



# Cisco Application Policy Infrastructure Controller Release Notes, Release 2.1(4)

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

Note: Use this document in combination with the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.1(4)*, which you can view at the following location:

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

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

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

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

You can watch videos that demonstrate how to perform specific tasks in the 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
March 14, 2018	2.1(4a): Release 2.1(4a) became available.
April 4, 2018	2.1(4a): In the Open Bugs section, added bug CSCvi33259.
September 17, 2019	2.1(4a): In the Open Bugs section, added bug CSCuu17314.
October 4, 2019	In the Miscellaneous Guidelines section, added the following bullet: <ul style="list-style-type: none"><li>■ 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 infraFexBndIgrp managed object.</li></ul>

## Contents

This document includes the following sections:

- Introduction
- Compatibility Information
- Usage Guidelines
- Verified Scalability Limits
- New and Changed Information
- Bugs
- Related Documentation

## 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 ACI, including a glossary of terms that are used in the 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 12.1(4)
  - Cisco AVS, Release 5.2(1)SV3(2.1)

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>

- The breakout of 40G ports to 4x10G on the N9332PQ switch is not supported in ACI-Mode.
- To connect the N2348UPQ to 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

Usage Guidelines

- 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.
- This release supports the following firmware:
  - 1.5(4e) CIMC HUU iso
  - 2.0(3i) CIMC HUU iso
  - 2.0(9c) 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.x. For more information about guidelines for upgrading VMware DVS from 5.x to 6.x and VMM integration, see the *Cisco ACI Virtualization Guide, Release 2.1(2)* at the following URL:  
<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>
- This release supports the Microsoft System Center Virtual Machine Manager (SCVMM) Update Rollup 9 and 10 releases, and the Microsoft Windows Azure Pack Update Rollup 9 and 10 releases.
- 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 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>

## Usage Guidelines

This section lists usage guidelines for the APIC software.

- The 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 APIC does not provide IPAM services for tenant workloads.
- To reach the APIC CLI from the GUI: select System > Controllers, highlight a controller, right-click and select "launch SSH". To get the list of commands, press the escape key twice.
- In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.
- For the following services, use a DNS-based host name with out-of-band management connectivity. IP addresses can be used with both in-band and out-of-band management connectivity.
  - Syslog server
  - Call Home SMTP server
  - Tech support export server
  - Configuration export server
  - Statistics export server
- Both leaf and spine switches can be managed from any host that has IP connectivity to the fabric.
- If an IP address is learned on one of two endpoints for which you are configuring an atomic counter policy, you should use an IP-based policy and not a client endpoint-based policy.
- When configuring two Layer 3 external networks on the same node, the loopbacks need to be configured separately for both Layer 3 networks.
- All endpoint groups (EPGs), including application EPGs and Layer 3 external EPGs, require a domain. Interface policy groups must also be associated with an Attach Entity Profile (AEP), and the AEP must be associated with domains. Based on the association of EPGs to domains and of the interface policy groups to domains, the ports and VLANs that the EPG uses are validated. This applies to all EPGs including bridged Layer 2 outside and routed Layer 3 outside EPGs. For more information, see the *Cisco Fundamentals Guide* and the *KB: Creating Domains, Attach Entity Profiles, and VLANs to Deploy an EPG on a Specific Port* article.

**Note:** When creating static paths for application EPGs or Layer 2/Layer 3 outside EPGs, the physical domain is not required. Upgrading without the physical domain will raise a fault on the EPG stating "invalid path configuration."
- An EPG can only associate with a contract interface in its own tenant.
- User passwords must meet the following criteria:
  - Minimum length is 8 characters
  - Maximum length is 64 characters
  - Fewer than three consecutive repeated characters

