



Cisco APIC OpenStack Plug-in Release Notes, Release 5.2(7)

Introduction

This document describes the features, bugs, and limitations for the Cisco Application Policy Infrastructure Controller (APIC) OpenStack Plug-in.

Cisco APIC OpenStack Plug-in allows policy deployment automation across Cisco Application Centric Infrastructure (ACI) and OpenStack, enabling a complete undercloud and overcloud visibility on Cisco ACI. The Cisco APIC OpenStack Plug-in allows dynamic creation of networking constructs to be driven directly from OpenStack, while providing extra visibility and control from the Cisco APIC.

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>

For more information about this product, see "Related Content."

Note: The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Date	Description
April 10, 2023	Added details of the 5.2(7.20230406) plugin.
January 31, 2023	Release 5.2(7) became available.

New Software Features

The following features were introduced in this release:

- The 5.2(7. 20230406) plugin release adds the ability to configure the policy request retry timer in the opflex-agent. Prior to the 5.2(7.20230406) release, the opflex-agent used a hard-coded value of 120 seconds when doing exponential backoffs for policy resolution failures. This value is now configurable, and the default has been changed from 120 seconds to 10 seconds. The value can be configured using the following tripleo heat template parameter:

```
OpflexRetryDelay:
  default: 10
  description: >
    The starting backoff value for retrying of policy requests, in
    seconds. The backoff is exponential, starting at this value and
    continuing up to 16 retries.
  type: number
```

The 5.2(7.20230406) plugin release adds an extension that allows users to extend the destination prefixes that do not require NAT to reach them. This "no-NAT CIDRs" extension is apic:no_nat_cidrs, which specifies a list of CIDRs, where each CIDR is a routable destination

prefix that should not have NAT applied to it. Below are examples of openstack CLI commands using the extension:

- Create a network named “foonet” with a 30.30.30.0/24 no-NAT CIDR.
`openstack network create foonet --apic-no-nat-cidrs 30.30.30.0/24`
- Update the “foonet” network with 30.30.30.0/24 and 40.40.0.0/16 no-NAT CIDRs.
`openstack network set --apic-no-nat-cidrs 30.30.30.0/24,40.40.0.0/16 foonet`
- Remove the no-NAT CIDRs from the “foonet” network.
`openstack network set --no-apic-no-nat-cidrs foonet`

The extension can be applied to either public/external networks or private networks.

The network that the extension is applied to, and if it is connected to a neutron router, determines the scope of its effect. When applied to private networks, the scope is only those instances that are connected to the private network, and only when that private network has connectivity to a public/external network via a Neutron router. When applied to public/external networks, the scope is all instances that are either directly connected to or have connectivity to that public/external network via a Neutron router.

Some specific examples of instances with *no-NAT* prefixes:

- The extension is applied to a public/external network:
 - Any instance(s) directly connected to the public/external network
 - Instances on private networks that have connectivity to the public/external network via a Neutron router
- The extension is applied to a private network:
 - The private network has connectivity to a public/external network via a neutron router
- The extension is applied to a private network, which is connected via a Neutron router to a public/external network that also has the extension:
 - Instances directly connected to the public/external network would only see the CIDRs in the extension on the public/external network
 - Instances connected to the private network with the extension would see both the CIDRs in the public/external and the private networks
- The 5.2(7) plugin release provides the ability to configure the destination of the droplog messages: `OpflexDroplogTarget`:

description: >

Target for droplog messages. If not configured, droplog messages are logged in the current opflex-agent log file. If set to "syslog", the log messages are sent to syslog. Any other value is expected to be a fully-specified path and file to place log messages (directory is expected to be pre-existing).

type: string
default: ''

This configuration feature is currently only available in the Red Hat OpenStack Platform (RHOSP) Director 16 (stable/queens) release.

