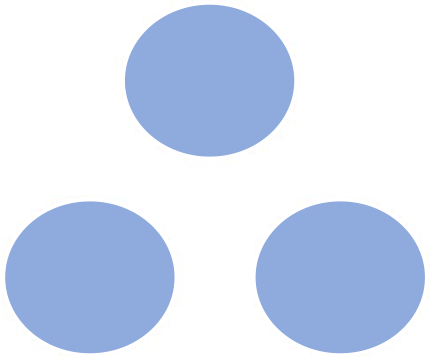
KubeCon | CloudNativeCon

China 2018

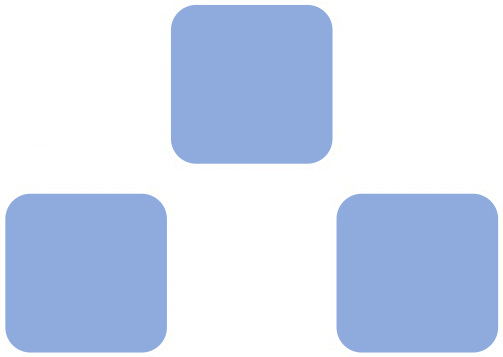
Kubernetes VM Solutions for Multi-Tenant Applications

Guangxu Li, Senior Software Engineer, ZTE
li.guangxu@zte.com.cn

Container and VM Ecosystem



Container



VM

- Kubernetes
- Docker Swarm
- Marathon
- Nomad

- OpenStack
- Others

Why We Run VM on Kubernetes?

- *Traditional Applications*
- *No linux based Applications*
- *Functions provided by host kernel are not satisfied*
- *OpenStack is too complex*
- *Unified infrastructure*
- *Better isolation*

VM related Projects

Virtlet

KubeVirt

RancherVM

Focus : deploy REAL vm (traditional vm app)

Kata Container

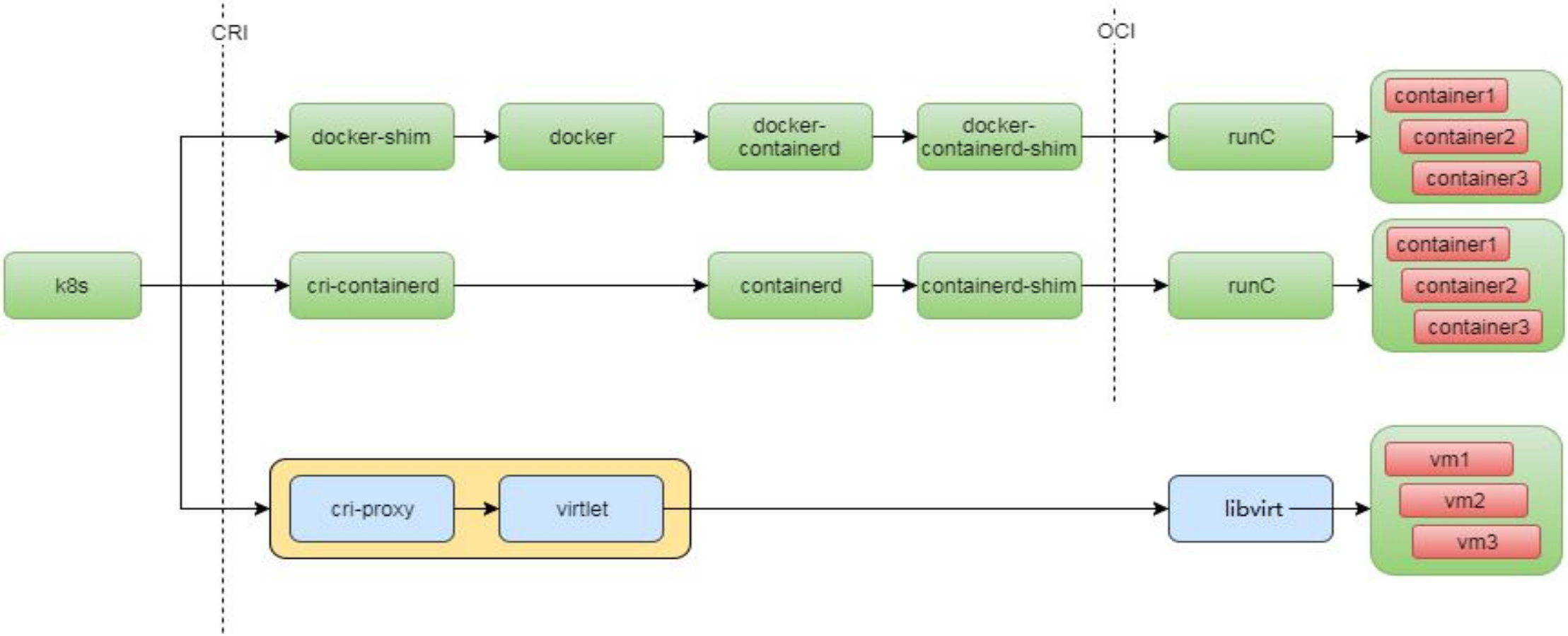
Focus : container security

Virtlet

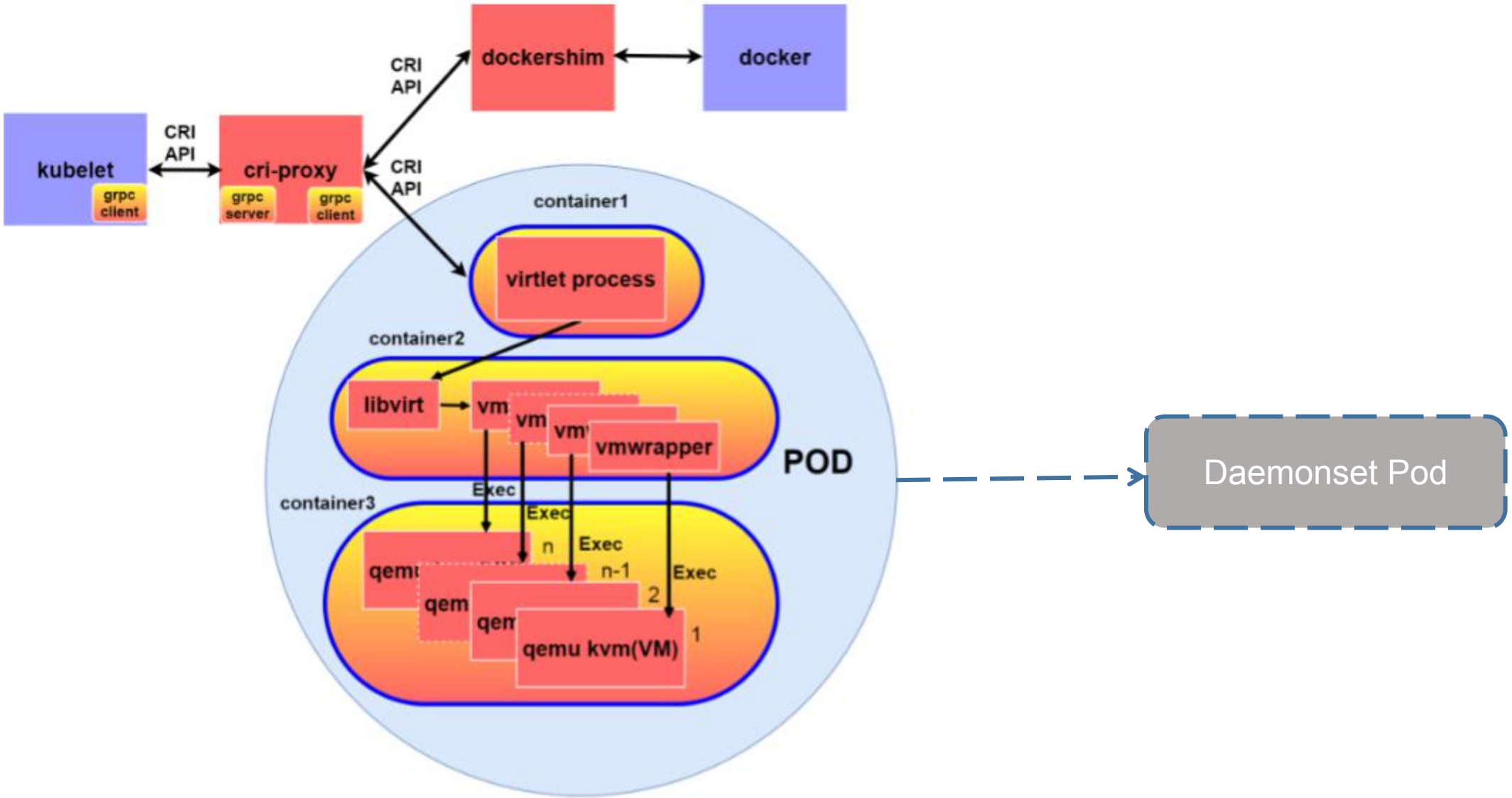
Virtlet *is a Kubernetes runtime server which allows you to run VM workloads, based on QCOW2 images.*

