EX 280 v12

Exam Instructions:

You will have 1 VMs in the exam

3 Hours Exam Cluster is already configured, and all required packages are installed.

In case you need any package, you can install with preconfigured repositories.

Docs are available in html and pdf format

Cluster Web Console and API url will be given in the

exam:

https://console.domain3.example.com:6443

https://api.domain3.example.com:6443

You have one user opsadm in workbecnch.example.com is given in exarm password of opsadm is given in instructions

{ use ssh to access the workbench }

Password of kubeadm is stored in file in workbench " /home/opsadm/kubeadminpassword.txt "

All the configuration tools to run OpenShift cluster already available in workbench.

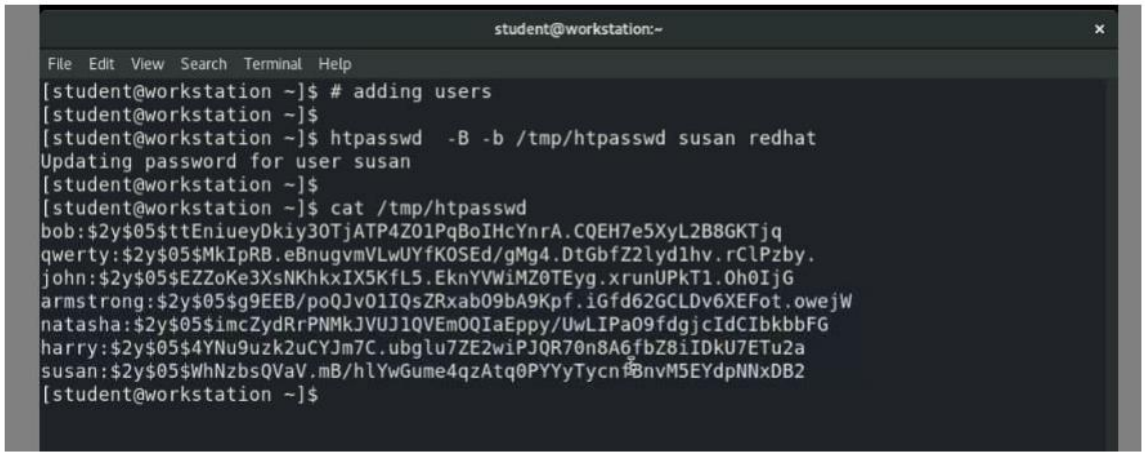
All Docs are available in html and pdf format

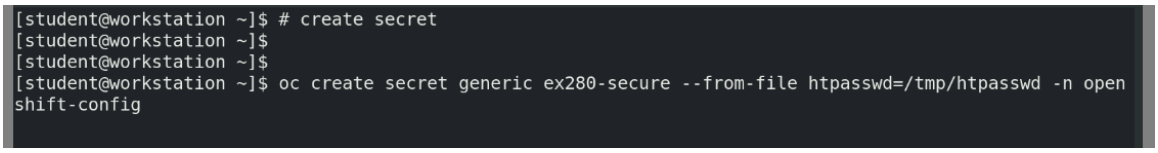
After entering in exam open a terminal and do ssh by root on workstation by given password. one common password will be given in the exam, we can use same password to access workstation VM as root.

Q1) Manage Identity Providers:

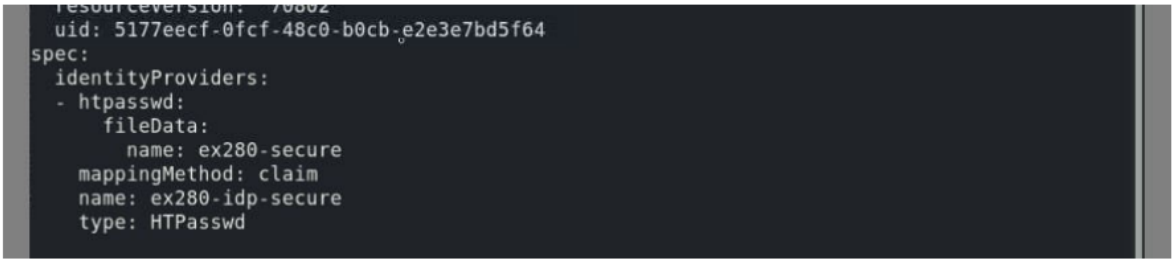
- configure the Oauth to use HTPasswd as the identity provider
- secret name should be ex280-secure and Identity provider name should be ex280-idp-secure
- Create user bob with password indionce
- Create user qwerty with password catalog
- Create user john with password john123
- Create user armstrong with password natasha123
- create user natasha with password arthstrong
- Create user harry with password harry123
- Create user susan with password susuan123

SOLUTION





>>>>> oc edit oauth cluster



need to remember full spec entry

new pods created

```
File  Edit  View  Search  Terminal  Help
[student@workstation ~]$ oc edit oauth cluster
Edit cancelled, no changes made.
[student@workstation ~]$ oc get pods -n openshift-authentication
NAME                              READY   STATUS        RESTARTS   AGE
oauth-openshift-656cbddb57-nqhj4  1/1     Terminating   1          356d
oauth-openshift-696db68646-56qm4  1/1     Running       0          40s
oauth-openshift-696db68646-dfzms  1/1     Running       0          71s
oauth-openshift-696db68646-tpjn7  0/1     Pending       0          10s
[student@workstation ~]$
```

login with every user

```
File  Edit  View  Search  Terminal  Help
[student@workstation ~]$ oc login -u bob -p redhat
Login successful.

You don't have any projects. You can try to create a new project, by running

    oc new-project <projectname>

[student@workstation ~]$ oc whoami
bob
[student@workstation ~]$
```

back to kubeadmin user

```
Using project "default".
[student@workstation ~]$ oc get users
NAME        UID                                    FULL NAME   IDENTITIES
admin       835bde25-34d7-47a8-a9d5-0875a846ab23               htpasswd_provider:admin
armstrong   415abead-f4c5-44be-ae9f-c7215b3516cd               ex280-idp-secure:armstrong
bob         4f72a9f0-f982-4818-bfe0-bd7e663553bc               ex280-idp-secure:bob
harry       46e75607-40b2-495e-ac5d-45e312581d3f               ex280-idp-secure:harry
john        430a2497-ba6f-467b-a1b1-65e5dedaefcd               ex280-idp-secure:john
natasha     98b1de65-65f5-458e-9532-154d605e2dc9               ex280-idp-secure:natasha
qwerty      56007198-554c-4b07-b288-bfe1ea9c8819               ex280-idp-secure:qwerty
susan       c7a7baef-df40-48c8-b180-475fb7c46571               ex280-idp-secure:susan
[student@workstation ~]$
```

Q2) Manage Cluster Project and Permissions:
- Create project with named apollo,test,demo
- bob user should have cluster administrator rights
- john user can create projects
- qwerty user can not create projects-
- natasha user can only view the resources of apollo and test project
- armstrong user should have admin access to apollo project.
- kubeadmin user should not exist (remove kubeadmin user)

```
[student@workstation ~]$ oc new-project apollo
Now using project "apollo" on server "https://api.ocp4.example.com:6443".

You can add applications to this project with the 'new-app' command. For exam
ple, try:

    oc new-app rails-postgresql-example

to build a new example application in Ruby. Or use kubectl to deploy a simple
 Kubernetes application:

    kubectl create deployment hello-node --image=k8s.gcr.io/e2e-test-images/a
gnhost:2.33 -- /agnhost serve-hostname
```

```
[student@workstation ~]$ oc new-project test
Now using project "test" on server "https://api.ocp4.example.com:6443".

You can add applications to this project with the 'new-app' command. For exam
ple, try:

    oc new-app rails-postgresql-example

to build a new example application in Ruby. Or use kubectl to deploy a simple
 Kubernetes application:

    kubectl create deployment hello-node --image=k8s.gcr.io/e2e-test-images/a
gnhost:2.33 -- /agnhost serve-hostname
```

```
[student@workstation ~]$ oc new-project demo
Now using project "demo" on server "https://api.ocp4.example.com:6443".

You can add applications to this project with the 'new-app' command. For exam
ple, try:

    oc new-app rails-postgresql-example

to build a new example application in Ruby. Or use kubectl to deploy a simple
 Kubernetes application:

    kubectl create deployment hello-node --image=k8s.gcr.io/e2e-test-images/a
gnhost:2.33 -- /agnhost serve-hostname
```

```
[student@workstation ~]$ oc adm policy add-cluster-role-to-user cluster-admin
 bob
clusterrole.rbac.authorization.k8s.io/cluster-admin added: "bob"
[student@workstation ~]$
```

```
[student@workstation ~]$ # to check bob user gets rights
[student@workstation ~]$
[student@workstation ~]$
[student@workstation ~]$ oc login -u bob -p redhat
Login successful.

You have access to 69 projects, the list has been suppressed. You can list al
l projects with 'oc projects'

Using project "demo".
[student@workstation ~]$ oc get nodes
NAME       STATUS   ROLES           AGE    VERSION
master01   Ready    master,worker   354d   v1.23.3+e419edf
master02   Ready    master,worker   354d   v1.23.3+e419edf
master03   Ready    master,worker   354d   v1.23.3+e419edf
[student@workstation ~]$
```

```
[student@workstation ~]$ oc adm policy remove-cluster-role-from-group self-pr
ovisioner system:authenticated:oauth
Warning: Your changes may get lost whenever a master is restarted, unless you
 prevent reconciliation of this rolebinding using the following command: oc a
nnotate clusterrolebinding.rbac self-provisioners 'rbac.authorization.kuberne
tes.io/autoupdate=false' --overwrite
clusterrole.rbac.authorization.k8s.io/self-provisioner removed: "system:authe
nticated:oauth"
[student@workstation ~]$ oc login -u qwerty -p redhat
Login successful.

You don't have any projects. Contact your system administrator to request a p
roject.
[student@workstation ~]$ oc new-project deepak
Error from server (Forbidden): You may not request a new project via this API
.
[student@workstation ~]$
```

```
[student@workstation ~]$ # jhon can create projects
[student@workstation ~]$
[student@workstation ~]$
[student@workstation ~]$ oc login -u bob -p redhat
Login successful.

You have access to 69 projects, the list has been suppressed. You can list al
l projects with 'oc projects'

Using project "default".
[student@workstation ~]$ oc adm policy add-cluster-role-to-user self-provisio
ner jhon
Warning: User 'jhon' not found
clusterrole.rbac.authorization.k8s.io/self-provisioner added: "jhon"
[student@workstation ~]$ oc adm policy add-cluster-role-to-user self-provisio
ner john
clusterrole.rbac.authorization.k8s.io/self-provisioner added: "john"
[student@workstation ~]$ oc login -u jhon -p redhat
Login failed (401 Unauthorized)
Verify you have provided correct credentials.
[student@workstation ~]$ oc login -u john -p redhat
Login successful.

You don't have any projects. You can try to create a new project, by running

    oc new-project <projectname>
```

```
[student@workstation ~]$ # natashs can view resources of appolo , test
[student@workstation ~]$
[student@workstation ~]$
[student@workstation ~]$ oc login -u bob -p redhat
Login successful.

You have access to 69 projects, the list has been suppressed. You can list al
l projects with 'oc projects'

Using project "default".
[student@workstation ~]$ oc policy add-role-to-user view natasha -n appolo
Error from server (NotFound): namespaces "appolo" not found
[student@workstation ~]$ oc policy add-role-to-user view natasha -n apollo
clusterrole.rbac.authorization.k8s.io/view added: "natasha"
[student@workstation ~]$ oc policy add-role-to-user view natasha -n test
clusterrole.rbac.authorization.k8s.io/view added: "natasha"
[student@workstation ~]$
```

```
[student@workstation ~]$ # armstrong is admin of apollo
[student@workstation ~]$
[student@workstation ~]$
[student@workstation ~]$
[student@workstation ~]$ oc policy add-role-to-user admin armstrong apollo
Warning: User 'apollo' not found
clusterrole.rbac.authorization.k8s.io/admin added: ["armstrong" "apollo"]
[student@workstation ~]$ oc policy add-role-to-user admin armstrong -n apollo
clusterrole.rbac.authorization.k8s.io/admin added: "armstrong"
[student@workstation ~]$
```

```
[student@workstation ~]$ # delete kubeadmin user
[student@workstation ~]$
[student@workstation ~]$ oc delete secrets kubeadmin -n kube-system
secret "kubeadmin" deleted
[student@workstation ~]$
```

