



CNUTCon 2017
全球运维技术大会

SNG海量日志监控平台

吴树生

SNG监控平台负责人

QCon

全球软件开发大会

10月17-19日 上海 · 宝华万豪酒店

➤ 扫码锁定席位

九折即将结束

团购还享更多优惠，折扣有效期至9月17日
扫描右方二维码即可查看大会信息及购票



如果在使用过程中遇到任何问题，可联系大会主办方，欢迎咨询！

微信: qcon-0410

电话: 010-84782011

ArchSummit

全球架构师峰会 2017

➤ 扫码锁定席位

12月8-9日 北京 · 国际会议中心

七折即将截止立省2040元

使用限时优惠码AS200，
以目前最优惠价格报名ArchSummit
仅限前20名用户，优惠码有效期至9月19日，
扫描右方二维码即可使用



如果在使用过程中遇到任何问题，可联系大会主办方，欢迎咨询！

微信: aschina666

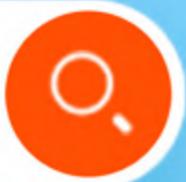
电话: 15201647919



极客搜索

全站干货，一键触达，只为技术

s.geekbang.org



扫描二维码立即体验

有没有一种搜索方式，能整合 InfoQ 中文站、极客邦科技旗下12大微信公众号矩阵的全部资源？

极客搜索，这款针对极客邦科技全站内容资源的轻量级搜索引擎，做到了！

扫描上方二维码，极客搜索！

这里只有 技术领导者

EGO会员第二季招募季正式开启



—— E小欧 ——

报名时间：9月1日-9月15日
扫描添加E小欧，
邀您进入EGO会员预报名群

立即报名



个人介绍

武汉大学、华为

腾讯

- 自研开发构建管理18万+服务器、200万+指标的分钟级实时监控平台monitor
- 开发构建支持异构业务数据、日均3000亿+流水的实时多维监控平台
- 开发构建日存储TB级的海量日志平台

TABLE OF CONTENTS

由面到点的异常分析案例

海量日志监控平台挑战

海量日志平台方案

异构数据监控解决方案

平台运维方案

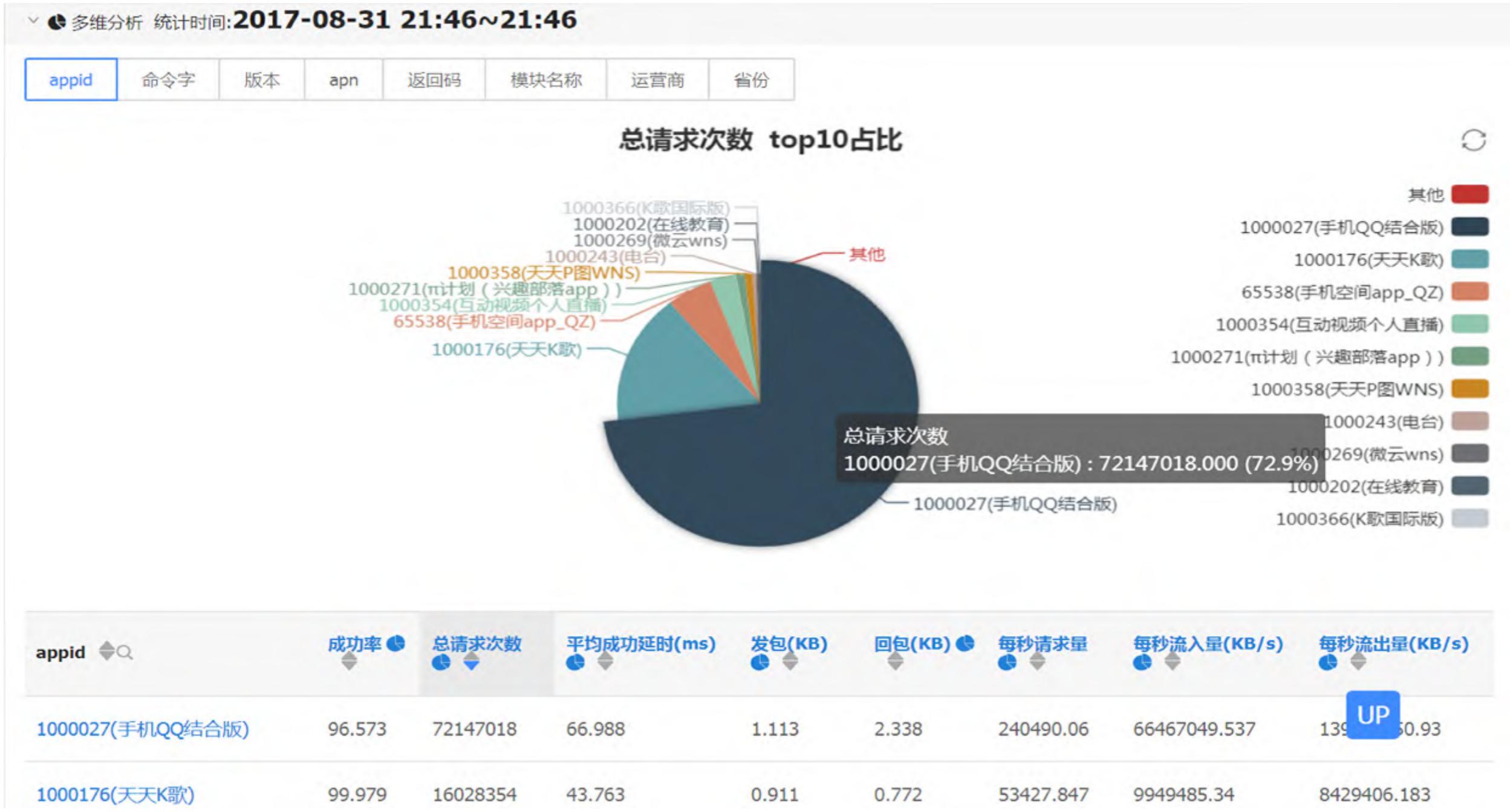
案例：由面到点的异常分析

2017年8月31日 21:40~21:50 空间X业务异常



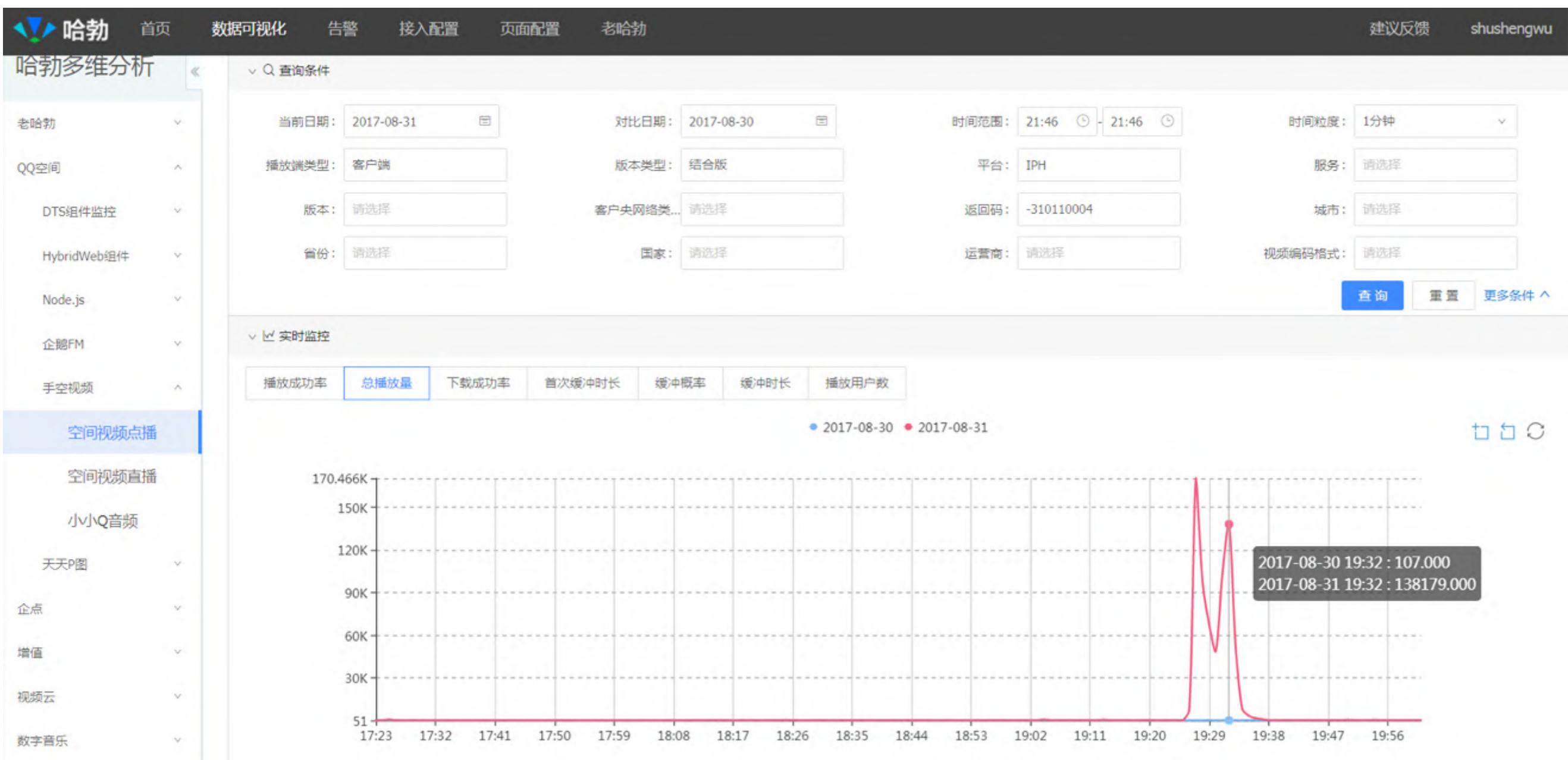
多维下钻分析方法

多维下钻分析获知问题根因



多维下钻获知根因

空间点播的IPH客户端点播有异常，返回码为-310110004



全链路故障分析方法

根据异常特征查找受影响案例

返回码 播放成功率 总播放量 下载成功率 首次缓冲时长 缓冲概率 缓冲时长 播放用户数 链接

| | | | | | | | | |
|------------|---|--------|---|---|---|---|---|-------|
| -310110004 | 0 | 138179 | 0 | 0 | 0 | 0 | 0 | 全链路监控 |
|------------|---|--------|---|---|---|---|---|-------|

