Cisco Application Policy Infrastructure Controller Release Notes, Release 4.1(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 14.1(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 bugs CSCvy30453 and CSCvy44940.
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).
September 16, 2020	In the Known Behaviors section, added the bullet that begins with: Beginning in Cisco APIC release 4.1(1), the IP SLA monitor policy validates the IP SLA port value.

Date	Description
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.
February 7, 2020	4.1(2x): Release 4.1(2x) became available; there are no changes to this document for this release. See the Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 14.1(2) for the changes in this release.
January 30, 2020	4.1(2w): Release 4.1(2w) became available. Added the resolved bugs for this release.
November 25, 2019	4.1(2g): In the Known Behaviors section, added bug CSCvs19322.
October 30, 2019	4.1(2u): Release 4.1(2u) became available; there are no changes to this document for this release. See the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 14.1(2)* for the changes in this release.
October 16, 2019	4.1(2s): Release 4.1(2s) became available; there are no changes to this document for this release. See the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 14.1(2)* for the changes in this release.
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	4.1(2g): In the Open Bugs section, added bug CSCuu17314, CSCve84297, and CSCvg70246.
September 11, 2019	4.1(2g): In the Resolved Bugs section, added bug CSCvp64857.

Date	Description
September 10, 2019	In the Known Behaviors secton, changed the bullet regarding the software check to validate Ethernet transceivers to specify that this check only exists in the 4.1(1) releases and the 4.1(2g) release. This check was removed in 4.1(2m) and all later releases. 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 31, 2019	4.1(2o): Release 4.1(2o) became available; there are no changes to this document for this release. See the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 14.1(2)* for the changes in this release.
August 12, 2019	4.1(2m): Release 4.1(2m) became available. Added the resolved bugs for this release.
August 5, 2019	4.1(2g): In the Open Bugs section, added bug CSCvp25660.
July 22, 2019	4.1(2g): In the GUI Guidelines section, added the following bullet: ■ When using the APIC GUI to configure an integration group, you cannot specify the connection URL (connUrl). You can only specify the connection URL by using the REST API. In the CLI Guidelines section, added the following bullet: ■ When using the APIC CLI to configure an integration group, you cannot specify the connection URL (connUrl). You can only specify the connection URL by using the REST API. In the Open Bugs section, added bug CSCvq39764.
July 17, 2019	4.1(2g): In the Open Bugs section, added bug CSCvq39922.
July 11, 2019	4.1(2g): In the Open Bugs section, added bug CSCvj89771.
July 9, 2019	In the New Software Features section, added guidelines and restrictions to the Remote leaf switches with Multi-Site Orchestrator feature.
June 27, 2019	In the Changes in Behavior section, added mention that APIC-X is now deprecated.
June 13, 2019	4.1(2g): In the Known Behavior section, added a known behavior.
June 11, 2019	4.1(2g): Release 4.1(2g) 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
Direct traffic forwarding between remote leaf switches in different remote locations	You can enable direct traffic forwarding between remote leaf switches in different remote locations. This functionality offers redundancy and high availability in the connections between the remote locations. For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide, Release 4.1(x)*.	None.
Support for Intersight Device Connector	Intersight Device Connector provides a secure way for connected devices to send information and receive control instructions from the Cisco Intersight portal using a secure Internet connection. For more information, see the *Cisco Cisco APIC and Intersight Device Connector.*	None.
Policy-based redirect bypass action	You can now specify the bypass action option when configuring Layer 4 to Layer 7 policy-based redirect. With this option, in a multi-node policy-based redirect service graph, when one node crosses the low threshold, traffic is	This feature is supported only on switch models with EX, FX, or FX2 at the end of the switch name.

Feature	Description	Guidelines and Restrictions
	still able to proceed through the rest of the service chain that is either up or cannot be bypassed. For more information, see the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.1(x)*.	This feature is not needed on a one-node service graph. If bypass is configured in such a case, the forwarding behavior is the same as the permit action. L3Out EPGs and regular EPGs can be consumer or provider EPGs. A service node that has NAT enabled cannot be bypassed, as that will break the traffic flow. The bypass action option is not supported in the following cases: ■ Layer 4 to Layer 7 service devices in one-arm mode ■ Layer 1/Layer 2 PBR nodes ■ Remote leaf switches Do not use the same PBR policy in more than one service graph if the bypass action is enabled. APIC will reject configurations if the same PBR policy with bypass action is used in multiple service graphs. To avoid this, configure different PBR policies that use the same PBR destination IP address, MAC address, and Health Group.
Policy-based redirect with a Layer 3 Outside	A uni-directional policy-based redirect with a Layer 3 Outside is now supported. For more information, see the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.1(x)*.	Use a specific L3Out EPG subnet if there are other L3Out EPGs in the same VRF instance; otherwise, you might use the other L3Outs by mistake. Ensure that IP address translation occurs on the service node. If the SNAT is

