OpenShift Container Platform 4.16

Release notes

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

Last Updated: 2024-08-29

OpenShift Container Platform 4.16 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 4.16 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. 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-2024:0041) is now available. This release uses Kubernetes 1.29 with CRI-O runtime. New features, changes, and known issues that pertain to OpenShift Container Platform 4.16 are included in this topic.

OpenShift Container Platform 4.16 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 4.16 is supported on Red Hat Enterprise Linux (RHEL) 8.8-8.10, and on Red Hat Enterprise Linux CoreOS (RHCOS) 9.4.

You must use RHCOS machines for the control plane, and you can use either RHCOS or RHEL for compute machines. RHEL machines are deprecated in OpenShift Container Platform 4.16 and will be removed in a future release.

Starting from OpenShift Container Platform 4.14, the Extended Update Support (EUS) phase for even-numbered releases increases the total available lifecycle to 24 months on all supported architectures, including **x86_64**, 64-bit ARM (**aarch64**), IBM Power® (**ppc64le**), and IBM Z® (**s390x**) architectures. Beyond this, Red Hat also offers a 12-month additional EUS add-on, denoted as *Additional EUS Term 2*, that extends the total available lifecycle from 24 months to 36 months. The Additional EUS Term 2 is available on all architecture variants of OpenShift Container Platform.

For more information about support for all versions, see the Red Hat OpenShift Container Platform Life Cycle Policy.

Commencing with the 4.16 release, Red Hat is simplifying the administration and management of Red Hat shipped cluster Operators with the introduction of three new life cycle classifications; Platform Aligned, Platform Agnostic, and Rolling Stream. These life cycle classifications provide additional ease and transparency for cluster administrators to understand the life cycle policies of each Operator and form cluster maintenance and upgrade plans with predictable support boundaries. For more information, see OpenShift Operator Life Cycles.

OpenShift Container Platform is designed for FIPS. When running Red Hat Enterprise Linux (RHEL) or Red Hat Enterprise Linux CoreOS (RHCOS) booted in FIPS mode, OpenShift Container Platform core components use the RHEL cryptographic libraries that have been submitted to NIST for FIPS 140-2/140-3 Validation on only the **x86_64**, **ppc64le**, and **s390x** architectures.

For more information about the NIST validation program, see Cryptographic Module Validation Program. For the latest NIST status for the individual versions of RHEL cryptographic libraries that have been submitted for validation, see Compliance Activities and Government Standards.

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 9.4

RHCOS now uses Red Hat Enterprise Linux (RHEL) 9.4 packages in OpenShift Container Platform 4.16. These packages ensure that your OpenShift Container Platform instances receive the latest fixes, features, enhancements, hardware support, and driver updates. As an Extended Update Support (EUS) release, OpenShift Container Platform 4.14 is excluded from this change and will continue to use RHEL 9.2 EUS packages for the entirety of its lifecycle.

1.3.1.2. Support for iSCSI boot volumes

With this release, you can now install RHCOS to Small Computer Systems Interface (iSCSI) boot devices. Multipathing for iSCSI is also supported. For more information, see Installing RHCOS manually on an iSCSI boot device and Installing RHCOS on an iSCSI boot device using iBFT

1.3.1.3. Support for RAID storage using Intel® Virtual RAID on CPU (VROC)

With this release, you can now install RHCOS to Intel® VROC RAID devices. For more information about configuring RAID to an Intel® VROC device, see Configuring an Intel® Virtual RAID on CPU (VROC) data volume.

1.3.2. Installation and update

1.3.2.1. Cluster API replaces Terraform for AWS installations

In OpenShift Container Platform 4.16, the installation program uses Cluster API instead of Terraform to provision cluster infrastructure during installations on Amazon Web Services. There are several additional required permissions as a result of this change. For more information, see Required AWS permissions for the IAM user.

Additionally, SSH access to control plane and compute machines is no longer open to the machine network, but is restricted to the security groups associated with the control plane and compute machines.

WARNING

Installing a cluster on Amazon Web Services (AWS) into a secret or top-secret region by using the Cluster API implementation has not been tested as of the release of OpenShift Container Platform 4.16. This document will be updated when installation into a secret region has been tested. There is a known issue with Network Load Balancer support for security groups in secret or top secret regions that causes installations to fail. For more information, see OCPBUGS-33311.

1.3.2.2. Cluster API replaces Terraform for VMware vSphere installations

In OpenShift Container Platform 4.16, the installation program uses Cluster API instead of Terraform to provision cluster infrastructure during installations on VMware vSphere.

1.3.2.3. Cluster API replaces Terraform for Nutanix installations

In OpenShift Container Platform 4.16, the installation program uses Cluster API instead of Terraform to provision cluster infrastructure during installations on Nutanix.

1.3.2.4. Cluster API replaces Terraform for Google Cloud Platform (GCP) installations (Technology Preview)

In OpenShift Container Platform 4.16, the installation program uses Cluster API instead of Terraform to provision cluster infrastructure during installations on GCP. This feature is available as a Technology Preview in OpenShift Container Platform 4.16. To enable Technology Preview features, set the **featureSet: TechPreviewNoUpgrade** parameter in the **install-config.yaml** file before installation. Alternatively, add the following stanza to the **install-config.yaml** file before installation to enable Cluster API installation without any other Technology Preview features:

```
featureSet: CustomNoUpgrade
featureGates:
- ClusterAPIInstall=true
```

For more information, see Optional configuration parameters.

1.3.2.5. Ingress capability

Ingress capability is now a configurable cluster capability and is optional for Red Hat HyperShift. It is not configurable and is always enabled for standalone OpenShift Container Platform.

WARNING

Do not disable Ingress capability. An OpenShift Container Platform cluster will not run with the Ingress capability disabled.

1.3.2.6. Installation on Alibaba Cloud by using Assisted Installer (Technology Preview)

With this release, the OpenShift Container Platform installation program no longer supports the installer-provisioned installation on the Alibaba Cloud platform. You can install a cluster on Alibaba Cloud by using Assisted Installer, which is currently a Technology Preview feature. For more information, see Installing on Alibaba cloud .

1.3.2.7. Optional cloud controller manager cluster capability

In OpenShift Container Platform 4.16, you can disable the cloud controller manager capability during installation. For more information, see Cloud controller manager capability.

1.3.2.8. FIPS installation requirements in OpenShift Container Platform 4.16

With this update, if you install a FIPS-enabled cluster, you must run the installation program from a RHEL 9 computer that is configured to operate in FIPS mode, and you must use a FIPS-capable version of the installation program. For more information, see Support for FIPS cryptography .

1.3.2.9. Optional additional tags for VMware vSphere

In OpenShift Container Platform 4.16, you can add up to ten tags to attach to the virtual machines (VMs) provisioned by a VMware vSphere cluster. These tags are in addition to the unique cluster-specific tag that the installation program uses to identify and remove associated VMs when a cluster is decommissioned.

You can define the tags on the VMware vSphere VMs in the **install-config.yaml** file during cluster creation. For more information, see Sample **install-config.yaml** file for an installer-provisioned VMware vSphere cluster.

You can define tags for compute or control plane machines on an existing cluster by using machine sets. For more information, see "Adding tags to machines by using machine sets" for compute or control plane machine sets.

1.3.2.10. Required administrator acknowledgment when updating from OpenShift Container Platform 4.15 to 4.16

OpenShift Container Platform 4.16 uses Kubernetes 1.29, which removed several deprecated APIs.

A cluster administrator must provide manual acknowledgment before the cluster can be updated from OpenShift Container Platform 4.15 to 4.16. This is to help prevent issues after updating to OpenShift Container Platform 4.16, 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 4.15 clusters require this administrator acknowledgment before they can be updated to OpenShift Container Platform 4.16.

For more information, see Preparing to update to OpenShift Container Platform 4.16 .

1.3.2.11. Secure kubeadmin password from being displayed in the console

With this release, you can prevent the **kubeadmin** password from being displayed in the console after the installation by using the **--skip-password-print** flag during cluster creation. The password remains accessible in the **auth** directory.

1.3.2.12. OpenShift-based Appliance Builder (Technology Preview)

With this release, the OpenShift-based Appliance Builder is available as a Technology Preview feature. The Appliance Builder enables self-contained OpenShift Container Platform cluster installations, meaning that it does not rely on internet connectivity or external registries. It is a container-based utility that builds a disk image that includes the Agent-based Installer, which can then be used to install multiple OpenShift Container Platform clusters.

For more information, see the OpenShift-based Appliance Builder User Guide .

1.3.2.13. Bring your own IPv4 (BYOIP) feature enabled for installation on AWS

With this release, you can enable bring your own public IPv4 addresses (BYOIP) feature when installing on Amazon Web Services (AWS) by using the **publicIpv4Pool** field to allocate Elastic IP addresses (EIPs). You must ensure that you have the required permissions to enable BYOIP. For more information, see Optional AWS configuration parameters.

1.3.2.14. Deploy GCP in the Dammam (Saudi Arabia) and Johannesburg (South Africa) regions

You can deploy OpenShift Container Platform 4.16 in Google Cloud Platform (GCP) in the Dammam, Saudi Arabia (**me-central2**) region and in the Johannesburg, South Africa (**africa-south1**) region. For more information, see Supported GCP regions.

1.3.2.15. Installation on NVIDIA H100 instance types on Google Cloud Platform (GCP)

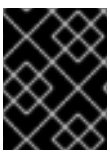
With this release, you can deploy compute nodes on GPU-enabled NVIDIA H100 machines when installing a cluster on GCP. For more information, see Tested instance types for GCP and Google's documentation about the Accelerator-optimized machine family.

1.3.3. Postinstallation configuration

1.3.3.1. Managing workloads on multi-architecture clusters by using the Multiarch Tuning Operator (Technology Preview)

With this release, you can manage workloads on multi-architecture clusters by using the Multiarch Tuning Operator. This Operator enhances the operational experience within multi-architecture clusters, and single-architecture clusters that are migrating to a multi-architecture compute configuration. It implements the **ClusterPodPlacementConfig** custom resource (CR) to support architecture-aware workload scheduling.

For more information, see Managing workloads on multi-architecture clusters by using the Multiarch Tuning Operator.



IMPORTANT

The Multiarch Tuning Operator is a Technology Preview feature only. It does not support clusters with restricted network scenarios.

1.3.3.2. Support for adding 64-bit x86 compute machines to a cluster with 64-bit ARM control plane machines

This feature provides support for adding 64-bit x86 compute machines to a multi-architecture cluster with 64-bit ARM control plane machines. With this release, you can add 64-bit x86 compute machines to

a cluster that uses 64-bit ARM control plane machines and already includes 64-bit ARM compute machines.

1.3.3.3. Support for installing an Agent-based Installer cluster with multi payload

This feature provides support for installing an Agent-based Installer cluster with **multi** payload. After installing the Agent-based Installer cluster with **multi** payload, you can add compute machines with different architectures to the cluster.

1.3.4. Web console

1.3.4.1. Language support for French and Spanish

With this release, French and Spanish are supported in the web console. You can update the language in the web console from the **Language** list on the **User Preferences** page.

1.3.4.2. Patternfly 4 is now deprecated with 4.16

With this release, Patternfly 4 and React Router 5 are deprecated in the web console. All plugins should migrate to Patternfly 5 and React Router 6 as soon as possible.

1.3.4.3. Administrator perspective

This release introduces the following updates to the **Administrator** perspective of the web console:

- A Google Cloud Platform (GCP) token authorization, **Auth Token GCP**, and a **Configurable TLS ciphers** filter was added to the **Infrastructure features** filter in the OperatorHub.
- A new quick start, **Impersonating the system:admin user**, is available with information on impersonating the **system:admin** user.
- A pod's last termination state is now available to view on the **Container list** and **Container details** pages.
- An **Impersonate Group** action is now available from the **Groups** and **Group details** pages without having to search for the appropriate **RoleBinding**.
- You can collapse and expand the **Getting started** section.

1.3.4.3.1. Node CSR handling in the OpenShift Container Platform web console

With this release, the OpenShift Container Platform web console supports node certificate signing requests (CSRs).

1.3.4.3.2. Cross Storage Class clone and restore

With this release, you can select a storage class from the same provider when completing clone or restore operations. This flexibility allows seamless transitions between storage classes with different replica counts. For example, moving from a storage class with 3 replicas to 2/1 replicas.

1.3.4.4. Developer Perspective

This release introduces the following updates to the **Developer** perspective of the web console:

- When searching, a new section was added to the list of **Resources** on the **Search** page to display the recently searched items in the order they were searched.

1.3.4.4.1. Console Telemetry

With this release, anonymized user analytics were enabled if cluster telemetry is also enabled. This is the default for most of the cluster and provides Red Hat with metrics for how the web console is used. Cluster administrators can update this in each cluster and opt-in, opt-out, or disable front-end telemetry.

1.3.5. OpenShift CLI (oc)

1.3.5.1. oc-mirror plugin v2 (Technology Preview)

The oc-mirror plugin v2 for OpenShift Container Platform includes new features and functionalities that improve the mirroring process for Operator images and other OpenShift Container Platform content.

The following are the key enhancements and features in oc-mirror plugin v2:

- **Automatic generation of IDMS and ITMS objects**
  oc-mirror plugin v2 automatically generates a comprehensive list of **ImageDigestMirrorSet** (IDMS) and **ImageTagMirrorSet** (ITMS) objects after each run. These objects replace the **ImageContentSourcePolicy** (ICSP) used in oc-mirror plugin v1. This enhancement eliminates the need for manual merging and cleanup of operator images and ensures all necessary images are included.

- **CatalogSource objects**:
  CatalogSource objects creation, where the plugin now generates CatalogSource objects for all relevant catalog indexes to enhance the application of oc-mirror's output artifacts to disconnected clusters.

- **Improved verification**:
  oc-mirror plugin v2 verifies that the complete image set specified in the image set config is mirrored to the registry, regardless of whether the images were previously mirrored or not. This ensures comprehensive and reliable mirroring.

- **Cache system**:
  The new cache system replaces metadata, maintaining minimal archive sizes by incorporating only new images into the archive. This optimizes storage and improves performance.

- **Selective mirroring by date**:
  Users can now generate mirroring archives based on the mirroring date, allowing for the selective inclusion of new images.

- **Enhanced image deletion control**
  The introduction of a **Delete** feature replaces automatic pruning, providing users with greater control over image deletion.

- **Support for registries.conf**:
  oc-mirror plugin v2 supports the **registries.conf** file that facilitates mirroring to multiple enclaves using the same cache. This enhances flexibility and efficiency in managing mirrored images.

- **Operator version filtering**:

Users can filter Operator versions by bundle name, offering more precise control over the versions included in the mirroring process.

Differences Between oc-mirror v1 and v2

While oc-mirror plugin v2 brings numerous enhancements, some features from oc-mirror plugin v1 are not yet present in oc-mirror plugin v2:

- Helm Charts: Helm charts are not present in oc-mirror plugin v2.
- **ImageSetConfig v1alpha2**: The API version **v1alpha2** is not available, users must update to **v2alpha1**.
- Storage Metadata (**storageConfig**): Storage metadata is not used in oc-mirror plugin v2 **ImageSetConfiguration**.
- Automatic Pruning: Replaced by the new **Delete** feature in oc-mirror plugin v2.
- Release Signatures: Release signatures are not generated in oc-mirror plugin v2.
- Some commands: The **init**, **list**, and **describe** commands are not available in oc-mirror plugin v2.

Using oc-mirror plugin v2

To use the oc-mirror plugin v2, add the **--v2** flag to the oc-mirror command line.

The oc-mirror OpenShift CLI (**oc**) plugin is used to mirror all the required OpenShift Container Platform content and other images to your mirror registry, simplifying the maintenance of disconnected clusters.

1.3.5.2. Introducing the oc adm upgrade status command (Technology Preview)

Previously, the **oc adm upgrade** command provided limited information about the status of a cluster update. This release adds the **oc adm upgrade status** command, which decouples status information from the **oc adm upgrade** command and provides specific information regarding a cluster update, including the status of the control plane and worker node updates.

1.3.5.3. Warning for duplicate resource short names

With this release, if you query a resource by using its short name, the OpenShift CLI (**oc**) returns a warning if more than one custom resource definition (CRD) with the same short name exists in the cluster.

Example warning

```
Warning: short name "ex" could also match lower priority resource examples.test.com
```

1.3.5.4. New flag to require confirmation when deleting resources (Technology Preview)

This release introduces a new **--interactive** flag for the **oc delete** command. When the **--interactive** flag is set to **true**, the resource is deleted only if the user confirms the deletion. This flag is available as a Technology Preview feature.

1.3.6. IBM Z and IBM LinuxONE

With this release, IBM Z® and IBM® LinuxONE are now compatible with OpenShift Container Platform 4.16. You can perform the installation with z/VM, LPAR, or Red Hat Enterprise Linux (RHEL) Kernel-

based Virtual Machine (KVM). For installation instructions, see Preparing to install on IBM Z and IBM LinuxONE.

IMPORTANT

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

IBM Z and IBM LinuxONE notable enhancements
The IBM Z® and IBM® LinuxONE release on OpenShift Container Platform 4.16 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:

- Agent-based Installer ISO boot for RHEL KVM
- Ingress Node Firewall Operator
- Multi-architecture compute machines in an LPAR
- Secure boot for z/VM and LPAR

1.3.7. IBM Power

IBM Power® is now compatible with OpenShift Container Platform 4.16. 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 4.16 adds improvements and new capabilities to OpenShift Container Platform components.

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

- CPU manager
- Ingress Node Firewall Operator

IBM Power, IBM Z, and IBM LinuxONE support matrix

Starting in OpenShift Container Platform 4.14, Extended Update Support (EUS) is extended to the IBM Power® and the IBM Z® platform. For more information, see the OpenShift EUS Overview.

Table 1.1. OpenShift Container Platform features

Feature	IBM Power®	IBM Z® and IBM® LinuxONE
Alternate authentication providers	Supported	Supported

Feature	IBM Power®	IBM Z® and IBM® LinuxONE
Agent-based Installer	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
FIPS cryptography	Supported	Supported
Helm	Supported	Supported
Horizontal pod autoscaling	Supported	Supported
Hosted control planes (Technology Preview)	Supported	Supported
IBM Secure Execution	Unsupported	Supported
Installer-provisioned Infrastructure Enablement for IBM Power® Virtual Server	Supported	Unsupported
Installing on a single node	Supported	Supported
IPv6	Supported	Supported
Monitoring for user-defined projects	Supported	Supported
Multi-architecture compute nodes	Supported	Supported
Multi-architecture control plane	Supported	Supported

Feature	IBM Power®	IBM Z® and IBM® LinuxONE
Multipathing	Supported	Supported
Network-Bound Disk Encryption - External Tang Server	Supported	Supported
Non-volatile memory express drives (NVMe)	Supported	Unsupported
nx-gzip for Power10 (Hardware Acceleration)	Supported	Unsupported
oc-mirror plugin	Supported	Supported
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
Secure Boot	Unsupported	Supported
Stream Control Transmission Protocol (SCTP)	Supported	Supported
Support for multiple network interfaces	Supported	Supported
The **openshift-install** utility to support various SMT levels on IBM Power® (Hardware Acceleration)	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 by using local storage, such as iSCSI, FC, or by using LSO with DASD, FCP, or EDEV/FBA.

Table 1.3. Operators

Feature	IBM Power®	IBM Z® and IBM® LinuxONE
cert-manager Operator for Red Hat OpenShift	Supported	Supported
Cluster Logging Operator	Supported	Supported
Cluster Resource Override Operator	Supported	Supported
Compliance Operator	Supported	Supported
Cost Management Metrics Operator	Supported	Supported
File Integrity Operator	Supported	Supported
HyperShift Operator	Technology Preview	Technology Preview
IBM Power® Virtual Server Block CSI Driver Operator	Supported	Unsupported
Ingress Node Firewall Operator	Supported	Supported
Local Storage Operator	Supported	Supported
MetalLB Operator	Supported	Supported

Feature	IBM Power®	IBM Z® and IBM® LinuxONE
Network Observability Operator	Supported	Supported
NFD Operator	Supported	Supported
NMState Operator	Supported	Supported
OpenShift Elasticsearch Operator	Supported	Supported
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. Authentication and authorization

1.3.8.1. Enabling Microsoft Entra Workload ID on existing clusters

In this release, you can enable Microsoft Entra Workload ID to use short-term credentials on an existing Microsoft Azure OpenShift Container Platform cluster. This functionality is now also supported in versions 4.14 and 4.15 of OpenShift Container Platform. For more information, see Enabling token-based authentication.

1.3.9. Networking

1.3.9.1. OpenShift SDN network plugin blocks future major upgrades

As part of the OpenShift Container Platform move to OVN-Kubernetes as the only supported network plugin, starting with OpenShift Container Platform 4.16, if your cluster uses the OpenShift SDN network plugin, you cannot upgrade to future major versions of OpenShift Container Platform without migrating to OVN-Kubernetes. For more information about migrating to OVN-Kubernetes, see Migrating from the OpenShift SDN network plugin.

If you try an upgrade, the Cluster Network Operator reports the following status:

```
- lastTransitionTime: "2024-04-11T05:54:37Z"
  message: Cluster is configured with OpenShiftSDN, which is not supported in the
    next version. Please follow the documented steps to migrate from OpenShiftSDN
    to OVN-Kubernetes in order to be able to upgrade. https://docs.openshift.com/container-
platform/4.16/networking/ovn_kubernetes_network_provider/migrate-from-openshift-sdn.html
  reason: OpenShiftSDNConfigured
  status: "False"
  type: Upgradeable
```

1.3.9.2. Dual-NIC Intel E810 Westport Channel as PTP grandmaster clock (Generally Available)

Configuring **linuxptp** services as grandmaster clock (T-GM) for dual Intel E810 Westport Channel network interface controllers (NICs) is now a generally available feature in OpenShift Container Platform. The host system clock is synchronized from the NIC that is connected to the Global Navigation Satellite Systems (GNSS) time source. The second NIC is synced to the 1PPS timing output provided by the NIC that is connected to GNSS. For more information see Configuring linuxptp services as a grandmaster clock for dual E810 Westport Channel NICs.

1.3.9.3. Dual-NIC Intel E810 PTP boundary clock with highly available system clock (Generally Available)

You can configure the **linuxptp** services **ptp4l** and **phc2sys** as a highly available (HA) system clock for dual PTP boundary clocks (T-BC).

For more information, see Configuring linuxptp as a highly available system clock for dual-NIC Intel E810 PTP boundary clocks.

1.3.9.4. Configuring pod placement to check network connectivity

To periodically test network connectivity among cluster components, the Cluster Network Operator (CNO) creates the **network-check-source** deployment and the **network-check-target** daemon set. In OpenShift Container Platform 4.16, you can configure the nodes by setting node selectors and run the source and target pods to check the network connectivity. For more information, see Verifying connectivity to an endpoint.

1.3.9.5. Define multiple CIDR blocks for one network security group (NSG) rule

With this release, IP addresses and ranges are handled more efficiently in NSGs for OpenShift Container Platform clusters hosted on Microsoft Azure. As a result, the maximum limit of Classless Inter-Domain Routings (CIDRs) for all Ingress Controllers in Microsoft Azure clusters, using the **allowedSourceRanges** field, increases from approximately 1000 to 4000 CIDRs.

1.3.9.6. Migration from OpenShift SDN to OVN-Kubernetes on Nutanix

With this release, migration from the OpenShift SDN network plugin to OVN-Kubernetes is now supported on Nutanix platforms. For more information, see Migration to the OVN-Kubernetes network plugin.

1.3.9.7. Improved integration between CoreDNS and egress firewall (Technology Preview)

With this release, OVN-Kubernetes uses a new **DNSNameResolver** custom resource to keep track of DNS records in your egress firewall rules, and is available as a Technology Preview. This custom resource supports the use of both wildcard DNS names and regular DNS names and allows access to DNS names regardless of the IP addresses associated with its change.

For more information, see Improved DNS resolution and resolving wildcard domain names .

1.3.9.8. Parallel node draining during SR-IOV network policy updates

With this release, you can configure the SR-IOV Network Operator to drain nodes in parallel during network policy updates. The option to drain nodes in parallel enables faster rollouts of SR-IOV network configurations. You can use the **SriovNetworkPoolConfig** custom resource to configure parallel node draining and define the maximum number of nodes in the pool that the Operator can drain in parallel.

