



中国移动容器实践之路

2018 中国·北京

2018 DevOpsDays · 北京站



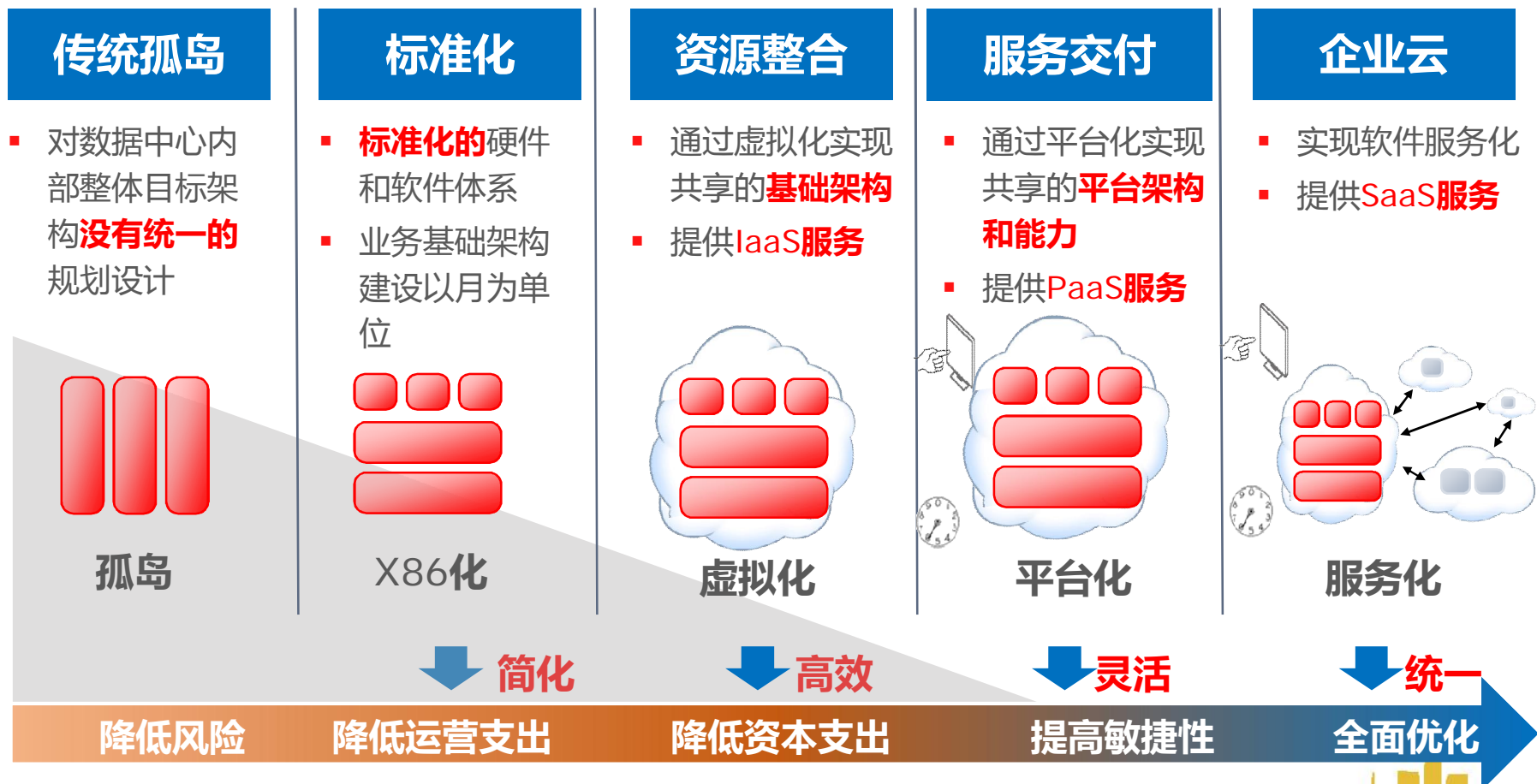


目录

- 1 研发背景
- 2 BC-PaaS架构、模块介绍
- 3 实践之展示
- 4 实践之经验



研发背景





研发背景 - 问题

- 资源静态划分，资源利用效率低
- 部署效率低下，无法满足业务的快速上线
- 应用弹性扩缩能力不足，应对互联网模式的业务能力不足
- 缺少业务生命周期统一管理的模式

