



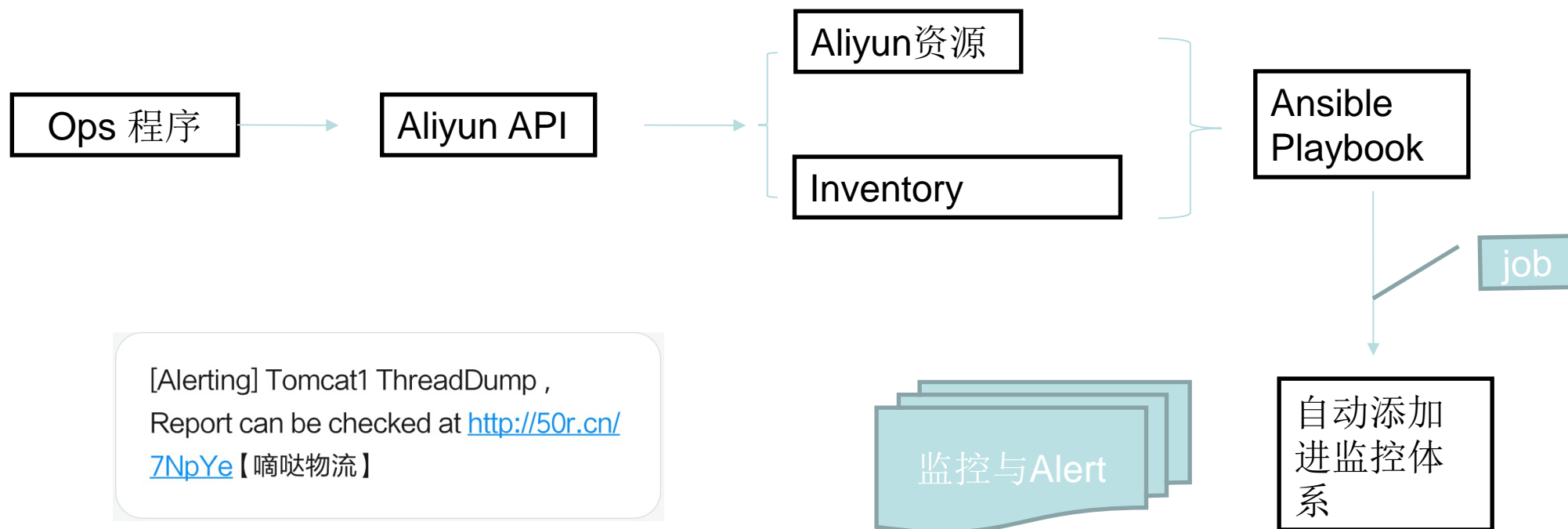
# 嘀哒物流的ELK容器化与警告

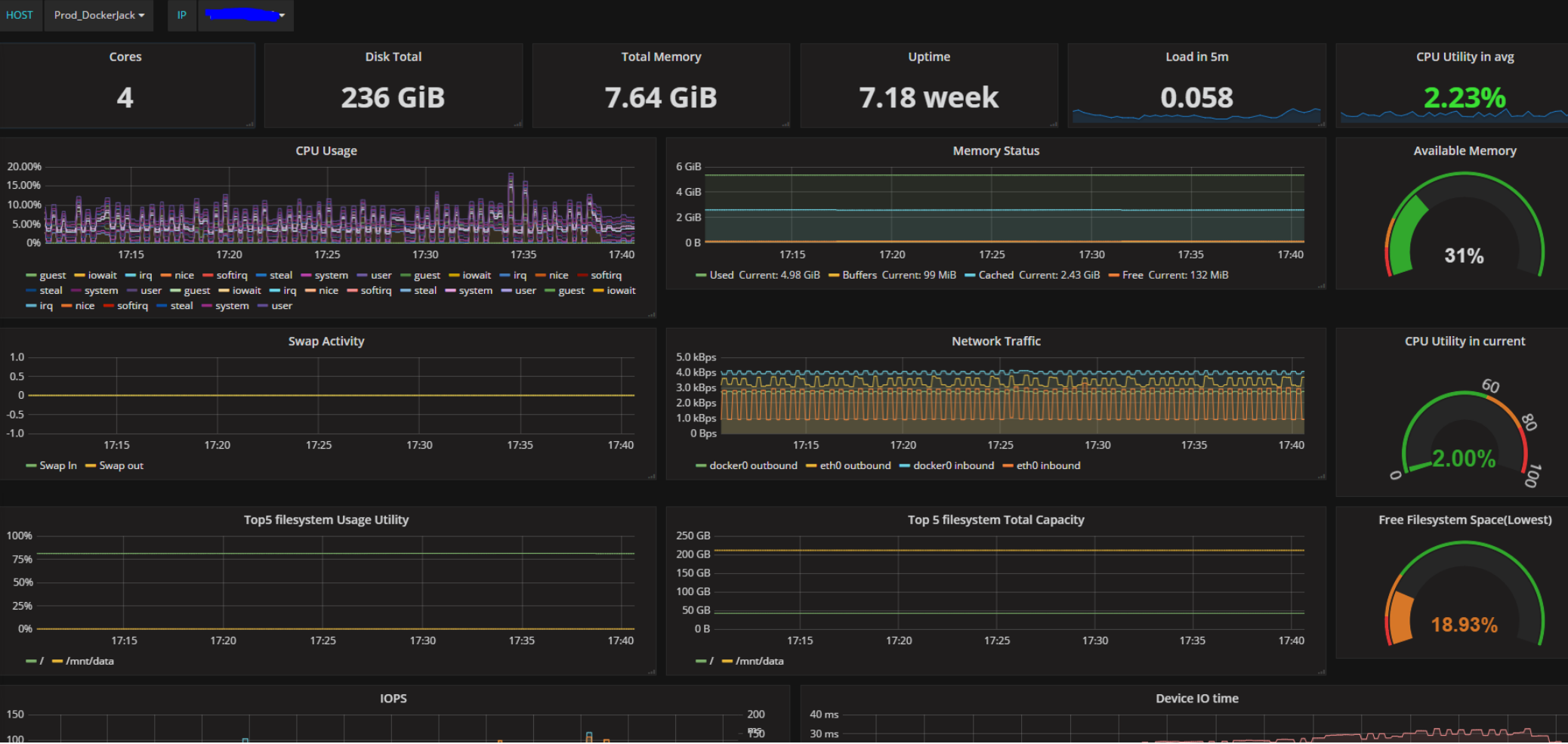
—在运维中的使用

瞿盛熙

- 2016年底成立
- 互联网运力交易平台
- 截至目前，成交金额累计超过数十亿
- 交易特点--低频高额

- 没有IDC,运算存储均在云上
- 基本框架:





MySQL Uptime

10.8 week

Current QPS

248.20

Max allowed coonection

4050

Current Connection

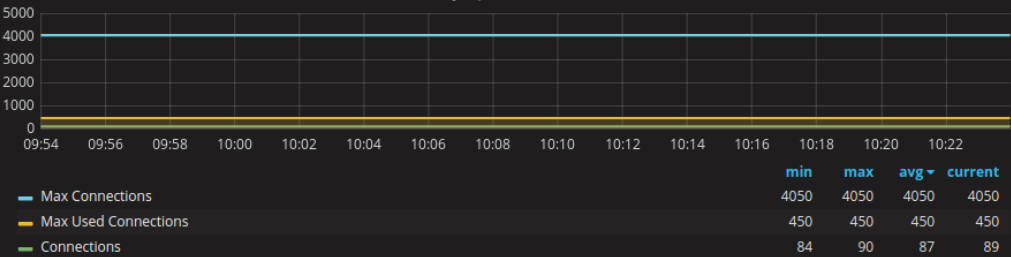
89

Total DeadLock

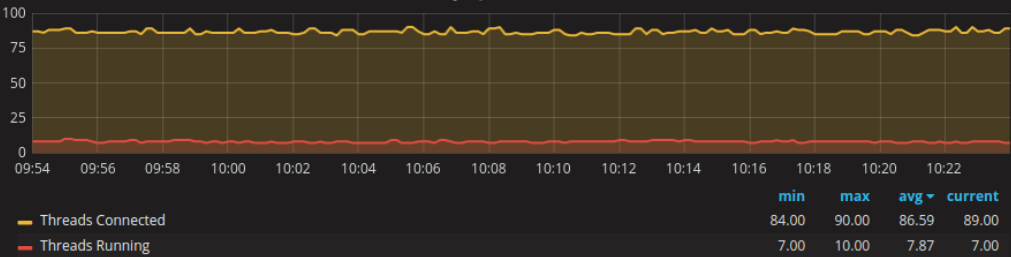
1

Empty Space

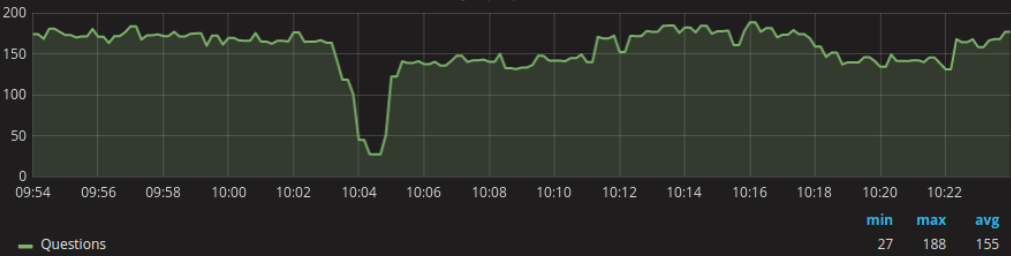
MySQL Connections



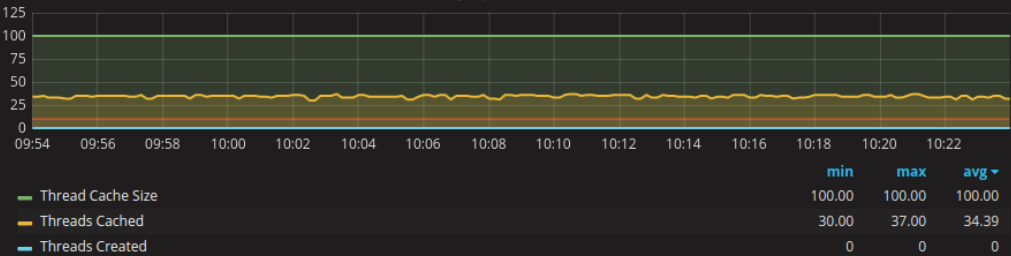
MySQL Active Threads



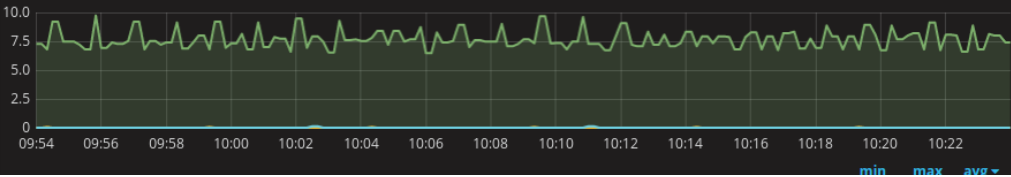
