

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

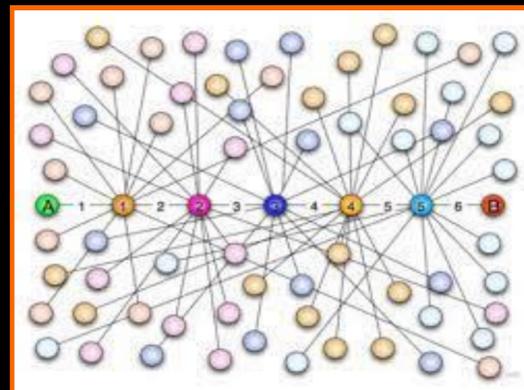
虚拟化和硬件

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



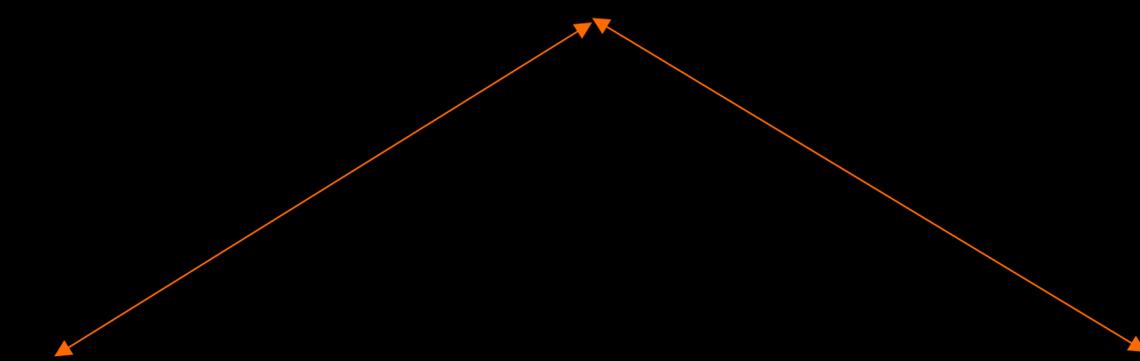
如何降低系统复杂度?



