Cisco Application Policy Infrastructure Controller Release Notes, Release 2.3(1)

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

Note: Use this document in combination with the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.3(1)*, 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 bugs. 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

You can watch videos that demonstrate how to perform specific tasks in the Cisco APIC on the Cisco ACI YouTube channel:

https://www.youtube.com/c/CiscoACIchannel

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
June 14, 2017	2.3(1e): Release 2.3(1e) became available.
July 9, 2017	2.3(1f): Release 2.3(1f) became available; there are no changes to this document for this release.
July 17, 2017	2.3(1e): Added CSCvd44106 to Open Bugs.
July 24, 2017	Added a change in behavior.
August 17, 2017	2.3(1f): Added Known Behavior CSCve34392.
August 24, 2017	Added restrictions to Symmetric Ether-channel hashing. 2.3(1e): Added bug CSCve76599 to known behavior 2.3(1f): Added a resolved bug.
August 30, 2017	Updated VMware Distributed Virtual Switch (DVS) from 6.0 to 6.5.
October 20, 2017	2.3(1i): Release 2.3(1i) became available; there are no changes to this document for this release.

Date	Description
October 25, 2017	2.3(1e): In the Open Bugs section, removed bugs CSCve52334, CSCve52459, CSCve58616, CSCve71413, CSCve75272, CSCve75969, and CSCve76166. These bugs were erroneously included.
October 30, 2017	2.3(1e): In the Open Bugs section, removed bug CSCve75781, which was erroneously included.
November 20, 2017	In the Usage Guidelines section, changed a mention of "Virtual Private Cloud (VPC)" to "virtual port channel (vPC)."
January 22, 2018	2.3(1l): Release 2.3(1l) became available. Added the resolved bugs for this release.
February 7, 2018	2.3(1e): In the Known Behaviors section, added bug CSCve67134.
February 13, 2018	2.3(1l): In the Compatibility Information section, added the following text: Starting with patch 2.3(1l), the supported Cisco AVS release is 5.2(1)SV3(3.5a).
February 22, 2018	In the New Software Features section, added the following item: Cisco Tetration Analytics support on the Cisco N9K- 93180YC-FX, N9K-93108TC-FX switches
February 23, 2018	2.3(1o): Release 2.3(1o) became available; there are no changes to this document for this release.
June 7, 2018	2.3(1e): In the Open Bugs section, added bug CSCvj75897.
June 19, 2018	2.3(1p): Release 2.3(1p) became available. Added the resolved bugs for this release.
August 13, 2018	In the New Software Features section, for the Traffic storm control unicast/multicast differentiation feature, added the following restriction: Traffic storm control unicast/multicast differentiation is not supported on Cisco Nexus C93128TX, C9396PX, C9396TX, C93120TX, C9332PQ, C9372PX, C9372TX, C9372PX-E, or C9372TX-E switches.
November 21, 2018	2.3(1e): In the Open Bugs section, added bug CSCvn15374.
May 6, 2019	2.3(1o): In the Known Behaviors section, added bug CSCvp36834.
August 5, 2019	2.3(1l): In the Open Bugs section, added bug CSCvj76503. 2.3(1o): In the Open Bugs section, added bug CSCvp42156. 2.3(1p): In the Resolved Bugs section, added bug CSCvp42156.
September 17, 2019	2.3(1e): In the Open Bugs section, added bug CSCuu17314 and CSCve84297.

Date	Description
October 4, 2019	In the Miscellaneous Guidelines section, added the following bullet: ■ When you create an access port selector in a leaf interface rofile, the fexId property is configured with a default value of 101 even though a FEX is not connected and the interface is not a FEX interface. The fexId property is only used when the port selector is associated with an infraFexBndlGrp managed object.

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 Cisco ACI, including a glossary of terms that are used in the Cisco ACI.

Compatibility Information

This release supports the following Cisco APIC servers:

Product ID	Description
APIC-L1	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1000 edge ports)
APIC-L2	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1000 edge ports)
APIC-M1	Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1000 edge ports)
APIC-M2	Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1000 edge ports)

The following list includes general 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 12.3(1e)
  - Cisco AVS, Release 5.2(1)SV3(3.5)
    - Starting with patch 12.3(1l), the supported Cisco AVS release is 5.2(1)SV3(3.5a).

    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

  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
- To connect the N2348UPQ to Cisco ACI leaf switches, the following options are available:
  - Directly connect the 40G FEX ports on the N2348UPQ to the 40G switch ports on the ACI leaf switches

  - Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the 10G ports on all other ACI leaf switches

    Note: A fabric uplink port cannot be used as a FEX fabric port.

