Kubeadm 部署的 Kubernetes 集群证书续期

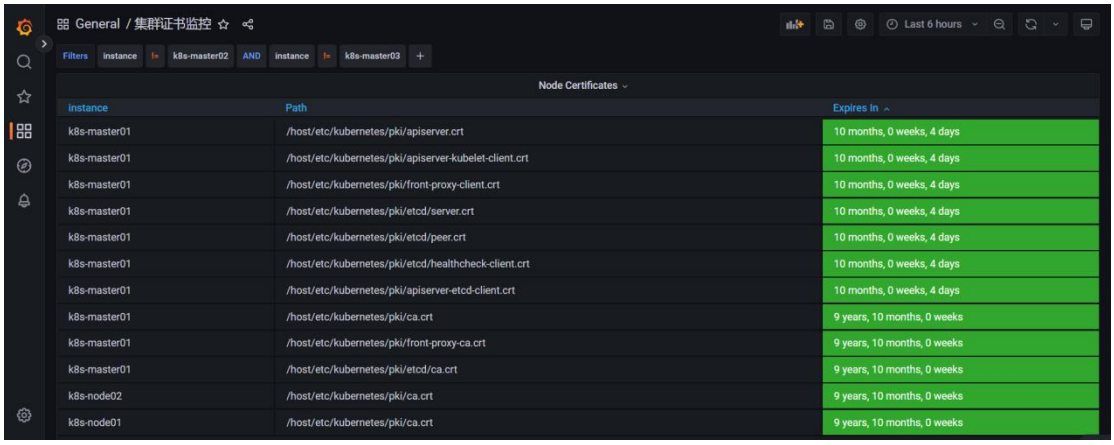
张岩峰老师微信，加我微信，邀请你加入 VIP 交流答疑群：

微信号：ZhangYanFeng0429

二维码：

1、前言

使用 kubeadm 部署的 kubernetes 集群，证书期限都是默认的（ca 根证书默认 10 年，apiserver、apiserver-kubelet-client 等证书默认 1 年有效期）。



上图是使用 prometheus 监控 kubernetes 集群证书期限

版权声明，本文档全部内容及版权归“张岩峰”老师所有，只可用于自己学习使用，禁止私自传阅，违者依法追责。

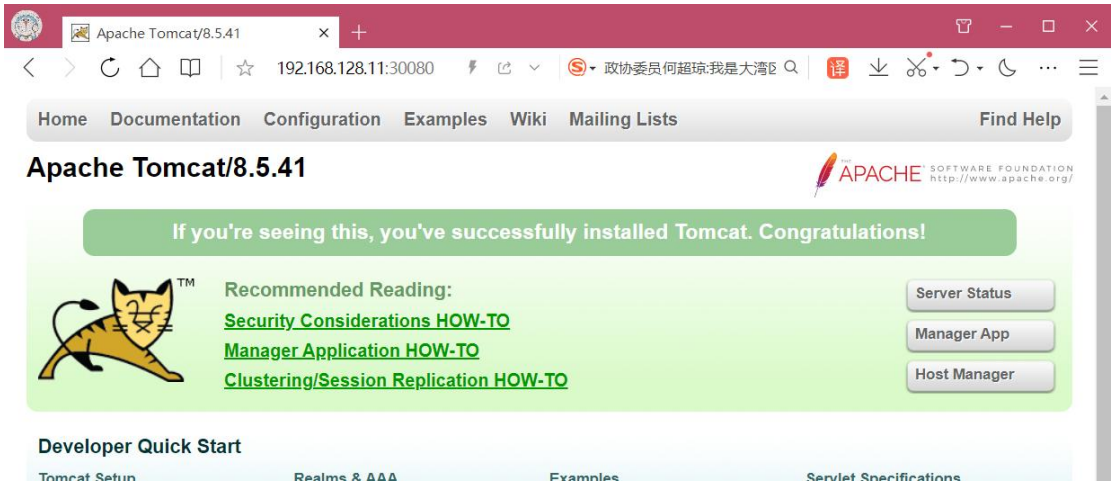
2、模拟证书过期

准备测试环境：

```
[root@k8s-master01 ~]# vi tomcat.yaml
apiVersion: v1
kind: Pod
metadata:
  name: demo-pod
  namespace: default
  labels:
    app: myapp
    env: dev
spec:
  containers:
  - name:  tomcat-pod-java
    ports:
    - containerPort: 8080
    image: tomcat:8.5-jre8-alpine
    imagePullPolicy: IfNotPresent
---
apiVersion: v1
kind: Service
metadata:
  name: tomcat
spec:
  type: NodePort
  ports:
    - port: 8080
      nodePort: 30080
  selector:
    app: myapp
    env: dev

[root@k8s-master01 ~]# kubectl apply -f tomcat.yaml
```

