容器服务助力云原生稳定性

汤志敏

阿里云智能资深技术专家

云原生场景的稳定性挑战和机遇

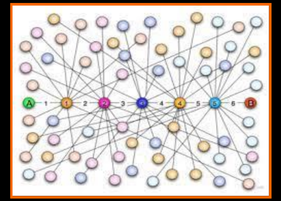
- 微服务应用
- Sidecar应用
- Kubernetes调度
- 容器网络、容器OS
- 操作系统和底层网络
- 虚拟化和硬件

更多的不确定性

开源软件、多云环境、弹性环境找不到现场

更大的规模

规模爆炸、可观测指标爆炸



如何降低系统复杂度？

- 声明式和不可变架构
- 智能化故障预防和定位
- 智能化节点托管

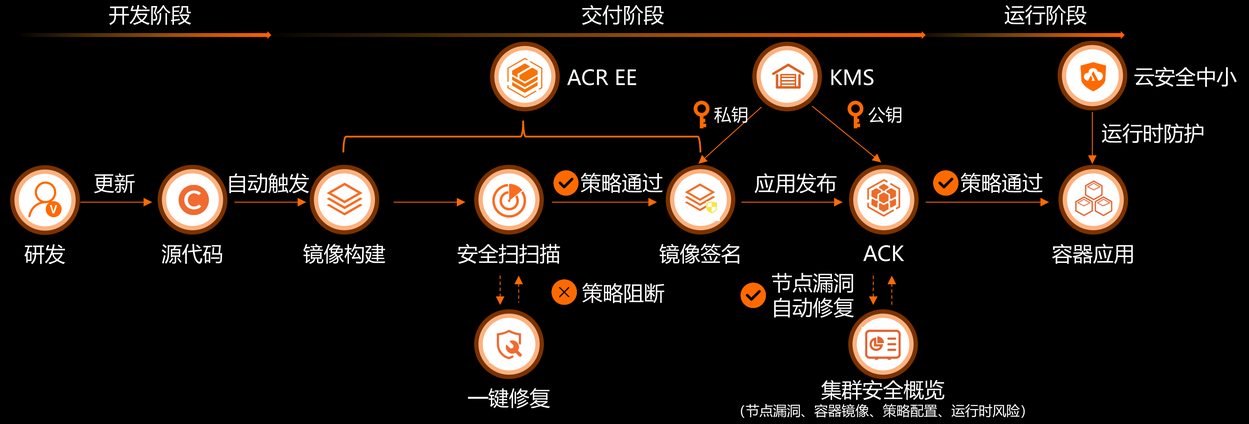
声明式和不可变架构

Declarative　　Immutable

加速问题定位、减少排查路径、可追溯

不可变镜像层	安全软件供应链	镜像不可变TAG/镜像签名
声明式可观测性	全景可观测性	Prometheus /OpenTelemetry/ebpf
声明式应用模型	统一应用模型	Helm Charts/OCI Artifacts/OAM
声明式节点管理	节点池管理	托管节点池/容器优化OS lifseaOS
基础设施即代码	基础设施层	Terraform/ROS

