OpenShift Container Platform 4.3

Release notes

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

Last Updated: 2020-04-02

OpenShift Container Platform 4.3 Release notes

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

Legal Notice

Abstract

The release notes for OpenShift Container Platform 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

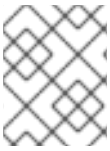
CHAPTER 1. OPENSHIFT CONTAINER PLATFORM 4.3 RELEASE NOTES

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-2020:0062) is now available. This release uses Kubernetes 1.16 with CRI-O runtime. New features, changes, and known issues that pertain to OpenShift Container Platform 4.3 are included in this topic.



NOTE

This is an increase of two versions of Kubernetes from OpenShift Container Platform 4.2, which used Kubernetes 1.14.

OpenShift Container Platform 4.3 clusters are available at https://cloud.redhat.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 4.3 is supported on Red Hat Enterprise Linux 7.6 or later, as well as Red Hat Enterprise Linux CoreOS 4.3.

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 or later for compute, or worker, machines.

IMPORTANT

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

1.2. NEW FEATURES AND ENHANCEMENTS

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

1.2.1. Installation and upgrade

1.2.1.1. OpenShift Container Platform upgrades phased rollout

In OpenShift Container Platform 4.1, Red Hat introduced the concept of upgrade channels for recommending the appropriate upgrade versions to your cluster. Upgrade channels separate upgrade strategies and also are used to control the cadence of updates. Channels are tied to a minor version of OpenShift Container Platform. For instance, OpenShift Container Platform 4.3 channels will never

include an upgrade to a 4.4 release. This ensures administrators make an explicit decision to upgrade to the next minor version of OpenShift Container Platform. Channels only control updates and have no impact on the version of the cluster you install; the **openshift-install** binary for a given patch level of OpenShift Container Platform always installs that patch level.

You must choose the upgrade channel version corresponding to the OpenShift Container Platform version you plan to upgrade to. OpenShift Container Platform 4.3 includes the upgrade from the previous 4.2 release.

See OpenShift 4.x Upgrades phased roll out for more information on the types of updates and upgrade channels.

Because upgrades are published to the channels as they are gradually rolled out to customers based on data from the Red Hat Service Reliability Engineering (SRE) team, you might not immediately see notification in the web console that updates from version 4.2.z to 4.3 are available at initial release.

1.2.1.2. Support for FIPS cryptography

You can now install an OpenShift Container Platform cluster that uses FIPS validated / Implementation Under Test cryptographic libraries. OpenShift Container Platform uses certain FIPS validated / Implementation Under Test modules within Red Hat Enterprise Linux (RHEL) and Red Hat CoreOS (RHCOS) for the operating system components that it uses. For more information, see Support for FIPS cryptography.

1.2.1.3. Deploy private clusters on AWS, Azure, or GCP

You can install a private cluster into an

- existing VPC on Amazon Web Services (AWS).
- existing VPC on Google Cloud Platform (GCP).
- existing Azure Virtual Network (VNet) on Microsoft Azure.

To create a private cluster on these cloud platforms, you must provide an existing private VPC/VNet and subnets to host the cluster. The installation program configures the Ingress Operator and API server for access from only the private network.

For more information on deploying private clusters to each supported cloud platform, see the installation guides for AWS, Azure, and GCP.

1.2.2. Security

1.2.2.1. Automated rotation of service serving certificates CA

Automated service CA rotation will be available in this release in a future z-stream update. In previous versions, the service CA did not automatically renew, leading to service disruption and requiring manual intervention. The service CA and signing key now auto-rotate before expiration. This allows administrators to plan for their environments in advance, avoiding service disruption.

1.2.2.2. Encrypt data stored in etcd

You can now encrypt data stored in etcd . Enabling etcd encryption for your cluster provides an additional layer of data security.

When you enable etcd encryption, the following OpenShift API server and Kubernetes API server resources are encrypted:

- Secrets
- ConfigMaps
- Routes
- OAuth access tokens
- OAuth authorize tokens

1.2.3. Cluster monitoring

1.2.3.1. Improvements for PromQL query browser in web console

Performance improvements are now available for the PromQL query browser used in the OpenShift Container Platform web console.

1.2.3.2. Use Pod capacity metric for KubeletTooManyPods alert

The **KubeletTooManyPods** alert now uses the Pod capacity metric as a threshold instead of a fixed number.

1.2.3.3. Monitor your own services (Technology Preview)

The existing monitoring stack can be extended so you can configure monitoring for your own Services.

1.2.3.4. Querying metrics in the web console (Technology Preview)

Querying metrics is now available through the Developer perspective inside the OpenShift Container Platform web console.

1.2.4. Machine API

1.2.4.1. Automatically repair damaged machines with machine health checking

A machine instance that is deleted out of band no longer attempts to recreate a new instance; instead, the machine enters a *failed* phase. You can automatically repair damaged machines in a machine pool by configuring and deploying a machine health check.

The controller that observes a MachineHealthCheck resource checks for the status that you define. If a machine fails the health check, it is automatically deleted and a new one is created to take its place. When a machine is deleted, you see a machine-deleted event. To limit disruptive impact of the machine deletion, the controller drains and deletes only one node at a time.

To stop the check, you remove the resource.

1.2.5. Logging

1.2.5.1. Log forwarding (Technology Preview)

The log forwarding feature provides a way to ship container and node logs to destinations that are not necessarily managed by the OpenShift Container Platform cluster logging infrastructure. Destination endpoints can be on or off your OpenShift Container Platform cluster. Log forwarding provides an easier way to forward logs than using Fluentd plug-ins without requiring you to set the cluster to Unmanaged. See Forwarding cluster logs to specific endpoints for more information.

1.2.6. Developer experience

1.2.6.1. OpenShift Do enhancements

OpenShift Do (odo) has a few enhancements that focus on the user experience of application deployment:

- **PushTimeout** has been added as a configurable wait parameter.
- Both the Service Catalog and component creation have been improved with extended output and information prompts.
- Architecture support has been expanded to IBM Z and PowerPC platforms, providing binaries that are available for installation.

1.2.6.2. Helm (Technology Preview)

Helm is a package manager for Kubernetes and OpenShift Container Platform applications. It uses a packaging format called Helm charts to simplify defining, installing, and upgrading of applications and Services.

Helm CLI is built and shipped with OpenShift Container Platform and is available in the web console's CLI menu to download.

1.2.7. Web console

1.2.7.1. New Project dashboard

The new **Project** dashboard is now available from the Administrator and Developer perspectives. This dashboard provides the following information about a project:

- status/health
- external links
- inventory
- utilization
- resource quota
- activity and top consumers

1.2.7.2. New NamespaceDashboard option in the ConsoleLink Custom Resource Definition

The new location option **NamespaceDashboard** in the ConsoleLink Custom Resource Definition lets you add project-specific links to the project dashboard.