Q3) Managing Groups:
- Create groups with name site-users and guest-users
- add qwerty user in guest-users group
- add harry and susan users in site-users
- Give edit permission to sites-users groups on test project
- Give view permission to guest-users groups on demo project

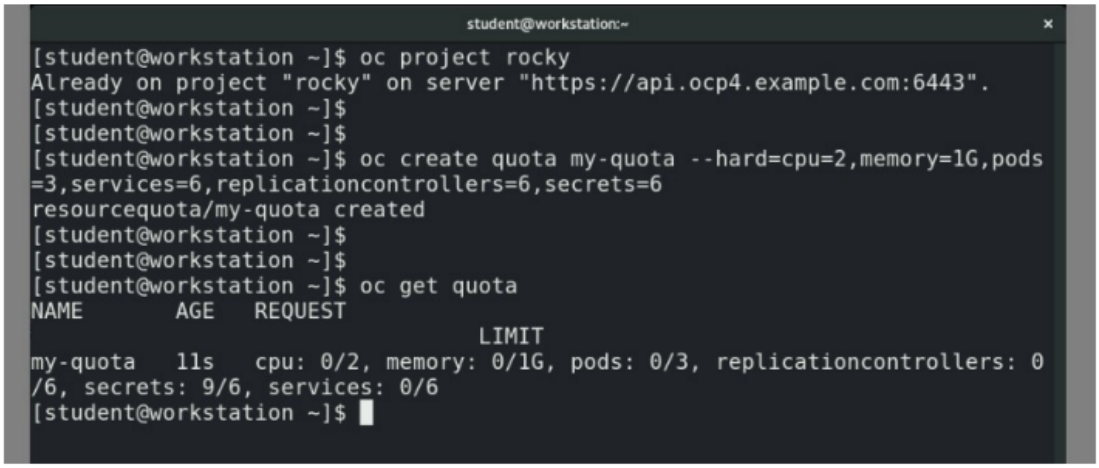
```
[student@workstation ~]$ # create groups
[student@workstation ~]$
[student@workstation ~]$ oc adm groups new site-users
group.user.openshift.io/site-users created
[student@workstation ~]$ oc adm groups new guest-users
group.user.openshift.io/guest-users created
[student@workstation ~]$
```

```
[student@workstation ~]$ oc adm groups add-users guest-users qwerty
group.user.openshift.io/guest-users added: "qwerty"
[student@workstation ~]$ oc adm groups add-users site-users harry susan
group.user.openshift.io/site-users added: ["harry" "susan"]
[student@workstation ~]$ oc get group
NAME          USERS
guest-users   qwerty
site-users    harry, susan
[student@workstation ~]$
```

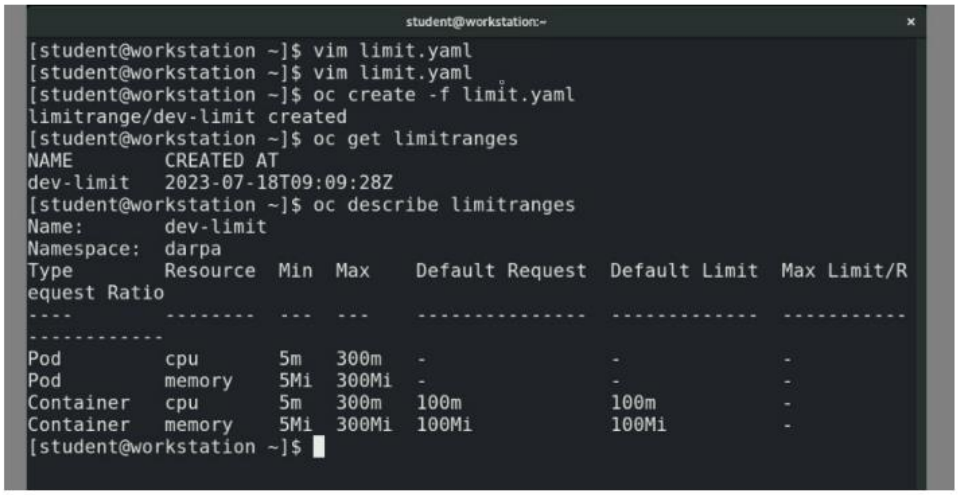
```
student@workstation:~
[student@workstation ~]$ oc policy add-role-to-group edit site-users -n test
clusterrole.rbac.authorization.k8s.io/edit added: "site-users"
[student@workstation ~]$ oc policy add-role-to-group view guest-users -n demo
clusterrole.rbac.authorization.k8s.io/view added: "guest-users"
[student@workstation ~]$
```

```
student@workstation:~
[student@workstation ~]$ oc get rolebinding -n test
NAME                   ROLE                              AGE
admin                  ClusterRole/admin                 54m
edit                   ClusterRole/edit                  5m17s
system:deployers       ClusterRole/system:deployer       54m
system:image-builders  ClusterRole/system:image-builder  54m
system:image-pullers   ClusterRole/system:image-puller   54m
view                   ClusterRole/view                  22m
[student@workstation ~]$ oc get rolebinding -n demo
NAME                   ROLE                              AGE
admin                  ClusterRole/admin                 54m
system:deployers       ClusterRole/system:deployer       54m
system:image-builders  ClusterRole/system:image-builder  54m
system:image-pullers   ClusterRole/system:image-puller   54m
view                   ClusterRole/view                  4m49s
[student@workstation ~]$
```

Q4) Create resource quota for project rocky:
- pods = 3
- cpu = 2
- services = 6
- memory = 1Gi
- secrets = 6
- replication controllers = 6



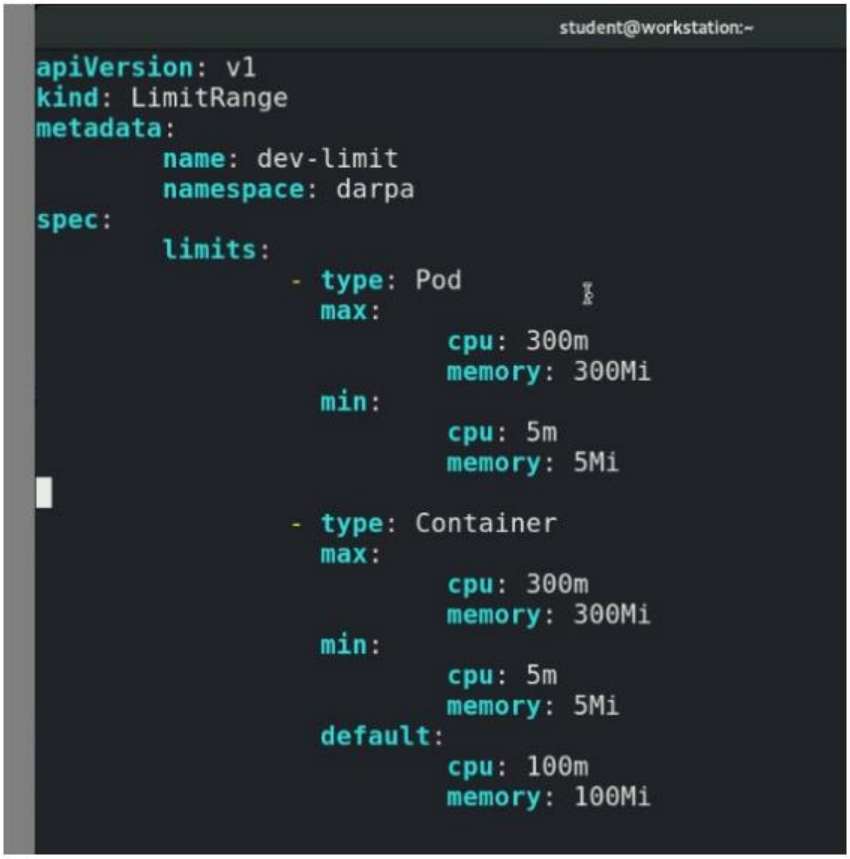
Q5) Create LimitRange for project darpa:
- Set the pod memory limit between 5Mi and 300Mi
- Set the container memory limit between 5Mi and 300Mi and container default request limit for memory is 100Mi
- Set the pod cpu limit between 5m and 300m
- Set the container cpu limit between 5m and 300m and container default request limit for cpu is 100m



