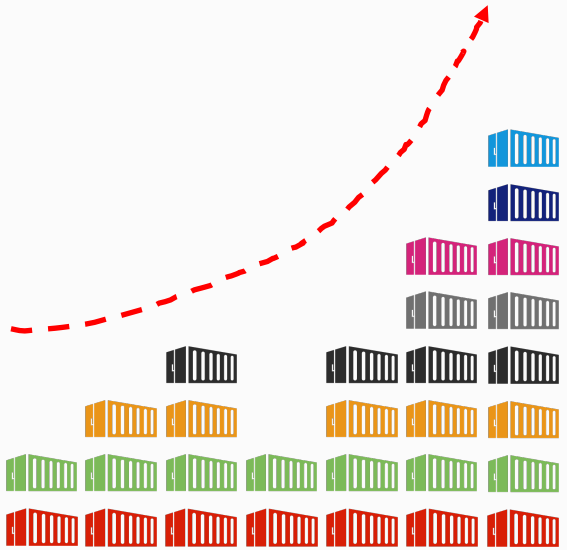
才云 Compass 容器云平台在中国银联的落地实践

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



企业容器服务平台的必要性

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

Kubernetes 现状和客户需求

多租户
多集群
多网络平面分离
SDN
固定 IP
SSO
OA 系统
商用存储
与现有 IAAS 集成
DNS
负载均衡
CICD
高可用
高性能
安全加固
…

客户需要什么

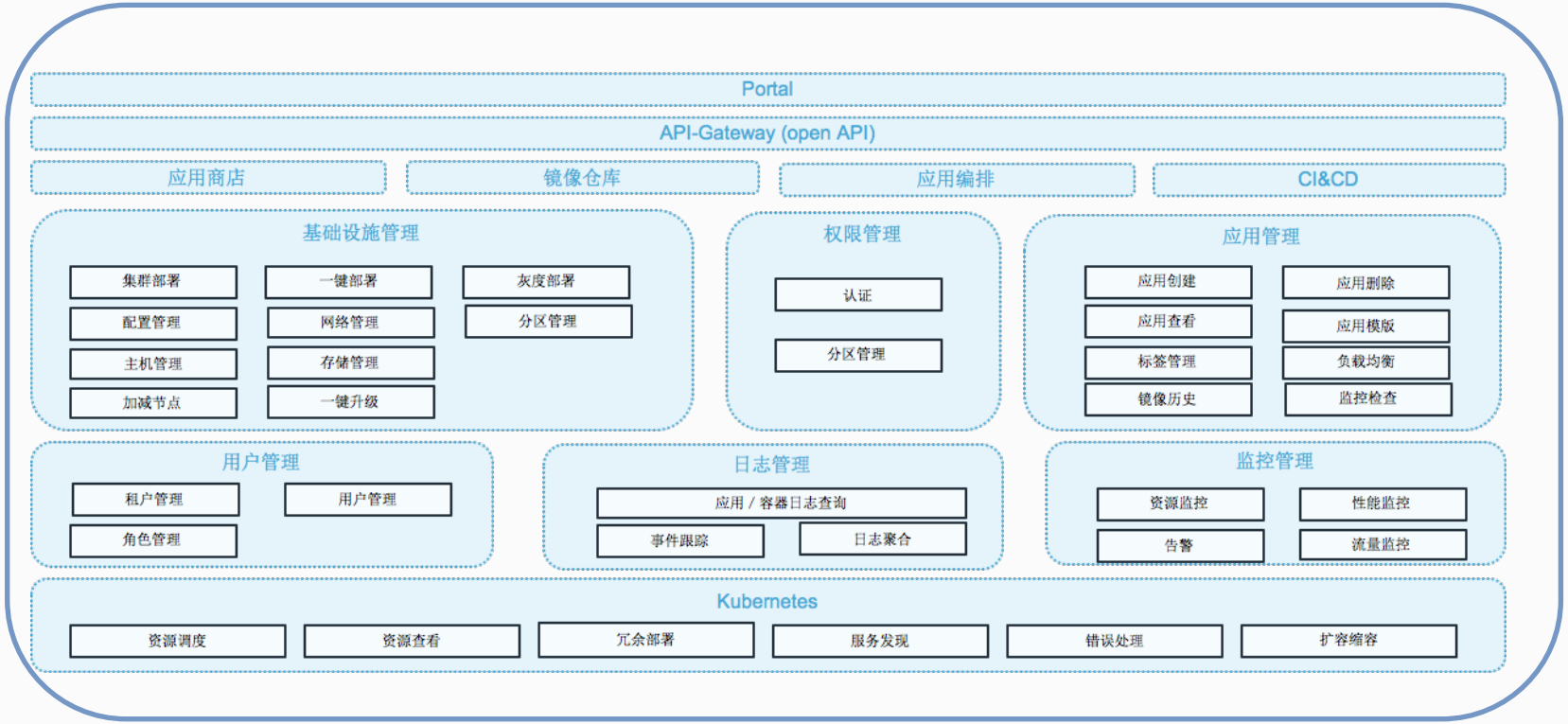
Namespace
Flat Network
Ceph RBD
GlusterFS
Trident
Kuryr-kubernetes
Kube-dns
Service
…

