**How to renew the ssl certificate**

<https://access.redhat.com/solutions/6458661>

**ERROR**

oc login -u kubeadmin https://api.cluster.example.com:6443 error: x509: certificate has expired or is not yet valid: current time 2021-09-23T09:46:28+01:00 is after 2021-08-20T20:16:38Z

**SOLUTION**

To renew the ingress CA:

Ssh in the any master node then execute the following command :

**$ export KUBECONFIG=/etc/kubernetes/static-pod-resources/kube-apiserver-certs/secrets/node-kubeconfigs/lb-int.kubeconfig**

**$ oc config use-context system:admin**

**$ oc get nodes**

**$ oc get csr**

Then go the openshift-ingress-operator namespace

Execute the following commands:

**$ oc project openshift-ingress-operator**

**$ oc get secret router-ca -oyaml > router-ca.yaml**

**$ oc delete secret router-ca**

**$ oc delete pod --all**

**$ oc get secret router-ca**

**$ oc get po**

To re-create the wild-card ingress certificate using the new ingress CA :

Execute the following commands:

**$ oc project openshift-ingress**

**$ oc get secret router-certs-default -o yaml > router-certs-default.yaml**

**$ oc delete secret router-certs-default**

**$ oc delete pod --all**

**$ oc get secret router-certs-default**

**$ oc get po**

After the renewal of default Ingress certificates, users may face x509: Certificate signed by unknown authority error while performing $ oc login from the bastion host, in that case, users need to copy the router-ca and add it to the bastion host's trust store.

**cat /run/secrets/kubernetes.io/serviceaccount/ca.crt > ~/ingress-ca.crt**

**$ cp /home/ocpadmin/ingress-ca.crt /etc/pki/ca-trust/source/anchors/**

**$ update-ca-trust**

authentication 4.10.13 True False True 20h OAuthServerConfigObservationDegraded: failed to apply IDP RHSSO-LNT config: x509: certificate signed by unknown authority

Check the sso

**$ curl -vvkI** [**https://sso-rh-sso.apps.idopadev15.insight.local**](https://sso-rh-sso.apps.idopadev15.insight.local)

**$ oc project openshift-config**

**$ oc get cm**

**$ oc get cm <cm name> -o yaml**

**$ oc get configmap <cm> -n openshift-config -o json | jq -r '.data."ca.crt" ' | openssl x509 -noout -text**

Go to the namespace

**$ oc project openshift-ingress-operator**

**$ oc get secrets | grep tls**

**$ oc extract secrets/router-ca**

Then again go to the namespace

**$ oc project openshift-config**

**$ oc get cm**

**$ oc create configmap <cm-name> --from-file=ca.crt=tls.crt -o json --dry-run=client | oc replace -f -**

Then go to namespace

**$ oc project openshift-authentication**

**$ oc get co**

**$ oc get pods**