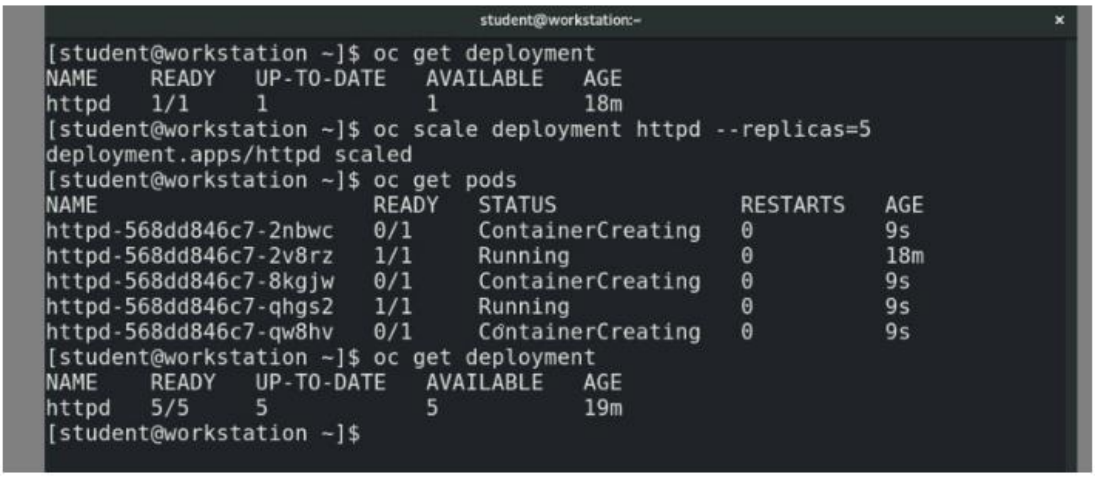
first go to projet darpa

> oc project darpa
the create file limits.yaml

vim limits.yaml {{ need to write full file }}



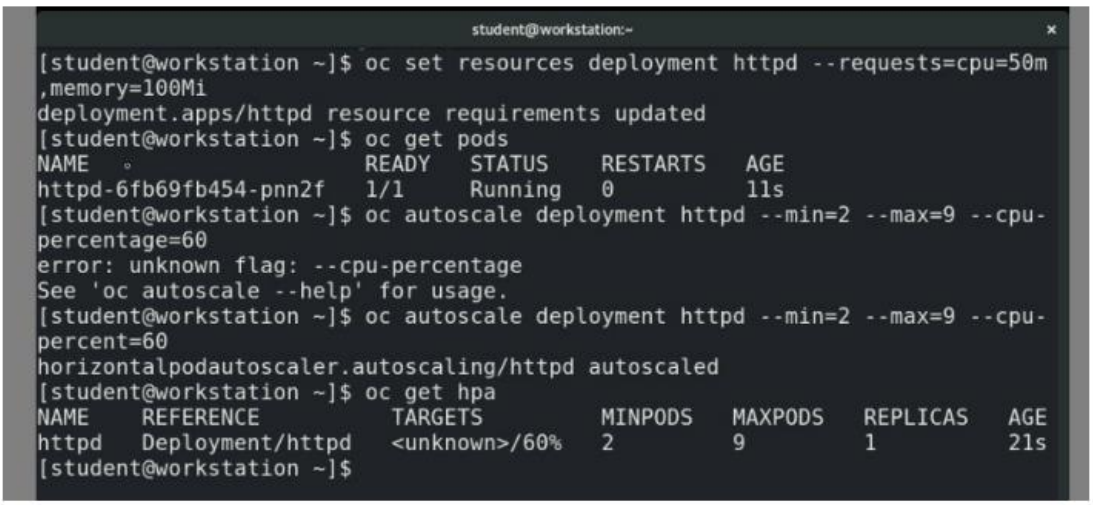
Q6) Scale Application Manually:
- scale the single-pod replicas to 5 under the project world and make sure all pods should run successfully.



Q7) Autoscale of Pods in scaling project:
- minimum replicas=2, maximum replicas=9 and cpu percentage=60%
- Default request for container memory should 100Mi and cpu 50m

for practice create oc new-project scaling

> oc project scaling



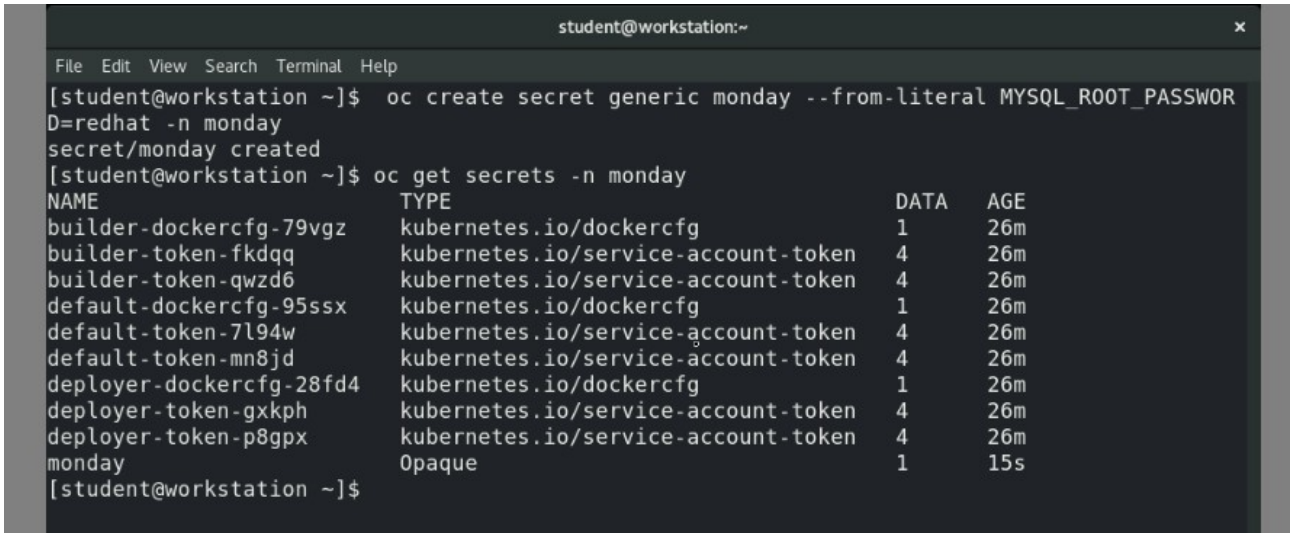
Q8) Create secret with named magic in math project
- The key name should be dirlong
- The value of key should be asdf234234=

<<< this question is randome >>>>>

example question

Q8) Create secret with named magic in monday project
- The key name should be MYSQL_ROOT_PASSWORD
- The value of key should be redhat
solution:-
oc create secret generic monday --from-literal MYSQL_ROOT_PASSWORD=redhat -n monday
oc get secret -n monday

solution ---
Go to project monday



same with 9th question

Q9) Use Secret in monday project
- There is one pod already exists.
- it should use magic secret previously created
- Application Should Produce Output.

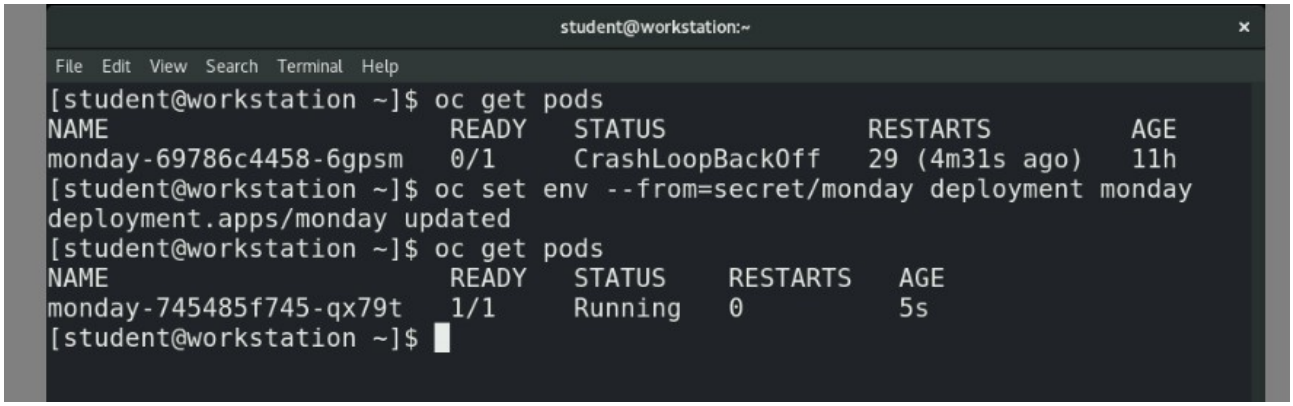
dont run this command in exam it is needed to create a exam env on your labs == (oc new-app --name monday --docker-image registry.access.redhat.com/rhscl/mysql-57-rhel7:5.7-47)

solution:-
oc project monday
oc get pods
oc get deployment (there can be deployment also not dc)
oc get dc (there can be dc also not deployment)
oc logs <podname>

oc get events

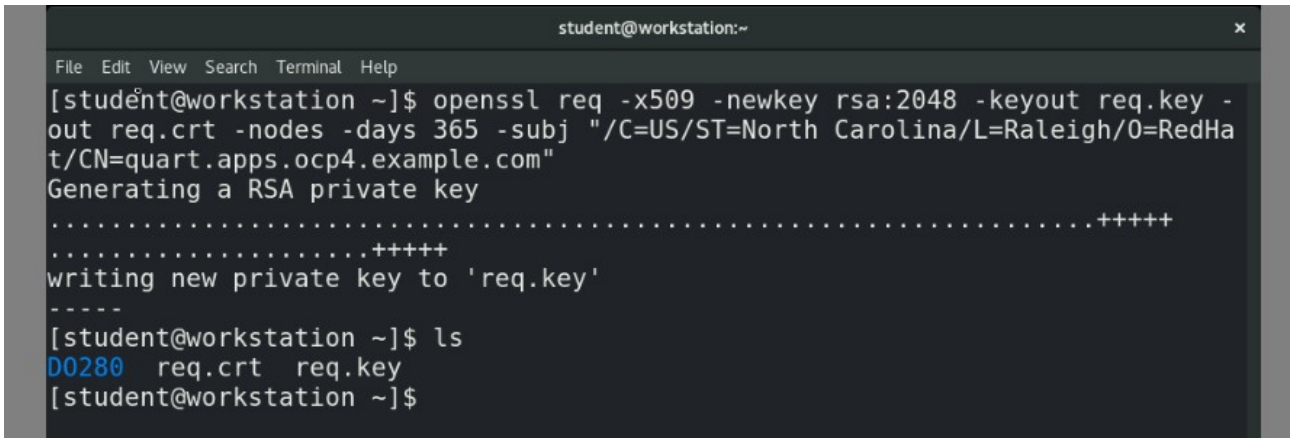
due to env variable the application will not be running. it you have set the variable anf after that also if application is not working than you can see the logs and events for further reasons. may be on worker node taint is applied. if it is than remove the taint from worker node only.

HOW TO SET THE ENV IN DEPLOYMENT WITH SECRET.
oc set env --help | less
oc set env --from=secret/monday deployment monday

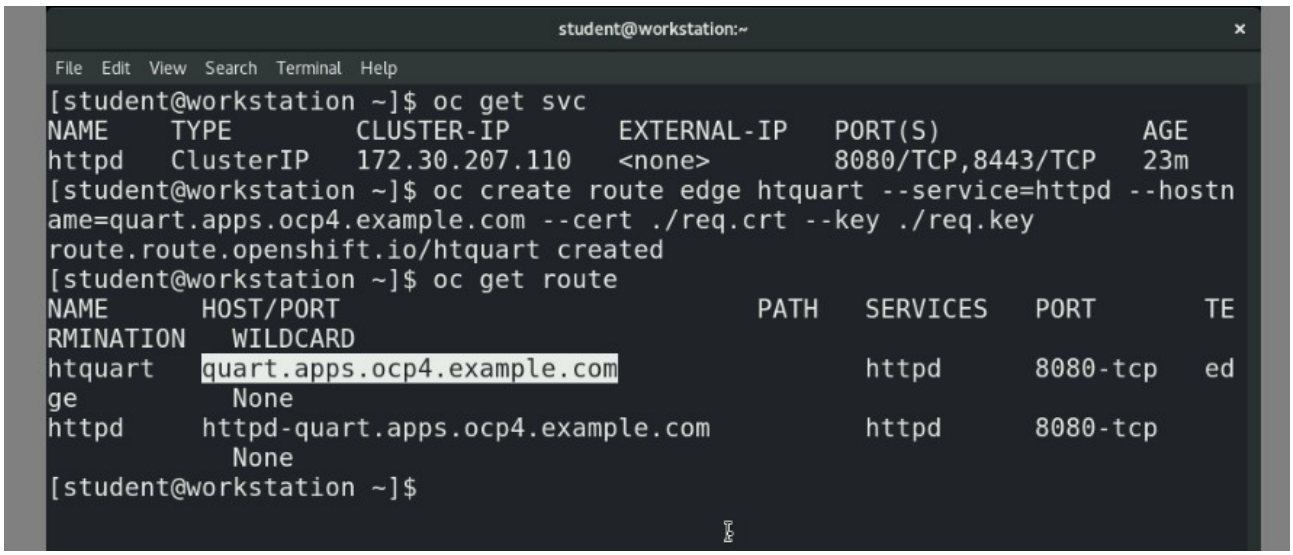


Q10) Create Secure Route in quart project
- One application is already running named with hello based on http and route htquart
- It should run on https with self-signed certificate.
- Subject is “/C=US/ST=North Carolina/L=Raleigh/O=RedHat/CN=quart.apps.ocp4.example.com"
- It should run on https with following url: https://quart.apps.domain3.example.com
- Application should produce output.