- Beginning with 5.2(7) plugin release, you can configure additional keystone notification parameters for neutron:

```
AciKeystoneNotificationExchange:
  type: string
  default: 'keystone'
  description: >
    When AciKeystoneNotificationPurge is set to true,
    determines which exchange to use for notifications.

AciKeystoneNotificationTopic:
  type: string
  default: 'notifications'
  description: >
    When AciKeystoneNotificationPurge is set to true,
    determines which topic to use for notifications.

AciKeystoneNotificationPool:
  type: string
  default: None
  description: >
    When AciKeystoneNotificationPurge is set to true,
    determines which pool to use for notifications.
    This value should only be configured to a value other
    than 'None' when there are other notification listeners
    subscribed to the same keystone exchange and topic, whose
    pool is set to 'None'.
```

These settings should only be used for installations that have multiple listeners for Keystone notifications, as noted in the template parameter descriptions.

The default value for `AciKeystoneNotificationPool` is not supported in this release. The default value is `None` (as displayed above). The `type` is a string, and due to the absence of a value, the default value (`None`) gets treated as “None”. Hence, ensure to set the `AciKeystoneNotificationPool` parameter explicitly to an empty string (“”) in the yaml files, instead of relying on the default value. For releases prior to Cisco APIC release 5.2(7), the pool was a named pool, with the value “cisco_aim_listener-workers”. The `rabbitmq` subsystem does not automatically delete a queue when it is no longer in use. You will need to manually delete the queue after upgrading to the 5.2(7) release.

- Beginning with the 5.2(7) plugin release, some installations may use system ID lengths longer than 16 characters through the following template parameter:

```
ACIApicSystemIdMaxLength:

  description: Maximum length of the ACIApicSystemId. Please consult the
  business unit before changing this value from the default.
  type: number
  default: 16
```

Consult the Business Unit (BU) before using this parameter, as there are limitations to its usage.

- Beginning with the 5.2(7) plugin release, an additional JSON parser is supported. The parser can be enabled for OVSDb interface on the agent, using the following template parameters::

```
OpflexEnableOvsdbAsyncParser:
  default: false
```

```
description: Enable new asynchronous parsing of messaging interface with
OVSDB
type: boolean
```

The asynchronous JSON parser was introduced to address scale issues, where the number of Open vSwitch (OVS) endpoints ("tap" ports) on a host is greater than 200. For installations that deploy opflex on controller nodes, the number of endpoints is a function of the number of neutron networks that have DHCP agents, since the DHCP agents run on the controller, and use a port that is connected to OVS. If more than 200 networks are configured in the installation, then there will be more than 200 OVS endpoints on the controller, and the asynchronous JSON parser should be used. If left unconfigured, the non-asynchronous JSON parser is used.

- A new extension was added in the 5.2(7) plugin release. The extension allows subnets to be configured underneath the Endpoint Group (EPG) in ACI instead of underneath the Bridge Domain (BD). The extension is applied to subnets in neutron, and can only be used when creating the subnet: **openstack subnet create --apic-epg-subnet --network foonet --subnet-range 40.40.40.0/24 foosubnet**

The extension applies to the subnet as long as subnet exists, and cannot be modified.

Cisco ACI Virtualization Compatibility Matrix

For information about Cisco ACI and OpenStack, see the Cisco Virtualization Compatibility Matrix at the following URL:

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

Changes in Behavior

Cisco APIC Releases 5.2(1) and later, have the following changes for clusters installed or upgraded using Red Hat OpenStack Platform (OSP) Director versions 13 or 16:

- Prior to Cisco OpenStack GBP/ML2 Plugin Release 5.2(1), the opflex-agent, mcast-daemon, and neutron-opflex-agent were in the same container: `ciscoaci_opflex_agent`. Starting with release 5.2(1), the neutron-opflex-agent is split into its own container - `ciscoaci_neutron_opflex_agent`, while the opflex-agent and mcast-daemon remain in the `ciscoaci_opflex_agent` container. This means that per-role services and the templates required to deploy OpenStack using Red Hat OpenStack Platform (OSP) are different from previous releases. For more information, see *Cisco ACI Installation Guide for Red Hat OpenStack Using the OpenStack Platform 16.1 Director* guide.
- Prior to Cisco APIC Release 5.2(1), the `/var/lib/opflex-agent-ovs` directory was only available inside the `ciscoaci_opflex_agent` container. In Cisco APIC Release 5.2(1), a directory on the host is bind-mounted as `/var/lib/opflex-agent-ovs` in both the `ciscoaci_opflex_agent` and `ciscoaci_neutron_opflex_agent` containers. This makes the `/var/lib/opflex-agent-ovs` directory accessible directly on the host, under `/var/lib/opflex/files`.
- Prior to Cisco APIC Release 5.2(1), the network namespace used for port-based Stateful Network Address Translation (SNAT) was recreated any time the neutron-opflex-agent was restarted (e.g. restarting `ciscoaci_opflex_agent` container). Starting with Cisco APIC Release 5.2(1), the SNAT namespace is only recreated if the IP address and MAC address of the interface inside the namespace doesn't match the IP and MAC address of the neutron port allocated to that host for SNAT.