1.2.7.3. Provide cluster-wide third-party user interfaces

You can now integrate cluster-wide third-party user interfaces to develop, administer, and configure Operator-backed services with the ConsoleLink Custom Resource Definition.

1.2.7.4. New ConsoleYAMLSample Custom Resource Definition

The new **ConsoleYAMLSample** Custom Resource Definition provides the ability to dynamically add YAML examples to any Kubernetes resource at any time.

See Customizing the web console for more information.

1.2.7.5. Open a Support case from the web console

You can now open a Red Hat Support case from the help menu in the web console.

1.2.7.6. View security vulnerabilities

You can now view your container vulnerabilities from the web console dashboard. This leverages the Quay Operator, which supports both on-premise and external Quay registries. Security vulnerabilities are only reported for images managed by Quay.

1.2.7.7. New User Management section

All user management resources are now available under the **User Resource** navigation section.

The ability to impersonate a user has also been added, which lets you view exactly what a user sees when navigating the console.

1.2.7.8. Create alert receivers

You can now create alert receivers to be informed about your cluster's state. You can create PagerDuty and webhook alert types.

1.2.7.9. Developer perspective

You can now use the Developer perspective to:

- Create serverless applications and revisions, and split traffic between the revisions.
- Delete an application and all its components.
- Assign RBAC permissions to users within a project.
- Bind an application with a Service using the binding connector.

1.2.7.10. CSI provisioners now shown on storage class creation page

Container Storage Interface (CSI) provisioners are now shown on the storage class creation page. Storage classes are hardcoded in the user interface; CSI-based storage classes are dynamic in nature and do not have static names. Now, users are able to list CSI-based provisioners in the storage class creation page and can also create one.

1.2.8. Networking

1.2.8.1. Configure network policy

The Kubernetes **v1** NetworkPolicy features are available in OpenShift Container Platform except for egress policy types and IPBlock.

IPBlock is supported in NetworkPolicy with limitations; it supports IPBlock without **except** clauses. If you create a policy with an **ipBlock** section including an **except** clause, the SDN Pods log warnings, and the entire **ipBlock** section of that policy is ignored.

1.2.8.2. Kuryr CNI support for Red Hat OpenStack Platform (RHOSP)

You can install a customized cluster on RHOSP 13 and 16 that uses Kuryr SDN. You can follow the installation guide for installing a cluster on OpenStack with Kuryr.

1.2.9. Scale

1.2.9.1. Cluster maximums

Updated guidance around Cluster maximums for OpenShift Container Platform 4.3 is now available.

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

1.2.10. Storage

1.2.10.1. OpenShift Container Storage 4.2

You can now deploy, manage, monitor, and migrate a Red Hat OpenShift Container Storage 4.2 cluster. See the Red Hat OpenShift Container Storage 4.2 Release Notes for more information.

1.2.10.2. Persistent storage Using iSCSI

Persistent volumes using iSCSI, previously in Technology Preview, is now fully supported in OpenShift Container Platform 4.3.

1.2.10.3. Raw block volume support

iSCSI raw block volumes, previously in Technology Preview, are now fully supported with OpenShift Container Platform 4.3.

Raw block volumes using Cinder are now in Technology Preview.

1.2.10.4. CSI volume expansion

You can now use the Container Storage Interface (CSI) to expand storage volumes after they have already been created. This feature is enabled by default in Technology Preview.

1.2.10.5. Use tolerations in Local Storage Operator

The Local Storage Operator now tolerates node taints, allowing you to provision local volumes from tainted nodes.

1.2.11. Operators

1.2.11.1. Samples Operator

The Samples Operator automatically recognizes the cluster architecture during installation and does not install incompatible x86_64 content on Power and Z architectures.

The Samples Operator also uses Prometheus metrics to gather information about which imagestreams have failed to import, and if the Samples Operator has invalid configurations. An alert is sent if an imagestream fails to import or the Samples Operator has an invalid configuration.

1.2.11.2. Image Registry Operator

The following enhancements are now available for the Image Registry Operator:

- The registry management state is set as **Removed** on Baremetal, vSphere, and Red Hat Virtualization platforms so other storage providers can be configured. New installations must set the registry state to **Managed** in addition to provisioning storage.
- An alert is sent when the registry storage has changed, as this could result in data loss.

1.2.11.3. Simplified mirroring of OperatorHub

Assuming there is a registry running in a disconnected environment available to both the disconnected cluster and to the workstation from which the **oc adm** commands are run, you can now mirror the OperatorHub by following three steps:

1. Mirror the Operator catalog into the container image and push to the disconnected registry using **oc adm catalog build**.
2. Parse the referenced Operator and app images and push to the disconnected registry using **oc adm catalog mirror**.
3. Enable the mirror catalog in the disconnected cluster using **oc apply -f ./manifests**.

See Using Operator Lifecycle Manager on restricted networks for details.

1.2.11.4. Operator telemetry and alerts

The Lifecycle Operator Manager (OLM) now reports installed Operator information. For example, the OLM sends alerts about Operators transitioning into the failure state.

1.3. NOTABLE TECHNICAL CHANGES

OpenShift Container Platform 4.3 introduces the following notable technical changes.

Operator SDK v0.12.0
OpenShift Container Platform 4.3 supports Operator SDK v0.12.0 or later.

The Operator test tooling (scorecard v2) now includes the following improvements:

- Categorizing Operator tests as required/optional.
- Configuring test selection and pass/fail behavior.
- Shipping custom tests.

For Helm-based Operators, improvements include

- Helm v3 support, starting with Operator SDK 0.14.0.
- Role-based access control (RBAC) generation.

Ansible-based Operator enhancements include

- Support for Prometheus metrics.
- Usage of Red Hat Universal Base Image (UBI).
- Molecule-based end to end testing.

Lastly, the Golang-based Operator improvements include

- OpenAPI spec generation.
- Kubernetes 1.14 support.
- Removal of **dep**-based projects. All Go projects are now scaffolded to use Go modules. The **operator-sdk new** command's **--dep-manager** flag has been removed.
- Required Go version update from v1.10 to v1.13.
- Support for Prometheus metrics.

Cluster logging out_forward configuration changes
Changes introduced by the new log forwarding feature modified the support for the Fluentd **out_forward** plug-in starting with the OpenShift Container Platform 4.3 release. For the 4.3 release, you can still use the legacy **out_forward** method, without using the new log forwarding feature, which is in Technology Preview.

To use the legacy **out_forward**, you must create a ConfigMap object to configure **out_forward** instead of editing the **secure-forward.conf** section in the **fluentd** ConfigMap. Additionally, you can add any certificates required by your configuration to a secret that is mounted to the Fluentd Pods. See Sending logs to external devices using Fluentd Forward plug-ins.

In 4.3, the legacy **out_forward** method is deprecated and will be removed in a future release.

