

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA Batch - 71

CS Practical 6

Scenario : Your organization is developing a Kubernetes application that needs to comply with strict security regulations. One of the requirements is to ensure that only verified, signed container images from your organization's private container registry are deployed in the Kubernetes cluster. To enforce this, you decide to implement Kubernetes image policies to control which container images can be used within the cluster.

Scenario :

You are tasked with implementing a solution to meet the following security requirements :

1. Allow only signed images from your private registry (`registry.example.com`).
2. Block any unsigned or unknown images from being pulled into the cluster.
3. Ensure that only images from specific trusted repositories (e.g., `registry.example.com/trusted-apps/*`) are permitted to run.

Steps and Screenshots :

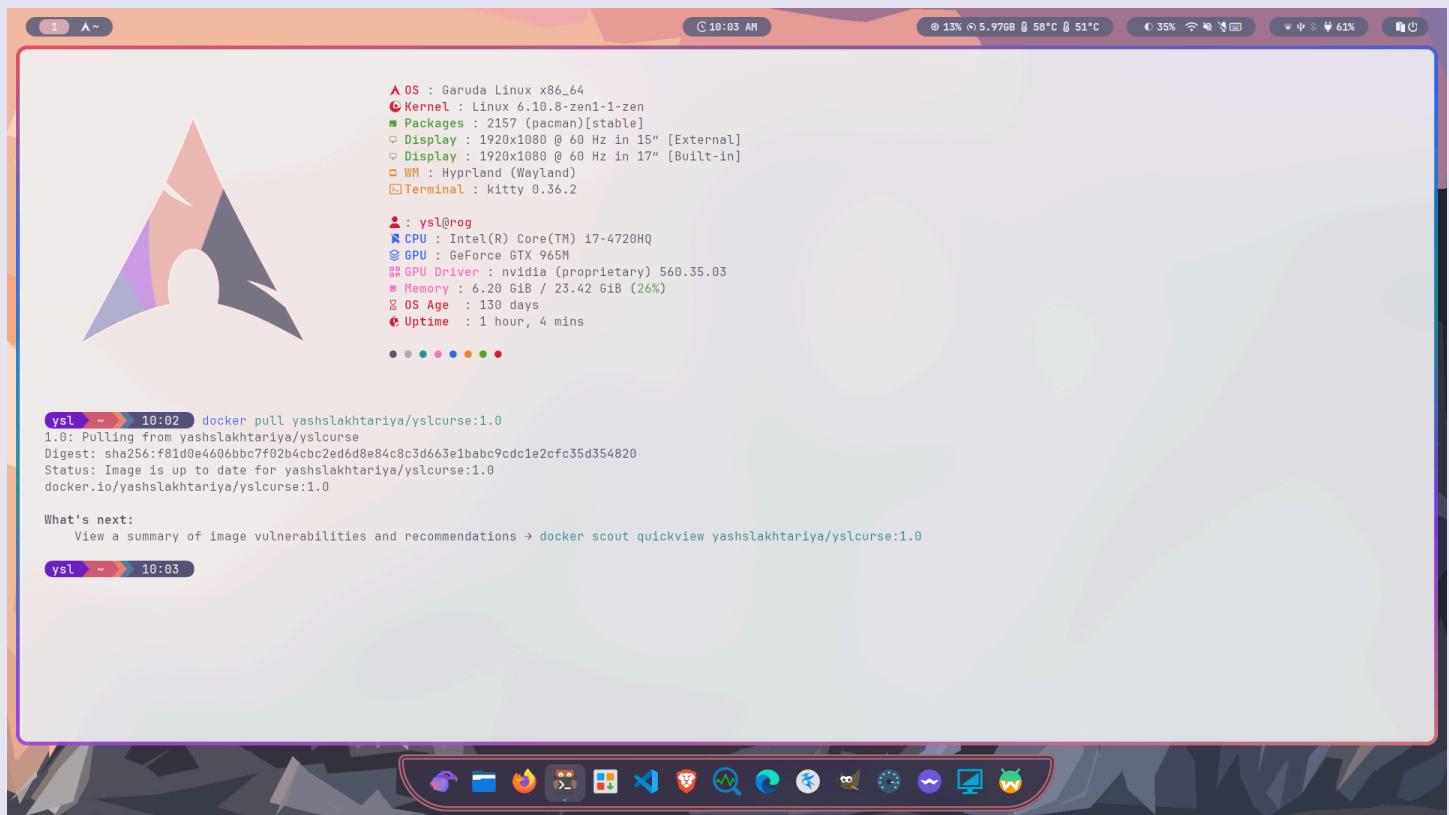
Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA Batch - 71

