



Cisco Application Policy Infrastructure Controller Release Notes, Release 3.2(1)

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

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

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

Note: Use this document with the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 13.2(1)*, which you can view at the following location:

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

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

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

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

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

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

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

You can access these documents from the following website:

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

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

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
------	-------------

Date	Description
December 9, 2022	In the Open Bugs section, added bug CSCvw33061.
August 1, 2022	In the Miscellaneous Compatibility Information section, added: <ul style="list-style-type: none"> ■ 4.1(2k) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
February 23, 2022	In the Miscellaneous Compatibility Information section, added: <ul style="list-style-type: none"> ■ 4.1(2g) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
February 9, 2021	In the Open Bugs section, added bug CSCvt07565.
February 3, 2021	In the Miscellaneous Compatibility Information section, for CIMC HUU ISO, added: <ul style="list-style-type: none"> ■ 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
December 16, 2020	In the Miscellaneous Compatibility Information section, CIMC release 4.1(1g) is now recommended for UCS C220/C240 M4 (APIC-L2/M2).
October 8, 2019	In the Miscellaneous Compatibility Information section, updated the latest supported CIMC releases to: <ul style="list-style-type: none"> — 4.0(2g) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) — 3.0(4I) CIMC HUU ISO (recommended) for UCS C220/C240 M3 (APIC-L1/M1)
October 4, 2019	In the Miscellaneous Guidelines section, added the following bullet: <ul style="list-style-type: none"> ■ When you create an access port selector in a leaf interface rofile, the feXld 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 feXld property is only used when the port selector is associated with an infraFexBndlGrp managed object.
October 3, 2019	In the Miscellaneous Guidelines section, added the bullet that begins as follows: <ul style="list-style-type: none"> ■ Fabric connectivity ports can operate at 10G or 25G speeds (depending on the model of the APIC server) when connected to leaf switch host interfaces.
September 17, 2019	3.2(1I): In the Open Bugs section, added bug CSCuu17314 and CSCve84297.
September 13, 2019	In the New Software Features section, for the rogue endpoint control policy feature, changed the following guidelines and restrictions text: <ul style="list-style-type: none"> ■ The rogue endpoint feature is not supported on remote leaf switches or Cisco ACI Multi-Site. <p>To the following text:</p> <ul style="list-style-type: none"> ■ The rogue endpoint feature can be used within each site of a Cisco ACI Multi-Site deployment to help with misconfigurations of servers that cause an endpoint to move within the site. The rogue endpoint feature is not designed for scenarios where the endpoint may move between sites.

Contents

Date	Description
September 10, 2019	<p>In the Known Behaviors section, added the following bullet:</p> <ul style="list-style-type: none"> ■ When there are silent hosts across sites, ARP glean messages might not be forwarded to remote sites if a 1st generation ToR switch (switch models without -EX or -FX in the name) happens to be in the transit path and the VRF is deployed on that ToR switch, the switch does not forward the ARP glean packet back into the fabric to reach the remote site. This issue is specific to 1st generation transit ToR switches and does not affect 2nd generation ToR switches (switch models with -EX or -FX in the name). This issue breaks the capability of discovering silent hosts.
August 5, 2019	3.2(1l): In the Open Bugs section, added bug CSCvj76503.
July 17, 2019	3.2(1l): In the Open Bugs section, added bug CSCvq39922.
April 6, 2019	3.2(1l) and 3.2(1m): In the Open Bugs section, moved bug CSCvj81562 from the 3.2(1m) section to the 3.2(1l) section. This bug applies to all 3.2(1) releases.
March 25, 2019	<p>In the Miscellaneous Compatibility Information section, added:</p> <ul style="list-style-type: none"> — 4.0(2f) CIMC HUU ISO (recommended) for UCS C220/C240 M4 — 3.0(4j) CIMC HUU ISO (recommended) for UCS C220/C240 M3
January 8, 2019	In the New Software Features section, added " EtherChannel support for 16 members."
November 21, 2018	3.2(1l): In the Open Bugs section, added bug CSCvn15374.
August 15, 2018	3.2(1l): In the Open Bugs section, added bug CSCvk38296.
August 7, 2018	In the Miscellaneous Compatibility Information section, added an entry for OpenStack and Kubernetes distributions.
July 30, 2018	3.2(1m): In the Open Bugs section, added bug CSCvj81562.
July 24, 2018	3.2(1l): In the Open Bugs section, added bug CSCvj66372.
July 20, 2018	3.2(1l): In the Resolved Bugs section, added bug CSCvg98346.
June 28, 2018	<p>For the description of the Forwarding scale profile policies enhancement new software feature, added the following text:</p> <p style="padding-left: 40px;">For the scale information, see the <i>Cisco APIC Forwarding Scale Profile Policy</i> document.</p> <p>3.2(1l): In the Open Bugs section, added bug CSCvk01926.</p>

Contents

Date	Description
June 6, 2018	<p>In the Virtualization Compatibility Guidelines section, added the following item:</p> <p>After you migrate VMs using a cross-data center VMware vMotion in the same VMware vCenter, you might find a stale VM entry under the source DVS. This stale entry can cause problems, such as host removal failure. The workaround for this problem is to enable "Start monitoring port state" on the vNetwork DVS. See the KB topic "Refreshing port state information for a vNetwork Distributed Virtual Switch" on the VMware Web site for instructions.</p>
June 5, 2018	<p>In the New Software Features section, changed the description of "Cisco ACI Virtual Edge: remote storage deployment" to:</p> <p>Beginning with this release, Cisco ACI Virtual Edge can be deployed on local storage or remote storage.</p>
May 27, 2018	<p>3.2(1l): In the Open Bugs section, added bug CSCvj65274.</p> <p>3.2(1m): Release 3.2(1m) became available. Added the resolved bugs for this release.</p>
May 25, 2018	<p>In the New Software Features section, added the limitations for the rogue endpoint control policy feature.</p>
May 22, 2018	<p>3.2(1l): Release 3.2(1l) became available.</p>

Contents

This document includes the following sections:

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

New and Changed Information

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

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

New Software Features

Table 2 New Software Features, Guidelines, and Restrictions

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

Table 2 New Software Features, Guidelines, and Restrictions

Feature	Description	Guidelines and Restrictions
802.1x multi-host mode and multi-auth mode	<p>This release adds the following 802.1x modes:</p> <ul style="list-style-type: none"> ■ Multi-host mode—Allows multiple hosts per port, but only the first one gets authenticated. The port is moved to the authorized state after the successful authorization of the first host. Subsequent hosts are not required to be authorized to gain network access once the port is in the authorized state. If the port becomes unauthorized when reauthentication fails or an EAPOL logoff message is received, all attached hosts are denied access to the network. The capability of the interface to shut down upon security association violation is disabled in multiple host mode. This mode is applicable for both switch-to-switch and host-to-switch topologies. ■ Multi-auth mode—Allows multiple hosts and all hosts are 	None.

