基于kubernetes的企业级容器云

周彩钦 | 联想PaaS团队资深工程师

2017/04/18

大纲

- 背景和挑战
- 企业级容器云设计与思考
- 让一切自动化
- 监控与日志
- Showcase
- 那些坑，那些事

背景和挑战

- IT环境比较复杂
- 集中运维模式，人少活多
- 应用类型比较复杂
- 缺少标准和规范

背景和挑战

- 内部系统演进

01 脚本化

每个项目自维护
难以规范和升级

02 工具化

抽象成工具
模板化
一键化
零散，不成体系

03 平台化

多个工具集成
最佳搭配
合力作战

背景和挑战

- 挑战

规范落地困难

系统分散，难以统一

依然不够自动化

服务割裂，申请流程

人工参与的半自动化

自服务平台

高效协作，加速迭代

资源使用率低

底层资源使用率低

背景和挑战

- 容器之道

加速交付

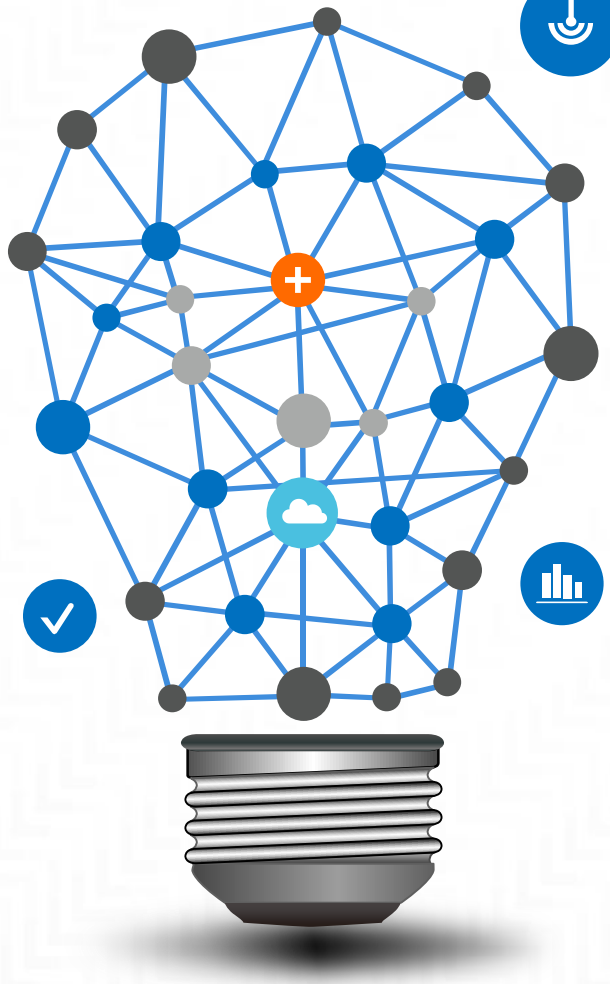
节约资源

统一规范

构建平台

企业级容器云设计与思考

- 设计思路



从需求出发

需求驱动，勿求大而全，没有银弹

从用户的角度思考

简单，学习成本低，改变成本小

从技术的角度评估

高效，稳定，可扩展

从长远技术方向考虑

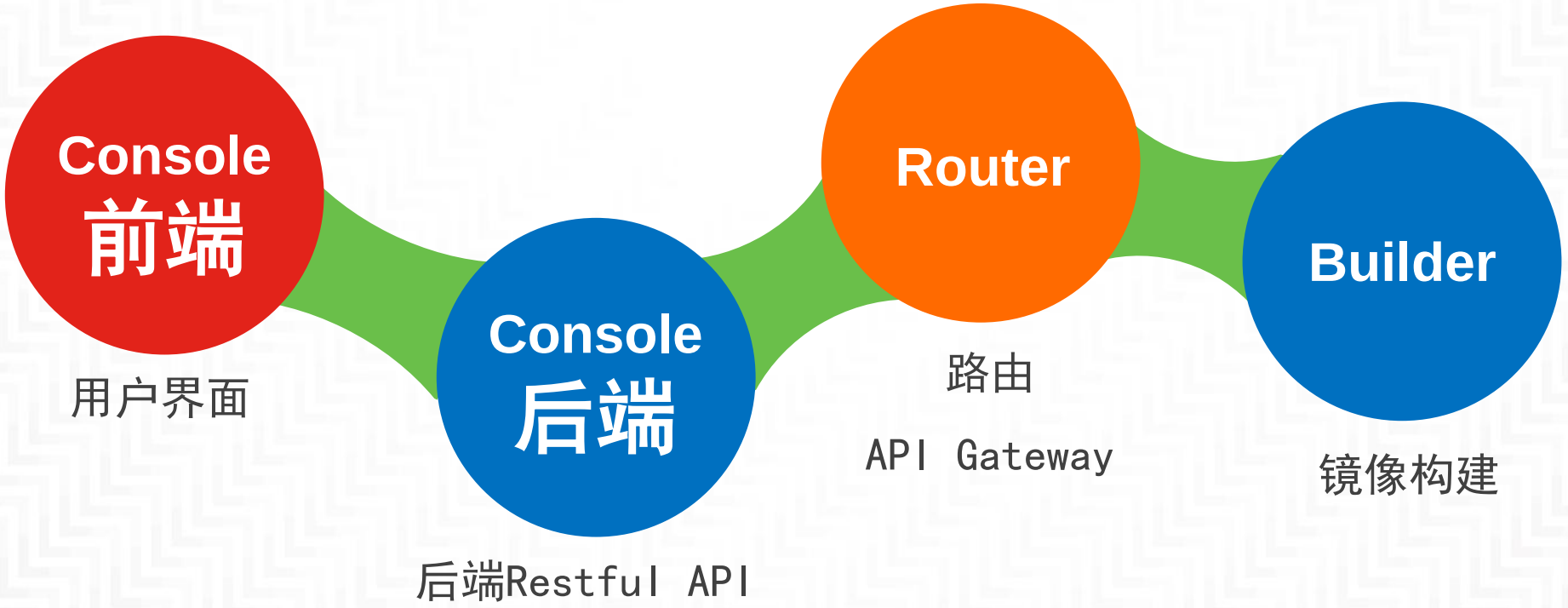
未来方向，新技术潮流，公司战略

从成本方面衡量

资源利用率，人力成本，投入产出比

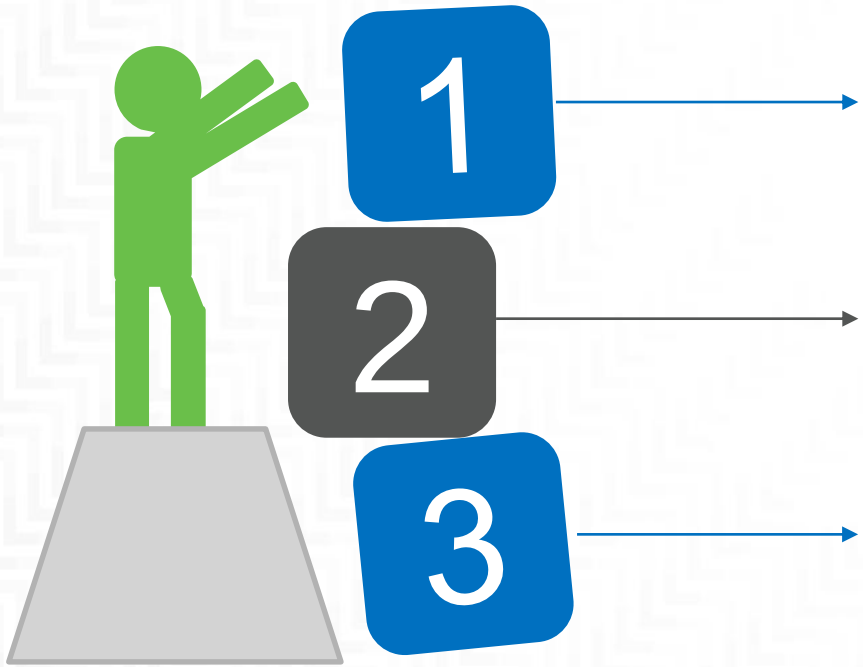
企业级容器云设计与思考

- 技术的抉择



容器云设计--多集群支持的容器云

- What?
  - 多个K8S容器云集群统一管理
- Why?



