基于Kubernetes构建企业级Serverless Container平台的探索与实践

王泽锋 kevin-wangzefeng

华为云K8S开源负责人

王泽锋 @kevin-wangzefeng

- 华为云K8S开源负责人
- Kubernetes 社区Maintainer
- 2013年起参与华为PaaS平台设计开发，专注于 PaaS 产品和容器开源社区
- 目前负责华为云Kubernetes开源团队在社区整体的贡献

Kubernetes在华为云的历程

2013

华为PaaS项目启动

基于CloudFoundry构建PaaS平台

2014

华为PaaS项目二期(FusionStage)

切换至Kubernetes平台，并大力投入K8S与CNCF

2016

华为云容器引擎服务发布

国内首家基于Kubernetes的公有云容器服务，提供企业级保障

2018

华为云容器实例服务发布

全球首家基于Kubernetes的公有云Serverless容器服务，容器免运维、按需使用

容器的三大好处， 为应用而生

资源隔离与利用率提升

秒级弹性

环境一致性，简化交付

容器的三大好处， 为应用而生

资源隔离与利用率提升

秒级弹性

环境一致性，简化交付

Kubernetes的使用形式

私有云自己部署 Kubernetes

优点

- DIY的乐趣/成就感

  也可能是苦难

- 全套私有，无隐私顾虑

  数据、请求都在本地

- 资源规划、安装部署、升级

Kubernetes的常见使用形态

私有云自己部署 Kubernetes

优点

- DIY的乐趣/成就感

  也可能是苦难

- 全套私有，无隐私顾虑

  数据、请求都在本地

- 资源规划、安装部署、升级

缺点

- 网络选型、存储选型
- 100% 运维成本
- 一次性、阶段性资源成本
- 集群规模受限于底层资源
- 资源利用率有限

公有云半托管Kubernetes专属集群

优点

- 独占集群

  用户间无干扰

- 现成的集群配置最佳实践
- 推荐的升级时机

  及时跟进社区新版本

- 与云平台共享运维成本

公有云半托管Kubernetes专属集群

优点

- 独占集群

