这是个巨坑 --- K8S 集群 1 年证书过期问题

作者：etscript
原文链接：https://ld246.com/article/1575013191401
来源网站：链滴

kubeadm 是 kubernetes 提供的一个初始化集群的工具，使用起来非常方便，但是它创建的apiserve、controller-manager等证书默认只有一年的有效期，同时kubelet 证书也只有一年有效期，一年之 kubernetes 将停止服务。

方法总结下来有以下几个：

1、官方推荐：一年之内 kubeadm upgrade 更新一次 kubernetes 系统。

2、坊间方法：源代码编译，使得kubeadm生成的证书时间边长。

3、手动更新证书（ kubeadm alpha phase ）。

4、启用自动轮换kubelet 证书

K8S中的证书文件介绍

Kubernetes 集群根证书

/etc/kubernetes/pki/ca.crt
/etc/kubernetes/pki/ca.key
.....

K8S中的证书更新相关介绍

stable.txt 或 kube-config.yaml

kubeadm命令升级master证书时，它也会默认从长城之外读取一个stable.txt的文件，也许可能生产境访问不到。

这时候就需要自备的kube-config.yaml文件。生成方式如下命令：
kubeadm config view > kube-config.yaml

环境已经GG，没办法现在生成那就自己写一个kube-config.yaml，内容如下：
apiVersion: kubeadm.k8s.io/v1beta1
kind: ClusterConfiguration
kubernetesVersion: v1.14.1 #-->这里改成你集群对应的版本
imageRepository: registry.cn-hangzhou.aliyuncs.com/google_containers
#这里使用国内的镜像仓库，否则在重新签发的时候会报错：could not fetch a Kubernetes version fom the internet: unable to get URL "https://dl.k8s.io/release/stable-1.txt"

开始更新

备份及清理工作

cd /etc/kubernetes
mkdir ./pki_bak
mkdir ./pki_bak/etcd
mkdir ./conf_bak
mv pki/apiserver* ./pki_bak/
mv pki/front-proxy-client.* ./pki_bak/
mv pki/etcd/healthcheck-client.* ./pki_bak/etcd/
mv pki/etcd/peer.* ./pki_bak/etcd/
mv pki/etcd/server.* ./pki_bak/etcd/
mv ./admin.conf ./conf_bak/

```
mv ./kubelet.conf ./conf_bak/
mv ./controller-manager.conf ./conf_bak/
mv ./scheduler.conf ./conf_bak/
```

开始更新

```
# 这个是版本比较老的kubeadm
# kube-config.yaml看着点路径
kubeadm alpha certs renew all --config=kube-config.yaml

# 完成后重启kube-apiserver,kube-controller,kube-scheduler,etcd这4个容器

————————————————————————
# 这是比较新的kubeadm
kubeadm alpha phase certs all  --config=kube-config.yaml
# 或者
kubeadm alpha phase certs all --apiserver-advertise-address=${MASTER_API_SERVER_IP} --ap
server-cert-extra-sans=主机内网ip,主机公网ip

kubeadm alpha phase kubeconfig all --config=kube-config.yaml
# 或者
kubeadm alpha phase kubeconfig all --apiserver-advertise-address=${MASTER_API_SERVER_I
}

# 完成后重启kube-apiserver,kube-controller,kube-scheduler,etcd这4个容器
# 如果有多台master，则将第一台生成的相关证书拷贝到其余master即可
```

启用自动轮换kubelet 证书

kubelet证书分为server和client两种， k8s 1.9默认启用了client证书的自动轮换，但server证书自动换需要用户开启

增加 kubelet 参数

```
# 在/etc/systemd/system/kubelet.service.d/10-kubeadm.conf 增加如下参数
Environment="KUBELET_EXTRA_ARGS=--feature-gates=RotateKubeletServerCertificate=true"
```

增加 controller-manager 参数

```
# 在/etc/kubernetes/manifests/kube-controller-manager.yaml 添加如下参数
  - command:
    - kube-controller-manager
    - --experimental-cluster-signing-duration=87600h0m0s
    - --feature-gates=RotateKubeletServerCertificate=true
    - ....
```

创建 rbac 对象

```
# 创建rbac对象，允许节点轮换kubelet server证书：
cat > ca-update.yaml << EOF
apiVersion: rbac.authorization.k8s.io/v1
```

```
kind: ClusterRole
metadata:
  annotations:
    rbac.authorization.kubernetes.io/autoupdate: "true"
  labels:
    kubernetes.io/bootstrapping: rbac-defaults
  name: system:certificates.k8s.io:certificatesigningrequests:selfnodeserver
rules:
- apiGroups:
  - certificates.k8s.io
  resources:
  - certificatesigningrequests/selfnodeserver
  verbs:
  - create
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: kubeadm:node-autoapprove-certificate-server
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: system:certificates.k8s.io:certificatesigningrequests:selfnodeserver
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:nodes
EOF

kubectl create –f ca-update.yaml
```

引用的阅读优秀文章

Kubeadm证书过期时间调整

k8s踩坑(三)、kubeadm证书/etcd证书过期处理

Kubeadm安装的K8S集群1年证书过期问题的解决思路