CHINA OpenInfra Days

CHINA OpenInfra Days | IT大咖说 知识共享平台

H3C CloudOS 3.0云原生容器应用引擎

刘梦雯 H3C云计算高级架构师

云计算的目的是什么？

顶配的机场

糟糕的出行体验

尖端的数据中心

频繁的业务故障

业务应用的敏捷交付和SLO保障是云计算的终极目标

挑战：混合IT基础设施

- 集中架构
- 有状态
- 紧耦合
- 对硬件有依赖
- 瀑布式开发

传统Old

混合Hybrid

- 兼容传统应用和云原生应用的PaaS框架
- 支持各种异构资源架构
- 多级资源调度模型
- 敏捷开发，DevOps
- 应用服务化

- 微服务化
- 弹性扩展
- 自动编排
- 容器化
- 快速部署
- 资源池化

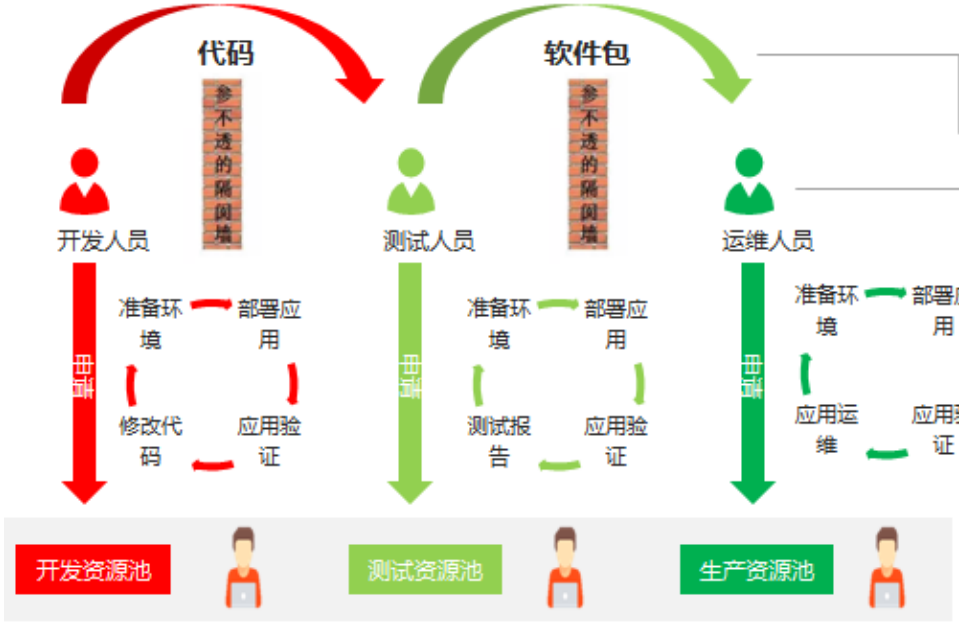
新兴New

传统应用和云原生应用将会长期并存，最佳模型就是采用混合IT

挑战：自动化程度不足

自动化程度不足以支撑业务自助交付、自动化响应、自动巡检与故障定位等

挑战：开发、测试、运维割裂



01 上线难以控制