Solutions
> create certificates

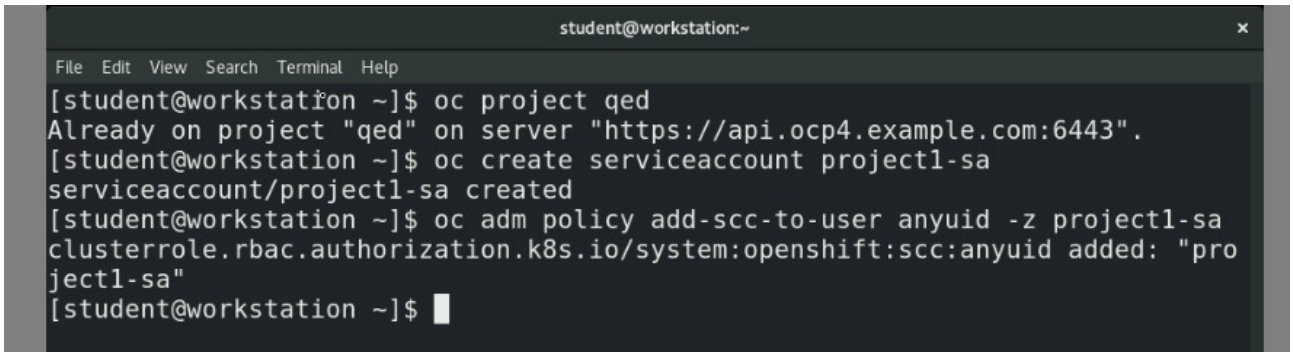


>> now create route



Q11) Create Service Account(user) in qed:
- Service Account (user) Should be project1-sa
- Service Account should be associated with anyuid SCC

Solution :-
oc project qed
oc create serviceaccount --help | less
oc create serviceaccount project1-sa -n qed
oc adm policy --help | less
oc adm policy add-scc-to-user --help | less
oc adm policy add-scc-to-user anyuid -z project1-sa



Q12) Deploy application in the project qed:
- There is one pod already running
- Modify the application as is should run with any user as provided by application
- Application should produce output

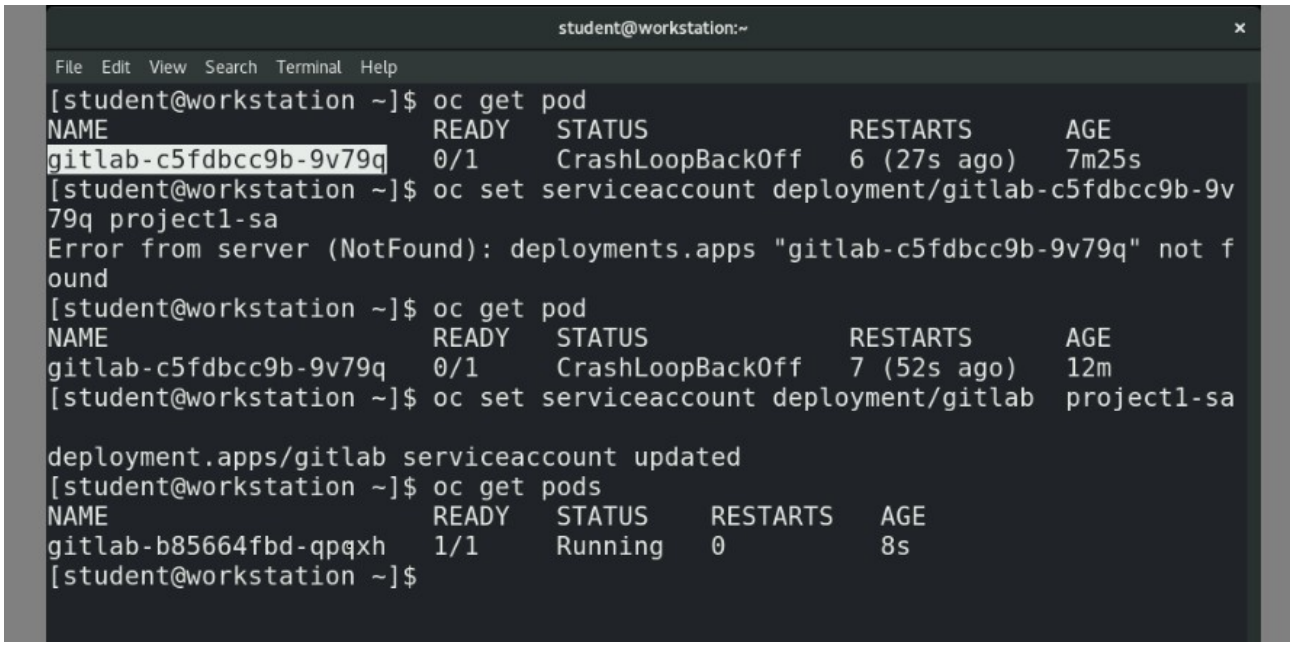
Dont run this command in exam it is needed to create a exam env on your labs
(oc new-app --name gitlab --docker-image gitlab/gitlab-ce:8.4.3-ce.0)
(oc expose service gitlab --port 80)

(oc get pods) - it will give you error now can try to resolve it.
Dont run this command in exam it is needed to create a exam env on your labs

Solution:-
oc project qed
oc get pods
oc get deployment (there can be deployment also not dc)
oc get dc (there can be dc also not deployment)
oc logs <podname>
oc get events

due to no permission the application will not be running it means you need to set the service account so that container can run with any user.

oc set serviceaccount –help|less



13) Install an helm chart etherpad from repository http://helm.ocp4.example.com/charts

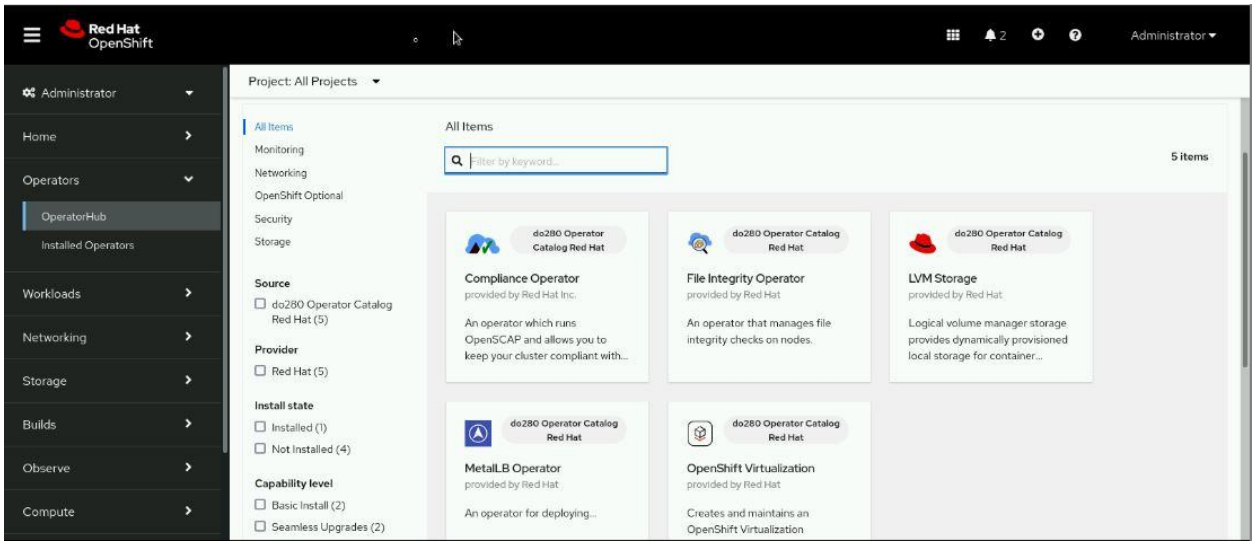
```
student@workstation:~
File  Edit  View  Search  Terminal  Help
[student@workstation ~]$ helm repo add do280-repo  http://helm.ocp4.example.com/charts
"do280-repo" has been added to your repositories
[student@workstation ~]$ helm search repo --versions
NAME                            CHART VERSION   APP VERSION     DESCRIPTION

do280-repo/etherpad             0.0.7           latest          A Helm chart for etherpad lite

do280-repo/etherpad             0.0.6           latest          A Helm chart for etherpad lite

do280-repo/examplechart         0.1.0                           A Helm chart for Kubernetes

do280-repo/influxdb             4.12.1          1.8.10          Scalable datastore for metrics, events, a
nd rea...
do280-repo/mysql-persistent     0.0.2           0.0.2           This content is expermental, do not use i
t in p...
```

