OpenShift Container Platform 4.10

Release notes

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

Last Updated: 2023-09-21

OpenShift Container Platform 4.10 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 4.10 RELEASE NOTES

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

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

1.1. ABOUT THIS RELEASE

OpenShift Container Platform (RHSA-2022:0056) is now available. This release uses Kubernetes 1.23 with CRI-O runtime. New features, changes, and known issues that pertain to OpenShift Container Platform 4.10 are included in this topic.

Red Hat did not publicly release OpenShift Container Platform 4.10.0 as the GA version and, instead, is releasing OpenShift Container Platform 4.10.3 as the GA version.

OpenShift Container Platform 4.10 clusters are available at https://console.redhat.com/openshift. The Red Hat OpenShift Cluster Manager application for OpenShift Container Platform allows you to deploy OpenShift clusters to either on-premise or cloud environments.

OpenShift Container Platform 4.10 is supported on Red Hat Enterprise Linux (RHEL) 8.4 through 8.7, as well as on Red Hat Enterprise Linux CoreOS (RHCOS) 4.10.

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

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

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

1.3. NEW FEATURES AND ENHANCEMENTS

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

1.3.1. Documentation

1.3.1.1. Getting started with OpenShift Container Platform

OpenShift Container Platform 4.10 now includes a getting started guide. Getting Started with OpenShift Container Platform defines basic terminology and provides role-based next steps for developers and administrators.

The tutorials walk new users through the web console and the OpenShift CLI (**oc**) interfaces. New users can accomplish the following tasks through the Getting Started:

- Create a project
- Grant view permissions
- Deploy a container image from Quay
- Examine and scale an application
- Deploy a Python application from GitHub
- Connect to a database from Quay
- Create a secret
- Load and view your application

For more information, see Getting Started with OpenShift Container Platform.

1.3.2. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.2.1. Improved customization of bare metal RHCOS installation

The **coreos-installer** utility now has **iso customize** and **pxe customize** subcommands for more flexible customization when installing RHCOS on bare metal from the live ISO and PXE images.

This includes the ability to customize the installation to fetch Ignition configs from HTTPS servers that use a custom certificate authority or self-signed certificate.

1.3.2.2. RHCOS now uses RHEL 8.4

RHCOS now uses Red Hat Enterprise Linux (RHEL) 8.4 packages in OpenShift Container Platform 4.10. These packages provide you the latest fixes, features, and enhancements, such as NetworkManager features, as well as the latest hardware support and driver updates.

1.3.3. Installation and upgrade

1.3.3.1. New default component types for AWS installations

The OpenShift Container Platform 4.10 installer uses new default component types for installations on AWS. The installation program uses the following components by default:

- AWS EC2 M6i instances for both control plane and compute nodes, where available
- AWS EBS gp3 storage

1.3.3.2. Enhancements to API in the **install-config.yaml** file

Previously, when a user installed OpenShift Container Platform on a bare metal installer-provisioned infrastructure, they had nowhere to configure custom network interfaces, such as static IPs or vLANs to communicate with the Ironic server.

When configuring a Day 1 installation on bare metal only, users can now use the API in the **install-**

config.yaml file to customize the network configuration (**networkConfig**). This configuration is set during the installation and provisioning process and includes advanced options, such as setting static IPs per host.

1.3.3.3. OpenShift Container Platform on ARM

OpenShift Container Platform 4.10 is now supported on ARM based AWS EC2 and bare-metal platforms. Instance availability and installation documentation can be found in Supported installation methods for different platforms.

The following features are supported for OpenShift Container Platform on ARM:

- OpenShift Cluster Monitoring
- RHEL 8 Application Streams
- OVNKube
- Elastic Block Store (EBS) for AWS
- AWS .NET applications
- NFS storage on bare metal

The following Operators are supported for OpenShift Container Platform on ARM:

- Node Tuning Operator
- Node Feature Discovery Operator
- Cluster Samples Operator
- Cluster Logging Operator
- Elasticsearch Operator
- Service Binding Operator

1.3.3.4. Installing a cluster on IBM Cloud using installer-provisioned infrastructure (Technology Preview)

OpenShift Container Platform 4.10 introduces support for installing a cluster on IBM Cloud using installer-provisioned infrastructure in Technology Preview.

The following limitations apply for IBM Cloud using IPI:

- Deploying IBM Cloud using IPI on a previously existing network is not supported.
- The Cloud Credential Operator (CCO) can use only Manual mode. Mint mode or STS are not supported.
- IBM Cloud DNS Services is not supported. An instance of IBM Cloud Internet Services is required.
- Private or disconnected deployments are not supported.

For more information, see Preparing to install on IBM Cloud .

1.3.3.5. Thin provisioning support for VMware vSphere cluster installation

OpenShift Container Platform 4.10 introduces support for thin-provisioned disks when you install a cluster using installer-provisioned infrastructure. You can provision disks as **thin**, **thick**, or **eagerZeroedThick**. For more information about disk provisioning modes in VMware vSphere, see Installation configuration parameters.

1.3.3.6. Installing a cluster into an Amazon Web Services GovCloud region

Red Hat Enterprise Linux CoreOS (RHCOS) Amazon Machine Images (AMIs) are now available for AWS GovCloud regions. The availability of these AMIs improves the installation process because you are no longer required to upload a custom RHCOS AMI to deploy a cluster.

For more information, see Installing a cluster on AWS into a government region .

1.3.3.7. Using a custom AWS IAM role for instance profiles

Beginning with OpenShift Container Platform 4.10, if you configure a cluster with an existing IAM role, the installation program no longer adds the **shared** tag to the role when deploying the cluster. This enhancement improves the installation process for organizations that want to use a custom IAM role, but whose security policies prevent the use of the **shared** tag.

1.3.3.8. CSI driver installation on vSphere clusters

To install a CSI driver on a cluster running on vSphere, you must have the following components installed:

- Virtual hardware version 15 or later
- vSphere version 6.7 Update 3 or later
- VMware ESXi version 6.7 Update 3 or later

Components with versions earlier than those above are still supported, but are deprecated. These versions are still fully supported, but version 4.11 of OpenShift Container Platform will require vSphere virtual hardware version 15 or later.

NOTE

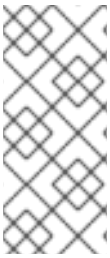
If your cluster is deployed on vSphere, and the preceding components are lower than the version mentioned above, upgrading from OpenShift Container Platform 4.9 to 4.10 on vSphere is supported, but no vSphere CSI driver will be installed. Bug fixes and other upgrades to 4.10 are still supported, however upgrading to 4.11 will be unavailable.

1.3.3.9. Installing a cluster on Alibaba Cloud using installer-provisioned infrastructure (Technology Preview)

OpenShift Container Platform 4.10 introduces the ability for installing a cluster on Alibaba Cloud using installer-provisioned infrastructure in Technology Preview. This type of installation lets you use the installation program to deploy a cluster on infrastructure that the installation program provisions and the cluster maintains.

1.3.3.10. Installing a cluster on Microsoft Azure Stack Hub using installer-provisioned infrastructure

OpenShift Container Platform 4.10 introduces support for installing a cluster on Azure Stack Hub using installer-provisioned infrastructure. This type of installation lets you use the installation program to deploy a cluster on infrastructure that the installation program provisions and the cluster maintains.



NOTE

Beginning with OpenShift Container Platform 4.10.14, you can deploy control plane and compute nodes with the **premium_LRS**, **standardSSD_LRS**, or **standard_LRS** disk type. By default, the installation program deploys control plane and compute nodes with the **premium_LRS** disk type. In earlier 4.10 releases, only the **standard_LRS** disk type was supported.

For more information, see Installing a cluster on Azure Stack Hub with an installer-provisioned infrastructure.

1.3.3.11. Conditional updates

OpenShift Container Platform 4.10 adds support for consuming conditional update paths provided by the OpenShift Update Service. Conditional update paths convey identified risks and the conditions under which those risks apply to clusters. The Administrator perspective on the web console only offers recommended upgrade paths for which the cluster does not match known risks. However, OpenShift CLI (**oc**) 4.10 or later can be used to display additional upgrade paths for OpenShift Container Platform 4.10 clusters. Associated risk information including supporting documentation references is displayed with the paths. The administrator may review the referenced materials and choose to perform the supported, but no longer recommended, upgrade.

For more information, see Conditional updates and Updating along a conditional upgrade path.

1.3.3.12. Disconnected mirroring with the oc-mirror CLI plugin (Technology Preview)

This release introduces the oc-mirror OpenShift CLI (**oc**) plugin as a Technology Preview. You can use the oc-mirror plugin to mirror images in a disconnected environment.

For more information, see Mirroring images for a disconnected installation using the oc-mirror plugin.

1.3.3.13. Installing a cluster on RHOSP that uses OVS-DPDK

You can now install a cluster on Red Hat OpenStack Platform (RHOSP) for which compute machines run on Open vSwitch with the Data Plane Development Kit (OVS-DPDK) networks. Workloads that run on these machines can benefit from the performance and latency improvements of OVS-DPDK.

For more information, see Installing a cluster on RHOSP that supports DPDK-connected compute machines.

1.3.3.14. Setting compute machine affinity during installation on RHOSP

You can now select compute machine affinity when you install a cluster on RHOSP. By default, compute machines are deployed with a **soft-anti-affinity** server policy, but you can also choose **anti-affinity** or **soft-affinity** policies.

1.3.4. Web console

1.3.4.1. Developer perspective

- With this update, you can specify the name of a service binding connector in the **Topology** view while making a binding connection.
- With this update, creating pipelines workflow has now been enhanced:
  - You can now choose a user-defined pipeline from a drop-down list while importing your application from the **Import from Git** pipeline workflow.
  - Default webhooks are added for the pipelines that are created using **Import from Git** workflow and the URL is visible in the side panel of the selected resources in the **Topology** view.
  - You can now opt out of the default Tekton Hub integration by setting the parameter **enable-devconsole-integration** to **false** in the **TektonConfig** custom resource.

    Example TektonConfig CR to opt out of Tekton Hub integration

    ```
    ...
    hub:
      params:
        - name: enable-devconsole-integration
          value: 'false'
    ...
    ```

  - **Pipeline builder** contains the Tekton Hub tasks that are supported by the cluster, all other unsupported tasks are excluded from the list.
- With this update, the application export workflow now displays the export logs dialog or alert while the export is in progress. You can use the dialog to cancel or restart the exporting process.
- With this update, you can add your new Helm Chart Repository to the **Developer Catalog** by creating a custom resource. Refer to the quick start guides in the **Developer** perspective to add a new **ProjectHelmChartRepository**.
- With this update, you can now access community devfiles samples using the **Developer Catalog**.

1.3.4.2. Dynamic plugin (Technology Preview)

Starting with OpenShift Container Platform 4.10, the ability to create OpenShift console dynamic plugins is now available as a Technology Preview feature. You can use this feature to customize your interface at runtime in many ways, including:

- Adding custom pages
- Adding perspectives and updating navigation items
- Adding tabs and actions to resource pages

For more information about the dynamic plugin, see Adding a dynamic plugin to the OpenShift Container Platform web console.

1.3.4.3. Running a pod in debug mode

With this update, you can run a pod in debug mode by using the `oc debug` command. When you debug a container that

With this update, you can now view debug terminals in the web console. When a pod has a container that is in a **CrashLoopBackOff** state, a debug pod can be launched. A terminal interface is displayed and can be used to debug the crash looping container.

- This feature can be accessed by the pod status pop-up window, which is accessed by clicking on the status of a pod, provides links to debug terminals for each crash looping container within that pod.
- You can also access this feature on the **Logs** tab of the pod details page. A debug terminal link is displayed above the log window when a crash looping container is selected.

Additionally, the pod status pop-up window now provides links to the **Logs** and **Events** tabs of the pod details page.

1.3.4.4. Customized workload notifications

With this update, you can customize workload notifications on the **User Preferences** page. **User workload notifications** under the **Notifications** tab allows you to hide user workload notifications that appear on the **Cluster Overview** page or in your drawer.

1.3.4.5. Improved quota visibility

With this update, non-admin users are now able to view their usage of the **AppliedClusterResourceQuota** on the **Project Overview**, **ResourceQuotas**, and **API Explorer** pages to determine the cluster-scoped quota available for use. Additionally, **AppliedClusterResourceQuota** details can now be found on the **Search** page.

1.3.4.6. Cluster support level

OpenShift Container Platform now enables you to view support level information about your cluster on the **Overview → Details** card, in the **Cluster Settings**, in the **About** modal, and adds a notification to your notifications drawer when your cluster is unsupported. From the **Overview** page, you can manage subscription settings under the **Service Level Agreement (SLA)**.

1.3.5. IBM Z and LinuxONE

With this release, IBM Z and LinuxONE are now compatible with OpenShift Container Platform 4.10. The installation can be performed with z/VM or RHEL KVM. For installation instructions, see the following documentation:

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

Notable enhancements
The following new features are supported on IBM Z and LinuxONE with OpenShift Container Platform 4.10:

- Horizontal pod autoscaling
- The following Multus CNI plugins are supported:

    - Bridge
    - Host-device
    - IPAM
    - IPVLAN
- Compliance Operator 0.1.49
- NMState Operator
- OVN-Kubernetes IPsec encryption
- Vertical Pod Autoscaler Operator

Supported features
The following features are also supported on IBM Z and LinuxONE:

- Currently, the following Operators are supported:
    - Cluster Logging Operator
    - Compliance Operator 0.1.49
    - Local Storage Operator
    - NFD Operator
    - NMState Operator
    - OpenShift Elasticsearch Operator
    - Service Binding Operator
    - Vertical Pod Autoscaler Operator
- Encrypting data stored in etcd
- Helm
- Multipathing
- Persistent storage using iSCSI
- Persistent storage using local volumes (Local Storage Operator)
- Persistent storage using hostPath
- Persistent storage using Fibre Channel
- Persistent storage using Raw Block
- OVN-Kubernetes
- Support for multiple network interfaces
- Three-node cluster support

- z/VM Emulated FBA devices on SCSI disks
- 4K FCP block device

These features are available only for OpenShift Container Platform on IBM Z and LinuxONE for 4.10:

- HyperPAV enabled on IBM Z and LinuxONE for the virtual machines for FICON attached ECKD storage

Restrictions
The following restrictions impact OpenShift Container Platform on IBM Z and LinuxONE:

- The following OpenShift Container Platform Technology Preview features are unsupported:
  - Precision Time Protocol (PTP) hardware
- The following OpenShift Container Platform features are unsupported:
  - Automatic repair of damaged machines with machine health checking
  - CodeReady Containers (CRC)
  - Controlling overcommit and managing container density on nodes
  - CSI volume cloning
  - CSI volume snapshots
  - FIPS cryptography
  - NVMe
  - OpenShift Metering
  - OpenShift Virtualization
  - Tang mode disk encryption during OpenShift Container Platform deployment
- Worker nodes must run Red Hat Enterprise Linux CoreOS (RHCOS)
- Persistent shared storage must be provisioned by using either OpenShift Data Foundation or other supported storage protocols
- Persistent non-shared storage must be provisioned using local storage, like iSCSI, FC, or using LSO with DASD, FCP, or EDEV/FBA

1.3.6. IBM Power

With this release, IBM Power is now compatible with OpenShift Container Platform 4.10. For installation instructions, see the following documentation:

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

Notable enhancements
The following new features are supported on IBM Power with OpenShift Container Platform 4.10:

- Horizontal pod autoscaling
- The following Multus CNI plugins are supported:
  - Bridge
  - Host-device
  - IPAM
  - IPVLAN
- Compliance Operator 0.1.49
- NMState Operator
- OVN-Kubernetes IPsec encryption
- Vertical Pod Autoscaler Operator

Supported features
The following features are also supported on IBM Power:

- Currently, the following Operators are supported:
  - Cluster Logging Operator
  - Compliance Operator 0.1.49
  - Local Storage Operator
  - NFD Operator
  - NMState Operator
  - OpenShift Elasticsearch Operator
  - SR-IOV Network Operator
  - Service Binding Operator
  - Vertical Pod Autoscaler Operator
- Encrypting data stored in etcd
- Helm
- Multipathing
- Multus SR-IOV
- NVMe
- OVN-Kubernetes
- Persistent storage using iSCSI
- Persistent storage using local volumes (Local Storage Operator)

- Persistent storage using hostPath
- Persistent storage using Fibre Channel
- Persistent storage using Raw Block
- Support for multiple network interfaces
- Support for Power10
- Three-node cluster support
- 4K Disk Support

Restrictions
The following restrictions impact OpenShift Container Platform on IBM Power:

- The following OpenShift Container Platform Technology Preview features are unsupported:
  - Precision Time Protocol (PTP) hardware
- The following OpenShift Container Platform features are unsupported:
  - Automatic repair of damaged machines with machine health checking
  - CodeReady Containers (CRC)
  - Controlling overcommit and managing container density on nodes
  - FIPS cryptography
  - OpenShift Metering
  - OpenShift Virtualization
  - Tang mode disk encryption during OpenShift Container Platform deployment
- Worker nodes must run Red Hat Enterprise Linux CoreOS (RHCOS)
- Persistent storage must be of the Filesystem type that uses local volumes, OpenShift Data Foundation, Network File System (NFS), or Container Storage Interface (CSI)

1.3.7. Security and compliance

Information regarding new features, enhancements, and bug fixes for security and compliance components can be found in the Compliance Operator and File Integrity Operator release notes.

For more information about security and compliance, see OpenShift Container Platform security and compliance.

1.3.8. Networking

1.3.8.1. Dual-stack services require that ipFamilyPolicy is specified

When you create a service that uses multiple IP address families, you must explicitly specify **ipFamilyPolicy: PreferDualStack** or **ipFamilyPolicy: RequireDualStack** in your Service object definition. This change breaks backward compatibility with earlier releases of OpenShift Container

Platform.

For more information, see BZ#2045576.

1.3.8.2. Change cluster network MTU after cluster installation

After cluster installation, if you are using the OpenShift SDN cluster network provider or the OVN-Kubernetes cluster network provider, you can change your hardware MTU and your cluster network MTU values. Changing the MTU across the cluster is disruptive and requires that each node is rebooted several times. For more information, see Changing the cluster network MTU.

1.3.8.3. OVN-Kubernetes support for gateway configuration

The OVN-Kubernetes CNI network provider adds support for configuring how egress traffic is sent to the node gateway. By default, egress traffic is processed in OVN to exit the cluster and traffic is not affected by specialized routes in the kernel routing table.

This enhancement adds a **gatewayConfig.routingViaHost** field. With this update, the field can be set at runtime as a post-installation activity and when it is set to **true**, egress traffic is sent from pods to the host networking stack. This update benefits highly specialized installations and applications that rely on manually configured routes in the kernel routing table.

This enhancement has an interaction with the Open vSwitch hardware offloading feature. With this update, when the **gatewayConfig.routingViaHost** field is set to **true**, you do not receive the performance benefits of the offloading because egress traffic is processed by the host networking stack.

IMPORTANT

To set egress traffic, use **gatewayConfig.routingViaHost** and delete the **gateway-mode-config** config map if you have set it up in the **openshift-network-operator** namespace. For more information regarding the **gateway-mode-config** solution and setting OVN-Kubernetes gateway mode in OpenShift Container Platform 4.10 and higher, see the soultion.

For configuration information, see Configuration for the OVN-Kubernetes CNI cluster network provider .

1.3.8.4. Enhancements to networking metrics

The following metrics are now available for clusters. The metric names that start with **sdn_controller** are unique to the OpenShift SDN CNI network provider. The metric names that start with **ovn** are unique to the OVN-Kubernetes CNI network provider:

- **network_attachment_definition_instances{networks="egress-router"}**
- **openshift_unidle_events_total**
- **ovn_controller_bfd_run**
- **ovn_controller_ct_zone_commit**
- **ovn_controller_flow_generation**
- **ovn_controller_flow_installation**

- **ovn_controller_if_status_mgr**
- **ovn_controller_if_status_mgr_run**
- **ovn_controller_if_status_mgr_update**
- **ovn_controller_integration_bridge_openflow_total**
- **ovn_controller_ofctrl_seqno_run**
- **ovn_controller_patch_run**
- **ovn_controller_pinctrl_run**
- **ovnkube_master_ipsec_enabled**
- **ovnkube_master_num_egress_firewall_rules**
- **ovnkube_master_num_egress_firewalls**
- **ovnkube_master_num_egress_ips**
- **ovnkube_master_pod_first_seen_lsp_created_duration_seconds**
- **ovnkube_master_pod_lsp_created_port_binding_duration_seconds**
- **ovnkube_master_pod_port_binding_chassis_port_binding_up_duration_seconds**
- **ovnkube_master_pod_port_binding_port_binding_chassis_duration_seconds**
- **sdn_controller_num_egress_firewall_rules**
- **sdn_controller_num_egress_firewalls**
- **sdn_controller_num_egress_ips**

The **ovnkube_master_resource_update_total** metric is removed for the 4.10 release.

1.3.8.5. Switching between YAML view and a web console form

- Previously, changes were not retained when switching between **YAML view** and **Form view** on the web console. Additionally, after switching to **YAML view**, you could not return to **Form view**. With this update, you can now easily switch between **YAML view** and **Form view** on the web console without losing changes.

1.3.8.6. Listing pods targeted by network policies

When using the network policy functionality in the OpenShift Container Platform web console, the pods affected by a policy are listed. The list changes as the combined namespace and pod selectors in these policy sections are modified:

- Peer definition
- Rule definition
- Ingress

- Egress

The list of impacted pods includes only those pods accessible by the user.

1.3.8.7. Enhancement to must-gather to simplify network tracing

The **oc adm must-gather** command is enhanced in a way that simplifies collecting network packet captures.

Previously, **oc adm must-gather** could start a single debug pod only. With this enhancement, you can start a debug pod on multiple nodes at the same time.

You can use the enhancement to run packet captures on multiple nodes at the same time to simplify troubleshooting network communication issues. A new **--node-selector** argument provides a way to identify which nodes you are collecting packet captures for.

For more information, see Network trace methods and Collecting a host network trace .

1.3.8.8. Pod-level bonding for secondary networks

Bonding at the pod level is vital to enable workloads inside pods that require high availability and more throughput. With pod-level bonding, you can create a bond interface from multiple single root I/O virtualization (SR-IOV) virtual function interfaces in kernel mode interface. The SR-IOV virtual functions are passed into the pod and attached to a kernel driver.

Scenarios where pod-level bonding is required include creating a bond interface from multiple SR-IOV virtual functions on different physical functions. Creating a bond interface from two different physical functions on the host can be used to achieve high availability at pod level.

1.3.8.9. Egress IP address support for clusters installed on public clouds

As a cluster administrator, you can associate one or more egress IP addresses with a namespace. An egress IP address ensures that a consistent source IP address is associated with traffic from a particular namespace that is leaving the cluster.

For the OVN-Kubernetes and OpenShift SDN cluster network providers, you can configure an egress IP address on the following public cloud providers:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

To learn more, refer to the respective documentation for your cluster network provider:

1.3.8.10. OpenShift SDN cluster network provider network policy support for egress policies and ipBlock except

If you use the OpenShift SDN cluster network provider, you can now use egress rules in network policy with **ipBlock** and **ipBlock.except**. You define egress policies in the **egress** array of the **NetworkPolicy** object.

For more information, refer to About network policy.

1.3.8.11. Ingress Controller router compression

This enhancement adds the ability to configure global HTTP traffic compression on the HAProxy Ingress Controller for specific MIME types. This update enables gzip-compression of your ingress workloads when there are large amounts of compressible routed traffic.

For more information, see Using router compression.

1.3.8.12. Support for CoreDNS customization

A cluster administrator can now configure DNS servers to allow DNS name resolution through the configured servers for the default domain. A DNS forwarding configuration can have both the default servers specified in the **/etc/resolv.conf** file and the upstream DNS servers.

For more information, see Using DNS forwarding.

1.3.8.13. Support for CoreDNS log level and Operator log level

This enhancement adds the ability to manually change the log level for an Operator individually or a cluster as a whole.

