Cisco Application Policy Infrastructure Controller Release Notes, Release 3.1(2)

Note: Due to bug CSCvi29916 that was discovered in the 3.1(2m) release, you should install or upgrade to the 3.1(2o) or later release. Do not use the 3.1(2m) release.

The Cisco Application Centric Infrastructure (ACI) is an architecture that allows the application to define the networking requirements in a programmatic way. This architecture simplifies, optimizes, and accelerates the entire application deployment lifecycle. Cisco Application Policy Infrastructure Controller (APIC) is the software, or operating system, that acts as the controller.

The *Cisco Application Centric Infrastructure Fundamentals* guide provides complete details about the Cisco ACI, including a glossary of terms that are used in the Cisco ACI.

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

Note: Use this document with the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 13.1(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
December 9, 2022	In the Open Bugs section, added bug CSCvw33061.
August 29, 2022	In the Miscellaneous Compatibility Information section, for CIMC HUU ISO, added 3.0(3f).
February 3, 2021	In the Miscellaneous Compatibility Information section, for CIMC HUU ISO, deleted the bullets that mentioned APIC-M3 and APIC-M4. These servers are not supported in this release.
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	3.1(2m): In the Open Bugs section, added bug CSCuu17314, CSCve84297, and CSCvg70246.
August 14, 2019	3.1(2v): Release 3.1(2v) became available. Added the open bugs for this release.
August 5, 2019	3.1(2m): In the Open Bugs section, added bug CSCvj76503.
March 15, 2019	3.1(2u): Release 3.1(2u) became available; there are no changes to this document for this release.
January 16, 2019	In the New Software Features section, removed "Maximum MTU increased to 9216." This information was erroneously included; the maximum MTU was not increased in this release.
January 7, 2019	3.1(2t): Release 3.1(2t) became available; there are no changes to this document for this release.
November 21, 2018	3.1(2m): In the Open Bugs section, added bug CSCvn15374.
November 14, 2018	3.1(2s): Release 3.1(2s) became available. Added the resolved bugs for this release.
June 26, 2018	3.1(2m): In the Open Bugs section, added bug CSCvi29916. 3.1(2o): In the Resolved Bugs section, added bug CSCvi29916.
June 13, 2018	3.1(2m): In the Known Behaviors section, added the bulleted list item that begins with: A fault is raised for a VMware VDS, Cisco ACI Virtual Edge, or Cisco AVS VMM domain indicating that complete tagging information could not be retrieved for a controller.

Date	Description
June 7, 2018	3.1(2q): Release 3.1(2q) became available. Added the resolved bugs for this release.
June 4, 2018	In the Changes in Behavior section, added the following item: The Cisco APIC-generated SNMP traps now include variable binding (varbind) timeticks.
May 22, 2018	3.1(2p): Release 3.1(2p) became available. Added the resolved bugs for this release.
May 18, 2018	In the New Software Features section, added the following item: Graceful Maintenance on switch maintenance groups
April 29, 2018	3.1(2o): Release 3.1(2o) became available. Added the open and resolved bugs for this release.
March 30, 2018	In the Miscellaneous Compatibility Information section, changed the Cisco AVS release to 5.2(1)SV3(3.21) and added Cisco ACI Virtual Edge 1.1(2a).
March 22, 2018	In the Changes in Behavior section, added the following item: If no statistics have been generated on a path in the lifetime of the fabric, no atomic counters are generated for the path. Also, the Traffic Map in the Visualization tab (Operations > Visualization in the Cisco APIC GUI) does not show all paths, only the active paths (paths that had traffic at some point in the fabric lifetime).
March 15, 2018	In the New Software Features section, added the following item: Cloud Foundry Integration with Cisco ACI
March 12, 2018	In the New Software Features section, added the following item: Cisco ACI Multi-Site support on the Cisco N9K-C9364C switch and N9K-C9508-FM-E2 and N9K-C9516-FM-E2 fabric modules
March 3, 2018	3.1(2m): Release 3.1(2m) 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

Table 2 New Software Features, Guidelines, and Restrictions

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

Table 2 New Software Features, Guidelines, and Restrictions

Feature	Description	Guidelines and Restrictions
BGP external routed network with the autonomous system override	The autonomous system override function replaces the autonomous system number from the originating router with the autonomous system number of the sending BGP router in the autonomous system path of the outbound routes. For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide*.	None.
Cisco ACI Multi-Site support on the Cisco N9K-C9364C switch and N9K-C9508-FM-E2 and N9K-C9516-FM-E2 fabric modules	Cisco ACI Multi-Site is now supported on the Cisco N9K-C9364C switch and N9K-C9508-FM-E2 and N9K-C9516-FM-E2 fabric modules.	None.
Cloud Foundry Integration with	Beginning in this release, Cloud Foundry is integrated with Cisco Application Centric Infrastructure (ACI). This feature enables customers to use all Cisco ACI security and policy	Cisco ACI integration applies to Cloud Foundry deployed on VMware vSphere where the Cisco

