



Cisco Application Policy Infrastructure Controller Release Notes, Release 4.2(1)

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

The [Cisco Application Centric Infrastructure Fundamentals, Release 4.2\(x\)](#) document provides complete details about the Cisco ACI, including a glossary of terms that are used in the Cisco ACI.

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

Note: Use this document with the [Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 14.2\(1\)](#).

Release notes are sometimes updated with new information about restrictions and bugs. See the following website for the most recent version of this document:

<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

You can watch videos that demonstrate how to perform specific tasks in the Cisco APIC on the [Cisco ACI YouTube channel](#).

For the verified scalability limits (except the CLI limits), see the [Verified Scalability Guide for Cisco APIC, Release 4.2\(1\), Multi-Site, Release 2.2\(1\), and Cisco Nexus 9000 Series ACI-Mode Switches, Release 14.2\(1\)](#).

For the CLI verified scalability limits, see the [Cisco APIC NX-OS Style CLI Configuration Guide, Release 4.2\(x\)](#).

Note: The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Table 1 shows the online change history for this document.

Table 1 Online History Change

| Date | Description |
|-------------------|---|
| December 9, 2022 | In the Open Bugs section, added bug CSCvw33061. |
| November 18, 2022 | In the Open Issues section, added bug CSCwc66053. |

Contents

| Date | Description |
|--------------------|--|
| August 1, 2022 | In the Miscellaneous Compatibility Information section, added: <ul style="list-style-type: none"> ■ 4.2(2a) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) ■ 4.1(2k) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) |
| March 21, 2022 | In the Miscellaneous Compatibility Information section, added: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 4.1(2g) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) |
| November 2, 2021 | In the Miscellaneous Compatibility Information section, added: <ul style="list-style-type: none"> ■ 4.1(3d) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) |
| August 4, 2021 | In the Open Issues section, added bugs CSCvy30453 and CSCvy44940. |
| July 26, 2021 | In the Miscellaneous Compatibility Information section, the CIMC 4.1(3c) release is now recommended for UCS C220/C240 M5 (APIC-L3/M3). |
| March 25, 2021 | In the Open Bugs section, added bug CSCvu74478. |
| March 11, 2021 | In the Miscellaneous Compatibility Information section, for CIMC HUU ISO, added: <ul style="list-style-type: none"> ■ 4.1(3b) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) Changed: <ul style="list-style-type: none"> ■ 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3) To: <ul style="list-style-type: none"> ■ 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) |
| February 9, 2021 | In the Open Bugs section, added bug CSCvt07565. |
| February 3, 2021 | In the Miscellaneous Compatibility Information section, for CIMC HUU ISO, added: <ul style="list-style-type: none"> ■ 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3) |
| September 29, 2020 | In the Miscellaneous Compatibility Information section, specified that the 4.1(1f) CIMC release is deferred. The recommended release is now 4.1(1g). |
| September 16, 2020 | In the Known Behaviors section, added the bullet that begins with: Beginning in Cisco APIC release 4.1(1), the IP SLA monitor policy validates the IP SLA port value. |
| April 17, 2020 | In the Miscellaneous Compatibility Information section, updated the CIMC HUU ISO information to include the 4.1(1c) and 4.1(1d) releases. |

Contents

| Date | Description |
|--------------------|---|
| March 6, 2020 | In the Miscellaneous Compatibility Information section, updated the CIMC HUU ISO information for the 4.0(2g) and 4.0(4e) CIMC releases. |
| January 7, 2020 | <p>In the Changes in Behavior section, added the following bullet:</p> <ul style="list-style-type: none"> ■ When you create a bridge domain using the Cisco APIC GUI, the ARP flooding option is now enabled by default. The ARP flooding option is still disabled by default when you use the create a bridge domain using the CLI or REST API. |
| October 29, 2019 | 4.2(1i): Release 4.2(1i) became available. Added the resolved bugs for this release. |
| October 8, 2019 | <p>In the Miscellaneous Compatibility Information section, updated the supported 4.0(4), 4.0(2), and 3.0(4) CIMC releases to:</p> <ul style="list-style-type: none"> — 4.0(4e) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3) — 4.0(2g) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) — 3.0(4i) CIMC HUU ISO (recommended) for UCS C220/C240 M3 (APIC-L1/M1) |
| October 4, 2019 | <p>In the Miscellaneous Guidelines section, added the following bullet:</p> <ul style="list-style-type: none"> ■ When you create an access port selector in a leaf interface rofile, the fexId property is configured with a default value of 101 even though a FEX is not connected and the interface is not a FEX interface. The fexId property is only used when the port selector is associated with an infraFexBndlGrp managed object. |
| October 3, 2019 | <p>In the Miscellaneous Guidelines section, added the bullet that begins as follows:</p> <ul style="list-style-type: none"> ■ Fabric connectivity ports can operate at 10G or 25G speeds (depending on the model of the APIC server) when connected to leaf switch host interfaces. |
| September 24, 2019 | <p>4.2(1i): In the Open Bugs section, added bug CSCvr25643.</p> <p>4.2(1j): In the Resolved Bugs section, added bug CSCvr25643.</p> |
| September 20, 2019 | 4.2(1j): Release 4.2(1j) became available. Added the resolved bugs for this release. |
| September 10, 2019 | <p>In the Known Behaviors section, added the following bullet:</p> <ul style="list-style-type: none"> ■ When there are silent hosts across sites, ARP glean messages might not be forwarded to remote sites if a 1st generation ToR switch (switch models without -EX or -FX in the name) happens to be in the transit path and the VRF is deployed on that ToR switch, the switch does not forward the ARP glean packet back into the fabric to reach the remote site. This issue is specific to 1st generation transit ToR switches and does not affect 2nd generation ToR switches (switch models with -EX or -FX in the name). This issue breaks the capability of discovering silent hosts. |
| September 8, 2019 | 4.2(1i): Release 4.2(1i) became available. |

Contents

This document includes the following sections:

- [New and Changed Information](#)
- [Upgrade and Downgrade Information](#)
- [Bugs](#)
- [Compatibility Information](#)
- [Usage Guidelines](#)
- [Related Documentation](#)

New and Changed Information

This section lists the new and changed features in this release and includes the following topics:

- [New Software Features](#)
- [New Hardware Features](#)
- [Changes in Behavior](#)

New Software Features

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

Table 2 New Software Features

| Feature | Description | Guidelines and Restrictions |
|--|--|-----------------------------|
| Ability to pin EPGs to an uplink on a VMware DVS | You can configure up to 32 uplinks for each instance of Cisco ACI Virtual Edge (in native switching mode) or VMware VDS. You also can rename the uplinks and configure failover for them within endpoint groups (EPGs) associated with the VMware VDS or Cisco ACI Virtual Edge. | None. |
| avread CLI command | Cisco APIC Release 4.2.(1) introduces the new avread command, which provides the same information as the acidiag avread command, but in a tabular format. For more information, see the Cisco APIC Troubleshooting Guide, Release 4.2(x) . | None. |
| BGP neighbor shutdown | The BGP neighbor shutdown feature is similar to the neighbor shutdown command in NX-OS, which shuts down the corresponding BGP neighbor. Use this policy to disable and enable the BGP neighbor's admin state. Using this feature shuts down the BGP sessions without the | None. |

New and Changed Information

| Feature | Description | Guidelines and Restrictions |
|---|--|---|
| | <p>need to delete the BGP peer configuration.</p> <p>For more information, see the Cisco APIC and BGP Neighbor Shutdown and Soft Reset document.</p> | |
| BGP neighbor soft reset | <p>The BGP neighbor soft reset feature provides automatic support for a dynamic soft reset of inbound and outbound BGP routing table updates that are not dependent upon stored routing table update information. Use this policy to enable the soft dynamic inbound reset and soft outbound reset.</p> <p>For more information, see the Cisco APIC and BGP Neighbor Shutdown and Soft Reset document.</p> | None. |
| Blocking ACI upgrades or downgrades if faults are present | <p>Beginning with release 4.2(1), when you attempt to trigger an upgrade or downgrade operation, the operation might be blocked if any faults on the fabric are detected, depending on the severity of the fault detected.</p> <p>For more information, see the Cisco APIC Installation, Upgrade, and Downgrade Guide.</p> | None. |
| cluster_health CLI command | <p>Cisco APIC Release 4.2.(1) introduces the new cluster_health command, which enables you to verify the Cisco APIC cluster status.</p> <p>For more information, see the Cisco APIC Troubleshooting Guide, Release 4.2(x).</p> | None. |
| fd_vlan mismatch enhancement | <p>If the same VLAN pool is being used on both a vPC and an orphan port, a fd_vlan mismatch will occur and a fault will be raised.</p> | None. |
| Floating Layer 3 Outside network connection | <p>You can configure a floating L3Out that allows a virtual router to move from under one leaf switch to another. The feature saves you from having to configure multiple L3Out interfaces to maintain routing when virtual machines move from one host to another. This feature is supported for VMware VDS.</p> | None. |
| IPv6 multicast support | <p>IPv6 multicast is now enabled with PIM6 protocol settings.</p> <p>For more information, see the Cisco ACI Support for Layer 3 IPv6 Multicast document.</p> | None. |
| Policy-based redirect backup policy | <p>This feature enables you to configure a backup node for a policy-based redirect (PBR) policy. If an active node goes down, traffic gets routed through the backup node instead of getting routed through one of the other active nodes. The backup node avoids a situation in which the connection could be reset if, for example, the data paths through another active node are traversing stateful</p> | <p>The backup policy option is supported only on leaf switches that have -EX or a later designation in the product ID.</p> <p>Resilient hashing must be</p> |

| Feature | Description | Guidelines and Restrictions |
|--|---|--|
| | <p>firewalls.</p> <p>For more information, see the Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.2(x).</p> | <p>enabled.</p> <p>Only Layer 3 PBR destinations are supported.</p> <p>Multiple backup PBR destinations per backup policy can be configured.</p> <p>For additional guidelines and restrictions, see the Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.2(x).</p> |
| <p>Redistributing static routes to BGP with prefix list</p> | <p>For Cisco APIC releases before release 4.2(1), you can configure a route map policy for the redistribution of static routes into BGP using the Create Route Map/Profile feature, which defines the route map for BGP dampening and route redistribution.</p> <p>This feature is used to set attributes, such as community, on certain static routes on one border leaf switch, and then, based on these attributes, configure these routes on other border leaf switches</p> <p>Beginning with Cisco APIC Release 4.2(1), this feature is extended for static routes. This allows you to configure a route map policy that will be applied while redistributing static routes into BGP.</p> <p>For more information, see the Cisco APIC and Redistributing Static Routes to BGP With Prefix List document.</p> | <p>None.</p> |
| <p>Route control on an aggregator route during import/export</p> | <p>When creating a subnet, the export route control subnet and import route control subnet allow Aggregate Export and Aggregate Import.</p> <p>For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 4.2(x).</p> | <p>None.</p> |
| <p>Route control per BGP peer</p> | <p>Route control policies determine what routes are advertised out to the external network (export) or allowed into the fabric (import).</p> <p>Prior to Cisco APIC release 4.2(1), you configure these policies at the L3Out level, under the L3Out profile (l3extInstP) or through the L3Out subnet under the L3Out (l3extSubnet), so those policies apply to protocols configured for all nodes or paths included in the L3Out. With this configuration, there could be multiple node</p> | <p>You must configure route profiles used per BGP peer under a tenant.</p> <p>The methods to configure route map match, set rule or route profile, and the behavior of each of those components, do not change from previous releases.</p> |