02 环境准备不易

03 资源获取繁琐

传统架构和模式无法满足业务要求，必须打破隔阂墙，持续快捷交付业务

趋势：云原生、微服务

云原生（Cloud-Native）

云原生是一种方法，用于构建和运行充分利用云计算模型优势的应用。
包含了一组应用的模式，用于帮助企业快速、持续、可靠交付业务。

Containers

解决部署问题，实现微服务和DevOps落地
提升应用可靠性和扩展性，提高运维效率

DevOps

持续集成、持续部署，快速的迭代优化
打通开发、测试、运维衔接壁垒

Microservices

自由的决策、快速的开发
更容易地迭代和扩展、快速影响业务需求

驱动云原生变革的三驾马车：容器、DevOps和微服务

趋势：站点可靠性工程（SRE）

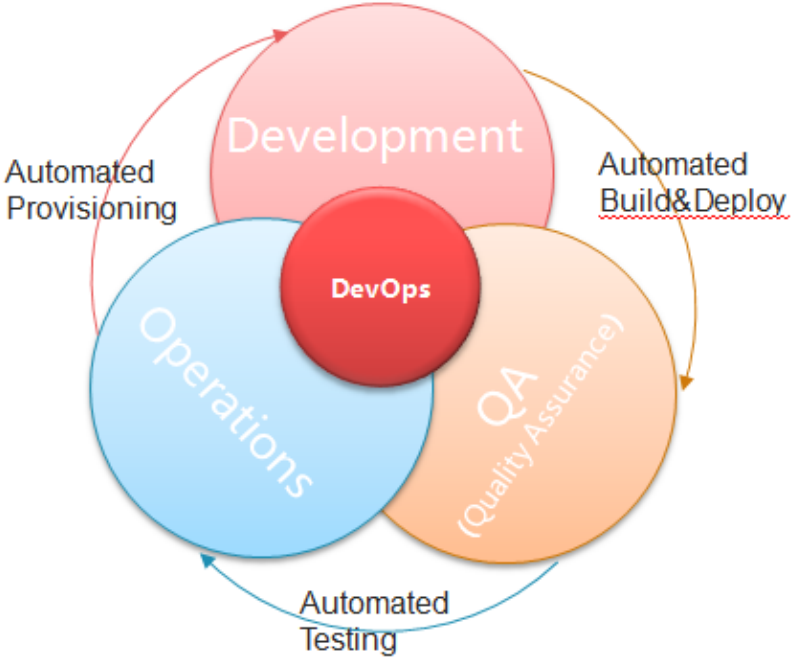
Google 用软件工程理念和自动化工具重新定义了系统运维

SRE方法论

- 确保长期关注研发工作
- 在保障服务SLO的前提下最大化迭代速度
- 监控系统
- 应急事件处理
- 变更管理
- 需求预测和容量规划
- 资源部署
- 效率与性能

