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.

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: http://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. (1110R)

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

Preface v

Audience v
Document Conventions vii
Related Documentation viii
Documentation Feedback viii
Obtaining Documentation and Submitting a Service Request viii

CHAPTER 1
New and Changed Information 1

CHAPTER 2
Initial POD Setup and Overview 3

First-Time Access 3
Cisco APIC Documentation Roadmap 3
Simplified Approach to Configuring in Cisco APIC 4
About the ACI Simulator 4
Guidelines and Restrictions When Using the ACI Simulator 4
Installing the Cisco Application Centric Infrastructure Fabric Hardware 6
Changing the BIOS Default Password 6
About the APIC 6
Setting up the APIC 7
Provisioning IPv6 Management Addresses on APIC Controllers 12
Accessing the GUI 13
Accessing the REST API 14
Accessing the Object Model CLI 14
Accessing the NX-OS Style CLI 15
Overview of the GUI 16
Overview of the GUI 16
Menu Bar and Submenu Bar 17

Menu Bar Tabs 17

System Tab 17
Tenants Tab 18
Fabric Tab 18
VM Networking Tab 18
L4-L7 Services Tab 18
Admin Tab 18
Operations Tab 18
Apps Tab 19

Menu Bar Tools 19

Search 19
Alerts 19
User Settings and Preferences 20
System Tools 20

Navigation Pane 21

Work Pane 22

Quick Start Pages 22

Deployment Warning and Policy Usage Information 22
Graphical Configuration of Ports 23
Viewing an API Interchange in the GUI 24
GUI Icons 26

Fault, Statistics, and Health Level Icons 26

Initializing the Fabric 27

About Fabric Initialization 27
Example Topology 27
Switch Discovery with the APIC 28

About Switch Discovery with the APIC 28
Preface

This preface includes the following sections:

- Audience, page v
- Document Conventions, page v
- Related Documentation, page vii
- Documentation Feedback, page viii
- Obtaining Documentation and Submitting a Service Request, page viii

**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

**Document Conventions**

Command descriptions use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bold</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>
</tbody>
</table>
### Document Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[x</td>
<td>y]</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>screen font</td>
<td>Terminal sessions and information the switch displays are in screen font.</td>
</tr>
<tr>
<td>boldface screen font</td>
<td>Information you must enter is in boldface screen font.</td>
</tr>
<tr>
<td>italic screen font</td>
<td>Arguments for which you supply values are in italic screen font.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters, such as passwords, are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</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.
Related Documentation

Application Policy Infrastructure Controller (APIC) Documentation

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 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.
New and Changed Information

This chapter contains the following sections:

- New and Changed Information, page 1

New and Changed Information

The following table provides an overview of the significant changes to this guide up to this current release. The table does 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 Behavior in Cisco APIC and Document Reorganization

<table>
<thead>
<tr>
<th>Cisco APIC Release Version</th>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.0(1k)</td>
<td>Redesign of the APIC GUI</td>
<td>--</td>
<td>This content is available in the section Overview of the GUI</td>
</tr>
</tbody>
</table>
Initial POD Setup and Overview

This chapter contains the following sections:

- First-Time Access, page 3
- Overview of the GUI, page 16
- Initializing the Fabric, page 27
- Switch Discovery with the APIC, page 28

First-Time Access

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 the choice of two additional user interfaces. They are the NX-OS style CLI and the Basic GUI. The existing methods of configuration using REST API and Advanced GUI are supported as well. The Advanced GUI is equivalent to the GUI of the previous releases. Cisco recommends that you use the Advanced GUI to manage any policy that you created in Release 1.2 or earlier releases.

In addition to the simple approach available for network administrators and other users of the NX-OS style CLI and the Basic GUI, there is intelligence embedded in these approaches as compared to the Advanced GUI or the REST API. In several instances, the NX-OS style CLI and the Basic GUI often 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.

Configurations using NX-OS style CLI and Basic GUI are compatible similar to the compatibility between existing methods of configuration using Advanced GUI and REST API. 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.

About the ACI Simulator

The ACI simulator provides real, fully-featured APIC controller software, along with a simulated fabric infrastructure of leaf switches and spine switches in one physical server. The physical server is a UCS C-series server.

The APIC controller software controls a set of five software-simulated ACI switches connected in a fabric topology. This allows the customer to explore the APIC GUI and to create configurations in the simulated fabric. Because the simulator can also be configured using the CLI or the REST API, it allows partners and customers to develop scripts and applications prior to investing in and purchasing the actual ACI switches.

Guidelines and Restrictions When Using the ACI Simulator

For details about the ACI simulator topology and connections, see the Cisco ACI Simulator Installation Guide.

