AIOps Challenge 智能运维挑战赛

2021国际AIOps挑战赛决赛
暨AIOps创新高峰论坛

基于多源数据的云环境异常检测与定位

队伍名称：伊莉丝·逐星

答辩选手：侯传嘉

单位与团队成员简介

团队名称

伊莉丝·逐星

团队成员

侯传嘉
北京大学软件与微电子学院

贾统
北京大学软件与微电子学院

第一章节

题目与数据分析

题目与数据分析

数据特征

- Metrics(性能指标)

  数据平稳且特征显著，无周期性和季节性

- Trace(调用链span)

  调用链具备少量断裂特征，且具备调用时间异常

- Log(实时日志)

  数据有明显的异常关键字，无序列特征

- KPI(黄金指标)

  数据特征与具体系统负载均衡架构相关，总体特征不明显

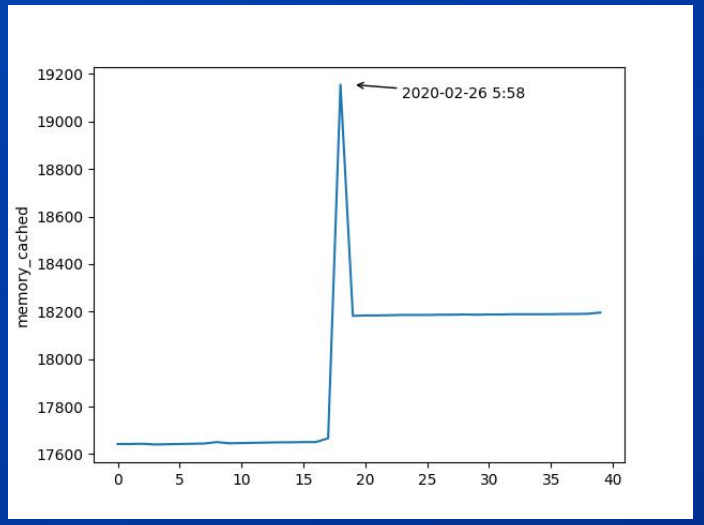

图1：System-A OOM故障的内存指标特征

57909	b5087b…	1614798568	Tomcat02	gc	4699112.530: [GC (Allocation Failure) 2021-03-04T03:09:28.519+0800: 469
57910	500aa8…	1614798577	Tomcat02	gc	4699121.031: [GC (CMS Initial Mark) [1 CMS-initial-mark: 3145425K(31457
57911	66a794…	1614798577	Tomcat02	gc	4699121.053: [CMS-concurrent-mark-start]
57912	e9244c…	1614798578	Tomcat02	gc	4699122.853: [CMS-concurrent-mark: 1.797/1.800 secs] [Times: user=5.44
57913	ce8031…	1614798578	Tomcat02	gc	4699122.853: [CMS-concurrent-preclean-start]
57914	fc2813…	1614798579	Tomcat02	gc	4699123.673: [Full GC (Allocation Failure) 2021-03-04T03:09:39.662+0800
57915	3bae72…	1614798589	Tomcat02	gc	4699134.003: [Full GC (Allocation Failure) 2021-03-04T03:09:49.992+0800
57916	c147c5…	1614798597	Tomcat02	gc	4699141.434: [GC (CMS Initial Mark) [1 CMS-initial-mark: 3145409K(31457
57917	acd8b7…	1614798597	Tomcat02	gc	4699141.450: [CMS-concurrent-mark-start]
57918	f3ec4b…	1614798597	Tomcat02	gc	4699141.743: [Full GC (Allocation Failure) 2021-03-04T03:09:57.731+0800
57919	e83ef5…	1614798607	Tomcat02	gc	4699151.285: [Full GC (Allocation Failure) 2021-03-04T03:10:07.274+0800
57920	a4974a…	1614798614	Tomcat02	gc	4699158.688: [GC (CMS Initial Mark) [1 CMS-initial-mark: 3145432K(31457
57921	a8371b…	1614798614	Tomcat02	gc	4699158.701: [CMS-concurrent-mark-start]
57922	8c4d0b…	1614798614	Tomcat02	gc	4699158.833: [Full GC (Allocation Failure) 2021-03-04T03:10:14.822+0800
57923	852d11…	1614798623	Tomcat02	gc	4699167.570: [Full GC (Allocation Failure) 2021-03-04T03:10:23.559+0800
57924	090593…	1614798630	Tomcat02	gc	4699174.581: [GC (CMS Initial Mark) [1 CMS-initial-mark: 3145432K(31457
57925	b16725…	1614798630	Tomcat02	gc	4699174.597: [CMS-concurrent-mark-start]
57926	1242e9…	1614798630	Tomcat02	gc	4699174.635: [Full GC (Allocation Failure) 2021-03-04T03:10:30.623+0800

