Cisco Application Policy Infrastructure Controller Release Notes, Release 5.2(3)

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 15.2(3).

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

Date	Description
May 1, 2024	In the Miscellaneous Compatibility Information section, removed the older CIMC releases to reduce the clutter.
November 29, 2022	In the Known Issues section, added: • If you are upgrading to Cisco APIC release 4.2(6o), 4.2(7l), 5.2(1g), or later, ensure that any VLAN encapsulation blocks that you are explicitly using for leaf switch front panel VLAN programming are set as " external (on the wire)." If these VLAN encapsulation blocks are instead set to " internal," the upgrade causes the front panel port VLAN to be removed, which can result in a datapath outage.
November 18, 2022	In the Open Issues section, added bug CSCwc66053.
September 27, 2022	In the Open Issues section, added bug CSCwc49449.
August 1, 2022	In the Miscellaneous Compatibility Information section, added: • 4.2(2a) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(2k) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
July 1, 2022	In the Open Issues section, added bug CSCwb93239.
June 30, 2022	In the section Miscellaneous Compatibility, added information about Cisco Nexus Dashboard Insights creating the cisco_SN_NI user.
April 12, 2022	In the Open Issues section, added bug CSCvz94062.
March 21, 2022	In the Miscellaneous Compatibility Information section, added: • 4.1(3f) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3)
March 16, 2022	In the Resolved Issues section, added bug CSCwb06808.
February 23, 2022	In the Miscellaneous Compatibility Information section, added: • 4.1(2g) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
December 18, 2021	Release 5.2(3g) became available. In the Resolved Issues section, added bug CSCwa47295.
November 24, 2021	Release 5.2(3f) became available. In the Resolved Issues section, added bugs CSCvz98577 and CSCwa22996.
November 2, 2021	In the Miscellaneous Compatibility Information section, added: • 4.1(3d) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3)
October 18, 2021	Release 5.2(3e) became available.

New Software Features

Feature	Description
BGP underlay for Cisco ACI Multi-Pod, Cisco ACI Multi-Site, and remote leaf switches	The border gateway protocol (BGP) is now available as an alternative to the Open Shortest Path First (OSPF) protocol for the Inter-Pod Network (IPN) underlay. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.2(x).
Cisco ACI Multi-Pod spine switches back-to-back	In some cases, two pods can now be interconnected directly ("back-to-back") without using an IPN device. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.2(x) and Cisco ACI Multi-Pod Spines Back-to-Back document.
Cisco NX-OS to Cisco ACI POAP auto-conversion	Cisco NX-OS to Cisco ACI power-on auto-provisioning (POAP) auto-conversion automates the process of upgrading software images and installing configuration files on nodes that are being deployed in the network for the first time. When a Cisco NX-OS node with the POAP auto-conversion feature boots and does not find the startup configuration, the node enters the POAP mode and starts DHCP discovery on all ports. The node locates a DHCP server and bootstraps itself with its interface IP address, gateway, and DNS server IP addresses. The device also obtains the IP address of a TFTP server and downloads a configuration script that enables the node to download and install the appropriate software image and configuration file. This process converts the Cisco NX-OS node from the standalone mode to the Cisco ACI-mode. For more information, see the Cisco APIC Getting Started Guide, Release 5.2(x).
Endpoint security group enhancements	Endpoint security groups (ESGs) now support more features and configurations, such as: • Inter-VRF service graphs between ESGs • ESG shutdown • Host-based routing/host route advertisement • ESGs can be specified as a source or destination of the following features: ◦ On Demand Atomic Counter ◦ On Demand Latency Measurement For the full list of newly-supported features and configurations, see the Cisco APIC Security Configuration Guide, Release 5.2(x).
ERSPAN supports IPv6 destinations	ERSPAN now supports IPv6 destinations.
Integrity check for exported configuration files that are saved on external servers	There is now an integrity check for exported configuration files that are saved on external servers, which ensures that the file's contents are not tampered with. For more information, see the Cisco ACI Configuration Files: Import and Export document.
Micro Bidirectional Forwarding Detection	Micro Bidirectional Forwarding Detection (BFD) establishes individual BFD sessions on each member link of a port channel for faster failure detection and easier troubleshooting. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.2(x).
Open Authorization 2.0 support	Open Authorization (OAuth) 2.0 is an open-standard authorization protocol. OAuth 2.0 allows you to access an application (Service Provider or SP) that is trusted or approved by an Identity Provider (IdP). OAuth 2.0 uses authorization tokens to provide identity and authorization claims to the consumer application. Beginning with Cisco APIC Release 5.2(3), OAuth 2 server can be used to set up an application (such as, Cisco APIC) as an identity server that authenticates users using single sign-on. For more information, see the Cisco APIC Security Configuration Guide, Release 5.2(x).

