Red Hat OpenShift Container Storage 4.7

4.7 Release Notes

Release notes for feature and enhancements, known issues, and other important release information

Last Updated: 2022-06-15

Red Hat OpenShift Container Storage 4.7 4.7 Release Notes

Release notes for feature and enhancements, known issues, and other important release information

Legal Notice

Abstract

The release notes for Red Hat OpenShift Container Storage 4.7 summarize all new features and enhancements, notable technical changes, and any known bugs upon general availability.

Table of Contents

CHAPTER 1. INTRODUCTION

Red Hat OpenShift Container Storage is software-defined storage that is optimized for container environments. It runs as an operator on OpenShift Container Platform to provide highly integrated and simplified persistent storage management for containers.

Red Hat OpenShift Container Storage is integrated into the latest Red Hat OpenShift Container Platform to address platform services, application portability, and persistence challenges. It provides a highly scalable backend for the next generation of cloud-native applications, built on a new technology stack that includes Red Hat Ceph Storage, the Rook.io Operator, and NooBaa's Multicloud Object Gateway technology.

Red Hat OpenShift Container Storage provides a trusted, enterprise-grade application development environment that simplifies and enhances the user experience across the application lifecycle in a number of ways:

- Provides block storage for databases.
- Shared file storage for continuous integration, messaging, and data aggregation.
- Object storage for cloud-first development, archival, backup, and media storage.
- Scale applications and data exponentially.
- Attach and detach persistent data volumes at an accelerated rate.
- Stretch clusters across multiple data-centers or availability zones.
- Establish a comprehensive application container registry.
- Support the next generation of OpenShift workloads such as Data Analytics, Artificial Intelligence, Machine Learning, Deep Learning, and Internet of Things (IoT).
- Dynamically provision not only application containers, but data service volumes and containers, as well as additional OpenShift Container Platform nodes, Elastic Block Store (EBS) volumes and other infrastructure services.

1.1. ABOUT THIS RELEASE

Red Hat OpenShift Container Storage 4.7 (RHSA-2021:2042 and RHSA-2021:2041) is now available. New enhancements, features, and known issues that pertain to OpenShift Container Storage 4.7 are included in this topic.

Red Hat OpenShift Container Storage 4.7 is supported on the Red Hat OpenShift Container Platform versions 4.7. For more information, see Red Hat OpenShift Container Storage Supportability and Interoperability Guide.

With the release of OpenShift Container Storage 4.7, version 4.4 is now end of life. For more information, see Red Hat OpenShift Container Platform Life Cycle Policy .

CHAPTER 2. NEW FEATURES

This section describes new features introduced in Red Hat OpenShift Container Storage 4.7.

IBM Power Systems general availability support

OpenShift Container Storage can now be installed and managed using IBM Power Systems. For more information see, Deploying OpenShift Container Storage using IBM Power Systems Guide .

Upgrading OpenShift Container Storage 4.6 to OpenShift Container Storage 4.7 on IBM Power Systems is not supported. IBM Power Systems on OpenShift Container Storage 4.7 must be a greenfield installation.

Unsupported features for IBM Power Systems are identified at Unsupported Features

IBM Z and LinuxONE general availability support

OpenShift Container Storage can now be installed and managed using IBM Z and LinuxONE. For more information see, Deploying OpenShift Container Storage using IBM Z and LinuxONE .

Upgrading OpenShift Container Storage 4.6 to OpenShift Container Storage 4.7 on IBM Z and LinuxONE is not supported. IBM Z and LinuxONE on OpenShift Container Storage 4.7 must be a greenfield installation.

Unsupported features for IBM Z and LinuxONE are identified at Unsupported Features

VMware vSphere 7 general availability support

OpenShift Container Storage can now be installed and managed using VMware vSphere 7. It supports internal clusters and consuming external clusters. Recommended versions are vSphere 6.7 Update 2 or vSphere 7. For more information, see VMware vSphere infrastructure requirements.

VMware vSphere installer-provisioned infrastructure general availability support

OpenShift Container Storage can now be installed and managed using VMware vSphere on both installer-provisioned infrastructure and user-provisioned infrastructure. For more information see, Deploying OpenShift Container Storage on VMware vSphere .