Feature	Description	Guidelines and Restrictions
		not properly done on the firewall, it could be classified to the L3Out internal and could cause a loop. An L3Out is supported only on the provider side of the last node.
Remote leaf switches with Multi-Site Orchestrator	The Multi-Site Orchestrator now supports APIC sites with remote leaf switches. For additional information, see the "Infrastructure Management" chapter in the *Cisco ACI Multi-Site Configuration Guide*.	It is not supported to stretch a bridge domain (BD) between Remote Leaf (RL) nodes associated to a given site (APIC domain) and leaf nodes part of a separate site of a Multi-Site deployment (in both scenarios where those leaf nodes are local or remote) and a fault is generated on APIC to highlight this restriction. This applies independently from the fact that BUM flooding is enabled or disabled when configuring the stretched BD on the Multi-Site Orchestrator (MSO). However, a BD can always be stretched (with BUM flooding enabled or disabled) between Remote Leaf nodes and Local Leaf nodes belonging to the same site (APIC domain).
Silent roll package upgrade	Silent roll package upgrade (SR upgrade) enables you manually to perform an internal package upgrade for ACI switch hardware SDK, drivers, and so on, without upgrading the entire ACI switch software OS. For more information, see the *Cisco APIC Installation, Upgrade, and Downgrade Guide*.	This feature supports the following switches: ■ N9K-C93216TC-FX2 ■ N9K-C93360YC-FX2
Upgrade Group field enhancement	You can now use the Upgrade Group field to select whether you are using an existing or new upgrade group when you are upgrading the leaf and spine switch software. For more information, see the *Cisco APIC Installation, Upgrade, and Downgrade Guide*.	None.

New Hardware Features

For new hardware features, see the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 14.1(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 4.1(2) releases in which the bug exists. A bug might also exist in releases other than the 4.1(2) releases.

Table 3 Open Bugs in This Release

Bug ID	Description	Exists in
CSCvv18827	The data in the Cisco APIC database may get deleted during an upgrade from a 3.0 or 3.1 release to a 4.0 or 4.1 release if the target release is rolled back to current running release within 2 minutes after the upgrade was started. The upgrade will continue anyway, but the Cisco APIC will lose all data in the database and a user with admin credentials cannot log in. Only the rescue-user/admin can log in. All shards for a process show as unexpected, and the database files are removed. The last working pre-upgrade database files are copied to the purgatory directory.	4.1(2x) and later

Bug ID	Description	Exists in
CSCvv21442	The Cisco APIC does not allow an upgrade to be cancelled. Rolling back the target version after an upgrade is started does not stop the upgrade and may cause Cisco APIC database loss. This enhancement is filed to block a Cisco APIC target version change unless the following conditions are met: 1. All Cisco APICs are online and the cluster is fully fit. 2. The upgrade job (maintUpgJob) for all Cisco APICs are completed. 3. The Installer.py process is not running on any of the Cisco APICs.	4.1(2x) and later
CSCvv41784	EIGRP summary routes are not advertised from one of the many interfaces under same interface profile.	4.1(2x) and later
CSCvs40434	When performing a network-centric migration to Cisco ACI, the surrounding network usually can handle only 1 EPG per bridge domain. If the surrounding network is not ready, there could be loop in the network.	4.1(2u)
CSCvr82304	vPod deployment fails in the VMware vCenter plugin with the following error: "Deploy ACI Virtual Pod - An Error Occured" In the logs (/var/log/vmware/vsphere-client/logs/vsphere_client_virgo.log), the following error can be seen: The following PortGroup could not be resolved	4.1(2o) and later
CSCvs03648	Cisco ACI UCSM integration does not work as expected. The Cisco APIC cannot discover a loose node UCS Fabric interconnect 6400 series when it is connected to the Cisco ACI fabric with a 100G interface.	4.1(2o) and later
CSCvv28749	A bridge domain subnet is explicitly marked as public. The same EPG subnet has the shared flag enabled and has an implicit private scope. The private scope should take precedence over the public scope and should not get advertised. However, the bridge domain subnet does get advertised through the L3Out.	4.1(2o) and later
CSCvv30303	The configuration of a bridge domain subnet scope as "public" and an EPG scope as "private" should not be allowed.	4.1(2o) and later
CSCvj14053	The health status of DHCP was not updated after a leaf switch upgrade for some of the leaf switches.	4.1(2m) and later
CSCvk04072	There is no record of who acknowledged a fault in the Cisco APIC, nor when the acknowledgement occurred.	4.1(2m) and later
CSCvr85945	There should be a description field in the subnet IP address tables.	4.1(2m) and later

