

# 源于社区 服务社区

 中国DevOps社区峰会 2023 · 广州

## 用可观测性之眼洞悉复杂生产系统

刘征、中国DevOps社区





# 刘征

## 中国DevOps社区-理事长

- 《DevOps实践指南》译者
- 《Google SRE 工作手册》译者
- 开源软件爱好者





# 目录

- 1 可观测性概念正本清源
- 2 循序渐进落地可观测性
- 3 持续改进和评估
- 4 问答





# 可观测性概念正本清源

- 术语定义和来历
- 当前时代背景下的定义
- 可观测性与 DevOps 的关系
- 可观测性与 SRE 的关系



# 没有人能忍受可怕的索伦之眼



眼睛能看到一切，眼睛也能影响它所看到的一切。被它或他盯上就等於受到索倫的影響。



可观测性：“度量一切，影响所有正在发生的问题，是生产环境不可或缺的稳定性的保障。”





可观测性的定义是什么？

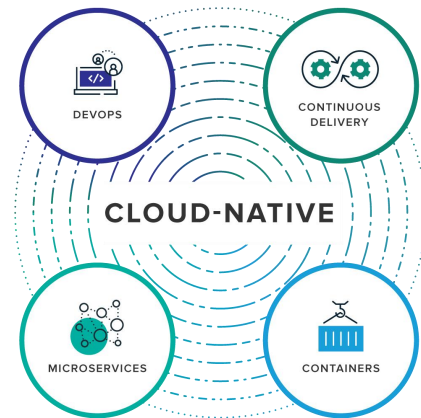
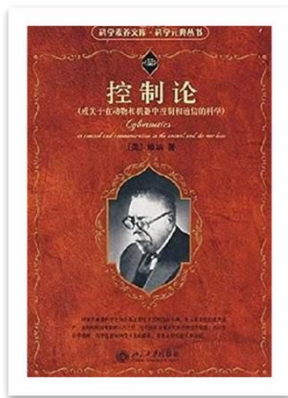
Observability  
o11y





# 源于数学&机械工程学科领域的《控制论》

- “可观测性”于1960年，在《控制论》中被首次提出。
- 定义：指系统可以由其外部输出推断其内部状态的程度。
- 特点：用已知的输入输出推断机械内部的工作状态。
- 将会不太适用于“虚拟的软件系统”
- 可观测性工程将开启你编写软件代码并与生产环境交互的全新模式。
- 未知的用户行为，未知的生产环境现象