图2：System-B Full GC的日志特征

第二章节

算法与架构设计

算法设计

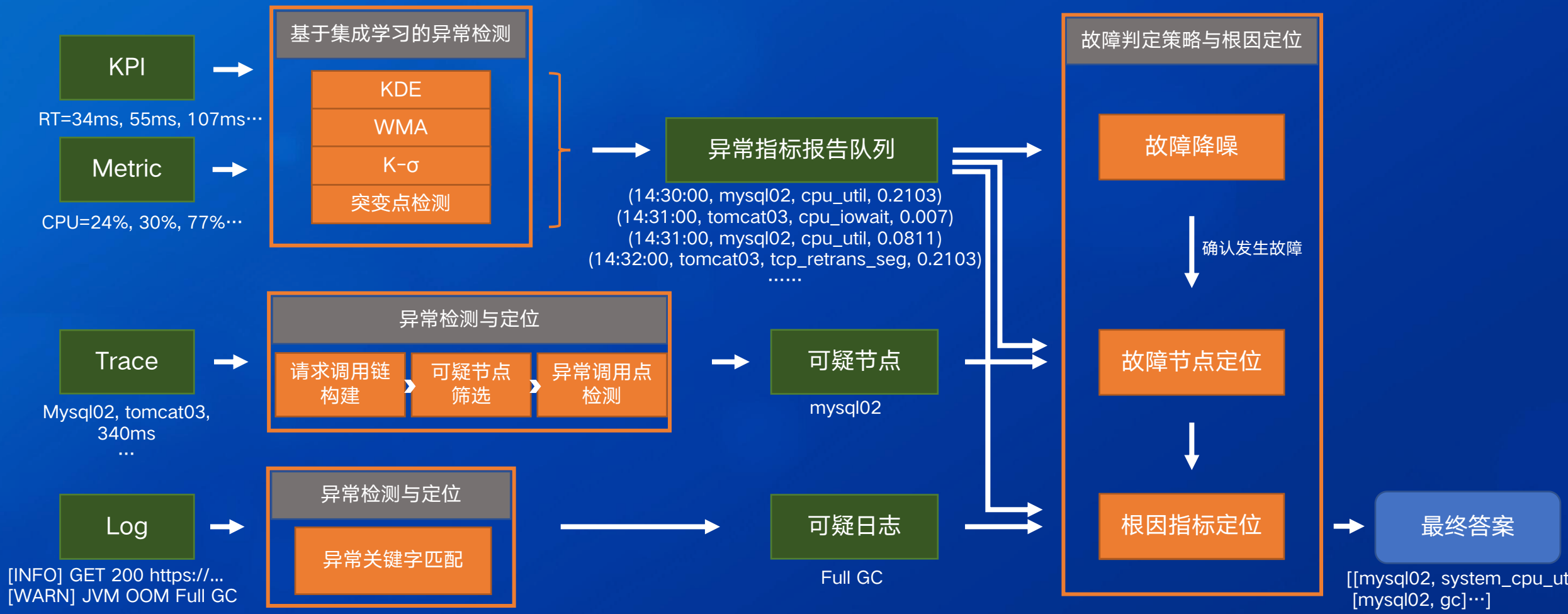

图3：算法流程设计

算法创新点：集成学习、多任务学习思想

Metric时间序列异常检测

集成学习，Bagging投票机制判定异常点

- 核密度估计(KDE)
  根据估计出的概率分布，判断数据点异常程度
- Weighted Moving Average/一次指数平滑法
  经典时间序列方法，针对平稳数据应用一次指数平滑
- K-Sigma检测
  基于统计量的异常检测，超过假设检验的合理范围则认为是异常
- 突变点检测

