Cisco Application Policy Infrastructure Controller Container Plug-ins Release 4.1(1), Release Notes

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

Cisco ACI CNI Plug-in is used to provide network services to Kubernetes, Red Hat OpenShift, Cloud Foundry, and Pivotal Cloud Foundry clusters on a Cisco ACI fabric. It allows the cluster pods to be treated as fabric endpoints in the fabric integrated overlay, as well as providing IP Address Management (IPAM), security and load balancing services.

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
2019-04-04	Release 4.1(1) became available.
2019-04-11	In Usage Guidelines section, added information about invoking the `acikubectl` CLI.

Contents

This document includes the following sections:

Cisco ACI Virtualization Compatibility Matrix

For information about Cisco ACI supported Container Products, see the *Cisco 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

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 are the new software features for this release:

- Support for Kubernetes 1.13.
- Support for OpenShift 3.10.
- Support for OpenShift 3.11.
- Support for Kubernetes deployment on Ubuntu 18.04.
- Virtual switch updated to OpenVSwitch 2.10.1.
- Support for adding EndpointGroup (EPG) and SecurityGroup (SG) annotations to Kubernetes ReplicationController and OpenShift DeploymentConfig resources.
- Kubernetes External Services can be shared between VRFs without external routing.
- acikubectl CLI can be accessed using `kubectl` or `oc` for more consistent user experience.
- Cluster report now collects all opflex-agent files (e.g. endpoints, services) to facilitate troubleshooting.
- Git commit ID is made available in all released images and packages for easier traceability to source.

Note: Because there are no changes to the Cloud Foundry and Pivotal Cloud Foundry support from the previous release, there are no new software packages that are posted in this release. Instead, use those packages that are posted for the previous release 3.2.(2).

Changes In Behavior

This section lists changes in behavior in this release.

- The aci-containers-controller no longer annotates the pods with the computed endpoint group and security group information (opflex.cisco.com/endpoint-group and opflex.cisco.com/security-group annotations). The host-agent on a given host now computes this information and the IP addresses for the pods on that host. (Any pods created before the upgrade will continue to have the annotations, but these annotations are redundant.)

Note: There is no change to the user's application of these endpoint group and security group annotations to namespaces, deployments, and pods. It continues to be supported exactly as in previous releases.

- When the scope of an APIC contract created for a load balancer service is to set to "global" by adding an annotation to the Kubernetes service resource definition as follows:

```
"metadata": {
  "annotations": {
    "opflex.cisco.com/ext_service_contract_scope" : "global"
  }
}
```

  it will also set the "import-security" attribute for the Subnet associated with the External Network/EPG that is consuming the contract. This allows the service to be reachable across the VRFs.

- The default subscription refresh time for the ACI containers to APIC has been set to 30 seconds.
- The container image tags will now track ACI releases. For example, in the current release the container images are tagged 4.1.1.x.

Known Limitations

This section lists the known limitations:

- When downgrading from ACI CNI-plugin 4.1(1) to an older release, the vxlan_sys_8472 interface on the host should be first deleted. The interface will be recreated when the host-agent pod restarts.
- OpenShift has the following issues:
  - The 3.10 installation has open issues regarding the following proxy configuration:

    https://github.com/openshift/openshift-ansible/issues/9519
  - Pod /etc/resolv.conf is populated with an incorrect nameserver, possibly with an IP address read from the wrong interface:

    https://bugzilla.redhat.com/show_bug.cgi?id=1680059

    https://github.com/openshift/origin/pull/21866
  - Use the suggested workaround in the issue description.
- The Cisco ACI CNI Plug-ins are not integrated with the Multi-Site Orchestrator. When deploying to a Multi-Site deployment, the Cisco ACI configurations implemented by the plug-ins must not be affected by the Multi-Site Orchestrator.

Usage Guidelines

- The Cisco ACI CNI Plug-in is supported with the following container solutions:
  - Canonical Kubernetes on Ubuntu 18.04 and 16.04

  - Red Hat Openshift on RHEL 7
  - Pivotal Cloud Foundry

- You should be familiar with installing and using Kubernetes or OpenShift. The CNI plug-in (and the corresponding deployment file) is provided to enable networking for an existing installer such as such as kubeadm, Kubespray, or openshift-ansible. Cisco ACI does not provide the Kubernetes or OpenShift installer.

