k3s证书过期&ks8证书过期&rancher 轮换

- 参考网址
  - https://mp.weixin.qq.com/s?__biz=MzkyNzM4Nzk1NQ==&mid=2247500723&idx=1&sn=64def8cd6ec7fd874440690f1f589a3a
  - http://kingsd.top/2020/07/01/k3s-cert-rotary/
  - https://www.cnblogs.com/databank/p/16334715.html

重要：本文提到要备份的地方，请老老实实的备份，否则集群损坏启动不了只能重装

【推荐】使用10年证书一键脚本

仅适用适用**kubeadm**安装的集群

https://github.com/yuyicai/update-kube-cert

https://jiovhm.com/uploads/software/k8s/update-kubeadm-cert.sh

```
# 查看证书过期情况
kubeadm certs check-expiration

# 赋予执行权限
chmod 777 update-kubeadm-cert.sh

# 一键更新所有证书
./update-kubeadm-cert.sh all

# 一键更新master证书（既排除etcd证书）
./update-kubeadm-cert.sh master
```

rancher证书过期

```
# 查看rancher证书是否过期状态
curl -Ikv https://ip:port

# 进入到容器
docker exec -it <rancher_server_id> /bin/bash
```

```
# 执行命令
kubectl --insecure-skip-tls-verify -n kube-system delete secrets k3s-serving
kubectl --insecure-skip-tls-verify delete secret serving-cert -n cattle-system

# 删除或者移动备份证书目录(容器内)
mv /var/lib/rancher/k3s/server/tls /var/lib/rancher/k3s/server/tls-20250507
rm -rf /var/lib/rancher/k3s/server/tls

# 如果容器无法进入
rm -rf data/k3s/server/tls


# 两次重启rancher，第一次为重新生成证书，第二次为加载证书


# 查看rancher-agent的集群代理容器状态
kubectl get po -n cattle-system

# 查看rancher agent容器状态，具体根据rancher版本查看对应的容器
docker ps -a| grep cattle

# 查看cattle-agent日志以获得更多信息
docker logs -f <cattle-agent-container-name>
```

- 集群不可用恢复

```
# 删除 agent，具体的名称要使用kubectl get ns
kubectl -n cattle-system delete daemonset.apps/cattle-node-agent deployment.apps/cattle-cluster-agent

# 更新集群，全局，系统设置，server-url；非必要步骤


# 设置环境变量
RANCHERURL="https://192.168.0.10:8000"
```

```
# □□ID
CLUSTERID="c-8dlc7"

# □□□□□□□□□□□□□□toke,□□,api&&keys□□Bearer Token□□□□
# Token
TOKEN="token-8kdfz:f4kgn4ptrq92wxkmqlzjhf9wntbxc4jpnnwq6spnv6mlhm76259wl6"

# □□jq
yum install -y epel-release
yum install -y  jq

# □□□□
curl -s -H "Authorization: Bearer ${TOKEN}"
"${RANCHERURL}/v3/clusterregistrationtokens?clusterId=${CLUSTERID}" | jq -r '.data[] |
select(.name != "system") | .command'


# □□□□□□□□□□
curl -s -k -H "Authorization: Bearer ${TOKEN}"
"${RANCHERURL}/v3/clusterregistrationtokens?clusterId=${CLUSTERID}" | jq -r '.data[] |
select(.name != "system") | .insecureCommand'


# □□□□□□
curl --insecure -sfL
https://192.168.0.10:8000/v3/import/sztcbkgpcffdvmrd8rn9qvd9flp595np5zcss6xljqk89jqkdx8rhf.yam
l |k3s kubectl apply -f -
```

- k3s□□□□

□□□k8s□□□□□□□□□□□□□□□□□□□□□k3s□□□□□k8s

```
# □□□k3s□k8s□□□□□□□□□□□□□□□□□
# □□□□□□□□□□□□□□□ --insecure-skip-tls-verify=true □□□□□□□□□□TLS

k3s kubectl  --insecure-skip-tls-verify=true  delete secret k3s-serving -n kube-system
```

```
# 删除k3s集群内的证书

kubectl delete secret k3s-serving -n kube-system



# 备份原文件

mkdir -p  tlsbak
cp /var/lib/rancher/k3s/server/tls/**  ./tlsbak -rf
rm /var/lib/rancher/k3s/server/tls/dynamic-cert.json

# 查看证书是否过期，或者直接从浏览器点击证书查看
openssl x509 -noout -dates -in server-ca.crt

# 重启k3s
systemctl restart k3s
```

手动续期k8s证书过期（很大几率导致集群无法启动，不推荐，有诸多排错过程）

```
# 备份配置文件

mkdir -p /data/vpclub/kubernetes-bak/kubernetes-20240620
cp /etc/kubernetes/** /data/vpclub/kubernetes-bak/kubernetes-20240620 -r

# 在主master执行，查看证书过期情况
kubeadm certs check-expiration

# 重新生成证书，如果你是单机，可以用这个命令
# 如果你是集群，不要用这个命令
# 如果你是集群，不要用这个命令
kubeadm certs renew all

# 如果你是集群，需要逐个更新证书，否则回导致三TCD集群不可用
kubeadm certs renew apiserver
kubeadm certs renew apiserver-etcd-client
kubeadm certs renew apiserver-kubelet-client
kubeadm certs renew etcd-healthcheck-client
kubeadm certs renew etcd-peer
kubeadm certs renew etcd-server
```

```
kubeadm certs renew front-proxy-client
kubeadm certs renew scheduler.conf
kubeadm certs renew admin.conf



# □□□master□□□□□□□□□□□□

# □□kubelet
systemctl restart kubelet
# □□docker
systemctl restart docker

# □□□□4□□□□□□POD□□□
# etcd □ kube-apiserver □ kube-scheduler □□kube-controlle
```

□□□□□□□□□**master□pki**□□□□□□□□etcd□□tls□□□□□□□□□etcd□□□□□□□**etcd tls**□□□□pki□□□□□□□□□□□□□□□□□□□□□□□□□□□,□□□□

```
# □□□□□□
kubeadm init phase certs all

# □□□□□□pki□□□□etcd□□□etcd2
mv etcd/ etcd2/

# □□□master□□pki□□□□□□□□□□□□
scp -r /etc/kubernetes/pki/** 172.18.41.4:/etc/kubernetes/pki/

# □ectd2□□□ **peer.crt**  **server.crt** □□□etcd□□
cp etcd2/*peer.crt ./etcd/
cp etcd2/*server.crt ./etcd/

# □□ kubeadm certs renew all □□□□□□
```

- K3S□□□□□□
  - □□□□□□□□□□□□□□□□□□□□□□□□□□

```
# □node□□

cat /etc/rancher/node/password
```

```
# 在 control panel （master）

cat /var/lib/rancher/k3s/server/cred/node-passwd

# 查看所有节点的密码

# 查看服务k3s.services的token

# 查看节点token
cat /var/lib/rancher/k3s/server/node-token

# 修改node节点token

sed -i  "s/<old-token>/<new-token>/g" /usr/lib/systemd/system/k3s.service

# 重新加载配置
systemctl daemon-reload

# 重启服务
systemctl restart k3s
```

评论 #37
创建于 2023 年 16 月 2023 08:51:27
更新于 2025 年 14 月 2025 07:32:01