Cisco Application Policy Infrastructure Controller Release Notes, Release 4.1(1)

Note: Release 4.1(1i) is deferred; do not install this release. Instead, install release 4.1(1i) or later.

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

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

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

Note: Use this document with the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 14.1(1)*, which you can view at the following location:

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html

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

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

You can watch videos that demonstrate how to perform specific tasks in the Cisco APIC on the Cisco ACI YouTube channel:

https://www.youtube.com/c/CiscoACIchannel

For the verified scalability limits (except the CLI limits), see the *Verified Scalability Guide* for this release.

For the CLI verified scalability limits, see the *Cisco NX-OS Style Command-Line Interface Configuration Guide* for this release.

You can access these documents from the following website:

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

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

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
December 9, 2022	In the Open Bugs section, added bug CSCvw33061.
August 1, 2022	In the Miscellaneous Compatibility Information section, added: ■ 4.2(2a) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) ■ 4.1(2k) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
March 21, 2022	In the Miscellaneous Compatibility Information section, added: ■ 4.1(3f) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3)
February 23, 2022	In the Miscellaneous Compatibility Information section, added: ■ 4.1(2g) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
November 2, 2021	In the Miscellaneous Compatibility Information section, added: ■ 4.1(3d) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3)
August 4, 2021	In the Open Issues section, added bug CSCvy30453.
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 11, 2021	In the Miscellaneous Compatibility Information section, for CIMC HUU ISO, added: ■ 4.1(3b) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) Changed: ■ 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3) To: ■ 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2
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: ■ 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.

Date	Description
August 19, 2020	Release 4.1(1i) became deferred.
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.
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.
October 8, 2019	In the Miscellaneous Compatibility Information section, updated the supported 4.0(4), 4.0(2), and 3.0(4) CIMC releases to: — 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	In the Miscellaneous Guidelines section, added the following bullet: ■ When you create an access port selector in a leaf interface rofile, the fexId property is configured with a default value of 101 even though a FEX is not connected and the interface is not a FEX interface. The fexId property is only used when the port selector is associated with an infraFexBndlGrp managed object.
October 3, 2019	In the Miscellaneous Guidelines section, added the bullet that begins as follows: ■ Fabric connectivity ports can operate at 10G or 25G speeds (depending on the model of the APIC server) when connected to leaf switch host interfaces.
September 17, 2019	4.1(1i): In the Open Bugs section, added bug CSCuu17314, CSCve84297, and CSCvg70246.
September 10, 2019	In the Known Behaviors section, added the bullet that begins with the following sentence: ■ ARP glean messages might not be forwarded across sites, breaking the capability of discovering silent hosts.
September 10, 2019	In the Known Behaviors section, added the following bullet: ■ 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.
August 14, 2019	4.1(1i): In the Open Bugs section, added bugs CSCvp38627, CSCvp82252, and CSCvq68833. 4.1(1j): In the Open Bugs section, added bug CSCvp53892. 4.1(1k): In the Open Bugs section, added bug CSCvp95621.
August 5, 2019	4.1(1i): In the Open Bugs section, added bug CSCvp25660.

Date	Description
July 22, 2019	4.1(1i): In the GUI Guidelines section, added the following bullet: ■ 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. In the CLI Guidelines section, added the following bullet: ■ 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. In the Open Bugs section, added bug CSCvq39764.
July 17, 2019	4.1(1i): In the Open Bugs section, added bug CSCvq39922.
July 11, 2019	4.1(1i): In the Open Bugs section, added bug CSCvj89771.
June 13, 2019	4.1(1): In the Known Behavior section, added a known behavior.
June 7, 2019	In the Hardware Compatibility section, added the following bullet: ■ First generation switches (models without -EX, -FX, or later designations) 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.
May 30, 2019	4.1(1l): Release 4.1(1l) became available. Added the open bugs for this release.
May 20, 2019	4.1(1k): Release 4.1(1k) became available. Added the resolved bugs for this release.
April 25, 2019	4.1(1j): Release 4.1(1j) became available. Added the resolved bugs for this release.
April 9, 2019	4.1(1i): In the Open Bugs section, added bug CSCvp24262.
April 6, 2019	In the New Software Features section, added mention of the Cisco Cloud APIC product.
April 3, 2019	In the Miscellaneous Guidelines section, added mention that connectivity filters are deprecated.
March 28, 2019	4.1(1i): Release 4.1(1i) became available.

Contents

This document includes the following sections:

New and Changed Information

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

New Software Features

The following sections list the new software features in this release:

Fabric Infrastructure

The following table lists the new fabric infrastructure features in this release:

Table 2 New Software Features—Fabric Infrastructure

Feature	Description	Guidelines and Restrictions
BGP multicast v4 address family support	APIC now supports the BGP multicast v4 address family.	None.
Cloud APIC	This release includes the release of the Cisco Cloud APIC product, which enables you to extend a Cisco ACI Multi-Site fabric to Amazon Web Services (AWS) public clouds. For more information, see the Cloud APIC documentation	See the *Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release*

Feature	Description	Guidelines and Restrictions
	set: https://www.cisco.com/c/en/us/support/cloud-systems-management/cloud-application-policy-infrastructure-controller/tsd-products-support-series-home.html	*4.1(1).*
EPG Communication tab	This release adds the EPG Communication tab. This tab enables you to create communication between two EPGs and to monitor which EPGs are communicating with one other through a contract and filters. Using this tab represents a simpler, faster way to set up a contract between the EPGs.	None.
FC-NPV enhancements	This release enhances FC NPV to support: Having an FCoE host that uses FEX over an FC NPV link 32G Brocade interoperability	None.
Filter groups	Support is now available for configuring filter groups, with flow entries that are used to filter the traffic, and associating them to SPAN source groups. For more information, see the *Cisco APIC Troubleshooting Guide, Release 4.1(x).*	None.
IP SLA	Internet protocol service level agreement (IP SLA) tracking is a common requirement in networks that allows a network administrator to collect information about network performance in real-time. With Cisco ACI IP SLA, you can track an IP address using ICMP and TCP probes. Tracking configurations can influence route tables, allowing for routes to be removed when tracking results come in negative and returning the route to the table when the results become positive again. For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide, Release 4.1(x).*	None.
Layer 1/Layer 2 policy-based redirect	This feature allows you to configure policy-based redirect on Layer 1 or Layer 2 service devices. For more information, see the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.1(x).*	■ Active-active deployment is not supported. ■ The two legs of the Layer 2 service device need to be configured on a different leaf switch to avoid packet loops. Per port VLAN is not supported. ■ Shared bridge domain is not supported. A Layer

