# K3S 简介

k3s 轻量级 Kubernetes，并完全符合 k8s 的发行版，有如下增强功能：

* 打包为单个二进制文件
* 基于 sqlite3 的轻量级存储后端作为默认存储机制。etcd3、MySQL 等任可用。
* 封装在简单的启动程序中，该程序处理很多复杂的 TLS 和选项
* 默认情况下是安全的，对轻量级环境有合理的默认值
* 添加了简单但功能强大的 batteries-included 功能，例如：本地存储提供程序，服务负载均衡，Helm controller 和 Traefik ingress controller
* 所有 control-plane 组件的操作都封装在单个二进制文件和进程中，这使 k3s 可以自动话和管理复杂的集群操作，如颁发证书
* 外部依赖最小化 （仅需 kernel & Cgroup）。

K3s 需要的依赖项：

* containerd
* Flannel
* CoreDNS
* CNI
* 主机实用程序 (iptables, socat, etc)
* Ingress controller (traefik)
* 嵌入式 service loadbalancer
* 嵌入式 network policy controller

# K3S 和 K8S 对比

## 2.1删除

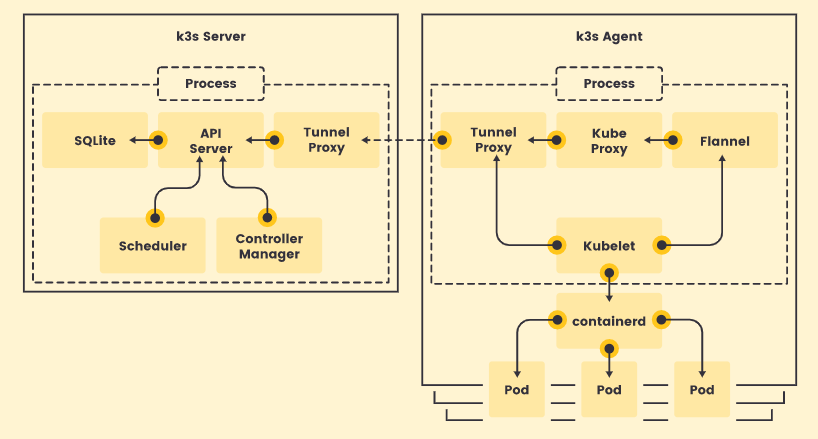
* 过时的功能和非默认功能
* Alpha功能
* 内置的云提供商插件
* 内置的存储驱动
* Docker (可选)

## 2.2新增

* 独立二进制文件，容易部署
* 使用SQLite3作为默认存储，MySQL, Etcd可选
* TLS管理，封装在简单的启动容器中，减少了复杂性
* 自动的Manifest和Helm Chart管理
* containerd, CoreDNS, Flannel

