

基于 Apache Doris 构建 10 倍性价比的日志分析方案

肖康

飞轮科技 技术副总裁

Apache Doris Committer

目录

1. 日志存储分析场景需求
2. 基于 ES 的日志平台痛点
3. 基于 Doris 的新一代日志分析平台
4. 实践案例

1 日志存储分析场景需求

日志存储分析的典型应用场景



可观测性

保障服务稳定 提升用户体验



网络安全

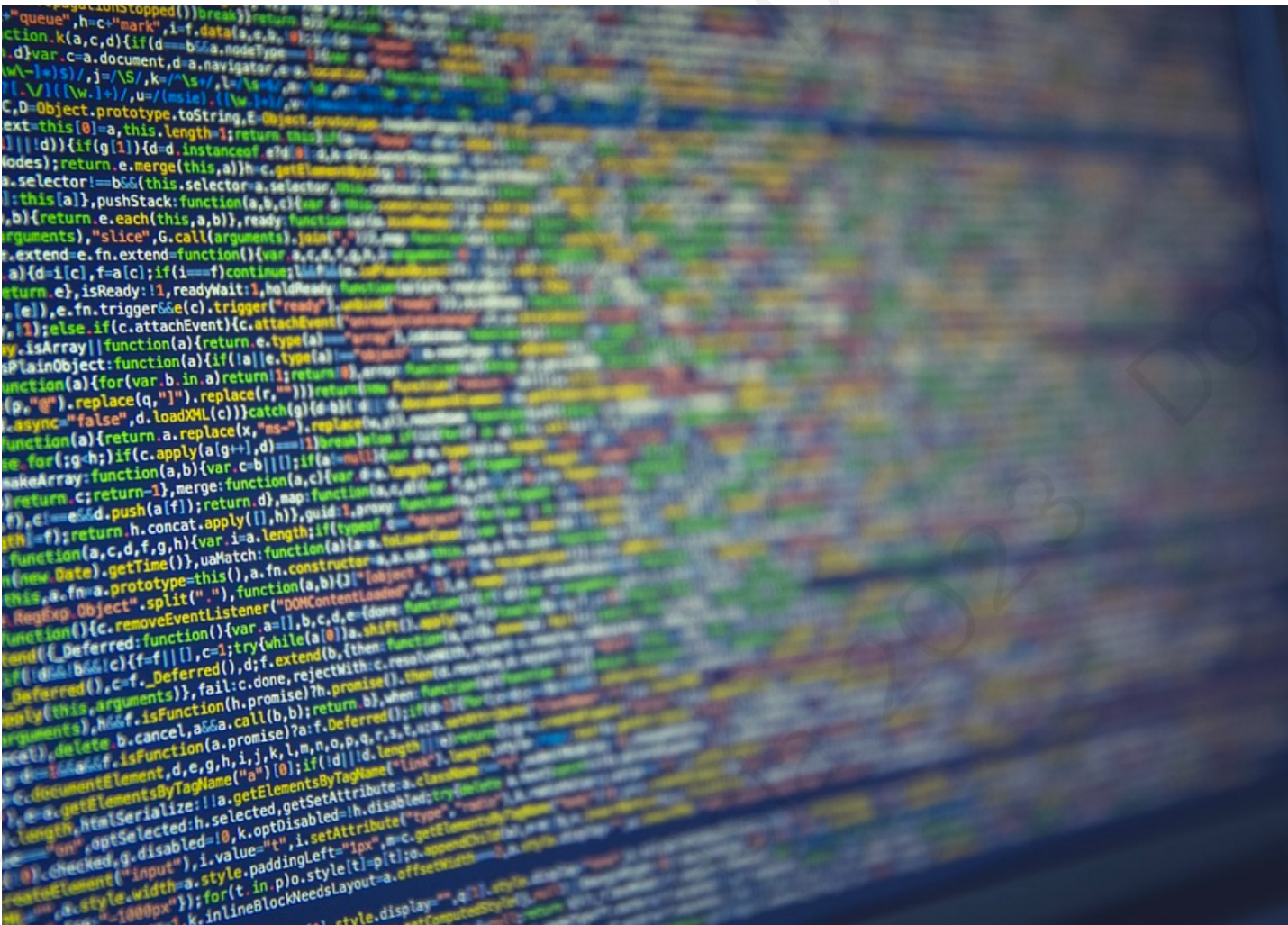
降低安全风险 提升系统安全性



业务分析

支持业务分析 加速业务增长

日志存储分析的3V



Variety - Schema Free

数据类型多样，Text和JSON
Schema Evolution



Volume - 数据量大

存储规模大、存储周期长
对存储成本敏感

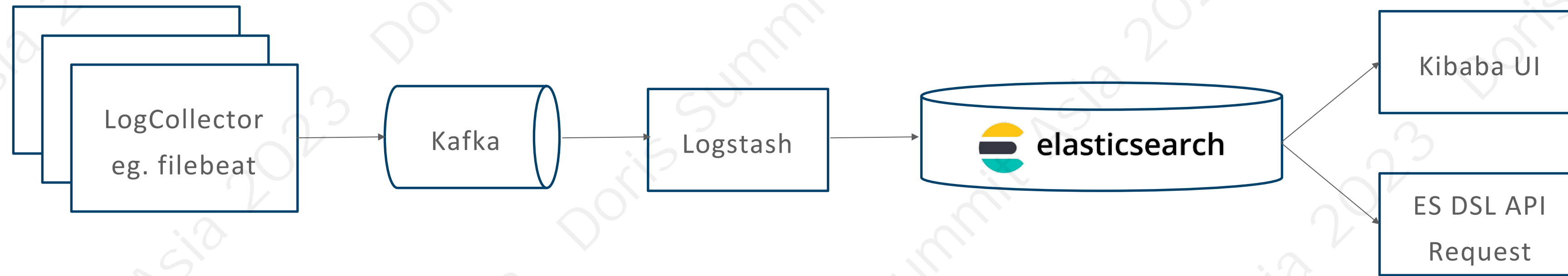


Velocity - 实时写入与检索

海量数据实时写入、低延迟可见
实时交互式分析

2 基于 ES 的日志系统痛点

基于 ES 的典型日志系统架构



每日增量：TB级

数据总量：PB级

查询并发：数十QPS

挑战1 – Schema Free 支持有限

字段类型 固定不变

- 字段类型冲突不允许写入
- 字段类型不能更改 => reindex重写数据

索引 固定不变

- 已有字段的索引不能增加或删除 => 全建索引
- 已有字段的索引不能调整分词等参数

```
{
  "mappings": {
    "properties": {
      "@timestamp": {
        "format": "strict_date_optional_time||epoch_second",
        "type": "date"
      },
      "message": {
        "type": "keyword",
        "index": false,
        "doc_values": false
      },
      "clientip": {
        "type": "ip"
      },
      "request": {
        "type": "match_only_text"
      },
      "status": {
        "type": "integer"
      },
      "size": {
        "type": "integer"
      }
    }
  }
}
```


挑战2 – 分析能力弱

Query DSL 学习门槛高	<ul style="list-style-type: none">DSL (Domain Specific Language) 面向搜索场景设计不符合使用习惯，写查询经常需要查手册
DSL功能单一 不支持Join	<ul style="list-style-type: none">只支持简单的单表分析不支持多表 Join、子查询、视图等复杂分析
DSL生态封闭	<ul style="list-style-type: none">ES生态自成体系，与BI类系统或数据生态工具打通较为困难

```
{
  "size": 0,
  "query": {
    "bool": {
      "must": [
        {
          "range": {
            "timestamp": {
              "gte": "1998-05-01T00:00:00Z",
              "lt": "1998-05-02T00:00:00Z"
            }
          }
        },
        {
          "match": {
            "message": "error"
          }
        }
      ]
    }
  },
  "aggs": {
    "by_hour": {
      "date_histogram": {
        "field": "timestamp",
        "calendar_interval": "hour"
      }
    }
  }
}
```