Feature	Description	Guidelines and Restrictions
	<p>authenticated separately. Each host must have the same EPG/VLAN information.</p> <ul style="list-style-type: none"> ■ Multi-domain mode—For separate data and voice domain. For use with IP phones. <p>For more information, see the <i>Cisco APIC Security Configuration Guide</i>.</p>	
AAA external logging (TACACS)	<p>Terminal Access Controller Access Control System (TACACS) and Terminal Access Controller Access Control System Plus (TACACS+) are simple security protocols that provide centralized validation of users attempting to gain access to network devices. TACACS+ furthers this capability by separating the authentication, authorization, and accounting functions in modules, and encrypting all traffic between the NAS and the TACACS+ daemon.</p> <p>TACACS external logging collects AAA data from a configured TACACS source (fabric-wide or tenant-only) and delivers it to one or more remote destination TACACS servers, as configured in a TACACS destination group. The collected data includes AAA session logs (SessionLR) such as log-ins, log-outs, and time ranges, for every Cisco Application Policy Infrastructure Controller (APIC) user, as well as AAA modifications (ModLR) such as the addition of a new user or a password change. Additionally, all configuration changes are logged and include the user ID and time stamp.</p> <p>For more information, see the <i>Cisco ACI TACACS External Logging</i> KB article.</p>	None.
Anycast services	<p>Anycast services are supported in the Cisco ACI fabric. A typical use case is to support ASA firewalls in the pods of a multipod fabric, but Anycast could be used to enable other services, such as DNS servers or printing services. In the ASA use case, a firewall is installed in every pod and Anycast is enabled, so that the firewall can be offered as an Anycast service. One instance of a firewall going down does not affect clients, as the requests are routed to the next, nearest instance available. You install ASA firewalls in each pod, then enable Anycast and configure the IP address and MAC address to be used.</p> <p>The Cisco APIC pushes the configuration of the Anycast MAC and IP addresses to the leaf switches where the VRF is deployed or where there is a contract to allow an Anycast EPG.</p> <p>For more information, see the <i>Cisco APIC and Anycast Services</i> KB article.</p>	For guidelines and limitations, see the <i>Cisco APIC and Anycast Services</i> KB article.
Cisco ACI Virtual	Beginning in this release, Cisco ACI Virtual Edge faults are reported to assist in troubleshooting. The Cisco ACI Virtual Edge monitors	No action is required to configure the collection of

New and Changed Information

Feature	Description	Guidelines and Restrictions
Edge health status	<p>states of objects—for example, an EPG, port, global policy, or Virtual Tunnel Endpoint (VTEP)—listed in a database. When an object undergoes a state change, that change is recorded.</p> <p>For more information, see the <i>Cisco ACI Virtual Edge Health Status</i> KB article.</p>	data into a health score.
Cisco ACI Virtual Edge license consumption	<p>Beginning with this release, you can track the number of Cisco ACI Virtual Edge licenses on each host. You can use the Cisco APIC GUI or NX-OS-style CLI commands to view license information.</p> <p>For more information, see "Viewing Cisco ACI Virtual Edge Licenses using the GUI" in the <i>Cisco ACI Virtual Edge Installation Guide</i> and <i>Cisco ACI Smart Licensing</i> KB article.</p>	None.
Cisco ACI Virtual Edge: Layer 4 to Layer 7 service graphs	<p>This release adds support for Layer 4 to Layer 7 service graphs for Cisco ACI Virtual Edge. You use service graphs to identify the set of network service functions that an application requires.</p> <p>For more information, see the section "Layer 4 to Layer 7 Services" in the <i>Cisco ACI Virtual Edge Configuration Guide</i> and the <i>Cisco APIC Layer 4 to Layer 7 Services Deployment Guide</i>.</p>	Layer 4 to Layer 7 services are supported only for routed mode; there is no support for transparent mode.
Cisco ACI Virtual Edge: remote storage deployment	Beginning with this release, Cisco ACI Virtual Edge can be deployed on local storage or remote storage.	None.
Cloning port configurations	<p>Support for cloning port configurations is added. After you configure a leaf switch port, you can copy the configuration and apply it to other ports.</p> <p>For more information, see "Access Interfaces" in the <i>Cisco APIC Layer 2 Networking Configuration Guide</i>.</p>	<p>This is only supported in the Cisco APIC GUI (not in the NX-OS-style CLI).</p> <p>Port cloning is used for small numbers of leaf switch ports (interfaces) that you deploy on multiple nodes in the fabric and that are individually configured, not for interfaces configured using fabric access policies.</p> <p>Port cloning is only supported for Layer 2 configurations.</p> <p>The following policies are not supported on a cloned port:</p> <ul style="list-style-type: none"> ■ Attachable Access Entity ■ Storm Control

New and Changed Information

Feature	Description	Guidelines and Restrictions
		<ul style="list-style-type: none"> ■ DWDM ■ MACsec
Contract and subject exceptions	<p>Contracts between EPGs are enhanced to include exceptions to subjects or contracts. This enables a subset of EPGs to be excluded in contract filtering. For example, a provider EPG can communicate with all consumer EPGs except those that match criteria configured in a subject exception in the contract governing their communication. Inter-EPG contracts and intra-EPG contracts are supported.</p> <p>For more information, see "Basic User Tenant Configuration" in the <i>Cisco APIC Basic Configuration Guide</i>.</p>	None.
Contract permit and deny log enhancements	<p>EPG information has been added to the output of contract Cisco ACI permit and deny logs.</p> <p>For more information, see Using the Cisco APIC Troubleshooting Tools in Cisco APIC Troubleshooting Guide.</p>	<p>The feature is supported for traffic on Cisco Nexus 9000 series switches with part numbers that end in EX and FX, and later (for example, N9K-C93180LC-EX).</p> <p>The following limitations apply:</p> <ul style="list-style-type: none"> ■ Depending on the position of the EPG in the network, EPG data may not be available for the logs. ■ When configuration changes occur, log data may be out of date. In steady state, log data will be accurate. ■ The most accurate EPG data in the permit and deny logs results when the logs are focussed on: <ul style="list-style-type: none"> ■ Flows from EPG to EPG, where the ingress policy is installed at the ingress TOR and the egress policy is installed at the

New and Changed Information

Feature	Description	Guidelines and Restrictions
		<p>egress TOR</p> <ul style="list-style-type: none"> ■ Flows from EPG to L3Out, where one policy is applied on the BL TOR and the other policy is applied on a non-BL TOR <p>The feature is not supported for microsegmentation EPGs or EPGs used in shared services (including shared L3Outs).</p>
Enhanced breakout support on profiled QSFP ports on N9K-C93180YC-FX switches	<p>Support is added for 100 Gigabit (Gb) (4X25Gb) and 40Gb (4X10Gb) dynamic breakouts on profiled QSFP ports on the N9K-C93180YC-FX switch (in ACI mode).</p> <p>For more information, see "Dynamic Breakout Ports" in the <i>Cisco APIC Layer 2 Networking Configuration Guide</i>.</p>	None.
EtherChannel support for 16 members	EtherChannels now support 16 members.	None.
Fibre Channel N-port virtualization	<p>A switch is in N-port virtualization (NPV) mode after enabling NPV. NPV mode applies to an entire switch. All end devices connected to a switch that are in NPV mode must log in as an N port to use this feature. All links from the edge switches (in NPV mode) to the NPV core switches are established as NP ports (not E ports), which are used for typical inter-switch links.</p> <p>Fibre Channel N-port virtualization (FC NPV) provides the following benefits:</p> <ul style="list-style-type: none"> ■ Increased number of hosts that connect to the fabric without adding domain IDs in the fabric ■ Connection of FC and FCoE hosts and targets to SAN fabrics using FC interfaces ■ Automatic traffic mapping ■ Static traffic mapping ■ Disruptive automatic load balancing <p>For more information, see the <i>Cisco APIC Layer 2 Networking Configuration Guide</i>.</p>	For guidelines and limitations, see the <i>Cisco APIC Layer 2 Networking Configuration Guide</i> .
Forwarding scale profile policies enhancement	The forwarding scale profile policy now includes the High LPM scale option. High longest prefix match (LPM) provides scalability similar to the dual-stack policy, except that the LPM scale is 128,000 and	None.

