



Cisco Application Policy Infrastructure Controller Release Notes, Release 4.1(1)

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

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

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

Note: Use this document with the *Cisco NX-OS Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches, Release 14.1(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>

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

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

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

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

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

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

You can access these documents from the following website:

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

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
March 28, 2019	Release 4.1(1i) became available.
April 3, 2019	In the Miscellaneous Guidelines section, added mention that connectivity filters are deprecated.
April 6, 2019	In the New Software Features section, added mention of the Cisco Cloud APIC product.

Contents

Date	Description
April 9, 2019	4.1(1i): In the Open Bugs section, added bug CSCvp24262.
April 25, 2019	4.1(1j): Release 4.1(1j) became available. Added the resolved bugs for this release.
May 20, 2019	4.1(1k): Release 4.1(1k) became available. Added the resolved bugs for this release.
May 30, 2019	4.1(1l): Release 4.1(1l) became available; there are no changes to this document for this release. See the Cisco NX-OS Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches, Release 14.1(1) for the changes in this release.
June 7, 2019	In the Hardware Compatibility section, added the following bullet: <ul style="list-style-type: none"><li data-bbox="467 632 1458 758">■ First generation switches (models without -EX, -FX, or later designations) do not support Contract filters with match type "IPv4" or "IPv6." Only match type "IP" is supported. Because of this, a contract will match both IPv4 and IPv6 traffic when the match type of "IP" is used.
June 13, 2019	4.1(1): In the Known Behavior section, added a known behavior.

Contents

This document includes the following sections:

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

New and Changed Information

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

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

New Software Features

The following sections list the new software features in this release:

- [Fabric Infrastructure](#)
- [Fabric Scale and Other Enhancements](#)
- [Solution Integration](#)
- [Virtualization](#)

Fabric Infrastructure

The following table lists the new fabric infrastructure features in this release:

Table 2 New Software Features—Fabric Infrastructure

Feature	Description	Guidelines and Restrictions
BGP multicast v4 address family support	APIC now supports the BGP multicast v4 address family.	None.
Cloud APIC	This release includes the release of the Cisco Cloud APIC product, which enables you to extend a Cisco ACI Multi-Site fabric to Amazon Web Services (AWS) public clouds. For more information, see the Cloud APIC documentation	See the <i>Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release</i>

Feature	Description	Guidelines and Restrictions
	set: https://www.cisco.com/c/en/us/support/cloud-systems-management/cloud-application-policy-infrastructure-controller/tsd-products-support-series-home.html	4.1(1).
EPG Communication tab	This release adds the EPG Communication tab. This tab enables you to create communication between two EPGs and to monitor which EPGs are communicating with one other through a contract and filters. Using this tab represents a simpler, faster way to set up a contract between the EPGs.	None.
FC-NPV enhancements	This release enhances FC NPV to support: <ul style="list-style-type: none"> ■ Having an FCoE host that uses FEX over an FC NPV link ■ 32G Brocade interoperability 	None.
Filter groups	Support is now available for configuring filter groups, with flow entries that are used to filter the traffic, and associating them to SPAN source groups. For more information, see the <i>Cisco APIC Troubleshooting Guide, Release 4.1(x)</i> .	None.
IP SLA	Internet protocol service level agreement (IP SLA) tracking is a common requirement in networks that allows a network administrator to collect information about network performance in real-time. With Cisco ACI IP SLA, you can track an IP address using ICMP and TCP probes. Tracking configurations can influence route tables, allowing for routes to be removed when tracking results come in negative and returning the route to the table when the results become positive again. For more information, see the <i>Cisco APIC Layer 3 Networking Configuration Guide, Release 4.1(x)</i> .	None.
Layer 1/Layer 2 policy-based redirect	This feature allows you to configure policy-based redirect on Layer 1 or Layer 2 service devices. For more information, see the <i>Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.1(x)</i> .	Active-active deployment is not supported. The two legs of the Layer 2 service device need to be configured on a different leaf switch to avoid packet loops. Per port VLAN is not supported. Shared bridge domain is not supported. A Layer 1/ Layer 2 device bridge domain

New and Changed Information

Feature	Description	Guidelines and Restrictions
		<p>cannot be shared with Layer 3 device or regular EPGs.</p> <p>Service node in managed mode is not supported.</p> <p>Layer 1/Layer 2 devices support physical domain only, VMM domain is not supported.</p>
Local SPAN with port-channels as the destination	<p>Support is now available for local SPAN with port-channels as the destination.</p> <p>For more information, see the <i>Cisco APIC Troubleshooting Guide, Release 4.1(x)</i>.</p>	Sources and the port-channel must be local on the same switch.
Mini ACI fabric with ACI Multi-Site topology	You can now use mini ACI fabric with ACI Multi-Site topology on a single pod.	None.
MLD snooping	<p>Support is now available for Multicast Listener Discovery (MLD) snooping.</p> <p>For more information, see the <i>Cisco APIC Layer 3 Networking Configuration Guide, Release 4.1(x)</i>.</p>	None.
Multi-tier architecture	<p>You can create a multi-tier ACI fabric topology that corresponds to a Core-Aggregation-Access architecture found in many existing data centers. While providing all of the benefits of the ACI fabric, the multi-tier architecture enhancement also mitigates the need to upgrade costly components such as rack space or cabling. The addition of a tier-2 leaf layer makes this topology possible. The tier-2 leaf layer supports connectivity to hosts or servers on the downlink ports and connectivity to the leaf layer (aggregation) on the uplink ports.</p> <p>For more information, see the <i>Cisco APIC Getting Started Guide, Release 4.1(x)</i>.</p>	None.
SSD monitoring	<p>The SSD monitoring feature enables you to override the preconfigured thresholds for the SSD lifetime parameters and raise faults when the SSD reaches some percentage of the configured thresholds. These faults allows network operators the capability to monitor and proactively replace any switch before the switch fails due to an SSD's lifetime parameter values becoming exceeded.</p> <p>For more information, see the <i>Cisco APIC SSD Monitoring KB article</i>.</p>	<p>This feature requires Micron M600 64 gb SSDs.</p> <p>You cannot configure this feature using the CLI.</p>
Virtual Port Channel	This feature allows the migration of nodes from non-EX,	None.

