K8S Certificate Rotation:

Or How I Learned to Start Worrying and Never Stop

Duffie Cooley & Nicholas Lane

VMware @mauilion

Wayfair @apinick

RESOURCES

github.com/mauilion/kind-certs

MAKE K8S

Let’s get a cluster started!

Which Certificates and Where

Control Plane
/etc/kubernetes/

- pki/apiserver-etcd-client.key
- pki/sa.key
- pki/front-proxy-ca.crt
- pki/ca.crt
- pki/apiserver.key
- pki/front-proxy-client.key
- pki/front-proxy-client.crt
- pki/front-proxy-ca.key
- pki/apiserver-kubelet-client.key
- pki/apiserver.crt
- pki/ca.key
- pki/apiserver-kubelet-client.crt
- pki/apiserver-etcd-client.crt
- pki/sa.pub

Component kubeconfigs:

- admin.conf
- kubelet.conf
- scheduler.conf
- controller-manager.conf

ETCD
/etc/etcd/pki

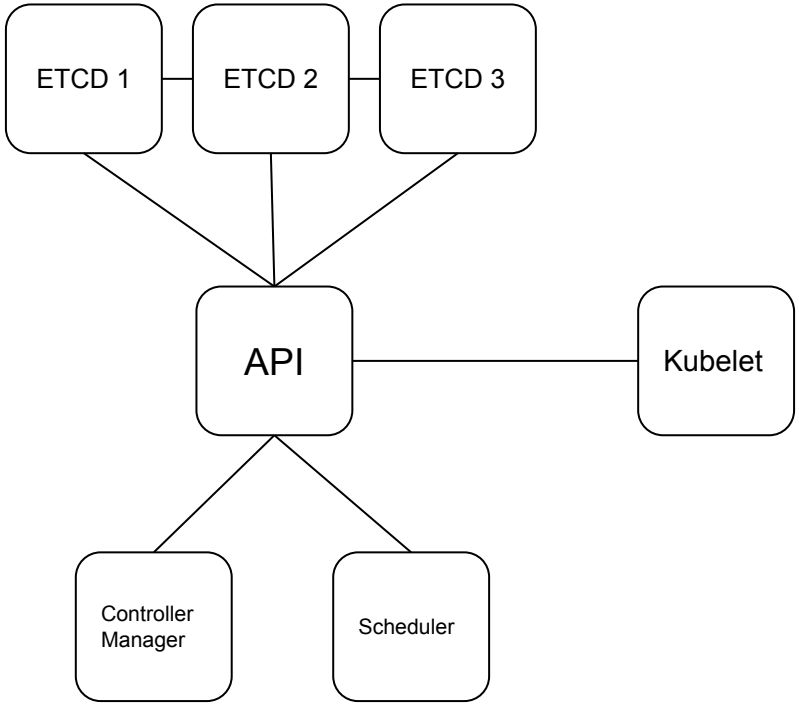
- pki/etcd/peer.crt
- pki/etcd/ca.crt
- pki/etcd/peer.key
- pki/etcd/server.crt
- pki/etcd/server.key
- pki/etcd/ca.key
- pki/etcd/healthcheck-client.crt
- pki/etcd/healthcheck-client.key

Kubelet
/etc/kubernetes/pki
/var/lib/kubelet/pki

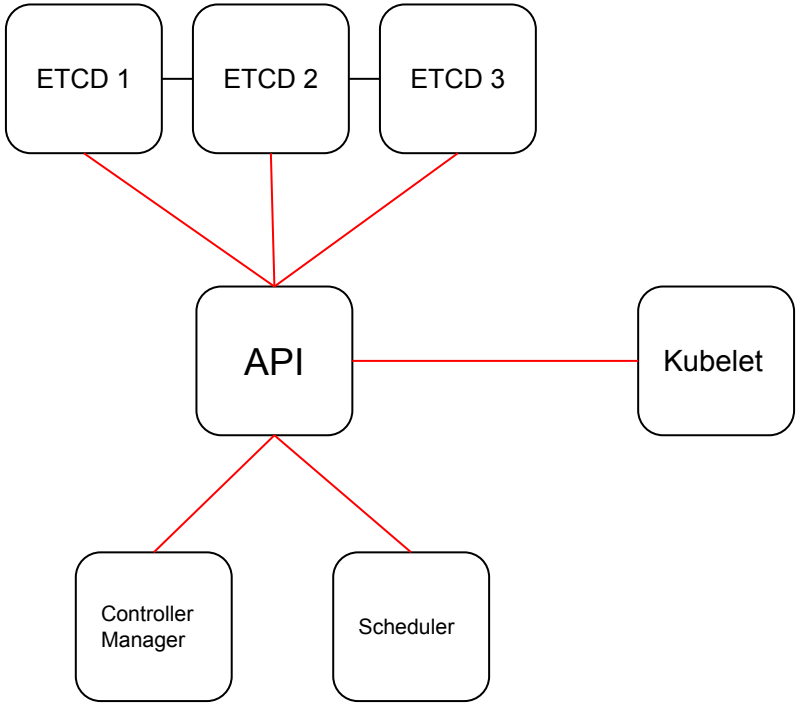
- kubelet.crt
- kubelet.key
- kubelet-client-current.pem