CS Practical 6

1. Try locally, pulling any docker image unsigned and untrusted



A screenshot of a Garuda Linux desktop environment. The terminal window shows the command `docker pull yashslakhtariya/yslcourse:1.0` being run at 10:02. The output indicates the image is up-to-date and pulled from docker.io. The desktop background features a large, stylized AEGIS logo.

```
▲ OS : Garuda Linux x86_64
● Kernel : Linux 6.10.8-zen1-1-zen
■ Packages : 2157 (pacman)[stable]
□ Display : 1920x1080 @ 60 Hz in 15" [External]
□ Display : 1920x1080 @ 60 Hz in 17" [Built-in]
□ WiFi : Hyperland (Wayland)
▣ Terminal : kitty 0.36.2

● : ysl@req
● CPU : Intel(R) Core(TM) i7-4720HQ
● GPU : GeForce GTX 965M
● GPU Driver : nvidia (proprietary) 560.35.03
● Memory : 6.20 GiB / 23.42 GiB (26%)
● OS Age : 130 days
● Uptime : 1 hour, 4 mins

● ● ● ● ● ● ●
```

```
ysl ~ 10:02 docker pull yashslakhtariya/yslcourse:1.0
1.0: Pulling from yashslakhtariya/yslcourse
Digest: sha256:f81d0e4606bbc7f02b4cbc2ed6d8e84c8c3d663e1bab9cd1e2fc35d354820
Status: Image is up to date for yashslakhtariya/yslcourse:1.0
docker.io/yashslakhtariya/yslcourse:1.0

What's next:
View a summary of image vulnerabilities and recommendations → docker scout quickview yashslakhtariya/yslcourse:1.0

ysl ~ 10:03
```

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA Batch - 71

CS Practical 6

2. Export Docker Trust environmental variable and try again, it will fail

The screenshot shows a terminal window titled 'Terminal' with a pink header. The terminal window has a light gray background and a dark gray border. At the top, there are several status icons: signal strength, battery level (8%), temperature (56°C), and network connection. The title bar also displays the time as 10:03 AM.

The terminal window contains the following text:

```
yl ~ 10:03 export DOCKER_CONTENT_TRUST=1
yl ~ 10:03 docker pull yashslakhtariya/yslcurse:1.0
What's next:
  View a summary of image vulnerabilities and recommendations → docker scout quickview yashslakhtariya/yslcurse:1.0
Error: remote trust data does not exist for docker.io/yashslakhtariya/yslcurse: notary.docker.io does not have trust data for docker.io/yashslakhtariya/yslcurse
yl ~ 10:03 |
```

Below the terminal window, the desktop environment's dock is visible, featuring a dark theme with various application icons. The desktop background is a colorful abstract design.

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA Batch - 71

CS Practical 6

3. Try pulling busybox, which is signed and trusted image from docker hub

The screenshot shows a terminal window titled 'yls' with a purple background. The terminal displays the following command and its output:

```
yls ~ 10:03 export DOCKER_CONTENT_TRUST=1
yls ~ 10:03 docker pull yashslakhtariya/yslcurse:1.0

What's next:
  View a summary of image vulnerabilities and recommendations → docker scout quickview yashslakhtariya/yslcurse:1.0
Error: remote trust data does not exist for docker.io/yashslakhtariya/yslcurse: notary.docker.io does not have trust data for docker.io/yashslakhtariya/yslcurse

yls ~ 10:03 docker pull busybox
Using default tag: latest
Pull (1 of 1): busybox:latest@sha256:34b191d63fb93e25e275bfccf1b5365664e5ac28f06d974e8d50090fbba49f41
docker.io/library/busybox@sha256:34b191d63fb93e25e275bfccf1b5365664e5ac28f06d974e8d50090fbba49f41: Pulling from library/busybox
Digest: sha256:34b191d63fb93e25e275bfccf1b5365664e5ac28f06d974e8d50090fbba49f41
Status: Image is up to date for busybox@sha256:34b191d63fb93e25e275bfccf1b5365664e5ac28f06d974e8d50090fbba49f41
Tagging busybox@sha256:34b191d63fb93e25e275bfccf1b5365664e5ac28f06d974e8d50090fbba49f41 as busybox:latest
docker.io/library/busybox:latest

What's next:
  View a summary of image vulnerabilities and recommendations → docker scout quickview busybox
yls ~ 10:03 |
```

