Cisco Container Platform 3.0.0 Release Notes

First Published: 2019-02-20

Last Modified: 2019-04-05

Introduction

Cisco Container Platform is a fully curated, lightweight container management platform for production-grade environments, powered by Kubernetes, and delivered with Cisco enterprise-class support. It reduces the complexity of configuring, deploying, securing, scaling, and managing containers using automation along with Cisco's best practices for security and networking. Cisco Container Platform is built with an open architecture using open source components.

Features

Feature	Description
Kubernetes Lifecycle Management	Enables you to deploy Kubernetes clusters, add or removed nodes, and upgrade Kubernetes clusters to latest versions.
Persistent Storage	Allows you to persist data for containerized applications between upgrades and updates through HyperFlex storage driver.
Monitoring and Logging	Provides dashboards, alerts, and indexing to monitor resource usage and behavior of platform components through Elasticsearch, Fluentd, and Kibana (EFK) stack and Prometheus.
Container Networking	Provides container to container and container to non-containerized application layers communication with security policies.
Load Balancing	Offers software Ingress load balancing through NGINX and node port functionality of Kubernetes for containerized applications.
Role Based Access Control	Integrates with Active Directory and offers permission-based rules.

Revision History

Release	Date	Description
1.0	May 22, 2018	First release
1.0.1	May 25, 2018	Updated the **Fixed Issues**and **Know Issues** sections
1.1.0	June 29, 2018	Added the **What's New** and **Upgrading Cisco Container Platform** sections Updated the **Fixed Issues**and **Know Issues** sections
1.4.0	July 31, 2018	Updated the **What's New**, **Fixed Issues**, and **Known Issues** sections
1.4.1	August 6, 2018	Added the **Fixed Issues, 1.4.1** section
1.5.0	September 6, 2018	Updated the **What's New**, **Fixed Issues**, and **Known Issues** sections
2.0.1	October 15, 2018	Updated the **What's New**, **Fixed Issues**, and **Known Issues** sections
2.1.0	November 1, 2018	Updated the **What's New**, **Fixed Issues**, and **Known Issues** sections
2.1.1	December 6, 2018	Added the **Fixed Issues, 2.1.1** section
2.2.2	December 13, 2018	Updated the **What's New**, **Fixed Issues**, and **Known Issues** sections
3.0.0	February 7, 2019	Updated the **System Requirements**, **Fixed Issues**, **Known Issues** and **What's New** sections
3.0.1	February 21, 2019	Updated the **Fixed Issues** section. Added a section on **Backing Up and Restoring Cisco Container Platform Data** .

System Requirements

- Cisco Container Platform Installer OVA
- Latest two versions of the tenant OVA
- vCenter cluster with High Availability (HA) and Distributed Resource Scheduler (DRS) enabled

- A DHCP server that provides IP addresses to the Cisco Container Platform installer VMs
- A shared datastore that is mounted on all the ESXi hosts in the cluster
- Cisco Container Platform Control Plane VMs need to have network access to the vCenter appliance API
- Cisco Container Platform 1.3.0 and later requires hypervisor hosts to be running CPUs with an Ivy Bridge or newer microarchitecture.
- Kubectl version 1.11+

What's New

- Support for Kubernetes 1.12 tenant clusters
  - Supports ACI 3.2(4e).

    Note: This version of ACI CNI supports Kubernetes 1.12.
- Controller and tenant cluster node IP addresses are automatically allocated by Cisco Container Platform
- Removal of support for Kubernetes 1.10
- For deployments or SSH access, supports the use of Ed25519 or ECDSA digital signature algorithms
- Removal of support for less secure RSA and DSA digital signature algorithms
- Password authentication for SSH access to VMs is no longer allowed
- User passphrase is required for passphrase changes
- In an ACI deployment, the Cisco Container Platform cluster name is the same as the ACI tenant name

  For example, if the Cisco Container Platform tenant name is `ccp-tenant-1`, the ACI tenant name is `ccp_tenant_1`.
- Support configuring LDAP/AD during installation and upgrade of Cisco Container Platform
- Support configuring NTP servers for the installer VM using the OVF property

Installing Cisco Container Platform

For step by step instructions on installing Cisco Container Platform, refer to the *Cisco Container Platform Installation Guide*.

