



# ES平台化建设与实践

张海雷@字节跳动





# 大纲

- 架构概览
- 平台化建设
- 实践总结





# ES@字节跳动



日志Debug

明细&聚合查询  
实时性强



Search

低延迟  
高吞吐



监控

实时性强  
兼顾Debug



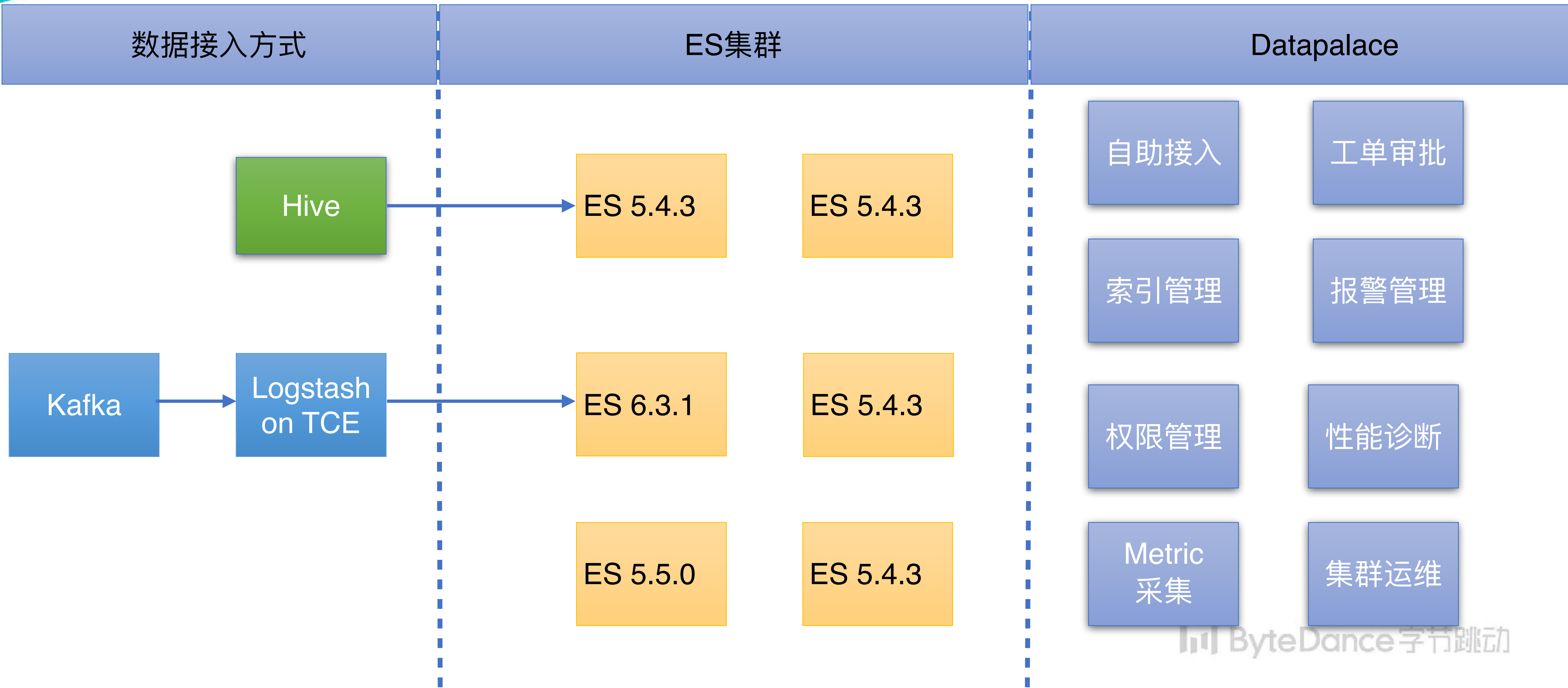
报表

高并发  
可更新



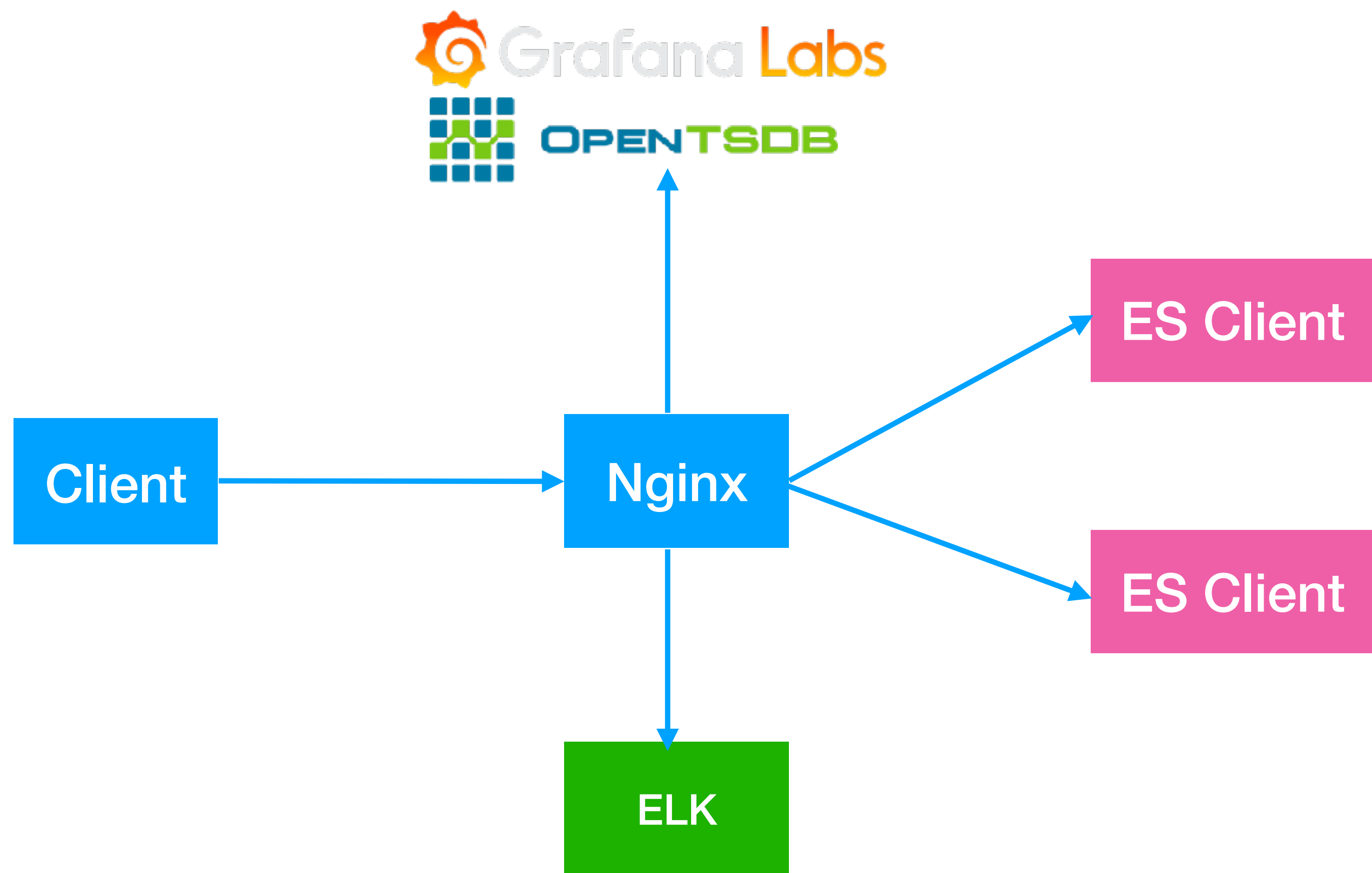


# ES架构@字节跳动





# 查询链路







# Logstash->ES

★从2.x升级到5.x

★改造Metric

★热更新

★stats API









# Hive->ES


使用开源的elasticsearch\_hadoop

需要解决的两个问题：

★写入重复：MR重试机制，解法设置\_id

★控速：修改MR参数mapreduce.job.running.map.limit





# 集群部署

★多集群还是多Tag?