# 各种厂商的解读

- 套用控制论，强调某些关键点
- 发展创新，靠近最新技术



# 系统的可观测性：应该具备的三大基本特征

## 度量能力

- 无论系统中发生多么费解的现象
- 它帮助你更好地理解 and 解释系统当前的状态



## 探索分析

- 能够在各类状态数据的所有维度和组合之间进行关联分析
- 无预定调试&排查模式和路径

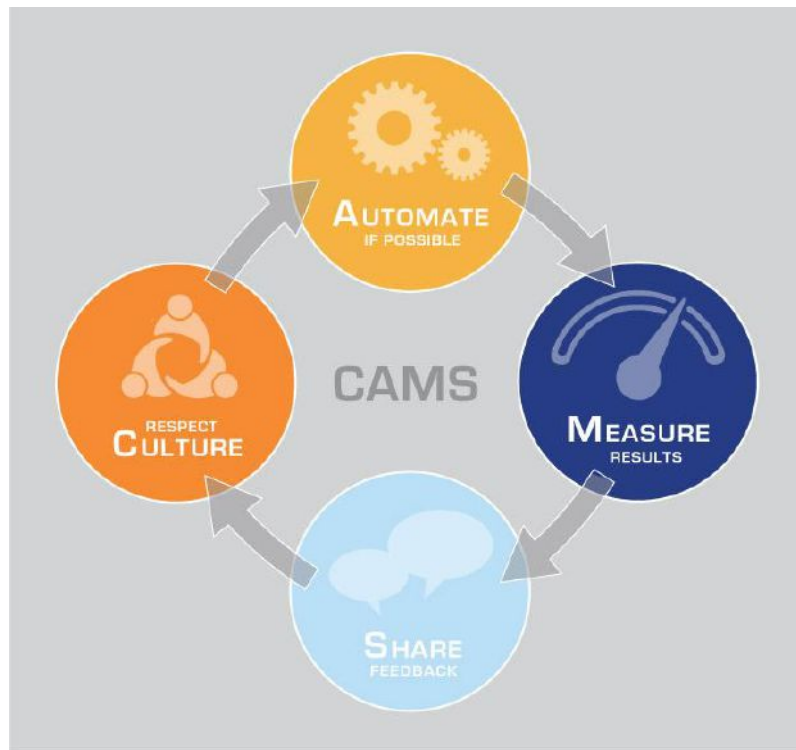
## 按需改变

- 最好是不需要改变原有代码
- 也能随心所欲的按需埋点洞察

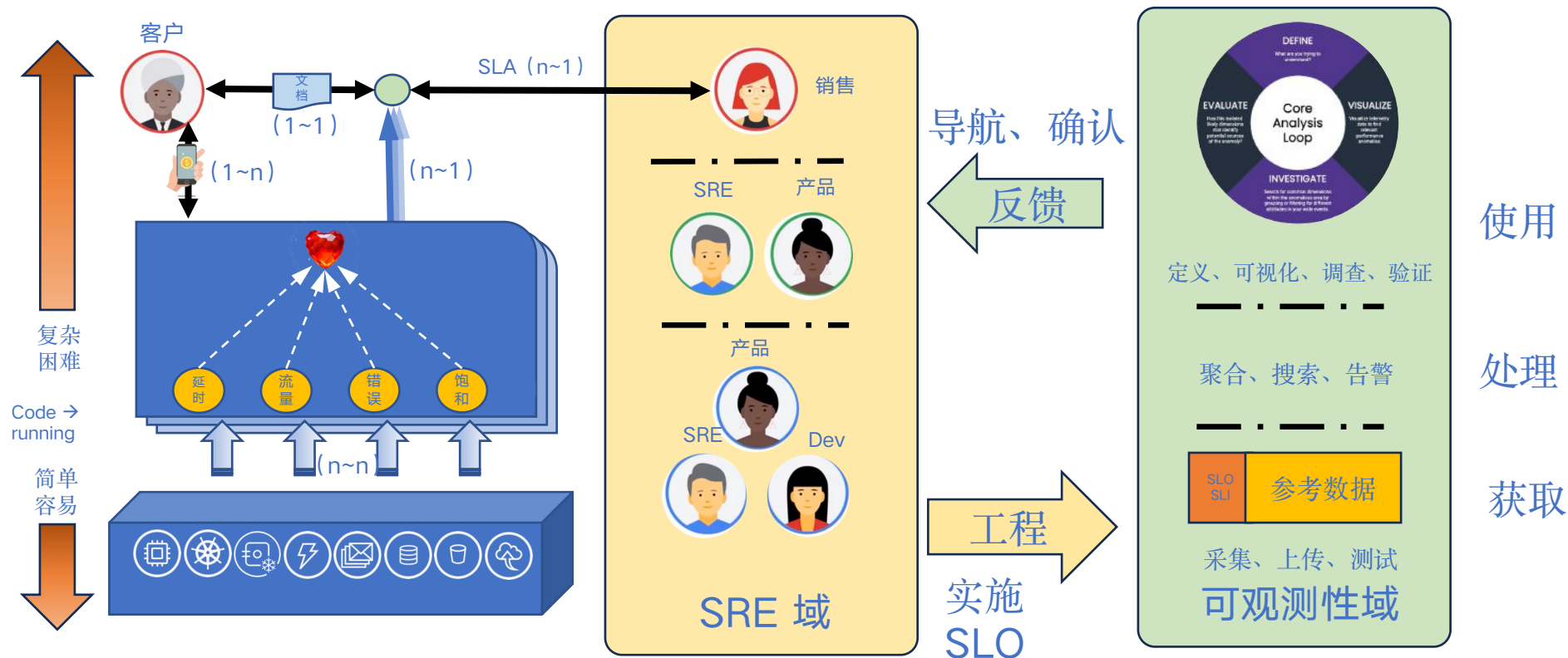


# 可观测性与 DevOps 的关系

- 持续验证、功能开关、灰度发布等
- 自动化和持续交付
- 跨团队协作、事后分享
- 故障排除和持续改进，无指责的事后回顾



# 可观测性与 SRE 的关系





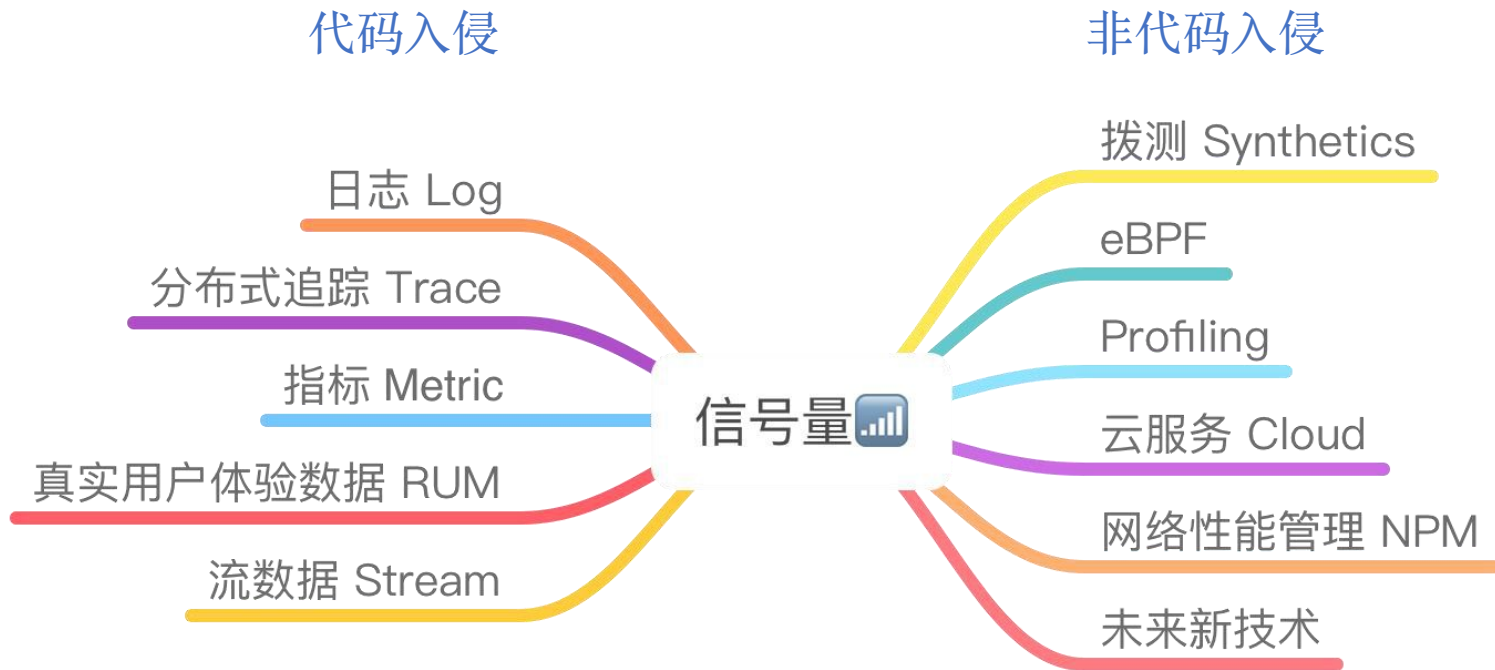
## 骤循序渐进落地可观测性

- 采集
- 处理
- 使用





# 可观测性数据来源





# 可观测性信号量 $\neq$ 可观测性



代码&内在

手工埋点

Log  
Metric  
Trace  
RUM  
Stream

OS & 集成

框架埋点

Log  
Trace  
RUM  
eBPF  
Profiling

环境&外在

环境采集

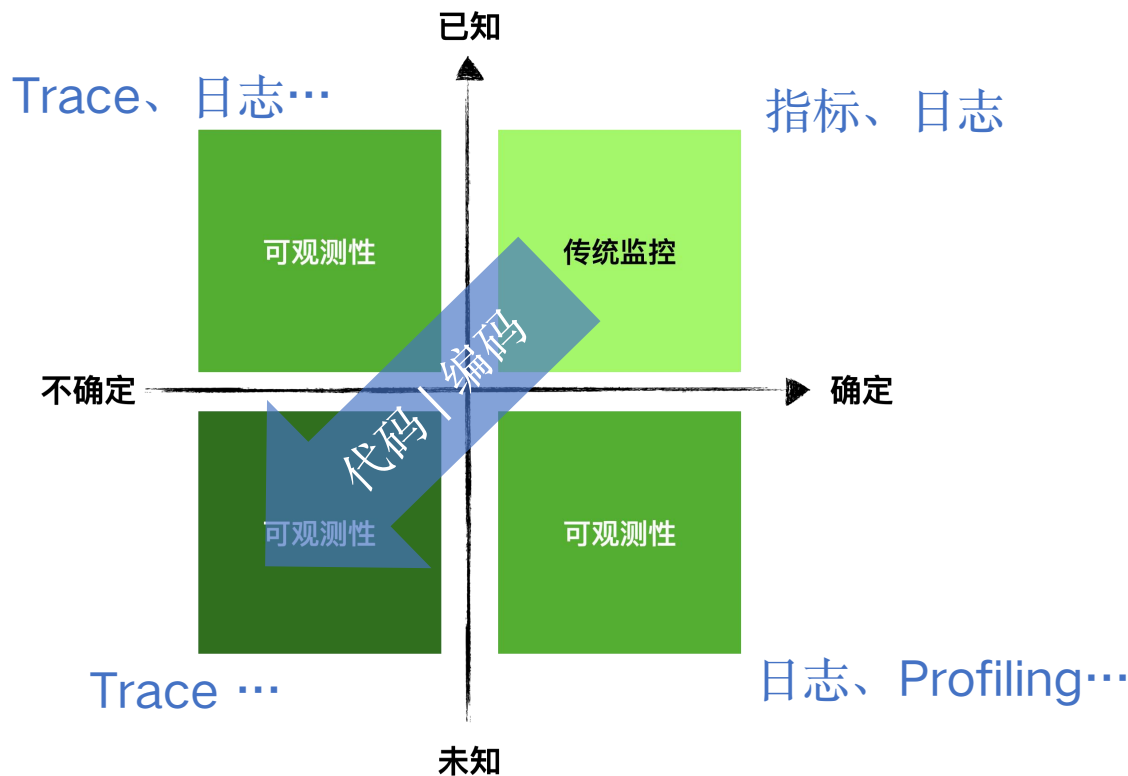
Log  
Metric  
Synthetics  
Cloud  
NPM





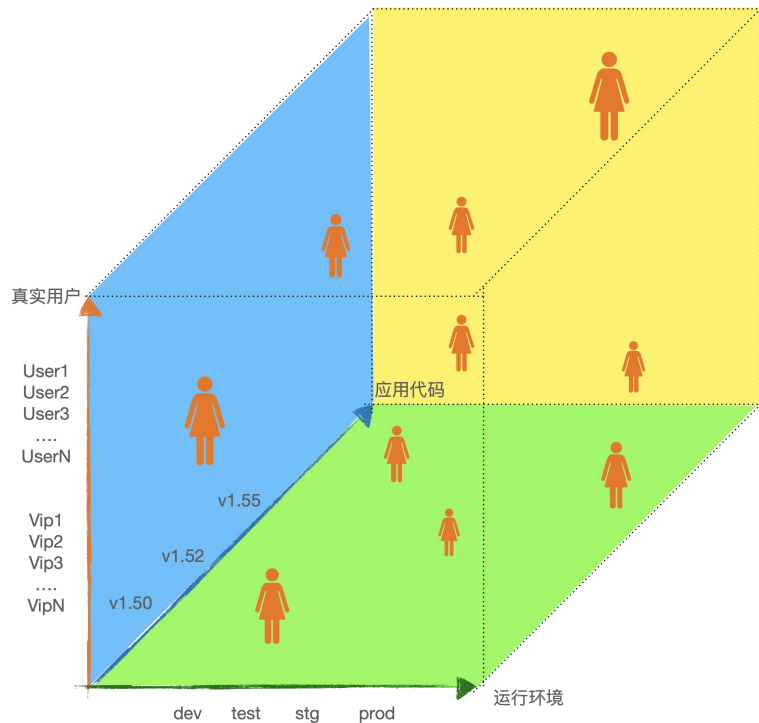


# 数据服务于：问题的解决，四大问题领域





# 可观测性数据意义最大化：用户 x 环境 x 代码 ??

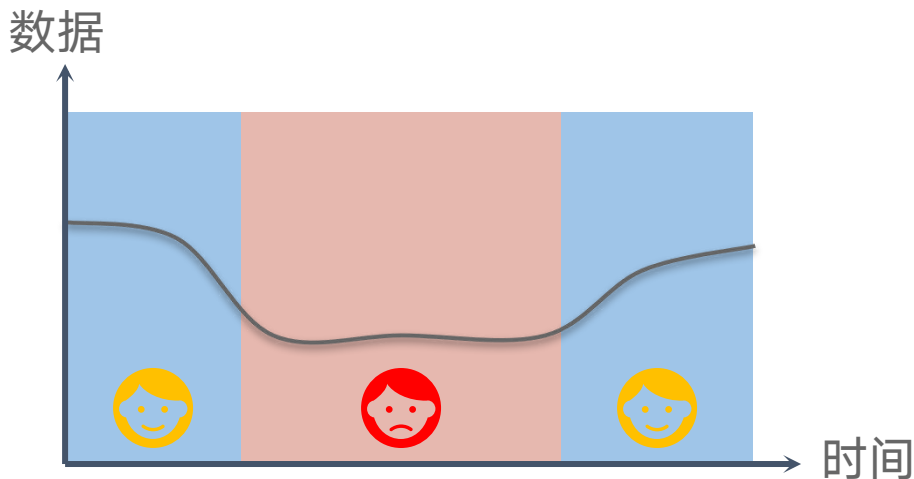


