Cisco Application Policy Infrastructure Controller Release Notes, Release 2.2(1)

This document describes the features, bugs, and limitations for the Cisco Application Policy Infrastructure Controller (APIC) software.

Note: Use this document in combination with the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.2(1)*, which you can view at the following location:

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

Additional product documentation is listed in the "Related Documentation" section.

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

http://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

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
January 18, 2017	2.2(1n): Release 2.2(1n) became available.
January 19, 2017	2.2(1n): In the New Software Features section, added the limitations for the breakout ports feature and NetFlow feature. Added the Changes in Behavior section with the following information: The Cisco Discovery Protocol (CDP) is now supported in policies that are used on FEX interfaces. In the Usage Guidelines section, removed mention of CDP not being supported in policies that are used on FEX interfaces.
January 23, 2017	2.2(1n): In the Compatibility Information section, added the following bullet: This release supports SCVMM 2016 and Microsoft Hyper-V 2016.

Date	Description
February 14, 2017	In the Compatibility Information section, changed: Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the N9396PX or N9372PX switches To: Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the 10G ports on all other ACI leaf switches Note: A fabric uplink port cannot be used as a FEX fabric port.
February 20, 2017	In the Usage Guidelines section, added: The APICs must have 1 SSD and 2 HDDs, and both RAID volumes must be healthy before upgrading to this release. The APIC will not boot if the SSD is not installed.
February 28, 2017	In the Usage Guidelines section, added: If the communication between the APIC and vCenter is impaired, some functionality is adversely affected. The APIC relies on the pulling of inventory information, updating vDS configuration, and receiving event notifications from the vCenter for performing certain operations.
March 10, 2017	2.2(1o): Release 2.2(1o) became available. Added the resolved bugs for this release.
March 16, 2017	In the New Software Features section, added a link to a YouTube video that highlights some of the new features.
March 29, 2017	2.2(1o): Release 2.2(1o). In the Resolved Bugs section, added bug CSCvb08670.
April 7, 2017	2.2(1o): In the Open Bugs section, added bug CSCvd30648.
April 17, 2017	Removed deprecated Knowledge Base articles.
November 20, 2017	In the Usage Guidelines section, changed a mention of “Virtual Private Cloud (VPC)” to “virtual port channel (vPC).”
December 6, 2017	In the Changes in Behavior section, added the following text: Squelching a fault code with the “Fault Severity Assignment Policies” will now apply to all future and actively-triggered faults of that code.
January 29, 2018	In the Changes in Behavior section, changed: The Cisco Discovery Protocol (CDP) is now supported in policies that are used on FEX interfaces. To: The Cisco Discovery Protocol (CDP) is now supported in policies that are used on FEX interfaces, including interfaces that are configured with vPC.

Date	Description
March 10, 2018	In the Usage Guidelines setion, added the following item: For the contract viewer app, the total contracts and filters configured for endpoint groups per tenant should not be more than 100.
November 21, 2018	2.2(1n): In the Open Bugs section, added bug CSCvn15374.
September 17, 2019	2.2(1n): In the Open Bugs section, added bug CSCuu17314 and CSCve84297.
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.

Contents

This document includes the following sections:

Introduction

The Cisco Application Centric Infrastructure (ACI) is an architecture that allows the application to define the networking requirements in a programmatic way. This architecture simplifies, optimizes, and accelerates the entire application deployment life cycle.

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.

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-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)

The following list includes general compatibility information:

- This release supports the hardware and software listed on the *ACI Ecosystem Compatibility List* document and the software listed as follows:
  - Cisco NX-OS Release 12.2(1)
  - Cisco AVS, Release 5.2(1)SV3(2.14)

    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:

    http://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: see the *ACI Ecosystem Compatibility List* document at the following URL:

    https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/solution-overview-listing.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 ACI leaf switches
  - Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the 10G ports on all other ACI leaf switches

