OpenShift Sandboxed Containers 1.5

OpenShift 沙盒容器发行注记

对于 OpenShift Container Platform

Last Updated: 2024-06-26

OpenShift Sandboxed Containers 1.5 OpenShift 沙盒容器发行注记

对于 OpenShift Container Platform

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

前言

使开源包含更多

红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。因此，这些更改会逐渐更新，尽可能地更新。详情请查看 CTO Chris Wright 的信息。

第 1 章 简介

第 2 章 OPENSHIFT 沙盒容器 1.5 发行注记

2.1. 关于此版本

本发行注记介绍了 OpenShift 沙盒容器 1.5 和 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。

2.2. 新功能及功能增强

2.2.1. AWS 和 Azure 的灵活的 pod VM 实例大小

在 OpenShift 沙盒容器 1.5 中，您可以指定 pod 虚拟机的实例大小。您可以使用 AWS 的 **PODVM_INSTANCE_TYPES** 字段，或在 **peer-pods-cm ConfigMap** CR 中使用 Azure 的 **AZURE_INSTANCE_SIZES**。如需更多信息，请参阅使用 Web 控制台为 AWS 创建 peer-pod ConfigMap，以及使用 Web 控制台为 Azure 创建 peer-pod ConfigMap。

2.2.2. 在 AWS 和 Azure 上创建 pod 虚拟机镜像

在 OpenShift 沙盒容器 1.5 中，如果 **peer-pods-secret** 和 **peer-pods-cm** 对象存在，则 pod 虚拟机镜像会被自动创建，并且 **peer-pods-cm** 不包含 **AZURE_IMAGE_ID** 或 **PODVM_AMI_ID** 变量。如需有关流程的更多信息，请参阅在 web 控制台中创建 KataConfig 自定义资源

2.2.3. 使管理员能够深入了解 kata 节点安装、卸载和更新操作

引进了一个名为 **kataNodes** 的新字段，显示用户对节点进入 **kata** 操作的状态进行更详细的视图。现有 **Is In Progress** 布尔值状态字段已被一个更说明的 **InProgress** 条件替代。

如需更多信息，请参阅 安装和卸载转换。

2.2.4. 对等 pod 支持 IBM Z 和 IBM (R) LinuxONE 上的 OpenShift 沙盒容器（技术预览）

用户现在可以使用 IBM Z 和 IBM® LinuxONE (390x 架构)上的对等 pod 部署 OpenShift 沙盒容器工作负载。这可让用户绕过嵌套虚拟化的需求。这个功能只是一个技术预览，且不被支持。如需更多信息，请参阅使用对等 pod 部署 OpenShift 沙盒容器工作负载。

2.3. 程序错误修复

- 在 OpenShift 沙盒容器 1.5.0 到 1.5.2 中，当用户创建对等 pod 时，pod 会一直处于 **ContainerCreating** 状态，并显示 "failed to identify the host primary interface" 错误，因为 Go 1.21.1 中的网络功能行为发生了变化。这个问题已在 OpenShift 沙盒容器 1.5.3 中解决。(KATA-2847)

- 在以前的版本中，在安装过程中启动 **KataConfig** CR 删除会导致 OpenShift 沙盒容器 Operator 尝试同时删除并重新创建，而无需完成任何过程。在这个版本中，Operator 会序列化删除，以便在安装完成后发生。(KATA-1851)

- 在以前的版本中，用户无法更新使用特别标记的节点部署的 kata-enabled 集群。对节点标签的更改不会触发部署更改。用户必须删除现有 **kataConfig** CR，并使用更新的标签创建新的 **kataConfig** CR。从上一版本（版本 1.4）开始，更新节点标签会自动触发部署更改。(KATA-1928)

- 在以前的版本中，当 QEMU 没有检测到 **virtiofsd** 时，QEMU 每次删除 **kata** 工作负载时，QEMU 会在系统日志中记录错误。在这个版本中，**kata** 运行时会在停止 **virtiofsd** 前停止 QEMU。在这个版本中，仅适用于 OpenShift Container Platform 4.13 和 4.14。(KATA-2133)

- 在以前的版本中，当您在 **KataConfig** CR 中启用对等 pod，然后在安装后检查 CR 时，**kata-remote** 运行时类不会在 **status.runtimeClass** 字段中显示。这个问题已在 OpenShift 沙盒容器 1.5.0 中解决。(KATA-2164)

