



KubeCon

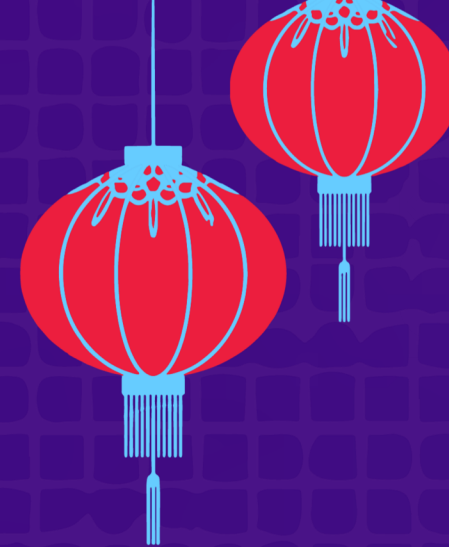


CloudNativeCon

OPEN SOURCE SUMMIT

China 2019





阿里巴巴利用 K8S、Kata 容器和裸金属服务器构建无服务器平台

张翼飞 阿里云技术专家

唐华敏 阿里云高级开发工程师





- Serverless Overview
- Serverless 平台建设
- Kata 安全容器
- Q&A

Serverless Overview – 现状



KubeCon

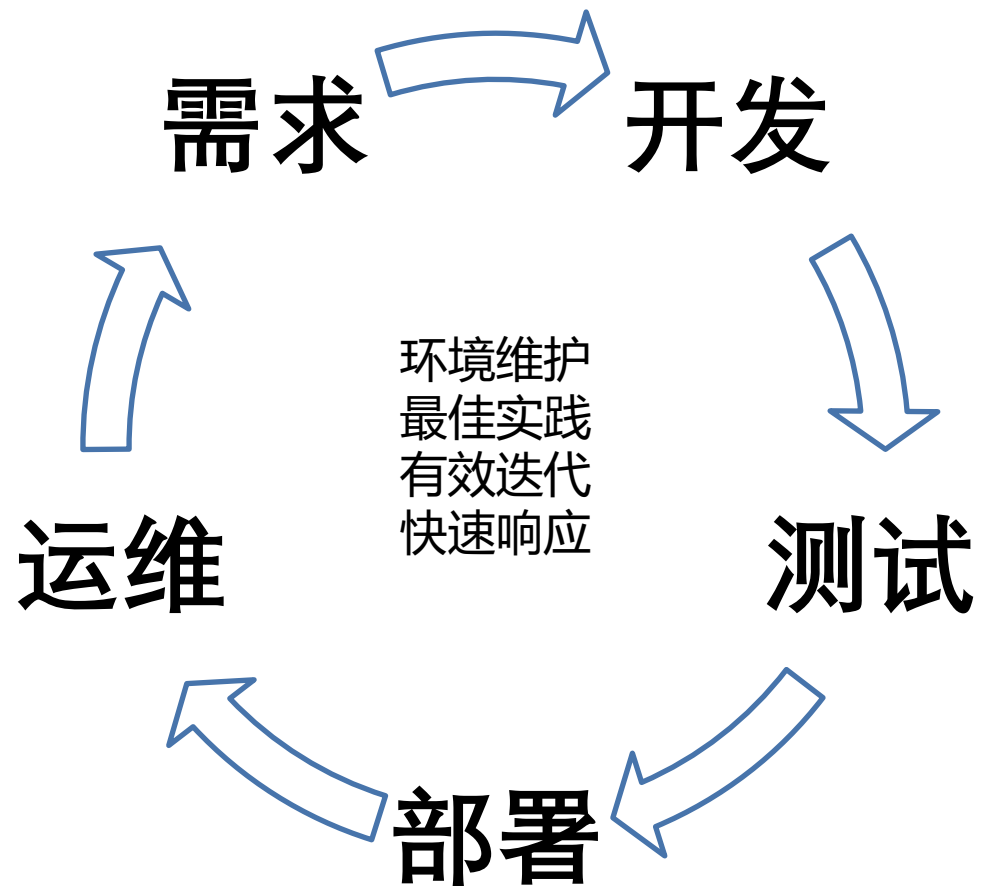


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019



Serverless Overview – 问题域



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

如何降低运行/运维
成本

如何降低开发成本

Serverless Overview – 定义



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

维基百科：

- Serverless computing is a cloud-computing execution model in which the cloud provider runs the server, and dynamically manages the allocation of machine resources. Pricing is based on the actual amount of resources consumed by an application, rather than on pre-purchased units of capacity.
- Serverless computing can simplify the process of deploying code into production. Scaling, capacity planning and maintenance operations may be hidden from the developer or operator. Serverless code can be used in conjunction with code deployed in traditional styles, such as microservices. Alternatively, applications can be written to be purely serverless and use no provisioned servers at all.

Serverless Overview – 角色



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

用户

- 无需关心服务器
- 按使用量付费
- 弹性伸缩
- etc.

平台

- 提供资源池服务
- 提供按需的计量/计费服务
- 提供弹性伸缩服务
- 提供安全的数据面服务
- etc.

