

# 从开源第一到企业落地 中国银联 Kubernetes 案例分享

肖 勤 | 才云科技



主办方： caicloud 才云



 TensorFlow

协办方： 网易云

# 科技创新打造才云独特技术优势



## Intelligent PaaS

Automatic micro-service management  
Streamlined Devops workflow  
Intelligent monitoring and log analysis  
App orchestration and solution management



## Cluster Management

PaaS + IaaS integration with hardened security and multi-tenancy  
Multi-cluster management and interaction  
Automatic operations  
Flexible networking solutions



## Diverse Workloads Support

Core, complex, stateful workloads in Enterprises  
Data-intensive workloads  
Workloads with diverse scheduling needs

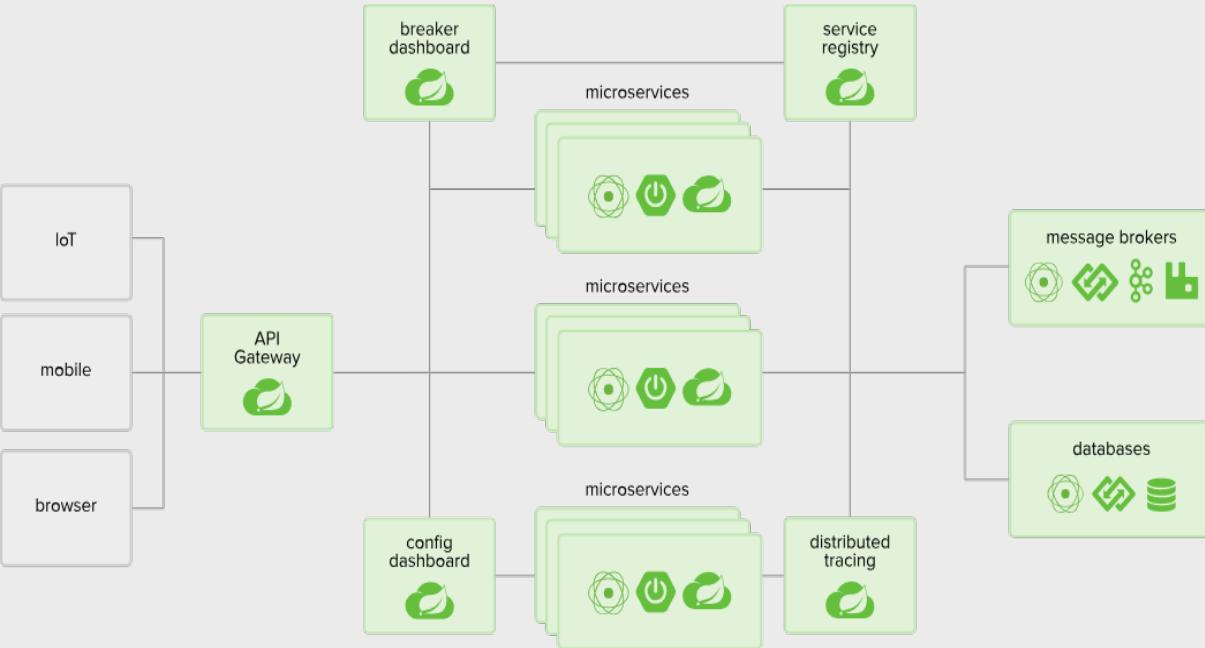


## Machine Learning Stack as a Service

GPU integration with containers and Kubernetes  
Distributed TensorFlow management  
Continuous Machine Learning pipeline

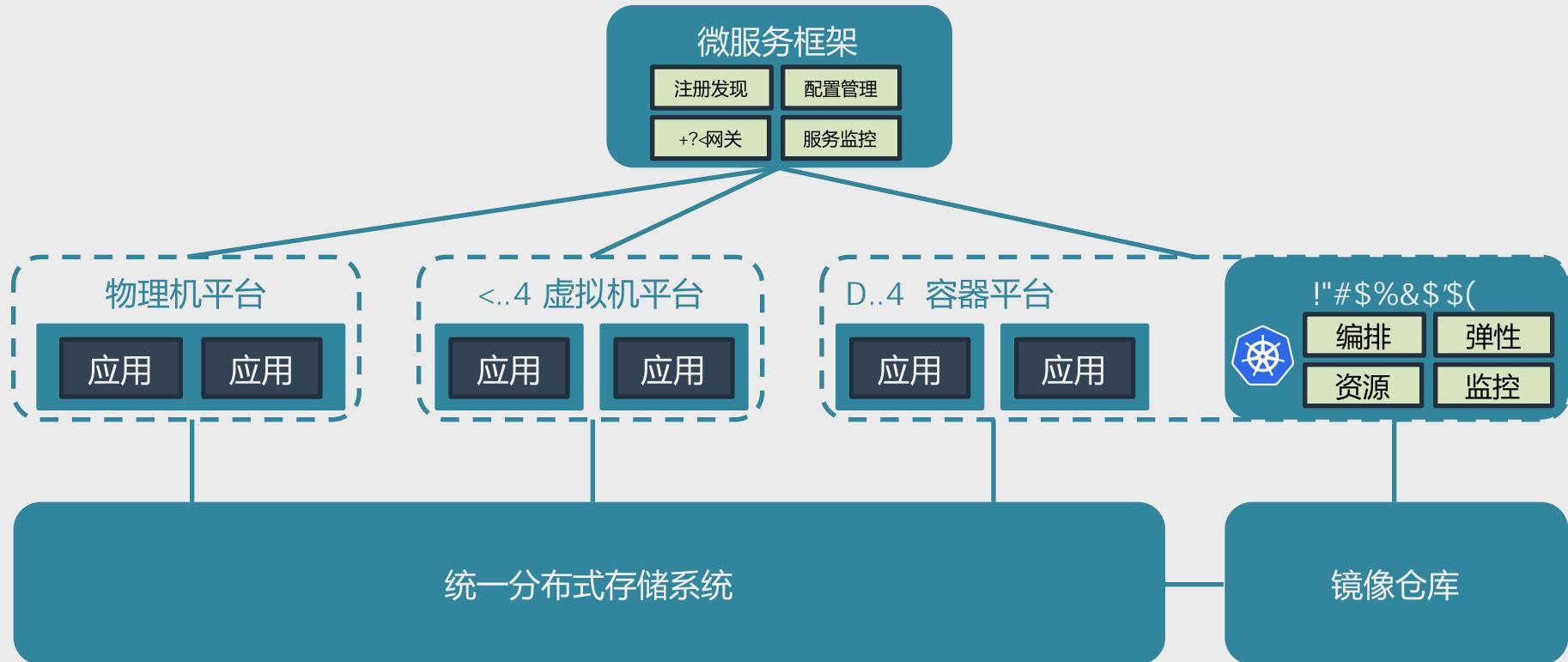
- 开源第一
  - kubernetes/kubernetes 38,918 stars 13,607 forks
  - 第一个毕业的 CNCF 项目
  - 最大的容器社区
  - 越来越多的公有云服务 EKS, GKE, AKS ...
- 企业落地会遇到的问题
  - 平台定位
  - 计算
  - 网络
  - 存储
  - 应用