- 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 switch, unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the N9332PQ switch will auto-negotiate to 10G without requiring any manual configuration.
- This release supports the following firmware:
  - 2.0(3i) CIMC HUU iso
  - 2.0(9c) CIMC HUU iso
  - 2.0(13i) CIMC HUU iso (recommended)
- Beginning with Cisco Application Virtual Switch (AVS) release 5.2(1)SV3(1.10), you can connect service virtual machines that are part of Layer 4 to Layer 7 service graphs to AVS. Layer 4 to Layer 7 service graphs for Cisco AVS can be configured for service virtual machines that are in VLAN mode. By using using an AVS VMM domain with both VLAN and VXLAN, you can have a virtual machine in VXLAN mode that is protected by service graphs that are using the service virtual machine in VLAN mode.
- This release supports VMM Integration and VMware Distributed Virtual Switch (DVS) 6.5. 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 2.3(1)* 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 Microsoft System Center Virtual Machine Manager (SCVMM) Update Rollup 9, 10, and 11 releases, and the Microsoft Windows Azure Pack Update Rollup 9, 10, and 11 releases.
- This release supports SCVMM 2016 and Microsoft Hyper-V 2016.
- 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 Adaptive Security Appliance (ASA) device package version 1.2.5.5 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
- A known issue exists with the Safari browser and unsigned certificates, which applies when connecting to the APIC GUI. For more information, see the *Cisco APIC Getting Started Guide*.
- For information about Cisco 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

- Beginning with this release, contracts using matchDscp filters are only supported on switches with “EX” on the end of the switch name. For example, N9K-93108TC-EX.
- When downgrading from Cisco APIC 2.2(2) to an older release, if you need to delete the Virtual Port Channel (VPC), upgrade to Cisco APIC 2.2(2), delete the VPC, and downgrade again.

Usage Guidelines

This section lists usage guidelines for the Cisco APIC software.

- The Cisco 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 Cisco APIC does not provide IPAM services for tenant workloads.
- To reach the Cisco 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
- Both leaf and spine switches can be managed from any host that has IP connectivity to the fabric.
- If an IP address is learned on one of two endpoints for which you are configuring an atomic counter policy, you should 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: When creating static paths for application EPGs or Layer 2/Layer 3 outside EPGs, the physical domain is not 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. You must view the statistics from any other node.
- 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 Basic GUI or 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.
- The CLI is supported only for users with administrative login privileges.
- Do not separate virtual port channel (vPC) member nodes into different configuration zones. If the nodes are in different configuration zones, then the vPCs’ modes become mismatched if the interface policies are modified and deployed to only one of the vPC member nodes.
- If you defined multiple login domains, you can choose the login domain that you want to use when logging in to a Cisco 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.
- A firmware maintenance group should contain a maximum of 80 nodes.
- When contracts are not associated with an endpoint group, DSCP marking is not supported for a VRF with a vzAny contract. DSCP is sent to a leaf along with the actrl rule, but a vzAny contract does not have an actrl rule. Therefore, the DSCP value cannot be sent.
- When creating a vPC domain between two leaf switches, both switches must be in the same switch generation. Switches not in the same generation are not compatible vPC peers. The generations are as follows:
  - Generation 1—Cisco Nexus N9000K switches without “EX” on the end of the switch name; for example, N9K-9312TX
  - Generation 2—Cisco Nexus N9K switches with “EX” on the end of the switch model name; for example, N9K-93108TC-EX

- Cisco ACI does not support a class E address as a VTEP address.
- In a multipod fabric, if a spine in POD1 uses the infra tenant L3extOut-1, the TORs of the other pods (POD2, POD3) cannot use the same infra L3extOut (L3extOut-1) for Layer 3 EVPN control plane connectivity. Each POD must use its own spine switch and infra L3extOut.
- A multipod deployment requires the 239.255.255.240 system Global IP Outside (GIPo) to be configured on the inter-pod network (IPN) as a PIM BIDIR range. This 239.255.255.240 PIM BIDIR range configuration on the IPN devices can be avoided by using the Infra GIPo as System GIPo feature. The Infra GIPo as System GIPo feature must be enabled only after upgrading all of the switches in the ACI fabric, including the leaf switches and spine switches, to the latest APIC release.
- The APICs must have 1 SSD and 2 HDDs, and both RAID volumes must be healthy before upgrading to this release. The APIC will not boot if the SSD is not installed.
- You do not need to create a customized monitoring policy for each tenant. By default, a tenant shares the common policy under tenant common. The APIC automatically creates a default monitoring policy and enables common observables. You can modify the default policy under tenant common based on the requirements of your fabric.
- 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.
- If you are upgrading VMware vCenter 6.0 to vCenter 6.5, you should first delete the following folder on the VMware vCenter:

  C:\ProgramData\cisco_aci_plugin

  If you do not delete the folder and you try to register a fabric again after the upgrade, you will see the following error message:

  Error while saving setting in C:\ProgramData\cisco_aci_plugin\<*user*>_<*domain*>.properties

  user is the user that is currently logged in to the vSphere Web Client, and *domain* is the domain to which the user belongs. Although you can still register a fabric, you do not have permissions to override settings that were created in the old VMware vCenter. You must enter any changes in the APIC configuration again after restarting VMware vCenter.
- In a multipod fabric setup, if a new spine switch is added to a pod, it must first be connected to at least one leaf switch in the pod. Then the spine switch will be able to discover and join the fabric.
- Caution: If you install 1 Gigabit Ethernet (GE) or 10GE links between the leaf and spine switches in the fabric, there is risk of packets being dropped instead of forwarded, because of inadequate bandwidth. To avoid the risk, use 40GE or 100GE links between the leaf and spine switches.
- When you create an access port selector in a leaf interface rofile, the fexId property is configured with a default value of 101 even though a FEX is not connected and the interface is not a FEX interface. The fexId property is only used when the port selector is associated with an infraFexBndlGrp managed object.

Verified Scalability Limits

For the verified scalability limits (except the CLI limits), see the *Verified Scalability Guide* for this release.

For the CLI verified scalability limits, see the *Cisco NX-OS Style Command-Line Interface Configuration Guide* for this release.

You can access these documents 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 and Changed Information

This section lists the new and changed features in this release and includes the following topics:

New Software Features

Table 2 lists the new software features in this release:

Table 2 New Software Features, Guidelines, and Restrictions

Feature	Description	Guidelines and Restrictions
Encapsulation Scope for SVI across Layer 3 Networks	By default, the transit VLAN is different for each Layer 3 Out. You can now reduce the transit VLAN consumption by choosing an encapsulation scope setting such that the transit VLAN remains the same in all Layer 3 Outs in the same VRF instance for a given VLAN encapsulation in an SVI interface. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide.	None.
Symmetric Ether-channel hashing	Symmetric Ether-channel hashing is now supported on the following switches: ■ N9K-93108TC-FX ■ N9K-93108YC-FX ■ N9K-93180YC-EX ■ N9K-C93108TC-EX ■ N9K-C93180LC-EX	The following are restrictions for Symmetric Ether-channel hashing: ■ Supported only for unicast IPv4/IPv6 data packets. ■ Not supported on VPC. ■ N9K-C93180YC-EX, N9K-C93108TC-EX, 9348GC-FXP, 93108TC-FX, and 93180YC-FX TORs support only one symmetric hashing

Feature	Description	Guidelines and Restrictions
		configuration. ■ Not supported on Cisco Nexus 2000 Series Fabric Extenders.
802.1Q tunnel core port functionality	You can configure multiple 802.1Q tunnels on the same core port to carry double-tagged traffic from multiple customers, each distinguished with an access encapsulation configured for each 802.1Q tunnel. You can also disable MAC Address Learning on 802.1Q tunnels. Both edge ports and core ports can belong to an 802.1Q tunnel with access encapsulation and disabled MAC Address Learning. Both edge ports and core ports in Dot1q Tunnels are supported on third-generation Cisco Nexus 9000 series switches with "FX" on the end of the switch model name.	None.
Hot Standby Router Protocol (HSRP) support – FX	Support for HSRP is enabled on FX platforms.	None.
DHCP Relay for Layer 3 (L3) Out Consumer	This is an extension of the existing Tenant DHCP relay feature. With this new extension, you can now configure a L3 Port (ext-svi/sub-if/routed) as a DHCP relay interface.	None.
Netflow on 9348GC-FXP, 93108TC-FX, and 93180YC-FX ToR switches	The feature enables you to perform Netflow monitoring of the traffic flowing through the Cisco Application Centric Infrastructure (Cisco ACI) fabric. Support is enabled in FX platforms.	None.
CDP on FEX support on 9348GC-FXP, 93108TC-FX, and 93180YC-FX ToR switches	This feature enables Cisco Discovery Protocol (CDP) support on FEX connected to FX Platform switches.	None.
Fibre Channel over Ethernet (FCOE) FEX support – FX	This feature enables FCOE support on FEX connected to FX Platform switches.	None.
Stretched Switched Virtual Interface (SVI) for Multipod (MPOD)	This feature enables support for an L3 out-SVI to be configured (stretched) on Border leaf switches across multiple PODs in a Cisco ACI MPOD topology. Supported only on EX and FX platforms.	None.
Reflective Relay	Reflective relay transfers switching for virtual machines	Reflective relay is supported