When you update to OpenShift Container Platform 4.3, any existing modifications to the **secure-forward.conf** section of the **fluentd** ConfigMap are removed. You can copy your current **secure-forward.conf** section before updating to use when creating the **secure-forward** ConfigMap object.

1.3.1. Unsupported features

Cluster logging no longer allows forwarding logs by editing the Fluentd Daemonset
Due to changes introduced by the new log forwarding feature, you can no longer forward logs to an external Elasticsearch instance by editing the Fluentd DaemonSet.

In previous versions, you could use the **ES_HOST** and **OPS_HOST** environment variables or configure the **fluent-plugin-remote-syslog** plug-in through the **fluentd** Daemonset.

You can forward logs to an external Elasticsearch instance and other endpoints using the new log forwarding feature or the Fluentd **forward** plug-ins. The documentation is now updated to reflect these changes.

1.3.1.1. Local storage provisioner

The previously deprecated Technical Preview of the **ose-local-storage-provisioner** container has been removed. It is recommended to use the OLM-based Local Storage Operator (**ose-local-storage-operator**).

1.3.1.2. Persistent volume snapshots

Persistent volume snapshots were deprecated in OpenShift Container Platform 4.2 and have been removed in OpenShift Container Platform 4.3.

1.3.2. Deprecated features

1.3.2.1. Pipelines build strategy

The pipelines build strategy is now deprecated. Use OpenShift Pipelines instead.

1.3.2.2. Beta workload alerts

The **apps/v1beta1**, **apps/v1beta2**, and **extensions/v1beta1** workloads are now deprecated with the introduction of Kubernetes 1.16.

The **UsingDeprecatedAPIExtensionsV1Beta1** alert is prompted when you use one of the deprecated APIs. These deprecated APIs will be removed in the next version of OpenShift Container Platform, so it is critical that you migrate to supported APIs.

1.3.2.3. Service Catalog, Template Service Broker, Ansible Service Broker, and their Operators

Service Catalog, Template Service Broker, Ansible Service Broker, and their associated Operators were deprecated in OpenShift Container Platform 4.2 and will be removed in a future OpenShift Container Platform release. If they are enabled in 4.3, the web console now warns the user that these features are still enabled.

The following alerts can be viewed from the **Monitoring → Alerts** page and have a **Warning** severity:

- **ServiceCatalogAPIServerEnabled**
- **ServiceCatalogControllerManagerEnabled**
- **TemplateServiceBrokerEnabled**
- **AnsibleServiceBrokerEnabled**

The following related APIs will be removed in a future release:

- **.servicecatalog.k8s.io/v1beta1**
- **.automationbroker.io/v1alpha1**
- **.osb.openshift.io/v1**

1.3.2.4. Deprecation of OperatorSources and CatalogSourceConfigs

OperatorSources and CatalogSourceConfigs are deprecated from OperatorHub. The following related APIs will be removed in a future release:

- **operatorsources.operators.coreos.com/v1**
- **catalogsourceconfigs.operators.coreos.com/v2**
- **catalogsourceconfigs.operators.coreos.com/v1**

1.3.2.5. VirtualBox support for CodeReady Containers

The support for using VirtualBox with CodeReady Containers (CRC) is now deprecated.

1.4. BUG FIXES

Authentication

- The Authentication Operator reported a static "available" string as a reason for the unavailability condition, which was unclear. This bug fix implements more precise reasons for unavailability conditions, and as a result, inspecting why the Operator is unavailable is more clear. (BZ#1740357)
- The **oauth-proxy** process was reloading CA certificates for each request and storing them in memory. High memory consumption caused the **oauth-proxy** container to be killed. With this bug fix, CA certificates are now cached unless they change. As a result, memory consumption for the **oauth-proxy** process has dropped significantly when multiple requests against it are issued. (BZ#1759169)
- Previously, the client CA certificate configured for the RequestHeader identity provider (IdP) was not announced among other certificates during TLS handshake with the OAuth server. When **login-proxies** tried to connect to the OAuth server, they would not use their client certificate, resulting in their request being unauthenticated, which in turn caused users of the IdP being unable to log in to the cluster. This bug fix adds the configured client CA among the rest in the TLS configuration, and as a result, authentication using the RequestHeader IdP works as expected. (BZ#1764558)
- The bootstrap user introduced in OpenShift Container Platform (OCP) 4.1 internally made CLI log flow always available. The message about how to retrieve an authentication token, which was there in OCP 3.x, no longer appeared for users that tried to log in from CLI in cases where only web console flows were configured. With this bug fix, the bootstrap user identity provider (IdP) is no longer configured when it is disabled by the user. As a result, after the bootstrap IdP is disabled by following the steps from the OCP documentation, the message about how to retrieve an authentication token in web console-only scenarios is now displayed. (BZ#1781083)
- Previously, the route to oauth-server did not react to Ingress domain changes, which degraded the Authentication Operator and caused the oauth-server to not authenticate properly. The oauth-server route now updates when an Ingress domain change is detected, allowing authentication to work in this scenario. (BZ#1707905)

Builds

- Builds started very soon after an imagestream was created might not leverage local pullthrough imagestream tags when specified. The build attempts to pull the image from the external image registry, and if the build is not set up with the authorization and certificates needed for that registry, the build would fail. The build controller is now updated to detect when its imagestream cache is missing the necessary information to allow for local pullthrough imagestream tags and retrieve that information from other means. Builds can now successfully leverage local imagestream tag pullthrough. (BZ#1753731)

- The build controller sometimes incorrectly assumed a build was instantiated from the build config endpoint when it was actually instantiated directly from the build endpoint. Therefore, confusing logging about non-existent build configs could appear in the build controller logs if a user instantiated an OpenShift build directly, as opposed to initiating a build request off of the build config API endpoint. The build controller is now updated to better check whether a build was instantiated from the build config endpoint and refrain from logging unnecessary error messages.The build controller logs no longer have these confusing error messages for build instantiated directly versus from the build config endpoint. (BZ#1767218), (BZ#1767219)

Cluster Version Operator

- Previously, the update protocol Cincinnati, designed to facilitate automatic updates, used tags for payload references. This could yield different results when applying the same release of the same graph at different points. Now the payload reference uses the image SHA instead, if the container registry provides the **manifestref**. This guarantees the exact release version a cluster is going to use. (BZ#1686589)

Console Kubevirt Plugin

- Previously, the specified **volumeMode** was not passed to newly created disks, so PVCs might not bind properly. The **volumeMode** is now passed properly to the newly created disks. (BZ#1753688)

- Previously, the virtual machine detail page did not load properly when accessed directly by the URL. The page now loads properly. (BZ#1731480)

- Previously, the **kubevirt-storage-class-defaults** ConfigMap setting was not reflected properly for VMware VM imports. Because of this, **blockMode** PVCs could not be used for VMware VM imports. The storage class defaults are now used properly when requesting VMware imported disks. (BZ#1762217)