  用户间无干扰

- 现成的集群配置最佳实践
- 推荐的升级时机

  及时跟进社区新版本

- 与云平台共享运维成本

缺点

- 价格门槛 —— Flavor 单价 * N
- 用户为资源利用率买单
- 分钟级的VM弹性阔容

另一个分支：容器实例服务

业界的容器实例服务

优点明显

- 免运维，开箱即用
- 细粒度资源定价
- 秒级扩缩，秒级计费
- ……

业界的容器实例服务

优点明显

- 免运维，开箱即用
- 细粒度资源定价
- 秒级扩缩，秒级计费
- ……

然而

- 私有API
- 不兼容K8S
- vendor lock-in
- ……

业界的容器实例服务

优点明显

- 免运维，开箱即用
- 细粒度资源定价
- 秒级扩缩，秒级计费
- ……

然而

- 私有API
- 不兼容K8S
- ven[illegible]ck-in
- ……

不是Kubernetes

业界的容器实例服务

优点明显

- 免运维，开箱即用
- 细粒度资源定价
- 秒级扩缩，秒级计费
- ……

然而

- 私有API
- 不兼容K8S
- ver…ck-in
- ……

不是Kubernetes

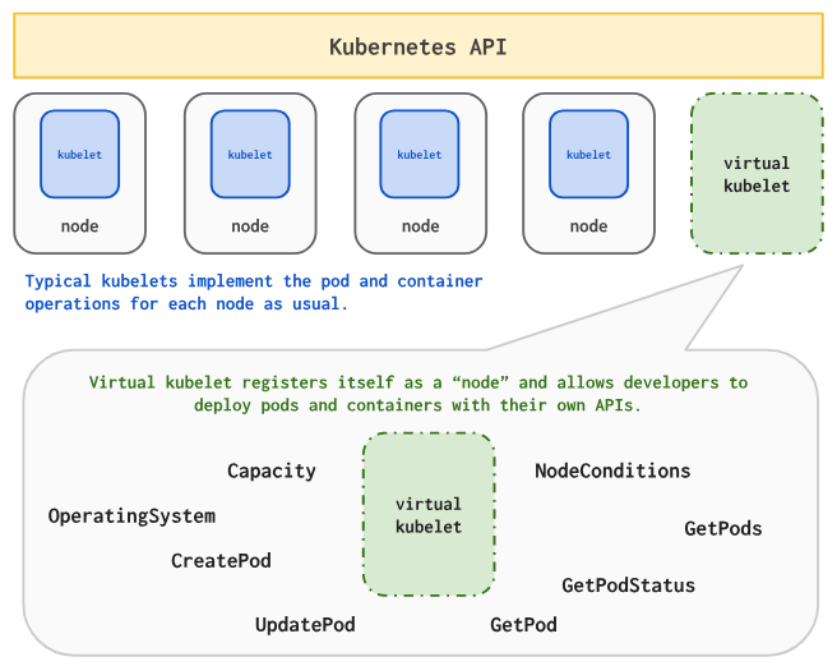
典型代表

Azure ACI

AWS Fargate

Container Instance → **Serverless Container**

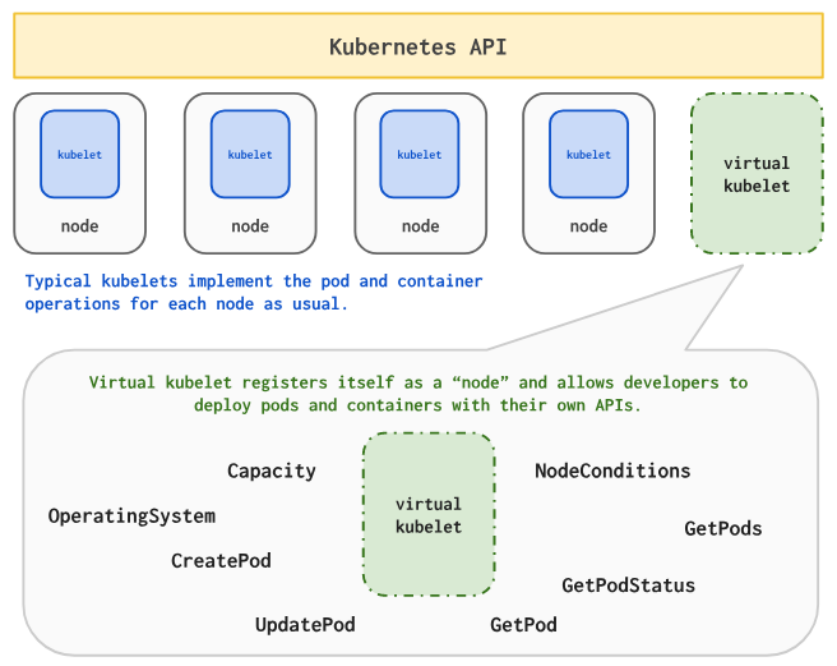
业界容器实例服务的兼容方案



业界容器实例服务的兼容方案

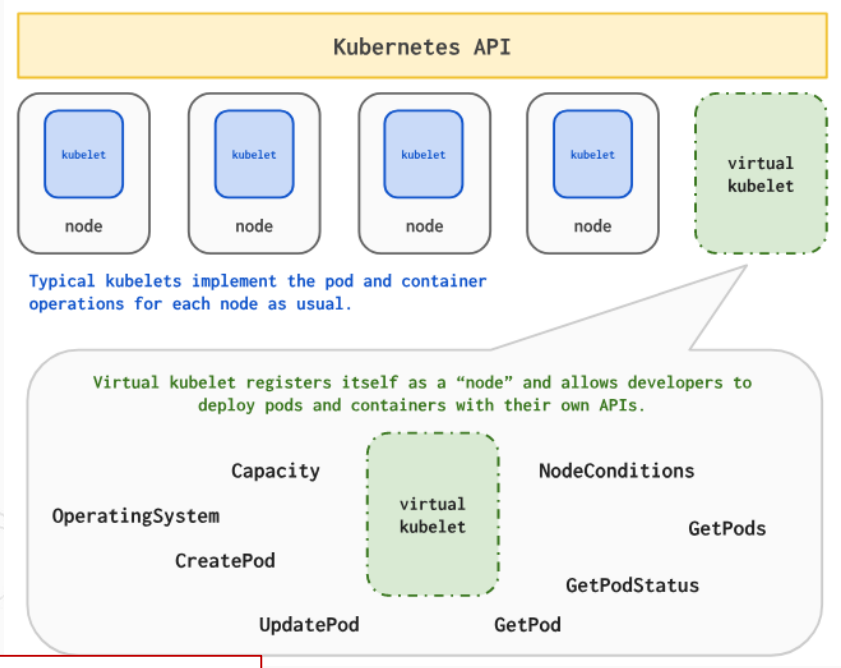
Virtual Kubelet

- 接管的pod本质上未受k8s调度
- 数据面方案不完整
  - 难以确定的Kube-proxy位置
  - 尚不明朗的容器存储



业界容器实例服务的兼容方案

- 接管的pod本质上未受k8s调度
- 数据面方案不完整
  - 难以确定的Kube-proxy位置
  - 尚不明朗的容器存储



Virtual-kubelet的适用场景不在于此

如果基于K8S多租构建Serverless Container?