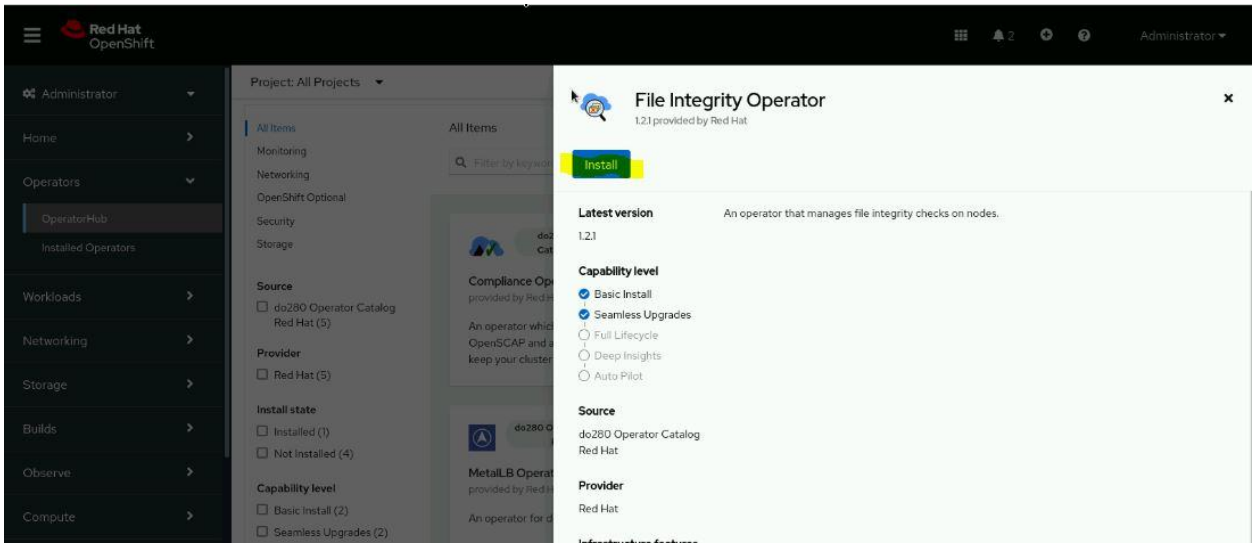
```
[student@workstation ~]$ helm install example-app do280-repo/etherpad
W0928 09:38:04.093363    6211 warnings.go:70] would violate PodSecurity "restricted:v1.24": allowPrivileg
eEscalation != false (container "etherpad" must set securityContext.allowPrivilegeEscalation=false), unre
stricted capabilities (container "etherpad" must set securityContext.capabilities.drop=["ALL"]), runAsNon
Root != true (pod or container "etherpad" must set securityContext.runAsNonRoot=true), seccompProfile (po
d or container "etherpad" must set securityContext.seccompProfile.type to "RuntimeDefault" or "Localhost"
)
NAME: example-app
LAST DEPLOYED: Thu Sep 28 09:38:03 2023
NAMESPACE: helm-pro
STATUS: deployed
REVISION: 1
TEST SUITE: None
```

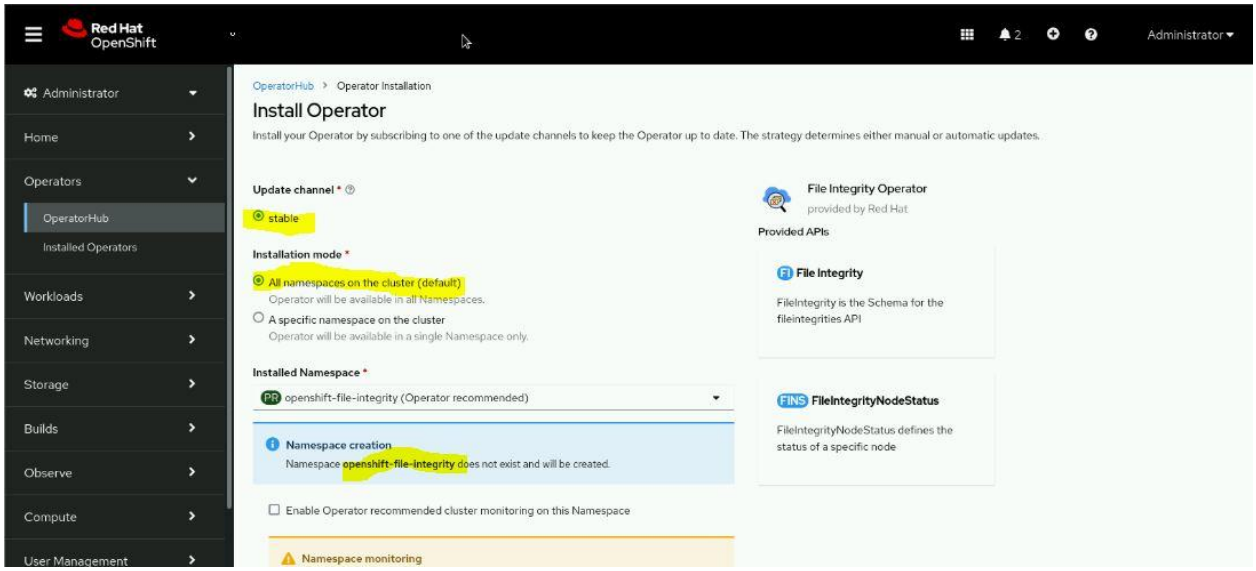
```
[student@workstation ~]$ oc get all
NAME                                      READY   STATUS    RESTARTS   AGE
pod/example-app-etherpad-65d78f5dd8-x66kn   0/1     Running   0          5s

NAME                           TYPE        CLUSTER-IP     EXTERNAL-IP   PORT(S)    AGE
service/example-app-etherpad   ClusterIP   172.30.85.92   <none>        9001/TCP   5s

NAME                                   READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/example-app-etherpad   0/1     1            0           5s

NAME                                              DESIRED   CURRENT   READY   AGE
replicaset.apps/example-app-etherpad-65d78f5dd8   1         1         0       5s

NAME                                          HOST/PORT                                                PAT
H   SERVICES              PORT   TERMINATION     WILDCARD
route.route.openshift.io/example-app-etherpad   example-app-etherpad-helm-pro.apps.ocp4.example.com
    example-app-etherpad   http   edge/Redirect   None
```

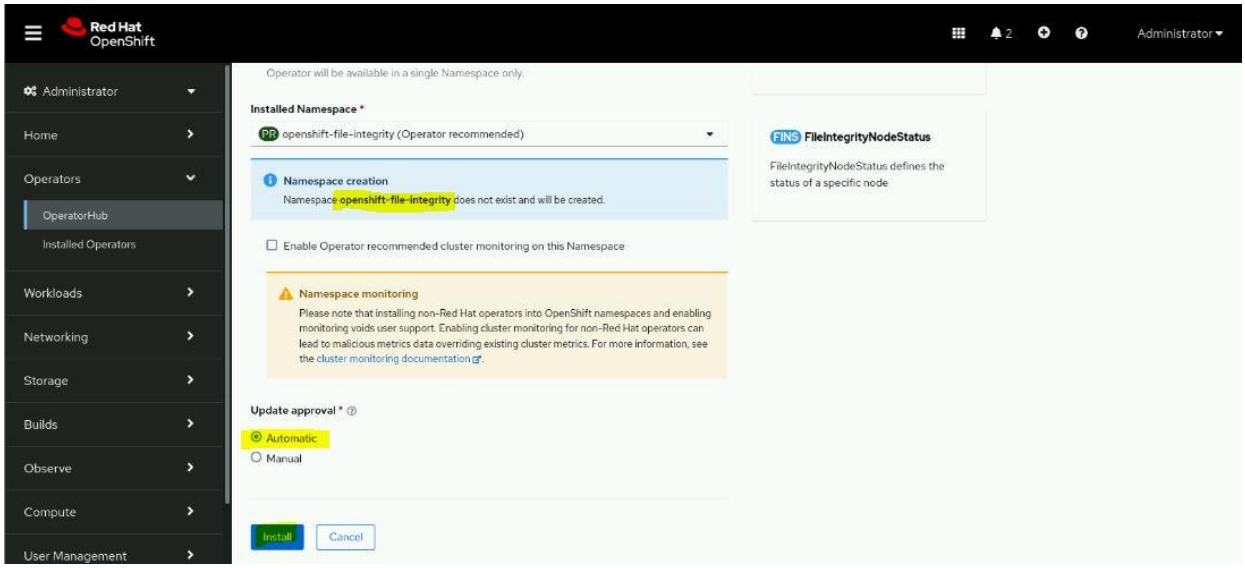
16) Install an operator called file-integrity-manager

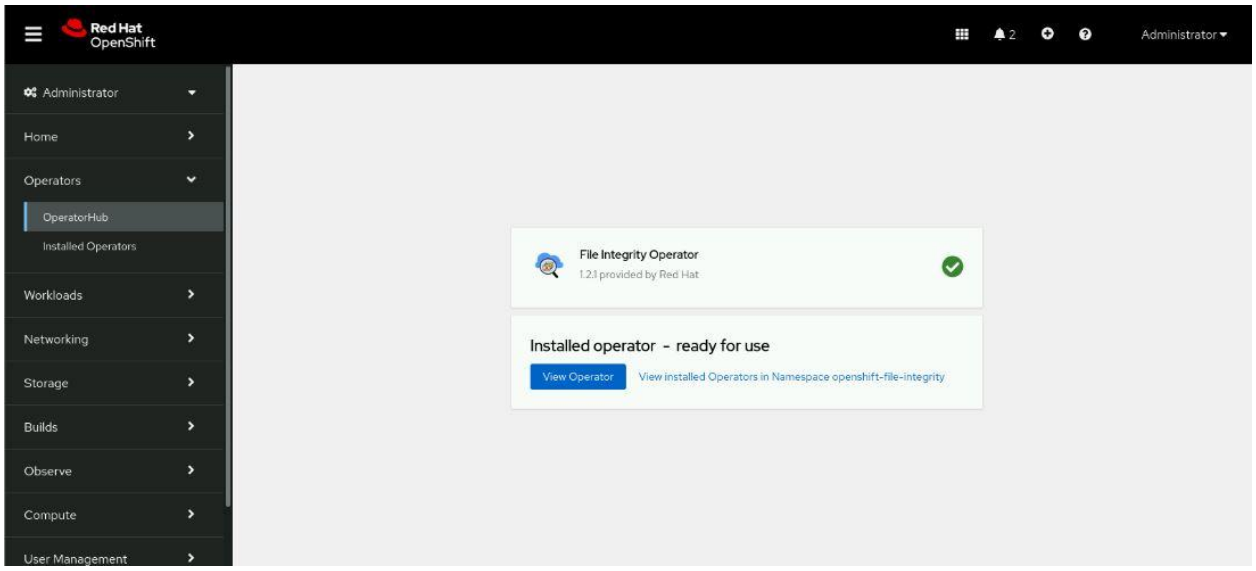
- Plan Automatic
- Using project openshift-file-integrity