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

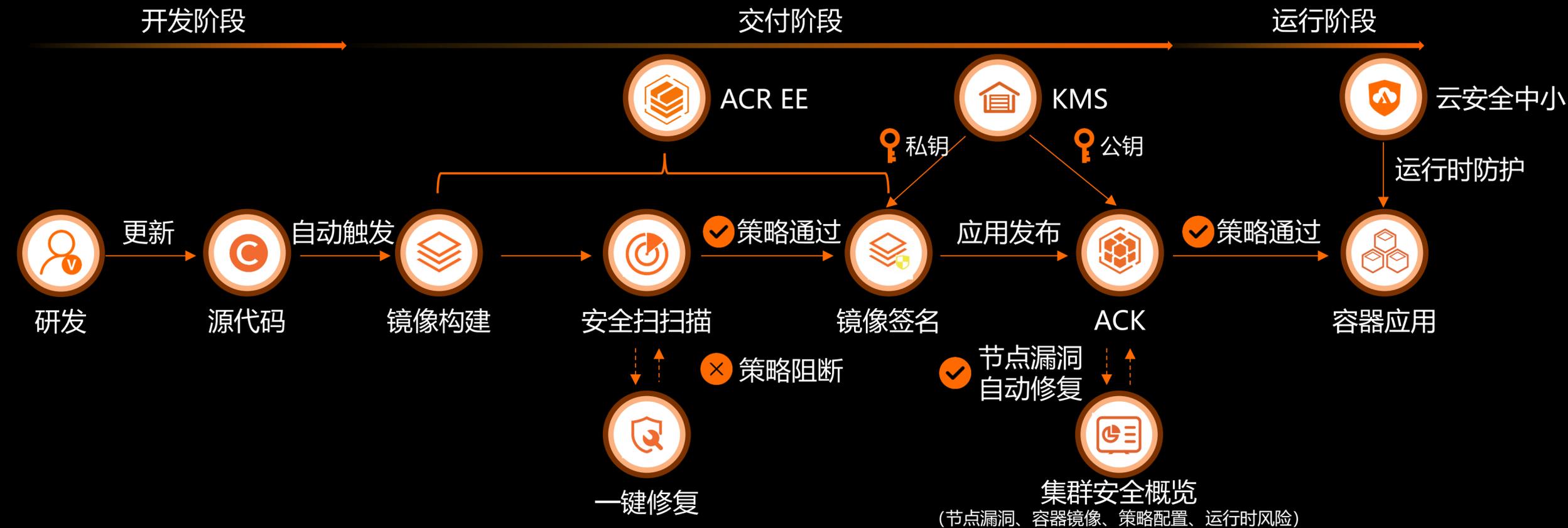
托管节点池/容器优化OS lifseaOS

基础设施即代码

基础设施层

Terraform/ROS

安全可信软件供应链

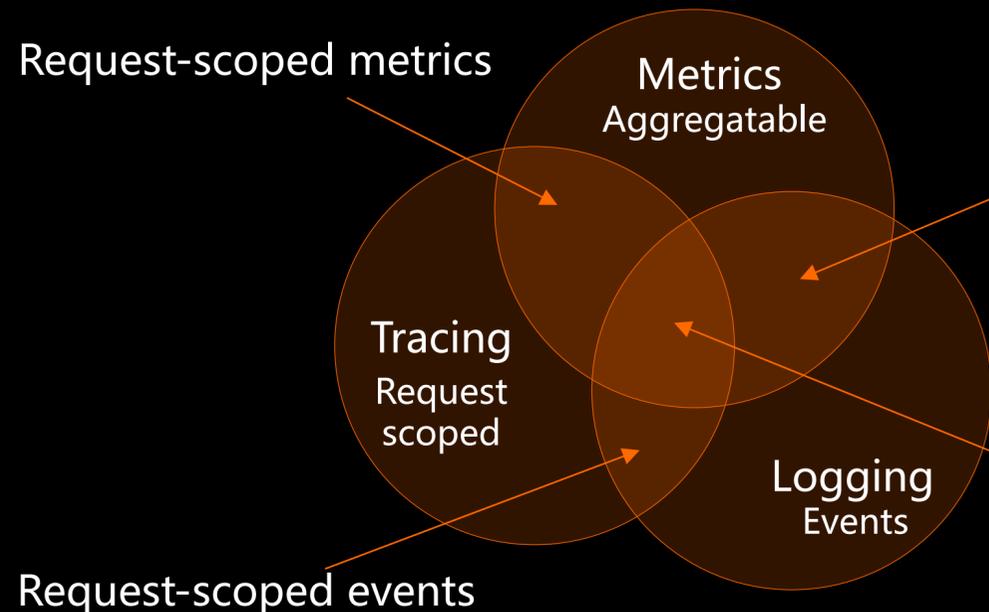


客户使用云原生 DevSecOps 能力，半年内实现万次镜像扫描，千次风险镜像拦截阻断，千次加签/验签安全交付。

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。

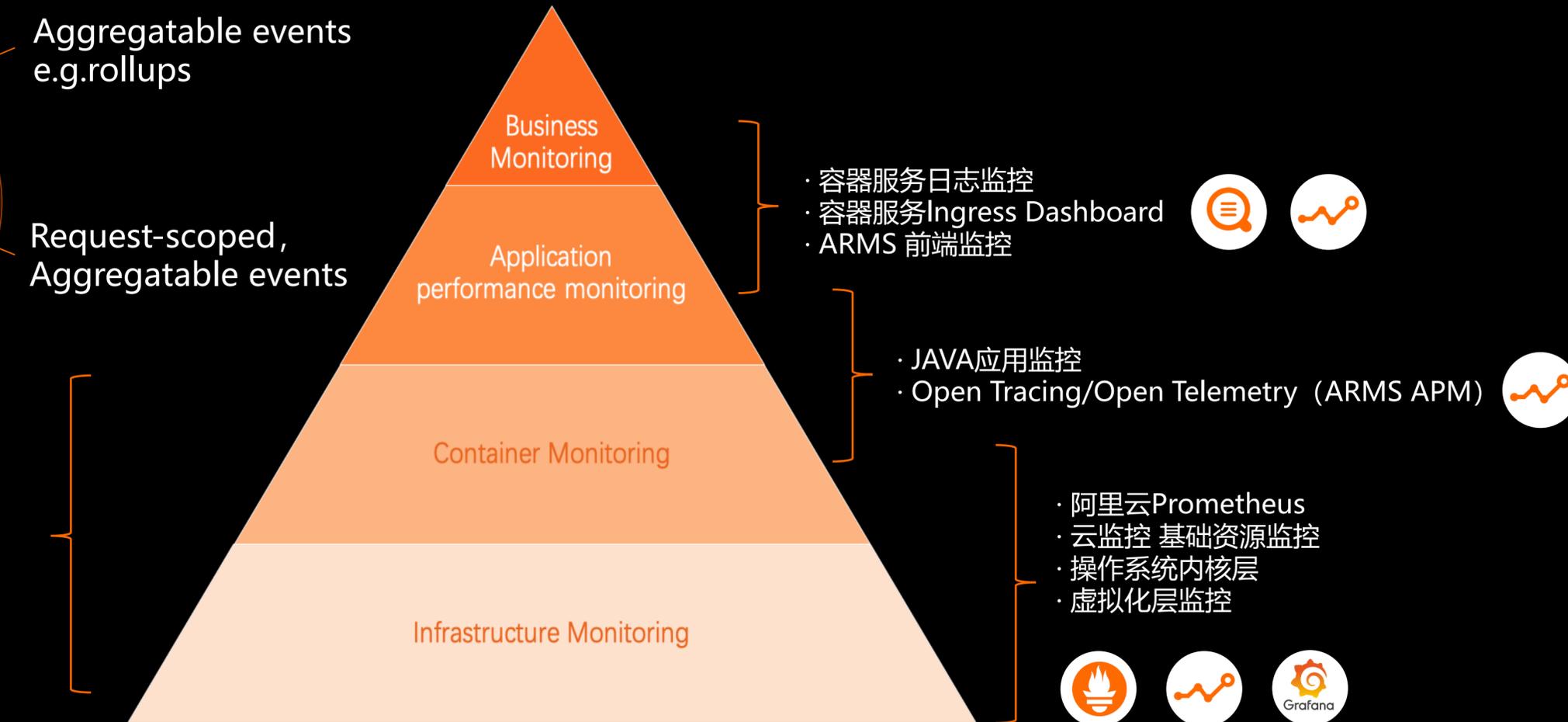
(以上数据为客户业务场景应用结果)

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)



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

The dashboard is divided into several main sections:

- 节点资源总览 (Node Resource Overview):** A summary table showing overall cluster health.

异常节点数	CPU总核数	集群CPU水位	Pod容量	文件系统容量	文件系统水位
0	24	10.0% (使用率) / 81.8% (请求率)	384	785 GB	18.3%
6	48.7 GB	70.9% (使用率) / 60.4% (请求率)	29.9%	0	0
- 节点信息明细 (Node Information Details):** A table listing individual nodes with their status, uptime, and resource usage.

节点	状态	uptime	CPU总	CPU使用%	CPU请求%	CPU限制%	内存总	内存使用%	内存请求%	内存限制%	磁盘总	磁盘使用%	Pod上限	已部署Pod	rtt	contrack表使用率
cn-beijing.192.168.5.163	Ready	2.8 week	3.9	6.145%	96.36%	433.9%	5.55 GiB	87.10%	79.15%	458.7%	121.77 GiB	22.43%	64	24	5.9 ms	0.7309%