https://github.com/Mirantis/virtlet

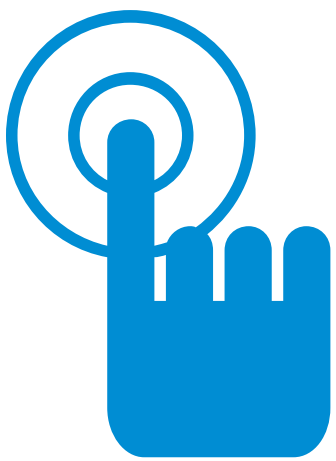
Virtlet compares with other CRI

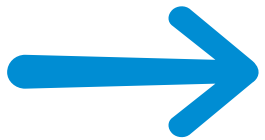


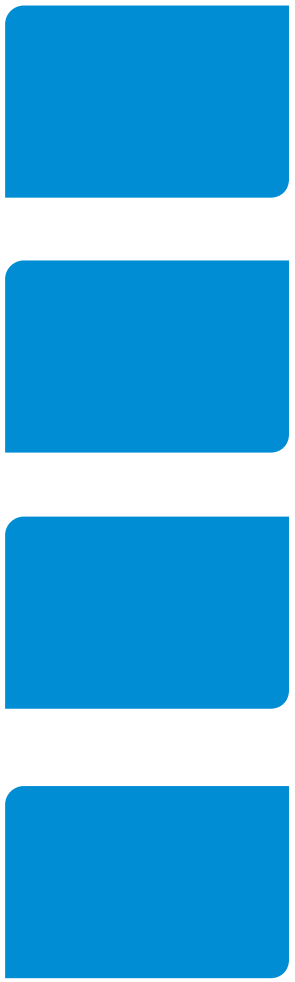
Virtlet Architecture



Virtlet Deploying Objects





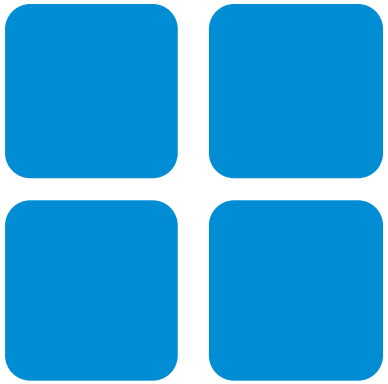


DaemonSet

ConfigMap

ClusterRole/Role

Service Account



virtlet solution

Virtlet Pros

define VM as Pod

supports using multiple interfaces

SR-IOV

NFV Environments

Virtlet Cons

limited storage options

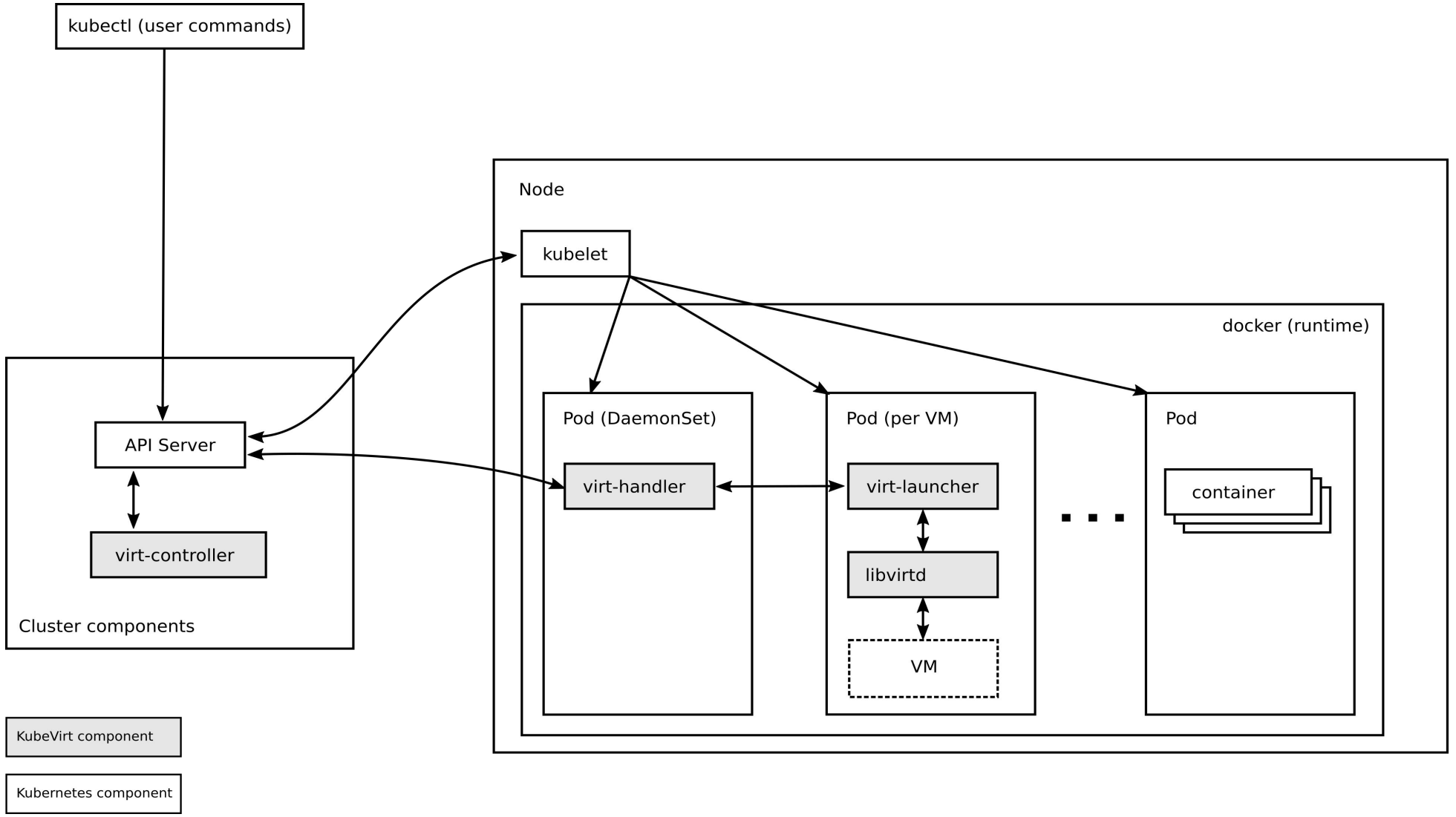
more configurations

VM actions limited by Pod

Building a virtualization API for Kubernetes

https://github.com/kubevirt

KubeVirt Architecture