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

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

容器服务平台概览肖像

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

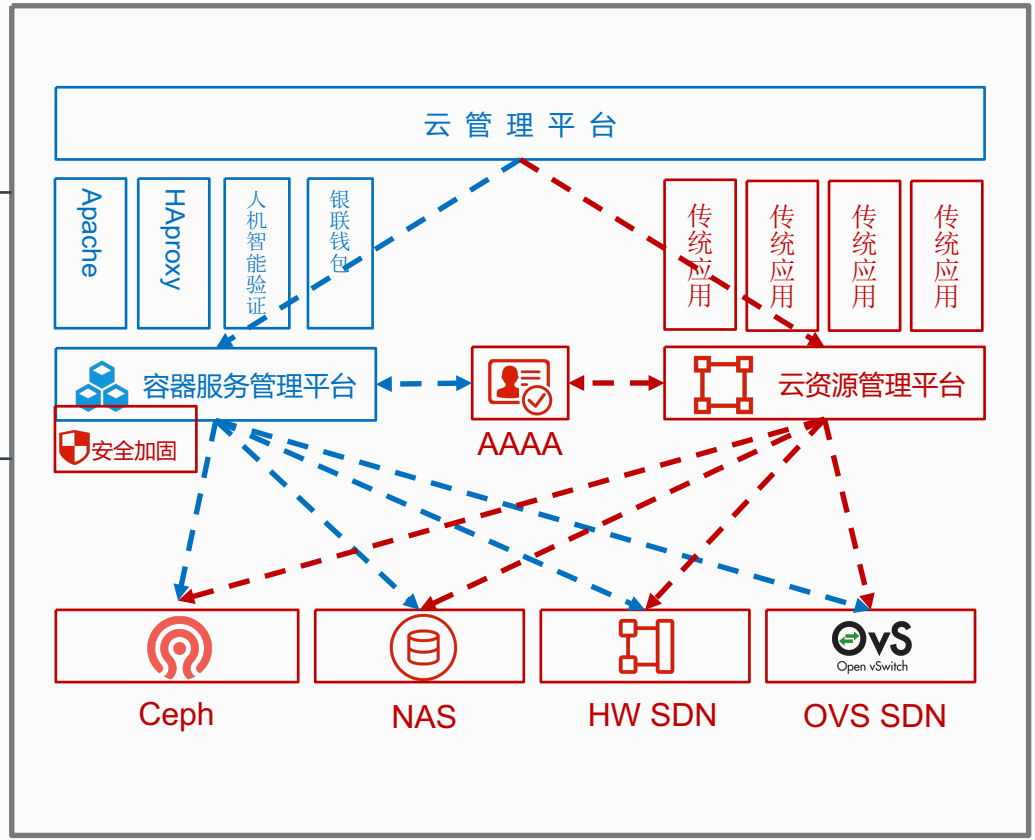
网络集成：与云资源管理平台SDN网络无缝集成

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

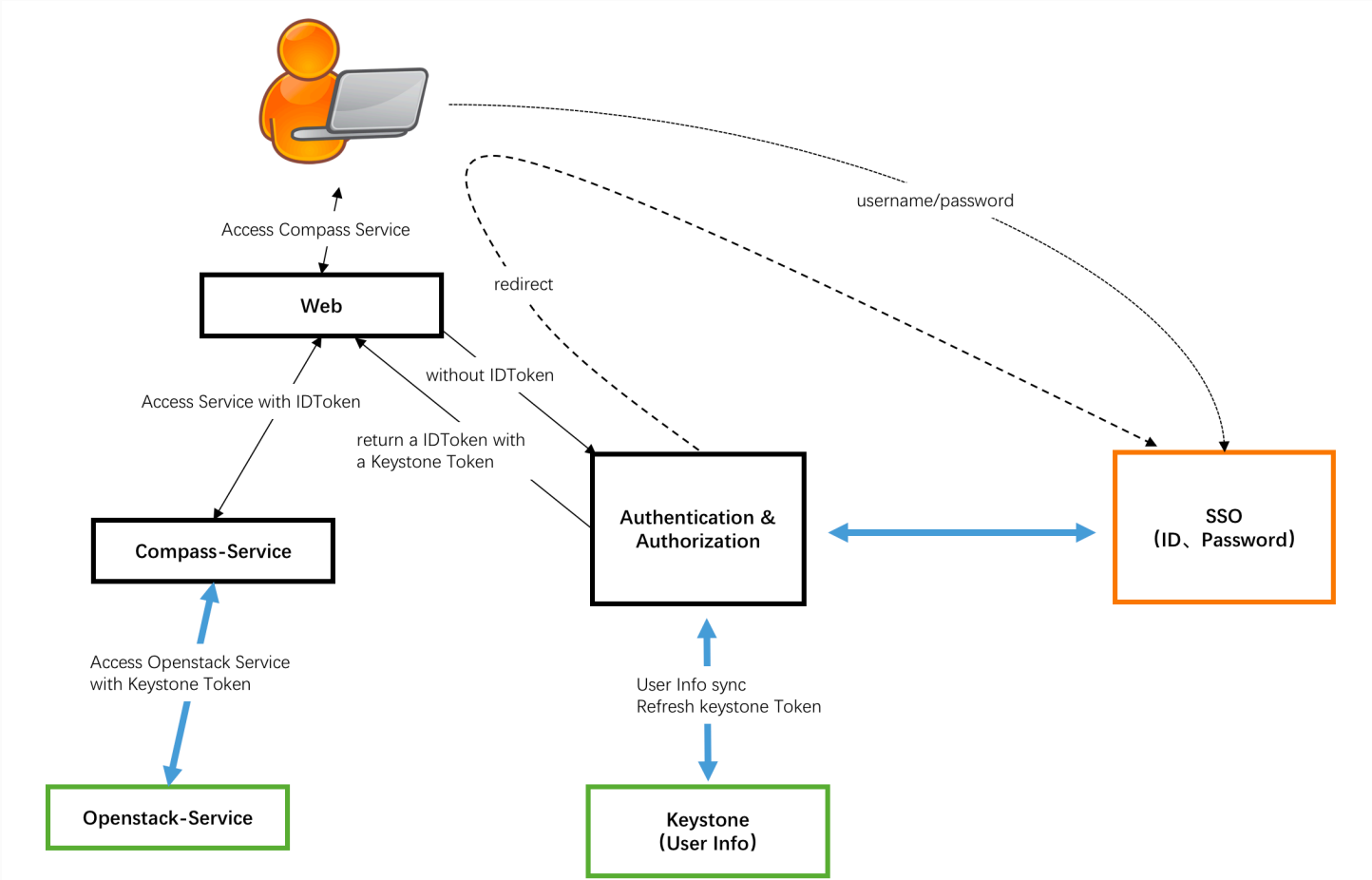


容器服务平台细节分享 – 设计要点

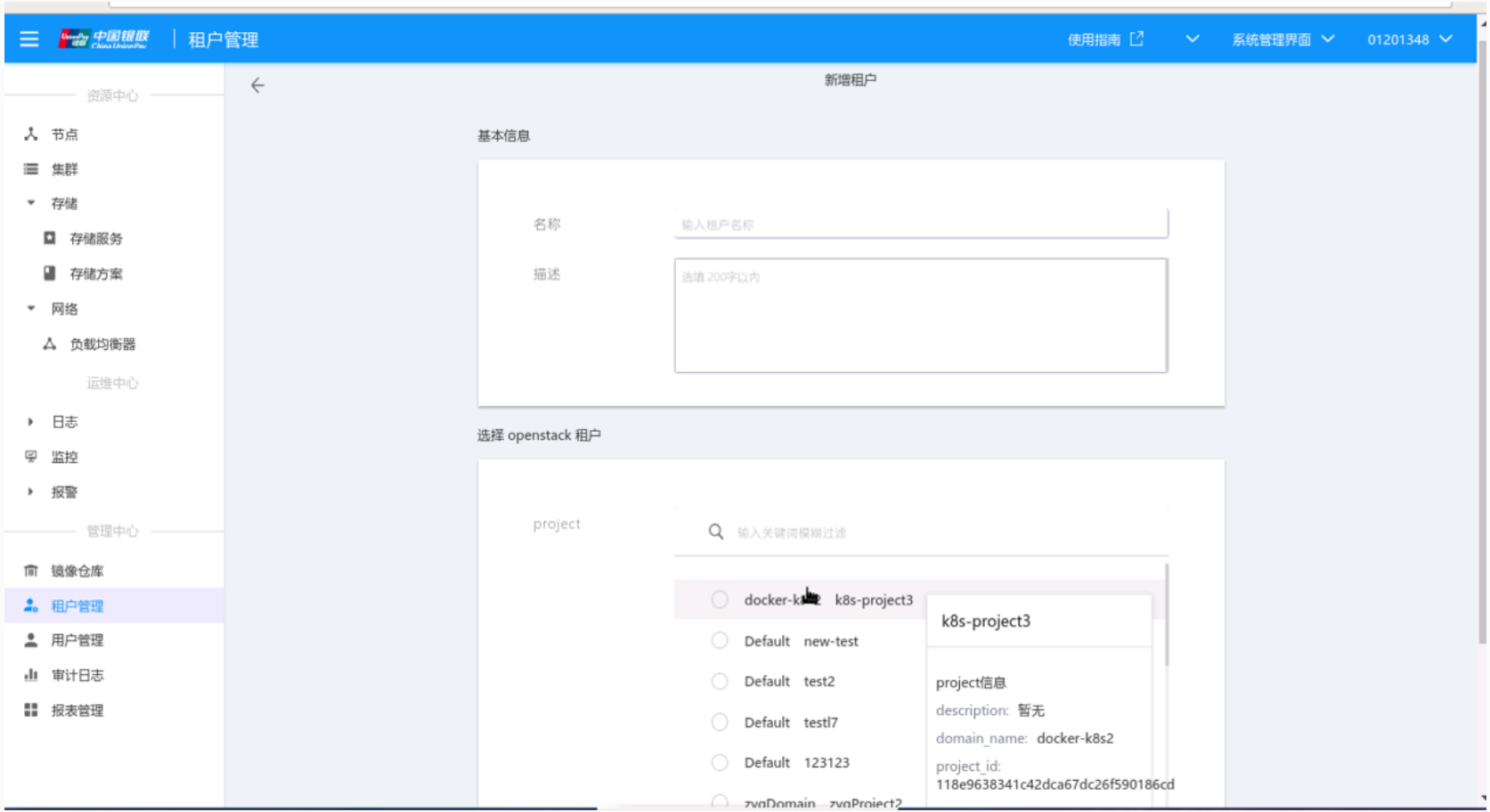
- SSO
  - 用户信息从 Keystone 同步
- Compass 租户与 Openstack 租户一一对应
- 使用 Neutron 提供容器网络
  - 多网络平面、租户网络隔离
  - GBP 模型对接：网络策略、带宽控制
  - 租户内容器服务虚拟机服务通过网络策略可以实现访问
  - 使用 LBaaS 提供负载均衡
    - LBaaS 由 F5 或 Nginx 实现
- 定制化服务发现
  - 租户 DNS？
- 使用 Netapp NAS 商用存储
  - 分区间通过 Export Policy 隔离