- 应用性能: 服务协议 [http] (Application Performance):** A detailed view of application metrics.
 - 成功安装 (Successful Installation):** Overall status.
 - 请求数/s (Requests/s):** Line chart showing request volume over time.
 - 请求数/s环比 (Requests/s Change):** Bar chart comparing current, previous, and future periods.
 - 请求数Top接口 (Request Top Interfaces):** Horizontal bar chart showing the most requested endpoints.
 - 平均响应时间 (Average Response Time):** Line chart showing response times.
 - 平均响应时间环比 (Average Response Time Change):** Bar chart showing response time trends.
 - 平均响应时间Top接口 (Average Response Time Top Interfaces):** Horizontal bar chart showing the slowest endpoints.
- 概览 (Overview):** A grid of key performance indicators.
 - 可用副本数: 2
 - 过去24h重启次数: 0
 - 异常事件数: 0
 - Pod最大CPU平均10s负载: 0.036
 - CPU限流率: 无限流
 - Pod最大内存使用率: 0%
 - 网络流量: 20 kB/s
 - 节点调度分布: 1
 - Pod最大CPU使用率: Limit没配置
 - 文件系统读写吞吐率: 1.5 MB/s
- 事件 [Beta] (Events):** A section for monitoring cluster events, showing a "成功安装" (Successful Installation) status and a list of recent events.



