Cisco Application Policy Infrastructure Controller Release Notes, Release 4.2(6)

© 2024 Cisco and/or its affiliates. All rights reserved.

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 14.2(6).

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

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.

Date	Description
November 29, 2022	In the Known Issues section, added: • If you are upgrading to Cisco APIC release 4.2(6o) 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.
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)
June 30, 2022	In the section Miscellaneous Compatibility, added information about Cisco Nexus Dashboard Insights creating the cisco_SN_NI user.
April 8, 2022	Moved bug CSCvu04758 from the Open Issues section to the Resolved Issues section. This bug was resolved starting with the 4.2(6d) release.
April 4, 2022	In the Open Issues section, added bug CSCvy49540.
March 21, 2022	In the Miscellaneous Compatibility Information section, added: • 4.1(3f) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3)
February 23, 2022	In the Miscellaneous Compatibility Information section, added: • 4.1(2g) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
February 10, 2022	In the Open Issues section, added bugs CSCvx76043 and CSCwa19126.
November 15, 2021	In the Open Issues section, added bugs CSCvy17504, CSCvy55588, and CSCvz31155.
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)

© 2024 Cisco and/or its affiliates. All rights reserved.

Date	Description
August 9, 2021	In the Open Issues section, added bugs CSCvx32437 and CSCvx59637. In the Resolved Issues section, added bugs CSCvw33277, CSCvu84392, and CSCvu36682.
August 4, 2021	In the Open Issues section, added bugs CSCvy30453, CSCvy44940, CSCvv18827, CSCvx54410, CSCvx74210, CSCvx90048, CSCvy30683, CSCvx59910, CSCvx28313, CSCvx64383, CSCvx59006, CSCvx70452, and CSCvy86541.
July 28, 2021	In the Changes in Behavior section, added: • The SQL database is no longer persistent during ungraceful reloads of the switches. Examples of ungraceful reload include kernel panics and forced power cycles. In the event of an ungraceful reload, the switch will reboot as stateless and must re-download its policies from the Cisco APIC. Graceful reloads, such as manual reloads and hap-resets, are still stateful and the switch will main-tain its database across the reload.
July 26, 2021	In the Miscellaneous Compatibility Information section, the CIMC 4.1(3c) release is now recommended for UCS C220/C240 M5 (APIC-L3/M3).
May 17, 2021	Release 4.2(6o) became available. Added the resolved issues for this release. Not related to the 4.2(6o) release, in the Changes in Behavior section, added: When the same subnet is configured under both a bridge domain and an EPG, the scope such as " Advertised Externally" and " Shared between VRFs" must match. Configurations with a mismatched scope are rejected beginning in releases 4.2(6d) and 5.1(1).
May 13, 2021	Removed bug CSCvt00629 from the open issues table. This bug was resolved in the 4.2(5k) release.
March 11, 2021	For the " BGP route map continue with auto-continue" new software feature, specified that this was included in the 4.2(6h) release. In the Miscellaneous Compatibility Information section, for CIMC HUU ISO, added: • 4.1(3b) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) Changed: • 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3) To: • 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2
March 5, 2021	Removed bug CSCvs04899 from the open issues table. This bug was resolved in the 4.2(4j) release. Removed bug CSCvv53757 from the open issues table. This bug was resolved in the 4.2(5l) release.
February 28, 2021	Release 4.2(6l) became available. Added the resolved issues for this release.
February 19, 2021	In the Open Issues section, removed bug CSCvs29556. This bug was resolved in 4.2(5k).
February 3, 2021	In the Miscellaneous Compatibility Information section, for CIMC HUU ISO, added: • 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3)
January 28, 2021	Release 4.2(6h) became available. Added the resolved issues for this release.
January 25, 2021	Release 4.2(6g) became deferred. For more information, see the DEFERRAL ADVISORY NOTICE for Cisco ACI - CSCvx13971.

© 2024 Cisco and/or its affiliates. All rights reserved.

Date	Description
January 22, 2021	Release 4.2(6g) became available. In the New Software Features section, added the Redistribution of Direct Routes to BGP From an L3Out feature.
November 26, 2020	Release 4.2(6d) became available.

New Software Features

Feature	Description
BGP route map continue with auto-continue	Beginning in the Cisco APIC 4.2(6h) release, you can use auto-continue to apply the continue statement in a route map for all user-configured sequences (contexts) in a given BGP route profile. Auto-continue is enabled per BGP route profile. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 4.2(x).
IGMP and MLD packet forwarding through 802.1Q tunnels	IGMP and MLD packets can now be forwarded through 802.1Q tunnels.
Link-level flow control	Link-level flow control is a congestion management technique that pauses data transmission until the congestion in the system is resolved. When a receiving device becomes congested, the device communicates with the transmitter by sending a pause frame. When the transmitting device receives a pause frame, the device stops the transmission of any further data frames based on the pause quanta value received in the link-level flow control feature pause frame. For more information, see the Cisco APIC Basic Configuration Guide, Release 4.2(x).
Applying a route map to interleak redistribution from direct subnets	Beginning in the Cisco APIC 4.2(6h) release, you can apply a route map to interleak redistribution from direct subnets (L3Out interfaces). For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 4.2(x).
Deny action in the route-map for interleak redistribution for static routes and direct subnets	Beginning in the Cisco APIC 4.2(6h) release, you can configure the deny action in the route-map for interleak redistribution for static routes and direct subnets. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 4.2(x).
SNMPv3 support for SHA-2	SNMPv3 now supports the Secure Hash Algorithm-2 (SHA-2) authentication type.
SSD write optimization	The SSD write strategy is optimized for improved performance and longer SSD life.