- 在以前的版本中，当 peer-pod 虚拟机运行时重启 **peerpodconfig-ctrl-caa-daemon** pod 可能会导致创建多个代表同一对等 pod 的虚拟机。只要原始对等 pod 仍在运行，则冗余实例就会存在，除非您从云供应商控制台或 CLI 中手动删除实例。在这个版本中，在重启 **peerpodconfig-ctrl-caa-daemon** pod 后，会创建一个新的 peer-pod 虚拟机，并立即删除旧实例。(KATA-2519)

- 在以前的版本中，当用户请求在 AWS 或 Azure 上运行的对等 pod 虚拟机的实例元数据时，AWS 或 Azure 实例元数据服务会返回 worker 节点的元数据，而不是 pod。随着版本 1.5.1 的更新，AWS 或 Azure 实例元数据服务会如预期返回 pod 的元数据。(KATA-2583)

2.4. 已知问题

- 在访问 OpenShift Container Platform 集群中从 **hostPath** 卷挂载的文件或目录时，您可能会收到 SELinux 拒绝。即使运行特权沙盒容器，这些拒绝也会发生，因为特权沙盒容器不会禁用 SELinux 检查。
  在主机中遵循 SELinux 策略可保证主机文件系统默认与沙盒工作负载完全隔离。这还对 **virtiofsd** 守护进程或 QEMU 中潜在的安全漏洞提供更强的保护。

  如果挂载的文件或目录在主机上没有特定的 SELinux 要求，您可以使用本地持久性卷作为替代方案。文件会自动重新标记为 **container_file_t**，遵循 SELinux 容器运行时。请参阅使用本地卷的持久性存储

  挂载文件或目录时，自动重新标记不是选项，则主机上应该具有特定的 SELinux 标签。相反，您可以在主机上设置自定义 SELinux 规则，以允许 **virtiofsd** 守护进程访问这些特定标签。(KATA-469)

- 一些 OpenShift 沙盒容器 Operator pod 使用容器 CPU 资源限制来增加 pod 的可用 CPU 数量。这些 pod 可能会收到比请求的 CPU 少。如果功能在容器内可用，您可以使用 **oc rsh <pod>** 访问 pod 并运行 **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 列表可能会不可预测地从 run 改为 run。

  作为临时解决方案，您可以使用 pod 注解来请求额外 CPU 而不是设置 CPU 限值。使用 pod 注解的 CPU 请求不受此问题的影响，因为处理器分配方法不同。以下注解必须添加到 pod 的元数据中，而不是设置 CPU 限制：

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

(KATA-1376)

- 当您在容器的安全上下文中设置 SELinux Multi-Category Security (MCS)标签时，pod 不会启动，并在 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。

(KATA-1875)

- OpenShift 沙盒容器的 FIPS 合规性只适用于 **kata** 运行时类。新的对等 pod 运行时类 **kata-remote** 尚未被完全支持，且尚未测试用于 FIPS 合规性。(KATA-2166)

- 具有 **io.katacontainers.config.hypervisor.virtio_fs_extra_args** 注解的 pod，其中包含 **--announce-submounts** 或 **--thread-pool-size** 不会启动。这是 OpenShift Container Platform 4.13 和 4.14 上的 OpenShift 沙盒容器 Operator 使用的 **virtiofsd** 组件回归。OpenShift Container Platform 4.12 和 4.11 不受影响。(KATA-2146)

- 临时内存卷的 **sizeLimit** 选项不适用于 OpenShift 沙盒容器。临时卷大小默认为分配给沙盒容器的内存的 50%。可以通过重新挂载卷来手动更改此卷的大小。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**，您可以使用以下命令将这个卷的大小增加到默认 50%：

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

(KATA-2579)

- **io.katacontainers.config.hypervisor.default_vcpus** 和 **io.katacontainers.config.hypervisor.default_memory** 注解遵循 QEMU 的语义，对对等 pod 有以下限制：

  - 如果将 **io.katacontainers.config.hypervisor.default_memory** 注解的值设置为小于 **256**，则会出现以下错误：

    ```
    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
    ```

  - 如果您使用 **io.katacontainers.config.hypervisor.default_memory: 256** 和 **io.katacontainers.config.hypervisor.default_vcpus: 1** 注解，则从列表中启动最小实例。

  - 如果您使用 **io.katacontainers.config.hypervisor.default_vcpus: 0** 注解，则所有注解都会被忽略，并且默认实例已启动。

相反，建议您将 **io.katacontainers.config.hypervisor.machine_type: <instance type/instance size>** 注解用于灵活的 pod 虚拟机大小。(KATA-2575, KATA-2577, KATA-2578)

