

才云 Compass 容器云平台在 中国银联的落地实践



唐继元 tangjiyuan@caicloud.io

才云科技容器云平台案例分享 – 中国银联



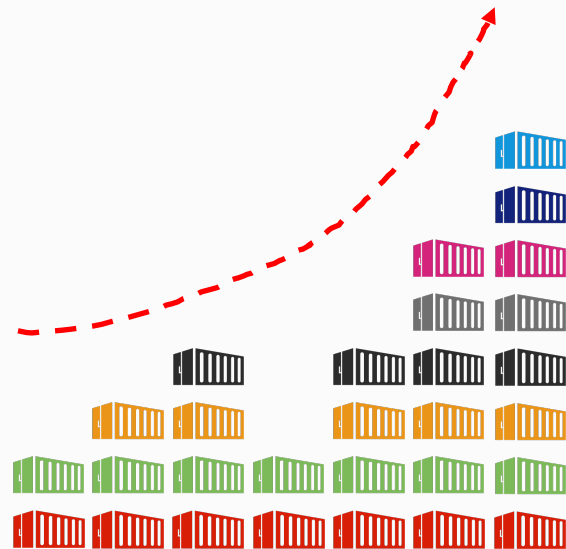
Kubernetes 现状与客户需求



才云 Compass 容器云平台架构



Compass 与云管平台集成方案





业务不断数字化转型

- 应用要求快速迭代
- 应用形态微服务化
- 容器成为应用载体
- 容器平台不是 PaaS



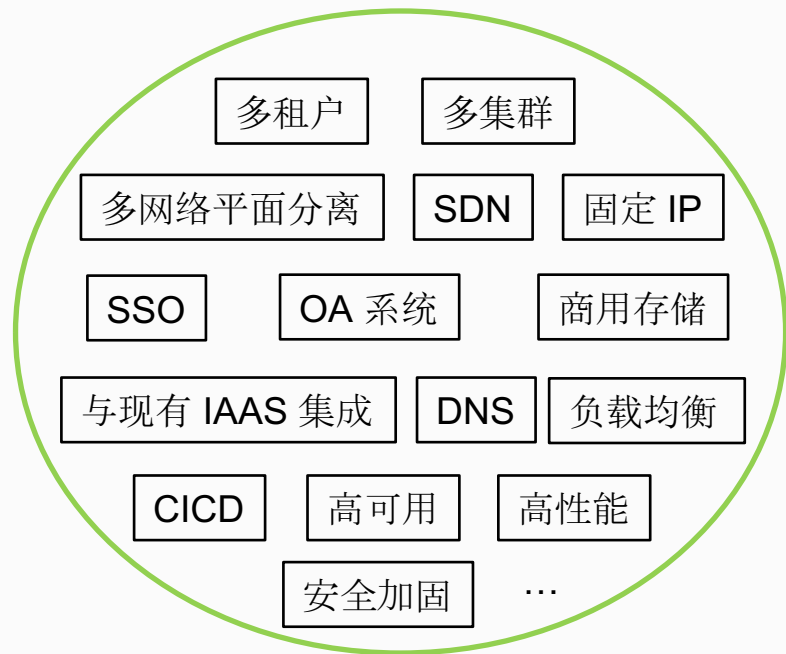
裸容器管理不堪重负

- 大量的裸容器运行
- 容器使用和管理难
- 应用编排和调度难
- 业务上线和升级难

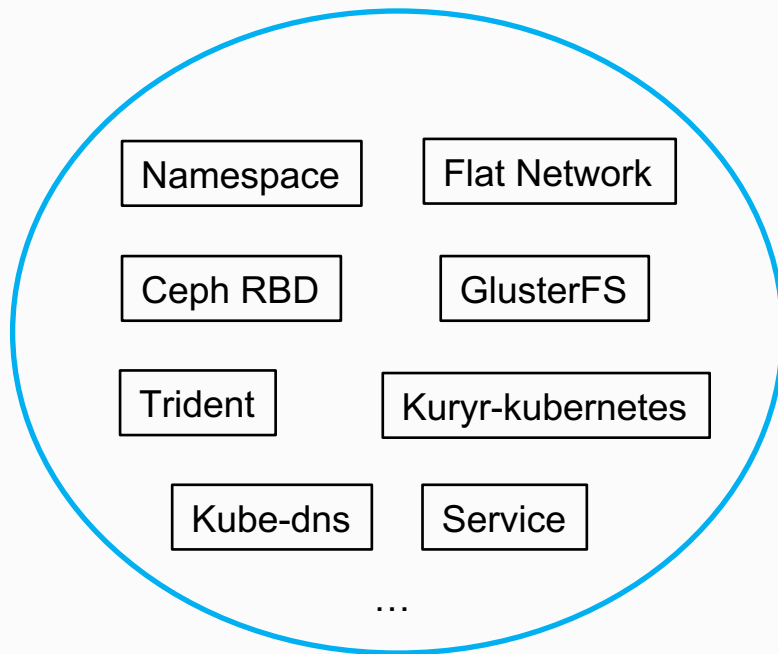


容器平台融入IT环境

- 应用不会都在容器上
- 已有在运行系统平台
- 业务交互和控制需求
- 平台一体化管理需求



客户需要什么



Kubernetes 现状

才云科技容器云平台案例分享 – 中国银联



Kubernetes 现状和客户需求



才云 Compass 容器云平台架构

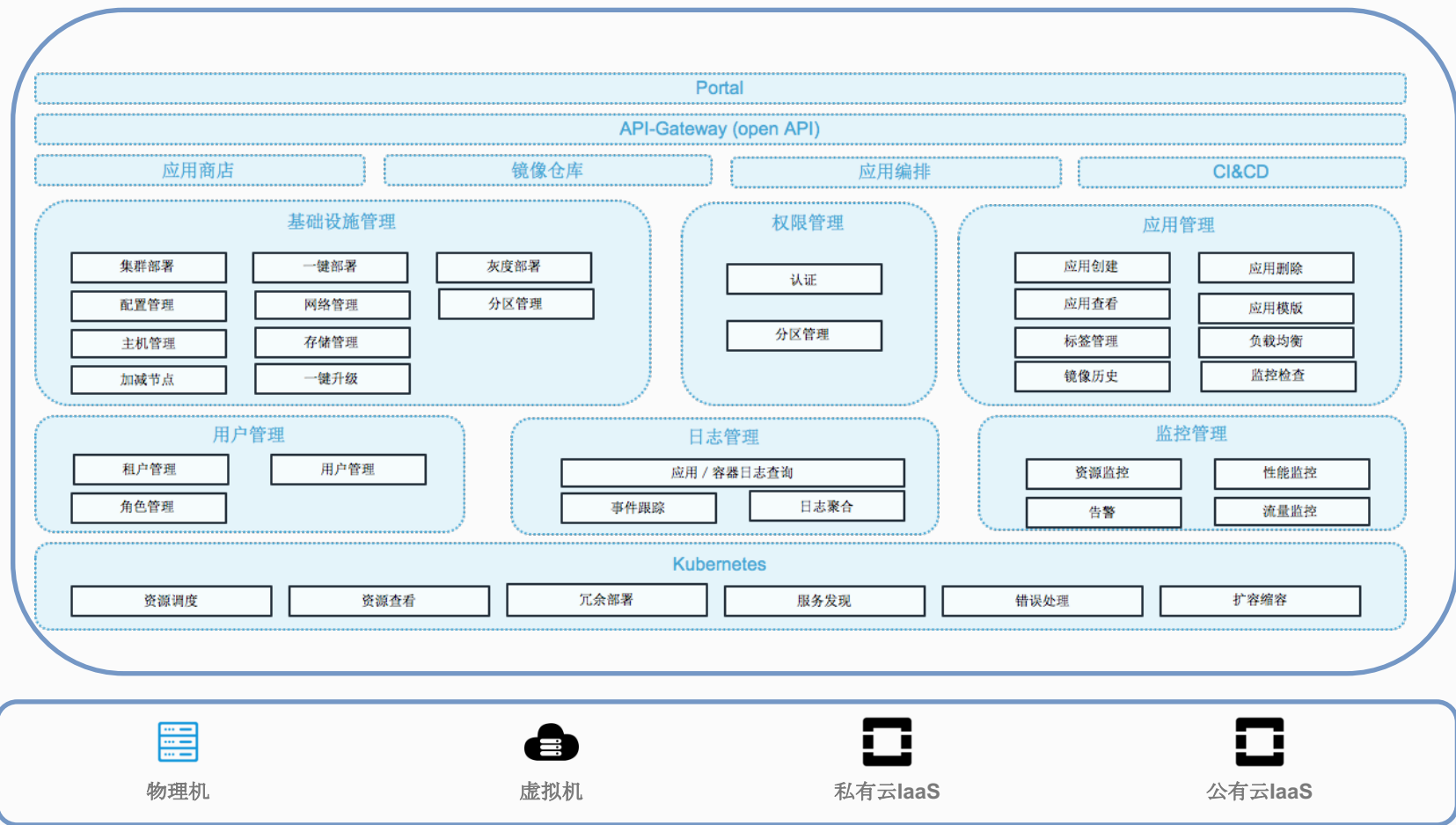


Compass 与云管平台集成方案



caicloud
