Cisco Application Policy Infrastructure Controller, Release 1.2(1m), Release Notes

This document describes the features, caveats, and limitations for the Cisco Application Policy Infrastructure Controller (APIC) software.

Note: Use this document in combination with the *Cisco NX-OS Release 11.2(1m) Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches*, which you can view at the following location:

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html

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
January 22, 2016	Created the release notes for Release 1.2(1m).
February 12, 2016	In the Compatibility Information section, changed the Cisco AVS release to 5.2(1)SV3(1.10a).
February 29, 2016	In the Installation Notes section, added mention that you should back up your configuration before installing or upgrading to this release. In the Compatibility Information section, updated the supported ASA device package version to "1.2.4.8 or later". Added a link to the cisco.com page that has the *Cisco ACI Virtualization Guide*. Added a link to the AVS Release Notes.
March 11, 2016	Added the new software features, changes in behavior, and resolved caveats that were documented in the deferred 1.2(1i) and 1.2(1k) releases.
March 16, 2016	In the Installation Notes section, added mention that ACI with SCVMM or Windows Azure Pack only supports ASCII characters.
August 11, 2016	In the Upgrading the APIC Controller section, added information about upgrading from an unlisted release.

Date	Description
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*.
- Back up your APIC configuration prior to installing or upgrading to this release. Single APIC clusters, which should not be run in production, can lose their configuration if database corruption occurs during the installation or upgrade.
- 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*.

  The SDK egg file needed for installation is included in the package:

  — acicobra-1.2_1m-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.

You can find all of the indicated documentation 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

Upgrading the APIC Controller

Table 2 lists the supported APIC upgrades. If you are upgrading from a release that is not listed in the table, you must first upgrade to one of the listed "From" releases, and then upgrade to this release.

Table 2 Supported APIC Upgrades

From	To	Limitations	Recommended Procedure
1.2(1i)	1.2(1m)	None	1. Upgrade APICs 2. After APICs are upgraded successfully, upgrade the switches using two or more maintenance groups

From	To	Limitations	Recommended Procedure
1.1(4x)	1.2(1m)	Due to bug CSCux40954, which was resolved in this release, the Cisco APIC firmware process using the **Upload** button from the GUI does not work. The upload appears to complete successfully, but the firmware is not updated in the repository. You must instead download the image using SCP or HTTP from a server to the APIC.	1. Upgrade APICs 2. After APICs are upgraded successfully, upgrade the switches using two or more maintenance groups
1.1(3f)	1.2(1m)	None	1. Upgrade APICs 2. After APICs are upgraded successfully, upgrade the switches using two or more maintenance groups
1.1(2h)	1.2(1m)	None	1. Upgrade APICs 2. After APICs are upgraded successfully, upgrade the switches using two or more maintenance groups
1.1(1x)	1.2(1m)	None	1. Upgrade APICs 2. After APICs are upgraded successfully, upgrade the switches using two or more maintenance groups
1.0(4o) or later	1.2(1m)	None	1. Upgrade APICs 2. After APICs are upgraded successfully, upgrade the switches using two or more maintenance groups

Downgrading the APIC Controller

Table 3 lists the supported APIC and switch downgrades.

Note: APIC Image downgrades will be blocked by default if the target image is not in a supported downgrade path.

Table 3 Supported APIC and Switch Downgrades

From	To	Limitations	Recommended Procedure

From	To	Limitations	Recommended Procedure
1.2(1x)	1.1(1o) and higher	None	1. Downgrade APICs. 2. After APICs are downgraded successfully, downgrade the switches using two or more maintenance groups.
1.2(1x)	1.0(4q) and lower	None	You must perform a stateless downgrade. See the procedure below.

