**L9**

**Sealed Secret**

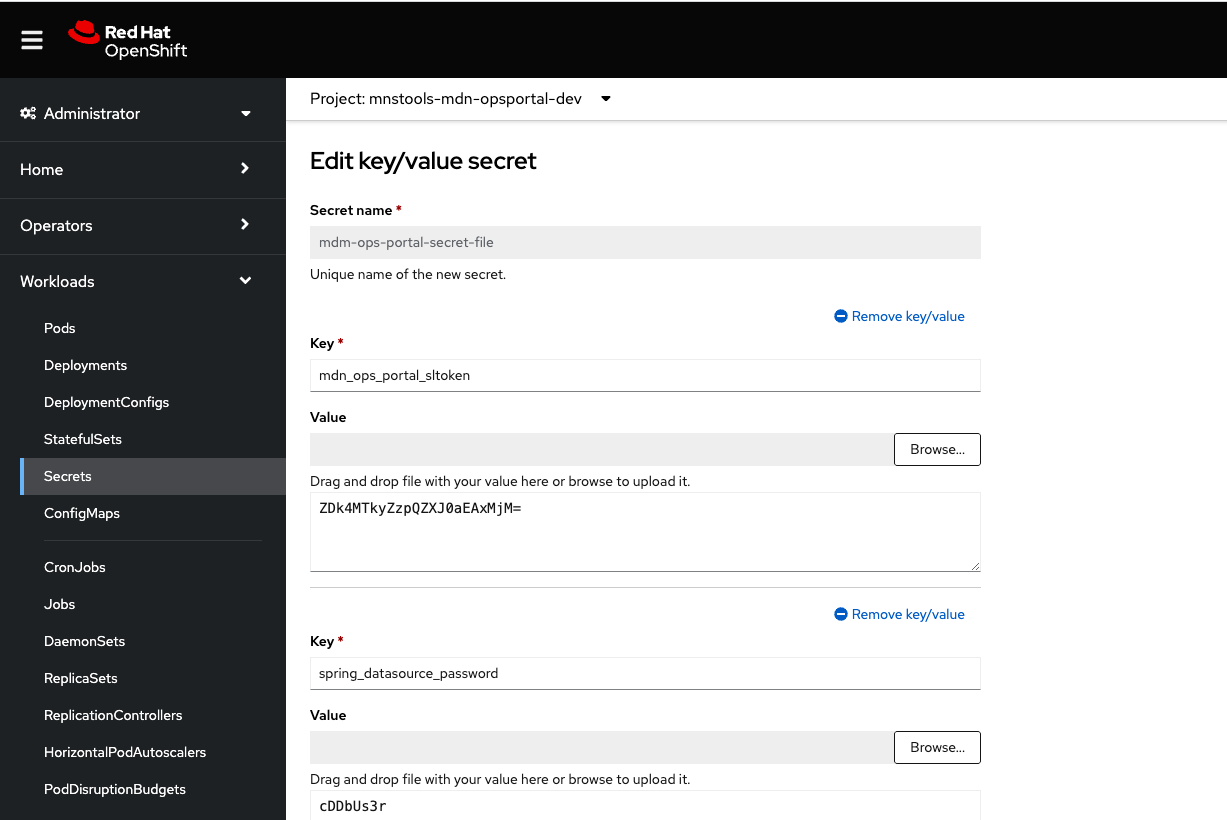
**Step 1:**

**Is to Make Yml file**

**TAKE ur key value pair and put in openshift go in WORKLOAD->secret ->make keyValur pair**

**This will make ur Key -value pair as a secret file (in base 64 file )**

**Download that file**

****

**SAVE and download.**

**Step 2:**

**Download Kub seal software in ur system**

d801332@localhost:~$ kubeseal --namespace mnaas-3scale --format yaml --controller-namespace sealed-secrets < .\argocd\base\repository-secret.yaml > .\argocd\base\repository-sealed-secret.yaml

**Explanation of above Query**

.\argocd\base\ : File path

repository-sealed-secret.yaml: File Name

**--namespace**: Switch

**mnaas-3scale**: My Namespace name of my project

--format yaml --controller-namespace sealed-secrets : FIXED

.\argocd\base\repository-secret.yaml : MY Base 64 secret file name which I havde made via OPensift , include address +Name

