Kata Containers源码分析

> 基于安全容器stable-2.5分支

源码结构

src/runtime：容器管理器运行的主要组件，提供containerd shimv2 runtime的实现。

src/agent：启动容器环境的虚拟机或Pod中运行的管理进程。

src/libs：kata container多个组件共享的库文件。

tests：不包括与主代码一起存在的单元测试。

tools/packaging：用于生成打包二进制文件的脚本和元数据。

tools/packaging/kernel：guest kernel的patch。

tools/osbuilder：用于为虚拟机管理程序创建“迷你操作系统”rootfs 和 initrd 映像以及内核的工具。

src/tools/agent-ctl：提供用于测试agent的低级访问的工具。

src/tools/trace-forwarder：agent追踪助手。

src/tools/runk：基于agent的标准OCI容器运行时。

ci：CI配置文件和脚本。

ecr_deploy（自研）：kata containers部署工具。

snap：构建kata containers快照镜像的资源。

utils：kata-manager安装工具。

docs：kata containers文档资料。

创建容器源码过程

> 容器类型：
>
> - PodContainer：需要关联到已经存在的pod的容器
> - PodSandbox：用于创建pod的基础容器。
> - SingleContainer：无pod运行容器。

PodSandbox或SingleContainer容器

runtime/pkg/containerd-shim-v2/service.go func Create

runtime/pkg/containerd-shim-v2/create.go func create

1、runtime/pkg/katautils/create.go func CreateSandbox

runtime/virtcontainers/implementation.go func CreateSandbox

runtime/virtcontainers/api.go func CreateSandbox

runtime/virtcontainers/sandbox.go func createSandbox

（1）runtime/virtcontainers/qemu.go func CreateVM

（2）runtime/virtcontainers/kata_agent.go　func createSandbox

2、runtime/pkg/containerd-shim-v2/container.go　func newContainer

PodContainer容器

runtime/pkg/containerd-shim-v2/service.go　func Create

runtime/pkg/containerd-shim-v2/create.go　func create

1、runtime/pkg/katautils/create.go　func CreateContainer

runtime/virtcontainers/sandbox.go　func CreateContainer

runtime/virtcontainers/container.go　func newContainer

2、runtime/pkg/containerd-shim-v2/container.go　func newContainer

启动容器源码过程

PodSandbox或SingleContainer容器

runtime/pkg/containerd-shim-v2/service.go　func Start

runtime/pkg/containerd-shim-v2/start.go　func startContainer

runtime/virtcontainers/sandbox.go　func Start

runtime/virtcontainers/container.go　func start

runtime/virtcontainers/kata_agent.go　func startContainer

PodContainer容器

runtime/pkg/containerd-shim-v2/service.go　func Start

runtime/pkg/containerd-shim-v2/start.go　func startContainer

runtime/virtcontainers/sandbox.go　func StartContainer

runtime/virtcontainers/container.go　func start

runtime/virtcontainers/kata_agent.go　func startContainer

停止容器源码过程

> 停止容器包括如下几种方式：
>
> - agent监听工作负载退出，告知运行时，运行时关闭容器。
> - 容器管理器强制删除容器。

工作负载退出关闭容器

PodSandbox或SingleContainer容器

runtime/pkg/containerd-shim-v2/wait.go　func wait

1、runtime/virtcontainers/sandbox.go　func Stop

（1）runtime/virtcontainers/container.go　func stop

runtime/virtcontainers/kata_agent.go func stopContainer

（2）runtime/virtcontainers/sandbox.go func stopVM

（2.1）runtime/virtcontainers/kata_agent.go func stopSandbox

（2.2）runtime/virtcontainers/qemu.go func StopVM

（3）runtime/virtcontainers/kata_agent.go func disconnect

2、runtime/virtcontainers/sandbox.go func Delete

（1）runtime/virtcontainers/container.go func delete

runtime/virtcontainers/sandbox.go func removeContainer

（2）runtime/virtcontainers/qemu.go func Cleanup

PodContainer容器

runtime/pkg/containerd-shim-v2/wait.go func wait

runtime/virtcontainers/sandbox.go func StopContainer

runtime/virtcontainers/container.go func stop

runtime/virtcontainers/kata_agent.go func stopContainer

强制删除容器

PodSandbox或SingleContainer容器

runtime/pkg/containerd-shim-v2/service.go func Delete

runtime/pkg/containerd-shim-v2/delete.go func deleteContainer

runtime/pkg/katautils/hook.go func PostStopHooks

PodContainer容器

runtime/pkg/containerd-shim-v2/service.go func Delete

runtime/pkg/containerd-shim-v2/delete.go func deleteContainer

1、runtime/virtcontainers/sandbox.go func StopContainer

runtime/virtcontainers/container.go func stop

runtime/virtcontainers/kata_agent.go func stopContainer

2、 runtime/virtcontainers/sandbox.go func DeleteContainer

runtime/virtcontainers/container.go func delete

runtime/virtcontainers/sandbox.go func removeContainer

3、runtime/pkg/katautils/hook.go func PostStopHooks