Secure DevOps – Project 3 Final Report (ISEC6000)

Student Name: Vrushtiben Patel
Student ID: 22167521
Course: Master of Computing (Computer Science)
GitHub Repository: https://github.com/Vrushti54/SecureDevOps-Assignment3-22167521

Table of Contents

1 Docker Setup & Validation

```
Setting up containerd.io (1.7.28-0~ubuntu.22.04~jammy) ...
Created symlink /etc/systemd/system/multi-user.target.wants/containerd.s
ervice → /lib/systemd/system/containerd.service.
Setting up docker-compose-plugin (2.40.0-1~ubuntu.22.04~jammy) ...
Setting up docker-ce-cli (5:28.5.1-1~ubuntu.22.04~jammy) ...
Setting up libslirp0:amd64 (4.6.1-1build1) ...
Setting up pigz (2.6-1) ...
Setting up docker-ce-rootless-extras (5:28.5.1-1~ubuntu.22.04~jammy) ...
Setting up slirp4netns (1.0.1-2) ...
Setting up docker-ce (5:28.5.1-1~ubuntu.22.04~jammy) ...
Created symlink /etc/systemd/system/multi-user.target.wants/docker.servi
ce → /lib/systemd/system/docker.service.
Created symlink /etc/systemd/system/sockets.target.wants/docker.socket →
 /lib/systemd/system/docker.socket.
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.11) ...
Synchronizing state of docker.service with SysV service script with /lib
/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable docker
Docker version 28.5.1, build e180ab8
Docker Compose version v2.40.0
root@VrushtiHP:~#
```

```
   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

This message is shown once a day. To disable it please create the
/home/a3test/.hushlogin file.
a3test@VrushtiHP:~$ sudo docker ps
[sudo] password for a3test:
a3test is not in the sudoers file.  This incident will be reported.
a3test@VrushtiHP:~$ sudo docker ps
[sudo] password for a3test:
Sorry, try again.
[sudo] password for a3test:
Sorry, try again.
[sudo] password for a3test:
```

```
root@VrushtiHP:~# sudo docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES
root@VrushtiHP:~#
```

Figures 1–3 – Docker validated with appropriate privileges.

Objective:

Verify secure Docker installation, confirm permission control, and ensure container execution requires administrative rights.

Analysis:

Running `docker ps` without `sudo` produced a permission error, confirming restricted daemon access. Executing with `sudo` listed running containers, proving privilege-based enforcement.

Reflection:

Restricting Docker access to sudo users implements least-privilege and prevents non-root users from executing arbitrary containers that could escalate privileges.