Feature	Description
Rogue/COOP exception list	The rogue/COOP exception list enables you to specify the MAC address of endpoints for which you want to have a higher tolerance for endpoint movement with rogue endpoint control before the endpoints get marked as rogue. Endpoints in the rogue/COOP exception list get marked as rogue only if they move 3000 or more times within 10 minutes. After an endpoint is marked as rogue, the endpoint is kept static to prevent learning. The rogue endpoint is deleted after 30 seconds. For more information, see the Cisco APIC Basic Configuration Guide, Release 5.2(x).
Security GUI screen enhancements	The security screens in the GUI are enhanced to show more information about the contract consumers and providers, and now include the ability to filter the data and view the resolved paths for an EPG or contract. For more information, see the online help pages for the **System > Security** and **Tenants > *tenant_name* > Security** screens.
Specifying a transport protocol for a syslog remote destination	You can now specify a transport protocol to use for sending the syslog messages when you create a syslog remote destination. For more information, see the Cisco APIC Basic Configuration Guide, Release 5.2(x).
Support for Layer 3 multicast on L3Outs with SVI	Layer 3 multicast on an L3Out with SVI adds support for enabling PIM on L3Out SVIs. This allows the ACI border leaf switch configured with an L3Out SVI to establish PIM adjacencies with an external multicast router or firewall. For more information, see Cisco APIC Layer 3 Networking Configuration Guide, Release 5.2(x).
Support for multiple encapsulations for L3Outs with SVI	Beginning with release 5.2(3), you can use different VLAN encapsulations for an external bridge domain for L3Outs configured with SVIs, where all of the different external encapsulation instances are treated as part of a single Layer 2 domain. Prior to release 5.2(3), L3Outs configured with SVIs are limited to one VLAN encapsulation for each external bridge domain. However, with the introduction of floating L3Outs in release 4.2(1), there are scenarios where multiple VLAN encapsulations are needed for the same external bridge domain. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.2(x) and Using Floating L3Out to Simplify Outside Network Connections document.
Support for Prometheus Node Exporter	Support is now available for monitoring metrics using the Prometheus Node Exporter. The Prometheus Node Exporter provides visibility to a wide variety of hardware and kernel-related metrics, where it collects technical information from Linux nodes, such as CPU, disk, and memory statistics. For more information, see the Monitoring Metrics Using the Prometheus Node Exporter document.
time-range REST API query option for viewing log record objects	Beginning with Cisco APIC release 5.2(3), with the new API query option time-range that is supported only for log record objects, the Cisco APIC can respond to the API query for the log record objects much faster. The Cisco APIC GUI also uses the time-range option for improved performance. This new query option for log record objects are not used in the CLI commands such as show faults history or show events. For more information about the time-range option, see the Cisco APIC REST API Configuration Guide, Release 4.2(x) and Later. For information about log record objects and using the GUI to view the objects, see the Cisco Application Centric Infrastructure Fundamentals, Releases 5.2(x).
USB port on Cisco ACI-mode switches can be disabled	You can now disable the USB port on a Cisco ACI-mode switch. If you have disabled the USB port, then when the switch is rebooted, the switch boots using the last known operating system image in the bootflash instead of using an image on a connected USB device. This feature provides an extra layer of protection in the event that someone power cycles the

Feature	Description
	switch to try to boot the switch from a USB image that contains malicious code. For more information, see the Disabling the USB Port on Cisco ACI-Mode Switches document.

New Hardware Features

For the new hardware features, see the Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 15.2(3).

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 5.2(3) releases in which the bug exists. A bug might also exist in releases other than the 5.2(3) releases.

Bug ID	Description	Exists in
CSCwf19660	Major fault F3083 ("IP detected on multiple MACs") is raised under a uEPG and ESG when an EPG selector is configured in the ESG.	5.2(3g) and later
CSCwb06808	In an OpenShift deployment that is running Cisco ACI CNI, errors similar to the following examples are observed in the aci-containers-controller pod: oc logs -n aci-containers-system aci-containers-controller-5845449f5d-sdkwg | grep "Error while refreshing subscription" time="2022-02-12T15:18:10Z" level=error msg="Error while refreshing subscription" code=0 mod=APICAPI status=400 text="Subscription refresh timeout" url=<...> In an OpenShift deployment that is running the Cisco ACI Neutron plugin, errors similar to the following examples are observed in the aim logs in /var/log/containers/aim/aim-aid.log*: 2022-01-11 10:01:18.696 250002 140706618431232 WARNING root [-] Could not refresh subscription: ...	5.2(3f) and later
CSCvg81020	For strict security requirements, customers require custom certificates that have RSA key lengths of 3072 and 4096.	5.2(3e) and later
CSCvm56946	Support for local user (admin) maximum tries and login delay configuration.	5.2(3e) 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".	5.2(3e) and later
CSCvx90225	The browser hangs when clicking on the alert bell in the header bar.	5.2(3e) and later

