

Capstone_Project :

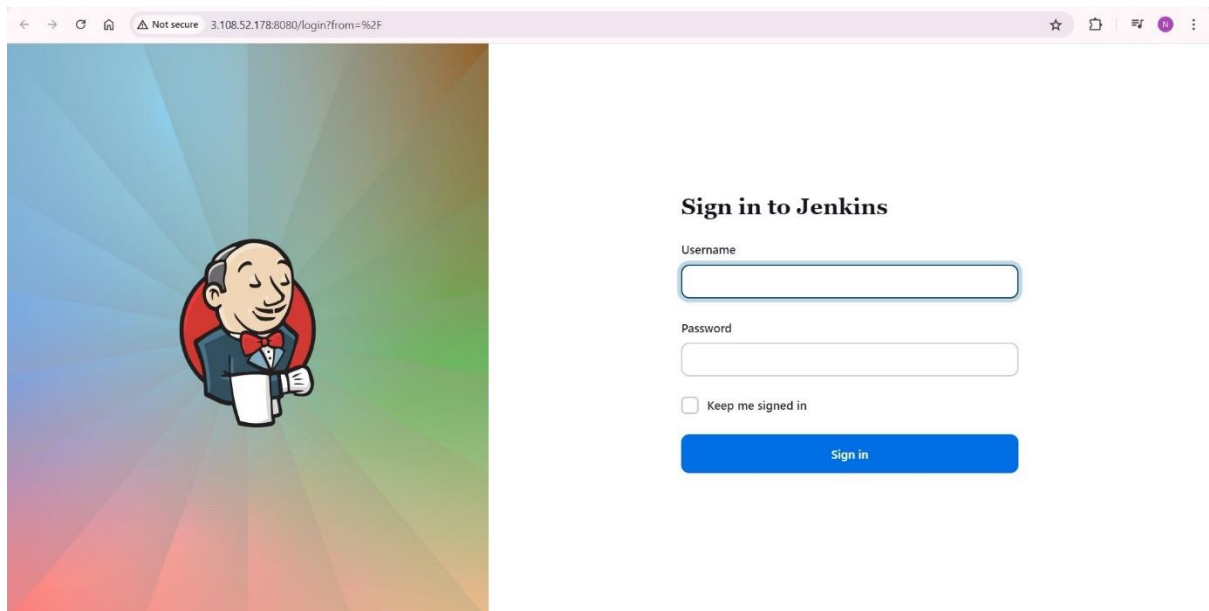
Application Deployment:

Deploy the given react application to a production ready state

GitHub URL:

https://github.com/Nidhyapandian/React_Project.git

Jenkins Login Page:



Sign in to Jenkins

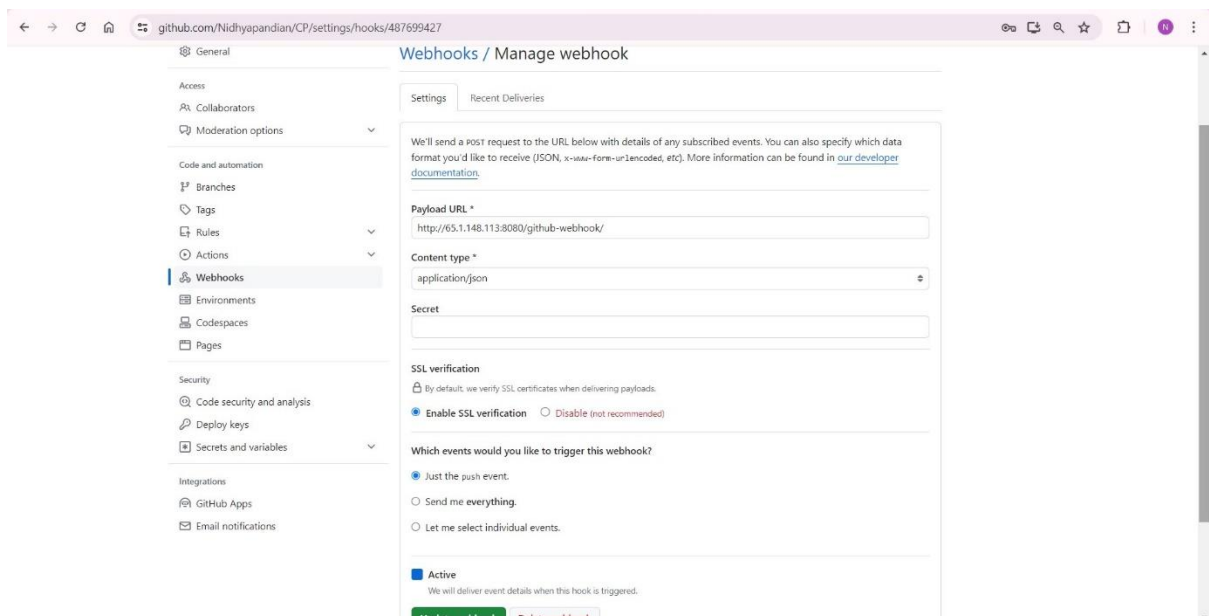
Username

Password

☐ Keep me signed in

Sign in

Webhook Configuration:



Webhooks / Manage webhook

Settings Recent Deliveries

We'll send a POST request to the URL below with details of any subscribed events. You can also specify which data format you'd like to receive (JSON, x-www-form-urlencoded, etc). More information can be found in [our developer documentation](#).

Payload URL *

http://65.1.148.113:8080/github-webhook/

Content type *

application/json

Secret

SSL verification

By default, we verify SSL certificates when delivering payloads.

☒ Enable SSL verification ☐ Disable (not recommended)

Which events would you like to trigger this webhook?

☒ Just the push event.

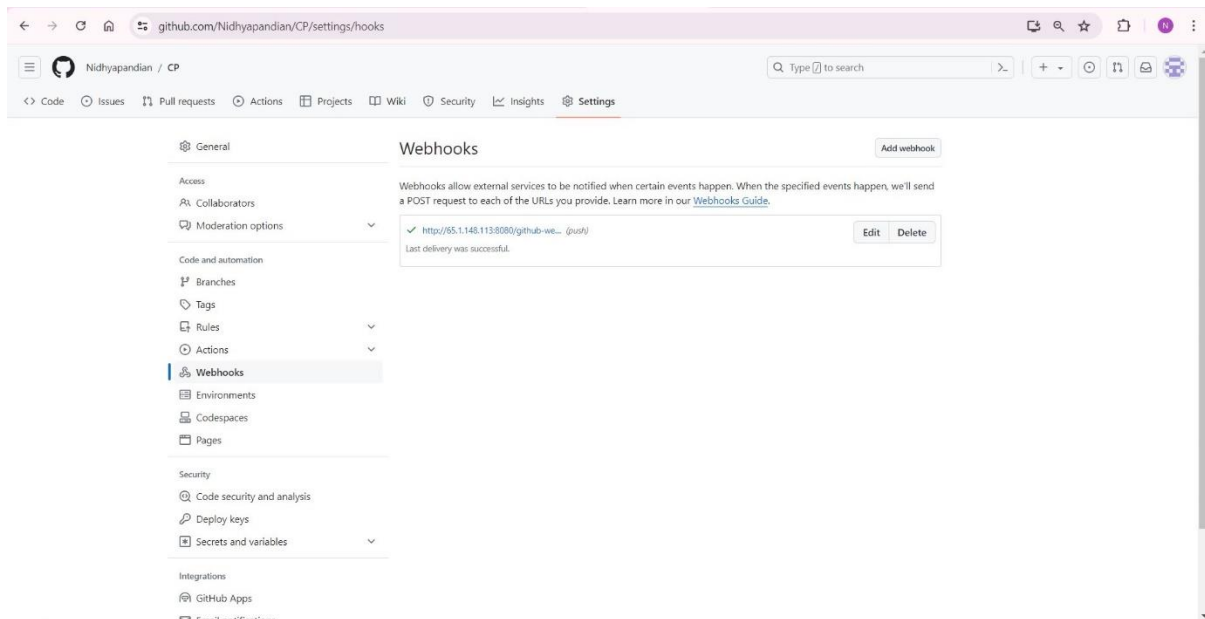
☐ Send me everything.

