Cisco Application Policy Infrastructure Controller Release Notes, Release 2.1(1)

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

Note: Use this document in combination with the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.1(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

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
October 2, 2016	2.1(1h): Release 2.1(1h) became available.
October 17, 2016	2.1(1h): Moved open bug CSCvb39702 to the known behaviors section. Removed open bugs CSCvb28090 and CSCva47275. Moved resolved bugs CSCva49352 and CSCva62763 to the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.1(1)* document.
October 20, 2016	In the Usage Guidelines section, added "ACI does not support a class E address as a VTEP address."
October 21, 2016	In the New Software Features section, changed instances of "N9K-C93180YC-EX" and "93xx-EX" to "9300-EX".
November 1, 2016	2.1(1h): Updated the resolved bugs table with an entirely new list.

Date	Description
November 10, 2016	In the Changes in Behavior section, added the following things: ■ You can now use the Layer 3 EVPN services over fabric WAN feature on 9300-EX switches. ■ You can now use the multipod feature and Layer 3 EVPN services over fabric WAN feature together on 9300-EX switches.
November 11, 2016	In the Usage Guidelines section, added a bullet about infra L3extOuts used for Layer 3 EVPN control plane connectivity. In the Changes in Behavior section, added that multiple infra L3Outs per POD are now supported.
November 29, 2016	In the Compatibility Informaiton section, added the 2.0(9c) CIMC HUU iso as a supported version.
November 30, 2016	2.1(1h): In the Open Bugs section, added bug CSCvc23017.
December 6, 2016	In the Compatibility Information section, added information about a known issue when using the Safari browser to connect to the APIC.
December 8, 2016	In the Compatibility Information section, changed the sentence that begins with "By using two AVS VMM domains (one with VLAN and one with VXLAN)..." to "By using using an AVS VMM domain with both VLAN and VXLAN..." In the Changes in Behavior section, added "You can now use both the VLAN mode and VXLAN mode on the same Cisco Application Virtual Switch (AVS)."
December 22, 2016	2.1(1i): Release 2.1(1i) became available; there are no changes to this document for this release.
February 14, 2017	In the Compatibility Information section, changed: Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the N9396PX or N9372PX switches To: Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the 10G ports on all other ACI leaf switches Note: A fabric uplink port cannot be used as a FEX fabric port.
February 28, 2017	In the Usage Guidelines section, added: If the communication between the APIC and vCenter is impaired, some functionality is adversely affected. The APIC relies on the pulling of inventory information, updating vDS configuration, and receiving event notifications from the vCenter for performing certain operations.

Date	Description
April 17, 2017	Removed deprecated Knowledge Base articles.
November 20, 2017	In the Usage Guidelines section, changed a mention of “Virtual Private Cloud (VPC)” to “virtual port channel (vPC).”
April 11, 2018	In the Compatibilty Information section, changed the supported Cisco AVS release to 5.2(1)SV3(2.5).
August 5, 2019	2.1(1h): In the Open Bugs section, added bug CSCvb94260.
September 17, 2019	2.1(1h): In the Open Bugs section, added bug CSCuu17314.
October 4, 2019	In the Miscellaneous Guidelines section, added the following bullet: ■ When you create an access port selector in a leaf interface rofile, the fexId property is configured with a default value of 101 even though a FEX is not connected and the interface is not a FEX interface. The fexId property is only used when the port selector is associated with an infraFexBndlGrp managed object.

Contents

This document includes the following sections:

Introduction

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

The *Cisco Application Centric Infrastructure Fundamentals* guide provides complete details about the 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(1)
  - Cisco AVS, Release 5.2(1)SV3(2.5)

    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

- 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(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
- 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.

- 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 infraFexBndlGrp managed object.

