# OpenShift Container Platform 4.15

## Release notes

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

Last Updated: 2024-03-19

# OpenShift Container Platform 4.15 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 4.15 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-2023:7198) is now available. This release uses Kubernetes 1.28 with CRI-O runtime. New features, changes, and known issues that pertain to OpenShift Container Platform 4.15 are included in this topic.

OpenShift Container Platform 4.15 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 4.15 is supported on Red Hat Enterprise Linux (RHEL) 8.8 and 8.9, and on Red Hat Enterprise Linux CoreOS (RHCOS) 4.15.

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

Starting with OpenShift Container Platform 4.12, an additional six months is added to the Extended Update Support (EUS) phase on even numbered releases from 18 months to two years. For more information, see the Red Hat OpenShift Container Platform Life Cycle Policy .

Starting with OpenShift Container Platform 4.14, Extended Update Support (EUS) is extended to 64-bit ARM, IBM Power® (ppc64le), and IBM Z® (s390x) platforms. For more information, see the OpenShift EUS Overview.

Maintenance support ends for version 4.12 on 17 July 2024 and goes to extended update support phase. For more information, see the Red Hat OpenShift Container Platform Life Cycle Policy .

Commencing with the 4.15 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 9.2

RHCOS now uses Red Hat Enterprise Linux (RHEL) 9.2 packages in OpenShift Container Platform 4.15. These packages ensure that your OpenShift Container Platform instance receives the latest fixes, features, enhancements, hardware support, and driver updates.

#### 1.3.1.2. Support for iSCSI devices (Technology Preview)

RHCOS now supports the **iscsi_bft** driver, letting you boot directly from iSCSI devices that work with the iSCSI Boot Firmware Table (iBFT), as a Technology Preview. This lets you target iSCSI devices as the root disk for installation.

For more information, see the RHEL documentation.

### 1.3.2. Installation and update

#### 1.3.2.1. Encrypting Azure storage account during installation

You can now encrypt Azure storage accounts during installation by providing the installation program with a customer managed encryption key. See Installation configuration parameters for descriptions of the parameters required to encrypt Azure storage accounts.

#### 1.3.2.2. CAPO integration into the cluster CAPI Operator (Tech Preview)

If you enable the **TechPreviewNoUpgrade** feature flag, the Cluster API (CAPI) Operator deploys the Cluster API Provider for OpenStack (CAPO) and manages its lifecycle. The CAPI Operator automatically creates **Cluster** and **OpenStackCluster** resources for the current OpenShift Container Platform cluster.

It is now possible to configure the CAPI **Machine** and CAPO **OpenStackMachine** resources in similar fashion to how Machine API (MAPI) resources are configured. It is important to note that the CAPI resources are equivalent to MAPI resources but not identical.

#### 1.3.2.3. IBM Cloud and user-managed encryption

You can now specify your own IBM® Key Protect for IBM Cloud® root key as part of the installation process. This root key is used to encrypt the root (boot) volume of control plane and compute machines, and the persistent volumes (data volumes) that are provisioned after the cluster is deployed.

For more information, see User-managed encryption for IBM Cloud .

### 1.3.2.4. Installing a cluster on IBM Cloud with limited internet access

You can now install a cluster on IBM Cloud® in an environment with limited internet access, such as a disconnected or restricted network cluster. With this type of installation, you create a registry that mirrors the contents of the OpenShift Container Platform installation images. You can create this registry on a mirror host, which can access both the internet and your restricted network.

For more information, see Installing a cluster on IBM Cloud in a restricted network .

### 1.3.2.5. Installing a cluster on AWS to extend nodes to Wavelength Zones

You can quickly install an OpenShift Container Platform cluster in Amazon Web Services (AWS) Wavelength Zones by setting the zone names in the edge compute pool of the **install-config.yaml** file, or install a cluster in an existing VPC with Wavelength Zone subnets.

You can also perform postinstallation tasks to extend an existing OpenShift Container Platform cluster on AWS to use AWS Wavelength Zones.

For more information, see Installing a cluster on AWS with compute nodes on AWS Wavelength Zones and Extend existing clusters to use AWS Local Zones or Wavelength Zones .

### 1.3.2.6. Customizing the cluster network MTU on AWS deployments

Before you deploy a cluster on AWS Local Zones infrastructure, you can customize the cluster network maximum transmission unit (MTU) for your cluster network to meet the needs of your infrastructure.

You can customize the MTU for a cluster by specifying the networking.clusterNetworkMTU parameter in the **install-config.yaml** configuration file.

For more information, see Customizing the cluster network MTU.

### 1.3.2.7. Installing a cluster on AWS with compute nodes on AWS Outposts

In OpenShift Container Platform version 4.14, you could install a cluster on AWS with compute nodes running in AWS Outposts as a Technology Preview. In OpenShift Container Platform 4.15, you can install a cluster on AWS into an existing VPC and provision compute nodes on AWS Outposts as a postinstallation configuration task.

For more information, see Installing a cluster on AWS into an existing VPC and Extending an AWS VPC cluster into an AWS Outpost.

### 1.3.2.8. Nutanix and fault tolerant deployments

By default, the installation program installs control plane and compute machines into a single Nutanix Prism Element (cluster). To improve the fault tolerance of your OpenShift Container Platform cluster, you can now specify that these machines be distributed across multiple Nutanix clusters by configuring failure domains.

For more information, see Fault tolerant deployments using multiple Prism Elements .

### 1.3.2.9. OpenShift Container Platform on 64-bit ARM

OpenShift Container Platform 4.15 now supports the ability to enable 64k page sizes in the RHCOS kernel using the Machine Config Operator (MCO). This setting is exclusive to machines with 64-bit ARM architectures. For more information, see the Machine configuration tasks documentation.

#### 1.3.2.10. Optional OLM cluster capability

In OpenShift Container Platform 4.15, you can disable the Operator Lifecycle Manager (OLM) capability during installation. For further information, see Operator Lifecycle Manager capability.

#### 1.3.2.11. Deploying Red Hat OpenStack Platform (RHOSP) with root volume and etcd on local disk (Technology Preview)

You can now move etcd from a root volume (Cinder) to a dedicated ephemeral local disk as a Day 2 deployment. With this Technology Preview feature, you can resolve and prevent performance issues of your RHOSP installation.

For more information, see Deploying on OpenStack with rootVolume and etcd on local disk.

#### 1.3.2.12. Configure vSphere integration with the Agent-based Installer

You can now configure your cluster to use vSphere while creating the **install-config.yaml** file for an Agent-based Installation. For more information, see Additional VMware vSphere configuration parameters.

#### 1.3.2.13. Additional bare metal configurations during Agent-based installation

You can now make additional configurations for the bare metal platform while creating the **install-config.yaml** file for an Agent-based Installation. These new options include host configuration, network configuration, and baseboard management controller (BMC) details.

These fields are not used during the initial provisioning of the cluster, but they eliminate the need to set the fields after installation. For more information, see Additional bare metal configuration parameters for the Agent-based Installer.

#### 1.3.2.14. Use the Dell iDRAC BMC to configure a RAID during installer-provisioned installation

You can now use the Dell iDRAC baseboard management controller (BMC) with the Redfish protocol to configure a redundant array of independent disks (RAID) for the bare metal platform during an installer-provisioned installation. For more information, see Optional: Configuring the RAID.

### 1.3.3. Postinstallation configuration

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

On OpenShift Container Platform 4.15 clusters with multi-architecture compute machines, you can now enable 64k page sizes in the Red Hat Enterprise Linux CoreOS (RHCOS) kernel on the 64-bit ARM compute machines in your cluster. For more information on setting this parameter, see Enabling 64k pages on the Red Hat Enterprise Linux CoreOS (RHCOS) kernel.

### 1.3.4. Web console

#### 1.3.4.1. Administrator perspective

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

- Enable and disable the tailing to Pod log viewer to minimize load time.
- View recommended values for **VerticalPodAutoscaler** on the **Deployment** page.

#### 1.3.4.1.1. Node uptime information

With this update, you can enable the ability to view additional node uptime information to track node restarts or failures. Navigate to the **Compute → Nodes** page, click **Manage columns**, and then select **Uptime**.

#### 1.3.4.1.2. Dynamic plugin enhancements

With this update, you can add a new details item to the default resource summary on the **Details** page using **console.resource/details-item**. The OpenShift Container Platform release also adds example implementation for annotation, label and the delete modal to the CronTab dynamic plugin.

For more information, see Dynamic plugin reference

For more information about **console.resource/details-item**, see OpenShift Container Platform console API.

#### 1.3.4.1.3. OperatorHub support for Azure AD Workload Identity

With this release, OperatorHub detects when a OpenShift Container Platform cluster running on Azure is configured for Azure AD Workload Identity. When detected, a "Cluster in Workload Identity / Federated Identity Mode" notification is displayed with additional instructions before installing an Operator to ensure it runs correctly. The **Operator Installation** page is also modified to add fields for the required Azure credentials information.

For the updated step for the **Install Operator** page, see Installing from OperatorHub using the web console.

### 1.3.4.2. Developer Perspective

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

- Pipeline history and logs based on the data from Tekton Results are available in the dashboard without requiring PipelineRun CRs on the cluster.

#### 1.3.4.2.1. Software Supply Chain Enhancements

The **PipelineRun Details** page in the **Developer** or **Administrator** perspective of the web console provides an enhanced visual representation of PipelineRuns within a Project.

For more information, see Red Hat OpenShift Pipelines.

#### 1.3.4.2.2. Red Hat Developer Hub in the web console

With this update, a quick start is now available for you to learn more about how to install and use the developer hub.

For more information, see Product Documentation for Red Hat Developer Hub .

#### 1.3.4.2.3. builds for OpenShift Container Platform is supported in the web console

With this update, builds for OpenShift Container Platform 1.0 is supported in the web console. Builds is an extensible build framework based on the Shipwright project. You can use builds for OpenShift Container Platform to build container images on an OpenShift Container Platform cluster.

For more information, see builds for OpenShift Container Platform .

### 1.3.5. IBM Z and IBM LinuxONE

With this release, IBM Z® and IBM® LinuxONE are now compatible with OpenShift Container Platform 4.15. You can perform the installation with z/VM, LPAR, or Red Hat Enterprise Linux (RHEL) Kernel-based Virtual Machine (KVM). For installation instructions, see the following documentation:

- Installing a cluster with 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 4.15 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
- cert-manager Operator for Red Hat OpenShift
- **s390x** control plane with **x86_64** multi-architecture compute nodes

**Installing a cluster in an LPAR on IBM Z and IBM LinuxONE**
OpenShift Container Platform now supports user-provisioned installation of OpenShift Container Platform 4.15 in a logical partition (LPAR) on IBM Z and IBM LinuxONE.

For installation instructions, see the following documentation:

- Installing a cluster in an LPAR on IBM Z® and IBM® LinuxONE
- Installing a cluster in an LPAR on IBM Z® and IBM® LinuxONE in a restricted network

### 1.3.6. IBM Power

IBM Power® is now compatible with OpenShift Container Platform 4.15. 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 4.15 adds improvements and new capabilities to OpenShift Container Platform components.

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

- Agent-based Installer
- cert-manager Operator for Red Hat OpenShift
- Multi-architecture IBM Power® control plane with support of Intel and IBM Power® workers
- nx-gzip for Power10 (Hardware Acceleration)
- The **openshift-install** utility to support various SMT levels on IBM Power® (Hardware Acceleration)

### 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 |
| 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 |

| Feature | IBM Power® | IBM Z® and IBM® LinuxONE |
|---|---|---|
| Helm | Supported | Supported |
| Horizontal pod autoscaling | Supported | Supported |
| Hosted control planes (Technology Preview) | Supported | Supported |
| IBM Secure Execution | Unsupported | Supported |
| IBM Power® Virtual Server Block CSI Driver Operator (Technology Preview) | Supported | Unsupported |
| Installer-provisioned Infrastructure Enablement for IBM Power® Virtual Server (Technology Preview) | 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 |
| Multipathing | Supported | Supported |
| Network-Bound Disk Encryption - External Tang Server | Supported | Supported |
| Non—volatile memory express drives (NVMe) | 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 |

| Feature | IBM Power® | IBM Z® and IBM® LinuxONE |
|---|---|---|
| Scheduler profiles | Supported | Supported |
| Stream Control Transmission Protocol (SCTP) | Supported | Supported |
| Support for multiple network interfaces | Supported | Supported |
| Three-node cluster support | Supported | Supported |
| Topology Manager | Supported | Unsupported |
| z/VM Emulated FBA devices on SCSI disks | Unsupported | Supported |
| 4K FCP block device | Supported | Supported |

**Table 1.2. Persistent storage options**

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

1. Persistent shared storage must be provisioned by using either Red Hat OpenShift Data Foundation or other supported storage protocols.

2. Persistent non-shared storage must be provisioned 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 |

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

| Feature | IBM Power® | IBM Z® and IBM® LinuxONE |
|---|---|---|
| Expansion | Supported | Supported |
| Snapshot | Supported | Supported |

### 1.3.7. Authentication and authorization

#### 1.3.7.1. OLM-based Operator support for Azure AD Workload Identity

With this release, some Operators managed by Operator Lifecycle Manager (OLM) on Azure clusters can use the Cloud Credential Operator (CCO) in manual mode with Azure AD Workload Identity. These Operators authenticate with short-term credentials that are managed outside the cluster.

For more information, see CCO-based workflow for OLM-managed Operators with Azure AD Workload Identity.

### 1.3.8. Networking

#### 1.3.8.1. OVN-Kubernetes network plugin support for IPsec encryption of external traffic general availability (GA)

OpenShift Container Platform now supports encryption of external traffic, also known as *north-south traffic*. IPsec already supports encryption of network traffic between pods, known as *east-west traffic*. You can use both features together to provide full in-transit encryption for OpenShift Container Platform clusters.

This feature is supported on the following platforms:

- Bare metal
- Google Cloud Platform (GCP)
- Red Hat OpenStack Platform (RHOSP)
- VMware vSphere

For more information, see Enabling IPsec encryption for external IPsec endpoints .

#### 1.3.8.2. IPv6 unsolicited neighbor advertisements now default on macvlan CNI plugin

Previously, if one pod (**Pod X**) was deleted, and a second pod ( **Pod Y**) was created with a similar configuration, **Pod Y** might have had the same IPv6 address as **Pod X**, but it would have a different MAC address. In this scenario, the router was unaware of the MAC address change, and it would continue sending traffic to the MAC address for **Pod X**.