全链路监控 Ver2.0.72 空间 大盘分析 链路分析 日志查询 返回码配置 接入配置 反馈 shushengwu

* 日志时段: 2017-08-31 21:41 至 2017-08-31 21:51 < 30分钟 30分钟 > Q 用户2 QQ号(选填) 关键字(选填) Q 查询

事件视图

数据更新/耗时: 2017-09-01 09:37:42 / 7.8619s 一秒内相同数据源事件合并展现 鼠标点击展开详情 ● 正常 ○ 警告 ● 错误 ● 用户

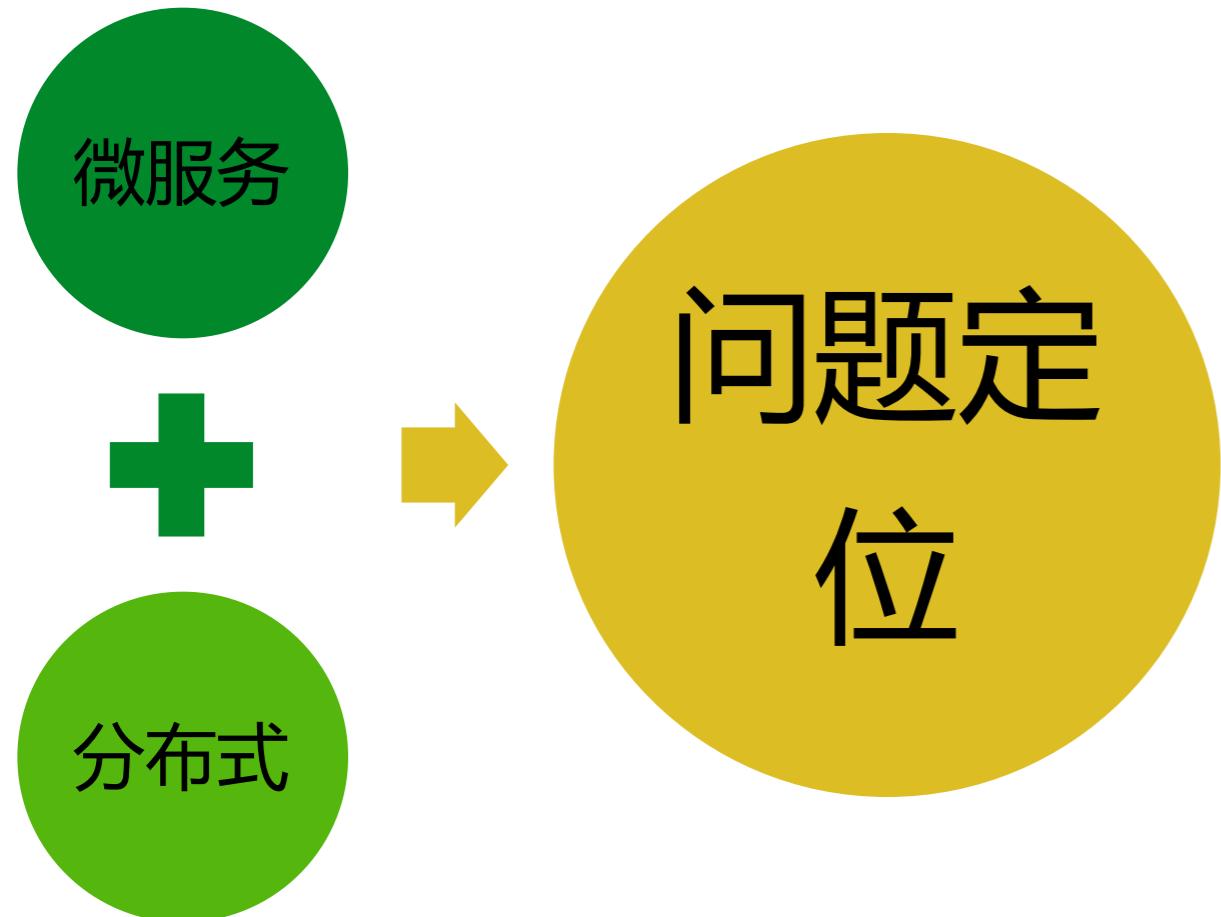
事件视图展示了从 21:45:36.000 到 21:50:41.000 的时间段内，'空间点播APP'和'wns-client'的事件分布。事件点以不同颜色表示：绿色（正常）、红色（错误）和蓝色（用户）。在'空间点播APP'事件中，可以看到多次连续的绿色点，中间夹杂着一两个红色点。在'wns-client'事件中，也有类似的模式。整个时间段内，事件点相对稀疏。

事件日志 用户信息 性能趋势

日志开始时间: 2017-08-31 21:45:36.000

| 时间 | 用户QQ | 数据源 | 事件名称 | 扩展字段 | 返回码 | 耗时ms |
|--------------|------|---------|---|-----------------|--------------|-------|
| 21:45:36.000 | | 空间点播APP | video_link_redirect(url重定向耗时): 正常 | 2430073723 WIFI | 0 : url重定向耗时 | 0.000 |
| 21:45:36.000 | | 空间点播APP | video_link_redirect_occur_times(url重定向次数): 正常 | 2430073723 WIFI | 0 : url重定向次数 | 0 |

