Cisco Application Policy Infrastructure Controller, Release 1.0(4h), Release Notes

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(4h) Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches. Additional product documentation is listed in the "Related Documentation" section.

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

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

Table 1 shows the online change history for this document.

Table 1. Online History Change

Date	Description
May 7, 2015	Created the release notes for Release 1.0(4h).
May 15, 2015	Added new upgrade information to the Upgrade Instructions section.
June 9, 2015	Removed CSCus67228 from Open Caveats.
June 10, 2015	Removed CSCus78491 from Resolved Caveats.
June 30, 2015	Updated the supported AVS version.
December 9, 2015	Fixed incorrect URLs to the documentation on cisco.com.
February 29, 2016	In the Compatibility Information section, added a link to the AVS Release Notes.

Contents

This document includes the following sections:

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

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_4h-py2.7.egg

This is the SDK file.

- http[s]://<APIC address>/cobra/_downloads/acicobra-1.0_4h-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) or 1.0(3x) release to the 1.0(4h) 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: If you are using L4-L7 services with a Bridge Domain (BD) for L4-L7 devices in the tenant common, please check to see if you have a vnsRsLIfCtxToBD (L4-L7 device selection policy) relation from any non-common tenant pointing to a BD in the tenant common. This can be determined in the UI or by using the Visore browser interface. An example of a Visore query with an appropriate filter is shown below (replace apic-host-name and challenge-key with appropriate values)

Visore Query Example

```
https://<apic-host-name>/visore.html?f=filter&challenge=<challenge-key>&cls=vnsRsLIfCtxToBD&prop=tDn&op=wcard&val1=uni%2Ftn-common%2FBD-&val2=
```

If the relation exists, run the script cleanupRsLIfCtxToBD.py after upgrading by pointing it at your APIC IP address. The script can be obtained from AS/TAC, or you can find it attached to this bug: CSCuu21167. To run the command, you will need python 2.7, and you will need to set the PYTHONPATH to point to the egg files of the specific version. An example is shown below.

Python Path Example

```
PYTHONPATH=/tmp/104h/acicobra-1.0_4h-py2.7.egg:/tmp/867h/acimodel-1.0_4h-py2.7.egg /opt/cisco/aci/python2.7/bin/python cleanupRsLIfCtxToBD.py -H 192.168.10.1 -P 443 -u admin -p <password-here> -S
```

This script will delete and re-add all the vnsRsLIfCtxToBD relations in your system. GraphInst might go to a fault state and recover, but no traffic disruption is expected.

Downgrade Instructions

Follow this procedure when downgrading from the 1.0(4h) release to a 1.0(2x) or 1.0(3x) 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(4h) supports the hardware and software listed on the ACI Ecosystem Compatibility List and the software listed as follows:
  - Cisco NX-OS Release 11.0(4h)
  - Cisco AVS, Release 5.2(1)Sv3(1.3b)

For more information about the supported AVS releases, see the AVS software compatibility information in the *Cisco Application Virtual Switch Release Notes* at the following URL:

https://www.cisco.com/c/en/us/support/switches/application-virtual-switch/products-release-notes-list.html

- 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(4h) supports the following firmware:
  - 1.5(4e) CIMC HUU iso
  - 2.0(3i) CIMC HUU iso (recommended)

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 release 1.0(4h).

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:

1. Click Show Certificate.
2. 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 tab that includes video demonstrations and documented content.

- 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 that you 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(4h) and Cisco Nexus 9000 Series ACI-Mode Switches, Release 11.0(4h). 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 per for Leaf Switches	Maximum Limits for Spine Switches
Leaf switches	50	-	-
Spine switches	6	-	-
Layer 3 contexts (VRF contexts or private networks)	100	100	

Feature	Maximum Limits for Fabric	Maximum Limits per for Leaf Switches	Maximum Limits for Spine Switches
Contracts/Filters	1,000 contracts, 10,000 filters	4,000 TCAM entries (specific to N9K-M12PQ) 16,000 tested TCAM entries (specified 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	-

Feature	Maximum Limits for Fabric	Maximum Limits per for Leaf Switches	Maximum Limits for Spine Switches
Tenant SPAN sessions Note: A uni-directional SPAN session counts as one, and a bi-directional SPAN session counts as two.	-	4	-
Fabric SPAN sessions Note: A uni-directional SPAN session counts as one, and a bi-directional SPAN session counts as two.	-	4	8 per line card
Number of parallel user sessions	100	-	-
vCenters	5	-	-
Multicast Groups	8,000	8,000	-

New and Changed Information

This section lists the new and changed features in Release 1.0(4h).

- New Hardware Features
- New Software Features

New Hardware Features

Cisco Release 1.0(4h) supports no new hardware features.

New Software Features

Cisco Release 1.0(4h) supports no new software features.

Caveats

This section contains lists of open and resolved caveats and known behaviors.

- Open Caveats
- Resolved Caveats
- Known Behaviors

Open Caveats

Table 3 lists the open caveats in the Cisco APIC Release 1.0(4h). Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 3. Open Caveats in Cisco Release 1.0(4h)

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 may enter into fsck due to a corrupted disk.
CSCur79696	When attempting to log into an LDAP provider configured in Strict SSL mode, and if 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.
CSCur97373	During a policy upgrade of the APIC controller, some APICs fail to reboot after the upgrade process has completed.
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 take more than 30 seconds to complete.
CSCus38227	When a Layer 2 or Layer 3 external instance profile is specified as a provider to a contract, and a collection of endpoint groups within a context is specified as the consumer, the provider will be skipped, which could result in the graph not getting deployed.
CSCus40477	Fault F0467 raised due to Invalid VLAN Configuration (rule: fv-nw-issues-config-failed).
CSCus56816	The serial baud rate is changed from 9600 to 115200.
CSCus71655	The APIC Controller Fan stats collection does not display the speed/PWM data regardless of the interval chosen.

