# Cisco Application Policy Infrastructure Controller Release Notes, Release 3.2(4)

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 lifecycle. Cisco Application Policy Infrastructure Controller (APIC) is the software, or operating system, that acts as the controller.

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.

This document describes the features, bugs, and limitations for the Cisco APIC.

Note: Use this document with the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 13.2(4)*, 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

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

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

Note: The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Table 1 shows the online change history for this document.

Table 1 Online History Change

| Date | Description |
|---|---|
| December 9, 2022 | In the Open Bugs section, added bug CSCvw33061. |
| August 1, 2022 | In the Miscellaneous Compatibility Information section, added:<br>■ 4.1(2k) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) |
| February 23, 2022 | In the Miscellaneous Compatibility Information section, added:<br>■ 4.1(2g) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) |
| February 9, 2021 | In the Open Bugs section, added bug CSCvt07565. |
| February 3, 2021 | In the Miscellaneous Compatibility Information section, for CIMC HUU ISO, added:<br>■ 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2 |
| December 16, 2020 | In the Miscellaneous Compatibility Information section, CIMC release 4.1(1g) is now recommended for UCS C220/C240 M4 (APIC-L2/M2). |
| October 8, 2019 | In the Miscellaneous Compatibility Information section, updated the latest supported CIMC releases to:<br>— 4.0(2g) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)<br>— 3.0(4l) CIMC HUU ISO (recommended) for UCS C220/C240 M3 (APIC-L1/M1) |
| October 4, 2019 | In the Miscellaneous Guidelines section, added the following bullet:<br>■ 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. |
| October 3, 2019 | In the Miscellaneous Guidelines section, added the bullet that begins as follows:<br>■ Fabric connectivity ports can operate at 10G or 25G speeds (depending on the model of the APIC server) when connected to leaf switch host interfaces. |
| September 17, 2019 | 3.2(4d): In the Open Bugs section, added bug CSCuu17314, CSCve84297, and CSCvg70246. |
| September 10, 2019 | In the Known Behaviors section, added the following bullet:<br>■ When there are silent hosts across sites, ARP glean messages might not be forwarded to remote sites if a 1st generation ToR switch (switch models without -EX or -FX in the name) happens to be in the transit path and the VRF is deployed on that ToR switch, the switch does not forward the ARP glean packet back into the fabric to reach the remote site. This issue is specific to 1st generation transit ToR switches and does not affect 2nd generation ToR switches (switch models with -EX or -FX in the name). This issue breaks the capability of discovering silent hosts. |



Cisco Confidential

| Date | Description |
|---|---|
| August 14, 2019 | 3.2(4e): In the Open Bugs section, added bugs CSCvp38627 and CSCvp82252. |
| July 17, 2019 | 3.2(4d): In the Open Bugs section, added bug CSCvq39922. |
| July 16, 2019 | 3.2(4e): In the Open Bugs section, added bug CSCvn64048. |
| July 11, 2019 | 3.2(4d): In the Open Bugs section, added bug CSCvj89771. |
| April 3, 2019 | In the Miscellaneous Guidelines section, added mention that connectivity filters are deprecated. |
| March 25, 2019 | In the Miscellaneous Compatibility Information section, added:<br>— 4.0(2f) CIMC HUU ISO (recommended) for UCS C220/C240 M4<br>— 3.0(4j) CIMC HUU ISO (recommended) for UCS C220/C240 M3 |
| March 19, 2019 | In the New Software Features section, for the SSD over-provisioning feature, changed:<br>"If you do not perform SSD over-provisioning on Cisco N9K-C9364C and N9K-C9336C-FX2 spine switches..."<br>To:<br>"If you do not perform SSD over-provisioning on Cisco N9K-C9364C and N9K-C9336C-FX2 switches..." |
| January 23, 2019 | In Miscellaneous Guidelines section, added the following text:<br>If you upgraded from a release prior to the 3.2(1) release and you had any apps installed prior to the upgrade, the apps will no longer work. To use the apps again, you must uninstall and reinstall them. |
| December 20, 2018 | 3.2(4e): Release 3.2(4e) became available. Added the resolved bugs for this release. |
| November 21, 2018 | 3.2(4d): In the Open Bugs section, added bug CSCvn15374. |
| November 15, 2018 | 3.2(4d): Release 3.2(4d) became available. |



Cisco Confidential

# Contents

This document includes the following sections:


- New and Changed Information
- Upgrade and Downgrade Information
- Bugs
- Compatibility Information
- Usage Guidelines
- Related Documentation


# New and Changed Information


### CONTENTS

### NEW AND CHANGED INFORMATION

**New Software Features**

**New Hardware Features**

**Changes in Behavior**

### UPGRADE AND DOWNGRADE INFORMATION

### BUGS

**Open Bugs**

**Resolved Bugs**

**Known Behaviors**

### COMPATIBILITY INFORMATION

**Virtualization Compatibility Information**

**Hardware Compatibility Information**

**Adaptive Security Appliance (ASA) Compatibility Information**

**Miscellaneous Compatibility Information**

## USAGE GUIDELINES

**Virtualization Compatibility Guidelines**

**GUI Guidelines**

**CLI Guidelines**

**Layer 2 and Layer 3 Configuration Guidelines**

**IP Address Guidelines**

**Miscellaneous Guidelines**

## RELATED DOCUMENTATION

**New Documentation**

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

## CONTENTS

## NEW AND CHANGED INFORMATION

**New Software Features**

**New Hardware Features**

**Changes in Behavior**

## UPGRADE AND DOWNGRADE INFORMATION

## BUGS

**Open Bugs**

**Resolved Bugs**

**Known Behaviors**

## COMPATIBILITY INFORMATION

**Virtualization Compatibility Information**

**Hardware Compatibility Information**

**Adaptive Security Appliance (ASA) Compatibility Information**

**Miscellaneous Compatibility Information**

## USAGE GUIDELINES

**Virtualization Compatibility Guidelines**

**GUI Guidelines**

**CLI Guidelines**

**Layer 2 and Layer 3 Configuration Guidelines**

**IP Address Guidelines**

**Miscellaneous Guidelines**

## RELATED DOCUMENTATION

**New Documentation**

- New Software Features
- New Hardware

# New Software Features

The following table lists the new software features in this release:

Table 2 New Software Features, Guidelines, and Restrictions

| Feature | Description | Guidelines and Restrictions |
|---|---|---|
| EIGRP authentication | You can now use the EIGRP protocol for authentication. EIGRP authentication uses route-map's keychain infrastructure for MD5 authentication.<br><br>For more information, see the *Cisco APIC Security Configuration Guide*. | Only MD5 Authentication is supported.<br><br>When there is authentication mismatch between two EIGRP peers, then the neighborship flaps. |
| IP address-based filtering on spine switches | You can now use IP address-based or subnet-based filtering on Cisco N9K-9348GC-FXP, N9K-9348GC-8U-FXP, N9K-93108TC-FX, and N9K-93180YC-FX switches and N9K-X9736C-FX line cards. Prior to this release, the | Spine switches do not support VRF instance filtering, so any rules posted with the VRF instance filter |



Cisco Confidential

| Feature | Description | Guidelines and Restrictions |
|---|---|---|
| | spine switch always exported all traffic flows in the flow table. The ACL programming for each rule remains the same as it was in previous releases. | will be programmed without the VRF instance key in the ACL.<br><br>You cannot use EX line cards with this feature. |
| SSD over-provisioning | Over-provisioning on a flash-based SSD improves SSD performance and lifetime endurance.<br><br>Using Cisco APIC, SSD over-provisioning can be applied to a switch by following the action as described in the fault that was raised.<br><br>SSD over-provisioning is applied during a switch's boot sequence. SSD over-provisioning might take up to an hour per spine switch to complete, which includes reformating and repartitioning the SSD. This is a disruptive process that will result in all switch data on the SSD being deleted.<br><br>After the switch is discovered by the fabric, the Cisco APIC pushes the policies onto the switch. | If you do not perform SSD over-provisioning on Cisco N9K-C9364C and N9K-C9336C-FX2 switches, Cisco APIC raises fault F2972. SSD over-provisioning is applied automatically during the switch boot process after you respond to the fault. SSD over-provisioning might take up to an hour per spine switch to complete. After the switch reloads, you do not need to take any other action regarding the fault. |

## New Hardware Features

For new hardware features, see the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 13.2(4)* 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

For the changes in behavior, see the Cisco ACI Releases Changes in Behavior document.

# Upgrade and Downgrade Information

For upgrade and downgrade considerations for the Cisco APIC, see the Cisco APIC documentation site 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

See the "Upgrading and Downgrading the Cisco APIC and Switch Software" section of the *Cisco APIC Installation, Upgrade, and Downgrade Guide*.



Cisco Confidential

# 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 3.2(4) releases in which the bug exists. A bug might also exist in releases other than the 3.2(4) releases.

Table 3 Open Bugs in This Release

| Bug ID | Description | Exists in |
|---|---|---|
| CSCvn64048 | The policymgr process in the APIC resets and results in a core file. Configurations can be missed if the core file is generated during a configuration import or during configuration steps. | 3.2(4e) and later |
| CSCvp38627 | Some tenants stop having updates to their state pushed to the APIC. The aim-aid logs have messages similar to the following example:<br><br>An unexpected error has occurred while reconciling tenant tn-prj_...: long int too large to convert to float | 3.2(4e) and later |
| CSCvp82252 | While modifying the host route of OpenStack, the following subnet trace is generated:<br><br>Response :<br>{<br>"NeutronError": {<br>"message": "Request Failed: internal server error while processing your request.",<br>"type": "HTTPInternalServerError",<br>"detail": ""<br>}<br>} | 3.2(4e) and later |
| CSCvp95407 | Access-control headers are not present in invalid requests. | 3.2(4e) and later |
| CSCvq63415 | Disabling dataplane learning is only required to support a policy-based redirect (PBR) use case on pre-"EX" leaf switches. There are few other reasons otherwise this feature should be disabled. There currently is no confirmation/warning of the potential impact that can be caused by disabling dataplane learning. | 3.2(4e) and later |



Cisco Confidential

| Bug ID | Description | Exists in |
|---|---|---|
| CSCvs10395 | Leaf switch downlinks all go down at one time due to FabricTrack. | 3.2(4e) and later |
| CSCvs88359 | This issue has the following symptoms:<br>1. The SSD of a switch fails in less than two years and needs replacement<br>2. The /mnt/pss/ssd_log_amp.log file shows daily P/E cycles that increase by 10+ each day.<br>The following fault is raised on the switch: "F3525: High SSD usage observed. Please check switch activity and contact Cisco Technical Support about high SSD usage." | 3.2(4e) and later |
| CSCvt37066 | When migrating an EPG from one VRF table to a new VRF table, and the EPG keeps the contract relation with other EPGs in the original VRF table. Some bridge domain subnets in the original VRF table get leaked to the new VRF table due to the contract relation, even though the contract does not have the global scope and the bridge domain subnet is not configured as shared between VRF tables. The leaked static route is not deleted even if the contract relation is removed. | 3.2(4e) and later |
| CSCuu17314 | CDP is not enabled on the management interfaces for the leaf switches and spine switches. | 3.2(4d) and later |
| CSCvd43548 | The stats for a given leaf switch rule cannot be viewed if a rule is double-clicked. | 3.2(4d) and later |
| 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. | 3.2(4d) 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. | 3.2(4d) 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.<br>Original :<br>Limit IP Learning To Subnet: [check box]<br>Suggestion :<br>Limit Local IP Learning To BD/EPG Subnet(s): [check box] | 3.2(4d) and later |
| CSCvf70411 | A route will be advertised, but will not contain the tag value that is set from the VRF route tag policy. | 3.2(4d) and later |
| CSCvg00627 | A tenant's flows/packets information cannot be exported. | 3.2(4d) and later |



Cisco Confidential

| Bug ID | Description | Exists in |
|---|---|---|
| CSCvg35344 | 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. | 3.2(4d) and later |
| CSCvg70246 | When configuring an L3Out under a user tenant that is associated with a VRF instance that is under the common tenant, a customized BGP timer policy that is attached to the VRF instance is not applied to the L3Out (BGP peer) in the user tenant. | 3.2(4d) and later |
| CSCvg81020 | For strict security requirements, customers require custom certificates that have RSA key lengths of 3072 and 4096. | 3.2(4d) and later |
| CSCvh52046 | This is an enhancement to allow for text-based banners for the Cisco APIC GUI login screen. | 3.2(4d) and later |
| CSCvh54578 | For a client (browser or ssh client) that is using IPv6, the Cisco APIC aaaSessionLR audit log shows "0.0.0.0" or some bogus value. | 3.2(4d) and later |
| CSCvh59843 | Enabling Multicast under the VRF on one or more bridge domains is difficult due to how the drop-down menu is designed. This is an enhancement request to make the drop-down menu searchable. | 3.2(4d) and later |
| CSCvi20535 | When a VRF table is configured to receive leaked external routes from multiple VRF tables, the Shared Route Control scope to specify the external routes to leak will be applied to all VRF tables. This results in an unintended external route leaking. This is an enhancement to ensure the Shared Route Control scope in each VRF table should be used to leak external routes only from the given VRF table. | 3.2(4d) 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. | 3.2(4d) and later |
| CSCvi80543 | This is an enhancement that allows failover ordering, categorizing uplinks as active or standby, and categorizing unused uplinks for each EPG in VMware domains from the APIC. | 3.2(4d) and later |
| CSCvi82903 | When authenticating with the Cisco APIC using ISE (TACACS), all logins over 31 characters fail. | 3.2(4d) and later |
| CSCvi95657 | On modifying a service parameter, the Cisco APIC sends 2 posts to the backend. The first post deletes all of the folders and parameters. The second post adds all of the remaining modified folders and parameters to the backend. These 2 posts will disrupt the running traffic. | 3.2(4d) and later |
| CSCvj04166 | The remote leaf TEP pool cannot be deleted after decommissioning the remote leaf and deleting the remote leaf vPC configuration. | 3.2(4d) and later |