在这三个维度的交叉点上获取：  
即时、准确和清晰的洞见。



# 可观测性数据的底层细节

- 用可观测数据度量和感知应用系统的状态，以及状态的变化过程
- 可观测性数据的两个维度“基数”和“维度”。



# 可观测性的数据结构

基数

country	year	cases	population
Afghanistan	1999	2666	19987071
Afghanistan	2000	2666	20095360
Brazil	1999	31737	172006362
Brazil	2000	80488	174004898
China	1999	212258	1272015272
China	2000	213766	128042583

维度

country	year	cases	population
Afghanistan	1999	2666	19987071
Afghanistan	2000	2666	20095360
Brazil	1999	31737	172006362
Brazil	2000	80488	174004898
China	1999	212258	1272015272
China	2000	213766	128042583

数值

country	year	cases	population
Afghanistan	99	75	19987071
Afghanistan	00	66	20095360
Brazil	99	737	172006362
Brazil	00	488	174004898
China	99	2258	1272015272
China	00	766	128042583

- 高基数字段：用户 ID、UUID、购物车 ID、请求 ID、容器 ID、主机名（弹性、不可变架构）、Pod ID 等等。
- 低基数字段：操作系统类型、云提供商、可用区、主机架构（AMD/arm）等等

- 高维度可观测性数据是一条结构化数据，代表一次事件，亦或是一个状态，它的“宽度”可以高达上千个键值对（字段），事件越宽所携带的上线文信息就越丰富。高维度数据的作用是用来回答：到底发生了什么？

- Trace - 是以‘追踪 ID’为线索的，一组具有调用逻辑关系的Span的集合。
- 讲述了：前端A 同时调用了缓存服务 B 和数据库服务 C 这样一次事件



# 在产品团队中推广可观测性

## 1. 应用可观测性驱动开发

- 了解和掌握 OTel&商业项目
- 使用自动化埋点
- 左移：尽早的实施自定义埋点
- 统一设计规划集中的数据后台

## 2. 实施基于 SLO 的告警

- 将有限的精力投入到有的放矢的 SLO 告警排查和处理中

## 3. 提高代码可观测性

- 是否按期望运行？与前一个版本相比如何？用户更喜欢吗？有没有发生新的异常？



# 统一数据模型：标准化、互操作性、简化开发和集成



## Elastic Common Schema (ECS)

- 背景：由 Elastic 推动的 Elastic Common Schema (ECS) 是一种用于标准化日志和事件数据的数据模型。它旨在消除在不同数据源和工具之间对字段和术语的混淆，使得数据更易于理解和可操作。
- 意义：ECS 的标准化使得日志、指标和其他可观测性数据的结构在整个生态系统中保持一致。这有助于不同的日志收集器、监控工具和安全信息与事件管理 (SIEM) 系统之间的集成，简化了数据分析和查询。

捐献

## CNCF Observability Metrics (COM)

- 背景：CNCF Observability Metrics (COM) 是由云原生计算基金会 (CNCF) 推动的可观测性数据模型。COM 旨在提供一种统一的方法，以在云原生环境中收集和表示指标数据。
- 意义：COM 的目标是为云原生应用程序和基础设施提供一个通用的度量标准。通过定义共同的指标和度量单位，COM 有助于确保不同的监控和度量工具之间的兼容性，从而简化了监控、自动化和调试任务。