日志监控功能



个例分析

- VIP投诉
- 从面到点定位

开发调试

- 查看关联日志
- 测试提单线索

监控告警

- 异常检测
- 告警
- 问题分析

TABLE OF CONTENTS

由面到点的异常分析案例

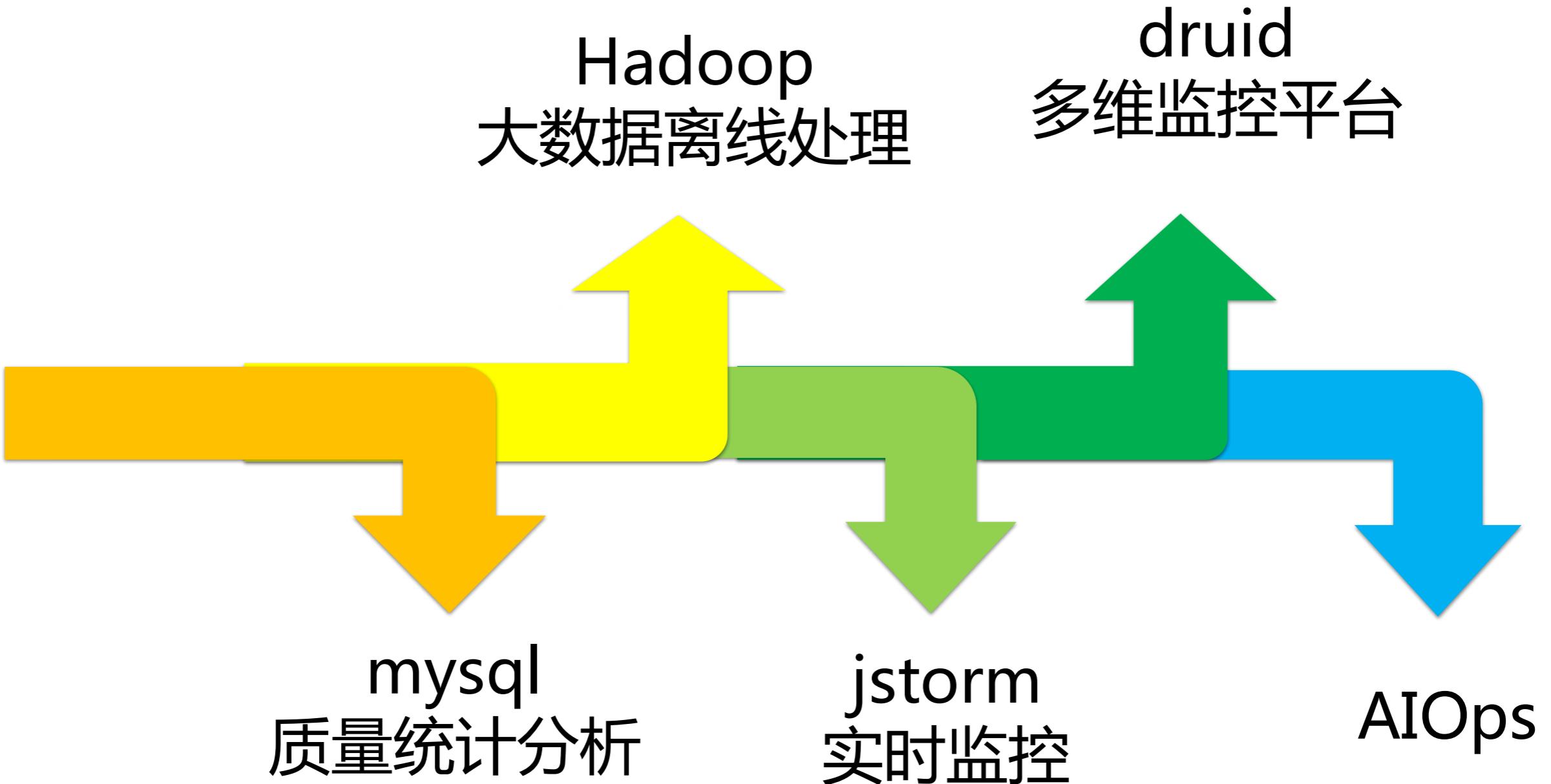
海量日志监控平台挑战

海量日志平台方案

异构数据监控解决方案

平台运维方案

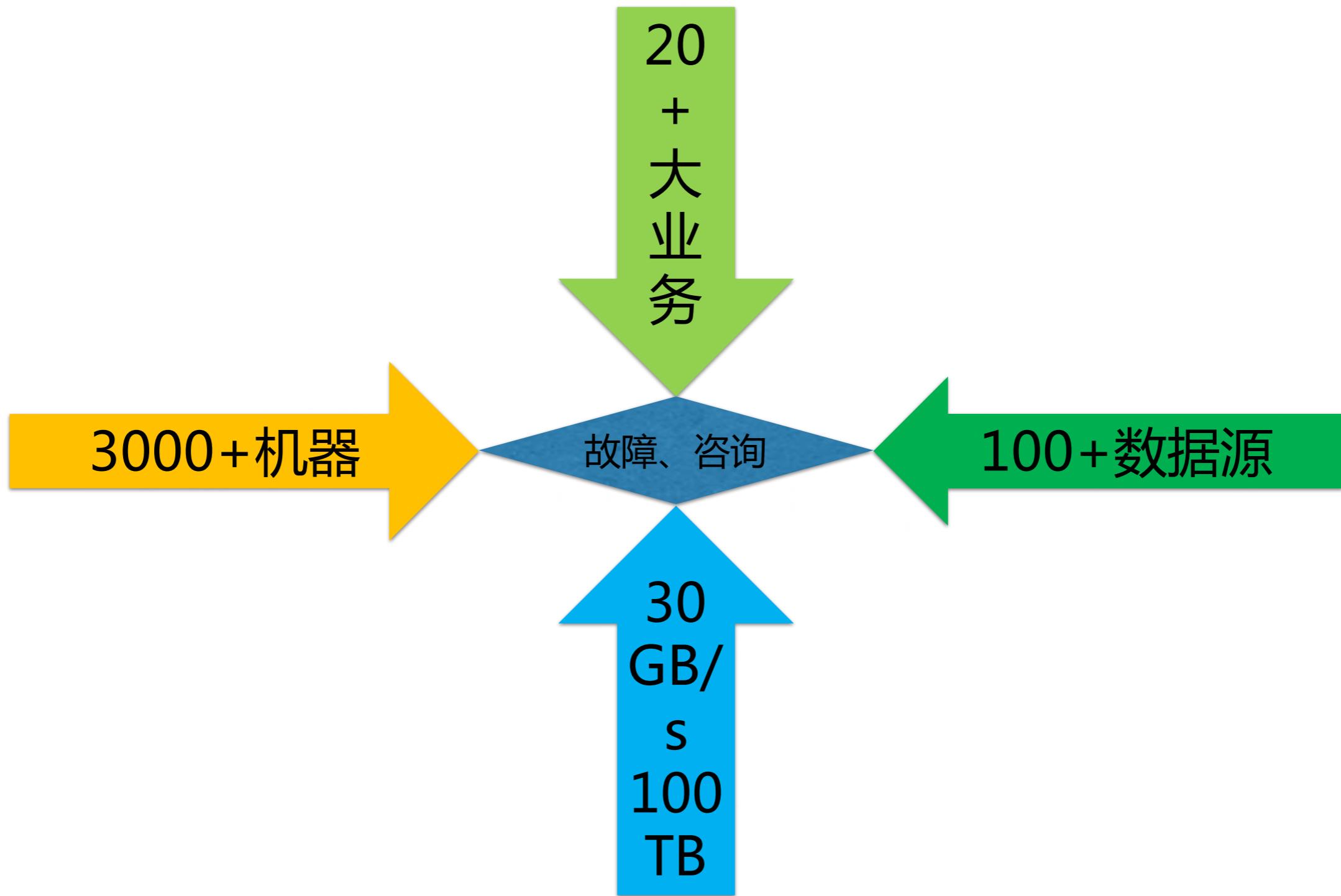
日志监控发展阶段



用户诉求



大数据平台业务挑战



大数据平台组件挑战