# 容器云平台与微服务框架同质化功能如何取舍

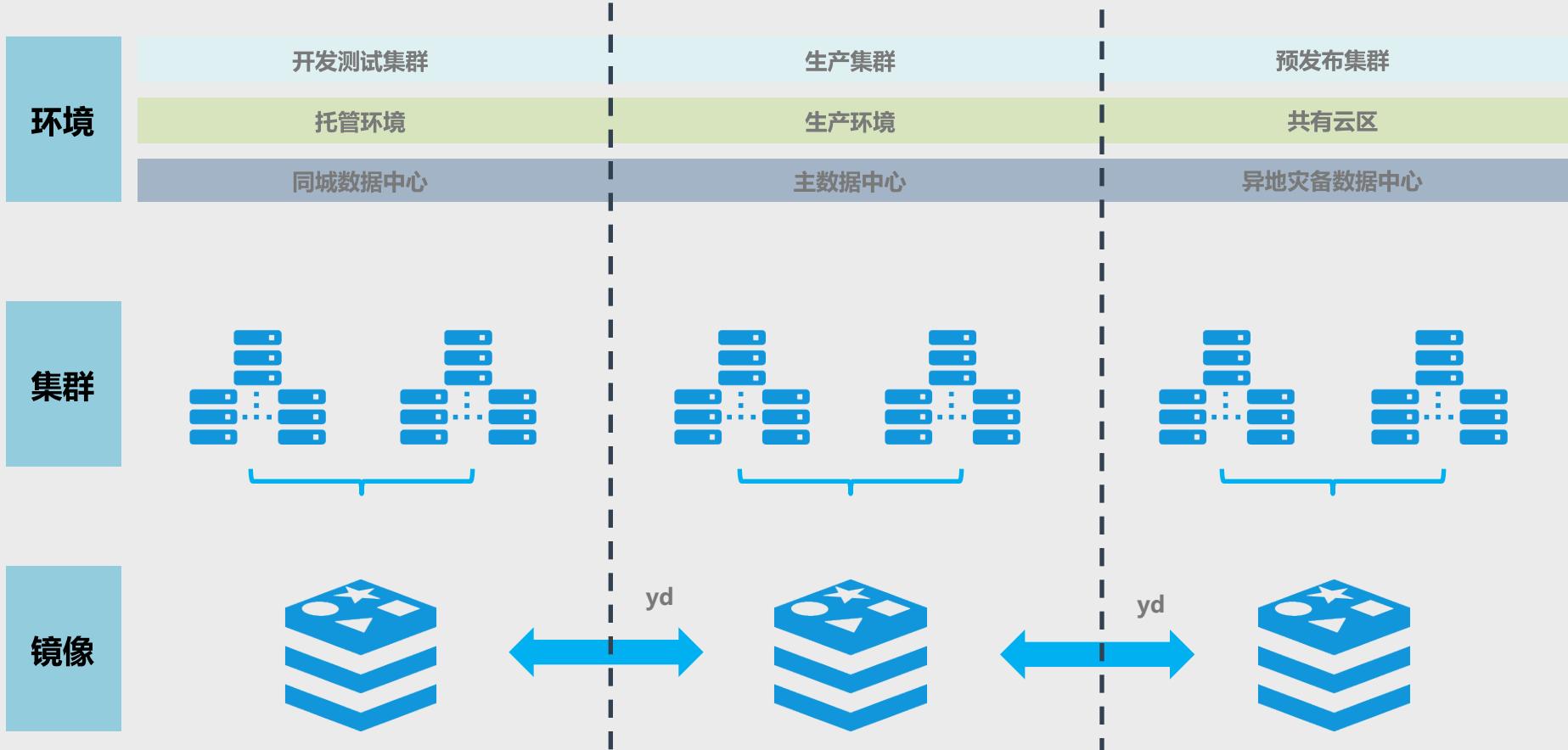


	Spring Cloud	Kubernetes
服务发现	Eureka	CoreDNS
负载均衡	Ribbon	Service
配置管理	Config	Configmap
故障容错	Hystrix	HPA
API gateway	Zuul	Ingress
链路追踪	Sleuth	Service Mesh
定时任务	Spring Batch	Cron Job

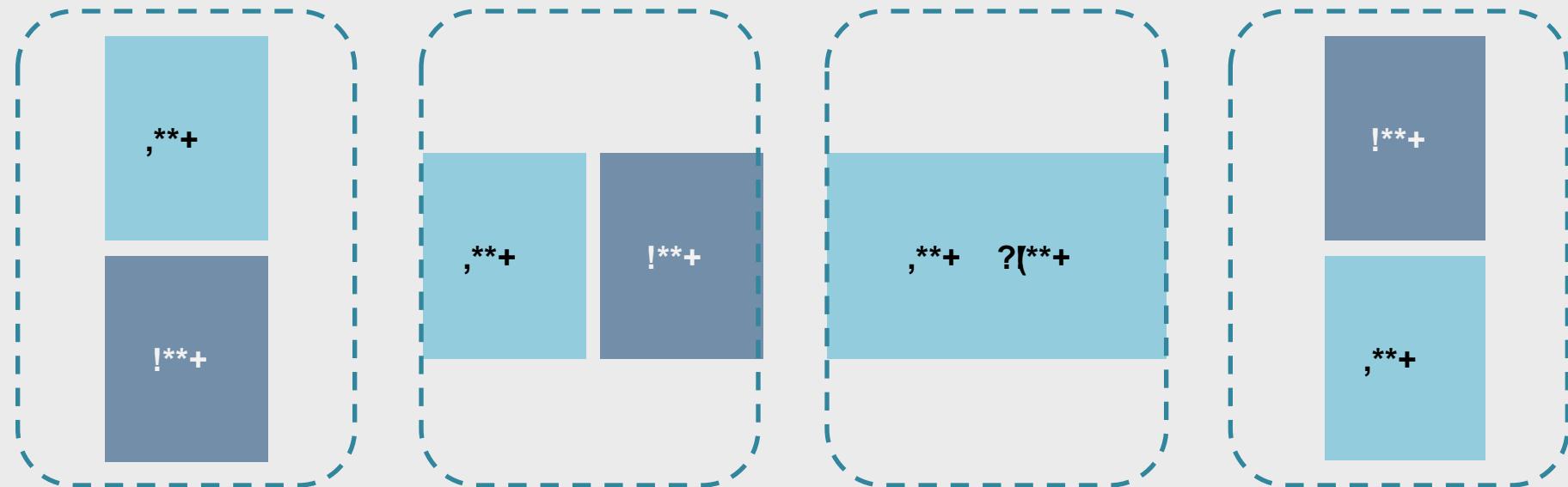
# 微服务分步迁移问题



# 容器云平台与多环境如何规划和适配



# ,\*\*+ S !\*\*+ 融合 > 计算



,&

9/>'

/()

