CNUTCon 2017 全球运维技术大会

基于日志trace的智能故障定位系统

曹轩

百度搜索运维团队技术负责人

主办方 Geekbang 极客邦科技 InfoQ

Geekbang.
极客邦科技

极客搜索

全站干货，一键触达，只为技术

s.geekbang.org

扫描二维码立即体验

有没有一种搜索方式，能整合 InfoQ 中文站、极客邦科技旗下12大微信公众号矩阵的全部资源?
极客搜索，这款针对极客邦科技全站内容资源的轻量级搜索引擎，做到了!

扫描上方二维码，极客搜索!

EGO EXTRA GEEKS' ORGANIZATION NETWORKS

这里只有
技术领导者

EGO会员第二季招募季正式开启

报名时间：9月1日-9月15日

扫描添加E小欧，

邀您进入EGO会员预报名群

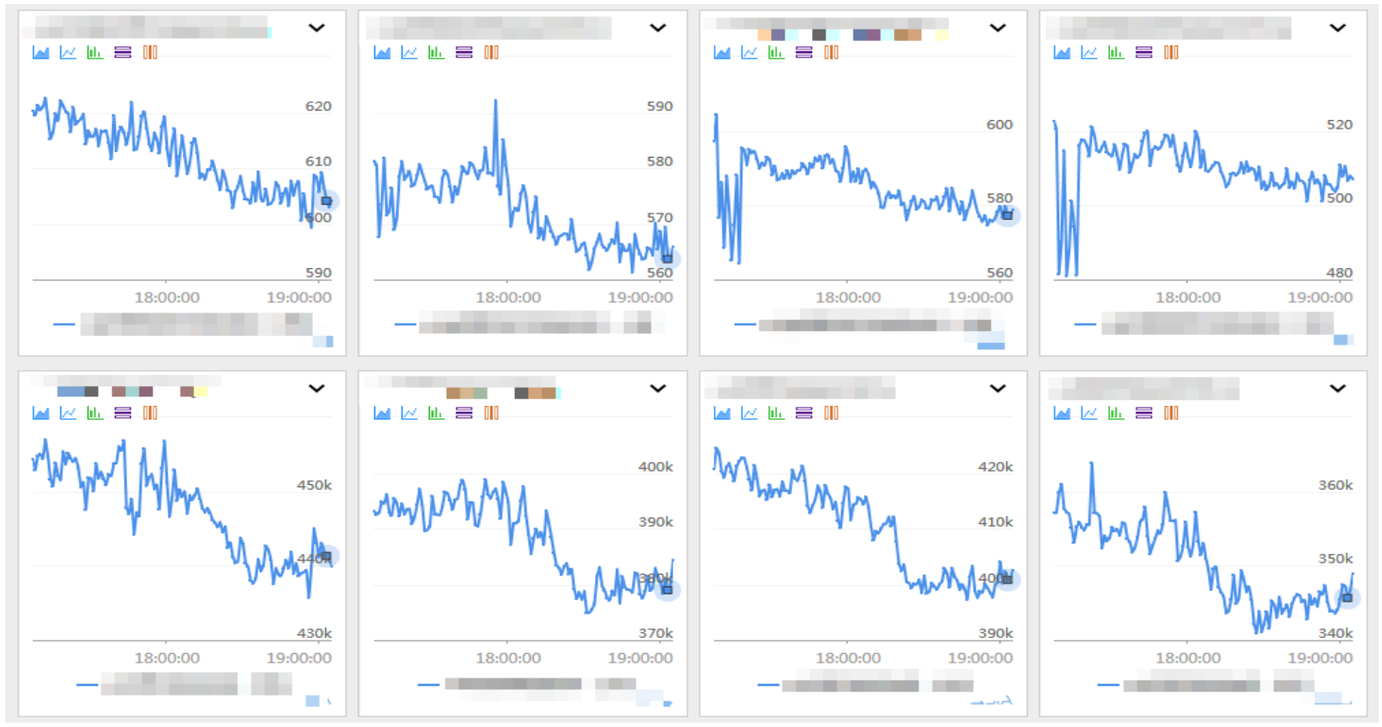
立即报名

E小欧

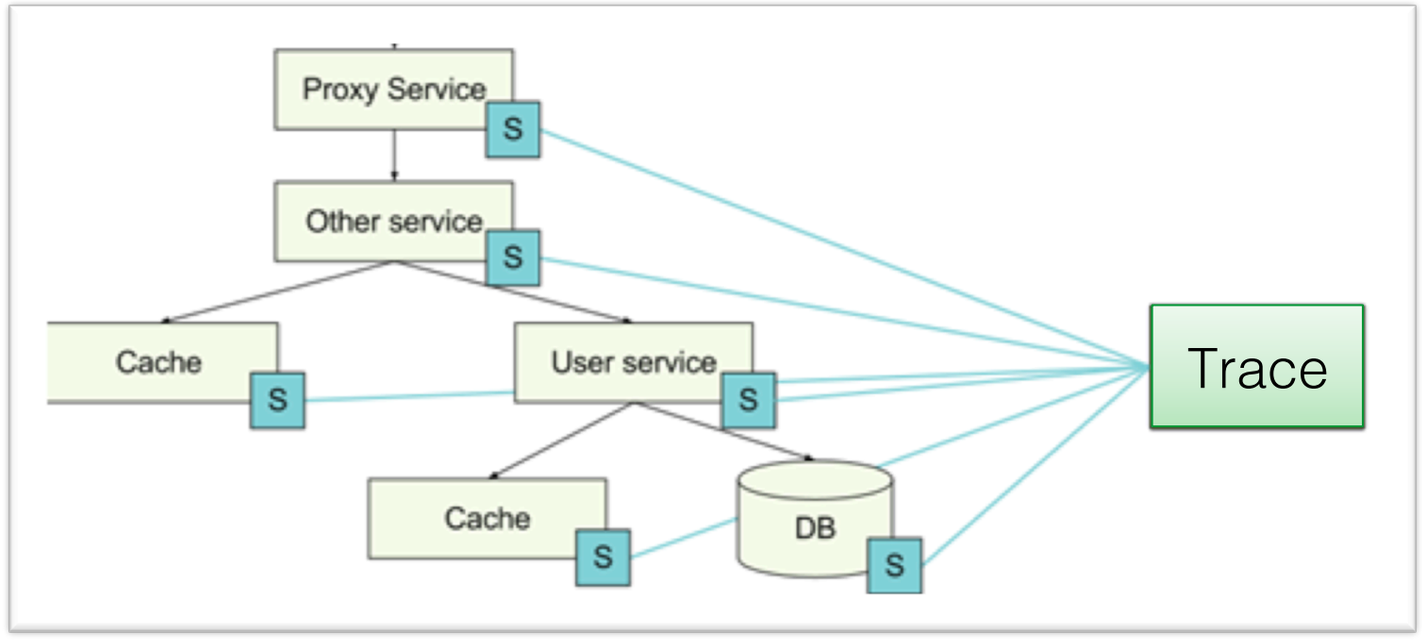
TABLE OF **CONTENTS**

传统故障定位系统及其局限

- 故障定位系统类型
  - 统计型
  - Trace 型

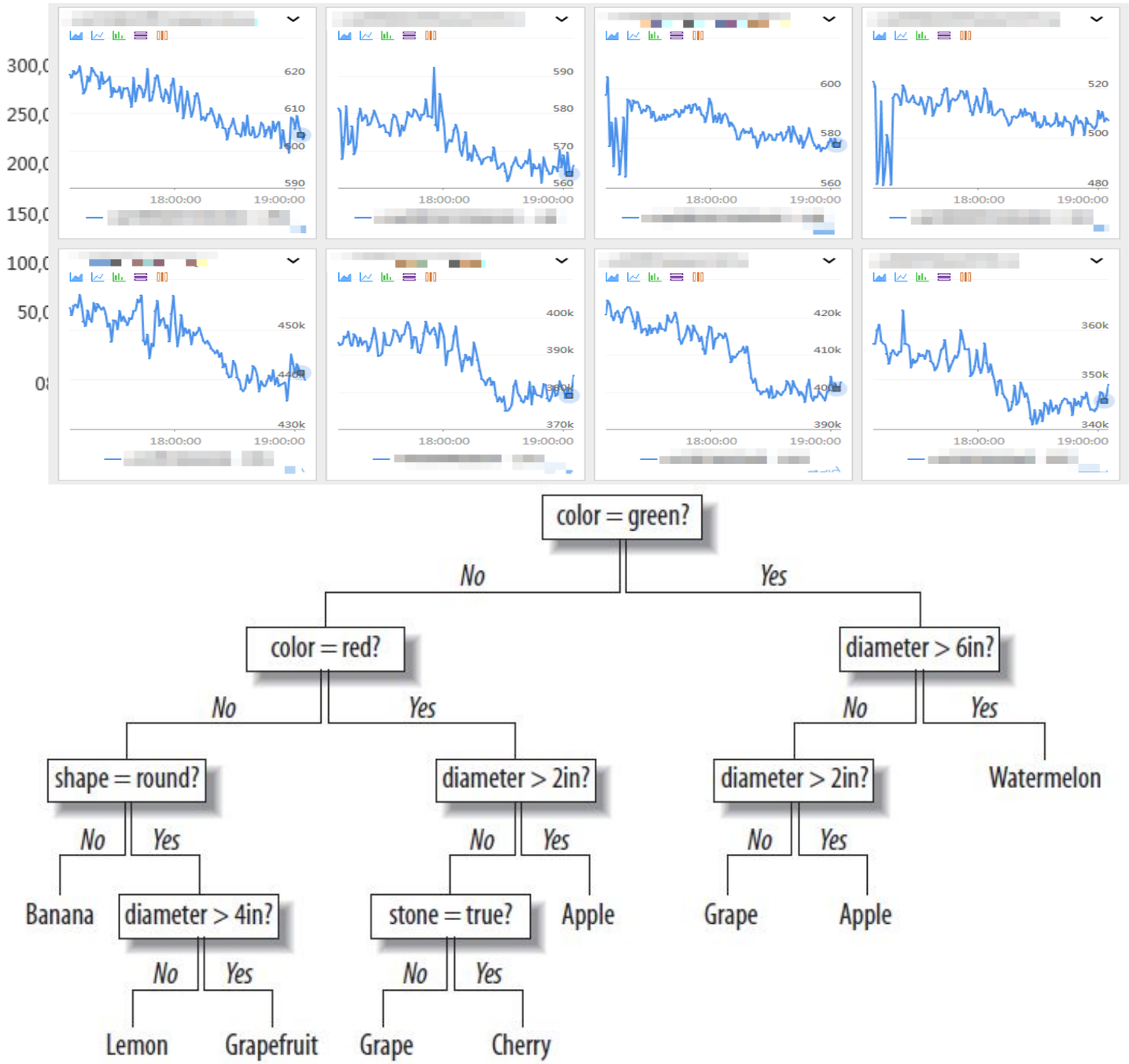



```
15/12/24 22:36:53 INFO Worker: Starting Spar
15/12/24 22:36:53 INFO Worker: Running Spark
15/12/24 22:36:53 INFO Worker: Spark home: /
15/12/24 22:37:04 INFO Utils: Successfully s
15/12/24 22:37:04 INFO WorkerWebUI: Started
15/12/24 22:37:04 INFO Worker: Connecting to
15/12/24 22:37:05 INFO Worker: Successfully
15/12/24 22:40:26 INFO Worker: Asked to laun
15/12/24 22:40:26 INFO SecurityManager: Chan
15/12/24 22:40:26 INFO SecurityManager: Chan
15/12/24 22:40:26 INFO SecurityManager: Secu
 Set(hadoop); users with modify permissions:
15/12/24 22:40:26 INFO ExecutorRunner: Launc
usr/local/spark1.5.1/lib/spark-assembly-1.5.
park1.5.1/lib/datanucleus-core-3.2.10.jar:/u
ark.driver.port=42076" "-XX:MaxPermSize=256m
//sparkDriver@192.168.137.117:42076/user/Coa
" "--app-id" "app-20151224224026-0000" "--wo
```