Upgrading Cisco Container Platform

- Upgrading Cisco Container Platform is supported from the 1.5.0 release for deployments using Calico or ACI for CNI.
- If an existing deployment uses Contiv for CNI, then upgrades to the current version are not supported.

Backing Up and Restoring Cisco Container Platform Data

It is required to open a support case for assistance in creating a complete backup and for performing a restore.

Fixed Issues

- Fixed list of AMI options for EKS clusters
- Cisco Container Platform web interface bug fixes

Known Issues

- When upgrading Cisco Container Platform or a tenant cluster from 3.0.x to 3.1.x, the managed IP addresses for nodes are not properly released. They remain allocated though not in use. This consumes four IP addresses for the Control Plane and one IP address each for the master and worker nodes of the tenant clusters. For this reason, you may have to expand the IP pool to support future upgrades.

  Note: Upgrading to Cisco Container Platform 3.2.0 (when available) or later versions will not consume extra IP addresses.

- Cisco Container Platform upgrade from a version earlier than 2.2.2 fails when the cluster name contains uppercase letters.

  Workaround

  1. SSH to the Cisco Container Platform Control Plane master VM and change the cluster name to lowercase in the `ccp-appdata` table:

     ```
     sudo apt-get update
      sudo apt-get install -y jq
      kubectl exec -it mysql-0 -- mysql -p$(kubectl get secret mysql -o json | jq -r
     '.data["mysql-root-password"]' | base64 -d) ccp-appdata -e "update keyvalues_keyvalue
      set value = replace(value, 'CCP-CLUSTER-NAME', lower('CCP-CLUSTER-NAME')) where
     instr(value, 'CCP-CLUSTER-NAME') > 0;"
      kubectl exec -it mysql-0 -- mysql -p$(kubectl get secret mysql -o json | jq -r
     '.data["mysql-root-password"]' | base64 -d) ccp-appdata -e "select * from
     keyvalues_keyvalue;"
     ```

  2. If you are using a localized version of vSphere, follow these steps to rename the datastore folder for the cluster data:

     1. In the vSphere web client, click **vCenter**.
     2. Click the **Storage** tab.
     3. From the left pane, choose the datastore that is used to create the cluster.
     4. Select the folder with the cluster name that you want to change.

        For example: `CCP-CLUSTER-NAME`

     5. Rename the folder to the lowercase of the same name.

        For example: `ccp-cluster-name`

  3. Follow these steps to ensure that any existing disk path uses lowercase names:

     1. Click the **Virtual Machines** tab, choose the VM named `ccp-cluster-name-masterxxxxx`, and then click **Edit settings**.
     2. Remove **Harddisk 2**.
     3. Click the **Manage Other Disks** tab and remove **Harddisk**.

4. Click **Add Existing Hard Disk** and choose the disk from `datastore/<your cluster name>/etcd.disk`.
5. Click **Add Existing Hard Disk** and choose the disk from `datastore/<your cluster name>/cert.disk`.

4. Start the upgrade of Cisco Container Platform using the same cluster name in lowercase.

- On Upgrading to HyperFlex 3.5.2, volume traffic disruption occurs.

  Note: This section is applicable only if you are using the HyperFlex Flex Volume plugin for Kubernetes.

  In HyperFlex 3.5.1 or earlier, the IP address used by the vSwitch on ESXi hosts was 169.254.1.1. The HyperFlex clusters whose **Storage Hypervisor Network** addresses are in the range 169.254.1.0/24 conflicted with 169.254.1.1. To work around this IP conflict issue, in HyperFlex 3.5.2, the default IP address is changed to 169.254.254.1. Due to this change, the Flex Volume configuration on the Kubernetes nodes will no longer be correct after an upgrade.

  Workarounds

  Note: You must use **only one** of the following two options to workaround this issue.

  Option 1: Change Configuration on HyperFlex Controller VMs

  You can use this option when there are no existing HyperFlex clusters that use the 169.154.1.0/24 range on ESXi. This avoids the need to change the Kubernetes node configuration for these clusters.

