

Implement Secure Containers using Kata Container and gVisor in Kubernetes

Atwatan Malik Mahardi
Cloud Engineer at PT. Boer Technology

Bogor, August 21, 2021

Platinum sponsor :



Gold sponsor :



Silver sponsor :

Custom sponsor :






About Me



Atwatan Malik Mahardi

Cloud Engineer at PT. Boer Technology



-  @atwatanmalikm
-  Atwatan Malik Mahardi
-  atwatanmalikm@gmail.com

Foundation sponsor:



Hosted by:

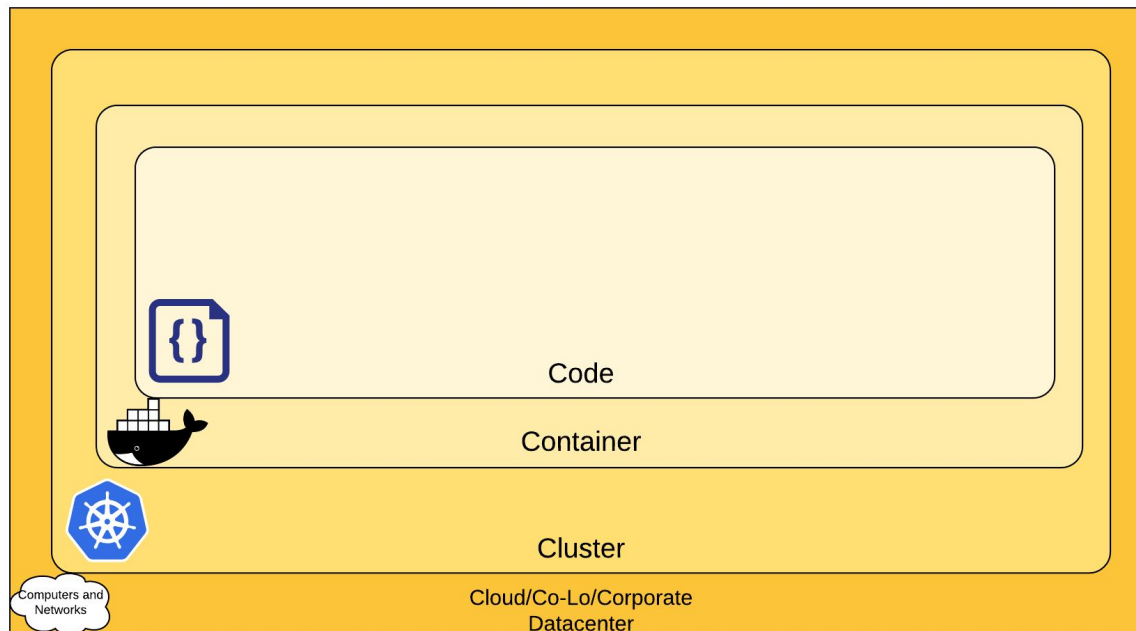


OpenStack Indonesia
Indonesia OpenStack Foundation Community
www.openstack.id

Agenda

- Container Runtime
- Kata Container
- gVisor
- Demo
- Q&A

The 4C's of Cloud Native Security





INDONESIA
OpenInfra Days

Container Runtime #1



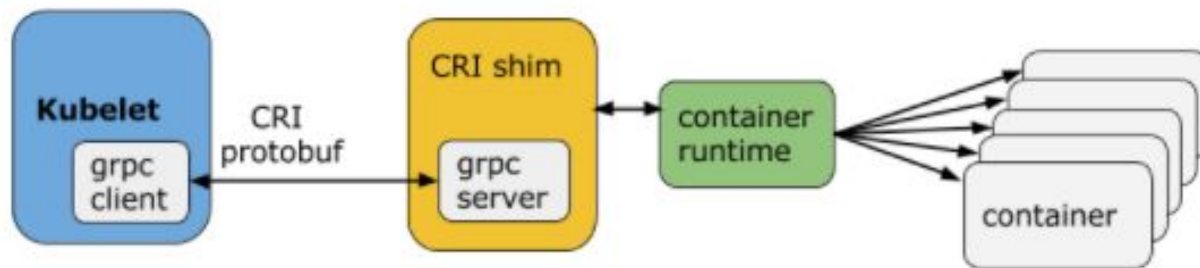
Container Runtime

At the lowest layers of a Kubernetes node is the software that, among other things, starts and stops containers. We call this the “**Container Runtime**”. The most widely known container runtime is Docker, but it is not alone in this space.