才云

才云容器云平台 Compass 产品架构



才云科技容器云平台案例分享 – 中国银联



Kubernetes 现状和客户需求



才云 Compass 容器云平台架构



Compass 与云管理平台集成方案



compass
by caicloud



应用上云：

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



容器服务管理平台：

- 目标是逐步替换裸容器系统
- 实现核心业务稳妥上线



网络集成：与云资源管理平台SDN网络无缝集成



存储集成：与云资源管理平台存储后端无缝集成



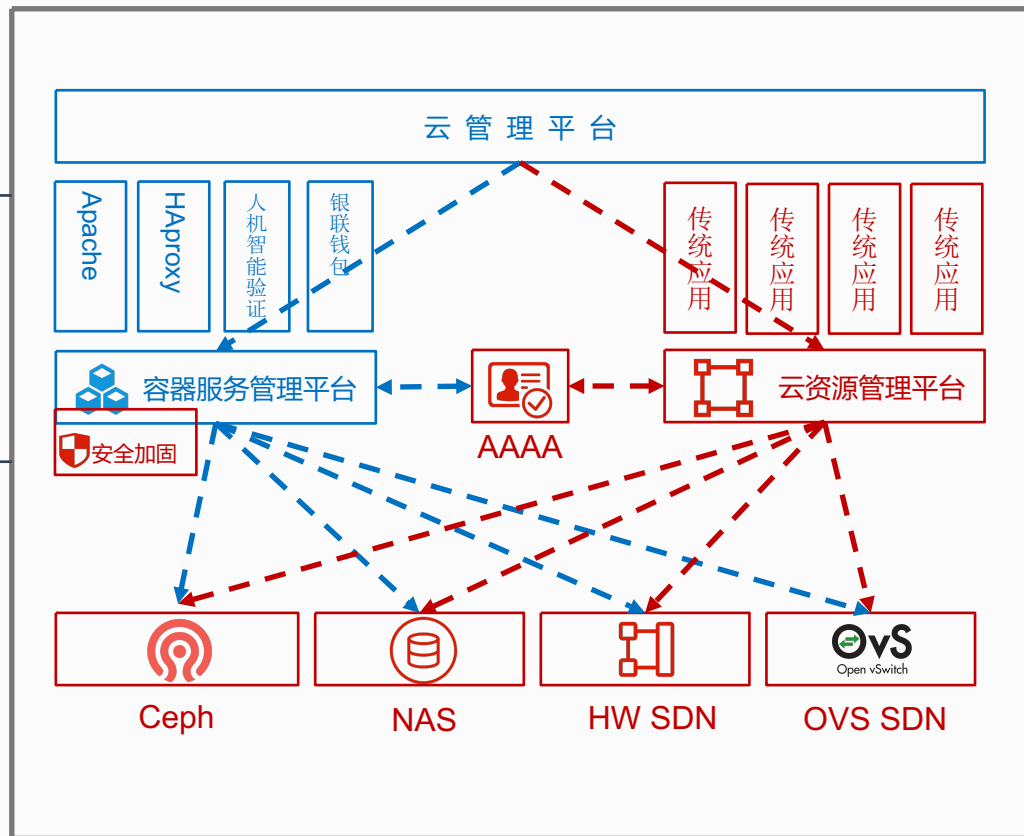
认证鉴权：与银联内部认证鉴权系统无缝整合



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



❑ SSO

- ❖ 用户信息从 Keystone 同步

❑ Compass 租户与 Openstack 租户一一对应

❑ 使用 Neutron 提供容器网络

- ❖ 多网络平面、租户网络隔离
- ❖ GBP 模型对接：网络策略、带宽控制
- ❖ 租户内容器服务虚拟机服务通过网络策略可以实现访问
- ❖ 使用 LBaaS 提供负载均衡
 - LBaaS 由 F5 或 Nginx 实现