Bug ID	Description	Exists in
CSCvy00746	A breakout parent port shows in the drop-down list for the SPAN source even after the port is broken out.	5.2(3e) 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.	5.2(3e) and later
CSCvy59543	The remote site unicast DTEP is missing in the route-map. Hence, the route is not getting redistributed into the fabric.	5.2(3e) and later
CSCvz67423	Configuration exports are failing with reason "Backup job has timed out" when two objects with different keys were converted into the same objects during a configuration export, which causes conflicts.	5.2(3e) and later
CSCvz72941	While performing ID recovery, id-import gets timed out. Due to this, ID recovery fails.	5.2(3e) and later
CSCvz79984	There is a stack trace dump in the DME log due to a CRIT level log message.	5.2(3e) and later
CSCvz81545	A Layer 3 Cisco APIC becomes disconnected from the rest of the fabric.	5.2(3e) and later
CSCvz83636	For a health record query using the last page and a time range, the GUI displays some health records with a creation time that is beyond the time range (such as 24h).	5.2(3e) and later
CSCvz94062	An SMU's upgrade status shows as "reload pending," but the reload is actually completed and the SMU is activated.	5.2(3e) and later
CSCvz96470	Consider the following scenario: 1. An EPG provider with subnet A defined under an EPG, is a provider for contract in VRF1. 2. Configure an l3out/Ext-EPG in VRF2 as contract consumer 3. Validate that the subnet flags are being used for route advertisement in the L3Out. 4. Now, configure the same subnet A as a route-leak under a VRF instance with route advertisement configured as FALSE. This route-leak policy should trigger a fault, as the EPG contract leak-route takes precedence. In this faulty state, the adv-external property under the VRF instance leakRoute shouldn’t take effect, as this policy is in a faulty state. However, irrespective of the fault , the VRF instance route leak flag takes precedence and routes are advertised out of the L3Out. This is when the provider EPG has a contract with the L3Out, and "Advertise External == False" on the bridge domain.	5.2(3e) 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.	5.2(3e) and later
CSCwb93239	The GUI displays the following error: Failed, Local Upload Failure Msg (Request failed with status code 413).	5.2(3e) and later
CSCwc49449	When a maintenance policy has multiple switch nodes, such as vPC pair nodes, an SMU's uninstallation gets stuck in the "queued" state for one of the nodes.	5.2(3e) and later

Bug ID	Description	Exists in
CSCwc66053	Preconfiguration validations for L3Outs that occur whenever a new configuration is pushed to the Cisco APIC might not get triggered.	5.2(3e) and later
CSCwe52465	The NICC app image fails to load.	5.2(3e) and later
CSCwe66712	For a customer using America/Mexico_City time, the DST time change will still happen on APIC in the year 2023.	5.2(3e) and later
CSCwf54771	User configuration is missing on APICs and switches following an ungraceful reload or power outage.	5.2(3e) 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.	5.2(3e) 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.	5.2(3e) 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.	5.2(3e) and later
CSCwi34095	App installation fails on the Cisco APIC with the error "Unable to add elasticsearch credentials". This is seen for any app making use of Elasticsearch, such as Nexus Insight Cloud Connector.	5.2(3e) and later
CSCwa47295	This bug has been filed to evaluate the Cisco Network Insights Base Application - NIB (its Nexus Insights Cloud Connector App on 5.x version onwards) for Cisco APIC against the vulnerability in the Apache Log4j Java library disclosed on December 9th, 2021. Cisco has reviewed this product and concluded that it contains a vulnerable version of Apache Log4j and is affected by the following vulnerability: CVE-2021-44228 - Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints This advisory is available at the following link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd	5.2(3e) and 5.2(3f)
CSCvz98577	In an OpenShift on OpenStack setup, after VM migration, and connectivity to the pods inside that VM may be lost when accessed from pods running on other VMs not on that same physical host.	5.2(3e)
CSCwa22996	The communication between two OpenShift pods (not on the same node) belonging to the same EPG is broken after the fabric was upgraded to the leaf switch software to 5.2(3e).	5.2(3e)

