

集群多还是多集群

云原生平台工程探索

崔秀龙（华为云）

Agenda



- 接下来的内容由现实和想象两部分组成，不过都不是技术内容
 - 听说 DevOps 死了？
 - 又一个“新”名词：平台工程
 - 集群多还是多集群？
 - 最后

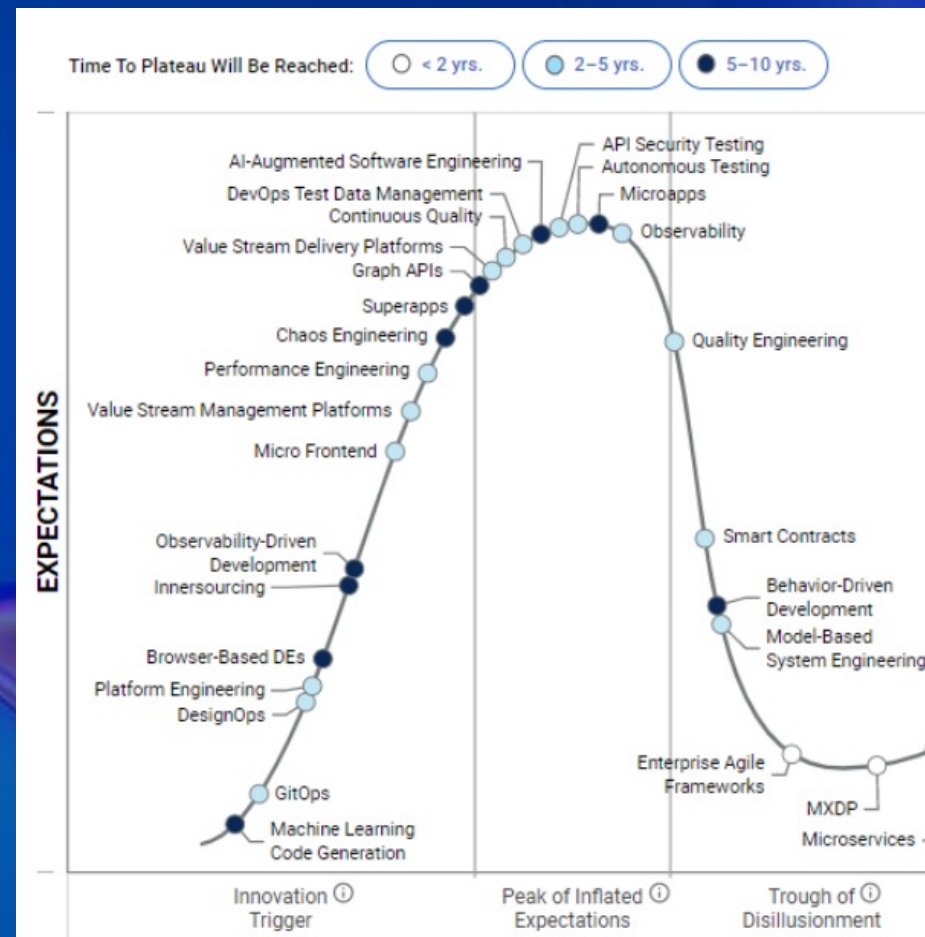
- 关于我自己
 - 云原生喝酒 SIG Founder；
 - 前马拉松爱好者
 - 前技术写手
 - 前...
 - 现华为云 SRE 工程师



