**Scenario**

Your company has recently decided to use Docker to run containers in production. They have built some Docker images to run their own proprietary software and need a place to store and manage these images. You have been asked to build a secure, private Docker registry for use by the company. In order to verify that everything works, you have also been asked to configure a Docker workstation server to push to and pull from the registry.

To complete this lab, ensure that the following requirements are met for the registry:

1. A private Docker registry is running on the Docker registry server using version 2 of the registry image.

docker run -d -p 5000:5000 --name registry registry:2

docker run -d -p 443:5000 --restart=always -v /reg:/var/lib/registry --name registry registry:2

2. The container name for the registry should be registry.

3. The registry should always automatically restart if it stops or the Docker daemon or server restarts.

4. The registry should require authentication. Set up an initial account with the username docker and the password d0ck3rrU73z.

5. The registry should use TLS with a self-signed certificate.

6. The registry should listen on port 443.

Set up the Docker workstation server to meet the following requirements:

1. Docker is logged in to the private registry.

2. Docker is configured to accept the self-signed cert. Do not turn off certificate verification using the insecure-registries setting.

3. To confirm that everything is working, push a test image called ip-10-0-1-101:443/test-image:1 to the private registry. You can pull any image from Docker hub and tag it with ip-10-0-1-101:443/test-image:1 as a test.

4. Delete the test image locally and pull it from the registry.

[NOTE: Write the series of commands to achieve above in this file below the question scenario with documentation]

=========================================================================================================================================

**Solution** 🡪

**Start a simple registry server**

docker run -d -p 443:5000 --restart=always -v /reg:/var/lib/registry --name registry registry:2

vi /lib/systemd/system/docker.service

Append this ‘-insecure-registry ip\_address:5000’ at the end of this line:

ExecStart=/usr/bin/dockerd -H fd:// –insecure-registry 172.17.0.139:443

service docker restart

systemctl daemon-reload

Confirm the docker registry is up and running:

curl -v 172.17.0.54:443/v2/

**Setup a self signed certificate**

mkdir -p docker\_reg\_certs

openssl req -newkey rsa:4096 -nodes -sha256 -keyout docker\_reg\_certs/domain.key -x509 -days 365 -out docker\_reg\_certs/domain.crt

install the certificates both in the server and the client by running these commands:

#come out of root

mkdir -p /etc/docker/certs.d/172.17.0.54:443

cp /root/docker\_reg\_certs/domain.crt /etc/docker/certs.d/172.17.0.54:443/ca.crt

cp /root/docker\_reg\_certs/domain.crt /usr/local/share/ca-certificates/ca.crt

Update certificates 🡪

update-ca-certificates

**Add user authentication for registry access**

mkdir docker\_reg\_auth

cd docker\_reg\_auth

docker run -it --entrypoint htpasswd -v $PWD/docker\_reg\_auth:/auth -w /auth registry:2 -Bbc /auth/htpasswd docker d0ck3rrU73z

service docker restart

**Start registry service with the new config**:

docker run -d -p 443:5000 --restart=always --name registrry -v $PWD/docker\_reg\_certs:/certs -v $PWD/docker\_reg\_auth:/auth -v /reg:/var/lib/registry -e REGISTRY\_HTTP\_TLS\_CERTIFICATE=/certs/domain.crt -e REGISTRY\_HTTP\_TLS\_KEY=/certs/domain.key -e "REGISTRY\_AUTH\_HTPASSWD\_REALM=Registry Realm" -e REGISTRY\_AUTH\_HTPASSWD\_PATH=/auth/htpasswd -e REGISTRY\_AUTH=htpasswd registry:2

Login to docker ,Push & pull images

docker login -udocker -pd0ck3rrU73z 172.17.0.54:443

#error - Using --password via the CLI is insecure. Use --password-stdin.

or

docker login --username docker --password-stdin

docker push 172.17.0.54:443/hello-world

docker pull q72.17.0.54:443/testing/test-image:1

docker logout

To retrieve list of all repositories in your private docker registry:

curl -u docker:d0ck3rrU73z -v -X GET <https://172.17.0.54:443/v2/_catalog>

Referances ---??

https://www.exoscale.com/syslog/setup-private-docker-registry/

https://docs.docker.com/registry/insecure/

https://www.exoscale.com/syslog/setup-private-docker-registry/

https://medium.com/@ifeanyiigili/how-to-setup-a-private-docker-registry-with-a-self-sign-certificate-43a7407a1613