Kubernetes容器云平台入门与进阶

讲师介绍

李振良（阿良）

资深运维工程师，8年运维实战经验，51CTO知名博主。曾就职在IDC，大数据，金融行业，现任职奇虎360公司。曾主导自动化运维与K8S容器平台建设，现管理近800台服务器，主要负责360浏览器业务与容器化迁移。

技术博客：http://blog.51cto.com/lizhenliang

阿良微信

入门须知

- 熟悉Linux基础命令
- 熟悉Docker基本管理
- 了解SSL证书工作原理
- 了解负载均衡工作原理（L4/L7）
- 了解集群，分布式概念
- 了解域名解析原理
- 了解网络协议

第 1 章 Kubernetes概述

1. Kubernetes是什么
2. Kubernetes特性
3. Kubernetes集群架构与组件
4. Kubernetes核心概念

Kubernetes是什么

- Kubernetes是Google在2014年开源的一个容器集群管理系统，Kubernetes简称K8S。
- K8S用于容器化应用程序的部署，扩展和管理。
- K8S提供了容器编排，资源调度，弹性伸缩，部署管理，服务发现等一系列功能。
- Kubernetes目标是让部署容器化应用简单高效。

官方网站：http://www.kubernetes.io

Kubernetes特性

- **自我修复**

在节点故障时重新启动失败的容器，替换和重新部署，保证预期的副本数量；杀死健康检查失败的容器，并且在未准备好之前不会处理客户端请求，确保线上服务不中断。

- **弹性伸缩**

使用命令、UI或者基于CPU使用情况自动快速扩容和缩容应用程序实例，保证应用业务高峰并发时的高可用性；业务低峰时回收资源，以最小成本运行服务。

- **自动部署和回滚**

K8S采用滚动更新策略更新应用，一次更新一个Pod，而不是同时删除所有Pod，如果更新过程中出现问题，将回滚更改，确保升级不受影响业务。

- **服务发现和负载均衡**

K8S为多个容器提供一个统一访问入口（内部IP地址和一个DNS名称），并且负载均衡关联的所有容器，使得用户无需考虑容器IP问题。