Feature	Description	Guidelines and Restrictions
Cisco ACI	features with Cloud Foundry containers. Cloud Foundry is a platform as a service (PaaS) that uses Linux containers to deploy and manage applications. For more information, see the *Cisco ACI and Cloud Foundry Integration* knowledge base article and the *Cisco Application Policy Infrastructure Controller OpenStack and Container Plugins, Release Notes*.	ACI provides the network fabric for VMware vSphere.
Graceful Maintenance on switch maintenance groups	In this release, when a user upgrades the Cisco ACI Fabric, there is now an option to enable Graceful Maintenance when upgrading the maintenance groups. When this option is enabled, the Cisco APIC will put the switches into the existing graceful insertion and removal (GIR) mode before reloading. This allows the switch to shut down all protocols gracefully before reloading for the upgrade.	This feature can only be used when all nodes in the fabric are upgraded to release 3.1(2) or later. Using this feature to upgrade nodes on a version prior to 3.1(2) can result in unexpected traffic loss when the nodes are being upgraded.
LACP support on Layer 2/Layer 3 traffic diversion for the graceful insertion and removal mode	The existing graceful insertion and removal (GIR) mode supports all Layer 3 traffic diversion. With LACP, all of the Layer 2 traffic is also diverted to the redundant node. After a node goes into maintenance mode, LACP running on the node immediately informs neighbors that it can no longer be aggregated as part of a port channel. All traffic is then diverted to the vPC peer node. For more information, see the *Cisco APIC Getting Started Guide*.	None.
Neighbor discovery router advertisement on Layer 3 Outsides	Router solicitation/router advertisement packets are used for auto-configuration and are configurable on Layer 3 interfaces, including routed interface, Layer 3 sub-interface, and SVI (external and pervasive). For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide*.	None.
QoS for Layer 3 Outsides	In this release, QoS policy enforcement on L3Out ingress traffic is enhanced. To configure QoS policies in an L3Out, the VRF instance must be set in egress mode (Policy Control Enforcement Direction = "egress") with policy control enabled (Policy Control Enforcement Preference = "Enforced"). You must configure the QoS class priority or DSCP setting in the contract that governs the Layer 3 external network. For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide*.	None.

New Hardware Features

For new hardware features, see the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 13.1(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

The following are changes in behavior for this release:

- The Basic GUI mode is deprecated. The Cisco APIC Basic mode is no longer available.
- In the GUI, when viewing a tenant, the Security Policies folder in the Navigation pane is now named Contracts. The Contracts folder contains the following subfolders: Standard, Taboos, Imported, and Filters.
- The Navigation pane folders of the Tenants tab and Virtual Networking tab have been restructured to reduce the number of folders.
- If no statistics have been generated on a path in the lifetime of the fabric, no atomic counters are generated for the path. Also, the Traffic Map in the Visualization tab (Operations > Visualization in the Cisco APIC GUI) does not show all paths, only the active paths (paths that had traffic at some point in the fabric lifetime).
- The Cisco APIC-generated SNMP traps now include variable binding (varbind) timeticks.

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

This section lists the open bugs. Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Exists In" column of the table specifies the 3.1(2) releases in which the bug exists. A bug might also exist in releases other than the 3.1(2) releases.

Table 3 Open Bugs in This Release

Bug ID	Description	Exists in
CSCvu01452	The MD5 checksum for the downloaded Cisco APIC images is not verified before adding it to the image repository.	3.1(2v)
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	3.1(2q) and later
CSCvi69269	When values under a custom QoS policy change, the changes are not reflected under the service graph that is attached to the profile.	3.1(2o) and later
CSCvi80543	This is an enhancement that allows failover ordering, categorizing uplinks as active or standby, and categorizing unused uplinks for each EPG in VMware domains from the APIC.	3.1(2o) and later
CSCuu17314	CDP is not enabled on the management interfaces for the leaf switches and spine switches.	3.1(2m) and later
CSCvd43548	The stats for a given leaf switch rule cannot be viewed if a rule is double-clicked.	3.1(2m) and later
CSCvd66359	The Port ID LLDP Neighbors panel displays the port ID when the interface does not have a description. Example: Ethernet 1/5, but if the interface has description, the Port ID property shows the Interface description instead of the port ID.	3.1(2m) and later
CSCve84297	A service cannot be reached by using the APIC out-of-band management that exists within the 172.17.0.0/16 subnet.	3.1(2m) and later
CSCvf32908	When using mongoDB for Cisco ACI apps, the app must be deleted before the upgrade and reinstalled after the upgrade to avoid corruption of application data.	3.1(2m) 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]	3.1(2m) and later

