

Kubernetes

xbZhong

2025-10-18

[本页PDF](#)

[Kubernetes 文档 | Kubernetes](#)

概念

Kubernetes是一个容器编排框架，提供了一个可弹性运行分布式系统的框架

它具有以下功能：

- 服务发现和负载均衡
- 存储编排
- 自动部署和回滚
- 自我修复
- 等等……

架构

Kubernetes架构

典型的MASTER-WORKER架构

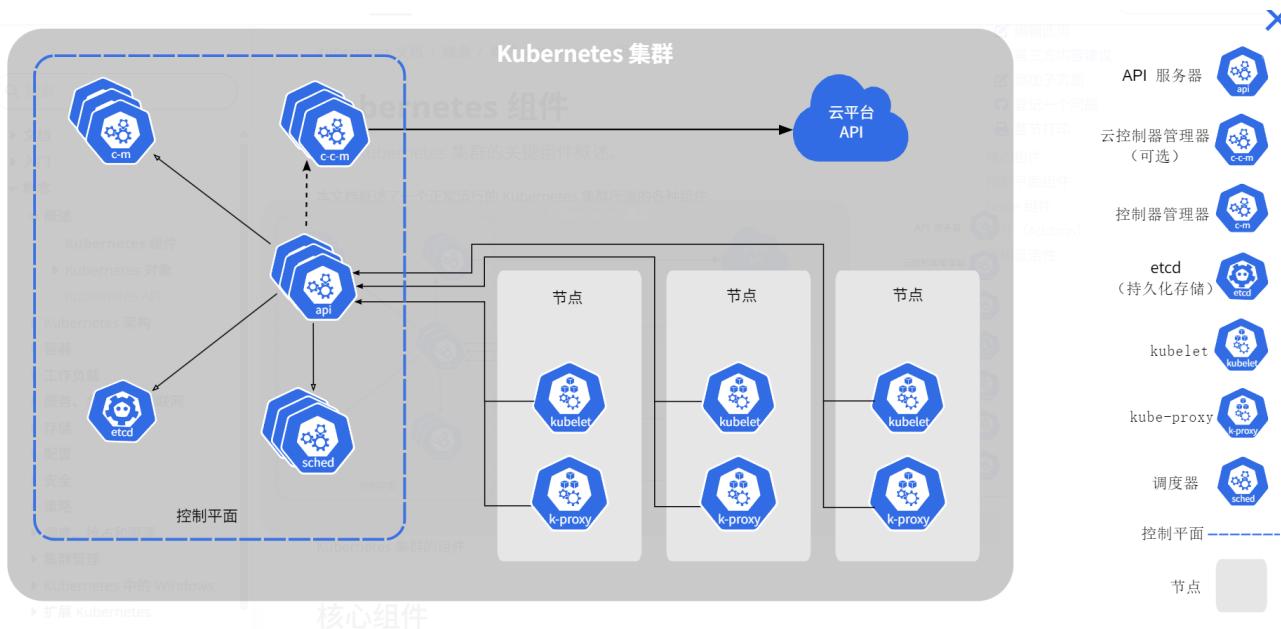


image-20251017150052951

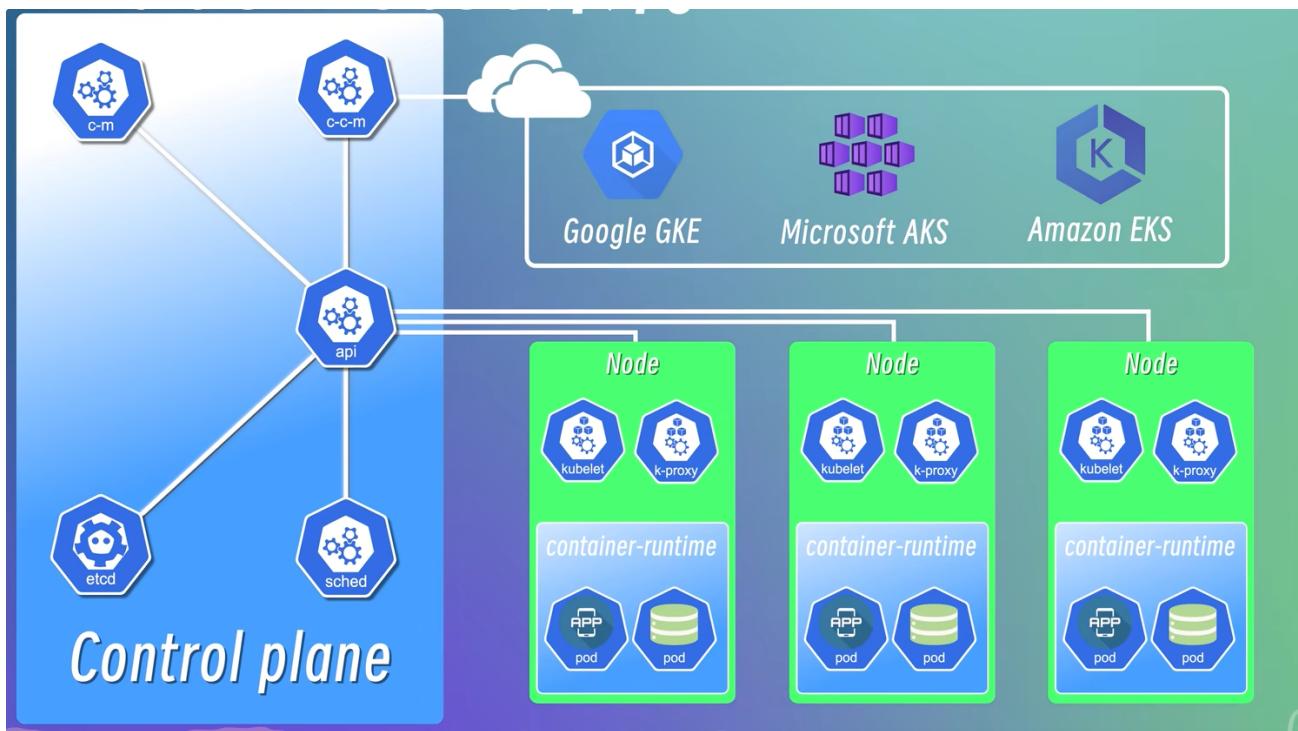


image-20251018161042945

• 控制平面

- `kube-apiserver`: 负责**处理接受外来请求的工作**，是控制平面的前端
- `etcd`: **分布式键值存储**，存储集群状态数据
- `kube-scheduler`: 负责**监视新创建的、未指定运行节点（node）的Pods**，并选择节点让Pod在上面运行
- `kube-controller-manager`: 运行控制器进程，**多个控制器会在同一个进程运行**
 - 监测集群中**各种资源对象**的状态，并根据状态做出响应
 - 有许多不同类型，在这不进行赘述

• 工作节点

- `kubelet`: 会在集群中每个节点上运行，**保证容器（containers）都运行在Pod中**
 - 会定期从 `apiserver` 接收新的或者修改后的pod规范，并将pod的工作信息等汇报给 `apiserver`
- `kube-proxy`: 网络代理，实现**服务间访问和负载均衡**
- `Container Runtime`: 负责管理 Kubernetes 环境中容器的执行和生命周期