KubeVirt Application Layout

KubeVirt Components

- virt-controller
- virt-handler
- libvirtd

KubeVirt Managed Pods

- VMI Foo
- VMI Bar

KubeVirt Pros & Cons

Pros

- Kubernetes cluster addon
- freedom - not limited by Pod definition

Cons

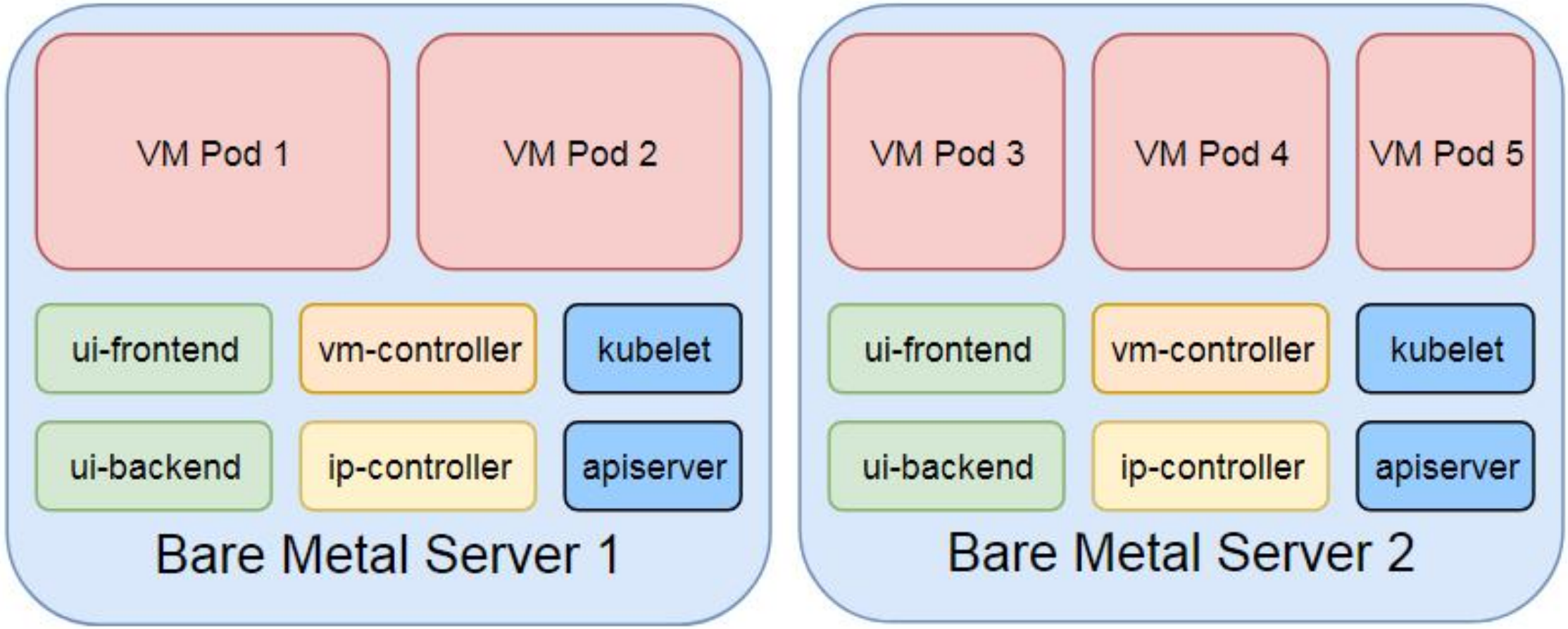
- VMs need to be managed separately from kubelet
- a new controller
- much bigger codebase

RancherVM

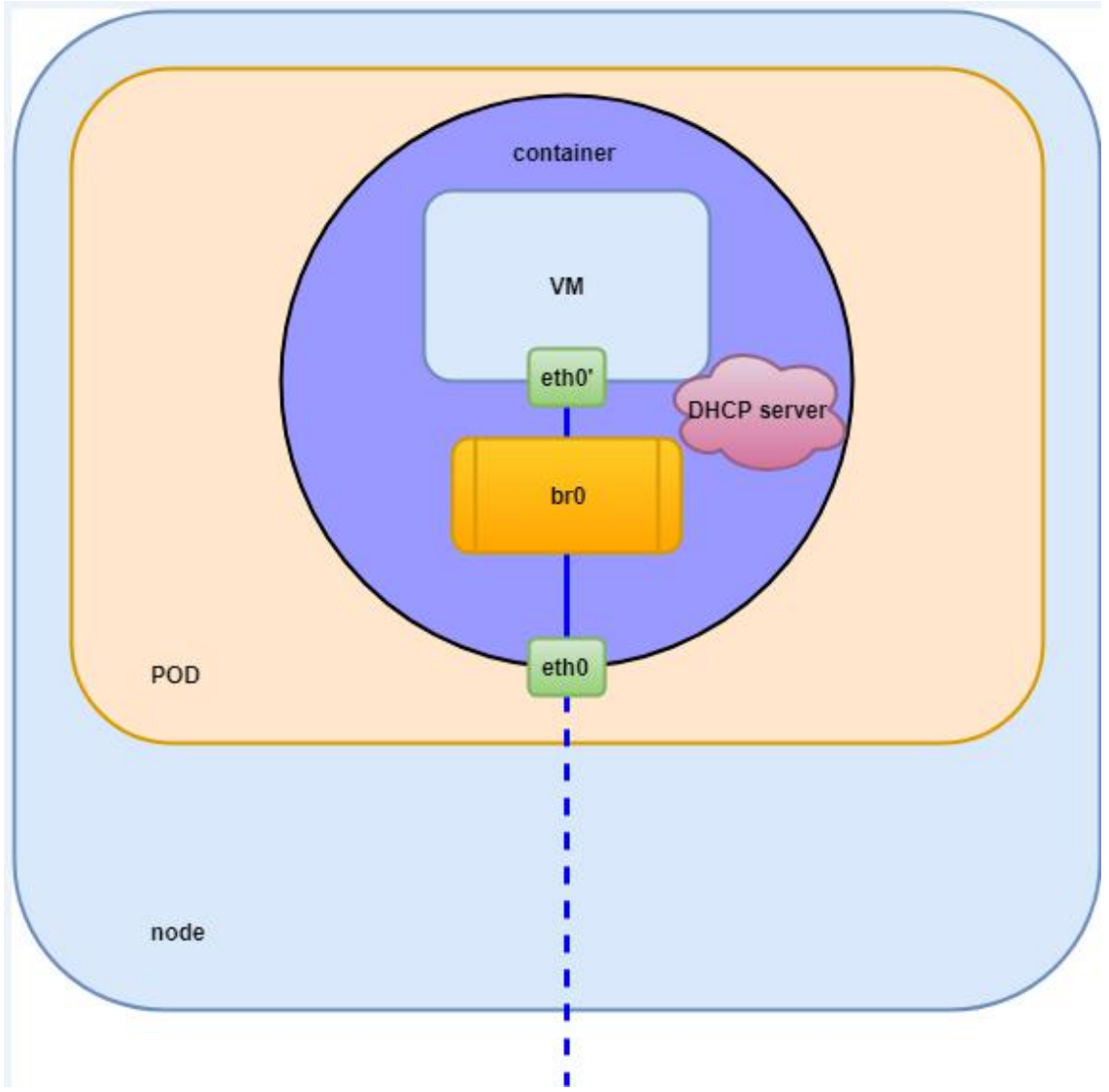
Package and run KVM images as Kubernetes pods, run at scale.

https://github.com/rancher/vm

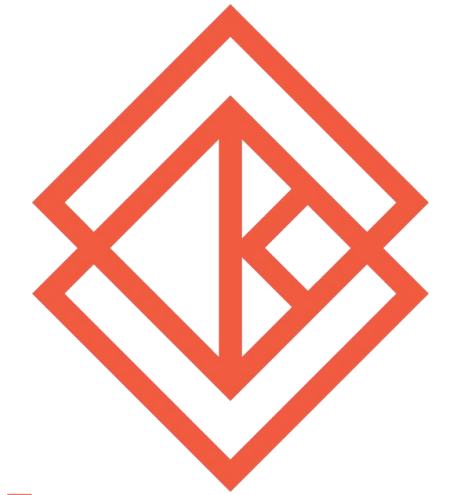
RancherVM Architecture

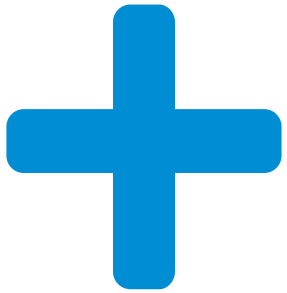


RancherVM Networking



Container Security





gVisor

NFV?