★SSD和HDD实现冷热分离

★多盘还是Raid?





# 为什么需要平台化

- ❖提升效率
- ❖降低沟通成本
- ❖扩展边界







# 自助接入

工单类型:

新建索引

新建Druid索引

自助接入Druid

新建集群

Druid沙盒测试 ?

1 申请接入新的Elasticsearch索引。

\* 负责人:

zhanghailei



\* ES集群所属部门

IT部



\* 所属服务组:

选择所属服务组



IT部 服务组

\* 目标ES集群:

选择集群



如果您希望指定索引所在的集群，请在此处选择；如果不希望指定，请选择无需指定。

\* 数据来源:

kafka



>10条/s的写入速度必须使用Kafka接入

\* Kafka集群:

集群1



请注意，集群1和不包含后缀的集群不再等价

\* Kafka Topic:

ad\_user\_context

\* 写入速度(messages/s):

不均匀的话填写峰值

\* 数据类型:



JSON



纯文本



protobuf



\* 示例数据:





# 接入流程





# 索引管理

	关心	集群入口	索引名称	划分	负责人	相关链接	Metrics	操作	部署方式
+	♡			按日		<a href="#">自助搜索</a> <a href="#">ES-SQL</a>	<a href="#">Metrics</a> ▾	<a href="#">≡ ▾</a>	TCE
+	♡			按日		<a href="#">自助搜索</a> <a href="#">ES-SQL</a>	<a href="#">Metrics</a> ▾	<a href="#">≡ ▾</a>	TCE
+	♡			按日		<a href="#">自助搜索</a> <a href="#">Kibana</a> <a href="#">ES-SQL</a>	<a href="#">Metrics</a> ▾	<a href="#">≡ ▾</a>	TCE
+	♡			按日		<a href="#">自助搜索</a> <a href="#">ES-SQL</a> <a href="#">Kibana</a>	<a href="#">Metrics</a> ▾	<a href="#">≡ ▾</a>	TCE
+	♡			按日		<a href="#">自助搜索</a> <a href="#">ES-SQL</a> <a href="#">Kibana</a>	<a href="#">Metrics</a> ▾	<a href="#">≡ ▾</a>	TCE
+	♡			按日		<a href="#">自助搜索</a> <a href="#">ES-SQL</a> <a href="#">Kibana</a>	<a href="#">Metrics</a> ▾	<a href="#">≡ ▾</a>	TCE
+	♡			按日		<a href="#">自助搜索</a> <a href="#">ES-SQL</a> <a href="#">Kibana</a>	<a href="#">Metrics</a> ▾	<a href="#">≡ ▾</a>	N/A

- 更新
- 更新mapping
- 以此为模板新建
- 自定义报警
-  
- django admin
- logstash conf管理
- [≡ ▾](#)
- TCE