不能将碰运气当成战略。—— SRE俗语

趋势：开发运维一体化（DevOps）

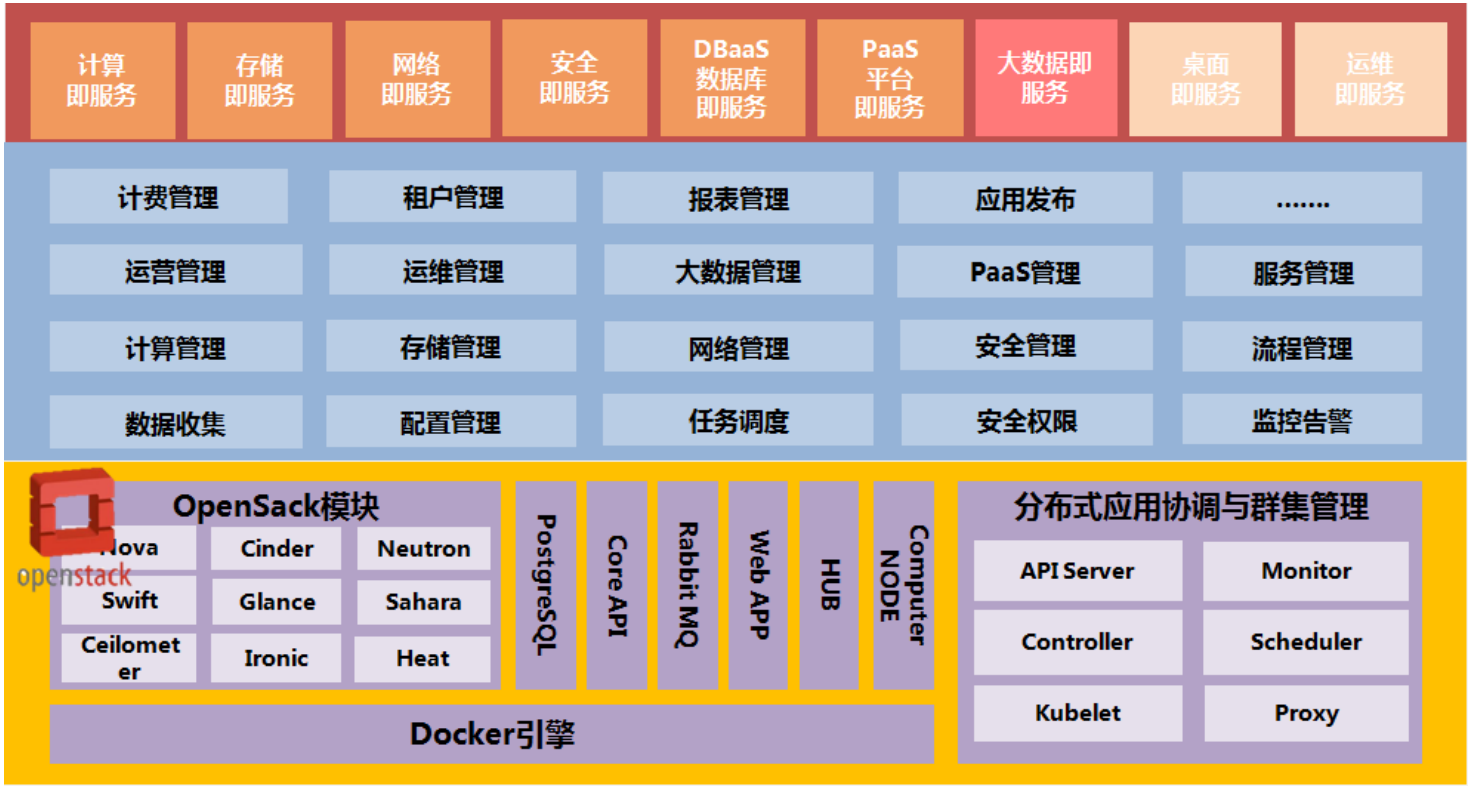


DevOps
(Development and Operations)

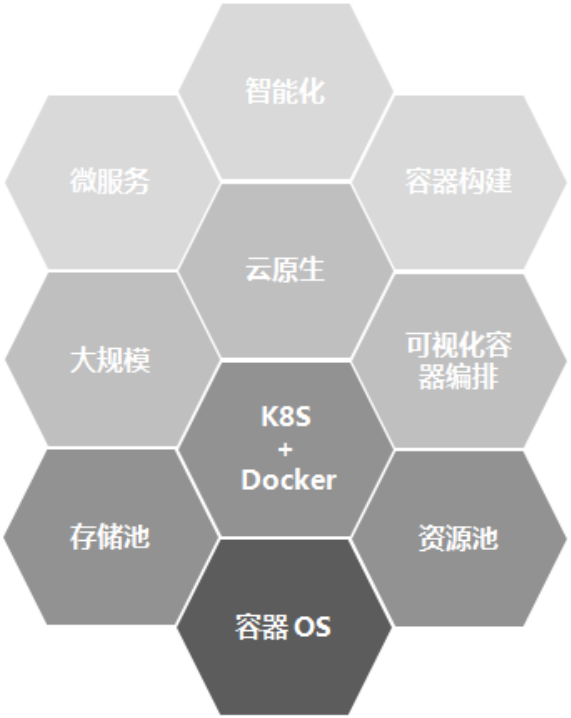
- 一组过程、方法、与系统的统称
- 促进开发、运维、质量保证各部门之间的有效沟通、协作与整合，提升效率
- 迭代开发、持续集成、持续部署，拥抱变化