With this update, pods created using the macvlan CNI plugin, where the IP address management CNI plugin has assigned IPs, now send IPv6 unsolicited neighbor advertisements by default onto the network. This enhancement notifies the network fabric of the new pod's MAC address for a particular IP to refresh IPv6 neighbor caches.

#### 1.3.8.3. Configuring the Whereabouts IP reconciler schedule

The Whereabouts reconciliation schedule was hard-coded to run once per day and could not be reconfigured. With this release, a **ConfigMap** object has enabled the configuration of the Whereabouts cron schedule. For more information, see Configuring the Whereabouts IP reconciler schedule .

#### 1.3.8.4. Status management updates for EgressFirewall and AdminPolicyBasedExternalRoute CR

The following updates have been made to the status management of **EgressFirewall** and **AdminPolicyBasedExternalRoute** custom resource policy:

- The **status.status** field is set to **failure** if at least one message reports **failure**.
- The **status.status** field is empty if no failures are reported and not all nodes have reported their status.
- The **status.status** field is set to **success** if all nodes report **success**.
- The **status.mesages** field lists messages. The messages are listed by the node name by default and are prefixed with the node name.

#### 1.3.8.5. Additional BGP metrics for MetalLB

With this update, MetalLB exposes additional metrics relating to communication between MetalLB and Border Gateway Protocol (BGP) peers. For more information, see MetalLB metrics for BGP and BFD.

#### 1.3.8.6. Supporting all-multicast mode

OpenShift Container Platform now supports configuring the all-multicast mode by using the tuning CNI plugin. This update eliminates the need to grant the **NET_ADMIN** capability to the pod's Security Context Constraints (SCC), enhancing security by minimizing potential vulnerabilities for your pods.

For more information about all-multicast mode, see About all-multicast mode.

#### 1.3.8.7. Multi-network policy support for IPv6 networks

With this update, you can now create multi-network policies for IPv6 networks. For more information, see Supporting multi-network policies in IPv6 networks .

#### 1.3.8.8. Ingress Operator metrics dashboard available

With this release, Ingress networking metrics are now viewable from within the OpenShift Container Platform web console. See Ingress Operator dashboard for more information.

#### 1.3.8.9. CoreDNS filtration of ExternalName service queries for subdomains

As of OpenShift Container Platform 4.15, CoreDNS has been updated from 1.10.1 to 1.11.1.

This update to CoreDNS resolved an issue where CoreDNS would incorrectly provide a response to a query for an **ExternalName** service that shared its name with a top-level domain, such as **com** or **org**. A query for subdomains of an external service should not resolve to that external service. See the associated CoreDNS GitHub issue for more information.

#### 1.3.8.10. CoreDNS metrics deprecation and removal

As of OpenShift Container Platform 4.15, CoreDNS has been updated from 1.10.1 to 1.11.1.

This update to CoreDNS resulted in the deprecation and removal of certain metrics that have been relocated, including the metrics **coredns_forward_healthcheck_failures_total**, **coredns_forward_requests_total**, **coredns_forward_responses_total**, and **coredns_forward_request_duration_seconds**. See CoreDNS Metrics for more information.

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

OpenShift Container Platform 4.15 adds support for the following SR-IOV devices:

- Mellanox MT2910 Family [ConnectX-7]

For more information, see Supported devices.

#### 1.3.8.12. Host network configuration policy for SR-IOV network VFs (Technology Preview)

With this release, you can use the **NodeNetworkConfigurationPolicy** resource to manage host network settings for Single Root I/O Virtualization (SR-IOV) network virtual functions (VF) in an existing cluster.

For example, you can configure a host network Quality of Service (QoS) policy to manage network access to host resources by an attached SR-IOV network VF. For more information, see Node network configuration policy for virtual functions.

### 1.3.9. Registry

#### 1.3.9.1. Support for private storage endpoint on Azure

With this release, the Image Registry Operator can be leveraged to use private storage endpoints on Azure. You can use this feature to seamlessly configure private endpoints for storage accounts when OpenShift Container Platform is deployed on private Azure clusters, so that users can deploy the image registry without exposing public-facing storage endpoints.

For more information, see the following sections:

- Configuring a private storage endpoint on Azure
- Optional: Preparing a private Microsoft Azure cluster for a private image registry

### 1.3.10. Storage

#### 1.3.10.1. Recovering volume groups from the previous LVM Storage installation

With this release, the **LVMCluster** custom resource (CR) provides support for recovering volume groups from the previous LVM Storage installation. If the **deviceClasses.name** field is set to the name of a volume group from the previous LVM Storage installation, LVM Storage recreates the resources related to that volume group in the current LVM Storage installation. This simplifies the process of using devices from the previous LVM Storage installation through the reinstallation of LVM Storage.

For more information, see Creating a Logical Volume Manager cluster on a worker node .

#### 1.3.10.2. Support for wiping the devices in LVM Storage

This feature provides a new optional field **forceWipeDevicesAndDestroyAllData** in the **LVMCluster** custom resource (CR) to force wipe the selected devices. Before this release, wiping the devices required you to manually access the host. With this release, you can force wipe the disks without manual intervention. This simplifies the process of wiping the disks.

> WARNING
>
> If **forceWipeDevicesAndDestroyAllData** is set to **true**, LVM Storage wipes all previous data on the devices. You must use this feature with caution.

For more information, see Creating a Logical Volume Manager cluster on a worker node .

### 1.3.10.3. Support for deploying LVM Storage on multi-node clusters

This feature provides support for deploying LVM Storage on multi-node clusters. Previously, LVM Storage only supported single-node configurations. With this release, LVM Storage supports all of the OpenShift Container Platform deployment topologies. This enables provisioning of local storage on multi-node clusters.

> WARNING
>
> LVM Storage only supports node local storage on multi-node clusters. It does not support storage data replication mechanism across nodes. When using LVM Storage on multi-node clusters, you must ensure storage data replication through active or passive replication mechanisms to avoid a single point of failure.

For more information, see Deploying LVM Storage.

### 1.3.10.4. Integrating RAID arrays with LVM Storage

This feature provides support for integrating RAID arrays that are created using the **mdadm** utility with LVM Storage. The **LVMCluster** custom resource (CR) provides support for adding paths to the RAID arrays in the **deviceSelector.paths** field and the **deviceSelector.optionalPaths** field.

For more information, see Integrating software RAID arrays with LVM Storage .

### 1.3.10.5. FIPS compliance support for LVM Storage

With this release, LVM Storage is designed for Federal Information Processing Standards (FIPS). When LVM Storage is installed on OpenShift Container Platform in FIPS mode, LVM Storage uses the RHEL cryptographic libraries that have been submitted to NIST for FIPS 140-3 validation only on the x86_64 architecture.

### 1.3.10.6. Retroactive default StorageClass assignment is generally available

Before OpenShift Container Platform 4.13, if there was no default storage class, persistent volumes claims (PVCs) that were created that requested the default storage class remained stranded in the pending state indefinitely, unless you manually delete and recreate them. Starting with OpenShift Container Platform 4.14, as a Technology Preview feature, the default storage class is assigned to these PVCs retroactively so that they do not remain in the pending state. After a default storage class is created, or one of the existing storage classes is declared the default, these previously stranded PVCs are assigned to the default storage class. This feature is now generally available.

For more information, see Absent default storage class .

#### 1.3.10.7. Local Storage Operator option to facilitate removing existing data on local volumes is generally available

This feature provides an optional field, **forceWipeDevicesAndDestroyAllData** defining whether or not to call **wipefs**, which removes partition table signatures (magic strings) making the disk ready to use for Local Storage Operator (LSO) provisioning. No other data besides signatures is erased. This feature is now generally available. Note that this feature does not apply to **LocalVolumeSet** (LVS).

For more information, see Provisioning local volumes by using the Local Storage Operator .

#### 1.3.10.8. Detach CSI volumes after non-graceful node shutdown is generally available

Starting with OpenShift Container Platform 4.13, Container Storage Interface (CSI) drivers can automatically detach volumes when a node goes down non-gracefully as a Technology Preview feature. When a non-graceful node shutdown occurs, you can then manually add an out-of-service taint on the node to allow volumes to automatically detach from the node. This feature is now generally available.

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

#### 1.3.10.9. Shared VPC is supported for the GCP Filestore CSI Driver Operator as generally available

Shared virtual private cloud (VPC) for the Google Compute Platform (GCP) Container Storage Interface (CSI) Driver Operator is now supported as a generally available feature. Shared VPC simplifies network management, allows consistent network policies, and provides a centralized view of network resources.

For more information, see Creating a storage class for GCP Filestore Storage .

#### 1.3.10.10. User-Managed encryption supports IBM VPC Block storage as generally available

The user-managed encryption feature allows you to provide keys during installation that encrypt OpenShift Container Platform node root volumes, and enables all managed storage classes to use the specified encryption key to encrypt provisioned storage volumes. This feature was introduced in OpenShift Container Platform 4.13 for Google Cloud Platform (GCP) persistent disk (PD) storage, Microsoft Azure Disk, and Amazon Web Services (AWS) Elastic Block storage (EBS), and is now supported on IBM Virtual Private Cloud (VPC) Block storage.

#### 1.3.10.11. SELinux relabeling using mount options (Technology Preview)

Previously, when SELinux was enabled, the persistent volume’s (PV’s) files were relabeled when attaching the PV to the pod, potentially causing timeouts when the PVs contained many files, as well as overloading the storage backend.

In OpenShift Container Platform 4.15, for Container Storage Interface (CSI) drivers that support this

In OpenShift Container Platform 4.15, for Container Storage Interface (CSI) driver that support this feature, the driver will mount the volume directly with the correct SELinux labels, eliminating the need to recursively relabel the volume, and pod startup can be significantly faster.

This feature is supported with Technology Preview status.

If the following conditions are true, the feature is enabled by default:

- The CSI driver that provides the volume has support for this feature with **seLinuxMountSupported: true** in its CSIDriver instance. The following CSI drivers that are shipped as part of OpenShift Container Platform announce SELinux mount support:
  - AWS Elastic Block Storage (EBS)
  - Azure Disk
  - Google Compute Platform (GCP) persistent disk (PD)
  - IBM Virtual Private Cloud (VPC) Block
  - OpenStack Cinder
  - VMware vSphere
- The pod that uses the persistent volume has full SELinux label specified in its **spec.securityContext** or **spec.containers[*].securityContext** by using **restricted** SCC.
- Access mode set to **ReadWriteOncePod** for the volume.

## 1.3.11. Oracle® Cloud Infrastructure

### 1.3.11.1. Using the Assisted Installer to install a cluster on OCI (Technology Preview)

You can run cluster workloads on Oracle® Cloud Infrastructure (OCI) infrastructure that supports dedicated, hybrid, public, and multiple cloud environments. Both Red Hat and Oracle test, validate, and support running OCI in an OpenShift Container Platform cluster on OCI.

OCI provides services that can meet your needs for regulatory compliance, performance, and cost-effectiveness. You can access OCI Resource Manager configurations to provision and configure OCI resources.

For more information, see Using the Assisted Installer to install a cluster on OCI .

### 1.3.11.2. Using the Agent-based Installer to install a cluster on OCI (Technology Preview)

You can use the Agent-based Installer to install a cluster on Oracle® Cloud Infrastructure (OCI), so that you can run cluster workloads on infrastructure that supports dedicated, hybrid, public, and multiple cloud environments.

The Agent-based installer provides the ease of use of the Assisted Installation service, but with the capability to install a cluster in either a connected or disconnected environment.

OCI provides services that can meet your regulatory compliance, performance, and cost-effectiveness needs. OCI supports 64-bit **x86** instances and 64-bit ARM instances.

For more information, see Using the Agent-based Installer to install a cluster on OCI .

### 1.3.12. Operator lifecycle

#### 1.3.12.1. Operator Lifecycle Manager (OLM) 1.0 (Technical Preview)

Operator Lifecycle Manager (OLM) has been included with OpenShift Container Platform 4 since its initial release. OpenShift Container Platform 4.14 introduced components for a next-generation iteration of OLM as a Technology Preview feature, known during this phase as *OLM 1.0*. This updated framework evolves many of the concepts that have been part of previous versions of OLM and adds new capabilities.

During this Technology Preview phase of OLM 1.0 in OpenShift Container Platform 4.15, administrators can explore the following features added to this release:

**Support for version ranges**

You can specify a version range by using a comparison string in an Operator or extension's custom resource (CR). If you specify a version range in the CR, OLM 1.0 installs or updates to the latest version of the Operator that can be resolved within the version range. For more information, see Updating an Operator and Support for version ranges

**Performance improvements in the Catalog API**

The Catalog API now uses an HTTP service to serve catalog content on the cluster. Previously, custom resource definitions (CRDs) were used for this purpose. The change to using an HTTP service to serve catalog content reduces the load on the Kubernetes API server. For more information, see Finding Operators to install from a catalog .

NOTE

For OpenShift Container Platform 4.15, documented procedures for OLM 1.0 are CLI-based only. Alternatively, administrators can create and view related objects in the web console by using normal methods, such as the **Import YAML** and **Search** pages. However, the existing **OperatorHub** and **Installed Operators** pages do not yet display OLM 1.0 components.

For more information, see About Operator Lifecycle Manager 1.0.

#### 1.3.12.2. Deprecation schema for Operator catalogs

The optional **olm.deprecations** schema defines deprecation information for Operator packages, bundles, and channels in a file-based catalog. Operator authors can use this schema in a **deprecations.yaml** file to provide relevant messages about their Operators, such as support status and recommended upgrade paths, to users running those Operators from a catalog. After the Operator is installed, any specified messages can be viewed as status conditions on the related **Subscription** object.

For information on the **olm.deprecations** schema, see Operator Framework packaging format.

### 1.3.13. Operator development

#### 1.3.13.1. Token authentication for Operators on cloud providers: Azure AD Workload Identity

With this release, Operators managed by Operator Lifecycle Manager (OLM) can support token authentication when running on Azure clusters configured for Azure AD Workload Identity. Updates to the Cloud Credential Operator (CCO) enable semi-automated provisioning of certain short-term credentials, provided that the Operator author has enabled their Operator to support Azure AD Workload Identity.

For more information, see CCO-based workflow for OLM-managed Operators with Azure AD Workload Identity.

