



KubeCon

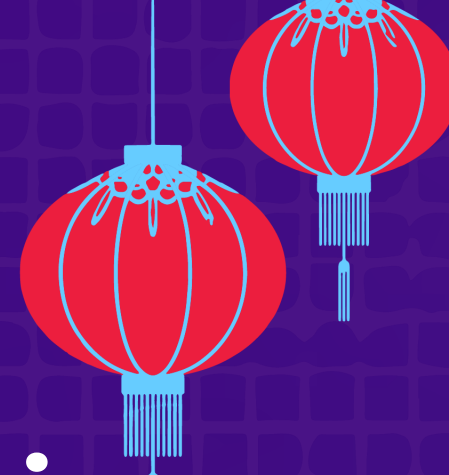
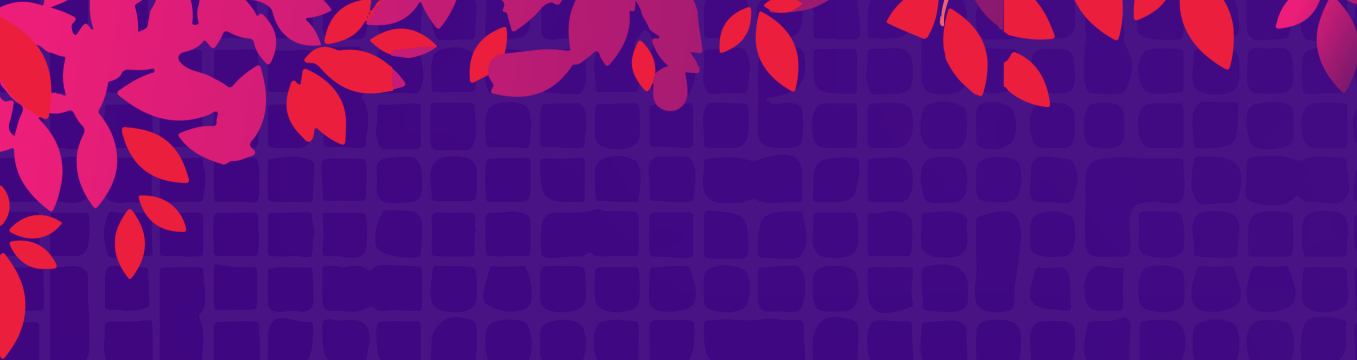


CloudNativeCon

OPEN SOURCE SUMMIT

China 2019





KubeCon



CloudNativeCon

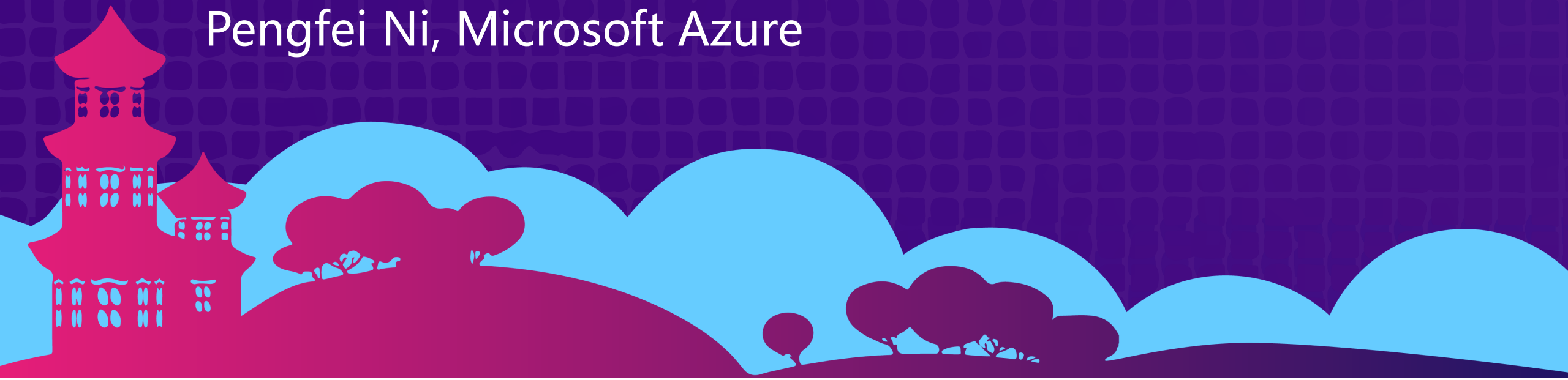


OPEN SOURCE SUMMIT

China 2019

Container Runtime Evolving in Kubernetes

Pengfei Ni, Microsoft Azure



Agenda



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

- Kubernetes Architecture
- Container Runtime Interface (CRI)
- Kubelet Container Runtime Evolving
- Future