推进开发运维一体化，释放人员关键价值

源自容器化的OpenStack云管理实践



H3C CloudOS 云原生容器引擎



H3C CloudOS 容器引擎

运维监控

- 容器、节点性能监控
- 容器、节点日志集中管理

可视化容器管理

- 容器镜像仓库
- 容器构建向导
- 可视化组合容器编排
- 容器业务拓扑

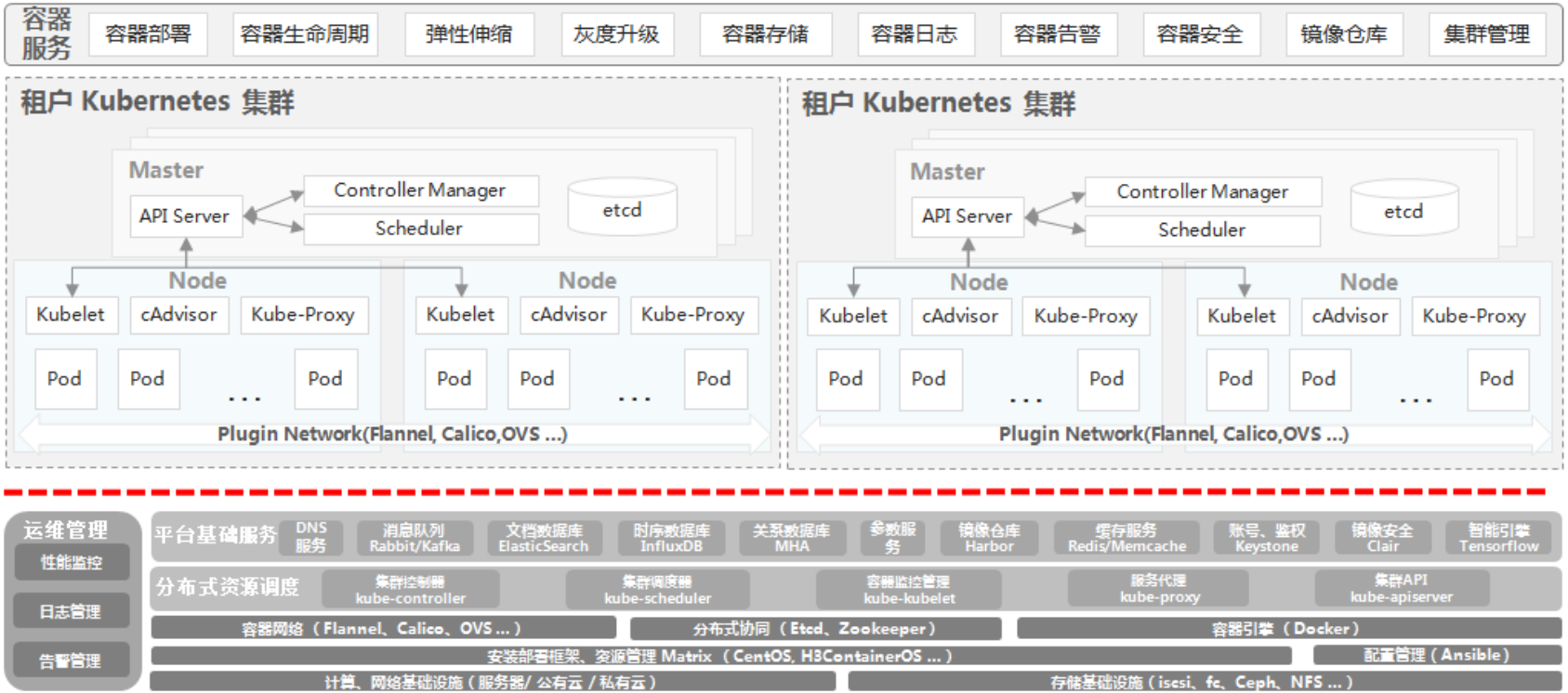
自动化节点管理

- 通过 PXE、ISO 进行节点部署
- CentOS、H3C ContainerOS 支持
- GPU 容器高性能计算支持
- 多 K8S 集群部署

容器托管

- Kubernetes + Docker 黄金组合
- 大规模容器部署
- 容器高可用，资源配合，弹性伸缩，灰度升级
- 多种后端存储支持

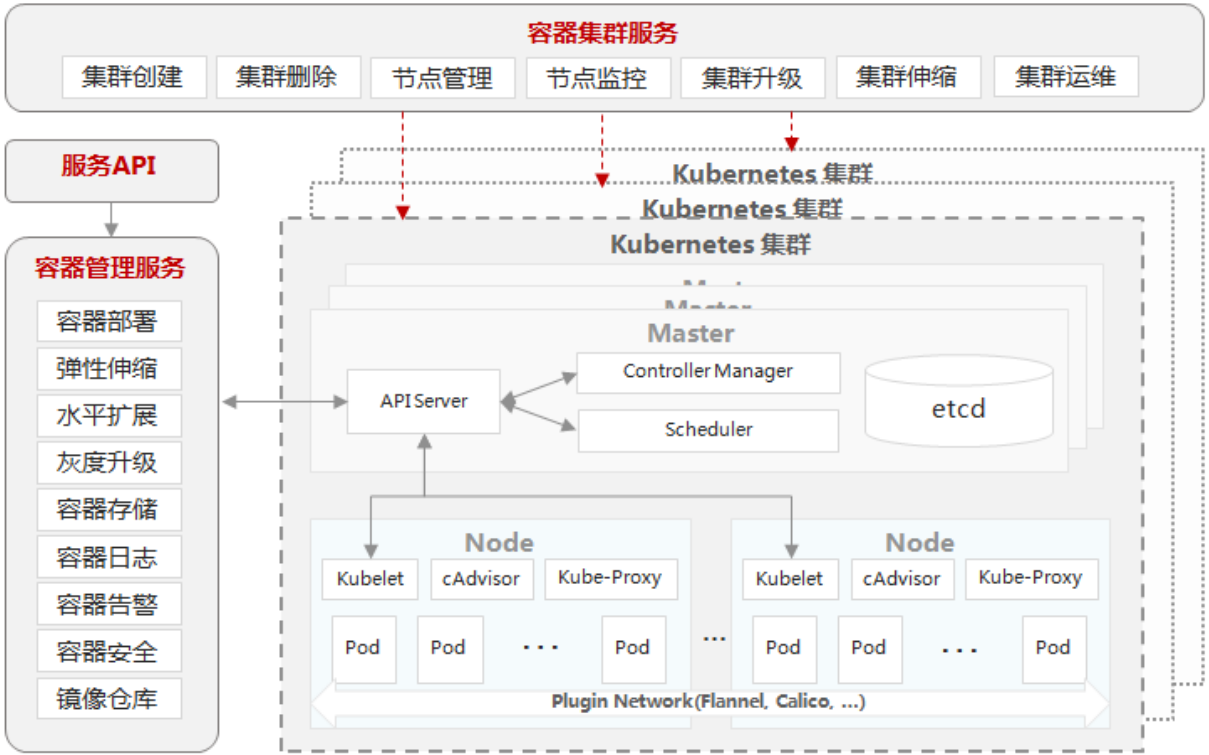
H3C CloudOS 容器引擎总体架构



相对开源K8s的改进与增强

H3C CloudOS 容器引擎	开源 Kubernetes
小规模情况下无需外置 LB，即可实现 VIP 及迁移能力	集群的访问必须有前置的 LB