## 1.3.14. Builds

## 1.3.15. Machine Config Operator

### 1.3.15.1. Improved MCO state reporting by node (Technology Preview)

With this release, you can monitor updates for individual nodes as a Technology Preview. For more information, see Checking machine config node status.

## 1.3.16. Machine API

### 1.3.16.1. Defining a VMware vSphere failure domain for a control plane machine set (Technology Preview)

By using a vSphere failure domain resource, you can use a control plane machine set to deploy control plane machines on hardware that is separate from the primary VMware vSphere infrastructure. A control plane machine set helps balance control plane machines across defined failure domains to provide fault tolerance capabilities to your infrastructure.

For more information, see Sample VMware vSphere failure domain configuration and Supported cloud providers.

## 1.3.17. Nodes

### 1.3.17.1. The /dev/fuse device enables faster builds on unprivileged pods

You can configure unprivileged pods with the **/dev/fuse** device to access faster builds.

For more information, see Accessing faster builds with /dev/fuse.

### 1.3.17.2. Log linking is enabled by default

Beginning with OpenShift Container Platform 4.15, log linking is enabled by default. Log linking gives you access to the container logs for your pods.

### 1.3.17.3. ICSP, IDMS, and ITMS are now compatible

**ImageContentSourcePolicy** (ICSP), **ImageDigestMirrorSet** (IDMS), and **ImageTagMirrorSet** (ITMS) objects now function in the same cluster at the same time. Previously, to use the newer IDMS or ITMS objects, you needed to delete any ICSP objects. Now, you can use any or all of the three types of objects to configure repository mirroring after the cluster is installed. For more information, see Understanding image registry repository mirroring.

IMPORTANT

Using an ICSP object to configure repository mirroring is a deprecated feature. 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.

### 1.3.18. Monitoring

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

#### 1.3.18.1. Updates to monitoring stack components and dependencies

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

- Alertmanager to 0.26.0
- kube-state-metrics to 2.10.1
- node-exporter to 1.7.0
- Prometheus to 2.48.0
- Prometheus Adapter to 0.11.2
- Prometheus Operator to 0.70.0
- Thanos Querier to 0.32.5

#### 1.3.18.2. Changes to alerting rules

NOTE

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

- The **NodeClockNotSynchronising** and **NodeClockSkewDetected** alerting rules are now disabled when the Precision Time Protocol (PTP) is in use.

#### 1.3.18.3. New Metrics Server component to access the Metrics API (Technology Preview)

This release introduces a Technology Preview option to add a Metrics Server component to the in-cluster monitoring stack. As a Technology Preview feature, Metrics Server is automatically installed instead of Prometheus Adapter if the **FeatureGate** custom resource is configured with the **TechPreviewNoUpgrade** option. If installed, Metrics Server collects resource metrics and exposes them in the **metrics.k8s.io** Metrics API service for use by other tools and APIs. Using Metrics Server instead of Prometheus Adapter 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 and Enabling features using feature gates.

#### 1.3.18.4. New feature to send exemplar data to remote write storage for user-defined projects

User-defined projects can now use remote write to send exemplar data scraped by Prometheus to remote storage. To use this feature, configure remote write using the **sendExemplars** option in the **RemoteWriteSpec** resource. For more information, see RemoteWriteSpec in the config map API reference for the Cluster Monitoring Operator.

#### 1.3.18.5. Improved alert querying for user-defined projects

Applications in user-defined projects now have API access to query alerts for application namespaces via the rules tenancy port for Thanos Querier. You can now construct queries that access the **/api/v1/alerts** endpoint via port 9093 for Thanos Querier, provided that the HTTP request contains a **namespace** parameter. In previous releases, the rules tenancy port for Thanos Querier did not provide API access to the **/api/v1/alerts** endpoint.

#### 1.3.18.6. Prometheus updated to tolerate jitters at scrape time

The default Prometheus configuration in the monitoring stack has been updated so that jitters are tolerated at scrape time. For monitoring deployments that have shown sub-optimal chunk compression for data storage, this update helps to optimize data compression, thereby reducing the disk space used by the time series database in these deployments.

#### 1.3.18.7. Improved staleness handling for the kubelet service monitor

Staleness handling for the kubelet service monitor 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. As a result, the dedicated service monitors feature has been disabled and is now deprecated, and setting the **DedicatedServiceMonitors** resource to **enabled** has no effect.

#### 1.3.18.8. Improved ability to troubleshoot reports of tasks failing

The reasons provided when tasks fail in monitoring components are now more granular so that you can more easily pinpoint whether a reported failure originated in components deployed in the **openshift-monitoring** namespace or in the **openshift-user-workload-monitoring** namespace. If the Cluster Monitoring Operator (CMO) reports task failures, the following reasons have been added to identify where the failures originated:

- The **PlatformTasksFailed** reason indicates failures that originated in the **openshift-monitoring** namespace.
- The **UserWorkloadTasksFailed** reason indicates failures that originated in the **openshift-user-workload-monitoring** namespace.

### 1.3.19. 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.

### 1.3.20. Scalability and performance

You can set the control plane hardware speed to one of **"Standard"**, **"Slower"**, or the default, **""**, which allows the system to decide which speed to use. This is a Technology Preview feature. For more information, see Setting tuning parameters for etcd.

#### 1.3.20.1. Hub-side templating for PolicyGenTemplate CRs

You can manage the configuration of fleets of clusters by using hub templates to populate the group and site values in the generated policies that get applied to managed clusters. By using hub templates in group and site **PolicyGenTemplate** (PGT) CRs you can significantly reduce the number of policies on the hub cluster. For more information, see Specifying group and site configuration in group PolicyGenTemplate CRs with hub templates.

#### 1.3.20.2. Node Tuning Operator (NTO)

The Cloud-native Network Functions (CNF) tests image for latency tests, **cnf-tests**, has been simplified. The new image has three tests for latency measurements. The tests run by default and require a performance profile configured on the cluster. If no performance profile is configured, the tests do not run.

The following variables are no longer recommended for use:

- **ROLE_WORKER_CNF**
- **NODES_SELECTOR**
- **PERF_TEST_PROFILE**
- **FEATURES**
- **LATENCY_TEST_RUN**
- **DISCOVERY_MODE**

To generate the **junit** report, the **--ginkgo.junit-report** flag replaces **--junit**.

For more information, see Performing latency tests for platform verification .

#### 1.3.20.3. Bare Metal Operator

For OpenShift Container Platform 4.15, when the Bare Metal Operator removes a host from the cluster it also powers off the host. This enhancement streamlines hardware maintenance and management.

## 1.4. NOTABLE TECHNICAL CHANGES

OpenShift Container Platform 4.15 introduces the following notable technical changes.

### Cluster metrics ports secured

With this release, the ports that serve metrics for the Cluster Machine Approver Operator and Cluster Cloud Controller Manager Operator use the Transport Layer Security (TLS) protocol for additional security. (OCPCLOUD-2272, OCPCLOUD-2271)

### Cloud controller manager for Google Cloud Platform

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

This release introduces the General Availability of using a cloud controller manager for Google Cloud Platform.

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

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

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

### Future restricted enforcement for pod security admission

Currently, pod security violations are shown as warnings in the audit logs without resulting in the rejection of the pod.

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

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

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

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

### Secrets are no longer automatically generated when the integrated OpenShift image registry is disabled

If you disable the **ImageRegistry** cluster capability or if you disable the integrated OpenShift image registry in the Cluster Image Registry Operator's configuration, a service account token secret and image pull secret are no longer generated for each service account.

For more information, see Automatically generated secrets.

### Open Virtual Network Infrastructure Controller default range

Previously, the IP address range **168.254.0.0/16** was the default IP address range that the Open Virtual Network Infrastructure Controller used for the transit switch subnet. With this update, the Controller uses **100.88.0.0/16** as the default IP address range. Do not use this IP range in your production infrastructure network. (OCPBUGS-20178)

### Introduction of HAProxy no strict-limits variable

The transition to HAProxy 2.6 included enforcement for the **strict-limits** configuration, which resulted in unrecoverable errors when **maxConnections** requirements could not be met. The **strict-limits** setting is not configurable by end users and remains under the control of the HAProxy template.

This release introduces a configuration adjustment in response to the migration to the **maxConnections** issues. Now, the HAProxy configuration switches to using **no strict-limits**. As a result, HAProxy no longer fatally exits when the **maxConnection** configuration cannot be satisfied. Instead, it emits warnings and continues running. When **maxConnection** limitations cannot be met, warnings such as the following examples might be returned:

- **[WARNING] (50) : [/usr/sbin/haproxy.main()] Cannot raise FD limit to 4000237, limit is 1048576.**

- **[ALERT] (50) : [/usr/sbin/haproxy.main()] FD limit (1048576) too low for maxconn=2000000/maxsock=4000237. Please raise 'ulimit-n' to 4000237 or more to avoid any trouble.**

To resolve these warnings, we recommend specifying **-1** or **auto** for the **maxConnections** field when tuning an IngressController. This choice allows HAProxy to dynamically calculate the maximum value based on the available resource limitations in the running container, which eliminates these warnings. (OCPBUGS-21803)

### The deployer service account is no longer created if the DeploymentConfig cluster capability is disabled

If you disable the **DeploymentConfig** cluster capability, the **deployer** service account and its corresponding secrets are no longer created.

For more information, see DeploymentConfig capability.

### Must-gather storage limit default

A default limit of 30% of the storage capacity of the node for the container has been added for data collected by the **oc adm must-gather** command. If necessary, you can use the **--volume-percentage** flag to adjust the default storage limit.

For more information, see Changing the must-gather storage limit.

### Agent-based Installer interactive network configuration displays on the serial console

With this update, when an Agent ISO is booted on a server with no graphical console, interactive network configuration is possible on the serial console. Status displays are paused on all other consoles while the interactive network configuration is active. Previously, the displays could be shown only on a graphical console. (OCPBUGS-19688)

## 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 4.15, refer to the table below. Additional details for more functionality that has been deprecated and removed are listed after the table.

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

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

### Operator lifecycle and development deprecated and removed features

Table 1.6. Operator lifecycle and development deprecated and removed tracker

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| SQLite database format for Operator catalogs | Deprecated | Deprecated | Deprecated |

### Images deprecated and removed features

**Table 1.7. Images deprecated and removed tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| **ImageChangesInProgress** condition for Cluster Samples Operator | Deprecated | Deprecated | Deprecated |
| **MigrationInProgress** condition for Cluster Samples Operator | Deprecated | Deprecated | Deprecated |

### Monitoring deprecated and removed features

**Table 1.8. Monitoring deprecated and removed tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| **dedicatedServiceMonitors** setting that enables dedicated service monitors for core platform monitoring | General Availability | General Availability | Deprecated |

### Installation deprecated and removed features

**Table 1.9. Installation deprecated and removed tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| OpenShift SDN network plugin | General Availability | Deprecated | Removed [1] |
| **--cloud** parameter for **oc adm release extract** | General Availability | Deprecated | Deprecated |
| CoreDNS wildcard queries for the **cluster.local** domain | Deprecated | Deprecated | Deprecated |
| **compute.platform.openstack.rootVolume.type** for RHOSP | General Availability | Deprecated | Deprecated |
| **controlPlane.platform.openstack.rootVolume.type** for RHOSP | General Availability | Deprecated | Deprecated |
| **ingressVIP** and **apiVIP** settings in the **install-config.yaml** file for installer-provisioned infrastructure clusters | Deprecated | Deprecated | Deprecated |
| **platform.gcp.licenses** for Google Cloud Provider | Deprecated | Removed | 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 | 4.13 | 4.14 | 4.15 |
|---|---|---|---|

### Storage deprecated and removed features

**Table 1.11. Storage deprecated and removed tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Persistent storage using FlexVolume | Deprecated | Deprecated | Deprecated |

### Networking deprecated and removed features

**Table 1.12. Networking deprecated and removed tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Kuryr on RHOSP | Deprecated | Deprecated | Removed |
| OpenShift SDN network plugin | General Availability | Deprecated | Deprecated |

### Web console deprecated and removed features

**Table 1.13. Web console deprecated and removed tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|

### Node deprecated and removed features

**Table 1.14. Node deprecated and removed tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| **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 |

### OpenShift CLI (oc) deprecated and removed features

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| **--include-local-oci-catalogs** parameter for **oc-mirror** | General Availability | Removed | Removed |
| **--use-oci-feature** parameter for **oc-mirror** | Deprecated | Removed | Removed |

### Workloads deprecated and removed features

**Table 1.15. Workloads deprecated and removed tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| **DeploymentConfig** objects | General Availability | Deprecated | Deprecated |

### Bare metal monitoring

**Table 1.16. Bare Metal Event Relay Operator tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Bare Metal Event Relay Operator | Technology Preview | Technology Preview | Deprecated |

## 1.5.1. Deprecated features

### 1.5.1.1. Deprecation of the OpenShift SDN network plugin

OpenShift SDN CNI is deprecated as of OpenShift Container Platform 4.14. As of OpenShift Container Platform 4.15, the network plugin is not an option for new installations. In a subsequent future release, the OpenShift SDN network plugin is planned to be removed and no longer supported. Red Hat will provide bug fixes and support for this feature until it is removed, but this feature will no longer receive enhancements. As an alternative to OpenShift SDN CNI, you can use OVN Kubernetes CNI instead.

### 1.5.1.2. Bare Metal Event Relay Operator

The Bare Metal Event Relay Operator is deprecated. The ability to monitor bare-metal hosts by using the Bare Metal Event Relay Operator will be removed in a future OpenShift Container Platform release.

### 1.5.1.3. Dedicated service monitors for core platform monitoring

With this release, the dedicated service monitors feature for core platform monitoring is deprecated. The ability to enable dedicated service monitors by configuring the **dedicatedServiceMonitors** setting in the **cluster-monitoring-config** config map object in the **openshift-monitoring** namespace will be removed in a future OpenShift Container Platform release. 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.

#### 1.5.1.4. oc registry info command is deprecated

With this release, the experimental **oc registry info** command is deprecated.

To view information about the integrated OpenShift image registry, run **oc get imagestream -n openshift** and check the **IMAGE REPOSITORY** column.

### 1.5.2. Removed features

#### 1.5.2.1. Removal of the OPENSHIFT_DEFAULT_REGISTRY

OpenShift Container Platform 4.15 has removed support for the **OPENSHIFT_DEFAULT_REGISTRY** variable. This variable was primarily used to enable backwards compatibility of the internal image registry for earlier setups. The **REGISTRY_OPENSHIFT_SERVER_ADDR** variable can be used in its place.