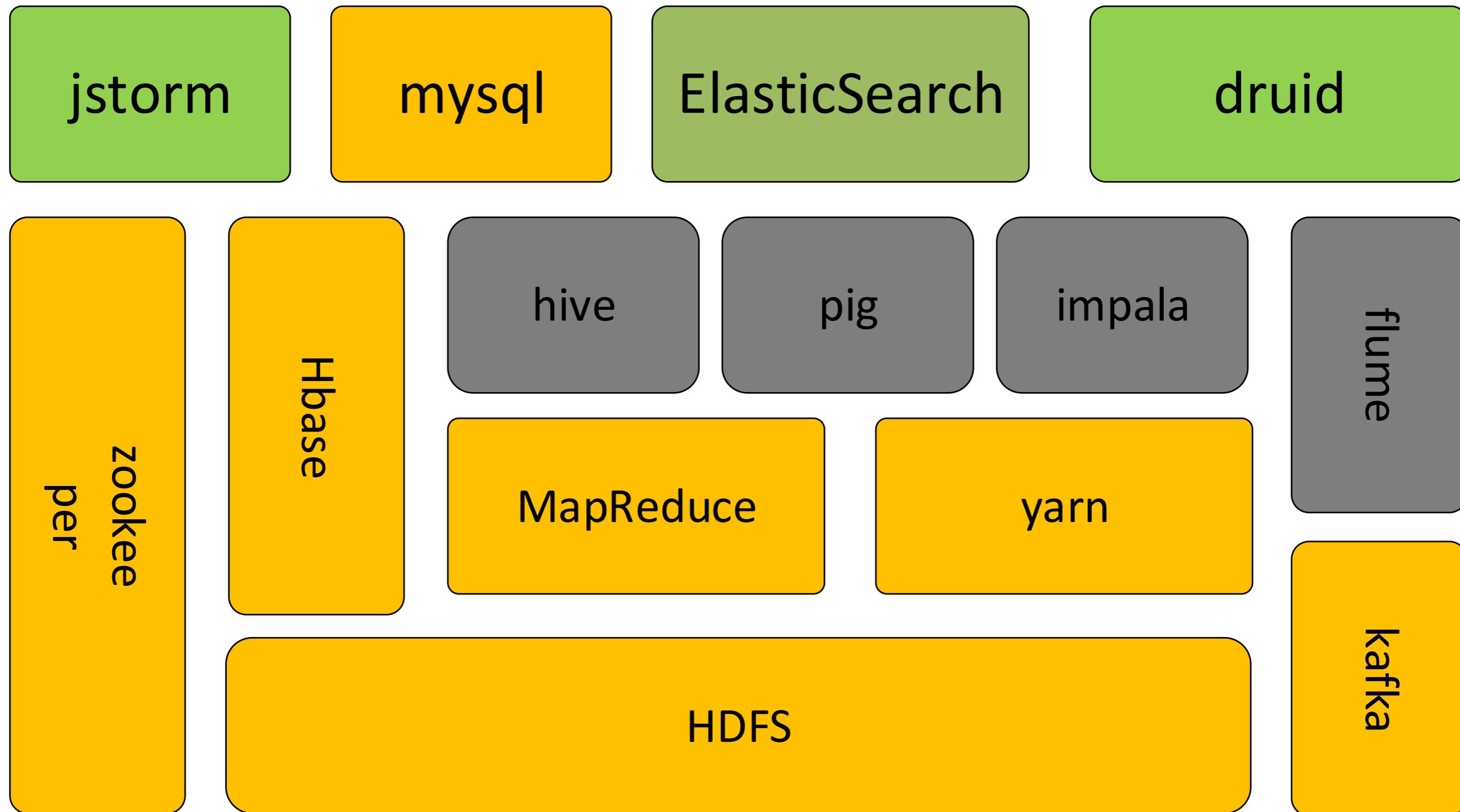


TABLE OF CONTENTS

由面到点的异常分析案例

海量日志监控平台挑战

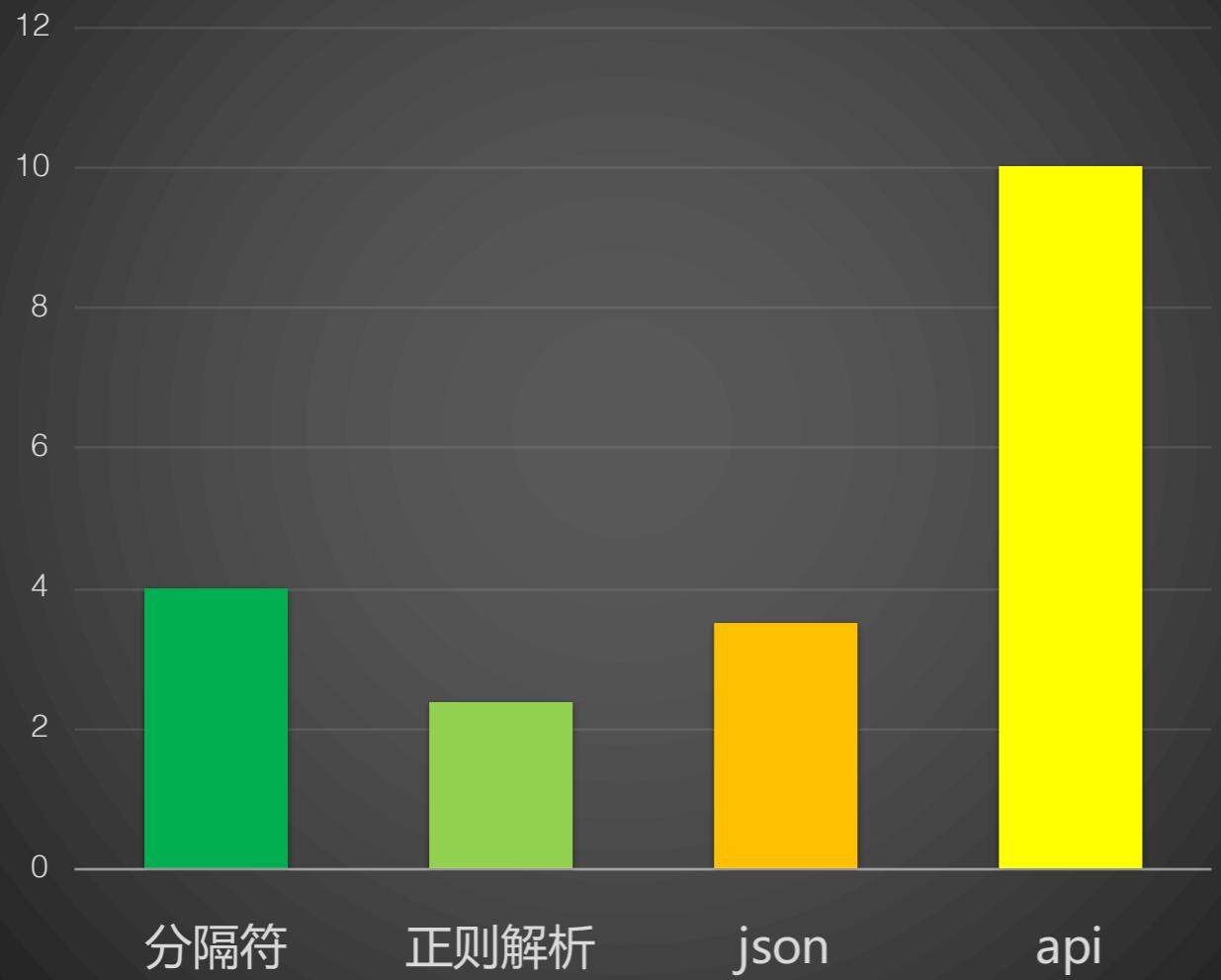
海量日志平台方案

异构数据监控的解决方案

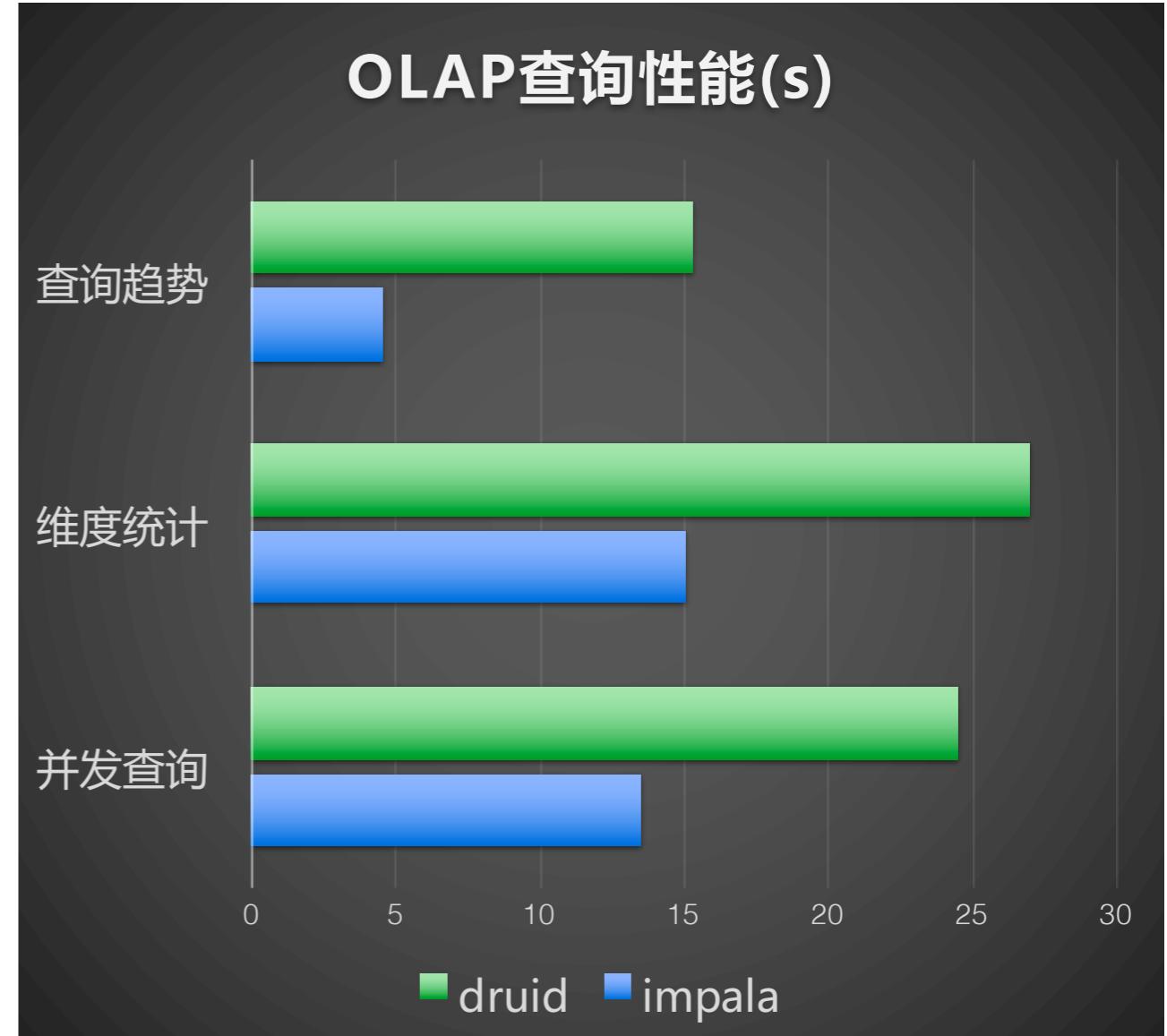
平台运维方案

性能评估

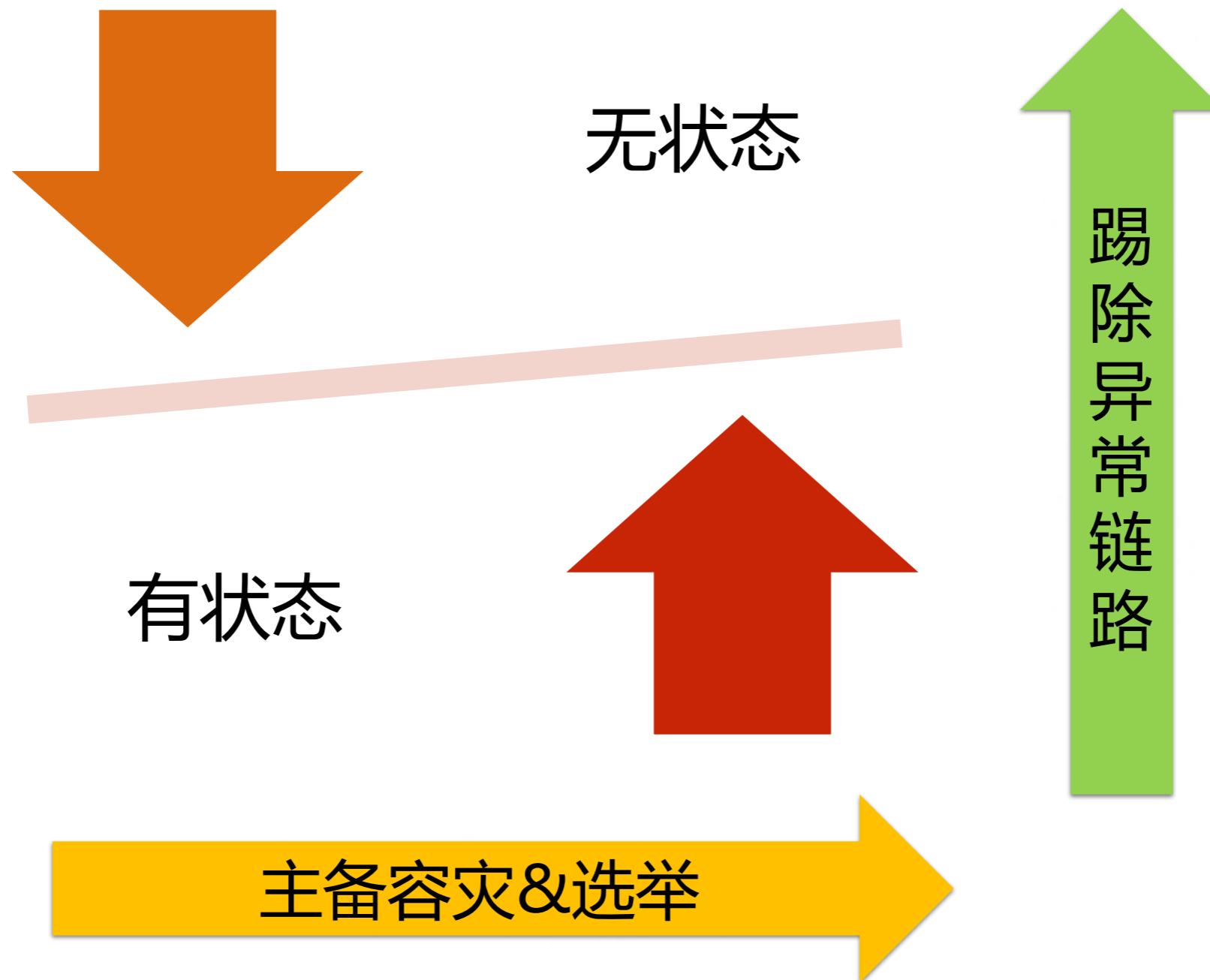
数据采集性能(w/s)



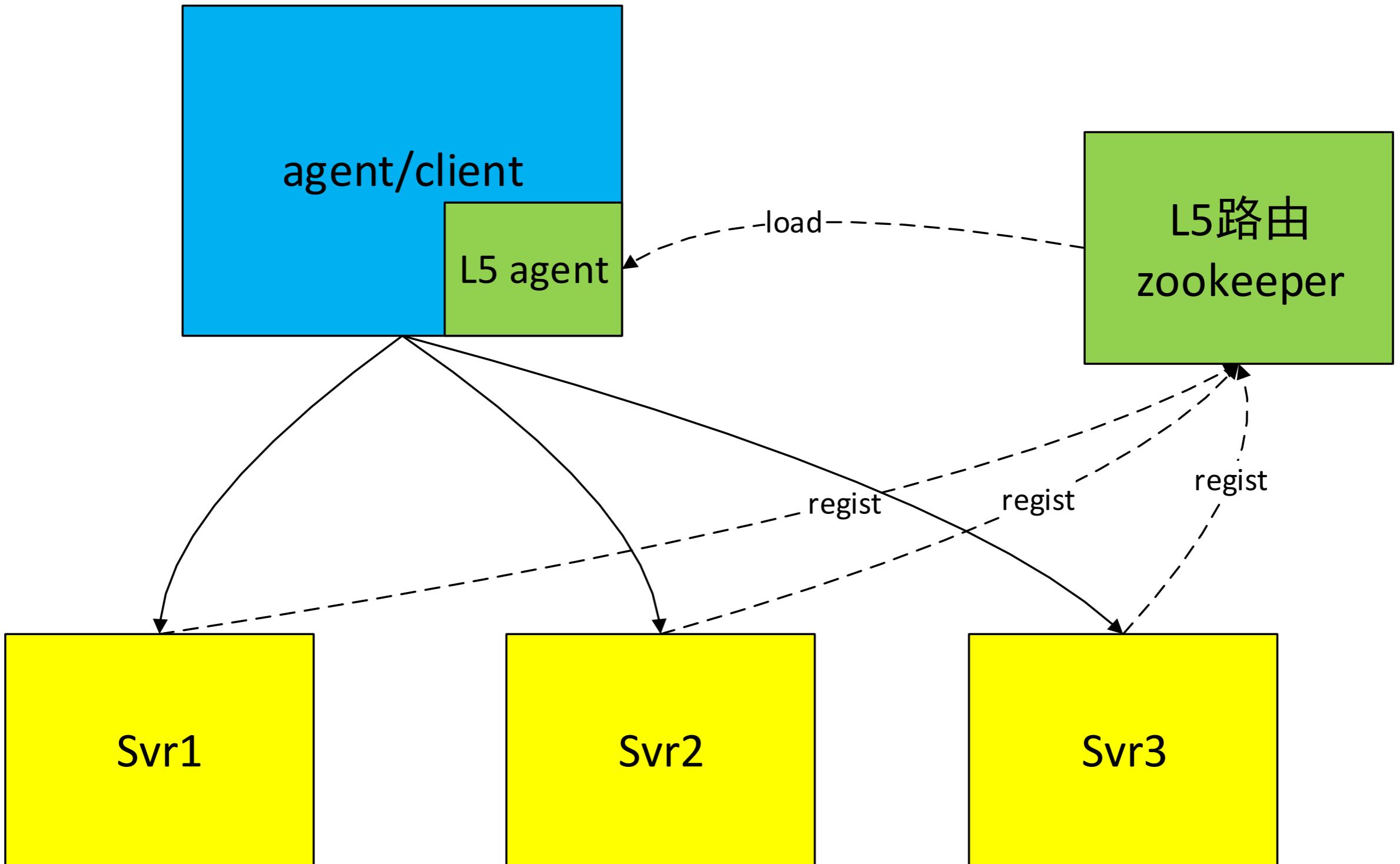
OLAP查询性能(s)