Feature	Description	Guidelines and Restrictions
	<p>the policy scale is 8,000.</p> <p>Scale improvements in the other forwarding scale options are also added in this release. For the scale information, see the <i>Cisco APIC Forwarding Scale Profile Policy</i> document.</p>	
Krowten application	<p>The Krowten application takes a snapshot of the current Cisco APIC topology so that the user can get a comprehensive view of the EPG/VLAN distribution and mapping across the Fabric.</p> <p>After the Krowten application is enabled, the snapshot is automatically created and you can display all the various existing topologies and their details.</p>	None.
Layer 3 EPG SPAN configurations support	<p>This release adds support for configuring a Layer 3 EPG SPAN policy for external access.</p> <p>For more information, see the Cisco APIC Troubleshooting Guide.</p>	None.
Layer 3 routed and sub-interface port channels	<p>Previously, Cisco APIC supported only Layer 2 port channels. Starting with release 3.2(1), Cisco APIC now supports Layer 3 port channels. You can configure these Layer 3 port channels through the CLI, GUI, or REST API.</p> <p>For more information, see the <i>Cisco APIC Layer 3 Networking Configuration Guide</i>.</p>	None.
Multi-node policy-based redirect	<p>Multi-node policy-based redirect (PBR) enhances PBR by supporting up to three nodes in a single service chain. You can configure which service node connector terminates the traffic and based on this configuration, the source and destination class IDs for the service chain are determined. In the multi-node PBR feature, policy-based redirection can be enabled on the consumer, provider, or both of the service node connectors. Multi-node PBR can also be configured for the forward or reverse directions. If the PBR policy is configured on a service node connector, then that connector does not terminate traffic.</p> <p>For more information, see the <i>Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 3.2(1)</i>.</p>	Multi-node PBR supports up to three nodes in a service chain that can be configured for policy-based routing.
Multi-tier applications with a service graph	<p>The Multi-Tier Application with Service Graph Quick Start dialog provides a consolidated method of configuring service graph components such as bridge domains, EPGs, VRF instances, services, and contracts. As opposed to configuring each object in different locations in the Cisco APIC, the Quick Start dialog gathers the necessary configurations and combines them into a simple, organized step-by-step process.</p> <p>For more information, see the <i>Cisco APIC Layer 4 to Layer 7</i></p>	None.

New and Changed Information

Feature	Description	Guidelines and Restrictions
	<i>Services Deployment Guide, Release 3.2(1).</i>	
Optimize contract performance	<p>In this release, you can enable bidirectional standard contracts for more efficient hardware TCAM storage of contract data. With optimization enabled, contract statistics for both directions are aggregated. To configure efficient TCAM contract data storage, enable the following options:</p> <ul style="list-style-type: none"> • Contracts applied in both directions between the provider and consumer • For filters with IP TCP or UDP protocols, enable the reverse port option. • When adding the contract subjects, enable the no stats directive. <p>For more information, see "Basic User Tenant Configuration" in the <i>Cisco APIC Basic Configuration Guide</i>.</p>	This feature is supported on Cisco Nexus 9000 series top of rack (TOR) switches with names ending with EX and FX, and later (for example, N9K-C93180LC-EX or N9K-C93180YC-FX).
Per leaf aggregate for the Data Plane Policer	<p>A clear semantic is given to the Data Plane Policer policy itself, as well as a new flag introducing the sharing-mode setting as presented in the CLI. Essentially, there is no longer an implicit behavior, which is different if the Data Plane Policer is applied to Layer 2 or Layer 3, or to a per-EPG case. Now, you have control of the behavior. If the sharing-mode is set to shared, then all the entities on the leaf referring to the same Data Plane Policer, will share the same HW policer. If the sharing-mode is set to dedicated then there would be a different HW policer allocated for each L2 or L3 or EPG member on the leaf. The policer is then dedicated to the entity that needs to be policed.</p> <p>For more information, see the <i>Cisco APIC Security Configuration Guide</i>.</p>	None.
Policy-based redirect and service graphs to Redirect All EPG-to-EPG traffic within the same VRF instance	<p>You can apply a service graph with a policy-based redirect policy that redirects traffic using the vzAny managed object. Such a policy enables all traffic from any endpoint group to be transmitted to any other endpoint group in the same VRF instance through a Layer 4 to Layer 7 device that is configured as one of the nodes in the service graph.</p> <p>For more information, see the <i>Cisco APIC Layer 4 to Layer 7 Services Deployment Guide</i>.</p>	For guidelines and limitations, see the <i>Cisco APIC Layer 4 to Layer 7 Services Deployment Guide</i> .
Policy-based redirect resilient hashing	<p>In symmetric policy-based redirect (PBR), incoming and return user traffic uses the same PBR node. However, if one of the PBR nodes goes down or fails, the existing traffic flows are rehashed to another node. This can cause issues such as existing traffic on the functioning node being load balanced to other PBR nodes that do not have current connection information. If the traffic is traversing a stateful firewall, a node going down or failing can also lead to the</p>	None.

