Cisco Application Policy Infrastructure Controller Release Notes, Release 4.0(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 14.0(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
October 24, 2018	4.0(1h): Release 4.0(1h) became available.
November 21, 2018	4.0(1h): In the Open Bugs section, added bug CSCvn15374.

Date	Description
December 21, 2018	In Miscellaneous Guidelines section, added information about SSD over-provisioning.
January 23, 2019	In Miscellaneous Guidelines section, added the following text: 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.
March 14, 2019	In the New Software Features section, for the fabric rendezvous point feature, added that auto-RP and bootstrap router (BSR) are not supported.
March 25, 2019	In the Miscellaneous Compatibility Information section, added: — 4.0(2f) CIMC HUU ISO (recommended) for UCS C220/C240 M4 and M5 — 3.0(4j) CIMC HUU ISO (recommended) for UCS C220/C240 M3
March 26, 2019	In the Miscellaneous Compatibility Information section, added: — 4.0(1a) CIMC HUU ISO for UCS C220 M5
April 3, 2019	In the Miscellaneous Guidelines section, added mention that connectivity filters are deprecated.
May 29, 2019	4.0(1h): In the Open Bugs section, added bug CSCvn79128.
July 11, 2019	4.0(1h): In the Open Bugs section, added bug CSCvj89771.
July 17, 2019	4.0(1h): In the Open Bugs section, added bug CSCvq39922.
July 22, 2019	4.0(1h): In the Open Bugs section, added bug CSCvq39764.
August 14, 2019	4.0(1h): In the Open Bugs section, added bugs CSCvp38627 and CSCvp82252.
September 10, 2019	In the Known Behaviors section, added the following bullet: ■ When there are silent hosts across sites, ARP glean messages might not be forwarded to remote sites if a 1st generation ToR switch (switch models without -EX or -FX in the name) happens to be in the transit path and the VRF is deployed on that ToR switch, the switch does not forward the ARP glean packet back into the fabric to reach the remote site. This issue is specific to 1st generation transit ToR switches and does not affect 2nd generation ToR switches (switch models with -EX or -FX in the name). This issue breaks the capability of discovering silent hosts.
September 17, 2019	4.0(1h): In the Open Bugs section, added bug CSCuu17314 and CSCve84297.
October 3, 2019	In the Miscellaneous Guidelines section, added the bullet that begins as follows: ■ Fabric connectivity ports can operate at 10G or 25G speeds (depending on the model of the APIC server) when connected to leaf switch host interfaces.

Date	Description
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.
October 8, 2019	In the Miscellaneous Compatibility Information section, updated the supported 4.0(4), 4.0(2), and 3.0(4) CIMC releases to: — 4.0(4e) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3) — 4.0(2g) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) — 3.0(4l) CIMC HUU ISO (recommended) for UCS C220/C240 M3 (APIC-L1/M1)

Contents

This document includes the following sections:

New and Changed Information

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

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

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

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
Cisco ACI Virtual Pod	Cisco ACI Virtual Pod (vPod) enables you to extend the Cisco ACI fabric into bare-metal cloud environments and other remote locations. Cisco ACI vPod is supported as a vLeaf switch for Cisco APIC with the VMware ESXi hypervisor. It manages a data center defined by the VMware vCenter Server. Cisco ACI vPod includes two types of virtual machine (VM) for the control planes: a virtual spine (vSpine) switch and a virtual leaf (vLeaf) switch. It also includes Cisco ACI Virtual Edge as the forwarding module on the compute node or host. For more information, see the following documents: ■ Cisco ACI Virtual Pod Release Notes ■ Cisco ACI Virtual Pod Installation Guide ■ Cisco ACI Virtual Pod Getting Started Guide	■ Cisco ACI vPod is in limited availability in Cisco APIC release 4.0(1). Contact your Cisco account team before using Cisco ACI vPod or Cisco ACI Virtual Edge as part of Cisco ACI vPod. ■ The remote location must have at least two servers where you can run the VMware ESXi hypervisor. ■ Deploy each virtual spine (vSpine) and virtual leaf (vLeaf) pair on two separate hosts with one vSpine and one vLeaf on each host. ■ At initial release, each instance of Cisco ACI vPod supports only two vSpine switches and two vLeafs--–one vSpine and one vLeaf on each host. ■ You can have up to eight instances of Cisco ACI Virtual Edge in each Cisco ACI vPod.
Cisco APIC policy export without additional configuration and support for the RO admin	When deployed and configured to do so, the Cisco Network Assurance Engine (NAE) creates export policies in the Cisco APIC for collecting data at timed intervals. You can identify a Cisco NAE export policy by its name, which is based on the assurance control configuration. If you delete a Cisco NAE export policy in the Cisco APIC, the Cisco NAE export policy will reappear in the Cisco APIC. For more information, see the *Cisco APIC Basic Configuration Guide, Release 4.0(1)*.	We recommend not deleting the Cisco NAE export policies.
Cisco APIC-X	Cisco APIC-X is a dedicated Cisco APIC controller that is used specifically for running telemetry applications.	None

