Cisco Application Policy Infrastructure Controller, Release 1.0(1e), Release Notes

Publication Date: August 4, 2014

This document describes the features, caveats, and limitations for the Cisco Application Policy Infrastructure Controller (APIC) software. For more information on specific hardware features, see the *Cisco NX-OS Release 11.0(1b) Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches*. Additional product documentation is listed in the "Related Documentation" section on page 7.

Release notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of this document:

http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/products-release-notes-list.html

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
August 04, 2014	Created release notes for Release 1.0(1e).
August 22, 2014	Updated the Known Behaviors section with links to the *Cisco ACI Fabric Documentation Roadmap* and the Cisco Application Policy Infrastructure Controller (APIC) website.
August 29, 2014	Removed the *Cisco APIC Python API and SDK* from the Known Behaviors section.
September 4, 2014	Updated the "Compatibility Information" section to include Cisco UCS Manager software Release 2.2(1c).
September 18, 2014	Added the Licensing Information section.
September 26, 2014	Removed the Licensing Information section.
October 6, 2014	Added the "Software Upgrade Recommendation" section.

Cisco Systems, Inc.
www.cisco.com

Table 1 Online History Change (continued)

Date	Description
October 20, 2014	• Added "Resolved Caveats" section. • Moved bug ID CSCuq05346 from Open Caveats to Resolved Caveats.
October 21, 2014	Added the *Cisco APIC Python SDK Documentation* to the "Web-Based Documentation" section.
November 10, 2014	Added "Known Behaviors".
January 12, 2015	Added a list of supported protocols to "Usage Guidelines".
February 13, 2015	Corrected a link to the APIC website in the "Related Documentation" section.

Contents

This document includes the following sections:

Introduction

The Cisco Application Centric Infrastructure (ACI) is an architecture that allows the application to define the networking requirements in a programmatic way. This architecture simplifies, optimizes, and accelerates the entire application deployment life cycle.

The *Cisco Application Centric Infrastructure Fundamentals* guide provides complete details about the ACI, including its two major components:

- Cisco Application Policy Infrastructure Controller (APIC)
- ACI Fabric, including Cisco Nexus 9000 spine and leaf switches

The *Cisco Application Centric Infrastructure Fundamentals* guide also includes a glossary of terms that are used in the ACI.

Key features of the ACI include the following:

- Simplified automation with an application-driven policy model
- Common platform for managing physical, virtual, and cloud-based environments
- Centralized visibility with real-time, application health monitoring
- Operational simplicity, with common policy, management, and operation models across application, network, and security resources

- Open software flexibility for DevOps teams and ecosystem partner integration
- Scalable performance and secure multi-tenancy

Cisco Application Policy Infrastructure Controller

The Cisco Application Policy Infrastructure Controller (APIC) enables applications to directly connect with a secure, shared, high-performance resource pool that includes networking and Layer 4 through 7 services.

The key features of the APIC include the following:

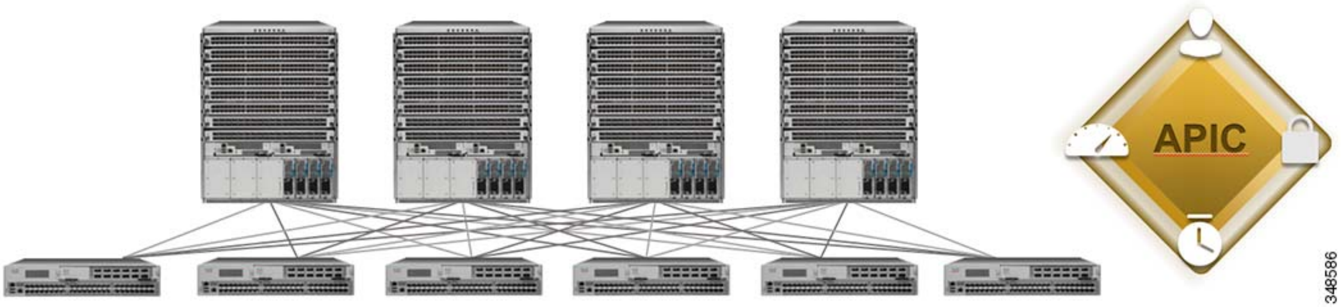
- Application centric network policies
- Data model-based declarative provisioning
- Application, topology monitoring, and troubleshooting
- Third-party integration (Layer 4 through 7 services, vCenter, vShield)
- Image management (spine and leaf)
- Cisco ACI inventory and configuration
- Implementation on a distributed framework across a cluster of appliances
- Health Scores for key Managed Objects (tenants, application profiles, switches, etc)
- Fault, event and performance management
- Cisco Application Virtual Switch (AVS) that can be used as a virtual Leaf for the Cisco APIC

