OpenShift Container Platform 4.1

Release notes

Highlights of what is new and what has changed with the OpenShift Container Platform 4.1 release

Last Updated: 2019-09-13

OpenShift Container Platform 4.1 Release notes

Highlights of what is new and what has changed with the OpenShift Container Platform 4.1 release

Legal Notice

Abstract

The release notes for OpenShift Container Platform 4.1 summarize all new features and enhancements, notable technical changes, major corrections from the previous version, and any known bugs upon general availability.

Table of Contents

CHAPTER 1. OPENSHIFT CONTAINER PLATFORM 4.1 RELEASE NOTES

Red Hat OpenShift Container Platform provides developers and IT organizations with a hybrid cloud application platform for deploying both new and existing applications on secure, scalable resources with minimal configuration and management overhead. OpenShift Container Platform supports a wide selection of programming languages and frameworks, such as Java, JavaScript, Python, Ruby, and PHP.

Built on Red Hat Enterprise Linux and Kubernetes, OpenShift Container Platform provides a more secure and scalable multi-tenant operating system for today's enterprise-class applications, while delivering integrated application runtimes and libraries. OpenShift Container Platform enables organizations to meet security, privacy, compliance, and governance requirements.

1.1. ABOUT THIS RELEASE

Red Hat OpenShift Container Platform (RHBA-2019:0758) is now available. This release uses Kubernetes 1.13. New features, changes, and known issues that pertain to OpenShift Container Platform 4.1 are included in this topic.

Red Hat did not publicly release OpenShift Container Platform 4.0 and, instead, is releasing OpenShift Container Platform 4.1 directly after version 3.11.

OpenShift Container Platform 4.1 clusters are available at https://cloud.openshift.com/openshift. The Red Hat OpenShift Cluster Manager application for OpenShift Container Platform allows you to deploy OpenShift clusters to either on-premise or cloud environments.

OpenShift Container Platform 4.1 is supported on Red Hat Enterprise Linux 7.6 and later, as well as Red Hat Enterprise Linux CoreOS 4.1.

You must use Red Hat Enterprise Linux CoreOS (RHCOS) for the control plane, or master, machines and can use either RHCOS or Red Hat Enterprise Linux 7.6 for compute, or worker, machines.

IMPORTANT

Because only Red Hat Enterprise Linux version 7.6 is supported for compute machines, you must not upgrade the Red Hat Enterprise Linux compute machines to version 8.

You can install OpenShift Container Platform 4.1 with installer-provisioned infrastructure on Amazon Web Services (AWS) or user-provided infrastructure on AWS, bare metal, or VMware vSphere hosts. If you use the installer-provisioned infrastructure installation, the cluster provisions and manages all of the cluster infrastructure for you.

OpenShift Container Platform requires all machines, including the computer that you run the installation process on, to have direct internet access to pull images for platform containers and provide telemetry data to Red Hat. You cannot specify a proxy server for OpenShift Container Platform.

1.1.1. Acknowledgments

Red Hat Global Support Services would like to recognize Rushil Sharma, JooHo Lee, and Suresh Gaikwad for their outstanding contributions in evaluating and testing OpenShift Container Platform 4.1.

1.1.2. Deprecated features

Large changes to the underlying architecture and installation process are applied in OpenShift Container Platform 4.1, and many features from OpenShift Container Platform 3.x are now deprecated.

Table 1.1. Features Deprecated in Version 4.1

Feature	Justification
Hawkular	Replaced by cluster monitoring.
Cassandra	Replaced by cluster monitoring.
Heapster	Replaced by Prometheus adapter.
Atomic Host	Replaced by Red Hat Enterprise Linux CoreOS.
System containers	Replaced by Red Hat Enterprise Linux CoreOS.
projectatomic/docker-1.13 additional search registries	CRI-O is the default container runtime for OpenShift Container Platform 4.x on RHCOS and Red Hat Enterprise Linux.
oc adm diagnostics	Operator-based diagnostics.
oc adm registry	Replaced by the Image Registry Operator.
Custom strategy builds using Docker	If you want to continue using custom builds, you should replace your Docker invocations with Podman or Buildah. The custom build strategy will not be removed, but the functionality changed significantly in OpenShift Container Platform 4.1.
Cockpit	Improved OpenShift Container Platform 4.1 web console.
Stand-alone registry installations	Quay is Red Hat's enterprise container image registry.
DNSmasq	CoreDNS is the default.
External etcd nodes	etcd is always on the cluster in OpenShift Container Platform 4.1.
CloudForms OpenShift Provider and Podified CloudForms	Replaced by built-in management tooling.
Volume Provisioning via installer	Replaced by dynamic volumes or, if NFS is required, NFS provisioner.
Blue-green installation method	Ease of upgrade is a core value of OpenShift Container Platform 4.1.

