



KubeCube设计实践

初学者玩好Kubernetes的正确姿势

祝剑锋

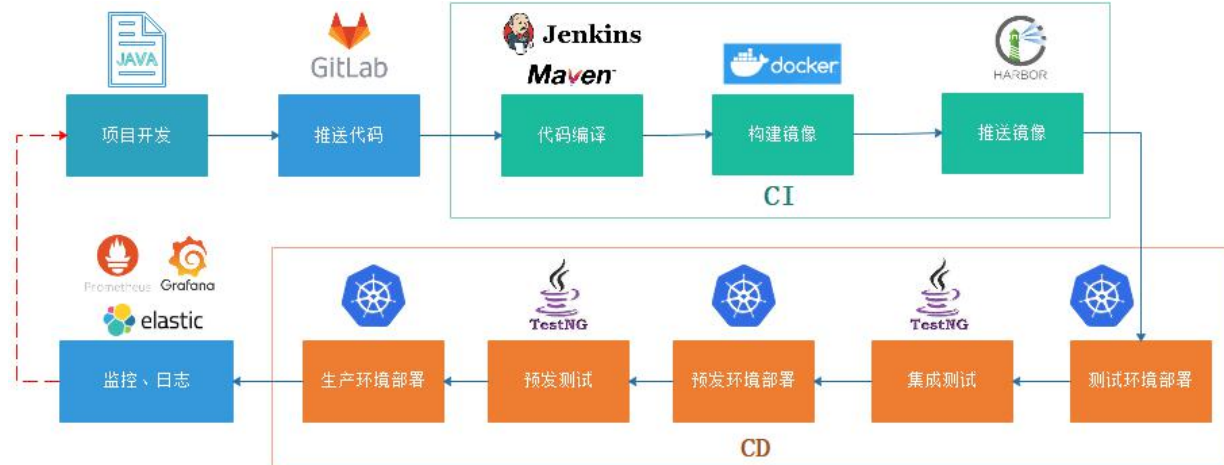
网易数帆 · 轻舟容器平台负责人



目录

- Why KubeCube
- KubeCube整体架构
- 功能设计及架构解读
 - 多集群
 - 多租户
 - 热插拔
 - 操作审计

Why Docker



<https://kubecube.io>

- 传统主机应用部署，需要投入精力解决的问题
 - 部署环境一致性，环境标准化及版本控制
 - 快速、自动扩容，应对突发流量
 - 资源利用率不高
 - 故障自愈
- Docker提供了轻量化的解决方案，但仍需要解决
 - 自动扩缩容
 - 故障自愈
 - 其他应用所需特性，如负载均衡、服务依赖、服务发现、配置管理等

Why Kubernetes

- K8s的出现使得上层应用不需要感知底层环境的差异，提供了应用生产级部署所需的很多需求。
- 但不可否认，K8s是一个复杂的分布式系统，要真正生产环境应用落地使用、维护，需要很强的经验支撑。
- 并且K8s设计的关注点在单集群单租户的能力，虽然社区有相关项目，但同样落地有一定的门槛。



K8s not enough

- 企业生产落地需要解决的问题
 - K8s学习曲线陡峭，配置复杂度高，需要储备人才，人力成本增大
 - 单集群无法满足生产需求，多集群管理效率低
 - 扩展企业落地特性代价较大，如多租户资源隔离
 - 监控、告警、日志等可观测建设成本较高，配置复杂，影响业务运维效率
 - 多架构支持，尤其是在金融、政企合作项目中，国产化支持必不可少
- 我们开源KubeCube的目的是为了简化企业容器化落地，让初学者也能更好的使用K8s