ACI Fabric and Switches

A clustered replicated APIC appliance manages the ACI fabric. Cisco Nexus 9000 Series switches can run with the ACI-compatible software to run in the leaf/spine fabric mode. These switches form a "fat-tree" network by connecting each leaf node to each spine node; all other devices connect to the leaf nodes.

Figure 1shows the ACI Fabric with Cisco Nexus 9508, Cisco Nexus 9300 Series leaf switches, and the APIC.

Figure 1 ACI Fabric with Spine and Leaf Switches, and the APIC,



Software Upgrade Recommendation

It is recommended that you upgrade your software to Cisco APIC Release 1.0(1k) because the release includes a resolution for the vulnerability of bash that is identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2014-6271 and CVE-2014-7169.

Installation Notes

For installation instructions, see the *Cisco ACI Fabric Hardware Installation Guide*.

For instructions on how to access the APIC for the first time, see the *Cisco APIC Getting Started Guide*.

Compatibility Information

Cisco APIC Release 1.0(1e) supports the following software:

- Cisco NX-OS Release 11.0(1b)
- Cisco AVS, Release 4.2(1)SV2(2.3)
- Cisco ASA 5585, Release 8.4 and later
- Cisco ASAv (virtual), Release 9.2.1
- Cisco UCS Manager software Release 2.2(1c) or later is required for the Cisco UCS Fabric Interconnect and other components, including the BIOS, CIMC, and the adapter
- F5, Big IP, LTM Physical, LTM Virtual, Release 11.4.1
- Citrix Netscaler, MPX, SDX, VPX, Release 10.1 and later
- Citrix Netscaler 1000v, ESX 5.0 and later
- VMware vCenter 5.1 and 5.5 and vShield 5.1 and 5.5

Usage Guidelines

This section list usage guidelines for the APIC software.

- The APIC GUI supports the following browsers:
  - Chrome version 35 and higher on Mac and Windows
  - Firefox version 26 on Mac, Linux, and Windows
  - Internet Explorer version 11 or higher
  - Safari 7.0.3

⚠ **Caution** 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**.
Select **Alway Trust** in the three drop-down lists that appear.

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

- The APIC GUI includes an online version of the Quick Start guide that includes video demonstrations.
- The infrastructure IP address range must not overlap with other IP addresses used in the fabric for inband and out-of-band networks.
- The APIC does not provide an IPAM solution, so ensure that IP addresses are unique within a private network/ context.
- Press the Escape key twice (<Esc> <Esc>) to display APIC CLI command options.
- For the following services, use a DNS-based host name with out-of-band management connectivity. IP addresses can be used with both inband and out-of-band management connectivity.
  - Syslog server
  - Call Home SMPT server
  - Tech support export server
  - Configuration export server
  - Statistics export server
- Inband management connectivity to the spine switches is possible from any host that is connected to the leaf switches of the Fabric, and leaf switches can be managed from any host that has IP connectivity to the fabric.
- The current list of protocols that are allowed (and cannot be blocked through contracts) include the following. Some of the protocols have SrcPort/DstPort distinction.
  - UDP DestPort 161: SNMP. These cannot be blocked through contracts. Creating an SNMP ClientGroup with a list of Client-IP Addresses restricts SNMP access to only those configured Client-IP Addresses. If no Client-IP address is configured, SNMP packets are allowed from anywhere.
  - TCP SrcPort 179: BGP
  - TCP DstPort 179: BGP
  - OSPF
  - UDP DstPort 67: BOOTP/DHCP
  - UDP DstPort 68: BOOTP/DHCP
  - IGMP
  - PIM
  - UDP SrcPort 53: DNS replies
  - TCP SrcPort 25: SMTP replies
  - TCP DstPort 443: HTTPS
  - UDP SrcPort 123: NTP

- UDP DstPort 123: NTP

Caveats

This section includes the following topics:

- Open Caveats, page 6
- Resolved Caveats, page 7
- Known Behaviors, page 7

Open Caveats

This section lists the open caveats in the Cisco ACI, Release 1.0(1e). Click the Bug ID shown in Table 2 to access the Bug Search Tool and see additional information about the bug.