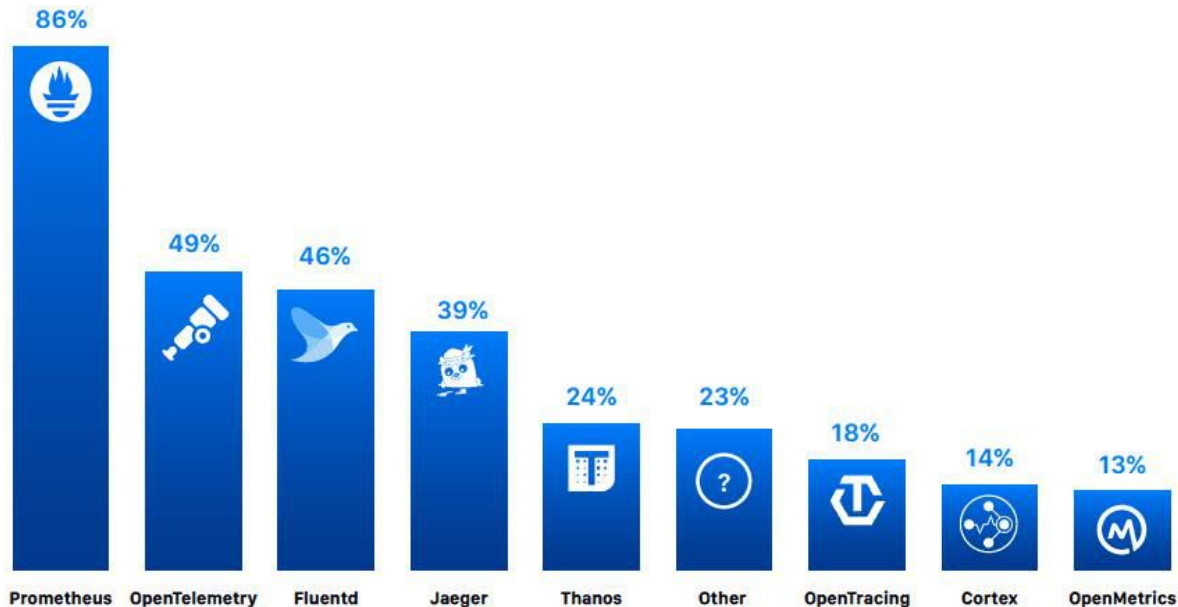
CLOUD NATIVE  
COMPUTING FOUNDATION





# Cloud Native Observability Microsurvey 2022- 1

Which, if any, of the following projects do you use for observability?

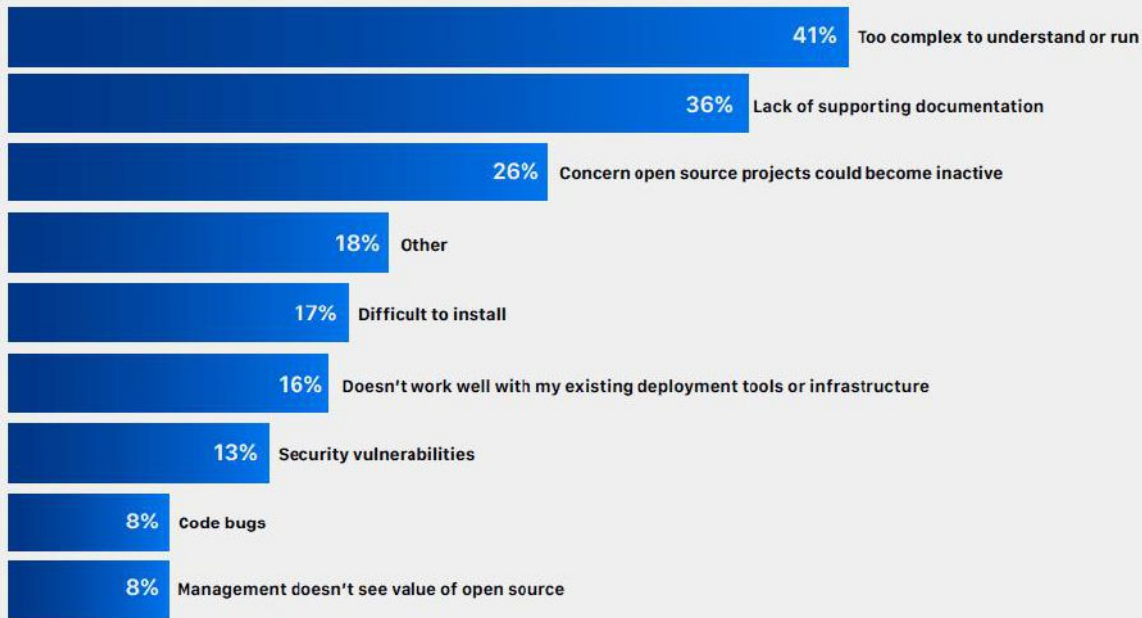






# Cloud Native Observability Microsurvey 2022-2

What practical, technical, or cultural challenges have you experienced or do you foresee using these projects?