For further information, see Configuring parallel node draining during SR-IOV network policy updates .

1.3.9.9. SR-IOV Network Operator no longer automatically creates the SriovOperatorConfig CR

As of OpenShift Container Platform 4.16, the SR-IOV Network Operator no longer automatically creates a **SriovOperatorConfig** custom resource (CR). Create the **SriovOperatorConfig** CR by using the procedure described in Configuring the SR-IOV Network Operator.

1.3.9.10. Supporting double-tagged packets (QinQ)

This release introduces 802.1Q-in-802.1Q also known as *QinQ support*. QinQ introduces a second VLAN tag, where the service provider designates the outer tag for their use, offering them flexibility, while the inner tag remains dedicated to the customer's VLAN. When two VLAN tags are present in a packet, the outer VLAN tag can be either 802.1Q or 802.1ad. The inner VLAN tag must always be 802.1Q.

For more information, see Configuring QinQ support for SR-IOV enabled workloads.

1.3.9.11. Configuring a user-managed load balancer for on-premise infrastructure

With this release, you can configure an OpenShift Container Platform cluster on any on-premise infrastructure, such as bare metal, VMware vSphere, Red Hat OpenStack Platform (RHOSP), or Nutanix, to use a user-managed load balancer in place of the default load balancer. For this configuration, you must specify **loadBalancer.type: UserManaged** in your cluster's **install-config.yaml** file.

For more information about this feature on bare-metal infrastructure, see Services for a user-managed load balancer in *Setting up the environment for an OpenShift installation* .

1.3.9.12. Detect and warning for iptables

With this release, if you have pods in your cluster using **iptables** rules the following event message is given to warn against future deprecation:

-

> This pod appears to have created one or more iptables rules. IPTables is deprecated and will no longer be available in RHEL 10 and later. You should consider migrating to another API such as nftables or eBPF.

For more information, see Getting started with nftables. If you are running third-party software, check with your vendor to ensure they will have an **nftables** based version available soon.

1.3.9.13. Ingress network flows for OpenShift Container Platform services

With this release, you can view the ingress network flows for OpenShift Container Platform services. You can use this information to manage ingress traffic for your network and improve network security.

For more information, see OpenShift Container Platform network flow matrix .

1.3.9.14. Patching an existing dual-stack network

With this release, you can add IPv6 virtual IPs (VIPs) for API and Ingress services to an existing dual-stack-configured cluster by patching the cluster infrastructure.

If you have already upgraded your cluster to OpenShift Container Platform 4.16 and you need to convert the single-stack cluster network to a dual-stack cluster network, you must specify the following for your cluster in the YAML configuration patch file:

- An IPv4 network for API and Ingress services on the first **machineNetwork** configuration.
- An IPv6 network for API and Ingress services on the second **machineNetwork** configuration.

For more information, see Converting to a dual-stack cluster network in *Converting to IPv4/IPv6 dual-stack networking*.

1.3.9.15. Integration of MetalLB and FRR-K8s (Technology Preview)

This release introduces **FRR-K8s**, a Kubernetes based **DaemonSet** that exposes a subset of the **FRR** API in a Kubernetes-compliant manner. As a cluster administrator, you can use the **FRRConfiguration** custom resource (CR) to configure the MetalLB Operator to use the **FRR-K8s** daemon set as the backend. You can use this to operate FRR services, such as receiving routes.

For more information, see Configuring the integration of MetalLB and FRR-K8s.

1.3.9.16. Creating a route with externally managed certificate (Technology Preview)

With this release, OpenShift Container Platform routes can be configured with third-party certificate management solutions, utilising the **.spec.tls.externalCertificate** field in the route API. This allows you to reference externally managed TLS certificates through secrets, streamlining the process by eliminating manual certificate management. By using externally managed certificates, you reduce errors, ensure a smoother certificate update process, and enable the OpenShift router to promptly serve renewed certificates. For more information, see Creating a route with externally managed certificate .

1.3.9.17. AdminNetworkPolicy is generally available

This feature provides two new APIs, **AdminNetworkPolicy** (ANP) and **BaselineAdminNetworkPolicy** (BANP). Before namespaces are created, cluster Administrators can use ANP and BANP to apply cluster-scoped network policies and safeguards for an entire cluster. Because it is cluster scoped, ANP provides Administrators a solution to manage the security of their network at scale without having to duplicate their network policies on each namespace.

For more information, see Converting to a dual-stack cluster network in *Converting to IPv4/IPv6 dual-stack networking*.

1.3.9.18. Limited live migration to the OVN-Kubernetes network plugin

Previously, when migrating from OpenShift SDN to OVN-Kubernetes, the only available option was an *offline* migration method. This process included some downtime, during which clusters were unreachable.

This release introduces a limited *live* migration method. The limited live migration method is the process in which the OpenShift SDN network plugin and its network configurations, connections, and associated resources are migrated to the OVN-Kubernetes network plugin without service interruption. It is available for OpenShift Container Platform. It is not available for hosted control plane deployment types. This migration method is valuable for deployment types that require constant service availability and offers the following benefits:

- Continuous service availability
- Minimized downtime
- Automatic node rebooting
- Seamless transition from the OpenShift SDN network plugin to the OVN-Kubernetes network plugin

Migration to OVN-Kubernetes is intended to be a one-way process.

For more information, see Limited live migration to the OVN-Kubernetes network plugin overview .

1.3.9.19. Overlapping IP configuration for multi-tenant networks with Whereabouts

Previously, it was not possible to configure the same CIDR range twice and to have the Whereabouts CNI plugin assign IP addresses from these ranges independently. This limitation caused issues in multi-tenant environments where different groups might need to select overlapping CIDR ranges.

With this release, the Whereabouts CNI plugin supports overlapping IP address ranges through the inclusion of a **network_name** parameter. Administrators can use the **network_name** parameter to configure the same CIDR range multiple times within separate **NetworkAttachmentDefinitions**, which enables independent IP address assignments for each range.

This feature also includes enhanced namespace handling, stores **IPPool** custom resources (CRs) in the appropriate namespaces, and supports cross-namespaces when permitted by Multus. These improvements provide greater flexibility and management capabilities in multi-tenant environments.

For more information about this feature, see Dynamic IP address assignment configuration with Whereabouts.

1.3.9.20. Support for changing the OVN-Kubernetes network plugin internal IP address ranges

If you use the OVN-Kubernetes network plugin, you can configure the transit, join, and masquerade subnets. The transit, join and masquerade subnets can be configured either during cluster installation or after. The subnet defaults are:

- Transit subnet: **100.88.0.0/16** and **fd97::/64**
- Join subnet: **100.64.0.0/16** and **fd98::/64**

- Masquerade subnet: **169.254.169.0/29** and **fd69::/125**

For more information about these configuration fields, see Cluster Network Operator configuration object. For more information about configuring the transit and join subnets on an existing cluster, see Configure OVN-Kubernetes internal IP address subnets.

1.3.9.21. IPsec telemetry

The Telemetry and the Insights Operator collects telemetry on IPsec connections. For more information, see Showing data collected by Telemetry.

1.3.10. Storage

1.3.10.1. HashiCorp Vault is now available for the Secrets Store CSI Driver Operator (Technology Preview)

You can now use the Secrets Store CSI Driver Operator to mount secrets from HashiCorp Vault to a Container Storage Interface (CSI) volume in OpenShift Container Platform. The Secrets Store CSI Driver Operator is available as a Technology Preview feature.

For the full list of available secrets store providers, see Secrets store providers.

For information about using the Secrets Store CSI Driver Operator to mount secrets from HashiCorp Vault, see Mounting secrets from HashiCorp Vault.

1.3.10.2. Volume cloning supported for Microsoft Azure File (Technology Preview)

OpenShift Container Platform 4.16 introduces volume cloning for the Microsoft Azure File Container Storage Interface (CSI) Driver Operator as a Technology Preview feature. Volume cloning duplicates an existing persistent volume (PV) to help protect against data loss in OpenShift Container Platform. You can also use a volume clone just as you would use any standard volume.

For more information, see Azure File CSI Driver Operator and CSI volume cloning.

1.3.10.3. Node Expansion Secret is generally available

The Node Expansion Secret feature allows your cluster to expand storage of mounted volumes, even when access to those volumes requires a secret (for example, a credential for accessing a Storage Area Network (SAN) fabric) to perform the node expand operation. OpenShift Container Platform 4.16 supports this feature as generally available.

1.3.10.4. Changing vSphere CSI maximum number of snapshots is generally available

The default maximum number of snapshots in VMware vSphere Container Storage Interface (CSI) is 3 per volume. In OpenShift Container Platform 4.16, you can now change this maximum number of snapshots to a maximum of 32 per volume. You also have granular control of the maximum number of snapshots for vSAN and Virtual Volume datastores. OpenShift Container Platform 4.16 supports this feature as generally available.

For more information, see Changing the maximum number of snapshots for vSphere.

1.3.10.5. Persistent volume last phase transition time parameter (Technology Preview)

In OpenShift Container Platform 4.16 introduces a new parameter, **LastPhaseTransitionTime**, which has a timestamp that is updated every time a persistent volume (PV) transitions to a different phase (**pv.Status.Phase**). This feature is being released with Technology Preview status.

1.3.10.6. Persistent storage using CIFS/SMB CSI Driver Operator (Technology Preview)

OpenShift Container Platform is capable of provisioning persistent volumes (PVs) with a Container Storage Interface (CSI) driver for the Common Internet File System (CIFS) dialect/Server Message Block (SMB) protocol. The CIFS/SMB CSI Driver Operator that manages this driver is in Technology Preview status.

For more information, see CIFS/SMB CSI Driver Operator.

1.3.10.7. RWOP with SELinux context mount is generally available

OpenShift Container Platform 4.14 introduced a new access mode with Technical Preview status for persistent volumes (PVs) and persistent volume claims (PVCs) called ReadWriteOncePod (RWOP). RWOP can be used only in a single pod on a single node compared to the existing ReadWriteOnce access mode where a PV or PVC can be used on a single node by many pods. If the driver enables it, RWOP uses the SELinux context mount set in the **PodSpec** or container, which allows the driver to mount the volume directly with the correct SELinux labels. This eliminates the need to recursively relabel the volume, and pod startup can be significantly faster.

In OpenShift Container Platform 4.16, this feature is generally available.

For more information, see Access modes.

1.3.10.8. vSphere CSI Driver 3.1 updated CSI topology requirements

To support VMware vSphere Container Storage Interface (CSI) volume provisioning and usage in multi-zonal clusters, the deployment should match certain requirements imposed by CSI driver. These requirements have changed starting with 3.1.0, and although OpenShift Container Platform 4.16 accepts both the old and new tagging methods, you should use the new tagging method since VMware vSphere considers the old way an invalid configuration. To prevent problems, you should not use the old tagging method.

For more information, see vSphere CSI topology requirements.

1.3.10.9. Support for configuring thick-provisioned storage

This feature provides support for configuring thick-provisioned storage. If you exclude the **deviceClasses.thinPoolConfig** field in the **LVMCluster** custom resource (CR), logical volumes are thick provisioned. Using thick-provisioned storage includes the following limitations:

- No copy-on-write support for volume cloning.
- No support for **VolumeSnapshotClass**. Therefore, CSI snapshotting is not supported.
- No support for over-provisioning. As a result, the provisioned capacity of PersistentVolumeClaims (PVCs) is immediately reduced from the volume group.
- No support for thin metrics. Thick-provisioned devices only support volume group metrics.

For information about configuring the **LVMCluster** CR, see About the LVMCluster custom resource.

1.3.10.10. Support for a new warning message when device selector is not configured in the LVMCluster custom resource

This update provides a new warning message when you do not configure the **deviceSelector** field in the **LVMCluster** custom resource (CR).

The **LVMCluster** CR supports a new field, **deviceDiscoveryPolicy**, which indicates whether the **deviceSelector** field is configured. If you do not configure the **deviceSelector** field, LVM Storage automatically sets the **deviceDiscoveryPolicy** field to **RuntimeDynamic**. Otherwise, the **deviceDiscoveryPolicy** field is set to **Preconfigured**.

It is not recommended to exclude the **deviceSelector** field from the **LMVCluster** CR. For more information about the limitations of not configuring the **deviceSelector** field, see About adding devices to a volume group.

1.3.10.11. Support for adding encrypted devices to a volume group

This feature provides support for adding encrypted devices to a volume group. You can enable disk encryption on the cluster nodes during an OpenShift Container Platform installation. After encrypting a device, you can specify the path to the LUKS encrypted device in the **deviceSelector** field in the **LVMCluster** custom resource. For information about disk encryption, About disk encryption and Configuring disk encryption and mirroring .

For more information about adding devices to a volume group, see About adding devices to a volume group.

1.3.11. Operator lifecycle

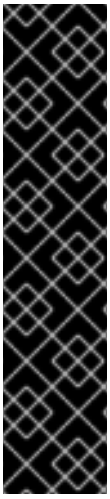
1.3.11.1. Operator API renamed to ClusterExtension (Technology Preview)

Earlier Technology Preview phases of Operator Lifecycle Manager (OLM) 1.0 introduced a new **Operator** API, provided as **operator.operators.operatorframework.io** by the Operator Controller component. In OpenShift Container Platform 4.16, this API is renamed **ClusterExtension**, provided as **clusterextension.olm.operatorframework.io**, for this Technology Preview phase of OLM 1.0.

This API still streamlines management of installed extensions, which includes Operators via the **registry+v1** bundle format, by consolidating user-facing APIs into a single object. The rename to **ClusterExtension** addresses the following:

- More accurately reflects the simplified functionality of extending a cluster's capabilities
- Better represents a more flexible packaging format
- **Cluster** prefix clearly indicates that **ClusterExtension** objects are cluster-scoped, a change from legacy OLM where Operators could be either namespace-scoped or cluster-scoped

For more information, see Operator Controller.



IMPORTANT

OLM 1.0 does not support dependency resolution. If an extension declares dependencies for other APIs or packages, the dependencies must be present on the cluster before you attempt to install the extension.

Currently, OLM 1.0 supports the installation of extensions that meet the following criteria:

- The extension must use the **AllNamespaces** install mode.
- The extension must not use webhooks.

Cluster extensions that use webhooks or that target a single or specified set of namespaces cannot be installed.

1.3.11.2. Improved status condition messages and deprecation notices for cluster extensions in Operator Lifecycle Manager (OLM) 1.0 (Technology Preview)

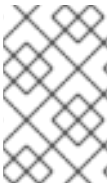
With this release, OLM 1.0 displays the following status condition messages for installed cluster extensions:

- Specific bundle name
- Installed version
- Improved health reporting
- Deprecation notices for packages, channels, and bundles

1.3.11.3. Support for legacy OLM upgrade edges in OLM 1.0 (Technology Preview)

When determining upgrade edges for an installed cluster extension, Operator Lifecycle Manager (OLM) 1.0 supports legacy OLM semantics starting in OpenShift Container Platform 4.16. This support follows the behavior from legacy OLM, including **replaces**, **skips**, and **skipRange** directives, with a few noted differences.

By supporting legacy OLM semantics, OLM 1.0 now honors the upgrade graph from catalogs accurately.



NOTE

Support for semantic versioning (semver) upgrade constraints was introduced in OpenShift Container Platform 4.15 but disabled in 4.16 in favor of legacy OLM semantics during this Technology Preview phase.

For more information, see Upgrade constraint semantics.

1.3.12. Builds

Unauthenticated users were removed from the system:webhook role binding
With this release, unauthenticated users no longer have access to the **system:webhook** role binding. Before OpenShift Container Platform 4.16, unauthenticated users could access the **system:webhook** role binding. Changing this access for unauthenticated users adds an additional layer of security and should only be enabled by users when necessary. This change is for new clusters; previous clusters are not affected.

There are use cases where you might want to allow unauthenticated users the **system:webhook** role binding for specific namespaces. The **system:webhook** cluster role allows users to trigger builds from external systems that do not use OpenShift Container Platform authentication mechanisms, such as GitHub, GitLab, and Bitbucket. Cluster admins can grant unauthenticated users access to the **system:webhook** role binding to facilitate this use case.

IMPORTANT

Always verify compliance with your organization's security standards when modifying unauthenticated access.

To grant unauthenticated users access to the **system:webhook** role binding in specific namespaces, see Adding unauthenticated users to the system:webhook role binding .

1.3.13. Machine Config Operator

1.3.13.1. Garbage collection of unused rendered machine configs

With this release, you can now garbage collect unused rendered machine configs. By using the **oc adm prune renderedmachineconfigs** command, you can view the unused rendered machine configs, determine which to remove, then batch delete the rendered machine configs that you no longer need. Having too many machine configs can make working with the machine configs confusing and can also contribute to disk space and performance issues. For more information, see Managing unused rendered machine configs.

1.3.13.2. Node disruption policies (Technology Preview)

By default, when you make certain changes to the parameters in a **MachineConfig** object, the Machine Config Operator (MCO) drains and reboots the nodes associated with that machine config. However, you can create a node disruption policy in the MCO namespace that defines a set of Ignition config objects changes that would require little or no disruption to your workloads. For more information, see Using node disruption policies to minimize disruption from machine config changes .

1.3.13.3. On-cluster RHCOS image layering (Technology Preview)

With Red Hat Enterprise Linux CoreOS (RHCOS) image layering, you can now automatically build the custom layered image directly in your cluster, as a Technology Preview feature. Previously, you needed to build the custom layered image outside of the cluster, then pull the image into the cluster. You can use the image layering feature to extend the functionality of your base RHCOS image by layering additional images onto the base image. For more information, see RHCOS image layering.

1.3.13.4. Updating boot images (Technology Preview)

By default, the MCO does not delete the boot image it uses to bring up a Red Hat Enterprise Linux CoreOS (RHCOS) node. Consequently, the boot image in your cluster is not updated along with your cluster. You can now configure your cluster to update the boot image whenever you update your cluster. For more information, see Updating boot images.

1.3.14. Machine management

1.3.14.1. Configuring expanders for the cluster autoscaler

With this release, the cluster autoscaler can use the **LeastWaste**, **Priority**, and **Random** expanders. You can configure these expanders to influence the selection of machine sets when scaling the cluster. For more information, see Configuring the cluster autoscaler.

1.3.14.2. Managing machines with the Cluster API for VMware vSphere (Technology Preview)

This release introduces the ability to manage machines by using the upstream Cluster API, integrated into OpenShift Container Platform, as a Technology Preview for VMware vSphere clusters. This capability is in addition or an alternative to managing machines with the Machine API. For more information, see About the Cluster API.

1.3.14.3. Defining a vSphere failure domain for a control plane machine set

With this release, the previously Technology Preview feature of defining a vSphere failure domain for a control plane machine set is Generally Available. For more information, see Control plane configuration options for VMware vSphere.

1.3.15. Nodes

1.3.15.1. Moving the Vertical Pod Autoscaler Operator pods

The Vertical Pod Autoscaler Operator (VPA) consists of three components: the recommender, updater, and admission controller. The Operator and each component has its own pod in the VPA namespace on the control plane nodes. You can move the VPA Operator and component pods to infrastructure or worker nodes. For more information, see Moving the Vertical Pod Autoscaler Operator components .

1.3.15.2. Additional information collected by must-gather

With this release, the **oc adm must-gather** command collects the following additional information:

- OpenShift CLI (**oc**) binary version
- Must-gather logs

These additions help identify issues that might stem from using a specific version of **oc**. The **oc adm must-gather** command also lists what image was used and if any data could not be gathered in the must-gather logs.

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

1.3.15.3. Editing the BareMetalHost resource

In OpenShift Container Platform 4.16 and later, you can edit the baseboard management controller (BMC) address in the **BareMetalHost** resource of a bare-metal node. The node must be in the **Provisioned**, **ExternallyProvisioned**, **Registering**, or **Available** state. Editing the BMC address in the **BareMetalHost** resource will not result in deprovisioning the node. See Editing a BareMetalHost resource for additional details.

1.3.15.4. Attaching a non-bootable ISO

In OpenShift Container Platform 4.16 and later, you can attach a generic, non-bootable ISO virtual media image to a provisioned node by using the **DataImage** resource. After you apply the resource, the ISO image becomes accessible to the operating system on the next reboot. The node must use Redfish

or drivers derived from it to support this feature. The node must be in the **Provisioned** or **ExternallyProvisioned** state. See Attaching a non-bootable ISO to a bare-metal node for additional details.

1.3.16. Monitoring

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

1.3.16.1. Updates to monitoring stack components and dependencies

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

- kube-state-metrics to 2.12.0
- Metrics Server to 0.7.1
- node-exporter to 1.8.0
- Prometheus to 2.52.0
- Prometheus Operator to 0.73.2
- Thanos to 0.35.0

1.3.16.2. Changes to alerting rules

NOTE

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

- Added the **ClusterMonitoringOperatorDeprecatedConfig** alert to monitor when the Cluster Monitoring Operator configuration uses a deprecated field.
- Added the **PrometheusOperatorStatusUpdateErrors** alert to monitor when the Prometheus Operator fails to update object status.

1.3.16.3. Metrics Server component to access the Metrics API general availability (GA)

The Metrics Server component is now generally available and automatically installed instead of the deprecated Prometheus Adapter. Metrics Server collects resource metrics and exposes them in the **metrics.k8s.io** Metrics API service for use by other tools and APIs, which frees the core platform Prometheus stack from handling this functionality. For more information, see MetricsServerConfig in the config map API reference for the Cluster Monitoring Operator.

1.3.16.4. New monitoring role to allow read-only access to the Alertmanager API

This release introduces a new **monitoring-alertmanager-view** role to allow read-only access to the Alertmanager API in the **openshift-monitoring** project.

1.3.16.5. VPA metrics are available in the kube-state-metrics agent

Vertical Pod Autoscaler (VPA) metrics are now available through the **kube-state-metrics** agent. VPA metrics follow a similar exposition format just as they did before being deprecated and removed from native support upstream.

1.3.16.6. Change in proxy service for monitoring components

With this release, the proxy service in front of Prometheus, Alertmanager, and Thanos Ruler has been updated from OAuth to **kube-rbac-proxy**. This change might affect service accounts and users accessing these API endpoints without the appropriate roles and cluster roles.

1.3.16.7. Change in how Prometheus handles duplicate samples

With this release, when Prometheus scrapes a target, duplicate samples are no longer silently ignored, even if they have the same value. The first sample is accepted and the **prometheus_target_scrapes_sample_duplicate_timestamp_total** counter is incremented, which might trigger the **PrometheusDuplicateTimestamps** alert.

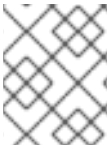
1.3.17. Network Observability Operator

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 is found in the Network Observability release notes.

1.3.18. Scalability and performance

1.3.18.1. Workload partitioning enhancement

With this release, platform pods deployed with a workload annotation that includes both CPU limits and CPU requests will have the CPU limits accurately calculated and applied as a CPU quota for the specific pod. In prior releases, if a workload partitioned pod had both CPU limits and requests set, they were ignored by the webhook. The pod did not benefit from workload partitioning and was not locked down to specific cores. This update ensures the requests and limits are now interpreted correctly by the webhook.



NOTE

It is expected that if the values for CPU limits are different from the value for requests in the annotation, the CPU limits are taken as being the same as the requests.

For more information, see Workload partitioning.

1.3.18.2. Linux Control Groups version 2 is now supported with the performance profile feature

Beginning with OpenShift Container Platform 4.16, Control Groups version 2 (cgroup v2), also known as cgroup2 or cgroupsv2, is enabled by default for all new deployments, even when performance profiles are present.

Since OpenShift Container Platform 4.14, cgroups v2 has been the default, but the performance profile feature required the use of cgroups v1. This issue has been resolved.

cgroup v1 is still used in upgraded clusters with performance profiles that have initial installation dates before OpenShift Container Platform 4.16. cgroup v1 can still be used in the current version by changing the **cgroupMode** field in the **node.config** object to **v1**.

For more information, see Configuring the Linux cgroup version on your nodes .

1.3.18.3. Support for increasing the etcd database size (Technology Preview)

With this release, you can increase the disk quota in etcd. This is a Technology Preview feature. For more information, see Increasing the database size for etcd.

