Cisco Application Policy Infrastructure Controller Release Notes, Release 4.0(2)

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 14.0(2)*, 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

Date	Description
December 9, 2022	In the Open Bugs section, added bug CSCvw33061.
August 1, 2022	In the Miscellaneous Compatibility Information section, added: ■ 4.2(2a) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) ■ 4.1(2k) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
March 21, 2022	In the Miscellaneous Compatibility Information section, added: ■ 4.1(3f) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3)
February 23, 2022	In the Miscellaneous Compatibility Information section, added: ■ 4.1(2g) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
November 2, 2021	In the Miscellaneous Compatibility Information section, added: ■ 4.1(3d) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3)
August 4, 2021	In the Open Issues section, added bug CSCvy30453.
July 26, 2021	In the Miscellaneous Compatibility Information section, the CIMC 4.1(3c) release is now recommended for UCS C220/C240 M5 (APIC-L3/M3).
March 11, 2021	In the Miscellaneous Compatibility Information section, for CIMC HUU ISO, added: ■ 4.1(3b) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) Changed: ■ 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3) To: ■ 4.1(2b) 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: ■ 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3)
September 29, 2020	In the Miscellaneous Compatibility Information section, specified that the 4.1(1f) CIMC release is deferred. The recommended release is now 4.1(1g).
April 17, 2020	In the Miscellaneous Compatibility Information section, updated the CIMC HUU ISO information to include the 4.1(1c) and 4.1(1d) releases.
March 6, 2020	In the Miscellaneous Compatibility Information section, updated the CIMC HUU ISO information for the 4.0(2g) and 4.0(4e) CIMC releases.

Date	Description
October 8, 2019	In the Miscellaneous Compatibility Information section, updated the supported 4.0(4), 4.0(2), and 3.0(4) CIMC releases to: — 4.0(4e) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3) — 4.0(2g) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) — 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: ■ 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: ■ 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	4.0(2c): In the Open Bugs section, added bug CSCuu17314, CSCve84297, and CSCvg70246.
September 10, 2019	In the Known Behaviors section, added the following bullet: ■ 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.
August 14, 2019	4.0(2c): In the Open Bugs section, added bugs CSCvp38627 and CSCvp82252.
August 5, 2019	4.0(2c): In the Open Bugs section, added bug CSCvp25660.
July 22, 2019	4.0(2c): In the Open Bugs section, added bug CSCvq39764.
July 17, 2019	4.0(2c): In the Open Bugs section, added bug CSCvq39922.
July 11, 2019	4.0(2c): In the Open Bugs section, added bug CSCvj89771.
May 29, 2019	4.0(2c): In the Open Bugs section, added bug CSCvn79128.
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: — 4.0(2f) CIMC HUU ISO (recommended) for UCS C220/C240 M4 and M5 — 3.0(4j) CIMC HUU ISO (recommended) for UCS C220/C240 M3

Date	Description
January 23, 2019	In Miscellaneous Guidelines section, added the following text: 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 21, 2018	In Miscellaneous Guidelines section, added information about SSD over-provisioning.
December 20, 2018	4.0(2c): Release 4.0(2c) became available.

Contents

This document includes the following sections:

New and Changed Information

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

New Software Features

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

Table 2 New Software Features

Feature	Description	Guidelines and Restrictions
Cisco ACI Virtual Pod	Cisco ACI Virtual Pod (vPod) enables you to extend the Cisco ACI fabric into bare-metal cloud environments and other remote locations. Cisco ACI vPod is supported as a vLeaf switch for Cisco APIC with the VMware ESXi hypervisor. It manages a data center defined by the VMware vCenter Server. Cisco ACI vPod includes two types of virtual machine (VM) for the control planes: a virtual spine (vSpine) switch and a virtual leaf (vLeaf) switch. It also includes Cisco ACI Virtual Edge as the forwarding module on the compute node or host. For more information, see the following documents: ■ *Cisco ACI Virtual Pod Release Notes* ■ *Cisco ACI Virtual Pod Installation Guide* ■ *Cisco ACI Virtual Pod Getting Started Guide*	■ Cisco ACI vPod is in general availability in Cisco APIC release 4.0(2) ■ vPod can be deployed only on VMware environment in the cloud. ■ Deploy each virtual spine (vSpine) and virtual leaf (vLeaf) pair on two separate hosts with one vSpine and one vLeaf on each host. ■ Each instance of Cisco ACI vPod supports only two vSpine switches and two vLeafs—one vSpine and one vLeaf on each