管理集群脑裂情况进行优化处理，避免脑裂发生时有状态容器出现异常	对管理集群脑裂无处理
操作系统关机、重启等正常维护情况处理	无处理，无保护
存储卷网络闪断自动恢复	无处理，需要人工恢复
Ingress 优化处理，支持会话保持的能力	ingress 情况下，不支持会话保持
无互联网支持部署	需要联网
内置动态参数服务及工具	静态configMap
内置高可用容器镜像仓库	无
图形化容器配置、编排	无
容器镜像构建向导	无
图形化容器部署、监控、资源管理等	无
容器安全扫描、容器镜像签名	无
多模容器网络（flannel、calico、ovs 等）	CNI 接口定义
微服务治理	无
容器 Web 式登录	无

容器集群服务



容器集群服务提供安全高可用的 Kubernetes 集群管理能力，简化集群的搭建和扩容等工作，用户可以独享 K8S 集群，并在集群上部署自己的业务。

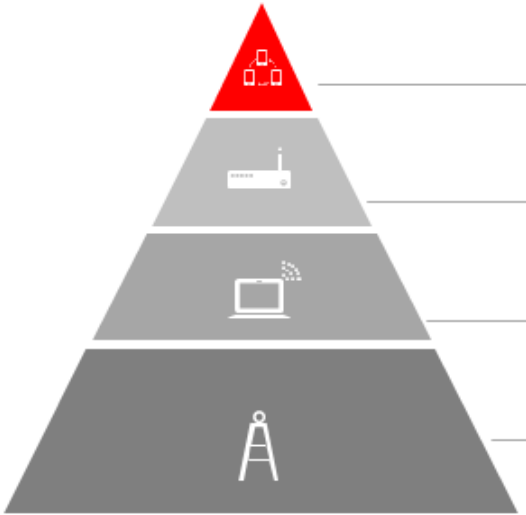
- **Kubernetes集群**

通过容器集群服务用户可以创建一个或多个Kubernetes集群，每个集群拥有至少 3 个控制节点（Master）和 1 个工作节点，且工作节点可动态伸缩，实现集群的安全高可用。