MySQL Questions



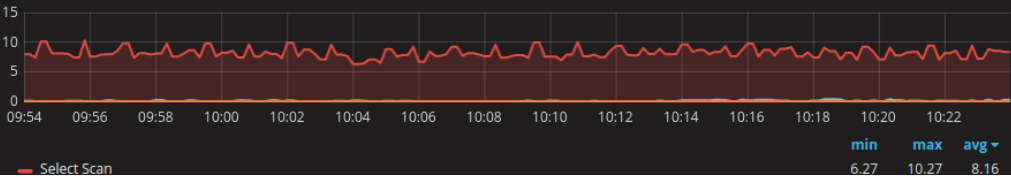
MySQL Thread Cache



MySQL Temporary Objects



MySQL Select Types



- 主要需求：

1. 日志信息搜集

- > 子系统工作情况
- > 定位错误

2. metric补充

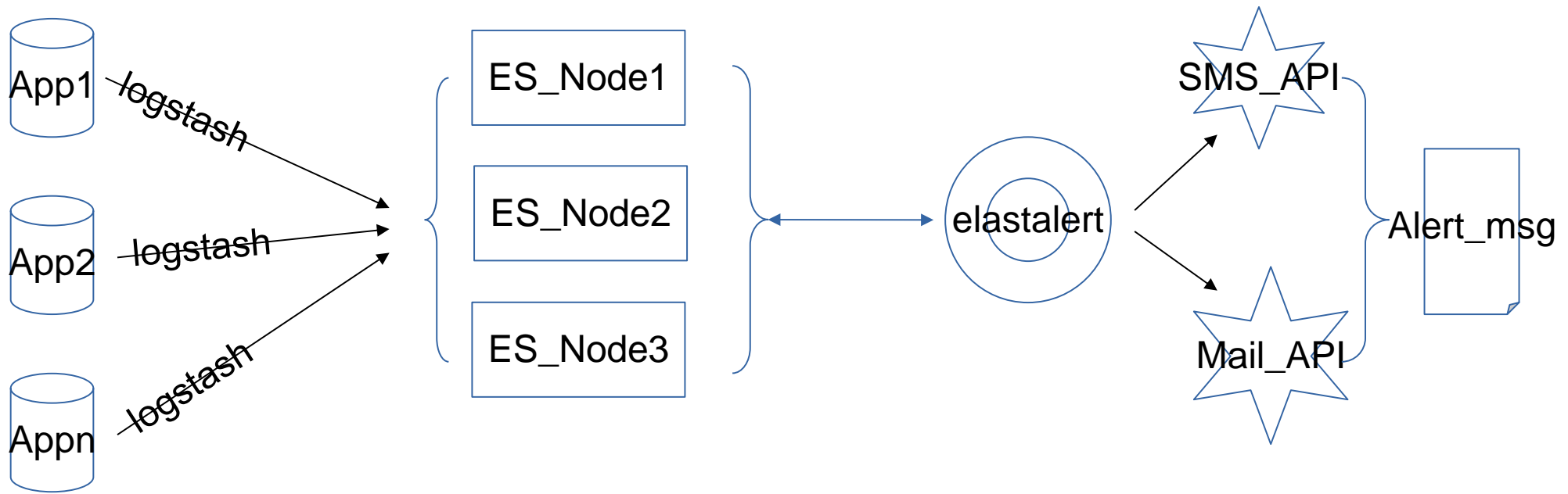
- > 基于prometheus的metric警告有所不足
- > 缺少基于日志内容的警告

...





# 如何使用ELK?





- Package安装vs Docker

- 关注点:

- 1.性能
2. 灵活性
3. 资源利用率