Feature	Description	Guidelines and Restrictions
		host. ■ You can have up to 32 instances of Cisco ACI Virtual Edge in each Cisco ACI vPod.
Network Insights − Resources	The Network Insights − Resources app includes the following functions: ■ Event Analytics ■ Resource Analytics ■ Flow Analtyics	The Network Insights − Resources app is in limited availability in this release. Contact your Cisco account team if you want to download this app.
SAN boot support	SAN boot is now supported through a FEX host interface (HIF) port vPC.	None.

New Hardware Features

For new hardware features, see the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 14.0(2)* 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*.

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 4.0(2) releases in which the bug exists. A bug might also exist in releases other than the 4.0(2) releases.

Table 3 Open Bugs in This Release

Bug ID	Description	Exists in
CSCuu17314	CDP is not enabled on the management interfaces for the leaf switches and spine switches.	4.0(2c) and later
CSCvd43548	The stats for a given leaf switch rule cannot be viewed if a rule is double-clicked.	4.0(2c) 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.	4.0(2c) 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.	4.0(2c) 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]	4.0(2c) and later
CSCvf70411	A route will be advertised, but will not contain the tag value that is set from the VRF route tag policy.	4.0(2c) and later
CSCvg00627	A tenant's flows/packets information cannot be exported.	4.0(2c) and later
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.	4.0(2c) 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.	4.0(2c) and later

Bug ID	Description	Exists in
CSCvg81020	For strict security requirements, customers require custom certificates that have RSA key lengths of 3072 and 4096.	4.0(2c) and later
CSCvh52046	This is an enhancement to allow for text-based banners for the Cisco APIC GUI login screen.	4.0(2c) 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.	4.0(2c) 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.	4.0(2c) 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.	4.0(2c) 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.	4.0(2c) 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.	4.0(2c) and later
CSCvi82903	When authenticating with the Cisco APIC using ISE (TACACS), all logins over 31 characters fail.	4.0(2c) and later
CSCvj56726	The connectivity filter configuration of an access policy group is deprecated and should be removed from GUI.	4.0(2c) and later
CSCvj89771	The Virtual Machine Manager (vmmmgr) process crashes and generates a core file.	4.0(2c) and later
CSCvj91789	M5 Cisco APIC uses only 2 out of 4 ports on a new NIC.	4.0(2c) and later
CSCvk04072	There is no record of who acknowledged a fault in the Cisco APIC, nor when the acknowledgement occurred.	4.0(2c) and later

Bug ID	Description	Exists in
CSCvk18014	The action named 'Launch SSH' is disabled when a user with read-only access logs into the Cisco APIC.	4.0(2c) and later
CSCvk22596	There is a policyelem core after removing an L3Out in the same VRF instance as the NetFlow exporter.	4.0(2c) and later
CSCvm56946	Support for local user (admin) maximum tries and login delay configuration.	4.0(2c) and later
CSCvm63668	A single user can send queries to overload the API gateway.	4.0(2c) and later
CSCvm64933	The Cisco APIC setup script will not accept an ID outside of the range of 1 through 12, and the Cisco APIC cannot be added to that pod. This issue will be seen in a multi-pod setup when trying add a Cisco APIC to a pod ID that is not between 1 through 12.	4.0(2c) and later
CSCvm88517	Issues can be observed with bridge domains, subnets, and VRF instance programming in the data path.	4.0(2c) 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: 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|| ../dme/svc/policyelem/src/gen/ifc/beh/imp/./rtctrl/RouteMapUtils.cc||239:q	4.0(2c) and later
CSCvn00576	An SHA2 CSR for the ACI HTTPS certificate cannot be configured in the APIC GUI.	4.0(2c) and later
CSCvn12839	Error "mac.add.ress not a valid MAC or IP address or VM name" is seen when searching the EP Tracker.	4.0(2c) and later
CSCvn62217	A fresh Cisco APIC installation requires CIMC version 3.0.x on M3 and M4.	4.0(2c) and later
CSCvn79128	When upgrading from some 3.2 or 3.1 releases to 4.0, some or all leaf switch maintenance groups will immediately start upgrading without being user-triggered. This issue occurs as soon as the APICs finish upgrading.	4.0(2c) and later