- 在从 OpenShift 沙盒容器 Operator 1.4.1 自动升级到 1.5 的过程中，升级会 处于待处理状态。如果您的订阅被设置为自动更新，则安装 OpenShift 沙盒容器的升级。但是，如果安装了 **KataConfig** CR （自定义资源），则 CSV 会处于 **pending** 状态。

  您可以运行以下命令来检查 **Subscription** 对象的状态：

  ```
  $ oc get sub osc-operator -n openshift-osc-operator -o yaml
  ```

  以下错误会出现在 **Subscription** 对象的 **status** 部分，以及 upgrade **InstallPlan** 对象的 **status** 部分：

  ```
  message: 'error validating existing CRs against new CRD"s schema for
  "kataconfigs.kataconfiguration.openshift.io":
      error validating custom resource against new schema for KataConfig /example-
  kataconfig:
      [].status.runtimeClass: Invalid value: "string": status.runtimeClass in body
      must be of type array: "string"'
  ```

  如果收到这个错误，则必须卸载，然后重新安装 OpenShift 沙盒容器 Operator：

  1. 删除在 **kata** 或 **kata-remote** 运行时中运行的任何工作负载(pod、部署、daemonset)。重新安装后需要重新创建这些工作负载。有关删除工作负载的更多信息，请参阅使用 CLI 删除 OpenShift 沙盒容器 pod。
  2. 删除 **KataConfig** CR。请参阅 使用 CLI 删除 KataConfig 自定义资源。

     重要

     如果工作负载正在运行，请不要删除 **KataConfig** CR。

     您可以使用以下命令检查 **KataConfig** CR 的删除状态：

     ```
     $ oc get kataconfig -n openshift-osc-operator
     ```

  3. 卸载 Operator。请参阅使用 CLI 删除 OpenShift 沙盒容器 Operator
  4. 重新安装 OpenShift 沙盒容器 Operator。请参阅使用 CLI 安装 OpenShift 沙盒容器 Operator。
     重新安装 OpenShift 沙盒容器 Operator 会安装版本 1.5.0。
  5. 创建 **KataConfig** CR。请参阅使用 CLI 创建 KataConfig 自定义资源。
  6. 重新创建工作负载。请参阅使用 CLI 在沙盒容器中部署工作负载。

  注意

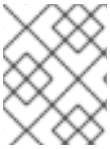
  如果将订阅设置为手动更新，请不要批准升级，直到 OpenShift 沙盒容器 Operator 1.5.1 可用为止。

  (KATA-2593)

2.5. 异步勘误更新

OpenShift 沙盒容器 4.15 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。所有的 OpenShift Container Platform 4.15 勘误都可以通过红帽客户门户网站获得。OpenShift Container Platform 生命周期包括了详细的与异步勘误相关的内容。

红帽客户门户网站的用户可以在红帽订阅管理（RHSM）帐户设置中启用勘误通知功能。当勘误通知被启用后，用户会在有与其注册的系统相关的勘误发行时接收到电子邮件通知。



注意

用户的红帽客户门户网站账户需要有注册的系统，以及使用 OpenShift Container Platform 的权限才可以接收到 OpenShift Container Platform 的勘误通知。

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 1.5 相关的异步勘误信息。

2.5.1. RHEA-2023:7493 - OpenShift 沙盒容器 1.5.0 镜像发行版本、程序错误修正和功能增强公告

发布日期：2023 年 11 月 27 日

OpenShift 沙盒容器发行版本 1.5.0 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 RHEA-2023:7493 公告中。

2.5.2. RHBA-2024:0147 - OpenShift 沙盒容器 1.5.1 镜像发行和程序错误公告

发布日期： 2024 年 1 月 11 日

OpenShift 沙盒容器版本 1.5.1 现已正式发布。此公告包含 OpenShift 沙盒容器的更新，并包括了相关的程序漏洞修复。

其程序错误修正列表包括在 RHBA-2024:0147 公告中。

2.5.3. RHBA-2024:0815 - OpenShift 沙盒容器 1.5.2 镜像发行版本和程序错误公告

发布日期： 2024 年 2 月 15 日

OpenShift 沙盒容器版本 1.5.2 现已正式发布。此公告包含 OpenShift 沙盒容器的更新，并包括了相关的程序漏洞修复。

其程序错误修正列表包括在 RHBA-2024:0815 公告中。

2.5.4. RHBA-2024:2035 - OpenShift 沙盒容器 1.5.3 镜像发行和程序错误公告

发布日期：2024 年 4 月 24 日

OpenShift 沙盒容器版本 1.5.3 现已正式发布。此公告包含 OpenShift 沙盒容器的更新，并包括了相关的程序漏洞修复。

其程序错误修正列表包括在 RHBA-2024:2035 公告中。