For more information, see Setting the CoreDNS log level

1.3.8.14. Support for configuring the maximum length of the syslog message in the Ingress Controller

You can now set the maximum length of the syslog message in the Ingress Controller to any value between 480 and 4096 bytes.

For more information, see Ingress Controller configuration parameters.

1.3.8.15. Set CoreDNS forwarding policy

You can now set the CoreDNS forwarding policy through the DNS Operator. The default value is **Random**, and you can also set the value to **RoundRobin** or **Sequential**.

For more information, see Using DNS forwarding.

1.3.8.16. Open vSwitch hardware offloading support for SR-IOV

You can now configure Open vSwitch hardware offloading to increase data processing performance on compatible bare metal nodes. Hardware offloading is a method for processing data that removes data processing tasks from the CPU and transfers them to the dedicated data processing unit of a network interface controller. Benefits of this feature include faster data processing, reduced CPU workloads, and lower computing costs.

For more information, see Configuring hardware offloading.

1.3.8.17. Creating DNS records by using the Red Hat External DNS Operator (Technology Preview)

You can now create DNS records by using the Red Hat External DNS Operator on cloud providers such as AWS, Azure, and GCP. You can install the External DNS Operator using OperatorHub. You can use parameters to configure **ExternalDNS** as required.

For more information, see Understanding the External DNS Operator .

1.3.8.18. Mutable Ingress Controller endpoint publishing strategy enhancement

Cluster administrators can now configure the Ingress Controller endpoint publishing strategy to change the load-balancer scope between **Internal** and **External** in OpenShift Container Platform.

For more information, see Ingress Controller endpoint publishing strategy .

1.3.8.19. OVS hardware offloading for clusters on RHOSP (Technology Preview)

For clusters that run on Red Hat OpenStack Platform (RHOSP), you can enable Open vSwitch (OVS) hardware offloading.

For more information, see Enabling OVS hardware offloading.

1.3.8.20. Reduction of RHOSP resources created by Kuryr

For clusters that run on RHOSP, Kuryr now only creates Neutron networks and subnets for namespaces that have at least one pod on the pods network. Additionally, pools in a namespace are populated after at least one pod on the pods network is created in the namespace.

1.3.8.21. Support for RHOSP DCN (Technology Preview)

You can now deploy a cluster on a Red Hat OpenStack Platform (RHOSP) deployment that uses a distributed compute node (DCN) configuration. This deployment configuration has several limitations:

- Only RHOSP version 16 is supported.
- For RHOSP 16.1.4, only hyper-converged infrastructure (HCI) and Ceph technologies are supported at the edge.
- For RHOSP 16.2, non-HCI and Ceph technologies are supported as well.
- Networks must be created ahead of time (Bring Your Own Network) as either tenant or provider networks. These networks must be scheduled in the appropriate availability zones.

1.3.8.22. Support for external cloud providers for clusters on RHOSP (Technology Preview)

Clusters that run on RHOSP can now use Cloud Provider OpenStack. This capability is available as part of the **TechPreviewNoUpgrade** feature set.

1.3.8.23. Configuring host network interfaces with NMState on installer-provisioned clusters

OpenShift Container Platform now provides a **networkConfig** configuration setting for installer-provisioned clusters, which takes an NMState YAML configuration to configure host interfaces. During installer-provisioned installations, you can add the **networkConfig** configuration setting and the NMState YAML configuration to the **install-config.yaml** file. Additionally, you can add the **networkConfig** configuration setting and the NMState YAML configuration to the bare metal host resource when using the Bare Metal Operator.

The most common use case for the **networkConfig** configuration setting is to set static IP addresses on a host's network interface during installation or while expanding the cluster.

For more information, see Configuring host network interfaces in the install-config.yaml file .

1.3.8.24. Boundary clock and PTP enhancements to linuxptp services

You can now specify multiple network interfaces in a **PtpConfig** profile to allow nodes running RAN vDU applications to serve as a Precision Time Protocol Telecom Boundary Clock (PTP T-BC). Interfaces configured as boundary clocks now also support PTP fast events.

For more information, see Configuring linuxptp services as boundary clock .

1.3.8.25. Support for Intel 800-Series Columbiaville NICs

Intel 800-Series Columbiaville NICs are now fully supported for interfaces configured as boundary clocks or ordinary clocks. Columbiaville NICs are supported in the following configurations:

- Ordinary clock
- Boundary clock synced to the Grandmaster clock
- Boundary clock with one port synchronizing from an upstream source clock, and three ports providing downstream timing to destination clocks

For more information, see Configuring PTP devices.

1.3.8.26. Kubernetes NMState Operator is GA for bare-metal, IBM Power, IBM Z, and LinuxONE installations

OpenShift Container Platform now provides the Kubernetes NMState Operator for bare-metal, IBM Power, IBM Z, and LinuxONE installations. The Kubernetes NMState Operator is still a Technology Preview for all other platforms. See About the Kubernetes NMState Operator for additional details.

1.3.8.27. SR-IOV support for Mellanox MT2892 cards

SR-IOV support is now available for Mellanox MT2892 cards.

1.3.8.28. Network Observability Operator to observe network traffic flow

As an administrator, you can now install the Network Observability Operator to observe the network traffic for your OpenShift Container Platform cluster in the console. You can view and monitor the network traffic data in different graphical representations. The Network Observability Operator uses eBPF technology to create the network flows. The network flows are enriched with OpenShift Container Platform information, and stored in Loki. You can use the network traffic information for detailed troubleshooting and analysis.

The Network Observability Operator is General Availability (GA) status in the 4.12 release of OpenShift Container Platform and is also supported in OpenShift Container Platform 4.10.

For more information, see Network Observability.

1.3.8.28.1. Network Observability Operator updates

The Network Observability Operator releases updates independently from the OpenShift Container Platform minor version release stream. Updates are available through a single, rolling stream which is supported on all currently supported versions of OpenShift Container Platform 4. Information regarding

new features, enhancements, and bug fixes for the Network Observability Operator can be found in the Network Observability release notes.

1.3.9. Hardware

1.3.9.1. Enhancements to MetalLB load balancing

The following enhancements to MetalLB and the MetalLB Operator are included in this release:

- Support for Border Gateway Protocol (BGP) is added.
- Support for Bidirectional Forwarding Detection (BFD) in combination with BGP is added.
- Support for IPv6 and dual-stack networking is added.
- Support for specifying a node selector on the **speaker** pods is added. You can now control which nodes are used for advertising load balancer service IP addresses. This enhancement applies to layer 2 mode and BGP mode.
- Validating web hooks are added to ensure that address pool and BGP peer custom resources are valid.
- The **v1alpha1** API version for the **AddressPool** and **MetalLB** custom resource definitions that were introduced in the 4.9 release are deprecated. Both custom resources are updated to the **v1beta1** API version.
- Support for speaker pod tolerations in the MetalLB custom resource definition is added.

For more information, see About MetalLB and the MetalLB Operator.

1.3.9.2. Support for modifying host firmware settings

OpenShift Container Platform supports the **HostFirmwareSettings** and **FirmwareSchema** resources. When deploying OpenShift Container Platform on bare metal hosts, there are times when you need to make changes to the host either before or after provisioning. This can include inspecting the host's firmware and BIOS details. There are two new resources that you can use with the Bare Metal Operator (BMO):

- **HostFirmwareSettings**: You can use the **HostFirmwareSettings** resource to retrieve and manage the BIOS settings for a host. The resource contains the complete BIOS configuration returned from the baseboard management controller (BMC). Whereas, the firmware field in the **BareMetalHost** resource returns three vendor-independent fields, the **HostFirmwareSettings** resource typically comprises many BIOS settings of vendor-specific fields per host model.
- **FirmwareSchema**: You can use the **FirmwareSchema** to identify the host's modifiable BIOS values and limits when making changes to host firmware settings.

See Bare metal configuration for additional details.

1.3.10. Storage

1.3.10.1. Storage metrics indicator

- With this update, workloads can securely share **Secrets** and **ConfigMap** objects across namespaces using inline ephemeral **csi** volumes provided by the Shared Resource CSI Driver.

Container Storage Interface (CSI) volumes and the Shared Resource CSI Driver are Technology Preview features. (BUILD-293)

1.3.10.2. Console Storage Plugin enhancement

- A new feature has been added to the Console Storage Plugin that adds Aria labels throughout the installation flow for screen readers. This provides better accessibility for users that use screen readers to access the console.
- A new feature has been added that provides metrics indicating the amount of used space on volumes used for persistent volume claims (PVCs). This information appears in the PVC list, and in the PVC details in the **Used** column. (**BZ#1985965**)

1.3.10.3. Persistent storage using the Alibaba AliCloud Disk CSI Driver Operator

OpenShift Container Platform is capable of provisioning persistent volumes (PVs) using the Container Storage Interface (CSI) driver for AliCloud Disk. The AliCloud Disk Driver Operator that manages this driver is generally available, and enabled by default in OpenShift Container Platform 4.10.

For more information, see AliCloud Disk CSI Driver Operator .

1.3.10.4. Persistent storage using the Microsoft Azure File CSI Driver Operator (Technology Preview)

OpenShift Container Platform is capable of provisioning persistent volumes (PVs) using the Container Storage Interface (CSI) driver for Azure File. The Azure File Driver Operator that manages this driver is in Technology Preview.

For more information, see Azure File CSI Driver Operator .

1.3.10.5. Persistent storage using the IBM VPC Block CSI Driver Operator

OpenShift Container Platform is capable of provisioning persistent volumes (PVs) using the Container Storage Interface (CSI) driver for IBM Virtual Private Cloud (VPC) Block. The IBM VPC Block Driver Operator that manages this driver is generally available, and enabled by default in OpenShift Container Platform 4.10.

For more information, see IBM VPC Block CSI Driver Operator .

1.3.10.6. Persistent storage using VMware vSphere CSI Driver Operator is generally available

OpenShift Container Platform is capable of provisioning persistent volumes (PVs) using the Container Storage Interface (CSI) driver for vSphere. This feature was previously introduced as a Technology Preview feature in OpenShift Container Platform 4.8 and is now generally available and enabled by default in OpenShift Container Platform 4.10.

For more information, see vSphere CSI Driver Operator .

vSphere CSI Driver Operator installation requires:

- Certain minimum component versions installed. See CSI driver installation on vSphere clusters
- Removal of any non-Red Hat vSphere CSI driver (Removing a non-Red Hat vSphere CSI Operator Driver)

- Removal of any storage class named **thin-csi**

Clusters are still upgraded even if the preceding conditions are not met, but it is recommended that you meet these conditions to have a supported vSphere CSI Operator Driver.

1.3.10.7. Persistent storage using Microsoft Azure Disk CSI Driver Operator is generally available

OpenShift Container Platform is capable of provisioning persistent volumes (PVs) using the Container Storage Interface (CSI) driver for Azure Disk. This feature was previously introduced as a Technology Preview feature in OpenShift Container Platform 4.8 and is now generally available, and enabled by default in OpenShift Container Platform 4.10.

For more information, see Azure Disk CSI Driver Operator .

1.3.10.8. Persistent storage using AWS Elastic File Storage CSI Driver Operator is generally available

OpenShift Container Platform is capable of provisioning persistent volumes (PVs) using the Container Storage Interface (CSI) driver for AWS Elastic File Storage (EFS). This feature was previously introduced as a Technology Preview feature in OpenShift Container Platform 4.9 and is now generally available in OpenShift Container Platform 4.10.

For more information, see AWS EFS CSI Driver Operator .

1.3.10.9. Automatic CSI migration supports Microsoft Azure file (Technology Preview)

Starting with OpenShift Container Platform 4.8, automatic migration for in-tree volume plugins to their equivalent Container Storage Interface (CSI) drivers became available as a Technology Preview feature. This feature now supports automatic migration for the Azure File in-tree plugin to the Azure File CSI driver.

For more information, see CSI automatic migration .

1.3.10.10. Automatic CSI migration supports VMware vSphere (Technology Preview)

Starting with OpenShift Container Platform 4.8, automatic migration for in-tree volume plugins to their equivalent Container Storage Interface (CSI) drivers became available as a Technology Preview feature. This feature now supports automatic migration for the vSphere in-tree plugin to the vSphere CSI driver.

For more information, see CSI automatic migration .

1.3.10.11. Using fsGroup to reduce pod timeouts

If a storage volume contains many files (roughly 1,000,000 or greater), you may experience pod timeouts.

OpenShift Container Platform 4.10 introduces the ability to use **fsGroup** and **fsGroupChangePolicy** to skip recursive permission change for the storage volume, therefore helping to avoid pod timeout problems.

For more information, see Using fsGroup to reduce pod timeouts .

1.3.11. Registry

1.3.12. Operator lifecycle

1.3.12.1. Disabling copied CSVs to support large clusters

When an Operator is installed by Operator Lifecycle Manager (OLM), a simplified copy of its cluster service version (CSV) is created in every namespace that the Operator is configured to watch. These CSVs are known as copied CSVs; they identify controllers that are actively reconciling resource events in a given namespace.

On large clusters, with namespaces and installed Operators potentially in the hundreds or thousands, copied CSVs can consume an untenable amount of resources, such as OLM's memory usage, cluster etcd limits, and networking bandwidth. To support these larger clusters, cluster administrators can now disable copied CSVs for Operators that are installed with the **AllNamespaces** mode.

For more details, see Configuring Operator Lifecycle Manager features.

1.3.12.2. Generic and complex constraints for dependencies

Operators with specific dependency requirements can now use complex constraints or requirement expressions. The new **olm.constraint** bundle property holds dependency constraint information. A message field allows Operator authors to convey high-level details about why a particular constraint was used.

For more details, see Operator Lifecycle Manager dependency resolution.

1.3.12.3. Operator Lifecycle Manager support for Hypershift

Operator Lifecycle Manager (OLM) components, including Operator catalogs, can now run entirely on Hypershift-managed control planes. This capability does not incur any cost to tenants on worker nodes.

1.3.12.4. Operator Lifecycle Manager support for ARM

Previously, the default Operator catalogs did not support ARM. With this enhancement, Operator Lifecycle Manager (OLM) adds default Operator catalogs to ARM clusters. As a result, the OperatorHub now includes content by default for Operators that support ARM. (BZ#1996928)

1.3.13. Operator development

1.3.13.1. Hybrid Helm Operator (Technology Preview)

The standard Helm-based Operator support in the Operator SDK has limited functionality compared to the Go-based and Ansible-based Operator support that has reached the Auto Pilot capability (level V) in the Operator maturity model.

Starting in OpenShift Container Platform 4.10 as a Technology Preview feature, the Operator SDK includes the Hybrid Helm Operator to enhance the existing Helm-based support abilities through Go APIs. Operator authors can generate an Operator project beginning with a Helm chart, and then add advanced, event-based logic to the Helm reconciler in Go language. Authors can use Go to continue adding new APIs and custom resource definitions (CRDs) in the same project.

For more details, see Operator SDK tutorial for Hybrid Helm Operators.

1.3.13.2. Custom metrics for Ansible-based Operators

Operator authors can now use the Ansible-based Operator support in the Operator SDK to expose custom metrics, emit Kubernetes events, and provide better logging.

For more details, see Exposing custom metrics for Ansible-based Operators.

1.3.13.3. Object pruning for Go-based Operators

The **operator-lib** pruning utility lets Go-based Operators clean up objects, such as jobs or pods, that can stay in the cluster and use resources. The utility includes common pruning strategies for Go-based Operators. Operator authors can also use the utility to create custom hooks and strategies.

For more information about the pruning utility, see Object pruning utility for Go-based Operators.

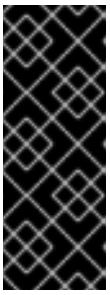
1.3.13.4. Digest-based bundle for disconnected environments

With this enhancement, Operator SDK can now package an Operator project into a bundle that works in a disconnected environment with Operator Lifecycle Manager (OLM). Operator authors can run the **make bundle** command and set **USE_IMAGE_DIGESTS** to **true** to automatically update your Operator image reference to a digest rather than a tag. To use the command, you must use environment variables to replace hard-coded related image references.

For more information about developing Operators for disconnected environments, see Enabling your Operator for restricted network environments.

1.3.14. Builds

- With this update, you can use CSI volumes in OpenShift Builds, which is a Technology Preview feature. This feature relies on the newly introduced Shared Resource CSI Driver and the Insights Operator to import RHEL Simple Content Access (SCA) certificates. For example, by using this feature, you can run entitled builds with **SharedSecret** objects and install entitled RPM packages during builds rather than copying your RHEL subscription credentials and certificates into the builds' namespaces. (BUILD-274)



IMPORTANT

The **SharedSecret** objects and OpenShift Shared Resources feature are only available if you enable the **TechPreviewNoUpgrade** feature set. These Technology Preview features are not part of the default features. Enabling this feature set cannot be undone and prevents upgrades. This feature set is not recommended on production clusters. See Enabling Technology Preview features using FeatureGates.

- With this update, workloads can securely share **Secrets** and **ConfigMap** objects across namespaces using inline ephemeral **csi** volumes provided by the Shared Resource CSI Driver. Container Storage Interface (CSI) volumes and the Shared Resource CSI Driver are Technology Preview features. (BUILD-293)

1.3.15. Jenkins

- With this update, you can run Jenkins agents as sidecar containers. You can use this capability to run any container image in a Jenkins pipeline that has a correctly configured pod template and Jenkins file. Now, to compile code, you can run two new pod templates named **java-build** and **nodejs-builder** as sidecar containers with Jenkins. These two pod templates use the latest

Java and NodeJS versions provided by the **java** and **nodejs** image streams in the **openshift** namespace. The previous non-sidecar **maven** and **nodejs** pod templates have been deprecated. (JKNS-132)

1.3.16. Machine API

1.3.16.1. Azure Ephemeral OS disk support

With this enhancement, you can create a machine set running on Azure that deploys machines on Ephemeral OS disks. Ephemeral OS disks use local VM capacity rather than remote Azure Storage.

For more information, see Machine sets that deploy machines on Ephemeral OS disks .

1.3.16.2. Azure Accelerated Networking support

With this release, you can enable Accelerated Networking for Microsoft Azure VMs by using the Machine API. Accelerated Networking uses single root I/O virtualization (SR-IOV) to provide VMs with a more direct path to the switch.

For more information, see Accelerated Networking for Microsoft Azure VMs.

1.3.16.3. Global Azure availability set support

With this release, you can use availability sets in global Azure regions that do not have multiple availability zones to ensure high availability.

1.3.16.4. GPU support on Google Cloud Platform

Google Cloud Platform (GCP) Compute Engine enables users to add GPUs to VM instances. Workloads that benefit from access to GPU resources can perform better on compute machines with this feature enabled. With this release, you can define which supported GPU to use for an instance by using the Machine API.

For more information, see Enabling GPU support for a machine set.

1.3.16.5. Cluster autoscaler node utilization threshold

With this enhancement, you can specify a node utilization threshold in the **ClusterAutoscaler** resource definition. This threshold represents the node utilization level below which an unnecessary node is eligible for deletion.

For more information, see About the cluster autoscaler.

1.3.17. Machine Config Operator

1.3.17.1. Enhanced configuration drift detection

With this enhancement, the Machine Config Daemon (MCD) now checks nodes for configuration drift if a filesystem write event occurs for any of the files specified in the machine config and before a new machine config is applied, in addition to node bootup. Previously, the MCD checked for configuration drift only at node bootup. This change was made because node reboots do not occur frequently enough to avoid the problems caused by configuration drift until an administrator can correct the issue.

Configuration drift occurs when the on-disk state of a node differs from what is configured in the machine config. The Machine Config Operator (MCO) uses the MCD to check nodes for configuration drift and, if detected, sets that node and machine config pool (MCP) to **degraded**.

For more information about configuration drift, see Understanding configuration drift detection .

1.3.18. Nodes

1.3.18.1. Linux control groups version 2 (Developer Preview)

You can now enable Linux control groups version 2 (cgroups v2) on specific nodes in your cluster. The OpenShift Container Platform process for enabling cgroups v2 disables all cgroups version 1 controllers and hierarchies. The OpenShift Container Platform cgroups version 2 feature is in Developer Preview and is not supported by Red Hat at this time. For more information, see Enabling Linux control groups version 2 (cgroups v2).

1.3.18.2. Support for swap memory use on nodes (Technology Preview)

You can enable swap memory use for OpenShift Container Platform workloads on a per-node basis. For more information, see Enabling swap memory use on nodes.

1.3.18.3. Place nodes into maintenance mode by using the Node Maintenance Operator

The Node Maintenance Operator (NMO) cordons off nodes from the rest of the cluster and drains all the pods from the nodes. By placing nodes under maintenance, you can investigate problems with a machine, or perform operations on the underlying machine, that might result in a node failure. This is a standalone version of NMO. If you installed OpenShift Virtualization, then you must use the NMO that is bundled with it.

1.3.18.4. Node Health Check Operator enhancements (Technology Preview)

The Node Health Check Operator provides these new enhancements:

- Support for running in disconnected mode
- Prevent conflicts with machine health check. For more information, see About how node health checks prevent conflicts with machine health checks

1.3.18.5. Poison Pill Operator enhancements

The Poison Pill Operator uses **NodeDeletion** as its default remediation strategy. The **NodeDeletion** remediation strategy removes the **node** object.

In OpenShift Container Platform 4.10, the Poison Pill Operator introduces a new remediation strategy called **ResourceDeletion**. The **ResourceDeletion** remediation strategy removes the pods and associated volume attachments on the node rather than the **node** object. This strategy helps to recover workloads faster.

1.3.18.6. Control plane node migration on RHOSP

You can now migrate control plane nodes from one RHOSP host to another without encountering a service disruption.

1.3.19. Red Hat OpenShift Logging

In OpenShift Container Platform 4.7, *Cluster Logging* became *Red Hat OpenShift Logging*. For more information, see Release notes for Red Hat OpenShift Logging .

1.3.20. Monitoring

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

1.3.20.1. Monitoring stack components and dependencies

Updates to versions of monitoring stack components and dependencies include the following:

- Alertmanager to 0.23.0
- Grafana to 8.3.4
- kube-state-metrics to 2.3.0
- node-exporter to 1.3.1
- prom-label-proxy to 0.4.0
- Prometheus to 2.32.1
- Prometheus adapter to 0.9.1
- Prometheus operator to 0.53.1
- Thanos to 0.23.1

1.3.20.2. New page for metrics targets in the OpenShift Container Platform web console

A new **Metrics Targets** page in the OpenShift Container Platform web console shows targets for default OpenShift Container Platform projects and for user-defined projects. You can use this page to view, search, and filter the endpoints that are currently targeted for scraping, which helps you to identify and troubleshoot problems.

1.3.20.3. Monitoring components updated to use TLS authentication for metrics collection

With this release, all monitoring components are now configured to use mutual TLS authentication, rather than Bearer Token static authentication for metrics collection. TLS authentication is more resilient to Kubernetes API outages and decreases the load on the Kubernetes API.

1.3.20.4. Cluster Monitoring Operator updated to use the global TLS security profile

With this release, the Cluster Monitoring Operator components now honor the global OpenShift Container Platform **tlsSecurityProfile** settings. The following components and services now use the TLS security profile:

- Alertmanager pods (ports 9092 and 9097)
- kube-state-metrics pod (ports 8443 and 9443)
- openshift-state-metrics pod (ports 8443 and 9443)
- node-exporter pods (port 9100)

- Grafana pod (port 3002)
- prometheus-adapter pods (port 6443)
- prometheus-k8s pods (ports 9092 and 10902)
- Thanos query pods (ports 9092, 9093 and 9094)
- Prometheus Operator (ports 8080 and 8443)
- telemeter-client pod (port 8443)

If you have enabled user-defined monitoring, the following pods now use the profile:

- prometheus-user-workload pods (ports 9091 and 10902)
- prometheus-operator pod (ports 8080 and 8443)

1.3.20.5. Changes to alerting rules

- New
  - Added a **namespace** label to all Thanos alerting rules.
  - Added the **openshift_io_alert_source="platform"** label to all platform alerts.
- Changed
  - Renamed **AggregatedAPIDown** to **KubeAggregatedAPIDown**.
  - Renamed **AggregatedAPIErrors** to **KubeAggregatedAPIErrors**.
  - Removed the **HighlyAvailableWorkloadIncorrectlySpread** alert.
  - Improved the description of the **KubeMemoryOvercommit** alert.
  - Improved **NodeFilesystemSpaceFillingUp** alerts to make it consistent with the Kubernetes garbage collection thresholds.
  - Excluded **ReadOnlyMany** volumes from the **KubePersistentVolumeFillingUp** alerts.
  - Extended **PrometheusOperator** alerts to include the Prometheus operator running in the **openshift-user-workload-monitoring** namespace.
  - Replaced the **ThanosSidecarPrometheusDown** and **ThanosSidecarUnhealthy** alerts by **ThanosSidecarNoConnectionToStartedPrometheus**.
  - Changed the severity of **KubeletTooManyPods** from **warning** to **info**.
  - Enabled exclusion of specific persistent volumes from **KubePersistentVolumeFillingUp** alerts by adding the **alerts.k8s.io/KubePersistentVolumeFillingUp: disabled** label to a persistent volume resource.

