



Cisco Application Policy Infrastructure Controller OpenStack Plug-in Release Notes, Release 4.2(3)

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 additional 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>

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
2019-12-13	Release 4.2(3) became available.
2020-02-20	Added TLS support for internal and external endpoints in New Software Features section.
2020-03-17	Added usage guideline not to use Cisco APIC 4.2(3) if you have Cisco ACI Virtual Edge and OpenStack or Kubernetes OpFlex.
2020-04-10	Removed Restricted Users from New Software Features. The feature has been removed from the release.

Contents

This document includes the following sections:

- [Cisco ACI Virtualization Compatibility Matrix](#)
- [New and Changed Information](#)
- [Supported Scale](#)

- [Known Limitations](#)
- [Usage Guidelines](#)
- [Bugs](#)
- [Related Documentation](#)
- [New Documentation](#)

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>

New and Changed Information

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

- [New Software Features](#)
- [Changes In Behavior](#)

New Software Features

TLS Support for Internal and External Endpoints

This feature allows you to use the Cisco ACI OpFlex plug-in with Red Hat OpenStack 13 deployed with Transport Layer Security (TLS) on internal endpoints (EPs), external EPs, or both. Steps for enabling this feature are provided in the “**Deploying with TLS**” section of [Cisco ACI Installation Guide for Red Hat OpenStack Using the Red Hat OpenStack Platform 13 Director](#).

Use Internal REST Endpoint for GBP Client Calls

Before the 4.2(2) release, Group Based Policy GBP client calls made by the plug-in could only target the publicly accessible REST endpoint. A flag was added to the 4.2(2) release to control whether the internal or public REST endpoint is used by the plug-in. This is configured under the `m12_apic_aim` section:

```
[m12_apic_aim]
enable_neutronclient_internal_ep_interface = True
```

The default value for this flag is `False`.

Run Bond Watch Service from Heat Template

When integrating Cisco Unified Computing System (UCS) B-Series to work with Cisco ACI and OpenStack orchestration, you can run the bond watch service by enabling it from the Heat template.

For information, see the procedure “Run the Bond Watch Service” in the “Configuring UCS B-Series” appendix of the *Cisco ACI Installation Guide for Red Hat OpenStack Using the OpenStack Platform 13 Director*.

Certificate-based Authentication

OpenStack Director deployments can now use certificate-based authentication with Cisco ACI. Two items should be added to the heat templates to enable this:

```
ACIApicCertName:
  type: string
  default: ''
ACIApicPrivateKey:
  type: string
  default: ''
```

Follow the procedure for creating a user with X509 certificate and add the name and private key to the Cisco ACI resources template file. Instructions for creating a user and X509 certificate can be found under the section "Creating a Local User and Adding a User Certificate" in the following link:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/b-Cisco-APIC-Security-Configuration-Guide-421/b-Cisco-APIC-Security-Configuration-Guide-421_chapter_011.html

The following is an example of how to provide the values in the .yaml file:

```
ACIApicCertName: admincert
ACIApicPrivateKey: |
  -----BEGIN PRIVATE KEY-----
  MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwgGJdAgEAAoGBAMq3hFRn7rMDCrL/
  6W+oEeb07gWbUxK8JvArTV3xXfw7hqVQ5LEfM7Ggosya4h0aG4ZiNKfJdMWHtFRt
  P2Fs9szvkD4wdkZ1rseq/9I3sUg84YcotK8y718ks8XF0NIOktNtX5MzBwjN8QFd
  SJ0np1UBCAu6kCGcvKDCi9u3dKsnAgMBAAECgYAHoeQ6F1Wt6MHo3mjIGvBdm9Hr
  ZR86F9pxdXfqvxE2U31s1QBfSNj16aHniTdVOCvsIdtwq82ZOFrZ+B5tSSB7opaR
  kv41EtiPgYtW5sdQ0p1D+WfbvJwtfTR1eYXpQb07fVprBXOYE48u9Bpeqngucy87
  V+1EgWd5VeHwkc07rQJBAM5o5Gj6gXFfbMQs2283Dv7ScnrE6mLmG6iqZvcO1/JI
  vinNg691G42tGh7V/Ra/Yc8wJPjPplug6WcNUUM0bsCQQD7a38snaL8+1V+741p
  /d7IS4HA41s112M+A/cD8Neme9vUhMqZGFYGRPWfOjr/FQzzrhXcEYeyOkXZa0WS
  iU+FAkEAufDoAmHYhecutjKqoq94xLmUA2CsvNcKB5EqHFm000AqftuTI8CCQ57o
  Ok8S1r+5MEDcQt0toU5bLa9g1YmMzQJBAAOAg4Tstv9mUWJATD1a4iTy3CxGf3GZs
  jzz+ndr2fdgdPEhEpLM73ZwzJ19tsqAo7OXif/wx6Gz6w7/hgCD0pV0CQEK+YaJS
  N4d1pREch0Ge9agqtZLeTvtxXNpF3MJ7iIxENB87Qa0ighKA98eKjydagtzRZGn7
  a3KGolZ0kxx7JfM=
  -----END PRIVATE KEY-----
```