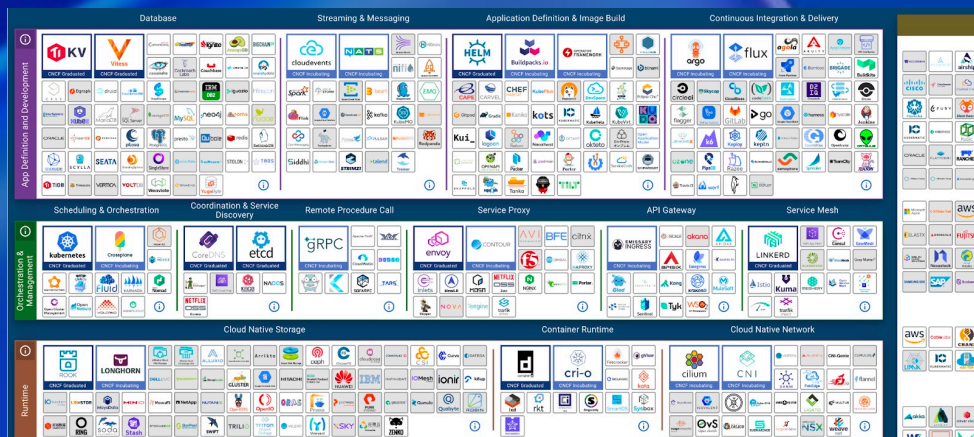
听说 DevOps 已经死了



- 2022年10月11日，InfoQ 爆文：《DevOps 已死，平台工程才是未来》，太长不看版：
 - 开发者并不想做运维，工程师不仅编写代码，还要运行他们编写的代码；
 - 反模式：高级工程师现在要负责环境配置，并需要处理比较初级的同事的请求；
 - 除了 CICD 之外，还有很多复杂的运维场景：配置管理、依赖管理、跨环境部署、统一的安全管控..
 - 虽然对于像谷歌、亚马逊、Airbnb 这些比较先进的组织来说，上述方法很有效，但对于其他大多数团队而言，要在实践中复制真正的 DevOps 并不简单。
 - 平台工程才是未来？

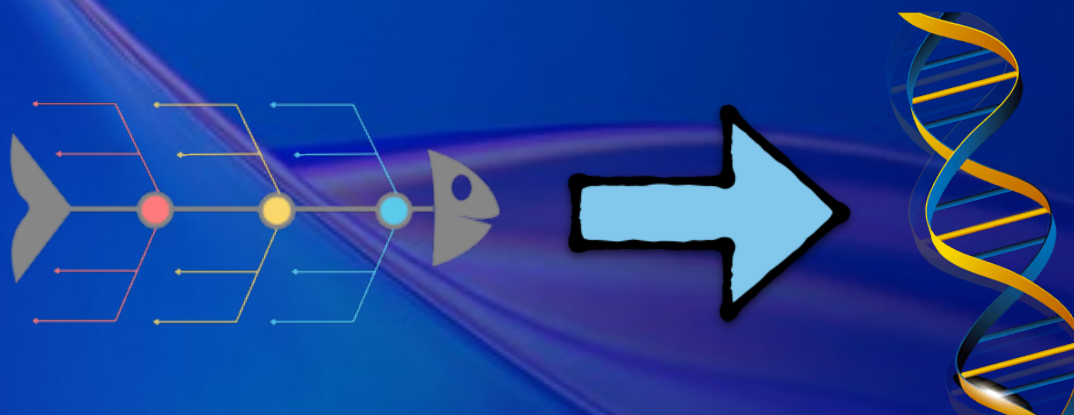


云原生工具恐慌



- 云原生体系对企业 IT 体系的挑战：
 - 从工具到生态
 - 从点缀到骨干
 - 从鱼骨到双螺旋

- 让程序员专注于业务代码的开发？
 - 一千多个卡片。。
 - License 你都能背下来吗？
 - 凭啥说 PodMan 比 Docker 好用？
 - 两年之后才发现没法升级怎么办？
 - 1.15 到 1.16 怎么那么难？



社交网络定选型？

- 成功采用开源软件的九九八十一难
 - 项目健康
 - 多样性如何？有基金会支撑吗？
 - 活跃吗？响应快吗？
 - 合法合规
 - 本体和依赖项都合法合规吗？
 - 各种授权限制允许我顺利使用吗？
 - 功能完备
 - 稳定性、可靠性，安全性满足要求吗？
 - 运维同学们买单吗？