- **机密和配置管理**

管理机密数据和应用程序配置，而不需要把敏感数据暴露在镜像里，提高敏感数据安全性。并可以将一些常用的配置存储在K8S中，方便应用程序使用。

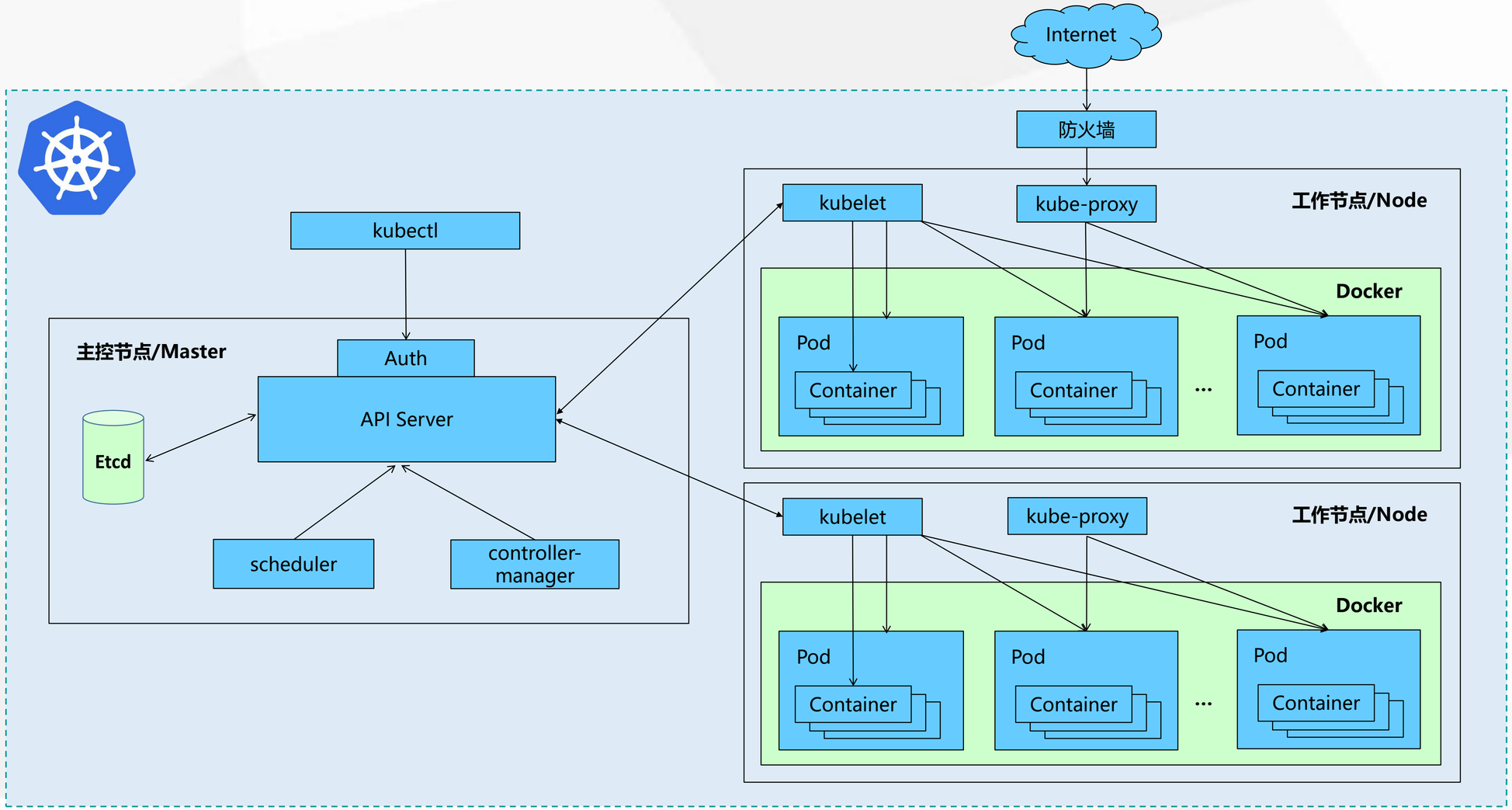
- **存储编排**

挂载外部存储系统，无论是来自本地存储，公有云（如AWS），还是网络存储（如NFS、GlusterFS、Ceph）都作为集群资源的一部分使用，极大提高存储使用灵活性。

- **批处理**

提供一次性任务，定时任务；满足批量数据处理和分析的场景。

Kubernetes集群架构与组件



Kubernetes集群架构与组件

Master组件

- **kube-apiserver**

Kubernetes API，集群的统一入口，各组件协调者，以RESTful API提供接口服务，所有对象资源的增删改查和监听操作都交给APIServer处理后再提交给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，可以任意部署,可以部署在同一个节点上,也可以部署在不同的节点上。

- **etcd**

分布式键值存储系统。用于保存集群状态数据，比如Pod、Service等对象信息。

Node组件

- **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，维护网络规则和四层负载均衡工作。

- **docker或rocket**

容器引擎，运行容器。

Kubernetes核心概念

- **Pod**
  - 最小部署单元
  - 一组容器的集合
  - 一个Pod中的容器共享网络命名空间
  - Pod是短暂的
- **Controllers**
  - ReplicaSet： 确保预期的Pod副本数量
  - Deployment： 无状态应用部署
  - StatefulSet： 有状态应用部署
  - DaemonSet： 确保所有Node运行同一个Pod
  - Job： 一次性任务
  - Cronjob： 定时任务

