elastic | 中国开发者大会

Elastic Stack在APM与AIOps领域的深度应用实践

高驰涛
云智慧

战略级赞助商 HUAWEI | 钻石级赞助商 普翔 | 白金级赞助商 华夏博格 神州数码 Digital China | 金牌级赞助商 iDataAPI

合作伙伴 开源中国 oschina.net 掘金 谱时 IT大咖说 otpub Broadview 百格活动 bagevent.com MAXHUB

Elastic Stack在APM 与 AIOps领域的深度应用实践

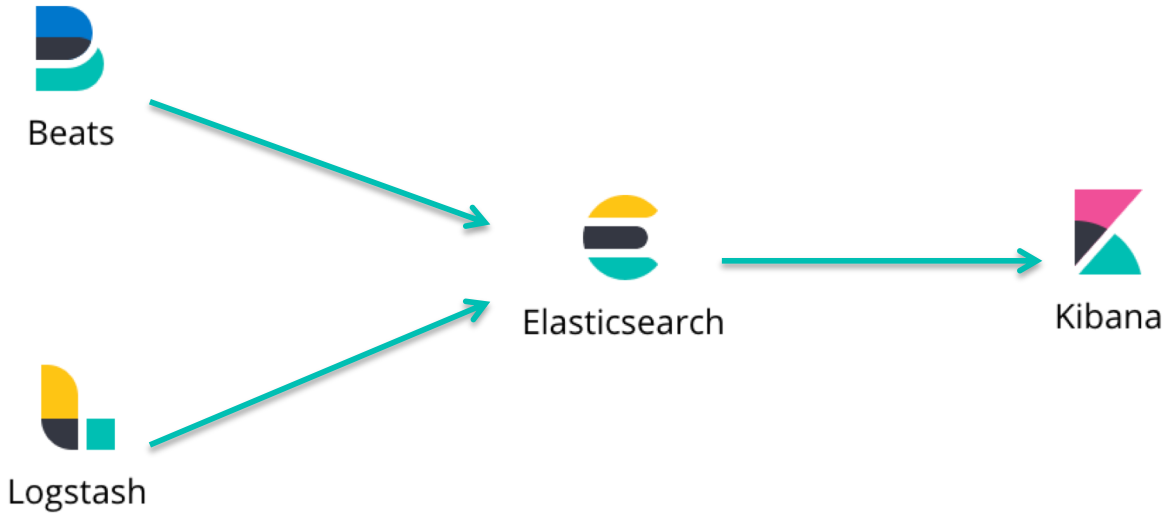
高驰涛（云智慧研发总监）

Nov. 10, 2018

elastic

- Elastic Stack & 可能的技术选型
- [日志]大数据架构演化
- 落地项目实践
- 改造建议和生产配置建议

Elastic Stack 全家桶



elastic

可能的技术选型

数据收集

Logstash

Beats

ETL

Logstash

Kafka-connect-ES

ES-river-Kafka

数据可视化

Kibana

CBoard

存储

Elasticsearch

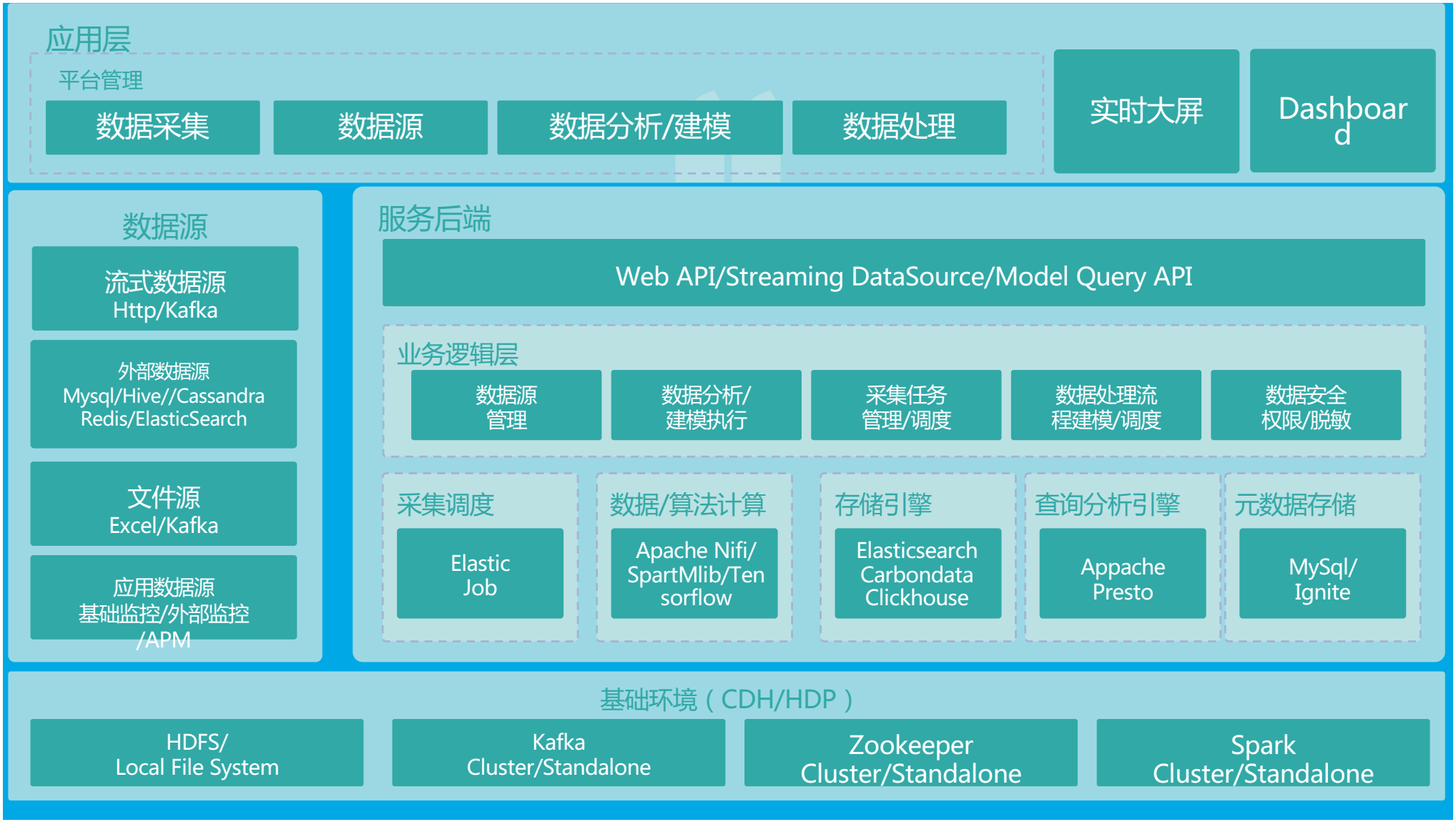
分析

X-pack

elastic

