Cisco Application Policy Infrastructure Controller Release Notes, Release 2.2(4)

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(4)*, 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

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:

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

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
April 6, 2018	2.2(4f): Release 2.2(4f) became available.
May 18, 2018	2.2(4p): Release 2.2(4p) became available. Added the resolved bugs for this release.
June 18, 2018	In the Compatibility Information section, changed: 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(4) at the following URL: To: This release supports VMM Integration and VMware Distributed Virtual Switch (DVS) 6.5. 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(2) (this document also applies to the 2.2(4) release) at the following URL:
July 2, 2018	2.2(4q): Release 2.2(4q) became available; there are no changes to this document for this release.
August 7, 2018	2.2(4r): Release 2.2(4r) became available. Added the resolved bugs for this release.

Date	Description
August 30, 2018	2.2(4f): In the Resolved Bugs section, added bug CSCvf98482.
November 21, 2018	2.2(4f): In the Open Bugs section, added bug CSCvn15374.
September 17, 2019	2.2(4f): 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 *Ciscof 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(4)
  - Cisco AVS, Release 5.2(1)SV3(3.4)

  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

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 APIC (the controller cluster) to the ACI fabric requires a 10G interface on the ACI leaf switch. You cannot connect the APIC directly to the N9332PQ ACI leaf switch, unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the N9332PQ switch will auto-negotiate to 10G without requiring any manual configuration.
- 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)
- 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
- 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 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) 6.5. 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(2)* (this document also applies to the 2.2(4) release) 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
- This release supports the Microsoft System Center Virtual Machine Manager (SCVMM) Update Rollup 9, 10, and 11 releases, and the Microsoft Windows Azure Pack Update Rollup 9, 10, and 11 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:

  https://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:

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

- Beginning with this release, contracts using matchDscp filters are only supported on switches with “EX” on the end of the switch name. For example, N9K-93108TC-EX.
- When downgrading from Cisco APIC 2.2(4) to an older release, if you need to delete the Virtual Port Channel (VPC), upgrade to Cisco APIC 2.2(4), delete the VPC, and downgrade again.

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 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 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 do not 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 switch 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 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.
- 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.
- 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 will be able to discover and join the fabric.
- 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.
- 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 APIC automatically creates a default monitoring policy and enables common observables. You can modify the default policy under tenant common based on the requirements of your fabric.
- 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.
- If you are upgrading VMware vCenter 6.0 to vCenter 6.5, 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

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. You must enter any changes in the APIC configuration again after restarting VMware vCenter.

- 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.
- 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.
- Limiting, Disabling, or Checking IP Learning: in Cisco APIC, you can configure the following options related to IP learning:

IP Learning Option	Location	Application
Limit IP Learning to Subnet	Tenants > tenant-name > Navigation > Bridge Domain > Bridge Domain name > Subnets > Create Subnet	When this option is enabled, IP address learning is limited to the bridge domain subnets only. Every bridge domain can have multiple subnets associated with it. By default, all IP addresses are learned.
Enforce Subnet Check	Fabric > Access Policies > Global Policies > Fabric Wide Setting Policy > Enforce Subnet Check	Fabric wide, this applies to all leaf switches. When this knob is enabled, it effectively turns on subnet check on every Bridge Domain, regardless of the setting “Limit IP learning to Subnet” on each Bridge Domain.
Disable Remote EP Learn	Fabric > Access Policies > Global Policies > Fabric Wide Setting Policy > Disable Remote EP Learn	Fabric wide, this applies only on border leaf switches with at least one external bridge domain programmed.

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:

https://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

There are no new software features in this release.

New Hardware Features

For new hardware features, see the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.2(4)* at the following location:

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

Bugs

This section contains lists of open and resolved bugs and 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(4) releases in which the bug exists. A bug might also exist in releases other than the 2.2(3) releases.