容器服务平台细节分享 – SSO

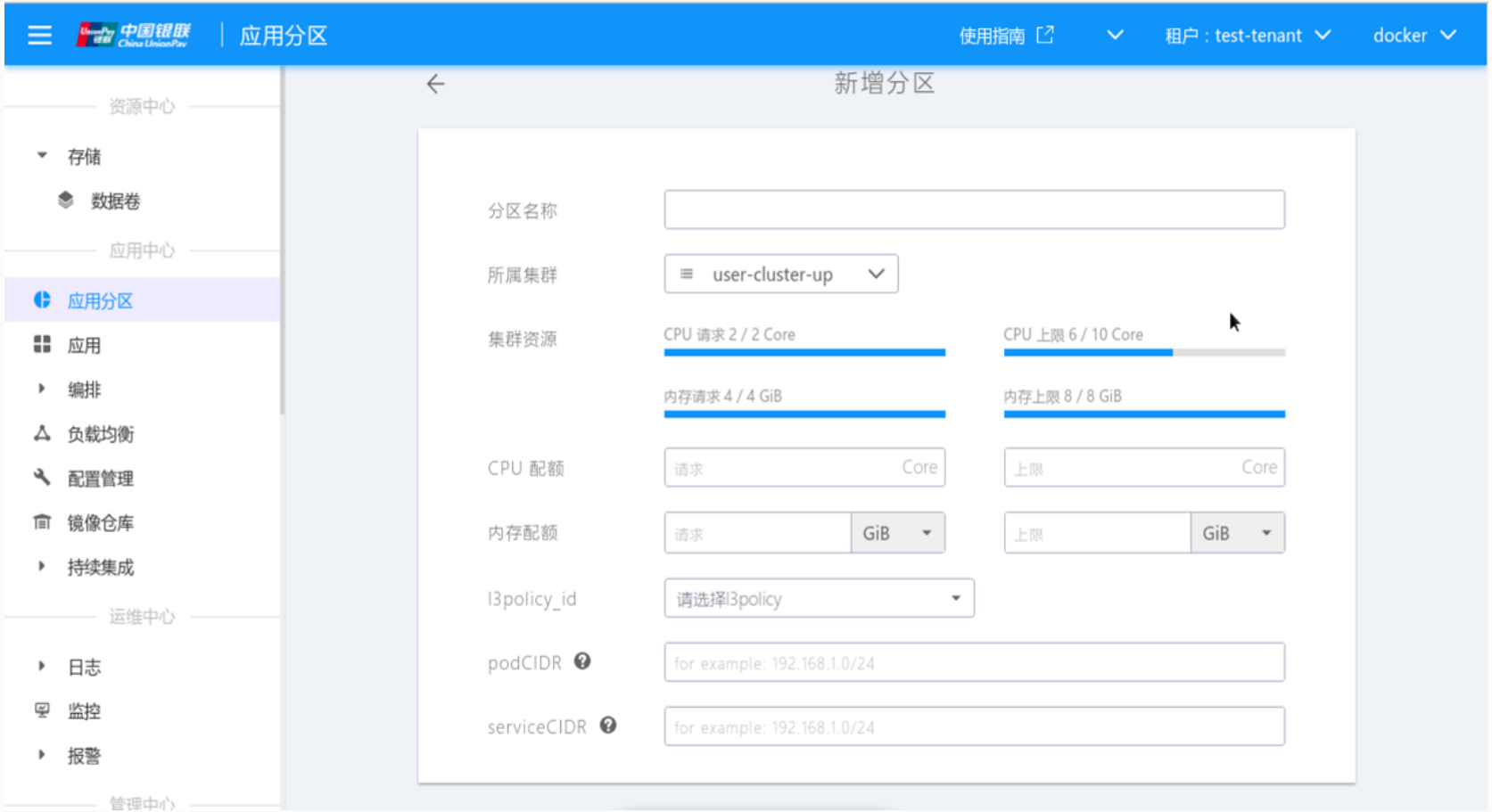
容器服务平台细节分享 – SSO



容器服务平台细节分享 – 租户对应



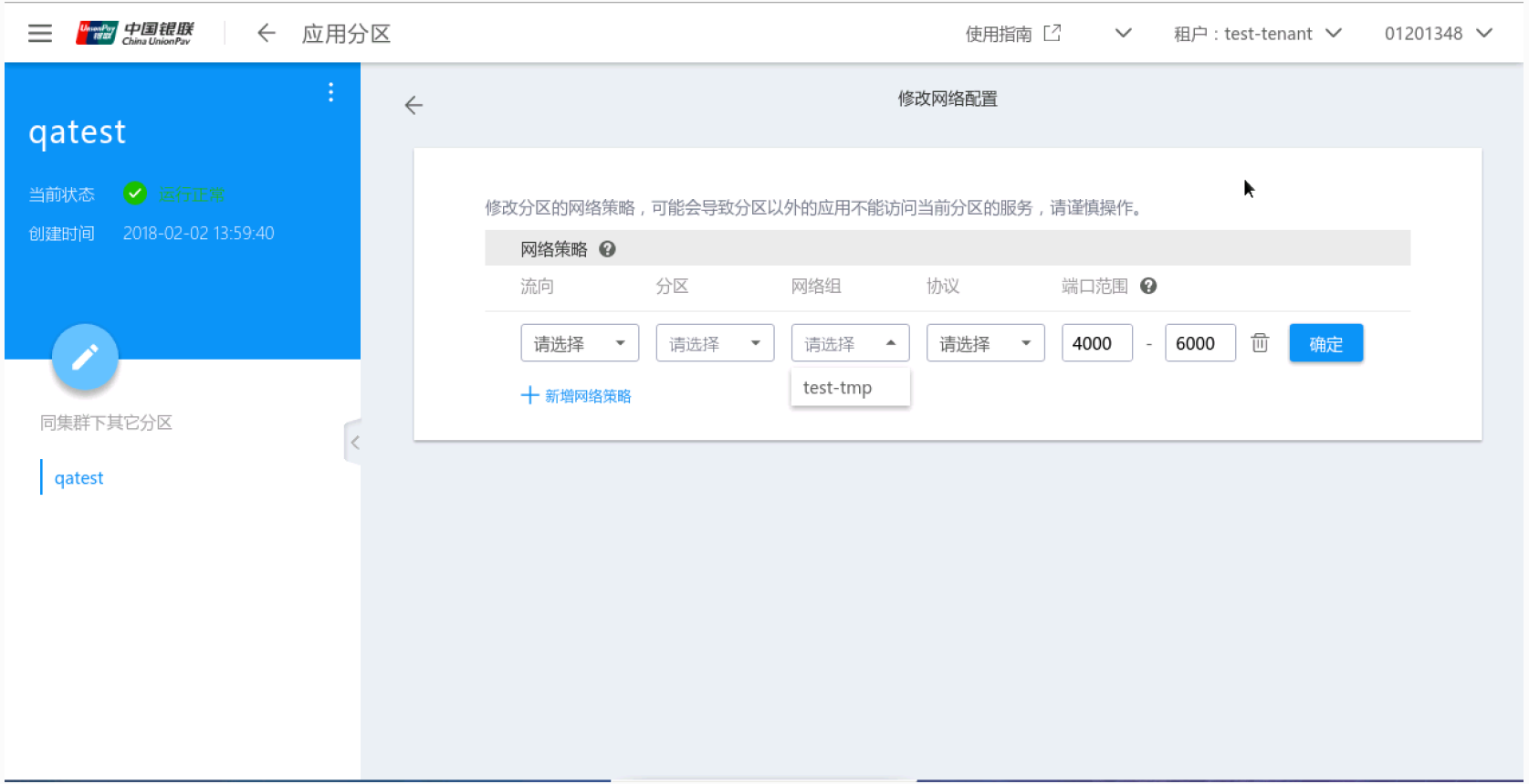
容器服务平台细节分享 – 网络对接



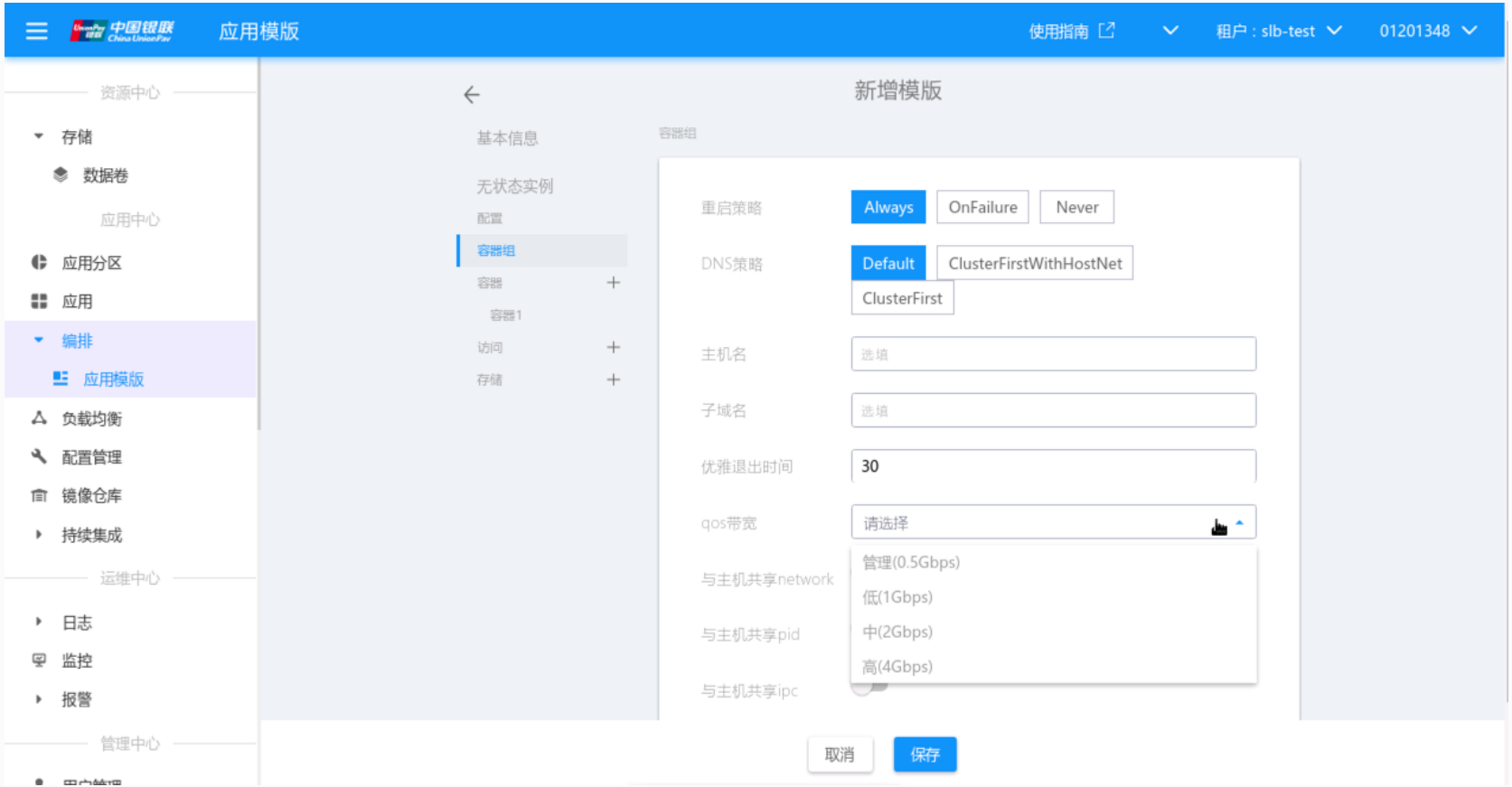
容器服务平台细节分享 – 网络对接

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