New Hardware Features

For the new hardware features, see the Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 14.2(6).

Changes in Behavior

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

© 2024 Cisco and/or its affiliates. All rights reserved.

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 4.2(6) releases in which the bug exists. A bug might also exist in releases other than the 4.2(6) releases.

Bug ID	Description	Exists in
CSCvy86541	Under the Upgrade Group Policy, the switches are added as a range. If the switches are added manually, everything works as expected.	4.2(6o) and later
CSCvx70452	The Cisco ACI Hyper-V Agent crashes or restarts with the following exception:System.OutOfMemoryException	4.2(6h) and later
CSCvx13971	Unexpected behavior during certain upgrade/downgrade scenarios can occur when using the redistribute direct feature and attached host feature.	4.2(6g)
CSCvt23284	If the DVS version is 6.6 or later or the VMware vCenter version is 7.0, using basic LACP will raise errors on the VMware vCenter, as these releases of DVS and VMware vCenter no longer support LACP.	4.2(6d) through 4.2(6l)
CSCvw33061	Traffic loss is observed from multiple endpoints deployed on two different vPC leaf switches.	4.2(6d) through 4.2(6l)
CSCvx31968	When pushing the new VMware VMM domain to VMware vCenter 7, the task "Reconfigure Distributed Port Group" for the DV-uplink-group completes with a status of "Link Aggregation Control Protocol group configured on <VMM_domain_name> conflicts with the Link Aggregation Control Protocol API version multipleLag." No fault is raised on the Cisco APIC.	4.2(6d) through 4.2(6l)
CSCvx73311	The "df -h" and "ls -al /tmp/" commands hang. High CPU utilization seen from glusterd. The "cat /sys/fs/cgroup/pids/system.slice/system-gluster.slice/glusterd.service/pids.current" command shows a number approaching 100.	4.2(6d) through 4.2(6l)
CSCvx79980	In a setup with 3 hosts from the same domain that have some number of virtual machines under them and the reserve host and other parameters are selected, after starting the "Migrate to ACI Virtual Edge" process, all hosts start to move at same time, causing a resource crunch. This issue occurs only once in a while. In a normal scenario, the hosts migrate one by one.	4.2(6d) through 4.2(6l)
CSCvd66359	The Port ID LLDP Neighbors panel displays the port ID when the interface does not have a description. Example: Ethernet 1/5, but if the interface has description, the Port ID property shows the Interface description instead of the port ID.	4.2(6d) and later
CSCvf70362	This enhancement is to change the name of "Limit IP Learning To Subnet" under the bridge domains to be more self-explanatory. Original: Limit IP Learning To Subnet: [check box] Suggestion: Limit Local IP Learning To BD/EPG Subnet(s): [check box]	4.2(6d) and later
CSCvg35344	Requesting an enhancement to allow exporting a contract by right clicking the contract itself and choosing "Export Contract" from the right click context menu. The current implementation of needing to right click the Contract folder hierarchy to export a contract is not intuitive.	4.2(6d) and later