Resolved Issues

Bug ID	Description	Fixed in
CSCwa47295	This bug has been filed to evaluate the Cisco Network Insights Base Application - NIB (its Nexus Insights Cloud Connector App on 5.x version onwards) for Cisco APIC against the vulnerability in the Apache Log4j Java library disclosed on December 9th, 2021. Cisco has reviewed this product and concluded that it contains a vulnerable version of Apache Log4j and is affected by the following vulnerability: CVE-2021-44228 - Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints This advisory is available at the following link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd	5.2(3g)
CSCvz98577	In an OpenShift on OpenStack setup, after VM migration, and connectivity to the pods inside that VM may be lost when accessed from pods running on other VMs not on that same physical host.	5.2(3f)
CSCwa22996	The communication between two OpenShift pods (not on the same node) belonging to the same EPG is broken after the fabric was upgraded to the leaf switch software to 5.2(3e).	5.2(3f)
CSCvs97029	All the external prefixes from VRF-A could be leaked to VRF-C even when an inter-VRF ESG leak route is configured for a specific prefix.	5.2(3e)
CSCvy17113	When there are two or more service graph associated contracts between the same pair of consumer and provider EPGs, and each contract is associated to a different Instp (by virtue of service graph configuration), imported/VRF-leaked Instp routes/subnets would not get cleaned up when one of those contracts is deleted from the list of contracts under the EPG. Imported routes /subnets would get cleaned up when the last contract between that EPG pair is deleted. There should be no impact to the traffic forwarding. This issue is about the cleanup of leaked routes.	5.2(3e)
CSCvy17504	When the OpFlexAgent moved from one vPC pair leaf switches to a new vPC pair, it may take up to 20 minutes for the OpFlexAgent detected the movement, and reconnect the OpFlex channel. Ideally, this should be completed within a few seconds.	5.2(3e)
CSCvy21881	An upgrade fails due to an incompatible target version. The upgradeStatusStr for maintUpgJob is empty, due to which the GUI is not able to show the correct state.	5.2(3e)
CSCvy29992	On the Cisco APIC CLI, the " moconfig commit" command triggers a " No such file or directory" error. The command successfully commits the changes, but the fact that this error shows up results in confusion for the end user.	5.2(3e)
CSCvy33994	On the Cisco APIC CLI, using the " moset" command to set an managed object attribute to the same value results in the following error: [Errno 1] Operation not permitted.	5.2(3e)
CSCvy85417	The show catalog is empty, which causes all switch discovery to fail because there is no catalog information present.	5.2(3e)

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 5.2(3) releases in which the bug exists. A bug might also exist in releases other than the 5.2(3) releases.

Bug ID	Description	Exists in
CSCvj26666	The " show run leaf|spine <nodeId>" command might produce an error for scaled up configurations.	5.2(3e) 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.	5.2(3e) 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.	5.2(3e) 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)	5.2(3e) 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.	5.2(3e) 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.	5.2(3e) 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.	5.2(3e) 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.	5.2(3e) 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.	5.2(3e) 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.	5.2(3e) and later
CSCvy34357	Starting with the 5.2(3) release, the following apps built with the following non-compliant Docker versions cannot be installed nor run: • ConnectivityCompliance 1.2 • SevOneAciMonitor 1.0	5.2(3e) and later

Bug ID	Description	Exists in
CSCvy45358	The file size mentioned in the status managed object for techsupport "dbgexpTechSupStatus" is wrong if the file size is larger than 4GB.	5.2(3e) and later
CSCvz06118	In the "Visibility and Troubleshooting Wizard," ERSPAN support for IPv6 traffic is not available.	5.2(3e) 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.	5.2(3e) and later
N/A	If you are upgrading to Cisco APIC release 4.2(6o), 4.2(7l), 5.2(1g), or later, ensure that any VLAN encapsulation blocks that you are explicitly using for leaf switch front panel VLAN programming are set as "external (on the wire)." If these VLAN encapsulation blocks are instead set to "internal," the upgrade causes the front panel port VLAN to be removed, which can result in a datapath outage.	5.2(3e) 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.	5.2(3e) 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.	5.2(3e) 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.	5.2(3e) 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.	5.2(3e) and later
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.	5.2(3e) and later

Bug ID	Description	Exists in
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.	5.2(3e) 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.	5.2(3e) and later
N/A	MPLS interface statistics shown in a switch's CLI get cleared after an admin or operational down event.	5.2(3e) 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.	5.2(3e) 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 5.2(x)

Hardware Compatibility Information

This release supports the following Cisco APIC servers:

Product ID	Description
APIC-L1	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1000 edge ports)
APIC-L2	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1000 edge

Product ID	Description
	ports)
APIC-L3	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1200 edge ports)
APIC-M1	Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1000 edge ports)
APIC-M2	Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1000 edge ports)
APIC-M3	Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1200 edge ports)

The following list includes general hardware compatibility information:

- For the supported hardware, see the Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 15.2(3).
- 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 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.

Product ID	Description
	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	15.2(3)
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	The latest recommended releases are as follows: • 4.2(3e) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) and UCS C225 M6 (APIC-L4/M4) • 4.1(2m) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)
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 5.2(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.

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 Data Center 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 15.2(3)	The release notes for Cisco NX-OS for Cisco Nexus 9000 Series ACI-Mode Switches.
Verified Scalability Guide for Cisco APIC, Release 5.2(3) and Cisco Nexus 9000 Series ACI-Mode Switches, Release 15.2(3)	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.

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology

diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.