版权声明，本文档全部内容及版权归“张岩峰”老师所有，只可用于自己学习使用，禁止私自传阅，违者依法追责。



在证书过期前，业务是可以正常访问的。

1、查看证书过期时间

```
[root@k8s-master01 ~]# kubeadm certs check-expiration
[root@k8s-master01 ~]# kubeadm certs check-expiration
[check-expiration] Reading configuration from the cluster...
[check-expiration] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'

CERTIFICATE                EXPIRES                  RESIDUAL TIME   CERTIFICATE AUTHORITY   EXTERNALLY MANAGED
admin.conf                 Jan 30, 2024 02:33 UTC   354d            ca                      no
apiserver                  Jan 30, 2024 02:33 UTC   354d            ca                      no
apiserver-etcd-client      Jan 30, 2024 02:33 UTC   354d            etcd-ca                 no
apiserver-kubelet-client   Jan 30, 2024 02:33 UTC   354d            ca                      no
controller-manager.conf    Jan 30, 2024 02:33 UTC   354d            ca                      no
etcd-healthcheck-client    Jan 30, 2024 02:33 UTC   354d            etcd-ca                 no
etcd-peer                  Jan 30, 2024 02:33 UTC   354d            etcd-ca                 no
etcd-server                Jan 30, 2024 02:33 UTC   354d            etcd-ca                 no
front-proxy-client         Jan 30, 2024 02:33 UTC   354d            front-proxy-ca          no
scheduler.conf             Jan 30, 2024 02:33 UTC   354d            ca                      no

CERTIFICATE AUTHORITY   EXPIRES                  RESIDUAL TIME   EXTERNALLY MANAGED
ca                      Jan 27, 2033 02:33 UTC   9y              no
etcd-ca                 Jan 27, 2033 02:33 UTC   9y              no
front-proxy-ca          Jan 27, 2033 02:33 UTC   9y              no
[root@k8s-master01 ~]#
```

2、设置当前系统时间（我这里是一主一从节点，让集群时间保持一致）

```
[root@k8s-master01 ~]# date -s "2025-01-1 10:00:00" ; hwclock -w
Wed Jan  1 10:00:00 EST 2025

[root@k8s-node01 ~]# date -s "2025-01-1 10:00:00" ; hwclock -w
Wed Jan  1 10:00:00 EST 2025

[root@k8s-node02 ~]# date -s "2025-01-1 10:00:00" ; hwclock -w
Wed Jan  1 10:00:00 EST 2025
```

3、执行 kuberctl 命令会发现提示证书过期

```
[root@k8s-master01 ~]# kubectl get nodes
Unable to connect to the server: x509: certificate has expired or is not yet valid: current time 2025-01-01T10:01:24-05:00 is after 2024-02-09T08:01:06Z
```

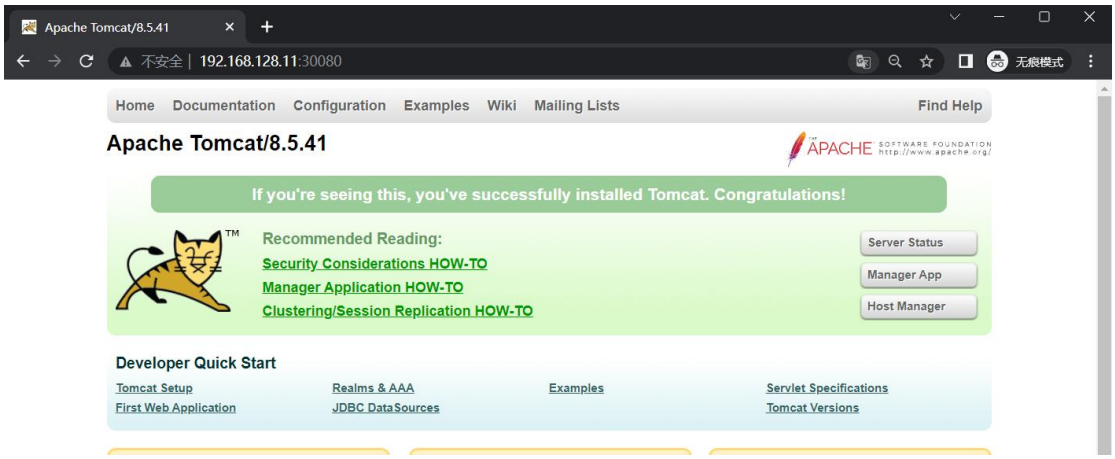
版权声明，本文档全部内容及版权归“张岩峰”老师所有，只可用于自己学习使用，禁止私自传阅，违者依法追责。

4、检查 apiserver.crt 证书有效期限

```
[root@k8s-master01 ~]# openssl x509 -in /etc/kubernetes/pki/apiserver.crt -noout -text | grep Not
            Not Before: Jan 30 02:33:56 2023 GMT
            Not After : Feb  9 08:01:06 2024 GMT
```

可以看到确实已经过期了

5、测试业务还是可以正常访问



可以看到，证书过期，不影响业务正常运行。

3、续费证书期限

1、备份证书所在目录

```
[root@k8s-master01 ~]# cp -r /etc/kubernetes /etc/kubernetes.bak
```