© 2024 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description	Exists in
CSCvq81020	For strict security requirements, customers require custom certificates that have RSA key lengths of 3072 and 4096.	4.2(6d) and later
CSCvi20535	When a VRF table is configured to receive leaked external routes from multiple VRF tables, the Shared Route Control scope to specify the external routes to leak will be applied to all VRF tables. This results in an unintended external route leaking. This is an enhancement to ensure the Shared Route Control scope in each VRF table should be used to leak external routes only from the given VRF table.	4.2(6d) and later
CSCvj56726	The connectivity filter configuration of an access policy group is deprecated and should be removed from GUI.	4.2(6d) and later
CSCvk18014	The action named 'Launch SSH' is disabled when a user with read-only access logs into the Cisco APIC.	4.2(6d) and later
CSCvm42914	This is an enhancement request to add policy group information to the properties page of physical interfaces.	4.2(6d) and later
CSCvm56946	Support for local user (admin) maximum tries and login delay configuration.	4.2(6d) and later
CSCvn12839	Error " mac.add.ress not a valid MAC or IP address or VM name" is seen when searching the EP Tracker.	4.2(6d) and later
CSCvp26694	A leaf switch gets upgraded when a previously-configured maintenance policy is triggered.	4.2(6d) and later
CSCvp62048	New port groups in VMware vCenter may be delayed when pushed from the Cisco APIC.	4.2(6d) and later
CSCvq57942	In a RedHat OpenStack platform deployment running the Cisco ACI Unified Neutron ML2 Plugin and with the CompHosts running OVS in VLAN mode, when toggling the resolution immediacy on the EPG<->VMM domain association (fvRsDomAtt.resImedcy) from Pre-Provision to On-Demand, the encap VLANs (vlanCktEp mo's) are NOT programmed on the leaf switches. This problem surfaces sporadically, meaning that it might take several resImedcy toggles between PreProv and OnDemand to reproduce the issue.	4.2(6d) and later
CSCvq63415	Disabling dataplane learning is only required to support a policy-based redirect (PBR) use case on pre-" EX" leaf switches. There are few other reasons otherwise this feature should be disabled. There currently is no confirmation/warning of the potential impact that can be caused by disabling dataplane learning.	4.2(6d) and later
CSCvr62453	When a Cisco ACI fabric upgrade is triggered and a scheduler is created and associated to the maintenance group, the scheduler will remain associated to the maintenance group. If the version is changed in the maintenance group, it will trigger the upgrade. This enhancement is to avoid unwanted fabric upgrades. Post-upgrade, the association of the scheduler should be removed from the maintenance group after the node upgrade reaches 100%.	4.2(6d) and later
CSCvr85945	There should be a description field in the subnet IP address tables.	4.2(6d) and later
CSCvs03055	While configuring a logical node profile in any L3Out, the static routes do not have a description.	4.2(6d) and later

© 2024 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description	Exists in
CSCvs11202	After exiting Maintenance (GIR) mode, the switch reloads automatically after 5 minutes without warning.This enhancement will provide messaging in the GUI to indicate that the reload is expected.	4.2(6d) and later
CSCvs53247	OpenStack supports more named IP protocols for service graph rules than are supported in the Cisco APIC OpenStack Plug-in.	4.2(6d) and later
CSCvs56642	This is an enhancement request for schedule-based Tech Support for leaf and spine switches.	4.2(6d) and later
CSCvs81944	The following example shows UNIX time in the subject header: Subject: Configuration import/export job 2020-01-27T09-00-16 finished with status: success Created: 1580144423366 ContentType: plain/text	4.2(6d) and later
CSCvt18530	The paths list in UCSM Integration Tab->Policy is empty. There are no paths and therefore no VLANs listed. The Leaf-Enforced mode on UCSM Integration filters out all VLANs, resulting in traffic loss.	4.2(6d) and later
CSCvt30716	UCSM Integration shows an old topology when the connection between the fabric interconnect and leaf switch pair is removed, because LooseNode information is not updated when LLDP connections go away. This persists even after you delete the integration and add the UCSM as a new integration.	4.2(6d) and later
CSCvt31539	The UCSM app fails to configure a native VLAN on the UCSM if you configure an EPG with the native VLAN set. The app sets the VLAN as a normal trunk-tagged VLAN on the UCSM. This causes the blackholing of traffic.	4.2(6d) and later
CSCvt64925	Changes to a Cisco APIC configuration are no longer pushed to the Cisco APIC.	4.2(6d) and later
CSCvt67097	In the Cisco APIC GUI, external EPGs under L2Out and L3Out in tenants are called " External Network Instance Profile" . This is the official name for object (l2extInstP and l3extInstP). However, these are typically referred to as external EPGs. This is an enhancement to update the GUI label from " External Network Instance Profile" to " External EPG" .	4.2(6d) and later
CSCvt92961	A TEP endpoint can expire on the leaf switch if the host does not respond on a unicast ARP refresh packet initiated by the leaf switch.	4.2(6d) and later
CSCvu84284	When a Cisco UCS M5 (M3 APIC) with an Intel copper-based NIC is downgraded to any release prior to 4.2(5), the Cisco APIC will not join the fabric because this Intel copper-based NIC is not supported in older releases.	4.2(6d) and later
CSCvv11517	The DHCP server response is dropped at the external router.	4.2(6d) and later
CSCvv11546	DHCP response is dropped at the border leaf switch.	4.2(6d) and later
CSCvv14373	The DHCP response does not reach the client.	4.2(6d) and later