Serverless Overview – 场景



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

适用

- 事件驱动型任务
- 定时任务
- 启动/处理延时不敏感的任务

不适用

- 启动延迟敏感的任务
- 处理延迟敏感的任务

Serverless 平台建设 – 挑战



KubeCon

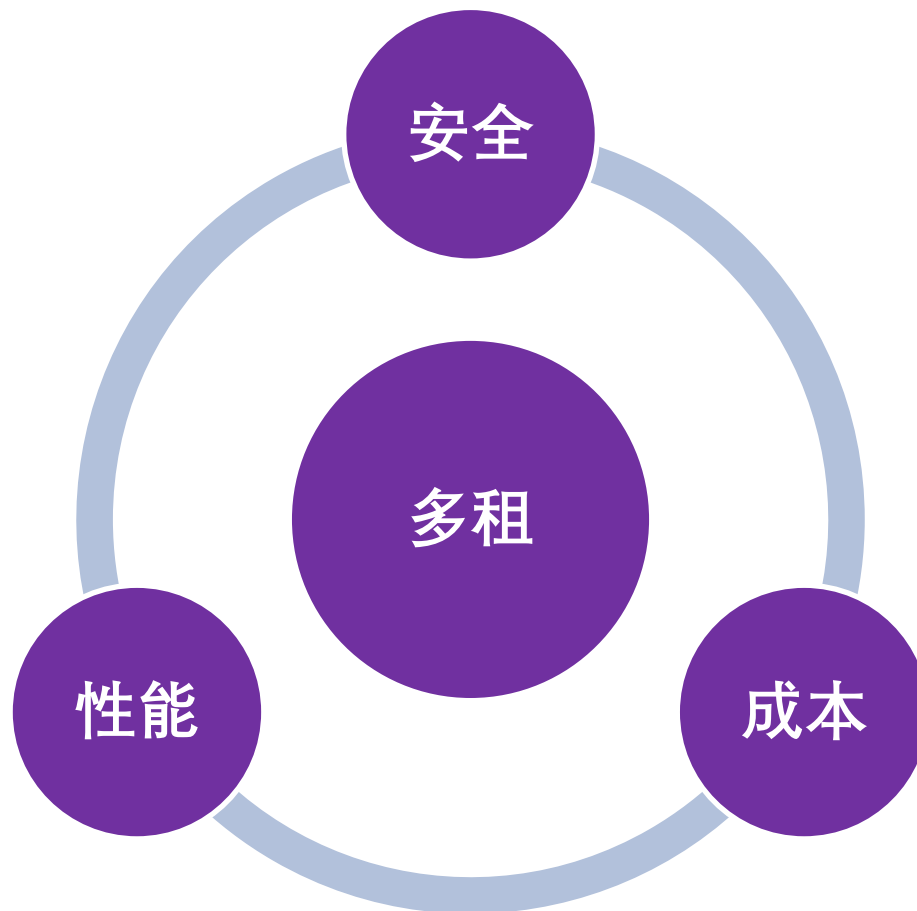


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019



Serverless 平台建设 – 挑战



KubeCon

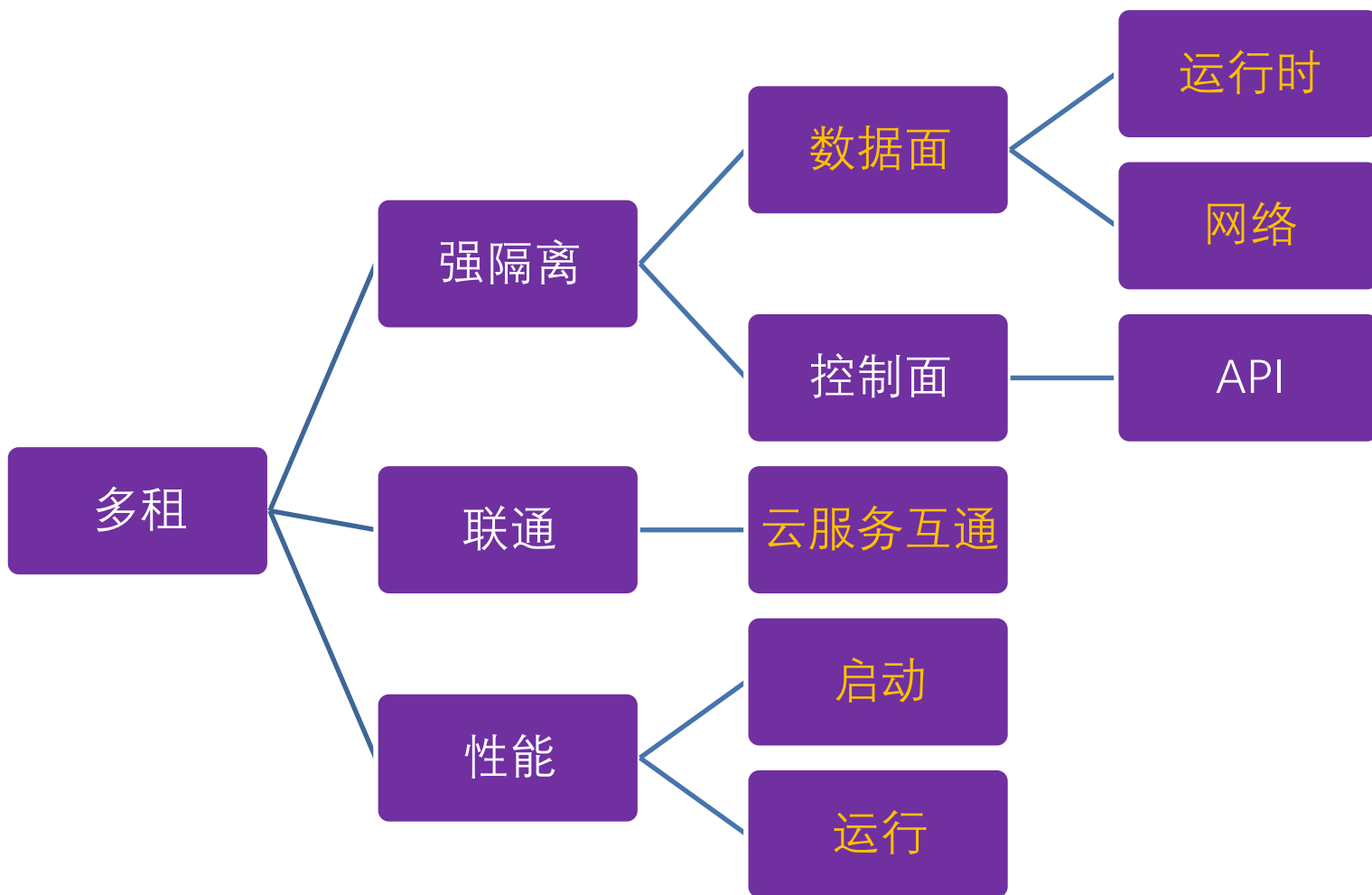