Table 2 Open Bugs in the 2.2(4) Release

Bug ID	Description	Exists in
CSCuu17314	CDP is not enabled on the management interfaces for the leaf switches and spine switches.	2.2(4f) 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(4f) and later
CSCvd33553	The Cisco APIC does not enforce the maximum disk limit used for the logs from a stateful application. If a stateful application is generating a large amount of logs, it can cause the Cisco APIC disk to get filled.	2.2(4f) and later

Bug ID	Description	Exists in
CSCvd43548	The stats for a given leaf switch rule cannot be viewed if a rule is double-clicked.	2.2(4f) 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(4f) and later
CSCvd74345	Using route peering with virtual devices in Layer 4 to Layer 7 service graphs causes the following fault to be raised: failed to attach/detach port groups to the Firewall VM	2.2(4f) and later
CSCvd82348	This issue applies to environments that are using the policy-based redirect feature for a Layer 4 to Layer 7 service graph. If the destination IP address for a service node is specified as the network IP address or the broadcast IP address, traffic is dropped.	2.2(4f) 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.	2.2(4f) and later
CSCvf70362	This enhancement is to change the name of "Limit IP Learning To Subnet" under the bridge domains to be more self-explanatory. Original : Limit IP Learning To Subnet: [check box] Suggestion : Limit Local IP Learning To BD/EPG Subnet(s): [check box]	2.2(4f) and later
CSCvi33259	Attempting to downgrade from a 2.3(1) release to the 2.2(4) release fails with the following error message: firmware not compatible	2.2(4f) and later
CSCvi82903	When authenticating with the Cisco APIC using ISE (TACACS), all logins over 31 characters fail.	2.2(4f) 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(4f) and later

Bug ID	Description	Exists in
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(4f) and later
CSCvr65035	The last APIC in the cluster gets rebooted when APIC-1 is decommissioned due to some issue seen on APIC-1 while upgrading. In addition, after decommissioning APIC-1, the other APICs still wait for APIC-1 to get upgraded.	2.2(4f) 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 3 Resolved Bugs in the 2.2(4) Release

Bug ID	Description	Fixed in
CSCuz67203	After upgrading, the AVS OpFlex channel stays in the disconnected state.	2.2(4f)
CSCvd75131	In a multipod setup when a spine switch is rebooted, traffic should not flow through the switch for 10 minutes after its routing protocol adjacencies come up. This is achieved by advertising a high metric into OSPF and IS-IS for 10 minutes. This works fine for OSPF, but not for IS-IS. The problem is that within the Cisco APIC, the default metric for routes redistributed into IS-IS (such as the remote POD tep pool) is 63. This is also the max-metric that can be set for redistributed routes into IS-IS in Cisco APIC. So when the spine that was just rebooted comes back up, it cannot advertise a worse metric than the default, which causes all of the leaf switches immediately to install the switch as an ECMP path for the route even though things such as COOP might not have converged yet. If traffic is hashed to this ECMP path, there could be traffic loss for several seconds.	2.2(4f)
CSCvd84590	The do_boot_cpu() process of a Cisco APIC server fails at GRUB when starting to boot the kernel.	2.2(4f)

Bug ID	Description	Fixed in
CSCvd98498	The fault code "F607564" is seen on the Cisco APICs after fabric recovery. This fault is seen after downgrading and upgrading the Cisco APIC.	2.2(4f)
CSCve34392	The tracking of VM and NiC information for an endpoint is incorrect. The managed objects fvRsToVm and fvRsToVm are missing for some fvEpDefRef managed objects.	2.2(4f)
CSCve52382	Tracking of VM and NiC information for an end point is incorrect. The managed objects fvRsToVm and fvRsToVm are missing for some fvEpDefRef managed objects.	2.2(4f)
CSCve81037	Tracking of VM and NiC information for an endpoint is incorrect. The managed objects fvRsToVm and fvRsToVm are missing for some fvEpDefRef managed objects.	2.2(4f)
CSCve92142	A filter points to the concrete object of another filter. As the result, an incorrect ACL entry will be installed on leaf switches or open virtual switches.	2.2(4f)
CSCvf09659	There is a delay in bringing up the DV ports when provisioning or powering up a large number of virtual machines, such as in a VDI environment. On the Cisco APIC, a fault reports that a Cisco AVS port is blocked and the Cisco AVS is waiting for an ACK packet from the leaf switch.	2.2(4f)
CSCvf12024	A leaf switch decommissioned from the fabric never reappears in the fabric membership window.	2.2(4f)
CSCvf15683	A Csico APIC unexpectedly reloads. The output from "show cores" indicates the kernel crashed and produced a vmcore.	2.2(4f)
CSCvf16377	If Sched A is associated with a fabric node firmware MaintPol, then if that MaintPol is deleted, Sched A is also deleted. The behavior above occurs even if Sched A is also associated with other policies, such as the Config Export Policy and the Techsupport Export Policy. Because Sched A is deleted, the config export policy and techsupport export policy using Sched A will have the fault "Failed to form relation to MO schedp-[sched_name] of class trigSchedP in context."	2.2(4f)
CSCvf35265	The system controller's status is "standby" after reloading.	2.2(4f)
CSCvf60077	Fault F1300 gets raised. This fault contains the following message: A Fabric Node Group (fabricNodeGrp) configuration was not deployed on the fabric node ### because: Node Not Registered for Node Group Policies	2.2(4f)
CSCvf66682	There is a global station table stale entry.	2.2(4f)
CSCvf91599	A service object group cannot be created or edited from the Cisco APIC GUI when importing an XML configuration from one data center to another. The parameter "service object group" is missing and previously configured object groups cannot be added or edited.	2.2(4f)
CSCvf98482	One or more controller in the Cisco APIC cluster may be seen in the data-layer-partially-diverged state. Many dbgr shards may be found with no leaders or non-optimal leaders. The process dbgr might crash repeatedly.	2.2(4f)