Feature	Description	Guidelines and Restrictions
	For more information, see the *Cisco APIC-X* document.	
Configuration synchronization issue reporting	If you encounter an issue with Cisco APIC, you can check the new Config Sync Issues link in the GUI to see if there are any transactions involving user-configurable objects that have yet to take effect. You can use information in the panel to help with debugging. For more information, see the *Cisco APIC Troubleshooting Guide, Release 4.0(1)*.	■ Clicking the Config Sync Issues link displays results only if there are any pending transactions. ■ Pending transactions are not configurable in the output table.
Fabric rendezvous point	This feature enables you to configure a fabric rendezvous point (RP) on all leaf switches where PIM is enabled on the VRF instance, which is required for inter-VRF multicast. For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide, Release 4.0(1)*.	■ Fabric RP does not support the following features: — Fast-convergence mode — Auto-RP — Bootstrap router (BSR) ■ The fabric IP: — Must be unique across all the static RP entries within the static RP and fabric RP. — Cannot be one of the Layer 3 out router IDs
Fabric-wide CPU, memory utilization, and temperature dashboard	CPU and memory utilization information is now available for the leaf switches and spine switches, provided at the fabric and pod levels. Temperature information is also available, where the temperature for the card with the highest temperature within the leaf switches or spine switches is displayed.	None.
FCoE support enhancement	The following capabilities are added: ■ Virtual port channel (vPC) with SAN boot ■ A virtual Fibre Channel (vFC) port can be bound to a member of a vPC For more information, see the *Cisco APIC Layer 2 Networking Configuration Guide, Release 4.0(1)*.	None.
Mini ACI fabric and virtual APIC	Cisco APIC now supports small scale deployments of Cisco APIC clusters with 2 of the 3 nodes installed inside VMware ESXi virtual machines. For more information, see *Cisco Mini ACI Fabric and*	For the small scale deployment scalability limits, see the *Verified Scalability Guide for Cisco APIC, Release 4.0(1), Multi-Site,*

Feature	Description	Guidelines and Restrictions
	Virtual APICs document.	*Release 2.0(1), and Cisco Nexus 9000 Series ACI-Mode Switches, Release 14.0(1)*.
Remote leaf switch enhancements	The remote leaf switch feature now supports the following features: ■ Endpoint tracker ■ Layer 4 to Layer 7 services ■ lLocal switching without a spine proxy ■ MACsec ■ Netflow ■ Policy-based redirect for tracking service nodes using IP SLA monitoring ■ Policy-based redirect resilient hashing ■ Q-in-Q encapsulation mapping for EPGs For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide, Release 4.0(1)*.	None.

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
Certificate-based authentication	You can log in using certificate-based authentication. For more information, see the *Cisco APIC Security Configuration Guide, Release 4.0(1)*.	■ Cisco ACI Multi-Site, VCPlugin, VRA, and SCVMM are not supported for certificate-based authentication. — Only one certificate-based root can be active per pod. — Certificate-based authentication must be disabled before downgrading from any releases to release 4.0(1). ■ To terminate a certificate-based authentication session,

Feature	Description	Guidelines and Restrictions
		you must log out and then remove the CAC card.
Dataplane IP learning per VRF	While endpoint learning is identified as both IP and MAC and is specific to PBR-related configurations, dataplane IP learning is specific to IP addressing only in VRFs. In APIC, you can enable or disable dataplane IP learning at the VRF level. For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide, Release 4.0(1)*.	■ When dataplane IP learning per VRF is disabled, all the remote IP address entries in the tenant VRF are removed. The local IP entries are aged out and, subsequently, will not be relearned through the dataplane, but can still be learned from the control plane. ■ When dataplane IP learning per VRF is disabled, already learned local IP endpoints are retained and require control plane refreshes to be kept alive (assuming IP aging is also enabled). Data path L3 traffic will not keep IP endpoints alive. ■ For Northstar/Donner-based ToRs, when dataplane IP learning per VRF is disabled, remote MAC addresses are not learned. Hardware Proxy mode on the corresponding BDs must be configured.
EPG shutdown	A new checkbox has been added to Create Application EPG and the EPG window allowing you to shut down the selected EPG. When the EPG is in "shutdown" mode, the ACI policy configuration related to the EPG is removed from all switches. For more information, see the online help.	None.
Fibre Channel NPV support enhancements	The following capabilities are added: ■ NPIV mode support ■ Fibre Channel (FC) host (F) port connectivity in 4, 16, 32G and auto speed configurations	None.

Feature	Description	Guidelines and Restrictions
	■ Fibre Channel (FC) uplink (NP) port connectivity in 4, 8, 16, 32G and auto speed configurations ■ Port-channel support on FC uplink ports ■ Trunking support on FC uplink ports For more information, see the *Cisco APIC Layer 2 Networking Configuration Guide, Release 4.0(1)*.	
GUI enhancement - single browser session	When logged in to the Cisco APIC, you can open additional browser tabs or windows without additional logins. For more information, see the *Cisco APIC Getting Started Guide, Release 4.0(1)*.	None.
Host route support	You can enable host-based routing on the bridge domain so that individual host routes (/32 prefixes) are advertised from the border leaf switches. For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide, Release 4.0(1)*.	Border leaf switches along with the subnet advertise the individual endpoint (EP) prefixes. The route information is advertised only if the host is connected to the local POD. If the EP is moved away from the local POD or after the EP is removed from the EP database (even if the EP is attached to a remote leaf switch), the route advertisement is then withdrawn.
Inter-VRF multicast	This feature enables the source VRF instance to perform the reverse path forwarding (RPF) lookup for a multicast route in the receiver VRF instance. For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide, Release 4.0(1)*.	■ All sources for a particular group must be in the same VRF instance (the source VRF instance). ■ You must have a configured fabric rendezvous point (RP). ■ Source VRF instance and source EPGs must be present on all leaf switches where there are receiver VRF instances. ■ For ASM: — The RP must be in the same VRF as the sources (the source VRF instance). — The source VRF instance must be using fabric