New and Changed Information

| Feature | Description | Guidelines and Restrictions |
|-------------------------------|--|--|
| | <p>profiles configured in the L3Out, and each could have multiple nodes or paths with the BGP neighbor specified. Because of this, there is no way to apply individual policies to each protocol entity.</p> <p>Beginning with Cisco APIC release 4.2(1), the route control per BGP peer feature is introduced to begin to address this situation, where more granularity in route export and import control is needed.</p> <p>For more information, see the Cisco APIC and Route Control Per BGP Peer document.</p> | <p>The route profile for this feature can only be set to Match Routing Policy Only (global policy), where the route profile is the only source of information to generate the per BGP peer route map. You cannot set the route profile for this feature to Match Prefix and Routing Policy.</p> <p>In addition, you must explicitly specify the bridge domain subnets in the prefix list if you want them to be exported.</p> <p>For additional guidelines and restrictions, see the Cisco APIC and Route Control Per BGP Peer document.</p> |
| SDWAN integration enhancement | <p>This release adds support for enabling returning traffic from a remote site that is destined for the ACI data center to receive differentiated services over the WAN. After the tenant admin registers the Cisco APIC to vManage, the Cisco APIC pulls the WAN-SLA policies and the WAN-VPN from vManage. Then, the Cisco APIC assigns a DSCP to each WAN-SLA policy and pushes a prefix list. The prefix list, which is taken from the EPG if the contract between this EPG and L3Out has WAN-SLA configured, enables quality of service on the returning traffic. The WAN-SLA policy and WAN-VPN are both available in the tenant common. Tenant admins map the WAN-VPNs to VRF instances on remote sites.</p> <p>For more information, see the Cisco ACI and SDWAN Integration KB article.</p> | None. |
| Simplified ELAM output | <p>This release adds an option to the Embedded Logic Analyzer Module (ELAM) tool that changes the output to a human-readable format, which enables you to find key information quickly and more efficiently. In addition, hexadecimal values have been converted to decimal values in some instances for improved readability. For backward compatibility, the existing usage of ELAM is kept intact.</p> <p>For more information, see the Cisco APIC Troubleshooting Guide, Release 4.2(x).</p> | This feature is supported only on switch models with EX, FX, or FX2 at the end of the switch name. |

| Feature | Description | Guidelines and Restrictions |
|-----------------------------|---|--|
| Storm control SNMP traps | This release supports triggering SNMP traps from Cisco ACI when storm control thresholds are met. | <p>There are two actions associated with storm control: drop and shutdown. With the shutdown action, interface traps will be raised, but the storm control traps to indicate that the storm is active or clear is not determined by the shutdown action. Storm control traps with the shutdown action on the policy should therefore be ignored.</p> <p>If the ports flap with the storm control policy on, clear and active traps are seen together when the stats are collected. Clear and active traps are typically not seen together, but this is expected behavior in this case.</p> <p>This feature is not supported on Cisco Nexus C93128TX, C9396PX, C9396TX, C93120TX, C9332PQ, C9372PX, C9372TX, C9372PX-E, nor C9372TX-E switches.</p> |

New Hardware Features

For new hardware features, see the [Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 4.2\(1\)](#).

Changes in Behavior

For the changes in behavior, see the [Cisco ACI Releases Changes in Behavior](#) document.

Upgrade and Downgrade Information

For upgrade and downgrade considerations for the Cisco APIC, see the "Upgrading and Downgrading the Cisco APIC and Switch Software" section of the [Cisco APIC Installation, Upgrade, and Downgrade Guide](#).

Bugs

This section contains lists of open and resolved bugs and known behaviors.

Bugs

- [Open Bugs](#)
- [Resolved Bugs](#)
- [Known Behaviors](#)

Open Bugs

This section lists the open bugs. Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Exists In" column of the table specifies the 4.2(1) releases in which the bug exists. A bug might also exist in releases other than the 4.2(1) releases.

Table 3 Open Bugs in This Release

| Bug ID | Description | Exists in |
|----------------------------|---|-------------------|
| CSCvr89940 | An APIC tenant purge fails after the OpenStack project is deleted if the public OpenStack endpoint URL access is blocked from the OpenStack mgmt network. | 4.2(1l) and later |
| CSCvt03360 | Zookeeper creates transactions files when the cluster is converging. During long periods of network unreachability, these files may get created at a more frequent rate, leading to space filling up. | 4.2(1l) and later |
| CSCvr48322 | When there are standby APICs in the fabric, the "show controller" command will take time to process the command. | 4.2(1j) and later |
| CSCvr77120 | When configuring a vzAny contract (regardless of the details) as a "Provided" contract, the command "show vrf XYZ detail" executed directly in the APIC CLI will display it as "Consumed" , and if configured as "Consumed" , it will show it as "Provided" . | 4.2(1j) and later |
| CSCvr89025 | If a Cisco APIC is receiving a large number of DHCP requests with unique client addresses, each request will result in a unique dhcpClient managed object being created on the APIC in the requesting state. Depending on the number of unique requests, these could add up over time and cause the dhcpd process on the APIC to hit scale issues, potentially crashing, although the APIC itself will not crash and the dhcpd process will crash and recover. The dhcpd crashing issue was observed with the dhcpClient managed object count was over 4 million. | 4.2(1j) and later |
| CSCvs92041 | Service Graph rendering fails if a service graph is attached to a unidirectional filter in a contract subject. For example: filter chain for provider to consumer: use service graph with PBR filter chain for consumer to provider: no service graph | 4.2(1j) and later |
| CSCvt01558 | A Cisco APIC might report high memory utilization when polling through SNMP. | 4.2(1j) and later |
| CSCvt07825 | After removing a configuration from Cisco ACI Multi-Site, the fabric nodes started reloading. The "show system reset-reason" command shows the following: Reason: reset-triggered-due-to-ha-policy-of-reset Service:policy_mgr hap reset | 4.2(1j) and later |

Bugs

| Bug ID | Description | Exists in |
|----------------------------|---|-------------------|
| CSCvt08833 | In a transit L3Out, after adding one new static route (a subnet of a summary route) on a border leaf switch, the OSPF summary route disappears from the route table of the border leaf switch because the route is deleted. | 4.2(1j) and later |
| CSCwv87993 | 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(1j) and later |
| CSCvd43548 | The stats for a given leaf switch rule cannot be viewed if a rule is double-clicked. | 4.2(1i) and later |
| CSCvd66359 | The Port ID LLDP Neighbors panel displays the port ID when the interface does not have a description. Example: Ethernet 1/5, but if the interface has description, the Port ID property shows the Interface description instead of the port ID. | 4.2(1i) 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(1i) and later |
| CSCvf70411 | A route will be advertised, but will not contain the tag value that is set from the VRF route tag policy. | 4.2(1i) and later |
| CSCvg00627 | A tenant's flows/packets information cannot be exported. | 4.2(1i) 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(1i) and later |
| CSCvg81020 | For strict security requirements, customers require custom certificates that have RSA key lengths of 3072 and 4096. | 4.2(1i) and later |
| CSCvh52046 | This is an enhancement to allow for text-based banners for the Cisco APIC GUI login screen. | 4.2(1i) and later |
| CSCvh54578 | For a client (browser or ssh client) that is using IPv6, the Cisco APIC aaaSessionLR audit log shows "0.0.0.0" or some bogus value. | 4.2(1i) and later |
| CSCvh59843 | Enabling Multicast under the VRF on one or more bridge domains is difficult due to how the drop-down menu is designed. This is an enhancement request to make the drop-down menu searchable. | 4.2(1i) and later |

Bugs

| Bug ID | Description | Exists in |
|----------------------------|---|-------------------|
| 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(1i) and later |
| CSCvi82903 | When authenticating with the Cisco APIC using ISE (TACACS), all logins over 31 characters fail. | 4.2(1i) and later |
| CSCvj14053 | The health status of DHCP was not updated after a leaf switch upgrade for some of the leaf switches. | 4.2(1i) and later |
| CSCvj56726 | The connectivity filter configuration of an access policy group is deprecated and should be removed from GUI. | 4.2(1i) and later |
| CSCvk04072 | There is no record of who acknowledged a fault in the Cisco APIC, nor when the acknowledgement occurred. | 4.2(1i) and later |
| CSCvk18014 | The action named 'Launch SSH' is disabled when a user with read-only access logs into the Cisco APIC. | 4.2(1i) and later |
| CSCvm32345 | A port group cannot be renamed. This is an enhancement request to enable the renaming of port groups. | 4.2(1i) and later |
| CSCvm42914 | This is an enhancement request to add policy group information to the properties page of physical interfaces. | 4.2(1i) and later |
| CSCvm56946 | Support for local user (admin) maximum tries and login delay configuration. | 4.2(1i) and later |
| CSCvm64933 | The Cisco APIC setup script will not accept an ID outside of the range of 1 through 12, and the Cisco APIC cannot be added to that pod. This issue will be seen in a multi-pod setup when trying add a Cisco APIC to a pod ID that is not between 1 through 12. | 4.2(1i) 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(1i) and later |
| CSCvo24284 | Fault delegates are raised on the Cisco APIC, but the original fault instance is already gone because the affected node has been removed from the fabric. | 4.2(1i) and later |
| CSCvo87667 | Post reload, the IGMP snooping table is not populated even when the IGMP report is sent by the receiver. | 4.2(1i) and later |
| CSCvp26694 | A leaf switch gets upgraded when a previously-configured maintenance policy is triggered. | 4.2(1i) and later |
| CSCvp62048 | New port groups in VMware vCenter may be delayed when pushed from the Cisco APIC. | 4.2(1i) and later |
| CSCvq22658 | Description fields are not available for resource pools (VLAN, VSAN, Mcast, VXLAN etc). | 4.2(1i) and later |