❑ 定制化服务发现

- ❖ 租户 DNS？

❑ 使用 Netapp NAS 商用存储

- ❖ 分区间通过 Export Policy 隔离

容器服务平台细节分享 – SSO

 **中国银联**
China UnionPay

中国银联统一业务门户



请输入您的用户名和密码

用户名:

密 码: [忘记密码?](#)

机 构:

登录

重置

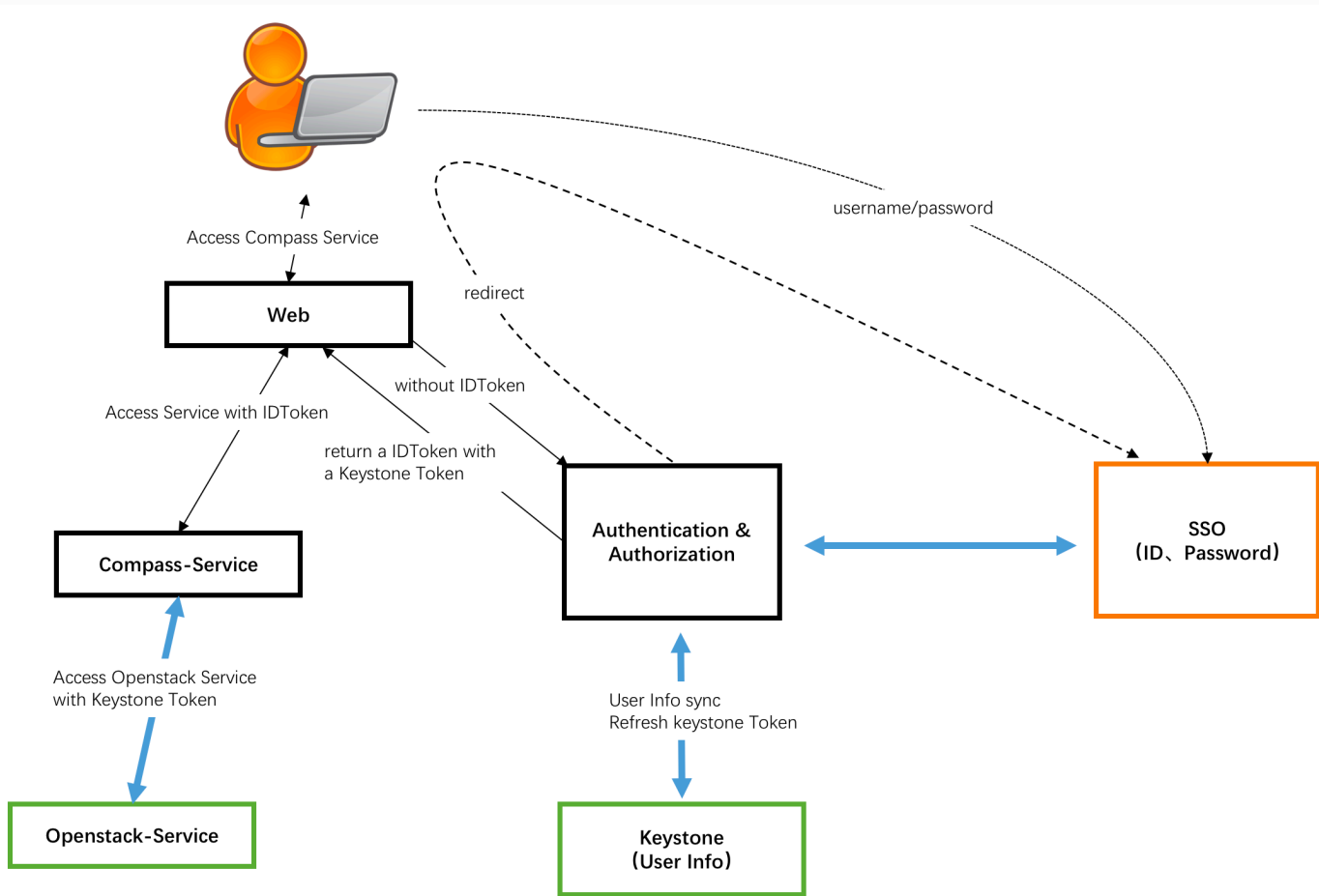
[中文版](#) | [English Version](#)

[文档下载](#)

严禁存储、传输、处理国家秘密信息

版权所有2009 中国银联

容器服务平台细节分享 – SSO



容器服务平台细节分享 – 租户对应

中国银联
租户管理

使用指南 系统管理界面 01201348

资源中心

节点
集群
存储
存储服务
存储方案
网络
负载均衡
运维中心
日志
监控
报警
管理中心
镜像仓库
租户管理
用户管理
审计日志
报表管理

新增租户

基本信息

名称 输入租户名称

描述 选填 200字以内

选择 openstack 租户

project 输入关键词模糊过滤

- ☒ docker-k8s k8s-project3
- ☐ Default new-test
- ☐ Default test2
- ☐ Default test17
- ☐ Default 123123
- ☐ zvmDomain zvmProject2


k8s-project3

project信息
description: 暂无
domain_name: docker-k8s2
project_id: 118e9638341c42dca67dc26f590186cd

容器服务平台细节分享 – 网络对接

中国银联
China UnionPay

应用分区

使用指南  租户: test-tenant docker

资源中心

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

新增分区

分区名称

所属集群

user-cluster-up

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

l3policy_id

请选择l3policy

podCIDR ?

for example: 192.168.1.0/24

serviceCIDR ?

for example: 192.168.1.0/24

GBP	Neutron	Compass
Policy Target	Port	Pod NIC
Policy Target Group	Subnet	CIDR
L2 Policy	Network	Partition
L3 Policy	Router	From Openstack Project
Policy rules set	Security Group	Network Policy

容器服务平台细节分享 – 网络策略 | 通断

中国银联
China UnionPay

应用分区

使用指南

租户: test-tenant

01201348

qatest

当前状态 运行正常

创建时间 2018-02-02 13:59:40

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	
请选择	请选择	请选择	请选择	4000 - 6000	确定
		test-tmp			

