RENEWING ALL KUBERNETES CERTIFICATES

Release 6.0

DECEMBER 7, 2022

AVANSEUS TECHNOLOGIES PVT. LTD.

REVISION HISTORY

Version	Date	Change description	Created by	Updated by	Reviewed by
V 1.0	December, 2022	Initial Release	Naveen Mahale	Raksha	Chiranjib

Table of Contents

PROBLEM

An error may appear on firing “kubectl” command shown below:

Unable to connect to the server: x509: certificate has expired or is not yet valid: current time 2022-07-28T12:55:22Z is after 2022-07-26T06:57:38Z

Example:

```
[ec2-user@ip-172-31-28-252 NFS_STORAGE_HELM]$ kubectl get all
Unable to connect to the server: x509: certificate has expired or is not yet valid: current time 2022-07-28T12:55:22Z is after 2022-07-26T06:57:38Z
```

ISSUE BEHIND THE PROBLEM

This error appears when some or all the SSL certificates used by Kubernetes application crosses the expiry date.

Fire the following command to understand the issue.

```
sudo kubeadm certs check-expiration
```

Example output: (Expiry date is old as of 28th July & residual time is invalid. This means certificates have expired).

```
[ec2-user@ip-172-31-28-252 NFS_STORAGE_HELM]$ sudo 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'
[check-expiration] Error reading configuration from the Cluster. Falling back to default configuration

CERTIFICATE                EXPIRES                  RESIDUAL TIME   CERTIFICATE AUTHORITY   EXTERNALLY MANAGED
admin.conf                 Jul 26, 2022 06:57 UTC   <invalid>                               no
apiserver                  Jul 26, 2022 06:57 UTC   <invalid>       ca                      no
apiserver-etcd-client      Jul 26, 2022 06:57 UTC   <invalid>       etcd-ca                 no
apiserver-kubelet-client   Jul 26, 2022 06:57 UTC   <invalid>       ca                      no
controller-manager.conf    Jul 26, 2022 06:57 UTC   <invalid>                               no
etcd-healthcheck-client    Jul 26, 2022 06:57 UTC   <invalid>       etcd-ca                 no
etcd-peer                  Jul 26, 2022 06:57 UTC   <invalid>       etcd-ca                 no
etcd-server                Jul 26, 2022 06:57 UTC   <invalid>       etcd-ca                 no
front-proxy-client         Jul 26, 2022 06:57 UTC   <invalid>       front-proxy-ca          no
scheduler.conf             Jul 26, 2022 06:57 UTC   <invalid>                               no

CERTIFICATE AUTHORITY   EXPIRES                  RESIDUAL TIME   EXTERNALLY MANAGED
ca                      Jul 24, 2031 06:57 UTC   8y              no
etcd-ca                 Jul 24, 2031 06:57 UTC   8y              no
front-proxy-ca          Jul 24, 2031 06:57 UTC   8y              no
```

SOLUTION

Renew all the certificates and reconfigure Kubernetes to use new certificates.

1. Command to renew the certificates

```
sudo kubeadm certs renew all
```

Example output:

```
[ec2-user@ip-172-31-28-252 NFS_STORAGE_HELM]$ sudo kubeadm certs renew all
[renew] Reading configuration from the cluster...
[renew] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
[renew] Error reading configuration from the Cluster. Falling back to default configuration

certificate embedded in the kubeconfig file for the admin to use and for kubeadm itself renewed
certificate for serving the Kubernetes API renewed
certificate the apiserver uses to access etcd renewed
certificate for the API server to connect to kubelet renewed
certificate embedded in the kubeconfig file for the controller manager to use renewed
certificate for liveness probes to healthcheck etcd renewed
certificate for etcd nodes to communicate with each other renewed
certificate for serving etcd renewed
certificate for the front proxy client renewed
certificate embedded in the kubeconfig file for the scheduler manager to use renewed

Done renewing certificates. You must restart the kube-apiserver, kube-controller-manager, kube-scheduler and etcd, so that they can use the new certificates.
[ec2-user@ip-172-31-28-252 NFS_STORAGE_HELM]$
```

2. Command to copy admin.conf file into ~/.kube/config

```
sudo cp /etc/kubernetes/admin.conf ~/.kube/config
sudo chown $(id -u):$(id -g) ~/.kube/config
```

3. kubectl command

User is now able to use the kubectl command to do normal activities. ***Restart all the Kubernetes applications that are using the new certificates.*** This is done using mentioned below commands:

```
kubectl -n kube-system delete pod -l 'component=kube-apiserver'
kubectl -n kube-system delete pod -l 'component=kube-controller-manager'
kubectl -n kube-system delete pod -l 'component=kube-scheduler'
kubectl -n kube-system delete pod -l 'component=etcd'
```

Example output:

```
[ec2-user@ip-172-31-28-252 NFS_STORAGE_HELM]$ kubectl -n kube-system delete pod -l 'component=kube-apiserver'
pod "kube-apiserver-ip-172-31-28-252.ap-south-1.compute.internal" deleted
[ec2-user@ip-172-31-28-252 NFS_STORAGE_HELM]$ kubectl -n kube-system delete pod -l 'component=kube-controller-manager'
pod "kube-controller-manager-ip-172-31-28-252.ap-south-1.compute.internal" deleted
[ec2-user@ip-172-31-28-252 NFS_STORAGE_HELM]$ kubectl -n kube-system delete pod -l 'component=kube-scheduler'
pod "kube-scheduler-ip-172-31-28-252.ap-south-1.compute.internal" deleted
[ec2-user@ip-172-31-28-252 NFS_STORAGE_HELM]$ kubectl -n kube-system delete pod -l 'component=etcd'
pod "etcd-ip-172-31-28-252.ap-south-1.compute.internal" deleted
```

The command deletes the running pods and Kubernetes immediately recreates those pods.

4. Command to verify the certificate expiration dates

```
sudo kubeadm certs check-expiration
```

Example output: (Expiration date increases by 1 year & residual time is 364 days)

```
[ec2-user@ip-172-31-28-252 NFS_STORAGE_HELM]$ sudo 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                 Jul 28, 2023 13:01 UTC   364d                                    no
apiserver                  Jul 28, 2023 13:01 UTC   364d            ca                      no
apiserver-etcd-client      Jul 28, 2023 13:01 UTC   364d            etcd-ca                 no
apiserver-kubelet-client   Jul 28, 2023 13:01 UTC   364d            ca                      no
controller-manager.conf    Jul 28, 2023 13:01 UTC   364d                                    no
etcd-healthcheck-client    Jul 28, 2023 13:01 UTC   364d            etcd-ca                 no
etcd-peer                  Jul 28, 2023 13:01 UTC   364d            etcd-ca                 no
etcd-server                Jul 28, 2023 13:01 UTC   364d            etcd-ca                 no
front-proxy-client         Jul 28, 2023 13:01 UTC   364d            front-proxy-ca          no
scheduler.conf             Jul 28, 2023 13:01 UTC   364d                                    no

CERTIFICATE AUTHORITY   EXPIRES                  RESIDUAL TIME   EXTERNALLY MANAGED
ca                      Jul 24, 2031 06:57 UTC   8y              no
etcd-ca                 Jul 24, 2031 06:57 UTC   8y              no
front-proxy-ca          Jul 24, 2031 06:57 UTC   8y              no
```

5. Reboot the master server

Restart the master host system and wait for the system to come up. All the worker nodes should connect back and the Kubernetes cluster will be active.