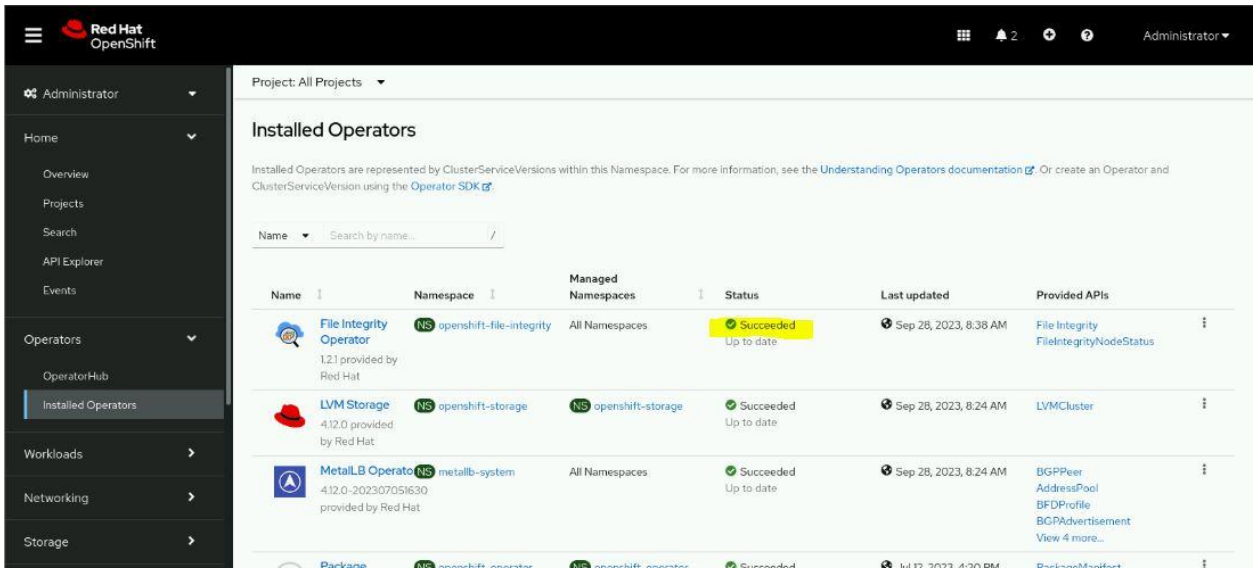

Red Hat OpenShift
Administrator
Project: All Projects
Administrator
Home
Operators
OperatorHub
Installed Operators
Workloads
Networking
Storage
Builds
Observe
Compute
All Items
Monitoring
Networking
OpenShift Optional
Security
Storage
Source
do280 Operator Catalog Red Hat (5)
Provider
Red Hat (5)
Install state
Installed (1)
Not Installed (4)
Capability level
Basic Install (2)
Seamless Upgrades (2)
All Items
Filter by keyword...
5 items
do280 Operator Catalog Red Hat
Compliance Operator
provided by Red Hat Inc.
An operator which runs OpenSCAP and allows you to keep your cluster compliant with...
File Integrity Operator
provided by Red Hat
An operator that manages file integrity checks on nodes.
LVM Storage
provided by Red Hat
Logical volume manager storage provides dynamically provisioned local storage for container...
MetalLB Operator
provided by Red Hat
An operator for deploying...
OpenShift Virtualization
provided by Red Hat
Creates and maintains an OpenShift Virtualization


Red Hat OpenShift
Administrator
Project: All Projects
File Integrity Operator
1.2.1 provided by Red Hat
Install
Latest version
1.2.1
An operator that manages file integrity checks on nodes.
Capability level
Basic Install
Seamless Upgrades
Full Lifecycle
Deep Insights
Auto Pilot
Source
do280 Operator Catalog Red Hat
Provider
Red Hat


Red Hat OpenShift
Administrator
OperatorHub > Operator Installation
Install Operator
Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.
Update channel *
stable
Installation mode *
All namespaces on the cluster (default)
Operator will be available in all Namespaces.
A specific namespace on the cluster
Operator will be available in a single Namespace only.
Installed Namespace *
openshift-file-integrity (Operator recommended)
Namespace creation
Namespace openshift-file-integrity does not exist and will be created.
Enable Operator recommended cluster monitoring on this Namespace
Namespace monitoring
File Integrity Operator
provided by Red Hat
Provided APIs
File Integrity
FileIntegrity is the Schema for the fileintegrities API
FileIntegrityNodeStatus
FileIntegrityNodeStatus defines the status of a specific node


Red Hat OpenShift
Administrator
Operator will be available in a single Namespace only.
Installed Namespace *
openshift-file-integrity (Operator recommended)
Namespace creation
Namespace openshift-file-integrity does not exist and will be created.
Enable Operator recommended cluster monitoring on this Namespace
Namespace monitoring
Please note that installing non-Red Hat operators into OpenShift namespaces and enabling monitoring voids user support. Enabling cluster monitoring for non-Red Hat operators can lead to malicious metrics data overriding existing cluster metrics. For more information, see the cluster monitoring documentation.
FileIntegrityNodeStatus
FileIntegrityNodeStatus defines the status of a specific node
Update approval *
Automatic
Manual
Install
Cancel
Home
Operators
OperatorHub
Installed Operators
Workloads
Networking
Storage
Builds
Observe
Compute
User Management


Red Hat OpenShift
Administrator
File Integrity Operator
1.2.1 provided by Red Hat
Installed operator - ready for use
View Operator
View installed Operators in Namespace openshift-file-integrity
Home
Operators
OperatorHub
Installed Operators
Workloads
Networking
Storage
Builds
Observe
Compute
User Management


Red Hat OpenShift
Administrator
Project: All Projects
Installed Operators
Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the Understanding Operators documentation. Or create an Operator and ClusterServiceVersion using the Operator SDK.
Name
Search by name...
Name
Namespace
Managed Namespaces
Status
Last updated
Provided APIs
File Integrity Operator
1.2.1 provided by Red Hat
openshift-file-integrity
All Namespaces
Succeeded
Up to date
Sep 28, 2023, 8:38 AM
File Integrity
FileIntegrityNodeStatus
LVM Storage
4.12.0 provided by Red Hat
openshift-storage
openshift-storage
Succeeded
Up to date
Sep 28, 2023, 8:24 AM
LVMCluster
MetalLB Operato
4.12.0-202307051630 provided by Red Hat
metallb-system
All Namespaces
Succeeded
Up to date
Sep 28, 2023, 8:24 AM
BGPPeer
AddressPool
BFDProfile
BGPAdvertisement
View 4 more...
Home
Overview
Projects
Search
API Explorer
Events
Operators
OperatorHub
Installed Operators
Workloads
Networking
Storage

14) Create a cronjob test-cron

- 04:05 time
- Every 2 day and every month
- Use image registry.io/imagename
- The service account and service account name is project1-sa
- Successful job history limit 14
- Project name should be cron-test

Create a cronjob using webconsole or take yaml from documentation

Both provided in instruction

```
[student@workstation ~]$ oc get all
NAME                     SCHEDULE      SUSPEND   ACTIVE   LAST SCHEDULE   AGE
cronjob.batch/cron-test   05 04 2 * *   False     0        <none>          22s
[student@workstation ~]$
```

```
        spec:
          containers:
          - args:
            - /bin/sh
            - -c
            - date; echo Hello from the Kubernetes cluster
            image: anyinge name given in exarm
            imagePullPolicy: IfNotPresent
            name: hello
            resources: {}
            terminationMessagePath: /dev/termination-log
            terminationMessagePolicy: File
          dnsPolicy: ClusterFirst
          restartPolicy: OnFailure
          schedulerName: default-scheduler
          securityContext: {}
          terminationGracePeriodSeconds: 30
  schedule: 05 04 2 * *
  successfulJobsHistoryLimit: 14
  suspend: false
status: {}
```

```
[student@workstation ~]$ # create service account
[student@workstation ~]$
[student@workstation ~]$ oc create sa jupiter
serviceaccount/jupiter created
[student@workstation ~]$ oc adm policy add-scc-to-user anyuid -z jupiter
clusterrole.rbac.authorization.k8s.io/system:openshift:scc:anyuid added: "jupiter"
[student@workstation ~]$ oc adm policy add-cluster-role-to-user cluster-admin -z jupiter
clusterrole.rbac.authorization.k8s.io/cluster-admin added: "jupiter"
[student@workstation ~]$
[student@workstation ~]$ # set service account in cron job
[student@workstation ~]$
[student@workstation ~]$ oc set sa cronjob.batch/cron-test jupiter
cronjob.batch/cron-test serviceaccount updated
[student@workstation ~]$
```

20) create an network policy to connect two pod which are resides in different projects

- First pod is in database namespace and second is in checker project
- Pod in project checker should communicate with database pod
- Create an network policy with name mysql-db-conn
- Policy uses labels to specify namespace with team=devsecops and for pods selector
- Uses label deployment=web-mysq
- Use port 3306/tcp
- Check the logs of checker pod for verification

NETWORK POLICY —>

—> USE THE LABEL GIVEN IN THE QUESTION FOR DATABASE DEPLOYMENT FROM THE YAML.