.\argocd\base\repository-sealed-secret.yaml : new File(Now this time sealed seceret file along with Adress)

**What I did** :

**kubeseal --namespace mnstools-mdn-opsportal-dev --format yaml --controller-namespace sealed-secrets < ~/Downloads/secret-mdm-ops-portal-secret-file.yaml > secret-mdn-ops-portal-secret-file-sealed.yaml**

**Step3:**

Upload my sealed secret file in Manifest code that is another GIT repo which is only responsible Carrying sealed secret and Microservice yml and pod information

That git repo you upload ur sealed secret file in common folder and make a entry in Kustimazation.yml these are kubernities file small version

**Step 4:**

Go in ARGOS Web page

Click on Sync, you can see ur Microservices and in PODS section u can see ur pod running

**Step 5**

Come in Application in itellij

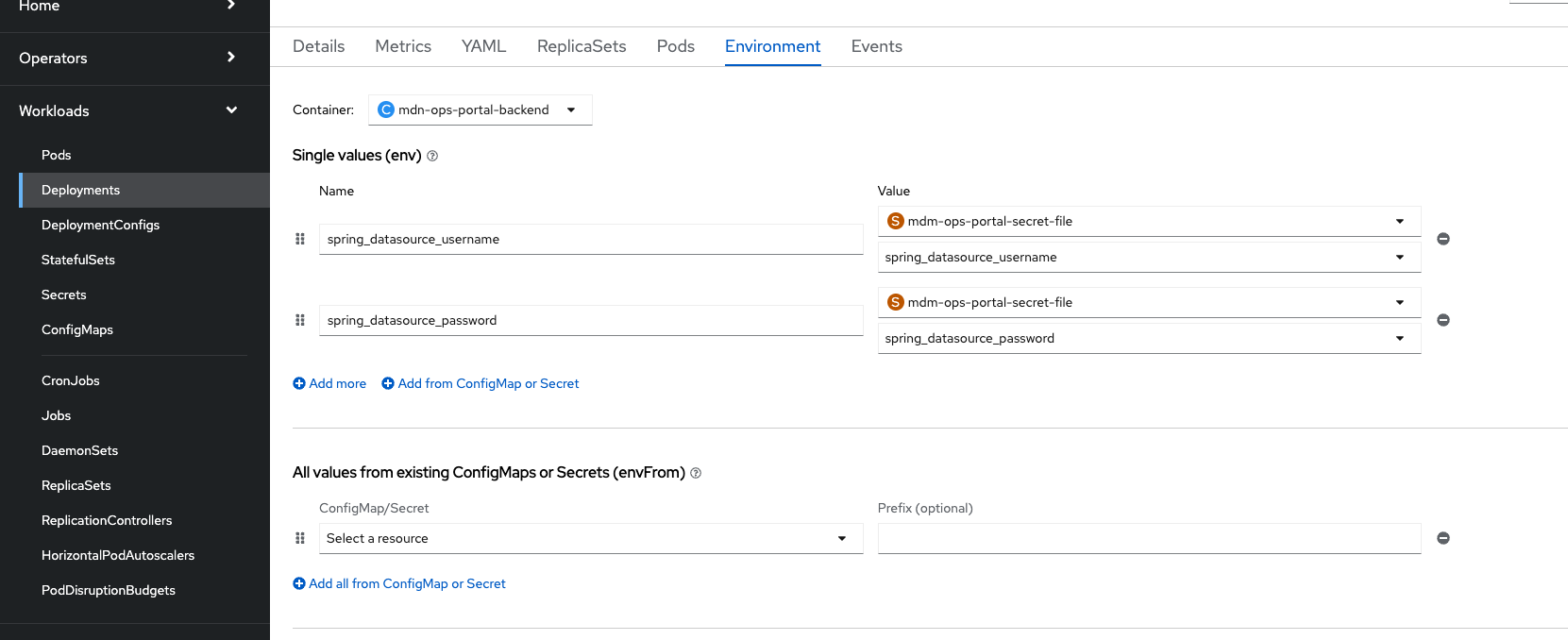
spring.datasource.username = ${spring\_datasource\_username}  
spring.datasource.password=${spring\_datasource\_password}