Note: The AciApicPassword should not be set when using certificate-based authentication.

Configure the VMM Domain Multicast Address

OpenStack Director deployments can now configure the OpenStack VMM Domain's multicast address, as well as the multicast address range to use for a pool for the VMM domain, when using VXLAN encapsulation. This is configured using the following heat template configuration variables:

```
AciVmmMcastRanges:
  type: string
  default: "225.2.1.1:225.2.255.255"
AciVmmMulticastAddress:
  type: string
  default: "225.1.2.3"
```

Only one VMM domain and associated multicast addresses can be configured. If additional OpenStack VMM domains are needed on the same deployment, then that must be done manually outside of OpenStack Director.

Configure Docker Registry

Starting with the 4.2(1) release, OpenStack Director 13 (Queens) deployments support configuration of a Docker registry. Users have the following choices for the registry:

- Upstream registry (allows for using a local satellite server – currently Redhat registry)
- Downstream registry address/port/URI (currently underlay controller, 8787, /rhosp13)

This is configured using the `build_openstack_aci_containers.py` script:

```
Usage: build_openstack_aci_containers.py [options]
Options:
-h, --help                show this help message and exit
-o OUTPUT_FILE, --output_file=OUTPUT_FILE
                        Environment file to create, default is
                        /home/stack/templates/ciscoaci_containers.yaml
-c CONTAINERS_TB, --container=CONTAINERS_TB
                        Containers to build, comma separated, default is all
-s UPSTREAM_REGISTRY, --upstream=UPSTREAM_REGISTRY
                        Upstream registry to pull base images from, eg.
                        registry.access.redhat.com/rhosp13, defaults to
                        registry.access.redhat.com/rhosp13
-d DESTINATION_REGISTRY, --destregistry=DESTINATION_REGISTRY
                        Destination registry to push to, eg:
                        1.100.1.1:8787/rhosp13
-t TAG, --tag=TAG        for images, defaults to 'latest'
```

Changes in Behavior

This section lists changes in behavior in this release.

- Starting with the 4.2(1) release, Debian packages are split into distribution-specific tarballs. Packages for the Xenial release are included in tarballs that have `-xenial` in the name, while packages for the Bionic release are included in tarballs that have `-bionic` in the name.
- Before the 4.2(1) release, the **Neutron router resource's** `apic:distinguished_names` extension reported the Distinguished Names (DNs) and CIDRs for the subnets attached to the router, as well as the DN of the associated Contract and ContractSubject in Cisco ACI. Starting with the 4.2(1) release, this extension only reports the Contract and ContractSubject DN.
- Before the 4.2(1) release, it was possible to attach unscoped Neutron subnets to routers such that Cisco ACI subnets referencing the same VRF would be created. These would result in Cisco ACI faults and loss of connectivity for the affected subnets.

Starting with the 4.2(1) release, if adding or removing an unscoped Neutron subnet to or from a router would result in overlapping Cisco ACI subnets, the operation is rejected with a `SubnetOverlapInRoutedVRF` exception. The `gbp-validate` tool also now reports any existing overlapping Subnets within a VRF as unrepairable errors.

For existing deployments, run `gbp-validate` immediately after upgrading to the release, and remove router interfaces needed to eliminate any overlap that is reported. If attempting to remove such interfaces results in `SubnetOverlapInRoutedVRF` exceptions, then temporarily set the `allow_routed_vrf_subnet_overlap` config variable to `True` until the overlap has been cleaned up and validation passes.

