ELK 系统综述

主讲人 - 林邦骏

网易在线游戏事业部

Contents

1 运维与基础架构部 ELK 系统整体现状

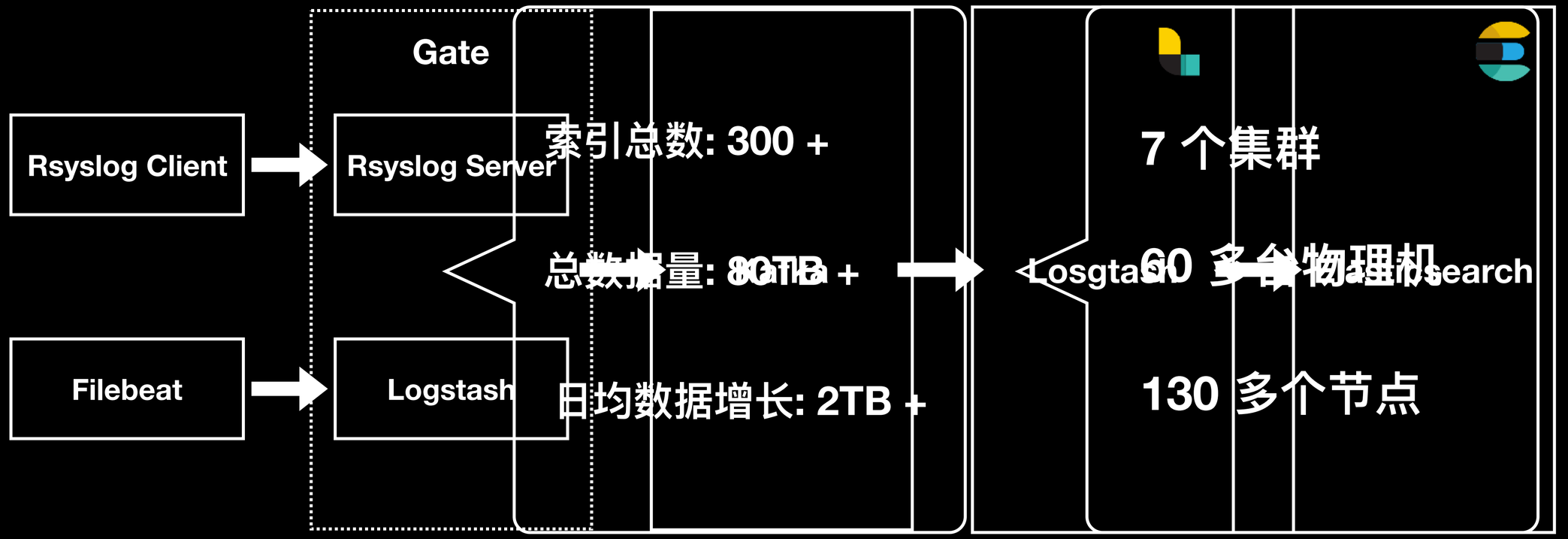
2 Logstash & Elasticsearch

3 周边功能

4 总结 & QA

ELK 系统整体现状

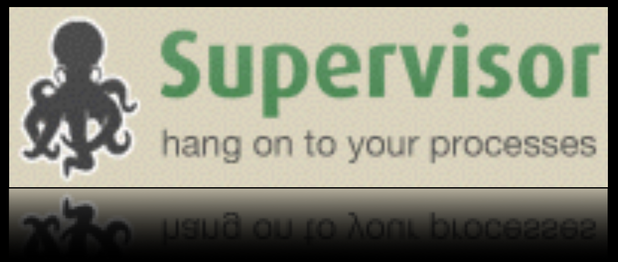
架构总览


Gate
Rsyslog Client
Rsyslog Server
Filebeat
Logstash
索引总数: 300 +
总数据量: 80TB +
日均数据增长: 2TB +
7 个集群
60 多台物理机
130 多个节点

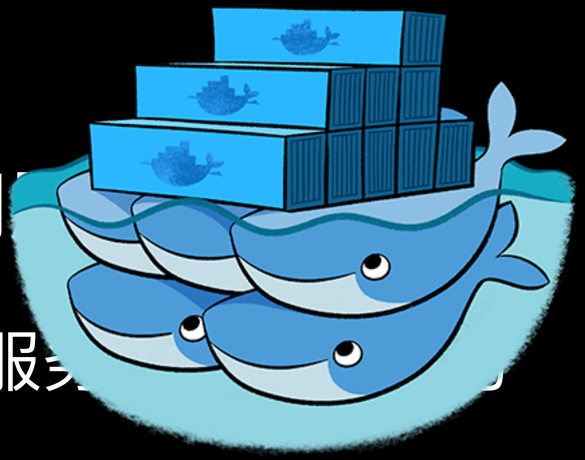
Logstash & Elasticsearch

ogstash 集群的演变

从 supervisor 到 swarm



- 服务器负载不均匀
- 资源难以调度
- 服务对外不透明
- 配置文件难以管理



- 资源难以调度
  - 自带调度策略
- 服务对外不透明
  - “半透明进程”服务
- 配置文件难以管理
  - 共享文件系统，便于管理配置文件

swarm 还缺了什么？

服务器负载不均匀

Why?