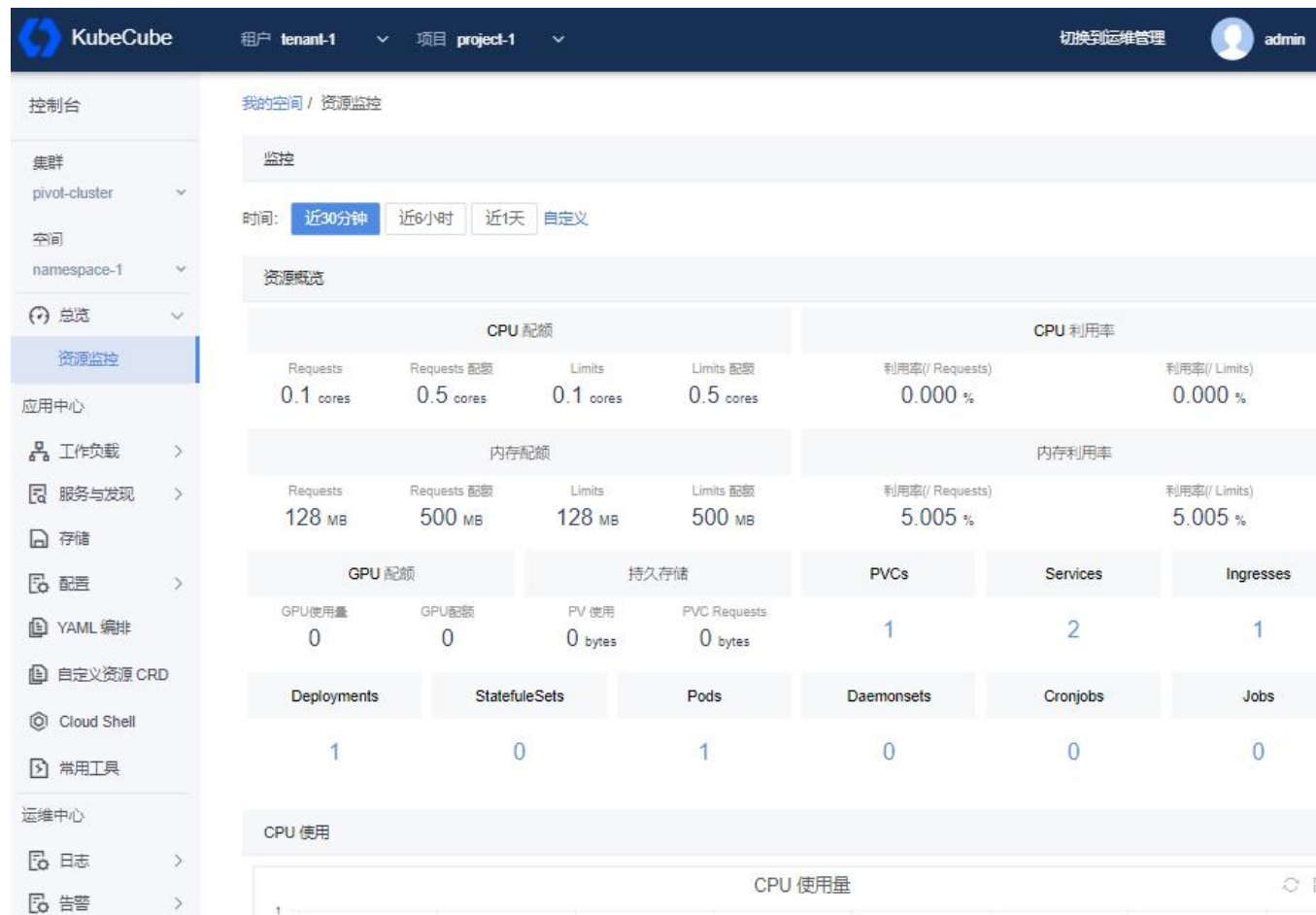
What is KubeCube



KubeCube

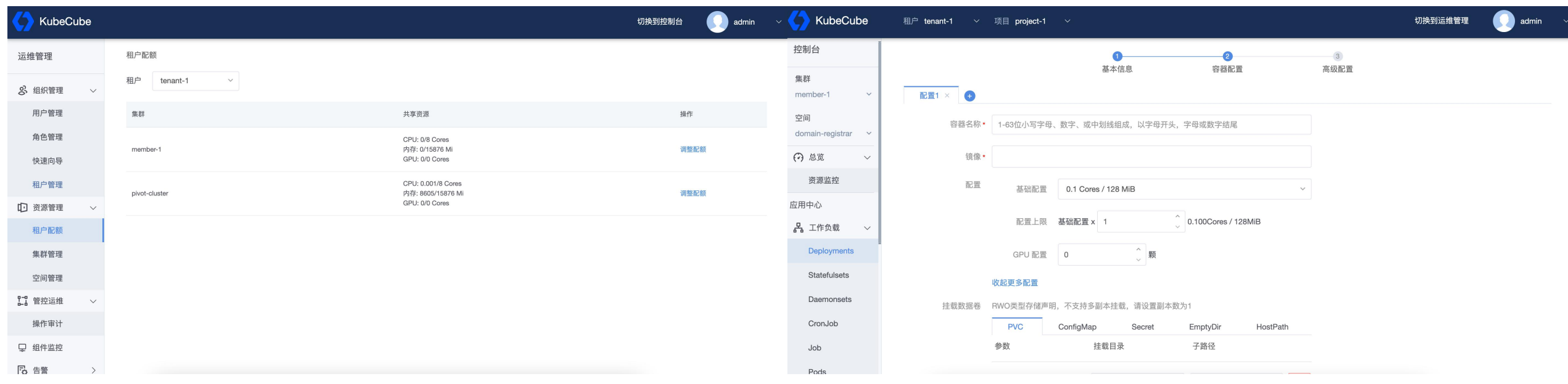
<https://kubecube.io>

- KubeCube (kubecube.io) 是一个开源的企业级容器平台，为企业提供kubernetes资源可视化管理以及统一的多集群多租户管理功能。
- KubeCube可以简化应用部署、管理应用的生命周期和提供丰富的监控和日志审计功能，帮助企业快速构建一个强大和功能丰富的容器云平台，并增强 DevOps 团队的能力。



What is KubeCube

- KubeCube仅对一些必需的功能进行了概念封装，如用户、角色、租户配额等，其他K8s原生资源尽量保持了原生化。初衷是为了平滑学习曲线，而不是创造一条新的学习曲线。
- 初学者可以通过可视化的配置及资源管理很容易的使用K8s，而随着使用者能力的提升，可以无缝转换到原生K8s概念。



The screenshot displays the KubeCube web interface. The top navigation bar includes the KubeCube logo, user information (admin), and navigation links for switching between control and maintenance views. The main content area is divided into three sections:

- 租户配额 (Tenant Quota):** A table showing shared resources for different clusters within a tenant.
- 控制台 (Control Panel):** A sidebar menu for managing various Kubernetes resources like clusters, namespaces, and deployments.
- 配置 (Configuration):** A detailed configuration form for a container, including fields for name, image, resources, and storage.