- At least three of the following character types: lowercase, uppercase, digit, symbol
  - Cannot be easily guessed
  - Cannot be the username or the reverse of the username
  - Cannot be any variation of " cisco" , " isco" , or any permutation of these characters or variants obtained by changing the capitalization of letters therein
- The power consumption statistics are not shown on leaf node slot 1. You must view the statistics from any other node.
  - For Layer 3 external networks created through the API or Advanced GUI and updated through the CLI, protocols need to be enabled globally on the external network through the API or Advanced GUI, and the node profile for all the participating nodes needs to be added through the API or Advanced GUI before doing any further updates through the CLI.
  - For Layer 3 external networks created through the Basic GUI or CLI, you should not to update them through the API. These external networks are identified by names starting with " \_\_ui\_ " .
  - The output from " show" commands issued in the NX-OS-style CLI are subject to change in future software releases. Cisco does not recommend using the output from the show commands for automation.
  - The CLI is supported only for users with administrative login privileges.
  - Do not separate virtual port channel (vPC) member nodes into different configuration zones. If the nodes are in **different configuration zones, then the vPCs' modes become mismatched if the interface policies are modified** and deployed to only one of the vPC member nodes.
  - If you defined multiple login domains, you can choose the login domain that you want to use when logging in to an 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 max 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
  - The Cisco Discovery Protocol (CDP) is not supported in policies that are used on FEX interfaces.
  - 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.

Verified Scalability Limits

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

### New Software Features

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

Table 2 New Software Features, Guidelines, and Restrictions

Feature	Description	Guidelines and Restrictions
Support for third-party Micron Solid State Drive (SSD) firmware auto update	During the boot up sequence, the firmware is checked and updated, if needed, to the recommended firmware version as according to Micron SSD.	None.

### New Hardware Features

For new hardware features, see the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.1(4)* at the following location:

## Bugs

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

## Changes in Behavior

There are no changes in behavior in this release.

## 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 2.1(4) releases in which the bug exists. A bug might also exist in releases other than the 2.1(4) releases.

Table 3 Open Bugs in the 2.1(4) Release

Bug ID	Description	Exists in
<a href="#">CSCuu17314</a>	CDP is not enabled on the management interfaces for the leaf switches and spine switches.	2.1(4a) and later
<a href="#">CSCyb22898</a>	When using the Advanced Encryption Standard (AES) encryption in the CLI, the passphrase displays in plain text.	2.1(4a) and later
<a href="#">CSCvb35030</a>	After upgrading to the 2.1(2) release from the 2.0(1) release, one IP of a vPC goes down. The IP comes back up due to a modify process, such as incrementing the IP on one leg and submitting, or due to deleting or adding the configuration on the logical interface profile of the L3Out.	2.1(4a) and later
<a href="#">CSCvb35148</a>	A fault gets raised when configuring PIM with SVI, and the fault does not get cleared even after removing the interface from SVI.	2.1(4a) and later
<a href="#">CSCvb45887</a>	LLDP/CDP adjacency faults get raised on the APIC for AVS, but the faults are not relevant for AVS.	2.1(4a) and later
<a href="#">CSCvb46199</a>	There are downgrade issues from the 2.1(2) release to the 2.0(2) release when the VMM and EPG are in different encapsulations.	2.1(4a) and later