Feature	Description	Guidelines and Restrictions
		1/ Layer 2 device bridge domain cannot be shared with Layer 3 device or regular EPGs. ■ Service node in managed mode is not supported. ■ Layer 1/Layer 2 devices support physical domain only, VMM domain is not supported.
Local SPAN with port-channels as the destination	Support is now available for local SPAN with port-channels as the destination. For more information, see the *Cisco APIC Troubleshooting Guide, Release 4.1(x)*.	Sources and the port-channel must be local on the same switch.
Mini ACI fabric with ACI Multi-Site topology	You can now use mini ACI fabric with ACI Multi-Site topology on a single pod.	None.
MLD snooping	Support is now available for Multicast Listener Discovery (MLD) snooping. For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide, Release 4.1(x)*.	None.
Multi-tier architecture	You can create a multi-tier ACI fabric topology that corresponds to a Core-Aggregation-Access architecture found in many existing data centers. While providing all of the benefits of the ACI fabric, the multi-tier architecture enhancement also mitigates the need to upgrade costly components such as rack space or cabling. The addition of a tier-2 leaf layer makes this topology possible. The tier-2 leaf layer supports connectivity to hosts or servers on the downlink ports and connectivity to the leaf layer (aggregation) on the uplink ports. For more information, see the *Cisco APIC Getting Started Guide, Release 4.1(x)*.	None.
SSD monitoring	The SSD monitoring feature enables you to override the preconfigured thresholds for the SSD lifetime parameters and raise faults when the SSD reaches some percentage of the configured thresholds. These faults allows network operators the capability to monitor and proactively replace any switch before the switch fails due to an SSD's lifetime parameter values becoming exceeded. For more information, see the *Cisco APIC SSD Monitoring*	■ This feature requires Micron M600 64 gb SSDs. ■ You cannot configure this feature using the CLI.

Feature	Description	Guidelines and Restrictions
	KB article.	
Virtual Port Channel migration	This feature allows the migration of nodes from non-EX, non-FX, and non-FX2 switch to an EX, FX, or FX2 switch. For more information, see the *Cisco Application Centric Infrastructure Fabric Hardware Installation Guide*.	None.

Fabric Scale and Other Enhancements

The following table lists the new fabric scale and other enhancements features in this release:

Table 3: New Software Features—Fabric Scale and Other Enhancements

Feature	Description	Guidelines and Restrictions
Bookmarks	You can now bookmark almost any page, which enables you to go back to that page easily by choosing the bookmark from your list of bookmarks. In previous releases, this feature was represented as favorites (the star icon), and had less capability. For more information, see the *Cisco APIC Getting Started Guide, Release 4.1(x)*.	None.
Confirmation and summary screens	Some of the wizards now include a confirmation screen and summary screen as the last steps. On the confirmation screen, you see a list of the policies that the wizard will create. You can change the names of the policies, if necessary. After the confirmation screen is the summary screen, which shows you the policies that the wizard created. You can no longer change the policies' names, but you can edit the properties of a policy.	None.
Default tab	This feature enables you to set a tab as the "favorite" on a page. Whenever you navigate to that page, that tab will be the default tab that is displayed. This feature is enabled only for the tabs in the Work pane. For more information, see the *Cisco APIC Getting Started Guide, Release 4.1(x)*.	None.
Error counter enhancement	Physical interface configuration now includes error counter statistics information.	None.
Export tech support configuration data enhancement	This enhancement allows the user to export tech support data or configurations with read-only privileges. For more information, see the *Cisco ACI Configuration Files: Import and Export* KB article.	None.

Feature	Description	Guidelines and Restrictions
GTP load balancing	This feature enables the Cisco APIC to perform fabric load balancing based on GTP TEID. For more information, see the *Cisco APIC Basic Configuration Guide, Release 4.1(x)*.	None.
Leaf switch uplink ports priority	When the fabric is scaled with numerous bridge domains, endpoint groups, and so on, and each are allocated a VLAN, this causes VLAN resource contention. Reloading a leaf switch in this state causes the leaf-to-spine switch uplink to enter the disabled state (those links do not come up). In this release, the leaf-to-spine switch uplinks are given a higher priority with the VLAN resource that is allocated to them, so that reloading a leaf switch while the switch is in a VLAN resource contention state does not affect the leaf-to-spine switch uplinks (the links come up).	None.
Multiple-context apps	You can now run an app in multiple GUI screens, or "contexts." For example, you can run the app while looking at a tenant's application profiles and while looking at the tenant's contracts. Prior to the 4.1 release, you could run an app only in one context; switching to a different context would close the app.	None.
New alerts	This release adds the following alerts: Leaf x is Inactive: This alert warns you that a leaf switch became inactive, powered down, or disconnected. New Switch Discovered: This informational alert informs you when a new switch is discovered. Node Outage: Indicates that a node is either down or reloading. Node x Must Be Reloaded: This alert warns you that an SSD must be reformatted and repartitioned. OSPF Connectivity is Down: This alert warns you when OSPF connectivity is down. The alert lists the interfaces that have OSPF configured, but are not able to communicate with one another, and provides a recommended troubleshooting action. Process Crash: This alert warns you that a process has crashed. Split-Fabric Detected: Indicates that the fabric is split and that the controller is operating in read-only mode.	None.
Scale changes	This release includes the following scale changes: ■ Maximum number of remote leaf switches: 128	None.

Feature	Description	Guidelines and Restrictions
	(single pod) ■ 100 sub-interfaces per VRF and per L3Out ■ 4,000 MAC address EPGs	
Object Store Browser improvements	The Object Store Browser has the following improvements: The Object Store Browser has a new, modernized look-and-feel. You can now search by class, distinguished name, or URL, instead of only class and distinguished name. After you find an object, you can make the object a favorite, which enables you to go to your list of favorites and load the object from there. You can now view the JSON response of your last query; previously you could only view the XML response. The Object Store Browser by default displays all of the properties, even those that have no value. You can now hide the properties that do not have a value. You can now navigate the distinguished name using the bread crumbs, which is simpler and easier to use. You can now only view a distinguished name's stats, faults, or health if there is applicable data.	None.

Solution Integration

The following table lists the new solution integration features in this release:

Table 4 New Software Features—Solution Integration

Feature	Description	Guidelines and Restrictions
Microsoft NLB	Support is now available for Microsoft Network Load Balancing (NLB). For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide, Release 4.1(x)*.	None.