集群	共享资源	操作
member-1	CPU: 0/8 Cores 内存: 0/15876 Mi GPU: 0/0 Cores	调整配额
pivot-cluster	CPU: 0.001/8 Cores 内存: 8605/15876 Mi GPU: 0/0 Cores	调整配额

配置 1

容器名称: 1-63位小写字母、数字、或中划线组成，以字母开头，字母或数字结尾

镜像: [Input Field]

配置: 基础配置 0.1 Cores / 128 MiB

配置上限: 基础配置 x 1 0.100Cores / 128MiB

GPU 配置: 0 颗

收起更多配置

挂载数据卷: RWO类型存储声明，不支持多副本挂载，请设置副本数为1

PVC ConfigMap Secret EmptyDir HostPath

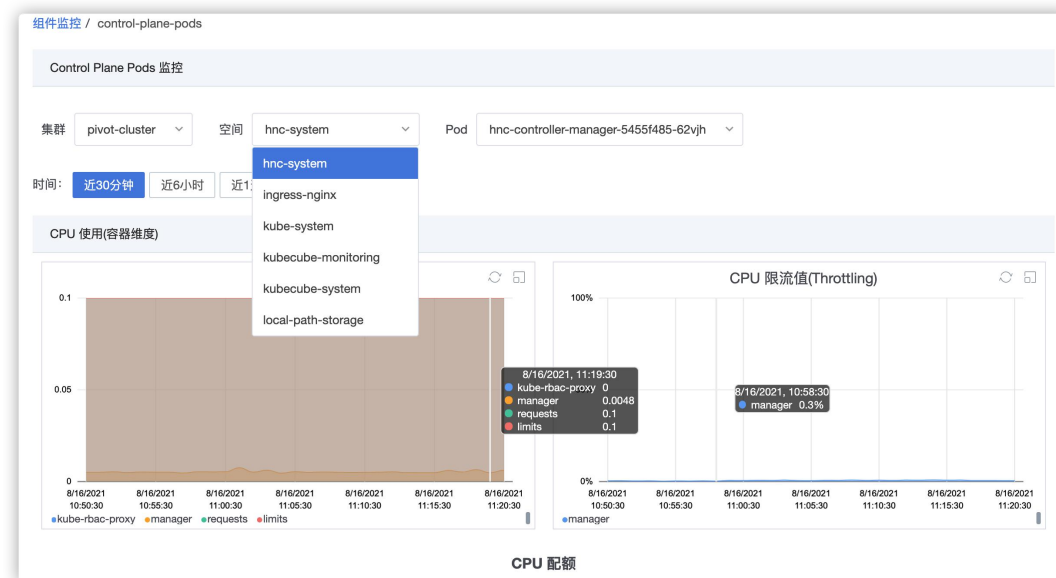
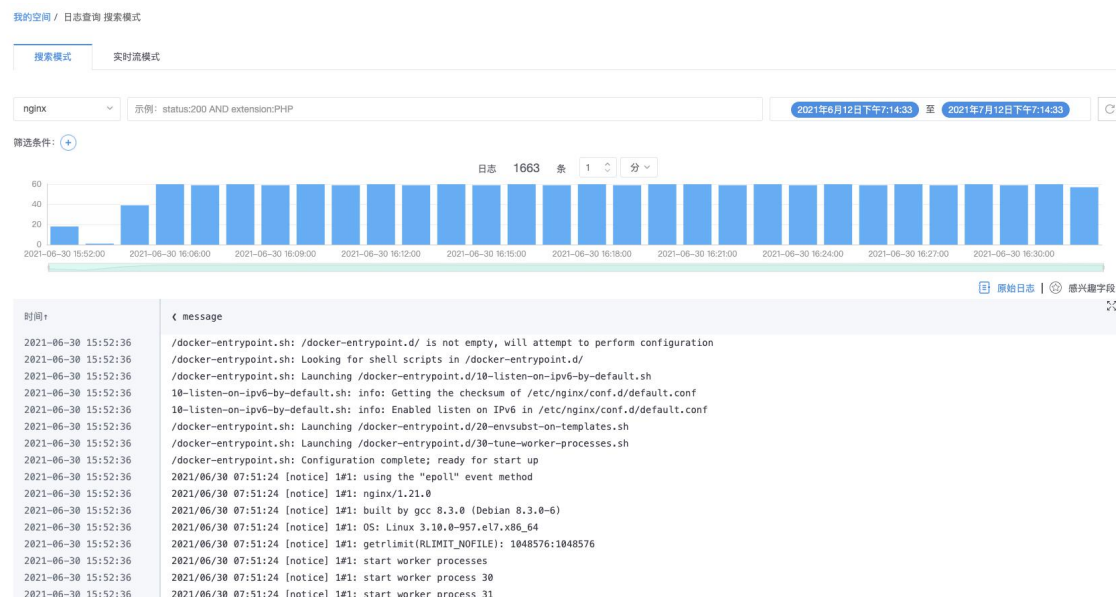
参数 挂载目录 子路径