What happens?

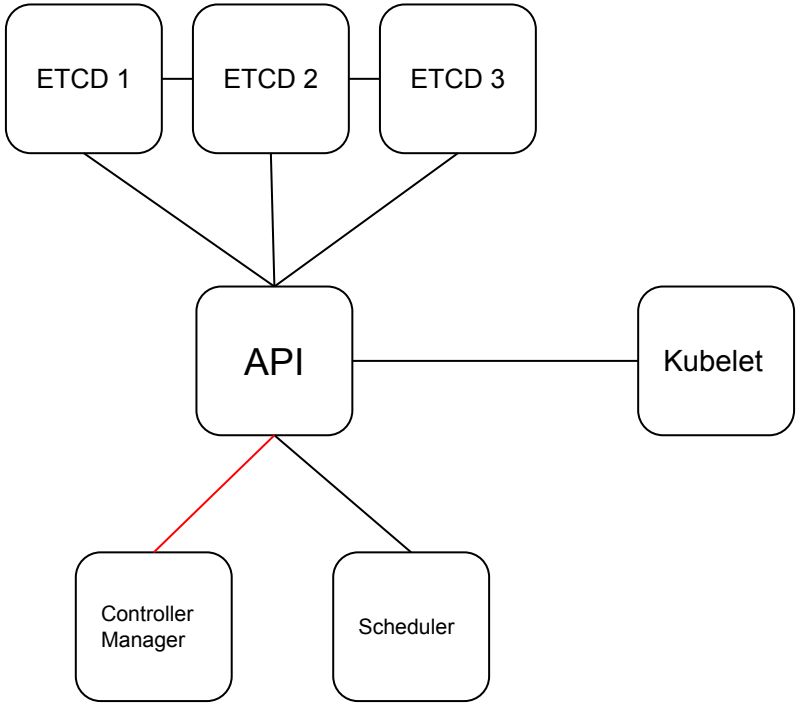
Healthy Cluster



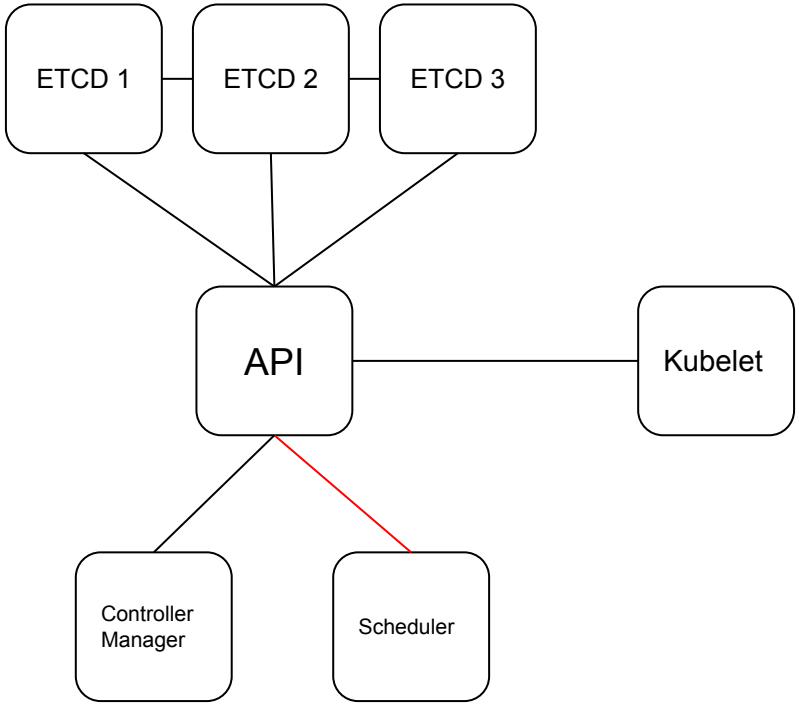
API Cert Expired



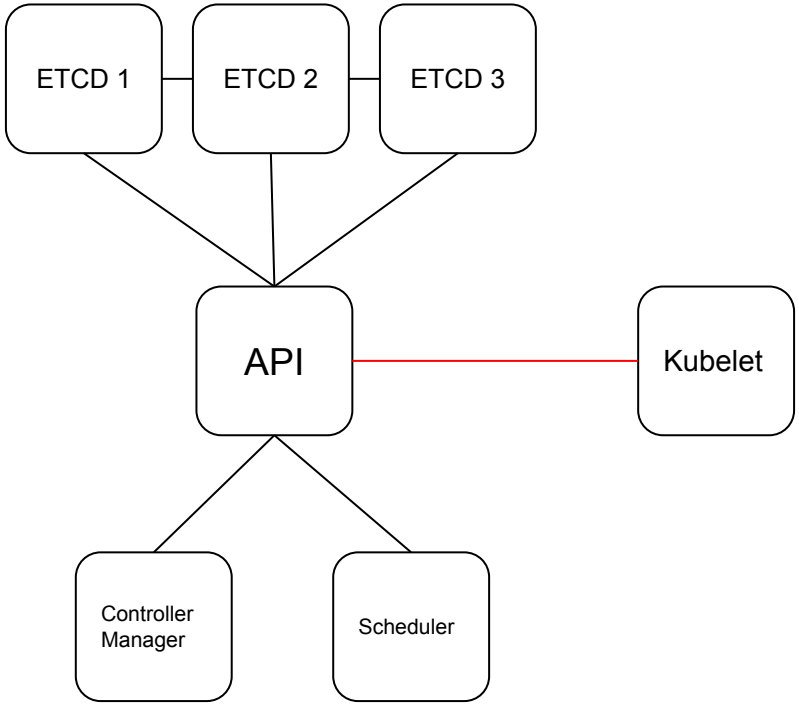