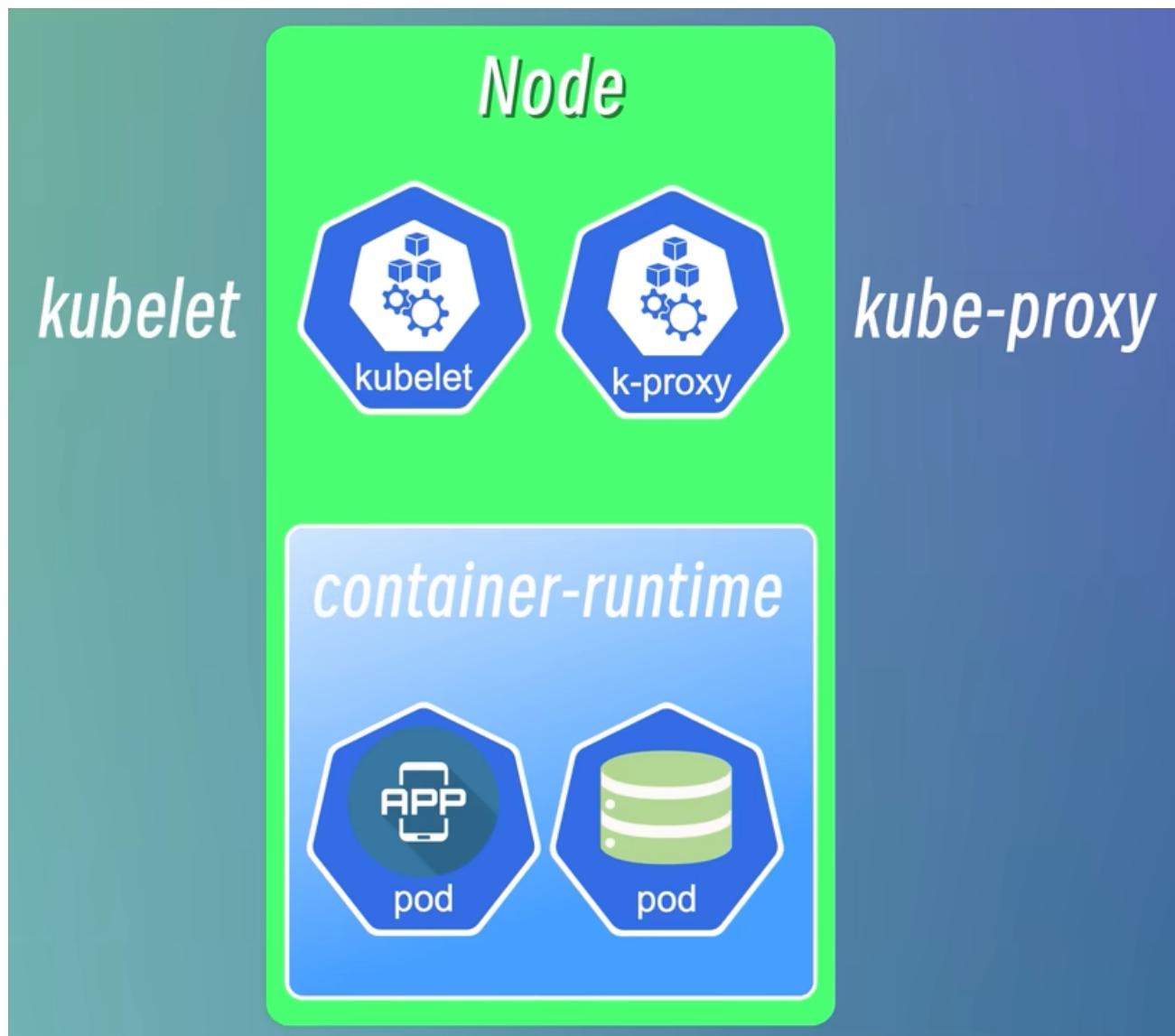


image-20251018160307336

常见资源对象



image-20251018153922491

Node (节点)

Node是K8s的工作单元主机，Pod是它上面运行的工作负载，控制面调度Pod到Node上运行

概念

- k8s集群中的工作机器，可以是**物理机或虚拟机**
- 提供计算资源来运行**pod**
- 由控制面进行**调度和管理**
- 节点上的**组件**包括 `kubelet`、容器运行时以及 `kube-proxy`
- 会为每个Pod创建一个**IP地址**（集群内部IP地址），实现Pod之间的通信

