioned that the operational state of the controller is unregistered, and the controller is no longer in service in the cluster.

You should be left with the remaining controllers in the APIC cluster that you desire.

---

**Contracting the APIC Cluster Using the REST API**

The cluster drives its actual size to the target size. If the target size is lower than the actual size, the cluster size contracts.

**Procedure**

**Step 1** Set the target cluster size so as to contract the APIC cluster size.

**Example:**
```
POST https://<IP address>/api/node/mo/uni/controller.xml
<infraClusterPol name='default' size=1/>
```

**Step 2** Decommission APIC3 on APIC1 for cluster contraction.

**Example:**
```
POST https://<IP address>/api/node/mo/topology/pod-1/node-1/av.xml
<infraWiNode id=3 adminSt='out-of-service'/>
```
Commissioning and Decommissioning Cisco APIC Controllers

Commissioning a Cisco APIC Controller in the Cluster Using the GUI

**Procedure**

**Step 1**
From the menu bar, choose **SYSTEM > Controllers**.

**Step 2**
In the **Navigation** pane, expand **Controllers > apic_controller_name > Cluster as Seen by Node**.

**Step 3**
From the **Work** pane, verify in the **Active Controllers** summary table that the cluster **Health State** is **Fully Fit** before continuing.

**Step 4**
From the **Work** pane, click the decommissioned controller that displaying **Unregistered** in the **Operational State** column. The controller is highlighted.

**Step 5**
From the **Work** pane, click **Actions > Commission**.

**Step 6**
In the **Confirmation** dialog box, click **Yes**.

**Step 7**
Verify that the commissioned Cisco APIC controller is in the operational state and the health state is **Fully Fit**.

Decommissioning a Cisco APIC Controller in the Cluster Using the GUI

**Procedure**

**Step 1**
On the menu bar, choose **System > Controllers**.

**Step 2**
In the **Navigation** pane, expand **Controllers > apic_controller_name > Cluster as Seen by Node**.

**Step 3**
In the **Work** pane, verify that the **Health State** in the **Active Controllers** summary table indicates the cluster is **Fully Fit** before continuing.

**Step 4**
In the **Navigation** pane, click an **apic_controller_name** that is within the cluster and not the controller that is being decommissioned. The controller details appear in the **Work** pane.

**Step 5**
In the **Work** pane, click **Actions > Decommission**. The **Confirmation** dialog box displays.

**Step 6**
Click **Yes**.

Example:

POST
https://<IP address>/api/node/mo/topology/pod-1/node-1/av.xml
<infraWiNode id=2 adminSt='out-of-service'/>
The decommissioned controller displays **Unregistered** in the **Operational State** column. The controller is then taken out of service and no longer visible in the **Work** pane.

**Note**
- The operation cluster size shrinks only after the last appliance is decommissioned, and not after the administrative size is changed. Verify after each controller is decommissioned that the operational state of the controller is unregistered, and the controller is no longer in service in the cluster.
- After decommissioning the APIC controller, you must reboot the APIC for Layer 4 to Layer 7 services. Reboot must be done before commissioning back the controller.

---

**Replacing a Cisco APIC in a Cluster Using the CLI**

**Note**
- For more information about managing clusters, see **Cluster Management Guidelines**.
- When you replace an APIC, the password will always be synced from the cluster. When replacing APIC 1, you will be asked for a password but it will be ignored in favor of the existing password in the cluster. When replacing APIC 2 or 3, you will not be asked for a password.

**Before you begin**

Before replacing an APIC, ensure that the replacement APIC is running the same firmware version as the APIC to be replaced. If the versions are not the same, you must update the firmware of the replacement APIC before you begin. Initial clustering of APICs running differing versions is an unsupported operation and may cause problems within the cluster.

**Procedure**

**Step 1**
Identify the APIC that you want to replace.

**Step 2**
Note the configuration details of the APIC to be replaced by using the `acidig avread` command.

**Step 3**
Decommission the APIC using the `controller controller-id decommission` command.

**Note**
Decommissioning the APIC removes the mapping between the APIC ID and Chassis ID. The new APIC typically has a different APIC ID, so you must remove this mapping in order to add a new APIC to the cluster.