1.3.18.4. Reserved core frequency tuning

With this release, the Node Tuning Operator supports setting CPU frequencies in the **PerformanceProfile** for reserved and isolated core CPUs. This is an optional feature that you can use to define specific frequencies. The Node Tuning Operator then sets those frequencies by enabling the **intel_pstate** CPUFreq driver in the Intel hardware. You must follow Intel's recommendations on frequencies for FlexRAN-like applications, which require the default CPU frequency to be set to a lower value than the default running frequency.

1.3.18.5. Node Tuning Operator intel_pstate driver default setting

Previously, for the RAN DU-profile, setting the **realTime** workload hint to **true** in the **PerformanceProfile** always disabled the **intel_pstate**. With this release, the Node Tuning Operator detects the underlying Intel hardware using **TuneD** and appropriately sets the **intel_pstate** kernel parameter based on the processor's generation. This decouples the **intel_pstate** from the **realTime** and **highPowerConsumption** workload hints. The **intel_pstate** now depends only on the underlying processor generation.

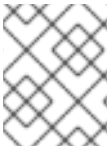
For pre-IceLake processors, the **intel_pstate** is deactivated by default, whereas for IceLake and later generation processors, the **intel_pstate** is set to **active**.

1.3.19. Edge computing

1.3.19.1. Using RHACM PolicyGenerator resources to manage GitOps ZTP cluster policies (Technology Preview)

You can now use **PolicyGenerator** resources and Red Hat Advanced Cluster Management (RHACM) to deploy polices for managed clusters with GitOps ZTP. The **PolicyGenerator** API is part of the Open Cluster Management standard and provides a generic way of patching resources which is not possible with the **PolicyGenTemplate** API. Using **PolicyGenTemplate** resources to manage and deploy polices will be deprecated in an upcoming OpenShift Container Platform release.

For more information, see Configuring managed cluster policies by using PolicyGenerator resources .



NOTE

The **PolicyGenerator** API does not currently support merging patches with custom Kubernetes resources that contain lists of items. For example, in **PtpConfig** CRs.

1.3.19.2. TALM policy remediation

With this release, Topology Aware Lifecycle Manager (TALM) uses a Red Hat Advanced Cluster Management (RHACM) feature to remediate **inform** policies on managed clusters. This enhancement

removes the need for the Operator to create **enforce** copies of **inform** policies during policy remediation. This enhancement also reduces the workload on the hub cluster due to copied policies, and can reduce the overall time required to remediate policies on managed clusters.

For more information, see Update policies on managed clusters .

1.3.19.3. Accelerated provisioning of GitOps ZTP (Technology Preview)

With this release, you can reduce the time taken for cluster installation by using accelerated provisioning of GitOps ZTP for single-node OpenShift. Accelerated ZTP speeds up installation by applying Day 2 manifests derived from policies at an earlier stage.

The benefits of accelerated provisioning of GitOps ZTP increase with the scale of your deployment. Full acceleration gives more benefit on a larger number of clusters. With a smaller number of clusters, the reduction in installation time is less significant.

For more information, see Accelerated provisioning of GitOps ZTP .

1.3.19.4. Image-based upgrade for single-node OpenShift clusters using Lifecycle Agent

With this release, you can use the Lifecycle Agent to orchestrate an image-based upgrade for single-node OpenShift clusters from OpenShift Container Platform <4.y> to <4.y+2>, and <4.y.z> to <4.y.z+n>. The Lifecycle Agent generates an Open Container Initiative (OCI) image that matches the configuration of participating clusters. In addition to the OCI image, the image-based upgrade uses the **ostree** library and the OADP Operator to reduce upgrade and service outage duration when transitioning between the original and target platform versions.

For more information, see Understanding the image-based upgrade for single-node OpenShift clusters .

1.3.19.5. Deploying IPsec encryption to managed clusters with GitOps ZTP and RHACM

You can now enable IPsec encryption in managed single-node OpenShift clusters that you deploy with GitOps ZTP and Red Hat Advanced Cluster Management (RHACM). You can encrypt external traffic between pods and IPsec endpoints external to the managed cluster. All pod-to-pod network traffic between nodes on the OVN-Kubernetes cluster network is encrypted with IPsec in Transport mode.

For more information, see Configuring IPsec encryption for single-node OpenShift clusters using GitOps ZTP and SiteConfig resources.

1.3.20. Hosted control planes

1.3.20.1. Hosted control planes is Generally Available on Amazon Web Services (AWS)

Hosted control planes for OpenShift Container Platform 4.16 is now Generally Available on the AWS platform.

1.3.21. Security

A new signer certificate authority (CA), **openshift-etcd**, is now available to sign certificates. This CA is contained in a trust bundle with the existing CA. Two CA secrets,**etcd-signer** and **etcd-metric-signer**, are also available for rotation. Starting with this release, all certificates will move to a proven library. This change allows for the automatic rotation of all certificates that were not managed by **cluster-etcd-operator**. All node-based certificates will continue with the current update process.

1.4. NOTABLE TECHNICAL CHANGES

OpenShift Container Platform 4.16 introduces the following notable technical changes.

HAProxy version 2.8

OpenShift Container Platform 4.16 uses HAProxy 2.8.

SHA-1 certificates no longer supported for use with HAProxy

SHA-1 certificates are no longer supported for use with HAProxy. Both existing and new routes that use SHA-1 certificates in OpenShift Container Platform 4.16 are rejected and no longer function. For more information about creating secure routes, see Secured Routes.

etcd tuning parameters

With this release, the etcd tuning parameters can be set to values that optimize performance and decrease latency, as follows.

- **""** (Default)
- **Standard**
- **Slower**

Unauthenticated users were removed from some cluster roles

With this release, unauthenticated users no longer have access to specific cluster roles that are necessary for certain feature sets. Before OpenShift Container Platform 4.16 unauthenticated users could access certain cluster roles. Changing this access for unauthenticated users adds an additional layer of security and should only be enabled when necessary. This change is for new clusters; previous clusters are not affected.

There are use cases where you might want to give access to unauthenticated users for specific cluster roles. To grant unauthenticated users access to specific cluster roles that are necessary for certain features, see Adding unauthenticated groups to cluster roles .

IMPORTANT

Always verify compliance with your organization's security standards when modifying unauthenticated access.

RHCOS dasd image artifacts no longer supported on IBM Z(R) and IBM(R) LinuxONE (s390x)

With this release, **dasd** image artifacts for the **s390x** architecture are removed from the OpenShift Container Platform image building pipeline. You can still use the **metal4k** image artifact, which is identical and contains the same functionality.

Support for EgressIP with ExternalTrafficPolicy=Local services

Previously, it was unsupported for EgressIP selected pods to also serve as backends for services with **externalTrafficPolicy** set to **Local**. When attempting this configuration, service ingress traffic reaching the pods was incorrectly rerouted to the egress node hosting the EgressIP. This affected how responses to incoming service traffic connections were handled and led to non-functional services when **externalTrafficPolicy** was set to **Local**, as connections were dropped and the service became unavailable.

With OpenShift Container Platform 4.16, OVN-Kubernetes now supports the use of **ExternalTrafficPolicy=Local** services and EgressIP configurations at the same time on the same set of selected pods. OVN-Kubernetes now only reroutes the traffic originating from the EgressIP pods

towards the egress node while routing the responses to ingress service traffic from the EgressIP pods via the same node where the pod is located.

Legacy service account API token secrets are no longer generated for each service account

Before OpenShift Container Platform 4.16, when the integrated OpenShift image registry was enabled, a legacy service account API token secret was generated for every service account in the cluster. Starting with OpenShift Container Platform 4.16, when the integrated OpenShift image registry is enabled, the legacy service account API token secret is no longer generated for each service account.

Additionally, when the integrated OpenShift image registry is enabled, the image pull secret generated for every service account no longer uses a legacy service account API token. Instead, the image pull secret now uses a bound service account token that is automatically refreshed before it expires.

For more information, see Automatically generated image pull secrets.

For information about detecting legacy service account API token secrets that are in use in your cluster or deleting them if they are not needed, see the Red Hat Knowledgebase article Long-lived service account API tokens in OpenShift Container Platform.

Support for external cloud authentication providers

In this release, the functionality to authenticate to private registries on Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure clusters is moved from the in-tree provider to binaries that ship with OpenShift Container Platform. This change supports the default external cloud authentication provider behavior that is introduced in Kubernetes 1.29.

The builder service account is no longer created if the Build cluster capability is disabled

With this release, if you disable the **Build** cluster capability, the **builder** service account and its corresponding secrets are no longer created.

For more information, see Build capability.

Default OLM 1.0 upgrade constraints changed to legacy OLM semantics (Technology Preview)

In OpenShift Container Platform 4.16, Operator Lifecycle Manager (OLM) 1.0 changes its default upgrade constraints from semantic versioning (semver) to legacy OLM semantics.

For more information, see Support for legacy OLM upgrade edges in OLM 1.0 (Technology Preview) .

Removal of the RukPak Bundle API from OLM 1.0 (Technology Preview)

In OpenShift Container Platform 4.16, Operator Lifecycle Manager (OLM) 1.0 removes the **Bundle** API, which was provided by the RukPak component. The RukPak **BundleDeployment** API remains and supports **registry+v1** bundles for unpacking Kubernetes YAML manifests organized in the legacy Operator Lifecycle Manager (OLM) bundle format.

For more information, see Rukpak (Technology Preview).

dal12 region was added

With this release, the **dal12** region has been added to the IBM Power® VS Installer.

Regions added to IBM Power(R) Virtual Server

This release introduces the ability to deploy to new IBM Power® Virtual Server (VS) regions **osa21**, **syd04**, **lon06**, and **sao01**.

IBM Power(R) Virtual Server updated to use Cluster API Provider IBM Cloud 0.8.0

With this release, the IBM Power® Virtual Server has been updated to use Cluster API Provider IBM Cloud version 0.8.0.

Additional debugging statements for ServiceInstanceNameToGUID

With this release, additional debugging statements were added to the **ServiceInstanceNameToGUID** function.

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 4.16, 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:

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

Operator lifecycle and development deprecated and removed features

Table 1.6. Operator lifecycle and development deprecated and removed tracker

Feature	4.14	4.15	4.16
Operator SDK	General Availability	General Availability	Deprecated
Scaffolding tools for Ansible-based Operator projects	General Availability	General Availability	Deprecated
Scaffolding tools for Helm-based Operator projects	General Availability	General Availability	Deprecated
Scaffolding tools for Go-based Operator projects	General Availability	General Availability	Deprecated
Scaffolding tools for Hybrid Helm-based Operator projects	Technology Preview	Technology Preview	Deprecated
Scaffolding tools for Java-based Operator projects	Technology Preview	Technology Preview	Deprecated

Feature	4.14	4.15	4.16
Platform Operators	Technology Preview	Technology Preview	Removed
Plain bundles	Technology Preview	Technology Preview	Removed
SQLite database format for Operator catalogs	Deprecated	Deprecated	Deprecated

Images deprecated and removed features

Table 1.7. Cluster Samples Operator deprecated and removed tracker

Feature	4.14	4.15	4.16
Cluster Samples Operator	General Availability	General Availability	Deprecated

Monitoring deprecated and removed features

Table 1.8. Monitoring deprecated and removed tracker

Feature	4.14	4.15	4.16
dedicatedServiceMonitors setting that enables dedicated service monitors for core platform monitoring	General Availability	Deprecated	Removed
prometheus-adapter component that queries resource metrics from Prometheus and exposes them in the metrics API.	General Availability	Deprecated	Removed

Installation deprecated and removed features

Table 1.9. Installation deprecated and removed tracker

Feature	4.14	4.15	4.16
OpenShift SDN network plugin	Deprecated	Removed [1]	Removed
--cloud parameter for **oc adm release extract**	Deprecated	Deprecated	Deprecated
CoreDNS wildcard queries for the **cluster.local** domain	Deprecated	Deprecated	Deprecated
compute.platform.openstack.rootVolume.type for RHOSP	Deprecated	Deprecated	Deprecated

Feature	4.14	4.15	4.16
controlPlane.platform.openstack.rootVolume.type for RHOSP	Deprecated	Deprecated	Deprecated
ingressVIP and **apiVIP** settings in the **install-config.yaml** file for installer-provisioned infrastructure clusters	Deprecated	Deprecated	Deprecated
Package-based RHEL compute machines	General Availability	General Availability	Deprecated
platform.aws.preserveBootstrapIgnition parameter for Amazon Web Services (AWS)	General Availability	General Availability	Deprecated
Terraform infrastructure provider for Amazon Web Services (AWS), VMware vSphere and Nutanix	General Availability	General Availability	Removed
Terraform infrastructure provider for Google Cloud Platform (GCP)	General Availability	General Availability	Removable as Technology Preview
Installing a cluster on Alibaba Cloud with installer-provisioned infrastructure	Technology Preview	Technology Preview	Removed

1. While the OpenShift SDN network plugin is no longer supported by the installation program in version 4.15, you can upgrade a cluster that uses the OpenShift SDN plugin from version 4.14 to version 4.15.

Updating clusters deprecated and removed features

Table 1.10. Updating clusters deprecated and removed tracker

Feature	4.14	4.15	4.16

Storage deprecated and removed features

Table 1.11. Storage deprecated and removed tracker

Feature	4.14	4.15	4.16
Persistent storage using FlexVolume	Deprecated	Deprecated	Deprecated
AliCloud Disk CSI Driver Operator	General Availability	General Availability	Removed

Networking deprecated and removed features

Table 1.12. Networking deprecated and removed tracker

Feature	4.14	4.15	4.16
Kuryr on RHOSP	Deprecated	Removed	Removed
OpenShift SDN network plugin	Deprecated	Deprecated	Deprecated
iptables	Deprecated	Deprecated	Deprecated

Web console deprecated and removed features

Table 1.13. Web console deprecated and removed tracker

Feature	4.14	4.15	4.16
Patternfly 4	General Availability	Deprecated	Deprecated
React Router 5	General Availability	Deprecated	Deprecated

Node deprecated and removed features

Table 1.14. Node deprecated and removed tracker

Feature	4.14	4.15	4.16
ImageContentSourcePolicy (ICSP) objects	Deprecated	Deprecated	Deprecated
Kubernetes topology label **failure-domain.beta.kubernetes.io/zone**	Deprecated	Deprecated	Deprecated
Kubernetes topology label **failure-domain.beta.kubernetes.io/region**	Deprecated	Deprecated	Deprecated
cgroup v1	General Availability	General Availability	Deprecated

Workloads deprecated and removed features

Table 1.15. Workloads deprecated and removed tracker

Feature	4.14	4.15	4.16
DeploymentConfig objects	Deprecated	Deprecated	Deprecated

Bare metal monitoring deprecated and removed features

Table 1.16. Bare Metal Event Relay Operator tracker

Feature	4.14	4.15	4.16
Bare Metal Event Relay Operator	Technology Preview	Deprecated	Deprecated

1.5.1. Deprecated features

1.5.1.1. Linux Control Groups version 1 is now deprecated

In Red Hat Enterprise Linux (RHEL) 9, the default mode is cgroup v2. When Red Hat Enterprise Linux (RHEL) 10 is released, systemd will not support booting in the cgroup v1 mode and only cgroup v2 mode will be available. As such, cgroup v1 is deprecated in OpenShift Container Platform 4.16 and later. cgroup v1 will be removed in a future OpenShift Container Platform release.

1.5.1.2. Cluster Samples Operator

The Cluster Samples Operator is deprecated with the OpenShift Container Platform 4.16 release. The Cluster Samples Operator will stop managing and providing support to the non-S2I samples (image streams and templates). No new templates, samples or non-Source-to-Image (Non-S2I) image streams will be added to the Cluster Samples Operator. However, the existing S2I builder image streams and templates will continue to receive updates until the Cluster Samples Operator is removed in a future release.

1.5.1.3. Package-based RHEL compute machines

With this release, installation of package-based RHEL worker nodes is deprecated. In a subsequent future release, RHEL worker nodes will be removed and no longer supported.

RHCOS image layering will replace this feature and supports installing additional packages on the base operating system of your worker nodes.

For more information about image layering, see RHCOS image layering.

1.5.1.4. Operator SDK CLI tool and related testing and scaffolding tools are deprecated

The Red Hat-supported version of the Operator SDK CLI tool, including the related scaffolding and testing tools for Operator projects, is deprecated and is planned to be removed in a future release of OpenShift Container Platform. Red Hat will provide bug fixes and support for this feature during the current release lifecycle, but this feature will no longer receive enhancements and will be removed from future OpenShift Container Platform releases.

The Red Hat-supported version of the Operator SDK is not recommended for creating new Operator projects. Operator authors with existing Operator projects can use the version of the Operator SDK CLI tool released with OpenShift Container Platform 4.16 to maintain their projects and create Operator releases targeting newer versions of OpenShift Container Platform.

The following related base images for Operator projects are *not* deprecated. The runtime functionality and configuration APIs for these base images are still supported for bug fixes and for addressing CVEs.

- The base image for Ansible-based Operator projects
- The base image for Helm-based Operator projects

For information about the unsupported, community-maintained, version of the Operator SDK, see Operator SDK (Operator Framework).

1.5.1.5. The preserveBootstrapIgnition parameter on Amazon Web Services (AWS) is deprecated

The **preserveBootstrapIgnition** parameter for Amazon Web Services in **the install-config.yaml** file has been deprecated. You can use the **bestEffortDeleteIgnition** parameter instead.

1.5.2. Removed features

1.5.2.1. Deprecated disk partition configuration method

The **nodes.diskPartition** section in the **SiteConfig** custom resource (CR) is deprecated with the OpenShift Container Platform 4.16 release. This configuration has been replaced with the **ignitionConfigOverride** method, which provides a more flexible way of creating a disk partition for any use case.

For more information, see Configuring disk partitioning with SiteConfig.

1.5.2.2. Removal of platform Operators and plain bundles (Technology Preview)

OpenShift Container Platform 4.16 removes platform Operators (Technology Preview) and plain bundles (Technology Preview), which were prototypes for Operator Lifecycle Manager (OLM) 1.0 (Technology Preview).

1.5.2.3. Dell iDRAC driver for BMC addressing removed

OpenShift Container Platform 4.16 supports baseboard management controller (BMC) addressing with Dell servers as documented in BMC addressing for Dell iDRAC. Specifically, it supports **idrac-virtualmedia**, **redfish**, and **ipmi**. In previous versions, **idrac** was included, but not documented or supported. In OpenShift Container Platform 4.16, **idrac** has been removed.

1.5.2.4. Dedicated service monitors for core platform monitoring

With this release, the dedicated service monitors feature for core platform monitoring has been removed. You can no longer enable this feature in the **cluster-monitoring-config** config map object in the **openshift-monitoring** namespace. To replace this feature, Prometheus functionality has been improved to ensure that alerts and time aggregations are accurate. This improved functionality is active by default and makes the dedicated service monitors feature obsolete.

1.5.2.5. Prometheus Adapter for core platform monitoring

With this release, the Prometheus Adapter component for core platform monitoring has been removed. It has been replaced by the new Metrics Server component.

1.5.2.6. MetalLB AddressPool custom resource definition (CRD) removed

The MetalLB **AddressPool** custom resource definition (CRD) has been deprecated for several versions. However, in this release, the CRD is completely removed. The sole supported method of configuring MetalLB address pools is by using the **IPAddressPools** CRD.

1.5.2.7. Service Binding Operator documentation removed

With this release, the documentation for the Service Binding Operator (SBO) has been removed because this Operator is no longer supported.

1.5.2.8. AliCloud CSI Driver Operator is no longer supported

OpenShift Container Platform 4.16 no longer supports AliCloud Container Storage Interface (CSI) Driver Operator.

1.5.2.9. Beta APIs removed from Kubernetes 1.29

Kubernetes 1.29 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 1.17. APIs removed from Kubernetes 1.29

Resource	Removed API	Migrate to	Notable changes
FlowSchema	**flowcontrol.apiserver.k8s.io/v1beta2**	**flowcontrol.apiserver.k8s.io/v1** or **flowcontrol.apiserver.k8s.io/v1beta3**	No
PriorityLevelConfiguration	**flowcontrol.apiserver.k8s.io/v1beta2**	**flowcontrol.apiserver.k8s.io/v1** or **flowcontrol.apiserver.k8s.io/v1beta3**	Yes

1.6. BUG FIXES

API Server and Authentication

- Previously, **ephemeral** and **csi** volumes were not properly added to security context constraints (SCCs) on upgraded clusters. With this release, SCCs on upgraded clusters are properly updated to have **ephemeral** and **csi** volumes. (OCPBUGS-33522)
- Previously, the **ServiceAccounts** resource could not be used with OAuth clients for a cluster with the **ImageRegistry** capability enabled. With this release, this issue is fixed. (OCPBUGS-30319)
- Previously, when you created a pod with an empty security context and you have access to all security context constraints (SCCs), the pod would receive the **anyuid** SCC. After the **ovn-controller** component added a label to the pod, the pod would be re-admitted for SCC selection, where the pod received an escalated SCC, such as **privileged**. With this release, this issue is resolved so the pod is not re-admitted for SCC selection. (OCPBUGS-11933)
- Previously, the **hostmount-anyuid** security context constraints (SCC) did not have a built-in cluster role because the name of the SCC was incorrectly named **hostmount** in the cluster role. With this release, the SCC name in the cluster role was updated properly to **hostmount-anyuid**, so the **hostmount-anyuid** SCC now has a functioning cluster role. (OCPBUGS-33184)
- Previously, clusters that were created before OpenShift Container Platform 4.7 had several secrets of type **SecretTypeTLS**. Upon upgrading to OpenShift Container Platform 4.16, these

secrets are deleted and re-created with the type **kubernetes.io/tls**. This removal could cause a race condition and the contents of the secrets could be lost. With this release, the secret type change now happens automatically and clusters created before OpenShift Container Platform 4.7 can upgrade to 4.16 without risking losing the contents of these secrets. (OCPBUGS-31384)

- Previously, some Kubernetes API server events did not have the correct timestamps. With this release, Kubernetes API server events now have the correct timestamps. (OCPBUGS-27074)

- Previously, the Kubernetes API Server Operator attempted to delete a Prometheus rule that was removed in OpenShift Container Platform 4.13 to ensure it was deleted. This resulted in failed deletion messages in the audit logs every few minutes. With this release, the Kubernetes API Server Operator no longer attempts to remove this nonexistent rule and there are no more failed deletion messages in the audit logs. (OCPBUGS-25894)

Bare Metal Hardware Provisioning

- Previously, newer versions of Redfish used Manager resources to deprecate the Uniform Resource Identifier (URI) for the RedFish Virtual Media API. This caused any hardware that used the newer Redfish URI for Virtual Media to not be provisioned. With this release, the Ironic API identifies the correct Redfish URI to deploy for the RedFish Virtual Media API so that hardware relying on either the deprecated or newer URI could be provisioned. (OCPBUGS-30171)

- Previously, the Bare Metal Operator (BMO) was not using a leader lock to control incoming and outgoing Operator pod traffic. After an OpenShift **Deployment** object included a new Operator pod, the new pod competed with system resources, such as the **ClusterOperator** status, and this terminated any outgoing Operator pods. This issue also impacted clusters that do not include any bare-metal nodes. With this release, the BMO includes a leader lock to manage new pod traffic, and this fix resolves the competing pod issue. (OCPBUGS-25766)

- Previously, when you attempted to delete a **BareMetalHost** object before the installation started, the metal3 Operator attempted to create a **PreprovImage** image. The process of creating this image caused the **BareMetalHost** object to still exist in certain processes. With this release, an exception is added for this situation so that the **BareMetalHost** object is deleted without impacting running processes. (OCPBUGS-33048)

- Previously, a Redfish virtual media in the context of Hewlett Packard Enterprise (HPE) Lights Out (iLO) 5 had its bare-metal machine compression forcibly disabled to work around other unrelated issues in different hardware models. This caused the **FirmwareSchema** resource to be missing from each iLO 5 bare-metal machine. Each machine needs compression to fetch message registries from their Redfish Baseboard Management Controller (BMC) endpoints. With this release, each iLO 5 bare-metal machine that needs the **FirmwareSchema** resource does not have compression forcibly disabled. (OCPBUGS-31104)