Feature	Description	Guidelines and Restrictions
		RP. — The same RP address configuration must be applied under the source and all receiver VRF instances for the given group-range.
L3Out support in service graphs	If a consumer or provider EPG is connected to an external routed network, the network can now be selected through the Service Graph wizard. For more information, see the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.0(1)*.	None.
Layer 3 destination (VIP) in the multi-tier application profile wizard	Through the Multi-Tier Application Profile wizard, you can now terminate Layer 3 traffic on the connector. For more information, see the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.0(1)*.	This setting is not considered under the following conditions: ■ Policy-based redirect is configured on the interface ■ The redirect capability is not enabled on the service node
MACsec encryption support on remote leaf switches	MACsec is now supported on remote leaf switches. For more information, see the *Cisco APIC Layer 2 Networking Configuration Guide, Release 4.0(1)*.	None.
Policy compression	Identical filter rules can now share a single TCAM table entry on switches, increasing the number of rules that can be configured in the fabric. For more information, see the *Cisco APIC Basic Configuration Guide, Release 4.0(1)*.	None.
Preferred group support in service graphs	EPGs created by service graphs can be included in contract preferred groups. A new policy (service EPG policy) is available for defining the preferred group membership type (include or exclude). Once configured, it can be applied through the device selection policy or through the application of a service graph template. For more information, see the *Cisco APIC Basic Configuration Guide, Release 4.0(1)* and *Cisco APIC Layer*	None.

Feature	Description	Guidelines and Restrictions
	4 to Layer 7 Services Deployment Guide, Release 4.0(1).	
QoS enhancements	The Cisco APIC now supports QoS levels 4, 5, and 6, and has configuration support for QoS L3Outs. For more information, see the *Cisco APIC QoS* document.	■ The number of classes that can be configured with the Strict priority still remains as 5. ■ The 3 new classes are not supported with non-EX and non-FX switches. ■ If traffic flows between non-EX or non-FX switches and EX or FX switches, the traffic will use QoS level 3. ■ For communicating with FEX for new classes, the traffic carries a Layer 2 COS value of 0.
QoS for ROCEv2	Cisco APIC now supports remote DMA over converged Ethernet (RoCE) technology for data transfer. You can enable RoCEv2 functionality in your fabric by configuring specific QoS options for Layer 3 traffic. For more information, see the *Cisco APIC QoS* document.	None.
SNMP trap support for BFD	The following new traps were added: ■ Rx/Tx High/Low Power Threshold ■ Rx/Tx Power Recovery Threshold ■ BFD Session Up ■ BFD Session Down For more information, see the *Cisco ACI MIB Support List*.	None.
Support for intra-EPG contracts in service graphs	You can now create service graphs using intra-EPG contracts for single node, 1-ARM PBRs and single node copy services. For more information, see the *Cisco APIC Basic Configuration Guide, Release 4.0(1)* and *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.0(1)*.	■ Intra-EPG contracts are not supported in AVS, AVE and Microsoft domains. Setting Intra-EPG contracts to be enforced may cause the ports to go into a blocked state in these domains. ■ Intra-EPG deny feature is not applicable for Service Graphs.

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
AppIQ	AppIQ/AppDynamics work together to map each application to a recommended Cisco APIC endpoint, which gives you a visual guide of the running state of the configurations. For more information, see the online help for this app.	None.
Cisco Tetration support for breakout interfaces	Cisco Tetration now supports the breakout interfaces feature of Cisco switches, which allows a single high-bandwidth switch port to be split into multiple logical interfaces.	None.
Cisco Tetration support for IP filtering on spine switches	Cisco Tetration now supports the IP filtering feature on spine switches in addition to previously being supported on leaf switches.	None.
Network Insights--– Resources app	The Network Insights - Resources app provides event analytics and license enhancements. For more information, see the online help for this app.	The Network Insights - Resources app is released with limited availability in Cisco APIC release 4.0(1). Contact your Cisco account team before using this app.

Virtualization

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

Table 5 New Software Features---Virtualization

Feature	Description	Guidelines and Restrictions
Enhanced LACP	You can improve uplink load balancing by applying different Link Aggregation Control Protocol (LACP) policies to different distributed virtual switch (DVS) uplink port groups. Cisco APIC now supports VMware's enhanced LACP feature, which is available for DVS 5.5 and later. Enhanced LACP is supported for VMware vSphere Distributed Switch (VDS) and Cisco ACI Virtual Edge. For more information, see the *Cisco ACI Virtualization Guide, Release 4.0(1)* and the *Cisco ACI Virtual Edge Configuration Guide*.	Enhanced LACP supports only active and passive LACP modes. Enhanced LACP is not available for Cisco ACI Virtual Edge when Cisco ACI Virtual Edge is part of Cisco ACI Virtual Pod. If you want to use a Link Aggregation Control Protocol (LACP) port channel with VMware DVS 6.6 and later,

Feature	Description	Guidelines and Restrictions
		you must create an enhanced LACP policy. See the "Enhanced LACP Support" section in the *Cisco ACI Virtual Edge Configuration Guide* and the *Cisco ACI Virtualization Guide*.
Exporting an existing VMware VDS to a ACI VMM domain	You can import a VMware VDS configured in the VMware vCenter into a Cisco ACI VMM domain. You can import the VDS if it resides under a network folder with the same name as the VDS. You import the VDS by creating a VDS domain in Cisco APIC with the same name as the VDS. For more information, see the *Cisco ACI Virtualization Guide, Release 4.0(1)*.	The VDS that you want to export from VMware vCenter must reside under a network folder with the same name as the VDS.
Promotion of VMM domains from read-only to fully managed	Existing read-only VMM domains can now be promoted to fully managed read-write VMM domains, enabling Cisco APIC to manage the configuration of the VDS in the VMware vCenter for any created EPGs and policies. For more information, see the *Cisco ACI Virtualization Guide, Release 4.0(1)*.	None.
Service VM orchestration	Service virtual machine (VM) orchestration is a policy-based feature that enables you to create and manage service VMs easily with Cisco APIC. Service VM orchestration also streamlines the configuration of service VMs, also known as concrete devices (CDev) and groups them into a device cluster, also known as a logical device (LDev). For more information, see the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.0(1)*.	Service VM orchestration is supported only for Cisco Adaptive Security Virtual Appliance (ASAv) and Palo Alto Networks devices.
vSphere proactive HA support for Cisco ACI Virtual Edge	You can improve Cisco ACI Virtual Edge availability by using VMware vSphere Proactive HA in vCenter 6.5. Cisco APIC and VMware vCenter work together to detect a nonworking Cisco ACI Virtual Edge, isolate its host, and move its VMs to a functioning host, preserving network connectivity. For more information, see the *Cisco ACI Virtual Edge Installation Guide*.	vSphere Proactive HA is not available for Cisco ACI Virtual Edge when it is part of Cisco ACI Virtual Pod.
VXLAN load-balancing and extra uplinks for Cisco ACI Virtual Edge	VXLAN load balancing is now a built-in feature for Cisco ACI Virtual Edge. You do not need to do any configuration to enable VXLAN load balancing. Extra uplinks also have been added to accommodate	VXLAN load balancing and extra uplinks are not supported for Cisco ACI Virtual Edge when it is part of Cisco ACI Virtual Pod (vPod