Bug ID	Description	Exists in
CSCvf70411	A route will be advertised, but will not contain the tag value that is set from the VRF route tag policy.	3.1(2m) and later
CSCvg00627	A tenant's flows/packets information cannot be exported.	3.1(2m) 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.	3.1(2m) and later
CSCvg37617	The zoning rule installation incorrectly permitted all of the traffic to and from the L3Out to EPG as the default permit without redirecting the traffic to the service node.	3.1(2m) and later
CSCvg60565	If a service graph is initially configured as uni-directional and later a filter is added and the service graph is made bi-direction, the service graph enters a faulty state.	3.1(2m) and later
CSCvg67522	When two different service chains (one for IPv4 traffic and the other for IPv6 traffic) are using the same exact forwarding path (the same bridge domain and VLAN on the service nodes), but different redirect policies (one for IPv4 and the other for IPv6), then the IP SLA objects might not be cleaned up when the contract is detached from the service graph.	3.1(2m) and later
CSCvg70246	When configuring an L3Out under a user tenant that is associated with a VRF instance that is under the common tenant, a customized BGP timer policy that is attached to the VRF instance is not applied to the L3Out (BGP peer) in the user tenant.	3.1(2m) and later
CSCvg74082	A newly-created VFC shows the admin state as down.	3.1(2m) and later
CSCvg79436	In Cloud Orchestrator Mode, dual stack (that is, IPv4 and IPv6) cannot be configured on the same interface.	3.1(2m) and later
CSCvg81020	For strict security requirements, customers require custom certificates that have RSA key lengths of 3072 and 4096.	3.1(2m) and later
CSCvg82738	Whenever a user expands a drop-down list that has many policies (>10K), the GUI tries to show all of them at once, which causes a timeout from the server, after which the server tries again. This process continues and the GUI becomes unresponsive.	3.1(2m) and later
CSCvg82990	The Cisco AVS DPA process might crash on AVS after upgrading to a 3.1.x release. This does not always occur. When it does occur, the DPA process restarts automatically.	3.1(2m) and later

Bug ID	Description	Exists in
CSCvg84464	There is an exhaustion of LPM entries due to the programming of an unnecessary EPG subnet gateway IP address.	3.1(2m) and later
CSCvh13127	There is an issue with upgrading in the following situation: ■ A node is decommissioned a few hours before initiating an upgrade. ■ An upgrade is triggered with the "doNotPause" flag turned on in the maintenance group. ■ The node is in the maintenance group that is being upgraded. In this situation, the upgrade stalls while waiting for that node to complete the upgrade.	3.1(2m) and later
CSCvh17321	On decommissioning and recomissioning of the Cisco APICs or nodes, extra prefix white list entries might be created on the TOR switches.	3.1(2m) and later
CSCvh52046	This is an enhancement to allow for text-based banners for the Cisco APIC GUI login screen.	3.1(2m) and later
CSCvh59843	Enabling Multicast under the VRF on one or more bridge domains is difficult due to how the drop-down menu is designed. This is an enhancement request to make the drop-down menu searchable.	3.1(2m) and later
CSCvi20535	When a VRF table is configured to receive leaked external routes from multiple VRF tables, the Shared Route Control scope to specify the external routes to leak will be applied to all VRF tables. This results in an unintended external route leaking. This is an enhancement to ensure the Shared Route Control scope in each VRF table should be used to leak external routes only from the given VRF table.	3.1(2m) and later
CSCvi41092	The APIC log files are extremely large, which takes a considerable amount of time to upload, especially for users with slow internet connectivity.	3.1(2m) and later
CSCvi82903	When authenticating with the Cisco APIC using ISE (TACACS), all logins over 31 characters fail.	3.1(2m) and later
CSCvj56726	The connectivity filter configuration of an access policy group is deprecated and should be removed from GUI.	3.1(2m) and later
CSCvj76503	A maintenance window triggered for an upgrade remains active for an unlimited time. Adding another node to this maintenance window automatically upgrades this newly added node. In some releases, such as 3.1(2m), a message may say that the window is triggered from X to Y time period; however, the maintenance window is still active for an unlimited time.	3.1(2m) and later
CSCvn00576	An SHA2 CSR for the ACI HTTPS certificate cannot be configured in the APIC GUI.	3.1(2m) and later