又一个“新”名词——平台工程

《团队拓扑结构》一书于 2019 年出版，成为成功的工程组织中最具影响力的现代团队设置蓝图之一。根据他们的蓝图，有四种基本的拓扑结构，团队应该围绕这些拓扑结构进行：

- 业务导向团队：与业务领域某个部分的工作流相匹配，处理核心业务逻辑。
- 赋能团队：帮助业务导向团队克服障碍并检测缺失的功能。
- 复杂子系统团队：在严重依赖数学/技术方面的专业知识时组建。
- 平台团队：提供一个令人信服的内部平台，提高业务导向团队的交付速度。

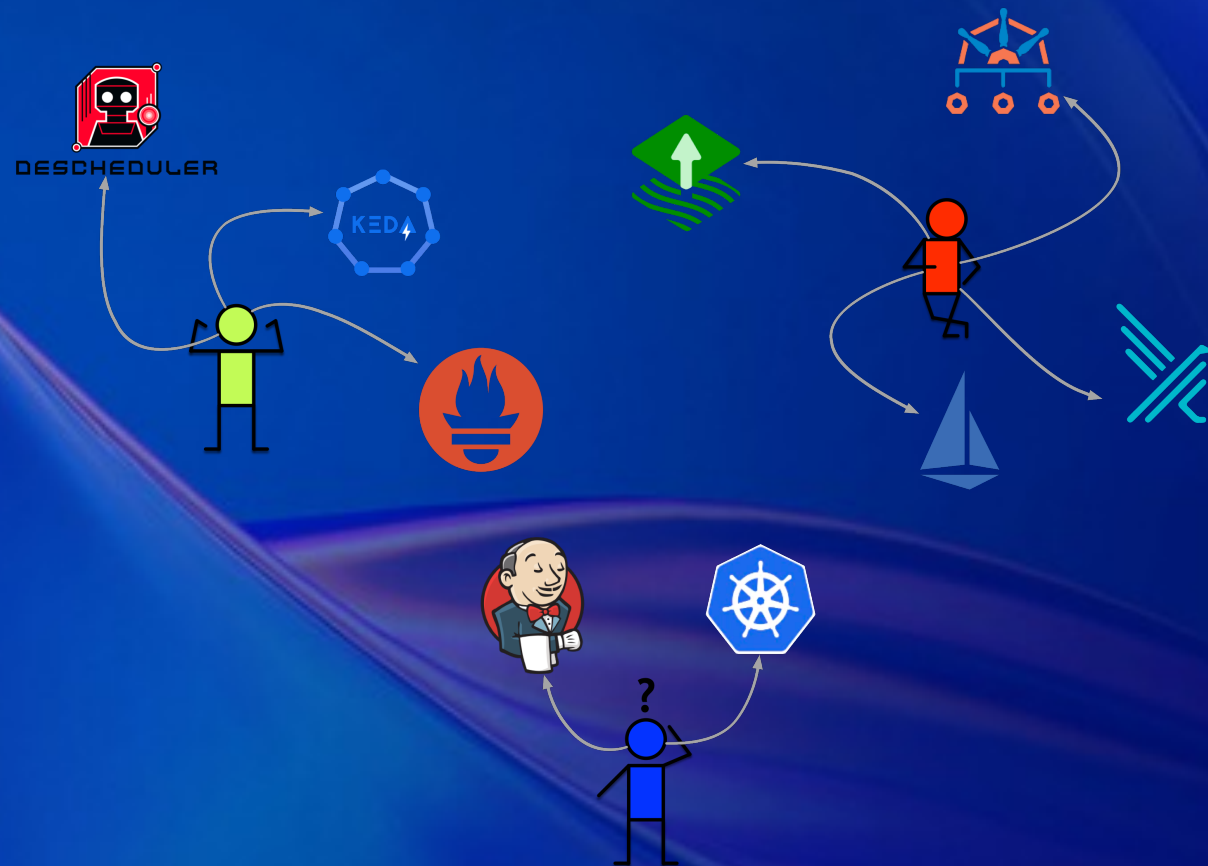
平台工程是一门设计和构建工具链和工作流的学科，在云原生时代为软件工程组织提供自助服务能力。平台工程师提供一个集成的产品，通常被称为“内部开发者平台”，涵盖了应用程序整个生命周期的操作需要。