© 2024 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description	Exists in
CSCvv18827	The data in the Cisco APIC database may get deleted during an upgrade from a 3.0 or 3.1 release to a 4.0 or 4.1 release if the target release is rolled back to current running release within 2 minutes after the upgrade was started. The upgrade will continue anyway, but the Cisco APIC will lose all data in the database and a user with admin credentials cannot log in. Only the rescue-user/admin can log in. All shards for a process show as unexpected, and the database files are removed. The last working pre-upgrade database files are copied to the purgatory directory.	4.2(6d) and later
CSCvw54371	The application EPG or the corresponding bridge domain's public subnet in VRF1 may be advertised out of an OSPF-enabled L3Out in VRF2 even though the L3Out does not participate in the shared service.	4.2(6d) and later
CSCvw69692	If a service graph gets attached to the inter-VRF contract after it was already attached to the intra-VRF contract, the pctag for the shadow EPG gets reprogrammed with a global value. The zoning-rule entries that matched the previous pctag as the source and EPG1 and EPG2 as the destination do not get reprogrammed and they remain in a stale status in the table. Traffic between EPG1 and EPG2 gets broken as the packets flowing from the PBR get classified with the new global pctag.	4.2(6d) and later
CSCvx10921	A standby APIC disappears from the GUI after cluster convergence.	4.2(6d) and later
CSCvx28313	On a recurring basis, after several days, ssh/GUI access is lost to some Cisco APICs using either a local account or remote user. For example, the same user can log in to APIC3, but not APIC1 nor APIC2. Restarting nginx eliminates the issue for several days, but the issue then occurs again. The Cisco APIC cluster is fully fit and no cores are seen.	4.2(6d) and later
CSCvx32437	When a power supply is disconnected for one PSU, it typically takes 5 minutes, but up to 20 minutes, to reflect the correct status in the Cisco APIC. A similar delay is observed when the power supply is connected again.	4.2(6d) and later
CSCvx54410	An endpoint move from a microsegmentation EPG to a base EPG causes the endpoint to disconnect for tag-based microsegmentation.	4.2(6d) and later
CSCvx59006	The External EPG tab displays the following tabs: General, Contracts, Inherited, and Contracts. The External EPG tab should display the following tabs: General, Contracts, Subject Labels, and EPG Labels.	4.2(6d) and later
CSCvx59637	Fault F0058 is raised when attempting to add the Tetration agent .rpm file firmware image in the Cisco APIC firmware.	4.2(6d) and later
CSCvx59910	Running " Visibility & Troubleshooting Reporting" gives a report of " Status - Pending" after trying for the second time. The first attempt works fine, but the second attempt gets stuck in the pending state. This issue is observed on all Cisco APICs, on all the browsers, and with different PCs.	4.2(6d) and later
CSCvx64383	Cleanup of backend data will not happen for an old bridge domain with a subnet and old CTX combination. Fault F0469 is raised when a new bridge domain is added into an old CTX with the same subnet.	4.2(6d) and later
CSCvx74210	One Cisco APIC experiences high Java CPU utilization, reaching over 400%.	4.2(6d) and later
CSCvx76043	A timeout is observed while using Drop/stats under Visibility & Troubleshooting in a scaled Cisco ACI fabric.	4.2(6d) and later

© 2024 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description	Exists in
CSCvx90048	The load time of the operational tab of an interface under a node is significantly longer the first time it is viewed. After this initial load, going to other interfaces under that same switch is comparatively faster.	4.2(6d) and later
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.	4.2(6d) and later
CSCvy30453	For a Cisco ACI fabric that is configured with fabricId=1, if APIC3 is replaced from scratch with an incorrect fabricId of " 2," APIC3's DHCPd will set the nodeRole property to " 0" (unsupported) for all dhcpClient managed objects. This will be propagated to the appliance director process for all of the Cisco APICs. The process then stops sending the AV/FNV update for any unknown switch types (switches that are not spine nor leaf switches). In this scenario, commissioning/decommissioning of the Cisco APICs will not be propagated to the switches, which causes new Cisco APICs to be blocked out of the fabric. Another symptom is that the " acidag fnvread" command's output has a value of " unknown" in the role column.	4.2(6d) and later
CSCvy30683	The " show" and " fabric" commands on the Cisco APIC CLI become unresponsive.	4.2(6d) and later
CSCvy44940	APIC symptoms: After a Cisco APIC has finished upgrading and has reloaded, the ifc_reader crashes about 6 times in 7 minutes. Afterward, the ifc_reader service stops, which causes Cisco APIC communication issues. ifc_reader DME issues are not reflected in the AV health values, rvread, nor the Cisco APIC GUI. acidiag avread, rvread, and the Cisco APIC GUI report a fully fit cluster. Cisco APIC GUI alarms raise a " split fabric" alert, and crashes in the NGINX process may be observed. Switch Symptoms: After the Cisco APICs have been upgraded, all switches start seeing NGINX DME crashes every few minutes. The rate of crashes increases with the rate of uribv4Nexthop.type API queries that result in switch queries. After the NGINX process has received 250 instances of the offending query, the switch will cut off the interfaces, as it has reached a failed state. This will lead to a loss of network connectivity on the affected devices.	4.2(6d) and later
CSCvy49540	HTTPS API Calls to the switch are not working. The NGINX service does not listen to the HTTPS port because the nginx.conf file is not properly populated.	4.2(6d) and later
CSCvy55588	" Show Usage" in the GUI for a TACACS policy in the fabric monitoring common policy do not work in release 4.2(5k) and later.	4.2(6d) and later
CSCvz31155	The show usage screen in the Cisco APIC GUI has empty output.	4.2(6d) and later
CSCwa19126	The Fabric Topology view shows old connections as well as new ones, which can be misleading. This behavior is cosmetic in nature and should have no impact on data/control plane.	4.2(6d) 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.	4.2(6d) and later
CSCwc66053	Preconfiguration validations for L3Outs that occur whenever a new configuration is pushed to the Cisco APIC might not get triggered.	4.2(6d) and later

© 2024 Cisco and/or its affiliates. All rights reserved.