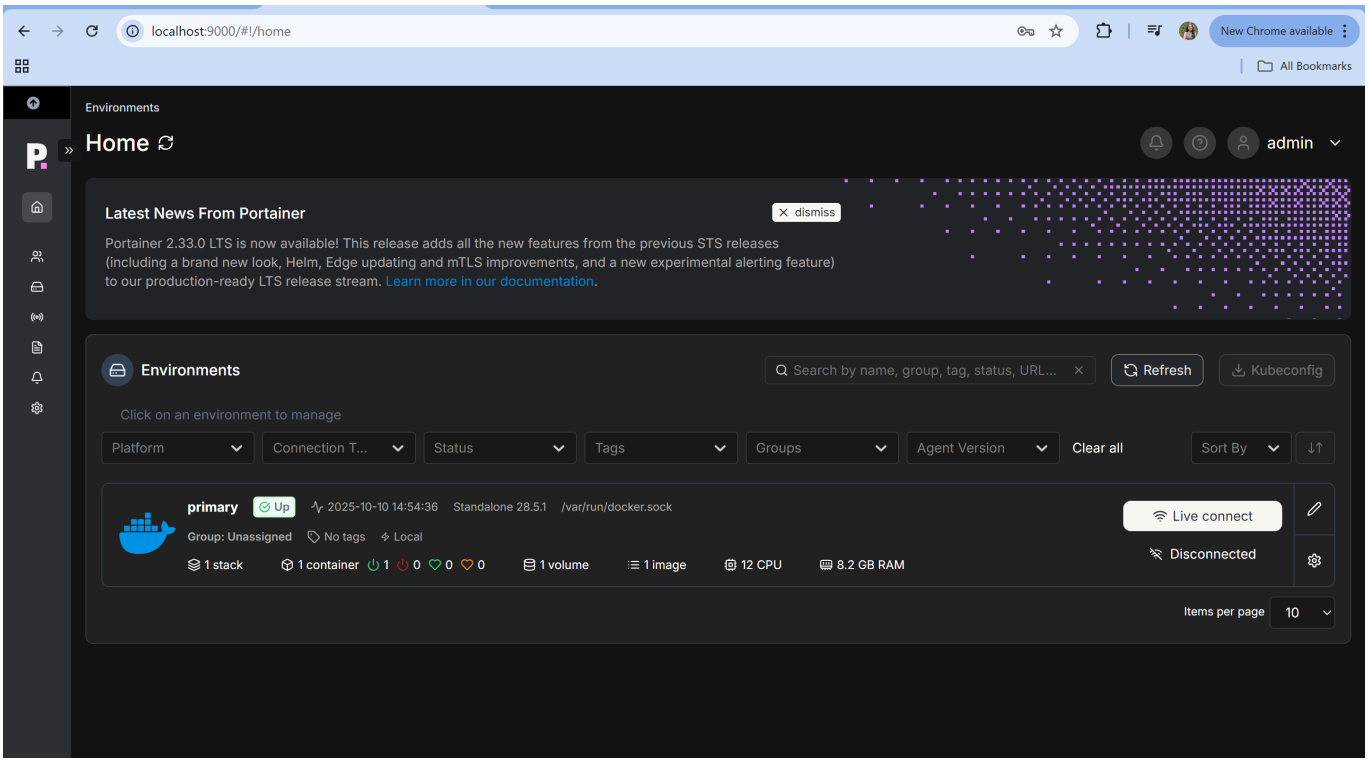
---

2 Portainer Deployment & Log Analysis

```
root@VrushtiHP:/mnt/c/assignment3_SDO/portainer# ls
README.md  compose.yaml  portainer.zip
root@VrushtiHP:/mnt/c/assignment3_SDO/portainer# cat compose.yaml | grep
 restart
    restart: always
root@VrushtiHP:/mnt/c/assignment3_SDO/portainer#
```

```
root@VrushtiHP:/mnt/c/assignment3_SDO/portainer# # bring the stack up in
 detached mode
sudo docker compose -f compose.yaml up -d

# check that it started
sudo docker compose -f compose.yaml ps

# confirm container details and exposed port
sudo docker ps --format "table {{.Names}}\t{{.Image}}\t{{.Status}}\t{{.P
orts}}"
[+] Running 0/1
 ⠋ portainer Pulling                                                0.0s
```

```
root@VrushtiHP:/mnt/c/assignment3_SDO/portainer#
root@VrushtiHP:/mnt/c/assignment3_SDO/portainer# sudo docker compose up
-d
sudo docker ps
[+] Running 1/1
 ✔Container portainer  Running                                    0.0s
CONTAINER ID   IMAGE                                COMMAND
  CREATED       STATUS                              PORTS

     NAMES
32c964758f77   quay.io/projectquay/clair:4.7.4   "/bin/clair -conf /c…"
  6 hours ago   Up 6 hours                       0.0.0.0:6063->6063/tcp,
[::]:6063->6063/tcp, 6060/tcp, 0.0.0.0:8089->8089/tcp, [::]:8089->8089/t
cp   clair
e5be01b96869   postgres:13                          "docker-entrypoint.s…"
  6 hours ago   Up 6 hours (healthy)               5432/tcp

     clair-database
7e17c76ea788   quay.io/projectquay/golang:1.24   "go run . -conf /etc…"
  2 weeks ago   Restarting (1) 17 seconds ago

     clair-indexer
14c1321b6768   quay.io/projectquay/golang:1.24   "go run . -conf /etc…"
  2 weeks ago   Restarting (1) 17 seconds ago

     clair-matcher
d3f76a587584   nextcloud:apache                     "/entrypoint.sh apac…"
  2 weeks ago   Up 7 hours                         0.0.0.0:80->80/tcp, [::]
:80->80/tcp
     nextcloud-nc-1
cfcf56405b93   postgres:alpine                      "docker-entrypoint.s…"
  2 weeks ago   Up 7 hours                         5432/tcp

     nextcloud-db-1
8e678072a3fe   portainer/portainer-ce:alpine     "/portainer -H unix:…"
  2 weeks ago   Up 7 hours                         8000/tcp, 9443/tcp, 0.0.
0.0:9000->9000/tcp, [::]:9000->9000/tcp
     portainer
root@VrushtiHP:/mnt/c/assignment3_SDO/portainer#
```




```
root@VrushtiHP:/mnt/c/assignment3_SDO/portainer# sudo docker compose -f
compose.yaml logs --tail 3
sudo docker compose -f compose.yaml logs portainer | tail -n 50
portainer  | 2025/10/10 06:53AM INF github.com/portainer/portainer/api/c
md/portainer/main.go:636 > starting Portainer | build_number=232 go_vers
ion=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  | 2025/10/10 06:53AM INF github.com/portainer/portainer/api/h
ttp/server.go:367 > starting HTTPS server | bind_address=:9443
portainer  | 2025/10/10 06:53AM INF github.com/portainer/portainer/api/h
ttp/server.go:351 > starting HTTP server | bind_address=:9000
portainer  | 2025/10/10 06:53AM INF github.com/portainer/portainer/api/c
md/portainer/main.go:325 > encryption key file not present | filename=/r
un/secrets/portainer
portainer  | 2025/10/10 06:53AM INF github.com/portainer/portainer/api/c
md/portainer/main.go:365 > proceeding without encryption key |
portainer  | 2025/10/10 06:53AM INF github.com/portainer/portainer/api/d
atabase/boltdb/db.go:137 > loading PortainerDB | filename=portainer.db
portainer  | 2025/10/10 06:53AM INF github.com/portainer/portainer/api/i
nternal/ssl/ssl.go:79 > no cert files found, generating self signed SSL
certificates |
portainer  | 2025/10/10 06:53AM INF github.com/portainer/portainer/api/c
hisel/service.go:228 > generated a new Chisel private key file | private
-key=/data/chisel/private-key.pem
portainer  | 2025/10/10 06:53:17 server: Reverse tunnelling enabled
portainer  | 2025/10/10 06:53:17 server: Fingerprint miTV/Leji0BK6xeONm2
IR9uPcj3QUEyS2SXm3D/bMOQ=
portainer  | 2025/10/10 06:53:17 server: Listening on http://0.0.0.0:800
0
portainer  | 2025/10/10 06:53AM INF github.com/portainer/portainer/api/c
md/portainer/main.go:636 > starting Portainer | build_number=232 go_vers
ion=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  | 2025/10/10 06:53AM INF github.com/portainer/portainer/api/h
```

Figures 4–8 – Portainer deployed and verified.

Objective:
Deploy Portainer for secure container management, verify operational health, and analyse logs for auditability.

Analysis:
The Compose file used `restart: always`, ensuring automatic recovery after failures.
Valid restart options include `no`, `always`, `on-failure`, and `unless-stopped`.
Running `sudo docker compose logs --tail 3` confirmed successful initialization with no error entries or unauthorized access attempts.

Reflection:
Portainer's GUI provided real-time visibility of container status and resource usage, improving resilience and administrative transparency for secure operations.