Table 2 Open Caveats

Bug ID	Description
CSCun44221	Some events on bootup are missed on leaf or spine switches.
CSCup50125	Users can change their password any number of times.The password change restriction policies are not obeyed.
CSCup79002	Host name resolution of the syslog server fails on leaf and spine switches over inband connectivity.
CSCup88278	Configuration modifications to the ERSPAN destination parameters (dst IP/TTL/flow id etc) do not take effect on the physical and virtual leaf switches.
CSCup92890	A user with read-only access can initiate a L4-L7 device package download.
CSCup90690	In the tracerouteExecTn managed object, the source node ID field contains only one of the two nodes when the source is behind a vPC.
CSCup93244	Download of an image into the repository fails if you have some special characters in your password.
CSCup96043	A fault for a switch firmware upgrade failure does not appear under the Firmware Groups tab.
CSCuq00217	An APIC process is busy when a scheduled export configuration is spawned every hour.
CSCuq10566	When shutting down a port channel that is a member of a vPC, the entire vPC will shut down.
CSCuq20849	The **techsupport remote** command displays an exception when trying to collect the techsupport on the CLI.
CSCuq21358	After the same tag is configured for two interfaces, a new tag cannot be added or an existing tag associated with a third interface.
CSCuq21360	Following a FEX or switch reload, configured interface tags are no longer configured correctly.

Resolved Caveats

This section lists the resolved caveats in the Cisco ACI, Release 1.0(1e). Click the Bug ID shown in Table 3 to access the Bug Search Tool and see additional information about the bug.

Table 3 Resolved Caveats

Bug ID	Description
CSCuq05346	Port-group settings need to be set to Accept for HA failover. Traffic doesn't flow through virtual GoTo devices after failover.

Known Behaviors

This section lists caveats that describe known behaviors in the Cisco ACI, Release 1.0(1e). Click the Bug ID shown in Table 4 to access the Bug Search Tool and see additional information about the bug.

Table 4 Known Behaviors

Bug ID	Description
CSCuo79243	In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.

Related Documentation

This section lists the product documentation for the Cisco APIC. Links to the documentation are available in the *Cisco ACI Fabric Documentation Roadmap* that is published here:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/roadmap/b_ACI_Fabric_Documentation_Roadmap.html

The Cisco Application Policy Infrastructure Controller (APIC) website is here:

http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Web-Based Documentation

- *Cisco APIC Management Information Model Reference*
- *Cisco APIC Online Help Reference*
- *Cisco ACI MIB Support List*
- *Cisco APIC Python SDK Documentation*

Downloadable Documentation

- *Cisco ACI Fundamentals*
- *Cisco APIC Getting Started Guide*
- *Cisco APIC REST API User Guide*

- *Cisco APIC Command Line Interface User Guide*
- *Cisco ACI Switch CLI Command Reference, NX-OS Release 11.0*
- *Cisco APIC Faults, Events, and Error Messages Guide*
- *Cisco ACI System Messages Reference Guide*
- *Cisco ACI Troubleshooting Guide*
- *Cisco NX-OS to APIC Mapping Guide*
- *Cisco APIC Layer 4 to Layer 7 Device Package Development Guide*
- *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*
- *Cisco AVS Configuration Guide*
- *Cisco AVS Installation and Upgrade Guide*
- *Cisco ACI MIB Quick Reference*
- *Cisco ACI Fabric Hardware Installation Guide*
- *Cisco ACI MIB Quick Reference*
- *Cisco APIC Release Notes*
- *Cisco Application Centric Infrastructure Release Notes*

Hardware Documentation

Cisco Nexus 9336PQ ACI-Mode Switch Hardware Installation Guide

Cisco Nexus 9508 ACI-Mode Switch Hardware Installation Guide

This document is to be used in conjunction with the documents listed in the "Known Behaviors" section.

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.