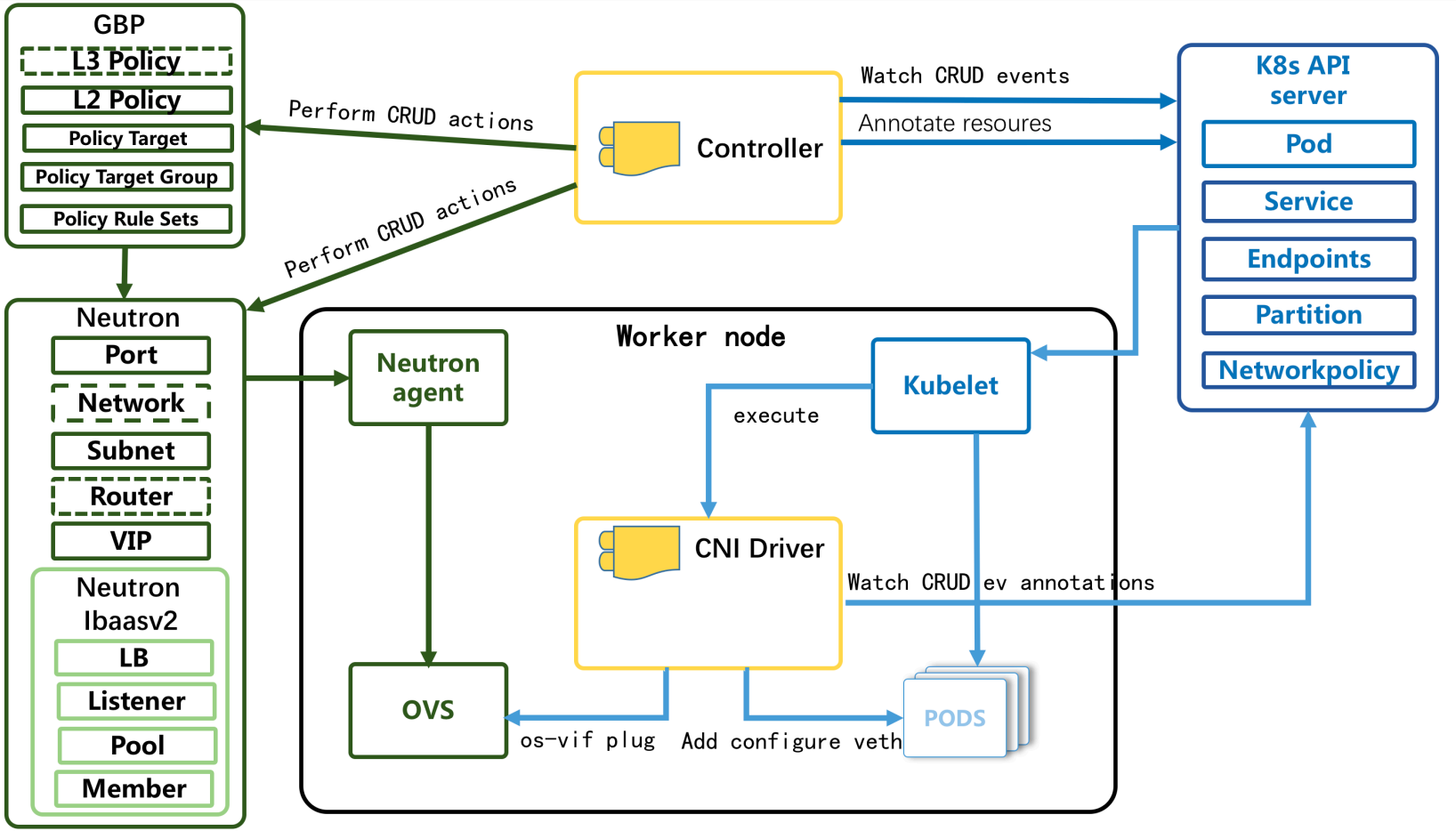
容器服务平台细节分享 – 网络策略 | 通断



容器服务平台细节分享 – 网络策略 | QOS

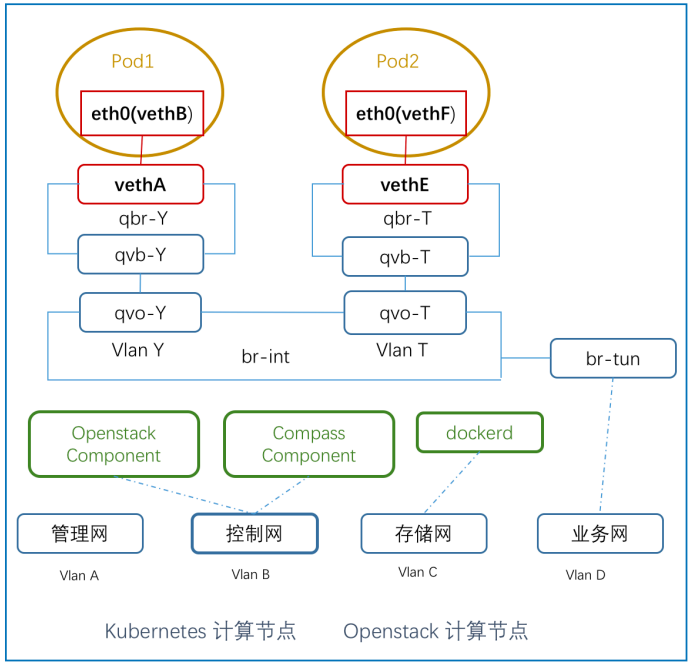


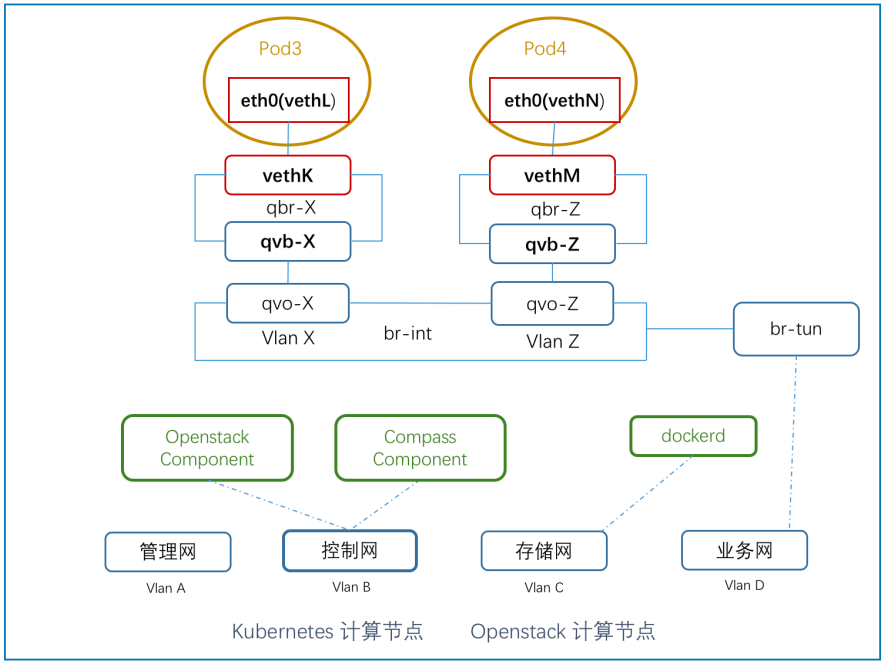
容器服务平台细节分享 – 网络对接 | 实现



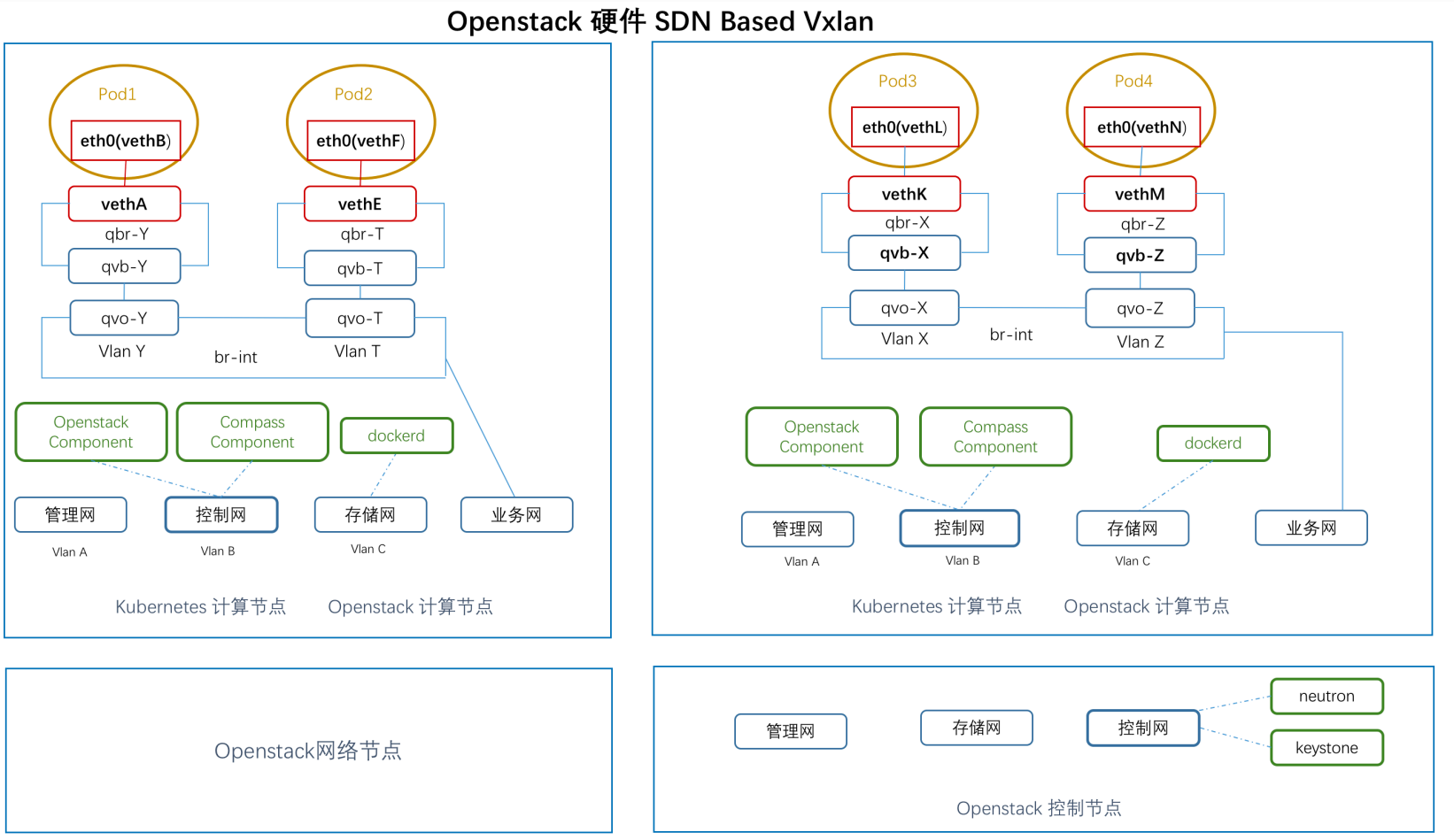
容器服务平台细节分享 – 网络对接 | 多平面