The following are behaviors that were new in previous releases and remain relevant:

New and Changed Information

- Beginning in Cisco APIC OpenStack Plug-in Release 4.1(1), using VXLAN on blade server systems is supported. See the Known Limitations section for more information.
- For OpenStack Director installs, the value for ACIOpflexUplinkInterface parameter needs to be an actual interface name. This is required to support both nested virtualization and non-nested configurations. Refer to the appropriate OpenStack Director documentation for additional information on how to configure this for your environment.
- For OpenStack Director 13 installs, enabling or disabling of LLDP is controlled by resource declaration. If you have the following in your yaml file:

```
OS::TripleO::Services::CiscoAciLldp: /opt/ciscoaci-tripleo-heat-templates/docker/services/cisco_lldp.yaml
```

Then LLDP will be enabled. If you do not want to use LLDP, then you must put the following in your yaml file:

```
OS::TripleO::Services::CiscoAciLldp: OS::Heat::None
```

The use of ACIUseLldp to control this behavior was removed beginning with OpenStack Director 13.

- For installations currently running release 3.2(2.20180710), 4.0(1.20181001), or 4.0(2.20181221), run the db_check script before upgrading to ensure that the OpenStack ACI Integration Module (AIM) database migration script completed successfully. The script is in support-tools-1.0.0.tar.gz in the tarball for the release on Cisco.com.

Contact the Cisco Technical Assistance Center (TAC) if the script indicates that there could be a potential problem.

- Cisco ACI software version 3.2(4e) or higher is recommended for this plug-in. You cannot use Cisco ACI software version 4.0(2c) for OpenStack as it has the following issues with floating IP usage: CSCvn77231.
- Starting in 4.01, agent-ovs was renamed opflex-agent. Operators must account for the change when stopping or starting the agent. Users who create their own installers also need to incorporate packaging changes for the agent.

In addition, the default values for two sockets used by the agent have changed:

```
Old: /var/run/opflex-agent-ovs-inspect.sock
```

```
New: /var/run/opflex-agent-inspect.sock
```

```
Old: /var/run/opflex-agent-ovs-notif.sock
```

```
New: /var/run/opflex-agent-notif.sock
```

The neutron-opflex-agent shares the notify socket with the opflex-agent, so its default value also changed to be consistent. All socket filenames can also be configured explicitly.

- If you are going to upgrade, you must upgrade the Cisco ACI fabric first before upgrading the Cisco APIC OpenStack plug-ins. The only exception is for the Cisco ACI fabric releases that have been explicitly validated for this specific plug-in version in the [Cisco ACI Virtualization Compatibility Matrix](#).
- Multiple OpenStack instances can share the same Cisco ACI fabric. Earlier versions of unified plug-in would attach all OpenStack VMM domains to every OpenStack cloud. This release allows cleaner separation by using this procedure:

Supported Scale

You must provision the VMM domains owned by each OpenStack cloud using the new host-domain-mapping CLI command:

```
# aimctl manager host-domain-mapping-v2-create [options] <host name> <domain name> <domain type>
```

The host name can be a wildcard, which is indicated using an asterisk surrounded by double quotes ("*"). A wildcard means that the mapping should be used for all hosts. When more than one OpenStack instance shares the fabric, an entry must be created in this table for each VMM domain in use by that OpenStack instance. As an example, if one OpenStack instance is using VMM Domains "ostack1" and "ostack2", the following commands would be run on that OpenStack controller to put entries to this table:

```
# aimctl manager host-domain-mapping-v2-create "*" ostack1 OpenStack
# aimctl manager host-domain-mapping-v2-create "*" ostack2 OpenStack
```

If the second OpenStack instance is using VMM Domain "ostack3", the following command would be run on that OpenStack controller to add an entry to its table:

```
# aimctl manager host-domain-mapping-v2-create "*" ostack3 OpenStack
```

- Earlier versions only supported one logical uplink for hierarchical port binding or non-opflex VLAN network binding. In this release, you can have multiple links for those use-cases when using unified plug-in.