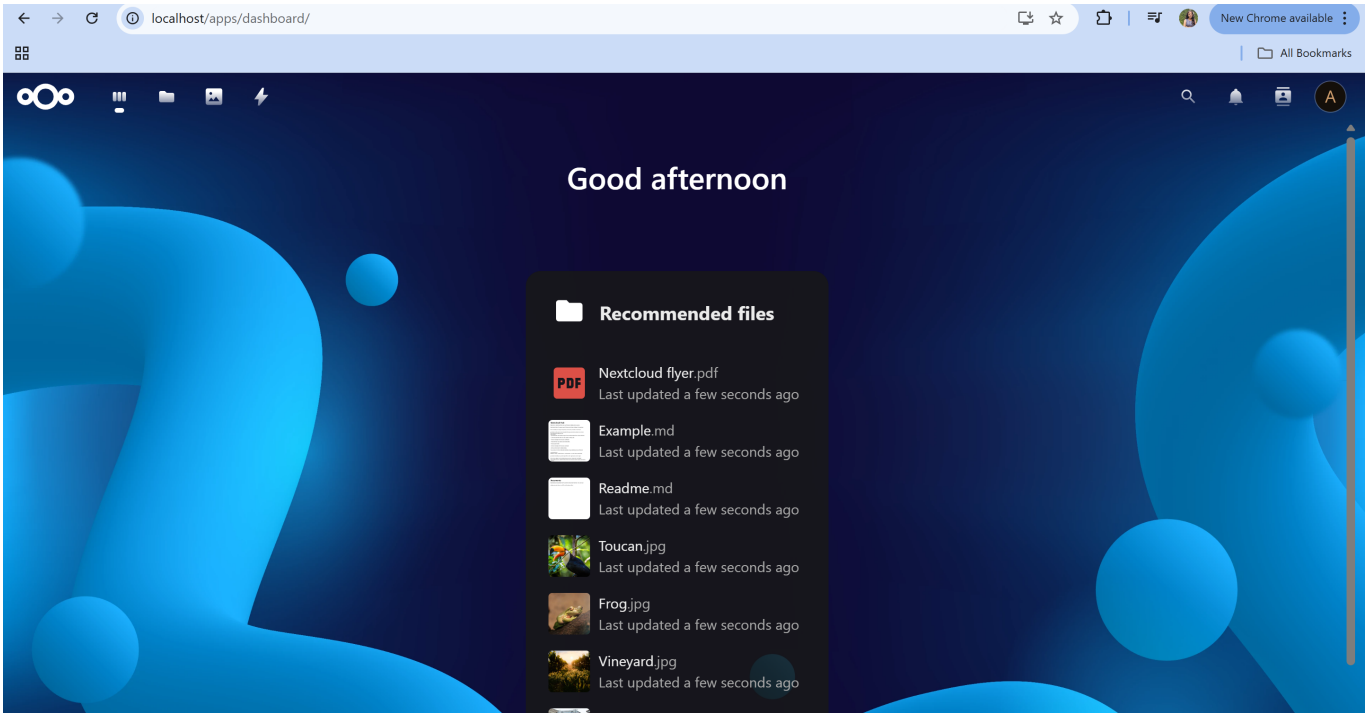
---

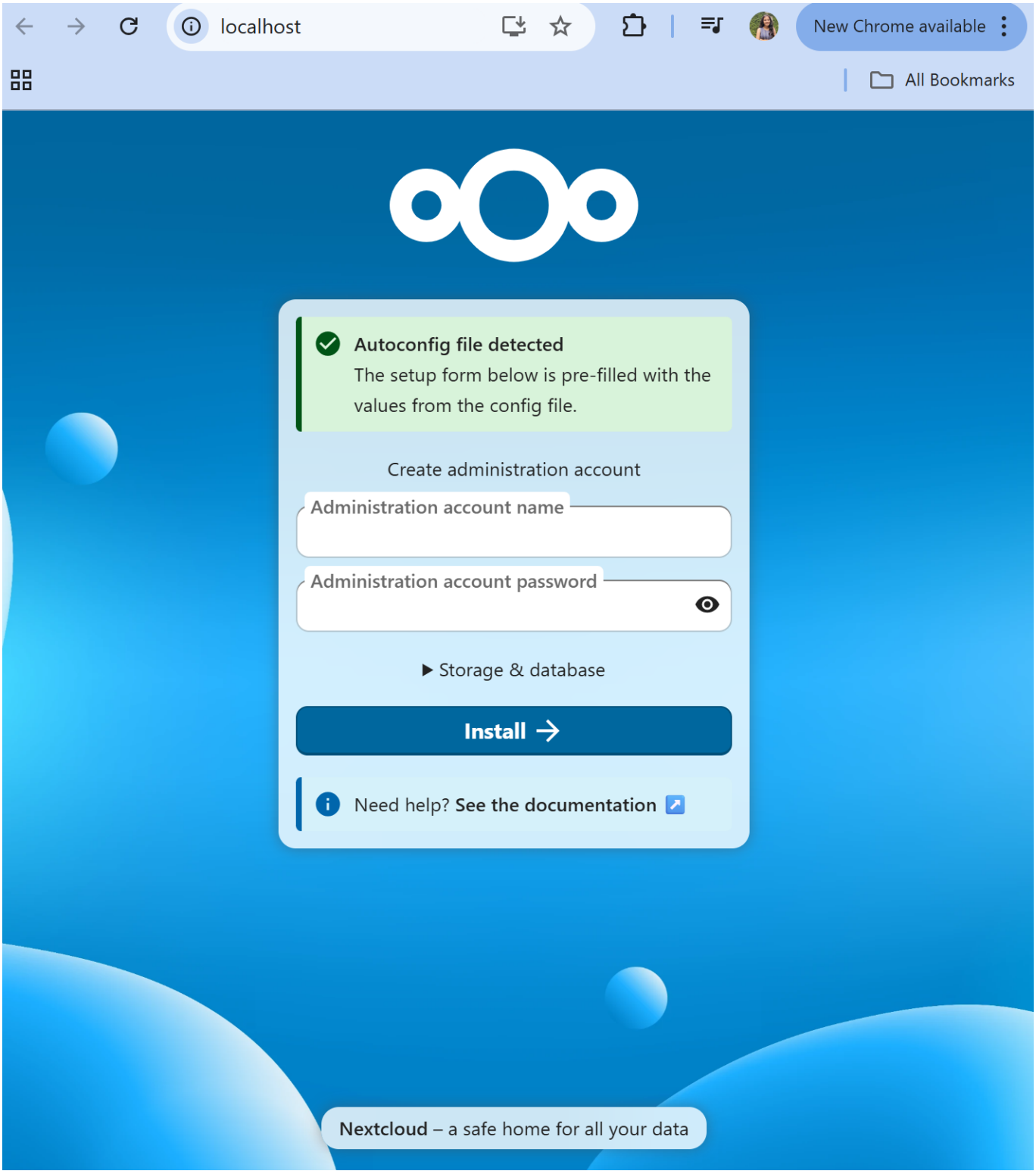
3 Nextcloud Multi-Container Setup

```
root@VrushtiHP:/mnt/c/assignment3_SDO/portainer# cd /mnt/c/assignment3_S
DO/nextcloud
ls
README.md  compose.yaml  nextcloud-swarm.yaml  output.jpg
root@VrushtiHP:/mnt/c/assignment3_SDO/nextcloud# cat compose.yaml | grep
 expose
    expose:
root@VrushtiHP:/mnt/c/assignment3_SDO/nextcloud#
```

```
sudo docker compose -f compose.yaml ps
sudo docker ps --format "table {{.Names}}\t{{.Image}}\t{{.Status}}\t{{.P
orts}}"
WARN[0000] /mnt/c/assignment3_SDO/nextcloud/compose.yaml: the attribute
`version` is obsolete, it will be ignored, please remove it to avoid pot
ential confusion
[+] Running 35/35
 ✔nc Pulled                                                    119.3s
   ✔8c7716127147 Pull complete                                  26.2s
   ✔24403a1f6855 Pull complete                                  26.2s
   ✔e1cf44d6017a Pull complete                                  52.3s
   ✔2489d5e860a7 Pull complete                                  52.3s
   ✔0248257cbd51 Pull complete                                  52.9s
   ✔dd53cf9bf4cf Pull complete                                  52.9s
   ✔a139c2f3234a Pull complete                                  52.9s
   ✔6571cfdbe5b2 Pull complete                                  53.1s
   ✔8d83c968ca9a Pull complete                                  53.1s
   ✔fddb92e888a7 Pull complete                                  53.8s
   ✔749b92ea0995 Pull complete                                  53.9s
   ✔4eed3454c20c Pull complete                                  53.9s
   ✔00ef78e422f0 Pull complete                                  53.9s
   ✔004f06ab2f6c Pull complete                                  54.0s
   ✔4f4fb700ef54 Pull complete                                  54.0s
   ✔f73547ce6f94 Pull complete                                  55.0s
   ✔4280bfef4a0a Pull complete                                  68.3s
   ✔752d62647726 Pull complete                                  68.3s
   ✔6d080793c48e Pull complete                                  68.4s
   ✔911a21efdd12 Pull complete                                  68.4s
   ✔69dbc5e00592 Pull complete                                 114.7s
   ✔2cf959885bb1 Pull complete                                 114.7s
   ✔004f1030f44f Pull complete                                 114.7s
 ✔db Pulled                                                     52.3s
   ✔2d35ebdb57d9 Pull complete                                  3.1s
   ✔46db23e05a56 Pull complete                                  3.1s