Openstack 纯软 vxlan

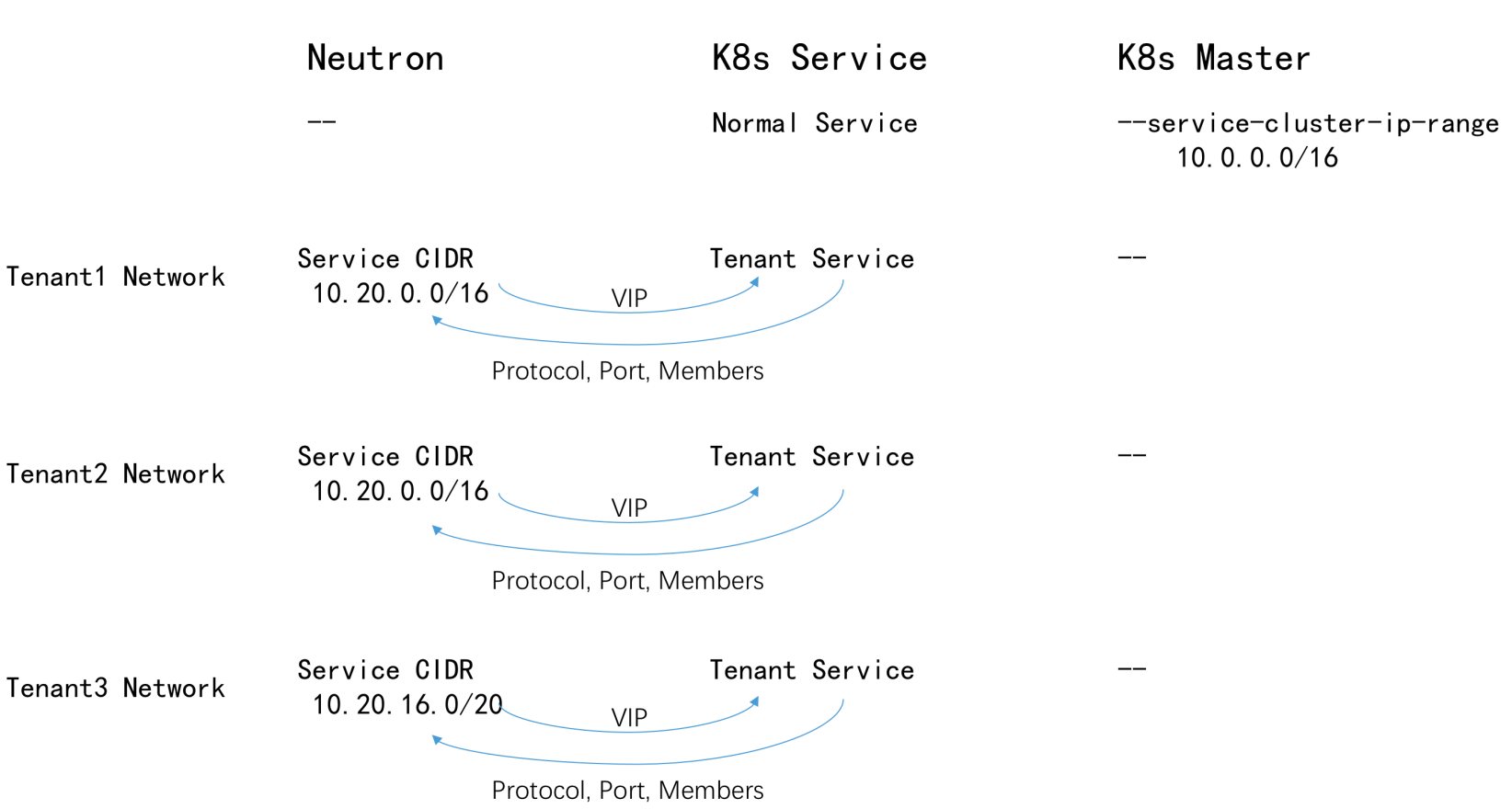




容器服务平台细节分享 – 网络对接 | 多平面

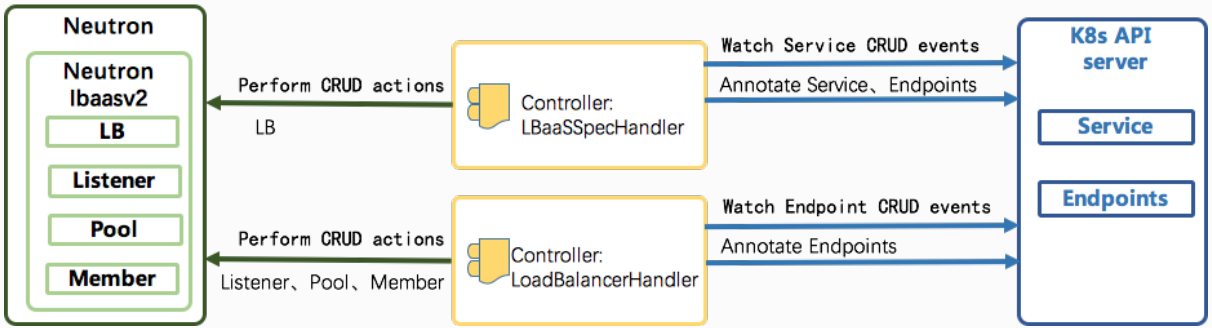


容器服务平台细节分享 – 网络对接 | LB

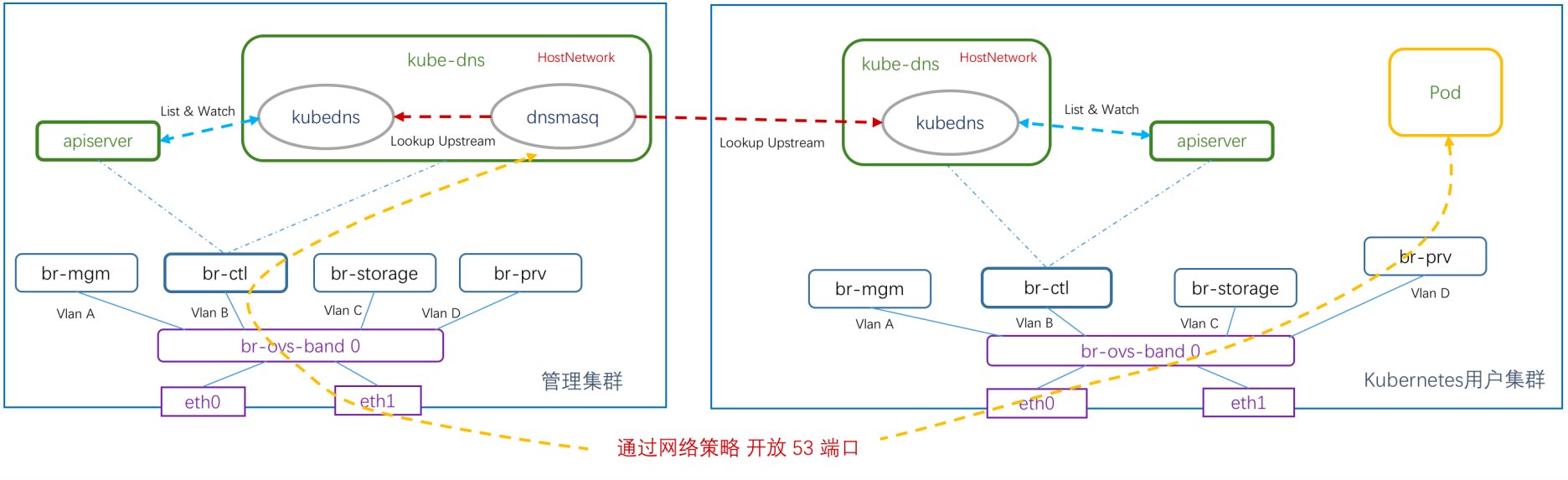


容器服务平台细节分享 – 网络对接 | LB

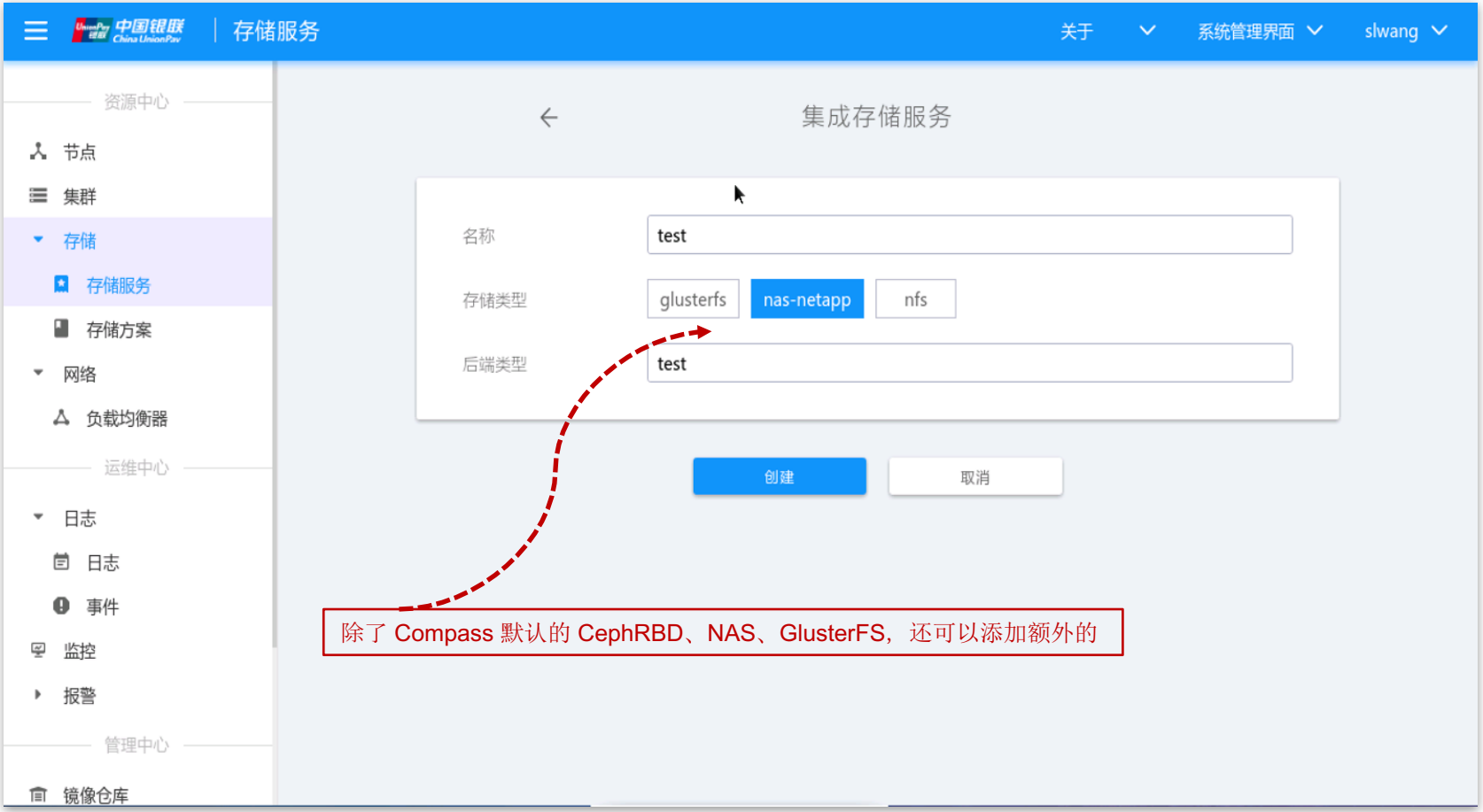
Neutron LBaaS	Kubernetes
Loadbalancer VIP	Service Cluster IP
Loadbalancer FIP	Service External IP
Protocol and Port of Listener	Protocol and Port of Service
Loadbalance Method of Member Pool	Loadbalance Method of Service/Endpoints
Members (IP, Port)	Endpoints (IP, Port)