Feature	Description	Guidelines and Restrictions
(802.1Qbg)	out of the host server to an external network switch. This feature provides connectivity between virtual machines on the same physical server and the rest of the network. It allows policies that you configure on the Cisco APIC to apply to traffic between the virtual machines on the same server.	on physical ports, port channels (PCs), and virtual port channels (VPCs) on physical domains, only. Reflective relay is supported on Cisco Nexus 9000 series switches with EX or FX at the end of the model name. Cisco Fabric Extender (FEX) and blade servers are not supported.
Filtering for Virtual Machines Using More than one Attribute	You can now filter for virtual machines by specifying more than one attribute.	None.
Matching Attributes for a Microsegment EPG While Filtering for Virtual Machines	You can now match any attribute or all attributes for a microsegment (uSeg) EPG while filtering for virtual machines.	You cannot match all attributes when filtering for network-based attributes. See the chapter "Microsegmentation with Cisco ACI" in the Cisco ACI Virtualization Guide.
Creating Block Statements When Defining Attributes for a uSeg EPG	You can now create block statements when defining attributes for a uSeg EPG, enabling you to create precise multilevel filtering rules.	You cannot have more than two sublevels within a block statement. See the chapter "Microsegmentation with Cisco ACI" in the Cisco ACI Virtualization Guide.
EPG Match Precedence	The EPG match precedence option enables you to override the default precedence rules when filtering for virtual machine-based attributes.	EPG match precedence is not supported for network-based attributes.
Virtual Machine-Based Tag Attribute	The virtual machine-based tag attribute enables you to define an attribute based on criteria that is not defined in other attributes.	You must add the tag in VMware vCenter before you define a tag attribute for a uSeg EPG. See the chapter "Microsegmentation with Cisco ACI" in the Cisco ACI

Feature	Description	Guidelines and Restrictions
		Virtualization Guide.
Control Plane Policing	Protects the control plane and separates it from the data plane, which ensures network stability, reachability, and packet delivery.	None.
Traffic storm control unicast/multicast differentiation	You can now configure storm control on each traffic type separately.	Traffic storm control unicast/multicast differentiation is not supported on Cisco Nexus C93128TX, C9396PX, C9396TX, C93120TX, C9332PQ, C9372PX, C9372TX, C9372PX-E, or C9372TX-E switches.
Support for Deny Prefix	Denying context rules for specific routes is now supported.	None.
FIPs for Switches	This release adds support for FIPs at the switch level.	None.
CORS HTTP Access Control	Sets the Access-Control-Allow-Credentials header in the web server responses.	None.
Data Plane/Port Security Timeout	Configuring delay time before MAC-learning is re-enabled is supported.	None.
Cisco APIC Quota Management	Starting in the Cisco Application Policy Infrastructure Controller (APIC) Release 2.3(1), there are admin can configure limits on number of objects a tenant admin can configure. This enables the admin to limit what managed objects that can be added under a given tenant or globally across tenants. See the Cisco APIC Quota Management Configuration knowledge base article.	None.
Contract Inheritance	To streamline associating contracts to new EPGs, you can now enable an EPG to inherit all the (provided/consumed) contracts associated directly to another EPG in the same tenant. Contract inheritance can be configured for application, microsegmented, L2Out, and L3Out EPGs. Any changes you make to the EPG contract master's contracts, are received by the inheriting EPG. For more information, see "Basic User Tenant Configuration" in the Cisco APIC Basic Configuration Guide.	None.
OpFlex Client Identity Detection	To deploy GOLF or Linux Opflex clients in an environment where the identity of the client cannot be guaranteed by the network, you can now dynamically validate the client's	When you enable certificate enforcement, connectivity is disabled with any GOLF or

Feature	Description	Guidelines and Restrictions
	identity based on a client certificate.	Linux OpFlex client that does not support client authentication.
Cisco Tetration Analytics support on the Cisco N9K-93180YC-FX, N9K-93108TC-FX switches	Cisco Tetration Analytics telemetry is now supported on the Cisco N9K- 93180YC-FX, N9K-93108TC-FX switches.	None.

New Hardware Features

For new hardware features, see the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.3(1)* at the following location:

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

Changes in Behavior

This section lists changes in behavior in this release.

- The OpFlex client is now authenticated through the SSL certificate. With a new installation of the Cisco APIC, this is now the default behavior. This behavior can be reverted back to no client authentication through the OpflexSettings object. Upon upgrading to a Cisco APIC installation of the 2.3(1) release, the default setting is to not authenticate clients. This behavior changes when the administrator posts OpflexSettings that specify for the Cisco APIC to authenticate clients.
- In this release, there is a performance improvement in the APIC GUI reload time of over 70% on application load over slow internet connections in comparison with earlier releases.
- Starting with APIC Release 2.3(1), integration of Cisco ACI with VMware vShield is deprecated and no longer supported.
- Nova v3 endpoints are now supported.

