OpenShift Container Platform 4.13

Release notes

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

Last Updated: 2023-10-13

OpenShift Container Platform 4.13 Release notes

Highlights of what is new and what has changed with this 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 4.13 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 (RHEL) and Kubernetes, OpenShift Container Platform provides a more secure and scalable multitenant 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

OpenShift Container Platform (RHSA-2023:1326) is now available. This release uses Kubernetes 1.26 with CRI-O runtime. New features, changes, and known issues that pertain to OpenShift Container Platform 4.13 are included in this topic.

OpenShift Container Platform 4.13 clusters are available at https://console.redhat.com/openshift. With the Red Hat OpenShift Cluster Manager application for OpenShift Container Platform, you can deploy OpenShift Container Platform clusters to either on-premises or cloud environments.

OpenShift Container Platform 4.13 is based on Red Hat Enterprise Linux (RHEL) 9.2. RHEL 9.2 has not yet been submitted for FIPS validation. Red Hat expects, though cannot commit to a specific timeframe, to obtain FIPS validation for RHEL 9.0 and RHEL 9.2 modules, and later even minor releases of RHEL 9.x. Updates will be available in Compliance Activities and Government Standards.

OpenShift Container Platform 4.13 is supported on Red Hat Enterprise Linux (RHEL) 8.6, 8.7, and 8.8 as well as on Red Hat Enterprise Linux CoreOS (RHCOS) 4.13.

You must use RHCOS machines for the control plane, and you can use either RHCOS or RHEL for compute machines.

1.2. OPENSHIFT CONTAINER PLATFORM LAYERED AND DEPENDENT COMPONENT SUPPORT AND COMPATIBILITY

The scope of support for layered and dependent components of OpenShift Container Platform changes independently of the OpenShift Container Platform version. To determine the current support status and compatibility for an add-on, refer to its release notes. For more information, see the Red Hat OpenShift Container Platform Life Cycle Policy.

1.3. NEW FEATURES AND ENHANCEMENTS

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

1.3.1. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.1.1. RHCOS now uses RHEL 9.2

RHCOS now uses Red Hat Enterprise Linux (RHEL) 9.2 packages in OpenShift Container Platform 4.13. This enables you to have the latest fixes, features, and enhancements, as well as the latest hardware support and driver updates.

1.3.1.1.1. Considerations for upgrading to OpenShift Container Platform with RHEL 9.2

With this release, OpenShift Container Platform 4.13 introduces a RHEL 9.2 based RHCOS and there are some considerations you must make before upgrading:

- Some component configuration options and services might have changed between RHEL 8.6 and RHEL 9.2, which means existing machine configuration files might no longer be valid.
- RHEL 6 base image containers are not supported on RHCOS container hosts, but are supported on RHEL 8 worker nodes. For more information, see the Red Hat Container Compatibility matrix.
- Some device drivers have been deprecated, see the RHEL documentation for more information.

1.3.1.2. IBM Power Virtual Server using installer-provisioned infrastructure (Technology Preview)

Installer-provisioned Infrastructure (IPI) provides a full-stack installation and setup of OpenShift Container Platform.

For more information, see Preparing to install on IBM Power Virtual Server .

1.3.1.3. IBM Secure Execution on IBM Z and IBM(R) LinuxONE

This feature was introduced as a Technology Preview in OpenShift Container Platform 4.12 and is now generally available in OpenShift Container Platform 4.13. IBM Secure Execution is a hardware enhancement that protects memory boundaries for KVM guests. IBM Secure Execution provides the highest level of isolation and security for cluster workloads, and you can enable it by using an IBM Secure Execution-ready QCOW2 boot image.

To use IBM Secure Execution, you must have host keys for your host machine(s) and they must be specified in your Ignition configuration file. IBM Secure Execution automatically encrypts your boot volumes using LUKS encryption.

For more information, see Installing RHCOS using IBM Secure Execution .

1.3.1.4. Assisted Installer SaaS provides platform integration support for IBM Power, IBM Z, and IBM(R) LinuxONE

Assisted Installer SaaS on console.redhat.com supports installation of OpenShift Container Platform on the IBM Power, IBM Z, and IBM® LinuxONE platforms using either the Assisted Installer user interface or the REST API. Integration enables users to manage their infrastructure from a single interface. There are a few additional installation steps to enable IBM Power, IBM Z, and IBM® LinuxONE integration with Assisted Installer SaaS.

For more information, see Installing an on-premise cluster using the Assisted Installer .

1.3.1.5. RHCOS now includes lsof

OpenShift Container Platform 4.13 now includes the **lsof** command in RHCOS.

1.3.2. Installation and update

1.3.2.1. Support for VMware vSphere version 8.0

OpenShift Container Platform 4.13 supports VMware vSphere version 8.0. You can continue to install an OpenShift Container Platform cluster on VMware vSphere version 7.0 Update 2.

1.3.2.2. VMware vSphere region and zone enablement

You can deploy an OpenShift Container Platform cluster to multiple vSphere datacenters or regions that run in a single VMware vCenter. Each datacenter can run multiple clusters or zones. This configuration reduces the risk of a hardware failure or network outage causing your cluster to fail.

IMPORTANT

The VMware vSphere region and zone enablement feature is only available with a newly installed cluster, because this feature requires the vSphere Container Storage Interface (CSI) driver as the default storage driver in the cluster.

A cluster that was upgraded from a previous release defaults to using the in-tree vSphere driver. As a result, you must enable CSI automatic migration for the cluster to use this feature. You can then configure multiple regions and zones for the upgraded cluster.

For more information, see VMware vSphere region and zone enablement .

1.3.2.3. Changes to the default vSphere install-config.yaml file

After you run the installation program for OpenShift Container Platform on vSphere, the default **install-config.yaml** file now includes **vcenters** and **failureDomains** fields, so that you can choose to specify multiple datacenters, region, and zone information for your cluster. You can leave these fields blank if you want to install an OpenShift Container Platform cluster in a vSphere environment that consists of single datacenter running in a VMware vCenter.

For more information, see Configuring regions and zones for a VMware vCenter .

1.3.2.4. External load balancers that support multiple vSphere subnets

You can configure an OpenShift Container Platform cluster to use an external load balancer that supports multiple subnets. If you use multiple subnets, you can explicitly list all the IP addresses in any networks that are used by your load balancer targets. This configuration can reduce maintenance overhead because you can create and destroy nodes within those networks without reconfiguring the load balancer targets.

For more information, see Configuring an external load balancer .

1.3.2.5. Support for encrypting a VM before installing a cluster on VMware vSphere

For OpenShift Container Platform 4.13, you can encrypt your virtual machines before you install a cluster on VMware vSphere with user-provisioned infrastructure.

For more information, see Requirements for encrypting virtual machines

1.3.2.6. Three-node cluster support

Beginning with OpenShift Container Platform 4.13, deploying a three-node cluster is supported on Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and VMware vSphere.

This type of OpenShift Container Platform cluster is a smaller, more resource efficient cluster, as it consists of only three control plane machines, which also act as compute machines.

For more information, see Installing a three-node cluster on AWS , Installing a three-node cluster on Azure, Installing a three-node cluster on GCP , and Installing a three-node cluster on vSphere .

1.3.2.7. IBM Cloud VPC and existing VPC resources

If you are deploying an OpenShift Container Platform cluster to an existing virtual private cloud (VPC), you can now use the **networkResourceGroupName** parameter to specify the name of the resource group that contains these existing resources. This enhancement lets you keep the existing VPC resources and subnets separate from the cluster resources that the installation program provisions. You can then use the **resourceGroupName** parameter to specify the name of an existing resource group that the installation program can use to deploy all of the installer-provisioned cluster resources. If **resourceGroupName** is undefined, a new resource group is created for the cluster.

For more information, see Additional IBM Cloud VPC configuration parameters .

1.3.2.8. Minimum required permissions for GCP to install and delete an OpenShift Container Platform cluster

In OpenShift Container Platform 4.13, instead of using the predefined roles, you can now define your custom roles to include the minimum required permissions for Google Cloud Platform (GCP) to install and delete an OpenShift Container Platform cluster. These permissions are available for installer-provisioned infrastructure and user-provisioned infrastructure.

1.3.2.9. User-defined tags for Azure

In OpenShift Container Platform 4.13, you can configure the tags in Azure for grouping resources and for managing resource access and cost. Support for tags is available only for the resources created in the Azure Public Cloud, and in OpenShift Container Platform 4.13 as a Technology Preview (TP). You can define the tags on the Azure resources in the **install-config.yaml** file only during OpenShift Container Platform cluster creation.

1.3.2.10. Installing an OpenShift Container Platform cluster on GCP into a shared Virtual Private Cloud (VPC)

In OpenShift Container Platform 4.13, you can install a cluster into a shared Virtual Private Cloud (VPC) on Google Cloud Platform (GCP). This installation method configures the cluster to share a VPC with another GCP project. A shared VPC enables an organization to connect resources from multiple projects over a common VPC network. A common VPC network can increase the security and efficiency of organizational communications by using internal IP addresses.

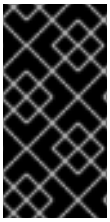
For more information, see Installing a cluster on GCP into a shared VPC .

1.3.2.11. Installing a cluster on GCP using Shielded VMs

In OpenShift Container Platform 4.13, you can use Shielded VMs when installing your cluster. Shielded VMs have extra security features including secure boot, firmware and integrity monitoring, and rootkit detection. For more information, see Enabling Shielded VMs and Google's documentation on Shielded VMs.

1.3.2.12. Installing a cluster on GCP using Confidential VMs

In OpenShift Container Platform 4.13, you can use Confidential VMs when installing your cluster. Confidential VMs encrypt data while it is being processed. For more information, see Google's documentation about Confidential Computing. You can enable Confidential VMs and Shielded VMs at the same time, although they are not dependent on each other.



IMPORTANT

Due to a known issue in OpenShift Container Platform 4.13.3 and earlier versions, you cannot use persistent volume storage on a cluster with Confidential VMs on Google Cloud Platform (GCP). This issue was resolved in OpenShift Container Platform 4.13.4. For more information, see OCPBUGS-11768.

1.3.2.13. Installing a cluster on AWS into an existing Virtual Private Cloud (VPC) improvements

In OpenShift Container Platform 4.13, the installation process for clusters that use AWS VPCs is simplified. This release also introduces the *edge pool*, a pool of machines that are optimized for AWS Local Zones.

For more information, see Installing a cluster using AWS Local Zones .

1.3.2.14. Required administrator acknowledgment when upgrading from OpenShift Container Platform 4.12 to 4.13

OpenShift Container Platform 4.13 uses Kubernetes 1.26, which removed several deprecated APIs.

A cluster administrator must provide a manual acknowledgment before the cluster can be upgraded from OpenShift Container Platform 4.12 to 4.13. This is to help prevent issues after upgrading to OpenShift Container Platform 4.13, where APIs that have been removed are still in use by workloads, tools, or other components running on or interacting with the cluster. Administrators must evaluate their cluster for any APIs in use that will be removed and migrate the affected components to use the appropriate new API version. After this is done, the administrator can provide the administrator acknowledgment.

All OpenShift Container Platform 4.12 clusters require this administrator acknowledgment before they can be upgraded to OpenShift Container Platform 4.13.

For more information, see Preparing to update to OpenShift Container Platform 4.13 .

1.3.2.15. Minimum required permissions for Microsoft Azure to install and delete an OpenShift Container Platform cluster

In OpenShift Container Platform 4.13, instead of using the built-in roles, you can now define your custom roles to include the minimum required permissions for Microsoft Azure to install and delete an OpenShift Container Platform cluster. These permissions are available for installer-provisioned infrastructure and user-provisioned infrastructure.

1.3.2.16. Single-architecture to multi-architecture payload migration

OpenShift Container Platform 4.13 introduces the **oc adm upgrade --to-multi-arch** command, which lets you migrate a cluster with single-architecture compute machines to a cluster with multi-architecture compute machines. By updating to a multi-architecture, manifest-listed payload, you can add mixed architecture compute machines to your cluster.

1.3.2.17. Configuring network components to run on the control plane in vSphere

If you need the virtual IP (VIP) addresses to run on the control plane nodes in a vSphere installation, you must configure the **ingressVIP** addresses to run exclusively on the control plane nodes. By default, OpenShift Container Platform allows any node in the worker machine configuration pool to host the **ingressVIP** addresses. Because vSphere environments deploy worker nodes in separate subnets from the control plane nodes, configuring the **ingressVIP** addresses to run exclusively on the control plane nodes prevents issues from arising due to deploying worker nodes in separate subnets. For additional details, see Configuring network components to run on the control plane in vSphere .

1.3.2.18. Installing an OpenShift Container Platform cluster on AWS with a single node

In OpenShift Container Platform 4.13, you can install a cluster with a single node on Amazon Web Services (AWS). Installing on a single node increases the resource requirements for the node. For additional details, see Installing a cluster on a single node .

1.3.2.19. Scale bare metal hosts in a user-provisioned cluster by using the Bare Metal Operator

With OpenShift Container Platform 4.13, you can scale bare metal hosts in an existing user-provisioned infrastructure cluster by using the Bare Metal Operator (BMO) and other metal^3 components. By using the Bare Metal Operator in a user-provisioned cluster, you can simplify and automate the management and scaling of hosts.

Using the BMO, you can add or remove hosts by configuring a **BareMetalHost** object. You can also keep track of existing hosts by enrolling them as **externallyProvisioned** in the **BareMetalHost** object inventory.

NOTE

You cannot use a provisioning network to scale user-provisioned infrastructure clusters by using the Bare Metal Operator. Because this workflow does not support a provisioning network, you can only use bare-metal host drivers that support virtual media network booting, for example **redfish-virtualmedia** and **idrac-virtualmedia**.

For more information about scaling a user-provisioned cluster by using the BMO, see Scaling a user-provisioned cluster with the Bare Metal Operator.

1.3.2.20. OpenShift Container Platform on 64-bit ARM

OpenShift Container Platform 4.13 is now supported on 64-bit ARM architecture-based Azure user-provisioned installations. The Agent based installation program is also now supported on 64-bit ARM systems. For more information about instance availability and installation documentation, see Supported installation methods for different platforms.

1.3.2.21. Support for the git-lfs package

The OpenShift Jenkins image now supports the **git-lfs** package. With this package, you can use artifacts larger than 200 megabytes (MB) in your OpenShift Jenkins image.

1.3.2.22. Using the oc-mirror plugin to include local OCI Operator catalogs is now generally available

You can now use the oc-mirror plugin to mirror local OCI Operator catalogs on disk to a mirror registry. This feature was previously introduced as a Technology Preview in OpenShift Container Platform 4.12 and is now generally available in OpenShift Container Platform 4.13.

This release introduces support for the following features when local OCI catalogs are included:

- Pruning images from the target mirror registry
- Incremental mirroring to only mirror what has changed since the last time you ran the tool
- Namespace hierarchy for alternative names for catalogs in the target mirror registry

IMPORTANT

- If you used the Technology Preview OCI local catalogs feature for the oc-mirror plugin for OpenShift Container Platform 4.12, you can no longer use the OCI feature of the oc-mirror plugin to copy a catalog locally and convert it to OCI format as a first step to mirroring to a fully disconnected cluster.
- When mirroring local OCI catalogs, any OpenShift Container Platform releases or additional images that you want to mirror along with the local OCI-formatted catalog must be pulled from a registry. You cannot mirror OCI catalogs along with an oc-mirror image set file on disk.
- The **--use-oci-feature** flag has been deprecated. Use the **--include-local-oci-catalogs** flag instead to enable mirroring of local OCI catalogs.

For more information, see Including local OCI Operator catalogs .

1.3.2.23. Deploy clusters that use failure domains on RHOSP (Technology Preview)

You can now deploy clusters that span multiple failure domains on RHOSP. For deployments at scale, failure domains improve resilience and performance.

For more information, see RHOSP parameters for failure domains.

1.3.2.24. Deploy clusters with user-managed load balancers on RHOSP (Technology Preview)

You can now deploy clusters on RHOSP with user-managed load balancers rather than the default, internal load balancer.

For more information, see Installation configuration for a cluster on OpenStack with a user-managed load balancer.

1.3.2.25. Using projects and categories when installing a cluster on Nutanix

In OpenShift Container Platform 4.13, you can use projects and categories to organize compute plane virtual machines in a cluster installed on Nutanix. Projects define logical groups of user roles for managing permissions, networks, and other parameters. You can use categories to apply policies to groups of virtual machines based on shared characteristics.

For more information, see Installing a cluster on Nutanix .

1.3.2.26. Agent-based Installer now performs network connectivity checks

For installations of OpenShift Container Platform 4.13 using the Agent-based Installer, a console application (with a textual user interface) performs a pull check early in the installation process to verify that the current host can retrieve the configured release image. The console application supports troubleshooting issues by allowing users to directly modify network configurations.