Verified Scalability Limits

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

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

You can access these documents from the following website:

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

New and Changed Information

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

New Software Features

Table 2 lists the new software features in this release:

Table 2 New Software Features, Guidelines, and Restrictions

Feature	Description	Guidelines and Restrictions
64-Way ECMP	64-way ECMP can be enabled on external links for the following switches: • N9K-X9736C-EX • N9K-X9732C-EX • N9K-C9504-FM-E • N9K-C9508-FM-E	None.
ACI Security Microsegmentation Closed Loop Feedback Solution with FirePOWER NGIPS for AVS, vDS, and Bare-Metal Workloads	The FirePOWER Next-Generation Intrusion Prevention System (NGIPS) can be used for vulnerability detection, which then performs automatic microsegmentation of rogue endpoints in ACI fabric for Cisco Application Virtual Switch (AVS), VMware vSphere Distributed Switch (VDS), and Bare-Metal workloads.	In the case of dynamic EPG deployment of ACI with DVS, this feature will only work on 9300-EX switches. This is because microsegmentation is only supported for DVS on 9300-EX switches. The host and virtual machine, which are the source of an external attack, must be connected to a 9300-EX switch.
Advertising EVPN Type 2 Host Routes	For optimal traffic forwarding in an EVPN topology, you can enable fabric spines to advertise host routes using EVPN type 2 (MAC-IP) routes to the DCIG along with public bridge domain subnets in the form of BGP EVPN type 5 (IP prefix) routes.	None.
Contract Permit Logging Support for Multipod	The contract permit logging feature is now supported with multipod.	This feature is supported only on 9300-EX switches.
Copy Services Support for Multipod	The copy services feature is now supported with multipod.	This feature is supported only on 9300-EX switches.

Feature	Description	Guidelines and Restrictions
Explicit Prefix List Support for Route Maps/Profile Enhancement	In the APIC, for public bridge domain subnets and external transit networks, inbound and outbound route controls are provided through an explicit prefix list. An explicit prefix list presents an alternate method of usage and is defined through a new match type that is called the "match route destination" (rtctrlMatchRtDest). The explicit prefix list is used for advertising bridge domain subnets through the bridge domain to the Layer 3 Outside relation and specifying a subnet in the l3extInstP with export/import route control for advertising transit and external networks. For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide*.	None.
Federal Information Processing Standards Support	The APIC can be configured the to use the Federal Information Processing Standards (FIPS) for cryptography.	None.
Global Toggling Between In-band Management and Out-of-band Management	A global toggle is implemented between in-band management connectivity and out-of-band management connectivity as the default connectivity mode between the APIC server and management devices external to the ACI fabric.	None.
IGMP Snooping	The APIC provides support for the following IGMP-related features: • Static port group implementation–IGMP static port grouping enables you to pre-provision ports that are already statically-assigned to an application EPG as the switch ports to receive and process IGMP multicast traffic. This pre-provisioning prevents the flooding of all ports on a bridge domain with Layer 2 multicast traffic. • Access group configuration for application EPGs–An access-group is used to control what streams can be joined behind a given port. For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide*.	Static group membership can be pre-provisioned only on static ports assigned to an application EPG. For access groups, only route-map-based access groups are allowed.
IP Address-Based Microsegmented Endpoint Groups Configured as Shared Services	IP address-based microsegmented endpoint groups can be configured as shared services, accessible by devices located on VRFs other than the one on which the endpoint group is located.	This configuration can only be applied to unicast IP addresses with a 32-bit netmask. For example: 125.125.125.111/32.
IP Aging	This feature tracks and ages unused IPs on an endpoint. For more information, see the *Cisco APIC Layer 3*	None.

Feature	Description	Guidelines and Restrictions
	Networking Configuration Guide.	
Layer 3 Multicast Support for Multipod	Layer 3 multicast is now supported with multipod. For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide*.	None.
Network-Based Microsegmented Endpoint Group Support on Bare-Metal Environments	Configuration of microsegmented endpoint groups based on MAC address or IP address attributes is now supported on physical as well as virtual environments.	None.
Policy-Based Redirect Support for Multipod	The policy-based redirect feature is now supported with multipod.	None.
Port Security Support	The port security feature is now supported on the 9300-EX switches.	None.
Translating QoS Ingress Markings to Egress Markings	The APIC enables translating the 802.1P Class of Service (CoS) field based on the ingress DSCP value. This functionality enables the ACI fabric to classify the traffic for devices that classify the traffic based only on the CoS value. The functionality also allows you to derive the dot1P CoS field based on the ingress dot1P value.	
Trunk Port Group	Trunk port groups can be used to aggregate the traffic of endpoint groups. For more information, see the *Cisco ACI Virtualization Guide, Release 2.1(1)* and *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 2.1(1)*.	Supported only under a VMware domain.
User-Identity Microsegmentation with FirePOWER and ACI for Secure VDI	You can now have a secure VDI deployment based on user-identity microsegmentation using FirePOWER and Active Directory integration. The solution works by applying an NAC policy to provide secure access to endpoints in a server endpoint group within the ACI fabric.	None.
Windows Azure Pack Enhancements	In the Windows Azure Pack tenant portal GUI, you can now add and provide a new context name while creating a bridge domain. In the Windows Azure Pack tenant portal GUI for a virtual private cloud (VPC) plan, the tenant can now delete a context. For more information, see the *Cisco ACI Virtualization Guide, Release 2.1(1)*.	None.