# 集群监控

## 集群健康

健康度  
节点数量  
Pending Task

## 系统层面

CPU  
Load  
Memory

## 性能诊断

SearchQueue  
BulkQueue  
Merge

## GC

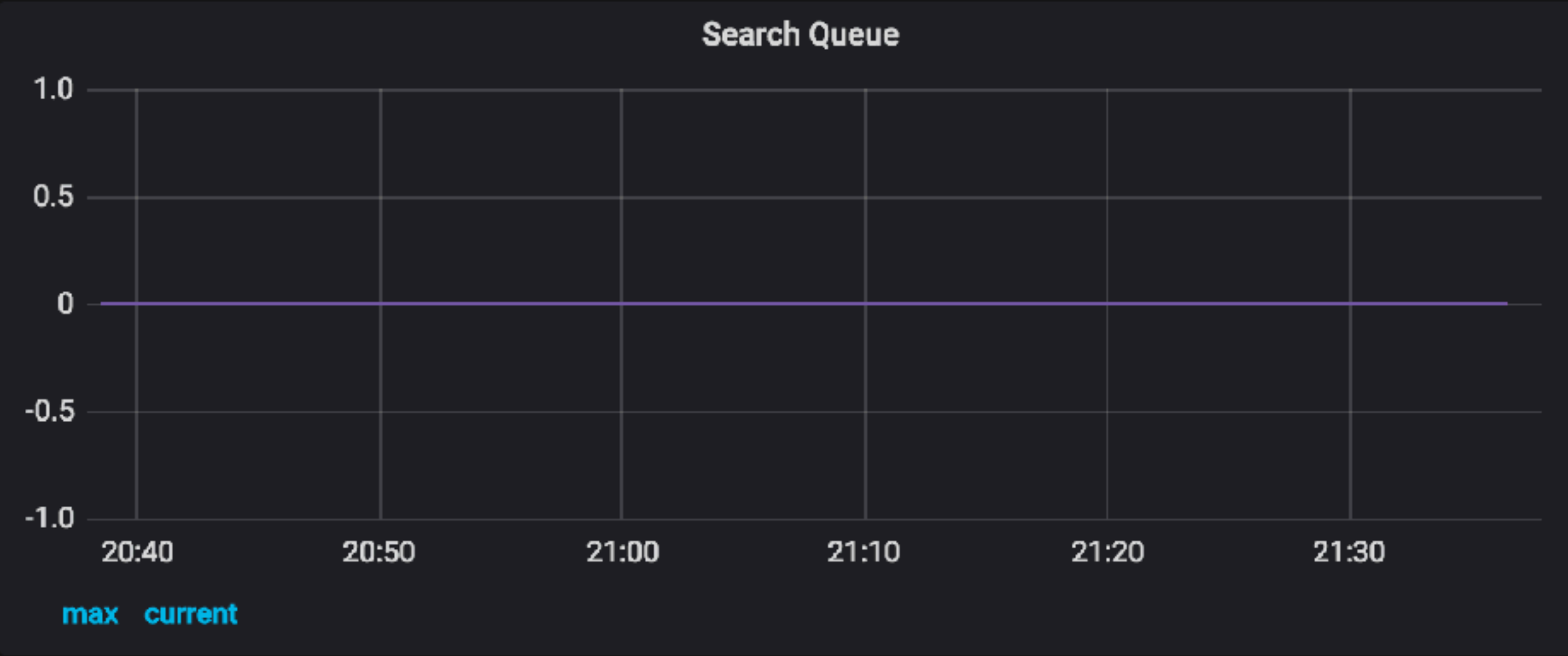
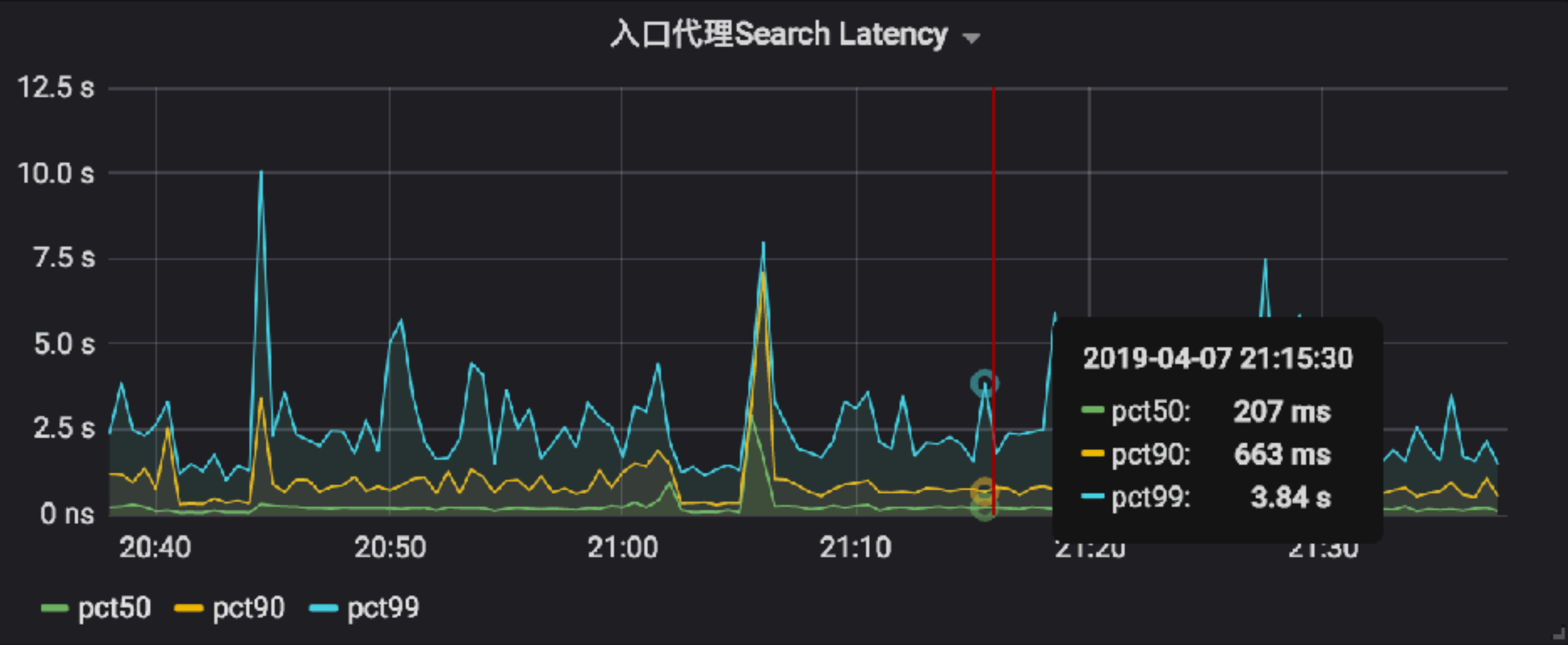
Young GC  
GC次数  
Old GC