Bugs

| Bug ID | Description | Exists in |
|----------------------------|---|-------------------|
| CSCvq31052 | Log3 is sometimes missing from the switch techsupport logs on the APIC when selecting the controller as the export destination. | 4.2(1i) and later |
| 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(1i) 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.reslmedcy) 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 reslmedcy toggles between PreProv and OnDemand to reproduce the issue. | 4.2(1i) 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(1i) and later |
| CSCvq63842 | F0467 fault is present on the infra overlay L3Out when the domain is not associated correctly. However, this fault should not be raised on infra overlay L3Out even when the domain association is incorrect. | 4.2(1i) and later |
| CSCvq74727 | When making a configuration change to an L3Out (such as contract removal or addition), the BGP peer flaps or the bgpPeerP object is deleted from the leaf switch. In the leaf switch policy-element traces, 'isClassic = 0, wasClassic =1' is set post-update from the Cisco APIC. | 4.2(1i) and later |
| CSCvq80820 | A previously-working traffic is policy dropped after the subject is modified to have the "no stats" directive. | 4.2(1i) and later |
| CSCvq86573 | Under a corner case, the Cisco APIC cluster DB may become partially diverged after upgrading to a release that introduces new services. A new release that introduces a new DME service (such as the domainmgr in the 2.3 release) could fail to receive the full size shard vector update in first two-minute window, which causes the new service flag file to be removed before all local leader shards are able to boot into the green field mode. This results in the Cisco APIC cluster DB becoming partially diverged. | 4.2(1i) and later |
| CSCvq88632 | This is an enhancement request for allowing DVS MTU to be configured from a VMM domain policy and be independent of fabricMTU. | 4.2(1i) and later |
| CSCvq89967 | An OSPF L3Out with a check in the BGP check box is missing the redistribute route-map. | 4.2(1i) and later |
| CSCvq92628 | If you downgrade from a 4.2 release to a 4.1 release or from a 4.2 release to a 4.0 release with the PIM v6 checkbox enabled, and then you upgrade to 4.2, the PIM v6 interface will not be created. | 4.2(1i) and later |

Bugs

| Bug ID | Description | Exists in |
|-----------------------------|---|-------------------|
| CSCCvq95687 | 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(1i) and later |
| CSCCvq95817 | The F3083 fault is thrown, notifying the user that an IP address is being used by multiple MAC addresses. When navigating to the Fabric -> Inventory -> Duplicate IP Usage section, AVS VTEP IP addresses are seen as being learned individually across multiple leaf switches, such as 1 entry for Leaf 101, and 1 entry for Leaf 102. Querying for the endpoint in the CLI of the leaf switch ("show endpoint ip <IP>") shows that the endpoint is learned behind a port channel/vPC, and not an individual link. | 4.2(1i) and later |
| CSCCvq96516 | There is an event manager process crash. | 4.2(1i) and later |
| CSCCvq97675 | A service cannot be reached by using the APIC out-of-band management that exists within the 172.17.0.0/16 sub-net. This enhancement request implements the GUI option to change the Docker0 IP address. Bug CSCCve84297 implements REST API way to change it. | 4.2(1i) and later |
| CSCCvr10020 | Fault alarms get generated at a higher rate with a lower threshold. There is no functional impact. | 4.2(1i) and later |
| CSCCvr10510 | There is a stale F2736 fault after configuring in-band IP addresses with the out-of-band IP addresses for the Cisco APIC. | 4.2(1i) and later |
| CSCCvr11388 | When the VRF instance of both of the service device bridge domains is changed, the svcdirHealthGrp managed objects in the switch may not be created for the new VRF instance. As a result traffic will get impacted and there will be faults raised in the switch and in the APIC at the tenant level. | 4.2(1i) and later |
| CSCCvr12971 | The Cisco APIC GUI produces the following error messages when opening an EPG policy: Received Invalid Json String. The server returned an unintelligible response. This issue might affect backup/restore functionality. | 4.2(1i) and later |
| CSCCvr19693 | When configuring local SPAN in access mode using the GUI or CLI and then running the "show running-config monitor access session<session>" command, the output does not include all source span interfaces. | 4.2(1i) and later |
| CSCCvr25643 | In an ACI fabric, the vPC IP address is managed by the dhcpd process. Sometimes when deleting vPC/vPC domains, the clean up does not complete. The fabricExplicitGep managed object gets deleted, but the corresponding fabricVpcResource managed object does not get deleted. As a result, upon creating a new vPC pair, the dhcpd process might assign the same IP address that the deleted vPC had. The dhcpd process will crash while assigning a different IP address for second time because of this bug. | 4.2(1i) and later |
| CSCCvr30815 | vmmPLInf objects are created with epGKey's and DN's that have truncated EPG names (truncated at "."). | 4.2(1i) and later |

Bugs

| Bug ID | Description | Exists in |
|----------------------------|--|-------------------|
| CSCvr33833 | A static subnet can be configured under an EPG even if the EPG is a part of bridge domain that already is associated with another static subnet, and the subnet space is the same as or is a super range of the subnet space of the EPG. Therefore, there can be situations where both the bridge domain and associated EPG have the same subnets, or the EPG's subnet can be part of the bridge domain subnet at the same time. | 4.2(1i) and later |
| CSCvr36851 | Descending option will not work for the Static Ports table. Even when the user clicks descending, the sort defaults to ascending. | 4.2(1i) and later |
| CSCvr38278 | When using AVE with Cisco APIC, fault F0214 gets raised, but there is no noticeable impact on AVE operation: descr: Fault delegate: Operational issues detected for OpFlex device: ..., error: [Inventory not available on the node at this time] | 4.2(1i) and later |
| CSCvr41750 | Policies may take a long time (over 10 minutes) to get programmed on the leaf switches. In addition, the APIC pulls inventory from the VMware vCenter repeatedly, instead of following the usual 24 hour interval. | 4.2(1i) and later |
| CSCvr43275 | While configuring a node in-band address using a wizard or configuring a subnet under the bridge domain (tenant > bridge domain > subnet), and "x.x.x.0/subnet" is chosen as the range, the following message displays: Incorrect message " Error 400 - Broadcast IP x.x.x.0/subnet" during inband config | 4.2(1i) and later |
| CSCvr51069 | In some circumstances, fault F1188 is generated. This fault is cosmetic. | 4.2(1i) and later |
| CSCvr51121 | If the current VMware vCenter crashes and is not recoverable, then a new VMware vCenter with an identical configuration is built, the Cisco APIC pushes the DVS and Quarantine port-groups. However, the APIC does not push the EPG port group. | 4.2(1i) and later |
| CSCvr58476 | The Cisco ACI Simulator version 4.2 gets stuck at the "installing the APIC software, this may take a few minutes...." screen and the installation does not proceed. | 4.2(1i) 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(1i) and later |
| CSCvr67887 | Fault: F3060 "license-manager-license-authorization-expired" is raised although "show license status" shows the REGISTERED status and the license authorization shows AUTHORIZED. | 4.2(1i) and later |
| CSCvr75684 | The admin password of ACI fabric is initially configured using the setup-script during the APIC node initialization, for example pw1. After that, customer may choose to change the admin password to a new one such as pw2. The new password pw2 is not preserved in the event of a database clean-up, which causes pw1 to be required for after a clean reload. The impact to the operation team is that they may not always document the very first Cisco APIC password, hence they will not be able to login to the Cisco APIC again due to forgetting the original admin password if the Cisco APIC had to be clean reloaded. | 4.2(1i) and later |

Bugs

| Bug ID | Description | Exists in |
|----------------------------|---|-------------------|
| CSCvr76318 | Cisco ACI plugin containers do not get updated. | 4.2(1i) and later |
| CSCvr82224 | A leaf switch port flaps without raising a warning. | 4.2(1i) and later |
| CSCvr82304 | vPod deployment fails in the VMware vCenter plugin with the following error: "Deploy ACI Virtual Pod - An Error Occured" In the logs (/var/log/vmware/vsphere-client/logs/vsphere_client_virgo.log), the following error can be seen: The following PortGroup could not be resolved | 4.2(1i) and later |
| CSCvr85515 | When trying to track an AVE endpoint IP address, running the "show endpoint ip x.x.x.x" command in the Cisco APIC CLI to see the IP address and checking the IP address on the EP endpoint in the GUI shows incorrect or multiple VPC names. | 4.2(1i) and later |
| CSCvr85821 | The API query /api/class/compCtrlr.json?rsp-subtree=full? returns a malformed JSON file. | 4.2(1i) and later |
| CSCvr85945 | There should be a description field in the subnet IP address tables. | 4.2(1i) and later |
| CSCvr92169 | The scope for host routes should be configurable; however, the option to define the scope is not available. | 4.2(1i) and later |
| CSCvr94305 | When a user logs into the Cisco APIC GUI and selects the SAL login domain, the authorization fails and the user gets thrown back to the initial login screen. The Cisco APIC NGINX logs show a failure to parse the AVPair value that is sent back by the SAML IDP. When checking the AVPair value returned by the Okta SAML IDP " <inRole value=" shell:domains=all//read-all" /> ", the value seems to have correct syntax. | 4.2(1i) and later |
| CSCvr94614 | There is a minor memory leak in svc_ifc_policydist when performing various tenant configuration removals and additions. | 4.2(1i) and later |
| CSCvr96785 | Configuring a static endpoint through the Cisco APIC CLI fails with the following error: Error: Unable to process the query, result dataset is too big Command execution failed. | 4.2(1i) and later |
| CSCvr98638 | When migrating an AVS VMM domain to Cisco ACI Virtual Edge, the Cisco ACI Virtual Edge that gets deployed is configured in VLAN mode rather than VXLAN Mode. Because of this, you will see faults for the EPGs with the following error message: " No valid encapsulation identifier allocated for the epg" | 4.2(1i) and later |
| CSCvs03055 | While configuring a logical node profile in any L3Out, the static routes do not have a description. | 4.2(1i) and later |