Feature	Justification
OpenShift Service Broker and Service Catalog	The Service Catalog and the OpenShift service brokers are being replaced over the course of several future OpenShift 4 releases. Reference the Operator Framework and Operator Lifecycle Manager (OLM) to continue providing your applications to OpenShift 4 clusters. These new technologies provide many benefits around complete management of the lifecycle of your application.
oc adm ca	Certificates are managed by Operators internally.
oc adm create-api-client-config	Functions are managed by Operators internally.
oc adm create-bootstrap-policy-file	
oc adm policy reconcile-sccs	Functions are managed by **openshift-apiserver** internally.
Web console	The web console from OpenShift Container Platform 3.11 has been replaced by a new web console in OpenShift Container Platform 4.1.

1.2. NEW FEATURES AND ENHANCEMENTS

This release adds improvements related to the following components and concepts.

1.2.1. Operators

Operators are pieces of software that ease the operational complexity of running another piece of software. They act like an extension of the software vendor's engineering team, watching over a Kubernetes environment (such as OpenShift Container Platform) and using its current state to make decisions in real time. Advanced Operators are designed to handle upgrades seamlessly, react to failures automatically, and not take shortcuts, like skipping a software backup process to save time.

1.2.1.1. Operator Lifecycle Manager (OLM)

This feature is now fully supported in OpenShift Container Platform 4.1.

The OLM aids cluster administrators in installing, upgrading, and granting access to Operators running on their cluster:

- Includes a catalog of curated Operators, with the ability to load other Operators into the cluster
- Handles rolling updates of all Operators to new versions
- Supports role-based access control (RBAC) for certain teams to use certain Operators

See Understanding the Operator Lifecycle Manager (OLM) for more information.

1.2.2. Installation and upgrade

Red Hat OpenShift Container Platform 4.1 has an installer-provisioned infrastructure, where the installation program controls all areas of the installation process. Installer-provisioned infrastructure also provides an opinionated best practices deployment of OpenShift Container Platform 4.1 for AWS instances only. This provides a slimmer default installation, with incremental feature buy-in through OperatorHub.

You can also install with a user-provided infrastructure on AWS, bare metal, or vSphere hosts. If you use the installer-provisioned infrastructure installation, the cluster provisions and manages all of the cluster infrastructure for you.

Upgrading from 3.x to 4.1 is currently not available. You must perform a new installation of OpenShift Container Platform 4.1.

Easy, over-the-air upgrades for asynchronous z-stream releases of OpenShift Container Platform 4.x is available. Cluster administrators can upgrade using the **Cluster Settings** tab in the web console. See Updating a cluster for more information.

1.2.2.1. OperatorHub

OperatorHub is available to administrators and helps with easy discovery and installation of all optional components and applications. It includes offerings from Red Hat products, Red Hat partners, and the community.

Table 1.2. Features provided with base installation and OperatorHub

Feature	New installer	OperatorHub
Console and authentication	* [x]	-
Prometheus cluster monitoring	* [x]	-
Over-the-air updates	* [x]	-
Machine management	* [x]	-
Optional service brokers	-	* [x]
Optional OpenShift Container Platform components	-	* [x]
Red Hat product Operators	-	* [x]
Red Hat partner Operators	-	* [x]
Community Operators	-	* [x]

See Understanding the OperatorHub for more information.

1.2.3. Storage

Storage support in OpenShift Container Platform 4.1 is the same as OpenShift Container Platform 3.11 with the exception of the following available in Technology Preview: EFS (CSI Driver handled via Amazon), Manila provisioner/operator, and Snapshot.