Kubernetes Architecture



KubeCon

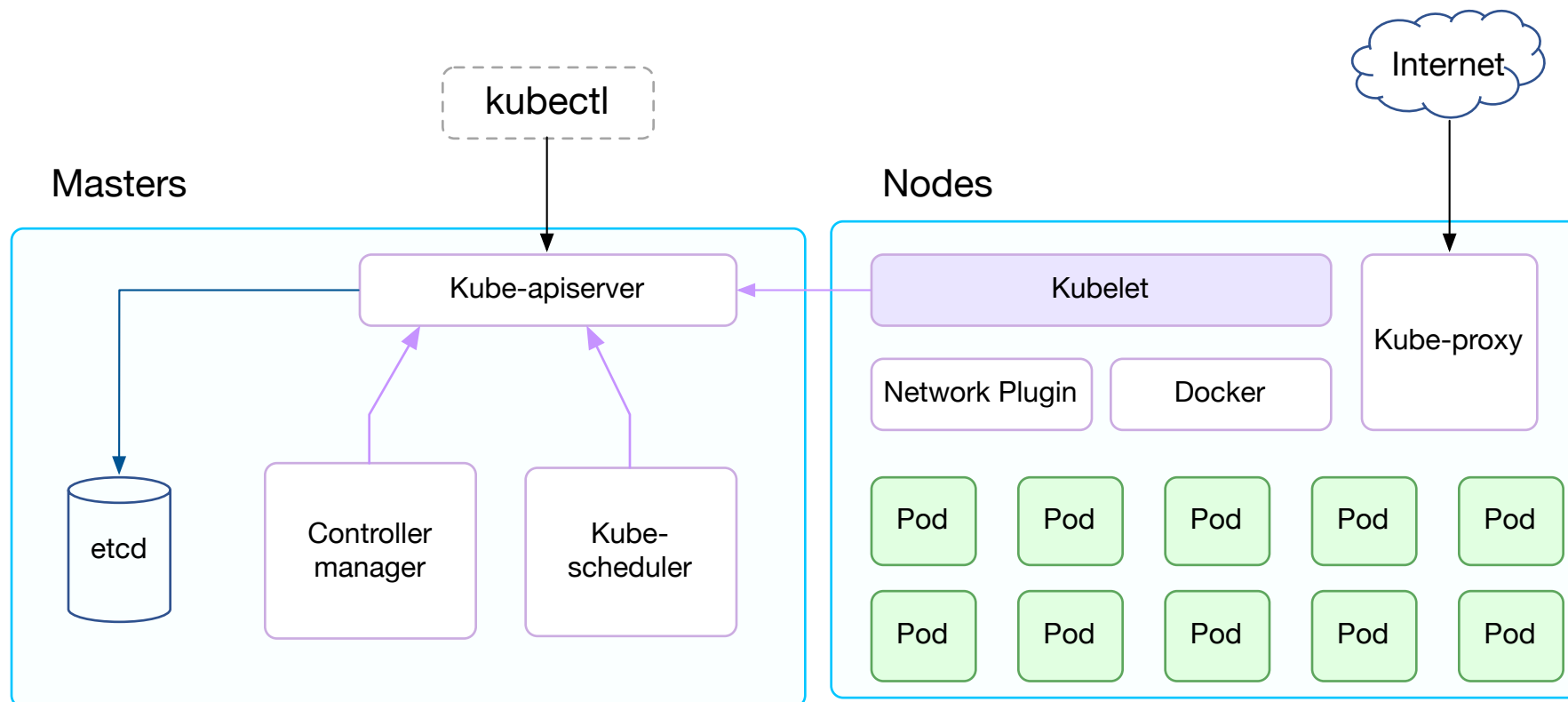


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019



Kubelet Architecture (continued)