## Bugs

Bug ID	Description	Exists in
<a href="#">CSCv49441</a>	Adding an image to the repository fails intermittently, regardless if the image was added by downloading it using the GUI or API, or uploading it using the GUI or API.	2.1(4a) and later
<a href="#">CSCv51008</a>	In the Edit VMM Domain Association dialog box, changing the VLAN mode and then clicking Cancel does not undo the VLAN mode change.	2.1(4a) and later
<a href="#">CSCvc23017</a>	If there are changes made in the RBAC policy prior to the upgrade from a 2.0 release to a 2.1 or later release, the process policy manager (policymgr) might continuously crash on the APIC.	2.1(4a) and later
<a href="#">CSCvd09418</a>	A message indicating a successful upgrade is seen within 20 minutes when upgrading a Cisco APIC. In comparison, upgrading a leaf switch with a large TCAM will take up to 90 minutes to bring up the port channels for use with compute or L3Outs.  After successfully upgrading the first VPC leaf switch, if you start a peer upgrade, you will have <b>traffic loss until the first leaf switch's port channel comes up.</b>	2.1(4a) and later
<a href="#">CSCvf29474</a>	Border leaf switch interface might take up to 50 minutes to come appear in Cisco APIC.	2.1(4a) and later
<a href="#">CSCvi33259</a>	Attempting to downgrade from a 2.3(1) release to the 2.1(4) release fails with the following error message:  firmware not compatible	2.1(4a) and later
<a href="#">CSCvp64280</a>	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:  <a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-n9kaci-bypass">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-n9kaci-bypass</a>	2.1(4a) 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 2.1(4) Release

Bug ID	Description	Fixed in
<a href="#">CSCuw91050</a>	The Cisco APIC dumps core files, and the affected Cisco APICs cannot fully join the cluster or might be stuck in a "data layer partially diverged" state.	2.1(4a)
<a href="#">CSCvb55909</a>	Using "_" in an SCVMM domain name on a Cisco APIC, the configuration of the Cisco ACI plan fails. For example: "ACI_SCVMM" does not work as VMM domain name.	2.1(4a)
<a href="#">CSCvc85195</a>	The policyelem process crashes because of MTS buffer exhaustion while sending messages to the eventmgr process.	2.1(4a)
<a href="#">CSCve34392</a>	Tracking of VM and NiC information for an end point is incorrect. The managed objects fvRsToVm and fvRsToVm are missing for some fvEpDefRef managed objects.	2.1(4a)
<a href="#">CSCve52382</a>	Tracking of VM and NiC information for an endpoint is incorrect. The managed objects fvRsToVm and fvRsToVm are missing for some fvEpDefRef managed objects.	2.1(4a)
<a href="#">CSCve81037</a>	Tracking of VM and NiC information for an endpoint is incorrect. The managed objects fvRsToVm and fvRsToVm are missing for some fvEpDefRef managed objects.	2.1(4a)
<a href="#">CSCve92142</a>	A filter is pointing the concrete object of another filter. As the result, an incorrect ACL entry will be installed on leaf switches or open virtual switches.	2.1(4a)
<a href="#">CSCve96001</a>	There are out of memory failures for NX-OS processes such as BGP.	2.1(4a)
<a href="#">CSCvf16377</a>	If Sched A is associated with a fabric node firmware MaintPol, then if that MaintPol is deleted, Sched A is also deleted.  The behavior above occurs even if Sched A is also associated with other policies such as Config Export Policy and Techsupport Export Policy. Because Sched A is deleted, the config export policy and techsupport export policy using Sched A will have the fault "Failed to form relation to MO schedp-[sched_name] of class trigSchedP in context.	2.1(4a)
<a href="#">CSCvf17828</a>	If a subnet is created with an IPv6 address with /53 as the subnet mask, the GUI does not validate this address.	2.1(4a)
<a href="#">CSCvf35265</a>	System controller's status is "standby" after reloading.	2.1(4a)
<a href="#">CSCvf66682</a>	There is a global station table stale entry.	2.1(4a)
<a href="#">CSCvf91599</a>	A service object group cannot be created or edited from the Cisco APIC GUI when importing an XML configuration from one data center to another. The parameter "service object group" is missing and previously configured object groups cannot be added or edited.	2.1(4a)