Feature	Description	Guidelines and Restrictions
	VXLAN load-balancing and improve overall performance. For more information, see the *Cisco ACI Virtual Edge Configuration Guide*.	mode).

New Hardware Features

For new hardware features, see the *Cisco NX-OS Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches, Release 14.0(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:

- In this release, the data plane forwarding impact to endpoints is decreased because the front panel port bring up is delayed during reload scenarios. This enhancement allows the upstream protocols (VXLAN, MP-BGP, and COOP) to converge.
- In the Apps tab, if you open an app, navigate to another menu tab, then navigate back to the Apps menu tab, the app now remains open. The app also continues to perform the operation that it was doing before you navigated away. In previous releases, the app would close if you navigated to a different menu tab, which also stopped the app's current operation.
- The Capacity Dashboard (Operations > Capacity Dashboard) has been reorganized. In previous releases, the dashboard displayed all of its information on one screen. In this release, the information is split between the new Fabric Capacity tab and Leaf Capacity tab. In addition, the leaf switches listed in the Leaf Capacity tab have a Configure Profile link, which opens the Forward Scale Profile form. The form enables you to configure the scale profile of the switch, if the switch model supports multiple profiles.
- Starting with this release, you cannot use Bash to upgrade the Cisco APIC and switch software. Use the NX-OS style CLI to upgrade the Cisco APIC and switch software instead. For more information, see the *Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*.
- The procedures for upgrading the software using the GUI has changed. For more information, see the *Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*.

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 4.0(1) releases in which the bug exists. A bug might also exist in releases other than the 4.0(1) releases.

Table 6 Open Bugs in This Release

Bug ID	Description	Exists in
CSCuu17314	CDP is not enabled on the management interfaces for the leaf switches and spine switches.	4.0(1h) and later
CSCve84297	A service cannot be reached by using the APIC out-of-band management that exists within the 172.17.0.0/16 subnet.	4.0(1h) and later
CSCvj89771	The Virtual Machine Manager (vmmmgr) process crashes and generates a core file.	4.0(1h) and later
CSCvk22596	There is a policyelem core after removing an L3Out in the same VRF instance as the NetFlow exporter.	4.0(1h) and later
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.	4.0(1h) and later

Bug ID	Description	Exists in
CSCvn15374	When upgrading Cisco APICs, constant heartbeat loss is seen, which causes the Cisco APICs to lose connectivity between one another. In the Cisco APIC appliance_director logs, the following message is seen several hundred times during the upgrade: appliance_director||DBG4||...||Lost heartbeat from appliance id= ... appliance_director||DBG4||...||Appliance has become unavailable id= ... On the switches, each process (such as policy-element) see rapidly changing leader elections and minority states: adrs_rv||DBG4||||Updated leader election on replica=(6,26,1)	4.0(1h) and later
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.	4.0(1h) and later
CSCvp38627	Some tenants stop having updates to their state pushed to the APIC. The aim-aid logs have messages similar to the following example: An unexpected error has occurred while reconciling tenant tn-prj_...: long int too large to convert to float	4.0(1h) and later
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	4.0(1h) and later

Bug ID	Description	Exists in

CSCvp82252	While modifying the host route of OpenStack, the following subnet trace is generated:
	Response :
	{
	"NeutronError": {
	"message": "Request Failed: internal server error while processing your request.",
	"type": "HTTPInternalServerError",
	"detail": ""
	}
	}
		4.0(1h) and later

CSCvq39764	When you click Restart for the Microsoft System Center Virtual Machine Manager (SCVMM) agent on a scaled-out setup, the service may stop. You can restart the agent by clicking Start.	4.0(1h) and later
CSCvq39922	Specific operating system and browser version combinations cannot be used to log in to the APIC GUI. Some browsers that are known to have this issue include (but might not be limited to) Google Chrome version 75.0.3770.90 and Apple Safari version 12.0.3 (13606.4.5.3.1).	4.0(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 7 Resolved Bugs in This Release

Bug ID	Description	Fixed in
CSCvc79359	This enhancement requests is to add support for the configuration of the DVS and AVS port binding mode from APIC GUI.	4.0(1h)
CSCvg17464	Currently there is no mechanism to monitor the usage of a resource pool (VXLAN, VLAN, or VSAN) within Cisco APIC. This may cause policy deployment problems if a resource is requesting an ID from an exhausted pool.	4.0(1h)
CSCvg29902	Stats are not visible for CoPP on any port where traffic is flowing.	4.0(1h)
CSCvg45850	If packet drops are encountered because of CRC errors, there are no faults generated in the Cisco APIC GUI. Ideally, a fault should be generated when the CRC keeps growing so that syslog/snmp-trap could be triggered to notify the user.	4.0(1h)
CSCvg98661	The Cisco ACI fabric port counter cannot be collected by using SNMP.	4.0(1h)