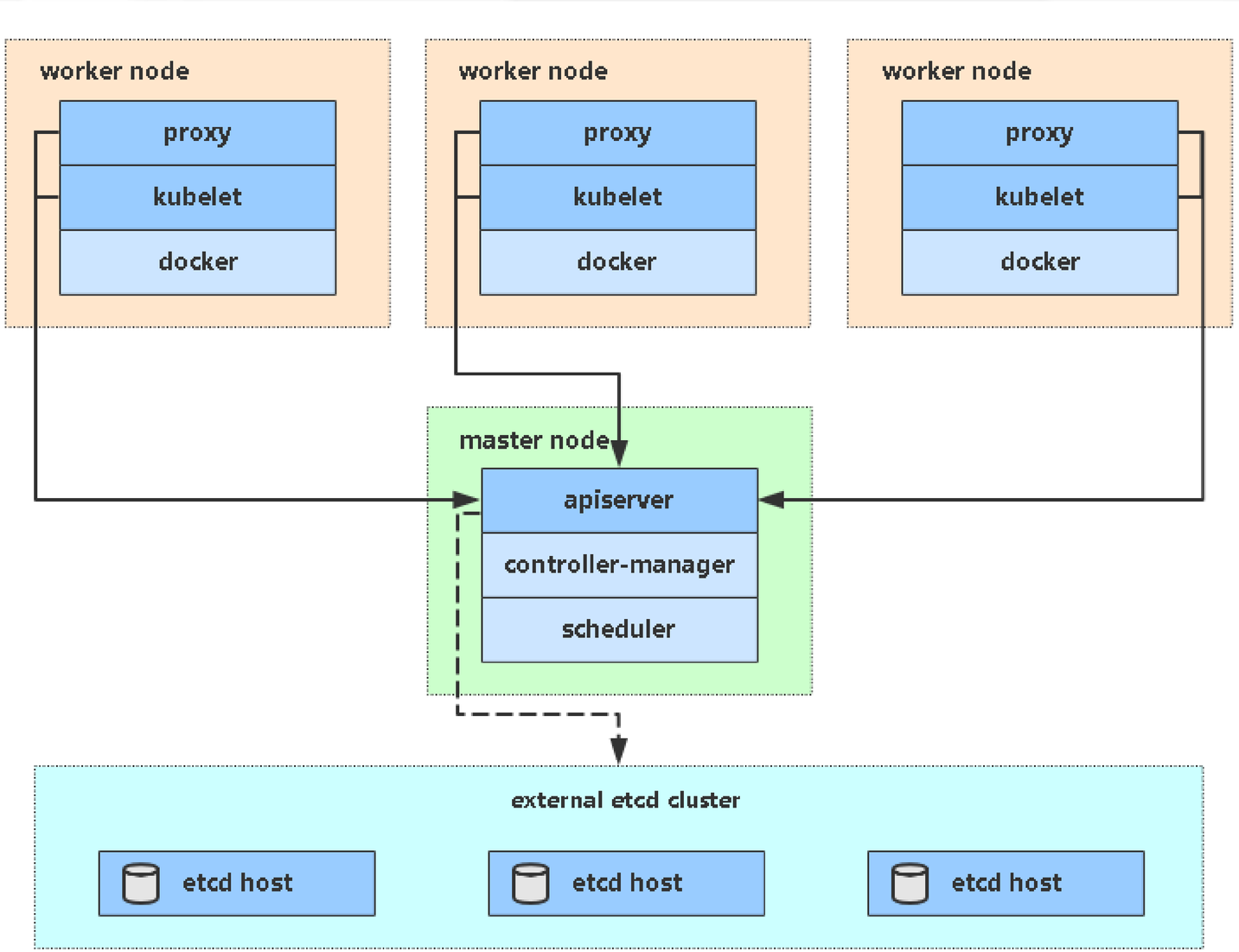
  更高级层次对象，部署和管理Pod
- **Service**
  - 防止Pod失联
  - 定义一组Pod的访问策略