无法感知进程的“需要”

How?

- 收集数据
- 计算阈值
- 更新容器

What’s more?

- 容器监控

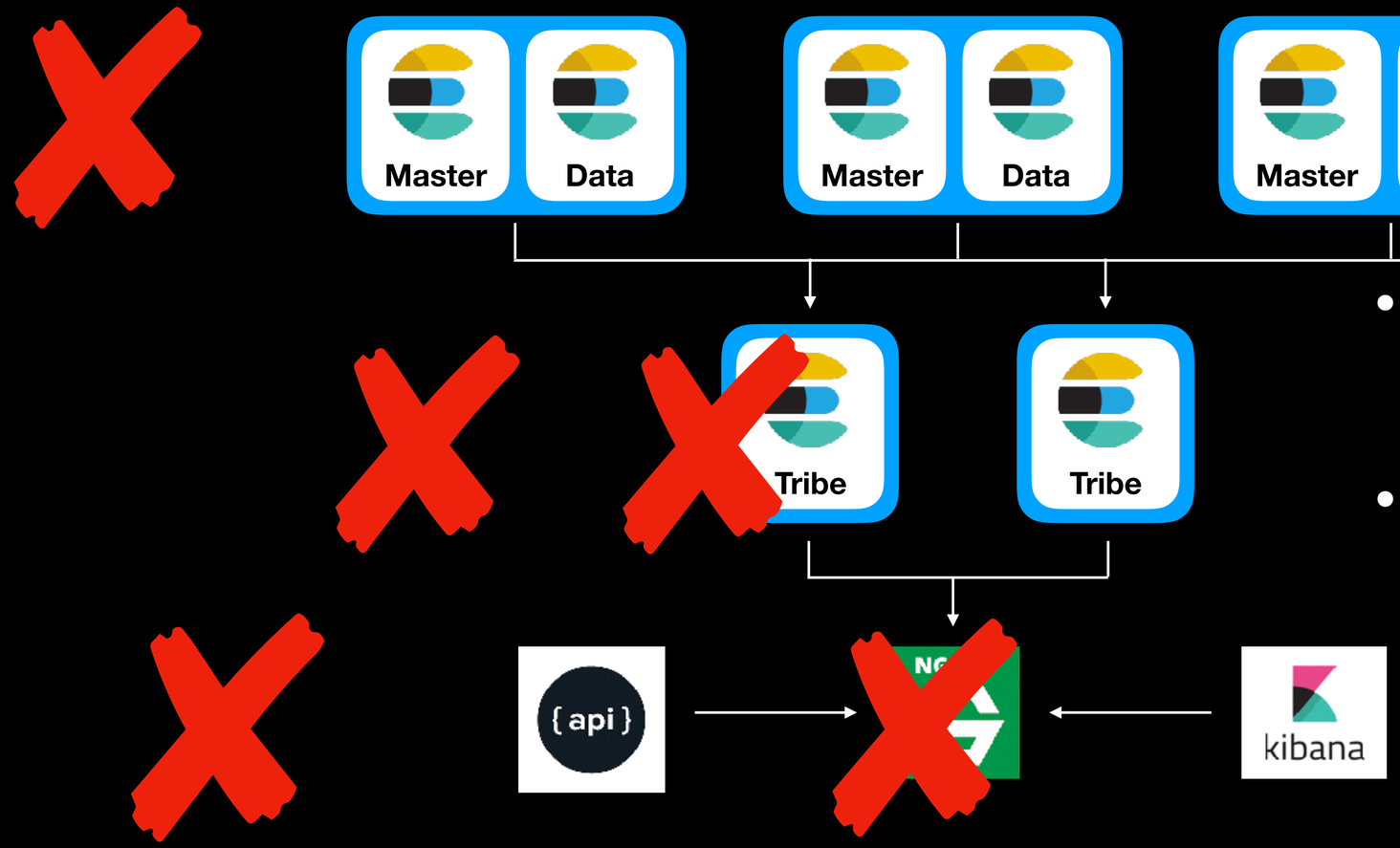
容器监控

Elasticsearch 集群的演变

— 架构篇

Tribe node 的实践

BUT !