Why KubeCube

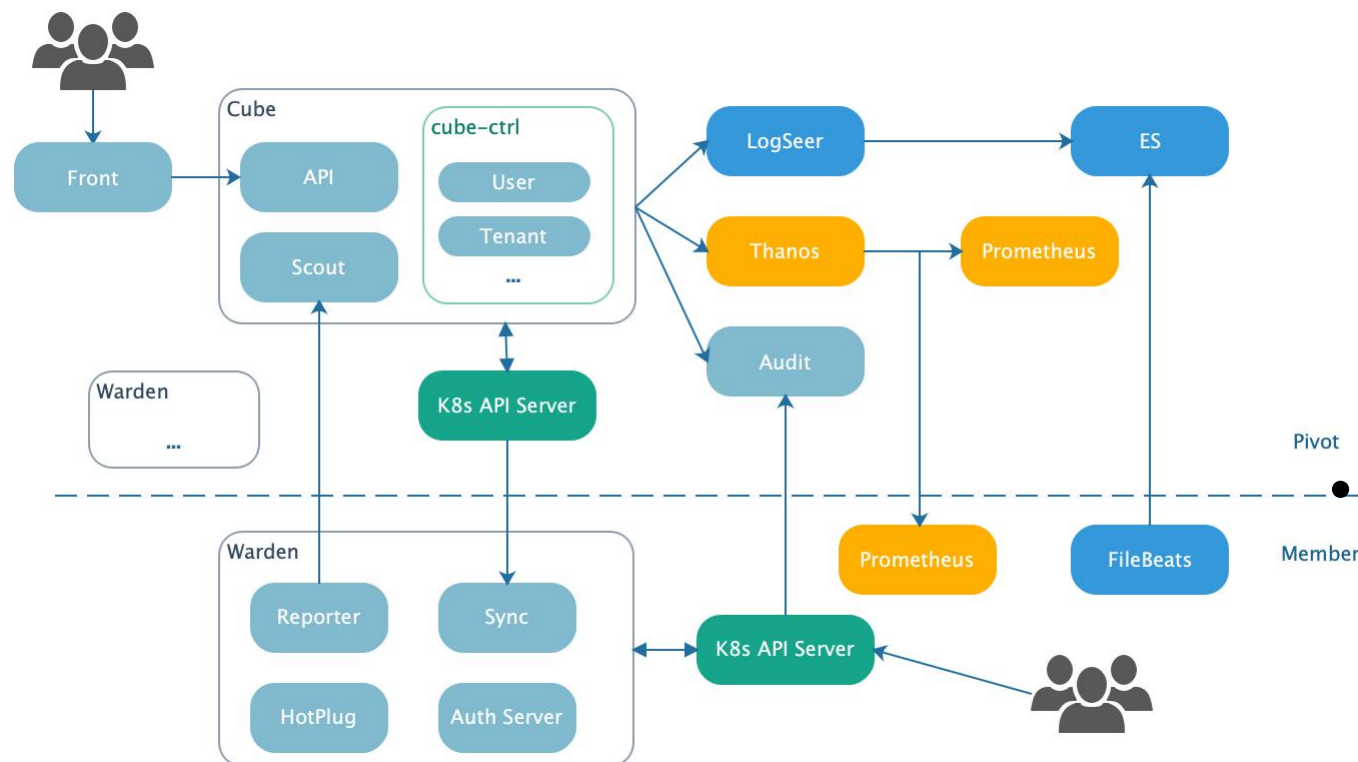
- 简化使用
 - 一键部署，All in one部署快速POC、多节点高可用部署生产环境更可靠
 - 开箱即用的可视化资源管理、日志、监控、告警功能，平缓学习曲线
 - 支持AMD及ARM处理器，支持主流国产芯片及操作系统
- 简化多集群管理
 - 多集群统一管理，提供统一的身份识别及访问控制
 - 网络异常时，各集群保持自治，不影响业务应用
 - 提供WebConsole、CloudShell等在线运维工具，提升效率
- 简化企业级所需能力获取
 - 多级租户模型，租户间权限、配额隔离
 - 提供操作审计，所有操作均可溯源，更安全
 - 原生友好，支持OpenAPI及K8s原生API，集成接入更方便

Why KubeCube

• 可观测功能展示



KubeCube整体架构



• 核心组件

- Front: 前端服务
- Cube: 管控服务，提供API及核心控制逻辑
- Warden (守望者): 成员集群的 agent，负责心跳上报、统一认证鉴权、管控资源同步、功能组件热插拔等

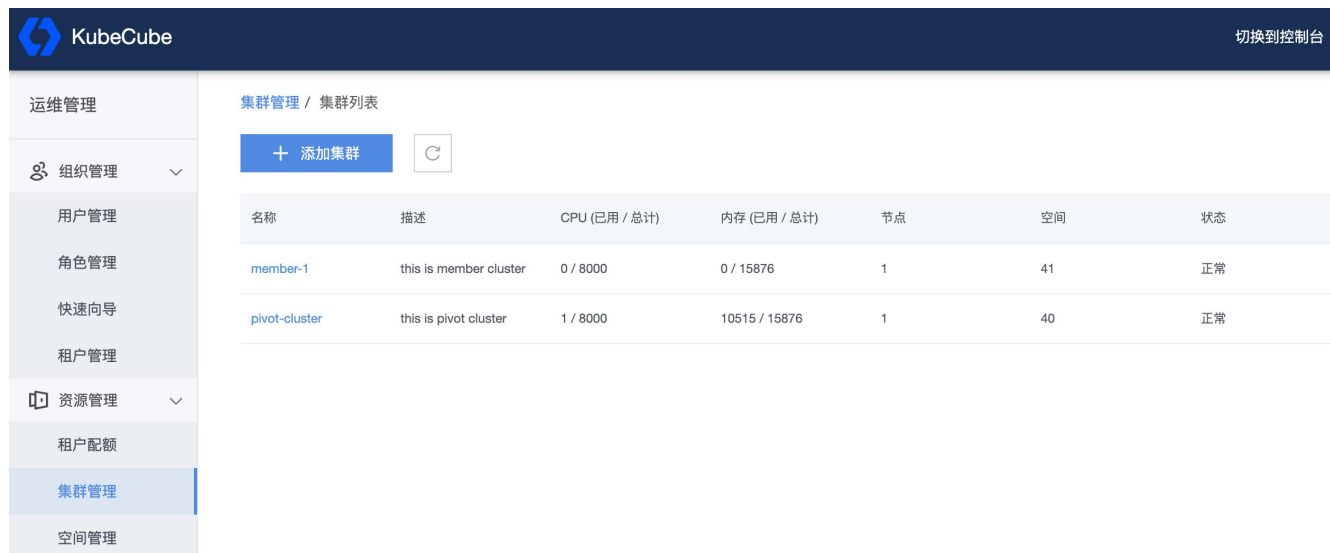
• 功能组件

- 监控: 采用Thanos+Prometheus-operator部署方式
- 日志: filebeats+logSeer
- 审计: 提供多种存储方式，支持原生K8s审计事件+自定义上报