For more information, see Verifying that the current installation host can pull release images .

1.3.3. Post-installation configuration

1.3.3.1. OpenShift Container Platform clusters with multi-architecture compute machines

OpenShift Container Platform 4.13 clusters with multi-architecture compute machines is now generally available. As a Day 2 operation, you can now create a cluster with compute nodes of different architectures on AWS and Azure installer provisioned infrastructures. User-provisioned installation on bare metal are in Technology Preview. For more information on creating a cluster with multi-architecture compute machines, see Configuring multi-architecture compute machines on an OpenShift Container Platform cluster.

1.3.3.2. Specifying multiple failure domains for your cluster on VSphere

As an administrator, you can specify multiple failure domains for your OpenShift Container Platform cluster that runs on a VMware VSphere instance. This means that you can distribute key control planes and workload elements among varied hardware resources for a datacenter. Additionally, you can configure your cluster to use a multiple layer 2 network configuration, so that data transfer among nodes can span across multiple networks.

For more information, see Specifying multiple failure domains for your cluster on VSphere .

1.3.4. Web console

1.3.4.1. Developer Perspective

With this release, you can now perform the following actions in the **Developer** perspective of the web console:

- Create a **Serverless Function** by using the **Import from Git** flow.
- Create a **Serverless Function** by using the **Create Serverless Function** flow available on **Add page**.
- Select **pipeline-as-code** as an option in the **Import from Git** workflow.
- View which pods are receiving traffic in the following locations in the user interface:
  - The side pane of the **Topology** view
  - The **Details** view for a pod
  - The **Pods** list view
- Customize the timeout period or provide your own image when instantiating a **Web Terminal**.
- As an administrator, set default resources to be pre-pinned in the **Developer** perspective navigation for all users.

1.3.4.1.1. Pipelines page improvements

In OpenShift Container Platform 4.13, you can see the following navigation improvements on the **Pipelines** page:

- The tab you previously selected remains visible when you return to the **Pipelines** page.
- The default tab for the **Repository details** page is now **PipelinesRuns**, but when you are following the **Create Git Repository** flow, the default tab is **Details**.

1.3.4.1.2. Helm page improvements

In OpenShift Container Platform 4.13, the **Helm** page now contains the following new and updated features:

- The terminology used on the page now refers to creating and deleting Helm releases rather than installing and uninstalling Helm charts.
- You can create and delete Helm releases asynchronously and not wait for actions to complete before performing the next task in the web console.
- The Helm release list now includes a **Status** column.

1.3.5. OpenShift CLI (oc)

1.3.5.1. New flag added to run must-gather in a specified namespace

With OpenShift Container Platform 4.13, the **--run-namespace** flag is now available for the **oc adm must-gather** command. You can use this flag to specify an existing namespace to run the must-gather tool in.

For more information, see About the must-gather tool.

1.3.5.2. Importing manifests with the OpenShift CLI (oc)

With OpenShift Container Platform 4.13, a new **oc** command line interface (CLI) flag, **--import-mode**, has been added to the following **oc** commands:

- **oc import-image**
- **oc tag**

With this enhancement, users can set the **--import-mode** flag to **Legacy** or **PreserveOriginal**, which provides users the option to import a single sub-manifest, or all manifests, of a manifest list when running the **oc import-image** or **oc tag** commands.

For more information, see Working with manifest lists.

1.3.5.3. Returning os/arch and digests of an image

With OpenShift Container Platform 4.13, running **oc describe** on an image now returns os/arch and digests of each manifest.

1.3.6. IBM Z and IBM(R) LinuxONE

With this release, IBM Z and IBM® LinuxONE are now compatible with OpenShift Container Platform 4.13. The installation can be performed with z/VM or Red Hat Enterprise Linux (RHEL) Kernel-based Virtual Machine (KVM). For installation instructions, see the following documentation:

- Installing a cluster with z/VM on IBM Z and IBM® LinuxONE
- Installing a cluster with z/VM on IBM Z and IBM® LinuxONE in a restricted network
- Installing a cluster with RHEL KVM on IBM Z and IBM® LinuxONE
- Installing a cluster with RHEL KVM on IBM Z and IBM® LinuxONE in a restricted network

IMPORTANT

Compute nodes must run Red Hat Enterprise Linux CoreOS (RHCOS)

IBM Z and IBM(R) LinuxONE notable enhancements
The IBM Z and IBM® LinuxONE release on OpenShift Container Platform 4.13 adds improvements and new capabilities to OpenShift Container Platform components and concepts.

This release introduces support for the following features on IBM Z and IBM® LinuxONE:

- Assisted Installer
- Cluster Resource Override Operator
- Egress IP
- MetalLB Operator
- Network-Bound Disk Encryption - External Tang Server

IBM Secure Execution
OpenShift Container Platform now supports configuring Red Hat Enterprise Linux CoreOS (RHCOS) nodes for IBM Secure Execution on IBM Z and IBM® LinuxONE (s390x architecture).

For installation instructions, see the following documentation:

- Installing RHCOS using IBM Secure Execution

1.3.7. IBM Power

With this release, IBM Power is now compatible with OpenShift Container Platform 4.13. For installation instructions, see the following documentation:

- Installing a cluster on IBM Power
- Installing a cluster on IBM Power in a restricted network

IMPORTANT

Compute nodes must run Red Hat Enterprise Linux CoreOS (RHCOS)

IBM Power notable enhancements

The IBM Power release on OpenShift Container Platform 4.13 adds improvements and new capabilities to OpenShift Container Platform components and concepts.

This release introduces support for the following features on IBM Power:

- Assisted Installer
- Cluster Resource Override Operator
- IBM Power Virtual Server Block CSI Driver Operator (Technology Preview)
- Egress IP
- Installer-provisioned Infrastructure Enablement for IBM Power Virtual Server (Technology Preview)
- MetalLB Operator
- Network-Bound Disk Encryption - External Tang Server

IBM Power,IBM Z, and IBM(R) LinuxONE support matrix

Table 1.1. OpenShift Container Platform features

Feature	IBM Power	IBM Z and IBM® LinuxONE
Alternate authentication providers	Supported	Supported
Assisted Installer	Supported	Supported
Automatic Device Discovery with Local Storage Operator	Unsupported	Supported
Automatic repair of damaged machines with machine health checking	Unsupported	Unsupported
Cloud controller manager for IBM Cloud	Supported	Unsupported
Controlling overcommit and managing container density on nodes	Unsupported	Unsupported
Cron jobs	Supported	Supported
Descheduler	Supported	Supported
Egress IP	Supported	Supported
Encrypting data stored in etcd	Supported	Supported
Helm	Supported	Supported
Horizontal pod autoscaling	Supported	Supported

Feature	IBM Power	IBM Z and IBM® LinuxONE
IPv6	Supported	Supported
Monitoring for user-defined projects	Supported	Supported
Multipathing	Supported	Supported
Network-Bound Disk Encryption - External Tang Server	Supported	Supported
Non–volatile memory express drives (NVMe)	Supported	Unsupported
OpenShift CLI (**oc**) plugins	Supported	Supported
Operator API	Supported	Supported
OpenShift Virtualization	Unsupported	Unsupported
OVN-Kubernetes, including IPsec encryption	Supported	Supported
PodDisruptionBudget	Supported	Supported
Precision Time Protocol (PTP) hardware	Unsupported	Unsupported
Red Hat OpenShift Local	Unsupported	Unsupported
Scheduler profiles	Supported	Supported
Stream Control Transmission Protocol (SCTP)	Supported	Supported
Support for multiple network interfaces	Supported	Supported
Three-node cluster support	Supported	Supported
Topology Manager	Supported	Unsupported
z/VM Emulated FBA devices on SCSI disks	Unsupported	Supported
4K FCP block device	Supported	Supported

Table 1.2. Persistent storage options

Feature	IBM Power	IBM Z and IBM® LinuxONE
Persistent storage using iSCSI	Supported [1]	Supported [1],[2]
Persistent storage using local volumes (LSO)	Supported [1]	Supported [1],[2]
Persistent storage using hostPath	Supported [1]	Supported [1],[2]
Persistent storage using Fibre Channel	Supported [1]	Supported [1],[2]
Persistent storage using Raw Block	Supported [1]	Supported [1],[2]
Persistent storage using EDEV/FBA	Supported [1]	Supported [1],[2]

1. Persistent shared storage must be provisioned by using either Red Hat OpenShift Data Foundation or other supported storage protocols.
2. Persistent non-shared storage must be provisioned using local storage, like iSCSI, FC, or using LSO with DASD, FCP, or EDEV/FBA.

Table 1.3. Operators

Feature	IBM Power	IBM Z and IBM® LinuxONE
Cluster Logging Operator	Supported	Supported
Cluster Resource Override Operator	Supported	Supported
Compliance Operator	Supported	Supported
File Integrity Operator	Supported	Supported
Local Storage Operator	Supported	Supported
MetalLB Operator	Supported	Supported
NFD Operator	Supported	Supported
NMState Operator	Supported	Supported
OpenShift Elasticsearch Operator	Supported	Supported
Service Binding Operator	Supported	Supported

Feature	IBM Power	IBM Z and IBM® LinuxONE
Vertical Pod Autoscaler Operator	Supported	Supported

Table 1.4. Multus CNI plugins

Feature	IBM Power	IBM Z and IBM® LinuxONE
Bridge	Supported	Supported
Host-device	Supported	Supported
IPAM	Supported	Supported
IPVLAN	Supported	Supported

Table 1.5. CSI Volumes

Feature	IBM Power	IBM Z and IBM® LinuxONE
Cloning	Supported	Supported
Expansion	Supported	Supported
Snapshot	Supported	Supported

1.3.8. Images

1.3.8.1. Support for manifest listed images on image streams

With OpenShift Container Platform 4.13, support for manifest listed images on image streams is now generally available.

1.3.9. Security and compliance

1.3.9.1. AES-GCM encryption is now supported

The AES-GCM encryption type is now supported when enabling etcd encryption for OpenShift Container Platform. Encryption keys for the AES-GCM encryption type are rotated weekly.

For more information, see Supported encryption types.

1.3.10. Networking

1.3.10.1. Enhancements to networking metrics

1.3.10.1.1. egress_ips_rebalance_total

- Metric name: **ovnkube_master_egress_ips_rebalance_total**
- Help message: **The total number of times assigned egress IP(s) needed to be moved to a different node.**

1.3.10.1.2. egress_ips_node_unreachable_total

- Metric name: **ovnkube_master_egress_ips_node_unreachable_total**
- Help message: **The total number of times assigned egress IP(s) were unreachable.**

1.3.10.1.3. egress_ips_unassign_latency_seconds

- Metric name: **ovnkube_master_egress_ips_unassign_latency_seconds**
- Help message: **The latency of egress IP unassignment from OVN northbound database.**

1.3.10.1.4. interfaces_total

- Metric name: **ovs_vswitchd_interfaces_total**
- Help message: **The total number of Open vSwitch interface(s) created for pods** and **Open vSwitch interface until its available.**

1.3.10.1.5. interface_up_wait_seconds_total

- Metric name: **ovs_vswitchd_interface_up_wait_seconds_total**
- Help message: **The total number of seconds that is required to wait for pod.** and **Open vSwitch interface until its available.**

1.3.10.1.6. ovnkube_resource_retry_failures_total

- Metric name: **ovnkube_resource_retry_failures_total**
- Help message: **The total number of times processing a Kubernetes resource reached the maximum retry limit and was no longer processed.**

1.3.10.2. Enhancements to networking alerts

- OVN Kubernetes retries a claim up to 15 times before dropping it. With this update, if this failure happens, OpenShift Container Platform alerts the cluster administrator. A description of each alert can be viewed in the console.

1.3.10.2.1. NoOvnMasterLeader

- Summary: There is no ovn-kubernetes master leader.
- Description in console:

> Networking control plane is degraded. Networking configuration updates applied to the cluster will not be implemented while there is no OVN Kubernetes leader. Existing workloads should continue to have connectivity. OVN-Kubernetes control plane is not functional.

1.3.10.2.2. OVNKubernetesNodeOVSOverflowUserspace

- Summary: OVS vSwitch daemon drops packets due to buffer overflow.
- Description in console:

> Netlink messages dropped by OVS vSwitch daemon due to netlink socket buffer overflow. This will result in packet loss.

1.3.10.2.3. OVNKubernetesNodeOVSOverflowKernel

- Summary: OVS kernel module drops packets due to buffer overflow.
- Description in console:

> Netlink messages dropped by OVS kernel module due to netlink socket buffer overflow. This will result in packet loss.

1.3.10.3. Network Observability Operator

The Network Observability Operator releases updates independently from the OpenShift Container Platform minor version release stream. Updates are available through a single, rolling stream which is supported on all currently supported versions of OpenShift Container Platform 4. Information regarding new features, enhancements, and bug fixes for the Network Observability Operator can be found in the Network Observability release notes.

1.3.10.4. Assign IP addresses in MetalLB IPAddressPool resources to specific namespaces and services

With this update, you can assign IP addresses from a MetalLB **IPAddressPool** resource to services, namespaces, or both. This is useful in a muti-tenant, bare-metal environment that requires MetalLB to pin IP addresses from an IP address pool to specific services and namespaces. You can assign IP addresses from many IP address pools to services and namespaces. You can then define the prioritization for these IP address pools so that MetalLB assigns IP addresses starting from the higher priority IP address pool.

For more information about assigning IP addresses from an IP address pool to services and namespaces, see Configuring MetalLB address pools.

1.3.10.5. Supporting OpenShift Container Platform installation on nodes with dual-port NICs (Technology Preview)

With this update, OpenShift Container Platform cluster can be deployed on a bond interface with 2 virtual function (VFs) on 2 physical functions (PFs) using the following methods:

- Agent-based installer
- Installer-provisioned infrastructure installation

- User-provisioned infrastructure installation

For more information about installing OpenShift Container Platform on nodes with dual-port NICs, see NIC partitioning for SR-IOV devices .

1.3.10.6. Support for switching the BlueField-2 network device from data processing unit (DPU) mode to network interface controller (NIC) mode is now GA

In this release, switching the BlueField-2 network device from data processing unit (DPU) mode to network interface controller (NIC) mode is now generally available.

For more information, see Switching BlueField-2 from DPU to NIC .

1.3.10.7. Hardware offload for the MT2892 Family [ConnectX-6 Dx] of network cards is GA

OpenShift Container Platform 4.13 adds OvS Hardware Offload support for the MT2892 Family [ConnectX-6 Dx] of network cards.

For more information, see Supported devices.

1.3.10.8. Migrating to the OpenShift SDN network plugin

If you are using the OVN-Kubernetes network plugin, you can migrate to the OpenShift SDN network plugin.

For more information, see Migrating to the OpenShift SDN network plugin .

1.3.10.9. CoreDNS updated to 1.10.1

OpenShift Container Platform 4.13 updates CoreDNS to 1.10.1. CoreDNS now uses the DNSSEC DO Bit that was specified on the originating client query. This reduces the DNS response UDP packet size when a client is not requesting DNSSEC. Consequently, the smaller packet size reduces both the chance of DNS truncation decreasing by TCP connection retries and overall DNS bandwidth.

1.3.10.10. Expand cluster network IP address range

The cluster network can be expanded to support the addition of nodes to the cluster. For example, if you deployed a cluster and specified **10.128.0.0/19** as the cluster network range and a host prefix of **23**, you are limited to 16 nodes. You can expand that to 510 nodes by changing the CIDR mask on a cluster to /**14**. For more information, see Configuring the cluster network range.

1.3.10.11. Dual-stack IPv4/IPv6 on VMware vSphere clusters

On installer-provisioned vSphere clusters, you can use dual-stack networking with IPv4 as the primary IP family, and IPv6 as the secondary address family. For more information, see Network configuration parameters.

1.3.10.12. IPv6 as primary IP address family on bare metal dual-stack clusters

During cluster installation on bare metal, you can configure IPv6 as the primary IP address family on a dual-stack cluster. To enable this feature when installing a new cluster, specify an IPv6 address family before an IPv4 address family for the machine network, cluster network, service network, API VIPs, and ingress VIPs.

For more information, refer to the following sources:

- Installer-provisioned infrastructure: Deploying with dual-stack networking
- User-provisioned infrastructure: Network configuration parameters

1.3.10.13. OVN-Kubernetes is available as a secondary network (Technology Preview)

With this release, the Red Hat OpenShift Networking OVN-Kubernetes network plug-in allows the configuration of secondary network interfaces for pods. As a secondary network, OVN-Kubernetes supports a layer 2 (switched) topology network. This is available as a Technology Preview feature.

For more information about OVN-Kubernetes as a secondary network, see Configuration for an OVN-Kubernetes additional network.