Bug ID	Description	Exists in
CSCvo24284	Fault delegates are raised on the Cisco APIC, but the original fault instance is already gone because the affected node has been removed from the fabric.	4.0(2c) and later
CSCvp25660	After upgrading APICs from a pre-4.0 version to 4.0 or newer, the leaf switches will not upgrade, or the switches will upgrade and then automatically downgrade back to the previous version.	4.0(2c) and later
CSCvp26694	A leaf switch gets upgraded when a previously-configured maintenance policy is triggered.	4.0(2c) 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: An unexpected error has occurred while reconciling tenant tn-prj_...: long int too large to convert to float	4.0(2c) and later
CSCvp57131	After a VC was disconnected and reconnected to the APIC, operational faults (for example, discovery mismatching between APIC and VC) were cleared, even the if faulty condition still existed.	4.0(2c) and later
CSCvp62048	New port groups in VMware vCenter may be delayed when pushed from the Cisco APIC.	4.0(2c) 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	4.0(2c) and later

Bug ID	Description	Exists in
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): 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, 10:27,10:28,10:30,10:31	4.0(2c) 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.	4.0(2c) and later

CSCvp82252	While modifying the host route of OpenStack, the following subnet trace is generated:
	Response :
	{
	"NeutronError": {
	"message": "Request Failed: internal server error while processing your request.",
	"type": "HTTPInternalServerError",
	"detail": ""
	}
	}
		4.0(2c) and later

CSCvp94085	The APIC Licensemgr generates a core file while parsing an XML response.	4.0(2c) and later
CSCvp95407	Access-control headers are not present in invalid requests.	4.0(2c) and later
CSCvp97092	Tenants that start with the word "infra" are treated as the default "infra" tenant.	4.0(2c) and later
CSCvp99430	The troubleshooting wizard is unresponsive on the APIC.	4.0(2c) and later
CSCvp99508	The GUI is slow when accessing access policies. This is an enhancement request to add pagination to resolve this issue.	4.0(2c) and later

Bug ID	Description	Exists in
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.	4.0(2c) and later
CSCvq14177	The Hyper-V agent is in the STOPPED state. Hyper-V agent logs indicate that process is stopping at the "Set-ExecutionPolicy Unrestricted" command.	4.0(2c) and later
CSCvq20055	In the APIC, the "show external-l3 static-route tenant <tenant_name>" command does not output as expected. Symptom 1: The APIC outputs static-routes for tenant A, but not B. The "show external-l3 static-route tenant <tenant_name> vrf <vrf_name> node <range>" command provides the missing output. Symptom 2: For the same tenant and a different L3Out , the command does not output all static-routes.	4.0(2c) 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.	4.0(2c) and later
CSCvq39764	When you click Restart for the Microsoft System Center Virtual Machine Manager (SCVMM) agent on a scaled-out setup, the service may stop. You can restart the agent by clicking Start.	4.0(2c) and later
CSCvq39922	Specific operating system and browser version combinations cannot be used to log in to the APIC GUI. 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).	4.0(2c) 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.	4.0(2c) and later
CSCvq45710	Fault F3206 for "Configuration failed for policy uni/infra/nodeauthpol-default, due to failedEPg or failedVlan is empty" is raised in the fabric when using the default 802.1x Node Authentication policy in the Switch Policy Group. In this scenario, Fail-auth EPG and VLAN has not been configured, as the 802.1x feature is not in use.	4.0(2c) 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.reslmedcy) from Pre-Provision to On-Demand, the encap VLANs (vlanCktEp mo's) are NOT programmed on the leaf switches. This problem surfaces sporadically, meaning that it might take several reslmedcy toggles between PreProv and OnDemand to reproduce the issue.	4.0(2c) and later