The following procedure performs a stateless downgrade:

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 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* document and the software listed as follows:
  - Cisco NX-OS Release 11.2(1m)
  - Cisco AVS, Release 5.2(1)SV3(1.10a)

    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

  See the *ACI Ecosystem Compatibility List* document at the following URL:

  https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/solution-overview-listing.html
- 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)
- Beginning with Cisco Application Virtual Switch (AVS) release 5.2(1)SV3(1.10), Layer 4 to Layer 7 service graphs are supported for Cisco AVS. Layer 4 to Layer 7 service graphs for Cisco AVS can be configured for virtual machines only and in VLAN mode only.
- This release supports VMM Integration and VMware Distributed Virtual Switch (DVS) 6.x. For more information about guidelines for upgrading VMware DVS from 5.x to 6.x and VMM integration, see the *Cisco ACI Virtualization Guide, Release 1.2(1x)* 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
- This release supports the partner packages specified in the *L4-L7 Compatibility List Solution Overview* document at the following URL:

  https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/solution-overview-listing.html
- This release supports the Adaptive Security Appliance (ASA) device package version 1.2.4.8 or later.
- If you are running a Cisco Adaptive Security Virtual Appliance (ASAv) version that is prior to version 9.3(2), you must configure SSL encryption as follows:

  (config)# ssl encryption aes128-sha1
- 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 42 (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 1.2(1m).

  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 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.
- For Layer 3 external networks created through the API or Advanced GUI and updated through the CLI, protocols need to be enabled globally on the external network through the API or Advanced GUI, and the node profile for all the participating nodes needs to be added through the API or Advanced GUI before doing any further updates through the CLI.
- For Layer 3 external networks created through the CLI, you should not to update them through the API. These external networks are identified by names starting with "__ui_".
- The output from "show" commands issued in the NX-OS-style CLI are subject to change in future software releases. Cisco does not recommend using the output from the show commands for automation.
- In this software version, the CLI is supported only for users with administrative login privileges.
- If you defined multiple login domains, you can choose the login domain that you want to use when logging in to an APIC. By default, the domain drop-down list is empty, and if you do not choose a domain, the DefaultAuth domain is used for authentication. This can result in login failure if the username is not in the DefaultAuth login domain. As such, you must enter the credentials based on the chosen login domain.
- 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 this release and includes the following topics:

- New Software Features
- New Hardware Features
- Changes in Behavior

New Software Features

Table 4 lists the new software features in this release:

Table 4 New Software Features, Guidelines, and Restrictions

Feature	Description	Guidelines and Restrictions
Basic GUI and Advanced GUI for the APIC	The APIC GUI now has two operating modes: the Basic GUI and Advanced GUI. The Basic GUI is simplified compared to the Advanced GUI, which provides for easier and faster configuration of ACI constructs. The Basic GUI has intelligence embedded that enables the APIC to create some of the ACI model constructs automatically for you, and the Basic GUI provides validations to ensure consistency in the configuration. This functionality reduces and prevents faults. The Advanced GUI is equivalent to the GUI of the previous releases. You should use the Advanced GUI to manage any policy that you created prior to release 1.2. For more information, see the *Cisco APIC Getting Started Guide*.	The performance for some Layer 3 configurations using the Basic GUI can be slow.
NX-OS-Style CLI for APIC	The APIC CLI is now similar to the NX-OS CLI. The NX-OS CLI has intelligence embedded that enables the APIC to create some of the ACI model constructs automatically for you, and the CLI provides validations to ensure consistency in the configuration. This functionality reduces and prevents faults. For more information, see the *Cisco APIC Getting Started Guide* and *Cisco APIC NX-OS Style Command-Line Interface Configuration Guide*.	The performance for some CLI commands can be slow in a scale setup. For more information, see Verified Scalability Limits.
Class of Service Preservation	The ACI fabric enables preserving 802.1p class of service (CoS) within the fabric. Enable the fabric global QoS policy dot1p-preserve option to guarantee that the 802.1p value in packets which enter and transit the ACI fabric is preserved.	None
Common Pervasive Gateway	This feature enables you to configure multiple ACI fabrics with an IPv4 common gateway on a per bridge domain basis. Doing so enables moving one or more virtual machine (VM) or conventional hosts across the fabrics while the host retains its IP address. VM host moves across fabrics can be done automatically by the VM hypervisor. The ACI fabrics can be co-located, or provisioned across multiple sites. The Layer 2 connection between the ACI	None