+ 新增网络策略

容器服务平台细节分享 – 网络策略 | QOS

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

新增模版

容器组

基本信息

无状态实例

配置

容器组

容器

容器1

访问

存储

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

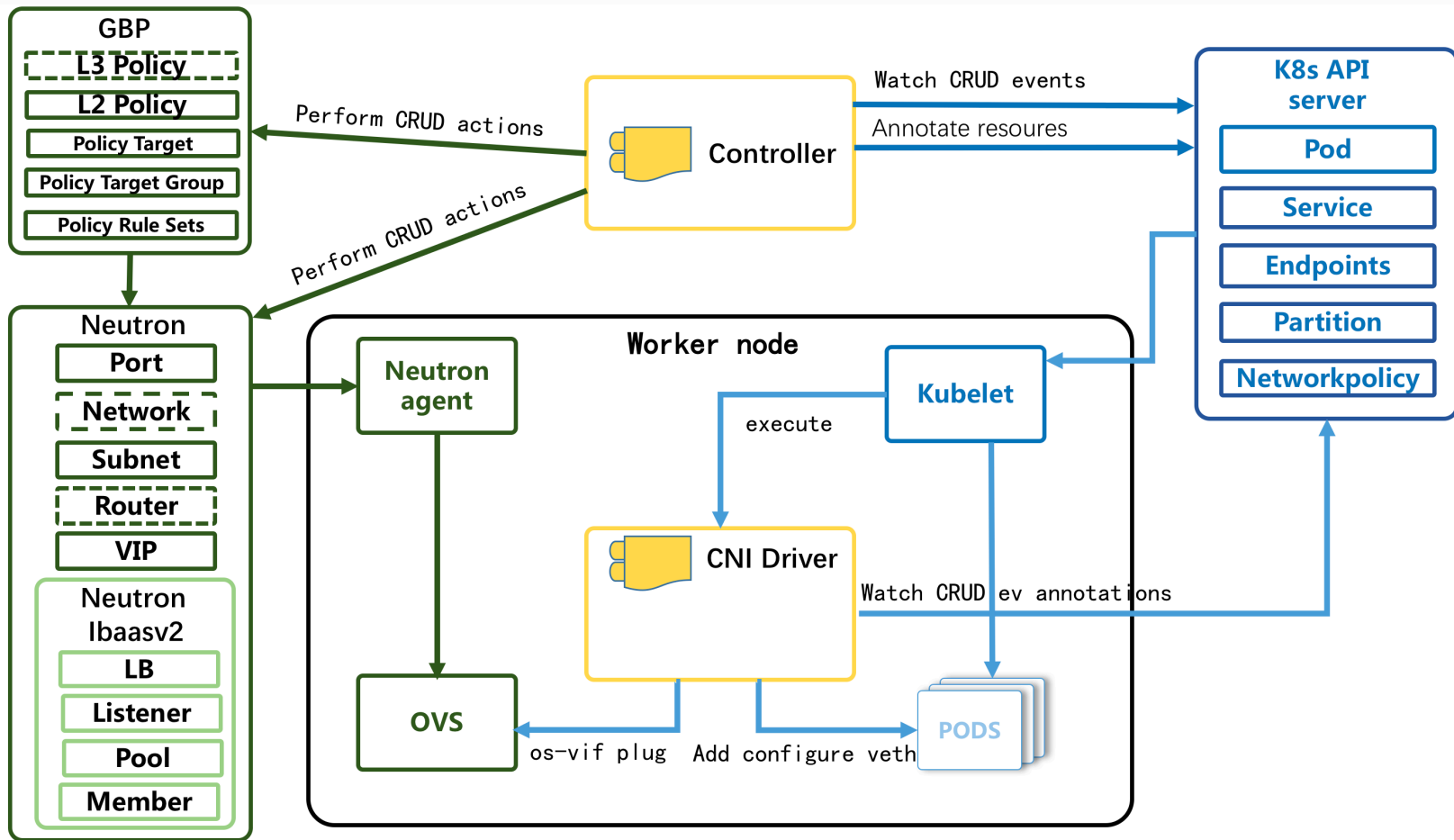
与主机共享pid

与主机共享ipc

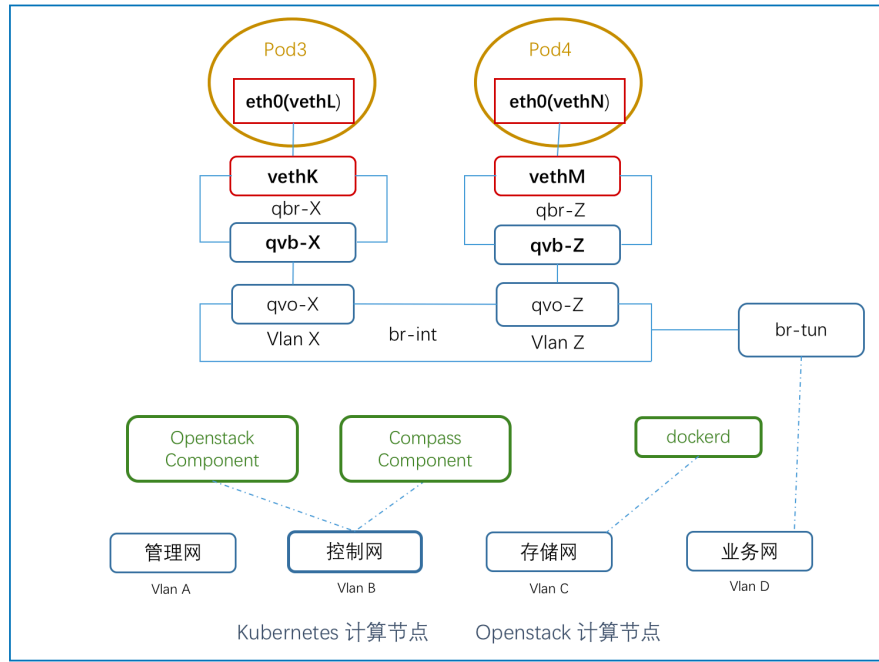
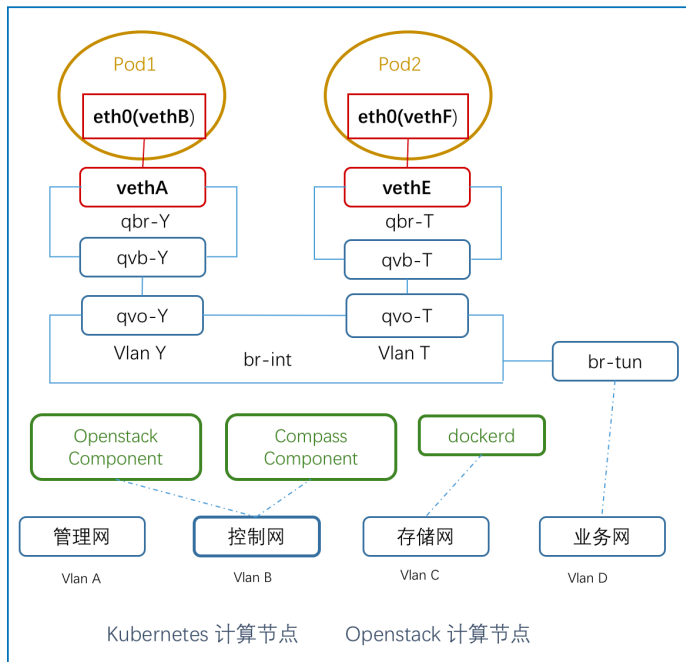
取消