Red Hat Virtualization general availability support

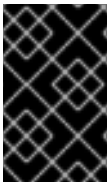
OpenShift Container Storage can now be installed using Red Hat Virtualization. For more information see, Deploying and managing OpenShift Container Storage using Red Hat Virtualization guide .

Encrypted storage data

Red Hat OpenShift Container Storage supports cluster-wide encryption (encryption-at-rest) for all the disks in the storage cluster. It is also used for the Multicloud Object Gateway data encryption. You can use an external Key Management System (KMS) to store the encryption keys in Red Hat OpenShift Container Storage 4.7.

Cluster-wide encryption is supported in OpenShift Container Storage 4.6 without KMS, while it is supported in OpenShift Container Storage 4.7 with and without KMS.

Currently, HashiCorp Vault is the only supported KMS. With OpenShift Container Storage 4.7.0 and 4.7.1, only HashiCorp Vault Key/Value (KV) secret engine API, version 1 is supported. Starting with OpenShift Container Storage 4.7.2, HashiCorp Vault KV secret engine API, versions 1 and 2 are supported.



IMPORTANT

Red Hat works with the technology partners to provide this documentation as a service to the customers. However, Red Hat does not provide support for the Hashicorp product. For technical assistance with this product, contact HashiCorp.

For more information, see Data encryption options and follow the OpenShift Container Storage documentation for deploying on your cloud or on-premise environment.

Flexible scaling of OpenShift Container Storage cluster

With flexible scaling enabled, you can add capacity by 1 or more OSDs at a time using the YAML instead of the default set of 3 OSDs. However, you need to make sure that you add disks in a way that the cluster remains balanced.

Flexible scaling is supported only for the internal-attached mode of storage cluster creation. Flexible scaling of storage clusters is available only for the new deployments of Red Hat OpenShift Container Storage 4.7 and not for the upgraded clusters.

To enable flexible scaling, create a cluster with minimum 3 nodes, and fewer than 3 availability zones. The OpenShift Web Console detects the 3 or more nodes spread across fewer than 3 availability zones and enables flexible scaling.

For more information, see Scaling Guide.

Updating backing stores configuration for object bucket class

With OpenShift Container Storage 4.7, you can update the configuration of the object backing stores for a bucket class using the OpenShift Web Console.

For more information, see Managing hybrid and multicloud resources Guide .

Adding namespace buckets using the Multicloud Object Gateway CLI and YAML

The Red Hat OpenShift Container Storage 4.7 documentation now includes instructions for adding namespace buckets using the Multicloud Object Gateway command-line interface and YAML. For more information, see Managing hybrid and multicloud resources Guide .

Guided tours

Self help guided tours are now available for OpenShift Container Storage 4.7 on the OpenShift Container Platform 4.7 web console.

The tours are a new capability to provide layered guidance in the console. The guided tours are available as **Quick Starts** in the **Overview** section on the top right corner of the console.

The **Quick Starts** helps customers to discover and enable OpenShift Container Storage, educates users on how to maximize OpenShift Container Storage features, and reduces the onboarding time of a new user.

The **Quick Starts** cover various topics as:

- Install OpenShift Container Storage Operator.
- Getting Started with OpenShift Container storage.
- OpenShift Container Storage Configuration & Management.

CHAPTER 3. ENHANCEMENTS

This section describes major enhancements introduced in Red Hat OpenShift Container Storage 4.7.

Better indication for successful upgrade of OpenShift Container Storage

Previously, it was difficult to determine if an OpenShift Container Storage upgrade had finished successfully. In some cases, the console would report everything was fine while in reality some components had not been upgraded to their new container images. With this update, the **StorageCluster** now checks and reports the running container images for all of its managed components, which aids in troubleshooting upgrade scenarios

OSD Pod Disruption Budgets redesign

Previously, the OpenShift Container Storage Pod Disruption Budgets (PDBs) by default have a **minUnavailable=0** and only allow rebooting of OSDs on a single node at a time. This caused the OCP console to constantly show a warning about nodes not being able to restart. With this update, OSD PDBs have the following redesigns:

- There is one OSD PDB in the beginning. This allows only one OSD to go down at any time.
- Once an OSD goes down, its failure domain is determined and any blocking OSD PDBs are created for other failure domains.
- The original OSD PDB created is deleted. As a result, all the OSDs can go down in the failure domain.