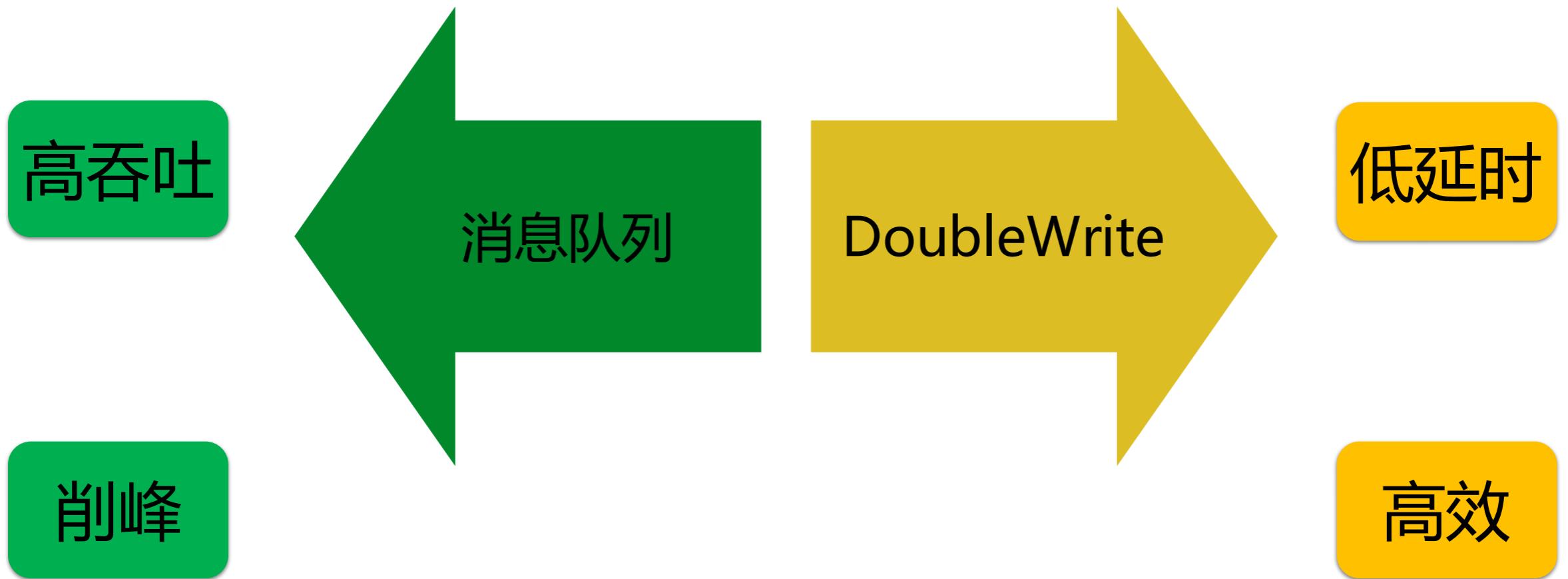
无状态化



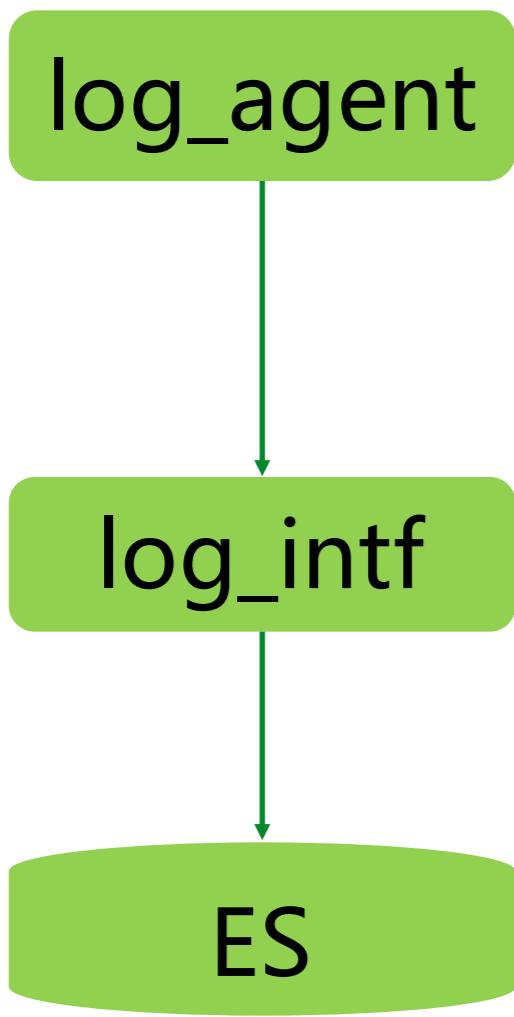
路由&负载均衡



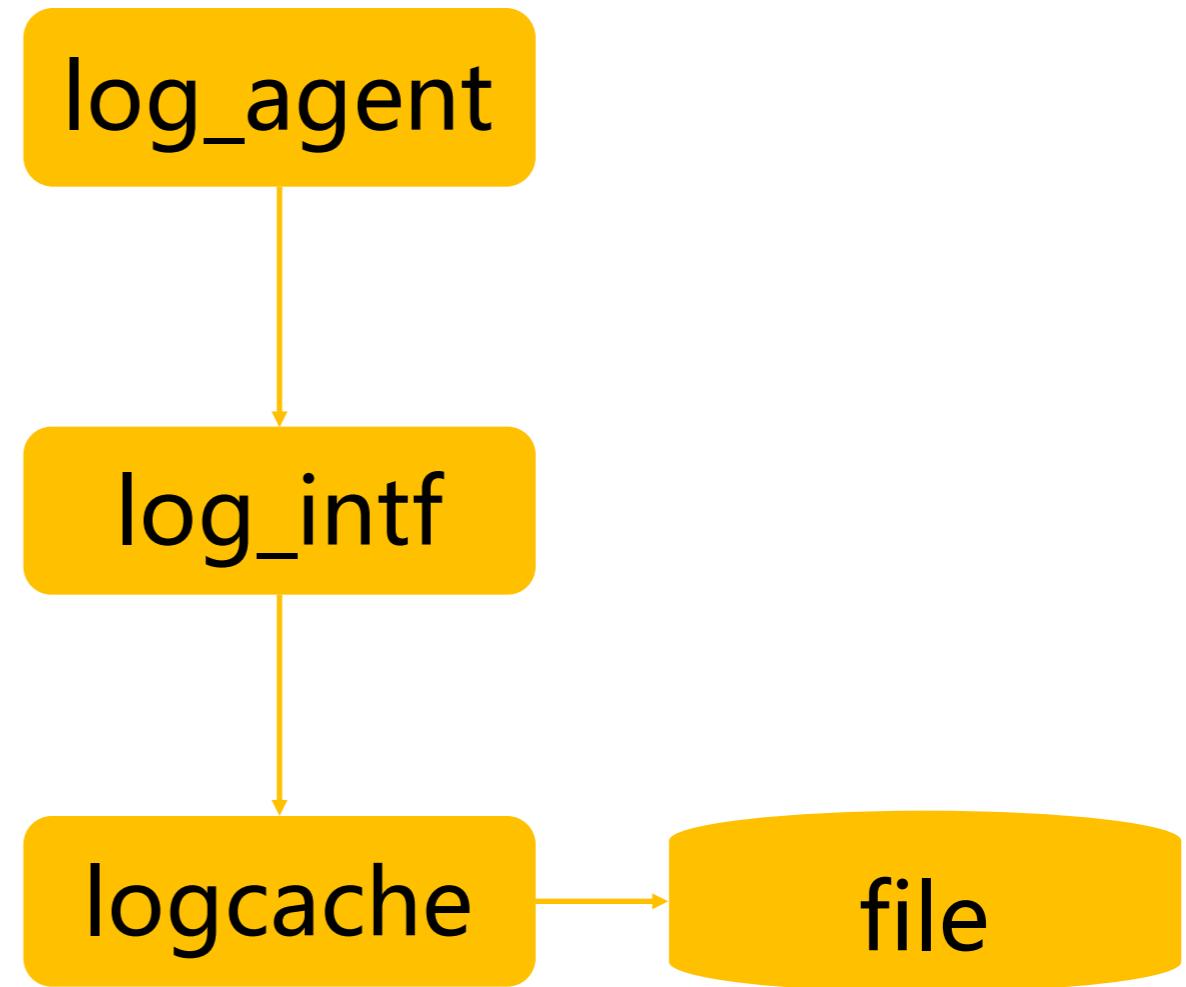
数据通道容灾



日志存储方案

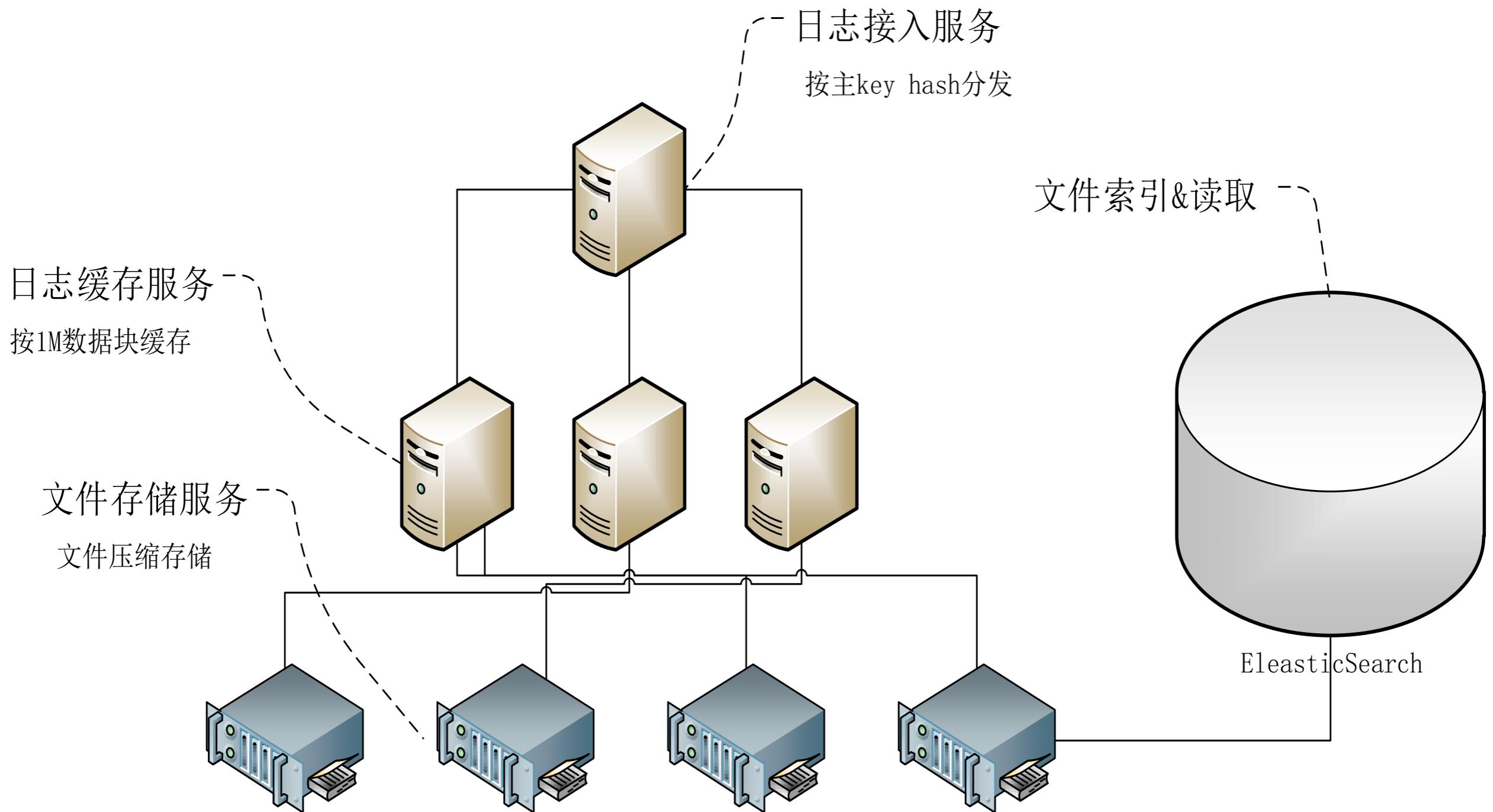


少量数据\TCP 传输
延时<30s\丢包率<0.1%



海量数据\UDP 传输
延时2~5分钟\丢包率<1%

自研日志存储



日志处理流程

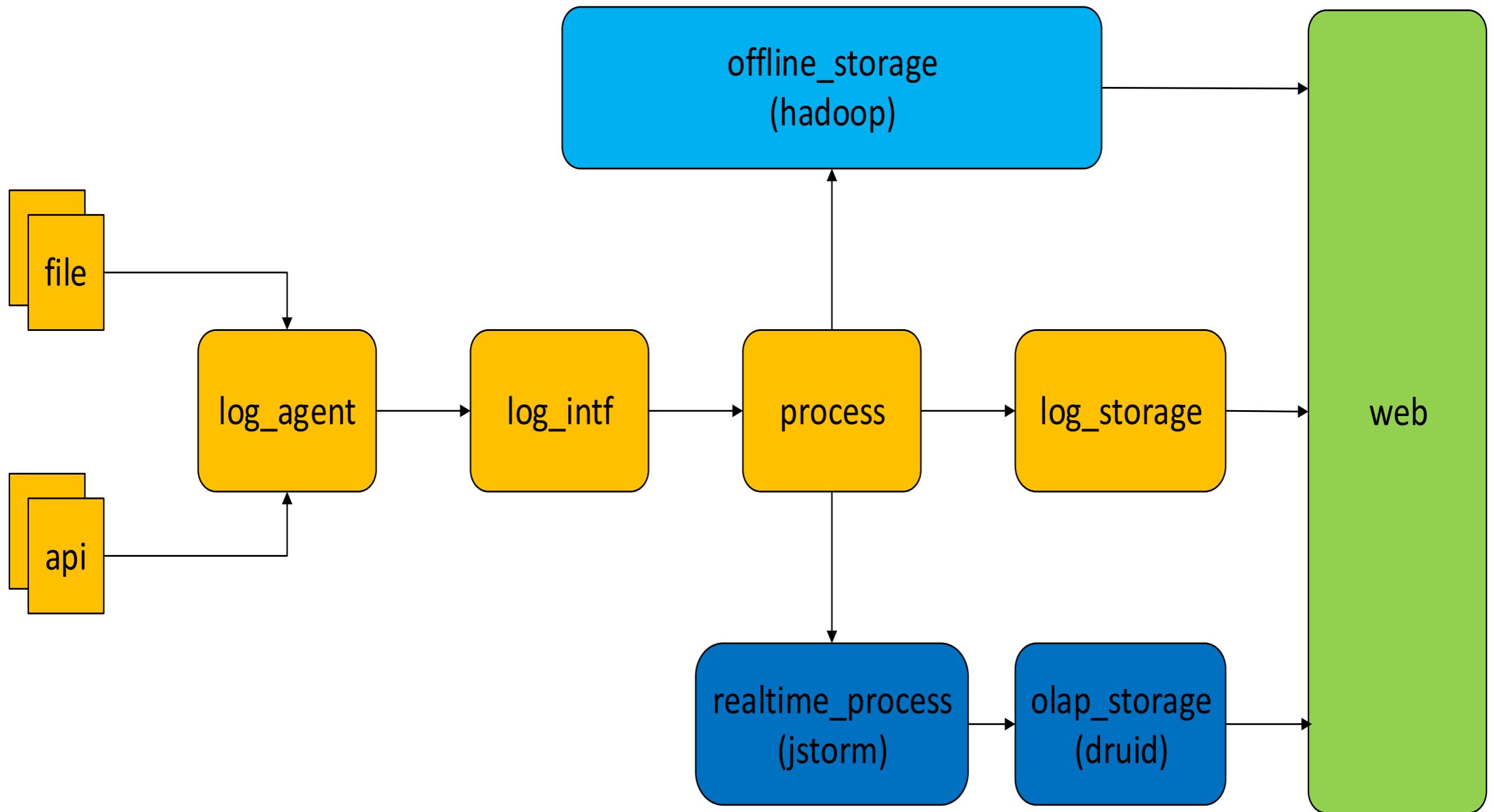


TABLE OF CONTENTS

由面到点的异常分析案例

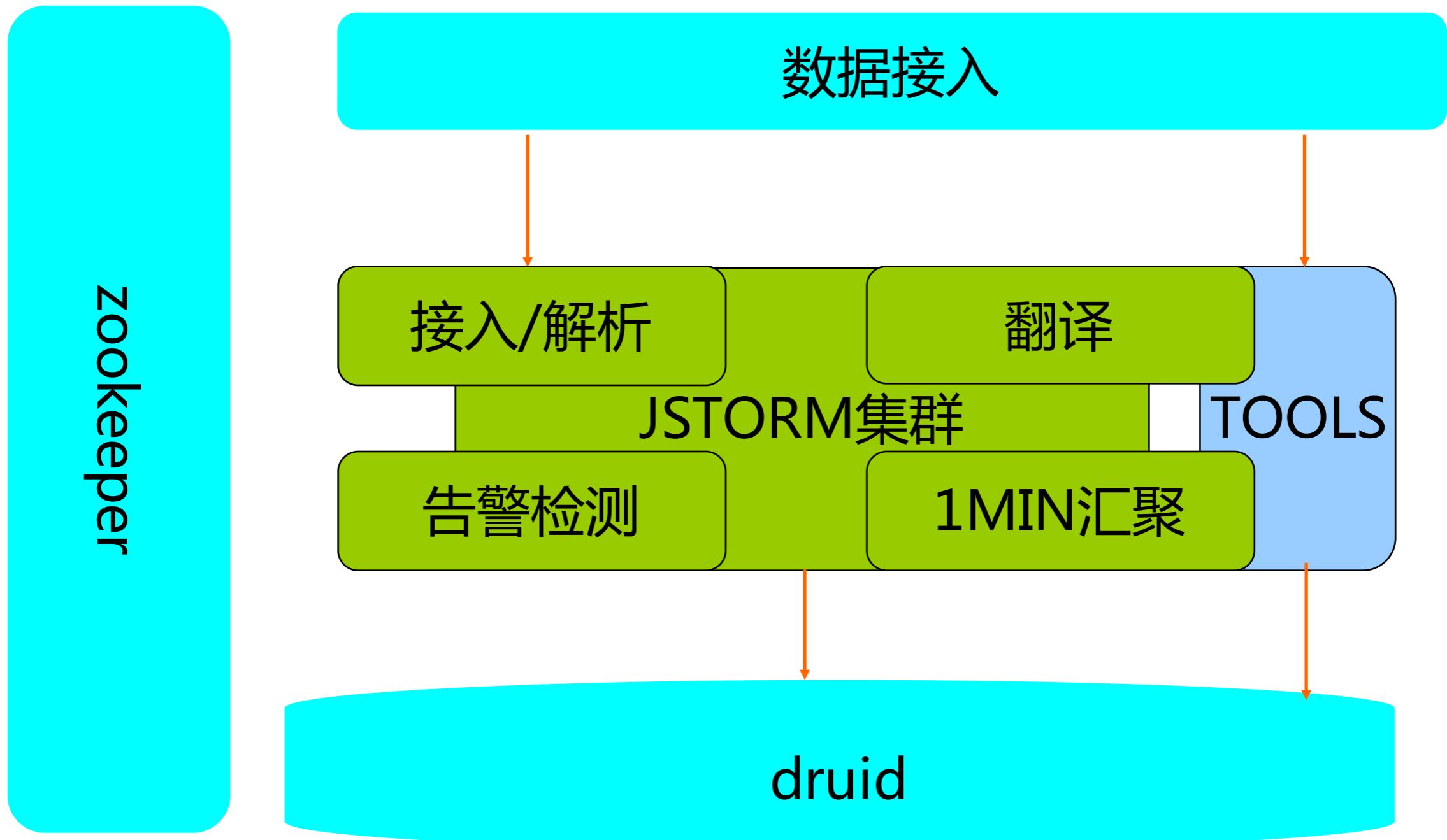
海量日志监控平台挑战

海量日志平台方案

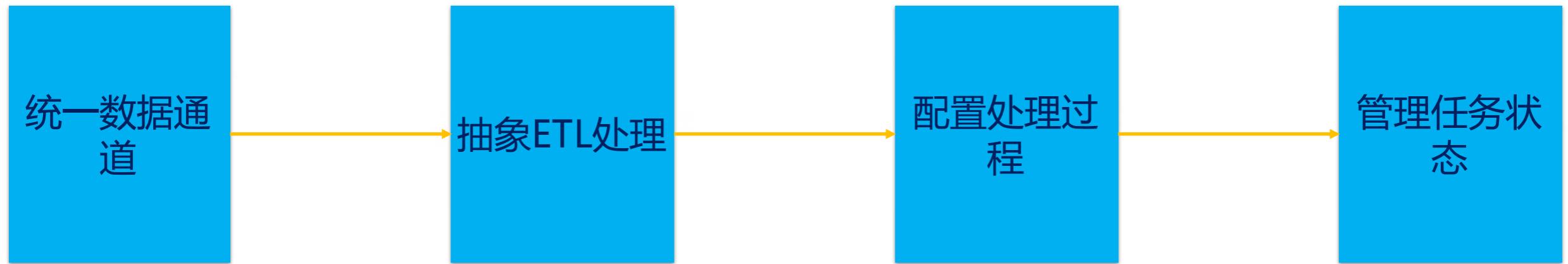
异构数据监控的解决方案

平台运维方案

异构数据处理



任务处理可配置化



| ID | 流程名称 | 数据源ID | 所属业务 | 所属产品 | 数据申请人 | 申请时间 | 运营状态 | 启停计算 | 相关操作 | | |