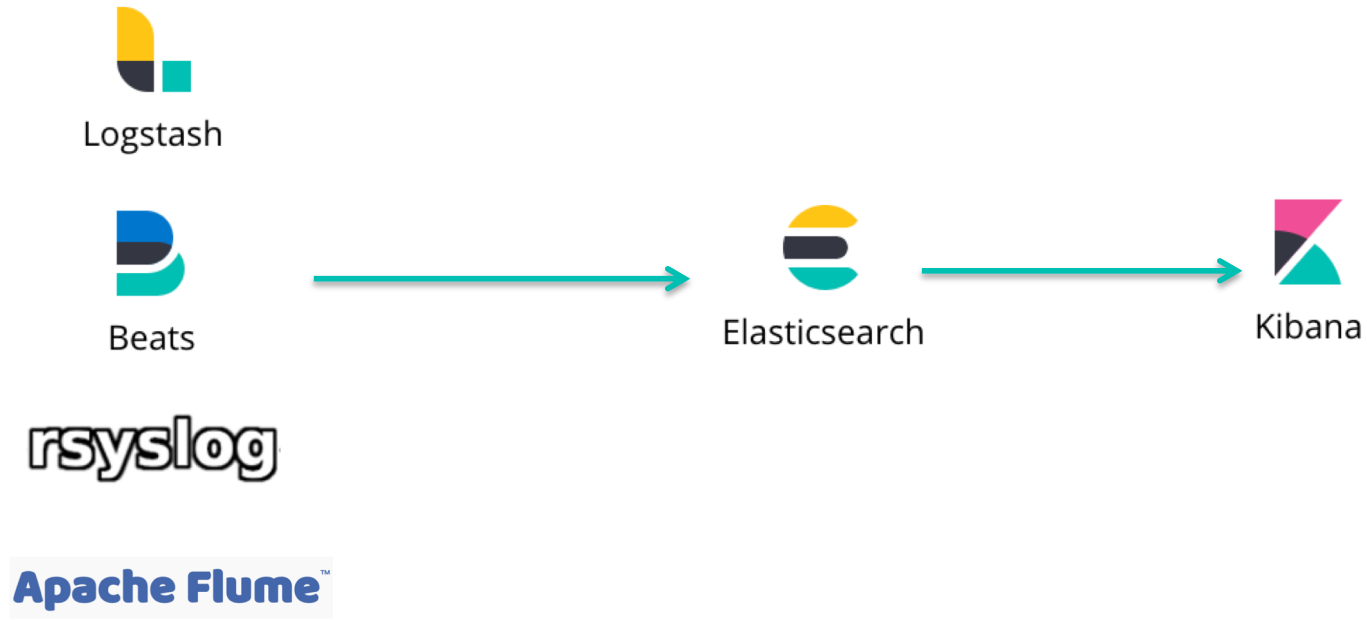
elastic

- Elastic Stack & 可能的技术选型
- [日志]大数据架构演化
- 落地项目实践
- 改造建议和生产配置建议


应用层
平台管理
数据采集
数据源
数据分析/建模
数据处理
实时大屏
Dashboard
数据源
流式数据源
Http/Kafka
外部数据源
Mysql/Hive//Cassandra
Redis/ElasticSearch
文件源
Excel/Kafka
应用数据源
基础监控/外部监控
/APM
服务后端
Web API/Streaming DataSource/Model Query API
业务逻辑层
数据源
管理
数据分析/
建模执行
采集任务
管理/调度
数据处理流
程建模/调度
数据安全
权限/脱敏
采集调度
Elastic
Job
数据/算法计算
Apache Nifi/
SpartMlib/Ten
sorflow
存储引擎
Elasticsearch
Carbondata
Clickhouse
查询分析引擎
Appache
Presto
元数据存储
MySql/
Ignite
基础环境（CDH/HDP）
HDFS/
Local File System
Kafka
Cluster/Standalone
Zookeeper
Cluster/Standalone
Spark
Cluster/Standalone