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019



Serverless 平台建设 – 解决方案



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

问题

- a 运行性能
- b 网络访问强隔离
网络访问互通
- c 运行时强隔离
毫秒级创建

解决方案

- a 弹性裸金属服务器
- b VPC 网络
- c 安全容器

Serverless 平台建设 – 解决方案



KubeCon



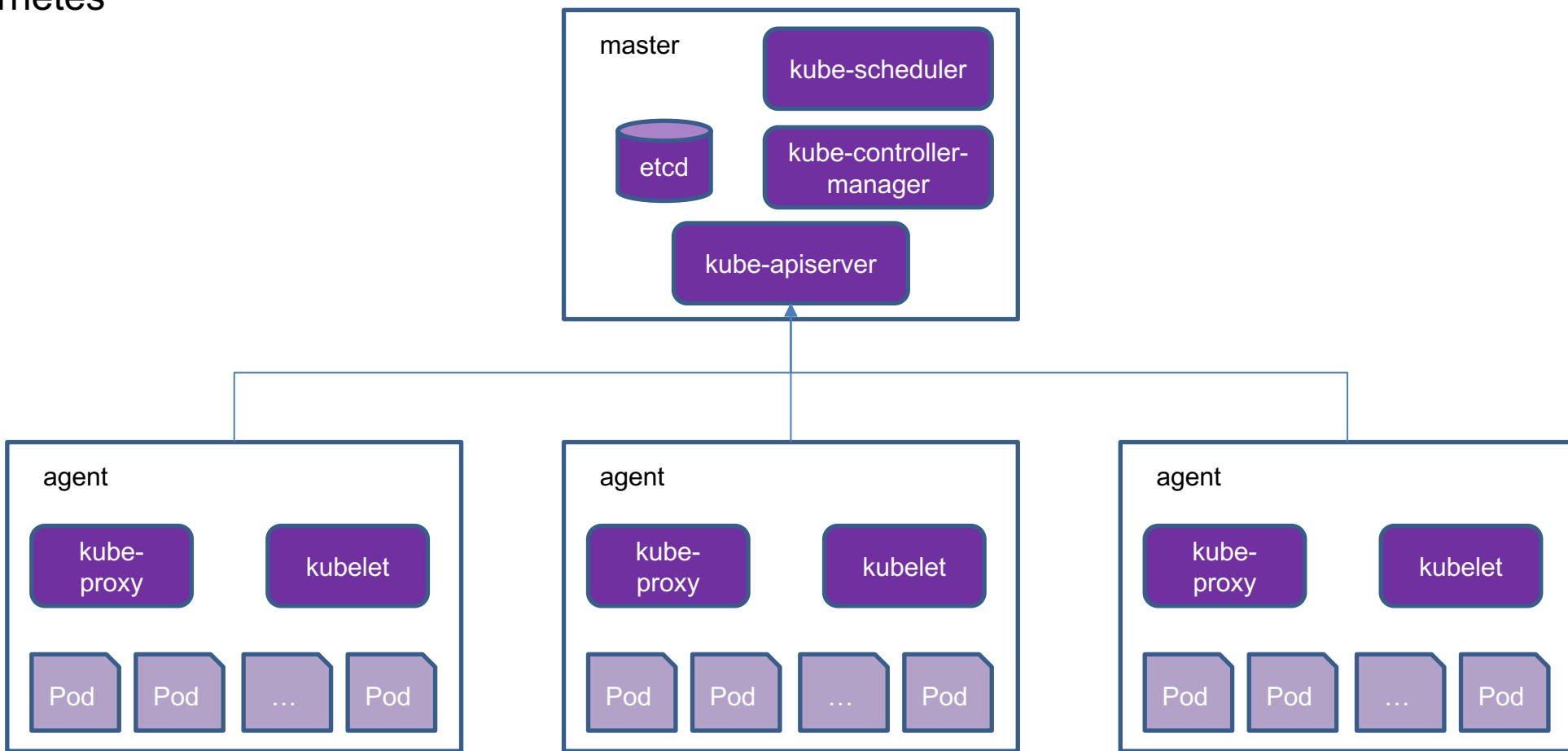
CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

