OpenShift sandboxed containers 1.7

Release notes

Last Updated: 2024-09-22

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

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 1.7 alongside Red Hat OpenShift Container Platform 4.16.

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 1.7.

2.1. PUBLIC CLOUD

AWS and Azure cloud provider credentials are retrieved automatically

The Operator uses the cloud provider credentials of the OpenShift cluster by default, unless the user explicitly sets the AWS or Azure cloud provider credentials.

Jira:KATA-2216

CHAPTER 3. BUG FIXES

This section describes bugs fixed in OpenShift sandboxed containers 1.7.

3.1. PERFORMANCE AND SCALING

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-2578, Jira:KATA-2577

CHAPTER 4. KNOWN ISSUES

This section describes known issues in OpenShift sandboxed containers 1.7.

4.1. SANDBOXED CONTAINERS

OpenShift sandboxed containers 1.7.0 does not work with OpenShift Container Platform 4.14 and older versions

You must upgrade to OpenShift Container Platform 4.15 or later before installing or upgrading the OpenShift sandboxed containers Operator. For more information, see OpenShift sandboxed containers operator 1.7 is not available and Upgrade to OSC 1.7.0 put running Peer Pods into ContainerCreating status in the KnowledgeBase.

Jira:KATA-3193, Jira:KATA-3155

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

CHAPTER 5. TECHNOLOGY PREVIEWS

This section provides a list of all Technology Previews available in OpenShift sandboxed containers 1.7.

See Technology Preview Features Support Scope for more information.

Confidential Containers on Microsoft Azure Cloud Computing Services, IBM Z, and IBM LinuxONE

Confidential Containers provides enhanced security for cloud-native applications, allowing them to run in secure and isolated environments known as Trusted Execution Environments (TEEs), which protect the containers and their data even when in use.

Note the following limitations:

- No encryption and integrity protection of the confidential virtual machine (CVM) root filesystem (rootfs): The CVM executes inside the TEE and runs the container workload. Lack of encryption and integrity protection of the rootfs could allow a malicious admin to exfiltrate sensitive data written to the rootfs or to tamper with the rootfs data. Integrity protection and encryption for the rootfs is currently work in progress. You must ensure that all your application writes are in memory.

- No encrypted container image support: Only signed container image support is currently available. Encrypted container image support is work in progress.

- Communication between the Kata shim and the agent components inside the CVM is subject to tampering: The agent components inside the CVM are responsible for executing Kubernetes API commands from the Kata shim running on the OpenShift worker node. We use an agent policy in the CVM that turns off Kubernetes exec and log APIs for the containers to avoid exfiltration of sensitive data via the Kubernetes API. However, this is incomplete; further work is ongoing to harden the communication channel between the shim and the agent components. The agent policy can be overridden at runtime by using pod annotations. Currently, runtime policy annotations in the pod are not verified by the attestation process.

- No native support for encrypted pod-to-pod communication: Pod-to-pod communication is unencrypted. You must use TLS at the application level for all pod-to-pod communication.

- Image double-pull on the worker node and inside the CVM: The container image is downloaded and executed in the CVM that executes inside the TEE. However, currently the image is also downloaded on the worker node.

- Building the CVM image for Confidential Containers requires the OpenShift sandboxed containers Operator to be available in the cluster.

Jira:KATA-2416

Peer pod support for IBM Z and IBM LinuxONE

You can deploy OpenShift sandboxed containers workloads, without nested virtualization, by using peer pods on IBM Z® and IBM® LinuxONE (s390x architecture).

Jira:KATA-2030

CHAPTER 6. 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 4.16 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.

6.1. RHBA-2024:6709 - OPENSHIFT SANDBOXED CONTAINERS 1.7.0 IMAGE RELEASE, BUG FIX, AND ENHANCEMENT ADVISORY

Issued: 2024-09-18

OpenShift sandboxed containers release 1.7.0 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-2024:6709 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
Public cloud	Jira:KATA-2216
Sandboxed containers	Jira:KATA-3193
kata-containers	Jira:KATA-3193