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

- Connecting the Cisco APIC (the controller cluster) to the Cisco ACI fabric requires a 10G interface on the Cisco ACI leaf. You cannot connect the Cisco APIC directly to the N9332PQ Cisco ACI Leaf.
- This release supports the following firmware:
  - 2.0(3i) CIMC HUU iso
  - 2.0(9c) CIMC HUU iso
  - 2.0(13i) CIMC HUU iso (recommended)
- Beginning with Cisco Application Virtual Switch (AVS) release 5.2(1)SV3(1.10), you can connect service virtual machines that are part of Layer 4 to Layer 7 service graphs to AVS. Layer 4 to Layer 7 service graphs for Cisco AVS can be configured for service virtual machines that are in VLAN mode. By using using an AVS VMM domain with both VLAN and VXLAN, you can have a virtual machine in VXLAN mode that is protected by service graphs that are using the service virtual machine in VLAN mode.
- This release supports VMM Integration and VMware Distributed Virtual Switch (DVS) 6.0.x. 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 2.2(1)* at the following URL:

  http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html
- This release supports the Microsoft System Center Virtual Machine Manager (SCVMM) Update Rollup 9 and 10 releases, and the Microsoft Windows Azure Pack Update Rollup 9 and 10 releases.
- This release supports SCVMM 2016 and Microsoft Hyper-V 2016.
- This release supports the partner packages specified in the *L4-L7 Compatibility List Solution Overview* document at the following URL:

  http://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/solution-overview-listing.html
- 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 (ASAv) version that is prior to version 9.3(2), you must configure SSL encryption as follows:

  (config)# ssl encryption aes128-sha1
- A known issue exists with the Safari browser and unsigned certificates, which applies when connecting to the APIC GUI. For more information, see the *Cisco APIC Getting Started Guide*.
- For information about Cisco APIC compatibility with UCS Director, see the appropriate *Cisco UCS Director Compatibility Matrix* document at the following URL:

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

Usage Guidelines

This section lists usage guidelines for the Cisco APIC software.

- The Cisco APIC GUI includes an online version of the Quick Start guide that includes video demonstrations.
- The infrastructure IP address range must not overlap with other IP addresses used in the fabric for in-band and out-of-band networks.
- The Cisco APIC does not provide IPAM services for tenant workloads.
- To reach the Cisco APIC CLI from the GUI: select System > Controllers, highlight a controller, right-click and select "launch SSH". To get the list of commands, press the escape key twice.
- In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.
- For the following services, use a DNS-based host name 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
- Both leaf and spine switches can be managed from any host that has IP connectivity to the fabric.
- 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.
- 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 and 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 Fundamentals Guide* and the *KB: Creating Domains, Attach Entity Profiles, and VLANs to Deploy an EPG on a Specific Port* article.

  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 will raise a fault on the EPG stating “invalid path configuration.”
- An EPG can only associate with a contract interface in its own tenant.
- 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

- The power consumption statistics are not shown on leaf node slot 1. You must view the statistics from any other node.
- For Layer 3 external networks created through the API or Advanced GUI and updated through the CLI, protocols need to be enabled globally on the external network through the API or Advanced GUI, and the node profile for all the participating nodes needs to be added through the API or Advanced GUI before doing any further updates through the CLI.
- For Layer 3 external networks created through the Basic GUI or CLI, you should not to update them through the API. These external networks are identified by names starting with “__ui_”.
- The output from "show" commands issued in the NX-OS-style CLI are subject to change in future software releases. Cisco does not recommend using the output from the show commands for automation.
- The CLI is supported only for users with administrative login privileges.
- 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 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 along with the actrl rule, but a vzAny contract does not have an actrl rule. Therefore, the DSCP value cannot be sent.
- When creating a vPC domain between two leaf switches, both switches must be in the same switch generation. Switches not in the same generation are not compatible vPC peers. The generations are as follows:
  - Generation 1—Cisco Nexus N9000K switches without “EX” on the end of the switch name; for example, N9K-9312TX
  - Generation 2—Cisco Nexus N9K switches with “EX” on the end of the switch model name; for example, N9K-93108TC-EX
- Cisco ACI does not support a class E address as a VTEP address.
- In a multipod fabric, if a spine 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.

- 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 ACI fabric, including the leaf switches and spine switches, to the latest APIC release.
- The APICs must have 1 SSD and 2 HDDs, and both RAID volumes must be healthy before upgrading to this release. The APIC will not boot if the SSD is not installed.
- If the communication between the APIC and vCenter is impaired, some functionality is adversely affected. The APIC relies on the pulling of inventory information, updating vDS configuration, and receiving event notifications from the vCenter for performing certain operations.
- For the contract viewer app, the total contracts and filters configured for endpoint groups per tenant should not be more than 100.
- 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.

