Cisco Application Policy Infrastructure Controller, Release 1.0(3f), Release Notes

Publication Date: February 11, 2015

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(3f) Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches*. Additional product documentation is listed in the "Related Documentation" section on page 11.

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
February 11, 2015	Created the release notes for Release 1.0(3f).
February 23, 2015	Updated "Compatibility Information".
February 24, 2015	Added a note to the description of the N9K-C9332PQ in the "New Hardware Features in Cisco Application Policy Infrastructure Controller Release 1.0(3f)" section.
March 3, 2015	• Added Bridge Domain to the "Verified Scalability Limits" section. • Added a new information to the "Usage Guidelines" explaining how to configure an atomic counter policy between two endpoints.

Table 1 Online History Change (continued)

Date	Description
March 11, 2015	Added CSCut25657 to "Open Caveats".
April 22, 2015	Added a note to the "Upgrade Instructions".
April 24, 2015	Removed CSCur50369 from Open Caveats and added the supported firmware version to "Compatibility Information".
June 9, 2015	Removed CSCus67228 from "Open Caveats".
July 9, 2015	Updated egg filename.

Contents

This document includes the following sections:

- Introduction, page 2
- Installation Notes, page 4
- Upgrade Instructions, page 4
- Downgrade Instructions, page 4
- Compatibility Information, page 5
- Usage Guidelines, page 5
- Verified Scalability Limits, page 6
- New and Changed Information, page 7
- Caveats, page 8
- Related Documentation, page 11

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:

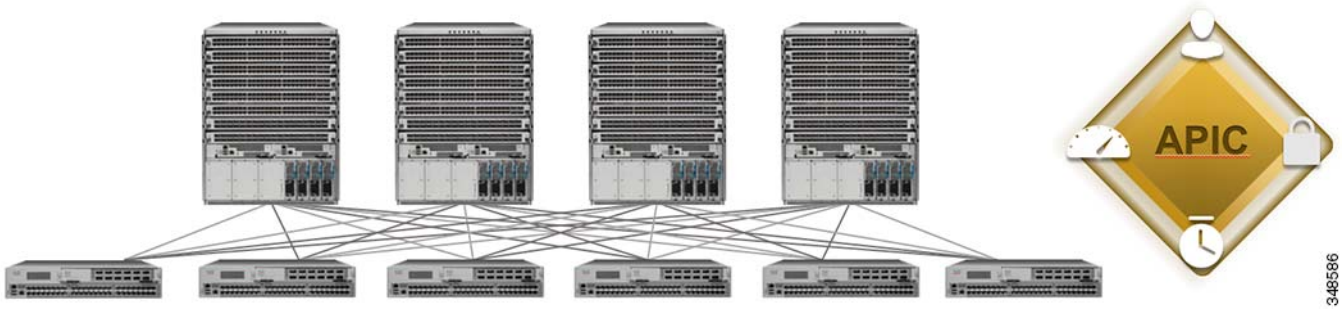
- Application centric network policies
- Data model-based declarative provisioning
- Application, topology monitoring, and troubleshooting
- Third-party integration (Layer 4 through 7 services, vCenter, vShield)
- Image management (spine and leaf)
- Cisco ACI inventory and configuration
- Implementation 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/acimodel-1.0_3f-py2.7.egg

  This is the SDK file.

  - http[s]://<APIC address>/cobra/_downloads/acicobra-1.0_3f-py2.7.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

Follow this procedure when upgrading from a 1.0(2x) release to a 1.0(3x) release:

1. Upgrade the APIC controller software image.
2. After all APICs in the cluster are successfully upgraded, upgrade all the switches in the fabric.

Note The switches may need to be rebooted after upgrading (See CSCut32029).

Downgrade Instructions

Follow this procedure when downgrading from a 1.0(3x) release to a 1.0(2x) release:

1. Downgrade the APIC controller software image.
2. After all APICs in the cluster are successfully downgraded, downgrade all the switches in the fabric.