Feature	Description	Guidelines and Restrictions
migration	non-FX, and non-FX2 switch to an EX, FX, or FX2 switch. For more information, see the <i>Cisco Application Centric Infrastructure Fabric Hardware Installation Guide</i> .	

Fabric Scale and Other Enhancements

The following table lists the new fabric scale and other enhancements features in this release:

Table 3: New Software Features—Fabric Scale and Other Enhancements

Feature	Description	Guidelines and Restrictions
Bookmarks	You can now bookmark almost any page, which enables you to go back to that page easily by choosing the bookmark from your list of bookmarks. In previous releases, this feature was represented as favorites (the star icon), and had less capability. For more information, see the <i>Cisco APIC Getting Started Guide, Release 4.1(x)</i> .	None.
Confirmation and summary screens	Some of the wizards now include a confirmation screen and summary screen as the last steps. On the confirmation screen, you see a list of the policies that the wizard will create. You can change the names of the policies, if necessary. After the confirmation screen is the summary screen, which shows you the policies that the wizard created. You can no longer change the policies' names, but you can edit the properties of a policy.	None.
Default tab	This feature enables you to set a tab as the "favorite" on a page. Whenever you navigate to that page, that tab will be the default tab that is displayed. This feature is enabled only for the tabs in the Work pane. For more information, see the <i>Cisco APIC Getting Started Guide, Release 4.1(x)</i> .	None.
Error counter enhancement	Physical interface configuration now includes error counter statistics information.	None.
Export tech support configuration data enhancement	This enhancement allows the user to export tech support data or configurations with read-only privileges. For more information, see the <i>Cisco ACI Configuration Files: Import and Export</i> KB article.	None.
GTP load balancing	This feature enables the Cisco APIC to perform fabric load balancing based on GTP TEID. For more information, see the <i>Cisco APIC Basic</i>	None.

Feature	Description	Guidelines and Restrictions
	<i>Configuration Guide, Release 4.1(x).</i>	
Leaf switch uplink ports priority	When the fabric is scaled with numerous bridge domains, endpoint groups, and so on, and each are allocated a VLAN, this causes VLAN resource contention. Reloading a leaf switch in this state causes the leaf-to-spine switch uplink to enter the disabled state (those links do not come up). In this release, the leaf-to-spine switch uplinks are given a higher priority with the VLAN resource that is allocated to them, so that reloading a leaf switch while the switch is in a VLAN resource contention state does not affect the leaf-to-spine switch uplinks (the links come up).	None.
Multiple-context apps	You can now run an app in multiple GUI screens, or "contexts." For example, you can run the app while looking at a tenant's application profiles and while looking at the tenant's contracts. Prior to the 4.1 release, you could run an app only in one context; switching to a different context would close the app.	None.
New alerts	<p>This release adds the following alerts:</p> <ul style="list-style-type: none"> ■ Leaf x is Inactive: This alert warns you that a leaf switch became inactive, powered down, or disconnected. ■ New Switch Discovered: This informational alert informs you when a new switch is discovered. ■ Node Outage: Indicates that a node is either down or reloading. ■ Node x Must Be Reloaded: This alert warns you that an SSD must be reformatted and repartitioned. ■ OSPF Connectivity is Down: This alert warns you when OSPF connectivity is down. The alert lists the interfaces that have OSPF configured, but are not able to communicate with one another, and provides a recommended troubleshooting action. ■ Process Crash: This alert warns you that a process has crashed. ■ Split-Fabric Detected: Indicates that the fabric is split and that the controller is operating in read-only mode. 	None.
Scale changes	<p>This release includes the following scale changes:</p> <ul style="list-style-type: none"> ■ Maximum number of remote leaf switches: 128 (single pod) 	None.

Feature	Description	Guidelines and Restrictions
	<ul style="list-style-type: none"> ■ 100 sub-interfaces per VRF and per L3Out ■ 30,000 IPv4/IPv6 LPM prefixes on a border leaf switch (EX, FX, and FX2 platforms) ■ 4,000 MAC address EPGs 	
Object Store Browser improvements	<p>The Object Store Browser has the following improvements:</p> <ul style="list-style-type: none"> ■ The Object Store Browser has a new, modernized look-and-feel. ■ You can now search by class, distinguished name, or URL, instead of only class and distinguished name. After you find an object, you can make the object a favorite, which enables you to go to your list of favorites and load the object from there. ■ You can now view the JSON response of your last query; previously you could only view the XML response. ■ The Object Store Browser by default displays all of the properties, even those that have no value. You can now hide the properties that do not have a value. ■ You can now navigate the distinguished name using the bread crumbs, which is simpler and easier to use. ■ You can now only view a distinguished name's stats, faults, or health if there is applicable data. 	None.