Bug ID	Description	Exists in
CSCvn15374	When upgrading Cisco APICs, constant heartbeat loss is seen, which causes the Cisco APICs to lose connectivity between one another. In the Cisco APIC appliance_director logs, the following message is seen several hundred times during the upgrade: appliance_director||DBG4||...||Lost heartbeat from appliance id= ... appliance_director||DBG4||...||Appliance has become unavailable id= ... On the switches, each process (such as policy-element) see rapidly changing leader elections and minority states: adrs_rv||DBG4|||Updated leader election on replica=(6,26,1)	3.1(2m) 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	3.1(2m) 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	3.1(2m) and later
CSCvq43101	When opening an external subnet, a user cannot see Aggregate Export/Import check boxes set in GUI even though they were already configured.	3.1(2m) 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.	3.1(2m) and later
CSCvr65035	The last APIC in the cluster gets rebooted when APIC-1 is decommissioned due to some issue seen on APIC-1 while upgrading. In addition, after decommissioning APIC-1, the other APICs still wait for APIC-1 to get upgraded.	3.1(2m) and later
CSCvr94614	There is a minor memory leak in svc_ifc_policydist when performing various tenant configuration removals and additions.	3.1(2m) and later
CSCvu21530	Protocol information is not shown in the GUI when a VRF table from the common tenant is being used in any user tenant.	3.1(2m) and later
CSCvu62465	For an EPG containing a static leaf node configuration, the Cisco APIC GUI returns the following error when clicking the health of Fabric Location: Invalid DN topology/pod-X/node-Y/local/svc-policyelem-id-0/ObservedEthIf, wrong rn prefix ObservedEthIf at position 63	3.1(2m) and later
CSCvv62861	A leaf switch reloads due to an out-of-memory condition after changing the contract scope to global.	3.1(2m) and later
CSCvw33061	Traffic loss is observed from multiple endpoints deployed on two different vPC leaf switches.	3.1(2m) and later
CSCvj29916	VMs on ESXi hosts running Cisco AVS software are unable to join the network. When running the "vemcmd show port" command, you can see that the VM is stuck in a "BLK" state with reason of "WAIT EPP."	3.1(2m)
CSCvj75897	A fault is raised that specifies problem that occurred while retrieving tagging information for a VMM controller. Inventory pull from the VMware vCenter takes a long time (>10 minutes) and it continuously completes with a partial inventory result. The processing of events from VMware vCenter is delayed, which may result in delays for the downloading of policies to the leaf switches when EPGs are deployed on-demand at the VMM domain. This would affect connectivity for newly deployed VMs or VMs which have been vMotioned.	3.1(2m)

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
CSCvj41914	An OpflexP core is seen on the leaf switch or spine switch. The leaf switch or spine switch will recover from this, and there should be no impact other than this core being generated and the the service being restarted.	3.1(2s)
CSCvj91044	There is an opflexp core in stats update. The opflexp process should recover and there should be no service impact.	3.1(2s)
CSCvj75897	A fault is raised that specifies problem that occurred while retrieving tagging information for a VMM controller. Inventory pull from the VMware vCenter takes a long time (>10 minutes) and it continuously completes with a partial inventory result. The processing of events from VMware vCenter is delayed, which may result in delays for the downloading of policies to the leaf switches when EPGs are deployed on-demand at the VMM domain. This would affect connectivity for newly deployed VMs or VMs which have been vMotioned.	3.1(2q)
CSCvj77609	In the 3.1 release, whenever the Cisco APIC detects an inconsistency with the port group attributes on VMware vCenter and Cisco APIC, the Cisco APIC re-pushes the port group attributes to resolve the inconsistency. This breaks vArmor integration assumptions, as prior to the 3.1 release the Cisco APIC only raised a fault whenever there was an inconsistency, but the port group attributes did not get re-pushed.	3.1(2q)
CSCvh97620	After deleting a bridge domain and creating a new bridge domain that uses the same subnet, the Cisco APIC generates a fault on the bridge domain stating that there is already another bridge domain with the same subnet within the same VRF instance. The error is similar to the following example: Fault delegate: BD Configuration failed for [BD_NEW_dn] due to duplicate-subnets-within-ctx: [BD_OLD_dn]	3.1(2p)
CSCvi77600	A crash occurs during the retrieval of vSphere tag information from VMware vCenter.	3.1(2p)
CSCvi86103	There are duplicate PVLAN entries in VMware vCenter. Depending on the version of Cisco APIC code, the Cisco APIC's vmmmgr process will also crash and create a core file.	3.1(2p)
CSCvj12441	VM ports do not come up after being connected or after other host/VM events, such as host/VM getting disconnected, and then reconnected.	3.1(2p)
CSCvj21756	Ports are stuck in wait EPP/ACK.	3.1(2p)
CSCvg21295	On configuring the same encapsulation (External SVI) and different IP address subnet on different border leaf switches, the configuration gets rejected.	3.1(2o)