Feature	Description	Guidelines and Restrictions
	fabrics can be a local link, or can be across a routed WAN link.	
Common Tenant	In the troubleshooting wizard, you can now configure a session with a bridge domain and context in the "Common" tenant.	None
Configuration Rollback	The Configuration Rollback feature allows a user to create snapshots in both a manual and scheduled manner. These snapshots can then be used to revert the configuration to a specific point in time.	None
Direct Server Return	The direct server return feature enables a server to respond directly to clients without having to go through the load balancer, which eliminates a bottleneck in the server-to-client path. For more information, see the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*.	None
Ingress Policy Enforcement for Layer 3 Out Scale	Starting with release 1.2(1), ingress-based policy enforcement enables defining policy enforcement for Layer 3 Out traffic with regard to egress and ingress directions. The default is ingress. During an upgrade to release 1.2(1) or higher, existing Layer 3 Out configurations are set to egress so that the behavior is consistent with the existing configuration; no special upgrade sequence needs to be planned. After the upgrade, an administrator changes the global property value to ingress. Once changed, the system reprograms the rules and prefix entries. Rules are removed from the egress leaf and installed on the ingress leaf, if not already present. If not already configured, an Actrl prefix entry is installed on the ingress leaf. Direct server return (DSR), and attribute-based EPGs require ingress-based policy enforcement. vzAny and taboo ignore ingress-based policy enforcement. Transit rules are applied at ingress. In Ingress Policy enforcement mode, if a contract is defined between an L3InstP and an endpoint group, all of the prefixes of the L3InstP are installed in a non-border leaf where that endpoint group is present.	None
Local Policy Enforcement	This feature enforces a physical leaf's policy on traffic that is across the fabric.	None
Maximum Prefix Limit	Tenant networking protocol policies for BGP l3extOut connections can be configured with a maximum prefix limit that enables monitoring and restricting the number of route prefixes received from a peer. Once the max prefix limit is exceeded, a log entry can be recorded, further prefixes can be rejected, the connection can be restarted if the count drops below the threshold in a fixed interval, or the connection is shut down. Only one option can be used at a time. The default setting is a limit of 20,000 prefixes, after which new prefixes are rejected. When the reject option is deployed, BGP accepts one more prefix beyond the configured limit and the APIC raises a fault.	
Microsegmentation for Microsoft	This feature supports virtual machine attribute-based endpoint groups for virtual endpoints that are attached to a VMM domain	None

Feature	Description	Guidelines and Restrictions
Virtualization	that has Microsoft SCVMM associated with it. This feature is dependent the Microsoft System Center UR9 release and the appropriate APIC agent. For more information, see the *Cisco ACI Virtualization Guide*.	
Microsegmentation with IP-based Endpoint Groups	This feature supports IP-based endpoint groups for physical or virtual endpoints as they are admitted into the fabric. This policy is applied at the physical node level. For more information, see the *Cisco ACI Virtualization Guide*.	You must use any of the following hardware to use this feature: • Nexus 9372PX-E • Nexus 9372TX-E • N9K-M6PQ-E
Role-Based Access Control Rule Enhancements	Layer 4 to Layer 7 policy configurations in a multi-tenant environment required administrator intervention to create certain objects that cannot be created by tenant administrators using the classic role-based access control (RBAC) domains and roles model definition. An Application Policy Infrastructure Controller (APIC) provides more granular RBAC privileges in the management information tree (MIT) such that you can grant tenant administrators the privileges that are required to create the objects. Tenant administrators can also create RBAC rules through self-service without administrator intervention to grant permissions for resources under their tenant subtree to other tenants and users in the system. For more information, see the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*.	None
Shared Layer 3 Out	A shared Layer 3 Out configuration provides routed connectivity to external networks as a shared service. An l3extInstP endpoint group (EPG) provides routed connectivity to external networks. It can be can be provisioned as a shared service in any tenant (user, common, infra, or mgmt.). Prior to release 1.2(1x), this configuration was only supported in the user and common tenants. An EPG in any tenant can use a shared services contract to connect with an `l3extInstP` EPG regardless of where in the fabric that `l3extInstP` EPG is provisioned. This simplifies the provisioning of routed connectivity to external networks; multiple tenants can share a single `l3extInstP` EPG for routed connectivity to external networks. Sharing an `l3extInstP` EPG is more efficient because it consumes only one session on the switch regardless of how many EPGs use the single shared `l3extInstP` EPG.	None
Simple Network Management Protocol support for APIC	The Simple Network Management Protocol (SNMP) is now supported for APIC.	None
Fabric Secure Mode	Fabric secure mode enhances physical fabric security by enforcing checks for leafs, spines, and APICs that join the fabric by requiring	None