Bug ID	Description	Exists in
CSCvq58304	VMM inventory-related faults are raised for VMware vCenter inventory, which is not managed by the VMM.	4.0(2c) and later
CSCvq61877	The SNMP process repeatedly crashes on the APICs. The cluster and shards look healthy and do not have any CPU or memory utilization issues.	4.0(2c) 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.	4.0(2c) 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.	4.0(2c) and later
CSCvq74727	When making a configuration change to an L3Out (such as contract removal or addition), the BGP peer flaps or the bgpPeerP object is deleted from the leaf switch. In the leaf switch policy-element traces, 'isClassic = 0, wasClassic =1' is set post-update from the Cisco APIC.	4.0(2c) and later
CSCvq80820	A previously-working traffic is policy dropped after the subject is modified to have the "no stats" directive.	4.0(2c) 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.	4.0(2c) and later
CSCvq88632	This is an enhancement request for allowing DVS MTU to be configured from a VMM domain policy and be independent of fabricMTU.	4.0(2c) and later
CSCvq95817	The F3083 fault is thrown, notifying the user that an IP address is being used by multiple MAC addresses. When navigating to the Fabric -> Inventory -> Duplicate IP Usage section, AVS VTEP IP addresses are seen as being learned individually across multiple leaf switches, such as 1 entry for Leaf 101, and 1 entry for Leaf 102. Querying for the endpoint in the CLI of the leaf switch ("show endpoint ip <IP>") shows that the endpoint is learned behind a port channel/vPC, and not an individual link.	4.0(2c) and later
CSCvr10510	There is a stale F2736 fault after configuring in-band IP addresses with the out-of-band IP addresses for the Cisco APIC.	4.0(2c) and later

Bug ID	Description	Exists in
CSCvr19693	When configuring local SPAN in access mode using the GUI or CLI and then running the "show running-config monitor access session<session>" command, the output does not include all source span interfaces.	4.0(2c) and later
CSCvr30815	vmmPLInf objects are created with epgKey's and DN's that have truncated EPG names (truncated at ".").	4.0(2c) and later
CSCvr36851	Descending option will not work for the Static Ports table. Even when the user clicks descending, the sort defaults to ascending.	4.0(2c) and later
CSCvr38278	When using AVE with Cisco APIC, fault F0214 gets raised, but there is no noticeable impact on AVE operation: descr: Fault delegate: Operational issues detected for OpFlex device: ..., error: [Inventory not available on the node at this time]	4.0(2c) 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.	4.0(2c) 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.	4.0(2c) and later
CSCvr92169	The scope for host routes should be configurable; however, the option to define the scope is not available.	4.0(2c) and later
CSCvr94614	There is a minor memory leak in svc_ifc_policydist when performing various tenant configuration removals and additions.	4.0(2c) and later
CSCvr96785	Configuring a static endpoint through the Cisco APIC CLI fails with the following error: Error: Unable to process the query, result dataset is too big Command execution failed.	4.0(2c) and later
CSCvr98638	When migrating an AVS VMM domain to Cisco ACI Virtual Edge, the Cisco ACI Virtual Edge that gets deployed is configured in VLAN mode rather than VXLAN Mode. Because of this, you will see faults for the EPGs with the following error message: "No valid encapsulation identifier allocated for the epg"	4.0(2c) and later
CSCvs03055	While configuring a logical node profile in any L3Out, the static routes do not have a description.	4.0(2c) and later