Virtualization

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

Table 5 New Software Features—Virtualization

Feature	Description	Guidelines and Restrictions
Cisco ACI integration with Cisco's SD-WAN	vManage integration enables tenant admins to apply preconfigured policies to specify the levels of packet loss, jitter, and latency for tenant traffic over the WAN. When a WAN SLA policy is applied to tenant traffic, the Cisco APIC sends the configured policies to a vManage controller. The vManage controller, which is configured as an external device manager that provides Cisco Software-Defined Wide Area Network (SD-WAN) capability, chooses the best possible WAN link that meets the loss, jitter, and latency parameters specified in the SLA policy. For more information, see the *Cisco ACI and SD-WAN Integration Guide.*	None.
Cisco ACI with Cisco UCSM integration	You can automate networking policies on Cisco UCS devices. To do so, you integrate Cisco UCSM into the Cisco Application Centric Infrastructure (ACI) fabric. Cisco APIC takes hypervisor NIC information from the Cisco UCSM and a virtual machine manager (VMM). The automation applies to all the devices that the Cisco UCSM manages. For more information, see the chapter "Cisco ACI with Cisco UCSM Integration" in the *Cisco ACI Virtualization Guide, Release 4.1(1).*	■ If you use Cisco Application Virtual Switch (AVS) or Microsoft System Center Virtual Machine Manager (SCVMM), you also must associate a switch manager with the VMM. ■ If you use Cisco ACI Virtual Edge or VMware vSphere Distributed Switch (VDS), make the association if you *do not* use LLDP or CDP in your VMM domain.

New Hardware Features

For new hardware features, see the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 14.1(1)* at the following location:

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html

Changes in Behavior

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 Cisco APIC documentation site at the following URL:

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

See the "Upgrading and Downgrading the Cisco APIC and Switch Software" section of the *Cisco APIC Installation, Upgrade, and Downgrade Guide.*

Bugs

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

- [Open Bugs](#)
- [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 4.1(1) releases in which the bug exists. A bug might also exist in releases other than the 4.1(1) releases.

Table 6 Open Bugs in This Release

Bug ID	Description	Exists in
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.	4.1(1l) 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.	4.1(1l) and later
CSCvp95621	The showconfig command fails and displays an exception.	4.1(1k) and later
CSCvq22658	Description fields are not available for resource pools (VLAN, VSAN, Mcast, VXLAN etc).	4.1(1k) 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,	4.1(1k) and later
CSCvp53892	When the APIC fails to retrieve/process the adjacency for one of the host uplink VMNICs, it does not continue to process the rest of the uplink VMNICs. The resulting behavior can be different depending upon the order in which the host VMNICs is processed; which can be different each time. With the remainder of the adjacency that is not being processed, this can result in APIC removing VLANs from the leaf switches depending upon the resolution immediacy of the VMM domain.	4.1(1j) and later

Bug ID	Description	Exists in
CSCvp68296	The APIC process information from the APIC GUI may have the wrong values.	4.1(1j) and later
CSCvp79155	Inventory pull operations or VMware vCenter updates are delayed.	4.1(1j) and later
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.	4.1(1j) and later
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	4.1(1j) and later
CSCvr12971	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.	4.1(1j) and later
CSCvr85821	The API query /api/class/compCtrlr.json?rsp-subtree=full? returns a malformed JSON file.	4.1(1j) and later
CSCuu17314	CDP is not enabled on the management interfaces for the leaf switches and spine switches.	4.1(1i) and later
CSCvd43548	The stats for a given leaf switch rule cannot be viewed if a rule is double-clicked.	4.1(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.	4.1(1i) and later
CSCve84297	A service cannot be reached by using the APIC out-of-band management that exists within the 172.17.0.0/16 subnet.	4.1(1i) and later

Bug ID	Description	Exists in
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]	4.1(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.	4.1(1i) and later
CSCvg00627	A tenant's flows/packets information cannot be exported.	4.1(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.	4.1(1i) and later
CSCvg70246	When configuring an L3Out under a user tenant that is associated with a VRF instance that is under the common tenant, a customized BGP timer policy that is attached to the VRF instance is not applied to the L3Out (BGP peer) in the user tenant.	4.1(1i) and later
CSCvg81020	For strict security requirements, customers require custom certificates that have RSA key lengths of 3072 and 4096.	4.1(1i) and later
CSCvh52046	This is an enhancement to allow for text-based banners for the Cisco APIC GUI login screen.	4.1(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.	4.1(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.	4.1(1i) and later
CSCvi20535	When a VRF table is configured to receive leaked external routes from multiple VRF tables, the Shared Route Control scope to specify the external routes to leak will be applied to all VRF tables. This results in an unintended external route leaking. This is an enhancement to ensure the Shared Route Control scope in each VRF table should be used to leak external routes only from the given VRF table.	4.1(1i) and later

Bug ID	Description	Exists in
CSCvj41092	The APIC log files are extremely large, which takes a considerable amount of time to upload, especially for users with slow internet connectivity.	4.1(1i) and later
CSCvi80543	This is an enhancement that allows failover ordering, categorizing uplinks as active or standby, and categorizing unused uplinks for each EPG in VMware domains from the APIC.	4.1(1i) and later
CSCvi82903	When authenticating with the Cisco APIC using ISE (TACACS), all logins over 31 characters fail.	4.1(1i) and later
CSCvj56726	The connectivity filter configuration of an access policy group is deprecated and should be removed from GUI.	4.1(1i) and later
CSCvj89771	The Virtual Machine Manager (vmmmgr) process crashes and generates a core file.	4.1(1i) and later
CSCvk04072	There is no record of who acknowledged a fault in the Cisco APIC, nor when the acknowledgement occurred.	4.1(1i) and later
CSCvk18014	The action named 'Launch SSH' is disabled when a user with read-only access logs into the Cisco APIC.	4.1(1i) and later
CSCvm32345	A port group cannot be renamed. This is an enhancement request to enable the renaming of port groups.	4.1(1i) and later
CSCvm42914	This is an enhancement request to add policy group information to the properties page of physical interfaces.	4.1(1i) and later
CSCvm56946	Support for local user (admin) maximum tries and login delay configuration.	4.1(1i) and later
CSCvm63668	A single user can send queries to overload the API gateway.	4.1(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.	4.1(1i) and later