|------|---------------------|-------------|------|---------|-------|---------------------|------|------|------|--|--|
| 5203 | boss外部调用 | dc02334 | 企点 | BOSS | | 2017-08-30 17:27:01 | 审核中 | | | | |
| 5181 | 企点分析与电话自身数据上报 | dc02195 | 企点 | 企点cc | | 2017-08-08 16:58:47 | 运行中 | | | | |
| 5120 | dispatch_空间数据IP下钻 | dc01803 | 老哈勃 | MM | | 2017-05-08 10:50:25 | 运行中 | | | | |
| 5116 | mm_acc | dc01802 | 老哈勃 | MM | | 2017-04-20 11:55:17 | 运行中 | | | | |
| 5182 | 企点分析与电话业务数据上报 | dc02168 | 企点 | 企点cc | | 2017-08-08 19:32:26 | 运行中 | | | | |
| 5188 | upload卡顿率 | dc00962 | 视频云 | upload | | 2017-08-17 12:08:48 | 运行中 | | | | |
| 5051 | CDN播放结束 | dc00977 | 视频云 | CDN | | 2016-12-15 11:35:15 | 已停用 | | | | |
| 5185 | QZHTTP-CGI监控,QZHTTP | qz_cgi_stat | 监控系统 | QZ组件监控 | | 2017-08-15 18:50:58 | 运行中 | | | | |
| 5186 | Qzone同步中心网络延时 | dtsnetdelay | QQ空间 | DTS组件监控 | | 2017-08-16 16:20:03 | 运行中 | | | | |

集中任务管理

flow名称:

测速QUA

flow管理员:



业务:

监控系统

分配计算
资源

数据量: (单位万/分钟)

6

数据源: (目前仅支持dc)

DC

分配计算
集群

集群设置:

(公共集群)

产品:

用户端监控

当前状态:

待审核

DCId:

dc01019

数据库Id: (可单击查看)

6 (公共druid)

模块:

用户端监控

数据协议:

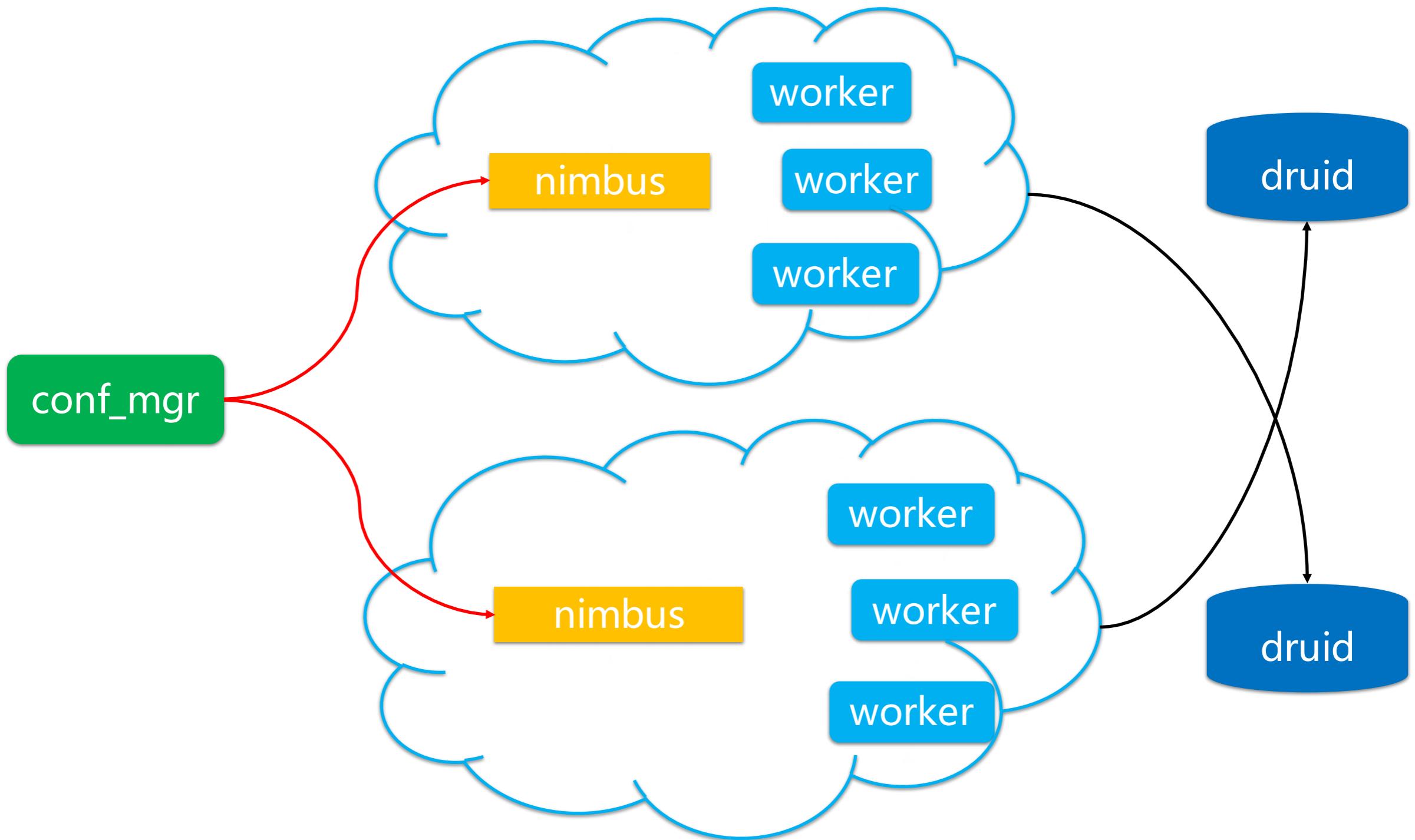
udp

L5Id: (为空则自动创建)*

[NOSET]