  Refer to the following documents on Cisco.com for details:

  - *Cisco ACI and Kubernetes Integration*
  - *Cisco ACI and OpenShift Integration*
  - *Cisco ACI CNI Plugin for Red Hat OpenShift Container Platform Architecture and Design Guide*
  - *Upgrading the Cisco ACI CNI Plug-in*

- The Cisco ACI CNI plug-in implements various functions running as containers inside pods. The released images for those containers for a given version are available on dockerhub under user noiro. A copy of those container images and the RPM/DEB packages for support tools (acc-provision and acikubectl) are also published on the Software Download page on Cisco.com.

- OpenShift has a tighter security model by default and many off-the-shelf Kubernetes applications such as guestbook may not run on OpenShift (if, for example, they run as root or open privileged ports like 80).

  Please refer to the following for details:

  https://blog.openshift.com/getting-any-docker-image-running-in-your-own-openshift-cluster/

- The Cisco ACI CNI Plug-in is not responsible for any configuration on OpenShift cluster or pods when it comes to working behind a proxy. Running OpenShift "oc new-app" for instance may require access to GitHub and if the proxy settings on the OpenShift cluster are not correctly set, this may fail. Ensure your proxy settings are correctly set.

- In this release, the maximum supported number of PBR based external services is 250 VIPs. Scalability is expected to increase in upcoming releases.

  NOTE: With OpenShift master nodes and router nodes will be tainted by default and you might see lower scale than an upstream Kubernetes install on the same hardware.

- For OpenShift, the external IP used for the LoadBalancer service type is automatically chosen from the subnet pool specified in the ingressIPNetworkCIDR configuration in the /etc/origin/master/master-config.yaml file. This subnet should match the extern_dynamic property configured in the input file provided to acc_provision script. If a specific IP is desired from this subnet pool, it can be assigned to the "loadBalancerIP" property in the LoadBalancer service spec. For more details refer to OpenShift documentation here:

  https://docs.openshift.com/container-platform/3.11/admin_guide/tcp_ingress_external_ports.html#unique-external-ips-ingress-traffic-configure-cluster

  Note: The extern_static subnet configuration in the acc_provision's input is not used for OpenShift.

- On a canonical Kubernetes deployment, the `acikubectl` CLI can be invoked using `kubectl` as follows:

```
kubectl aci --help
```

- On a Red Hat OpenShift deployment, the `acikubectl` CLI can be invoked using `oc` as follows:

```
export KUBECTL_PLUGINS_PATH=/var/lib/aci-containers/kubectl/plugins:{$KUBECTL_PLUGINS_PATH} oc
plugin aci help
```

- The Git commit for different components can be obtained as follows:

```
acc-provision --release #for acc-provision

acikubectl version #for ACI container controller
```

Supported Scale

The Kubernetes, OpenShift, Cloud Foundry, and Pivotal Cloud Foundry Platform scale limits are shown in Table 2:

Table 2: Supported Scale Limits

Limit Type	Maximum Supported
Nodes/Leaf	40
VPC links/Leaf	40
Endpoints[1]/Leaf	4000
Endpoints/Host	400
Virtual Endpoints[2]/Leaf	40,000

[1] An Endpoint corresponds to a Pod's network interface

[2] 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 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.

Bugs

This section contains lists of bugs and known behaviors.

Resolved Bugs

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

Table 3: Resolved Bugs in the 4.1(1) Release

Bug ID	Description
CSCvn77226	In the VLAN ecnap mode some pod endpoints do not get discovered after container bring up.
CSCvo79252	Completed Pods are retained in OVS, causing networking error.
CSCvo42782	In acc-provision, use infra-vlan configured on fabric if it conflicts with input yaml file.
CSCvo24445	acc-provision add service catalog ports for openshift.
CSCvo09390	acikubectl debug logs node not working.

Known Behaviors

This section lists known behaviors. Click the Bug ID to access the Bug Search Tool and see additional information about the bug.

Table 4: Known Behaviors in the 4.1(1) Release

Bug ID	Description
CSCvn13789	Cisco ACI CNI plug-in does not support N/S load-balancer for pods hosted on UCS-B with FI connectivity or for VMs in nested mode that can vMotion.
CSCvm66785	Containers IP is shown as learned on all cluster interfaces.

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.

New Documentation

Upgrading the Cisco ACI CNI Plug-in