Bugs

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

- Open Bugs
- Resolved Bugs
- Known Behaviors

Open Bugs

This section lists the open bugs. Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Exists In" column of the table specifies the 2.3(1) releases in which the bug exists. A bug might also exist in releases other than the 2.3(1) releases.

Table 3 Open Bugs in the 2.3(1) Release

Bug ID	Description	Exists in
CSCvq86573	Under a corner case, the Cisco APIC cluster DB may become partially diverged after upgrading to a release that introduces new services. A new release that introduces a new DME service (such as the domainmgr in the 2.3 release) could fail to receive the full size shard vector update in first two-minute window, which causes the new service flag file to be removed before all local leader shards are able to boot into the green field mode. This results in the Cisco APIC cluster DB becoming partially diverged.	2.3(1p) and later
CSCvi41092	The APIC log files are extremely large, which takes a considerable amount of time to upload, especially for users with slow internet connectivity.	2.3(1o) and later
CSCvp42156	When you downgrade the Cisco APIC from the 2.3(1) release or later to a release that is earlier than 2.3(1), all of the APICs reload simultaneously. There is no noticeable impact to your fabric.	2.3(1o)
CSCvj76503	A maintenance window triggered for an upgrade remains active for an unlimited time. Adding another node to this maintenance window automatically upgrades this newly added node. In some releases, such as 3.1(2m), a message may say that the window is triggered from X to Y time period; however, the maintenance window is still active for an unlimited time.	2.3(1l) and later
CSCvf70411	A route will be advertised, but will not contain the tag value that is set from the VRF route tag policy.	2.3(1f) and later
CSCvq35344	Requesting an enhancement to allow exporting a contract by right clicking the contract itself and choosing "Export Contract" from the right click context menu. The current implementation of needing to right click the Contract folder hierarchy to export a contract is not intuitive.	2.3(1f) and later
CSCvn00576	An SHA2 CSR for the ACI HTTPS certificate cannot be configured in the APIC GUI.	2.3(1f) and later
CSCuu17314	CDP is not enabled on the management interfaces for the leaf switches and spine switches.	2.3(1e) and later
CSCvd43548	The stats for a given leaf switch rule cannot be viewed if a rule is double-clicked.	2.3(1e) and later
CSCvd44106	After downgrading Cisco APIC from a 2.3 release to a 2.2 release, a node might show a different TEP IP address.	2.3(1e) and later

Bug ID	Description	Exists in
CSCvd66359	The Port ID LLDP Neighbors panel displays the port ID when the interface does not have a description. Example: Ethernet 1/5, but if the interface has description, the Port ID property shows the Interface description instead of the port ID.	2.3(1e) and later
CSCve67986	Virtual machines are not placed into micro segment EPGs when their attributes match.	2.3(1e) and later
CSCve84297	A service cannot be reached by using the APIC out-of-band management that exists within the 172.17.0.0/16 subnet.	2.3(1e) and later
CSCvf70362	This enhancement is to change the name of "Limit IP Learning To Subnet" under the bridge domains to be more self-explanatory. Original : Limit IP Learning To Subnet: [check box] Suggestion : Limit Local IP Learning To BD/EPG Subnet(s): [check box]	2.3(1e) and later
CSCvh52046	This is an enhancement to allow for text-based banners for the Cisco APIC GUI login screen.	2.3(1e) and later
CSCvi82903	When authenticating with the Cisco APIC using ISE (TACACS), all logins over 31 characters fail.	2.3(1e) and later
CSCvj75897	A fault is raised that specifies problem that occurred while retrieving tagging information for a VMM controller. Inventory pull from the VMware vCenter takes a long time (>10 minutes) and it continuously completes with a partial inventory result. The processing of events from VMware vCenter is delayed, which may result in delays for the downloading of policies to the leaf switches when EPGs are deployed on-demand at the VMM domain. This would affect connectivity for newly deployed VMs or VMs which have been vMotioned.	2.3(1e) and later