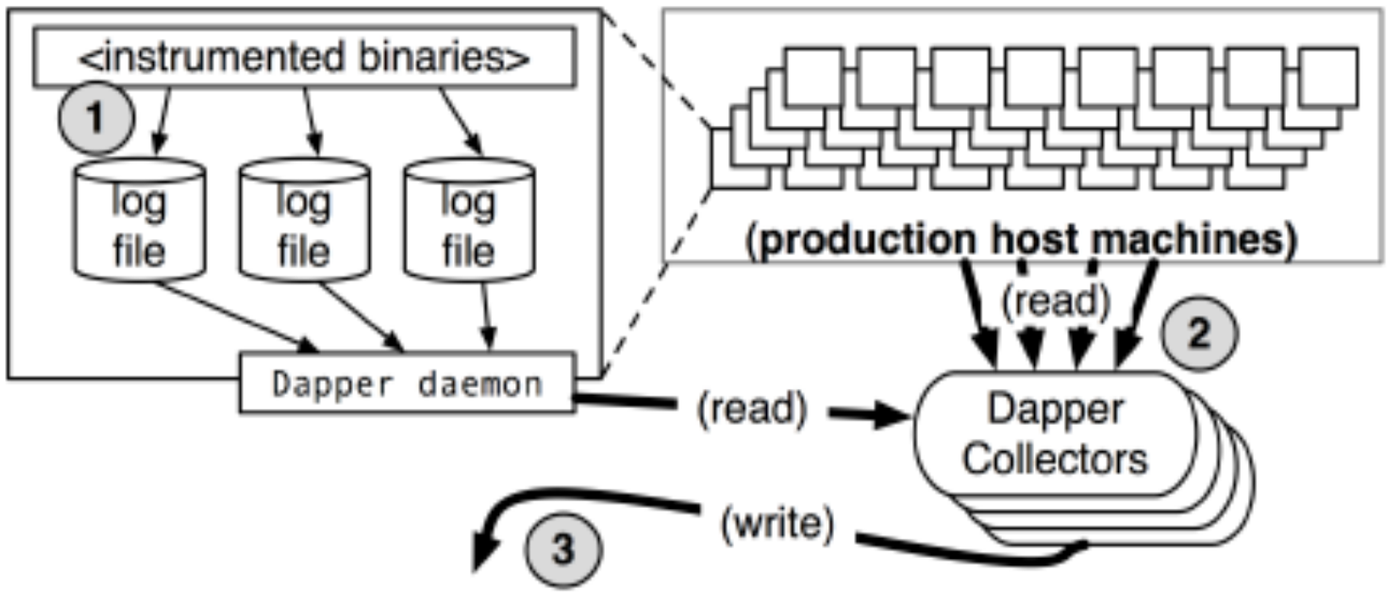
传统故障定位系统及其局限

- 统计型
  - 场景
    - resource
    - workload
    - Latency
  - 特点
    - dashboard
    - Time series
    - 决策树
    - 多维度汇聚
    - 用于缩小问题范围