NOTE

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

1.3.20.6. Changes to metrics

- Pod-centric cAdvisor metrics available at the slice level have been dropped.
- The following metrics are now exposed:
  - **kube_poddisruptionbudget_labels**
  - **kube_persistentvolumeclaim_labels**
  - **kube_persistentvolume_labels**
- Metrics with the name **kube_*annotation** have been removed from **kube-state-metrics**.

NOTE

Red Hat does not guarantee backward compatibility for metrics.

1.3.20.7. Added hard anti-affinity rules and pod disruption budgets for certain components

With this release, hard anti-affinity rules and pod disruption budgets have been enabled for the following monitoring components to reduce downtime during patch upgrades:

- Alertmanager

NOTE

As part of this change, the number of Alertmanager replicas has been reduced from three to two. However, the persistent volume claim (PVC) for the removed third replica is not automatically removed as part of the upgrade process. If you have configured persistent storage for Alertmanager, you can remove this PVC manually from the Cluster Monitoring Operator. See the "Known Issues" section for more information.

- Prometheus adapter
- Prometheus
- Thanos Querier

If you have enabled user-defined monitoring, the following components also use these rules and budgets:

- Prometheus
- Thanos Ruler

1.3.20.8. Alert routing for user-defined projects (Technology Preview)

This release introduces a Technology Preview feature in which an administrator can enable alert routing for user-defined projects monitoring. Users can then add and configure alert routing for their user-defined projects.

1.3.20.9. Alertmanager

Access to the third-party Alertmanager web user interface from the OpenShift Container Platform route has been removed.

1.3.20.10. Prometheus

- OpenShift Container Platform cluster administrators can now configure query logging for Prometheus.
- Access to the third-party Prometheus web user interface is deprecated and will be removed in a future OpenShift Container Platform release.

1.3.20.11. Prometheus adapter

- The Prometheus adapter now uses the Thanos Querier API rather than the Prometheus API.
- OpenShift Container Platform cluster administrators can now configure audit logs for the Prometheus adapter.

1.3.20.12. Thanos Querier

- Access to the third-party Thanos Querier web user interface from the OpenShift Container Platform route has been removed.
- The **/api/v1/labels**, **/api/v1/label/*/values**, and **/api/v1/series** endpoints on the Thanos Querier tenancy port are now exposed.
- OpenShift Container Platform cluster administrators can now configure query logging.
- If user workload monitoring is enabled, access to the third-party Thanos Ruler web user interface from the OpenShift Container Platform route has been removed.

1.3.20.13. Grafana

Access to the third-party Grafana web user interface is deprecated and will be removed in a future OpenShift Container Platform release.

1.3.21. Scalability and performance

1.3.21.1. New Special Resource Operator metrics

The Special Resource Operator (SRO) now exposes metrics to help you watch the health of your SRO custom resources and objects. For more information, see Prometheus Special Resource Operator metrics.

1.3.21.2. Special Resource Operator custom resource definition fields

Using **oc explain** for Special Resource Operator (SRO) now provides online documentation for SRO custom resource definitions (CRD). This enhancement provides better specifics for CRD fields. (BZ#2031875)

1.3.21.3. New Node Tuning Operator metric added to Telemetry

A Node Tuning Operator (NTO) metric is now added to Telemetry. Follow the procedure in Showing data collected by Telemetry to see all the metrics collected by Telemetry.

1.3.21.4. NFD Topology Updater is now available

The Node Feature Discovery (NFD) Topology Updater is a daemon responsible for examining allocated resources on a worker node. It accounts for resources that are available to be allocated to new pod on a per-zone basis, where a zone can be a Non-Uniform Memory Access (NUMA) node. See Using the NFD Topology Updater for more information.

1.3.21.5. Hyperthreading-aware CPU manager policy (Technology Preview)

Hyperthreading-aware CPU manager policy in OpenShift Container Platform is now available without the need for extra tuning. The cluster administrator can enable this feature if required. Hyperthreads are abstracted by the hardware as logical processors. Hyperthreading allows a single physical processor to execute two heavyweight threads (processes) at the same time, dynamically sharing processor resources.

1.3.21.6. NUMA-aware scheduling with NUMA Resources Operator (Technology Preview)

The default OpenShift Container Platform scheduler does not see individual non-uniform memory access (NUMA) zones in the compute node. This can lead to sub-optimal scheduling of latency-sensitive workloads. A new NUMA Resources Operator is available which deploys a NUMA-aware secondary scheduler. The NUMA-aware secondary scheduler makes scheduling decisions for workloads based on a complete picture of available NUMA zones in the cluster. This ensures that latency-sensitive workloads are processed in a single NUMA zone for maximum efficiency and performance.

For more information, see About NUMA-aware scheduling.

1.3.21.7. Filtering custom resources during ZTP spoke cluster installation using SiteConfig filters

You can now use filters to customize **SiteConfig** CRs to include or exclude other CRs for use in the installation phase of the zero touch provisioning (ZTP) GitOps pipeline. For more information, see Filtering custom resources using SiteConfig filters .

1.3.21.8. Disable chronyd in the PolicyGenTemplate CR for vDU use cases

On nodes running RAN vDU applications, you must disable **chronyd** if you update to OpenShift Container Platform 4.10 from earlier versions. To disable **chronyd**, add the following line in the **[service]** section under **.spec.profile.data** of the **TunedPerformancePatch.yaml** file. The **TunedPerformancePatch.yaml** file is referenced in the group **PolicyGenTemplate** CR:

```
[service]
service.chronyd=stop,disable
```

For more information, Recommended cluster configurations to run vDU applications .

1.3.22. Backup and restore

1.3.23. Developer experience

1.3.23.1. Pruning deployment replica sets (Technology Preview)

This release introduces a Technology Preview flag **--replica-sets** to the **oc adm prune deployments** command. By default, only replication controllers are pruned with the **oc adm prune deployments** command. When you set **--replica-sets** to **true**, replica sets are also included in the pruning process.

For more information, see Pruning deployment resources.

1.3.24. Insights Operator

1.3.24.1. Importing simple content access certificates

In OpenShift Container Platform 4.10, Insights Operator now imports your simple content access certificates from Red Hat OpenShift Cluster Manager by default.

For more information, see Importing simple content access certificates with Insights Operator .

1.3.24.2. Insights Operator data collection enhancements

To reduce the amount of data sent to Red Hat, Insights Operator only gathers information when certain conditions are met. For example, Insights Operator only gathers the Alertmanager logs when Alertmanager fails to send alert notifications.

In OpenShift Container Platform 4.10, the Insights Operator collects the following additional information:

- (Conditional) The logs from pods where the **KubePodCrashlooping** and **KubePodNotReady** alerts are firing
- (Conditional) The Alertmanager logs when the **AlertmanagerClusterFailedToSendAlerts** or **AlertmanagerFailedToSendAlerts** alerts are firing
- Silenced alerts from Alertmanager
- The node logs from the journal unit (kubelet)
- The **CostManagementMetricsConfig** from clusters with **costmanagement-metrics-operator** installed
- The time series database status from the monitoring stack Prometheus instance
- Additional information about the OpenShift Container Platform scheduler

With this additional information, Red Hat improves OpenShift Container Platform functionality and enhances Insights Advisor recommendations.

1.3.25. Authentication and authorization

1.3.25.1. Syncing group membership from OpenID Connect identity providers

This release introduces support for synchronizing group membership from an OpenID Connect provider to OpenShift Container Platform upon user login. You can enable this by configuring the **groups** claim in the OpenShift Container Platform OpenID Connect identity provider configuration.

For more information, see Sample OpenID Connect CRs.

1.3.25.2. Additional supported OIDC providers

The Okta and Ping Identity OpenID Connect (OIDC) providers are now tested and supported with OpenShift Container Platform.

For the full list of OIDC providers, see Supported OIDC providers .

1.3.25.3. oc commands now obtain credentials from Podman configuration locations

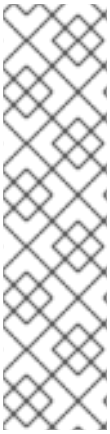
Previously, **oc** commands that used the registry configuration, for example **oc registry login** or **oc image** commands, obtained credentials from Docker configuration locations. With OpenShift Container Platform 4.10, if a registry entry cannot be found in the default Docker configuration location, **oc** commands obtain the credentials from Podman configuration locations. You can set your preference to either **docker** or **podman** by using the **REGISTRY_AUTH_PREFERENCE** environment variable to prioritize the location.

Users also have the option to use the **REGISTRY_AUTH_FILE** environment variable, which serves as an alternative to the existing **--registry-config** CLI flag. The **REGISTRY_AUTH_FILE** environment variable is also compatible with **podman**.

1.3.25.4. Support for Google Cloud Platform Workload Identity

You can now use the Cloud Credential Operator (CCO) utility **ccoctl** to configure the CCO to use the Google Cloud Platform Workload Identity. When the CCO is configured to use GCP Workload Identity, the in-cluster components can impersonate IAM service accounts using short-term, limited-privilege security credentials to components.

For more information, see Using manual mode with GCP Workload Identity .



NOTE

In OpenShift Container Platform 4.10.8, image registry support for using GCP Workload Identity was removed due to the discovery of an adverse impact to the image registry . To use the image registry on an OpenShift Container Platform 4.10.8 cluster that uses Workload Identity, you must configure the image registry to use long-lived credentials instead.

With OpenShift Container Platform 4.10.21, support for using GCP Workload Identity with the image registry is restored. For more information about the status of this feature between OpenShift Container Platform 4.10.8 and 4.10.20, see the related Knowledgebase article.

1.4. NOTABLE TECHNICAL CHANGES

OpenShift Container Platform 4.10 introduces the following notable technical changes.

TLS X.509 certificates must have a Subject Alternative Name
X.509 certificates must have a properly set the Subject Alternative Name field. If you update your cluster without this, you risk breaking your cluster or rendering it inaccessible.

In older versions of OpenShift Container Platform, X.509 certificates worked without a Subject Alternative Name, so long as the Common Name field was set. This behavior was removed in OpenShift Container Platform 4.6.

In some cases, certificates without a Subject Alternative Name continued to work in OpenShift Container Platform 4.6, 4.7, 4.8, and 4.9. Because it uses Kubernetes 1.23, OpenShift Container Platform 4.10 does not allow this under any circumstances.

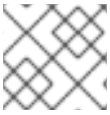
Cloud controller managers for additional cloud providers
The Kubernetes community plans to deprecate the Kubernetes controller manager in favor of using cloud controller managers to interact with underlying cloud platforms. As a result, there is no plan to add Kubernetes controller manager support for any new cloud platforms. The implementation that is added in this release of OpenShift Container Platform supports using cloud controller managers for Google Cloud Platform (GCP), VMware vSphere, IBM Cloud, and Alibaba Cloud as a Technology Preview.

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

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

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

Operator SDK v1.16.0
OpenShift Container Platform 4.10 supports Operator SDK v1.16.0. See Installing the Operator SDK CLI to install or update to this latest version.



NOTE

Operator SDK v1.16.0 supports Kubernetes 1.22.

Many deprecated **v1beta1** APIs were removed in Kubernetes 1.22, including **sigs.k8s.io/controller-runtime v0.10.0** and **controller-gen v0.7**. This is a breaking change if you need to scaffold **v1beta1** APIs for custom resource definitions (CRDs) or webhooks to publish your project into older cluster versions.

For more information about changes introduced in Kubernetes 1.22, see Validating bundle manifests for APIs removed from Kubernetes 1.22 and Beta APIs removed from Kubernetes 1.22 in the OpenShift Container Platform 4.9 release notes.

If you have any Operator projects that were previously created or maintained with Operator SDK v1.10.1, see Upgrading projects for newer Operator SDK versions to ensure your projects are upgraded to maintain compatibility with Operator SDK v1.16.0.

Changed Cluster Autoscaler alert severity
Previously, the **ClusterAutoscalerUnschedulablePods** alert showed a severity of **warning**, which suggested it required developer intervention. This alert is informational and does not describe a problematic condition that requires intervention. With this release, the **ClusterAutoscalerUnschedulablePods** alert is reduced in severity from **warning** to **info**. (BZ#2025230)

Network Observability operator for observing network flows
The Network Observability Operator is General Availability (GA) status in the 4.12 release of OpenShift Container Platform and is also supported in OpenShift Container Platform 4.10.

For more information, see Network Observability.

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 4.10, refer to the table below. Additional details for more fine-grained functionality that has been deprecated and removed are listed after the table.

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

- **GA**: *General Availability*
- **DEP**: *Deprecated*
- **REM**: *Removed*

Table 1.1. Deprecated and removed features tracker

Feature	OCP 4.8	OCP 4.9	OCP 4.10
Package manifest format (Operator Framework)	REM	REM	REM
SQLite database format for Operator catalogs	GA	DEP	DEP
oc adm catalog build	REM	REM	REM
--filter-by-os flag for **oc adm catalog mirror**	REM	REM	REM
v1beta1 CRDs	DEP	REM	REM
Docker Registry v1 API	DEP	REM	REM
Metering Operator	DEP	REM	REM
Scheduler policy	DEP	DEP	REM
ImageChangesInProgress condition for Cluster Samples Operator	DEP	DEP	DEP
MigrationInProgress condition for Cluster Samples Operator	DEP	DEP	DEP
Use of **v1** without a group in **apiVersion** for OpenShift Container Platform resources	DEP	REM	REM
Use of **dhclient** in RHCOS	DEP	REM	REM
Cluster Loader	DEP	DEP	REM
Bring your own RHEL 7 compute machines	DEP	DEP	REM
lastTriggeredImageID field in the **BuildConfig** spec for Builds	DEP	REM	REM

Feature	OCP 4.8	OCP 4.9	OCP 4.10
Jenkins Operator	DEP	DEP	REM
HPA custom metrics adapter based on Prometheus	REM	REM	REM
vSphere 6.7 Update 2 or earlier	GA	DEP	DEP
Virtual hardware version 13	GA	DEP	DEP
VMware ESXi 6.7 Update 3 or earlier	GA	DEP	DEP
Minting credentials for Microsoft Azure clusters	GA	GA	REM
Persistent storage using FlexVolume			DEP
Non-sidecar pod templates for Jenkins			DEP
Multicluster console (Technology Preview)			REM

1.5.1. Deprecated features

1.5.1.1. IBM POWER8, IBM z13 all models, LinuxONE Emperor, LinuxONE Rockhopper, and x86_64 v1 architectures will be deprecated

RHCOS functionality in IBM POWER8, IBM z13 all models, LinuxONE Emperor, LinuxONE Rockhopper, and AMD64 (x86_64) v1 CPU architectures will be deprecated in an upcoming release. Additional details for when support will discontinue for these architectures will be announced in a future release.

NOTE

AMD and Intel 64-bit architectures (x86-64-v2) will still be supported.

1.5.1.2. Default Docker configuration location deprecation

Previously, **oc** commands that used a registry configuration would obtain credentials from the Docker configuration location, which was **~/.docker/config.json** by default. This has been deprecated and will be replaced by a Podman configuration location in a future version of OpenShift Container Platform.

1.5.1.3. Empty file and stdout support deprecation in oc registry login

Support for empty files using the **--registry-config** and **--to** flags in **oc registry login** has been deprecated. Support for **-** (standard output) has also been deprecated as an argument when using **oc registry login**. They will be removed in a future version of OpenShift Container Platform.

1.5.1.4. Non-sidecar pod templates for Jenkins deprecation

In OpenShift Container Platform 4.10, the non-sidecar **maven** and **nodejs** pod templates for Jenkins are deprecated. These pod templates are planned for removal in a future release. Bug fixes and support

are provided through the end of that future life cycle, after which no new feature enhancements are made. Instead, with this update, you can run Jenkins agents as sidecar containers. (JKNS-257)

1.5.1.5. Third-party monitoring components user interface deprecation

For the following monitoring stack components, access to third-party web user interfaces (UIs) is deprecated and is planned to be removed in a future OpenShift Container Platform release:

- Grafana
- Prometheus

As an alternative, users can navigate to the **Observe** section of the OpenShift Container Platform web console to access dashboards and other UIs for platform components.

1.5.1.6. Persistent storage using FlexVolume

In OpenShift Container Platform 4.10, persistent storage using FlexVolume is deprecated. This feature is still fully supported, but only important bugs will be fixed. However, it may be removed in a future OpenShift Container Platform release. Out-of-tree Container Storage Interface (CSI) driver is the recommended way to write volume drivers in OpenShift Container Platform. Maintainers of FlexVolume drivers should implement a CSI driver and move users of FlexVolume to CSI. Users of FlexVolume should move their workloads to CSI driver.

1.5.1.7. RHEL 7 support for the OpenShift CLI (oc) is deprecated

Support for using Red Hat Enterprise Linux (RHEL) 7 with the OpenShift CLI (**oc**) is deprecated and will be removed in a future OpenShift Container Platform release.

1.5.2. Removed features

OpenShift Container Platform 4.10 removes the Jenkins Operator, which was a Technology Preview feature, from the **OperatorHub** page in the OpenShift Container Platform web console interface. Bug fixes and support are no longer available.

Instead, you can continue to deploy Jenkins on OpenShift Container Platform by using the templates provided by the Samples Operator. Alternatively, you can install the Jenkins Helm Chart from the Developer Catalog by using the **Helm** page in the **Developer** perspective of the web console.

1.5.2.1. OpenShift CLI (oc) commands removed

The following OpenShift CLI (**oc**) commands were removed with this release:

- **oc adm completion**
- **oc adm config**
- **oc adm options**

1.5.2.2. Scheduler policy removed

Support for configuring a scheduler policy has been removed with this release. Use a scheduler profile instead to control how pods are scheduled onto nodes.

1.5.2.3. RHEL 7 support for compute machines removed

Support for running Red Hat Enterprise Linux (RHEL) 7 compute machines in OpenShift Container Platform has been removed. If you prefer using RHEL compute machines, they must run on RHEL 8.

You cannot upgrade RHEL 7 compute machines to RHEL 8. You must deploy new RHEL 8 hosts, and the old RHEL 7 hosts must be removed.

1.5.2.4. Third-party monitoring component user interface access removed

With this release, you can no longer access third-party web user interfaces (UIs) for the following monitoring stack components:

- Alertmanager
- Thanos Querier
- Thanos Ruler (if user workload monitoring is enabled)

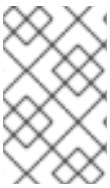
Instead, you can navigate to the **Observe** section of the OpenShift Container Platform web console to access metrics, alerting, and metrics targets UIs for platform components.

1.5.2.5. Support for minting credentials for Microsoft Azure removed

Support for using the Cloud Credential Operator (CCO) in mint mode on Microsoft Azure clusters has been removed. This change is due to the planned retirement of the Azure AD Graph API by Microsoft on 30 June 2022 and is being backported to all supported versions of OpenShift Container Platform in z-stream updates.

For previously installed Azure clusters that use mint mode, the CCO attempts to update existing secrets. If a secret contains the credentials of previously minted app registration service principals, it is updated with the contents of the secret in **kube-system/azure-credentials**. This behavior is similar to passthrough mode.

For clusters with the credentials mode set to its default value of **""**, the updated CCO automatically changes from operating in mint mode to operating in passthrough mode. If your cluster has the credentials mode explicitly set to mint mode (**"Mint"**), you must change the value to **""** or **"Passthrough"**.



NOTE

In addition to the **Contributor** role that is required by mint mode, the modified app registration service principals now require the **User Access Administrator** role that is used for passthrough mode.

While the Azure AD Graph API is still available, the CCO in upgraded versions of OpenShift Container Platform attempts to clean up previously minted app registration service principals. Upgrading your cluster before the Azure AD Graph API is retired might avoid the need to clean up resources manually.

If the cluster is upgraded to a version of OpenShift Container Platform that no longer supports mint mode after the Azure AD Graph API is retired, the CCO sets an **OrphanedCloudResource** condition on the associated **CredentialsRequest** but does not treat the error as fatal. The condition includes a message similar to **unable to clean up App Registration / Service Principal:**

<app_registration_name>. Cleanup after the Azure AD Graph API is retired requires manual intervention using the Azure CLI tool or the Azure web console to remove any remaining app registration service principals.

To clean up resources manually, you must find and delete the affected resources.

1. Using the Azure CLI tool, filter the app registration service principals that use the **<app_registration_name>** from an **OrphanedCloudResource** condition message by running the following command:

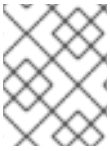
```
$ az ad app list --filter "displayname eq '<app_registration_name>'" --query '[].objectId'
```

Example output

```
[
  "038c2538-7c40-49f5-abe5-f59c59c29244"
]
```

2. Delete the app registration service principal by running the following command:

```
$ az ad app delete --id 038c2538-7c40-49f5-abe5-f59c59c29244
```



NOTE

After cleaning up resources manually, the **OrphanedCloudResource** condition persists because the CCO cannot verify that the resources were cleaned up.

1.6. BUG FIXES

Bare Metal Hardware Provisioning

- Previously, using a MAC address to configure a provisioning network interface was unsupported when switching the provisioning network from **Disabled** to **Managed**. With this update, a **provisioningMacAddresses** field is added to the **provisioning.metal3.io** CRD. Use this field to identify the provisioning network interface using its MAC address rather than its name. (BZ#2000081)

- Previously, Ironic failed to attach virtual media images for provisioning SuperMicro X11/X12 servers because these models expect a non-standard device string, for example **UsbCd**, for CD-based virtual media. With this update, provisioning now overrides **UsbCd** on SuperMicro machines provisioned with CD-based virtual media. (BZ#2009555)

- Previously, Ironic failed to attach virtual media images on SuperMicro X11/X12 servers due to overly restrictive URl validations on the BMCs of these machines. With this update, the **filename** parameter has now been removed from the URL if the virtual media image is backed by a local file. As a result, the parameter still passes if the image is backed by an object store. (BZ#2011626)

- Previously, the **curl** utility, used by the machine downloader image, did not support classless inter-domain routing (CIDR) with **no_proxy**. A a result, any CIDR in `noProxy` was ignored when downloading the Red Hat Enterprise Linux CoreOS (RHCOS) image. With this update, proxies are now removed from the environment before calling **curl** when appropriate. As a result, when downloading the machine image, any CIDR in **no_proxy** is no longer ignored. (BZ#1990556)

- Previously, virtual media based deployments of OpenShift Container Platform have been observed to intermittently fail on iDRAC hardware types. This occurred when outstanding Lifecycle Controller jobs clashed with virtual media configuration requests. With this update, virtual media deployment failure has been fixed by purging any Lifecycle Controller job while registering iDRAC hardware prior to deployment. (BZ#1988879)

- Previously, users had to enter a long form of an IPv6 address in the installation configuration file, for example **2001:0db8:85a3:0000:0000:8a2e:0370:7334**. Ironic could not find an interface matching this IP address causing the installation to fail. With this update, the IPv6 address supplied by the user is converted to a short form address, for example, **2001:db8:85a3::8a2e:370:7334**. As a result, installation is now successful. (BZ#2010698)

- Before this update, when a Redfish system features a Settings URI, the Ironic provisioning service always attempts to use this URI to make changes to boot-related BIOS settings. However, bare-metal provisioning fails if the Baseboard Management Controller (BMC) features a Settings URI but does not support changing a particular BIOS setting by using this Settings URI. In OpenShift Container Platform 4.10 and later, if a system features a Settings URI, Ironic verifies that it can change a particular BIOS setting by using the Settings URI before proceeding. Otherwise, Ironic implements the change by using the System URI. This additional logic ensures that Ironic can apply boot-related BIOS setting changes and bare-metal provisioning can succeed. (OCPBUGS-6886)

Builds

- Before this update, if you created a build configuration containing an image change trigger in OpenShift Container Platform 4.7.x or earlier, the image change trigger might trigger builds continuously.
  This issue happened because, with the deprecation and removal of the **lastTriggeredImageID** field from the **BuildConfig** spec for Builds, the image change trigger controller stopped checking that field before instantiating builds. OpenShift Container Platform 4.8 introduced new fields in the status that the image change trigger controller needed to check, but did not.