Bug ID	Description	Fixed in
CSCvh42067	The Cisco APIC does not send varbind timeticks in traps.	4.0(1h)
CSCvh52171	Configuration zones have pending changes, but there is no warning or notification, thus it is very easy to forget that there are pending changes in the configuration zones.	4.0(1h)
CSCvh55189	API implementation currently allows you to delete the fvIp object using the REST API. However, this delete operation is not synchronized to the actual endpoint on the leaf switch and causes inconsistencies between the Cisco APIC objects and the leaf switch.	4.0(1h)
CSCvi08110	Policies cannot be configured in the Cisco APIC after performing an upgrade. The following error displays: "Error 400:System is not ready to receive new configuration." This issue is due to an invalid subnet being configured on the L3Outs in the system running a pre-1.2(2j) release.This issue has existed since the 2.3(1) release and will happen only when you upgrade from a pre-1.2(2j) release. In the 1.2(2j) release, this configuration valid and does not result in an error.	4.0(1h)
CSCvi19268	The health score for a leaf switch is reporting a low value. By expanding the objects, the connected and functional access ports have a 0% Health Score.	4.0(1h)
CSCvi59444	The stale fault delegate is raised when a configured syslog/callhome server is not reachable. It does not clear after configuring a successful syslog/callhome policy or after the deletion of non-reachable server policy.	4.0(1h)
CSCvi60841	Prior to this enhancement, the Cisco APIC GUI was not reporting CRC errors per interface. Now, the GUI reports CRC errors on a per-interface basis.	4.0(1h)
CSCvi86103	There are duplicate PVLAN entries in VMware vCenter. Depending on the version of Cisco APIC code, the Cisco APIC's vmmmgr process will also crash and create a core file.	4.0(1h)
CSCvi95657	On modifying a service parameter, the Cisco APIC sends 2 posts to the backend. The first post deletes all of the folders and parameters. The second post adds all of the remaining modified folders and parameters to the backend. These 2 posts will disrupt the running traffic.	4.0(1h)
CSCvj04166	The remote leaf TEP pool cannot be deleted after decommissioning the remote leaf and deleting the remote leaf vPC configuration.	4.0(1h)
CSCvj09453	The actrlRule is has the wrong destination.	4.0(1h)
CSCvj12175	When using a custom role that has admin permissions, the leaf switches nor the spine switches cannot be connected to using ssh. Also, the acidiag commands nor the fabric show commands cannot be run.	4.0(1h)
CSCvj15521	A link down trap is generated when a leaf switch or spine switch link is brought up.	4.0(1h)
CSCvj41914	An OpflexP core is seen on the leaf switch or spine switch. The leaf switch or spine switch will recover from this, and there should be no impact other than this core being generated and the the service being restarted.	4.0(1h)
CSCvj48153	Large scale interface configurations are not deployed after being configured on Cisco APIC. On the shard leader, the policy mgr CPU usage is high.	4.0(1h)

Bug ID	Description	Fixed in
CSCvj51464	Assume the following topology: Tenant 1: VRF 1 > EPG A, EPG B Tenant 2: VRF 2 > EPG C, EPG D If you provide a global contract from EPG A to be consumed by vzAny on VRF 2 (tenant 2), then communication between EPG A and B would be allowed, even though EPG B has no contracts configured. Zoning rules should be programmed on the consumer only, but in this case the rules are also applied on the provider side.	4.0(1h)
CSCvj51711	After making physical changes to the vPC interfaces, the health score of the leaf is 80, but there are no faults under the leaf switch. Under the Health tab for the leaf switch, the Network Connection Group object has a health score of 0.	4.0(1h)
CSCvj52529	When you create an IP address pool under the subnet of an EPG, only the IPv4 address is allowed from the GUI.	4.0(1h)
CSCvj64016	When trying to register a new spine switch, in the fabric membership, there is a serial number printed in hex. Example: 0x4647453230303530124354.	4.0(1h)
CSCvj65791	Fault F1651 is raised after failing to write to the remote location. It does not clear after a successful On Demand Techsupport or after deletion of the policy. The fault is subsequently unable to be removed by TAC using the various Test API methods available to them.	4.0(1h)
CSCvj75392	Cisco APIC can be seen repeatedly logging into the RHV controller at a rapid rate in the RHV Event tab. This can also lead to a memory usage increase on the controller, as each login is a new session. Specifically, the Postgres process on the RHV controller increases.	4.0(1h)
CSCvj77484	After creating an Cisco ACI Virtual Edge domain, you receive the following fault: "F0564 Controller profile <Controller IP> with name <Controller name> in datacenter <Data Canter name> in domain <AVE domain> configuration failed due to Missing infra VLAN for the controller."	4.0(1h)
CSCvj91044	There is an opflexp core in stats update. The opflexp process should recover and there should be no service impact.	4.0(1h)
CSCvj95652	Users are unable to login with TACACS+ on Cisco APICs when a DNS hostname is defined. Fault F0023 is observed on the TACACS+ provider.	4.0(1h)
CSCvj96267	Assigning any 169.x.x.x IP address to a ESX host vmk that is tied to a VMM DVS/port-group causes the following fault to be raised: Fault delegate: [FSM:FAILED]: Get IP address of the interface: vmkX on host Where "X" is the vmk #.	4.0(1h)
CSCvk01823	Decoy service (uwsqi processes) is holding memory after each time a CLI command is run. Memory utilization keeps increasing for each process until it reaches the max threshold of 8G.	4.0(1h)
CSCvk01926	DLC stuck after a failed try.	4.0(1h)