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

容器AIOps套件-故障预防与定位

AIOps for Kubernetes Cluster: Fault Prevention and Problem Determination

全栈巡检

集群健康度巡查

应用可用性巡检

平台安全性巡检

升级检查

版本兼容性评估

配置冲突检测

业务影响评估

智能诊断

集群事件流分析

网络仿真与诊断

OS内核指标分析

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**

专家系统+AI算法

容器服务 - ACK集群

公有云

IDC

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

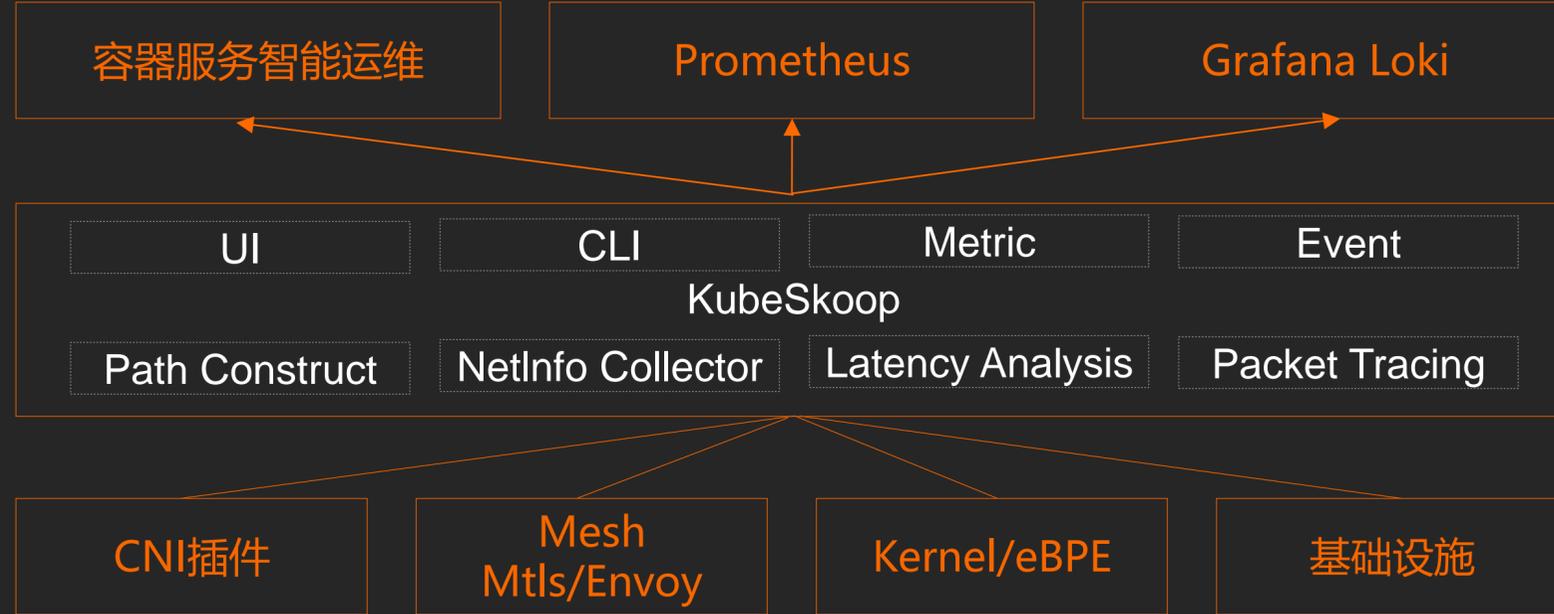
K8s 常见网络问题

网络不通
Dns/SVC/Pod

深度网络监控
应用层、内核

网络抖动

使用 KubeSkoop 诊断



根因定位

全链路一键诊断

网络栈延迟分析

网络异常事件识别回溯

ACK 托管节点池

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

自升级

Kubelet

节点组件

自愈

运行时

内核

安全修复

CVE修复

内核加固

弹性

快速启动

快速扩容

容器优化OS: LifseaOS
原子更新、精简内核

通用OS
Alibaba Cloud Linux、CentOS

- 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)



容器服务 – ACK集群

THANKS

原生万物 云上创新