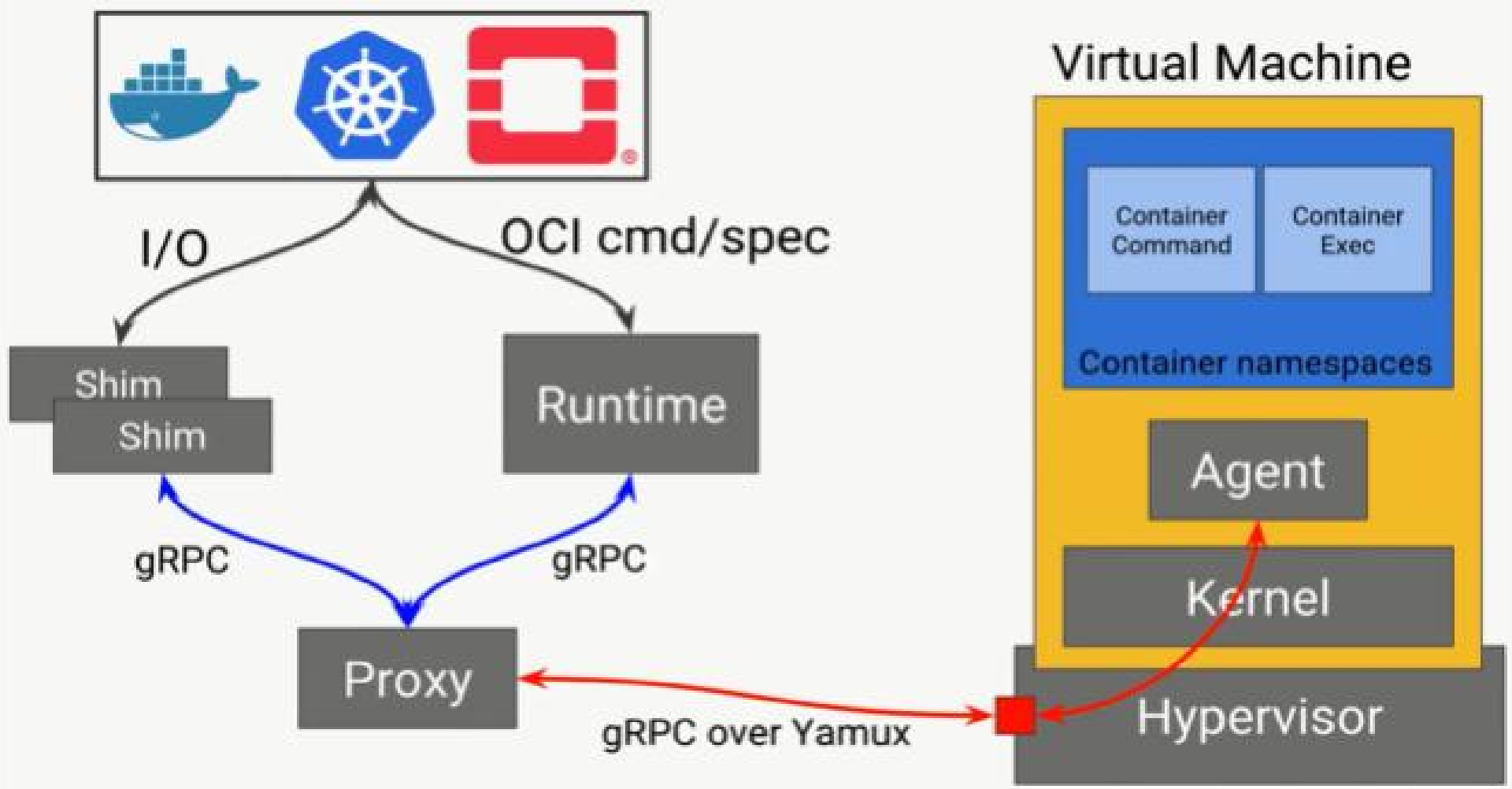
Kata Container

The speed of containers, the security of VMs

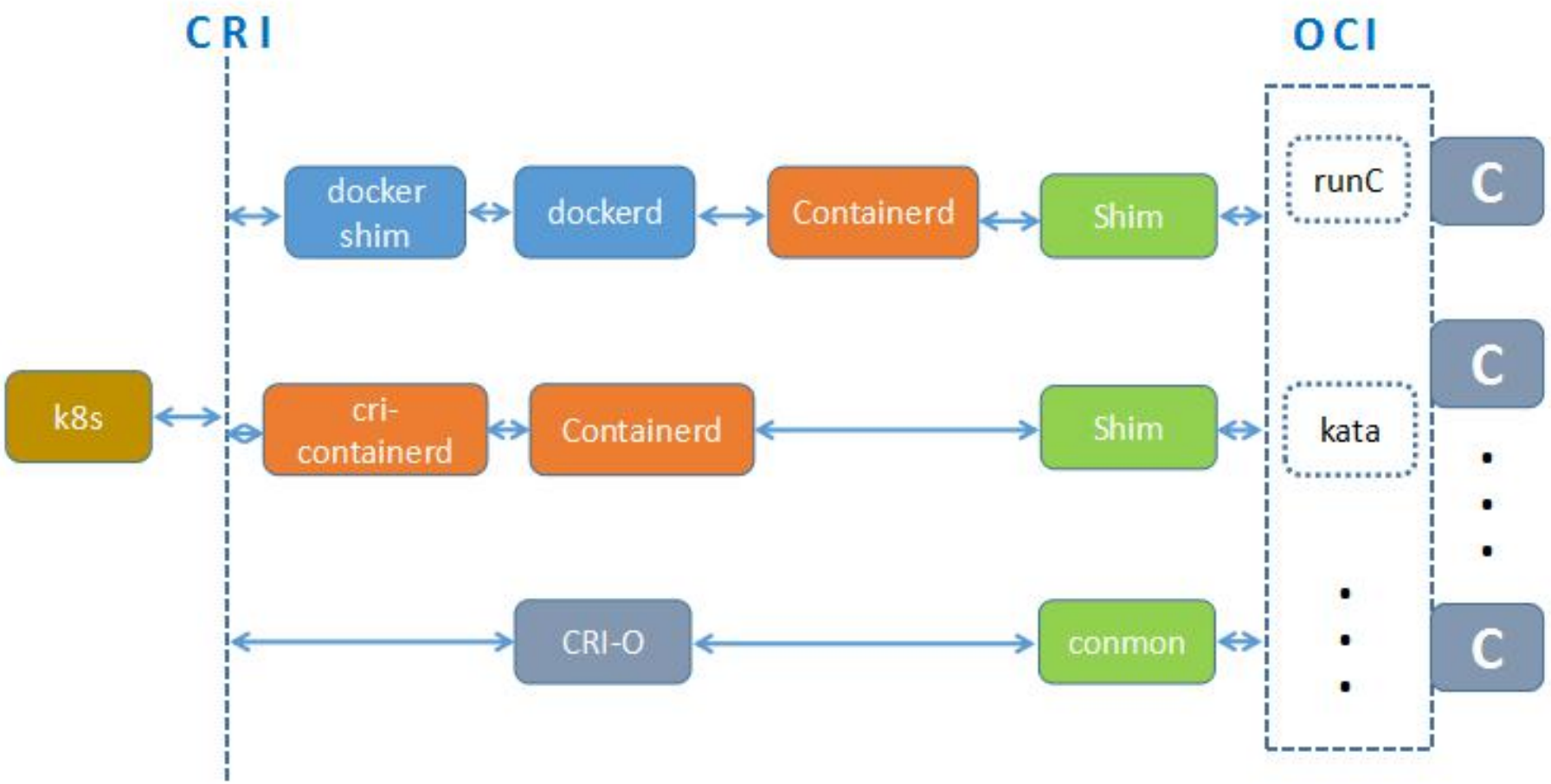