Bug ID	Description	Exists in
CSCvs10076	An error is raised while building an ACI container image because of a conflict with the /opt/ciscoaci-tripleo-heat-templates/tools/build_openstack_aci_containers.py package.	4.0(2c) and later
CSCvs16565	An endpoint is unreachable from the leaf node because the static pervasive route (toward the remote bridge domain subnet) is missing.	4.0(2c) and later
CSCvs21834	Randomly, the Cisco APIC GUI alert list shows an incorrect license expiry time.Sometimes it is correct, while at others times it is incorrect.	4.0(2c) 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".	4.0(2c) and later
CSCvs29556	When logging into the Cisco APIC using "apic#fallback\\user", the "Error: list index out of range" log message displays and the lastlogin command fails. There is no operational impact.	4.0(2c) and later
CSCvs32589	In Cisco ACI Virtual Edge, there are faults related to VMNICs. On the Cisco ACI Virtual Edge domain, there are faults related to the HpNic, such as "Fault F2843 reported for AVE | Uplink portgroup marked as invalid".	4.0(2c) and later
CSCvs47757	The plgnhandler process crashes on the Cisco APIC, which causes the cluster to enter a data layer partially diverged state.	4.0(2c) and later
CSCvs48552	When physical domains and external routed domains are attached to a security domain, these domains are mapped as associated tenants instead of associated objects under Admin > AAA > security management > Security domains.	4.0(2c) and later
CSCvs55753	A Cisco ACI leaf switch does not have MP-BGP route reflector peers in the output of "show bgp session vrf overlay-1". As a result, the switch is not able to install dynamic routes that are normally advertised by MP-BGP route reflectors. However, the spine switch route reflectors are configured in the affected leaf switch's pod, and pod policies have been correctly defined to deploy the route reflectors to the leaf switch. Additionally, the bgpPeer managed objects are missing from the leaf switch's local MIT.	4.0(2c) and later
CSCvs57061	In a GOLF configuration, when an L3Out is deleted, the bridge domains stop getting advertised to the GOLF router even though another L3Out is still active.	4.0(2c) 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.	4.0(2c) and later
CSCvs76244	The tmpfs file system that is mounted on /data/log becomes 100% utilized.	4.0(2c) and later

Bug ID	Description	Exists in
CSCvs78996	The policy manager (PM) may crash when use testapi to delete MO from policymgr db.	4.0(2c) and later
CSCvs81881	The Cisco APIC PSU voltage and amperage values are zero.	4.0(2c) and later
CSCvs81907	SNMP does not respond to GETs or sending traps on one or more Cisco APICs despite previously working properly.	4.0(2c) and later
CSCvt00796	The policymgr DME process can crash because of an OOM issue, and there are many pcons.DelRef managed objects in the DB.	4.0(2c) 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. 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.	4.0(2c) and later
CSCvt13978	VPC protection created in prior to the 2.2(2e) release may not to recover the original virtual IP address after fabric ID recovery. Instead, some of vPC groups get a new vIP allocated, which does not get pushed to the leaf switch. The impact to the dataplane does not come until the leaf switch had a clean reboot/upgrade, because the rebooted leaf switch gets a new virtual IP that is not matched with a vPC peer. As a result, both sides bring down the virtual port channels, then the hosts behind the vPC become unreachable.	4.0(2c) and later
CSCvt19061	Updating the interface policy group breaks LACP if eLACP is enabled on a VMM domain. If eLACP was enabled on the domain, Creating, updating, or removing an interface policy group with the VMM AEP deletes the basic LACP that is used by the domain.	4.0(2c) 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.	4.0(2c) and later
CSCvt40736	The login history of local users is not updated in Admin > AAA > Users > (double click on local user) Operational > Session.	4.0(2c) and later
CSCvt55566	In the Cisco APIC GUI, after removing the Fabric Policy Group from "System > Controllers > Controller Policies > show usage", the option to select the policy disappears, and there is no way in the GUI to re-add the policy.	4.0(2c) and later