When using the ACI simulator, the following guidelines and restrictions must be considered:

- The ACI simulator GUI includes an online version under Quick Start that includes video demonstrations.

- Do not change the following:
  - The default names in the initial setup for node names and the cluster configuration.
  - The cluster size and the number of APIC nodes.
  - The infra VLAN.

- The ACI simulator uses NAT for inband management. Inband IP addresses configured by policy are not used. Instead, APIC and node inband IP addresses are internally allocated.

- The ACI simulator does not support the following:
• Configuring a DHCP server policy.
• Configuring a DNS service policy.
• Data path forwarding because the simulator includes simulated switches.
• Cisco Discovery Protocol (CDP) between a leaf switch and a hypervisor or between a leaf switch and an unmanaged/Layer 2 switch. Only Link Layer Discovery Protocol (LLDP) is supported in these cases.
• Configuring out-of-band management access for switches.

• APIC out-of-band management IP/gateway cannot be modified using an out-of-band management policy and can be configured only during the APIC first-time setup screen.
• Keep the vMotion PNIC outside the simulator network.
• The infrastructure EPG in the infrastructure tenant is for internal use only.
• The MP-BGP route reflector and the OSPF external routed network protocols do not work if you are using the simulator.
• Virtual shell (VSH) and ishell commands do not work on switches. These commands are implemented on the Cisco NX-OS software, and the Cisco NX-OS software is not available on the simulator.
• Statistics are simulated. As a result, threshold crossing alert (TCA) faults are generated in the simulator to demonstrate the fault generation on the statistics threshold crossing.
• Create a syslog and Call Home source policy under common policy. This policy applies at the system level and sends all syslog and Call Home messages system wide. The GUI path to create syslog and Call Home under common policy are as follows: Admin / External Data Collector/ Monitoring Destinations / [Callhome | SNMP | Syslog].
• The Cisco ACI simulator simulates faults for counters, which can cause the health score of the top-of-rack (TOR) switch to go down. The faults look like the following:

```xml
<faultInst ack="no" cause="threshold-crossed" changeSet="" childAction="" code="F54431"
created="2014-01-21T17:20:13.179+00:00" descr="TCA: l2IngrBytes5min dropRate value 9049.94 raised above threshold 9000 and value is recovering "dn="topology/pod-1/node-17/sys/ctx-[vxlan-2621440]/bd-[vxlan-15826914]/vlan-[vlan-1031]/fault-F54431" domain="infra" highestSeverity="minor" lastTransition="2014-01-21T17:20:13.244+00:00" lc="raised" modTs="never" occur="1"origSeverity="minor" prevSeverity="minor" rule="tca-l2-ingr-bytes-drop-rate" severity="minor" status="" subject="counter" type="operational"/>
<faultInst ack="no" cause="threshold-crossed" changeSet="" childAction="" code="F54447"
created="2014-01-21T17:20:13.244+00:00" descr="TCA: l2IngrPkts5min dropRate value 3.55333 raised above threshold 10" dn="topology/pod-1/node-17/sys/ctx-[vxlan-2621440]/bd-[vxlan-15826914]/vlan-[vlan-1031]/fault-F54447" domain="infra" highestSeverity="warning" lastTransition="2014-01-21T19:42:37.983+00:00" lc="retaining" modTs="never" occur="9" origSeverity="warning" prevSeverity="warning" rule="tca-l2-ingr-pkts-drop-rate" severity="cleared" status="" subject="counter" type="operational"/>
```

• You can test L4-L7 services by connecting your service appliance using in-band management connectivity between the simulator and the appliance.

For more details about L4-L7 services guidelines when using the simulator, see the guidelines section in the Cisco ACI Simulator Release Notes.
Installing the Cisco Application Centric Infrastructure Fabric Hardware

For details about installing the ACI fabric hardware, see the Application Centric Infrastructure Fabric Hardware Installation 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. 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. At the **Enter Password** dialog box, enter the current password. **Note** The default is 'password'.
3. In the **Setup Utility**, choose the **Security** tab, and choose **Set Administrator Password**.
4. In the **Enter Current Password** dialog box, enter the current password.
5. In the **Create New Password** dialog box, enter the new password.
6. In the **Confirm New Password** dialog box, re-enter the new password.
7. Choose the **Save & Exit** tab.
8. In the **Save & Exit Setup** dialog box, choose **Yes**.
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, multitenant 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 APIC

When the APIC is launched for the first time, the 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 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 APIC through the CIMC KVM or continue to access the 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 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 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 APIC and 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 APIC (the controller cluster) to the ACI fabric requires a 10G interface on the ACI leaf. You cannot connect the APIC directly to the N9332PQ ACI leaf switch, unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the N9332PQ switch will auto-negotiate to 10G without requiring any manual configuration.