"&6\$%

# 容器化+S!融合>计算



## 容器平台与传统平台集成：

- 与租户共享
- 认证鉴权一体化
- 管理界面统一
- 底层资源完全打通



## 应用上云：

- 前端应用：人机智能验证平台，银联钱包应用
- 核心应用：人机智能验证平台，银联钱包应用



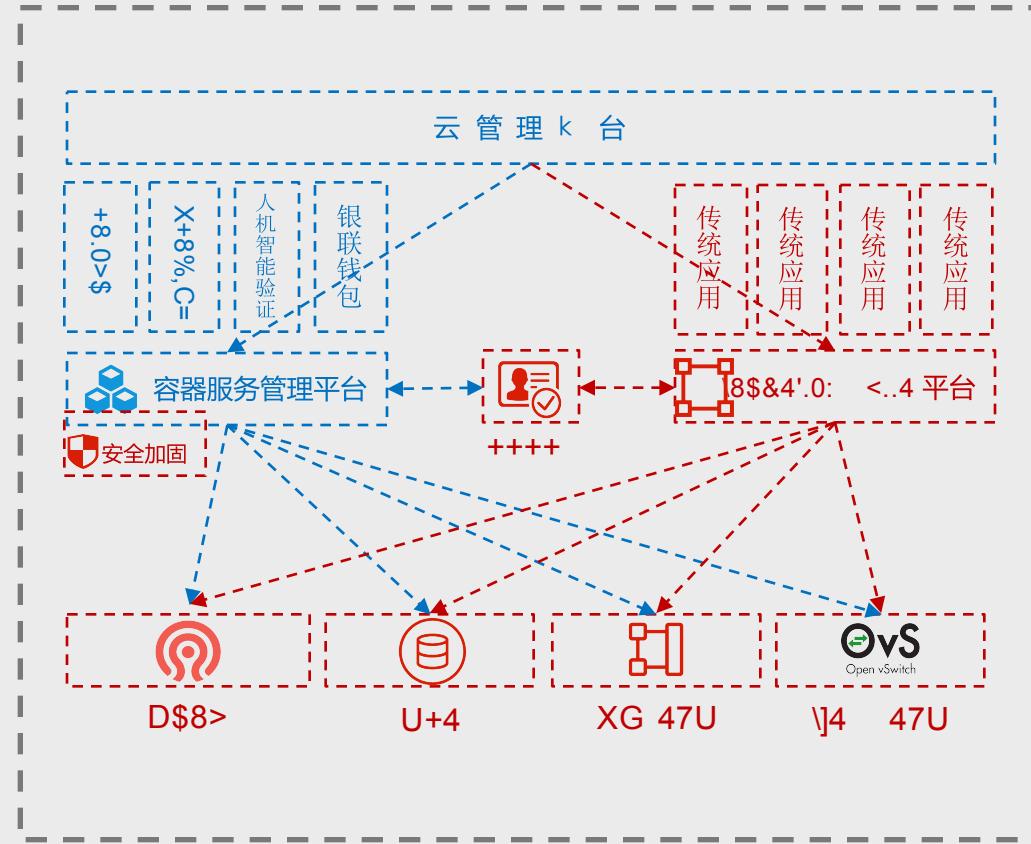
认证鉴权：与银联内部认证鉴权系统无缝整合

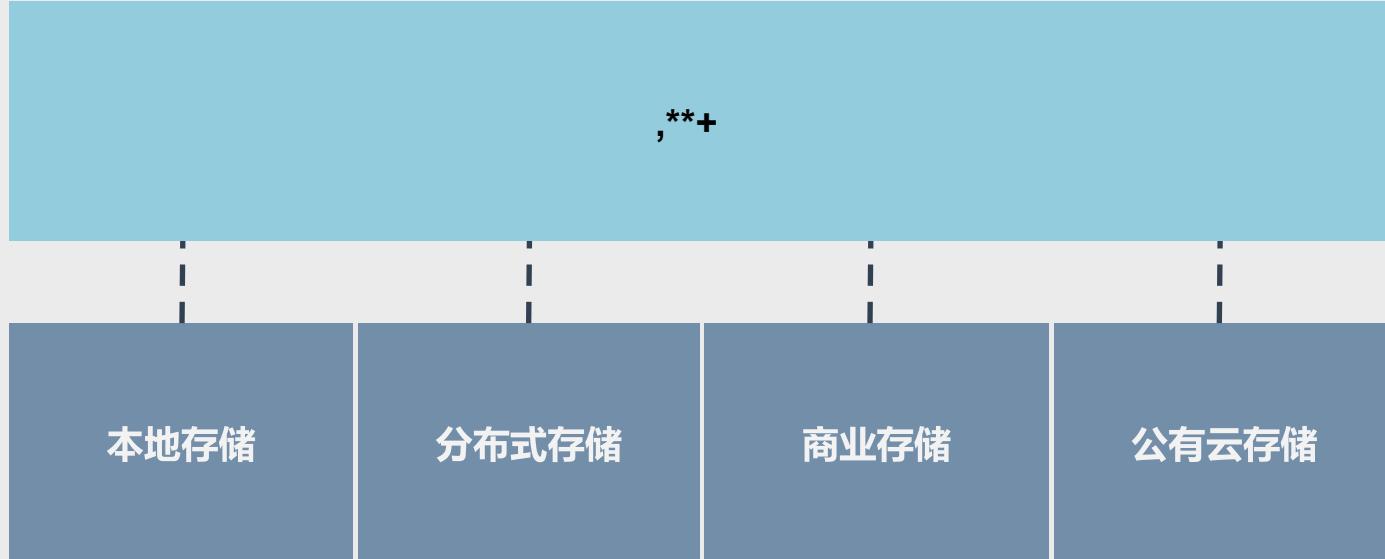


云管平台：管理平面与云资源管理平台整合



安全加固：符合银监会及银联内部安全策略





# CaaS与IaaS融合 - 存储

**存储服务**

- 节点
- 集群
- 存储**
- 存储服务
- 存储方案
- 网络
- 负载均衡器
- 运维中心
- 日志
- 日志
- 事件
- 监控
- 报警
- 管理中心

**存储方案**

- 资源中心
- 节点
- 集群
- 存储**
- 存储服务
- 存储方案**
- 网络
- 负载均衡器
- 运维中心
- 日志
- 日志
- 事件
- 监控
- 报警
- 管理中心

**租户管理**

名称: unionpay

创建时间: 2018-02-11

描述: 银联生产用户

**user-cluster 集群的数据卷**

可选择的存储方案: default-trident-storageclass, test

存储方案	可创建数据卷数量	可创建数据卷总容量
default-trident-storageclass	100	200 GB
test	100	100 GB

已分配

存储方案	可创建数据卷数量	可创建数据卷总容量
default-trident-storageclass	100	200 GB
test	100	100 GB

4 层协议端口

417 GiB  
2.09 TiB

取消 确定

**Kubernetes Cluster**

The diagram illustrates the storage integration between CaaS and IaaS. It shows the flow of data from the Kubernetes Master (K8S Apiserver, PV Controller) to the Node (Kubelet, NFS/RBD Plugin), through the External Provisioner (volumeController, classController, claimController), and finally to various storage providers (NetApp NAS, ONTAP, Ceph, RBD Network Disk).

Key components and interactions:

- Kubernetes Cluster:** Contains K8S Apiserver, PV Controller, and Node.
- External Provisioner:** Manages storage classes and volumes, interacting with the Master and Nodes.
- Nodes:** Contain Kubelet and specific storage plugins (NFS or RBD).
- Storage Providers:** NetApp NAS (ONTAP), Ceph, and RBD Network Disk.
- Flow:**
  - Master creates/delete PV (pv.Spec.NFS = nfsSource).
  - External Provisioner lists & watches PV, classStorage, and pod, pv, pvc.
  - External Provisioner creates/delete PV and volume.
  - Node lists & watches pod, pv, pvc.
  - Node attaches/detaches disk to node.
  - Node mounts/unmounts volume described by PV.

Annotations:

- Only reflects the creation flow.
- when volume.Status.Phase == VolumeReleased or VolumeBound delete k8s pv
- Mount/Unmount volume described by pv
- Attach/Detach disk to node
- Mount/Unmount disk described by pv

## 存储方案 1



AWS EBS

Volume Type : ReadOnlyMany

## 存储方案 2



GlusterFS-A

Cluster ID : 13579...