# k3s 架构

## 整体架构

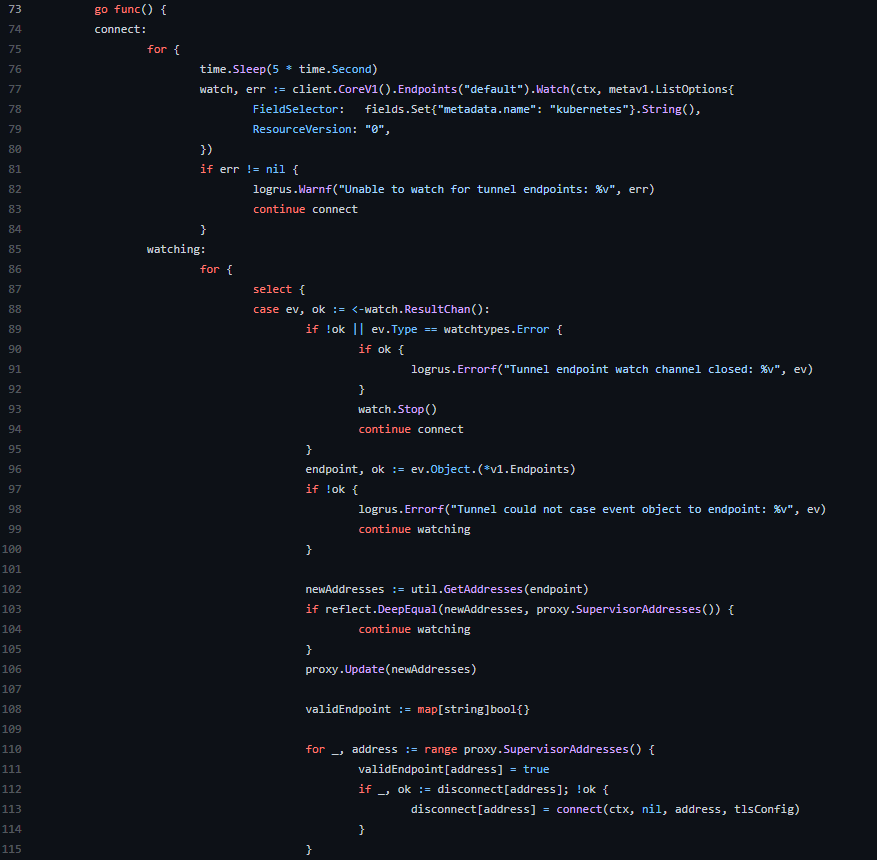


K3s Server: 管理节点，可运行 k3s server 相关命令，包含调度等

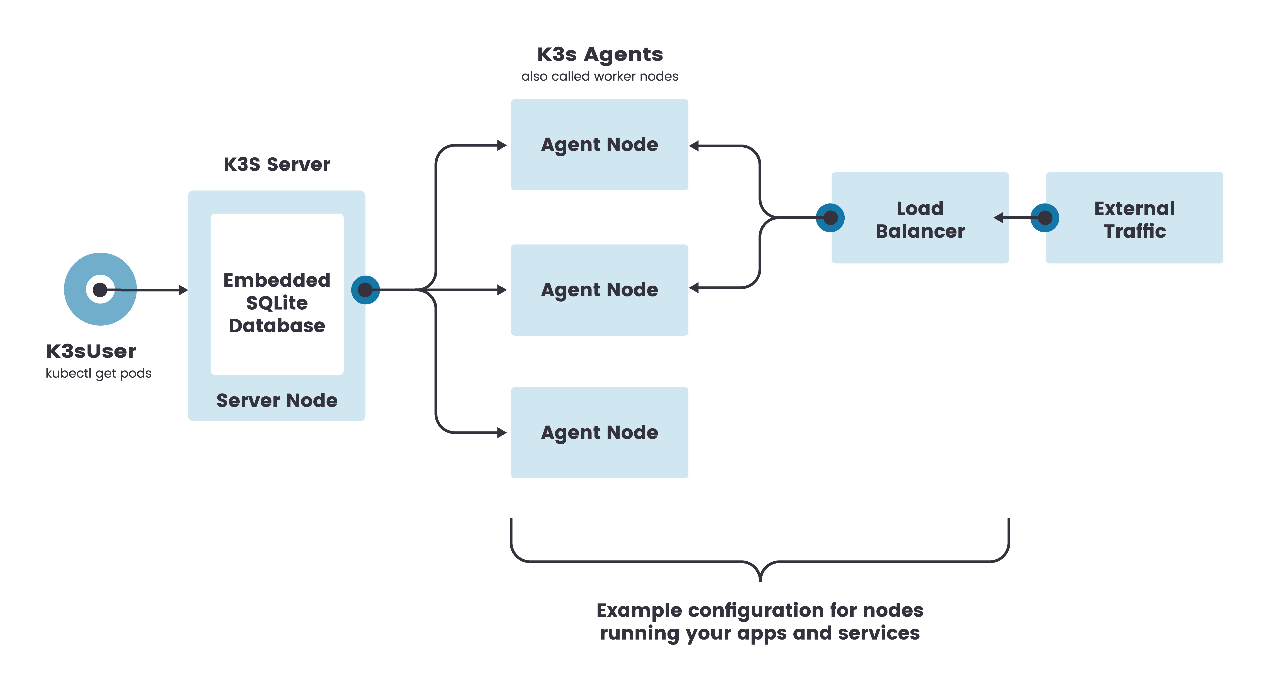
K3s Agent: 工作节点，可运行 k3s agent 相关命令，运行相关容器应用

Tunnel Proxy：通信通道，k3s 新增功能，使用websocket 实现。它简化了 k8s 中，worker节点连接 master 节点，当master 节点信息改变（IP等），需要手动修改 worker 节点配置。