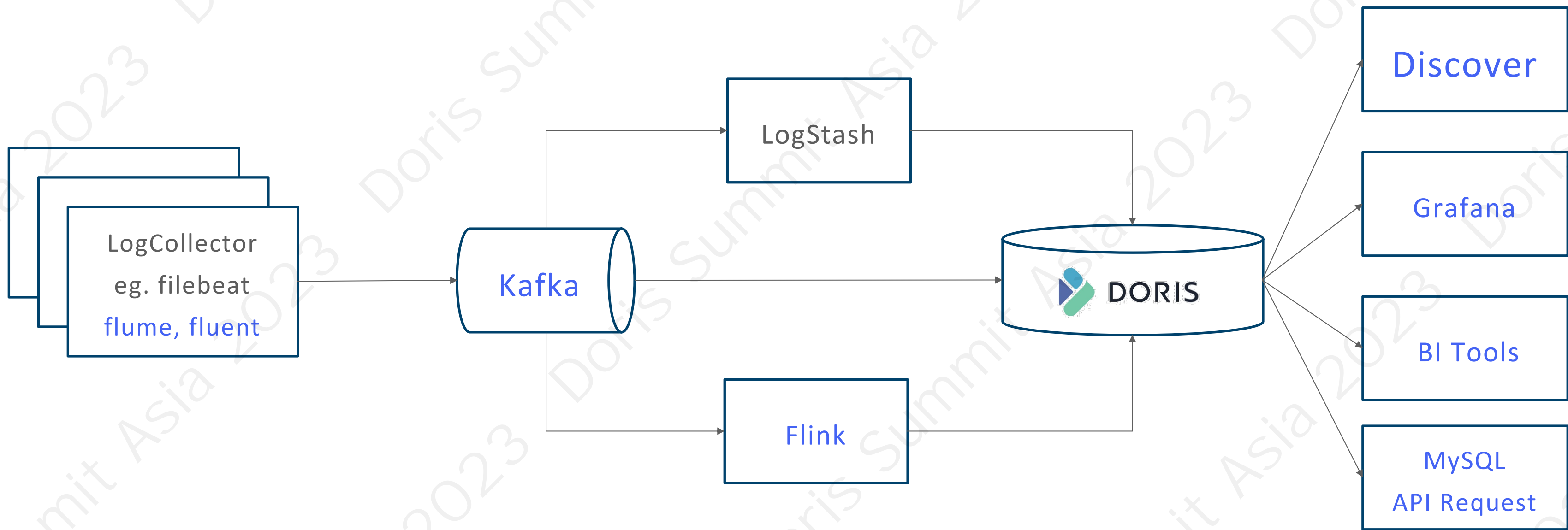
挑战3 – 性价比低

写入性能低	<ul style="list-style-type: none">• 数据写入需要构建索引、消耗大量CPU资源、写入效率低下• 业务高峰期容易触发reject，写入延迟升高
存储成本高	<ul style="list-style-type: none">• 正排、倒排、列存等多份数据存储，高度冗余• 整体数据压缩比约1:1.5，远低于常见的1:5
大查询不稳定	<ul style="list-style-type: none">• 写入高峰时易导致集群不稳定• 大查询易触发JVM OOM，影响整个集群写入和查询



3 基于Doris的新一代日志分析平台

基于 Apache Doris 的新一代日志系统架构



更多日志接入方式

统一存储，消除数据孤岛

开放生态，更强分析能力

优势1 – 原生的半结构化数据支持

<p>丰富的数据类型</p>	<ul style="list-style-type: none">• Text, JSON, Array, Map• Variant, 允许一个字段多种类型	<div><div><pre>{ "id": 134567, "name": "name1" }</pre></div><div>➔</div><div><pre>{ "id": "vip_48679", "name": "name2" }</pre></div></div>
<p>Schema Evolution</p>	<ul style="list-style-type: none">• 在线毫秒级增减字段• 在线按需增减索引，增量构建索引• 在线按需更改类型	<pre>ALTER TABLE t ADD COLUMN c; ALTER TABLE t ADD INDEX idx_a(a) USING INVERTED; BUILD INDEX idx_a ON t PARTITION(p20230808);</pre>