- From Cisco APIC Release 5.2(1), the location of the socket used for inspection of the opflex-agent has changed. Running gbp_inspect requires using the --socket argument, passing the path /run/opflex/opflex-agent-inspect.sock.

Supported Scale

For the verified scalability limits (except for CLI limits), see the Verified Scalability Guide for this release. For Kubernetes-based Integrations (including Docker, OpenShift, and Rancher), and OpenStack Platform Scale Limits, see the following table.

Note: The scalability information in the following table applies to Kubernetes or OpenStack resources integrated with OpFlex into the Cisco ACI fabric. It does not apply to Microsoft SCVMM hosts or Cisco ACI Virtual Edge instances.

Limit Type	Maximum Supported
Number of OpFlex hosts per leaf	120
Number of OpFlex hosts per port	20
Number of vPC links per leaf	40
Number of endpoints per leaf	10,000
Number of endpoints per host	400
Number of virtual endpoints per leaf	40,000

Notes:

- For containers, an endpoint corresponds to a pod's network interface.
- For OpenStack, an endpoint corresponds to any of the following:
 - A virtual machine (VM) interface (also known as vnic)
 - A DHCP agent's port in OpenStack (if in DHCP namespace on the network controller)
 - A floating IP address
- Total virtual endpoints on a leaf can be calculated as virtual endpoints / leaf = VPCs x EPGs, where:
 - VPCs is the number of VPC links on the switch in the attachment profile used by the OpenStack Virtual Machine Manager (VMM).
 - EPGs is the number of EPGs provisioned for the OpenStack VMM.

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

Known Limitations

This section lists the known limitations.

- Cisco ACI Unified Plug-in for OpenStack does not support the following features:

- ESX hypervisor support
 - ASR1K edgeNAT support
 - GBP/NFP Service chaining
 - ML2 Network constraints
- Dual-stack operation requires that all IPv4 and IPv6 subnets – both for internal and external networks – use the same VRF in Cisco ACI. The one exception to this is when separate external networks are used for IPv4 and IPv6 traffic. In that workflow, the IPv4 and IPv6 subnets used for internal networks plus the IPv6 subnets used for external networks all belong to one VRF, while the subnets for the IPv4 external network belong to a different VRF. IPv4 NAT can then be used for external networking.
 - For installations with B-series that use VXLAN encapsulation, Layer 2 Policies (for example, bridge domains) should each contain only one Policy Target Group (that is, Endpoint Group) to ensure a functional data plane.
 - The Cisco ACI OpenStack Plug-in is not integrated with the Multi-Site Orchestrator. When deploying to a Multi-Site deployment, the Cisco ACI configurations implemented by the plug-in must not be affected by the Multi-Site Orchestrator.
 - When you delete the Overcloud Heat stack, the Overcloud nodes are freed but the virtual machine manager (VMM) domain remains present in Cisco APIC. The VMM appears in Cisco APIC as a stale VMM domain along with the tenant unless you delete the VMM domain manually. Before you delete the VMM domain, verify that the stack has been deleted from the undercloud, and check that any hypervisors appearing under the VMM domain are no longer in the connected state. After both these conditions are met, you can safely delete the VMM domain Cisco APIC.
 - Due to a bug in upstream Neutron, subport bindings are not cleaned up in trunk workflows. This has existed in earlier releases and is equally applicable to usage with Open vSwitch (OVS) reference implementation agents as well as OpFlex agents. For more information about the Neutron bug, see bug 1639111 on the Launchpad.net website.