With the new design, users can drain multiple nodes in the same failure domain.

Update RGW address in the external mode

With this update, you can change the RGW address without affecting the Multicloud Object Gateway's(MCG) work if the MCG is configured with an RGW backingstore in the external mode.

Free space on RGW

Earlier, NooBaa bucket showed the storage capacity of 1PiB for all the buckets and did not show the free space on RGW. With this enhancement, the storage capacity of the Red Hat Ceph cluster is exported in the status field and now the NooBaa operator listens to the changes to this status field and updates the available capacity of every RGW based backingstore.

Allow the configuration of the Service monitor port to differ from the default ceph-mgr Prometheus port for external mode

With this enhancement, if the external Red Hat Ceph cluster is configured with a **ceph-mgr** Prometheus module listening on the non-default port (9283) then OpenShift Container Storage now can connect and consume those metrics, that is, the OpenShift Container Storage now accepts any monitoring port.

ocs-operator accepts non-default ports for monitoring services for external mode

Previously, there were no provisions in the **ocs-operator** to pass on a monitoring Prometheus service port other than the default port 9283. This made the port unusable for monitoring services. With this update, the **ocs-operator** has been enabled to accept and propagate non-default monitoring ports from external cluster JSON input and monitoring services work as expected.

Use an existing secret to create a new backingstore

With this enhancement, a new backingstore can be created through the Multicloud Object Gateway CLI using an existing secret.

Prioritize creating new OSD deployments over updating existing OSD deployments

Previously, for OSDs on Persistent Volume Claims, Rook implicitly favored updating existing OSDs before creating new OSDs resulting in new capacity not being added to the cluster until the end of the OSD reconcile. With this enhancement, the cluster now favors scaling up OSDs over updating existing OSDs to make new capacity available as soon as storage has been provisioned and this also reduces the reconcile time to 5-10 minutes from 15 while scaling up the number of OSDs in the cluster.

Public route for RGW

With this update, the OpenShift Container Storage operator now creates a route for the Red Hat Ceph Storage's RADOS Object Gateway (RGW) service.

OpenShift Container Storage deployed on ROKS without credentials in the IBM cloud setup

With this update, for the ease of installation in the IBM cloud setup when OpenShift Container Storage is deployed on ROKS and no credentials are provided for using ROKS as the default backingstore, a PV pool default BackingStore is created.

Prometheus alert for OSD restart

This enhancement adds a Prometheus alert to notify if an OpenShift Container Storage OSD restarts more than 5 times in 5 minutes. The alert message is as follows:

> Storage daemon osd.x has restarted 5 times in the last 5 minutes. Please check the pod events or ceph status to find out the cause.

where, **x** represents the OSD number.

System alerts for namespace buckets

With the release of the Red Hat OpenShift Container Storage 4.7, system alerts have been added for the namespace buckets and resources to get a better understanding of the current state of the system.

Log messages printing to the noobaa-endpoint pod log

Earlier, log messages were printed to the noobaa-endpoint pod log even if the debug option was not set. With this release, the log messages are printed to the noobaa-endpoint pod log only when the debug option is set.

CHAPTER 4. BUG FIXES

This section describes notable bug fixes introduced in Red Hat OpenShift Container Storage 4.7.

MGR pod restarts even if the MONs are down

Previously, when the nodes restarted the MGR pod might get stuck in a pod initialisation state which resulted in the inability to create new persistent volumes (PVs). With this update, the MGR pod restarts even if the MONs are down.

(BZ#2005515)

Multicloud Object Gateway is now available when hugepages are enabled on OpenShift Container Platform

Previously, Multicloud Object Gateway (MCG) db pod crashed as the Postgres failed to run on kubernetes when hugepages were enabled. With the current update, the hugepages for the MCG Postgres pods are disabled, and hence the MCG db pods do not crash.

(BZ#1968438)

PodDisruptionBudget alert no longer continiously shown

Previously, the **PodDisruptionBudget** alert, which is an OpenShift Container Platform alert, was continuously shown for object storage devices (OSDs). The underlying issue has been fixed, and the alert no longer shows.

(BZ#1788126)

must-gather log collection fail

Earlier, the copy pod did not try to re-flush the data at regular intervals causing the **must-gather** command to fail after the default 10 minutes time out. With this update, the copy pod keeps trying to collect the data at regular intervals generated by the **must-gather** command and now the **must-gather** commands run to completion.