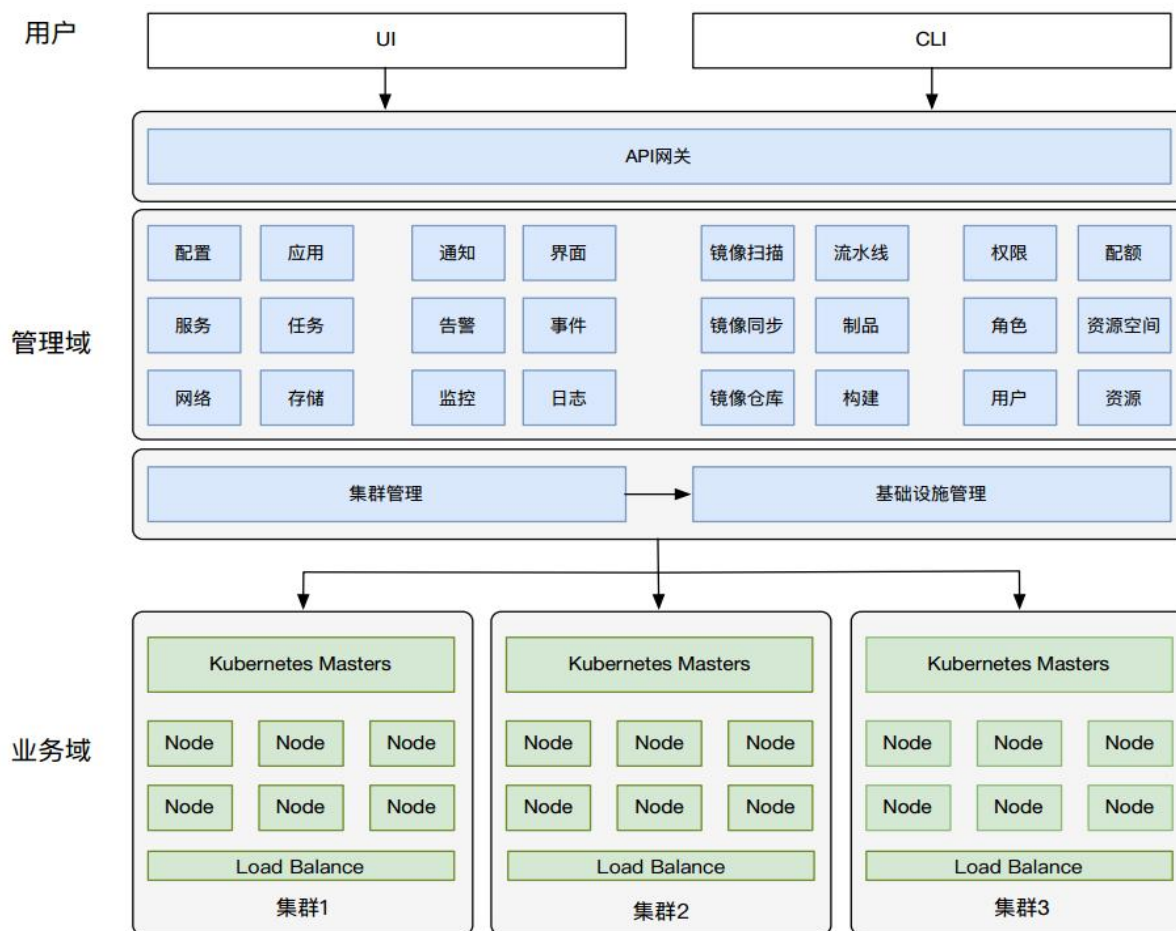


研发背景 - 选型

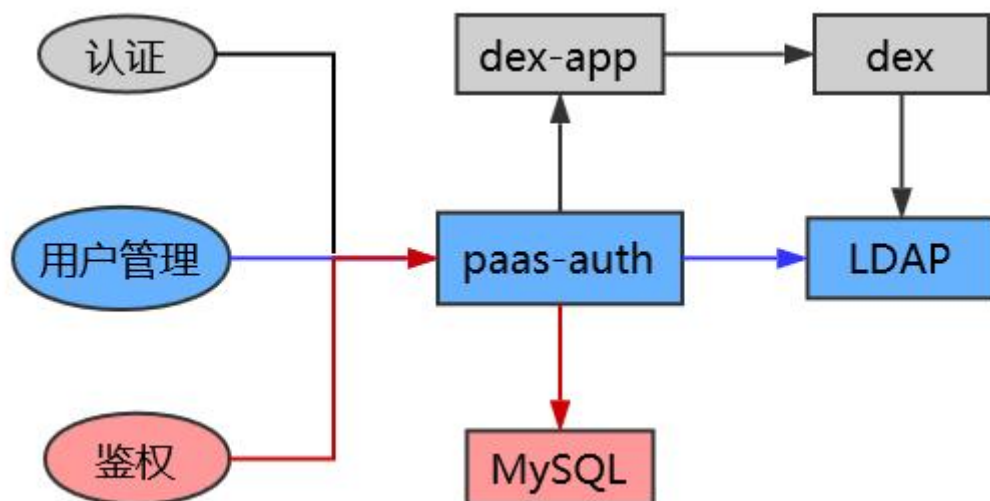
对比项	Mesos	Kubernetes
社区	Apache，活跃程度一般	CNCF，活跃程度高
定位	Mesos只分配集群计算资源，不负责任务调度。	DCOS，面向应用本身即可做资源管理，又可做应用编排
入门	Mesos入门较高，需要定制化的功能较多	Kubernetes概念较多，学习成本较大，但原生支持任务编排，不需要第三方任务管理器，开箱可用
用户群	国外有Airbnb, Apple, Uber, Twitter，国内有携程，爱奇艺在使用。	Aporeto, Apprenda, Aqua, Citrix, Coreos, Deis, Redhat, Mirantis, Rancher