Bug ID	Description	Fixed in
CSCvh42067	The Cisco APIC does not send varbind timeticks in traps.	3.1(2o)
CSCvi09430	QoS values are not preserved when a service graph is rendered.	3.1(2o)
CSCvi29916	VMs on ESXi hosts running Cisco AVS software are unable to join the network. When running the "vemcmd show port" command, you can see that the VM is stuck in a "BLK" state with reason of "WAIT EPP."	3.1(2o)
CSCvi56652	QoS values are not preserved when a service graph is rendered.	3.1(2o)
CSCvi75240	Duplicate Address Detection (DAD) disables the secondary IPv6 address if the user configures a shared IPv6 address on a Layer 3 SVI.	3.1(2o)
CSCvi87761	The policy element creates a stale entry for the out-of-band management next-hop.	3.1(2o)
CSCvi91875	The port property is required for the snmpTrapFwdServerP class.	3.1(2o)
CSCvf92483	This issue occurs while using the import-config file command on the CLI where the file is the output of export-config command. The file contains the output of show running-config of the scope where export-config was executed. The error occurs only when the file contains crypto commands, the Bash shell throws the error and hangs without returning the prompt.	3.1(2m)
CSCvg02551	When the IS-IS to OSPF Multi-Site CPTEP route leaking is not programmed, inter-site BGP session might go down on the spine switch. This behavior might cause traffic drop.	3.1(2m)
CSCvg29330	The incorrect information displays on the topology for the OpenStack compute node.	3.1(2m)
CSCvg53205	A fault for a 100% drop rate is observed for an endpoint-to-external IP address atomic counters policy after disabling/enabling a switch.	3.1(2m)
CSCvg56414	An external IP address-to-external IP address atomic counters policy does not give the results for the flow that matches the configured external IP addresses.	3.1(2m)
CSCvg60014	Clicking the Submit button in a wizard will fail if any of the entered values are invalid.	3.1(2m)
CSCvg64560	When installing the Hyper-V agent, MSI gives the following error: "This application is only supported on English language version of Windows server 2012, or higher operating system."	3.1(2m)
CSCvg67592	The FEX access policy is not in Configured Access Policies under the EPG.	3.1(2m)
CSCvg71915	When the fabric ID is changed in the sam.config file and the Cisco APIC is rebooted, if DHCP discovery reaches the Cisco APIC before it reaches the node identity policy, a fault for the wrong fabric gets generated.	3.1(2m)
CSCvg73647	The "fabric <node> <command>" command cannot be run from the Cisco APIC to any switch because the output shows.	3.1(2m)
CSCvg75150	A service graph is in the applied state even if the VRF instance associated with the consumer EGP or consumer-facing service node EPG gets deleted.	3.1(2m)
CSCvg77689	In a Multipod setup, if a node with a looseNode is moved from one pod to another, the fabricLooseNode policy associated with previous pod does not get deleted and causes a "Specified node not present in the specified pod - fault-F2547" fault. The fault is harmless and does not depict any functional failure.	3.1(2m)

