Cisco Application Policy Infrastructure Controller Release Notes, Release 2.2(2)

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(2)*, 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 11, 2017	2.2(2e): Release 2.2(2e) became available.
April 18, 2017	2.2(2e): Moved Known Behavior CSCvd30648 to the Resolved Bugs table.
April 25, 2017	2.2(2f): Release 2.2(2f) became available. Added the resolved bugs for this release.
May 1, 2017	2.2(2g): Release 2.2(2g) became available; there are no changes to this document for this release.
May 5, 2017	2.2(2f): Added CSCvd20382 to Known Behaviors.
May 16, 2017	2.2(2i): Release 2.2(2i) became available. Added the resolved bugs for this release.
June 16, 2017	2.2(2j): Release 2.2(2j) became available; there are no changes to this document for this release.
July 16, 2017	2.2(2k): Release 2.2(2k) became available. Added the resolved bug CSCvf00823 for this release.
July 19, 2017	2.2(2k): Added resolved bug CSCvf14956.

Date	Description
August 12, 2017	2.2(2q): Release 2.2(2q) became available; a new software feature, Enforce Subnet Check Global Knob, added.
November 20, 2017	In the Usage Guidelines section, changed a mention of “Virtual Private Cloud (VPC)” to “virtual port channel (vPC).”
November 29, 2017	In the New Software Features section, added the following new feature: Layer 4 to Layer 7 Service Graph Support for Virtual Appliances on an SCVMM Domain
December 6, 2017	In the New Software Features section, added the following new feature: Fibre Channel over Ethernet support on N9K-C93180YC-FX and N9K-C93108TC-FX switches
January 25, 2018	In the Usage Guidelines section, removed a reference to VMware vCenter 6.5. In the New Software Features section, removed the following table entry: VMware vCenter 6.5 support for VMware VDS and Cisco AVS VMware vCenter 6.5 is not supported in this release.
January 31, 2018	Readded the references to VMware vCenter 6.5 that were removed on January 25, 2018. VMware vCenter 6.5 is now supported.
February 22, 2018	In the New Software Features section, added the following item: Cisco Tetration Analytics support on the Cisco N9K-93180YC-EX, N9K-93108TC-EX, and N9K-93180LC-EX switches
March 30, 2018	In the Compatibility Information section, changed the Cisco AVS release to 5.2(1)SV3(3.2) and the VMM Integration and VMware Distributed Virtual Switch (DVS) release to 6.5.
November 21, 2018	2.2(2e): In the Open Bugs section, added bug CSCvn15374.
September 17, 2019	2.2(2e): In the Open Bugs section, added bug CSCuu17314. 2.2(2i): In the Open Bugs section, added bug 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(2e)
  - Cisco AVS, Release 5.2(1)SV3(3.2)

    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. 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)
- 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) 6.5. 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(2e)* 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

- If you are using virtualization, you must install one of the following Microsoft System Center Virtual Machine Manager (SCVMM) with Administrator Console releases:
  - 2016 RTM (Build 4.0.1662.0) or later
  - 2012 R2 with Update Rollup 9 (Build 3.2.8145.0) or later
- 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(2) to an older release, if you need to delete the Virtual Port Channel (VPC), upgrade to Cisco APIC 2.2(2), 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: Choose System > Controllers, highlight a controller, right-click and choose "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.
- 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.

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

Table 2 lists the new software features in this release:

Table 2 New Software Features, Guidelines, and Restrictions

Feature	Description	Guidelines and Restrictions
Enforce Subnet Check Global Knob	Enabling the Enforce Subnet Check Global knob implicitly enforces subnet check at BD (configured BD subnets) for local IP learns and VRF (configured subnets under VRF) for Remote IP learns. Note: When enabling the knob, the following one-time operations are done in the Cisco ACI fabric:	None.