跨数据中心

技术和管理难度大

混合基础架构

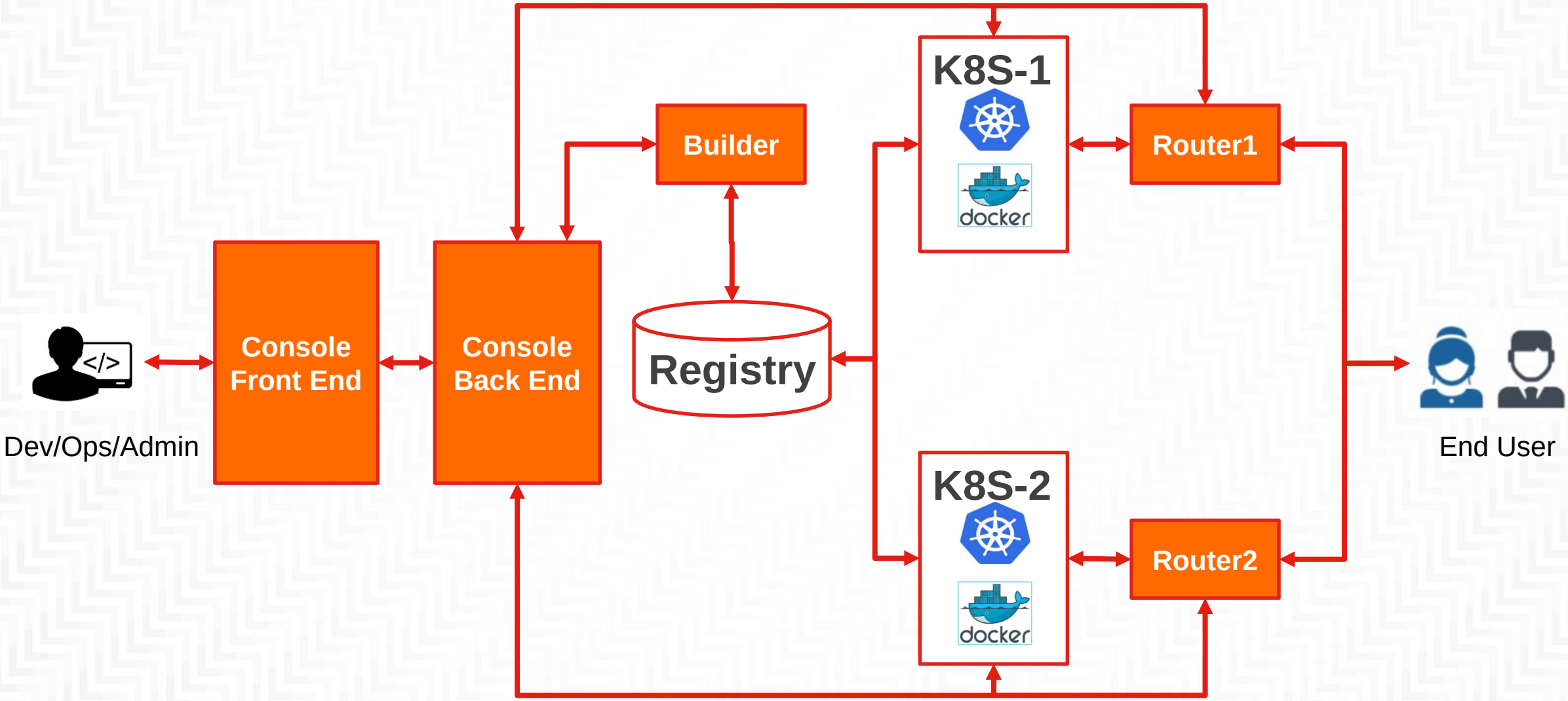
物理机，VMWare，OpenStack，AWS，Azure

统一用户体验

多集群统一管理，无需切换平台系统

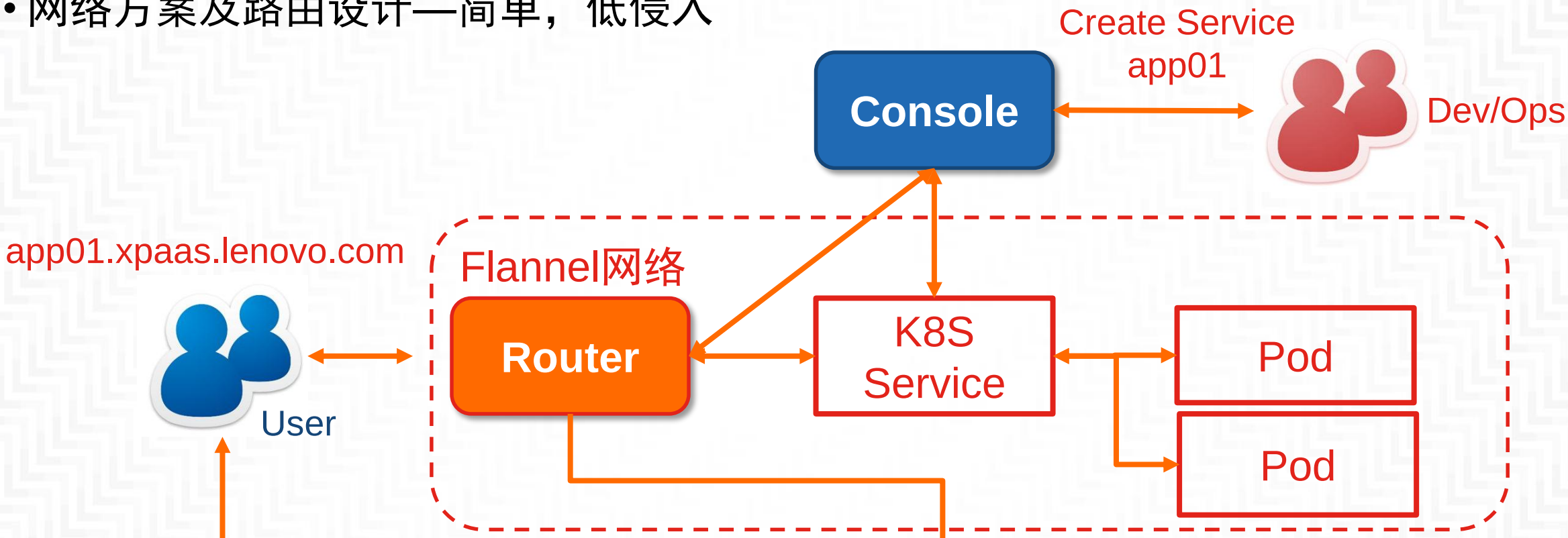
容器云设计--多集群支持的容器云

- 多集群，一平台