(BZ#1884546)

You cannot create a PVC from a volume snapshot in the absence of **volumesnapshotclass**

A PVC can not be created from a volume snapshot in the absence of **volumesnapshotclass**. This issue is caused because the status of the volume snapshot changes to a **not ready** state on deleting the **volumesnapshotclass**. This issue has been fixed in OCP 4.7.0 and higher.

(BZ#1902711)

Core dump not propogated if a process crashed

Previously, core dumps were not propagated if a process crashed. With this release, a log-collector - a sidecar running next to the main ceph daemon has been introduced. On this, a **ShareProcessNamespace** flag is enabled and with this flag signals can be intercepted between containers allowing the coredumps to be generated.

(BZ#1904917)

Mulitple OSD removal job no longer fails

Previously, when triggering the job for multiple OSD removal, the template included a comma with the OSD IDs in the job name. This was causing the job template to fail. With this update, the OSD IDs have

been removed from the job name to maintain a valid format. The job names have been changed from **ocs-osd-removal-${FAILED_OSD_IDS}** to **ocs-osd-removal-job**.

(BZ#1908678)

Increased mon failover timeout

With this update **mon** failover timeout has been increased to 15 minutes on IBM Cloud. Previously, the **mons** would begin to failover while they were still coming up.

(BZ#1922421)

Rook now refuses to deploy OSD with a message on detecting unclean disks from previous OpenShift Container Storage installation

Previously, if a disk that had not been cleaned from a previous installation of OpenShift Container Storage was reused, Rook failed abruptly. With this update, Rook can now detect that the disk belongs to a different cluster and reject OSD deployment in that disk with an error message (BZ#1922954)

mon failover no longer makes Ceph inaccessible

Previously, if a mon went down while another mon was failing over, it caused the mons to lose quorum. When mons lose quorum Ceph becomes inaccessible. This update prevents voluntary mon drains while a mon is failing over so that Ceph never becomes inaccessible.

(BZ#1935065)

cpehcsi node plugin pods preoccupying ports for GRPC metrics

Previously, the **cephcsi** pods exposed GRPC metrics for debugging purposes, and hence the **cephcsi** node plugin pods used ports 9090 for RBD and 9091 for CephFS. As a result, the **cephsi** pods failed to come up due to the unavailability of the ports. With this release, GRPC metrics are disabled by default as it only required for debugging purposes and now **cephcsi** does not use the ports 9091 and 9090 on the node where node plugin pods are running.

(BZ#1937245)

rook-ceph-mds did not register the pod IP on monitor servers

Earlier, the **rook-ceph-mds** did not register the pod IP on the monitor servers and hence every mount on the filesystem timed out and PVCs could not be provisioned resulting in CephFS volume provisioning failure. With this release, an argument **--public-addr=podIP** is added to the MDS pod when the host network is not enabled. Hence, now the CephFS volume provisioning does not fail.

(BZ#1939272)

Errors in must gather due to failed rule evaluation

Earlier, the recording rule record: **cluster:ceph_disk_latency:join_ceph_node_disk_irate1m** did not get evaluated because **many-to-many** match is not allowed in Prometheus. As a result, there were errors in the **must gather** and in the deployment due to this failed rule evaluation. With this release, the query for recording rule has been updated to eliminate the **many-to-many** match scenarios, and hence now the Prometheus rule evaluations should not fail and there should not be any errors seen in the deployment.

(BZ#1904302)

CHAPTER 5. TECHNOLOGY PREVIEWS

This section describes technology preview features introduced in Red Hat OpenShift Container Storage 4.7.

Persistent volume encryption through storage class

You can encrypt persistent volumes (block only) with storage class encryption using an external Key Management System (KMS) to store device encryption keys. Persistent volume encryption is only available for RADOS Block Device (RBD) persistent volumes. Storage class encryption is supported in OpenShift Container Storage 4.7 or higher. For more information, see how to create a storage class with persistent volume encryption.

Disaster recovery using arbiter

Red Hat OpenShift Container Storage now provides metro disaster recovery (stretched cluster - Arbiter) feature. This feature allows you to enable a single cluster to be stretched across two zones with a third zone as the location for the arbiter during the storage cluster creation. For more information, see Disaster Recovery in the *Planning your deployment* guide.