如果基于K8S多租构建Serverless Container

优势

- 支持k8s原生API和命令行
- 低价格门槛

  细粒度资源、秒级计费

  平台为资源利用率买单
- 用户零运维，开箱即用

如果基于K8S多租构建Serverless Container

优势

- 支持k8s原生API和命令行
- 低价格门槛

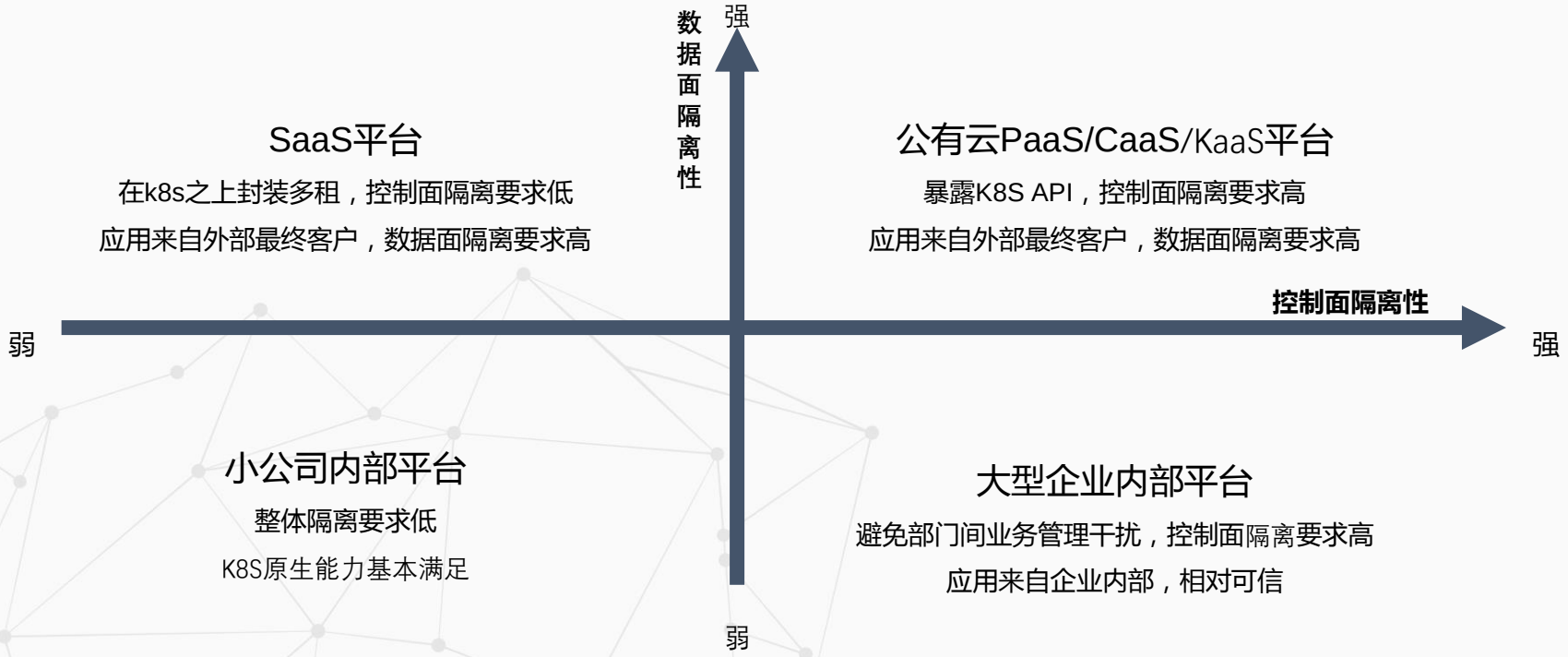
  细粒度资源、秒级计费

  平台为资源利用率买单
- 用户零运维，开箱即用

