构建可观察性数据中台

周琦

阿里云计算资深专家

关于我与分享主题

阿里云

周琦（简志）

- 飞天初创研发之一，负责神农（监控/分析/诊断）平台
- 阿里云日志服务（SLS）负责人
  - 支撑阿里+蚂蚁经济体，作为日志/Metric/Trace基础设施
  - 服务阿里云上W级企业客户

数据量：20PB/Day

接入亿级终端　　**查询分析：>1亿/Day**

阿里云访问量最大产品之一

阿里经济体Trace/Log/Metric基础平台

《构建可观察性数据中台》

- 历史背景
- 中台思考与设计
- 案例分享
- 总结

从过去看未来：工程师生涯5年变化

阿里云

技术研发岗	安心写代码
测试部门变化	为质量和可用性负责
承担部分SRE职责	吃自己的狗粮
商业化/影响力	为自己、产品代言

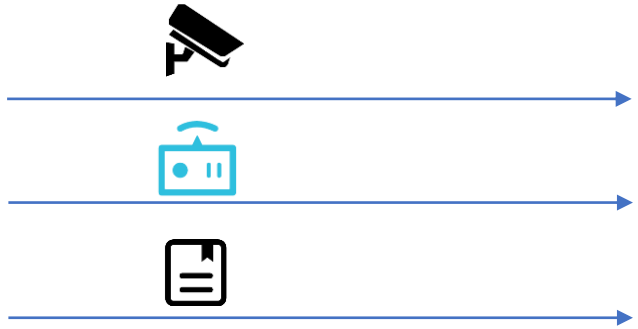
- Scope变大：同时能服务全球客户
- 商业速度加快：快速拿结果

大量实时、碎片化、关键的数据分析工作

研发中	集成中	上线中	上线后
• 研发 • Debug	• 研发 • 测试 • 联调	• 开发迭代 • 监控 • 运维	• 开发迭代 • 运维 • 运营 • 安全

- Scope变大：服务全球
- 关注面增多：系统，软件，用户…
- 多能：承担测试、部分运维与运营工作
- 需要快速响应

对工作的抽象：如何管理一套复杂系统



可度量皆可被管理

--管理学原理

数据采集+清洗 >	建模与规则 >	初步结果 >	汇总、生成、处理
安全场景：安全事件管理/运营			
Logs	Rule Engine	Event	Alarm
运营场景：活动跟踪与留存过滤统计			
User Click	Metric	Dashboard	Report
监控场景：监控线上业务负载，并进行告警			
Metric	Rule Engine	Dashboard	Alarm
日志分析场景：Access Log中突发错误定位			
Logs	Rule Engine	Dashboard	Alarm

观测源

处理操作

工作的挑战

阿里云

1. 构建监控程序，增加覆盖面

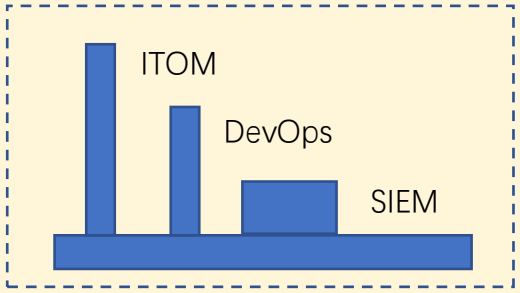
- 不同监控项，不同工具，不同存储
- 标准不统一，数据存储N份
- 不同软件，不同的体验