KubeCon

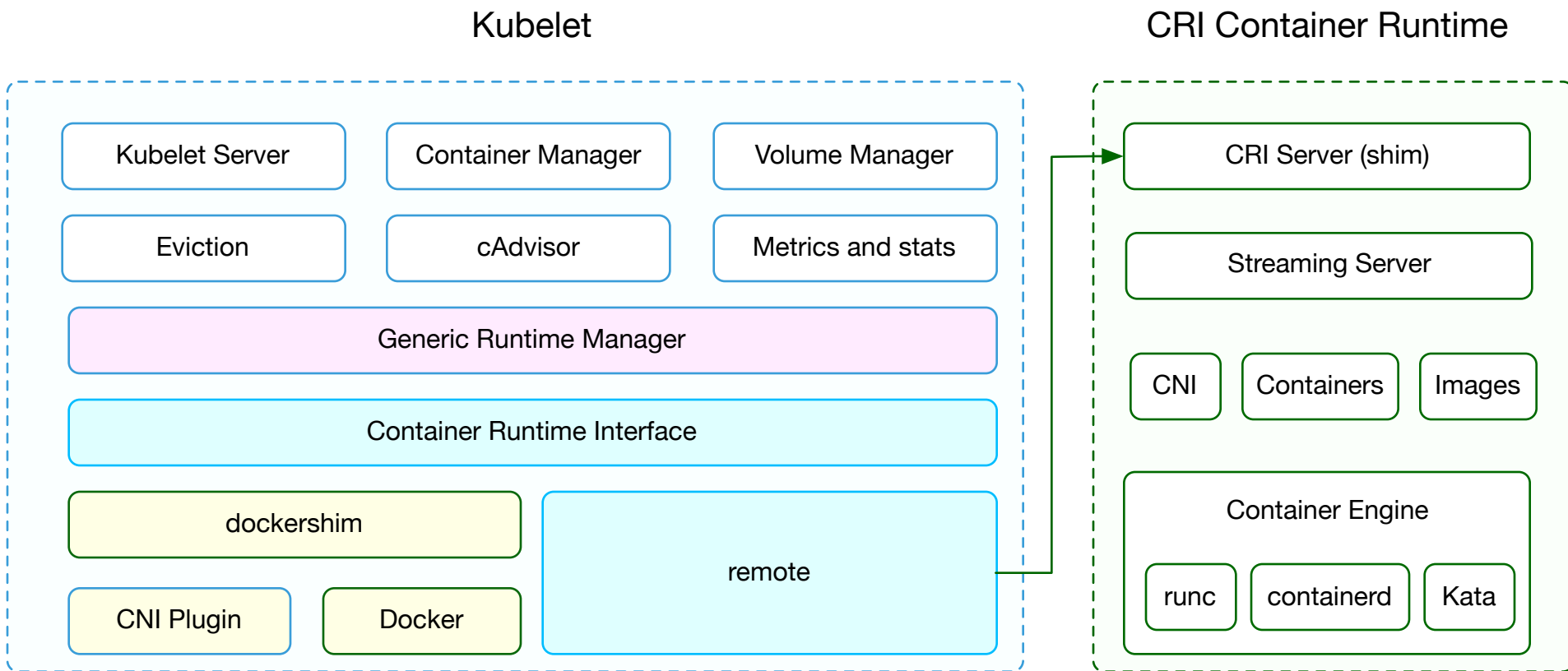


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019



Kubelet Container Runtime



KubeCon



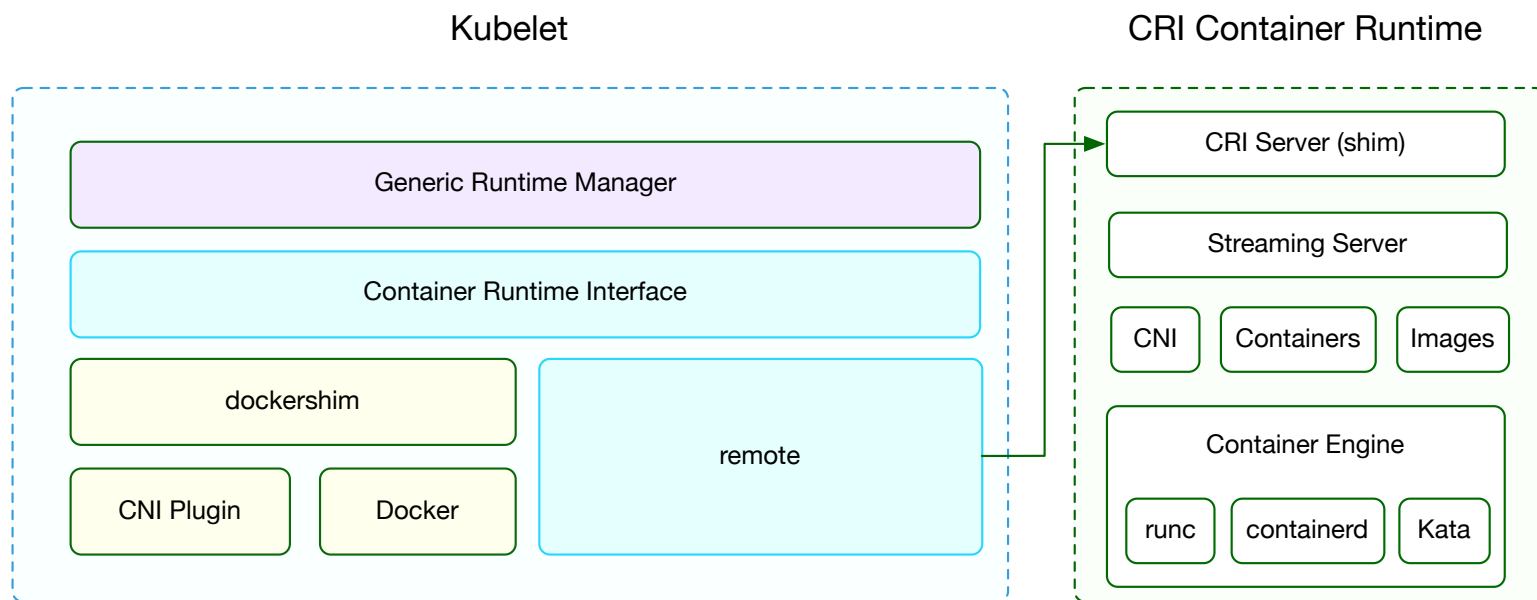
CloudNativeCon



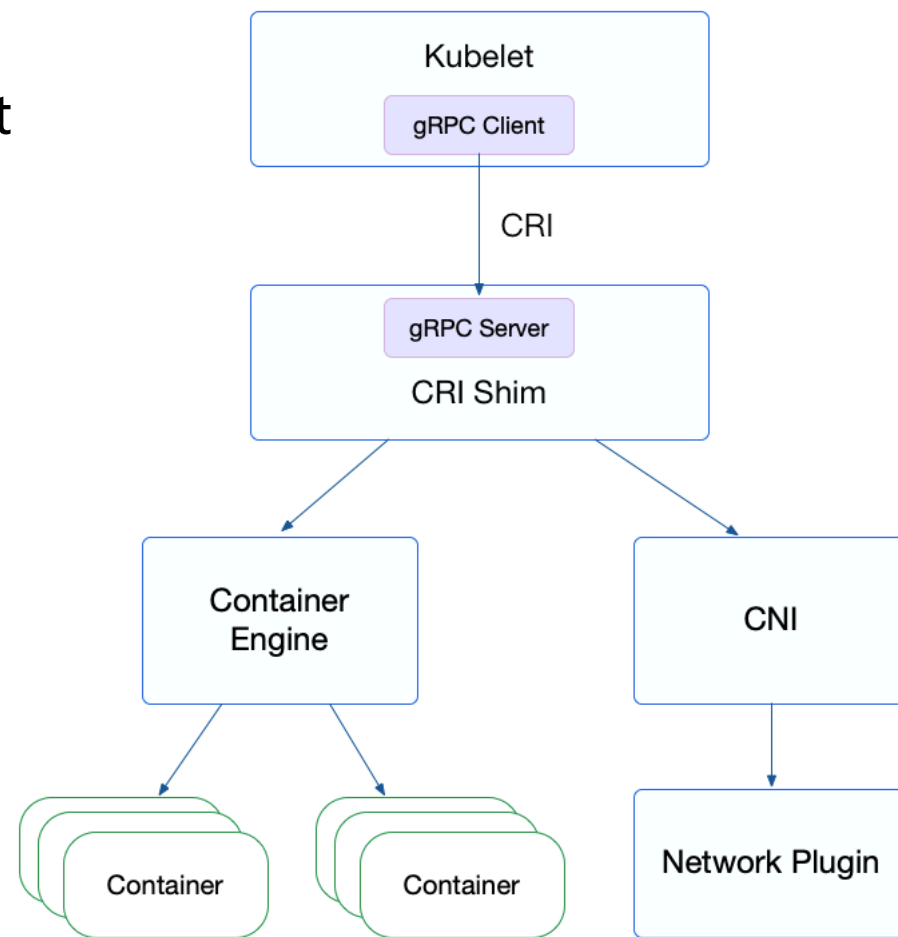
OPEN SOURCE SUMMIT

China 2019

- Kubelet manages container runtime via CRI
- Container runtime manages images, containers and networking
- Container runtimes
 - Built-in: docker
 - Remote: cri-o, ...



- Container Runtime Interface (CRI)
 - gRPC interfaces for container and image mgt
 - Streaming server library
 - CRI Tools
- Kubelet as the client for CRI server
- Easy to integrate based on gRPC framework
- Container runtime should take care of container networking (e.g. CNI)
- Kubelet config: `--container-runtime-endpoint`