Verified Scalability Limits

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:

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

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 video on the Cisco ACI YouTube channel highlights some of the new software features in this release:

https://youtu.be/_gOC5eaXamQ

Table 2 lists all of the new software features in this release:

Table 2 New Software Features, Guidelines, and Restrictions

Feature	Description	Guidelines and Restrictions
802.1Q Tunnels	You can configure 802.1Q tunnels to enable point-to-multi-point tunneling of Ethernet frames in the fabric, with Quality of Service (QoS) priority settings. For more information, see the *Cisco APIC Layer 2 Networking Configuration Guide*.	For the guidelines and restrictions of this feature, see the *Cisco APIC Layer 2 Networking Configuration Guide*.
Breakout Ports	With this release, you can break out a 40 Gigabit Ethernet (GE) leaf switch port to be connected to 4-10GE-capable (downlink) devices that are connected with Cisco 40-Gigabit to 4X10-Gigabit breakout cables. For more information, see the *Cisco APIC Layer 2 Networking Configuration Guide*.	This feature is supported only on the access facing ports of the N9K-C9332PQ switch.
Cisco ACI App Center	The Cisco ACI App Center allows you to enable the capabilities of the Cisco APIC fully by writing applications that are running on the controller. Using the Cisco ACI App Center, customers, developers, and partners can build applications to simplify, enhance, and visualize their use cases. These applications are hosted and shared at the Cisco ACI App Center and installed in the Cisco APIC. For more information, see the *Cisco ACI App Center Developer Guide*.	None.
HSRP Support	HSRP is a first-hop redundancy protocol (FHRP) that allows a transparent failover of the first-hop IP router. HSRP provides first-hop routing redundancy for IP hosts on Ethernet networks configured with a default router IP	For the guidelines and restrictions of this feature, see the *Cisco APIC Layer 3 Networking Configuration*

Feature	Description	Guidelines and Restrictions
	address. You use HSRP in a group of routers for selecting an active router and a standby router. In a group of routers, the active router is the router that routes packets, and the standby router is the router that takes over when the active router fails or when preset conditions are met. For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide*.	*Guide*.
Cisco APIC High Availability Standby	The high availability functionality for an APIC cluster enables you to operate the APICs in a cluster in an active/standby mode. In an APIC cluster, the designated active APICs share the load and the designated standby APICs can act as an replacement for any of the APICs in an active cluster. For more information, see the *Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*.	An admin user can set up the high availability functionality when the APIC is launched for the first time. We recommend that you have at least 3 active APICs in a cluster, and one or more standby APICs. An admin user must initiate the switch over to replace an active APIC with a standby APIC.
Contract Preferred Groups	Support is added for contract preferred groups that enable greater control of communication between EPGs in a VRF. If most of the EPGs in the VRF should have open communication, but a few should only have limited communication with the other EPGs, you can configure a combination of a contract preferred group and contracts with filters to control communication precisely.	None.
ICMP and UDP Flow Logging for Distributed Firewall	Beginning with Cisco AVS release 5.2(1)SV3(2.8), Cisco AVS monitors ICMP and UDP flows as well as TCP flows by default when you enable Distributed Firewall. However, Cisco AVS does not deny ICMP and UDP flows as it does TCP flows. For more information, see the Distributed Firewall section of the Cisco AVS chapter of the *Cisco ACI Virtualization Guide, Release 2.2(1)* and the *Cisco AVS Troubleshooting Guide*.	None.
NetFlow	The NetFlow technology provides the metering base for a key set of applications, including network traffic accounting, usage-based network billing, network planning, as well as denial of services monitoring, network monitoring, outbound marketing, and data mining for both service providers and enterprise customers. Cisco provides a set of NetFlow applications to collect NetFlow export data, perform data volume reduction, perform post-processing, and provide end-user applications with easy access to NetFlow data. If you have enabled NetFlow	This feature is supported only on EX switches. For additional limitations, see the *Cisco APIC and NetFlow* document.

Feature	Description	Guidelines and Restrictions
	monitoring of the traffic flowing through your datacenters, this feature enables you to perform the same level of monitoring of the traffic flowing through the Cisco ACI fabric. For more information, see the *Cisco ACI Virtualization Guide, Release 2.2(1)*.	
RBAC Change Remote User Role	Remote users can now request a role change. For more information see, *Cisco ACI AAA RBAC Rules and Privileges* document.	None.
Support for FCoE Configuration over FEX Ports	You can now configure FCoE over FEX ports. For more information, see the *Cisco APIC Basic Configuration Guide, Release 2.2(1)*.	None.