Cisco Confidential

| Bug ID | Description | Exists in |
|---|---|---|
| CSCvj09453 | The actrlRule is has the wrong destination. | 3.2(4d) and later |
| CSCvj56726 | The connectivity filter configuration of an access policy group is deprecated and should be removed from GUI. | 3.2(4d) and later |
| CSCvk04072 | There is no record of who acknowledged a fault in the Cisco APIC, nor when the acknowledgement occurred. | 3.2(4d) and later |
| CSCvk12786 | Apps fail to install/uninstall/run when the cluster is not healthy and nodes are powered down/unreachable without being decommissioned. | 3.2(4d) and later |
| CSCvk18014 | The action named 'Launch SSH' is disabled when a user with read-only access logs into the Cisco APIC. | 3.2(4d) and later |
| CSCvm56946 | Support for local user (admin) maximum tries and login delay configuration. | 3.2(4d) and later |
| CSCvm63668 | A single user can send queries to overload the API gateway. | 3.2(4d) and later |
| CSCvm89559 | The svc_ifc_policye process consumes 100% of the CPU cycles. The following messages are observed in svc_ifc_policymgr.bin.log:<br><br>8816\|\|18-10-12 11:04:19.101\|\|route_control\|\|ERROR\|\|co=doer:255:127:0xff00000000c42ad2:11\|\|Route entry order exceeded max for st10960-2424833-any-2293761-33141-shared-svc-int Order:18846Max:17801\|\|<br><br>../dme/svc/policyelem/src/gen/ifc/beh/imp/./rtctrl/RouteMapUtils.cc\|\|239:q | 3.2(4d) and later |
| CSCvn00576 | An SHA2 CSR for the ACI HTTPS certificate cannot be configured in the APIC GUI. | 3.2(4d) and later |
| CSCvp26694 | A leaf switch gets upgraded when a previously-configured maintenance policy is triggered. | 3.2(4d) and later |
| CSCvp62048 | New port groups in VMware vCenter may be delayed when pushed from the Cisco APIC. | 3.2(4d) and later |



Cisco Confidential

| Bug ID | Description | Exists in |
|---|---|---|
| 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.<br><br>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.<br><br>Cisco has released software updates that address this vulnerability. There are workarounds that address this vulnerability.<br><br>This advisory is available at the following link:<br><br>Cisco Nexus 9000 Series Fabric Switches ACI Mode Fabric Infrastructure VLAN Unauthorized Access Vulnerability | 3.2(4d) and later |
| CSCvp72283 | An APIC running the 3.0(1k) release sometimes enters the "Data Layer Partially Diverged" state. The acidiag rvread command shows the following output for the service 10 (observer):<br><br>Non optimal leader for shards :10:1,10:3,10:4,10:6,10:7,10:9,10:10,10:12,10:13,10:15,10:16,10:18,10:19,10:21,10:22,10:24,10:25,<br><br>10:27,10:28,10:30,10:31 | 3.2(4d) and later |
| CSCvp79454 | Syslog is not sent upon any changes in the fabric. Events are properly generated, but no Syslog is sent out of the oobmgmt ports of any of the APICs. | 3.2(4d) and later |
| CSCvp94085 | The APIC Licensemgr generates a core file while parsing an XML response. | 3.2(4d) and later |
| CSCvp99430 | The troubleshooting wizard is unresponsive on the APIC. | 3.2(4d) and later |
| CSCvq04110 | The APIC API and CLI allow for the configuration of multiple native VLANs on the same interface. When a leaf switch port has more than one native VLAN configured (which is a misconfiguration) in place, and a user tries to configure a native VLAN encap on another port on the same leaf switch, a validation error is thrown that indicates an issue with the misconfigured port. This error will occur even if the current target port has no misconfigurations in place. | 3.2(4d) and later |
| CSCvq31358 | "show external-l3 interfaces node <id> detail" will display "missing" for both "Oper Interface" and "Oper IP", even though the L3Out is functioning as expected. | 3.2(4d) and later |



Cisco Confidential

| Bug ID | Description | Exists in |
|---|---|---|
| CSCvq39922 | Specific operating system and browser version combinations cannot be used to log in to the APIC GUI.<br><br>Some browsers that are known to have this issue include (but might not be limited to) Google Chrome version 75.0.3770.90 and Apple Safari version 12.0.3 (13606.4.5.3.1). | 3.2(4d) 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. | 3.2(4d) and later |
| CSCvq57942 | In a RedHat OpenStack platform deployment running the Cisco ACI Unified Neutron ML2 Plugin and with the CompHosts running OVS in VLAN mode, when toggling the resolution immediacy on the EPG<->VMM domain association (fvRsDomAtt.resImedcy) from Pre-Provision to On-Demand, the encap VLANs (vlanCktEp mo's) are NOT programmed on the leaf switches.<br><br>This problem surfaces sporadically, meaning that it might take several resImedcy toggles between PreProv and OnDemand to reproduce the issue. | 3.2(4d) and later |
| CSCvq58304 | VMM inventory-related faults are raised for VMware vCenter inventory, which is not managed by the VMM. | 3.2(4d) and later |
| CSCvq63491 | When using Open vSwitch, which is used as part of ACI integration with Kubernetes or Red Hat Open Shift, there are some instances when memory consumption of the Open vSwitch grows over a time. | 3.2(4d) and later |
| 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. | 3.2(4d) and later |
| CSCvr30815 | vmmPLInf objects are created with epgKey's and DN's that have truncated EPG names ( truncated at "."). | 3.2(4d) and later |
| CSCvr41750 | Policies may take a long time (over 10 minutes) to get programmed on the leaf switches. In addition, the APIC pulls inventory from the VMware vCenter repeatedly, instead of following the usual 24 hour interval. | 3.2(4d) 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. | 3.2(4d) and later |
| CSCvr85515 | When trying to track an AVE endpoint IP address, running the "show endpoint ip x.x.x.x" command in the Cisco APIC CLI to see the IP address and checking the IP address on the EP endpoint in the GUI shows incorrect or multiple VPC names. | 3.2(4d) and later |
| CSCvr94614 | There is a minor memory leak in svc_ifc_policydist when performing various tenant configuration removals and additions. | 3.2(4d) and later |