**Step 4**
To commission the new APIC, follow these steps:
- a) Disconnect the old APIC from the fabric.
- b) Connect the replacement APIC to the fabric.

  The new APIC controller appears in the APIC GUI menu **System > Controllers > apic_controller_name > Cluster as Seen by Node** in the **Unauthorized Controllers** list.

  c) Commission the new APIC using the `controller controller-id commission` command.
Shutting Down the APICs in a Cluster

Shutting Down all the APICs in a Cluster

Before you shutdown all the APICs in a cluster, ensure that the APIC cluster is in a healthy state and all the APICs are showing fully fit. Once you start this process, we recommend that no configuration changes are done during this process. Use this procedure to gracefully shut down all the APICs in a cluster.

Procedure

Step 1  Log in to Cisco APIC with appliance ID 1.
Step 2  On the menu bar, choose System > Controllers.
Step 3  In the Navigation pane, expand Controllers > apic_controller_name.
        You must select the third APIC in the cluster.
Step 4  Right-click the controller and click Shutdown.
Step 5  Repeat the steps to shutdown the second APIC in the cluster.
Step 6  Log in to Cisco IMC of the first APIC in the cluster to shutdown the APIC.
Step 7  Choose Server > Server Summary > Shutdown Server.
        You have now shutdown all the three APICs in a cluster.

Bringing Back the APICs in a Cluster

Use this procedure to bring back the APICs in a cluster.

Procedure

Step 1  Log in to Cisco IMC of the first APIC in the cluster.
Step 2  Choose Server > Server Summary > Power On to power on the first APIC.
Step 3  Repeat the steps to power on the second APIC and then the third APIC in the cluster.

d) Boot the new APIC.
e) Allow several minutes for the new APIC information to propagate to the rest of the cluster.
The new APIC controller appears in the APIC GUI menu System > Controllers > apic_controller_name
> Cluster as Seen by Node in the Active Controllers list.
After all the APICs are powered on, ensure that all the APICs are in a fully fit state. Only after verifying that the APICs are in a fully fit state, you must make any configuration changes on the APIC.

---

**Cold Standby**

**About Cold Standby for APIC Cluster**

The Cold Standby functionality for an APIC cluster enables you to operate the APICs in a cluster in an **Active/Standby** mode. In an APIC cluster, the designated active APICs share the load and the designated standby APICs can act as a replacement for any of the APICs in an active cluster.

As an admin user, you can set up the Cold Standby functionality when the APIC is launched for the first time. We recommend that you have at least three active APICs in a cluster, and one or more standby APICs. As an admin user, you can initiate the switch over to replace an active APIC with a standby APIC.

**Important Notes**

- The standby APIC is automatically updated with firmware updates to keep the backup APIC at the same firmware version as the active cluster.
- During an upgrade process, once all the active APICs are upgraded, the standby APIC is also be upgraded automatically.
- Temporary IDs are assigned to standby APICs. After a standby APIC is switched over to an active APIC, a new ID is assigned.
- Admin login is not enabled on standby APIC. To troubleshoot Cold Standby, you must log in to the standby using SSH as `rescue-user`.
- During switch over the replaced active APIC is powered down, to prevent connectivity to the replaced APIC.
- Switch over fails under the following conditions:
  - If there is no connectivity to the standby APIC.
  - If the firmware version of the standby APIC is not the same as that of the active cluster.
- After switching over a standby APIC to active, if it was the only standby, you must configure a new standby.
- The following limitations are observed for retaining out of band address for standby APIC after a fail over.
  - Standby (new active) APIC may not retain its out of band address if more than 1 active APICs are down or unavailable.
  - Standby (new active) APIC may not retain its out of band address if it is in a different subnet than active APIC. This limitation is only applicable for APIC release 2.x.
  - Standby (new active) APIC may not retain its IPv6 out of band address. This limitation is not applicable starting from APIC release 3.1x.
**Verifying Cold Standby Status**