多集群设计及实现

- 为什么需要多集群管理
 - 生产级落地，需要经过多个环境验证，一个集群不满足隔离需求
 - 使用多个集群，如没有统一的用户、权限等管理，会存在重复工作，效率降低且容易错误。

- KubeCube提供多集群统一的
 - 身份识别
 - 访问控制
 - 多租户管理
 - 权限管理



集群管理 / 集群列表

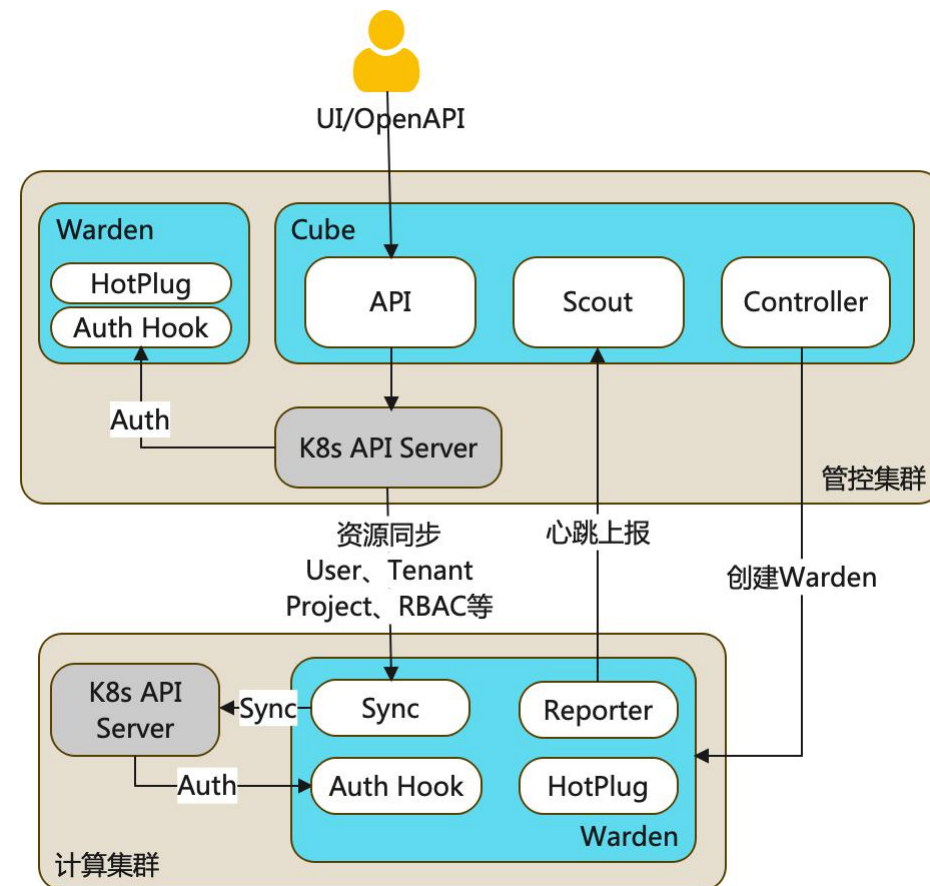
+ 添加集群

名称	描述	CPU (已用 / 总计)	内存 (已用 / 总计)	节点	空间	状态
member-1	this is member cluster	0 / 8000	0 / 15876	1	41	正常
pivot-cluster	this is pivot cluster	1 / 8000	10515 / 15876	1	40	正常

多集群设计及实现

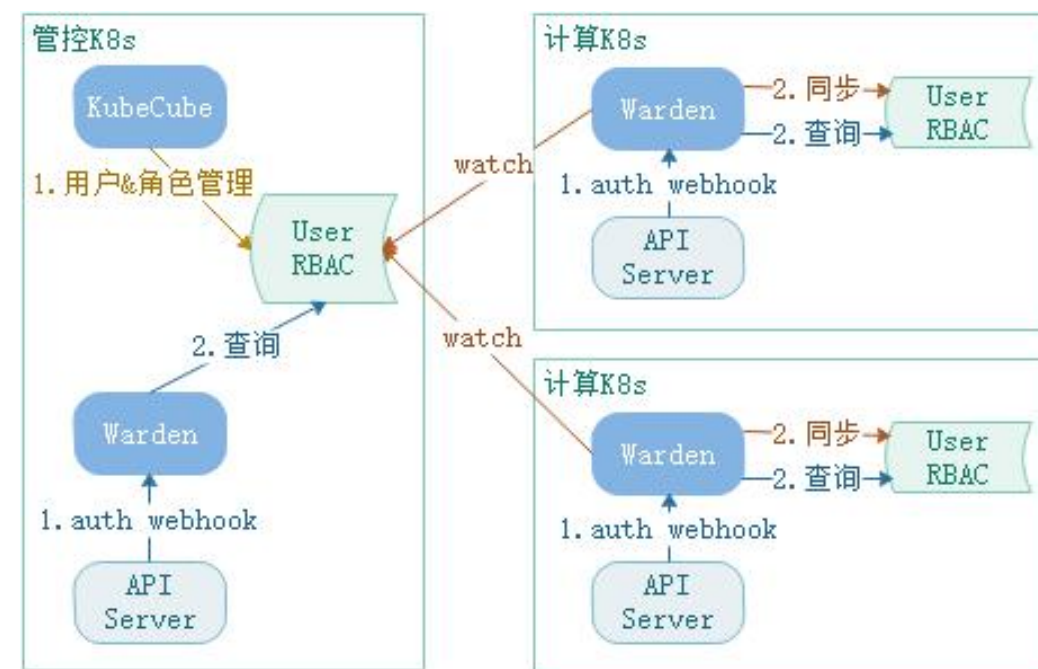
• How

- 添加集群时，自动部署Warden
- 计算集群定时上报心跳，实时掌握集群状态
- 用户、租户、权限等资源跨集群同步
- 认证、鉴权各集群独立完成，集群高度自治



