Cisco Application Policy Infrastructure Controller, Release 1.3(2), Release Notes

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

Note: Use this document in combination with the *Cisco NX-OS Release 11.3(2) Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches*, 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 caveats. 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

Note: The 1.3(2) release is a continuation of the 1.3(1) release, and so the 1.3(1) documentation also contains information that is relevant to the 1.3(2) release.

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
June 7, 2016	Created the release notes for the 1.3(2f) release.
June 22, 2016	In the Changes in Behavior section, added a change in AVS certifications.
July 11, 2016	1.3(2h): Added the content for release 1.3(2h).
August 8, 2016	1.3(2i): Release 1.3(2i) became available; there are no changes to this document for this release.
September 2, 2016	Added pointers to the release notes for release 1.3(1).
October 20, 2016	In the Usage Guidelines section, added "ACI does not support a class E address as a VTEP address."
December 6, 2016	In the Compatibility Information section, added information about a known issue when using the Safari browser to connect to the APIC.

Date	Description
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.
April 13, 2017	1.3(2k): Release 1.3(2k) became available. Added the resolved caveats for this release.
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).

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 hardware and software listed on the *ACI Ecosystem Compatibility List* document and the software listed as follows:
  - Cisco NX-OS Release 11.3(2)
  - Cisco AVS, Release 5.2(1)SV3(1.25)

    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 N9332PQ switch
  - Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the N9396PX or N9372PX switches
- 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 (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 two AVS VMM domains (one with VLAN and one with 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 1.3(1g)* 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 release and the Microsoft Windows Azure Pack Update Rollup 9 release.

- 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.
- When configuring an atomic counter policy between two endpoints, and an IP is learned on one of the two endpoints, it is recommended to 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: In the 1.0(4x) and earlier releases, when creating static paths for application EPGs or Layer 2/Layer 3 outside EPGs, the physical domain was not required. In this release, it is 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.
- 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 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.
- In this software version, 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.
- ACI does not support a class E address as a VTEP address.
- 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.

Verified Scalability Limits

Table 2 shows the CLI scalability limits.

Table 2 CLI Scalability Limits

Configurable Option	Scale
Number of tenants	500
Number of Layer 3 (L3) contexts	300
Number of endpoint groups (EPGs)	3,500
Number of endpoints (EPs)	20,000
Number of bridge domains (BDs)	3,500
Number of BGP + number of OSPF sessions + EIGRP (for external connection)	300
Maximum number of vPCs	48
Maximum number of PCs, access ports	48
Maximum number of encaps per access port	1,750
Number of multicast groups	8,000
Maximum number of vzAny provided contracts	16
Maximum number of vzAny consumed contracts	16
Maximum amount of encaps per endpoint group	2 static, 1 dynamic

Configurable Option	Scale
Security TCAM size	4,000
Number of VRFs	500
Separate-Config-Set	
Tenants	100
Endpoint groups	1,000
Bridge domains	500
VRFs	100
SPAN destinations	3
NTP servers	2
Contracts	100
DNS servers	2
Syslog servers	1

For additional verified scalability limits, see the *Verified Scalability Guide* for this release:

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

For new software features, see the Cisco Application Policy Infrastructure Controller, Release 1.3(1), Release Notes at the following location:

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

Note: The 1.3(2) release is a continuation of the 1.3(1) release, and so the 1.3(1) documentation also contains information that is relevant to the 1.3(2) release.

New Hardware Features

For new hardware features, see the *Cisco NX-OS Release 11.3(1) Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches* at the following location:

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

Changes in Behavior

This section lists changes in behavior in this release.

- Starting with the 1.2(3) release, AVS uses site-specific certifications. Prior to the 1.2(3) release, AVS used image-based certifications. Because of the change in certifications, if you upgrade from a release prior to the 1.2(3) release, you must use an alternate upgrade procedure. For the upgrade procedure, see the *Cisco AVS Installation Guide* at the following website:

  https://www.cisco.com/c/en/us/support/switches/application-virtual-switch/products-installation-guides-list.html

Caveats

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

- Open Caveats
- Resolved Caveats
- Known Behaviors

Open Caveats

This section lists the open caveats. Click the bug ID to access the Bug Search tool and see additional information about the bug. If a caveat is fixed in a patch of this release, the "Fixed In" column of the tables specifies the release.

Open Caveats in the 1.3(2f) Release

Table 3 lists the open caveats in the 1.3(2f) release.

Table 3 Open Caveats in the 1.3(2f) Release

Bug ID	Description	Fixed In
CSCuz03535	Because of the MTU setting on the APIC interface (1500 B), packets bigger than 1476 bytes (+50 bytes for encapsulation) get dropped.	

Open Caveats in the 1.3(2h) Release

There are no new open caveats in the 1.3(2h) release.

Open Caveats in the 1.3(2i) Release

There are no new open caveats in the 1.3(2i) release.

Open Caveats in the 1.3(2k) Release

There are no new open caveats in the 1.3(2k) release.

Resolved Caveats

This section lists the resolved caveats. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Resolved Caveats in the 1.3(2f) Release

Table 4 lists the resolved caveats in the 1.3(2f) release.