Feature	Description	Guidelines and Restrictions
	<p>connection being reset.</p> <p>Policy-based redirect resilient hashing is the process of mapping traffic flows to physical nodes and avoiding the rehashing of any traffic other than the flows from the failed node. The traffic from the failed node is remapped to a "backup" node. The existing traffic on the "backup" node is not moved.</p> <p>For more information, see the <i>Cisco APIC Layer 4 to Layer 7 Services Deployment Guide</i>.</p>	
Remote leaf switches enhancements	<p>Support is added for the following features with remote leaf switches:</p> <ul style="list-style-type: none"> • FEX devices connected to remote leaf switches • TEP to TEP atomic counters between remote leaf switches or remote leaf switches and local leaf switches • Cisco AVS with VLAN and Cisco AVS with VXLAN • Cisco ACI Virtual Edge with VLAN and Cisco ACI Virtual Edge with VXLAN <p>For more information, see "Remote Leaf Switches" in the <i>Cisco APIC Layer 3 Networking Configuration Guide</i>.</p>	None.
Rogue endpoint control policy	<p>The global rogue endpoint control policy for the fabric is introduced to detect unauthorized endpoints. A rogue endpoint attacks top of rack (ToR) switches through frequently and repeatedly injecting packets on different ToR ports and changing 802.1Q tags (thus, emulating endpoint moves), which causes learned sclass and EPG port changes. Misconfigurations can also cause frequent IP and MAC address changes (moves).</p> <p>Such rapid movement in the fabric causes significant network instability, high CPU usage, and in rare instances, endpoint mapper (EPM) and EPM client (EPMC) crashes due to significant and prolonged messaging and transaction service (MTS) buffer consumption. Also, such frequent moves might result in the EPM and EPMC logs rolling over very quickly, hampering debugging for unrelated endpoints.</p> <p>The rogue endpoint control feature addresses this vulnerability by quickly:</p> <ul style="list-style-type: none"> ■ Identifying such rapidly moving MAC and IP endpoints ■ Stopping the movement by temporarily making endpoints static (thus, quarantining the endpoint) ■ Keeping the endpoint static for the rogue EP detection interval and, after this time expires, deleting the rogue MAC or IP address ■ Generating a host tracking packet to enable the system to 	<ul style="list-style-type: none"> ■ Changing rogue endpoint control policy parameters will not affect existing rogue endpoints. ■ If a rogue endpoint is enabled, loop detection and bridge domain move frequency will not take effect. ■ Disabling the rogue endpoint feature clears all rogue endpoints. ■ You must disable the rogue endpoint feature prior to upgrading or downgrading the Cisco APIC. ■ The endpoint mapper (EPM) has value limits for rogue endpoint parameters. If you set

New and Changed Information

Feature	Description	Guidelines and Restrictions
	<p>re-learn the impacted MAC or IP address</p> <ul style="list-style-type: none"> ■ Raising a fault to enable corrective action <p>For more information, see "Provisioning Core ACI Fabric Services" in the <i>Cisco APIC Basic Configuration Guide</i>.</p>	<p>the parameter values outside of this range, the Cisco APIC raises a fault for each mismatched parameter. For the valid ranges, see the <i>Cisco APIC Basic Configuration Guide</i>.</p> <ul style="list-style-type: none"> ■ The rogue endpoint feature can be used within each site of a Cisco ACI Multi-Site deployment to help with misconfigurations of servers that cause an endpoint to move within the site. The rogue endpoint feature is not designed for scenarios where the endpoint may move between sites.
Service graphs for contracts involving microsegmented EPGs	<p>Beginning with this release, Layer 4 to Layer 7 service graphs are supported for contracts between microsegmented EPGs and between microsegmented EPGs and regular EPGs. Service graphs enable you to refine the contracts by adding such services as a firewall or load-balancing.</p> <p>For more information, see the <i>Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 3.2(1)</i>.</p>	None.
Simplified fabric external access policy configuration	<p>In this release, fabric external access policy creation is simplified in the Cisco APIC GUI.</p> <p>For the policy configuration wizard for ports, Port Channels, Virtual Port Channels or Fibre Channels, navigate to Fabric > External Access Policies > Quick Start > Interfaces and Policies > Configure Interface.</p>	None.
Smart Callhome	<p>Smart Callhome provides an email-based notification for critical system policies in a similar way as Callhome. However, Smart Callhome collects a more specific selection of faults to deliver in email messages.</p> <p>The fault triggers that are typical of the Smart Callhome feature correspond to the kind of events that threaten to disrupt your network. Examples are:</p> <ul style="list-style-type: none"> ■ Temperature Faults: The temperature of a sensor exceeds a 	None.

Feature	Description	Guidelines and Restrictions
	<p>threshold.</p> <ul style="list-style-type: none"> ■ Fan/ Power Supply Faults: A fan or power supply unit goes offline. ■ Disk Utilization Faults: The disk usage of a device exceeds a threshold. <p>Smart Callhome collects faults and emails them to a network support engineer, a Network Operations Center, or to Cisco Smart Callhome services to generate a case with the Technical Assistance Center (TAC).</p> <p>For more information, see the <i>Cisco ACI Smart Callhome</i> KB article.</p>	
Smart Licensing and Cisco ACI	<p>Starting with Cisco APIC release 3.2(1), Smart Licensing is enabled in the Cisco ACI fabric and by extension in the Cisco APIC as a Cisco Smart Licensing-enabled product. Cisco Smart Licensing is a unified management system that manages all of the software licenses across Cisco products.</p> <p>For more information, see the <i>Cisco ACI Smart Licensing</i> KB article.</p>	<p>For guidelines and limitations, see the <i>Cisco ACI Smart Licensing</i> KB article.</p>
Two-Way Active Measurement Protocol (TWAMP)	<p>The Two-Way Active Measurement Protocol (TWAMP) defines a standard (RFC 5357) for measuring round-trip network performance between any two devices that support the TWAMP protocols. The TWAMP Server/Reflector is supported as part of the IP SLA responder in NX-OS. Cisco APIC configures the TWAMP support for switch groups and provides the monitoring of the test sessions and connections.</p> <p>For more information, see the <i>Cisco ACI TWAMP</i> KB article.</p>	<p>The devices must support the following TWAMP protocols:</p> <ul style="list-style-type: none"> ■ TWAMP-Control Protocol: Set up performance measurement sessions ■ TWAMP-Test Protocol: Send and receive performance-measurement probes <p>The TWAMP client resides on an open-source third-party TWAMP utility application that must be reachable by any of the switch nodes through a management port, in-band management port, or L3Out interface.</p>
VM folder attribute for microsegmentation	<p>This release adds support for the VM folder as an VM-based attribute for microsegmentation with Cisco ACI.</p>	<p>The VM folder attribute is supported for Cisco ACI Virtual Edge, Cisco AVS, and</p>

Upgrade and Downgrade Information

Feature	Description	Guidelines and Restrictions
with Cisco ACI	For more information, see the "Microsegmentation with Cisco ACI" chapter in the <i>Cisco ACI Virtualization Guide, Release 3.2(1)</i> .	VMware VDS. The attribute is not supported for Microsoft vSwitch.

New Hardware Features

For new hardware features, see the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 13.2(1)* at the following location:

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

Changes in Behavior

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

Upgrade and Downgrade Information

For upgrade and downgrade considerations for the Cisco APIC, see the Cisco APIC documentation site at the following URL:

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

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

Bugs

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

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

Open Bugs

This section lists the open bugs. Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Exists In" column of the table specifies the 3.2(1) releases in which the bug exists. A bug might also exist in releases other than the 3.2(1) releases.