  With this update, the image change trigger controller continuously checks the correct fields in the spec and status for the last triggered image ID. Now, it only triggers a build when necessary. (BZ#2004203)

- Before this update, image references in Builds needed to specify the Red Hat registry name explicitly. With this update, if an image reference does not contain the registry, the Build searches the Red Hat registries and other well-known registries to locate the image. (BZ#2011293)

Jenkins

- Before this update, version 1.0.48 of the OpenShift Jenkins Sync Plugin introduced a **NullPointerException** error when Jenkins notified the plugin of new jobs that were not associated with an OpenShift Jenkins Pipeline Build Strategy Build Config. Ultimately, this error was benign because there was no **BuildConfig** object to associate with the incoming Jenkins Job. Core Jenkins ignored the exception in our plugin and moved on to the next listener. However, a long stack trace showed up in the Jenkins log that distracted users. With this update, the plugin resolves the issue by making the proper checks to avoid this error and the subsequent stack trace. (BZ#2030692)

- Before this update, performance improvements in version 1.0.48 of the OpenShift Sync Jenkins plugin incorrectly specified the labels accepted for **ConfigMap** and **ImageStream** objects intended to map into the Jenkins Kubernetes plugin pod templates. As a result, the plugin no longer imported pod templates from **ConfigMap** and **ImageStream** objects with a **jenkins-agent** label.

This update corrects the accepted label specification so that the plugin imports pod templates from **ConfigMap** and **ImageStream** objects that have the **jenkins-agent** label. (2034839)

Cloud Compute

- Previously, editing a machine specification on Red Hat OpenStack Platform (RHOSP) would cause OpenShift Container Platform to attempt to delete and recreate the machine. As a result, this caused an unrecoverable loss of the node it was hosting. With this fix, any edits made to the machine specification after creation are ignored. (BZ#1962066)

- Previously, on clusters that run on Red Hat OpenStack Platform (RHOSP), floating IP addresses were not reported for machine objects. As a result, certificate signing requests (CSRs) that the kubelet created were not accepted, preventing nodes from joining the cluster. All IP addresses are now reported for machine objects. (BZ#2022627)

- Previously, the check to ensure that the AWS machine was not updated before requeueing was removed. Consequently, problems arose when the AWS machine's virtual machine had been removed, but its object was still available. If this happens, the AWS machine would requeue in an infinite loop and could not be deleted or updated. This update restores the check that was used to ensure that the AWS machine was not updated before requeueing. As a result, machines no longer requeue if they have been updated. (BZ#2007802)

- Previously, modifying a selector changed the list of machines that a machine set observed. As a result, leaks could occur because the machine set lost track of machines it had already created. This update ensures that the selector is immutable once created. As a result, machine sets now lists the correct machines. (BZ#2005052)

- Previously, if a virtual machine template had snapshots, an incorrect disk size was picked due to an incorrect usage of the **linkedClone** operation. With this update, the default clone operation is changed to **fullClone** for all situations. **linkedClone** must now be specified by the user. (BZ#2001008)

- Previously, the custom resource definition (CRD) schema requirements did not allow numeric values. Consequently, marshaling errors occurred during upgrades. This update corrects the schema requirements to allow both string and numeric values. As a result, marshaling errors are no longer reported by the API server conversion. (BZ#1999425)

- Previously, if the Machine API Operator was moved, or the pods were deployed as a result of a name change, the **MachineNotYetDeleted** metric would reset for each monitored machine. This update changes the metric query to ignore the source pod label. As a result, the **MachineNotYetDeleted** metric now properly alerts in scenarios where the Machine API Operator pod has been renamed. (BZ#1986237)

- Previously, egress IPs on vSphere were picked up by the vSphere cloud provider within the kubelet. These were unexpected by the certificate signing requests (CSR) approver. Consequently, nodes with egress IPs would not have their CSR renewals approved. This update allows the CSR approver to account for egress IPs. As a result, nodes with egress IPs on vSphere SDN clusters now continue to function and have valid CSR renewals. (BZ#1860774)

- Previously, worker nodes failed to start, and the installation program failed to generate URL images due to the broken path defaulting for the disk image and incompatible changes in the Google Cloud Platform (GCP) SDK. As a result, the machine controller was unable to create machines. This fix repairs the URL images by changing the base path in the GCP SDK. (BZ#2009111)

- Previously, the machine would freeze during the deletion process due to a lag in the vCenter's **powerOff** task. VMware showed the machine to be powered off, but OpenShift Container

Platform reported it to be powered on, which resulted in the machine freezing during the deletion process. This update improves the **powerOff** task handling on vSphere to be checked before the task to delete from the database is created, which prevents the machine from freezing during the deletion process. (BZ#2011668)

- After installing or updating OpenShift Container Platform, the value of the metrics showed one pending CSR after the last CSR was reconciled. This resulted in the metrics reporting one pending CSR when there should be no pending CSRs. This fix ensures the pending CSR count is always valid post-approval by updating the metrics at the end of each reconcile loop. (BZ#2013528)

- Previously, AWS checked for credentials when the **cloud-provider** flag was set to empty string. The credentials were checked by making calls to the metadata service, even on non-AWS platforms. This caused latency in the ECR provider startup and AWS credential errors logged in all platforms, including non-AWS. This fix prevents the credentials check from making any requests to the metadata service to ensure that credential errors are no longer being logged. (BZ#2015515)

- Previously, the Machine API sometimes reconciled a machine before AWS had communicated VM creation across its API. As a result, AWS reported the VM does not exist and the Machine API considered it failed. With this release, the Machine API waits until the AWS API has synched before trying to mark the machine as provisioned. (BZ#2025767)

- Previously, a large volume of nodes created simultaneously on UPI clusters could lead to a large number of CSRs being generated. As a result, certificate renewals were not automated because the approver stops approving certificates when there are over 100 pending certificate requests. With this release, existing nodes are accounted for when calculating the approval cut-off and UPI clusters can now benefit from automated certificate renewal even with large scale refresh requests. (BZ#2028019)

- Previously, the generated list of instance types embedded in Machine API controllers was out of date. Some of these instance types were unknown and could not be annotated for scale-from-zero requirements. With this release, the generated list is updated to include support for newer instance types. (BZ#2040376)

- Previously, AWS Machine API controllers did not set the IOPS value for block devices other than the IO1 type, causing IOPS fields for GP3 block devices to be ignored. With this release, the IOPS is set on all supported block device types and users can set IOPS for block devices that are attached to the machine. (BZ#2040504)

Cloud Credential Operator

- Previously, when using the Cloud Credential Operator in manual mode on an Azure cluster, the **Upgradeable** status was not set to **False**. This behavior was different for other platforms. With this release, Azure clusters using the Cloud Credential Operator in manual mode have the **Upgradeable** status set to **False**. (BZ#1976674)

- Previously, the now unnecessary **controller-manager-service** service resource that was created by the Cloud Credential Operator was still present. With this release, the Cluster Version Operator cleans it up. (BZ#1977319)

- Previously, changes to the log level setting for the Cloud Credential Operator in the **CredentialsRequest** custom resource were ignored. With this release, logging verbosity can be controlled by editing the **CredentialsRequest** custom resource. (BZ#1991770)

- Previously, the Cloud Credential Operator (CCO) pod restarted with a continuous error when AWS was the default secret annotator for Red Hat OpenStack Platform (RHOSP). This update

fixes the default setting for the CCO pod and prevents the CCO pod from failing. (BZ#1996624)

Cluster Version Operator

- Previously, a pod might fail to start due to an invalid mount request that was not a part of the manifest. With this update, the Cluster Version Operator (CVO) removes any volumes and volume mounts from in-cluster resources that are not included in the manifest. This allows pods to start successfully. (BZ#2002834)

- Previously, when monitoring certificates were rotated, the Cluster Version Operator (CVO) would log errors and monitoring would be unable to query metrics until the CVO pod was manually restarted. With this update, the CVO monitors the certificate files and automatically recreates the metrics connection whenever the certificate files change. (BZ#2027342)

Console Storage Plugin

- Previously, a loading prompt was not present while the persistent volumes (PVs) were being provisioned and the capacity was **0** TiB which created a confusing scenario. With this update, a loader is added for the loading state which provides details to the user if the PVs are still being provisioned or capacity is to be determined. It will also inform the user of any errors in the process. (BZ#1928285)

- Previously, the grammar was not correct in certain places and there were instances where translators were unable to interpret the context. This had a negative impact on readability. With this update, the grammar in various places is corrected, the storage classes for translators is itemized, and the overall readability is improved. (BZ#1961391)

- Previously, when pressing a pool inside the block pools page, the final **Ready** phase persisted after deletion. Consequently, the pool was in the **Ready** state even after deletion. This update redirects users to the **Pools** page and refreshes the pools after detention. (BZ#1981396)

Domain Name System (DNS)

- Previously, the DNS Operator did not cache responses from upstream resolvers that were configured using **spec.servers**. With this update, the DNS Operator now caches responses from all upstream servers. (BZ#2006803)

- Previously, the DNS Operator did not enable the **prometheus** pug-in in the server blocks for custom upstream resolvers. Consequently, CoreDNS did not report metrics for upstream resolvers and only reported metrics for the default server block. With this update, the DNS Operator was changed to enable the **prometheus** plugin in all server blocks. CoreDNS now reports Prometheus metrics for custom upstream resolvers. (BZ#2020489)

- Previously, an upstream DNS that provided a response greater than 512 characters caused an application to fail. This occurred because it could not clone the repository from GitHub because to DNS could not be resolved. With this update, the **bufsize** for KNI CoreDNS is set to 521 to avoid name resolutions from GitHub. (BZ#1991067)

- When the DNS Operator reconciles its operands, the Operator gets the cluster DNS service object from the API to determine whether the Operator needs to create or update the service. If the service already exists, the Operator compares it with what the Operator expects to get to determine whether an update is needed. Kubernetes 1.22, on which OpenShift Container Platform 4.9 is based, introduced a new **spec.internalTrafficPolicy** API field for services. The Operator leaves this field empty when it creates the service, but the API sets a default value for this field. The Operator was observing this default value and trying to update the field back to the empty value. This caused the Operator's update logic to continuously try to revert the

default value that the API set for the service's internal traffic policy. With this fix, when comparing services to determine whether an update is required, the Operator now treats the empty value and default value for **spec.internalTrafficPolicy** as equal. As a result, the Operator no longer spuriously tries to update the cluster DNS service when the API sets a default value for the service's **spec.internalTrafficPolicy field**. (BZ#2002461)

- Previously, the DNS Operator did not enable the cache plugin for server blocks in the CoreDNS **Corefile** configuration map corresponding to entries in the **spec.servers** field of the **dnses.operator.openshift.io/default** object. As a result, CoreDNS did not cache responses from upstream resolvers that were configured using **spec.servers**. With this bug fix, the DNS Operator is changed to enable the cache plugin for all server blocks, using the same parameters that the Operator already configured for the default server block. CoreDNS now caches responses from all upstream resolvers. (BZ#2006803)

Image Registry

- Previously, the registry internally resolved **\docker.io** references into **\registry-1.docker.io** and used it to store credentials. As a result, credentials for **\docker.io** images could not be located. With this update, the **\registry-1.docker.io** hostname has been changed back to **\docker.io** when searching for credentials. As a result, the registry can correctly find credentials for **\docker.io images**. (BZ#2024859)

- Previously, the image pruner job did not retry upon failure. As a result, a single failure could degrade the Image Registry Operator until the next time it ran. With this fix, the temporary problems with the pruner do not degrade the Image Registry Operator. (BZ#2051692)

- Previously, the Image Registry Operator was modifying objects from the informer. As a result, these objects could be concurrently modified by the informer and cause race conditions. With this fix, controllers and informers have different copies of the object and do not have race conditions. (BZ#2028030)

- Previously, **TestAWSFinalizerDeleteS3Bucket** would fail because of an issue with the location of the configuration object in the Image Registry Operator. This update ensures that the configuration object is stored in the correct location. As a result, the Image Registry Operator no longer panics when running **TestAWSFinalizerDeleteS3Bucket**. (BZ#2048443)

- Previously, error handling caused the **access denied** error to be output as **authentication required**. This bug resulted in incorrect error logs. Through Docker distribution error handling, the error output was changed from **authentication required** to **access denied**. Now the **access denied** error provides more precise error logs. (BZ#1902456)

- Previously, the registry was immediately exiting on a shut down request. As a result, the router did not have time to discover that the registry pod was gone and could send requests to it. With this fix, when the pod is deleted it stays active for a few extra seconds to give other components time to discover its deletion. Now, the router does not send requests to non-existent pods during upgrades, which no longer leads to disruptions. (BZ#1972827)

- Previously, the registry proxied response from the first available mirrored registry. When a mirror registry was available but did not have the requested data, pull-through did not try to use other mirrors even if they contained the required data. With this fix, pull-through tries other mirror registries if the first mirror replied with **Not Found**. Now, pull-through can discover data if it exists on any mirror registry. (BZ#2008539)

Image Streams

- Previously, the image policy admission plugin did not recognize deployment configurations, notably that stateful sets could be updated. As a result, image stream references stayed

unresolved in deployment configurations when the **resolve-names** annotation was used. Now, the plugin is updated so that it resolves annotations in deployment configurations and stateful sets. As a result, image stream tags get resolved in created and edited deployment configurations. (BZ#2000216)

- Previously, when global pull secrets were updated, existing API server pod pull secrets were not updated. Now, the mount point for the pull secret is changed from the **/var/lib/kubelet/config.json** file to the **/var/lib/kubelet** directory. As a result, the updated pull secret now appears in existing API server pods. (BZ#1984592)

- Previously, the image admission plugin did not check annotations inside deployment configuration templates. As a result, annotations inside deployment configuration templates could not be handled in replica controllers, and they were ignored. Now, the image admission plugin analyzes the template of deployment configurations. With this fix, the image admission plugin recognizes the annotations on the deployment configurations and on their templates. (BZ#2032589)

Installer

- The OpenShift Container Platform Baremetal IPI installer previously used the first nodes defined under hosts in **install-config** as control plane nodes rather than filtering for the hosts with the **master** role. The role of **master** and **worker** nodes is now recognized when defined. (BZ#2003113)

- Before this update, it was possible to set host bits in the provisioning network CIDR. This could cause the provisioning IP to differ from what was expected leading to conflict with other IP addresses on the provisioning network. With this update, validation ensures that the provisioning network CIDR cannot contain host bits. If a provisioning Network CIDR includes host bits, the installation program stops and logs an error message. (BZ#2006291)

- Previously, pre-flight checks did not account for Red Hat OpenStack Platform (RHOSP) resource utilization. As a result, those checks failed with an incorrect error message when utilization, rather than quota, impeded installation. Pre-flight checks now process both RHOSP quota and utilization. The checks fail with correct error messages if the quota is sufficient but resources are not. (BZ#2001317)

- Before this update, the oVirt Driver could specify ReadOnlyMany (ROX) and ReadWriteMany (RWX) access modes when creating a PVC from a configuration file. This caused an error because the driver does not support shared disks and, as a result, could not support these access modes. With this update, the access mode has been limited to single node access. The system prevents any attempt to specify ROX or RWX when creating PVC and logs an error message. (BZ#1882983)

- Previously, disk uploads in the Terraform provider were not handled properly. As a result, the OpenShift Container Platform installation program failed. With this update, disk upload handling has been fixed, and disk uploads succeed. (BZ#1917893)

- Previously, when installing a Microsoft Azure cluster with a special size, the installation program would check if the total number of virtual CPUs (vCPU) met the minimum resource requirement to deploy the cluster. Consequently, this could cause an install error. This update changes the check the installation program makes from the total number of vCPUs to the number of vCPUs available. As a result, a concise error message is given that lets the Operator know that the virtual machine size does not meet the minimum resource requirements. (BZ#2025788)

- Previously, RAM validation for Red Hat OpenStack Platform (RHOSP) checked for values using a wrong unit, and as a result the validation accepted flavors that did not meet minimum RAM requirements. With this fix, RAM validation now rejects flavors with insufficient RAM.

(BZ#2009699)

- Previously, OpenShift Container Platform control plane nodes were missing Ingress security group rules when they were schedulable and deployed on Red Hat OpenStack Platform (RHOSP). As a result, OpenShift Container Platform deployments on RHOSP failed for compact clusters with no dedicated workers. This fix adds Ingress security group rules on Red Hat OpenStack Platform (RHOSP) when control plane nodes are schedulable. Now, you can deploy compact three-node clusters on RHOSP. (BZ#1955544)

- Previously, if you specified an invalid AWS region, the installation program continued to try and validate availability zones. This caused the installation program to become unresponsive for 60 minutes before timing out. The installation program now verifies the AWS region and service endpoints before availability zones, which reduces the amount of time the installation program takes to report the error. (BZ#2019977)

- Previously, you could not install a cluster to VMware vSphere if the vCenter hostname began with a number. The installation program has been updated and no longer treats this type of hostname as invalid. Now, a cluster deploys successfully when the vCenter hostname begins with a number. (BZ#2021607)

- Previously, if you specified a custom disk instance type when deploying a cluster on Microsoft Azure, the cluster might not deploy. This occurred because the installation program incorrectly determined that the minimum resource requirements had been met. The installation program has been updated, and now reports an error when the number of vcpus available for the instance type in the selected region does not meet the minimum resource requirements. (BZ#2025788)

- Previously, if you defined custom IAM roles when deploying an AWS cluster, you might have to manually remove bootstrap instance profiles after uninstalling the cluster. Intermittently, the installation program did not remove bootstrap instance profiles. The installation program has been updated, and all machine instance profiles are removed when the cluster is uninstalled. (BZ#2028695)

- Previously, the default provisioningIP value was different when the host bits were set in the provisioning network CIDR. This resulted in a different value for the provisioningIP than expected. This difference caused a conflict with the other IP addresses on the provisioning network. This fix adds a validation to ensure that the ProvisioningNetworkCIDR does not have host bits set. As a result, if the ProvisioningNetworkCIDR has the host bits set, the installation program will stop and report the validation error. (BZ#2006291)

- Previously, the BMC driver IPMI was not supported for a secure UEFI boot. This resulted in an unsuccessful boot. This fix adds a validation check to ensure that **UEFISecureBoot** mode is not used with bare-metal drivers. As a result, a secure UEFI boot is successful. (BZ#2011893)

- With this update, the 4.8 UPI template is updated from version 3.1.0 to 3.2.0 to match the Ignition version. (BZ#1949672)

- Previously, when asked to mirror the contents of the base registry, the OpenShift Container Platform installation program would exit with a validation error, citing incorrect **install-config** file values for **imageContentSources**. With this update, the installation program now allows **imageContentSources** values to specify base registry names and the installation program no longer exits when specifying a base registry name. (BZ#1960378)

- Previously, the UPI ARM templates were attaching an SSH key to the virtual machine (VM) instances created. As a result, the creation of the VMs fails when the SSH key provided by the user is the **ed25519** type. With this update, the creation of the VMs succeeds regardless of the type of the SSH key provided by the user. (BZ#1968364)

- After successfully creating a **aws_vpc_dhcp_options_association** resource, AWS might still report that the resource does not exist. Consequently, the AWS Terraform provider fails the installation. With this update, you can retry the query of the **aws_vpc_dhcp_options_association** resource for a period of time after creation until AWS reports that the resource exists. As a result, installations succeed despite AWS reporting that the **aws_vpc_dhcp_options_association** resource does not exist. (BZ#2032521)

- Previously, when installing OpenShift Container Platform on AWS with local zones enabled, the installation program could create some resources on a local zone rather than an availability zone. This caused the installation program to fail because load balancers cannot run on local zones. With this fix, the installation program ignores local zones and only considers availability zones when installing cluster components. (BZ#1997059)

- Previously, terraform could attempt to upload the bootstrap ignition configuration file to Azure before it had finished creating the configuration file. If the upload started before the local file was created, the installation would fail. With this fix, terraform uploads the ignition configuration file directly to Azure rather than creating a local copy first. (BZ#2004313)

- Previously, a race condition could occur if the **cluster-bootstrap** and Cluster Version Operator components attempted to write a manifest for the same resource to the Kubernetes API at the same time. This could result in the **Authentication** resource being overwritten by a default copy, which removed any customizations made to that resource. With this fix, the Cluster Version Operator has been blocked from overwriting the manifests that come from the installation program. This prevents any user-specified customizations to the **Authentication** resource from being overwritten. (BZ#2008119)

- Previously, when installing OpenShift Container Platform on AWS, the installation program created the bootstrap machine using the **m5.large** instance type. This caused the installation to fail in regions where that instance type is not available. With this fix, the bootstrap machine uses the same instance type as the control plane machines. (BZ#2016955)

- Previously, when installing OpenShift Container Platform on AWS, the installation program did not recognize EC2 G and Intel Virtualization Technology (VT) instances and defaulted them to X instances. This caused incorrect instance quotas to be applied to these instances. With this fix, the installation program recognizes EC2 G and VT instances and applies the correct instance quotas. (BZ#2017874)

Kubernetes API server
Kubernetes Scheduler

- Before this update, upgrading to the current release did not set the correct weights for the **TaintandToleration**, **NodeAffinity**, and **InterPodAffinity** parameters. This update resolves the issue so that upgrading correctly sets the weights for **TaintandToleration** to **3**, **NodeAffinity** to **2**, and **InterPodAffinity** to **2**. (BZ#2039414)

- In OpenShift Container Platform 4.10, code for serving insecure metrics is removed from the **kube-scheduler** code base. Now, metrics are served only through a secure server. Bug fixes and support are provided through the end of a future life cycle. After which, no new feature enhancements are made. (BZ#1889488)

Machine Config Operator

- Previously, the Machine Config Operator (MCO) stored pending configuration changes to the disk before operating system (OS) changes were applied. As a result, in situations such as power loss, the MCO assumed OS changes had already been applied on restart, and validation skipped

over changes such as **kargs** and **kernel-rt**. With this update, configuration changes to disk are stored after OS changes are applied. Now, if power is lost during the configuration application, the MCO knows it must reattempt the configuration application on restart. (BZ#1916169)

- Previously, an old version of the Kubernetes client library in the **baremetal-runtimecfg** project prevented the timely closing of client connections following a VIP failover. This could result in long delays for monitor containers that rely on the API. This update allows the timely closing of client connections following a VIP failover. (BZ#1995021)

- Previously, when updating SSH keys, the Machine Config Operator (MCO) changed the owner and group of the **authorized_keys** file to **root**. This update ensures that the MCO preserves **core** as the owner and group when it updates the **authorized_keys** file. (BZ#1956739)

- Previously, a warning message sent by the **clone_slave_connection** function was incorrectly stored in a **new_uuid** variable, which is intended to store only the connection's UUID. As a result, **nmcli** commands that include the **new_uuid** variable were failing due to the incorrect value being stored in the **new_uuid** variable. With this fix, the **clone_slave_connection** function warning message is redirected to **stderr**. Now, **nmcli** commands that reference the **new_uuid** variable do not fail. (BZ#2022646)

- Previously, an old version of the Kubernetes client library was present in the **baremetal-runtimecfg** project. When a Virtual IP (VIP) failed, the client connections might not be closed in a timely manner. This could result in long delays for monitor containers that rely on talking to the API. This fix updates the client library. Now, connections are closed as expected on VIP failovers and the monitor containers do not hang for an excessive period of time. (BZ#1995021)