Bug ID	Description	Fixed in
CSCvg00499	LLDP adjacency to looseNode objects is up, but the VLANs are not programmed on the ports. Run the following command in the leaf switch's CLI to see that there is no leqptRsLsNodeToIf object for the interface: moquery -c leqptRsLsNodeToIf	2.2(4f)
CSCvg10823	Cisco Nexus 9000 Series Fabric Switches - ACI mode includes a version of GLIBC that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2017-1000366 This bug was opened to address the potential impact on this product.	2.2(4f)
CSCvg15128	Performing a pre-upgrade copy from APIC1 to APIC3 fails due to the SSH connection failing.	2.2(4f)
CSCvg24076	/data/log is 100% full due to multiple 21M log files.	2.2(4f)
CSCvg32919	One or more Cisco APICs are in a Data Layer Partially Diverged state. Running "show cores" on a Cisco APIC shows core files for the svc_ifc_observer process. Running "ps -ef | grep observer" shows that there is no svc_ifc_observer process running.	2.2(4f)
CSCvg33397	A standby Cisco APIC fails to replace an active Cisco APIC.	2.2(4f)
CSCvg48627	The Cisco APIC GUI allows users to configure an Out-of-Band Contract with a Directive of Logging when this is not supported, which can lead to the following programming fault being generated: actrl-provisioning-failed rule failed due to software programming error	2.2(4f)
CSCvg60902	The VMMMgr process crashes shortly after being started. The VMMMgr logs show the following error right before the crash: UNCONDITIONAL ASSERT () (lHpNicMo != __null) failed @ ../svc/vmmmgr/src/gen/ifc/app/./imp/comp/TaskCompHpNicAddorDelVtepNicImp.cc:126	2.2(4f)
CSCvg68942	If a Q-in-Q tunnel configuration is removed incorrectly with a missing CDP interface policy on the leaf switch, it can result in multiple policyelem cores causing the leaf switches to go into an inactive state and continuously reload. Because the leaf switches continuously reload, the Cisco APIC cannot keep track of all of the objects. Because of this, there stale objects remain on those leaf switches. Leaf switch profiles become missing, which causes the CDP interface policy to be missing on the leaf switches. Therefore, the relation between the interface to the CDP interface policy is "unformed" and crashes the switches.	2.2(4f)
CSCvg95130	Connectivity from all VMs needing to go through the fabric is lost. The Hyper-V agent logs might show information indicating that it is still trying to connect to the old TEP IP address (pre-replacement) as opposed to the new one (post-replacement).	2.2(4f)
CSCvg96793	All ESXi hosts show as disconnected under the VMM Integration when you click on the VMM domain. The VMware vCenter might still show as online. The svc_ifc_opflexelem.log file for the leaf switches will show DVS as not found.	2.2(4f)
CSCvh11314	There are inventory sync failure faults and various VMM faults for the affected VMM domain.	2.2(4f)