优势2 – 基于SQL的分析引擎

简单易用

- 支持标准SQL，无额外学习成本
- SQL语法与MySQL高度兼容

丰富的数据生态

- MySQL协议兼容，可直接使用MySQL CLI
- 无缝对接各类BI工具以及大数据生态组件

强大的分析能力

- 支持检索、聚合、多表JOIN、子查询、窗口函数、UDF、视图/物化视图等功能

H

查询

数据

集成

权限

数据

已保存查询

查询记录

Q 搜索

▼ internal

caol_test

cdc_test

dataworks_test

db1

demo

kzw_poc_test

lh_test

qualitydb

test

test_lyy

tpch

wd_test

wytpch

information_schema

jdbc

Q1(1)

2023-06-28 11:07 *

2023-06-28 11:07(1) *

2023-06-28 11:07(2) *

+

运行

internal.tp...

c1

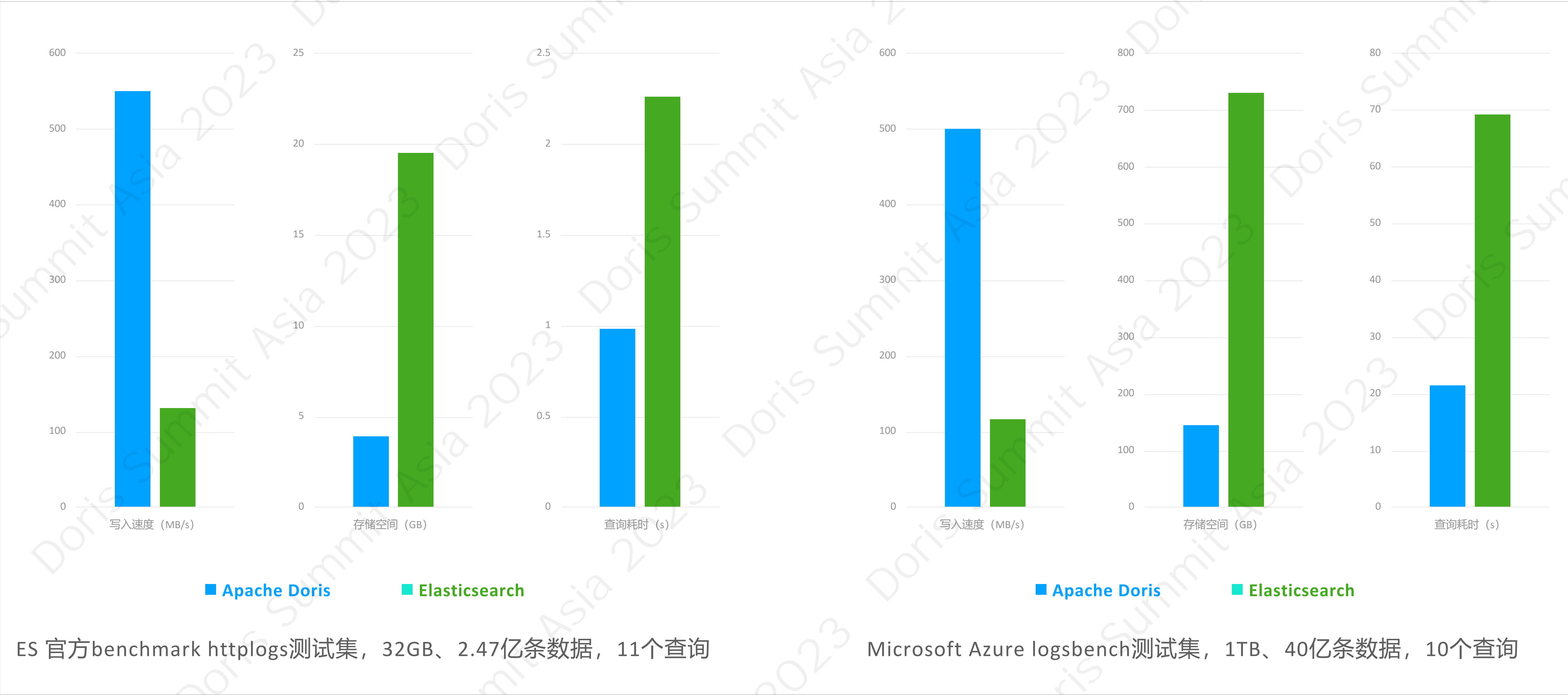
```
1 select
2   l_returnflag,
3   l_linestatus,
4   sum(l_quantity) as sum_qty,
5   sum(l_extendedprice) as sum_base_price,
6   sum(l_extendedprice * (1 - l_discount)) as sum_disc_price,
7   sum(l_extendedprice * (1 - l_discount) * (1 + l_tax)) as sum_charge,
8   avg(l_quantity) as avg_qty,
9   avg(l_extendedprice) as avg_price,
10  avg(l_discount) as avg_disc,
11  count(*) as count order
```