1.3.10.14. Node selector added to egress firewall for OVN-Kubernetes network plugin

In OpenShift Container Platform 4.13, **nodeSelector** has been added to the egress firewall destination spec in OVN-Kubernetes network plug-in. This feature allows users to add a label to one or multiple nodes and the IP addresses of the selected nodes are included in the associated rule. For more information, see Example nodeSelector for EgressFirewall

1.3.10.15. Kuryr to OVN-Kubernetes migration procedure for clusters that run on RHOSP (Technology Preview)

You can now migrate a cluster that runs on RHOSP and uses Kuryr to OVN-Kubernetes.

For more information, see Migrating from the Kuryr network plugin to the OVN-Kubernetes network plugin.

1.3.10.16. Improved egress IP support for clusters that run on RHOSP

For clusters that run on RHOSP and use OVN-Kubernetes, manually reassigning floating IP addresses for reservation ports is no longer necessary. If a reservation port is removed from one node and recreated on another one, the reassignment now happens automatically.

1.3.10.17. Supported hardware for SR-IOV (Single Root I/O Virtualization)

OpenShift Container Platform 4.13 adds support for the following SR-IOV devices:

- Intel E810-XXVDA4T

For more information, see Supported devices.

1.3.11. Storage

1.3.11.1. Support for customer-managed keys for re-encryption in the KMS

With this update, the default credentials request for AWS has been modified to allow customer-managed keys to be used for re-encryption in the Key Management Service (KMS). For clusters with the Cloud Credential Operator (CCO) configured to use manual mode, administrators must apply those changes manually by adding **kms:ReEncrypt*** permission to their key policy. Other administrators are not impacted by this change. (**OCPBUGS-5410**)

1.3.11.2. Dual-stack support for Logical volume manager storage (LVM Storage)

In OpenShift Container Platform 4.13, LVM Storage is supported in dual-stack for IPv4 and IPv6 network environments. For more information, see Converting to a dual-stack cluster network .

1.3.11.3. Support for LVM Storage in GitOps ZTP

In OpenShift Container Platform 4.13, you can add and configure Logical volume manager storage (LVM Storage) through GitOps ZTP. For more information, see Configuring LVM Storage using PolicyGenTemplate CRs and LVM Storage.

1.3.11.4. Support for LVM Storage in disconnected environments

In OpenShift Container Platform 4.13, you can install LVM Storage in disconnected environments. For more information, see Installing LVM Storage in a disconnected environment .

1.3.11.5. User-managed encryption is generally available

The user-managed encryption feature allows you to provide keys during installation that encrypt OpenShift Container Platform node root volumes, and enables all managed storage classes to use these keys to encrypt provisioned storage volumes. This allows you to encrypt storage volumes with your selected key, instead of the platform's default account key.

This features supports the following storage types:

- Amazon Web Services (AWS) Elastic Block storage (EBS) (for more information, see User-managed encryption)
- Microsoft Azure Disk storage (for more information, see User-managed encryption)
- Google Cloud Platform (GCP) persistent disk (PD) storage (for more information, see User-managed encryption)

1.3.11.6. Detach CSI volumes after non-graceful node shutdown (Technology Preview)

Container Storage Interface (CSI) drivers can now automatically detach volumes when a node goes down non-gracefully. When a non-graceful node shutdown occurs, you can then manually add an out-of-service taint on the node to allow volumes to automatically detach from the node. This feature is supported with Technology Preview status.

For more information, see Detach CSI volumes after non-graceful node shutdown .

1.3.11.7. VMware vSphere encryption support is generally available

You can encrypt virtual machines (VMs) and persistent volumes (PVs) on OpenShift Container Platform running on vSphere.

For more information, see vSphere persistent disks encryption.

1.3.11.8. VMware vSphere CSI topology support for multiple datacenters is generally available

OpenShift Container Platform 4.12 introduced the ability to deploy OpenShift Container Platform for vSphere on different zones and regions, which allows you to deploy over multiple compute clusters, thus helping to avoid a single point of failure. OpenShift Container Platform 4.13 introduces support for

deploying over multiple datacenters and to set up the topology using failure domains created during installation or post-installation.

For more information, see vSphere CSI topology.

1.3.11.9. Creating more than one default storage class is generally available

OpenShift Container Platform 4.13 allows you create more than one default storage class. This feature makes it easier to change the default storage class because you can create a second storage class defined as the default. You then temporarily have two default storage classes before removing default status from the previous default storage class. While it is acceptable to have multiple default storage classes for a short time, you should ensure that eventually only one default storage class exists.

For more information, see Changing the default storage class and Multiple default storage classes.

1.3.11.10. Managing the default storage class is generally available

OpenShift Container Platform 4.13 introduces the **spec.storageClassState** field in the **ClusterCSIDriver** object, which allows you to manage the default storage class generated by OpenShift Container Platform to accomplish several different objectives:

- When you have other preferred storage classes, preventing the storage operator from re-creating the initial default storage class.
- Renaming, or otherwise changing, the default storage class
- Enforcing static provisioning by disabling dynamic provisioning.

For more information, see Managing the default storage class.

1.3.11.11. Retroactive default StorageClass assignment (Technology Preview)

Previously, if there was no default storage class, persistent volumes claims (PVCs) that were created that requested the default storage class remained stranded in the pending state indefinitely, unless you manually delete and recreate them. OpenShift Container Platform can now retroactively assign a default storage class to these PVCs, so that they do not remain in the pending state. With this feature enabled, after a default storage class is created, or one of the existing storage classes is declared the default, these previously stranded PVCs are assigned to the default storage class.

This feature is supported with Technology Preview status.

For more information, see Absent default storage class.

1.3.11.12. IBM Power Virtual Server Block CSI Driver Operator (Technology Preview)

OpenShift Container Platform is capable of provisioning persistent volumes (PVs) by using the Container Storage Interface (CSI) driver for IBM Power Virtual Server Block Storage.

For more information, see IBM Power Virtual Server Block CSI Driver Operator.

1.3.11.13. CSI inline ephemeral volumes is generally available

Container Storage Interface (CSI) inline ephemeral volumes were introduced in OpenShift Container Platform 4.5 as a Technology Preview feature, which allows you to define a pod spec that creates inline ephemeral volumes when a pod is deployed and delete them when a pod is destroyed. This feature is

now generally available.

This feature is only available with supported Container Storage Interface (CSI) drivers.

This feature also includes the CSI Volume Admission plug-in, which provides a mechanism where the use of an individual CSI driver capable of provisioning CSI ephemeral volumes can be restricted on pod admission. Administrators or distributions can add a **csi-ephemeral-volume-profile** label to a **CSIDriver** object, and the label is then inspected by the Admission plug-in and used in enforcement, warning, and audit decisions.

For more information, see CSI inline ephemeral volumes .

1.3.11.14. Automatic CSI migration for Microsoft Azure File is generally available

Starting with OpenShift Container Platform 4.8, automatic migration for in-tree volume plugins to their equivalent Container Storage Interface (CSI) drivers became available as a Technology Preview feature. Support for Azure File was provided in this feature in OpenShift Container Platform 4.10. OpenShift Container Platform 4.13 now supports automatic migration for Azure File as generally available. CSI migration for Azure File is now enabled by default and requires no action by an administrator.

This feature automatically translates in-tree objects to their counterpart CSI representations and should be completely transparent to users. Translated objects are not stored on disk, and user data is not migrated.

Although storage class referencing to the in-tree storage plug-in will continue working, it is recommended that you switch the default storage class to the CSI storage class.

For more information, see CSI Automatic Migration.

1.3.11.15. Automatic CSI migration for VMware vSphere is generally available

Starting with OpenShift Container Platform 4.8, automatic migration for in-tree volume plugins to their equivalent Container Storage Interface (CSI) drivers became available as a Technology Preview feature. Support for vSphere was provided in this feature in OpenShift Container Platform 4.10. OpenShift Container Platform 4.13 now supports automatic migration for vSphere as generally available. CSI migration for vSphere is now enabled by default and requires no action by an administrator.

This feature automatically translates in-tree objects to their counterpart CSI representations and should be completely transparent to users.

Although storage class referencing to the in-tree storage plug-in will continue working, it is recommended that you switch the default storage class to the CSI storage class.

For new installations of OpenShift Container Platform 4.13, or later, automatic migration is enabled by default. However, when upgrading from OpenShift Container Platform 4.12, or earlier, to 4.13, automatic CSI migration for vSphere only occurs if you opt in. Carefully review the indicated consequences before opting in to migration.

For more information, see CSI Automatic Migration.

1.3.11.16. Cross account support for AWS EFS CSI driver is generally available

Cross account support allows you to have an OpenShift Container Platform cluster in one Amazon Web Services (AWS) account and mount your file system in another AWS account using the AWS Elastic File System (EFS) Container Storage Interface (CSI) driver.

For more information, see AWS EFS CSI cross account support .

1.3.11.17. Delegate FSGroup to CSI Driver instead of Kubelet is generally available

This feature allows OpenShift Container Platform to supply a pod's FSGroup to a Container Storage Interface (CSI) driver when a volume is mounted. Microsoft Azure File CSI driver depends on this feature.

1.3.11.18. Azure File supporting NFS is generally available

OpenShift Container Platform 4.13 supports Azure File Container Storage Interface (CSI) Driver Operator with Network File System (NFS) as generally available.

For more information, see NFS support.

1.3.12. Operator lifecycle

1.3.12.1. Finding Operator versions by using the OpenShift CLI

In OpenShift Container Platform 4.13, you can find which versions and channels of an Operator you can install on your system by running the following OpenShift CLI (**oc**) command:

Example oc describe command syntax

```
$ oc describe packagemanifests <operator_name> -n <catalog_namespace>
```

You can specify the output format of an Operator's version and channel information by running the following command:

Example oc get command syntax

```
$ oc get packagemanifests <operator_name> -n <catalog_namespace> -o <output_format>
```

For more information, see Installing a specific version of an Operator .

1.3.12.2. Operators in multitenant clusters

The default behavior for Operator Lifecycle Manager (OLM) aims to provide simplicity during Operator installation. However, this behavior can lack flexibility, especially in multitenant clusters.

Guidance and a recommended solution for Operator management in multitenant clusters has been added with the following topics:

- Operators in multitenant clusters
- Preparing for multiple instances of an Operator for multitenant clusters

1.3.12.3. Colocation of Operators in a namespace

Operator Lifecycle Manager (OLM) handles OLM-managed Operators that are installed in the same namespace, meaning their Subscription resources are colocated in the same namespace, as related Operators. Even if they are not actually related, OLM considers their states, such as their version and update policy, when any one of them is updated.

Guidance on Operator colocation and an alternative procedure that uses custom namespaces has been added with the following topics:

- Colocation of Operators in a namespace
- Installing global Operators in custom namespaces

1.3.12.4. Updated web console behavior when disabling copied CSVs

The OpenShift Container Platform web console has been updated to provide better Operator discovery when copied cluster service versions (CSVs) are disabled on a cluster.

When copied CSVs are disabled by a cluster administrator, the web console is modified to show copied CSVs from the **openshift** namespace in every namespace for regular users, even though the CSVs are not actually copied to every namespace. This allows regular users to still be able to view the details of these Operators in their namespaces and create custom resources (CRs) brought in by globally installed Operators.

For more information, see Disabling copied CSVs.

1.3.13. Operator development

1.3.13.1. Setting a suggested namespace template with default node selector

With this release, Operator authors can set a default node selector on the suggested namespace where the Operator runs. The suggested namespace is created using the namespace manifest in the YAML which is included in the **ClusterServiceVersion** (CSV). When adding the Operator to a cluster using OperatorHub, the web console automatically populates the suggested namespace for the cluster administrator during the installation process.

For more information, see Setting a suggested namespace with default node selector .

1.3.13.2. Node Tuning Operator

The Node Tuning Operator (NTO) can now be enabled/disabled using the **NodeTuning** cluster capability. If disabled at cluster install, it can be re-enabled later. For more information, see Node Tuning capability.

1.3.14. Machine API

1.3.14.1. Additional platform support for control plane machine sets

- With this release, control plane machine sets are supported for Google Cloud Platform clusters.
- This release includes an enhancement to the user experience for the control plane machine set on Microsoft Azure clusters. For Azure clusters that are installed with or upgraded to OpenShift Container Platform version 4.13, you are no longer required to create a control plane machine set custom resource (CR).
    - Clusters that are installed with version 4.13 have a control plane machine set that is active by default.
    - For clusters that are upgraded to version 4.13, an inactive CR is generated for the cluster and can be activated after you verify that the values in the CR are correct for your control plane machines.

For more information, see Getting started with the Control Plane Machine Set Operator .

1.3.15. Machine Config Operator

1.3.15.1. Red Hat Enterprise Linux CoreOS (RHCOS) image layering is generally available

Red Hat Enterprise Linux CoreOS (RHCOS) image layering is now generally available. With this feature, you can extend the functionality of your base RHCOS image by layering additional images onto the base image.

For more information, see Red Hat Enterprise Linux CoreOS (RHCOS) image layering .

1.3.15.2. Support for adding third party and custom content to RHCOS

You can now use Red Hat Enterprise Linux CoreOS (RHCOS) image layering to add Red Hat Enterprise Linux (RHEL) and third-party packages to cluster nodes.

For more information, see Red Hat Enterprise Linux CoreOS (RHCOS) image layering .

1.3.15.3. Support for setting the core user password

You can now create a password for the RHCOS **core** user. If you cannot use SSH or the **oc debug node** command to access a node, this password allows you to use the **core** user to access the node through a cloud provider serial console or a bare metal baseboard controller manager (BMC).

For more information, see Changing the core user password for node access .

1.3.16. Nodes

1.3.16.1. Image registry repository mirroring by tags

You can now pull images from a mirrored registry by using image tags in addition to digest specifications. To accomplish this change, the **ImageContentSourcePolicy** (ICSP) object is deprecated. You can now use an **ImageDigestMirrorSet** (IDMS) object to pull images by using digest specifications or an **ImageTagMirrorSet** (ITMS) object to pull images by using image tags.

If you have existing YAML files that you used to create ICSP objects, you can use the **oc adm migrate icsp** command to convert those files to an IDMS YAML file.

For more information on these new objects, see Configuring image registry repository mirroring .

For more information on converting existing ICSP YAML files to IDMS YAML files, see Converting ImageContentSourcePolicy (ICSP) files for image registry repository mirroring.

1.3.16.2. crun general availability

The crun low-level container runtime is now generally available in OpenShift Container Platform 4.13. There is no new functionality in the GA version.

1.3.16.3. Linux Control Group version 2 (cgroup v2) general availability

Linux Control Group version 2 (cgroup v2) is now generally available in OpenShift Container Platform 4.13. There is no new functionality in the GA version.

1.3.16.4. Pod disruption budget (PDB) unhealthy pod eviction policy (Technology Preview)

With this release, specifying an unhealthy pod eviction policy for pod disruption budgets (PDBs) is available as a Technology Preview feature. This can help evict malfunctioning applications during a node drain.

To use this Technology Preview feature, you must enable the **TechPreviewNoUpgrade** feature set.

WARNING

Enabling the **TechPreviewNoUpgrade** feature set on your cluster cannot be undone and prevents minor version updates. You should not enable this feature set on production clusters.

For more information, see Specifying the eviction policy for unhealthy pods .

1.3.16.5. Support for graceful node shutdown

A graceful node shutdown delays the eviction of pods during a node shutdown. In OpenShift Container Platform 4.13, you can configure the kubelet to enable a graceful node shutdown so that pods running critical workloads are not interrupted.

To configure graceful node shutdowns, you can specify a termination grace period for regular and critical pods in the **KubeletConfig** custom resource. A termination grace period defines a time period for the pod to complete any ongoing tasks before terminating. You can also add priority classes to pods to specify the order of termination.

For further information see Managing graceful node shutdown.

1.3.16.6. Metal3 remediation support

Previously, Machine Health Checks could self-remediate or use the Self Node Remediation provider. With this release, the new Metal3 remediation provider is also supported on bare metal clusters.

For more information, see About power-based remediation of bare metal.

1.3.17. Monitoring

The monitoring stack for this release includes the following new and modified features.

1.3.17.1. Updates to monitoring stack components and dependencies

This release includes the following version updates for monitoring stack components and dependencies:

- Alertmanager to 0.25.0
- kube-state-metrics to 2.8.1
- node-exporter to 1.5.0

- prom-label-proxy to 0.6.0
- Prometheus to 2.42.0
- prometheus-operator to 0.63.0
- Thanos to 0.30.2

1.3.17.2. Changes to alerting rules

NOTE

Red Hat does not guarantee backward compatibility for recording rules or alerting rules.

- The **NodeFilesystemAlmostOutOfSpace** alert no longer fires for certain **tmpfs** mount points that are always full by design.