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 whether the bug was resolved in the base release or a patch release.

Bug ID	Description	Fixed in
CSCvt23284	If the DVS version is 6.6 or later or the VMware vCenter version is 7.0, using basic LACP will raise errors on the VMware vCenter, as these releases of DVS and VMware vCenter no longer support LACP.	4.2(6o)
CSCvw33061	Traffic loss is observed from multiple endpoints deployed on two different vPC leaf switches.	4.2(6o)
CSCvx31968	When pushing the new VMware VMM domain to VMware vCenter 7, the task "Reconfigure Distributed Port Group" for the DV-uplink-group completes with a status of "Link Aggregation Control Protocol group configured on <VMM_domain_name> conflicts with the Link Aggregation Control Protocol API version multipleLag." No fault is raised on the Cisco APIC.	4.2(6o)
CSCvx73311	The "df -h" and "ls -al /tmp/" commands hang. High CPU utilization seen from glusterd. The "cat /sys/fs/cgroup/pids/system.slice/system-gluster.slice/glusterd.service/pids.current" command shows a number approaching 100.	4.2(6o)
CSCvx79980	In a setup with 3 hosts from the same domain that have some number of virtual machines under them and the reserve host and other parameters are selected, after starting the "Migrate to ACI Virtual Edge" process, all hosts start to move at same time, causing a resource crunch. This issue occurs only once in a while. In a normal scenario, the hosts migrate one by one.	4.2(6o)
CSCvx45585	The urlToken is not returned after logging in to the Cisco APIC.	4.2(6l)
CSCvx13971	Unexpected behavior during certain upgrade/downgrade scenarios can occur when using the redistribute direct feature and attached host feature.	4.2(6h)
CSCvg00627	A tenant's flows/packets information cannot be exported.	4.2(6d)
CSCvo41153	We do not support a bridge domain in hardware proxy mode for flood in encapsulation. However, there is no warning or validation in the GUI. This bug is to add validation and a warning message when the user is trying to configure flood in encapsulation.	4.2(6d)
CSCvo87667	Post reload, the IGMP snooping table is not populated even when the IGMP report is sent by the receiver.	4.2(6d)
CSCvq54761	The application EPG or the corresponding bridge domain's public subnet may be advertised out of an L3Out in another VRF instance without a contract with the L3Out under certain conditions.	4.2(6d)
CSCvq95687	Currently, under Fabric > Inventory > Pod > Leaf Switch > General, the memory usage takes in consideration the MemFree field rather than the MemAvailable, which would be a more accurate representation of the usable memory in the system. In some cases, the GUI might show that the memory utilization is around 90% while in reality it's 50%, because there is still the cached/buffered memory to take into account. This buffered/cached memory will free up a big chunk of memory in case more memory is needed.	4.2(6d)

© 2024 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description	Fixed in
CSCvs01864	This bug is an enhacement to add an option to configure an interface description for subport blocks in the Cisco APIC GUI.	4.2(6d)
CSCvs49777	Cisco Application Policy Infrastructure Controller (APIC) includes a version of SQLite that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:CVE-2019-5018This bug was opened to address the potential impact on this product.	4.2(6d)
CSCvs51137	Creating a new interface policy group with a different LACP policy or LLDP/CDP policy results in changes in the VMM vSwitch policy of the AEP, which brings down the DVS.	4.2(6d)
CSCvt34925	This bug is an enhancement to enable the configuring of SNMPv3 with SHA2 and AES256. This configuration is needed for as a security enhancement.	4.2(6d)
CSCvt50251	CloudSec encryption may not function when certain features are enabled, such as remote leaf switches and Cisco ACI Multi-Site intersite L3Outs.	4.2(6d)
CSCvt68314	Fault F0948 is raised in the fabric, where the child-most affected object is " rsBDToProfile" .	4.2(6d)
CSCvt94286	Deploy the TACACS server for in-band management. When adding or modifying the TACACS+ provider key, the Cisco APIC can be reached only through SSH and the login fails on the fabric. After deleting the provider entry and reconfiguring, the fabric can be logged into.	4.2(6d)
CSCvu04758	Faults F115712 and F114632 are seen on virtual leaf switch interfaces and the faults are repeatedly raised and cleared every few minutes.	4.2(6d)
CSCvu34069	APIC ->System- >Controller -> topology displays that APIC2 is connected to both pod1 and pod2	4.2(6d)
CSCvu36682	After upgrading to release 4.2(3q), the Event Manger generates a core and crashes continuously, leading to a diverged cluster.	4.2(6d)
CSCvu49644	A tunnel endpoint doesn't receive a DHCP lease. This occurs with a newly deployed or upgraded Cisco ACI Virtual Edge.	4.2(6d)
CSCvu58269	DHCP clients in the Cisco ACI fabric fail to obtain addresses from a DHCP server if inter-VRF DHCP is being used and the DHCP provider is an L3Out in a different VRF table than the client.	4.2(6d)
CSCvu59991	Syslog messages are not sent to the inband virtual machine after adding or deleting an inband VRF table.	4.2(6d)
CSCvu60050	Traffic drops between select EPGs involved in shared-service contract. The shared routes gets programmed with a pctag of 0 which causes traffic from the source EPG to the destination to get dropped.	4.2(6d)
CSCvu72345	When using the Visibility & Troubleshooting tool for the reachability of two endpoints, there are errors such as " Bad Gateway" and " The server is temporarily busy due to a higher than usual request volume. Please try again later."	4.2(6d)
CSCvu84392	The policy-mgr crashes on multiple Cisco APICs during an upgrade.	4.2(6d)