2、批量续约证书

```
[root@k8s-master01 ~]# kubeadm certs renew all
```

3、查看证书过期时间

```
[root@k8s-master01 ~]# kubeadm certs check-expiration
[root@k8s-master01 ~]# kubeadm certs check-expiration
[check-expiration] Reading configuration from the cluster...
[check-expiration] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'

CERTIFICATE                EXPIRES                  RESIDUAL TIME   CERTIFICATE AUTHORITY   EXTERNALLY MANAGED
admin.conf                 Jan 01, 2026 15:00 UTC   364d            ca                      no
apiserver                  Jan 01, 2026 15:00 UTC   364d            ca                      no
apiserver-etcd-client      Jan 01, 2026 15:00 UTC   364d            etcd-ca                 no
apiserver-kubelet-client   Jan 01, 2026 15:00 UTC   364d            ca                      no
controller-manager.conf    Jan 01, 2026 15:00 UTC   364d            ca                      no
etcd-healthcheck-client    Jan 01, 2026 15:00 UTC   364d            etcd-ca                 no
etcd-peer                  Jan 01, 2026 15:00 UTC   364d            etcd-ca                 no
etcd-server                Jan 01, 2026 15:00 UTC   364d            etcd-ca                 no
front-proxy-client         Jan 01, 2026 15:00 UTC   364d            front-proxy-ca          no
scheduler.conf             Jan 01, 2026 15:00 UTC   364d            ca                      no

CERTIFICATE AUTHORITY   EXPIRES                  RESIDUAL TIME   EXTERNALLY MANAGED
ca                      Mar 03, 2033 03:54 UTC   8y              no
etcd-ca                 Mar 03, 2033 03:54 UTC   8y              no
front-proxy-ca          Mar 03, 2033 03:54 UTC   8y              no
[root@k8s-master01 ~]#
```

版权声明，本文档全部内容及版权归“张岩峰”老师所有，只可用于自己学习使用，禁止私自传阅，违者依法追责。

4、重新拷贝认证文件

```
    [root@k8s-master01      ~]#      cp      /etc/kubernetes/admin.conf
/root/.kube/config
    cp: overwrite  ‘/root/.kube/config’ ? y
```

5、检查 node 和 pod 状态

```
    [root@k8s-master01 ~]# kubectl get nodes
    NAME           STATUS   ROLES                  AGE    VERSION
    k8s-master01   Ready    control-plane,master   667d   v1.23.14
    k8s-node01     Ready    worker                 667d   v1.23.14
    k8s-node02     Ready    worker                 667d   v1.23.14

    [root@k8s-master01 ~]# kubectl get pods -A
```

```
[root@k8s-master01 ~]# kubectl get pods -A
NAMESPACE          NAME                                       READY   STATUS    RESTARTS       AGE
calico-apiserver   calico-apiserver-bc645fdc-jw49f            1/1     Running   1 (666d ago)   667d
calico-apiserver   calico-apiserver-bc645fdc-rq2dz            1/1     Running   2 (666d ago)   667d
calico-system      calico-kube-controllers-897f789cf-z2jcd    1/1     Running   1 (666d ago)   667d
calico-system      calico-node-fdg7p                          1/1     Running   1 (666d ago)   667d
calico-system      calico-node-nzlwk                          1/1     Running   1 (666d ago)   667d
calico-system      calico-node-wzt84                          1/1     Running   1 (666d ago)   667d
calico-system      calico-typha-b5c76958d-fxj2l               1/1     Running   1 (666d ago)   667d
calico-system      calico-typha-b5c76958d-vg2q6               1/1     Running   1 (666d ago)   667d
calico-system      csi-node-driver-7qzxw                      2/2     Running   2 (666d ago)   667d
calico-system      csi-node-driver-c652b                      2/2     Running   2 (666d ago)   667d
calico-system      csi-node-driver-kq62j                      2/2     Running   2 (666d ago)   667d
default            demo-pod                                   1/1     Running   0              666d
kube-system        coredns-6d8c4cb4d-9kgfm                    1/1     Running   1 (666d ago)   667d
kube-system        coredns-6d8c4cb4d-kk8rn                    1/1     Running   1 (666d ago)   667d
kube-system        etcd-k8s-master01                          1/1     Running   1 (666d ago)   667d
kube-system        kube-apiserver-k8s-master01                1/1     Running   1 (666d ago)   667d
kube-system        kube-controller-manager-k8s-master01       1/1     Running   1 (666d ago)   667d
kube-system        kube-proxy-5k82r                           1/1     Running   1 (666d ago)   667d
kube-system        kube-proxy-ddh6w                           1/1     Running   1 (666d ago)   667d
kube-system        kube-proxy-f4nfw                           1/1     Running   1 (666d ago)   667d
kube-system        kube-scheduler-k8s-master01                1/1     Running   1 (666d ago)   667d
kube-system        tigera-operator-6bbf97c9cf-lcdbw           1/1     Running   1 (666d ago)   667d
```

版权声明，本文档全部内容及版权归“张岩峰”老师所有，只可用于自己学习使用，禁止私自传阅，违者依法追责。