Note Switch models N9K-C9372PX, N9K-C9332PQ, and N9K-C9372TX are not supported for downgrading in the APIC 1.0(2x) or the Cisco Nexus 9000 11.0(2x) releases. If your fabric has these models, do not downgrade.

Compatibility Information

- Cisco APIC Release 1.0(3f) supports the hardware and software listed on the *ACI Ecosystem Compatibility List* and the software listed as follows:
  - Cisco NX-OS Release 11.0(3f)
  - Cisco AVS, Release 5.2(1)Sv3(1.3)
  - 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
- The breakout of 40G ports to 4x10G on the N9332PQ switch is not supported in ACI-Mode.
- To connect the APIC (the controller cluster) to the ACI fabric, it is required to have a 10G interface on the ACI leaf. You cannot connect the APIC directly to the N9332PQ ACI Leaf.
- Cisco APIC Release 1.0(3f) supports the following firmware:
  - 1.5(4e) CIMC HUU iso
  - 2.0(3i) CIMC HUU iso

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(3f).

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.
- 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.

Verified Scalability Limits

Table 2 contains the maximum verified scale limits for a subset of ACI parameters for the Cisco ACI Release 1.0(3f) and Cisco Nexus 9000 Series ACI-Mode Switches, Release 11.0(3f). These values are based on a profile where each feature was scaled to the numbers specified in the table. The numbers in this table do not represent the theoretically possible ACI fabric scale.

Please contact your Cisco account representative to discuss your use-case or other ACI scale parameters that are not listed here.

Table 2 Verified Scalability Limits

Feature	Maximum Limits for Fabric	Maximum Limits for Leaf Switches	Maximum Limits per Spine Switches
Leaf switches	50	-	-
Spine switches	6	-	-
Layer 3 contexts (VRF contexts or private networks)	100	100	

Table 2 Verified Scalability Limits

Feature	Maximum Limits for Fabric	Maximum Limits for Leaf Switches	Maximum Limits per Spine Switches
Contracts/Filters	1,000 contracts, 10,000 filters	4,000 TCAM entries (specific to N9K-M12PQ) 16,000 tested TCAM entries (specific to N9K-M6PQ) **Note** TCAM entries are used for filters. A filter consisting of more than 1 port (for example, a range of ports) may consume more than 1 entry.	-
End points	100,000	12,000 IPv4 hosts	-
Bridge domains	--	EPG=BD is 3,500 and Multicast Groups < 5,000 Or EPG+BD <= 3,500 and Multicast Groups < 6,750	--
External EPGs per Layer 3 Out	2 per layer 3 outside policy	-	-
Dynamic route peering sessions	-	32	-
Layer 3 outside policies	1 per VRF	-	-
Number or routes (longest prefix matches [LPMs]) on border leaf switches	8,000	4,000	-
Tenant SPAN sessions	-	4	-
Fabric SPAN sessions	-	4	8 per line card
Number of parallel user sessions	100	-	-
vCenters	5	-	-

New and Changed Information

This section lists the new and changed features in Release 1.0(3f), and includes the following topics:

- New Hardware Features in Cisco Application Policy Infrastructure Controller Release 1.0(3f), page 8
- New Software Features in Cisco Application Policy Infrastructure Controller Release 1.0(3f), page 8

New Hardware Features in Cisco Application Policy Infrastructure Controller Release 1.0(3f)

The Cisco Application Policy Infrastructure Controller Release 1.0(3f) supports the following new hardware:

- N9K-C9332PQ - Cisco Nexus 9332PQ 32-port 40 Gigabit Ethernet QSFP+ Top-of-rack (ToR) Layer 3 switch

  Note Please note that the QSFP-4x10G-AOC1M breakout cable is not supported for ACI mode.