Feature	Description	Guidelines and Restrictions
	■ Flush all remote IPs in the fabric ■ Flush all IPs outside the BD subnets for local learns	
BGP Timers per Layer 3 Out	BGP timers can be defined and associated on a per VRF per node basis.	None.
Layer 3 Out to Layer 3 Out Inter-VRF Leaking	Shared Layer 3 Outs in different VRFs can communicate with each other using a contract.	None.
Multiple BGP Communities Assigned per Route Prefix	Multiple BGP communities can now be assigned per route prefix using the BGP protocol.	None.
VMware vCenter 6.5 support for VMware VDS and Cisco AVS	Beginning in this APIC release and in Cisco AVS Release 5.3(1)SV3(3.2), VMware VDS and Cisco AVS are supported in VMware vCenter 6.5.	None.
Audit Fault Correlation	Cisco APIC supports the health score evaluation to ignore acknowledged faults, such as those faults that can be safely ignored and prevent the health score from being degraded. You can modify the health score evaluation policy based on the penalty of the health score at the fault severity level. For more information about health score, see the *Cisco Application Centric Infrastructure Best Practices Guide* at the following location: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/ACI_Best_Practices/b_ACI_Best_Practices.html	None.
Simplified Service Graph Integration with Windows Azure Pack	Windows Azure Pack Service Graph Integration-Windows Azure Pack service graph integration enables you to automate the creation of service graph and to deploy services to Windows Azure Pack tenants. This feature also supports NAT integration, which enables tenant VRFs with private subnets to communicate with external networks. For more information, see the *Cisco ACI Virtualization Guide, Release 2.2(1)*. Windows Azure Pack Shared Services across Tenant VRFs-With this feature, tenants are responsible for ensuring that subnets are unique if the subnets are used for shared services across VRFs. If the shared service consumer is in a different VRF than the provider, route leaking between the VRFs automatically occurs to enable	None.

Feature	Description	Guidelines and Restrictions
	the communication. For more information, see the *Cisco ACI Virtualization Guide, Release 2.2(1)*.	
VMware vCenter Plug-in Iupport for Cisco AVS Installation and Upgrade	Beginning with Cisco AVS Release 5.2(1)SV3(3.1), you can install, uninstall, upgrade, and downgrade Cisco AVS using the VMware vCenter plug-in.	None.
ACI App Center	Beginning with Cisco APIC release 2.2(2), five levels of the Hierarchical Data Format (HDF) for API are supported.	None.
Enable/Disable Remote IP Endpoint Learning	With this release, you can enable or disable remote IP endpoint learning on VRFs with at least one interface (external SVI or external Layer 3 interface) and ingress policy enforcement enabled. The scope of this policy is fabric-wide. After configuration, the policy is pushed to each leaf switch as it comes up. Previously learned remote IP endpoints are flushed. Note: Consult with your Technical Support representative before using this configuration option. You should enable this policy in fabrics which include the Cisco Nexus 93128 TX, 9396 PX, or 9396 TX switches with the N9K-M12PQ uplink module, after all the nodes have been successfully upgraded to APIC Release 2.2(2e).When remote IP endpoint learning is disabled, and you make either of the following configuration changes, you may need to manually flush previously learned IP endpoints: ■ You configure the VRF for ingress policy enforcement ■ You add one Layer 3 interface in the VRF To manually flush previously learned IP endpoints, enter the following command on both VPC peers: vsh -c "clear system internal epm endpoint vrf <vrf-name> remote”	None.
Maximum Transmission Unit (MTU)	With this release, you can create a Control Plane (CP) MTU policy that sets the global MTU size for control plane packets sent by the nodes (APIC and the switches) in the	None.

Feature	Description	Guidelines and Restrictions
	fabric. In a multipod topology, the MTU setting for the fabric external ports must be greater than or equal to the CP MTU value set. Otherwise, the fabric external ports might drop the CP MTU packets. If you change the Inter-Pod Network (IPN) or CP MTU, Cisco recommends changing the CP MTU value first, then changing the MTU value on the spine of the remote pod. This reduces the risk of losing connectivity between the pods due to MTU mismatch.	
Layer 4 to Layer 7 Service Graph Support for Virtual Appliances on an SCVMM Domain	During Layer 4 to Layer 7 service graph deployment, a Cisco APIC automatically creates port groups for virtual appliances and updates the vNICs of the virtual appliance. In previous releases, this capability was supported only on a VMware VMM domain. In this release, this capability is also supported on a Microsoft SCVMM domain.	The virtual appliance must be running on a VMware ESXi that uses a Cisco ACI vDS, or that uses a Microsoft Hyper-V with a Cisco ACI logical switch.
Fibre Channel over Ethernet support on N9K-C93180YC-FX and N9K-C93108TC-FX switches	Fibre Channel over Ethernet (FCoE) is now supported on the Cisco Nexus C93180YC-FX and C93108TC-FX switches.	None.
Cisco Tetration Analytics support on the Cisco N9K-93180YC-EX, N9K-93108TC-EX, and N9K-93180LC-EX switches	Cisco Tetration Analytics telemetry is now supported on the following Cisco switches: • Cisco N9K-93180YC-EX • Cisco N9K-93108TC-EX • Cisco N9K-93180LC-EX	None.

New Hardware Features

For new hardware features, see the *Cisco NX-OS Release 12.2(2e) Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches* 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

This section lists changes in behavior in this release.