New Hardware Features

For new hardware features, see the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.1(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

This section lists changes in behavior in this release.

- In the APIC GUI, “Route Profiles” are renamed.
  - In the Navigation pane and Work pane, “Route Profiles" are now referred to as "Route Maps/Profiles".
  - The “Create Route Profile” action and its dialog box are now referred to as “Create Route Map”.
- You can now use the Layer 3 EVPN services over fabric WAN feature on 9300-EX switches.
- You can now use the multipod feature and Layer 3 EVPN services over fabric WAN feature together on 9300-EX switches.
- Multiple infra L3Outs per POD are now supported. Each POD can have one infra L3Out with a different OSPF area ID assigned to it.
- You can now use both the VLAN mode and VXLAN mode on the same Cisco Application Virtual Switch (AVS).

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(1) releases in which the bug exists. A bug might also exist in releases other than the 2.1(1) releases.

Table 3 Open Bugs in the 2.1(1h) Release

Bug ID	Description	Exists in
CSCuu17314	CDP is not enabled on the management interfaces for the leaf switches and spine switches.	2.1(1h) and later

Bug ID	Description	Exists in
CSCvb22898	When using the Advanced Encryption Standard (AES) encryption in the CLI, the passphrase displays in plain text.	2.1(1h) and later
CSCvb35030	After upgrading to the 2.1(1) release from the 2.0(1) release, one IP of a vPC goes down. The IP comes back up due to a modify process, such as incrementing the IP on one leg and submitting, or due to deleting or adding the configuration on the logical interface profile of the L3Out.	2.1(1h) and later
CSCvb35148	A fault gets raised when configuring PIM with SVI, and the fault does not get cleared even after removing the interface from SVI.	2.1(1h) and later
CSCvb45887	LLDP/CDP adjacency faults get raised on the APIC for AVS, but the faults are not relevant for AVS.	2.1(1h) and later
CSCvb46199	There are downgrade issues from the 2.1(1) release to the 2.0(2) release when the VMM and EPG are in different encapsulations.	2.1(1h) and later
CSCvb49441	Adding an image to the repository fails intermittently, regardless if the image was added by downloading it using the GUI or API, or uploading it using the GUI or API.	2.1(1h) and later
CSCvb51008	In the Edit VMM Domain Association dialog box, changing the VLAN mode and then clicking Cancel does not undo the VLAN mode change.	2.1(1h) and later
CSCvb94260	Symptom #1. For a three node APIC cluster, APIC2 or APIC3 or both may stuck at 75% waiting for lower nodes completing the upgrade, even after APIC1 has been upgraded successfully. However, the APIC2 and APIC3 "acidiag avread" output shows that APIC1's version is still the previous version. Symptom #2. All three APICs have been upgraded successfully and become fully fit. The "acidiag avread" output for the APICs shows that only the local APIC is running the newer version while the other two APICs are running the previous version.	2.1(1h) and later
CSCvc23017	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(1h) and later

Bug ID	Description	Exists in
CSCvp64280	A vulnerability in the fabric infrastructure VLAN connection establishment of the Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an unauthenticated, adjacent attacker to bypass security validations and connect an unauthorized server to the infrastructure VLAN. The vulnerability is due to insufficient security requirements during the Link Layer Discovery Protocol (LLDP) setup phase of the infrastructure VLAN. An attacker could exploit this vulnerability by sending a malicious LLDP packet on the adjacent subnet to the Cisco Nexus 9000 Series Switch in ACI mode. A successful exploit could allow the attacker to connect an unauthorized server to the infrastructure VLAN, which is highly privileged. With a connection to the infrastructure VLAN, the attacker can make unauthorized connections to Cisco Application Policy Infrastructure Controller (APIC) services or join other host endpoints. Cisco has released software updates that address this vulnerability. There are workarounds that address this vulnerability. This advisory is available at the following link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-n9kaci-bypass	2.1(1h) 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(1) Release