2. 接入与分析过程

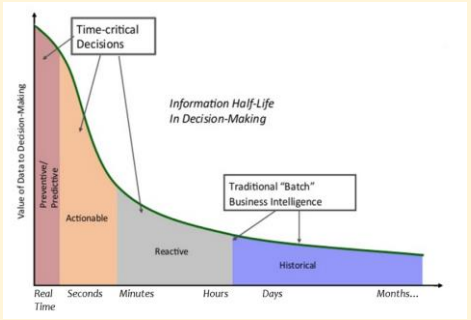
- 性能无法水平扩展
- 精度或延时无法达到诉求
- 不同软件不同标准

3. 判断、处理与分析

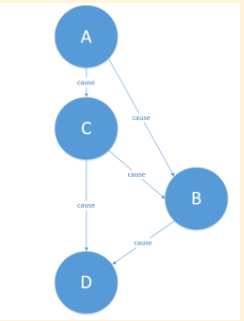
- 监控项太多
- 无用数据太多
- 根因较难定位



底座（中台）模式



秒级大数据分析能力

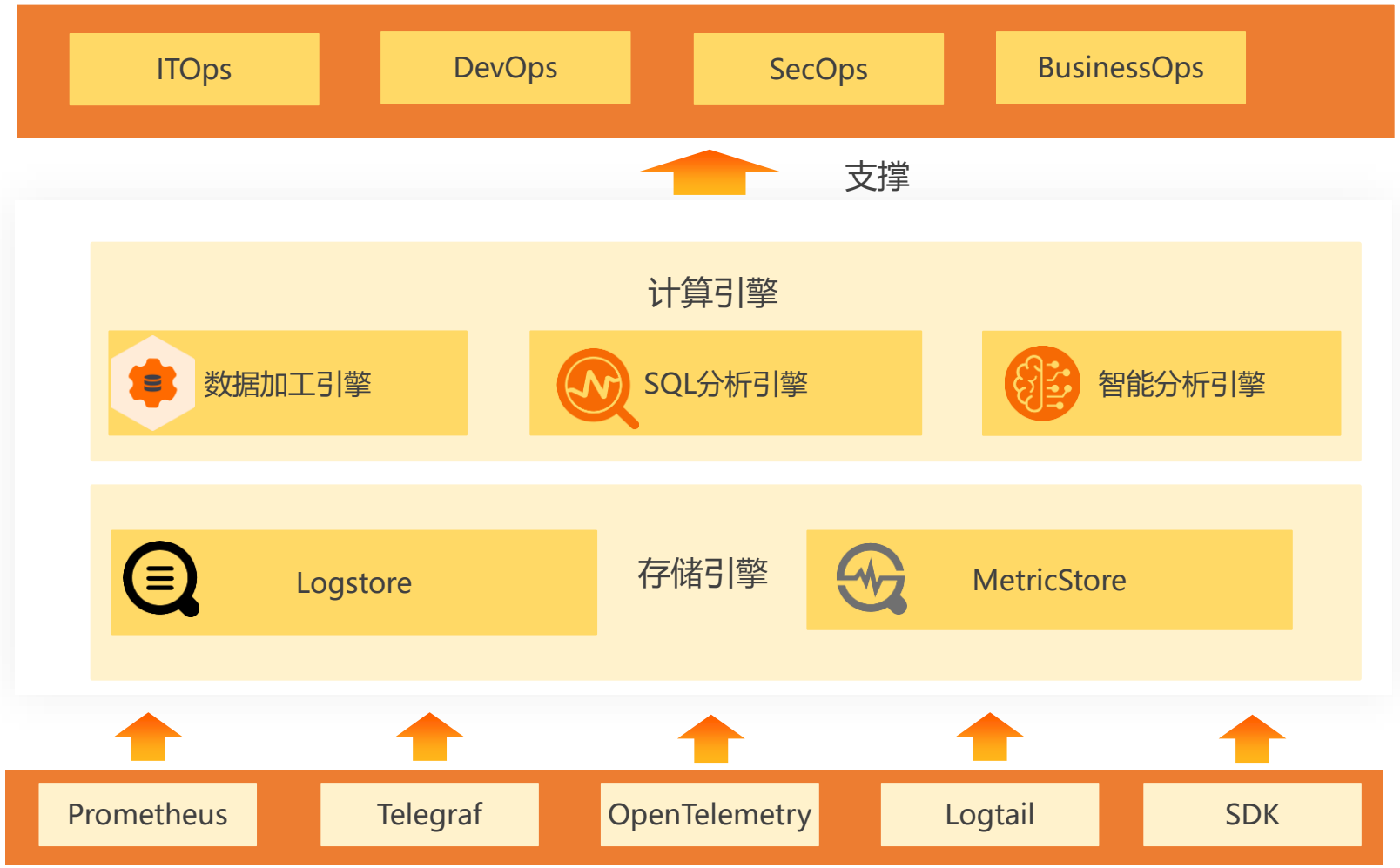


支撑AIOps算法

系统构建问题

算法 + 算力问题

SLS 构建可观察性数据中台（1-2-3）



1个中台
2种存储
3类计算

- DSL（数据加工/ETL）
- SQL（查询分析）
- AIOps（智能分析）

做什么？

提供存储、计算

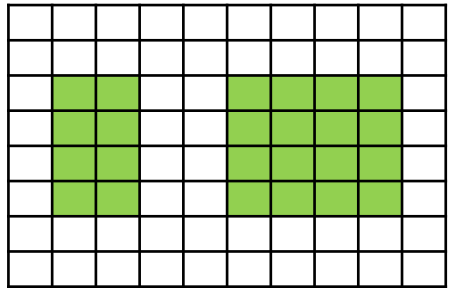
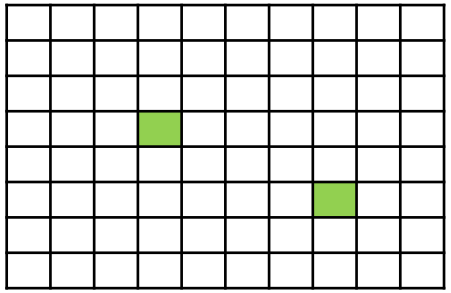
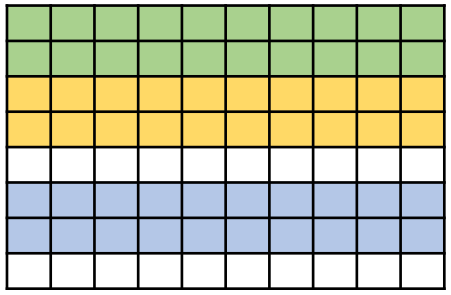
兼容各种数据源与协议