查询结果

l_returnflag	l_linestatus	sum_qty	sum_base_price	sum_disc_price	sum_charge	avg_qty
A	F	37734107	56586554400.73	53758257134.87	55909065222.82769	25.522
N	F	991417	1487504710.38	1413082168.0541	1469649223.194375	25.5164
N	O	74476040	111701729697.74	106118230307.6056	110367043872.49701	25.5022
R	F	37719753	56568041380.9	53741292684.604	55889619119.83193	25.5057

优势3 – 超高性价比

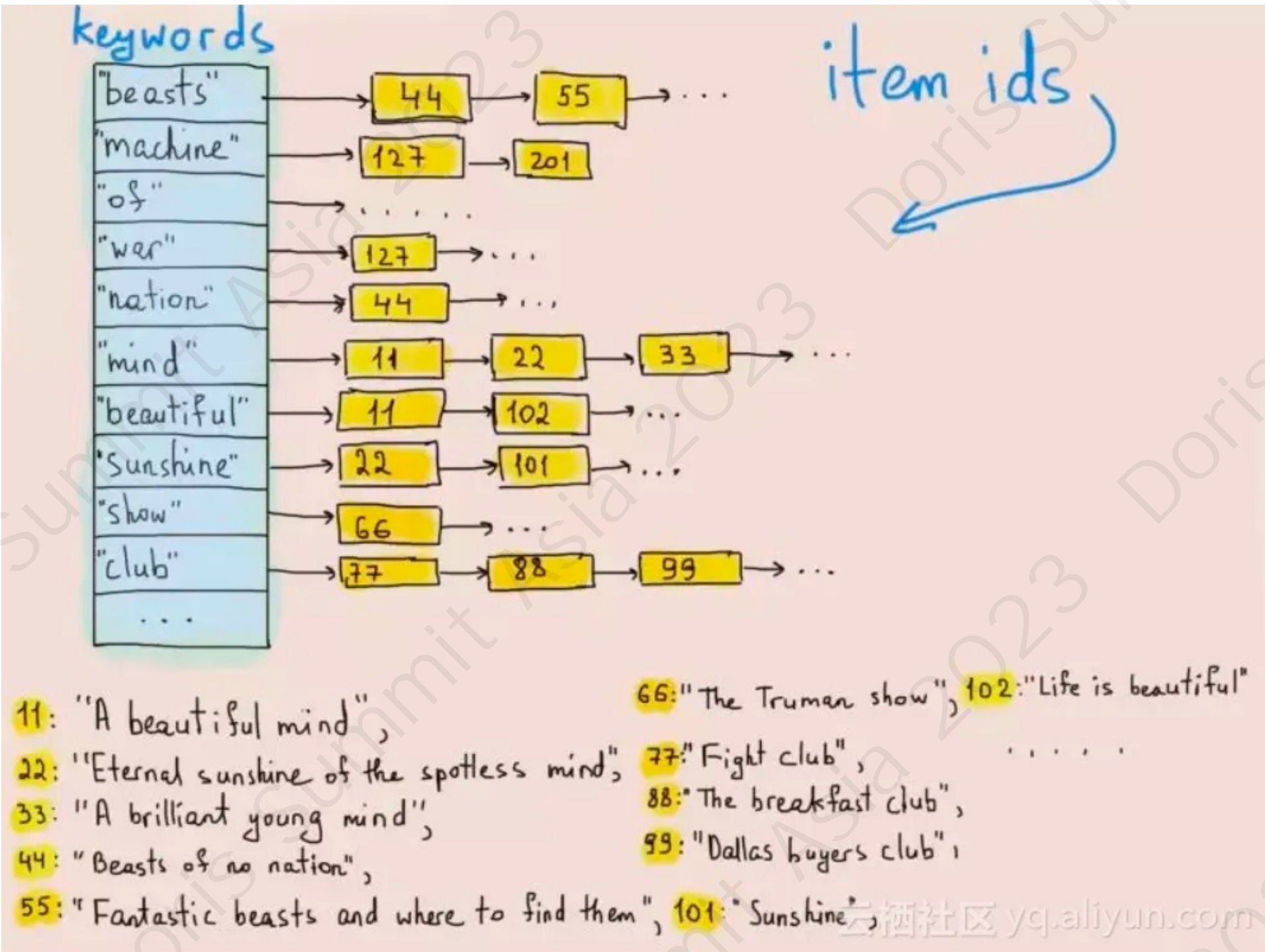
相对于ES **3 ~ 5倍** 写入吞吐提升, **80%** 存储空间降低, **2 ~ 3倍** 查询性能提升