- Before this update, the Machine Config Operator (MCO) stored pending configuration changes to disk before it applied them to Red Hat Enterprise Linux CoreOS (RHCOS). If a power loss interrupted the MCO from applying the configuration, it treated the configuration as applied and did not validate the changes. If this configuration contained invalid changes, applying them failed. With this update, the MCO saves a configuration to disk only after being applied. This way, if the power is lost while the MCO is applying the configuration, it reapplies the configuration after it restarts. (BZ#1916169)

- Before this update, when you used the Machine Config Operator (MCO) to create or update an SSH key, it set the owner and group of the **authorized_keys** file to **root**. This update resolves the issue. When the MCO creates or updates the **authorized_keys** file, it correctly sets or preserves **core** as the owner and group of the file. (BZ#1956739)

- Previously, in clusters that use Stateless Address AutoConfiguration (SLAAC), the Ironic **addr-gen-mode** parameter was not being persisted to the OVNKubernetes bridge. As a result, the IPv6 addresses could change when the bridge was created. This broke the cluster because node IP changes are unsupported. This fix persists the **addr-gen-mode** parameter when creating the bridge. The IP address is now consistent throughout the deployment process. (BZ#1990625)

- Previously, if a machine config included a compressed file with the **spec.config.storage.files.contents.compression** parameter set to **gzip**, the Machine Config Daemon (MCD) incorrectly wrote the compressed file to disk without extracting it. With this fix, the MCD now extracts a compressed file when the compression parameter is set to **gzip**. (BZ#1970218)

- Previously, **systemd** units were cleaned up only when completely removed. As a result, **systemd** units could not be unmasked by using a machine config because the masks were not being removed unless the **systemd** unit was completely removed. With this fix, when you configure a **systemd** unit as **mask: true** in a machine config, any existing masks are removed. As a result, **systemd** units can now be unmasked. (BZ#1966445)

Management Console

- Previously, the **OperatorHub** category and card links did not include valid **href** attributes. Consequently, the **OperatorHub** category and card links could not be opened in a new tab. This update adds valid **href** attributes to the **OperatorHub** category and card links. As a result, the **OperatorHub** and its card links can be opened in new tabs. (BZ#2013127)

- Previously, on the **Operand Details** page, a special case was created where the conditions table for the **status.conditions** property always rendered before all other tables. Consequently, the **status.conditions** table did not follow the ordering rules of descriptors, which caused unexpected behavior when users tried to change the order of the tables. This update removes the special case for **status.conditions** and only defaults to rendering it first if no descriptor is defined for that property. As a result, the table for **status.condition** is rendered according to descriptor ordering rules when a descriptor is defined on that property. (BZ#2014488)

- Previously, the **Resource Details** page metrics tab was exceeding the cluster-scoped Thanos endpoint. Consequently, users without authorization for this endpoint would receive a **401** response for all queries. With this update, the Thanos tenancy endpoints are updated, and redundant namespace query arguments are removed. As a result, users with the correct role-based access control (RBAC) permissions can now see data in the metrics tab of the **Resource Details** page. (BZ#2015806)

- Previously, when an Operator added an API to an existing API group, it did not trigger API discovery. Consequently, new APIs were not seen by the front end until the page was refreshed. This update makes APIs added by Operators viewable by the front end without a page refresh. (BZ#1815189)

- Previously, in the Red Hat OpenShift Cluster Manager for Red Hat OpenStack Platform (RHOSP), the control plane was not translated into simplified Chinese. As a result, naming differed from OpenShift Container Platform documentation. This update fixes the translation issue in the Red Hat OpenShift Cluster Manager. (BZ#1982063)

- Previously, filtering of virtual tables in the Red Hat OpenShift Cluster Manager was broken. Consequently, all of the available **nodes** would not appear following a search. This update includes new virtual table logic that fixes the filtering issue in the Red Hat OpenShift Cluster Manager. (BZ#1990255)

Monitoring

- Previously, during OpenShift Container Platform upgrades, the Prometheus service could become unavailable because either two Prometheus pods were located on the same node or the two nodes running the pods rebooted during the same interval. This situation was possible because the Prometheus pods had soft anti-affinity rules regarding node placement and no **PodDisruptionBudget** resources provisioned. Consequently, metrics were not collected and rules were not evaluated over a period of time.
  To fix this issue, the Cluster Monitoring Operator (CMO) now configures hard anti-affinity rules to ensure that the two Prometheus pods are scheduled on different nodes. The CMO also provisions **PodDisruptionBudget** resources to ensure that at least one Prometheus pod is always running. As a result, during upgrades, the nodes now reboot in sequence to ensure that at least one Prometheus pod is always running. (BZ#1933847)

- Previously, the Thanos Ruler service would become unavailable when the node that contains the two Thanos Ruler pods experienced an outage. This situation occurred because the Thanos Ruler pods had only soft anti-affinity rules regarding node placement. Consequently, user-defined rules would not be evaluated until the node came back online.

With this release, the Cluster Monitoring Operator (CMO) now configures hard anti-affinity rules to ensure that the two Thanos Ruler pods are scheduled on different nodes. As a result, a single-node outage no longer creates a gap in user-defined rule evaluation. (BZ#1955490)

- Previously, the Prometheus service would become unavailable when the two Prometheus pods were located on the same node and that node experienced an outage. This situation occurred because the Prometheus pods had only soft anti-affinity rules regarding node placement. Consequently, metrics would not be collected, and rules would not be evaluated until the node came back online.
  With this release, the Cluster Monitoring Operator configures hard anti-affinity rules to ensure that the two Prometheus pods are scheduled on different nodes. As a result, Prometheus pods are now scheduled on different nodes, and a single node outage no longer creates a gap in monitoring.(BZ#1949262)

- Previously, during OpenShift Container Platform patch upgrades, the Alertmanager service might become unavailable because either the three Alertmanager pods were located on the same node or the nodes running the Alertmanager pods happened to reboot at the same time. This situation was possible because the Alertmanager pods had soft anti-affinity rules regarding node placement and no **PodDisruptionBudget** provisioned. This release enables hard anti-affinity rules and **PodDisruptionBudget** resources to ensure no downtime during patch upgrades for the Alertmanager and other monitoring components. (BZ#1955489)

- Previously, a false positive **NodeFilesystemSpaceFillingUp** alert was triggered when the file system space was occupied by many Docker images. For this release, the threshold to fire the **NodeFilesystemSpaceFillingUp** warning alert is now reduced to 20% space available, rather than 40%, which stops the false positive alert from firing. (BZ#1987263)

- Previously, alerts for the Prometheus Operator component did not apply to the Prometheus Operator that runs the **openshift-user-workload-monitoring** namespace when user-defined monitoring is enabled. Consequently, no alerts fired when the Prometheus Operator that manages the **openshift-user-workload-monitoring** namespace encountered issues.
  With this release, alerts have been modified to monitor both the **openshift-monitoring** and **openshift-user-workload-monitoring** namespaces. As a result, cluster administrators receive alert notifications when the Prometheus Operator that manages user-defined monitoring encounters issues. (BZ#2001566)

- Previously, if the number of DaemonSet pods for the **node-exporter** agent was not equal to the number of nodes in the cluster, the Cluster Monitoring Operator (CMO) would report a condition of **degraded**. This issue would occur when one of the nodes was not in the **ready** condition.
  This release now verifies that the number of DaemonSet pods for the **node-exporter** agent is not less than the number of ready nodes in the cluster. This process ensures that a **node-exporter** pod is running on every active node. As a result, the CMO will not report a degraded condition if one of the nodes is not in a ready state. (BZ#2004051)

- This release fixes an issue in which some pods in the monitoring stack would start before TLS certificate-related resources were present, which resulted in failures and restarts. (BZ#2016352)

- Previously, if reporting metrics failed due to reaching the configured sample limit, the metrics target would still appear with a status of **Up** in the web console UI even though the metrics were missing. With this release, Prometheus bypasses the sample limit setting for reporting metrics, and the metrics now appear regardless of the sample limit setting. (BZ#2034192)

Networking

- When using the OVN-Kubernetes network provider in OpenShift Container Platform versions

prior to 4.8, the node routing table was used for routing decisions. In newer versions of OpenShift Container Platform, the host routing table is bypassed. In this release, you can now specify whether you want to use or bypass the host kernel networking stack for traffic routing decisions. (BZ#1996108)

- Previously, when Kuryr was used in a restricted installation with proxy, the Cluster Network Operator was not enforcing usage of the proxy to allow communication with the Red Hat OpenStack Platform (RHOSP) API. Consequently, cluster installation did not progress. With this update, the Cluster Network Operator can communicate with the RHOSP API through the proxy. As a result, installation now succeeds. (BZ#1985486)

- Before this update, the SRIOV webhook blocked the creation of network policies on OpenShift Container Platform on Red Hat OpenStack Platform (RHOSP) environments. With this update, the SRIOV webhook reads and validates the RHOSP metadata and can now be used to create network policies. (BZ#2016334)

- Previously, the **MachineConfig** object could not be updated because the SRIOV Operator did not pause the **MachineConfig** pool object. With this update, the SRIOV Operator pauses the relevant machine config pool before running any configuration requiring reboot. (BZ#2021151)

- Previously, there were timing issues with **keepalived** that resulted in its termination when it should have been running. This update prevents multiple **keepalived** commands from being sent in a short period of time. As a result, timing issues are no longer a problem and **keepalive** continuously runs. (BZ#2022050)

- Previously, when Kuryr was used in a restricted installation with proxy, the Cluster Networking Operator was not enforcing usage of the proxy to allow communication with the Red Hat OpenStack Platform (RHOSP) API. Consequently, cluster installation did not progress. With this update, the Cluster Network Operator can communicate with the RHOSP API through the proxy. As a result, installation now succeeds. (BZ#1985486)

- Previously, pods that used secondary interfaces with IP addresses provided by the Whereabouts Container Network Interface (CNI) plugin might get stuck in the **ContainerCreating** state because of IP address exhaustion. Now, Whereabouts properly accounts for released IP addresses from cluster events, such as reboots, that previously were not tracked. (BZ#1914053)

- Previously, when using the OpenShift SDN cluster network provider, idled services used an increasing amount of CPU to un-idle services. In this release, the idling code for kube-proxy is optimized to reduce CPU utilizing for service idling. (BZ#1966521)

- Previously, when using the OVN-Kubernetes cluster network provider, the presence of any unknown field in an internal configuration map could cause the OVN-Kubernetes pods to fail to start during a cluster upgrade. Now the presence of unknown fields causes a warning, rather than a failure. As a result, the OVN-Kubernetes pods now successfully start during a cluster upgrade. (BZ#1988440)

- Previously, a webhook for the SR-IOV Network Operator blocked network policies for OpenShift installations on OpenStack. Users were not able to create SR-IOV network policies. This update fixes the webhook. Users can now create SR-IOV network policies for installations on OpenStack. (BZ#2016334)

- Previously, the CRI-O runtime engine passed pod UIDs by using the **K8S_POD_UID** variable. But when pods were deleted and recreated at the same time that Multus was setting up networking for the deleted pod's sandbox, this method resulted in additional metadata and unnecessary processing. In this update, Multus handles pod UIDs, and unnecessary metadata processing is avoided. (BZ#2017882)

- Previously, in deployments of OpenShift on a single node, default settings for the SR-IOV Network Operator prevented users from making certain modifications to nodes. By default, after configuration changes are applied, affected nodes are drained and then restarted with the new configuration. This behavior does not work when there is only one node. In this update, when you install the SR-IOV Network Operator in a single-node deployment, the Operator changes its configuration so the **.spec.disableDrain** field is set to **true**. Users can now apply configuration changes successfully in single-node deployments. (BZ#2021151)

- Client-go versions 1.20 and earlier did not have sufficient technique for retrying requests to the Kubernetes API. As a result, retries to the Kubernetes API were not sufficient. This update fixes the problem by introducing client-go 1.22. (BZ#2052062)

Node

- Previously, network, IPC, and UTS namespace resources managed by CRI-O were only freed when the Kubelet removed stopped pods. With this update, the Kubelet frees these resources when the pods are stopped. (BZ#2003193)

- Previously, when logging into a worker node, messages might appear indicating a **systemd-coredump** services failure. This was due to the unnecessary inclusion of the **system-systemd** namespace for containers. A filter now prevents this namespace from impacting the workflow. (BZ#1978528)

- Previously, when clusters were restarted, the status of terminated pods might have been reset to **Running**, which would result in an error. This has been corrected and now all terminated pods remain terminated and active pods reflect their correct status. (BZ#1997478)

- Previously, certain stop signals were ignored in OpenShift Container Platform, causing services in the container to continue running. With an update to the signal parsing library, all stop signals are now respected. (BZ#2000877)

- Previously, pod namespaces managed by CRI-O, for example network, IPC, and UTS, were not unmounted when the pod was removed. This resulted in leakage, driving the Open vSwitch CPU to 100%, which caused pod latency and other performance impacts. This has been resolved and pod namespaces are unmounted when removed. (BZ#2003193)

OpenShift CLI (oc)

- Previously, due to the increasing number of custom resource definitions (CRD) installed in the cluster, the requests reaching for API discovery were limited by client code restrictions. Now, both the limit number and QPS have been boosted, and client-side throttling should appear less frequently. (BZ#2042059)

- Previously, some minor requests did not have the user agent string set correctly, so the default Go user agent string was used instead for **oc**. The user agent string is now set correctly for all mirror requests, and the expected **oc** user agent string is now sent to registries. (BZ#1987257)

- Previously, **oc debug** assumed that it was always targeting Linux-based containers by trying to run a Bash shell, and if Bash was not present in the container, it attempted to debug as a Windows container. The **oc debug** command now uses pod selectors to determine the operating system of the containers and now works properly on both Linux and Windows-based containers. (BZ#1990014)

- Previously, the **--dry-run** flag was not working properly for several **oc set** subcommands, so **--dry-run=server** was performing updates to resources rather than performing a dry run. The **--dry-run** flags are now working properly to perform dry runs on the **oc set** subcommands. (BZ#2035393)

OpenShift containers

- Previously, a container using SELinux could not read **/var/log/containers** log files due to a missing policy. This update makes all log files in **/var/log** accessible including those accessed through symlink. (BZ#2005997)

OpenShift Controller Manager

- Previously, the **openshift_apps_deploymentconfigs_last_failed_rollout_time** metric improperly set the **namespace** label as the value of the **exported_namespace** label. The **openshift_apps_deploymentconfigs_last_failed_rollout_time** metric now has the correct **namespace** label set. (BZ#2012770)

Operator Lifecycle Manager (OLM)

- Before this update, default catalog sources for the **marketplace-operator** did not tolerate tainted nodes and the **CatalogSource** pod would only have the default settings for tolerations, **nodeSelector**, and **priorityClassName**. With this update, the **CatalogSource** specification now includes the optional **spec.grpcPodConfig** field that can override tolerations, **nodeSelector**, and **priorityClassName** for the pod. (BZ#1927478)

- Before this update, the **csv_suceeded** metric would be lost when the OLM Operator was restarted. With this update, the **csv_succeeded** metric is emitted at the beginning of the OLM Operator's startup logic. (BZ#1927478)

- Before this update, the **oc adm catalog mirror** command did not set minimum and maximum values for the **--max-icsp-size** flag. As a result, the field accepted values that were less than zero or were too large. With this update, values are limited to sizes greater than zero and less than 250001. Values outside of this range fail validation. (BZ#1972962)

- Before this update, bundled images did not contain the related images needed for Operator deployment in file-based catalogs. As a result, images were not mirrored to disconnected clusters unless specified in the **relatedImages** field of the ClusterServiceVersion (CSV). With this update, the **opm render** command adds the CSV Operator images to the **relatedImages** file when the file-based catalog bundle image is rendered. The images necessary for Operator deployment are now mirrored to disconnected clusters even if they are not listed in the **relatedImages** field of the CSV. (BZ#2002075)

- Before this update, it could take up to 15 minutes for Operators to perform **skipRange** updates. This was a known issue that could be resolved if cluster administrators deleted the **catalog-operator** pod in the **openshift-operator-lifecycle-manager** namespace. This caused the pod to be automatically recreated and triggered the **skipRange** upgrade. With this update, obsolete API calls have been fixed in Operator Lifecycle Manager (OLM), and **skipRange** updates trigger immediately. (BZ#2002276)

- Occasionally, update events on clusters would happen at the same time that Operator Lifecycle Manager (OLM) modified an object from the lister cache. This caused concurrent map writes. This fix updates OLM so it no longer modifies objects retrieved from the lister cache. Instead, OLM modifies a copy of the object where applicable. As a result, OLM no longer experiences concurrent map writes. (BZ#2003164)

- Previously, Operator Lifecycle Manager (OLM) could not establish gRPC connections to catalog source pods that were only reachable through a proxy. If a catalog source pod was behind a proxy, OLM could not connect to the proxy and the hosted Operator content was unavailable for installation. This bug fix introduces a **GRPC_PROXY** environment variable that defines a proxy that OLM uses to establish connections to gRPC catalog sources. As a result, OLM can now be configured to use a proxy when connecting to gRPC catalog sources. (BZ#2011927)

- Previously, skipped bundles were not verified to be members of the same package. Bundles could skip across packages, which broke upgrade chains. This bug fix adds validation to ensure skipped bundles are in the same package. As a result, no bundle can skip bundles in another package, and upgrade graphs no longer break across packages. (BZ#2017327)

- In the **CatalogSource** object, the **RegistryServiceStatus** field stores service information that is used to generate an address that Operator Lifecycle Manager (OLM) relies on to establish a connection with the associated pod. If the **RegistryServiceStatus** field is not nil and is missing the namespace, name, and port information for its service, OLM is unable to recover until the associated pod has an invalid image or spec. With this bug fix, when reconciling a catalog source, OLM now ensures that the **RegistryServiceStatus** field of the **CatalogSource** object is valid and updates its status to reflect the change. Additionally, this address is stored within the status of the catalog source in the **status.GRPCConnectionState.Address** field. If the address changes, OLM updates this field to reflect the new address. As a result, the **.status.connectionState.address** field of a catalog source should no longer be nil. (BZ#2026343)

OpenShift API server
OpenShift Update Service
Red Hat Enterprise Linux CoreOS (RHCOS)

- Previously, when the RHCOS live ISO added a UEFI boot entry for itself, it assumed the existing UEFI boot entry IDs were consecutive, thereby causing the live ISO to fail in the UEFI firmware when booting on systems with non-consecutive boot entry IDS. With this fix, the RHCOS live ISO no longer adds a UEFI boot entry for itself and the ISO boots successfully. (BZ#2006690)

- To help you determine whether a user-provided image was already booted, information has been added on the terminal console describing when the machine was provisioned through Ignition and whether a user Ignition configuration was provided. This allows you to verify that Ignition ran when you expected it to. (BZ#2016004)

- Previously, when reusing an existing statically keyed LUKS volume during provisioning, the encryption key was not correctly written to disk and Ignition would fail with a "missing persisted keyfile" error. With this fix, Ignition now correctly writes keys for reused LUKS volumes so that existing statically keyed LUKS volumes can be reused during provisioning. (BZ#2043296)

- Previously, **ostree-finalize-staged.service** failed while upgrading a Red Hat Enterprise Linux CoreOS (RHCOS) node to 4.6.17. To fix this, the sysroot code now ignores any irregular or non-symlink files in **/etc**. (BZ#1945274)

- Previously, **initramfs** files were missing udev rules for by-id symlinks of attached SCSI devices. Because of this, Ignition configuration files that referenced these symlinks would result in a failed boot of the installed system. With this update, the **63-scsi-sg3_symlink.rules** for SCSI rules are added in dracut. (BZ#1990506)

- Previously, on bare-metal machines, a race condition occurred between **system-rfkill.service** and **ostree-remount.service**. Consequently, the **ostree-remount** service failed and the node operating system froze during the boot process. With this update, the **/sysroot/** directory is now read-only. As a result, the issue no longer occurs. (BZ#1992618)

- Previously, Red Hat Enterprise Linux CoreOS (RHCOS) live ISO boots added a UEFI boot entry, prompting a reboot on systems with a TPM. With this update, the RHCOS live ISO no longer adds a UEFI boot entry so the ISO does not initiate a reboot after first boot. (BZ#2004449)

Performance Addon Operator

- The spec.cpu.reserved` flag might not be correctly set by default if **spec.cpu.isolated** is the

only parameter defined in **PerformanceProfile**. You must set the settings for both **spec.cpu.reserved** and **spec.cpu.isolated** in the **PerformanceProfile**. The sets must not overlap and the sum of all CPUs mentioned must cover all CPUs expected by the workers in the target pool. (BZ#1986681)

- Previously, the **oc adm must-gather** tool failed to collect node data if the **gather-sysinfo** binary was missing in the image. This was caused by a missing **COPY** statement in the Dockerfile. To avoid this issue, you must add the necessary **COPY** statements to the Dockerfile to generate and copy the binaries. (BZ#2021036)

- Previously, the Performance Addon Operator downloaded its image from the registry without checking whether it was available on the CRI-O cache. Consequently, the Performance Addon Operator failed to start if it could not reach the registry, or if the download timed out. With this update, the Operator only downloads its image from the registry if it cannot pull the image from the CRI-O cache. (BZ#2021202)

- When upgrading OpenShift Container Platform to version 4.10, any comment (**#comment**) in the tuned profile that does not start at the beginning of the line causes a parsing error. Performance Addon Operator issues can be solved by upgrading it to the same level (4.10) as OpenShift Container Platform. Comment-related errors can be worked around by putting all comments on a single line, with the # character at the start of the line. (BZ#2059934)

Routing

- Previously, if the cluster administrator provided a default ingress certificate that was missing the newline character for the last line, the OpenShift Container Platform router would write out a corrupt PEM file for HAProxy. Now, it writes out a valid PEM file even if the input is missing a newline character. (BZ#1894431)

- Previously, a route created where the combined name and namespace for the DNS segment was greater than 63 characters long would be rejected. This expected behavior could cause problems integrating with upgraded versions of OpenShift Container Platform. Now, an annotation allows non-conformant DNS hostnames. With **AllowNonDNSCompliantHostAnnotation** set to **true**, the non-conformant DNS hostname, or one longer than 63 characters, is allowed. (BZ#1964112)

- Previously, the Cluster Ingress Operator would not create wildcard DNS records for Ingress Controllers when the cluster's **ControlPlaneTopology** was set to **External**. In Hypershift clusters where the **ControlPlaneTopology** was set to **External** and the Platform was AWS, the Cluster Ingress Operator never became available. This updates limits the disabling of DNS updates when the **ControlPlaneTopology** is **External** and the platform is IBM Cloud. As a result, wildcard DNS entries are created for Hypershift clusters running on AWS. (BZ#2011972)

- Previously, the cluster ingress router was blocked from working because the Ingress Operator failed to configure a wildcard DNS record for the cluster ingress router on Azure Stack Hub IPI. With this fix, the Ingress Operator now uses the configured ARM endpoint to configure DNS on Azure Stack Hub IPI. As a result, the cluster ingress router now works properly. (BZ#2032566)

- Previously, the cluster-wide prox configuration could not accept IPv6 addresses for the **noProxy** setting. Consequently, it was impossible to install a cluster whose configuration was having **noProxy** with IPv6 addresses. With this update, the Cluster Network Operator is now able to parse IPv6 addresses for the **noProxy** setting of the cluster-wide proxy resource. As a result, it is now possible to exclude IPv6 addresses for the **noProxy** setting. (BZ#1939435)