Cisco Confidential

| Bug ID | Description | Exists in |
|---|---|---|
| CSCvr96785 | Configuring a static endpoint through the Cisco APIC CLI fails with the following error:<br>Error: Unable to process the query, result dataset is too big<br>Command execution failed. | 3.2(4d) and later |
| CSCvs29366 | For a DVS with a controller, if another controller is created in that DVS using the same host name, the following fault gets generated: "hostname or IP address conflicts same controller creating controller with same name DVS". | 3.2(4d) and later |
| CSCvs47757 | The plgnhandler process crashes on the Cisco APIC, which causes the cluster to enter a data layer partially diverged state. | 3.2(4d) and later |
| CSCvs66244 | The CLI command "show interface x/x switchport" shows VLANs configured and allowed through a port. However, when going to the GUI under Fabric > Inventory > node_name > Interfaces > Physical Interfaces > Interface x/x > VLANs, the VLANs do not show. | 3.2(4d) and later |
| CSCvs78996 | The policy manager (PM) may crash when use testapi to delete MO from policymgr db. | 3.2(4d) and later |
| CSCvt07565 | The eventmgr database size may grow to be very large (up to 7GB). With that size, the Cisco APIC upgrade will take 1 hour for the Cisco APIC node that contains the eventmgr database.<br>In rare cases, this could lead to a failed upgrade process, as it times out while working on the large database file of the specified controller. | 3.2(4d) and later |
| CSCvt40736 | The login history of local users is not updated in Admin > AAA > Users > (double click on local user) Operational > Session. | 3.2(4d) and later |
| CSCvu01452 | The MD5 checksum for the downloaded Cisco APIC images is not verified before adding it to the image repository. | 3.2(4d) and later |
| CSCvu21530 | Protocol information is not shown in the GUI when a VRF table from the common tenant is being used in any user tenant. | 3.2(4d) and later |



Cisco Confidential

| Bug ID | Description | Exists in |
|---|---|---|
| CSCvu39569 | The following error is encountered when accessing the Infrastructure page in the ACI vCenter plugin after inputting vCenter credentials.<br><br>"The Automation SDK is not authenticated"<br><br>VMware vCenter plug-in is installed using powerCLI. The following log entry is also seen in vsphere_client_virgo.log on the VMware vCenter:<br><br>/var/log/vmware/vsphere-client/log/vsphere_client_virgo.log<br><br>[ERROR] http-bio-9090-exec-3314 com.cisco.aciPluginServices.core.Operation<br><br>sun.security.validator.ValidatorException: PKIX path validation failed:<br><br>java.security.cert.CertPathValidatorException: signature check failed | 3.2(4d) and later |
| CSCvu62465 | For an EPG containing a static leaf node configuration, the Cisco APIC GUI returns the following error when clicking the health of Fabric Location:<br><br>Invalid DN topology/pod-X/node-Y/local/svc-policyelem-id-0/ObservedEthIf, wrong rn prefix ObservedEthIf at position 63 | 3.2(4d) and later |
| CSCvv62861 | A leaf switch reloads due to an out-of-memory condition after changing the contract scope to global. | 3.2(4d) and later |
| CSCvw33061 | Traffic loss is observed from multiple endpoints deployed on two different vPC leaf switches. | 3.2(4d) and later |
| CSCvj89771 | The Virtual Machine Manager (vmmmgr) process crashes and generates a core file. | 3.2(4d) |
| 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:<br><br>appliance_director\|\|DBG4\|\|...\|\|Lost heartbeat from appliance id= ...<br><br>appliance_director\|\|DBG4\|\|...\|\|Appliance has become unavailable id= ...<br><br>On the switches, each process (such as policy-element) see rapidly changing leader elections and minority states:<br><br>adrs_rv\|\|DBG4\|\|\|Updated leader election on replica=(6,26,1) | 3.2(4d) |

## 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.



Cisco Confidential

Table 4 Resolved Bugs in This Release

| Bug ID | Description | Fixed in |
|---|---|---|
| CSCvm16596 | Sometime during the decommissioning of a leaf switch, the topomgr process of Cisco APIC may crash. | 3.2(4e) |
| CSCvn09842 | When upgrading the Cisco APICs, constant heartbeat loss is seen, causing the Cisco APICs to lose connectivity between one another. On the Cisco APIC appliance_director logs, the following messages are seen several hundred times during the upgrade:<br>appliance_director\|\|DBG4\|\|...\|\|Lost heartbeat from appliance id= ...<br>appliance_director\|\|DBG4\|\|...\|\|Appliance has become unavailable id= ...<br>On the switches, each process (such as policy-element) sees rapidly-changing leader elections and minority states:<br>adrs_rv\|\|DBG4\|\|\|\|Updated leader election on replica=(6,26,1) | 3.2(4e) |
| CSCvn15376 | When upgrading the Cisco APICs, constant heartbeat loss is seen, causing the Cisco APICs to lose connectivity between one another. On the Cisco APIC appliance_director logs, the following messages are seen several hundred times during the upgrade:<br>appliance_director\|\|DBG4\|\|...\|\|Lost heartbeat from appliance id= ...<br>appliance_director\|\|DBG4\|\|...\|\|Appliance has become unavailable id= ...<br>On the switches, each process (such as policy-element) sees rapidly-changing leader elections and minority states:<br>adrs_rv\|\|DBG4\|\|\|\|Updated leader election on replica=(6,26,1) | 3.2(4e) |
| CSCvn15769 | There are recurring crashes and core dumps on different Cisco APICs (which are VMM domain shard leaders), as well as high CPU utilization (around 200% so to 2x maxed out CPU cores) for the VMMMGr process, as well as multiple inv sync issues.<br>These issues are preventing the VMMMGr process from processing any operational/configuration changes that are made on the RHVs. | 3.2(4e) |
| CSCvn17432 | A Cisco ACI Virtual Edge VM is not being powered on after the host exits maintenance mode. | 3.2(4e) |
| CSCvn30618 | On all 3 Cisco APICs in the cluster, the data layer is partially diverged and policydist dumps cores after the Cisco APICs are upgraded. | 3.2(4e) |
| CSCvn41995 | The Cisco APIC cluster is partially diverged after an IPN flap. After restarting mgmt on APIC 1, the cluster came back fully fit, but the shard in question still was showing as having a non-optimal leader. After this issue occurs, there are intermittent issues with configuring objects in the fabric. | 3.2(4e) |
| CSCvn46423 | After upgrading to a release greater than 3.2, existing endpoints in OpenStack VMMs may no longer be able to send/receive traffic. The required EPGs will not be present on the leaf switch. | 3.2(4e) |
| CSCvn46473 | fvEpDefRef objects may still get created in the MIT of the leaf switch for OpenStack VMMs, which may unnecessarily hold EPGs on a leaf switch. | 3.2(4e) |