小规模应用

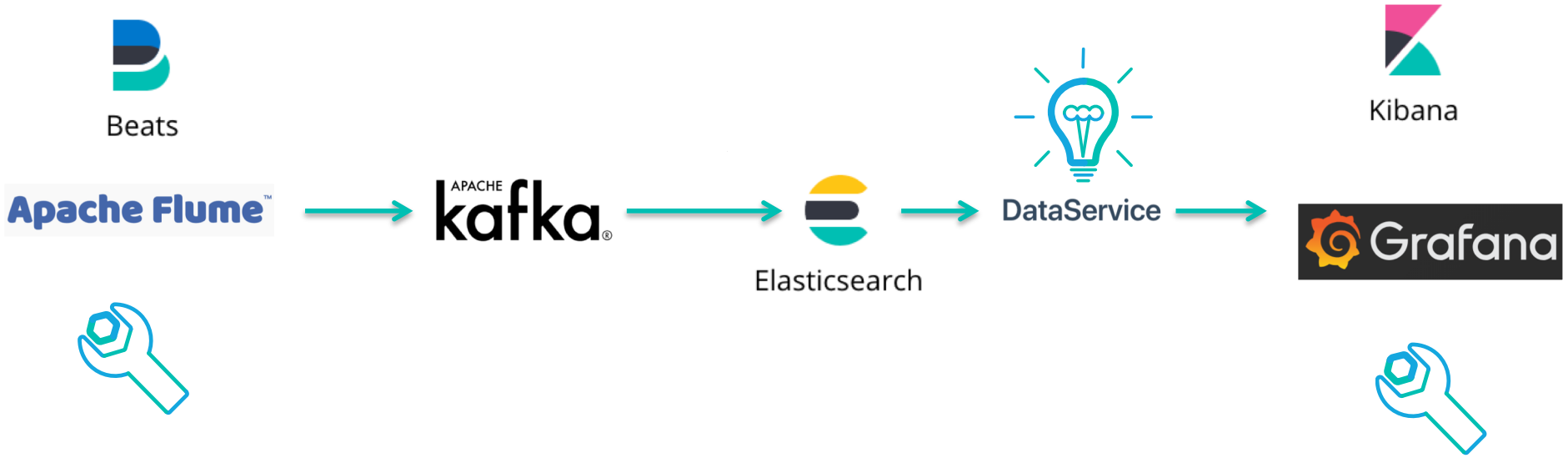
(10G – 100G/天，数据7天在线)



elastic

中等规模应用

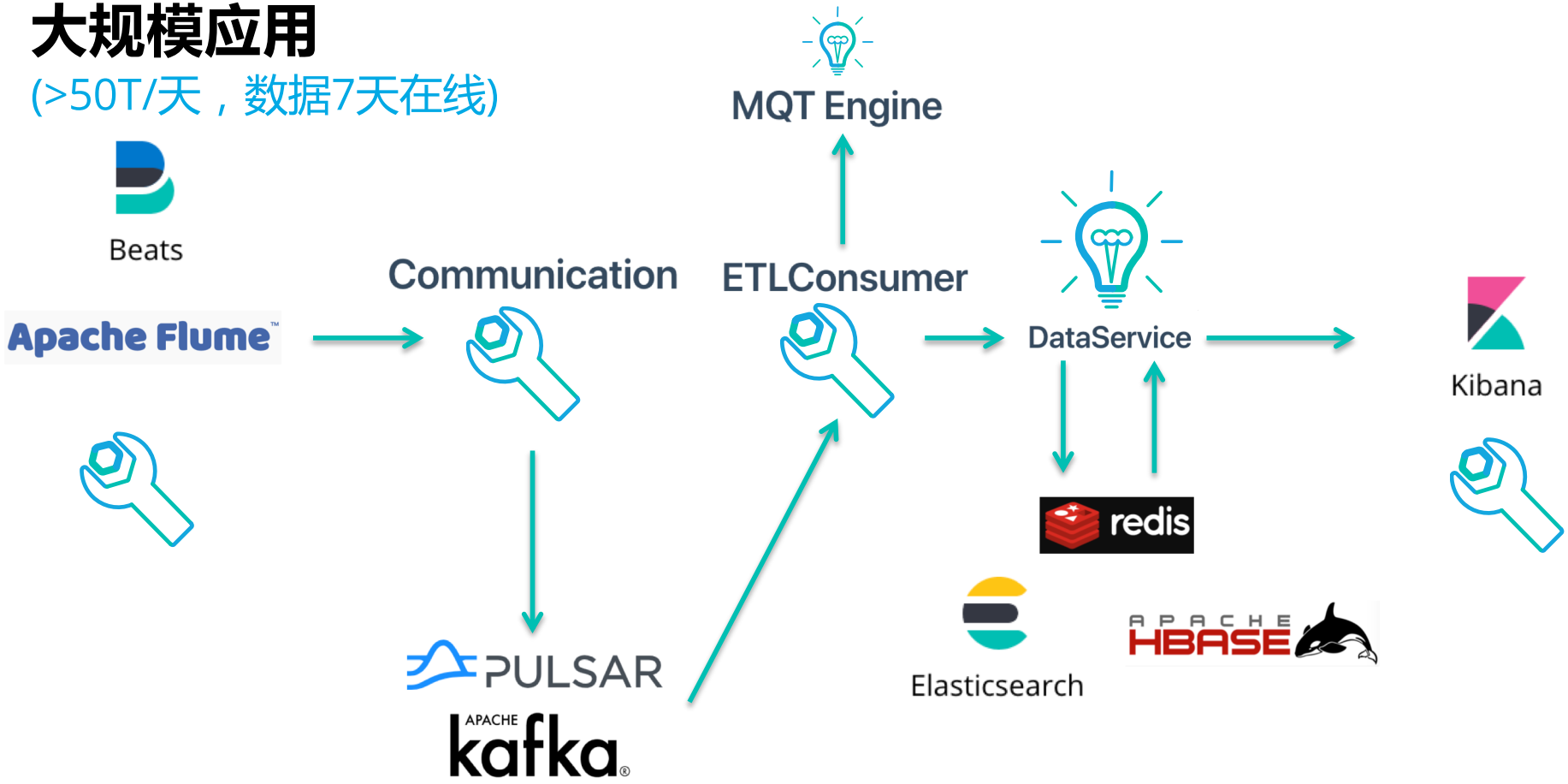
(1T – 10T/天，数据7天在线)