  After upgrading HyperFlex to 3.5.2, follow these steps to change the default IP address to 169.254.1.1:

  1. Run the following command to find iscsiTargetAddress = "169.254.254.1" and replace it with iscsiTargetAddress = "169.254.1.1" in the application.conf file:

     ```
       sed -i -e 's/iscsiTargetAddress*169.254.1.1/iscsiTargetAddress*169.254.254.1/g'
     /opt/springpath/storfs-mgmt/hxSvcMgr-1.0/conf/application.conf
     ```

  2. Run the following command to find istgtConfTargetAddress = "169.254.254.1" and replace it with istgtConfTargetAddress = "169.254.1.1" in the application.conf file:

     ```
      sed -i -e
     's/istgtConfTargetAddress*169.254.254.1/istgtConfTargetAddress*169.254.1.1/g'
     /opt/springpath/storfs-mgmt/hxSvcMgr-1.0/conf/application.conf
     ```

  3. Run the following commands to restart the following services:

     ```
      restart hxSvcMgr
      restart stMgr
     ```

  Option 2: Change Configuration on all Kubernetes VMs

  You can use this option when there are existing HyperFlex clusters that use the 169.154.1.0/24 range on ESXi. After a Kubernetes cluster operation such as scale up or upgrade, this step must be repeated on the new VMs. For this reason, we recommend option 1 as the preferred solution.

  After upgrading HyperFlex to 3.5.2, run the following command for every Kubernetes VM to find "targetIp": "169.254.1.1" and replace it with "targetIp": "169.254.254.1" in the hxflexvolume.json file:

  ```
  ssh -l <ssh user> -i <private key file> <VM IP> -- sed -i -e
  's/169.254.1.1/169.254.254.1/g' /etc/kubernetes/hxflexvolume.json
  ```

  Note:

  The `<ssh user>` must match the ssh user that you specified during cluster creation.

The `<private key file>` must correspond to the public key that you specified during cluster creation.

- The **Upgrade** button on the **Cluster Details** screen of the Cisco Container Platform web interface is not working currently.

  Workaround

  You can upgrade a tenant cluster from the **Clusters** screen.

- During a Control Plane upgrade, if you change the **SUBNET CIDR** field on the **Verify Network** screen, the **IP ADDRESS RANGE** is updated.

  Workaround

  Note: You must use **only one** of the following two options to workaround this issue.

  Option 1:

  Go to the **Authenticate CCP** screen, enter the necessary data, and then click **NEXT**.

  The original IP address range is restored.

  Option 2:

  In a Contiv or Calico deployment, find the original IP address range from the **Network Editing** screen.

  Note:

  - In an ACI deployment earlier than the 2.2.x, the original start and end IP address is the existing Control Plane IP address.
  - In an ACI deployment 2.2.x and later, the original start and end IP address is the same as that which is configured during the Cisco Container Platform installation.

- In an ACI deployment with Kubernetes 1.12, Cisco Container Platform configures the NGINX controller and Fluentd pod during the deployment. If the pods restart post-deployment, the pod configurations are lost.

  Workaround

  Run the following command to configure the pods again:

  ```
  kubectl annotate pod <POD NAME> -n ccp
  opflex.cisco.com/computed-endpoint-group='{"policy-space":"<ACI TENANT
  NAME>","name":"kubernetes|kube-default"}' --overwrite=True
  ```

- During an ACI tenant upgrade, you can safely ignore the Subnet field.
- Cisco Container Platform must use a Kubernetes 1.11 or 1.12 image that is associated with this release. Older versions of the tenant base image are not supported.
- ACI tenant cluster does not work with a link-local interface with Kubernetes 1.11.3.
- You can use only the latest two versions of the tenant image that are associated with the current release. Use of older versions of the tenant image is not supported.
- You will get errors when you scale up tenant clusters or add new node pools to clusters that were created using an older version of **Cisco Container Platform**.

  Workaround

  You must upgrade Cisco Container Platform before attempting to scale up tenant clusters or add new node pools.