CRI Interface



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

gRPC Server

RuntimeService

RunPodSandbox

StopPodSandbox

RemovePodSandbox

PodSandboxStatus

ListPodSandbox

UpdateRuntimeConfig

ContainerStats

CreateContainer

StartContainer

StopContainer

RemoveContainer

ListContainers

ContainerStatus

ExecSync

Exec

Attach

PortForward

Version

Status

ImageService

ListImages

PullImage

ImageStatus

RemoveImage

ImageFsInfo

CRI Streaming Interface



KubeCon



CloudNativeCon

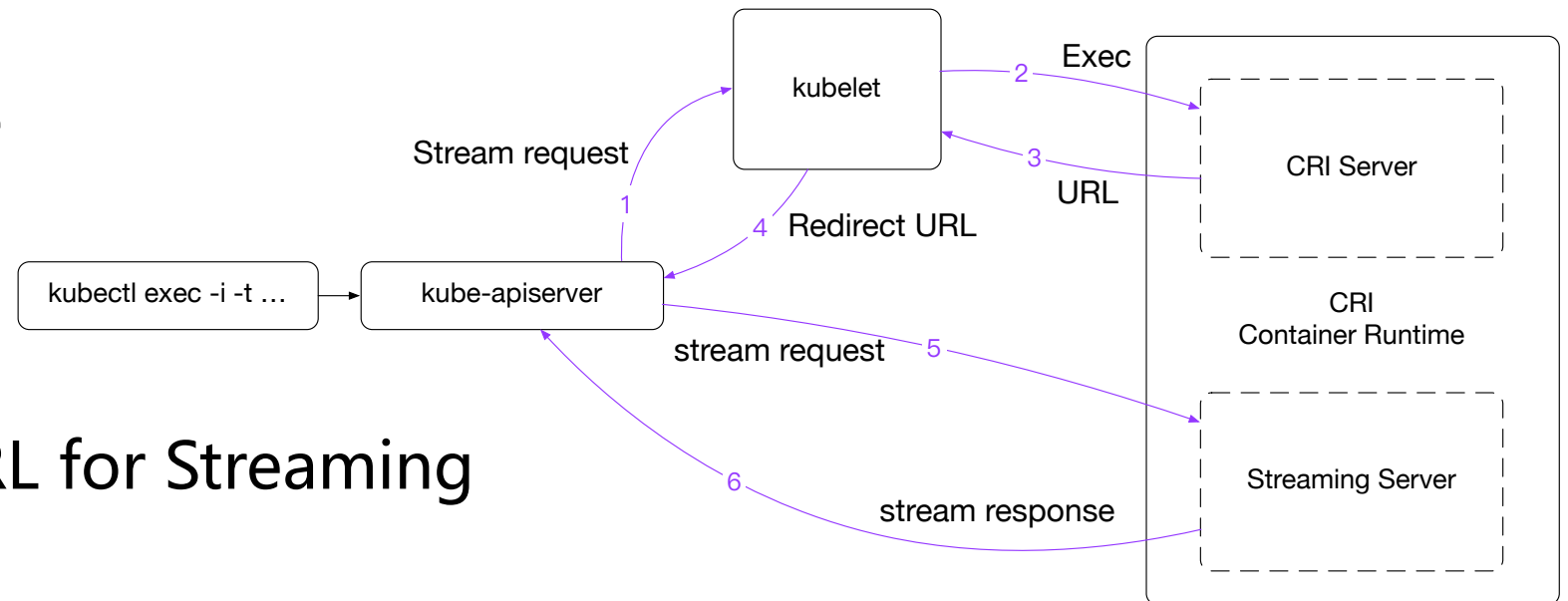


OPEN SOURCE SUMMIT

China 2019

- Streaming interface
 - Exec
 - Attach
 - PortForward
- Runtime returns URL for Streaming Server
- Streaming server library

<https://github.com/kubernetes/kubernetes/tree/master/pkg/kubelet/server/streaming>