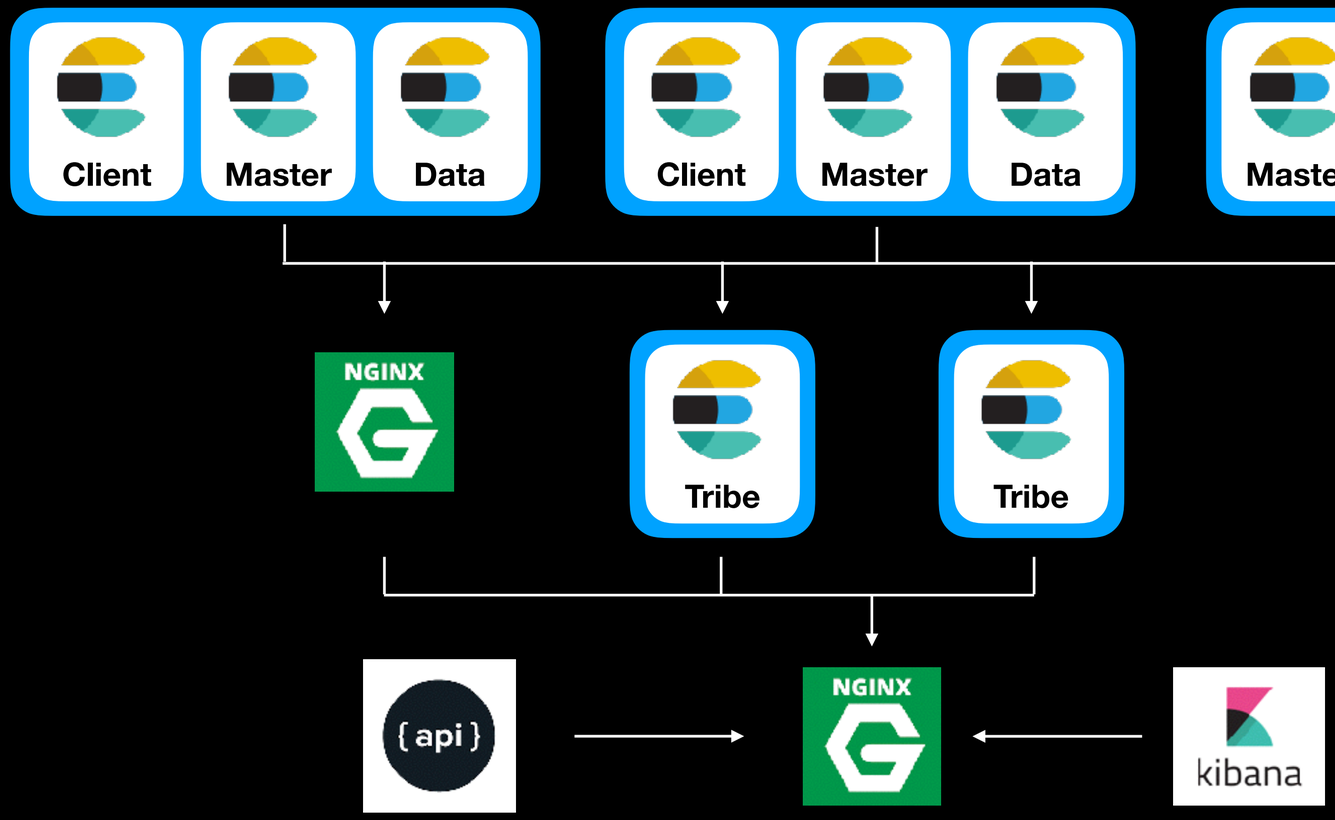


集群只有 Master, Data

...