# 高效存储可观测性数据

## 挑战：一写多读，在高基数和高维度的任意组合下高速搜索

- **时间序列数据库：高基数导致时间线爆炸**
  - InfluxDB：专门用于存储和查询时间序列数据的开源数据库。
  - Prometheus：开源的系统监控和警报工具，使用自身的时间序列数据库。
  - Graphite：开源的可视化工具，使用时间序列数据库来存储性能数据。
- **日志存储：不是为Tracing 优化而设计的**
  - Elasticsearch：用于搜索和分析大量数据的分布式开源搜索引擎，通常与Logstash和Kibana一起使用（ELK堆栈）。
  - Splunk：商业日志管理工具，用于搜索、监视和分析机器生成的大量数据。
- **关系型数据库：传统关系型数据库不适合**
  - MySQL、PostgreSQL、Oracle：传统的关系型数据库，也可以用于存储监控数据。
- **列式存储：未来可期的存储项目ClickHouse，但未对o11y优化**
  - Apache Cassandra：高度可扩展的分布式数据库系统，适用于大规模存储和处理数据。
  - ClickHouse：列式数据库管理系统，用于高性能分析型工作负载。
- **对象存储：延迟太高**
  - Amazon S3、Google Cloud Storage、Azure Blob Storage：云存储服务，适用于存储大量监控数据。
- **内存数据库：规模不够**
  - Redis：开源的内存键值存储系统，可用于缓存和实时数据分析。
- **分布式存储系统：查询延迟高**
  - Hadoop HDFS：分布式文件系统，可用于存储大规模的监控数据。





# 运算和预处理可观测性的考量

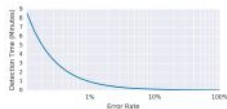


- 实时性：
  - 数据的新鲜度 \* 采集速度
- 常用运算：
  - P99, P95, P90, 切片, 平均值
- 异常检测：
  - 当前 vs. 基线
- AI 推理和判断
  - 自动驾驶的实现前提：交通环境和规则是确定性的
  - AIOps 除非监督异常行为预判外，不确定是云环境&服务运行常态

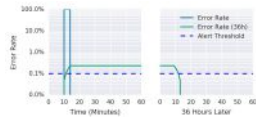


# 基于 SLO 的告警逻辑

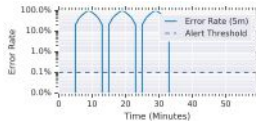
1 一触即发



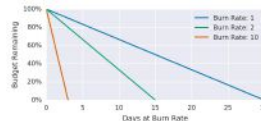
2 延长告警时间窗口



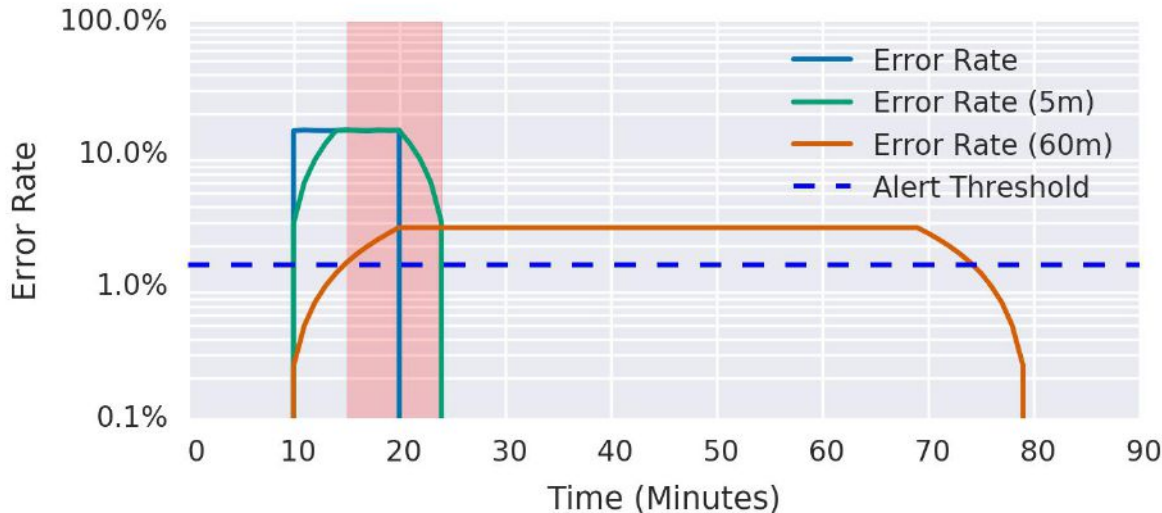
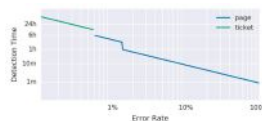
3 延迟触发前持续时间



4 单燃烧率触发



5 多燃烧率触发



## 6 推荐的告警逻辑

举例：SLO 为 99.9%的接口错误率

- 多时间窗口 (5m~3d)
- 多燃烧率 (1~14.4)
- 多告警级别 (短信、工单)