Container Runtime Evolving



KubeCon

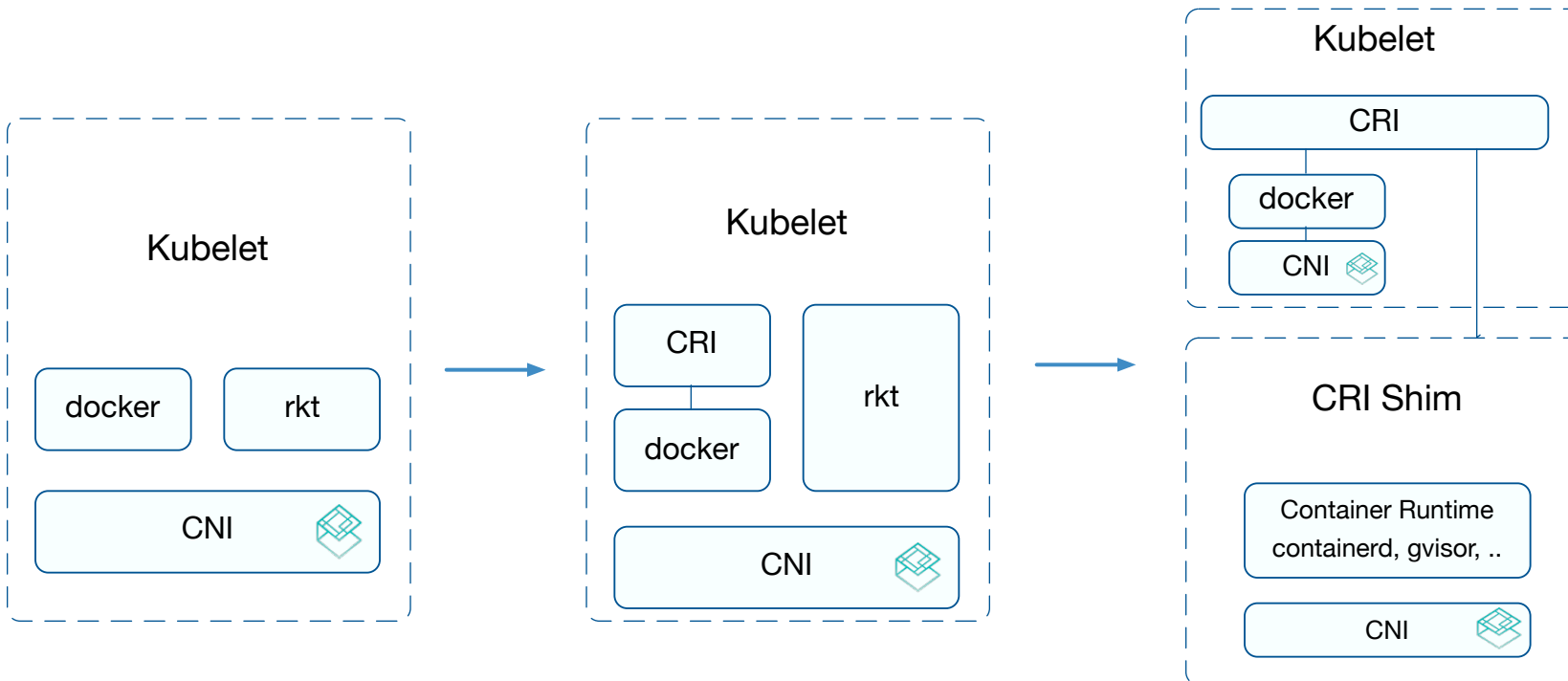


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019



CRI Container Runtimes



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

CRI Container Runtime	Community	Features	Container Engine
Dockershim	Kubernetes	Kubelet built-in	docker
cri-o	Kubernetes	OCI-compatible and no need of docker	OCI (runc、kata、gVisor...)
cri-containerd	Containerd	OCI-compatible and no need of docker	OCI (runc、kata、gVisor...)
Frakti	Kubernetes	Virtualization	hyperd、docker
rktlet	Kubernetes	rkt supported	rkt
PouchContainer	Alibaba	Rich container engine	OCI (runc、kata...)
Virtlet	Mirantis	VM and QCOW2	Libvirt (KVM)

Container Runtime landscape



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019



CNCF Graduated



cri-o

CNCF Incubating



rkt

CNCF Incubating



Firecracker



gVisor



kata



Ixd



Nabla Containers



Pouch



OPEN CONTAINER INITIATIVE
runc



Singularity



SmartOS



unik

CRI TOOLS - CRICTL



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

- Sub-project of SIG Node
- CLI for CRI-compatible container runtimes
- Facilitates container runtime inspecting and debugging
- Simple UX
 - *crictl pods*
 - *crictl ps*
 - *crictl images*
 - *crictl exec*
 - ...

CRI TOOLS - CRITEST



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

- Test framework for CRI container runtimes
- Validate whether container runtime meets CRI requirements
- Benchmark CRI interfaces
 - *critest -benchmark*
- Integrated into devops is encouraged
- Publish validation results to [TestGrid](#) is encouraged

Future of Container Runtime



KubeCon



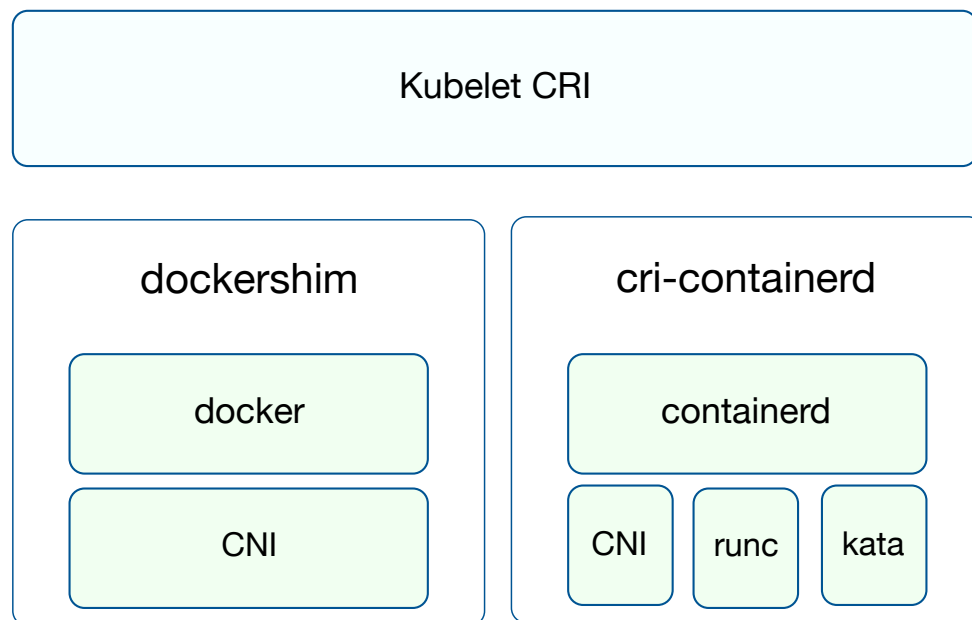
CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