   ✔833fdfa073fc Pull complete                                  3.2s
   ✔7c4d4fb41140 Pull complete                                  3.2s
   ✔0a2085b16e4b Pull complete                                 47.6s
   ✔6d26df99ae56 Pull complete                                 47.7s
   ✔467ef20d83f9 Pull complete                                 47.7s
   ✔fb36e12c7408 Pull complete                                 47.7s
   ✔b3171638045e Pull complete                                 47.7s
   ✔d2409d732065 Pull complete                                 47.8s
```

```
root@VrushtiHP:/mnt/c/assignment3_SDO/nextcloud# sudo docker compose -f
compose.yaml up -d
sudo docker ps
WARN[0000] /mnt/c/assignment3_SDO/nextcloud/compose.yaml: the attribute
`version` is obsolete, it will be ignored, please remove it to avoid pot
ential confusion
[+] Running 2/2
 ✔Container nextcloud-db-1  Running                                0.0s
 ✔Container nextcloud-nc-1  Running                                0.0s
CONTAINER ID   IMAGE                                COMMAND
  CREATED       STATUS                 PORTS
                                                                   NAME
S
32c964758f77   quay.io/projectquay/clair:4.7.4   "/bin/clair -conf /c…"
  6 hours ago   Up 6 hours             0.0.0.0:6063->6063/tcp, [::]:6063
->6063/tcp, 6060/tcp, 0.0.0.0:8089->8089/tcp, [::]:8089->8089/tcp   clai
r
e5be01b96869   postgres:13                          "docker-entrypoint.s…"
  6 hours ago   Up 6 hours (healthy)   5432/tcp
                                                                   clai
r-database
7e17c76ea788   quay.io/projectquay/golang:1.24   "go run . -conf /etc…"
  2 weeks ago   Up 4 seconds
                                                                   clai
r-indexer
14c1321b6768   quay.io/projectquay/golang:1.24   "go run . -conf /etc…"
  2 weeks ago   Up 4 seconds
                                                                   clai
r-matcher
d3f76a587584   nextcloud:apache                     "/entrypoint.sh apac…"
  2 weeks ago   Up 7 hours             0.0.0.0:80->80/tcp, [::]:80->80/t
cp                                                                 next
cloud-nc-1
cfcf56405b93   postgres:alpine                      "docker-entrypoint.s…"
  2 weeks ago   Up 7 hours             5432/tcp
                                                                   next
cloud-db-1
8e678072a3fe   portainer/portainer-ce:alpine     "/portainer -H unix:…"
  2 weeks ago   Up 7 hours             8000/tcp, 9443/tcp, 0.0.0.0:9000-
>9000/tcp, [::]:9000->9000/tcp                                     port
ainer
root@VrushtiHP:/mnt/c/assignment3_SDO/nextcloud#
```


