Cisco Application Policy Infrastructure Controller Release Notes, Release 6.0(2)

Introduction

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

This document describes the features, issues, and limitations for the Cisco APIC software. For the features, issues, and limitations for the Cisco NX-OS software for the Cisco Nexus 9000 series switches, see the Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 16.0(2).

For more information about this product, see " Related Content."

Date	Description
June 16, 2024	In the Miscellaneous Compatibility Information section, added support for 4.3.2.250016 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3).
May 1, 2024	In the Miscellaneous Compatibility Information section, added support for 4.3.2.240009 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) and UCS C225 M6 (APIC-L4/M4)
August 2, 2023	Release 6.0(2j) became available. Added the resolved bugs for this release.
July 5, 2023	In the Related Content section, added information about the APIC REST API Configuration Procedures document on developer.cisco.com.
June 21, 2023	In the Miscellaneous Compatibility Information section, added: • 4.2(3e) CIMC HUU ISO (recommended) for UCS C225 M6 (APIC-L4/M4)
March 1, 2023	Release 6.0(2h) became available.

New Software Features

Product Impact	Feature	Description
Base Functionality	Support for Cisco APIC virtual form factor in ESXi	You can deploy a Cisco APIC cluster wherein all the Cisco APICs in the cluster are virtual APICs. You can deploy a virtual APIC on an ESXi using the OVF template. For more information, see the Deploying Cisco Virtual APIC Using VMware vCenter document.
	Support for Cisco APIC cloud form factor using AWS	You can deploy a Cisco APIC cluster wherein all the Cisco APICs in the cluster are virtual APICs. You can deploy a virtual APIC on AWS using the CloudFormation template. For more information, see the Deploying Cisco Virtual APIC Using AWS document.
	BGP additional paths	The BGP speaker can propagate and receive multiple paths for the same prefix without the new paths replacing any previous paths. This feature allows BGP speaker peers to negotiate whether they support advertising and receiving multiple paths per prefix and advertising such paths. Cisco APIC supports only the receive functionality. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 6.0(x).

Product Impact	Feature	Description
	Proportional ECMP	You can use the next-hop propagate and redistribute attached host features to avoid sub-optimal routing in the Cisco ACI fabric. When these features are enabled, packet flows from a non-border leaf switch are forwarded directly to the leaf switch connected to the next-hop address. All next-hops are now used for ECMP forwarding from the hardware. In addition, Cisco ACI now redistributes ECMP paths into BGP for both directly connected next-hops and recursive next-hops. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 6.0(x).
	Support for config stripe winner policies	When you configure the Layer 3 IPv4 multicast, you can now configure the config stripe winner policy for a multicast group range within a pod. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 6.0(x).
Security	First hop security (FHS) support for VMM	FHS is supported on the VMware DVS VMM domain. Ensure to enable intra EPG isolation for implementing FHS within an EPG. For more information, see the Cisco APIC Security Configuration Guide, Release 6.0(x).
	TACACS external logging for switches	You can enable TACACS external logging for switches. When enabled, the Cisco APIC collects the same types of AAA data from the switches in the chosen TACACS monitoring destination group. For more information, see the Cisco ACI TACACS External Logging.
Performance and Scalability	Scale enhancements	• 10,000 VRF instances per fabric • Mis-Cabling Protocol (MCP): 2,000 VLANs per interface and 12,000 logical ports (port x VLAN) per leaf switch • 200 IP SLA probes per leaf switch • 24 leaf switches (12 pairs) in the same L3Out • 2,000 sub-interfaces (BGP, OSPF, and static) • 2,000 bidirectional forwarding detection (BFD) sessions • Longest Prefix Matches (LPM): 440,000 IPv4 and 100,000 IPv6 routes
Upgrade/Downgrade	Auto firmware update for Cisco APIC on discovery	When you add a new Cisco APIC to the fabric either through Product Returns & Replacements (RMA), cluster expansion, or commission, it is automatically upgraded to the same version of the existing cluster. For more information, see the the Cisco APIC Installation and ACI Upgrade and Downgrade Guide.
	Installing switch software maintenance upgrade patches without reloading	Some switch software maintenance upgrade (SMU) patches do not require you to reload the switch after you install those patches. For more information, see the Cisco APIC Installation and ACI Upgrade and Downgrade Guide.
Interoperability	Cisco Nexus Cloud support	This release adds support for Cisco Nexus Cloud, which enables telemetry collection from the Cisco Nexus switches. For more information, see the Cisco Nexus Cloud documentation.
Ease of Use	Troubleshooting Cisco APIC QoS Policies	You can view the QoS statistics by using the Cisco APIC GUI. For more information, see the Cisco APIC and QoS document.