Bug ID	Description	Fixed in
CSCvk04065	When performing upgrades of Cisco ACI switches in the Cisco ACI fabric, the switches will disappear from the GUI during the reboot process.	4.0(1h)
CSCvk06927	Periodically, the following event is observed: <eventRecord affected="topology/pod-1/node-1/lon/svc-ifc_observer/rpl-local-local" cause="transition" changeSet="" childAction="" code="E4208012" created="2018-06-18T12:24:26.535+00:00" descr="[GenericSQLiteException] ErrorCode=5. Msg=database is locked. SQLiteError at base::Bool db::SQLiteStatement::exec():148. . Path=/data2/dbstats/observer_255.db" dn="subj-[topology/pod-1/node-1/lon/svc-ifc_observer/rpl-local-local]/rec-4295778251" id="4295778251" ind="modification" modTs="never" severity="major" status="" trig="admin,config,implicit" txId="18374686479677880037" user="internal"/>	4.0(1h)
CSCvk12786	Apps fail to install/uninstall/run when the cluster is not healthy and nodes are powered down/unreachable without being decommissioned.	4.0(1h)
CSCvk18442	When a trunk port group is initially created, it uses the port channel policy that is set upon the time of creation. Altering the port channel policy updates the EPG-provisioned port groups, but does not update the trunk port group.	4.0(1h)
CSCvk22426	The command "show running-config" prints the following error and aborts: Error while processing mode: route-profile Error while processing mode: template Error while processing mode: vrf Error while processing mode: leaf Error while processing mode: configure Error: No class with prefix "type" found	4.0(1h)
CSCvk23003	There are stale remote IP endpoints on border leaf switches due to not clearing the endpoints after disabling remote endpoint learning.	4.0(1h)
CSCvk23618	When using the snmpwalk application for cpmCPUMemoryUsed, cpmCPUMemoryFree, cpmCPUMemoryHCUsed, or cpmCPUMemoryHCFree, the values displayed are are invalid.	4.0(1h)
CSCvk24509	After an HP VC switchover, some stable objects remain with the previous switch. F0467 faults related to invalid path configuration can be observed. This issue has no impact on the traffic path.	4.0(1h)
CSCvk25228	rxload and txload do not update and stay at 1/255 regardless of traffic flow.	4.0(1h)
CSCvk26251	After upgrading, there are no contract associations under Security Policies in the Common tenant. However, in reality contracts are applied in the customer EPGs, but are not visible under Common contracts. The VRF instance association to bridge domains is broken. The operation tab does not show the associated bridge domain (only L3outs are present).	4.0(1h)
CSCvk26672	A deleted v3 user still exists when checked using the snmpwalk application.	4.0(1h)

Bug ID	Description	Fixed in
CSCvk27549	The consumer shadow EPG in an inter-VRF instance service graph does not update its pcTag to a global pcTag when an EPG consumes the inter-VRF instance contract. The contract was previously already deployed between a provider and consumer in the same VRF instance. When a provider EPG and consumer EPG are configured for inter-VRF instance communication, traffic is only permitted from the provider EPG to the consumer EPG when the pcTag of the provider is less than hexadecimal 0x4000/decimal 16384. When the provider pcTag is below this value, we considered it to be a global pcTag. If the provider pcTag is above this value, the packet is dropped with drop vector SECURITY_GROUP_DENY. Contract drops are seen for packets entering the fabric from the Layer 4 to Layer 7 service device's consumer-side interface with a non-global source pcTag. The issue does not occur when the service graph is removed from the contract subject.	4.0(1h)
CSCvk29490	In the pod peering profile under Infra > Policies, the column name "Control Plane TEP" is incorrect. It should actually be "Dataplane TEP."	4.0(1h)
CSCvk44519	After upgrading to the 3.2(2l) release, the Cisco APICs are fully fit and converged, but configuration changes to firmware groups do not work. The configuration changes are accepted without errors, but the changes are not reflected in the GUI. Other configurations made on shard-32 are also accepted, but appear to fail.	4.0(1h)
CSCvk45056	Cisco APIC reloads unexpectedly, and a vmcore is generated.	4.0(1h)
CSCvk45734	Prior to the 2.2 release, in the Cisco APIC CLI, you would configure the NTP template and add a server using the following commands: # template ntp-fabric default # server <IP address or name> prefer use-vrf <epg_name> In the 2.2 release and later, you must use "use-epg" instead of "use-vrf."	4.0(1h)
CSCvk50417	On a vMotion, there is a 9-second outage while the VM is migrated.	4.0(1h)
CSCvk57005	The spine switch reloads due to an opflex_proxy HAP reset.	4.0(1h)
CSCvk59292	When using Firefox 61.0.1 (64-bit) to configure the interface description under "Fabric -> inventory -> Pod 1 -> Physical Interface -> eth 1/1 -> config," the following error message is raised: Validation failed: Validation failed. infraHPathS cannot associate to: Rn=hpaths-user1-121-1	4.0(1h)
CSCvk60363	Analytics policies cannot be created with the same names as clusters that were configured and removed from the Cisco APIC previously.	4.0(1h)
CSCvk65851	The configuration import failed with the following error when importing a configuration which was exported using config export policy with AES encryption enabled. The following error appears when importing the configuration: Error: [shard 32] failed to apply tree: AuthKey must be provided when AuthType is provided	4.0(1h)