Bug ID	Description	Fixed in
CSCvh16532	When attempting to log into the Cisco APIC GUI, you might receive the error "AAA Server Authentication DENIED." You might also see the following message in a network trace when the LDAP server responds to the Cisco APIC's search query: "In order to perform this operation a successful bind must be completed."	2.2(4f)
CSCvh16963	The admin user in fallback and other local authentication domains is placed in the bashusers cgroup. This could result in the user being locked out of the Cisco APIC or being unable to execute commands if /tmp and other tmpfs directories are being utilized.	2.2(4f)
CSCvh17864	The STP policy does not change or has mixed behavior after switching to another policy or reverting to the default policy.	2.2(4f)
CSCvh25010	When the infraAccNodePGrp managed object is disassociated from a leaf switch, the uni/fabric/monfab-default policy replaces the user-configured fabric monitoring policy on the leaf switch.	2.2(4f)
CSCvh51665	Fault F1313 is triggered for a VMNIC on a Cisco AVS-integrated hypervisor. The fault states the following error in the fault description: [API call for adding VNic failed.]	2.2(4f)
CSCvh52433	1G ports on APIC-SIM-S2 do not come up.	2.2(4f)
CSCvh68033	Leaf switches will continuously see a crash due to the vleaf_elem process.	2.2(4f)
CSCvh73078	After changing the BGP Route Reflector AS number, no routes are redistributed from the border leaf switches to the non-border leaf switches for certain VRF instances. If the BGP Route Reflector AS number is switched back to the original, then all routes are redistributed correctly.	2.2(4f)
CSCvh69798	The vmmmgr process stops logging to the "svc_ifc_vmmmgr.bin.log" file in some situations.	2.2(4p)
CSCvi75240	Duplicate Address Detection (DAD) disables the secondary IPv6 address if the user configures a shared IPv6 address on a Layer 3 SVI.	2.2(4p)
CSCvi77600	A crash occurs during the retrieval of vSphere tag information from VMware vCenter.	2.2(4p)
CSCvi86103	There are duplicate PVLAN entries in VMware vCenter. Depending on the version of Cisco APIC code, the Cisco APIC's vmmmgr process will also crash and create a core file.	2.2(4p)
CSCvj90443	A vPC is assigned a duplicate vIP address, resulting in traffic loss.	2.2(4r)

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(4) releases in which the known behavior exists. A bug might also exist in releases other than the 2.2(4) releases.

Table 4 Known Behaviors in the 2.2(4) 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(4f) and later
CSCuo79243	In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.	2.2(4f) and later
CSCuo79250	The node ID policy can be replicated from an old appliance that is decommissioned when it joins a cluster.	2.2(4f) 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(4f) and later
CSCup79002	The hostname resolution of the syslog server fails on leaf and spine switches over in-band connectivity.	2.2(4f) and later
CSCuq21360	Following a FEX or switch reload, configured interface tags are no longer configured correctly.	2.2(4f) 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(4f) 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(4f) 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(4f) and later
CSCut51929	The traffic destined to a shared service provider endpoint group picks an incorrect class ID (PcTag) and gets dropped.	2.2(4f) 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(4f) and later
CSCuu61998	Newly added microsegment EPG configurations must be removed before downgrading to a software release that does not support it.	2.2(4f) 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(4f) and later
CSCuu84328	In a NIC teaming topology that is connected to different leaf switches that are not in a Virtual Port Channel, an endpoint group is deployed only on the leaf switch where an endpoint is learned. The vPC must be configured on the leaf switch side for interfaces connected to NIC-teamed interfaces of the hypervisors.	2.2(4f) and later
CSCuw34026	If the " Remove related objects of Graph Template" wizard is used in the Cisco APIC GUI, the Cisco APIC does not clean up objects that are in other tenants.	2.2(4f) and later
CSCva32534	Creating or deleting a fabricSetupP policy results in an inconsistent state.	2.2(4f) and later

Bug ID	Description	Exists in
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(4f) 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(4f) and later
CSCva97082	When downgrading from a 2.2(2e) 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(4f) 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(4f) and later
CSCvb52882	Modifying DNS settings for the APIC does not update the DN settings inside the container for a stateful app.	2.2(4f) and later
CSCvd20382	The Cisco APIC does not allow the underscore (or " _ ") symbol in the hostname as a valid character.	2.2(4f) 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:

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