New Hardware Features

- This release adds support for the APIC-L4 and APIC-M4 servers. For more information, see the Cisco APIC M4/L4 Server Installation and Service Guide.
- For the new ACI-mode switch hardware features, see the Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 16.0(2).

Changes in Behavior

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

Open Issues

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 6.0(2) releases in which the bug exists. A bug might also exist in releases other than the 6.0(2) releases.

Bug ID	Description	Exists in
CSCvg81020	For strict security requirements, customers require custom certificates that have RSA key lengths of 3072 and 4096.	6.0(2h) and later
CSCvm56946	Support for local user (admin) maximum tries and login delay configuration.	6.0(2h) and later
CSCvt99966	A SPAN session with the source type set to "Routed-Outside" goes down. The SPAN configuration is pushed to the anchor or non-anchor nodes, but the interfaces are not pushed due to the following fault: "Failed to configure SPAN with source SpanFL3out due to Source fvIfConn not available".	6.0(2h) and later
CSCvy40511	Traffic from an endpoint under a remote leaf switch to an external node and its attached external networks is dropped. This occurs if the external node is attached to an L3Out with a vPC and there is a redistribution configuration on the L3Out to advertise the reachability of the external nodes as direct-attached hosts.	6.0(2h) and later
CSCwa58709	The GIPo address is only visible on APIC 1 when using the command "cat /data/data_admin/sam_exported.config". The command output from the other APICs outputs do not show the GIPo address.	6.0(2h) and later
CSCwd26277	When deploying a service graph, the dialog does not list all bridge domains for the provider connector. This issue is observed when you enter or edit the bridge domain name in the consumer connector field. After this, the provider connector will only list the bridge domain that is selected by the consumer connector field.	6.0(2h) and later
CSCwd81562	A Cisco APIC that was previously part of the Cisco APIC cluster will not rejoin the cluster after the reload, decommission, and commission process.	6.0(2h) and later
CSCwd82212	There is a login denied error while importing or exporting a configuration.	6.0(2h) and later
CSCwe01680	User is not allowed to configure static route for an inband EPG which is not deployed on the current APIC.	6.0(2h) and later

Bug ID	Description	Exists in
CSCwe13941	Following are some of the symptoms seen because of this issue : 1. Failure to verify APIC's CIMC credentials. 2. Failure to verify the power status. 3. Failure to verify the serial number of the APIC as seen in CIMC. These symptoms can be seen during the following workflows: 1. APIC Cluster Initial Bootstrap. 2. Adding a new APIC to the cluster - Expansion. 3. Replacing an APIC in the cluster - RMA operation. 4. Recommission of APIC following a decommission.	6.0(2h) and later
CSCwe39842	PXE boot for vmedia installation of the Cisco APIC 6.0(2) release does not work on APIC-SERVER-M2/M3/L2/L3.	6.0(2h) and later
CSCwe41446	When APICs are upgraded to the 6.0(2) release and switches are still on older releases, the upgraded standby Cisco APIC cannot join the cluster.	6.0(2h) and later
CSCwe46071	A leaf node gets stuck in bootstrap. Although bootstrap eventually gets forced completed, the node might not download the entire expected configuration, resulting in a node that is not fully functional.	6.0(2h) and later
CSCwe47966	SMU installation fails in the 6.0(2) release due to collecting the techsupport files prior to installing the SMU.	6.0(2h) and later
CSCwe52465	The NICC app image fails to load.	6.0(2h) and later
CSCwe58398	This is added functionality for upgrade show command. 1. acidiag show postupgrade -service <dme> -> This gives details for dmes and which shard still have pending postUpgradeCb. 2.acidiag show postupgrade -service <dme> -shard <shard_id> -> This gives the details of log path for the dmes and shard for which postUpgradeCb has been completed.	6.0(2h) and later
CSCwe92155	After configuring syslog using TCP on port 59500, the logit was sent out normally and netstat showed that it was established. However, after aborting the connection from the syslog server side, the TCP connection went from ESTABLISHED to CLOSE_WAIT and disappeared from the APIC side.	6.0(2h) and later
CSCwe93045	There is general slowness when an application contacts the Cisco APIC cluster through the REST API. The same slowness is experienced when accessing using the Cisco APIC GUI.	6.0(2h) and later
CSCwf16927	The system time does not reflect the daylight saving adjustments done in Egypt for releases prior to 5.3.1 and 6.0.4	6.0(2h) and later
CSCwf54771	User configuration is missing on APICs and switches following an ungraceful reload or power outage.	6.0(2h) and later

