OpenShift sandboxed containers 1.6

发行注记

Last Updated: 2024-06-29

法律通告

摘要

本发行注记总结了所有新功能、功能增强、重要的技术变化、以及对以前版本中的错误作出的主要修正。另外，还包括在此版本正式发行(GA)时存在的已知问题的信息。

目录

使开源包含更多

红帽致力于替换我们的代码、文档和 Web 属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。详情请查看 CTO Chris Wright 的信息。

对红帽文档提供反馈

您可以通过为 HCIDOCS 项目创建 Jira 问题来提供反馈或报告错误，您可以在其中跟踪您的反馈的过程。您必须有一个 Red Hat Jira 帐户并登录。

1. 启动 **Create Issue** 表单。
2. 完成 **Summary**、**Description** 和 **Reporter** 字段。
   在 **Description** 字段中，包含文档 URL、章节号以及问题的详细描述。
3. 点 **Create**。

第 1 章 关于此版本

本发行注记介绍了 OpenShift 沙盒容器 1.6 和 Red Hat OpenShift Container Platform 4.15 的开发。

OpenShift Container Platform 专为 FIPS 设计。当以 FIPS 模式运行 Red Hat Enterprise Linux (RHEL) 或 Red Hat Enterprise Linux CoreOS (RHCOS)时，OpenShift Container Platform 核心组件使用 RHEL 加密库，在 **x86_64**、**ppc64le**、**s390x** 架构上提交给 NIST 的 FIPS 140-2/140-3 Validation。

有关 NIST 验证程序的更多信息，请参阅加密模块验证程序。有关为验证提交的 RHEL 加密库的单独版本的最新 NIST 状态，请参阅 Compliance Activities 和 Government Standards。

第 2 章 新功能及功能增强

本节介绍 OpenShift 沙盒容器 1.6 中引入的新功能和增强。

2.1. 公有云

新的 pod VM 镜像创建流改进了用户体验

在本发行版本中，在安装 **kata** 运行时后创建 pod 虚拟机镜像。您可以在创建镜像时查看状态更新。

Jira:KATA-2781

第 3 章 程序错误修复

本节介绍 OpenShift 沙盒容器 1.6 中修复的错误。

3.1. 沙盒容器

带有 io.katacontainers.config.hypervisor.virtio_fs_extra_args 注解的 Pod 不会启动

在以前的版本中，**virtiofsd** 不接受 **-thread-pool-size=16** 选项。这个问题已在 **virtiofsd-1.5.0-1.el9_2.1** 中解决，它在 OpenShift Container Platform 4.13.24 和 4.14.4 中提供。

Jira:KATA-2146

3.2. 性能和扩展

RHEL 9 计算节点会导致严重数据库工作负载性能下降

在 Red Hat Enterprise Linux (RHEL) 9 计算节点上运行的数据库工作负载中观察到严重的性能下降。这个问题已在 OpenShift Container Platform 4.13、4.14 和 4.15 中解决。

Jira:KATA-2247

过度指标报告会导致 Prometheus pod 失败

在以前的版本中，**kata_shim_netdev** 指标报告大量指标，这会导致 Prometheus pod 失败并显示 **内存不足** 错误。在当前发行版本中，这个问题已被解决。

Jira:KATA-2639

controller-manager pod 失败并显示 内存不足 错误

在以前的版本中，当 OpenShift 沙盒容器 Operator 部署到单节点中时，运行 OpenShift Container Platform 4.14.12 的裸机集群时，**controller-manager** pod 会失败，并显示 **内存不足** 错误。在当前发行版本中，这个问题已通过增加 pod 资源来解决。

Jira:KATA-2790

第 4 章 已知问题

本节介绍 OpenShift 沙盒容器 1.6 中已知的问题。

4.1. 安全性

沙盒容器不支持 SELinux 多类别安全标签

当您在容器安全上下文中设置 SELinux Multi-Category Security (MCS)标签时，pod 不会启动。pod 日志中显示以下错误：

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

在创建沙盒容器时，运行时无法访问容器的安全上下文。这意味着 **virtiofsd** 没有使用适当的 SELinux 标签运行，且无法访问容器的主机文件。因此，您无法依赖 MCS 标签来基于每个容器隔离沙盒容器中的文件。这意味着所有容器都可以访问沙盒容器中的所有文件。目前，这个问题还没有临时解决方案。