Solution Integration

The following table lists the new solution integration features in this release:

Table 4 New Software Features—Solution Integration

Feature	Description	Guidelines and Restrictions
Microsoft NLB	<p>Support is now available for Microsoft Network Load Balancing (NLB).</p> <p>For more information, see the <i>Cisco APIC Layer 3 Networking Configuration Guide, Release 4.1(x)</i>.</p>	None.

Virtualization

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

Table 5 New Software Features—Virtualization

Feature	Description	Guidelines and Restrictions
Cisco ACI integration with Cisco's SD-WAN	vManage integration enables tenant admins to apply preconfigured policies to specify the levels of packet loss, jitter, and latency for tenant traffic over the WAN. When a WAN SLA policy is applied to tenant traffic, the Cisco APIC sends the configured policies to a vManage controller. The vManage controller, which is configured as an external device manager that provides Cisco Software-Defined Wide Area Network (SD-WAN) capability, chooses the best possible WAN link that meets the loss, jitter, and latency parameters specified in the SLA policy. For more information, see the <i>Cisco ACI and SD-WAN Integration Guide</i> .	None.
Cisco ACI with Cisco UCSM integration	You can automate networking policies on Cisco UCS devices. To do so, you integrate Cisco UCSM into the Cisco Application Centric Infrastructure (ACI) fabric. Cisco APIC takes hypervisor NIC information from the Cisco UCSM and a virtual machine manager (VMM). The automation applies to all the devices that the Cisco UCSM manages. For more information, see the chapter "Cisco ACI with Cisco UCSM Integration" in the <i>Cisco ACI Virtualization Guide, Release 4.1(1)</i> .	If you use Cisco Application Virtual Switch (AVS) or Microsoft System Center Virtual Machine Manager (SCVMM), you also must associate a switch manager with the VMM. If you use Cisco ACI Virtual Edge or VMware vSphere Distributed Switch (VDS), make the association if you <i>do not</i> use LLDP or CDP in your VMM domain.

New Hardware Features

For new hardware features, see the *Cisco NX-OS Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches, Release 14.1(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

The following are changes in behavior for this release:

- You no longer need to include the IP prefix of the Layer 3 interface when configuring source SPAN with Layer 3 interface filtering. For more information, see the *Cisco APIC Troubleshooting Guide, Release 4.1(x)*.

Upgrade and Downgrade Information

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

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

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

Bugs

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

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

Open Bugs

This section lists the open bugs. Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Exists In" column of the table specifies the 4.1(1) releases in which the bug exists.

Table 6 Open Bugs in This Release

Bug ID	Description	Exists in
CSCvp07262	Configuration import (configImportP) with importMode="atomic" and importType="replace" may not work.	4.1(1i) and later
CSCvp24262	A policy-based redirect service graph configured with vzAny as the consumer and vzAny as the provider does not function. If you are using or want to use this capability, we recommend that you do not upgrade to the 4.1(1) release.	4.1(1i)

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 7 Resolved Bugs in This Release

Bug ID	Description	Fixed in
CSCvm55394	A shard is stuck and cannot move forward. Continuous handleTxCheckTimeout can be seen in the source log with no new transaction being sent to the replica.	4.1(1i)

Bugs

Bug ID	Description	Fixed in
CSCvn77241	During same-VC-cross-DC VM migrations, there is one task triggered per VM to verify its migration status. However, if too many VMs are migrated within a short period of time, the amount of tasks due to the bulk migration might exceed the size of the task queue, which leads to huge amount of faults.	4.1(1i)
CSCvo23714	NGINX gets has an out of memory issue approximately every 10 hours due to the memory usage growing to up to 8GB.	4.1(1i)
CSCvo39336	If many faults flap on the switch nodes, the GUI may run slowly and have poor response.	4.1(1i)
CSCvo47323	ARP poisoning occurs when return traffic from the uplink to the SNAT interface is sent back to the uplink. All of the uplink IP addresses appear as coming from the SNAT MAC address.	4.1(1i)
CSCvo57185	The GUI doesn't display hypervisor details on double clicking if there are more than 16.	4.1(1i)
CSCvm12790	A remote leaf switch configures a static route to the Cisco APIC based on which Cisco APIC replies for its DHCP. This route does not get deleted after the remote leaf switch is commissioned. This behavior might cause the static route to get redistributed to the IPN, which then points the route to this specific IPN back to the remote leaf switch. Because the Cisco APIC in question and remote leaf switch will now have a routing issue, they cannot communicate. From this Cisco APIC, the remote leaf switch cannot be managed.	4.1(1i)
CSCvk35070	After creating and deleting the pod 2 TEP Pool under "Pod Fabric Setup Policy", the pod 1 Infra VLAN "172.31.0.0/16" leaks to the "overlay-1" route map on the leaf switch.	4.1(1i)
CSCvm57106	After upgrading to the 3.2(3n) release, fault F608054 appeared, indicating fsm-sync-with-quorum-fsm-fail.	4.1(1i)
CSCvn11128	APIC accepts the "_" (underscore) symbol as delimiter for VMware VMM domain integration, even though it is not a supported symbol. This is an enhancement request to implement a check in the APIC GUI to not accept "_".	4.1(1i)
CSCvn67689	Changing the "DH Param" setting on the APIC from the default "None" results in the following pop-up error message: Error: 400 - Failed to update communication configuration (Configuration not valid for server (Nginx)) The configuration does not get applied.	4.1(1i)
CSCvo45535	Changing the timezone on the APIC leads to different timezones on the APICs and leaf switches. For example, choosing the Europe/Istanbul timezone leads to the time on the leaf/spine switches to be GMT+3 (which is correct, due to daylight saving time), while on the APIC the timezone shows as +2. This causes an issue with syslog messages sent from the APICs and leaf switches, as they have different timestamps.	4.1(1i)
CSCvi48314	Currently, the ACI upgrade process involves uploading of the images to the spine/leaf switch and activating the newer code. These upload/activating procedures cannot be separated and must be performed in one maintenance window. This causes the maintenance window to be longer.	4.1(1i)
CSCvm10827	Database files and logs related to a previous upgrade are not collected in the techsupport files.	4.1(1i)