Bug ID	Description	Exists in
CSCvt67279	After VMware vCenter generates a huge amount of events and after the eventId increments beyond 0xFFFFFFFF, the Cisco APIC VMM manager service may start ignoring the newest event if the eventId is lower than the last biggest event ID that Cisco APIC received. As a result, the changes to virtual distributed switch or AVE would not reflect to the Cisco APIC, causing required policies to not get pushed to the Cisco ACI leaf switch. For AVE, missing those events could put the port in the WAIT_ATTACH_ACK status.	4.0(2c) and later
CSCvt87506	SSD lifetime can be exhausted prematurely if unused Standby slot exists	4.0(2c) and later
CSCvt93482	The per feature container for techsupport "objectstore_debug_info" fails to collect on spines due to invalid filepath. Given filepath: more /debug/leaf/nginx/objstore*/mo | cat Correct filepath: more /debug/spine/nginx/objstore*/mo | cat TAC uses this file/data to collect information about excessive DME writes.	4.0(2c) and later
CSCvu01452	The MD5 checksum for the downloaded Cisco APIC images is not verified before adding it to the image repository.	4.0(2c) and later
CSCvu12092	AVE is not getting the VTEP IP address from the Cisco APIC. The logs show a "pending pool" and "no free leases".	4.0(2c) 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.	4.0(2c) and later
CSCvu39569	The following error is encountered when accessing the Infrastructure page in the ACI vCenter plugin after inputting vCenter credentials. "The Automation SDK is not authenticated" VMware vCenter plug-in is installed using powerCLI. The following log entry is also seen in vsphere_client_virgo.log on the VMware vCenter: /var/log/vmware/vsphere-client/log/vsphere_client_virgo.log [ERROR] http-bio-9090-exec-3314 com.cisco.aciPluginServices.core.Operation sun.security.validator.ValidatorException: PKIX path validation failed: java.security.cert.CertPathValidatorException: signature check failed	4.0(2c) and later
CSCvu50088	When trying to assign a description to a FEX downlink/host port using the Config tab in the Cisco APIC GUI, the description will get applied to the GUI, but it will not propagate to the actual interface when queried using the CLI or GUI.	4.0(2c) and later

Bug ID	Description	Exists in
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: Invalid DN topology/pod-X/node-Y/local/svc-policyelem-id-0/ObservedEthIf, wrong rn prefix ObservedEthIf at position 63	4.0(2c) and later
CSCvu74566	There is a BootMgr memory leak on a standby Cisco APIC. If the BootMgr process crashes due to being out of memory, it continues to crash, but system will not be rebooted. After the standby Cisco APIC is rebooted by hand, such as by power cycling the host using CIMC, the login prompt of the Cisco APIC will be changed to localhost and you will not be able to log into the standby Cisco APIC.	4.0(2c) and later
CSCvw33061	Traffic loss is observed from multiple endpoints deployed on two different vPC leaf switches.	4.0(2c) and later
CSCvy30453	For a Cisco ACI fabric that is configured with fabricId=1, if APIC3 is replaced from scratch with an incorrect fabricId of "2," APIC3's DHCPd will set the nodeRole property to "0" (unsupported) for all dhcpClient managed objects. This will be propagated to the appliance director process for all of the Cisco APICs. The process then stops sending the AV/FNV update for any unknown switch types (switches that are not spine nor leaf switches). In this scenario, commissioning/decommissioning of the Cisco APICs will not be propagated to the switches, which causes new Cisco APICs to be blocked out of the fabric. Another symptom is that the "acidag fnvread" command's output has a value of "unknown" in the role column.	4.0(2c) 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 4 Resolved Bugs in This Release

Bug ID	Description	Fixed in
CSCvi72733	This is an enhancement for displaying an alert in the GUI if a switch/module or some process has crashed.	4.0(2c)
CSCvk24883	Non-zero bit rates display for interface counters in the admin-down state.	4.0(2c)
CSCvk68748	The GUI shows 50% health score even though no faults are seen related to leaf switches or tenants. Only a few faults are seen regarding the system-wide faults, which are not impacting. Smart Licensing is not activated; however, on a DR fabric running the same Cisco APIC code, the system health is 99.	4.0(2c)
CSCvm01718	When using AVS there is no default monitoring policy. Creating a custom monitoring policy will not work either.	4.0(2c)