不做什么

不做业务

存储引擎（业界现状）

阿里云

Hadoop 存储	搜索引擎（ES）	NoSQL（Hbase/TSDB）	FIFO （Kafka）
			
适合：Log、海量Metric数据	适合：Log、Trace	适合：Metric	适合：实时数据转存
实时性：小时、分钟	实时性：秒级	实时性：秒级	实时性：秒级

流动性

- 不同存储格式
- 分散在多个系统中
- 流转依靠较慢ETL

接口易用性

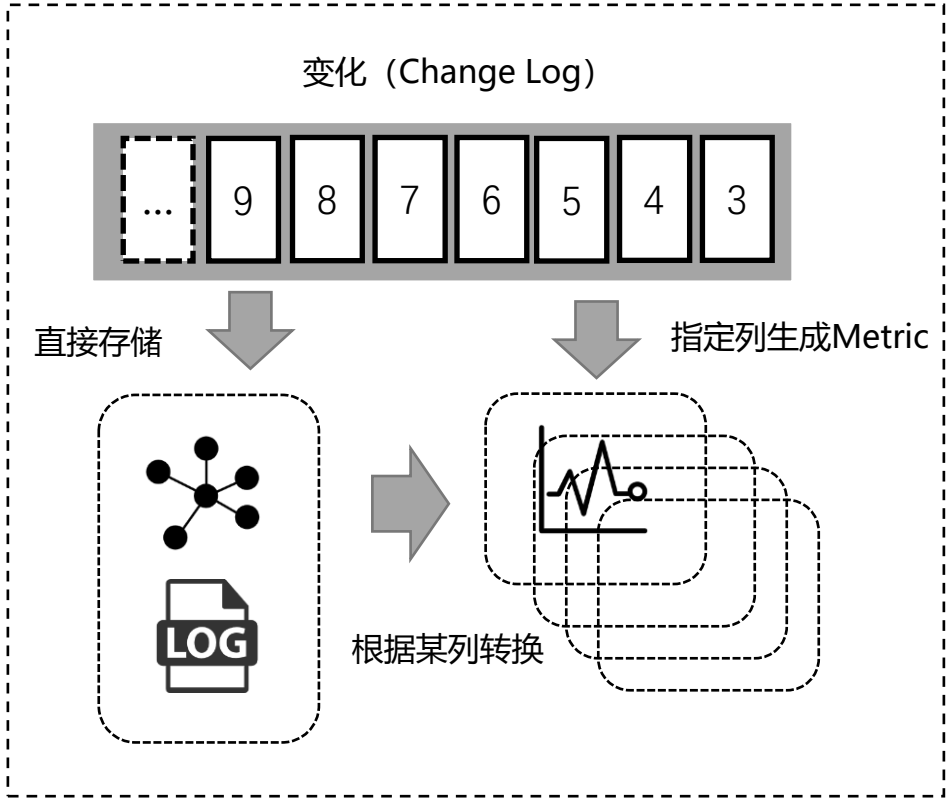
- Log、Metric、Trace接口不统一
- 不同API与交互方式
- 不适合二次开发

