Cisco Application Policy Infrastructure Controller, Release 1.1(2h), 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 11.1(2h) 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
August 17, 2015	Created the release notes for Release 1.1(2h)
August 18, 2015	In the New Software Features section, added VMware vSphere 6.0 support. In the Upgrading the APIC Controller section, removed the note in the row for upgrading from 1.0(3x) to 1.0(4x). In the Compatibility Information section, changed the supported Cisco AVS release to 5.2(1)SV3(1.5a).
August 21, 2015	In the Open Caveats section, added bug CSCuv70029. In the Installation Notes section, added that acimodel-1.1_2h-py.egg is also required.
August 26, 2015	In the Resolved Caveats section, added bug CSCuu73404.
August 28, 2015	Rewrote the procedure in the Downgrading the APIC Controller section to provide more information about stateless downgrades.
September 9, 2015	In the Compatibility Information section, changed the note about TLS 1.0 and UCSD integration.
September 16, 2015	In the Known Behaviors section, added bug CSCuv16874.
October 16, 2015	In the Compatibility Information section, added the supported ASA device package version. Also added information about AVS and DVS support with Layer 4 to Layer 7 service insertion or service chaining.
November 13, 2015	In the Known Behaviors section, added bug CSCuw81638.

Date	Description
December 3, 2015	In the "Installation Notes" section, fixed the .egg file URLs.
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.
March 16, 2016	In the Installation Notes section, added mention that ACI with SCVMM or Windows Azure Pack only supports ASCII characters.
February 28, 2017	In the Usage Guidelines section, added: If the communication between the APIC and vCenter is impaired, some functionality is adversely affected. The APIC relies on the pulling of inventory information, updating vDS configuration, and receiving event notifications from the vCenter for performing certain operations.

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 a glossary of terms that are used in the ACI.

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 from the URLs below.

  The following file is the SDK:

  - http[s]://<APIC address>/cobra/_downloads/acimodel-1.1_2h-py.egg

  The following file includes the Python packages that model the Cisco ACI Management Information Tree:

  - http[s]://<APIC address>/cobra/_downloads/acicobra-1.1_2h-py2.7.egg

  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.

- Cisco ACI with Microsoft System Center Virtual Machine Manager (SCVMM) or Microsoft Windows Azure Pack only supports ASCII characters. Non-ASCII characters are not supported. Ensure that English is set in the System Locale settings for Windows, otherwise ACI with SCVMM and Windows Azure Pack will not install. In addition, if the System Locale is later modified to a non-English Locale after the installation, the integration components might fail when communicating with the APIC and the ACI fabric.

Upgrading the APIC Controller

Table 2 lists the supported APIC upgrades.

Table 2 Supported APIC Upgrades

From	To	Limitations	Recommended Procedure
1.1(1x)	1.1(2h)	None	1. Upgrade APICs 2. After APICs are upgraded successfully, upgrade the switches using two or more maintenance groups

From	To	Limitations	Recommended Procedure
1.0(4x)	1.1(2h)	None	3. Upgrade APICs 4. After APICs are upgraded successfully, upgrade the switches using two or more maintenance groups
1.0(3x)	1.1(2h)	None	1. Upgrade APICs 2. After APICs are upgraded successfully, upgrade the switches using two or more maintenance groups
1.0(3x)	1.0(4x)	None	1. Upgrade APICs 2. After APICs are upgraded successfully, upgrade the switches using two or more maintenance groups
1.0(2x)	1.0(4x)	None	1. Upgrade APICs 2. After APICs are upgraded successfully, upgrade the switches using two or more maintenance groups
1.0(2x)	1.0(3x)	None	1. Upgrade APICs 2. After APICs are upgraded successfully, upgrade the switches using two or more maintenance groups

Downgrading the APIC Controller

Downgrading from this release to 1.1(10) or 1.0(40) is supported. However, this release does not support a stateful downgrade to 1.0(3x) or earlier releases. If you wish to downgrade from this release to 1.0(3x) or earlier must perform a stateless downgrade, as shown in the following procedure.

Note: You must plan for a Fabric outage, as this procedure rebuilds the Fabric.

1 Export the Fabric configuration.

2 Run the "eraseconfig" command on the APIC controllers. This will reboot the controllers. Ensure that the controllers have been rebooted before moving on to step 3.

3 Run the "setup-clean-config.sh" script on the switch nodes and reload all of the switches. Steps 2 and 3 clear the configuration on the Fabric, making this is a stateless downgrade.

4 Rediscover the Fabric.

5 Downgrade the Fabric to the desired release.

6 Run the "eraseconfig setup" command on the APIC controllers. This step is required so that the script can run additional commands that might be required for the version that is being used. The "eraseconfig setup" command will reload the APICs.