kata containers

https://github.com/kata-containers

Kata Container Architecture

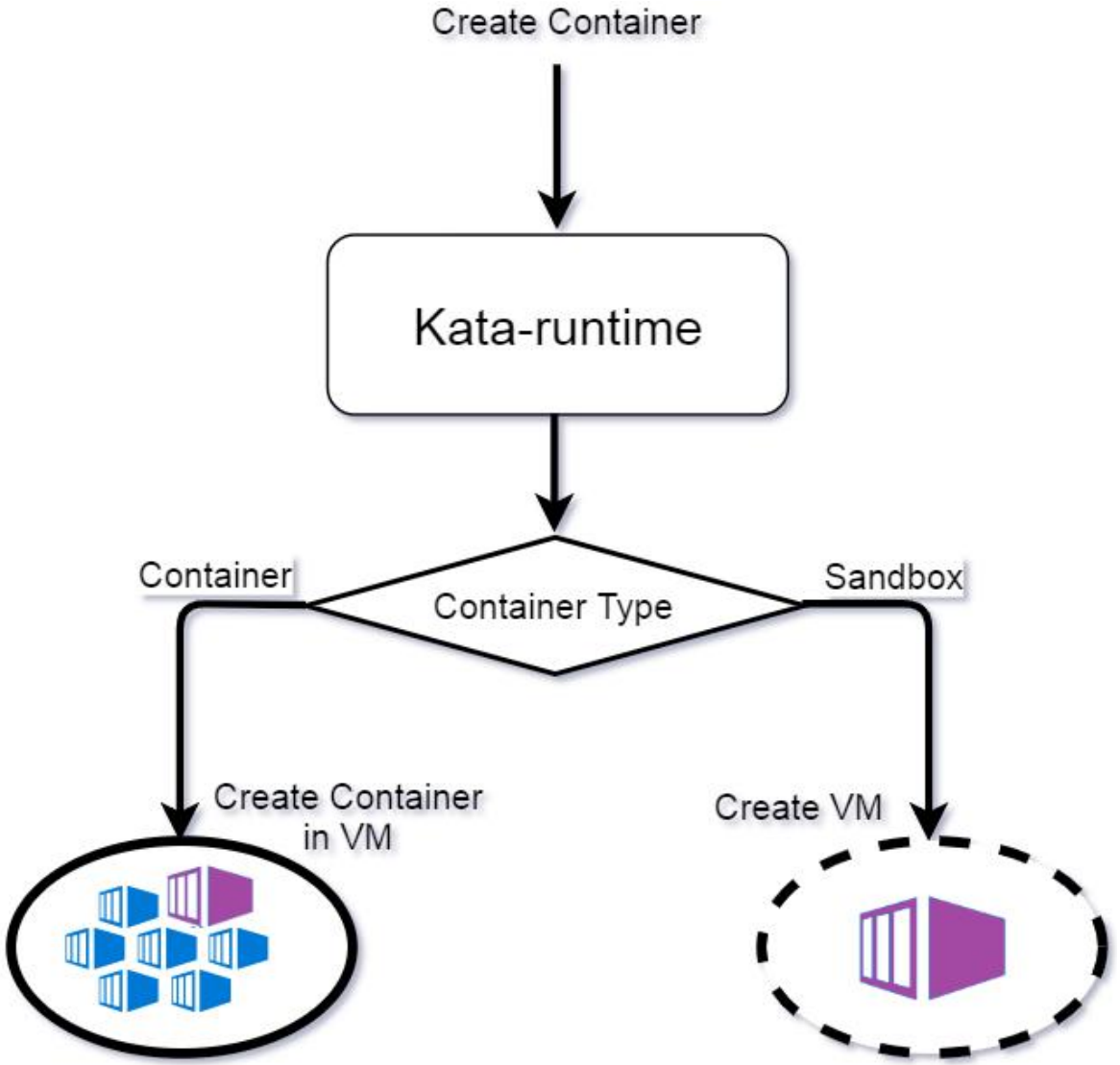


How to use kata container?