Bug ID	Description	Exists in
CSCvs04899	When you run the 'show vpc map' command in the APIC CLI, it only prints the column headers, but none of the vPC information. If you go to the leaf switch CLI and run the 'show vpc extended' command, it will show the vPCs there.	4.1(2m) and later
CSCvs13857	L3Out encapsulated routed interfaces and routed interfaces do not have any monitoring policy attached to them. As a result, there is no option to change the threshold values of the faults that occur due to these interfaces.	4.1(2m) and later
CSCvs29281	An SNMP v3 trap is sent 2 minutes after a PSU is removed from the Cisco APIC, and a core file for the eventmgr is generated.	4.1(2m) and later
CSCvs49411	Special characters are not allowed in the GUI for the SNMP community string, but you can still post a configuration that has special characters in the string by using the REST API.	4.1(2m) and later
CSCvt91540	- After decommissioning a fabric node, it is not displayed in the maintenance group configuration anymore. - Due to the lingering configuration pointing to the decommissioned node, F1300 gets raised with the description: "A Fabric Node Group (fabricNodeGrp) configuration was not deployed on the fabric node <#> because: Node Not Registered for Node Group Policies" - The dn mentioned in the fault will point to a maintenance group (maintgrp).	4.1(2m) and later
CSCuu17314	CDP is not enabled on the management interfaces for the leaf switches and spine switches.	4.1(2g) and later
CSCvd43548	The stats for a given leaf switch rule cannot be viewed if a rule is double-clicked.	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) and later

Bug ID	Description	Exists in
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]	4.1(2g) and later
CSCvf70411	A route will be advertised, but will not contain the tag value that is set from the VRF route tag policy.	4.1(2g) and later
CSCvg00627	A tenant's flows/packets information cannot be exported.	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) and later
CSCvg81020	For strict security requirements, customers require custom certificates that have RSA key lengths of 3072 and 4096.	4.1(2g) and later
CSCvh52046	This is an enhancement to allow for text-based banners for the Cisco APIC GUI login screen.	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) and later

Bug ID	Description	Exists in
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.	4.1(2g) and later
CSCvi82903	When authenticating with the Cisco APIC using ISE (TACACS), all logins over 31 characters fail.	4.1(2g) and later
CSCvj56726	The connectivity filter configuration of an access policy group is deprecated and should be removed from GUI.	4.1(2g) and later
CSCvj89771	The Virtual Machine Manager (vmmmgr) process crashes and generates a core file.	4.1(2g) and later
CSCvk18014	The action named 'Launch SSH' is disabled when a user with read-only access logs into the Cisco APIC.	4.1(2g) and later
CSCvm32345	A port group cannot be renamed. This is an enhancement request to enable the renaming of port groups.	4.1(2g) and later
CSCvm42914	This is an enhancement request to add policy group information to the properties page of physical interfaces.	4.1(2g) and later
CSCvm56946	Support for local user (admin) maximum tries and login delay configuration.	4.1(2g) and later
CSCvm63668	A single user can send queries to overload the API gateway.	4.1(2g) 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.	4.1(2g) 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	4.1(2g) and later

Bug ID	Description	Exists in
CSCvn00576	An SHA2 CSR for the ACI HTTPS certificate cannot be configured in the APIC GUI.	4.1(2g) and later
CSCvn12839	Error "mac.add.ress not a valid MAC or IP address or VM name" is seen when searching the EP Tracker.	4.1(2g) and later
CSCvn99797	When 3 DNS providers are added, F3546 faults are raised for: Policy Configuration for DNS Profile: default failed due to : provider-limit-exceeded. To debug/rectify: DNS Provider count cannot exceed 2. The first 2 DNS providers you provide will be used for name resolution. The rest of the nameservers will be not be used for name resolution.	4.1(2g) and later
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.	4.1(2g) and later
CSCvo42420	After changing the VRF instance association of a shared-services bridge domain, a shared-services route is still present in the old VRF instance.	4.1(2g) 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.	4.1(2g) and later
CSCvp26694	A leaf switch gets upgraded when a previously-configured maintenance policy is triggered.	4.1(2g) and later
CSCvp38968	A service graph with a Layer 1 device goes to the "failed" state when an inter-tenant contract is used. The error in the graph will be "id-allocation-failure".	4.1(2g) and later
CSCvp43877	When using the "Clone" option for a policy group or interface profile and an existing name is used, the cloned policy overwrites the old policy. A warning should be displayed regarding the policy name that already exists.	4.1(2g) and later
CSCvp44764	With the PBR feature, the svcredirDestmon object in the leaf switch is incorrectly removed. As a result, a service device cannot be tracked and the switch incorrectly reports the status to APIC that the service device is down. When this happens, the switch attempts to take corrective action based on the user configuration (the threshold action configuration). The switch attempts to skip the service node if thresholdDownAction is set to "bypass," send the traffic directly to the destination if thresholdDownAction is set to "permit," or drop the traffic if thresholdDownAction is set to "deny".	4.1(2g) and later
CSCvp51422	BD stretch should not be supported in MSC configuration when cross site boundary with Remote Leaf is involved.	4.1(2g) and later