- **Label：** 标签，附加到某个资源上，用于关联对象、查询和筛选
- **Namespace：** 命名空间，将对象逻辑上隔离

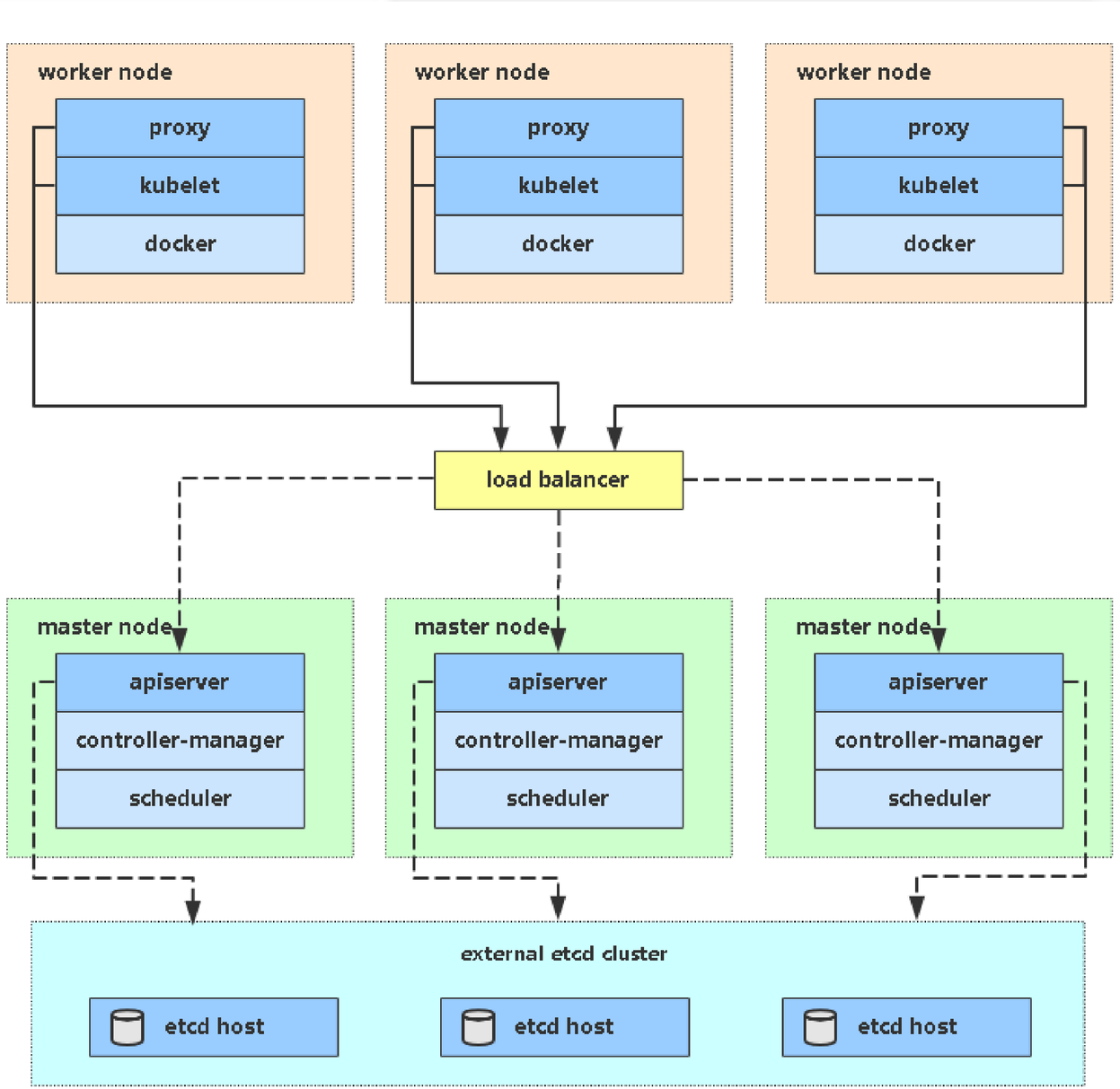
第 2 章 搭建一个完整的Kubernetes集群

1. 生产环境K8S平台规划
2. 服务器硬件配置推荐
3. 官方提供三种部署方式
4. 为Etcd和APISever自签SSL证书
5. Etcd数据库集群部署
6. 部署Master组件
7. 部署Node组件
8. 部署K8S集群网络
9. 部署Web UI（Dashboard）
10. 部署集群内部DNS解析服务（CoreDNS）