增量与全量训练机制

对于以上算法，维护一定时间长度内的历史数据（增量更新）
如果检测到异常点，则不更新模型
如果连续出现多个异常点（如多于15个），则认为发生了概念漂移，全量更新模型

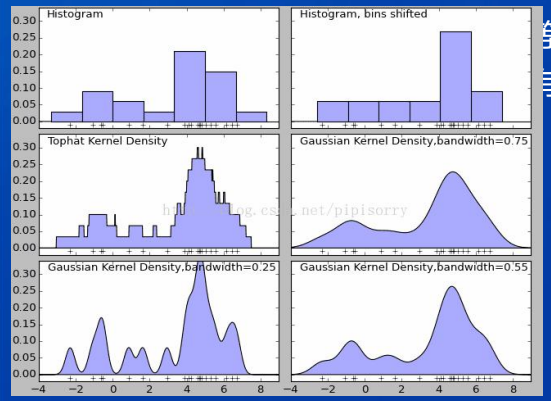

图4：核密度估计分布示例

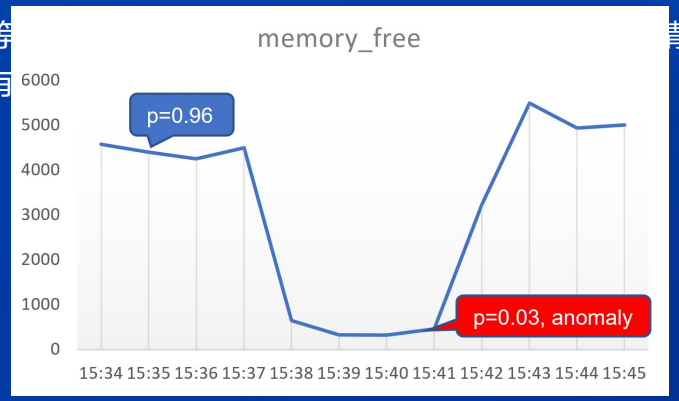

图5：利用核密度估计进行异常检测

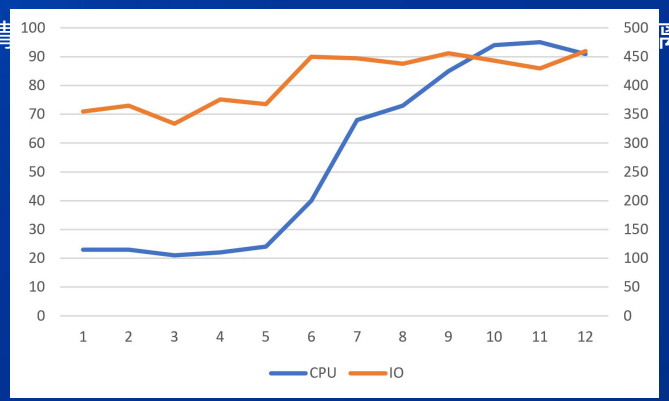

图6：相同的变化幅度对于不同指标的意义不同，需要结合历史波动考虑

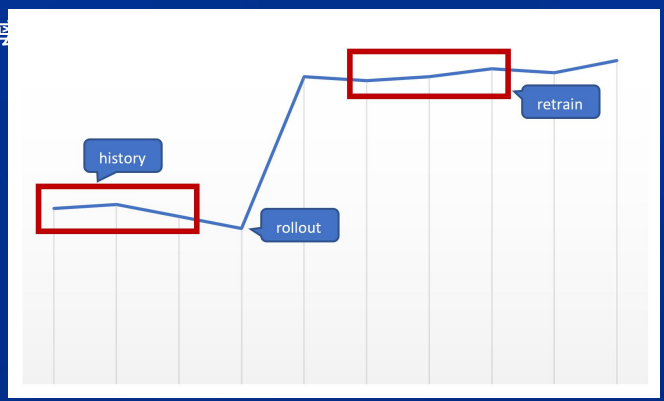

图7：模型的全量更新

基于Trace的异常检测与定位

请求追踪链路构建、追踪链路超时检测、异常位置决策

- 请求追踪链路构建

利用trace ID关联相同请求的追踪链路

- 追踪链路超时检测

1、计算所有节点的实际调用时间为节点的调用时间减其子节点的最大调用时间

2、设置阈值判断调用时间超时的节点

- 异常位置决策

每隔五分钟统计发生超时异常的节点，取出现异常最频繁的节点作为最终异常定位的结

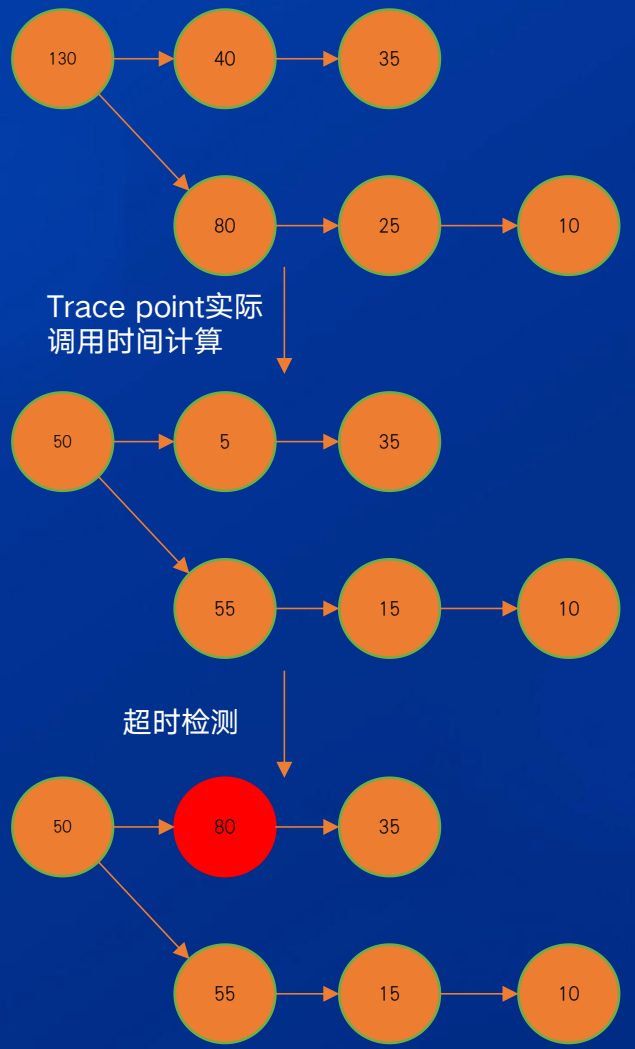

图8：追踪链路异常检测

基于日志的异常检测与定位

选用基于异常相关关键字的匹配，比赛数据的性质不适合于模板挖掘等高级算法

57909	b5087b…	1614798568	Tomcat02	gc	4699112.530:	[GC (Allocation Failure) 2021-03-04T03:09:28.519+0800: 469
57910	500aa8…	1614798577	Tomcat02	gc	4699121.031:	[GC (CMS Initial Mark) [1 CMS-initial-mark: 3145425K(31457
57911	66a794…	1614798577	Tomcat02	gc	4699121.053:	[CMS-concurrent-mark-start]
57912	e9244c…	1614798578	Tomcat02	gc	4699122.853:	[CMS-concurrent-mark: 1.797/1.800 secs] [Times: user=5.44
57913	ce8031…	1614798578	Tomcat02	gc	4699122.853:	[CMS-concurrent-preclean-start]
57914	fc2813…	1614798579	Tomcat02	gc	4699123.673:	[Full GC (Allocation Failure) 2021-03-04T03:09:39.662+0800
57915	3bae72…	1614798589	Tomcat02	gc	4699134.003:	[Full GC (Allocation Failure) 2021-03-04T03:09:49.992+0800