### Verifying Cold Standby Status Using CLI

To verify the Cold Standby status of APIC, log in to the APIC as admin and enter the command `show controller`.

```
apic1# show controller
Fabric Name : vegas
Operational Size : 3
Cluster Size : 3
Time Difference : 496
Fabric Security Mode : strict

<table>
<thead>
<tr>
<th>ID</th>
<th>Pod</th>
<th>Address</th>
<th>In-Band IPv4</th>
<th>In-Band IPv6 Version</th>
<th>Flags</th>
<th>Serial Number</th>
<th>Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>1*</td>
<td>1</td>
<td>10.0.0.1</td>
<td>0.0.0.0</td>
<td>fc00::1</td>
<td></td>
<td></td>
<td>172.23.142.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.0.0.2</td>
<td>0.0.0.0</td>
<td>fc00::1</td>
<td></td>
<td></td>
<td>172.23.142.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.0.0.3</td>
<td>0.0.0.0</td>
<td>fc00::1</td>
<td></td>
<td></td>
<td>172.23.142.8</td>
</tr>
<tr>
<td>21~</td>
<td>1</td>
<td>10.0.0.21</td>
<td>2.2(0.172)</td>
<td>crva- FCH1748V0DF</td>
<td>fully-fit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.2(0.172)</td>
<td>crva- FCH1747V0YF</td>
<td>fully-fit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.2(0.172)</td>
<td>crva- FCH1725V2DK</td>
<td>fully-fit</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Flags - c:Commissioned | r:Registered | v:Valid Certificate | a:Approved | f/s:Failover fail/success

(*)Current (~)Standby

### Verifying Cold Standby Status Using GUI

1. On the menu bar, choose **System > Controllers**.
2. In the **Navigation** pane, expand **Controllers > apic_controller_name > Cluster as Seen by Node**.
3. In the **Work** pane, the standby controllers are displayed under **Standby Controllers**.
Switching Over Active APIC with Standby APIC Using GUI

Use this procedure to switch over an active APIC with a standby APIC.

Before you begin

Procedure

**Step 1**  
On the menu bar, choose **System > Controllers**.

**Step 2**  
In the **Navigation** pane, expand **Controllers > apic_controller_name > Cluster as Seen by Node**.  
The `apic_controller_name` should be other than the name of the controller being replaced.

**Step 3**  
In the **Work** pane, verify that the **Health State** in the **Active Controllers** summary table indicates the active controller is **Fully Fit** before continuing.

**Step 4**  
Click an `apic_controller_name` that you want to switch over.

**Step 5**  
In the **Work** pane, click **Actions > Replace**.  
The **Replace** dialog box displays.

**Step 6**  
Choose the **Backup Controller** from the drop-down list and click **Submit**.  
It may take several minutes to switch over an active APIC with a standby APIC and for the system to be registered as active.

**Step 7**  
Verify the progress of the switch over in the **Failover Status** field in the **Active Controllers** summary table.

Switching Over Active APIC with Standby APIC Using CLI

Use this procedure to switch over an active APIC with a standby APIC.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
`replace-controller replace ID number Backup serial number`  
*Example:*  
apic1#replace-controller replace 2 FCH1804V27L  
Do you want to replace APIC 2 with a backup? (Y/n): Y | Replaces an active APIC with a standby APIC. |
| **Step 2**  
`replace-controller reset ID number`  
*Example:*  
apic1# replace-controller reset 2  
Do you want to reset failover status of APIC 2? (Y/n): Y | Resets failover status of the active controller. |
Switching Over Active APIC with Standby APIC Using REST API

Use this procedure to switch over an active APIC with standby APIC using REST API.

**Procedure**

Switch over active APIC with standby APIC.

**URL for POST:** https://ip address/api/node/mo/topology/pod-initiator_pod_id/node-initiator_id/av.xml

**Body:** `<infraWiNode id=outgoing_apic_id targetMbSn=backup-serial-number/>`

where `initiator_id` = id of an active APIC other than the APIC being replaced.

`pod-initiator_pod_id` = pod ID of the active APIC

`backup-serial-number` = serial number of standby APIC

**Example:**

https://ip address/api/node/mo/topology/pod-1/node-1/av.xml

`<infraWiNode id=2 targetMbSn=FCH1750V00Q/>`