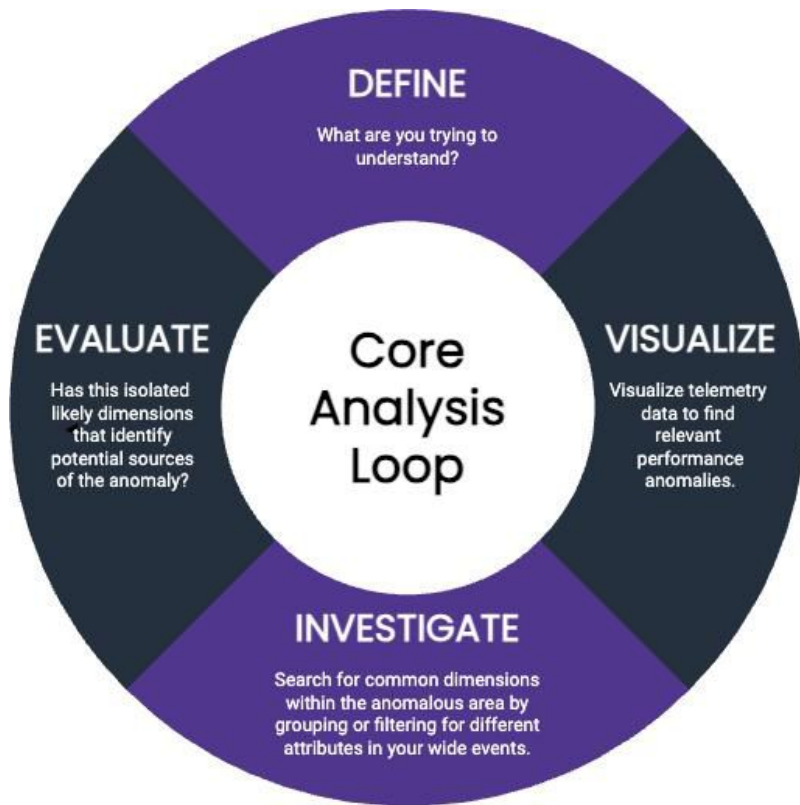
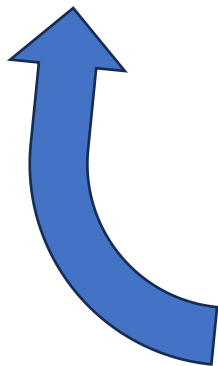
详见：《Google SRE 工作手册》



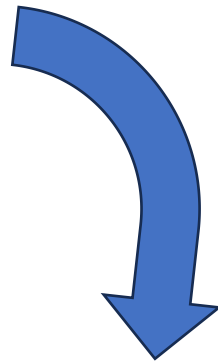


# 运维界的第一性原理：核心分析循环

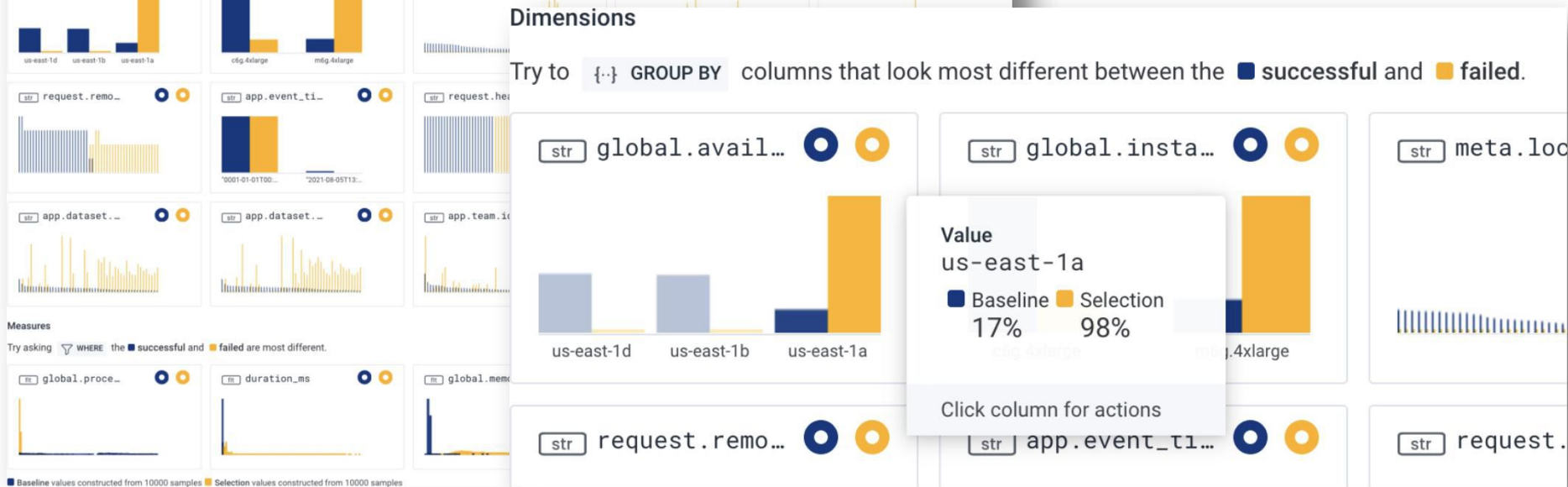
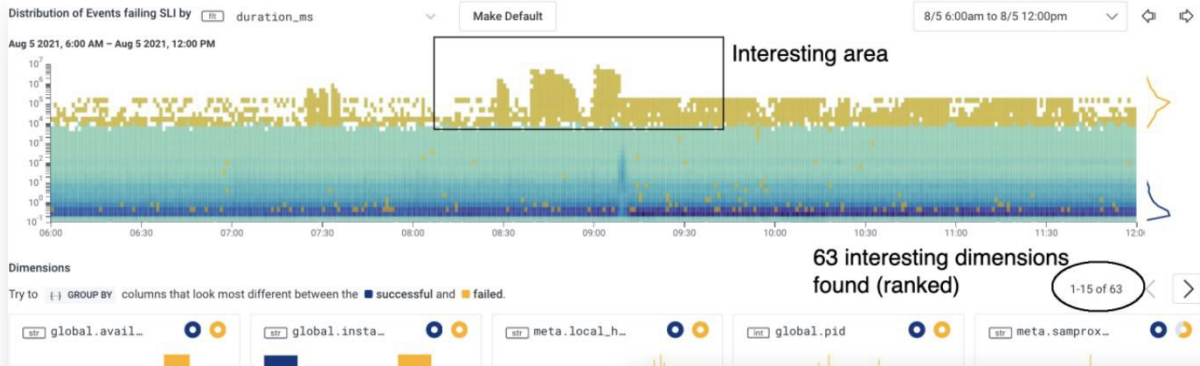
- 被动干预：  
告警事件触发