Bug ID	Description	Fixed in
CSCvm12790	A remote leaf switch configures a static route to the Cisco APIC based on which Cisco APIC replies for its DHCP. This route does not get deleted after the remote leaf switch is commissioned. This behavior might cause the static route to get redistributed to the IPN, which then points the route to this specific IPN back to the remote leaf switch. Because the Cisco APIC in question and remote leaf switch will now have a routing issue, they cannot communicate. From this Cisco APIC, the remote leaf switch cannot be managed.	4.0(2c)
CSCvm67928	When exporting the Cisco APIC configuration and using AES encryption to export secure passwords, HSRP passwords are not among those exported and require reconfiguration upon import.	4.0(2c)
CSCvm76293	The Cisco APIC stops displaying VM stats after some time.	4.0(2c)
CSCvm83098	After launching the Create Attachable Access Entity Profile or Configure Interface Wizard, the configuration options do not show. After this is triggered, the wizard cannot be cancelled, requiring the page to be refreshed.	4.0(2c)
CSCvm83669	There is a VLAN overlapping scenario. After configuring new static ports and a physical domain under an existing EPG, there is a Layer 2 loop. This issue is due to an FD VLAN encapsulation mismatch on two leaf switches.	4.0(2c)
CSCvm84779	A white box in the GUI appears when trying to look at leaf switches that are running an older release.	4.0(2c)
CSCvm84821	Adding a large piece of information, such as a signed certificate, makes the system go into an inconsistent state.	4.0(2c)
CSCvm87337	OpenStack VM Layer 3 communications might not work, which impacts floating IP addresses and VMs that are in different EPGs and on different compute nodes.	4.0(2c)
CSCvm90287	The GUI is displaying the wrong AAEP for a FEX port.	4.0(2c)
CSCvm96379	Security group rules are not properly implemented on compute nodes.	4.0(2c)
CSCvm96886	Some unnecessary health score change notifications sent to the GUI might affect GUI performance.	4.0(2c)
CSCvm97431	During vPC creation in the quick start wizard, the following warning appears: "VPC pair has not been created, please create a VPC pair from the table (VPC Switch Pairs) on the left"	4.0(2c)
CSCvn07827	PLR fails after upgrading to a Cisco APIC 4.0 release.	4.0(2c)
CSCvn09864	A vulnerability in certain data-log files of Cisco Application Policy Infrastructure Controller (APIC) could allow an authenticated, local attacker to to gain access to sensitive information.. The vulnerability is due to a lack of properer data protection mechanisms on an affected device. An attacker could exploit this vulnerability by by generating certain systems logs within he Cisco APIC. An exploit could allow the attacker to gain access to private key and corresponding certificate information on an affected device.	4.0(2c)

Bug ID	Description	Fixed in
CSCvn13119	The MegaSAS.log in the / directory on the Cisco APICs can get very large, causing the fault F1527 to be raised.	4.0(2c)
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)	4.0(2c)
CSCvn15478	The Firmware Repository does not display in the Cisco APIC GUI in Internet Explorer 11. This issue occurs on only the Firmware Repository in the GUI that relates to firmware.	4.0(2c)
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. These issues are preventing the VMMMGr process from processing any operational/configuration changes that are made on the RHVs.	4.0(2c)
CSCvn29918	An AVS port group is removed from the leaf switch while OpFlex is active and VMs/VMKs are still assigned to the port group.	4.0(2c)
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.	4.0(2c)
CSCvn46596	There is traffic loss of up to 11 minutes during a vMotion failure in Intra/Inter vPOD.	4.0(2c)
CSCvn52419	Traffic from an individual interface or port channel is being forward dropped on the egress leaf switch. The tunnel back to the ingress leaf switch is missing on the egress leaf switch.	4.0(2c)

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 4.0(2) releases in which the known behavior exists. A bug might also exist in releases other than the 4.0(2) 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.	4.0(2c) and later