优势3 – 超高性价比

	Elasticsearch	Apache Doris	Apache Doris 冷热分层
日增数据 (TB)	100	100	100
热数据天数	3	7	7
冷数据天数	27	23	23
数据压缩比	1.5	7.5	7.5
热数据存储空间 (TB)	200	40	40
冷数据存储空间 (TB)	1800	360	360
服务器配置	16C 64G 26.3TB	16C 64G 26.3TB	16C 64G 6.1TB
服务器数量	95	19	19
计算资源成本 (万元/月)	23.1	4.6	4.6
云盘存储成本 (万元/月)	71.7	14.3	1.4
对象存储成本 (万元/月)	0	0	3.8
云资源总成本 (万元/月)	94.8	18.9	9.8
综合性价比	1	5倍	9.7倍

关键技术 – 倒排索引



```
CREATE TABLE httplog
(
  `ts` DATETIME,
  `clientip` VARCHAR(20),
  `request` TEXT,
  INDEX idx_clientip (`clientip`) USING INVERTED,
  INDEX idx_request (`request`) USING INVERTED PROPERTIES("parser" = "unicode")
)
DUPLICATE KEY(`ts`)
...

-- 查看最新的10条数据
SELECT * FROM httplog ORDER BY ts DESC LIMIT 10;
-- 查询clientip为'8.8.8.8'的最新10条数据
SELECT * FROM httplog WHERE clientip = '8.8.8.8' ORDER BY ts DESC LIMIT 10;
-- 检索request字段中有error或者404的最新10条数据
SELECT * FROM httplog WHERE request MATCH_ANY 'error 404' ORDER BY ts DESC LIMIT 10;
-- 检索request字段中有image和faq的最新10条数据
SELECT * FROM httplog WHERE request MATCH_ALL 'image faq' ORDER BY ts DESC LIMIT 10;
```

关键技术 – 日志检索查询优化

```
SELECT * FROM log
WHERE ts >= t1 AND ts <= t2 AND message MATCH 'error'
ORDER BY ts DESC LIMIT 100
```