Bug ID	Description	Fixed in
CSCvg81853	When looking at the Encap Already In Use fault (F0467), debugMessage is blank.	3.1(2m)
CSCvg82489	The warning messages on the creation wizards for "Fabric - Access Policies - Switch Policies - Policies - Forwarding Scale Profile", "Fabric - Access Policies - Switch Policies - Policy Groups - Leaf Policy groups - modify Forward Scale Profile Policy", and "Fabric - Access Policies - Switch Policies - Profiles - Leaf Profiles" are outdated.	3.1(2m)
CSCvg86073	With a 0.0.0.0/0 subnet and a specific subnet with an import route-map, the GUI shows only a 212.1.0.0/24 subnet.	3.1(2m)
CSCvg87788	An inconsistent configuration involving the l3extRsPathL3OutAtt managed object with ifInstT="ext-svi" might be accepted.	3.1(2m)
CSCvg93599	The svc_ifc_plgnhandler in /data/volume is not auto rotated, which causes /data/log to be almost full and raises an alert on the Cisco APIC.	3.1(2m)
CSCvg95080	A remote leaf switch TEP pool is not getting deleted if the remote leaf switches are decommissioned before deleting the vPC.	3.1(2m)
CSCvg95130	Connectivity from all VMs needing to go through the fabric is lost. The Hyper-V agent logs might show information indicating that it is still trying to connect to the old TEP IP address (pre-replacement) as opposed to the new one (post-replacement).	3.1(2m)
CSCvh00839	On importing an exported configuration, the import will succeed and might report a warning about a failure to extract the CISCO.CloudMode.1.0.zip archive. If the CISCO.CloudMode.1.0 device package was deleted, it will not be restored on import.	3.1(2m)
CSCvh02537	The IpCktEp policy might not be propagated to the leaf switch even after the policy has been configured properly on the Cisco APIC.	3.1(2m)
CSCvh07062	There will be fault in the Cisco APIC for a remote leaf switch after upgrading the Cisco APIC upgrade or decommissioning and recommissioning the Cisco APIC.	3.1(2m)
CSCvh07097	The acked fault count is incorrect under following circumstances: • Fault that was already acknowledged gets cleared. • Acknowledge only the fault instance or the associated fault delegate.	3.1(2m)
CSCvh07996	There are duplicate CoPP rules in the TCAM.	3.1(2m)
CSCvh08044	In the case where the user posts policies to download a specific image version and also to upgrade to that version in quick succession before waiting for the image to get downloaded, the current running catalog gets picked up for checking the compatibility. In the event where the current running catalog does not support the newly requested version of the image, the upgrade will fail with the message "version not compatible," even though the user would expect compatibility.	3.1(2m)
CSCvh10960	Upon restoration of a configuration, if there are many (>100) interface policy groups associated to a single AEP, the full restoration takes hours. Similar problems can be seen with other mass associations on the fabric.	3.1(2m)
CSCvh11314	There are inventory sync failure faults and various VMM faults for the affected VMM domain.	3.1(2m)

Bug ID	Description	Fixed in
CSCvh12315	The Cisco APIC will not allow the deletion of a remote leaf switch or POD TEP pool if there are any dhcpClient managed objects present with an IP address that is assigned from that TEP pool.	3.1(2m)
CSCvh13005	The DNS policy is designed as per ctx/vrf, but when it comes to the Cisco APIC, only the default DNS profile can be used.	3.1(2m)
CSCvh16532	When attempting to log into the Cisco APIC GUI, you might receive the error "AAA Server Authentication DENIED." You might also see the following message in a network trace when the LDAP server responds to the Cisco APIC's search query: "In order to perform this operation a successful bind must be completed."	3.1(2m)
CSCvh16963	Shell commands cannot be executed.	3.1(2m)
CSCvh17075	If many unreachable stats export destinations are configured, the observer element on a switch might dump a core and restart.	3.1(2m)
CSCvh17864	The STP policy does not change or has mixed behavior after switching to another policy or reverting to the default policy.	3.1(2m)
CSCvh18069	An iACL entry with a subnet mask of 0 or 32 is not allowed in the CoPP Pre-Filter creation wizard in the GUI.	3.1(2m)
CSCvh18128	Under VM Networking > Microsoft > [SCVMM Domain] > Controllers > [SCVMM Controller] > DVS - apicVswitch_[name] > Portgroups > apicInfra_[name], the IP addresses display as 0.0.0.0 under the Management Network Adapters, even though the Hyper-V host has an IP address assigned through DHCP in the infra network for the VTEP interface.	3.1(2m)
CSCvh51665	Fault F1313 is triggered that affects a VMNIC on an AVS-integrated hypervisor. The fault states the following error in the fault description: [API call for adding VNic failed.]	3.1(2m)
CSCvh55609	When importing a configuration that includes an EPG whose bridge domain is associated with VRF "copy" (fvRsCtx=copy), the import completes, but tn-common will be corrupted.	3.1(2m)