☐ Let me select individual events.

☒ Active

We will deliver event details when this hook is triggered.

Update webhook Delete webhook



Console Output:

Started by user [Nidhya](#)

Obtained Jenkinsfile from git https://github.com/Nidhyapandian/React_Project.git

[Pipeline] Start of Pipeline

[Pipeline] node

Running on [jenkins](#) in /var/lib/jenkins/workspace/React_Project

[Pipeline] {

[Pipeline] stage

[Pipeline] { (Declarative: Checkout SCM)

[Pipeline] checkout

Selected Git installation does not exist. Using Default

The recommended git tool is: NONE

No credentials specified

> git rev-parse --resolve-git-dir /var/lib/jenkins/workspace/React_Project/.git # timeout=10

Fetching changes from the remote Git repository

> git config remote.origin.url https://github.com/Nidhyapandian/React_Project.git # timeout=10

Fetching upstream changes from https://github.com/Nidhyapandian/React_Project.git

> git --version # timeout=10

> git --version # 'git version 2.34.1'

> git fetch --tags --force --progress -- https://github.com/Nidhyapandian/React_Project.git

+refs/heads/*:refs/remotes/origin/* # timeout=10

> git rev-parse refs/remotes/origin/dev^{commit} # timeout=10

Checking out Revision 9e6415071e6ae494b60c44c0ba577a879c7ee9dc (refs/remotes/origin/dev)

> git config core.sparsecheckout # timeout=10

> git checkout -f 9e6415071e6ae494b60c44c0ba577a879c7ee9dc # timeout=10

Commit message: "Update Jenkinsfile"

First time build. Skipping changelog.

[Pipeline] }

[Pipeline] // stage

[Pipeline] withEnv

[Pipeline] {

[Pipeline] stage

[Pipeline] { (Build)

[Pipeline] sh

+ chmod +x build.sh

[Pipeline] sh

+ ./build.sh

```
web is up-to-date
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Deploy)
[Pipeline] withCredentials
Masking supported pattern matches of $DOCKER_PASSWORD
[Pipeline] {
[Pipeline] sh
+ docker login -u smart24 --password-stdin docker.io
+ echo ****
WARNING! Your password will be stored unencrypted in /var/lib/jenkins/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store
```

```
Login Succeeded
[Pipeline] script
[Pipeline] {
[Pipeline] echo
Current branch is: dev
[Pipeline] sh
+ docker-compose down
Stopping web ...
Stopping web ... done
Removing web ...
Removing web ... done
Removing network react_project_default
[Pipeline] sh
+ chmod +x build.sh
[Pipeline] sh
+ ./build.sh
Creating network "react_project_default" with the default driver
Creating web ...
Creating web ... done
[Pipeline] echo
Changes in this dev branch
[Pipeline] sh
+ docker tag nginximage smart24/dev
[Pipeline] sh
+ docker push smart24/dev
Using default tag: latest
The push refers to repository [docker.io/smart24/dev]
00a429d72c9b: Preparing
56b6d3be75f9: Preparing
0c6c257920c8: Preparing
92d0d4e97019: Preparing
7190c87a0e8a: Preparing
933a3ce2c78a: Preparing
32cfaf91376f: Preparing
32148f9f6c5a: Preparing
933a3ce2c78a: Waiting
32cfaf91376f: Waiting
32148f9f6c5a: Waiting
7190c87a0e8a: Layer already exists
00a429d72c9b: Layer already exists
0c6c257920c8: Layer already exists
92d0d4e97019: Layer already exists
56b6d3be75f9: Layer already exists
32cfaf91376f: Layer already exists
```