elastic

大规模应用

(>50T/天，数据7天在线)

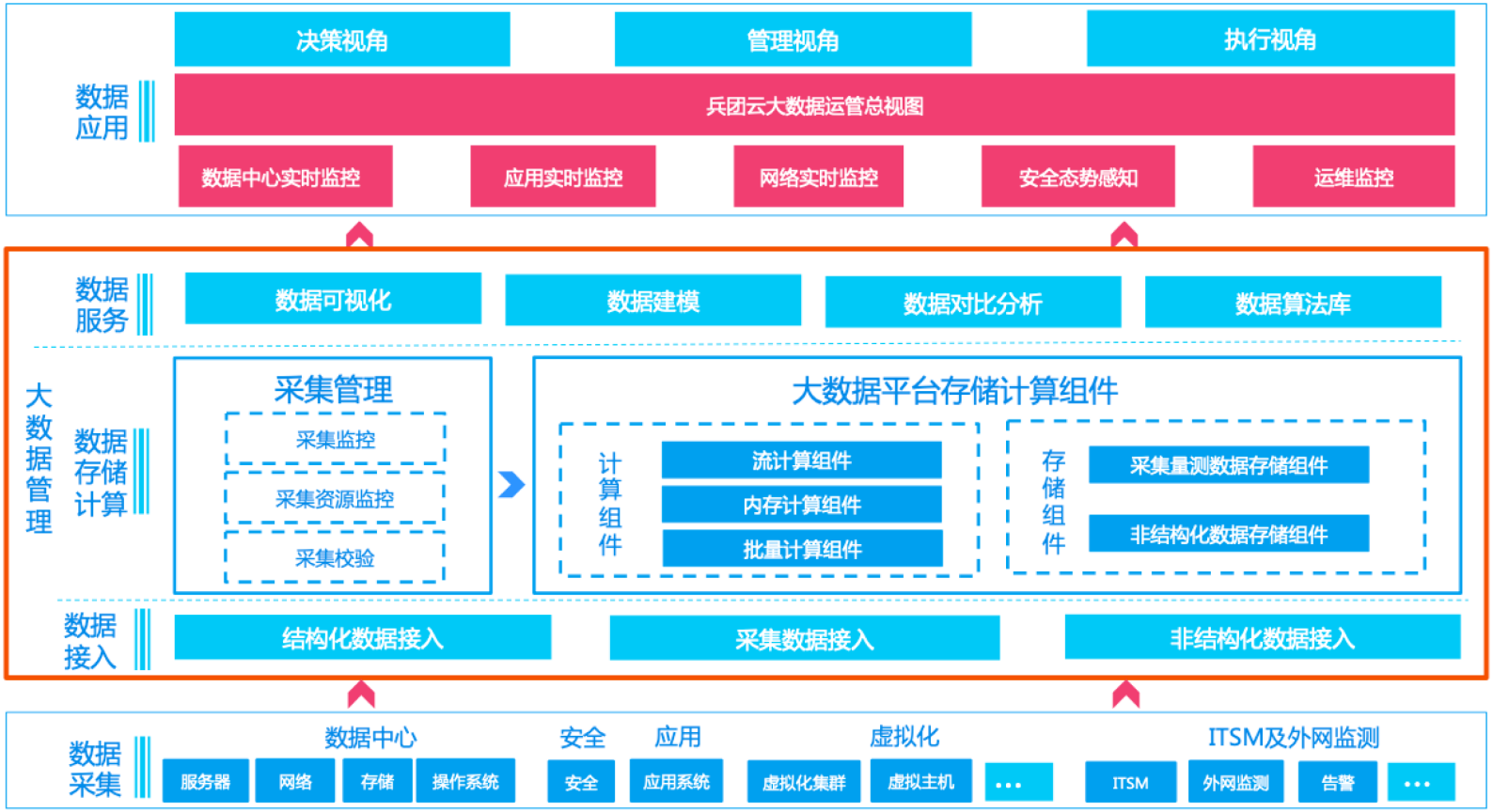


elastic

elastic

- Elastic Stack & 可能的技术选型
- [日志]大数据架构演化
- 落地项目实践
- 改造建议和生产配置建议

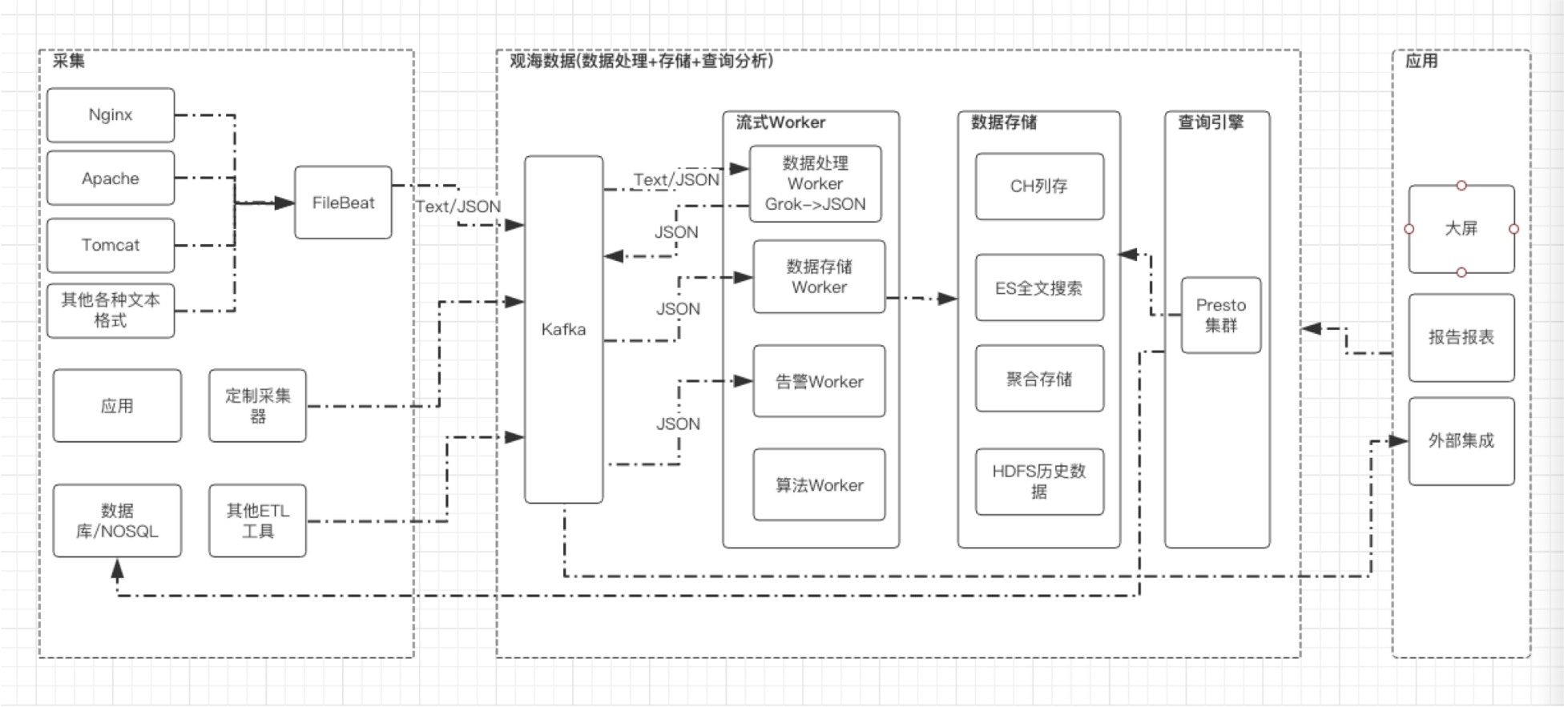
西北某兵团



elastic

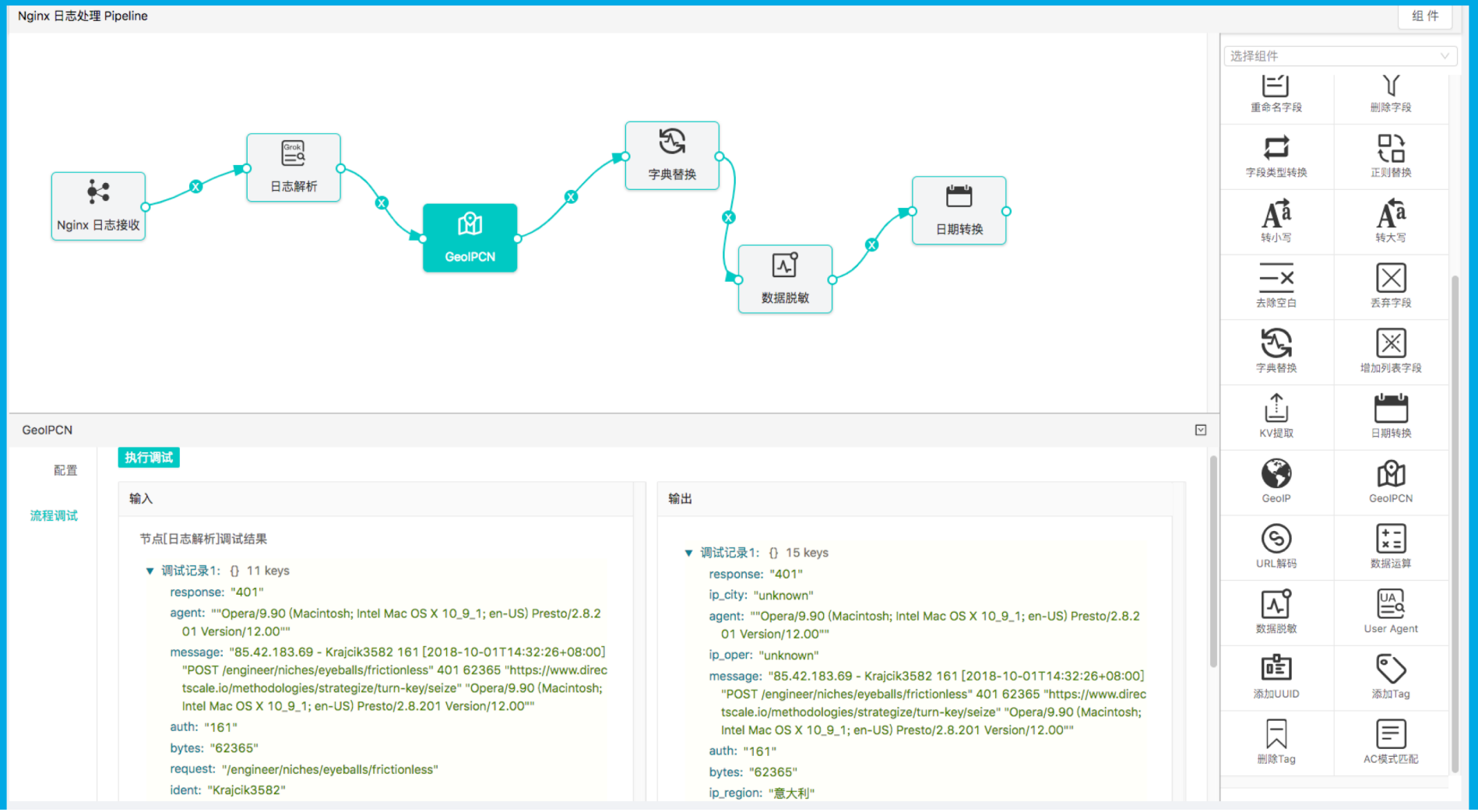
[redacted]大数据运管平台总视图
2017 - 06 - 12 17:40:59
部门带宽占比
