Cisco Application Policy Infrastructure Controller, Release 1.0(2j), Release Notes

Publication Date: November 11, 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(2j) Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches*. Additional product documentation is listed in the "Related Documentation" section on page 10.

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
November 11, 2014	Created the release notes for Release 1.0(2j).
November 25, 2014	Updated the "Upgrade Instructions" section.
November 26, 2014	Added the "Compatibility Information" section.
December 4, 2014	Removed the Downgrade Instructions section and added a note on downgrading in the "Usage Guidelines".
January 12, 2015	Added a list of supported protocols to "Usage Guidelines".
January 22, 2015	Added bug ID CSCur38673 to the"Open Caveats" section.
February 13, 2015	Corrected a link to the APIC website in the "Related Documentation" section.
March 3, 2015	Added a new information to the "Usage Guidelines" explaining how to configure an atomic counter policy between two endpoints.
March 11, 2015	Added CSCut25657 to "Open Caveats".

Cisco Systems, Inc.
www.cisco.com

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

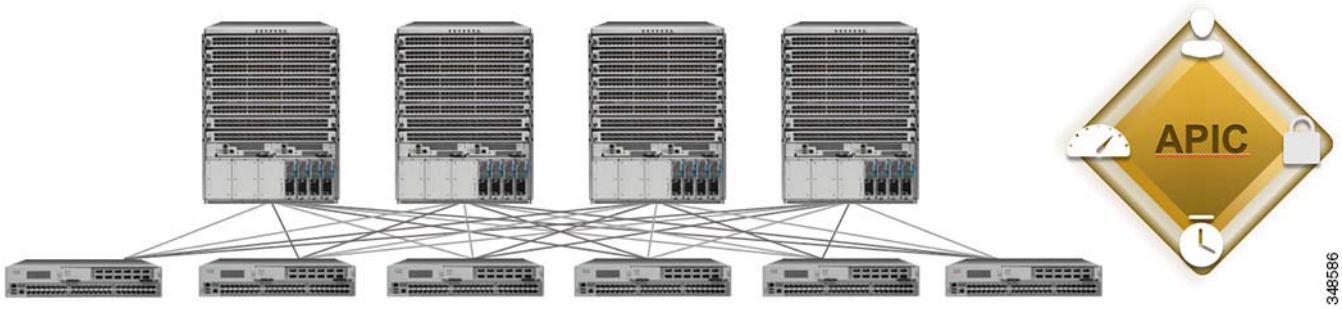
- Application, topology monitoring, and troubleshooting
- Third-party integration (Layer 4 through 7 services, vCenter, vShield)
- Image management (spine and leaf)
- Cisco ACI inventory and configuration
- Implementation on a distributed framework across a cluster of appliances
- Health Scores for key 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 1 shows 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,



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*.
- For the Cisco APIC Python SDK documentation, including installation instructions, see the *Cisco APIC Python SDK Documentation*.

  Two installation egg files are needed for installation. You can download these files from a running APIC at the following URLs:

  – http[s]://<APIC address>/cobra/_downloads/acicobrasdk.egg

  This is the SDK file.

  – http[s]://<APIC address>/cobra/_downloads/acicobramodel.egg

This file includes the Python packages that model the Cisco ACI Management Information Tree.

Both files are required.

Note Installation of the SDK with SSL support on Unix/Linux and Mac OS X requires a compiler. For a Windows installation, you can install the compiled shared objects for the SDK dependencies using wheel packages.

Note The model package depends on the SDK package; be sure to install the SDK package first.

Upgrade Instructions

When upgrading from a 1.0(1x1x) release to a 1.0(2x) release, you must upgrade the switch software image for all the spine and leaf switches in the fabric first. After that upgrade is successfully completed, upgrade the APIC controller software image.

However, if you are upgrading within a 1.0(1x) release software sequence or within a 1.0(2x) release software sequence, you must first upgrade the APIC controller software image. And then, after that is successfully completed, upgrade all the switches in the fabric.

Compatibility Information

Cisco APIC Release 1.0(2j) supports the hardware and software listed on the *ACI Ecosystem Compatibility List* and the software listed as follows:

- Cisco NX-OS Release 11.0(2j)
- Cisco AVS, Release 5.2(1)Sv3(1.2)
- 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

Usage Guidelines

This section lists usage guidelines for the APIC software.

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

Note Restart your browser after upgrading to 1.0(2j).

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

If you do not follow these steps above, 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.
- In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.
- 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 SMTP 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

Note The APIC 1.0(1n) release is the earliest version supported for downgrading from a 1.0(2x) release. When downgrading from 1.0(2x) to 1.0(1n), first downgrade the switch software image for all the spine and leaf switches in the fabric. After that downgrade is successfully completed, downgrade the APIC controller software image.

- When configuring an AC (atomic counter) policy between two endpoints, and an IP is learned on one of the two endpoints, it is recommended to use an IP-based policy, and not a client endpoint based policy.