Kubernetes



Serverless 平台建设 – 解决方案



KubeCon

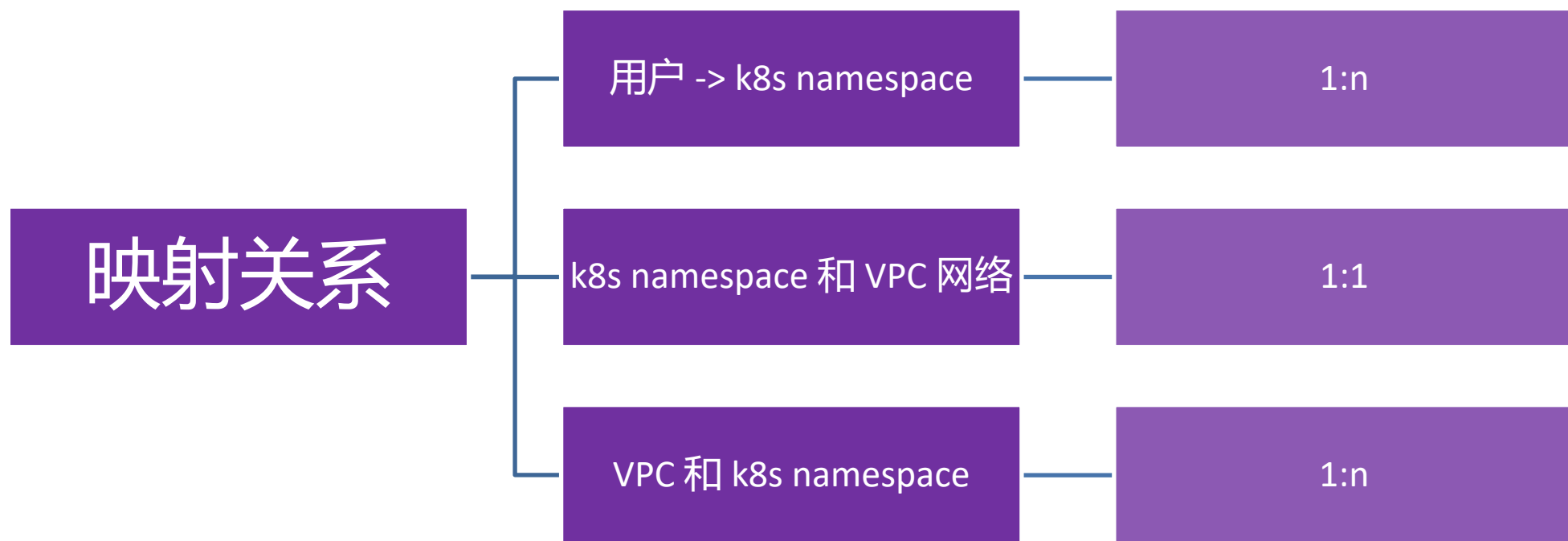


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019



Serverless 平台建设 – 解决方案



KubeCon

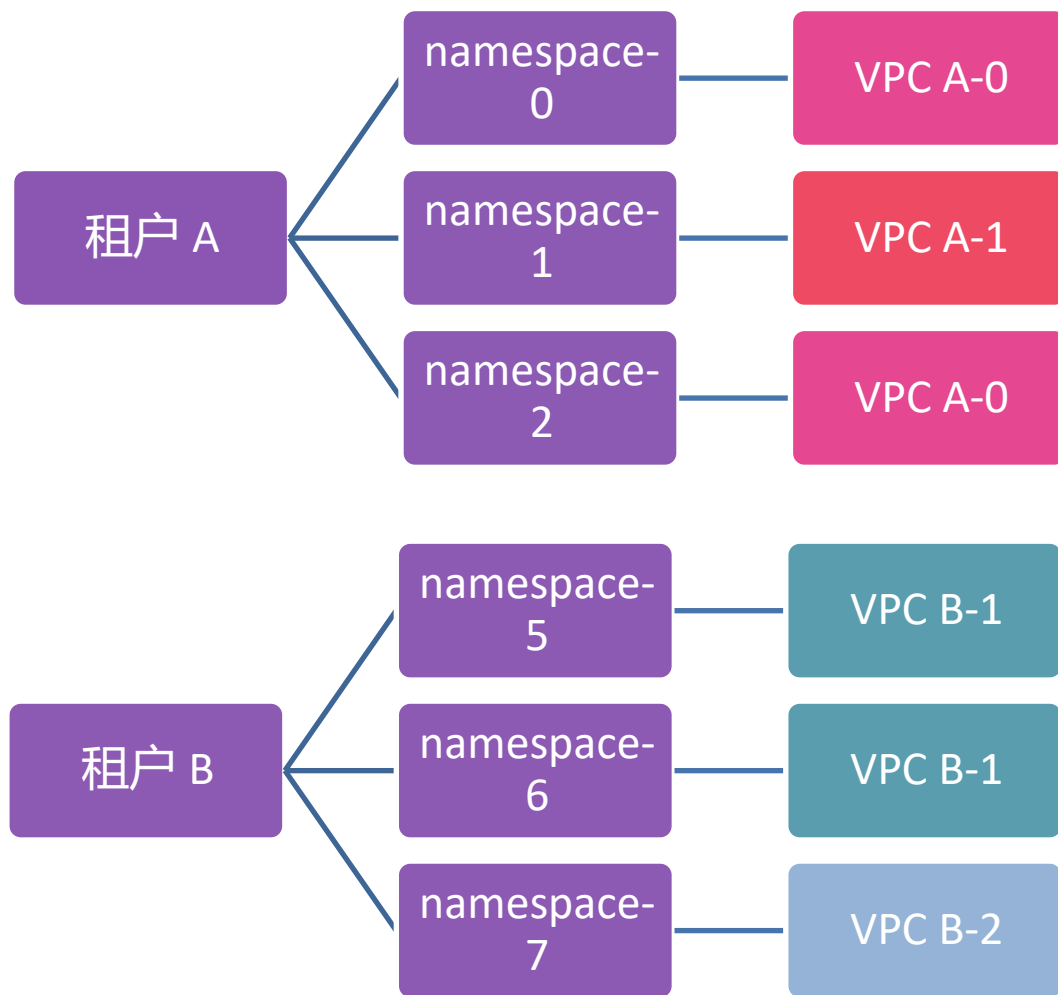


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019



Serverless 平台建设 – 架构图



KubeCon

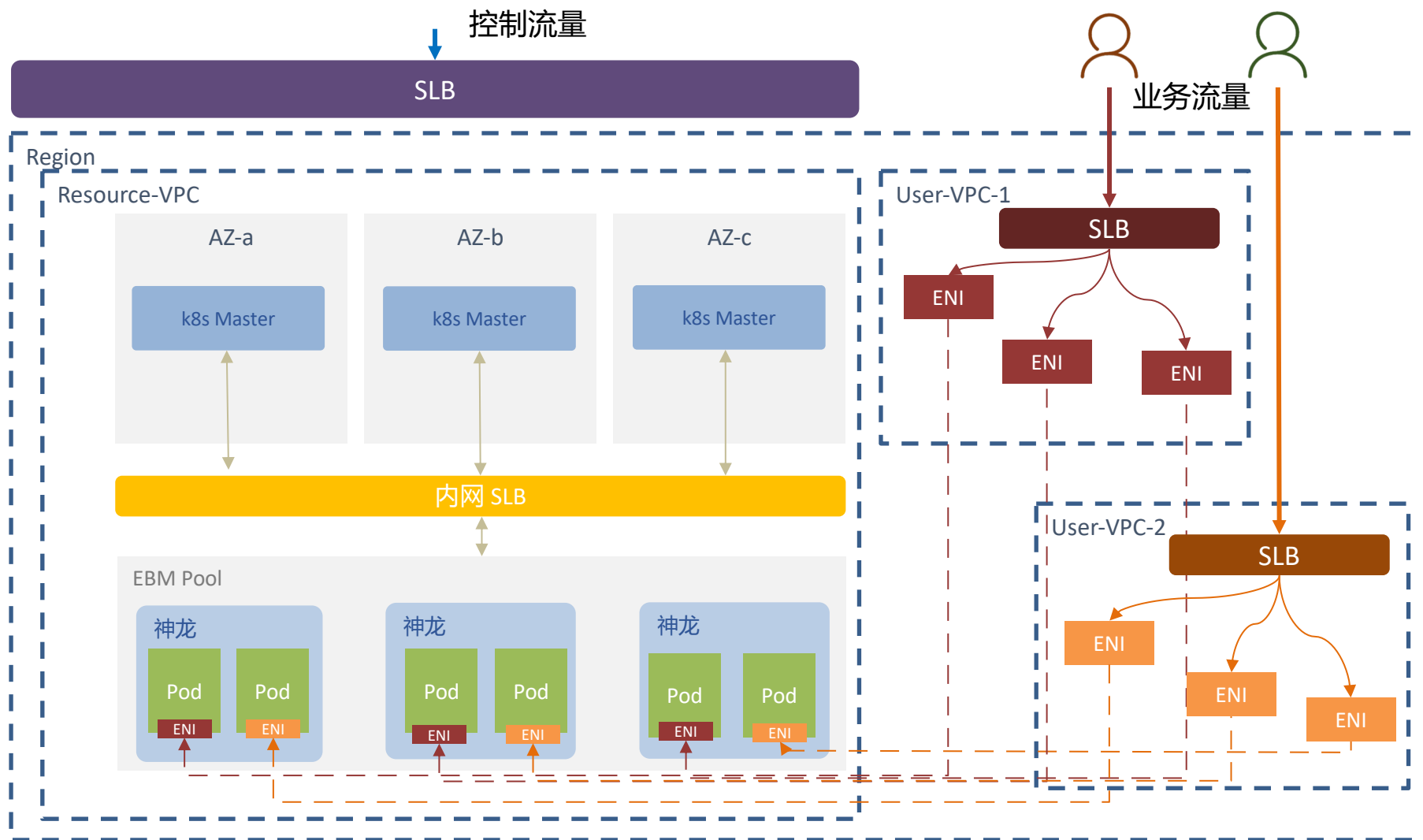


