



# 全观察性智能监控解决方案

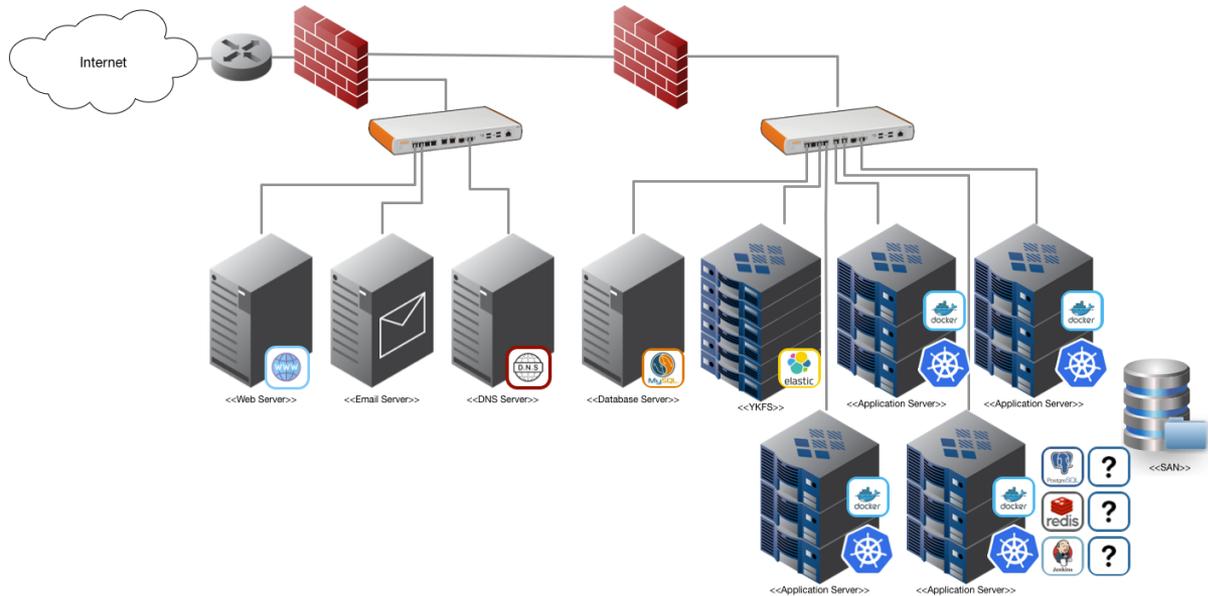
---

Jerry (朱杰)  
Elastic 架构师



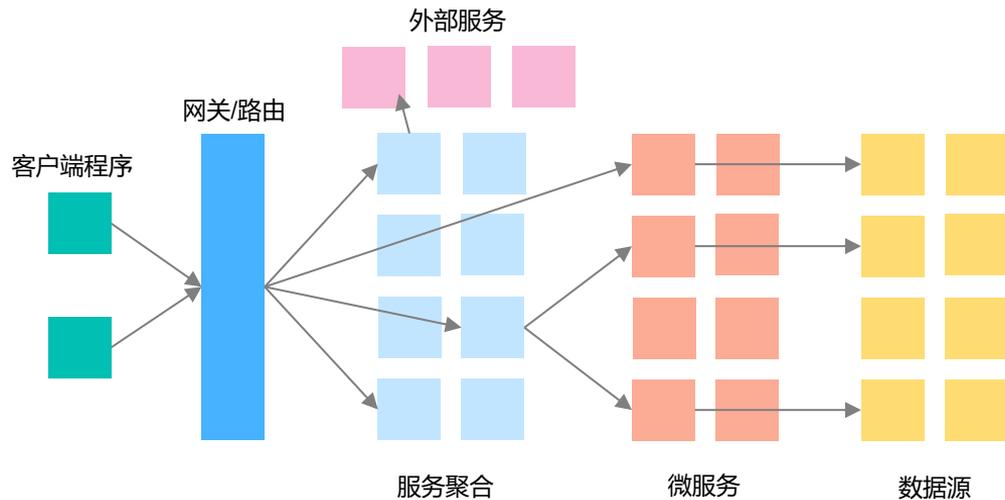
# 当今运维监控的挑战 – 复杂的基础设施

- 基础架构层面是复杂的
- 多种服务器
- 多种网络设备
- 多种安全设备
- 多种存储设备



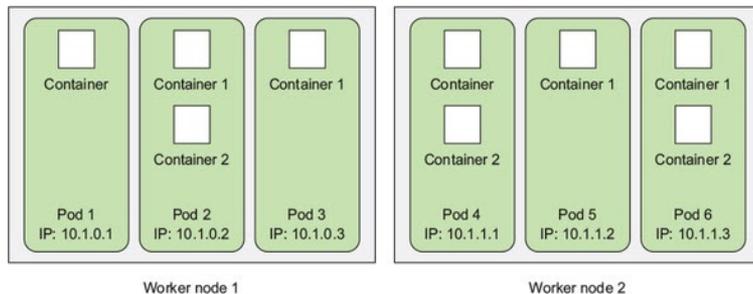
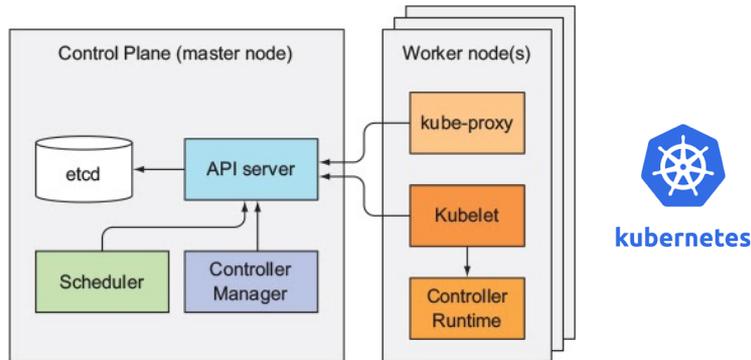
# 当今运维监控的挑战 – 服务的分布化

- 程序设计层面微服务变成主流
- 服务的层次比较多
- 各层之间的调用错综复杂



# 当今运维监控的挑战 – 服务编排

- 容器化是服务编排的主流趋势
- 程序分布在多个容器中



# 软硬件演变使得监控变得更加复杂



硬件层：虚拟化 -> 容器化

软件层：单机 -> N层 -> SOA -> 微服务

监控变得更加复杂