Caching policy for object buckets

In Red Hat OpenShift Container Storage's Multicloud Object Gateway, you can now create a cache bucket. A cache bucket is a namespace bucket with a hub target and a cache target. For more information, see Caching policy for object buckets.

Red Hat OpenStack Platform technology preview support

OpenShift Container Storage can now be installed and managed using Red Hat OpenStack Platform. For more information see, Deploying and managing OpenShift Container Storage using Red Hat OpenStack Platform guide.

Minimum deployment technology preview support

OpenShift Container Storage can now be deployed with minimum configuration when the standard deployment resource requirement is not met. For more information, see minimum deployment resource requirements in the Planning Guide.

Compact deployment technology preview support

OpenShift Container Storage can now be installed on a three-node OpenShift compact bare metal cluster, where all the workloads run on three strong master nodes. There are no worker or storage nodes.

For information on how to configure OpenShift Container Platform on a compact bare metal cluster, see Configuring a three-node cluster and Delivering a Three-node Architecture for Edge Deployments.

Expand storage capacity using additional device

Administrators can now scale up storage capacity using storage classes other than the one defined during deployment. First define a new storage class based on an existing storage provider, and select that storage class when there is a need to expand the OpenShift Container Storage capacity. See Scaling storage for more information.

CHAPTER 6. DEVELOPER PREVIEWS

This section describes development preview features introduced in Red Hat OpenShift Container Storage 4.7.

Developer preview feature is subject to Developer preview support limitations. Developer preview releases are not intended to be run in production environments. The clusters deployed with the developer preview features are considered to be development clusters and are not supported through the Red Hat Customer Portal case management system. If you need assistance with developer preview features, reach out to the ocs-devpreview@redhat.com mailing list and a member of the Red Hat Development Team will assist you as quickly as possible based on availability and work schedules.

Cloning or restoring a snapshot with the new read only access mode

With the Red Hat OpenShift Container Storage 4.7, you can create a clone or restore a volume snapshot with the readonly (RXO) access mode. For more information, see Creating a clone or restoring a snapshot with the new ROX access mode.

Multi-cluster disaster recovery

Red Hat OpenShift Container Storage provides multi-cluster asynchronous replication of storage volumes across two OpenShift Container Storage clusters serving two Openshift Container Platform clusters. Any stateful application, including its stateless counterparts need some preparation prior to deploying the same on a peer cluster.

Availability of different storage classes based on the media type

Users now have the ability to use mixed media in their clusters to reduce cost while providing the well performed devices to important workloads and slow devices for other workloads.

Flexible devices

Users now have the flexibility to determining which devices they can use. Red Hat supports as a development preview any drive size up to 16TB without any configuration change on bare metal installations.

Support for write-ahead logging PVC for OSDs

OpenShift Container Storage now supports deploying an OSD while separating Bluestore's **rocksdb** database and **rocksdb** write-ahead log onto different devices. OSDs are less performant on HDD due to minimal IOPS when compared to SSDs. This allows the user to increase the performance by using SSDs for the metadata for a given OSD in HDD.

CHAPTER 7. KNOWN ISSUES

This section describes known issues in Red Hat OpenShift Container Storage 4.7.

RGW metrics are no longer available if an active mgr changes in the RHCS cluster

When an active MGR goes down in an external cluster mode, OpenShift Container Platform (OCP) stops collecting any further metrics from the Red Hat Ceph Storage (RHCS) cluster, even when the MGR comes back on. This means RADOS Object Gateway (RGW) metrics are no longer collected once the connection to the present active MGR is lost.

For Red Hat OpenShift Container Storage 4.7, the workaround is as follows:

Once the external RHCS gets back an active MGR, run the python script **ceph-external-cluster-details-exporter.py** once again and collect the JSON output file. At the OCP side, update the external secret named: **rook-ceph-external-cluster-details** with the output of the previously collected JSON file. This triggers a reconciliation and OCP starts picking up the metrics again.

(BZ#1908238)

OSD keys in Vault are not deleted during OpenShift Container Storage cluster uninstallation

Currently, Key Encryption Keys for OSDs are soft-deleted from Vault during Openshift Container Storage cluster deletion when Vault Key/Value (K/V) Secret engine API, version 2 is used for cluster-wide encryption with KMS. This means the key metadata is still visible, and any version of the key can be retrieved.