- Before OpenShift Container Platform 4.8, the IngressController API did not have any subfields under the **status.endpointPublishingStrategy.hostNetwork** and **status.endpointPublishingStrategy.nodePort** fields. These fields could be null even if the

spec.endpointPublishingStrategy.type was set to **HostNetwork** or **NodePortService**. In OpenShift Container Platform 4.8, the **status.endpointPublishingStrategy.hostNetwork.protocol** and **status.endpointPublishingStrategy.nodePort.protocol** subfields were added, and the Ingress Operator set default values for these subfields when the Operator admitted or re-admitted an IngressController that specified the "HostNetwork" or "NodePortService" strategy type. With this bug, however, the Operator ignored updates to these spec fields, and updating **spec.endpointPublishingStrategy.hostNetwork.protocol** or **spec.endpointPublishingStrategy.nodePort.protocol** to **PROXY** to enable proxy protocol on an existing IngressController had no effect. To work around this issue, it was necessary to delete and recreate the IngressController to enable PROXY protocol. With this update, the Ingress Operator is changed so that it correctly updates the status fields when **status.endpointPublishingStrategy.hostNetwork** and **status.endpointPublishingStrategy.nodePort** are null and when the IngressController spec fields specify proxy protocol with the **HostNetwork** or **NodePortService** endpoint publishing strategy type. As a result, setting **spec.endpointPublishingStrategy.hostNetwork.protocol** or **spec.endpointPublishingStrategy.nodePort.protocol** to **PROXY** now takes proper effect on upgraded clusters. (BZ#1997226)

Samples

- Before this update, if the Cluster Samples Operator encountered an **APIServerConflictError** error, it reported **sample-operator** as having **Degraded status** until it recovered. Momentary errors of this type were not unusual during upgrades but caused undue concern for administrators monitoring the Operator status. With this update, if the Operator encounters a momentary error, it no longer indicates **openshift-samples** as having **Degraded status** and tries again to connect to the API server. Momentary shifts to **Degraded status** no longer occur. (BZ#1993840)

- Before this update, various allowed and blocked registry configuration options in the cluster image configuration might prevent the Cluster Samples Operator from creating image streams. As a result, the samples operator might mark itself as degraded, which impacted the general OpenShift Container Platform install and upgrade status.
  In various circumstances, the management state of the Cluster Samples Operator can make the transition to **Removed**. With this update, these circumstances now include when the image controller configuration parameters prevent the creation of image streams by using either the default image registry or the image registry specified by the **samplesRegistry** setting. The Operator status now also indicates that the cluster image configuration is preventing the creation of the sample image streams. (BZ#2002368)

Storage

- Previously, the Local Storage Operator (LSO) took a long time to delete orphaned persistent volumes (PVs) due to the accumulation of a 10-second delay. With this update, the LSO does not use the 10-second delay, PVs are deleted promptly, and local disks are made available for new persistent volume claims sooner. (BZ#2001605)

- Previously, Manila error handling would degrade the Manila Operator, and the cluster. Errors are now treated as non-fatal so that the Manila Operator is disabled, rather than degrading the cluster. (BZ#2001620)

- In slower cloud environments, such as when using Cinder, the cluster might become degraded. Now, OpenShift Container Platform accommodates slower environments so that the cluster does not become degraded. (BZ#2027685)

Telco Edge

- If a generated policy has a complianceType of **mustonlyhave**, Operator Lifecycle Manager (OLM) updates to metadata are then reverted as the policy engine restores the 'expected' state of the CR. Consequently, OLM and the policy engine continuously overwrite the metadata of the CR under conflict. This results in high CPU usage. With this update, OLM and the policy engine no longer conflict, which reduces CPU usage. (**BZ#2009233**)

- Previously, user-supplied fields in the **PolicyGenTemplate** overlay were not copied to generated manifests if the field did not exist in the base source CR. As a result, some user content was lost. The **policyGen** tool is now updated to support all user supplied fields. (**BZ#2028881**)

- Previously, DNS lookup failures might cause the Cluster Baremetal Operator to continually fail when installed on unsupported platforms. With this update, the Operator remains disabled when installed on an unsupported platform. (**BZ#2025458**)

Web console (Administrator perspective)
Web console (Developer perspective)

- Before this update, resources in the **Developer** perspective of the web console had invalid links to details about that resource. This update resolves the issue. It creates valid links so that users can access resource details. (BZ#2000651)

- Before this update, you could only specify a subject in the **SinkBinding** form by label, not by name. With this update, you can use a drop-down list to select whether to specify a subject by name or label. (BZ#2002266)

- Before this update, the web terminal icon was available in the web console's banner head only if you installed the Web Terminal Operator in the **openShift-operators** namespace. With this update, the terminal icon is available regardless of the namespace where you install the Web Terminal Operator. (2006329)

- Before this update, the service binding connector did not appear in topology if you used a **resource** property rather than a **kind** property to define a **ServiceBinding** custom resource (CR). This update resolves the issue by reading the CR's **resource** property to display the connector on the topology. (BZ#2013545)

- Before this update, the name input fields used a complex and recursive regular expression to validate user inputs. This regular expression made name detection very slow and often caused errors. This update resolves the issue by optimizing the regular expression and avoiding recursive matching. Now, name detection is fast and does not cause errors. (BZ#2014497)

- Before this update, feature flag gating was missing from some extensions contributed by the knative plugin. Although this issue did not affect what was displayed, these extensions ran unnecessarily, even if the serverless operator was not installed. This update resolves the issue by adding feature flag gating to the extensions where it was missing. Now, the extensions do not run unnecessarily. (BZ#2016438)

- Before this update, if you repeatedly clicked links to get details for resources such as custom resource definitions or pods and the application encountered multiple code reference errors, it failed and displayed a **t is not a function** error. This update resolves the issue. When an error occurs, the application resolves a code reference and stores the resolution state so that it can correctly handle additional errors. The application no longer fails when code reference errors occur. (BZ#2017130)

- Before this update, users with restricted access could not access their config map in a shared namespace to save their user settings on a cluster and load them in another browser or machine. As a result, user preferences such as pinned navigation items were only saved in the

local browser storage and not shared between multiple browsers. This update resolves the issue: The web console Operator automatically creates RBAC rules so that each user can save these settings to a config map in a shared namespace and more easily switch between browsers. (BZ#2018234)

- Before this update, trying to create connections between virtual machines (VMs) in the **Topology** view failed with an "Error creating connection" message. This issue happened because this action relied on a method that did not support custom resource definition (CRDs). This update resolves the issue by adding support for CRDs. Now you can create connections between VMs. (BZ#2020904)

- Before this update, the tooltip for tasks in the **PipelineRun details** showed misleading information. It showed the time elapsed since the task ran, not how long they ran. For example, it showed 122 hours for a task that ran for a couple of seconds 5 days ago. With this update, the tooltip shows the duration of the task. (BZ#2011368)

1.7. TECHNOLOGY PREVIEW FEATURES

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

Technology Preview Features Support Scope

In the table below, features are marked with the following statuses:

- **TP**: *Technology Preview*
- **GA**: *General Availability*
- **-**: *Not Available*
- **DEP**: *Deprecated*

Table 1.2. Technology Preview tracker

Feature	OCP 4.8	OCP 4.9	OCP 4.10
Precision Time Protocol (PTP) hardware configured as ordinary clock	TP	GA	GA
PTP single NIC hardware configured as boundary clock	-	-	TP
PTP events with ordinary clock	-	TP	GA
oc CLI plugins	GA	GA	GA
CSI Volumes in OpenShift Builds	-	-	TP
Service Binding	TP	TP	GA
Raw Block with Cinder	GA	GA	GA

Feature	OCP 4.8	OCP 4.9	OCP 4.10
CSI volume expansion	TP	TP	TP
CSI AliCloud Disk Driver Operator	-	-	GA
CSI Azure Disk Driver Operator	TP	TP	GA
CSI Azure File Driver Operator	-	-	TP
CSI Azure Stack Hub Driver Operator	-	GA	GA
CSI GCP PD Driver Operator	GA	GA	GA
CSI IBM VPC Block Driver Operator	-	-	GA
CSI OpenStack Cinder Driver Operator	GA	GA	GA
CSI AWS EBS Driver Operator	TP	GA	GA
CSI AWS EFS Driver Operator	-	TP	GA
CSI automatic migration	TP	TP	TP
CSI inline ephemeral volumes	TP	TP	TP
CSI vSphere Driver Operator	TP	TP	GA
Shared Resource CSI Driver	-	-	TP
Automatic device discovery and provisioning with Local Storage Operator	TP	TP	TP
OpenShift Pipelines	GA	GA	GA
OpenShift GitOps	GA	GA	GA
OpenShift sandboxed containers	TP	TP	GA
Vertical Pod Autoscaler	GA	GA	GA
Cron jobs	GA	GA	GA
PodDisruptionBudget	GA	GA	GA
Adding kernel modules to nodes with kvc	TP	TP	TP

Feature	OCP 4.8	OCP 4.9	OCP 4.10
Egress router CNI plugin	GA	GA	GA
Scheduler profiles	TP	GA	GA
Non-preempting priority classes	TP	TP	TP
Kubernetes NMState Operator	TP	TP	GA
Assisted Installer	TP	TP	GA
AWS Security Token Service (STS)	GA	GA	GA
Kdump	TP	TP	TP
OpenShift Serverless	GA	GA	GA
OpenShift on ARM platforms	-	-	GA
Serverless functions	TP	TP	TP
Data Plane Development Kit (DPDK) support	TP	GA	GA
Memory Manager	-	GA	GA
CNI VRF plugin	TP	GA	GA
Cluster Cloud Controller Manager Operator	-	GA	GA
Cloud controller manager for Alibaba Cloud	-	-	TP
Cloud controller manager for Amazon Web Services	-	TP	TP
Cloud controller manager for Google Cloud Platform	-	-	TP
Cloud controller manager for IBM Cloud	-	-	TP
Cloud controller manager for Microsoft Azure	-	TP	TP
Cloud controller manager for Microsoft Azure Stack Hub	-	GA	GA
Cloud controller manager for Red Hat OpenStack Platform (RHOSP)	-	TP	TP
Cloud controller manager for VMware vSphere	-	-	TP

Feature	OCP 4.8	OCP 4.9	OCP 4.10
Driver Toolkit	TP	TP	TP
Special Resource Operator (SRO)	-	TP	TP
Simple Content Access	-	TP	GA
Node Health Check Operator	-	TP	TP
Network bound disk encryption (Requires Clevis, Tang)	-	GA	GA
MetalLB Operator	-	GA	GA
CPU manager	GA	GA	GA
Pod-level bonding for secondary networks	-	-	GA
IPv6 dual stack	-	GA	GA
Selectable Cluster Inventory	-	-	TP
Hyperthreading-aware CPU manager policy	-	-	TP
Dynamic Plugins	-	-	TP
Hybrid Helm Operator	-	-	TP
Alert routing for user-defined projects monitoring	-	-	TP
Disconnected mirroring with the oc-mirror CLI plugin	-	-	TP
Mount shared entitlements in BuildConfigs in RHEL	-	-	TP
Support for RHOSP DCN	-	-	TP
Support for external cloud providers for clusters on RHOSP	-	-	TP
OVS hardware offloading for clusters on RHOSP	-	-	TP
External DNS Operator	-	-	TP
Web Terminal Operator	TP	TP	GA
Topology Aware Lifecycle Manager	-	-	TP
NUMA-aware scheduling with NUMA Resources Operator	-	-	TP

1.8. KNOWN ISSUES

- In OpenShift Container Platform 4.1, anonymous users could access discovery endpoints. Later releases revoked this access to reduce the possible attack surface for security exploits because some discovery endpoints are forwarded to aggregated API servers. However, unauthenticated access is preserved in upgraded clusters so that existing use cases are not broken.
  If you are a cluster administrator for a cluster that has been upgraded from OpenShift Container Platform 4.1 to 4.10, you can either revoke or continue to allow unauthenticated access. It is recommended to revoke unauthenticated access unless there is a specific need for it. If you do continue to allow unauthenticated access, be aware of the increased risks.

  WARNING

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

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

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

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

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

  (BZ#1821771)

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

- Currently, containers start with non-empty inheritable Linux process capabilities. To work around this issue, modify the entry point of a container using a utility such as **capsh(1)** to drop inheritable capabilities before the primary process starts. (BZ#2076265)

- When upgrading to OpenShift Container Platform 4.10, the Cluster Version Operator blocks the upgrade for approximately five minutes while failing precondition checks. The error text, which says **It may not be safe to apply this update**, might be misleading. This error occurs when one or multiple precondition checks fail. In some situations, these precondition checks might only fail for a short period of time, for example, during an etcd backup. In these situations, the Cluster Version Operator and corresponding Operators will, by design, automatically resolve the failing precondition checks and the CVO successfully starts the upgrade.
  Users should check the status and conditions of their Cluster Operators. If the **It may not be safe to apply this update** error is displayed by the Cluster Version Operator, these statuses and conditions will provide more information about the severity of the message. For more information, see BZ#1999777, BZ#2061444, BZ#2006611.

- The assignment of egress IP addresses to control plane nodes with the egress IP feature is not supported on a cluster provisioned on Amazon Web Services (AWS). (BZ#2039656)

- Previously, there was a race condition between Red Hat OpenStack Platform (RHOSP) credentials secret creation and **kube-controller-manager** startup. As a result, Red Hat OpenStack Platform (RHOSP) cloud provider would not be configured with RHOSP credentials and would break support when creating Octavia load balancers for **LoadBalancer** services. To work around this, you must restart the **kube-controller-manager** pods by deleting the pods manually from the manifests. When you use the workaround, the **kube-controller-manager** pods restart and RHOSP credentials are properly configured. (BZ#2004542)

- The ability to delete operands from the web console using the **delete all operands** option is currently disabled. It will be re-enabled in a future version of OpenShift Container Platform. For more information, see BZ#2012120 and BZ#2012971.

- This release contains a known issue with Jenkins. If you customize the hostname and certificate of the OpenShift OAuth route, Jenkins no longer trusts the OAuth server endpoint. As a result, users cannot log in to the Jenkins console if they rely on the OpenShift OAuth integration to manage identity and access.
  Workaround: See the Red Hat Knowledge base solution, Deploy Jenkins on OpenShift with Custom OAuth Server URL. (**BZ#1991448**)

- This release contains a known issue with Jenkins. The **xmlstarlet** command line toolkit, which is required to validate or query XML files, is missing from this RHEL-based image. This issue impacts deployments that do not use OpenShift OAuth for authentication. Although OpenShift OAuth is enabled by default, users can disable it.
  Workaround: Use OpenShift OAuth for authentication. (BZ#2055653)

- Google Cloud Platform (GCP) UPI installation fails when the instance group name is longer than the maximum size of 64 characters. You are restricted in the naming process after adding the "-instance-group" suffix. Shorten the suffix to "-ig" to reduce the number of characters. (BZ#1921627)

- For clusters that run on RHOSP and use Kuryr, a bug in the OVN Provider driver for Octavia can cause load balancer listeners to be stuck in a **PENDING_UPDATE** state while the load balancer that they are attached to remains in an **ACTIVE** state. As a result, the **kuryr-controller** pod can crash. To resolve this problem, update RHOSP to version 16.1.9 (BZ#2019980) or version 16.2.4 (BZ#2045088).

- If an incorrect network is specified in the vSphere **install-config.yaml** file, then an error message from Terraform is generated after a while. Add a check during the creation of manifests to notify the user if the network is invalid. (BZ#1956776)

- The Special Resource Operator (SRO) might fail to install on Google Cloud Platform due to a software-defined network policy. As a result, the simple-kmod pod is not created. (BZ#1996916)

- Currently, idling a stateful set is unsupported when you run **oc idle** for a service that is mapped to a stateful set. There is no known workaround at this time. (BZ#1976894)

- The China (Nanjing) and UAE (Dubai) regions of Alibaba Cloud International Portal accounts do not support installer-provisioned infrastructure (IPI) installations. The China (Guangzhou) and China (Ulanqab) regions do not support a Server Load Balancer (SLB) if using Alibaba Cloud International Portal accounts and, therefore, also do not support IPI installations. (BZ#2048062)

- The Korea (Seoul) **ap-northeast-2** region of Alibaba Cloud does not support installer-provisioned infrastructure (IPI) installations. The Korea (Seoul) region does not support a Server Load Balancer (SLB) and, therefore, also does not support IPI installations. If you want to use OpenShift Container Platform in this region, contact Alibaba Cloud. (BZ#2062525)

- Currently, the **Knative Serving - Revision CPU, Memory, and Network usage** and **Knative Serving - Revision Queue proxy Metrics** dashboards are visible to all the namespaces, including those that do not have Knative services. (BZ#2056682)

- Currently, in the **Developer** perspective, the **Observe** dashboard opens for the most recently viewed workload rather than the one you selected in the **Topology** view. This issue happens because the session uses the Redux store rather than the query parameters in the URL. (BZ#2052953)

- Currently, the **ProjectHelmChartRepository** custom resource (CR) does not show up in the cluster because the API schema for this CR has not been initialized in the cluster yet. (BZ#2054197)

- Currently, while running high-volume pipeline logs, the auto-scroll functionality does not work and logs are stuck showing older messages. This issue happens because running high-volume pipeline logs generates a large number of calls to the **scrollIntoView** method. (BZ#2014161)

- Currently, when you use the **Import from Git** form to import a private Git repository, the correct import type and a builder image are not identified. This issue happens because the secret to fetch the private repository details is not decoded. (BZ#2053501)

- During an upgrade of the monitoring stack, Prometheus and Alertmanager might become briefly unavailable. No workaround for this issue is necessary because the components will be available after a short time has passed. No user intervention is required. (BZ#203059)

- For this release, monitoring stack components have been updated to use TLS authentication for metrics collection. However, sometimes Prometheus tries to keep HTTP connections to metrics targets open using expired TLS credentials even after new ones have been provided. Authentication errors then occur, and some metrics targets become unavailable. When this issue occurs, a **TargetDown** alert will fire. To work around this issue, restart the pods that are reported as down. (BZ#2033575)

- For this release, the number of Alertmanager replicas in the monitoring stack was reduced from three to two. However, the persistent volume claim (PVC) for the removed third replica is not automatically removed as part of the upgrade process. After the upgrade, an administrator can remove this PVC manually from the Cluster Monitoring Operator. (BZ#2040131)

- Previously, the **oc adm must-gather** tool did not collect performance specific data when more than one **--image** argument was supplied. Files, including node and performance related files,

were missing when the operation finished. The issue affects OpenShift Container Platform versions between 4.7 and 4.10. This issue can be resolved by executing the **oc adm must-gather** operation twice, once for each image. As a result, all expected files can be collected. (BZ#2018159)

- When using the Technology Preview oc-mirror CLI plugin, there is a known issue that can occur when updating your cluster after mirroring an updated image set to the mirror registry. If a new version of an Operator is published to a channel by deleting the previous version of that Operator and then replacing it with a new version, an error can occur when applying the generated **CatalogSource** file from the oc-mirror plugin, because the catalog is seen as invalid. As a workaround, delete the previous catalog image from the mirror registry, generate and publish a new differential image set, and then apply the **CatalogSource** file to the cluster. You must follow this workaround each time you publish a new differential image set, until this issue is resolved. (BZ#2060837)

- The processing of the **StoragePVC** custom resource during the GitOps ZTP flow does not exclude the **volume.beta.kubernetes.io/storage-class** annotation when a user does not include a value for it. This annotation causes the **spec.storageClassName** field to be ignored. To avoid this, set the desired **StorageClass** name in the **volume.beta.kubernetes.io/storage-class** annotation within your **PolicyGenTemplate** when using a **StoragePVC** custom resource. (BZ#2060554)

- Removing a Bidirectional Forwarding Detection (BFD) custom profile enabled on a border gateway protocol (BGP) peer resource does not disable the BFD. Instead, the BGP peer starts using the default BFD profile. To disable BFD from a BGP peer resource, delete the BGP peer configuration and recreate it without a BFD profile. (BZ#2050824)

- For clusters that run on RHOSP and use Mellanox NICs as part of a single-root I/O virtualization configuration (SR-IOV), you may not be able to create a pod after you start one, restart the SR-IOV device plugin, and then stop the pod. No workaround is available for this issue.

- OpenShift Container Platform supports deploying an installer-provisioned cluster without a DHCP server. However, without a DHCP server, the bootstrap VM does not receive an external IP address for the **baremetal** network. To assign an IP address to the bootstrap VM, see Assigning a bootstrap VM an IP address on the baremetal network without a DHCP server . (BZ#2048600)

- OpenShift Container Platform supports deploying an installer-provisioned cluster with static IP addresses on the **baremetal** network for environments without a DHCP server. If a DHCP server is present, nodes might retrieve an IP address from the DHCP server on reboot. To prevent DHCP from assigning an IP address to a node on reboot, see Preventing DHCP from assigning an IP address on node reboot. (BZ#2036677)

- The RHCOS kernel experiences a soft lockup and eventually panics due to a bug in the Netfilter module. A fix is planned to resolve this issue in a future z-stream release of OpenShift Container Platform. (BZ#2061445)

- Due to the inclusion of old images in some image indexes, running **oc adm catalog mirror** and **oc image mirror** might result in the following error: **error: unable to retrieve source image**. As a temporary workaround, you can use the **--skip-missing** option to bypass the error and continue downloading the image index. For more information, see Service Mesh Operator mirroring failed.

- It is not possible to create a macvlan on the physical function (PF) when a virtual function (VF) already exists. This issue affects the Intel E810 NIC. (BZ#2120585)

- If a cluster that was deployed through ZTP has policies that do not become compliant, and no

ClusterGroupUpdates object is present, you must restart the TALM pods. Restarting TALM creates the proper **ClusterGroupUpdates** object, which enforces the policy compliance. (OCPBUGS-4065)

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

1.9. ASYNCHRONOUS ERRATA UPDATES

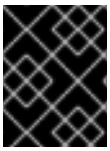
Security, bug fix, and enhancement updates for OpenShift Container Platform 4.10 are released as asynchronous errata through the Red Hat Network. All OpenShift Container Platform 4.10 errata are available on the Red Hat Customer Portal . See the OpenShift Container Platform Life Cycle for more information 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 4.10. Versioned asynchronous releases, for example with the form OpenShift Container Platform 4.10.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-2022:0056 - OpenShift Container Platform 4.10.3 image release, bug fix, and security update advisory

Issued: 2022-03-10

OpenShift Container Platform release 4.10.3, which includes security updates, is now available. The list of bug fixes that are included in the update is documented in the RHSA-2022:0056 advisory. A secondary set of bug fixes can be found in the RHEA-2022:0748 advisory. The RPM packages that are included in the update are provided by the RHSA-2022:0055 advisory.

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

```
$ oc adm release info 4.10.3 --pullspecs
```

1.9.1.1. Bug fixes

- Previously, OpenShift Container Platform, with OVN-Kubernetes, managed ingress access to

services via ExternalIP. When upgrading from 4.10.2 to 4.10.3, access **ExternalIP** stops work with issues like "No Route to Host". With this update, administrators will now have to direct traffic from externalIPs to the cluster. For guidance, see (KCS*) and (**Kubernetes External IPs**) (**BZ#2076662**)

1.9.2. RHBA-2022:0811 - OpenShift Container Platform 4.10.4 bug fix and security update

Issued: 2022-03-15

OpenShift Container Platform release 4.10.4, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHBA-2022:0811 advisory. The RPM packages that are included in the update are provided by the RHSA-2022:0810 advisory.

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

```
$ oc adm release info 4.10.4 --pullspecs
```

1.9.2.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.3. RHBA-2022:0928 - OpenShift Container Platform 4.10.5 bug fix and security update

Issued: 2022-03-21

OpenShift Container Platform release 4.10.5, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHBA-2022:0928 advisory. The RPM packages that are included in the update are provided by the RHSA-2022:0927 advisory.

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

```
$ oc adm release info 4.10.5 --pullspecs
```

1.9.3.1. Known issues

- There is an issue adding a cluster through zero touch provisioning (ZTP) with the name **ztp***. Adding **ztp** as the name of a cluster causes a situation where **ArgoCD** deletes policies that ACM copies in to the cluster namespace. Naming the cluster with **ztp** leads to a reconciliation loop, and the policies will not be compliant. As a workaround, do not name clusters with **ztp** at the beginning of the name. By renaming the cluster, collision will stop the reconciliation loop and the policies will be compliant. (**BZ#2049154**)

1.9.3.2. Bug fixes

- Previously, the **Observer** dashboard from the **Topology** view in the **Developer** console opened to the last viewed workload rather than the selected one. With this update, the **Observe** dashboard in the **Developer** console always opens to the selected workload from the **Topology** view. (**BZ#2059805**)

1.9.3.3. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.4. RHBA-2022:1026 - OpenShift Container Platform 4.10.6 bug fix and security update

Issued: 2022-03-28

OpenShift Container Platform release 4.10.6, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHBA-2022:1026 advisory. The RPM packages that are included in the update are provided by the RHSA-2022:1025 advisory.