Bugs

Bug ID	Description	Fixed in
CSCvo15401	Database files and logs related to a previous upgrade are not collected in the techsupport files.	4.1(1i)
CSCvn10244	If a techsupport that is exported to the APIC and is generated after a configuration snapshot, rolling back to that snapshot removes the techsupport configuration and the logs that are saved to the APIC. The exported logs should instead be preserved as long as possible, and rolling back the snapshot should not cause the log/trace removal.	4.1(1i)
CSCvn12389	<p>If multiple path attachments (l2extRsPathL2OutAtt) are configured for the same interface under different node profiles (l2extLNodeP) or different interface profiles (l2extLIffP), the configuration is blocked by the policy manager (PM), but is allowed by the policy distributed (PD), causing an inconsistency between the components. As a result, the posted configuration will not be displayed under the GUI.</p> <p>Additionally, depending on the APIC version, the configuration push failure from the PD to PM may cause all subsequent configurations for the shard to fail. As a result, all configuration changes for a particular tenant may appear to fail.</p>	4.1(1i)
CSCvo42782	If the infra-VLAN in the input to acc-provision is different from what it detects on the fabric, acc-provision warns you that infra-VLAN configuration is incorrect, but it still uses the requested VLAN as the desired value for infra-VLAN.	4.1(1i)
CSCvn30897	If you configure two OSPF L3Outs with external network "0.0.0.0/0," with one being border leaf 101 and the other being border leaf 102, sometimes a route is learned from border leaf 102, but the "Visibility & Troubleshooting" shows the destination border leaf as border leaf 101.	4.1(1i)
CSCvg41187	<p>In an ACI GOLF deployment, the external GOLF router will advertise its routes using BGP EVPN to the spine switches, which will reoriginate those into VPNv4 and advertise to the leaf switches that should import them. These VPNv4 routes will have the VXLAN VNID of the originating VRF instance set in the "label" field, and in the hardware a rewrite entry is added for this VNID corresponding to the VXLAN tunnel that extends to the GOLF router.</p> <p>Due to hardware restrictions within a single VRF instance on an ACI leaf switch, there can only be one VXLAN VNID rewrite entry per tunnel. If two VRF instances in ACI are configured with the same route-target import/export policy, then the leaf switch will attempt to import the VPNv4 routes in the same VRF instance with different VXLAN VNIDs.</p> <p>Because only a single rewrite VNID can be installed per tunnel per VRF instance, this will prevent some rewrite VNIDs from being installed in hardware. As a result, you may see that traffic that is from the leaf switch going to the GOLF router will either have a VNID of 0 or will have the wrong VNID set.</p>	4.1(1i)
CSCvn95704	On the Mgmt tenant, when trying to configure monitoring policies, the button does not take any actions and monitoring policies cannot be configured on this tenant.	4.1(1i)
CSCvn07827	PLR fails after upgrading to a Cisco APIC 4.0 release.	4.1(1i)
CSCvi63720	SNMP commands on the CLI causes an error to display.	4.1(1i)
CSCvk74125	The @ symbol cannot be used when configuring an SNMP community due to the symbol being interpreted as a delimiter for the context. Using @ results in unknown context errors incrementing in the "show snmp" command.	4.1(1i)

Bugs

Bug ID	Description	Fixed in
CSCvn80201	The APIC syslog does not log the username for login/logout attempts.	4.1(1i)
CSCvn67742	The Cisco APIC sets the mcast attribute to "yes" after disabling PIM on an L3Out. However, the APIC should instead set the attribute to "no."	4.1(1i)
CSCvk31427	The current implementation of APIC techsupport collects the latest 10,000 logs of audit and faults. That works for certain scenarios. However, there are many troubleshooting scenarios that need to get all records of the audits, faults, and events. This enhancement is requesting the implementation of the collection of all audit, fault, and event logs in separate compressed gzip files.	4.1(1i)
CSCvn70746	The Dashboard UI can display negative fault counts or wrong fault counts inconsistently with the "Fault Summary" UI.	4.1(1i)
CSCvn81454	The F0053 fault is generated.	4.1(1i)
CSCvn65756	The F3222 fault displays after you delete a pool.	4.1(1i)
CSCvo35391	The following issues are observed: <ul style="list-style-type: none"> ■ The LLDPAD process crashes on an APIC. ■ The LLDPAD service cannot start anymore after the core, not even after a cold reboot of the APIC. ■ EDAC errors are observed in dmesg prior to the LLDPAD crash. ■ The LLDPAD crash causes the directly-connected leaf switches to lose the APIC controller LLDP adjacency (lldpCtrlrAdjEp). ■ eth2-1 and eth2-2 do not receive any frames/packets anymore, as observed with the ifconfig command. <ul style="list-style-type: none"> — TX counters are going up. ■ The APIC gets a reduced health score in avread (health: 2) and perceives the cluster state incorrectly due to there being no RX frames/packets. 	4.1(1i)
CSCvj89447	The Name column is missing on the Subnets table from the External Network Policy screen in the Routed Outside Policy screen. The Name field is missing on the Create Subnet panel.	4.1(1i)
CSCvk41676	The neutron call using ip cidr for the --allowed-address-pairs feature is not supported with the ACI plugin for OpenStack.	4.1(1i)
CSCvn87426	The query lists out incorrect objects that do not match the "eq" or "ne" filter.	4.1(1i)
CSCvo17041	The same IP address added under NTP in different formats (with/without leading zeroes) are treated as unique entries on the APIC. A switch will have single entry. Deleting one of the entries on the APIC will delete that entry from the switch.	4.1(1i)
CSCvn98133	The 'showconfig' command from the APIC does not print the config and instead generates a traceback. This will result in an invalid user_config file in the APIC 1of3 techsupport file.	4.1(1i)