BC-PaaS – 架构



BC-PaaS – 用户



➤ dex：使用OpenID连接方式，支持各种后端对接，可连接LDAP、MySQL、GitHub等，提供认证服务的一个组件。

➤ dex-app：一个OAuth2的Client，连接普通用户与dex的使用。

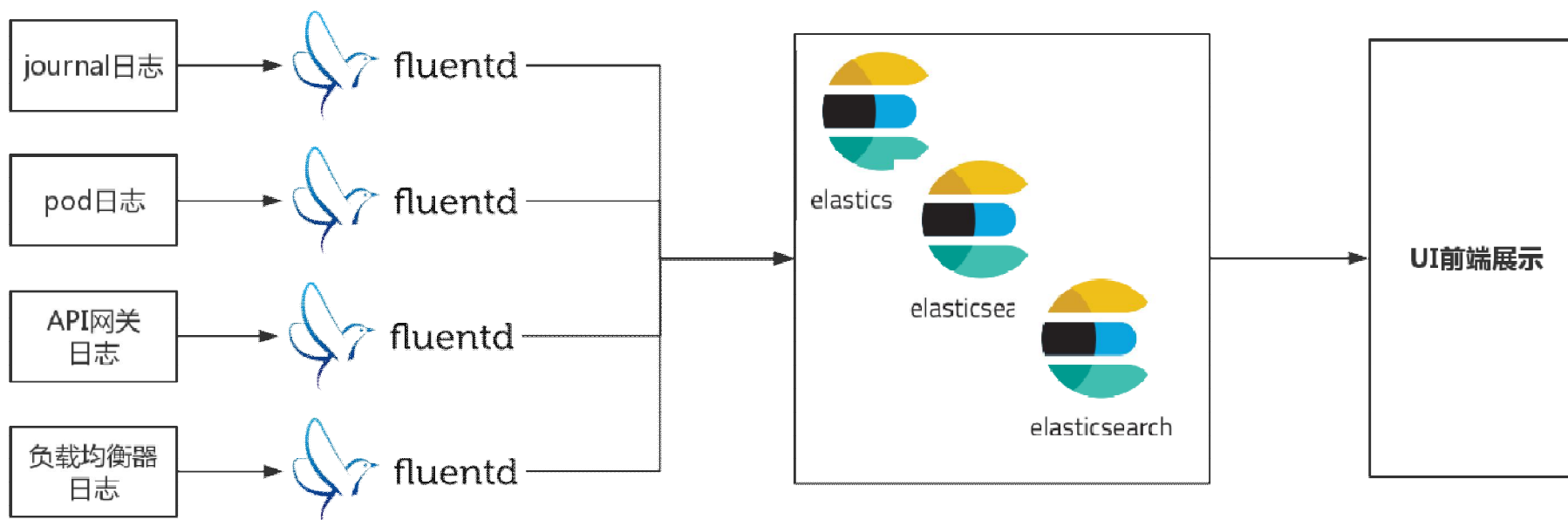
➤ LDAP：存放用户的基本信息，比如用户名、密码、邮箱等。

➤ MySQL：存放用户的权限信息等，比如系统的权限项，用户与权限的绑定等。