数据互通

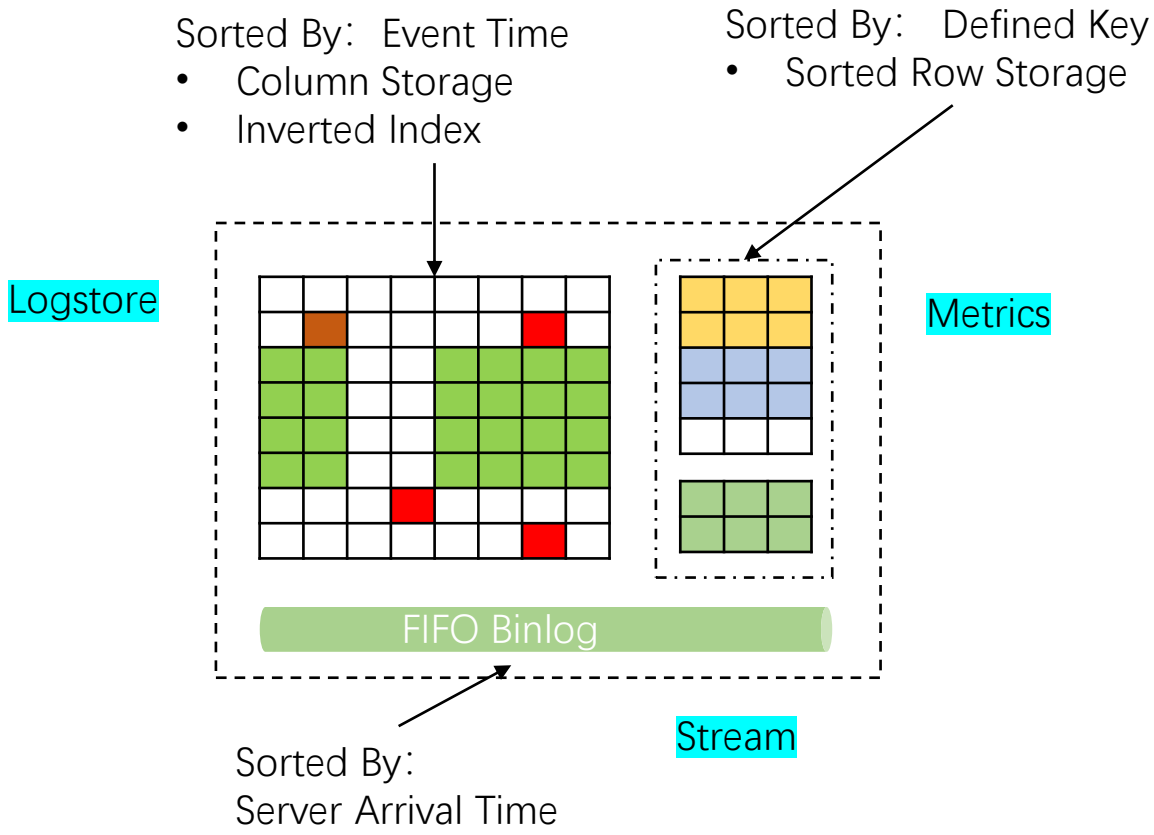
数据打通、交换难

统一存储设计

监控数据的生成



Logstore/MetricStore



计算三种问题与解法

阿里云

海量日志，如何变成有效数据？

业务系统多种格式混杂，如何区分？
如何进行规整，增强（Enrich）
所见即所得构建

数据加工
(DSL/ETL)

系统复杂，如何高效灵活分析？

面对PB级数据，如何所见即所得分析
对Log/Metric类分析如何融合

数据分析查询
(SQL92 + Search + PromQL)

如何抽丝剥茧，找到重要信息？

Error日志有几万条，重要信息被淹没，
数百个实例，其中有1-2个不正常，如何排查？
超时SQL，有哪些形态？

自定义计算
(AIOps、算法引擎)

DSL：数据加工（ETL）

```
e_kv('request_uri')
e_table_map(res_rds_mysql(...table='users'...))
e_table_map(res_rds_mysql(...table='servers'...))
```

时间	内容
08-17 23:05:17	__source__ : 192.168.7.171 __tag__:__path__ : /usr/local/nginx/logs/access.LOG __tag__:__receive_time__ : 1566177280 __topic__ : request_method : GET request_uri : console.xxxx.com/v2?project=notes&DisplayName=xyz&accounttraceid=3a076840-0477-43d0-8474-9da06167czb2 status : 200

时间	内容
08-17 23:06:37	__source__ : 192.168.7.171 __tag__:__path__ : /usr/local/nginx/logs/access.LOG __tag__:__receive_time__ : 1566177473 __topic__ : ecs_id : i-2te4h5q4jjgg9450t5g1 ecs_tag : v1.0.1 project : notes project_tag : 企业 project_type : vip request_method : GET request_uri : console.xxxx.com/v2?project=notes&DisplayName=xyz&accounttraceid=3a076840-0477-43d0-8474-9da06167czb2 status : 200 uid : 553153 vpc_id : vpc-uf6k5gm0zbd76aqgdzqli