To use this feature, the AIM CLI must be used to provide the mapping of physnets in OpenStack and an interface on a specific host. The following aimctl CLI command is used to configure this mapping:

```
# aimctl manager host-link-network-label-create <host_name> <network_label> <interface_name>
```

As an example, host h1.example.com is provisioned to map its eth1 interface to physnet1:

```
# aimctl manager host-link-network-label-create h1.example.com physnet1 eth1
```

- Previously it was not possible for a single L3 Out to be shared across multiple OpenStack instances when using AIM, because both OpenStack instances would attempt to use an External Network Endpoint Group of the same name. This release adds scoping of the Application Profile for the External Network Endpoint Group using the `apic_system_id`, which is configured in the `[DEFAULT]` section of the `aimctl.conf` file.
- In earlier versions, the AIM plug-in would take ownership of pre-existing L3 Outs when NAT was not being used, which led to scenarios where the AIM plug-in would delete the pre-existing L3 Out in some corner cases. With this release, the AIM plug-in will not take ownership of any pre-existing L3 Outs.
- Legacy plug-in is not supported with the Ocata Plug-ins and will not be supported on future versions of OpenStack. The legacy plug-in for Newton is supported. All customers are recommended to use unified mode for both Newton and Ocata.
- The OpFlex agent does not support client authentication. This means that the SSL certificate check must be disabled in Cisco APIC GUI.
 1. In the Cisco APIC GUI, on the menu bar, choose System > System Settings > Fabric Wide Setting.
 2. Ensure that the OpFlex Client Authentication check box is not checked.

Supported Scale

For the verified scalability limits (except the CLI limits), see the *Verified Scalability Guide* for this release. For the OpenStack Platform Scale Limits, see the following table.

Known Limitations

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

Table 3 OpenStack Platform Scale Limits in the 4.2(3) Release

Limit Type	Maximum Supported
Number of OpFlex hosts per leaf	40
Number of vPC links per leaf	40
Number of endpoints per leaf	4,000
Number of endpoints per host	400
Number of virtual endpoints per leaf	40,000

Notes:

- An endpoint is defined as one of the following:
 - A VM interface (also known as vnic),
 - A DHCP agent's port in Openstack (if in DHCP namespace on the network controller), or
 - A floating IP address
- Total virtual endpoints on a leaf can be calculated as:

$$\text{Virtual Endpoints / leaf} = \text{VPCs} \times \text{EPGs}$$

Where:

VPCs is the number of VPC links on the switch in the Attachment Profile used by the Openstack 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
- Cisco ACI Unified Plug-in for OpenStack supports OpenStack address scopes and dual stack IPv4 and IPv6 deployments.

- 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.
- NFV features, including SVI networks, trunk ports, and Service Function Chaining plug-in and workflow, are supported starting with the Ocata release of the plug-in.
- 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. Once both of these conditions are met, you can safely delete the VMM domain Cisco APIC.

Usage Guidelines

- 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.

Usage Guidelines

- Before performing an upgrade from 3.1(1) using OpenStack Director or attempting a Cisco APIC ID recovery procedure, all AIM processes on all controllers need to be shut down. To shut down all the AIM processes on all controllers, run the following command on the undercloud:

```
for IP in $(nova list | grep ACTIVE | sed 's/.*ctlplane=//' | sed 's/|//') ; do
ssh -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no heat-admin@$IP \
"sudo systemctl stop aim-event-service-rpc; sudo systemctl stop aim-aid; sudo systemctl stop
aim-event-service-polling" ;
done
```

If upgrading, you do not need to explicitly restart the AIM processes as the upgrade will automatically restart them.

If attempting a Cisco APIC ID recovery, you must restart the AIM processes on all the controllers manually after ID Recovery is complete.

- 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_state
```

- 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).

Usage Guidelines

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

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).

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

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

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]
...
```

Bugs

```
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.

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 for this release. Check the bug ID to access the Bug Search tool and see additional information about the bug.

Table 4 Open Bugs in the 4.2(3) Release

Bug ID	Description
CSCvs49419	opflex_agent disconnects from the leaf switch every 5 minutes: Need to check results of stat init

Resolved Bugs

This section lists the resolved bugs for this release. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Table 5 Resolved Bugs in the 4.2(3) Release

Bug ID	Description
CSCvr56253	When deploying with Juju Charms, sometimes neutron-opflex-agent needs to be restarted

Related Documentation

Bug ID	Description
CSCvr59278	Removing tripleo-ciscoaci rpm is not deleting /var/www/html/acirepo directory
CSCvr76318	ACI plugin update from 4.1.1 to 4.1.2 doesn't happen for OSP13
CSCvs10076	Error during ACI container build for ACI Red Hat integration because of package conflict
CSCvs41879	Enhancement AIM support OpenStack TLS endpoint encryption

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 Cisco APIC documentation website, you can narrow down the displayed documentation list to make it easier to find the desired document.

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

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

© 2019-2020 Cisco Systems, Inc. All rights reserved.