- Previously, the title for the Import VM wizard was incorrect and could be confusing. The wizard now has the correct title of **Import Virtual Machine**. (BZ#1768442)

- Previously, the confirmation buttons for storage and network configuration in the VM migration wizard were located in the wrong place. These confirmation buttons are now located in the correct location. (BZ#1778783)

- Previously, the **Create Virtual Machine**wizard did not prompt for confirmation before creating a VM, which meant the user could unexpectedly create a VM. With this fix, the user must click "Create Virtual Machine" on the review page before a VM is created. (BZ#1674407)

- Previously, the **Create Virtual Machine**wizard had required fields that were not always intuitive when importing a VM. The **Create Virtual Machine**wizard has been redesigned to work as expected. (BZ#1710939)

- Previously, error messages for validating VM names were not helpful. These error messages have been improved to be more descriptive. (BZ#1743938)

Containers

- Previously, CRI-O was not properly filtering Podman containers during a restore operation. Because Podman containers do not have CRI-O-specific metadata, at startup, CRI-O would interpret the Podman containers it saw as CRI-O containers that were incorrectly created. It would therefore ask the storage library to delete the containers. This bug fix now properly filters Podman containers on CRI-O restore so that they are no longer deleted from storage upon startup. (BZ#1758500)

Developer Console

- An invalid property was introduced into the Pipeline Operator during an upgrade. As a result, Pipelines could no longer start from the UI. The property is now updated to use a valid specification. As a result, Pipelines start from the UI again. (BZ#1763725)

Etcd

- Etcd would become overloaded with a large number of objects, causing the cluster to go down when etcd failed. Now, the etcd client balancer facilitates peer failovers in the event of a client connection timeout. (BZ#1706103)

- Etcd would fail during the upgrade process and result in disaster recovery remediation steps. Now, etcd has been updated to resolve gRPC package to prevent catastrophic cluster failure. (BZ#1733594)

Image Registry

- After changing the storage type in the image registry Operator's configuration, both the previous and new storage types appeared Operator's status. Because of this behavior, the image registry Operator was not removed after you deleted its configuration. Now only the new storage type is displayed, so the image registry Operator is removed after you change the storage type that the image uses. BZ#1722878)

- Because it was possible for older imagestreams to have invalid names, image pruning failed when the specs for the imagestream's tags were invalid. Now, the image pruner always prune images when the associated imagestream has an invalid name. BZ#1749256)

- When the image registry operator's management state was **Removed**, it did not report itself as Available or the correct version number. Because of this issue, upgrades failed when the image registry operator was set to **Removed**. Now when you set the image registry Operator's status to **Removed**, it reports itself as Available and at the correct version. You can complete upgrades even if you remove the image registry from the cluster. (BZ#1753778)

- It was possible to configure the image registry Operator with an invalid Azure container name, and the image registry did not deploy on Azure because of the invalid name. Now the image registry Operator's API schema ensures that the Azure container name that you enter conforms to Azure's API requirements and is valid, which ensures that the Operator can deploy. (BZ#1750675)

kube-apiserver

- An unnecessary service monitoring object was created for each of the following contollers: kube-apiserver, kube-controller-manager, and kube-scheduler. The unused service monitoring object is no longer created. (BZ#1735509)

- When a cluster is in a non-upgradeable state because either Technology Preview features or custom features are enabled, no alert was sent. The cluster will now send a **TechPreviewNoUpgrade** alert through Prometheus if an upgrade is attempted on a cluster in a non-upgradeable state. (BZ#1731228)

kube-controller-manager

- When defining a StatefulSet resource object, custom labels were not applied when creating PersistentVolumeClaim resource objects from the template specified by **volumeClaimTemplates** parameter. Custom labels are now applied correctly to

PersistentVolumeClaim objects created from the **volumeClaimTemplates** objects defined by a StatefulSet resource. (BZ#1753467)

- Previously, if the lease ConfigMap for the Kubernetes Controller Manager (KCM) was deleted, KCM did not have permission to recreate the ConfigMap and was unable to do so. The KCM can now recreate the lease ConfigMap if it is deleted. (BZ#1780843)

Logging

- Mismatches between cluster version and ClusterLogging version would cause ClusterLogging to fail to deploy. Now, the kubeversion is verified that it supports the deployed ClusterLogging version. (BZ#1765261)

- The data in journald for facility values was not sanitized and values were incorrect, causing fluentd to emit error messages at the wrong level. Now, fluentd logs at the debug level and these errors are reported correctly. (BZ#1753936,BZ#1766187)

- The oauth-proxy was misconfigured in a way that users were unable to log in after logging out. Now, the oauth-proxy has been reconfigured so that users can log in again after logging out. (BZ#1725517)

- Eventrouter was not able to handle unknown event types, which would result in Eventrouter crashing. Now, Eventrouter properly handles unknown event types. (BZ#1753568)

Management Console

- The Management Console Dashboard Details were unnecessarily watching the Infrastructure resources. As a result, errors regarding early web socket connection terminations were possible. Now, the Details card does not watch Infrastructure resources and only fetches the resource data once. Errors are not reported after implementing this fix. (BZ#1765083)

- The console Operator would record an initial empty string value for the console URL before the router had a chance to provide the host name. Now, the Operator waits until the hostname is filled and eliminates the empty string value. (BZ#1768684)

Metering Operator

- Previously, the **containerImage** field in the **metering-operator** CSV bundle referenced an image tag that was not listed in the **image-references** file that ART uses for substitution purposes. This meant that ART wasn't able to properly substitute the origin image listed in the **containerImage field** with the associated **image-registry** repository and **sha256** tag. This bug fix replaces the image tag **latest** with **release-4.3**, which is what was defined in the **image-references** file. As a result, ART is now able to successfully substitute the **metering-operator** container image. (BZ#1782237)

- Previously, Hadoop **Dockerfile.rhel** copied the **gcs-connector** JAR file to the wrong location in the container. The path has been corrected to now point to the right location. (BZ#1767629)

Networking

- Previously, not all related objects were deleted when the CNO was changed, which left stale network-attachment-definitions. The code has been refactored to now do this in a more generic way in OpenShift Container Platform 4.3 so that the related objects are cleaned up properly. (BZ#1755586)

- Previously, some updates were dropped which caused events to be missed. Events are no longer dropped. (BZ#1747532)

- Previously, in clusters that had high network traffic volumes with packet loss, a once-successful connection to a service could fail with a **Connection reset by peer** error. As a result, clients had to reconnect and retransmit. An update has been made to iptables rules to process TCP retransmits correctly. Established connections will remain open until they are closed. (BZ#1762298)

- Previously, NetworkPolicy rule applications to new namespaces could occur slowly in clusters that had many namespaces, namespace changes, and NetworkPolicies that select namespaces. New namespaces could take significant amounts of time before they could be accessed from other namespaces. Due to an update in Namespace and NetworkPolicy code, NetworkPolicies should be applied promptly to new namespaces. (BZ#1752636)