Out-of-tree dockershim



Security hardened container engine



KubeCon

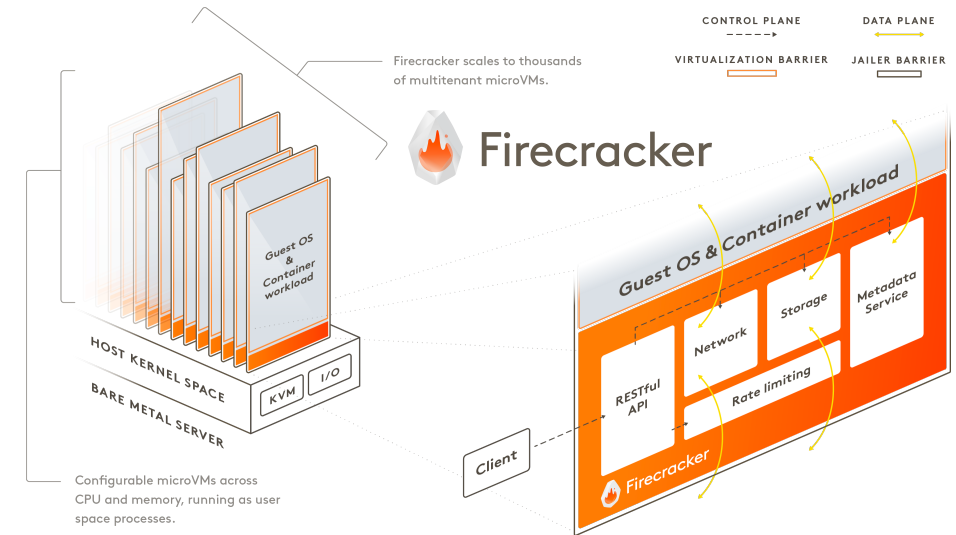
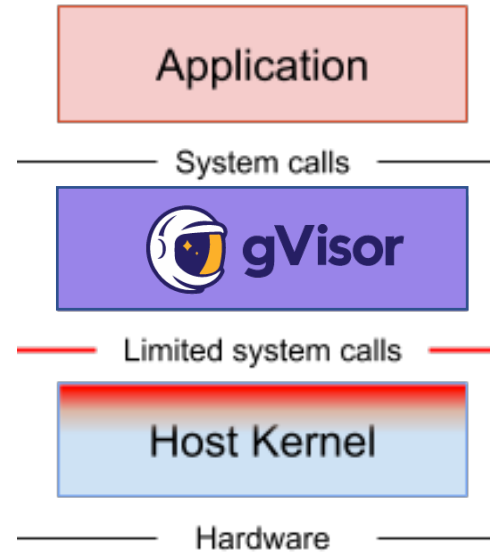
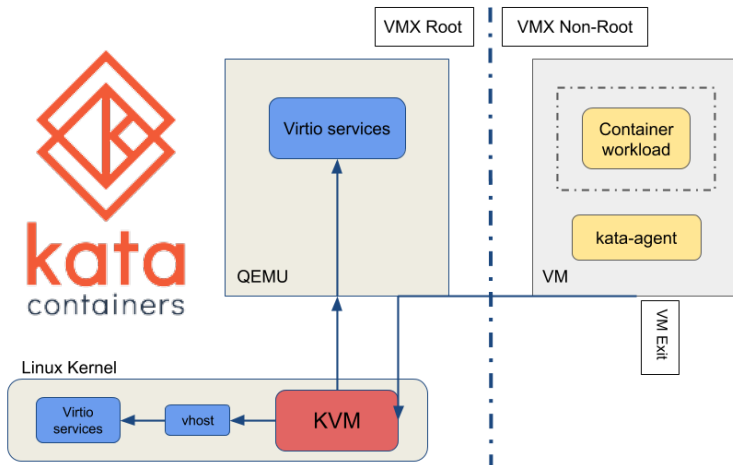


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019



Multiple Container Runtimes



CloudNativeCon

OPEN SOURCE SUMMIT

China 2019

- RuntimeClass (v1.14 beta)
 - runc + kata
 - runc + gVisor
 - Windows server containers + Hyper-V containers

```
apiVersion: node.k8s.io/v1beta1
kind: RuntimeClass
metadata:
  name: myclas
# RuntimeClass is a non-namespaced
resource
handler: myconfiguration
```

```
apiVersion: v1
kind: Pod
metadata:
  name: mypod
spec:
  runtimeClassName: myclass
# ...
```