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019



Kata 安全容器-强隔离



KubeCon



CloudNativeCon

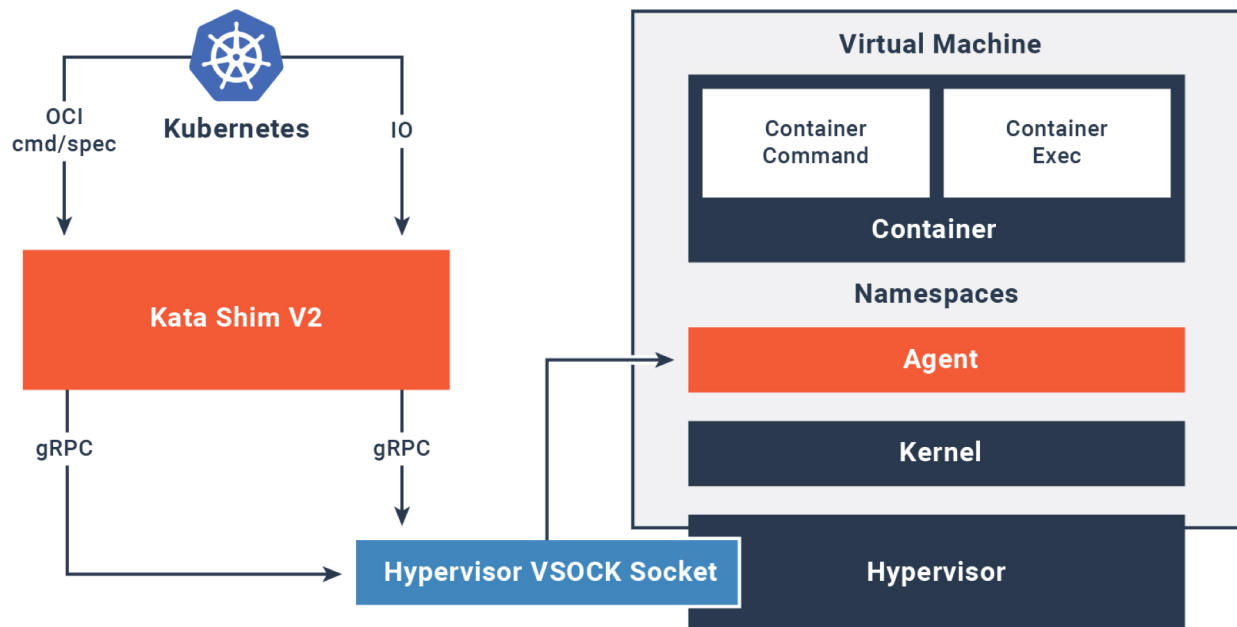


OPEN SOURCE SUMMIT

China 2019



Kata Shim V2



Kata 安全容器-强隔离



KubeCon

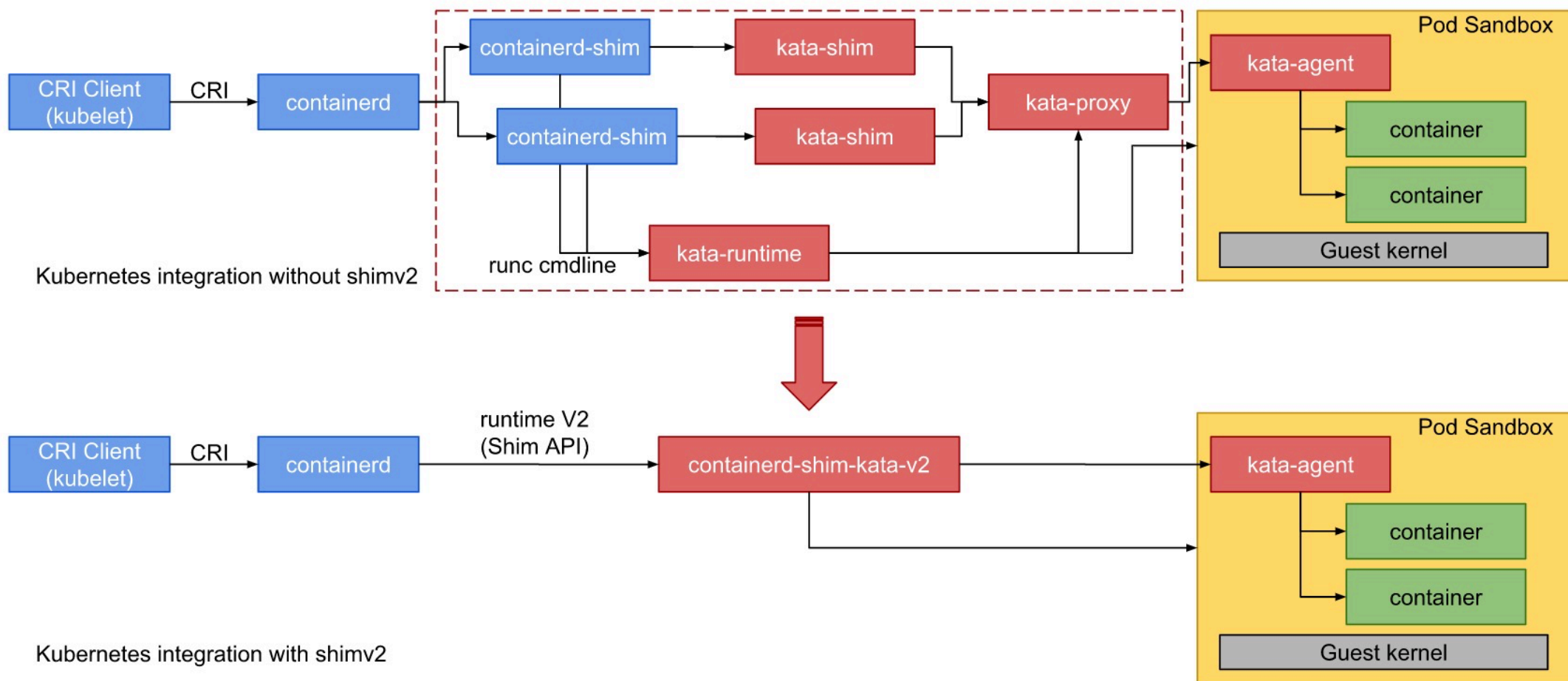


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019



Kata 安全容器 – 技术架构