财务局 发改委 国土局 教育局 十二师 水利局
13.25%
15.13%
21.88%
13.5%
16.75%
19.5%
部门专网网络流量
(Mbps)
使用 未使用
150
120
90
60
30
0
财务局 发改委 国土局 教育局 十二师 水利局
各机构资源分配情况
cpu mem disk
(C/G)
(G)
100
80
60
40
20
0
6,000
5,000
4,000
3,000
2,000
1,000
0
财务局 发改委 国土局 教育局 十二师 水利局
流量使用
业务应用
克达拉
[redacted]
舒克
昆玉
网络可用率
网络流量
告警数量
告警数量对比
(个)
今年 去年
18
15
12
9
6
3
0
1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月
网络设备统计(拓扑)
设备类别
设备名称
设备总数
网络设备
路由器 319
交换机 249
光纤交换机 0
安全设备
防火墙 7
入侵检测 0
安全网闸 12
存储设备
磁盘阵列 0
网络存储器 0
磁带库 0
计算机设备
服务器 59
客户机 0
虚拟机 827
健康度
部门专网
响应时间
可用率
优秀 人社专网 104ms 99.99%
优秀 国土专网 66ms 99.99%
优秀 司法专网 48ms 99.99%
优秀 卫生专网 51ms 99.99%
良好 统计专网 74ms 99.9%