The terminal window is part of a desktop environment, with a taskbar at the bottom showing various application icons.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 6

4. Now, try on IBM Cloud Kubernetes Cluster using image policy :

```
apiVersion: portieris.cloud.ibm.com/v1
kind: ImagePolicy
metadata:
  name: img-policy-g3-yash
spec:
  repositories:
    # Docker hub Container Registry
    - name: "docker.io/*"
      policy:

    # CoreOS Container Registry
    - name: "quay.io/*"
      policy:

    # Google Container Registry
    - name: "gcr.io/*"
      policy:

    # Azure Container Registry
    - name: "*azurecr.io/*"
      policy:

    # Amazon Elastic Container Registry
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 6

- name: "*amazonaws.com/*"

policy:

The screenshot shows a web browser window for the IBM Cloud Kubernetes interface. The URL is <https://au-syd.containers.cloud.ibm.com/kubeproxy/clusters/cr3cpfcs0m882o64nbq0/service/#/create?namespace=default>. The page title is "Create". On the left, there's a sidebar with navigation links like Config and Storage, Cluster, and Settings. The main area has tabs for "Create from input", "Create from file", and "Create from form". A text input field contains YAML code for an ImagePolicy:

```
1 apiVersion: policy.coreos.cloud.ibm.com/v1
2 kind: ImagePolicy
3 metadata:
4   name: img-policy-g3-yash
5 spec:
6   repositories:
7     # Docker hub Container Registry
8     - name: "docker.io/**"
9     policy:
10    # CoreOS Container Registry
11    - name: "quay.io/**"
12    policy:
13    # Google Container Registry
14    - name: "gcr.io/**"
15    policy:
16    # Azure Container Registry
17
```

At the bottom of the input field are "Upload" and "Cancel" buttons.

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA Batch - 71

CS Practical 6

The screenshot shows a web browser interface for managing Kubernetes resources. The URL is <https://au-syd.containers.cloud.ibm.com/kubeproxy/clusters/cr3cpfcs0m882o6nbq0/service/#/customresourcedefinition/imagepolicies.portieris.cloud.ibm.com>. The left sidebar shows navigation options like Config and Storage, Cluster, Settings, and About. The main content area shows the 'Accepted Names' section for the 'imagepolicies' CRD, with a table listing objects. One object, 'img-policy-g3-yash', is highlighted with a red box. Below it is the 'Versions' section, and further down is the 'Conditions' section, which lists two conditions: 'NamesAccepted' and 'Established', both set to True.

Name	Namespace	Created
img-policy-g3-yash	default	54 seconds ago

Name	Served	Storage
v1	True	True

Type	Status	Last transition time	Reason	Message
NamesAccepted	True	10 days ago	NoConflicts	no conflicts found
Established	True	10 days ago	InitialNamesAccepted	the initial names have been accepted

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 6

5. Create deployment from previous image from IBM Container Registry, which is not allowed in above image policy, it will return error

The screenshot shows a terminal session within a code editor interface. The terminal window title is "deployment-2.yaml - ysl-project". The terminal content is as follows:

```
File Edit Selection View Go Run Terminal Help Q ysl-project
EXPLORER ... deployment-2.yaml deployment.yaml deployment2yaml M
YSL-PROJECT > public deployment-2yaml deploymentyaml Dockerfile imagepolicyyaml ingressyaml serviceyaml textfile
deployment-2.yaml
1 apiVersion: apps/v1
2 kind: Deployment
3 metadata:
4   name: yashlanu-deployment-prjkt
5 spec:
6   selector:
7     matchLabels:
8       app: yashlanu-node-prjkt
9   replicas: 1
10  template:
11    metadata:
12      labels:
13        app: yashlanu-node-prjkt
14    spec:
15      containers:
16        - name: nodecontainer
17          image: au.icr.io/yashlani-nmspc/yslprjkt:2.0
18
19
PORTS SQL CONSOLE GITLENS TERMINAL COMMENTS
Use 'ibmcloud plugin update container-service' to upgrade the plug-in.
Use 'ibmcloud config --check-version=false' to disable update check.