集群多还是多集群



- 多年以前一个网友嘲笑某项目——他们那不是大数据，那叫数据大。
- 多集群和集群多？
 - 应用水平、建设思路，保障目的各有不同
 - 不同团队八仙过海，各显神通
 - 团队之间的知识技能难于共享
 - 重复建设和步调混乱
- Cloudscope Kubernetes Manager



规范建设—把技术关在笼子里

- 云原生生态和传统运维体系的融合

- 云原生标签工程师：制定 Kubernetes 负载和 Istio 的标签规范
 - 用 CI/CD 工具，将必要的规范内置到部署流程之中
 - 既有的可观测性体系通过标签方式，完成对云原生生态的融合

- 风险控制的云原生落地

- 容器镜像生命周期管理
- 完整的供应链安全保障（漏洞扫描、签名验签、访问控制...）
- 跨 Region/AZ 的浸泡、金丝雀能力
- 容灾架构在 Kubernetes 集群上的应用
- 云原生工作负载变更的风控流程

- 最佳实践的广泛应用

- Dockerfile 镜像规范
- Kubernetes Manifests 规范
- 可观测性和安全性基线规范
- 使用 CI/CD，结合 Linter、OPA、Kyverno 等进行静态检查和动态保障

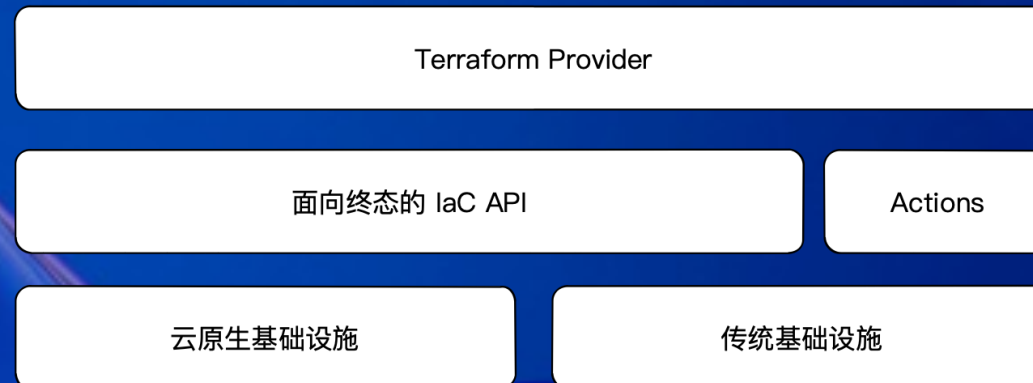
- 运维能力的标准化

- 环境标准化建设，例如准入和巡检
- 配置管理标准化
- 对开源软件的运维能力进行补齐
- Kubernetes/Istio 的应用场景标准化

基础设施管理



- 面向 IaC 和终态，将传统基础设施的管理过程，转换为更为现代化的用声明式 API 资源对象
 - Kubernetes 集群
 - Istio
 - 虚拟机
 - 网络
 - 中间件
 - ...



工具建设



- 开发和CICD

- 各种门禁检查
- 标准构建能力
- 环境对接和管理
- IDE Helper

- 运维安全

- 规章制度建设
- 堡垒机操作风控
- 基于 IaC 技术的



- 部署变更

- 配置变更管理
- 软件变更管理
- 灰度变更过程
- 变更结果监控和反馈

- 可观测性

- 以云原生业务应用为中心
- 面向快速定位定界
- 大数据和专家系统加持
- 打通虚拟机和云原生世界

平台工程就是 SRE 能力中台



最新消息：据说中台也死了：)

Thanks

接受简历投喂