Table 3 Open Bugs in This Release

Bug ID	Description	Exists in

Bugs

Bug ID	Description	Exists in
CSCvk04072	There is no record of who acknowledged a fault in the Cisco APIC, nor when the acknowledgement occurred.	3.2(1m) and later
CSCvs47757	The plnghandler process crashes on the Cisco APIC, which causes the cluster to enter a data layer partially diverged state.	3.2(1m) and later
CSCvs78996	The policy manager (PM) may crash when use testapi to delete MO from policymgr db.	3.2(1m) and later
CSCuu17314	CDP is not enabled on the management interfaces for the leaf switches and spine switches.	3.2(1l) and later
CSCvd43548	The stats for a given leaf switch rule cannot be viewed if a rule is double-clicked.	3.2(1l) 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.	3.2(1l) 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.	3.2(1l) 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]	3.2(1l) and later
CSCvf70411	A route will be advertised, but will not contain the tag value that is set from the VRF route tag policy.	3.2(1l) and later
CSCvg00627	A tenant's flows/packets information cannot be exported.	3.2(1l) and later
CSCvg35344	Requesting an enhancement to allow exporting a contract by right clicking the contract itself and choosing "Export Contract" from the right click context menu. The current implementation of needing to right click the Contract folder hierarchy to export a contract is not intuitive.	3.2(1l) and later

Bugs

Bug ID	Description	Exists in
CSCvg81020	For strict security requirements, customers require custom certificates that have RSA key lengths of 3072 and 4096.	3.2(11) and later
CSCvh52046	This is an enhancement to allow for text-based banners for the Cisco APIC GUI login screen.	3.2(11) and later
CSCvh54578	For a client (browser or ssh client) that is using IPv6, the Cisco APIC aaaSessionLR audit log shows "0.0.0.0" or some bogus value.	3.2(11) and later
CSCvh59843	Enabling Multicast under the VRF on one or more bridge domains is difficult due to how the drop-down menu is designed. This is an enhancement request to make the drop-down menu searchable.	3.2(11) and later
CSCvi20535	When a VRF table is configured to receive leaked external routes from multiple VRF tables, the Shared Route Control scope to specify the external routes to leak will be applied to all VRF tables. This results in an unintended external route leaking. This is an enhancement to ensure the Shared Route Control scope in each VRF table should be used to leak external routes only from the given VRF table.	3.2(11) and later
CSCvi41092	The APIC log files are extremely large, which takes a considerable amount of time to upload, especially for users with slow internet connectivity.	3.2(11) and later
CSCvi66563	There are duplicate IP addresses across 2 vPCs.	3.2(11) and later
CSCvi80543	This is an enhancement that allows failover ordering, categorizing uplinks as active or standby, and categorizing unused uplinks for each EPG in VMware domains from the APIC.	3.2(11) and later
CSCvi82903	When authenticating with the Cisco APIC using ISE (TACACS), all logins over 31 characters fail.	3.2(11) and later
CSCvi95657	On modifying a service parameter, the Cisco APIC sends 2 posts to the backend. The first post deletes all of the folders and parameters. The second post adds all of the remaining modified folders and parameters to the backend. These 2 posts will disrupt the running traffic.	3.2(11) and later
CSCvi99042	Health Group usage does not show the correct leaf switch information.	3.2(11) and later
CSCvj04166	The remote leaf TEP pool cannot be deleted after decommissioning the remote leaf and deleting the remote leaf vPC configuration.	3.2(11) and later

Bugs

Bug ID	Description	Exists in
CSCvj09453	The actrlRule is has the wrong destination.	3.2(11) and later
CSCvj26666	The "show run leaf spine <nodeld>" command might produce an error for scaled up configurations.	3.2(11) and later
CSCvj56726	The connectivity filter configuration of an access policy group is deprecated and should be removed from GUI.	3.2(11) and later
CSCvj66372	The Cisco APICs are fully fit and converged, but configuration changes to a tenant are accepted, but not deployed. However, changes made to other tenants or policies can still be applied and deployed.	3.2(11) and later
CSCvj76503	A maintenance window triggered for an upgrade remains active for an unlimited time. Adding another node to this maintenance window automatically upgrades this newly added node. In some releases, such as 3.1(2m), a message may say that the window is triggered from X to Y time period; however, the maintenance window is still active for an unlimited time.	3.2(11) and later
CSCvj81562	In the Cisco APIC release 3.2(1), the vmmmgr repeatedly crashes, which leads to the cluster being diverged.	3.2(11) and later
CSCvk01926	Smart Licensing does not work, and when querying the licenseManager object, the "dlcOperStatus" is always set to "in-progress."	3.2(11) and later
CSCvk38296	When deploying a single node PBR with a one-arm load balancer and without SNAT, the PBR datapath does not work as expected.	3.2(11) and later
CSCvm89559	The svc_ifc_policye process consumes 100% of the CPU cycles. The following messages are observed in svc_ifc_policymgr.bin.log: 8816 18-10-12 11:04:19.101 route_control ERROR co=doer:255:127:0xff0000000c42ad2:11 Route entry order exceeded max for st10960-2424833-any-2293761-33141-shared-svc-int Order:18846Max:17801 ../dme/svc/policyelem/src/gen/ifc/beh/imp/./rtctrl/RouteMapUtils.cc 239;q	3.2(11) and later
CSCvn00576	An SHA2 CSR for the ACI HTTPS certificate cannot be configured in the APIC GUI.	3.2(11) and later

Bugs

Bug ID	Description	Exists in
CSCvn15374	<p>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:</p> <pre>appliance_director DBG4 ... Lost heartbeat from appliance id= ... appliance_director DBG4 ... Appliance has become unavailable id= ...</pre> <p>On the switches, each process (such as policy-element) see rapidly changing leader elections and minority states:</p> <pre>adrs_rv DBG4 ... Updated leader election on replica=(6,26,1)</pre>	3.2(11) and later
CSCvp64280	<p>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.</p> <p>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.</p> <p>Cisco has released software updates that address this vulnerability. There are workarounds that address this vulnerability.</p> <p>This advisory is available at the following link:</p> <p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-n9kaci-bypass</p>	3.2(11) and later
CSCvp72283	<p>An APIC running the 3.0(1k) release sometimes enters the "Data Layer Partially Diverged" state. The aci diag rvread command shows the following output for the service 10 (observer):</p> <pre>Non optimal leader for shards :10:1,10:3,10:4,10:6,10:7,10:9,10:10,10:12,10:13,10:15,10:16,10:18,10:19,10:21,10:22,10:24,10:25, 10:27,10:28,10:30,10:31</pre>	3.2(11) and later
CSCvq39922	<p>Specific operating system and browser version combinations cannot be used to log in to the APIC GUI.</p> <p>Some browsers that are known to have this issue include (but might not be limited to) Google Chrome version 75.0.3770.90 and Apple Safari version 12.0.3 (13606.4.5.3.1).</p>	3.2(11) and later
CSCvq43101	<p>When opening an external subnet, a user cannot see Aggregate Export/Import check boxes set in GUI even though they were already configured.</p>	3.2(11) and later