Cisco Confidential

| Bug ID | Description | Fixed in |
|---|---|---|
| CSCvn57629 | Unable to show the configuration of an access leaf IPG from the Cisco APIC GUI under Fabric -> Access Policies -> Interfaces -> Leaf Interfaces -> Policy Groups. | 3.2(4e) |
| CSCvb51187 | The following fault F0467 is raised on an L3Out that is configured only for static routes when other OSPF L3Outs exist that share the same VRF instance. While the fault is present, configurations made to the L3Out are not deployed to the switches. | 3.2(4d) |
| CSCvg48627 | The Cisco APIC GUI allows users to configure an Out-of-Band Contract with a Directive of Logging when this is not supported, which can lead to the following programming fault being generated:<br><br>actrl-provisioning-failed rule failed due to software programming error | 3.2(4d) |
| CSCvi59444 | The stale fault delegate is raised when a configured syslog/callhome server is not reachable. It does not clear after configuring a successful syslog/callhome policy or after the deletion of non-reachable server policy. | 3.2(4d) |
| CSCvj23488 | User is allowed to configure a BD to use the "oob" VRF instance. | 3.2(4d) |
| CSCvk38296 | When deploying a single node PBR with a one-arm load balancer and without SNAT, the PBR datapath does not work as expected. | 3.2(4d) |
| CSCvm06854 | When looking at a VMM domain in the Cisco APIC, you may see faults saying that the last inventory pull returned partial. | 3.2(4d) |
| CSCvm09583 | CPU utilization on the leaf switch that is attached to the OpenStack compute/controller has high CPU utilization when the number of endpoints increases. | 3.2(4d) |
| CSCvm11162 | F1527, F1528, or F1529 faults for the /data/log folder being at or over 75% appear around midnight local time for a minute or two before clearing. | 3.2(4d) |
| CSCvm11332 | The Transport Gateway/Smart Software Manager Satellite product cannot be reregistered using the Cisco APIC GUI because the option "Reregister product if already registered" button is missing. | 3.2(4d) |
| CSCvm12554 | When an L3Out and application EPG are configured in a contract preferred group-enabled VRF instance, and the application EPG is deployed on a vPC or non-vPC, then only one leaf switch in the VPC has the prefix entry for the L3Out, or the ingress leaf switch (in the non-vPC case) does not have the prefix entry for the L3Out.<br><br>In the vPC case, one leaf switch does not have the entry and drops the traffic.<br><br>In the non-vPC case, the ingress leaf switch does not have the entry and drops the traffic. | 3.2(4d) |
| CSCvm15454 | The product Cisco Application Policy Infrastructure Controller (APIC) includes a version of the Linux kernel that is affected by the IP Fragment Reassembly Denial of Service Vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:<br><br>CVE-2018-5391<br><br>Cisco has confirmed that this product is impacted. | 3.2(4d) |



Cisco Confidential

| Bug ID | Description | Fixed in |
|---|---|---|
| CSCvm35382 | Unable to log in and the following message is received:<br><br>REST Endpoint user authorization datastore is not initialized - Check Fabric Membership Status of this fabric node | 3.2(4d) |
| CSCvm37174 | After a clean reload of a leaf switch, VMM integrated VLANs may not be pushed to some switches. You can run the "show vlan extended \| grep vlan-X" replacing X with the encap VLAN to see if the VLAN is deployed to the switch.<br><br>Basically EPG is not deployed on the link between leaf switch and blade switch, that got added later. | 3.2(4d) |
| CSCvm43044 | Bridge domain subnets from the consumer VRF instance do not get leaked into the provider VRF instance if the contract is consumed first and the scope for the bridge domain subnet is changed to shared at a later time. | 3.2(4d) |
| CSCvm45121 | When configuring a sub-interface on a border leaf switch, sub-interface fails VRF validation due to mismatching interface types with parent interface. | 3.2(4d) |
| CSCvm46349 | on_demand techsupport is not collected from leaf switches and spine switches, and the following error message is observed:<br><br>Failed to open file=/var/log/dme/oldlog/tmp1536309556861/techsup_1536309556861 error=No child processes; return value=32560 | 3.2(4d) |
| CSCvm49815 | The Cisco APIC GUI gets stuck when expanding a tab in the navigation pane if that pane contains a large amount of objects. | 3.2(4d) |
| CSCvm56674 | After a leaf switch is upgraded or clean reloaded, newly created EPGs are not correctly deployed on the leaf switch. VMM inventory objects for the newly created EPGs are missing on the leaf switch. | 3.2(4d) |
| CSCvm58089 | When an IPv6 address is configured in the Cisco APIC GUI under Tenant MGMT > Node Management Addresses > Static Node Management Addresses, and the IPv6 address is given a prefix length such as /120 , /121 , or /122 , the address is programmed as /64 when checked using the ifconfig command on the Cisco APIC. | 3.2(4d) |
| CSCvm58194 | A VM experiences traffic loss for a few seconds after a vMotion completion event. | 3.2(4d) |
| CSCvm60100 | When attempting to deploy Cisco ACI Virtual Edge using the Cisco ACI plugin for VMware vCenter, the operation fails with "Failed to deploy OVF package" and "An error occurring during the deployment of the OVF from the Content Library". | 3.2(4d) |
| CSCvm70003 | Traffic from GOLF to EPG is dropping when the VRF instance is in enforced mode. Zoning rules are programmed properly. You see security drops and elam shows that source EPG ID is 0x0. | 3.2(4d) |
| CSCvm76293 | The Cisco APIC stops displaying VM stats after some time. | 3.2(4d) |
| CSCvm79579 | A monitoring policy cannot be created to squelch (or suppress) the "IP detached" event, because the GUI does not display the event code. | 3.2(4d) |
| CSCvm80684 | Some unnecessary health score change notifications sent to GUI might affect GUI performance. | 3.2(4d) |