#### 1.5.2.2. Installing clusters on Red Hat OpenStack Platform (RHOSP) with Kuryr is removed

As of OpenShift Container Platform 4.15, support for installing clusters on RHOSP with kuryr is removed.

### 1.5.3. Future Kubernetes API removals

The next minor release of OpenShift Container Platform is expected to use Kubernetes 1.29. Kubernetes 1.29 has removed a deprecated API.

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

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

## 1.6. BUG FIXES

**API Server and Authentication**

- Previously, the **termination.log** in the kube-apiserver log folder had invalid permissions due to settings in the upstream library. With this release, the upstream library was updated and the **terminate.log** now has the expected permissions. (OCPBUGS-11856)

- Previously, the Cluster Version Operator (CVO) enabled a capability if the existing manifest got the capability annotation after an upgrade. This caused the console to be enabled after upgrading to OpenShift Container Platform 4.14 for users who had previously disabled the console capability. With this release, the unnecessary console capability was removed from the existing manifest and the console capability is no longer implicitly enabled. (OCPBUGS-20331)

- Previously, when the **openshift-kube-controller-manager** namespace was deleted, the following error was logged repeatedly: **failed to synchronize namespace**. With this release, the error is no longer logged when the **openshift-kube-controller-manager** namespace is deleted. (OCPBUGS-17458)

**Bare Metal Hardware Provisioning**

- Previously, deploying IPv6-only hosts from a dual-stack GitOps ZTP hub prevented the correct callback URL from being passed to the baseboard management controller (BMC).

Consequently, an IPv4 URL was passed unconditionally. This issue has been resolved, and the IP version of the URL now depends on the IP version of the BMC address. (OCPBUGS-23759)

- Previously, the Bare Metal Operator (BMO) container had a **hostPort** specified as **60000**, but the **hostPort** was not actually in use despite the specification. As a result, other services could not use port 60000. This fix removes the **hostPort** specification from the container configuration. Now, port 60000 is available for use by other services. (OCPBUGS-18788)

- Previously, the Cluster Baremetal Operator (CBO) failed when it checked the infrastructure **platformStatus** field and returned **nil**. With OpenShift Container Platform 4.15, the CBO has been updated so that it checks and returns a blank value when **apiServerInternalIPs** returns **nil**, which resolves this issue. (OCPBUGS-17589)

- Previously, the **inspector.ipxe** configuration 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, which supplied a malformed IPv6 host header since it did not contain brackets.
  With OpenShift Container Platform 4.15, the **inspector.ipxe** configuration has been updated to use the **IRONIC_URL_HOST** variable, which accounts for IPv6 addresses and resolves the issue. (OCPBUGS-27060)

- Previously, there was a bug when attempting to deploy OpenShift Container Platform on a new bare metal host using RedFish Virtual Media with Cisco UCS hardware. This bug blocked bare metal hosts from new provisions, because Ironic was unable to find a suitable virtual media device. With this update, Ironic does more checks in all available virtual media devices. As a result, Cisco UCS hardware can now be provisioned when using RedFish Virtual Media. (OCPBUGS-23105)

- Previously, when installing OpenShift Container Platform with the **bootMode** field set to **UEFISecureBoot** on a node where the **secureBoot** field was set to **disabled**, the installation program failed to start. With this update, Ironic has been updated so that you can install OpenShift Container Platform with **secureBoot** set to **enabled**. (OCPBUGS-9303)

### Builds

- Previously, timestamps were not preserved when copying contents between containers. With this release, the **-p** flag is added to the **cp** command to allow timestamps to be preserved. (OCPBUGS-22497)

### Cloud Compute

- Previously, an error in the parsing of taints from the **MachineSet** spec meant that the autoscaler could not account for any taint set directly on the spec. Consequently, when relying on the **MachineSet** taints for scaling from zero, the taints from the spec were not considered, which could cause incorrect scaling decisions. With this update, parsing issues within the scale from zero logic have been resolved. As a result, auto scaler can now scale up correctly and identify taints that would prevent workloads from scheduling. (OCPBUGS-27750)

- Previously, an Amazon Web Services (AWS) code that provided image credentials was removed from the kubelet in OpenShift Container Platform 4.14. Consequently, pulling images from Amazon Elastic Container Registry (ECR) failed without a specified pull secret, because the kubelet could no longer authenticate itself and pass credentials to the container runtime. With this update, a separate credential provider has been configured, which is now responsible for providing ECR credentials for the kubelet. As a result, the kubelet can now pull private images from ECR. (OCPBUGS-27486)

- Previously when deploying a hosted control plane (HCP) KubeVirt cluster the **--node-selector** command, the node selector was not applied to the **kubevirt-cloud-controller-manager** pods within the HCP namespace. Consequentially, you could not pin the entire HCP pods to specific nodes. With this update, this issue has been fixed. (OCPBUGS-27071)

- Previously, the default virtual machine (VM) type for the Microsoft Azure load balancer was changed from **Standard** to **VMSS**. Consequently, the service type load balancer could not attach standard VMs to load balancers. This update reverts these changes to the previous configuration to maintain compatibility with OpenShift Container Platform deployments. As a result, load balancer attachments are now more consistent. (OCPBUGS-26210)

- Previously, deployments on RHOSP nodes with additional ports with the **enable_port_security** field set to **false** were prevented from creating **LoadBalancer** services. With this update, this issue is resolved. (OCPBUGS-22246)

- Previously worker nodes on Red Hat OpenStack Platform (RHOSP) were named with domain components if the Nova metadata service was unavailable the first time the worker nodes booted. OpenShift Container Platform expects the node names to be the same as the Nova instance. The name discrepancy caused the nodes' certificate request to be rejected and the nodes could not join the cluster. With this update, the worker nodes will wait and retry the metadata service indefinitely on first boot ensuring the nodes are correctly named. (OCPBUGS-22200)

- Previously, the cluster autoscaler crashed when used with nodes that have Container Storage Interface (CSI) storage. The issue is resolved in this release. (OCPBUGS-23096)

- Previously, in certain proxied environments, the Amazon Web Services (AWS) metadata service might not have been present on initial startup, and might have only been available shortly after startup. The kubelet hostname fetching did not account for this delay and, consequently, the node would fail to boot because it would not have a valid hostname. This update ensures that the hostname fetching script retries on failure for some time. As a result, inaccessibility of the metadata service is tolerated for a short period of time. (OCPBUGS-20369)

- In OpenShift Container Platform version 4.14 and later, there is a known issue that causes installation of Microsoft Azure Stack Hub to fail. Microsoft Azure Stack Hub clusters that are upgraded to 4.14 or later might encounter load balancer configuration issues as nodes scale up or down. Installing or upgrading to 4.14 in Microsoft Azure Stack Hub environments is not recommended until this issue is resolved. (OCPBUGS-20213)

- Previously, some conditions during the startup process of the Cluster Autoscaler Operator caused a lock that prevented the Operator from successfully starting and marking itself available. As a result, the cluster became degraded. The issue is resolved with this release. (OCPBUGS-18954)

- Previously, attempting to perform a Google Cloud Platform XPN internal cluster installation failed when control nodes were added to a second internal instance group. This bug has been fixed. (OCPBUGS-5755)

- Previously, the termination handler prematurely exited before marking a node for termination. This condition occurred based on the timing of when the termination signal was received by the controller. With this release, the possibility of early termination is accounted for by introducing an additional check for termination. (OCPBUGS-2117)

### Cloud Credential Operator

- Previously, the Cloud Credential Operator utility (**ccoctl**) created custom GCP roles at the cluster level, so each cluster contributed to the quota limit on the number of allowed custom roles. Because of GCP deletion policies, deleted custom roles continue to contribute to the quota limit for many days after they are deleted. With this release, custom roles are added at the project level instead of the cluster level to reduce the total number of custom roles created. Additionally, an option to clean up custom roles is now available when deleting the GCP resources that the **ccoctl** utility creates during installation. These changes can help avoid reaching the quota limit on the number of allowed custom roles. (OCPBUGS-28850)

- Previously, when the Cloud Credential Operator (CCO) was in default mode, CCO used an incorrect client for root credential queries. The CCO failed to find the intended secret and wrongly reported a **credsremoved** mode in the **cco_credentials_mode** metric. With this release, the CCO now uses the correct client to ensure accurate reporting of the **cco_credentials_mode** metric. (OCPBUGS-26510)

- Previously, buckets created by running the **ccoctl azure create** command were prohibited from allowing public blob access due to a change in the default behavior of Microsoft Azure buckets. With this release, buckets created by running the **ccoctl azure create** command are explicitly set to allow public blob access. (OCPBUGS-22369)

- Previously, an Azure Managed Identity role was omitted from the Cloud Controller Manager service account. As a result, the Cloud Controller Manager could not manage service type load balancers in environments deployed to existing VNets with a private publishing method. With this release, the missing role was added to the Cloud Credential Operator utility (**ccoctl**) and Azure Managed Identity installations into an existing VNet with private publishing is possible. (OCPBUGS-21745)

- Previously, the Cloud Credential Operator did not support updating the vCenter server value in the root secret **vshpere-creds** that is stored in the **kube-system** namespace. As a result, attempting to update this value caused both the old and new values to exist because the component secrets were not synchronized correctly. With this release, the Cloud Credential Operator resets the secret data during synchronization so that updating the vCenter server value is supported. (OCPBUGS-20478)

- Previously, the Cloud Credential Operator utility (**ccoctl**) failed to create AWS Security Token Service (STS) resources in China regions because the China region DNS suffix **.amazonaws.com.cn** differs from the suffix **.amazonaws.com** that is used in other regions. With this release, **ccoctl** can detect the correct DNS suffix and use it to create the required resources. (OCPBUGS-13597)

### Cluster Version Operator

- The Cluster Version Operator (CVO) continually retrieves update recommendations and evaluates known conditional update risks against the current cluster state. Previously, failing risk evaluations blocked the CVO from fetching new update recommendations. When the risk evaluations were failing because the update recommendation service served a poorly-defined update risk, this issue could prevent the CVO from noticing the update recommendation service serving an improved risk declaration. With this release, the CVO continues to poll the update recommendation service regardless of whether update risks are successfully evaluated or not. (OCPBUGS-25949)

### Developer Console

- Previously, **BuildRun** logs were not visible in the **Logs** Tab of the BuildRun due to the 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 for both v1alpha1 and v1beta1 versions of the builds Operator. (OCPBUGS-29283)

- Previously, the console UI failed when a **Task** in the Pipeline Builder that was previously installed from the **ArtifactHub** was selected and an error page displayed. With this update, the console UI no longer expects optional data and the console UI no longer fails. (OCPBUGS-24001)

- Previously, the **Edit Build** and **BuildRun** options in the **Actions** menu of the Shipwright Plugin did not allow you to edit in the YAML tab. With this update, you can edit in the YAML tab. (OCPBUGS-23164)

- Previously, the console searched only for the file name **Dockerfile** in a repository to identify the repository suitable for the **Container** strategy in the Import Flows. Since other containerization tools are available, support for the **Containerfile** file name is now suitable for the **Container** strategy. (OCPBUGS-22976)

- Previously, when an unauthorized user opened a link to the console that contains path and query parameters, and they were redirected to a login page, the query parameters did not restore after the login was successful. As a result, the user needed to restore the search or click the link to the console again. With this update, the latest version saves and restores the query parameters similar to the path. (OCPBUGS-22199)

- Previously, when navigating to the **Create Channel** page from the **Add** or **Topology** view, the default name as **Channel** is present, but the **Create** button is disabled with **Required** showing under the name field. With this update, if the default channel name is added then the **Required** message will not display when clicking the **Create** button. (OCPBUGS-19783)

- Previously, there were similar options to choose from when using the quick search function. With this update, the **Source-to-image** option is differentiated from the **Samples** option in the **Topology** quick search. (OCPBUGS-18371)

- Previously, when {serverless-product-name} Operator was installed and the Knative (Kn) serving instance had not been created, then when navigating to the **Global configuration** page from **Administration → Cluster Settings** and clicking **Knative-serving** a **404 page not found** error was displayed. With this update, before adding **Knative-serving** to the **Global configuration**, a check is in place to determine if a Knative serving instance is created. (OCPBUGS-18267)

- Previously there was an issue with the **Edit Knative Service** form that prevented users from editing the Knative service they previously created. With this update, you can edit a Knative service that was previously created. (OCPBUGS-6513)

#### etcd Cluster Operator

- Previously, the **cluster-backup.sh** script cached the **etcdctl** binary on the local machine indefinitely, making updates impossible. With this update, the **cluster-backup.sh** script pulls the latest **etcdctl** binary each time it is run. (OCPBUGS-19052)

#### Hosted Control Plane

- Previously, when using a custom Container Network Interface (CNI) plugin in a hosted cluster, role-based access control (RBAC) rules were configured only when you set the **hostedcluster.spec.networking.networkType** field to **Calico**. Role-based access control (RBAC) rules were not configured when you set the **hostedcluster.spec.networking.networkType** field to **Other**. With this release, RBAC rules are configured properly, when you set the **hostedcluster.spec.networking.networkType** field to **Other**. (OCPBUGS-28235)

- Previously, a node port failed to expose properly because the **ipFamilyPolicy** field was set to **SingleStack** for the **kube-apiserver** resource. With this update, if the **ipFamilyPolicy** is set to **PreferredDualStack**, node port is exposed properly. (OCPBUGS-23350)

- Previously, after configuring the Open Virtual Network (OVN) for a hosted cluster, the **cloud-network-config-controller**, **multus-admission-controller**, and`ovnkube-control-plane` resources were missing the **hypershift.openshift.io/hosted-control-plane:{hostedcluster resource namespace}-{cluster-name}** label. With this update, after configuring the Open Virtual Network (OVN) for a hosted cluster, the **cloud-network-config-controller**, **multus-admission-controller**, and`ovnkube-control-plane` resources contain the **hypershift.openshift.io/hosted-control-plane:{hostedcluster resource namespace}-{cluster-name}** label. (OCPBUGS-19370)

- Previously, after creating a hosted cluster, to create a config map, if you used a name other than **user-ca-bundle**, the deployment if the Control Plane Operator (CPO) failed. With this update, you can use unique names to create a config map. The CPO is deployed successfully. (OCPBUGS-19419)