Bugs

Bug ID	Description	Exists in
CSCvq86573	Under a corner case, the Cisco APIC cluster DB may become partially diverged after upgrading to a release that introduces new services. A new release that introduces a new DME service (such as the domainmgr in the 2.3 release) could fail to receive the full size shard vector update in first two-minute window, which causes the new service flag file to be removed before all local leader shards are able to boot into the green field mode. This results in the Cisco APIC cluster DB becoming partially diverged.	3.2(11) and later
CSCvr30815	vmmPLInf objects are created with epgKey's and DN's that have truncated EPG names (truncated at ".").	3.2(11) 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.	3.2(11) and later
CSCvr94614	There is a minor memory leak in svc_ifc_policydist when performing various tenant configuration removals and additions.	3.2(11) and later
CSCvt07565	The eventmgr database size may grow to be very large (up to 7GB). With that size, the Cisco APIC upgrade will take 1 hour for the Cisco APIC node that contains the eventmgr database. In rare cases, this could lead to a failed upgrade process, as it times out while working on the large database file of the specified controller.	3.2(11) and later
CSCvu01452	The MD5 checksum for the downloaded Cisco APIC images is not verified before adding it to the image repository.	3.2(11) and later
CSCvu21530	Protocol information is not shown in the GUI when a VRF table from the common tenant is being used in any user tenant.	3.2(11) and later
CSCvu62465	For an EPG containing a static leaf node configuration, the Cisco APIC GUI returns the following error when clicking the health of Fabric Location: Invalid DN topology/pod-X/node-Y/local/svc-policyelem-id-0/ObservedEthlf, wrong rn prefix ObservedEthlf at position 63	3.2(11) and later
CSCvv62861	A leaf switch reloads due to an out-of-memory condition after changing the contract scope to global.	3.2(11) and later
CSCvw33061	Traffic loss is observed from multiple endpoints deployed on two different vPC leaf switches.	3.2(11) and later
CSCvj65274	When upgrading to Cisco APIC version 3.2(11) / 13.2(11), switch nodes might encounter a process crash/core with the eventmgr service.	3.2(11)

Bugs

Resolved Bugs

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

Table 4 Resolved Bugs in This Release

Bug ID	Description	Fixed in
CSCvj65274	When upgrading to Cisco APIC version 3.2(1) / 13.2(1), switch nodes might encounter a process crash/core with the eventmgr service.	3.2(1m)
CSCvf32908	When using mongoDB for Cisco ACI apps, the app must be deleted before the upgrade and reinstalled after the upgrade to avoid corruption of application data.	3.2(1)
CSCvf92483	This issue occurs while using the import-config file command on the CLI where the file is the output of export-config command. The file contains the output of show running-config of the scope where export-config was executed. The error occurs only when the file contains crypto commands, the Bash shell throws the error and hangs without returning the prompt.	3.2(1)
CSCvg02551	When the IS-IS to OSPF Multi-Site CPTep route leaking is not programmed, inter-site BGP session might go down on the spine switch. This behavior might cause traffic drop.	3.2(1)
CSCvg37617	The zoning rule installation incorrectly permitted all of the traffic to and from the L3Out to EPG as the default permit without redirecting the traffic to the service node.	3.2(1)
CSCvg53205	A fault for a 100% drop rate is observed for an endpoint-to-external IP address atomic counters policy after disabling/enabling a switch.	3.2(1)
CSCvg56414	An external IP address-to-external IP address atomic counters policy does not give the results for the flow that matches the configured external IP addresses.	3.2(1)
CSCvg60014	Clicking the Submit button in a wizard will fail if any of the entered values are invalid.	3.2(1)
CSCvg60565	If a service graph is initially configured as uni-directional and later a filter is added and the service graph is made bi-direction, the service graph enters a faulty state.	3.2(1)
CSCvg67522	When two different service chains (one for IPv4 traffic and the other for IPv6 traffic) are using the same exact forwarding path (the same bridge domain and VLAN on the service nodes), but different redirect policies (one for IPv4 and the other for IPv6), then the IP SLA objects might not be cleaned up when the contract is detached from the service graph.	3.2(1)
CSCvg74082	A newly-created VFC shows the admin state as down.	3.2(1)
CSCvg75150	A service graph is in the applied state even if the VRF instance associated with the consumer EGP or consumer-facing service node EPG gets deleted.	3.2(1)
CSCvg79436	In Cloud Orchestrator Mode, dual stack (that is, IPv4 and IPv6) cannot be configured on the same interface.	3.2(1)
CSCvg82738	Whenever a user expands a drop-down list that has many policies (>10K), the GUI tries to show all of them at once, which causes a timeout from the server, after which the server tries again. This process continues and the GUI becomes unresponsive.	3.2(1)

Bugs

Bug ID	Description	Fixed in
CSCvlg86073	With a 0.0.0.0/0 subnet and a specific subnet with an import route-map, the GUI shows only a 212.1.0.0/24 subnet.	3.2(1I)
CSCvlg95080	A remote leaf switch TEP pool is not getting deleted if the remote leaf switches are decommissioned before deleting the vPC.	3.2(1I)
CSCvlg98346	The LLDP counters on the leaf switch will show increasing counts, but the LLDP neighbors will show the correct counts. If you check the Cisco APIC ctrladj and port role, it will show as active. Traffic is not impacted.	3.2(1I)
CSCvvh00839	On importing an exported configuration, the import will succeed and might report a warning about a failure to extract the CISCO.CloudMode.1.0.zip archive. If the CISCO.CloudMode.1.0 device package was deleted, it will not be restored on import.	3.2(1I)
CSCvvh02537	The IpCktEp policy might not be propagated to the leaf switch even after the policy has been configured properly on the Cisco APIC.	3.2(1I)
CSCvvh07062	There will be fault in the Cisco APIC for a remote leaf switch after upgrading the Cisco APIC upgrade or decommissioning and recommissioning the Cisco APIC.	3.2(1I)
CSCvvh07996	There are duplicate CoPP rules in the TCAM.	3.2(1I)
CSCvvh08044	In the case where the user posts policies to download a specific image version and also to upgrade to that version in quick succession before waiting for the image to get downloaded, the current running catalog gets picked up for checking the compatibility. In the event where the current running catalog does not support the newly requested version of the image, the upgrade will fail with the message "version not compatible," even though the user would expect compatibility.	3.2(1I)
CSCvvh12315	The Cisco APIC will not allow the deletion of a remote leaf switch or POD TEP pool if there are any dhcpClient managed objects present with an IP address that is assigned from that TEP pool.	3.2(1I)
CSCvvh13127	There is an issue with upgrading in the following situation: <ul style="list-style-type: none"> ■ A node is decommissioned a few hours before initiating an upgrade. ■ An upgrade is triggered with the "doNotPause" flag turned on in the maintenance group. ■ The node is in the maintenance group that is being upgraded. <p>In this situation, the upgrade stalls while waiting for that node to complete the upgrade.</p>	3.2(1I)
CSCvvh17075	If many unreachable stats export destinations are configured, the observer element on a switch might dump a core and restart.	3.2(1I)
CSCvvh17321	On decommissioning and recommissioning of the Cisco APICs or nodes, extra prefix white list entries might be created on the TOR switches.	3.2(1I)
CSCvvh18069	An iACL entry with a subnet mask of 0 or 32 is not allowed in the CoPP Pre-Filter creation wizard in the GUI.	3.2(1I)

Bugs

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 3.2(1) releases in which the known behavior exists. A bug might also exist in releases other than the 3.2(1) releases.