4. 是否持久化

# Kubernetes?

有考虑使用Kubernetes做部署,之所以暂时没有使用:

- 1.精力时间有限
- 2.抽象概念层次较多, Pod, Deployment, Service, Port, NodePort, TargetPort. 需要时间让团队熟悉.
- 3.阿里云的Cloud provider似乎还没有整合进Kubernetes
- 4.翻墙
- 3.基于目前使用需求.且并非单纯的Docker环境

最终，我们采用了下面的部署方式：

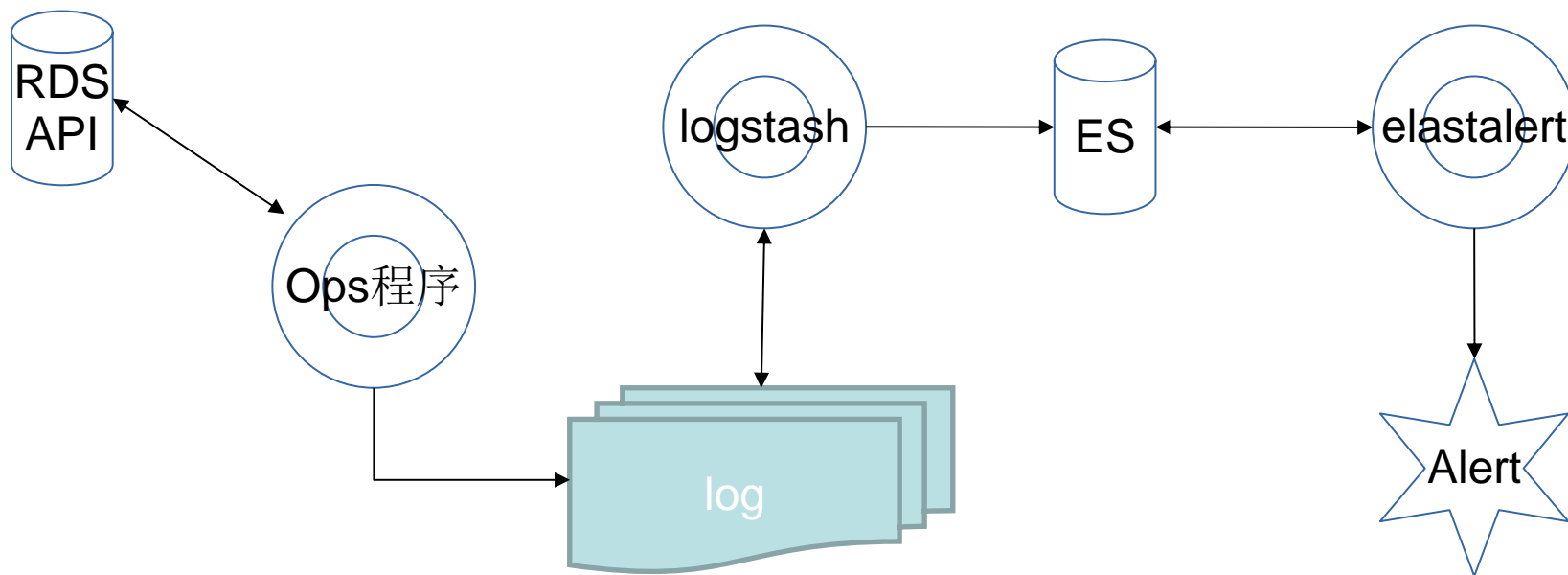
- 1.使用Docker engine
- 2.部署自己的镜像仓库
- 3.基于官方的镜像,重新build自己的镜像，安装相关插件
- 4.使用安全组控制访问ES