# 传统的监控解决方案

运维: Log 监控



**Log**

Web Logs  
App Logs  
Database Logs  
Container Logs

运维: Infra监控



**Metrics**

Container Metrics  
Host Metrics  
Database Metrics  
Network Metrics  
Storage Metrics

开发团队



**APM**

Real User Monitoring  
Txn Perf Monitoring  
Distributed Tracing

运维: Service监控

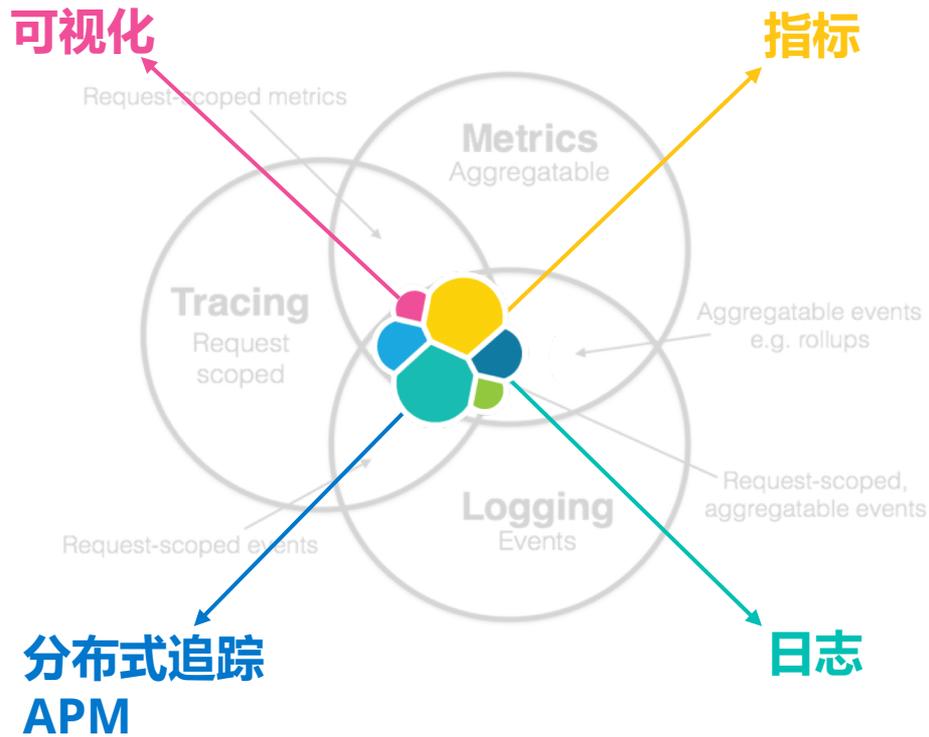


**Uptime**

Uptime  
Response Time

# 传统运维监控的不足

- 数据孤岛，分散在不同部门，分析排查故障困难
- 多个厂商的多种工具，无法自动化统一分析
- 故障是立体的，日志 指标 APM都只能看到一方面的可观察性
- 只是收集，没有做到真正分析，不能发挥出大数据的价值