多集群统一访问控制

- 如何统一
 - 权限系统基于K8s原生RBAC
 - 权限信息实现跨集群同步（存储分布式）
 - 鉴权服务跨集群部署（服务分布式）
- 其他能力
 - 集群自治：管控与计算网络中断时，仅认证及权限信息同步受影响，认证&鉴权本集群内通信，无影响
 - 支持多种访问方式：使得在保持KubeCube认证鉴权的前提下直接暴露原生K8s API成为可能。用户已有工具可无缝使用



多租户设计及实现

- 为什么设计多租户
 - 容器化改造的很大一部分原因是希望降低成本，不同部门/团队共享计算资源是首选
 - 共享的同时需要保持基本的资源配额、权限隔离，防止资源抢占影响业务及操作其他团队应用

多租户设计及实现

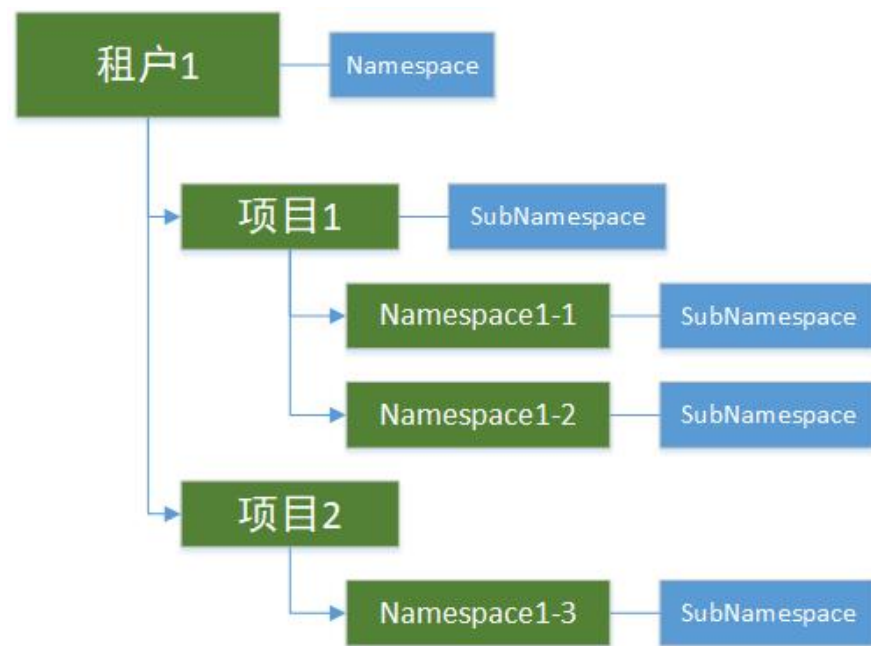
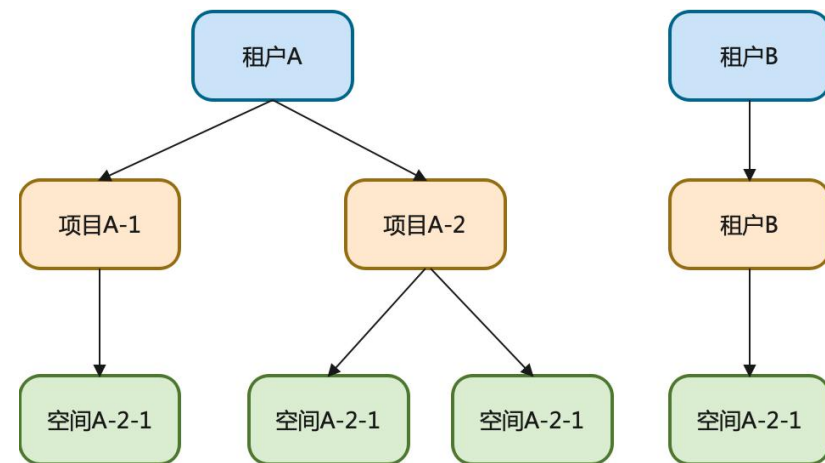
- 模型设计

