



# Cisco Container Platform 4.2.0 Release Notes

**First Published:** 2019-08-29

**Last Modified:** 2019-09-27

## 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 <b>Fixed Issues</b> and <b>Know Issues</b> sections
1.1.0	June 29, 2018	Added the <b>What's New</b> and <b>Upgrading Cisco Container Platform</b> sections Updated the <b>Fixed Issues</b> and <b>Know Issues</b> sections
1.4.0	July 31, 2018	Updated the <b>What's New</b> , <b>Fixed Issues</b> , and <b>Known Issues</b> sections
1.4.1	August 6, 2018	Added the <b>Fixed Issues, 1.4.1</b> section
1.5.0	September 6, 2018	Updated the <b>What's New</b> , <b>Fixed Issues</b> , and <b>Known Issues</b> sections
2.0.1	October 15, 2018	Updated the <b>What's New</b> , <b>Fixed Issues</b> , and <b>Known Issues</b> sections
2.1.0	November 1, 2018	Updated the <b>What's New</b> , <b>Fixed Issues</b> , and <b>Known Issues</b> sections
2.1.1	December 6, 2018	Added the <b>Fixed Issues, 2.1.1</b> section
2.2.2	December 13, 2018	Updated the <b>What's New</b> , <b>Fixed Issues</b> , and <b>Known Issues</b> sections
3.0.0	February 7, 2019	Updated the <b>System Requirements</b> , <b>Fixed Issues</b> , <b>Known Issues</b> , and <b>What's New</b> sections
3.0.1	February 21, 2019	Updated the <b>Fixed Issues</b> section
3.1.0	March 20, 2019	Updated the <b>System Requirements</b> , <b>Fixed Issues</b> , <b>Known Issues</b> , and <b>What's New</b> sections
3.2.0	April 29, 2019	Updated the <b>System Requirements</b> , <b>Fixed Issues</b> , <b>Known Issues</b> , and <b>What's New</b> sections

Release	Date	Description
3.2.1	May 6, 2019	Updated the <b>Fixed Issues</b> and <b>Known Issues</b> sections
4.0.0	June 11, 2019	Updated the <b>System Requirements</b> , <b>What's New</b> , <b>Fixed Issues</b> , and <b>Known Issues</b> sections
4.0.1	July 3, 2019	Updated the <b>What's New</b> and <b>Known Issues</b> sections
4.1.0	July 25, 2019	Updated the <b>What's New</b> , <b>Fixed Issues</b> , and <b>Known Issues</b> sections
4.2.0	August 29, 2019	Updated the <b>What's New</b> , <b>Fixed Issues</b> , and <b>Known Issues</b> sections
4.2.1	September 27, 2019	Updated the <b>What's New</b> and <b>Fixed Issues</b> sections

## 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
- Kubectl version within one minor version of target Kubernetes cluster
- HyperFlex version 4.0+ is required to use the HyperFlex Container Storage Interface (CSI) storage plugin

## What's New

- Transition to Kubernetes Container Storage Interface (CSI)  
Cisco Container Platform has deprecated the use of FlexVolume and recommends Container Storage Interface (CSI), which is a more robust framework.
- Ivy Bridge architecture is no longer a mandatory requirement for hypervisor hosts
- Support for upgrading Azure Kubernetes Service (AKS) Clusters
- Expanded functionality in v3 API endpoints
- Support for multi-master clusters in v3 clusters
- Support for v2 and v3 cluster operations using the Cisco Container Platform dashboard

- Support for multiple GPUs in v3 cluster types
- Container package and library security updates
- Support for v3 tenant cluster upgrades using the Cisco Container Platform web interface

## 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 2.2.2 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

The IP addresses required for the new Control Plane must be from the original IP address pool range of the Control Plane that was created during installation. If this is not possible, you must open a [support case](#) for assistance in creating a complete backup.