用户元信息表

uid	project	type	tag
553153	notes	vip	企业
123531	it	vip	个人
235	知识库	free	个人

ECS服务器元信息表

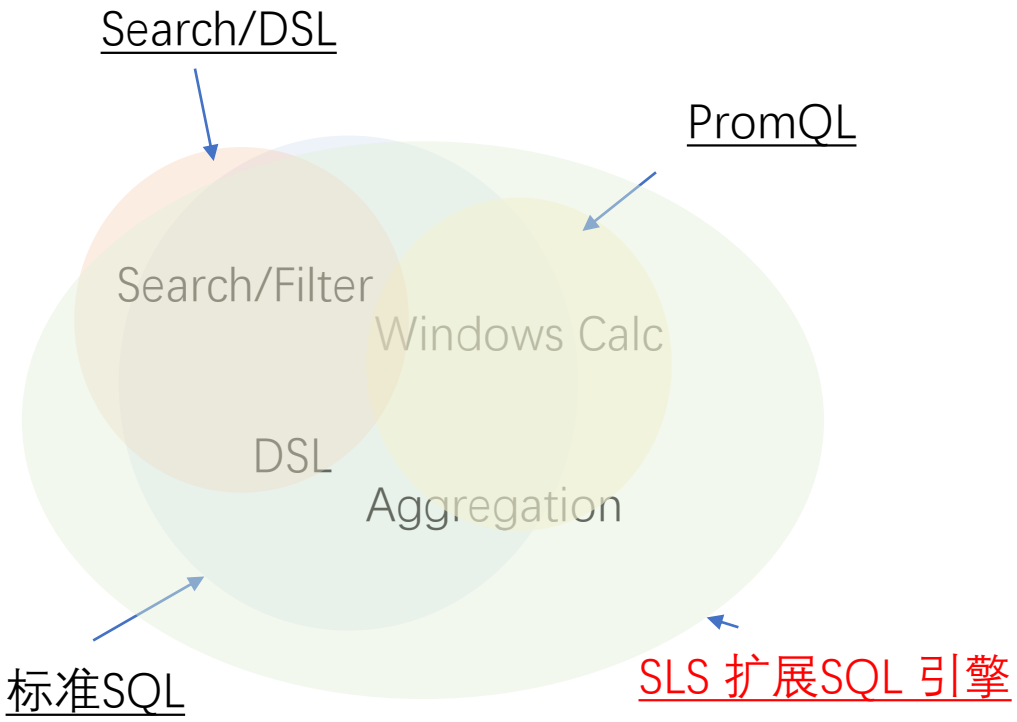
ecs_id	intranet_ip	vpc_id	tag
i-2te4h5q4jjgg9450t5g1	192.168.7.171	vpc-uf6k5gm0zbd76aqgdzqli	v1.0.1
i-2te4h5q4jjgg9450t5g1	192.168.7.172	vpc-uf6k5gm0zbd76aqgdzqli	v1.0.0
i-2te4h5q4jjgg9450t5g1	192.168.7.173	vpc-uf6k5gm0zbd76aqgdzqli	v1.0.0

RDS
表格

OSS
CSV文件

日志服务
Logstore

计算引擎与语法（SQL = Search + PromQL + SQL92）



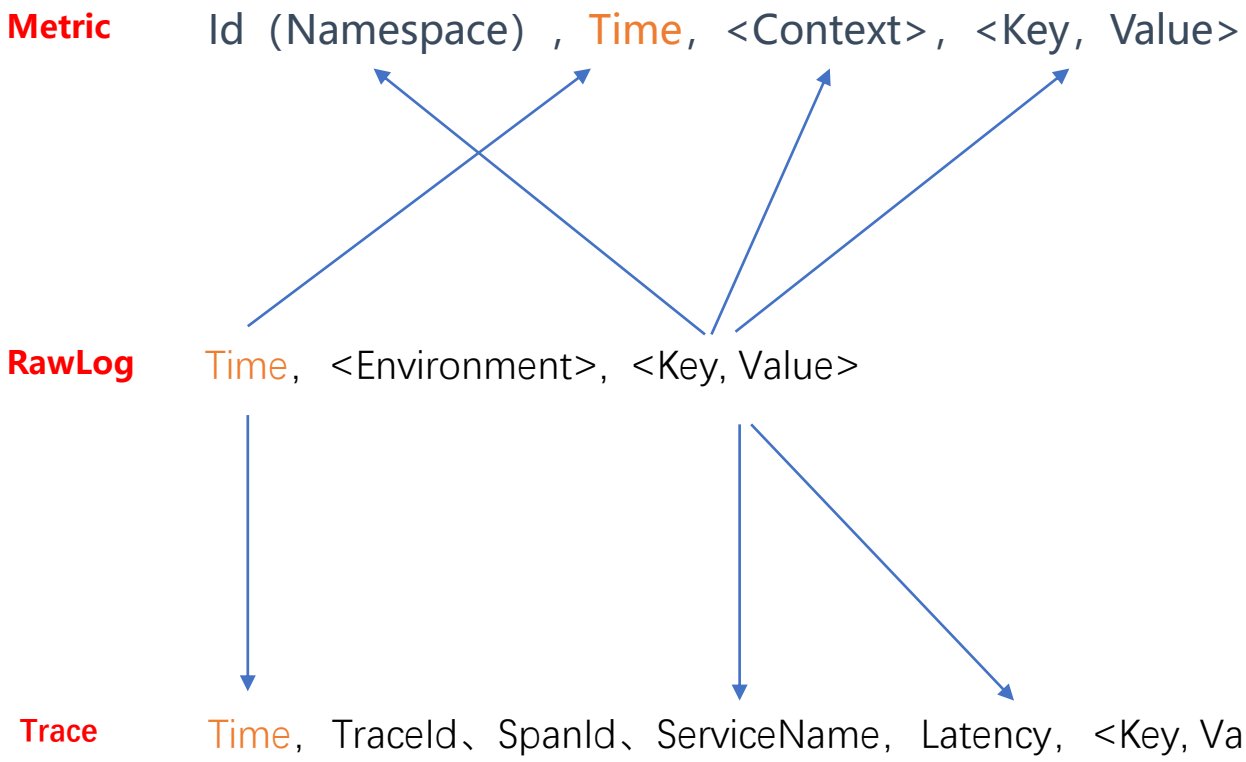
SELECT * from log where name='up' and machine like 'et2*'