Jira:KATA-1875

4.2. 性能和扩展

如果 CPU 离线，增加容器 CPU 资源限值会失败

如果请求的 CPU 离线，使用容器 CPU 资源限制来增加 pod 的可用 CPU 数量会失败。如果功能可用，您可以通过运行 **oc rsh <pod> 命令来访问 pod**，然后运行 **lscpu** 命令诊断 CPU 资源问题：

```
$ lscpu
```

输出示例：

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

离线 CPU 列表是无法预计的，可以从 run 改为 run。

临时解决方案：使用 pod 注解来请求额外的 CPU，如下例所示：

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

Jira:KATA-1376

增加 sizeLimit 不会扩展临时卷

您不能使用 pod 规格中的 **sizeLimit** 参数来扩展临时卷，因为卷大小默认为分配给沙盒容器的 50%。

临时解决方案：通过重新挂载卷来更改大小。例如，如果分配给沙盒容器的内存为 6 GB，并且临时卷挂载到 **/var/lib/containers**，您可以通过运行以下命令来将此卷的大小增加到 3 GB：

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

Jira:KATA-2579

当资源请求注解与系统资源不匹配时，对等 pod 会失败

io.katacontainers.config.hypervisor.default_vcpus 和 **io.katacontainers.config.hypervisor.default_memory** 注解的值遵循 QEMU 的语义，它有以下对对等 pod 的限制：

- 如果将 **io.katacontainers.config.hypervisor.default_memory** 设置为 **256**，则会显示以下错误：

  > 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

- 如果将 **io.katacontainers.config.hypervisor.default_memory** 设置为 **256**，将 **io.katacontainers.config.hypervisor.default_vcpus** 设置为 **1**，则会从列表中启动最小的实例类型或实例类型。

- 如果将 **io.katacontainers.config.hypervisor.default_vcpus** 设置为 **0**， 则所有注解都会被忽略，并启动默认实例。

临时解决方案：将 **io.katacontainers.config.hypervisor.machine_type** 设置为配置映射中指定的默认 AWS 实例类型或 Azure 实例大小，以启用灵活的 pod 虚拟机大小。

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

第 5 章 异步勘误更新

OpenShift 沙盒容器的安全更新、程序错误修正、功能增强更新将会通过红帽网络以异步勘误的形式发布。

Red Hat OpenShift Container Platform 4.15 勘误可以通过 红帽客户门户网站 获得。

如需了解有关异步勘误的详细信息，请参阅 OpenShift Container Platform 生命周期。

您可以在 Red Hat Subscription Management 设置中启用勘误电子邮件通知。您必须有一个有注册的系统和 OpenShift Container Platform 权利的红帽客户门户网站帐户。

本节的内容将会持续更新，以提供以后发行的与 OpenShift 沙盒容器相关的异步勘误信息。

5.1. RHBA-2024:3964 - OPENSHIFT 沙盒容器 1.6.0 镜像发行版本、程序错误修正和功能增强公告

发布日期：24 年 6 月 18 日

OpenShift 沙盒容器发行版本 1.6.0 现已正式发布。此公告包含带有改进和程序错误修复的 OpenShift 沙盒容器的更新。

其程序错误修正列表包括在 RHBA-2024:3964 公告中。

附录 A. 按组件划分的问题单列表

在本文档中列出了 Bugzilla 和 JIRA 问题单以供参考。这些链接会指向本文档中描述问题单的发行注记。

组件	票证
性能/扩展	Jira:KATA-1376,JIRA:KATA-2579,JIRA:KATA-2575,JIRA:KATA-2247,JIRA:KATA-2639,JIRA:KATA-2790
公有云	Jira:KATA-2781
沙盒容器	Jira:KATA-2146
安全性	Jira:KATA-1875