this key: spring.datasource.username = ${Value}

Value== spring\_datasource\_username

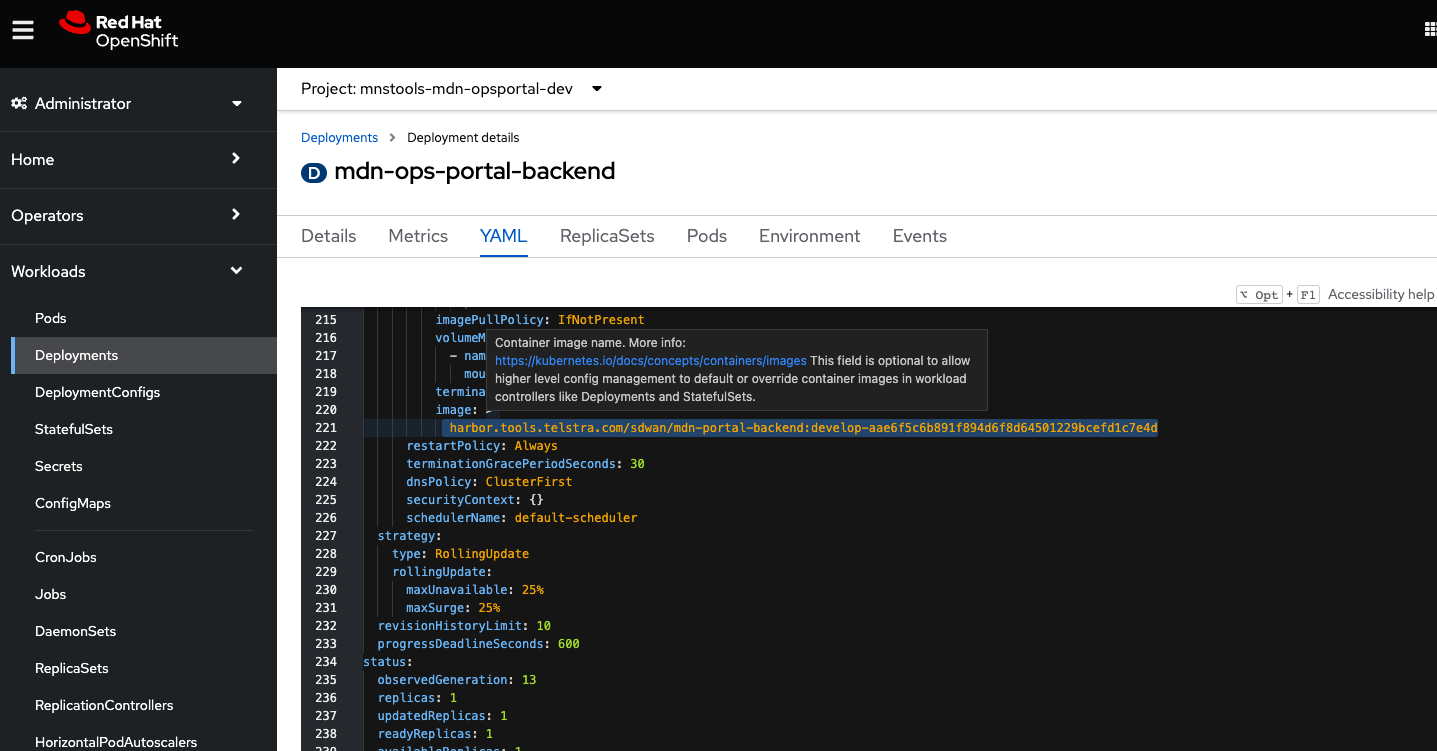
Which is further connected to one secret file and in that secret file my values are present exact value in encrypted format