## Bugs

Bug ID	Description	Fixed in
<a href="#">CSCvg09830</a>	<p>In the Microsoft Windows Azure Pack (WAP) GUI, in the admin portal, in the Plan -&gt; Networking (ACI) section, if you create and save the plan, then all available services are checked by default. In the tenant portal, if the plan only has one shared service, this is not an issue as there is no doubt as to which services are available. The tenant can be confused as to which service is available when there are two or more shared services marked.</p> <p>When checking the Cisco APIC GUI to investigate the if the shared services were actually created, there are no abnormal findings regarding the intended configuration. The imported contracts of the consumer tenants will be created after WAP tenants have checked and applied the shared service in the tenant portal, as per the normal workflow.</p>	2.1(4a)
<a href="#">CSCvg17850</a>	<p>If SCVMM loses communication with the DNS server, the Cisco APIC Agent Service cannot resolve the fully qualified domain name of the VMM cluster host name and the Cisco APIC Agent Service starts to delete the vmmDomain and logical network.</p> <p>Also, the PS command fails to delete the logical network, but the logical network gets deleted on SCVMM without any change in the Cisco APIC.</p>	2.1(4a)
<a href="#">CSCvg22348</a>	The warning message is incorrect when a user decommissions a Cisco APIC.	2.1(4a)
<a href="#">CSCvg24076</a>	/data/log is 100% full due to multiple 21M log files.	2.1(4a)
<a href="#">CSCvg24772</a>	<p>With SCVMM integration, when creating a network from the Windows Azure Pack portal, the port reports an error message similar to the following example:</p> <p style="padding-left: 40px;">network name is too long, use a shorter network name</p> <p>The network fails to be created and no endpoint group is programmed in the Cisco APIC.</p>	2.1(4a)
<a href="#">CSCvg32919</a>	One or more Cisco APICs are in a Data Layer Partially Diverged state. Running "show cores" on a Cisco APIC shows core files for the svc_ifc_observer process. Running "ps -ef   grep observer" shows that there is no svc_ifc_observer process running.	2.1(4a)
<a href="#">CSCvg48627</a>	<p>The Cisco APIC GUI allows users to configure an Out-of-Band Contract with a Directive of Logging when this is not supported, which can lead to the following programming fault being generated:</p> <p>actrl-provisioning-failed rule failed due to software programming error</p>	2.1(4a)
<a href="#">CSCvg60902</a>	<p>The VMMMgr process crashes shortly after being started. The VMMMgr logs show the following error right before the crash:</p> <p>UNCONDITIONAL ASSERT () (IHPNicMo != __null) failed @        ../svc/vmmmgr/src/gen/ifc/app/./imp/comp/TaskCompHPNicAddorDelVtepNicImp.cc:126</p>	2.1(4a)
<a href="#">CSCvg96793</a>	All ESXi hosts show as disconnected under the VMM integration when you click on the VMM domain. The VMware vCenter might still show as online. The svc_ifc_opflexelem.log file for the leaf switches will show DVS as not found.	2.1(4a)

## Bugs

Bug ID	Description	Fixed in
<a href="#">CSCvh16532</a>	When attempting to log into the Cisco APIC GUI, you might receive the error "AAA Server Authentication DENIED."  You might also see the following message in a network trace when the LDAP server responds to the Cisco APIC's search query: "In order to perform this operation a successful bind must be completed."	2.1(4a)

## 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 2.1(4) releases in which the known behavior exists. A bug might also exist in releases other than the 2.1(4) releases.

Table 5 Known Behaviors in the 2.1(4) Release

Bug ID	Description	Exists in
<a href="#">CSCuo52668</a>	The 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.	2.1(4a) and later
<a href="#">CSCuo79243</a>	In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.	2.1(4a) and later
<a href="#">CSCuo79250</a>	The node ID policy can be replicated from an old appliance that is decommissioned when it joins a cluster.	2.1(4a) and later
<a href="#">CSCup47703</a>	The DSCP value specified on an external endpoint group does not take effect on the filter rules on the leaf switch.	2.1(4a) and later
<a href="#">CSCup79002</a>	The hostname resolution of the syslog server fails on leaf and spine switches over in-band connectivity.	2.1(4a) and later
<a href="#">CSCuq21360</a>	Following a FEX or switch reload, configured interface tags are no longer configured correctly.	2.1(4a) and later
<a href="#">CSCur39124</a>	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).	2.1(4a) and later
<a href="#">CSCur71082</a>	If the APIC is rebooted using the CIMC power reboot, the system enters into fsck due to a corrupted disk.	2.1(4a) and later
<a href="#">CSCus15627</a>	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.	2.1(4a) and later
<a href="#">CSCut51929</a>	The traffic destined to a shared service provider endpoint group picks an incorrect class ID (PcTag) and gets dropped.	2.1(4a) and later
<a href="#">CSCuu09236</a>	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.	2.1(4a) and later