57916	c147c5…	1614798597	Tomcat02	gc	4699141.434:	[GC (CMS Initial Mark) [1 CMS-initial-mark: 3145409K(31457
57917	acd8b7…	1614798597	Tomcat02	gc	4699141.450:	[CMS-concurrent-mark-start]
57918	f3ec4b…	1614798597	Tomcat02	gc	4699141.743:	[Full GC (Allocation Failure) 2021-03-04T03:09:57.731+0800
57919	e83ef5…	1614798607	Tomcat02	gc	4699151.285:	[Full GC (Allocation Failure) 2021-03-04T03:10:07.274+0800
57920	a4974a…	1614798614	Tomcat02	gc	4699158.688:	[GC (CMS Initial Mark) [1 CMS-initial-mark: 3145432K(31457
57921	a8371b…	1614798614	Tomcat02	gc	4699158.701:	[CMS-concurrent-mark-start]
57922	8c4d0b…	1614798614	Tomcat02	gc	4699158.833:	[Full GC (Allocation Failure) 2021-03-04T03:10:14.822+0800
57923	852d11…	1614798623	Tomcat02	gc	4699167.570:	[Full GC (Allocation Failure) 2021-03-04T03:10:23.559+0800
57924	090593…	1614798630	Tomcat02	gc	4699174.581:	[GC (CMS Initial Mark) [1 CMS-initial-mark: 3145432K(31457
57925	b16725…	1614798630	Tomcat02	gc	4699174.597:	[CMS-concurrent-mark-start]
57926	1242e9…	1614798630	Tomcat02	gc	4699174.635:	[Full GC (Allocation Failure) 2021-03-04T03:10:30.623+0800

图9：A系统日志的典型异常关键字

根因定位的提交策略

决策模块读取异常队列的状态，根据一组策略决定是否发生了故障（提交答案）

- 异常队列的长度和时间跨度大于阈值
  - 短时间内的异常报告**突增(Burst)**很可能表征了重要故障的发生
- 异常队列**保持连续**
- 按照时间为队列中的待考察异常报告赋予**衰变因子**，定时舍弃
- 根据队列内异常报告所属节点占比与Trace检测的结果**加权**进行根因定位