Bug ID	Description	Exists in
CSCwf55317	1. Go to **Tenant > Application Profile > Topology**. 2. Drag and drop a contract. Problem 1: No pop up displays. Drag and drop an EPG icon, then cancel the create view. Problem 2: The pop up remains open.	6.0(2h) and later
CSCwf59938	Fault code F1414 is triggered and cleared manually. After certain time, the fault is triggered again. This issue occurs when using the syslog server FQDN.	6.0(2h) and later
CSCwf72015	vAPICs hosted on ESXi hosts directly connected to the fabric must see the leaf switch using LLDP. Hosts cannot be connected by an intermediate switch, including UCS Fabric Interconnects. This applies to vAPIC clusters and vAPICs used in ACI mini deployments.	6.0(2h) and later
CSCwf92856	During upgrade " deserialization error" is seen on APIC 1 PD.	6.0(2h) and later
CSCwf94095	When attempting to authenticate using the CLI or HTTPS to an APIC running release 6.0(2h), any of the APICs in the cluster will randomly fail authentication one out of three times, and sometimes two out of three times. The CLI or GUI presents an " access denied" error, causing the user to believe a password may have been entered incorrectly. However, when this error occurs, a packet capture reveals that the APIC never sources an authentication request to the TACACS server.	6.0(2h) and later
CSCwh05135	Override vpc interface policy doesnot consistently take precedence over regular vpc interface policy.Upon a leaf reload, its quite random which policy takes precedence, and accordingly the vlans get programmed.If the override or regular AEP is missing the relevant domain association/vlans, then those vlans are not programmed causing outages.	6.0(2h) and later
CSCwh07037	An outage occurred because traffic coming from the TEPs was dropped by the receiving leaf switches with INFRA_ENCAP_SRC_TEP_MISS.	6.0(2h) and later
CSCwh17898	The " panic: runtime error: invalid memory address or nil pointer dereference." Error occurred and then F1419 (Service kron failed on apic) was raised.	6.0(2h) and later
CSCwh18649	Inter-pod/Inter-site BGP peer is incorrectly marked as " manual,wan" under the BGP for the peer managed object of a spine switch.	6.0(2h) and later
CSCwh28834	The " show running config" command does not work in the APIC CLI and generates the following errors: Error while processing mode: interface Error while processing mode: leaf Error while processing mode: configure Error: ERROR occurred: <class 'xml.etree.ElementTree.ParseError'>, not well-formed (invalid token): line 1, column 51242, File " /mgmt/opt/controller/yaci/yaci/_cfg.py" , line 18, in _execute_func subCmd.runningConfig(ctx, **kwargs)	6.0(2h) and later
CSCwh41632	Enhancement - show apic upgrade complete only after postUpgradeCb is done	6.0(2h) and later
CSCwh41865	When upgrading an APIC, the " from" version is displayed as " to" version in the event record.	6.0(2h) and later