Bug ID	Description	Fixed in
CSCvk66627	When submitting an interface configuration under Fabric > Topology > Interfaces tab, the GUI stops at a Loading... screen and the configuration is not saved. When looking at the Developer Tools of your browser it is seen that the POST for /ncapi/config.json results in a 502 error.	4.0(1h)
CSCvk67458	Cisco ACI configuration zones have modes of Enabled or Disabled. A configuration zone mode of Enabled is the same as the default behavior (no configuration zone). A configuration zone mode of Disabled means that the configuration zone is active and new policy updates will be queued/postponed. This enhancement request is filed to rename Enabled to Inactive and Disabled to Active, as this would be clearer.	4.0(1h)
CSCvm06854	When looking at a VMM domain in the Cisco APIC, you may see faults saying that the last inventory pull returned partial.	4.0(1h)
CSCvm09583	CPU utilization on the leaf switch that is attached to the OpenStack compute/controller has high CPU utilization when the number of endpoints increases.	4.0(1h)
CSCvm11332	The Transport Gateway/Smart Software Manager Satellite product cannot be reregistered using the Cisco APIC GUI because the option "Reregister product if already registered" button is missing.	4.0(1h)
CSCvm12554	When an L3Out and application EPG are configured in a contract preferred group-enabled VRF instance, and the application EPG is deployed on a vPC or non-vPC, then only one leaf switch in the VPC has the prefix entry for the L3Out, or the ingress leaf switch (in the non-vPC case) does not have the prefix entry for the L3Out. In the vPC case, one leaf switch does not have the entry and drops the traffic. In the non-vPC case, the ingress leaf switch does not have the entry and drops the traffic.	4.0(1h)
CSCvm15454	The product Cisco Application Policy Infrastructure Controller (APIC) includes a version of the Linux kernel that is affected by the IP Fragment Reassembly Denial of Service Vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID: CVE-2018-5391 Cisco has confirmed that this product is impacted.	4.0(1h)
CSCvm46349	on_demand techsupport is not collected from leaf switches and spine switches, and the following error message is observed: Failed to open file=/var/log/dme/oldlog/tmp1536309556861/techsup_1536309556861 error=No child processes; return value=32560	4.0(1h)
CSCvm56674	After a leaf switch is upgraded or clean reloaded, newly created EPGs are not correctly deployed on the leaf switch. VMM inventory objects for the newly created EPGs are missing on the leaf switch.	4.0(1h)
CSCvm58089	When an IPv6 address is configured in the Cisco APIC GUI under Tenant MGMT > Node Management Addresses > Static Node Management Addresses, and the IPv6 address is given a prefix length such as /120 , /121 , or /122 , the address is programmed as /64 when checked using the ifconfig command on the Cisco APIC.	4.0(1h)

Bug ID	Description	Fixed in
CSCvm64156	Changing the control plane MTU to 9216 causes BGP to flap between the spine switches and leaf switches. As a result, the routes are not properly redistributed in the fabric. In the BGP logs, you can see the holdtime expiring and the neighbors between the leaf switches and spine switches consistently flapping.	4.0(1h)
CSCvm70003	Traffic from GOLF to EPG is dropping when the VRF instance is in enforced mode. Zoning rules are programmed properly. You see security drops and elam shows that source EPG ID is 0x0.	4.0(1h)
CSCvm79317	Duplicated DME logs are collected for ACI leaf switch running 13.2.	4.0(1h)
CSCvm79440	Non-DME logs include EPM/EPMC. HAL ELMC NX-OS are excluded for category-based tech-support collection.	4.0(1h)
CSCvm79579	A monitoring policy cannot be created to squelch (or suppress) the "IP detached" event, because the GUI does not display the event code.	4.0(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 4.0(1) releases in which the known behavior exists. A bug might also exist in releases other than the 4.0(1) releases.

Table 8 Known Behaviors in This Release

Bug ID	Description	Exists in
CSCuo52668	The Cisco APIC does not validate duplicate IP addresses that are assigned to two device clusters. The communication to devices or the configuration of service devices might be affected.	4.0(1h) and later
CSCuo79243	In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.	4.0(1h) and later
CSCuo79250	The node ID policy can be replicated from an old appliance that is decommissioned when it joins a cluster.	4.0(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.	4.0(1h) and later
CSCup79002	The hostname resolution of the syslog server fails on leaf and spine switches over in-band connectivity.	4.0(1h) and later
CSCuq21360	Following a FEX or switch reload, configured interface tags are no longer configured correctly.	4.0(1h) and later
CSCur39124	Switches can be downgraded to a 1.0(1) version if the imported configuration consists of a firmware policy with a desired version set to 1.0(1).	4.0(1h) and later
CSCur71082	If the Cisco APIC is rebooted using the CIMC power reboot, the system enters into fsck due to a corrupted disk.	4.0(1h) and later

Bug ID	Description	Exists in
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.	4.0(1h) and later
CSCut51929	The traffic destined to a shared service provider endpoint group picks an incorrect class ID (PcTag) and gets dropped.	4.0(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.	4.0(1h) and later
CSCuu61998	Newly added microsegment EPG configurations must be removed before downgrading to a software release that does not support it.	4.0(1h) and later
CSCuu64219	Downgrading the fabric starting with the leaf switch will cause faults such as policy-deployment-failed with fault code F1371.	4.0(1h) and later
CSCuw81638	The OpenStack metadata feature cannot be used with Cisco ACI integration with the Juno release (or earlier) of OpenStack due to limitations with both OpenStack and Cisco's ML2 driver.	4.0(1h) and later
CSCva32534	Creating or deleting a fabricSetupP policy results in an inconsistent state.	4.0(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 Cisco APIC uses open source DHCP, which creates some resources that the Cisco APIC cannot delete when a pod is deleted.	4.0(1h) and later
CSCva86794	When a Cisco APIC cluster is upgrading, the Cisco APIC cluster might enter the minority status if there are any connectivity issues. In this case, user logins can fail until the majority of the Cisco APICs finish the upgrade and the cluster comes out of minority.	4.0(1h) and later
CSCva97082	When downgrading to a 2.0(1) release, the spines and its interfaces must be moved from infra L3out2 to infra L3out1. After infra L3out1 comes up, delete L3out2 and its related configuration, and then downgrade to a 2.0(1) release.	4.0(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.	4.0(1h) and later
CSCvg41711	In the leaf mode, the command "template route group <group-name> tenant <tenant-name>" fails, declaring that the tenant passed is invalid.	4.0(1h) and later
CSCvg79127	When First hop security is enabled on a bridge domain, traffic is disrupted.	4.0(1h) and later
CSCvg81856	Cisco ACI Multi-Site Orchestrator BGP peers are down and a fault is raised for a conflicting rtrId on the fvRtdEpP managed object during L3extOut configuration.	4.0(1h) and later
CSCvh76076	The PSU SPROM details might not be shown in the CLI upon removal and insertion from the switch.	4.0(1h) and later
CSCvh93612	If two intra-EPG deny rules are programmed-–one with the class-eq-deny priority and one with the class-eq-filter priority-–changing the action of the second rule to "deny" causes the second rule to be redundant and have no effect. The traffic still gets denied, as expected.	4.0(1h) and later