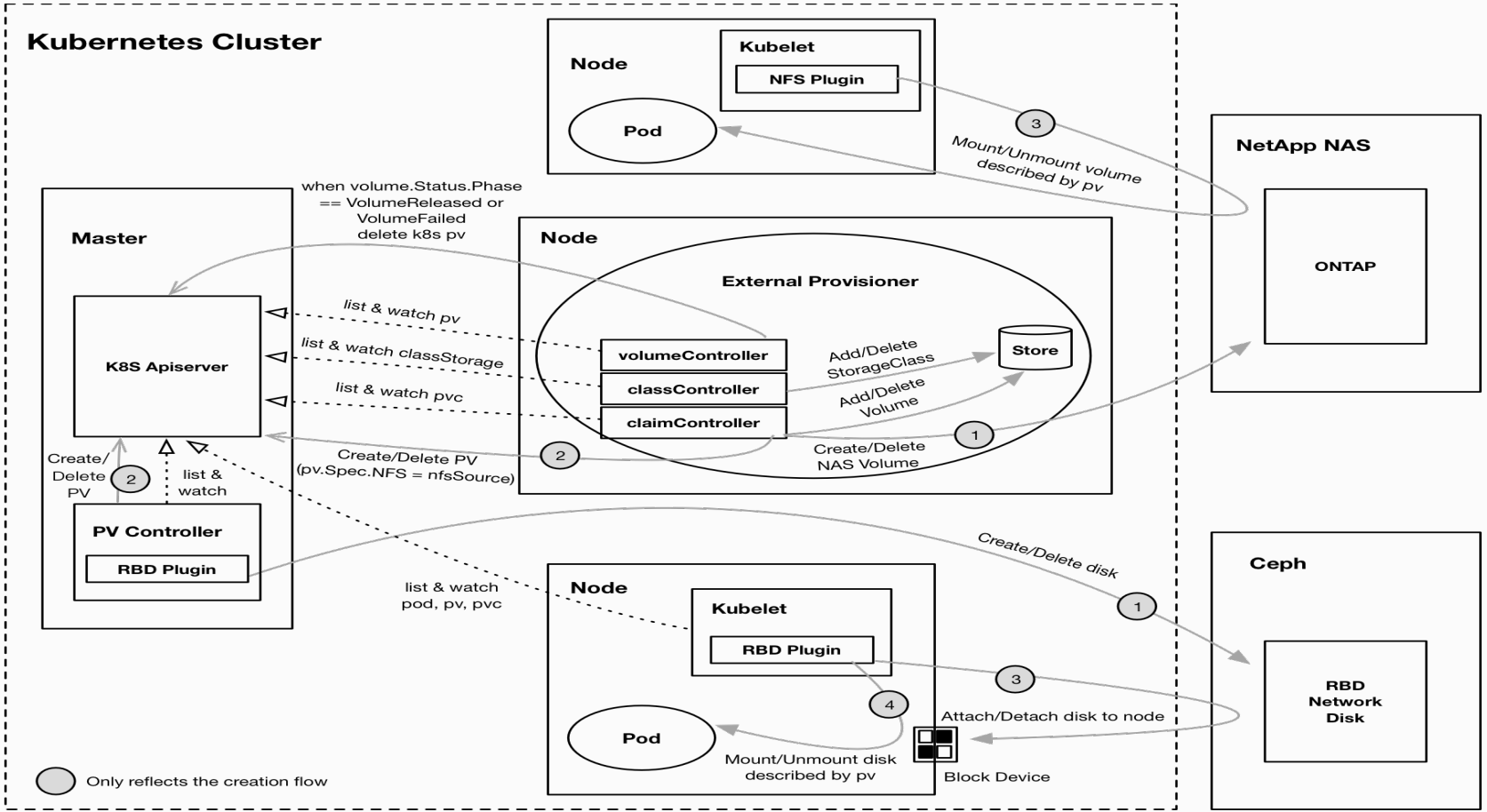
容器服务平台细节分享 – 网络对接 | 服务发现



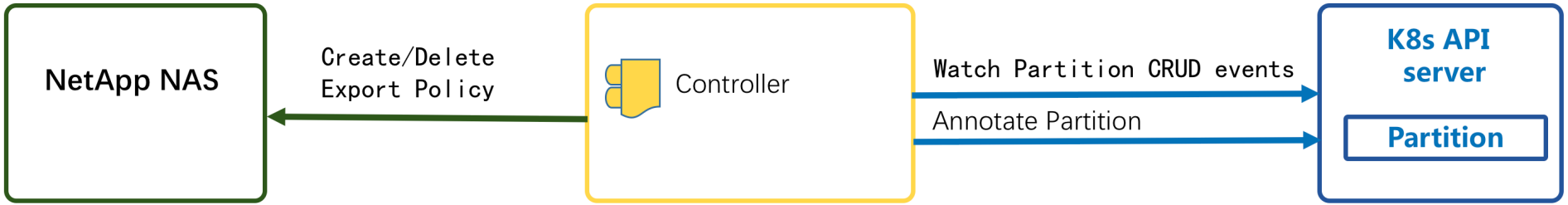
容器服务平台细节分享 – 商用存储 | NAS



容器服务平台细节分享 – 存储集成

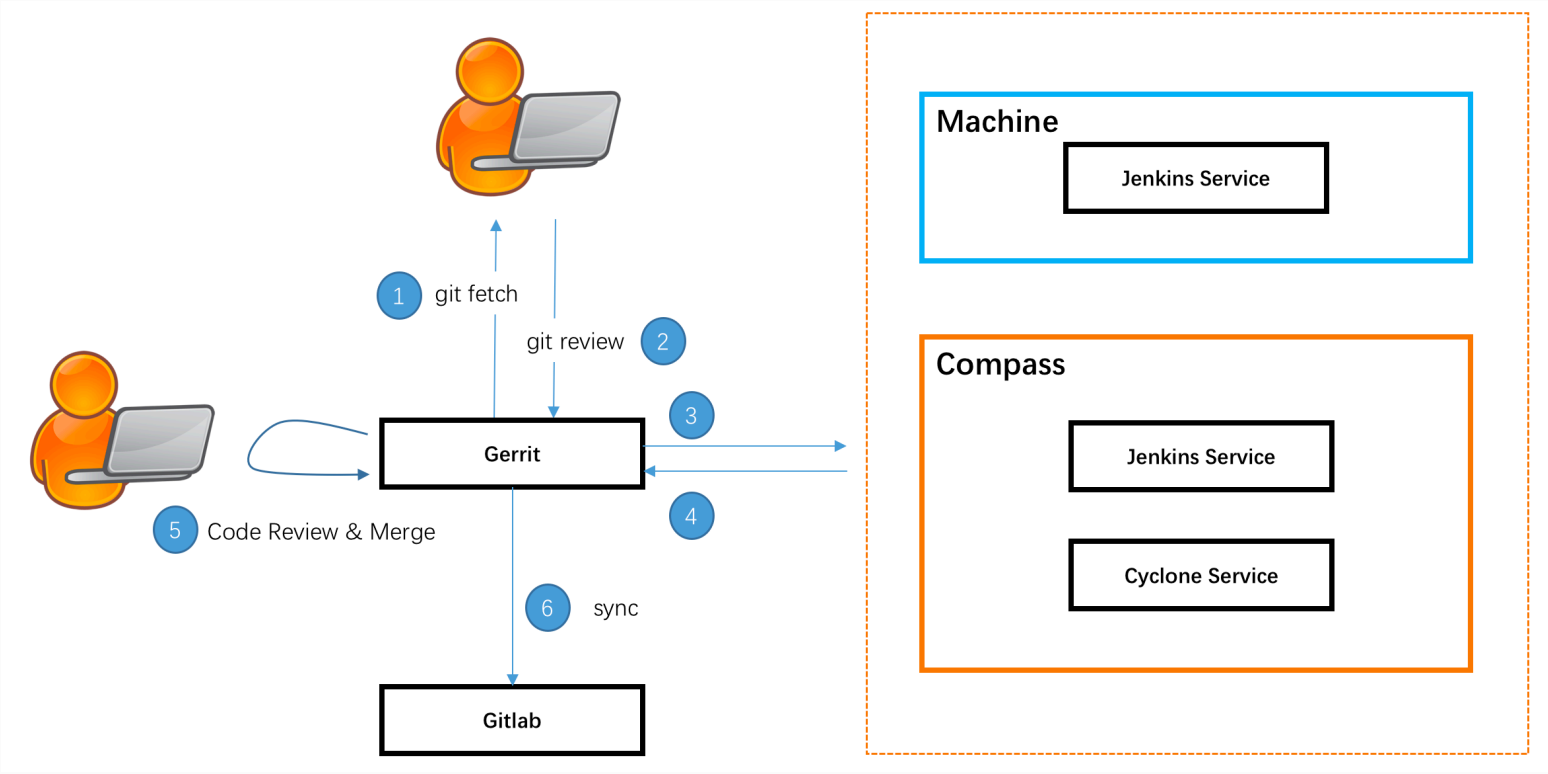


容器服务平台细节分享 – NAS 多分区隔离