Bug ID	Description	Exists in
CSCwh44987	When a non-default OOB management EPG is configured and a default one is removed from the configuration, the default EPG will be recreated automatically after a fabric upgrade. This is causes fault F0523 " Configuration failed for EPG default due to Not Associated With Management Zone" .	6.0(2h) and later
CSCwh47794	The ACI VMM Tags tab returns " the server returned unintelligible response" message even though the tag is retrievable using the CLI.	6.0(2h) and later
CSCwh53706	In scale setups, when there are more than the usual number of objects and if the user tries to load the Capacity Dashboard page, the page times out. A few queries that are hit from the browser and the page become stuck for few seconds.	6.0(2h) and later
CSCwh53727	The API call /mqapi2/deployment.query.json?mode=getvmmCapInfo that is done against the Cisco APICs by an external management system takes too long to process.	6.0(2h) and later
CSCwh56716	When the Cisco APICs use Direct Connect to CSSM, running the " show license usage" command on APIC 1, 2, or 3 shows ACI_LEAF_ESS_10G 6 in use. When APICs 2 and 3 are restarted, this output is unchanged. When APIC 1 is restarted, the output becomes " No Licenses in use" on APICs 1, 2, and 3. The " Registering for Smart Licensing with Direct Connect to CSSM Using the GUI" process has to be done again.This was tested in the lab with Cisco APIC releases 5.2(6g), 5.2(7g), and 6.0(2j)	6.0(2h) and later
CSCwh61315	After issuing the APIC CLI " replace-controller reset x" commands, the failover status of the active controller does not change to default when checking using the 'show controller' commands.	6.0(2h) and later
CSCwh63412	Audit logs under System > History > Audit Logs are limited to the current logged in user. Only the user with the username admin can see the audit logs from all users, but other users despite having admin privileges cannot see the audit logs from other users. The audit logs under Tenants are visible to every user.	6.0(2h) and later
CSCwh67428	The GUI does not display maxSpeed and direction information in the equipment view.	6.0(2h) and later
CSCwh74484	ACI pushes the VLANs from the old VLAN pool after changing the vNIC template in the UCSM	6.0(2h) and later
CSCwh75348	Decommission an APIC causes the message " the node configuration will be wiped out from controller" to display even though the controllers still retain the user configuration.	6.0(2h) and later
CSCwh76879	Following the RMA workflow for replacing an APIC results in the APIC always having ID 1. A user should instead use the Add node workflow from the existing cluster to add the RMAed node.	6.0(2h) and later
CSCwh76885	If the CIMC is not available, out-of-band management cannot be used for BootX workflows for cluster bringup. The CIMC field should be optional so that if only OOB is configured, cluster bringup will still work.	6.0(2h) and later
CSCwh77285	OpFlex OOM crashes in leaf switches.	6.0(2h) and later
CSCwh78409	The SNMPD service failed on all Cisco APICs after configuring SNMPv3.	6.0(2h) and later

Bug ID	Description	Exists in
CSCwh81272	The system resets due to a policyelem high availability policy reset.	6.0(2h) and later
CSCwh83273	A Cisco APIC cannot be added to the cluster because the GUI rejects the ID if is not within the range of 1-7.The Initial Setup Configuration states that the fabric ID valid range is 1-128.	6.0(2h) and later
CSCwh84052	When using the OpenStack integration, the Cisco APIC VMM Manager process may consume more memory than is available and then end.	6.0(2h) and later
CSCwh87245	An edmManagedNic or compManagedNic object may be mapped to the wrong server (compHv).	6.0(2h) and later
CSCwh87458	Search Filters in Endpoint - Operational - Client Endpoints do not show up in the endpoint learning filter.	6.0(2h) and later
CSCwh95573	Fault " F4142" is raised when there is inconsistency in FNV and the idmgr database. Even though the addrAssigner in FNV is set to 0 and the corresponding " identContextElement" managed object is missing from the idmgr database, the fault gets raised.	6.0(2h) and later
CSCwh98712	When running " show running-config" from API CLI, the command takes several minutes to complete. Several thousand API requests are seen in access.log querying ptpRsProfile on every static path.	6.0(2h) and later
CSCwi01316	In the following topology: Tenant 1: VRF 1 > EPG A, EPG B. There is an any-to-any Intra VRF instance contract and EPG A and B are providers for an inter-VRF instance contract. VRF 2 > L3Out or EPG. The VRF instance consumes the inter-VRF instance contract. Traffic will unexpectedly get sent to the wrong rule when inter-VRF instance traffic is flowing.	6.0(2h) and later
CSCwi03663	Recent upgraded versions of SCP servers do not support some of the old ciphers or host key algorithms causing SCP to/from APIC to break.	6.0(2h) and later
CSCwi06427	Navigating to FABRIC -> Inventory -> Pod1 -> Operational -> Routes -> IPv6 learned routes results in the following error message:Value is not specified for the argument 'undefined'	6.0(2h) and later
CSCwi09894	In a mini ACI fabric, the physical APIC does not join the cluster after power cycling the entire setup.	6.0(2h) and later
CSCwi12992	After upgrade to ACI 5.2(8), the custom SSL certificate is not installed in the Cisco APICs and the default self-signed SSL certificate is used instead.	6.0(2h) and later
CSCwi24526	The Tech Support 2of3 was not getting collected for vAPIC properly which is the reason you see the size difference for 2of3 bw APIC and vAPIC. The other TS 1of3 and 3of3 are properly collected for vAPIC.	6.0(2h) and later
CSCwi40671	In a remote leaf switch, when the initial policy download happens, nginx generates a core. The process recovers by itself after a restart. This issue does not have any major functionality impact.	6.0(2h) and later
CSCwi52324	The fault F3227 " ACI failed processing an already accepted configuration change" continuously gets raised	6.0(2h) and later