Feature	Description	Guidelines and Restrictions
	manual approval before they can join the fabric.	
Static Route with Weights	The ACI fabric static route preference feature keeps static route preferences intact across leaf switches so that route selection happens based on this preference.	None
Unmanaged Mode	The unmanaged mode for services enables you to choose the APIC's behavior for allocating network resources and programming the fabric. When enabled, the unmanaged mode restricts the APIC to allocate only the network resources for a service appliance and to program only the fabric (leaf). The configuration of the device is left to be done externally by you. For more information, see the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*.	None
vRealize Integration	You can integrate ACI with VMWare's vRealize Orchestration (vRO), vRealize Automation (vRA), and vCenter. For more information, see the *Cisco ACI Virtualization Guide*.	None
vSphere vMotion support across two vSphere Distributed Switches (vDSs) vSphere vMotion support across two vCenters	vSphere vMotion capabilities have been enhanced in this release, enabling users to perform live migration of virtual machines across virtual switches, and vCenter Server systems. For more information, see the *VMware vSphere 6.0 Release Notes*.	None

New Hardware Features

This release supports no new hardware features.

Changes in Behavior

This section lists changes in behavior in this release.

- If an APIC REST query must return more than 100,000 objects, then an error is returned instead. The error message is "Unable to process the query, result dataset is too big" and the http error code is "400" (BAD_REQUEST). For queries that could return a large number of objects, the appropriate filters should be used. For example, filter for objects that are modified within a given time range, specified classes in the response subtree instead of the full subtree, or query from a subset of nodes instead of from all nodes. The limit of 100,000 objects can be increased to up to 500,000 by configuring the policy. However, increasing the limit might lead to slower response and the potential for memory exhaustion.

Caveats

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

- Open Caveats
- Resolved Caveats
- Known Behaviors

Open Caveats

Table 5 lists the open caveats in this release. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 5 Open Caveats in Cisco APIC Release 1.2(1m)

Bug ID	Description
CSCuw61081	Live migration of a virtual machine initiated from SCVMM might fail if there is a compliance check failure on the virtual machine network.
CSCux39365	Port channel association to external connectivity using the CLI or Basic GUI might fail if the name is large.
CSCux43024	Configuring a VRF or context filter for SPAN-ing fabric ports by using the CLI does not succeed.
CSCuw61304	After a clean reboot and import of the configuration, a fault is raised for mgmt node connection groups.
CSCuw93034	Using the browser upload button to upload an image to the APIC from a local machine and canceling the upload midway, a stale image file remains in the /firmware/fwrepos/fwrepo.Uploads/ directory.
CSCux09127	If the Troubleshooting wizard is configured with the Layer 4 to Layer 7 service provider as the source and the Layer 4 to Layer 7 service consumer as the destination, it might not work.
CSCux25207	After upgrading TORs from the 1.1(4e) release to the 1.2(1k) release, when the maint-grp-1 set of the TORs are rebooted, there is traffic loss on the virtual machines.
CSCux40946	In some configuration sequences, the public subnets of some of the bridge domains might not be advertised to external networks, even though the protocols (BGP, OSPF, EIGRP) are configured with the 'default' route-map in the 'out' direction.
CSCux43480	External Layer 3 configuration for Layer 4 to Layer 7 route peering is unsupported through the CLI.
CSCux99581	After deleting and recreating an export policy with the same name, any subsequent triggering of export does not work.