挑战 从海量日志中全文检索关键词



基于分区、主键的时间范围快速跳过
基于倒排索引的全文检索精准定位

挑战 按时间排序取满足条件的最新N条日志

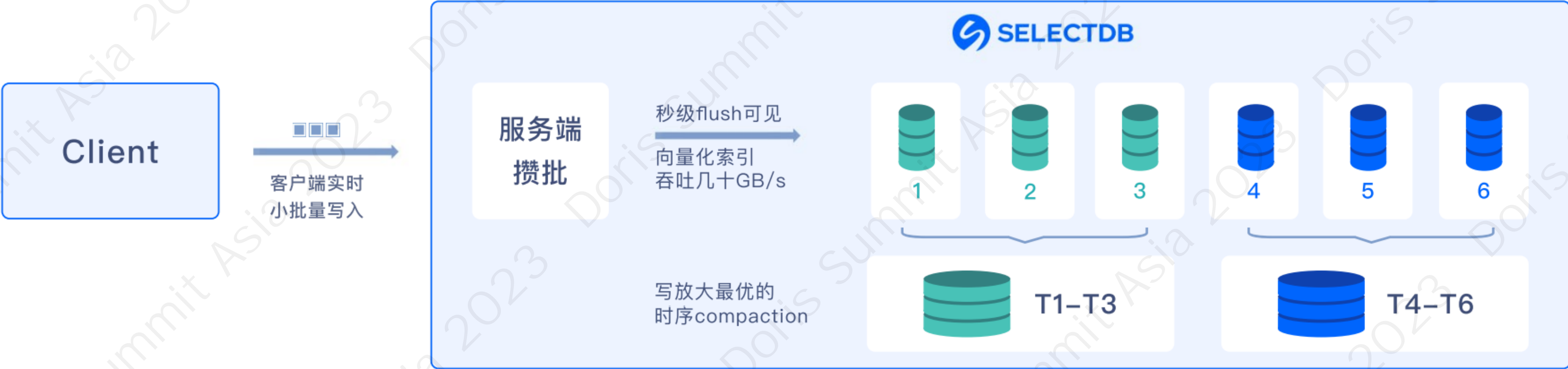


按时间排序的时序存储模型
基于动态剪枝的TopN查询算法

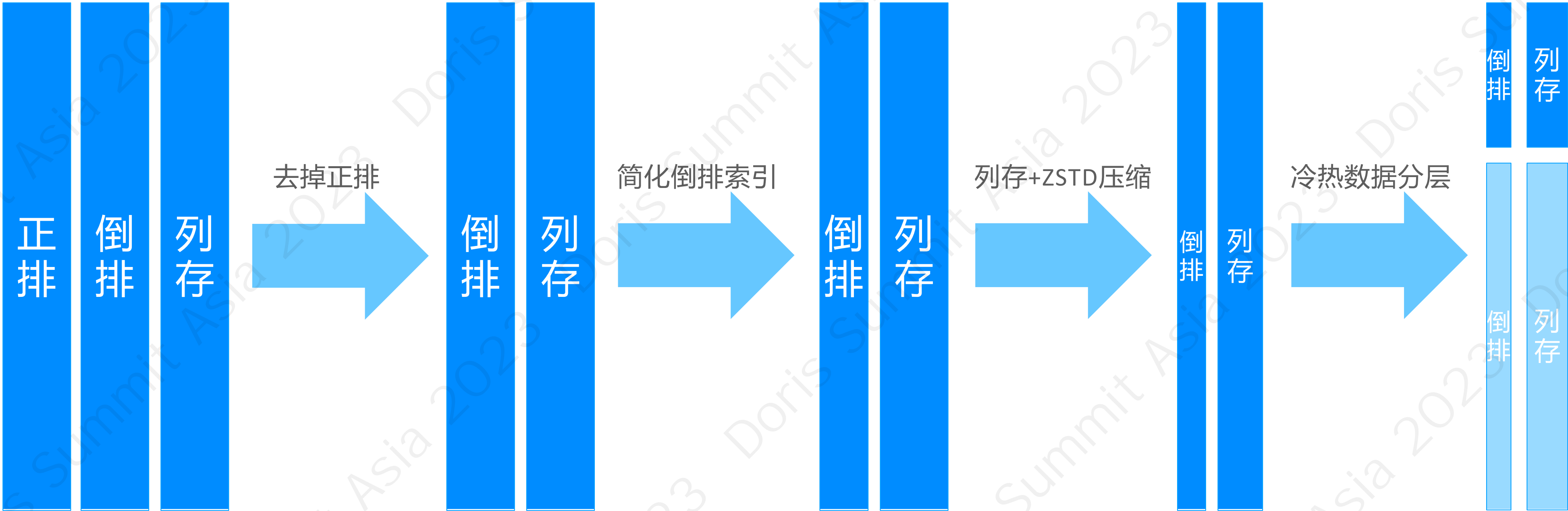


效果： **百亿**日志检索**秒级**响应

关键技术 - 导入性能优化



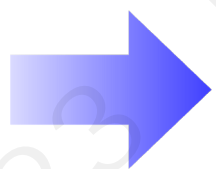
关键技术 – 存储成本优化



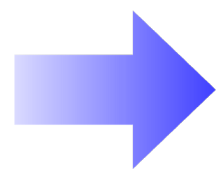
4 实践案例

实践案例1 – 网络安全

“Doris只用原来 **1/5** 的服务器，承载了 **1GB/s** 的写入流量，安全分析查询响应速度更快”



DORIS



消息系统数据导入

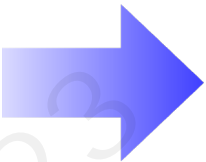
统一日志存储分析平台

安全数据分析

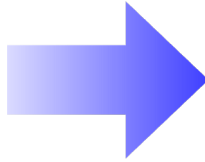
集群规模：10台物理机
数据增量：每天新增150亿条日志、8.3TB，Doris压缩后1.4TB（包括倒排索引，压缩率5.9）
数据总量：3副本保存60天，总共252TB、9千亿条
写入性能：线上平均20w/s、100MB/s，峰值100w/s、500MB/s，压测3台机器200w/s、1GB/s

实践案例2 – 通信制造

“Doris全文检索能满足日志检索分析的需求，日志存储空间下降到ES的 **1/6**，系统成本大幅降低”



DORIS



Logstash日志采集处理