传统故障定位系统及其局限

- Trace 型
  - 场景
    - 单 PV 根因追查
    - Debug
    - 策略调优
  - 特点
    - 全局唯一描述符关联
    - 复现
    - 从 Warning/Fatal 日志获取信息
    - 非零即一的判定
    - 抽样

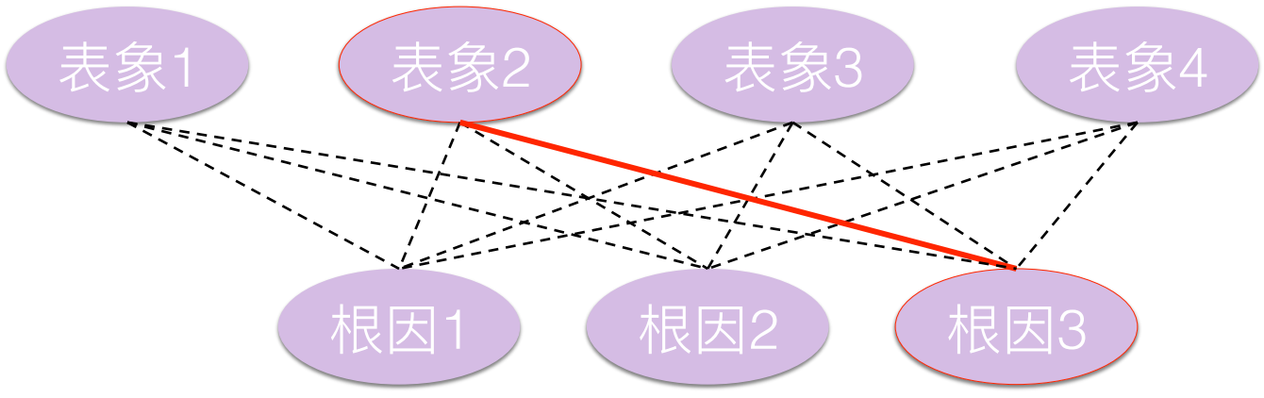


trace id	span 12	span 23	span 34	span 45	span 56	...
123456	*nil*	*nil*	**<data>**	**<data>**	*nil*	...
246802	**<data>**	*nil*	*nil*	*nil*	**<data>**	...
357913	*nil*	**<data>**	*nil*	*nil*	*nil*	...
...	...	...	...	...	...	...

(Central Bigtable repository for trace data)

传统故障定位系统及其局限

- 局限
  - 统计型
    - 概率模型，无法得到精确结论
    - 汇聚粒度问题，面临数据完整性和效率的取舍
    - 不易在根因和表象间建立明确的关联



  - Trace 型
    - 大规模复杂异常时，抽样个别 PV 的定位结论，容易以偏概全，缺少汇聚回归
    - 受限于人工分析，速率通常在分钟级每 PV
    - 依赖于人的经验
    - 丢失了时间轴上的因果信息