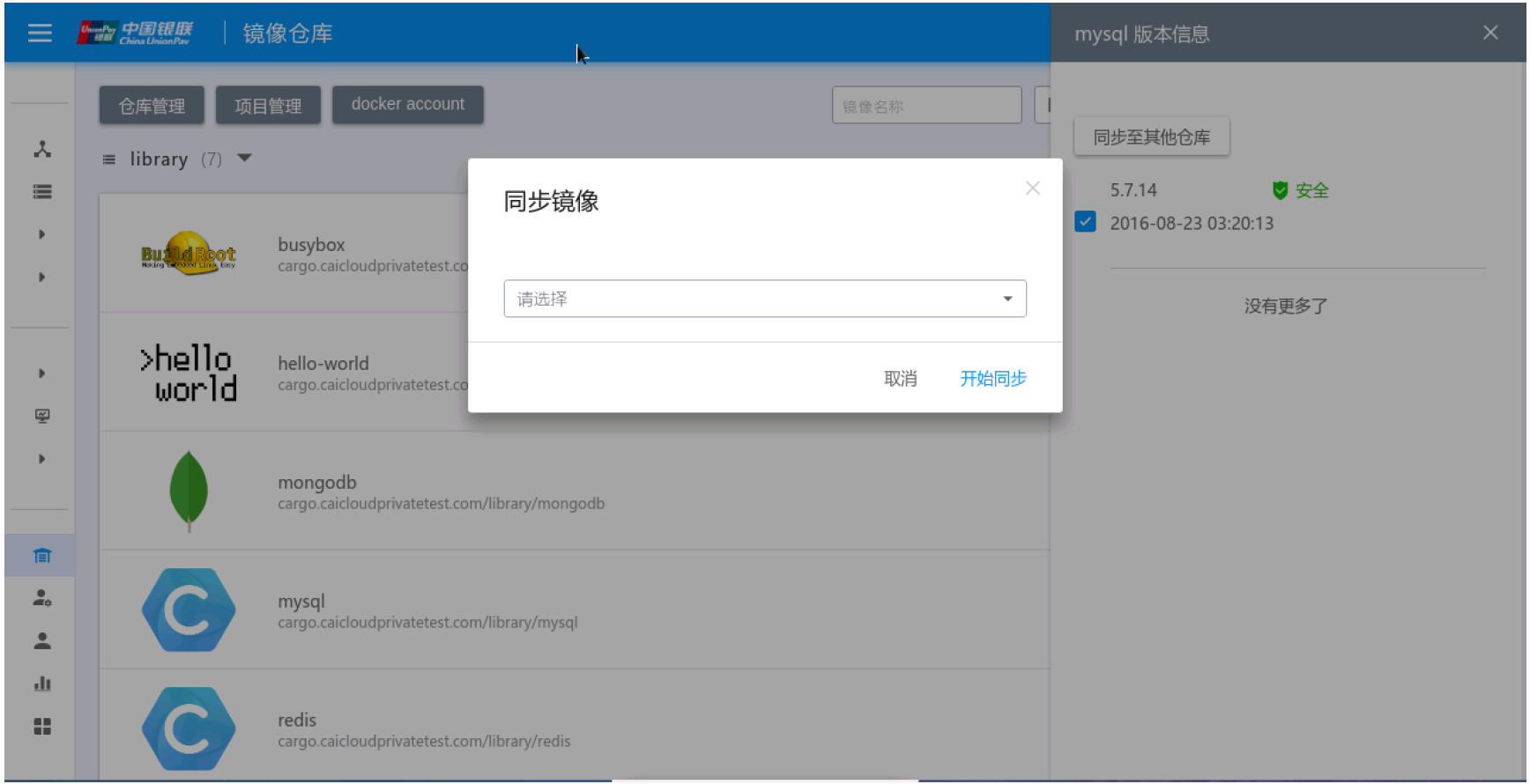


分区内创建使用 NetApp NAS 的 PVC + 分区 Export Policy → NAS 存储分区隔离

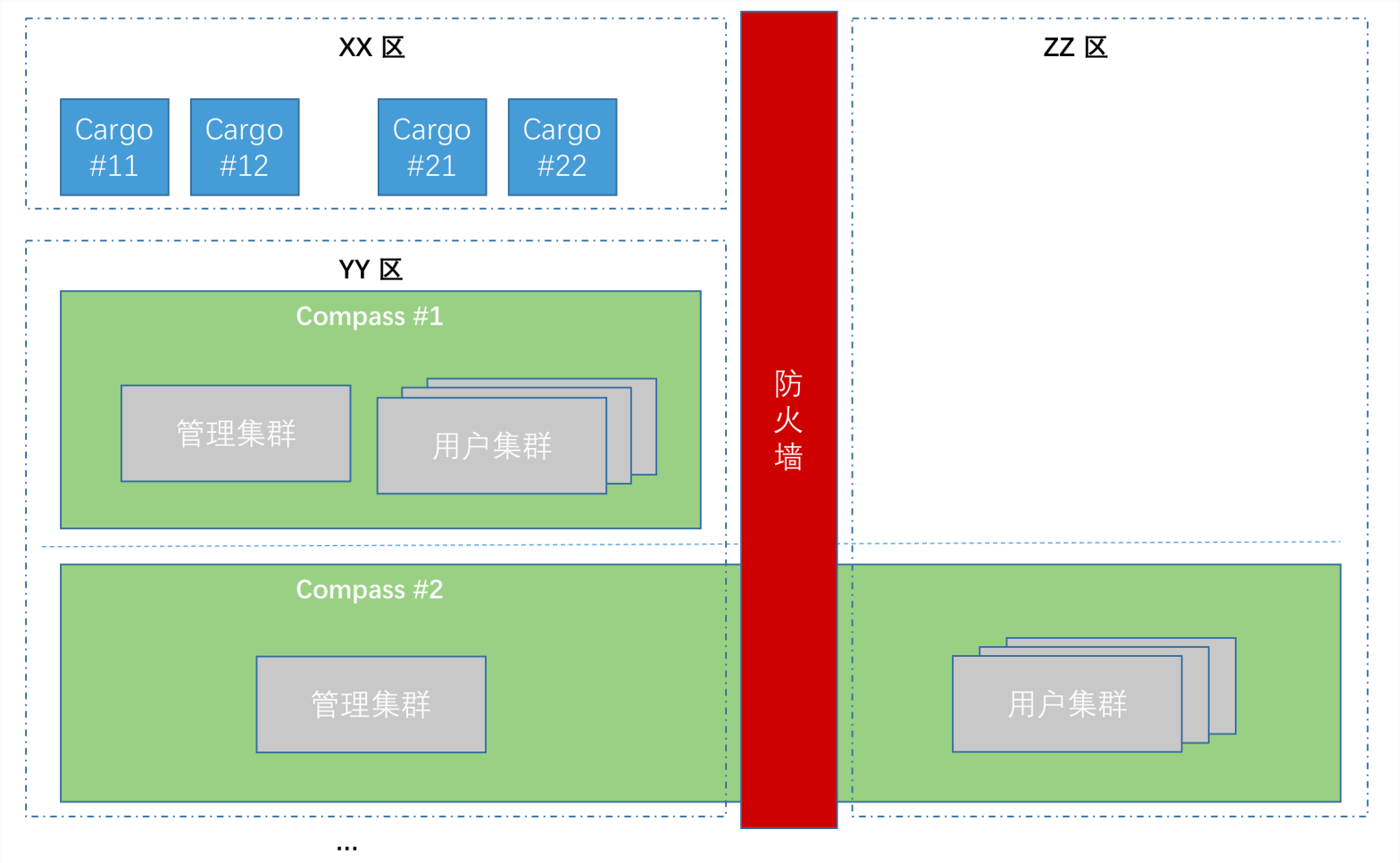
容器服务平台细节分享 – 持续集成



容器服务平台细节分享 – 持续发布



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