Cisco APIC OpenStack Plug-in Release Notes, Release 6.0(3)

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
December 19, 2023	Release 6.0(3) became available.

New Software Features

Following are the new features introduced in the 6.0(3) plug-in release:

- Support for configuration of Endpoint movement detection in Gen1 hardware. This configuration allows users to control how the fabric performs EP movement detection. First generation switches are unable to use GARPs for EP movement detection in hardware when the EP “move” is on the same port. Additional configuration is needed in the BD to punt all GARPs to the switch CPU for processing. A new Tripleo parameter, `AciGen1HwGratArps`, controls this behavior in the fabric. The default configuration is to disable sending GARPs to the switch CPU. If your installation still uses first generation switches, then, set this value to “True”.
- Support for setting the scope of a subnet. Prior to release 6.0(3), setting the scope attribute was not supported. Two new extensions have been introduced to control setting this attribute. You can use:

  --apic-advertised-externally-enable or --apic-advertised-externally-disable to change the state of apic:advertised_externally,

  --apic-shared-between-vrfs-enable or --apic-shared-between-vrfs-disable to change the state of apic:shared_between_vrfs.

  By default the subnet is public, so apic:advertised_externally is True and apic:shared_between_vrfs is False.

Depending on the state of both extensions, you can get four different scope types:

- advertised_externally = public
- shared_between_vrfs = shared
- advertised_externally & shared_between_vrfs = public,shared
- neither = private

The following is an example of creating a shared subnet shared between VRFs but not advertised externally:

```
openstack subnet create foobarsubnet --network foobarnet --subnet-range 192.8.2.0/24 -apic
  advertised-externally-disable --apic-shared-between-vrfs-enable
```

- The statistics collection behavior for the OpFlex Agent can be configured. The following Tripleo parameters have been added:
  - OpflexStatisticsMode
  - OpflexStatisticsInterfaceEnabled
  - OpflexStatisticsInterfaceInterval
  - OpflexStatisticsContractEnabled
  - OpflexStatisticsContractInterval
  - OpflexStatisticsSecurityGroupEnabled
  - OpflexStatisticsSecurityGroupInterval
  - OpflexStatisticsServiceFlowDisabled
  - OpflexStatisticsServiceEnabled
  - OpflexStatisticsServiceInterval
  - OpflexStatisticsTableDropEnabled
  - OpflexStatisticsTableDropInterval
  - OpflexStatisticsSystemEnabled
  - OpflexStatisticsSystemInterval

  Each parameter controls whether a given class of statistics collection is enabled, and when enabled, how often they are collected. The “OpflexStaticsMode” is a global control for all statistics. Setting this value to “off” disables all statistics collection, regardless of the other statistics collection parameters. The default value of “real” enables statistics collection, with fined-grained control per class through the other parameters. The unit for interval parameters is milliseconds.

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

In Cisco APIC Releases 6.0(3) and later, we can provide a custom policy.json file for configuring GBP, using:

```
GbpCustomPolicies: '{"get_network": "rule:admin_or_owner or rule:shared or rule:external",
"update_subnet": "rule:admin_only", "delete_subnet": "rule:admin_only"}'
```

You can set the `GbpPolicyOverride` flag as well.

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
CSCwh75828	Disable GARP based EP detection on Bridge Domains provisioned by Openstack Plugin in ACI.
CSCwh71494	Kubernetes Network Policy supports only a single address family.
CSCwf95778	ICMP unreachable packets are dropped, causing path MTU discovery to fail.

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