容器云设计—网络和路由

- 网络方案及路由设计—简单，低侵入

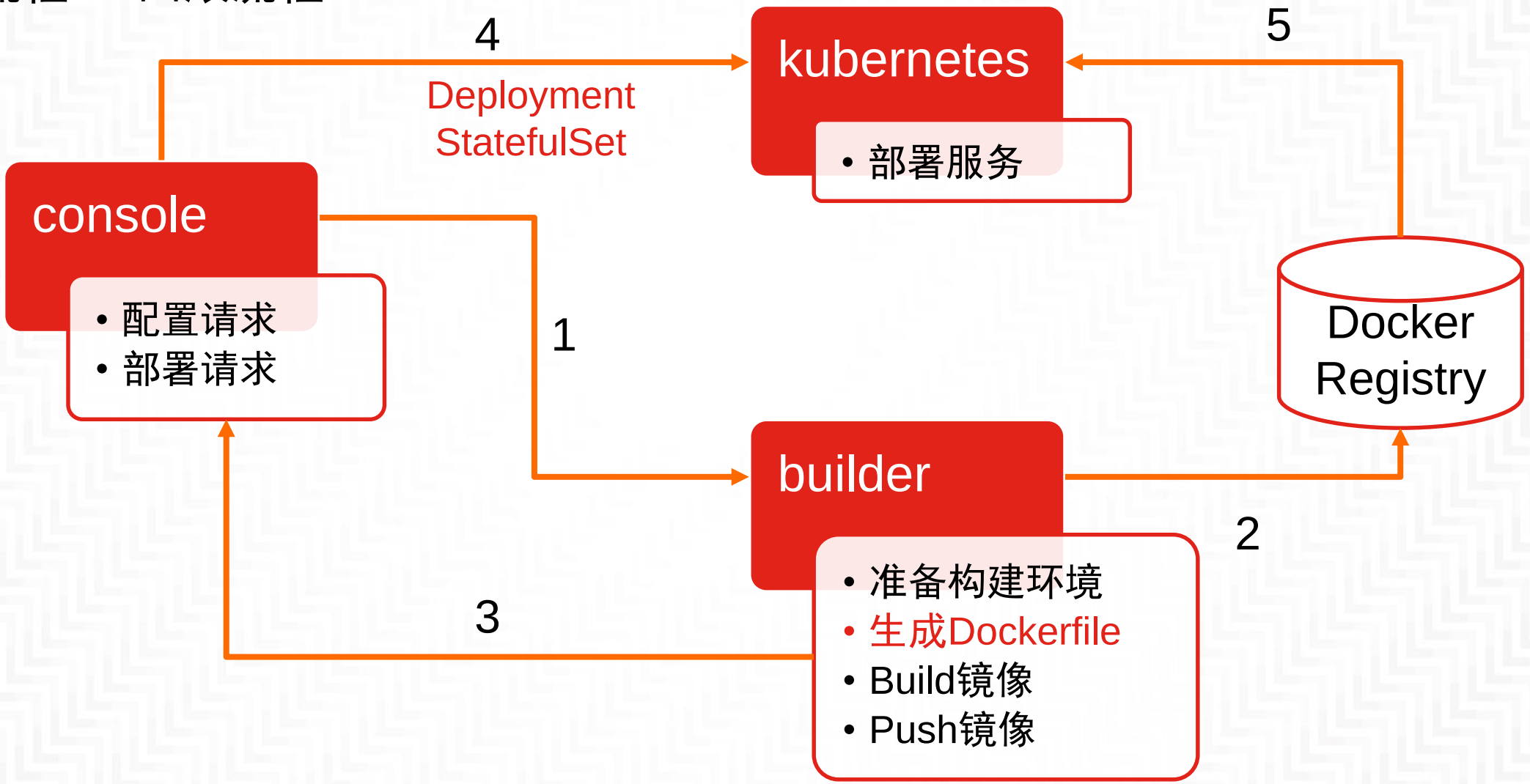


Service Name	K8S Cluster IP
app01.xpaas.lenovo.com	172.19.228.1
app02.xpaas.lenovo.com	172.19.228.2
...	...