保存

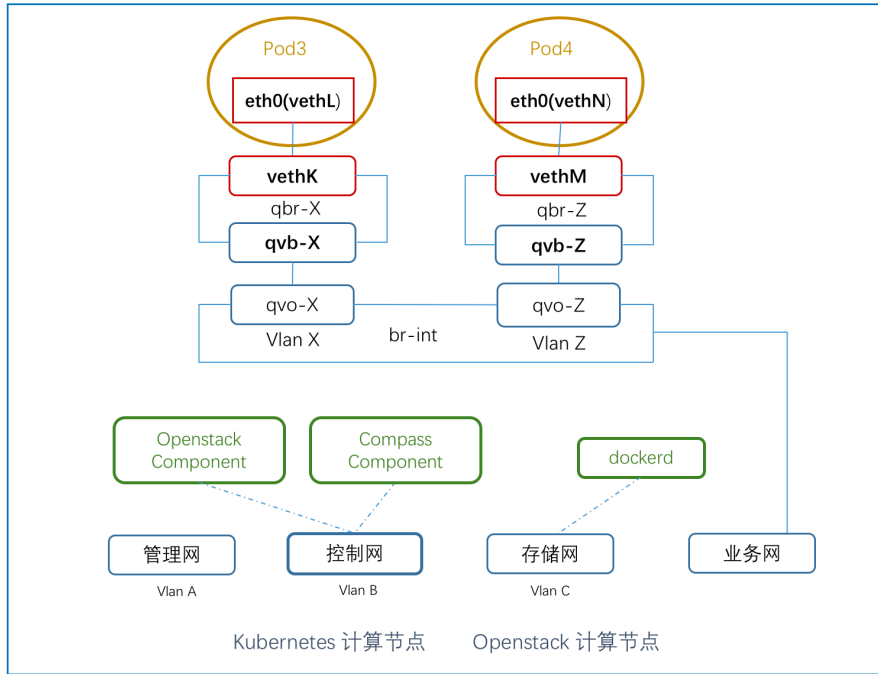
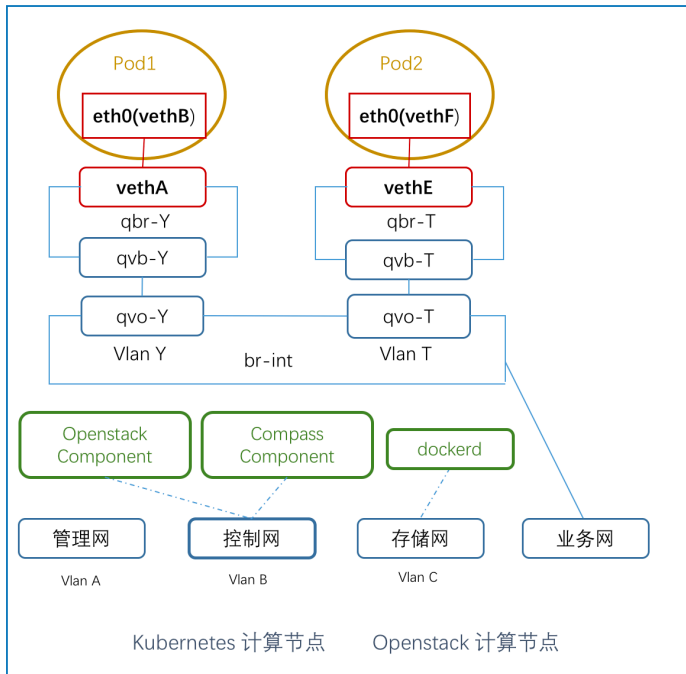
容器服务平台细节分享 – 网络对接 | 实现

