Intruction to create ImagePullSecrets to gitlab

1. Go to settings, click on repository, **Deploy tokens. Save username and secret key**
2. Create file .dockerconfigjson with the following format

{

"auths": {

"https://registry.gitlab.com":{

"username":"REGISTRY\_USERNAME",

"password":"REGISTRY\_PASSWORD",

"auth":"BASE\_64\_BASIC\_AUTH\_CREDENTIALS (see below)"

}

}

}

1. in “auth” puth the output of the follow command:

echo -n "{REGISTRY\_USERNAME}:{REGISTRY\_PASSWORD}" | base64

1. execute cat .dockerconfigjson | base64. This will output the base64 you need for the registry secret.
2. Create a file with the following content (in commons we have an example named registry-qa-credentials.yml)

apiVersion: v1

kind: Secret

metadata:

name: registry-credentials

namespace: default

type: kubernetes.io/dockerconfigjson

data:

.dockerconfigjson: BASE\_64\_ENCODED\_DOCKER\_FILE

1. Execute kubectl apply -f <filename>
2. Add the metadata.name into the imagePullSecrets

Introduction To deploy ingress-ngnx

1. Install ingress-ngnx in the kubernete cluster
2. Install cert-manager(for tls certificate), you can follow this instruction <https://cert-manager.io/docs/installation/>.
3. Execute kubectl apply -f infra/common/production\_issuer.yaml
4. Execute kubectl infra/k8s/ingress-srv.yaml

NOTAS: if after all this step, the certificate TLS is not working, execute kubectl get all -n cert-manager, look for the pod/cert-manager and see what is the log error.  
  
this repo <https://github.com/compumike/hairpin-proxy> help with propagation check fail.

And this is an example : <https://www.digitalocean.com/community/tutorials/how-to-set-up-an-nginx-ingress-on-digitalocean-kubernetes-using-helm>

Intruction to deploy product-service into kubernete

1. Create a S3 bucket in aws(this will be use in the “AWS\_BUCKET” secret)
2. Create a user in AWS with access to the create s3 bucket,
3. Create the mongo data base
4. Add a secret with name “products-secrets” into the kubernete cluster with this values:
   1. AWS\_ACCESS\_KEY\_ID: AKIARVE4WCVDIQH3SN5P
   2. AWS\_ACCESS\_SECRET: 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
   3. AWS\_REGION: us-east-1
   4. AWS\_BUCKET: [delivery-app-qa](https://s3.console.aws.amazon.com/s3/buckets/delivery-app-qa?region=us-east-1)
   5. DATABASE\_SSL: true
   6. DATABASE\_HOST
   7. DATABASE\_SRV
   8. DATABASE\_NAME
   9. DATABASE\_USERNAME
   10. DATABASE\_PASSWORD

Introduction to deploy deliverya-api into kubernete

Requisitos: have deployed the product service.

1. Execute delivery-mongo-depl.yaml
2. Configure the mongo cluster following this video <https://www.youtube.com/watch?v=W-lJX3_uE5I&t=0s>
3. Create user and a token in the product-api|
4. Add secret with name “delivery-secrets”, with the keys required for start the project,(you can use infra/common/ delivery-secrets.yaml as example)