Bug ID	Description	Exists in
CSCvp56705	If the COOP process stops, then an alert is generated in the APIC and any later alerts do not get cleared after the process restarts.	4.1(2g) 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.	4.1(2g) and later
CSCvp62048	New port groups in VMware vCenter may be delayed when pushed from the Cisco APIC.	4.1(2g) and later
CSCvp68296	The APIC process information from the APIC GUI may have the wrong values.	4.1(2g) 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): 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	4.1(2g) and later
CSCvp73395	When connecting the ExternalSwitch app to a UCSM environment, ACI VLANs are not deployed to the fabric-connected vNICS that were configured as part of a redundancy peer. The VLANs are allocated from the ACI VLAN pools, but are never added to the UCSM LAN group nor VLANs, and are not added to the vNICs when the vNICs are configured with Redundant Peer configurations in UCSM.	4.1(2g) and later
CSCvp79155	Inventory pull operations or VMware vCenter updates are delayed.	4.1(2g) 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.	4.1(2g) and later
CSCvp80983	The ipv4RouteMo/ipv6RouteMo is not present in case of a shared service route leak. The route could have been deleted when EPG to BD association is removed and not added back when this association is created again.	4.1(2g) and later
CSCvp86156	If a user manually modifies an object controlled by the ACI CNI, the configuration will not be restored for up to 14 minutes.	4.1(2g) and later
CSCvp94060	No fault is raised when First Hop Security is enabled in a Layer 2 only Bridge Domain.	4.1(2g) and later

Bug ID	Description	Exists in
CSCvp94085	The APIC Licensemgr generates a core file while parsing an XML response.	4.1(2g) and later
CSCvp95407	Access-control headers are not present in invalid requests.	4.1(2g) and later
CSCvp97092	Tenants that start with the word "infra" are treated as the default "infra" tenant.	4.1(2g) and later
CSCvp99430	The troubleshooting wizard is unresponsive on the APIC.	4.1(2g) and later
CSCvp99508	The GUI is slow when accessing access policies. This is an enhancement request to add pagination to resolve this issue.	4.1(2g) and later
CSCvq02715	There are issues with out-of-band SSH connectivity to the leaf and spine switches if the out-of-band VRF instance is deleted and re-created with the same name.	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) and later
CSCvq16739	For virtual pod and physical pod wizards, when a user tries to configure TEP addresses, there is an error on a preconfigured data plane TEP IP address. This error does not let the user proceed with rest of the configuration.	4.1(2g) and later
CSCvq19984	aci-container-controllers will delete all the contract relationships under the default_ext_epg if it loses connectivity to the APIC during the API call to get the subtree for the contract relationships.	4.1(2g) 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.	4.1(2g) and later

Bug ID	Description	Exists in
CSCvq22658	Description fields are not available for resource pools (VLAN, VSAN, Mcast, VXLAN etc).	4.1(2g) and later
CSCvq24993	The MTU cannot be modified on the SPAN destination after it is configured.	4.1(2g) and later
CSCvq28342	In a fabric with only fixed spine switches, the modular security license is still used when enabling MACsec. The fixed spine switch should share the same Add-on Security license entitlement with the leaf switch, because the features charge the same price.	4.1(2g) 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.	4.1(2g) and later
CSCvq38191	An eventmgr core file gets generated when a user performs the syslog debug command "logit".	4.1(2g) and later
CSCvq39477	A user with read-only permissions cannot collect the techsupport files using the CLI nor a policy.	4.1(2g) 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.	4.1(2g) 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).	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) and later
CSCvq55982	APIC running 4.1(2g) throws fault for pingcheck failed.	4.1(2g) and later
CSCvq56057	ACI running 4.1.1j.	4.1(2g) and later

Bug ID	Description	Exists in
CSCvq56243	When toggling the "legacy mode" option on a bridge domain, there should be a warning message that displays.	4.1(2g) 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. This problem surfaces sporadically, meaning that it might take several resImedcy toggles between PreProv and OnDemand to reproduce the issue.	4.1(2g) and later
CSCvq58304	VMM inventory-related faults are raised for VMware vCenter inventory, which is not managed by the VMM.	4.1(2g) and later
CSCvq58839	Configuration import fails due to a Global AES encryption key mismatch for pimIfPol.	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) and later
CSCvq77297	Plugin-handler triggers pre-remove the lifecycle hook for a scale-out app that is being removed. It keeps checking the status of pre-remove lifecycle hook using a Kron API, but if Kron is down, the plugin-handler waits for Kron to come back in the same transaction. This can cause the APIC cluster to diverge.	4.1(2g) and later
CSCvq80820	A previously-working traffic is policy dropped after the subject is modified to have the "no stats" directive.	4.1(2g) and later
CSCvq85224	The GUI navigates to the incorrect tree item from Virtual Networking -> domains - container domains.	4.1(2g) and later