- Previously, the **inspector.ipxe** configuration file used the **IRONIC_IP** variable, which did not account for IPv6 addresses because they have brackets. Consequently, when the user supplied an incorrect **boot_mac_address**, iPXE fell back to the **inspector.ipxe** configuration file, which supplied a malformed IPv6 host header since it did not contain brackets. With this release, the **inspector.ipxe** configuration file has been updated to use the **IRONIC_URL_HOST** variable, which accounts for IPv6 addresses and resolves the issue. (OCPBUGS-22699)

- Previously, Ironic Python Agent assumed all server disks to have a 512 byte sector size when trying to wipe disks. This caused the disk wipe to fail. With this release, Ironic Python Agent checks the disk sector size and has separate values for disk wiping so that the disk wipe succeeds. (OCPBUGS-31549)

Builds

- Previously, clusters that updated from earlier versions to 4.16 continued to allow builds to be triggered by unauthenticated webhooks. With this release, new clusters require build webhooks to be authenticated. Builds are not triggered by unauthenticated webhooks unless a cluster administrator allows unauthenticated webhooks in the namespace or cluster. (OCPBUGS-33378)

- Previously, if the developer or cluster administrator used lowercase environment variable names for proxy information, these environment variables were carried into the build output container image. At runtime, the proxy settings were active and had to be unset. With this release, lowercase versions of the ***_PROXY** environment variables are prevented from leaking into built container images. Now, **buildDefaults** are only kept during the build and settings created for the build process only are removed before pushing the image in the registry. (OCPBUGS-34825)

Cloud Compute

- Previously, the Cloud Controller Manager (CCM) Operator used predefined roles on Google Cloud Platform (GCP) instead of granular permissions. With this release, the CCM Operator is updated to use granular permissions on GCP clusters. (OCPBUGS-26479)

- Previously, the installation program populated the **network.devices**, **template** and **workspace** fields in the **spec.template.spec.providerSpec.value** section of the VMware vSphere control plane machine set custom resource (CR). These fields should be set in the vSphere failure domain, and the installation program populating them caused unintended behaviors. Updating these fields did not trigger an update to the control plane machines, and these fields were cleared when the control plane machine set was deleted.
  With this release, the installation program is updated to no longer populate values that are included in the failure domain configuration. If these values are not defined in a failure domain configuration, for instance on a cluster that is updated to OpenShift Container Platform 4.16 from an earlier version, the values defined by the installation program are used. (OCPBUGS-32947)

- Previously, a node associated with a rebooting machine briefly having a status of **Ready=Unknown** triggered the **UnavailableReplicas** condition in the Control Plane Machine Set Operator. This condition caused the Operator to enter the **Available=False** state and trigger alerts because that state indicates a nonfunctional component that requires immediate administrator intervention. This alert should not have been triggered for the brief and expected unavailabilty while rebooting. With this release, a grace period for node unreadiness is added to avoid triggering unnecessary alerts. (OCPBUGS-34970)

- Previously, a transient failure to fetch bootstrap data during machine creation, such as a transient failure to connect to the API server, caused the machine to enter a terminal failed state. With this release, failure to fetch bootstrap data during machine creation is retried indefinitely until it eventually succeeds. (OCPBUGS-34158)

- Previously, the Machine API Operator operator panicked when deleting a server in an error state because it was not passed a port list. With this release, deleting a machine stuck in an **ERROR** state does not crash the controller. (OCPBUGS-34155)

- Previously, an optional internal function of the cluster autoscaler caused repeated log entries when it was not implemented. The issue is resolved in this release. (OCPBUGS-33932)

- Previously, if the control plane machine set was created with a template without a path during installation on a VMware vSphere cluster, the Control Plane Machine Set Operator rejected modification or deletion of the control plane machine set custom resource (CR). With this release, the Operator allows template names for vSphere in the control plane machine set definition. (OCPBUGS-32295)

- Previously, the Control Plane Machine Set Operator crashed when attempting to update a VMware vSphere cluster because the infrastructure resource was not configured. With this release, the Operator can handle this scenario so that the cluster update is able to proceed. (OCPBUGS-31808)

- Previously, when a user created a compute machine set with taints, they could choose to not specify the **Value** field. Failure to specify this field caused the cluster autoscaler to crash. With this release, the cluster autoscaler is updated to handle an empty **Value** field. (OCPBUGS-31421)

- Previously, IPv6 services were wrongly marked as internal on the RHOSP cloud provider, making it impossible to share IPv6 load balancers between OpenShift Container Platform services. With this release, IPv6 services are not marked as internal, allowing IPv6 load balancers to be shared between services that use stateful IPv6 addresses. This fix allows load balancers to use stateful IPv6 addresses that are defined in the **loadBalancerIP** property of the service. (OCPBUGS-29605)

- Previously, when a control plane machine was marked as unready and a change was initiated by the modifying the control plane machine set, the unready machine was removed prematurely. This premature action caused multiple indexes to be replaced simultaneously. With this release, the control plane machine set no longer deletes a machine when only a single machine exists within the index. This change prevents premature roll-out of changes and prevents more than one index from being replaced at a time. (OCPBUGS-29249)

- Previously, connections to the Azure API sometimes hung for up to 16 minutes. With this release, a timeout is introduced to prevent hanging API calls. (OCPBUGS-29012)

- Previously, the Machine API IBM Cloud controller did not integrate the full logging options from the **klogr** package. As a result, the controller crashed in Kubernetes version 1.29 and later. With this release, the missing options are included and the issue is resolved. (OCPBUGS-28965)

- Previously, the Cluster API IBM Power Virtual Server controller pod would start on the unsupported IBM Cloud platform. This caused the controller pod to get stuck in the creation phase. With this release, the cluster detects the difference between IBM Power Virtual Server and IBM Cloud. The cluster then only starts on the supported platform. (OCPBUGS-28539)

- Previously, the machine autoscaler could not account for any taint set directly on the compute machine set spec due to a parsing error. This could cause undesired scaling behavior when relying on a compute machine set taint to scale from zero. The issue is resolved in this release and the machine autoscaler can now scale up correctly and identify taints that prevent workloads from scheduling. (OCPBUGS-27509)

- Previously, machine sets that ran on Microsoft Azure regions with no availability zone support always created **AvailabilitySets** objects for Spot instances. This operation caused Spot instances to fail because the instances did not support availability sets. With this release, machine sets do not create **AvailabilitySets** objects for Spot instances that operate in non-zonal configured regions. (OCPBUGS-25940)

- Previously, the removal of code that provided image credentials from the kubelet in OpenShift Container Platform 4.14 caused pulling images from the Amazon Elastic Container Registry (ECR) to fail without a specified pull secret. This release includes a separate credential provider that provides ECR credentials for the kubelet. (OCPBUGS-25662)

- Previously, the default VM type for the Azure load balancer was changed from **Standard** to **VMSS**, but the service type load balancer code could not attach standard VMs to load balancers. With this release, the default VM type is reverted to remain compatible with OpenShift Container Platform deployments. (OCPBUGS-25483)

- Previously, OpenShift Container Platform did not include the cluster name in the names of the RHOSP load balancer resources that were created by the OpenStack Cloud Controller Manager. This behavior caused issues when **LoadBalancer** services had the same name in multiple clusters that ran in a single RHOSP project. With this release, the cluster name is included in the names of Octavia resources. When upgrading from a previous cluster version, the load balancers are renamed. The new names follow the pattern **kube_service_<cluster-name>_<namespace>_<service-name>** instead of **kube_service_kubernetes_<namespace>_<service-name>**. (OCPBUGS-13680)

- Previously, when you created or deleted large volumes of service objects simultaneously, service controller ability to process each service sequentially would slow down. This caused short timeout issues for the service controller and backlog issues for the objects. With this release, the service controller can now process up to 10 service objects simultaneously to reduce the backlog and timeout issues. (OCPBUGS-13106)

- Previously, the logic that fetches the name of a node did not account for the possibility of multiple values for the returned hostname from the AWS metadata service. When multiple domains are configured for a VPC Dynamic Host Configuration Protocol (DHCP) option, this hostname might return multiple values. The space between multiple values caused the logic to crash. With this release, the logic is updated to use only the first returned hostname as the node name. (OCPBUGS-10498)

- Previously, the Machine API Operator requested unnecessary **virtualMachines/extensions** permissions on Microsoft Azure clusters. The unnecessary credentials request is removed in this release. (OCPBUGS-29956)

Cloud Credential Operator

- Previously, the Cloud Credential Operator (CCO) was missing some permissions required to create a private cluster on Microsoft Azure. These missing permissions prevented installation of an Azure private cluster using Microsoft Entra Workload ID. This release includes the missing permissions and enables installation of an Azure private cluster using Workload ID. (OCPBUGS-25193)

- Previously, a bug caused the Cloud Credential Operator (CCO) to report an incorrect mode in the metrics. Even though the cluster was in the default mode, the metrics reported that it was in the credentials removed mode. This update uses a live client in place of a cached client so that it is able to obtain the root credentials, and the CCO no longer reports an incorrect mode in the metrics. (OCPBUGS-26488)

- Previously, the Cloud Credential Operator credentials mode metric on an OpenShift Container Platform cluster that uses Microsoft Entra Workload ID reported using manual mode. With this release, clusters that use Workload ID are updated to report that they are using manual mode with pod identity. (OCPBUGS-27446)

- Previously, creating an Amazon Web Services (AWS) root secret on a bare metal cluster caused the Cloud Credential Operator (CCO) pod to crash. The issue is resolved in this release. (OCPBUGS-28535)

- Previously, removing the root credential from a Google Cloud Platform (GCP) cluster that used the Cloud Credential Operator (CCO) in mint mode caused the CCO to become degraded after approximately one hour. In a degraded state, the CCO cannot manage the component credential secrets on a cluster. The issue is resolved in this release. (OCPBUGS-28787)

- Previously, the Cloud Credential Operator (CCO) checked for a nonexistent **s3:HeadBucket** permission during installation on Amazon Web Services (AWS). When the CCO failed to find this permission, it considered the provided credentials insufficient for mint mode. With this release,

the CCO no longer checks for the nonexistent permission. (OCPBUGS-31678)

Cluster Version Operator

- This release expands the **ClusterOperatorDown** and **ClusterOperatorDegraded** alerts to cover ClusterVersion conditions and send alerts for **Available=False** (**ClusterOperatorDown**) and **Failing=True** (**ClusterOperatorDegraded**). In previous releases, those alerts only covered **ClusterOperator** conditions. (OCPBUGS-9133)

- Previously, Cluster Version Operator (CVO) changes that were introduced in OpenShift Container Platform 4.15.0, 4.14.0, 4.13.17, and 4.12.43 caused failing risk evaluations to block the CVO from fetching new update recommendations. When the risk evaluations failed, the bug caused the CVO to overlook the update recommendation service. With this release, the CVO continues to poll the update recommendation service, regardless of whether update risks are being successfully evaluated and the issue has been resolved. (OCPBUGS-25708)

Developer Console

- Previously, when a serverless function was created in the create serverless form, **BuilldConfig** was not created. With this update, if the Pipelines Operator is not installed, the pipeline resource is not created for particular resource, or the pipeline is not added while creating a serverless function, it will create **BuildConfig** as expected. (OCPBUGS-34143)

- Previously, after installing the Pipelines Operator, Pipeline templates took some time to become available in the cluster, but users were still able to create the deployment. With this update, the **Create** button on the **Import from Git** page is disabled if there is no pipeline template present for the resource selected. (OCPBUGS-34142)

- Previously, the maximum number of nodes was set to **100** on the **Topology** page. A persistent alert, "Loading is taking longer than expected." was provided. With this update, the limit of nodes is increased to **300**. (OCPBUGS-32307)

- With this update, an alert message to notify you that Service Bindings are deprecated with OpenShift Container Platform 4.15 was added to the **ServiceBinding list**, **ServiceBinding details**, **Add**, and **Topology** pages when creating a **ServiceBinding**, binding a component, or a **ServiceBinding** was found in the current namespace. (OCPBUGS-32222)

- Previously, the Helm Plugin index view did not display the same number of charts as the Helm CLI if the chart names varied. With this release, the Helm catalog now looks for **charts.openshift.io/name** and **charts.openshift.io/provider** so that all versions are grouped together in a single catalog title. (OCPBUGS-32059)

- Previously, the **TaskRun** status was not displayed near the **TaskRun** name on the **TaskRun details** page. With this update, the **TaskRun** status is located beside the name of the **TaskRun** in the page heading. (OCPBUGS-31745)

- Previously, there is an error when adding parameters to the Pipeline when the resources field was added to the payload, and as resources are deprecated. With this update, the resources fields have been removed from the payload, and you can add parameters to the Pipeline. (OCPBUGS-31082)

- This release updates the OpenShift Pipelines plugin to support the latest Pipeline Trigger API version for the custom resource definitions (CRDs) **ClusterTriggerBinding**, **TriggerTemplate** and **EventListener**. (OCPBUGS-30958)

- Previously, **CustomTasks** were not recognized or remained in a **Pending** state. With this update, **CustomTasks** can be easily identified from the Pipelines **List** and **Details** pages. (OCPBUGS-29513)

- Previously, if there was a build output image with an **Image** tag then the **Output Image** link would not redirect to the correct **ImageStream** page. With this update, this has been fixed by generating a URL for the **ImageStream** page without adding the tag in the link. (OCPBUGS-29355)

- Previously, **BuildRun** logs were not visible in the **Logs** tab of the **BuildRun** page due to a recent update in the API version of the specified resources. With this update, the logs of the **TaskRuns** were added back into the **Logs** tab of the **BuildRun** page for both v1alpha1 and v1beta1 versions of the Builds Operator. (OCPBUGS-27473)

- Previously, the annotations to set scale bound values were setting to **autoscaling.knative.dev/maxScale** and **autoscaling.knative.dev/minScale**. With this update, the annotations to set scale bound values are updated to **autoscaling.knative.dev/min-scale** and **autoscaling.knative.dev/max-scale** to determine the minimum and maximum numbers of replicas that can serve an application at any given time. You can set scale bounds for an application to help prevent cold starts or control computing costs. (OCPBUGS-27469)

- Previously, the **Log** tab for **PipelineRuns** from the Tekton Results API never finished loading. With this release, this tab loads fully complete for PipelineRuns loaded from the Kubernetes API or the Tekton Results API. (OCPBUGS-25612)

- Previously, there was no indicator shown to differentiate between **PipelineRuns** that are loaded from the Kubernetes API or the Tekton Results API. With this update, a small archived icon in the **PipelineRun list** and **details** page to differentiate between **PipelineRuns** that are loaded from the Kubernetes API or the Tekton Results API. (OCPBUGS-25396)

- Previously, on the **PipelineRun list** page, all TaskRuns were fetched and separated based on **pipelineRun** name. With this update, TaskRuns are fetched only for **Failed** and **Cancelled** PipelineRun. A caching mechanism was also added to fetch PipelineRuns and TaskRuns associated to the **Failed** and **Cancelled** PipelineRuns. (OCPBUGS-23480)

- Previously, the visual connector was not present between the VMs node and other non-VMs nodes in the **Topology** view. With this update, the visual connector is located between VMs nodes and non-VMs nodes. (OCPBUGS-13114)

Edge computing

- Previously, an issue with image based upgrades on clusters that use proxy configurations caused operator rollouts that lengthened startup times. With this release, the issue has been fixed and upgrade times are reduced. (OCPBUGS-33471)

etcd Cluster Operator

- Previously, the **wait-for-ceo** command that was used during bootstrap to verify etcd rollout did not report errors for some failure modes. With this release, those error messages now are visible on the **bootkube** script if the **cmd** exits in an error case. (OCPBUGS-33495)

- Previously, the etcd Cluster Operator entered a state of panic during pod health checks and this caused requests to an **etcd** cluster to fail. With this release, the issue is fixed so that these panic situations no longer occur. (OCPBUGS-27959)

- Previously, the etcd Cluster Operator wrongly identified non-running controllers as deadlocked and this caused an unnecessary pod restart. With this release, this issue is now fixed so that the

Operator marks a non-running controller as an unhealthy etcd member without restarting a pod. (OCPBUGS-30873)

Hosted control planes

- Previously, Multus Container Network Interface (CNI) required certificate signing requests (CSRs) to be approved when you used the **Other** network type in hosted clusters. The proper role-based access control (RBAC) rules were set only when the network type was **Other** and was set to Calico. As a consequence, the CSRs were not approved when the network type was **Other** and set to Cilium. With this update, the correct RBAC rules are set for all valid network types, and RBACs are now properly configured when you use the **Other** network type. (OCPBUGS-26977)

- Previously, an Amazon Web Services (AWS) policy issue prevented the Cluster API Provider AWS from retrieving the necessary domain information. As a consequence, installing an AWS hosted cluster with a custom domain failed. With this update, the policy issue is resolved. (OCPBUGS-29391)

- Previously, in disconnected environments, the HyperShift Operator ignored registry overrides. As a consequence, changes to node pools were ignored, and node pools encountered errors. With this update, the metadata inspector works as expected during the HyperShift Operator reconciliation, and the override images are properly populated. (OCPBUGS-34773)

- Previously, the HyperShift Operator was not using the **RegistryOverrides** mechanism to inspect the image from the internal registry. With this release, the metadata inspector works as expected during the HyperShift Operator reconciliation, and the **OverrideImages** are properly populated. (OCPBUGS-32220)

- Previously, the Red Hat OpenShift Cluster Manager container did not have the correct Transport Layer Security (TLS) certificates. As a result, image streams could not be used in disconnected deployments. With this update, the TLS certificates are added as projected volumes. (OCPBUGS-34390)

- Previously, the **azure-kms-provider-active** container in the KAS pod used an entrypoint statement in shell form in the Dockerfile. As a consequence, the container failed. To resolve this issue, use the **exec** form for the entrypoint statement. (OCPBUGS-33940)

- Previously, the **konnectivity-agent** daemon set used the **ClusterIP** DNS policy. As a result, when CoreDNS was down, the **konnectivity-agent** pods on the data plane could not resolve the proxy server URL, and they could fail to **konnectivity-server** in the control plane. With this update, the **konnectivity-agent** daemon set was modified to use **dnsPolicy: Default**. The **konnectivity-agent** uses the host system DNS service to look up the proxy server address, and it does not depend on CoreDNS anymore. (OCPBUGS-31444)

- Previously, the inability to find a resource caused re-creation attempts to fail. As a consequence, many **409** response codes were logged in Hosted Cluster Config Operator logs. With this update, specific resources were added to the cache so that the Hosted Cluster Config Operator does not try to re-create existing resources. (OCPBUGS-23228)

- Previously, the pod security violation alert was missing in hosted clusters. With this update, the alert is added to hosted clusters. (OCPBUGS-31263)

- Previously, the **recycler-pod** template in hosted clusters in disconnected environments pointed to **quay.io/openshift/origin-tools:latest**. As a consequence, the recycler pods failed to start. With this update, the recycler pod image now points to the OpenShift Container Platform payload reference. (OCPBUGS-31398)

- With this update, in disconnected deployments, the HyperShift Operator receives the new **ImageContentSourcePolicy** (ICSP) or **ImageDigestMirrorSet** (IDMS) from the management cluster and adds them to the HyperShift Operator and the Control Plane Operator in every reconciliation loop. The changes to the ICSP or IDMS cause the **control-plane-operator** pod to be restarted. (OCPBUGS-29110)

- With this update, the **ControllerAvailabilityPolicy** setting becomes immutable after it is set. Changing between **SingleReplica** and **HighAvailability** is not supported. (OCPBUGS-27282)

- With this update, the **machine-config-operator** custom resource definitions (CRDs) are renamed to ensure that resources are being omitted properly in hosted control planes. (OCPBUGS-34575)

- With this update, the size is reduced for audit log files that are stored in the **kube-apiserver**, **openshift-apiserver**, and **oauth-apiserver** pods for hosted control planes. (OCPBUGS-31106)

- Previously, the Hypershift Operator was not using the **RegistryOverrides** mechanism to inspect the image from the internal registry. With this release, the metadata inspector works as expected during the Hypershift Operator reconciliation, and the **OverrideImages** are properly populated. (OCPBUGS-29494)

Image Registry

- Previously, after you imported image streams tags, the **ImageContentSourcePolicy** (ICSP) custom resource (CR) could not co-exist with the **ImageDigestMirrorSet** (IDMS) or **ImageTagMirrorSet** (ITMS) CR. OpenShift Container Platform chose ICSP instead of the other CR types. With this release, these custom resources can co-exist, so after you import image stream tags, OpenShift Container Platform can choose the required CR. (OCPBUGS-30279)

- Previously, the **oc tag** command did not validate tag names when the command created new tags. After images were created from tags with invalid names, the **podman pull** command would fail. With this release, a validation step checks new tags for invalid names and you can now delete existing tags that have invalid names, so that this issue no longer exists. (OCPBUGS-25703)

- Previously, the Image Registry Operator had maintained its own list of IBM Power® Virtual Server regions, so any new regions were not added to the list. With this release, the Operator relies on an external library for accessing regions so that it can support new regions. (OCPBUGS-26767)

- Previously, the image registry Microsoft Azure path-fix job incorrectly required the presence of **AZURE_CLIENT_ID** and **TENANT_CLIENT_ID** parameters to function. This caused a valid configuration to throw an error message. With this release, a check is added to the Identity and Access Management (IAM) service account key to validate if these parameters are needed, so that a cluster upgrade operation no longer fails. (OCPBUGS-32328)

- Previously, the image registry did not support Amazon Web Services (AWS) region **ca-west-1**. With this release, the image registry can now be deployed in this region. (OCPBUGS-29233)

- Previously, when the **virtualHostedStyle** parameter was set to **regionEndpoint** in the Image Registry Operator configuration, the image registry ignored the virtual hosted style configuration. With this release, the issue is resolved so that a new upstream distribution configuration, force path style, is used instead of the downstream only version, virtual hosted style. (OCPBUGS-34166)

- Previously, when running an OpenShift Container Platform cluster on IBM Power® Virtual Server where service-endpoint override was enabled, the Cloud Credential Operator (CCO) Operator

would ignore the overriding service endpoints. With this release, the CCO Operator no longer ignores overriding service endpoints. (OCPBUGS-32491)

- Previously, the Image Registry Operator ignored endpoint service cluster-level overrides, making configuring your cluster in an IBM Cloud® disconnected environment difficult. This issue only existed on installer-provisioned infrastructure. With this release, the Image Registry Operator no longer ignores these cluster-level overrides. (OCPBUGS-26064)

Installer

- Previously, installation of a three-node cluster with an invalid configuration on Google Cloud Platform (GCP) failed with a panic error that did not report the reason for the failure. With this release, the installation program validates the installation configuration to successfully install a three-node cluster on GCP. (OCPBUGS-35103)

- Previously, installations with the Assisted Installer failed if the pull secret contained a colon in the password. With this release, pull secrets containing a colon in the password do not cause the Assisted Installer to fail. (OCPBUGS-34400)

- Previously, the **monitor-add-nodes** command, which is used to monitor the process of adding nodes to an Agent-based cluster, failed to run due to a permission error. With this release, the command operates in the correct directory where it has permissions. (OCPBUGS-34388)

- Previously, long cluster names were trimmed without warning the user. With this release, the installation program warns the user when trimming long cluster names. (OCPBUGS-33840)

- Previously, when installing a cluster, the Ingress capability was enabled even if it was disabled in **install-config.yaml** because it is required. With this release, the installation program fails if the Ingress capability is disabled in **install-config.yaml**. (OCPBUGS-33794)

- Previously, OpenShift Container Platform did not perform quota checking for clusters installed in the **ca-west-1** an Amazon Web Services (AWS) region. With this release, quotas are properly enforced in this region. (OCPBUGS-33649)

- Previously, the installation program could sometimes fail to detect that the OpenShift Container Platform API is unavailable. An additional error was resolved by increasing the disk size of the bootstrap node in Microsoft Azure installations. With this release, the installation program correctly detects if the API is unavailable. (OCPBUGS-33610)

- Previously, control plane nodes on Microsoft Azure clusters were using **Read-only** caches. With this release, Microsoft Azure control plane nodes use **ReadWrite** caches. (OCPBUGS-33470)

- Previously, when installing an Agent-based cluster with a proxy configured, the installation failed if the proxy configuration contained a string starting with a percent sign (**%**). With this release, the installation program correctly validates this configuration text. (OCPBUGS-33024)

- Previously, installations on GCP could fail because the installation program attempted to create a bucket twice. With this release, the installation program no longer attempts to create the bucket twice. (OCPBUGS-32133)

- Previously, a rare timing issue could prevent all control plane nodes from being added to an Agent-based cluster during installation. With this release, all control plane nodes are successfully rebooted and added to the cluster during installation. (OCPBUGS-32105)

- Previously, when using the Agent-based installation program in a disconnected environment, unnecessary certificates were added to the Certificate Authority (CA) trust bundle. With this release, the CA bundle **ConfigMap** only contains CAs explicitly specified by the user.