## Bugs

Bug ID	Description	Exists in
<a href="#">CSCuu61998</a>	Newly added microsegment EPG configurations must be removed before downgrading to a software release that does not support it.	2.1(4a) and later
<a href="#">CSCuu64219</a>	Downgrading the fabric starting with the leaf switch will cause faults such as policy-deployment-failed with fault code F1371.	2.1(4a) and later
<a href="#">CSCuw81638</a>	The OpenStack metadata feature cannot be used with ACI integration with the Juno release (or earlier) of OpenStack due to limitations with both OpenStack and Cisco's ML2 driver.	2.1(4a) and later
<a href="#">CSCva32534</a>	Creating or deleting a fabricSetupP policy results in an inconsistent state.	2.1(4a) and later
<a href="#">CSCva60439</a>	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 APIC uses open source DHCP, which creates some resources that the APIC cannot delete when a pod is deleted.	2.1(4a) and later
<a href="#">CSCva86794</a>	When an APIC cluster is upgrading, the 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 APICs finish the upgrade and the cluster comes out of minority.	2.1(4a) and later
<a href="#">CSCva97082</a>	When downgrading from a 2.1(2) 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.	2.1(4a) and later
<a href="#">CSCvb39702</a>	No fault gets raised upon using the same encapsulation VLAN in a copy device in tenant common, even though a fault should get raised.	2.1(4a) 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*.
- If you have VLAN pools that are colliding with an infra VLAN and you upgrade to the 2.3(1) release, if you upgrade the CIMC firmware from pre-2.3(1) to post-2.3(1), you will see the following fault: Error:400 - Encapsulation value ? collides with INFRA.

## 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 tables describe the core APIC documentation.

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

Table 6 Release Notes

Document	Description
<i>Cisco ACI Simulator Release Notes, Release 2.1(4)</i>	Provides release information for the Cisco ACI Simulator product.
<i>Cisco Application Policy Infrastructure Controller, Release 2.1(4), Release Notes</i>	This document. Provides release information for the Application Policy Infrastructure Controller (APIC) product.
<i>Cisco Nexus 9000 Series ACI-Mode Switch FPGA/EPLD Upgrade Release Notes, Release 12.1(4)</i>	Provides release information for the Cisco Nexus 9000 series ACI-mode switch FPGA/EPLD product.
<i>Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.1(4)</i>	Provides release information for the Cisco NX-OS for Cisco Nexus 9000 series ACI-mode switches product.

Table 7 Installation, Upgrade, and Configuration Documentation

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

## Related Documentation

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

Table 8 Interface Documentation

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

Table 9 Reference Documentation

Document	Description
----------	-------------

## Related Documentation

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

Table 10 Layer 4 to Layer 7 Documentation

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

Table 11 Virtualization Documentation

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

Table 12 Cisco ACI with OpenStack Documentation

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

Table 13 Troubleshooting Documentation

Document	Description
<i>Cisco APIC Troubleshooting Guide</i>	Describes how to troubleshoot common APIC issues.
<i>Troubleshooting Cisco Application Centric Infrastructure</i>	Additional information about how to troubleshoot common APIC issues.



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](http://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.

© 2016–2019 Cisco Systems, Inc. All rights reserved.