Bug ID	Description	Exists in
CSCvq86573	Under a corner case, the Cisco APIC cluster DB may become partially diverged after upgrading to a release that introduces new services. A new release that introduces a new DME service (such as the domainmgr in the 2.3 release) could fail to receive the full size shard vector update in first two-minute window, which causes the new service flag file to be removed before all local leader shards are able to boot into the green field mode. This results in the Cisco APIC cluster DB becoming partially diverged.	4.1(2g) and later
CSCvq87663	When creating a subject and leaving "Wan SLA Policy" as unspecified (field not required), Fault F3330 is raised. Fault code: F3330 Description: Failed to form relation to MO uni/tn-common/sdwanpolcont/sdwanslapol- of class extdevSDWanSlaPol Type: Config	4.1(2g) 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.	4.1(2g) and later
CSCvq89967	An OSPF L3Out with a check in the BGP check box is missing the redistribute route-map.	4.1(2g) and later
CSCvq95687	Currently, under Fabric > Inventory > Pod > Leaf Switch > General, the memory usage takes in consideration the MemFree field rather than the MemAvailable, which would be a more accurate representation of the usable memory in the system. In some cases, the GUI might show that the memory utilization is around 90% while in reality it's 50%, because there is still the cached/buffered memory to take into account. This buffered/cached memory will free up a big chunk of memory in case more memory is needed.	4.1(2g) 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.	4.1(2g) and later
CSCvq96516	There is an event manager process crash.	4.1(2g) 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.	4.1(2g) and later

Bug ID	Description	Exists in
CSCvr12971	The Cisco APIC GUI produces the following error messages when opening an EPG policy: Received Invalid Json String. The server returned an unintelligible response.This issue might affect backup/restore functionality.	4.1(2g) and later
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.	4.1(2g) and later
CSCvr30815	vmmPLInf objects are created with epgKey's and DN's that have truncated EPG names (truncated at ".").	4.1(2g) and later
CSCvr36851	Descending option will not work for the Static Ports table. Even when the user clicks descending, the sort defaults to ascending.	4.1(2g) 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]	4.1(2g) 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.	4.1(2g) and later
CSCvr43275	While configuring a node in-band address using a wizard or configuring a subnet under the bridge domain (tenant > bridge domain > subnet), and "x.x.x.0/subnet" is chosen as the range, the following message displays: Incorrect message " Error 400 - Broadcast IP x.x.x.0/subnet" during inband config	4.1(2g) and later
CSCvr51069	In some circumstances, fault F1188 is generated. This fault is cosmetic.	4.1(2g) and later
CSCvr67887	Fault: F3060 "license-manager-license-authorization-expired" is raised although "show license status" shows the REGISTERED status and the license authorization shows AUTHORIZED.	4.1(2g) and later
CSCvr76318	Cisco ACI plugin containers do not get updated.	4.1(2g) and later
CSCvr82224	A leaf switch port flaps without raising a warning.	4.1(2g) 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.	4.1(2g) and later

Bug ID	Description	Exists in
CSCvr85821	The API query /api/class/compCtrlr.json?rsp-subtree=full? returns a malformed JSON file.	4.1(2g) and later
CSCvr92169	The scope for host routes should be configurable; however, the option to define the scope is not available.	4.1(2g) and later
CSCvr94305	When a user logs into the Cisco APIC GUI and selects the SAL login domain, the authorization fails and the user gets thrown back to the initial login screen. The Cisco APIC NGINX logs show a failure to parse the AVPair value that is sent back by the SAML IDP. When checking the AVPair value returned by the Okta SAML IDP "<inRole value="shell:domains=all//read-all"/>", the value seems to have correct syntax.	4.1(2g) and later
CSCvr94614	There is a minor memory leak in svc_ifc_policydist when performing various tenant configuration removals and additions.	4.1(2g) 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.	4.1(2g) 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"	4.1(2g) and later
CSCvs03055	While configuring a logical node profile in any L3Out, the static routes do not have a description.	4.1(2g) and later
CSCvs04981	F2928 "KeyRing Certificate expired" faults raised and do not get cleared.	4.1(2g) and later
CSCvs05817	While using the UCSM plugin/VMM domain, during a vPC link failover test, VLANs from the vNIC template are removed. However, global (uplink) VLANs and the VLAN group remain untouched. In addition, the VMM domain is removed.	4.1(2g) and later
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.	4.1(2g) and later
CSCvs16565	An endpoint is unreachable from the leaf node because the static pervasive route (toward the remote bridge domain subnet) is missing.	4.1(2g) and later