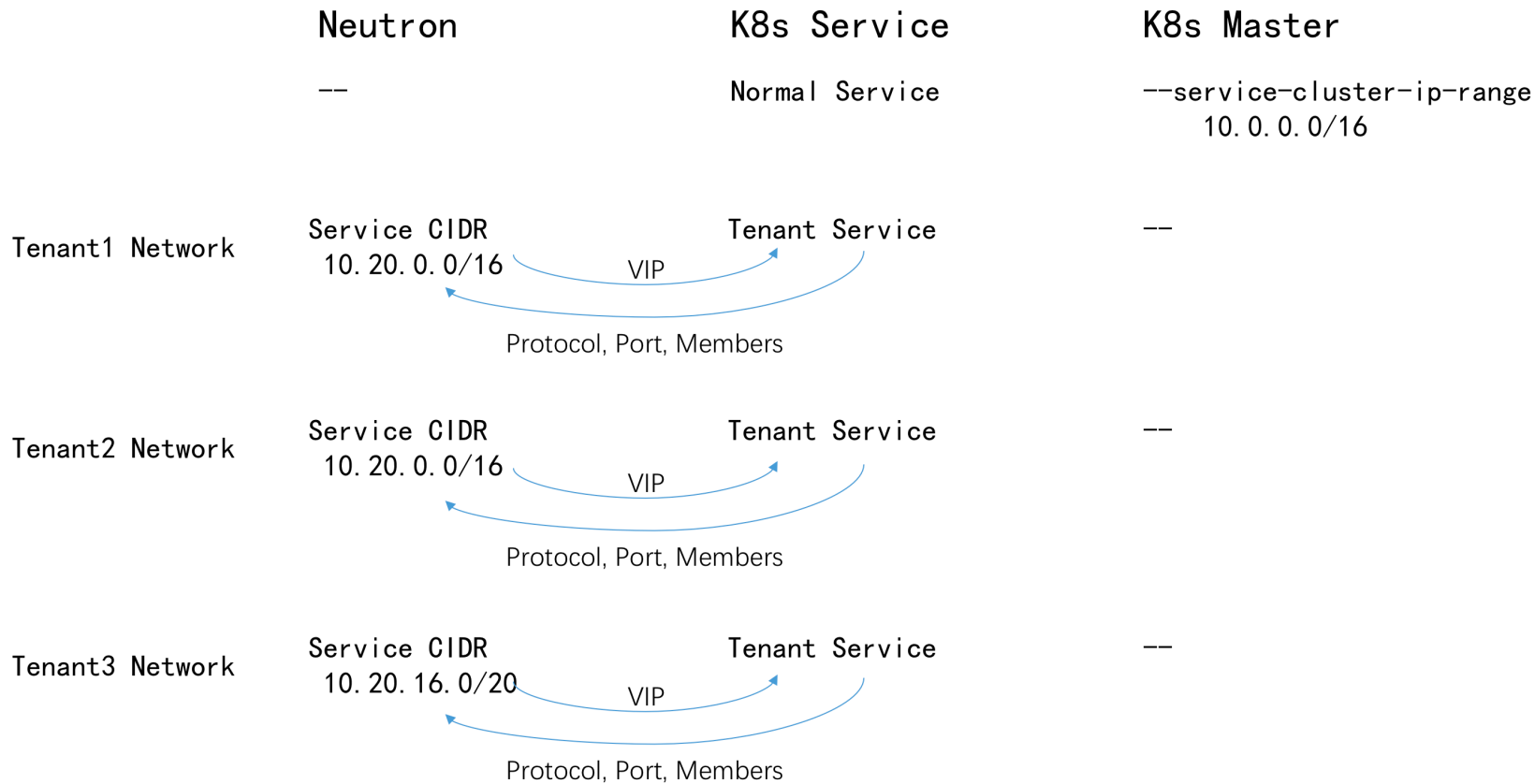


Openstack 纯软 vxlan

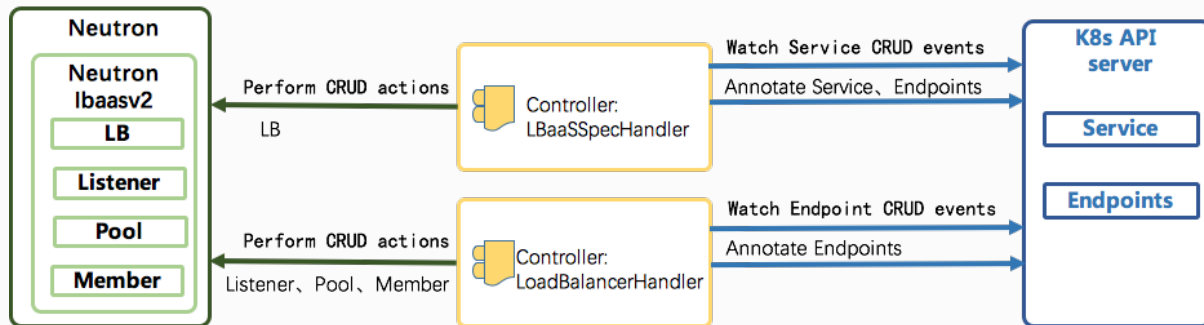


Openstack 硬件 SDN Based Vxlan

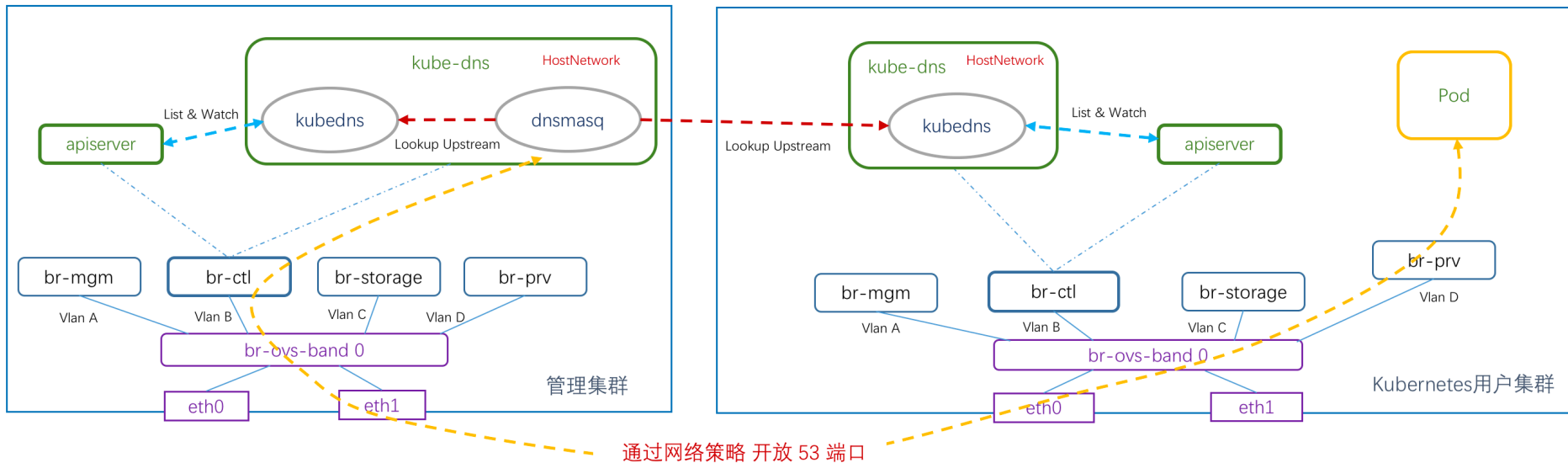




Neutron LBaaS	Kubernetes
Loadbalancer VIP	Service Cluster IP
Loadbalancer FIP	Service External IP
Protocol and Port of Listener	Protocol and Port of Service
Loadbalance Method of Member Pool	Loadbalance Method of Service/Endpoints
Members (IP, Port)	Endpoints (IP, Port)



