

# 我如何在京东运营JDOS

聊聊开源落地的那些事儿

吕江昭

京东基础架构部 软件开发工程师

主办方：



caicloud 才云



 TensorFlow

协办方：





# JDOS：京东数据中心基础设施资源调度和应用管理一站式平台



资源调度：多种优化调度算法保障不同类型任务  
合理使用资源，显著提升资源利用率

应用管理：提供一系列工具保障应用发布、高效  
完成

# 我如何在京东运营JDOS——JDOS是什么？



承载京东所有线上业务，容器数量达到百万级别





# 也聊聊京东Kubernetes开源 落地的那些事儿



## 选型

容器编排管理：Kubernetes

网络：neutron、ovs、自研BGP网络服务（skynet）

存储：LVM、自研容器分布式存储（ContainerFS）

DNS：自研高性能DNS（ContainerDNS）

LB：自研高性能LB（ContainerLB）

镜像中心：Harbor

日志：自研日志系统

监控：cAdvisor、Prometheus

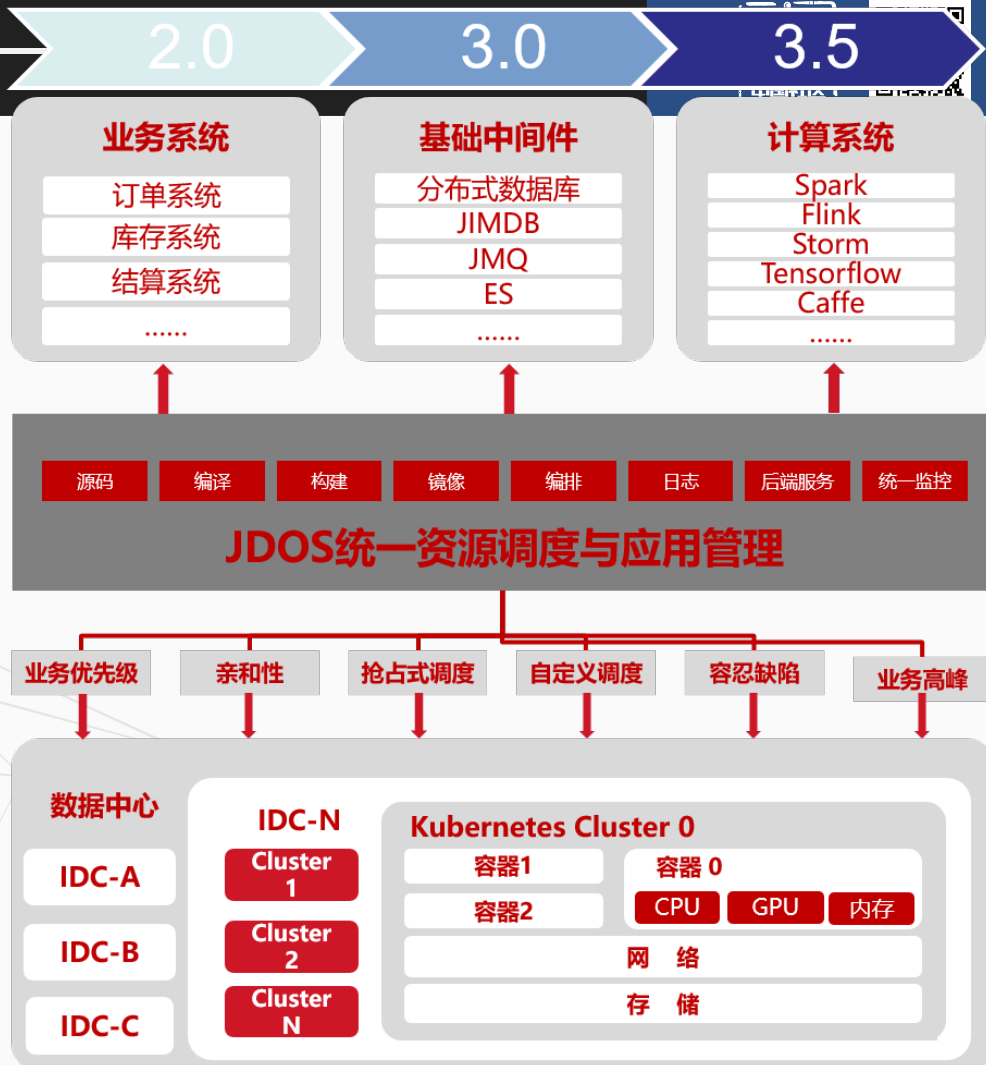


## Kubernetes定制与优化

- ◆ Pod IP保持不变
- ◆ Group-controller ( 支持灰度发布、本地rebuild Pod )
- ◆ Scheduler调度算法和性能优化
- ◆ Node-controller/endpoint-controller功能裁剪
- ◆ configMap支持静态挂载
- ◆ service支持更为灵活的set-based selector
- ◆ 支持 reuse容器策略
- ◆ 支持 request 和 limit 的修改