(OCPBUGS-32042)

- Previously, the installation program required a non-existent permission **s3:HeadBucket** when installing a cluster on Amazon Web Services (AWS). With this release, the installation program correctly requires the permission **s3:ListBucket** instead. (OCPBUGS-31813)

- Previously, if the installation program failed to gather logs from the bootstrap due to an SSH connection issue, it would also not provide virtual machine (VM) serial console logs even if they were collected. With this release, the installation program provides VM serial console logs even if the SSH connection to the bootstrap machine fails. (OCPBUGS-30774)

- Previously, when installing a cluster on VMware vSphere with static IP addresses, the cluster could create control plane machines without static IP addresses due to a conflict with other Technology Preview features. With this release, the Control Plane Machine Set Operator correctly manages the static IP assignment for control plane machines. (OCPBUGS-29114)

- Previously, when installing a cluster on GCP with user-provided DNS, the installation program still attempted to validate DNS within the GCP DNS network. With this release, the installation program does not perform this validation for user-provided DNS. (OCPBUGS-29068)

- Previously, when deleting a private cluster on IBM Cloud® that used the same domain name as a non-private IBM Cloud® cluster, some resources were not deleted. With this release, all private cluster resources are deleted when the cluster is removed. (OCPBUGS-28870)

- Previously, when installing a cluster using a proxy with a character string that used the percent sign (**%**) in the configuration string, the cluster installation failed. With this release, the installation program correctly validates proxy configuration strings containing "%". (OCPBUGS-27965)

- Previously, the installation program still allowed the use of the **OpenShiftSDN** network plugin even though it was removed. With this release, the installation program correctly prevents installing a cluster with this network plugin. (OCPBUGS-27813)

- Previously, when installing a cluster on Amazon Web Services (AWS) Wavelengths or Local Zones into a region that supports either Wavelengths or Local Zones, but not both, the installation failed. With this release, installations into regions that support either Wavelengths or Local Zones can succeed. (OCPBUGS-27737)

- Previously, when a cluster installation was attempted that used the same cluster name and base domain as an existing cluster and the installation failed due to DNS record set conflicts, removal of the second cluster would also remove the DNS record sets in the original cluster. With this release, the stored metadata contains the private zone name rather than the cluster domain, so only the correct DNS records are deleted from a removed cluster. (OCPBUGS-27156)

- Previously, platform specific passwords that were configured in the installation configuration file of an Agent-based installation could be present in the output of the **agent-gather** command. With this release, passwords are redacted from the **agent-gather** output. (OCPBUGS-26434)

- Previously, a OpenShift Container Platform cluster installed with version 4.15 or 4.16 showed a default upgrade channel of version 4.14. With this release, clusters have the correct upgrade channel after installation. (OCPBUGS-26048)

- Previously, when deleting a VMware vSphere cluster, some **TagCategory** objects failed to be deleted. With this release, all cluster-related objects are correctly deleted when the cluster is removed. (OCPBUGS-25841)

- Previously, when specifying the **baremetal** platform type but disabling the **baremetal** capability

in **install-config.yaml**, the installation failed after a long timeout without a helpful error. With this release, the installation program provides a descriptive error and does not attempt a bare metal installation if the **baremetal** capability is disabled. (OCPBUGS-25835)

- Previously, installations on VMware vSphere using the Assisted Installer could fail by preventing VMware vSphere from initializing nodes correctly. With this release, Assisted Installer installations on VMware vSphere successfully complete with all nodes initialized. (OCPBUGS-25718)

- Previously, if a VM type was selected that did not match the architecture specified in the **install-config.yaml** file, the installation would fail. With this release, a validation check ensures that the architectures match before the installation begins. (OCPBUGS-25600)

- Previously, agent-based installations could fail if an invalid number of control plane replicas was specified, such as 2. With this release, the installation program enforces the requirement of specifying either 1 or 3 control plane replicas for agent-based installations. (OCPBUGS-25462)

- Previously, when installing a cluster on VMware vSphere using the control plane machine set Technology Preview feature, the resulting control plane machine sets had duplicate failure domains in their configuration. With this release, the installation program creates the control plane machine sets with the correct failure domains. (OCPBUGS-25453)

- Previously, the required **iam:TagInstanceProfile** permission was not validated before an installer-provisioned installation, causing an installation to fail if the Identity and Access Management (IAM) permission was missing. With this release, a validation check ensures that the permission is included before the installation begins. (OCPBUGS-25440)

- Previously, the installation program did not prevent users from installing a cluster on non-bare-metal platforms with the Cloud Credential capability disabled, although it is required. With this release, the installation program produces an error and prevents installation with the Cloud Credential capability disabled, except for on the bare-metal platform. (OCPBUGS-24956)

- Previously, setting an architecture different from the one supported by the instance type resulted in the installation failing mid-process, after some resources were created. With this release, a validation check verifies that the instance type is compatible with the specified architecture. If the architecture is not compatible, the process fails before the installation begins. (OCPBUGS-24575)

- Previously, the installation program did not prevent a user from installing a cluster on a cloud provider with the Cloud Controller Manager disabled, which failed without a helpful error message. With this release, the installation program produces an error stating that the Cloud Controller Manager capability is required for installations on cloud platforms. (OCPBUGS-24415)

- Previously, the installation program could fail to remove a cluster installed on IBM Cloud® due to unexpected results from the IBM Cloud® API. With this release, clusters installed on IBM Cloud® can reliably be deleted by the installation program. (OCPBUGS-20085)

- Previously, the installation program did not enforce the requirement that FIPS-enabled clusters were installed from FIPS-enabled Red Hat Enterprise Linux (RHEL) hosts. With this release, the installation program enforces the FIPS requirement. (OCPBUGS-15845)

- Previously, proxy information that was set in the **install-config.yaml** file was not applied to the bootstrap process. With this release, proxy information is applied to bootstrap ignition data, which is then applied to the bootstrap machine. (OCPBUGS-12890)

- Previously, when the IBM Power® Virtual Server platform had no Dynamic Host Configuration

Protocol (DHCP) network name, the DHCP resource was not deleted. With this release, a check looks for any DHCP resources with an **ERROR** state and deletes them so that this issue no longer occurs. (OCPBUGS-35224)

- Previously, when creating an IBM Power® Virtual Server cluster on installer-provisioned infrastructure by using the Cluster API, the load balancer would become busy and stall. With this release, you can use the **AddIPToLoadBalancerPool** command in a **PollUntilContextCancel** loop to restart the load balancer. (OCPBUGS-35088)

- Previously, an installer-provisioned installation on a bare-metal platform with FIPS-enabled nodes caused installation failures. With this release, the issue is resolved. (OCPBUGS-34985)

- Previously, when creating an install configuration for an installer-provisioned installation on IBM Power® Virtual Server, the survey stopped if the administrator did not enter a command on the OpenShift CLI (**oc**). The survey stopped because no default region was set in the **install-config** survey. With this release, the issue is resolved. (OCPBUGS-34728)

- Previously, solid state drives (SSD) that used SATA hardware were identified as removable. The Assisted Installer for OpenShift Container Platform reported that no eligible disks were found and the installation stopped. With this release, removable disks are eligible for installation. (OCPBUGS-34652)

- Previously, Agent-based installations with dual-stack networking failed due to IPv6 connectivity check failures, even though IPv6 connectivity could be established between nodes. With this release, the issue has been resolved. (OCPBUGS-31631)

- Previously, due to a programming error, a script created compute server groups with the policy set for control planes. As a consequence, the **serverGroupPolicy** property of **install-config.yaml** files was ignored for compute groups. With this fix, the server group policy set in the **install-config.yaml** file for compute machine pools is applied at installation in the script flow. (OCPBUGS-31050)

- Previously, when configuring an Agent-based installation that uses the **openshift-baremetal-install** binary, the Agent-based installer erroneously attempted to verify the libvirt network interfaces. This might cause the following error:

  > Platform.BareMetal.externalBridge: Invalid value: "baremetal": could not find interface "baremetal"

  With this update, as the Agent-based installation method does not require libvirt, this erroneous validation has been disabled and the issue is resolved. (OCPBUGS-30941)

- Previously, using network types with dual-stack networking other than Open vSwitch-based software-defined networking (SDN) or Open Virtual Network (OVN) caused a validation error. With this release, the issue is resolved. (OCPBUGS-30232)

- Previously, a closed IPv6 port range for **nodePort** services in user-provisioned-infrastructure installations on RHOSP caused traffic through certain node ports to be blocked. With this release, appropriate security group rules have been added to the **security-group.yaml** playbook, resolving the issue. (OCPBUGS-30154)

- Previously, manifests that were generated by using the command **openshift-install agent create cluster-manifests** command were not directly applied to an OpenShift Container Platform cluster because the manifests did not include type data. With this release, type data has been added to the manifests. Administrators can now apply the manifests to initiate a Zero Touch Provisioning (ZTP) installation that uses the same settings as the Agent-based installation. (OCPBUGS-29968)

- Previously, a file required for the **aarch64** architecture was renamed by mistake while generating the **aarch64** agent ISO. With this release, the specified file does not get renamed. (OCPBUGS-28827)

- Previously, when installing a cluster on VMware vSphere, the installation would fail if an ESXi host was in maintenance mode due to the installation program failing to retrieve version information from the host. With this release, the installation program does not attempt to retrieve version information from ESXi hosts that are in maintenance mode, allowing the installation to proceed. (OCPBUGS-27848)

- Previously, the IBM Cloud® Terraform Plugin incorrectly prevented the use of non-private service endpoints during cluster installation. With this release, the IBM Cloud® Terraform Plugin supports non-private service endpoints during installation. (OCPBUGS-24473)

- Previously, installing a cluster on VMware vSphere required specifying the full path to the datastore. With this release, the installation program accepts full paths and relative paths for the datastore. (OCPBUGS-22410)

- Previously, when you installed an OpenShift Container Platform cluster by using the Agent-based installation program, a large number of manifests before installation could fill the Ignition storage causing the installation to fail. With this release, the Ignition storage has been increased to allow for a much greater amount of installation manifests. (OCPBUGS-14478)

- Previously, when the **coreos-installer iso kargs show <iso>** command was used on Agent ISO files, the output would not properly show the kernel arguments embedded in the specified ISO. With this release, the command output displays the information correctly. (OCPBUGS-14257)

- Previously, Agent-based installations created **ImageContentSource** objects instead of **ImageDigestSources** even though the former object is deprecated. With this release, the Agent-based installation program creates **ImageDigestSource** objects. (OCPBUGS-11665)

- Previously, there was an issue with the destroy functionality of the Power VS where not all resources were deleted as expected. With this release, the issue has been resolved. (OCPBUGS-29425)

Insights Operator

- The Insights Operator now collects instances outside of the **openshift-monitoring** of the following custom resources:

  - Kind: **Prometheus** Group: **monitoring.coreos.com**

  - Kind: **AlertManager** Group: **monitoring.coreos.com** (OCPBUGS-35086)

Kubernetes Controller Manager

- Previously, when deleting a **ClusterResourceQuota** resource using the foreground deletion cascading strategy, the removal failed to complete. With this release, **ClusterResourceQuota** resources are deleted properly when using the foreground cascading strategy. (OCPBUGS-22301)

Machine Config Operator

- Previously, the **MachineConfigNode** object was not created with a proper owner. As a result, the **MachineConfigNode** object could not be garbage collected, meaning that previously generated, but no longer useful, objects were not removed. With this release, the proper owner

is set upon the creation of the **MachineConfigNode** object and objects that become obsolete are available for garbage collection. (OCPBUGS-30090)

- Previously, the default value of the **nodeStatusUpdateFrequency** parameter was changed from **0s** to **10s**. This change inadvertently caused the **nodeStatusReportFrequency** to increase significantly, because the value was linked to the **nodeStatusReportFrequency** value. This resulted in high CPU usage on control plane operators and the API server. This fix manually sets the **nodeStatusReportFrequency** value to **5m**, which prevents this high CPU usage. (OCPBUGS-29713)

- Previously, a typographical error in an environment variable prevented a script from detecting if the **node.env** file was present. Because of this, the **node.env** file would be overwritten on every restart, preventing the kubelet hostname from being fixed. With this fix the typographical error is corrected. As a result, edits to the **node.env** are now persist across reboots. (OCPBUGS-27261)

- Previously, when the **kube-apiserver** server Certificate Authority (CA) certificate was rotated, the Machine Config Operator (MCO) did not properly react and update the on-disk kubelet kubeconfig. This meant that the kubelet and some pods on the node were eventually unable to communicate with the APIserver, causing the node to enter the **NotReady** state. With this release, the MCO properly reacts to the change, and updates the on-disk kubeconfig such that authenticated communication with the APIServer can continue when this rotates, and also restarts kubelet/MCDaemon pod. The certificate authority has 10-year validity, so this rotation should happen rarely and is generally non-disruptive. (OCPBUGS-25821)

- Previously, when a new node was added to or removed from a cluster, the **MachineConfigNode** (MCN) objects did not react. As a result, extraneous MCN objects existed. With this release, the Machine Config Operator removes and adds MCN objects as appropriate when nodes are added or removed. (OCPBUGS-24416)

- Previously, the **nodeip-configuration** service did not send logs to the serial console, which made it difficult to debug problems when networking is not available and there is no access to the node. With this release, the **nodeip-configuration** service logs output to the serial console for easier debugging when there is no network access to the node. (OCPBUGS-19628)

- Previously, when a **MachineConfigPool** had the **OnClusterBuild** functionality enabled and the **configmap** was updated with an invalid **imageBuilderType**, the machine-config ClusterOperator was not degraded. With this release, the Machine Config Operator (MCO) **ClusterOperator** status now validates the **OnClusterBuild** inputs each time it syncs, ensuring that if those are invalid, the **ClusterOperator** is degraded. (OCPBUGS-18955)

- Previously, when the **machine config not found** error was reported, there was not enough information to troubleshoot and correct the problem. With this release, an alert and metric have been added to the Machine Config Operator. As a result, you have more information to troubleshoot and remediate the **machine config not found** error. (OCPBUGS-17788)

- Previously, the Afterburn service used to set the hostname on nodes timed out while waiting for the metadata service to become available, causing issues when deploying with OVN-Kubernetes. Now, the Afterburn service waits longer for the metadata service to become available, resolving these timeouts. (OCPBUGS-11936)

- Previously, when a node was removed from a **MachineConfigPool**, the Machine Config Operator (MCO) did not report an error or the removal of the node. The MCO does not support managing nodes when they are not in a pool and there was no indication that node management ceased after the node was removed. With this release, if a node is removed from all pools, the MCO now logs an error. (OCPBUGS-5452)

Management Console

- Previously, the **Debug container** link was not shown for pods with a **Completed** status. With this release, the link shows as expected. (OCPBUGS-34711)
- Previously, due to an issue in PatternFly 5, text boxes in the web console were no longer resizable. With this release, text boxes are again resizable. (OCPBUGS-34393)
- Previously, French and Spanish were not available in the web console. With this release, translations for French and Spanish are now available. (OCPBUGS-33965)
- Previously, the masthead logo was not restricted to a **max-height** of 60px. As a result, logos that are larger than 60px high display at their native size and cause the masthead size too to be too large. With this release, the masthead logo is restricted to a max-height of 60px. (OCPBUGS-33523)
- Previously, there was a missing return statement in the **HealthCheck** controller causing it to panic under certain circumstances. With this release, the proper return statement was added to the **HealthCheck** controller so it no longer panics. (OCPBUGS-33505)
- Previously, an incorrect field was sent to the API server that was not noticeable. With the implementation of Admission Webhook display warning the same action would return a warning notification. A fix was provided to resolve the issue. (OCPBUGS-33222)
- Previously, the message text of a **StatusItem** might have been vertically misaligned with the icon when a timestamp was not present. With this release, the message text is correctly aligned. (OCPBUGS-33219)
- Previously, the creator field was autopopulated and not mandatory. Updates to the API made the field empty from OpenShift Container Platform 4.15 and higher. With this release, the field is marked as mandatory for correct validation. (OCPBUGS-31931)
- Previously, the YAML editor in the web console did not have the **Create** button and samples did not show on the web console. With this release, you can now see the **Create** button and the samples. (OCPBUGS-31703)
- Previously, changes to the bridge server flags on an external OpenID Connect (OIDC) feature caused the bridge server fail to start in local development. With this release, the flags usage are updated and the bridge server starts. (OCPBUGS-31695)
- Previously, when editing a VMware vSphere connection, the form could be submitted even if no values were actually changed. This resulted in unnecessary node reboots. With this release, the console now detects the form changes, and does not allow submission if no value was changed. (OCPBUGS-31613)
- Previously, the **NetworkAttachmentDefinition** was always created in the default namespace if the form method **from the console** was used. The selected name is also not honored, and creates the **NetworkAttachmentDefinition** object with the selected name and a random suffix. With this release, the **NetworkAttachmentDefinition** object is created in the current project. (OCPBUGS-31558)
- Previously, when clicking the **Configure** button by the **AlertmanagerRecieversNotConfigured** alert, the **Configuration** page did not show. With this release, the link in the **AlertmanagerRecieversNotConfigured** alert is fixed and directs you to the **Configuration** page. (OCPBUGS-30805)

- Previously, plugins using **ListPageFilters** were only using two filters: label and name. With this release, a parameter was added that enables plugins to configure multiple text-based search filters. (OCPBUGS-30077)

- Previously, there was no response when clicking on quick start items. With this release, the quick start window shows when clicking on the quick start selections. (OCPBUGS-29992)

- Previously, the OpenShift Container Platform web console terminated unexpectedly if authentication discovery failed on the first attempt. With this release, authentication initialization was updated to retry up to 5 minutes before failing. (OCPBUGS-29479)

- Previously there was an issue causing an error message on the **Image Manifest Vulnerability** page after an Image Manifest Vulnerability (IMV) was created in the CLI. With this release, the error message no longer shows. (OCPBUGS-28967)

- Previously, when using the modal dialog in a hook as part of the actions hook, an error occurred because the console framework passed null objects as part of the render cycle. With this release, **getGroupVersionKindForResource** is now null-safe and will return **undefined** if the **apiVersion** or **kind** are undefined. Additionally, the run time error for **useDeleteModal** no longer occurs, but note that it will not work with an **undefined** resource. (OCPBUGS-28856)

- Previously, the **Expand PersistentVolumeClaim** modal assumes the **pvc.spec.resources.requests.stroage** value includes a unit. With this release, the size is updated to 2GiB and you can change the value of the persistent volume claim (PVC). (OCPBUGS-27779)

- Previously, the value of image vulnerabilities reported in the OpenShift Container Platform web console were inconsistent. With this release, the image vulnerabilities on the **Overview** page were removed. (OCPBUGS-27455)

- Previously, a certificate signing request (CSR) could show for a recently approved Node. With this release, the duplication is detected and does not show CSRs for approved Nodes. (OCPBUGS-27399)

- Previously, the **Type** column was not first on the condition table on the **MachineHealthCheck detail** page. With this release, the **Type** is now listed first on the condition table. (OCPBUGS-27246)

- Previously, the console plugin proxy was not copying the status code from plugin service responses. This caused all responses from the plugin service to have a **200** status, causing unexpected behavior, especially around browser caching. With this release, the console proxy logic was updated to forward the plugin service proxy response status code. Proxied plugin requests now behave as expected. (OCPBUGS-26933)

- Previously, when cloning a persistent volume claim (PVC), the modal assumes **pvc.spec.resources.requests.storage** value includes a unit. With this release, **pvc.spec.resources.requests.storage** includes a unit suffix and the **Clone PVC** modal works as expected. (OCPBUGS-26772)

- Previously, escaped strings were not handled properly when editing VMware vSphere connection, causing broken VMware vSphere configuration. With this release, the escape strings work as expected and the VMware vSphere configuration no longer breaks. (OCPBUGS-25942)

- Previously, when configuring a VMware vSphere connection, the **resourcepool-path** key was not added to the VMware vSphere config map which might have caused issues connecting to VMware vSphere. With this release, there are no longer issues connecting to VMware vSphere.