容器服务平台细节分享 – 网络对接 | 服务发现



容器服务平台细节分享 – 商用存储 | NAS

中国银联
China UnionPay

存储服务

关于

系统管理界面

slwang

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

镜像仓库

集成存储服务

名称

test

存储类型

glusterfs

nas-netapp

nfs

后端类型

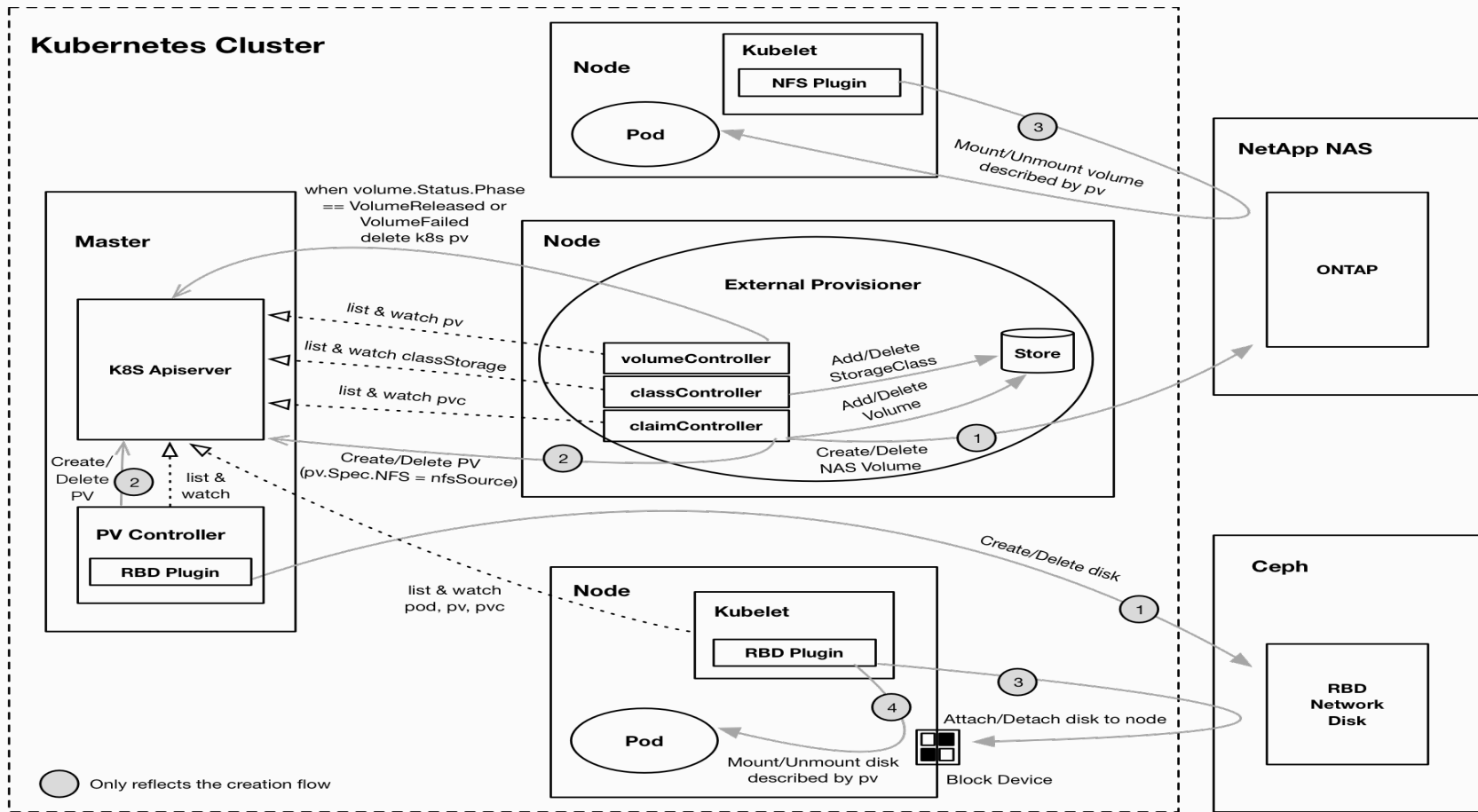
test

创建

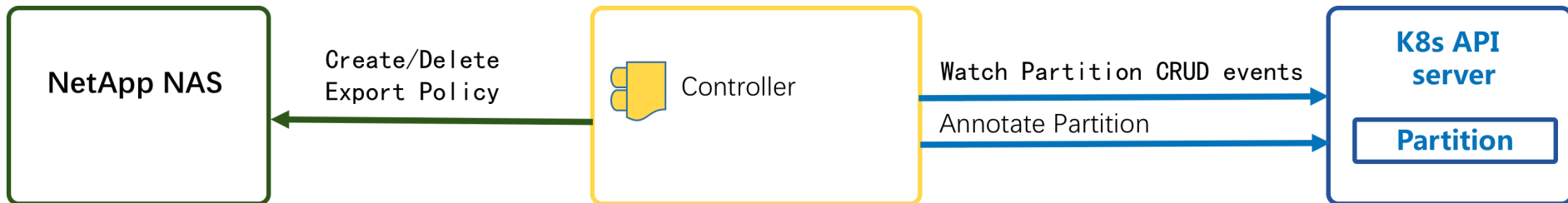
取消

除了 Compass 默认的 CephRBD、NAS、GlusterFS，还可以添加额外的

容器服务平台细节分享 – 存储集成



容器服务平台细节分享 – NAS 多分区隔离



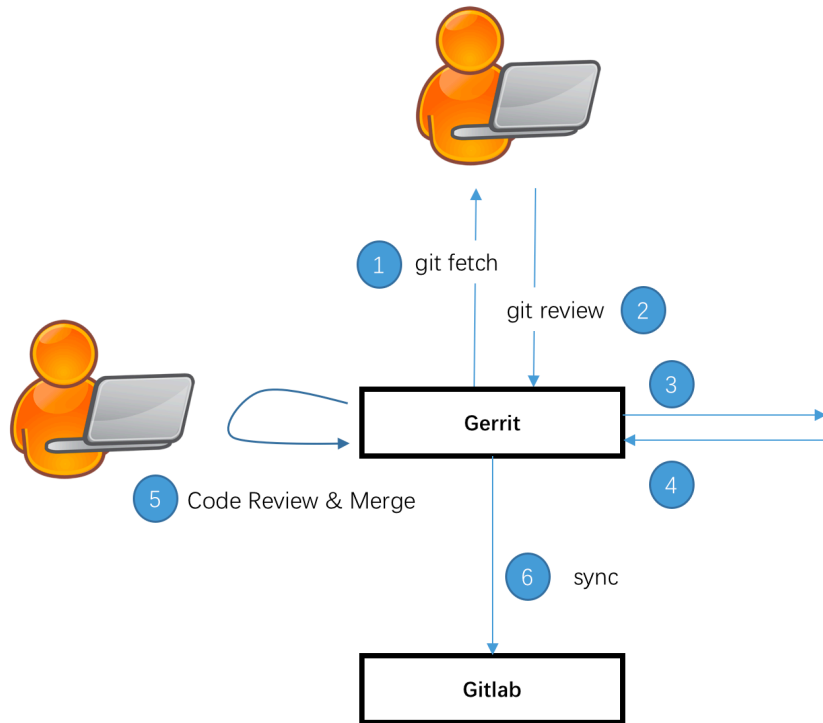
分区内创建使用 NetApp NAS 的 PVC



分区 Export Policy



NAS 存储分区隔离



容器服务平台细节分享 – 持续发布

The screenshot displays the Caicloud web interface for managing container images. A modal window titled "同步镜像" (Synchronize Image) is open in the center, featuring a dropdown menu labeled "请选择" (Please select) and two buttons: "取消" (Cancel) and "开始同步" (Start