Bugs

| Bug ID | Description | Exists in |
|----------------------------|---|-------------------|
| CSCvs03648 | Cisco ACI UCSM integration does not work as expected. The Cisco APIC cannot discover a loose node UCS Fabric interconnect 6400 series when it is connected to the Cisco ACI fabric with a 100G interface. | 4.2(1i) and later |
| CSCvs04899 | When you run the 'show vpc map' command in the APIC CLI, it only prints the column headers, but none of the vPC information. If you go to the leaf switch CLI and run the 'show vpc extended' command, it will show the vPCs there. | 4.2(1i) and later |
| CSCvs04981 | F2928 " KeyRing Certificate expired" faults raised and do not get cleared. | 4.2(1i) and later |
| CSCvs05817 | While using the UCSM plugin/VMM domain, during a vPC link failover test, VLANs from the vNIC template are removed. However, global (uplink) VLANs and the VLAN group remain untouched. In addition, the VMM domain is removed. | 4.2(1i) and later |
| CSCvs10076 | An error is raised while building an ACI container image because of a conflict with the /opt/ciscoaci-tripleo-heat-templates/tools/build_openstack_aci_containers.py package. | 4.2(1i) and later |
| CSCvs12118 | After removing and re-applying the IP SLA monitoring policy on a PBR policy, tracking does not work correctly. | 4.2(1i) and later |
| CSCvs13857 | L3Out encapsulated routed interfaces and routed interfaces do not have any monitoring policy attached to them. As a result, there is no option to change the threshold values of the faults that occur due to these interfaces. | 4.2(1i) and later |
| CSCvs13980 | Upgrading to the 4.2(1i) release, Layer 3 packet drops are no longer seen, but Layer 3 drop flows are still seen. However, Layer 3 drop flows do not give as much information. | 4.2(1i) and later |
| CSCvs16317 | An app does not get fully removed from all Cisco APICs. | 4.2(1i) and later |
| CSCvs16565 | An endpoint is unreachable from the leaf node because the static pervasive route (toward the remote bridge domain subnet) is missing. | 4.2(1i) and later |
| CSCvs21834 | Randomly, the Cisco APIC GUI alert list shows an incorrect license expiry time. Sometimes it is correct, while at others times it is incorrect. | 4.2(1i) and later |
| CSCvs29281 | An SNMP v3 trap is sent 2 minutes after a PSU is removed from the Cisco APIC, and a core file for the eventmgr is generated. | 4.2(1i) and later |
| CSCvs29366 | For a DVS with a controller, if another controller is created in that DVS using the same host name, the following fault gets generated: " hostname or IP address conflicts same controller creating controller with same name DVS". | 4.2(1i) and later |
| CSCvs29556 | When logging into the Cisco APIC using " apic#fallback\user", the " Error: list index out of range" log message displays and the lastlogin command fails. There is no operational impact. | 4.2(1i) and later |
| CSCvs31335 | App techsupport collection does not work sometimes when triggered from the Cisco APIC GUI. | 4.2(1i) and later |

Bugs

| Bug ID | Description | Exists in |
|----------------------------|---|-------------------|
| CSCvs32589 | In Cisco ACI Virtual Edge, there are faults related to VMNICs. On the Cisco ACI Virtual Edge domain, there are faults related to the HpNic, such as " Fault F2843 reported for AVE Uplink portgroup marked as invalid" . | 4.2(1i) and later |
| CSCvs39652 | Host subnets (/32) that are created under an SCVMM-integrated EPG get pushed as a virtual machine subnet under the virtual machine network in SCVMM. Virtual machine networks on SCVMM do not support /32 virtual machine subnets and fail to come up. Virtual machines that were previously associated to the virtual machine networks lose connectivity. | 4.2(1i) and later |
| CSCvs47757 | The plgnhandler process crashes on the Cisco APIC, which causes the cluster to enter a data layer partially diverged state. | 4.2(1i) and later |
| CSCvs48552 | When physical domains and external routed domains are attached to a security domain, these domains are mapped as associated tenants instead of associated objects under Admin > AAA > security management > Security domains. | 4.2(1i) and later |
| CSCvs49411 | Special characters are not allowed in the GUI for the SNMP community string, but you can still post a configuration that has special characters in the string by using the REST API. | 4.2(1i) 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(1i) and later |
| CSCvs55753 | A Cisco ACI leaf switch does not have MP-BGP route reflector peers in the output of " show bgp session vrf overlay-1" . As a result, the switch is not able to install dynamic routes that are normally advertised by MP-BGP route reflectors. However, the spine switch route reflectors are configured in the affected leaf switch's pod, and pod policies have been correctly defined to deploy the route reflectors to the leaf switch. Additionally, the bgpPeer managed objects are missing from the leaf switch's local MIT. | 4.2(1i) and later |
| CSCvs57061 | In a GOLF configuration, when an L3Out is deleted, the bridge domains stop getting advertised to the GOLF router even though another L3Out is still active. | 4.2(1i) and later |
| CSCvs62693 | The Name column of the the output of the " show zoning-rule" CLI command that is executed on a leaf switch running a 14.x release does not populate all of the expected contracts names. This issue makes it difficult to identify which rule ID is associated to which contract from the " show zoning-rule" command that is executed on a given leaf switch. | 4.2(1i) and later |
| CSCvs66244 | The CLI command " show interface x/x switchport" shows VLANs configured and allowed through a port. However, when going to the GUI under Fabric > Inventory > node_name > Interfaces > Physical Interfaces > Interface x/x > VLANs, the VLANs do not show. | 4.2(1i) and later |
| CSCvs74120 | Selecting the RADIUS login domain from the GUI results in the following error: Error: 400 - unknown property value test, name realm, class aaaConsoleAuth [(Dn0)] Dn0=uni/userext/authrealm/consoleauth, | 4.2(1i) and later |
| CSCvs76244 | The tmpfs file system that is mounted on /data/log becomes 100% utilized. | 4.2(1i) and later |
| CSCvs78996 | The policy manager (PM) may crash when use testapi to delete MO from policymgr db. | 4.2(1i) and later |

Bugs

| Bug ID | Description | Exists in |
|----------------------------|--|-------------------|
| CSCvs81881 | The Cisco APIC PSU voltage and amperage values are zero. | 4.2(1i) and later |
| CSCvs81907 | SNMP does not respond to GETs or sending traps on one or more Cisco APICs despite previously working properly. | 4.2(1i) and later |
| CSCvs94915 | If a FEX hardware model is N2K-C2348UPQ-10GE, this FEX does not consume a FEX_48_10G license. | 4.2(1i) and later |
| CSCvt00796 | The policymgr DME process can crash because of an OOM issue, and there are many pcons.DelRef managed objects in the DB. | 4.2(1i) and later |
| CSCvt07565 | The eventmgr database size may grow to be very large (up to 7GB). With that size, the Cisco APIC upgrade will take 1 hour for the Cisco APIC node that contains the eventmgr database. In rare cases, this could lead to a failed upgrade process, as it times out while working on the large database file of the specified controller. | 4.2(1i) and later |
| CSCvt13978 | VPC protection created in prior to the 2.2(2e) release may not to recover the original virtual IP address after fabric ID recovery. Instead, some of vPC groups get a new vIP allocated, which does not get pushed to the leaf switch. The impact to the dataplane does not come until the leaf switch had a clean reboot/upgrade, because the rebooted leaf switch gets a new virtual IP that is not matched with a vPC peer. As a result, both sides bring down the virtual port channels, then the hosts behind the vPC become unreachable. | 4.2(1i) and later |
| CSCvt19061 | Updating the interface policy group breaks LACP if eLACP is enabled on a VMM domain. If eLACP was enabled on the domain, Creating, updating, or removing an interface policy group with the VMM AEP deletes the basic LACP that is used by the domain. | 4.2(1i) and later |
| CSCvt28235 | Fault F1527 is raised when the /data/log directory is over 75% full. The /data/log directory contains a large amount of gzipped 21M svc_ifc_licensemgr.bin.warnplus.log files. The /data/log directory does not reach 80% or 90% full. | 4.2(1i) and later |
| CSCvt37066 | When migrating an EPG from one VRF table to a new VRF table, and the EPG keeps the contract relation with other EPGs in the original VRF table. Some bridge domain subnets in the original VRF table get leaked to the new VRF table due to the contract relation, even though the contract does not have the global scope and the bridge domain subnet is not configured as shared between VRF tables. The leaked static route is not deleted even if the contract relation is removed. | 4.2(1i) and later |
| CSCvt40736 | The login history of local users is not updated in Admin > AAA > Users > (double click on local user) Operational > Session. | 4.2(1i) and later |

Bugs

| Bug ID | Description | Exists in |
|----------------------------|--|-------------------|
| CSCvt44854 | <p>- Leaf or spine switch is stuck in 'downloading-boot-script' status. The node never fully registers and does not become active in the fabric.</p> <p>- You can check the status by running 'cat /mit/sys/summary grep state' on the CLI of the spine or leaf:</p> <p>If the state is set to 'downloading-boot-script' for a long period of time (> 5 minutes), you may be running into this issue.</p> <p>- Checking policy element logs on the spine or leaf switch will confirm if the bootscript file cannot be found on the Cisco APIC:</p> <ol style="list-style-type: none"> 1. Change directory to /var/log/dme/log. 2. Grep all svc_ifc_policyelem.log files for "downloadUrl - failed, error=HTTP response code said error" . <p>If you see this error message, check to make sure all Cisco APICs have the node bootscript files located in /firmware/fwrepos/fwrepo/boot.</p> | 4.2(1i) and later |
| CSCvt48819 | When using the Internet Explore browser, there is console error. This error will break some pages under Fabric -> Inventory -> [ANY POD] -> [ANY LEAF] / [ANY SPINE] -> Interfaces -> Physical, PC, VPC, FC, FC PC. | 4.2(1i) and later |
| CSCvt55566 | In the Cisco APIC GUI, after removing the Fabric Policy Group from " System > Controllers > Controller Policies > show usage" , the option to select the policy disappears, and there is no way in the GUI to re-add the policy. | 4.2(1i) and later |
| CSCvt67279 | After VMware vCenter generates a huge amount of events and after the eventId increments beyond 0xFFFFFFFF, the Cisco APIC VMM manager service may start ignoring the newest event if the eventId is lower than the last biggest event ID that Cisco APIC received. As a result, the changes to virtual distributed switch or AVE would not reflect to the Cisco APIC, causing required policies to not get pushed to the Cisco ACI leaf switch. For AVE, missing those events could put the port in the WAIT_ATTACH_ACK status. | 4.2(1i) and later |
| CSCvt68786 | A Cisco ACI Virtual Edge EPG is not programmed on a port channel toward the blade switch after it is deleted and recreated. | 4.2(1i) and later |
| CSCvt87506 | SSD lifetime can be exhausted prematurely if unused Standby slot exists | 4.2(1i) and later |
| CSCvt91540 | <p>- After decommissioning a fabric node, it is not displayed in the maintenance group configuration anymore.</p> <p>- Due to the lingering configuration pointing to the decommissioned node, F1300 gets raised with the description:</p> <p>" A Fabric Node Group (fabricNodeGrp) configuration was not deployed on the fabric node <#> because: Node Not Registered for Node Group Policies"</p> <p>- The dn mentioned in the fault will point to a maintenance group (maintgrp).</p> | 4.2(1i) and later |