Bug ID	Description	Exists in
CSCvm89559	The svc_ifc_policye process consumes 100% of the CPU cycles. The following messages are observed in svc_ifc_policymgr.bin.log: 8816||18-10-12 11:04:19.101||route_control||ERROR||co=doer:255:127:0xff00000000c42ad2:11||Route entry order exceeded max for st10960-2424833-any-2293761-33141-shared-svc-int Order:18846Max:17801|| ../dme/svc/policyelem/src/gen/ifc/beh/imp/./rtctrl/RouteMapUtils.cc||239:q	4.1(1i) and later
CSCvn00576	An SHA2 CSR for the ACI HTTPS certificate cannot be configured in the APIC GUI.	4.1(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.	4.1(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.	4.1(1i) and later
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.	4.1(1i) and later
CSCvp07262	Configuration import (configImportP) with importMode="atomic" and importType="replace" may not work.	4.1(1i) and later
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.	4.1(1i) and later
CSCvp26694	A leaf switch gets upgraded when a previously-configured maintenance policy is triggered.	4.1(1i) and later
CSCvp38627	Some tenants stop having updates to their state pushed to the APIC. The aim-aid logs have messages similar to the following example: An unexpected error has occurred while reconciling tenant tn-prj_...: long int too large to convert to float	4.1(1i) and later
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".	4.1(1i) and later
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.	4.1(1i) and later

Bug ID	Description	Exists in
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.	4.1(1i) and later
CSCvp62048	New port groups in VMware vCenter may be delayed when pushed from the Cisco APIC.	4.1(1i) and later
CSCvp64280	A vulnerability in the fabric infrastructure VLAN connection establishment of the Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an unauthenticated, adjacent attacker to bypass security validations and connect an unauthorized server to the infrastructure VLAN. The vulnerability is due to insufficient security requirements during the Link Layer Discovery Protocol (LLDP) setup phase of the infrastructure VLAN. An attacker could exploit this vulnerability by sending a malicious LLDP packet on the adjacent subnet to the Cisco Nexus 9000 Series Switch in ACI mode. A successful exploit could allow the attacker to connect an unauthorized server to the infrastructure VLAN, which is highly privileged. With a connection to the infrastructure VLAN, the attacker can make unauthorized connections to Cisco Application Policy Infrastructure Controller (APIC) services or join other host endpoints. Cisco has released software updates that address this vulnerability. There are workarounds that address this vulnerability. This advisory is available at the following link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-n9kaci-bypass	4.1(1i) and later
CSCvp72283	An APIC running the 3.0(1k) release sometimes enters the "Data Layer Partially Diverged" state. The acidiag rvread command shows the following output for the service 10 (observer): Non optimal leader for shards :10:1,10:3,10:4,10:6,10:7,10:9,10:10,10:12,10:13,10:15,10:16,10:18,10:19,10:21,10:22,10:24,10:25, 10:27,10:28,10:30,10:31	4.1(1i) and later
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.	4.1(1i) and later

Bug ID	Description	Exists in

CSCvp82252	While modifying the host route of OpenStack, the following subnet trace is generated:
	
	Response :
	
	{
	
	   "NeutronError" : {
	
	      "message" : "Request Failed: internal server error while processing your request.",
	
	      "type" : "HTTPInternalServerError",
	
	      "detail" : " "
	
	   }
	
	}
		4.1(1i) and later

CSCvp86156	If a user manually modifies an object controlled by the ACI CNI, the configuration will not be restored for up to 14 minutes.	4.1(1i) and later
CSCvp94060	No fault is raised when First Hop Security is enabled in a Layer 2 only Bridge Domain.	4.1(1i) and later
CSCvp94085	The APIC Licensemgr generates a core file while parsing an XML response.	4.1(1i) and later
CSCvp95407	Access-control headers are not present in invalid requests.	4.1(1i) and later
CSCvp97092	Tenants that start with the word "infra" are treated as the default "infra" tenant.	4.1(1i) and later
CSCvp99430	The troubleshooting wizard is unresponsive on the APIC.	4.1(1i) and later
CSCvp99508	The GUI is slow when accessing access policies. This is an enhancement request to add pagination to resolve this issue.	4.1(1i) and later
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.	4.1(1i) and later

Bug ID	Description	Exists in
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.	4.1(1i) and later
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.	4.1(1i) and later
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.	4.1(1i) and later
CSCvq20055	In the APIC, the "show external-l3 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-l3 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.	4.1(1i) and later
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.	4.1(1i) and later
CSCvq31358	"show external-l3 interfaces node <id> detail" will display "missing" for both "Oper Interface" and "Oper IP", even though the L3Out is functioning as expected.	4.1(1i) and later
CSCvq38191	An eventmgr core file gets generated when a user performs the syslog debug command "logit".	4.1(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.	4.1(1i) and later
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).	4.1(1i) and later
CSCvq43101	When opening an external subnet, a user cannot see Aggregate Export/Import check boxes set in GUI even though they were already configured.	4.1(1i) and later
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.	4.1(1i) and later

Bug ID	Description	Exists in
CSCvq56057	ACI running 4.1.1j.	4.1(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.resImedcy) from Pre-Provision to On-Demand, the encap VLANs (vlanCktEp mo's) are NOT programmed on the leaf switches. This problem surfaces sporadically, meaning that it might take several resImedcy toggles between PreProv and OnDemand to reproduce the issue.	4.1(1i) and later
CSCvq58304	VMM inventory-related faults are raised for VMware vCenter inventory, which is not managed by the VMM.	4.1(1i) and later
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.	4.1(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.	4.1(1i) and later
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.	4.1(1i) and later
CSCvq68833	When upgrading from a 4.0 release to a 4.1 release while using a certificate with the APIC local user, the "Mandatory permission VMM Connectivity and VMM EP are required" fault occurs when accessing the Infrastructure page.	4.1(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.	4.1(1i) and later
CSCvq80820	A previously-working traffic is policy dropped after the subject is modified to have the "no stats" directive.	4.1(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.	4.1(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.	4.1(1i) and later

Bug ID	Description	Exists in
CSCvq95817	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.	4.1(1i) and later
CSCvr10510	There is a stale F2736 fault after configuring in-band IP addresses with the out-of-band IP addresses for the Cisco APIC.	4.1(1i) and later
CSCvr19693	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.	4.1(1i) and later
CSCvr30815	vmmPLInf objects are created with epgKey's and DN's that have truncated EPG names (truncated at ".").	4.1(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.	4.1(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]	4.1(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.	4.1(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	4.1(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.	4.1(1i) and later
CSCvr76318	Cisco ACI plugin containers do not get updated.	4.1(1i) and later