- Previously, SDN pods did not clean up Egress IP addresses when they restarted on a node, resulting in IP address conflicts. SDN pods now clean up stale Egress IP addresses as they start, preventing such conflicts from occuring. (link: BZ#1753216)

- Previously, DNS names were queried every time they occured in an EgressNetworkPolicy. Records were queried regardless of whether a particular DNS record had been refreshed by a previous query, resulting in slow network performance. DNS records are now queried based on unique names rather than per each EgressNetworkPolicy. As a result, DNS query performance has been significantly improved. (BZ#1684079)

- Route creation between multiple service endpoints was not possible from the console. Now, the GUI has been updated to add or remove up to three alternative service endpoints. (BZ#1725006)

Node

- Previously, when containers had a high (or > 1) restart count, the kubelet could inject duplicate container metrics into the metrics stream, causing the **/metrics** endpoint on the kubelet to throw a 500 error. With this bug fix, only metrics of the most current container (running or stopped) are included. As a result, the **/metrics** endpoint now allows metrics to flow to Prometheus without causing a 500 error. (BZ#1779285)

- Upstream changes were made to the long path names test. Pods with names longer than 255 character were not logged and no warning was issued. Now, the long names test is removed and Pods with names longer than 255 characters will log as expected. (BZ#1711544)

- The **LocalStorageCapacityIsolation** feature was disabled, and users were unable to use the **Statefulset.emptyDir.sizeLimit** parameter. Now, the **LocalStorageCapacityIsolation** feature has been enabled and the **Statefulset.emptyDir.sizeLimit** parameter can be set. (BZ#1758434)

oc

- Previously when using server-side print, the wide output option was ignored when used in a watch (**oc get clusteroperators -o wide**). The operation has been fixed to now properly recognize all the possible options when using server-side print. (BZ#1685189)

- The **oc explain** command links to upstream documentation were out of date. These links have been updated and are now valid. (BZ#1727781)

- Full usage menu information was printed along with bad flag error messages, causing the error message to be lost at times. Now, when the **oc command --help** command is run, the bad flag error is the only information displayed. (BZ#1748777)

- The **oc status** command was not displaying DaemonSets in a consistent format due to missing status code information. Now, the Daemonsets, Deployments, and Deployment Configurations are printed properly in the output of the **oc status** command. (BZ#1540560)

- The commands **oc version** and **oopenshift-install version** would show as Dirty due to incorectly set flags. These flags have been updated and the commands no longer display a Dirty **GitTreeState** or **GitVersion**. (BZ#1715001)

- The **oc status** command would suggest **oc set probe pod** to verify pods are still running, including pods that may have been owned by controllers. Now, pods that are owned by controllers are ignored for probe suggestions. (BZ#1712697)

- Previously, the **oc new-build** help command was not properly filtering flags. This caused irrelevant flags to be printed when invoking **oc new-build --help**. This has been fixed, and now the help command only prints relevant output. (BZ#1737392)

openshift-apiserver

- The **ClusterResourceQuota** in 4.2 and 4.3 were not allowing non-strings as limit values because the OpenAPI schema was wrong. Therefore, integer quota values could not be set in **ClusterResourceQuota** objects, even though doing so was previously possible in 4.1. The OpenAPI schema for **ClusterResourceQuota** has been fixed to allow integers so that integers can now be used as quota values in **ClusterResourceQuota** again. (BZ#1756417)

- During upgrades, **openshift-apiserver** would report **degraded**. The reason for degradation was **MultipleAvailable**, but this was not understandable to the user. This bug fix now lists the reason for the degradation, so that no information is hidden from the user. (BZ#1767156)

Web Console

- The console workload shows a restricted access error if the knative serverless TP1 Operator is installed and you are logged in as non-admin user. With this bug fix, the Overview sidebar resources now work as expected for both normal and knative-specific deployments. A non-admin user can now view the workloads. (BZ#1758628)

- The topology view data model was originally a subset of the project Workloads page. As more feature were added, the topology view grew to be similar but did not share the same code. As use cases became more complex, certain edge cases were being missed in the new code. In certain situations, the Pod list from the topology view was incorrect. With this bug fix, code logic is now shared between the topology view and project Workloads page. As a result, whether viewing the sidebar Pod list from topology or from the project Workloads list, the Pod details are now identical. (BZ#1760827)

- Previously, when the Route object was created, the first port from the list of available ports was set instead of setting the selected port from the target-port dropdown menu. Because of this, the user was unable to select their desired target port. The port selected from the target port dropdown menu is now applied when creating a Route object; if no port is selected, the first port from the list is set. (BZ#1760836)

- Previously, certain features, such as the name of the application and the build status, were not rendered in the **Topology** view on the Edge browser. With this bug fix, the Edge browser renders the application name and the build status as expected. (BZ#1760858)

- In the web console Overview, a non-admin user was not able to view workloads when the Knative Operator was installed, even if a deployment that was not a Knative workload was selected. This bug fix adds a check in case there are no configurations found so that the system will not add

Knative-specific resources in Overview. This enables a non-admin user to now view the workloads as expected. (BZ#1760810)

- Previously, when the Topology context menu was open, the associated node was not easily identifiable. This caused confusion for users because they did not know which node the context menu referred to. Now when right-clicking a node to open the context menu, a visual hover, or drop shadow, is applied to the node for easier identification. (BZ#1776401)

- Previously, the **Import from Git** form in the web console used a regular expression too restrictive to validate the Git URL, which disallowed some valid URLs. The regular expression has been updated to accept all valid Git URLs. (BZ#1766350), (BZ#1771851)

- Error messages from the developer console were duplicated. Now, this system has been updated to reflect values from the client side. As a result, error messages are now clear and concise. (BZ#1688613)

- Previously, the web console could experience a runtime error when visiting the Resources tab of an OLM operand resource. The web console could also freeze when trying to sort the Resources tab for an OLM operand resource. These issues are now resolved. (BZ#1756319)

- Previously, visiting the OpenShift web console pod details page in Microsoft Edge could result in a runtime error, preventing the page from displaying. The issue is now resolved and the pod details page now displays correctly. (BZ#1768654)

- Previously, if a dashboard card watched Prometheus results, the dashboard page's performance could decrease due to an incorrect comparison between old alerts and new alerts. The comparison defect has been fixed. (BZ#1781053)

- In previous versions, the documentation link on the Network Policy page was incorrect. It has been replaced with the correct link. (BZ#1692227)

- Previously, Prometheus queries contained a range selector, which prevented the chart on the default page of the Prometheus UI from rendering. The queries no longer contain range selectors, so the query now renders properly. (BZ#1746979)

- **Recycle** was the default value for the Persistent Volume Reclaim policy even though that option was deprecated. Persistent Volumes contained deprecated values by default. The default Persistent Volume Reclaim policy is now **Retain**, so new Persistent Volumes do not contain deprecated values. (BZ#1751647)