Known Behaviors

This section lists bugs that describe known behaviors. Click the Bug ID to access the Bug Search Tool and see additional information about the bug. The "Exists In" column of the table specifies the 3.1(2) releases in which the known behavior exists. A bug might also exist in releases other than the 3.1(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.	3.1(2m) 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.	3.1(2m) and later
CSCuo79250	The node ID policy can be replicated from an old appliance that is decommissioned when it joins a cluster.	3.1(2m) and later
CSCup47703	The DSCP value specified on an external endpoint group does not take effect on the filter rules on the leaf switch.	3.1(2m) and later
CSCup79002	The hostname resolution of the syslog server fails on leaf and spine switches over in-band connectivity.	3.1(2m) and later
CSCuq21360	Following a FEX or switch reload, configured interface tags are no longer configured correctly.	3.1(2m) and later
CSCur39124	Switches can be downgraded to a 1.0(1) version if the imported configuration consists of a firmware policy with a desired version set to 1.0(1).	3.1(2m) and later
CSCur71082	If the Cisco APIC is rebooted using the CIMC power reboot, the system enters into fsck due to a corrupted disk.	3.1(2m) and later
CSCus15627	The Cisco APIC Service (ApicVMMService) shows as stopped in the Microsoft Service Manager (services.msc in control panel > admin tools > services). This happens when a domain account does not have the correct privilege in the domain to restart the service automatically.	3.1(2m) and later
CSCut51929	The traffic destined to a shared service provider endpoint group picks an incorrect class ID (PcTag) and gets dropped.	3.1(2m) and later
CSCuu09236	Traffic from an external Layer 3 network is allowed when configured as part of a vzAny (a collection of endpoint groups within a context) consumer.	3.1(2m) and later
CSCuu61998	Newly added microsegment EPG configurations must be removed before downgrading to a software release that does not support it.	3.1(2m) and later
CSCuu64219	Downgrading the fabric starting with the leaf switch will cause faults such as policy-deployment-failed with fault code F1371.	3.1(2m) and later
CSCuw34026	If the "Remove related objects of Graph Template" wizard is used in the Cisco APIC GUI, the Cisco APIC does not clean up objects that are in other tenants.	3.1(2m) and later

Bug ID	Description	Exists in
CSCuw81638	The OpenStack metadata feature cannot be used with Cisco ACI integration with the Juno release (or earlier) of OpenStack due to limitations with both OpenStack and Cisco's ML2 driver.	3.1(2m) and later
CSCva32534	Creating or deleting a fabricSetupP policy results in an inconsistent state.	3.1(2m) and later
CSCva60439	After a pod is created and nodes are added in the pod, deleting the pod results in stale entries from the pod that are active in the fabric. This occurs because the Cisco APIC uses open source DHCP, which creates some resources that the Cisco APIC cannot delete when a pod is deleted.	3.1(2m) 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.	3.1(2m) and later
CSCva97082	When downgrading to a 2.0(1) release, the spines and its interfaces must be moved from infra L3out2 to infra L3out1. After infra L3out1 comes up, delete L3out2 and its related configuration, and then downgrade to a 2.0(1) release.	3.1(2m) and later
CSCvb39702	No fault gets raised upon using the same encapsulation VLAN in a copy device in tenant common, even though a fault should get raised.	3.1(2m) and later
CSCvg41711	In the leaf mode, the command "template route group <group-name> tenant <tenant-name>" fails, declaring that the tenant passed is invalid.	3.1(2m) and later
CSCvg79127	When First hop security is enabled on a bridge domain, traffic is disrupted.	3.1(2m) and later
CSCvg81856	Cisco ACI Multi-Site Orchestrator BGP peers are down and a fault is raised for a conflicting rtrId on the fvRtdEpP managed object during L3extOut configuration.	3.1(2m) and later
CSCvh76076	The PSU SPROM details might not be shown in the CLI upon removal and insertion from the switch.	3.1(2m) 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 fault is raised for a VMware VDS, Cisco ACI Virtual Edge, or Cisco AVS VMM domain indicating that complete tagging information could not be retrieved for a controller. VMM manager logs contain multiple errors similar to the following examples:

  CURL failure: http status 503

  Error in URL: https://<*vCenterIP*>/rest/com/vmware/cis/tagging...

  This problem can occur when VMware vCenter is running as a service on Microsoft Windows Server 2008 R2 and the data center where the VMM domain is deployed has more than 100 VMware vSphere tags defined.

  This a known issue in the Windows TCP stack when VMware vCenter runs on Windows Server 2008 and many requests are sent to the server. See the VMware KB topic KB2033822 (https://kb.vmware.com/s/article/2033822). The KB topic includes a workaround provided by Microsoft.