1.2.4. Scale

1.2.4.1. Cluster limits

Updated guidance around Cluster Limits for OpenShift Container Platform 4.1 is now available.

Use the OpenShift Container Platform Limit Calculator to estimate cluster limits for your environment.

1.2.4.2. Node Tuning Operator

The Node Tuning Operator is now part of a standard OpenShift Container Platform installation in version 4.1 and later.

The Node Tuning Operator helps you manage node-level tuning by orchestrating the tuned daemon. The majority of high-performance applications require some level of kernel tuning. The Node Tuning Operator provides a unified management interface to users of node-level sysctls and more flexibility to add custom tuning, which is currently a Technology Preview feature, specified by user needs. The Operator manages the containerized tuned daemon for OpenShift Container Platform as a Kubernetes DaemonSet. It ensures the custom tuning specification is passed to all containerized tuned daemons running in the cluster in the format that the daemons understand. The daemons run on all nodes in the cluster, one per node.

1.2.5. Cluster monitoring

1.2.5.1. Autoscale pods horizontally based on the custom metrics API (Technology Preview)

This feature, currently in Technology Preview, enables you to configure horizontal pod autoscaling (HPA) based on the custom metrics API. As part of this Technology Preview, a Prometheus Adapter component can be deployed to provide any app metrics for the custom metrics API.

Limitations:

- The adapter only connects to a single Prometheus instance (or a set of load-balanced replicas, using Kubernetes services).
- Manually deploying adapter and configuring it to use Prometheus.
- Syntax for the Prometheus Adapter configuration could change in the future.
- The **APIService** configuration to wire Kubernetes' API aggregation to the instance of the custom metrics adapter will be overwritten in future releases, if OpenShift Container Platform ships an out-of-the-box custom metrics adapter.

1.2.5.2. New alerting user interface

An alerting UI is now natively integrated into the OpenShift Container Platform web console. You can now view cluster-level alerts and alerting rules from a single place, as well as configure silences.

1.2.5.3. Telemeter

Telemeter collects anonymized cluster-related metrics to proactively help customers with their OpenShift Container Platform clusters. This helps:

- Gather crucial health metrics of OpenShift Container Platform installations.
- Enable a viable feedback loop of OpenShift Container Platform upgrades.
- Gather the cluster's number of nodes per cluster and their size (CPU cores and RAM).
- Gather the size of etcd.
- Gather details about the health condition and status for any OpenShift framework component installed on an OpenShift cluster.

1.2.5.4. Autoscale pods horizontally based on the resource metrics API

By default, OpenShift Cluster Monitoring exposes CPU and Memory utilization through the Kubernetes resource metrics API. There is no longer a requirement to install a separate metrics server.

1.2.6. Developer experience

1.2.6.1. Code ready containers

A local desktop instance of OpenShift Container Platform 4.1 replaces the functions of **oc cluster** commands, Minishift, and CDK. OpenShift Container Platform 4.1 focuses on ease of access and native experience, with a native installation program on macOS and Microsoft Windows, native hypervisor support, and tray icon integration.

1.2.6.2. Multi-stage Dockerfile Builds Generally Available

Multi-stage Dockerfiles are now supported in all **Docker** strategy builds.

1.2.7. Registry

1.2.7.1. The registry is now managed by an Operator

The registry is now managed by an Operator instead of **oc adm registry**.

1.2.8. Networking

1.2.8.1. Cluster Network Operator (CNO)

The cluster network is now configured and managed by an Operator. The Operator upgrades and monitors the cluster network.

1.2.8.2. OpenShift SDN

The default mode is now **NetworkPolicy**.

1.2.8.3. Multus

Multus is a meta plug-in for Kubernetes Container Network Interface (CNI), which enables a user to create multiple network interfaces per pod.

1.2.8.4. SR-IOV

OpenShift Container Platform 4.1 includes the Technical Preview capability to use specific SR-IOV hardware on OpenShift Container Platform nodes, which enables the user to attach SR-IOV virtual function (VF) interfaces to Pods in addition to other network interfaces.