© 2024 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description	Fixed in
CSCvv00341	After a switch replacement, the Cisco APIC will no longer be able to run show commands on it, such as " fabric 101 show int bri" , where " 101" is the Node ID of the replaced switch. The Cisco APIC will be able to send the command to the switch, but the return will be empty due to an old SSH key (the key of the old switch).	4.2(6d)
CSCvv01908	APIC fabricId is incorrectly reported as 1 by topSystem managed object, even if the Cisco APIC fabricId is configured as a different value at initial setup.	4.2(6d)
CSCvv08475	When using the command " show run vpc context," some of the leaf switch pairs are not included in the output.	4.2(6d)
CSCvv14321	In the GUI, after expanding the contract and clicking on the subject, it takes approximately 10-20 seconds to load the configured filters.	4.2(6d)
CSCvv15139	The " Locator LED" and " Indicator LED Color" fields in the Cisco APIC GUI for a physical interface do not accurately reflect the state of the locator LED. If you change the state of the Locator LED, the change will not be reflected in the GUI, but will be pushed to the switch correctly.	4.2(6d)
CSCvv15930	Visibility & Troubleshooting tool returns " Internal query error:list index out of range" followed by " Server API calls return error. Please click OK to go back to the first page." .	4.2(6d)
CSCvv17139	Cisco ACI snapshots cannot be compared and the following error is generated: File SNAPSHOT_NAME is not a valid snapshot. Could not parse NAPSHOT_NAME_1.json: Invalid control character at: line 1 column X	4.2(6d)
CSCvv21442	The Cisco APIC does not allow an upgrade to be cancelled. Rolling back the target version after an upgrade is started does not stop the upgrade and may cause Cisco APIC database loss. This enhancement is filed to block a Cisco APIC target version change unless the following conditions are met: 1. All Cisco APICs are online and the cluster is fully fit. 2. The upgrade job (maintUpgJob) for all Cisco APICs are completed. 3. The Installer.py process is not running on any of the Cisco APICs.	4.2(6d)
CSCvv25475	After a delete/add of a Cisco ACI-managed DVS, dynamic paths are not programmed on the leaf switch and the compRsDlPol managed object has a missing target. The tDn property references the old DVS OID instead of the latest value.	4.2(6d)
CSCvv28749	A bridge domain subnet is explicitly marked as public. The same EPG subnet has the shared flag enabled and has an implicit private scope. The private scope should take precedence over the public scope and should not get advertised. However, the bridge domain subnet does get advertised through the L3Out.	4.2(6d)
CSCvv30303	The configuration of a bridge domain subnet scope as " public" and an EPG scope as " private" should not be allowed.	4.2(6d)
CSCvv37322	In the Common tenant, clicking on an FHS policy for the first time generates a POST and that gets sent from the GUI as the logged in user to create the child raguardpol. There is no confirmation or notification. However, in the audit logs, there is an entry to log this configuration. Location in GUI: First Hop Security policy under Common tenant ---> Policies ---> Protocol ---> First Hop Security ---> Feature Policies --> Default	4.2(6d)