Bug ID	Description	Exists in
CSCwi66348	A Cisco ACI switch can spend hours to complete the bootstrap process. At the worst, the expected completion time should be about 90 minutes.	6.0(2h) and later
CSCwi78474	An upgraded Cisco APIC may attempt the second upgrade to same version and assume itself as APIC 1, which can cause all Cisco APICs to stop the postUpgradeCb process, which stops the upgrade.	6.0(2h) and later
CSCwi97842	After upgrading, the Cisco APIC cluster is diverged and policymgr is down and repeatedly crashing on one Cisco APIC.	6.0(2h) and later
CSCwi99378	There are packet drops between the pods.	6.0(2h) and later
CSCwj08117	After a reboot is triggered, any of the Cisco APICs take around 1 hour to reach the cluster fully fit status and the affected DME is ifc_observer. During the issue, there is non-optimal leader for some shards for the service ifc_observer, which it clears after 30 minutes.	6.0(2h) and later
CSCwj13396	ACI switches show in maintenance with the CLI command "acidiag fnvread" on Cisco APIC, but they show "normal" in vsh and even top. System also shows In service. - Switches do not show up in the GUI nor API for configurations, as APIC vectors it as in maintenance. This severely impacts the ability to make changes. - Switches may continue to work normally even though no new configurations can be made on them.	6.0(2h) and later
CSCwj17966	The Cisco APIC bootmgr or appliance director allows an incorrect attribute/value update to be received in LLDP TLV due to miscabling.	6.0(2h) and later
CSCwj23752	Changing in the name of the remote-destination group stops the sending of syslog messages to the remote destination. Changing the port number or forwarding facility does not affect the sending of the messages. Only when the name is changed does the leaf switch stop sending the syslog messages. Enabling and disabling the policy does not resume the sending of the messages.	6.0(2h) and later
CSCwj32118	Tech support did not include manifest.json. Due to the difference in the name of device as per the "topsystem" and "hostname" commands, the code that is responsible for generating manifest file tracebacked and failed. This is an issue in tech support component.	6.0(2h) and later
CSCwj38953	log_bin_decode crashes on distinguished name decoding failures.	6.0(2h) and later
CSCwj42913	REST API can be used to configure static ports for nodes that are restricted in by a node rule.	6.0(2h) and later
CSCwj43407	Altering the IP SLA policy for an IP SLA track member led to the crashing of switches.	6.0(2h) and later
CSCwj55258	Fault F4144 will not clear from the Cisco APIC even with matching dhcpPool and Fabric Node Vector information.	6.0(2h) and later
CSCwj57993	The F0413 PSU fault is not reported by SMART callhome. The tcpdump command on the leaf switch does not show SMTP messages being sent for this fault for which the PSU was removed.	6.0(2h) and later