1.2.9. Web console

1.2.9.1. Developer Catalog

OpenShift Container Platform 4.1 features a redesigned Developer Catalog that brings all of the new Operators and existing broker services together, with new ways to discover, sort, and understand how to best use each type of offering. The Developer Catalog is the entry point for a developer to access all services available to them. It merges all capabilities from Operators, the Service Catalog, brokers, and Source-to-Image (S2I).

1.2.9.2. New management screens

New management screens in OpenShift Container Platform 4.1 support automated operations. Examples include the management of machine sets and machines, taints, tolerations, and cluster settings.

1.2.10. Security

In OpenShift Container Platform 4.1, Operators are utilized to install, configure, and manage the various certificate signing servers. Certificates are managed as secrets stored within the cluster itself.

1.3. NOTABLE TECHNICAL CHANGES

OpenShift Container Platform 4.1 introduces the following notable technical changes.

Builds powered by buildah
Source and Docker strategy builds are now performed by buildah instead of the docker daemon.

SecurityContextConstraints
SecurityContextConstraints now only exist in the **security.openshift.io** group.

Service CA bundle changes
Pods can trust cluster-created certificates, which are only signed for internal DNS names, by using a CA bundle that is automatically injected into any configMap annotated with **service.beta.openshift.io/inject-cabundle=true**. The CA bundle will be made available as PEM-encoded data under the key **service-ca.crt**. This annotation results in wiping out existing content in the configMap.

Pods that currently consume the service-serving CA bundle from **/var/run/secrets/kubernetes.io/serviceaccount/service-ca.crt** should migrate to obtaining the CA bundle from a configMap annotated with **service.beta.openshift.io/inject-cabundle=true**.

The **/var/run/secrets/kubernetes.io/serviceaccount/service-ca.crt** file is now deprecated and will be removed in a future release.

OpenShift Service Broker and Service Catalog deprecation
The Service Catalog and the OpenShift service brokers are being replaced over the course of several future OpenShift 4 releases. Red Hat will be deprecating the Template Service Broker and OpenShift Ansible Broker once important dependent content is ported to new Operator-driven solutions. Users are encouraged to look at the Operator Framework and Operator Lifecycle Manager (OLM) to continue providing their applications to OpenShift 4 clusters. These new technologies provide many benefits around complete management of the lifecycle of your application.

Service Catalog no longer installed by default
The Service Catalog is not installed by default in OpenShift Container Platform 4.1. You must install it if you plan on using any of the services from the OpenShift Ansible broker or template service broker. In OpenShift Container Platform 4.1, the Service Catalog API server is installed into the **openshift-service-catalog-apiserver** namespace and the Service Catalog controller manager is installed into the **openshift-service-catalog-controller-manager** namespace. In OpenShift Container Platform 3.11, both of these components were installed into the **kube-service-catalog** namespace.

Template Service Broker no longer installed by default
The Template Service Broker is not installed by default in OpenShift Container Platform 4.1. Cluster administrators can install the Template Service Broker if users will need access to template applications from the web console.

OpenShift Ansible Service Broker no longer installed by default
The OpenShift Ansible Service Broker is not installed by default in OpenShift Container Platform 4.1.

Several `oc adm` commands are now deprecated
Deprecated **oc adm** commands include:

- **oc adm create-master-certs** - Create keys and certificates
- **oc adm create-key-pair** - Create an RSA key pair.
- **oc adm create-server-cert** - Create a key and server certificate.
- **oc adm create-signer-cert** - Create a self-signed CA.

The configurability of the imagepolicyadmission plug-in is not present
The configurability of the **imagepolicyadmission** plug-in is not present in OpenShift Container Platform 4.1. The plug-in runs, but currently only with default configuration. Configuring it requires using the unsupported overrides mechanism.

1.4. TECHNOLOGY PREVIEW FEATURES

Some features in this release are currently in Technology Preview. These experimental features are not intended for production use. Note the following scope of support on the Red Hat Customer Portal for these features:

Technology Preview Features Support Scope

In the table below, features marked **TP** indicate *Technology Preview* and features marked **GA** indicate *General Availability*.