Bug ID	Description	Exists in
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.	4.1(2g) 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".	4.1(2g) 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.	4.1(2g) and later
CSCvs31335	App techsupport collection does not work sometimes when triggered from the Cisco APIC GUI.	4.1(2g) 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".	4.1(2g) and later
CSCvs39652	Host subnets (/32) that are created under an SCVMM-integrated EPG get pushed as a virtual machine subnet under the virtual machine network in SCVMM. Virtual machine networks on SCVMM do not support /32 virtual machine subnets and fail to come up. Virtual machines that were previously associated to the virtual machine networks lose connectivity.	4.1(2g) and later
CSCvs47757	The plgnhandler process crashes on the Cisco APIC, which causes the cluster to enter a data layer partially diverged state.	4.1(2g) 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.	4.1(2g) and later
CSCvs53247	OpenStack supports more named IP protocols for service graph rules than are supported in the Cisco APIC OpenStack Plug-in.	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) and later

Bug ID	Description	Exists in
CSCvs74120	Selecting the RADIUS login domain from the GUI results in the following error: Error: 400 - unknown property value test, name realm, class aaaConsoleAuth [(Dn0)] Dn0=uni/userext/authrealm/consoleauth,	4.1(2g) and later
CSCvs76244	The tmpfs file system that is mounted on /data/log becomes 100% utilized.	4.1(2g) and later
CSCvs78996	The policy manager (PM) may crash when use testapi to delete MO from policymgr db.	4.1(2g) and later
CSCvs81881	The Cisco APIC PSU voltage and amperage values are zero.	4.1(2g) and later
CSCvs81907	SNMP does not respond to GETs or sending traps on one or more Cisco APICs despite previously working properly.	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) 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.	4.1(2g) and later
CSCvt28235	Fault F1527 is raised when the /data/log directory is over 75% full. The /data/log directory contains a large amount of gzipped 21M svc_ifc_licensemgr.bin.warnplus.log files. The /data/log directory does not reach 80% or 90% full.	4.1(2g) 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.	4.1(2g) and later

Bug ID	Description	Exists in
CSCvt40736	The login history of local users is not updated in Admin > AAA > Users > (double click on local user) Operational > Session.	4.1(2g) and later
CSCvt44854	- Leaf or spine switch is stuck in 'downloading-boot-script' status. The node never fully registers and does not become active in the fabric. - You can check the status by running 'cat /mit/sys/summary | grep state' on the CLI of the spine or leaf switch: If the state is set to 'downloading-boot-script' for a long period of time (> 5 minutes) you may be running into this issue. - Checking the policy element logs on the spine or leaf switch will confirm if the bootscript file cannot be found on the Cisco APIC: 1. Change directory to /var/log/dme/log. 2. Grep all svc_ifc_policyelem.log files for "downloadUrl - failed, error=HTTP response code said error" If you see this error message, check to make sure all Cisco APICs have the node bootscript files located in /firmware/fwrepos/fwrepo/boot.	4.1(2g) and later
CSCvt48819	When using the Internet Explore browser, there is console error. This error will break some pages under Fabric -> Inventory -> [ANY POD] -> [ANY LEAF] / [ANY SPINE] -> Interfaces -> Physical, PC, VPC, FC, FC PC.	4.1(2g) 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.	4.1(2g) and later
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.	4.1(2g) and later
CSCvt68786	A Cisco ACI Virtual Edge EPG is not programmed on a port channel toward the blade switch after it is deleted and recreated.	4.1(2g) and later
CSCvt87506	SSD lifetime can be exhausted prematurely if unused Standby slot exists	4.1(2g) and later