Bug ID	Description	Exists in
CSCvj26666	The "show run leaf|spine <nodeId>" command might produce an error for scaled up configurations.	4.0(1h) 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.	4.0(1h) and later
CSCvm71833	Switch upgrades fail with the following error: Version not compatible.	4.0(1h) and later

- 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.
- When there are silent hosts across sites, ARP glean messages might not be forwarded to remote sites if a 1st generation ToR switch (switch models without -EX or -FX in the name) happens to be in the transit path and the VRF is deployed on that ToR switch, the switch does not forward the ARP glean packet back into the fabric to reach the remote site. This issue is specific to 1st generation transit ToR switches and does not affect 2nd generation ToR switches (switch models with -EX or -FX in the name). This issue breaks the capability of discovering silent hosts.

Compatibility Information

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

Virtualization Compatibility Information

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

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

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

- This release supports VMM Integration and VMware Distributed Virtual Switch (DVS) 6.5.x. For more information about guidelines for upgrading VMware DVS from 5.x to 6.x and VMM integration, see the *Cisco ACI Virtualization Guide, Release 4.0(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) 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 14.0(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.

- Connecting the Cisco APIC (the controller cluster) to the Cisco ACI fabric requires a 10G interface on the Cisco ACI leaf switch. You cannot connect the Cisco APIC directly to the Cisco 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.
- The N9K-C9348GC-FXP switch does not read SPROM information if the PSU is in a shut state. You might see an empty string in the Cisco APIC output.
- When the fabric node switch (spine or leaf) is out-of-fabric, the environmental sensor values, such as Current Temperature, Power Draw, and Power Consumption, might be reported as "N/A." A status might be reported as "Normal" even when the Current Temperature is "N/A."

Adaptive Security Appliance (ASA) Compatibility Information

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

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

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

Miscellaneous Compatibility Information

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

- This release supports the following software:
  - Cisco NX-OS Release 14.0(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(4e) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3)
  - 4.0(2g) CIMC HUU ISO (recommended) for UCS C220/C240 M4 and M5 (APIC-L2/M2 and APIC-L3/M3)
  - 4.0(1a) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3)
  - 3.0(4l) CIMC HUU ISO (recommended) for UCS C220/C240 M3 (APIC-L1/M1)
  - 3.0(4d) CIMC HUU ISO for UCS C220/C240 M3 and M4 (APIC-L1/M1 and APIC-L2/M2)
  - 3.0(3f) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)

- 3.0(3e) CIMC HUU ISO for UCS C220/C240 M3 (APIC-L1/M1)
- 2.0(13i) CIMC HUU ISO
- 2.0(9c) CIMC HUU ISO
- 2.0(3i) CIMC HUU ISO

- This release supports the partner packages specified in the *L4-L7 Compatibility List Solution Overview* document at the following URL:

  https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/solution-overview-listing.html

- A known issue exists with the Safari browser and unsigned certificates, which applies when connecting to the Cisco APIC GUI. For more information, see the *Cisco APIC Getting Started Guide*.
- For compatibility with OpenStack and Kubernetes distributions, see the *Cisco Application Policy Infrastructure Controller OpenStack and Container Plugins Release Notes, Release 4.0(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\<*user*>_<*domain*>.properties.

  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:
  - 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.
- 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*.
- 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 do not perform SSD over-provisioning on Cisco N9K-C9364C and N9K-C9336C-FX2 spine switches, Cisco APIC raises fault F2972. SSD over-provisioning is applied automatically during the switch boot process after you respond to the fault. SSD over-provisioning might take up to an hour per spine switch to complete. After the switch reloads, you do not need to take any other action regarding the fault.
- 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
  ```
- Fabric connectivity ports can operate at 10G or 25G speeds (depending on the model of the APIC server) when connected to leaf switch host interfaces. We recommend connecting two fabric uplinks, each to a separate leaf switch or vPC leaf switch pair.

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

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 Virtual Edge Configuration Guide, Release 2.0(1)*
- *Cisco ACI Virtual Edge Installation Guide, Release 2.0(1)*
- *Cisco ACI Virtual Edge Release Notes, Release 2.0(1)*
- *Cisco ACI Virtualization Guide, Release 4.0(1)*
- *Cisco APIC NX-OS Style CLI Command Reference, Release 4.0(1)*
- *Cisco Application Virtual Switch Configuration Guide, Release 5.2(1)SV3(3.25)*
- *Cisco Application Virtual Switch Installation Guide, Release 5.2(1)SV3(3.25)*
- *Cisco Application Virtual Switch Release Notes, 5.2(1)SV3(3.25)*