答案选择

根据异常报告的Metric**指标类型比例**判定故障类型

对故障类型相对应的指标，进行二次检测，生成最终的答案

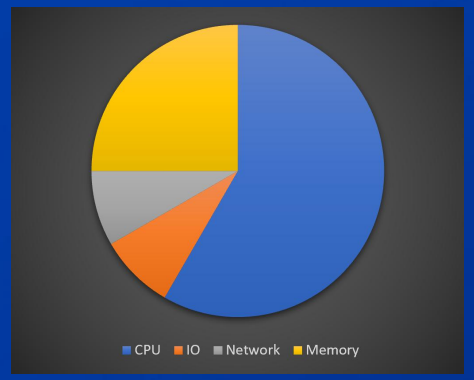

图12：根据异常指标比例判定故障类型

$< Timestamp, CMDB\_ID, Metric\ Name, value >$

异常报告四元组，队列由多个报告组成

图10：根据异常队列特性确定故障的发生

$$R = \mu R_{qual} + R_{trace}$$

加权得分最高者为故障根因节点

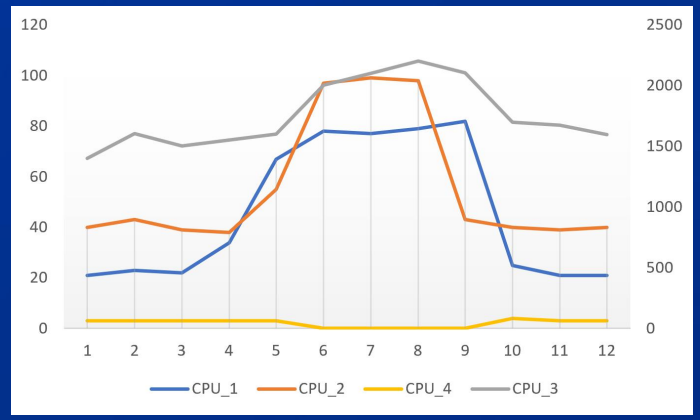

图11：不同根因指标的实际含义、取值范围、分布函数和异常幅度均不同；为了提高召回率，可以对属于同一故障类型的可疑指标进行二次检测

实现

基于Python语言，代码：800+行

- 逻辑轻巧，使用资源少，利于落地
- 异构数据源独立线程处理，降低相互影响
- 所有数据利用内存交互，降低延迟
- 线程保活策略，提升容错性

配置设计

- 采用JSON配置文件区分不同系统(A/B)
- 无Magic Number，全部参数配置化
- 指标名称类别，关键字可调
- 子功能可独立开启/关闭，互不影响