生产环境K8S平台规划 – 单Master集群



生产环境K8S平台规划 – 多Master集群（HA）



生产环境K8S平台规划

角色	IP	组件
k8s-master1	192.168.31.63	kube-apiserver kube-controller-manager kube-scheduler etcd
k8s-master2	192.168.31.64	kube-apiserver kube-controller-manager kube-scheduler
k8s-node1	192.168.31.65	kubelet kube-proxy docker etcd
k8s-node2	192.168.31.66	kubelet kube-proxy docker etcd
Load Balancer（Master）	192.168.31.61 192.168.31.60 (VIP)	Nginx L4
Load Balancer（Backup）	192.168.31.62	Nginx L4

服务器硬件配置推荐

实验环境	k8s master/node	2C2G+	
测试环境	k8s-master	CPU	2核
		内存	4G
		硬盘	20G
	k8s-node	CPU	4核
		内存	8G
		硬盘	20G
生产环境	k8s-master	CPU	8核
		内存	16G
		硬盘	100G
	k8s-node	CPU	16核
		内存	64G
		硬盘	500G

官方提供的三种部署方式

- **minikube**

Minikube是一个工具，可以在本地快速运行一个单点的Kubernetes，仅用于尝试Kubernetes或日常开发的用户使用。

部署地址：https://kubernetes.io/docs/setup/minikube/

- **kubeadm**

Kubeadm也是一个工具，提供kubeadm init和kubeadm join，用于快速部署Kubernetes集群。

部署地址：https://kubernetes.io/docs/reference/setup-tools/kubeadm/kubeadm/

- **二进制**

推荐，从官方下载发行版的二进制包，手动部署每个组件，组成Kubernetes集群。

下载地址：https://github.com/kubernetes/kubernetes/releases

为Etcd和APIServer自签SSL证书

使用cfssl工具自签证书。

Etcd数据库集群部署

◆ **二进制包下载地址**

https://github.com/etcd-io/etcd/releases

◆ **查看集群状态**

```
/opt/etcd/bin/etcdctl \
--ca-file=/opt/etcd/ssl/ca.pem --cert-file=/opt/etcd/ssl/server.pem --key-file=/opt/etcd/ssl/server-key.pem \
--endpoints="https://192.168.31.63:2379,https://192.168.31.65:2379,https://192.168.31.66:2379" \
cluster-health
```

