Cisco Container Platform 1.1.0 Release Notes

First Published: 2018-06-29

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

Release	Date	Description
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, on page 2 and Upgrading Cisco Container Platform, on page 3 sections Updated the Fixed Issues, on page 3 and Known Issues, on page 3 sections

System Requirements

- The Cisco Container Platform Installer OVA
- The tenant OVA
- A vCenter cluster with High Availability (HA) and Distributed Resource Scheduler (DRS) enabled
- A DHCP server that provides IP addresses to the Cisco Container Platform VMs
- A vCenter datastore that is mounted on all the ESX hosts in the cluster
- Cisco Container Platform control plane VMs needs to have network access to vCenter appliance API

What's New

Dashboard

- **Features**
  - The **VIP POOLS** page is replaced with the **Networks** page
  - Some of the ACI related text fields are replaced with drop-down lists that have values provided by the ACI API
  - Clusters are upgraded using the **Actions** > **Upgrade Security**
  - The user role is shown in the **Logout** drop-down list
  - An option is added to show a banner in the Cisco Container Platform web interface after a user has logged in
- **Enhancements**
  - Cluster actions are hidden during pending operations
  - API error messages are shown to the users
- **Application Security**
  - Updated to newer versions of base container images
  - Certificate validity dates are updated to conform to CSDL requirements

- Added authorization for helm chart operations
- A newer base image is used on the Control Plane and the tenant clusters

- **Addons**
  - Updated EFK and monitoring services

- **Installer**
  - Unsuccessful installations can now be retried by restarting the Installer
  - Error messages from the Installer are now less general and show issues found by underlying components
  - NTP servers can now be set during install for the Installer and Cisco Container Platform Control Plane nodes

Installing Cisco Container Platform

For step by step instructions on installing Cisco Container Platform, refer to the *Cisco Container Platform 1.1.0 Installation Guide*.

Upgrading Cisco Container Platform

- Upgrading Cisco Container Platform is supported from the 1.0.0 release for deployments using Calico or ACI for CNI
- If an existing deployment uses Contiv for CNI, you need to install the Cisco Container Platform 1.1.0 version in a new environment.

Fixed Issues

The issues fixed in this release are as follows:

- Increase general stability for long-running clusters
- Fix several bugs related to helm/tiller
- Dashboard
  - Add Infrastructure Provider related information to the ACI summary
  - Update right-side information for the ACI create cluster modal
  - Host Bootstrap static files locally
- Installer
  - The Installer OVA status is now updated faster

Known Issues

The known issues in this release are as follows:

- Contiv as the CNI for tenant clusters is only supported as Tech Preview.
- In an ACI environment, the link to a tenant cluster Kubernetes Dashboard from 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
- If ACI fabric is running 3.1(1i), you need to turn on the promiscuous mode in the corresponding tenant port group in order to make the ACI load balancer functional.
- 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, various networks are used internally by Contiv, and communication to IP addresses outside the cluster is blocked if there is an overlap.
- A master VIP is required for a tenant cluster upgrade. Currently, this is an optional field when you deploy the installer. We recommend that you specify a value for the master VIP.
- 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 is required before a tenant cluster upgrade. After an upgrade, the Cisco Container Platform web interface may be different from its previous version.

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 login to the Cisco Bug Search Tool.

If you do not have a Cisco username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

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 1.1.0`** in the **Search For** field, and then press the **`Enter`** key. (Leave the other fields empty.)

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 available for the Cisco Container Platform 1.1.0 release.

Document	Description
Cisco Container Platform 1.1.0 Installation Guide	Provides information on installing Cisco Container Platform on your deployment environment.
Cisco Container Platform 1.1.0 User Guide	Provides information on administering and managing Kubernetes clusters, and deploying applications on them.

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.