Bugs

| Bug ID | Description | Exists in |
|----------------------------|---|-------------------|
| CSCvt93482 | <p>The per feature container for techsupport " objectstore_debug_info" fails to collect on spines due to invalid filepath.</p> <p>Given filepath: more /debug/leaf/nginx/objstore*/mo cat</p> <p>Correct filepath: more /debug/spine/nginx/objstore*/mo cat</p> <p>TAC uses this file/data to collect information about excessive DME writes.</p> | 4.2(1i) and later |
| CSCvu01259 | AAEP gets deleted while changing some other policy in the policy group. This only happens when using Firefox and changing a value in the leaf access port policy group. The issue is not seen when using other browsers. | 4.2(1i) and later |
| CSCvu01452 | The MD5 checksum for the downloaded Cisco APIC images is not verified before adding it to the image repository. | 4.2(1i) and later |
| CSCvu08233 | Inside the /firmware/fwrepos/fwrepo/boot directory, there is a Node-0 bootscript that seemingly points to a random leaf SN, depending on the Cisco APIC from which you're viewing the directory. | 4.2(1i) and later |
| CSCvu12092 | AVE is not getting the VTEP IP address from the Cisco APIC. The logs show a " pending pool" and " no free leases" . | 4.2(1i) and later |
| CSCvu21530 | Protocol information is not shown in the GUI when a VRF table from the common tenant is being used in any user tenant. | 4.2(1i) and later |
| CSCvu39569 | <p>The following error is encountered when accessing the Infrastructure page in the ACI vCenter plugin after inputting vCenter credentials.</p> <p>" The Automation SDK is not authenticated"</p> <p>VMware vCenter plug-in is installed using powerCLI. The following log entry is also seen in vsphere_client_virgo.log on the VMware vCenter:</p> <p>/var/log/vmware/vsphere-client/log/vsphere_client_virgo.log</p> <p>[ERROR] http-bio-9090-exec-3314 com.cisco.aciPluginServices.core.Operation</p> <p>sun.security.validator.ValidatorException: PKIX path validation failed:</p> <p>java.security.cert.CertPathValidatorException: signature check failed</p> | 4.2(1i) and later |
| CSCvu49644 | A tunnel endpoint doesn't receive a DHCP lease. This occurs with a newly deployed or upgraded Cisco ACI Virtual Edge. | 4.2(1i) and later |
| CSCvu50088 | When trying to assign a description to a FEX downlink/host port using the Config tab in the Cisco APIC GUI, the description will get applied to the GUI, but it will not propagate to the actual interface when queried using the CLI or GUI. | 4.2(1i) and later |
| CSCvu51617 | When changing the SNMP policy from policy1 to policy2 and if policy2 has the same SNMP v3 user configured with a different authentication key, the pod policy reports fault F2194 for all switches. The Cisco APICs in the cluster will accept the new policy; however, the switches in the fabric will not and will continue using the older policy1. | 4.2(1i) and later |

Bugs

| Bug ID | Description | Exists in |
|----------------------------|---|-------------------|
| CSCvu62465 | For an EPG containing a static leaf node configuration, the Cisco APIC GUI returns the following error when clicking the health of Fabric Location: Invalid DN topology/pod-X/node-Y/local/svc-policyelem-id-0/ObservedEthIf, wrong rn prefix ObservedEthIf at position 63 | 4.2(1i) and later |
| CSCvu67388 | When creating a VMware VMM domain and specifying a custom delimiter using the character _ (underscore), it is rejected, even though the help page says it is an acceptable character. | 4.2(1i) and later |
| CSCvu74478 | A prefix with an aggregate entry gets removed from Cisco APIC when downgrading the Cisco APIC from 4.2(5) to an earlier release. Due to this, the route map does not get created on the switches, and so routes are not advertised externally. | 4.2(1i) and later |
| CSCvu74566 | There is a BootMgr memory leak on a standby Cisco APIC. If the BootMgr process crashes due to being out of memory, it continues to crash, but system will not be rebooted. After the standby Cisco APIC is rebooted by hand, such as by power cycling the host using CIMC, the login prompt of the Cisco APIC will be changed to localhost and you will not be able to log into the standby Cisco APIC. | 4.2(1i) and later |
| CSCwv18827 | 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(1i) and later |
| CSCwv21442 | 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(1i) and later |
| CSCwv25475 | After a delete/add of a Cisco ACI-managed DVS, dynamic paths are not programmed on the leaf switch and the compRsDIPol managed object has a missing target. The tDn property references the old DVS OID instead of the latest value. # moquery -c compRsDIPol | 4.2(1i) and later |
| CSCwv28749 | 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(1i) and later |
| CSCwv30303 | The configuration of a bridge domain subnet scope as "public" and an EPG scope as "private" should not be allowed. | 4.2(1i) and later |
| CSCwv41784 | EIGRP summary routes are not advertised from one of the many interfaces under same interface profile. | 4.2(1i) and later |

Bugs

| Bug ID | Description | Exists in |
|-----------------------------|---|-------------------|
| CSCvv62861 | A leaf switch reloads due to an out-of-memory condition after changing the contract scope to global. | 4.2(1i) and later |
| 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(1i) and later |
| CSCvw33061 | Traffic loss is observed from multiple endpoints deployed on two different vPC leaf switches. | 4.2(1i) 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 ptag for the shadow EPG gets reprogrammed with a global value. The zoning-rule entries that matched the previous ptag 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 ptag. | 4.2(1i) 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(1i) and later |
| CSCwvc66053 | Preconfiguration validations for L3Outs that occur whenever a new configuration is pushed to the Cisco APIC might not get triggered. | 4.2(1i) and later |

Resolved Bugs

This section lists the resolved bugs. Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Fixed In" column of the table specifies whether the bug was resolved in the base release or a patch release.

Table 4 Resolved Bugs in This Release

| Bug ID | Description | Fixed in |
|----------------------------|---|----------|
| CSCuu17314 | CDP is not enabled on the management interfaces for the leaf switches and spine switches. | 4.2(1i) |
| CSCve84297 | A service cannot be reached by using the APIC out-of-band management that exists within the 172.17.0.0/16 subnet. | 4.2(1i) |

Bugs

| Bug ID | Description | Fixed in |
|----------------------------|---|----------|
| CSCvg70246 | When configuring an L3Out under a user tenant that is associated with a VRF instance that is under the common tenant, a customized BGP timer policy that is attached to the VRF instance is not applied to the L3Out (BGP peer) in the user tenant. | 4.2(1i) |
| CSCvi41092 | The APIC log files are extremely large, which takes a considerable amount of time to upload, especially for users with slow internet connectivity. | 4.2(1i) |
| CSCvi80543 | This is an enhancement that allows failover ordering, categorizing uplinks as active or standby, and categorizing unused uplinks for each EPG in VMware domains from the APIC. | 4.2(1i) |
| CSCvm63668 | A single user can send queries to overload the API gateway. | 4.2(1i) |
| CSCvm89559 | The svc_ifc_policye process consumes 100% of the CPU cycles. The following messages are observed in svc_ifc_policymgr.bin.log: 8816 18-10-12 11:04:19.101 route_control ERROR co=doer:255:127:0xff0000000c42ad2:11 Route entry order exceeded max for st10960-2424833-any-2293761-33141-shared-svc-int Order:18846Max:17801 ../dme/svc/policyelem/src/gen/ifc/beh/imp/./rtctrl/RouteMapUtils.cc 239:q | 4.2(1i) |
| CSCvn00576 | An SHA2 CSR for the ACI HTTPS certificate cannot be configured in the APIC GUI. | 4.2(1i) |
| CSCvn99797 | When 3 DNS providers are added, F3546 faults are raised for: Policy Configuration for DNS Profile: default failed due to : provider-limit-exceeded. To debug/rectify: DNS Provider count cannot exceed 2. The first 2 DNS providers you provide will be used for name resolution. The rest of the nameservers will be not be used for name resolution. | 4.2(1i) |
| CSCvo42420 | After changing the VRF instance association of a shared-services bridge domain, a shared-services route is still present in the old VRF instance. | 4.2(1i) |
| CSCvp25660 | After upgrading APICs from a pre-4.0 version to 4.0 or newer, the leaf switches will not upgrade, or the switches will upgrade and then automatically downgrade back to the previous version. | 4.2(1i) |
| CSCvp38968 | A service graph with a Layer 1 device goes to the "failed" state when an inter-tenant contract is used. The error in the graph will be "id-allocation-failure". | 4.2(1i) |
| CSCvp43877 | When using the "Clone" option for a policy group or interface profile and an existing name is used, the cloned policy overwrites the old policy. A warning should be displayed regarding the policy name that already exists. | 4.2(1i) |