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: web-allow-prod
  namespace: default
spec:
  podSelector:
    matchLabels:
      netwroking.k8s.io/v1/network: database
  ingress:
  - from:
    - namespaceSelector:
        matchLabels:
          team: devsecops
      podSelector:
        matchLabels:
          deployment: my-web-mysql
    ports:
      - protocol: TCP
        port: 3306
```

(CREATE IN DATABASE NAMESPACE)

18) Create a pv

- Name is landing-pv
- Size - 1Gi
- Policy - retain
- Mode - ReadOnlyMany

Create a pvc

- Name is landing-pvc
- Size same as pv
- Mount pvc to /usr/share/nginx/html
- Project name is page
- Mode same as pv

Create an Deployment with

- Name landing
- Image is registry.ocp4.example.com:8443/redhattraining/hello-world-nginx:v1.0
- Application uses this link to show output http://contet.example.ocp4.com
- After attaching storage it shows desired output
- Name of deployment is landing

Solution

Check details of storage class

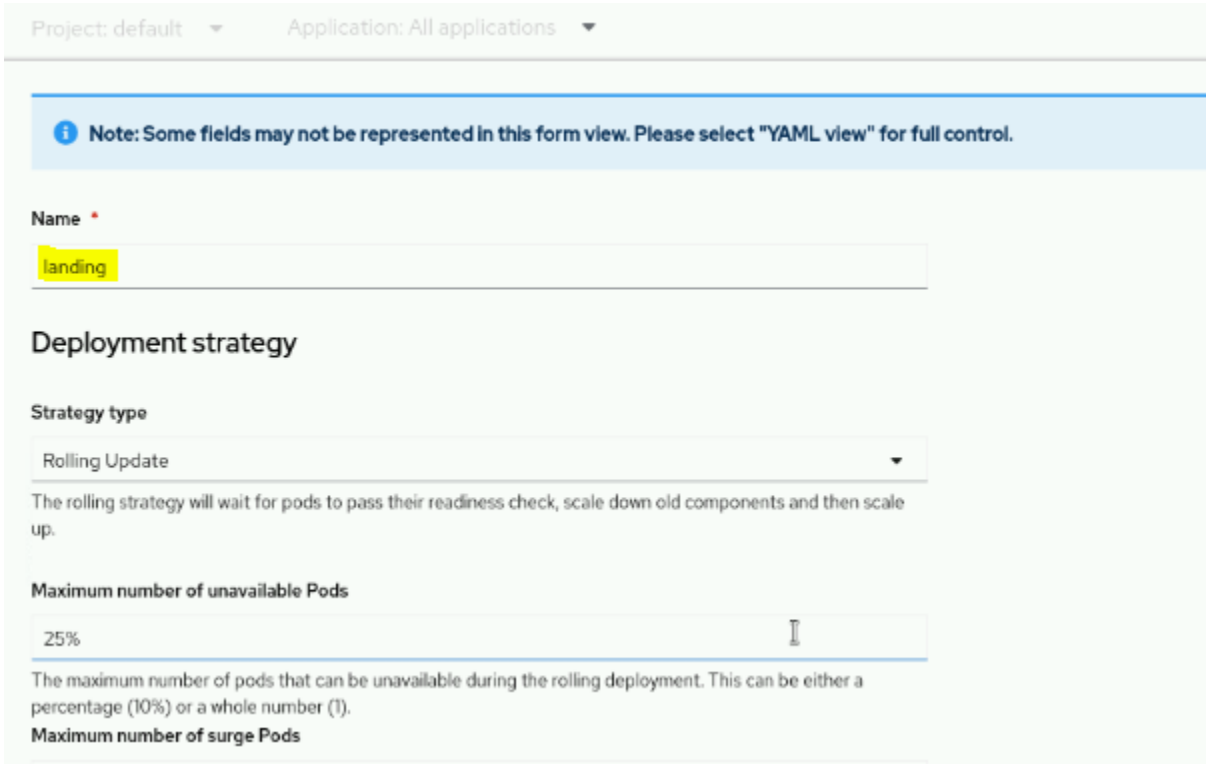
```
[student@workstation ~]$ oc describe storageclasses.storage.k8s.io nfs2
Name:                  nfs2
IsDefaultClass:        No
Annotations:           <none>
Provisioner:           example.com/external-nfs
Parameters:            path=/open001,readOnly=false,server=192.168.50.254
AllowVolumeExpansion:  <unset>
MountOptions:          <none>
ReclaimPolicy:         Delete
VolumeBindingMode:     Immediate
Events:                <none>
[student@workstation ~]$
```

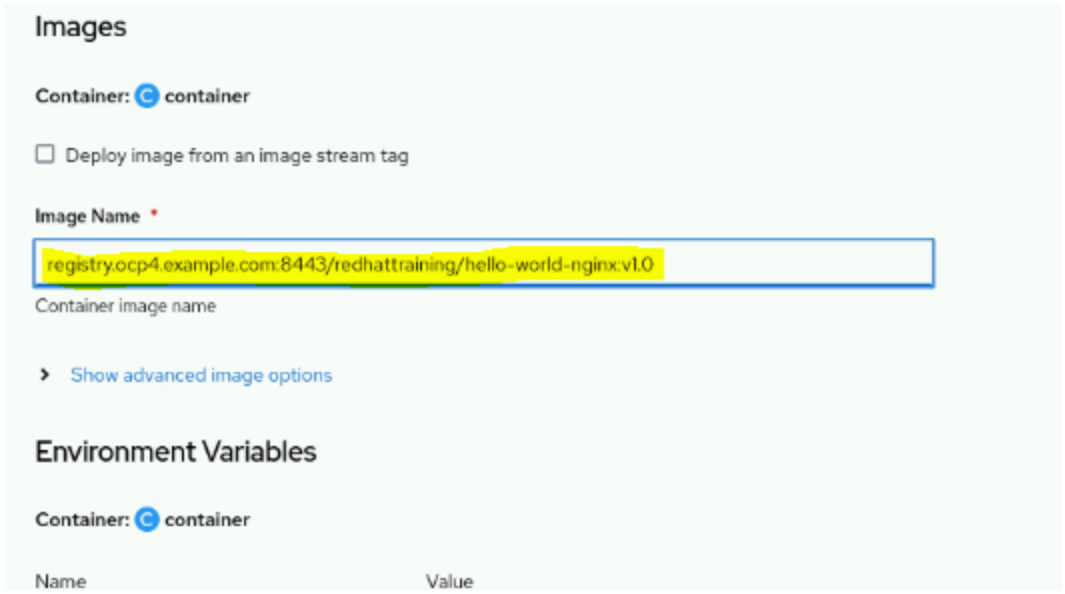
Create pv

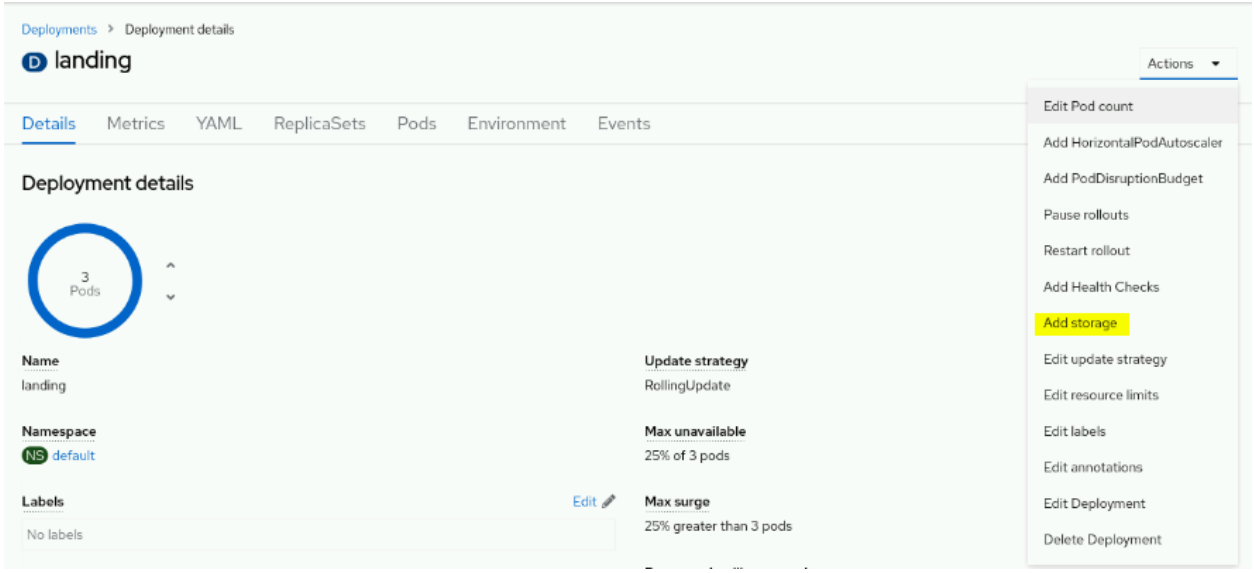
```
apiVersion: v1
kind: PersistentVolume
metadata:
  name: landing-pv
spec:
  capacity:
   storage: 1Gi
  accessModes:
  - ReadOnlyMany
  nfs:
   path: /open001
   server: 192.168.50.254
  persistentVolumeReclaimPolicy: Retain
~
~
```

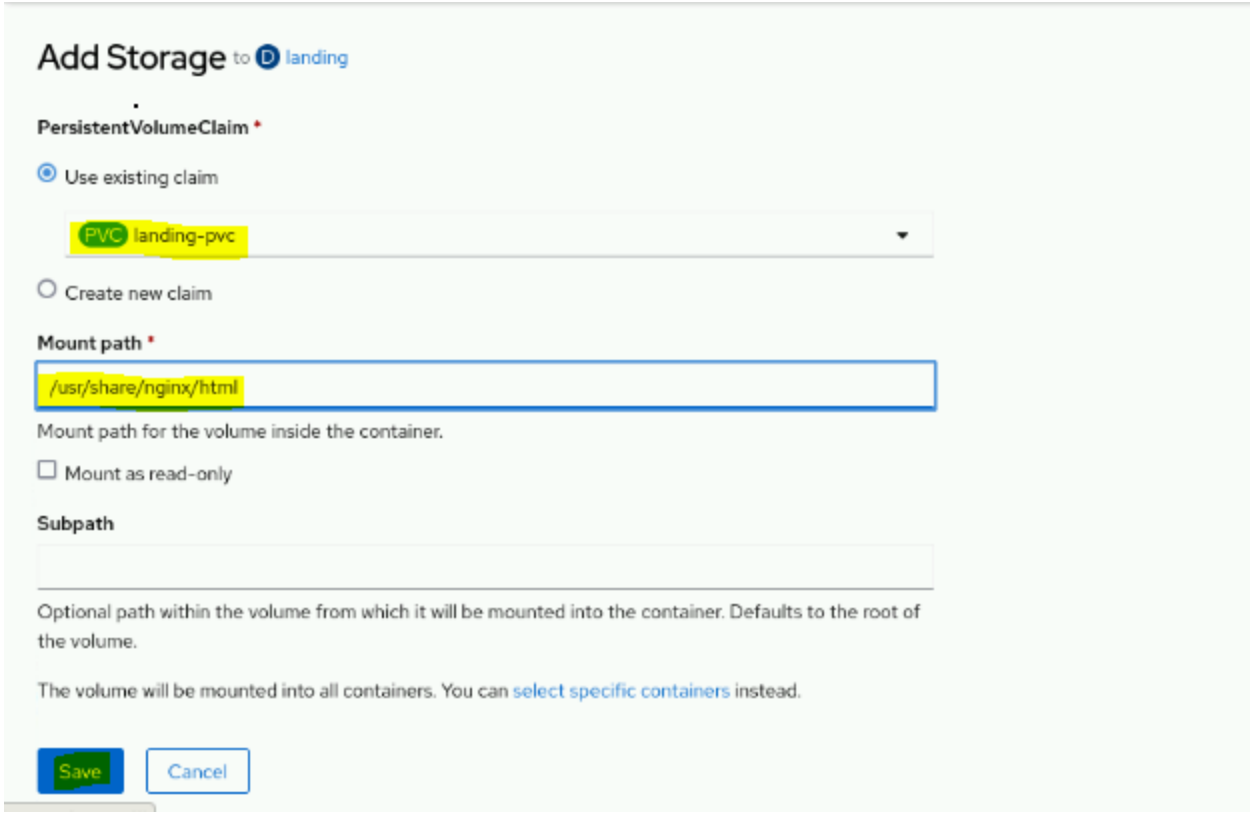
Create pvc in project page

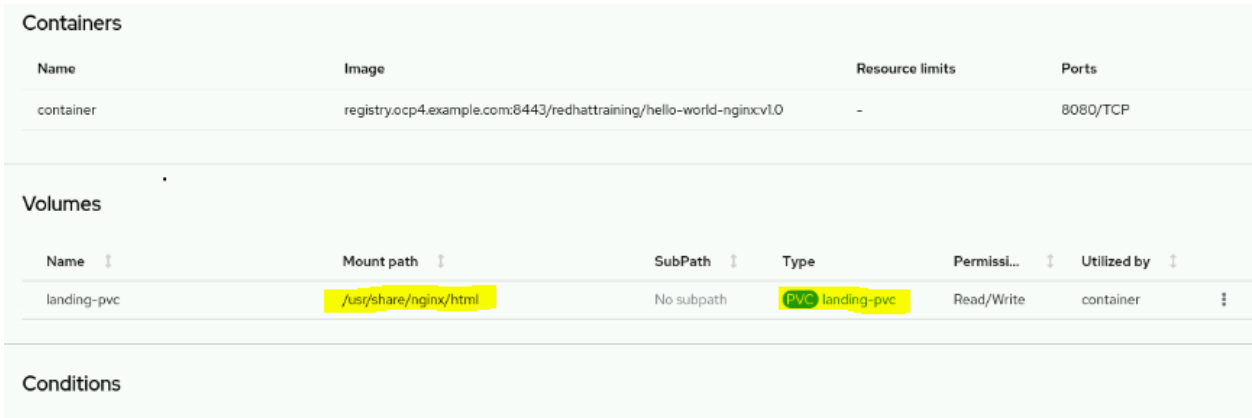
```yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: landing-pvc
spec:
  accessModes:
  - ReadOnlyMany
  resources:
   requests:
    storage: 1Gi
  storageClassName: nfs2
~
~
```




Images
Container: container
Deploy image from an image stream tag
Image Name *
registry.ocp4.example.com:8443/redhattraining/hello-world-nginx:v1.0
Container image name
Show advanced image options
Environment Variables
Container: container
Name
Value


Deployments > Deployment details
landing
Actions
Details
Metrics
YAML
ReplicaSets
Pods
Environment
Events
Deployment details
3
Pods
Name
landing
Namespace
NS default
Labels
Edit
No labels
Update strategy
RollingUpdate
Max unavailable
25% of 3 pods
Max surge
25% greater than 3 pods
Edit Pod count
Add HorizontalPodAutoscaler
Add PodDisruptionBudget
Pause rollouts
Restart rollout
Add Health Checks
Add storage
Edit update strategy
Edit resource limits
Edit labels
Edit annotations
Edit Deployment
Delete Deployment





Expose deployment
Expose svc nginx –hostname contet.example.ocp4.com
Curl on route to check

15) Create an project template with limitrange with container

- minimum memory is 5Mi max is 1Gi defaultrequest 254 Mi defaultlimit is 512 Mi .
- make sure this template available as default request new-project template for users.

Create limit range using web console and move ..