- Previously, hosted clusters with **.status.controlPlaneEndpoint.port: 443** would mistakenly expose port 6443 for public and private routers. With this update, hosted clusters with **.status.controlPlaneEndpoint.port: 443** only expose the port 443. (OCPBUGS-20161)

- Previously, if the Kube API server is exposed by using IPv4 and IPv6, and the IP address is set in the **HostedCluster** resource, the IPv6 environment did not work properly. With this update, when the Kube API server is exposed by using IPv4 and IPv6, the IPv6 environment works properly. (OCPBUGS-20246)

- Previously, if the console Operator and Ingress pods were located on the same node, the console Operator would fail and mark the console cluster Operator as unavailable. With this release, if the console Operator and Ingress pods are located on the same node, the console Operator no longer fails. (OCPBUGS-23300)

- Previously, if uninstallation of a hosted cluster is stuck, status of the Control Plane Operator (CPO) was reported incorrectly. With this update, the status of the CPO is reported correctly. (OCPBUGS-26412)

- Previously, if you tried to override the OpenShift Container Platform version while the initial upgrade was in progress, a hosted cluster upgrade would fail. With this update, if you override the current upgrade with a new OpenShift Container Platform version, the upgrade completes successfully. (OCPBUGS-18122)

- Previously, if you update the pull secret for the hosted control planes, it did not reflect on the worker nodes immediately. With this update, when you change the pull secret, reconciliation is triggered and worker nodes are updated with a new pull secret immediately. (OCPBUGS-19834)

- Previously, the Hypershift Operator would report time series for node pools that no longer existed. With this release, the Hypershift Operator reports time series for node pools correctly. (OCPBUGS-20179)

- Previously, the **--enable-uwm-telemetry-remote-write** flag was enabled by default. This setting blocked the telemetry reconciliation. With this update, you can disable the **--enable-uwm-telemetry-remote-write** flag to allow telemetry reconciliation. ( OCPBUGS-26410)

- Previously, the control Plane Operator (CPO) failed to update the VPC endpoint service when an IAM role path ARN was provided as the additional allowed principal: **arn:aws:iam::${ACCOUNT_ID}:role/${PATH}/name** With this update, The CPO updates the

VPC endpoint service with the **arn:aws:iam::${ACCOUNT_ID}:role/${PATH}/name** allowed principal successfully. (OCPBUGS-23511)

- Previously, to customize OAuth templates, if you configured the **HostedCluster.spec.configuration.oauth** field, this setting did not reflect in a hosted cluster. With this update, you can configure the **HostedCluster.spec.configuration.oauth** field in a hosted cluster successfully. (OCPBUGS-15215)

- Previously, when deploying a hosted cluster by using a dual stack networking, by default, the **clusterIP** field was set to an IPv6 network instead of an IPv4 network. With this update, when deploying a hosted cluster by using a dual stack networking, the **clusterIP** field is set to IPv4 network by default. (OCPBUGS-16189)

- Previously, when deploying a hosted cluster, if you configure the **advertiseAddress** field in the **HostedCluster** resource, the hosted cluster deployment would fail. With this release, you can deploy a hosted cluster successfully after configuring the **advertiseAddress** field in the **HostedCluster** resource. (OCPBUGS-19746)

- Previously, when you set the **hostedcluster.spec.networking.networkType** field to **Calico** in a hosted cluster, the Cluster Network Operator did not have enough role-based access control (RBAC) permissions to deploy the **network-node-identity** resource. With this update, the **network-node-identity** resource is deployed successfully. ( OCPBUGS-23083)

- Previously, you could not update the default configuration for audit logs in a hosted cluster. Therefore, components of a hosted cluster could not generate audit logs. With this update, you can generate audit logs for components of a hosted cluster by updating the default configuration. (OCPBUGS-13348)

Image Registry

- Previously, the Image Registry pruner relied on a cluster role that was managed by the OpenShift API server. This could cause the pruner job to intermittently fail during an upgrade. Now, the Image Registry Operator is responsible for creating the pruner cluster role, which resolves the issue. (OCPBUGS-18969)

- The Image Registry Operator makes API calls to the storage account list endpoint as part of obtaining access keys. In projects with several OpenShift Container Platform clusters, this might lead to API limits being reached. As a result, **429** errors were returned when attempting to create new clusters. With this update, the time between calls has been increased from 5 minutes to 20 minutes, and API limits are no longer reached. (OCPBUGS-18469)

- Previously, the default low settings for QPS and Burst caused the image registry to return with a gateway timeout error when API server requests were not returned in an appropriate time. To resolve this issue, users had to restart the image registry. With this update, the default settings for QPS and Burst have been increased, and this issue no longer occurs. (OCPBUGS-18999)

- Previously, when creating the deployment resource for the Cluster Image Registry Operator, error handling used a pointer variable without checking if the value was **nil** first. Consequently, when the pointer value was **nil**, a panic was reported in the logs. With this update, a nil check was added so that the panic is no longer reported in the logs. (OCPBUGS-18103)

- Previously, the OpenShift Container Platform 4.14 release introduced a change that gave users the perception that their images were lost when updating from OpenShift Container Platform version 4.13 to 4.14. A change to the default internal registry caused the registry to use an incorrect path when using the Microsoft Azure object storage. With this release, the correct path is used and a job has been added to the registry operator that moves any blobs pushed to the registry that used the wrong storage path into the correct storage path, which effectively merges the two distinct storage paths into a single path.

> NOTE
>
> This fix does **not** work on Azure Stack Hub (ASH). ASH users who used OCP versions 4.14.0 through 4.14.13 when upgrading to 4.14.14+ will need to execute manual steps to move their blobs to the correct storage path.

(OCPBUGS-29525)

Installer

- Previously, installing a cluster on AWS might fail in some cases due to a validation error. With this update, the installation program produces the necessary cloud configuration object to satisfy the machine config operator. This results in the installation succeeding. (OCPBUGS-12707)

- Previously, installing a cluster on GCP using a service account attached to a VM for authentication might fail due to an internal data validation bug. With this release, the installation program has been updated to correctly validate the authentication parameters when using a service account attached to a VM. (OCPBUGS-19376)

- Previously, the vSphere connection configuration interface showed the network name instead of the cluster name in the "vCenter cluster" field. With this update, the "vCenter cluster" field has been updated to display the cluster name. (OCPBUGS-23347)

- Previously, when you authenticated with the **credentialsMode** parameter not set to **Manual** and you used the **gcloud cli** tool, the installation program retrieved Google Cloud Platform (GCP) credentials from the **osServiceAccount.json** file. This operation caused the GCP cluster installation to fail. Now, a validation check scans the **install-config.yaml** file and prompts you with a message if you did not set **credentialsMode** to **Manual**. Note that in **Manual** mode, you must edit the manifests and provide the credentials. (OCPBUGS-17757)

- Previously when you attempted to install an OpenShift Container Platform on VMware vSphere by using installer-provisioned infrastructure, a resource pool object would include a double backslash. This format caused the installation program to generate an incorrect path to network resources that in turn caused the installation operation to fail. After the installation program processed this resource pool object, the program outputted a "network not found" error message. Now, the installation program retrieves the cluster object for the purposes of joining the InventoryPath with the network name so that the program specifies the correct path to the resource pool object. (OCPBUGS-23376)

- Previously, after installing an Azure Red Hat OpenShift cluster, some cluster Operators were unavailable. This was the result of one of the cluster's load balancers not being created as part of the installation process. With this update, the load balancer is correctly created. After installing a cluster, all cluster Operators are available. (OCPBUGS-24191)

- Previously, if the VMware vSphere cluster contained an ESXi host that was offline, the installation failed with a "panic: runtime error: invalid memory address or nil pointer dereference" message. With this update, the error message states that the ESXi host is unavailable. (OCPBUGS-20350)

- Previously, if you only used the default machine configuration to specify existing AWS security groups when installing a cluster on AWS (**platform.aws.defaultMachinePlatform.additonalSecurityGroupsIDs**), the security groups were not applied to control plane machines. With this update, existing AWS security groups are correctly applied to control planes when they are specified using the default machine configuration. (OCPBUGS-20525)

- Previously, installing a cluster on AWS failed when the specified machine instance type (**platform.aws.type**) did not support the machine architecture that was specified for control plane or compute machines (**controlPlane.architecture** and **compute.architecture**). With this update, the installation program now checks to determine if the machine instance type supports the specified architecture and displays an error message if it does not. (OCPBUGS-26051)

- Previously, the installation program did not validate some configuration settings before installing the cluster. This behavior occurred when these settings were only specified in the default machine configuration (**platform.azure.defaultMachinePlatform**). As a result, the installation would succeed even if the following conditions were met:

  - An unsupported machine instance type was specified.

  - Additional functionality, such as accelerated networking or the use of Azure ultra disks, was not supported by the specified machine instance type.

  With this fix, the installation program now displays an error message that specifies the unsupported configuration. (OCPBUGS-20364)

- Previously, when installing an AWS cluster to the Secret Commercial Cloud Services (SC2S) region and specifying existing AWS security groups, the installation failed with an error that stated that the functionality was not available in the region. With this fix, the installation succeeds. (OCPBUGS-18830)

- Previously, when you specified Key Management Service (KMS) encryption keys in the **kmsKeyARN** section of the **install-config.yaml** configuration file for installing a cluster on Amazon Web Services (AWS), permission roles were not added during the cluster installation operation. With this update, after you specify the keys in the configuration file, an additional set of keys are added to the cluster so that the cluster successfully installs. If you specify the **credentialsMode** parameter in the configuration file, all KMS encryption keys are ignored. (OCPBUGS-13664)

- Previously, Agent-based installations on Oracle® Cloud Infrastructure (OCI) did not show a console displaying installation progress to users, making it more difficult to track installation progress. With this update, Agent-based installations on OCI now display installation progress on the console. (OCPBUGS-19092)

- Previously, if static networking was defined in the **install-config.yaml** or **agent-config.yaml** files for the Agent-based Installer, and an interface name was over 15 characters long, the network manager did not allow the interface to come up. With this update, interface names longer than 15 characters are truncated and the installation can proceed. (OCPBUGS-18552)

- Previously, if the user did not specify the **rendezevousIP** field in the **agent-config.yaml** file and hosts were defined in the same file with static network configuration, then the first host was designated as a rendezvous node regardless of its role. This caused the installation to fail. With this update, the Agent-based Installer prioritizes the rendezvous node search by first looking among the hosts with a **master** role and a static IP defined. If none is found, then a potential candidate is searched for through the hosts that do not have a role defined. Hosts with a static network configuration that are explicitly configured with a **worker** role are ignored. (OCPBUGS-5471)

- Previously, the Agent console application was shown during the boot process of all Agent-based installations, enabling network customizations before proceeding with the installation.

Because network configuration is rarely needed during cloud installations, this would unnecessarily slow down installations on Oracle® Cloud Infrastructure (OCI).
With this update, Agent-based installations on OCI no longer show the Agent console application and proceed more quickly. (OCPBUGS-19093)

- Previously, the Agent-based Installer enabled an external Cloud Controller Manager (CCM) by default when the platform was defined as **external**. This prevented users from disabling the external CCM when performing installations on cloud platforms that do not require one. With this update, users are required to enable an external CCM only when performing an Agent-based installation on Oracle® Cloud Infrastructure (OCI). (OCPBUGS-18455)

- Previously, the **agent wait-for** command failed to record logs in the **.openshift_install.log** file. With this update, logs are recorded in the **.openshift_install.log** file when you use the **agent wait-for** command. (OCPBUGS-5728)

- Previously, the **assisted-service** on the bootstrap machine became unavailable after the bootstrap node rebooted, preventing any communication from the **assisted-installer-controller**. This stopped the **assisted-installer-controller** from removing uninitialized taints from worker nodes, causing the cluster installation to hang waiting on cluster Operators.
With this update, the **assisted-installer-controller** can remove the uninitialized taints even if **assisted-service** becomes unavailable, and the installation can proceed. ( OCPBUGS-20049)

- Previously, the platform type was erroneously required to be lowercase in the **AgentClusterInstall** cluster manifest used by the Agent-based Installer. With this update, mixed case values are required, but the original lowercase values are now accepted and correctly translated. (OCPBUGS-19444)

- Previously, the **manila-csi-driver-controller-metrics** service had empty endpoints due to an incorrect name for the app selector. With this release the app selector name is changed to **openstack-manila-csi** and the issue is fixed. ( OCPBUGS-9331)

- Previously, the assisted installer removed the uninitialized taints for all vSphere nodes which prevented the vSphere CCM from initializing the nodes properly. This caused the vSphere CSI operator to degrade during the initial cluster installation because the node's provider ID was missing. With this release, the assisted installer checks if vSphere credentials were provided in the **install-config.yaml**. If credentials were provided, the OpenShift version is greater or equal to 4.15, and the agent installer was used, the assisted-installer and assisted-installer-controller do not remove the uninitialized taints. This means that the node's providerID and VM's UUID are properly set and the vSphere CSI operator is installed. (OCPBUGS-29485)

### Kubernetes Controller Manager

- Previously, when the **maxSurge** field was set for a daemon set and the toleration was updated, pods failed to scale down, which resulted in a failed rollout due to a different set of nodes being used for scheduling. With this release, nodes are properly excluded if scheduling constraints are not met, and rollouts can complete successfully. (OCPBUGS-19452)

### Machine Config Operator

- Previously, a misspelled environment variable prevented a script from detecting that the **node.env** file was present. This caused the contents of the **node.env** file to be overwritten after each boot, and the kubelet hostname could not be changed. With this update, the environment variable spelling is corrected and edits to the **node.env** file persist across reboots. (OCPBUGS-27307)

- Previously, the Machine Config Operator allowed user-provided certificate authority updates to be made without requiring a new machine config to trigger. Because the new write method for these updates was missing a newline character, it caused validation errors for the contents of the CA file on-disk and the Machine Config Daemon became degraded. With this release, the CA file contents are fixed, and updates proceed as expected. (OCPBUGS-25424)

- Previously, the Machine Config Operator allowed user-provided certificate authority bundle changes to be applied to the cluster without needing a machine config, to prevent disruption. Because of this, the **user-ca** bundle was not propagating to applications running on the cluster and required a reboot to see the changes take effect. With this update, the MCO now runs the **update-ca-trust** command and restarts the CRI-O service so that the new CA properly applies. (OCPBUGS-24035)

- Previously, the initial mechanism used by the Machine Config Operator to handle image registry certs would delete and create new config maps rather than patching existing ones. This caused a significant increase in API usage from the MCO. With this update, the mechanism has been updated so that it uses a JSON patch instead, thereby resolving the issue. (OCPBUGS-18800)

- Previously, the Machine Config Operator was pulling the **baremetalRuntimeCfgImage** container image multiple times: the first time to obtain node details and subsequent times to verify that the image is available. This caused issues during certificate rotation in situations where the mirror server or Quay was not available, and subsequent image pulls would fail. However, if the image is already on the nodes due to the first image pull then the nodes should start the kubelet regardless. With this update, the **baremetalRuntimeCfgImage** image is only pulled one time, thereby resolving the issue. (OCPBUGS-18772)

- Previously, the **nmstatectl** command failed to retrieve the correct permanent MAC address during OpenShift Container Platform updates for some network environments. This caused the interface to be renamed and the bond connection on the node to break during the update. With this release, patches were applied to the **nmstate** package and MCO to prevent renaming, and updates proceed as expected. (OCPBUGS-17877)

- Previously, the Machine Config Operator became the default provider of image registry certificates and the **node-ca** daemon was removed. This caused issues with the HyperShift Operator, because removing the **node-ca** daemon also removed the image registry path in the Machine Config Server (MCS), which HyperShift uses to get the Ignition configuration and start the bootstrap process. With this update, a flag containing the MCS image registry data is provided, which Ignition can use during the bootstrap process, thereby resolving the issue. (OCPBUGS-17811)

- Previously, older RHCOS boot images contained a race condition between services on boot that prevented the node from running the **rhcos-growpart** command before it pulled images, preventing the node from starting up. This caused node scaling to sometimes fail on clusters that use old boot images because it was determined there was no room left on the disk. With this update, processes were added to the Machine Config Operator for stricter ordering of services so that nodes boot correctly.