- 使用 Tribe 节点
- Nginx 负载均衡

集群的改进



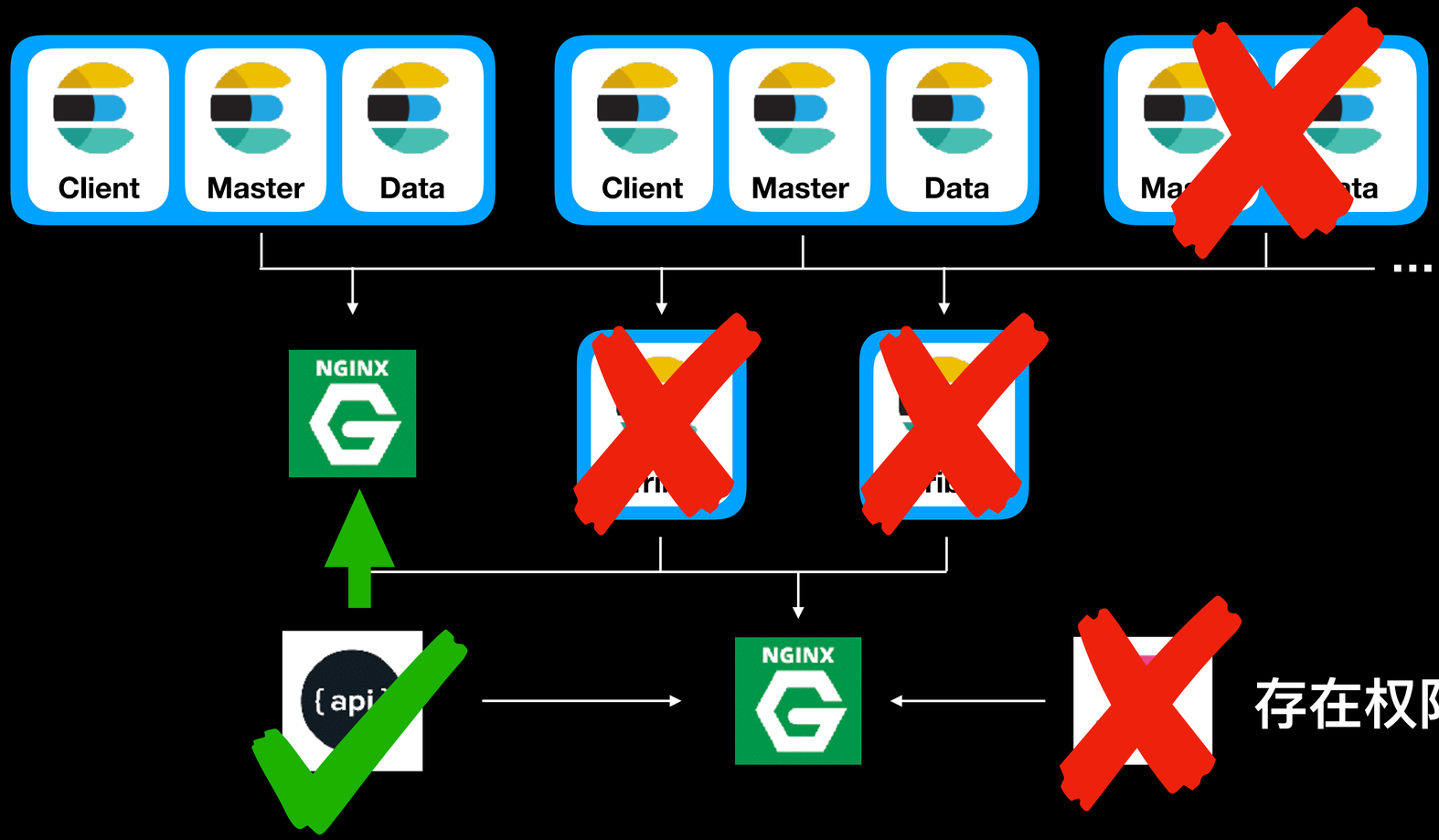
- 集群引入 Client
  - … 分摊 Master 节点工作
- 加入新的 Nginx
  - 以反代的方式模仿 Tribe 的行为

集群的改进

核心: 转发请求


```
upstream es_tribe {
    server 1.1.1.1:9200;
}

upstream es_cluster1 {
  server 10.0.0.1:9200;
  server 10.0.0.2:9200;
}

upstream es_cluster2 {
  server 10.0.1.1:9200;
  server 10.0.1.2:9200;
}

server {
   listen 9200;

   location ^~ /(index1|index2) {
     proxy_pass http://es_cluster1;
   }
   ...
}
```

效果与缺陷



存在权限校验, kibana 必须经过 ES 节点

Elasticsearch 集群的演变

— 优化篇

分片调优

Why?

- 查询效率
- 写入效率

What effect?

- 分片数量
- 分片大小
- 磁盘 IO

How?

- 收集数据
- 预估大小
- 更新配置

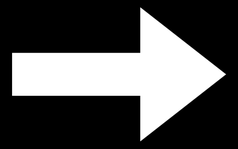
What's More?