➤ paas-auth：自研组件，提供用户管理的功能，创建用户等；提供权限控制的功能，添加权限，赋予用户权限等。



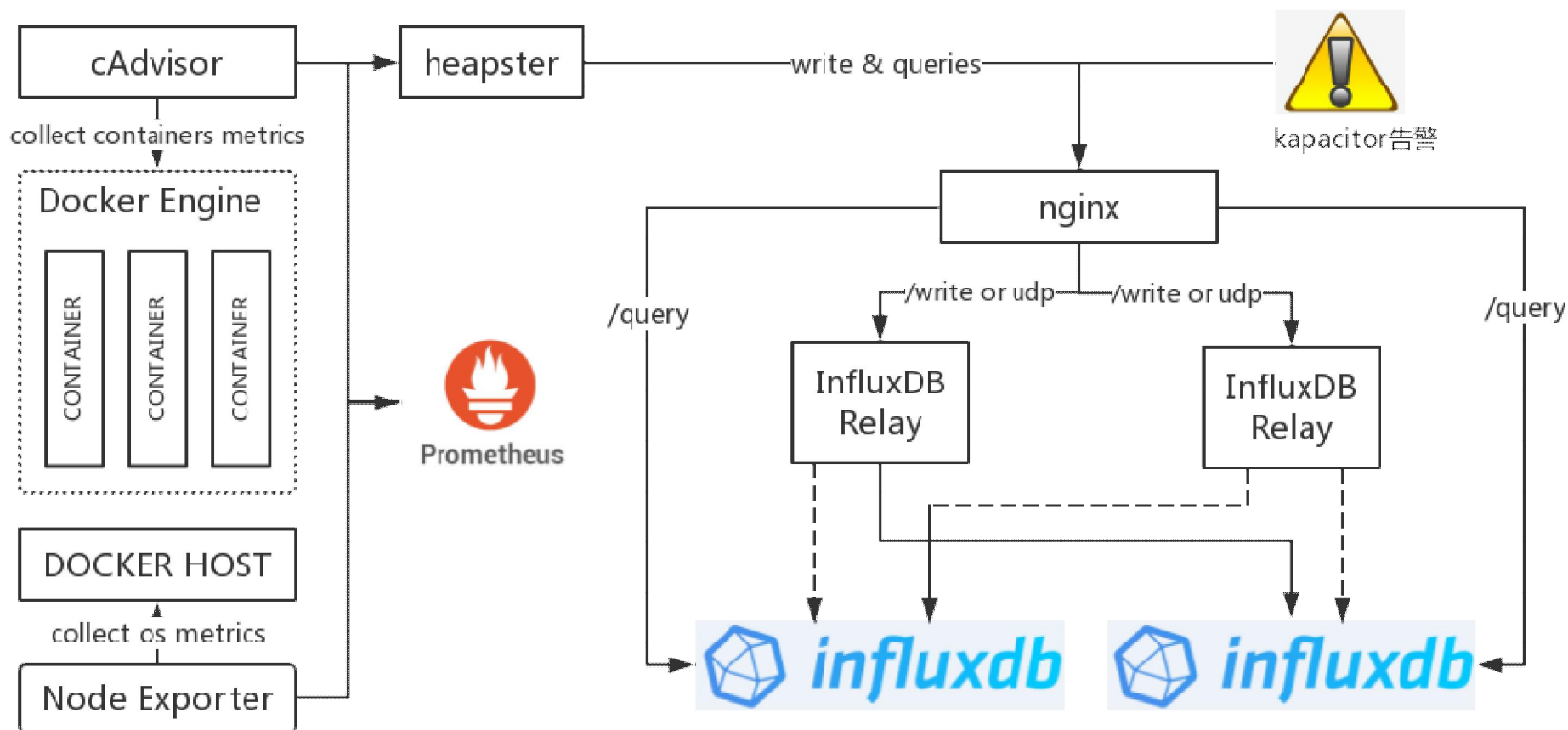
BC-PaaS – 日志



- 每台主机上以daemonset的形式运行fluentd。
- 每个类型的日志对应一个topic，按月建立索引。
- 应用的日志自己解析。



BC-PaaS – 监控告警

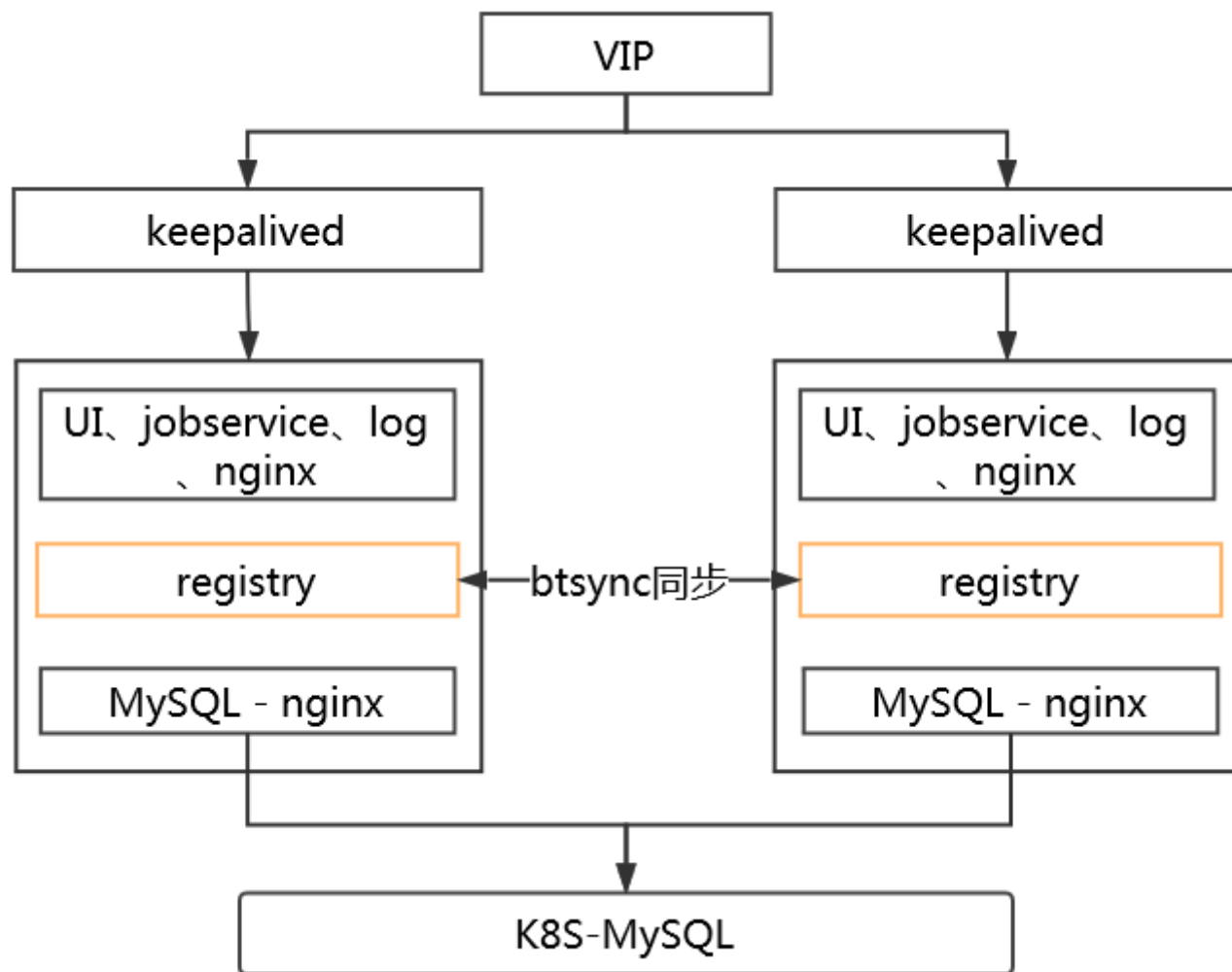


BC-PaaS – 监控告警

kubelet	内置cAdvisor，其为运行容器的用户提供出色的资源使用和性能特征。这是一个运行守护进程，能够搜集、集料、处理和导出运行中的容器的信息。
node-exporter	node-exporter用于收集主机资源指标，如arp、bcache、conntrack、cpu、diskstats、filesystem等
kube-state-metrics	kube-state-metrics用于收集kubernetes自有对象的监控指标，如deployment、pod、node等。
自定义	按照prometheus指标标准，暴露url即可