Table 1.3. Technology Preview Tracker

Feature	OCP 3.11	OCP 4.1
Prometheus Cluster Monitoring	GA	GA
Local Storage Persistent Volumes	TP	TP
CRI-O for runtime pods	GA* [a]	GA
Tenant Driven Snapshotting	TP	TP
oc CLI Plug-ins	TP	TP
Service Catalog	GA	GA
Template Service Broker	GA	GA
OpenShift Ansible Service Broker	GA	GA
Network Policy	GA	GA
Multus	-	GA
Service Catalog Initial Experience	GA	GA
New Add Project Flow	GA	GA
Search Catalog	GA	GA
Cron Jobs	GA	GA
Kubernetes Deployments	GA	GA
StatefulSets	GA	GA
Explicit Quota	GA	GA
Mount Options	GA	GA
System Containers for CRI-O	-	-
Hawkular Agent	-	-
Pod PreSets	-	-
experimental-qos-reserved	TP	TP

Feature	OCP 3.11	OCP 4.1
Pod sysctls	GA	GA. See Known issues for current limitations.
Central Audit	GA	GA
Static IPs for External Project Traffic	GA	GA
Template Completion Detection	GA	GA
replicaSet	GA	GA
Fluentd Mux	TP	TP
Clustered MongoDB Template	-	-
Clustered MySQL Template	-	-
ImageStreams with Kubernetes Resources	GA	GA
Device Manager	GA	GA
Persistent Volume Resize	GA	GA
Huge Pages	GA	GA
CPU Pinning	GA	GA
Admission Webhooks	TP	GA
External provisoner for AWS EFS	TP	TP
Pod Unidler	TP	TP
Node Problem Detector	TP	TP
Ephemeral Storage Limit/Requests	TP	TP
Descheduler	TP	TP
CephFS	TP	TP
Podman	TP	TP

Feature	OCP 3.11	OCP 4.1
Kuryr CNI Plug-in	TP	TP
Sharing Control of the PID Namespace	TP	TP
Manila Provisioner	TP	TP
Cluster Administrator console	GA	GA
Cluster Autoscaling (AWS Only)	GA	GA
Container Storage Interface (CSI)	TP	TP
Operator Lifecycle Manager	TP	GA
Red Hat OpenShift Service Mesh	TP	TP
"Fully Automatic" Egress IPs	GA	GA
Pod Priority and Preemption	GA	GA
Multi-stage builds in Dockerfiles	TP	GA
HPA custom metrics adapter based on Prometheus		TP
Machine health checks		TP
SR-IOV		TP

[a] Features marked with * indicate delivery in a z-stream patch.

1.5. KNOWN ISSUES

- Unsafe sysctl cannot be used in OpenShift Container Platform 4.1. (BZ#1690754)
- If an instance is removed from the cloud provider (either via a user deletion, or cloud-provider event of some kind), and the machine-object is reconciled again for some reason, the machine-controller might determine the instance no longer exists and attempt to create the instance. This is undocumented behavior and should not be relied upon for workflows. This operation might interfere with current or future components, such as the node-health-checker. (BZ#1712068)
- Builds which use shell substitution to populate an environment variable may fail. (BZ#1712245)

- When deleting a machine-object, either directly or by scaling down the owning machine-set, if the associated node has already been deleted somehow (possibly by a cluster administrator), the machine-controller will fail to successfully delete the backing cloud instance, and the machine-object will be stuck in **deleting** status. (BZ#1713061)

- Querying **Jolokia** on **JBoss EAP** images fails as the result of empty certificates presented to the client. The **Jolokia** SSL client authentication will fail and may require a username and password challenge if enabled. (BZ#1708640)

- The **TokenRequest** API is not available in OpenShift Container Platform 4.1. Requesting a **ServiceAccountTokenVolumeProjection** volume is not available in OpenShift Container Platform 4.1. The kubelet will present an error if a **ServiceAccountTokenVolumeProjection** is used. (BZ#1695196)

- The **es nodeCount** in ElasticSearch CRD instances can not be scaled up if deployed with three nodes. Scaling works correctly if deployed with one, two, four, five or six ElasticSearch CRD instances. (BZ#1712955)