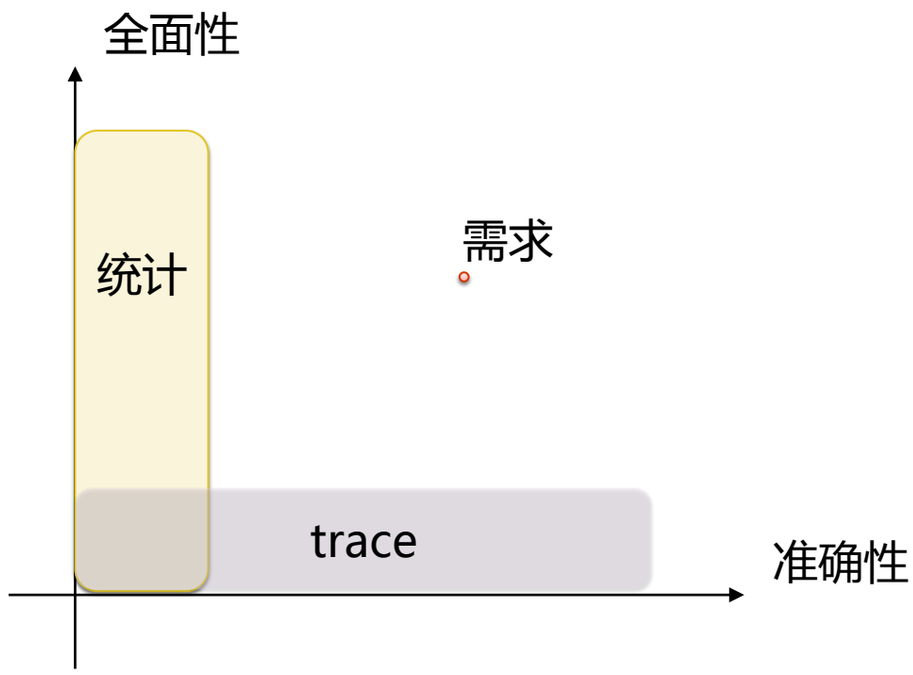


TABLE OF **CONTENTS**

基于机器学习的智能 TRACE 系统

局限

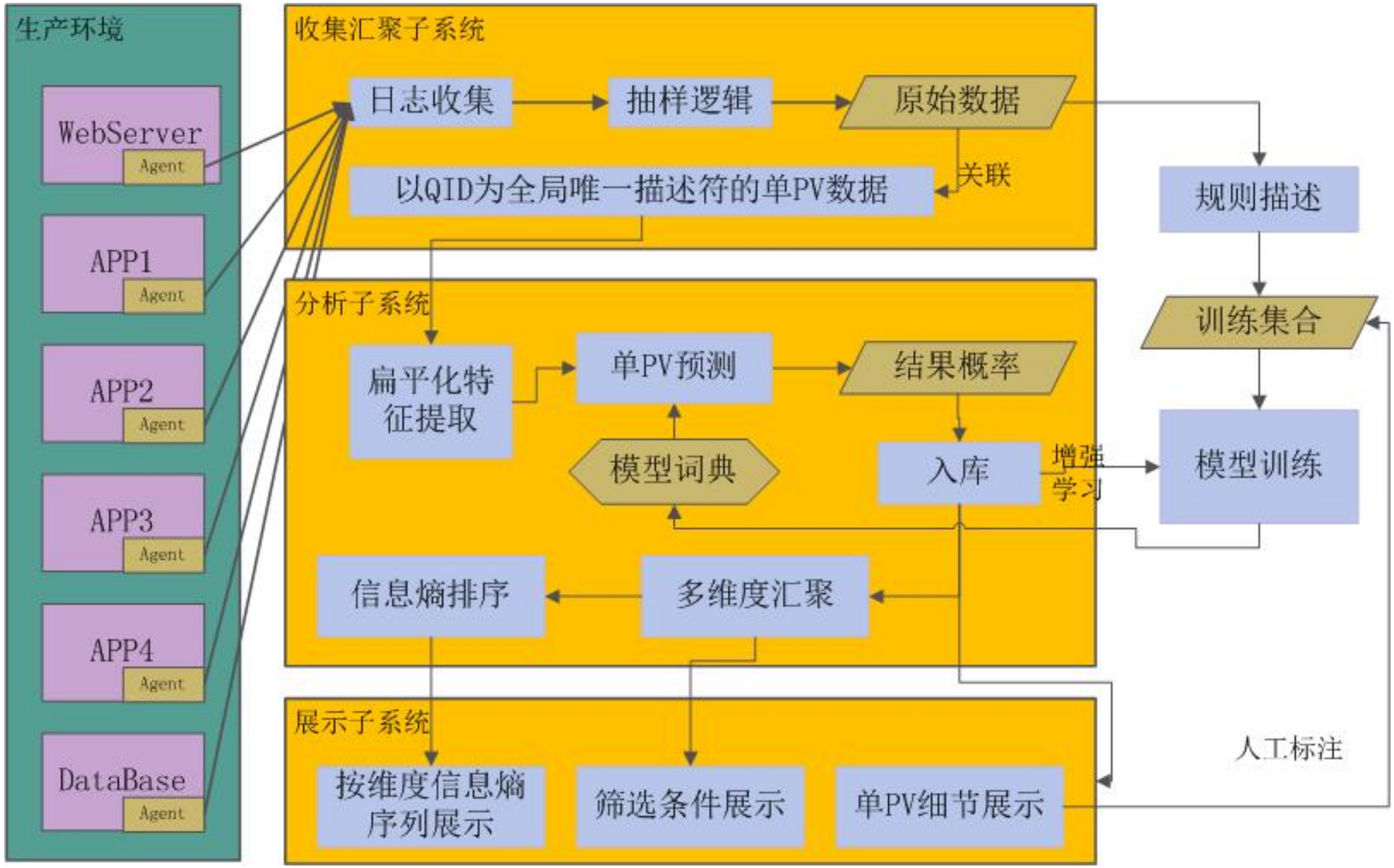
- Trace 型
  - 大规模复杂异常时，抽样个别 PV 的定位结论，容易以偏概全，缺少汇聚回归
  - 受限于人工分析，速率通常在分钟级每 PV
  - 依赖于人的经验
  - 丢失了时间轴上的因果信息
- 统计型
  - 概率模型，无法得到精确结论
  - 汇聚粒度问题，面临数据完整性和效率的取舍
  - 不易在根因和表象间建立明确的关联