# 智能运维成熟度阶梯

	数据收集	数据准备	数据分析
高级	日志 指标 APM	大量结构化	人工分析, 规则告警, 机器学习, 关联分析
中级	日志 指标	少量结构化	人工分析, 规则告警
初级	日志集中化	不抽取	人工分析, 仅仅全文搜索

# Elastic的解决方案

开发 & 运维团队



日志数据

指标数据

APM数据

Uptime数据

Web日志  
App日志  
数据库日志  
容器日志

容器指标  
主机指标  
数据库指标  
网络指标  
存储指标

用户行为监控  
交易性能监控  
分布式追踪

Uptime  
响应时间

Elastic Common Schema

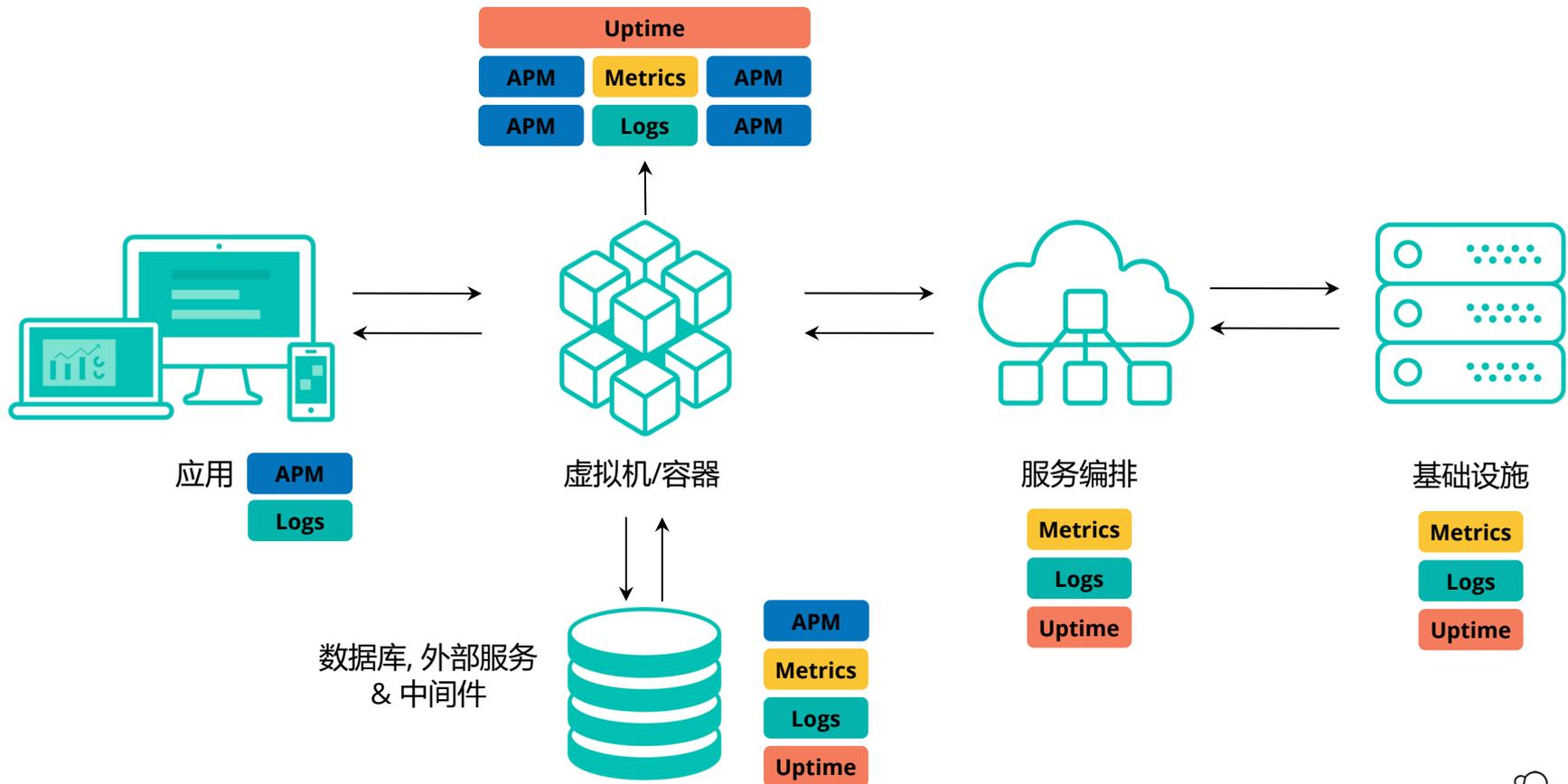


kibana



elasticsearch

# 不同的层需要不同类型的监控



# 实现全方位可观察性的难点