- **容器管理服务**

提供一站式容器生命周期管理能力，并对外提供兼容Kubernetes API的“服务 API”。

容器安全扫描服务



容器运行安全

确保容器运行时加载的镜像是受信的、未被篡改的

容器主机安全

确保容器运行在受信的节点上

容器镜像扫描

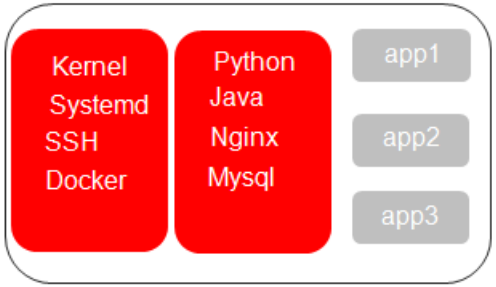
容器安全扫描，可以对各个容器中的层级进行对应的扫描，避免产生安全隐患

可信计算

TPM+SeLinux

容器安全确保了容器从镜像到运行态全生命周期的安全性

容器操作系统



传统操作系统

传统操作系统，如 CentOS、Ubuntu 等功能完善，可靠稳定。但同样的存在体积大、系统容易被污染、升级困难等缺点。

操作系统大小	大
操作系统空间	易被污染
操作系统升级	逐包升级，时间长
安装部署	安装配置困难
功能完善度	高

容器操作系统

容器操作系统高度精简，体积轻巧，全容器化部署，升级简易。

小	操作系统大小
不易被污染	操作系统空间
A – B 升级	操作系统升级
远程安装配置	安装部署
低	功能完善度

开发测试服务

提供研发项目的智能化整体解决方案

应用场景

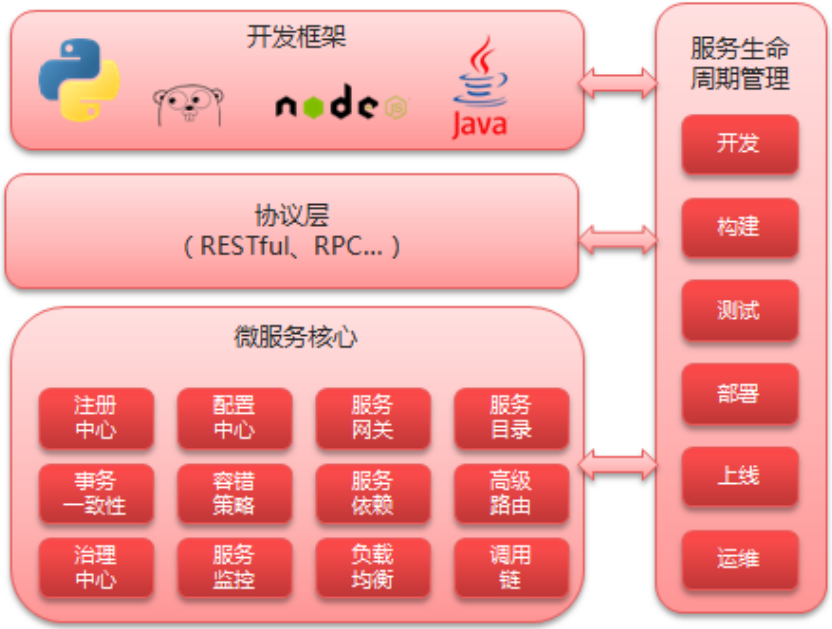
- 政府软件产业主题合作下，提供公共研发平台
- 企业快速启动研发，不必投资相关专用基础设施
- 金融大客户研发机构敏捷转型及对应工具链切换
- 高校、培训机构提供便利统一的研发服务/训练平台
- 中小互联网企业解决分布式协同研发

关键技术与规格

- 采取统一持续发布，项目集看板，scrum敏捷框架
- 利用发布门禁机制控制产品持续发布质量
- 多级管理据视图，可在任何级别下查看数据和图表
- Smart Sense智能感知项目潜在风险，预测发布状态，以及项目过程的阻塞点
- 基于功能/变更的代码管控
- 租户隔离确保代码库物理安全隔离

微服务治理

涵盖服务注册发现等能力的微服务治理框架，推进应用微服务化进程



应用场景

- 提供基于微服务架构的应用生命周期管理，完成传统应用向微服务化的转型，提供微服务应用运行环境。
- 提供云上自动部署和运维能力，解决手动部署效率低、升级困难、难于监控定位等运维难题，快速交付各类业务应用。

关键技术与规格

- 开箱即用，打包微服务完整的注册、发现、治理等能力；
- 多语言，支持多种语言的原生接口；
- 可扩展，提供可扩展框架，支持扩展微服务的高级能力；
- 高可靠，采用可隔离仓、熔断机制等技术，保障用户应用的高可靠性；
- 自动化运维，采用跟踪链分析，可监控端到端服务调用链、各服务的调用频率、时延等各项指标；

其余特色功能

卡片式容器镜像管理

镜像构建向导

拖拽式容器编排

容器健康检查

容器灰度升级

基于ELK日志管理

多种类型的存储卷

丰富的集群及容器监控

CHINA
OpenInfra Days

Thank You