实现代码：https://github.com/k3s-io/k3s/blob/master/pkg/agent/tunnel/tunnel.go

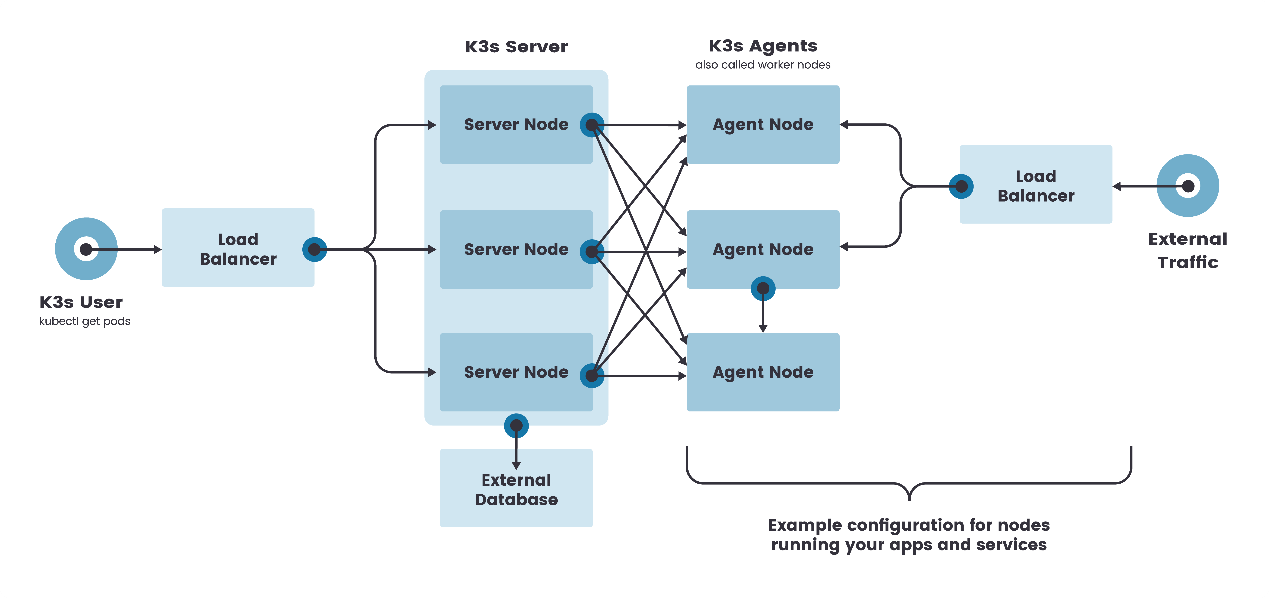


## 单 k3s server 结构



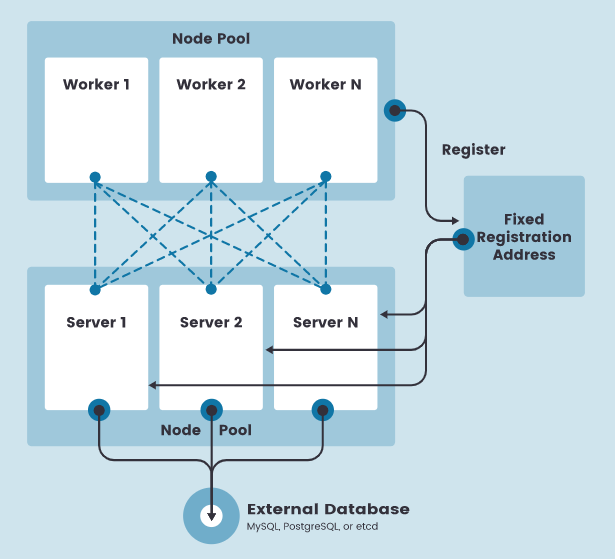
使用嵌入式数据库，不具备高可用性

## 集群 k3s server 结构



外置数据库，高可用

## 3.4 节点注册



**agent 节点注册：**

每个节点必须使用固定的注册地址向 Kubernetes API 注册，注册后，agent 节点直接与其中一个 server 节点建立连接

Agent 节点使用 `k3s agent` 进程发起 websocket 连接注册，连接由作为代理进程一部分运行的客户端负载均衡器维护。

Agent 将使用节点集群 secret 及随机生成的节点密码向 k3s server注册，密码存储在 `/etc/rancher/node/password` (v1.20.2之前 `/var/lib/rancher/k3s/server/cred/node-passwd`)

节点密码 secret 存储在 `kube-system` 命名空间中，名称使用模板 <host>.node-password.k3s