Bug ID	Description	Exists in
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.	4.1(1i) and later
CSCvr92169	The scope for host routes should be configurable; however, the option to define the scope is not available.	4.1(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.	4.1(1i) and later
CSCvr94614	There is a minor memory leak in svc_ifc_policydist when performing various tenant configuration removals and additions.	4.1(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.	4.1(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"	4.1(1i) and later
CSCvs03055	While configuring a logical node profile in any L3Out, the static routes do not have a description.	4.1(1i) and later
CSCvs04981	F2928 "KeyRing Certificate expired" faults raised and do not get cleared.	4.1(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.	4.1(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.	4.1(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.	4.1(1i) and later

Bug ID	Description	Exists in
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.	4.1(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".	4.1(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.	4.1(1i) and later
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".	4.1(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.	4.1(1i) and later
CSCvs47757	The plgnhandler process crashes on the Cisco APIC, which causes the cluster to enter a data layer partially diverged state.	4.1(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.	4.1(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.	4.1(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.	4.1(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.	4.1(1i) and later
CSCvs76244	The tmpfs file system that is mounted on /data/log becomes 100% utilized.	4.1(1i) and later
CSCvs78996	The policy manager (PM) may crash when use testapi to delete MO from policymgr db.	4.1(1i) and later

Bug ID	Description	Exists in
CSCvs81881	The Cisco APIC PSU voltage and amperage values are zero.	4.1(1i) and later
CSCvs81907	SNMP does not respond to GETs or sending traps on one or more Cisco APICs despite previously working properly.	4.1(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.	4.1(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.	4.1(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.	4.1(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.	4.1(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.	4.1(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.	4.1(1i) and later
CSCvt40736	The login history of local users is not updated in Admin > AAA > Users > (double click on local user) Operational > Session.	4.1(1i) and later

Bug ID	Description	Exists in
CSCvt44854	- Leaf or spine switch is stuck in 'downloading-boot-script' status. The node never fully registers and does not become active in the fabric. - You can check the status by running 'cat /mit/sys/summary | grep state' on the CLI of the spine or leaf switch: If the state is set to 'downloading-boot-script' for a long period of time (> 5 minutes) you may be running into this issue. - Checking the policy element logs on the spine or leaf switch will confirm if the bootscript file cannot be found on the Cisco APIC: 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" If you see this error message, check to make sure all Cisco APICs have the node bootscript files located in /firmware/fwrepos/fwrepo/boot.	4.1(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.	4.1(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.	4.1(1i) and later
CSCvt87506	SSD lifetime can be exhausted prematurely if unused Standby slot exists	4.1(1i) and later
CSCvt93482	The per feature container for techsupport "objectstore_debug_info" fails to collect on spines due to invalid filepath. Given filepath: more /debug/leaf/nginx/objstore*/mo | cat Correct filepath: more /debug/spine/nginx/objstore*/mo | cat TAC uses this file/data to collect information about excessive DME writes.	4.1(1i) and later
CSCvu01452	The MD5 checksum for the downloaded Cisco APIC images is not verified before adding it to the image repository.	4.1(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".	4.1(1i) and later

Bug ID	Description	Exists in
CSCvu21530	Protocol information is not shown in the GUI when a VRF table from the common tenant is being used in any user tenant.	4.1(1i) and later
CSCvu39569	The following error is encountered when accessing the Infrastructure page in the ACI vCenter plugin after inputting vCenter credentials. "The Automation SDK is not authenticated" VMware vCenter plug-in is installed using powerCLI. The following log entry is also seen in vsphere_client_virgo.log on the VMware vCenter: /var/log/vmware/vsphere-client/log/vsphere_client_virgo.log [ERROR] http-bio-9090-exec-3314 com.cisco.aciPluginServices.core.Operation sun.security.validator.ValidatorException: PKIX path validation failed: java.security.cert.CertPathValidatorException: signature check failed	4.1(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.	4.1(1i) and later
CSCvu62465	For an EPG containing a static leaf node configuration, the Cisco APIC GUI returns the following error when clicking the health of Fabric Location: Invalid DN topology/pod-X/node-Y/local/svc-policyelem-id-0/ObservedEthIf, wrong rn prefix ObservedEthIf at position 63	4.1(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.	4.1(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.	4.1(1i) and later
CSCvw33061	Traffic loss is observed from multiple endpoints deployed on two different vPC leaf switches.	4.1(1i) and later

Bug ID	Description	Exists in
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.	4.1(1i) and later
CSCvp24262	A policy-based redirect service graph configured with vzAny as the consumer and vzAny as the provider does not function. If you are using or want to use this capability, we recommend that you do not upgrade to the 4.1(1) release.	4.1(1i)

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 7 Resolved Bugs in This Release

Bug ID	Description	Fixed in
CSCvp21665	ACI Application (App) does not get enabled (started). There will be a fault raised for that App, stating Gluster-FS health is not OK. But Gluster-FS status is actually OK.	4.1(1k)
CSCvp68528	Sometimes Apps might not be able to access the filesystem. File access can return disk i/o error. The fix for this bug improves filesystem reliability.	4.1(1k)
CSCvp68533	The data stored by an App might be lost during an APIC upgrade. This can impact the functionality of the App.	4.1(1k)
CSCvp24262	A policy-based redirect service graph configured with vzAny as the consumer and vzAny as the provider does not function. If you are using or want to use this capability, we recommend that you do not upgrade to the 4.1(1) release.	4.1(1j)
CSCuu31743	When creating a firmware download job on the APIC GUI by using Admin > Download Tasks > "create outside firmware source" and selecting SCP while your web browser is connected to APIC1, APIC2 might actually be downloading the file.This is an enhancement request for the APIC GUI to indicate which APIC is trying to download the file when the download fails so that further troubleshooting can be done on the correct port.	4.1(1i)
CSCva02247	When attempting to upload a firmware file to an APIC, an error indicating the "repository [is] over 80% full" appears. Even deleting previously uploaded firmware files does not clear out enough space.	4.1(1i)
CSCvd12514	There is no way to see the next DHCP address to be assigned from a DHCP pool.	4.1(1i)

