Kubernetes Certificate and Version Update

Updated on: 19 October 2022

Contents

Update Certificates without upgrading kubernetes version

If certs get expired in the middle of production workloads or near expiry, please follow below steps to update certificates without upgrading kubernetes version

If the certificates get expired in the middle of production, then you may see below error while executing kubectl commands:

Unable to connect to the server: x509: certificate has expired or is not yet valid

Then follow the below process to resume clusters without any issues:

Step 1: Check expiration date for certificates by running below command

$ kubeadm alpha certs check-expiration

Step 2: Backup old certificates to use in case of any issues

$ mkdir -p /root/pki-backup/2022/k8s-old-certs/pki

$ cp -p /etc/kubernetes/pki/*.* /root/pki-backup/2022/k8s-old-certs/pki

$ cp -p /etc/kubernetes/*.conf /root/pki-backup/2022/k8s-old-certs

$ mkdir -p /root/pki-backup/2022/k8s-old-certs/.kube

$ cp -p ~/.kube/config /root/pki-backup/2022/k8s-old-certs/.kube/.

Step 3: Run below command to renew all the certificates

$ kubeadm alpha certs renew all

Step 4: Check certificates expiry date again to cross-check if certificates are updates

$ kubeadm alpha certs check-expiration

(Note: It should show the expiry date of certificates after 1 year and Residual time as 364 days)

Step 5: Restart daemon and kubelet service

$ systemctl daemon-reload && systemctl restart kubelet

Step 6 : Restart the container of kube-apiserver.

$ docker ps | grep kube-apiserver

$ docker restart <kube-apiserver container-id>

Step 7: check start date and expired date in kube-apiserver using curl call.

$ curl -ikv https://localhost:6443

Step 8: Copy updated certificates to ~/.kube/config

$ cp -r /etc/kubernetes/admin.conf ~/.kube/config

Upgrade certificates with Kubernetes Version

Step 1: Check which version of kubernetes to upgrade to

$ yum list --showduplicates kubeadm --disableexcludes=kubernetes

Step 2: Upgrade control plane nodes

$ yum install -y kubeadm-1.xx.x-0 –disableexcludes=kubernetes

Step 3: Verify If download of new version works

$ kubeadm version

Step 4: Check if cluster can be upgraded and fetches the version to upgrade to

$ kubeadm upgrade plan

Step 5: Choose a version to upgrade to and run command

$ kubeadm upgrade apply v1.xx.x

Step 6: Manually upgrade CNI provider plugin

This step is not required on control plane nodes if the CNI provider runs as a DaemonSet

Step 7: Drain the control plane node

Prepare the node for maintenance by marking it unschedulable and evicting the workloads

$ kubectl drain <cp-node-name> --ignore-daemonsets

Step 8: Upgrade kubelet and kubectl

$ yum install -y kubelet-1.xx.x-0 kubectl-1.xx.x-0 --disableexcludes=kubernetes

Step 9: Restart kubelet

$ systemctl restart kubelet

Step 10: Uncordon the control plane

$ kubectl uncordon <cp-node-name>

Deploy networking once again and restart kubelet if node is still in NotReady state

Step 11: Copy certificates to ~/.kube/config

$ cp -r /etc/kubernetes/admin.conf ~/.kube/config

References

- https://v1-17.docs.kubernetes.io/docs/tasks/administer-cluster/kubeadm/kubeadm-upgrade/
- https://www.ibm.com/docs/en/fci/1.1.0?topic=kubernetes-renewing-cluster-certificates
- https://kubernetes.io/docs/tasks/administer-cluster/kubeadm/kubeadm-upgrade/

https://esdscorp-my.sharepoint.com/:v:/g/personal/rishi_esds_co_in/EUSlpt75WFJGkSzil3X93zABPg9SPxNlnGvkkEnUUHwF6w