- You can now view the audit logs from the Troubleshooting tab of a fault.
- The "Layer 3 EVPN Services for Fabric WAN" feature name has been changed to "Cisco ACI GOLF."
- The following changes to NX-OS style CLI commands have occurred between Cisco APIC release 2.0(2f) and this release:
  - The following commands were modified:
    - ldap-server host–Previously the key command was a keyword in the command. For increased security, it is now an interactive sub-command, as shown in the following example:

```
apic1(config)# ldap-server host <dns-name | ip_address>
apic1(config-host)# key
Enter Key:
Enter Key again:
```

    - tacacs-server host–Previously the key command was a keyword in the command. For increased security, it is now an interactive sub-command, as shown in the following example:

```
apic1(config)# tacacs-server host <dns-name | ip_address>
apic1(config-host)# key
Enter Key:
Enter Key again:
```

    - crypto-aes–Previously the passphrase command was a keyword in the command. For increased security, it is now an interactive sub-command, as shown in the following example:

```
apic1(config)# crypto aes
apic1(config-host)# passphrase
Enter passphrase:
Enter passphrase again:
```

    - (crypto-keyring) csr–Previously password was a keyword in the csr command. For increased security, it is now an interactive sub-command, as shown in the following example:

```
apic1(config)# crypto keyring
apic1(config-keyring)# csr
apic1(config-csr)# password
Enter password:
Enter password again:
```

    - [vrf] template route-profile <WORD> <WORD> <NUMBER> – This command in Named L3Out mode has changed to include the required route-control context name and the optional relative number of the route-profile entry. It is not backward compatible. When upgrading to APIC Release 2.2(2x), if your configuration includes Named L3Out configurations with this command, export the configuration, edit this command to add the route-control context name, and import the configuration.
    - [match bridge-domain] inherit route-profile <WORD> <WORD> – This command in Named L3Out mode has changed to include the optional profile name and the required route control context name. It is not backward compatible. When upgrading to APIC Release 2.2(2x), if your configuration includes Named L3Out configurations with this command, export the configuration, edit this command to add the required route-control context name, and import the configuration.
    - [show][cmd] [exec] show acllog deny * –To agree with the feature name (ACL Deny Logs) in the GUI, the command is changed from show acllog drop to show acllog deny.

- [ntp] server <WORD> [prefer] [key <>] [use-vrf <>] – This command was changed to enable configuration replay using the show running-config command. The configuration mode was also changed (see below).

— The following commands were moved out of pod configuration mode to support multipod:

- ntp server–This command is moved into template ntp-fabric configuration mode.
- bgp-fabric–This command is moved into bgp-fabric mode.
- Isis fabric–This command is moved into isis-fabric mode.
- snmp-server protocol enable–This command is moved into snmp-fabric mode.

— The features including the following commands were never released, so the commands were removed from the CLI:

- `endpoint rogue-detect *`
- `[interface] ip igmp snooping optimise-multicast-flood`
- `[template ip igmp snooping policy] ip igmp snooping optimise-multicast-flood`

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(2) releases in which the bug exists. A bug might also exist in releases other than the 2.2(2) releases.

Table 3 Open Bugs in the 2.2(2) Release

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]	2.2(2q) and later
CSCvi82903	When authenticating with the Cisco APIC using ISE (TACACS), all logins over 31 characters fail.	2.2(2q) 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(2i) and later
CSCuu17314	CDP is not enabled on the management interfaces for the leaf switches and spine switches.	2.2(2e) 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(2e) and later

Bug ID	Description	Exists in
CSCvc91298	The APIC SCVMM agent stops responding with the following APIC error message: Fault delegate: Connection to VMM controller is failing repeatedly with error:[]. Please verify network connectivity of VMM controller and check VMM controller user credentials are valid. When using the Configuration Manager Trace Log Tool to troubleshoot, the tool stops at the following processs: LogPsCommand|| Executing PS command Get-SCVmNetwork.	2.2(2e) and later
CSCvd15194	When there is an L3Out configuration on a sub-interface and if any operation results in a policy tag (pcTag) change of the external Layer 3 EPG (l3extInstP object) within the L3Out, the sub-interface might flap.	2.2(2e) and later
CSCvd21880	Continuous upgrade and downgrade results in policyelem core on ToR.	2.2(2e) 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(2e) and later
CSCvd43548	The stats for a given leaf switch rule cannot be viewed if a rule is double-clicked.	2.2(2e) and later
CSCvd51969	The policy element process generates a core on a leaf switch that has a vzAnyCons configuration.	2.2(2e) and later
CSCvd60582	While creating a DVS using the vRealize workflow, you cannot choose DVS version 6.5.	2.2(2e) 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(2e) 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(2e) and later
CSCvd74774	In a shared service scenario, where routes are leaked from an L3Out on VRF2 into VRF1 through a contract between the application EPG or external Layer 3 (l3extInstP) EPG on VRF1 and the external Layer 3 (l3extInstP) EPG on VRF2, upon removing contracts, L3Out (VRF2) routes might not be withdrawn from VRF1.	2.2(2e) 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(2e) and later