Usage Guidelines

- The OpflexDroplogConfig parameter added in the 5.2(6) plugin release allows configuration of the opflex-agent droplog feature across all hosts when deployed using OpenStack Platform (OSP) Director 16. The parameter requires a valid json blob, which is used for each host's opflex-agent droplog configuration file.
- The APIC SNAT subnet only extension is used to control IP address allocation from a subnet on a neutron external network. When setting the gateway on a neutron router, if no subnet or IP address is specified, neutron picks the subnet with the lowest UUID value, and allocates an IP address from that subnet to use for the router gateway port. In order to avoid exhausting IP addresses intended for SNAT, this extension can be enabled on subnets used for SNAT:

```
openstack subnet set --apic-snat-subnet-only-enable foosubnet
```

Once enabled, whenever a neutron router is attached to the external network that owns the SNAT subnet, that subnet will not be used to allocate gateway IP addresses. This extension can also be disabled, allowing allocations from the subnet:

```
openstack subnet set --apic-snat-subnet-only-disable foosubnet
```

The default value for the extension is False, which means existing workflows will behave the same as before. If a user tries specifying a subnet or IP address on a subnet with this extension *enabled* when setting a router gateway, that operation will fail.

- Logging of dropped packets on hosts can be enabled in Hat OpenStack Platform (RHOSP) Director 16 This is one using the following tripleo parameter specified in the `/opt/ciscoaci-tripleo-heat-templates/deployment/ deployment/opflex/opflex-agent-container-puppet.yaml` template:

```
OpflexEnableDroplog:
    default: false
    description: Enable droplog feature on hypervisors
    type: Boolean
```

Setting this parameter to true enables logging of dropped packets on the hypervisor.

- A new template has been added for RHOSP 16, in order to support simultaneous operation of hypervisors using both optimized and non-optimized DHCP and metadata. This template is found on the undercloud in `/opt/ciscoaci-tripleo-heat-templates/deployment/neutron_opflex/neutron-opflex-agent-container-puppet-controller.yaml`, and should only be used to deploy the neutron-opflex-agent service on controller nodes.
- We recommended that service VMs used in service function chaining (SFC) workflows use static IP addressing and not rely on DHCP. When the service VM becomes part of a service chain in OpenStack and correspondingly a service graph on Cisco ACI, the associated EPG is removed. Thus, services such as DHCP are not available for the endpoint. This is applicable with OVS reference implementation agents as well as OpFlex agents.
- When you run the host report ansible-playbook (`/opt/ciscoaci-tripleo-heat-templates/tools/report.yml`), the step to copy files from a running container may return an error, causing the host report to fail. If this happens, rerun the playbook until it succeeds. The failure is due to a known issue in Red Hat OpenStack Platform (OSP) 13 Director. For more information, see the Red Hat Bugzilla bug 1767289. You can find the related product note in the Red Hat Customer portal knowledge base article "docker cp command sometimes failed with invalid argument."
- If you are using Cisco ACI Virtual Edge with OpenStack or Kubernetes OpFlex on the same leaf, do not use Cisco APIC version 4.2(3), or you will encounter the bug CSCvs49419. If you have that configuration and need features from the Cisco APIC 4.2(x) release train, use the 4.2(2) or 4.2(4) version.
- JuJu charms users must first update the Charms before installing the updated plug-in.
- Newer RHEL installations limit the maximum number of multicast group subscriptions to 20. This is configured with the `net.ipv4.igmp_max_memberships` sysctl variable. Installations using VXLAN encapsulation for OpenStack VMM domains should set this value higher than the total number of endpoint groups (EPGs) that might appear on the node (one for each Neutron network with Neutron workflow, or one for each Policy Target Group with Group Based Policy workflow).

Note: Controller hosts running DHCP agents that are connected to OpFlex networks have an EPG for each network.

- When using the allowed address pair feature with the Cisco ACI plug-in, be aware of the following differences from upstream implementation:

- As OpenStack allows the same `allowed_address_pair` to be configured on multiple interfaces for HA, the OpFlex agent requires that the specific VNIC that currently owns a specific `allowed_address_pair` to assert that address ownership using Gratuitous ARP.
- When using the promiscuous mode, the vSwitch stops enforcing the port security check. To get reverse traffic for a different IP or MAC address, you still need to use the `allowed-address-pair` feature. If you are running tempest, you will see `test_port_security_macspoofing_port` fail in scenario testing, as that test does not use the `allowed-address-pair` feature.