Bug ID	Description	Fixed in
CSCuz01754	The fault "Port is down, reason:noOperMembers(connected), used by:EPG" is classified as F0532 fltEthpmIfPortDownInfraEpg, even when there is no Infra on that port.	2.1(1h)
CSCuz33199	The F1800 “actrl-resource-unavailable” and F1801 “actrl-resource-unavailable” faults get raised in a condition where there is a bridge domain subnet present and the same subnet is also configured under an L3out for the same VRF.	2.1(1h)
CSCva21366	APICs are dropped out of the cluster due to a changed chassisID under avread. Check avread on all three APICs and the leaf switches with APICs that are connected to them.	2.1(1h)
CSCva28754	In the APIC GUI, under Fabric > Access Policies > Profiles > FEX Profile > Interface Selectors for FEX, there is functionality to sort, but the sort is not working correctly. The GUI is showing unexpected behavior and does not match the sorting function as in other portions of the GUI.	2.1(1h)
CSCva36618	The out-of-band management IP address is not configured on the interface of the APIC, even though there is a static node management address configured.	2.1(1h)

Bug ID	Description	Fixed in
CSCva56307	Policy group and interface override policies are prefixed with “__ui_” when created through the advanced GUI. However, these policies should not have this prefix when created through the advanced GUI.	2.1(1h)
CSCva68670	When an administrator runs the "show events" command with a specific time frame from the APIC CLI, the returned output displays events that do not match the specified time frame.	2.1(1h)
CSCva73290	The controllers cannot see the name of the leaf switch to which they are connected in the web interface under fabric and fabric membership. The “show switch” command in the APIC CLI does show the names of all switches correctly.	2.1(1h)
CSCva77846	An RBAC-configured user that is mapped to a security domain and Tenant cannot see the application profiles line in the GUI if the configuration was created when one leaf switch was down. When an RBAC domain is updated, the update is not sent to the NGINX DME in the leaf switches or in other APICs, which causes this behavior to happen.	2.1(1h)
CSCva79604	EIGRP failed to redistribute a direct attach subnet that belongs to another L3out.	2.1(1h)
CSCva94456	Stale rules and endpoint profile remained in old leaf switches after AVS migration to new leaf switches.	2.1(1h)
CSCva95211	If a scheduler is mapped to two maintenance groups, deleting one maintenance group removes the schedulers.	2.1(1h)
CSCvb01840	Common tenant relay policies are displayed when selecting the policies in a user tenant.	2.1(1h)
CSCvb03981	A recurring snapshot cannot be created per tenant by using configuration rollback.	2.1(1h)
CSCvb10039	After fabric discovery, the following fault display: "Specified node not present in the specified pod."	2.1(1h)
CSCvb10727	When creating IP address pool in the mgmt tenant, the address block does not pass validation.	2.1(1h)
CSCvb13193	The access.log file of Nginx was moved to the /var/log/dme/log directory, but the access.log file is not auto-rotated.	2.1(1h)
CSCvb34479	The error "TypeError: Cannot read property 'findParentRecord' of null" displays when using the APIC Visibility and Troubleshooting dialog.	2.1(1h)
CSCvb73132	The VPCs in VPC pairs have different VPC IDs, which prevents the VPCs from coming up.	2.1(1h)

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(1) releases in which the known behavior exists. A bug might also exist in releases other than the 2.1(1) releases.