Bug ID	Description	Exists in
CSCvd84085	Stale contract rules are seen with vzAnyCons after changing the scope from “global” to “vrf.”	2.2(2e) and later
CSCvd86761	After a Cisco APIC cluster diverges due to unexpected leaf switch reload or some other event, which prevents an application from opening. The following error message displays: The application can not be run because it has validation errors. Please uninstall and install again.	2.2(2e) and later
CSCvd87004	VMM manager process on Cisco APIC may restart with a core file generation.	2.2(2e) and later
CSCvd97299	CDP Interface Policy admininstration state is incorrectly mentioned in the policy creation window.	2.2(2e) 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(2e) 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(2e) 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(2) Release

Bug ID	Description	Fixed in
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(2e)
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(2e)
CSCvd30648	When configuring route leaking between VRFs, traffic between a shared L3Out and a VzAny consumer might be dropped.	2.2(2e)
CSCvd86761	After the Cisco APIC cluster diverges due to an unexpected leaf switch reload or some other event, you might be unable to open an application. The following error displays: The application cannot be run because it has validation errors. Please uninstall and install again.	2.2(2f)
CSCvd80437	Shared service deny actrlRules might be missing in some consumer Virtual Routing and Forwarding instance (VRF) after the provider VRF is changed from unenforced to enforced.	2.2(2f)
CSCve11737	When the user deletes the null0 next hop from an IPv6 static route, the null0 next hop is deleted on the Cisco APIC, but still exists on the leaf switch.	2.2(2f)
CSCve26851	When an http request is sent to a container with a header and the value 'CONTENT-LENGTH': is empty, it must be handled.	2.2(2i)
CSCve15161	Capacity dashboard in the Cisco APIC must have VRF per leaf limit increased to 400.	2.2(2i)
CSCve41607	Cisco APIC cluster failure to delete the file might occur after you delete the application.	2.2(2i)
CSCve39804	Cisco APIC might not be responsive after an upgrade.	2.2(2i)
CSCvf00823	Cisco APIC might not sync inventory for a domain from VMware vCenter.	2.2(2k)
CSCvf14956	DHCP lease on Cisco Application Virtual Switch (AVS) client might not renew, even when an ACK (acknowledgement) is sent.	2.2(2k)

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(2) releases in which the known behavior exists. A bug might also exist in releases other than the 2.2(2) releases.

Table 5 Known Behaviors in the 2.2(2) 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(2e) and later
CSCuo79243	In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.	2.2(2e) and later
CSCuo79250	The node ID policy can be replicated from an old appliance that is decommissioned when it joins a cluster.	2.2(2e) 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(2e) and later
CSCup79002	The hostname resolution of the syslog server fails on leaf and spine switches over in-band connectivity.	2.2(2e) and later
CSCuq21360	Following a FEX or switch reload, configured interface tags are no longer configured correctly.	2.2(2e) 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(2e) 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(2e) 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(2e) and later
CSCut51929	The traffic destined to a shared service provider endpoint group picks an incorrect class ID (PcTag) and gets dropped.	2.2(2e) 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(2e) and later
CSCuu61998	Newly added microsegment EPG configurations must be removed before downgrading to a software release that does not support it.	2.2(2e) 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(2e) and later
CSCva32534	Creating or deleting a fabricSetupP policy results in an inconsistent state.	2.2(2e) 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(2e) 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(2e) and later

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

New Documentation

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

- *Cisco ACI Virtualization Guide, Release 2.2(2e)*
- *Cisco APIC and 802.1Q Tunnels*

- *Cisco APIC and Dynamic Breakout Ports*
- *Cisco APIC and NetFlow*
- *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 2.2(2e)*
- *Cisco APIC NX-OS Style CLI Command Reference, Release 2.2(2e)*
- *Cisco APIC Redundancy*
- *Cisco APIC REST API Configuration Guide*
- *Cisco APIC with HSRP*
- *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(2e) and Cisco Nexus 9000 Series ACI-Mode Switches, Release 12.2(2e)*
- *Cisco APIC Layer 2 Configuration Guide*
- *Cisco APIC Layer 3 Configuration Guide*