## Fixed Issues

- Cisco Container Platform web interface bugs
- Fixed ability to add Azure cloud provider details while creating an Azure tenant cluster
- Grafana is configured with the appropriate credentials for Prometheus
- During v3 tenant cluster upgrades Nginx and MetalLB charts are upgraded
- Time taken for installing the control plane is reduced

## Known Issues

- Taints and labels for node groups are not supported.
- If you want to create a v3 cluster, you must manually add a v3 vSphere provider in addition to the automatically generated v2 vSphere provider.
- The v3 tenant clusters indicate a **READY** status before provisioning is fully completed.
- Provisioning of control plane nodes may have a delay of up to 10 minutes during the installation process.
- The **vSphere** tab for v3 clusters is not enabled for control planes that are configured to use contiv-vpp network plugin in tenant clusters.
- Istio and Harbor add-ons are available only for v2 clusters.
- Cisco Container Platform 2.2.2, is exposed to the TTA-2019-001 Calico vulnerability. This vulnerability is addressed in Cisco Container Platform 3.0+.

### Workaround

For a tenant cluster that runs Cisco Container Platform 2.2.2, follow these steps to address the vulnerability:

1. Modify the `calico-config` ConfigMap to set the `log_level` to `warning` or higher.

```
kubectl edit configmap -n kube-system calico-config
```

2. Modify the `calico-node` container in the `calico-node` daemonset to set the environment variable `FELIX_LOGSEVERITYSCREEN` to `info` or higher.

```
kubectl patch ds -n kube-system calico-node --patch \ '{"spec": {"template":
{"spec": {"containers": [
  Unknown macro: {"name"}
]}}}'`
```

3. To generate a new secret, follow these steps in the `kube-system` namespace:

1. Find the correct secret.

```
kubectl get secrets -n kube-system | grep calico-node
```

2. Delete the secret.

```
kubectl delete secret -n kube-system
```

A new secret is automatically generated by the token controller.

- Earlier versions of Cisco Container Platform 4.2.0, are exposed to the TTA-2019-002 Calico vulnerability. This vulnerability is addressed in Cisco Container Platform 4.2.0.

### Workaround

For a tenant cluster that runs an earlier version of Cisco Container Platform 4.2.0, follow these steps to address the vulnerability:

1. Download `calicoctl`.

```
curl -O -L
https://github.com/projectcalico/calicoctl/releases/download/v3.7.4/calicoctl
```

2. Ensure `calicoctl` is executable.

```
chmod +x calicoctl
```

3. Apply the attached network policy.

```
sudo DATASTORE_TYPE=kubernetes KUBECONFIG=/etc/kubernetes/admin.conf ./calicoctl
apply -f <DENY_POD_IPIP>.yaml
```

4. Verify the iptable rule.

```
-A cali-po-XXXXXX -s <POD CIDR> -p ipencap -m comment --comment "cali:XXXXXX"
-j DROP
```

- In Cisco Container Platform 4.1.0, Azure Kubernetes Service (AKS) cluster creation fails if you use Kubernetes 1.13.5. The **Clusters** page displays an **UNKNOWN** status for the cluster.

### Workaround

Upgrade to Cisco Container Platform 4.2.0, and then attempt to create Azure Kubernetes Service (AKS) clusters using Kubernetes 1.13.9.

- Azure Kubernetes Service (AKS) cluster creation may fail due to issues in the underlying Azure infrastructure components.

#### Workaround

Create a new AKS cluster.

- Even though the Cisco Container Platform web interface to create AKS clusters indicates that the Pod CIDR and Service CIDR are optional parameters, it is required to specify these parameters.
- When you create local user accounts, it is required to specify the **First Name** and **Last Name** fields.
- Kubernetes dashboard pod may be in a CrashLoopBackOff state on a cluster.

