**Harbor Installation process**

Connect to a master of the cluster via ssh and do the following commands:

helm repo add harbor https://helm.goharbor.io

helm fetch harbor/harbor --untar

cd /harbor

Copy the certificates ("CERT.key" and "CERT.crt" files) provided by the RootCA (TrustCA) to the /harbor location via SCP

kubectl create namespace harbor

kubectl create secret tls "NAME" --key "CERT.key" --cert "CERT.crt" --namespace harbor #NAME can be chosen by us

vim values.yaml

expose:

# Set the way how to expose the service. Set the type as "ingress",

# "clusterIP", "nodePort" or "loadBalancer" and fill the information

# in the corresponding section

type: ingress

tls:

# Enable the tls or not. Note: if the type is "ingress" and the tls

# is disabled, the port must be included in the command when pull/push

# images. Refer to https://github.com/goharbor/harbor/issues/5291

# for the detail.

enabled: true

# Fill the name of secret if you want to use your own TLS certificate.

# The secret contains keys named:

# "tls.crt" - the certificate (required)

# "tls.key" - the private key (required)

# "ca.crt" - the certificate of CA (optional), this enables the download

# link on portal to download the certificate of CA

# These files will be generated automatically if the "secretName" is not set

secretName: "NAME" <----Name of the Secret we have created

# By default, the Notary service will use the same cert and key as

# described above. Fill the name of secret if you want to use a

# separated one. Only needed when the type is "ingress".

notarySecretName: ""

# The common name used to generate the certificate, it's necessary

# when the type isn't "ingress" and "secretName" is null

commonName: ""

ingress:

hosts:

core: ADDRESS <----harbor-address (for example mgmt-registry.tank.local)

notary: ADDRESS <----harbor-address (for example mgmt-registry.tank.local)

helm install harbor . -n harbor