(OCPBUGS-25927)

- Previously, there was missing text in the **Customer feedback** modal. With this release, the link text is restored and the correct Red Hat image is displayed. (OCPBUGS-25843)

- Previously, the **Update cluster** modal would not open when clicking **Select a version** from the **Cluster Settings** page. With this release, the **Update cluster** modal shows when clicking **Select a version**. (OCPBUGS-25780)

- Previously, on a mobile device, the filter part in the resource section of the **Search** page did not work on a mobile device. With this release, filtering now works as expected on a mobile device. (OCPBUGS-25530)

- Previously, the console Operator was using a client instead of listeners for fetching a cluster resource. This caused the Operator to do operations on resources with an older revision. With this release, the console Operator uses list to fetch data from cluster instead of clients. (OCPBUGS-25484)

- Previously, the console was incorrectly parsing restore size values from volume snapshots in the restore as new persistent volume claims (PVC) modal. With this release, the modal parses the restore size correctly. (OCPBUGS-24637)

- Previously, the **Alerting**, **Metrics**, and **Target** pages were not available in the console due to a change on the routing library. With this release, routes load correctly. (OCPBUGS-24515)

- Previously, there was a runtime error on the **Node details** page when a **MachineHealthCheck** without conditions existed. With this release, the **Node details** page loads as expected. (OCPBUGS-24408)

- Previously, the console backend would proxy operand list requests to the public API server endpoint, which caused CA certificate issues under some circumstances. With this release, the proxy configuration was updated to point to the internal API server endpoint which fixed this issue. (OCPBUGS-22487)

- Previously, a deployment could not be scaled up or down when a **HorizontalPodAutoscaler** was present. With this release, when a deployment with an **HorizontalPodAutoscaler** is scaled down to **zero**, an **Enable Autoscale** button is displayed so you can enable pod autoscaling. (OCPBUGS-22405)

- Previously, when editing a file, the **Info alert:Non-printable file detected. File contains non-printable characters. Preview is not available.** error was presented. With this release, a check was added to determine if a file is binary, and you are able to edit the file as expected. (OCPBUGS-18699)

- Previously, the console API conversion webhook server could not update serving certificates at runtime, and would fail if these certificates were updated by deleting the signing key. This would cause the console to not recover when CA certs were rotated. With this release, console conversion webhook server was updated to detect CA certificate changes, and handle them at runtime. The server now remains available and the console recovers as expected after CA certificates are rotated. (OCPBUGS-15827)

- Previously, production builds of the console front-end bundle have historically had source maps disabled. As a consequence, browser tools for analyzing source code could not be used on production builds. With this release, the console Webpack configuration is updated to enable source maps on production builds. Browser tools will now work as expected for both dev and production builds. (OCPBUGS-10851)

- Previously, the console redirect service had the same service Certificate Authority (CA) controller annotation as the console service. This caused the service CA controller to sometimes incorrectly sync CA certs for these services, and the console would not function correctly after removing and reinstalling. With this release, the console Operator was updated to remove this service CA annotation from the console redirect service. The console services and CA certs now function as expected when the Operator transitions from a removed to a managed state. (OCPBUGS-7656)

- Previously, removing an alternate service when editing a Route by using the **Form view** did not result in the removal of the alternate service from the Route. With this update, the alternate service is now removed. (OCPBUGS-33011)

- Previously, nodes of paused **MachineConfigPools** migh be incorrectly unpaused when performing a cluster update. With this release, nodes of paused **MachineConfigPools** correctly stay paused when performing a cluster update. (OCPBUGS-23319)

Monitoring

- Previously, the Fibre Channel collector in the **node-exporter** agent failed if certain Fibre Channel device drivers did not expose all attributes. With this release, the Fibre Channel collector disregards these optional attributes and the issue has been resolved. (OCPBUGS-20151)

- Previously, the **oc get podmetrics** and **oc get nodemetrics** commands were not working properly. With this release, the issue has been resolved. (OCPBUGS-25164)

- Previously, setting an invalid **.spec.endpoints.proxyUrl** attribute in the **ServiceMonitor** resource would result in breaking, reloading, and restarting Prometheus. This update fixes the issue by validating the **proxyUrl** attribute against invalid syntax. (OCPBUGS-30989)

Networking

- Previously, the API documentation for the **status.componentRoutes.currentHostnames** field in the Ingress API included developer notes. After you entered the **oc explain ingresses.status.componentRoutes.currentHostnames --api-version=config.openshift.io/v1** command, developer notes would show in the output along with the intended information. With this release, the developer notes are removed from the **status.componentRoutes.currentHostnames** field, so that after you enter the command, the output lists current hostnames used by the route. (OCPBUGS-31058)

- Previously, the load balancing algorithm did not differentiate between active and inactive services when determining weights, and it employed a random algorithm excessively in environments with many inactive services or environments routing backends with weight **0**. This led to increased memory usage and a higher risk of excessive memory consumption. With this release, changes optimize traffic direction towards active services only and prevent unnecessary use of a random algorithm with higher weights, reducing the potential for excessive memory consumption. (OCPBUGS-29690)

- Previously, if multiple routes were specified in the same certificate or if a route specified the default certificate as a custom certificate, and HTTP/2 was enabled on the router, an HTTP/2 client could perform connection coalescing on routes. Clients, such as a web browser, could re-use connections and potentially connect to the wrong backend server. With this release, the OpenShift Container Platform router now checks when the same certificate is specified on more than one route or when a route specifies the default certificate as a custom certificate. When either one of these conditions is detected, the router configures the HAProxy load balancer so to not allow HTTP/2 client connections to any routes that use these certificate. (OCPBUGS-29373)

- Previously, if you configured a deployment with the **routingViaHost** parameter set to **true**, traffic failed to reach the IPv6 **ExternalTrafficPolicy=Local** load balancer service. With this release, the issue is fixed. (OCPBUGS-27211)

- Previously, a pod selected by an **EgressIp** object that was hosted on a secondary network interface controller (NIC) caused connections to node IP addresses to timeout. With this release, the issue is fixed. (OCPBUGS-26979)

- Previously, a leap file package that the OpenShift Container Platform Precision Time Protocol (PTP) Operator installed could not be used by the **ts2phc** process because the package expired. With this release, the leap file package is updated to read leap events from Global Positioning System (GPS) signals and update the offset dynamically so that the expired package situation no longer occurs. (OCPBUGS-25939)

- Previously, pods assigned an IP from the pool created by the Whereabouts CNI plugin were getting stuck in the **ContainerCreating** state after a node forced a reboot. With this release, the Whereabouts CNI plugin issue associated with the IP allocation after a node force reboot is resolved. (OCPBUGS-24608)

- Previously, there was a conflict between two scripts on OpenShift Container Platform in IPv6, including single and dual-stack, deployments. One script set the hostname to a fully qualified domain name (FQDN) but the other script might set it to a short name too early. This conflict happened because the event that triggered setting the hostname to FQDN might run after the script that set it to a short name. This occurred due to asynchronous network events. With this release, new code has been added to ensure that the FQDN is set properly. This new code ensures that there is a wait for a specific network event before allowing the hostname to be set. (OCPBUGS-22324)

- Previously, if a pod selected by an **EgressIP** through a secondary interface had its label removed, another pod in the same namespace would also lose its **EgressIP** assignment, breaking its connection to the external host. With this release, the issue is fixed, so that when a pod label is removed and it stops using the **EgressIP**, other pods with the matching label continue to use the **EgressIP** without interruption. (OCPBUGS-20220)

- Previously, the global navigation satellite system (GNSS) module was capable of reporting both the GPS **fix** position and the GNSS **offset** position, which represents the offset between the GNSS module and the constellations. The previous T-GM did not use the **ubloxtool** CLI tool to probe the **ublox** module for reading **offset** and **fix** positions. Instead, it could only read the GPS **fix** information via GPSD. The reason for this was that the previous implementation of the **ubloxtool** CLI tool took 2 seconds to receive a response, and with every call it increased CPU usage by threefold. With this release, the **ubloxtool** request is now optimized, and the GPS **offset** position is now available. (OCPBUGS-17422)

- Previously, **EgressIP** pods hosted by a secondary interface would not failover because of a race condition. Users would receive an error message indicating that the **EgressIP** pod could not be assigned because it conflicted with an existing IP address. With this release, the **EgressIP** pod moves to an egress node. (OCPBUGS-20209)

- Previously, when a MAC address changed on the physical interface being used by OVN-Kubernetes, it would not be updated correctly within OVN-Kubernetes and could cause traffic disruption and Kube API outages from the node for a prolonged period of time. This was most common when a bond interface was being used, where the MAC address of the bond might swap depending on which device was the first to come up. With this release, the issues if fixed so that OVN-Kubernetes dynamically detects MAC address changes and updates it correctly. (OCPBUGS-18716)

- Previously, IPv6 was unsupported when assigning an egress IP to a network interface that was not the primary network interface. This issue has been resolved, and the egress IP can be IPv6. (OCPBUGS-24271)

- Previously, the **network-tools** image, which is a debugging tool, included the Wireshark network protocol analyzer. Wireshark had a dependency on the **gstreamer1** package, and this package has specific licensing requirements. With this release, the **gstreamer1** package is removed from the network-tools image and the image now includes the **wireshark-cli** package. (OCPBUGS-31699)

- Previously, when the default gateway of a node was set to **vlan** and multiple network manager connection had the same name, the node would fail as it could not configure the default OVN-Kubernetes bridge. With this release, the **configure-ovs.sh** shell script includes an **nmcli connection show uuid** command that retrieves the correct network manager connection if many connections with the same name exist. (OCPBUGS-24356)

- For OpenShift Container Platform clusters on Microsoft Azure, when using OVN-Kubernetes as the Container Network Interface (CNI), there was an issue where the source IP recognized by the pod was the OVN gateway router of the node when using a load balancer service with **externalTrafficPolicy: Local**. This occurred due to a Source Network Address Translation (SNAT) being applied to UDP packets.
  With this update, session affinity without a timeout is possible by setting the affinity timeout to a higher value, for example, **86400** seconds, or 24 hours. As a result, the affinity is treated as permanent unless there are network disruptions like endpoints or nodes going down. As a result, session affinity is more persistent. (OCPBUGS-24219)

Node

- Previously, OpenShift Container Platform upgrades for Ansible caused an error as the IPsec configuration was not idempotent. With this update, the issue is resolved. Now, all IPsec configurations for OpenShift Ansible playbooks are idempotent. (OCPBUGS-30802)

- Previously, the CRI-O removed all of the images installed between minor version upgrades of OpenShift Container Platform to ensure stale payload images did not take up space on the node. However, it was decided this was a performance penalty, and this functionality was removed. With this fix, the kubelet will still garbage collect stale images after disk usage hits a certain level. As a result, OpenShift Container Platform no longer removes all images after an upgrade between minor versions. (OCPBUGS-24743)

Node Tuning Operator (NTO)

- Previously, the distributed unit profile on single-node OpenShift Container Platform was degraded because the **net.core.busy_read**, **net.core.busy_poll**, and **kernel.numa_balancing sysctls** did not exist in the real-time kernel. With this release, the Tuned profile is no longer degraded and the issue has been resolved. (OCPBUGS-23167)

- Previously, the Tuned profile reported a **Degraded** condition after **PerformanceProfile** was applied. The profile had attempted to set a **sysctl** value for the default Receive Packet Steering (RPS) mask, but the mask was already configured with the same value using an **/etc/sysctl.d** file. With this update, the **sysctl** value is no longer set with the Tuned profile and the issue has been resolved. (OCPBUGS-24638)

- Previously, the Performance Profile Creator (PPC) incorrectly populated the **metadata.ownerReferences.uid** field for Day 0 performance profile manifests. As a result, it was impossible to apply a performance profile at Day 0 without manual intervention. With this

release, the PPC does not generate the **metadata.ownerReferences.uid** field for Day 0 manifests. As a result, you can apply a performance profile manifest at Day 0 as expected. (OCPBUGS-29751)

- Previously, the TuneD daemon could unnecessarily reload an additional time after a Tuned custom resource (CR) update. With this release, the Tuned object has been removed and the TuneD (daemon) profiles are carried directly in the Tuned Profile Kubernetes objects. As a result, the issue has been resolved. (OCPBUGS-32469)

OpenShift CLI (oc)

- Previously, when mirroring operator images with incompatible semantic versioning, oc-mirror plugin v2 (Technology Preview) would fail and exit. This fix ensures that a warning appears in the console, indicating the skipped image and allowing the mirroring process to continue without interruption. (OCPBUGS-34587)

- Previously, oc-mirror plugin v2 (Technology Preview) failed to mirror certain Operator catalogs that included image references with both **tag** and **digest** formats. This issue prevented the creation of cluster resources, such as **ImageDigestMirrorSource** (IDMS) and **ImageTagMirrorSource** (ITMS). With this update, oc-mirror resolves the issue by skipping images that have both **tag** and **digest** references, while displaying an appropriate warning message in the console output. (OCPBUGS-33196)

- Previously, with oc-mirror plugin v2 (Technology Preview), mirroring errors were only displayed in the console output, making it difficult for users to analyze and troubleshoot other issues. For example, an unstable network might require a rerun, while a manifest unknown error might need further analysis to skip an image or Operator. With this update, a file is generated that contains all errors in the workspace **working-dir/logs** folder. And all the errors that occur during the mirroring process are now logged in **mirroring_errors_YYYYMMdd.txt**. (OCPBUGS-33098)

- Previously, the Cloud Credential Operator utility (**ccoctl**) could not run on a RHEL 9 host with FIPS enabled. With this release, a user can run a version of the **ccoctl** utility that is compatible with the RHEL version of their host, including RHEL 9. (OCPBUGS-32080)

- Previously, when mirroring operator catalogs, **oc-mirror** would rebuild the catalogs and regenerate their internal cache based on **imagesetconfig** catalog filtering specifications. This process required the **opm** binary from within the catalogs. Starting with version 4.15, operator catalogs include the **opm** RHEL 9 binary, which caused the mirroring process to fail when executed on RHEL 8 systems. With this release, **oc-mirror** no longer rebuilds catalogs by default; instead, it simply mirrors them to their destination registries.
  To retain the catalog rebuilding functionality, use **--rebuild-catalog**. However, note that no changes were made to the current implementation, so using this flag might result in the cache not being generated or the catalog not being deployed to the cluster. If you use this command, you can export **OPM_BINARY** to specify a custom **opm** binary that corresponds to the catalog versions and platform found in OpenShift Container Platform. Mirroring of catalog images is now done without signature verification. Use **--enable-operator-secure-policy** to enable signature verification during mirroring. (OCPBUGS-31536)

- Previously, some credentials requests were not extracted properly when running the **oc adm release extract --credentials-requests** command with an **install-config.yaml** file that included the **CloudCredential** cluster capability. With this release, the **CloudCredential** capability is correctly included in the OpenShift CLI (**oc**) so that this command extracts credentials requests properly. (OCPBUGS-24834)

- Previously, users encountered sequence errors when using the **tar.gz** artifact with the oc-mirror plugin. To resolve this, the oc-mirror plugin now ignores these errors when executed with the **--skip-pruning** flag. This update ensures that the sequence error, which no longer affects the

order of **tar.gz** usage in mirroring, is effectively handled. (OCPBUGS-23496)

- Previously, when using the oc-mirror plugin to mirror local Open Container Initiative Operator catalogs located in hidden folders, oc-mirror previously failed with an error: ".hidden_folder/data/publish/latest/catalog-oci/manifest-list/kubebuilder/kube-rbac-proxy@sha256:db06cc4c084dd0253134f156dddaaf53ef1c3fb3cc809e5d81711baa4029ea4c is not a valid image reference: invalid reference format ". With this release, oc-mirror now calculates references to images within local Open Container Initiative catalogs differently, ensuring that the paths to hidden catalogs no longer disrupt the mirroring process. (OCPBUGS-23327)

- Previously, oc-mirror would not stop and return a valid error code when mirroring failed. With this release, oc-mirror now exits with the correct error code when encountering "operator not found", unless the **--continue-on-error** flag is used. (OCPBUGS-23003)

- Previously, when mirroring operators, oc-mirror would ignore the **maxVersion** constraint in **imageSetConfig** if both **minVersion** and **maxVersion** were specified. This resulted in mirroring all bundles up to the channel head. With this release, oc-mirror now considers the **maxVersion** constraint as specified in **imageSetConfig**. (OCPBUGS-21865)

- Previously, oc-mirror failed to mirror releases using **eus-*** channels, as it did not recognize that **eus-*** channels are designated for even-numbered releases only. With this release, oc-mirror plugin now properly acknowledges that **eus-*** channels are intended for even-numbered releases, enabling users to successfully mirror releases using these channels. (OCPBUGS-19429)

- Previously, the addition of the **defaultChannel** field in the **mirror.operators.catalog.packages** file enabled users to specify their preferred channel, overriding the **defaultChannel** set in the operator. With this release, oc-mirror plugin now enforces an initial check if the **defaultChannel** field is set, users must also define it in the channels section of the **ImageSetConfig**. This update ensures that the specified **defaultChannel** is properly configured and applied during operator mirroring. (OCPBUGS-385)

- Previously, when running a cluster with FIPS enabled, you might have received the following error when running the OpenShift CLI (**oc**) on a RHEL 9 system: **FIPS mode is enabled, but the required OpenSSL backend is unavailable**. With this release, the default version of OpenShift CLI (**oc**) is compiled with Red Hat Enterprise Linux (RHEL) 9 and works properly when running a cluster with FIPS enabled on RHEL 9. Additionally, a version of **oc** compiled with RHEL 8 is also provided, which must be used if you are running a cluster with FIPS enabled on RHEL 8. (OCPBUGS-23386, OCPBUGS-28540)

- Previously, role bindings related to the **ImageRegistry** and **Build** capabilities were created in every namespace, even if the capability was disabled. With this release, the role bindings are only created if the respective cluster capability is enabled on the cluster. (OCPBUGS-34384)

- Previously, during the disk-to-mirror process for fully disconnected environments, oc-mirror plugin v1 would fail to mirror the catalog image when access to Red Hat registries was blocked. Additionally, if the **ImageSetConfiguration** used a **targetCatalog** for the mirrored catalog, mirroring would fail due to incorrect catalog image references regardless of the workflow. This issue has been resolved by updating the catalog image source for mirroring to the mirror registry. (OCPBUGS-34646)

Operator Lifecycle Manager (OLM)

- Previously, Operator catalogs were not being refreshed properly, due to the **imagePullPolicy** field being set to **IfNotPresent** for the index image. This bug fix updates OLM to use the appropriate image pull policy for catalogs, and as a result catalogs are refreshed properly.

(OCPBUGS-30132)

- Previously, cluster upgrades could be blocked due to OLM getting stuck in a **CrashLoopBackOff** state. This was due to an issue with resources having multiple owner references. This bug fix updates OLM to avoid duplicate owner references and only validate the related resources that it owns. As a result, cluster upgrades can proceed as expected. (OCPBUGS-28744)

- Previously, default OLM catalog pods backed by a **CatalogSource** object would not survive an outage of the node that they were being run on. The pods remained in termination state, despite the tolerations that should move them. This caused Operators to no longer be able to be installed or updated from related catalogs. This bug fix updates OLM so catalog pods that get stuck in this state are deleted. As a result, catalog pods now correctly recover from planned or unplanned node maintenance. (OCPBUGS-32183)

- Previously, installing an Operator could sometimes fail if the same Operator had been previously installed and uninstalled. This was due to a caching issue. This bug fix updates OLM to correctly install the Operator in this scenario, and as a result this issue no longer occurs. (OCPBUGS-31073)

- Previously, the **catalogd** component could crash loop after an etcd restore. This was due to the garbage collection process causing a looping failure state when the API server was unreachable. This bug fix updates **catalogd** to add a retry loop, and as a result **catalogd** no longer crashes in this scenario. (OCPBUGS-29453)

- Previously, the default catalog source pod would not receive updates, requiring users to manually re-create it to get updates. This was caused by image IDs for catalog pods not getting detected correctly. This bug fix updates OLM to correctly detect catalog pod image IDs, and as a result, default catalog sources are updated as expected. (OCPBUGS-31438)

- Previously, users could experience Operator installation errors due to OLM not being able to find existing **ClusterRoleBinding** or **Service** resources and creating them a second time. This bug fix updates OLM to pre-create these objects, and as a result these installation errors no longer occur. (OCPBUGS-24009)

Red Hat Enterprise Linux CoreOS (RHCOS)

- Previously, the OVS network configured before the **kdump** service generated its special **initramfs**. When the **kdump** service started, it picked up the network-manager configuration files and copied them into the **kdump initramfs**. When the node rebooted into the **kdump initramfs**, the kernel crash dump upload over the network failed because OVN did not run into the **initramfs** and the virtual interface was not configured. With this release, the ordering has been updated so that the **kdump** starts and builds the **kdump initramfs** before the OVS networking configuration is set up and the issue has been resolved. (OCPBUGS-30239)

Scalability and performance

- Previously, the Machine Config Operator (MCO) on single-node OpenShift Container Platform was rendered after the Performance Profile rendered, so the control plane and worker machine config pools were not created at the right time. With this release, the Performance Profile renders correctly and the issue is resolved. (OCPBUGS-22095)

- Previously, the TuneD and **irqbalanced** daemons modified the Interrupt Request (IRQ) CPU affinity configuration, which created conflicts in the IRQ CPU affinity configuration and caused unexpected behavior after a single-node OpenShift node restart. With this release, only the **irqbalanced** daemon determines IRQ CPU affinity configuration. (OCPBUGS-26400)

- Previously, during OpenShift Container Platform updates in performance-tuned clusters, resuming a **MachineConfigPool** resource resulted in additional restarts for nodes in the pool. With this release, the controller reconciles against the latest planned machine configurations before the pool resumes, which prevents additional node reboots. (OCPBUGS-31271)

- Previously, ARM installations used 4k pages in the kernel. With this release, support was added for installing 64k pages in the kernel at installation time only, providing a performance boost on the NVIDIA CPU. Driver Tool Kit (DTK) was also updated to compile kernel modules for the 64k page size ARM kernel. (OCPBUGS-29223)

Storage

- Previously, some **LVMVolumeGroupNodeStatus** operands were not deleted on the cluster during the deletion of the **LVMCluster** custom resource (CR). With this release, deleting the **LVMCluster** CR triggers the deletion of all the **LVMVolumeGroupNodeStatus** operands. (OCPBUGS-32954)

- Previously, LVM Storage uninstallation was stuck waiting for the deletion of the **LVMVolumeGroupNodeStatus** operands. This fix corrects the behavior by ensuring all operands are deleted, allowing LVM Storage to be uninstalled without delay. (OCPBUGS-32753)

- Previously, LVM Storage did not support minimum storage size for persistent volume claims (PVCs). This can lead to mount failures while provisioning PVCs. With this release, LVM Storage supports minimum storage size for PVCs. The following are the minimum storage sizes that you can request for each file system type:

  - **block**: 8 MiB

  - **xfs**: 300 MiB

  - **ext4**: 32 MiB
    If the value of the **requests.storage** field in the **PersistentVolumeClaim** object is less than the minimum storage size, the requested storage size is rounded to the minimum storage size. If the value of the **limits.storage field** is less than the minimum storage size, PVC creation fails with an error. (OCPBUGS-30266)

- Previously, LVM Storage created persistent volume claims (PVCs) with storage size requests that were not multiples of the disk sector size. This can cause issues during LVM2 volume creation. This fix corrects the behavior by rounding the storage size requested by PVCs to the nearest multiple of 512. (OCPBUGS-30032)

- Previously, the **LVMCluster** custom resource (CR) contained an excluded status element for a device that is set up correctly. This fix filters the correctly set device from being considered for an excluded status element, so it only appears in the ready devices. (OCPBUGS-29188)

- Previously, CPU limits for the Amazon Web Services (AWS) Elastic File Store (EFS) Container Storage Interface (CSI) driver container could cause performance degradation of volumes managed by the AWS EFS CSI Driver Operator. With this release, the CPU limits from the AWS EFS CSI driver container are removed to help prevent potential performance degradation. (OCPBUGS-28551)

- Previously, the Microsoft Azure Disk CSI driver was not properly counting allocatable volumes on certain instance types and exceeded the maximum. As a result, the pod could not start. With this release, the count table for the Microsoft Azure Disk CSI driver has been updated to include new instance types. The pod now runs and data can be read and written to the properly configured volumes. (OCPBUGS-18701)

- Previously, the secrets store Container Storage Interface driver on Hosted Control Planes failed to mount secrets because of a bug in the CLI. With this release, the driver is able to mount volumes and the issue has been resolved. (OCPBUGS-34759)
- Previously, static Persistent Volumes (PVs) in Microsoft Azure Workload Identity clusters could not be configured due to a bug in the driver, causing PV mounts to fail. With this release, the driver works and static PVs mount correctly. (OCPBUGS-32785)

1.7. TECHNOLOGY PREVIEW FEATURES STATUS

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:

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

Networking Technology Preview features

Table 1.18. Networking Technology Preview tracker

Feature	4.14	4.15	4.16
Ingress Node Firewall Operator	General Availability	General Availability	General Availability
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	Technology Preview	General Availability	General Availability
OVN-Kubernetes network plugin as secondary network	General Availability	General Availability	General Availability
Updating the interface-specific safe sysctls list	Technology Preview	Technology Preview	Technology Preview
Egress service custom resource	Technology Preview	Technology Preview	Technology Preview

Feature	4.14	4.15	4.16
VRF specification in **BGPPeer** custom resource	Technology Preview	Technology Preview	Technology Preview
VRF specification in **NodeNetworkConfigurationPolicy** custom resource	Technology Preview	Technology Preview	Technology Preview
Admin Network Policy (**AdminNetworkPolicy**)	Technology Preview	Technology Preview	General Availability
IPsec external traffic (north-south)	Technology Preview	General Availability	General Availability
Integration of MetalLB and FRR-K8s	Not Available	Not Available	Technology Preview
Dual-NIC hardware as PTP boundary clock	General Availability	General Availability	General Availability
Dual-NIC Intel E810 PTP boundary clock with highly available system clock	Not Available	Not Available	General Availability
Intel E810 Westport Channel NIC as PTP grandmaster clock	Technology Preview	Technology Preview	General Availability
Dual-NIC Intel E810 Westport Channel as PTP grandmaster clock	Not Available	Technology Preview	General Availability
Configure the **br-ex** bridge needed by OVN-Kuberenetes using NMState	Not Available	Not Available	Technology Preview
Creating a route with externally managed certificate	Not Available	Not Available	Technology Preview
Live migration to OVN-Kubernetes from OpenShift SDN	Not Available	Not Available	General Availability
Overlapping IP configuration for multi-tenant networks with Whereabouts	Not Available	Not Available	General Availability
Improved integration between CoreDNS and egress firewall	Not Available	Not Available	Technology Preview

Storage Technology Preview features

Table 1.19. Storage Technology Preview tracker

Feature	4.14	4.15	4.16
Automatic device discovery and provisioning with Local Storage Operator	Technology Preview	Technology Preview	Technology Preview
Google Filestore CSI Driver Operator	General Availability	General Availability	General Availability
IBM Power® Virtual Server Block CSI Driver Operator	Technology Preview	General Availability	General Availability
Read Write Once Pod access mode	Technology Preview	Technology Preview	General Availability
Build CSI Volumes in OpenShift Builds	General Availability	General Availability	General Availability
Shared Resources CSI Driver in OpenShift Builds	Technology Preview	Technology Preview	Technology Preview
Secrets Store CSI Driver Operator	Technology Preview	Technology Preview	Technology Preview
CIFS/SMB CSI Driver Operator	Not Available	Not Available	Technology Preview