- 目前ELK在嘀哒主要使用在
  - 1.基于kibana的日志搜索
  - 2.基于关键词的警告

## Yelp/elastalert, 灵活定义间隔与触发条件 二次开发, 一次读入多个配置

```
_type: didapay
host: 172.17.0.1
kibana_link: http://172.17.0.1/app/kibana#/dashboard/temp/AVuuFhgPuV3d8e53x4ap
message: 2017-04-27 14:25:01.269 [http-nio-30000-exec-2] ERROR d.api.pay.service.EasterPayService - 请求东方付通返回余额信息发生错误!
num_hits: 8
num_matches: 2
match: /test/didapay/test/didapay-test
```

# RDS的死锁



\_type: deadlock

host: rds\_ma

kibana\_link: [http://\[redacted\]/app/kibana#/dashboard/temp/AVuklr-3uV3d8e53v1O6](http://[redacted]/app/kibana#/dashboard/temp/AVuklr-3uV3d8e53v1O6)

message: [redacted] 2017-04-25T10:47:07 33580302 0 [redacted] company PRIMARY RECORD S w 0 insert into teamcompany ( platform\_id, team\_id, team\_name, cy\_company\_id, fd\_company\_id, create\_date, if\_system, type ) values ( 'JS\*DDWL\*0001', concat('default',(select t.seq\_id from company t where t.if\_admin='Y' and t.platform\_id='JS\*DDWL\*0001')), '??', 144450, (select t.seq\_id from company t where t.if\_admin='Y' and t.platform\_id='JS\*DDWL\*0001'), now(), 'N', '1' )