- Previously, after upgrading your cluster, the web console could use cached CSS stylesheets, which might cause some rendering issues when loading the console. The problem has been fixed, and the web console now correctly uses the correct stylesheets after an upgrade. (BZ#1772687)

- Previously, when using the web console in some situations part of the options menu was hidden behind other elements on the page. The options menu no longer appears behind other page elements and will expand in a viewable space on the page to ensure the entire menu is always visible. (BZ#1723254)

- Previously, long node names could overflow the table column in the OpenShift console pods table. With this bug fix, they now correctly wrap. (BZ#1713193)

- Previously, creating a report query using an example YAML would result in an error. This bug fix adds a new YAML example for report queries that contains all required fields so that an error does not occur. (BZ#1753124)

- Previously on the Install Plan Details page, the namespace for associated catalog sources was set incorrectly. This resulted in broken links because the namespace did not exist. This bug fix uses the **status.plan** field of the InstallPlan resource to associate the catalog source with the correct namespace to build links from. Thus, the catalog source links now work as expected. (BZ#1767072)

- Previously, unknown custom resources were automatically split into words to estimate what the user should see. However, some resources were split inappropriately. With this bug fix, custom resources now use the name as defined in the Custom Resource Definition, rather than being split into separate words.(BZ#1722811)

1.5. 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*. Features marked as **-** indicate that the feature is removed from the release or deprecated.

Table 1.1. Technology Preview Tracker

Feature	OCP 4.1	OCP 4.2	OCP 4.3
Prometheus Cluster Monitoring	GA	GA	GA
Precision Time Protocol (PTP)	-	-	TP
CRI-O for runtime Pods	GA	GA	GA
oc CLI Plug-ins	TP	TP	TP
Service Catalog	GA	GA	–
Template Service Broker	GA	GA	-
OpenShift Ansible Service Broker	GA	GA	-
Network Policy	GA	GA	GA
Multus	GA	GA	GA
New Add Project Flow	GA	GA	GA
Search Catalog	GA	GA	GA

Feature	OCP 4.1	OCP 4.2	OCP 4.3
Cron Jobs	GA	GA	GA
Kubernetes Deployments	GA	GA	GA
StatefulSets	GA	GA	GA
Explicit Quota	GA	GA	GA
Mount Options	GA	GA	GA
System Containers for Docker, CRI-O	-	-	-
Hawkular Agent	-	-	-
Pod PreSets	-	-	-
experimental-qos-reserved	TP	TP	TP
Pod sysctls	GA	GA	GA
Central Audit	-	-	-
Static IPs for External Project Traffic	GA	GA	GA
Template Completion Detection	GA	GA	GA
replicaSet	GA	GA	GA
Clustered MongoDB Template	-	-	-
Clustered MySQL Template	-	-	-
ImageStreams with Kubernetes Resources	GA	GA	GA
Device Manager	GA	GA	GA
Persistent Volume Resize	GA	GA	GA

Feature	OCP 4.1	OCP 4.2	OCP 4.3
Huge Pages	GA	GA	GA
CPU Pinning	GA	GA	GA
Admission Webhooks	GA	GA	GA
External provisioner for AWS EFS	TP	TP	TP
Pod Unidler	TP	TP	TP
Node Problem Detector	TP	TP	TP
Ephemeral Storage Limit/Requests	TP	TP	TP
CephFS	TP	TP	TP
Podman	TP	TP	TP
Kuryr CNI Plug-in	-	TP	GA
Sharing Control of the PID Namespace	TP	TP	TP
Manila Provisioner	TP	TP	TP
Cluster Administrator console	GA	GA	GA
Cluster Autoscaling	GA	GA	GA
Container Storage Interface (CSI)	TP	GA	GA
Operator Lifecycle Manager	GA	GA	GA
Red Hat OpenShift Service Mesh	GA	GA	GA
"Fully Automatic" Egress IPs	GA	GA	GA

Feature	OCP 4.1	OCP 4.2	OCP 4.3
Pod Priority and Preemption	GA	GA	GA
Multi-stage builds in Dockerfiles	GA	GA	GA
OVN-Kubernetes Pod network provider	TP	TP	TP
HPA custom metrics adapter based on Prometheus	TP	TP	TP
Machine health checks	TP	TP	GA
Persistent Storage with iSCSI	TP	TP	GA
Raw Block with iSCSI	-	TP	GA
Raw Block with Cinder	-	-	TP
OperatorHub		GA	GA
Three-node bare metal deployments	-	TP	TP
SR-IOV Network Operator	-	TP	GA
Helm CLI	-	-	TP
Service Binding	-	-	TP
Log forwarding	-	-	TP
User workload monitoring	-	-	TP
OpenShift Serverless	TP	TP	TP
Compute Node Topology Manager	-	-	TP

1.6. KNOWN ISSUES

- If you have Service Mesh installed, upgrade Service Mesh before upgrading OpenShift Container Platform. For a workaround, see Updating OpenShift Service Mesh from version 1.0.1 to 1.0.2.

- Determination of active Pods when a rollout fails can be incorrect in the **Topology** view. (BZ#1760828)

- When a user with limited cluster-wide permissions creates an application using the **Container Image** option in the **Add** page, and chooses the **Image name from internal registry** option, no imagestreams are detected in the project, though an imagestream exists. (BZ#1784264)

- The **ImageContentSourcePolicy** is not supported by the registry at the time of release (BZ#1787112). In disconnected environments, Jenkins can be enabled to pull through by default. Use this command as a workaround to use Jenkins in disconnected environments:

```
$ oc tag <jenkins_source_image> jenkins:2 --reference-policy=source -n openshift
```

- The OpenShift Cluster Version Operator (CVO) does not correctly mount SSL certificates from the host, which prevents cluster version updates when using MITM proxy checking. (BZ#1773419)

- When adding **defaultProxy** and **gitProxy** under **builds.config.openshift.io**, the Jenkins pipeline build cannot retrieve the proxy configuration. (BZ#1753562)

- When installing on Red Hat OpenStack Platform 13 or 16, where the OpenStack endpoints are configured with self-signed TLS certificates the installation will fail. (BZ#1786314,BZ#1769879,BZ#1735192)

- Installer-provisioned infrastructure installations on OpenStack fail with **Security group rule already exists** error when OpenStack Neutron is under heavy load. (BZ#1788062)

- Clusters will display errors and abnormal states after **etcd** backup or restore functions are conducted during the **etcd** encryption migration process. (BZ#1776811)

- RHCOS master and worker nodes may go into a **NotReady,SchedulingDisabled** state while upgrading from 4.2.12 to 4.3.0. (BZ#1786993)

- The public cloud access image for RHEL cannot be used directly if you enable FIPS mode. This is caused by public cloud images not allowing kernel integrity checks. To do this, you must upload your own images. (BZ#1788051)

- The Operator Lifecycle Manager (OLM) does not work in OpenShift Container Platform when Kuryr SDN is enabled. (BZ#1786217)

- The **oc adm catalog build** and **oc adm catalog mirror** commands do not work for the restricted cluster. (BZ#1773821)

- When upgrading a OpenShift Container Platform cluster from 4.1 to 4.2 to 4.3, there is a possibility that the Node Tuning Operator tuned Pods can get stuck in the **ContainerCreating** state.
  To confirm the issue, run:

```
$ oc get pods -n openshift-cluster-node-tuning-operator
```

  One or more tuned Pods are stuck in the **ContainerCreating** state.