Bugs

| Bug ID | Description | Fixed in |
|----------------------------|--|----------|
| CSCvp44764 | <p>With the PBR feature, the svcdirDestmon object in the leaf switch is incorrectly removed. As a result, a service device cannot be tracked and the switch incorrectly reports the status to APIC that the service device is down.</p> <p>When this happens, the switch attempts to take corrective action based on the user configuration (the threshold action configuration). The switch attempts to skip the service node if thresholdDownAction is set to "bypass," send the traffic directly to the destination if thresholdDownAction is set to "permit," or drop the traffic if thresholdDownAction is set to "deny".</p> | 4.2(1i) |
| CSCvp51422 | Bridge domain stretch should not be supported in MSC configuration when cross site boundary with Remote Leaf is involved. | 4.2(1i) |
| CSCvp57131 | After a VC was disconnected and reconnected to the APIC, operational faults (for example, discovery mismatching between APIC and VC) were cleared, even the if faulty condition still existed. | 4.2(1i) |
| CSCvp68296 | The APIC process information from the APIC GUI may have the wrong values. | 4.2(1i) |
| CSCvp72283 | <p>An APIC running the 3.0(1k) release sometimes enters the "Data Layer Partially Diverged" state. The aci diag rvc read command shows the following output for the service 10 (observer):</p> <p>Non optimal leader for shards :10:1,10:3,10:4,10:6,10:7,10:9,10:10,10:12,10:13,10:15,10:16,10:18,10:19,10:21,10:22,10:24,10:25, 10:27,10:28,10:30,10:31</p> | 4.2(1i) |
| CSCvp73395 | When connecting the ExternalSwitch app to a UCSM environment, ACI VLANs are not deployed to the fabric-connected vNICs that were configured as part of a redundancy peer. The VLANs are allocated from the ACI VLAN pools, but are never added to the UCSM LAN group nor VLANs, and are not added to the vNICs when the vNICs are configured with Redundant Peer configurations in UCSM. | 4.2(1i) |
| CSCvp79155 | Inventory pull operations or VMware vCenter updates are delayed. | 4.2(1i) |
| CSCvp79454 | Syslog is not sent upon any changes in the fabric. Events are properly generated, but no Syslog is sent out of the oobmgmt ports of any of the APICs. | 4.2(1i) |
| CSCvp80983 | The ipv4RouteMo/ipv6RouteMo is not present in case of a shared service route leak. The route could have been deleted when EPG to BD association is removed and not added back when this association is created again. | 4.2(1i) |
| CSCvp80983 | The ipv4RouteMo/ipv6RouteMo is not present in case of a shared service route leak. The route could have been deleted when EPG to BD association is removed and not added back when this association is created again. | 4.2(1i) |
| CSCvp86156 | If a user manually modifies an object controlled by the ACI CNI, the configuration will not be restored for up to 14 minutes. | 4.2(1i) |

Bugs

| Bug ID | Description | Fixed in |
|----------------------------|---|----------|
| CSCvp94060 | No fault is raised when First Hop Security is enabled in a Layer 2 only Bridge Domain. | 4.2(1i) |
| CSCvp94085 | The APIC Licensemgr generates a core file while parsing an XML response. | 4.2(1i) |
| CSCvp95407 | Access-control headers are not present in invalid requests. | 4.2(1i) |
| CSCvp97092 | Tenants that start with the word "infra" are treated as the default "infra" tenant. | 4.2(1i) |
| CSCvp99430 | The troubleshooting wizard is unresponsive on the APIC. | 4.2(1i) |
| CSCvp99508 | The GUI is slow when accessing access policies. This is an enhancement request to add pagination to resolve this issue. | 4.2(1i) |
| CSCvq02715 | There are issues with out-of-band SSH connectivity to the leaf and spine switches if the out-of-band VRF instance is deleted and re-created with the same name. | 4.2(1i) |
| CSCvq03722 | When performing a clean reboot using the "acidiag touch setup" or the "acidiag touch clean", during the boot up of the APIC, you will observe a significant delay between the enter key to continue and the interactive setup parameter menu. There is no other operational impact other than slower boot up due to the system delay. | 4.2(1i) |
| CSCvq04110 | The APIC API and CLI allow for the configuration of multiple native VLANs on the same interface. When a leaf switch port has more than one native VLAN configured (which is a misconfiguration) in place, and a user tries to configure a native VLAN encap on another port on the same leaf switch, a validation error is thrown that indicates an issue with the misconfigured port. This error will occur even if the current target port has no misconfigurations in place. | 4.2(1i) |
| CSCvq05143 | <p>Using a PBR service graph with ASA in two-arm mode. After upgrade from release 2.3(1) > 3.1 > 3.2(6i), it is noticed that the service graph (in the common tenant) has a couple of faults. The service graph is working for old configured EPGs (verified by checking traffic redirected to FW), but new EPGs cannot be applied to the service graph. The service graph state is also "not applied".</p> <p>One of the faults mentions that the service graph contract cannot be used as provider and consumer and that it is only supported in single-node PBR with 1-ARM.</p> <p>The contract is not being applied in any vzAny consumer/provider.</p> <p>The "Epp not found. Retry or abort task" error appears in the policymanager.</p> <p>Adding an arp filter on the contract does not it triggers anything, although the modification is seen in the policy distributor.</p> | 4.2(1i) |
| CSCvq14177 | The Hyper-V agent is in the STOPPED state. Hyper-V agent logs indicate that process is stopping at the "Set-ExecutionPolicy Unrestricted" command. | 4.2(1i) |
| CSCvq16739 | For virtual pod and physical pod wizards, when a user tries to configure TEP addresses, there is an error on a preconfigured data plane TEP IP address. This error does not let the user proceed with rest of the configuration. | 4.2(1i) |

Bugs

| Bug ID | Description | Fixed in |
|----------------------------|---|----------|
| CSCvq19984 | aci-container-controllers will delete all the contract relationships under the default_ext_epg if it loses connectivity to the APIC during the API call to get the subtree for the contract relationships. | 4.2(1i) |
| CSCvq20055 | In the APIC, the " show external-I3 static-route tenant <tenant_name>" command does not output as expected. Symptom 1: The APIC outputs static-routes for tenant A, but not B. The " show external-I3 static-route tenant <tenant_name> vrf <vrf_name> node <range>" command provides the missing output. Symptom 2: For the same tenant and a different L3Out , the command does not output all static-routes. | 4.2(1i) |
| CSCvq24993 | The MTU cannot be modified on the SPAN destination after it is configured. | 4.2(1i) |
| CSCvq28342 | In a fabric with only fixed spine switches, the modular security license is still used when enabling MACsec. The fixed spine switch should share the same Add-on Security license entitlement with the leaf switch, because the features charge the same price. | 4.2(1i) |
| CSCvq31358 | "show external-I3 interfaces node <id> detail" will display "missing" for both "Oper Interface" and "Oper IP", even though the L3Out is functioning as expected. | 4.2(1i) |
| CSCvq38191 | An eventmgr core file gets generated when a user performs the syslog debug command "logit" . | 4.2(1i) |
| CSCvq39477 | A user with read-only permissions cannot collect the techsupport files using the CLI nor a policy. | 4.2(1i) |
| CSCvq39922 | Specific operating system and browser version combinations cannot be used to log in to the APIC GUI. Some browsers that are known to have this issue include (but might not be limited to) Google Chrome version 75.0.3770.90 and Apple Safari version 12.0.3 (13606.4.5.3.1). | 4.2(1i) |
| CSCvq43101 | When opening an external subnet, a user cannot see Aggregate Export/Import check boxes set in GUI even though they were already configured. | 4.2(1i) |
| CSCvq45710 | Fault F3206 for " Configuration failed for policy uni/infra/nodeauthpol-default, due to failedEPg or failedVlan is empty" is raised in the fabric when using the default 802.1x Node Authentication policy in the Switch Policy Group. In this scenario, Fail-auth EPG and VLAN has not been configured, as the 802.1x feature is not in use. | 4.2(1i) |
| CSCvq55982 | APIC running 4.1(2g) throws fault for pingcheck failed. | 4.2(1i) |
| CSCvq56057 | ACI running 4.1.1j. | 4.2(1i) |
| CSCvq56243 | When toggling the " legacy mode" option on a bridge domain, there should be a warning message that displays. | 4.2(1i) |

Bugs

| Bug ID | Description | Fixed in |
|----------------------------|---|----------|
| CSCvq58304 | VMM inventory-related faults are raised for VMware vCenter inventory, which is not managed by the VMM. | 4.2(1i) |
| CSCvq58839 | Configuration import fails due to a Global AES encryption key mismatch for pimIfPol. | 4.2(1i) |
| CSCvq61877 | The SNMP process repeatedly crashes on the APICs. The cluster and shards look healthy and do not have any CPU or memory utilization issues. | 4.2(1i) |
| CSCvq63491 | When using Open vSwitch, which is used as part of ACI integration with Kubernetes or Red Hat Open Shift, there are some instances when memory consumption of the Open vSwitch grows over a time. | 4.2(1i) |
| CSCvq77297 | Plugin-handler triggers pre-remove the lifecycle hook for a scale-out app that is being removed. It keeps checking the status of pre-remove lifecycle hook using a Kron API, but if Kron is down, the plugin-handler waits for Kron to come back in the same transaction. This can cause the APIC cluster to diverge. | 4.2(1i) |
| CSCvq85224 | The GUI navigates to the incorrect tree item from Virtual Networking -> domains - container domains. | 4.2(1i) |
| CSCvq87663 | When creating a subject and leaving "Wan SLA Policy" as unspecified (field not required), Fault F3330 is raised. Fault code: F3330 Description: Failed to form relation to MO uni/tn-common/sdwanpolcont/sdwanslapol- of class extdevSDWanSlaPol Type: Config | 4.2(1i) |
| CSCvr25643 | In an ACI fabric, the vPC IP address is managed by the dhcpd process. Sometimes when deleting vPC/vPC domains, the clean up does not complete. The fabricExplicitGEp managed object gets deleted, but the corresponding fabricVpcResource managed object does not get deleted. As a result, upon creating a new vPC pair, the dhcpd process might assign the same IP address that the deleted vPC had. The dhcpd process will crash while assigning a different IP address for second time because of this bug. | 4.2(1j) |
| CSCvr26608 | There is a memory leak in core_thread::ThreadContext. | 4.2(1i) |

Known Behaviors

This section lists bugs that describe known behaviors. Click the Bug ID to access the Bug Search Tool and see additional information about the bug. The "Exists In" column of the table specifies the 4.2(1) releases in which the known behavior exists. A bug might also exist in releases other than the 4.2(1) releases.

Table 5 Known Behaviors in This Release

| Bug ID | Description | Exists in |
|--------|-------------|-----------|
|--------|-------------|-----------|

Bugs

| Bug ID | Description | Exists in |
|----------------------------|---|-------------------|
| CSCvj26666 | The "show run leaf spine <nodeId>" command might produce an error for scaled up configurations. | 4.2(1i) 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(1i) 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(1i) and later |
| CSCvq58953 | One of the following symptoms occurs: <ul style="list-style-type: none"> ■ App installation/enable/disable takes a long time and does not complete. ■ Nomad leadership is lost. The output of the aci diag scheduler logs members command contains the following error: Error querying node status: Unexpected response code: 500 (rpc error: No cluster leader) | 4.2(1i) 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(1i) and later |

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

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

- If you use the REST API to upgrade an app, you must create a new firmware.OSource to be able to download a new app image.
- In a multipod configuration, before you make any changes to a spine switch, ensure that there is at least one operationally "up" external link that is participating in the multipod topology. Failure to do so could bring down the multipod connectivity. For more information about multipod, see the Cisco Application Centric Infrastructure Fundamentals document and the Cisco APIC Getting Started Guide.
- With a non-english SCVMM 2012 R2 or SCVMM 2016 setup and where the virtual machine names are specified in non-english characters, if the host is removed and re-added to the host group, the GUID for all the virtual machines under that host changes. Therefore, if a user has created a micro segmentation endpoint group using "VM name" attribute specifying the GUID of respective virtual machine, then that micro segmentation endpoint group will not work if the host (hosting the virtual machines) is removed and re-added to the host group, as the GUID for all the virtual machines would have changed. This does not happen if the virtual name has name specified in all english characters.