New Hardware Features

For new hardware features, see the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.2(1)* at the following location:

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

Changes in Behavior

This section lists changes in behavior in this release.

- The Cisco Discovery Protocol (CDP) is now supported in policies that are used on FEX interfaces, including interfaces that are configured with vPC.
- Squelching a fault code with the “Fault Severity Assignment Policies” will now apply to all future and actively-triggered faults of that code.

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 2.2(1) releases in which the bug exists. A bug might also exist in releases other than the 2.2(1) releases.

Table 3 Open Bugs in the 2.2(1) Release

Bug ID	Description	Exists in
CSCvd30648	When configuring route leaking between VRFs, traffic between a shared L3Out and a VzAny consumer might be dropped.	2.2(1o) and later
CSCuu17314	CDP is not enabled on the management interfaces for the leaf switches and spine switches.	2.2(1n) and later
CSCvb93559	If the primary RADIUS server is slow in response, the APIC does not switch to the secondary RADIUS server. This can result in authentication failures. The switch to the secondary RADIUS server happens only when the primary server is dead.	2.2(1n) and later
CSCvc15521	In the case of an AVS domain containing only VxLAN EPGs, an associated VLAN pool cannot be deleted. The VLAN pool can be deleted by removing all EPG to VMM domain associations.	2.2(1n) and later
CSCvc29147	If the microsegmentation EPG has the default resolution immediacy as "immediate" when it is attached to a VMM domain, when the resolution immediacy is changed to "on demand" as soon as it is attached to the VMM domain, the EPG gets removed from the TOR switch. This can lead to loss of connectivity for the VMs for up to 60 seconds.	2.2(1n) and later
CSCvd30648	When configuring route leaking between VRFs, traffic between a shared L3Out and a VzAny consumer might be dropped.	2.2(1n) and later
CSCvd43548	The stats for a given leaf switch rule cannot be viewed if a rule is double-clicked.	2.2(1n) 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.	2.2(1n) and later

Bug ID	Description	Exists in
CSCve84297	A service cannot be reached by using the APIC out-of-band management that exists within the 172.17.0.0/16 subnet.	2.2(1n) and later
CSCvn15374	When upgrading Cisco APICs, constant heartbeat loss is seen, which causes the Cisco APICs to lose connectivity between one another. In the Cisco APIC appliance_director logs, the following message is seen several hundred times during the upgrade: appliance_director||DBG4||...||Lost heartbeat from appliance id= ... appliance_director||DBG4||...||Appliance has become unavailable id= ... On the switches, each process (such as policy-element) see rapidly changing leader elections and minority states: adrs_rv||DBG4||||Updated leader election on replica=(6,26,1)	2.2(1n) 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	2.2(1n) and later

Resolved Bugs

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

Table 4 Resolved Bugs in the 2.2(1) Release

Bug ID	Description	Fixed in

Bug ID	Description	Fixed in
CSCvb22898	When using the Advanced Encryption Standard (AES) encryption in the CLI, the passphrase displays in plain text.	2.2(1n)
CSCvb35030	After upgrading to the 2.1(1) release from the 2.0(1) release, one IP of a vPC goes down. The IP comes back up due to a modify process, such as incrementing the IP on one leg and submitting, or due to deleting or adding the configuration on the logical interface profile of the L3Out.	2.2(1n)
CSCvb35148	A fault gets raised when configuring PIM with SVI, and the fault does not get cleared even after removing the interface from SVI.	2.2(1n)
CSCvb46199	There are downgrade issues from the 2.1(1) release to the 2.0(2) release when the VMM and EPG are in different encapsulations.	2.2(1n)
CSCvb46199	There are downgrade issues when a VMM and the EPGs are in a different encapsulation.	2.2(1n)
CSCvb49441	Adding an image to the repository fails intermittently, regardless if the image was added by downloading it using the GUI or API, or uploading it using the GUI or API.	2.2(1n)
CSCvb51008	In the Edit VMM Domain Association dialog box, changing the VLAN mode and then clicking Cancel does not undo the VLAN mode change.	2.2(1n)
CSCvb08670	Node ID added to Cisco APIC cluster might get a duplicate fabric address. This issue can be triggered by a reload of a leaf, spine, or vleaf. Note: See the workaround in the Bug Search Tool before upgrading to 2.2(1o).	2.2(1o)

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 2.2(1) releases in which the known behavior exists. A bug might also exist in releases other than the 2.2(1) releases.