*.xpaas.lenovo.com	Router IP

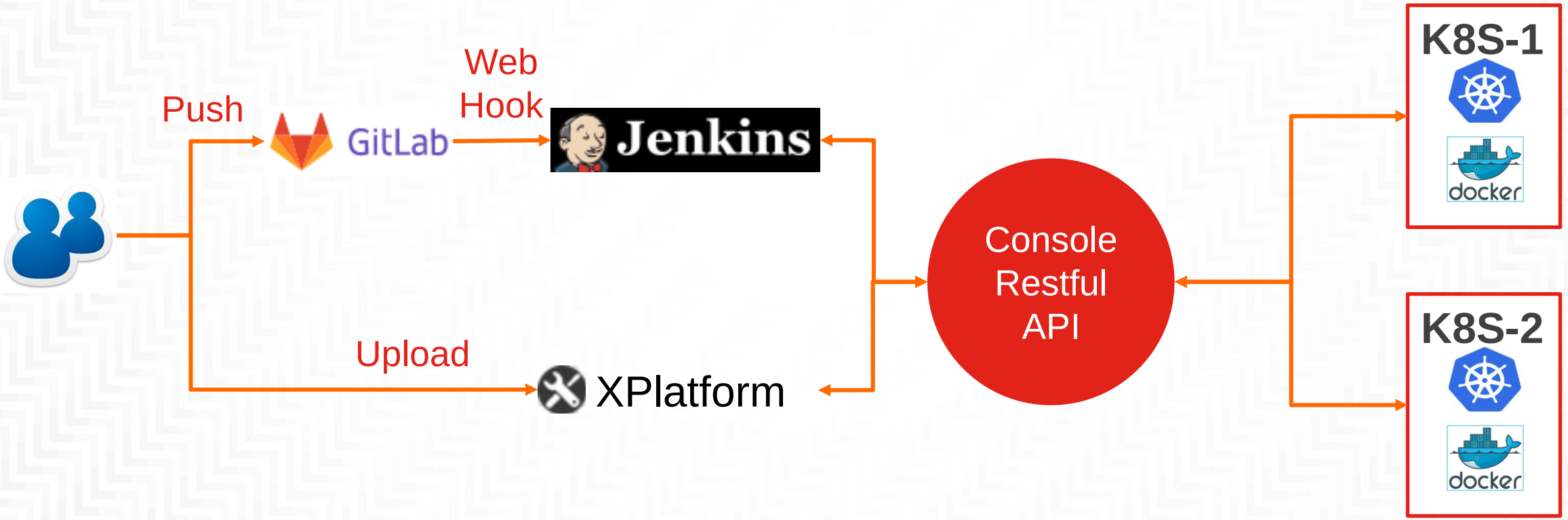
容器云设计—部署和回滚

- 部署流程 or 回滚流程



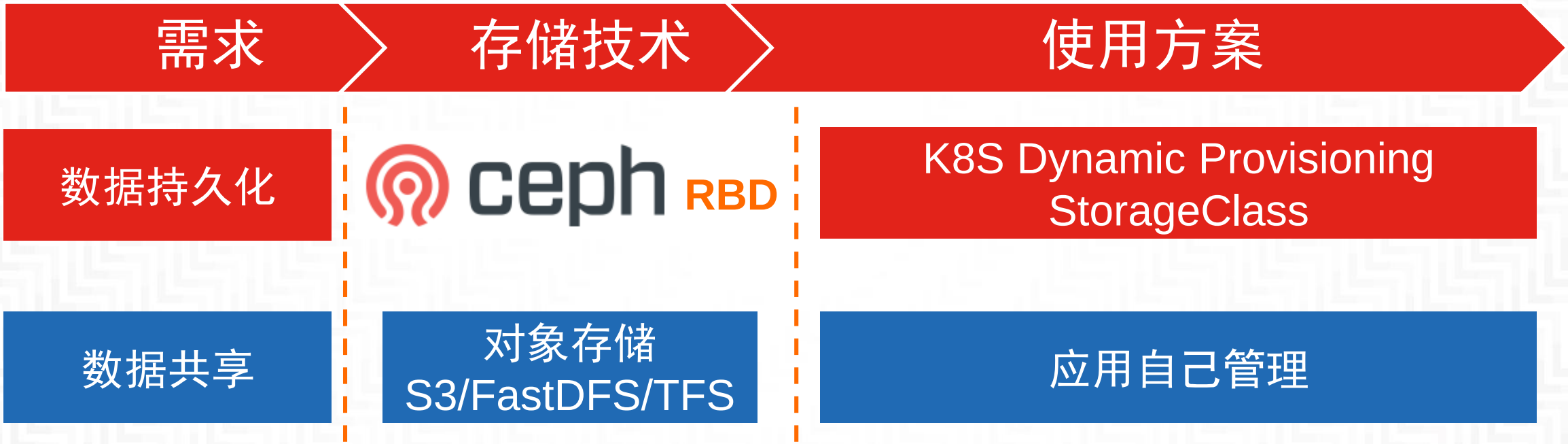
容器云设计-- DevOps的支持

- 常用DevOps工具的支持，快速融入现有开发体系



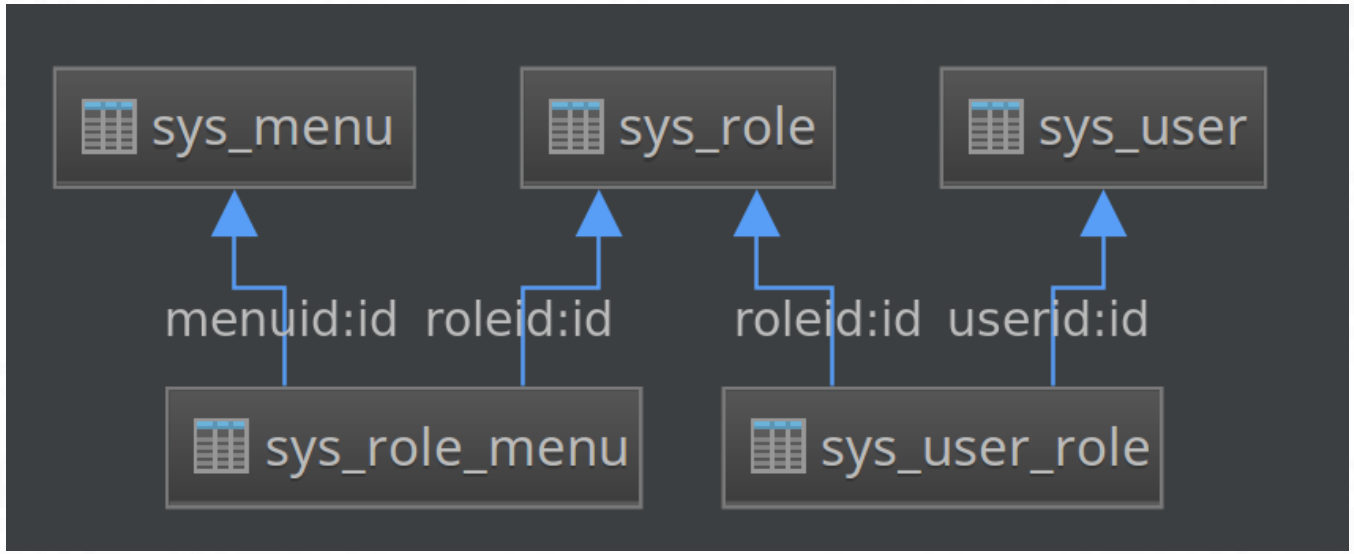
容器云设计– 存储方案

- 存储方案选择，主要给服务组件提供服务，如MySQL，Redis等