- ElasticSearch instances created from OperatorHub deploy with a one CPU limit, even though no limits are specified. (BZ#1710657)

- After an AWS installation, the **openshiftClustID** tag is not present. (BZ#1685089)

- scc(CRD) resources can not be upgraded by using the **oc patch** and **oc edit** commands. As a result, strategic merges also fail. (BZ#1707679)

- The OpenShift Container Platform 4.1 registry service utilizes port 5000 instead of port 443. (BZ#1701422)

- Machineset scaling in AWS environments may fail if the resources requested are unavailable in the chosen Availability Zone. (BZ#1713157)

- Using **OAuth** endpoints after configuring ingress wildcard certificates from custom PKIs result in login errors. (BZ#1712525)

- Source-to-Image (S2I) builds in OpenShift Container Platform 4.1 may take longer to complete. This is because OpenShift Container Platform 4.1 does not utilize a shared image cache for building images like in previous versions of OpenShift Container Platform. (BZ#1685352)

- The **cloud-credential-operator** may crash on clusters with large numbers of projects or namespaces due to memory limitations. (BZ#1711402)

- The Marketplace can not detect **opsrc** after a cluster upgrade is performed. As a result, the **csc** packages are empty and can not download **packagemanifests**. Marketplace can repair this problem approximately one hour later when it syncs again. (BZ#1695550)

- In OpenShift Container Platform 4.1, **oc** and **openshift-install** version may have a dirty **GitTreeState:** when checking the **oc version**. (BZ#1715001)

- In AWS environments, if a master node is stopped, the **kubeapiserver** cannot be deployed due a pod stuck in a **Pending** status. (BZ#1713292)

- All m4 instances on AWS fail to verify (CVE-2019-1109) using Broadwell CPU model 79 (type m4) because the **microcode_ctl** will not update. (BZ#1710981)

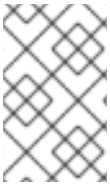
- New ElasticSearch deployments can not be created if another ElasticSearch deployment is stuck in a deleting state. (BZ#1711044)

- There is no *Open Java Console* link available in the OpenShift Container Platform 4.1 web console. (BZ#1713656)
- The **openshift-cluster-node-tuning-operator** may generate a large number of secrets after several days of uptime. (BZ#1714484)
- Autoscaling for Memory Utilization is not working as expected. Creating HPA for memory-based autoscaling is failing while looking for resources. (BZ#1707785)
- After successfully performing updates, **oc clusterversion** may report that the update could not be applied. (BZ#1711964)
- The installer may have a **0** return code when hitting a FATAL event. (BZ#1712409)

1.6. ASYNCHRONOUS ERRATA UPDATES

Security, bug fix, and enhancement updates for OpenShift Container Platform 4.1 are released as asynchronous errata through the Red Hat Network. All OpenShift Container Platform 4.1 errata is available on the Red Hat Customer Portal . See the OpenShift Container Platform Life Cycle for more information about asynchronous errata.

Red Hat Customer Portal users can enable errata notifications in the account settings for Red Hat Subscription Management (RHSM). When errata notifications are enabled, users are notified via email whenever new errata relevant to their registered systems are released.



NOTE

Red Hat Customer Portal user accounts must have systems registered and consuming OpenShift Container Platform entitlements for OpenShift Container Platform errata notification emails to generate.

This section will continue to be updated over time to provide notes on enhancements and bug fixes for future asynchronous errata releases of OpenShift Container Platform 4.1. Versioned asynchronous releases, for example with the form OpenShift Container Platform 4.1.z, will be detailed in subsections. In addition, releases in which the errata text cannot fit in the space provided by the advisory will be detailed in subsections that follow.

IMPORTANT

For any OpenShift Container Platform release, always review the instructions on updating your cluster properly.

1.6.1. RHBA-2019:0758 - OpenShift Container Platform 4.1 Image Release advisory

Issued: 2019-06-04

OpenShift Container Platform release 4.1 is now available. The list of packages included in the update are documented in the RHBA-2019:1173 advisory. The container images and bug fixes included in the update are provided by the RHBA-2019:0758 advisory.