we can see in OPENSHIFT we can see values how are they mapping

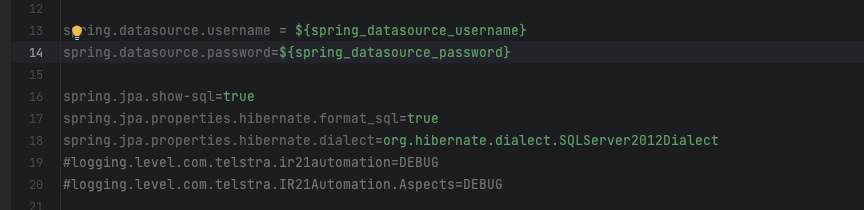
****

How above screen will come first we have to chage App.properties file then commit and merge to develop and deploy on Bamboo == Harbor image (bvxdhgcudb74ed)

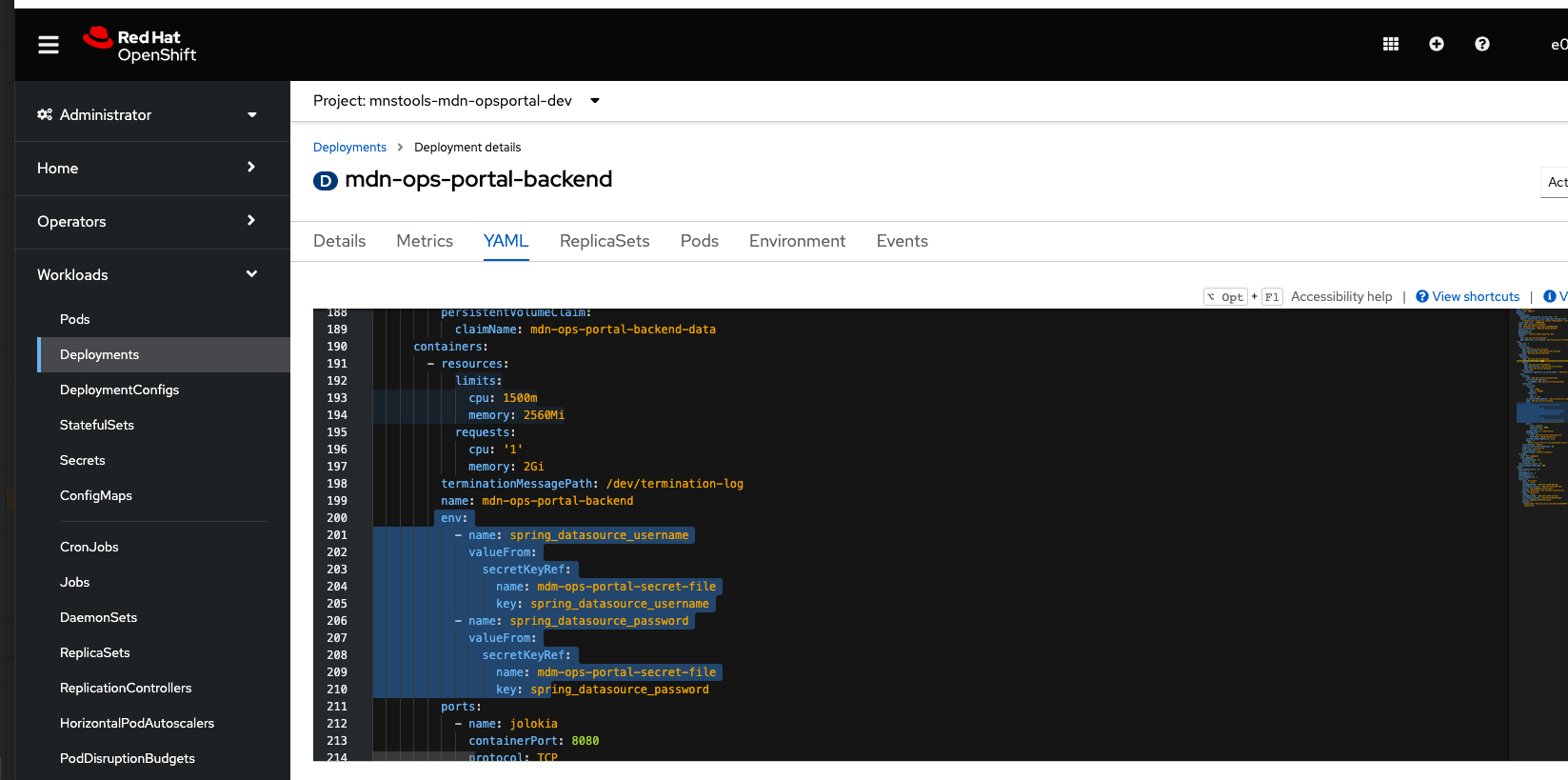
In bamboo in script it is return whatever the images comeup (bvxdhgcudb74ed)the same image will present in OPenshift deployment.yml file



