OpenShift sandboxed containers 1.6

Release notes

Last Updated: 2024-06-26

Legal Notice

Abstract

The release notes 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

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message.

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

You can provide feedback or report an error by creating a Jira issue for the HCIDOCS project, where you can track the progress of your feedback. You must have a Red Hat Jira account and be logged in.

1. Launch the Create Issue form.
2. Complete the **Summary**, **Description**, and **Reporter** fields.
   In the **Description** field, include the documentation URL, chapter or section number, and a detailed description of the issue.
3. Click **Create**.

CHAPTER 1. ABOUT THIS RELEASE

These release notes track the development of OpenShift sandboxed containers 1.6 alongside Red Hat OpenShift Container Platform 4.15.

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

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

CHAPTER 2. NEW FEATURES AND ENHANCEMENTS

This section describes new features and enhancements introduced in OpenShift sandboxed containers 1.6.

2.1. PUBLIC CLOUD

New pod VM image creation flow improves the user experience

In this release, the pod VM image is created after the **kata** runtime is installed. You can view status updates while the image is being created.

Jira:KATA-2781

CHAPTER 3. BUG FIXES

This section describes bugs fixed in OpenShift sandboxed containers 1.6.

3.1. SANDBOXED CONTAINERS

Pod with `io.katacontainers.config.hypervisor.virtio_fs_extra_args` annotation does not start

Previously, **virtiofsd** did not accept the **--thread-pool-size=16** option. This issue has been fixed in **virtiofsd-1.5.0-1.el9_2.1**, which is available in OpenShift Container Platform 4.13.24 and 4.14.4.

Jira:KATA-2146

3.2. PERFORMANCE AND SCALING

RHEL 9 compute nodes cause severe database workload performance degradation

Severe performance degradations were observed in database workloads running on Red Hat Enterprise Linux (RHEL) 9 compute nodes. This issue has been fixed in OpenShift Container Platform 4.13, 4.14, and 4.15.

Jira:KATA-2247

Excessive metric reporting causes Prometheus pods to fail

Previously, the **kata_shim_netdev** metric reported an excessively large volume of metrics, which caused Prometheus pods to fail with **out of memory** errors. In the current release, the issue has been fixed.

Jira:KATA-2639

`controller-manager` pod fails with `out of memory` errors

Previously, when the OpenShift sandboxed containers Operator was deployed on a single-node, bare-metal cluster running OpenShift Container Platform 4.14.12, the **controller-manager** pod failed with **out of memory** errors. In the current release, the issue has been fixed by increasing the pod's resources.

Jira:KATA-2790

CHAPTER 4. KNOWN ISSUES

This section describes known issues in OpenShift sandboxed containers 1.6.

4.1. SECURITY

Sandboxed containers do not support SELinux multi-category security labels

When you set SELinux Multi-Category Security (MCS) labels in the security context of a container, the pod does not start. The following error is displayed in the pod log:

```
Error: CreateContainer failed: EACCES: Permission denied: unknown
```

The runtime does not have access to the security context of the containers when the sandboxed container is created. This means that **virtiofsd** does not run with the appropriate SELinux label and cannot access host files for the container. As a result, you cannot rely on MCS labels to isolate files in the sandboxed container on a per-container basis. This means that all containers can access all files within the sandboxed container. Currently, there is no workaround for this issue.

Jira:KATA-1875

4.2. PERFORMANCE AND SCALING

Increasing container CPU resource limits fails if CPUs are offline

Using container CPU resource limits to increase the number of available CPUs for a pod fails if the requested CPUs are offline. If the functionality is available, you can diagnose CPU resource issues by running the **oc rsh <pod>** command to access a pod and then running the **lscpu** command:

```
$ lscpu
```

Example output:

```
CPU(s):                  16
On-line CPU(s) list:     0-12,14,15
Off-line CPU(s) list:    13
```

The list of offline CPUs is unpredictable and can change from run to run.

Workaround: Use a pod annotation to request additional CPUs, as in the following example:

```
metadata:
  annotations:
    io.katacontainers.config.hypervisor.default_vcpus: "16"
```

Jira:KATA-1376

Increasing the sizeLimit does not expand an ephemeral volume

You cannot use the **sizeLimit** parameter in the pod specification to expand ephemeral volumes because the volume size default is 50% of the memory assigned to the sandboxed container.

Workaround: Change the size by remounting the volume. For example, if the memory assigned to the sandboxed container is 6 GB and the ephemeral volume is mounted at /**var**/**lib**/**containers**, you can increase the size of this volume beyond the 3 GB default by running the following command:

```
$ mount -o remount,size=4G /var/lib/containers
```

Jira:KATA-2579

Peer pod fails when its resource request annotations do not match system resources

The values of the **io.katacontainers.config.hypervisor.default_vcpus** and **io.katacontainers.config.hypervisor.default_memory** annotations follow the semantics for QEMU, which has the following limitations for peer pods:

- If you set **io.katacontainers.config.hypervisor.default_memory** to less than **256**, the following error is displayed:

  ```
  Failed to create pod sandbox: rpc error: code = Unknown desc = CreateContainer failed:
  Memory specified in annotation io.katacontainers.config.hypervisor.default_memory is less
  than minimum required 256, please specify a larger value: unknown
  ```

- If you set **io.katacontainers.config.hypervisor.default_memory** to **256** and **io.katacontainers.config.hypervisor.default_vcpus** to **1**, the smallest instance type or instance size is launched from the list.

- If you set **io.katacontainers.config.hypervisor.default_vcpus** to **0**, all annotations are ignored and the default instance is launched.

Workaround: Set **io.katacontainers.config.hypervisor.machine_type** to the default AWS instance type or Azure instance size specified in the config map to enable flexible pod VM sizes.

Jira:KATA-2575, Jira:KATA-2577, Jira:KATA-2578

CHAPTER 5. ASYNCHRONOUS ERRATA UPDATES

Security, bug fix, and enhancement updates for OpenShift sandboxed containers are released as asynchronous errata through the Red Hat Network.

Red Hat OpenShift Container Platform 4.15 errata are available on the Red Hat Customer Portal .

See the OpenShift Container Platform Life Cycle for details about asynchronous errata.

You can enable errata email notifications in your Red Hat Subscription Management settings. You must have a Red Hat Customer Portal account with systems registered and OpenShift Container Platform entitlements.

This section will continue to be updated over time to provide notes on enhancements and bug fixes for future asynchronous errata releases of OpenShift sandboxed containers.

5.1. RHBA-2024:3964 - OPENSHIFT SANDBOXED CONTAINERS 1.6.0 IMAGE RELEASE, BUG FIX, AND ENHANCEMENT ADVISORY

Issued: 2024-06-18

OpenShift sandboxed containers release 1.6.0 is now available. This advisory contains an update for OpenShift sandboxed containers with enhancements and bug fixes.

The list of bug fixes included in the update is documented in the RHBA-2024:3964 advisory.

APPENDIX A. LIST OF TICKETS BY COMPONENT

Bugzilla and JIRA tickets are listed in this document for reference. The links lead to the release notes in this document that describe the tickets.

Component	Tickets
Performance / Scaling	Jira:KATA-1376, Jira:KATA-2579, Jira:KATA-2575, Jira:KATA-2247, Jira:KATA-2639, Jira:KATA-2790
Public cloud	Jira:KATA-2781
Sandboxed containers	Jira:KATA-2146
Security	Jira:KATA-1875