部署Master组件

1. kube-apiserver
2. kube-controller-manager
3. kube-scheduler

配置文件 -> systemd管理组件 -> 启动

部署Node组件

1. docker
2. kubelet
3. kube-proxy

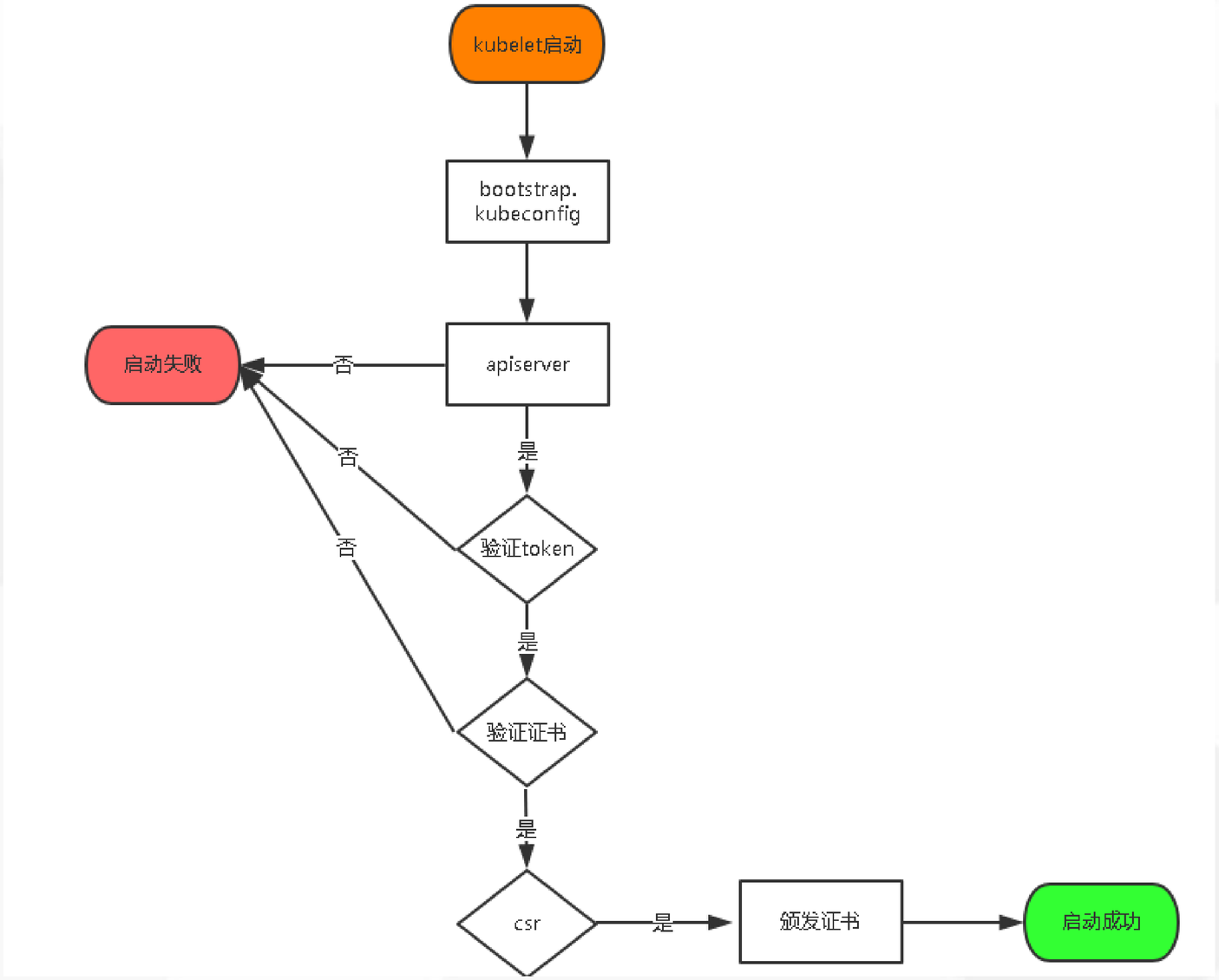
配置文件 -> systemd管理组件 -> 启动

部署Node组件

访问和工具层	帮助用户更高效的完成任务，包括Web控制台、RESTful API、CI/CD、监控管理、日志管理等...
PaaS服务层	为开发、测试和运维人员提供统一的平台服务
容器编排层	 Kubernetes
容器引擎层	 Docker
IaaS基础设施层	提供基础运行环境，例如虚拟机、物理机、网络、存储、数据库、公有云等...

分层结构

部署Node组件



TLS Bootstrapping 机制流程（kubelet）

部署K8S集群网络

CNI插件：

https://github.com/containernetworking/plugins/releases

常见CNI网络部署：

https://kubernetes.io/docs/setup/production-environment/tools/kubeadm/create-cluster-kubeadm/

部署一个测试示例

```
kubectl create deployment nginx --image=nginx
kubectl get pod
kubectl expose deployment nginx --port=80 --target-port=80 --type=NodePort
kubectl get svc nginx
```

部署Web UI & DNS

Web UI：

https://github.com/kubernetes/dashboard

https://kubernetes.io/docs/tasks/access-application-cluster/web-ui-dashboard/

DNS：

https://github.com/kubernetes/kubernetes/tree/master/cluster/addons/dns/coredns

Master高可用架构