Cisco Confidential

| Bug ID | Description | Fixed in |
|---|---|---|
| CSCvm83098 | After launching the Create Attachable Access Entity Profile or Configure Interface Wizard, no content appears to show configuration options. After this is triggered, the wizard will not cancel, requiring the page to be refreshed. | 3.2(4d) |
| CSCvm84779 | A white box in the GUI appears when trying to look at leaf switches that are running an older release. | 3.2(4d) |
| CSCvm84821 | Adding a large piece of information, such as a signed certificate, makes the system go into an inconsistent state. | 3.2(4d) |
| CSCvm87337 | OpenStack VM Layer 3 communications might not work, which impacts floating IP addresses and VMs that are in different EPGs and on different computer nodes. | 3.2(4d) |
| CSCvm96379 | Security group rules are not properly implemented on compute nodes. | 3.2(4d) |
| CSCvm96886 | Some unnecessary health score change notifications sent to GUI might affect GUI performance. | 3.2(4d) |
| CSCvn02543 | When navigating Interface Policy Groups (IPGs) in the Access Policies and the IPG are shown without Pages. If there are a lot of IPGs are configured, the Cisco APIC GUI response is very slow or may give an error "Unable to process the query, result dataset is too big". | 3.2(4d) |
| CSCvn04133 | If a port is associated to a port group and is operational, and a connectivity filter is added to another port group for the same port number, but a different leaf switch, the VLANs on the leaf switch in the first port group get deleted even though the new connectivity filter is added to a different switch and port group, but the same port number. | 3.2(4d) |

## 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 3.2(4) releases in which the known behavior exists. A bug might also exist in releases other than the 3.2(4) releases.

Table 5 Known Behaviors in This 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. | 3.2(4d) and later |
| CSCuo79243 | In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30. | 3.2(4d) and later |
| CSCuo79250 | The node ID policy can be replicated from an old appliance that is decommissioned when it joins a cluster. | 3.2(4d) and later |



Cisco Confidential

| Bug ID | Description | Exists in |
|---|---|---|
| CSCup47703 | The DSCP value specified on an external endpoint group does not take effect on the filter rules on the leaf switch. | 3.2(4d) and later |
| CSCup79002 | The hostname resolution of the syslog server fails on leaf and spine switches over in-band connectivity. | 3.2(4d) and later |
| CSCuq21360 | Following a FEX or switch reload, configured interface tags are no longer configured correctly. | 3.2(4d) and later |
| CSCur39124 | Switches can be downgraded to a 1.0(1) version if the imported configuration consists of a firmware policy with a desired version set to 1.0(1). | 3.2(4d) and later |
| CSCur71082 | If the Cisco APIC is rebooted using the CIMC power reboot, the system enters into fsck due to a corrupted disk. | 3.2(4d) 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. | 3.2(4d) and later |
| CSCut51929 | The traffic destined to a shared service provider endpoint group picks an incorrect class ID (PcTag) and gets dropped. | 3.2(4d) 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. | 3.2(4d) and later |
| CSCuu61998 | Newly added microsegment EPG configurations must be removed before downgrading to a software release that does not support it. | 3.2(4d) and later |
| CSCuu64219 | Downgrading the fabric starting with the leaf switch will cause faults such as policy-deployment-failed with fault code F1371. | 3.2(4d) and later |
| CSCuw81638 | The OpenStack metadata feature cannot be used with Cisco ACI integration with the Juno release (or earlier) of OpenStack due to limitations with both OpenStack and Cisco's ML2 driver. | 3.2(4d) and later |
| CSCva32534 | Creating or deleting a fabricSetupP policy results in an inconsistent state. | 3.2(4d) 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. | 3.2(4d) and later |



Cisco Confidential

| Bug ID | Description | Exists in |
|---|---|---|
| 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. | 3.2(4d) and later |
| CSCva97082 | When downgrading 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. | 3.2(4d) 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. | 3.2(4d) and later |
| CSCvg41711 | In the leaf mode, the command "template route group <group-name> tenant <tenant-name>" fails, declaring that the tenant passed is invalid. | 3.2(4d) and later |
| CSCvg79127 | When First hop security is enabled on a bridge domain, traffic is disrupted. | 3.2(4d) and later |
| CSCvg81856 | Cisco ACI Multi-Site Orchestrator BGP peers are down and a fault is raised for a conflicting rtrId on the fvRtdEpP managed object during L3extOut configuration. | 3.2(4d) and later |
| CSCvh76076 | The PSU SPROM details might not be shown in the CLI upon removal and insertion from the switch. | 3.2(4d) and later |
| CSCvh93612 | If two intra-EPG deny rules are programmed–one with the class-eq-deny priority and one with the class-eq-filter priority–changing the action of the second rule to "deny" causes the second rule to be redundant and have no effect. The traffic still gets denied, as expected. | 3.2(4d) and later |
| CSCvj90385 | With a uniform distribution of EPs and traffic flows, a fabric module in slot 25 sometimes reports far less than 50% of the traffic compared to the traffic on fabric modules in non-FM25 slots. | 3.2(4d) and later |

- 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*.
- With a non-english SCVMM 2012 R2 or SCVMM 2016 setup and where the virtual machine names are specified in non-english characters, if the host is removed and re-added to the host group, the GUID for all the virtual machines under that host changes. Therefore, if a user has created a micro segmentation endpoint group using "VM name" attribute specifying the GUID of respective virtual machine, then that micro segmentation endpoint group will not work if the host (hosting the virtual machines) is removed and re-added to the host group, as the GUID for all the virtual machines would have changed. This does not happen if the virtual name has name specified in all english characters.
- A query of a configurable policy that does not have a subscription goes to the policy distributor. However, a query of a configurable policy that has a subscription goes to the policy manager. As a result, if the policy propagation from the policy distributor to the policy manager takes a prolonged amount of time, then in such



Cisco Confidential

cases the query with the subscription might not return the policy simply because it has not reached policy manager yet.

- When there are silent hosts across sites, ARP glean messages might not be forwarded to remote sites if a 1st generation ToR switch (switch models without -EX or -FX in the name) happens to be in the transit path and the VRF is deployed on that ToR switch, the switch does not forward the ARP glean packet back into the fabric to reach the remote site. This issue is specific to 1st generation transit ToR switches and does not affect 2nd generation ToR switches (switch models with -EX or -FX in the name). This issue breaks the capability of discovering silent hosts.

# Compatibility Information

The following sections list compatibility information for the Cisco APIC software.

## Virtualization Compatibility Information

This section lists virtualization compatibility information for the Cisco APIC software.