7 Run the "setup-clean-config.sh" script on the switch nodes and reload them.

8 Complete the initial setup script on the APIC controllers.

9 Import the Fabric configuration using the import "merge" mode.

Compatibility Information

- This release supports the hardware and software listed on the ACI Ecosystem Compatibility List and the software listed as follows:
  - Cisco NX-OS Release 11.1(2h)
  - Cisco AVS, Release 5.2(1)SV3(1.5a)

    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 N2348UPQ to ACI leaf switches, the following options are available:
  - Directly connect the 40G FEX ports on the N2348UPQ to the 40G switch ports on the N9332PQ switch
  - Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the N9396PX or N9372PX switches
- 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.
- This release supports the following firmware:
  - 1.5(4e) CIMC HUU iso
  - 2.0(3i) CIMC HUU iso (recommended)
- The Cisco Application Virtual Switch (AVS) in either VLAN or VXLAN mode is not supported with Layer 4 to Layer 7 service insertion or service chaining. VMware vSphere Distributed Switch (VDS) is the only supported configuration.
- This release supports the partner packages specified here: https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/solution-overview-c22-734587.html
- This release supports Adaptive Security Appliance (ASA) device package version 1.2.3.4.
- For information about APIC compatibility with UCS Director, see the appropriate *Cisco UCS Director Compatibility Matrix* document at the following URL:

  https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-director/products-device-support-tables-list.html

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 1.1(2h).

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 the 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 in-band and out-of-band networks.
- The APIC does not provide IPAM services for tenant workloads.
- To reach the APIC CLI from the GUI: select System > Controllers, highlight a controller, right-click and select "launch SSH". To get the list of commands, press the escape key twice.
- 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 in-band and out-of-band management connectivity.
  - Syslog server
  - Call Home SMTP server
  - Tech support export server
  - Configuration export server
  - Statistics export server
- In-band 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 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.

- When configuring two Layer 3 external networks on the same node, the loopbacks need to be configured separately for both Layer 3 networks.
- All endpoint groups (EPGs), including application EPGs and Layer 3 external EPGs, require a domain. Interface policy groups must also be associated with an Attach Entity Profile (AEP), and the AEP must be associated with domains. Based on the association of EPGs to domains and of the interface policy groups to domains, the ports and VLANs that the EPG uses are validated. This applies to all EPGs including bridged Layer 2 outside and routed Layer 3 outside EPGs. For more information, see the *Cisco Fundamentals Guide* and the *KB: Creating Domains, Attach Entity Profiles, and VLANs to Deploy an EPG on a Specific Port* article.

Note: In the 1.0(4x) and earlier releases, when creating static paths for application EPGs or layer 2/layer 3 outside EPGs, the physical domain was not required. In this release, it is required. Upgrading without the physical domain will raise a fault on the EPG stating "invalid path configuration."

- An EPG can only associate with a contract interface in its own tenant.
- User passwords must meet the following criteria:
  - Minimum length is 8 characters
  - Maximum length is 64 characters
  - Fewer than three consecutive repeated characters
  - At least three of the following character types: lowercase, uppercase, digit, symbol
  - Cannot be easily guessed
  - Cannot be the username or the reverse of the username
  - Cannot be any variation of "cisco", "isco", or any permutation of these characters or variants obtained by changing the capitalization of letters therein
- The power consumption statistics are not shown on leaf node slot 1.
- If the communication between the APIC and vCenter is impaired, some functionality is adversely affected. The APIC relies on the pulling of inventory information, updating vDS configuration, and receiving event notifications from the vCenter for performing certain operations.

Verified Scalability Limits

For the verified scalability limits, see the *Verified Scalability Guide* for this release:

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

New and Changed Information

This section lists the new and changed features in Release 1.1(2h) and includes the following topics:

New Software Features

Table 3 lists the new software features in this release:

Table 3 New Software Features, Guidelines, and Restrictions

Feature	Description	Guidelines and Restrictions
ACI Optimizer	After entering your network requirements in an Optimizer Config Template, the ACI Optimizer tells you how many leafs you will need for your network and suggests how to deploy each application and external EPG on each leaf without violating any constraints. Also, after entering your existing topology in an Optimizer Config Template, the ACI Optimizer helps you determine if you have what you need, if you are exceeding any limitations, and suggests how to deploy each application and external EPG on each leaf.	When using the ACI Optimizer, Scale constraints may be violated if the given topology is not enough.
AES encryption for configuration files	As of release 1.1(2), the secure properties of APIC configuration files can be encrypted by enabling AES-256 encryption.	AES encryption is a global configuration option; all secure properties conform to the AES configuration setting. It is not possible to export just a portion of the ACI fabric such as a tenant configuration with AES encryption.
SCVMM clustering support	You can now install the APIC SCVMM agent on a Highly Available System Center Virtual Machine Manager (SCVMM).	None.
VMware vSphere 6.0 support	ACI now supports VMware vCenter 6.0. See the *Cisco ACI Virtualization Guide* for more information.	The vCenter 6.0 feature of vMotion across a vCenter/datacenter is not supported.
Windows Azure Pack with L3out support	Windows Azure Pack tenants can now configure their networks to connect outside of the fabric. This is done by establishing a security contract to L3ExtOut for both incoming and outgoing traffic. See the *Cisco ACI Virtualization Guide* for more information.	None.

New Hardware Features

This release supports no new hardware features.