Space precluded documenting all of the container images for this release in the advisory. See the following article for notes on the container images in this release: OpenShift Container Platform 4.1.0 container image list

1.6.2. RHBA-2019:1381 - OpenShift Container Platform 4.1.2 Bug Fix Update

Issued: 2019-06-18

OpenShift Container Platform release 4.1.2 is now available. The list of packages included in the update are documented in the RHBA-2019:1381 advisory. The container images and bug fixes included in the update are provided by the RHBA-2019:1382 advisory.

Space precluded documenting all of the container images for this release in the advisory. See the following article for notes on the container images in this release:

OpenShift Container Platform 4.1.2 container image list

1.6.2.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.1 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

1.6.3. RHBA-2019:1590 - OpenShift Container Platform 4.1.3 Bug Fix Update

Issued: 2019-06-26

OpenShift Container Platform release 4.1.3 is now available. The list of packages included in the update are documented in the RHBA-2019:1590 advisory. The container images and bug fixes included in the update are provided by the RHBA-2019:1589 advisory.

Space precluded documenting all of the container images for this release in the advisory. See the following article for notes on the container images in this release:

OpenShift Container Platform 4.1.3 container image list

1.6.3.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.1 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

1.6.4. RHSA-2019:1591 - Low: OpenShift Container Platform 4.1 image security update

Issued: 2019-06-26

An update for ose-cluster-kube-apiserver-operator-container and ose-cluster-openshift-apiserver-operator-container is now available for OpenShift Container Platform 4.1. Details of the update are documented in the RHSA-2019:1591 advisory.

1.6.5. RHSA-2019:1636 - Important: OpenShift Container Platform 4.1 jenkins-2-plugins security update

Issued: 2019-07-03

An update for jenkins-2-plugins is now available for OpenShift Container Platform 4.1. Details of the update are documented in the RHSA-2019:1636 advisory.

1.6.6. RHBA-2019:1634 - OpenShift Container Platform 4.1.4 Bug Fix Update

Issued: 2019-07-04

OpenShift Container Platform release 4.1.4 is now available. The list of packages included in the update are documented in the RHBA-2019:1634 advisory. The container images and bug fixes included in the update are provided by the RHBA-2019:1635 advisory.

Space precluded documenting all of the container images for this release in the advisory. See the following article for notes on the container images in this release:

OpenShift Container Platform 4.1.4 container image list

1.6.6.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.1 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

1.6.7. RHBA-2019:1767 - OpenShift Container Platform 4.1.6 Bug Fix Update

Issued: 2019-07-17

OpenShift Container Platform release 4.1.6 is now available. The list of packages included in the update are documented in the RHBA-2019:1767 advisory. The container images and bug fixes included in the update are provided by the RHBA-2019:1766 advisory.

Space precluded documenting all of the container images for this release in the advisory. See the following article for notes on the container images in this release:

OpenShift Container Platform 4.1.6 container image list

1.6.7.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.1 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

1.6.8. RHBA-2019:1808 - OpenShift Container Platform 4.1.7 Bug Fix Update

Issued: 2019-07-24

OpenShift Container Platform release 4.1.7 is now available. The list of packages included in the update are documented in the RHBA-2019:1808 advisory. The container images and bug fixes included in the update are provided by the RHBA-2019:1809 advisory.

Space precluded documenting all of the container images for this release in the advisory. See the following article for notes on the container images in this release:

OpenShift Container Platform 4.1.7 container image list

1.6.8.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.1 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

1.6.9. RHBA-2019:1866 - OpenShift Container Platform 4.1.8 Bug Fix Update

Issued: 2019-07-31

OpenShift Container Platform release 4.1.8 is now available. The list of packages included in the update are documented in the RHBA-2019:1865 advisory. The container images and bug fixes included in the update are provided by the RHBA-2019:1866 advisory.