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

```
$ oc adm release info 4.10.6 --pullspecs
```

1.9.4.1. Features

1.9.4.2. Updates from Kubernetes 1.23.5

This update contains changes from Kubernetes 1.23.3 up to 1.23.5. More information can be found in the following changelogs: 1.23.4 and 1.23.5

1.9.4.3. Bug fixes

- Previously, the query for subnets in Cisco ACI's neutron implementation, which is avaiable in Red Hat OpenStack Platform (RHOSP)-16, returned unexpected results for a given network. Consequently, the RHOSP **cluster-api-provider** could potentially try to provision instances with duplicated ports on the same subnet, which caused failed provision. With this update, an additional filter is added in the RHOSP **cluster-api-provider** to ensure there is only one port per subnet. As a result, it is now possible to deploy OpenShift Container Platform on RHOSP-16 with Cisco ACI. (**BZ#2050064**)

- Previously, **oc adm must gather** fell back to the **oc adm inspect** command when the specified image could not run. Consequently, it was difficult to understand information from the logs when the fall back happened. With this update, the logs are improved to make it explicit when a fall back inspection is performed. As a result, the output of **oc adm must gather** is easier to understand. (**BZ#2049427**)

- Previously, the **oc debug node** command did not have timeout specified on idle. Consequently, the users were never logged out of the cluster. With this update, a **TMOUT** environment variable for debug pod has been added to counter inactivity timeout. As a result, the session will be automatically terminated after **TMOUT** inactivity. (**BZ#2060888**)

- Previously, the Ingress Operator performed health checks against the Ingress canary route. When the health check completed, the Ingress Operator did not close the TCP connection to the **LoadBalancer** because **keepalive** packets were enabled on the connection. While performing the next health check, a new connection was established to the **LoadBalancer** instead of using the existing connection. Consequently, this caused connections to accumulate on the **LoadBalancer**. Over time, this exhausted the number of connections on the **LoadBalancer**. With this update, Keepalive is disabled when connecting to the Ingress canary route. As a result, a new connection is made and closed each time the canary probe is run. While Keepalive is disabled, there is no longer an accumulation of established connections. (**BZ#2063283**)

- Previously, the sink for event sources in the **Trigger/Subscription** modal in the **Topology** UI showed all resources, irrespective of whether they were created as a standalone or an underlying resource included with back KSVC, Broker, or KameletBinding. Consequently, users could sink to the underlying addressable resources as they showed up in the sink drop-down menu. With this update, a resource filter has been added to show only standalone resource sink events. (BZ#2059807)

1.9.4.4. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.5. RHSA-2022:1162 - OpenShift Container Platform 4.10.8 bug fix and security update

Issued: 2022-04-07

OpenShift Container Platform release 4.10.8, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHSA-2022:1162 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:1161 advisory.

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

```
$ oc adm release info 4.10.8 --pullspecs
```

1.9.5.1. Removed features

Starting with OpenShift Container Platform 4.10.8, support for Google Cloud Platform Workload Identity has been removed from OpenShift Container Platform 4.10 for the image registry. This change is due to the discovery of an adverse impact to the image registry .

With OpenShift Container Platform 4.10.21, support for using GCP Workload Identity with the image registry is restored. For more information about the status of this feature between OpenShift Container Platform 4.10.8 and 4.10.20, see the related Knowledgebase article.

1.9.5.2. Known issues

- Currently, the web console does not display virtual machine templates that are deployed to a custom namespace. Only templates deployed to the default namespace are displayed in the web console. As a workaround, avoid deploying templates to a custom namespace. (BZ#2054650)

1.9.5.3. Bug fixes

- Previously, the Infrastructure Operator could not provision X11- and X12-based systems due to validation errors created by the bare metal controller (BMC) when special characters such as question marks or equal signs were used in the **filename** parameters of URLs. With this update, the **filename** parameter is removed from the URL if the virtual media image is backed by a local file. (BZ#2011626)

- Previously, when cloning a virtual machine from a template, Operator-made changes reverted after dismissing the dialog box if the boot disk was edited and the storage class was changed. With this update, changes made to storage class remain set after closing the dialogue box. (BZ#2049762)

- Previously, the **startupProbe** field was added to a container's definition. As a result, **startupProbe** causes problems when creating a debug pod. With this update, **startupProbe** is removed by default from the debug pod by the **Expose --keep-startup flag** parameter, which is now set to false by default. (BZ#2068474)

- Previously, the Local Storage Operator (LSO) added an **OwnerReference** object to the persistent volumes (PV) it created, which sometimes caused an issue where a delete request for a PV could leave the PV in the **terminating** state while still attached to the pod. With this update, the LSO no longer creates an **OwnerReference** object and cluster administrators are now able to manually delete any unused PVs after a node is removed from the cluster. (BZ#2065714)

- Before this update, import strategy detection did not occur when a secret was provided for a private Git repository. Consequently, the secrets value was not decoded before it was used. With this update, the secret value is now decoded before use. (BZ#2057507)

1.9.5.4. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.6. RHBA-2022:1241 - OpenShift Container Platform 4.10.9 bug fix update

Issued: 2022-04-12

OpenShift Container Platform release 4.10.9 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:1241 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:1240 advisory.

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

```
$ oc adm release info 4.10.9 --pullspecs
```

1.9.6.1. Known issues

- When updating to OpenShift Container Platform 4.10.9, the etcd pod fails to start and the etcd Operator falls into a **degraded** state. A future version of OpenShift Container Platform will resolve this issue. For more information, see etcd pod is failing to start after updating OpenShift Container Platform 4.9.28 or 4.10.9 and Potential etcd data inconsistency issue in OCP 4.9 and 4.10.

1.9.6.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.7. RHSA-2022:1357 - OpenShift Container Platform 4.10.10 bug fix and security update

Issued: 2022-04-20

OpenShift Container Platform release 4.10.10 is now available. The bug fixes that are included in the update are listed in the RHSA-2022:1357 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:1355 advisory.

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

```
$ oc adm release info 4.10.10 --pullspecs
```

1.9.7.1. Bug fixes

- Previously, the cluster storage Operator credentials request for Amazon Web Services (AWS) did not include KMS statements. Consequently, persistent volumes (PVs) failed to deploy due to the inability to provide a key. With this update, the default credentials request for AWS now allows the mounting of encrypted volumes using customer-managed keys from KMS. Administrators who create credentials requests in manual mode with Cloud Credential Operator (CCO) must apply those changes manually. Other administrators should not be impacted by this change. (**BZ#2072191**)

1.9.7.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.8. RHBA-2022:1431 - OpenShift Container Platform 4.10.11 bug fix update

Issued: 2022-04-25

OpenShift Container Platform release 4.10.11 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:1431 advisory. There are no RPM packages for this release.

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

```
$ oc adm release info 4.10.11 --pullspecs
```

1.9.8.1. Bug fixes

- Previously, when cloning a virtual machine from a template, Operator-made changes reverted after dismissing the dialog box if the boot disk was edited and the storage class was changed. With this update, changes made to storage class remain set after closing the dialogue box. (**BZ#2049762**)

1.9.8.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster using the CLI for instructions.

1.9.9. RHBA-2022:1601 - OpenShift Container Platform 4.10.12 bug fix and security update

Issued: 2022-05-02

OpenShift Container Platform release 4.10.12, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHBA-2022:1601 advisory. The RPM packages that are included in the update are provided by the RHSA-2022:1600 advisory.

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

```
$ oc adm release info 4.10.12 --pullspecs
```

1.9.9.1. Bug fixes

- Previously, the Infrastructure Operator could not provision X11- and X12-based systems. This was due to validation errors created by the bare metal controller (BMC) when special characters such as question marks or equal signs were used in the **filename** parameters of URLs. With this update, the **filename** parameter is removed from the URL if the virtual media image is backed by a local file. (BZ#2011626)

1.9.9.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster using the CLI for instructions.

1.9.10. RHBA-2022:1690 - OpenShift Container Platform 4.10.13 bug fix update

Issued: 2022-05-11

OpenShift Container Platform release 4.10.13 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:1690 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:1689 advisory.

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

```
$ oc adm release info 4.10.13 --pullspecs
```

1.9.10.1. Bug fixes

- Previously, when creating an Ingress Object in OpenShift Container Platform 4.8, the API restrictions prevented users from defining routes with hostnames and installing numeric clusters. This fix removes the API's number restriction, allowing users to create clusters with numbers and define routes using hostnames. (BZ#2072739)

- Previously, pods related to jobs would get stuck in the Terminating state in OpenShift Container Platform 4.10 due to the **JobTrackingWithFinalizers** feature. This fix disables the **JobTrackingWithFinalizers** feature, resulting in all pods to run as intended. (BZ2075831)

1.9.10.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster using the CLI for instructions.

1.9.11. RHBA-2022:2178 - OpenShift Container Platform 4.10.14 bug fix update

Issued: 2022-05-18

OpenShift Container Platform release 4.10.14 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:2178 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:2177 advisory.

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

```
$ oc adm release info 4.10.14 --pullspecs
```

1.9.11.1. Features

1.9.11.1.1. Update the control plane independently of other worker nodes

With this update, you can now perform a partial cluster update within the **Update Cluster** modal. You are able to update the worker or custom pool nodes to accommodate the time it takes for maintenance. You can also pause and resume within the progress bar of each pool. If one or more worker or custom pools are paused, an alert is displayed at the top of the **Cluster Settings** page. (BZ#2076777)

For more information, see Preparing to perform an EUS-to-EUS update and Updating a cluster using the web console.

1.9.11.1.2. General availability of the Web Terminal Operator

With this update, the **Web Terminal Operator** is now generally available.

1.9.11.1.3. Support for the AWS premium_LRS and standardSSD_LRS disk types

With this update, you can deploy control plane and compute nodes with the **premium_LRS**, **standardSSD_LRS**, or **standard_LRS** disk type. By default, the installation program deploys control plane and compute nodes with the **premium_LRS** disk type. In earlier 4.10 releases, only the **standard_LRS** disk type was supported. (BZ#2079589)

1.9.11.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster using the CLI for instructions.

1.9.12. RHBA-2022:2258 - OpenShift Container Platform 4.10.15 bug fix update

Issued: 2022-05-23

OpenShift Container Platform release 4.10.15 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:2258 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:2257 advisory.

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

```
$ oc adm release info 4.10.15 --pullspecs
```

1.9.12.1. Bug fixes

- Previously, the Image Registry Operator blocked installer-provisioned infrastructure (IPI) installations on IBM Cloud. With this update, clusters that mint credentials manually will now require the administrator role. (BZ#2083559)

1.9.12.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster using the CLI for instructions.

1.9.13. RHBA-2022:4754 - OpenShift Container Platform 4.10.16 bug fix update

Issued: 2022-05-31

OpenShift Container Platform release 4.10.16 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:4754 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:4753 advisory.

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

```
$ oc adm release info 4.10.16 --pullspecs
```

1.9.13.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster using the CLI for instructions.

1.9.14. RHBA-2022:4882 - OpenShift Container Platform 4.10.17 bug fix update

Issued: 2022-06-07

OpenShift Container Platform release 4.10.17 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:4882 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:4881 advisory.

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

```
$ oc adm release info 4.10.17 --pullspecs
```

1.9.14.1. Bug fixes

- Previously, the federation endpoint for Prometheus that stored user-defined metrics was not exposed. Therefore, you could not access it to scrape these metrics from a network location outside the cluster. With this update, you can now use the federation endpoint to scrape user-defined metrics from a network location outside the cluster. (**BZ#2090602**)
- Previously, for user-defined projects, you could not change the default data retention time period value of 24 hours for the Thanos Ruler monitoring component. With this update, you can now change how long Thanos Ruler metrics data is retained for user-defined projects. (**BZ#2090422**)

1.9.14.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.15. RHBA-2022:4944 - OpenShift Container Platform 4.10.18 bug fix and security update

Issued: 2022-06-13

OpenShift Container Platform release 4.10.18, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHBA-2022:4944 advisory. The RPM packages that are included in the update are provided by the RHSA-2022:4943 advisory.

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

```
$ oc adm release info 4.10.18 --pullspecs
```

1.9.15.1. Bug fixes

- Previously, Alibaba Cloud was only supported for disk volumes larger than 20 GiB. Consequently, attempts to dynamically provision a new volume for a persistent volume claim (PVC) smaller than 20GiB failed. With this update, OpenShift Container Platform will automatically increase the volume size for a PVC and it will provision volumes at least with 20 GiB in size. (BZ#2076671)

- Previously, the Ingress Operator had unnecessary logic to remove a finalizer on **LoadBalancer-type** services in previous versions of OpenShift Container Platform. With this update, the Ingress Operator no longer includes this logic. (BZ#2082161)

1.9.15.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.16. RHBA-2022:5172 - OpenShift Container Platform 4.10.20 bug fix update

Issued: 2022-06-28

OpenShift Container Platform release 4.10.20 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:5172 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:5171 advisory.

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

```
$ oc adm release info 4.10.20 --pullspecs
```

1.9.16.1. Bug fixes

- Previously, Bond Container Network Interface (CNI) version 1.0 was not compatible with the Multus Container Network Interface (CNI) plugin. Consequently, the Bond-CNI IP address management (IPAM) improperly populated the **network-status** annotation. With this update, IPAM and Bond-CNI now supports Bond-CNI 1.0. (BZ#2084289)

- Before this update, the **Start Pipeline** dialog box displayed **gp2** as the storage class, regardless of the actual storage class used. With this update, the **Start Pipeline** dialog box displays the actual storage class name.

1.9.16.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.17. RHBA-2022:5428 - OpenShift Container Platform 4.10.21 bug fix update

Issued: 2022-07-06

OpenShift Container Platform release 4.10.21 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:5428 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:5427 advisory.

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

```
$ oc adm release info 4.10.21 --pullspecs
```

1.9.17.1. New features

The feature change in OpenShift Container Platform 4.10.8 to remove support for Google Cloud Platform (GCP) Workload Identity for the image registry has been resolved in OpenShift Container Platform 4.10.21.

1.9.17.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.18. RHBA-2022:5513 - OpenShift Container Platform 4.10.22 bug fix update

Issued: 2022-07-11

OpenShift Container Platform release 4.10.22 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:5513 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:5512 advisory.

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

```
$ oc adm release info 4.10.22 --pullspecs
```

1.9.18.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.19. RHBA-2022:5568 - OpenShift Container Platform 4.10.23 bug fix update

Issued: 2022-07-20

OpenShift Container Platform release 4.10.23 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:5568 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:5567 advisory.

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

```
$ oc adm release info 4.10.23 --pullspecs
```

1.9.19.1. Features

1.9.19.2. Updating managed clusters with Topology Aware Lifecycle Manager (Technology Preview)

You can now use the upstream Topology Aware Lifecycle Manager to perform updates on multiple single-node Openshift clusters by using Red Hat Advanced Cluster Management (RHACM) policies. For more information, see About the Topology Aware Lifecycle Manager configuration .

1.9.19.3. Low-latency Redfish hardware event delivery (Technology Preview)

OpenShift Container Platform now provides a hardware event proxy that enables applications running on bare-metal clusters to respond quickly to Redfish hardware events, such as hardware changes and failures.

The hardware event proxy supports a publish-subscribe service that allows relevant applications to consume hardware events detected by Redfish. The proxy must be running on hardware that supports Redfish v1.8 and later. An Operator manages the lifecycle of the **hw-event-proxy** container.

You can use a REST API to develop applications to consume and respond to events such as breaches of temperature thresholds, fan failure, disk loss, power outages, and memory failure. Reliable end-to-end messaging without persistent stores is based on the Advanced Message Queuing Protocol (AMQP). The latency of the messaging service is in the 10 millisecond range.

NOTE

This feature is supported for single node OpenShift clusters only.

1.9.19.4. Zero touch provisioning is generally available

Use zero touch provisioning (ZTP) to provision distributed units at new edge sites in a disconnected environment. This feature was previously introduced as a Technology Preview feature in OpenShift Container Platform 4.9 and is now generally available and enabled by default in OpenShift Container Platform 4.11. For more information, see Preparing the hub cluster for ZTP .

1.9.19.5. Indication of done for ZTP

A new tool is available that simplifies the process of checking for a completed zero touch provisioning (ZTP) installation using the Red Hat Advanced Cluster Management (RHACM) static validator inform policy. It provides an indication of done for ZTP installations by capturing the criteria for a completed installation and validating that it moves to a compliant state only when ZTP provisioning of the spoke cluster is complete.

This policy can be used for deployments of single node clusters, three-node clusters, and standard clusters. To learn more about the validator inform policy, see Indication of done for ZTP installations .

1.9.19.6. Enhancements to ZTP

For OpenShift Container Platform 4.10, there are a number of updates that make it easier to configure the hub cluster and generate source CRs. New PTP and UEFI secure boot features for spoke clusters are also available. The following is a summary of these features:

- You can add or modify existing source CRs in the **ztp-site-generate** container, rebuild it, and make it available to the hub cluster, typically from the disconnected registry associated with the hub cluster.
- You can configure PTP fast events for vRAN clusters that are deployed using the GitOps zero touch provisioning (ZTP) pipeline.

- You can configure UEFI secure boot for vRAN clusters that are deployed using the GitOps ZTP pipeline.
- You can use Topology Aware Lifecycle Manager to orchestrate the application of the configuration CRs to the hub cluster.

1.9.19.7. ZTP support for multicluster deployment

Zero touch provisioning (ZTP) provides support for multicluster deployment, including single node clusters, three-node clusters, and standard OpenShift clusters. This includes the installation of OpenShift and deployment of the distributed units (DUs) at scale. This gives you the ability to deploy nodes with master, worker, and master and worker roles. ZTP multinode support is implemented through the use of **SiteConfig** and **PolicyGenTemplate** custom resources (CRs). The overall flow is identical to the ZTP support for single node clusters, with some differentiation in configuration depending on the type of cluster:

In the **SiteConfig** file:

- Single node clusters must have exactly one entry in the **nodes** section.
- Three-node clusters must have exactly three entries defined in the **nodes** section.
- Standard OpenShift clusters must have exactly three entries in the **nodes** section with role: master and one or more additional entries with role: worker.

The **PolicyGenTemplate** file tells the Policy Generator where to categorize the generated policies. Example **PolicyGenTemplate** files provide you with example files to simplify your deployments:

- The example common **PolicyGenTemplate** file is common across all types of clusters.
- Example group **PolicyGenTemplate** files for single node, three-node, and standard clusters are provided.
- Site-specific **PolicyGenTemplate** files specific to each site are provided.

To learn more about multicluster deployment, see Deploying a managed cluster with SiteConfig and ZTP.

1.9.19.8. Support for unsecured OS images with Assisted Installer

This release includes the following warning when enabling TLS for the HTTPD server using the Assisted Installer in IPI or ZTP disconnected environments. When enabling TLS for the HTTPD server in these environments, you must confirm the root certificate is signed by an authority trusted by the client and verify the trusted certificate chain between your OpenShift Container Platform hub and spoke clusters and the HTTPD server. Using a server configured with an untrusted certificate prevents the images from being downloaded to the image creation service. Using untrusted HTTPS servers is not supported.

1.9.19.9. Known issues

- The Kubelet service monitor scrape interval is currently set to a hard-coded value. This means that there is less available CPU resources for workloads. (BZ#2035046)
- Deploying a single node OpenShift cluster for vRAN Distributed Units can take up to 4 hours. (BZ#2035036)

- Currently, if an RHACM policy was enforced to a target cluster, you can create a **ClusterGroupUpgrade** CR including that enforced policy again as a **managedPolicy** to the same target cluster. This should not be possible. (BZ#2044304)

- If a **ClusterGroupUpgrade** CR has a **blockingCR** specified, and that **blockingCR** fails silently, for example if there is a typo in the list of clusters, the **ClusterGroupUpgrade** CR is applied even though the **blockingCR** is not applied in the cluster. (BZ#2042601)

- If a **ClusterGroupUpgrade** CR validation fails for any reason, for example, because of an invalid spoke name, no status is available for the **ClusterGroupUpgrade** CR, as if the CR is disabled. (BZ#2040828)

- Currently, for **ClusterGroupUpgrade** CR state changes, there is only a single condition type available - **Ready**. The **Ready** condition can have a status of **True** or **False** only. This does not reflect the range of states the **ClusterGroupUpgrade** CR can be in. (BZ#2042596)

- When deploying a multi-node cluster on bare-metal nodes, the machine config pool (MCP) adds an additional CRI-O drop-in that circumvents the container mount namespace drop-in. This results in CRI-O being in the base namespace while the kubelet is in the hidden namespace. All containers fail to get any kubelet-mounted filesystems, such as secrets and tokens. (BZ#2028590)

- Installing RHACM 2.5.0 in the customized namespace causes the **infrastructure-operator** pod to fail due to insufficient privileges. (BZ#2046554)

- OpenShift Container Platform limits object names to 63 characters. If a policy name defined in a **PolicyGenTemplate** CR approaches this limit, the Topology Aware Lifecycle Manager cannot create child policies. When this occurs, the parent policy remains in a **NonCompliant** state. (BZ#2057209)

- In the default ZTP Argo CD configuration, cluster names cannot begin with **ztp**. Using names starting with **ztp** for clusters deployed with Zero Touch Provisioning (ZTP) results in provisioning not completing. As a workaround, ensure that either cluster names do not start with **ztp**, or adjust the Argo CD policy application namespace to a pattern that excludes the names of your clusters but still matches your policy namespace. For example, if your cluster names start with **ztp**, change the pattern in the Argo CD policy app configuration to something different, like **ztp-**. (BZ#2049154)

- During a spoke cluster upgrade, one or more reconcile errors is recorded in the container log. The number of errors corresponds to the number of child policies. The error causes no noticeable impact to the cluster. The following is an example of the reconcile error:

```
2022-01-21T00:14:44.697Z        INFO    controllers.ClusterGroupUpgrade Upgrade is
completed
2022-01-21T00:14:44.892Z        ERROR   controller-
runtime.manager.controller.clustergroupupgrade      Reconciler error        {"reconciler group":
"ran.openshift.io", "reconciler kind": "ClusterGroupUpgrade", "name": "timeout",
"namespace": "default", "error": "Operation cannot be fulfilled on
clustergroupupgrades.ran.openshift.io \"timeout\": the object has been modified; please apply
your changes to the latest version and try again"}
sigs.k8s.io/controller-runtime/pkg/internal/controller.(*Controller).processNextWorkItem
        /go/pkg/mod/sigs.k8s.io/controller-
runtime@v0.9.2/pkg/internal/controller/controller.go:253
sigs.k8s.io/controller-runtime/pkg/internal/controller.(*Controller).Start.func2.2
        /go/pkg/mod/sigs.k8s.io/controller-
runtime@v0.9.2/pkg/internal/controller/controller.go:214
```

(BZ#2043301)

- During a spoke cluster upgrade from 4.9 to 4.10, with heavy workload running, the **kube-apiserver** pod can take longer than the expected time to start. As a result, the upgrade does not complete and the **kube-apiserver** rolls back to the previous version. (BZ#2064024)

- If you deploy the AMQ Interconnect Operator, pods run on IPv4 nodes only. The AMQ Interconnect Operator is not supported on IPv6 nodes. (ENTMQIC-3297)

1.9.19.10. Bug fixes

- Previously, the Ingress Operator detected changes made through the Ingress Controller and set the **Upgradeable** status condition of the Ingress Operator to **False**. The **False** status condition blocked upgrades. With this update, the Ingress Operator no longer blocks upgrades. (BZ#2097735)

1.9.19.11. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.20. RHSA-2022:5664 - OpenShift Container Platform 4.10.24 bug fix and security update

Issued: 2022-07-25

OpenShift Container Platform release 4.10.24 is now available. The bug fixes that are included in the update are listed in the RHSA-2022:5664 advisory. There are no RPM packages for this release.