Workaround: Manually delete the metadata for the key using **vault kv metadata delete** command.

(BZ#1975323)

MDS report oversized cache

Rook has not previously applied **mds_cache_memory_limit** upon upgrades. This means OpenShift Container Storage 4.2 clusters that did not have that option applied were not updated with the correct value, which is typically half the size of the pod's memory limit. Therefore, MDSs in standby-replay may report oversized cache.

(BZ#1944148)

Storage cluster phase is Ready when both flexibleScaling and arbiter are enabled

There are incorrect specifications of the storage cluster CR when arbiter and flexible scaling are enabled. This means the user sees the storage cluster in **READY** state even though there are logs or messages with the error **arbiter and flexibleScaling both can not be enabled**. This does not affect functionality.

(BZ#1946595)

Arbiter nodes can not be labelled with the OpenShift Container Storage node label

Arbiter nodes are considered as valid non-arbiter nodes if they are labelled with the OpenShift Container Storage node label, **cluster.ocs.openshift.io/openshift-storage**. This means the placement for the non-arbiter resources becomes undetermined. To work around this issue, do not label the arbiter nodes with the OpenShift Container Storage node label so that only arbiter resources are placed on the arbiter nodes.

(BZ#1947110)

Issue with noobaa-db-pg-0

noobaa-db-pg-0 pod does not migrate to other nodes when the hosting node goes down. NooBaa will not work when a node is down as migration of **noobaa-db-pg-0** pod is blocked.

(BZ#1783961)

Restore Snapshot/Clone operations with greater size than parent PVC results in endless loop

Ceph CSI does not support restoring a snapshot or creating clones with a size greater than the parent PVC. Therefore, **Restore Snapshot/Clone** operations with a greater size results in an endless loop. To workaround this issue, delete the pending PVC. In order to get a larger PVC, complete one of the following based on the operation you are using:

- If using Snapshots, restore the existing snapshot to create a volume of the same size as the parent PVC, then attach it to a pod and expand the PVC to the required size. For more information, see Volume snapshots.
- If using Clone, clone the parent PVC to create a volume of the same size as the parent PVC, then attach it to a pod and expand the PVC to the required size. For more information, see Volume cloning.

(BZ#1870334)

Ceph status is HEALTH_WARN after disk replacement

After disk replacement, a warning **1 daemons have recently crashed** is seen even if all OSD pods are up and running. This warning causes a change in Ceph's status. The Ceph status should be **HEALTH_OK** instead of **HEALTH_WARN**. To workaround this issue, **rsh** to the **ceph-tools** pod and silence the warning, the Ceph health will then be back to **HEALTH_OK**.

(BZ#1896810)

Device replacement action cannot be performed through the user interface for an encrypted OpenShift Container Storage cluster

On an encrypted OpenShift Container Storage cluster, the discovery result CR discovers the device backed by a Ceph OSD (Object Storage Daemon) differently from the one reported in the Ceph alerts. When clicking the alert, the user is presented with **Disk not found** message. Due to the mismatch, console UI cannot enable the disk replacement option for an OpenShift Container Storage user. To workaround this issue, use the CLI procedure for failed device replacement in the Replacing Devices guide.

(BZ#1906002)

Newly restored PVC can not be mounted

Newly restored PVC can not be mounted, if some of the OCP nodes are running on a Red Hat Enterprise Linux version of less than 8.2 and the snapshot from which it was restored is deleted. To avoid this issue, do not delete the snapshot from which the PVC is restored until the restored PVC is deleted.

(BZ#1956232)

The status of the disk is replacement ready before start replacement is clicked

The user interface can not differentiate between a new disk failure on a different or same node and the

previously failed disk if both the disks have the same name. Due to this same name issue, disk replacement is not allowed as the user interface considers that this newly failed disk is already replaced. To work around this issue, follow the below steps:

1. On OpenShift Container Platform Web Console → click **Administrator**.
2. Click **Home → Search**.
3. In **resources dropdown** → search for **TemplateInstance**.
4. Select **TemplateInstance** and make sure to choose **openshift-storage namespace**.
5. Delete all template instances.

(BZ#1958875)