Space precluded documenting all of the container images for this release in the advisory. See the following article for notes on the container images in this release:

OpenShift Container Platform 4.1.8 container image list

1.6.9.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.1 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

1.6.10. RHBA-2019:2010 - OpenShift Container Platform 4.1.9 Bug Fix Update

Issued: 2019-08-08

OpenShift Container Platform release 4.1.9 is now available. The list of packages included in the update are documented in the RHBA-2019:2009 advisory. The container images and bug fixes included in the update are provided by the RHBA-2019:2010 advisory.

Space precluded documenting all of the container images for this release in the advisory. See the following article for notes on the container images in this release:

OpenShift Container Platform 4.1.9 container image list

1.6.10.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.1 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

1.6.11. RHBA-2019:2417 - OpenShift Container Platform 4.1.11 Bug Fix Update

Issued: 2019-08-14

OpenShift Container Platform release 4.1.11 is now available. The list of packages included in the update are documented in the RHBA-2019:2416 advisory. The container images and bug fixes included in the update are provided by the RHBA-2019:2417 advisory.

Space precluded documenting all of the container images for this release in the advisory. See the following article for notes on the container images in this release:

OpenShift Container Platform 4.1.11 container image list

1.6.11.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.1 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

1.6.12. RHBA-2019:2547 - OpenShift Container Platform 4.1.13 Bug Fix Update

Issued: 2019-08-28

OpenShift Container Platform release 4.1.13 is now available. The list of packages included in the update are documented in the RHBA-2019:2546 advisory. The container images and bug fixes included in the update are provided by the RHBA-2019:2547 advisory.

Space precluded documenting all of the container images for this release in the advisory. See the following article for notes on the container images in this release:

OpenShift Container Platform 4.1.13 container image list

1.6.12.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.1 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

1.6.13. RHBA-2019:2660 - OpenShift Container Platform 4.1.14 Bug Fix Update

Issued: 2019-09-10

OpenShift Container Platform release 4.1.14 is now available. The list of packages included in the update are documented in the RHBA-2019:2660 advisory. The container images and bug fixes included in the update are provided by the RHSA-2019:2594 advisory.

Space precluded documenting all of the container images for this release in the advisory. See the following article for notes on the container images in this release:

OpenShift Container Platform 4.1.14 container image list

1.6.13.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.1 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

1.6.14. RHBA-2019:2681 - OpenShift Container Platform 4.1.15 Bug Fix Update

Issued: 2019-09-12

OpenShift Container Platform release 4.1.15 is now available. The list of packages included in the update are documented in the RHBA-2019:2681 advisory. The container images and bug fixes included in the update are provided by the RHBA-2019:2680 advisory.

Space precluded documenting all of the container images for this release in the advisory. See the following article for notes on the container images in this release:

OpenShift Container Platform 4.1.15 container image list

1.6.14.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.1 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

CHAPTER 2. OPENSHIFT CONTAINER PLATFORM VERSIONING POLICY

OpenShift Container Platform provides strict backwards compatibility guarantees for all supported APIs, excluding alpha APIs (which may be changed without notice) and beta APIs (which may occasionally be changed in a non-backwards compatible manner).

Red Hat did not publicly release OpenShift Container Platform 4.0 and, instead, is releasing OpenShift Container Platform 4.1 directly after version 3.11.

The OpenShift Container Platform version must match between master and node hosts, excluding temporary mismatches during cluster upgrades. For example, in a 4.1 cluster, all masters must be 4.1 and all nodes must be 4.1. If you installed an earlier version of **oc**, you cannot use it to complete all of the commands in OpenShift Container Platform 4.1. You must download and install the new version of **oc**.

Changes of APIs for non-security related reasons will involve, at minimum, two minor releases (3.4 to 3.5 to 3.6, for example) to allow older **oc** to update. Using new capabilities may require newer **oc**. A 3.2 server may have additional capabilities that a 3.1 **oc** cannot use and a 3.2 **oc** may have additional capabilities that are not supported by a 3.1 server.

Table 2.1. Compatibility Matrix

	X.Y (**oc** Client)	**X.Y+N** [a] (**oc** Client)
X.Y (Server)	1	3
X.Y+N [a] (Server)	2	1

[a] Where **N** is a number greater than 1.

1 Fully compatible.

2 **oc** client may not be able to access server features.

3 **oc** client may provide options and features that may not be compatible with the accessed server.