- 三级关系模型：租户、项目、空间
- 每层均为 1:N 的关系

- 从之前客户需求看，三层模型已经能满足需求

- 实现

- 层级关系基于HNC实现，主要使用了层级关系及权限传播能力



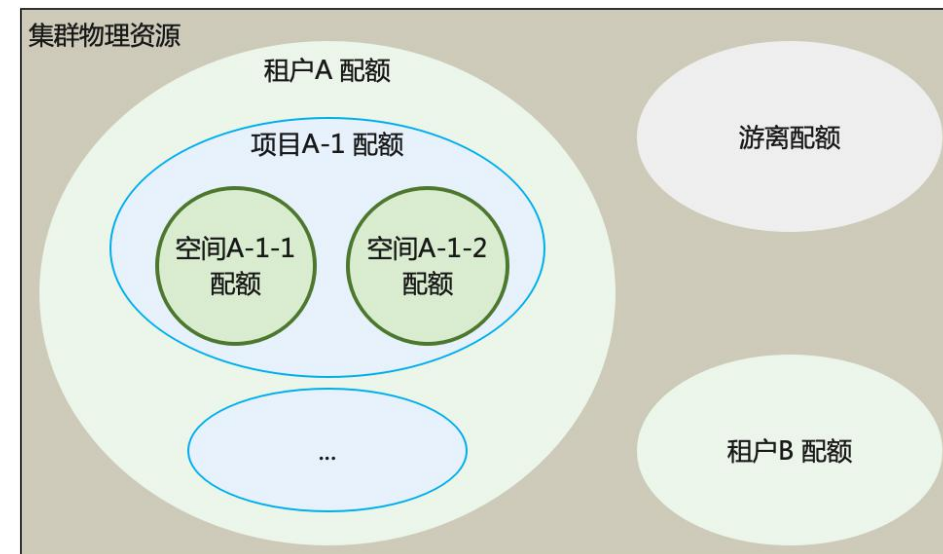
多租户设计及实现

• 权限隔离

- 内置系统管理员、租户管理员、项目管理员及普通用户
- 角色定义及授权使用原生RBAC

• 配额隔离

- 配额由租户层级开始，依次细化至空间粒度
- 各级通过WebHook保证隔离性
- 产品设计角度，屏蔽项目配额，使项目成为逻辑概念，简化使用



轻量化部署及热插拔

- 在以往的客户对接中，有不少客户已有部分系统的建设，如日志等基础服务，并不需要全部的组件
- 为满足不同客户的功能需求，提供了功能最小化安装，其他功能可通过配置热插拔
- 热插拔功能支持扩展

最小功能集

- K8s资源管理
- 多租户
- 多集群
- 监控、告警

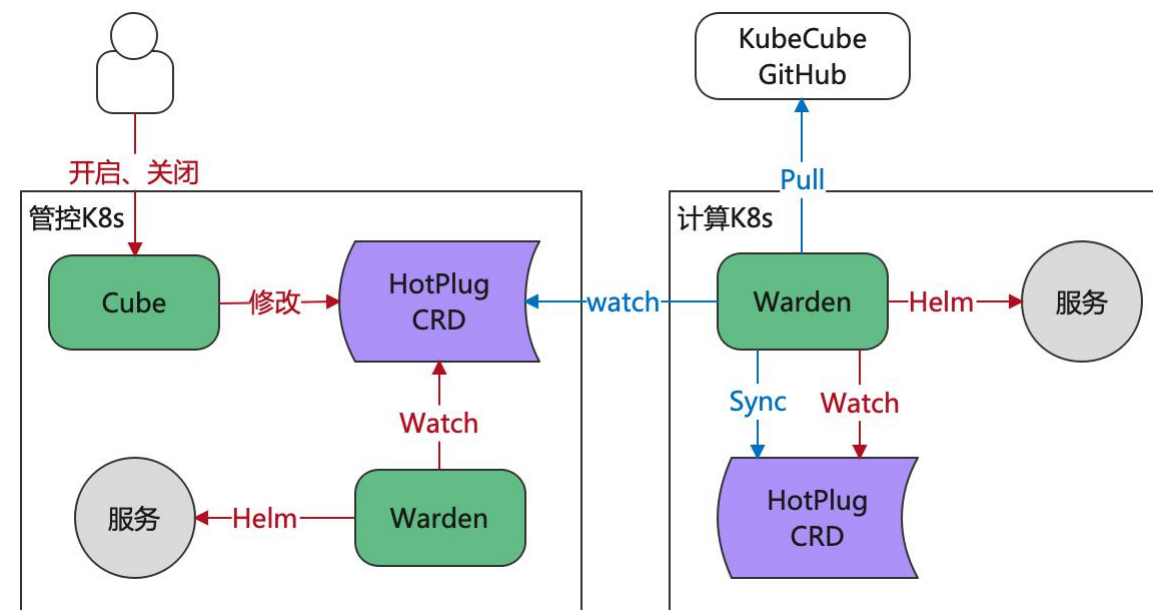
热插拔功能

- 日志
- 操作审计

轻量化部署及热插拔

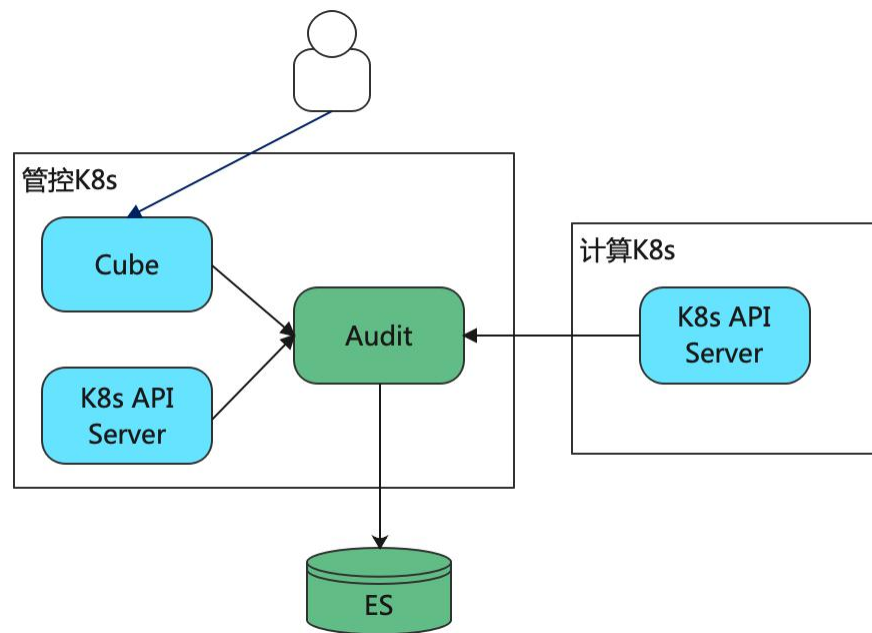
- 配置跨集群同步
 - Warden启动后，会从GitHub拉取Helm部署包
 - Warden实时同步管控集群的HotPlug配置