Volume Type : ReadWriteOnce

## 存储方案 3



CephRBD00

3FFC : SSD GFFC

Volume Type : ReadWriteOnce

## 存储方案 4



NFS01

Volume Type : ReadWriteOnce

## c 后 端 d 储 服 务



GCE



AWS



Azure



GlusterFS



Ceph



Cinder



商业存储



iSCSI



FC-SAN



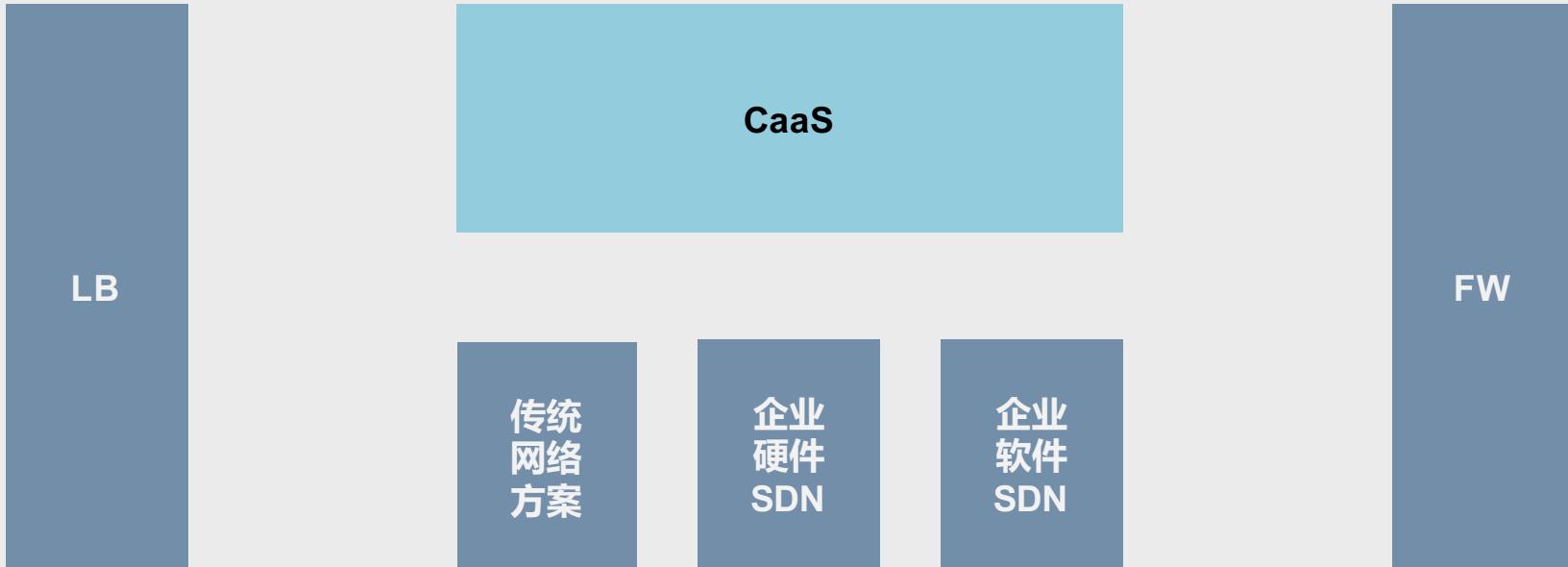
NFS

- 存储服务支持多样存储后端
- 存储方案定义详细存储需求

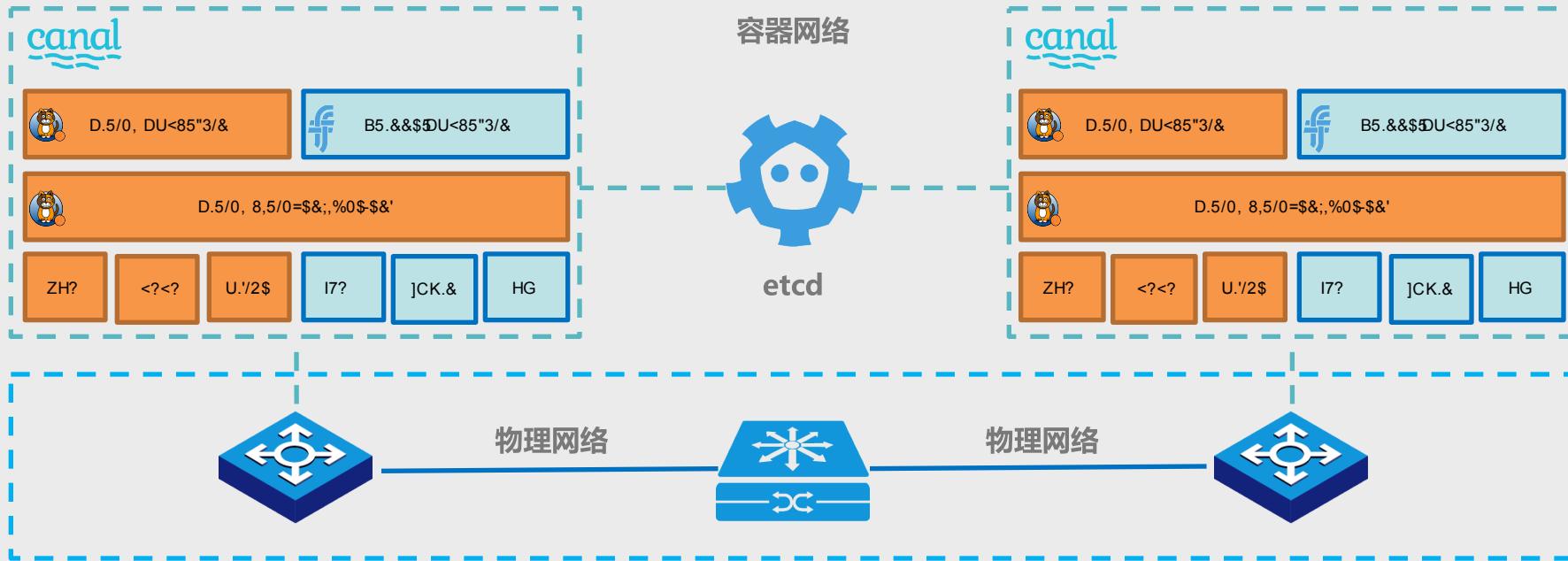
- 支持租户存储容量配额管理
- 支持本地存储Local storage

- StorageClass
- PV+PVC

## 网络策略控制



# !\*\*+ S !\*\*+ 融合 > 网络 ?对底层网络透明



- 多种网络方案集群粒度可选
- 底层合法物理网络形态无感
- 应用间网络访问控制策略支持
- Flannel+Calico多种网络方案

# CaaS与IaaS融合 – 网络 | 与底层网络深度集成 | L2L3

中国银联 China UnionPay | 应用分区

使用指南 | 租户 : test-tenant | docker

新增分区

资源中心

存储

数据卷

应用中心

应用分区

应用

编排

负载均衡

配置管理

镜像仓库

持续集成

运维中心

日志

监控

报警

管理中心

分区名称

所属集群

集群资源

CPU 配额

内存配额

I3policy\_id

podCIDR

serviceCIDR

新增分区

分区名称:

所属集群:

集群资源

CPU 请求 2 / 2 Core

CPU 上限 6 / 10 Core

内存请求 4 / 4 GiB

内存上限 8 / 8 GiB

CPU 配额

请求:  Core

上限:  Core

内存配额

请求:  GiB

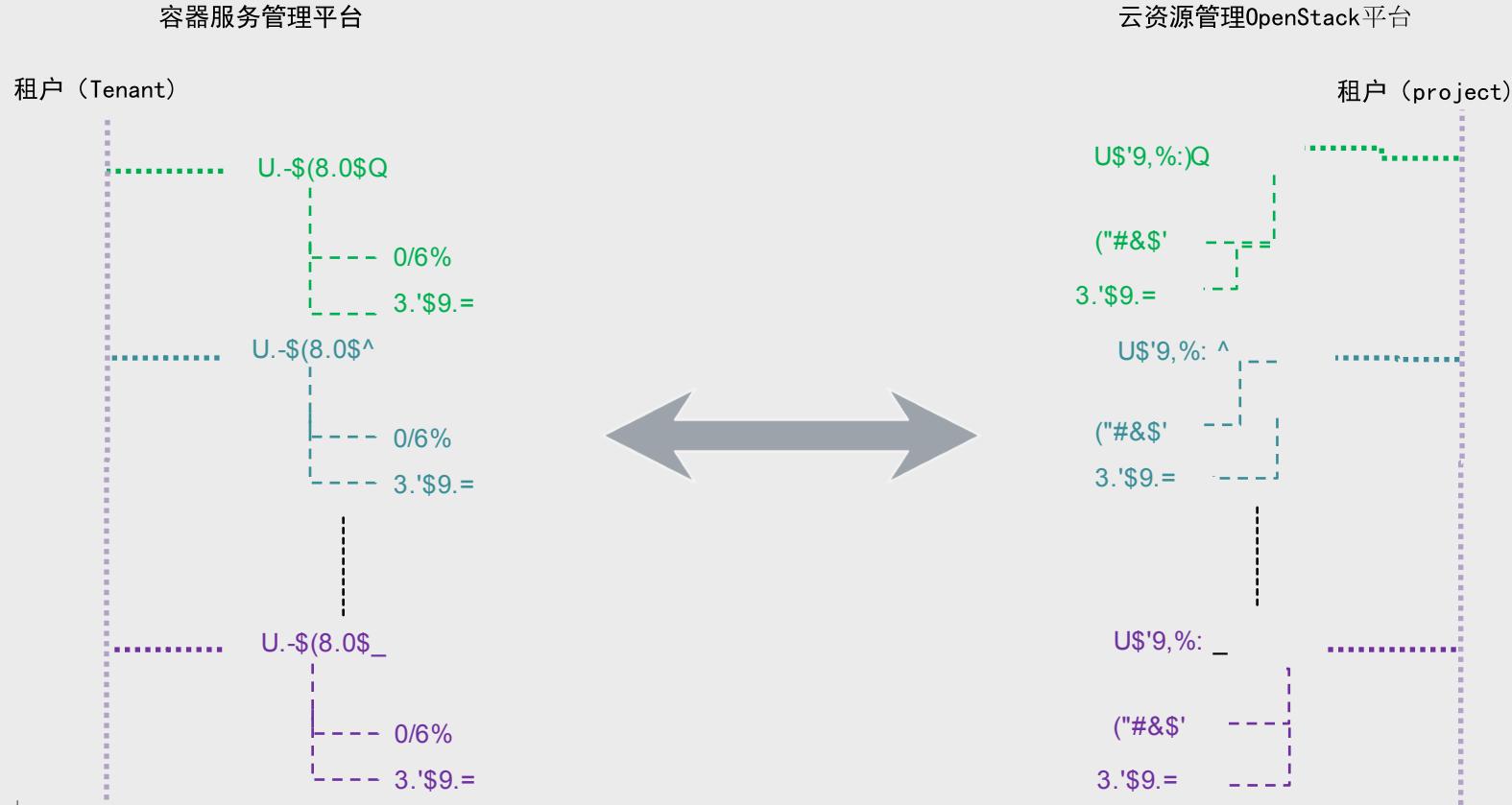
上限:  GiB

I3policy\_id:

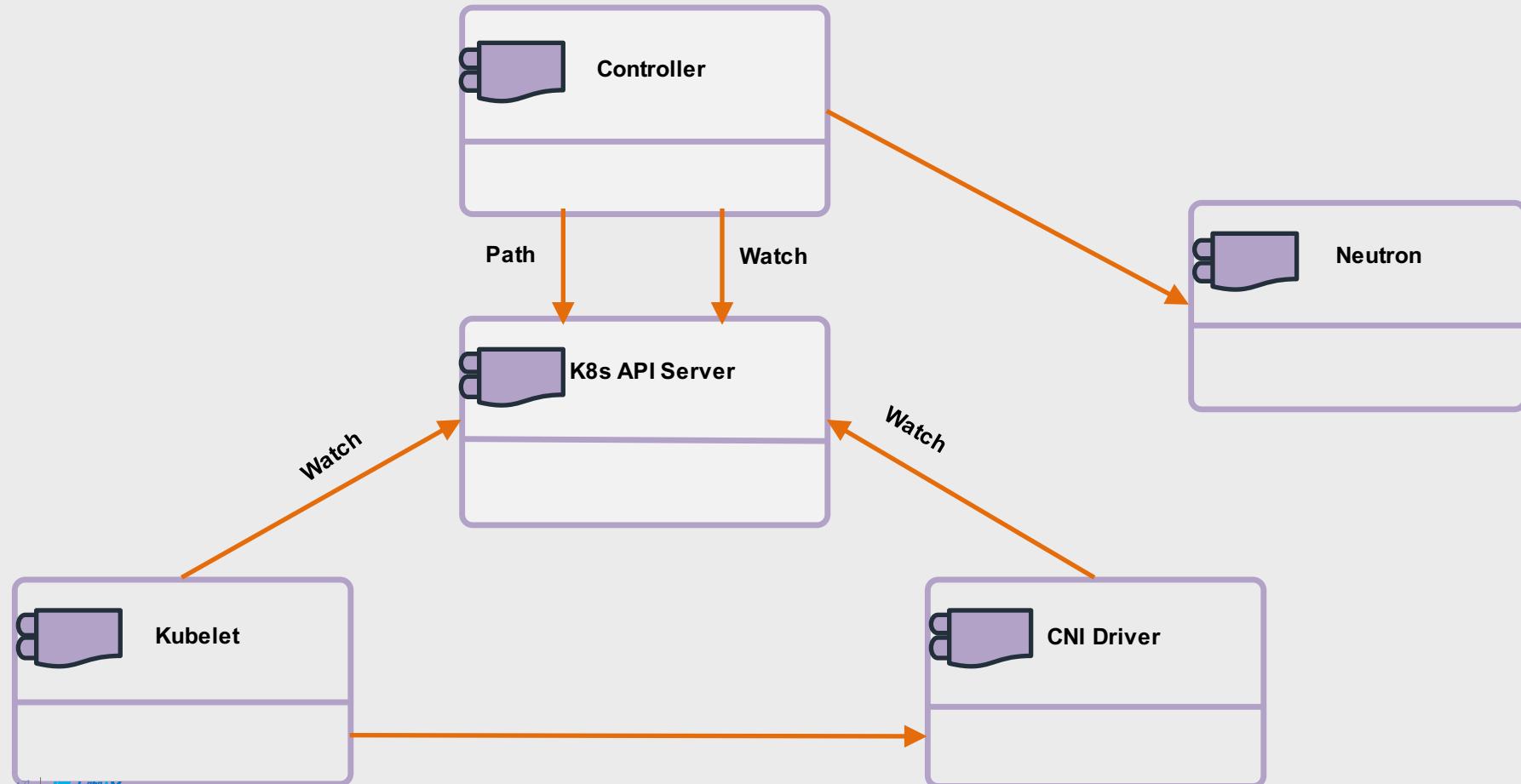
podCIDR:

serviceCIDR:

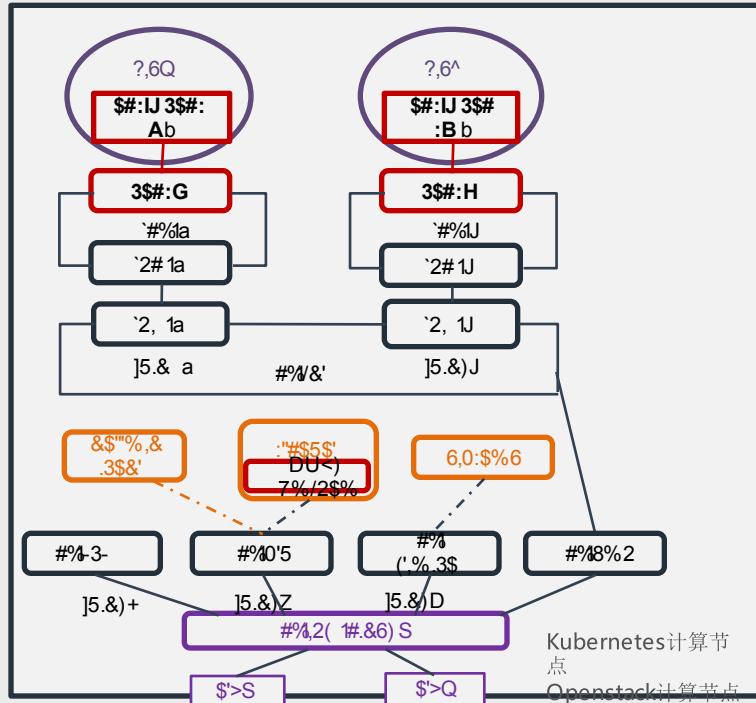
# 容器服务管理平台 > 网络 ?与底层网络深度集成 ?;D;E



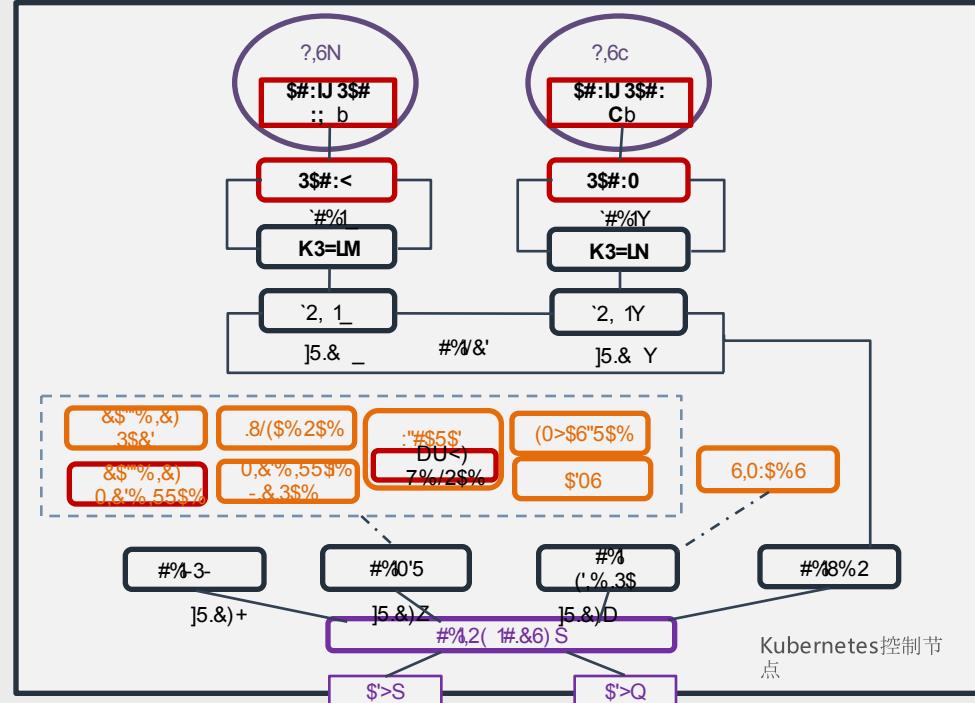
# CaaS与IaaS融合 – 网络 | 与底层网络深度集成 | L2L3



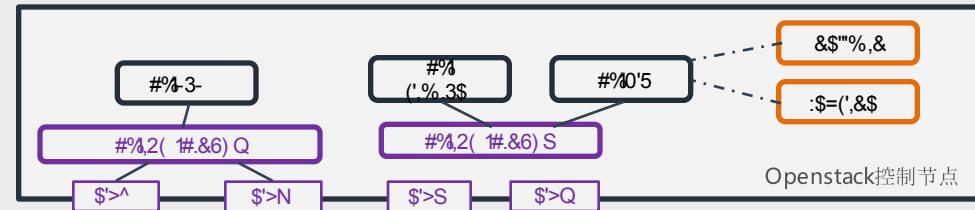
# ，\*\*+ S !\*\*+ 融合 > 网络 ?与底层网络深度集成 ?;D;E