Bugs

Bug ID	Description	Fixed in
CSCvn30026	The subject and body fields do not allow modification.	4.1(1i)
CSCvn94771	There is a lot of lag when entering the command " show endpoint ip <ip>" .	4.1(1i)
CSCvd12514	There is no way to see the next DHCP address to be assigned from a DHCP pool.	4.1(1i)
CSCvo05509	This is an enhancement request to include the ethpmFcot MO to ACI leaf switch techsupport files.	4.1(1i)
CSCvn93417	This is an enhancement request to include the output of /proc/kpm_err_stat in ACI switch techsupports.	4.1(1i)
CSCvi45842	This is an enhancement to set the reload delay timer between the ACI ToRs upgrades if the maximum concurrent nodes is 1.	4.1(1i)
CSCvn67365	This is an enhancement to update OpenSSH to version 7.8+ to remediate CVE-2018-15473. More info can be found here: https://tools.cisco.com/security/center/viewAlert.x?alertId=58762	4.1(1i)
CSCvn81863	TPM is supposed to be used to encrypt certain partitions, but on a 4.0 release, the image can be installed without TPM being enabled, and the APIC can also boot up without it.	4.1(1i)
CSCvn56421	Traffic returning from a PBR node is redirected back to the PBR node, forming a loop.	4.1(1i)
CSCvo31212	When a spine switch is used as an L3Out device to IPN/ISN, in a multi-pod with Cisco ACI Multi-Site configuration, after switching over the sup in a 9508 chassis, a flapping event might be seen in the logs for a DHCP client interface operational state on the L3Out external interface.	4.1(1i)
CSCva02247	When attempting to upload a firmware file to an APIC, an error indicating the " repository [is] over 80% full" appears. Even deleting previously uploaded firmware files does not clear out enough space.	4.1(1i)
CSCcu31743	When creating a firmware download job on the APIC GUI by using Admin > Download Tasks > "create outside firmware source" and selecting SCP while your web browser is connected to APIC1, APIC2 might actually be downloading the file. This is an enhancement request for the APIC GUI to indicate which APIC is trying to download the file when the download fails so that further troubleshooting can be done on the correct port.	4.1(1i)
CSCvo59407	When the FEX is removed the ACI leaf switch, the FEX status become offline and is completely removed after around 20 minutes. However, the license consumption on the APIC is not updated nor released.	4.1(1i)
CSCvo51421	When the TACACS user privilege is admin, the vCenter plugin only gets read permissions when fetching the privileges from the APIC.	4.1(1i)
CSCvn79128	When upgrading from some 3.2 or 3.1 releases to 4.0, some or all leaf switch maintenance groups will immediately start upgrading without being user-triggered. This issue occurs as soon as the APICs finish upgrading.	4.1(1i)
CSCvo35552	When using a specific out-of-band or in-band contract to only allow certain protocols, all ports are open.	4.1(1i)

Bugs

Bug ID	Description	Fixed in
CSCvn78438	When using the "show vsan-domain detail" command, all interfaces that are configured with "NP" show as "F" mode, and the following error displays at the end of the output: Error: Invalid RN rsvsanPathAtt-[topology/pod-1/node-1301/sys/conng/path-[10Gb-CCH-Server-VPC-SR227]]	4.1(1i)
CSCvn27112	When using the Firefox browser to view "Operations > Visibility & Troubleshooting," the zoom icons are missing on the result page.	4.1(1i)
CSCvo29820	Where a trunk port group was created and what was pushed to it cannot be verified within the APIC GUI.	4.1(1i)
CSCvo66664	XML special characters in the SNMP location and name are not properly escaped when exported into XML. This causes issues in being able to parse the XML output properly. In addition, Cisco ACI Multi-Site Orchestrator (MSO) queries the SNMP information and attempts to parse the XML export of the SNMP config. If the SNMP community policy or SNMP location have special characters (&, <, >), pushing policies onto these sites may fail, as MSO cannot parse the XML output.	4.1(1i)
CSCvp24262	A policy-based redirect service graph configured with vzAny as the consumer and vzAny as the provider does not function. If you are using or want to use this capability, we recommend that you do not upgrade to the 4.1(1) release.	4.1(1j)
CSCvp21665	ACI Application (App) does not get enabled (started). There will be a fault raised for that App, stating Gluster-FS health is not OK. But Gluster-FS status is actually OK.	4.1(1k)
CSCvp68533	The data stored by an App might be lost during an APIC upgrade. This can impact the functionality of the App.	4.1(1k)
CSCvp68528	Sometimes Apps might not be able to access the filesystem. File access can return disk i/o error. The fix for this bug improves filesystem reliability.	4.1(1k)

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 4.1(1) releases in which the known behavior exists.