1.3.17.3. New option to add secrets to the Alertmanager configuration

With this release, you can add secrets to the Alertmanager configuration for core platform monitoring and for user-defined projects. If you need to authenticate with a receiver so that Alertmanager can send alerts to it, you can now configure Alertmanager to use a secret that contains authentication credentials for the receiver.

1.3.17.4. New option to configure node-exporter collectors

With this release, you can customize Cluster Monitoring Operator (CMO) config map settings for the following node-exporter collectors. The following node-exporter collectors are now optional and can be enabled or disabled:

- **buddyinfo** collector
- **cpufreq** collector
- **netclass** collector
- **netdev** collector
- **netlink** backend for the **netclass** collector
- **tcpstat** collector

1.3.17.5. New option to filter node-related dashboards by node role

In the OpenShift Container Platform web console, you can now filter data in node-related monitoring dashboards based on node roles. You can use this new filter to quickly select relevant node roles if you want to see dashboard data only for nodes with certain roles, such as worker nodes.

1.3.17.6. New option to enable metrics collection profiles (Technology Preview)

This release introduces a Technology Preview feature for default platform monitoring in which an administrator can set a metrics collection profile to collect either the default amount of metrics data or a minimal amount of metrics data. When you enable the minimal profile, basic monitoring features such as alerting continue to work, but the CPU and memory resources required by Prometheus decrease.

1.3.18. Scalability and performance

1.3.18.1. NUMA-aware scheduling with the NUMA Resources Operator is generally available

NUMA-aware scheduling with the NUMA Resources Operator was previously introduced as a Technology Preview in OpenShift Container Platform 4.10 and is now generally available in OpenShift Container Platform 4.13.

The NUMA Resources Operator deploys a NUMA-aware secondary scheduler that makes scheduling decisions for workloads based on a complete picture of available NUMA zones in clusters. This enhanced NUMA-aware scheduling ensures that latency-sensitive workloads are processed in a single NUMA zone for maximum efficiency and performance.

This update adds the following features:

- Fine-tuning of API polling for NUMA resource reports.
- Configuration options at the node group level for the node topology exporter.

For more information, see Scheduling NUMA-aware workloads.

1.3.18.2. Support for workload partitioning for three-node clusters and standard clusters (Technology Preview)

Before this update, workload partitioning was supported for single-node OpenShift clusters only. Now, you can also configure workload partitioning for three-node compact clusters and standard clusters. Use workload partitioning to isolate OpenShift Container Platform services, cluster management workloads, and infrastructure pods to run on a reserved set of CPUs.

For more information, see Workload partitioning.

1.3.18.3. Configuring power states using GitOps ZTP

OpenShift Container Platform 4.12 introduced the ability to set power states for critical and non-critical workloads. In OpenShift Container Platform 4.13, you can now configure power states with GitOps ZTP.

For more information about the feature, see Configuring power states using PolicyGenTemplates CRs .

1.3.18.4. Pre-caching container images for managed cluster updates with TALM and GitOps ZTP

This release adds two new Topology Aware Lifecycle Manager (TALM) features for use with GitOps ZTP:

- A new check ensures that there is sufficient available disk space on the managed cluster host before cluster updates. Now, during container image pre-caching, TALM compares the available host disk space with the estimated OpenShift Container Platform image size to ensure that there is enough disk space on the host.
- A new **excludePrecachePatterns** field in the **ConfigMap** CR is available that controls which pre-cache images TALM downloads to the cluster host before an update.

For more information see Using the container image pre-cache filter.

1.3.18.5. HTTP transport replaces AMQP for PTP and bare-metal events (Technology Preview)

HTTP is now the default transport in the PTP and bare-metal events infrastructure. AMQ Interconnect is end of life (EOL) from 30 June 2024.

For more information, see About the PTP fast event notifications framework.

1.3.18.6. Support for Intel E810 Westport Channel NIC as PTP grandmaster clock (Technology Preview)

You can now configure the Intel E810 Westport Channel NIC as a PTP grandmaster clock by using the PTP Operator. PTP grandmaster clocks use **ts2phc** (time stamp 2 physical clock) for system clock and network time synchronization.

For more information, see Configuring linuxptp services as a grandmaster clock .

1.3.18.7. Configuring crun as the default container runtime for managed clusters in GitOps ZTP

A **ContainerRuntimeConfig** CR that configures crun as the default container runtime has been added to the GitOps ZTP **ztp-site-generate** container.

For optimal performance in clusters that you install with GitOps ZTP, enable crun for control plane and worker nodes in single-node OpenShift, three-node OpenShift, and standard clusters alongside additional Day 0 installation manifest CRs.

For more information, see Configuring crun as the default container runtime .

1.3.18.8. Documentation enhancement: Overview of etcd is now available

An overview of etcd, including the benefits it provides and how it works, is now available in the OpenShift Container Platform documentation. As the primary data store for Kubernetes, etcd provides a reliable approach to cluster configuration and management on OpenShift Container Platform through the etcd Operator. For more information, see Overview of etcd.

1.3.19. Insights Operator

In OpenShift Container Platform 4.13, the Insights Operator now collects the following information:

- The **openshift_apps_deploymentconfigs_strategy_total** metric. This metric gathers deployment strategy information from a deployment's configuration.
- Additional machine resource definitions to identify why machines are failing.
- The default **ingresscontroller.operator.openshift.io** resource to inform Insights if the Authentication Operator is degraded.

1.3.20. Hosted control planes (Technology Preview)

1.3.20.1. Hosted control planes section is now available in the documentation

The OpenShift Container Platform documentation now includes a section dedicated to hosted control planes, where you can find an overview of the feature and information about configuring and managing hosted clusters. For more information, see Hosted control planes.

1.3.20.2. Updating hosted control planes

The OpenShift Container Platform documentation now includes information about updating hosted control planes. Updating hosted control planes involves updating the hosted cluster and the node pools. For more information, see Updates for hosted control planes .

1.3.21. Requirements for installing OpenShift Container Platform on a single node

4.13 now supports **x86_64** and **arm64** CPU architectures.

1.4. NOTABLE TECHNICAL CHANGES

OpenShift Container Platform 4.13 introduces the following notable technical changes.

Cloud controller managers for additional cloud providers
The Kubernetes community plans to deprecate the use of the Kubernetes controller manager to interact with underlying cloud platforms in favor of using cloud controller managers. As a result, there is no plan to add Kubernetes controller manager support for any new cloud platforms.

The Nutanix implementation that is added in this release of OpenShift Container Platform uses cloud controller managers. In addition, this release introduces the General Availability of using cloud controller managers for VMware vSphere.

To learn more about the cloud controller manager, see the Kubernetes Cloud Controller Manager documentation.

To manage the cloud controller manager and cloud node manager deployments and lifecycles, use the Cluster Cloud Controller Manager Operator.

For more information, see the Cluster Cloud Controller Manager Operator entry in the *Platform Operators reference*.

The MCD now syncs kubelet CA certificates on paused pools
Previously, the Machine Config Operator (MCO) updated the kubelet client certificate authority (CA) certificate, **/etc/kubernetes/kubelet-ca.crt**, as a part of the regular machine config update. Starting with OpenShift Container Platform 4.13, the **kubelet-ca.crt** no longer gets updated as a part of the regular machine config update. As a result of this change, the Machine Config Daemon (MCD) automatically keeps the **kubelet-ca.crt** up to date whenever changes to the certificate occur.

Also, if a machine config pool is paused, the MCD is now able to push the newly rotated certificates to those nodes. A new rendered machine config, which contains the changes to the certificate, is generated for the pool, like in previous versions. The pool will indicate that an update is required; this condition will be removed in a future release of this product. However, because the certificate is updated separately, it is safe to keep the pool paused, assuming there are no further updates.

Also, the **MachineConfigControllerPausedPoolKubeletCA** alert has been removed, because the nodes should always have the most up-to-date **kubelet-ca.crt**.

Change in SSH key location
OpenShift Container Platform 4.13 introduces a RHEL 9.2 based RHCOS. Before this update, SSH keys were located in **/home/core/.ssh/authorized_keys** on RHCOS. With this update, on RHEL 9.2 based RHCOS, SSH keys are located in **/home/core/.ssh/authorized_keys.d/ignition**.

Future restricted enforcement for pod security admission
Currently, pod security violations are shown as warnings and logged in the audit logs, but do not cause the pod to be rejected.

Global restricted enforcement for pod security admission is currently planned for the next minor release of OpenShift Container Platform. When this restricted enforcement is enabled, pods with pod security violations will be rejected.

To prepare for this upcoming change, ensure that your workloads match the pod security admission profile that applies to them. Workloads that are not configured according to the enforced security standards defined globally or at the namespace level will be rejected. The **restricted-v2** SCC admits workloads according to the Restricted Kubernetes definition.

If you are receiving pod security violations, see the following resources:

- See Identifying pod security violations for information about how to find which workloads are causing pod security violations.
- See Security context constraint synchronization with pod security standards to understand when pod security admission label synchronization is performed. Pod security admission labels are not synchronized in certain situations, such as the following situations:
  - The workload is running in a system-created namespace that is prefixed with **openshift-**.
  - The workload is running on a pod that was created directly without a pod controller.
- If necessary, you can set a custom admission profile on the namespace or pod by setting the **pod-security.kubernetes.io/enforce** label.

The oc-mirror plugin now retrieves graph data container images from an OpenShift API endpoint

The oc-mirror OpenShift CLI (**oc**) plugin now downloads the graph data tarball from an OpenShift API endpoint instead of downloading the entire graph data repository from GitHub. Retrieving this data from Red Hat instead of an external vendor is more suitable for users with stringent security and compliance restrictions on external content.

The data that the oc-mirror plugin downloads now excludes content that is in the graph data repository but not needed by the OpenShift Update Service. The container also uses UBI Micro as the base image instead of UBI, resulting in a container image that is significantly smaller than before.

These changes do not affect the user workflow for the oc-mirror plugin.

The Dockerfile for the graph data container image is now retrieved from an OpenShift API endpoint

If you are creating a graph data container image for the OpenShift Update Service by using the Dockerfile, note that the graph data tarball is now downloaded from an OpenShift API endpoint instead of GitHub.

For more information, see Creating the OpenShift Update Service graph data container image .

The nodeip-configuration service is now enabled on a vSphere user-provisioned infrastructure cluster

In OpenShift Container Platform 4.13, the **nodeip-configuration** service is now enabled on a vSphere user-provisioned infrastructure cluster. This service determines the network interface controller (NIC) that OpenShift Container Platform uses for communication with the Kubernetes API server when the node boots. In rare circumstances, the service might select an incorrect node IP after an upgrade. If this happens, you can use the **NODEIP_HINT** feature to restore the original node IP. See Troubleshooting network issues.

Operator SDK 1.28

OpenShift Container Platform 4.13 supports Operator SDK 1.28. See Installing the Operator SDK CLI to install or update to this latest version.

NOTE

Operator SDK 1.28 supports Kubernetes 1.26.

If you have Operator projects that were previously created or maintained with Operator SDK 1.25, update your projects to keep compatibility with Operator SDK 1.28.

- Updating Go-based Operator projects
- Updating Ansible-based Operator projects
- Updating Helm-based Operator projects
- Updating Hybrid Helm-based Operator projects
- Updating Java-based Operator projects

Change in disk ordering behavior for RHCOS based on RHEL 9.2

OpenShift Container Platform 4.13 introduces a RHEL 9.2 based RHCOS. With this update, symbolic disk naming can change across reboots. This can cause issues if you apply configuration files after installation or when provisioning a node that references a disk which uses symbolic naming, such as **/dev/sda**, for creating services. The effects of this issue depend on the component you are configuring. It is recommended to use a specific naming scheme for devices, including for any specific disk references, such as **dev/disk/by-id**.

With this change, you might need to adjust existing automation workflows in the cases where monitoring collects information about the install device for each node.

For more information, see the RHEL documentation.

Documentation about backup, restore, and disaster recovery for hosted control planes moved

In the documentation for OpenShift Container Platform 4.13, the procedures to back up and restore etcd on a hosted cluster and to restore a hosted cluster within an AWS region were moved from the "Backup and restore" section to the "Hosted control planes" section. The content itself was not changed.

1.5. DEPRECATED AND REMOVED FEATURES

Some features available in previous releases have been deprecated or removed.

Deprecated functionality is still included in OpenShift Container Platform and continues to be supported; however, it will be removed in a future release of this product and is not recommended for new deployments. For the most recent list of major functionality deprecated and removed within OpenShift Container Platform 4.13, refer to the table below. Additional details for more functionality that has been deprecated and removed are listed after the table.

In the following tables, features are marked with the following statuses:

- *General Availability*
- *Deprecated*
- *Removed*

Operator deprecated and removed features

Table 1.6. Operator deprecated and removed tracker

Feature	4.11	4.12	4.13
SQLite database format for Operator catalogs	Deprecated	Deprecated	Deprecated

Images deprecated and removed features

Table 1.7. Images deprecated and removed tracker

Feature	4.11	4.12	4.13
ImageChangesInProgress condition for Cluster Samples Operator	Deprecated	Deprecated	Deprecated
MigrationInProgress condition for Cluster Samples Operator	Deprecated	Deprecated	Deprecated

Installation deprecated and removed features

Table 1.8. Installation deprecated and removed tracker

Feature	4.11	4.12	4.13
vSphere 7.0 Update 1 or earlier	Deprecated	Deprecated	Removed [1]
VMware ESXi 7.0 Update 1 or earlier	Deprecated	Deprecated	Removed [1]
CoreDNS wildcard queries for the **cluster.local** domain	General Availability	Deprecated	Deprecated
ingressVIP and **apiVIP** settings in the **install-config.yaml** file for installer-provisioned infrastructure clusters	General Availability	Deprecated	Deprecated

1. For OpenShift Container Platform 4.13, you must install the OpenShift Container Platform cluster on a VMware vSphere version 7.0 Update 2 or later instance, including VMware vSphere version 8.0, that meets the requirements for the components that you use.

Storage deprecated and removed features

Table 1.9. Storage deprecated and removed tracker

Feature	4.11	4.12	4.13
Persistent storage using FlexVolume	Deprecated	Deprecated	Deprecated

Specialized hardware and driver enablement deprecated and removed features

Table 1.10. Specialized hardware and driver enablement deprecated and removed tracker

Feature	4.11	4.12	4.13
Special Resource Operator (SRO)	Technology Preview	Removed	Removed

Multi-architecture deprecated and removed features

Table 1.11. Multi-architecture deprecated and removed tracker

Feature	4.11	4.12	4.13
IBM Power8 all models (**ppc64le**)	General Availability	Deprecated	Removed
IBM Power AC922 (**ppc64le**)	General Availability	Deprecated	Removed
IBM Power IC922 (**ppc64le**)	General Availability	Deprecated	Removed
IBM Power LC922 (**ppc64le**)	General Availability	Deprecated	Removed
IBM z13 all models (**s390x**)	General Availability	Deprecated	Removed
IBM® LinuxONE Emperor (**s390x**)	General Availability	Deprecated	Removed
IBM® LinuxONE Rockhopper (**s390x**)	General Availability	Deprecated	Removed
AMD64 (x86_64) v1 CPU	General Availability	Deprecated	Removed

Networking deprecated and removed features

Table 1.12. Networking deprecated and removed tracker

Feature	4.11	4.12	4.13
Kuryr on RHOSP	General Availability	Deprecated	Deprecated

Web console deprecated and removed features

Table 1.13. Web console deprecated and removed tracker

Feature	4.11	4.12	4.13
Multicluster console	Technology Preview	Technology Preview	Removed

Node deprecated and removed features

Table 1.14. Node deprecated and removed tracker

Feature	4.11	4.12	4.13
ImageContentSourcePolicy (ICSP) objects	General Availability	General Availability	Deprecated
Kubernetes topology label **failure-domain.beta.kubernetes.io/zone**	General Availability	General Availability	Deprecated
Kubernetes topology label **failure-domain.beta.kubernetes.io/region**	General Availability	General Availability	Deprecated

1.5.1. Deprecated features

1.5.1.1. Red Hat Virtualization (RHV) as a host platform for OpenShift Container Platform will be deprecated

Red Hat Virtualization (RHV) as a host platform for OpenShift Container Platform is now deprecated, and will be removed in the next OpenShift Container Platform release, currently planned as OpenShift Container Platform 4.14.

1.5.1.2. Wildcard DNS queries for the cluster.local domain are deprecated

CoreDNS will stop supporting wildcard DNS queries for names under the **cluster.local** domain. These queries will resolve in OpenShift Container Platform 4.13 as they do in earlier versions, but support will be removed from a future OpenShift Container Platform release.

1.5.1.3. Kuryr support for clusters that run on RHOSP

In OpenShift Container Platform 4.12, support for Kuryr on clusters that run on RHOSP was deprecated. Support will be removed no earlier than OpenShift Container Platform 4.14.