Caveats

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

- Open Caveats
- Resolved Caveats
- Known Behaviors

Open Caveats

Table 4 lists the open caveats in the Cisco APIC Release 1.1(2h) release. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 4 Open Caveats in Cisco APIC Release 1.1(2h)

Bug ID	Description
CSCur36058	The switch disappears for several minutes from topology, firmware, and maintenance policies while being upgraded.
CSCuu49742	In Microsoft SCVMM, if a VM network is already attached and used by virtual machines, and if an admin changes the VLAN number of this VM network on SCVMM, the virtual machine VLAN information is not automatically updated on Hyper-V Host virtual machines.
CSCuv70029	A spine drops the Multiprotocol Border Gateway Protocol (MBGP) routes when it receives the prefixes that have its own fabric autonomous system number in the BGP AS-PATH attribute in the default VRF.

Resolved Caveats

Table 5 lists the resolved caveats in the Cisco APIC Release 1.1(2h) release. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 5 Resolved Caveats in Cisco APIC Release 1.1(2h)

Bug ID	Description
CSCuu42733	The APIC appliance sees a crash in the DMEs while getting a replication transaction, or when a configuration is missing on the APIC that was introduced with a different version.
CSCuu73404	When an endpoint group (EPG) is deployed on two interfaces of a ToR such that one interface has the VLAN scope configured as global and the other has the VLAN scope configured as local, the common domain (the domain associated with both the EPG and the interface) must be picked for EPG deployment. Sometimes, when the interface with a global VLAN scope is associated with multiple domains (domains with overlapping VLAN namespaces), instead of the common domain getting picked up for deployment, another domain gets picked up. This leads to an EPG not getting deployed on the port with a local VLAN scope.
CSCuu84437	VTEP tunnels for VXLAN load balancing might go missing and lead to traffic drop when OpFlex times out due to the stress load on rebooting a couple of hosts with a few hundred vEths.
CSCuu84497	If a user selects a custom time range while keeping the category field to be "system info" in the GUI for the tech support policy, the tech support files are not exported.
CSCuu84967	Expired user authentication certificates cannot be deleted.

Bug ID	Description
CSCuu87980	Only admin users can access the "Visibility Tool" (Troubleshooting Wizard). Role-admin users cannot access the tool.

Known Behaviors

Table 6 lists caveats that describe known behaviors in the Cisco NX-OS Release 1.1(2h) release. Click the Bug ID to access the Bug Search Tool and see additional information about the bug.

Table 6 Known Behaviors in Cisco APIC Release 1.1(2h)

Bug ID	Description
CSCuo52668	The APIC does not validate duplicate IPs assigned to two device clusters. The communication to devices or the configuration of service devices might be affected.
CSCuo79243	In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.
CSCuo79250	The node ID policy can be replicated from an old appliance that is decommissioned when it joins a cluster.
CSCup47703	The DSCP value specified on an external endpoint group does not take effect on filter rules on the leaf switch.
CSCup79002	The hostname resolution of the syslog server fails on leaf and spine switches over in-band connectivity.
CSCup94070	After importing an exported configuration, graph instances are not created and L4-L7 packages are missing in the system.
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).
CSCur48950	Some reported client endpoints are not present on the APIC during an upgrade.
CSCur71082	The APIC is rebooted using the CIMC power reboot. On reboot, the system enters into fsck due to a corrupted disk.
CSCus15627	The Cisco APIC Service (ApicVMMService) shows as stopped in the Microsoft Service Manager (services.msc in control panel > admin tools > services) after valid domain credentials are entered during installation or configuration of the service.
CSCut51929	The traffic destined to a shared service provider endpoint group picks an incorrect class Id (PcTag) and gets dropped.
CSCuu09236	Traffic from an external layer 3 network is allowed when configured as part of a vzAny (a collection of endpoint groups within a context) consumer.
CSCuu61998	The microsegment endpoint group is in the incorrect state after downgrading.
CSCuu64219	Downgrading the fabric starting with the leaf will cause faults such as policy-deployment-failed with fault code F1371.

Bug ID	Description
CSCuv16874	Open Shortest Path First (OSPF) is now enabled on the loopback interfaces to ensure that proper equal-cost multi-path routing (ECMP) is available with a not-so-stubby area (NSSA) area. This impacts the OSPF forwarder address in the link state advertisement, meaning the loopback address will be linked to the OSPF router ID. As a result, you might see that you are learning the same router ID in multiple VRFs. This can have an impact if you are stitching together the NSSA and non-NSSA areas by a directly connected external device, such as an ASA firewall, because the external device will learn the router ID from two separate OSPF areas. As the forwarder address will now match the router ID, it might potentially begin to blackhole traffic in one of the OSPF areas, most likely the NSSA area.
CSCuw81638	The OpenStack metadata feature cannot be used with ACI integration with the Juno release (or earlier) of OpenStack due to limitations with both OpenStack and Cisco's ML2 driver.

Related Documentation

The Cisco Application Policy Infrastructure Controller (APIC) documentation can be accessed from the following website:

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

New Documentation

This section lists the new Cisco APIC product documents for this release.

- *KB: Importing and Exporting Configuration Files*
- *KB: Using the ACI Optimizer*