Compatibility Information

- A query of a configurable policy that does not have a subscription goes to the policy distributor. However, a query of a configurable policy that has a subscription goes to the policy manager. As a result, if the policy propagation from the policy distributor to the policy manager takes a prolonged amount of time, then in such cases the query with the subscription might not return the policy simply because it has not reached policy manager yet.
- When there are silent hosts across sites, ARP glean messages might not be forwarded to remote sites if a leaf switch without -EX or a later designation in the product ID happens to be in the transit path and the VRF is deployed on that leaf switch, the switch does not forward the ARP glean packet back into the fabric to reach the remote site. This issue is specific to transit leaf switches without -EX or a later designation in the product ID and does not affect leaf switches that have -EX or a later designation in the product ID. This issue breaks the capability of discovering silent hosts.

Compatibility Information

The following sections list compatibility information for the Cisco APIC software.

Virtualization Compatibility Information

This section lists virtualization compatibility information for the Cisco APIC software.

- For a table that shows the supported virtualization products, see the [ACI Virtualization Compatibility Matrix](#).
- This release supports VMM Integration and VMware Distributed Virtual Switch (DVS) 6.5 and 6.7. For more information about guidelines for upgrading VMware DVS from 5.x to 6.x and VMM integration, see the [Cisco ACI Virtualization Guide, Release 4.2\(x\)](#).
- For information about Cisco APIC compatibility with Cisco UCS Director, see the appropriate *Cisco UCS Director Compatibility Matrix* document at the following URL:

<https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-director/products-device-support-tables-list.html>

Hardware Compatibility Information

This release supports the following Cisco APIC servers:

| Product ID | Description |
|------------|--|
| APIC-L1 | Cisco APIC with large CPU, hard drive, and memory configurations (more than 1000 edge ports) |
| APIC-L2 | Cisco APIC with large CPU, hard drive, and memory configurations (more than 1000 edge ports) |
| APIC-L3 | Cisco APIC with large CPU, hard drive, and memory configurations (more than 1200 edge ports) |
| APIC-M1 | Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1000 edge ports) |
| APIC-M2 | Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1000 edge ports) |
| APIC-M3 | Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1200 edge ports) |

The following list includes additional hardware compatibility information:

- For the supported hardware, see the [Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 14.2\(1\)](#).
- To connect the N2348UPQ to Cisco ACI leaf switches, the following options are available:
 - Directly connect the 40G FEX ports on the N2348UPQ to the 40G switch ports on the Cisco ACI leaf switches
 - Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the 10G ports on all other Cisco ACI leaf switches.

Note: A fabric uplink port cannot be used as a FEX fabric port.

- The Cisco UCS M5-based Cisco APIC supports dual speed 10G and 25G interfaces. The Cisco UCS M4-based Cisco APIC and previous versions support only the 10G interface. Connecting the Cisco APIC to the Cisco ACI fabric requires a same speed interface on the Cisco ACI leaf switch. You cannot connect the Cisco APIC directly to the Cisco N9332PQ ACI leaf switch, unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the Cisco N9332PQ switch auto-negotiate to 10G without requiring any manual configuration.
- The Cisco N9K-X9736C-FX (ports 29 to 36) and Cisco N9K-C9364C-FX (ports 49-64) switches do not support 1G SFPs with QSA.
- Cisco N9K-C9508-FM-E2 fabric modules must be physically removed before downgrading to releases earlier than Cisco APIC 3.0(1).
- The Cisco N9K-C9508-FM-E2 and N9K-X9736C-FX locator LED enable/disable feature is supported in the GUI and not supported in the Cisco ACI NX-OS Switch CLI.
- Contracts using matchDscp filters are only supported on switches with "EX" on the end of the switch name. For example, N9K-93108TC-EX.
- N9K-C9508-FM-E2 and N9K-C9508-FM-E fabric modules in the mixed mode configuration are not supported on the same spine switch.
- The N9K-C9348GC-FXP switch does not read SPROM information if the PSU is in a shut state. You might see an empty string in the Cisco APIC output.
- When the fabric node switch (spine or leaf) is out-of-fabric, the environmental sensor values, such as Current Temperature, Power Draw, and Power Consumption, might be reported as "N/A." A status might be reported as "Normal" even when the Current Temperature is "N/A."
- First generation switches (switches without -EX, -FX, -GX, or a later suffix in the product ID) do not support Contract filters with match type "IPv4" or "IPv6." Only match type "IP" is supported. Because of this, a contract will match both IPv4 and IPv6 traffic when the match type of "IP" is used.

Adaptive Security Appliance (ASA) Compatibility Information

This section lists ASA compatibility information for the Cisco APIC software.

- This release supports Adaptive Security Appliance (ASA) device package version 1.2.5.5 or later.

Compatibility Information

- If you are running a Cisco Adaptive Security Virtual Appliance (ASA) version that is prior to version 9.3(2), you must configure SSL encryption as follows:

```
(config)# ssl encryption aes128-sha1
```

Miscellaneous Compatibility Information

This section lists miscellaneous compatibility information for the Cisco APIC software.

- This release supports the following software:

- Cisco NX-OS Release 14.2(1)
- Cisco AVS, Release 5.2(1)SV3(4.10)

For more information about the supported AVS releases, see the AVS software compatibility information in the [Cisco AVS Release Notes, Release 5.2\(1\)SV3\(4.10\)](#).

- Cisco UCS Manager software release 2.2(1c) or later is required for the Cisco UCS Fabric Interconnect and other components, including the BIOS, CIMC, and the adapter.
- 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 Day-2 Operations Apps Support Matrix](#)

- The latest recommended CIMC releases are as follows:

- 4.2(3e) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3)
- 4.2(3b) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
- 4.2(2a) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
- 4.1(3m) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
- 4.1(3f) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
- 4.1(3d) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
- 4.1(3c) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
- 4.1(2m) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
- 4.1(2k) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)
- 4.1(2g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)
- 4.1(2b) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)
- 4.1(1g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3)
- 4.1(1f) CIMC HUU ISO for UCS C220 M4 (APIC-L2/M2) (deferred release)
- 4.1(1d) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3)
- 4.1(1c) CIMC HUU ISO for UCS C220 M4 (APIC-L2/M2)
- 4.0(4e) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3)

Usage Guidelines

- 4.0(2g) CIMC HUU ISO for UCS C220/C240 M4 and M5 (APIC-L2/M2 and APIC-L3/M3)
 - 4.0(1a) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3)
 - 3.0(4l) CIMC HUU ISO (recommended) for UCS C220/C240 M3 (APIC-L1/M1)
 - 3.0(4d) CIMC HUU ISO for UCS C220/C240 M3 and M4 (APIC-L1/M1 and APIC-L2/M2)
 - 3.0(3f) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)
 - 3.0(3e) CIMC HUU ISO for UCS C220/C240 M3 (APIC-L1/M1)
 - 2.0(13i) CIMC HUU ISO
 - 2.0(9c) CIMC HUU ISO
 - 2.0(3i) CIMC HUU ISO
- This release supports the partner packages specified in the [L4-L7 Compatibility List Solution Overview](#) document.
 - 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 Plugins Release 4.2\(1\), Release Notes](#).
 - For compatibility with Day-2 Operations apps, see the [Cisco Day-2 Operations Apps Support Matrix](#).

Usage Guidelines

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

Virtualization Compatibility Guidelines

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

- Do not separate virtual port channel (vPC) member nodes into different configuration zones. If the nodes are in different configuration zones, then the vPCs' **modes become mismatched if the interface policies are modified** and deployed to only one of the vPC member nodes.
- If you are upgrading VMware vCenter 6.0 to vCenter 6.7, you should first delete the following folder on the VMware vCenter: C:\ProgramData\cisco_aci_plugin.

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

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

The *user* is the user that is currently logged in to the vSphere Web Client, and *domain* is the domain to which the user belongs. Although you can still register a fabric, you do not have permissions to override settings that were created in the old VMware vCenter. Enter any changes in the Cisco APIC configuration again after restarting VMware vCenter.

Usage Guidelines

- If the communication between the Cisco APIC and VMware vCenter is impaired, some functionality is adversely affected. The Cisco APIC relies on the pulling of inventory information, updating VDS configuration, and receiving event notifications from the VMware vCenter for performing certain operations.
- After you migrate VMs using a cross-data center VMware vMotion in the same VMware vCenter, you might find a stale VM entry under the source DVS. This stale entry can cause problems, such as host removal failure. The workaround for this problem is to enable "Start monitoring port state" on the vNetwork DVS. See the KB topic "Refreshing port state information for a vNetwork Distributed Virtual Switch" on the VMware Web site for instructions.
- When creating a vPC domain between two leaf switches, both switches either must not have -EX or a later designation in the product ID or must have -EX or a later designation in the product ID.
- The following Red Hat Virtualization (RHV) guidelines apply:
 - We recommend that you use release 4.1.6 or later.
 - Only one controller (compCtrlr) can be associated with a Red Hat Virtualization Manager (RHVM) data center.
 - Deployment immediacy is supported only as pre-provision.
 - IntraEPG isolation, micro EPGs, and IntraEPG contracts are not supported.
 - Using service nodes inside a RHV domain have not been validated.