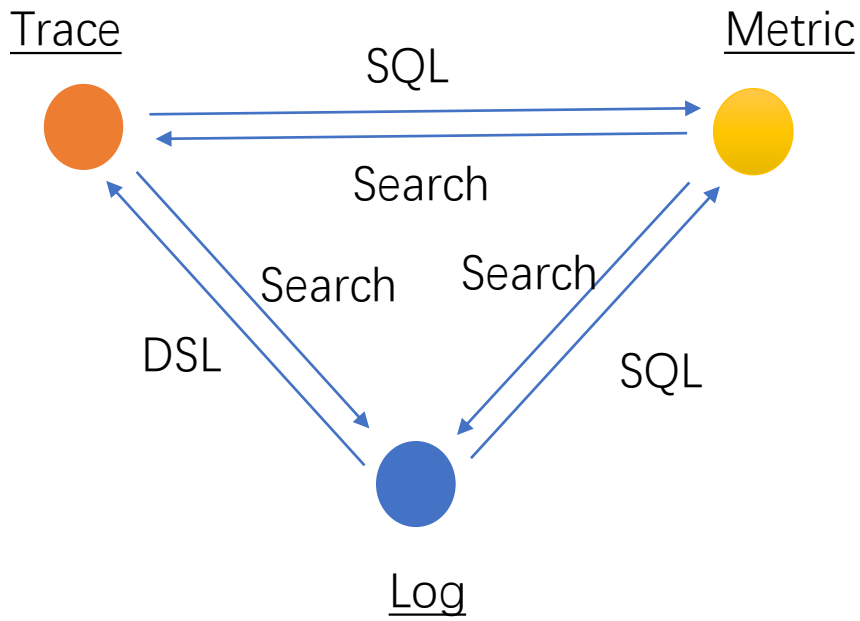
SELECT promql_query('up')FROM metrics
SELECT promql_query_range('up','1m')FROM metrics

SELECT sum(value) FROM (SELECT promql_query('up')FROM metrics)

```
select ts_predicate_arma(time, value,5,1,1,1,1,true) from
(SELECT (time/1000) as time, value from (
select promql_query_range('1 -
avg(irate(node_cpu_seconds_total{instance=~".*",mode="idle"
}[10m]))','10m')as t from metrics
) order by time asc ) limit 10000
```

三类数据相互转化


Metric
Id（Namespace），Time，<Context>，<Key，Value>
RawLog
Time，<Environment>，<Key, Value>
Trace
Time，TraceId、SpanId、ServiceName，Latency，<Key, Value>