容器云设计-- 企业权限设计

- 功能权限：允许或拒绝用户使用系统提供的某个功能



功能/资源
修改系统配置
增加服务模板
创建服务

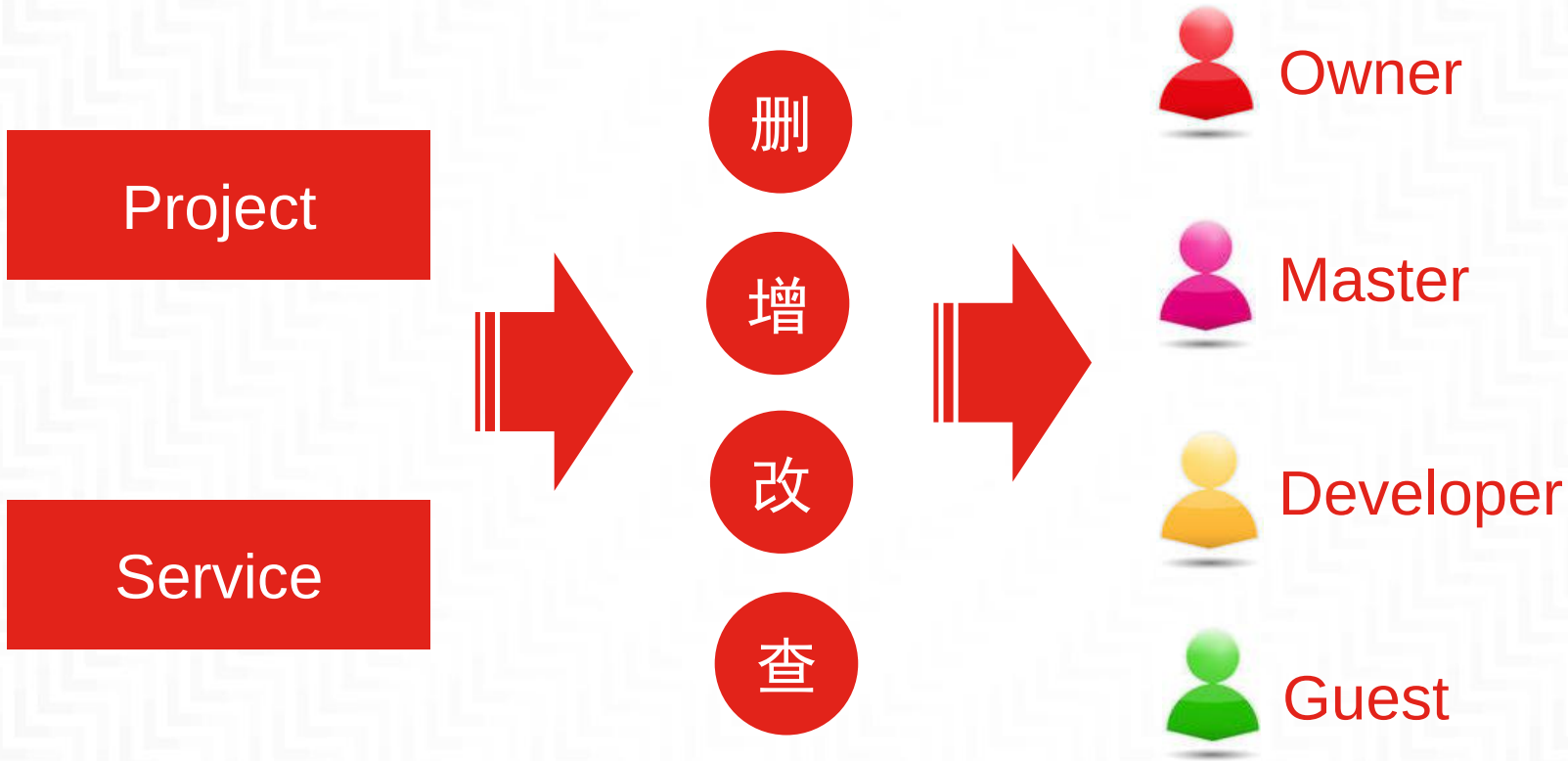
* * * *

角色
Admin
OPS
User

用户
user01
user02

容器云设计-- 企业权限设计

- 业务权限/数据权限：允许或拒绝用户进行某个数据的增删改查操作

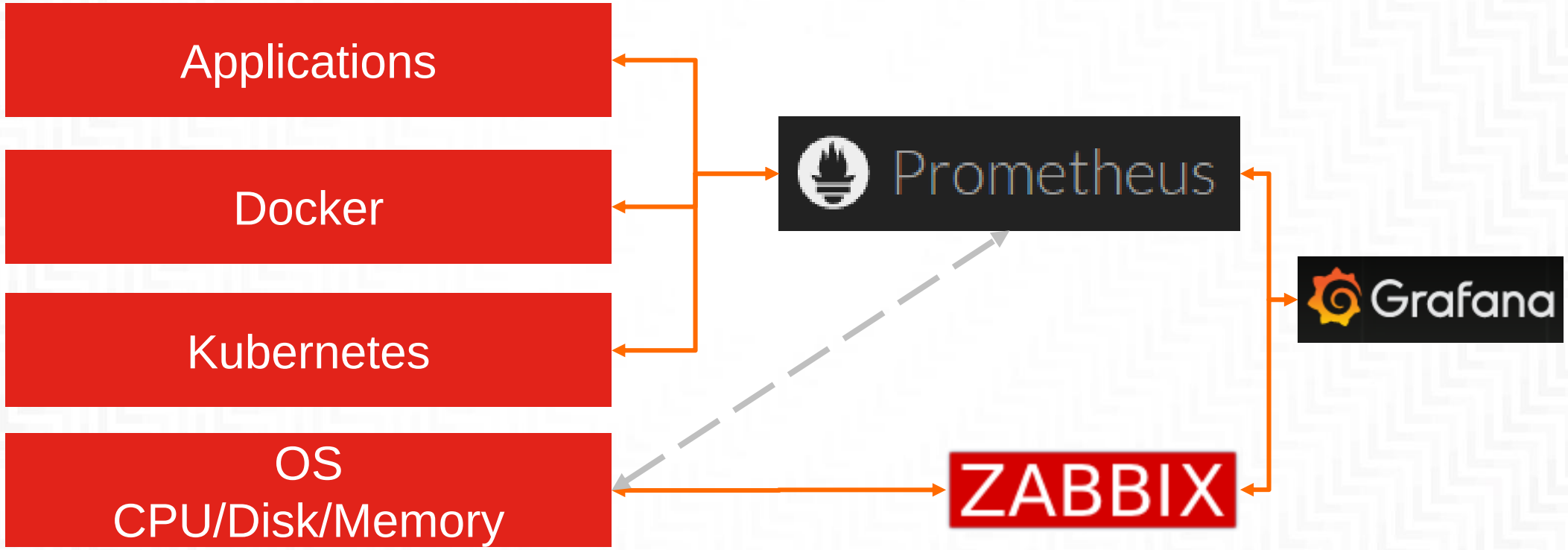


让一切自动化--工欲善其事，必先利其器

- 从设计开始之初就把自动化理念融入进来