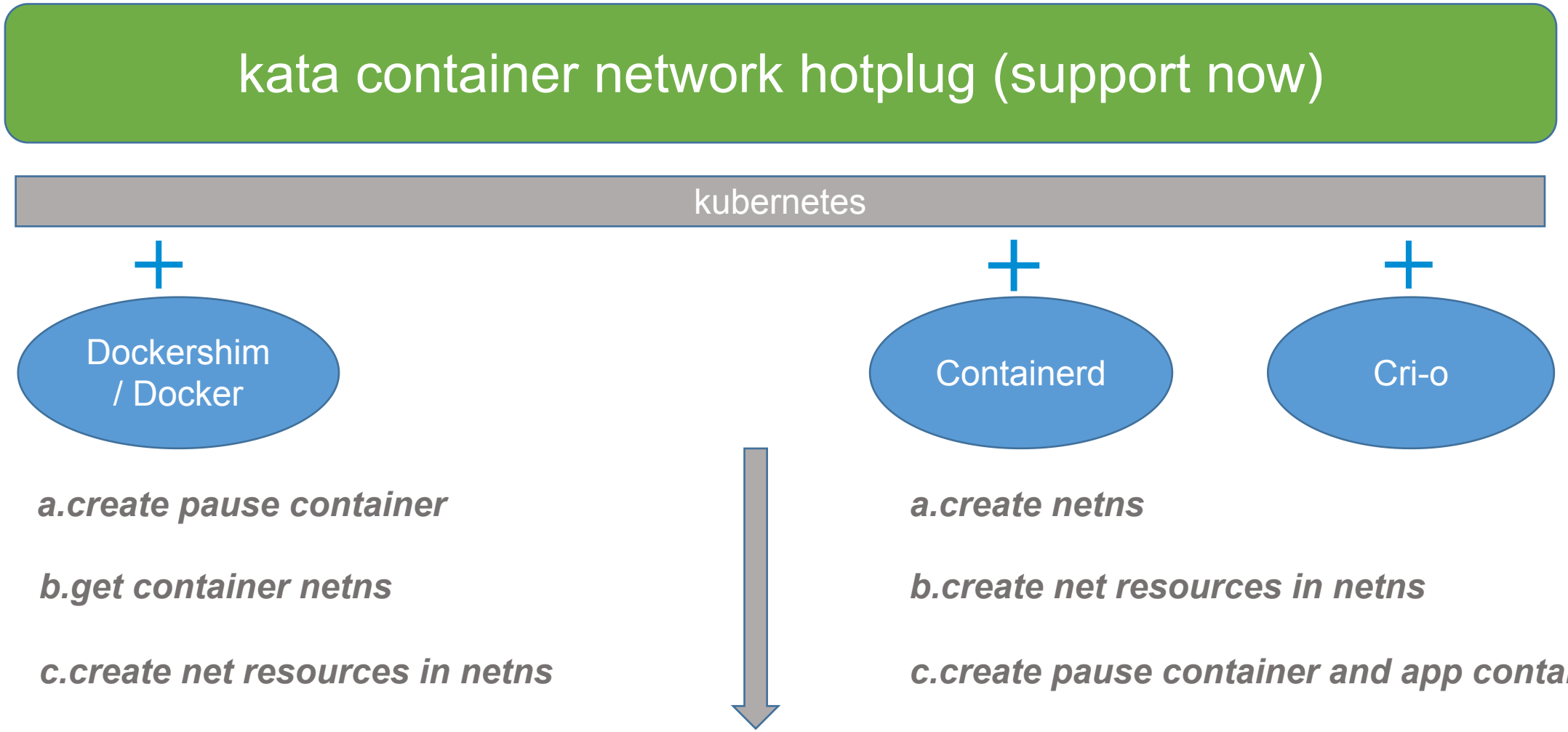


k8s + docker + kata not easy

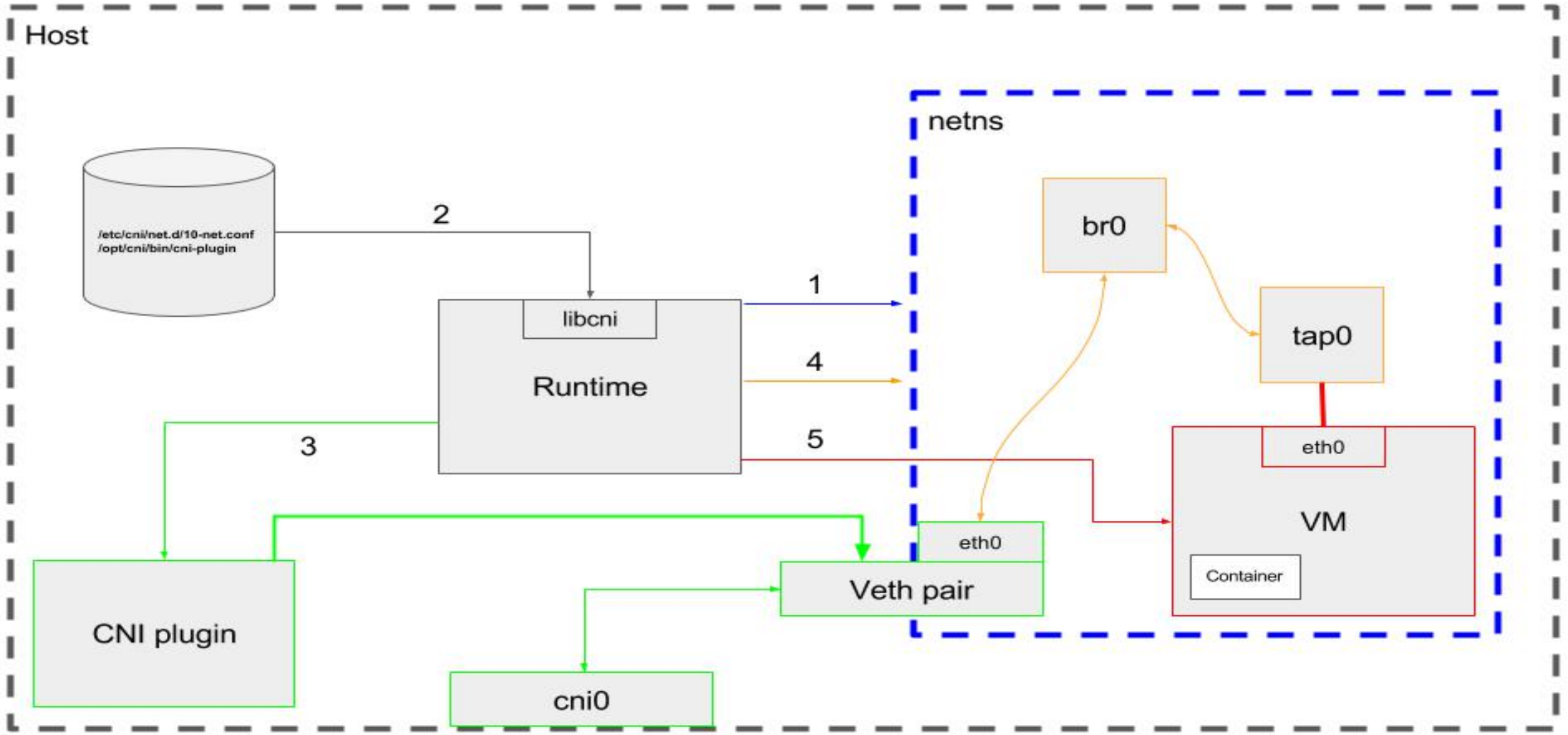
kubernetes(dockershim)
 does not support to choose
OCI runtime