Trace
Metric
SQL
Search
Search
Search
DSL
SQL
Log

提供常用AI算法

阿里云

趋势预测

- 趋势预测
- 趋势预警

异常发现

- 断层识别
- 智能基线
- 周期发现

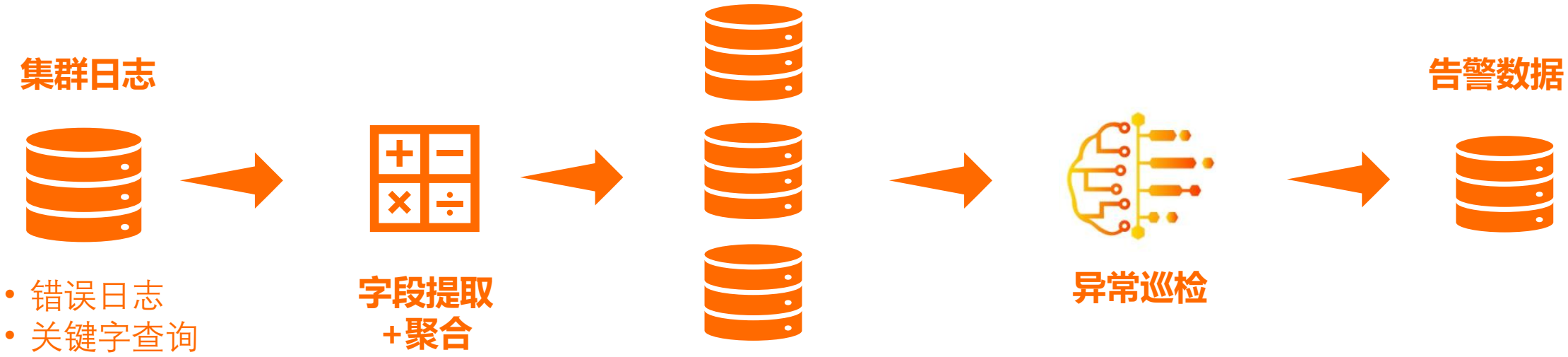
聚类

- 时序聚类
- 日志聚类

根因推导

- KPI定位
- 频繁+差异模式

案例：K8S立体巡检（应用/POD/机器）



问题：应用层运行大量作业在Pod中，Pod运行在物理机中

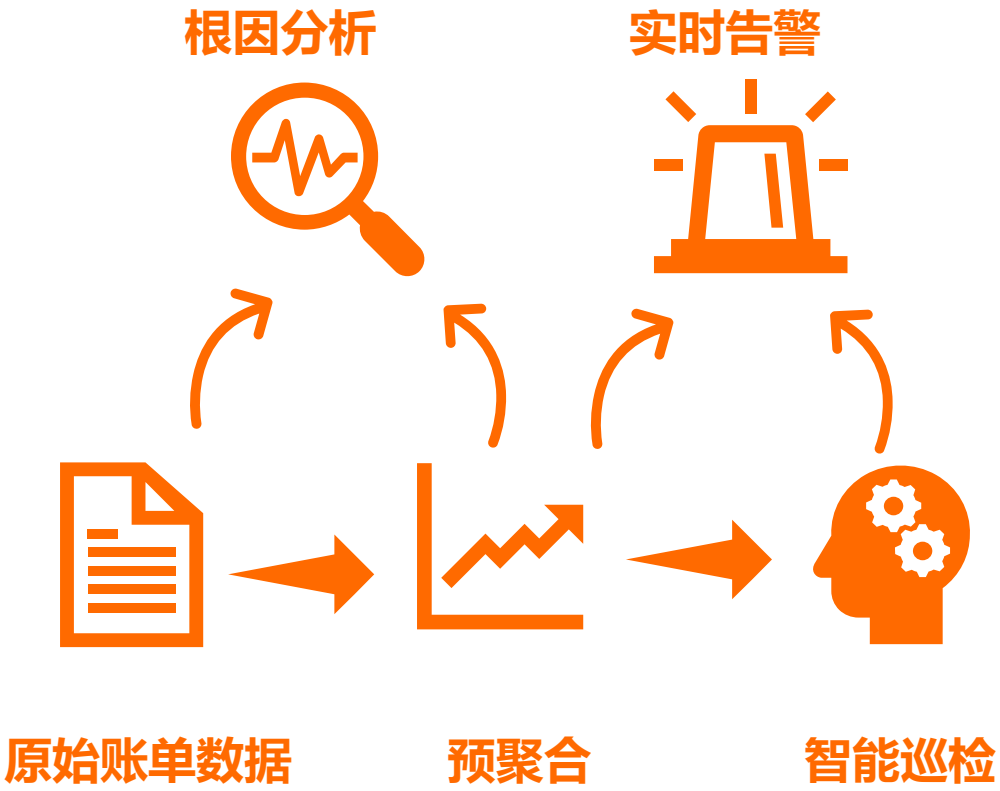
1. 对各层日志进行提取，形成指标
2. 对指标进行自动化巡检与分析


ETL三层服务关系监控 (属于 sls-ml-huhehaote-wuming)
时间选择
编辑
订阅
告警
刷新
分享
全屏
标题设置
重置时间
ETL作业ID 2020-08-13 09:00:00~2020-08-14 09:00:00
schedule
1ecf46762a8e10ac44589d4b4b46f464
1f01a84b14647107d3f6e8ca6c57dd5d
2162b7eac660df5c92504fb0fdde7d4c
220797ce8e34a1356d4c6c751e9a7264
总数: 3026
1
/ 152
单个作业的可视化情况 2020-08-13 09:00:00~2020-08-14 09:00:00
140K
120K
100K
80K
60K
40K
20K
0
09:00
11:00
13:00
15:00
17:00
19:00
21:00
23:00
01:00
03:00
05:00
07:00
100
80
60
40
20
0
etl_accept
etl_droppec
etl_delivere
etl_failed
etl_latency
异常ETL Job 2020-08-13 09:00:00~2020-08-14 09:00:00
schedule
6dbdafc4dffd4963349d09022dd3dc88
555854ad89f96b2d1ec833690ca0dd5a
328252fcd6186c3014f822a87efba69b
4c6e6c64515f6585c636394910fb6c49
总数: 556
1
/ 28
ETL异常指标 2020-08-13 09:00:00~2020-08-14 09:00:00
time
index_name
score
暂无数据
总数: 0
1
/ 0
etl_accept 2020-08-13 09:00:00~2020-08-14 09:00:00
120K
100K
80K
60K
40K
20K
09:00
11:00
13:00
15:00
17:00
19:00
21:00
23:00
01:00
03:00
05:00
07:00
score:
0.95
查询
etl_latency 2020-08-13 09:00:00~2020-08-14 09:00:00
70
60
50
40
30
20
10
0
09:00
11:00
13:00
15:00
17:00
19:00
21:00
23:00
01:00
03:00
05:00
07:00
etl_failed 2020-08-13 09:00:00~2020-08-14 09:00:00
1
0
09:00
11:00
13:00
15:00
17:00
19:00
21:00
23:00
01:00
03:00
05:00
07:00
Pod信息 2020-08-13 09:00:00~2020-08-14 09:00:00
单个Pod的可视化情况 2020-08-13 09:00:00~2020-08-14 09:00:00