解决

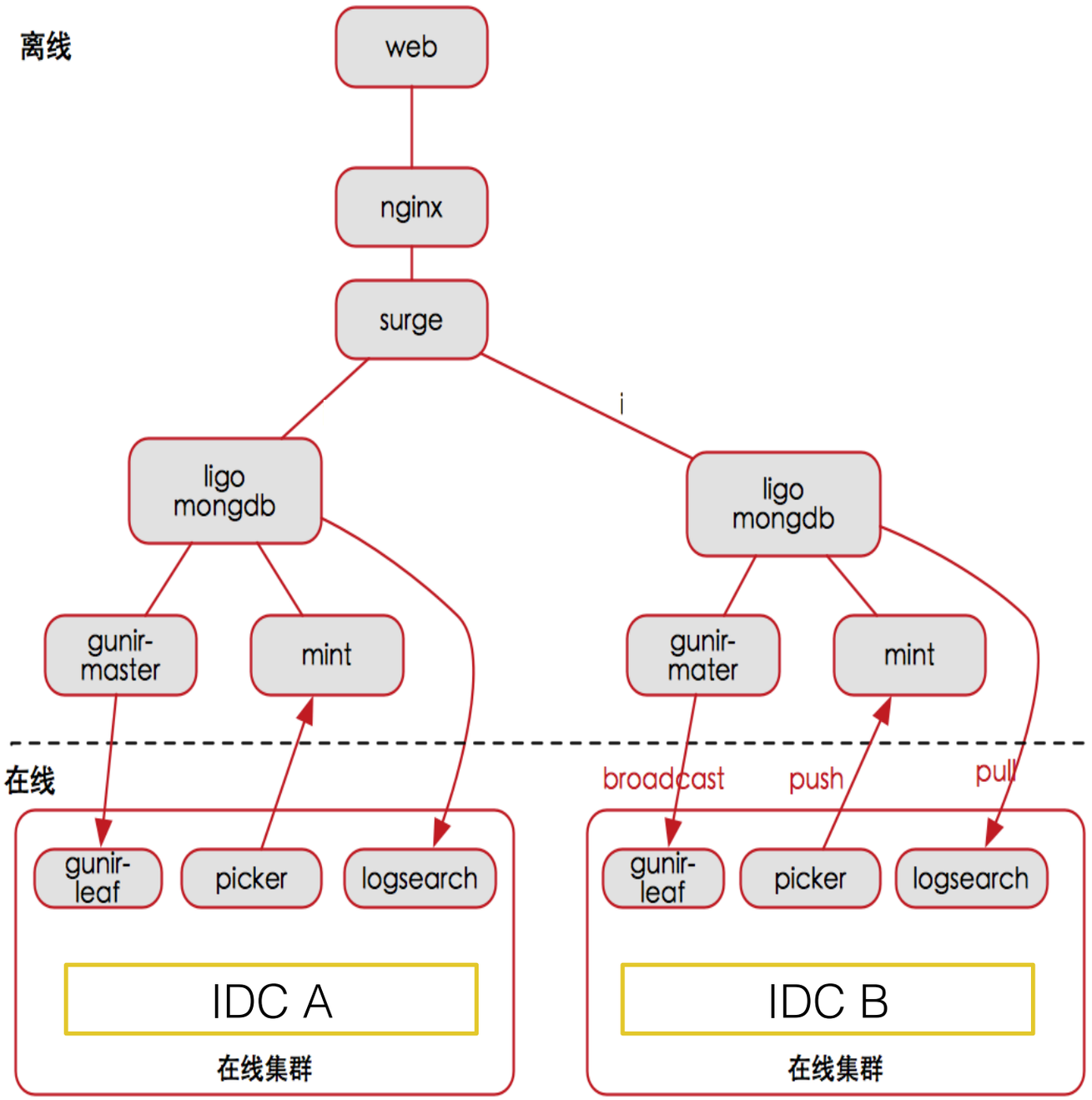
- 机器学习
  - 机器学习技术的进步，使高并发、单 PV 根因追查成为可能
  - 人的知识以模型方式沉淀
- 多维度汇聚统计 & 展示
  - 对根因统计而非对表象统计
  - 根因大幅剔除冗余信息
  - 对各维度做信息熵排序，优先展示存在异常的维度
  - 时间也作为维度之一，结合事件流图，因果序列信息仍然得到充分利用

既准确，又全面

基于机器学习的智能 TRACE 系统



基于机器学习的智能 TRACE 系统



模块组成：

- JS+Nginx：多活的展示系统
- Surge：特征提取、汇聚的策略、日志 trace
- Ligo：流量转发、调度、需求汇总；
- Gunir-master：筛选异常 PV，用户指定时间范围同步查询；
- Mint：ID:[ip:path:offset]
- Mongodb：cache 的作用

TABLE OF **CONTENTS**

传统故障定位辅助系统及其局限

基于机器学习的智能 trace 系统

GBDT 单 PV 根因预测模型

数据多维度汇聚与维度间信息熵排序

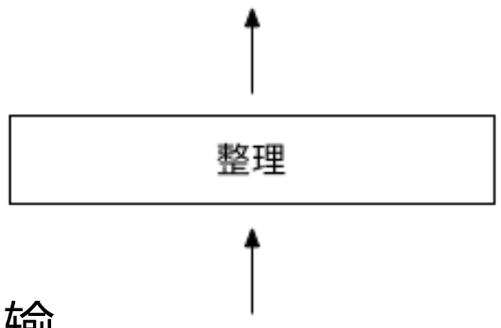
GBDT 单 PV 根因预测模型

feature_a	feature_b	feature_c	feature_d	feature_e	feature_f
0	0	1	0	0	0
1	0	0	0	0	0
0	0	0	0	1	1

expected
B
A
C

predict
B
B
C

qid	feature_a	feature_b	feature_c	feature_d	feature_e	feature_f	label
9e6d88e1000149f9	1	1	0	0	0	0	A
123456789abcdefg	0	0	1	1	0	0	B
aaabbbcccdddeeef	0	0	0	0	1	1	C