Installation Technology Preview features

Table 1.20. Installation Technology Preview tracker

Feature	4.14	4.15	4.16
Installing OpenShift Container Platform on Oracle® Cloud Infrastructure (OCI) with VMs	Developer Preview	Technology Preview	Technology Preview
Installing OpenShift Container Platform on Oracle® Cloud Infrastructure (OCI) on bare metal	Developer Preview	Developer Preview	Developer Preview
Adding kernel modules to nodes with kvc	Technology Preview	Technology Preview	Technology Preview
Enabling NIC partitioning for SR-IOV devices	Technology Preview	Technology Preview	Technology Preview
User-defined labels and tags for Google Cloud Platform (GCP)	Technology Preview	Technology Preview	Technology Preview

Feature	4.14	4.15	4.16
Installing a cluster on Alibaba Cloud by using installer-provisioned infrastructure	Technology Preview	Technology Preview	Not Available
Installing a cluster on Alibaba Cloud by using Assisted Installer	Not Available	Not Available	Technology Preview
Mount shared entitlements in BuildConfigs in RHEL	Technology Preview	Technology Preview	Technology Preview
OpenShift Container Platform on Oracle® Cloud Infrastructure (OCI)	Developer Preview	Technology Preview	Technology Preview
Selectable Cluster Inventory	Technology Preview	Technology Preview	Technology Preview
Static IP addresses with VMware vSphere (IPI only)	Technology Preview	Technology Preview	General Availability
Support for iSCSI devices in RHCOS	Not Available	Technology Preview	General Availability
Installing a cluster on GCP using the Cluster API implementation	Not Available	Not Available	Technology Preview
Support for Intel® VROC-enabled RAID devices in RHCOS	Technology Preview	Technology Preview	General Availability

Node Technology Preview features

Table 1.21. Nodes Technology Preview tracker

Feature	4.14	4.15	4.16
MaxUnavailableStatefulSet featureset	Technology Preview	Technology Preview	Technology Preview

Multi-Architecture Technology Preview features

Table 1.22. Multi-Architecture Technology Preview tracker

Feature	4.14	4.15	4.16
IBM Power® Virtual Server using installer-provisioned infrastructure	Technology Preview	General Availability	General Availability

Feature	4.14	4.15	4.16
kdump on **arm64** architecture	Technology Preview	Technology Preview	Technology Preview
kdump on **s390x** architecture	Technology Preview	Technology Preview	Technology Preview
kdump on **ppc64le** architecture	Technology Preview	Technology Preview	Technology Preview
Multiarch Tuning Operator	Not available	Not available	Technology Preview

Specialized hardware and driver enablement Technology Preview features

Table 1.23. Specialized hardware and driver enablement Technology Preview tracker

Feature	4.14	4.15	4.16
Driver Toolkit	General Availability	General Availability	General Availability
Kernel Module Management Operator	General Availability	General Availability	General Availability
Kernel Module Management Operator - Hub and spoke cluster support	General Availability	General Availability	General Availability
Node Feature Discovery	General Availability	General Availability	General Availability

Scalability and performance Technology Preview features

Table 1.24. Scalability and performance Technology Preview tracker

Feature	4.14	4.15	4.16
factory-precaching-cli tool	Technology Preview	Technology Preview	Technology Preview
Hyperthreading-aware CPU manager policy	Technology Preview	Technology Preview	Technology Preview
HTTP transport replaces AMQP for PTP and bare-metal events	Technology Preview	Technology Preview	General Availability

Feature	4.14	4.15	4.16
Mount namespace encapsulation	Technology Preview	Technology Preview	Technology Preview
Node Observability Operator	Technology Preview	Technology Preview	Technology Preview
Tuning etcd latency tolerances	Technology Preview	Technology Preview	General Availability
Increasing the etcd database size	Not Available	Not Available	Technology Preview
Using RHACM **PolicyGenerator** resources to manage GitOps ZTP cluster policies	Not Available	Not Available	Technology Preview

Operator lifecycle and development Technology Preview features

Table 1.25. Operator lifecycle and development Technology Preview tracker

Feature	4.14	4.15	4.16
Operator Lifecycle Manager (OLM) v1	Technology Preview	Technology Preview	Technology Preview
RukPak	Technology Preview	Technology Preview	Technology Preview
Platform Operators	Technology Preview	Technology Preview	Removed
Scaffolding tools for Hybrid Helm-based Operator projects	Technology Preview	Technology Preview	Deprecated
Scaffolding tools for Java-based Operator projects	Technology Preview	Technology Preview	Deprecated

OpenShift CLI (oc) Technology Preview features

Table 1.26. OpenShift CLI (oc) Technology Preview tracker

Feature	4.14	4.15	4.16
oc-mirror plugin v2	Not Available	Not Available	Technology Preview

Feature	4.14	4.15	4.16
Enclave support	Not Available	Not Available	Technology Preview
Delete functionality	Not Available	Not Available	Technology Preview

Monitoring Technology Preview features

Table 1.27. Monitoring Technology Preview tracker

Feature	4.14	4.15	4.16
Metrics Collection Profiles	Technology Preview	Technology Preview	Technology Preview
Metrics Server	Not Available	Technology Preview	General Availability

Red Hat OpenStack Platform (RHOSP) Technology Preview features

Table 1.28. RHOSP Technology Preview tracker

Feature	4.14	4.15	4.16
Dual-stack networking with installer-provisioned infrastructure	Technology Preview	General Availability	General Availability
Dual-stack networking with user-provisioned infrastructure	Not Available	General Availability	General Availability
RHOSP integration into the Cluster CAPI Operator	Not Available	Technology Preview	Technology Preview
Control Plane with **rootVolumes** and **etcd** on local disk	Not Available	Technology Preview	Technology Preview

Hosted control planes Technology Preview features

Table 1.29. Hosted control planes Technology Preview tracker

Feature	4.14	4.15	4.16
Hosted control planes for OpenShift Container Platform on Amazon Web Services (AWS)	Technology Preview	Technology Preview	General Availability

Feature	4.14	4.15	4.16
Hosted control planes for OpenShift Container Platform on bare metal	General Availability	General Availability	General Availability
Hosted control planes for OpenShift Container Platform on OpenShift Virtualization	General Availability	General Availability	General Availability
Hosted control planes for OpenShift Container Platform using non-bare metal agent machines	Not Available	Technology Preview	Technology Preview
Hosted control planes for an ARM64 OpenShift Container Platform cluster on Amazon Web Services	Technology Preview	Technology Preview	Technology Preview
Hosted control planes for OpenShift Container Platform on IBM Power	Technology Preview	Technology Preview	Technology Preview
Hosted control planes for OpenShift Container Platform on IBM Z	Technology Preview	Technology Preview	Technology Preview

Machine management Technology Preview features

Table 1.30. Machine management Technology Preview tracker

Feature	4.14	4.15	4.16
Managing machines with the Cluster API for Amazon Web Services	Technology Preview	Technology Preview	Technology Preview
Managing machines with the Cluster API for Google Cloud Platform	Technology Preview	Technology Preview	Technology Preview
Managing machines with the Cluster API for VMware vSphere	Not Available	Not Available	Technology Preview
Defining a vSphere failure domain for a control plane machine set	Not Available	Technology Preview	General Availability
Cloud controller manager for Alibaba Cloud	Technology Preview	Technology Preview	Technology Preview
Cloud controller manager for Google Cloud Platform	Technology Preview	General Availability	General Availability
Cloud controller manager for IBM Power® Virtual Server	Technology Preview	Technology Preview	Technology Preview

Authentication and authorization Technology Preview features

Table 1.31. Authentication and authorization Technology Preview tracker

Table 1.31. Authentication and authorization Technology Preview tracker

Feature	4.14	4.15	4.16
Pod security admission restricted enforcement	Technology Preview	Technology Preview	Technology Preview

Machine Config Operator Technology Preview features

Table 1.32. Machine Config Operator Technology Preview tracker

Feature	4.14	4.15	4.16
Improved MCO state reporting	Not Available	Technology Preview	Technology Preview
On-cluster RHCOS image layering	Not Available	Not Available	Technology Preview
Node disruption policies	Not Available	Not Available	Technology Preview
Updating boot images	Not Available	Not Available	Technology Preview

Edge computing Technology Preview features

Table 1.33. Edge computing Technology Preview tracker

Feature	4.14	4.15	4.16
Accelerated provisioning of GitOps ZTP	Not Available	Not Available	Technology Preview

1.8. KNOWN ISSUES

- 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)
- Run Once Duration Override Operator (RODOO) cannot be installed on clusters managed by the Hypershift Operator. (OCPBUGS-17533)
- OpenShift Container Platform 4.16 installation on AWS in a secret or top secret region fails due to an issue with Network Load Balancers (NLBs) and security groups in these regions. (OCPBUGS-33311)
- When you run Cloud-native Network Functions (CNF) latency tests on an OpenShift Container Platform cluster, the **oslat** test can sometimes return results greater than 20 microseconds. This results in an **oslat** test failure. (RHEL-9279)

- When installing a cluster on Amazon Web Services (AWS) using Local Zones, edge nodes fail to deploy if deployed in the **us-east-1-iah-2a** region. (OCPBUGS-35538)

- Installing OpenShift Container Platform 4.16 with the Infrastructure Operator, Central Infrastructure Management, or ZTP methods using ACM versions 2.10.3 or earlier is not possible. This is because of a change in the dynamically linked installer binary,**openshift-baremetal-install**, which in OpenShift Container Platform 4.16 requires a Red Hat Enterprise Linux (RHEL) 9 host to run successfully. It is planned to use the statically linked binary in future versions of ACM to avoid this issue. (ACM-12405)

- When installing a cluster on AWS, the installation can time out if the load balancer DNS time-to-live (TTL) value is very high. (OCPBUGS-35898)

- For a bonding network interface that holds a **br-ex** bridge device, do not set the **mode=6 balance-alb** bond mode in a node network configuration. This bond mode is not supported on OpenShift Container Platform and it can cause the Open vSwitch (OVS) bridge device to disconnect from your networking environment. (OCPBUGS-34430)

- Do not update firmware for the **BareMetalHosts** (BMH) resource by editing the **HostFirmwareComponents** resource. Otherwise, the BMH remains in the **Preparing** state and executes the firmware update repeatedly. There is no workaround. (OCPBUGS-35559)

- Deploying an installer-provisioned cluster on bare metal fails when a proxy is used. A service in the bootstrap virtual machine cannot access IP address **0.0.0.0** through the proxy because of a regression bug. As a workaround, add **0.0.0.0** to the **noProxy** list. For more information, see Setting proxy settings. (OCPBUGS-35818)

- When installing a cluster on Amazon Web Services (AWS) in a VPC that contains multiple CIDR blocks, if the machine network is configured to use a non-default CIDR block in the **install-config.yaml** file, the installation fails. (OCPBUGS-35054)

- When a OpenShift Container Platform 4.16 cluster is installed or configured as a postinstallation activity on a single VIOS host with virtual SCSI storage on IBM Power® with multipath configured, the CoreOS nodes with multipath enabled fail to boot. This behavior is expected as only one path is available to the node. (OCPBUGS-32290)

- When using CPU load balancing on cgroupv2, a pod can fail to start if another pod that has access to exclusive CPUs already exists. This can happen when a pod is deleted and another one is quickly created to replace it. As a workaround, ensure that the old pod is fully terminated before attempting to create the new one. (OCPBUGS-34812)

- Enabling LUKS encryption on a system using 512 emulation disks causes provisioning to fail and the system launches the emergency shell in the initramfs. This happens because of an alignment bug in **sfdisk** when growing a partition. As a workaround, you can use Ignition to perform the resizing instead. (OCPBUGS-35410)

- OpenShift Container Platform version 4.16 disconnected installation fails on IBM Power® Virtual Server. (OCPBUGS-36250)

- In hosted control planes for OpenShift Container Platform, if you disable the Ingress capability, the Console Operator returns the following error message:

  ```
  RouteHealthAvailable: failed to GET route.
  ```

  To avoid this error, do not disable the **Ingress** capability in an OpenShift Container Platform managed cluster. (OCPBUGS-33788)

- The current PTP grandmaster clock (T-GM) implementation has a single National Marine Electronics Association (NMEA) sentence generator sourced from the GNSS without a backup NMEA sentence generator. If NMEA sentences are lost before reaching the e810 NIC, the T-GM cannot synchronize the devices in the network synchronization chain and the PTP Operator reports an error. A proposed fix is to report a **FREERUN** event when the NMEA string is lost. Until this limitation is addressed, T-GM does not support PTP clock holdover state. (OCPBUGS-19838)

- When a worker node's Topology Manager policy is changed, the NUMA-aware secondary pod scheduler does not respect this change, which can result in incorrect scheduling decisions and unexpected topology affinity errors. As a workaround, restart the NUMA-aware scheduler by deleting the NUMA-aware scheduler pod. (OCPBUGS-34583)

- Due to an issue with Kubernetes, the CPU Manager is unable to return CPU resources from the last pod admitted to a node to the pool of available CPU resources. These resources are allocatable if a subsequent pod is admitted to the node. However, this pod then becomes the last pod, and again, the CPU manager cannot return this pod's resources to the available pool. This issue affects CPU load balancing features, which depend on the CPU Manager releasing CPUs to the available pool. Consequently, non-guaranteed pods might run with a reduced number of CPUs. As a workaround, schedule a pod with a **best-effort** CPU Manager policy on the affected node. This pod will be the last admitted pod and this ensures the resources will be correctly released to the available pool. (OCPBUGS-17792)

- After applying a **SriovNetworkNodePolicy** resource, the CA certificate might be replaced during SR-IOV Network Operator webhook reconciliation. As a consequence, you might see **unknown authority** errors when applying SR-IOV Network node policies. As a workaround, try to re-apply the failed policies. (OCPBUGS-32139)

- If you delete a **SriovNetworkNodePolicy** resource for a virtual function with a **vfio-pci** driver type, the SR-IOV Network Operator is unable to reconcile the policy. As a consequence the **sriov-device-plugin** pod enters a continuous restart loop. As a workaround, delete all remaining policies affecting the physical function, then re-create them. (OCPBUGS-34934)

- If the controller pod terminates while cloning is in progress, the Microsoft Azure File clone persistent volume claims (PVCs) remain in the Pending state. To resolve this issue, delete any affected clone PVCs, and then recreate the PVCs. (OCPBUGS-35977)

- There is no log pruning available for azcopy (underlying tool running copy jobs) in Microsoft Azure, so this might eventually lead to filling up a root device of the controller pod, and you have to manually clean this up. (OCPBUGS-35980)

- The limited live migration method stops when the **mtu** parameter of a **ConfigMap** object in the **openshift-network-operator** namespace is missing.
  In most cases, the **mtu** field of the **ConfigMap** object is created by the **mtu-prober** job during installation. However, if the cluster was upgraded from an early release, for example, OpenShift Container Platform 4.4.4, the **ConfigMap** object might be absent.

  As a temporary workaround, you can manually create the **ConfigMap** object before starting the limited live migration process. For example:

  ```
  apiVersion: v1
  kind: ConfigMap
  metadata:
    name: mtu
  ```

```
  namespace: openshift-network-operator
data:
  mtu: "1500" 1
```

1 The **mtu** value must be aligned with the MTU of the node interface.

(OCPBUGS-35316)

- In hosted clusters, self-signed certificates from the API cannot be replaced. (OCPSTRAT-1516)
- Low-latency applications that rely on high-resolution timers to wake up their threads might experience higher wake up latencies than expected. Although the expected wake up latency is under 20µs, latencies exceeding this time can occasionally be seen when running the **cyclictest** tool for long durations. Testing has shown that wake up latencies are under 20µs for over 99.99999% of the samples. (OCPBUGS-34022)

1.9. ASYNCHRONOUS ERRATA UPDATES

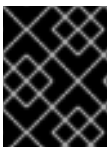
Security, bug fix, and enhancement updates for OpenShift Container Platform 4.16 are released as asynchronous errata through the Red Hat Network. All OpenShift Container Platform 4.16 errata is available on the Red Hat Customer Portal . See the OpenShift Container Platform Life Cycle for more information 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 4.16. Versioned asynchronous releases, for example with the form OpenShift Container Platform 4.16.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. RHBA-2024:5757 - OpenShift Container Platform 4.16.9 bug fix update

Issued: 29 August 2024

OpenShift Container Platform release 4.16.9 is now available. The list of bug fixes that are included in the update is documented in the RHBA-2024:5757 advisory. The RPM packages that are included in the update are provided by the RHBA-2024:5760 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 4.16.9 --pullspecs
```

1.9.1.1. Enhancements

- The Insights Operator (IO) can now collect data from the **haproxy_exporter_server_threshold** metric. (OCPBUGS-38230)

1.9.1.2. Updating

To update an existing OpenShift Container Platform 4.16 cluster to this latest release, see Updating a cluster using the CLI.

1.9.2. RHSA-2024:5422 - OpenShift Container Platform 4.16.8 bug fix and security update

Issued: 20 August 2024

OpenShift Container Platform release 4.16.8, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2024:5422 advisory. The RPM packages that are included in the update are provided by the RHBA-2024:5425 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 4.16.8 --pullspecs
```

1.9.2.1. Bug fixes

- Previously, when you clicked the Red Hat OpenShift Lightspeed link on the **Settings** page of your OpenShift Container Platform cluster, the OpenShift Lightspeed modal in Operator Hub did not open. With this update, the OpenShift Lightspeed modal opens as expected. (OCPBUGS-38093)

- Previously, when you mirrored Operator catalogs with the **--rebuild-catalogs** argument, catalog cache was recreated on the local machine. This required extraction and use of the **opm** binary from the catalog image, which caused failure of either the mirroring operation or the catalog source. These failures would happen because the supported operating system and the platform of the **opm** binary caused a mismatch with the operating system and platform of **oc-mirror**. With this release, the value of **true** is applied to the **--rebuild-catalogs** argument by default; any catalog rebuilds do not re-create internal cache. Additionally, this release updates the image from **opm serve /configs --cache-dir=/tmp/cache** to **opm serve /configs** so that the creation of cache happens at pod startup. Cache at startup might increase pod startup time. (OCPBUGS-38035)

- Previously, the **PrometheusRemoteWriteBehind** alert was only triggered after Prometheus sent data to the **remote-write** endpoint on at least one occasion. With this release, the alert now also triggers if a connection could never be established with the endpoint, such as when an error exists with the endpoint URL from the time you added it to the **remote-write** endpoint configuration. (OCPBUGS-36918)

- Previously, the build controller did not gracefully handle multiple **MachineOSBuild** objects that use the same secret. With this release, the build controller can handle these objects as expected. (OCPBUGS-36171)

- Previously, role bindings related to the **ImageRegistry**, **Build**, and **DeploymentConfig** capabilities were created in every namespace, even if the capability was disabled. With this release, the role bindings are only created if the cluster capability is enabled on the cluster. (OCPBUGS-34384)

1.9.2.2. Known issues

- An error might occur when deleting a pod that uses an SR-IOV network device. 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 reboots. Deleting the pod might take a few extra seconds due to this error. (OCPBUGS-11281, OCPBUGS-18822, RHEL-5988)

1.9.2.3. Updating

To update an existing OpenShift Container Platform 4.16 cluster to this latest release, see Updating a cluster using the CLI.

1.9.3. RHSA-2024:5107 - OpenShift Container Platform 4.16.7 bug fix and security update

Issued: 13 August 2024

OpenShift Container Platform release 4.16.7, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2024:5107 advisory. The RPM packages that are included in the update are provided by the RHBA-2024:5110 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 4.16.7 --pullspecs
```

1.9.3.1. Bug fixes

- Previously, the **openshift-install** CLI sometimes failed to connect to the bootstrap node when collecting bootstrap gather logs. The installation program reported an error message such as **The bootstrap machine did not execute the release-image.service systemd unit**. With this release and after the bootstrap gather logs issue occurs, the installation program now reports **Invalid log bundle or the bootstrap machine could not be reached and bootstrap logs were not collected**, which is a more accurate error message. (OCPBUGS-37838)

- Previously, after a firmware update through the **HostFirmwareComponents** resource, the resource would not show the newer information about the installed firmware in **Status.Components**. With this release, after a firmware update is run and the **BareMetalHosts** (BMH) object moves to **provisioning**, the newer information about the firmware is populated in the **HostFirmwareComponents** resource under **Status.Components.** (OCPBUGS-37765)

- Previously, oc-mirror plugin v2 for tags were not created for the OpenShift Container Platform release images. Some container registries depend on these tags as mandatory tags. With this release, these tags are added to all release images. (OCPBUGS-37757)

- Previously, extracting the IP address from the Cluster API Machine object only returned a single address. On VMware vSphere, the returned address would always be an IPv6 address and this caused issues with the **must-gather** implementation if the address was non-routable. With this release, the Cluster API Machine object returns all IP addresses, including IPv4, so that the **must-gather** issue no longer occurs on VMware vSphere. (OCPBUGS-37607)

- Previously, the installation program incorrectly required Amazon Web Services (AWS) permissions for creating Identity and Access Management (IAM) roles for an OpenShift Container Platform cluster that already had these roles. With this release, the installation program only requests permissions for roles not yet created. (OCPBUGS-37494)

- Previously, when you attempted to install a cluster on Red Hat OpenStack Platform (RHOSP) and you used special characters, such as the hash sign (**#**) in a cluster name, the Neutron API failed to tag a security group with the name of the cluster. This caused the installation of the cluster to fail. With this release, the installation program uses an alternative endpoint to tag security groups and this endpoint supports the use of special characters in tag names. (OCPBUGS-37492)

- Previously, the Dell iDRAC baseboard management controller (BMC) with the Redfish protocol caused clusters to fail on the Dell iDRAC servers. With this release, an update to the **idrac-redfish** management interface to unset the **ipxe** parameter fixed this issue. (OCPBUGS-37262)

- Previously, the **assisted-installer** did not reload new data from the **assisted-service** when the **assisted-installer** checked control plane nodes for readiness and a conflict existed with a write operation from the **assisted-installer-controller**. This conflict prevented the **assisted-installer** from detecting a node that was marked by the **assisted-installer-controller** as **Ready** because the **assisted-installer** relied on older information. With this release, the **assisted-installer** can receive the newest information from the **assisted-service**, so that it the **assisted-installer** can accurately detect the status of each node. (OCPBUGS-37167)

- Previously, the DNS-based egress firewall incorrectly caused memory increases for nodes running in a cluster because of multiple retry operations. With this release, the retry logic is fixed so that DNS pods no longer leak excess memory to nodes. (OCPBUGS-37078)

- Previously, **HostedClusterConfigOperator** resource did not delete the **ImageDigestMirrorSet** (IDMS) object after a user removed the **ImageContentSources** field from the **HostedCluster** object. This caused the IDMS object to remain in the **HostedCluster** object. With this release, **HostedClusterConfigOperator** removes all IDMS resources in the **HostedCluster** object so that this issue no longer exists. (OCPBUGS-36766)

- Previously, in a cluster that runs OpenShift Container Platform 4.16 with the Telco RAN DU reference configuration, long duration **cyclictest** or **timerlat** tests could fail with maximum latencies detected above **20** us. This issue occured because the **psi** kernel command line argument was being set to **1** by default when cgroup v2 is enabled. With this release, the issue is fixed by setting **psi=0** in the kernel arguments when enabling cgroup v2. The **cyclictest** latency issue reported in OCPBUGS-34022 is now also fixed. (OCPBUGS-37271)

1.9.3.2. Updating

To update an existing OpenShift Container Platform 4.16 cluster to this latest release, see Updating a cluster using the CLI.

1.9.4. RHSA-2024:4965 - OpenShift Container Platform 4.16.6 bug fix

Issued: 6 August 2024

OpenShift Container Platform release 4.16.6 is now available. The list of bug fixes that are included in the update is documented in the RHSA-2024:4965 advisory. The RPM packages that are included in the update are provided by the RHBA-2024:4968 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 4.16.6 --pullspecs
```

1.9.4.1. Enhancements

The following enhancements are included in this z-stream release:

1.9.4.1.1. Ingress Controller certificate expiration dates collected

- The Insights Operator now collects information about all Ingress Controller certificate expiration dates. The information is put into a JSON file in the path **aggregated/ingress_controllers_certs.json**. (OCPBUGS-37671)

1.9.4.1.2. Enabling debug log levels

- Previously, you could not control log levels for the internal component that selects IP addresses for cluster nodes. With this release, you can now enable debug log levels so that you can either increase or decrease log levels on demand. To adjust log levels, you must create a config map manifest file with a configuration similar to the following:

  ```
  apiVersion: v1
  data:
    enable-nodeip-debug: "true"
  kind: ConfigMap
  metadata:
    name: logging
    namespace: openshift-vsphere-infra
  # ...
  ```

  (OCPBUGS-35891)

1.9.4.1.3. Ironic and Inspector **htpasswd** improvement

- Previously, the Ironic and Inspector **htpasswd** were provided to the **ironic-image** using environment variables, which is not secure. From this release, the Ironic **htpasswd** is provided to **ironic-image** using the **/auth/ironic/htpasswd** file, and the Inspector **htpasswd** is provided to **ironic-image** using the **/auth/inspector/htpasswd** file for better security. (OCPBUGS-36285)

1.9.4.2. Bug fixes

- Previously, installer-created subnets were being tagged with **kubernetes.io/cluster/<clusterID>: shared**. With this release, subnets are now tagged with **kubernetes.io/cluster/<clusterID>: owned**. (OCPBUGS-37510)

- Previously, the same node was queued multiple times in the draining controller, which caused the the same node to be drained twice. With this release, a node will only be drained once. (OCPBUGS-37470)

- Previously, cordoned nodes in machine config pools (MCPs) with higher **maxUnavailable** than unavailable nodes might be selected as an update candidate. With this release, cordoned nodes will never be queued for an update. (OCPBUGS-37460)

- Previously, oc-mirror plugin v2, when running behind proxy with the system proxy configuration set, would attempt to recover signatures for releases without using the system proxy configuration. With this release, the system proxy configuration is taken into account during signature recovery as well and the issue is resolved. (OCPBUGS-37445)

- Previously, an alert for **OVNKubernetesNorthdInactive** would not fire in circumstances where it should fire. With this release, the issue is fixed so that the alert for **OVNKubernetesNorthdInactive** fires as expected. (OCPBUGS-37362)

- Previously, the Load Balancer ingress rules were continuously revoked and authorized, causing unnecessary Amazon Web Services (AWS) Application Programming Interface (API) calls and cluster provision delays. With this release, the Load Balancer checks for ingress rules that need to be applied and the issue is resolved. (OCPBUGS-36968)

- Previously, in the OpenShift Container Platform web console, one inactive or idle browser tab caused the session to expire for all other tabs. With this release, activity in any tab will prevent session expiration. (OCPBUGS-36864)

- Previously, the Open vSwitch (OVS) pinning procedure set the CPU affinity of the main thread, but other CPU threads did not pick up this affinity if they had already been created. As a consequence, some OVS threads did not run on the correct CPU set, which might interfere with the performance of pods with a Quality of Service (QoS) class of **Guaranteed**. With this update, the OVS pinning procedure updates the affinity of all the OVS threads, ensuring that all OVS threads run on the correct CPU set. (OCPBUGS-36608)

- Previously, the etcd Operator checked the health of etcd members in serial with an all-member timeout that matched the single-member timeout. That allowed one slow member check to consume the entire timeout, and cause later member checks to fail with the error **deadline-exceeded**, regardless of the health of that later member. Now, etcd checks the health of members in parallel so the health and speed of one member's check doesn't affect the other members' checks. (OCPBUGS-36489)

1.9.4.3. Updating

To update an existing OpenShift Container Platform 4.16 cluster to this latest release, see Updating a cluster using the CLI.