Controller Cert Expired



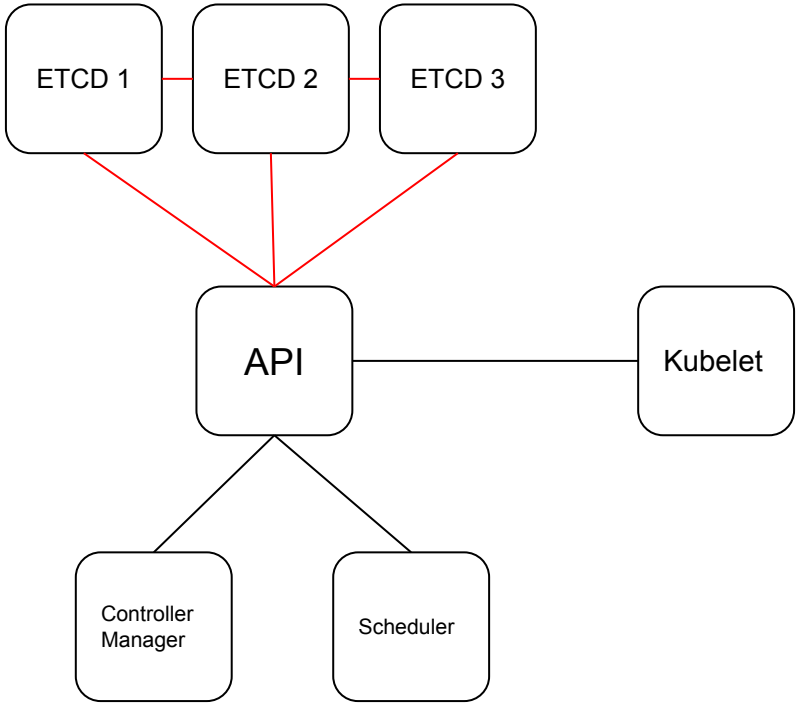
Scheduler Cert Expired



Kubelet Cert Expired



ETCD Certs Expired



ALL Certs Expired

Live Demo!