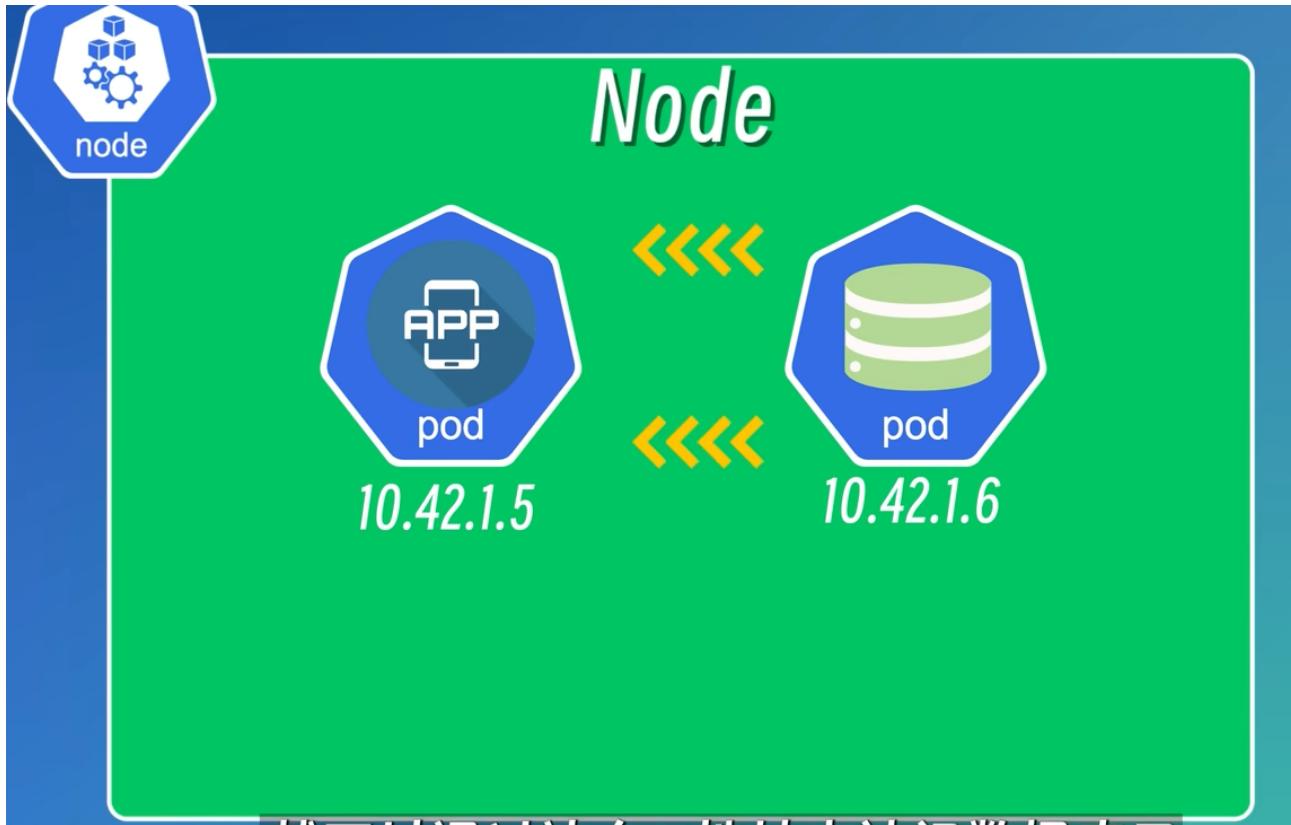


image-20251018151215574

说明

- 节点名称在集群中**唯一**
- 当 `kubelet` 启动参数中 `--register-node=true` 时，节点会**自动向 API Server 注册**
- 节点的状态包括以下内容：
 - 地址：节点的 IP、主机名等
 - 状况：表示节点是否健康、是否可调度
 - 容量与可分配：节点可提供与已分配的资源
 - 信息：节点的操作系统、内核、Kubelet 版本等
- 节点会通过**周期性心跳**上报状态，控制面据此判断节点是否“可用”

Pod

- k8s中的最小部署单元，但不是一个稳定的实体，容易**被创建和销毁**
 - 发生故障的时候k8s会销毁pod，并创建一个新的pod进行替代

- 一个Pod里可以有一个或多个容器，**共享网络和卷**
- 使用多个容器应当是这多个容器**紧密关联**，否则应该拆分为多个Pod部署

Service

为Pod提供稳定的访问入口和服务发现

- 定义服务访问规则和抽象，实际由 `kube-proxy` 实现转发



image-20251018151814388

- 可以提供服务发现，实现负载均衡，类似**网关**
- 可以为**内部服务**和**外部服务**提供访问入口
 - 使用节点的IP地址和端口号映射到 `Service` 的IP地址和端口号是实现**外部服务**