1.9.5. RHBA-2024:4855 - OpenShift Container Platform 4.16.5 bug fix

Issued: 31 July 2024

OpenShift Container Platform release 4.16.5 is now available. The list of bug fixes that are included in the update is documented in the RHBA-2024:4855 advisory. The RPM packages that are included in the update are provided by the RHSA-2024:4858 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 4.16.5 --pullspecs
```

1.9.5.1. Bug fixes

- Previously, with oc-mirror plugin v2 (Technology Preview), when a generated archive was moved to a different machine, the mirroring from archive to the mirror registry operation failed and outputted the following error message:

  ```
  [ERROR]: [ReleaseImageCollector] open ${FOLDER}/working-dir/hold-release/ocp-release/4.15.17-x86_64/release-manifests/image-references: no such file or directory
  ```

  With this release, the machine that runs oc-mirror receives an automatic update to change its target location to the working directory. (OCPBUGS-37040)

- Previously, the OpenShift CLI (**oc**) command **openshift-install destroy cluster** stalled and caused the following error message:

  ```
  VM has a local SSD attached but an undefined value for 'discard-local-ssd' when using A3 instance types
  ```

  With this release, after you issue the command, local SSDs are removed so that this bug no longer persists. (OCPBUGS-36965)

- Previously, when the Cloud Credential Operator checked if passthrough mode permissions were correct, the Operator sometimes received a response from the Google Cloud Platform (GCP) API about an invalid permission for a project. This bug caused the Operator to enter a degraded state that in turn impacted the installation of the cluster. With this release, the Cloud Credential Operator checks specifically for this error so that it diagnoses it separately without impacting the installation of the cluster. (OCPBUGS-36834)

- Previously, with oc-mirror plugin v2 (Technology Preview), when a generated archive was moved to a different machine, the mirroring from archive to the mirror registry operation failed and outputted the following error message:

  ```
  [ERROR]: [ReleaseImageCollector] open ${FOLDER}/working-dir/hold-release/ocp-release/4.15.17-x86_64/release-manifests/image-references: no such file or directory
  ```

  With this release, the machine that runs oc-mirror receives an automatic update to change its target location to the working directory. (OCPBUGS-37040)

1.9.5.2. Updating

To update an existing OpenShift Container Platform 4.16 cluster to this latest release, see Updating a cluster using the CLI.

1.9.6. RHSA-2024:4613 - OpenShift Container Platform 4.16.4 bug fix and security update

Issued: 24 July 2024

OpenShift Container Platform release 4.16.4, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2024:4613 advisory. The RPM packages that are included in the update are provided by the RHSA-2024:4616 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 4.16.4 --pullspecs
```

1.9.6.1. Bug fixes

- Previously, a change to the Ingress Operator added logic to **clear spec.host** and set **spec.subdomain** on the canary route. However, the Operator's service account did not have the necessary **routes/custom-host** permission to update **spec.host** or **spec.subdomain** on an existing route. With this release, the permission is added to the **ClusterRole** resource for the Operator's service account and the issue is resolved. (OCPBUGS-32887)

- Previously, the number of calls to the subscription's **fetchOrganization** endpoint from the Console Operator was too high, which caused issues with installation. With this release, the organization ID is cached and the issue is resolved. (OCPBUGS-34012)

- Previously, role bindings related to the **ImageRegistry**, **Build**, and **DeploymentConfig** capabilities were created in every namespace, even if the respective capability was disabled. With this release, the role bindings are only created if the respective cluster capability is enabled on the cluster. (OCPBUGS-34384)

- Previously, the MetalLB Operator deployed the downstream image when deploying with FRR-K8s, the Border Gateway Protocol (BGP) backend for MetalLB. With this release, the MetalLB Operator deploys the upstream image instead of the dowstream one. (OCPBUGS-35864)

- Previously, when LUKS encryption was enabled on a system using 512 emulation (512e) disks, the encryption failed at the **ignition-ostree-growfs** step and reported an error because of an alignment issue. With this release, a workaround is added in the **ignition-ostree-growfs** step to detect this situation and resolve the alignment issue. (OCPBUGS-36147)

- Previously, the **--bind-address** parameter for localhost caused liveness test failure for IBM Power Virtual Server clusters. With this release, the **--bind-address** parameter for localhost is removed and the issue is resolved. (OCPBUGS-36317)

- Previously, Operator bundle unpack jobs that had already been created were not found by the Operator Lifecycle Manager (OLM) when installing an Operator. With this release, the issue is resolved. (OCPBUGS-36450)

- Previously, the etcd data store used for Cluster API-provisioned installations was only removed when either the bootstrap node or the cluster was destroyed. With this release, if there is an error during infrastructure provisioning, the data store is removed and does not take up unnecessary disk space. (OCPBUGS-36463)

- Previously, enabling custom feature gates could cause the installation to fail in AWS if the feature gate **ClusterAPIInstallAWS=true** was not enabled. With this release, the **ClusterAPIInstallAWS=true** feature gate is no longer required. (OCPBUGS-36720)

- Previously, if **create cluster** was run after the **destroy cluster** command, an error would report that local infrastructure provisioning artifacts already exist. With this release, leftover artifacts are removed with **destroy cluster** and the issue is resolved. (OCPBUGS-36777)

- Previously, the **OperandDetails** page displayed information for the first custom resource definition (CRD) that matched by name. With this release, the **OperandDetails** page displays information for the CRD that matches by name and by the version of the operand. (OCPBUGS-

36841)

- Previously, if the **openshift.io/internal-registry-pull-secret-ref** annotation was removed from a **ServiceAccount** resource, OpenShift Container Platform re-created the deleted annotation and created a new managed image pull secret. This contention could cause the cluster to get overloaded with image pull secrets. With this release, OpenShift Container Platform attempts to reclaim managed image pull secrets that were previously referenced and deletes managed image pull secrets that remain orphaned after reconciliation. (OCPBUGS-36862)

- Previously, some of the processes remained running after the installation program stopped due to setup failures. With this release, all installation processes stop when the installation program stops running. (OCPBUGS-36890)

- Previously, there was no runbook for the **ClusterMonitoringOperatorDeprecatedConfig** alert. With this release, the runbook for the **ClusterMonitoringOperatorDeprecatedConfig** alert is added and the issue is resolved. (OCPBUGS-36907)

- Previously, the **Cluster overview page** included a *View all steps in documentation* link that resulted in a 404 error for ROSA and OSD clusters. With this update, the link does not appear for ROSA and OSD clusters. (OCPBUGS-37063)

- Previously, there was a mismatch between OpenSSL versions of Machine Config Operator tools used by OpenShift Container Platform and the OpenSSL version that runs on the hosted control plane. With this release, the issue is resolved. (OCPBUGS-37241)

1.9.6.2. Updating

To update an existing OpenShift Container Platform 4.16 cluster to this latest release, see Updating a cluster using the CLI.

1.9.7. RHSA-2024:4469 - OpenShift Container Platform 4.16.3 bug fix and security update

Issued: 16 July 2024

OpenShift Container Platform release 4.16.3, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2024:4469 advisory. The RPM packages that are included in the update are provided by the RHBA-2024:4472 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 4.16.3 --pullspecs
```

1.9.7.1. Enhancements

The following enhancements are included in this z-stream release:

1.9.7.1.1. Configuring Capacity Reservation by using machine sets

- OpenShift Container Platform release 4.16.3 introduces support for on-demand Capacity Reservation with Capacity Reservation groups on Microsoft Azure clusters. For more information, see *Configuring Capacity Reservation by using machine sets* for compute or control plane machine sets. (OCPCLOUD-1646)

1.9.7.1.2. Adding alternative ingress for disabled ingress clusters

- With this release, the console Operator configuration API can add alternative ingress to environments where the ingress cluster capability has been disabled. (OCPBUGS-33788)

1.9.7.2. Bug fixes

- Previously, if **spec.grpcPodConfig.securityContextConfig** was not set for CatalogSource objects in namespaces with the PodSecurityAdmission "restricted" level enforced, the default securityContext was set as **restricted**. With this release, the OLM catalog operator configures the catalog pod with the securityContexts necessary to pass PSA validation and the issue has been resolved. (OCPBUGS-34979)

- Previously, the **HighOverallControlPlaneCPU** alert triggered warnings based on criteria for multi-node clusters with high availability. As a result, misleading alerts were triggered in single-node OpenShift clusters because the configuration did not match the environment criteria. This update refines the alert logic to use single-node OpenShift-specific queries and thresholds and account for workload partitioning settings. As a result, CPU utilization alerts in single-node OpenShift clusters are accurate and relevant to single-node configurations. (OCPBUGS-35831)

- Previously, the **--bind-address** to localhost caused the liveness test to fail for PowerVS clusters. With this release, the **--bind-address** to localhost is removed and the issue has been resolved. (OCPBUGS-36317)

- Previously, nodes that were booted using 4.1 and 4.2 boot images for OpenShift Container Platform got stuck during provisioning because the **machine-config-daemon-firstboot.service** had incompatible machine-config-daemon binary code. With this release, the binary has been updated and the issue has been resolved. (OCPBUGS-36330)

- Previously, there was no access to the source registry when the **diskToMirror** action was performed on a fully disconnected environment. When using **oc-mirror v2** in **MirrorToDisk**, the catalog image and contents are stored under a subfolder under **working-dir** that corresponds to the digest of the image. Then, while using **DiskToMirror**, oc-mirror attempts to call the source registry to resolve the catalog image tag to a digest to find the corresponding subfolder on disk. With this release, **oc-mirror** interrogates the local cache during the **diskToMirror** process to determine this digest. (OCPBUGS-36386)

- Previously, if a new deployment was performed at the OSTree level on a host that was identical to the current deployment but on a different stateroot, the OSTree saw them as equal. This behavior incorrectly prevented the boot loader from updating when **set-default** was invoked, as OSTree did not recognize the two stateroots as a differentiation factor for deployments. With this release, OSTree's logic has been modified to consider the stateroots and allows OSTree to properly set the default deployment to a new deployment with different stateroots. (OCPBUGS-36386)

- Previously, Installer logs for AWS clusters contained unnecessary messages about the Elastic Kubernetes Service (EKS) that could lead to confusion. With this release, the EKS log lines are disabled and the issue has been resolved. (OCPBUGS-36447)

- Previously, a change of dependency targets was introduced in OpenShift Container Platform 4.14 that prevented disconnected ARO installs from scaling up new nodes after they upgraded to affected versions. With this release, disconnected ARO installs can scale up new nodes after upgrading to OpenShift Container Platform 4.16. (OCPBUGS-36536)

- Previously, connection refused on **port 9637** reported as *Target Down* for Windows nodes because CRIO does not run on Windows nodes. With this release, Windows nodes are excluded from the Kubelet Service Monitor. (OCPBUGS-36717)

1.9.7.3. Updating

To update an existing OpenShift Container Platform 4.16 cluster to this latest release, see Updating a cluster using the CLI.

1.9.8. RHSA-2024:4316 - OpenShift Container Platform 4.16.2 bug fix and security update

Issued: 9 July 2024

OpenShift Container Platform release 4.16.2, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2024:4316 advisory. The RPM packages that are included in the update are provided by the RHBA-2024:4319 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 4.16.2 --pullspecs
```

1.9.8.1. Bug fixes

- Previously, for clusters upgraded from older versions of OpenShift Container Platform, enabling **kdump** on an OVN-enabled cluster sometimes prevented the node from rejoining the cluster or returning to the **Ready** state. With this release, stale data is removed from older OpenShift Container Platform versions and ensures this stale data is always cleaned up. The node can now start correctly and rejoin the cluster. (OCPBUGS-36198)

- Previously, unexpected output would appear in the terminal when creating an installer-provisioned infrastructure (IPI) cluster. With this release, the issue has been resolved and the unexpected output no longer appears. (OCPBUGS-36156)

- Previously, the OpenShift Container Platform console did not show filesystem metrics on the nodes list. With this release, the filesystem metrics now appear in the nodes table. (OCPBUGS-35946)

- Previously, the Prometheus dashboard showed up empty for non-multi-cluster environments. With this release, the dashboard populates the dashboard panels as expected for both cases. (OCPBUGS-35904)

- Previously, a regression in 4.16.0 caused new baremetal installer-provisioned infrastructure (IPI) installations to fail when proxies were used. This was caused by one of the services in the bootstrap virtual machine (VM) trying to access IP address 0.0.0.0 through the proxy. With this release, this service no longer accesses 0.0.0.0. (OCPBUGS-35818)

- Previously, the Cluster API Provider IBM Cloud waited for some resources to be created before creating the load balancers on IBM Power Virtual Server clusters. This delay sometimes resulted in the load balancers not being created before the 15 minute timeout. With this release, the timeout has been increased. (OCPBUGS-35722)

- Previously, when installing a cluster on Red Hat OpenStack Platform (RHOSP) using the Cluster

API implementation, the additional security group rule added to control plane nodes for compact clusters was forcing IPv4 protocol and prevented deploying dual-stack clusters. This was a regression from installations using Terraform. With this release, the rule now uses the correct protocol based on the requested IP version. (OCPBUGS-35718)

- Previously, the internal image registry would not correctly authenticate users on clusters configured with external OpenID Connect (OIDC) users, making it impossible for users to push or pull images to and from the internal image registry. With this release, the internal image registry starts using the SelfSubjectReview API, dropping use of the OpenShift Container Platform specific user API, which is not available on clusters configured with external OIDC users, making it possible to successfully authenticate with the image registry again. (OCPBUGS-35567)

- Prevously, an errant code change resulted in a duplicated **oauth.config.openshift.io** item on the **Global Configuration** page. With this update, the duplicated item is removed. (OCPBUGS-35565)

- Previously, with **oc-mirror** v2, when mirroring fails due to various reasons, such as network errors or invalid operator catalog content, **oc-mirror** did not generate cluster resources. With this bug fix, **oc-mirror** v2 performs the following actions:

  - Pursues mirroring other images when errors occur on Operator images and additional images, and aborts mirroring when errors occur on release images.

  - Generates cluster resources for the cluster based on subset of correctly mirrored images.

  - Collects all mirroring errors in a log file.

  - Logs all mirroring errors in a separate log file. (OCPBUGS-35409)

- Previously, pseudolocalization was not working in the OpenShift Container Platform console due to a configuration issue. With this release, the issue is resolved and pseudolocalization works again. (OCPBUGS-35408)

- Previously, the **must-gather** process ran too long while collecting CPU-related performance data for nodes due to collecting the data sequentially for each node. With this release, the node data is collected in parallel, which significantly shortens the **must-gather** data collection time. (OCPBUGS-35357)

- Previously, builds could not set the **GIT_LFS_SKIP_SMUDGE** environment variable and use its value when cloning source code. This caused builds to fail for some git repositories with LFS files. With this release, the build is allowed to set this environment variable and use it during the git clone step of the build. (OCPBUGS-35283)

- Previously, registry overrides were present in non-relevant data plane images. With this release, the way OpenShift Container Platform propagates the override-registries has been modified and the issue is fixed. (OCPBUGS-34602)

- Previously, RegistryMirrorProvider images were not being updated during the reconciliation because RegistryMirrorProvider was modifying the cached image directly instead of the internal entries. With this release, the way we update the images has been modified, avoiding the cache and doing it directly in the entries so the bug no longer presents. (OCPBUGS-34569)

- Previously, the **alertmanager-trusted-ca-bundle ConfigMap** was not injected into the user-defined Alertmanager container, which prevented the verification of HTTPS web servers receiving alert notifications. With this update, the trusted CA bundle **ConfigMap** is mounted

into the Alertmanager container at the **/etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem** path. (OCPBUGS-34530)

- Previously, for Amazon Web Services (AWS) clusters that use Security Token Service (STS), the Cloud Credential Operator (CCO) checked the value of **awsSTSIAMRoleARN** in the **CredentialsRequest** custom resource to create a secret. When **awsSTSIAMRoleARN** was not present, CCO logged an error. The issue is resolved in this release. (OCPBUGS-34117)

- Previously, with the OVN-Kubernetes setting for routing-via-host set to shared gateway mode, its default value, OVN-Kubernetes did not correctly handle traffic streams that mixed non-fragmented and fragmented packets from the IP layer on cluster ingress. This caused connection resets or packet drops. With this release, OVN-Kubernetes correctly reassembles and handles external traffic IP packet fragments on ingress. (OCPBUGS-29511)

1.9.8.2. Known issue

- If the **ConfigMap** maximum transmission unit (MTU) is absent in the namespace **openshift-network-operator**, users have to create the **ConfigMap** manually with the machine MTU value, before starting the live migration. Otherwise, the live migration will get stuck and fail. (OCPBUGS-35829)

1.9.8.3. Updating

To update an existing OpenShift Container Platform 4.16 cluster to this latest release, see Updating a cluster using the CLI.

1.9.9. RHSA-2024:4156 - OpenShift Container Platform 4.16.1 bug fix and security update

Issued: 3 July 2024

OpenShift Container Platform release 4.16.1, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2024:4156 advisory. The RPM packages that are included in the update are provided by the RHSA-2024:4159 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 4.16.1 --pullspecs
```

1.9.9.1. Bug fixes

- Previously, an error in **growpart** caused the device to be locked, which prevented the Linux Unified Key Setup-on-disk-format (LUKS) device from being opened. As a result, the node was unable to boot and went into emergency mode. With this release, the call to the **growpart** is removed and this issue is fixed. (OCPBUGS-35973)

- Previously, a bug in systemd might have caused the **coreos-multipath-trigger.service** unit to hang indefinitely. As a result, the system would never finish booting. With this release, the systemd unit was removed and the issue is fixed. (OCPBUGS-35748)

- Previously, the KMS key was applied as an empty string, which caused the key to be invalid. With this release, the empty string is removed and the KMS key is only applied when one exists from the **install-config.yaml**. (OCPBUGS-35531)

- Previously, there was no validation of the values for confidential compute and on host maintenance set by the user. With this release, when confidential compute is enabled by the user the value for **onHostMaintenance** must be set to **onHostMaintenance: Terminate**. (OCPBUGS-35493)

- Previously, in user-provisioned infrastructure (UPI) clusters or clusters that were upgraded from older versions, **failureDomains** might be missing in Infrastructure objects, which caused certain checks to fail. With this release, a **failureDomains** fallback is synthesized from **cloudConfig** if none are available in **infrastructures.config.openshift.io**. (OCPBUGS-35446)

- Previously, when a new version of a custom resource definition (CRD) specified a new conversion strategy, this conversion strategy was expected to successfully convert resources. This was not the case because Operator Lifecycle Manager (OLM) cannot run the new conversion strategies for CRD validation without actually performing the update operation. With this release, the OLM generates a warning message during the update process when CRD validations fail with the existing conversion strategy and the new conversion strategy is specified in the new version of the CRD. (OCPBUGS-35373)

- Previously, Amazon Web Services (AWS) HyperShift clusters leveraged their Amazon Virtual Private Cloud (VPC)'s primary classless inter-domain routing (CIDR) range to generate security group rules on the data plane. As a consequence, installing AWS HyperShift clusters into an AWS VPC with multiple CIDR ranges could cause the generated security group rules to be insufficient. With this update, security group rules are generated based on the provided Machine CIDR range to resolve this issue. (OCPBUGS-35056)

- Previously, the Source-to-Image (S2I) build strategy needed to be explicitly added to the **func.yaml** in order to create the Serverless function. Additionally, the error message did not indicate the problem. With this release, if S2I is not added, users can still create the Serverless function. However, if it is not S2I, users cannot create the function. Additionally, the error messages have been updated to provide more information. (OCPBUGS-34717)

- Previously, the **CurrentImagePullSecret** field on the **MachineOSConfig** object was not being used in when rolling out new on-cluster layering build images.. With this release, the **CurrentImagePullSecret** field on the **MachineOSConfig** object is allowed to be used by the image rollout process. (OCPBUGS-34261)

- Previously, when sending multiple failing port-forwarding requests, CRI-O memory usage increases until the node dies. With this release, the memory leakage when sending a failing port-forward request is fixed and the issue is resolved. (OCPBUGS-30978)

- Previously, the **oc get podmetrics** and **oc get nodemetrics** commands were not working properly. This update fixes the issue. (OCPBUGS-25164)

1.9.9.2. Updating

To update an existing OpenShift Container Platform 4.16 cluster to this latest release, see Updating a cluster using the CLI.

1.9.10. RHSA-2024:0041 - OpenShift Container Platform 4.16.0 image release, bug fix, and security update advisory

Issued: 27 June 2024

OpenShift Container Platform release 4.16.0, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2024:0041 advisory. The RPM packages that are included in the update are provided by the RHSA-2024:0045 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 4.16.0 --pullspecs
```