New and Changed Information

This section lists the new and changed features in Release 1.0(2j), and includes the following topics:

New Hardware Features in Cisco Application Policy Infrastructure Controller Release 1.0(2j)

The Cisco Application Policy Infrastructure Controller Release 1.0(2j) supports the following new hardware features:

- N9K-M6PQ - ACI Uplink Module for Nexus 9300 with six 40-Gigabit port QSFP support.
- N9K-C9504 - Cisco Nexus 9504 chassis with 4 slots
- N9K-SUP-B - Cisco Nexus 9500 Series supervisor module
- N9K-C9504-FM - Fabric module
- N9K-C9396TX - Cisco Nexus 9300 48-port, 1/10 Gbps Base-T and 6-port or 12-port, 40 Gigabit Ethernet QSFP switch

New Software Features in Cisco Application Policy Infrastructure Controller Release 1.0(2j)

The Cisco Application Policy Infrastructure Controller Release 1.0(2j) supports the following new software features:

- Traffic Storm Control – Enables you to create policies that prevent disruptions on Layer 2 ports by broadcast, multicast, or unicast traffic storms For more information, see *KB: Configuring Traffic Storm Control with Cisco APIC*. The link to KB articles is available in the "Related Documentation" section on page 10.
- Static management IP addresses – Enables you to configure static inband connectivity. For more information, see *KB: Configuring Static Management Access with Cisco APIC*. The link to KB articles is available in the "Related Documentation" section on page 10.
- Increased contract scale – The maximum contract limit for fabric is now 1,000 contracts and 10,000 filters. The maximum limit for leaf switches is 4K TCAM entries (specific to N9K-M12PQ) and 16K TCAM entries (specific to N9K-M6PQ).
- Enhancement on config import – Enables the backups of APIC policies to be imported into the APIC, which allows the system to be restored to a previous configuration. You can do an atomic replace, which enables you to roll back to a previous config state.

Caveats

This section includes the following topics:

Open Caveats

This section lists the open caveats in the Cisco ACI, Release 1.0(2j). Click a 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
CSCup97544	When there are more than 64 leaves in the fabric, leaf-to-leaf atomic counters may show incorrect values.
CSCuq82045	For an endpoint group (EPG) mapped to a bridge domain (BD) in legacy mode, if the encap specified at the static path attachment of a port to an EPG is different from the encap mentioned at the BD level, no fault is raised in the current release.
CSCuq82069	The current release does not support unicast routing for a bridge domain in legacy mode and faults are not raised.
CSCur03329	Faults caused by issues related to cluster expansion/shrinking can get lost after a controller reboot.
CSCur12062	The *Application EPGs* page does not properly display the relation between an endpoint group and a contract.
CSCur30817	No error message appears when a new configuration import/export job is triggered while a previous job is pending.
CSCur32882	Changing the REST SSL certificate policy may not take effect on all APIC nodes.
CSCur36058	The switch disappears for several minutes from topology, firmware, and maintenance policies while being upgraded.

Table 2 Open Caveats (continued)

Bug ID	Description
CSCur36121	An APIC Out-of-band management subnet should not overlap with an Infra TEP address subnet. The APIC will not be accessible and the cluster will not converge if there is a conflict
CSCur37585	When the clock between nodes gets re-synched, atomic counters to and from the node shows incorrect drops or incorrect excess packet counts for the first couple of minutes. The suspect flag in the counters is also not set. The condition gets fixed after couple of seconds.
CSCur38673	Ongoing diagnostic test configuration options need to be removed for FEX.
CSCur39124	Switches could get downgraded to a 1.0(1x) version if the imported configuration consists of a firmware policy with a desired version set to 1.0(1x).
CSCur40736	The SVI configuration page does not prompt for or enforce the configuration of a subnet mask.
CSCur44725	The IGMP snoop configuration is not deployed to the infrastructure bridge domain (BD) if that BD is associated to a different private network (Ctx).
CSCur66532	Connecting to an APIC will fail when using HTTPS.
CSCut25657	Traffic between application endpoint groups and external Layer 3 networks on different leafs is dropped if multiple external Layer 3 networks are configured in the same context.

Resolved Caveats

This section lists the resolved caveats in the Cisco ACI, Release 1.0(2j) Click a 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
CSCun44221	Some events on bootup are missed on leaf or spine switches.
CSCuo79243	In some of the 5-minute statistics data the count of ten-second samples is 29 instead of 30.
CSCup47703	The DSCP value specified on an external endpoint group does not take effect on filter rules on the leaf switch.
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 traceroutExecTn managed object, the source node ID field contains only one of the two nodes when the source is behind a vPC.
CSCup93244	The download of an image into the repository fails if you have any special characters in your password.

Table 3 Resolved Caveats (continued)

Bug ID	Description
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.
CSCuq72437	Queries to the fault/health/audit records stored on an APIC that occur at the same time as fault records are written to the database cause database corruption.
CSCuq73081	A graph instance gets stuck in the applying state but no faults appear at the tenant level in the GUI.
CSCuq73335	Modifying or deleting endpoint group configuration parameters can cause the corresponding Graph Instance to go into a “missing config-params” fault state.
CSCuq75324	Importing firmware policies that are stale affects fabric discovery.
CSCuq90805	In vCenter 5.5 deployments, auto-placement of a VNIC can cause the MAC address to disappear.
CSCur26940	Users can configure an endpoint to "any" or "any" to an endpoint flow-based atomic counter rule, which is not supported.
CSCur34218	If a vShield controller is configured and operational in a version earlier than 1.0(2j), a policy based upgrade to 1.0(2j), or subsequent release, will fail in a vShield configuration. Also, a vShield configuration exported from an APIC version earlier than 1.0(2j) cannot be imported back in the APIC running software version 1.0(2j) or later.

Known Behaviors

This section lists caveats that describe known behaviors in the Cisco ACI, Release 1.0(2j). Click a 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
CSCuq21360	Following a FEX or switch reload, configured interface tags are no longer configured correctly.
CSCur49173	Nodes are not joining the fabric after being decommissioned.
CSCur48950	Some reported client endpoints are not present on the APIC during an upgrade.
CSCur62241	The APIC web server rejects ssl connections from older clients.

- During the upgrade from a 1.0(1x2x) to a 1.0(2x) release, endpoints reporting will be delayed until all APICs are upgraded to 1.0(2x).

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

- *Knowledge Base Articles* (KB Articles) are available at the following URL:

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