- 自动化任务

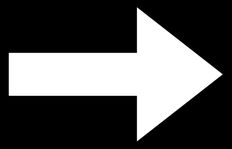
自动化任务

单个索引最大容量
m Gm 节点数

读取最近 N 天数据，
收集数据，存入 ES
预估 30 天数据大小



按天或者按月分索引

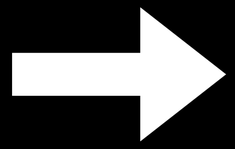


分片数量的多少

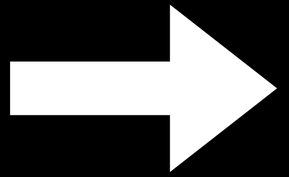
自动化任务

索引数据的时间戳

节点所在磁盘的 IO



越新的数据放在 IO 性能越好的节点上，反之亦然



索引的“上浮与下沉”

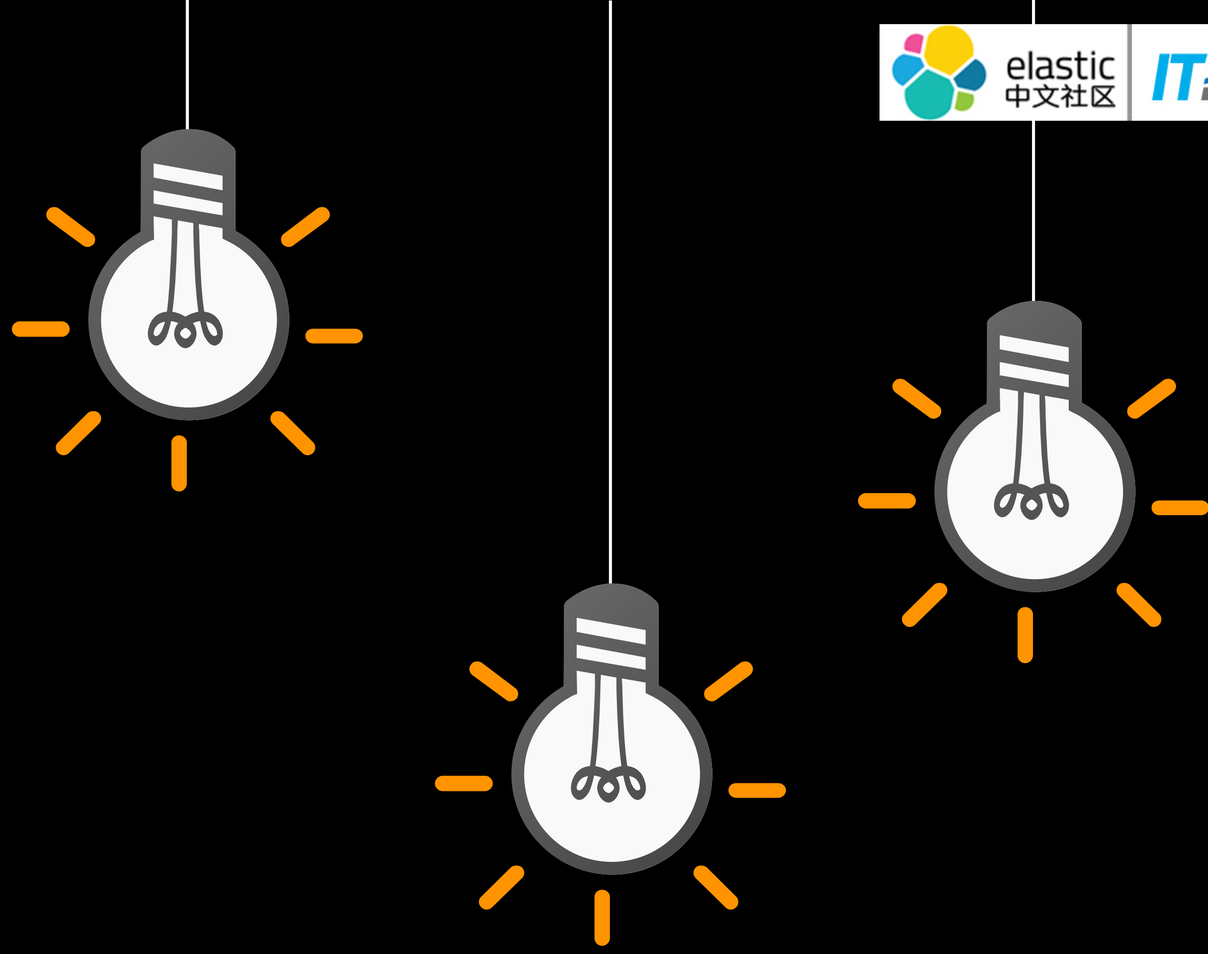
周边功能

周边功能

- 索引自助接入、自助下线
- 自助更新 Logstash 正则
- 日志告警
- 索引权限管理、操作记录审计

总结

More like a platform, More close to SAAS



Q&A

THANKS

主讲人 - 林邦骏

运维与基础架构部