Table 7 Known Behaviors in the 2.2(1) Release

Bug ID	Description	Exists in
CSCuo52668	The Cisco APIC does not validate duplicate IP addresses that are assigned to two device clusters. The communication to devices or the configuration of service devices might be affected.	2.2(1n) and later
CSCuo79243	In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.	2.2(1n) and later
CSCuo79250	The node ID policy can be replicated from an old appliance that is decommissioned when it joins a cluster.	2.2(1n) and later
CSCup47703	The DSCP value specified on an external endpoint group does not take effect on the filter rules on the leaf switch.	2.2(1n) and later

Bug ID	Description	Exists in
CSCup79002	The hostname resolution of the syslog server fails on leaf and spine switches over in-band connectivity.	2.2(1n) and later
CSCuq21360	Following a FEX or switch reload, configured interface tags are no longer configured correctly.	2.2(1n) and later
CSCur39124	Switches can be downgraded to a 1.0(1x) version if the imported configuration consists of a firmware policy with a desired version set to 1.0(1x).	2.2(1n) and later
CSCur71082	If the Cisco APIC is rebooted using the CIMC power reboot, the system enters into fsck due to a corrupted disk.	2.2(1n) and later
CSCus15627	The Cisco APIC Service (ApicVMMService) shows as stopped in the Microsoft Service Manager (services.msc in control panel > admin tools > services). This happens when a domain account does not have the correct privilege in the domain to restart the service automatically.	2.2(1n) and later
CSCut51929	The traffic destined to a shared service provider endpoint group picks an incorrect class ID (PcTag) and gets dropped.	2.2(1n) and later
CSCuu09236	Traffic from an external Layer 3 network is allowed when configured as part of a vzAny (a collection of endpoint groups within a context) consumer.	2.2(1n) and later
CSCuu61998	Newly added microsegment EPG configurations must be removed before downgrading to a software release that does not support it.	2.2(1n) and later
CSCuu64219	Downgrading the fabric starting with the leaf switch will cause faults such as policy-deployment-failed with fault code F1371.	2.2(1n) and later
CSCva32534	Creating or deleting a fabricSetupP policy results in an inconsistent state.	2.2(1n) and later
CSCva60439	After a pod is created and nodes are added in the pod, deleting the pod results in stale entries from the pod that are active in the fabric. This occurs because the Cisco APIC uses open source DHCP, which creates some resources that the Cisco APIC cannot delete when a pod is deleted.	2.2(1n) and later
CSCva86794	When a Cisco APIC cluster is upgrading, the Cisco APIC cluster might enter the minority status if there are any connectivity issues. In this case, user logins can fail until the majority of the Cisco APICs finish the upgrade and the cluster comes out of minority.	2.2(1n) and later
CSCva97082	When downgrading from a 2.2(1) release to a 2.0(1) release, the spines and its interfaces must be moved from infra L3out2 to infra L3out1. After infra L3out1 comes up, delete L3out2 and its related configuration, and then downgrade to a 2.0(1) release.	2.2(1n) and later
CSCvb39702	No fault gets raised upon using the same encapsulation VLAN in a copy device in tenant common, even though a fault should get raised.	2.2(1n) and later
CSCvb52882	Modifying DNS settings for the APIC does not update the DN settings inside the container for a stateful app.	2.2(1n) and later

- 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*.

Related Documentation

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

http://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 tables describe the core APIC documentation.

Note: Not every document has a new version for each release. Unless specified otherwise, the latest document version applies if the document was not revised for a specific release.

Table 8 Release Notes

Document	Description
Cisco ACI Simulator Release Notes, Release 2.2(1)	Provides release information for the Cisco ACI Simulator product.
Cisco Application Policy Infrastructure Controller, Release 2.2(1), Release Notes	This document. Provides release information for the Application Policy Infrastructure Controller (APIC) product.
Cisco Nexus 9000 Series ACI-Mode Switch FPGA/EPLD Upgrade Release Notes, Release 12.2(1)	Provides release information for the Cisco Nexus 9000 series ACI-mode switch FPGA/EPLD product.
Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.2(1)	Provides release information for the Cisco NX-OS for Cisco Nexus 9000 series ACI-mode switches product.