OK
The configuration for cr3cpfcs0m882o64nbq0 was downloaded successfully.

Added context for cr3cpfcs0m882o64nbq0 to the current kubeconfig file.
You can now execute 'kubectl' commands against your cluster. For example, run 'kubectl get nodes'.

yml .../ysl-project P main !? 10:00 kubectl config current-context
mycluster-dal10-b3c.4x16-group3/cr3cpfcs0m882o64nbq0
yml .../ysl-project P main !? 10:00 kubectl apply -f deployment-2.yaml
Error from server: error when creating "deployment-2.yaml": admission webhook "just-hooks.securityenforcement.admission.cloud.ibm.com" denied the request:
Deny "au.icr.io/yashlani-nmspc/yslprjkt:2.0", no matching repositories in the ImagePolicies
yml .../ysl-project P main !? 10:01
```

The terminal shows the user attempting to apply the deployment configuration. The command `kubectl apply -f deployment-2.yaml` fails with an error message indicating that the admission webhook "just-hooks" denied the request because there are no matching repositories in the ImagePolicies for the specified image "au.icr.io/yashlani-nmspc/yslprjkt:2.0".

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 6

6. Now, try allowing icr registry

```
apiVersion: portieris.cloud.ibm.com/v1
kind: ImagePolicy
metadata:
  name: img-policy-g3-yashlo-only
spec:
  repositories:
    # My registry
    - name: "au.icr.io/*"
  policy:
```

The screenshot shows a terminal window within a code editor interface. The terminal command is:

```
ysl .../ysl-project > kubectl apply -f deployment.yaml
deployment.apps/yashlanu-deployment-prjkt created
```

A red box highlights the command 'kubectl apply -f deployment.yaml'. The status message 'deployment.apps/yashlanu-deployment-prjkt created' is displayed below it.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 6

7. Now, try enabling vulnerability checker via policy

```
apiVersion: portieris.cloud.ibm.com/v1
kind: ImagePolicy
metadata:
  name: img-policy-g3-yashlo-vuln
spec:
  repositories:
    # My registry
    - name: "au.icr.io/*"
  policy:
    vulnerability:
      ICCRVA:
        enabled: true
```

```
yml .../yml-project 1 main !? > 10:33 kubectl apply -f imagepolicy-3.yaml
imagepolicy.imagepolicy.portieris.cloud.ibm.com/img-policy-g3-yashlo-vuln created

yml .../yml-project 1 main !? > 10:33
```

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA **Batch - 71**

CS Practical 6

The screenshot shows a terminal window with several log entries from Kubernetes:

```
yml : ..\yml-project > main !? > 10:38 kubectl apply -f deployment-2.yaml  
deployment.apps/yashlanu-deployment-prjkt-2 created  
  
yml : ..\yml-project > main !? > 10:40 kubectl apply -f deployment-2.yaml  
deployment.apps/yashlanu-deployment-prjkt-2 unchanged  
  
yml : ..\yml-project > main !? > 10:41 kubectl apply -f deployment-2.yaml  
Error from server: error when creating "deployment-2.yaml": admission webhook "trust.hooks.securityenforcement.admission.cloud.ibm.com" denied the request:  
Failed to get Vulnerability Advisor for IBM Cloud Container Registry scan result for "au.icr.io/praveen-yagna-np/ibmimageyagna:1.0": Not found  
  
yml : ..\yml-project > main !? > 10:42 kubectl apply -f deployment-2.yaml  
Error from server: error when creating "deployment-2.yaml": admission webhook "trust.hooks.securityenforcement.admission.cloud.ibm.com" denied the request:  
Failed to get Vulnerability Advisor for IBM Cloud Container Registry scan result for "au.icr.io/kirtannamespace/newkirtanimg": Not found  
  
yml : ..\yml-project > main !? > 10:44
```

Below the terminal, the status bar shows:

Ln 17, Col 54 Spaces: 2 UTF-8 LF ↵ YAML ⌘ Go Live ⌘ Prettier

(As seen, trying different images gives error due to issues in vulnerability checker, but otherwise it should give error of unsafe image)