933a3ce2c78a: Layer already exists
32148f9f6c5a: Layer already exists
latest: digest: sha256:2f761077517e027b07bd16bb9c6f2133c27471bde65853b0ca81a371f86653f7
size: 1989
[Pipeline] echo
Docker image pushed successfully.
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // withCredentials
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // withEnv
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS

The screenshot displays the AWS Management Console interface for EC2 instances. At the top, the navigation bar shows the AWS logo, 'Services', a search bar, and the user's name 'Nidhya'. The main content area is titled 'Instances (1/2)' and includes a search bar and a table of instances.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IP
Capstone_project	i-005afc17a48be80a7	Running	t2.micro	Initializing	View alarms +	ap-south-1b	ec2-65-2-73-69.ap-sout...	65.2.73.69
Monitoring_server	i-0c9195a8ea8a5277c	Running	t2.micro	Initializing	View alarms +	ap-south-1a	ec2-43-205-117-67.ap-...	43.205.117.67

The 'Capstone_project' instance is selected, and its details are shown in the 'Instance summary' section. The summary includes the instance ID, name, IP address, hostname type, and various DNS names.

Instance summary

- Instance ID: i-005afc17a48be80a7 (Capstone_project)
- IP address: -
- Hostname type: IP name: ip-172-31-13-185.ap-south-1.compute.internal
- Answer private resource DNS name: IP-v4 (A)
- Public IPv4 address: 65.2.73.69 | [open address](#)
- Instance state: **Running**
- Private IP DNS name (IPv4 only): ip-172-31-13-185.ap-south-1.compute.internal
- Instance type: t2.micro
- Private IPv4 addresses: 172.31.13.185
- Public IPv4 DNS: ec2-65-2-73-69.ap-south-1.compute.amazonaws.com | [open address](#)
- Elastic IP addresses: -

The footer of the console shows the copyright notice: © 2024 Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences.

Security Group Configuration:

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ModifyInboundSecurityGroupRules;securityGroupId=sg-0f59038e81ef1ec5

Services

Search

[Alt+S]

Mumbai

Nidhya

EC2

Security group rule ID	Type	Protocol	Port range	Source	Description - optional	
sgr-078a80d8d49c70568	HTTP	TCP	80	Custom	Nginx Port	Delete
sgr-04c65ade73529b5f3	Custom TCP	TCP	8080	Custom	Jenkins Port	Delete
sgr-05ff42eddda09ec5e	Custom TCP	TCP	5000	Custom	Container port	Delete
sgr-0eeafa835159e44c	SSH	TCP	22	Custom		Delete
-	Custom TCP	TCP	9100	Anywh...	Node-Exporter Port	Delete

Add rule

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

CloudShellFeedback

© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

Security Group configuration for Monitoring Server:

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ModifyInboundSecurityGroupRules;securityGroupId=sg-03f1b6289d8622cb7

Services

Search

[Alt+S]

Mumbai

Nidhya

EC2

Edit inbound rules

Inbound rules control the incoming traffic that's allowed to reach the instance.