主要挑战：

- K8S只支持软多租

Kubernetes多租形态的选择



如果基于K8S多租构建Serverless Container

优势

- 支持k8s原生API和命令行
- 低价格门槛

  细粒度资源、秒级计费

  平台为资源利用率买单
- 用户零运维，开箱即用

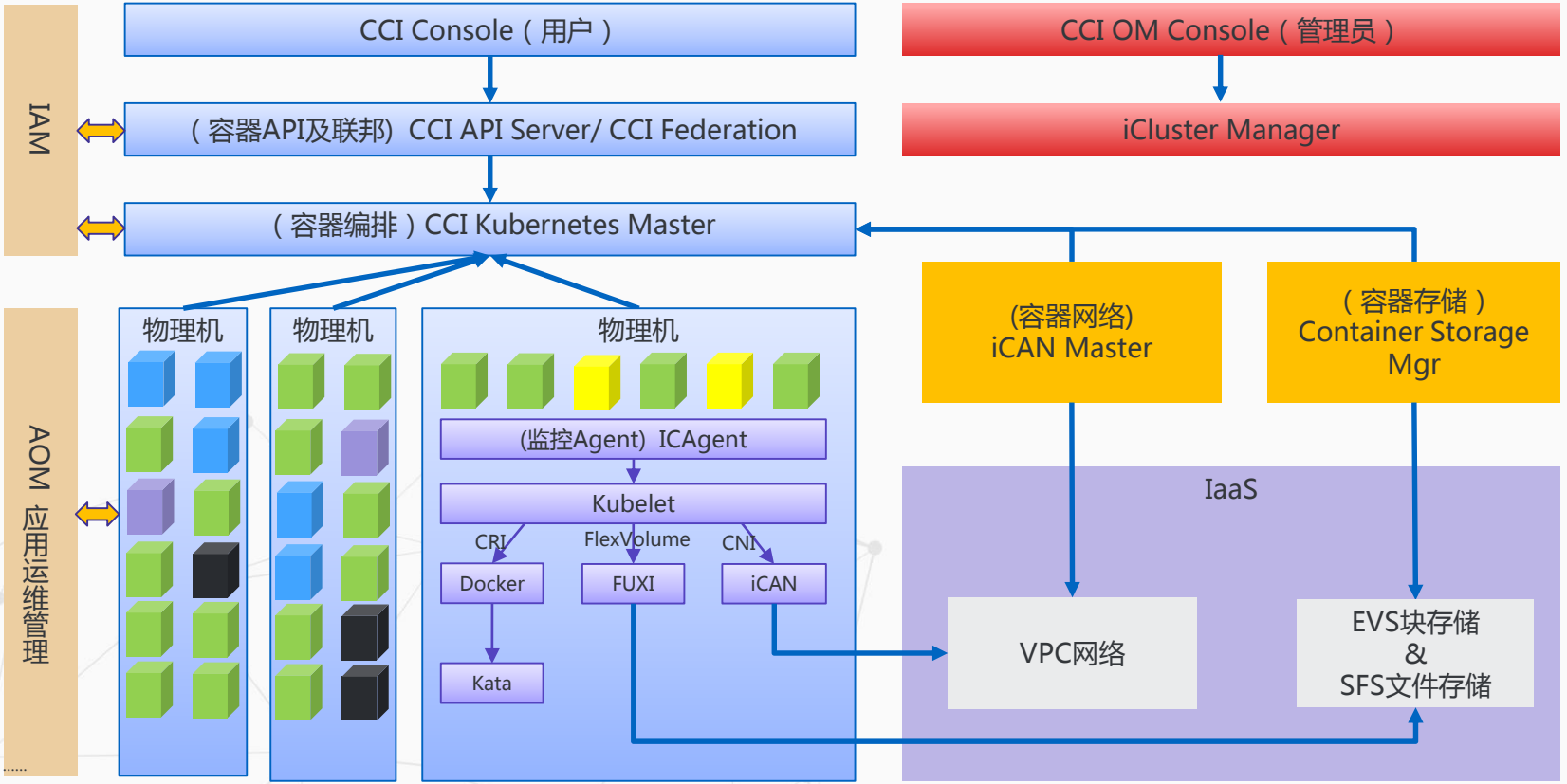
主要挑战：

- K8S只支持软多租
- 租户概念和访问控制

  Control plan fairness
- 节点隔离和Runtime安全