Bug ID	Description	Exists in
CSCwj69046	SAML authentication fails when using the HTTPS Proxy 5.2 image.	6.0(2h) and later
CSCwk13546	There are stale hvExtPl objects due to the hvsExtPol managed object not being cleaned up when an EPG is deleted. Fault F1606 is raised, but has no operational impact: desc :Fault delegate: Operational issues detected on portgroup error: Cannot find an EPG policy in the domain for the port group.	6.0(2h) and later
CSCwe50393	Using the back-to-back spine switch wizard will not display node IDs for the switch selection, and so the task in the wizard cannot be completed.	6.0(2h)
CSCwf80352	Cisco APIC does not accept special characters " #" and " ;" in then fabric name field when upgrading to the 6.0(2) release. For example, if the fabric name is " Test#03, it will be truncated to " Test" , which causes prevents switches from joining the fabric after they are reloaded during the upgrade. In this example, the Cisco APIC expects the name " Test#03" , but the switch is assigned the name " Test" .	6.0(2h)
CSCwh01298	The SSHD daemon does not listen on the IPV6 address.	6.0(2h)

Resolved Issues

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 the 6.0(2) release in which the bug was first fixed.

Bug ID	Description	Fixed in
CSCwe50393	Using the back-to-back spine switch wizard will not display node IDs for the switch selection, and so the task in the wizard cannot be completed.	6.0(2j)
CSCwf80352	Cisco APIC does not accept special characters " #" and " ;" in then fabric name field when upgrading to the 6.0(2) release. For example, if the fabric name is " Test#03, it will be truncated to " Test" , which causes prevents switches from joining the fabric after they are reloaded during the upgrade. In this example, the Cisco APIC expects the name " Test#03" , but the switch is assigned the name " Test" .	6.0(2j)
CSCwh01298	The SSHD daemon does not listen on the IPV6 address.	6.0(2j)
CSCvz72941	While performing ID recovery, id-import gets timed out. Due to this, ID recovery fails.	6.0(2h)
CSCwc66053	Preconfiguration validations for L3Outs that occur whenever a new configuration is pushed to the Cisco APIC might not get triggered.	6.0(2h)
CSCwe19885	The Nexus Insights application cannot stream the telemetry data to NDI, even though the Cisco ACI site is registered and active.	6.0(2h)

Known Issues

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 6.0(2) releases in which the bug exists. A bug might also exist in releases other than the 6.0(2) releases.

Bug ID	Description	Exists in
CSCvj26666	The "show run leaf|spine <nodeId>" command might produce an error for scaled up configurations.	6.0(2h) 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.	6.0(2h) 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.	6.0(2h) and later
CSCvq58953	One of the following symptoms occurs: App installation/enable/disable takes a long time and does not complete. Nomad leadership is lost. The output of the acidiag scheduler logs members command contains the following error: Error querying node status: Unexpected response code: 500 (rpc error: No cluster leader)	6.0(2h) and later
CSCvr89603	The CRC and stomped CRC error values do not match when seen from the APIC CLI compared to the APIC GUI. This is expected behavior. The GUI values are from the history data, whereas the CLI values are from the current data.	6.0(2h) 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.	6.0(2h) 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.	6.0(2h) and later
CSCvx75380	svcredirDestmon objects get programmed in all of the leaf switches where the service L3Out is deployed, even though the service node may not be connected to some of the leaf switch. There is no impact to traffic.	6.0(2h) and later
CSCvx78018	A remote leaf switch has momentary traffic loss for flushed endpoints as the traffic goes through the tglean path and does not directly go through the spine switch proxy path.	6.0(2h) and later
CSCvy07935	xR IP flush for all endpoints under the bridge domain subnets of the EPG being migrated to ESG. This will lead to a temporary traffic loss on remote leaf switch for all EPGs in the bridge domain. Traffic is expected to recover.	6.0(2h) and later
CSCvy10946	With the floating L3Out multipath recursive feature, if a static route with multipath is configured, not all paths are installed at the non-border leaf switch/non-anchor nodes.	6.0(2h) and later
CSCvy34357	Starting with the 6.0(2) release, the following apps built with the following non-compliant Docker versions cannot be installed nor run: • ConnectivityCompliance 1.2 • SevOneAciMonitor 1.0	6.0(2h) and later
CSCvy45358	The file size mentioned in the status managed object for techsupport "dbgexpTechSupStatus" is wrong if the file size is larger than 4GB.	6.0(2h) and later