Synchronization). The background interface includes a top navigation bar with the "镜像仓库" (Image Repository) section selected. Below this, there are tabs for "仓库管理" (Repository Management), "项目管理" (Project Management), and "docker account". The main content area shows a list of image repositories under the "library (7)" filter, including "busybox", "hello-world", "mongodb", "mysql", and "redis". On the right side, a panel titled "mysql 版本信息" (MySQL Version Information) displays details for version 5.7.14, marked as "安全" (Secure), with a timestamp of 2016-08-23 03:20:13 and a "同步至其他仓库" (Synchronize to other repository) button.

同步镜像

请选择

取消 开始同步

mysql 版本信息

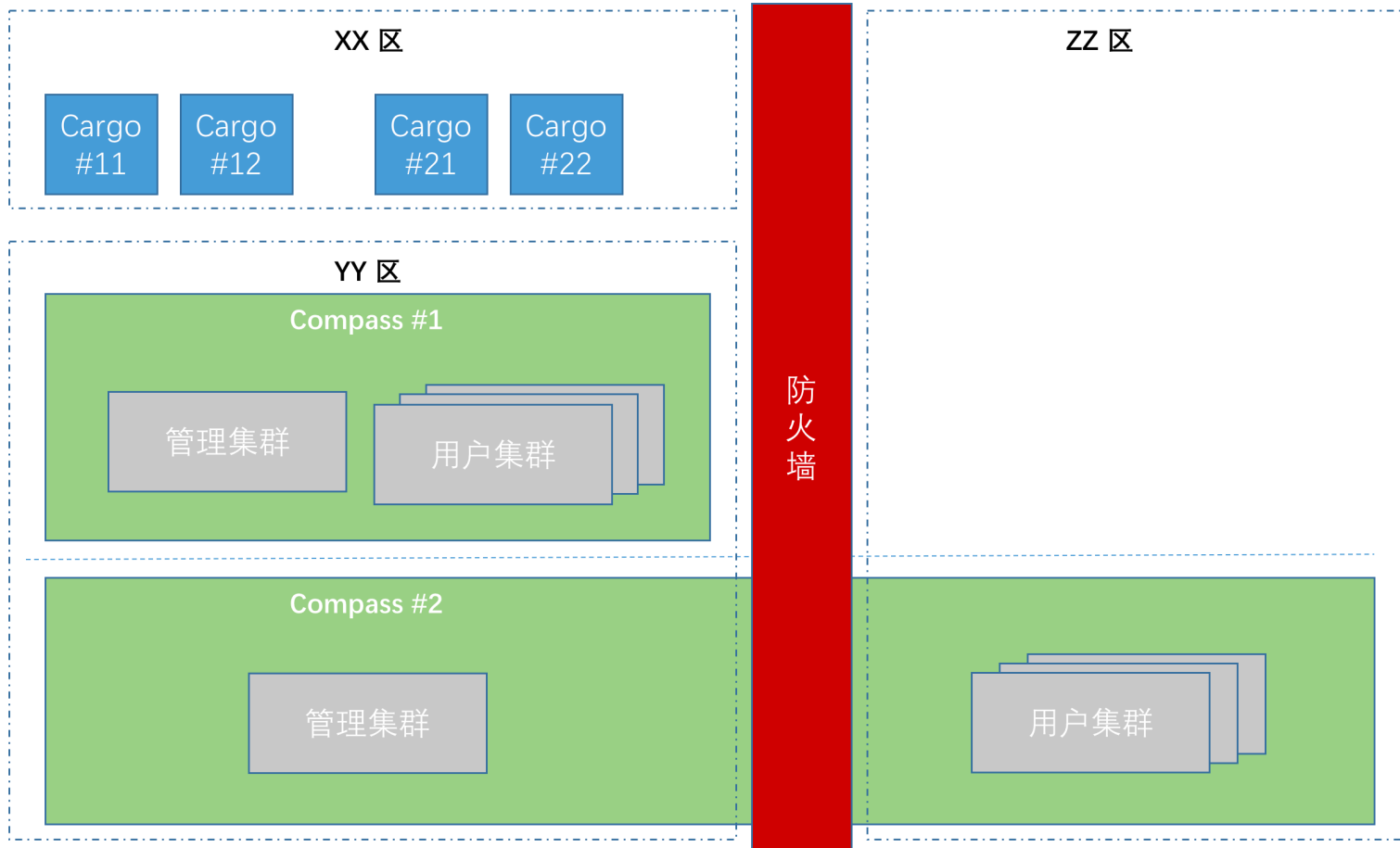
同步至其他仓库

5.7.14 安全

2016-08-23 03:20:13

没有更多了

容器服务平台细节分享 – 部署情况





容器服务平台细节分享 – 跳转到 Openstack