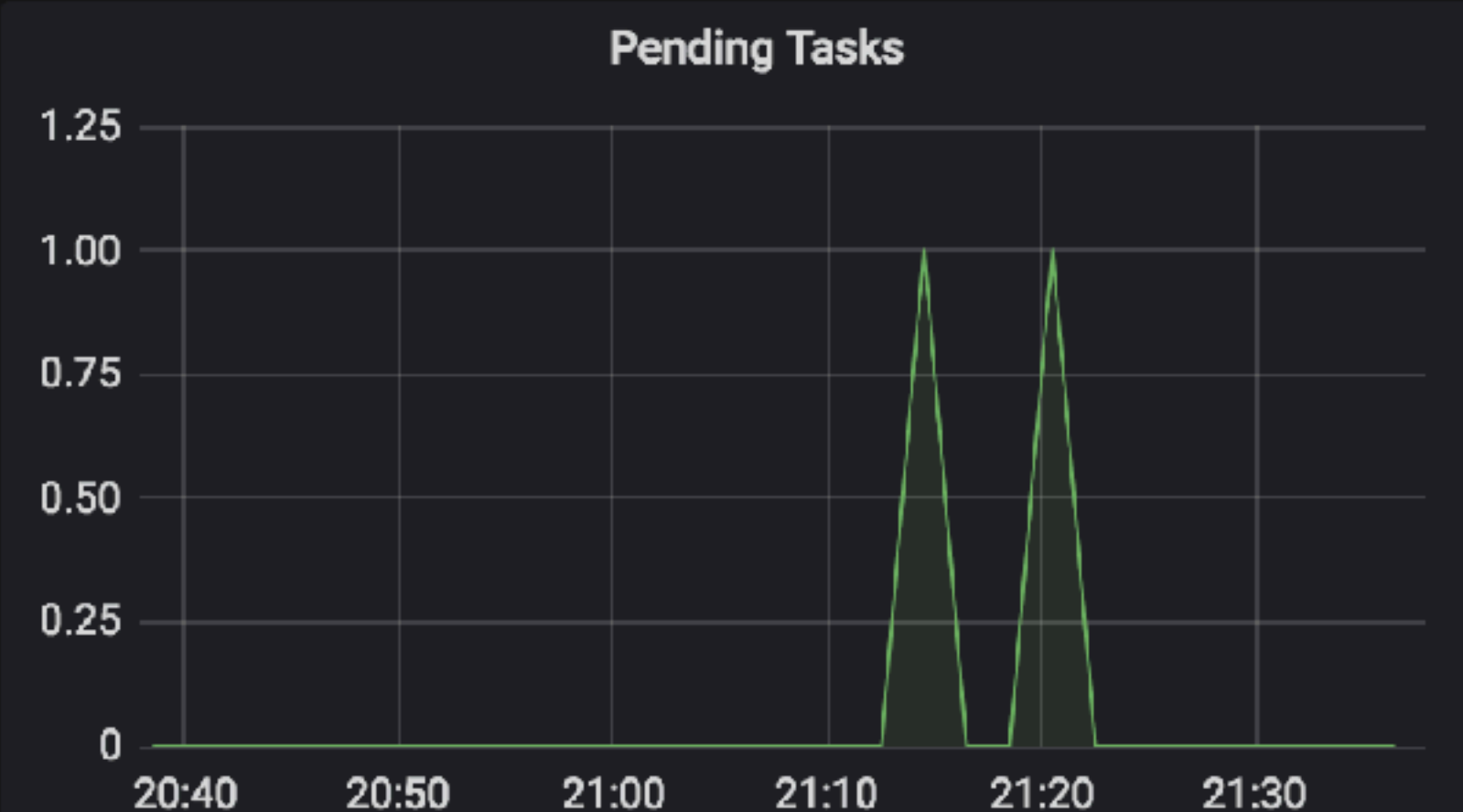


# 集群健康

查询性能



集群基本状态





# 平台化挑战

## 业务隔离

查询隔离  
索引隔离  
业务混部

## 权限控制

数据安全  
账号统一  
防止误操作

## 使用不当

ShardNum设置  
不断更新Mapping  
重查询

## ES稳定性

分布式设计  
Shard分配策略  
OOM  
路由转发





# 困扰我们最多的问题

BulkQueue不均衡，整个集群变慢

OOM

坏盘

Master不可用



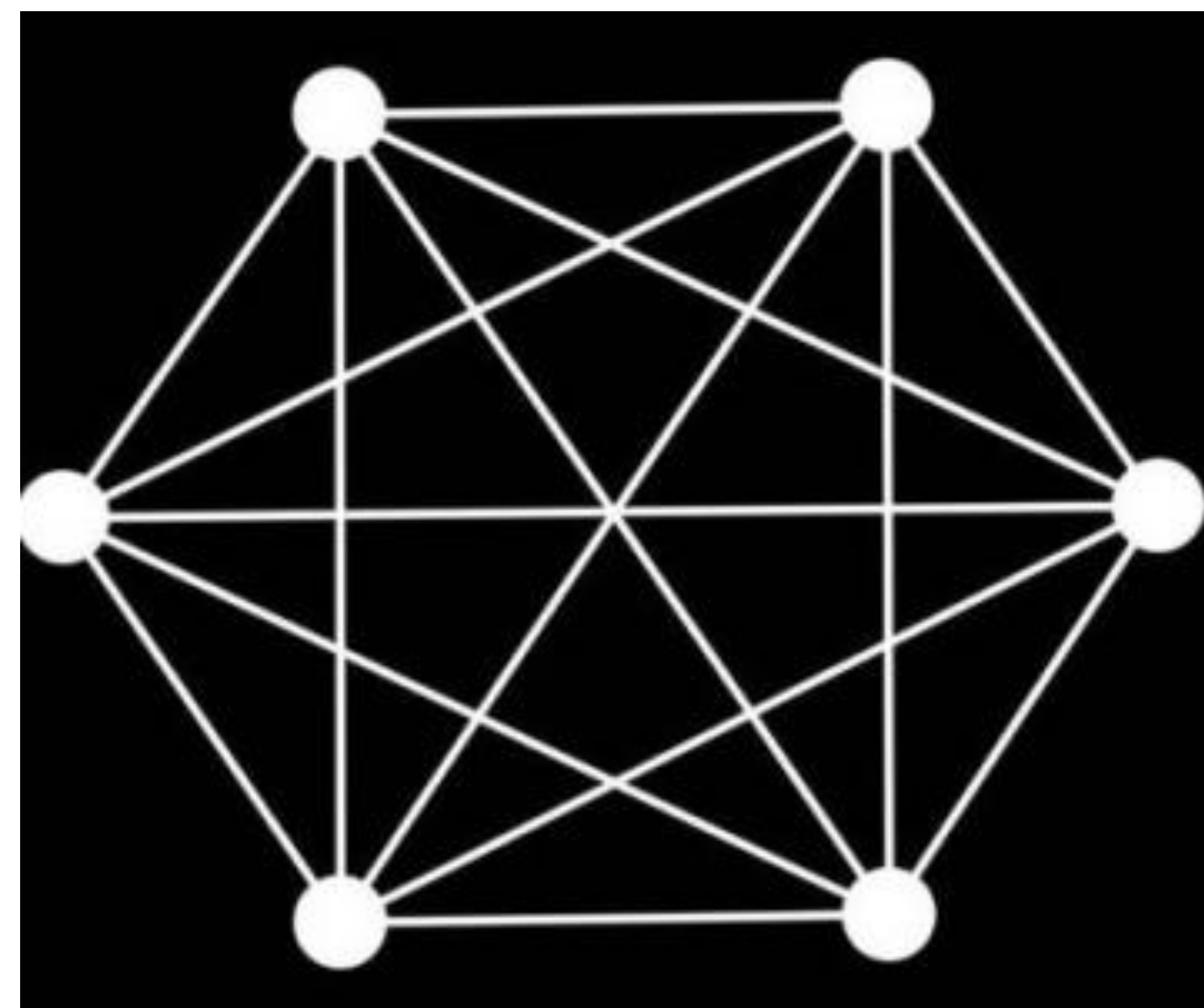
# BulkQueue不平衡

## 缺点

网状结构，一个节点故障，整个集群受影响

## 本质

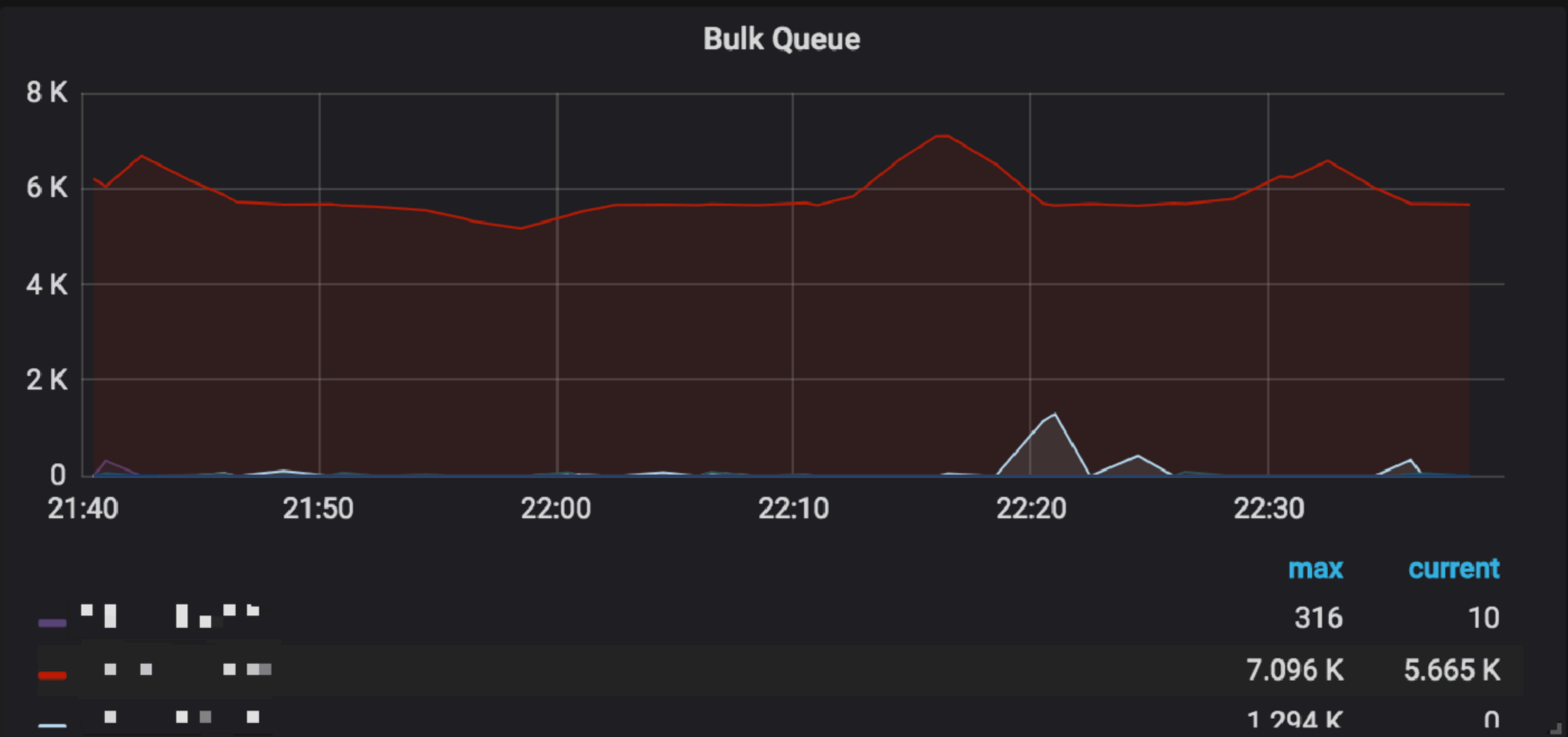
shard分配不平衡导致单个节点偏压





# BulkQueue不平衡

索引瓶颈







# OOM

## 原因

- 重查询，例如Cardinality
- 负载不均衡，bulk queue堆积

## 解法

- 查询优化
- 负载均衡
- 使用G1GC