- 充分利用Docker的优势，加速平台的迭代
- 配置即代码

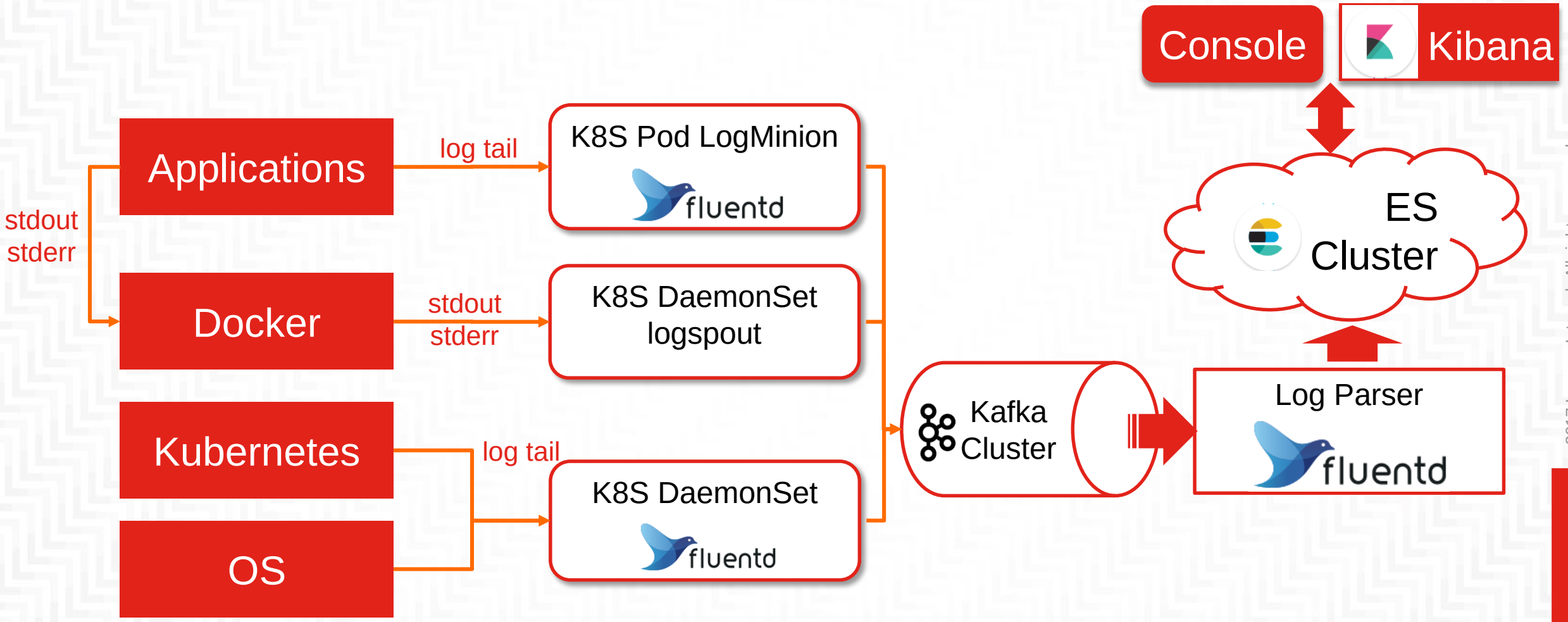
监控与日志

- 监控：传统监控+新监控平台



监控与日志

- 日志平台：多种采集手段并行

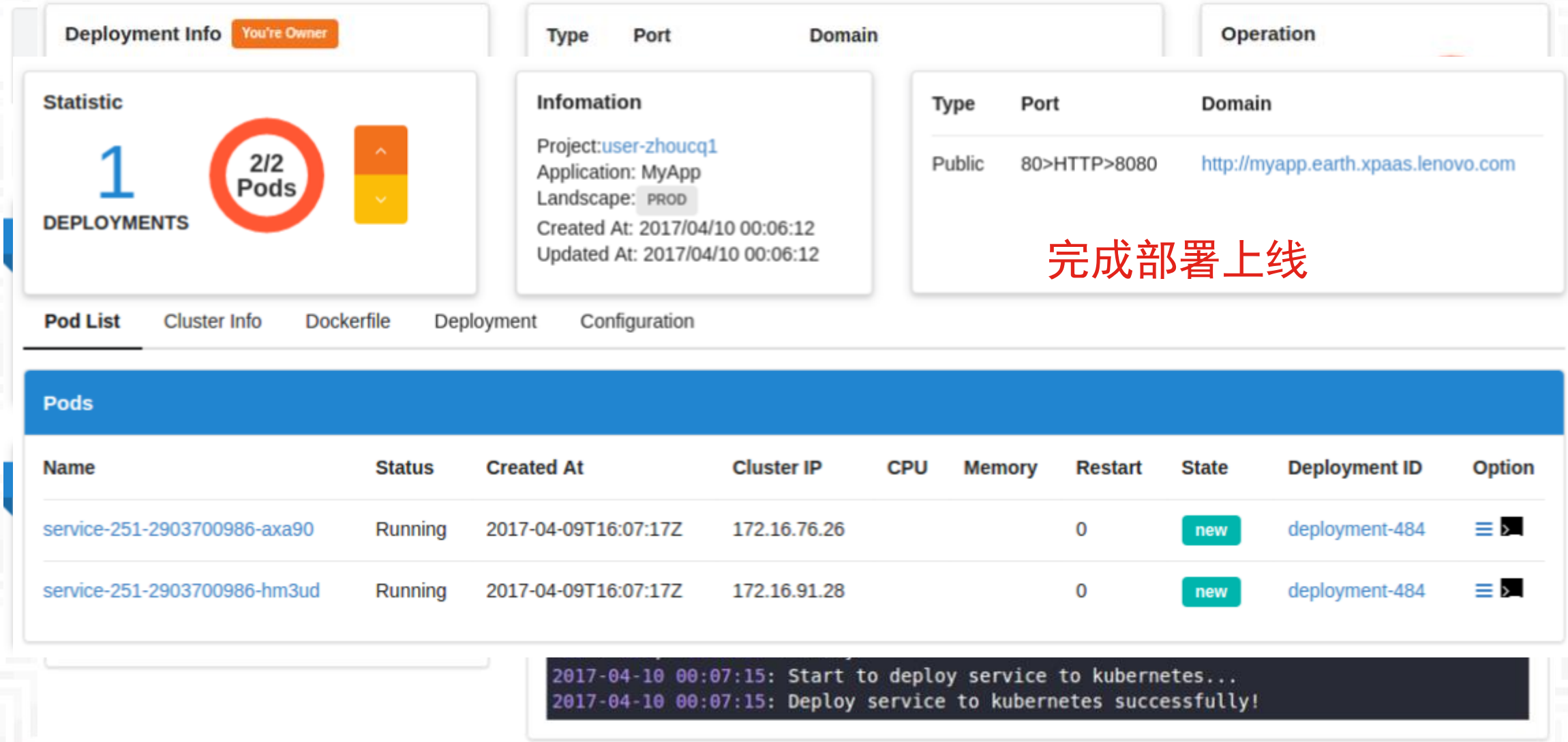


Showcase

- 平台主要功能特点
  - 多集群管理
  - 自服务式应用发布和上线部署
  - 应用快速Scale Out
  - 应用滚动更新
  - 集群容器登陆
  - 应用日志查看
  - 支持MySQL/Redis等常用组件服务市场