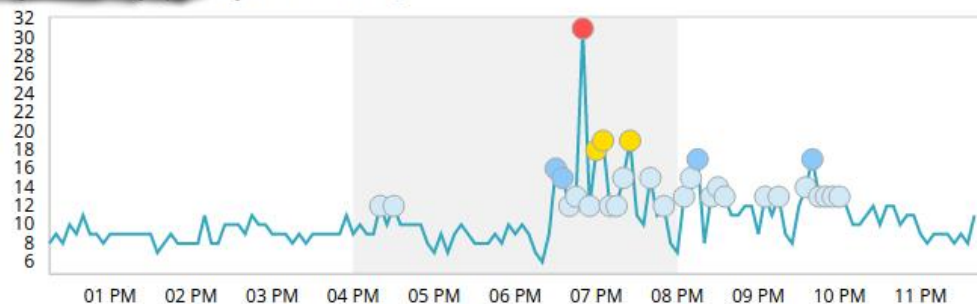
num\_hits: 5

num\_matches: 5

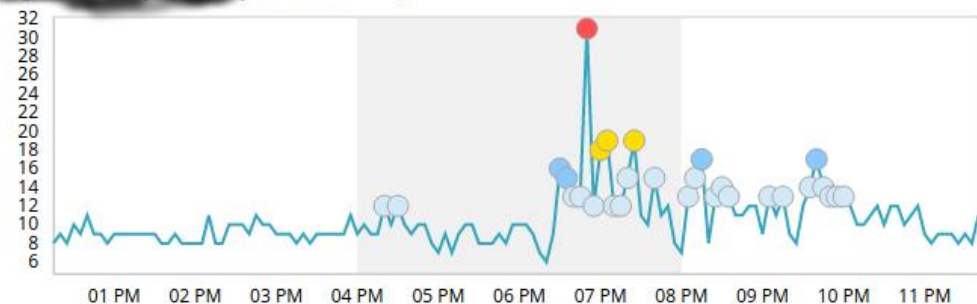
# 基于ML的预警

## Anomalies

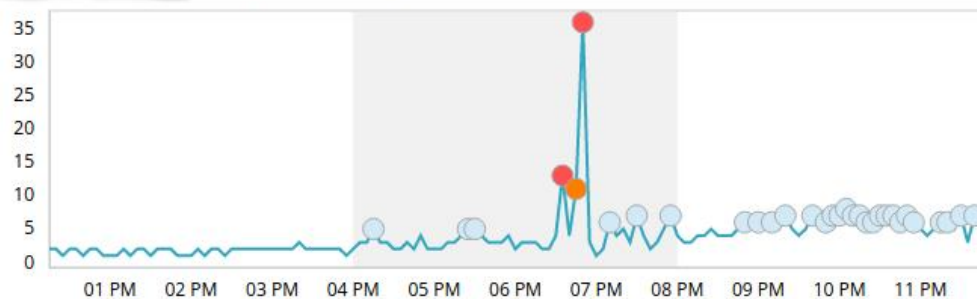
distinct\_count(mysql.status.threads.connected) - metricset.host.keyword  
yaqje2016ext.mysql.rds.aliyuncs.com:3306 ⓘ



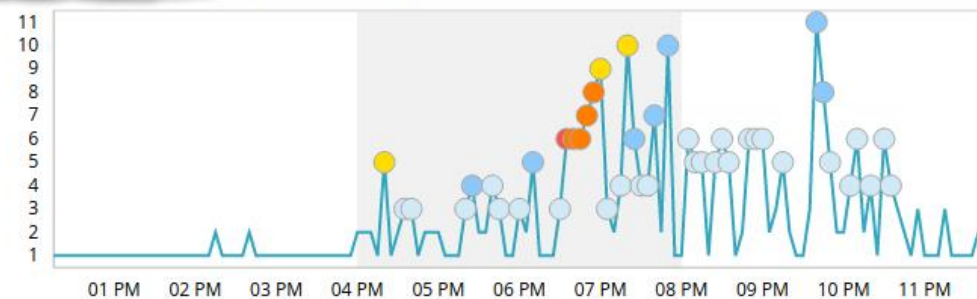
distinct\_count(mysql.status.threads.cached) - metricset.host.keyword  
yaqje2016ext.mysql.rds.aliyuncs.com:3306 ⓘ



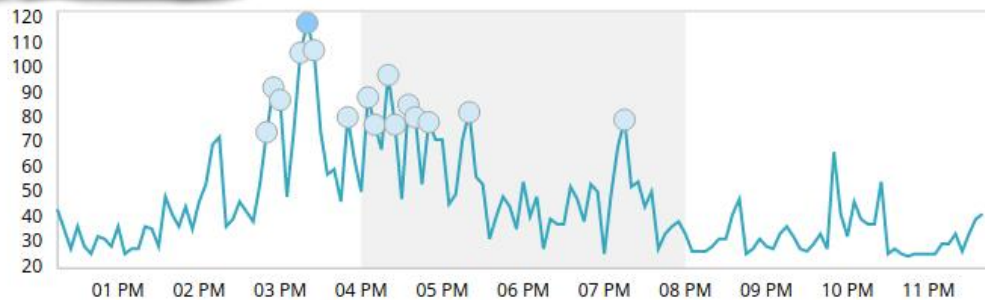
distinct\_count(mysql.status.threads.running) - metricset.host.keyword  
yaqje2016ext.mysql.rds.aliyuncs.com:3306 ⓘ




distinct\_count(mysql.status.aborted.clients) - metricset.host.keyword  
yaqje2016ext.mysql.rds.aliyuncs.com:3306 ⓘ



distinct\_count(mysql.status.command.update) - metricset.host.keyword  
yaqje2016ext.mysql.rds.aliyuncs.com:3306 ⓘ







下一步？

- 将在未来2~3月内，使用K8s部署ELK
- metricbeat + machine learning,探索对metric的趋势分析模型，尝试融合或替代Prometheus
- 跨云的日志搜集



# Thank U

Mobile: 15150676721