- 热插拔核心逻辑
 - Warden监听HotPlug变更
 - 渲染参数
 - 通过Helm部署或卸载相关服务



操作审计设计及实现

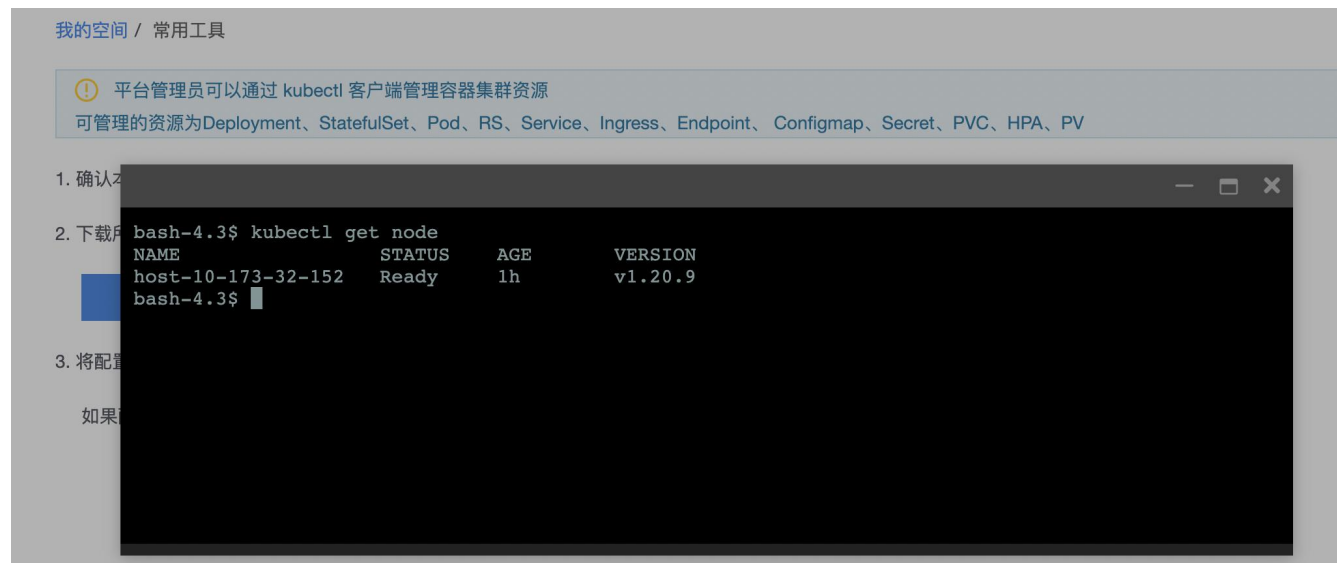
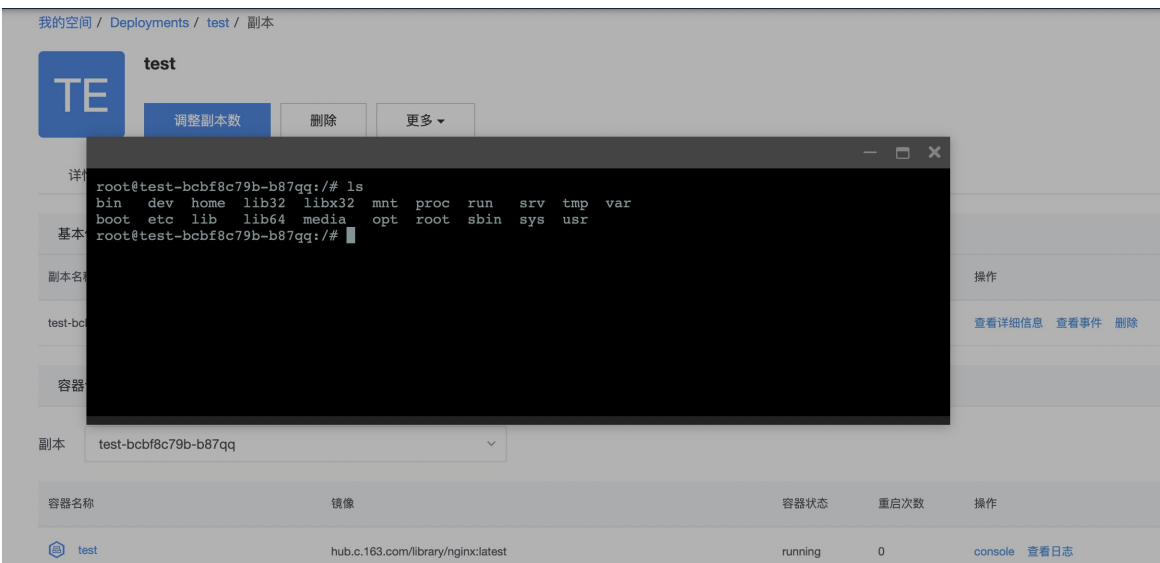
- 审计服务存储后端目前支持ES，可对接用户已有ES
- 审计内容包含
 - KubeCube自定义操作
 - K8s 原生操作审计



其他功能

- 在线工具

- WebConsole: 页面快速访问Pod, 用于排查问题及debug
- CloudShell: 页面快速访问K8s, 提供在线kubectl, 多集群操作更方便
- 集群访问证书在线下载



KubeCube微信交流群

- 欢迎大家进群交流