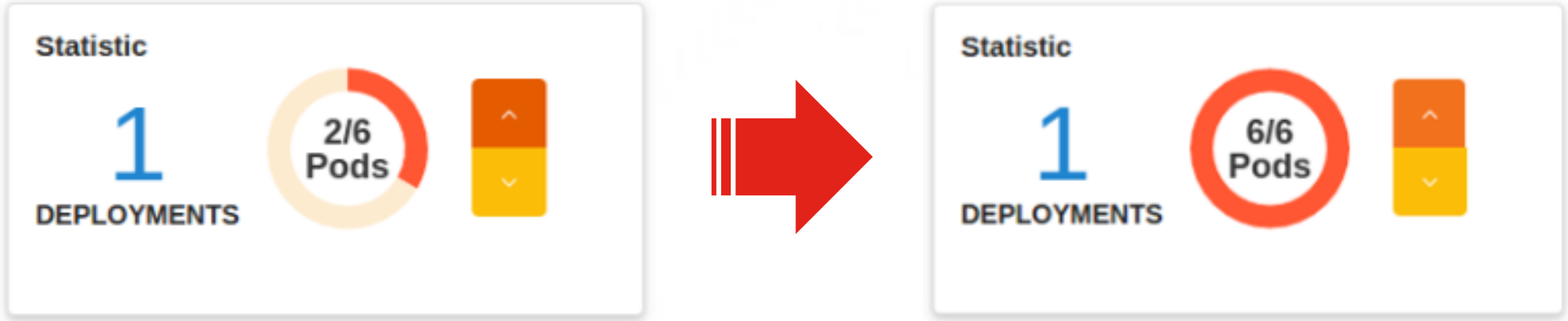
Showcase

- 部署示例：配置简单，自服务



Showcase

- Scale Out横向扩展：简单，快速



{“spec”:{ “replicas”:"6"}}

Showcase

- 滚动更新：实时查看更新进度

Pod List | Cluster Info | Dockerfile | Deployment | Configuration

Pods

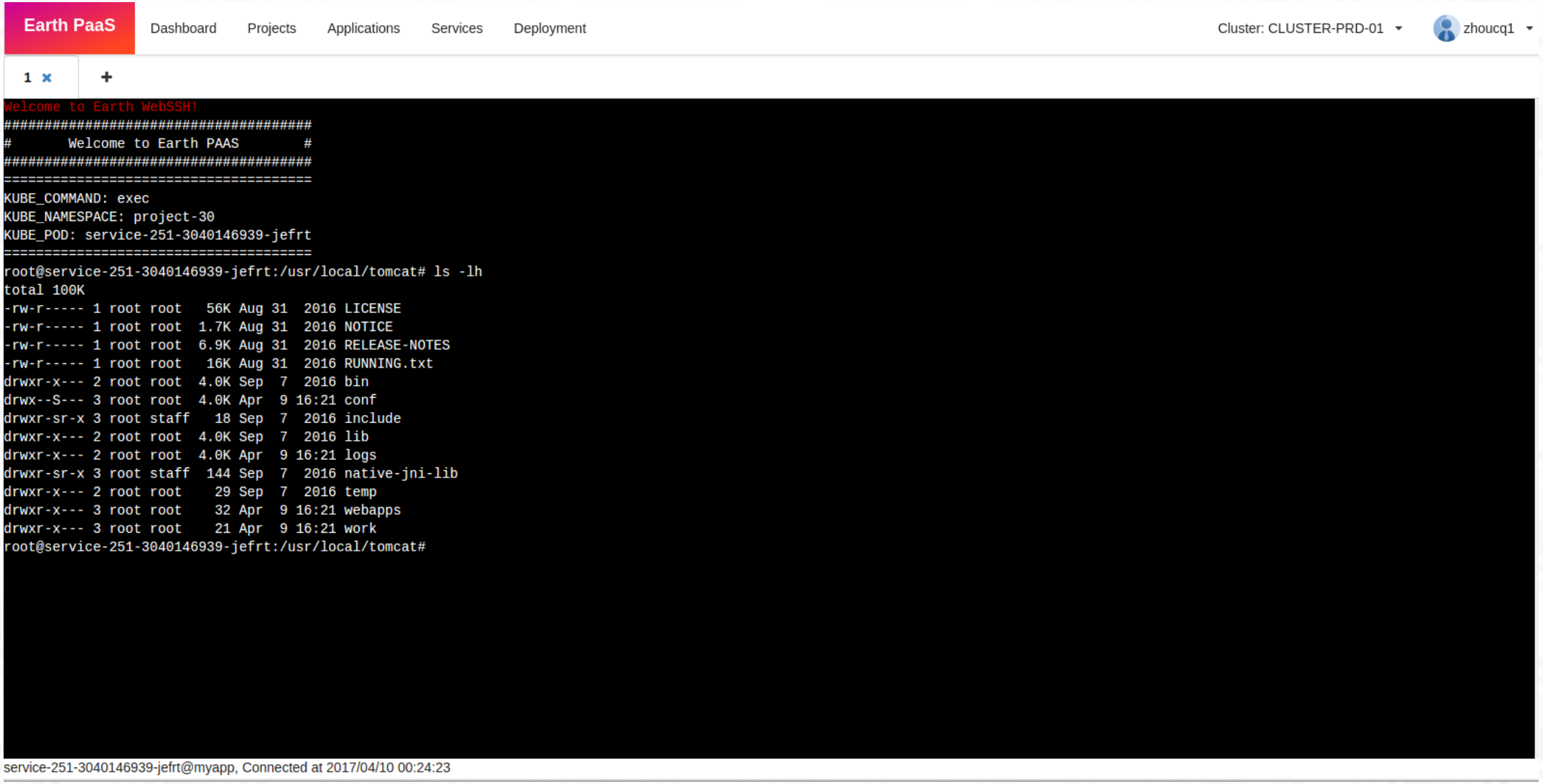
Name	Status	Created At	Cluster IP	CPU	Memory	Restart	State	Deployment ID	Option
service-253-158004328-mz50a	Running	2017-04-16T18:07:40Z	172.16.76.30			0	old	deployment-516	
service-253-158004328-q5fqo	Running	2017-04-16T18:08:30Z	172.16.77.11			0	old	deployment-516	
service-253-293925993-dk6zu	Running	2017-04-16T18:09:50Z	172.16.91.2			0	new	deployment-517	

Pods

Name	Status	Created At	Cluster IP	CPU	Memory	Restart	State	Deployment ID	Option
service-253-293925993-a1dhx	Running	2017-04-16T18:10:00Z	172.16.77.3			0	new	deployment-517	
service-253-293925993-dk6zu	Running	2017-04-16T18:09:50Z	172.16.91.2			0	new	deployment-517	

