**SSL certificate change for selfcare setup on 12th Apr’2023:**

1. SSL renewal on **selfcare.actcorp.in** is on WAF where angular servers are added.
2. But after angular the request goes to HA proxy server, then from HA proxy it goes to **selfcareprod-apigateway.actcorp.in** ingress controller. This ingress is using SSL certificate through the secret **selfcare-backend-tls**.
3. This secret should get created with the latest certificate and the key.
4. **certifcate file** - .crt file (combination of server cert, root cert and intermediate cert) (if the extension is .pem, change it to .crt)
5. **key file** - server key file, .key extension
6. Upload both the certificate on master node. Currently the cert files are uploaded to Master node on /app/k8s/ingress/ directory
7. Once uploaded, change the owner:group to engteam:engteam.
8. Check the sercret of ingress with **kubectl get ingress selfcare-prod-ingress -n selfcare -o yaml**

A screenshot of a computer

Description automatically generated

Get the secret name from here. Then delete the secret using below command.

**kubectl delete secret selfcare-backend-tls --namespace selfcare**

And create the secret again using below command

**kubectl create secret tls selfcare-backend-tls --namespace selfcare --key ServerKey.key --cert CertificateBundle1.crt**

**kubectl create secret tls hrms-web-ingress-tls --namespace hrms --key ACT\_2024.key --cert bundle.crt**

Check with below command before and after.

**curl** [**https://selfcareprod-apigateway.actcorp.in**](https://selfcareprod-apigateway.actcorp.in) **–** see whether curl is working or not

**openssl s\_client -servername selfcareprod-apigateway.actcorp.in -connect selfcareprod-apigateway.actcorp.in:443 2>/dev/null | openssl x509 -noout -dates** – verify the new date validity of the certificate