  NOTE

  In these situations, updating to newer boot images prevents similar issues from occurring.

  (OCPBUGS-15087)

- Previously, the Machine Config Operator (MCO) leveraged the **oc image extract** command to pull images during updates but the **ImageContentSourcePolicy** (ICSP) object was not respected when pulling those images. With this update, the MCO now uses the **podman pull** command internally and images are pulled from the location as configured in the ICSP. (OCPBUGS-13044)

Management Console

- Previously, the **Expand PVC** modal assumed the existing PVC had a **spec.resources.requests.storage** value that includes a unit. As a result, when the **Expand PVC** modal was used to expand a PVC that had a **requests.storage** value without a unit, the console would display an incorrect value in the modal. With this update, the console was updated to handle storage values with and without a unit. (OCPBUGS-27909)

- Previously, the console check to determine if a file is binary was not robust enough. As a result, XML files were misidentified as binary and not displaying in the console. With this update, an additional check was added to more precisely check if a file is binary. (OCPBUGS-26591)

- Previously, the **Node Overview** page failed to render when a **MachineHealthCheck** without **spec.unhealthyConditions** existed on a cluster. With this update, the **Node Overview** page was updated to allow for **MachineHealthChecks** without **spec.unhealthyConditions**. Now, the **Node Overview** page renders even if **MachineHealthChecks** without **spec.unhealthyConditions** are present on the cluster. ( OCPBUGS-25140)

- Previously, the console was not up-to-date with the newest matchers key for alert notification receivers, and the alert manager receivers created by the console utilized the older match key. With this update, the console uses matchers instead, and converts any existing match instances to matchers when modifying an existing alert manager receiver. (OCPBUGS-23248)

- Previously, impersonation access was incorrectly applied. With this update, the console correctly applies impersonation access. (OCPBUGS-23125)

- Previously, when the Advanced Cluster Management for Kubernetes (ACM) and multicluster engine for Kubernetes (MCE) Operators are installed and their plugins are enabled, the YAML code Monaco editor failed to load. With this update, optional resource chaining was added to prevent a failed resource call, and the YAML editor no longer fails to load when the ACM and MCE Operators are installed and their plugins enabled. (OCPBUGS-22778)

Monitoring

- Previously, the monitoring-plugin component did not start if IPv6 was disabled for a cluster. This release updates the component to support the following internet protocol configurations in a cluster: IPv4 only, IPv6 only, and both IPv4 and IPv6 simultaneously. This change resolves the issue, and the monitoring-plugin component now starts up if the cluster is configured to support only IPv6. (OCPBUGS-21610)

- Previously, instances of Alertmanager for core platform monitoring and for user-defined projects could inadvertently become peered during an upgrade. This issue could occur when multiple Alertmanager instances were deployed in the same cluster. This release fixes the issue by adding a **--cluster.label** flag to Alertmanager that helps to block any traffic that is not intended for the cluster. (OCPBUGS-18707)

- Previously, it was not possible to use text-only email templates in an Alertmanager configuration to send text-only email alerts. With this update, you can configure Alertmanager to send text-only email alerts by setting the **html** field of the email receiver to an empty string. ( OCPBUGS-11713)

Networking

- Previously, when creating an IngressController with an empty spec, the IngressController's status showed **Invalid**. However, the **route_controller_metrics_routes_per_shard** metric would still get created. When the invalid IngressController was deleted, the **route_controller_metrics_routes_per_shard** metric would not clear, and it would show information for that metric. With this update, metrics are only created for IngressControllers that are admitted, which resolves this issue. (OCPBUGS-3541)

- Previously, timeout values larger than what Go programming language could parse were not properly validated. Consequently, timeout values larger than what HAProxy could parse caused issues with HAProxy. With this update, if the timeout specifies a value larger than what can be parsed, it is capped at the maximum that HAProxy can parse. As a result, issues are no longer caused for HAProxy. (OCPBUGS-6959)

- Previously, an external neighbor could have its MAC address changed while the cluster was shutting down or hibernating. Although a Gratuitous Address Resolution Protocol (GARP) should notify other neighbors about this change, the cluster would not process the GARP because it was not running. When the cluster was brought back up, that neighbor might not be reachable from the OVN-Kubernetes cluster network because the stale MAC address was being used. This update enables an aging mechanism so that a neighbor's MAC address is periodically refreshed every 300 seconds. (OCPBUGS-11710)

- Previously, when an IngressController was configured with SSL/TLS, but did not have the **clientca-configmap** finalizer, the Ingress Operator would try to add the finalizer without checking whether the IngressController was marked for deletion. Consequently, if an IngressController was configured with SSL/TLS and was subsequently deleted, the Operator would correctly remove the finalizer. It would then repeatedly, and erroneously, try and fail to update the IngressController to add the finalizer back, resulting in error messages in the Operator's logs.
With this update, the Ingress Operator no longer adds the **clientca-configmap** finalizer to an IngressController that is marked for deletion. As a result, the Ingress Operator no longer tries to perform erroneous updates, and no longer logs the associated errors. (OCPBUGS-14994)

- Previously, a race condition occurred between the handling of pods that had been scheduled and the pods that had been completed on a node when OVN-Kubernetes started. This condition often occurred when nodes rebooted. Consequently, the same IP was erroneously assigned to multiple pods. This update fixes the race condition so that the same IP is not assigned to multiple pods in those circumstances. (OCPBUGS-16634)

- Previously, there was an error that caused a route to be rejected due to a duplicate host claim. When this occurred, the system would mistakenly select the first route it encountered, which was not always the conflicting route. With this update, all routes for the conflicting host are first retrieved and then sorted based on their submission time. This allows the system to accurately determine and select the newest conflicting route. (OCPBUGS-16707)

- Previously, when a new **ipspec-host** pod was started, it would clear or remove the existing **XFRM** state. Consequently, it would remove existing north-south traffic policies. This issue has been resolved. (OCPBUGS-19817)

- Previously, the **ovn-k8s-cni-overlay, topology:layer2** NetworkAttachmentDefinition did not work in a hosted pod when using the Kubevirt provider. Consequently, the pod did not start. This issue has been resolved, and pods can now start with an **ovn-k8s-cni-overlay** NetworkAttachmentDefinition. (OCPBUGS-22869)

- Previously, the Azure upstream DNS did not comply with non-EDNS DNS queries because it returned a payload larger than 512 bytes. Because CoreDNS 1.10.1 no longer uses EDNS for upstream queries and only uses EDNS when the original client query uses EDNS, the combination would result in an overflow **servfail** error when the upstream returned a payload

larger than 512 bytes for non-EDNS queries using CoreDNS 1.10.1. Consequently, upgrading from OpenShift Container Platform 4.12 to 4.13 led to some DNS queries failing that previously worked.
With this release, instead of returning an overflow **servfail** error, the CoreDNS now truncates the response, indicating that the client can try again in TCP. As a result, clusters with a noncompliant upstream now retry with TCP when experiencing overflow errors. This prevents any disruption of functionality between OpenShift Container Platform 4.12 and 4.13. (OCPBUGS-27904), (OCPBUGS-28205)

- Previously, there was a limitation in private Microsoft Azure clusters where secondary IP addresses designated as egress IP addresses lacked outbound connectivity. This meant that pods associated with these IP addresses were unable to access the internet. However, they could still reach external servers within the infrastructure network, which is the intended use case for egress IP addresses. This update enables egress IP addresses for Microsoft Azure clusters, allowing outbound connectivity to be achieved through outbound rules. (OCPBUGS-5491)

- Previously, when using multiple NICS, egress IP addresses were not correctly reassigned to the correct egress node when labeled or unlabeled. This bug has been fixed, and egress IP addresses are now reassigned to the correct egress node. (OCPBUGS-18162)

- Previously, a new logic introduced for determining where to run the Keepalived process did not consider the ingress VIP or VIPs. As a result, the Keepalived pods might not have ran on ingress nodes, which could break the cluster. With this fix, the logic now includes the ingress VIP or VIPs, and the Keepalived pods should always be available. (OCPBUGS-18771)

- Previously on Hypershift clusters, pods were not always being scheduled on separate zones. With this update, the **multus-admission-controller** deployment now uses a **PodAntiAffinity** spec for Hypershift to operate in the proper zone. (OCPBUGS-15220)

- Previously, a certificate that existed for 10 minutes was used to implement Multus. With this update, a per node certificate is used for the Multus CNI plugin and the certificate's existence is increased to a 24 hour duration. (OCPBUGS-19861), (OCPBUGS-19859)

- Previously, the **spec.desiredState.ovn.bridge-mappings** API configuration deleted all the external IDs in Open vSwitch (OVS) local tables on each Kubernetes node. As a result, the OVN chassis configuration was deleted, breaking the default cluster network. With this fix, you can use the **ovn.bridge-mappings** configuration without affecting the OVS configuration. (OCPBUGS-18869)

- Previously, if NMEA sentences were lost on their way to the E810 controller, the T-GM would not be able to synchronize the devices in the network synchronization chain. If these conditions were met, the PTP operator reported an error. With this release, a fix is implemented to report 'FREERUN' in case of a loss of the NMEA string. (OCPBUGS-20514)

- Previously, pods assigned an IP from the pool created by the Whereabouts CNI plugin persisted in the **ContainerCreating** state after a node force reboot. With this release, the Whereabouts CNI plugin issue associated with the IP allocation after a node force reboot is resolved. (OCPBUGS-18893)

- Previously, when using the assisted installer, OVN-Kubernetes took a long time to bootstrap. This issue occurred because there were three **ovnkube-control-plane** nodes. The first two started up normally, but the third delayed the installation time. The issue would only resolve after a timeout expiration; afterwards, installation would continue.
With this update, the third **ovnkube-control-plane** node has been removed. As a result, the installation time has been reduced. (OCPBUGS-29480)

### Node

- Due to how the Machine Config Operator (MCO) handles machine configurations for worker pools and custom pools, the MCO might apply an incorrect cgroup version argument for custom pools. As a consequence, nodes in the custom pool might feature an incorrect cgroup kernel argument that causes unpredictable behavior. As a workaround, specify cgroup version kernel arguments for worker and control plane pools only.(OCPBUGS-19352)

- Previously, CRI-O was not configuring the cgroup hierarchy correctly to account for the unique way that **crun** creates cgroups. As a consequence, disabling the CPU quota with a PerformanceProfile did not work. With this fix, using a PerformanceProfile to disable CPU quota works as expected. (OCPBUGS-20492)

- Previously, because of a default setting (**container_use_dri_devices, true**), containers were unable to use dri devices. With this fix, containers can use dri devices as expected. (OCPBUGS-24042)

- Previously, the kubelet was running with the **unconfined_service_t** SELinux type. As a consequence, all our plugins failed to deploy due to an Selinux denial. With this fix, the kubelet now runs with the **kubelet_exec_t** SELinux type. As a result, plugins deploy as expected. (OCPBUGS-20022)

- Previously, the **CRI-O** would automatically remove container images on an upgrade. This caused issues in pre-pulling images. With this release, when OpenShift Container Platform performs a minor upgrade, the container images will not be automatically removed and instead are subject to kubelet’s image garbage collection, which will trigger based on disk usage. (OCPBUGS-25228)

- Previously, when adding RHCOS machines to an existing cluster using ansible playbooks, machines were installed with openvswitch version 2.7. With this update, RHCOS machines added to existing clusters using ansible playbooks are installed with openvswitch version 3.1. This openvswitch version increases network performance. (OCPBUGS-18595)

### Node Tuning Operator (NTO)

- Previously, the Tuned profile reports **Degraded** condition after applying a PerformanceProfile. The generated Tuned profile was trying to set a **sysctl** value for the default Receive Packet Steering (RPS) mask when it already configured the same value using an **/etc/sysctl.d** file. Tuned warns about that and the Node Tuning Operator (NTO) treats that as a degradation with the following message **The TuneD daemon issued one or more error message(s) when applying the profile profile. TuneD stderr: net.core.rps_default_mask**. With this update, the duplication was solved by not setting the default RPS mask using Tuned. The **sysctl.d** file was left in place as it applies early during boot. (OCPBUGS-25092)

- Previously, the Node Tuning Operator (NTO) did not set the **UserAgent** and used a default one. With this update, the NTO sets the **UserAgent** appropriately, which makes debugging the cluster easier. (OCPBUGS-19785)

- Previously, when the Node Tuning Operator (NTO) pod restarted while there were a large number of CSVs in the cluster, the NTO pod would fail and entered into **CrashBackLoop** state. With this update, pagination has been added to the list CSVs requests and this avoids the **api-server** timeout issue that resulted in the **CrashBackLoop** state. (OCPBUGS-14241)