Table 5 Known Behaviors in the 2.1(1) Release

Bug ID	Description	Exists in

Bug ID	Description	Exists in
CSCuo52668	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(1h) and later
CSCuo79243	In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.	2.1(1h) and later
CSCuo79250	The node ID policy can be replicated from an old appliance that is decommissioned when it joins a cluster.	2.1(1h) and later
CSCup47703	The DSCP value specified on an external endpoint group does not take effect on the filter rules on the leaf switch.	2.1(1h) and later
CSCup79002	The hostname resolution of the syslog server fails on leaf and spine switches over in-band connectivity.	2.1(1h) and later
CSCuq21360	Following a FEX or switch reload, configured interface tags are no longer configured correctly.	2.1(1h) and later
CSCur39124	Switches can be downgraded to a 1.0(1x) version if the imported configuration consists of a firmware policy with a desired version set to 1.0(1x).	2.1(1h) and later
CSCur71082	If the APIC is rebooted using the CIMC power reboot, the system enters into fsck due to a corrupted disk.	2.1(1h) and later
CSCus15627	The Cisco APIC Service (ApicVMMService) shows as stopped in the Microsoft Service Manager (services.msc in control panel > admin tools > services). This happens when a domain account does not have the correct privilege in the domain to restart the service automatically.	2.1(1h) and later
CSCut51929	The traffic destined to a shared service provider endpoint group picks an incorrect class ID (PcTag) and gets dropped.	2.1(1h) and later
CSCuu09236	Traffic from an external Layer 3 network is allowed when configured as part of a vzAny (a collection of endpoint groups within a context) consumer.	2.1(1h) and later
CSCuu61998	Newly added microsegment EPG configurations must be removed before downgrading to a software release that does not support it.	2.1(1h) and later
CSCuu64219	Downgrading the fabric starting with the leaf switch will cause faults such as policy-deployment-failed with fault code F1371.	2.1(1h) and later
CSCuw81638	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(1h) and later
CSCva32534	Creating or deleting a fabricSetupP policy results in an inconsistent state.	2.1(1h) 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 APIC uses open source DHCP, which creates some resources that the APIC cannot delete when a pod is deleted.	2.1(1h) and later
CSCva86794	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(1h) and later

Bug ID	Description	Exists in
CSCva97082	When downgrading from a 2.1(1) release to a 2.0(1) release, the spines and its interfaces must be moved from infra L3out2 to infra L3out1. After infra L3out1 comes up, delete L3out2 and its related configuration, and then downgrade to a 2.0(1) release.	2.1(1h) and later
CSCvb39702	No fault gets raised upon using the same encapsulation VLAN in a copy device in tenant common, even though a fault should get raised.	2.1(1h) and later

- In a multipod configuration, before you make any changes to a spine switch, ensure that there is at least one operationally “up” external link that is participating in the multipod topology. Failure to do so could bring down the multipod connectivity. For more information about multipod, see the *Cisco Application Centric Infrastructure Fundamentals* document and the *Cisco APIC Getting Started Guide*.

Related Documentation

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

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

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

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

The following 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
Cisco ACI Simulator Release Notes, Release 2.1(1)	Provides release information for the Cisco ACI Simulator product.
Cisco Application Policy Infrastructure Controller, Release 2.1(1), Release Notes	This document. Provides release information for the Application Policy Infrastructure Controller (APIC) product.
Cisco Nexus 9000 Series ACI-Mode Switch FPGA/EPLD Upgrade Release Notes, Release 12.1(1)	Provides release information for the Cisco Nexus 9000 series ACI-mode switch FPGA/EPLD product.
Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.1(1)	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
Cisco APIC Basic Configuration Guide	Describes steps that you must perform to configure your ACI fabric.
Cisco APIC Getting Started Guide	Describes the first things that you must do to use the APIC after you install the APIC software.
Cisco Nexus 93108TC-EX ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 93180YC-EX ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.
Cisco Nexus 9332PQ ACI-Mode Switch Hardware Installation Guide	Describes how to install and start up the switch and how to replace modules.

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

Table 8 Interface Documentation

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

Table 9 Reference Documentation

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

Table 10 Layer 4 to Layer 7 Documentation

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

Table 11 Virtualization Documentation

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

Table 12 ACI with OpenStack Documentation

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

Table 13 Troubleshooting Documentation

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

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

New Documentation

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

- *Cisco ACI Virtualization Guide, Release 2.1(1)*
- *Cisco APIC and Federal Information Processing Standards (FIPS)*
- *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 2.1(1)*
- *Cisco APIC NX-OS Style CLI Command Reference, Release 2.1(1)*
- *Cisco APIC REST API Configuration Guide*
- *Cisco Nexus 9000 Series ACI-Mode Switch FPGA/EPLD Upgrade Release Notes, Release 12.1(1)*
- *Verified Scalability Guide for Cisco ACI, Release 2.1(1) and Cisco Nexus 9000 Series ACI-Mode Switches, Release 12.1(1)*