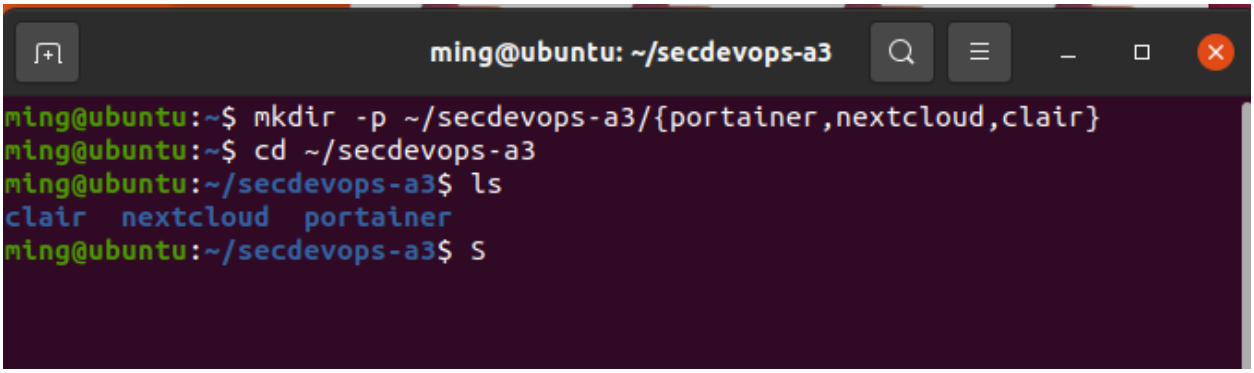
Assignment 3
Secure DevOps Pipeline for Application Deployment

Unit: ISEC6000 Secure DevOps
Name: Ming Yong Tan
Student ID: 21920794
Github repo link:
1. https://github.com/mingyongtan/task1-2-3_devsops_21920794/tree/main
2. https://github.com/mingyongtan/express-es6-sample
4. https://github.com/mingyongtan/threatdragon_devsops_21920794

Task 1 — Docker & Compose

1.1 Install Docker Engine + Compose

Quick Folder setup for the assignment. All folders given from the assessment are already unzipped and moved to the folder below.



Delete any existing container and update package before install docker

sudo apt-get update -y

sudo apt-get install -y ca-certificates curl gnupg lsb-release

sudo install -m 0755 -d /etc/apt/keyrings

curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg

echo "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg] https://download.docker.com/linux/ubuntu $(. /etc/os-release && echo $UBUNTU_CODENAME) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

sudo apt-get update -y

sudo apt-get install -y docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin

Versions for evidence

docker --version

docker compose version

```
ming@ubuntu:~$ sudo apt-get remove -y docker docker-engine docker.io containerd
runc || true
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package 'docker-engine' is not installed, so not removed
Package 'docker' is not installed, so not removed
Package 'containerd' is not installed, so not removed
Package 'runc' is not installed, so not removed
Package 'docker.io' is not installed, so not removed
0 upgraded, 0 newly installed, 0 to remove and 120 not upgraded.
ming@ubuntu:~$ sudo apt-get update -y
Hit:1 https://download.docker.com/linux/ubuntu focal InRelease
Hit:2 https://packages.microsoft.com/repos/code stable InRelease
Hit:3 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:5 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:6 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
ming@ubuntu:~$ sudo apt-get install -y ca-certificates curl gnupg lsb-release
Reading package lists... Done
```

```
ming@ubuntu:~$ # Docker's official repo
ming@ubuntu:~$ sudo install -m 0755 -d /etc/apt/keyrings
ming@ubuntu:~$ curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gp
g --dearmor -o /etc/apt/keyrings/docker.gpg
ming@ubuntu:~$ echo \
> "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg
] \
> https://download.docker.com/linux/ubuntu $(. /etc/os-release && echo $UBUNTU_C
ODENAME) stable" | \
> sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
ming@ubuntu:~$ sudo apt-get update -y
Hit:1 https://download.docker.com/linux/ubuntu focal InRelease
Hit:2 https://packages.microsoft.com/repos/code stable InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:4 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:5 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:6 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
ming@ubuntu:~$
ming@ubuntu:~$
ming@ubuntu:~$ # Engine + CLI + Buildx + Compose plugin
ming@ubuntu:~$ sudo apt-get install -y docker-ce docker-ce-cli containerd.io doc
```

```
ming@ubuntu:~$ # Engine + CLI + Buildx + Compose plugin
ming@ubuntu:~$ sudo apt-get install -y docker-ce docker-ce-cli containerd.io doc
ker-buildx-plugin docker-compose-plugin
Reading package lists... Done
Building dependency tree
Reading state information... Done
containerd.io is already the newest version (1.7.27-1).
docker-buildx-plugin is already the newest version (0.23.0-1~ubuntu.20.04~focal)
.
docker-ce-cli is already the newest version (5:28.1.1-1~ubuntu.20.04~focal).
docker-ce is already the newest version (5:28.1.1-1~ubuntu.20.04~focal).
docker-compose-plugin is already the newest version (2.35.1-1~ubuntu.20.04~focal
).
0 upgraded, 0 newly installed, 0 to remove and 120 not upgraded.
ming@ubuntu:~$
ming@ubuntu:~$
ming@ubuntu:~$ # Version evidence
ming@ubuntu:~$ docker --version
Docker version 28.1.1, build 4eba377
ming@ubuntu:~$ docker compose version
Docker Compose version v2.35.1
ming@ubuntu:~$
```

1.2 Restrict Docker to sudo only

Refresh session (so the group removal takes effect):

exec su -l "$USER" – Starts a fresh login shell so the group removal takes effect immediately.

```
ming@ubuntu:~$ exec su -l "$USER"
Password:
ming@ubuntu:~$ id; groups
uid=1000(ming) gid=1000(ming) groups=1000(ming),4(adm),24(cdrom),27(sudo),30(dip
),46(plugdev),120(lpadmin),132(lxd),133(sambashare)
ming adm cdrom sudo dip plugdev lpadmin lxd sambashare
ming@ubuntu:~$ docker ps
permission denied while trying to connect to the Docker daemon socket at unix://
/var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.49/containers/js
on": dial unix /var/run/docker.sock: connect: permission denied
ming@ubuntu:~$ sudo docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES
ming@ubuntu:~$
```

1.3 Short Security Summary (why this restriction matters)

- dockerd runs as root; access to /var/run/docker.sock is effectively root-equivalent (you can start privileged containers, mount /, modify network/iptables, read host files, etc.).
- Requiring sudo enforces least privilege and records actions in sudo audit logs.

- This reduces the blast radius from compromised low-priv accounts or scripts and prevents silent misuse of the Docker daemon.

Task 2: Deploy Portainer for Docker Management

2.1 Download and inspect compose.yaml file.

Download the file from the blackboard and insert it into secdevops-a3/portainer folder.

```
ming@ubuntu:~$ cd secdevops-a3
ming@ubuntu:~/secdevops-a3$ ls
clair  nextcloud  portainer
ming@ubuntu:~/secdevops-a3$ cd portainer
ming@ubuntu:~/secdevops-a3/portainer$ ls
compose.yaml  README.md
ming@ubuntu:~/secdevops-a3/portainer$
```

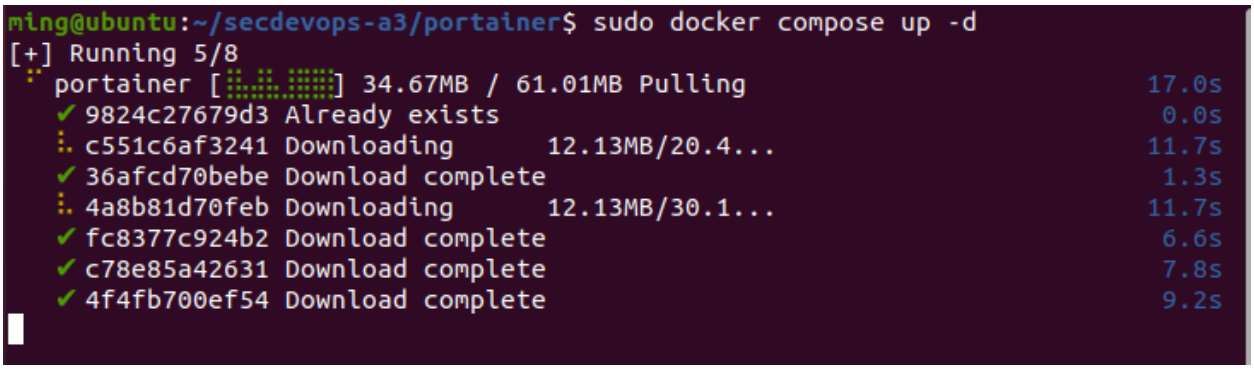
```
ming@ubuntu:~/secdevops-a3/portainer$ sed -n '1,200p' compose.yaml
services:
  portainer:
    image: portainer/portainer-ce:alpine
    container_name: portainer
    command: -H unix:///var/run/docker.sock
    ports:
      - "9000:9000"
    volumes:
      - "/var/run/docker.sock:/var/run/docker.sock"
      - "portainer_data:/data"
    restart: always

volumes:
  portainer_data:ming@ubuntu:~/secdevops-a3/portainer$
```

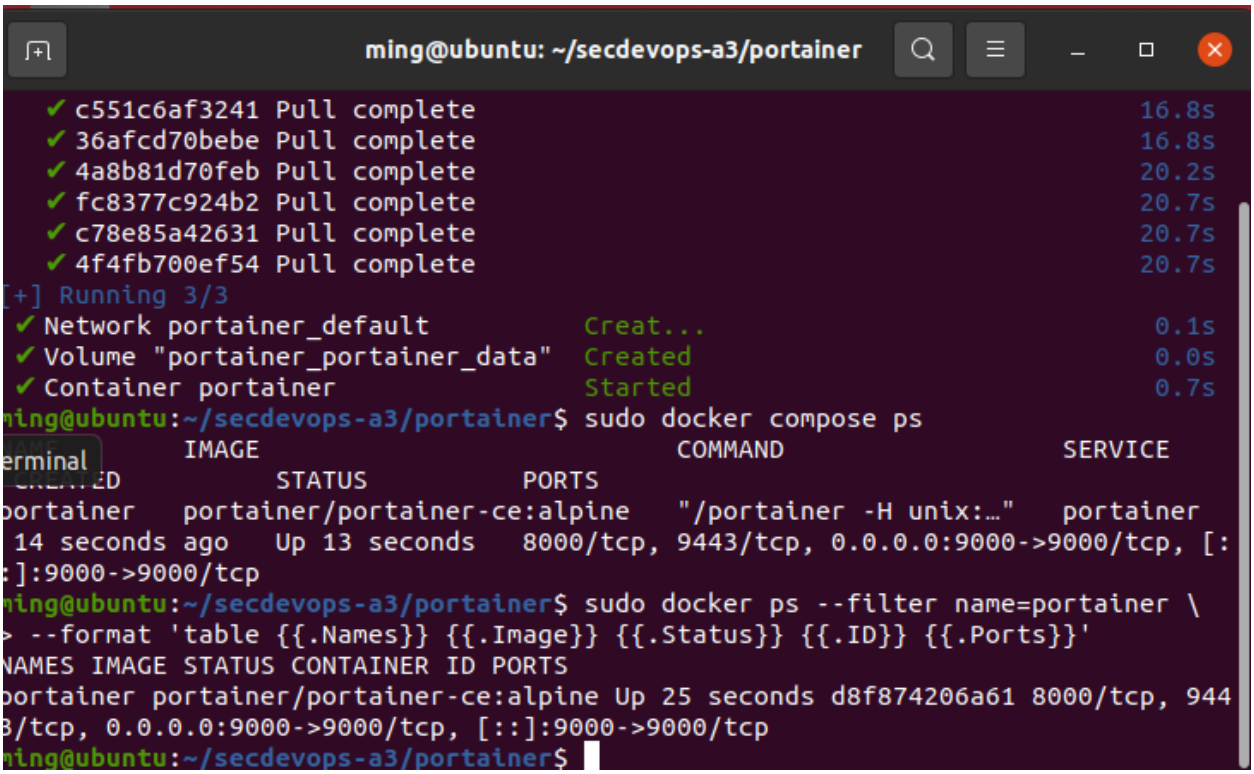
2.2 Valid restart options

- no – never restart (default if not set)
- on-failure[:N] – restart only on non-zero exit (optionally up to N times)
- always – always restart if it stops
- unless-stopped – restart unless you explicitly stop it

2.3 Deploy Portainer stack

a. Report the steps with evidence (e.g., screenshots). You must show evidence that atleast one container is running. Additionally, report the detail of the deployed Portainer container (e.g., Status, Id etc).



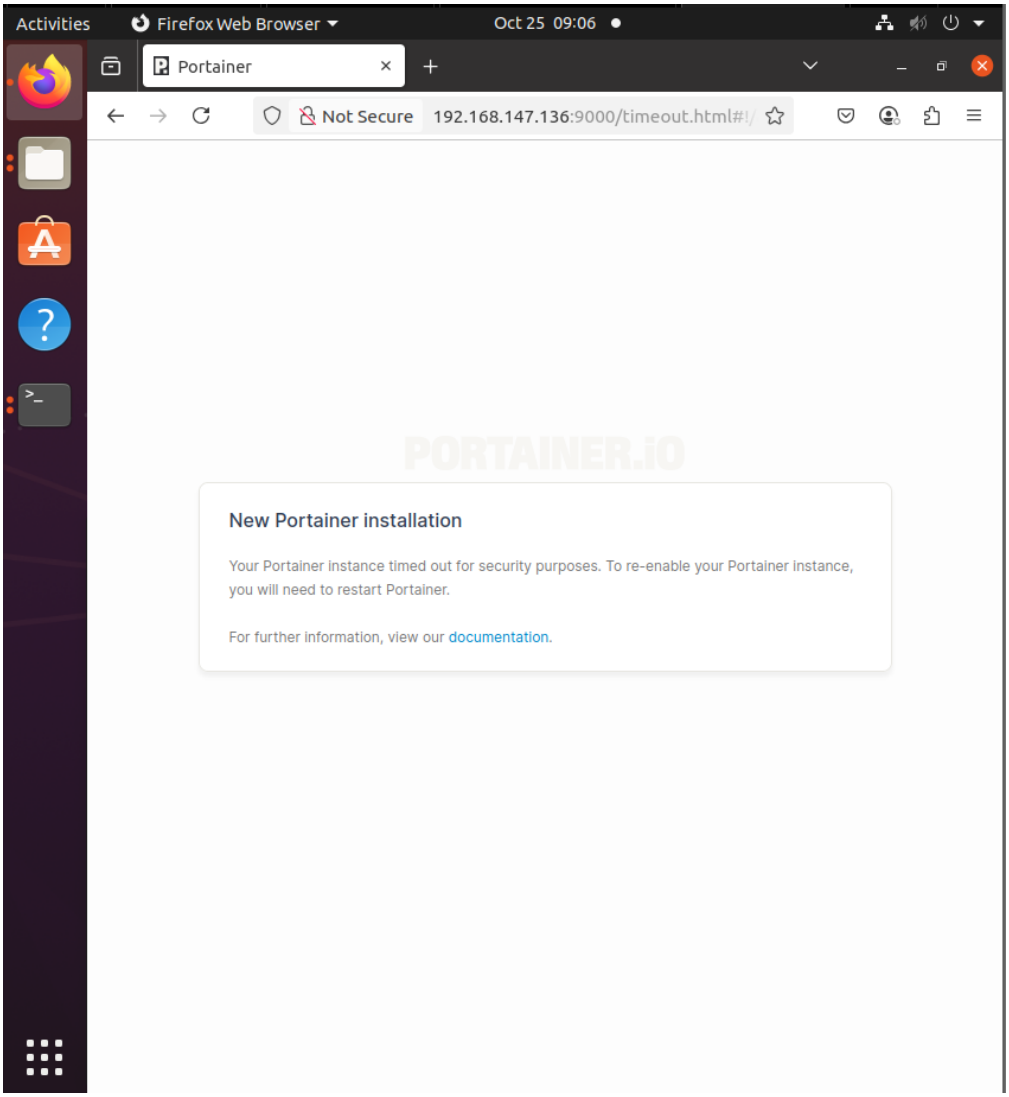


Evidence: screenshot docker compose ps showing at least one running container; screenshot the docker ps table (Status, ID, Ports).

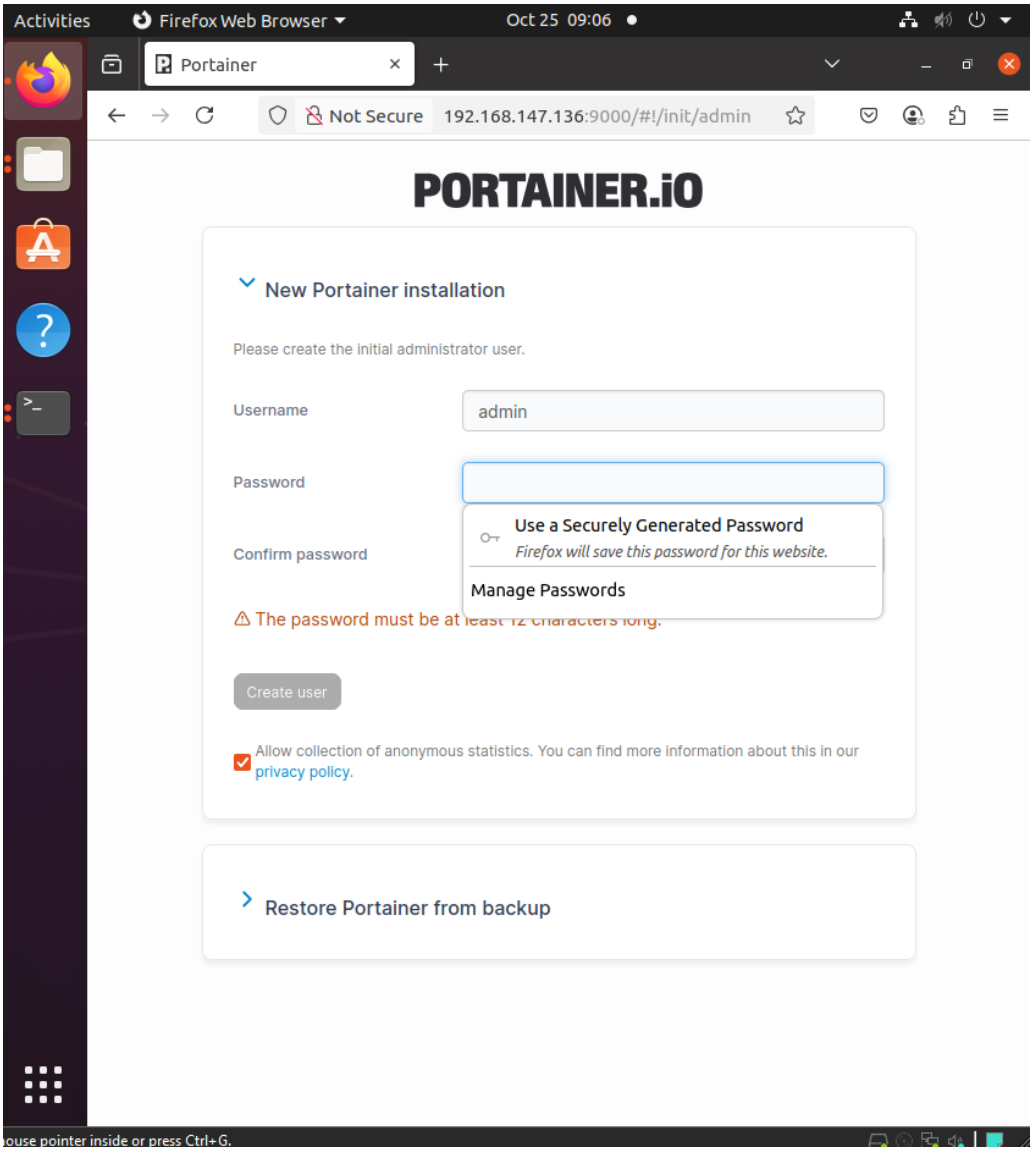
b. Navigate in your web browser to access the Portainer web interface and create an account. Don't forget to attach the related screenshot in the report.

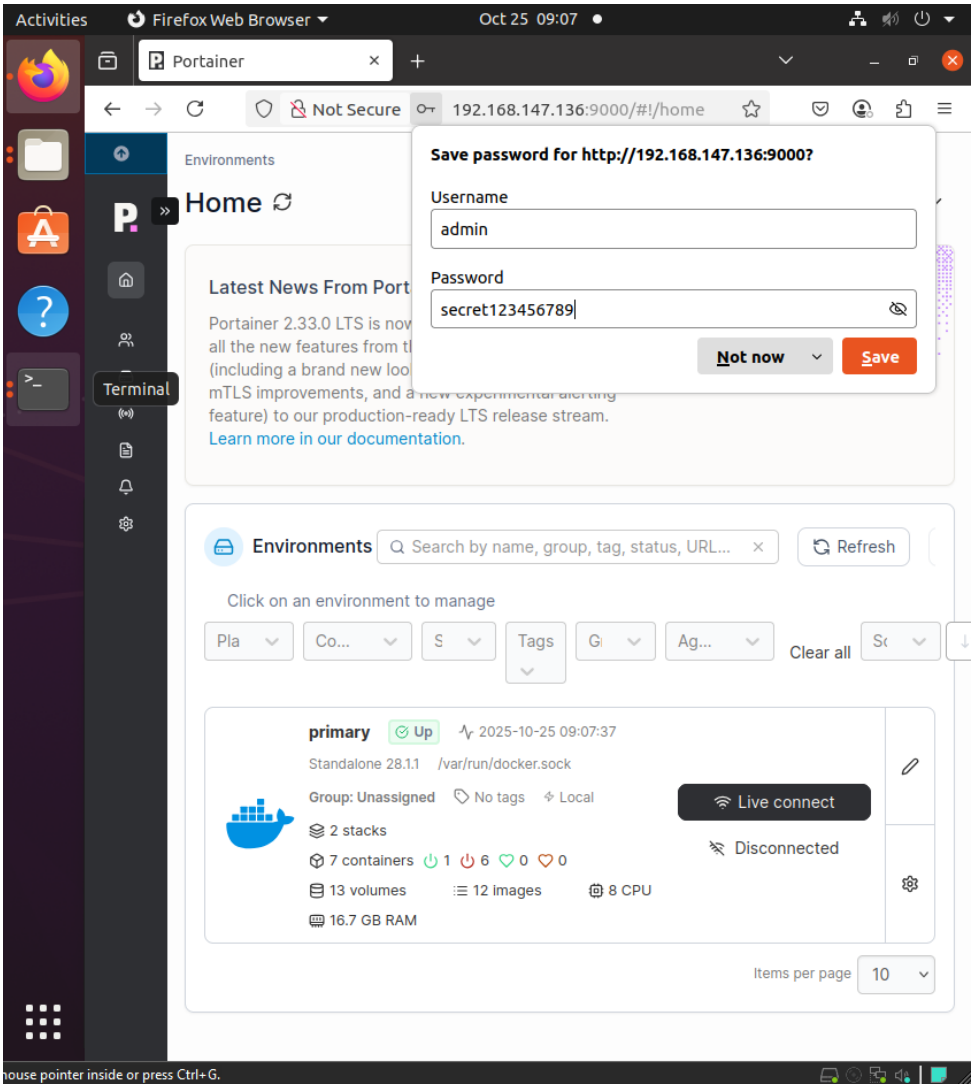
http://192.168.147.136:9000

Ming Yong Tan 21920794



Ming Yong Tan 21920794





2.4 Access log monitoring

a. Show the three most recent lines of logs from the running stack. (Both the Docker-compose CLI command and output should be reported.)

sudo docker compose logs --tail=3

shows the most recent events from the running stack

```
ming@ubuntu:~/secdevops-a3/portainer$ sudo docker compose logs --tail=3
portainer  | 2025/10/25 04:06PM INF github.com/portainer/portainer/api/cmd/porta
iner/main.go:636 > starting Portainer | build_number=232 go_version=1.24.6 image
_tag=2.33.2-linux-amd64 nodejs_version=18.20.8 version=2.33.2 webpack_version=5.
88.2 yarn_version=1.22.22
portainer  | 2025/10/25 04:06PM INF github.com/portainer/portainer/api/http/serv
er.go:367 > starting HTTPS server | bind_address=:9443
portainer  | 2025/10/25 04:06PM INF github.com/portainer/portainer/api/http/serv
er.go:351 > starting HTTP server | bind_address=:9000
ming@ubuntu:~/secdevops-a3/portainer$
```

b. Access and filter Portainer log for any suspicious activities.

sudo docker logs portainer --since 30m 2>&1 | \

egrep -i 'fail|error|unauth|forbidden|denied|login|401|403|x509|tls' || true

```
ming@ubuntu:~/secdevops-a3/portainer$ sudo docker logs portainer --since 30m 2>&
1 | \
> egrep -i 'fail|error|unauth|forbidden|denied|login|401|403|x509|tls' || true
ming@ubuntu:~/secdevops-a3/portainer$
```

- “bind_address=:PORT” = the container is listening.
- Whether you can reach it from your host/browser depends on published ports (see sudo docker compose ps or sudo docker ps).
- In your case, you published 9000 → browse to http://192.168.147.136:9000. If you also publish 9443 in compose.yaml, you can use https://192.168.147.136:9443 (preferred).

Task 3: Setup a NextCloud stack with PostgreSQL

3.1 Inspect compose.yaml and explain expose:

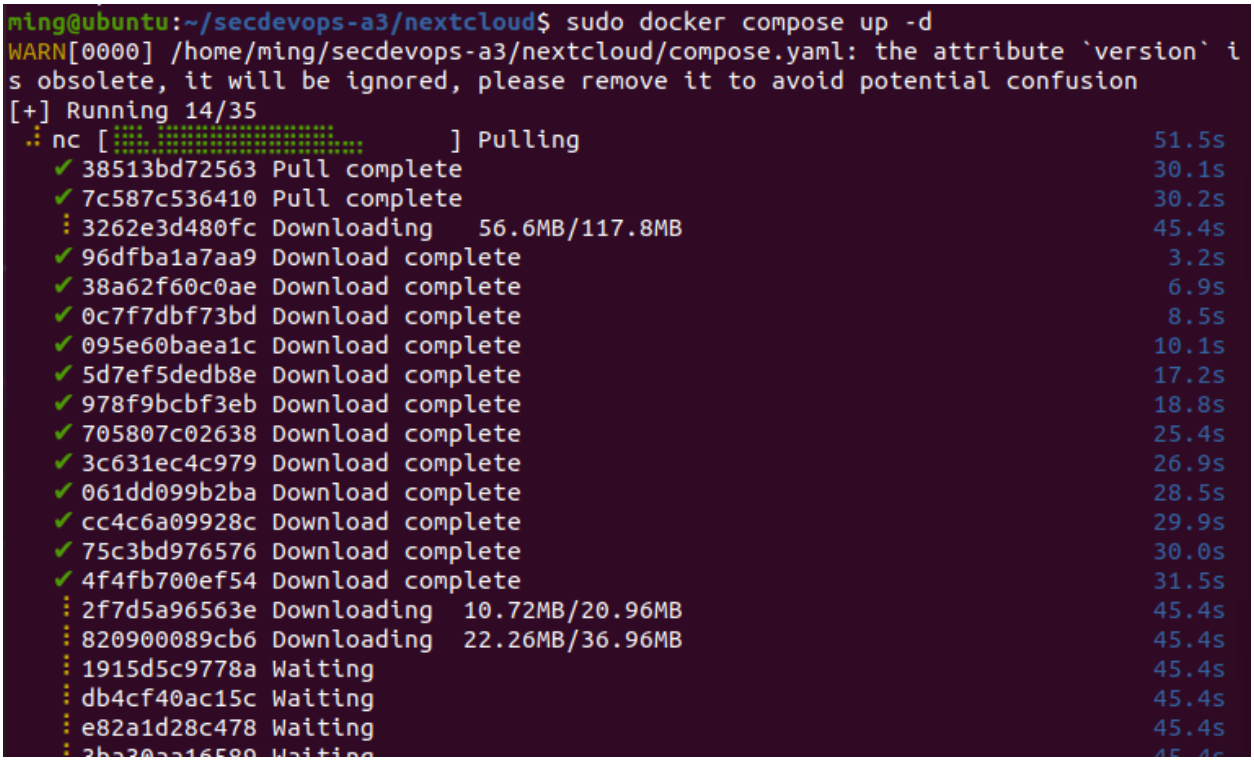
cd ~/secdevops-a3/nextcloud

sed -n '1,200p' compose.yaml

awk '/^[[:space:]]*expose:/, /^[[:space:]]*[^-]/ {print}' compose.yaml

```
ming@ubuntu:~/secdevops-a3/nextcloud$ sed -n '1,200p' compose.yaml
version: "3.9"
services:
  nc:
    image: nextcloud:apache
    environment:
      - POSTGRES_HOST=db
      - POSTGRES_PASSWORD=nextcloud
      - POSTGRES_DB=nextcloud
      - POSTGRES_USER=nextcloud
    ports:
      - 80:80
    depends_on:
      - db
    restart: always
    volumes:
      - nc_data:/var/www/html
  db:
    image: postgres:alpine
    environment:
      - POSTGRES_PASSWORD=nextcloud
      - POSTGRES_DB=nextcloud
      - POSTGRES_USER=nextcloud
    restart: always
    volumes:
      - db_data:/var/lib/postgresql/data
    expose:
      - 5432
volumes:
  db_data:
  nc_data:
ming@ubuntu:~/secdevops-a3/nextcloud$ awk '/^[[:space:]]*expose:/, /^[[:space:]]*[^-
 ]/ {print}' compose.yaml
    expose:
ming@ubuntu:~/secdevops-a3/nextcloud$
```

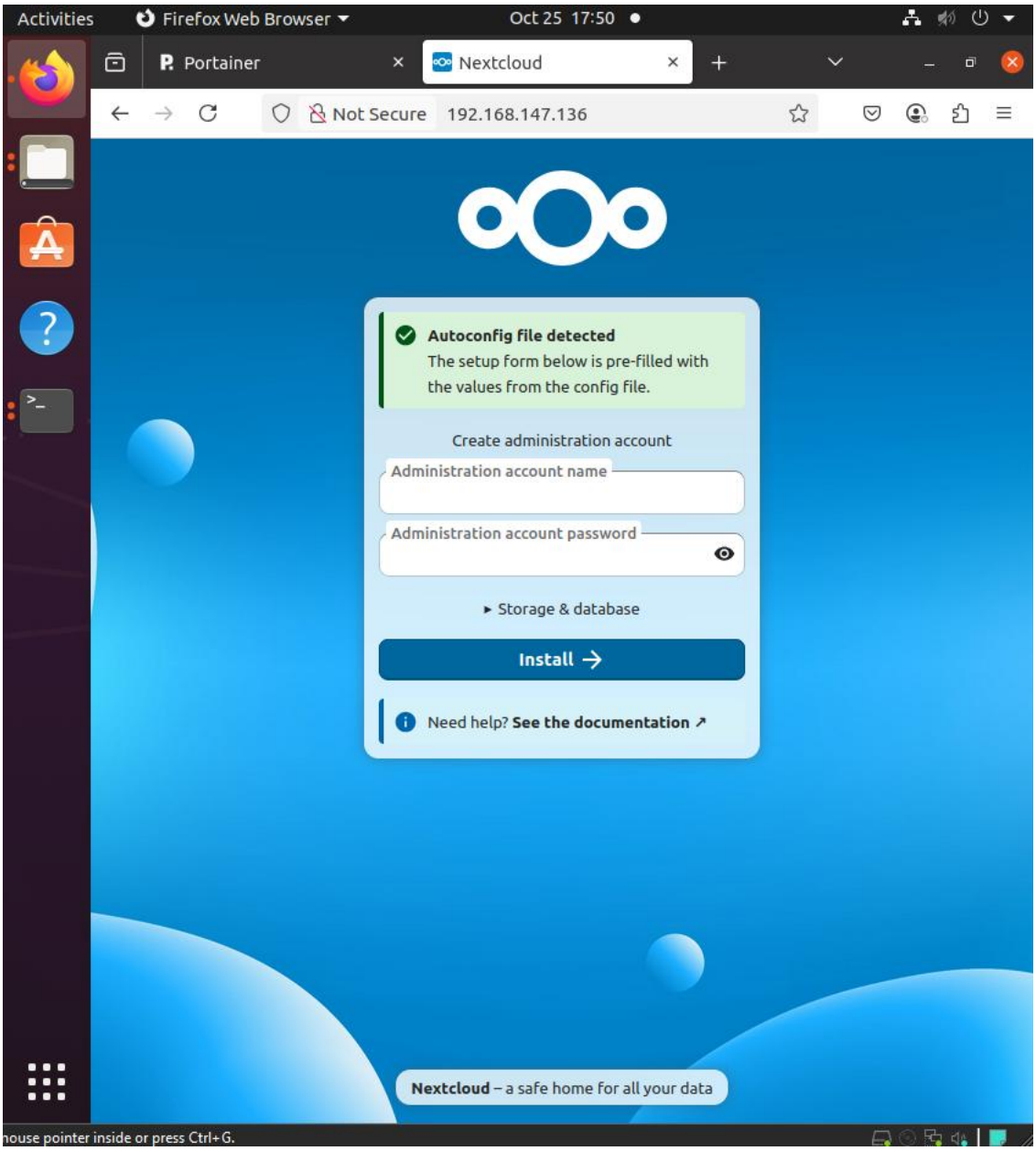
3.2 Deploy the Nextcloud + PostgreSQL stack



```
ming@ubuntu:~/secdevops-a3/nextcloud$ sudo docker compose pull
WARN[0000] /home/ming/secdevops-a3/nextcloud/compose.yaml: the attribute `version` i
s obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Pulling 25/25
 ✔ nc Pulled                                                              185.4s
   ✔ 38513bd72563 Pull complete                                            26.7s
   ✔ 7c587c536410 Pull complete                                            26.7s
   ✔ 3262e3d480fc Pull complete                                            99.0s
   ✔ 96dfba1a7aa9 Pull complete                                            99.0s
   ✔ 38a62f60c0ae Pull complete                                            99.4s
   ✔ 0c7f7dbf73bd Pull complete                                            99.5s
   ✔ 095e60baea1c Pull complete                                            99.5s
   ✔ 5d7ef5dedb8e Pull complete                                            99.6s
   ✔ 978f9bcbf3eb Pull complete                                            99.6s
   ✔ 705807c02638 Pull complete                                           100.2s
   ✔ 3c631ec4c979 Pull complete                                           100.2s
   ✔ 061dd099b2ba Pull complete                                           100.2s
   ✔ cc4c6a09928c Pull complete                                           100.3s
   ✔ 75c3bd976576 Pull complete                                           100.3s
   ✔ 4f4fb700ef54 Pull complete                                           100.3s
   ✔ 2f7d5a96563e Pull complete                                           101.1s
   ✔ 820900089cb6 Pull complete                                           103.0s
   ✔ 1915d5c9778a Pull complete                                           103.0s
   ✔ db4cf40ac15c Pull complete                                           103.0s
   ✔ e82a1d28c478 Pull complete                                           103.0s
   ✔ 3ba30aa16589 Pull complete                                           180.1s
   ✔ a3c9de2a4636 Pull complete                                           180.1s
   ✔ 1051a3a2ebd1 Pull complete                                           180.1s
 ✔ db Pulled                                                               3.3s
ming@ubuntu:~/secdevops-a3/nextcloud$ sudo docker compose up -d
WARN[0000] /home/ming/secdevops-a3/nextcloud/compose.yaml: the attribute `version` i
s obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Running 5/5
 ✔ Network nextcloud_default    Created                                    0.1s
 ✔ Volume "nextcloud_nc_data"   Created                                    0.0s
 ✔ Volume "nextcloud_db_data"   Created                                    0.0s
 ✔ Container nextcloud-db-1     Started                                    1.2s
 ✔ Container nextcloud-nc-1     Started                                    0.4s
ming@ubuntu:~/secdevops-a3/nextcloud$
```

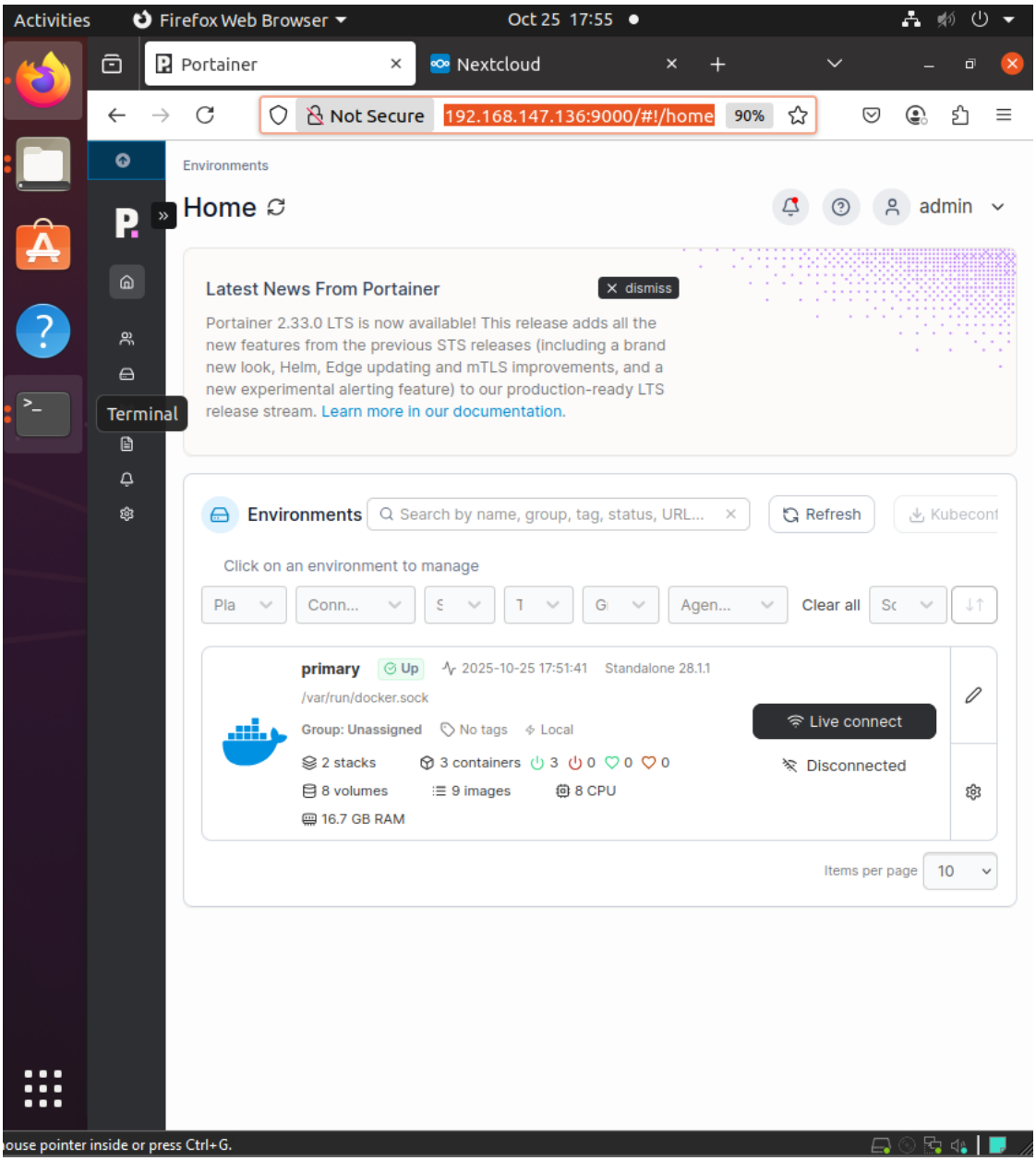
a. (i) Show the NextCloud web interface using your web browser, (ii) Report the fetched URL. Attach the related screen in the report.

http://192.168.147.136:80/



b. (i) Show the Portainer web interface using web browser after login to the portainer (refer Task 2). Attach the related screen in the report. (ii) Report the fetched URL. Attach the related screen in the report.

http://192.168.147.136:9000/#!/home



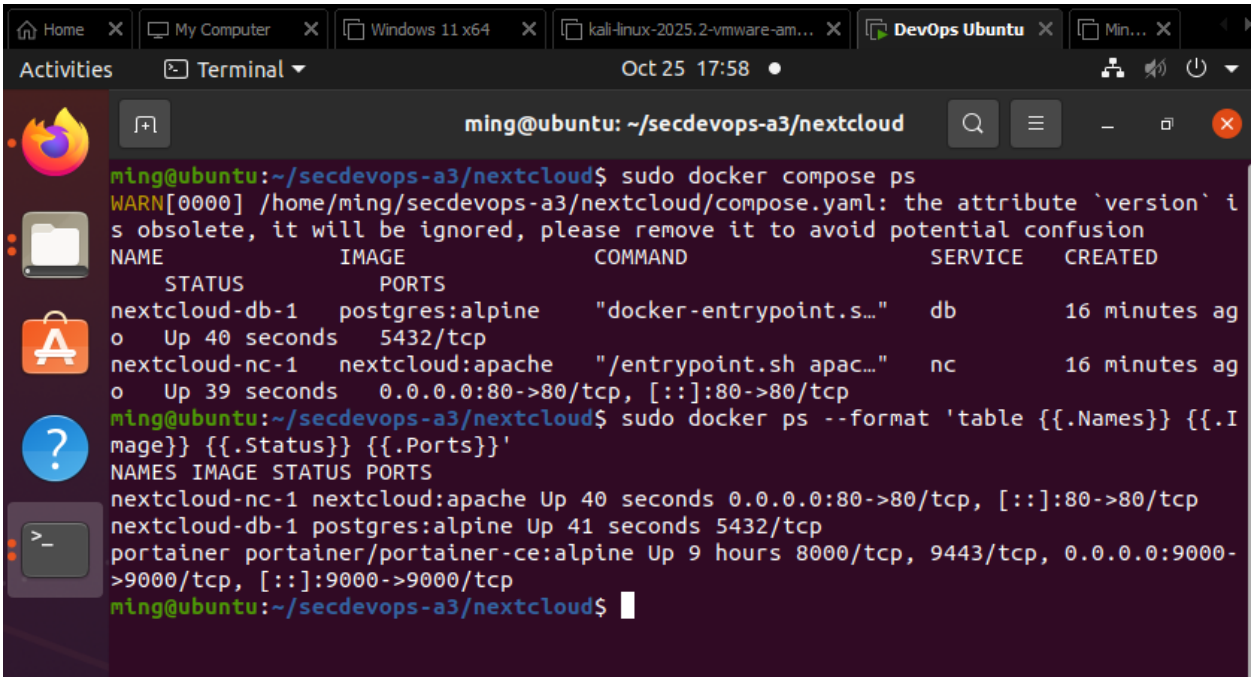
3.3 CLI management

a) sudo docker compose stop
sudo docker compose start
sudo docker compose restart

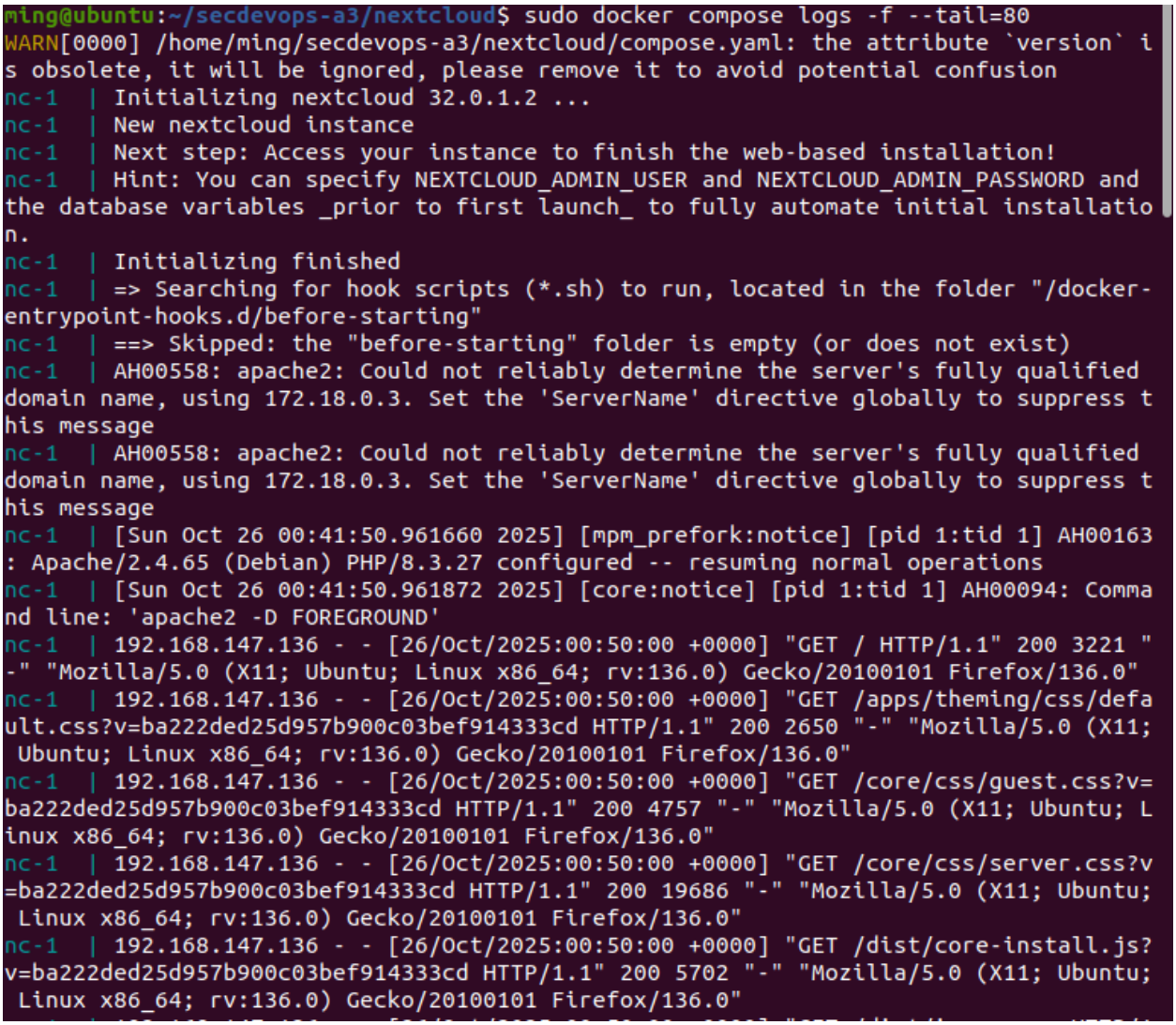
```
ming@ubuntu:~/secdevops-a3/nextcloud$ sudo docker compose stop
WARN[0000] /home/ming/secdevops-a3/nextcloud/compose.yaml: the attribute `version` i
s obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Stopping 2/2
 ✔ Container nextcloud-nc-1  Stopped                                          1.2s
 ✔ Container nextcloud-db-1  Stopped                                          0.2s
ming@ubuntu:~/secdevops-a3/nextcloud$ sudo docker compose start
WARN[0000] /home/ming/secdevops-a3/nextcloud/compose.yaml: the attribute `version` i
s obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Running 2/2
 ✔ Container nextcloud-db-1  Started                                          0.2s
 ✔ Container nextcloud-nc-1  Started                                          0.2s
ming@ubuntu:~/secdevops-a3/nextcloud$ sudo docker compose restart
WARN[0000] /home/ming/secdevops-a3/nextcloud/compose.yaml: the attribute `version` i
s obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Restarting 2/2
 ✔ Container nextcloud-nc-1  Started                                          1.4s
 ✔ Container nextcloud-db-1  Started                                          0.3s
ming@ubuntu:~/secdevops-a3/nextcloud$
```

b) sudo docker compose ps

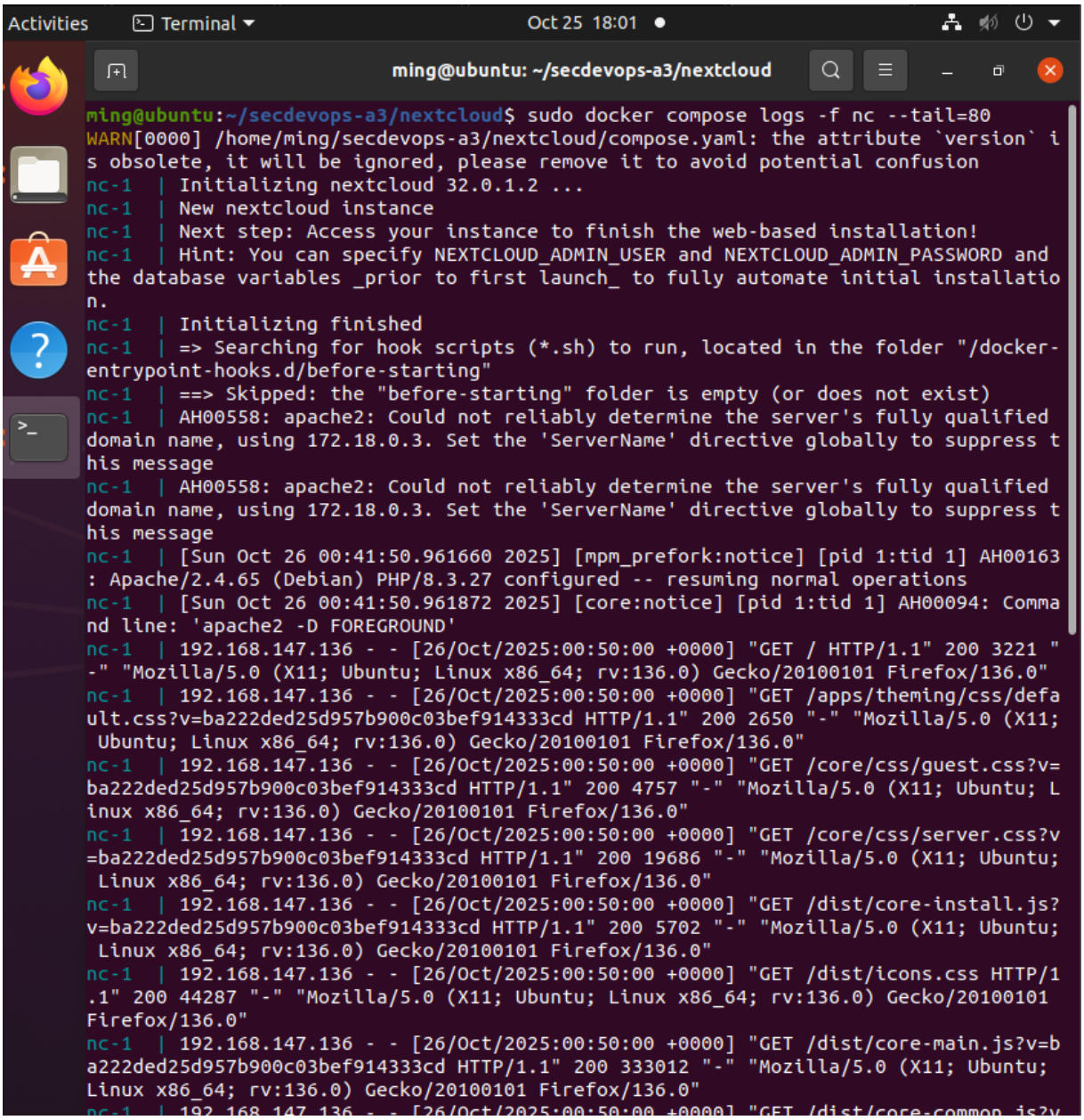
sudo docker ps --format 'table {{.Names}} {{.Image}} {{.Status}} {{.Ports}}'



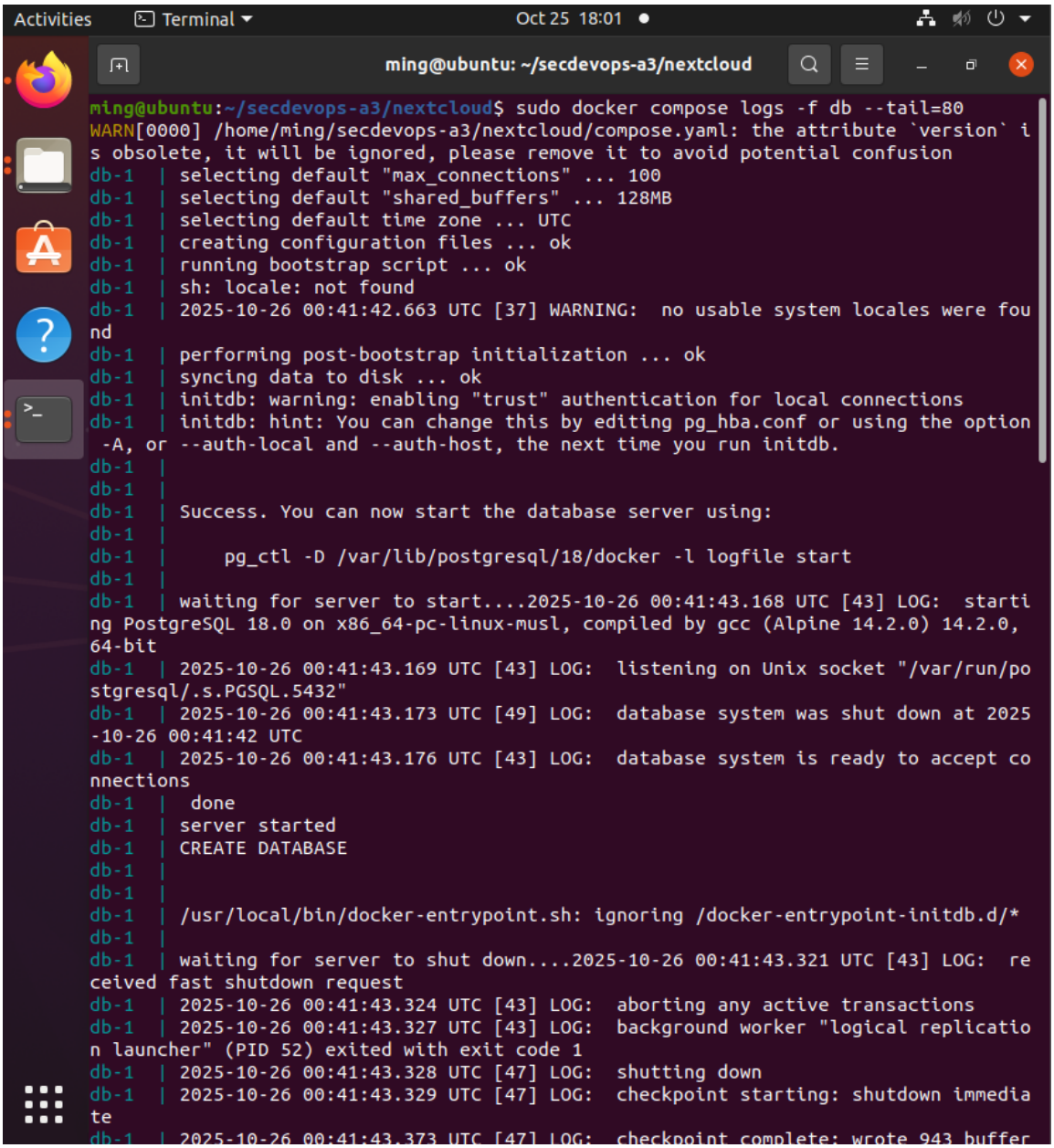
c) sudo docker compose logs -f --tail=80



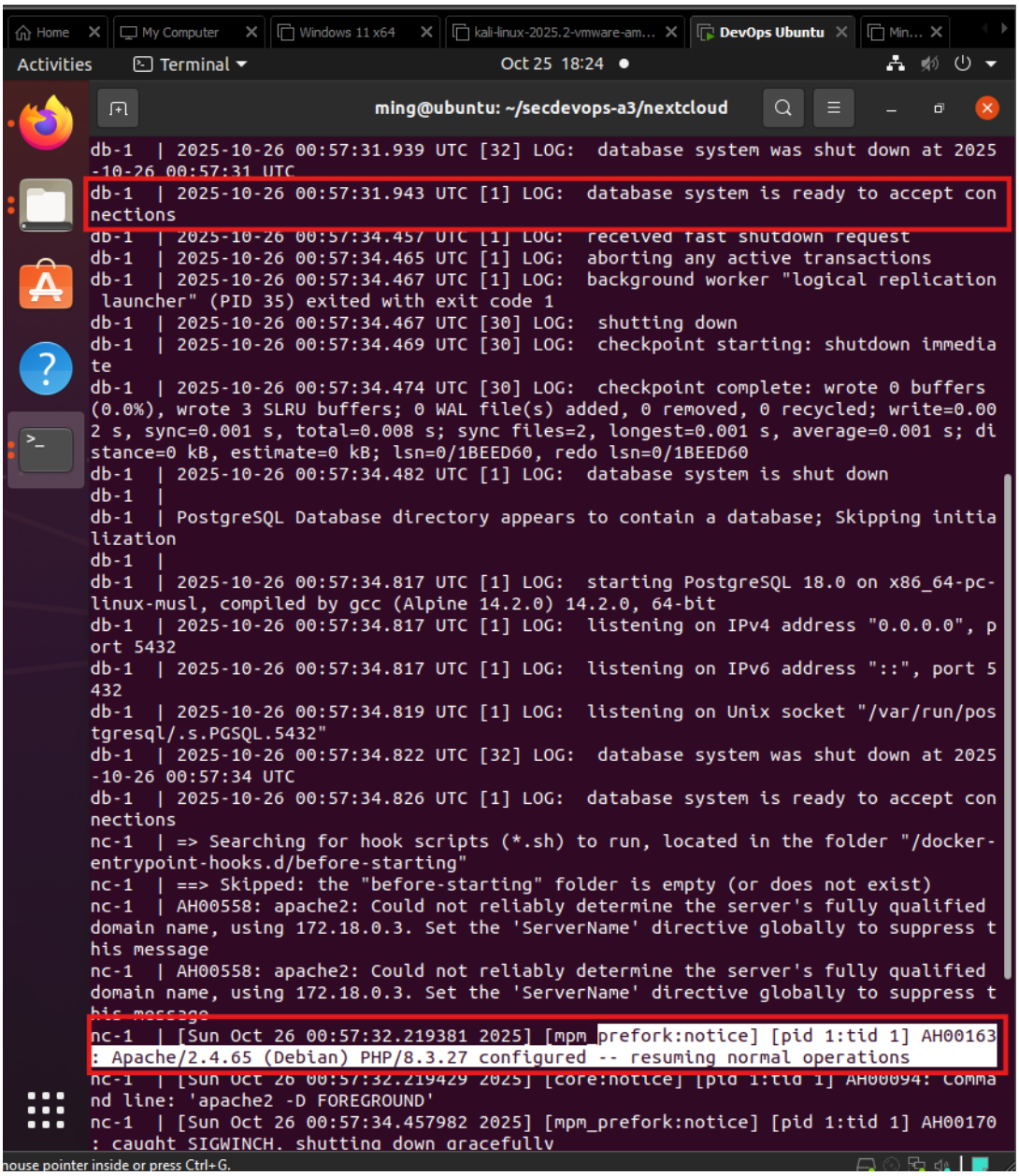
sudo docker compose logs -f nc --tail=80



sudo docker compose logs -f db --tail=80



d) sudo docker compose logs --since 5m | sed -n '1,120p'



DB became ready first; Nextcloud/Apache started after.

e) sudo docker ps -f "label=com.docker.compose.project=nextcloud" \

--format 'table {{.Names}}\t{{.Image}}\t{{.ID}}\t{{.Status}}\t{{.Ports}}'

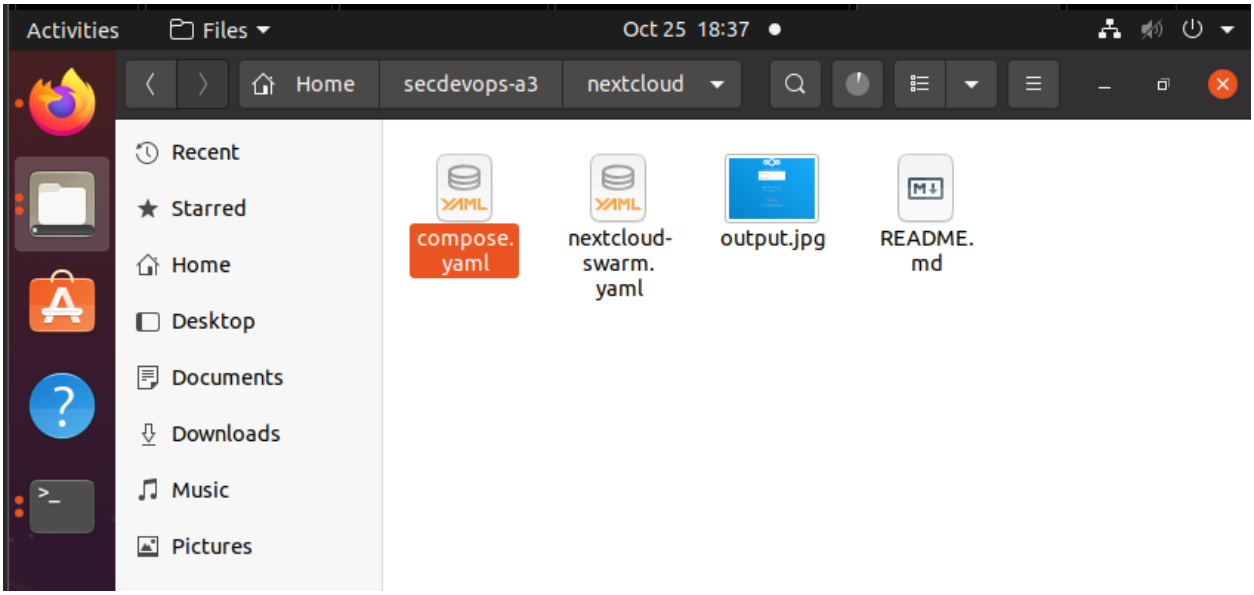
```
ming@ubuntu:~/secdevops-a3/nextcloud$ sudo docker ps -f "label=com.docker.compose.pr
oject=nextcloud" \
>   --format 'table {{.Names}}\t{{.Image}}\t{{.ID}}\t{{.Status}}\t{{.Ports}}'
NAMES             IMAGE                COMPOSE ID    STATUS          PORTS
nextcloud-nc-1    nextcloud:apache     003bbc2f871a    Up 29 minutes    0.0.0.0:80->80/tc
p, [::]:80->80/tcp
nextcloud-db-1    postgres:alpine      82920936abd5    Up 29 minutes    5432/tcp
```

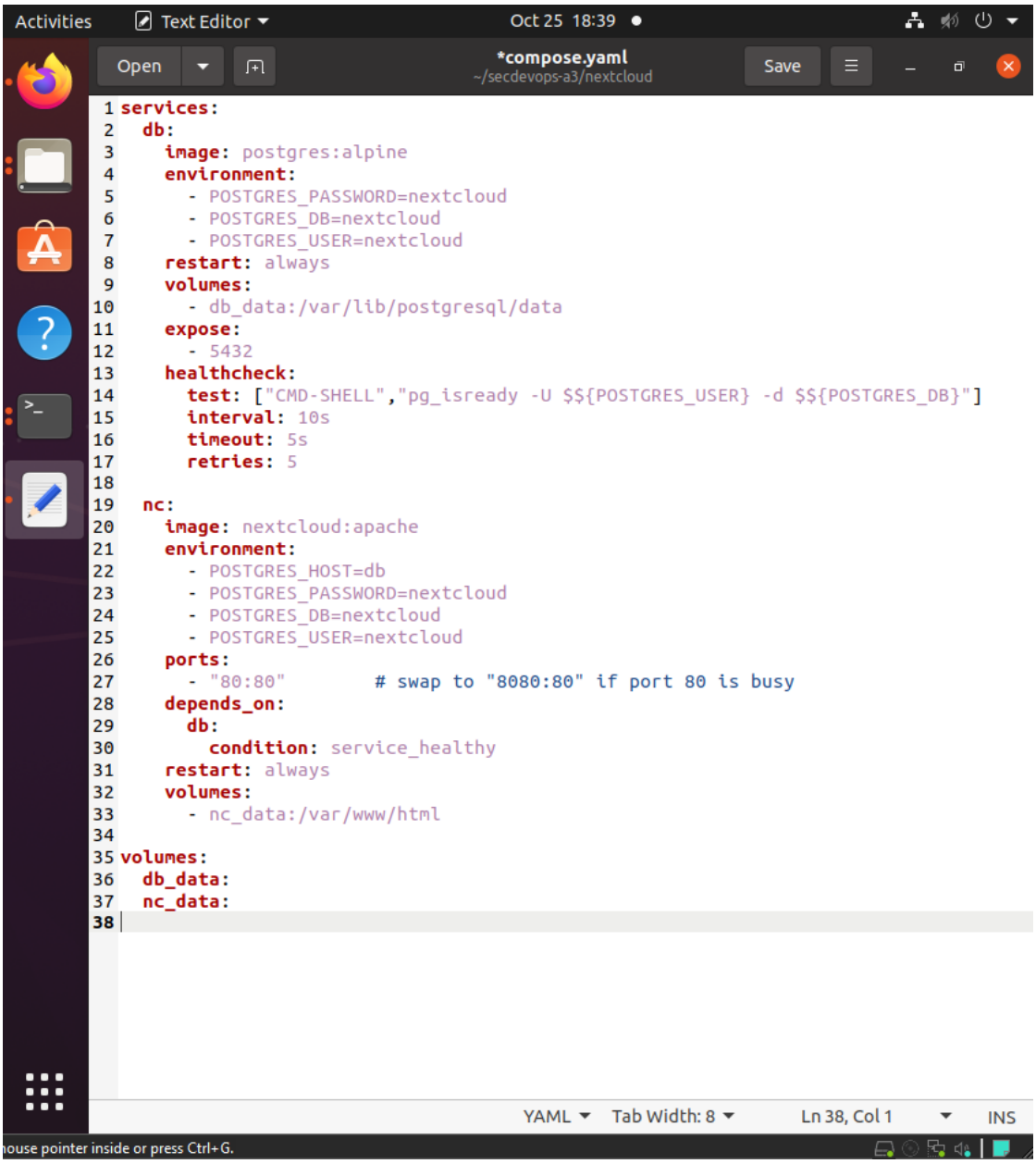
3.4 Ensure DB starts before Nextcloud

Edit file: ~/secdevops-a3/nextcloud/compose.yaml

Make db report healthy before nc starts.

Removes the obsolete `version:` key, adds DB `healthcheck`, and switches `depends_on` to `condition: service_healthy`.





sudo docker compose config # quick syntax check
sudo docker compose up -d
sudo docker compose ps
sudo docker compose logs --since 2m | egrep -i 'ready|health|starting|postgres|apache' || true

```
ming@ubuntu:~/secdevops-a3/nextcloud$ sudo docker compose up -d
[+] Running 2/2
 ✔ Container nextcloud-db-1  Healthy                                    10.9s
 ✔ Container nextcloud-nc-1  Running                                     0.0s
ming@ubuntu:~/secdevops-a3/nextcloud$ sudo docker compose ps
NAME             IMAGE              COMMAND                  SERVICE   CREATED
    STATUS                    PORTS
nextcloud-db-1   postgres:alpine    "docker-entrypoint.s…"   db        11 seconds ag
o   Up 10 seconds (healthy)   5432/tcp
nextcloud-nc-1   nextcloud:apache   "/entrypoint.sh apac…"   nc        58 minutes ag
o   Up 42 minutes             0.0.0.0:80->80/tcp, [::]:80->80/tcp
ming@ubuntu:~/secdevops-a3/nextcloud$ sudo docker compose logs --since 2m | egrep -i
 'ready|health|starting|postgres|apache' || true
db-1  | PostgreSQL Database directory appears to contain a database; Skipping initia
lization
db-1  | 2025-10-26 01:39:49.744 UTC [1] LOG:  starting PostgreSQL 18.0 on x86_64-pc-
linux-musl, compiled by gcc (Alpine 14.2.0) 14.2.0, 64-bit
db-1  | 2025-10-26 01:39:49.745 UTC [1] LOG:  listening on Unix socket "/var/run/pos
tgresql/.s.PGSQL.5432"
db-1  | 2025-10-26 01:39:49.752 UTC [1] LOG:  database system is ready to accept con
nections
ming@ubuntu:~/secdevops-a3/nextcloud$
```

Task 4: Container Security Scanning with Clair

4.1 Install PostgreSQL + Clair via Docker Compose

a. Get Clair source at a real release and build a local image

git clone --depth=1 --branch v4.8.0 https://github.com/quay/clair clair-src

cd clair-src

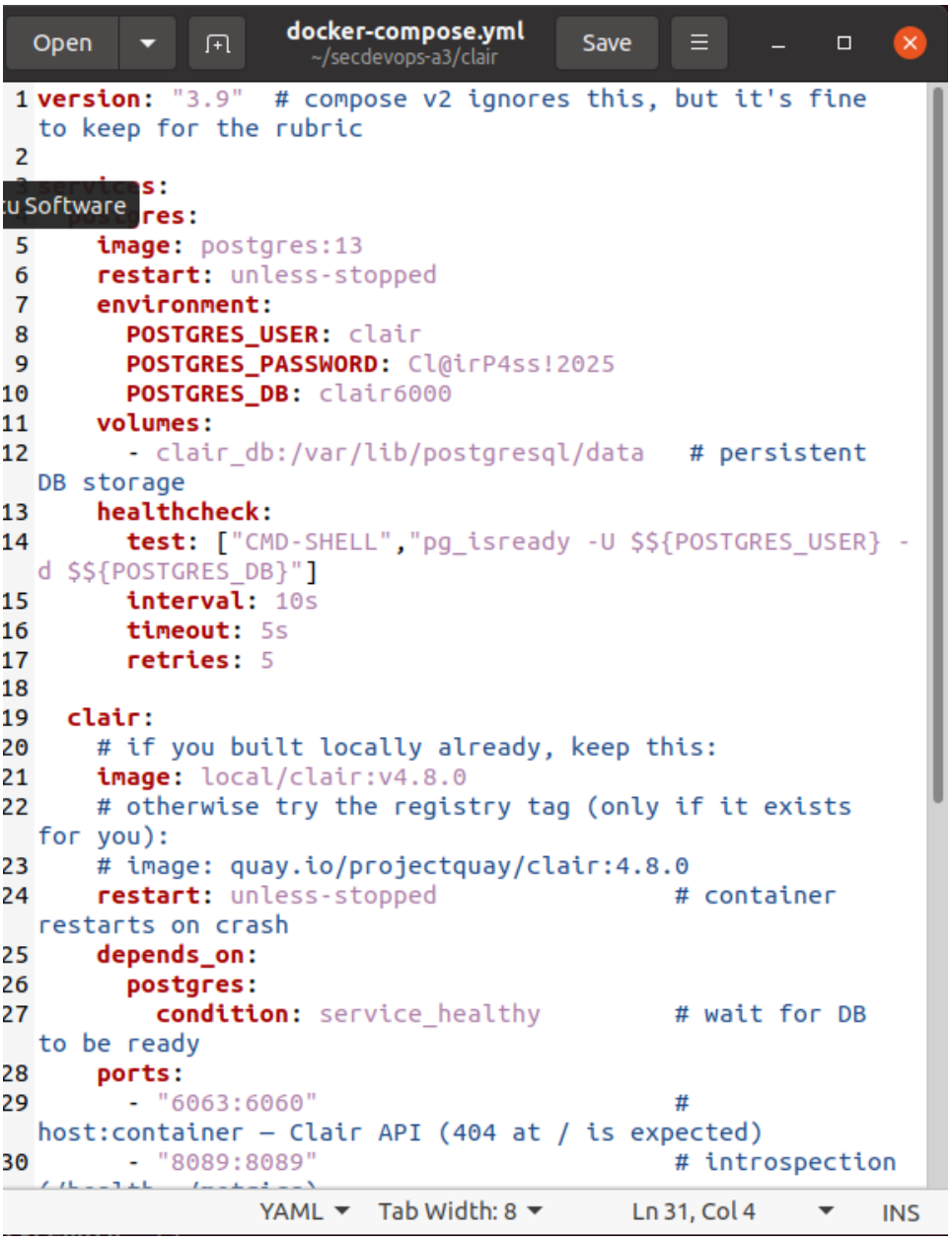
sudo docker build -t local/clair:v4.8.0 .

cd ..

```
ming@ubuntu:~/secdevops-a3/clair$ cd clair-src
ming@ubuntu:~/secdevops-a3/clair/clair-src$ sudo docker build -t local/clair:v4.8.0
.
[+] Building 270.0s (15/15) FINISHED                                docker:default
 => [internal] load build definition from Dockerfile                          0.0s
 => => transferring dockerfile: 2.44kB                                        0.0s
 => resolve image config for docker-image://docker.io/docker/dockerfile:1.7   4.1s
 => docker-image://docker.io/docker/dockerfile:1.7@sha256:a57df69d0ea827fb726  6.2s
 => => resolve docker.io/docker/dockerfile:1.7@sha256:a57df69d0ea827fb7266491  0.0s
 => => sha256:96918c57e42509b97f10c074d80672ecdbd3bb7dcd38c 11.98MB / 11.98MB  6.0s
 => => sha256:a57df69d0ea827fb7266491f2813635de6f17269be881f6 8.40kB / 8.40kB  0.0s
 => => sha256:b5f3b260a9678e1d83d2fce86eeddf79420b79147eaba2a2598 482B / 482B  0.0s
 => => sha256:68ebc061390d9a7d6e194f9d58309c754a53cb8b4e3b0d8 1.26kB / 1.26kB  0.0s
 => => extracting sha256:96918c57e42509b97f10c074d80672ecdbd3bb7dcd38c1bd9596  0.1s
 => [internal] load metadata for registry.access.redhat.com/ubi8/ubi-minimal:  2.6s
 => [internal] load metadata for quay.io/projectquay/golang:1.22               3.8s
 => [internal] load .dockerignore                                             0.0s
 => => transferring context: 261B                                             0.0s
 => [build 1/4] FROM quay.io/projectquay/golang:1.22@sha256:7e1adf584d1af60  130.3s
 => => resolve quay.io/projectquay/golang:1.22@sha256:7e1adf584d1af60e607f212  0.0s
 => => sha256:9dbb4ca640f33810dca91c39a5d916c2db1248f79a666 10.32kB / 10.32kB  0.0s
 => => sha256:0840e693392a1639fa286f1c359585db91184e5c08d2 78.95MB / 78.95MB  73.5s
 => => sha256:db949d251283515b4db8781a18c35c348c504d06d 182.10MB / 182.10MB  118.4s
 => => sha256:7e1adf584d1af60e607f212a4a4cfbe817366419a02115bae67 955B / 955B  0.0s
 => => sha256:3aa5d9f5ee1396eaba377555895cd5c1a67e5f8454b71464475 596B / 596B  0.0s
 => => extracting sha256:0840e693392a1639fa286f1c359585db91184e5c08d2ed32f710  5.2s
 => => extracting sha256:db949d251283515b4db8781a18c35c348c504d06d7dc143a2d6  11.6s
```

b&c) Compose file (uses local image + Postgres 13)

```
version: "3.9"

services: postgres: image: postgres:13 restart: unless-stopped environment: POSTGRES_USER: clair POSTGRES_PASSWORD: Cl@irP4ss!2025 POSTGRES_DB: clair6000 volumes: - clair_db:/var/lib/postgresql/data # persistent DB storage healthcheck: test: ["CMD-SHELL","pg_isready -U $${POSTGRES_USER} -d $${POSTGRES_DB}"] interval: 10s timeout: 5s retries: 5

clair: # if you built locally already, keep this: image: local/clair:v4.8.0 # otherwise try the registry tag (only if it exists for you): # image: quay.io/projectquay/clair:4.8.0 restart: unless-stopped # container restarts on crash depends_on: postgres: condition: service_healthy # wait for DB to be ready ports: - "6063:6060" # host:container — Clair API (404 at / is expected) - "8089:8089" # introspection (/health, /metrics) environment: - CLAIR_DATABASE=postgres://clair:Cl@irP4ss!2025@postgres:5432/clair6000?sslmode=disable - CLAIR_UPDATER_ENABLED=true - CLAIR_NOTIFIERS_ENABLED=false # set true only if you wire a notifier service - CLAIR_NOTIFIERS_ENDPOINT=http://clair-notifier:6061/notify - CLAIR_API_MAXCONN=1024 # Clair v4 requires a config file. We mount a minimal working one and point Clair to it: volumes: - ./config.yaml:/etc/clair/config.yaml:ro command: ["-conf","/etc/clair/config.yaml","-mode","combo"]

volumes: clair_db:
```



Minimal Clair config (single DB named clair6000)

cat > config.yaml <<EOF
http_listen_addr: :6060

```
log_level: info
indexer:
connstring: host=clair-db port=5432 user=clair password=${CLAIR_DB_PASS}
dbname=clair6000 sslmode=disable
migrations: true
matcher:
connstring: host=clair-db port=5432 user=clair password=${CLAIR_DB_PASS}
dbname=clair6000 sslmode=disable
migrations: true
indexer_addr: http://clair:6060
notifier:
connstring: host=clair-db port=5432 user=clair password=${CLAIR_DB_PASS}
dbname=clair6000 sslmode=disable
migrations: true
EOF
# start services
sudo docker compose up -d
sudo docker compose ps
# verify DB exists (psql defaults to -d <user>; explicitly connect to postgres or clair6000)
sudo docker compose exec -T clair-db psql -U clair -d postgres -c '\l' # shows clair6000
sudo docker compose exec -T clair-db psql -U clair -d clair6000 -c 'SELECT 1;'
```

```
ming@ubuntu:~/secdevops-a3/clair$ export CLAIR_DB_PASS='Cl@irP4ss!2025'   # pick you
r own strong pass
ming@ubuntu:~/secdevops-a3/clair$ echo "CLAIR_DB_PASS=$CLAIR_DB_PASS" > .env
ming@ubuntu:~/secdevops-a3/clair$ cat > config.yaml <<EOF
> http_listen_addr: :6060
> log_level: info
> indexer:
>   connstring: host=clair-db port=5432 user=clair password=${CLAIR_DB_PASS} dbname=
clair6000 sslmode=disable
> matcher:
>   connstring: host=clair-db port=5432 user=clair password=${CLAIR_DB_PASS} dbname=
clair6000 sslmode=disable
>   indexer_addr: http://clair:6060
> notifier:
>   connstring: host=clair-db port=5432 user=clair password=${CLAIR_DB_PASS} dbname=
clair6000 sslmode=disable
> EOF
ming@ubuntu:~/secdevops-a3/clair$
ming@ubuntu:~/secdevops-a3/clair$ # 4) Bring it up + verify
ming@ubuntu:~/secdevops-a3/clair$ sudo docker compose up -d
[+] Running 15/15
 ✔ clair-db Pulled                                                        1237.1s
   ✔ 38513bd72563 Already exists                                             0.0s
   ✔ c309a3f2c49e Pull complete                                              1.5s
   ✔ 791d044c481d Pull complete                                              8.4s
   ✔ fd42d1702722 Pull complete                                              8.4s
   ✔ 0a7a21b1445a Pull complete                                              8.9s
   ✔ 7ce064935b1d Pull complete                                              9.0s
   ✔ f70fc6fcc299 Pull complete                                              9.0s
   ✔ 6dd4a54b1ffc Pull complete                                              9.2s
   ✔ da4dca14e77b Pull complete                                           1233.7s
   ✔ f7b65550c417 Pull complete                                           1233.7s
   ✔ 332b803ad560 Pull complete                                           1233.7s
   ✔ 4fc9573f19ca Pull complete                                           1233.7s
   ✔ a04efa95ee02 Pull complete                                           1233.7s
   ✔ 18feef15783f Pull complete                                           1233.7s
[+] Running 4/4
 ✔ Network clair_default       Created                                       0.1s
 ✔ Volume "clair_clair_db"     Created                                       0.0s
 ✔ Container clair-clair-db-1  Healthy                                      11.1s
 ✔ Container clair-clair-1     Started                                      10.9s
ming@ubuntu:~/secdevops-a3/clair$ sudo docker compose ps
```

```
ming@ubuntu:~/secdevops-a3/clair$ sudo docker compose exec -T clair-db psql -U clair
 -d clair6000 -c '\dt'
               List of relations
 Schema |           Name            | Type  | Owner
--------+---------------------------+-------+-------
 public | dist                      | table | clair
 public | dist_scanartifact         | table | clair
 public | enrichment                | table | clair
 public | file                      | table | clair
 public | file_scanartifact         | table | clair
 public | indexreport               | table | clair
 public | key                       | table | clair
 public | layer                     | table | clair
 public | libindex_migrations       | table | clair
 public | libvuln_migrations        | table | clair
 public | manifest                  | table | clair
 public | manifest_index            | table | clair
 public | manifest_layer            | table | clair
 public | notification              | table | clair
 public | notification_body         | table | clair
 public | notifier_migrations       | table | clair
 public | notifier_update_operation | table | clair
 public | package                   | table | clair
 public | package_scanartifact      | table | clair
 public | receipt                   | table | clair
 public | repo                      | table | clair
 public | repo_scanartifact         | table | clair
 public | scanned_layer             | table | clair
 public | scanned_manifest          | table | clair
 public | scanner                   | table | clair
 public | scannerlist               | table | clair
 public | uo_enrich                 | table | clair
 public | uo_vuln                   | table | clair
 public | update_operation          | table | clair
 public | updater_status            | table | clair
 public | vuln                      | table | clair
(31 rows)
```

d. Start Clair service

sudo docker compose ps

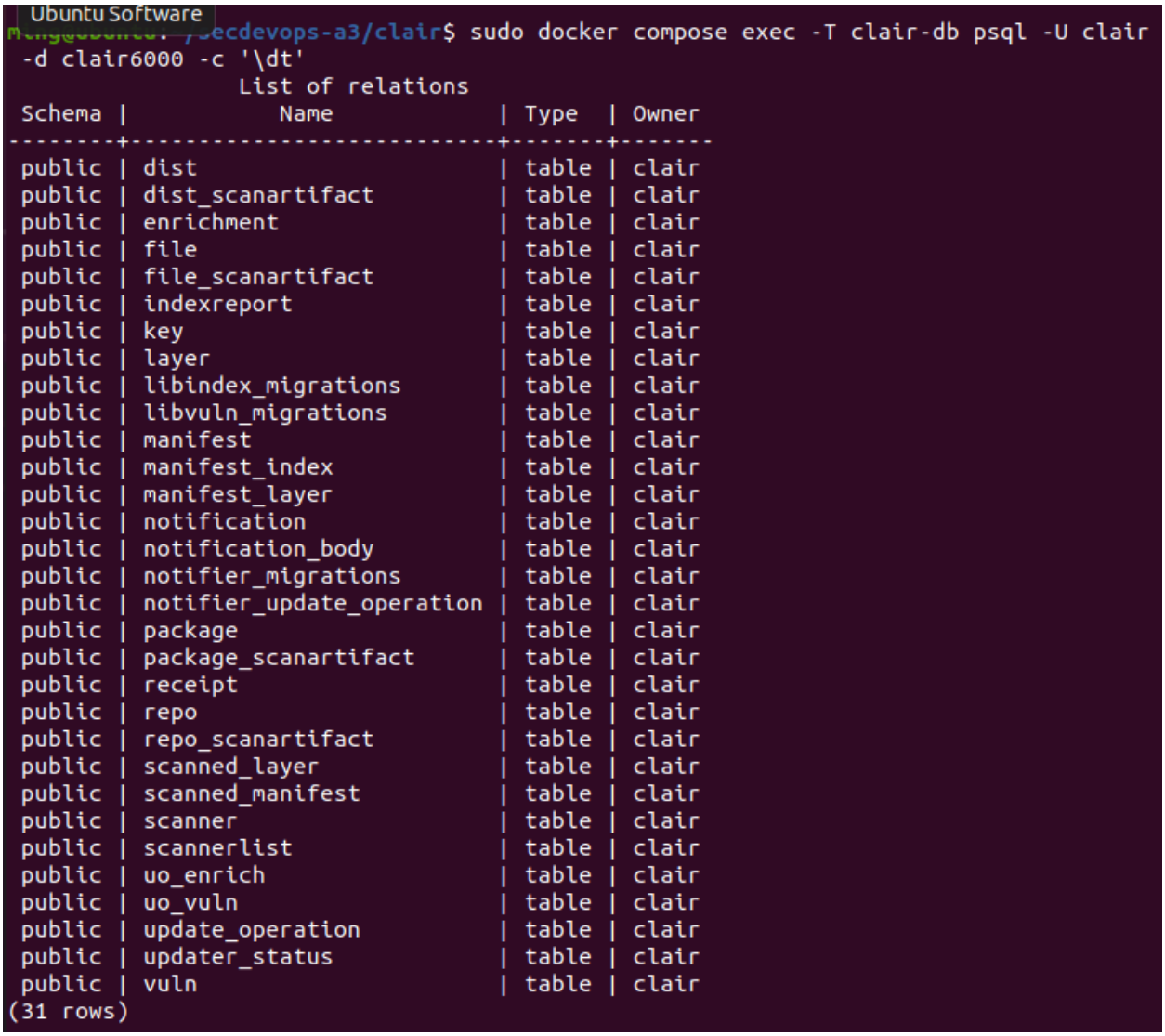
```
ming@ubuntu:~/secdevops-a3/clair$ sudo docker compose ps
NAME               IMAGE                COMMAND                  SERVICE    CREATED
       STATUS                   PORTS
clair-clair-1      local/clair:v4.8.0   "/usr/bin/clair -con…"   clair      5 minute
s ago   Up 4 minutes             0.0.0.0:6063->6060/tcp, [::]:6063->6060/tcp, 0.0.0.
0:6064->6061/tcp, [::]:6064->6061/tcp
clair-clair-db-1   postgres:13          "docker-entrypoint.s…"   clair-db   5 minute
s ago   Up 5 minutes (healthy)   5432/tcp
```

sudo docker compose logs --tail=120 clair | egrep -i 'ready|initialize|serv|migrat'

```
ming@ubuntu:~/secdevops-a3/clair$ sudo docker compose restart clair
[+] Restarting 1/1
 ✔ Container clair-clair-1  Started                                    0.4s
ming@ubuntu:~/secdevops-a3/clair$ sleep 2
ming@ubuntu:~/secdevops-a3/clair$ curl -i http://127.0.0.1:8089/health
curl: (7) Failed to connect to 127.0.0.1 port 8089: Connection refused
ming@ubuntu:~/secdevops-a3/clair$ sudo docker compose logs --tail=120 clair | egrep
-i 'ready|initialize|serv|migrat'
clair-1  | {"level":"info","component":"libvuln/updates/Manager.driveUpdater","updat
er":"suse-updater-suse.linux.enterprise.server.15","time":"2025-10-26T09:14:13Z","me
ssage":"starting update"}
clair-1  | {"level":"info","updater":"suse-updater-suse.linux.enterprise.server.15",
"component":"pkg/ovalutil/Fetcher.Fetch","database":"https://support.novell.com/secu
rity/oval/suse.linux.enterprise.server.15.xml","time":"2025-10-26T09:14:13Z","messag
e":"starting fetch"}
clair-1  | {"level":"info","component":"libvuln/updates/Manager.driveUpdater","updat
er":"suse-updater-suse.linux.enterprise.server.12","time":"2025-10-26T09:14:23Z","me
ssage":"starting update"}
clair-1  | {"level":"info","updater":"suse-updater-suse.linux.enterprise.server.12",
"component":"pkg/ovalutil/Fetcher.Fetch","database":"https://support.novell.com/secu
rity/oval/suse.linux.enterprise.server.12.xml","time":"2025-10-26T09:14:23Z","messag
e":"starting fetch"}
clair-1  | {"level":"info","updater":"suse-updater-suse.linux.enterprise.server.11",
"component":"libvuln/updates/Manager.driveUpdater","time":"2025-10-26T09:15:18Z","me
ssage":"starting update"}
clair-1  | {"level":"info","updater":"suse-updater-suse.linux.enterprise.server.11",
"component":"pkg/ovalutil/Fetcher.Fetch","database":"https://support.novell.com/secu
rity/oval/suse.linux.enterprise.server.11.xml","time":"2025-10-26T09:15:18Z","messag
e":"starting fetch"}
```

sudo docker compose ps

sudo docker compose exec -T clair-db psql -U clair -d clair6000 -c '\dt' # shows migrated tables



e) To show that API is reachable

curl -i http://127.0.0.1:6063/

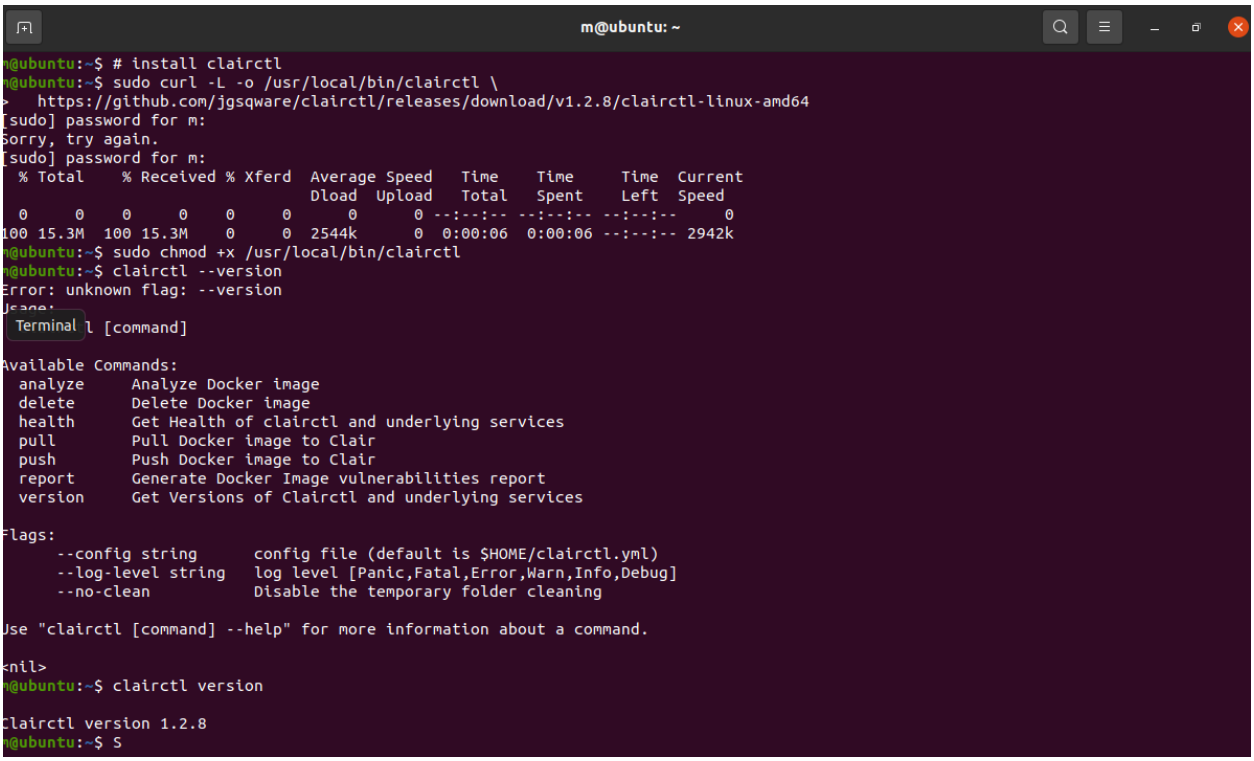
```
ming@ubuntu:~/secdevops-a3/clair$ curl -i http://127.0.0.1:6063/
HTTP/1.1 404 Not Found
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff
Date: Sun, 26 Oct 2025 09:19:41 GMT
Content-Length: 19
```

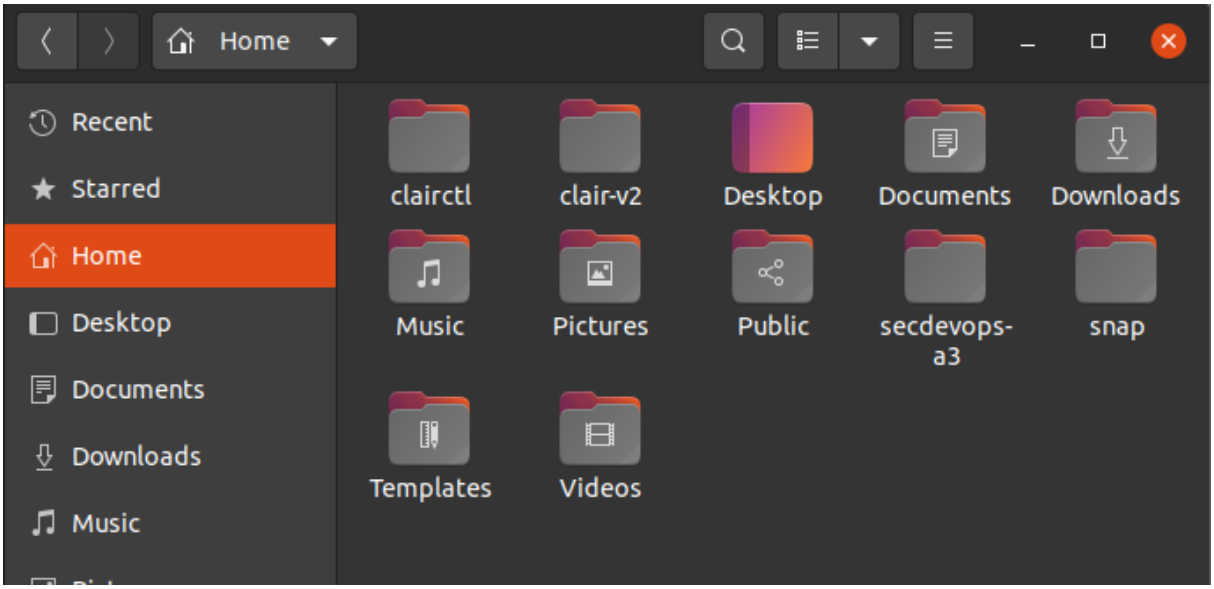
```
root@ubuntu:~/clair-v2# curl -i http://127.0.0.1:6063/          # expect HTTP/1.1 404 Not Found (GOOD)
HTTP/1.1 404 Not Found
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff
Date: Tue, 28 Oct 2025 06:33:33 GMT
Content-Length: 19

404 page not found
root@ubuntu:~/clair-v2# curl -i http://127.0.0.1:6064/metrics   # expect HTTP/1.1 200 OK (Prometheus)
HTTP/1.1 404 Not Found
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff
Date: Tue, 28 Oct 2025 06:33:33 GMT
Content-Length: 19

404 page not found
root@ubuntu:~/clair-v2#
```

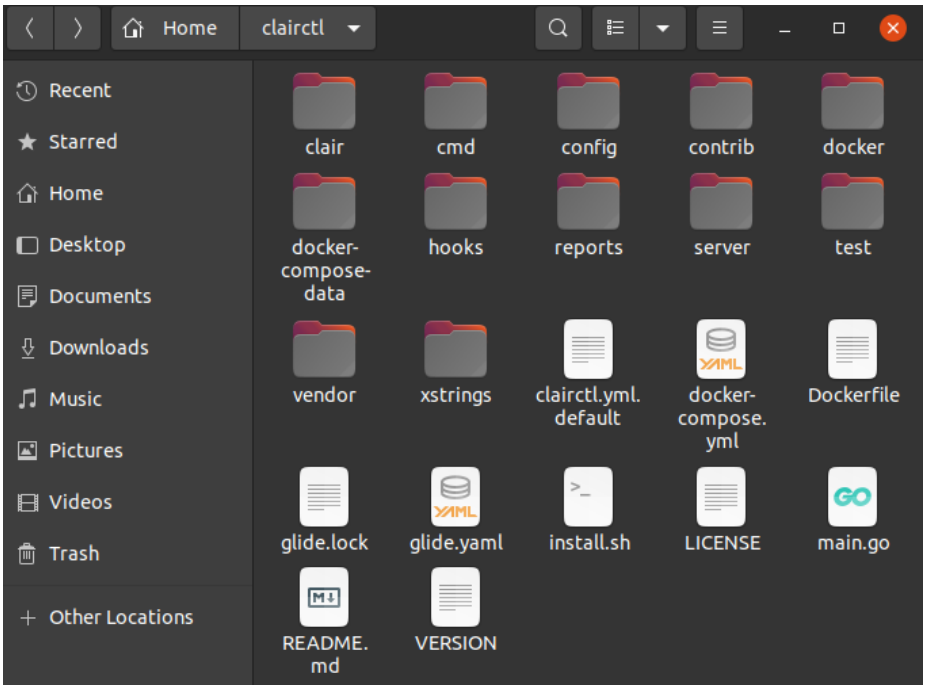
4.2 Perform Container Security Scanning

a. Installing clairctl

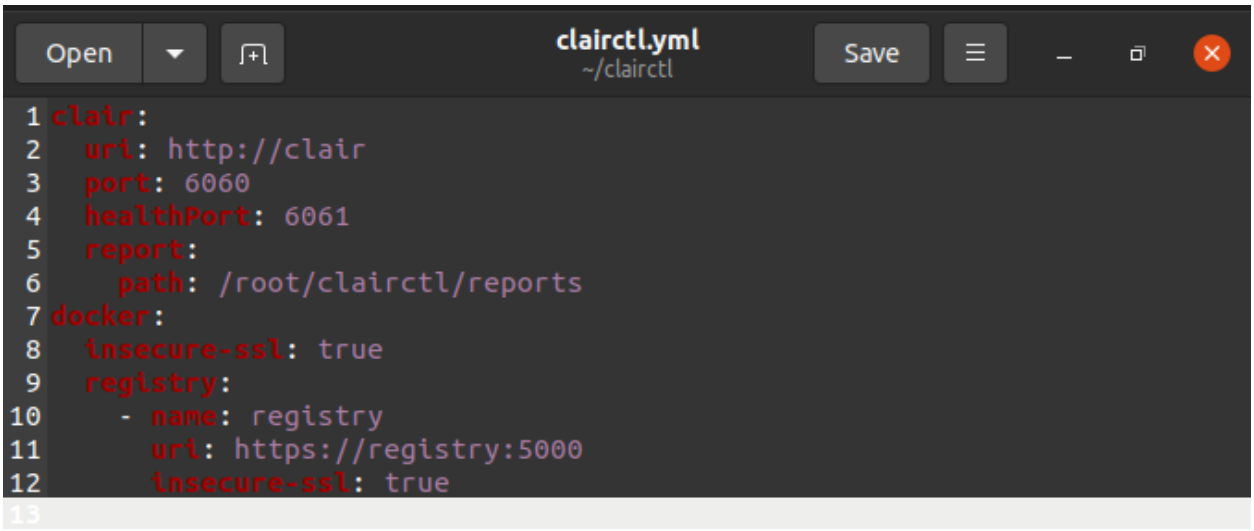
clone and install Clairctl
cd ~
git clone https://github.com/jgsqware/clairctl.git
cd clairctl
go build # or download from the GitHub release binary
verify installation
clairctl version


m@ubuntu: ~
m@ubuntu:~$ # install clairctl
m@ubuntu:~$ sudo curl -L -o /usr/local/bin/clairctl \
>   https://github.com/jgsqware/clairctl/releases/download/v1.2.8/clairctl-linux-amd64
[sudo] password for m:
Sorry, try again.
[sudo] password for m:
  % Total   % Received % Xferd Average Speed   Time   Time   Time Current
                                 Dload Upload   Total   Spent   Left Speed
  0   0   0   0   0   0   0   0 --:--:-- --:--:-- --:--:--   0
100 15.3M 100 15.3M   0   0 2544k   0 0:00:06 0:00:06 --:--:-- 2942k
m@ubuntu:~$ sudo chmod +x /usr/local/bin/clairctl
m@ubuntu:~$ clairctl --version
Error: unknown flag: --version
Usage:
Terminal l [command]
Available Commands:
analyze Analyze Docker image
delete Delete Docker image
health Get Health of clairctl and underlying services
pull Pull Docker image to Clair
push Push Docker image to Clair
report Generate Docker Image vulnerabilities report
version Get Versions of Clairctl and underlying services
Flags:
--config string config file (default is $HOME/clairctl.yml)
--log-level string log level [Panic,Fatal,Error,Warn,Info,Debug]
--no-clean Disable the temporary folder cleaning
Use "clairctl [command] --help" for more information about a command.
<nil>
m@ubuntu:~$ clairctl version
clairctl version 1.2.8
m@ubuntu:~$ S

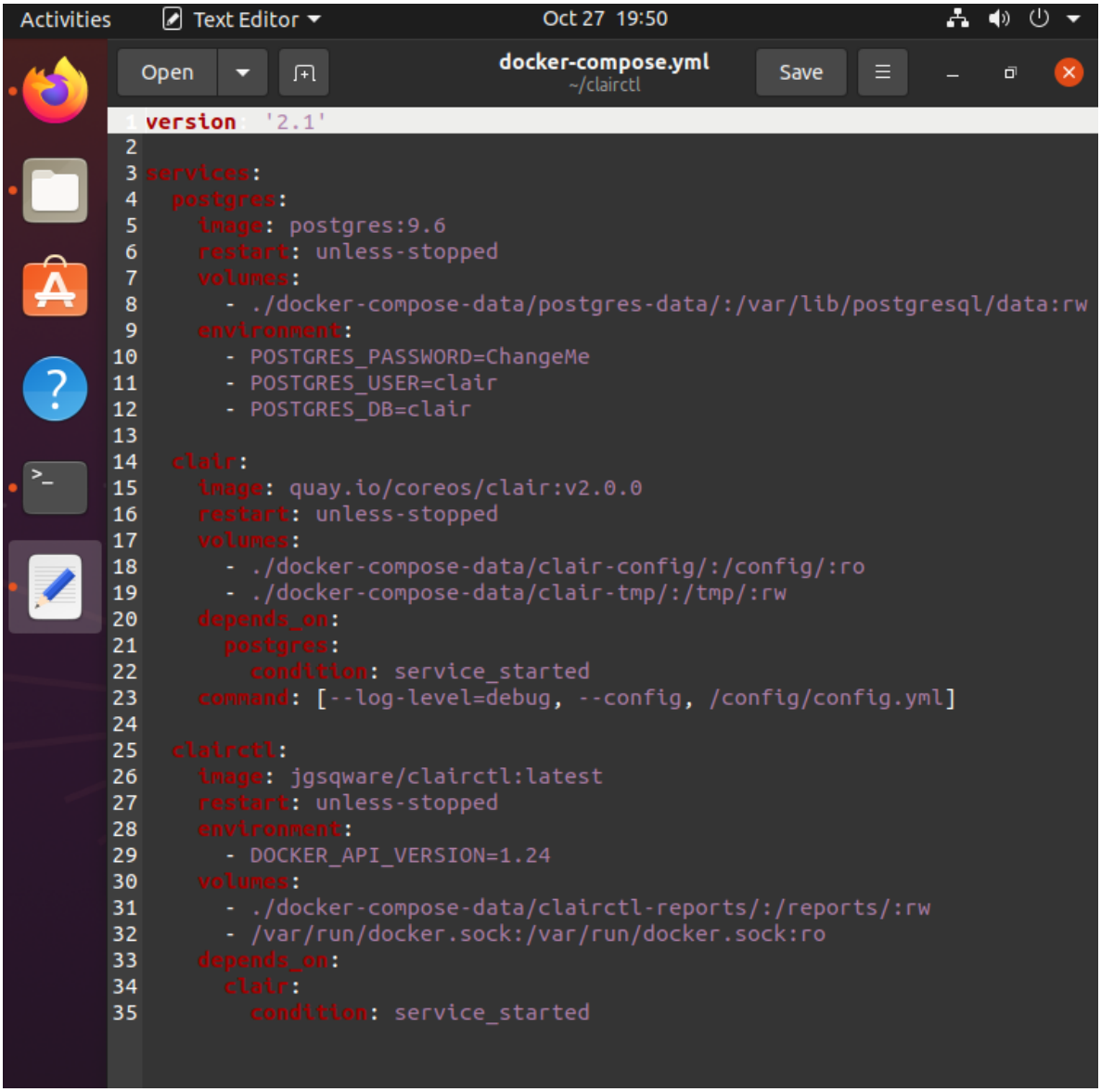

Home
Recent
Starred
Home
Desktop
Documents
Downloads
Music
clairctl
clair-v2
Desktop
Documents
Downloads
Music
Pictures
Public
secdevops-a3
snap
Templates
Videos

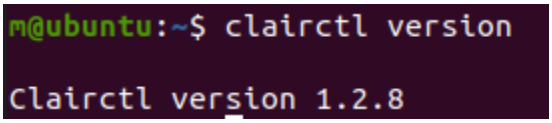



```
cat > ~/.clairctl.yml <<'YAML'
clair:
 uri: http://clair
 port: 6060
 healthPort: 6061
 report:
  path: /root/clairctl/reports
docker:
 insecure-ssl: true
 registry:
  - name: registry
    uri: https://registry:5000
    insecure-ssl: true
YAML
```



version: '2.1'
services: postgres: image: postgres:9.6 restart: unless-stopped volumes: - ./docker-compose-data/postgres-data/:/var/lib/postgresql/data:rw environment: - POSTGRES_PASSWORD=ChangeMe - POSTGRES_USER=clair - POSTGRES_DB=clair clair: image: quay.io/coreos/clair:v2.0.0 restart: unless-stopped volumes: - ./docker-compose-data/clair-config/:/config/:ro - ./docker-compose-data/clair-tmp/:/tmp/:rw depends_on: postgres: condition: service_started command: [--log-level=debug, --config, /config/config.yml]
clairctl: image: jgsqware/clairctl:latest restart: unless-stopped environment: - DOCKER_API_VERSION=1.24 volumes: - ./docker-compose-data/clairctl-reports/:/reports/:rw - /var/run/docker.sock:/var/run/docker.sock:ro depends_on: clair: condition: service_started





b. Scanning the NextCloud image

Push Nextcloud to local registry
docker run -d --restart=always --name registry -p 5000:5000 registry:2
docker tag nextcloud:latest localhost:5000/nextcloud:latest
docker push localhost:5000/nextcloud:latest

```
m@ubuntu:~/clair-v2$ docker run -d --restart=always --name registry -p 50
00:5000 registry:2
d3d5b756b058ce1597ce6b3ad66de6c27a074de1b9f2d30b7268b94cdabca2f2
m@ubuntu:~/clair-v2$ docker tag nextcloud:latest localhost:5000/nextcloud
:latest
m@ubuntu:~/clair-v2$ docker push localhost:5000/nextcloud:latest
The push refers to repository [localhost:5000/nextcloud]
72c5cbcb60d9: Pushed
569e3380c6c9: Pushed
ea88b097d252: Pushed
d39eaa5c1ce0: Pushed
aefebd58a16b: Pushed
f31beee0dec1: Pushed
c5d35f8473a3: Pushed
7717bbb8b074: Pushed
5f70bf18a086: Pushed
6da6ce241629: Pushed
e0be901b9885: Pushed
b0b0c4c00ce3: Pushed
eab84bfa29de: Pushed
bf8e40ac3c46: Pushed
cbf34dbfe55c: Pushed
```

curl -i http://127.0.0.1:6063/ | head -n1

clairctl --config ~/.clairctl.yml health

```
m@ubuntu:~/clair-v2$ curl -i http://127.0.0.1:6063/ | head -n1
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  C
urrent
                                 Dload  Upload   Total   Spent    Left  S
peed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--
100    19  100    19    0     0  19000      0 --:--:-- --:--:-- --:--:--
19000
HTTP/1.1 404 Not Found
m@ubuntu:~/clair-v2$ clairctl --config ~/.clairctl.yml health

Clair: ✔
```

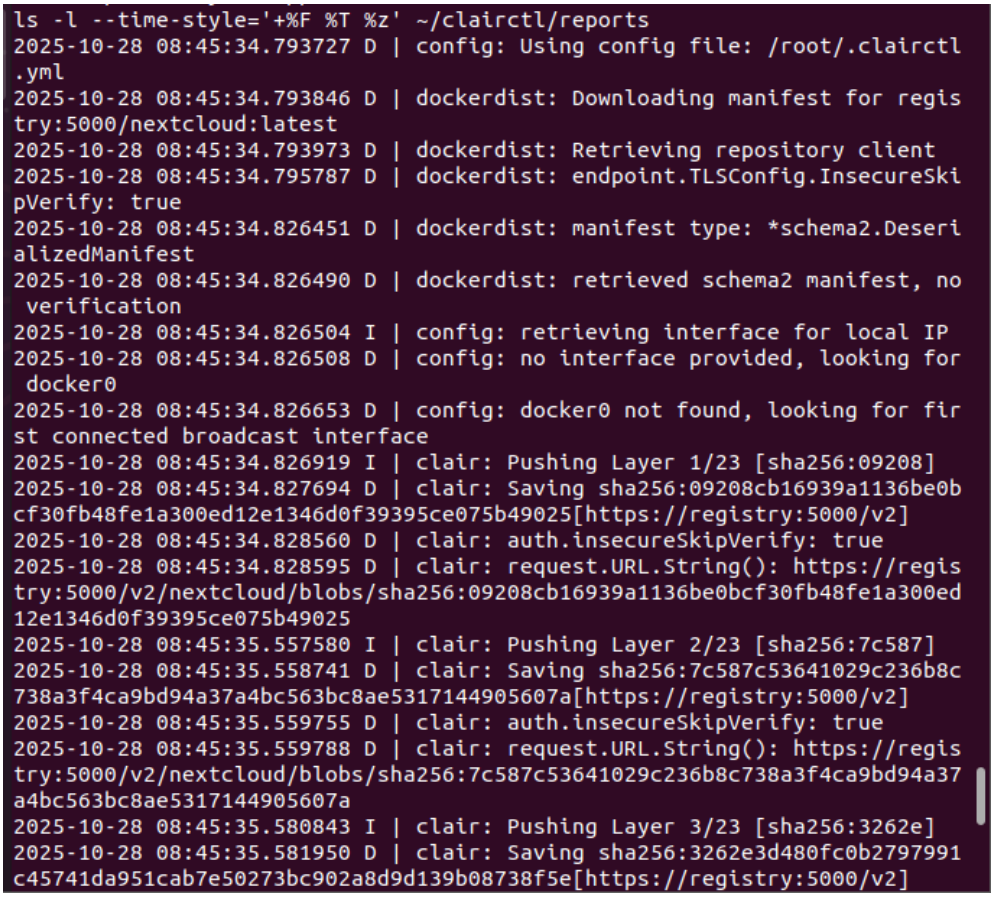
docker tag nextcloud:latest localhost:5000/nextcloud:latest

docker push localhost:5000/nextcloud:latest

```
m@ubuntu:~/clair-v2$ docker tag nextcloud:latest localhost:5000/nextcloud
:latest
m@ubuntu:~/clair-v2$ docker push localhost:5000/nextcloud:latest
The push refers to repository [localhost:5000/nextcloud]
72c5cbcb60d9: Layer already exists
569e3380c6c9: Layer already exists
ea88b097d252: Layer already exists
d39eaa5c1ce0: Layer already exists
aefebd58a16b: Layer already exists
f31beee0dec1: Layer already exists
c5d35f8473a3: Layer already exists
7717bbb8b074: Layer already exists
5f70bf18a086: Layer already exists
6da6ce241629: Layer already exists
e0be901b9885: Layer already exists
b0b0c4c00ce3: Layer already exists
eab84bfa29de: Layer already exists
bf8e40ac3c46: Layer already exists
cbf34dbfe55c: Layer already exists
5b90ee3c1b2c: Layer already exists
5e86fb8dd799: Layer already exists
5267a9f8a6b2: Layer already exists
a9cd4deb2ac4: Layer already exists
64013f07709c: Layer already exists
ec1c6a2202b4: Layer already exists
a70a53678e39: Layer already exists
d7c97cb6f1fe: Layer already exists
latest: digest: sha256:0081e9d77cfb46d077d48eeb578f0ad754e09e34235ae60f06
b7ee91dae474c2 size: 5122
```

```
NET=clair-v2_clairnet
mkdir -p ~/clairctl/reports

# analyze
docker run --rm -it --network "$NET" -u 0:0 \
  -e TZ=Australia/Perth -v /etc/localtime:/etc/localtime:ro \
  -v /var/run/docker.sock:/var/run/docker.sock \
  -v $HOME/.clairctl.yml:/root/.clairctl.yml:ro \
  -v $HOME/clairctl:/root/clairctl \
  jgsqware/clairctl:latest \
  clairctl --config /root/.clairctl.yml --log-level Debug analyze registry:5000/nextcloud:latest

# HTML report
docker run --rm -it --network "$NET" -u 0:0 \
  -e TZ=Australia/Perth -v /etc/localtime:/etc/localtime:ro \
  -v /var/run/docker.sock:/var/run/docker.sock \
```

```
 -v $HOME/.clairctl.yml:/root/.clairctl.yml:ro \
 -v $HOME/clairctl:/root/clairctl \
 jgsqware/clairctl:latest \
 clairctl --config /root/.clairctl.yml report registry:5000/nextcloud:latest --format html

# JSON report saved to host
docker run --rm -it --network "$NET" -u 0:0 \
 -e TZ=Australia/Perth -v /etc/localtime:/etc/localtime:ro \
 -v /var/run/docker.sock:/var/run/docker.sock \
 -v $HOME/.clairctl.yml:/root/.clairctl.yml:ro \
 -v $HOME/clairctl:/root/clairctl \
 jgsqware/clairctl:latest \
 sh -lc 'clairctl --config /root/.clairctl.yml report registry:5000/nextcloud:latest --format
json > /root/clairctl/reports/nextcloud.json'

# receipts for your appendix
ls -l --time-style='+%F %T %z' ~/clairctl/reports
```



```
ls -l --time-style='+%F %T %z' ~/clairctl/reports
2025-10-28 08:45:34.793727 D | config: Using config file: /root/.clairctl
.yml
2025-10-28 08:45:34.793846 D | dockerdist: Downloading manifest for regis
try:5000/nextcloud:latest
2025-10-28 08:45:34.793973 D | dockerdist: Retrieving repository client
2025-10-28 08:45:34.795787 D | dockerdist: endpoint.TLSConfig.InsecureSki
pVerify: true
2025-10-28 08:45:34.826451 D | dockerdist: manifest type: *schema2.Deseri
alizedManifest
2025-10-28 08:45:34.826490 D | dockerdist: retrieved schema2 manifest, no
 verification
2025-10-28 08:45:34.826504 I | config: retrieving interface for local IP
2025-10-28 08:45:34.826508 D | config: no interface provided, looking for
 docker0
2025-10-28 08:45:34.826653 D | config: docker0 not found, looking for fir
st connected broadcast interface
2025-10-28 08:45:34.826919 I | clair: Pushing Layer 1/23 [sha256:09208]
2025-10-28 08:45:34.827694 D | clair: Saving sha256:09208cb16939a1136be0b
cf30fb48fe1a300ed12e1346d0f39395ce075b49025[https://registry:5000/v2]
2025-10-28 08:45:34.828560 D | clair: auth.insecureSkipVerify: true
2025-10-28 08:45:34.828595 D | clair: request.URL.String(): https://regis
try:5000/v2/nextcloud/blobs/sha256:09208cb16939a1136be0bcf30fb48fe1a300ed
12e1346d0f39395ce075b49025
2025-10-28 08:45:35.557580 I | clair: Pushing Layer 2/23 [sha256:7c587]
2025-10-28 08:45:35.558741 D | clair: Saving sha256:7c587c53641029c236b8c
738a3f4ca9bd94a37a4bc563bc8ae5317144905607a[https://registry:5000/v2]
2025-10-28 08:45:35.559755 D | clair: auth.insecureSkipVerify: true
2025-10-28 08:45:35.559788 D | clair: request.URL.String(): https://regis
try:5000/v2/nextcloud/blobs/sha256:7c587c53641029c236b8c738a3f4ca9bd94a37
a4bc563bc8ae5317144905607a
2025-10-28 08:45:35.580843 I | clair: Pushing Layer 3/23 [sha256:3262e]
2025-10-28 08:45:35.581950 D | clair: Saving sha256:3262e3d480fc0b2797991
c45741da951cab7e50273bc902a8d9d139b08738f5e[https://registry:5000/v2]
```

```
2025-10-28 08:45:43.150905 D | clair: json: registry:5000/nextcloud:lates
t
2025-10-28 08:45:43.161529 I | clair: analysing layer [sha256:1051a] 1/23
2025-10-28 08:45:43.167830 I | clair: analysing layer [sha256:a3c9d] 2/23
2025-10-28 08:45:43.174575 I | clair: analysing layer [sha256:3ba30] 3/23
2025-10-28 08:45:43.180863 I | clair: analysing layer [sha256:e82a1] 4/23
2025-10-28 08:45:43.189349 I | clair: analysing layer [sha256:db4cf] 5/23
2025-10-28 08:45:43.195954 I | clair: analysing layer [sha256:1915d] 6/23
2025-10-28 08:45:43.201511 I | clair: analysing layer [sha256:82090] 7/23
2025-10-28 08:45:43.210464 I | clair: analysing layer [sha256:2f7d5] 8/23
2025-10-28 08:45:43.217312 I | clair: analysing layer [sha256:4f4fb] 9/23
2025-10-28 08:45:43.225491 I | clair: analysing layer [sha256:75c3b] 10/2
3
2025-10-28 08:45:43.232423 I | clair: analysing layer [sha256:cc4c6] 11/2
3
2025-10-28 08:45:43.238090 I | clair: analysing layer [sha256:061dd] 12/2
3
2025-10-28 08:45:43.243670 I | clair: analysing layer [sha256:3c631] 13/2
3
2025-10-28 08:45:43.247894 I | clair: analysing layer [sha256:70580] 14/2
3
2025-10-28 08:45:43.253672 I | clair: analysing layer [sha256:978f9] 15/2
3
2025-10-28 08:45:43.259483 I | clair: analysing layer [sha256:5d7ef] 16/2
3
2025-10-28 08:45:43.265983 I | clair: analysing layer [sha256:095e6] 17/2
3
2025-10-28 08:45:43.272538 I | clair: analysing layer [sha256:0c7f7] 18/2
3
2025-10-28 08:45:43.277557 I | clair: analysing layer [sha256:38a62] 19/2
3
2025-10-28 08:45:43.283333 I | clair: analysing layer [sha256:96dfb] 20/2
3
2025-10-28 08:45:43.289444 I | clair: analysing layer [sha256:3262e] 21/2
3
2025-10-28 08:45:43.294426 I | clair: analysing layer [sha256:7c587] 22/2
3
2025-10-28 08:45:43.300354 I | clair: analysing layer [sha256:09208] 23/2
3

Image: registry:5000/registry:5000/nextcloud:latest
 23 layers found

  ➜ Analysis [sha256:1051a] found 0 vulnerabilities.
  ➜ Analysis [sha256:a3c9d] found 0 vulnerabilities.
```

c. Generating and reviewing the report.

```
Image: registry:5000/registry:5000/nextcloud:latest
 23 layers found

  ➜ Analysis [sha256:1051a] found 0 vulnerabilities.
  ➜ Analysis [sha256:a3c9d] found 0 vulnerabilities.
  ➜ Analysis [sha256:3ba30] found 0 vulnerabilities.
  ➜ Analysis [sha256:e82a1] found 0 vulnerabilities.
  ➜ Analysis [sha256:db4cf] found 0 vulnerabilities.
  ➜ Analysis [sha256:1915d] found 0 vulnerabilities.
  ➜ Analysis [sha256:82090] found 0 vulnerabilities.
  ➜ Analysis [sha256:2f7d5] found 0 vulnerabilities.
  ➜ Analysis [sha256:4f4fb] found 0 vulnerabilities.
  ➜ Analysis [sha256:75c3b] found 0 vulnerabilities.
  ➜ Analysis [sha256:cc4c6] found 0 vulnerabilities.
  ➜ Analysis [sha256:061dd] found 0 vulnerabilities.
  ➜ Analysis [sha256:3c631] found 0 vulnerabilities.
  ➜ Analysis [sha256:70580] found 0 vulnerabilities.
  ➜ Analysis [sha256:978f9] found 0 vulnerabilities.
  ➜ Analysis [sha256:5d7ef] found 0 vulnerabilities.
  ➜ Analysis [sha256:095e6] found 0 vulnerabilities.
  ➜ Analysis [sha256:0c7f7] found 0 vulnerabilities.
  ➜ Analysis [sha256:38a62] found 0 vulnerabilities.
  ➜ Analysis [sha256:96dfb] found 0 vulnerabilities.
  ➜ Analysis [sha256:3262e] found 0 vulnerabilities.
  ➜ Analysis [sha256:7c587] found 0 vulnerabilities.
  ➜ Analysis [sha256:09208] found 0 vulnerabilities.
```

mkdir -p ~/clairctl/reports

clairctl --config ~/.clairctl.yml report ${BRIDGE_IP}:5000/nextcloud:latest --format html

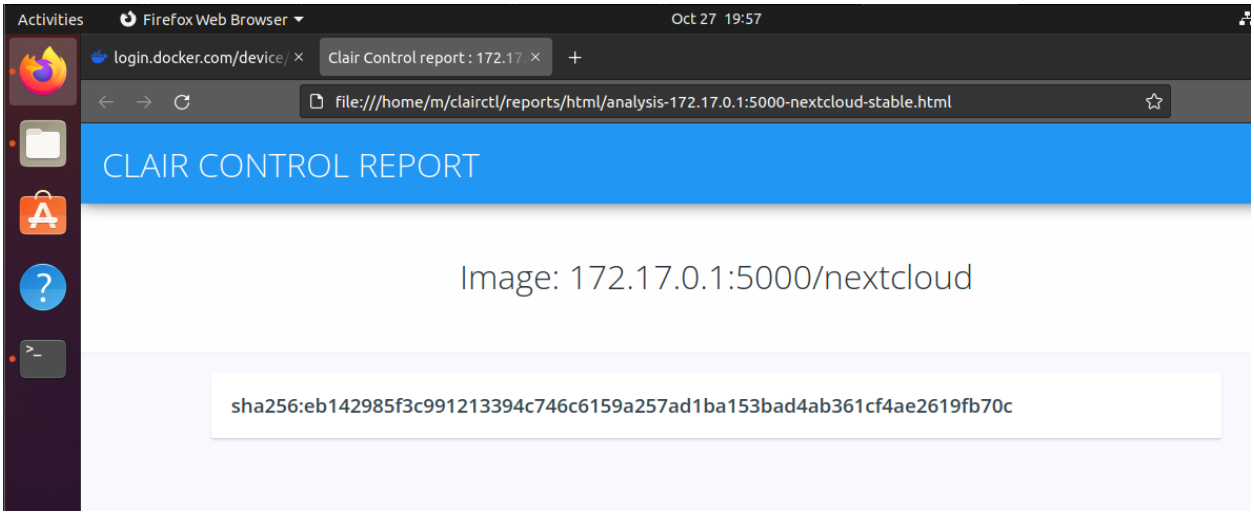
ls -la ~/clairctl/reports

```
m@ubuntu:~$ mkdir -p ~/clairctl/reports
m@ubuntu:~$ clairctl --config ~/.clairctl.yml report ${BRIDGE_IP}:5000/ne
xtcloud:latest --format html
client quit unexpectedly
2025-10-27 23:53:51.954850 C | cmd: retrieving manifest for "172.17.0.1:5
000/nextcloud:latest": Get https://172.17.0.1:5000/v2/: http: server gave
 HTTP response to HTTPS client
m@ubuntu:~$ ls -la ~/clairctl/reports
total 16
drwxrwxr-x  4 m docker 4096 Oct 27 20:10 .
drwxrwxr-x 15 m m      4096 Oct 27 22:53 ..
drwxrwxr-x  2 m m      4096 Oct 27 19:13 html
drwxrwxr-x  2 m m      4096 Oct 27 20:10 json
```

ls -lh reports/html

```
m@ubuntu:~/clairctl$ ls -lh reports/html
total 12K
-rw-rw-r-- 1 m m 12K Oct 27 19:13 analysis-172.17.0.1:5000-nextcloud-stabl
e.html
```

xdg-open reports/html/analysis-172.17.0.1:5000-nextcloud-stable.html



D. Remediation notes

- Base image hygiene: keep Nextcloud at latest (pull updated tag regularly).

- Patch cadence: rebuild/push when upstream OS packages patch CVEs.

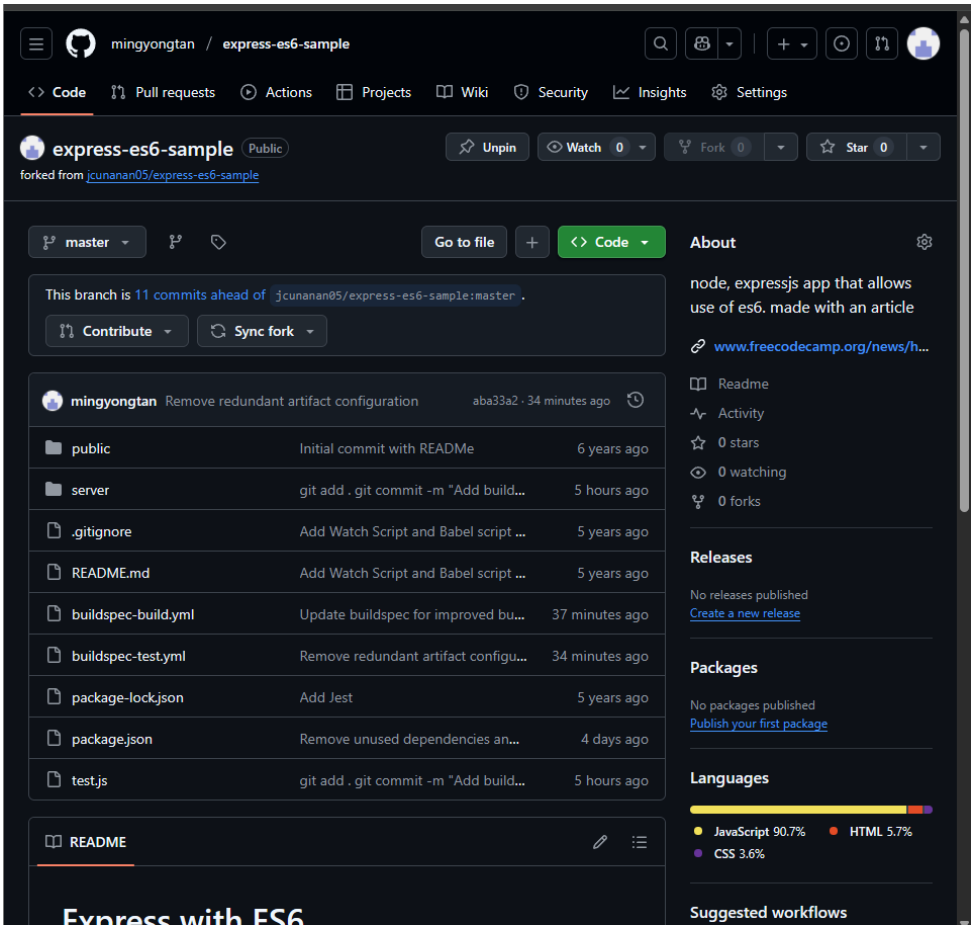
- Hardening: run as non-root, add minimal capabilities, enforce read-only FS where possible, pin digest for immutability.

Task 5: AWS CodePipeline for Node.js

Repository: https://github.com/mingyongtan/express-es6-sample

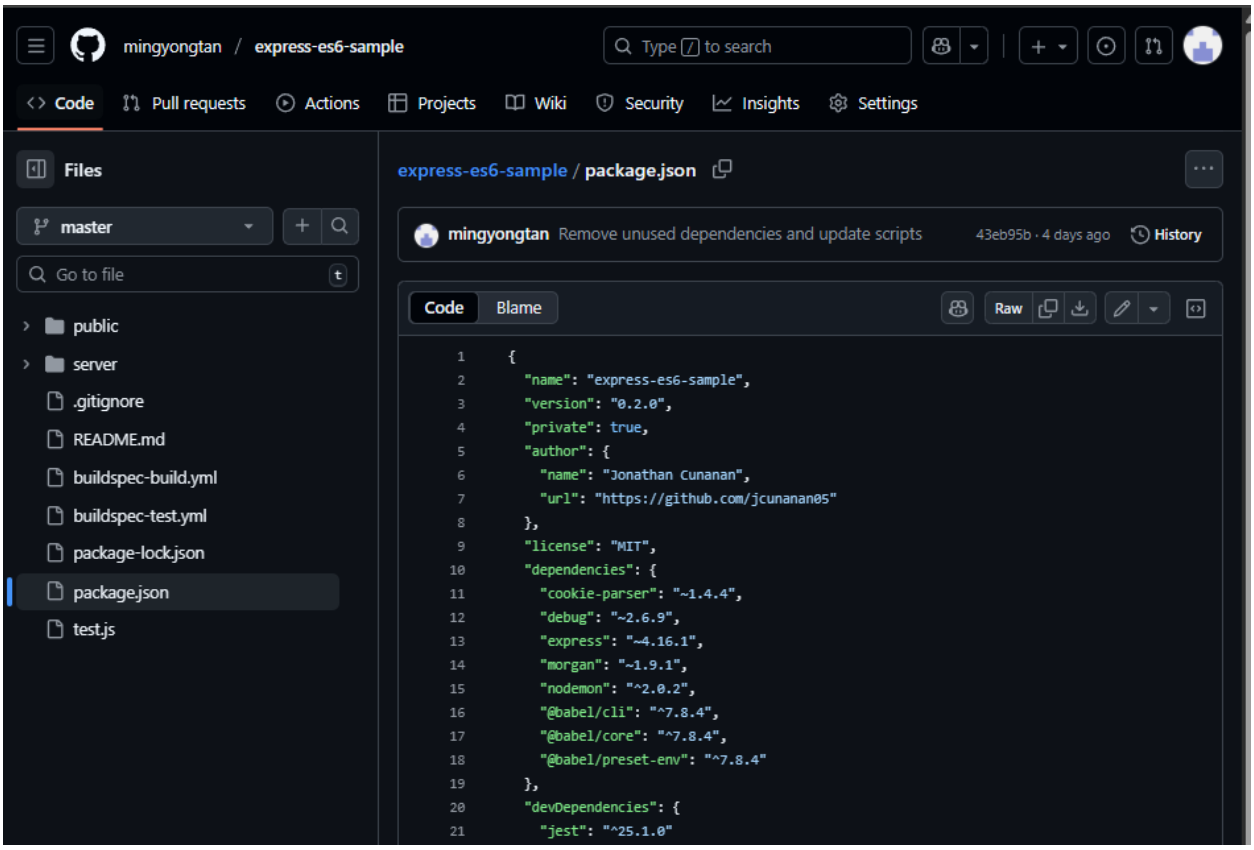
Actions:

- Forked from jcunanan05/express-es6-sample
- Kept private (OAuth used)
- Latest commit: aba33a21 (includes buildspec-build.yml, buildspec-test.yml)



Replace package.json

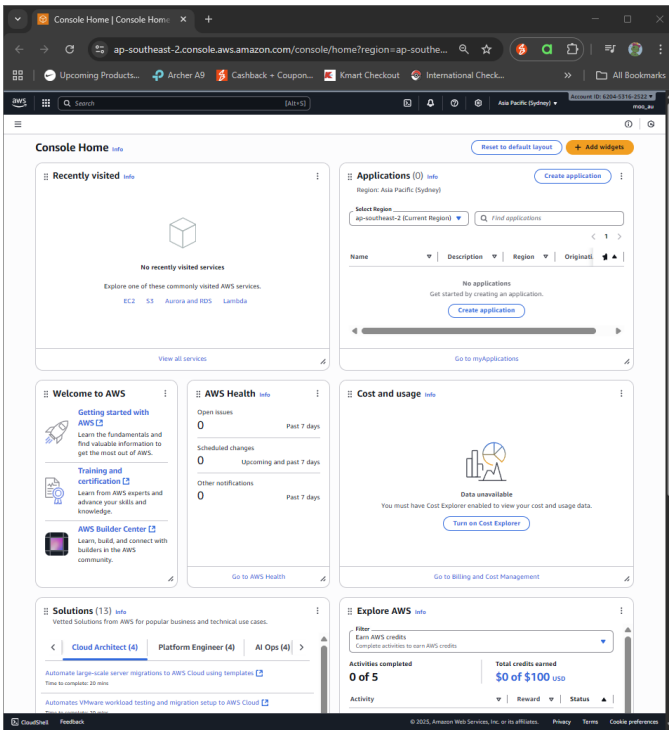
Ming Yong Tan 21920794



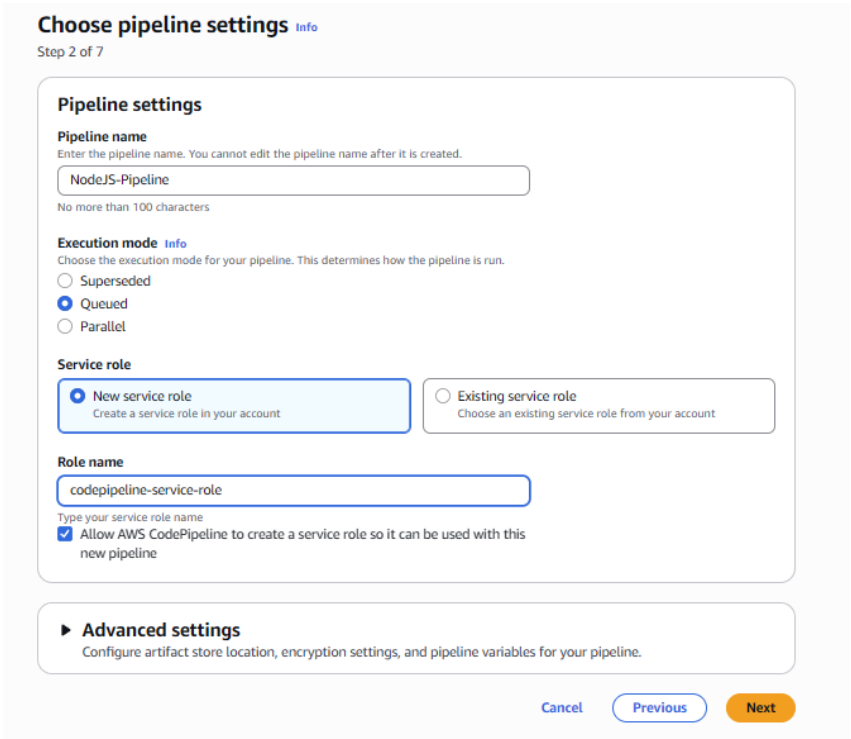
git clone https://github.com/mingyongtan/express-es6-sample.git
cd express-es6-sample
cp ~/Downloads/package.json ./package.json # replace with the provided one
git add package.json
git commit -m "Replace package.json per assignment spec"
git push origin master

Ming Yong Tan 21920794

Create AWS codepipeline

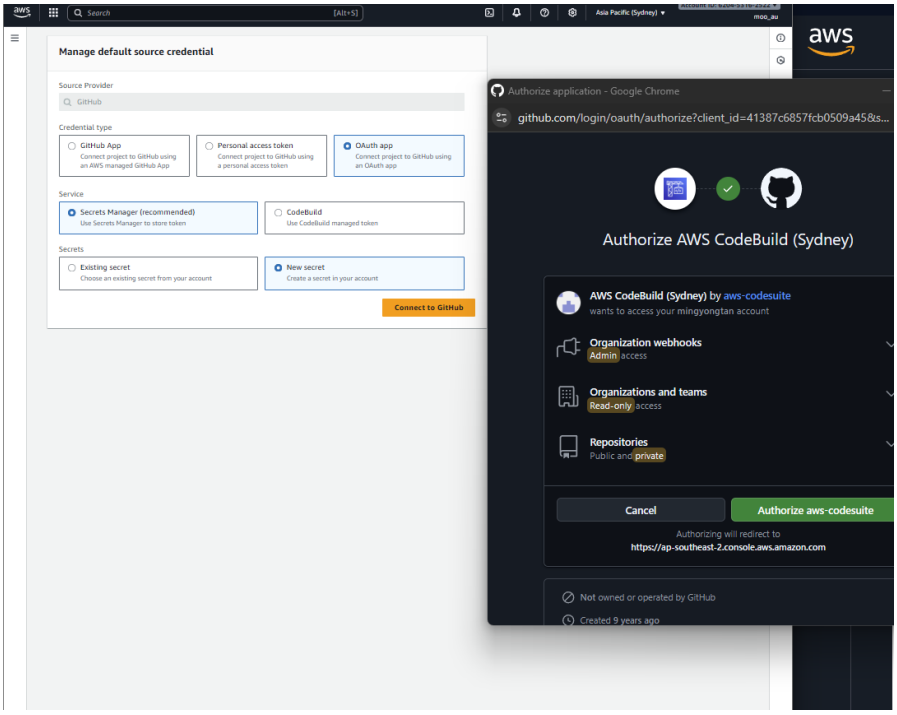


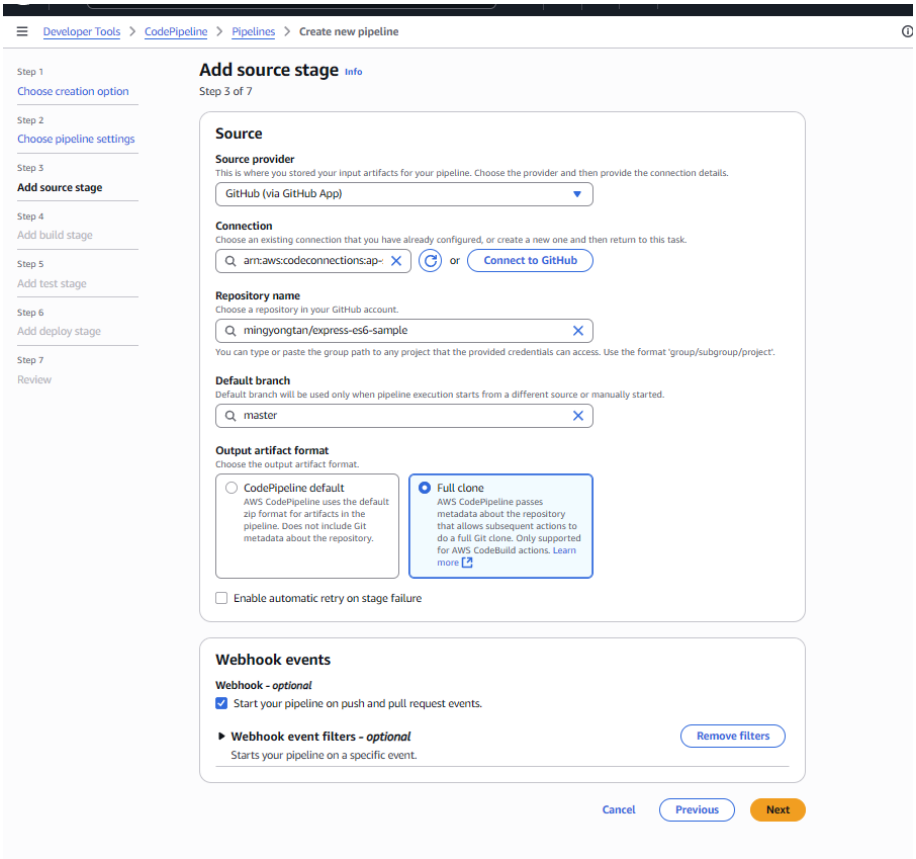
Configure AWS CodePipeline



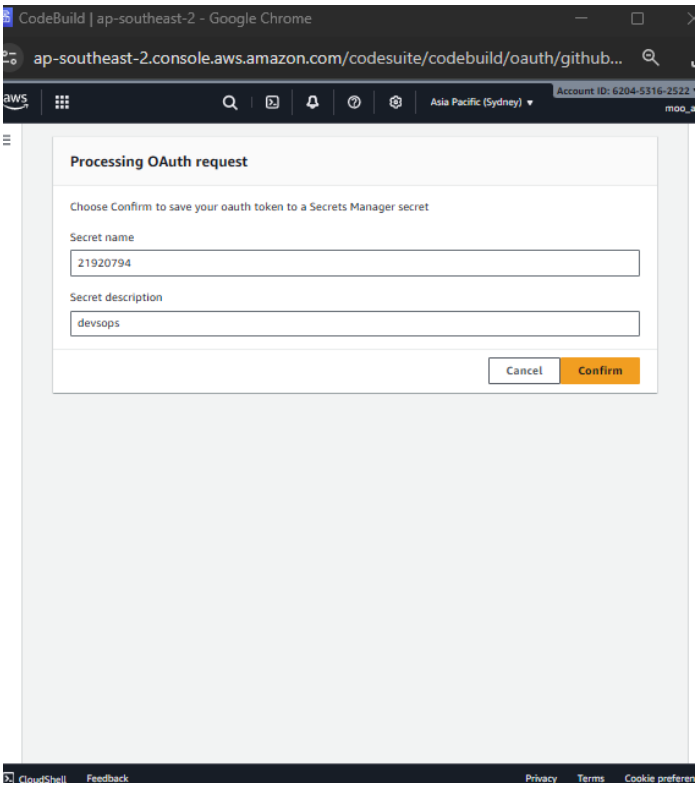
1. Stage 1: Source

Oauth github with aws first.





Ming Yong Tan 21920794



Step 3: Add source stage

Source action provider

Source action provider
GitHub (via GitHub App)

OutputArtifactFormat
CODEBUILD_CLONE_REF

DetectChanges
true

ConnectionArn
arn:aws:codeconnections:us-west-1:023373559263:connection/1659a502-8171-45c8-9e12-a284ee3414c0

FullRepositoryId
mingyongtan/express-es6-sample

Default branch
master

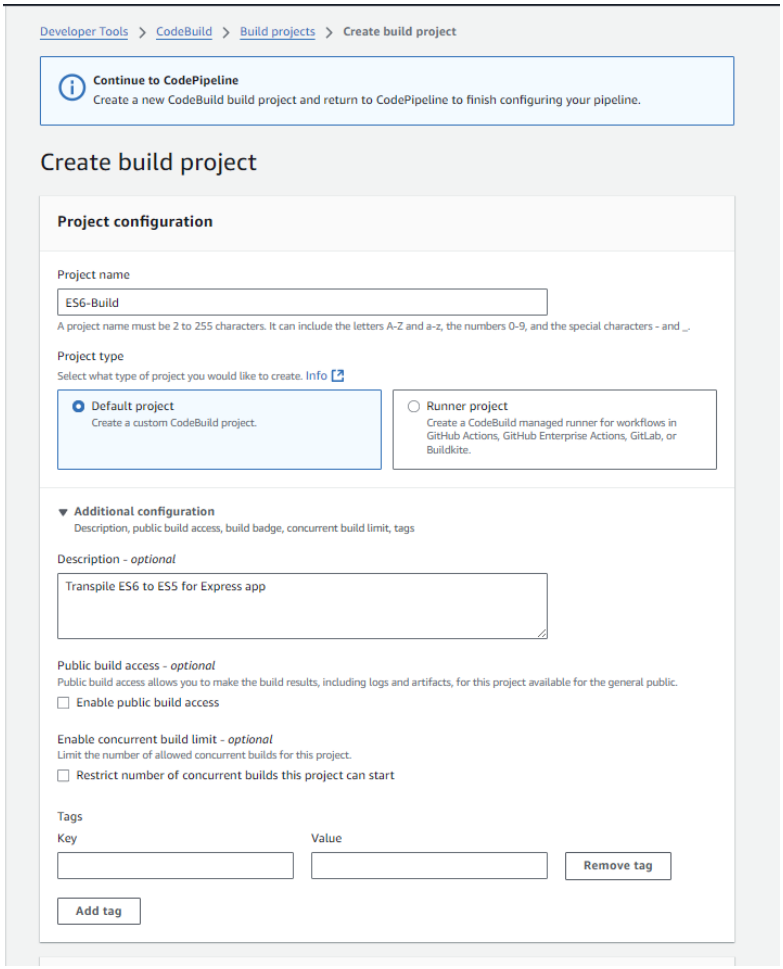
Enable automatic retry on stage failure
Enabled

Trigger configuration

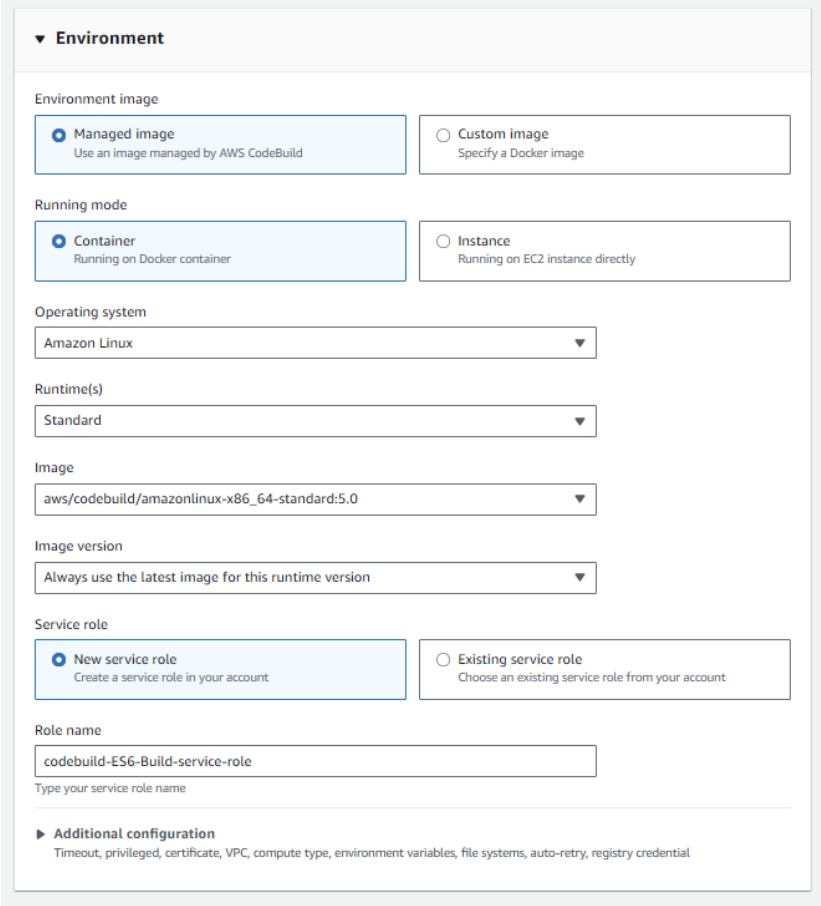
You can add additional pipeline triggers after the pipeline is created.

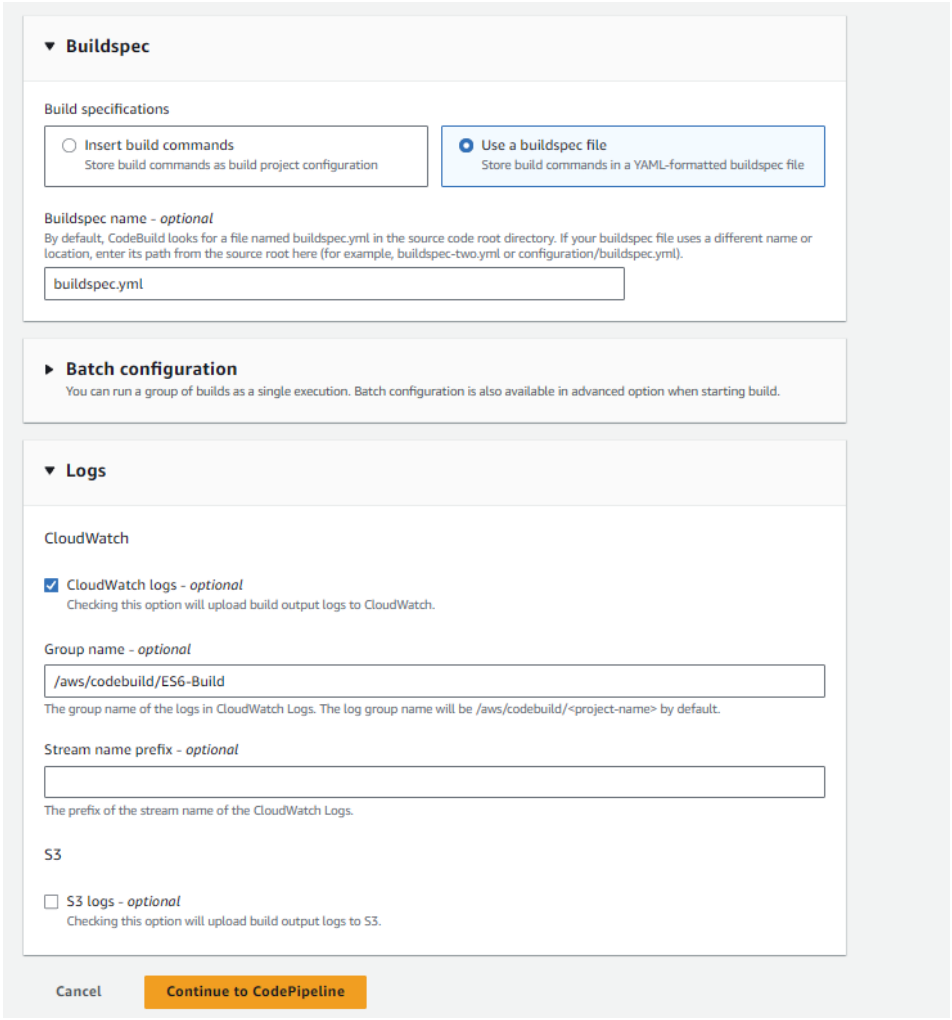
Trigger type
No filter

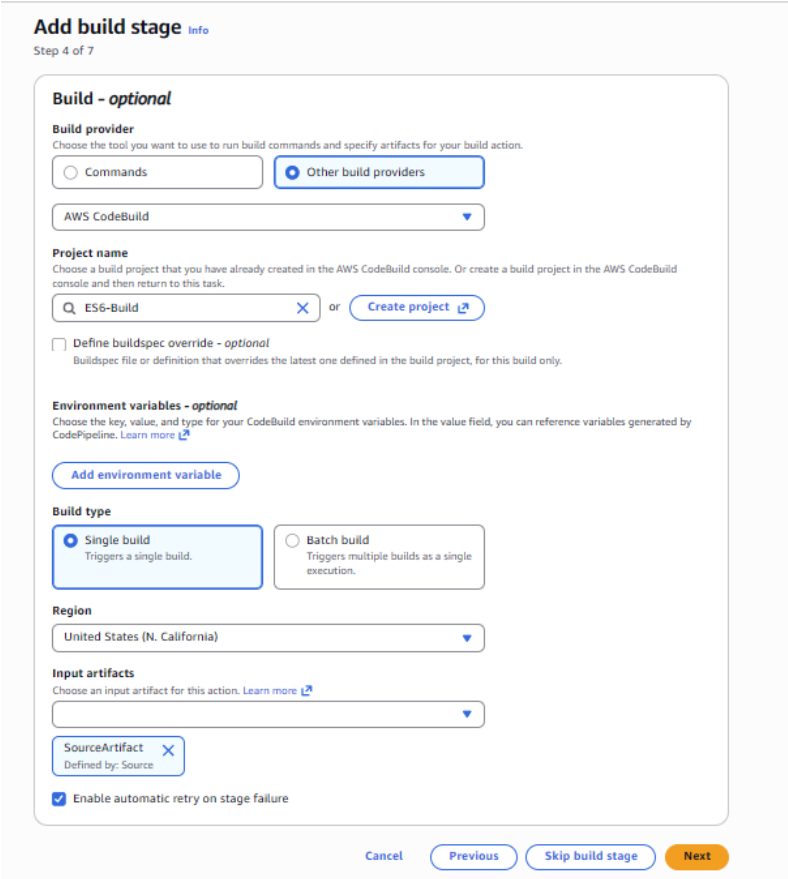
2. Stage 2: Build

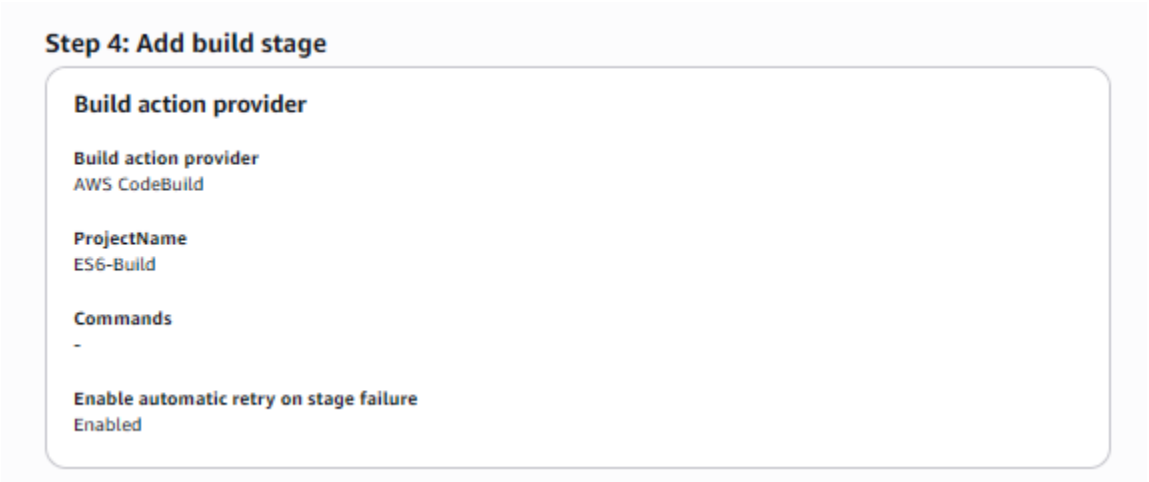


Ming Yong Tan 21920794

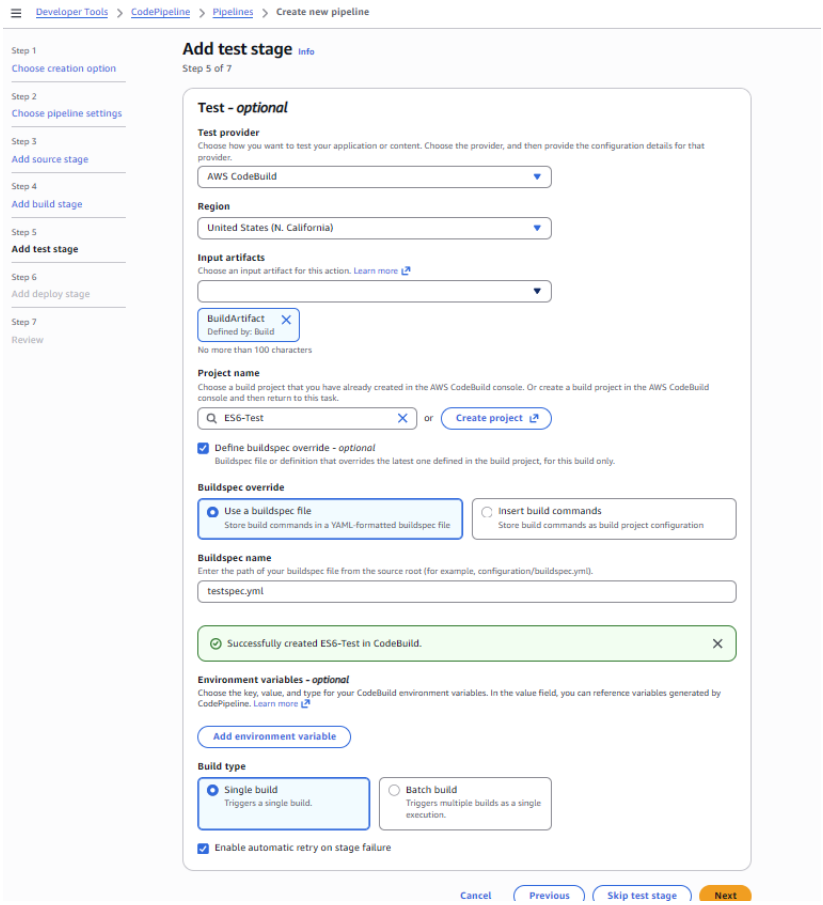


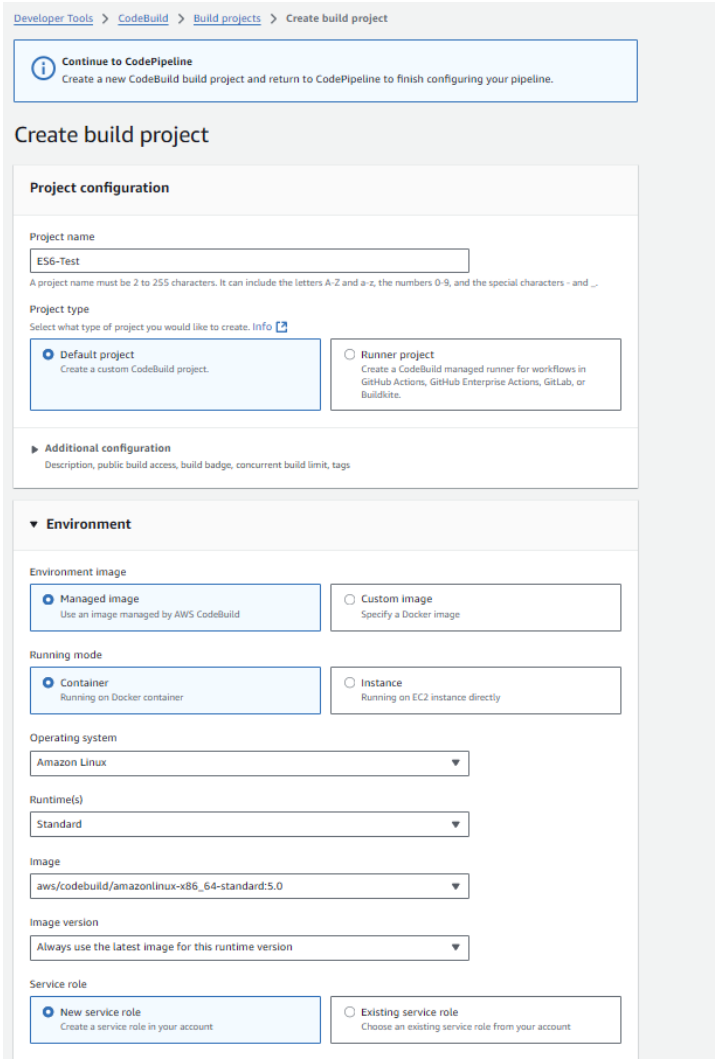

Buildspec
Build specifications
Insert build commands
Store build commands as build project configuration
Use a buildspec file
Store build commands in a YAML-formatted buildspec file
Buildspec name - optional
By default, CodeBuild looks for a file named buildspec.yml in the source code root directory. If your buildspec file uses a different name or location, enter its path from the source root here (for example, buildspec-two.yml or configuration/buildspec.yml).
buildspec.yml
Batch configuration
You can run a group of builds as a single execution. Batch configuration is also available in advanced option when starting build.
Logs
CloudWatch
CloudWatch logs - optional
Checking this option will upload build output logs to CloudWatch.
Group name - optional
/aws/codebuild/ES6-Build
The group name of the logs in CloudWatch Logs. The log group name will be /aws/codebuild/<project-name> by default.
Stream name prefix - optional
The prefix of the stream name of the CloudWatch Logs.
S3
S3 logs - optional
Checking this option will upload build output logs to S3.
Cancel
Continue to CodePipeline

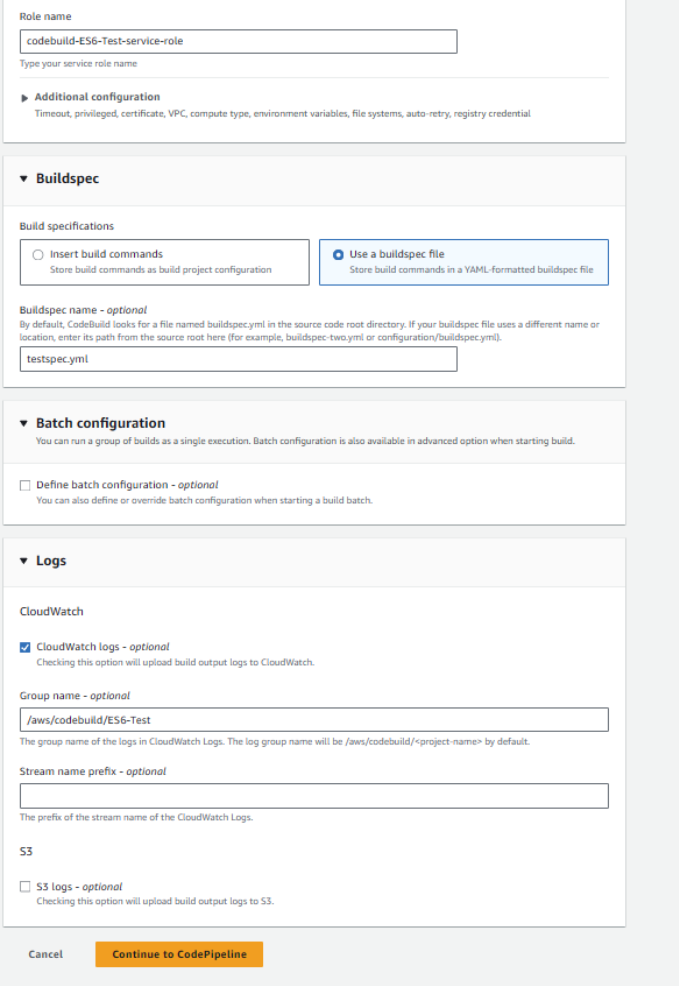

Add build stage Info
Step 4 of 7
Build - optional
Build provider
Choose the tool you want to use to run build commands and specify artifacts for your build action.
Commands
Other build providers
AWS CodeBuild
Project name
Choose a build project that you have already created in the AWS CodeBuild console. Or create a build project in the AWS CodeBuild console and then return to this task.
ES6-Build
or
Create project
Define buildspec override - optional
Buildspec file or definition that overrides the latest one defined in the build project, for this build only.
Environment variables - optional
Choose the key, value, and type for your CodeBuild environment variables. In the value field, you can reference variables generated by CodePipeline. Learn more
Add environment variable
Build type
Single build
Triggers a single build.
Batch build
Triggers multiple builds as a single execution.
Region
United States (N. California)
Input artifacts
Choose an input artifact for this action. Learn more
SourceArtifact
Defined by: Source
Enable automatic retry on stage failure
Cancel
Previous
Skip build stage
Next

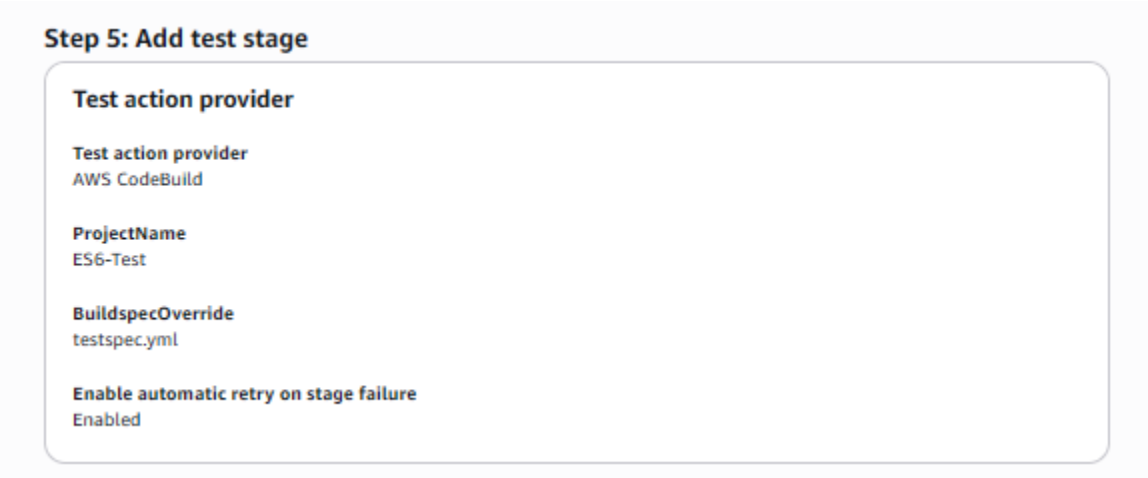

Step 4: Add build stage
Build action provider
Build action provider
AWS CodeBuild
ProjectName
ES6-Build
Commands
-
Enable automatic retry on stage failure
Enabled

3. Stage 3: Test



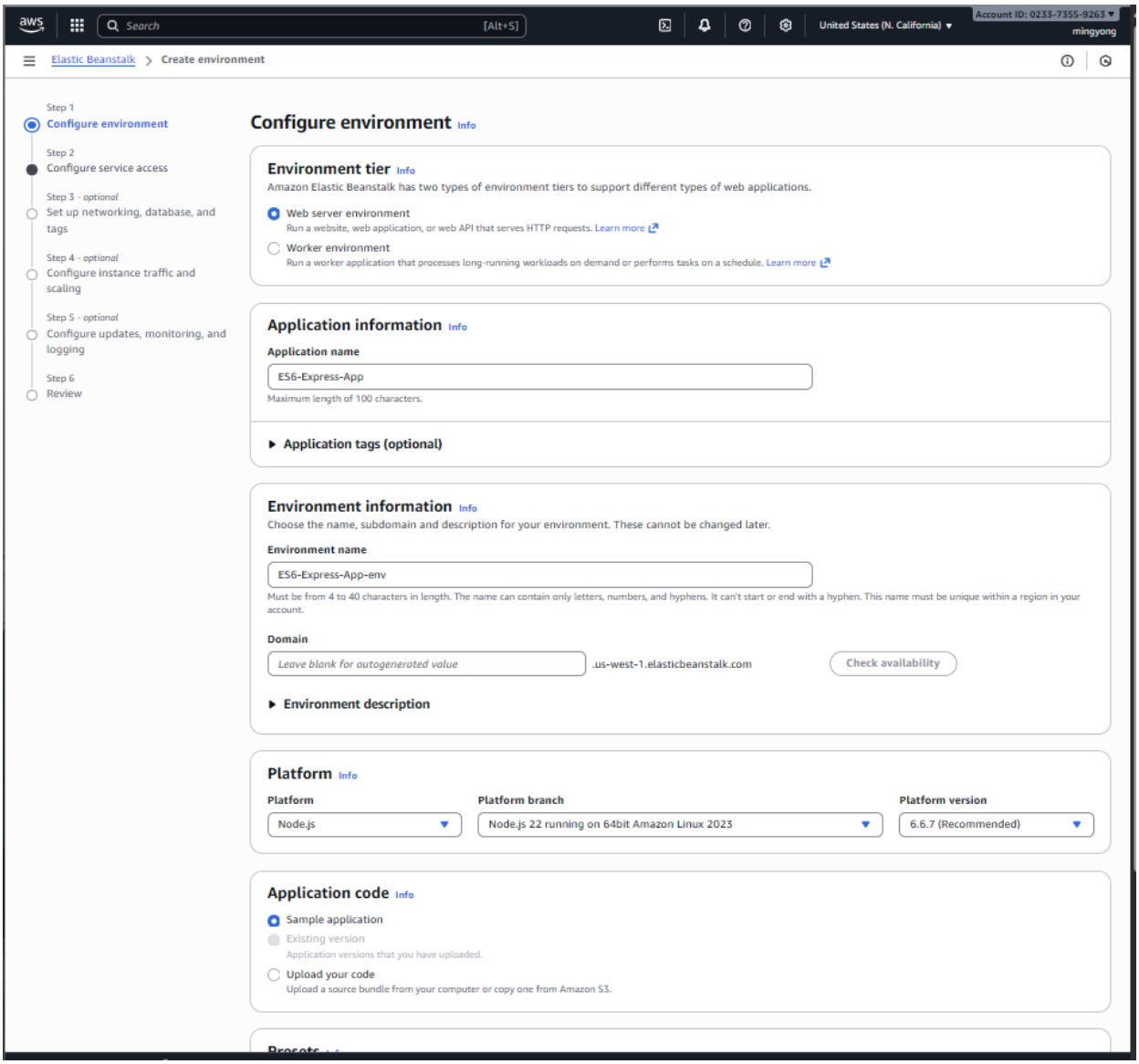

Developer Tools > CodeBuild > Build projects > Create build project
Continue to CodePipeline
Create a new CodeBuild build project and return to CodePipeline to finish configuring your pipeline.
Create build project
Project configuration
Project name
ES6-Test
A project name must be 2 to 255 characters. It can include the letters A-Z and a-z, the numbers 0-9, and the special characters - and _.
Project type
Select what type of project you would like to create. Info
Default project
Create a custom CodeBuild project.
Runner project
Create a CodeBuild managed runner for workflows in GitHub Actions, GitHub Enterprise Actions, GitLab, or Buildkite.
Additional configuration
Description, public build access, build badge, concurrent build limit, tags
Environment
Environment image
Managed image
Use an image managed by AWS CodeBuild
Custom image
Specify a Docker image
Running mode
Container
Running on Docker container
Instance
Running on EC2 instance directly
Operating system
Amazon Linux
Runtime(s)
Standard
Image
aws/codebuild/amazonlinux-x86_64-standard:5.0
Image version
Always use the latest image for this runtime version
Service role
New service role
Create a service role in your account
Existing service role
Choose an existing service role from your account


Role name
codebuild-ES6-Test-service-role
Type your service role name
Additional configuration
Timeout, privileged, certificate, VPC, compute type, environment variables, file systems, auto-retry, registry credential
Buildspec
Build specifications
Insert build commands
Store build commands as build project configuration
Use a buildspec file
Store build commands in a YAML-formatted buildspec file
Buildspec name - optional
By default, CodeBuild looks for a file named buildspec.yml in the source code root directory. If your buildspec file uses a different name or location, enter its path from the source root here (for example, buildspec-two.yml or configuration/buildspec.yml).
testspec.yml
Batch configuration
You can run a group of builds as a single execution. Batch configuration is also available in advanced option when starting build.
Define batch configuration - optional
You can also define or override batch configuration when starting a build batch.
Logs
CloudWatch
CloudWatch logs - optional
Checking this option will upload build output logs to CloudWatch.
Group name - optional
/aws/codebuild/ES6-Test
The group name of the logs in CloudWatch Logs. The log group name will be /aws/codebuild/<project-name> by default.
Stream name prefix - optional
The prefix of the stream name of the CloudWatch Logs.
S3
S3 logs - optional
Checking this option will upload build output logs to S3.
Cancel
Continue to CodePipeline

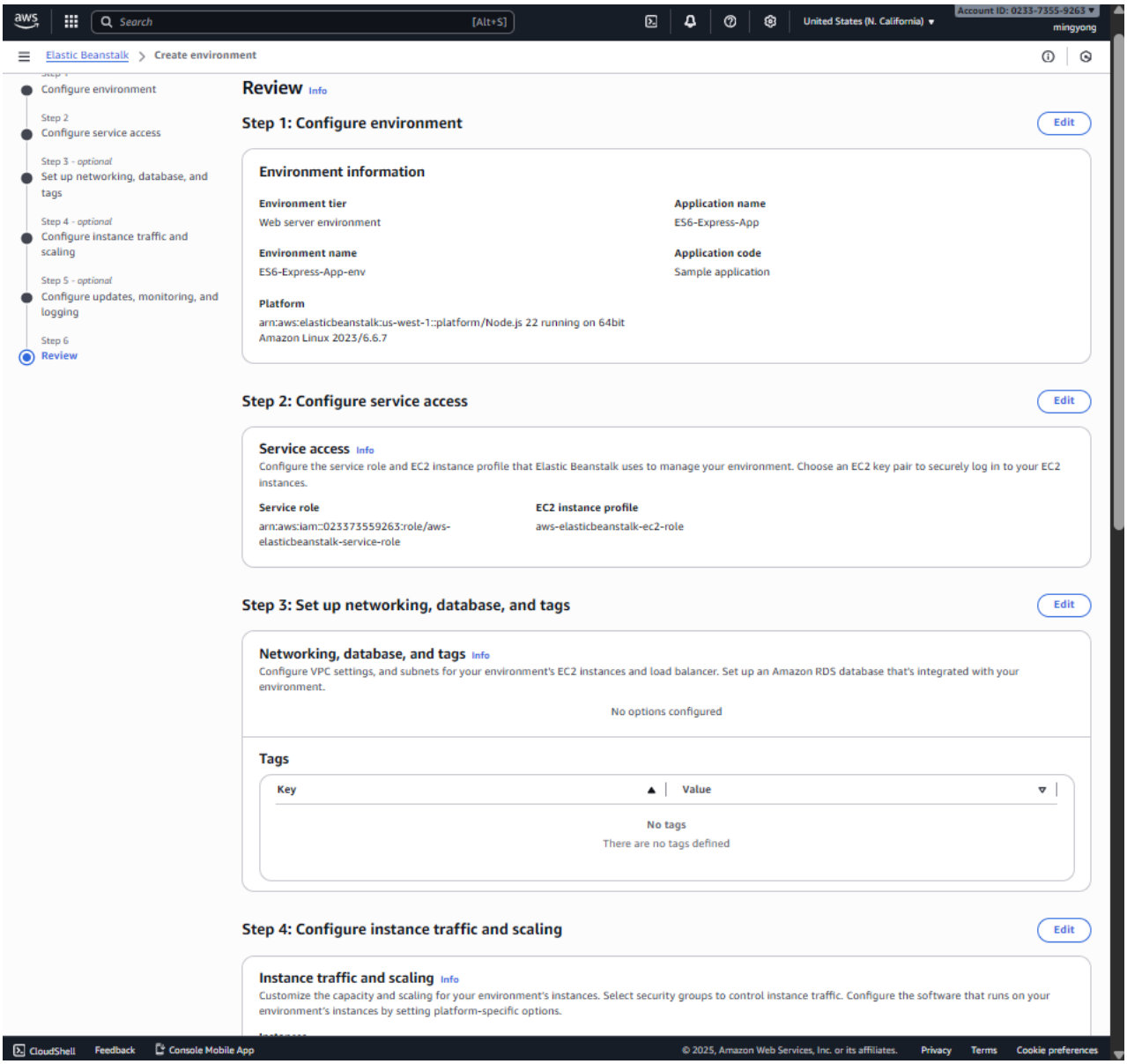

Step 5: Add test stage
Test action provider
Test action provider
AWS CodeBuild
ProjectName
ES6-Test
BuildspecOverride
testspec.yml
Enable automatic retry on stage failure
Enabled

4. Stage 4 Delopy

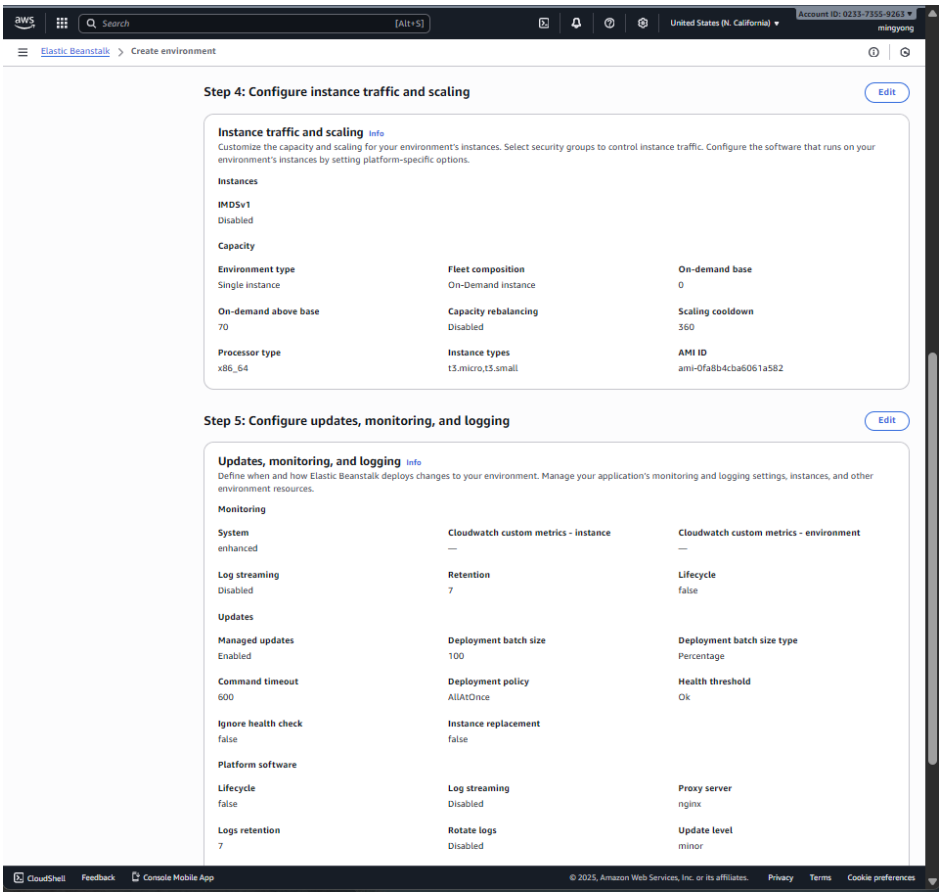
Need to precreate the environment and application first.

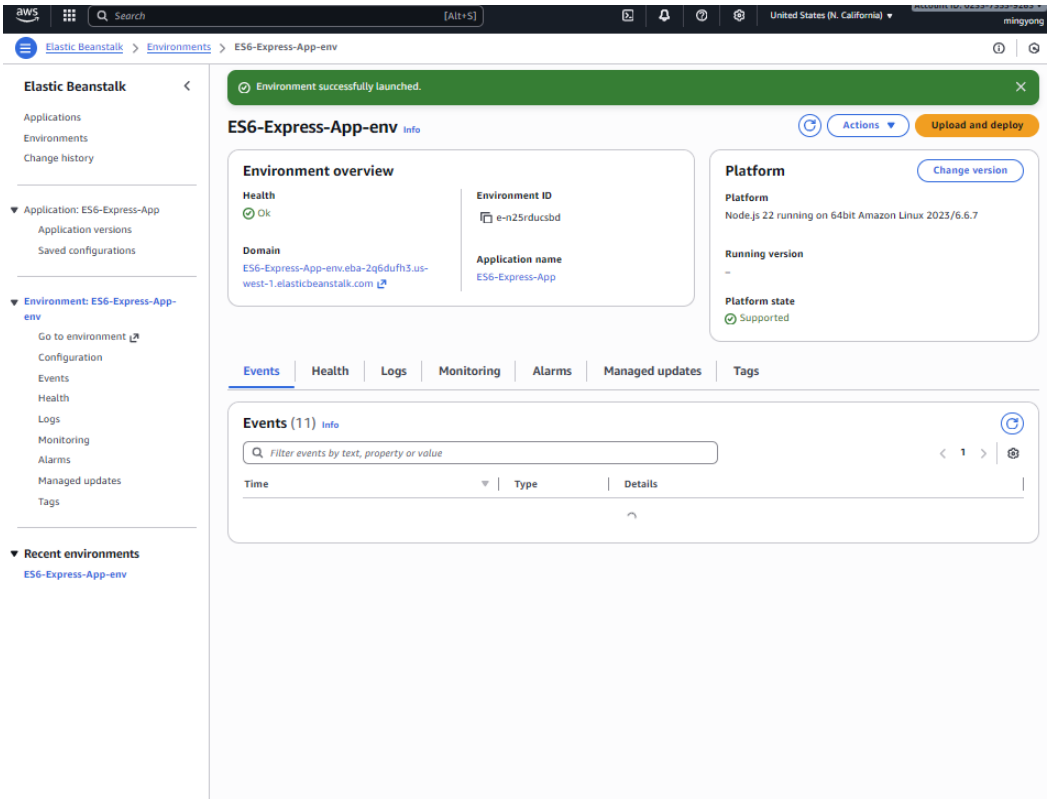


Ming Yong Tan 21920794



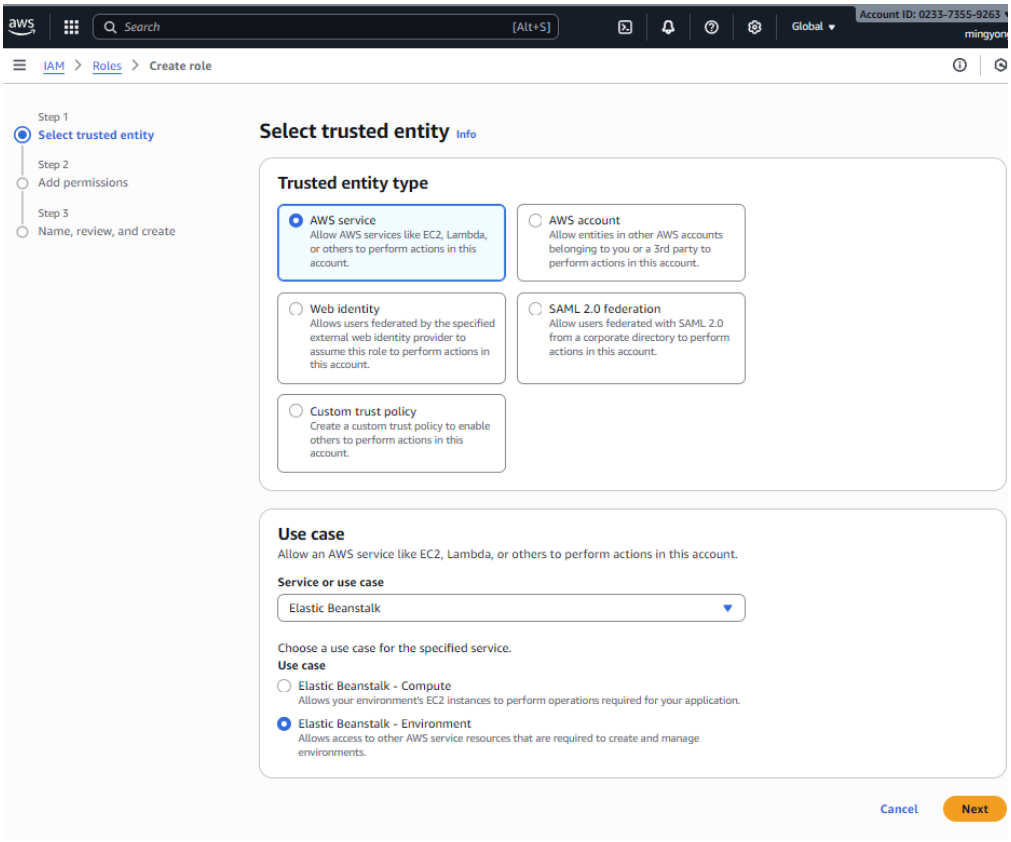
Ming Yong Tan 21920794

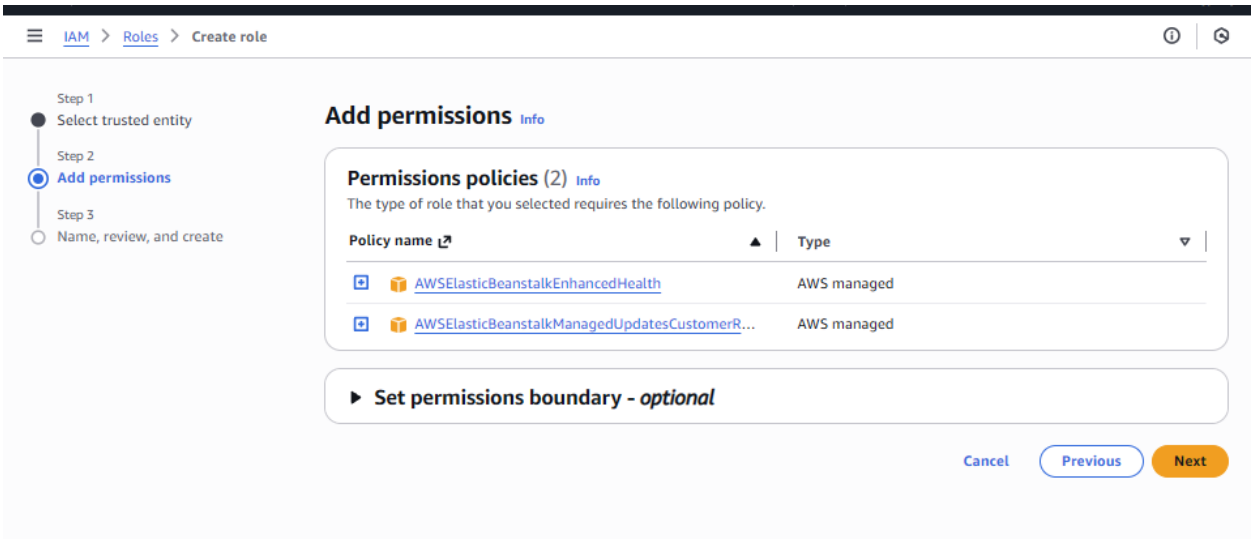


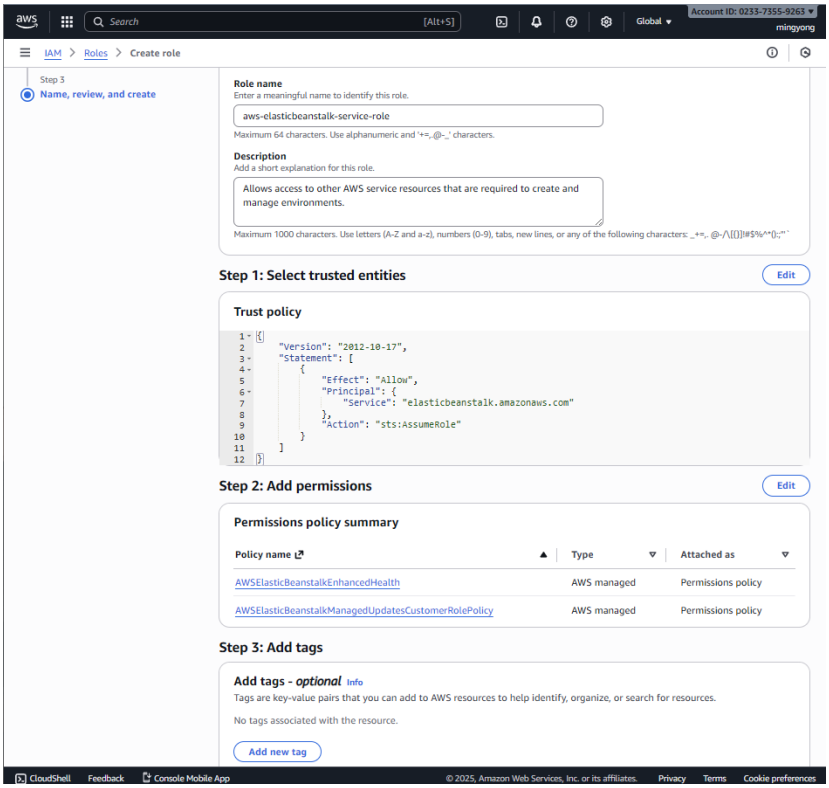


Ming Yong Tan 21920794

Create IAM role for application and envoironmet

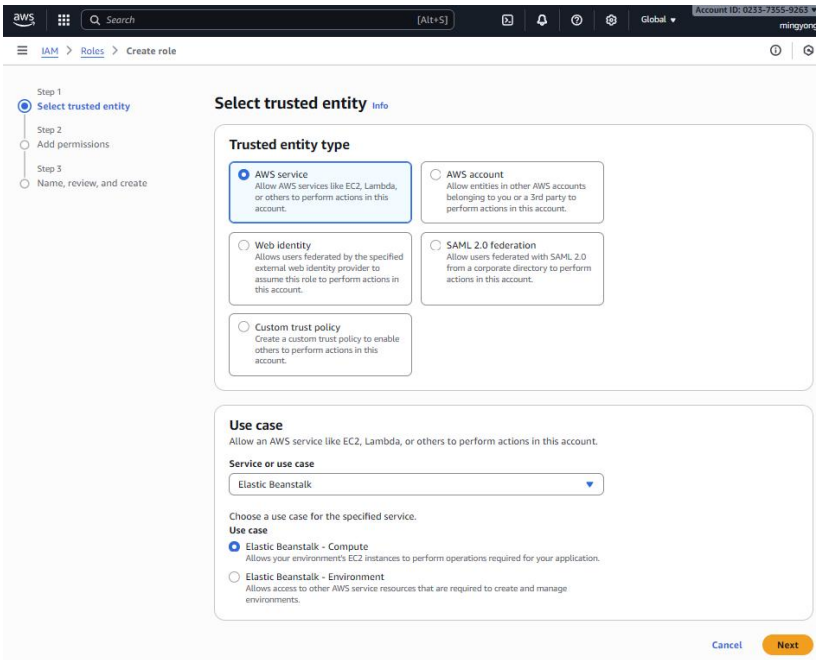


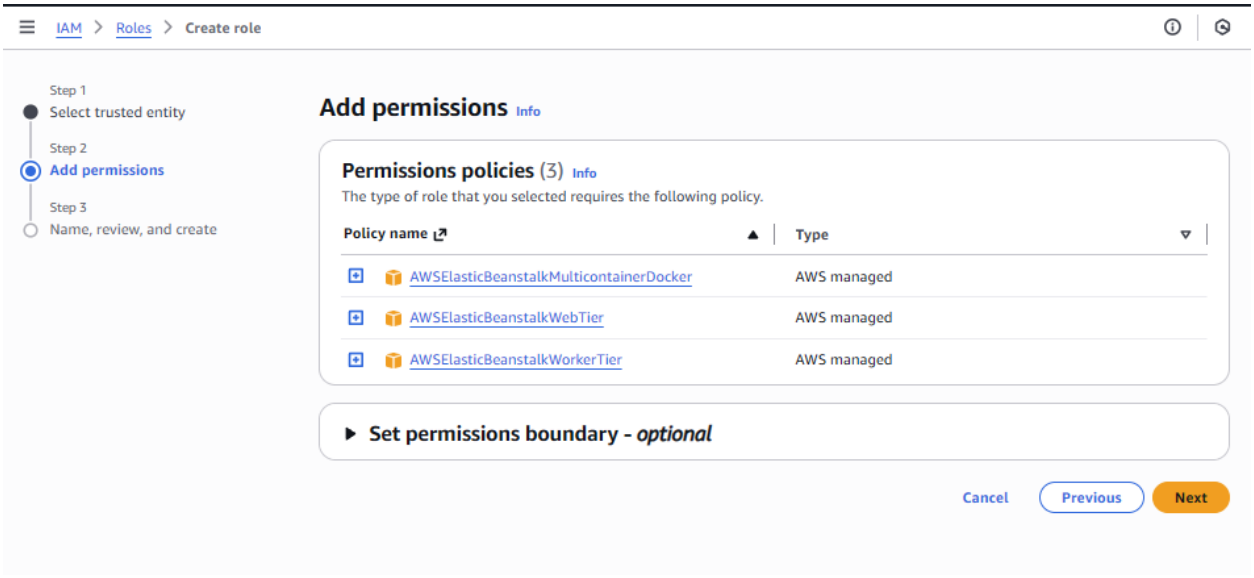


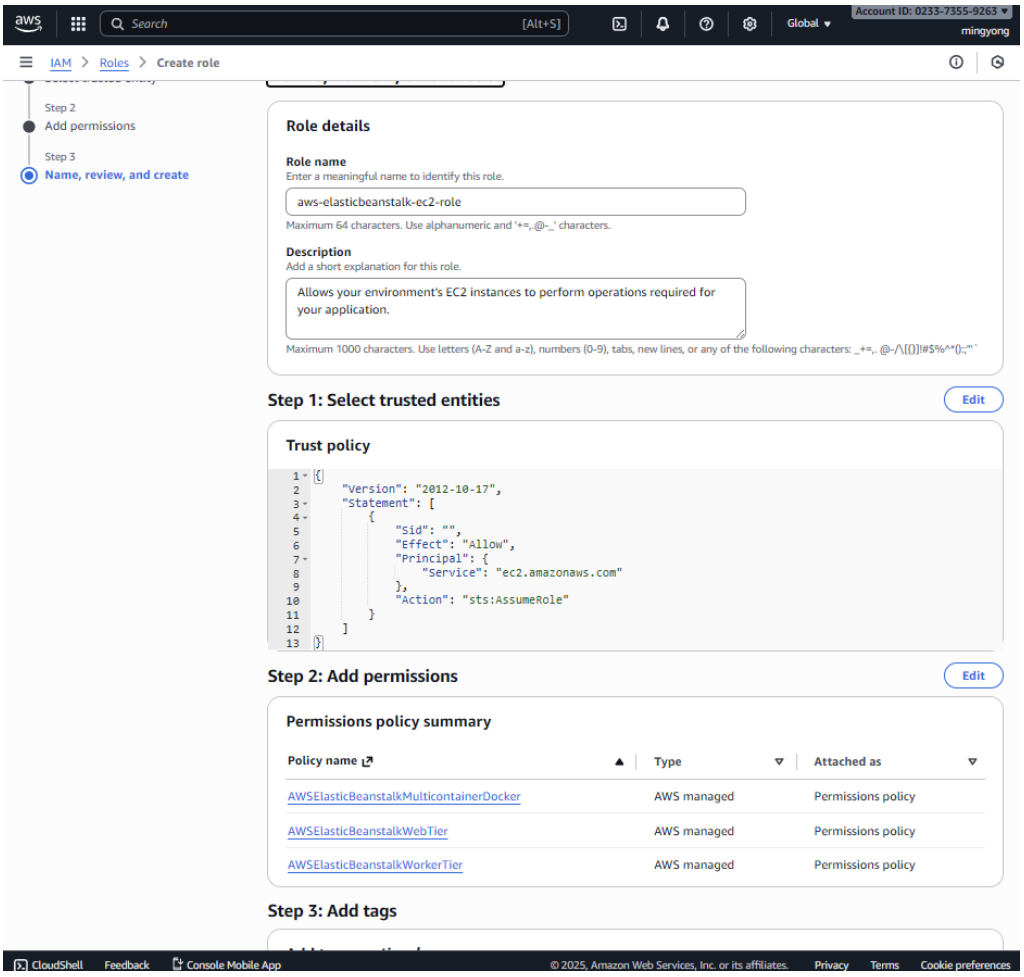


Create EC2 instance profile

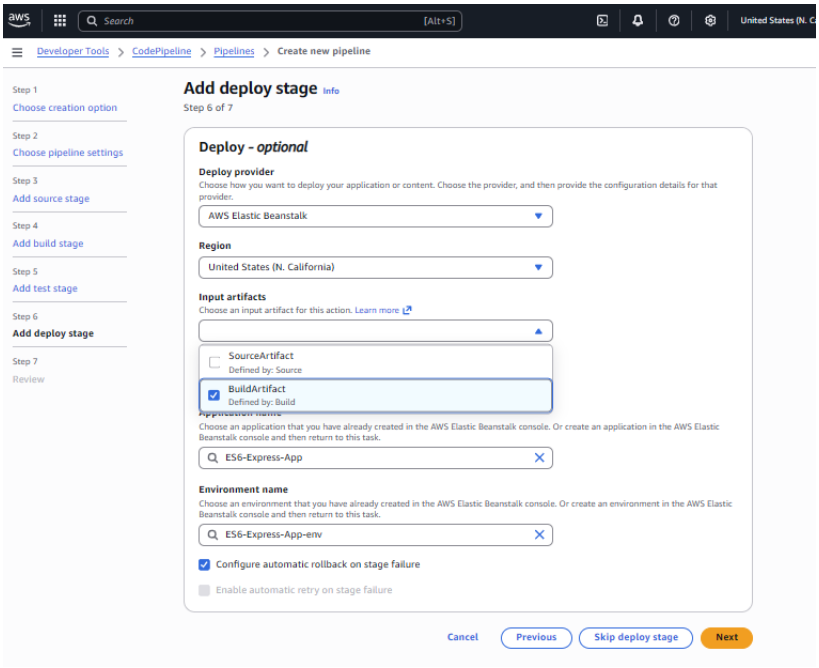
Ming Yong Tan 21920794







Deploy stage

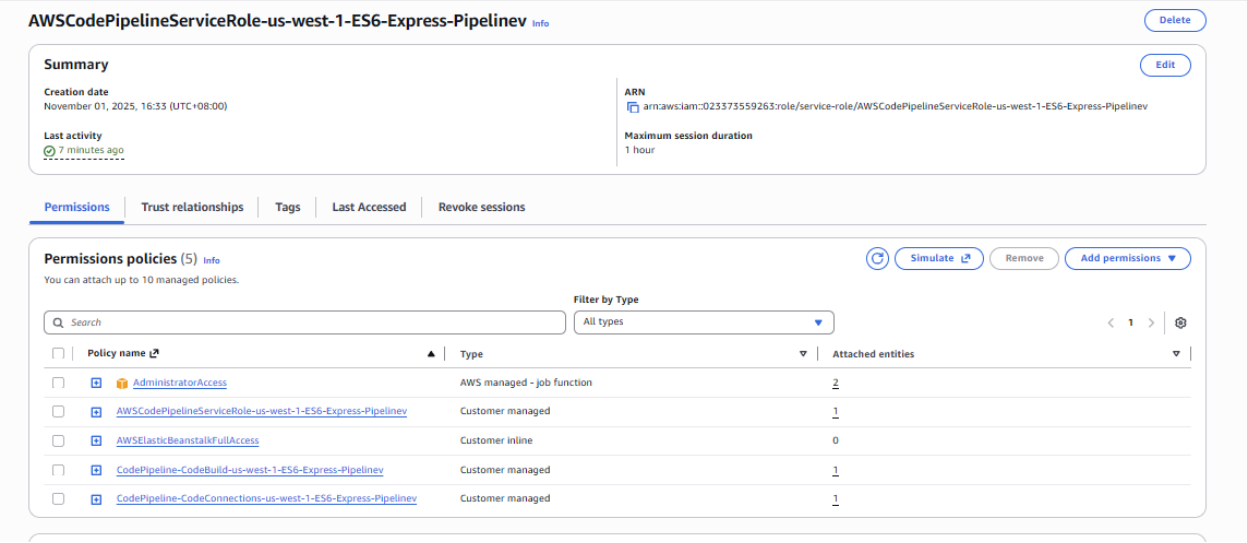


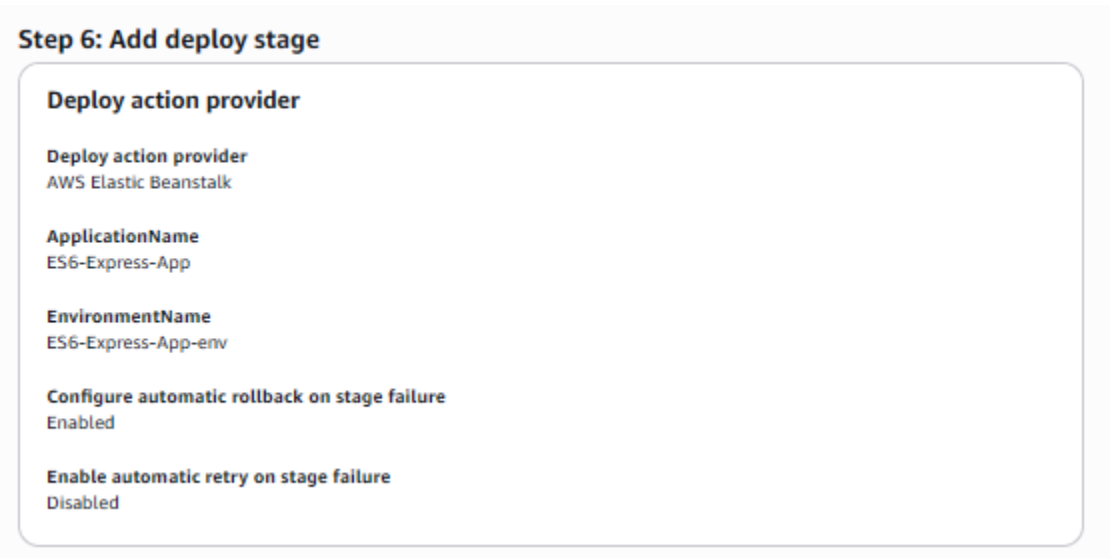
IAM Fix:

- Attached AWSElasticBeanstalkFullAccess to AWSCodePipelineServiceRole-us-west-1-ES6-Express-Pipelinev

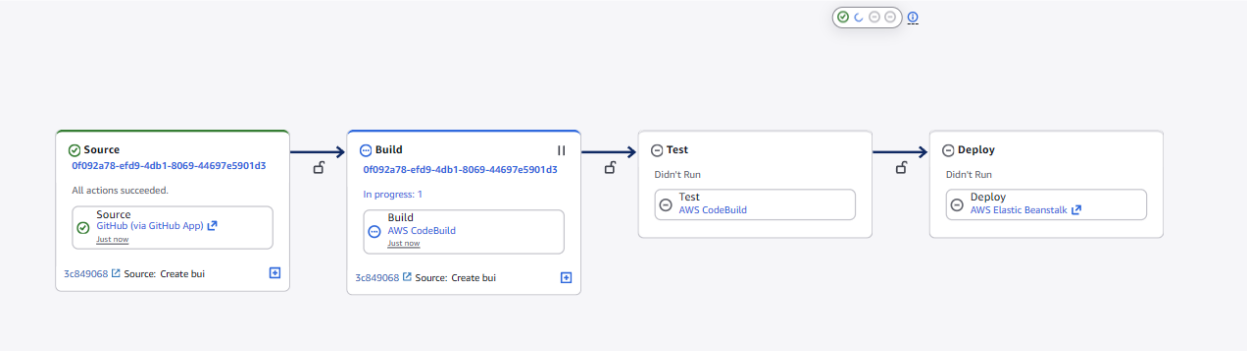
```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "elasticbeanstalk:*",
    "ec2:Describe*",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:CreateSecurityGroup",
    "ec2:DeleteSecurityGroup",
    "autoscaling:Describe*",
    "autoscaling:UpdateAutoScalingGroup",
    "autoscaling:SuspendProcesses",
    "autoscaling:ResumeProcesses",
    "cloudformation:*",
    "s3:PutObject",
    "s3:GetObject",
    "s3:ListBucket",
    "logs:DescribeLogGroups",
    "logs:CreateLogGroup",
    "logs:PutRetentionPolicy"
```

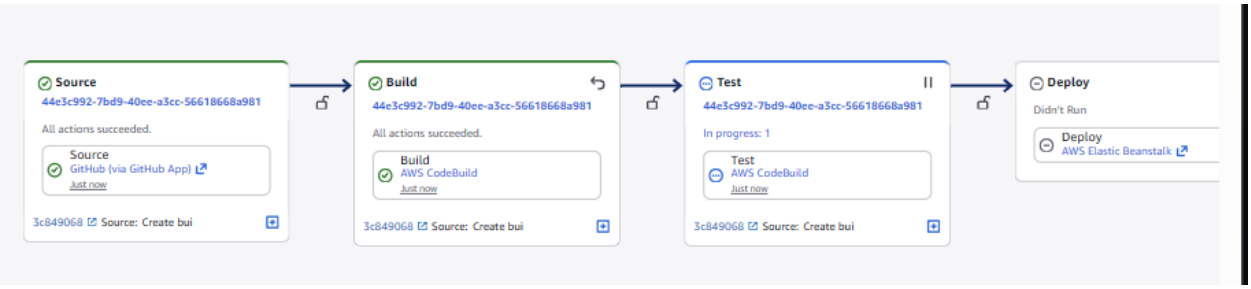
```
    ],
    "Resource": "*"
   },
   {
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": "elasticbeanstalk.amazonaws.com"
     }
    }
   }
  ]
}
```

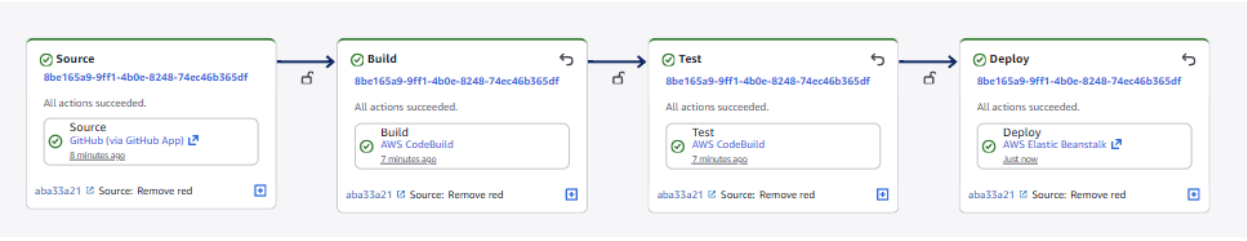


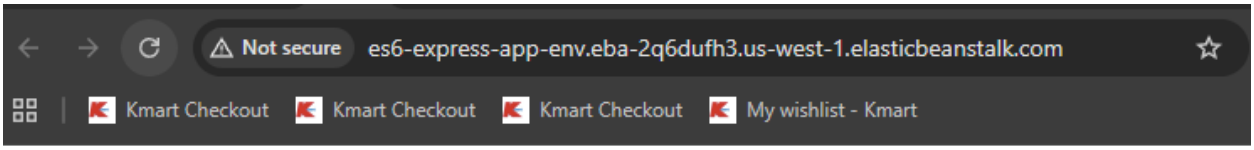


1. Put evidence in report that AWS Beanstalk application is successfully deployed and verify application reachable



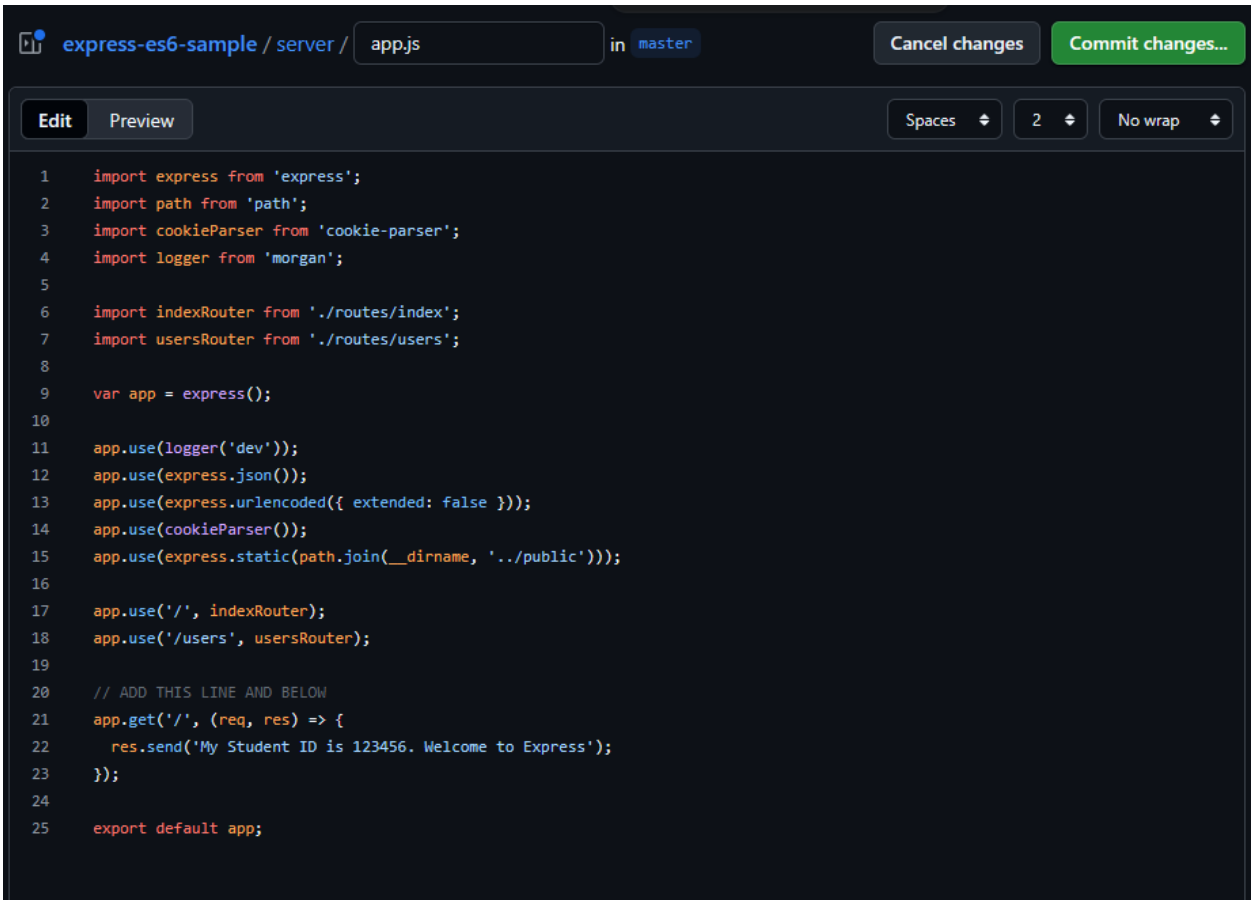




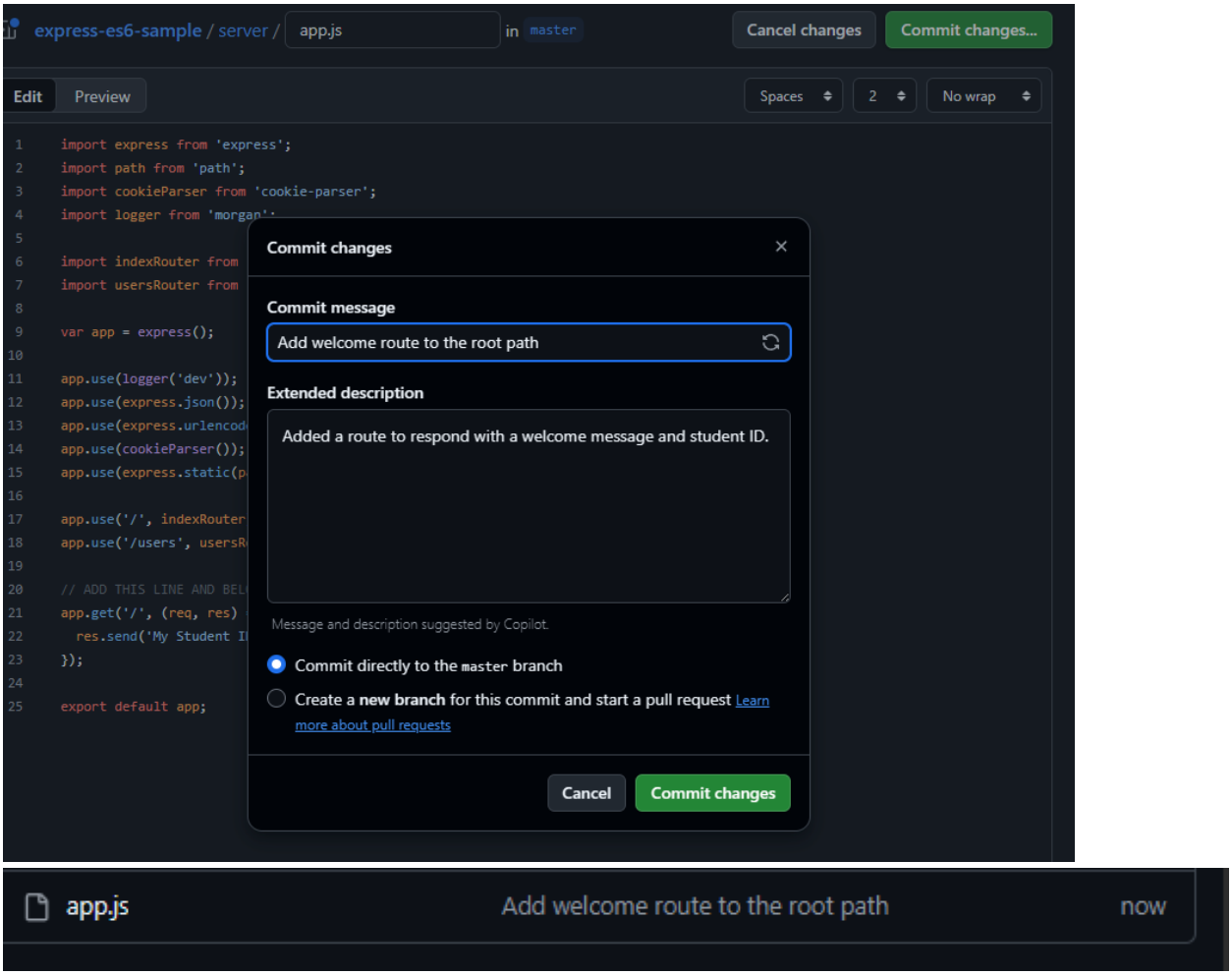


2. Modify the Application Code

a. Modify the source code so that the text reads `My Student ID is xxxxxx. Welcome to Express` (replace the xxxxxx with your student Id). (Screenshot must be in the report).

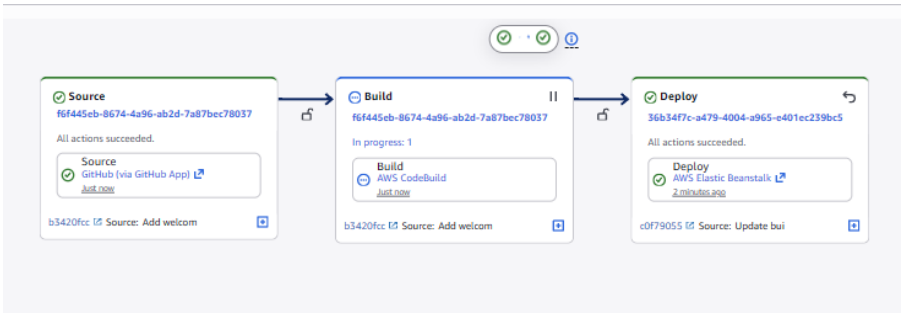


b. Push the code change to the forked repository.



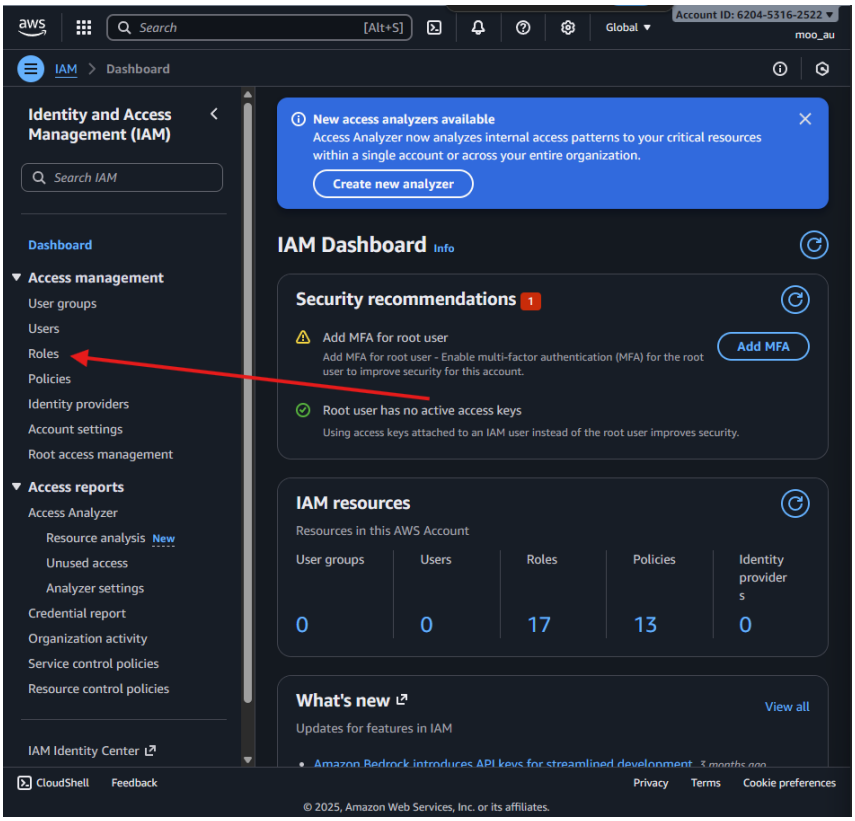
c. The pipeline should automatically detect the change, build, and deploy the updated application to AWS Beanstalk. (Check whether the automatic updating of the change is taking place or not).

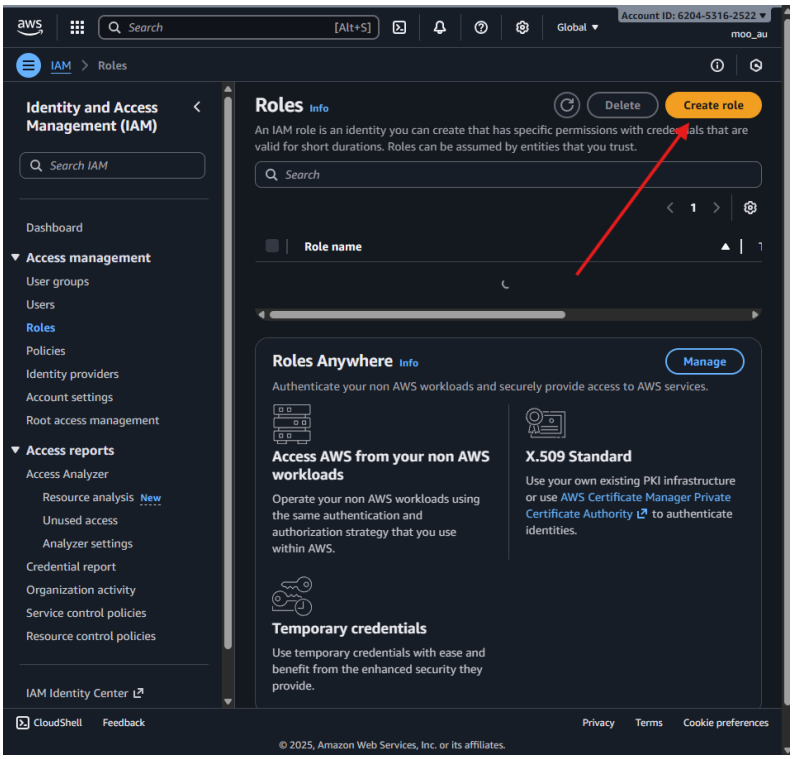
Auto update.



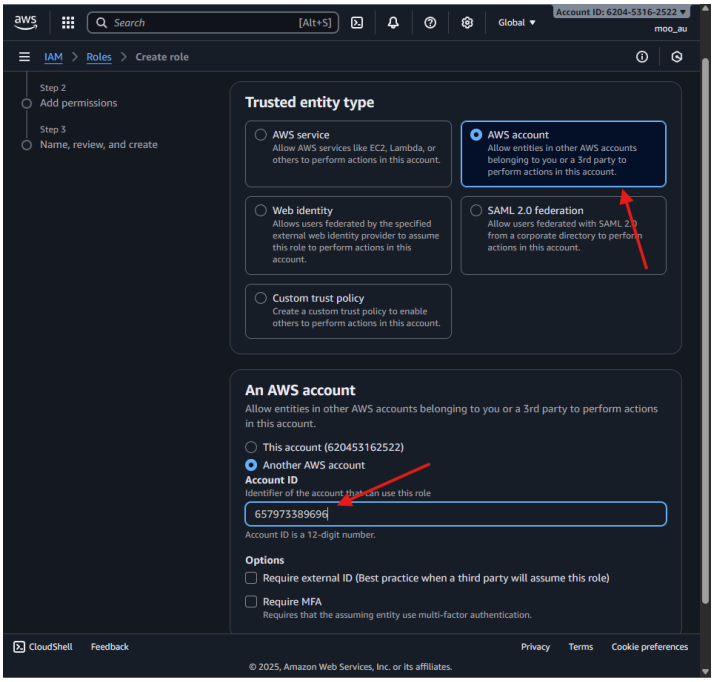
3. Create a Cross-Account IAM Role:

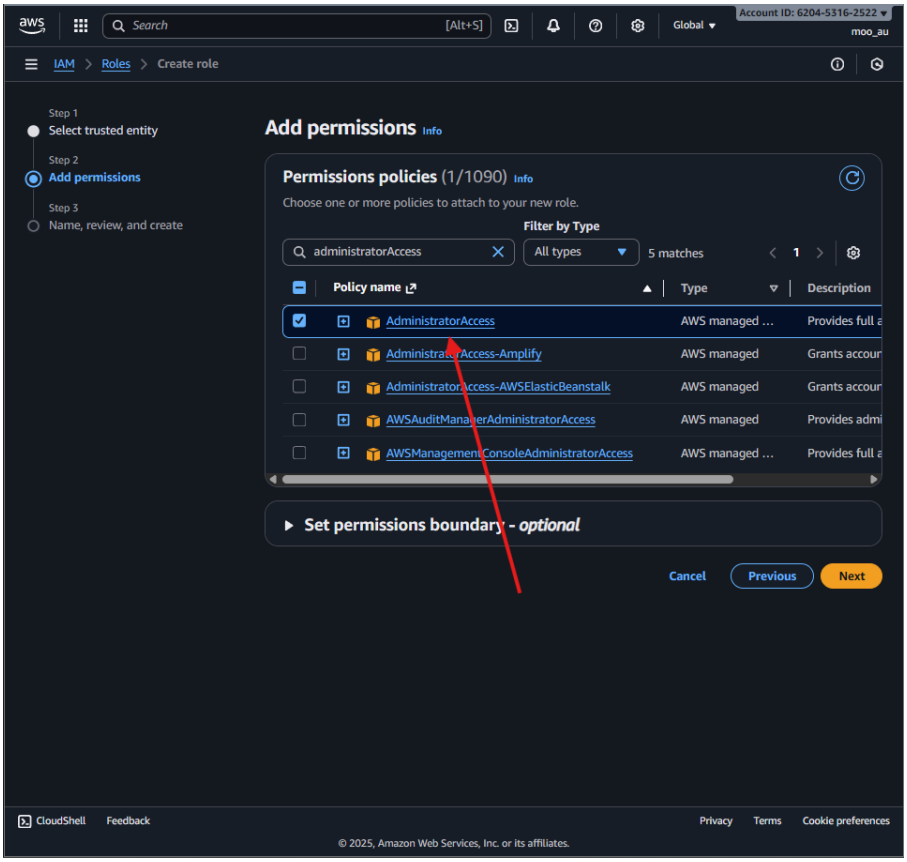
Ming Yong Tan 21920794

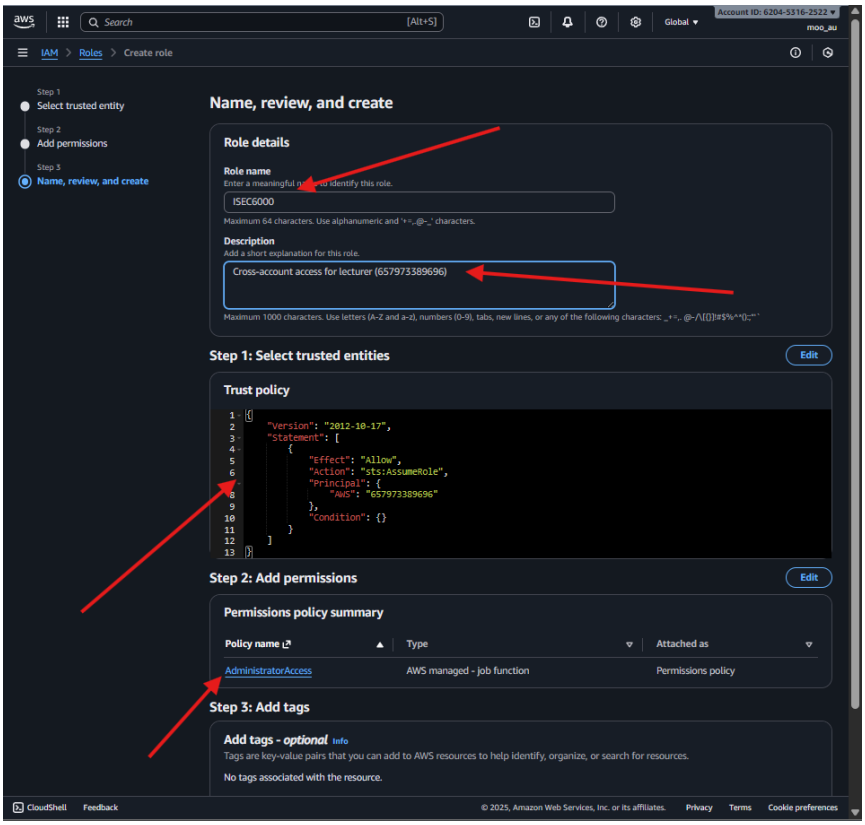




Ming Yong Tan 21920794







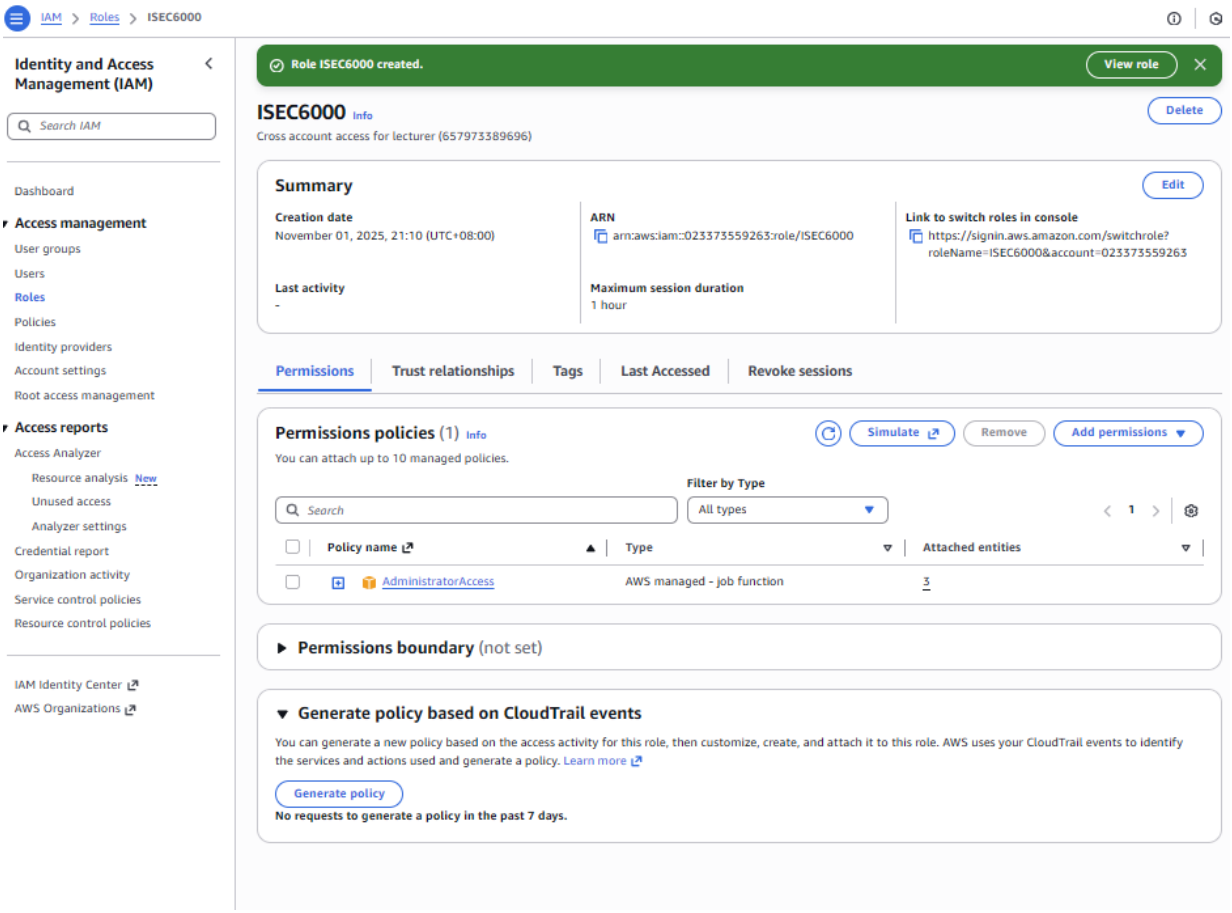
Permissions:

- AdministratorAccess (full access for review)

Security Controls:

- Access restricted to **one specific AWS account**
- Temporary credentials via sts:AssumeRole
- Role can be deleted after review

Ming Yong Tan 21920794

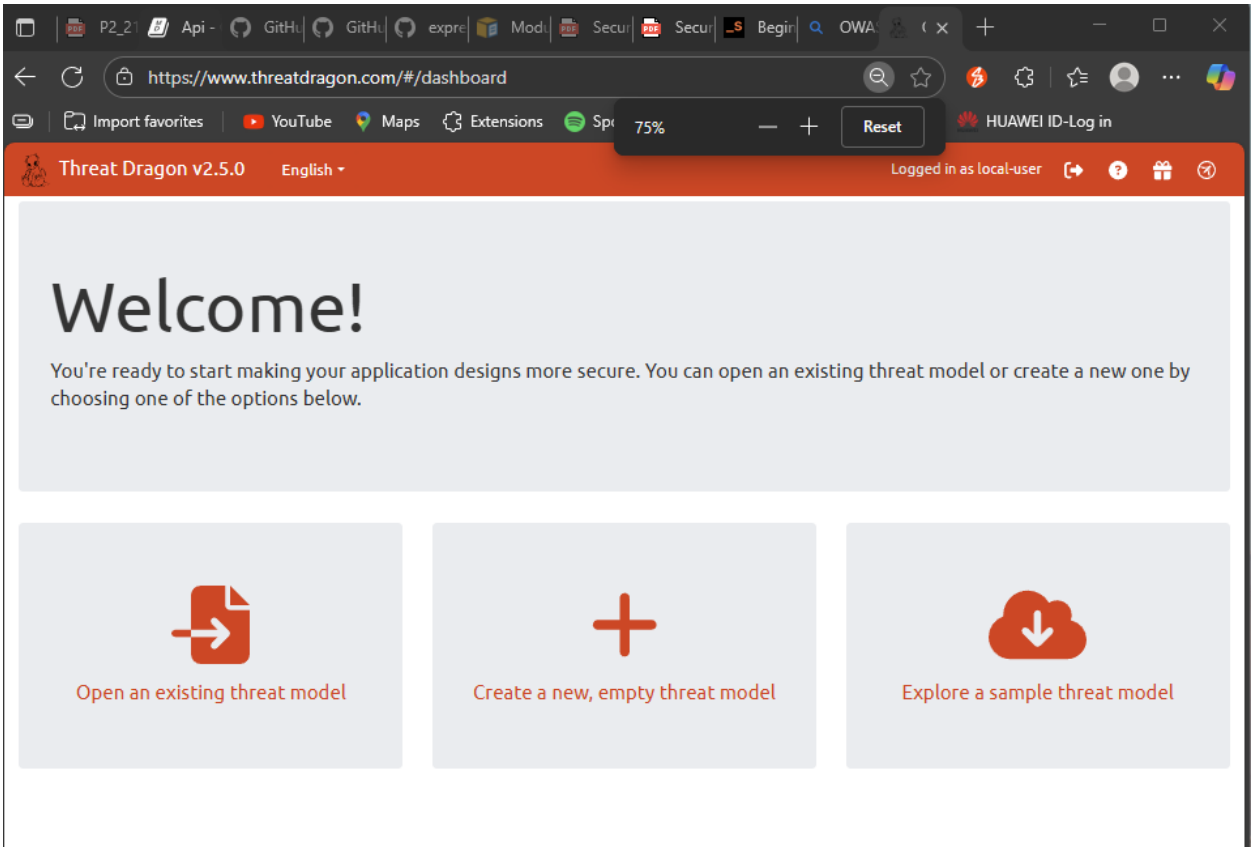


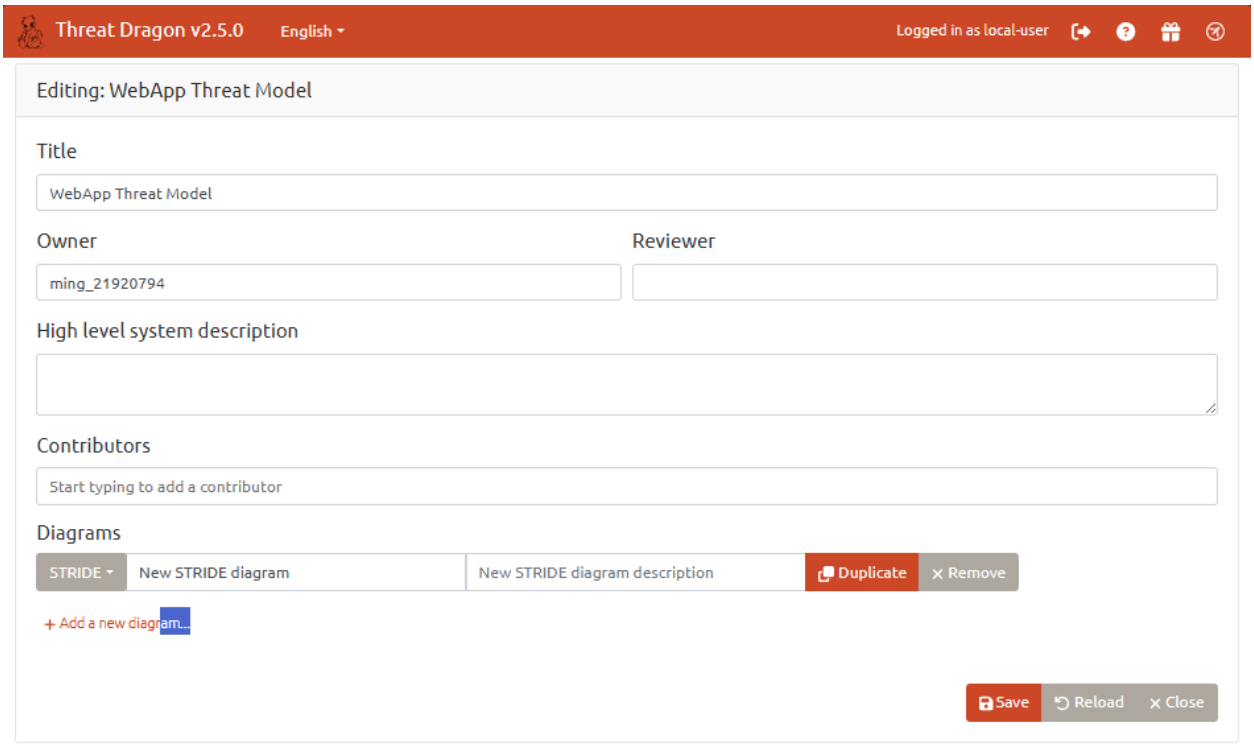
Ming Yong Tan 21920794

Task 6: Threat Modelling using STRIDE

1. Create a New Model:

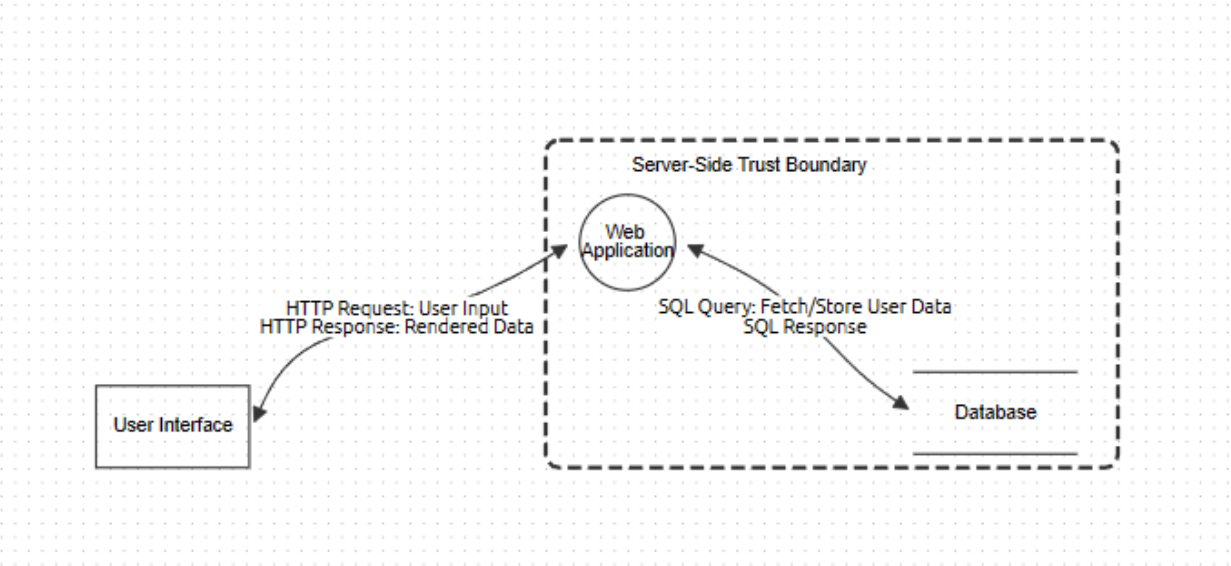
[OWASP Threat Dragon]



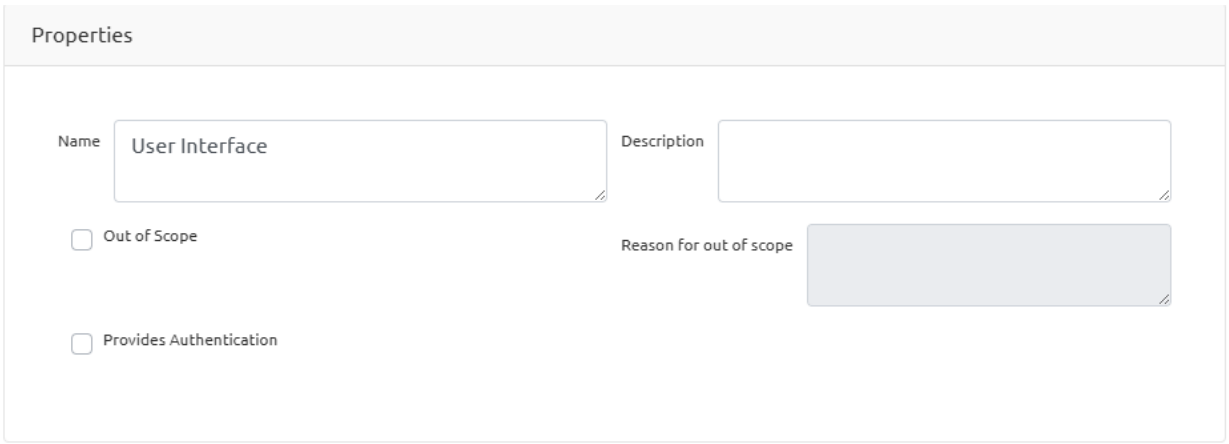


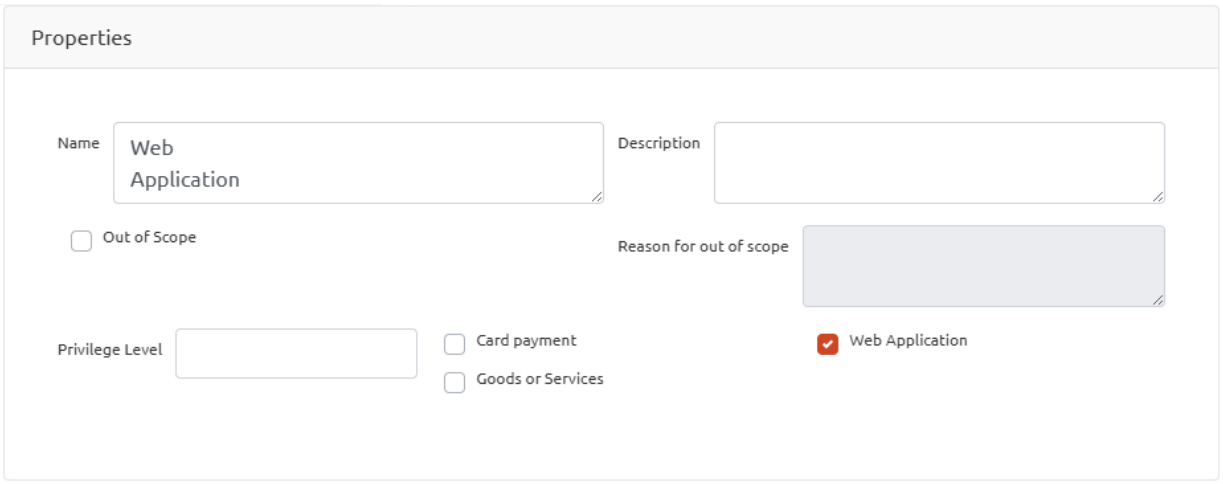
Click save and go back to the main page.

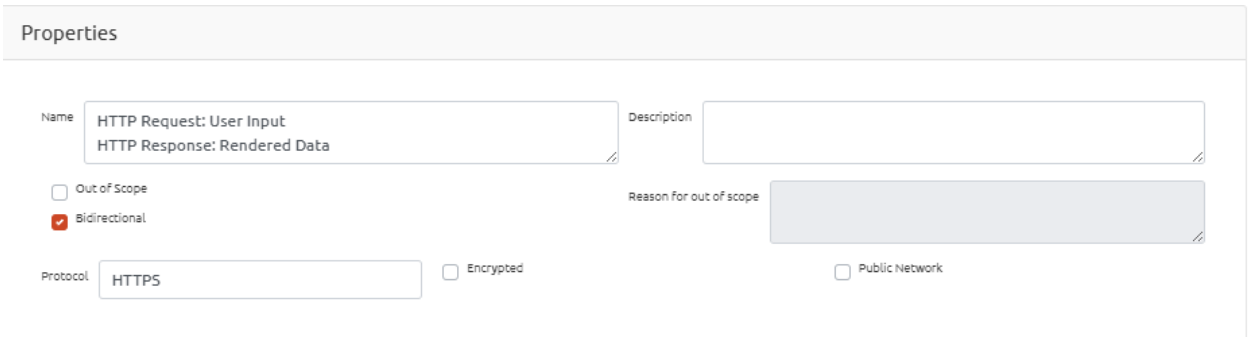
2. Map the System Components:

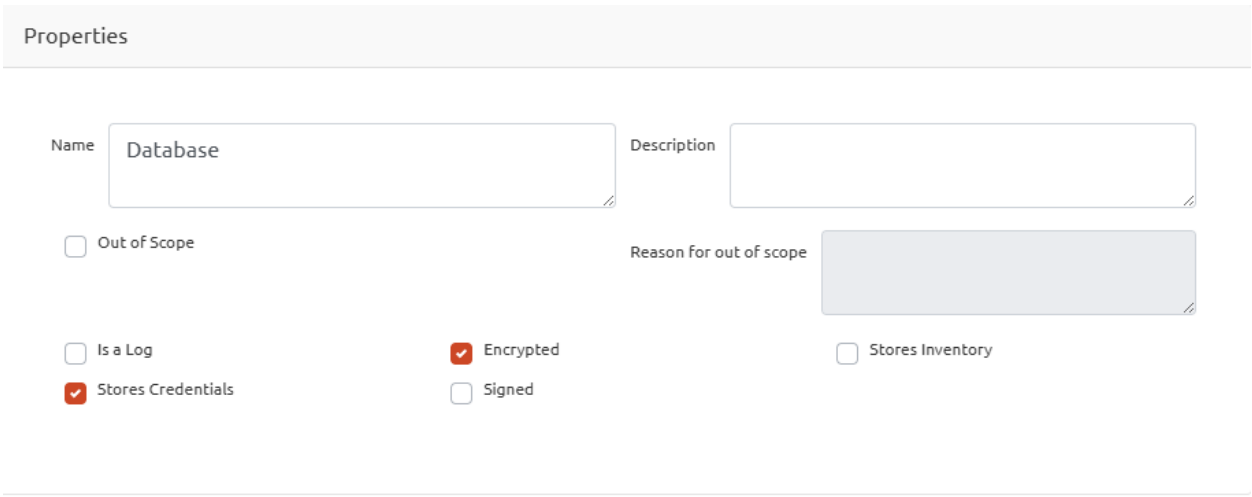


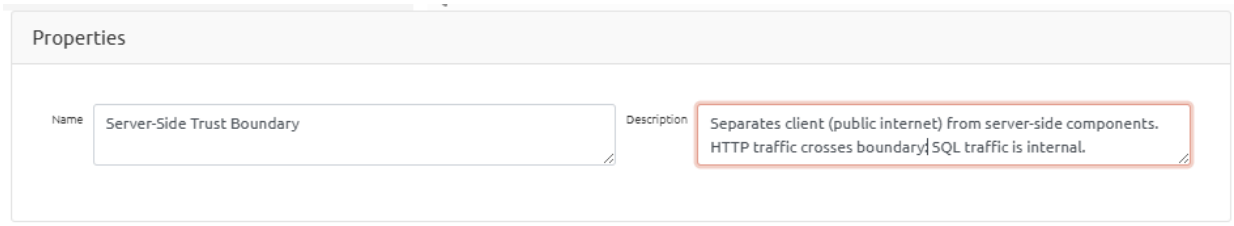
Ming Yong Tan 21920794











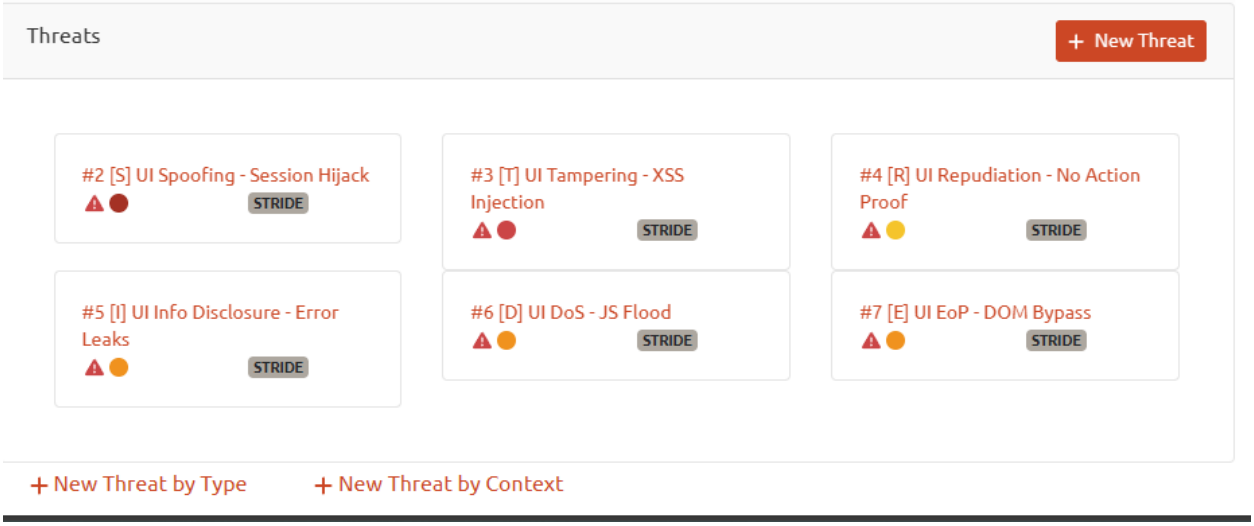
3. Identify Threats Using STRIDE:

User Interface (Actor)

Properties:

Number	Title	Type	Severity	Status	Score	Description
2	[S] UI Spoofing - Session Hijack		Critical	Open		Attacker steals cookies to impersonate user.
3	[T] UI Tampering - XSS Injection		High	Open		Malicious script alters form input.
4	[R] UI Repudiation - No Action Proof		Low	Open		User denies submitting data.
5	[I] UI Info Disclosure - Error Leaks		Medium	Open		Verbose errors expose system info.
6	[D] UI DoS - JS Flood		Medium	Open		Malformed input freezes browser.
7	[E] UI EoP - DOM Bypass		Medium	Open		Client-side logic trusts manipulated DOM.

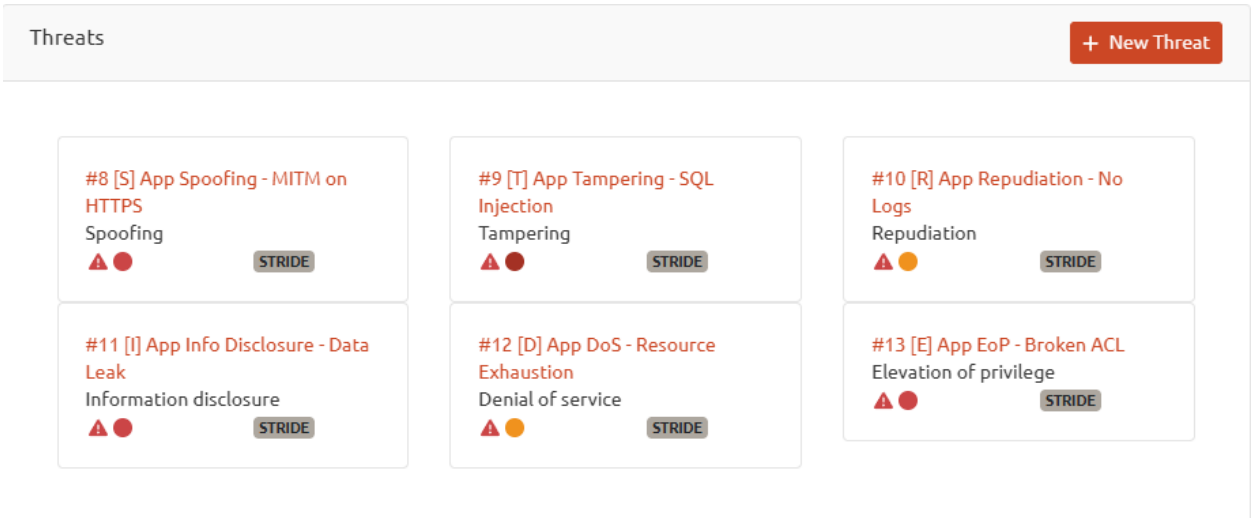
Ming Yong Tan 21920794



Web Application (Process)

Properties: Web Application

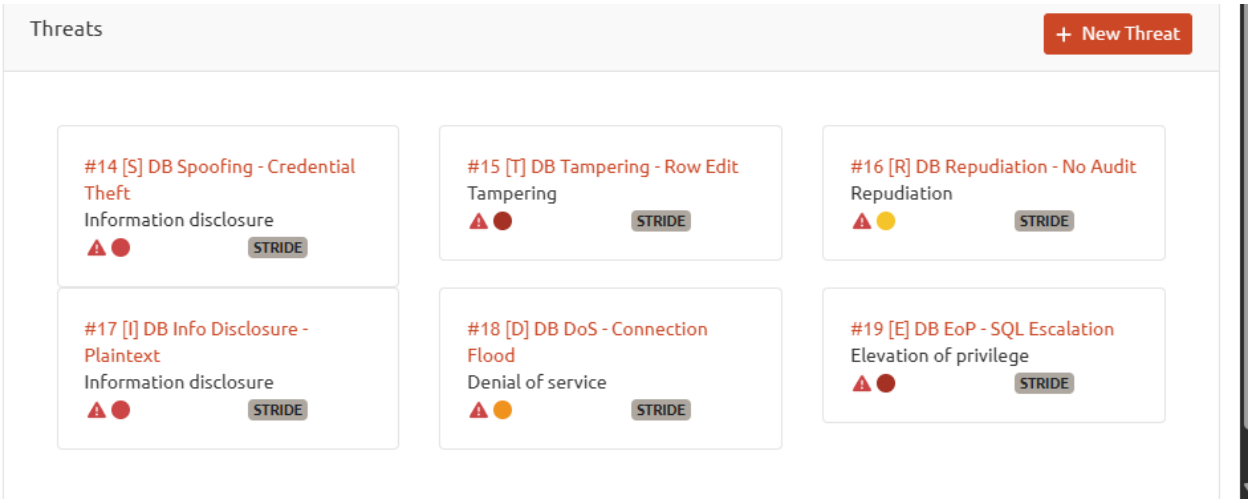
Number	Title	Type	Severity	Status	Score	Description
8	[S] App Spoofing - MITM on HTTPS	Spoofing	High	Open		Intercepts traffic over public network.
9	[T] App Tampering - SQL Injection	Tampering	Critical	Open		Input modifies DB queries.
10	[R] App Repudiation - No Logs	Repudiation	Medium	Open		Actions not traceable.
11	[I] App Info Disclosure - Data Leak	Information disclosure	High	Open		PII sent unencrypted.
12	[D] App DoS - Resource Exhaustion	Denial of service	Medium	Open		High load crashes server.
13	[E] App EoP - Broken ACL	Elevation of privilege	High	Open		Unauthorized endpoint access.



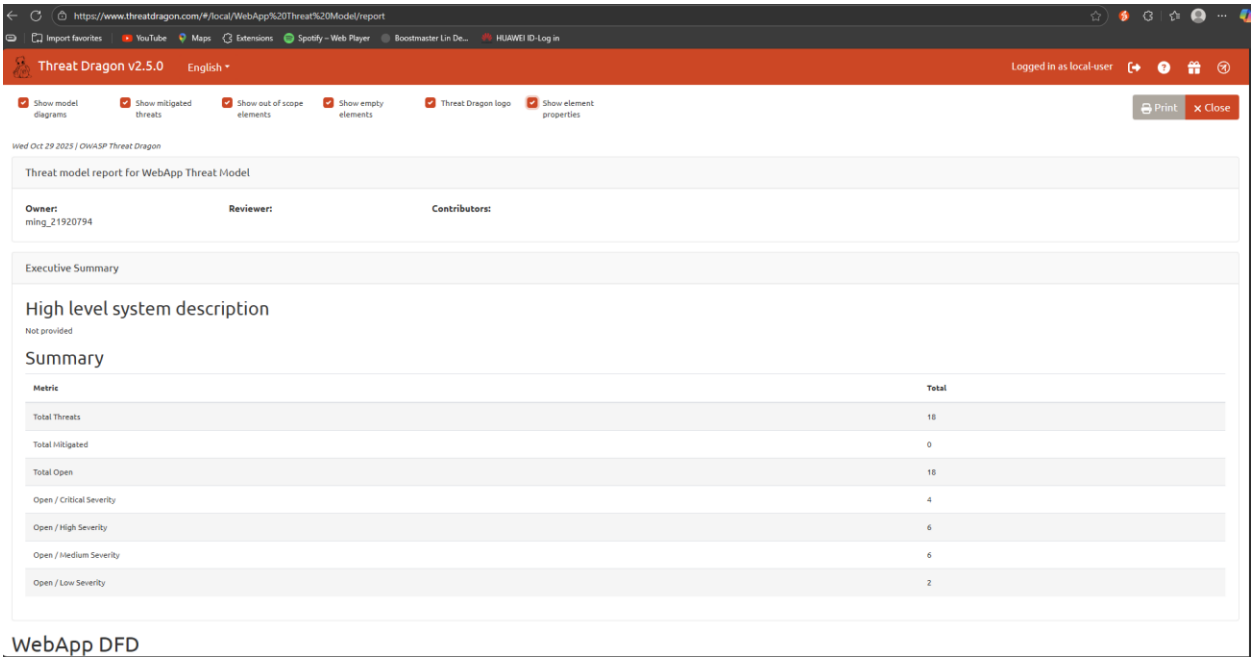
Database (Store)

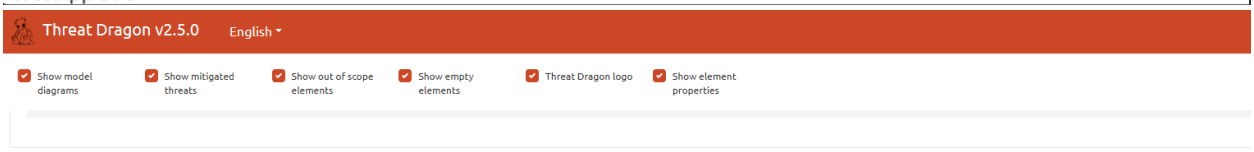
Properties: Encrypted, Stores Credentials

Number	Title	Type	Severity	Status	Score	Description
14	[S] DB Spoofing - Credential Theft	Information disclosure	High	Open		Stolen DB login.
15	[T] DB Tampering - Row Edit	Tampering	Critical	Open		Direct data change.
16	[R] DB Repudiation - No Audit	Repudiation	Low	Open		No change trail.
17	[I] DB Info Disclosure - Plaintext	Information disclosure	High	Open		Data at rest exposed.
18	[D] DB DoS - Connection Flood	Denial of service	Medium	Open		Too many connections.
19	[E] DB EoP - SQL Escalation	Elevation of privilege	Critical	Open		Read → admin via injection.



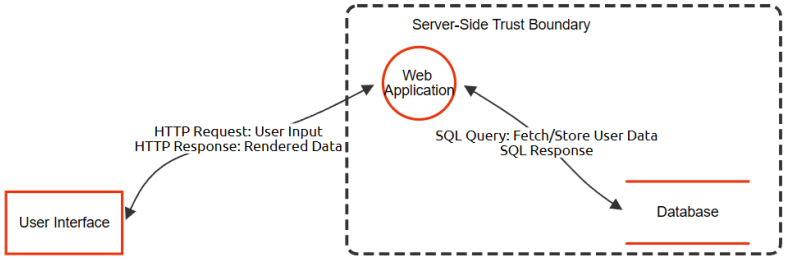
4. Document and Mitigate Threats:





WebApp DFD

21920794



Ming Yong Tan 21920794