Table 4 Resolved Caveats in the 1.3(2f) Release

Bug ID	Description
CSCuz34848	Integrated Hyper-V hosts are not showing up in the Hypervisors section of the APIC GUI under the Microsoft VMM domain.
CSCuz36977	When configuring a subnet under a Layer 3 external network, there is no validity check. Illegal subnets can be configured as external subnets.
CSCuz42600	The field for "L3out pcTag" is missing at the following GUI location: Tenant > External Routed Network > (pick the L3out) > Network > (pick the network), then go to the Policy > General tab.
CSCuz47137	The APIC GUI treats the "Primary VLAN" encapsulation field as mandatory if the static VLAN mode is chosen in the "Create VMM Domain association" GUI wizard. As a workaround, specify a valid value in the "Primary VLAN" field in the GUI. This issue is not present when an EPG is deployed through the APIC REST interface, or when using the APIC CLI.
CSCuz47137	The APIC GUI requires the user to specify both the primary VLAN and port encap when static VLAN mode is selected in the VMM domain association.
CSCuz48319	The managed object fvSharedService on the APIC shows references to endpoint groups with contracts that do not exist anymore on the system.
CSCuz48900	When viewing the Operations tab of Techsupports, On-demand Techsupports, and Core files, the administrator is unable to view the files sizes of successful exports.
CSCuz50321	The mnt/pss/snmp.d directory within an on-demand switch techsupport export archive is missing read permissions. This can cause problems with extraction and analysis.
CSCuz67203	After upgrading from 1.2(3c) to 1.3(1g), all AVS (VXLAN/LS) lose their OpFlex channels (they become disconnected). Some VM ports become blocked, and the issue spreads across the entire DVS environment.
CSCuz71294	Migration of a mgmt vmk on ESXi to an AVS port-group fails.
CSCuz72347	A vulnerability in the installation procedure of the Cisco Application Policy Infrastructure Controller (APIC) device could allow an authenticated, local attacker to escalate to root-level privileges.

Resolved Caveats in the 1.3(2h) Release

Table 4 lists the resolved caveats in the 1.3(2h) release.

Table 5 Resolved Caveats in the 1.3(2h) Release

Bug ID	Description
CSCuz96719	The OpFlex state is displayed as "Send" after upgrading to the 1.3(2f) release, which results in some of the endpoints being down.
CSCva00950	OpFlex flaps with timer issues when both OpFlex channels go down at the same time.

Resolved Caveats in the 1.3(2i) Release

There are no new resolved caveats in the 1.3(2i) release.

Resolved Caveats in the 1.3(2k) Release

Table 6 lists the resolved caveats in the 1.3(2k) release.

Table 6 Resolved Caveats in the 1.3(2k) Release

Bug ID	Description
CSCuz52389, CSCvb48563, CSCvc23465	OpenSSL is affected by the vulnerability identified by one or more Common Vulnerability and Exposures (CVE) IDs.
CSCvc41605	VLAN encapsulations are reallocated after upgrading.
CSCvb08670	A node ID added to the Cisco APIC cluster might get a duplicate fabric address.
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.

Known Behaviors

This section lists caveats that describe known behaviors. Click the Bug ID to access the Bug Search Tool and see additional information about the bug.

Known Behaviors in the 1.3(2f) Release

Table lists caveats that describe known behaviors in the 1.3(2f) release.

Table 7 Known Behaviors in the 1.3(2f) Release

Bug ID	Description
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.
CSCuo79243	In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.
CSCuo79250	The node ID policy can be replicated from an old appliance that is decommissioned when it joins a cluster.
CSCup47703	The DSCP value specified on an external endpoint group does not take effect on the filter rules on the leaf switch.
CSCup79002	The hostname resolution of the syslog server fails on leaf and spine switches over in-band connectivity.
CSCup94070	After importing an exported configuration, graph instances are not created and Layer 4 to Layer 7 packages are missing in the system.

Bug ID	Description
CSCuq21360	Following a FEX or switch reload, configured interface tags are no longer configured correctly.
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).
CSCur71082	If the APIC is rebooted using the CIMC power reboot, the system enters into fsck due to a corrupted disk.
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.
CSCut51929	The traffic destined to a shared service provider endpoint group picks an incorrect class ID (PcTag) and gets dropped.
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.
CSCuu61998	Newly added microsegment EPG configurations must be removed before downgrading to a software release that does not support it.
CSCuu64219	Downgrading the fabric starting with the leaf will cause faults such as policy-deployment-failed with fault code F1371.
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.
CSCuy25817	Downgrading an APIC configured with Intra-EPG deny configuration from the 1.2(2) release to an earlier release is not supported. The Intra-EPG deny configuration must be manually cleaned up before downgrading.

Known Behaviors in the 1.3(2h) Release

There are no new known behaviors in the 1.3(2h) release.

Known Behaviors in the 1.3(2i) Release

There are no new known behaviors in the 1.3(2i) release.

Known Behaviors in the 1.3(2k) Release

There are no new known behaviors in the 1.3(2k) release.

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 8 Installation, Upgrade, and Configuration Documentation

Document	Description
Cisco ACI Basic Configuration Guide	Describes steps that you must perform to configure your ACI fabric.
Cisco APIC Controller and Switch Upgrade and Downgrade Guide	Describes how to upgrade or downgrade the APIC controller's appliance firmware. Note: This document replaces the *Cisco APIC Firmware Management Guide*.
Cisco APIC Getting Started Guide	Describes the first things that you must do to use the APIC after you install the APIC software.
Cisco Application Policy Infrastructure Controller (APIC) Installation Guide	Describes how to install the APIC software.
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.
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.

Related Documentation

Document	Description
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.
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 9 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 10 Reference Documentation

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

Table 11 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 12 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 5 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 6 Troubleshooting Documentation

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