1.5.1.4. ImageContentSourcePolicy objects

The **ImageContentSourcePolicy** (ICSP) object is now deprecated. You can now use an **ImageDigestMirrorSet** (IDMS) object to pull images by using digest specifications or an **ImageTagMirrorSet** (ITMS) object to pull images by using image tags.

For more information on these new objects, see Configuring image registry repository mirroring .

For more information on converting existing ICSP YAML files to IDMS YAML files, see Converting ImageContentSourcePolicy (ICSP) files for image registry repository mirroring.

1.5.1.5. Toolbox is deprecated in RHCOS

The toolbox script is deprecated and support will be removed from a future OpenShift Container Platform release.

1.5.1.6. RHEL 9 driver deprecations

OpenShift Container Platform 4.13 introduces a RHEL 9.2 based RHCOS. Some kernel device drivers are deprecated in RHEL 9. See the RHEL documentation for more information.

1.5.1.7. VMware vSphere configuration parameters

OpenShift Container Platform 4.13 deprecates the following vSphere configuration parameters. You can continue to use these parameters, but the installation program does not automatically specify these parameters in the **install-config.yaml** file.

- **platform.vsphere.vCenter**
- **platform.vsphere.username**
- **platform.vsphere.password**
- **platform.vsphere.datacenter**
- **platform.vsphere.defaultDatastore**
- **platform.vsphere.cluster**
- **platform.vsphere.folder**
- **platform.vsphere.resourcePool**
- **platform.vsphere.apiVIP**
- **platform.vsphere.ingressVIP**
- **platform.vsphere.network**

For more information, see Deprecated VMware vSphere configuration parameters .

1.5.1.8. Kubernetes topology labels

Two commonly used Kubernetes topology labels are being replaced. The **failure-domain.beta.kubernetes.io/zone** label is replaced with **topology.kubernetes.io/zone**. The **failure-domain.beta.kubernetes.io/region** label is replaced with **topology.kubernetes.io/region**. The replacement labels are available starting with Kubernetes 1.17 and OpenShift Container Platform version 4.4.

Currently, both the deprecated and replacement labels are supported, but support for the deprecated labels is planned to be removed in a future release. To prepare for the removal, you can modify any resources (such as volumes, deployments, or other workloads) that reference the deprecated labels to use the replacement labels instead.

1.5.2. Removed features

1.5.2.1. Beta APIs removed from Kubernetes 1.26

Kubernetes 1.26 removed the following deprecated APIs, so you must migrate manifests and API clients to use the appropriate API version. For more information about migrating removed APIs, see the Kubernetes documentation.

Table 1.15. APIs removed from Kubernetes 1.26

Resource	Removed API	Migrate to
FlowSchema	**flowcontrol.apiserver.k8s.io/v1beta1**	**flowcontrol.apiserver.k8s.io/v1beta3**
HorizontalPodAutoscaler	**autoscaling/v2beta2**	**autoscaling/v2**
PriorityLevelConfiguration	**flowcontrol.apiserver.k8s.io/v1beta1**	**flowcontrol.apiserver.k8s.io/v1beta3**

1.5.3. Future Kubernetes API removals

The next minor release of OpenShift Container Platform is expected to use Kubernetes 1.27. Currently, Kubernetes 1.27 is scheduled to remove a deprecated API.

See the Deprecated API Migration Guide in the upstream Kubernetes documentation for the list of planned Kubernetes API removals.

See Navigating Kubernetes API deprecations and removals for information about how to check your cluster for Kubernetes APIs that are planned for removal.

1.5.3.1. Specific hardware models on ppc64le, s390x, and x86_64 v1 CPU architectures are removed

In OpenShift Container Platform 4.13, support for RHCOS functionality is removed for the following deprecated hardware models:

- IBM Power8 all models (**ppc64le**)
- IBM Power AC922 (**ppc64le**)
- IBM Power IC922 (**ppc64le**)
- IBM Power LC922 (**ppc64le**)
- IBM z13 all models (**s390x**)
- IBM® LinuxONE Emperor (**s390x**)
- IBM® LinuxONE Rockhopper (**s390x**)
- AMD64 (**x86_64**) v1 CPU

1.6. BUG FIXES

Bare Metal Hardware Provisioning

- Previously, when you attempted to deploy an OpenShift Container Platform cluster node on a server that is configured with the Integrated Lights-Out (iLO) Management Interface Driver, provisioning of the node would fail. The failure occurs because of a missing **[ilo]/use_web_server_for_images** configuration parameter in the iLO drive that caused the driver to attempt to use object storage as the default storage mechanism. Object storage is not present in the product. With this update, OpenShift Container Platform 4.13 and later versions includes **[ilo]/use_web_server_for_images** in the iLO driver's configuration, so that the driver uses a web server that runs in the **metal3** pod. (OCPBUGS-5068)

Cloud Compute

- For some configurations of Google Cloud Platform clusters, the internal load balancer uses instance groups that are created by the installation program. Previously, when a control plane machine was replaced manually, the new control plane node was not assigned to a control plane instance group. This prevented the node from being reachable via the internal load balancer. To resolve the issue, administrators had to manually move the control plane machine to the correct instance group by using the Google Cloud console.
With this release, replacement control plane nodes are assigned to the correct instance group. (BZ#1970464, OCPCLOUD-1562)

- Previously, a compute machine set for Google Cloud Platform could try to reconcile invalid machines, which caused them to be stuck with no phase assigned. With this release, machines with an invalid configuration are put into the **Failed** state. (OCPBUGS-4574)

- Previously, a control plane machine set replica was considered ready when its backing machine entered the **Running** state, even though the linked node needed to also be ready for the replica to be considered ready. With this release, a node and its machine must be in the **Ready** state for the control plane machine set replica to be considered ready. (OCPBUGS-8424)

- Previously, the **mapi_instance_create_failed** alert metric did not start when an error occurred for the Accelerated Networking feature on Microsoft Azure clusters. This release adds the missing alert so that clusters with Accelerated Networking enabled can generate alerts when required. (OCPBUGS-5235)

- Previously, when a machine entered the **Running** state, no further changes to the state of its node were checked for. The previous resolution of OCPBUGS-8424 introduced the requirement for a node and its machine to be in the **Ready** state for the control plane machine set replica to be considered ready. As a result, if the control plane machine set missed the stage when the node and machine were ready, its replica could not become ready. This behavior caused the Control Plane Machine Set Operator to become unavailable, blocking upgrades. With this release, when a machine is running but the node is not ready, the node is checked at regular intervals until it becomes ready. This fix prevents the Control Plane Machine Set Operator from becoming unavailable and blocking upgrades. (OCPBUGS-10771)

- Previously, when a machine health check exceeded the **maxUnhealthy** threshold and generated an alert, the metric was not reset when the cluster became healthy enough to reconcile machine health checks successfully, and the alert continued. With this release, the logic that determines when to trigger an alert is improved so that the alert now clears when the cluster is healthy. (OCPBUGS-4725)

- The previous resolution of OCPBUGS-5546 removed the **clusterName** assignment of **MachineConfig.Name** in the machine configuration object. As a result, the value of the parameter was an empty string and, when it was combined with the value of **machineName** to create an IP address name, it created an invalid value. The invalid value caused machines to fail during provisioning. With this release, the value for **clusterName** is obtained from the infrastructure object so that it creates a valid IP address name. (OCPBUGS-7696)

- The Kubernetes 1.26 release introduced changes to the node infrastructure, such as removing an unhealthy node with a **NotReady** status from the public load balancer to prevent the node from receiving routing traffic. These changes impacted a node that ran inside a cluster on Microsoft Azure. As a result, the node was unable to regain a **Ready** status and subsequently establish an outbound connection. With this update, a node marked with a **NotReady** status is now detected by **kube-proxy** health probes without the need of node detachment from the public load balancer. This means that a node can retain an outbound internet connection throughout these phases. (OCPBUGS-7359)

Cloud Credential Operator

- Amazon Simple Storage Service (Amazon S3) updated their Amazon S3 bucket configuration so a bucket created in an Amazon Web Services (AWS) region has S3 Block Public Access enabled and access control limits (ACLs) disabled by default. This configuration limits S3 bucket resources to private use. The OpenShift Container Platform 4.13 updates the CCO utility (**ccoctl**) and the installation program to account for the default S3 bucket configuration so that S3 bucket resources are publicly available. (OCPBUGS-11706 and OCPBUGS-11661)

Developer Console

- Previously, the OpenShift Container Platform used API version **v1alpha1** for Knative Serving and Eventing but because of a bug, API version **v1beta1** was not supported. With this fix, the OpenShift Container Platform supports both the API versions. (OCPBUGS-5164)

- Previously, when editing any pipeline in the OpenShift Container Platform console, the correct data was not rendered in the **Pipeline builder** and **YAML view** configuration options. Because of this issue, you could not edit the pipeline in the **Pipeline builder**. With this update, data is parsed correctly and you can edit the pipeline using the builder. (OCPBUGS-5016)

- Previously, the topology sidebar did not display updated information. When you updated the resources directly from the topology sidebar, you had to reopen the sidebar to see the changes. With this fix, the updated resources are displayed correctly. As a result, you can see the latest changes directly in the topology sidebar. (OCPBUGS-4691)

- Previously, the **Samples** page in the OpenShift Container Platform did not allow distinguishing between the types of samples listed. With this fix, you can identify the sample from the badges displayed on the **Samples** page. (OCPBUGS-10679)

Documentation

Previously, the OpenShift Container Platform documentation included a sub-section titled "Expanding a cluster with on-premise bare metal nodes." However, this has been removed in order to maintain accurate, up to date documentation.

etcd Cluster Operator

- Previously, the Control Plane Machine Set Operator attempted to recreate a control plane machine before the cluster bootstrapping completed. This resulted in the removal of the bootstrap node from the etcd cluster membership that caused etcd quorum loss and the cluster to go offline. With this update, the Control Plane Machine Set Operator only recreates a control plane machine after the etcd Cluster Operator removes the bootstrap node. (OCPBUGS-10960)

Hosted Control Plane

- Previously, the **HostedControlPlane** object did not identify changes to scheduler profiles that were set by a **HostedCluster** resource. Further, **HostedControlPlane** did not propagate changes to the scheduler, so the scheduler did not restart control plane pods for them to

receive the latest scheduler profile changes. With this update, **HostedControlPlane** now recognizes changes to scheduler profiles and then dynamically restarts the scheduler, so that the scheduler can apply profile changes to pods. (OCPBUGS-7091)

- Previously, a hosted cluster did not account for OpenID Connect (OIDC) providers, **oidc**, unavailability that caused the deletion of **machine** and **machineset** objects to stale. With this update, a hosted cluster can detect the status of an unavailable **odic** provider, so that the deletion of **machine** and **machineset** objects to not stale because of an unavailable **oidc** provider. (OCPBUGS-10227)

- Previously, the **spec.metadata.annotations** parameter value in an Amazon Web Services (AWS) compute machine set was not copied from a compute machine to its node. This caused the node to have missing annotations specified in the compute machine set. With this release, annotations are correctly applied to the node. (OCPBUGS-4566)

Installer

- Previously, DNS records that the installation program created were not removed when uninstalling a private cluster. With this update, the installation program now correctly removes these DNS records. (OCPBUGS-7973)

- Previously, the bare-metal installer-provisioned infrastructure used port 80 for providing images to the Baseboard Management Controller (BMC) and the deployment agent. Security risks could exist with port 80, because this port is commonly chosen for internet communications. The bare metal installer-provisioned infrastructure now uses port 6180 for serving images that are used by the **metal3** pod on deployed clusters. (OCPBUGS-8511)

- Previously, SSH access to bootstrap and cluster nodes failed when the bastion host ran in the same VPC network as the cluster nodes. Additionally, this configuration caused SSH access from the temporary bootstrap node to the cluster nodes to fail. These issues are now fixed by updating the IBM Cloud security group rules to support SSH traffic between the temporary bootstrap node and cluster nodes, and to support SSH traffic from a bastion host to cluster nodes on the same VPC network. Log and debug information can be accurately collected for analysis during installer-provisioned infrastructure failure. (OCPBUGS-8035)

- Previously, if you configured the rendezvous IP to the IP address of the host that has a **role** parameter set to **worker** and you generated an ISO image, the Agent-based installer would fail to install the cluster. Now, when you attempt to generate an ISO image based on this configuration, you will receive a validation failure message. On receiving this message, you must update the **rendezvousIP** field in the **agent-config.yaml** file to use the IP of a host with the **master** role. (OCPBUGS-2088)

- Previously, the installation program did not accept the following new regions defined in the **aws-sdk-go** library: **ap-south-2**, **ap-southeast-4**, **eu-central-2**, **eu-south-2**, and **me-central-1**. When you used the installation program to create the installation configuration file, the installation program would not list these new regions or accept manual entries for these regions. With this update, the installation program supports these regions and you can specify them when you create the installation configuration file. (OCPBUGS-10213)

- Previously, an issue existed with the code base that sets **Machine.PrimaryNetwork** based on the **controlPlane.platform.openstack.failureDomain** field in the **install-config.yaml** file. This issue impacts OpenShift Container Platform that runs with Kuryr from identifying the port on a Red Hat OpenStack Platform (RHOSP) subnet that control plane machines use for communicating between them. With this update, when you set **control-plane** for **portTarget** in the **failureDomain** Technology Preview component, the installation program sets the port's information in the **Machine.PrimaryNetwork** field, so that your OpenShift Container Platform cluster successfully runs with Kuryr. (OCPBUGS-10658)

- Previously, uninstalling an AWS cluster that was deployed to the **us-gov-west-1** region failed because AWS resources could not be untagged. This resulted in the process going into an infinite loop, where the installation program tried to untag the resources. This update prevents the retry. As a result, uninstalling the cluster succeeds. (BZ#2070744)

- Previously, a private OpenShift Container Platform cluster running on Google Cloud Platform (GCP) would receive additional firewall rules so that GCP could perform health checks for both internal and external load balancers. Private clusters only use internal load balancers, so performing health checks for external load balancers is unnecessary. With this update, a private cluster that runs on GCP no longer receives these additional firewall rules that stemmed from health checks for external load balancers. (BZ#2110982)

Kubernetes Scheduler

- Previously, when the **LifeCycleUtilization** profile was excluded to test namespace filtering, the following error was logged in the Descheduler Operator logs: **belowE0222 12:43:14.331258 1 target_config_reconciler.go:668] key failed with : only namespace exclusion supported with LowNodeUtilization**. Consequently, the descheduler cluster pod would not start. With this update, the namespace exclusion now works with the **LifeCycleUtilization** profile. (OCPBUGS-7876)

Management Console

- Previously, user permissions were not checked when rendering the **Create Pod** button, and the button rendered for users without needed permissions. With this update, user permissions are checked when rendering the **Create Pod** button, and it renders for users for users with the needed permissions. (BZ#2005232)

- Previously, the **Pod** resource had a **PDB** ***add***, ***edit***, and ***remove*** actions in the Pod resource action menu that are not required. With this update, the actions are removed. (BZ#2110565)

- Previously, the **PodDisruptionBudget** field on the **Details** page had an incorrect help message. With this update, the help message is now more descriptive. (BZ#2084452)

- Previously, when navigating to the root path of the console, the URL redirected to the **Overview** page even if metrics were disabled and it did not appear in the navigation menu. With this update, when clicking the masthead logo or navigating to the root path of the console, the URL redirects to the **project list** page if metrics are disabled. (OCPBUGS-3033)

- Previously, the cluster dropdown was positioned so that it was not always visible, making it unclear which cluster you were viewing. With this update, the cluster dropdown is now in the masthead so the cluster dropdown is always visible, and you can always see which cluster you are viewing. (OCPBUGS-7089)

- Previously, the node progress bars were set to display when the cluster version had a status of **Failing**, **UpdatingAndFailing**, and **Updating**, causing the node progress bars to display when the cluster is not updating. With this update, the node progress bars only display when the cluster version has a status of **UpdatingAndFailing** or **Updating**. (OCPBUGS-6049)

- Previously, when downloading a **kubeconfig** file for a ServiceAccount, an error was displayed and the ServiceAccount token was unable to be reached. This error was due to the removal of automatically generated secrets. With this update, the download **kubeconfig** action has been removed and the error no longer occurs. (OCPBUGS-7308)

- Previously, the **Terminal** tab on the **Node details** page displayed an error because of missing annotations that were caused by pod security measures. Without the required annotations, the node debug pod cannot start. With this update, OpenShift Container Platform adds these

annotations, so the node debug pod can start and the **Terminal** tab loads without any errors. (OCPBUGS-4252)

- Previously, if a cluster administrator attempted to issue the **oc delete csv** command when uninstalling the Operator, the Operator's subscription becomes stuck. The administrator was unable to reinstall the Operator because a conflict existed with the subscription. With this update, a detailed error message displays when an administrator attempts to reinstall the uninstalled Operator. (OCPBUGS-3822)