Bug ID	Description
CSCus74493	Interface policies are not applied to all ports if the interface policy group is associated with a policy before the policy is created.
CSCut10398	The help screen for the endpoint retention policy has incorrect default values. This is cosmetic. The help screen should also note that setting the bounce entry aging interval to a value less than the remote endpoint aging interval will create a traffic loss situation when hosts migrate between leaf switches.
CSCut25587	Under high scale circumstances, a new leaf may not get all contracts downloaded.
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.
CSCut36428	The endpoint attachment notification: ■ Does not always result in an attachment notification ■ Is only sent to a subset of deployed service graph instances ■ Is sent to the incorrect service graph instance
CSCut46796	The zoning-rule is missing after deleting or adding 0/0 and/or a particular subnet present in a Layer 3 external network.
CSCut51929	The traffic destined to a shared service provider endpoint group (EPG) picks an incorrect class Id (PcTag) instead of the EPG's class Id and the class Id gets dropped.
CSCut54322	The GUI wizard for a Layer 3 external network used as a consumer does not support the Two Nodes - Firewall in Routed and ADC in Two-Arm mode template.
CSCut56623	When a Layer 3 external network is configured with DSCP marking, it is not copied to a filter rule on the node.
CSCut56639	When DSCP marking is configured on an external endpoint group, it is not copied to the filter rule on the node.
CSCut80792	WebServer uses ciphers that use SHA1. Web browsers, such as chrome, report a warning indicating that SHA1 is obsolete and a stronger hashing algorithm should be used. (as shown in the attached enclosure)
CSCuu02614	After an endpoint is learned, and a graph is removed and reattached, the endpoint will not be added to the L4-L7 device configuration.
CSCuu14565	The tunnel interface for an AVS host (using opflex) is not created if the vPC interface is deleted and added back again within 5 mins. This can impact forwarding for VMs on that host.
CSCuu16805	In the 1.0(4h) release, support for filtering techsupport information for a specified time-window and category was added to generate a techsupport file with a reduced size. If the time-window and/or category filters are set in the GUI for an on-demand techsupport policy named tsod-ts_exp_pol, and then if techsupport collection is triggered through the CLI, the filters still get applied although no filters are specified in the CLI command.

Bug ID	Description
CSCuu16881	A fault is raised indicating that an image downloaded into the repository is bad, although the image is good.
CSCuu23146	Tech support filtering based on category could miss some files when triggered from the GUI.

Resolved Caveats

Table 4 lists the resolved caveats in the Cisco APIC Release 1.0(4h). Click the bug ID to access the Bug Search Tool and see additional information about the bug.

Table 4. Resolved Caveats in Cisco Release 1.0(4h)

Bug ID	Description
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
CSCus11097	The NTPD configuration is wiped out on a power shutdown.
CSCus68295	An enhancement is needed to synchronize the hardware clock to the NTP clock once per day.
CSCus82518	Flood towards the ESX for VXLAN port groups will not work.
CSCus83262	When configuring LDAP Providers and using special characters you may run into the following error. "Server Error backend returned unparsable response" This was using LDAP provider with the hostname 1.1.1.1
CSCut70441	The VTEP tunnel is not present on the leaf.
CSCut85550	The static route definitions are not deleted after removing a public subnet. Checking show ip route vrf all | egrep x.x.x.x shows the subnet is present in the routing table of the leaves while a particular subnet has already been removed from the Bridge Domain.
CSCut02482	The process ipfib crashes on the leaf.
CSCut26163	The script wrapper process is still present after deleting Cisco.haproxy package.
CSCut45754	After a vCenter upgrade, the APIC was not able to collect inventory or start event listener. As a result, vCenter port group objects were not created. On the APIC, we saw a lot of recurring SOAP timeout errors returned by vSphere APIs while trying to pull inventory and when trying to create an event collector.
CSCut58693	Some ESXi hosts may not be displayed under vDS controllers in the APIC.
CSCus65107	The APIC may fail to pull inventory from the vCenter in case one of the ESX hosts in the vCenter is not responding.

Bug ID	Description
CSCut65913	After a DME service has crashed, it does not recover. This issue prevents a service from restarting due to a crash if the internal journal is corrupted. There will be multiple restarts after the first crash, preventing service from coming back online. Cluster health will show degraded due to the service not running.
CSCus74188	Traffic loss occurs after deleting and restoring the 0.0.0.0 prefix.
CSCut02297	Fault F0214 with severity Major observed with description similar to: "Operational issues detected for OpFlex device: 175192220 0.0.0.0 for logical switch comp/prov-VMware/ctrlr-[Company-AVS]-Company-vcenter01/sw-dvs-65500 detected, error: [Invalid dvs name]"
CSCut19696	The policy manager cores on 2 APICs after posting a configuration.
CSCut78100	The vSwitch on the vCenter does not pick the inherited policies from the interface policy group if one overide policy is defined.
CSCut96930	Nginx terminates when the trust point is deleted.
CSCuu05227	VXLAN tunnels are removed when ports are removed/added into the PC configuration.

Known Behaviors

Table 5 lists the known behaviors in the Cisco APIC Release 1.0(4h). Click the Bug ID to access the Bug Search Tool and see additional information about the bug.

Table 5. Known Behaviors in Cisco Release 1.0(4h)

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(2x)/1.0(3x) release, endpoints reporting will be delayed until all APICs are upgraded to 1.0(4x).

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:

https://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:

https://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:*

https://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:

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