Resolved Caveats

Table 6 lists the resolved caveats in this release. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 6 Resolved Caveats in Cisco APIC Release 1.2(1m)

Bug ID	Description
CSCuw16683	A fault for prefix-entry-already-in-use is present when the fault is not expected.

Bug ID	Description
CSCuw18244	A deployment query for an in-band endpoint group is not showing all in-band zones that are associated with the endpoint group.
CSCuw22254	An invalid path fault occurs when the same domain is attached to the selector domain and the domain is present on the override.
CSCuw23295	When running a troubleshooting wizard session, if a VMKernel endpoint that is attached to a virtual distributed switch is used for the source or destination, the troubleshooting wizard fails and the following error message returns: "Error processing data returned from server: TypeError: Cannot read property 'findParentRecord' of null".
CSCuw27075	In the "Show Usage" table of the GUI, spine nodes are shown for an endpoint group to IP atomic counter policies.
CSCuw27454	The deployment query for dhcpRelayP sometimes returns nodes where the policy was previously deployed.
CSCuw27507	In the "Show Usage" table of the GUI, diagnostics policies applicable to leaf nodes are shown to be deployed on spine nodes as well, and vice versa.
CSCuw35070	If there are two or more primary IP addresses configured and if one of the primary IP addresses that is in use is deleted, then the deleted IP address is still used as the primary IP address. None of the remaining primary addresses are used.
CSCuw52253	Pagination support for Layer 4 to Layer 7 parameter in case a huge list of parameters is to be configured.
CSCuw95500	Audit deduplication causes some objects to be deleted.
CSCux11026	The vmmmgr process crashes due to VMM reconfiguration.
CSCux40954	The Cisco APIC firmware process using the **Upload** button from the GUI does not work. The upload appears to complete successfully, but the firmware is not updated in the repository.
CSCux48724	Headers are missing in the output of the **fabric show** commands.
CSCux51883	After upgrading to the 1.2(1i) release, there is packet loss when pinging the oobmgmt port and the oobmgmt MAC address is flaps between ports on the switch upstream.
CSCux52176	After changing the UCS FI OOB management address, VMM connectivity is broken. The "moquery -c fvDyPathAtt" command shows the entries as zero.
CSCux54801	If a DHCP relay policy is already associated to the endpoint group of the respective external Layer 3 policy, attempting to configure multiple Layer 3 interface profiles under an SVI using the same IP address with VLAN encapsulation in access mode, the following error is generated: "Server Error:400 - child (Rn) of class dhcpGwDef is already attached. dn[(Dno)] Dno=, Rn=gwdef-[IP_ADDRESS],"
CSCux56954	The showconfig command may fail with a CERTIFICATE_VERIFY_FAILED error.
CSCux59930	The "show vlan extended" command does not show the infra VLAN in the ACI firmware release 1.2.
CSCux61566	The policymgr dumps a core after upgrading from the 1.1(1j) release to the 1.2(1) release, prior to upgrading the leafs.
CSCux73674	If an endpoint moves to a different PathEP, the learned path is not updated.

Known Behaviors

Table 7 lists caveats that describe known behaviors in this release. Click the Bug ID to access the Bug Search Tool and see additional information about the bug.

Table 7 Known Behaviors in Cisco APIC Release 1.2(1m)

Bug ID	Description
CSCu052668	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.
CSCu079243	In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.
CSCu079250	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 Layer 4 to Layer 7 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.
CSCuw09389	For direct server return operations, if the client is behind the Layer 3 out, the server-to-client response will not be forwarded through the fabric.
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