- Previously, if one or more existing plugins failed, the web console would not display a toast notification that prompted you to refresh the console. This action is required so that you can view a plugin after an operator adds the plugin to the console. With this update, the web console checks when the operator adds a plugin and then displays a toast notification on the console, regardless of any previously failed plugins. (OCPBUGS-10249)

- Previously, a terminated container would render **{{label}}** and **{{exitCode}}** codes for each terminated container. With this update, the internationalization code is fixed to render a readable output message. (OCPBUGS-4206)

- Previously, a regression was introduced causing the **Cluster Settings** page to return an error when the **clusterversion status.availableUpdates** had a value of **null** and **Upgradeable=False**. With this update, **status.availableUpdates** are allowed to have a **null** value. (OCPBUGS-6053)

Monitoring

- Previously, the Kubernetes scheduler could skip scheduling certain pods for a node that received multiple restart operations. OpenShift Container Platform 4.13 counteracts this issue by including the **KubePodNotScheduled** alert for pods that cannot be scheduled within 30 minutes. (OCPBUGS-2260)

- Previously, if more than one label was defined for Thanos Ruler, then the statefulset could enter a recreation loop because the **prometheus-operator** did not add the labels in a specified order each time it reconciled the custom resource. After this fix, the **prometheus-operator** now sorts extra labels before adding them to the statefulset. (OCPBUGS-6055)

- With this release, the **NodeFilesystemAlmostOutOfSpace** no longer launches for certain read-only **tmpfs** instances. This change fixes an issue in which the alert launches for certain **tmpfs** mount points that were full by design. (OCPBUGS-6577)

Networking

- Previously, the Ingress Operator displayed a success message for the **updateIngressClass** function logs when an error message should be displayed. With this update, the log message for Ingress Operator is accurate. (OCPBUGS-6700)

- Previously, the Ingress Operator did not specify **ingressClass.spec.parameters.scope**, while the Ingress Class API object specifies type **cluster** by default. This caused unnecessary updates to all Ingress Classes when the Operator starts. With this update, the Ingress Operator specifies **ingressClass.spec.parameters.scope** of type **cluster**. (OCPBUGS-6701)

- Previously, the Ingress Operator had the wrong service name in **ensureNodePortService** log message causing incorrect information to be logged. With this update, the Ingress Operator accurately logs the service in **ensureNodePortService**. (OCPBUGS-6698)

- Previously, in OpenShift Container Platform 4.7.0 and 4.6.20, the Ingress Operator used an annotation for router pods that was specific for OpenShift Container Platform. This was a

temporary way to configure the liveness probe's grace period in order to fix a bug. As a result, OpenShift Container Platform was required to carry a patch to implement the fix. With this update, the Ingress Operator uses **terminationGracePeriodSeconds** API field making the previous patch removable in future releases. (OCPBUGS-4703)

- Previously, CoreDNS was using the old toolchain for building of the main binary and the old base image. With this update, OpenShift Container Platform is using 4.13 for the build toolchain and the base image. (OCPBUGS-6228)

Node

- Previously, the **LowNodeUtilization** strategy, which is enabled by the **LifecycleAndUtilization** descheduler profile, did not support namespace exclusion. With this release, namespaces are excluded properly when the **LifecycleAndUtilization** descheduler profile is set. (OCPBUGS-513)

- Previously, a regression in behavior caused Machine Config Operator (MCO) to create a duplicate **MachineConfig** object in the **kubeletconfig** or **containerruntimeconfig** custom resource (CR). The duplicate object degraded and the cluster failed to upgrade. With this update, the **kubeletconfig** and **containerruntimeconfig** controllers can detect any duplicate objects and then delete them. This action removes the degraded **MachineConfig** object error and does not impact the cluster upgrade operation. (OCPBUGS-7719)

Node Tuning Operator (NTO)

- Previously, the **hwlatdetect** tool that the Cloud-native Functions (CNF) tests image uses for running latency tests on a CNF-enabled OpenShift Container Platform cluster was configured with a detection period of 10 seconds. This configuration when combined with the detection width configuration of 0.95 of a second increased the likelihood of **hwlatdetect** missing a latency spike, because the tool monitors a node about 9.5% of the time over the allocated detection period. With this update, the detection period is set to 1 second, so that the tool can now monitor nodes for about 95% of the time over the allocated detection period. The remaining 5% of monitoring time is left unallocated so that the kernel can perform system tasks. (OCPBUGS-12433)

OpenShift CLI (oc)

- Previously, **oc adm upgrade** command did not read **Failing=True** status in ClusterVersion. With this update, **oc adm upgrade** includes **Failing=True** condition information when summarizing cluster state. This raises the visibility of **Degraded=True** status for **ClusterOperators** and other issues which can impact the behavior of the current cluster or future updates. (OCPBUGS-3714)

- Previously, the **oc-mirror** command built the catalog content in the console for OCI and FBC Operators from a mirrored disk image. Consequently, not all content of the catalog was mirrored so some content was missing from the catalog. With this update, the catalog image is built to reflect the mirrored content prior to pushing it to the destination registry resulting in a more complete catalog. (OCPBUGS-5805)

- Previously, the oc-mirror OpenShift CLI (**oc**) plugin added the Operator catalog as an entry in the **ImageContentSourcePolicy** resource. This resource does not require this entry, because the Operator catalog is consumed directly from the destination registry in the **CatalogSource** resource. This issue impacted the cluster from receiving the release image signature resources because of an unexpected entry in the **ImageContentSourcePolicy** resource. With this update, the oc-mirror plugin removes Operator catalog entry from the **ImageContentSourcePolicy** resource, so that a cluster receives signature resources from the Operator catalog in the **CatalogSource** resource. (OCPBUGS-10320)

Operator Lifecycle Manager (OLM)

- The status of an Operator's custom resource (CR) includes a list of components owned by the Operator. This list is ordered by **group/version/kind** (GVK), but the order of objects with the same GVK might change. If an Operator owns many components with the same GVK, it can cause Operator Lifecycle Manager (OLM) to continuously update the status of the Operator CR, because the order of its components has changed. This bug fix updates OLM so that the order of an Operator's component references is deterministic. As a result, OLM no longer attempts to update the CR repeatedly when the list of components remains constant. (OCPBUGS-2556)

- Operator Lifecycle Manager (OLM) manages a set of **CatalogSource** objects from which Operators can be searched for and installed from. These catalog sources are the default sources for this action and are managed by Red Hat. However, it was possible to change these default catalog sources in a way that the OLM system would not notice. Modifying a default catalog source in a way that rendered it inoperable could cause cascading issues through OLM that might prevent a user from installing new or upgrading existing Operators on their cluster. This bug fix updates the **catalog-operator** runtime, which manages the default catalog sources, to be made aware of other changes to the **CatalogSource** spec. As a result, when a change is made to a default catalog source, OLM detects the change and resets it back to default. (OCPBUGS-5466)

Red Hat Enterprise Linux CoreOS (RHCOS)

- Previously, on Azure, the SR-IOV interface was configured by NetworkManager during boot because the udev rule that marks it as **NM_UNMANAGED** was not in the **initramfs** file. With this update, the udev rule is now in the **initramfs** file and the SR-IOV interface should always be unmanaged by NetworkManager. (OCPBUGS-7173)

Security Profiles Operator

- Previously, a Security Profiles Operator (SPO) SELinux policy did not inherit low-level policy definitions from the container template if you selected another template, such as **net_container**. The policy would not work because it required low-level policy definitions that only existed in the container template. This issue occured when the SPO SELinux policy attempted to translate SELinux policies from the SPO custom format to the Common Intermediate Language (CIL) format. With this update, the container template appends to any SELinux policies that require translation from SPO to CIL. Additionally, the SPO SELinux policy can now inherit low-level policy definitions from any supported policy template. (OCPBUGS-12879)

Scalability and performance

- Previously, when a performance profile was generated, the CRI-O runtime files created automatically were configured to use **runc** as the CRI-O runtime.
  Now that setting **crun** as the container runtime is generally available when a performance profile is generated, the runtime CRI-O files created match the **defaultRuntime** configured in the **ContainerRuntimeConfig** CR. This can be either **crun** or **runc**. The default is **runc**. (OCPBUGS-11813)

Storage

- Previously, the **openshift-manila-csi-driver** namespace did not include labels that are required for the management of workload partitioning. These missing labels impacted the operation of restricting Manila CSI pods to run on a selected set of CPUs. With this update, the **openshift-manila-csi-driver** namespace now includes the **workload.openshift.io/allowed** label. (OCPBUGS-11341)

Windows containers

- Previously, Microsoft Windows container workloads were not completely emptied during the Windows node upgrade process. This resulted in service disruptions because the workloads remained on the node being upgraded. With this update, the Windows Machine Config Operator (WMCO) drains workloads and then cordons nodes until node upgrades finish. This action ensures a seamless upgrade for Microsoft Windows instances. (OCPBUGS-5732)

- Previously, the Windows Machine Config Operator (WMCO) could not drain **DaemonSet** workloads. This issue caused Windows`DaemonSet` pods to block Windows nodes that the WMCO attempted to remove or upgrade. With this update, an WMCO includes additional role-based access control (RBAC) permissions, so that the WMCO can remove **DaemonSet** workloads. An WMCO can also delete any processes that were created with the **containerd** shim, so that **DaemonSet** containers do not exist on a Windows instance after a WMCO removes a node from a cluster. (OCPBUGS-5354)

- Previously, the **containerd** container runtime reported an incorrect version on each Windows node because repository tags were not propagated to the build system. This configuration caused **containerd** to report its Go build version as the version for each Windows node. With this update, the correct version is injected into the binary during build time, so that **containerd** reports the correct version for each Windows node. (OCPBUGS-5378)

1.7. 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 following tables, features are marked with the following statuses:

- *Technology Preview*
- *General Availability*
- *Not Available*
- *Deprecated*

Networking Technology Preview features

Table 1.16. Networking Technology Preview tracker

Feature	4.11	4.12	4.13
PTP dual NIC hardware configured as boundary clock	Technology Preview	Technology Preview	General Availability
Ingress Node Firewall Operator	Not Available	Technology Preview	Technology Preview
Advertise using BGP mode the MetalLB service from a subset of nodes, using a specific pool of IP addresses	Technology Preview	General Availability	General Availability

Feature	4.11	4.12	4.13
Advertise using L2 mode the MetalLB service from a subset of nodes, using a specific pool of IP addresses	Technology Preview	Technology Preview	Technology Preview
Multi-network policies for SR-IOV networks	Not Available	Technology Preview	Technology Preview
OVN-Kubernetes network plugin as secondary network	Not Available	Not Available	Technology Preview
Updating the interface-specific safe sysctls list	Not Available	Technology Preview	Technology Preview
MT2892 Family [ConnectX-6 Dx] SR-IOV support	Not Available	Technology Preview	General Availability
MT2894 Family [ConnectX-6 Lx] SR-IOV support	Not Available	Technology Preview	General Availability
MT42822 BlueField-2 in ConnectX-6 NIC mode SR-IOV support	Not Available	Technology Preview	General Availability
Silicom STS Family SR-IOV support	Not Available	Technology Preview	General Availability
MT2892 Family [ConnectX-6 Dx] OvS Hardware Offload support	Not Available	Technology Preview	General Availability
MT2894 Family [ConnectX-6 Lx] OvS Hardware Offload support	Not Available	Technology Preview	General Availability
MT42822 BlueField-2 in ConnectX-6 NIC mode OvS Hardware Offload support	Not Available	Technology Preview	General Availability
Switching Bluefield-2 from DPU to NIC	Not Available	Technology Preview	General Availability
Intel E810-XXVDA4T	Not Available	Not Available	General Availability

Storage Technology Preview features

Table 1.17. Storage Technology Preview tracker

Feature	4.11	4.12	4.13
Shared Resources CSI Driver and Build CSI Volumes in OpenShift Builds	Technology Preview	Technology Preview	Technology Preview
CSI volume expansion	Technology Preview	General Availability	General Availability
CSI Azure File Driver Operator	Technology Preview	General Availability	General Availability
CSI Google Filestore Driver Operator	Not Available	Technology Preview	Technology Preview
CSI automatic migration (Azure file, VMware vSphere)	Technology Preview	Technology Preview	General Availability
CSI automatic migration (Azure Disk, OpenStack Cinder)	General Availability	General Availability	General Availability
CSI automatic migration (AWS EBS, GCP disk)	Technology Preview	General Availability	General Availability
CSI inline ephemeral volumes	Technology Preview	Technology Preview	General Availability
CSI generic ephemeral volumes	Not Available	General Availability	General Availability
IBM Power Virtual Server Block CSI Driver Operator	Not Available	Not Available	Technology Preview
Automatic device discovery and provisioning with Local Storage Operator	Technology Preview	Technology Preview	Technology Preview
NFS support for Azure File CSI Operator Driver	Not Available	Generally Available	Generally Available

Installation Technology Preview features

Table 1.18. Installation Technology Preview tracker

Feature	4.11	4.12	4.13
Adding kernel modules to nodes with kvc	Technology Preview	Technology Preview	Technology Preview
IBM Cloud VPC clusters (x86_64)	Technology Preview	General Availability	General Availability

Feature	4.11	4.12	4.13
Selectable Cluster Inventory	Technology Preview	Technology Preview	Technology Preview
Multi-architecture compute machines	Not Available	Technology Preview	General Availability
Mount shared entitlements in BuildConfigs in RHEL	Technology Preview	Technology Preview	Technology Preview
Agent-based OpenShift Container Platform Installer	Not Available	General Availability	General Availability
Enabling NIC partitioning for SR-IOV devices	Not Available	Not Available	Technology Preview
Azure Tagging	Not Available	Not Available	Technology Preview
GCP Confidential VMs	Not Available	Not Available	Technology Preview

Node Technology Preview features

Table 1.19. Nodes Technology Preview tracker

Feature	4.11	4.12	4.13
Non-preempting priority classes	General Availability	General Availability	General Availability
Linux Control Group version 2 (cgroup v2)	Developer Preview	Technology Preview	General Availability
crun container runtime	Not Available	Technology Preview	General Availability
Cron job time zones	Not Available	Technology Preview	Technology Preview

Multi-Architecture Technology Preview features

Table 1.20. Multi-Architecture Technology Preview tracker

Feature	4.11	4.12	4.13

Feature	4.11	4.12	4.13
kdump on **arm64** architecture	Not Available	Technology Preview	Technology Preview
kdump on **s390x** architecture	Technology Preview	Technology Preview	Technology Preview
kdump on **ppc64le** architecture	Technology Preview	Technology Preview	Technology Preview
IBM Secure Execution on IBM Z and IBM® LinuxONE	Not Available	Technology Preview	General Availability
IBM Power Virtual Server using installer-provisioned infrastructure	Not Available	Not Available	Technology Preview

Specialized hardware and driver enablement Technology Preview features

Table 1.21. Specialized hardware and driver enablement Technology Preview tracker

Feature	4.11	4.12	4.13
Driver Toolkit	Technology Preview	Technology Preview	General Availability
Special Resource Operator (SRO)	Technology Preview	Technology Preview	Not Available
Hub and spoke cluster support	Not Available	Not Available	Technology Preview

Web console Technology Preview features

Table 1.22. Web console Technology Preview tracker

Feature	4.11	4.12	4.13
Dynamic Plug-ins	Technology Preview	General Availability	General Availability

Scalability and performance Technology Preview features

Table 1.23. Scalability and performance Technology Preview tracker

Feature	4.11	4.12	4.13

Feature	4.11	4.12	4.13
Hyperthreading-aware CPU manager policy	Technology Preview	Technology Preview	Technology Preview
Node Observability Operator	Not Available	Technology Preview	Technology Preview
factory-precaching-cli tool	Not Available	Not Available	Technology Preview
Single-node OpenShift cluster expansion with worker nodes	Not Available	Technology Preview	General Availability
Topology Aware Lifecycle Manager (TALM)	Technology Preview	Technology Preview	General Availability
Mount namespace encapsulation	Not Available	Not Available	Technology Preview
NUMA-aware scheduling with NUMA Resources Operator	Technology Preview	Technology Preview	General Availability
HTTP transport replaces AMQP for PTP and bare-metal events	Not Available	Not Available	Technology Preview
Intel E810 Westport Channel NIC as PTP grandmaster clock	Not Available	Not Available	Technology Preview
Workload partitioning for three-node clusters and standard clusters	Not Available	Not Available	Technology Preview

Operator Technology Preview features

Table 1.24. Operator Technology Preview tracker

Feature	4.11	4.12	4.13
Hybrid Helm Operator	Technology Preview	Technology Preview	Technology Preview
Java-based Operator	Not Available	Technology Preview	Technology Preview
Multi-cluster Engine Operator	Technology Preview	Technology Preview	Technology Preview
Node Observability Operator	Not Available	Not Available	Technology Preview