Bug ID	Description	Fixed in
CSCvg41187	In an ACI GOLF deployment, the external GOLF router will advertise its routes using BGP EVPN to the spine switches, which will reoriginate those into VPNv4 and advertise to the leaf switches that should import them. These VPNv4 routes will have the VXLAN VNID of the originating VRF instance set in the "label" field, and in the hardware a rewrite entry is added for this VNID corresponding to the VXLAN tunnel that extends to the GOLF router. Due to hardware restrictions within a single VRF instance on an ACI leaf switch, there can only be one VXLAN VNID rewrite entry per tunnel. If two VRF instances in ACI are configured with the same route-target import/export policy, then the leaf switch will attempt to import the VPNv4 routes in the same VRF instance with different VXLAN VNIDs. Because only a single rewrite VNID can be installed per tunnel per VRF instance, this will prevent some rewrite VNIDs from being installed in hardware. As a result, you may see that traffic that is from the leaf switch going to the GOLF router will either have a VNID of 0 or will have the wrong VNID set.	4.1(1i)
CSCvi45842	This is an enhancement to set the reload delay timer between the ACI ToRs upgrades if the maximum concurrent nodes is 1.	4.1(1i)
CSCvi48314	Currently, the ACI upgrade process involves uploading of the images to the spine/leaf switch and activating the newer code.These upload/activating procedures cannot be separated and must be performed in one maintenance window. This causes the maintenance window to be longer.	4.1(1i)
CSCvi63720	SNMP commands on the CLI causes an error to display.	4.1(1i)
CSCvj89447	The Name column is missing on the Subnets table from the External Network Policy screen in the Routed Outside Policy screen. The Name field is missing on the Create Subnet panel.	4.1(1i)
CSCvk31427	The current implementation of APIC techsupport collects the latest 10,000 logs of audit and faults. That works for certain scenarios. However, there are many troubleshooting scenarios that need to get all records of the audits, faults, and events. This enhancement is requesting the implementation of the collection of all audit, fault, and event logs in separate compressed gzip files.	4.1(1i)
CSCvk35070	After creating and deleting the pod 2 TEP Pool under "Pod Fabric Setup Policy", the pod 1 Infra VLAN "172.31.0.0/16" leaks to the "overlay-1" route map on the leaf switch.	4.1(1i)
CSCvk41676	The neutron call using ip cidr for the --allowed-address-pairs feature is not supported with the ACI plugin for OpenStack.	4.1(1i)
CSCvk74125	The @ symbol cannot be used when configuring an SNMP community due to the symbol being interpreted as a delimiter for the context. Using @ results in unknown context errors incrementing in the "show snmp" command.	4.1(1i)
CSCvm10827	Database files and logs related to a previous upgrade are not collected in the techsupport files.	4.1(1i)

Bug ID	Description	Fixed in
CSCvm12790	A remote leaf switch configures a static route to the Cisco APIC based on which Cisco APIC replies for its DHCP. This route does not get deleted after the remote leaf switch is commissioned. This behavior might cause the static route to get redistributed to the IPN, which then points the route to this specific IPN back to the remote leaf switch. Because the Cisco APIC in question and remote leaf switch will now have a routing issue, they cannot communicate. From this Cisco APIC, the remote leaf switch cannot be managed.	4.1(1i)
CSCvm55394	A shard is stuck and cannot move forward. Continuous handleTxCheckTimeout can be seen in the source log with no new transaction being sent to the replica.	4.1(1i)
CSCvm57106	After upgrading to the 3.2(3n) release, fault F608054 appeared, indicating fsm-sync-with-quorum-fsm-fail.	4.1(1i)
CSCvn07827	PLR fails after upgrading to a Cisco APIC 4.0 release.	4.1(1i)
CSCvn10244	If a techsupport that is exported to the APIC and is generated after a configuration snapshot, rolling back to that snapshot removes the techsupport configuration and the logs that are saved to the APIC. The exported logs should instead be preserved as long as possible, and rolling back the snapshot should not cause the log/trace removal.	4.1(1i)
CSCvn11128	APIC accepts the "_" (underscore) symbol as delimiter for VMware VMM domain integration, even though it is not a supported symbol.This is an enhancement request to implement a check in the APIC GUI to not accept "_".	4.1(1i)
CSCvn12389	If multiple path attachments (l2extRsPathL2OutAtt) are configured for the same interface under different node profiles (l2extLNodeP) or different interface profiles (l2extLIfP), the configuration is blocked by the policy manager (PM), but is allowed by the policy distributed (PD), causing an inconsistency between the components. As a result, the posted configuration will not be displayed under the GUI. Additionally, depending on the APIC version, the configuration push failure from the PD to PM may cause all subsequent configurations for the shard to fail. As a result, all configuration changes for a particular tenant may appear to fail.	4.1(1i)
CSCvn27112	When using the Firefox browser to view "Operations > Visibility & Troubleshooting," the zoom icons are missing on the result page.	4.1(1i)
CSCvn30026	The subject and body fields do not allow modification.	4.1(1i)
CSCvn30897	If you configure two OSPF L3Outs with external network "0.0.0.0/0," with one being border leaf 101 and the other being border leaf 102, sometimes a route is learned from border leaf 102, but the "Visibility & Troubleshooting" shows the destination border leaf as border leaf 101.	4.1(1i)
CSCvn56421	Traffic returning from a PBR node is redirected back to the PBR node, forming a loop.	4.1(1i)
CSCvn65756	The F3222 fault displays after you delete a pool.	4.1(1i)
CSCvn67365	This is an enhancement to update OpenSSH to version 7.8+ to remediate CVE-2018-15473.More info can be found here: https://tools.cisco.com/security/center/viewAlert.x?alertId=58762	4.1(1i)

Bug ID	Description	Fixed in
CSCvn67689	Changing the "DH Param" setting on the APIC from the default "None" results in the following pop-up error message: Error: 400 - Failed to update communication configuration (Configuration not valid for server (Nginx)) The configuration does not get applied.	4.1(1i)
CSCvn67742	The Cisco APIC sets the mcast attribute to "yes" after disabling PIM on an L3Out. However, the APIC should instead set the attribute to "no."	4.1(1i)
CSCvn70746	The Dashboard UI can display negative fault counts or wrong fault counts inconsistently with the "Fault Summary" UI.	4.1(1i)
CSCvn77241	During same-VC-cross-DC VM migrations, there is one task triggered per VM to verify its migration status. However, if too many VMs are migrated within a short period of time, the amount of tasks due to the bulk migration might exceed the size of the task queue, which leads to huge amount of faults.	4.1(1i)
CSCvn78438	When using the "show vsan-domain detail" command, all interfaces that are configured with "NP" show as "F" mode, and the following error displays at the end of the output: Error: Invalid RN rsvsanPathAtt-[topology/pod-1/node-1301/sys/conng/path-[10Gb-CCH-Server-VPC-SR227]]	4.1(1i)
CSCvn79128	When upgrading from some 3.2 or 3.1 releases to 4.0, some or all leaf switch maintenance groups will immediately start upgrading without being user-triggered. This issue occurs as soon as the APICs finish upgrading.	4.1(1i)
CSCvn80201	The APIC syslog does not log the username for login/logout attempts.	4.1(1i)
CSCvn81454	The F0053 fault is generated.	4.1(1i)
CSCvn81863	TPM is supposed to be used to encrypt certain partitions, but on a 4.0 release, the image can be installed without TPM being enabled, and the APIC can also boot up without it.	4.1(1i)
CSCvn87426	The query lists out incorrect objects that do not match the "eq" or "ne" filter.	4.1(1i)
CSCvn93417	This is an enhancement request to include the output of /proc/kpm_err_stat in ACI switch techsupports.	4.1(1i)
CSCvn94771	There is a lot of lag when entering the command "show endpoint ip <ip>".	4.1(1i)
CSCvn95704	On the Mgmt tenant, when trying to configure monitoring polices, the button does not take any actions and monitoring policies cannot be configured on this tenant.	4.1(1i)
CSCvn98133	The 'showconfig' command from the APIC does not print the config and instead generates a traceback. This will result in an invalid user_config file in the APIC 1of3 techsupport file.	4.1(1i)
CSCvo05509	This is an enhancement request to include the ethpmFcot MO to ACI leaf switch techsupport files.	4.1(1i)
CSCvo15401	Database files and logs related to a previous upgrade are not collected in the techsupport files.	4.1(1i)