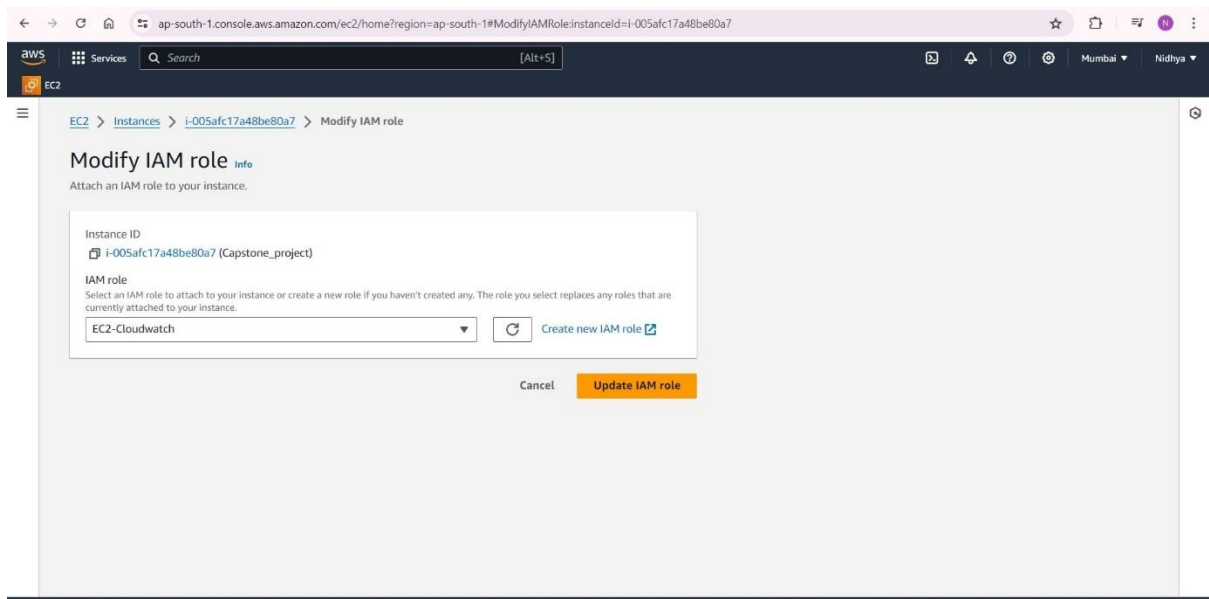
Inbound rules

Security group rule ID	Type	Protocol	Port range	Source	Description - optional	
sgr-0ed9d2335cb0f66d3	SSH	TCP	22	Custom		Delete
-	Custom TCP	TCP	9090	Anywh...	Prometheus Port	Delete
-	Custom TCP	TCP	3000	Anywh...	Grafana Port	Delete
-	Custom TCP	TCP	9100	Anywh...	Node-Exporter Port	Delete