- For a table that shows the supported virtualization products, see the ACI Virtualization Compatibility Matrix at the following URL:

  https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/aci/virtualization/matrix/virtmatrix.html

- This release supports VMM Integration and VMware Distributed Virtual Switch (DVS) 6.5 and 6.7. 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 3.2(4)* 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

- For information about Cisco APIC compatibility with Cisco 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

- If you use Microsoft vSwitch and want to downgrade to Cisco APIC Release 2.3(1) from a later release, you first must delete any microsegment EPGs configured with the Match All filter.

## Hardware 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) |



Cisco Confidential

| | |
|---|---|
| APIC-M2 | Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1000 edge ports) |

The following list includes additional hardware compatibility information:

- For the supported hardware, see the *Cisco NX-OS Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches, Release 13.2(4)* at the following location:

  https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.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 Cisco ACI leaf switches
  - Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the 10G ports on all other Cisco ACI leaf switches.

    Note: A fabric uplink port cannot be used as a FEX fabric port.
- Connecting the Cisco APIC (the controller cluster) to the Cisco ACI fabric requires a 10G interface on the Cisco ACI leaf switch. You cannot connect the Cisco APIC directly to the Cisco N9332PQ ACI leaf switch, unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the Cisco N9332PQ switch auto-negotiate to 10G without requiring any manual configuration.
- The Cisco N9K-X9736C-FX (ports 29 to 36) and Cisco N9K-C9364C-FX (ports 49-64) switches do not support 1G SFPs with QSA.
- Cisco N9K-C9508-FM-E2 fabric modules must be physically removed before downgrading to releases earlier than Cisco APIC 3.0(1).
- The Cisco N9K-C9508-FM-E2 and N9K-X9736C-FX locator LED enable/disable feature is supported in the GUI and not supported in the Cisco ACI NX-OS Switch CLI.
- Contracts using matchDscp filters are only supported on switches with "EX" on the end of the switch name. For example, N9K-93108TC-EX.
- N9K-C9508-FM-E2 and N9K-C9508-FM-E fabric modules in the mixed mode configuration are not supported on the same spine switch.
- The N9K-C9348GC-FXP switch does not read SPROM information if the PSU is in a shut state. You might see an empty string in the Cisco APIC output.
- When the fabric node switch (spine or leaf) is out-of-fabric, the environmental sensor values, such as Current Temperature, Power Draw, and Power Consumption, might be reported as "N/A." A status might be reported as "Normal" even when the Current Temperature is "N/A."

## Adaptive Security Appliance (ASA) Compatibility Information

This section lists ASA compatibility information for the Cisco APIC software.

- This release supports Adaptive Security Appliance (ASA) device package version 1.2.5.5 or later.



Cisco Confidential

- If you are running a Cisco Adaptive Security Virtual Appliance (ASA) version that is prior to version 9.3(2), you must configure SSL encryption as follows:

```
(config)# ssl encryption aes128-sha1
```

## Miscellaneous Compatibility Information

This section lists miscellaneous compatibility information for the Cisco APIC software.

- This release supports the following software:
  - Cisco NX-OS Release 13.2(4)
  - Cisco AVS, Release 5.2(1)SV3(3.11)

    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 latest recommended CIMC releases are as follows:
  - 4.1(2m) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
  - 4.1(2k) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)
  - 4.1(2g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)
  - 4.1(2b) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)
  - 4.1(1g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3)
  - 4.1(1f) CIMC HUU ISO for UCS C220 M4 (APIC-L2/M2) (deferred release)
  - 4.1(1d) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3)
  - 4.1(1c) CIMC HUU ISO for UCS C220 M4 (APIC-L2/M2)
  - 4.0(4e) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3)
  - 4.0(2g) CIMC HUU ISO for UCS C220/C240 M4 and M5 (APIC-L2/M2 and APIC-L3/M3)
  - 4.0(1a) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3)
  - 3.0(4l) CIMC HUU ISO (recommended) for UCS C220/C240 M3 (APIC-L1/M1)
  - 3.0(4d) CIMC HUU ISO for UCS C220/C240 M3 and M4 (APIC-L1/M1 and APIC-L2/M2)
  - 3.0(3f) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)
  - 3.0(3e) CIMC HUU ISO for UCS C220/C240 M3 (APIC-L1/M1)
  - 2.0(13i) CIMC HUU ISO



Cisco Confidential

- 2.0(9c) CIMC HUU ISO
- 2.0(3i) CIMC HUU ISO

- 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

- A known issue exists with the Safari browser and unsigned certificates, which applies when connecting to the Cisco APIC GUI. For more information, see the *Cisco APIC Getting Started Guide*.
- For compatibility with OpenStack and Kubernetes distributions, see the *Cisco Application Policy Infrastructure Controller OpenStack and Container Plugins, Release 3.2(4), Release Notes.*

# Usage Guidelines

The following sections list usage guidelines for the Cisco APIC software.

## Virtualization Compatibility Guidelines

This section lists virtualization-related usage guidelines for the Cisco APIC software.

- 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 are upgrading VMware vCenter 6.0 to vCenter 6.7, 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.

  The *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. Enter any changes in the Cisco APIC configuration again after restarting VMware vCenter.
- If the communication between the Cisco APIC and VMware vCenter is impaired, some functionality is adversely affected. The Cisco APIC relies on the pulling of inventory information, updating VDS configuration, and receiving event notifications from the VMware vCenter for performing certain operations.
- After you migrate VMs using a cross-data center VMware vMotion in the same VMware vCenter, you might find a stale VM entry under the source DVS. This stale entry can cause problems, such as host removal failure. The workaround for this problem is to enable "Start monitoring port state" on the vNetwork DVS. See the KB topic "Refreshing port state information for a vNetwork Distributed Virtual Switch" on the VMware Web site for instructions.
- 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:



Cisco Confidential

  - Generation 1–Cisco Nexus 9200 and 9300 platform switches without "EX" on the end of the switch name; for example, Cisco Nexus 93120TX.
  - Generation 2–Cisco Nexus 9300-EX and FX platform switches; for example, Cisco Nexus 93108TC-EX.

- The following Red Hat Virtualization (RHV) guidelines apply:
  - We recommend that you use release 4.1.6 or later.
  - Only one controller (compCtrlr) can be associated with a Red Hat Virtualization Manager (RHVM) data center.
  - Deployment immediacy is supported only as pre-provision.
  - IntraEPG isolation, micro EPGs, and IntraEPG contracts are not supported.
  - Using service nodes inside a RHV domain have not been validated.

## GUI Guidelines

This section lists GUI-related usage guidelines for the Cisco APIC software.