案例：账单中心基于SLS开发“成本管家”

问题：云产品账单数据、分析、预警、分摊、根因分析等。

- 2天开发完成，超过5W客户使用
- 涉及算法：
  - 根因分析（AIOps 2019赛题）
  - 消费预测（时序预测）
  - 异常巡检（变点检测）




账单分析
设置
总览
明细
说明
自定义分析
优化
SLS账单分析
成本管家
自定义分析
总览
明细
优化
资源成本分摊
ECS账单分析
OSS账单分析
SLS账单分析
batchcompute费用分析
财务月报
说明
设置
Data Transformation T...
aliyun_bill
数据加工
1天（相对）
自动刷新
分享
查询分析属性
另存为快速查询
另存为告警
查询/分析
32
0
08月14日
08月14日
08月14日
08月14日
08月14日
08月15日
08月15日
日志总条数：558 查询状态：结果精确
原始日志
日志聚类 new
LiveTail
统计图表
内容列显示
列设置
快速分析
搜索
BillingDate
BillingItem
BillingType
CostUnit
Currency
DeductedByCashCoupons
DeductedByCoupons
DeductedByPrepaidCard
时间
内容
1 08-15 05:00:00 Currency : CNY DeductedByCashCoupons : 0.0 DeductedByCoupons : 0.0 DeductedByPrepaidCard : 0.0 InvoiceDiscount : 0.005 Item : PayAsYouGoBill OutstandingAmount : 0.03 OwnerID : PaymentAmount : 0.0 PaymentTime : PretaxAmount : 0.03 PretaxGrossAmount : 0.04 ProductCode : bwp ProductDetail : NAT共享带宽包（按量付费） ProductName : NAT网关 ProductType : RecordID : 2020080593421059 RoundDownDiscount : 0.005 Status : PayUnsettle SubOrderId : SubscriptionType : PayAsYouGo UsageEndTime : 2020-08-15 06:00:00 UsageStartTime : 2020-08-15 05:00:00 __source__ : bill __tag__:__receive_time__ : 1597448023 __topic__ :
2 08-15 05:00:00 Currency : CNY DeductedByCashCoupons : 0.0 DeductedByCoupons : 0.0 DeductedByPrepaidCard : 0.0 InvoiceDiscount : 1.962 Item : PayAsYouGoBill OutstandingAmount : 1.37 OwnerID : PaymentAmount : 0.0 PaymentTime : PretaxAmount : 1.37 PretaxGrossAmount : 3.34 ProductCode : redisa ProductDetail : 云数据库KvStore-按量付费 ProductName : 云数据库 Redis 版 ProductType : RecordID : 2020080593421060 RoundDownDiscount : 0.008 Status : PayUnsettle SubOrderId : SubscriptionType : PayAsYouGo UsageEndTime : 2020-08-15 06:00:00 UsageStartTime : 2020-08-15 05:00:00 __source__ : bill __tag__:__receive_time__ : 1597448023 __topic__ :
3 08-15 05:00:00 Currency : CNY DeductedByCashCoupons : 0.0 DeductedByCoupons : 0.0 DeductedByPrepaidCard : 0.0 InvoiceDiscount : 1.373 Item : PayAsYouGoBill OutstandingAmount : 0.95 OwnerID : PaymentAmount : 0.0 PaymentTime : PretaxAmount : 0.95 PretaxGrossAmount : 2.337 ProductCode : dds ProductDetail : 云数据库MongoDB副本集版（按量付费） ProductName : 云数据库 MongoDB ProductType : RecordID : 2020080593421064 RoundDownDiscount : 0.014 Status : PayUnsettle SubOrderId : SubscriptionType : PayAsYouGo UsageEndTime : 2020-08-15 06:00:00 UsageStartTime : 2020-08-15 05:00:00 __source__ : bill
日志总条数：558，每页显示：20
上一页
1
2
3
4
28
下一页
1/28
到第
页
确定

粗浅的心得体会

AIOps = AI + DevOps/ITOps/SecOps/BusinesOps...
- 数据是根本
- 算力是基础
- 算法是核心

Domain Knowledge是AIOps落地关键
- 模板化
- 知识表示与推理
- 迁移学习

SLS 致力为AIOps提供中台能力
- 低成本的存储与计算
- 开源软件兼容与对接

欢迎各位老师的合作与交流！

SLS 团队官方微信

我的微信

阿里云

奥运会全球指定云服务商