观海数据平台



elastic

观海数据平台


Nginx 日志处理 Pipeline
组 件
选择组件
Nginx 日志接收
日志解析
GeoIPCN
字典替换
数据脱敏
日期转换
重命名字段
删除字段
字段类型转换
正则替换
转小写
转大写
去除空白
丢弃字段
字典替换
增加列表字段
KV提取
日期转换
GeoIP
GeoIPCN
URL解码
数据运算
数据脱敏
User Agent
添加UUID
添加Tag
删除Tag
AC模式匹配
GeoIPCN
配置
流程调试
执行调试
输入
节点[日志解析]调试结果
调试记录1: {} 11 keys
response: "401"
agent: ""Opera/9.90 (Macintosh; Intel Mac OS X 10_9_1; en-US) Presto/2.8.201 Version/12.00""
message: "85.42.183.69 - Krajcik3582 161 [2018-10-01T14:32:26+08:00] "POST /engineer/niches/eyeballs/frictionless" 401 62365 "https://www.directscale.io/methodologies/strategize/turn-key/seize" "Opera/9.90 (Macintosh; Intel Mac OS X 10_9_1; en-US) Presto/2.8.201 Version/12.00""
auth: "161"
bytes: "62365"
request: "/engineer/niches/eyeballs/frictionless"
ident: "Krajcik3582"
输出
调试记录1: {} 15 keys
response: "401"
ip_city: "unknown"
agent: ""Opera/9.90 (Macintosh; Intel Mac OS X 10_9_1; en-US) Presto/2.8.201 Version/12.00""
ip_oper: "unknown"
message: "85.42.183.69 - Krajcik3582 161 [2018-10-01T14:32:26+08:00] "POST /engineer/niches/eyeballs/frictionless" 401 62365 "https://www.directscale.io/methodologies/strategize/turn-key/seize" "Opera/9.90 (Macintosh; Intel Mac OS X 10_9_1; en-US) Presto/2.8.201 Version/12.00""
auth: "161"
bytes: "62365"
ip_region: "意大利"

观海数据平台
观海数据
首页 / 数据分析
请输入模型名称
搜索
全部
filebeat
概览
数据源
数据分析
+ 新建
FilebeatAgentMonitor
Authur 添加于2018-09-26 16:04:15
test0925_debug
添加于2018-09-25 14:05:47
test
添加于2018-09-21 18:43:24
test_oom
添加于2018-09-17 10:06:35
testoom0917
添加于2018-09-17 20:01:14
模型请求API
请求地址:
http://139.219.5.186/api/v1/dataquerymodels/ffcb500ea8b541e0bf17ec3c6
contentType:
application/json
访问令牌(Token):
b62afb390834448ba4a632282df6a2f5
请求样例(CURL方式):
curl --request POST \
--url http://139.219.5.186/api/v1/dataquerymodels/ffcb500ea8b541e0bf1
--header 'content-type:application/json' \
--header 'CWAccessToken:b62afb390834448ba4a632282df6a2f5' \
--data '{params:{}}'

观海数据平台

apache_log
无描述
过去 30 天
30秒
请求总数
15,897
返回码
200 206 304 404 302
请求方法
POST GET HEAD
请求IP分布
120.77.178.154
101.246.53.248
14.18.152.242
183.13.61.75
106.110.143.187
113.139.188.96
请求path
/Api/Index/getCatalogSonList
/Api/Index/getCatalogList
/Api/Index/getPhaseList
/Api/Index/getSubjectList
/Home/Index/geturl/keyinfo/A...
/Api/Vedio/getVideoUrl
世界地图
12693 – 15864
9520 – 12692
6347 – 9519
3174 – 6346
1 – 3173
请求随时间变化分布
15K
12K
9K
6K
3K
0
08:00:00 2018-07-15
20:00:00 2018-07-19
08:00:00 2018-07-24
20:00:00 2018-07-28
08:00:00 2018-08-02
20:00:00 2018-08-06
08:00:00 2018-08-11
时间
运营商分布
10K
8K
6K
4K
2K
0
电信
移动
联通
广电网
Isp
中国地图
9172 – 11413
6930 – 9171
4687 – 6929
2444 – 4686
201 – 2443
每分钟入口流量
昨天
10M
8M
6M
4M
2M
0
00:00:00 2018-08-14
02:30:00 2018-08-14
05:00:00 2018-08-14
07:30:00 2018-08-14
10:00:00 2018-08-14
12:30:00 2018-08-14
15:00:00 2018-08-14
17:30:00 2018-08-14
20:00:00 2018-08-14
22:30:00 2018-08-14
时间

北京电信IDC客户全国感知监控

XPCC
兵团电子政务大数据运管平台数据中心实时监控
2018-5-29 22:28:50

一体化智能业务运维监控大屏

富力集团安全态势感知

1.27 亿条
65.12 GB
最近24小时数据处理接入
总共9个
9 个流式
数据源
4 个
模型总数
1.27 亿条
112.51 GB
最近24小时数据处理输出
1.27 亿条
112.49 GB
近24小时流式数据源写入
1125 次
近24小时模型查询次数
最近一小时数据处理情况
1分钟
5分钟
处理流程:
All
250万条
200万条
150万条
100万条
50万条
0万条
3GB
2GB
10:29:47
10:33:47
10:37:47
10:41:47
10:45:47
10:49:47
10:53:47
10:57:47
11:1:47
输入记录数
输出记录数
错误记录数
254.21 亿条
21.96 TB
近24小时流式数据源写入
最近一小时流式数据源写入情况
数据源:
All
记录数
10:27:47
10:31:47
10:35:47
10:39:47
10:43:47
10:47:47
10:51:47
10:55:47
10:59:47
最近一小时流式数据源写入情况
1分钟
5分钟
记录数
字节数
2,100万条
1,800万条
1,500万条
1,200万条
900万条
600万条
300万条
0万条
18GB
15GB
12GB
9GB
6GB
3GB
0GB
19:16:12
19:22:12
19:28:12
19:34:12
19:40:12
19:46:12
19:52:12
19:58:12
20:4:12
20:10:12
20:16:12
记录数
字节数

