What’s new with Kata?
Agenda

- *Refresher* — What is Kata Containers
- What’s new
- What’s next
What is Kata?
Kata Containers
Open Source, Open Design, Open Development, Open Community
Kata Containers
Open Source, Open Design, Open Development, Open Community

- Open Governance project with Architecture Committee:
  - Archana Shinde, Intel
  - Eric Ernst, Apple
  - Fabiano Fidencio, RedHat
  - Peng Tao, Ant Financial
  - Samuel Ortiz, Apple
Kata Containers
Open Source, Open Design, Open Development, Open Community

• Open Governance project with Architecture Committee:
  • Archana Shinde, Intel
  • Eric Ernst, Apple
  • Fabiano Fidencio, RedHat
  • Peng Tao, Ant Financial
  • Samuel Ortiz, Apple

Source: https://katacontainers.biterg.io/
Kata Containers is a secure container runtime that provides stronger workload isolation using hardware virtualization technology as a second layer of defense.
Primary threat model
Protect host infrastructure, including other workloads

Assume each workload is untrusted
Host Linux Kernel

- Workload A
- Workload B

CPU
MEM
Network
Storage

Virtual Machine

- Workload A
- Linux Kernel

Hardware Virtualisation

Virtual Machine

- Workload B
- Linux Kernel

Hardware Virtualisation

Host Linux Kernel

Capabilities
- SELinux
- SELinux
How to wrap a pod in a VM
Supported VMMs:
- Cloud Hypervisor
- Firecracker
- QEMU
What’s new?
Kata 2.x improvements, updates

- Agent reimplemented in rust, asynchronous support added
- Default shared filesystem now virtio-fs
- virtio-fs limitation for inotify
  - Implement workaround in Kata to present watchable mount
- Open-telemetry support
- QEMU: Default machine type now Q35
What’s next?
Performance Improvements
Performance Improvements

Networking

Provide a VM native interface when feasible

Storage

Directly consume block device at virtual machine layer

CPU performance Isolation

Better cpuset support: use cpuset in guest as well as host

Isolating user vCPU from VMM/IO threads
Confidential Computing
Existing threat model

- Don’t trust the workload.
- Prevent workload $\leftarrow$ workload attacks
- Prevent workload $\rightarrow$ host attacks
- Workload is forced to trust host / provider
Extended threat model

- Workload does not trust the cloud service provider
- Host is outside the trust boundary
- Prevent host $\rightarrow$ workload attacks
Kata, Confidential Computing

**Protect** data while it is being used/processed

- Memory and CPU state encryption and integrity checking

**Attest** the tenant software and hardware stack

- Hardware based quoting
- Software stack measurement
Hardware implementations, support

AMD SEV, IBM PEF and secure execution, Intel TDX

Hypervisor Dependencies

Intel TDX KVM upstreaming WIP

Hypervisor Dependencies
Get involved!

- github.com/kata-containers
- Apache 2.0 license
- katacontainers.io
- Slack: #kata-dev on bit.ly/kataslack