- Keystone configuration update

When the OpenStack plug-in is installed in the unified mode, the Cisco installer adds the required configuration for keystone integration with AIM. When not using unified mode, or when using your own installer, the configuration section must be provisioned manually:

```
[apic_aim_auth]
auth_plugin=v3password
auth_url=http://<IP Address of controller>:35357/v3
username=admin
password=<admin_password>
user_domain_name=default
project_domain_name=default
project_name=admin
```

- When using optimized DHCP, the DHCP lease times are set by the configuration variable `apic_optimized_dhcp_lease_time` under the `[ml2_apic_aim]` section.
 - This requires a restart of `neutron-server` to take effect
 - If this value is updated, existing instances will continue using the old lease time, provided their neutron port is not changed (e.g. rebooting the instance would trigger a port change, and cause it to get the updated lease time). New instances will however use the updated lease time.
- In upstream Neutron, the "advertise_mtu" option has been removed.

Since the `aim_mapping` driver still uses this configuration, the original configuration which appeared in the default section should be moved to the `aim_mapping` section. For example:

```
[aim_mapping]
advertise_mtu = True
```

It is set to `True` by default in the code (if not explicitly specified in the config file).

- The Unified Plug-in allows coexistence of GBP and ML2 networking models on a single OpenStack Cloud installation. However, they must operate on different VRFs. We recommend using a single model per OpenStack Project.
- If a default VRF is implicitly created for a tenant in ML2, it is not implicitly deleted until the tenant is deleted (even if it not being used anymore).
- Unified model impact of the transaction Model Updates in Newton.

When GBP and ML2 co-exist, GBP implicitly created some neutron resources. In Newton, the neutron transaction model has been updated and has added various checks. Some of those checks spuriously see this nested transaction usage as an error and log and raise an exception. The

exception is handled correctly by GBP and there is no functional impact but unfortunately the neutron code also logs some exceptions in neutron log file – leading to the impression that the action had failed.

While most such exceptions are logged at the DEBUG level, occasionally you might see some exceptions being logged at the ERROR level. If such an exception log is followed by a log message which indicates that the operation is being retried, the exception is being handled correctly. One such example is the following:

Delete of policy-target on a policy-target-group associated to a network-service-policy could raise this exception:

```
2017-03-18 12:52:34.421 27767 ERROR neutron.api.v2.resource [...] delete failed
2017-03-18 12:52:34.421 27767 ERROR neutron.api.v2.resource Traceback ...:
2017-03-18 12:52:34.421 27767 ERROR neutron.api.v2.resource File
"/usr/lib/python2.7/site-packages/neutron/api/v2/resource.py", line 84, ...
...
2017-03-18 12:52:34.421 27767 ERROR neutron.api.v2.resource raise ...
2017-03-18 12:52:34.421 27767 ERROR neutron.api.v2.resource ResourceClosedError: This
transaction is closed
```

Note: Cisco is working with the upstream community for further support on Error level logs.

- When a Layer 2 policy is deleted in GBP, some implicit artifacts related to it may not be deleted (resulting in unused BDs/subnets on Cisco APIC). If you hit that situation, the workaround is to create a new empty Layer 2 policy in the same context and delete it.
- If you use tempest to validate OpenStack, the following tests are expected to fail and can be ignored:

```
tempest.scenario.test_network_basic_ops.TestNetworkBasicOps.test_update_router_admin_s
tate
```

- Neutron-server logs may show the following message when DEBUG level is enabled:

```
Timed out waiting for RPC response: Timeout while waiting on RPC response - topic:
"<unknown>", RPC method: "<unknown>" info: "<unknown>"
```

This message can be ignored.

- High Availability LBaaSv2 is not supported.
- OpenStack Newton is the last version to support non-unified plug-in. OpenStack Ocata and future releases will only be supported with the unified plug-in.
- For deployments running Cisco ACI version 4.1(2g) and using the Group Based Policy workflow and associated APIs, contract filters set to an EtherType of ARP can result in the filter being incorrectly set as “Unspecified” on the leaf. If an EtherType of ARP is required, then you must use a Cisco ACI release other than 4.1(2g).
- Some deployments require installation of an “allow” entry in IP Tables for IGMP. This must be added to all hosts running an OpFlex agent and using VXLAN encapsulation to the leaf. The rule must be added using the following command:

```
# iptables -A INPUT -p igmp -j ACCEPT
```

In order to make this change persistent across reboots, add the command either to /etc/rc.d/rc.local or to a cron job that runs after reboot.