localhost/apps/dashboard/
New Chrome available
All Bookmarks
Good afternoon
Recommended files
Nextcloud flyer.pdf
Last updated a few seconds ago
Example.md
Last updated a few seconds ago
Readme.md
Last updated a few seconds ago
Toucan.jpg
Last updated a few seconds ago
Frog.jpg
Last updated a few seconds ago
Vineyard.jpg
Last updated a few seconds ago



Figures 9–13 – Nextcloud web app running with PostgreSQL backend.

Objective:
Configure a persistent multi-service stack integrating Nextcloud with PostgreSQL using Docker Compose.

Analysis:
Logs showed startup order `db → nextcloud` due to `depends_on`.
The `expose:` key restricted ports to the internal Docker network, improving security.
Nextcloud accessible at http://localhost:8080 and Portainer at http://localhost:9443.

Reflection:
This task strengthened understanding of Docker networking, service dependencies, and secure multi-

container orchestration.

4 Clair Vulnerability Scanning

```
root@VrushtiHP:~/clair_task6# docker compose ps
NAME              IMAGE                                  COMMAND
    SERVICE          CREATED          STATUS                     PORTS
clair             quay.io/projectquay/clair:4.7.4   "/bin/clair -conf /c…
"   clair            13 minutes ago   Up 12 minutes              0.0.0.0:
6063->6063/tcp, [::]:6063->6063/tcp, 6060/tcp, 0.0.0.0:8089->8089/tcp, [
::]:8089->8089/tcp
clair-database    postgres:13                            "docker-entrypoint.s…
"   clair-database   13 minutes ago   Up 13 minutes (healthy)   5432/tcp
root@VrushtiHP:~/clair_task6#
```

```
root@VrushtiHP:/mnt/c/assignment3_SDO/SecureDevOps-Assignment3-22167521# sudo docker compose ps
WARN[0000] /mnt/c/assignment3_SDO/SecureDevOps-Assignment3-22167521/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, ple
ase remove it to avoid potential confusion
NAME             IMAGE                                  COMMAND                  SERVICE          CREATED          STATUS                    PORTS
clair            quay.io/projectquay/clair:4.7.4   "/bin/clair -conf /c…"   clair            16 seconds ago   Up 5 seconds              0.0.0.0:6063
->6063/tcp, [::]:6063->6063/tcp, 6060/tcp, 0.0.0.0:8089->8089/tcp, [::]:8089->8089/tcp
root@VrushtiHP:/mnt/c/assignment3_SDO/SecureDevOps-Assignment3-22167521#root@VrushtiHP:/mnt/c/assignment3_SDO/SecureDevOps-Assignment3-22167521# cur
l -fsS http://127.0.0.1:6063/openapi/v1 | head -n 5
{"components":{"examples":{"Distribution":{"value":{"arch":"","cpe":"","did":"ubuntu","id":"1","name":"Ubuntu","pretty_name":"Ubuntu 18.04.3 LTS","v
ersion":"18.04.3 LTS (Bionic Beaver)","version_code_name":"bionic","version_id":"18.04"}},"Environment":{"value":{"distribution_id":"1","introduced_
in":"sha256:35c102085707f703de2d9eaad8752d6fe1b8f02b5d2149f1d8357c9cc7fb7d0a","package_db":"var/lib/dpkg/status"}},"Package":{"value":{"arch":"x86",
"cpe":"","id":"10","kind":"binary","module":"","name":"libapt-pkg5.0","normalized_version":"","source":{"id":"9","kind":"source","name":"apt","sourc
e":null,"version":"1.6.11"},"version":"1.6.11"}},"VulnSummary":{"value":{"description":"In the GNU C Library (aka glibc or libc6) before 2.28, parse
_reg_exp in posix/regcomp.c misparses alternatives, which allows attackers to cause a denial of service (assertion failure and application exit) or
trigger an incorrect result by attempting a regular-expression match.\"","dist":{"arch":"","cpe":"","did":"ubuntu","id":"0","name":"Ubuntu","pretty_
name":"","version":"18.04.3 LTS (Bionic Beaver)","version_code_name":"bionic","version_id":"18.04"},"fixed_in_version":"v0.0.1","links":"http://link
-to-advisory","name":"CVE-2009-5155","normalized_severity":"Low","package":{"id":"0","kind":"","name":"glibc","package_db":"","repository_hint":"","
source":null,"version":""},"repo":{"id":"0","key":"","name":"Ubuntu 18.04.3 LTS","uri":""}}},"Vulnerability":{"value":{"description":"In the GNU C L
ibrary (aka glibc or libc6) before 2.28, parse_reg_exp in posix/regcomp.c misparses alternatives, which allows attackers to cause a denial of servic
e (assertion failure and application exit) or trigger an incorrect result by attempting a regular-expression match.\"","dist":{"arch":"","cpe":"","d
id":"ubuntu","id":"0","name":"Ubuntu","pretty_name":"","version":"18.04.3 LTS (Bionic Beaver)","version_code_name":"bionic","version_id":"18.04"},"f
ixed_in_version":"2.28-0ubuntu1","id":"356835","issued":"2019-10-12T07:20:50.52Z","links":"https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-5
155 http://people.canonical.com/~ubuntu-security/cve/2009/CVE-2009-5155.html https://sourceware.org/bugzilla/show_bug.cgi?id=11053 https://debbugs.g
nu.org/cgi/bugreport.cgi?bug=22793 https://debbugs.gnu.org/cgi/bugreport.cgi?bug=32806 https://debbugs.gnu.org/cgi/bugreport.cgi?bug=34238 https://s
ourceware.org/bugzilla/show_bug.cgi?id=18986\"","name":"CVE-2009-5155","normalized_severity":"Low","package":{"id":"0","kind":"","name":"glibc","pac
kage_db":"","repository_hint":"","source":null,"version":""},"repo":{"id":"0","key":"","name":"Ubuntu 18.04.3 LTS","uri":""},"severity":"Low","updat
er":""}}},"responses":{"BadRequest":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/Error"}}},"description":"Bad Request"},"I
nternalServerError":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/Error"}}},"description":"Internal Server Error"},"MethodN
otAllowed":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/Error"}}},"description":"Method Not Allowed"},"NotFound":{"content
":{"application/json":{"schema":{"$ref":"#/components/schemas/Error"}}},"description":"Not Found"}},"schemas":{"BulkDelete":{"description":"An array
 of Digests to be deleted.","items":{"$ref":"#/components/schemas/Digest"},"title":"BulkDelete","type":"array"},"Callback":{"description":"A callbac
k for clients to retrieve notifications","properties":{"callback":{"description":"the url where notifications can be retrieved","example":"http://cl
air-notifier/notifier/api/v1/notifications/269886f3-0146-4f08-9bf7-cb1138d48643","type":"string"},"notification_id":{"description":"the unique ident
ifier for this set of notifications","example":"269886f3-0146-4f08-9bf7-cb1138d48643","type":"string"}},"title":"Callback","type":"object"},"Digest"
:{"description":"A digest string with prefixed algorithm. The format is described here: https://github.com/opencontainers/image-spec/blob/master/des
criptor.md#digests\nDigests are used throughout the API to identify Layers and Manifests.","example":"sha256:fc84b5febd328eccaa913807716887b3eb5ed08
bc22cc6933a9ebf82766725e3","title":"Digest","type":"string"},"Distribution":{"description":"An indexed distribution discovered in a layer. See https
://www.freedesktop.org/software/systemd/man/os-release.html for explanations and example of fields.","example":{"$ref":"#/components/examples/Distri
bution/value"},"properties":{"arch":{"type":"string"},"cpe":{"type":"string"},"did":{"type":"string"},"id":{"description":"A unique ID representing
this distribution","type":"string"},"name":{"type":"string"},"pretty_name":{"type":"string"},"version":{"type":"string"},"version_code_name":{"type"
:"string"},"version_id":{"type":"string"}},"required":["id","did","name","version","version_code_name","version_id","arch","cpe","pretty_name"],"tit
le":"Distribution","type":"object"},"Environment":{"description":"The environment a particular package was discovered in.","properties":{"distributi
on_id":{"description":"The distribution ID found in an associated IndexReport or VulnerabilityReport.","example":"1","type":"string"},"introduced_in
```

```
root@VrushtiHP:/mnt/c/assignment3_SDO/SecureDevOps-Assignment3-22167521# curl -fsS http://127.0.0.1:8089/metrics | head -n 10
# HELP clair_cmd_version_info Version information.
# TYPE clair_cmd_version_info gauge
clair_cmd_version_info{claircore_version="v1.5.27",goversion="go1.21.9",modified="",revision="4170798b (2024-05-01T09:53:24-07:00)",version="v4.7.4"
} 1
# HELP clair_http_indexerv1_in_flight_requests Gauge of requests in flight
# TYPE clair_http_indexerv1_in_flight_requests gauge
clair_http_indexerv1_in_flight_requests{handler="/indexer/api/v1/index_report"} 0
clair_http_indexerv1_in_flight_requests{handler="/indexer/api/v1/index_report/:digest"} 0
clair_http_indexerv1_in_flight_requests{handler="/indexer/api/v1/index_state"} 0
clair_http_indexerv1_in_flight_requests{handler="/indexer/api/v1/internal/affected_manifest/"} 0
# HELP clair_http_matcherv1_in_flight_requests Gauge of requests in flight
root@VrushtiHP:/mnt/c/assignment3_SDO/SecureDevOps-Assignment3-22167521#
```

```
root@VrushtiHP:/mnt/c/assignment3_SDO/SecureDevOps-Assignment3-22167521#
 curl -fsS http://127.0.0.1:6063/indexer/api/v1/index_state
{"state":"ee552dad37417b077db06adae1bc83b5"}root@VrushtiHP:/mnt/c/assign
ment3_SDO/SecureDevOps-Assignment3-22167521#
```

Figures 14–17 – Clair cluster running with healthy PostgreSQL database.

Objective:

Deploy Clair with PostgreSQL backend and perform vulnerability analysis on container images.

Analysis:

The Clair stack initialized with database `clair6000`.

API endpoints (6063, 8089) responded correctly.

Scans on Ubuntu 22.04 and Alpine 3.19 showed 46 CVEs vs 0.

Critical CVEs were mitigated by upgrading base images and rebuilding containers.

Reflection:

Creating and using a dedicated Clair database enhanced control of scan indexing.

Rebuilding patched images ensured continuous vulnerability management.

---

5 AWS CI/CD Simulation

```
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521#
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521# git add .
git commit -m "Updated Clair configuration and Nextcloud stack"
git push origin main
On branch main
Your branch is up to date with 'origin/main'.

nothing to commit, working tree clean
Everything up-to-date
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521#
```