安全可信软件供应链



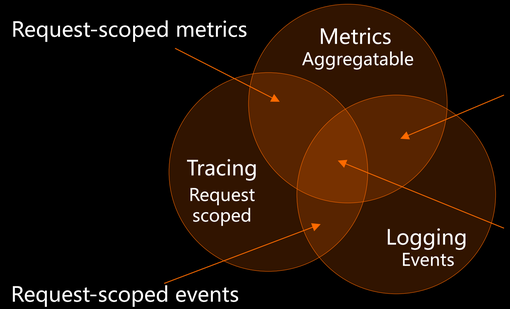
salesforce

客户使用云原生 DevSecOps 能力，半年内实现万次镜像扫描，千次风险镜像拦截阻断，千次加签/验签安全交付。

基于全自动化软件供应链安全流程，应用安全交付效率提升 3 倍。

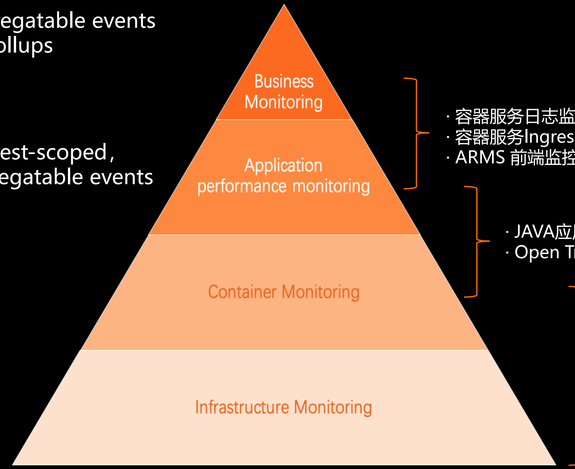
（以上数据为客户业务场景应用结果）

容器全景可观测体系



From blog of Peter Bourgon

· 容器服务事件中心
· 容器服务报警中心
· Kubernetes监控
（无侵入、架构拓扑感知）



· 容器服务日志监控
· 容器服务Ingress Dashboard
· ARMS 前端监控

· JAVA应用监控
· Open Tracing/Open Telemetry（ARMS APM）

· 阿里云Prometheus
· 云监控 基础资源监控
· 操作系统内核层
· 虚拟化层监控

Prometheus For ACK Pro

Prometheus For ACK Pro包含一组符合关联分析逻辑且可交互的大盘，包含

- 全局资源总览、节点总览
- Kubernetes核心托管管控（APIServer、etcd、scheduler）
- 集群事件分析
- eBPF无侵入式应用指标，系统指标，网络指标

容器AIOps套件-故障预防与定位

AIOps for Kubernetes Cluster: Fault Prevention and Problem Determination

10年大规模容器运维经验沉淀，自动化诊断覆盖90%的问题场景

全栈巡检	升级检查	智能诊断
集群健康度巡查	版本兼容性评估	集群事件流分析
应用可用性巡检	配置冲突检测	网络仿真与诊断
平台安全性巡检	业务影响评估	OS内核指标分析

专家系统+AI算法

容器服务 – ACK集群

公有云 | IDC

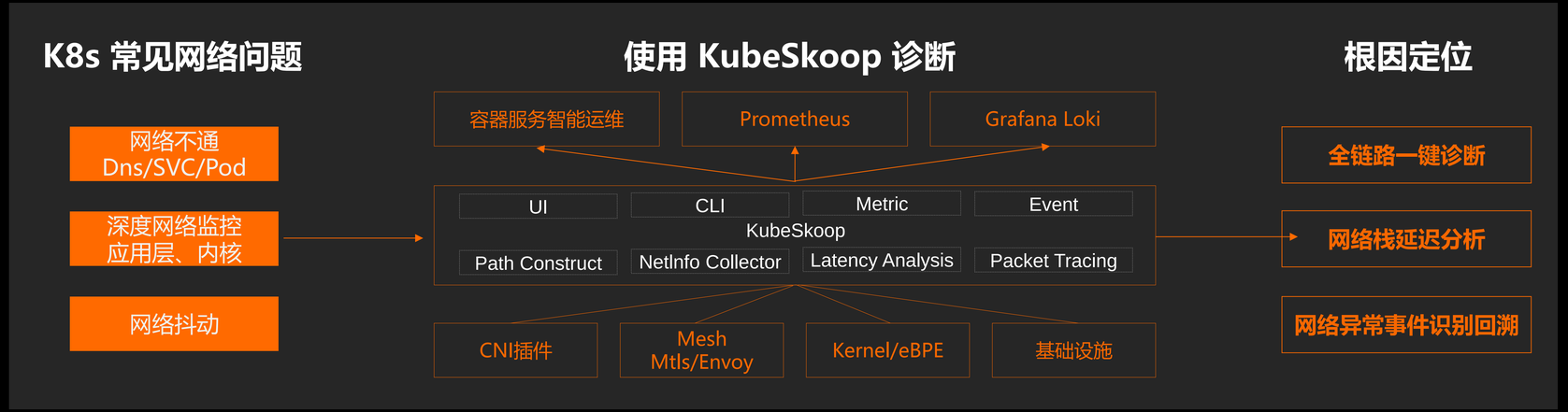
在偶发性网络抖动场景，基于ACK内核网络智能化分析，快速定位异常网络栈路径，**定位时间从周缩短到小时**

在JAVA容器应用响应时间抖动场景，使用AI智能诊断，联动Ingress、容器、内核快速定位，**从小时优化到分钟级别**

(以上数据为客户业务场景应用结果)

容器网络智能诊断-Skoop

即将开源



托管节点池

用户专注上层应用部署，ACK负责节点池基础运维管理

- 节点诊断和自愈：运行时、操作系统
- CVE安全问题自动修复
- 节点kubelet小版本自动升级
- 节点组件自动升级
  （containerd/systemd等）

THANKS