

link: null  
title: 珠峰架构师成长计划  
description: 关闭selinux  
vi /etc/selinux/config  
keywords: null  
author: null  
date: null  
publisher: 珠峰架构师成长计划  
stats: paragraph=18 sentences=21, words=165

## 1. Kubernetes介绍

- Kubernetes是Google在2014年6月开源的一个容器集群管理系统，使用Go语言开发，Kubernetes也叫k8s
- K8s是Google内部一个叫Borg的容器集群管理系统衍生来的，Borg已经在Google大规模生产运行了十年之久
- K8s主要用于自动化部署、扩展和管理容器应用，提供了资源调度、部署管理、服务发现、扩容缩容、监控等一整套功能
- 2015年7月，K8s v 1.0正式发布，截止到2018年1月27日最稳定版本是v1.9.2
- k8s目标是让部署容器化应用简洁高效
- 官网[www.kubernetes.io](http://www.kubernetes.io) (<http://www.kubernetes.io>)

## 2. Kubernetes主要功能

功能 说明 数据卷 Pod中容器之间共享数据，可以使用数据卷 应用程序健康检查 容器内服务可能进程堵塞无法处理请求，可以设置监控检查策略保证应用健壮性 复制应用程序实例 控制器维护着Pod副本数量，保证一个Pod或一组同类的Pod数量始终可用 弹性伸缩 根据设定的指标(CPU利用率)自动缩放Pod副本数 服务发现 使用环境变量或DNS服务插件保证容器中程序发现Pod入口访问地址 负载均衡 一组Pod副本分配一个私有的集群IP地址，负载均衡转发到后端容器。在集群内部其它Pod可通过这个ClusterIP访问应用 滚动更新 更新服务不中断，一次更新一个Pod, 而不是删除整个服务 服务编排 通过文件描述部署服务，使得应用程序部署变的更高效 资源监控 Node节点组成cAdvisor资源收集工具，可通过Heapster汇总整个集群节点资源数据，然后存储到InfluxDB时序数据库，再由Grafana展示 提供认证和授权 支持角色访问控制(RBAC)认证授权等策略

## 3. 基本对象概念

功能 说明 Pod Pod是最小的部署单元，一个Pod有一个或多个容器组成，Pod中容器共享存储和网络，在同一个台Docker主机上运行 Service Service是一个应用程序抽象，定义了Pod逻辑集合和访问这个Pod集合的策略。Service代理Pod集合对外表现是为一个访问入口，分配一个集群IP地址，来自这个IP的请求将负载均衡转发后端Pod中的容器。Service通过Label Selector选择一组Pod提供服务 Volume 数据卷，共享Pod中容器使用的数据 Namespace 命名空间将对象逻辑上分配到不同Namespace,可以是不同的项目、用户等区管理，并设定控制策略，从而实现多租户。命名空间也称为虚拟集群 Label 标签用于区分对象(比如Pod、Service),键/值对存在; 每个对象可以有多个标签，通过标签关联对象

## 4. 高层抽象

功能 说明 ReplicaSet 下一个Replication Controller,确保任何给定时间指定的Pod副本数量，并提供声明式更新等功能。RC与RS唯一区别就是label selector支持不同，RS支持新的基于集合的标签，RC仅支持基于等式的标签 Deployment Deployment是一个更高层次的API对象，它管理ReplicaSets和Pod,并提供声明式更新等功能。官方建议使用Deployment管理ReplicaSets,而不是直接使用ReplicaSets,这意味着可能永远不需要直接操作ReplicaSet对象 StatefulSet StatefulSet适合持久性的应用程序，有唯一的网络标识符(IP),持续存储，有序的部署、扩展、删除和滚动更新 DaemonSet DaemonSet确保所有(或一些)节点运行同一个Pod。当节点加入Kubemets集群中，Pod会被调度到该节点上运行，当节点从集群中移除时，DaemonSet的Pod会被删除。删除DaemonSet会清理它所有创建的Pod. Job 一次性任务，任务完成后Pod销毁，不再重新启动新容器，还可以任务定时运行

## 5. 系统架构和组件功能

功能 说明 kube-apiserver Kubernetes API,集群的统一入口，各组件协调者，以HTTP API提供接口服务，所以对资源资源的增删改查和监控操作都交给APIServer处理后并提交给Etcd存储 kube-controller-manager 处理集群中常规后台任务，一个资源对应一个控制器，而ControllerManager就是负责管理这些控制器的 kube-scheduler 根据调度算法为新创建的Pod选择一个Node节点

功能 说明 kubelet kubelet是Master在Node节点上的Agent,管理本机运行容器的生命周期，比如创建容器，Pod挂载数据卷、下载secret、获取容器和节点状态等工作。kubelet将每个Pod转换成一组容器 kube-proxy 在Node节点上实现Pod网络代理，维护网络规划 和四层负载均衡工作 docker或rocket/rkt 运行容器

功能 说明 etcd 分布式键值存储系统，用于保持集群状态，比如Pod、Service等对象信息

## 6. 集群部署

- 环境规划
- 安装Docker
- 自签TLS证书
- 部署Etcd集群
- 部署Flannel网络
- 创建Node节点 kubeconfig文件
- 获取K8S二进制包
- 运行Master组件
- 运行Node组件
- 查询集群状态
- 启动一个测试示例
- 部署WebUI(Dashboard)

软件 版本 Linux操作系统 CentOS7.4\_x64 Kubernetes 1.9 Docker 17.12-ce Etcd 3.0 角色 IP 组件 master 192.168.0.211 kube-apiserver、kube-container-manager、kube-scheduler、etcd node01 192.168.0.212 kubelet、kube-proxy、docker、flannel、etcd node02 192.168.0.213 kubelet、kube-proxy、docker、flannel、etcd 组件 作用 kube-apiserver kube-container-manager kube-scheduler kubelet、kube kube-proxy docker 容器 flannel 容器之间的跨主机通信 etcd 用于集群间通信

关闭selinux vi /etc/selinux/config

```
SELINUX=disabled
```

cat /etc/docker/daemon.json