- 主动干预：  
系统监控巡检









# 可观测性持续改进和评估

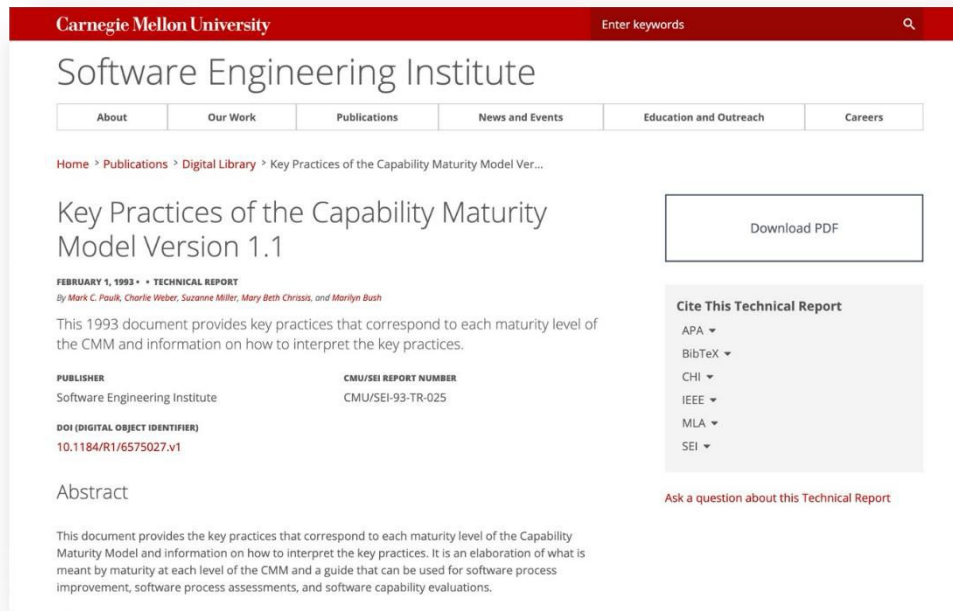
- 能力成熟度模型的作用和意义
- 可参考的两个模型
- 在组织内使用可观测性成熟度模型





# 参考模型的作用和意义

- 提供起点，批判依据，客观的度量和识别目标。
- 模型不会适用于所有企业，有待人的适配，模型本身也需要不断发展
- 目标：
  - 系统和工程师的生活均可持续发展
  - 提高客户满意度实现企业价值





# 可参考的能力模型： Liz Fong-Jones 2019 InfoQ 文章

## 在复杂系统中可持续地运维卓越的生产系统



有抵御系统故障的可靠性



能持续交付高质量代码



可管理复杂度和技术债



可按预定节奏发布软件



能清晰理解用户的行为



# 在组织内使用可观测性成熟度模型

- 用于度量团队表现的优缺点
- 从对业绩具有较大影响的应用系统的优化开始
- 将可观测性能力和其它能力交织在一起
- 授权给特定的变革负责人，并得到管理层的支持和重视

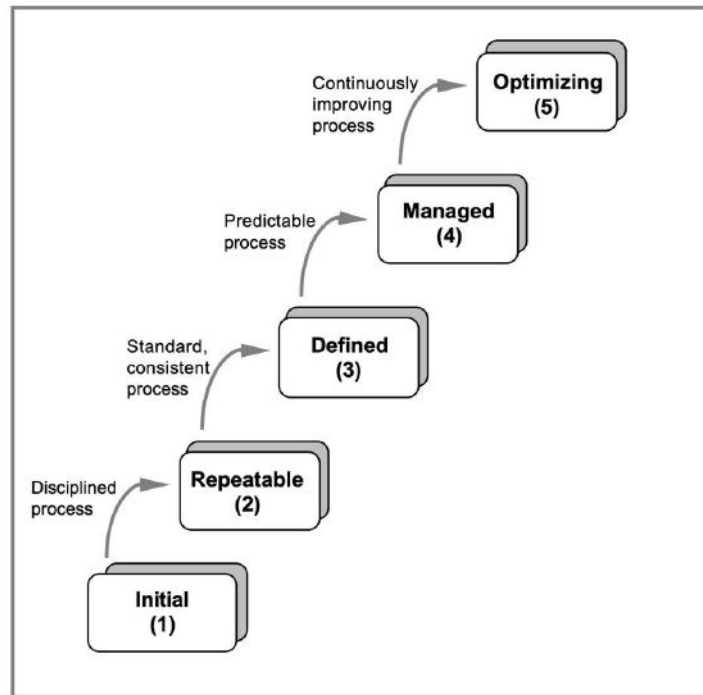


Figure 2.2 The Five Levels of Software Process Maturity

# 源于社区 服务社区

## THANKS!

个人微信号



微信公众号