- 网络隔离

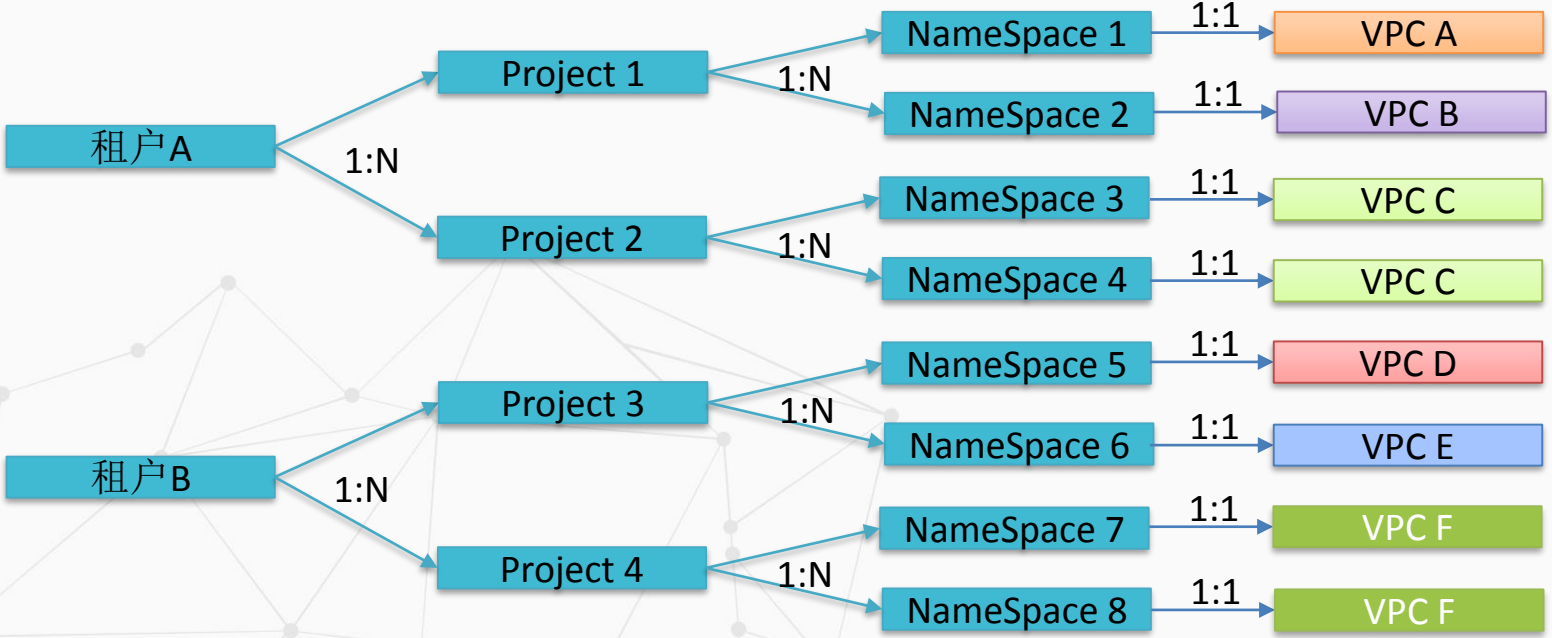
华为云的探索与实践

以Kubernetes为基础打造CCI容器实例服务

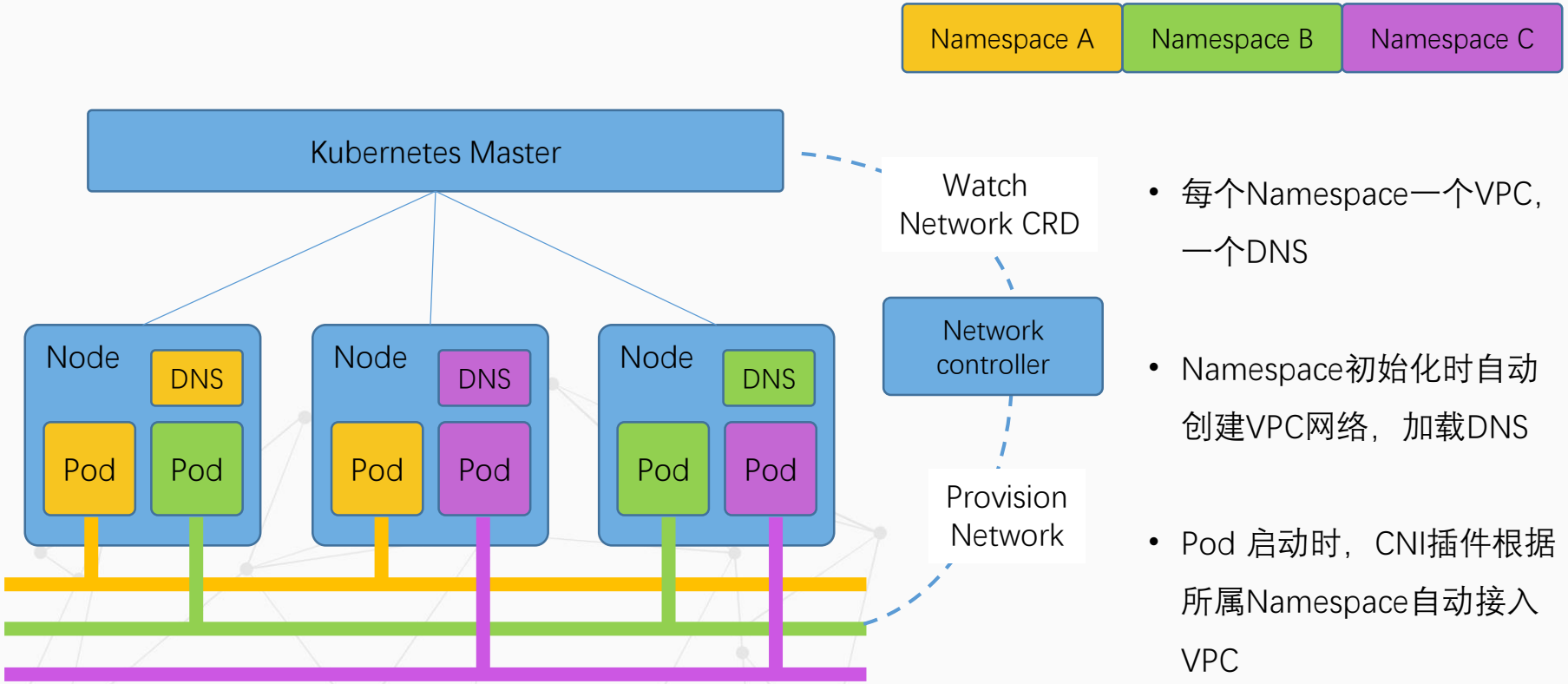


CCI中租户概念的封装

CCI对接IAM支持多租户能力，支持单租户下有多个Project，每个Project下可以建立多个Kubernetes Namespace，每个Namespace当前可以独立关联IaaS VPC.