Table 9 Installation, Upgrade, and Configuration Documentation

Document	Description
Cisco APIC Basic Configuration Guide	Describes steps that you must perform to configure your ACI fabric.
Cisco APIC Getting Started Guide	Describes the first things that you must do to use the APIC after you install the APIC software.
Cisco Nexus 93108TC-EX ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 93180YC-EX ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9332PQ ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.

Document	Description
Cisco Nexus 9336PQ ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9372PX ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9372TX and 9372-TX-E ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9396PX ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9396TX ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9504 ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9508 ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9516 ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 93180LC-EX ACI Mode Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco APIC Management, Installation, Upgrade, and Downgrade Guide	Describes how to upgrade or downgrade the APIC controller's appliance firmware and how to install the APIC software. This document also describes any limitations when upgrading or downgrading.
Minimum and Recommended Cisco ACI and APIC Releases	Lists the minimum and recommended ACI and APIC software releases for both new and existing deployments.
Operating Cisco Application Centric Infrastructure	Describes how to perform day-to-day operations with the ACI.
Verified Scalability Guide for Cisco ACI and Cisco Nexus 9000 Series ACI-Mode Switches	Describes the maximum verified scalability limits for ACI parameters for the Cisco ACI and Cisco Nexus 9000 Series ACI-Mode Switches.

Table 10 Interface Documentation

Document	Description
Cisco APIC NX-OS Style Command-Line Interface Configuration Guide	Describes how to configure the APIC using the NX-OS-style CLI.
Cisco APIC REST API User Guide	Describes how to use the APIC REST APIs.

Table 11 Reference Documentation

Document	Description
Cisco Application Centric Infrastructure Fundamentals	Provides a basic understanding of the capabilities of the ACI and APIC.

Table 12 Layer 4 to Layer 7 Documentation

Document	Description
Cisco APIC Layer 4 to Layer 7 Device Package Development Guide	Describes how to develop a device package for the Layer 4 to Layer 7 services.
Cisco APIC Layer 4 to Layer 7 Service Graph Deployment Guide	Describes how to deploy a Layer 4 to Layer 7 service graph in greater detail than the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide* with common use cases.
Cisco APIC Layer 4 to Layer 7 Services Deployment Guide	Describes how to deploy the Layer 4 to Layer 7 services using the APIC.

Table 13 Virtualization Documentation

Document	Description
Cisco ACI Virtualization Guide	Describes how to deploy ACI with virtualization solutions, such as Cisco AVS, VMware VDS, or Microsoft SCVMM.

Table 5 ACI with OpenStack Documentation

Document	Description
Cisco ACI Installation Guide for Mirantis OpenStack	Describes how to install the plugin that allows you to use Mirantis OpenStack with ACI.
Cisco ACI with OpenStack OpFlex Deployment Guide for Red Hat	Describes how to deploy ACI with OpenStack OpFlex on the Red Hat platform.
Cisco ACI with OpenStack OpFlex Deployment Guide for Ubuntu	Describes how to deploy ACI with OpenStack OpFlex on the Ubuntu platform.
Installing the Cisco APIC OpenStack Driver	Describes how to install the APIC OpenStack driver.
OpenStack Group-Based Policy User Guide	Describes how to use group-based policies.

Table 15 Troubleshooting Documentation

Document	Description
Cisco APIC Troubleshooting Guide	Describes how to troubleshoot common APIC issues.

Document	Description
Troubleshooting Cisco Application Centric Infrastructure	Additional information about how to troubleshoot common APIC issues.

New Documentation

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

- *Cisco ACI Virtualization Guide, Release 2.2(1)*
- *Cisco APIC and NetFlow*
- *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 2.2(1)*
- *Cisco APIC NX-OS Style CLI Command Reference, Release 2.2(1)*
- *Cisco APIC Redundancy*
- *Cisco APIC REST API Configuration Guide*
- *Cisco App Center Developer Guide*
- *Cisco App Center User Guide*
- *Cisco Nexus 93180LC-EX ACI Mode Hardware Installation Guide*
- *Verified Scalability Guide for Cisco ACI, Release 2.2(1) and Cisco Nexus 9000 Series ACI-Mode Switches, Release 12.2(1)*