# 我如何在京东运营JDOS

不仅仅是k8s







# 大规模k8s集群的运营哲学



## 大规模集群下的参数调优和配置

- ◆ 宿主机资源保留
- ◆ 心跳上报时间优化
- ◆ QPS限制
- ◆ max-request
- ◆ Etcd配置自动压缩和较大的空间配额、定期去碎片化



## 组件部署

- ◆ apiserver前加负载均衡
- ◆ controller和scheduler通过选举
- ◆ etcd存储拆分



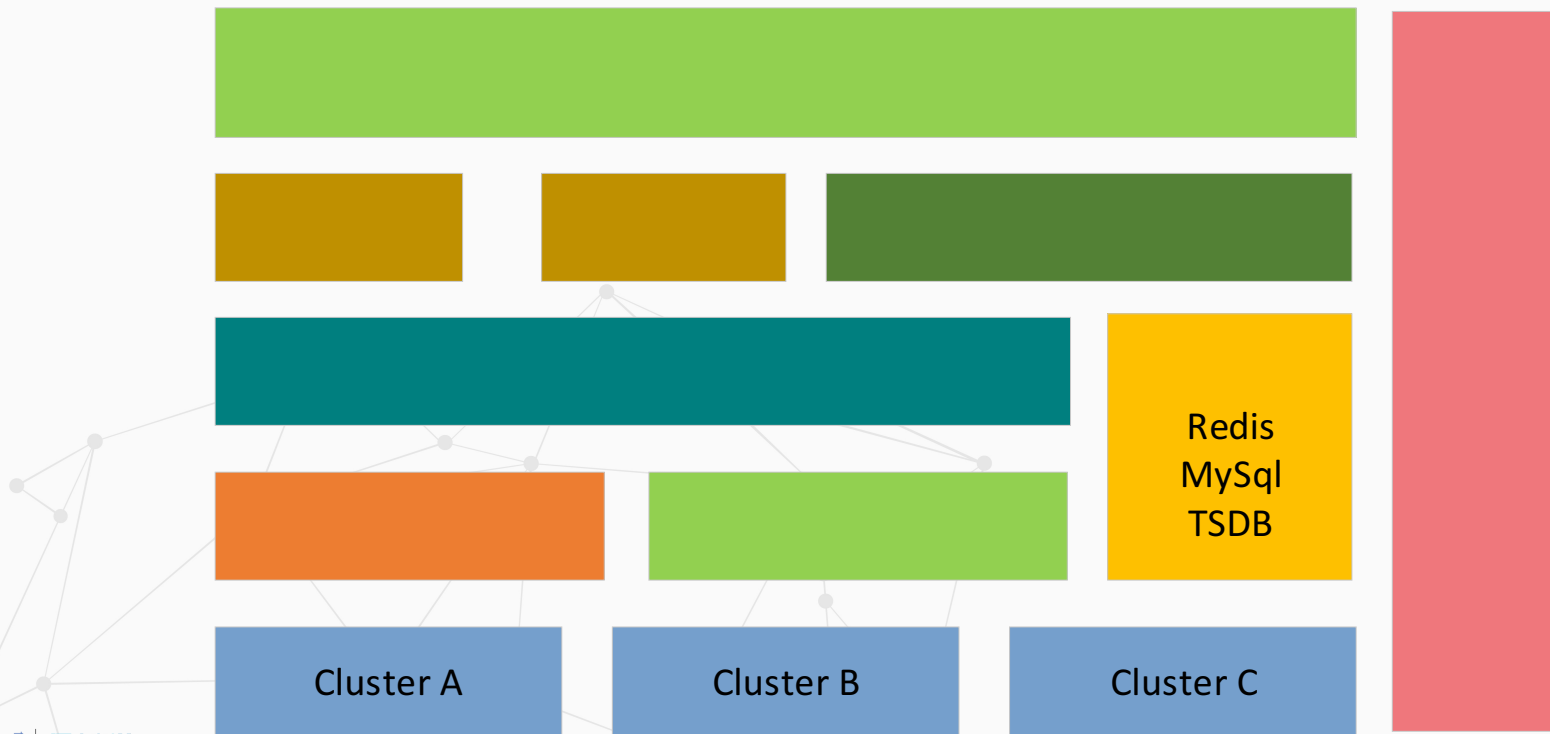
## Node管理

通过一系列label管理node生命周期、属性和用途等

- ◆ [jdos.jd.com/net.status](https://jdos.jd.com/net.status)
- ◆ [jdos.jd.com/image.status](https://jdos.jd.com/image.status)
- ◆ [jdos.jd.com/net.pod](https://jdos.jd.com/net.pod)
- ◆ [jdos.jd.com/rack](https://jdos.jd.com/rack)
- ◆ [jdos.jd.com/status](https://jdos.jd.com/status)
- ◆ [jdos.jd.com/zone](https://jdos.jd.com/zone)
- ◆ [jdos.jd.com/disk.type](https://jdos.jd.com/disk.type)
- ◆ [jdos.jd.com/cpu.model](https://jdos.jd.com/cpu.model)