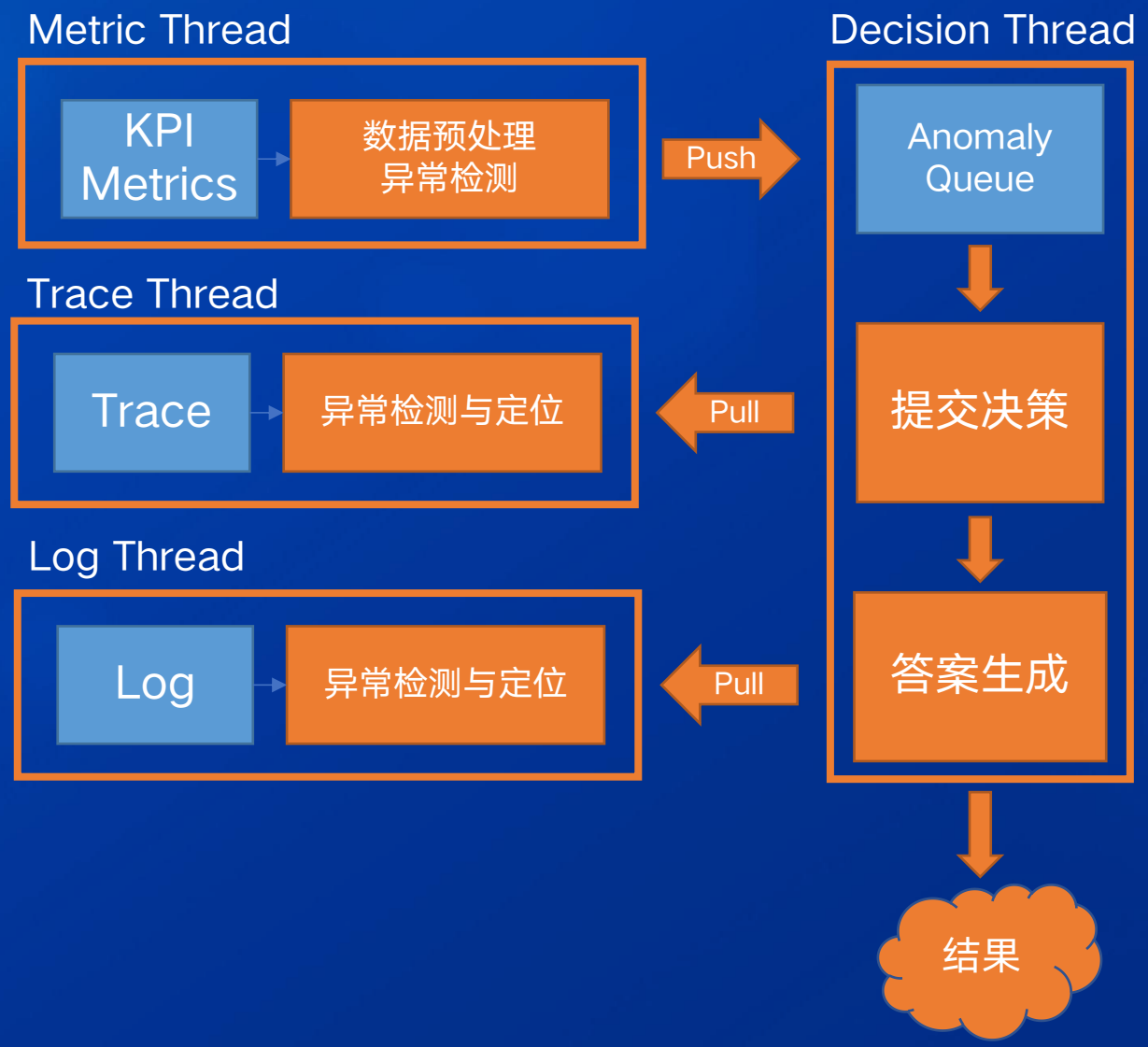

图13：系统架构设计

第三章节

总结与思考

总结与分析

比赛总结

- 预赛复赛总分均位于第7名；算法对A系统十分有效
- 尝试多种深度神经网络、基于日志模板的异常检测模型构建方法后，选取了目前的方案
- 感谢主办方提供宝贵的真实数据和计算资源

可以改进的地方

1. 对Trace和KPI的利用还不够深入
2. 时间所限，很多算法参数未经过优化，有提升空间
3. 异常队列的派生特征可以进一步挖掘
4. 网络类故障的感知不够灵敏

思考

1. 怎样进一步提升异常检测和故障诊断算法的通用性和可扩展性？

   自适应、自更新、自演化算法设计