Container Runtime Interface (CRI)

A plugin interface which enables kubelet to use a wide variety of container runtimes, without the need to recompile.

Kubelet communicates with the container runtime (or a CRI shim for the runtime) over Unix sockets using the gRPC framework, where kubelet acts as a client and the CRI shim as the server.

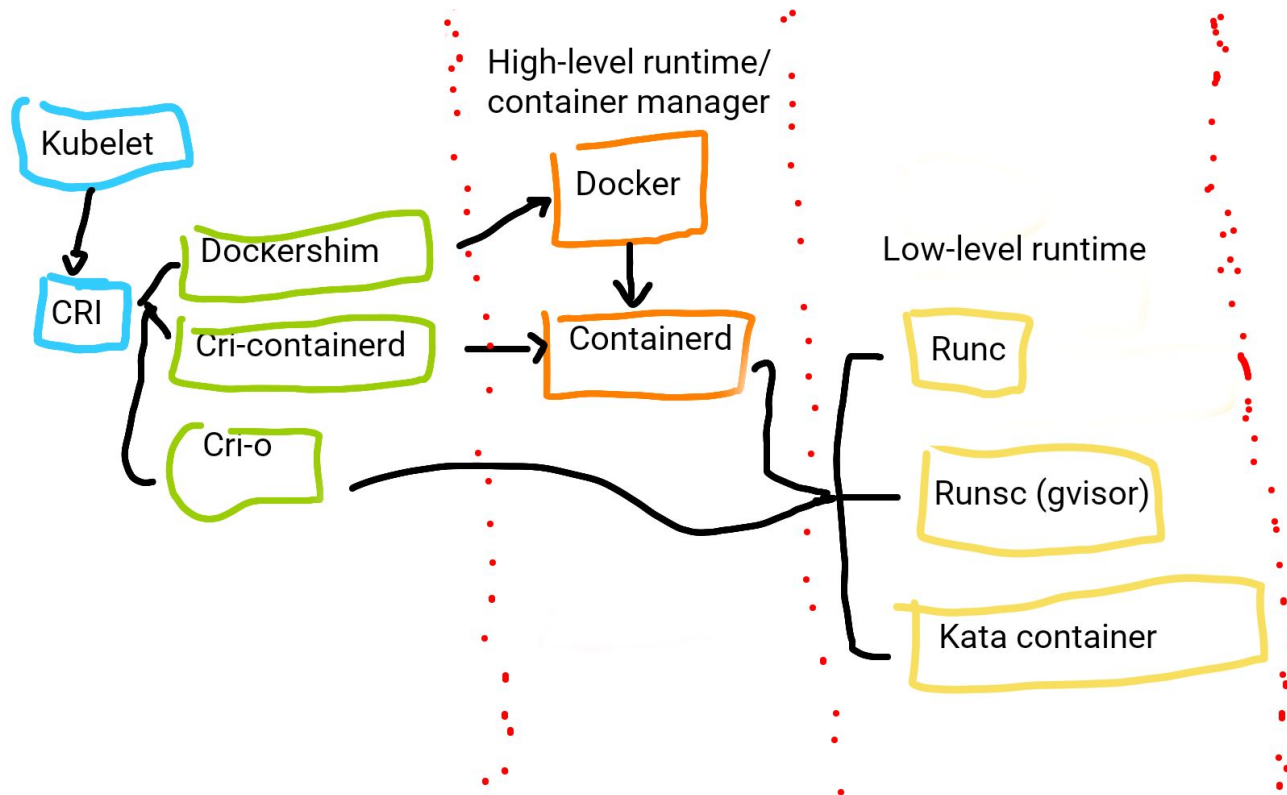




Container Runtime Interface (CRI)

- Containerd
- CRI-O
- Docker

Container Runtime Interface (CRI)







Kata Container #2



About Kata Containers

Kata Containers is an open source community working to build a secure container runtime with lightweight virtual machines that feel and perform like containers, but provide stronger workload isolation using hardware virtualization technology as a second layer of defense.