BC-PaaS – 镜像仓库



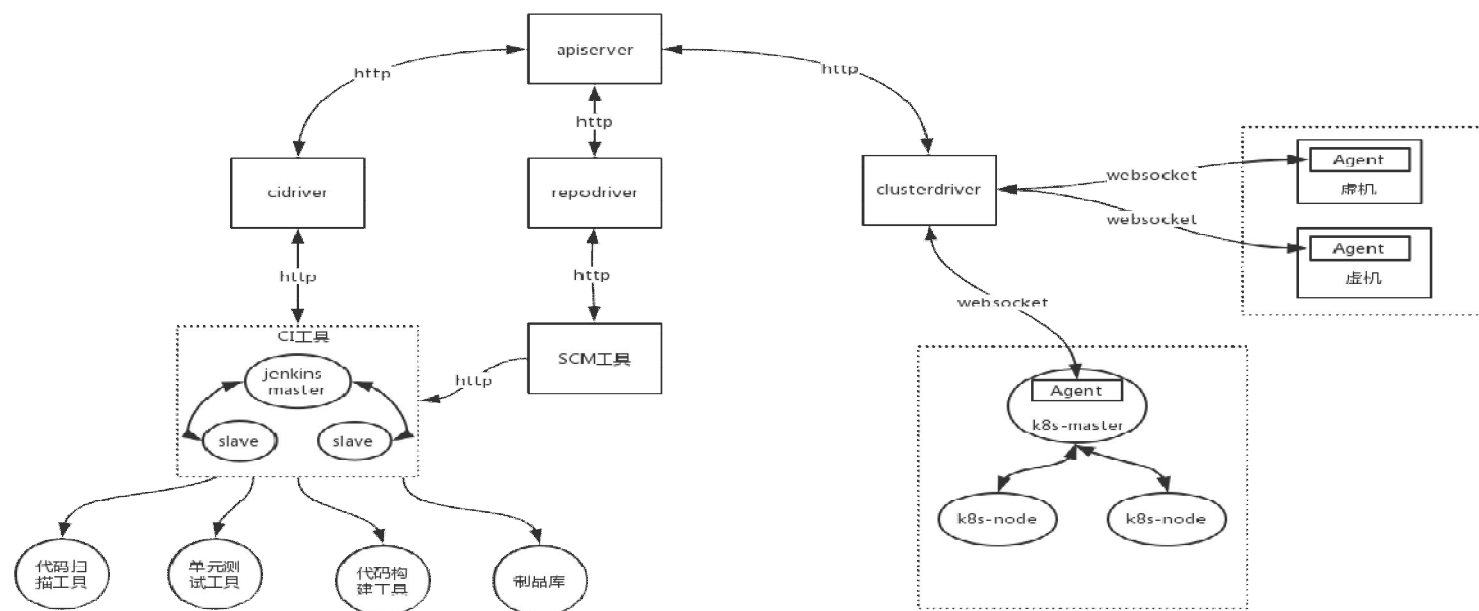
➤ 将mysql实例从harbor中抽离出来，利用外部的mysql

➤ 在harbor的主机上启动一个nginx，来对mysql的访问进行高可用配置。

➤ 利用btsync对registry存储的镜像数据进行实时同步。



BC-PaaS – CI/CD



- **api server**: 负责提供对内和对外的rest请求
- **ci driver**: 负责处理流水线相关的rest请求
- **repodriver**: 负责处理与代码相关的rest请求
- **clusterdriver**: 负责处理与集群环境相关和部署相关的请求



实践之展示





实践之经验

- CentOS推荐使用xfs文件系统，同时需支持d_type.
- Docker 1.13默认拒绝所有iptables，iptables -P FORWARD ACCEPT
- Alpine基础镜像，推荐使用3.7及之后的版本。之前的版本可能出现dns查询超时。





THANKS

2018 DevOpsDays • 北京站