### OpenShift CLI (oc)

- Previously, to filter operator packages by channel, for example, **mirror.operators.catalog.packages.channels**, you had to specify the default channel for the

package, even if you did not intend to use the packages from that channel. Based on this information, the resulting catalog is considered invalid if the **imageSetConfig** does not contain the default channel for the package.
This update introduces the **defaultChannel** field in the **mirror.operators.catalog.packages** section. You can now select a default channel. This action enables **oc-mirror** to build a new catalog that defines the selected channel in the **defaultChannel** field as the default for the package. (OCPBUGS-385)

- Previously, using **eus-** channels for mirroring in **oc-mirror** resulted in failure. This was due to the restriction of **eus-** channels to mirror only even-numbered releases. With this update, **oc-mirror** can now effectively use **eus-** channels for mirroring releases. ( OCPBUGS-26065)

- Previously, while using **oc-mirror** for mirroring local OCI operator catalogs from a hidden folder resulted in the following error: **error: ".hidden_folder/data/publish/latest/catalog-oci/manifest-list/kubebuilder/kube-rbac-proxy@sha256:<SHASUM>" is not a valid image reference: invalid reference format**. With this update, the image references are adjusted in the local OCI catalog to prevent any errors during mirroring. (OCPBUGS-25077)

- Previously, the OpenShift Container Platform CLI (**oc**) version was not printed when running the **must-gather** tool. With this release, the **oc** version is now listed in the summary section when running **must-gather**. (OCPBUGS-24199)

- Previously, if you ran a command in **oc debug**. such as **oc debug node/worker — sleep 5; exit 1**, without attaching to the terminal, a **0** exit code was always returned regardless of the command’s exit code. With this release, the exit code is now properly returned from the command. (OCPBUGS-20342)

- Previously, when mirroring, **HTTP401** errors were observed due to expired authentication tokens. These errors occurred during the catalog introspection phase or the image mirroring phase. This issue has been fixed for catalog introspection. Additionally, fixing the Network Time Protocol (NTP) resolves the problem seen during the mirroring phase. For more information, see the article on "Access to the requested resource" error when mirroring images. (OCPBUGS-7465)

Operator Lifecycle Manager (OLM)

- After you install an Operator, if the catalog becomes unavailable, the subscription for the Operator is updated with a **ResolutionFailed** status condition. Before this update, when the catalog became available again, the **ResolutionFailed** status was not cleared. With this update, this status is now cleared from the subscription after the catalog becomes available, as expected. (OCPBUGS-29116)

- With this update, OLM performs a best-effort verification that existing custom resources (CRs) are not invalidated when you install an updated custom resource definition (CRD). (OCPBUGS-18948)

- Before this update, the install plan for an Operator displayed duplicate values in the **clusterSeviceVersionNames** field. This update removes the duplicate values. ( OCPBUGS-17408)

- Before this update, if you created an Operator group with same name as a previously existing cluster role, Operator Lifecycle Manager (OLM) overwrote the cluster role. With this fix, OLM generates a unique cluster role name for every Operator group by using the following syntax:

  **Naming syntax**

  ```
  olm.og.<operator_group_name>.<admin_edit_or_view>-<hash_value>
  ```

For more information, see Operator groups. (OCPBUGS-14698)

- Previously, if an Operator installation or upgrade took longer than 10 minutes, the operation could fail with the following error:

  > Bundle unpacking failed. Reason: DeadlineExceeded, Message: Job was active longer than specified deadline

  This issue occurred because Operator Lifecycle Manager (OLM) had a bundle unpacking job that was configured with a timeout of 600 seconds. Bundle unpacking jobs could fail because of network or configuration issues in the cluster that might be transient or resolved with user intervention. With this bug fix, OLM automates the re-creation of failed unpack jobs indefinitely by default.

  This update adds the optional **operatorframework.io/bundle-unpack-min-retry-interval** annotation for Operator groups. This annotation sets a minimum interval to wait before attempting to re-create the failed job. (OCPBUGS-6771)

- In Operator Lifecycle Manager (OLM), the Catalog Operator was logging many errors regarding missing **OperatorGroup** objects in namespaces that had no Operators installed. With this fix, if a namespace has no **Subscription** objects in it, OLM no longer checks if an **OperatorGroup** object is present in the namespace. (OCPBUGS-25330)

- With the security context constraint (SCC) API, users are able to configure security contexts for scheduling workloads on their cluster. Because parts of core OpenShift Container Platform components run as pods that are scheduled on control plane nodes, it is possible to create a SCC that prevents those core components from being properly scheduled in **openshift-*** namespaces.
  This bug fix reduces the role-based access control (RBAC) scope for the **openshift-operator-lifecycle-manager** service account used to run the **package-server-manager** core component. With this update, it is now significantly less likely that an SCC can be applied to the cluster that causes unexpected scheduling issues with the **package-server-manager** component.

  > **WARNING**
  >
  > The SCC API can globally affect scheduling on an OpenShift Container Platform cluster. When applying such constraints to workloads on the cluster, carefully read the SCC documentation.

  (OCPBUGS-20347)

### Scalability and performance

- Previously, a race condition between **udev** events and the creation queues associated with physical devices led to some of the queues being configured with the wrong Receive Packet Steering (RPS) mask when they should be reset to zero. This resulted in the RPS mask being configured on the queues of the physical devices, meaning they were using RPS instead of Receive Side Scaling (RSS), which could impact the performance. With this fix, the event was changed to be triggered per queue creation instead of at device creation. This guarantees that no queue will be missing. The queues of all physical devices are now set up with the correct RPS mask which is empty. (OCPBUGS-18662)

- Previously, due to differences in setting up a container's **cgroup** hierarchy, containers that use the **crun** OCI runtime along with a **PerformanceProfile** configuration encountered performance degradation. With this release, when handling a **PerformanceProfile** request, CRI-O accounts for the differences in **crun** and correctly configures the CPU quota to ensure performance. (OCPBUGS-20492)

Storage

- Previously, LVM Storage did not support disabling over-provisioning, and the minimum value for the **thinPoolConfig.overprovisionRatio** field in the **LVMCluster** CR was 2. With this release, you can disable over-provisioning by setting the value of the **thinPoolConfig.overprovisionRatio** field to 1. ( OCPBUGS-24396)

- Previously, if the **LVMCluster** CR was created with an invalid device path in the **deviceSelector.optionalPaths** field, the **LVMCluster** CR was in **Progressing** state. With this release, if the **deviceSelector.optionalPaths** field contains an invalid device path, LVM Storage updates the **LVMCluster** CR state to **Failed**. (OCPBUGS-23995)

- Previously, the LVM Storage resource pods were preempted while the cluster was congested. With this release, upon updating OpenShift Container Platform, LVM Storage configures the **priorityClassName** parameter to ensure proper scheduling and preemption behavior while the cluster is congested. (OCPBUGS-23375)

- Previously, upon creating the **LVMCluster** CR, LVM Storage skipped the counting of volume groups. This resulted in the **LVMCluster** CR moving to **Progressing** state even when the volume groups were valid. With this release, upon creating the **LVMCluster** CR, LVM Storage counts all the volume groups, and updates the **LVMCluster** CR state to **Ready** if the volume groups are valid. (OCPBUGS-23191)

- Previously, if the default device class was not present on all selected nodes, LVM Storage failed to set up the **LVMCluster** CR. With this release, LVM Storage detects all the default device classes even if the default device class is present only on one of the selected nodes. With this update, you can define the default device class only on one of the selected nodes. (OCPBUGS-23181)

- Previously, upon deleting the worker node in the single-node OpenShift (SNO) and worker node topology, the **LVMCluster** CR still included the configuration of the deleted worker node. This resulted in the **LVMCluster** CR remaining in **Progressing** state. With this release, upon deleting the worker node in the SNO and worker node topology, LVM Storage deletes the worker node configuration in the **LVMCluster** CR, and updates the **LVMCluster** CR state to **Ready**. (OCPBUGS-13558)

- Previously, CPU limits for the AWS EFS 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 have been removed to help prevent potential performance degradation. (OCPBUGS-28645)

- Previously, if you used the **performancePlus** parameter in the Azure Disk CSI driver and provisioned volumes 512 GiB or smaller, you would receive an error from the driver that you need a disk size of at least 512 GiB. With this release, if you use the **performancePlus** parameter and provision volumes 512 GiB or smaller, the Azure Disk CSI driver automatically resizes volumes to be 513 GiB. (OCPBUGS-17542)

## 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:

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

### Networking Technology Preview features

**Table 1.17. Networking Technology Preview tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Ingress Node Firewall Operator | Technology Preview | 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 | Technology Preview | Technology Preview |
| OVN-Kubernetes network plugin as secondary network | Technology Preview | General Availability | General Availability |
| Updating the interface-specific safe sysctls list | Technology Preview | Technology Preview | Technology Preview |
| Egress service custom resource | Not Available | Technology Preview | Technology Preview |
| VRF specification in **BGPPeer** custom resource | Not Available | Technology Preview | Technology Preview |
| VRF specification in **NodeNetworkConfigurationPolicy** custom resource | Not Available | Technology Preview | Technology Preview |
| Admin Network Policy (**AdminNetworkPolicy**) | Not Available | Technology Preview | Technology Preview |

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| IPsec external traffic (north-south) | Not Available | Technology Preview | General Availability |
| Host network settings for SR-IOV VFs | Not Available | Not Available | Technology Preview |

## Storage Technology Preview features

### Table 1.18. Storage Technology Preview tracker

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Automatic device discovery and provisioning with Local Storage Operator | Technology Preview | Technology Preview | Technology Preview |
| Google Filestore CSI Driver Operator | Technology Preview | General Availability | General Availability |
| IBM Power® Virtual Server Block CSI Driver Operator | Technology Preview | Technology Preview | Technology Preview |
| Read Write Once Pod access mod | Not available | Technology Preview | Technology Preview |
| Build CSI Volumes in OpenShift Builds | Technology Preview | General Availability | General Availability |
| Shared Resources CSI Driver in OpenShift Builds | Technology Preview | Technology Preview | Technology Preview |
| Secrets Store CSI Driver Operator | Not available | Technology Preview | Technology Preview |

## Installation Technology Preview features

### Table 1.19. Installation Technology Preview tracker

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Installing OpenShift Container Platform on Oracle® Cloud Infrastructure (OCI) with VMs | N/A | Developer Preview | Technology Preview |
| Installing OpenShift Container Platform on Oracle® Cloud Infrastructure (OCI) on bare metal | N/A | Developer Preview | Developer Preview |

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Adding kernel modules to nodes with kvc | Technology Preview | Technology Preview | Technology Preview |
| Azure Tagging | Technology Preview | General Availability | General Availability |
| Enabling NIC partitioning for SR-IOV devices | Technology Preview | Technology Preview | Technology Preview |
| GCP Confidential VMs | Technology Preview | General Availability | General Availability |
| User-defined labels and tags for Google Cloud Platform (GCP) | Not Available | Technology Preview | Technology Preview |
| Installing a cluster on Alibaba Cloud by using installer-provisioned infrastructure | Technology Preview | Technology Preview | Technology Preview |
| Mount shared entitlements in BuildConfigs in RHEL | Technology Preview | Technology Preview | Technology Preview |
| OpenShift Container Platform on Oracle Cloud Infrastructure (OCI) | Not Available | Developer Preview | Technology Preview |
| Selectable Cluster Inventory | Technology Preview | Technology Preview | Technology Preview |
| Static IP addresses with vSphere (IPI only) | Not Available | Technology Preview | Technology Preview |
| Support for iSCSI devices in RHCOS | Not Available | Not Available | Technology Preview |

### Node Technology Preview features

**Table 1.20. Nodes Technology Preview tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Cron job time zones | Technology Preview | General Availability | General Availability |
| **MaxUnavailableStatefulSet** featureset | Not Available | Technology Preview | Technology Preview |

### Multi-Architecture Technology Preview features

**Table 1.21. Multi-Architecture Technology Preview tracker**

Table 1.21. Multi-Architecture Technology Preview tracker

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| IBM Power® Virtual Server using installer-provisioned infrastructure | Technology Preview | Technology Preview | Technology Preview |
| **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 |

### Specialized hardware and driver enablement Technology Preview features

Table 1.22. Specialized hardware and driver enablement Technology Preview tracker

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Driver Toolkit | General Availability | General Availability | General Availability |
| Hub and spoke cluster support | General Availability | General Availability | General Availability |

### Web console Technology Preview features

Table 1.23. Web console Technology Preview tracker

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Multicluster console | Technology Preview | Technology Preview | Technology Preview |

### Scalability and performance Technology Preview features

Table 1.24. Scalability and performance Technology Preview tracker

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| factory-precaching-cli tool | Technology Preview | Technology Preview | Technology Preview |
| Hyperthreading-aware CPU manager policy | Technology Preview | Technology Preview | Technology Preview |

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| HTTP transport replaces AMQP for PTP and bare-metal events | Technology Preview | Technology Preview | Technology Preview |
| Mount namespace encapsulation | Technology Preview | Technology Preview | Technology Preview |
| NUMA-aware scheduling with NUMA Resources Operator | General Availability | General Availability | General Availability |
| Node Observability Operator | Technology Preview | Technology Preview | Technology Preview |
| Single-node OpenShift cluster expansion with worker nodes | General Availability | General Availability | General Availability |
| Topology Aware Lifecycle Manager (TALM) | General Availability | General Availability | General Availability |
| Tuning etcd latency tolerances | Not Available | Technology Preview | Technology Preview |
| Workload partitioning for three-node clusters and standard clusters | Technology Preview | General Availability | General Availability |

### Operator lifecycle and development Technology Preview features

**Table 1.25. Operator lifecycle and development Technology Preview tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Operator Lifecycle Manager (OLM) v1 | Not Available | Technology Preview | Technology Preview |
| RukPak | Technology Preview | Technology Preview | Technology Preview |
| Platform Operators | Technology Preview | Technology Preview | Technology Preview |
| Hybrid Helm Operator | Technology Preview | Technology Preview | Technology Preview |
| Java-based Operator | Technology Preview | Technology Preview | Technology Preview |

### Monitoring Technology Preview features

Table 1.26. Monitoring Technology Preview tracker

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Alerting rules based on platform monitoring metrics | Technology Preview | General Availability | General Availability |
| Metrics Collection Profiles | Technology Preview | Technology Preview | Technology Preview |
| Metrics Server | Not Available | Not Available | Technology Preview |