Table 8 Known Behaviors in This Release

Bug ID	Description	Exists in
CSCvj26666	The "show run leaf spine <nodeld>" command might produce an error for scaled up configurations.	4.1(1i) and later
CSCvj90385	With a uniform distribution of EPs and traffic flows, a fabric module in slot 25 sometimes reports far less than 50% of the traffic compared to the traffic on fabric modules in non-FM25 slots.	4.1(1i) and later

Bug ID	Description	Exists in
CSCvm71833	Switch upgrades fail with the following error: Version not compatible.	4.1(1i) and later

- In 4.1 or later, a software check has been added to identify Fiber Channel (FC) and Ethernet transceivers. Before ACI 4.1, this check was not present in the software. This check is required to make sure FC ports and Ethernet ports are properly identified. All transceivers that have the correct SPROM programming should continue to work post-upgrade. If any transceivers have an incorrectly programmed SPROM which does not correctly identify them as an FC or Ethernet transceivers, they will fail transceiver validation and fail to come up on 4.1. In this scenario, contact your respective vendors to update and address the programmed SPROM values.
- If you use the REST API to upgrade an app, you must create a new firmware.OSource to be able to download a new app image.
- In a multipod configuration, before you make any changes to a spine switch, ensure that there is at least one operationally "up" external link that is participating in the multipod topology. Failure to do so could bring down the multipod connectivity. For more information about multipod, see the Cisco Application Centric Infrastructure Fundamentals document and the Cisco APIC Getting Started Guide.
- With a non-english SCVMM 2012 R2 or SCVMM 2016 setup and where the virtual machine names are specified in non-english characters, if the host is removed and re-added to the host group, the GUID for all the virtual machines under that host changes. Therefore, if a user has created a micro segmentation endpoint group using "VM name" attribute specifying the GUID of respective virtual machine, then that micro segmentation endpoint group will not work if the host (hosting the virtual machines) is removed and re-added to the host group, as the GUID for all the virtual machines would have changed. This does not happen if the virtual name has name specified in all english characters.
- A query of a configurable policy that does not have a subscription goes to the policy distributor. However, a query of a configurable policy that has a subscription goes to the policy manager. As a result, if the policy propagation from the policy distributor to the policy manager takes a prolonged amount of time, then in such cases the query with the subscription might not return the policy simply because it has not reached policy manager yet.

Compatibility Information

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

Virtualization Compatibility Information

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

- For a table that shows the supported virtualization products, see the ACI Virtualization Compatibility Matrix at the following URL:

<https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/aci/virtualization/matrix/virtmatrix.html>

- This release supports VMM Integration and VMware Distributed Virtual Switch (DVS) 6.5.x. For more information about guidelines for upgrading VMware DVS from 5.x to 6.x and VMM integration, see the *Cisco ACI Virtualization Guide, Release 4.1(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>

Compatibility Information

- This release supports the Microsoft System Center Virtual Machine Manager (SCVMM) 2012 Update Rollup 9, 10, and 11 releases and the Microsoft Windows Azure Pack Update Rollup 9, 10, and 11 releases.
- This release supports Microsoft SCVMM Update Rollup 1, 2, 2.1, and 3 releases for SCVMM 2016 and Microsoft Hyper-V 2016.
- For information about Cisco APIC compatibility with Cisco UCS Director, see the appropriate *Cisco UCS Director Compatibility Matrix* document at the following URL:

<https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-director/products-device-support-tables-list.html>
- If you use Microsoft vSwitch and want to downgrade to Cisco APIC Release 2.3(1) from a later release, you first must delete any microsegment EPGs configured with the Match All filter.

Hardware Compatibility Information

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

- For the supported hardware, see the *Cisco NX-OS Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches, Release 14.1(1)* at the following location:

<https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html>
- To connect the N2348UPQ to Cisco ACI leaf switches, the following options are available:
 - Directly connect the 40G FEX ports on the N2348UPQ to the 40G switch ports on the Cisco ACI leaf switches
 - Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the 10G ports on all other Cisco ACI leaf switches.

Note: A fabric uplink port cannot be used as a FEX fabric port.
- M5 Cisco APIC supports dual speed 10G and 25G interfaces. The M4 Cisco APIC and previous versions support only the 10G interface. Connecting the Cisco APIC to the Cisco ACI fabric requires a same speed interface on the Cisco ACI leaf switch. You cannot connect the Cisco APIC directly to the Cisco N9332PQ ACI leaf switch, unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the Cisco N9332PQ switch auto-negotiate to 10G without requiring any manual configuration.
- The Cisco N9K-X9736C-FX (ports 29 to 36) and Cisco N9K-C9364C-FX (ports 49-64) switches do not support 1G SFPs with QSA.
- Cisco N9K-C9508-FM-E2 fabric modules must be physically removed before downgrading to releases earlier than Cisco APIC 3.0(1).
- The Cisco N9K-C9508-FM-E2 and N9K-X9736C-FX locator LED enable/disable feature is supported in the GUI and not supported in the Cisco ACI NX-OS Switch CLI.
- Contracts using matchDscp filters are only supported on switches with "EX" on the end of the switch name. For example, N9K-93108TC-EX.
- N9K-C9508-FM-E2 and N9K-C9508-FM-E fabric modules in the mixed mode configuration are not supported on the same spine switch.