elastic

- Elastic Stack & 可能的技术选型
- [日志]大数据架构演化
- 落地项目实践
- 改造建议和生产配置建议

ES的配置建议和搭配使用（8C64G, ES 6.2.2） - 系统调参

优化文件符

/etc/security/limits.conf
elastic soft nofile 65535
elastic hard nofile 65535
elastic soft nproc 65535
elastic hard nproc 65535
elastic soft memlock unlimited
elastic hard memlock unlimited
sysctl -w vm.max_map_count = 262144

禁用swap

sed -i '/swap/s/^/#/' /etc/fstab
swapoff -a

写入削峰

优化dirty脏内存页
/etc/sysctl.conf
sysctl -w vm.dirty_ratio=10
sysctl -w vm.dirty_background_ratio=5
sysctl -w vm.dirty_writeback_centisecs=200

优化系统回收inode cache权重

/etc/sysctl.conf
sysctl -w vm.vfs_cache_pressure=200
sysctl -w vm.dirty_expire_centisecs=6000

elastic

ES的配置建议和搭配使用（8C64G, ES 6.2.2） - 提高读写IO

path.data: /data/es622/data,/data1/es622/data[,...]

高效利用多块磁盘IO，提高查询和数据写入效率，使用多块磁盘均衡存取数据，可以获得N倍IO性能提升

- 补充修改为图文说明

ES的配置建议和搭配使用（8C64G, ES 6.2.2）

提高写入和查询效率

- thread_pool.search.size: 48
  - 建议为cpu核数的2-3倍，提高查询效率
- thread_pool.search.queue_size: 20000
- thread_pool.index.size: 9
  - 设为CPU核数 + 1
- thread_pool.index.queue_size: 40000

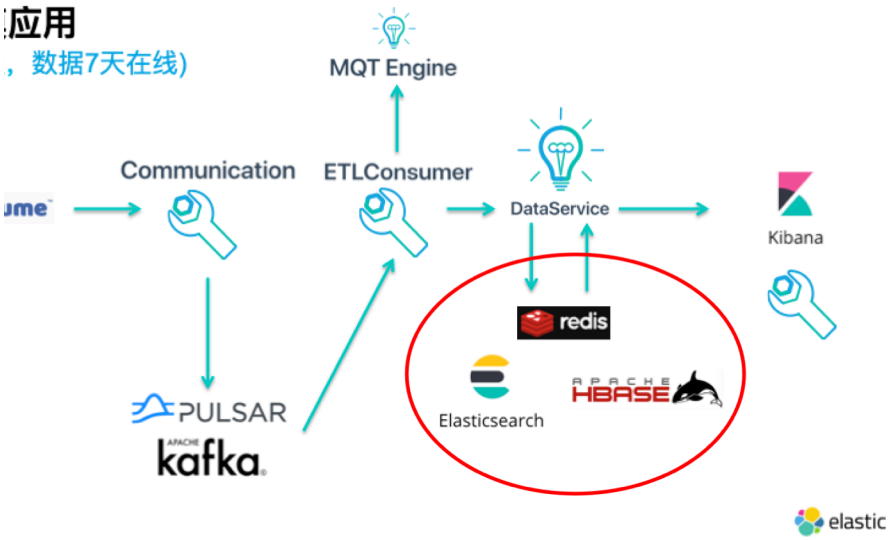
合并静态Segment	number_of_shards
通过_forcemerge api进行合并，减少segments个数提高查询效率 max_num_segments取值为 ： max_num_segments = (单个索引大小G / 分片数 / 2G) 示例： 1024G / 16 / 2G = 32	一个分片只能有效利用1核cpu number_of_shards取值为 ： number_of_shards = (单节点CPU核数 * 节点数量) / 2 示例： (8C * 32节点) / 2 = 128

- template模块设置
  - "codec": “best_compression” 启用压缩
  - "refresh_interval": “30s” 适当增大数据落盘刷新，提高写入效率，降低segment数量
  - “number_of_shards”: “8”
    - 提高查询效率，经验证，一个分片数只能有效利用1核cpu。增加分片数，提高cpu使用率和查询效率

elastic

ES的配置建议和搭配使用（8C64G, ES 6.2.2）

数据裁剪和数据字典



数据裁剪

对大文本进行裁剪
hash后，将hash key放入ES进行索引，
将原始文本以KV形式存入Hbase

elastic

日志类型大数据收集分析平台的改造建议

数据减少不必要的落盘次数
将Extract从ETL中拆离为独立服务
将Transform过程封装为Pipeline Plugin
使用Pipeline优化ETL流水处理

搞懂你的数据

AMA

elastic

elastic
中文社区

专业、垂直、纯粹的 Elastic 开源技术交流社区
https://elasticsearch.cn/

elastic