About High Availability for APIC Cluster

The High Availability 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.

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

**Table 2: 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><strong>Note</strong></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>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>This value is for the infrastructure virtual routing and forwarding (VRF) only. Default value. Do not change. Do not set up your host on the network 10.0.0.0/8.</td>
</tr>
</tbody>
</table>
### Initial POD Setup and Overview

#### Setting up the APIC

<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</td>
<td>4                               Default value. Do not change.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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</td>
<td>225.0.0.0/15                                                                  Valid range: 225.0.0.0/15 to 231.254.0.0/15, prefixlen must be 15 (128k IPs) Default value. Do not change.</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                                                                          Valid values are as follows</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• auto</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 10baseT/Half</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 10baseT/Full</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 100baseT/Half</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 100baseT/Full</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1000baseT/Full</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Do not change values</td>
<td></td>
</tr>
<tr>
<td>Strong password check</td>
<td>Check for a strong password</td>
<td>[Y]</td>
</tr>
</tbody>
</table>
### Password

**Name:** Password  
**Description:** Password of the system administrator  
This password must be at least 8 characters with one special character.  
**Default Value:** —

### Table 3: 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><strong>Note</strong></td>
<td>When setting up APIC in an active-standby mode, you must have at least 3 active APICs in a cluster.</td>
<td></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>
</tbody>
</table>
| IP address pool for tunnel endpoint addresses | Tunnel endpoint address pool | 10.0.0.0/16  
This value is for the infrastructure virtual routing and forwarding (VRF) only.  
Default value. Do not change. Do not set up your host on the network 10.0.0.0/8. |
<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</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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>Default value. Do not change.</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></td>
<td><strong>Valid values are as follows</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• auto</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 10baseT/Half</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 10baseT/Full</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 100baseT/Half</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 100baseT/Full</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1000baseT/Full</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Do not change values</td>
<td></td>
</tr>
<tr>
<td>Strong password check</td>
<td>Check for a strong password</td>
<td>[Y]</td>
</tr>
</tbody>
</table>
The following is a sample of the initial setup dialog as displayed on the console:

Cluster configuration ...
- Enter the fabric name [ACI Fabric1 #1]:
- Enter the number of controllers in the fabric (1-16) [3]:
- Enter the controller ID (1-3) [2]:
- Enter the controller name [apic2]:
- Enter address pool for TEP addresses [10.0.0.0/16]:
- Enter the VLAN ID for infra network (1-4) [4]: <<< This is for the simulator APIC
- Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
- Enter the IP address for out-of-band management: 192.168.10.2/24
- Enter the IP address of the default gateway [None]: 192.168.10.254
- Enter the interface speed/duplex mode [auto]:

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

Note
- It can take a few minutes to login as an administrator.
- Until the entire cluster boots up, you cannot log in to apic2 and apic3.

---

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) [4093]:
- 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)
- (IPv6 Address)
Accessing the GUI

Procedure

Step 1  Open one of the supported browsers:

- Chrome version 35 (at minimum)
- Firefox version 26 (at minimum)
- Internet Explorer version 11 (at minimum)
- Safari version 7.0.3 (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.

Step 5  In the Mode field, from the drop-down list, choose the Advanced or the Basic mode as desired.
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.

Note
- Only https is enabled by default. By default, http and http-to-https redirection are disabled.
- You must send an authentication message to initiate an API session. Use the administrator login name and password that you configured during the initial setup.

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

Step 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`.

Step 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.