### Red Hat OpenStack Platform (RHOSP) Technology Preview features

Table 1.27. RHOSP Technology Preview tracker

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| External load balancers with installer-provisioned infrastructure | Technology Preview | General Availability | General Availability |
| Dual-stack networking with installer-provisioned infrastructure | Not Available | Technology Preview | General Availability |
| Dual-stack networking with user-provisioned infrastructure | Not Available | Not Available | General Availability |
| CAPO integration into the cluster CAPI Operator [1] | Not Available | Not Available | Technology Preview |
| Control Plane with **rootVolumes** and **etcd** on local disk | Not Available | Not Available | Technology Preview |

1. For more information, see CAPO integration into the cluster CAPI Operator.

### Architecture Technology Preview features

Table 1.28. Architecture Technology Preview tracker

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Hosted control planes for OpenShift Container Platform on Amazon Web Services (AWS) | Technology Preview | Technology Preview | Technology Preview |
| Hosted control planes for OpenShift Container Platform on bare metal | Technology Preview | Technology Preview | General Availability |

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Hosted control planes for OpenShift Container Platform on OpenShift Virtualization | Not Available | Technology Preview | General Availability |

### Machine management Technology Preview features

**Table 1.29. Machine management Technology Preview tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Managing machines with the Cluster API | Technology Preview | Technology Preview | Technology Preview |
| Defining a vSphere failure domain for a control plane machine set | Not Available | Not Available | Technology Preview |
| Cloud controller manager for Alibaba Cloud | Technology Preview | Technology Preview | Technology Preview |
| Cloud controller manager for Amazon Web Services | Technology Preview | General Availability | General Availability |
| Cloud controller manager for Google Cloud Platform | Technology Preview | Technology Preview | General Availability |
| Cloud controller manager for IBM Power® VS | Technology Preview | Technology Preview | Technology Preview |
| Cloud controller manager for Microsoft Azure | Technology Preview | General Availability | General Availability |

### Authentication and authorization Technology Preview features

**Table 1.30. Authentication and authorization Technology Preview tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Pod security admission restricted enforcement | Technology Preview | Technology Preview | Technology Preview |

### Machine Config Operator Technology Preview features

**Table 1.31. Machine Config Operator Technology Preview tracker**

| Feature | 4.13 | 4.14 | 4.15 |
|---|---|---|---|
| Improved MCO state reporting | 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)

- When installing a cluster on VMware vSphere with static IP addresses (Tech Preview), the installation program can apply an incorrect configuration to the control plane machine sets (CPMS). This can result in control plane machines being recreated without static IP addresses defined. (OCPBUGS-28236)

- Specifying a standard Ebdsv5 or Ebsv5 family machine type instance is not supported when installing an Azure cluster. This limitation is the result of the Azure terraform provider not supporting these machine types. (OCPBUGS-18690)

- When running a cluster with FIPS enabled, you might receive 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**. As a workaround, use the **oc** binary provided with the OpenShift Container Platform cluster. (OCPBUGS-23386)

- In 4.15 with IPv6 networking running on Red Hat OpenStack Platform (RHOSP) environments, **IngressController** objects configured with the **endpointPublishingStrategy.type=LoadBalancerService** YAML attribute will not function correctly. (BZ#2263550, BZ#2263552)

- In 4.15 with IPv6 networking running on Red Hat OpenStack Platform (RHOSP) environments, health monitors created with IPv6 **ovn-octavia** load balancers will not function correctly. (OCPBUGS-29603)

- In 4.15 with IPv6 networking running on Red Hat OpenStack Platform (RHOSP) environments, sharing a IPv6 load balancer with multiple services is not allowed because of an issue that mistakenly marks IPv6 load balancer as internal to the cluster.(OCPBUGS-29605)

- When installing an OpenShift Container Platform cluster with static IP addressing and Tang encryption, nodes start without network settings. This condition prevents nodes from accessing the Tang server, causing installation to fail. To address this condition, you must set the network settings for each node as **ip** installer arguments.

  1. For installer-provisioned infrastructure, before installation provide the network settings as **ip** installer arguments for each node by executing the following steps.

     a. Create the manifests.

     b. For each node, modify the **BareMetalHost** custom resource with annotations to include the network settings. For example:

     ```
     $ cd ~/clusterconfigs/openshift
     $ vim openshift-worker-0.yaml
     ```

```
apiVersion: metal3.io/v1alpha1
kind: BareMetalHost
metadata:
  annotations:
    bmac.agent-install.openshift.io/installer-args: '["--append-karg", "ip=<static_ip>::<gateway>:<netmask>:<hostname_1>:<interface>:none", "--save-partindex", "1", "-n"]' ① ② ③ ④ ⑤
    inspect.metal3.io: disabled
    bmac.agent-install.openshift.io/hostname: <fqdn> ⑥
    bmac.agent-install.openshift.io/role: <role> ⑦

  generation: 1
  name: openshift-worker-0
  namespace: mynamespace
spec:
  automatedCleaningMode: disabled
  bmc:
    address: idrac-virtualmedia://<bmc_ip>/redfish/v1/Systems/System.Embedded.1 ⑧
    credentialsName: bmc-secret-openshift-worker-0
    disableCertificateVerification: true
  bootMACAddress: 94:6D:AE:AB:EE:E8
  bootMode: "UEFI"
  rootDeviceHints:
    deviceName: /dev/sda
```

For the **ip** settings, replace:

① **<static_ip>** with the static IP address for the node, for example, **192.168.1.100**

② **<gateway>** with the IP address of your network's gateway, for example, **192.168.1.1**

③ **<netmask>** with the network mask, for example, **255.255.255.0**

④ **<hostname_1>** with the node's hostname, for example, **node1.example.com**

⑤ **<interface>** with the name of the network interface, for example, **eth0**

⑥ **<fqdn>** with the fully qualified domain name of the node

⑦ **<role>** with **worker** or **master** to reflect the node's role

⑧ **<bmc_ip>** with the BMC IP address and the protocol and path of the BMC, as needed.

c. Save the file to the **clusterconfigs/openshift** directory.

d. Create the cluster.

2. When installing with the Assisted Installer, before installation modify each node's installer arguments using the API to append the network settings as **ip** installer arguments. For example:

```
$ curl https://api.openshift.com/api/assisted-install/v2/infra-
```

```
envs/${infra_env_id}/hosts/${host_id}/installer-args \
-X PATCH \
-H "Authorization: Bearer ${API_TOKEN}" \
-H "Content-Type: application/json" \
-d '
   {
     "args": [
       "--append-karg",
       "ip=<static_ip>::<gateway>:<netmask>:<hostname_1>:<interface>:none", 1 2
3 4 5
       "--save-partindex",
       "1",
       "-n"
     ]
   }
  ' | jq
```

For the previous network settings, replace:

1. **<static_ip>** with the static IP address for the node, for example, **192.168.1.100**
2. **<gateway>** with the IP address of your network's gateway, for example, **192.168.1.1**
3. **<netmask>** with the network mask, for example, **255.255.255.0**
4. **<hostname_1>** with the node's hostname, for example, **node1.example.com**
5. **<interface>** with the name of the network interface, for example, **eth0**.

Contact Red Hat Support for additional details and assistance.

(OCPBUGS-23119)

- In OpenShift Container Platform 4.15, all nodes use Linux control group version 2 (cgroup v2) for internal resource management in alignment with the default RHEL 9 configuration. However, if you apply a performance profile in your cluster, the low-latency tuning features associated with the performance profile do not support cgroup v2.
  As a result, if you apply a performance profile, all nodes in the cluster reboot to switch back to the cgroup v1 configuration. This reboot includes control plane nodes and worker nodes that were not targeted by the performance profile.

  To revert all nodes in the cluster to the cgroups v2 configuration, you must edit the **Node** resource. For more information, see Configuring Linux cgroup v2 . You cannot revert the cluster to the cgroups v2 configuration by removing the last performance profile. (OCPBUGS-16976)

- Currently, 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, such as **dev69**, instead of its original name, such as **ensf0v2**. Although this error is not severe, the Multus and SR-IOV logs might show the error while the system recovers on its own. Deleting the pod might take a few seconds longer due to this error. (OCPBUGS-11281, OCPBUGS-18822, RHEL-5988)

- 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 you use **preempt-rt** patches with the real time kernel and you update the SMP affinity of a network interrupt, the corresponding Interrupt Request (IRQ) thread does not immediately receive the update. Instead, the update takes effect when the next interrupt is received, and the thread is subsequently migrated to the correct core. (RHEL-9148)

- The global navigation satellite system (GNSS) module in an Intel Westport Channel e810 NIC that is configured as a grandmaster clock (T-GM) can report the GPS **FIX** state and the GNSS offset between the GNSS module and the GNSS constellation satellites.
  The current T-GM implementation does not use the **ubxtool** CLI to probe the **ublox** module for reading the GNSS offset and GPS **FIX** values. Instead, it uses the **gpsd** service to read the GPS **FIX** information. This is because the current implementation of the **ubxtool** CLI takes 2 seconds to receive a response, and with every call, it increases CPU usage threefold. (OCPBUGS-17422)

- The current grandmaster clock (T-GM) implementation has a single NMEA sentence generator sourced from the GNSS without a backup NMEA sentence generator. If NMEA sentences are lost on their way to 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. ( OCPBUGS-19838)

- Currently, the **YAML** tab of some pages in the web console stops unexpectedly on some browsers when the multicluster engine for Kubernetes operator (MCE) is installed. The following message is displayed: "Oh no! Something went wrong." (OCPBUGS-29812)

- If you have IPsec enabled on the cluster and IPsec encryption is configured between the cluster and an external node, stopping the IPsec connection on the external node causes a loss of connectivity to the external node. This connectivity loss occurs because on the OpenShift Container Platform side of the connection, the IPsec tunnel shutdown is not recognized. (RHEL-24802)

- If you have IPsec enabled on the cluster, and your cluster is a hosted control planes for OpenShift Container Platform cluster, the MTU adjustment to account for the IPsec tunnel for pod-to-pod traffic does not happen automatically. (OCPBUGS-28757)

- If you have IPsec enabled on the cluster, you cannot modify existing IPsec tunnels to external hosts that you have created. Modifying an existing NMState Operator **NodeNetworkConfigurationPolicy** object to adjust an existing IPsec configuration to encrypt traffic to external hosts is not recognized by OpenShift Container Platform. (RHEL-22720)

- If you have IPsec enabled on the cluster, on the node hosting the north-south IPsec connection, restarting the **ipsec.service** systemd unit or restarting the **ovn-ipsec-host** pod causes a loss of the IPsec connection. (RHEL-26878)

- There is currently a known issue where the version of the **opm** CLI tool released with OpenShift Container Platform 4.15 does not support RHEL 8. As a workaround, RHEL 8 users can navigate to the OpenShift mirror site and download the latest version of the tarball released with OpenShift Container Platform 4.14.

- Currently, defining a **sysctl** value for a setting with a slash in its name, such as for bond devices, in the **profile** field of a Tuned resource might not work. Values with a slash in the **sysctl** option name are not mapped correctly to the **/proc** filesystem. As a workaround, create a **MachineConfig** resource that places a configuration file with the required values in the **/etc/sysctl.d** node directory. ( RHEL-3707)

- 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 in turn 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 because these features 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)

- When a node reboot occurs all pods are restarted in a random order. In this scenario it is possible that **tuned** pod started after the workload pods. This means the workload pods start with partial tuning, which can affect performance or even cause the workload to fail. (OCPBUGS-26400)

- The installation of OpenShift Container Platform might fail when a performance profile is present in the extra manifests folder and targets the primary or worker pools. This is caused by the internal install ordering that processes the performance profile before the default primary and worker **MachineConfigPools** are created. It is possible to workaround this issue by including a copy of the stock primary or worker **MachineConfigPools** in the extra manifests folder. (OCPBUGS-27948) (OCPBUGS-18640)

## 1.9. ASYNCHRONOUS ERRATA UPDATES

Security, bug fix, and enhancement updates for OpenShift Container Platform 4.15 are released as asynchronous errata through the Red Hat Network. All OpenShift Container Platform 4.15 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 4.15. Versioned asynchronous releases, for example with the form OpenShift Container Platform 4.15.z, will be detailed in subsections. In addition, releases in which the errata text cannot fit in the space provided by the advisory will be detailed in subsections that follow.

IMPORTANT

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

### 1.9.1. RHSA-2024:1210 - OpenShift Container Platform 4.15.2 bug fix and security update

Issued: 2024-3-13

OpenShift Container Platform release 4.15.2, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2024:1210 advisory. The RPM packages that are included in the update are provided by the RHBA-2024:1213 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 4.15.2 --pullspecs
```

### 1.9.1.1. Known issues

- Providing a performance profile as an extra manifest at Day 0 did not work in OpenShift Container Platform 4.15.0, but it is now possible in 4.15.2 with the following limitation:
  The installation of OpenShift Container Platform might fail when a performance profile is present in the extra manifests folder and targets the primary or worker pools. This is caused by the internal installation ordering that processes the performance profile before the default primary and worker **MachineConfigPools** are created. It is possible to workaround this issue by including a copy of the stock primary or worker **MachineConfigPools** in the extra manifests folder. (OCPBUGS-27948, OCPBUGS-29752)

### 1.9.1.2. Bug fixes

- Previously, when updating to OpenShift Container Platform 4.15, **CatalogSource** objects never refreshed, which caused the optional Operator catalogs to fail to update. With this release, the image pull policy is changed to **Always**, which enables the optional Operator catalogs to update correctly. (OCPBUGS-30193)

- Previously, the **nodeStatusReportFrequency** setting was linked to the **nodeStatusUpdateFrequency** setting. With this release, the **nodeStatusReportFrequency** setting is set to 5 minutes. (OCPBUGS-29797)

- Previously, under certain conditions, the installer would fail with the error message **unexpected end of JSON input**. With this release, the error message is clarified and suggests users set the **serviceAccount** field in the **install-config.yaml** file to fix the issue. ( OCPBUGS-29495)

- Previously, the **oauthMetadata** property provided in the **HostedCluster** object was not honored. With this release, the **oauthMetadata** property is honored by the **HostedCluster** object. (OCPBUGS-29025)

### 1.9.1.3. Updating

To update an existing OpenShift Container Platform 4.15 cluster to this latest release, see Updating a cluster using the CLI.