An Introduction and Overview

Graham Whaley
Senior Software Engineer, Intel OTC
graham.whaley@intel.com
Contents

What is Kata?
Architecture and Integrations
Roadmap
Getting started and Contributing
What is Kata Containers?
Speed vs Security

Virtual Machines

Isolation

Speed
Integrations
A little history

Open source project hosted by the OpenStack Foundation

Merger of two established projects which both started in 2015

- Hyper.SH runV and Intel® Clear Containers

V1.0 released May 22nd 2018
V1.3.1 released October 22nd 2018
Traditional Containers

- **Process A**
  - Filter: seccomp
  - MAC
  - CAPS

- **Process B**
  - Filter: seccomp
  - MAC
  - CAPS

- **Process C**
  - Filter: seccomp
  - MAC
  - CAPS

**Namespaces**

**Linux Kernel**

**Resources**
- CPU
- MEMORY
- NETWORK
- STORAGE
Traditional Containers in a VM
Kata Containers

Diagram showing virtual machines and processes with namespaces and hardware virtualization.
Architecture and Integrations
The components

- QEMU package
- Runtime
- Kernel
- Rootfs image
- Agent
- Shim
- Proxy
Kata basic architecture

I/O

OCI cmd/spec

Shim

Runtime

gRPC

gRPC

Virtual Machine

Container Command

Container Exec

Container namespaces

Agent

Kernel

Hypervisor

Hypervisor VSOCK socket

*Other names and brands may be claimed as the property of others.
CRI-O and Kata

Kubelet

Container Runtime Interface (CRI)

CRI-O or containerd

runc

kata-runtime

Pod

VM

redis redis

redis redis
Networking and Storage
Basic Kata Networking
Kata vhost user networking

DPDK, VPP, OPENvSwitch → VHOST USER SOCKET

VIRTUAL MACHINE

POD
Kata Physical Networking
Kata Storage

- Overlay
- Device mapper
- Image file
- Ceph, gluster etc.

Virtual Machine

- 9pfs
- Block device
- nvdimm
- DAX
- Network

*Other names and brands may be claimed as the property of others.
Roadmap
Security and isolation

- In Container
  - Seccomp
- On Host
  - Cgroup isolation
  - More namespace isolation
  - Root-less QEMU
  - SELinux policy
Networking

TC Mirroring
Optimising default path
Docker swarm DNS
enlightened CNI plugins
Filesystems (volumes)

Virtio-FS (vsock/FUSE)
NFS-vsock
cache enablements
Other features

Live Upgrades
More device mappings
More hypervisors
non-Linux workloads
Always size and speed
It is Open Source!

Getting, Using, Contributing
Links

● **Source code:**
  ○ Kata Containers: [https://github.com/kata-containers/](https://github.com/kata-containers/)
  ○ Apache 2 license
  ○ Packages and instructions: [https://github.com/kata-containers/documentation/](https://github.com/kata-containers/documentation/)
    ○ RPM, DEB, apk, snap, Clear Linux

● **Community**
  ● Slack: katacontainers.slack.com
  ● IRC: #kata-dev@freenode
  ● Mailing-list: kata-dev@lists.katacontainers.io
Questions?
Comments?
Experiences?