Compatibility Information

- The N9K-C9348GC-FXP switch does not read SPROM information if the PSU is in a shut state. You might see an empty string in the Cisco APIC output.
- When the fabric node switch (spine or leaf) is out-of-fabric, the environmental sensor values, such as Current Temperature, Power Draw, and Power Consumption, might be reported as "N/A." A status might be reported as "Normal" even when the Current Temperature is "N/A."
- First generation switches (models without -EX, -FX, or later designations) do not support Contract filters with match type "IPv4" or "IPv6." Only match type "IP" is supported. Because of this, a contract will match both IPv4 and IPv6 traffic when the match type of "IP" is used.

Adaptive Security Appliance (ASA) Compatibility Information

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

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

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

Miscellaneous Compatibility Information

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

- This release supports the following software:
 - Cisco NX-OS Release 14.1(1)
 - Cisco AVS, Release 5.2(1)SV3(3.11)

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

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

 - Cisco UCS Manager software release 2.2(1c) or later is required for the Cisco UCS Fabric Interconnect and other components, including the BIOS, CIMC, and the adapter.
- This release supports the following firmware:
 - 4.0(2f) CIMC HUU ISO (recommended) for UCS C220/C240 M4 and M5
 - 4.0(1a) CIMC HUU ISO for UCS C220 M5
 - 3.0(4j) CIMC HUU ISO (recommended) for UCS C220/C240 M3
 - 3.0(4d) CIMC HUU ISO for UCS C220/C240 M3 and M4
 - 3.0(3f) CIMC HUU ISO for UCS C220/C240 M4
 - 3.0(3e) CIMC HUU ISO for UCS C220/C240 M3
 - 2.0(13i) CIMC HUU ISO

Usage Guidelines

- 2.0(9c) CIMC HUU ISO
- 2.0(3i) CIMC HUU ISO
- This release supports the partner packages specified in the *L4-L7 Compatibility List Solution Overview* document at the following URL:
<https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/solution-overview-listing.html>
- A known issue exists with the Safari browser and unsigned certificates, which applies when connecting to the Cisco APIC GUI. For more information, see the *Cisco APIC Getting Started Guide*.
- For compatibility with OpenStack and Kubernetes distributions, see the *Cisco Application Policy Infrastructure Controller OpenStack and Container Plugins Release Notes, Release 4.1(1)*.

Usage Guidelines

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

Virtualization Compatibility Guidelines

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

- Do not separate virtual port channel (vPC) member nodes into different configuration zones. If the nodes are in different configuration zones, then the vPCs' **modes become mismatched if the interface policies are modified** and deployed to only one of the vPC member nodes.
- If you are upgrading VMware vCenter 6.0 to vCenter 6.7, you should first delete the following folder on the VMware vCenter: C:\ProgramData\cisco_aci_plugin.

If you do not delete the folder and you try to register a fabric again after the upgrade, you will see the following error message:

```
Error while saving setting in C:\ProgramData\cisco_aci_plugin\

```

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

- If the communication between the Cisco APIC and VMware vCenter is impaired, some functionality is adversely affected. The Cisco APIC relies on the pulling of inventory information, updating VDS configuration, and receiving event notifications from the VMware vCenter for performing certain operations.
- After you migrate VMs using a cross-data center VMware vMotion in the same VMware vCenter, you might find a stale VM entry under the source DVS. This stale entry can cause problems, such as host removal failure. The workaround for this problem is to enable "Start monitoring port state" on the vNetwork DVS. See the KB topic "Refreshing port state information for a vNetwork Distributed Virtual Switch" on the VMware Web site for instructions.
- When creating a vPC domain between two leaf switches, both switches must be in the same switch generation. Switches not in the same generation are not compatible vPC peers. The generations are as follows:

Usage Guidelines

- Generation 1—Cisco Nexus 9200 and 9300 platform switches without "EX" on the end of the switch name; for example, Cisco Nexus 93120TX.
- Generation 2—Cisco Nexus 9300-EX and FX platform switches; for example, Cisco Nexus 93108TC-EX.
- The following Red Hat Virtualization (RHV) guidelines apply:
 - We recommend that you use release 4.1.6 or later.
 - Only one controller (compCtrlr) can be associated with a Red Hat Virtualization Manager (RHVM) data center.
 - Deployment immediacy is supported only as pre-provision.
 - IntraEPG isolation, micro EPGs, and IntraEPG contracts are not supported.
 - Using service nodes inside a RHV domain have not been validated.

GUI Guidelines

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

- The Cisco APIC GUI includes an online version of the Quick Start Guide that includes video demonstrations.
- To reach the Cisco APIC CLI from the GUI: choose System > Controllers, highlight a controller, right-click, and choose "launch SSH". To get the list of commands, press the escape key twice.
- The Basic GUI mode is deprecated. We do not recommend using Cisco APIC Basic mode for configuration. However, if you want to use Cisco APIC Basic mode, use the following URL:

APIC_URL/indexSimple.html

CLI Guidelines

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

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

Layer 2 and Layer 3 Configuration Guidelines

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

- For Layer 3 external networks created through the API or GUI and updated through the CLI, protocols need to be enabled globally on the external network through the API or GUI, and the node profile for all the participating nodes needs to be added through the API or GUI before doing any further updates through the CLI.
- When configuring two Layer 3 external networks on the same node, the loopbacks need to be configured separately for both Layer 3 networks.

Usage Guidelines

- All endpoint groups (EPGs), including application EPGs and Layer 3 external EPGs, require a domain. Interface policy groups must also be associated with an Attach Entity Profile (AEP), and the AEP must be associated with domains. Based on the association of EPGs to domains and of the interface policy groups to domains, the ports VLANs that the EPG uses are validated. This applies to all EPGs including bridged Layer 2 outside and routed Layer 3 outside EPGs. For more information, see the *Cisco APIC Layer 2 Networking Configuration Guide*.