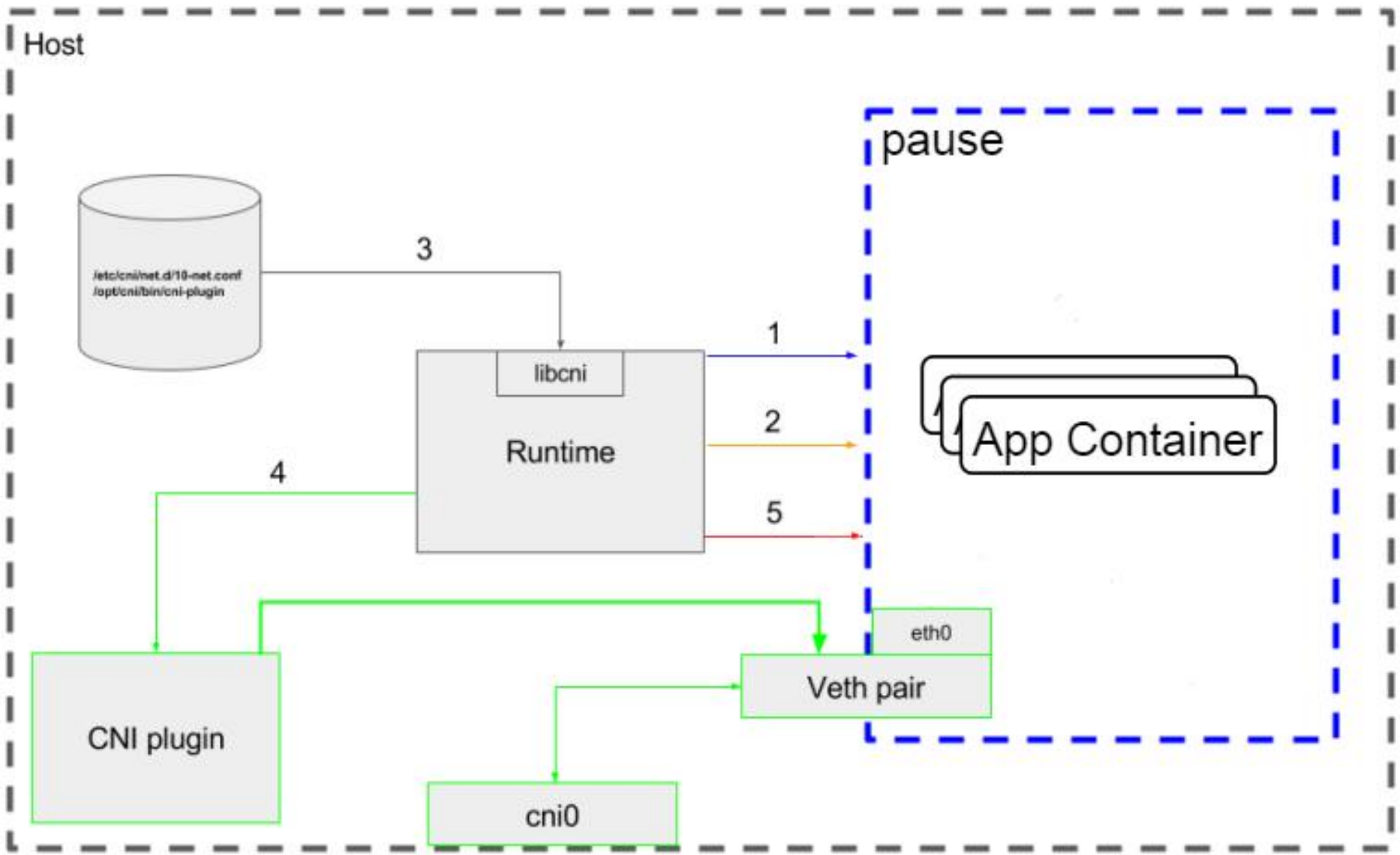
k8s + docker + kata not easy



k8s + docker + kata create pod



k8s + docker + runc create pod



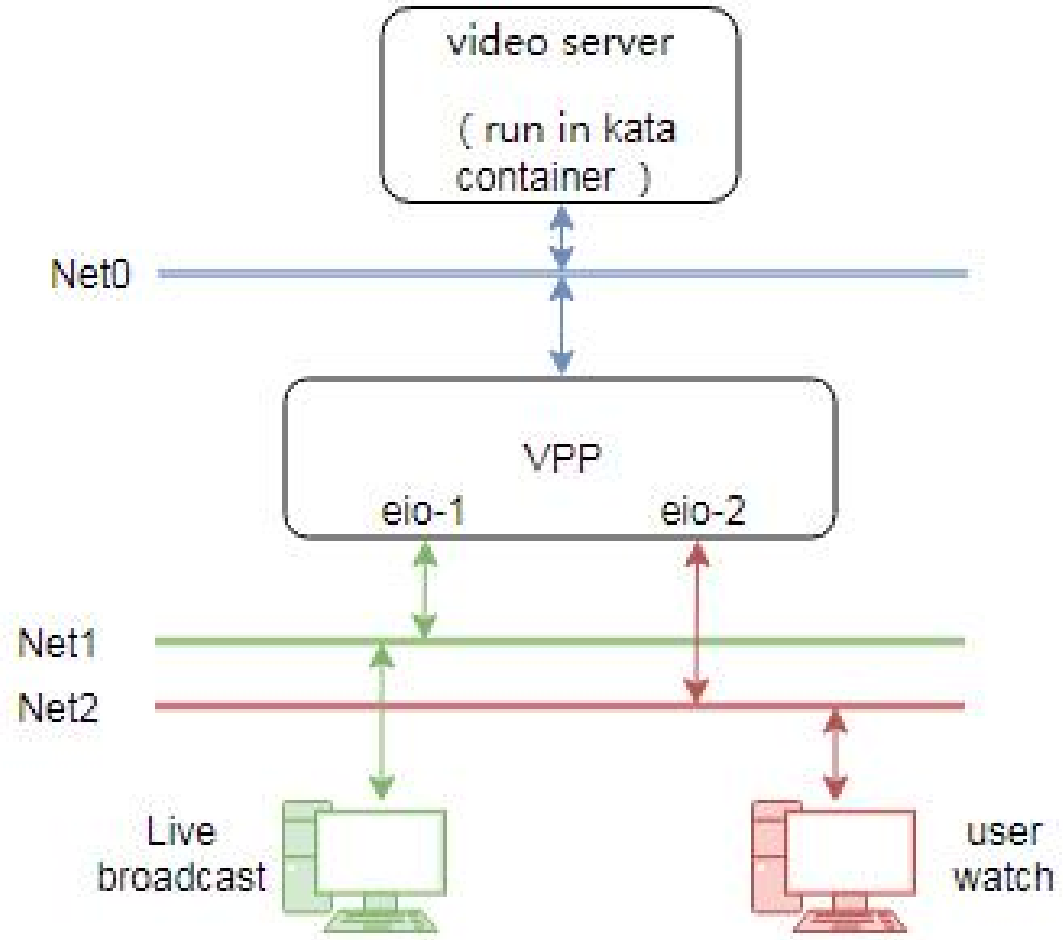
How ZTE Uses kata container in NFV

ZTE OpenPalette

kubernetes based PAAS

+

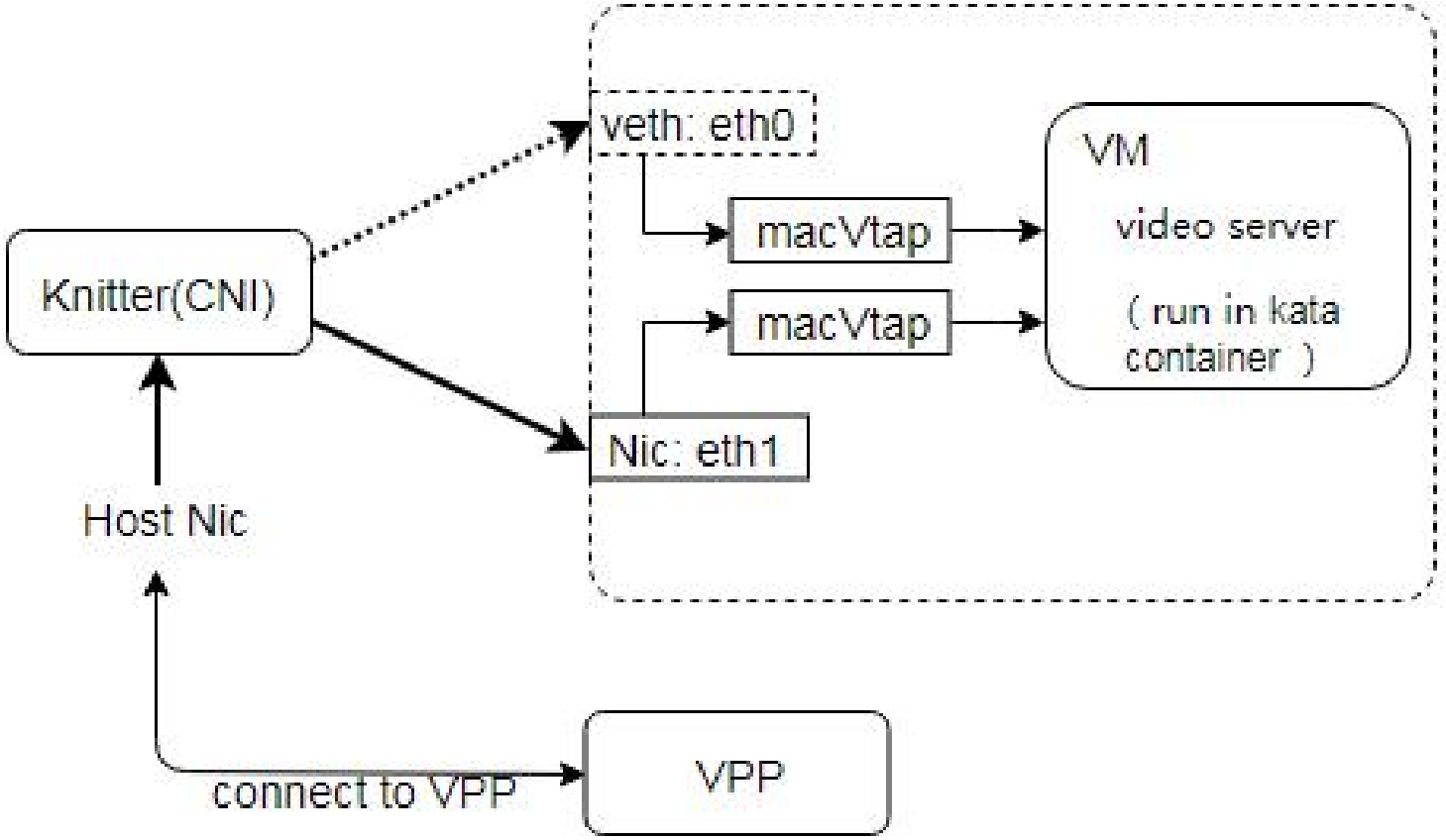
kata container 1.3



How ZTE Use kata container in NFV

ZTE Knitter

CNI based networking solution



gVisor

gVisor *is a user-space kernel that implements a substantial portion of the Linux system surface*