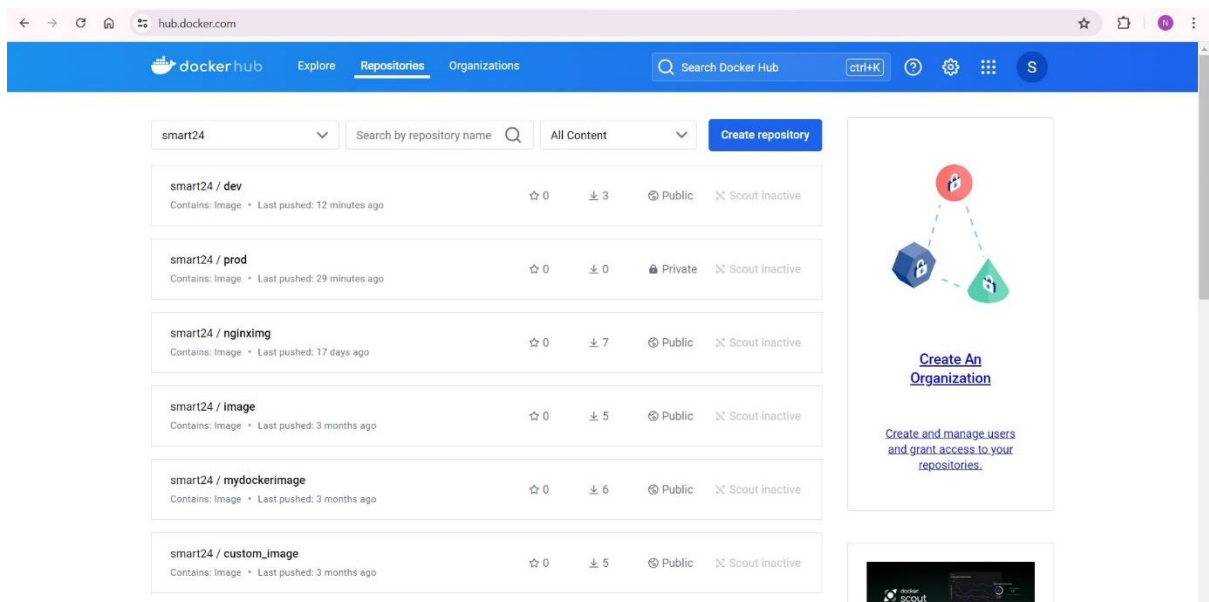
Add rule

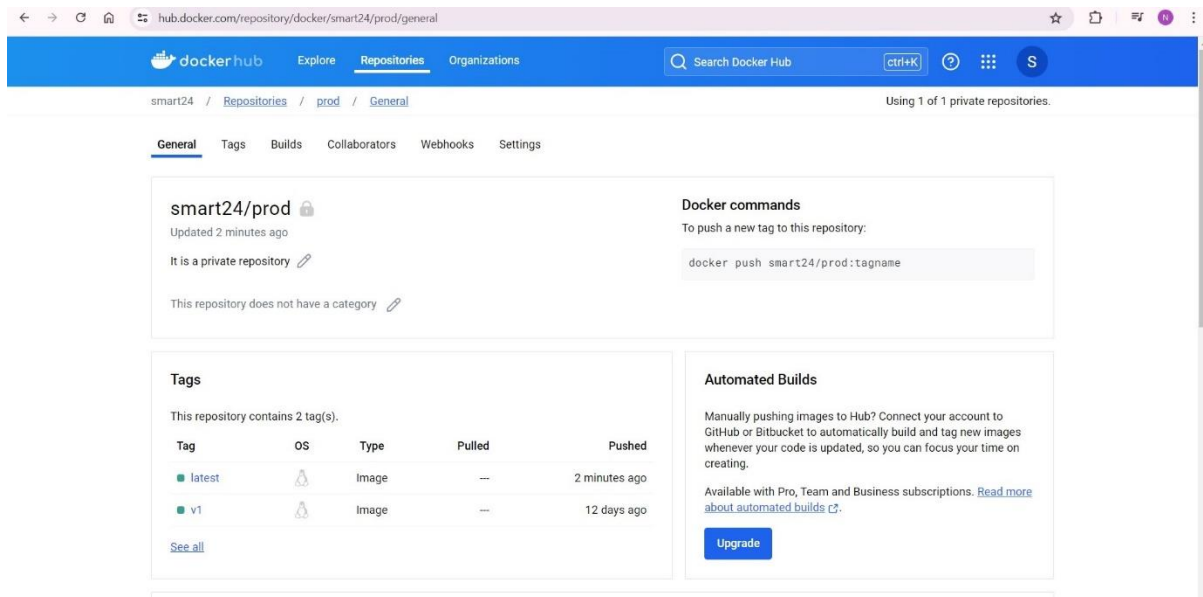
CloudShellFeedback

© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences



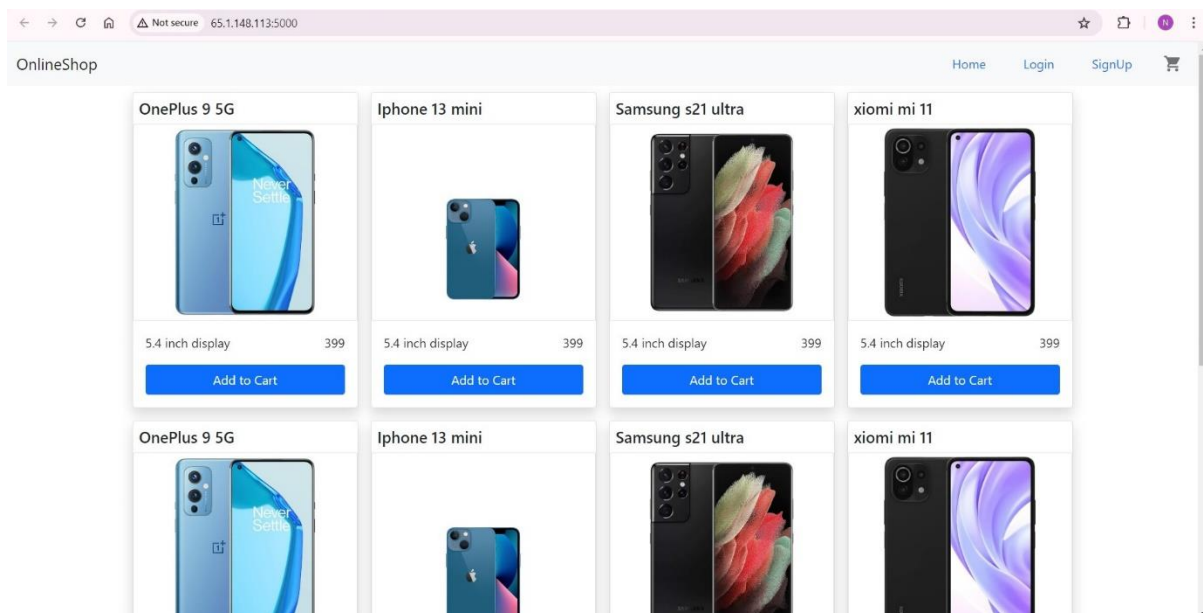
Dockerhub Registry showing images pushed into prod and dev repo:






Output:

Deployed site:



← → 🔍 📄 ⚠️ Not secure 65.1.148.113:5000/login ☆ 🗑️ ⓘ ⋮

OnlineShop Home Login **SignUp** 🛒



Login Into your account

Email address


Password

Login

Have an account? [Login In here](#)