Ingress

集群外部访问集群内服务的统一入口

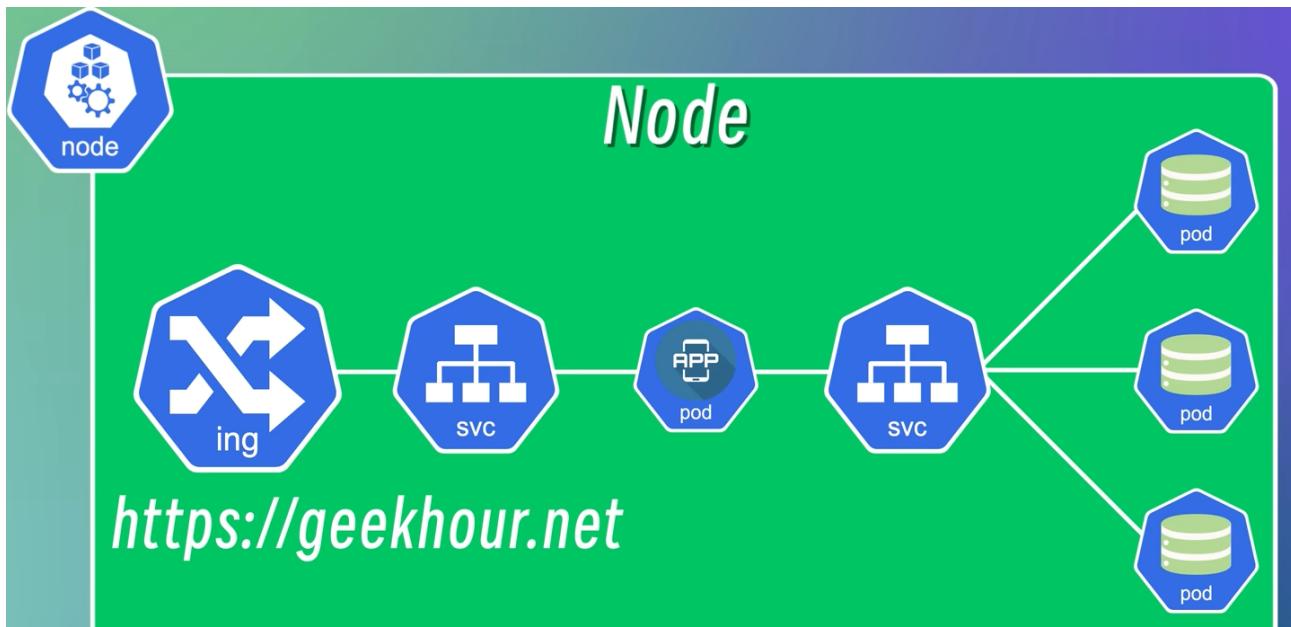


image-20251018152403502

- 可以根据请求的域名和路径转发到不同的服务上
- 可配置不同的转发规则
- 可实现负载均衡，配置SSL证书

ConfigMap

存储**非敏感配置数据**的资源对象，用于将配置从容器镜像中分离出来，使Pod可以动态获取配置

- 存储明文信息，不建议存储敏感信息
- 使**应用程序和配置解耦**，配置变更时不用重新构建镜像
- 方便Pod进行配置的动态获取

Secret

存储**敏感配置数据**的资源对象

- 默认使用**base64编码**存储，不直接明文展示
- 并不是一种加密方式，需要配合k8s其他组件实提高安全性

Volumes

实现Pod数据的持久化存储

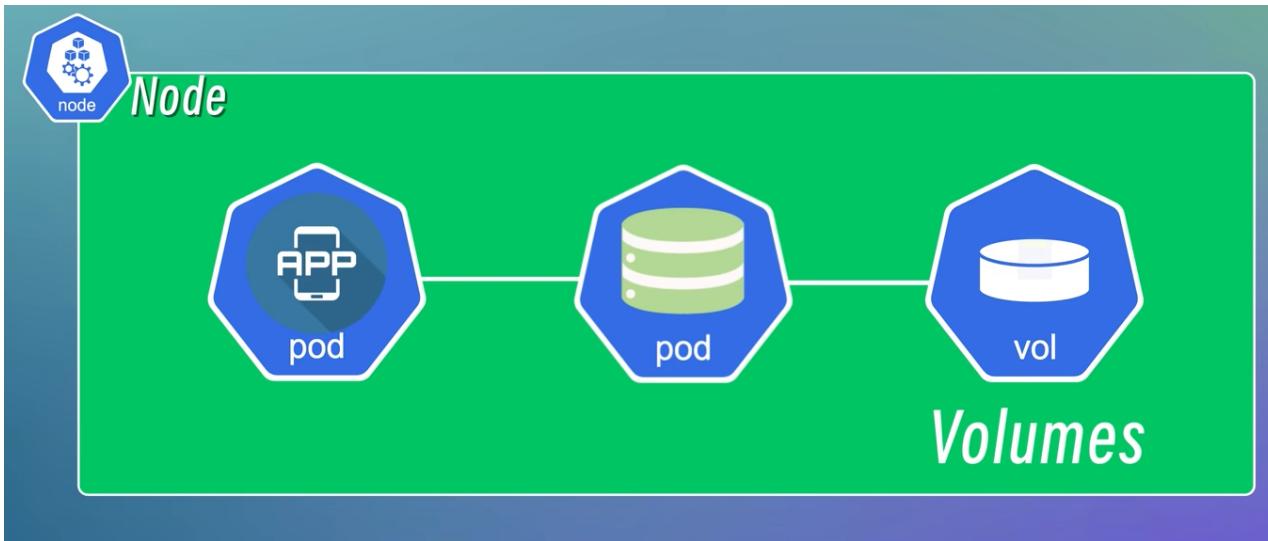


image-20251018153151400

- 可以实现数据持久化，保存应用运行产生的文件，防止文件丢失
- 可以实现容器间共享数据
- 可直接挂载宿主机目录进行存储，也可以绑定外部远程存储

Deployment

负责管理和控制 Pod 的运行与副本数量

- 适合管理无状态应用
- 可自动维持期望副本数，执行Pod的自动重建
- 支持版本回滚、更新

StatefulSet

用于部署和管理有状态应用的控制器

- 适合管理有状态应用
- 可以保证Pod的唯一标识、启动顺序和停止顺序受控、稳定的存储卷

Minikube

迷你版的 Kubernetes，可以在本地部署一个完整的单节点Kubernetes集群