# 坏盘

坏盘是常态！ ！ ！

节点状态最近变动记录 (176 alived / 176 total)

IP : PORT	消息
192.168.1.101	<div>✔ joined at 2019-03-29 15:44:14</div> <div>lost at 2019-03-27 17:22:12</div> <div>joined at 2019-03-27 17:04:10</div> <div>lost at 2019-03-27 16:22:07</div> <div>joined at 2019-03-27 16:02:17</div> <div>lost at 2019-03-27 16:00:13</div> <div>joined at 2019-03-27 15:58:07</div> <div>lost at 2019-03-27 15:36:11</div>
192.168.1.103	<div>✔ joined at 2019-03-27 19:56:14</div> <div>lost at 2019-03-27 18:54:11</div>
192.168.1.102	<div>✔ joined at 2019-03-27 19:56:13</div> <div>lost at 2019-03-27 18:54:11</div>
192.168.1.300	<div>✔ joined at 2019-03-27 19:56:12</div> <div>lost at 2019-03-27 18:54:11</div>





# 找不到Master

在5.4.3版本上频繁出现，一个节点挂掉整个集群崩溃：找不到Master

本质是节点状态不一致以后shard failed 把master的task queue堵死,详见

<https://github.com/elastic/elasticsearch/issues/27194>



# ES的瓶颈

## 场景

写入速度：百万级

延迟：分钟级

查询：明细&聚合

## 瓶颈

写入速度：单节点1W

存储空间：接近100T

写入延迟：非常高

查询和写入互相影响

## ClickHouse

写入速度：单节点10W+

存储空间：ES的1/5~1/10

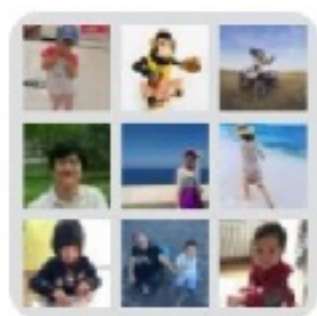
写入延迟：无

查询稳定性：优于ES，缺点是明细查询不如ES





# 线上交流



字节跳动大数据技术交流群





**THANKS.**