Bug ID	Description	Exists in
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.	4.1(2g) and later
CSCvu01259	AAEP gets deleted while changing some other policy in the policy group. This only happens when using Firefox and changing a value in the leaf access port policy group. The issue is not seen when using other browsers.	4.1(2g) and later
CSCvu01452	The MD5 checksum for the downloaded Cisco APIC images is not verified before adding it to the image repository.	4.1(2g) and later
CSCvu08233	Inside the /firmware/fwrepos/fwrepo/boot directory, there is a Node-0 bootscript that seemingly points to a random leaf SN, depending on the Cisco APIC from which you're viewing the directory.	4.1(2g) 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".	4.1(2g) 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.	4.1(2g) 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	4.1(2g) and later
CSCvu49644	A tunnel endpoint doesn't receive a DHCP lease. This occurs with a newly deployed or upgraded Cisco ACI Virtual Edge.	4.1(2g) 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.	4.1(2g) 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	4.1(2g) and later
CSCvu67388	When creating a VMware VMM domain and specifying a custom delimiter using the character _ (underscore), it is rejected, even though the help page says it is an acceptable character.	4.1(2g) 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.	4.1(2g) and later
CSCvv25475	After a delete/add of a Cisco ACI-managed DVS, dynamic paths are not programmed on the leaf switch and the compRsDlPol managed object has a missing target. The tDn property references the old DVS OID instead of the latest value.# moquery -c compRsDlPol	4.1(2g) and later
CSCvv62861	A leaf switch reloads due to an out-of-memory condition after changing the contract scope to global.	4.1(2g) and later
CSCvw33061	Traffic loss is observed from multiple endpoints deployed on two different vPC leaf switches.	4.1(2g) 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.	4.1(2g) and later
CSCvq41830	NGINX spikes to 100% CPU usage.	4.1(2g)
CSCvq68833	When upgrading from a 4.0 release to a 4.1 release while using a certificate with the APIC local user, the "Mandatory permission VMM Connectivity and VMM EP are required" fault occurs when accessing the Infrastructure page.	4.1(2g)

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
CSCvm28482	If you have two different L3outs due to design requirements and both are running BGP on the same node and the same vrf, configuration does not allow to use the same loopback to be used as update source for bgp peering for both L3outs. In this customer scenario we have seeing that if the second L3out has no loopback created, in that case it picks the first loopback, however after reload we have seeing it might pick another interface to source the BGP sessions which breaks BGP after reload of the switch.	4.1(2g)
CSCvn07827	PLR fails after upgrading to a Cisco APIC 4.0 release.	4.1(2g)
CSCvn28063	After performing an upgrade on a spine in a remote POD, the upgrade will not complete. The spine may boot up with the same version if reloaded manually. You may also notice that the spine is stuck in a bootloop with the following error raised on the console: [1041.090380] obfl_klm writing reset reason 58, LC insertion sequence failure => [Failures < MAX] : powercycle [1042.207780] write_mtd_flash_panic: successfully wrote 88 bytes at address 0xd68 to RR Iter: 0.	4.1(2g)
CSCvn79909	SNAPSHOT taken by remote user shows it has been created by ADMIN in Audit logs, and no information about the actual remote user creator of the snapshot.	4.1(2g)
CSCvn97710	When the APICs are booted up with different fabric IDs during bootstrap, instead of creating a wiring mismatch, the APICs are brought into the cluster and the policy element (PE) data management engine (DME) in the leaf switches update their fabric ID. Fix: We ignore the fabric ID changes on the PE side and the node sticks to the first fabric ID that it learned. We do not raise a wiring mismatch and block the APICs because it will break upgrades.	4.1(2g)
CSCvo17056	SNMPv3 traps generated by the APIC are dropped by NMS systems that have replay protection enabled.	4.1(2g)
CSCvo23714	NGINX has an out of memory issue approximately every 10 hours due to the memory usage growing to up to 8GB.	4.1(2g)
CSCvo39336	If many faults flap on the switch nodes, the GUI may run slowly and have poor response.	4.1(2g)
CSCvo58876	A fault gets raised for an app and the fault content includes the following message: WARNING: Your kernel does not support swap limit capabilities, memory limited without swap. But, when the logs get analyzed the real issue is not related to the above warning message.	4.1(2g)
CSCvo62969	SVI Primary IP pushed without subnet mask might cause an outage as the route will be advertised by the presence of valid secondary IP but adjacency wont be built.	4.1(2g)
CSCvo80048	Serial port baud rate changed.	4.1(2g)
CSCvo86747	The properties of a Layer 4 to Layer 7 device cannot be viewed.	4.1(2g)

Bug ID	Description	Fixed in
CSCvo88534	When modifying properties, without clicking on "submit", if you download the configuration, the changes will be pushed regardless.	4.1(2g)
CSCvo98381	Removing an FC interface policy causes the Eth interface policy associated with the same AEP also being deleted.	4.1(2g)
CSCvp07262	Configuration import (configImportP) with importMode="atomic" and importType="replace" may not work.	4.1(2g)
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	4.1(2g)
CSCvp42686	GUI is slow and becomes unresponsive once the Operational Tab is opened for the EPG.	4.1(2g)
CSCvp53892	When the APIC fails to retrieve/process the adjacency for one of the host uplink VMNICs, it does not continue to process the rest of the uplink VMNICs. The resulting behavior can be different depending upon the order in which the host VMNICs is processed; which can be different each time. With the remainder of the adjacency that is not being processed, this can result in APIC removing VLANs from the leaf switches depending upon the resolution immediacy of the VMM domain.	4.1(2g)
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	4.1(2g)