```
apiVersion: v1
kind: LimitRange
metadata:
  creationTimestamp: "2023-09-29T09:19:32Z"
  name: mem-limit-range
  namespace: "6654"
  resourceVersion: "476088"
  uid: f6f5d12b-1209-47b5-bd8b-07eab7de4080
spec:
  limits:
  - default:
      memory: 512Mi
    defaultRequest:
      memory: 256Mi
    max:
      memory: 1Gi
    min:
      memory: 128Mi
    type: Container
"/tmp/oc-edit-970466099.yaml" 23L, 575C
```

```
[student@workstation ~]$ oc adm create-bootstrap-project-template -o yaml > template.yaml
[student@workstation ~]$
[student@workstation ~]$
[student@workstation ~]$ oc get limitranges mem-limit-range -o yaml > file
```

```
[student@workstation ~]$
[student@workstation ~]$ vim template.yaml
[student@workstation ~]$ # combine both files template+limitrange
[student@workstation ~]$
[student@workstation ~]$
```

```
    kind: ClusterRole
    name: admin
  subjects:
  - apiGroup: rbac.authorization.k8s.io
    kind: User
    name: ${PROJECT_ADMIN_USER}
- apiVersion: v1
  kind: LimitRange
  metadata:
    name: ${PROJECT_NAME}-limits
  spec:
    limits:
    - default:
        memory: 512Mi
      defaultRequest:
        memory: 256Mi
      max:
        memory: 1Gi
      min:
        memory: 128Mi
      type: Container
parameters:
- name: PROJECT_NAME
- name: PROJECT_DISPLAYNAME
- name: PROJECT_DESCRIPTION
- name: PROJECT_ADMIN_USER
- name: PROJECT_REQUESTING_USER
```

```
[student@workstation ~]$ oc create -f template.yaml -n openshift-config
template.template.openshift.io/project-request created
[student@workstation ~]$
```

```
[student@workstation ~]$
[student@workstation ~]$ oc edit projects.config.openshift.io cluster
```

```
  - apiVersion: config.openshift.io/v1
    kind: ClusterVersion
    name: version
    uid: db3a68ee-9e5c-47cc-9301-b1ce0d707a0a
  resourceVersion: "1781"
  uid: 82190a26-2ff0-437c-8535-530d499f61f0
spec:
  projectRequestTemplate:
    name: project-request
```

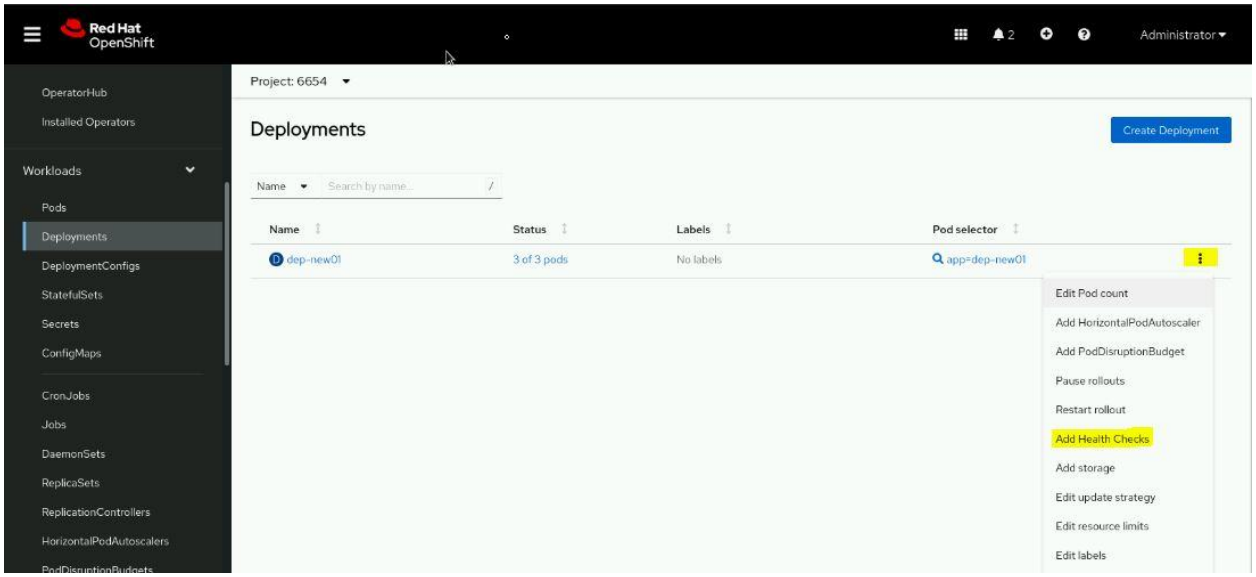
```
[student@workstation ~]$ oc edit projects.config.openshift.io cluster
project.config.openshift.io/cluster edited
[student@workstation ~]$ oc get pods -n openshift-apiserver
NAME                         READY   STATUS    RESTARTS   AGE
apiserver-7c949fbc9d-xbnlc   2/2     Running   12         148d
[student@workstation ~]$ oc get pods -n openshift-apiserver -w
NAME                         READY   STATUS        RESTARTS   AGE
apiserver-7c949fbc9d-xbnlc   2/2     Terminating   12         148d
apiserver-f9674c5b4-g57mp    0/2     Pending       0          3s
apiserver-7c949fbc9d-xbnlc   1/2     Terminating   12         148d
```

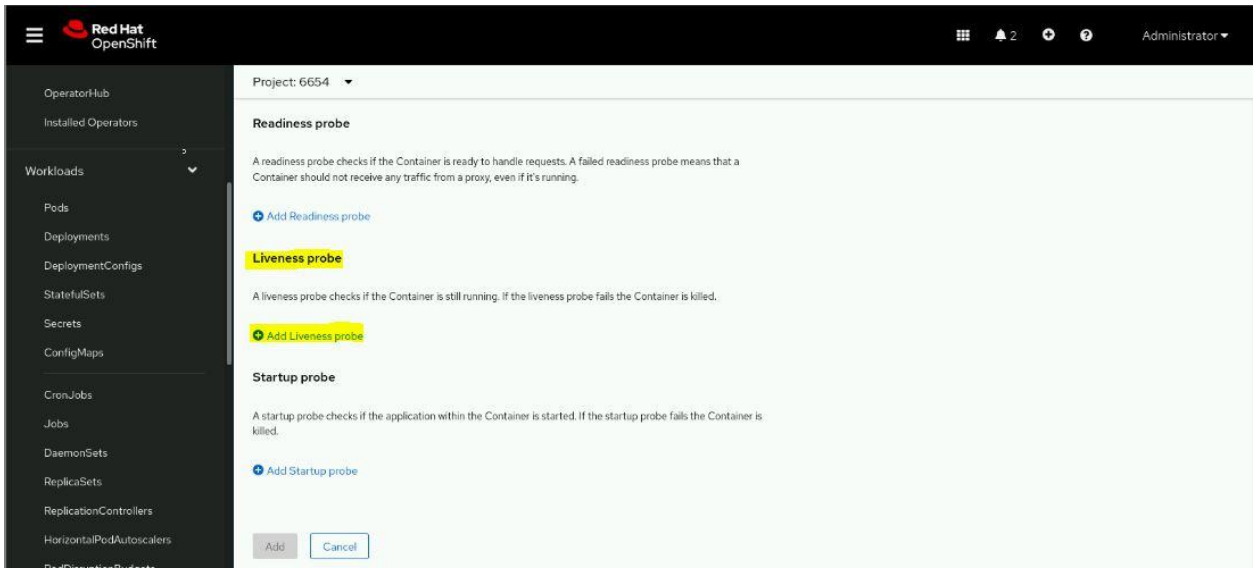
```
[student@workstation ~]$ oc get pods -n openshift-apiserver
NAME                         READY   STATUS    RESTARTS   AGE
apiserver-f9674c5b4-g57mp    2/2     Running   0          112s
[student@workstation ~]$
```

```
[student@workstation ~]$ oc new-project 9988
Now using project "9988" on server "https://api.ocp4.example.com:6443".

You can add applications to this project with the 'new-app' command. For example, try:

    oc new-app rails-postgresql-example

to build a new example application in Ruby. Or use kubectl to deploy a simple Kubernetes application:

    kubectl create deployment hello-node --image=k8s.gcr.io/e2e-test-images/agnhost:2.33 -- /agnhost serv
e-hostname

[student@workstation ~]$ oc get limitranges
NAME           CREATED AT
memtotal-mem   2023-09-29T10:07:34Z
[student@workstation ~]$ oc get limitranges -n 9988
NAME           CREATED AT
memtotal-mem   2023-09-29T10:07:34Z
[student@workstation ~]$
```

21) Start a Probe in project start

- Create a Liveliness Health Probe in project tuesday which has 1 pod running
- With port 8443
- Initial delay of 3 sec
- Time out for the probe is 10 sec
- Probe must survive atleast 3 crash





18) Collect Cluster information and create a tar file with name system10<cluster.id>.tar.gz and send it to redhat support.

- Use command tar cvaf
- One script has been provided to upload tar in redhat support
- /usr/bin/script/script system10<cluster.id>.tar.gz
- This script can be performed multiple times and it will overwrite the tar file every time

Solution:

```
[student@workstation ~]$ # collect all cluster information
[student@workstation ~]$
[student@workstation ~]$ oc adm must-gather
```

```
[student@workstation ~]$ tar cvaf system10-0ac9f411-9bc0-4cd4-9c63-1146da12ac83.tar.gz m
ust-gather.local.3396062060357082571/
```

```
pvc.yml
pv.yaml
sc.yml
system10-0ac9f411-9bc0-4cd4-9c63-1146da12ac83.tar.gz
Templates
template.yaml
Videos
[student@workstation ~]$ /usr/bin/script system10-0ac9f411-9bc0-4cd4-9c63-1146da12ac83.t
ar.gz
```