© 2024 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description	Fixed in
CSCvv38458	Interface counters are cleared successfully in the CLI, but the original CRC stomped value is still observed in the GUI.	4.2(6d)
CSCvv38465	Mroute will not be populated into MRIB. Leaf shows we process the PIM register which should in turn populate the mroute entry but it does not due to this threshold being exceeded.	4.2(6d)
CSCvv41784	EIGRP summary routes are not advertised from one of the many interfaces under same interface profile.	4.2(6d)
CSCvv46447	The following errors are seen on a Cisco APIC. GUI: Error the messaging layer was unable to deliver the stimulus (connection error, Address already in use) CLI: apic# show controller Bind failed. Error Code : 98 Message: Address already in use	4.2(6d)
CSCvv50268	Port-groups named "||" may be created in VMware vCenter when a vmmEpPD MO (VMM port group) is not present when the l3extRsDynPathAtt (L3Out dynamic attachment) associated with a vmmDom is deleted. L3Out dynamic attachments in VMM are created when the floating SVI feature is implemented on the L3Outs. The port-groups named "||" that get installed in VMware vCenter can cause bug CSCvu41160 to occur, where the Cisco APIC is unable to properly parse the port group names. Bug CSCvu41160 prevents the parsing issue, while this bug aims to prevent the "||" port-group creation in the first place.	4.2(6d)
CSCvv50789	Configuring Logical Interface Profile in L3Out, "Forwarding IP Address" box may or may not show up.	4.2(6d)
CSCvv52392	When executing "show running-config" or "show running-config vpc" from the Cisco APIC while running a 4.2 release, the following errors can be seen: Error while processing mode: vpc Error while processing mode: configure Error: Incorrect Pod ID 3 for node 3201 in dn	4.2(6d)
CSCvv55905	The configuration from the GUI is accepted, but is reverted back after submission. The underlying problem is that the Cisco APIC policy distributor process continues to retry the same tasks after 4 to 5 minutes because there is no ACK for the completion by the Cisco APIC policy manager. Because of this issue, any recently-implemented configuration (using the GUI or REST API) is not processed, but gets stuck in the queue.	4.2(6d)
CSCvv60463	Without Intersight enabled, there is an alert under the GUI notifications: Intersight Proxy not configured Configure Intersight Proxy to use the Network Insights - Base application for free. Configure Proxy from Intersight	4.2(6d)
CSCvv60573	The following error message in appears in the GUI for Fibre Channel interfaces on N9K-C93180YC-FX: "Configuration is mismatch with applied interface"	4.2(6d)

© 2024 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description	Fixed in
CSCvv62861	A leaf switch reloads due to an out-of-memory condition after changing the contract scope to global.	4.2(6d)
CSCvv64745	An SNMP v3 trap is sent 2 minutes after a PSU is removed from the Cisco APIC.	4.2(6d)
CSCvv65304	Running 'acidiag verifyapic' on a newly-received Cisco APIC with a previously-identified cert subject difference will return "apic_cert_format_check: failed".	4.2(6d)
CSCvv68416	vAPIC does not take the latest passphrase from the GUI when sending a certificate request.	4.2(6d)
CSCvv70570	A standby Cisco APIC doesn't upgrade during a Cisco APIC cluster upgrade and raises fault F1824.	4.2(6d)
CSCvv82431	The policy manager crashes consistently and eventually stops running. The Cisco APIC cluster becomes diverged.	4.2(6d)
CSCvv83486	After deleting the OnDemand tech-support policy following the workaround for CSCvk60397, one fault F0756 was still seen.	4.2(6d)
CSCvv85990	In the L3Out creation wizard, the node profile and interface profile name changes to default if you change the node profile and interface profile names on page 2, then you return to page 1. The values of the other fields retain their configured values. For the interface profile name, this issue is only seen with an SVI vPC.	4.2(6d)
CSCvv86355	The Logical Interface Profiles (Folder) shows different IP addresses assigned to each interface than what is configured in the interface profile. This is a cosmetic issue because the interfaces are programmed correctly.	4.2(6d)
CSCvv87993	Some configuration is missing on a switch node due to the corresponding policies not being pushed to the switch from the Cisco APIC. This may manifest as a vast variety of symptoms depending on which particular policies weren't pushed.	4.2(6d)
CSCvv88974	When a route-map is configured using match rules (prefix-list), the CLI output of show running-config shows the wrong prefix length. Only "le 32|128" is displayed in the CLI regardless of the actual range configured in GUI.	4.2(6d)
CSCvv95671	The appliance element DME fails to subscribe to the policy from policymgr DME, which prevents the Cisco APIC from being able to configure the inband interface.	4.2(6d)
CSCvv99002	If a Cisco APIC is accidentally powered off while the initial setup script running, the initial setup will not start at next boot time. The previous admin password can be used to log in, and the Cisco APIC boots with the last running configuration.	4.2(6d)
CSCvw00513	The Cisco APIC fails to start the auditd service and the following message is displayed on the console when apic boots up: [FAILED] Failed to start Security Auditing Service.	4.2(6d)
CSCvw01447	When creating a new SNMP monitoring destination group, you will get a warning that "the value in this field is invalid" if you start the string with numbers for the community name. This was allowed in previous versions.	4.2(6d)
CSCvw05086	An interface between a leaf switch and spine switch is brought down into the out-of-service state, accompanied with fault F0454 (out of service due to Controller UUID mismatch).	4.2(6d)