离线训练的工作流：

1 访问日志存储中获取全量日志，格式为qid:<log>

2 访问特征提取模块提取特征，格式qid:[feature]

3 规则引擎根据feature为每个query自动标记label，输出：qid:[label set]

4 标记样本用于模型训练

```
[
  {"qid":9e6d88e1000149f9, "feature_a": 1, "feature_b": 1, "label": "A"},
  {"qid":123456789abcdefg, "feature_c": 1, "feature_d": 1, "label": "B"},
  {"qid":aaabbbcccdddeeef, "feature_e": 1, "feature_f": 1, "label": "C"}
]
```

GBDT 单 PV 根因预测模型

Algorithm 10.3 *Gradient Tree Boosting Algorithm.*

1. Initialize $f_0(x) = \arg\min_\gamma \sum_{i=1}^{N} L(y_i, \gamma)$.
2. For $m = 1$ to M:
   (a) For $i = 1, 2, \ldots, N$ compute

$$r_{im} = -\left[\frac{\partial L(y_i, f(x_i))}{\partial f(x_i)}\right]_{f=f_{m-1}}.$$

   (b) Fit a regression tree to the targets r_{im} giving terminal regions R_{jm}, $j = 1, 2, \ldots, J_m$.
   (c) For $j = 1, 2, \ldots, J_m$ compute

$$\gamma_{jm} = \arg\min_{\gamma} \sum_{x_i \in R_{jm}} L\left(y_i, f_{m-1}(x_i) + \gamma\right).$$

   (d) Update $f_m(x) = f_{m-1}(x) + \sum_{j=1}^{J_m} \gamma_{jm} I(x \in R_{jm})$.
3. Output $\hat{f}(x) = f_M(x)$.

GBDT 单 PV 根因预测模型

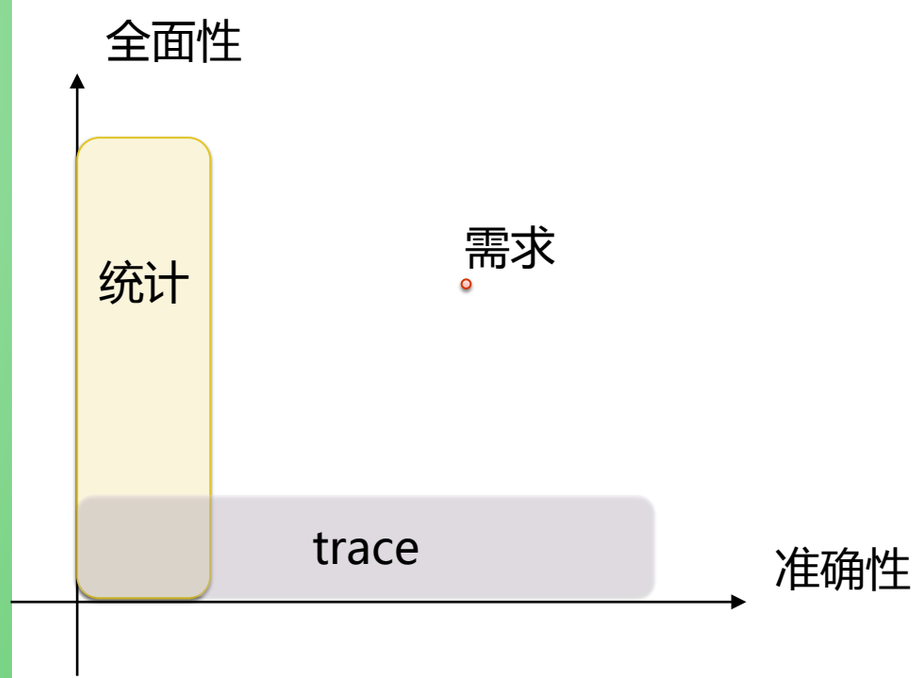
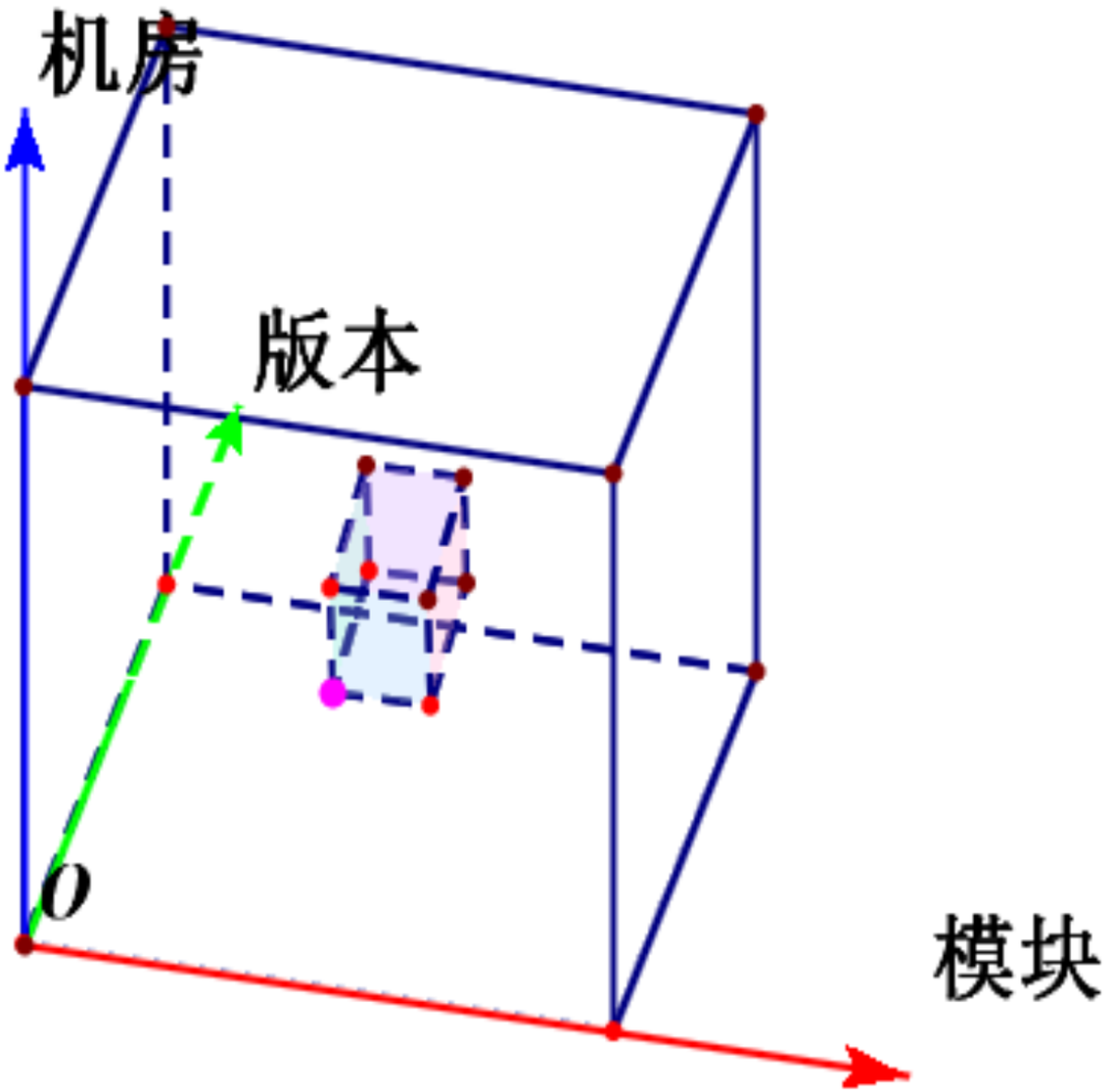