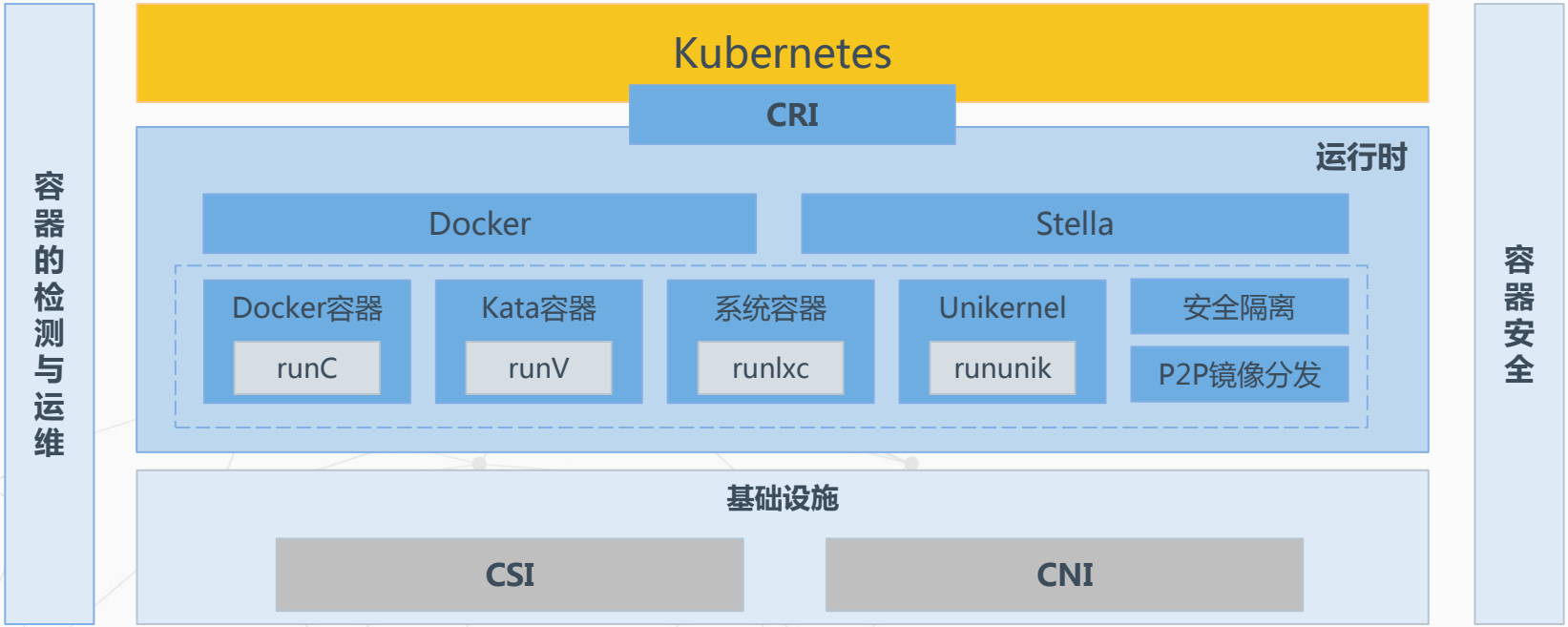
多租场景的网络隔离



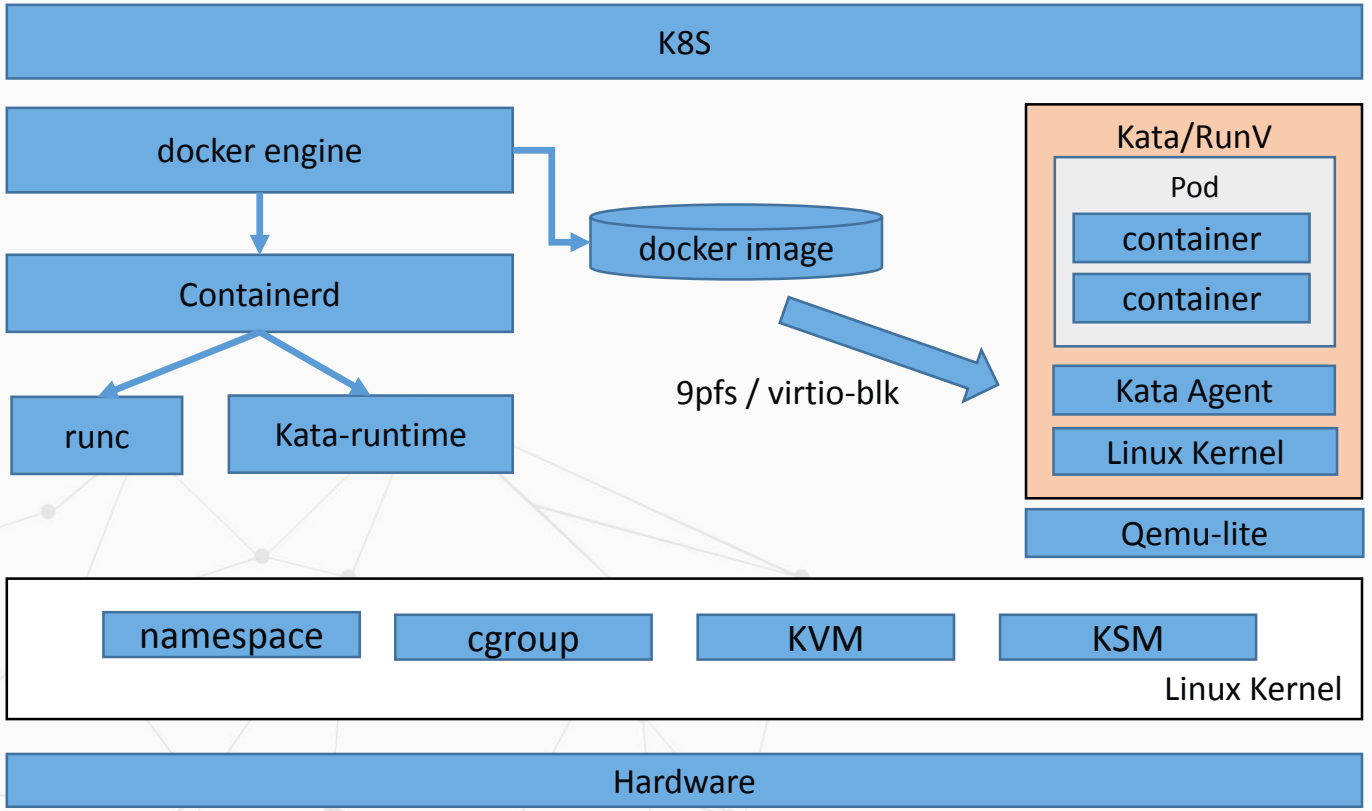
- 每个Namespace一个VPC，一个DNS
- Namespace初始化时自动创建VPC网络，加载DNS
- Pod 启动时，CNI插件根据所属Namespace自动接入VPC