- For deployments that use B-series servers, an additional service must be started on the hosts to ensure that connectivity is maintained with the leaf at all times. Complete the following steps:

Step 1. Install the Cisco APIC API package (python-apicapi for Debian packaging, apicapi for RPM packaging) for any servers running an OpFlex agent.

Step 2. Add the OpFlex uplink bond name to /etc/environments (that is, opflex_bondif=bond1).

This is needed if the interface is other than default (bond0).

Step 3. Enable the apic-bond-watch service using the following command:

```
sudo systemctl enable apic-bond-watch
```

Step 4. Start the apic-bond-watch service using the following command:

```
sudo systemctl start apic-bond-watch
```

For OpenStack Director installations using VXLAN encapsulation for VMM domains, two additional configuration items may be needed to handle large installations. The number of multicast groups should be configured to match the maximum number of endpoint groups for the host, and the maximum auxiliary memory for sockets needs to be increased for IPC. These are configured using the extra-config.yaml file, with the following parameters:

```
ControllerParameters:
  ExtraSysctlSettings:
    net.ipv4.igmp_max_memberships:
      value: 4096
    net.core.optmem_max:
      value: 1310720
ComputeParameters:
  ExtraSysctlSettings:
    net.ipv4.igmp_max_memberships:
      value: 1024
```

The IGMP max memberships value should be greater than or equal to the number of Neutron networks that the host has Neutron ports on. For example, if a compute host has 100 instances, and each instance is on a different Neutron network, then this number must be set to at least 100. Controller hosts running the neutron-dhcp-agent will need set this value to match the number of Neutron networks managed by that agent, which means this number will probably need to be higher on controller hosts than compute hosts.

- For installations not using OpenStack Director, the maximum allowed packet size for the database must be configured to support database transactions for tenants in AIM with large configurations. The default value installed by OpenStack director in /etc/my.cnf.d/galera.cnf is sufficient for most installations:

```
[mysqld]
...
max_allowed_packet = 16M
[mysqldump]
max_allowed_packet = 16M"
```

- After deploying Queens with Juju charms (18 or 19), sometimes a VM spawn fails. The failure is due to a neutron-opflex-agent failing to start on the host that the VM was scheduled to. The host can be

determined using the `neutron agent-list` command: The `neutron-opflex-agent` is missing for the effected compute node.

Restart of `neutron-opflex-agent` on the affected node fixes the problem and can be used as a workaround after a fresh deployment.

- When you do an upgrade involving Red Hat OSP13, the installer doesn't delete the `/var/www/html/acirpo` directory. This causes problems when building new containers. When performing an upgrade using OSP13, be sure to manually delete this directory before installing the new RPM.

Open Issues

There are no known issues in this release.

Resolved Issues

Click the bug ID to access the Bug Search tool and see additional information about the bug.

Bug ID	Description
CSCwd65420	ACI + OSP 16 :: metadata service is not reachable after host reboot.
CSCwd19840	Request for higher scale - opflex-agent crashes after upgrade to 5.2.4 due to scale exceeded.
CSCwe39731	The XML-RPC server in supervisor before 3.0.1, 3.1.x before 3.1.4, 3 ...
CSCwe39730	The XML-RPC server in supervisor before 3.0.1, 3.1.x before 3.1.4, 3 ...
CSCwe39728	The XML-RPC server in supervisor before 3.0.1, 3.1.x before 3.1.4, 3 ...
CSCwe93096	Agent policy retry backoff is hardcoded.

Known Issues

There are no known issues in this release.

Related Content

See the [Cisco Application Policy Infrastructure Controller \(APIC\)](#) page for the documentation.

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.

You can watch videos that demonstrate how to perform specific tasks in the Cisco APIC on the [Cisco Data Center Networking](#) YouTube channel.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to apic-docfeedback@cisco.com. We appreciate your feedback.

Legal Information

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:

<http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2023 Cisco Systems, Inc. All rights reserved.