Bug ID	Description	Exists in
CSCvz06118	In the "Visibility and Troubleshooting Wizard," ERSPAN support for IPv6 traffic is not available.	6.0(2h) and later
CSCvz84444	While navigating to the last records in the various History sub tabs, it is possible to not see any results. The first, previous, next, and last buttons will then stop working too.	6.0(2h) and later
CSCvz85579	VMMmgr process experiences a very high load for an extended period of time that impacts other operations that involve it. The process may consume excessive amount of memory and get aborted. This can be confirmed with the command "dmesg -T | grep oom_reaper" if messages such as the following are reported: oom_reaper: reaped process 5578 (svc_ifc_vmmmgr.)	6.0(2h) and later
CSCwa78573	When the "BGP" branch is expanded in the Fabric > Inventory > POD 1 > Leaf > Protocols > BGP navigation path, the GUI freezes and you cannot navigate to any other page. This occurs because the APIC gets large set of data in response, which cannot be handled by the browser for parts of the GUI that do not have the pagination.	6.0(2h) and later
CSCwe18213	The logical switch created for the EPG remains in the NSX-T manager after the EPG is disassociated from the domain, or the logical switch does not get created when the EPG is associated with the domain.	6.0(2h) and later
CSCwk21572	License manager occasionally cores after image upgrade.	6.0(2h) and later
N/A	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.	6.0(2h) and later
N/A	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.	6.0(2h) and later
N/A	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.	6.0(2h) and later
N/A	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.	6.0(2h) and later

Bug ID	Description	Exists in
N/A	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.	6.0(2h) and later
N/A	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.	6.0(2h) and later
N/A	Typically, faults are generally raised based on the presence of the BGP route target profile under the VRF table. However, if a BGP route target profile is configured without actual route targets (that is, the profile has empty policies), a fault will not be raised in this situation.	6.0(2h) and later
N/A	MPLS interface statistics shown in a switch's CLI get cleared after an admin or operational down event.	6.0(2h) and later
N/A	MPLS interface statistics in a switch's CLI are reported every 10 seconds. If, for example, an interface goes down 3 seconds after the collection of the statistics, the CLI reports only 3 seconds of the statistics and clears all of the other statistics.	6.0(2h) and later

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.
- For information about Cisco APIC compatibility with Cisco UCS Director, see the appropriate Cisco UCS Director Compatibility Matrix document.
- This release supports the following additional virtualization products:

Product	Supported Release	Information Location
Microsoft Hyper-V	• SCVMM 2019 RTM (Build 10.19.1013.0) or newer • SCVMM 2016 RTM (Build 4.0.1662.0) or newer • SCVMM 2012 R2 with Update Rollup 9 (Build 3.2.8145.0) or newer	N/A
VMM Integration and VMware Distributed Virtual Switch (DVS)	6.5, 6.7, and 7.0	Cisco ACI Virtualization Guide, Release 6.0(x)

Hardware Compatibility Information

This release supports the following Cisco APIC servers:

Product ID	Description
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-L4	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1200 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)
APIC-M4	Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1200 edge ports)

The following list includes general hardware compatibility information:

- For the supported hardware, see the Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 16.0(2).
- Contracts using matchDscp filters are only supported on switches with "EX" on the end of the switch name. For example, N9K-93108TC-EX.
- 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.

The following table provides compatibility information for specific hardware:

Product ID	Description
Cisco UCS M4-based Cisco APIC	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-negotiates to 10G without requiring any manual configuration.
Cisco UCS M5-based Cisco APIC	The Cisco UCS M5-based Cisco APIC supports dual speed 10G and 25G interfaces. 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-negotiates to 10G without requiring any manual configuration.
N2348UPQ	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

Product ID	Description
	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.
N9K-C9348GC-FXP	This 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.
N9K-C9364C-FX	Ports 49-64 do not support 1G SFPs with QSA.
N9K-C9508-FM-E	The Cisco N9K-C9508-FM-E2 and N9K-C9508-FM-E fabric modules in the mixed mode configuration are not supported on the same spine switch.
N9K-C9508-FM-E2	The Cisco 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 locator LED enable/disable feature is supported in the GUI and not supported in the Cisco ACI NX-OS switch CLI.
N9K-C9508-FM-E2	This fabric module must be physically removed before downgrading to releases earlier than Cisco APIC 3.0(1).
N9K-X9736C-FX	The locator LED enable/disable feature is supported in the GUI and not supported in the Cisco ACI NX-OS Switch CLI.
N9K-X9736C-FX	Ports 29 to 36 do not support 1G SFPs with QSA.