No can u see seleted line my local Imtelij code is deployed along with application.properties ,

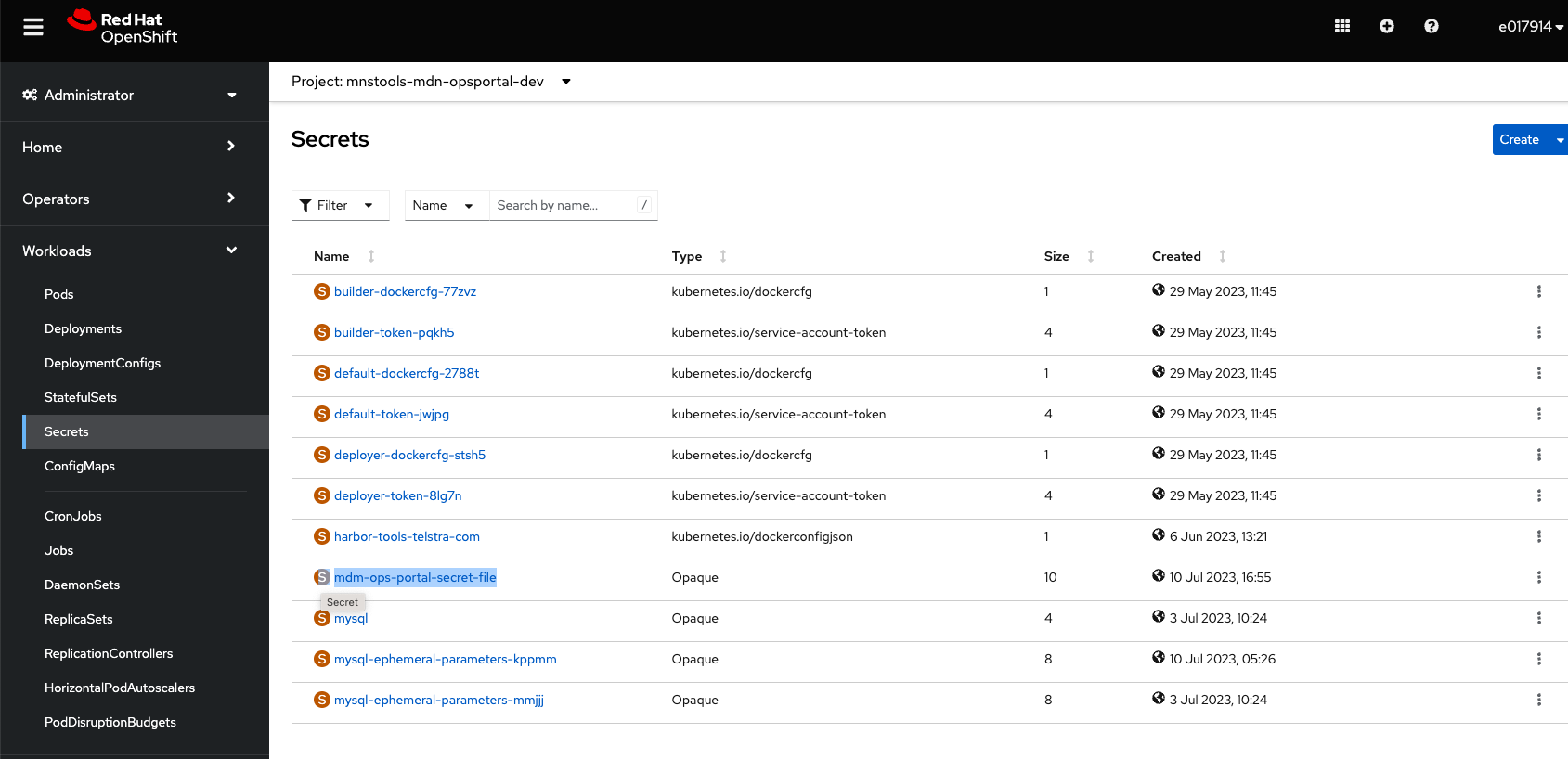


Now in openshift deployment.yml will check harbor iomage code which have 2 values comes in structure ${dbvhdvb} , now start it search in ENV: parameter’s