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

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

IP Address Guidelines

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

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

Miscellaneous Guidelines

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

- User passwords must meet the following criteria:
 - Minimum length is 8 characters
 - Maximum length is 64 characters
 - Fewer than three consecutive repeated characters
 - At least three of the following character types: lowercase, uppercase, digit, symbol
 - Cannot be easily guessed
 - Cannot be the username or the reverse of the username
 - Cannot be any variation of " cisco" , " isco" , or any permutation of these characters or variants obtained by changing the capitalization of letters therein
- In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.
- The power consumption statistics are not shown on leaf node slot 1.
- If you defined multiple login domains, you can choose the login domain that you want to use when logging in to a Cisco APIC. By default, the domain drop-down list is empty, and if you do not choose a domain, the DefaultAuth domain is used for authentication. This can result in login failure if the username is not in the DefaultAuth login domain. As such, you must enter the credentials based on the chosen login domain.
- A firmware maintenance group should contain a maximum of 80 nodes.
- When contracts are not associated with an endpoint group, DSCP marking is not supported for a VRF with a vzAny contract. DSCP is sent to a leaf switch along with the actrl rule, but a vzAny contract does not have an actrl rule. Therefore, the DSCP value cannot be sent.
- The Cisco APICs must have 1 SSD and 2 HDDs, and both RAID volumes must be healthy before upgrading to this release. The Cisco APIC will not boot if the SSD is not installed.
- In a multipod fabric setup, if a new spine switch is added to a pod, it must first be connected to at least one leaf switch in the pod. Then the spine switch is able to discover and join the fabric.

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

- A maximum of eight span sessions (port only, port-VLAN only, or tenant span only) can be configured at a time in one direction (either ingress or egress). If the direction is both (ingress and egress), the maximum span sessions allowed is four. For a combination of span types, limit the number of sessions to four in one direction.
- For a Cisco APIC REST API query of event records, the Cisco APIC system limits the response to a maximum of 500,000 event records. If the response is more than 500,000 events, it returns an error. Use filters to refine your queries. For more information, see *Cisco APIC REST API Configuration Guide*.

Usage Guidelines

- Subject Alternative Names (SANs) contain one or more alternate names and uses any variety of name forms for the entity that is bound by the Certificate Authority (CA) to the certified public key. These alternate names are called "Subject Alternative Names" (SANs). Possible names include:
 - DNS name
 - IP address
- If a node has port profiles deployed on it, some port configurations are not removed if you decommission the node. You must manually delete the configurations after decommissioning the node to cause the ports to return to the default state. To do this, log into the switch, run the `setup-clean-config.sh` script, wait for the script to complete, then enter the reload command.
- When using the SNMP trap aggregation feature, if you decommission Cisco APICs, the trap forward server will receive redundant traps.
- If you upgraded from a release prior to the 3.2(1) release and you had any apps installed prior to the upgrade, the apps will no longer work. To use the apps again, you must uninstall and reinstall them.
- Connectivity filters were deprecated in the 3.2(4) release. Feature deprecation implies no further testing has been performed and that Cisco recommends removing any and all configurations that use this feature. The usage of connectivity filters can result in unexpected access policy resolution, which in some cases will lead to VLANs being removed/reprogrammed on leaf interfaces. You can search for the existence of any connectivity filters by using the `moquery` command on the APIC:
 - > `moquery -c infraConnPortBlk`
 - > `moquery -c infraConnNodeBlk`
 - > `moquery -c infraConnNodeS`
 - > `moquery -c infraConnFexBlk`
 - > `moquery -c infraConnFexS`

Related Documentation

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

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

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

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

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

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

New Documentation

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

- *Cisco ACI and SDWAN Integration*
- *Cisco ACI Configuration Files: Import and Export*
- *Cisco ACI Virtual Edge Configuration Guide, Release 2.1(1)*
- *Cisco ACI Virtual Edge Installation Guide, Release 2.1(1)*
- *Cisco ACI Virtual Edge Release Notes, Release 2.1(1)*
- *Cisco ACI Virtual Pod Getting Started Guide, Release 4.1(1)*
- *Cisco ACI Virtual Pod Installation Guide, Release 4.1(1)*
- *Cisco ACI Virtual Pod Release Notes, 4.1(1)*
- *Cisco ACI Virtualization Guide, Release 4.1(1)*
- *Cisco APIC Basic Configuration Guide, Release 4.1(x)*
- *Cisco APIC Getting Started Guide, Release 4.1(x)*
- *Cisco APIC Layer 2 Networking Configuration Guide, Release 4.1(x)*
- *Cisco APIC Layer 3 Networking Configuration Guide, Release 4.1(x)*
- *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.1(x)*

Related Documentation

- *Cisco APIC NX-OS Style CLI Command Reference, Release 4.1(1)*
- *Cisco APIC Security Configuration Guide, Release 4.1(x)*
- *Cisco APIC Troubleshooting Guide, Release 4.1(x)*
- *Cisco Application Centric Infrastructure Fundamentals, Release 4.1(x)*
- *Cisco Application Centric Infrastructure Fundamentals, Release 4.1(x)*
- *Cisco Application Virtual Switch Configuration Guide, Release 5.2(1)SV3(3.25)*
- *Cisco Application Virtual Switch Installation Guide, Release 5.2(1)SV3(3.25)*
- *Cisco Application Virtual Switch Release Notes, 5.2(1)SV3(3.25)*

You can find these documents on 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>

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

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

© 2019 Cisco Systems, Inc. All rights reserved.