KubeCon

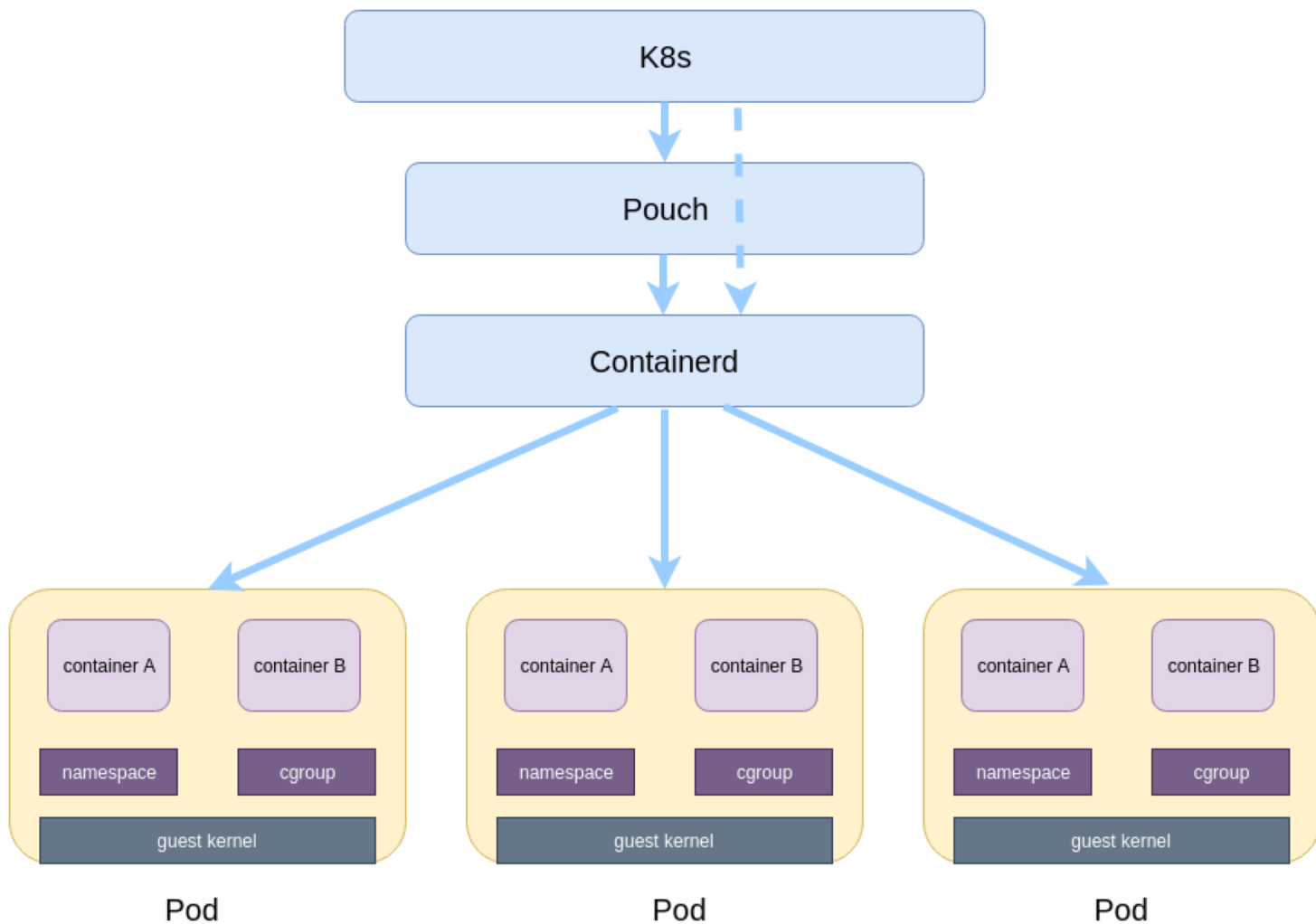


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019



- 宿主机：神龙
- guest kernel：4.9
- hypervisor：qemu

Kata 安全容器 – 网络方案



KubeCon

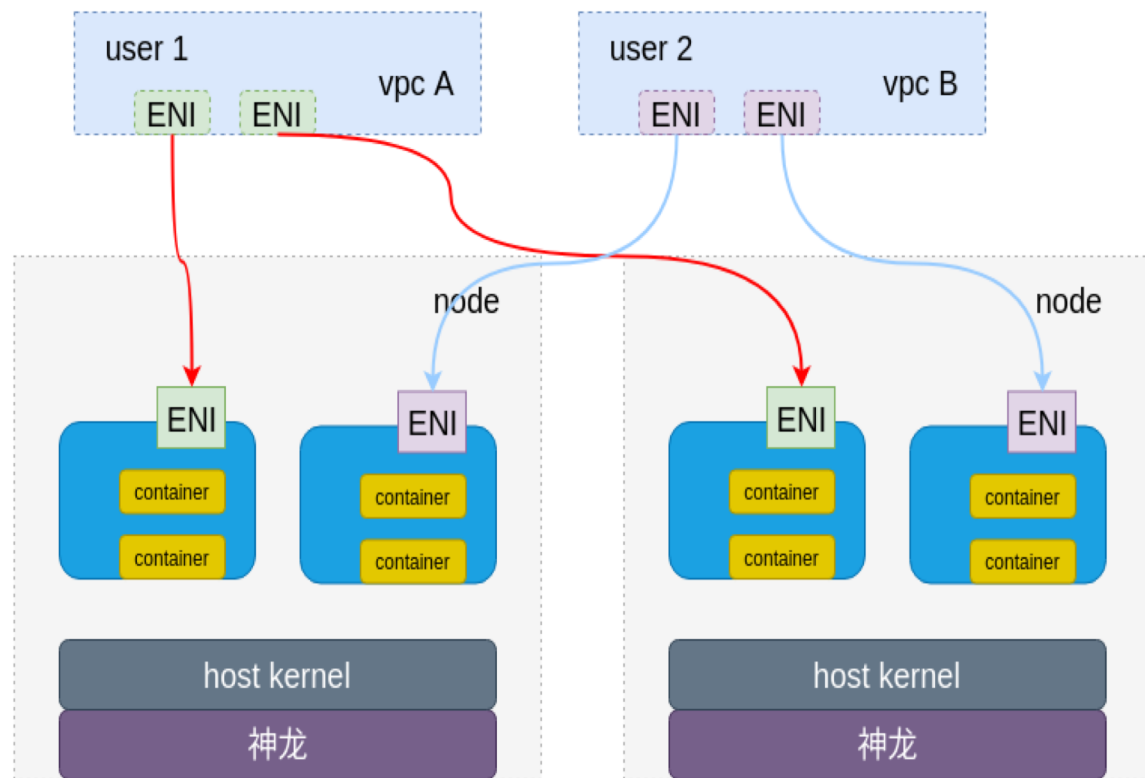


CloudNativeCon



OPEN SOURCE SUMMIT

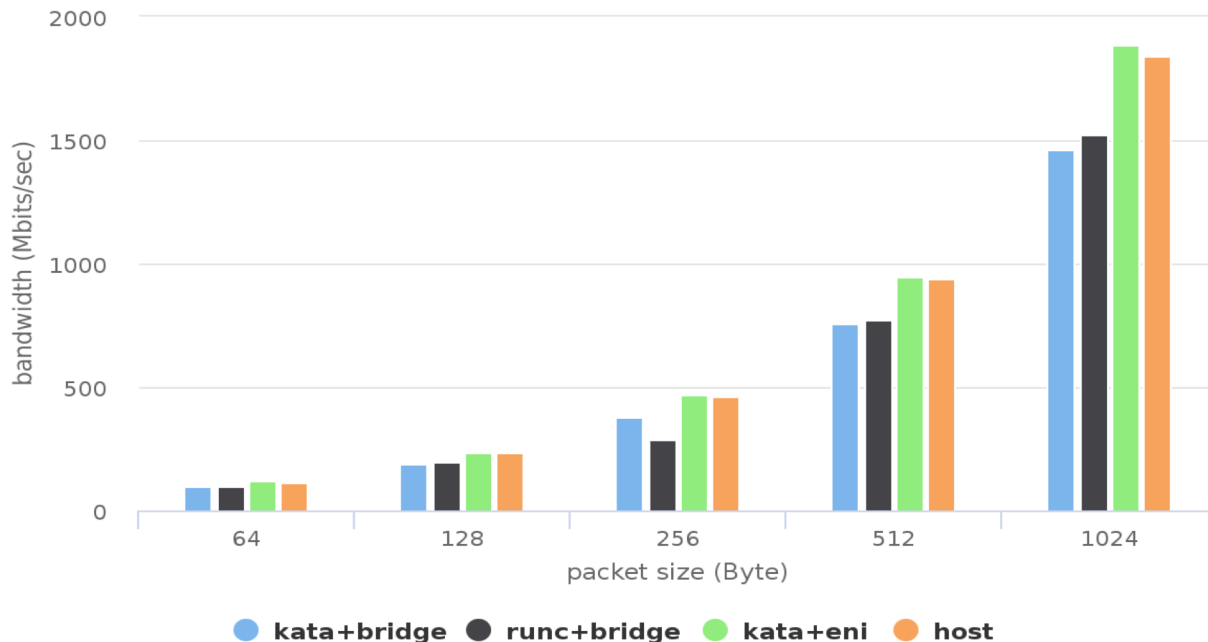
China 2019



网络多租户隔离

- 不同vpc的网络二层隔离