集群规模：20台物理机

数据增量：每天新增1000亿条日志、50TB，Doris压缩后7TB（包括倒排索引，压缩率7.1）

数据总量：2副本保存90天，总共1.26PB、9万亿条

写入性能：线上平均150w/s、500MB/s，峰值600w/s，2GB/s

统一日志存储分析平台

日志检索下载

实践案例3 – 可观测性

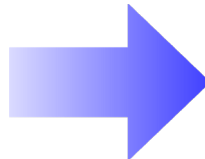
“Doris提供了灵活的半结构化数据类型variant，成本相比云上ES节省 **70%**，查询性能提升**2-3倍**”



可观测性数据采集器



DORIS



可观测性可视化分析

Log Trace 统一存储平台

- 集群规模：10台虚拟机
- 数据增量：每天新增400亿条数据、40TB，Doris压缩后7TB（包括倒排索引，压缩率5.7）
- 数据总量：1副本保存30天，总共150TB、1.2万亿条
- 写入性能：线上平均40w/s、400MB/s，峰值100w/s，1GB/s，秒级实时写入
- 查询并发：线上百QPS，p99延迟230ms

可视化日志检索





获取更多社区动态与最佳实践

Apache Doris 官方平台:

- Apache Doris 官网: doris.apache.org
- Apache Doris GitHub: github.com/apache/doris/

获取更多峰会资料:

- Doris Summit 峰会官网: doris-summit.org.cn
- Doris Summit 峰会回放: <https://space.bilibili.com/1196172099/channel/collectiondetail?sid=1824324>