\8\$&('0: 网络节点



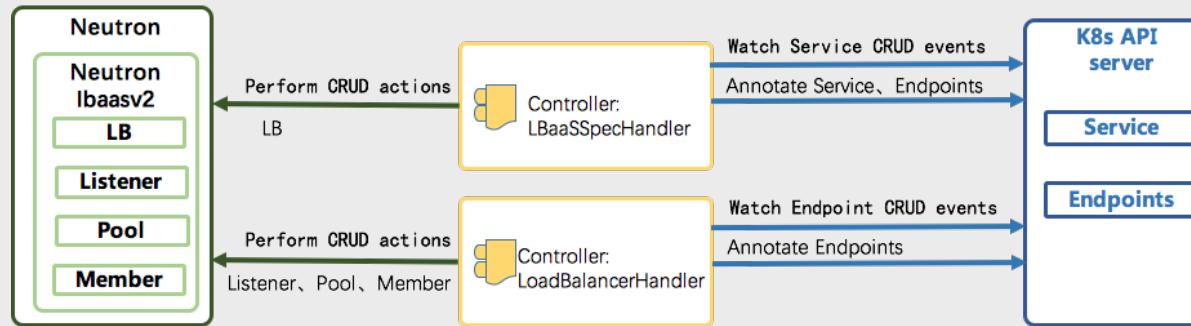
Kubernetes控制节点



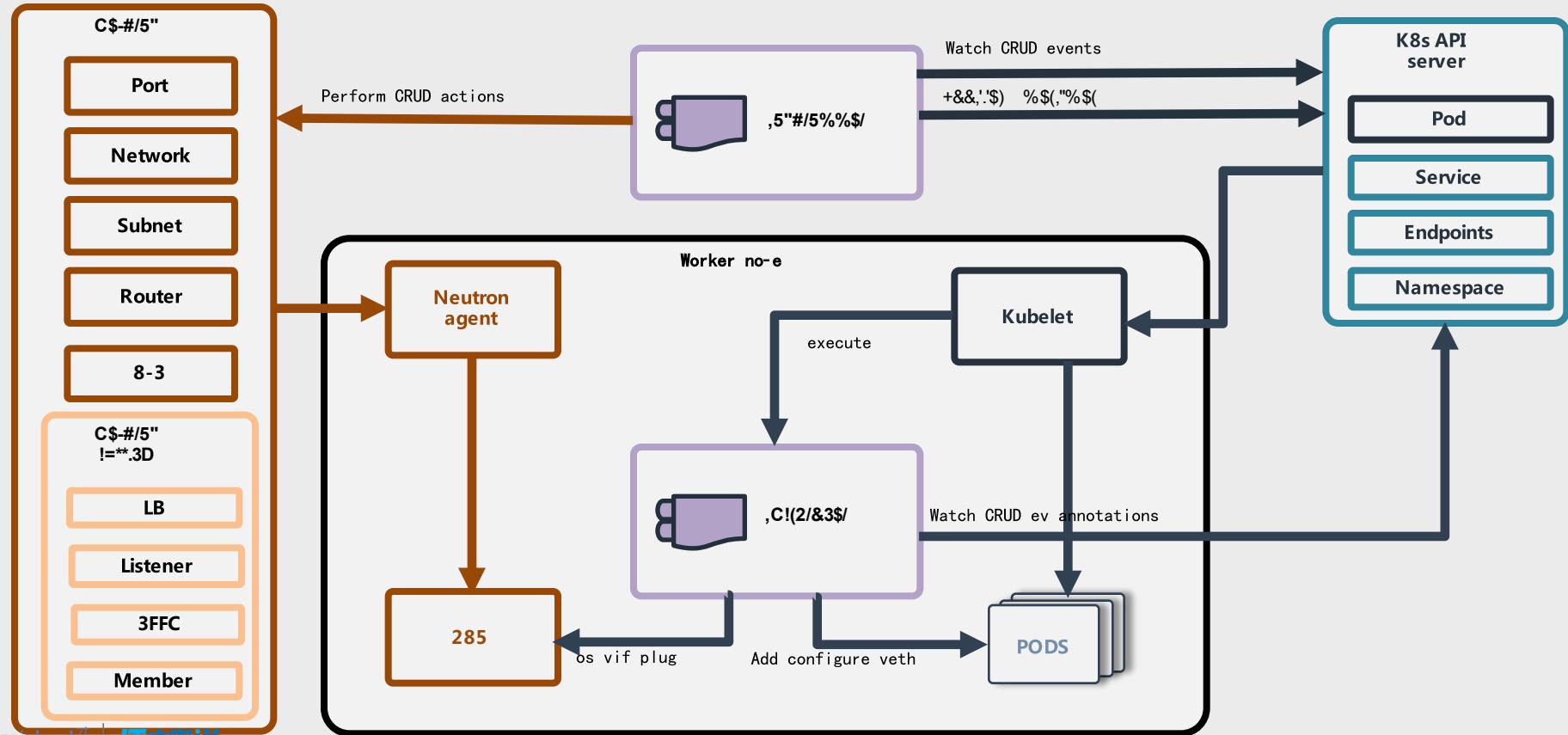
Openstack控制节点

# CaaS与IaaS融合 – 网络 | 与底层网络深度集成 | LB

Neutron LBaaS	Kubernetes
Loadbalancer VIP	Service Cluster IP
Loadbalancer FIP	Service External IP
Protocol and Port of Listener	Protocol and Port of Service
Loadbalance Method of Member Pool	Loadbalance Method of Service/Endpoints
Members (IP, Port)	Endpoints (IP, Port)



# S !\*\*+ 融合 > 网络 ?与底层网络深度集成 ?;DL;O



# CaaS与IaaS融合 – 网络 | 与底层网络深度集成 | 通断

应用分区

修改网络配置

修改分区的网络策略，可能会导致分区以外的应用不能访问当前分区的服务，请谨慎操作。

网络策略

流向 分区 网络组 协议 端口范围

请选择 请选择 请选择 请选择 4000 - 6000 确定

+ 新增网络策略 test-tmp

同集群下其它分区

qatest

修改网络配置

修改分区的网络策略，可能会导致分区以外的应用不能访问当前分区的服务，请谨慎操作。

网络策略

流向	分区	网络组	协议	端口范围	
out	00e5625f-a8ff-441b-9ee7-793c29ab0fdf	HTTP	2	- 200	
in	test-hq	00e5625f-a8ff-441b-9ee7-793c29ab0fdf	TCP	4	- 88

# CaaS与IaaS融合 – 网络 | 与底层网络深度集成 | 带宽

中国银行  
UnionPay  
中国银联  
China UnionPay

应用模版

使用指南 ▾ 租户 : slb-test ▾ 01201348 ▾

资源中心

- 存储
- 数据卷
- 应用中心

应用分区

应用

编排

应用模版

负载均衡

配置管理

镜像仓库

持续集成

运维中心

- 日志
- 监控
- 报警

管理中心

- 用户管理

新增模版

基本信息

容器组

重启策略

Always

OnFailure

Never

DNS策略

Default

ClusterFirstWithHostNet

ClusterFirst

主机名

选填

子域名

选填

优雅退出时间

30

qos带宽

请选择

管理(0.5Gbps)

低(1Gbps)

中(2Gbps)

高(4Gbps)