- 同vpc内不同云产品网络互通

Kata/RunC网络性能对比



Kata 安全容器 - IO优化



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

9pfs上生产的问题：

- io性能差
- qemu hang住

2种优化手段：

- qcow2
- devicemapper，性能好，>4.19内核

IO优化 – qcow2方案



KubeCon

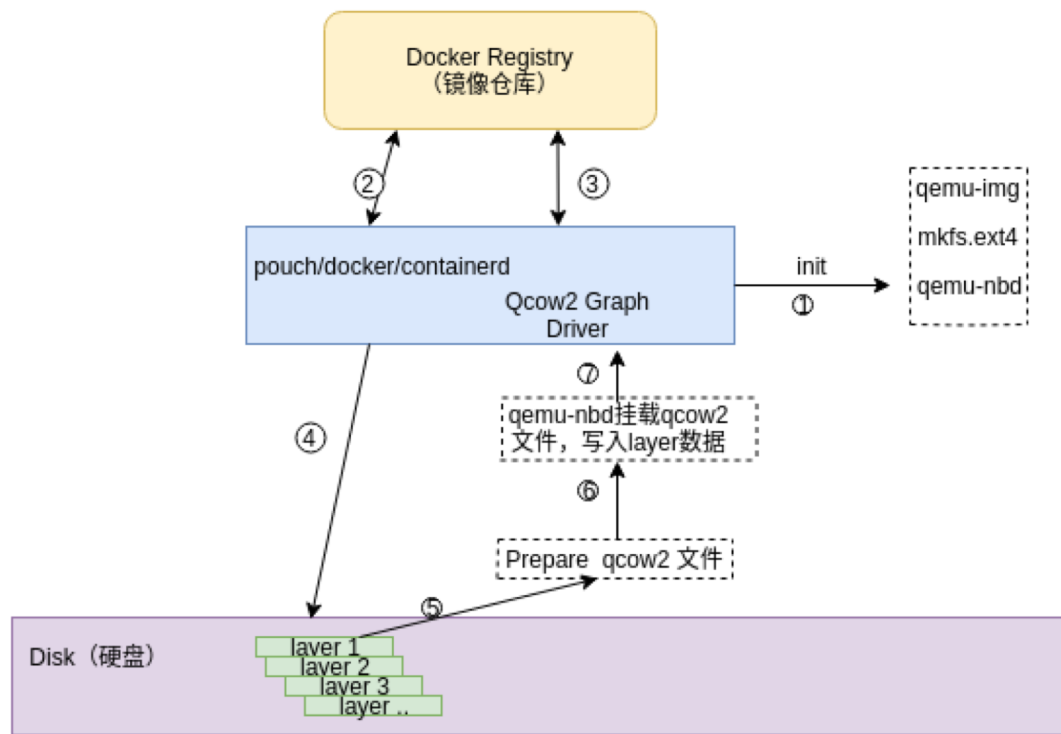


CloudNativeCon



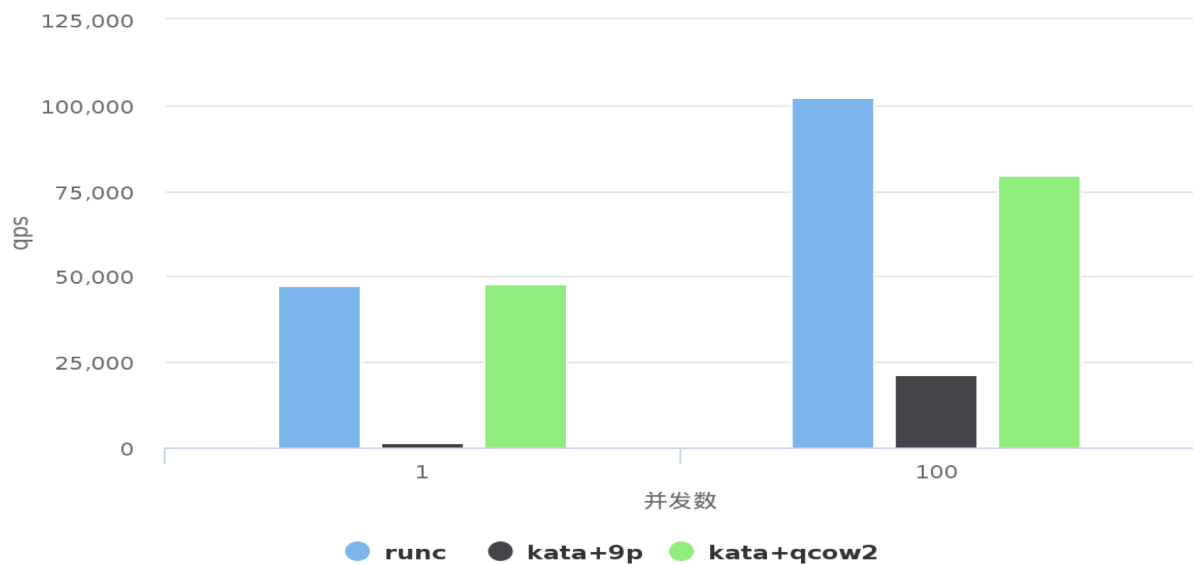
OPEN SOURCE SUMMIT

China 2019