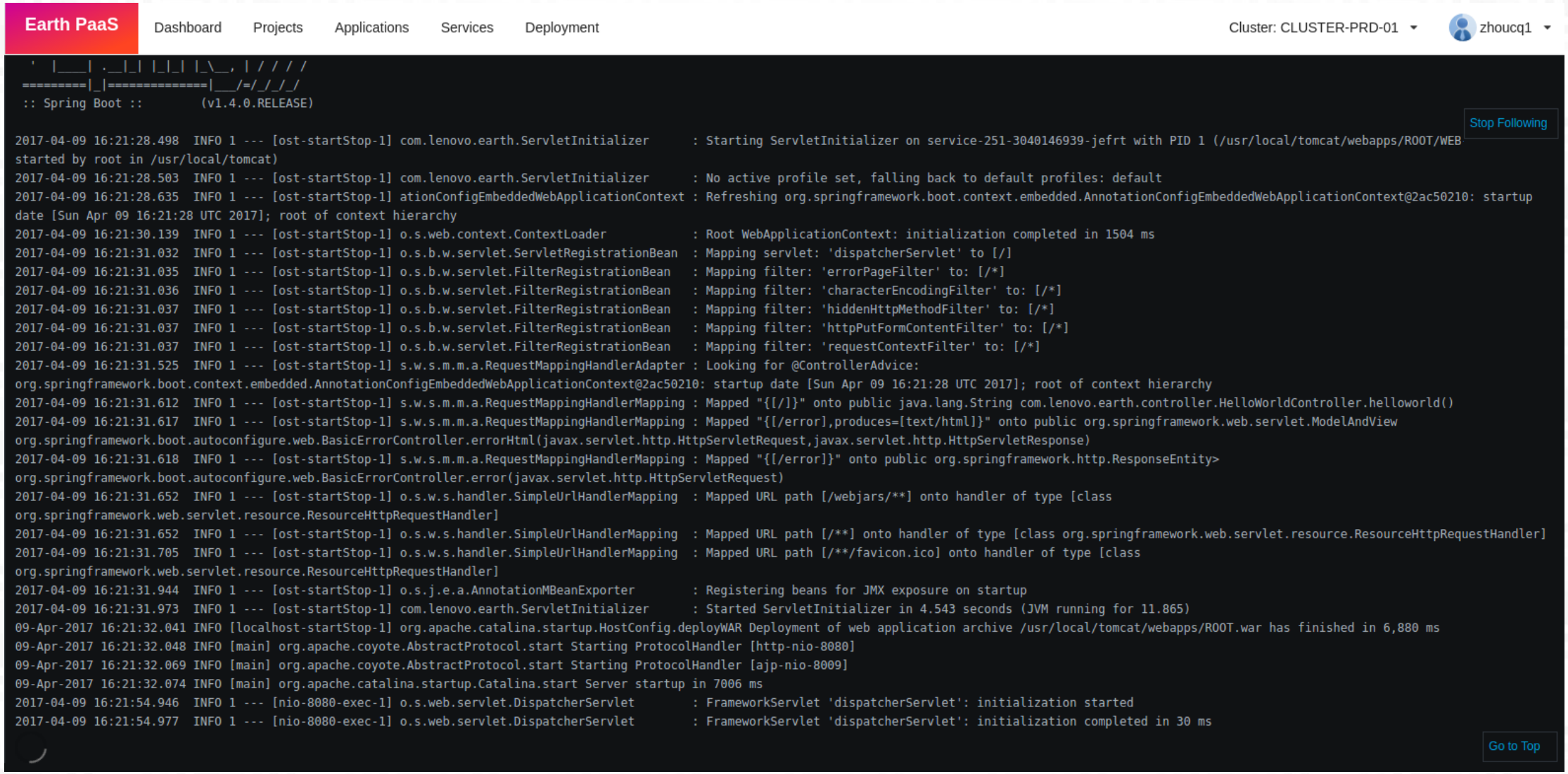
Showcase

- 容器访问：使用exec的api，通过websocket提供web终端



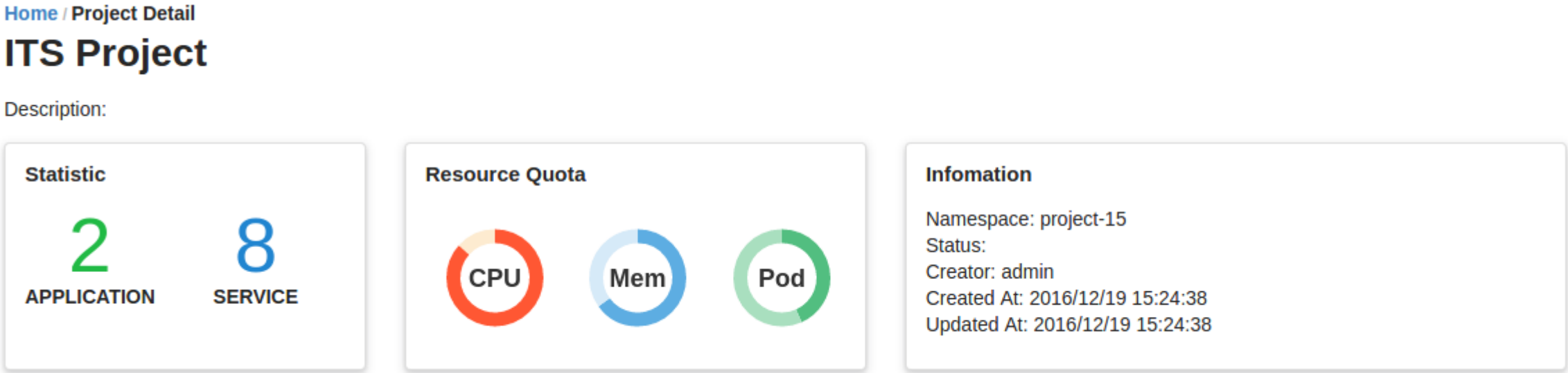
Showcase

- 日志查看：实时查看应用日志



Showcase

- 资源管理：项目级别的资源控制



那些坑，那些事

- **底层平台的那些坑**
  - K8S Deployment ID出现重复，导致部署后不更新应用 https://github.com/kubernetes/kubernetes/issues/29735
  - K8S Dashboard卡顿的问题
  - harbor服务器重启后出现mysql无主进程

- **平台开发的那些事**
  - 平台健壮性：当服务器频繁挂掉的时候，才知道现实和理想的距离
  - Angular2出新版本了，更还是不更

小结

- 背景和挑战
- 企业级容器云设计与思考
  - 设计思路
  - 多集群支持和整体架构
  - 网络方案和路由设计
  - 部署、回滚流程
  - DevOps支持
  - 存储方案
  - 权限设计
- 通过Ansible让运维自动化
- 监控与日志
- Showcase，系统流程示例
- 踩过的坑

zhoucq1@lenovo.com
caiqinzhou@gmail.com