TABLE OF **CONTENTS**

数据多维度汇聚与维度间信息熵排序

- 止损的方式是通过找到小范围的类聚，并尝试在维度内替换和剪裁
- 定位的首要目的是逐步缩小问题范围

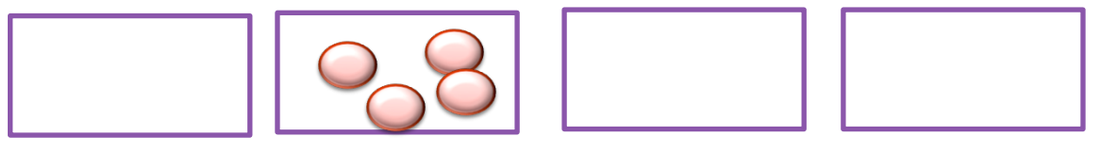


数据多维度汇聚与维度间信息熵排序

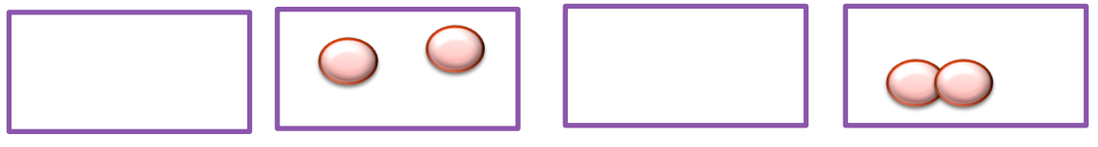
Entropy策略

<u>信息熵</u>

- 用来描述信源的不确定度
- 在本系统内用于计算维度的显著性
- 不同维度上显著性可比，显著性最大的往往就是根因



Entropy=0



Entropy=1

Entropy=2

维度	显著性特征top3		
故障分类ID	1:100%	2:0%	3:0%
错误码	503_503:89%	509_599:10%	599_599:1%
机房	IDC A:21%	IDC_B:20%	IDC_C:17%
cip	-	-	-

$$Entropy\ (S) = -\sum_{i=1}^{n} P_i \log P_i$$

THANKS!

智 能 时 代 的 新 运 维

CNUTCon 2017