To resolve the issue, apply the following workaround. Run:

```
$ oc delete daemonset/tuned -n openshift-cluster-node-tuning-operator
$ oc get daemonset/tuned -n openshift-cluster-node-tuning-operator
$ oc get pods -n openshift-cluster-node-tuning-operator
```

Verify that the Pods are now in a **Running** state. (BZ#1791916)

- The Node Feature Discovery (NFD) Operator version 4.3 fails to deploy from OpertorHub on the OpenShift Container Platform web console. As a workaround, download the **oc** client for your operating system, and place the **kubeconfig** file from the installer in **~/.kube/config**. Run these commands to deploy the NFD Operator from the CLI and GitHub:

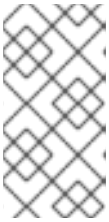
```
$ cd $GOPATH/src/openshift
$ git clone https://github.com/openshift/cluster-nfd-operator.git
$ cd cluster-nfd-operator
$ git checkout release-4.3
$ PULLPOLICY=Always make deploy
$ oc get pods -n openshift-nfd
```

Example output:

```
$ oc get pods -n openshift-nfd
NAME READY STATUS RESTARTS AGE
nfd-master-gj4bh 1/1 Running 0 9m46s
nfd-master-hngrm 1/1 Running 0 9m46s
nfd-master-shwg5 1/1 Running 0 9m46s
nfd-operator-b74cbdc66-jsgqq 1/1 Running 0 10m
nfd-worker-87wpn 1/1 Running 2 9m47s
nfd-worker-d7kj8 1/1 Running 1 9m47s
nfd-worker-n4g7g 1/1 Running 1 9m47s
```

(BZ#1793535)

- If a cluster-wide egress proxy is configured and then later unset, Pods for applications that have been previously deployed by OLM-managed Operators can enter a **CrashLoopBackOff** state. This is caused by the deployed Operator still being configured to rely on the proxy.



NOTE

This issue applies for environment variables, Volumes, and VolumeMounts created by the cluster-wide egress proxy. This same issue occurs when setting environment variables, Volumes, and VolumeMounts using the SubscriptionsConfig object.

A fix is planned for a future release of OpenShift Container Platform, however you can workaround the issue by deleting the Deployment using the CLI or web console. This triggers OLM to regenerate the Deployment and starts up Pods with the correct networking configuration.

Cluster administrators can get a list of all affected OLM-managed Deployments by running the following command:

```
$ oc get deployments --all-namespaces \
  -l olm.owner,olm.owner!=packageserver 1
```

1 Exclude **packageserver**, which is unaffected.

(BZ#1751903)

- There is an issue with the Machine Config Operator (MCO) supporting Day 2 proxy support, which describes when an existing non-proxied cluster is reconfigured to use a proxy. The MCO should apply newly configured proxy CA certificates in a ConfigMap to the RHCOS trust bundle; this is not working. As a workaround, you must manually add the proxy CA certificate to your trust bundle and then update the trust bundle:

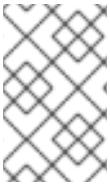
```
$ cp /opt/registry/certs/<my_root_ca>.crt /etc/pki/ca-trust/source/anchors/
$ update-ca-trust extract
$ oc adm drain <node>
$ systemctl reboot
```

(BZ#1784201)

1.7. ASYNCHRONOUS ERRATA UPDATES

Security, bug fix, and enhancement updates for OpenShift Container Platform 4.3 are released as asynchronous errata through the Red Hat Network. All OpenShift Container Platform 4.3 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 4.3. Versioned asynchronous releases, for example with the form OpenShift Container Platform 4.3.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.

1.7.1. RHBA-2020:0062 - OpenShift Container Platform 4.3 Image release and bug fix advisory

Issued: 2020-01-23

OpenShift Container Platform release 4.3 is now available. The list of container images and bug fixes includes in the update are documented in the RHBA-2020:0062 advisory. The RPM packages included in the update are provided by the RHBA-2019:0063 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 4.3.0 container image list

1.7.2. RHBA-2020:0390 - OpenShift Container Platform 4.3.1 Bug Fix Update

Issued: 2020-02-12

OpenShift Container Platform release 4.3.1 is now available. The list of packages included in the update are documented in the RHBA-2020:0390 advisory. The container images and bug fixes included in the update are provided by the RHBA-2020:0391 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 4.3.1 container image list

1.7.2.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.3 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

1.7.3. RHBA-2020:0491 - OpenShift Container Platform 4.3.2 Bug Fix Update

Issued: 2020-02-19

OpenShift Container Platform release 4.3.2 is now available. The list of packages included in the update are documented in the RHBA-2020:0491 advisory. The container images and bug fixes included in the update are provided by the RHBA-2020:0492 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 4.3.2 container image list

1.7.3.1. Bug Fixes

- Amazon Web Services (AWS) installer-provisioned infrastructure and Red Hat OpenStack Platform (RHOSP) user-provisioned infrastructure were missing security group rules allowing bi-directional traffic between control plane hosts and workers on TCP and UDP ports 30000-32767. This caused newly introduced OVN Networking components to not work properly in clusters lacking these security group rules. Now security group rules are available to allow the aforementioned bi-directional traffic support. (**BZ#1779469**)

- The OpenShift Pipeline Operator v0.9.x+ did not work with UI code after the removal of an API reference. The **serviceAccount** field in Pipeline Runs was replaced with the **serviceAccountName** field, but was still being used by the Operator. This caused pipelines created in OpenShift Container Platform to not create Pipeline Runs correctly. The API references have been fixed, and pipelines work again with the OpenShift Pipeline Operator v0.9.x+. (**BZ#1788201**)

- Previously, users would be given a *Restricted Access* error when trying to access the **Installed Operators** page in the web console. This happened because the console was trying to access the subscription resource outside of the current namespace to show subscription details. Users can now access the **Installed Operators** page. The **Subscription** tab will be hidden from users who can not access the subscription resource. (BZ#1791101)

1.7.3.2. Upgrading

To upgrade an existing OpenShift Container Platform 4.3 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

1.7.4. RHBA-2020:0528 - OpenShift Container Platform 4.3.3 Bug Fix Update

Issued: 2020-02-24

OpenShift Container Platform release 4.3.3 is now available. The list of packages included in the update are documented in the RHBA-2020:0527 advisory. The container images and bug fixes included in the update are provided by the RHBA-2020:0528 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 4.3.3 container image list

1.7.4.1. Bug Fixes

- The API group of KnativeServing resources **serving.knative.dev** is deprecated and it has changed to **operator.knative.dev** in Serverless Operator 1.4. (BZ#1779469)

1.7.4.2. Upgrading

To upgrade an existing OpenShift Container Platform 4.3 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

1.7.5. RHSA-2020:0562 - Moderate: OpenShift Container Platform 4.3 Security Update

Issued: 2020-02-24

An update for jenkins-slave-base-rhel7-container is now available for OpenShift Container Platform 4.3. Details of the update are documented in the RHSA-2020:0562 advisory.