- N9K-C9372PX - Cisco Nexus 9372PX 48-port, 10 Gigabit Ethernet SFP+ and 6-port 40 Gigabit Ethernet QSFP+ Top-of-rack (ToR) Layer 3 switch
- N9K-C9372TX - Cisco Nexus 9372TX 48-port, 1/10 Gbps Base-T and 6-port, 40 Gigabit Ethernet QSFP Top-of-rack (ToR) Layer 3 switch

New Software Features in Cisco Application Policy Infrastructure Controller Release 1.0(3f)

The Cisco Application Policy Infrastructure Controller Release 1.0(3f) supports the following new software features:

- Stretched Fabric - This feature allows for each leaf and all spines that participate in creating a fabric to be located up to 30 KMs apart and removes the restriction for every leaf to be connected to all spines.

  For more information about the stretched fabric feature, see the *KB: ACI Stretched Fabric Design* knowledge base article:

  http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_kb-aci-stretched-fabric.html

Caveats

This section includes the following topics:

- Open Caveats, page 9
- Resolved Caveats, page 9
- Known Behaviors, page 11

Open Caveats

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

Table 3 Open Caveats

Bug ID	Description
CSCur36058	The switch disappears for several minutes from topology, firmware, and maintenance policies while being upgraded.
CSCur71082	The APIC is rebooted using CIMC power reboot. On reboot, the system enters into fsck due to a corrupted disk. On recovery of the APIC, some service crashes multiple times and stops permanently.
CSCur79696	When attempting to log into an LDAP provider configured in Strict SSL mode, and the system is not configured with the CA certificate for that LDAP SSL server, the nginx daemon will gracefully restart itself to attempt to work around an openldap library SSL certificate caching bug.
CSCur87395	A tenant cannot be deleted because it is part of "mgmt" or "all" security domains. This may occur after an upgrade from a release 1.0.1x to 1.0.2x
CSCur97373	During a policy upgrade of the APIC controller, some APICs fail to reboot after the upgrade process has completed.
CSCus11097	The NTPD configuration is wiped out on a power shutdown.
CSCus21730	Policy Elements crash on the leaf after deleting an infrastructure configuration such as infraAccBndlGrp, Selectors, or VLAN/VXLAN Namespace.
CSCus26627	On large scale setups, some login requests are taking more than 30 seconds.
CSCus56816	The serial baud rate is changed from 9600 to 115200.
CSCus68295	An enhancement is needed to sync the hardware clock to the NTP clock once per day.
CSCus71655	The APIC Controller Fan stats collection does not display the speed/PWM data regardless of the interval chosen.
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(3f) Click a Bug ID shown in Table 4 to access the Bug Search Tool and see additional information about the bug.

Table 4 Resolved 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.

Table 4 Resolved Caveats (continued)

Bug ID	Description
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.
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.
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).
CSCur65254	The policy element process crashes when upgrading the spine with supervisor slot-2 as active, preventing the spine from joining the fabric.
CSCur73212	The static route to the DHCP provider's subnet is not deleted from the consumer's private network after deleting the contract and the DHCP label from the consumer Bridge Domain.
CSCur82721	DHCP clients are assigned IP addresses after deleting the relay agent label in the bridge domain of the client.
CSCus63191	There is no infra VLAN connectivity to the leaf in the simulator from the ESX (host) added to the AVS.
CSCus69032	The image download gets stuck and does not complete.

Known Behaviors

This section lists caveats that describe known behaviors in the Cisco ACI, Release 1.0(3f). Click a Bug ID shown in Table 5 to access the Bug Search Tool and see additional information about the bug.

Table 5 Known Behaviors

Bug ID	Description
CSCuq21360	Following a FEX or switch reload, configured interface tags are no longer configured correctly.
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).
CSCur49173	Nodes are not joining the fabric after being decommissioned.
CSCur48950	Some reported client endpoints are not present on the APIC during an upgrade.

- During the upgrade from a 1.0(1x) 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*
- *Cisco 10-Gigabit Ethernet Transceiver Modules Compatibility Matrix:*

  http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/10GE_Tx_Matrix.html

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.