## Kubelet启动过程

TLS BootStrapping 官方文档：

<https://kubernetes.io/docs/reference/command-line-tools-reference/kubelet-tls-bootstrapping/#initialization-process>

* 1. 查找kubeconfig文件，文件一般位于/etc/kubernetes/kubelet.kubeconfig
  2. 从kubeconfig文件中检索APIServer的URL和证书
  3. 然后去和APIServer进行交互

查看kubelet.kubeconfig证书有效期：

首先对kubelet.kubeconfi的certificate-authority-data字段进行解密：

echo "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUQ0akNDQXNxZ0F3SUJBZ0lVVXdzUHFhWGxWVUdWb3lvYkZyZFpIRmZIQk04d0RRWUpLb1pJaHZjTkFRRUwKQlFBd2R6RUxNQWtHQTFVRUJoTUNRMDR4RURBT0JnTlZCQWdUQjBKb

GFXcHBibWN4RURBT0JnTlZCQWNUQjBKbAphV3BwYm1jeEV6QVJCZ05WQkFvVENrdDFZbVZ5Ym1WMFpYTXhHakFZQmdOVkJBc1RFVXQxWW1WeWJtVjBaWE10CmJXRnVkV0ZzTVJNd0VRWURWUVFERXdwcmRXSmxjbTVsZEdWek1CNFhEVEl3TURrd05UQXlNVFF3TUZvWERUSTEKTU

Rrd05EQXlNVFF3TUZvd2R6RUxNQWtHQTFVRUJoTUNRMDR4RURBT0JnTlZCQWdUQjBKbGFXcHBibWN4RURBTwpCZ05WQkFjVEIwSmxhV3BwYm1jeEV6QVJCZ05WQkFvVENrdDFZbVZ5Ym1WMFpYTXhHakFZQmdOVkJBc1RFVXQxClltVnlibVYwWlhNdGJXRnVkV0ZzTVJNd0VRWUR

WUVFERXdwcmRXSmxjbTVsZEdWek1JSUJJakFOQmdrcWhraUcKOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQXUrV291WmpLS1RmUnMwbkY1NTdCUk8wVTlkSUVvRVlydEFHawp5aWZET0s5MGdNeDBRTzlhMGpJOXd0OFlNM284cmpGcmVjdWJ5Q1RzK1JSMTFmd0EvdGIwc0kr

U1NlRVVYVGo3ClFlaklVK1pBTzdzNGRvM2hveGYrbzBsS2tPbVIvTVZTa2NYUFl2ZzJhc0tGTnI0NkZCSVFZRkh4NzJCcGIreFMKVmViMWhqNTFXTVBmSkdZcW4vRWZYS3hlb3dvNEE5WXJHdXoxVDVGWVNtcjJWa3VIOXEwajRsRE9TbkQ4WnF0eQpDZW1HZVI5M1IraklmTkxCN

DZHZC9vVm9veEJYb0dPemlvUURLZDM1QllXaExvZzVmT2cyMko4ZmNrTEI0bk9wCnBjb24xZ01vOGtlS0xZSlBxTmp6ZGFuL0hNN1dtaElMb2JIUVF3V0NjK1hjTkxnaUxRSURBUUFCbzJZd1pEQU8KQmdOVkhROEJBZjhFQkFNQ0FRWXdFZ1lEVlIwVEFRSC9CQWd3QmdFQi93SU

JBakFkQmdOVkhRNEVGZ1FVN3NuYQoweGhZUU5wNDJ0ZzhmdGxjVVdiSlE3b3dId1lEVlIwakJCZ3dGb0FVN3NuYTB4aFlRTnA0MnRnOGZ0bGNVV2JKClE3b3dEUVlKS29aSWh2Y05BUUVMQlFBRGdnRUJBTEFGdUdiTmNoTGk4aFdWbURRUGlIR2E0Z2JzdG1NWjZ1eC8KVnNqVnF

IcnkrMXdXcm8rWDc1SDJ6QXV3d3RIMHFYUGhKZjRid2hWMTREb1k0eGpVYW9aTjF0ejU3VEpQUXczNApuT3lRa1VmOFhZcDJpK1BBczZ6ZUgrVUZjQUJqeGIrdFRuYlU0MENqakx6L2ZaRjJURkxscWtTUzVnOSttQnkrCkx1bkVGY1E5Z1hLaHFvbWJ5TkpNcytsY0hacFJ6YmF4

NE9oeTRZTU1qNENaQjNKZG9TUDR5dkRQMnZWNXZvbmcKcU0rUHl3SVl2TjhUN3hFeTIrbTZxWGNla3gyRmlVeFJDeTMyWkRGbGQrTDhFamdrelN2YVNpQ2thWjF6TlczRwpZWTBFWkhGcGM2S1lrdlJDWWVvMGRDRkwyVSsxckpEMFVWbGRKS0dnUEcyMjh2aUY5cTA9Ci0tLS0tR

U5EIENFUlRJRklDQVRFLS0tLS0K" | base64 --decode >/tmp/1

然后使用OpenSSL即可查看证书过期时间：

openssl x509 -in /tmp/1 -noout -dates

## TLS Bootstrapping初始化流程

1. Kubelet启动
2. Kubelet查看kubelet.kubeconfig文件，假设没有这个文件
3. Kubelet会查看本地的bootstrap.kubeconfig
4. Kubelet读取bootstrap.kubeconfig文件，检索apiserver的url和一个token
5. Kubelet链接apiserver，使用这个token进行认证
   1. Apiserver会识别tokenid，apiserver会查看该tokenid对于的bootstrap的一个secret
   2. 找个这个secret中的一个字段，apiserver把这个token识别成一个username，名称是system:bootstrap:<token-id>，属于system:bootstrappers这个组，这个组具有申请csr的权限，该组的权限绑定在一个叫system:node-bootstrapper的clusterrole
      1. # clusterrole k8s集群级别的权限控制，它作用整个k8s集群
      2. # clusterrolebinding 集群权限的绑定，它可以帮某个clusterrole绑定到一个用户、组或者seviceaccount
   3. CSR：相当于一个申请表，可以拿着这个申请表去申请我们的证书。
6. 经过上面的认证，kubelet就有了一个创建和检索CSR的权限
7. Kubelet为自己创建一个CSR，名称为kubernetes.io/kube-apiserver-client-kubelet
8. CSR被允许有两种方式：
   1. K8s管理员使用kubectl手动的颁发证书
   2. 如果配置了相关权限，kube-controller-manager会自动同意。
      1. Controller-manager有一个CSRApprovingController。他会校验kubelet发来的csr的username和group是否有创建csr的权限，而且还要验证签发着是否是kubernetes.io/kube-apiserver-client-kubelet
      2. Controller-manager同意CSR请求
9. CSR被同意后，controller-manager创建kubelet的证书文件
10. Controller-manager将证书更新至csr的status字段
11. Kubelet从apiserver获取证书
12. Kubelet从获取到的key和证书文件创建kubelet.kubeconfig
13. Kubelet启动完成并正常工作
14. 可选：如果配置了自动续期，kubelet会在证书文件过期的时候利用之前的kubeconfig文件去申请一个新的证书，相当于续约。
15. 新的证书被同意或签发，取决于我们的配置
    1. Kubelet创建的CSR是属于一个O：system:nodes
    2. CN：system:nodes:主机名