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

```
$ oc adm release info 4.10.24 --pullspecs
```

1.9.20.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.21. RHSA-2022:5730 - OpenShift Container Platform 4.10.25 bug fix and security update

Issued: 2022-08-01

OpenShift Container Platform release 4.10.25, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHSA-2022:5730 advisory. The RPM packages that are included in the update are provided by the RHSA-2022:5729 advisory.

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

```
$ oc adm release info 4.10.25 --pullspecs
```

1.9.21.1. Bug fixes

- Previously, where clusters had a Security Context Constraint (SCC), the default IngressController Deployment could cause pods to fail to start. This was due to the default container name **router** being created without requesting sufficient permissions in the **securityContext** of the container. With this update, router pods will be admitted to the correct SCC and created without error. (BZ#2079034)

- Previously, routers in the terminating state delay the **oc cp** command, which delayed the **must-gather**. With this update, a timeout for each **oc cp** command has been set eliminating the delay of the **must-gathers**. (BZ#2106842)

1.9.21.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.22. RHSA-2022:5875 - OpenShift Container Platform 4.10.26 bug fix and security update

Issued: 2022-08-08

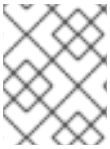
OpenShift Container Platform release 4.10.26, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHSA-2022:5875 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:5874 advisory.

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

```
$ oc adm release info 4.10.26 --pullspecs
```

1.9.22.1. Bug fixes

- Previously, new regions were not recognized by the AWS SDK and the machine controller could not use them. This problem occurred because the AWS SDK only recognized regions from the time AWS SDK was vendored. With this update, administrators can use **DescribeRegions** to check the specified region for a machine and create new machines in regions unknown to SDK. (BZ#2109124)



NOTE

This is a new AWS permission and you must update credentials for manual mode clusters with the new permission.

1.9.22.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.23. RHBA-2022:6095 - OpenShift Container Platform 4.10.28 bug fix and security update

Issued: 2022-08-23

OpenShift Container Platform release 4.10.28, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHBA-2022:6095 advisory. The RPM packages that are included in the update are provided by the RHSA-2022:6094 advisory.

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

```
$ oc adm release info 4.10.28 --pullspecs
```

1.9.23.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.24. RHSA-2022:6133 - OpenShift Container Platform 4.10.30 bug fix and security update

Issued: 2022-08-31

OpenShift Container Platform release 4.10.30, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHSA-2022:6133 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:6132 advisory.

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

```
$ oc adm release info 4.10.30 --pullspecs
```

1.9.24.1. Features

1.9.24.1.1. General availability of pod-level bonding for secondary networks

With this update, **Using pod-level bonding** is now generally available.

1.9.24.2. Bug fixes

- Previously, the functionality of Bond-CNI was limited to only active-backup mode. With this update, the bonding modes supported are:
  - **balance-rr** -0
  - **active-backup** -1
  - **balance-xor** -2

  (BZ#2102047)

1.9.24.3. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.25. RHSA-2022:6258 - OpenShift Container Platform 4.10.31 bug fix and security update

Issued: 2022-09-07

OpenShift Container Platform release 4.10.31, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHSA-2022:6258 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:6257 advisory.

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

```
$ oc adm release info 4.10.31 --pullspecs
```

1.9.25.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.26. RHBA-2022:6372 - OpenShift Container Platform 4.10.32 bug fix

Issued: 2022-09-13

OpenShift Container Platform release 4.10.32 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:6372 advisory. There are no RPM packages for this release.

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

```
$ oc adm release info 4.10.32 --pullspecs
```

1.9.26.1. Bug fixes

- Previously, dual-stack clusters using the PROXY protocol only enabled it on IPv6 and not IPv4. With this update, OpenShift Container Platform now enables the PROXY protocol for both IPv6 and IPv4 on dual-stack clusters. (**BZ#2096362**)

1.9.26.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.27. RHBA-2022:6532 - OpenShift Container Platform 4.10.33 bug fix and security update

Issued: 2022-09-20

OpenShift Container Platform release 4.10.33, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHBA-2022:6532 advisory. The RPM packages that are included in the update are provided by the RHSA-2022:6531 advisory.

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

```
$ oc adm release info 4.10.33 --pullspecs
```

1.9.27.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.28. RHBA-2022:6663 - OpenShift Container Platform 4.10.34 bug fix and security update

Issued: 2022-09-27

OpenShift Container Platform release 4.10.34, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHBA-2022:6663 advisory. The RPM packages that are included in the update are provided by the RHSA-2022:6661 advisory.

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

```
$ oc adm release info 4.10.34 --pullspecs
```

1.9.28.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.29. RHBA-2022:6728 - OpenShift Container Platform 4.10.35 bug fix update

Issued: 2022-10-04

OpenShift Container Platform release 4.10.35, is now available. The bug fixes that are included in the update are listed in the RHBA-2022:6728 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:6727 advisory.

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

```
$ oc adm release info 4.10.35 --pullspecs
```

1.9.29.1. Bug fixes

- Previously, the logic in the Ingress Operator did not validate whether a kubernetes service object in the **openshift-ingress** namespace was created by the Ingress Controller it was attempting to reconcile with. Consequently, the Operator would modify or remove kubernetes services with the same name and namespace regardless of ownership. With this update, the Ingress Operator now checks for the ownership of existing kubernetes services it attempts to create or remove. If the ownership does not match, the Ingress Operator provides an error. (**OCPBUGS-1623**)

1.9.29.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.30. RHSA-2022:6805 - OpenShift Container Platform 4.10.36 bug fix update

Issued: 2022-10-12

OpenShift Container Platform release 4.10.36, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHSA-2022:6805 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:6803 advisory.

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

```
$ oc adm release info 4.10.36 --pullspecs
```

1.9.30.1. Bug fixes

- Previously, the router process was ignoring the **SIGTERM** shutdown signal during initialization. This resulted in container shutdown times of one hour. With this update, the router now responds to **SIGTERM** signals during initialization. (BZ#2098230)

1.9.30.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.31. RHBA-2022:6901 - OpenShift Container Platform 4.10.37 bug fix update

Issued: 2022-10-18

OpenShift Container Platform release 4.10.37, is now available. The bug fixes that are included in the update are listed in the RHBA-2022:6901 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:6899 advisory.

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

```
$ oc adm release info 4.10.37 --pullspecs
```

1.9.31.1. Bug fixes

- Previously, adding an IP address to one or more control plane nodes caused the etcd cluster Operator to fail to regenerate etcd serving certificates for the node. With this update, the etcd cluster Operator regenerates serving certificates for changes to an existing node. (OCPBUGS-1758)

1.9.31.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.32. RHBA-2022:7035 - OpenShift Container Platform 4.10.38 bug fix update

Issued: 2022-10-25

OpenShift Container Platform release 4.10.38, is now available. The bug fixes that are included in the update are listed in the RHBA-2022:7035 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:7033 advisory.

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

```
$ oc adm release info 4.10.38 --pullspecs
```

1.9.32.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.33. RHSA-2022:7211 - OpenShift Container Platform 4.10.39 bug fix and security update

Issued: 2022-11-01

OpenShift Container Platform release 4.10.39, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHSA-2022:7211 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:7210 advisory.

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

```
$ oc adm release info 4.10.39 --pullspecs
```

1.9.33.1. Notable technical changes

- With this release, when the service account issuer is changed to a custom one, existing bound service tokens are no longer invalidated immediately. Instead, when the service account issuer is changed, the previous service account issuer continues to be trusted for 24 hours.

For more information, see Configuring bound service account tokens using volume projection .

1.9.33.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.34. RHBA-2022:7298 - OpenShift Container Platform 4.10.40 bug fix update

Issued: 2022-11-09

OpenShift Container Platform release 4.10.40, is now available. The bug fixes that are included in the update are listed in the RHBA-2022:7298 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:7297 advisory.

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

```
$ oc adm release info 4.10.40 --pullspecs
```

1.9.34.1. Bug fixes

- Before this update, the **noAllowedAddressPairs** setting applied to all subnets on the same network. With this update, the **noAllowedAddressPairs** setting now only applies to its matching subnet. (**OCPBUGS-1951**)

1.9.34.2. Notable technical changes

- The Cloud Credential Operator utility (**ccoctl**) now creates secrets that use regional endpoints for the AWS Security Token Service (AWS STS) . This approach aligns with AWS recommended best practices.

1.9.34.3. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.35. RHBA-2022:7866 - OpenShift Container Platform 4.10.41 bug fix and security update

Issued: 2022-11-18

OpenShift Container Platform release 4.10.41, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHBA-2022:7866 advisory. The RPM packages that are included in the update are provided by the RHSA-2022:7865 advisory.

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

```
$ oc adm release info 4.10.41 --pullspecs
```

1.9.35.1. Notable technical changes

- With this release, when you delete GCP resources with the Cloud Credential Operator utility, you must specify the directory containing the files for the component **CredentialsRequest** objects.

1.9.35.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.36. RHBA-2022:8496 - OpenShift Container Platform 4.10.42 bug fix update

Issued: 2022-11-22

OpenShift Container Platform release 4.10.42 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:8496 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:8495 advisory.

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

```
$ oc adm release info 4.10.42 --pullspecs
```

1.9.36.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.37. RHBA-2022:8623 - OpenShift Container Platform 4.10.43 bug fix update

Issued: 2022-11-29

OpenShift Container Platform release 4.10.43 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:8623 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:8622 advisory.

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

```
$ oc adm release info 4.10.43 --pullspecs
```

1.9.37.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.38. RHBA-2022:8882 - OpenShift Container Platform 4.10.45 bug fix update

Issued: 2022-12-14

OpenShift Container Platform release 4.10.45 is now available. The bug fixes that are included in the update are listed in the RHBA-2022:8882 advisory. The RPM packages that are included in the update are provided by the RHBA-2022:8881 advisory.

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

```
$ oc adm release info 4.10.45 --pullspecs
```

1.9.38.1. Bug fixes

- Previously, some object storage instances responded with **204 No Content** when no content displayed. The Red Hat OpenStack Platform (RHOSP) SDK used in OpenShift Container Platform did not handle 204s correctly. With this update, the installation program works around the issue when there are zero items to list. (**OCPBUGS-4160**)

1.9.38.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.39. RHBA-2022:9099 - OpenShift Container Platform 4.10.46 bug fix and security update

Issued: 2023-01-04

OpenShift Container Platform release 4.10.46, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHBA-2022:9099 advisory. The RPM packages that are included in the update are provided by the RHSA-2022:9098 advisory.

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

```
$ oc adm release info 4.10.46 --pullspecs
```

1.9.39.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.40. RHSA-2023:0032 - OpenShift Container Platform 4.10.47 bug fix and security update

Issued: 2023-01-04

OpenShift Container Platform release 4.10.47, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHSA-2023:0032 advisory. The RPM packages that are included in the update are provided by the RHBA-2023:0031 advisory.

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

```
$ oc adm release info 4.10.47 --pullspecs
```

1.9.40.1. Enhancements

- IPv6 unsolicited neighbor advertisements and IPv4 gratuitous address resolution protocol now default on the SR-IOV CNI plugin. Pods created with the Single Root I/O Virtualization (SR-IOV) CNI plugin, where the IP address management CNI plugin has assigned IPs, now send IPv6 unsolicited neighbor advertisements and/or IPv4 gratuitous address resolution protocol by default onto the network. This enhancement notifies hosts of the new pod's MAC address for a particular IP to refresh ARP/NDP caches with the correct information. For more information, see Supported devices.

1.9.40.2. Bug fixes

- Previously, in CoreDNS v1.7.1, all upstream cache refreshes used DNSSEC. Bufsize was hardcoded to 2048 bytes for the upstream query, causing some DNS upstream queries to break when there were UDP Payload limits within the networking infrastructure. With this update, OpenShift Container Platform always uses bufsize 512 for upstream cache requests as that is the bufsize specified in the Corefile. Customers might be impacted if they rely on the incorrect functionality of bufsize 2048 for upstream DNS requests. (**OCPBUGS-2902**)

- Previously, OpenShift Container Platform did not handle object storage instances that responded with **204 No Content**. This caused problems for the Red Hat OpenStack Platform (RHOSP) SDK. With this update, the installation program works around the issue when there are zero objects to list in a Swift container. (**OCPBUGS-5112**)

1.9.40.3. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.41. RHSA-2023:0241 - OpenShift Container Platform 4.10.50 bug fix and security update

Issued: 2023-01-24

OpenShift Container Platform release 4.10.50, which includes security updates, is now available. The bug fixes that are included in the update are listed in the RHSA-2023:0241 advisory. The RPM packages that are included in the update are provided by the RHBA-2023:0240 advisory.

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

```
$ oc adm release info 4.10.50 --pullspecs
```

1.9.41.1. Bug fixes

- Previously, when rotating Red Hat OpenStack Platform (RHOSP) credentials, the Cinder Container Storage Interface driver would continue to use old credentials. Using any old credentials that were invalid would cause all volume operations to fail. With this update, the Cinder Container Storage Interface driver is updated automatically when the Red Hat OpenStack Platform (RHOSP) credentials are updated. (**OCPBUGS-4717**)

- * Previously, pod failures were artificially extending the validity period of certificates causing them to incorrectly rotate. With this update, the certificate validity period is accurately determined, which helps certificates to rotate correctly. (**BZ#2020484**)

1.9.41.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.42. RHSA-2023:0561 - OpenShift Container Platform 4.10.51 bug fix and security update

Issued: 2023-02-08

OpenShift Container Platform release 4.10.51, which includes security updates, is now available. Bug fixes included in the update are listed in the RHSA-2023:0561 advisory. RPM packages included in the update are provided by the RHSA-2023:0560 advisory.

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

```
$ oc adm release info 4.10.51 --pullspecs
```

1.9.42.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.43. RHSA-2023:0698 - OpenShift Container Platform 4.10.52 bug fix and security update

Issued: 2023-02-15

OpenShift Container Platform release 4.10.52, which includes security updates, is now available. Bug fixes included in the update are listed in the RHSA-2023:0698 advisory. RPM packages included in the update are provided by the RHSA-2023:0697 advisory.

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

```
$ oc adm release info 4.10.52 --pullspecs
```

1.9.43.1. Bug fixes

- Previously, when a Redfish system features a Settings URI, the Ironic provisioning service always attempts to use this URI to make changes to boot related BIOS settings. However, bare-metal provisioning fails if the Baseboard Management Controller (BMC) features a Settings URI but

does not support changing a particular BIOS setting by using this Settings URI. In OpenShift Container Platform 4.10 and later, if a system features a Settings URI, Ironic verifies that it can change a particular BIOS setting by using the Settings URI before proceeding. Otherwise, Ironic implements the change by using the System URI. This additional logic ensures that Ironic can apply boot-related BIOS setting changes and bare-metal provisioning can succeed. (OCPBUGS-6886)

- Previously due to a missing definition for **spec.provider**, the **Operator details** page failed when trying to show **ClusterServiceVersion**. With this update, the user interface works without **spec.provider** and the **Operator details** page does not fail. (OCPBUGS-6690)

1.9.43.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.44. RHSA-2023:0698 - OpenShift Container Platform 4.10.53 bug fix and security update

Issued: 2023-03-01

OpenShift Container Platform release 4.10.53, which includes security updates, is now available. Bug fixes included in the update are listed in the RHSA-2023:0899 advisory. RPM packages included in the update are provided by the RHBA-2023:0898 advisory.

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

```
$ oc adm release info 4.10.53 --pullspecs
```

1.9.44.1. Bug fixes

- In order to be compatible with OpenStack clouds that do not have Swift installed, Cluster Image Registry Operator (CIRO) has a mechanism for automatically choosing the storage back-end during the first boot. If Swift is available, Swift is used. Otherwise, a persistent volume claim (PVC) is issued and block storage is used. Previously, the CIRO would fall back to using a PVC when it failed to reach Swift. In particular, a lack of connectivity during the first boot would make CIRO fall back to using a PVC. With this change, a failure to reach the OpenStack API, or other incidental failures, cause CIRO to retry the probe. The fallback to PVC occurs only if the OpenStack catalog is correctly found, and it does not contain object storage, or if the current user does not have permission to list containers. (OCPBUGS-5974)

- Previously, the User Provisioned Infrastructure (UPI) did not create a server group for compute machines. OpenShift Container Platform 4.10 updates the UPI script, so that the script creates a server group for compute machines. The UPI script installation method now aligns with the installer-provisioned installation (IPI) method. (OCPBUGS-2731)

1.9.44.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.45. RHSA-2023:1154 - OpenShift Container Platform 4.10.54 bug fix and security update

Issued: 2023-03-15

OpenShift Container Platform release 4.10.54, which includes security updates, is now available. Bug fixes included in the update are listed in the RHSA-2023:1154 advisory. RPM packages included in the update are provided by the RHBA-2023:1153 advisory.

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

```
$ oc adm release info 4.10.54 --pullspecs
```

1.9.45.1. Bug fixes

- Previously, when editing any pipeline in the OpenShift Container Platform console, the correct data was not rendered in the **Pipeline builder** and **YAML view** configuration options, which prevented you from editing the pipeline in the **Pipeline builder**. With this update, data is parsed correctly and you can edit the pipeline using the builder. (**OCPBUGS-7657**)

1.9.45.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.46. RHSA-2023:1392 - OpenShift Container Platform 4.10.55 bug fix and security update

Issued: 2023-03-29

OpenShift Container Platform release 4.10.55, which includes security updates, is now available. Bug fixes included in the update are listed in the RHSA-2023:1392 advisory. RPM packages included in the update are provided by the RHBA-2023:1391 advisory.

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

```
$ oc adm release info 4.10.55 --pullspecs
```

1.9.46.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.47. RHSA-2023:1656 - OpenShift Container Platform 4.10.56 bug fix and security update

Issued: 2023-04-12

OpenShift Container Platform release 4.10.56, which includes security updates, is now available. Bug fixes included in the update are listed in the RHSA-2023:1656 advisory. RPM packages included in the update are provided by the RHSA-2023:1655 advisory.

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

```
$ oc adm release info 4.10.56 --pullspecs
```

1.9.47.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.48. RHBA-2023:1782 - OpenShift Container Platform 4.10.57 bug fix update

Issued: 2023-04-19

OpenShift Container Platform release 4.10.57 is now available. Bug fixes included in the update are listed in the RHBA-2023:1782 advisory. There are no RPM packages for this update.

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

```
$ oc adm release info 4.10.57 --pullspecs
```

1.9.48.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.49. RHBA-2023:1867 - OpenShift Container Platform 4.10.58 bug fix and security update

Issued: 2023-04-26

OpenShift Container Platform release 4.10.58 is now available. Bug fixes included in the update are listed in the RHBA-2023:1867 advisory. RPM packages included in the update are provided by the RHSA-2023:1866 advisory.

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

```
$ oc adm release info 4.10.58 --pullspecs
```

1.9.49.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.50. RHBA-2023:2018 - OpenShift Container Platform 4.10.59 bug fix update

Issued: 2023-05-03

OpenShift Container Platform release 4.10.59 is now available. Bug fixes included in the update are listed in the RHBA-2023:2018 advisory. RPM packages included in the update are provided by the RHSA-2023:2017 advisory.

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

```
$ oc adm release info 4.10.59 --pullspecs
```

1.9.50.1. Bug fixes

- Previously, the topology sidebar did not display updated information. When you updated the resources directly from the topology sidebar, you had to reopen the sidebar to see the changes. With this fix, the updated resources are displayed correctly. As a result, you can see the latest changes directly in the topology sidebar. (OCPBUGS-12438)

- Previously, when creating a **Secret**, the **Start Pipeline** model created an invalid JSON value. As a result, the **Secret** was unusable and the **PipelineRun** could fail. With this fix, the **Start Pipeline** model creates a valid JSON value for the secret. Now, you can create valid secrets while starting a pipeline. (OCPBUGS-7961)

1.9.50.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.51. RHBA-2023:3217 - OpenShift Container Platform 4.10.60 bug fix and security update

Issued: 2023-05-24

OpenShift Container Platform release 4.10.60, which includes security updates, is now available. Bug fixes included in the update are listed in the RHBA-2023:3217 advisory. RPM packages included in the update are provided by the RHSA-2023:3216 advisory.

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

```
$ oc adm release info 4.10.60 --pullspecs
```

1.9.51.1. Features

1.9.51.1.1. Controls for the verbosity of MetalLB logs

- With this release, you can control the verbosity of MetalLB logs. You can control logging levels by using the following values for the **logLevel** specification in the MetalLB custom resource (CR):
  - all
  - debug
  - info
  - warn
  - error
  - none

  For example, you can specify the **debug** value to include diagnostic logging information that is helpful for troubleshooting.

  For more information about logging levels for MetalLB, see Setting the MetalLB logging levels (OCPBUGS-11861)

1.9.51.2. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster within a minor version by using the CLI for instructions.

1.9.52. RHSA-2023:3363 - OpenShift Container Platform 4.10.61 bug fix and security update

Issued: 2023-06-07

OpenShift Container Platform release 4.10.61, which includes security updates, is now available. Bug fixes included in the update are listed in the RHSA-2023:3363 advisory. RPM packages included in the update are provided by the RHSA-2023:3362 advisory.

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

```
$ oc adm release info 4.10.61 --pullspecs
```

1.9.52.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster using the CLI for instructions.

1.9.53. RHSA-2023:3626 - OpenShift Container Platform 4.10.62 bug fix and security update

Issued: 2023-06-23

OpenShift Container Platform release 4.10.62, which includes security updates, is now available. Bug fixes included in the update are listed in the RHBA-2023:3626 advisory. RPM packages included in the update are provided by the RHSA-2023:3625 advisory.

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

```
$ oc adm release info 4.10.62 --pullspecs
```

1.9.53.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster using the CLI for instructions.

1.9.54. RHSA-2023:3911 - OpenShift Container Platform 4.10.63 bug fix and security update

Issued: 2023-07-06

OpenShift Container Platform release 4.10.63, which includes security updates, is now available. This update includes a Red Hat security bulletin for customers who run OpenShift Container Platform in FIPS mode. For more information, see RHSB-2023:001.

Bug fixes included in the update are listed in the RHSA-2023:3911 advisory. RPM packages included in the update are provided by the RHSA-2023:3910 advisory.

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

```
$ oc adm release info 4.10.63 --pullspecs
```

1.9.54.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster using the CLI for instructions.

1.9.55. RHBA-2023:4217 - OpenShift Container Platform 4.10.64 bug fix update

Issued: 2023-07-26

OpenShift Container Platform release 4.10.64 is now available. Bug fixes included in the update are listed in the RHBA-2023:4217 advisory. RPM packages included in the update are provided by the RHBA-2023:4219 advisory.

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

```
$ oc adm release info 4.10.64 --pullspecs
```

1.9.55.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster using the CLI for instructions.

1.9.56. RHBA-2023:4445 - OpenShift Container Platform 4.10.65 bug fix update

Issued: 2023-08-09

OpenShift Container Platform release 4.10.65 is now available. Bug fixes included in the update are listed in the RHBA-2023:4445 advisory. RPM packages included in the update are provided by the RHBA-2023:4447 advisory.

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

```
$ oc adm release info 4.10.65 --pullspecs
```

1.9.56.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster using the CLI for instructions.

1.9.57. RHBA-2023:4667 - OpenShift Container Platform 4.10.66 bug fix update

Issued: 2023-08-23

OpenShift Container Platform release 4.10.66 is now available. Bug fixes included in the update are listed in the RHBA-2023:4667 advisory. RPM packages included in the update are provided by the RHBA-2023:4669 advisory.

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

```
$ oc adm release info 4.10.66 --pullspecs
```

1.9.57.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster using the CLI for instructions.

1.9.58. RHBA-2023:4896 - OpenShift Container Platform 4.10.67 bug fix and security update

Issued: 2023-09-06

OpenShift Container Platform release 4.10.67, which includes security updates, is now available. Bug fixes included in the update are listed in the RHBA-2023:4896 advisory. RPM packages included in the update are provided by the RHSA-2023:4898 advisory.

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

```
$ oc adm release info 4.10.67 --pullspecs
```

1.9.58.1. Updating

To update an existing OpenShift Container Platform 4.10 cluster to this latest release, see Updating a cluster using the CLI for instructions.