定义数
据源

任务分配



平台化服务

关键指标

H5监控

CGI拨测

路由监控

容量

高负载

变更体检

模块调用监控

统一API

monitor基础监控

哈勃多维监控

全链路日志

告警平台

TABLE OF CONTENTS

由面到点的异常分析案例

海量日志监控平台挑战

海量日志平台方案

异构数据监控的解决方案

平台运维方案

容量监控

单机最大值类{[N][ITIL平台]-[ITIL监控][移动监控]-[MM客户端][SET_SZ][接入]}{host-10- - -}

}:[CPU Average Used当前值100

大于85 「58/68」 (69123){

10. }[09-08 22:5

<http://e16cY> .140/c/c

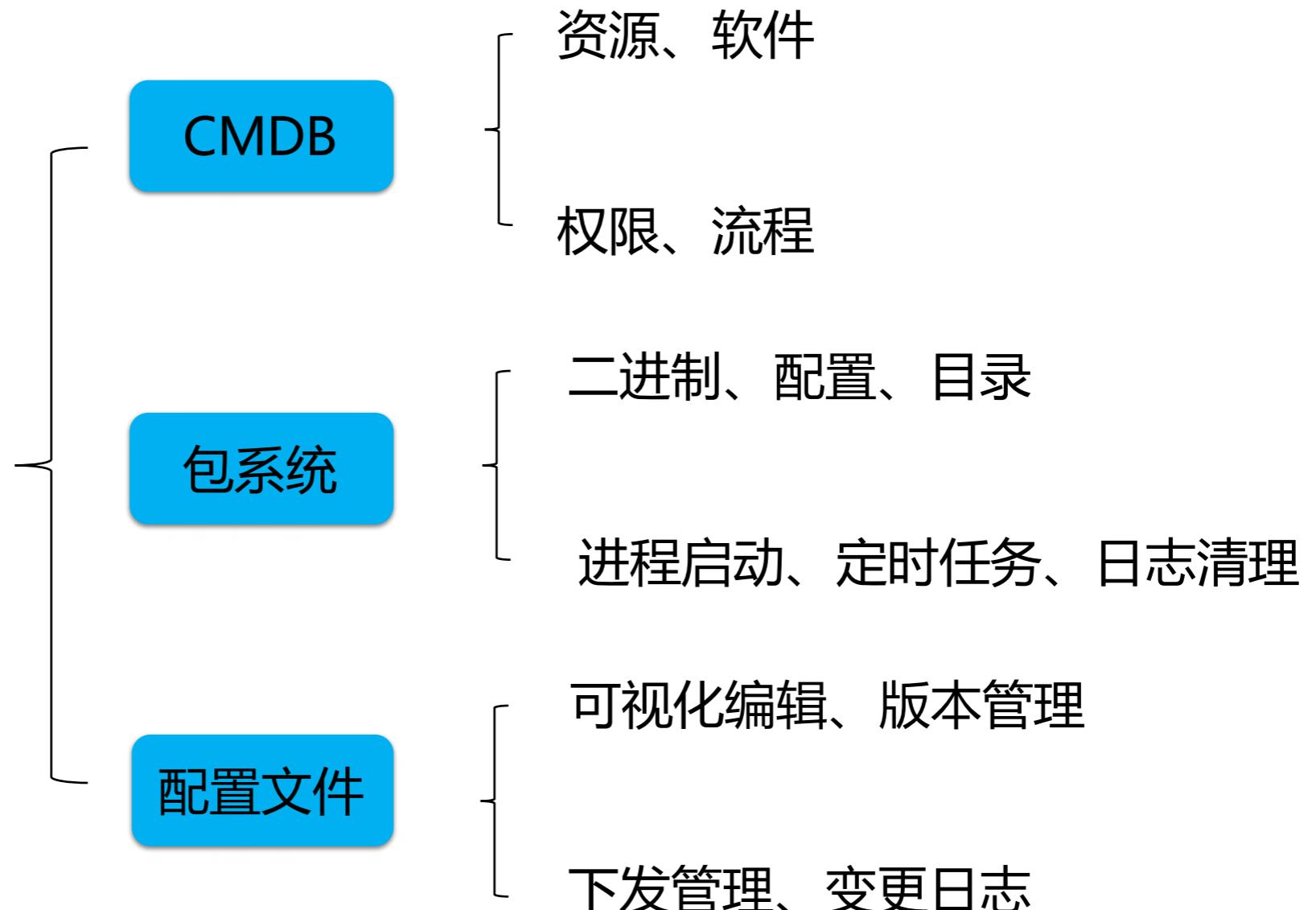
服务器10.

在2017-09-02

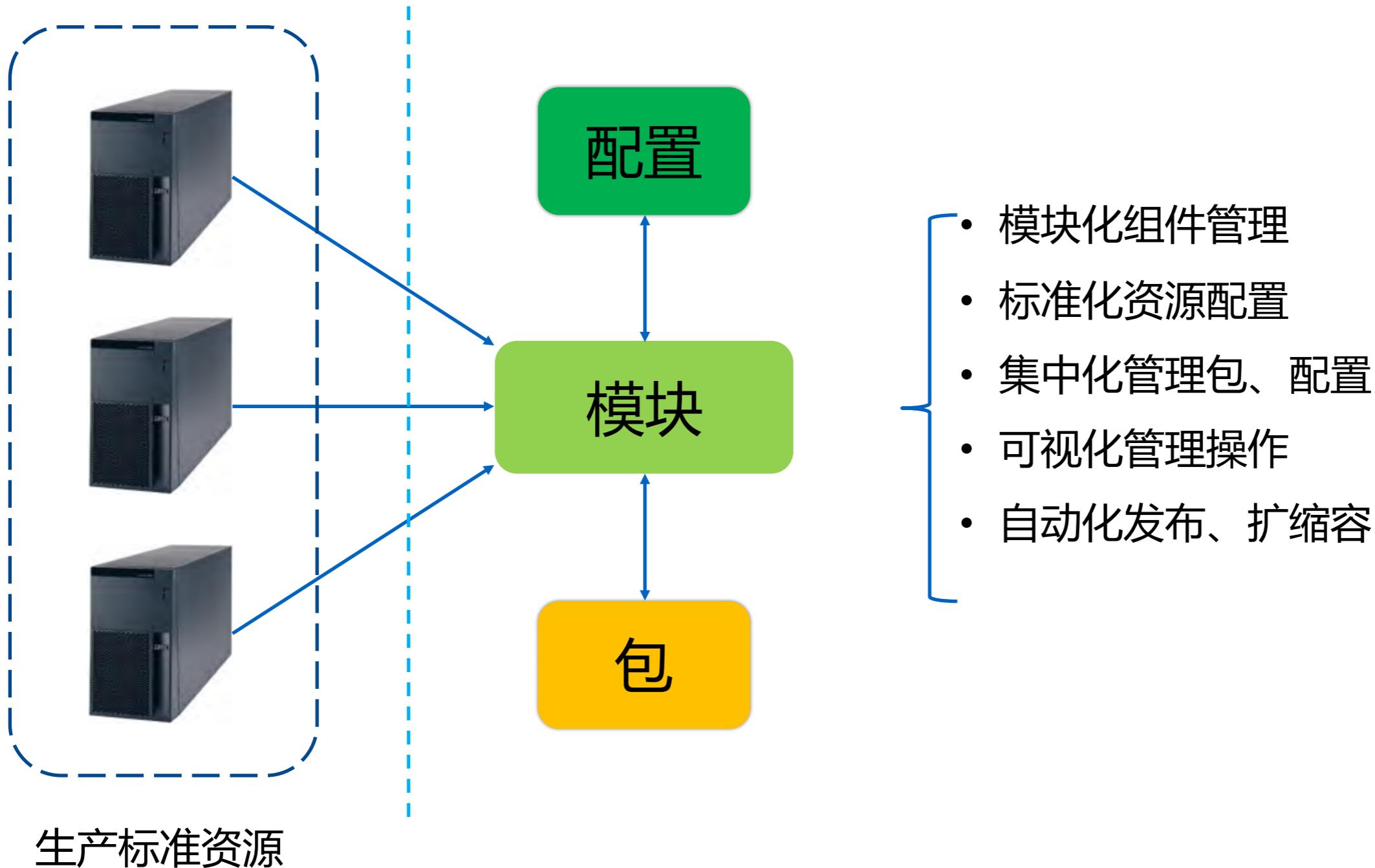
07:12:13发生了硬盘告警。

故障描述：硬盘使用率告警:分区13
使用率96.03%,大于等于96%,剩余
容量10.35G

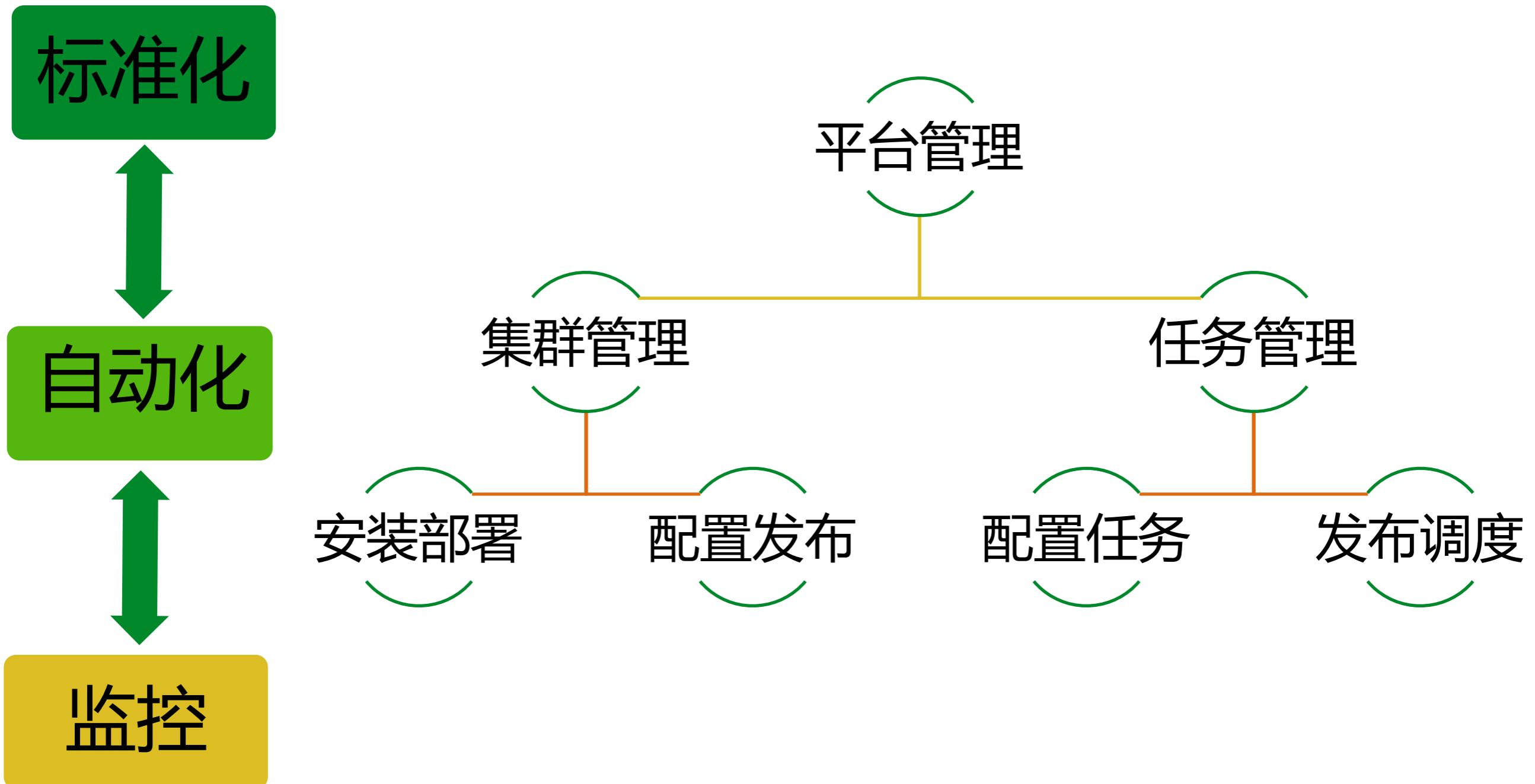
标准化模块



自动化管理



平台管理总结



联系我们



吴树生

广东 深圳



扫一扫上面的二维码图案，加我微信

THANKS!

智 能 时 代 的 新 运 维

CNUTCon 2017