- The Cisco APIC GUI includes an online version of the Quick Start Guide that includes video demonstrations.
- To reach the Cisco APIC CLI from the GUI: choose System > Controllers, highlight a controller, right-click, and choose "launch SSH". To get the list of commands, press the escape key twice.
- The Basic GUI mode is deprecated. We do not recommend using Cisco APIC Basic mode for configuration. However, if you want to use Cisco APIC Basic mode, use the following URL:

  *APIC_URL*/indexSimple.html

## CLI Guidelines

This section lists CLI-related usage guidelines for the Cisco APIC software.

- The output from show commands issued in the NX-OS-style CLI are subject to change in future software releases. We do not recommend using the output from the show commands for automation.
- The CLI is supported only for users with administrative login privileges.
- If FIPS is enabled in the Cisco ACI setups, then SHA256 support is mandatory on the SSH Client. Additionally, to have the SHA256 support, the openssh-client must be running version 6.6.1 or higher.

## Layer 2 and Layer 3 Configuration Guidelines

This section lists Layer 2 and Layer 3-related usage guidelines for the Cisco APIC software.

- For Layer 3 external networks created through the API or GUI and updated through the CLI, protocols need to be enabled globally on the external network through the API or GUI, and the node profile for all the participating nodes needs to be added through the API or GUI before doing any further updates through the CLI.
- When configuring two Layer 3 external networks on the same node, the loopbacks need to be configured separately for both Layer 3 networks.



Cisco Confidential

- 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 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 APIC Layer 2 Networking Configuration Guide*.

  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 raises a fault on the EPG stating "invalid path configuration."

- In a multipod fabric, if a spine switch 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.

- 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 Cisco APIC automatically creates a default monitoring policy and enables common observable. You can modify the default policy under tenant common based on the requirements of your fabric.

- The Cisco APIC does not provide IPAM services for tenant workloads.

- Do not mis-configure Control Plane Policing (CoPP) pre-filter entries. CoPP pre-filter entries might impact connectivity to multi-pod configurations, remote leaf switches, and Cisco ACI Multi-Site deployments.

- You cannot use remote leaf switches with Cisco ACI Multi-Site.

## IP Address Guidelines

This section lists IP address-related usage guidelines for the Cisco APIC software.

- For the following services, use a DNS-based hostname 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

- The infrastructure IP address range must not overlap with other IP addresses used in the fabric for in-band and Out-of-band networks.

- 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.

- 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 Cisco ACI fabric, including the leaf switches and spine switches, to the latest Cisco APIC release.

- Cisco ACI does not support a class E address as a VTEP address.



Cisco Confidential

## Miscellaneous Guidelines

This section lists miscellaneous usage guidelines for the Cisco APIC software.

- 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
- In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.
- The power consumption statistics are not shown on leaf node slot 1.
- 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 switch along with the actrl rule, but a vzAny contract does not have an actrl rule. Therefore, the DSCP value cannot be sent.
- The Cisco APICs must have 1 SSD and 2 HDDs, and both RAID volumes must be healthy before upgrading to this release. The Cisco APIC will not boot if the SSD is not installed.
- 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 is 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.
- For a Cisco APIC REST API query of event records, the Cisco APIC system limits the response to a maximum of 500,000 event records. If the response is more than 500,000 events, it returns an error. Use filters to refine your queries. For more information, see *Cisco APIC REST API Configuration Guide*.
- Subject Alternative Names (SANs) contain one or more alternate names and uses any variety of name forms for the entity that is bound by the Certificate Authority (CA) to the certified public key. These alternate names are called "Subject Alternative Names" (SANs). Possible names include:
  - DNS name
  - IP address



Cisco Confidential

- If a node has port profiles deployed on it, some port configurations are not removed if you decommission the node. You must manually delete the configurations after decommissioning the node to cause the ports to return to the default state. To do this, log into the switch, run the setup-clean-config.sh script, wait for the script to complete, then enter the reload command.
- When using the SNMP trap aggregation feature, if you decommission Cisco APICs, the trap forward server will receive redundant traps.
- If you upgraded from a release prior to the 3.2(1) release and you had any apps installed prior to the upgrade, the apps will no longer work. To use the apps again, you must uninstall and reinstall them.
- Connectivity filters are deprecated in this release. Feature deprecation implies no further testing has been performed and that Cisco recommends removing any and all configurations that use this feature. The usage of connectivity filters can result in unexpected access policy resolution, which in some cases will lead to VLANs being removed/reprogrammed on leaf interfaces. You can search for the existence of any connectivity filters by using the moquery command on the APIC:

  ```
  > moquery -c infraConnPortBlk
  > moquery -c infraConnNodeBlk
  > moquery -c infraConnNodeS
  > moquery -c infraConnFexBlk
  > moquery -c infraConnFexS
  ```

- Fabric connectivity ports can operate at 10G or 25G speeds (depending on the model of the APIC server) when connected to leaf switch host interfaces. We recommend connecting two fabric uplinks, each to a separate leaf switch or vPC leaf switch pair.

  For APIC-M3/L3, virtual interface card (VIC) 1445 has four ports (port-1, port-2, port-3, and port-4 from left to right). Port-1 and port-2 make a single pair corresponding to eth2-1 on the APIC server; port-3 and port-4 make another pair corresponding to eth2-2 on the APIC server. Only a single connection is allowed for each pair. For example, you can connect one cable to either port-1 or port-2 and another cable to either port-3 or port-4, but not 2 cables to both ports on the same pair. Connecting 2 cables to both ports on the same pair creates instability in the APIC server. All ports must be configured for the same speed: either 10G or 25G.
- 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.

# 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 list provides links to the release notes and verified scalability documentation:



Cisco Confidential

- Verified Scalability
- Cisco ACI Simulator Release Notes
- Cisco NX-OS Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches
- Cisco Application Policy Infrastructure Controller OpenStack and Container Plugins Release Notes
- Cisco Application Virtual Switch Release Notes

## New Documentation

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

- *Cisco ACI Virtual Edge Configuration Guide, Release 1.2(2)*
- *Cisco ACI Virtual Edge Installation Guide, Release 1.2(2)*
- *Cisco ACI Virtual Edge Release Notes, Release 1.2(2)*
- *Cisco ACI Virtualization Guide, Release 3.2(4)*
- *Cisco APIC NX-OS Style CLI Command Reference, Release 3.2(4)*
- *Cisco Application Virtual Switch Configuration Guide, Release 5.2(1)SV3(3.25)*
- *Cisco Application Virtual Switch Installation Guide, Release 5.2(1)SV3(3.25)*
- *Cisco Application Virtual Switch Release Notes, 5.2(1)SV3(3.25)*



Cisco Confidential

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2018-2022 Cisco Systems, Inc. All rights reserved.