Bug ID	Description	Fixed in
CSCvp64857	A vulnerability in the REST API for software device management in Cisco Application Policy Infrastructure Controller (APIC) Software could allow an authenticated, remote attacker to escalate privileges to root on an affected device. The vulnerability is due to incomplete validation and error checking for the file path when specific software is uploaded. An attacker could exploit this vulnerability by uploading malicious software using the REST API. A successful exploit could allow an attacker to escalate their privilege level to root. The attacker would need to have the administrator role on the device. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-ccapic-restapi	4.1(2g)
CSCvp71082	The same GIPo is allocated for different BDs when BD scale is low (less then 7K BDs in total).	4.1(2g)

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": ""
	
	}
	
	}
		4.1(2g)

CSCvp85106	Not Found (403, 404) when clicking on help icon under Admin/Firmware.	4.1(2g)
CSCvp95621	The showconfig command fails and displays an exception.	4.1(2g)
CSCvq03722	When performing a clean reboot using the acidiag touch setup or the acidiag reboot commands, during the boot up of APIC, you will observe a significant delay between the enter key to continue and the interactive setup parameter menu. No other operational impact other than slower boot up due to system delay.	4.1(2g)
CSCvq41830	NGINX spikes to 100% CPU usage.	4.1(2m)
CSCvq68833	When upgrading from a 4.0 release to a 4.1 release while using a certificate with the APIC local user, the "Mandatory permission VMM Connectivity and VMM EP are required" fault occurs when accessing the Infrastructure page.	4.1(2m)

Bug ID	Description	Fixed in
CSCvs40434	When performing a network-centric migration to Cisco ACI, the surrounding network usually can handle only 1 EPG per bridge domain. If the surrounding network is not ready, there could be loop in the network.	4.1(2w)

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 4.1(2) releases in which the known behavior exists. A bug might also exist in releases other than the 4.1(2) releases.

Table 5 Known Behaviors in This Release

Bug ID	Description	Exists in
CSCvj26666	The "show run leaf|spine <nodeId>" command might produce an error for scaled up configurations.	4.1(2g) 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.	4.1(2g) and later
CSCvs19322	Upgrading Cisco APIC from a 3.x release to a 4.x release causes Smart Licensing to lose its registration. Registering Smart Licensing again will clear the fault.	4.1(2g) 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.	4.1(2g) and later

- Beginning in Cisco APIC release 4.1(1), the IP SLA monitor policy validates the IP SLA port value. Because of the validation, when TCP is configured as the IP SLA type, Cisco APIC no longer accepts an IP SLA port value of 0, which was allowed in previous releases. An IP SLA monitor policy from a previous release that has an IP SLA port value of 0 becomes invalid if the Cisco APIC is upgraded to release 4.1(1) or later. This results in a failure for the configuration import or snapshot rollback.

  The workaround is to configure a non-zero IP SLA port value before upgrading the Cisco APIC, and use the snapshot and configuration export that was taken after the IP SLA port change.

- In the 4.1(1) and 4.1(2g) releases, there is a software check to validate Ethernet transceivers. Before ACI 4.1, this check was not present in the software. This check is required to make sure Ethernet ports are properly identified. If the software check detects an Ethernet transceiver to have Fibre Channel SPROM values, the transceiver will fail the validation check and will be put into a downed state. If any Ethernet transceivers have an incorrectly programmed SPROM which identifies them as FC compliant, they will fail the transceiver validation and fail to come up on 4.1(2). In this scenario, contact your respective vendors to update and address the programmed SPROM values. All Ethernet transceivers that have the expected Ethernet SPROM programming should continue to work after the upgrade. This software check was removed from the 4.1(2m) release and all later releases.

- If you use the REST API to upgrade an app, you must create a new firmware.OSource to be able to download a new app image.
- 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 4.1(1)* at the following URL:

  https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html
- 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 14.1(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."
- First generation switches (switches without -EX, -FX, -GX, or a later suffix in the product ID) do not support Contract filters with match type "IPv4" or "IPv6." Only match type "IP" is supported. Because of this, a contract will match both IPv4 and IPv6 traffic when the match type of "IP" is used.

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 14.1(2)
  - Cisco AVS, Release 5.2(1)SV3(3.80)

    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 4.1(2).*
- For compatibility with Day-2 Operations apps, see the Cisco Day-2 Operations Apps Support Matrix.

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.
- When using the APIC GUI to configure an integration group, you cannot specify the connection URL (connUrl). You can only specify the connection URL by using the REST API.
- 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.
- When using the APIC CLI to configure an integration group, you cannot specify the connection URL (connUrl). You can only specify the connection URL by using the REST API.

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.

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 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 APIC and Intersight Device Connector*

You can find these documents on 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