Bug ID	Description	Exists in
CSCuo79243	In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.	4.0(2c) and later
CSCuo79250	The node ID policy can be replicated from an old appliance that is decommissioned when it joins a cluster.	4.0(2c) and later
CSCup47703	The DSCP value specified on an external endpoint group does not take effect on the filter rules on the leaf switch.	4.0(2c) and later
CSCup79002	The hostname resolution of the syslog server fails on leaf and spine switches over in-band connectivity.	4.0(2c) and later
CSCuq21360	Following a FEX or switch reload, configured interface tags are no longer configured correctly.	4.0(2c) 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).	4.0(2c) and later
CSCur71082	If the Cisco APIC is rebooted using the CIMC power reboot, the system enters into fsck due to a corrupted disk.	4.0(2c) 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.	4.0(2c) and later
CSCut51929	The traffic destined to a shared service provider endpoint group picks an incorrect class ID (PcTag) and gets dropped.	4.0(2c) 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.	4.0(2c) and later
CSCuu61998	Newly added microsegment EPG configurations must be removed before downgrading to a software release that does not support it.	4.0(2c) and later
CSCuu64219	Downgrading the fabric starting with the leaf switch will cause faults such as policy-deployment-failed with fault code F1371.	4.0(2c) and later
CSCva32534	Creating or deleting a fabricSetupP policy results in an inconsistent state.	4.0(2c) and later

Bug ID	Description	Exists in
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.	4.0(2c) 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.	4.0(2c) 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.	4.0(2c) 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.	4.0(2c) 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.	4.0(2c) and later
CSCvg79127	When first hop security is enabled on a bridge domain, traffic is disrupted.	4.0(2c) 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.	4.0(2c) and later
CSCvh76076	The PSU SPROM details might not be shown in the CLI upon removal and insertion from the switch.	4.0(2c) 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.	4.0(2c) and later
CSCvj26666	The "show run leaf|spine <nodeId>" command might produce an error for scaled up configurations.	4.0(2c) and later
CSCvs77929	In the 4.x and later releases, if a firmware policy is created with different name than the maintenance policy, the firmware policy will be deleted and a new firmware policy gets created with the same name, which causes the upgrade process to fail.	4.0(2c) 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 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 leaf switch without -EX or a later designation in the product ID happens to be in the transit path and the VRF is deployed on that leaf switch, the switch does not forward the ARP glean packet back into the fabric to reach the remote site. This issue is specific to transit leaf switches without -EX or a later designation in the product ID and does not affect leaf switches that have -EX or a later designation in the product ID. 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 4.0(2)* 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

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-L3	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1200 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)
APIC-M3	Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1200 edge ports)

The following list includes additional hardware compatibility information:

- For the supported hardware, see the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 14.0(2)* 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.
- The Cisco UCS M5-based Cisco APIC supports dual speed 10G and 25G interfaces. The Cisco UCS M4-based Cisco APIC and previous versions support only the 10G interface. Connecting the Cisco APIC to the Cisco ACI fabric requires a same speed 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.
- 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 14.0(2)
  - 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:
  - 4.2(3e) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3)
  - 4.2(3b) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
  - 4.2(2a) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
  - 4.1(3m) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
  - 4.1(3f) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
  - 4.1(3d) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
  - 4.1(3c) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
  - 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
  - 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 Notes, Release 4.0(2).*

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 either must not have -EX or a later designation in the product ID or must have -EX or a later designation in the product ID.

- 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.
- 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.

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
- 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 do not perform SSD over-provisioning on Cisco N9K-C9364C and N9K-C9336C-FX2 spine 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.
- 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 were deprecated in the 3.2(4) 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:

- 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 2.0(2)*
- *Cisco ACI Virtual Edge Installation Guide, Release 2.0(2)*
- *Cisco ACI Virtual Edge Release Notes, Release 2.0(2)*
- *Cisco ACI Virtualization Guide, Release 4.0(2)*
- *Cisco Application Virtual Switch Release Notes, 5.2(1)SV3(3.40)*
- Cisco ACI Virtual Pod Getting Started Guide, Release 4.0(2)
- Cisco ACI Virtual Pod Installation Guide, Release 4.0(2)
- Cisco ACI Virtual Pod Release Notes, Release 4.0(2c)