Feature	4.11	4.12	4.13
Network Observability Operator	Not Available	General Availability	General Availability
Platform Operators	Not Available	Technology Preview	Technology Preview
RukPak	Not Available	Not Available	Technology Preview
Cert-manager Operator	Technology Preview	General Availability	General Availability

Monitoring Technology Preview features

Table 1.25. Monitoring Technology Preview tracker

Feature	4.11	4.12	4.13
Alert routing for user-defined projects monitoring	Technology Preview	General Availability	General Availability
Alerting rules based on platform monitoring metrics	Not Available	Technology Preview	Technology Preview
Metrics Collection Profiles	Not Available	Not Available	Technology Preview

Red Hat OpenStack Platform (RHOSP) Technology Preview features

Table 1.26. RHOSP Technology Preview tracker

Feature	4.11	4.12	4.13
Support for RHOSP DCN	Technology Preview	General Availability	General Availability
Support for external cloud providers for clusters on RHOSP	Technology Preview	General Availability	General Availability

Architecture Technology Preview features

Table 1.27. Architecture Technology Preview tracker

Feature	4.11	4.12	4.13
Hosted control planes for OpenShift Container Platform on bare metal	Not Available	Technology Preview	Technology Preview
Hosted control planes for OpenShift Container Platform on Amazon Web Services (AWS)	Technology Preview	Technology Preview	Technology Preview
Hosted control planes for OpenShift Container Platform on OpenShift Virtualization	Not Available	Not Available	Technology Preview

Machine management Technology Preview features

Table 1.28. Machine management Technology Preview tracker

Feature	4.11	4.12	4.13
Managing machines with the Cluster API	Technology Preview	Technology Preview	Technology Preview
Cloud controller manager for Alibaba Cloud	Technology Preview	Technology Preview	Technology Preview
Cloud controller manager for Amazon Web Services	Technology Preview	Technology Preview	Technology Preview
Cloud controller manager for Google Cloud Platform	Technology Preview	Technology Preview	Technology Preview
Cloud controller manager for IBM Cloud	Technology Preview	General Availability	General Availability
Cloud controller manager for IBM Cloud Power VS	Not Available	Technology Preview	Technology Preview
Cloud controller manager for Microsoft Azure	Technology Preview	Technology Preview	Technology Preview
Cloud controller manager for Nutanix	Not Available	Not Available	General Availability
Cloud controller manager for Red Hat OpenStack Platform (RHOSP)	Technology Preview	General Availability	General Availability
Cloud controller manager for VMware vSphere	Technology Preview	Technology Preview	General Availability

Authentication and authorization Technology Preview features

Table 1.29. Authentication and authorization Technology Preview tracker

Table 1.29. Authentication and authorization Technology Preview tracker

Feature	4.11	4.12	4.13
Pod security admission restricted enforcement	Not Available	Technology Preview	Technology Preview

Machine Config Operator Technology Preview features

Table 1.30. Machine Config Operator Technology Preview tracker

Feature	4.11	4.12	4.13
Red Hat Enterprise Linux CoreOS (RHCOS) image layering	Not Available	Technology Preview	General Availability

1.8. KNOWN ISSUES

- In OpenShift Container Platform 4.1, anonymous users could access discovery endpoints. Later releases revoked this access to reduce the possible attack surface for security exploits because some discovery endpoints are forwarded to aggregated API servers. However, unauthenticated access is preserved in upgraded clusters so that existing use cases are not broken.
  If you are a cluster administrator for a cluster that has been upgraded from OpenShift Container Platform 4.1 to 4.13, you can either revoke or continue to allow unauthenticated access. Unless there is a specific need for unauthenticated access, you should revoke it. If you do continue to allow unauthenticated access, be aware of the increased risks.

WARNING

If you have applications that rely on unauthenticated access, they might receive HTTP **403** errors if you revoke unauthenticated access.

Use the following script to revoke unauthenticated access to discovery endpoints:

```
## Snippet to remove unauthenticated group from all the cluster role bindings
$ for clusterrolebinding in cluster-status-binding discovery system:basic-user
system:discovery system:openshift:discovery ;
do
### Find the index of unauthenticated group in list of subjects
index=$(oc get clusterrolebinding ${clusterrolebinding} -o json | jq 'select(.subjects!=null) |
.subjects | map(.name=="system:unauthenticated") | index(true)');
### Remove the element at index from subjects array
oc patch clusterrolebinding ${clusterrolebinding} --type=json --patch "[{'op': 'remove','path':
'/subjects/$index'}]";
done
```

This script removes unauthenticated subjects from the following cluster role bindings:

- **cluster-status-binding**
- **discovery**
- **system:basic-user**
- **system:discovery**
- **system:openshift:discovery**

(BZ#1821771)

- The **oc annotate** command does not work for LDAP group names that contain an equal sign (**=**), because the command uses the equal sign as a delimiter between the annotation name and value. As a workaround, use **oc patch** or **oc edit** to add the annotation. (BZ#1917280)

- Adding a Git Repository and configuring it with a GitLab and Bitbucket **pipeline-as-code** repository creates an invalid repository resource. As a result, the **spec.git_provider.url** Git provider URL is removed for GitLab and Bitbucket providers.
  Workaround: Add the mandatory **spec.git_provider.user** field for Bitbucket. In addition, select either **Git access token** or **Git access token secret** to continue adding a Git Repository. (OCPBUGS-7036)

- Currently, a certificate compliance issue, specifically outputted as **x509: certificate is not standards compliant**, exists when you run the installation program on macOS for the purposes of installing an OpenShift Container Platform cluster on VMware vSphere. This issue relates to a known issue with the **golang** compiler in that the compiler does not recognize newly supported macOS certificate standards. No workaround exists for this issue. (OSDOCS-5694)

- When you include more than three failure domains in the **ControlPlaneMachineSet** definition, the load balancing algorithm does not prioritize existing control plane machines. If you add a fourth failure domain that is alphabetically higher in precedence than the existing three failure domains to the definition, the fourth failure domain takes precedence over any existing failure domains. This behavior can apply rolling forward updates to a control plane machine. You can prevent this issue by setting existing in-use failure domains to a higher precedence than the new and unused failure domains. This action stabilizes each control plane machine during the course of adding more than three failure domains to the definition. (OCPBUGS-11968)

- On a single-node OpenShift instance, rebooting without draining the node to remove all of the running pods can cause issues with workload container recovery. After the reboot, the workload restarts before all the device plugins are ready, resulting in resources not being available or the workload running on the wrong NUMA node. The workaround is to restart the workload pods when all of the device plugins have re-registered themselves during the reboot recovery procedure. (OCPBUGS-2180)

- An error might occur when deleting a pod that uses an SR-IOV netdevice. This error is caused by a change in RHEL 9 where the previous name of a network interface is added to its alternative names list when it is renamed. As a consequence, when a pod attached to an SR-IOV virtual function (VF) is deleted, the VF returns to the pool with a new unexpected name, for example, **dev69**, instead of its original name, for example, **ensf0v2**. Although this error is non-fatal, Multus and SR-IOV logs might show the error while the system recovers on its own. Deleting the pod might take a few extra seconds due to this error. (OCPBUGS-11281)

- An incorrect priority class name and syntax error in the YAML definition of the daemon set responsible for updating the interface-specific safe sysctl is preventing the modification of the safe sysctl list for interfaces by using the **cni-sysctl-allowlist** config map in the **openshift-multus** namespace.

Workaround: Manually or by using a daemon set, modify the file **/etc/cni/tuning/allowlist.conf** on the nodes to address this issue. (OCPBUGS-11046)

- A new feature introduced in OpenShift Container Platform 4.12 that enables UDP GRO also causes all veth devices to have one RX queue per available CPU (previously each veth had one queue). Those queues are dynamically configured by Open Virtual Network, and there is no synchronization between latency tuning and this queue creation. The latency tuning logic monitors the veth NIC creation events and starts configuring the RPS queue CPU masks before all the queues are properly created. This means that some of the RPS queue masks are not configured. Since not all NIC queues are configured properly there is a chance of latency spikes in a real-time application that uses timing-sensitive CPUs for communicating with services in other containers. Applications that do not use kernel networking stack are not affected. (OCPBUGS-4194)

- The Cluster Network Operator (CNO) controller is monitoring more resources than it needs to. As a result, its reconciler is being triggered too frequently, causing a much higher rate of API requests than necessary. There is approximately 1 config map access request made every second. This increases the load on both the CNO and the **kube-apiserver**. (OCPBUGS-11565)

- For OpenShift Container Platform 4.13, the Driver Toolkit (DTK) container image requires the **ubi9** image as the second layer of the software stack for building driver containers. If you attempt to use the **ubi8** image as the second layer in the your software stack, you will receive a build error. (OCPBUGS-11120)

- In some OpenShift Container Platform installations on the vSphere platform when using the CSI driver, the vSphere CSI driver might not come up correctly because during startup it fails to retrieve information about a node from vCenter, and then the CSI driver does not retry. Workaround: By using SSH to connect to the node that is the current leader of the vsphere-syncer process and restarting the vsphere-syncer container (using crictl), this issue can be mitigated and the driver successfully comes up. (OCPBUGS-13385)

- For OpenShift Container Platform 4.13, installing version 4.13 on top of Red Hat OpenStack Platform (RHOSP) 16.2 with baremetal workers fails because baremetal workers are not able to boot from the Red Hat Enterprise Linux CoreOS (RHCOS) image that comes with OpenShift 4.13. The fundamental issue is the RHCOS image lacks a byte order marker. These fixes are planned for the next 16.2 build. (OCPBUGS-13395)

- Due to a known issue in RHEL 9.2, you cannot use persistent volumes on a GCP cluster with Confidential VMs. (OCPBUGS-7582)

- Red Hat Enterprise Linux (RHEL) workers running in a OpenShift Container Platform 4.12 cluster with **openvswitch2.15** installed fail when upgrading to OpenShift Container Platform 4.13. The **upgrade.yml** playbook fails with the following error message **package openvswitch2.17-2.17.0-88.el8fdp.x86_64 conflicts with openvswitch2.15 provided by openvswitch2.15-2.15.0-136.el8fdp.x86_64**.
  To work around this issue, before you update to OpenShift Container Platform 4.13, manually remove the **openvswitch2.15** package and install the **openvswitch2.17** package. Then, run the **upgrade.yml** playbook to update RHEL workers and complete the update process. (OCPBUGS-11677)

- There is a disk discovery delay when attaching storage to workloads. (OCPBUGS-11149)

- When updating from OpenShift Container Platform 4.12 to 4.13, the Mellanox NIC renames SR-IOV network node policies such as **ens7f0** to **ens7f0np0**. This name change is because of the update to the RHEL 9 kernel. Consequently, virtual functions (VFs) cannot be created because

the interface cannot be found. Your SR-IOV network node policies must take this renaming into account. For example, if **ens7f0** is referenced in your policy, add **ens7f0np0** to your policy before updating.
To work around this issue, you must manually edit the **SriovNetworkNodePolicy** custom resource (CR) to add **ens7f0np0** before updating to OpenShift Container Platform 4.13. (OCPBUGS-13186) The following code provides an example of the policy updates with both names being added to **SriovNetworkNodePolicy** to ensure compatibility:

```
# ...
deviceType: netdevice
nicSelector:
  deviceID: “101d”
  pfNames:
    - ens7f0
    - ens7f0np0
  vendor: ‘15b3’
nodeSelector:
  feature.node.kubernetes.io/sriov-capable: ‘true’
numVfs: 4
# ...
```

- Resetting a MAC address on an SR-IOV virtual function (VF) upon pod deletion might fail for Intel E810 NICs. As a result, creating a pod with an SR-IOV VF might take up to 2 minutes on Intel E810 NIC cards. (OCPBUGS-5892)

- If you specify an invalid subscription channel in the subscription policy that you use to perform a cluster upgrade, the Topology Aware Lifecycle Manager (TALM) indicates that the upgrade is successful immediately after TALM enforces the policy because the **Subscription** resource remains in the **AtLatestKnown** state. (OCPBUGS-9239)

- After a system crash, **kdump** fails to generate the **vmcore** crash dump file on HPE Edgeline e920t and HPE ProLiant DL110 Gen10 servers with Intel E810 NIC and ice driver installed. (RHELPLAN-138236)

- In GitOps ZTP, when you provision a managed cluster that contains more than a single node using a **SiteConfig** CR, disk partition fails when one or more nodes has a **diskPartition** resource configured in the **SiteConfig** CR. (OCPBUGS-9272)

- In clusters configured with PTP boundary clocks (T-BC) and deployed DU applications, messages are intermittently not sent from the follower interface of the T-BC on the vDU host for periods of up to 40 seconds. The rate of errors in the logs can vary. An example error log is below:

  Example output

  ```
  2023-01-15T19:26:33.017221334+00:00 stdout F phc2sys[359186.957]: [ptp4l.0.config] nothing to synchronize
  ```

  (RHELPLAN-145492)

- When you install a single-node OpenShift cluster using GitOps ZTP and configure PTP and bare-metal events with HTTP transport, the **linuxptp-daemon** daemon pod intermittently fails to deploy. The required **PersistentVolumeClaim** (**PVC**) resource is created but is not mounted in the pod. The following volume mount error is reported:

  Example output

Example output

```
mount: /var/lib/kubelet/plugins/kubernetes.io/local-volume/mounts/local-pv-bc42d358:
mount(2) system call failed: Structure needs cleaning.
```

To workaround the issue, delete the **cloud-event-proxy-store-storage-class-http-events PVC** CR and re-deploy the PTP Operator. (OCPBUGS-12358)

- During GitOps Zero Touch Provisioning (ZTP) provisioning of a single-node OpenShift managed cluster with secure boot enabled in the **SiteConfig** CR, multiple **ProvisioningError** errors are reported for the **BareMetalHost** CR during host provisioning. The error indicates that the secure boot setting is successfully applied in the Baseboard Management Controller (BMC), but the host is not powered on after the **BareMetalHost** CR is applied. To workaround this issue, perform the following steps:

  1. Reboot the host. This ensures that the GitOps ZTP pipeline applies the secure boot setting.
  2. Restart GitOps ZTP provisioning of the cluster with the same configuration.

  (OCPBUGS-8434)

- After installing a dual-stack GitOps ZTP hub cluster, enabling dual-stack Virtual IP addresses (VIPs), and enabling the **virtualMediaViaExternalNetwork** flag in a **Provisioning** CR, the **IRONIC_EXTERNAL_URL_V6** environment variable incorrectly gets assigned an IPv4 address. (OCPBUGS-4248)

- ZT servers have the **BiosRegistry** language set to **en-US** instead of **en**. This causes a problem during GitOps ZTP provisioning of managed cluster hosts. The **FirmwareSchema** CR generated for the ZT server doesn't have the **allowable_values**, **attribute_type**, and **read_only** fields populated. (OCPBUGS-4388)

- In OpenShift Container Platform version 4.13.0, an error occurs when you try to install a cluster with the Agent-based installer. After the read disk stage, an error is returned and the cluster installation gets stuck. This error has been detected on HPE ProLiant Gen10 servers. (OCPBUGS-13138)

- RFC2544 performance tests show that the **Max delay** value for a packet to traverse the network is over the minimum threshold. This regression is found in OpenShift Container Platform 4.13 clusters running the Telco RAN DU profile. (OCPBUGS-13224)

- Performance tests run on a single-node OpenShift cluster with OpenShift Container Platform 4.13 installed show an **oslat** maximum latency result greater than 20 microseconds. (RHELPLAN-155443)

- Performance tests run on a single-node OpenShift cluster with OpenShift Container Platform 4.13 installed show a **cyclictest** maximum latency result greater than 20 microseconds. (RHELPLAN-155460)

- The **cpu-load-balancing.crio.io: "disable"** annotation associated with the low latency tuning described in Disabling CPU load balancing for DPDK does not work on systems that do not have workload partitioning configured. More specifically, this affects clusters where the infrastructure does not set the **cpuPartitioningMode** to the **AllNodes** value as described in Workload partitioning.
  This affects the achievable latency of such clusters and might prevent proper operation of low latency workloads. (OCPBUGS-13163)

- OpenShift Container Platform 4.12 clusters on the Nutanix platform may have an

Upgradeable=False condition if they are missing configuration needed for the Nutanix Cloud Control Manager (CCM). To resolve this condition, see: How to create the ConfigMaps and Secrets needed to upgrade to OpenShift 4.13 when using Nutanix as a Platform.

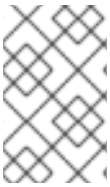
- Currently, when using a persistent volume (PV) that contains a very large number of files, the pod might not start or can take an excessive amount of time to start. For more information, see this knowledge base article. (**BZ1987112**)

- Creating pods with Azure File NFS volumes that are scheduled to the control plane node causes the mount to be denied. (**OCPBUGS-18581**)
  To work around this issue: If your control plane nodes are schedulable, and the pods can run on worker nodes, use **nodeSelector** or Affinity to schedule the pod in worker nodes.