Bug ID	Description	Fixed in
CSCvo17041	The same IP address added under NTP in different formats (with/without leading zeroes) are treated as unique entries on the APIC. A switch will have single entry. Deleting one of the entries on the APIC will delete that entry from the switch.	4.1(1i)
CSCvo23714	NGINX gets has an out of memory issue approximately every 10 hours due to the memory usage growing to up to 8GB.	4.1(1i)
CSCvo29820	Where a trunk port group was created and what was pushed to it cannot be verified within the APIC GUI.	4.1(1i)
CSCvo31212	When a spine switch is used as an L3Out device to IPN/ISN, in a multi-pod with Cisco ACI Multi-Site configuration, after switching over the sup in a 9508 chassis, a flapping event might be seen in the logs for a DHCP client interface operational state on the L3Out external interface.	4.1(1i)
CSCvo35391	The following issues are observed:

The LLDPAD process crashes on an APIC.

The LLDPAD service cannot start anymore after the core, not even after a cold reboot of the APIC.

EDAC errors are observed in dmesg prior to the LLDPAD crash.

The LLDPAD crash causes the directly-connected leaf switches to lose the APIC controller LLDP adjacency (lldpCtrlrAdjEp).

eth2-1 and eth2-2 do not receive any frames/packets anymore, as observed with the ifconfig command.

TX counters are going up.

The APIC gets a reduced health score in avread (health: 2) and perceives the cluster state incorrectly due to there being no RX frames/packets. | 4.1(1i) |
CSCvo35552	When using a specific out-of-band or in-band contract to only allow certain protocols, all ports are open.	4.1(1i)
CSCvo39336	If many faults flap on the switch nodes, the GUI may run slowly and have poor response.	4.1(1i)
CSCvo42782	If the infra-VLAN in the input to acc-provision is different from what it detects on the fabric, acc-provision warns you that infra-VLAN configuration is incorrect, but it still uses the requested VLAN as the desired value for infra-VLAN.	4.1(1i)
CSCvo45535	Changing the timezone on the APIC leads to different timezones on the APICs and leaf switches. For example, choosing the Europe/Istanbul timezone leads to the time on the leaf/spine switches to be GMT+3 (which is correct, due to daylight saving time), while on the APIC the timezone shows as +2.This causes an issue with syslog messages sent from the APICs and leaf switches, as they have different timestamps.	4.1(1i)
CSCvo47323	ARP poisoning occurs when return traffic from the uplink to the SNAT interface is sent back to the uplink. All of the uplink IP addresses appear as coming from the SNAT MAC address.	4.1(1i)
CSCvo51421	When the TACACS user privilege is admin, the vCenter plugin only gets read permissions when fetching the privileges from the APIC.	4.1(1i)

Bug ID	Description	Fixed in
CSCvo57185	The GUI doesn't display hypervisor details on double clicking if there are more than 16.	4.1(1i)
CSCvo59407	When the FEX is removed the ACI leaf switch, the FEX status become offline and is completely removed after around 20 minutes. However, the license consumption on the APIC is not updated nor released.	4.1(1i)
CSCvo66664	XML special characters in the SNMP location and name are not properly escaped when exported into XML. This causes issues in being able to parse the XML output properly. In addition, Cisco ACI Multi-Site Orchestrator (MSO) queries the SNMP information and attempts to parse the XML export of the SNMP config. If the SNMP community policy or SNMP location have special characters (&, <, >), pushing policies onto these sites may fail, as MSO cannot parse the XML output.	4.1(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 4.1(1) releases in which the known behavior exists. A bug might also exist in releases other than the 4.1(1) releases.

Table 8 Known Behaviors in This Release

Bug ID	Description	Exists in
CSCvj26666	The "show run leaf|spine <nodeId>" command might produce an error for scaled up configurations.	4.1(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.	4.1(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.	4.1(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.

- In the 4.1(1) release, a software check has been added to validate Ethernet transceivers. Before ACI 4.1, this check was not present in the software. This check is required to make sure Ethernet ports are properly identified. If the software check detects an Ethernet transceiver to have Fibre Channel SPROM values, the transceiver will fail the validation check and will be put into a downed state. If any Ethernet transceivers have an

incorrectly programmed SPROM which identifies them as FC compliant, they will fail the transceiver validation and fail to come up on 4.1(1). In this scenario, contact your respective vendors to update and address the programmed SPROM values.

All Ethernet transceivers that have the expected Ethernet SPROM programming should continue to work after the upgrade.

■ 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.

■ 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 at the following URL:

https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/aci/virtualization/matrix/virtmatrix.html

■ This release supports VMM Integration and VMware Distributed Virtual Switch (DVS) 6.5 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 4.1(1)* at the following URL:

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

■ For information about Cisco APIC compatibility with Cisco UCS Director, see the appropriate *Cisco UCS Director Compatibility Matrix* document at the following URL:

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

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 14.1(1)* at the following location:

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html

■ To connect the N2348UPQ to Cisco ACI leaf switches, the following options are available:

— Directly connect the 40G FEX ports on the N2348UPQ to the 40G switch ports on the Cisco ACI leaf switches

— Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the 10G ports on all other Cisco ACI leaf switches.

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

■ 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.