iSula 统一容器引擎

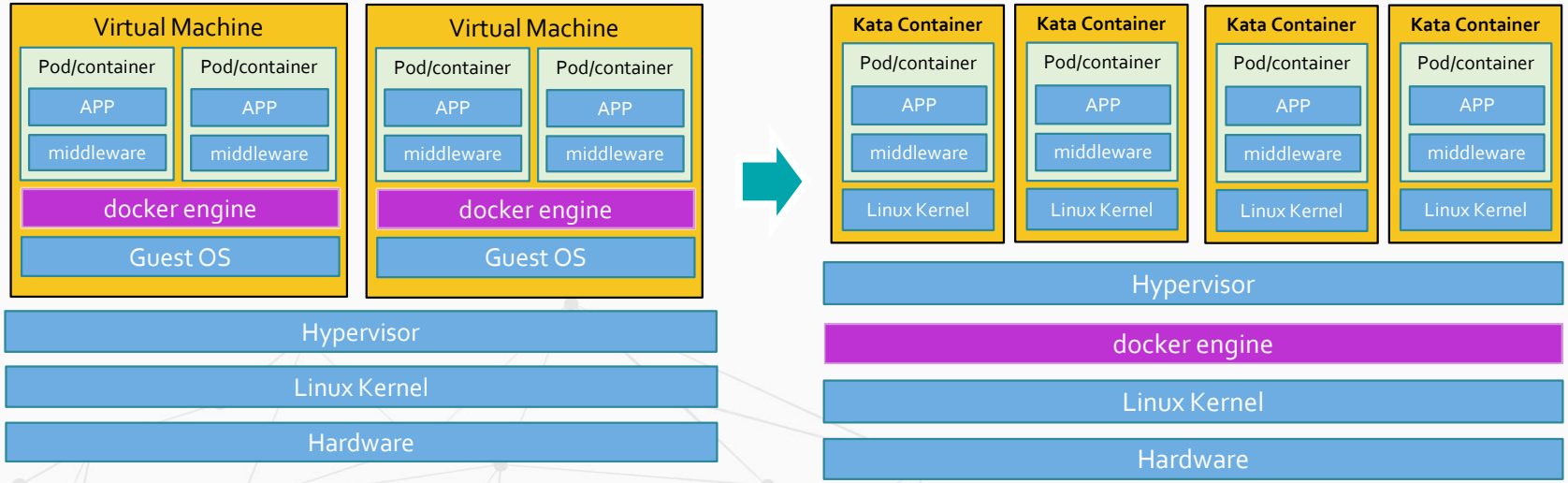
多运行时，多容器形态，按需使用



华为iSula安全容器



通过Kata容器实现多租户容器强隔离



- 虚拟化层的存在，保障了容器在多租户场景下的安全性。
- 高度裁剪和优化过的KVM、guest OS保证了VM启动时间极短，性能损耗极小。
- 接口层支持对接docker引擎或crio，镜像完全兼容docker镜像，无需修改。完美融入K8S容器生态。

CCI：Serverless Kubernetes，让弹性与成本可以兼得

K8S-Native Serverless Container

- **原生支持Kubernetes API与命令行**
- 无需用户感知K8S集群及物理资源，**设施免运维**
- 提供图形化控制台，端到端完整用户体验

Hypervisor-Based Secure Container

- 原生支持Kata Container，Docker生态兼容
- 内核虚拟化技术，**全面的安全隔离与防护**
- 自有硬件虚拟化加速技术，**更高的安全容器性能**

高性能、异构基础设施

- 异构服务器：X86、ARM服务器
- 异构芯片加速：GPU、FPGA加速芯片
- 华为云高速网络与存储集成：EVS、OBS、VPC、ELB...

https://www.huaweicloud.com/product/cci.html

后续计划

- Tenant API
  - Exposing “root scope” API for Tenants
- Control plan fairness
  - Max inflight API calls
  - Rate limiting
- Network CRD
- Multi-tenancy conformance profile

Q & A

华为云Kubernetes

容器技术公众号

Thank You!

主办方：

协办方：