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.x. For more information about guidelines for upgrading VMware DVS from 5.x to 6.x and VMM integration, see the *Cisco ACI Virtualization Guide, Release 3.1(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

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

Hardware Compatibility Information

This release supports the following Cisco APIC servers:

Product ID	Description
APIC-L1	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1000 edge ports)

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

The following list includes general hardware compatibility information:

- For the supported hardware, see the *Cisco NX-OS Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches, Release 13.1(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.
- Connecting the Cisco APIC (the controller cluster) to the Cisco ACI fabric requires a 10G interface on the Cisco ACI leaf switch. You cannot connect the Cisco APIC directly to the Cisco N9332PQ ACI leaf switch, unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the Cisco N9332PQ switch auto-negotiate to 10G without requiring any manual configuration.
- The Cisco N9K-X9736C-FX (ports 29 to 36) and Cisco N9K-C9364C-FX (ports 49-64) switches do not support 1G SFPs with QSA.
- Cisco N9K-C9508-FM-E2 fabric modules must be physically removed before downgrading to releases earlier than Cisco APIC 3.0(1).
- The fifth Cisco N9K-C9508-FM-E2 (also defined as FM-25) is not supported.
- 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 13.1(2)
  - Cisco AVS, Release 5.2(1)SV3(3.21)

    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 ACI Virtual Edge 1.1(2a)
  - 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.
- This release supports the following firmware:
  - 2.0(3i) CIMC HUU ISO
  - 2.0(9c) CIMC HUU ISO
  - 2.0(13i) CIMC HUU ISO
  - 3.0(3f) CIMC HUU ISO
- This release supports the partner packages specified in the *L4-L7 Compatibility List Solution Overview* document at the following URL:

  https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/solution-overview-listing.html
- A known issue exists with the Safari browser and unsigned certificates, which applies when connecting to the Cisco APIC GUI. For more information, see the *Cisco APIC Getting Started Guide*.
- For compatibility with OpenStack and Kubernetes distributions, see the *Cisco Application Policy Infrastructure Controller OpenStack and Container Plugins, Release 3.1(2), Release Notes.*

Usage Guidelines

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

Virtualization Compatibility Guidelines

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

- Do not separate virtual port channel (vPC) member nodes into different configuration zones. If the nodes are in different configuration zones, then the vPCs' modes become mismatched if the interface policies are modified and deployed to only one of the vPC member nodes.
- If you are upgrading VMware vCenter 6.0 to vCenter 6.5, you should first delete the following folder on the VMware vCenter: C:\ProgramData\cisco_aci_plugin.

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

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

  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.
- When creating a vPC domain between two leaf switches, both switches must be in the same switch generation. Switches not in the same generation are not compatible vPC peers. The generations are as follows:
  - Generation 1—Cisco Nexus 9200 and 9300 platform switches without "EX" on the end of the switch name; for example, Cisco Nexus 93120TX.
  - Generation 2—Cisco Nexus 9300-EX and FX platform switches; for example, Cisco Nexus 93108TC-EX.
- The following Red Hat Virtualization (RHV) guidelines apply:
  - We recommend that you use release 4.1.6 or later.
  - Only one controller (compCtrlr) can be associated with a Red Hat Virtualization Manager (RHVM) data center.
  - Deployment immediacy is supported only as pre-provision.
  - IntraEPG isolation, micro EPGs, and IntraEPG contracts are not supported.
  - Using service nodes inside a RHV domain have not been validated.

GUI Guidelines

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

- The Cisco APIC GUI includes an online version of the Quick Start Guide that includes video demonstrations.

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

  APIC_URL/indexSimple.html

CLI Guidelines

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

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

Layer 2 and Layer 3 Configuration Guidelines

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

- For Layer 3 external networks created through the API or GUI and updated through the CLI, protocols need to be enabled globally on the external network through the API or GUI, and the node profile for all the participating nodes needs to be added through the API or GUI before doing any further updates through the CLI.
- When configuring two Layer 3 external networks on the same node, the loopbacks need to be configured separately for both Layer 3 networks.
- 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.
- 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 and OpenShift Integration*
- *Cisco ACI and Red Hat Virtualization Integration*
- *Cisco ACI Virtual Edge Configuration Guide*
- *Cisco ACI Virtual Edge Installation Guide*
- *Cisco ACI Virtual Edge Release Notes, Release 1.0(1)*
- *Cisco ACI Virtualization Guide, Release 3.1(2)*
- *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 3.1(2)*
- *Cisco Application Policy Infrastructure Controller OpenStack and Container Plugins Release 3.1(2) Release Notes*
- *Cisco AVS Configuration Guide*
- *Cisco AVS Installation Guide*
- *Cisco AVS Release Notes*
- *Verified Scalability Guide for Cisco APIC, Release 3.1(2) and Cisco Nexus 9000 Series ACI-Mode Switches, Release 13.1(2)*