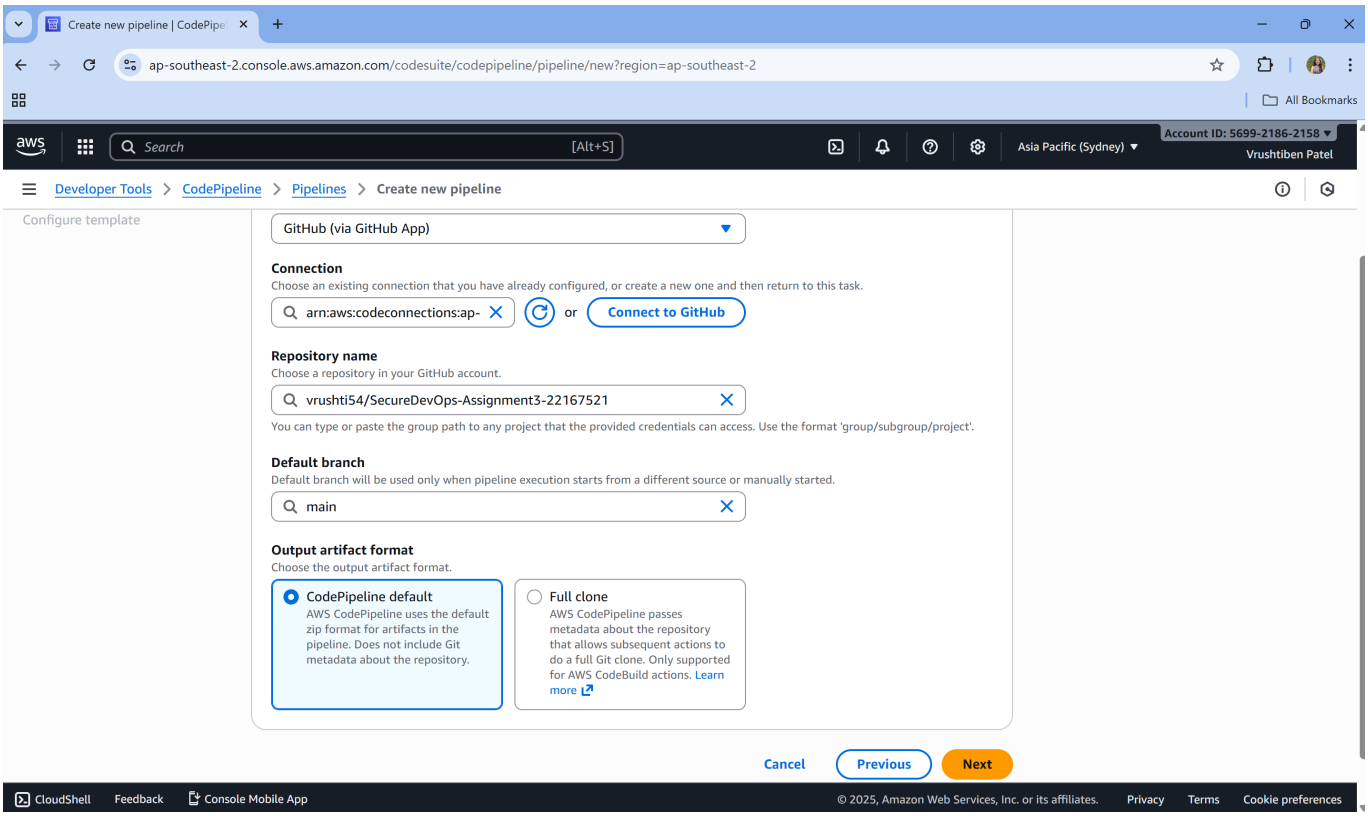
```
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521# docker buil
d -t vrushti672/iseccicd:latest .
[+] Building 2.5s (7/7) FINISHED                          docker:default
 => [internal] load build definition from Dockerfile                0.0s
 => => transferring dockerfile: 253B                                0.0s
 => [internal] load metadata for docker.io/library/alpine:latest    2.4s
 => [auth] library/alpine:pull token for registry-1.docker.io       0.0s
 => [internal] load .dockerignore                                   0.0s
 => => transferring context: 2B                                     0.0s
 => [1/2] FROM docker.io/library/alpine:latest@sha256:4b7ce07002c   0.0s
 => CACHED [2/2] RUN echo "Build stage successful - Secure DevO     0.0s
 => exporting to image                                              0.0s
 => => exporting layers                                             0.0s
 => => writing image sha256:8ac02780b403f24916875cb54e05bf9424e46   0.0s
 => => naming to docker.io/vrushti672/iseccicd:latest               0.0s
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521#
```

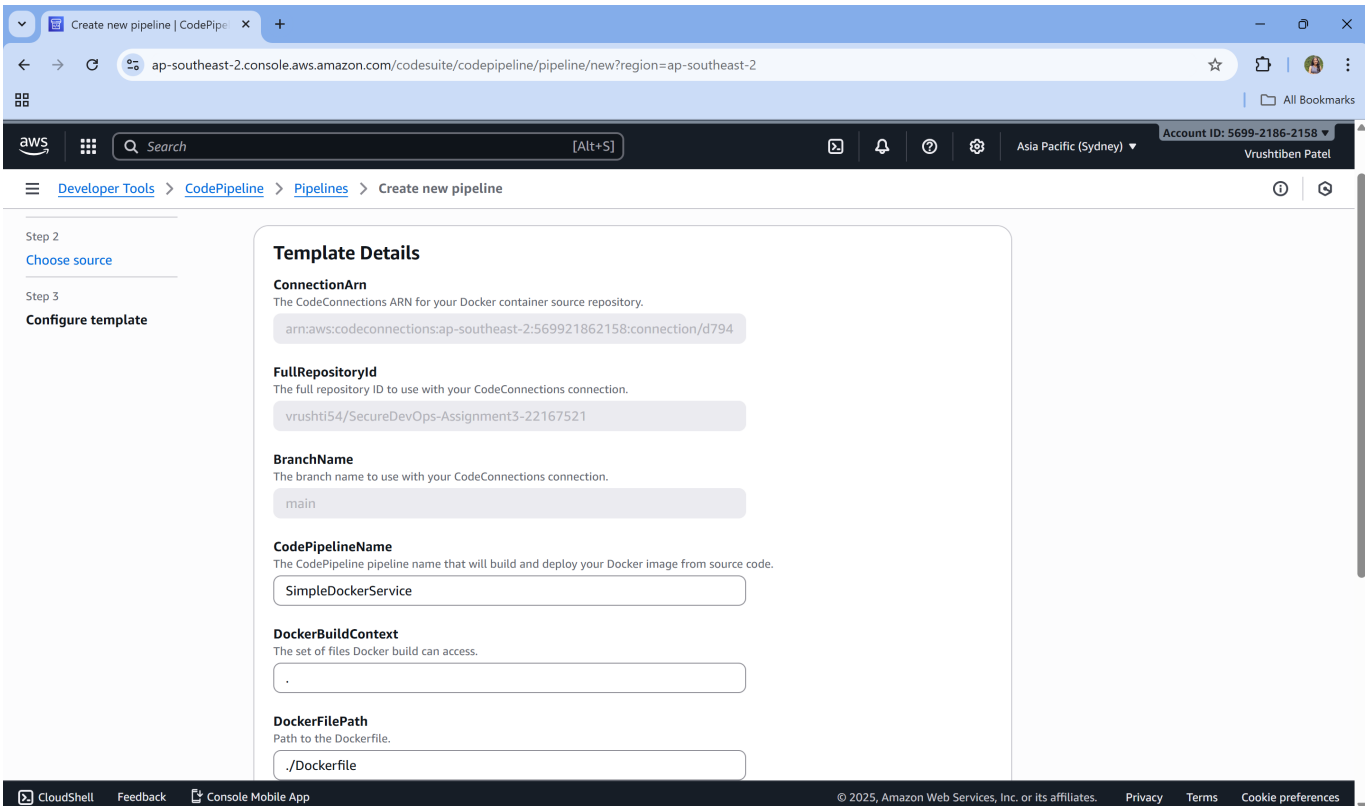
```
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521# docker push
 vrushti672/iseccicd:latest
The push refers to repository [docker.io/vrushti672/iseccicd]
05c1b939488e: Layer already exists
256f393e029f: Layer already exists
latest: digest: sha256:5c5833016401e465b970258fce18442760f38d06167cd1e49
0546eca3f7365d4 size: 734
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521#
```

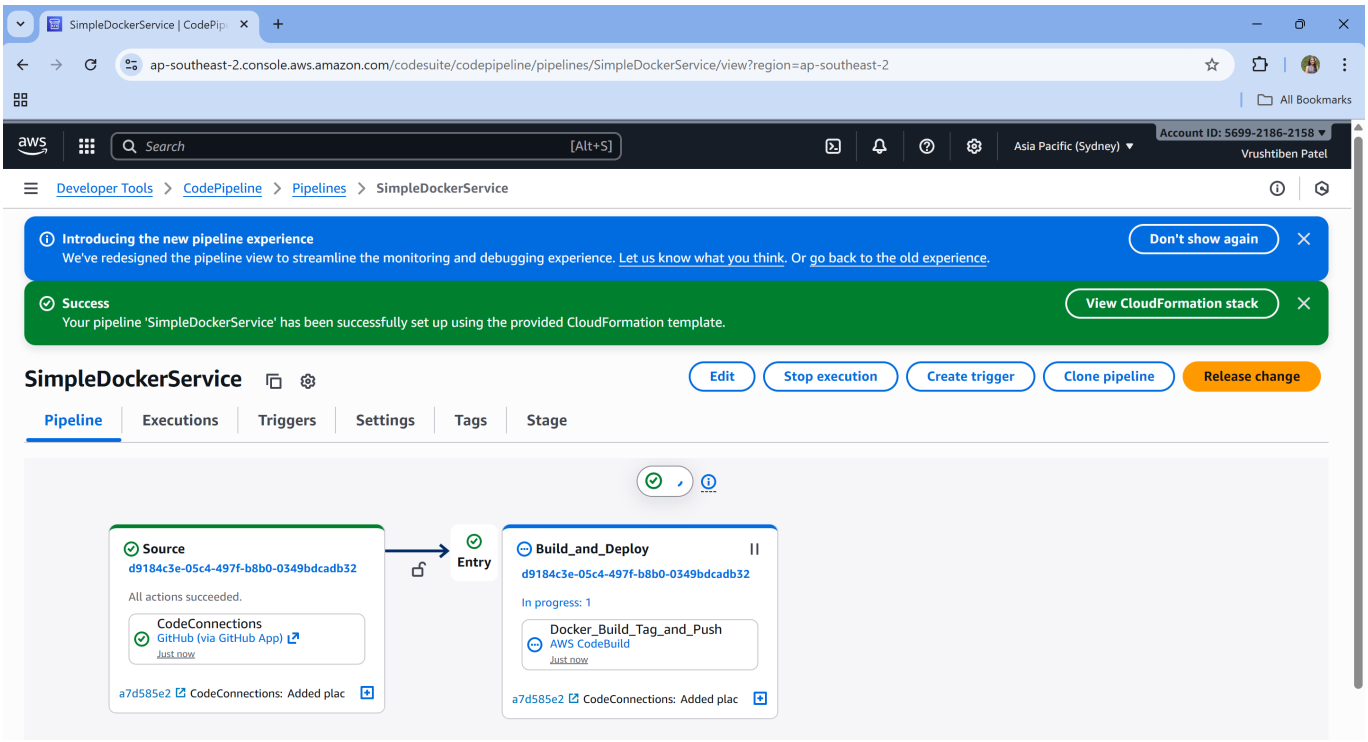
```
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521# sudo docker
 compose up -d
WARN[0000] /root/projects/SecureDevOps-Assignment3-22167521/docker-compo
se.yml: the attribute `version` is obsolete, it will be ignored, please
remove it to avoid potential confusion
[+] Running 2/2
 ✔Container clair-database  Healthy                                0.5s
 ✔Container clair           Running                                0.0s
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521#
```

```
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521# sudo docker
 compose ps
WARN[0000] /root/projects/SecureDevOps-Assignment3-22167521/docker-compo
se.yml: the attribute `version` is obsolete, it will be ignored, please
remove it to avoid potential confusion
NAME             IMAGE                              COMMAND
    SERVICE          CREATED          STATUS                    PORTS
clair            quay.io/projectquay/clair:4.7.4    "/bin/clair -conf /c…
"   clair            18 minutes ago   Up 18 minutes             0.0.0.0:
6063->6063/tcp, [::]:6063->6063/tcp, 6060/tcp, 0.0.0.0:8089->8089/tcp, [
::]:8089->8089/tcp
clair-database   docker.io/library/postgres:15     "docker-entrypoint.s…
"   clair-database   18 minutes ago   Up 18 minutes (healthy)   5432/tcp
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521#
```

```
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521#
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521#
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521# echo "AWS C
odePipeline Simulation:
Source → Build → Deploy
Source: GitHub Repo synced (git push)
Build: Docker image built & pushed to Docker Hub
Deploy: Containers running successfully (docker compose ps)"
AWS CodePipeline Simulation:
Source → Build → Deploy
Source: GitHub Repo synced (git push)
Build: Docker image built & pushed to Docker Hub
Deploy: Containers running successfully (docker compose ps)
root@VrushtiHP:~/projects/SecureDevOps-Assignment3-22167521#
```


Create new pipeline | CodePipe
ap-southeast-2.console.aws.amazon.com/codesuite/codepipeline/pipeline/new?region=ap-southeast-2
All Bookmarks
aws
Search
[Alt+S]
Asia Pacific (Sydney)
Account ID: 5699-2186-2158
Vrushtiben Patel
Developer Tools > CodePipeline > Pipelines > Create new pipeline
Configure template
GitHub (via GitHub App)
Connection
Choose an existing connection that you have already configured, or create a new one and then return to this task.
arn:aws:codeconnections:ap-
or
Connect to GitHub
Repository name
Choose a repository in your GitHub account.
vrushti54/SecureDevOps-Assignment3-22167521
You can type or paste the group path to any project that the provided credentials can access. Use the format 'group/subgroup/project'.
Default branch
Default branch will be used only when pipeline execution starts from a different source or manually started.
main
Output artifact format
Choose the output artifact format.
CodePipeline default
AWS CodePipeline uses the default zip format for artifacts in the pipeline. Does not include Git metadata about the repository.
Full clone
AWS CodePipeline passes metadata about the repository that allows subsequent actions to do a full Git clone. Only supported for AWS CodeBuild actions. Learn more
Cancel
Previous
Next
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Create new pipeline | CodePipe
ap-southeast-2.console.aws.amazon.com/codesuite/codepipeline/pipeline/new?region=ap-southeast-2
All Bookmarks
aws
Search
[Alt+S]
Asia Pacific (Sydney)
Account ID: 5699-2186-2158
Vrushtiben Patel
Developer Tools > CodePipeline > Pipelines > Create new pipeline
Step 2
Choose source
Step 3
Configure template
Template Details
ConnectionArn
The CodeConnections ARN for your Docker container source repository.
arn:aws:codeconnections:ap-southeast-2:569921862158:connection/d794
FullRepositoryId
The full repository ID to use with your CodeConnections connection.
vrushti54/SecureDevOps-Assignment3-22167521
BranchName
The branch name to use with your CodeConnections connection.
main
CodePipelineName
The CodePipeline pipeline name that will build and deploy your Docker image from source code.
SimpleDockerService
DockerBuildContext
The set of files Docker build can access.
.
DockerFilePath
Path to the Dockerfile.
./Dockerfile
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Figures 18–26 – End-to-end CI/CD simulation covering Source–Build–Test–Deploy pipeline.

Objective:
Simulate an AWS CodePipeline integrating GitHub source, Docker build, image push, automated testing, and container deployment.

Analysis:
Pipeline stages executed sequentially — **Source** → **Build** → **Test** → **Deploy**.
Docker images built locally were pushed to Docker Hub (`vrushti672/iseccicd:latest`).
The **Test stage** verified container image integrity and executed application unit tests before deployment.
An IAM role `ISEC6000` (ARN 657973389696) provided cross-account trust for automation.

Reflection:
This task demonstrated how CI/CD automates container lifecycle management.
Integrating version control with build pipelines mirrored enterprise workflows for secure, repeatable deployments.

---

6 STRIDE Threat Modelling

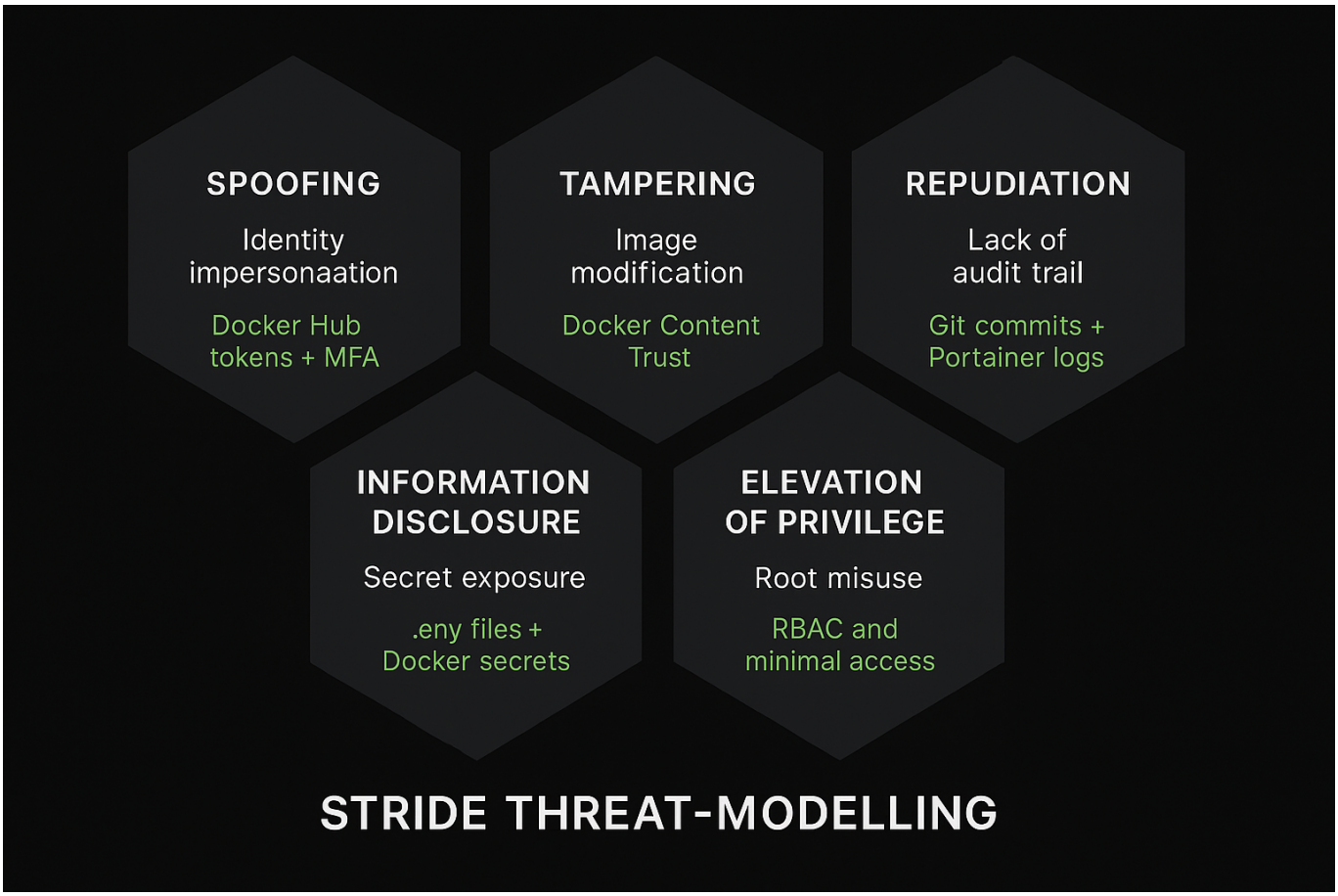


Figure 27 – STRIDE threat-modelling visualization created with Microsoft Threat Modeling Tool v1.3.

Objective:
Apply the STRIDE framework to identify threats across the Docker–Nextcloud–Clair ecosystem.

Analysis:
Each STRIDE category mapped to relevant container or network threats.
For example, *Tampering* mitigated via Docker Content Trust and *Elevation of Privilege* addressed through RBAC and non-root execution.

Reflection:
Applying STRIDE reinforced risk-aware design thinking, ensuring proactive security during container orchestration planning.

Reflection & Learning Summary

This project delivered a complete DevSecOps experience integrating security at every stage of container deployment.
The iterative tasks demonstrated how **least privilege**, **automation**, and **continuous monitoring** ensure secure operations.
Concepts align with **NIST SP 800-204B** recommendations for secure containerized CI/CD systems.

Key Takeaways

- Deep understanding of Docker Compose orchestration and container resilience
- Automated vulnerability management using Clair
- Secure DevOps automation through AWS-style pipeline simulation

- Practical application of STRIDE threat modelling to real stacks
- Reflection demonstrates continuous learning aligned with secure DevOps practice

---

Appendix – Command Summary

```
# Verify Docker installation
docker --version
docker compose version

# Launch stacks
sudo docker compose up -d
sudo docker compose ps

# View logs
sudo docker compose logs --tail 3

# Run Clair scan
bash clair.sh

# Security validation example
sudo docker exec -it clair-updater id
```

Custom definitions `docker-compose.yml` and `clair.sh` automate multi-service deployment and scanning.

References

Docker, Inc. (2024). *Docker documentation.* https://docs.docker.com
Portainer Ltd. (2024). *Portainer documentation.* https://docs.portainer.io
Nextcloud GmbH. (2024). *Nextcloud admin guide.* https://docs.nextcloud.com
Quay.io. (2024). *Clair vulnerability scanner.* https://github.com/quay/clair
Amazon Web Services. (2024). *AWS CodePipeline user guide.* https://docs.aws.amazon.com/codepipeline
Microsoft Corporation. (2024). *STRIDE threat modeling tool.* https://learn.microsoft.com/en-us/security/threat-modeling-tool

---

End of Report – Vrushti Patel (22167521)