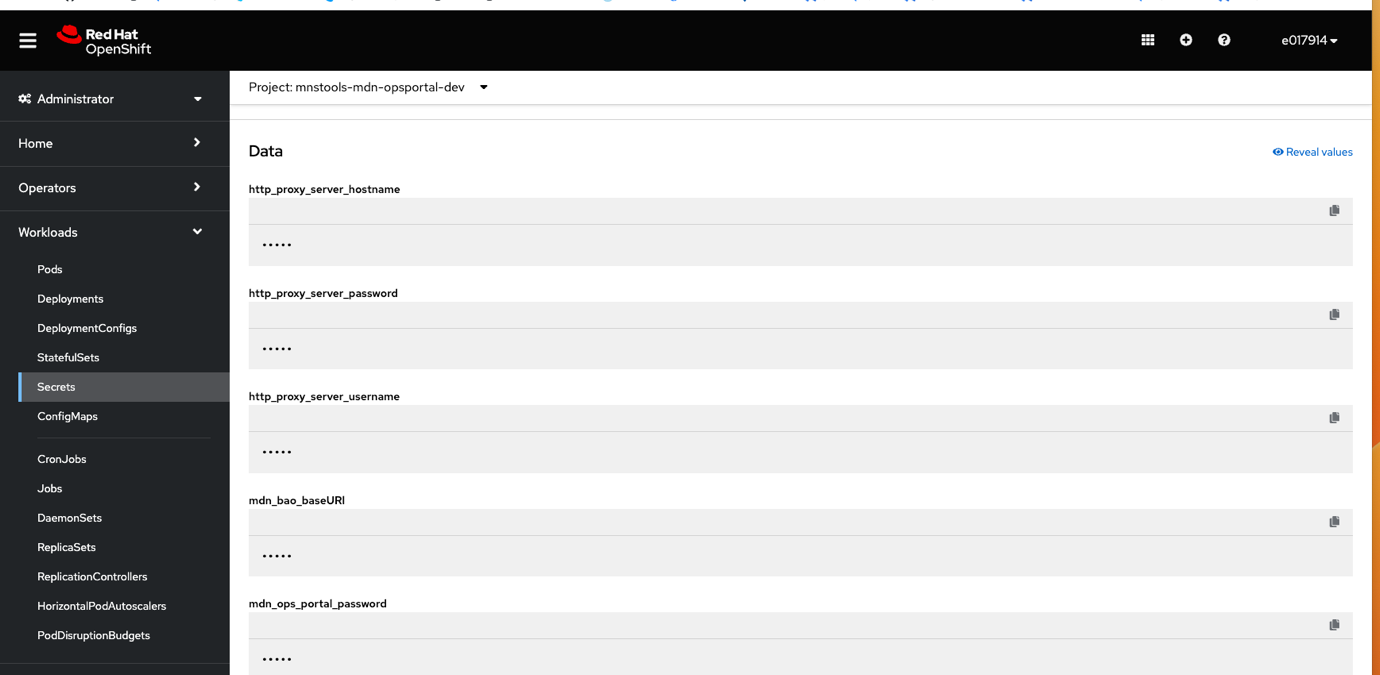
You can see in openshift in selected area

Now that key which has come from Intellij –connected to env –paramets—furthur connected to some secretKeyRef –inside that sealed seceret file my value I can see that too in Encrypted format .