Miscellaneous Compatibility Information

This release supports the following products:

Product	Supported Release
Cisco NX-OS	16.0(2)
Cisco UCS Manager	2.2(1c) or later is required for the Cisco UCS Fabric Interconnect and other components, including the BIOS, CIMC, and the adapter.
CIMC HUU ISO	**Note**: Install only the CIMC versions mentioned here in this table. Though other firmware versions may be supported on standard UCS C220/C225 servers, they are not supported on APIC and could lead to issues, including failure to boot. • 4.3.2.240009 CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) and UCS C225 M6 (APIC-L4/M4) • 4.3.2.230207 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) and UCS C225 M6 (APIC-L4/M4) • 4.3.2.250016 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3). • 4.2(3e) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) and UCS C225 M6 (APIC-L4/M4) • 4.2(3b) CIMC HUU ISO for UCS C225 M6 (APIC-L4/M4) • 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)

Product	Supported Release
	• 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(4d) CIMC HUU ISO for UCS C220/C240 M3 and M4 (APIC-L2/M2) • 3.0(3f) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) • 2.0(13i) CIMC HUU ISO • 2.0(9c) CIMC HUU ISO • 2.0(3i) CIMC HUU ISO
Network Insights Base, Network Insights Advisor, and Network Insights for Resources	For the release information, documentation, and download links, see the Cisco Network Insights for Data Center page. For the supported releases, see the Cisco Data Center Networking Applications Compatibility Matrix.

- This release supports the partner packages specified in the L4-L7 Compatibility List Solution Overview document.
- 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, Release 6.0(x).
- For compatibility with Day-2 Operations apps, see the Cisco Data Center Networking Applications Compatibility Matrix.
- Cisco Nexus Dashboard Insights creates a user in Cisco APIC called cisco_SN_NI. This user is used when Nexus Dashboard Insights needs to make any changes or query any information from the Cisco APIC. In the Cisco APIC, navigate to the **Audit Logs** tab of the **System > History** page. The cisco_SN_NI user is displayed in the User column.
- Cisco APIC uses an SSL library called CiscoSSL, which is a customized version of the OpenSSL library to support CVE fixes and FIPS compliance. Cisco maintains an extended support contract with OpenSSL. CVE fixes from OpenSSL upstream is regularly incorporated in the older versions of CiscoSSL library as well.

Related Content

See the Cisco Application Policy Infrastructure Controller (APIC) page for the documentation.

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.

You can watch videos that demonstrate how to perform specific tasks in the Cisco APIC on the Cisco Cloud Networking YouTube channel.

Temporary licenses with an expiry date are available for evaluation and lab use purposes. They are strictly not allowed to be used in production. Use a permanent or subscription license that has been purchased through Cisco for production purposes. For more information, go to Cisco Data Center Networking Software Subscriptions.

The following table provides links to the release notes, verified scalability documentation, and new documentation:

Document	Description
Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 16.0(2)	The release notes for Cisco NX-OS for Cisco Nexus 9000 Series ACI-Mode Switches.
Verified Scalability Guide for Cisco APIC, Release 6.0(2) and Cisco Nexus 9000 Series ACI-Mode Switches, Release 16.0(2)	This guide contains the maximum verified scalability limits for Cisco Application Centric Infrastructure (ACI) parameters for Cisco APIC and Cisco Nexus 9000 Series ACI-Mode Switches.
APIC REST API Configuration Procedures	This document resides on developer.cisco.com and provides information about and procedures for using the Cisco APIC REST APIs. The new REST API procedures for this release reside only here and not in the configuration guides. However, older REST API procedures are still in the relevant configuration guides.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to apic-docfeedback@cisco.com. We appreciate your feedback.

Legal Information