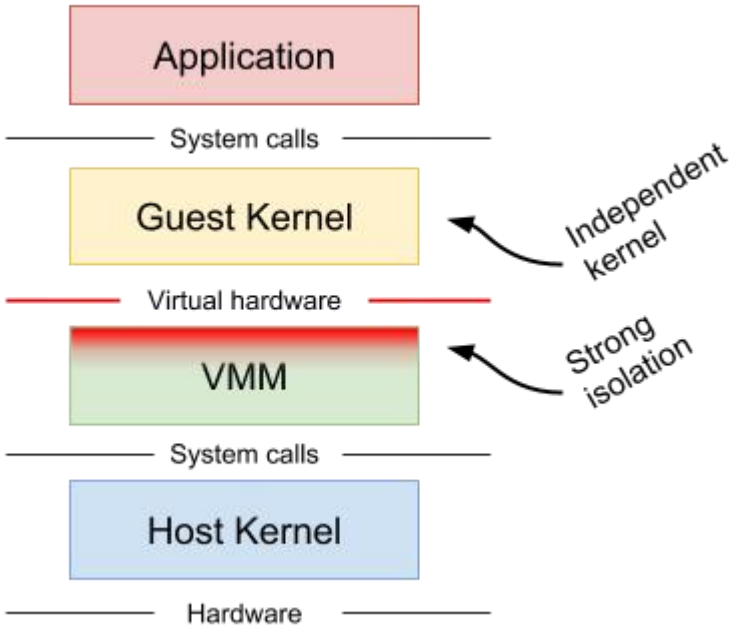
https://github.com/google/gvisor

Why does gVisor exist?

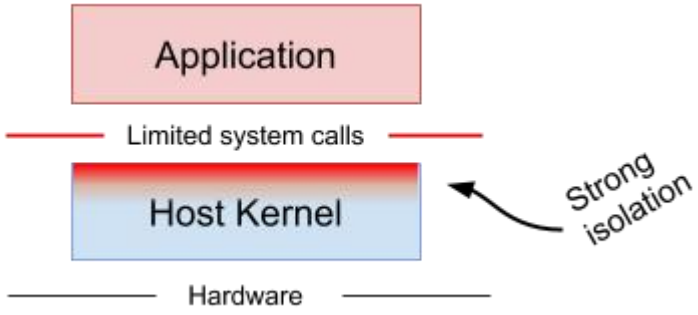
- ✓ *a single, shared kernel also mean that container escape is possible*
- ✓ *gVisor implements Linux by way of Linux*
- ✓ *another approach to enhance container isolation*

gVisor is special

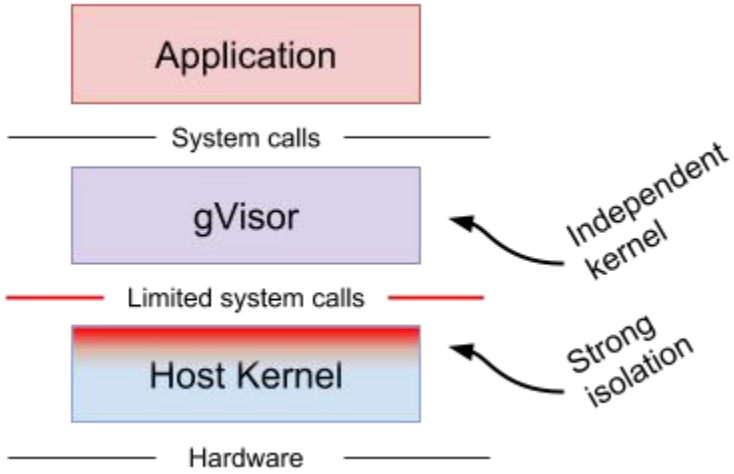
Machine-level virtualization



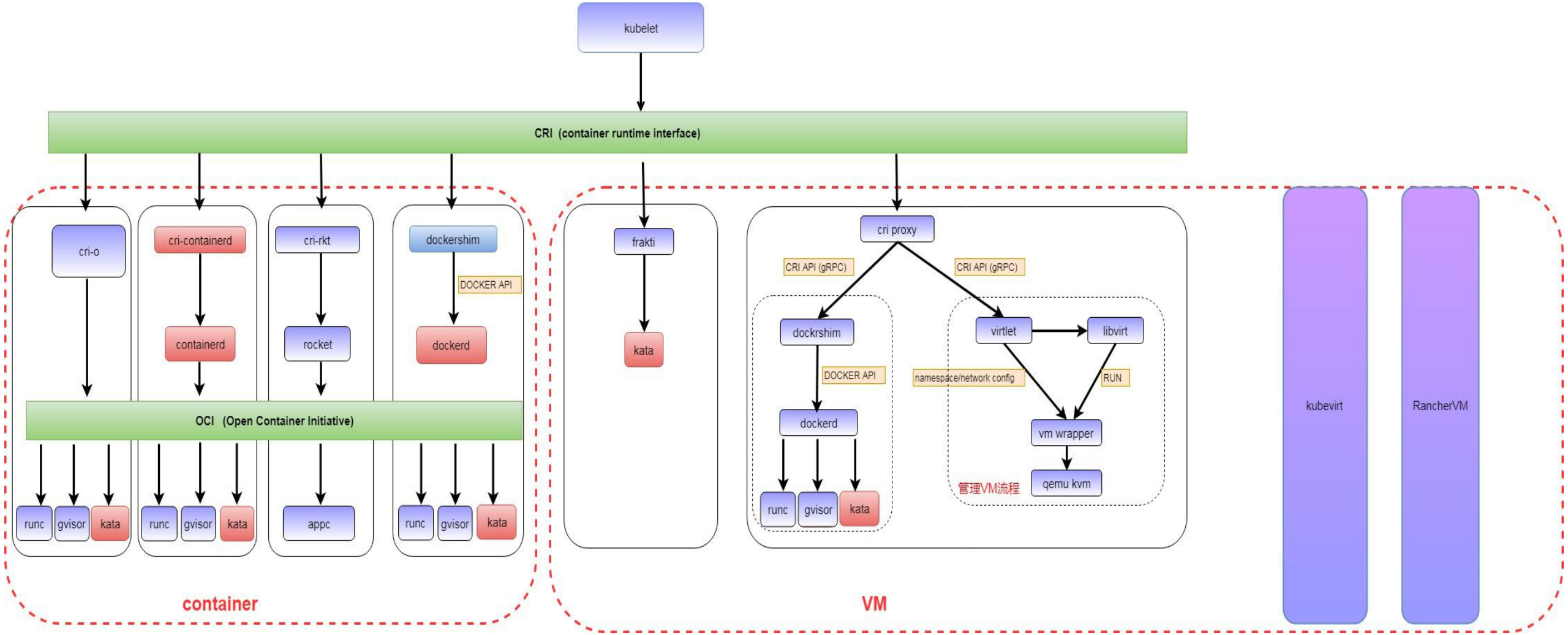
Rule-based execution



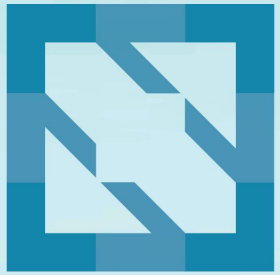
gVisor



Technology landscape



DEMO



KubeCon | CloudNativeCon

China 2018