Serverless Containers



KubeCon



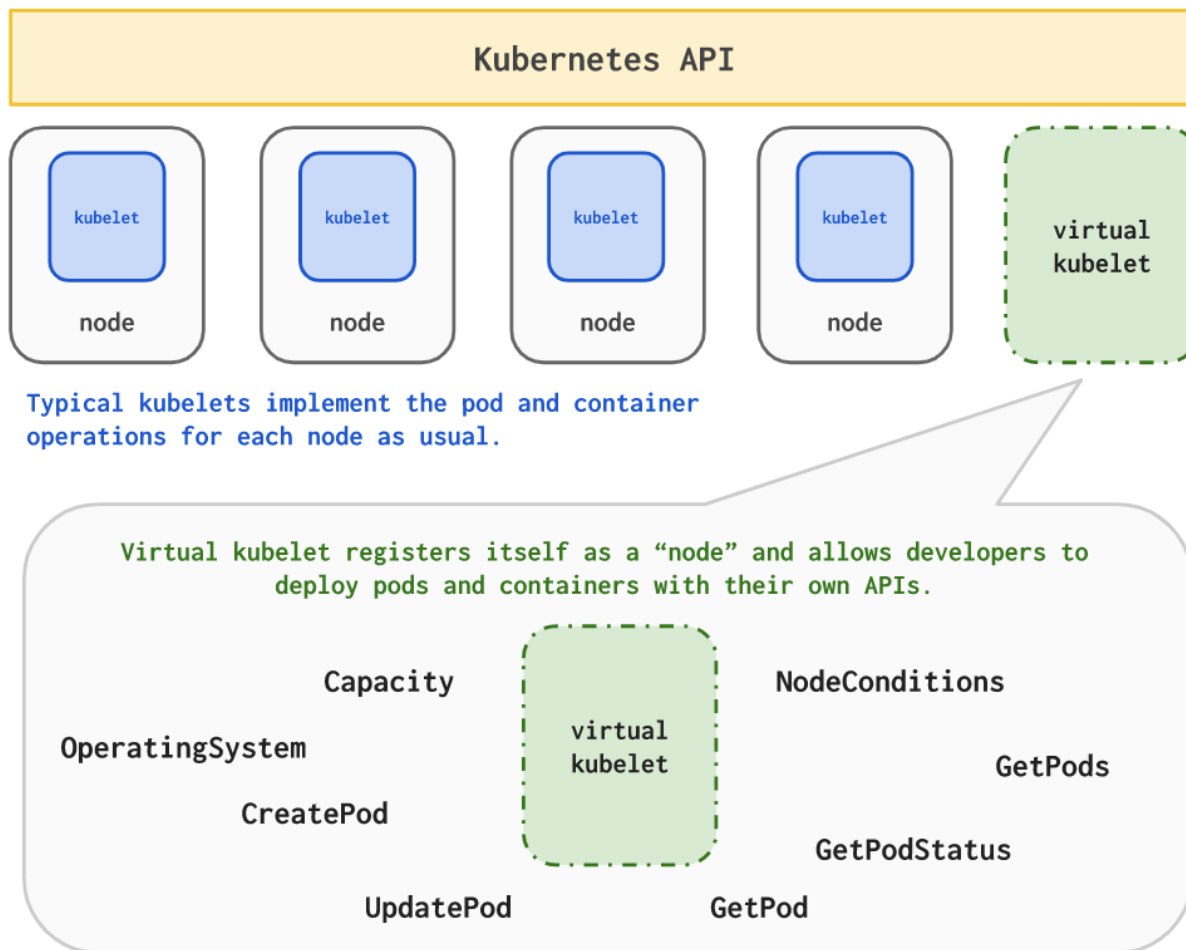
CloudNativeCon

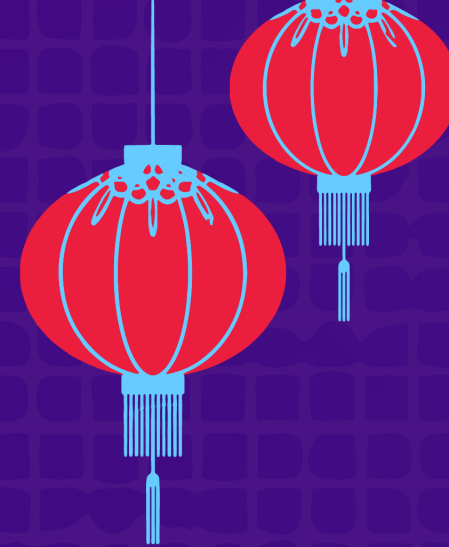
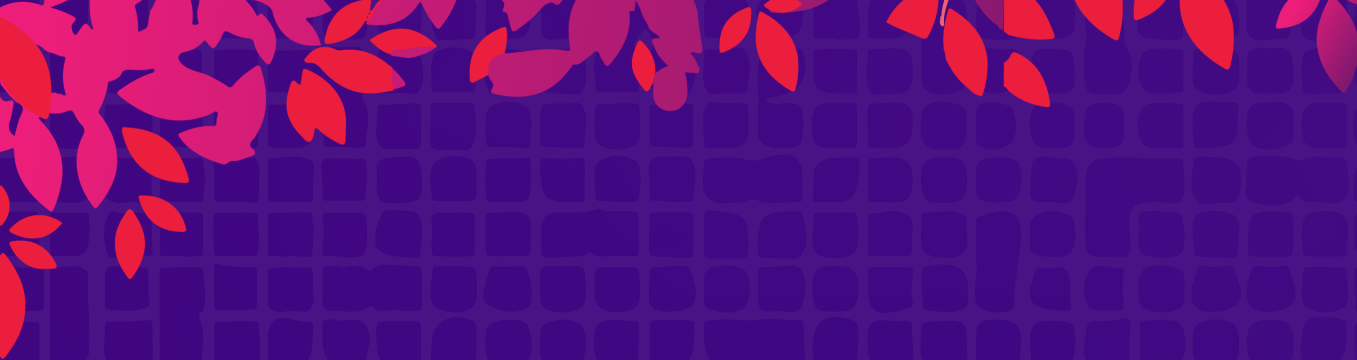


OPEN SOURCE SUMMIT

China 2019

- Virtual Kubelet
 - Masquerade kubelet
 - Virtual nodes
- Serverless container providers
 - Azure Container Instance
 - AWS Fargate
 - Service Fabric
 - IoT Edge
- Serverless Kubernetes





KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

QA