1.9. ASYNCHRONOUS ERRATA UPDATES

Security, bug fix, and enhancement updates for OpenShift Container Platform 4.13 are released as asynchronous errata through the Red Hat Network. All OpenShift Container Platform 4.13 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 through 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 4.13. Versioned asynchronous releases, for example with the form OpenShift Container Platform 4.13.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.

1.9.1. RHSA-2023:1326 - OpenShift Container Platform 4.13.0 image release, bug fix, and security update advisory

Issued: 2023-05-17

OpenShift Container Platform release 4.13.0, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2023:1326 advisory. The RPM packages that are included in the update are provided by the RHSA-2023:1325 advisory.

Space precluded documenting all of the container images for this release in the advisory.

You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.0 --pullspecs
```

1.9.2. RHSA-2023:3304 - OpenShift Container Platform 4.13.1 bug fix and security update

Issued: 2023-05-30

OpenShift Container Platform release 4.13.1, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2023:3304 advisory. The RPM packages that are included in the update are provided by the RHSA-2023:3303 advisory.

Space precluded documenting all of the container images for this release in the advisory.

You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.1 --pullspecs
```

1.9.2.1. Bug fixes

- Previously, assisted installations could encounter a transient error. If that error occurred, the installation failed to recover. With this update, transient errors are re-tried correctly. (OCPBUGS-13138)
- Previously, oc-mirror OpenShift CLI (**oc**) plugin would fail with a **401 unauthorized** error for some registries when a nested path exceeded the expected maximum path-components. With this update, the default integer of the **--max-nested-paths** flag is set to 0 (no limit). As a result, the generated **ImageContentSourcePolicy** will contain source and mirror references up to the repository level as opposed to the namespace level used by default. (OCPBUGS-13591)

1.9.2.2. Updating

To update an existing OpenShift Container Platform 4.13 cluster to this latest release, see Updating a cluster using the CLI.

1.9.3. RHSA-2023:3367 - OpenShift Container Platform 4.13.2 bug fix and security update

Issued: 2023-06-07

OpenShift Container Platform release 4.13.2, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2023:3367 advisory. The RPM packages that are included in the update are provided by the RHSA-2023:3366 advisory.

Space precluded documenting all of the container images for this release in the advisory.

You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.2 --pullspecs
```

1.9.3.1. Updating

To update an existing OpenShift Container Platform 4.13 cluster to this latest release, see Updating a cluster using the CLI.

1.9.4. RHSA-2023:3537 - OpenShift Container Platform 4.13.3 bug fix and security update

Issued: 2023-06-13

OpenShift Container Platform release 4.13.3, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2023:3537 advisory. The RPM packages that are included in the update are provided by the RHSA-2023:3536 advisory.

Space precluded documenting all of the container images for this release in the advisory.

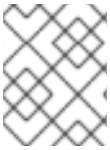
You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.3 --pullspecs
```

1.9.4.1. Features

1.9.4.1.1. Support for iPXE network booting with ZTP

GitOps Zero Touch Provisioning (ZTP) uses the Bare Metal Operator (BMO) to boot Red Hat Enterprise Linux CoreOS (RHCOS) on the target host as part of the deployment of spoke clusters. With this update, GitOps ZTP leverages the capabilities of the BMO by adding the option of Preboot Execution Environment (iPXE) network booting for these RHCOS installations.



NOTE

To use iPXE network booting, you must use Red Hat Advanced Cluster Management (RHACM) 2.8 or later.

For more information, see Deploying a managed cluster with SiteConfig and GitOps ZTP .

1.9.4.2. Bug fixes

- Previously on single-node OpenShift, in case of node reboot there was a race condition that could result in admission of application pods requesting devices on the node even if devices were unhealthy or unavailable to be allocated. This resulted in runtime failures when the application tried to access devices. With this update, the resources requested by the pod are only allocated if the device plugin has registered itself to kubelet and healthy devices are present on the node to be allocated.
  If these conditions are not met, the pod can fail at admission with **UnexpectedAdmissionError** error, which is an expected behavior. If the application pod is part of deployments, in case of failure subsequent pods are spun up and ultimately successfully run when devices are suitable to be allocated. (OCPBUGS-14438)

- Previously, client TLS (mTLS) was configured on an Ingress Controller, and the certificate authority (CA) in the client CA bundle required more than 1MB of certificate revocation list (CRLs) to be downloaded. The CRL **ConfigMap** object size limitations prevented updates from occurring. As a result of the missing CRLs, connections with valid client certificates may have been rejected with the error **unknown ca**. With this update, the CRL **ConfigMap** for each Ingress Controller no longer exists; instead, each router pod directly downloads CRLs, ensuring connections with valid client certificates are no longer rejected. (OCPBUGS-13967)

- Previously, because client TLS (mTLS) was configured on an Ingress Controller, mismatches between the distributing certificate authority (CA) and the issuing CA caused the incorrect

certificate revocation list (CRL) to be downloaded. As a result, the incorrect CRL was downloaded instead of the correct CRL, causing connections with valid client certificates to be rejected with the error message **unknown ca**. With this update, downloaded CRLs are now tracked by the CA that distributes them. This ensures that valid client certificates are no longer rejected. (OCPBUGS-13964)

1.9.4.3. Updating

To update an existing OpenShift Container Platform 4.13 cluster to this latest release, see Updating a cluster using the CLI.

1.9.5. RHSA-2023:3614 - OpenShift Container Platform 4.13.4 bug fix and security update

Issued: 2023-06-23

OpenShift Container Platform release 4.13.4, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2023:3614 advisory. The RPM packages that are included in the update are provided by the RHSA-2023:3612 advisory.

Space precluded documenting all of the container images for this release in the advisory.

You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.4 --pullspecs
```

1.9.5.1. Bug fixes

- Previously, you could not use persistent volume storage on a cluster with Confidential virtual machines (VMs) on Google Cloud Platform (GCP). This issue persists with OpenShift Container Platform 4.13.3 and earlier versions. From OpenShift Container Platform 4.13.4 and later versions, you can now use persistent volume storage on a cluster with Confidential VMs on GCP. (OCPBUGS-11768)

1.9.5.2. Updating

To update an existing OpenShift Container Platform 4.13 cluster to this latest release, see Updating a cluster using the CLI.

1.9.6. RHSA-2023:4091 - OpenShift Container Platform 4.13.5 bug fix and security update

Issued: 2023-07-20

OpenShift Container Platform release 4.13.5, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2023:4091 advisory. The RPM packages that are included in the update are provided by the RHSA-2023:4093 advisory.

Space precluded documenting all of the container images for this release in the advisory.

You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.5 --pullspecs
```

1.9.6.1. Bug fixes

- Previously, the Gateway API feature did not provide DNS records with a trailing dot for the Gateway domain. This caused the status of the DNS record to never become available on the GCP platform. With this update, the DNS records for Gateway API Gateways are properly provisioned and the Gateway API feature works on GCP because the gateway service dns controller now adds a trailing dot if it is missing in the domain. (OCPBUGS-15434)

- Previously, if you used the **Pipelines** page of the **Developer** console to add a repository, and you entered a GitLab or Bitbucket Pipelines as Code repository URL as the **Git Repo URL**, the created **Repository** resource was invalid. This was caused by a missing schema issue in the **git_provider.url** spec, which is now fixed. (OCPBUGS-15410)

- In this release, the **git_provider.user** spec has been added for Pipelines as Code **Repository** objects. This spec requires you to provide a username if the Git provider is Bitbucket. (OCPBUGS-15410)

- In this release, the **Secret** field in the **Pipelines → Create → Add Git Repository** page is now mandatory. You must click **Show configuration options**, and then configure either a Git access token or a Git access token secret for your repository. (OCPBUGS-15410)

- Previously, if you tried to edit a Helm chart repository in the **Developer** console by navigating to **Helm**, clicking the **Repositories** tab, then selecting **Edit HelmChartRepository** through the kebab menu for your Helm chart repository, an **Error** page was displayed that showed a **404: Page Not Found** error. This was caused by a component path that was not up to date. This issue is now fixed. (OCPBUGS-15130)

1.9.6.2. Updating

To update an existing OpenShift Container Platform 4.13 cluster to this latest release, see Updating a cluster using the CLI.

1.9.7. RHSA-2023:4226 - OpenShift Container Platform 4.13.6 bug fix and security update

Issued: 2023-07-27

OpenShift Container Platform release 4.13.6, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2023:4226 advisory. The RPM packages that are included in the update are provided by the RHBA-2023:4229 advisory.

Space precluded documenting all of the container images for this release in the advisory.

You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.6 --pullspecs
```

1.9.7.1. Updating

To update an existing OpenShift Container Platform 4.13 cluster to this latest release, see Updating a cluster using the CLI.

1.9.8. RHSA-2023:4456 - OpenShift Container Platform 4.13.8 bug fix and security update

Issued: 2023-08-08

OpenShift Container Platform release 4.13.8, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2023:4456 advisory. The RPM packages that are included in the update are provided by the RHSA-2023:4459 advisory.

Space precluded documenting all of the container images for this release in the advisory.

You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.8 --pullspecs
```

1.9.8.1. Bug fixes

- Previously, the real load balancer address in the Red Hat OpenStack Platform (RHOSP) was not visible. With this update, the real load balancer address has been added and is visible in the RHOSP load balancer object annotation. (**OCPBUGS-15973**)

1.9.8.2. Updating

To update an existing OpenShift Container Platform 4.13 cluster to this latest release, see Updating a cluster using the CLI.

1.9.9. RHSA-2023:4603 - OpenShift Container Platform 4.13.9 bug fix and security update

Issued: 2023-08-16

OpenShift Container Platform release 4.13.9, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2023:4603 advisory. The RPM packages that are included in the update are provided by the RHBA-2023:4606 advisory.

Space precluded documenting all of the container images for this release in the advisory.

You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.9 --pullspecs
```

1.9.9.1. Updating

To update an existing OpenShift Container Platform 4.13 cluster to this latest release, see Updating a cluster using the CLI.

1.9.10. RHSA-2023:4731 - OpenShift Container Platform 4.13.10 bug fix and security update

Issued: 2023-08-30

OpenShift Container Platform release 4.13.10, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2023:4731 advisory. The RPM packages that are included in the update are provided by the RHBA-2023:4734 advisory.

Space precluded documenting all of the container images for this release in the advisory.

You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.10 --pullspecs
```

1.9.10.1. Bug fixes

- Previously, clusters using Mint mode and had their root secret removed would encounter an issue during an upgrade from 4.13.8 to 4.13.9. This was caused by a modification in the credentials request of the Ingress Operator that was backported to 4.13.9. With this update, these clusters have no issues updating to versions 4.13.9 and greater. (**OCPBUGS-17733**)

1.9.10.2. Known issue

- The addition of a new feature in OpenShift Container Platform 4.12 that enables UDP generic receive offload (GRO) also causes all virtual ethernet pair (veth) devices to have one RX queue per available CPU. Previously each veth had one queue. Those queues are dynamically configured by Open Virtual Network (OVN) and there is no synchronization between latency tuning and this queue creation.
  The latency tuning logic monitors the veth NIC creation events and starts configuring the Receive Packet Steering (RPS) queue CPU masks before all the queues are properly created. This means that some of the RPS queue masks are not configured. Since not all NIC queues are configured properly, there is a chance of latency spikes in a real-time application that uses timing sensitive CPUs for communicating with services in other containers. Applications that do not use kernel networking stack are not affected. (**OCPBUGS-17794**)

1.9.10.3. Updating

To update an existing OpenShift Container Platform 4.13 cluster to this latest release, see Updating a cluster using the CLI.

1.9.11. RHBA-2023:4905 - OpenShift Container Platform 4.13.11 bug fix

Issued: 2023-09-05

OpenShift Container Platform release 4.13.11 is now available. The list of bug fixes that are included in the update is documented in the RHBA-2023:4905 advisory.

Space precluded documenting all of the container images for this release in the advisory.

You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.11 --pullspecs
```

1.9.11.1. Updating

To update an existing OpenShift Container Platform 4.13 cluster to this latest release, see Updating a cluster using the CLI.

1.9.12. RHBA-2023:5011 - OpenShift Container Platform 4.13.12 bug fix

Issued: 2023-09-12

OpenShift Container Platform release 4.13.12 is now available. The list of bug fixes that are included in the update is documented in the RHBA-2023:5011 advisory. The RPM packages that are included in the update are provided by the RHBA-2023:5014 advisory.

Space precluded documenting all of the container images for this release in the advisory.

You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.12 --pullspecs
```

1.9.12.1. Features

1.9.12.1.1. Exclude SR-IOV network topology for NUMA-aware scheduling

With this release, you can exclude advertising the Non-Uniform Memory Access (NUMA) node for the SR-IOV network to the Topology Manager. By not advertising the NUMA node for the SR-IOV network, you can permit more flexible SR-IOV network deployments during NUMA-aware pod scheduling.

For example, in some scenarios, it is a priority to maximize CPU and memory resources for a pod on a single NUMA node. By not providing a hint to the Topology Manager about the NUMA node for the pod's SR-IOV network resource, the Topology Manager can deploy the SR-IOV network resource and the pod CPU and memory resources to different NUMA nodes. In earlier OpenShift Container Platform releases, the Topology Manager attempted to place all resources on the same NUMA node only.

For more information about this more flexible SR-IOV network deployment during NUMA-aware pod scheduling, see Exclude the SR-IOV network topology for NUMA-aware scheduling .

1.9.12.1.2. Using a custom Red Hat Enterprise Linux CoreOS (RHCOS) image for a Google Cloud Provider cluster

By default, the installation program downloads and installs the Red Hat Enterprise Linux CoreOS (RHCOS) image that is used to start control plane and compute machines. With this enhancement, you can now override the default behavior by modifying the installation configuration file (install-config.yaml) to specify a custom RHCOS image. Before you deploy the cluster, you can modify the following installation parameters:

- **controlPlane.platform.gcp.osImage.project**
- **controlPlane.platform.gcp.osImage.name**
- **compute.platform.gcp.osImage.project**
- **compute.platform.gcp.osImage.name**
- **platform.gcp.defaultMachinePlatform.osImage.project**
- **platform.gcp.defaultMachinePlatform.osImage.name**

For more information about these parameters, see Additional Google Cloud Platform configuration parameters.

1.9.12.1.3. Support for allocateLoadBalancerNodePorts in Service object of Network API

The **ServiceSpec** component in Network API under the **Service** object describes the attributes that a user creates on a service. The **allocateLoadBalancerNodePorts** attribute within the **ServiceSpec**

component is now supported in OpenShift Container Platform 4.13. The **allocateLoadBalancerNodePorts** attribute defines whether the **NodePorts** will be automatically allocated for services of the **LoadBalancer** type.

1.9.12.2. Bug fixes

- Previously, the OpenShift Container Platform router directed traffic to a route with a weight of 0 when it had only one back end. With this update, the router will not send traffic to routes with a single back end with weight 0. (OCPBUGS-17107)

1.9.12.3. Updating

To update an existing OpenShift Container Platform 4.13 cluster to this latest release, see Updating a cluster using the CLI.

1.9.13. RHSA-2023:5155 - OpenShift Container Platform 4.13.13 bug fix and security update

Issued: 2023-09-20

OpenShift Container Platform release 4.13.13, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2023:5155 advisory. The RPM packages that are included in the update are provided by the RHBA-2023:5158 advisory.

Space precluded documenting all of the container images for this release in the advisory.

You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.13 --pullspecs
```

1.9.13.1. Updating

To update an existing OpenShift Container Platform 4.13 cluster to this latest release, see Updating a cluster using the CLI.

1.9.14. RHBA-2023:5382 - OpenShift Container Platform 4.13.14 bug fix

Issued: 2023-10-05

OpenShift Container Platform release 4.13.14, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHBA-2023:5382 advisory. The RPM packages that are included in the update are provided by the RHBA-2023:5388 advisory.

Space precluded documenting all of the container images for this release in the advisory.

You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.14 --pullspecs
```

1.9.14.1. Updating

To update an existing OpenShift Container Platform 4.13 cluster to this latest release, see Updating a cluster using the CLI.

1.9.15. RHBA-2023:5467 - OpenShift Container Platform 4.13.15 bug fix

Issued: 2023-10-10

OpenShift Container Platform release 4.13.15, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHBA-2023:5467 advisory. The RPM packages that are included in the update are provided by the RHBA-2023:5470 advisory.

Space precluded documenting all of the container images for this release in the advisory.

You can view the container images in this release by running the following command:

```
$ oc adm release info 4.13.15 --pullspecs
```

1.9.15.1. Updating

To update an existing OpenShift Container Platform 4.13 cluster to this latest release, see Updating a cluster using the CLI.