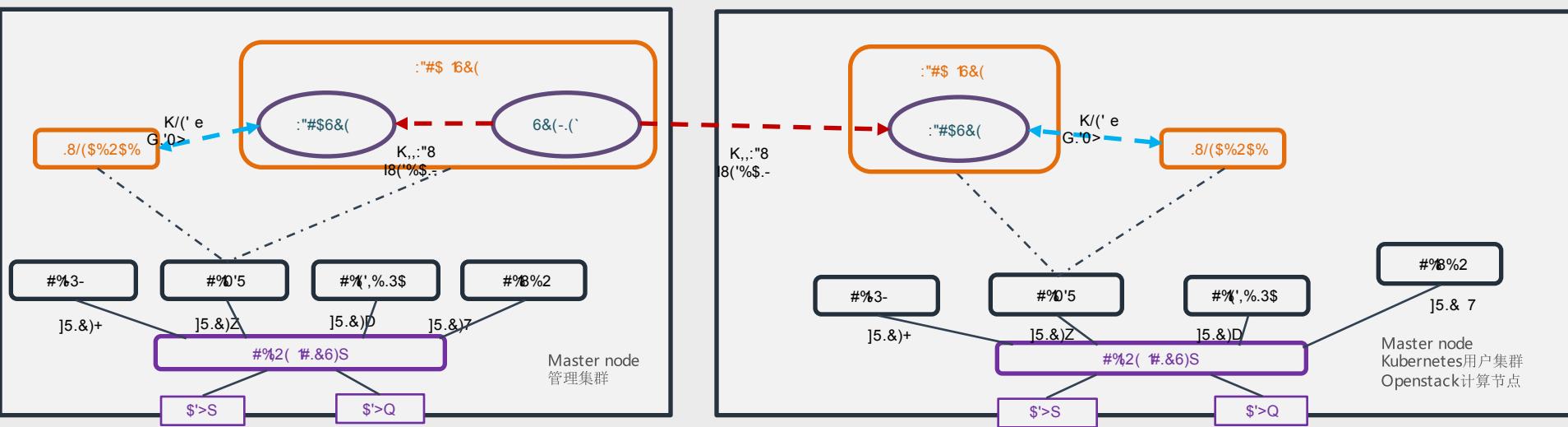
与主机共享network

与主机共享pid

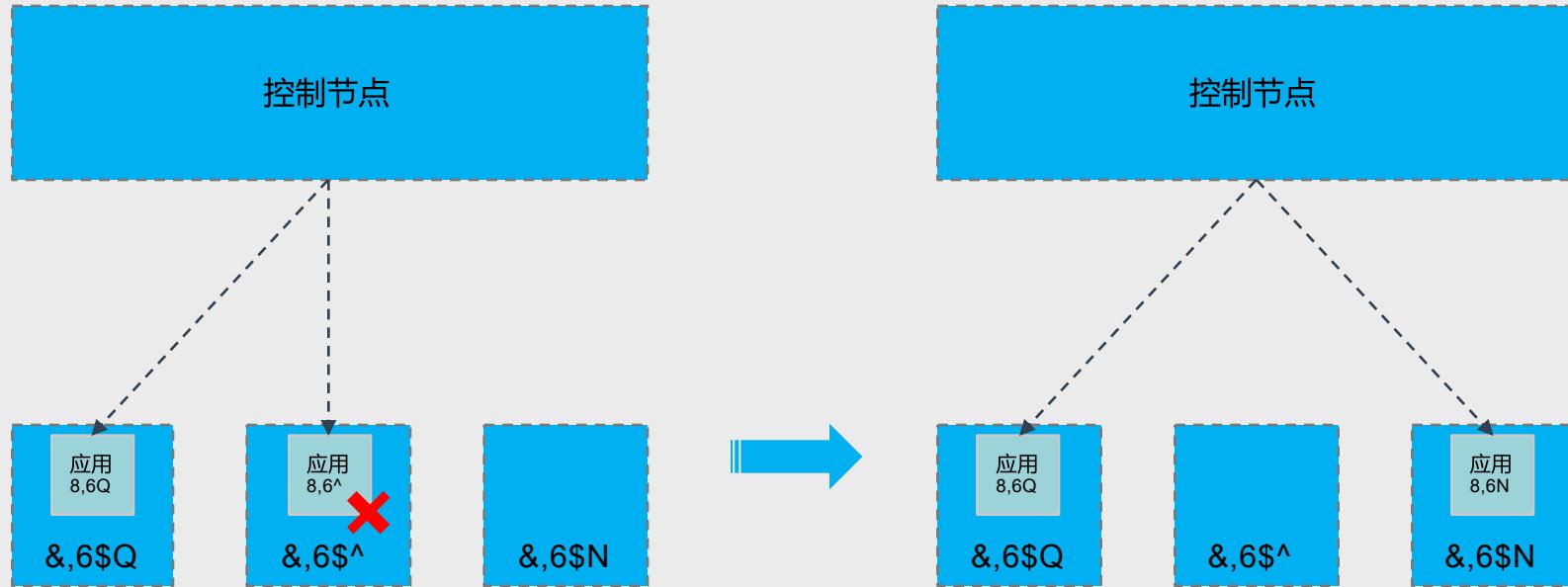
与主机共享ipc

取消 保存

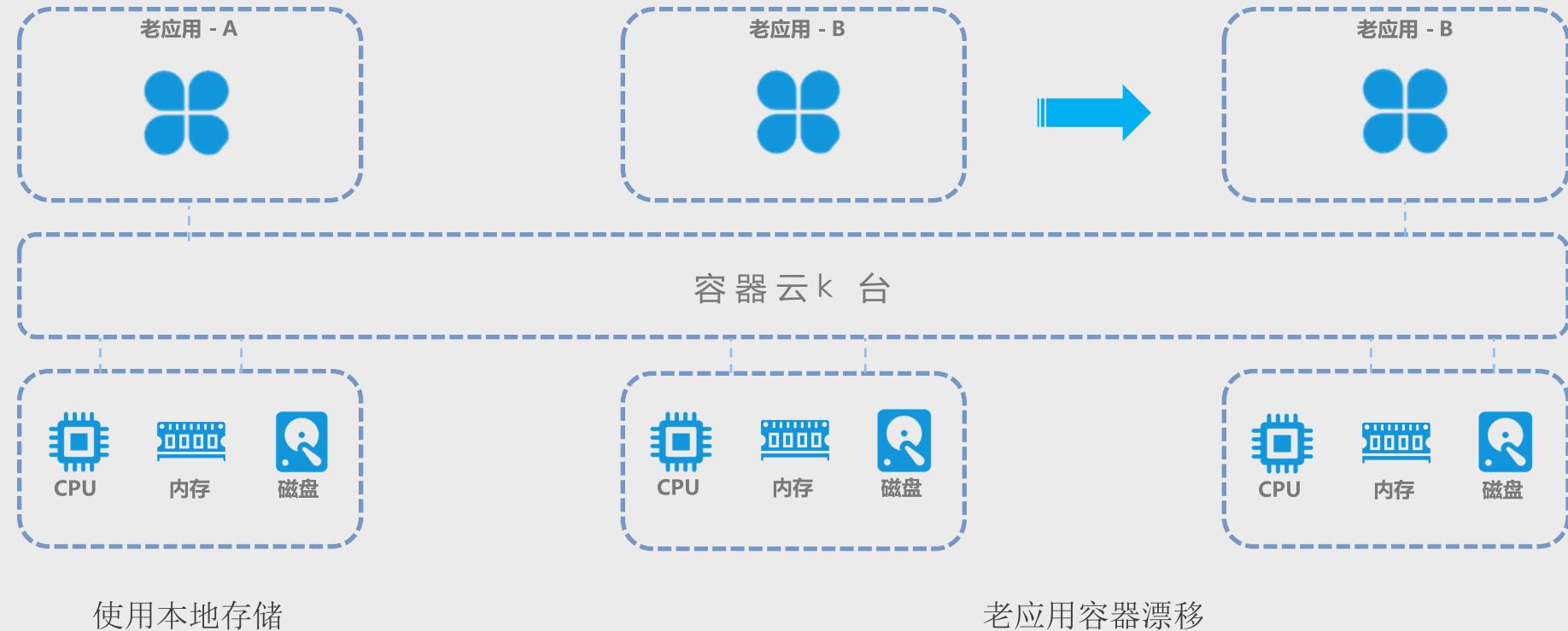
# !\*\*+ S !\*\*+ 融合 > 网络 ?与底层网络深度集成 ?服务发现



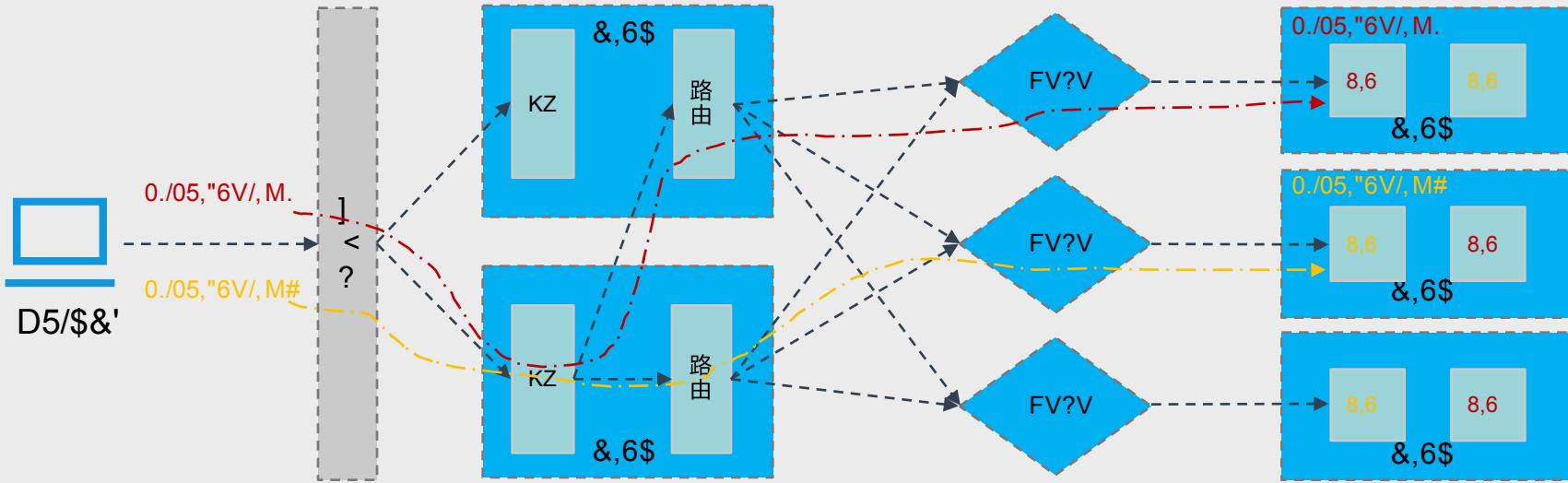
# 容器!) 不固定问题



# 容器云平台承载历史包袱老应用



# 外部访问容器云平台容器应用



# 谢谢



主办方:



协办方:

