

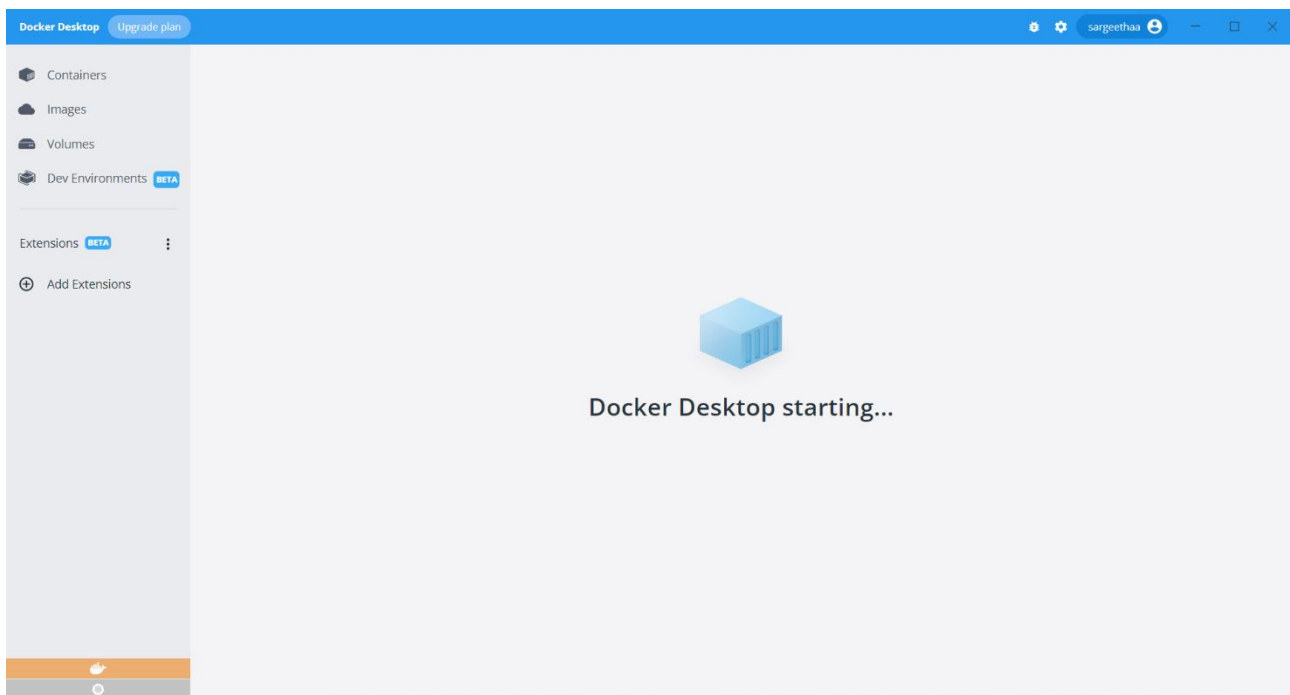
DEPLOYMENT OF APP IN IBM CLOUD

CONTAINERIZE THE APP

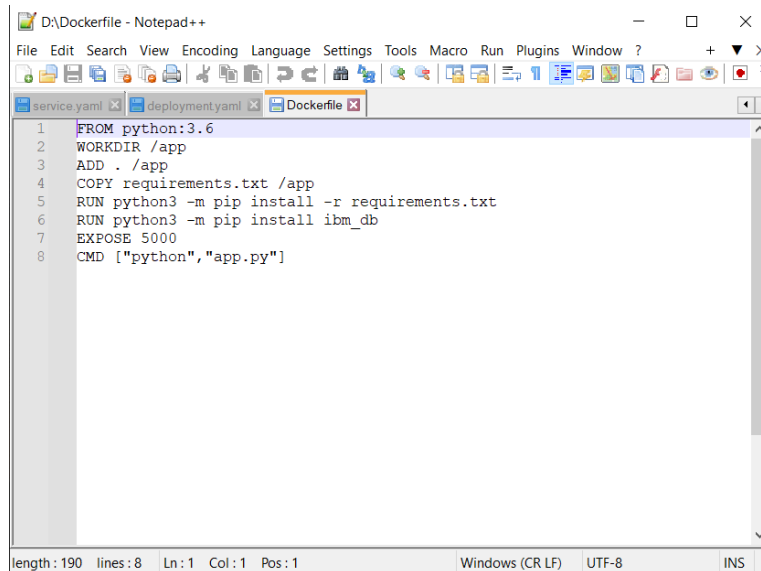
Date	30 October 2022
Team ID	PNT2022TMID54057
Project Name	Nutrition Assistant Application
Maximum Marks	4 Marks

CONTAINERIZE THE APP OF DEPLOYMENT :

DESKTOP :

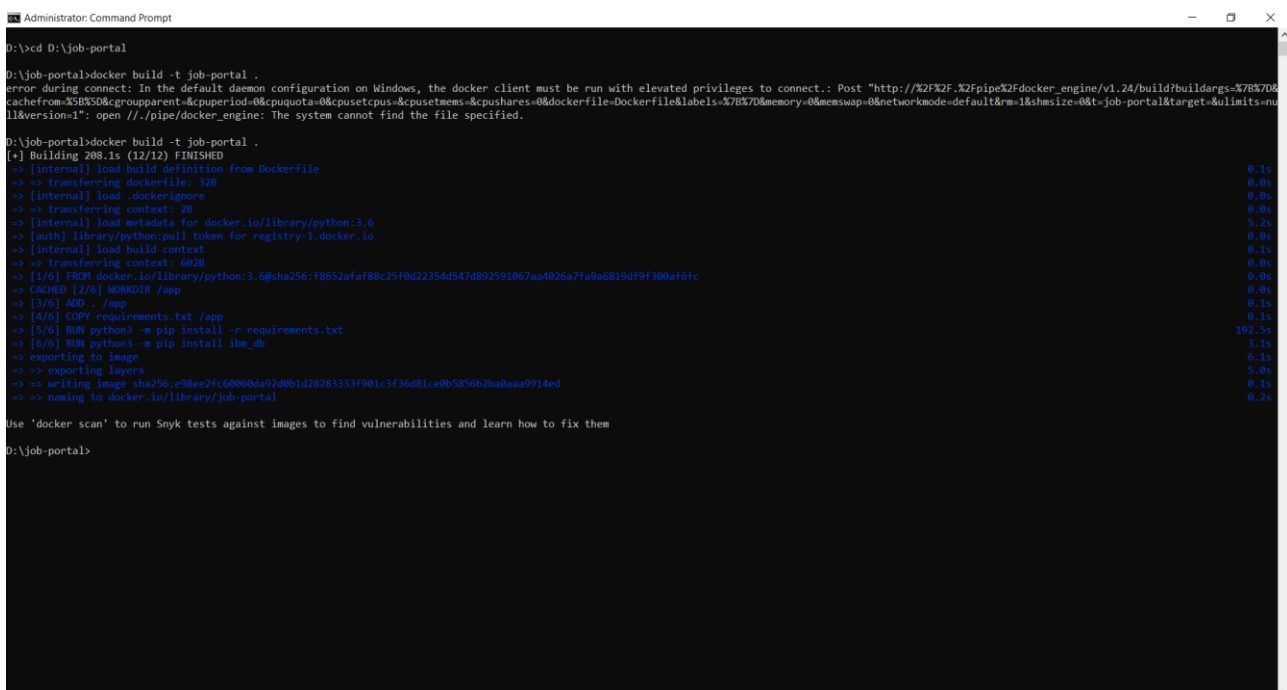


DOCKER FILE :



```
1 FROM python:3.6
2 WORKDIR /app
3 ADD . /app
4 COPY requirements.txt /app
5 RUN python3 -m pip install -r requirements.txt
6 RUN python3 -m pip install ibm_db
7 EXPOSE 5000
8 CMD ["python", "app.py"]
```

BUILDING THE REPOSITORY CONTAINER :



```
D:\job-portal>docker build -t job-portal .
error during connect: In the default daemon configuration on Windows, the docker client must be run with elevated privileges to connect.: Post "http://X2F32F.X2FpipeX2Fdocker_engine/v1.24/build?buildargs=X7B57D&
cachefrom=X5B3X0&cgroupparent=&cgroupquota=&cpusetcpus=&cpusetmems=&cpushares=&@&dockerfile=Dockerfile&labels=X7B57D&memory=&mcmemswap=&mnetworkmode=default&rm=1&shmsize=&@&t=job-portal&target=&ulimits=nu
ll&version=1": open //./pipe/docker_engine: The system cannot find the file specified.

D:\job-portal>docker build -t job-portal .
[+] Building 208.1s (12/12) FINISHED
=> [internal] load build definition from Dockerfile 0.15s
=> => transferring Dockerfile: 32B 0.04s
=> [internal] load .dockerignore 0.05s
=> => transferring context: 2B 0.04s
=> [internal] load metadata for docker.io/library/python:3.6 5.24s
=> [auth] library/python:pull token for registry-1.docker.io 0.04s
=> [internal] load build context 0.15s
=> => transferring context: 602B 0.04s
=> [1/6] FROM docker.io/library/python:3.6@sha256:f8652afaf88c25f0d22354d547d892591067aa4826a7fa9a6819df9f300af6fc 0.05s
=> CACHED [2/6] WORKDIR /app 0.05s
=> [3/6] ADD . /app 0.14s
=> [4/6] COPY requirements.txt /app 0.14s
=> [5/6] RUN python3 -m pip install -r requirements.txt 192.55s
=> [6/6] RUN python3 -m pip install ibm_db 3.14s
=> exporting to image 5.15s
=> => exporting layers 5.04s
=> => writing image sha256:e98ee2fc6006dda92d0b1d2828333f901c3f36d81ce0b5856b2ba0aaa9914ed 0.14s
=> => naming to docker.io/library/job-portal 0.24s

Use 'docker scan' to run Snyk tests against images to find vulnerabilities and learn how to fix them

D:\job-portal>
```

CONTAINER:

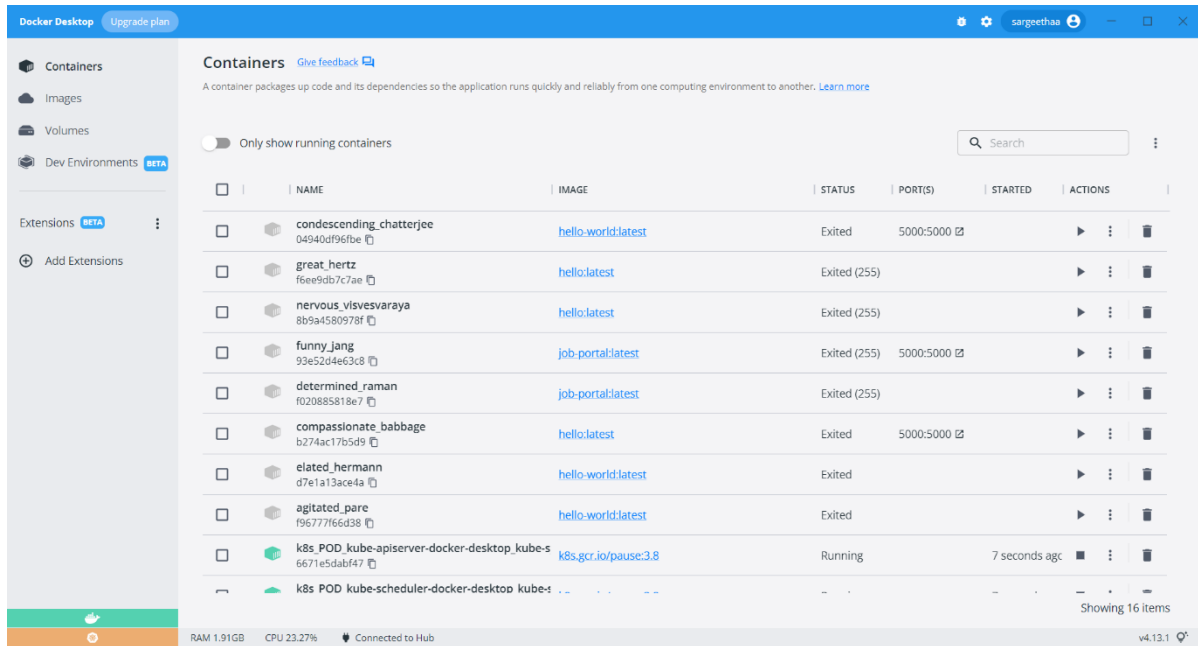


IMAGE :