2. 怎样解决有标注运维数据不足的问题？

   无监督学习/主动学习/半监督学习/迁移学习

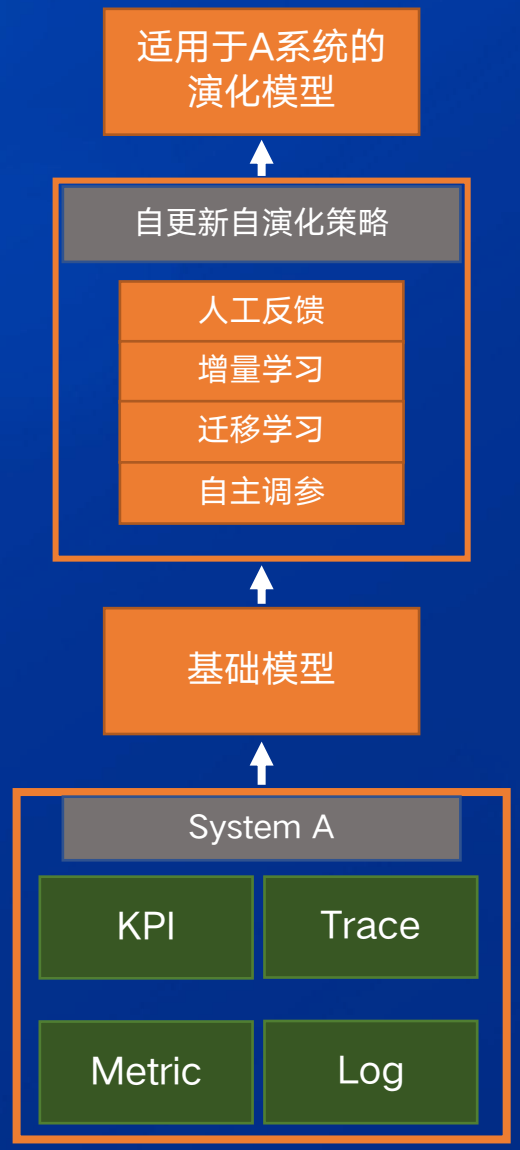

图14：自演化自适应的检测模型

Q&A

2021国际AIOps挑战赛决赛暨AIOps创新高峰论坛

THANKS

谢 谢 观 看

第一届国际互联网产业科技创新大会暨互联网创新产品展览会

The First International Internet Industry Science And Technology Innovation Conference & Internet Innovation Product Exhibition