- Kubernetes 1.11.3 API server has a known memory leak issue
- When using HyperFlex as the dynamic provisioner, mounting volumes may fail with the following error message:

```
MountVolume.SetUp failed for volume "xxxxx" : mount command failed, status: Failed to
mount volume xxxxx, reason:
```

Workaround

1. Restart the scvmclient on the esx server using the following command:

   ```
   /etc/init.d/scvmclient restart
   ```

2. Ensure that the status is running.

- Contiv as the CNI for tenant clusters is only supported as Tech Preview, and upgrading to a newer version of Cisco Container Platform is not supported.
- In an ACI environment, the link to a tenant cluster Kubernetes Dashboard from the Cisco Container Platform dashboard is not supported. To view the tenant cluster in the Kubernetes Dashboard, you need to obtain the Ingress IP of external IP address using `kubectl get svc`.
- The Cisco Container Platform web interface displays links to external pages such as Smart Licensing. You cannot launch these pages if you do not have access to them.
- Virtual IP address is not released when cluster creation fails.
- In a Contiv deployment, you should not use `matchExpressions` for a NetworkPolicy.
- In a Contiv deployment, network policy does not work with the hostnetwork pod.
- In a Contiv deployment, the pod CIDR must be at least a /14 network.
- In a Calico deployment:
  - The network policy matching on labels will not block hostnetwork access to pods or services.
  - Host IP change may impact pod networking. To resolve the issue, you need to restart the Calico pods.
- `istioctl` is not installed when you enable Istio.

  Workaround

  Run the following command to deploy istioctl:

  ```
  export ISTIO_VERSION=1.0
  curl -L https://git.io/getLatestIstio | sh -
  chmod +x istio-${ISTIO_VERSION}/bin/istioctl
  sudo mv istio-${ISTIO_VERSION}/bin/istioctl /usr/local/bin/
  istioctl version
  ```

  For more information, refer to the *Monitoring Istio Service Meshes* section of the *Cisco Container Platform User Guide*.
- When upgrading Istio from the 0.8 version to the 1.0 version, the backend services stop responding and you need to manually restart them.
- When you upgrade tenant clusters, the Prometheus and EFK components are purged before installing the new versions. If you want to save history, a manual backup and migration are required before a tenant cluster upgrade.

- Taking a snapshot of the VMs managed by Cisco Container Platform is currently unsupported and results in failures during upgrades.
- ACI deployments are only supported in online mode.
- ACI deployments do not support Kubernetes security context.
- cert-manager is now deployed in tenant clusters. It is supported as Tech Preview.

Viewing Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool enables you to access the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. You can search for bugs using bug IDs or keywords.

Before you begin

Ensure that you have a Cisco username and password to log in to the Cisco Bug Search Tool. If you do not have a Cisco username and password, you can register for an account.

Procedure

Step 1 Log in to the Cisco Bug Search Tool with your Cisco username and password.

Step 2 To search for a specific bug, enter the bug ID in the **Search For** field and press the **Enter** key.

Step 3 To search for the bugs that belong to the current release, enter **Cisco Container Platform 3.0.0** in the **Search For** field, and then press the **Enter** key.

Note
- Once the search results are displayed, you can use the **Filter** options to easily find the bugs that are of interest to you.
- You can search for bugs by status, severity, modified date, and so on.

Step 4 To export the results to a spreadsheet, click the **Export Results to Excel** link.

For more information on the Cisco Bug Search Tool, refer to http://www.cisco.com/web/applicat/cbsshelp/help.html.

Related Documentation

The following table lists the documents that are available for Cisco Container Platform.

Document	Description
Cisco Container Platform Installation Guide	Describes installing Cisco Container Platform on your deployment environment.
Cisco Container Platform User Guide	Describes administering and managing Kubernetes clusters, and deploying applications on them.

Document	Description
Cisco Container Platform API Guide	Describes the Cisco Container Platform APIs.

These documents are available on cisco.com.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

What's New in Cisco Product Documentation lists all new and revised Cisco technical documentation. You can subscribe to it, and receive free RSS feed service directly to your desktop using a reader application.