- 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 14.1(1)

    — Cisco AVS, Release 5.2(1)SV3(3.11)

      For more information about the supported AVS releases, see the AVS software compatibility information in the *Cisco Application Virtual Switch Release Notes* at the following URL:

      https://www.cisco.com/c/en/us/support/switches/application-virtual-switch/products-release-notes-list.html

    — Cisco 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.

- 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)

  — 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 at the following URL:

  https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/solution-overview-listing.html

- A known issue exists with the Safari browser and unsigned certificates, which applies when connecting to the Cisco APIC GUI. For more information, see the *Cisco APIC Getting Started Guide.*

- For compatibility with OpenStack and Kubernetes distributions, see the *Cisco Application Policy Infrastructure Controller OpenStack and Container Plugins Release Notes, Release 4.1(1).*

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.

- 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.

■ You cannot use remote leaf switches with Cisco ACI Multi-Site.

IP Address Guidelines

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

■ For the following services, use a DNS-based hostname with out-of-band management connectivity. IP addresses can be used with both in-band and out-of-band management connectivity.

— Syslog server

— Call Home SMTP server

— Tech support export server

— Configuration export server

— Statistics export server

■ The infrastructure IP address range must not overlap with other IP addresses used in the fabric for in-band and Out-of-band networks.

■ If an IP address is learned on one of two endpoints for which you are configuring an atomic counter policy, you should use an IP-based policy and not a client endpoint-based policy.

■ A multipod deployment requires the 239.255.255.240 system Global IP Outside (GIPo) to be configured on the inter-pod network (IPN) as a PIM BIDIR range. This 239.255.255.240 PIM BIDIR range configuration on the IPN devices can be avoided by using the Infra GIPo as System GIPo feature. The Infra GIPo as System GIPo feature must be enabled only after upgrading all of the switches in the Cisco ACI fabric, including the leaf switches and spine switches, to the latest Cisco APIC release.

■ Cisco ACI does not support a class E address as a VTEP address.

Miscellaneous Guidelines

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

■ User passwords must meet the following criteria:

— Minimum length is 8 characters

— Maximum length is 64 characters

— Fewer than three consecutive repeated characters

— At least three of the following character types: lowercase, uppercase, digit, symbol

— Cannot be easily guessed

— Cannot be the username or the reverse of the username

— Cannot be any variation of "cisco", "isco", or any permutation of these characters or variants obtained by changing the capitalization of letters therein

- In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.

- The power consumption statistics are not shown on leaf node slot 1.

- If you defined multiple login domains, you can choose the login domain that you want to use when logging in to a Cisco APIC. By default, the domain drop-down list is empty, and if you do not choose a domain, the DefaultAuth domain is used for authentication. This can result in login failure if the username is not in the DefaultAuth login domain. As such, you must enter the credentials based on the chosen login domain.

- A firmware maintenance group should contain a maximum of 80 nodes.

- When contracts are not associated with an endpoint group, DSCP marking is not supported for a VRF with a vzAny contract. DSCP is sent to a leaf switch along with the actrl rule, but a vzAny contract does not have an actrl rule. Therefore, the DSCP value cannot be sent.

- The Cisco APICs must have 1 SSD and 2 HDDs, and both RAID volumes must be healthy before upgrading to this release. The Cisco APIC will not boot if the SSD is not installed.

- In a multipod fabric setup, if a new spine switch is added to a pod, it must first be connected to at least one leaf switch in the pod. Then the spine switch is able to discover and join the fabric.

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

- For a Cisco APIC REST API query of event records, the Cisco APIC system limits the response to a maximum of 500,000 event records. If the response is more than 500,000 events, it returns an error. Use filters to refine your queries. For more information, see *Cisco APIC REST API Configuration Guide*.

- Subject Alternative Names (SANs) contain one or more alternate names and uses any variety of name forms for the entity that is bound by the Certificate Authority (CA) to the certified public key. These alternate names are called "Subject Alternative Names" (SANs). Possible names include:

  — DNS name

  — IP address

- If a node has port profiles deployed on it, some port configurations are not removed if you decommission the node. You must manually delete the configurations after decommissioning the node to cause the ports to return to the default state. To do this, log into the switch, run the setup-clean-config.sh script, wait for the script to complete, then enter the reload command.

- When using the SNMP trap aggregation feature, if you decommission Cisco APICs, the trap forward server will receive redundant traps.

■ 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 rofile, the fexId property is configured with a default value of 101 even though a FEX is not connected and the interface is not a FEX interface. The fexId property is only used when the port selector is associated with an infraFexBndlGrp managed object.

Related Documentation

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

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

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

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

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

- Verified Scalability

- Cisco ACI Simulator Release Notes

- Cisco NX-OS Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches

- Cisco Application Policy Infrastructure Controller OpenStack and Container Plugins Release Notes

- Cisco Application Virtual Switch Release Notes

New Documentation

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

- *Cisco ACI and SDWAN Integration*

- *Cisco ACI Configuration Files: Import and Export*

- *Cisco ACI Virtual Edge Configuration Guide, Release 2.1(1)*

- *Cisco ACI Virtual Edge Installation Guide, Release 2.1(1)*

- *Cisco ACI Virtual Edge Release Notes, Release 2.1(1)*

- *Cisco ACI Virtual Pod Getting Started Guide, Release 4.1(1)*

- *Cisco ACI Virtual Pod Installation Guide, Release 4.1(1)*

- *Cisco ACI Virtual Pod Release Notes, 4.1(1)*

- *Cisco ACI Virtualization Guide, Release 4.1(1)*

- *Cisco APIC Basic Configuration Guide, Release 4.1(x)*

- *Cisco APIC Getting Started Guide, Release 4.1(x)*

- *Cisco APIC Layer 2 Networking Configuration Guide, Release 4.1(x)*

- *Cisco APIC Layer 3 Networking Configuration Guide, Release 4.1(x)*

- *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.1(x)*

- *Cisco APIC NX-OS Style CLI Command Reference, Release 4.1(1)*

- *Cisco APIC Security Configuration Guide, Release 4.1(x)*

- *Cisco APIC Troubleshooting Guide, Release 4.1(x)*

- *Cisco Application Centric Infrastructure Fundamentals, Release 4.1(x)*

- *Cisco Application Centric Infrastructure Fundamentals, Release 4.1(x)*

- *Cisco Application Virtual Switch Configuration Guide, Release 5.2(1)SV3(3.25)*

- *Cisco Application Virtual Switch Installation Guide, Release 5.2(1)SV3(3.25)*

- *Cisco Application Virtual Switch Release Notes, 5.2(1)SV3(3.25)*

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