Table 5 Known Behaviors in This 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.	3.2(1) and later
CSCuo79243	In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.	3.2(1) and later
CSCuo79250	The node ID policy can be replicated from an old appliance that is decommissioned when it joins a cluster.	3.2(1) and later
CSCup47703	The DSCP value specified on an external endpoint group does not take effect on the filter rules on the leaf switch.	3.2(1) and later
CSCup79002	The hostname resolution of the syslog server fails on leaf and spine switches over in-band connectivity.	3.2(1) and later
CSCuq21360	Following a FEX or switch reload, configured interface tags are no longer configured correctly.	3.2(1) and later
CSCur39124	Switches can be downgraded to a 1.0(1) version if the imported configuration consists of a firmware policy with a desired version set to 1.0(1).	3.2(1) and later
CSCur71082	If the Cisco APIC is rebooted using the CIMC power reboot, the system enters into fsck due to a corrupted disk.	3.2(1) and later
CSCus15627	The Cisco APIC Service (ApicVMMSservice) 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.	3.2(1) and later
CSCut51929	The traffic destined to a shared service provider endpoint group picks an incorrect class ID (PcTag) and gets dropped.	3.2(1) 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.	3.2(1) and later

Bugs

Bug ID	Description	Exists in
CSCuu61998	Newly added microsegment EPG configurations must be removed before downgrading to a software release that does not support it.	3.2(1) and later
CSCuu64219	Downgrading the fabric starting with the leaf switch will cause faults such as policy-deployment-failed with fault code F1371.	3.2(1) and later
CSCuw81638	The OpenStack metadata feature cannot be used with Cisco ACI integration with the Juno release (or earlier) of OpenStack due to limitations with both OpenStack and Cisco's ML2 driver.	3.2(1) and later
CSCva32534	Creating or deleting a fabricSetupP policy results in an inconsistent state.	3.2(1) 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.	3.2(1) 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.	3.2(1) and later
CSCva97082	When downgrading 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.	3.2(1) 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.	3.2(1) and later
CSCvg41711	In the leaf mode, the command "template route group <group-name> tenant <tenant-name>" fails, declaring that the tenant passed is invalid.	3.2(1) and later
CSCvg79127	When First hop security is enabled on a bridge domain, traffic is disrupted.	3.2(1) and later
CSCvg81856	Cisco ACI Multi-Site Orchestrator BGP peers are down and a fault is raised for a conflicting rtrId on the fvRtdEpP managed object during L3extOut configuration.	3.2(1) and later
CSCvh76076	The PSU SPROM details might not be shown in the CLI upon removal and insertion from the switch.	3.2(1) and later
CSCvh93612	If two intra-EPG deny rules are programmed—one with the class-eq-deny priority and one with the class-eq-filter priority— changing the action of the second rule to “deny” causes the second rule to be redundant and have no effect. The traffic still gets denied, as expected.	3.2(1) 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*.
- With a non-english SCVMM 2012 R2 or SCVMM 2016 setup and where the virtual machine names are specified in non-english characters, if the host is removed and re-added to the host group, the GUID for all the virtual machines under that host changes. Therefore, if a user has created a micro segmentation endpoint group using “VM name” attribute specifying the GUID of respective virtual machine, then that micro segmentation endpoint group will not work if the host (hosting the virtual machines) is removed and re-added to the host group, as the GUID for all the virtual machines would have changed. This does not happen if the virtual name has name specified in all english characters.
- A query of a configurable policy that does not have a subscription goes to the policy distributor. However, a query of a configurable policy that has a subscription goes to the policy manager. As a result, if the policy propagation from the policy distributor to the policy manager takes a prolonged amount of time, then in such cases the query with the subscription might not return the policy simply because it has not reached policy manager yet.
- When there are silent hosts across sites, ARP glean messages might not be forwarded to remote sites if a 1st generation ToR switch (switch models without -EX or -FX in the name) happens to be in the transit path and the VRF is deployed on that ToR switch, the switch does not forward the ARP glean packet back into the fabric to reach the remote site. This issue is specific to 1st generation transit ToR switches and does not affect 2nd generation ToR switches (switch models with -EX or -FX in the name). This issue breaks the capability of discovering silent hosts.

Compatibility Information

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

Virtualization Compatibility Information

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

- For a table that shows the supported virtualization products, see the ACI Virtualization Compatibility Matrix at the following URL:
<https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/aci/virtualization/matrix/virtmatrix.html>
- This release supports VMM Integration and VMware Distributed Virtual Switch (DVS) 6.5.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 3.2(1)* at the following URL:
<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>
- For information about Cisco APIC compatibility with Cisco UCS Director, see the appropriate *Cisco UCS Director Compatibility Matrix* document at the following URL:
<https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-director/products-device-support-tables-list.html>

- If you use Microsoft vSwitch and want to downgrade to Cisco APIC Release 2.3(1) from a later release, you first must delete any microsegment EPGs configured with the Match All filter.

Hardware Compatibility Information

This release supports the following Cisco APIC servers:

Product ID	Description
APIC-L1	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1000 edge ports)
APIC-L2	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1000 edge ports)
APIC-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 hardware compatibility information:

- For the supported hardware, see the *Cisco NX-OS Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches, Release 13.2(1)* at the following location:
<https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html>
- To connect the N2348UPO to Cisco ACI leaf switches, the following options are available:
 - Directly connect the 40G FEX ports on the N2348UPO to the 40G switch ports on the Cisco ACI leaf switches
 - Break out the 40G FEX ports on the N2348UPO to 4x10G ports and connect to the 10G ports on all other Cisco ACI leaf switches.

Note: A fabric uplink port cannot be used as a FEX fabric port.
- Connecting the Cisco APIC (the controller cluster) to the Cisco ACI fabric requires a 10G interface on the Cisco ACI leaf switch. You cannot connect the Cisco APIC directly to the Cisco N9332PO ACI leaf switch, unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the Cisco N9332PO switch auto-negotiate to 10G without requiring any manual configuration.
- The Cisco N9K-X9736C-FX (ports 29 to 36) and Cisco N9K-C9364C-FX (ports 49-64) switches do not support 1G SFPs with QSA.
- Cisco N9K-C9508-FM-E2 fabric modules must be physically removed before downgrading to releases earlier than Cisco APIC 3.0(1).
- The fifth Cisco N9K-C9508-FM-E2 (also defined as FM-25) is not supported.
- The Cisco N9K-C9508-FM-E2 and N9K-X9736C-FX locator LED enable/disable feature is supported in the GUI and not supported in the Cisco ACI NX-OS Switch CLI.

Compatibility Information

- Contracts using matchDscp filters are only supported on switches with “EX” on the end of the switch name. For example, N9K-93108TC-EX.
- N9K-C9508-FM-E2 and N9K-C9508-FM-E fabric modules in the mixed mode configuration are not supported on the same spine switch.
- The N9K-C9348GC-FXP switch does not read SPROM information if the PSU is in a shut state. You might see an empty string in the Cisco APIC output.
- When the fabric node switch (spine or leaf) is out-of-fabric, the environmental sensor values, such as Current Temperature, Power Draw, and Power Consumption, **might be reported as “N/A.”** A status might be reported as “Normal” even when the Current Temperature is “N/A.”