GUI Guidelines

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

- The Cisco APIC GUI includes an online version of the Quick Start Guide that includes video demonstrations.
- To reach the Cisco APIC CLI from the GUI: choose System > Controllers, highlight a controller, right-click, and choose "launch SSH". To get the list of commands, press the escape key twice.
- When using the APIC GUI to configure an integration group, you cannot specify the connection URL (connUrl). You can only specify the connection URL by using the REST API.
- The Basic GUI mode is deprecated. We do not recommend using Cisco APIC Basic mode for configuration. However, if you want to use Cisco APIC Basic mode, use the following URL:

APIC_URL/indexSimple.html

CLI Guidelines

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

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

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

Layer 2 and Layer 3 Configuration Guidelines

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

- For Layer 3 external networks created through the API or GUI and updated through the CLI, protocols need to be enabled globally on the external network through the API or GUI, and the node profile for all the participating nodes needs to be added through the API or GUI before doing any further updates through the CLI.
- When configuring two Layer 3 external networks on the same node, the loopbacks need to be configured separately for both Layer 3 networks.
- All endpoint groups (EPGs), including application EPGs and Layer 3 external EPGs, require a domain. Interface policy groups must also be associated with an Attach Entity Profile (AEP), and the AEP must be associated with domains. Based on the association of EPGs to domains and of the interface policy groups to domains, the ports VLANs that the EPG uses are validated. This applies to all EPGs including bridged Layer 2 outside and routed Layer 3 outside EPGs. For more information, see the *Cisco APIC Layer 2 Networking Configuration Guide*.

Note: When creating static paths for application EPGs or Layer 2/Layer 3 outside EPGs, the physical domain is not required. Upgrading without the physical domain raises a fault on the EPG stating "invalid path configuration."

- In a multipod fabric, if a spine switch in POD1 uses the infra tenant L3extOut-1, the TORs of the other pods (POD2, POD3) cannot use the same infra L3extOut (L3extOut-1) for Layer 3 EVPN control plane connectivity. Each POD must use its own spine switch and infra L3extOut.
- You do not need to create a customized monitoring policy for each tenant. By default, a tenant shares the common policy under tenant common. The Cisco APIC automatically creates a default monitoring policy and enables common observable. You can modify the default policy under tenant common based on the requirements of your fabric.
- The Cisco APIC does not provide IPAM services for tenant workloads.
- Do not mis-configure Control Plane Policing (CoPP) pre-filter entries. CoPP pre-filter entries might impact connectivity to multi-pod configurations, remote leaf switches, and Cisco ACI Multi-Site deployments.

IP Address Guidelines

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

- For the following services, use a DNS-based hostname with out-of-band management connectivity. IP addresses can be used with both in-band and out-of-band management connectivity.
 - Syslog server
 - Call Home SMTP server
 - Tech support export server
 - Configuration export server
 - Statistics export server

Usage Guidelines

- The infrastructure IP address range must not overlap with other IP addresses used in the fabric for in-band and Out-of-band networks.
- If an IP address is learned on one of two endpoints for which you are configuring an atomic counter policy, you should use an IP-based policy and not a client endpoint-based policy.
- A multipod deployment requires the 239.255.255.240 system Global IP Outside (GIPO) to be configured on the inter-pod network (IPN) as a PIM BIDIR range. This 239.255.255.240 PIM BIDIR range configuration on the IPN devices can be avoided by using the Infra GIPO as System GIPO feature. The Infra GIPO as System GIPO feature must be enabled only after upgrading all of the switches in the Cisco ACI fabric, including the leaf switches and spine switches, to the latest Cisco APIC release.
- Cisco ACI does not support a class E address as a VTEP address.

Miscellaneous Guidelines

This section lists miscellaneous usage guidelines for the Cisco APIC software.

- User passwords must meet the following criteria:
 - Minimum length is 8 characters
 - Maximum length is 64 characters
 - Fewer than three consecutive repeated characters
 - At least three of the following character types: lowercase, uppercase, digit, symbol
 - Cannot be easily guessed
 - Cannot be the username or the reverse of the username
 - Cannot be any variation of " cisco" , " isco" , or any permutation of these characters or variants obtained by changing the capitalization of letters therein
- In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.
- The power consumption statistics are not shown on leaf node slot 1.
- If you defined multiple login domains, you can choose the login domain that you want to use when logging in to a Cisco APIC. By default, the domain drop-down list is empty, and if you do not choose a domain, the DefaultAuth domain is used for authentication. This can result in login failure if the username is not in the DefaultAuth login domain. As such, you must enter the credentials based on the chosen login domain.
- A firmware maintenance group should contain a maximum of 80 nodes.
- When contracts are not associated with an endpoint group, DSCP marking is not supported for a VRF with a vzAny contract. DSCP is sent to a leaf switch along with the actrl rule, but a vzAny contract does not have an actrl rule. Therefore, the DSCP value cannot be sent.
- The Cisco APICs must have 1 SSD and 2 HDDs, and both RAID volumes must be healthy before upgrading to this release. The Cisco APIC will not boot if the SSD is not installed.
- In a multipod fabric setup, if a new spine switch is added to a pod, it must first be connected to at least one leaf switch in the pod. Then the spine switch is able to discover and join the fabric.

Caution: If you install 1-Gigabit Ethernet (GE) or 10GE links between the leaf and spine switches in the fabric, there is risk of packets being dropped instead of forwarded, because of inadequate bandwidth. To avoid the risk, use 40GE or 100GE links between the leaf and spine switches.

- For a Cisco APIC REST API query of event records, the Cisco APIC system limits the response to a maximum of 500,000 event records. If the response is more than 500,000 events, it returns an error. Use filters to refine your queries. For more information, see [Cisco APIC REST API Configuration Guide, Release 4.2\(x\)](#).
- Subject Alternative Names (SANs) contain one or more alternate names and uses any variety of name forms for the entity that is bound by the Certificate Authority (CA) to the certified public key. These alternate names are called "Subject Alternative Names" (SANs). Possible names include:
 - DNS name
 - IP address
- If a node has port profiles deployed on it, some port configurations are not removed if you decommission the node. You must manually delete the configurations after decommissioning the node to cause the ports to return to the default state. To do this, log into the switch, run the `setup-clean-config.sh` script, wait for the script to complete, then enter the `reload` command.
- When using the SNMP trap aggregation feature, if you decommission Cisco APICs, the trap forward server will receive redundant traps.
- If you upgraded from a release prior to the 3.2(1) release and you had any apps installed prior to the upgrade, the apps will no longer work. To use the apps again, you must uninstall and reinstall them.
- Connectivity filters were deprecated in the 3.2(4) release. Feature deprecation implies no further testing has been performed and that Cisco recommends removing any and all configurations that use this feature. The usage of connectivity filters can result in unexpected access policy resolution, which in some cases will lead to VLANs being removed/reprogrammed on leaf interfaces. You can search for the existence of any connectivity filters by using the `moquery` command on the APIC:

```
> moquery -c infraConnPortBlk
> moquery -c infraConnNodeBlk
> moquery -c infraConnNodeS
> moquery -c infraConnFexBlk
> moquery -c infraConnFexS
```
- Fabric connectivity ports can operate at 10G or 25G speeds (depending on the model of the APIC server) when connected to leaf switch host interfaces. We recommend connecting two fabric uplinks, each to a separate leaf switch or vPC leaf switch pair.

For APIC-M3/L3, virtual interface card (VIC) 1445 has four ports (port-1, port-2, port-3, and port-4 from left to right). Port-1 and port-2 make a single pair corresponding to eth2-1 on the APIC server; port-3 and port-4 make another pair corresponding to eth2-2 on the APIC server. Only a single connection is allowed for each pair. For example, you can connect one cable to either port-1 or port-2 and another cable to either port-3 or port-4, but not 2 cables to both ports on the same pair. Connecting 2 cables to both ports on the same pair creates instability in the APIC server. All ports must be configured for the same speed: either 10G or 25G.

- When you create an access port selector in a leaf interface profile, the `fexId` property is configured with a default value of 101 even though a FEX is not connected and the interface is not a FEX interface. The `fexId` property is only used when the port selector is associated with an `infraFexBndIgrp` managed object.

Related Documentation

The Cisco Application Policy Infrastructure Controller (APIC) documentation can be accessed from the following website:

<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

The documentation includes installation, upgrade, configuration, programming, and troubleshooting guides, technical references, release notes, and knowledge base (KB) articles, as well as other documentation. KB articles provide information about a specific use case or a specific topic.

By using the "Choose a topic" and "Choose a document type" fields of the APIC documentation website, you can narrow down the displayed documentation list to make it easier to find the desired document.

The following list provides links to the release notes and verified scalability documentation:

- [Verified Scalability](#)
- [Cisco ACI Simulator Release Notes](#)
- [Cisco NX-OS Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches](#)
- [Cisco Application Policy Infrastructure Controller OpenStack and Container Plugins Release Notes](#)
- [Cisco Application Virtual Switch Release Notes](#)

New Documentation

This section lists the new Cisco ACI product documents for this release.

- [Cisco ACI Support for Layer 3 IPv6 Multicast](#)
- [Cisco ACI Virtual Edge Configuration Guide, Release 2.2\(1a\)](#)
- [Cisco ACI Virtual Edge Installation Guide, Release 2.2\(x\)](#)
- [Cisco ACI Virtual Edge Release Notes, Release 2.2\(1a\)](#)
- [Cisco ACI Virtual Pod Getting Started Guide, Release 4.2\(x\)](#)
- [Cisco ACI Virtual Pod Installation Guide, Release 4.2\(x\)](#)
- [Cisco ACI Virtual Pod Release Notes, Release 4.2\(1i\)](#)
- [Cisco ACI Virtualization Guide, Release 4.2\(x\)](#)
- [Cisco ACI Support for BGP Neighbor Shutdown and Soft Reset](#)
- [Cisco APIC and Redistributing Static Routes to BGP With Prefix List](#)
- [Cisco APIC and Route Control Per BGP Peer](#)
- [Cisco APIC Getting Started Guide, Release 4.2\(x\)](#)
- [Cisco APIC Layer 2 Networking Configuration Guide, Release 4.2\(x\)](#)
- [Cisco APIC Layer 3 Networking Configuration Guide, Release 4.2\(x\)](#)

Related Documentation

- [Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.2\(x\)](#)
- [Cisco APIC NX-OS Style CLI Command Reference, 4.2\(x\)](#)
- [Cisco APIC NX-OS Style CLI Configuration Guide, Release 4.2\(x\)](#)
- [Cisco APIC Security Configuration Guide, Release 4.2\(x\)](#)
- [Cisco APIC Support for CDP and LLDP in Management Interface](#)
- [Cisco Application Centric Infrastructure Fundamentals, Releases 4.2\(x\)](#)
- [Cisco AVS Release Notes, Release 5.2\(1\)SV3\(4.10\)](#)

You can find these documents on the following website:

<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

Related Documentation

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: 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.

© 2019-2024 Cisco Systems, Inc. All rights reserved.