Kubelet unable to load bootstrap kubeconfig:

Problem statement:

Kubernetes client certificate issue with error: part of the existing bootstrap client certificate is expired …Failed to run kubelet: unable to load bootstrap kubeconfig file: state /etc/Kubernetes/bootstrap-kubelet.conf: no such a file or directory.

Solution:

1. Run the following command to confirm the certificates have been renewed and will expire in 364 days:

```
# kubeadm alpha certs check-expiration
```

The output should look similar to the following:

```
CERTIFICATE                EXPIRES                  RESIDUAL TIME   EXTERNALLY MANAGED
admin.conf                 Dec 20, 2021 02:35 UTC   364d            no
apiserver                  Dec 20, 2021 02:35 UTC   364d            no
apiserver-etcd-client      Dec 20, 2021 02:35 UTC   364d            no
apiserver-kubelet-client   Dec 20, 2021 02:35 UTC   364d            no
controller-manager.conf    Dec 20, 2021 02:35 UTC   364d            no
etcd-healthcheck-client    Dec 20, 2021 02:35 UTC   364d            no
etcd-peer                  Dec 20, 2021 02:35 UTC   364d            no
etcd-server                Dec 20, 2021 02:35 UTC   364d            no
front-proxy-client         Dec 20, 2021 02:35 UTC   364d            no
scheduler.conf             Dec 20, 2021 02:35 UTC   364d            no
```

2. Confirm the kubelet services are running and that communication between the worker nodes and the Kubernetes master is working.

3. After waiting a few minutes, run the following command from the Kubernetes master node to confirm that the worker nodes are available:

```
# kubectl get nodes
```

If you get a response similar to the following:

```
# The connection to the server 9.37.21.119:6443 was refused - did you specify the right host or port?
```

continue with the next steps to resolve the issue. Otherwise, your Kubernetes cluster certificates have been successfully renewed.

4. Run the following command:

```
# diff $HOME/fcik8s-old-certs/kubelet.conf /etc/kubernetes/kubelet.conf
```

If there is no output, the kubelet.conf file was not updated with the new certificate information.

5. Update the /etc/kubernetes/kubelet.conf file and display the difference from the old version to the new one:

```
# cd /etc/kubernetes

# sudo kubeadm alpha kubeconfig user --org system:nodes --client-name system:node:$(hostname) > kubelet.conf

# diff $HOME/fcik8s-old-certs/kubelet.conf /etc/kubernetes/kubelet.conf
```

If the output shows a difference, the file kubelet.conf was updated with the new certificate information.

6.Run the following command:

```
# diff ~/.kube/config $HOME/fcik8s-old-certs/.kube/config
```

If there is no output, the config file still has the outdated keys and certificate values in it.

7. Update client-certificate-data and client-key-data in ~/.kube/config with the values from the updated file in /etc/kubernetes/kubelet.conf:

```
# cat /etc/kubernetes/kubelet.conf
```

Select and copy the output after client-key-data:.

In the ~/.kube/config file, replace the information after client-key-data: with the text copied in the previous step.

```
# cat /etc/kubernetes/kubelet.conf
```

Select and copy the output after client-certificate-data:.

In the ~/.kube/config file, replace the information after client-certificate-data: with the text copied in the previous step.

8. Restart the kubelet service:

```
# systemctl daemon-reload&&systemctl restart kubelet
```

This command is successful if there is no output.

9. Verify master and worker nodes are available:

```
# kubectl get nodes
```

10.Verify all pods are in the running state:

```
# kubectl get pods
```