© 2024 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description	Fixed in
CSCvw05302	+ ACI reports fault F1419. + The processes show process ID zero from the scheduler. + The processes are actually running when checked using systemctl with root access.	4.2(6d)
CSCvw11709	If a PBR service graph is applied between two EPGs of the same VRF table, then when the PBR node is located in a different VRF table (which is not a supported configuration), a drop rule gets installed in the PBR VRF table to drop all traffic with a source pcTag of the provider of the service graph.	4.2(6d)
CSCvw27947	A Cisco APIC upgrade gets stuck in the scheduled state.	4.2(6d)
CSCvw33173	The message " Faults/health summary disabled due to max limit reached" is visible under Fabric -> Inventory -> Topology -> Summary, even when the user has not reached the documented limit.	4.2(6d)
CSCvw33277	The fault F3227 " ACI failed processing an already accepted configuration change" continuously gets raised.	4.2(6d)
CSCvw37981	Selecting an external IP address that is reachable from a single L3Out, the Cisco APIC shows the following error: " Not Supported: External address <External-IP> is reachable from GOLF interface" .	4.2(6d)

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 4.2(6) releases in which the bug exists. A bug might also exist in releases other than the 4.2(6) releases.

Bug ID	Description	Exists in
N/A	If you are upgrading to Cisco APIC release 4.2(6o) 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.	4.2(6o) and later
CSCvj26666	The " show run leaf|spine <nodeId>" command might produce an error for scaled up configurations.	4.2(6d) and later
CSCvj90385	With a uniform distribution of EPs and traffic flows, a fabric module in slot 25 sometimes reports far less than 50% of the traffic compared to the traffic on fabric modules in non-FM25 slots.	4.2(6d) and later
CSCvq39764	When you click Restart for the Microsoft System Center Virtual Machine Manager (SCVMM) agent on a scaled-out setup, the service may stop. You can restart the agent by clicking Start.	4.2(6d) and later

© 2024 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description	Exists in
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)	4.2(6d) 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.	4.2(6d) and later
CSCvs19322	Upgrading Cisco APIC from a 3.x release to a 4.x release causes Smart Licensing to lose its registration. Registering Smart Licensing again will clear the fault.	4.2(6d) and later
CSCvs77929	In the 4.x and later releases, if a firmware policy is created with different name than the maintenance policy, the firmware policy will be deleted and a new firmware policy gets created with the same name, which causes the upgrade process to fail.	4.2(6d) 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.	4.2(6d) 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.	4.2(6d) 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.	4.2(6d) 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.	4.2(6d) 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.	4.2(6d) and later

© 2024 Cisco and/or its affiliates. All rights reserved.

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.	4.2(6d) 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 4.2(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 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

© 2024 Cisco and/or its affiliates. All rights reserved.

Product ID	Description
	ports)

The following list includes general hardware compatibility information:

- For the supported hardware, see the Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 14.2(6).
- 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. **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 supporFut 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

© 2024 Cisco and/or its affiliates. All rights reserved.

Product ID	Description
	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.

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 release supports the following products:

Product	Supported Release
Cisco NX-OS	14.2(6)
Cisco AVS	5.2(1)SV3(4.10) For more information about the supported AVS releases, see the AVS software compatibility information in the Cisco Application Virtual Switch Release Notes, Release 5.2(1)SV3(4.11).
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	• 4.3.2.240009 CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) • 4.2(3e) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.2(3b) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.2(2a) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(3m) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(3f) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(3d) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(3c) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(2m) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) • 4.1(2k) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) • 4.1(2g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) • 4.1(2b) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) • 4.1(1g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3)

© 2024 Cisco and/or its affiliates. All rights reserved.

Product	Supported Release
	• 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 4.2(x).
- For compatibility with OpenStack and Kubernetes distributions, see the Cisco Application Policy Infrastructure Controller Container Plug-in Release 4.2(3), Release Notes.
- 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

© 2024 Cisco and/or its affiliates. All rights reserved.

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 ACI Virtual Edge Release Notes, Release 2.2(6)	The release notes for Cisco ACI Virtual Edge.
Cisco ACI Virtual Pod Release Notes, Release 4.2(6)	The release notes for Cisco ACI Virtual Pod.
Cisco Application Centric Infrastructure Simulator Appliance Release Notes, Release 4.2(6)	The release notes for the Cisco ACI Simulator Appliance.
Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 14.2(6)	The release notes for Cisco NX-OS for Cisco Nexus 9000 Series ACI-Mode Switches.
Verified Scalability Guide for Cisco APIC, Release 4.2(6), Multi-Site, Release 3.0(4), and Cisco Nexus 9000 Series ACI-Mode Switches, Release 14.2(6)	This guide contains the maximum verified scalability limits for Cisco Application Centric Infrastructure (ACI) parameters for Cisco APIC, Cisco ACI Multi-Site, 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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2020-2024 Cisco Systems, Inc. All rights reserved.