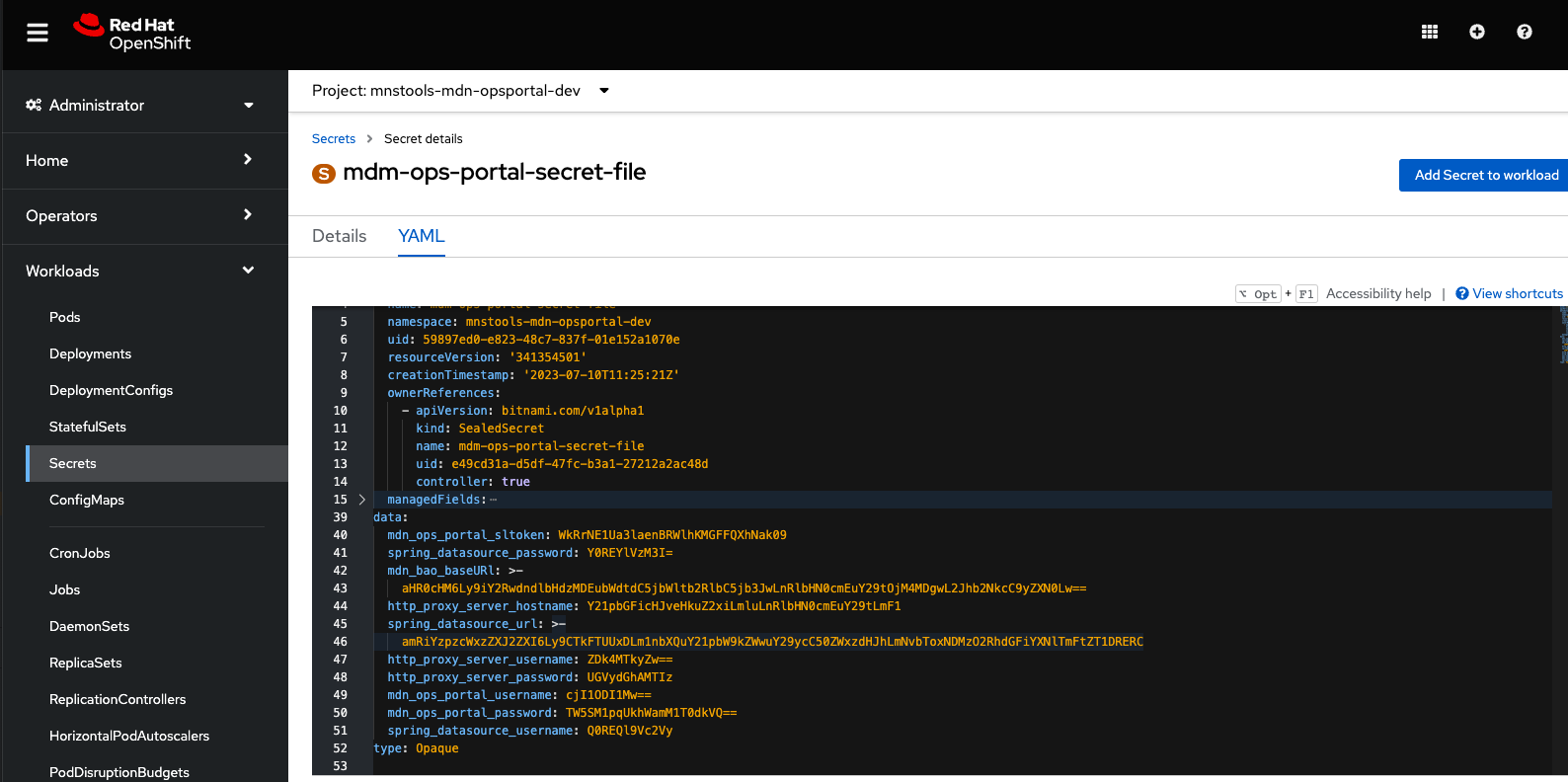


secretKeyRef : you can match secret file name matches

now open that file

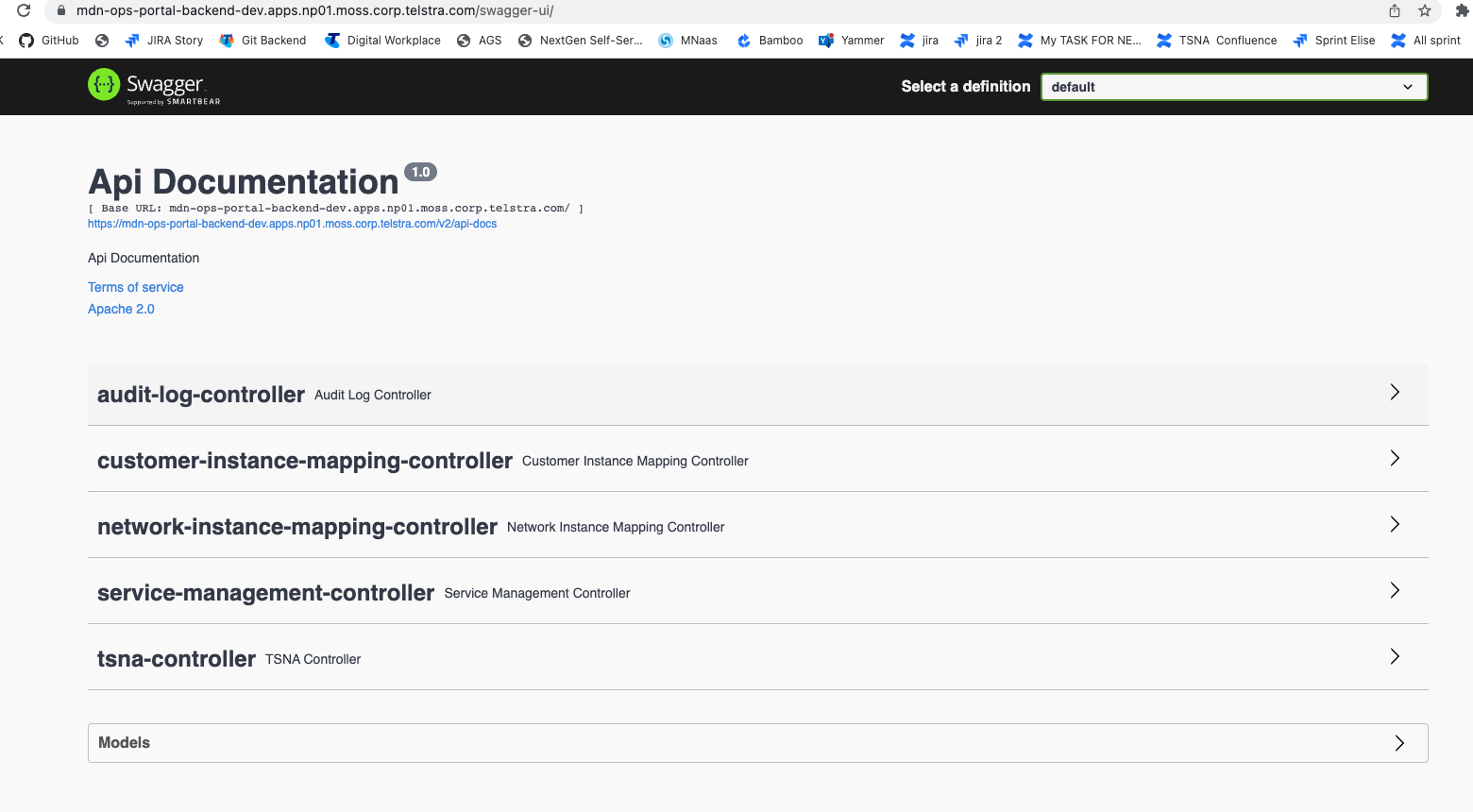


If you click on yml



See values in Sealed secret file is also encrypted

We can our API now on swagger VDI

That is on CLOUD 

That is on Cloud now

Y I am calling cloud because MOSS ek asa managed service platefoem jo ki AWS pe deployed hai

See our POD as well on ARGOS

NOTE: after cMERGING UR CODE with Dev branch

Make sure

To Update Deployemnt.yml in MENIFEST branch other GIT

Now do refrensh ARGO and OPENSHIFT