Bug ID	Description	Exists in
CSCvn15374	When upgrading Cisco APICs, constant heartbeat loss is seen, which causes the Cisco APICs to lose connectivity between one another. In the Cisco APIC appliance_director logs, the following message is seen several hundred times during the upgrade: appliance_director||DBG4||...||Lost heartbeat from appliance id= ... appliance_director||DBG4||...||Appliance has become unavailable id= ... On the switches, each process (such as policy-element) see rapidly changing leader elections and minority states: adrs_rv||DBG4|||Updated leader election on replica=(6,26,1)	2.3(1e) and later
CSCvp64280	A vulnerability in the fabric infrastructure VLAN connection establishment of the Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an unauthenticated, adjacent attacker to bypass security validations and connect an unauthorized server to the infrastructure VLAN. The vulnerability is due to insufficient security requirements during the Link Layer Discovery Protocol (LLDP) setup phase of the infrastructure VLAN. An attacker could exploit this vulnerability by sending a malicious LLDP packet on the adjacent subnet to the Cisco Nexus 9000 Series Switch in ACI mode. A successful exploit could allow the attacker to connect an unauthorized server to the infrastructure VLAN, which is highly privileged. With a connection to the infrastructure VLAN, the attacker can make unauthorized connections to Cisco Application Policy Infrastructure Controller (APIC) services or join other host endpoints. Cisco has released software updates that address this vulnerability. There are workarounds that address this vulnerability. This advisory is available at the following link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-n9kaci-bypass	2.3(1e) and later
CSCvq43101	When opening an external subnet, a user cannot see Aggregate Export/Import check boxes set in GUI even though they were already configured.	2.3(1e) and later
CSCvr65035	The last APIC in the cluster gets rebooted when APIC-1 is decommissioned due to some issue seen on APIC-1 while upgrading. In addition, after decommissioning APIC-1, the other APICs still wait for APIC-1 to get upgraded.	2.3(1e) and later
CSCvr94614	There is a minor memory leak in svc_ifc_policydist when performing various tenant configuration removals and additions.	2.3(1e) and later

Resolved Bugs

This section lists the resolved bugs. Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Fixed In" column of the table specifies whether the bug was resolved in the base release or a patch release.

Table 3 Resolved Bugs in the 2.3(1) Release

Bug ID	Description	Fixed in
CSCuw91050	The Cisco APIC dumps core files, and the affected Cisco APICs cannot fully join the cluster or might be stuck in a “data layer partially diverged” state.	2.3(1l)
CSCvd30648	When configuring route leaking between VRFs, traffic between a shared L3Out and a VzAny consumer might be dropped.	2.3(1e)
CSCve66852	After a remote user logs in, an error message appears that is similar to the following example: configured object ((Dn0)) not found error for userPreferences object	2.3(1l)
CSCve76599	After upgrading to Cisco APIC 2.2(2i) or 2.3(1e), there might be faults for the FPGA mismatch.	2.3(1f)
CSCve92205	Deleting a remote user from the GUI does not work.	2.3(1l)
CSCvf02563	When a user logs into a Cisco ACI cluster using the Remote Auth mechanism (such as Radius or TACACS+), the Cicso APIC creates a local entry of the remote user, which can be seen using the GUI. Traditionally, the Cicso APIC GUI allows the deletion of remote users created in this manner, but it was not working in the previous releases of 2.3(1).	2.3(1l)
CSCvg00499	LLDP adjacency to looseNode objects is up, but the VLANs are not programmed on the ports. Run the following command in the leaf switch's CLI to see that there is no leqptRsLsNodeToIf object for the interface: moquery -c leqptRsLsNodeToIf	2.3(1p)
CSCvg60902	The VMMMgr process crashes shortly after being started. The VMMMgr logs show the following error right before the crash: UNCONDITIONAL ASSERT () (lHpNicMo != __null) failed @ ../svc/vmmmgr/src/gen/ifc/app/./imp/comp/TaskCompHpNicAddorDelVtepNicImp.cc:126	2.3(1l)
CSCvg61345	The Cisco AVS DPA process might crash on AVS after upgrading to a 3.1 release. This does not always occur. When it does occur, the DPA process restarts automatically.	2.3(1l)
CSCvg96793	All ESXi hosts show as disconnected under the VMM Integration when you click on the VMM domain. The VMware vCenter might still show as online. The svc_ifc_opflexelem.log file for the leaf switches will show DVS as not found.	2.3(1l)
CSCvh16532	When attempting to log into the Cisco APIC GUI, you might receive the error "AAA Server Authentication DENIED." You might also see the following message in a network trace when the LDAP server responds to the APIC's search query: "In order to perform this operation a successful bind must be completed."	2.3(1l)
CSCvp42156	When you downgrade the Cisco APIC from the 2.3(1) release or later to a release that is earlier than 2.3(1), all of the APICs reload simultaneously. There is no noticeable impact to your fabric.	2.3(1p)

Known Behaviors

This section lists bugs that describe known behaviors. Click the Bug ID to access the Bug Search Tool and see additional information about the bug. The "Exists In" column of the table specifies the 2.3(1) releases in which the known behavior exists. A bug might also exist in releases other than the 2.3(1) releases.