Features

	Security	Runs in a dedicated kernel, providing isolation of network, I/O and memory and can utilize hardware-enforced isolation with virtualization VT extensions.
	Compatibility	Supports industry standards including OCI container format, Kubernetes CRI interface, as well as legacy virtualization technologies.
	Performance	Delivers consistent performance as standard Linux containers; increased isolation without the performance tax of standard virtual machines.
	Simplicity	Eliminates the requirement for nesting containers inside full blown virtual machines; standard interfaces make it easy to plug in and get started.



INDONESIA
OpenInfra Days

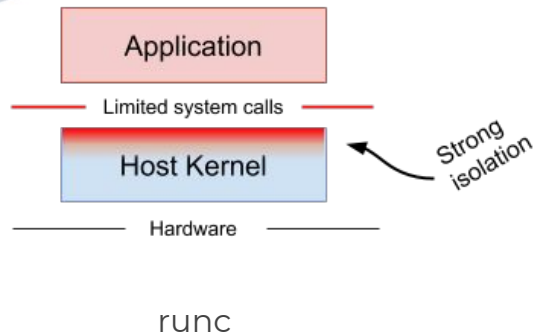
gVisor #3

About gVisor

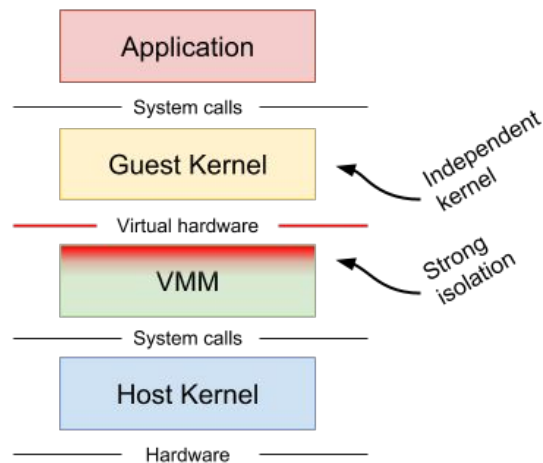
gVisor is an application kernel, written in **Go**, that implements a substantial portion of the Linux system call interface. It provides an additional layer of isolation between running applications and the host operating system.

gVisor includes an Open Container Initiative (OCI) runtime called **runsc** that makes it easy to work with existing container tooling. The runsc runtime integrates with Docker and Kubernetes, making it simple to run sandboxed containers.

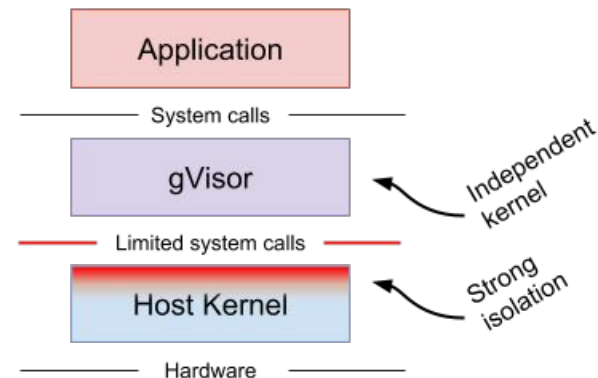
Difference



runc



Kata Container



gVisor



INDONESIA
OpenInfra Days

Demo #4



References

<https://kubernetes.io/docs/>

<https://katacontainers.io/docs/>

<https://gvisor.dev/docs/>

Sponsored by:



Open Infrastructure
FOUNDATION



nVIDIA®



intek

INDOCENTER

Hosted by:



OpenStack Indonesia

Indonesia OpenStack Foundation Community
www.openstack.id

Community Partners:



Thanks!

Do you have any questions?

-  @atwatanmalikm
-  Atwatan Malik Mahardi
-  atwatanmalikm@gmail.com

Platinum sponsor :



Gold sponsor :



Silver sponsor :

Custom sponsor :