#### Workaround

Connect to the master node of a cluster using SSH and execute the following commands:

```
kubectl apply -f /opt/ccp/manifests/kubernetes-dashboard-role.yaml
kubectl apply -f /opt/ccp/manifests/kubernetes-dashboard-rolebinding.yaml
```

- Mounting volumes fail when using pods with Persistent Volumes provisioned using HyperFlex CSI or HyperFlex.

As a result, the following errors may occur:

- The pod remains in the `ContainerCreating` state.
- Viewing pod details results in errors.

For example:

```
kubectl describe pod <Pod name>

Warning FailedMount ... Unable to mount volumes for pod ...: timeout expired waiting
for volumes to attach or mount for pod
Warning FailedMount ... MountVolume.MountDevice failed for volume ... : rpc error:
code = DeadlineExceeded desc = context deadline exceeded
```

- The log file on the HyperFlex controller VM contains errors.

For example:

```
Error found in /var/log/springpath/debug-scvmlclient.log:

scvmlclient[xxx:xxx]: USER: ALERT: ISTGT.ISTGT.GenericMessage: istgt_lu_disk_init:xxx:
Retrying open for LU1: LUNxxx: retryCnt:1
scvmlclient[xxx:xxx]: USER: ALERT: ISTGT.ISTGT.GenericMessage: istgt_lu_disk_init:xxx:
LU1: LUNxxx: open error(errno=25000)
```

#### Workaround

Follow these steps to reset the state of the HyperFlex FlexVolumes and CSI volumes:

1. Delete the Persistent Volume Claims and Persistent Volumes that are created using HyperFlex FlexVolume or CSI provisioners.

```
kubectl delete pvc <Persistent volume claim name>
kubectl delete pv <Persistent volume name>
```

2. Log in to the HyperFlex controller VM with the HyperFlex Management IP address.

```
/usr/share/zookeeper/bin/zkCli.sh
```

3. On the zkCli console, run the following commands:

```
rmdir /hxVolumeInv
exit
```

4. To clear the HyperFlex Persistent Volume state, run the following commands on each HyperFlex controller VM:

```
rm /nfs/SYSTEM/istgt.conf
restart scvmclient
restart hxSvcMgr
```

5. Verify if the volume is mounted.

```
ls /nfs/SYSTEM
```

If the volume is not mounted, run the following command to mount it:

```
initctl emit --no-wait system-datastore-created
```

- Deploying tenant clusters with GPU requires manual configuration.

After cluster creation, run the following command to manually install the Nvidia Device Plugin on the tenant cluster:

```
kubectl apply -f
https://raw.githubusercontent.com/NVIDIA/k8s-device-plugin/master/nvidia-device-plugin.yml
```

- You cannot modify the size of the repository of a Harbor tenant cluster in the 3.2.0 and 3.2.1 version of Cisco Container Platform.

### Workaround

Provision a Harbor tenant using Cisco Container Platform 4.0.0.

- When you upgrade from the Cisco Container Platform 3.0 version, the managed IP addresses that belong to the old clusters not properly released.
- In the Cisco Container Platform web interface, the EKS clusters are visible only to Admin users.
- Limitations when using vSphere with Cisco Container Platform:
  - You must not place the Cisco Container Platform VMs in a nested folder. It must be retained in the default installation location.
  - You must not configure Cisco Container Platform to use datastores located in folders or in a Storage DRS (SDRS).
- cert-manager is now deployed in tenant clusters. It is supported as Tech Preview.
- 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.

- 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.
- During an ACI tenant upgrade, you can safely ignore the Subnet field.
- Cisco Container Platform must use the Kubernetes images that are associated with the current 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.

- 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.
- 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.
 

For more information on installing Istio, refer to the [latest Istio documentation](#).
  - 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.

## 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 4.2.0** 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.
Cisco Container Platform API Guide	Describes the Cisco Container Platform APIs.

These documents are available on [cisco.com](http://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.

---

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](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. (1721R)

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 Cisco Systems, Inc. All rights reserved.