Table 4 Known Behaviors in the 2.3(1e) Release

Bug ID	Description	Exists in
CSCuo52668	The Cisco APIC does not validate duplicate IP addresses that are assigned to two device clusters. The communication to devices or the configuration of service devices might be affected.	2.3(1e) and later
CSCuo79243	In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.	2.3(1e) and later
CSCuo79250	The node ID policy can be replicated from an old appliance that is decommissioned when it joins a cluster.	2.3(1e) and later
CSCup47703	The DSCP value specified on an external endpoint group does not take effect on the filter rules on the leaf switch.	2.3(1e) and later
CSCup79002	The hostname resolution of the syslog server fails on leaf and spine switches over in-band connectivity.	2.3(1e) and later
CSCuq21360	Following a FEX or switch reload, configured interface tags are no longer configured correctly.	2.3(1e) and later
CSCur39124	Switches can be 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).	2.3(1e) and later
CSCur71082	If the Cisco APIC is rebooted using the CIMC power reboot, the system enters into fsck due to a corrupted disk.	2.3(1e) and later
CSCus15627	The Cisco APIC Service (ApicVMMService) shows as stopped in the Microsoft Service Manager (services.msc in control panel > admin tools > services). This happens when a domain account does not have the correct privilege in the domain to restart the service automatically.	2.3(1e) and later
CSCut51929	The traffic destined to a shared service provider endpoint group picks an incorrect class ID (PcTag) and gets dropped.	2.3(1e) and later
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.	2.3(1e) and later

Bug ID	Description	Exists in
CSCuu61998	Newly added microsegment EPG configurations must be removed before downgrading to a software release that does not support it.	2.3(1e) and later
CSCuu64219	Downgrading the fabric starting with the leaf switch will cause faults such as policy-deployment-failed with fault code F1371.	2.3(1e) and later
CSCva32534	Creating or deleting a fabricSetupP policy results in an inconsistent state.	2.3(1e) and later
CSCva60439	After a pod is created and nodes are added in the pod, deleting the pod results in stale entries from the pod that are active in the fabric. This occurs because the Cisco APIC uses open source DHCP, which creates some resources that the Cisco APIC cannot delete when a pod is deleted.	2.3(1e) and later
CSCva86794	When a Cisco APIC cluster is upgrading, the Cisco APIC cluster might enter the minority status if there are any connectivity issues. In this case, user logins can fail until the majority of the Cisco APICs finish the upgrade and the cluster comes out of minority.	2.3(1e) and later
CSCva97082	When downgrading from a 2.2(2e) release to a 2.0(1) release, the spines and its interfaces must be moved from infra L3out2 to infra L3out1. After infra L3out1 comes up, delete L3out2 and its related configuration, and then downgrade to a 2.0(1) release.	2.3(1e) and later
CSCvb39702	No fault gets raised upon using the same encapsulation VLAN in a copy device in tenant common, even though a fault should get raised.	2.3(1e) and later
CSCvb52882	Modifying DNS settings for the APIC does not update the DN settings inside the container for a stateful app.	2.3(1e) and later
CSCve67134	Remote users cannot be deleted.	2.3(1e) and later
CSCve76599	After upgrading to Cisco APIC 2.2(2i) or 2.3(1e), there might be faults for the FPGA mismatch.	2.3(1e) and later
CSCve34392	Managed Objects (MOs) fvRsToVm and fvRsToVm might be missing for some fvEpDefRef MOs after VM migration.	2.3(1f) and later
CSCvp36834	When you downgrade the Cisco APIC from the 2.3(1) release or later to a release that is earlier than 2.3(1), all of the APICs reload simultaneously. There is no noticeable impact to your fabric.	2.3(1o)

- In a multipod configuration, before you make any changes to a spine switch, ensure that there is at least one operationally “up” external link that is participating in the multipod topology. Failure to do so could bring down

the multipod connectivity. For more information about multipod, see the *Cisco Application Centric Infrastructure Fundamentals* document and the *Cisco APIC Getting Started Guide*.

- Precision Time Protocol packets are not allowed to pass-through the Cisco ACI fabric.

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

The documentation includes installation, upgrade, configuration, programming, and troubleshooting guides, technical references, release notes, and knowledge base (KB) articles, as well as other documentation. KB articles provide information about a specific use case or a specific topic.

By using the “Choose a topic” and “Choose a document type” fields of the APIC documentation website, you can narrow down the displayed documentation list to make it easier to find the desired document.