Step 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:

```bash
$ 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.

Accessing the NX-OS Style 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

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. From this level, you can reach these configuration modes:

• To continue in the NX-OS style CLI, you can stay in EXEC mode or you can type configure to enter global configuration mode.

For information about NX-OS style CLI commands, see the Cisco APIC NX-OS Style CLI Command Reference.

• To reach the object model CLI, type bash.

For information about object mode CLI commands, see the Cisco APIC Command-Line Interface User Guide, APIC Releases 1.0 and 1.1.
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.

Figure 1: APIC GUI Regions

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 17
2. Submenu bar—See Menu Bar and Submenu Bar, on page 17
3. Navigation pane—See Navigation Pane, on page 21
4. Work pane—See Work Pane, on page 22

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 24.

The Basic UI will be deprecated after this release and Cisco does not recommend using the Basic UI for configurations. If you want to use the Basic UI, use the following URL:

APIC URL/indexSimple.html
Cisco recommends that you do not mix configuration modes (Advanced or Basic). When you create a configuration in either mode and change the configuration using the other mode, unintended changes can occur. For example, if you apply an interface policy to two ports using the Advanced mode and then change the settings of one port using the Basic mode, your changes might be applied to both ports.

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.

Tip
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>![Search]</td>
<td>Search, on page 19</td>
</tr>
<tr>
<td>![Alerts]</td>
<td>Alerts, on page 19</td>
</tr>
<tr>
<td>![User Settings and Preferences]</td>
<td>User Settings and Preferences, on page 20</td>
</tr>
<tr>
<td>![System Tools]</td>
<td>System Tools, on page 20</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.
Tenants Tab

Use the Tenants tab in the menu bar to perform tenant management. In the submenu bar, you see an Add Tenant link, and a drop-down list that contains all the tenants. Up to five of the most recently used tenants are also displayed on the submenu bar.

- 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.

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.
- **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.

VM Networking Tab

Use the VM 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. You can view existing service nodes in the Inventory submenu tab.

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*

![Search Icon]

**Alerts**

When critical system notifications are available, the alert menu bar icon will be animated. To view the alerts, click the following icon.

*Figure 3: Alerts*

![Alert Icon]

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 resolve the underlying issue.
User Settings and Preferences

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

*Figure 4: User Settings and Preferences*

The following selections are available:

- **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 X509 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 the Deployment Warning dialog box when logging in. See Deployment Warning and Policy Usage Information, on page 22.
  * **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 22.
- **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.

*Figure 5: System Tools*
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 24.
- **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.

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.
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.

**Quick Start Pages**

Many APIC menu and submenu tabs open to 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.

**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

Configure
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

In the Work pane's Configure 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 Configure 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.
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

Step 1  Log in to the APIC GUI.

Step 2  In the upper right corner of the APIC window, click the "welcome, <name>" message to view the drop-down list.

Step 3  In the drop-down list, choose the Show API Inspector. The API Inspector opens in a new browser window.

Step 4  In the Filters toolbar of the API Inspector 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

Step 5  In the Search toolbar, you can search the displayed messages for an exact string or by a regular expression. This table shows the search controls:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>In this text box, enter a string for a direct search or enter a regular expression for a regex search. As you type, the first matched field in the log list is highlighted.</td>
</tr>
<tr>
<td>Reset</td>
<td>Click this button to clear the contents of the Search text box.</td>
</tr>
<tr>
<td>Regex</td>
<td>Check this checkbox to use the contents of the Search text box as a regular expression for a search.</td>
</tr>
<tr>
<td>Match case</td>
<td>Check this checkbox to make the search case sensitive.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disable</td>
<td>Check this checkbox to disable the search and clear the highlighting of search matches in the log list.</td>
</tr>
<tr>
<td>Next</td>
<td>Click this button to cause the log list to scroll to the next matched entry. This button appears only when a search is active.</td>
</tr>
<tr>
<td>Previous</td>
<td>Click this button to cause the log list to scroll to the previous matched entry. This button appears only when a search is active.</td>
</tr>
<tr>
<td>Filter</td>
<td>Check this checkbox to hide nonmatched lines. This checkbox appears only when a search is active.</td>
</tr>
<tr>
<td>Highlight all</td>
<td>Check this checkbox to highlight all matched fields. This checkbox appears only when a search is active.</td>
</tr>
</tbody>
</table>

**Step 6**

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
response: {"subscriptionId":"72057598349672459","imdata":[]}```
**GUI Icons**

*Table 4: 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="Help Icon" /></td>
<td>Displays online help information for the current menu page</td>
</tr>
<tr>
<td><img src="image" alt="Quick Start Icon" /></td>
<td>Displays Quick Start concept information for the current menu page</td>
</tr>
<tr>
<td><img src="image" alt="Video Icon" /></td>
<td>Plays a Quick Start video</td>
</tr>
<tr>
<td><img src="image" alt="Procedure Icon" /></td>
<td>Displays a Quick Start procedure</td>
</tr>
<tr>
<td><img src="image" alt="Actions Icon" /></td>
<td>Displays a drop-down list of actions</td>
</tr>
<tr>
<td><img src="image" alt="Refresh Icon" /></td>
<td>Refresh the displayed information</td>
</tr>
<tr>
<td><img src="image" alt="Download Icon" /></td>
<td>Download to a file</td>
</tr>
<tr>
<td><img src="image" alt="Upload Icon" /></td>
<td>Upload a file</td>
</tr>
</tbody>
</table>

**Fault, Statistics, and Health Level Icons**

*Table 5: 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>
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.
For the actual simulator topology see the Cisco ACI Simulator Installation Guide.

Switch Discovery with the APIC

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.