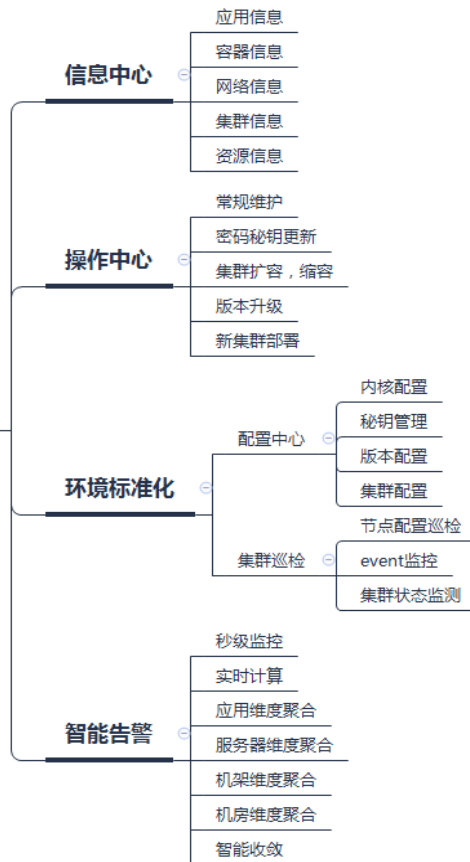
## JDOS运营平台





## JDOS运营平台

### 超大规模容器集群管理系统





## JDOS运营平台



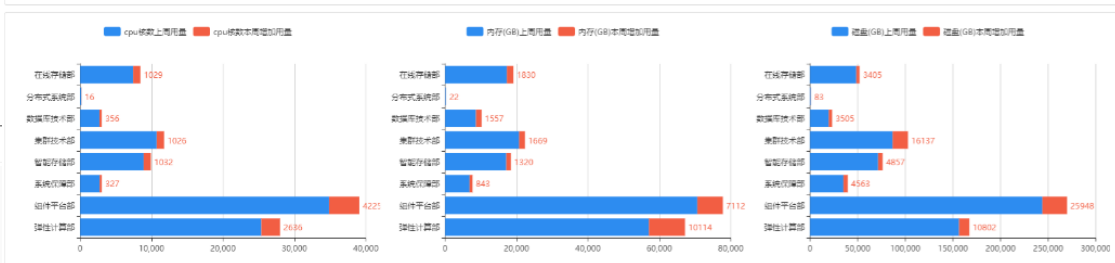
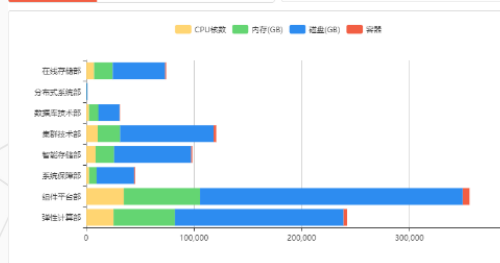
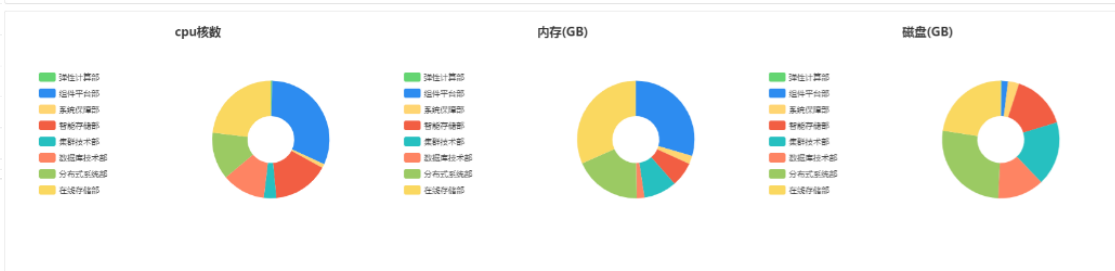
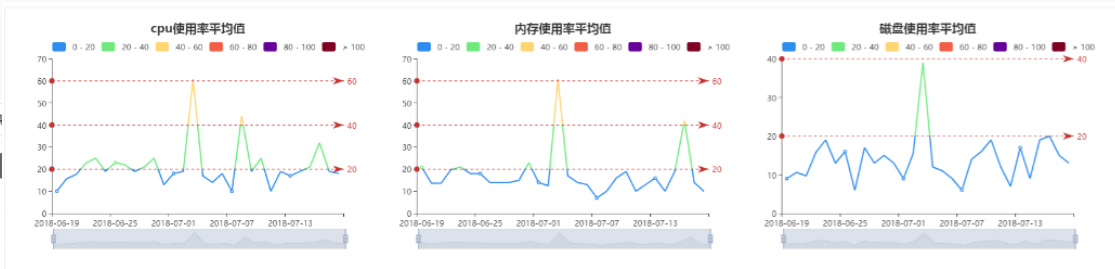
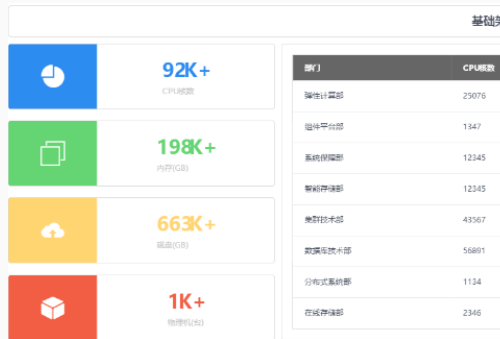
The screenshot shows the HCMP (Home Cluster Management Platform) interface. The top navigation bar includes a logo and the text 'HCMP'. Below it, there are tabs for '首页' (Home), '一键运维' (One-click Maintenance), '物理机查询' (Physical Machine Query), '应用查询' (Application Query), and '容器查询' (Container Query). The '一键运维' tab is active. The main content area is titled '一键运维' and features an input field for '输入IP:' with the placeholder '请输入IP'. To the right of the input field are three buttons: '运维记录' (Maintenance Record), '运维邮件' (Maintenance Email), and '恢复邮件' (Recovery Email). Below the input field is a table with the following structure:

id	故障原因	更新时间
----	------	------

# 我如何在京东运营JDOS—大规模k8s集群运营



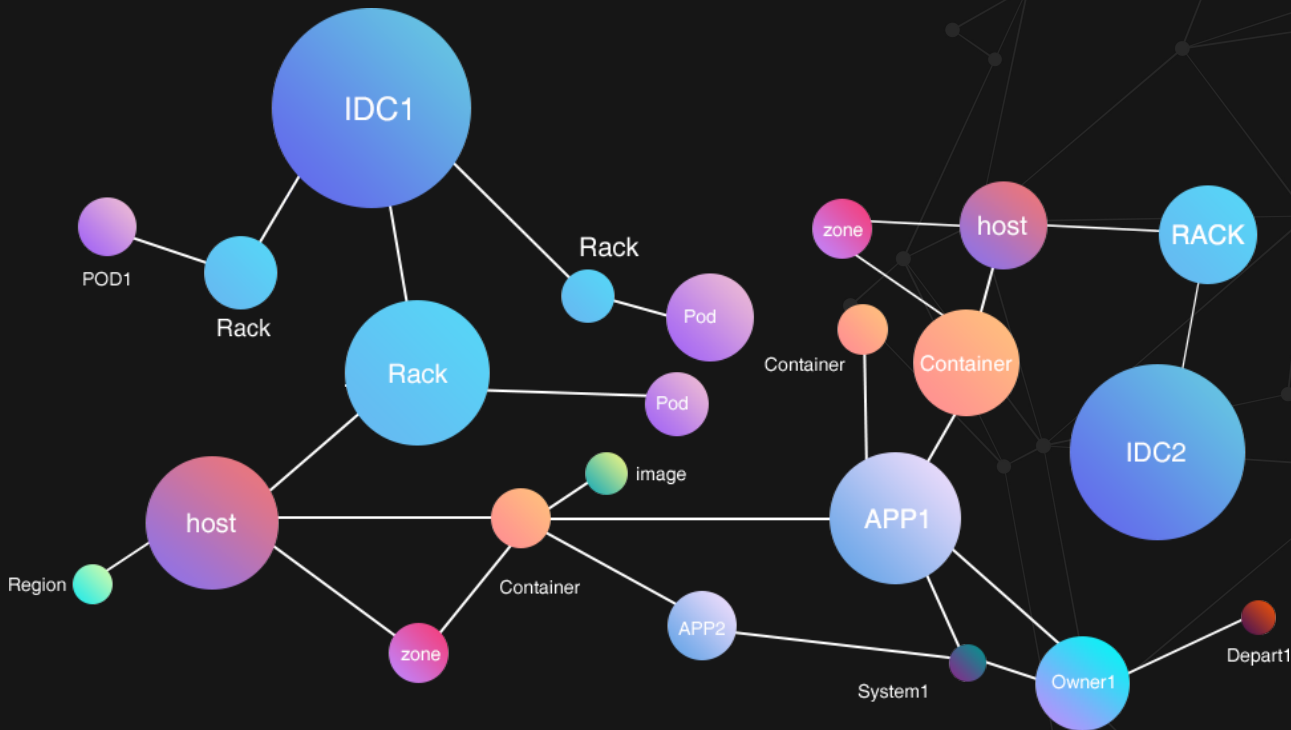
## JDOS运营平台





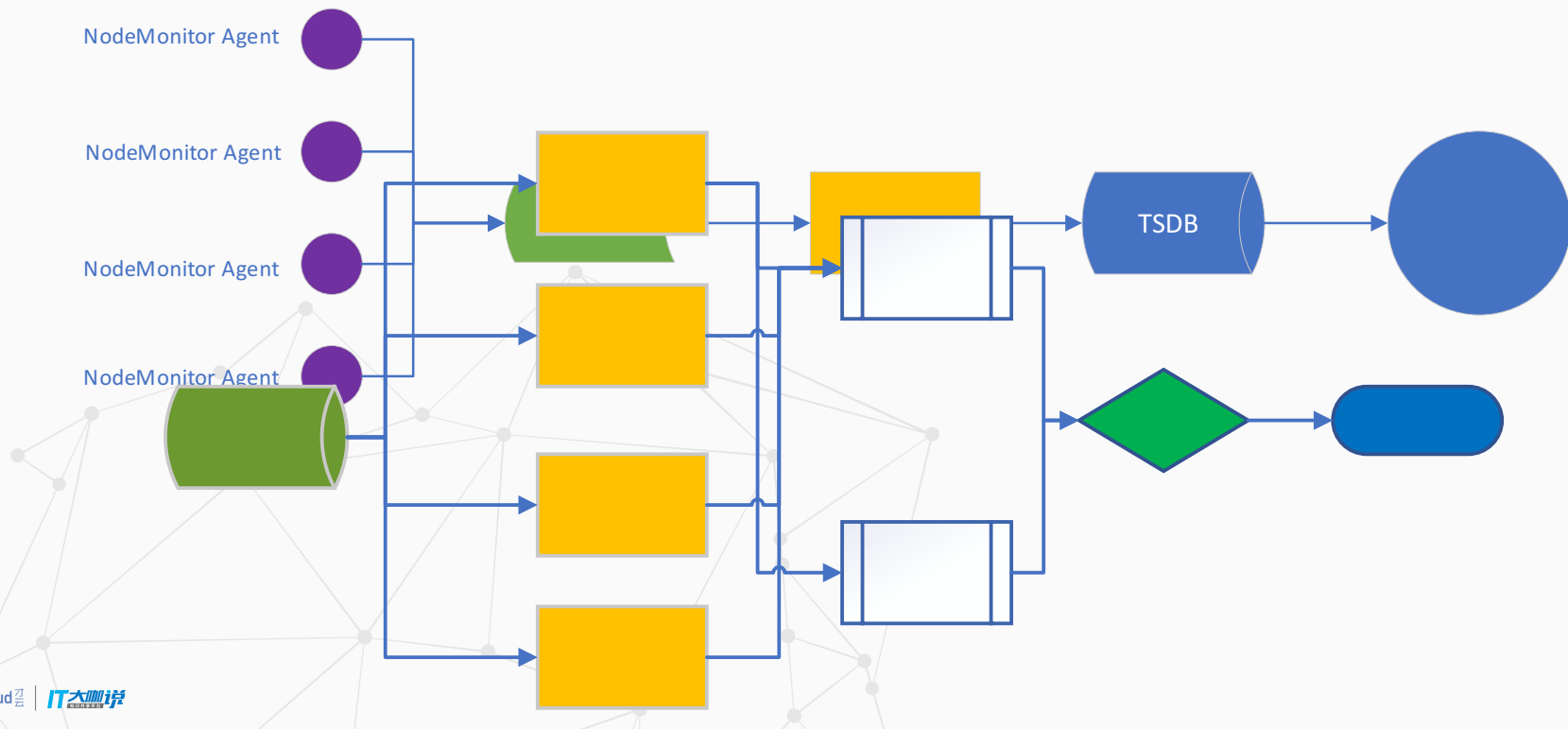


## JDOS知识图谱





## 智能告警系统





## 巡检系统

巡检简报				
检查点	Error统计	Alarm统计	Warn统计	Info统计
kubelet进程检查	0	0	0	90
kubelet健康检查	0	0	0	90
/export使用率检查	0	0	0	90
进程数检查	0	6	0	84
ntp时间误差检查				90
系统日志级别检查				90
系统内核版本检查				90
数据口网卡crc错误检查				90
文件句柄数检查				90
kernel中pid_max值检查				90
fstab检查				90
nf_conntrack检查				90
内存使用率检查				90
负载检查	0	0	0	90
kubelet版本检查	0	0	0	90
cadvisor进程检查	0	0	0	90
thor进程检查	0	0	0	90
cadvisor cgroup cpu quota检查	1	0	0	89
cadvisor cgroup memory检查	0	0	0	90
cadvisor cgroup memory swap检查	0	0	0	90



## 运维工具

- ◆ Ansible
- ◆ serf
- ◆ Kubernetes Connection Plugin(自研)

```
[aa:vars]
gztest-13d39fc2-1267172821-vdfgk | 'SUCCESS' | rc=0 >>