The following tables describe the core APIC documentation.

Note: Not every document has a new version for each release. Unless specified otherwise, the latest document version applies if the document was not revised for a specific release.

Table 5 Release Notes

Document	Description
Cisco ACI Simulator Release Notes, Release 2.3(1)	Provides release information for the Cisco ACI Simulator product.
Cisco Application Policy Infrastructure Controller, Release 2.3(1), Release Notes	This document. Provides release information for the Application Policy Infrastructure Controller (APIC) product.
Cisco Nexus 9000 Series ACI-Mode Switch FPGA/EPLD Upgrade Release Notes, Release 12.3(1)	Provides release information for the Cisco Nexus 9000 series ACI-mode switch FPGA/EPLD product.
Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.3(1)	Provides release information for the Cisco NX-OS for Cisco Nexus 9000 series ACI-mode switches product.

Table 6 Installation, Upgrade, and Configuration Documentation

Document	Description
Cisco APIC Basic Configuration Guide	Describes steps that you must perform to configure your ACI fabric.
Cisco APIC Getting Started Guide	Describes the first things that you must do to use the APIC after you install the APIC software.
Cisco Nexus 93108TC-EX ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.

Document	Description
Cisco Nexus 93180YC-EX ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9332PQ ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9336PQ ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9372PX ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9372TX and 9372-TX-E ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9396PX ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9396TX ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9504 ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9508 ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9516 ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 93180LC-EX ACI Mode Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco APIC Management, Installation, Upgrade, and Downgrade Guide	Describes how to upgrade or downgrade the APIC controller's appliance firmware and how to install the APIC software. This document also describes any limitations when upgrading or downgrading.
Minimum and Recommended Cisco ACI and APIC Releases	Lists the minimum and recommended ACI and APIC software releases for both new and existing deployments.
Operating Cisco Application Centric Infrastructure	Describes how to perform day-to-day operations with the ACI.
Verified Scalability Guide for Cisco ACI and Cisco Nexus 9000 Series ACI-Mode Switches	Describes the maximum verified scalability limits for ACI parameters for the Cisco ACI and Cisco Nexus 9000 Series ACI-Mode Switches.

Table 7 Interface Documentation

Document	Description

Document	Description
Cisco APIC NX-OS Style Command-Line Interface Configuration Guide	Describes how to configure the APIC using the NX-OS-style CLI.
Cisco APIC REST API User Guide	Describes how to use the APIC REST APIs.

Table 8 Reference Documentation

Document	Description
Cisco Application Centric Infrastructure Fundamentals	Provides a basic understanding of the capabilities of the ACI and APIC.

Table 9 Layer 4 to Layer 7 Documentation

Document	Description
Cisco APIC Layer 4 to Layer 7 Device Package Development Guide	Describes how to develop a device package for the Layer 4 to Layer 7 services.
Cisco APIC Layer 4 to Layer 7 Service Graph Deployment Guide	Describes how to deploy a Layer 4 to Layer 7 service graph in greater detail than the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide* with common use cases.
Cisco APIC Layer 4 to Layer 7 Services Deployment Guide	Describes how to deploy the Layer 4 to Layer 7 services using the APIC.

Table 10 Virtualization Documentation

Document	Description
Cisco ACI Virtualization Guide	Describes how to deploy ACI with virtualization solutions, such as Cisco AVS, VMware VDS, or Microsoft SCVMM.

Table 11 ACI with OpenStack Documentation

Document	Description
Cisco ACI Installation Guide for Mirantis OpenStack	Describes how to install the plugin that allows you to use Mirantis OpenStack with ACI.
Cisco ACI with OpenStack OpFlex Deployment Guide for Red Hat	Describes how to deploy ACI with OpenStack OpFlex on the Red Hat platform.
Cisco ACI with OpenStack OpFlex Deployment Guide for Ubuntu	Describes how to deploy ACI with OpenStack OpFlex on the Ubuntu platform.
Installing the Cisco APIC OpenStack Driver	Describes how to install the APIC OpenStack driver.
OpenStack Group-Based Policy User Guide	Describes how to use group-based policies.

Table 12 Troubleshooting Documentation

Document	Description
Cisco APIC Troubleshooting Guide	Describes how to troubleshoot common APIC issues.
Troubleshooting Cisco Application Centric Infrastructure	Additional information about how to troubleshoot common APIC issues.

New Documentation

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

- *Cisco ACI Virtualization Guide*
- *Cisco APIC Quota Management Configuration*
- *Cisco APIC Security Configuration Guide*
- *Cisco APIC Verified Scalability Guide*
- *Cisco CLI Command Reference*
- *CoPP KB Article*
- *Open Source Used in Cisco APIC*