Adaptive Security Appliance (ASA) Compatibility Information

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

- This release supports Adaptive Security Appliance (ASA) device package version 1.2.5.5 or later.
- If you are running a Cisco Adaptive Security Virtual Appliance (ASA) version that is prior to version 9.3(2), you must configure SSL encryption as follows:

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

Miscellaneous Compatibility Information

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

- This release supports the following software:

- Cisco NX-OS Release 13.0
- Cisco AVS, Release 5.2(1)SV3(3.11)

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

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

- Cisco UCS Manager software release 2.2(1c) or later is required for the Cisco UCS Fabric Interconnect and other components, including the BIOS, CIMC, and the adapter.
- This release supports the following firmware:
 - 4.1(2k) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
 - 4.1(2g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)
 - 4.1(2b) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)
 - 4.1(1g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)
 - 3.0(4l) CIMC HUU ISO (recommended) for UCS C220/C240 M3 (APIC-L1/M1)
 - 3.0(4d) CIMC HUU ISO

Usage Guidelines

- 3.0(3f) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)
 - 3.0(3e) CIMC HUU ISO for UCS C220/C240 M3 (APIC-L1/M1)
 - 2.0(13i) CIMC HUU ISO
 - 2.0(9c) CIMC HUU ISO
 - 2.0(3i) CIMC HUU ISO
- This release supports the partner packages specified in the *L4-L7 Compatibility List Solution Overview* document at the following URL:
<https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/solution-overview-listing.html>
 - A known issue exists with the Safari browser and unsigned certificates, which applies when connecting to the Cisco APIC GUI. For more information, see the *Cisco APIC Getting Started Guide*.
 - For compatibility with OpenStack and Kubernetes distributions, see the *Cisco Application Policy Infrastructure Controller OpenStack and Container Plugins, Release 3.2(1), Release Notes*.

Usage Guidelines

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

Virtualization Compatibility Guidelines

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

- Do not separate virtual port channel (vPC) member nodes into different configuration zones. If the nodes are in different configuration zones, then the vPCs' **modes become mismatched if the interface policies are modified** and deployed to only one of the vPC member nodes.
- If you are upgrading VMware vCenter 6.0 to vCenter 6.5, 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\

```

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

- If the communication between the Cisco APIC and VMware vCenter is impaired, some functionality is adversely affected. The Cisco APIC relies on the pulling of inventory information, updating VDS configuration, and receiving event notifications from the VMware vCenter for performing certain operations.
- After you migrate VMs using a cross-data center VMware vMotion in the same VMware vCenter, you might find a stale VM entry under the source DVS. This stale entry can cause problems, such as host removal failure. The workaround for this problem is to enable "Start monitoring port state" on the vNetwork DVS. See the KB topic

Usage Guidelines


"Refreshing port state information for a vNetwork Distributed Virtual Switch" on the VMware Web site for instructions.

- When creating a vPC domain between two leaf switches, both switches 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 9200 and 9300 platform switches **without "EX" on the end** of the switch name; for example, Cisco Nexus 93120TX.
 - Generation 2—Cisco Nexus 9300-EX and FX platform switches; for example, Cisco Nexus 93108TC-EX.
- The following Red Hat Virtualization (RHV) guidelines apply:
 - We recommend that you use release 4.1.6 or later.
 - Only one controller (compCtrlr) can be associated with a Red Hat Virtualization Manager (RHVM) data center.
 - Deployment immediacy is supported only as pre-provision.
 - IntraEPG isolation, micro EPGs, and IntraEPG contracts are not supported.
 - Using service nodes inside a RHV domain have not been validated.

GUI Guidelines

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



- The  icon in the Cisco APIC opens the menu for Show Me How modules, which provide step-by-step help through specific configurations.
 - If you deviate while in progress of a Show Me How module, you will no longer be able to continue.
 - You must have IPv4 enabled to use the Show Me How modules.
- The Cisco APIC GUI includes an online version of the Quick Start Guide that includes video demonstrations.
- To reach the Cisco APIC CLI from the GUI: choose System > Controllers, highlight a controller, right-click, and choose "launch SSH". To get the list of commands, press the escape key twice.
- The Basic GUI mode is deprecated. We do not recommend using Cisco APIC Basic mode for configuration. However, if you want to use Cisco APIC Basic mode, use the following URL:

`APIC_URL/indexSimple.html`

CLI Guidelines

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

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

Layer 2 and Layer 3 Configuration Guidelines

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

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

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

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

IP Address Guidelines

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

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

Usage Guidelines

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

Miscellaneous Guidelines

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

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

- The Cisco APICs must have 1 SSD and 2 HDDs, and both RAID volumes must be healthy before upgrading to this release. The Cisco APIC will not boot if the SSD is not installed.
- In a multipod fabric setup, if a new spine switch is added to a pod, it must first be connected to at least one leaf switch in the pod. Then the spine switch is able to discover and join the fabric.

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

- For a Cisco APIC REST API query of event records, the Cisco APIC system limits the response to a maximum of 500,000 event records. If the response is more than 500,000 events, it returns an error. Use filters to refine your queries. For more information, see *Cisco APIC REST API Configuration Guide*.
- Subject Alternative Names (SANs) contain one or more alternate names and uses any variety of name forms for the entity that is bound by the Certificate Authority (CA) to the certified public key. These alternate names are **called** "Subject Alternative Names" (SANs). Possible names include:
 - DNS name
 - IP address
- If a node has port profiles deployed on it, some port configurations are not removed if you decommission the node. You must manually delete the configurations after decommissioning the node to cause the ports to return to the default state. To do this, log into the switch, run the `setup-clean-config.sh` script, wait for the script to complete, then enter the reload command.
- When using the SNMP trap aggregation feature, if you decommission Cisco APICs, the trap forward server will receive redundant traps.
- If you upgraded from a release prior to the 3.2(1) release and you had any apps installed prior to the upgrade, the apps will no longer work. To use the apps again, you must uninstall and reinstall them.
- Fabric connectivity ports can operate at 10G or 25G speeds (depending on the model of the APIC server) when connected to leaf switch host interfaces. We recommend connecting two fabric uplinks, each to a separate leaf switch or vPC leaf switch pair.

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

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

Related Documentation

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

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

Related Documentation

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

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

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

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

New Documentation

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

- *Cisco ACI and OpFlex Connectivity for Orchestrators*
- *Cisco ACI Smart Callhome*
- *Cisco ACI Smart Licensing*
- *Cisco ACI TACACS External Logging*
- *Cisco ACI TWAMP*
- *Cisco ACI Virtual Edge Configuration Guide, Release 1.2(1)*
- *Cisco ACI Virtual Edge Health Status*
- *Cisco ACI Virtual Edge Installation Guide, Release 1.2(1)*
- *Cisco ACI Virtual Edge Release Notes, Release 1.2(1)*
- *Cisco ACI Virtualization Guide, Release 3.2(1)*
- *Cisco APIC and Anycast Services*
- *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 3.2(1)*
- *Cisco APIC NX-OS Style CLI Command Reference, Release 3.2(1)*
- *Cisco Application Virtual Switch Configuration Guide, Release 5.2(1)SV3(3.25)*
- *Cisco Application Virtual Switch Installation Guide, Release 5.2(1)SV3(3.25)*
- *Cisco Application Virtual Switch Release Notes, 5.2(1)SV3(3.25)*
- *Verified Scalability Guide for Cisco APIC, Release 3.2(1), Multi-Site, Release 1.2(1) and Cisco Nexus 9000 Series ACI-Mode Switches, Release 13.2(1)*

Related Documentation

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2018-2022 Cisco Systems, Inc. All rights reserved.