1. Generate the rsa private key

**openssl genrsa -out private-key-francis.key 2048**

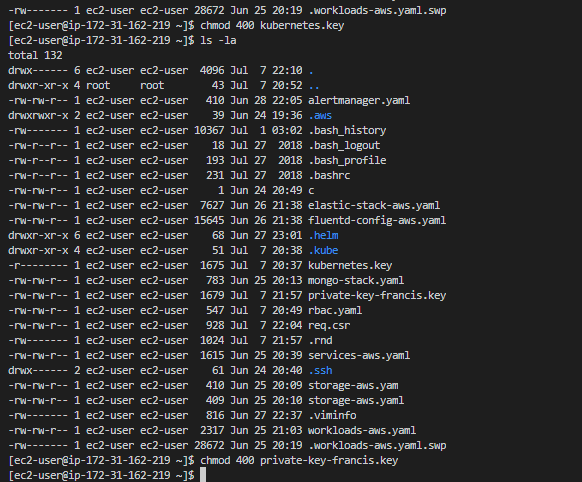
1. Create a certificate signing request

**openssl req -new -key private-key-francis.key -out req.csr -subj "/CN=francis-linux/O=francis-linux"**

1. **Download and copy key from s3 to local final system**

**aws s3 cp s3://tushar-state-store/tushar.k8s.local/pki/private/ca/6711023300517791819727797149.key kubernetes.key**

1. Give permissions to both the keys. Kuberneted and private key



1. Copy Kubernetes crt from this command:

**aws s3 cp s3://tushar-state-store/tushar.k8s.local/pki/issued/ca/6711023300517791819727797149.crt kubernetes.crt**

1. Approve certificate

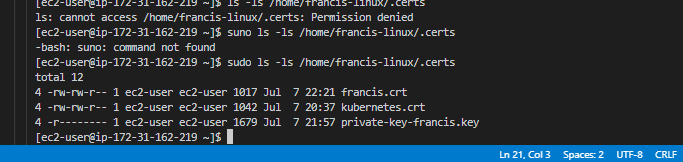
openssl x509 -req -in req.csr -CA kubernetes.crt -CAkey kubernetes.key -CAcreateserial -out francis.crt -days 365

1. Create a hidden folder in the user directory

Sudo mkdir /home/francis-linux/.certs

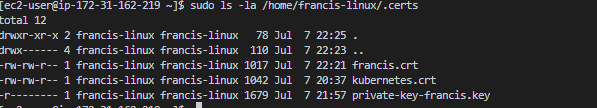
**sudo mv francis.crt /home/francis-linux/.certs**

**sudo mv private-key-francis.key /home/francis-linux/.certs**



**sudo chown -R francis-linux:francis-linux /home/francis-linux/.certs/**

**Final output should be this :**



**After setting up the certificate go to the user**

**And set config view certificate**

**kubectl config set-credentials francis-linux --client-certificate=francis.crt --client-key=private-key-francis.key**

**and set kuberneted certificate in config**

**kubectl config set-cluster tushar.k8s.local --certificate-authority=kubernetes.crt**