1.7.6. RHBA-2020:0675 - OpenShift Container Platform 4.3.5 Bug Fix Update

Issued: 2020-03-10

OpenShift Container Platform release 4.3.5 is now available. The list of packages included in the update are documented in the RHBA-2020:0675 advisory. The container images and bug fixes included in the update are provided by the RHBA-2020:0676 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 4.3.5 container image list

1.7.6.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.3 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

IMPORTANT

If you are upgrading to this release from OpenShift Container Platform 4.2 or OpenShift Container Platform 4.3.3 or earlier, you must restart all Pods after the upgrade is complete.

This is because the service CA is automatically rotated as of OpenShift Container Platform 4.3.5. The service CA is rotated during the upgrade and a restart is required afterward to ensure that all services are using the new service CA before the previous service CA expires.

After this one-time manual restart, subsequent upgrades and rotations will ensure restart before the service CA expires without requiring manual intervention.

1.7.7. RHSA-2020:0679 - Moderate: OpenShift Container Platform 4.3 Security Update

Issued: 2020-03-10

An update for skopeo is now available for OpenShift Container Platform 4.3. Details of the update are documented in the RHSA-2020:0679 advisory.

1.7.8. RHSA-2020:0680 - Low: OpenShift Container Platform 4.3 Security Update

Issued: 2020-03-10

An update for podman is now available for OpenShift Container Platform 4.3. Details of the update are documented in the RHSA-2020:0680 advisory.

1.7.9. RHSA-2020:0681 - Moderate: OpenShift Container Platform 4.3 Security Update

Issued: 2020-03-10

An update for openshift-enterprise-apb-base-container, openshift-enterprise-mariadb-apb, openshift-enterprise-mysql-apb, and openshift-enterprise-postgresql-apb is now available for OpenShift Container Platform 4.3. Details of the update are documented in the RHSA-2020:0681 advisory.

1.7.10. RHSA-2020:0683 - Moderate: OpenShift Container Platform 4.3 Security Update

Issued: 2020-03-10

An update for openshift-enterprise-ansible-operator-container is now available for OpenShift Container Platform 4.3. Details of the update are documented in the RHSA-2020:0683 advisory.

1.7.11. RHBA-2020:0857 - OpenShift Container Platform 4.3.8 Bug Fix Update

Issued: 2020-03-24

OpenShift Container Platform release 4.3.8 is now available. The list of packages included in the update are documented in the RHBA-2020:0857 advisory. The container images and bug fixes included in the update are provided by the RHBA-2020:0858 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 4.3.8 container image list

1.7.11.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.3 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

IMPORTANT

If you are upgrading to this release from OpenShift Container Platform 4.2 or OpenShift Container Platform 4.3.3 or earlier, you must restart all Pods after the upgrade is complete.

This is because the service CA is automatically rotated as of OpenShift Container Platform 4.3.5. The service CA is rotated during the upgrade and a restart is required afterward to ensure that all services are using the new service CA before the previous service CA expires.

After this one-time manual restart, subsequent upgrades and rotations will ensure restart before the service CA expires without requiring manual intervention.

1.7.12. RHSA-2020:0863 - Moderate: OpenShift Container Platform 4.3 Security Update

Issued: 2020-03-24

An update for openshift-enterprise-builder-container and openshift-enterprise-cli-container is now available for OpenShift Container Platform 4.3. Details of the update are documented in the RHSA-2020:0863 advisory.

1.7.13. RHSA-2020:0866 - Moderate: OpenShift Container Platform 4.3 Security Update

Issued: 2020-03-24

An update for openshift-enterprise-template-service-broker-operator-container is now available for OpenShift Container Platform 4.3. Details of the update are documented in the RHSA-2020:0866 advisory.

1.7.14. RHSA-2020:0928 - Moderate: OpenShift Container Platform 4.3 Security Update

Issued: 2020-03-24

An update for openshift-clients is now available for OpenShift Container Platform 4.3. Details of the update are documented in the RHSA-2020:0928 advisory.

1.7.15. RHBA-2020:0929 - OpenShift Container Platform 4.3.9 Bug Fix Update

Issued: 2020-04-01

OpenShift Container Platform release 4.3.9 is now available. The list of packages included in the update are documented in the RHBA-2020:0929 advisory. The container images and bug fixes included in the update are provided by the RHBA-2020:0930 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 4.3.9 container image list

1.7.15.1. Upgrading

To upgrade an existing OpenShift Container Platform 4.3 cluster to this latest release, see Updating a cluster by using the CLI for instructions.

IMPORTANT

If you are upgrading to this release from OpenShift Container Platform 4.2 or OpenShift Container Platform 4.3.3 or earlier, you must restart all Pods after the upgrade is complete.

This is because the service CA is automatically rotated as of OpenShift Container Platform 4.3.5. The service CA is rotated during the upgrade and a restart is required afterward to ensure that all services are using the new service CA before the previous service CA expires.

After this one-time manual restart, subsequent upgrades and rotations will ensure restart before the service CA expires without requiring manual intervention.

1.7.16. RHSA-2020:0933 - Moderate: OpenShift Container Platform 4.3 Security Update

Issued: 2020-04-01

An update for ose-openshift-apiserver-container is now available for OpenShift Container Platform 4.3. Details of the update are documented in the RHSA-2020:0933 advisory.

1.7.17. RHSA-2020:0934 - Moderate: OpenShift Container Platform 4.3 Security Update

Issued: 2020-04-01

An update for ose-openshift-controller-manager-container is now available for OpenShift Container Platform 4.3. Details of the update are documented in the RHSA-2020:0934 advisory.

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, released 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 4.3 cluster, all masters must be 4.3 and all nodes must be 4.3. If you installed an earlier version of **oc**, you cannot use it to complete all of the commands in OpenShift Container Platform 4.3. 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 (4.1 to 4.2 to 4.3, for example) to allow older **oc** to update. Using new capabilities may require newer **oc**. A 4.3 server may have additional capabilities that a 4.2 **oc** cannot use and a 4.3 **oc** may have additional capabilities that are not supported by a 4.2 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.