qcow2 graphdriver 设计

Nginx性能测试对比



iTushuo.com

9p和qcow2 存储的测试对比

Kata 安全容器 – 监控方案



KubeCon

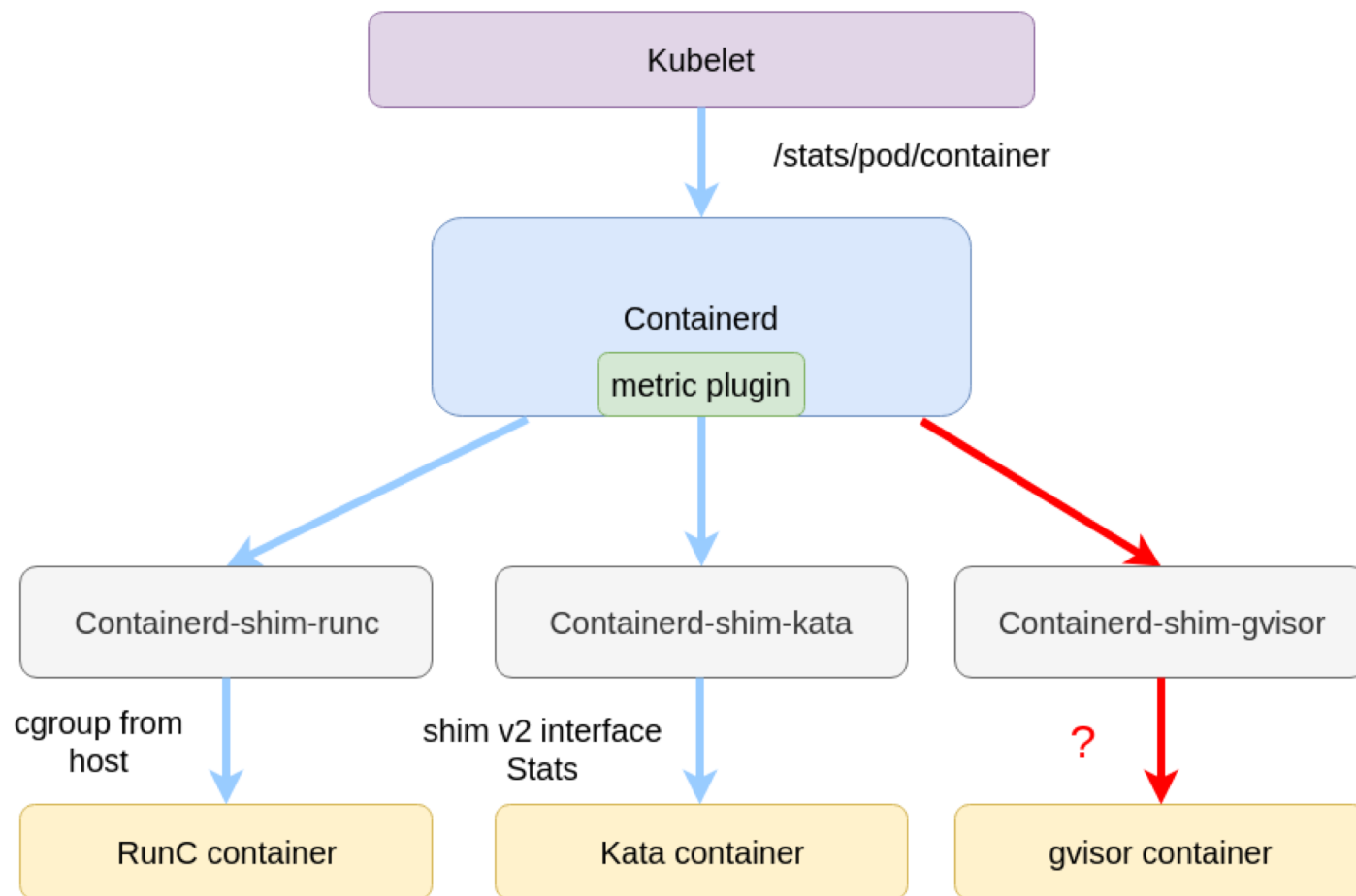


CloudNativeCon



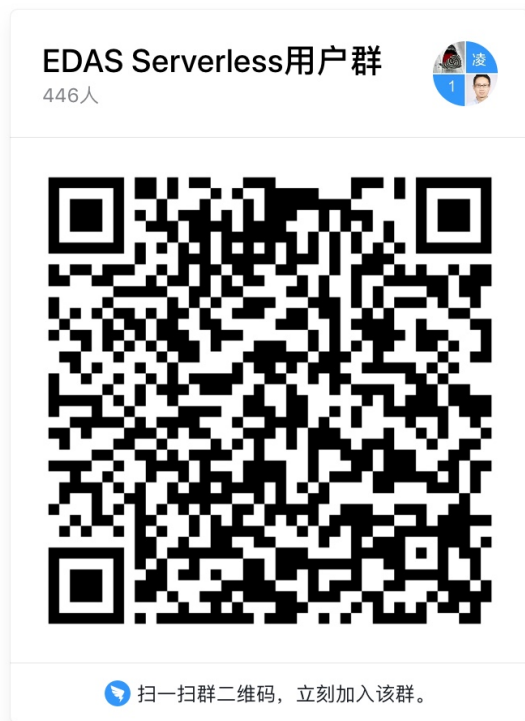
OPEN SOURCE SUMMIT

China 2019



适用于多运行时的监控框架

阿里云 Serverless App Engine



即将推出：ACK 安全容器

结尾



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

Thanks