root      1      0      0      Oct18 ?      00:00:00 /bin/sh -c /bin/sh -c '/etc/init.d/cron restart && sleep 999999d
Use 'kubectl describe pod/gztest-13d39fc2-1267172821-vdfgk' to see all of the containers in this pod.

gztest-39562c42-1982562632-14nn0 | SUCCESS | rc=0 >>
root      1      0      0      Oct18 ?      00:00:00 /bin/sh -c /bin/sh -c '/etc/init.d/cron restart && sleep 999999d
Use 'kubectl describe pod/gztest-39562c42-1982562632-14nn0' to see all of the containers in this pod.

gztest-39562c42-1982562632-1ks4q | SUCCESS | rc=0 >>
root      1      0      0      Oct18 ?      00:00:00 /bin/sh -c /bin/sh -c '/etc/init.d/cron restart && sleep 999999d
Use 'kubectl describe pod/gztest-39562c42-1982562632-1ks4q' to see all of the containers in this pod.
```



## 其他小工具

- ◆ API日志分析工具：python+spark分析统计api请求的各维度信息
- ◆ Kubesql：将k8s中各种资源处理成关系数据库的表，通过sql语句查询
- ◆ Event事件监听和告警



# 经验分享：遇到的问题解决方法



## Etcd相关

- ◆ Etcd磁盘繁忙、tcp连接数过多
- ◆ Etcd后端存储经常满
- ◆ 故障恢复（一台或多台节点不可用）
- ◆ 强制数据恢复、灾备
- ◆ Etcd raft bug ( v3.0.17 ) -> v3.2.13



## apiserver相关

- ◆ gRPC bug问题：同一资源的请求并发较高时触发，升级gRPC包和etcd client包解决
- ◆ 连接不均衡问题：kubelet上报心跳是TCP长连接





## Controller-manager相关

- ◆ Endpoint controller默认情况下会将NotReady节点上的所有Pod从对应service endpoint中摘除，可能会导致严重故障
- ◆ Node controller由于各种原因判断节点NotReady，易误判，一旦误判会导致节点上Pod被驱逐，引发故障



## Scheduler相关

- ◆ 优化调度算法、性能，支持高并发创建Pod，大数据混部等特殊场景
- ◆ 通过调度算法优化计算资源配置和共享，实现数据中心整体资源利用率大幅提升



## 驱逐相关

- ◆ 是否需要驱逐，根据实际情况
- ◆ Hard evict



## 内存超卖？

- ◆长尾效应
- ◆可以尝试，密切关注，收益明显





## 推动开源

◆ <https://github.com/tiglabs/>

# 谢 谢



主办方：



caicloud 才云



 TensorFlow

协办方：



网易云