← → 🔍 📄 ⚠️ Not secure 65.1.148.113:5000/signup ☆ 🗑️ ⓘ ⋮

OnlineShop Home Login **SignUp** 🛒



Sign Up your account

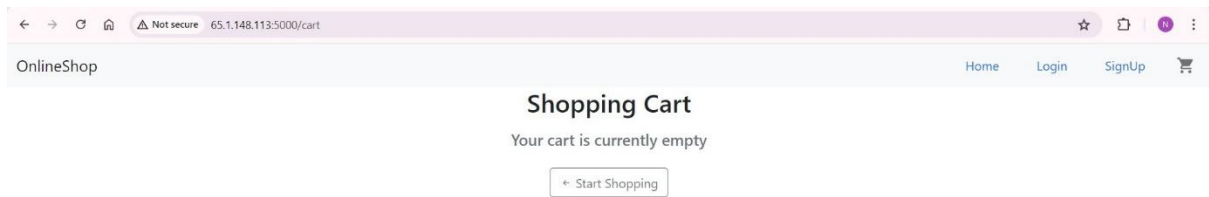
User Name

Email address

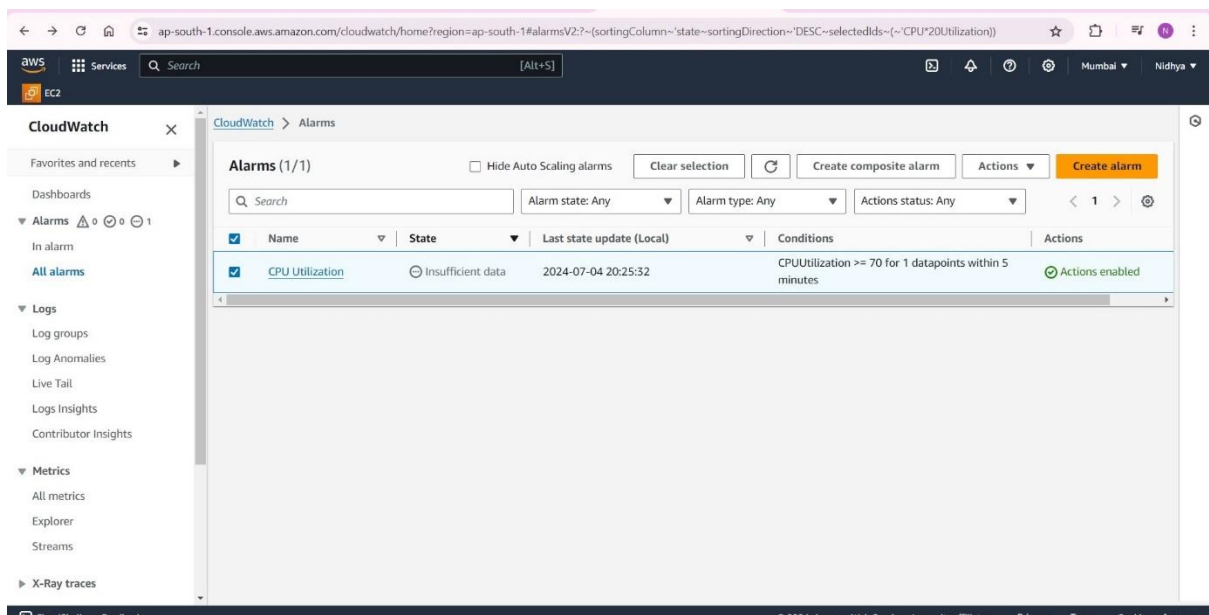
Password

Sign Up

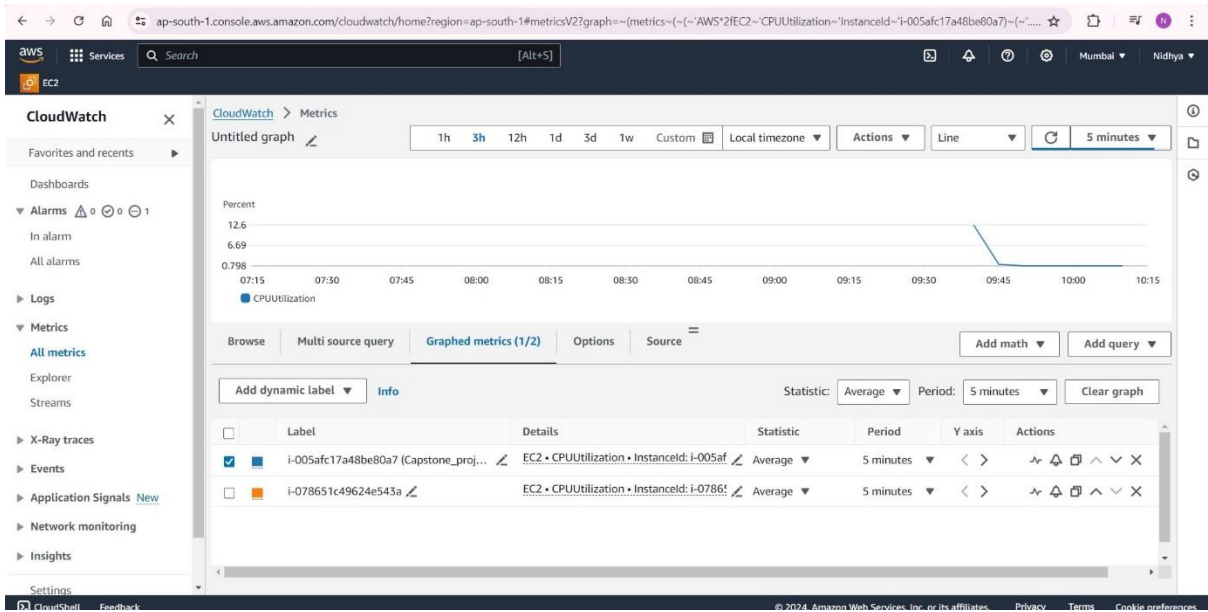
Have an account? [Login In here](#)



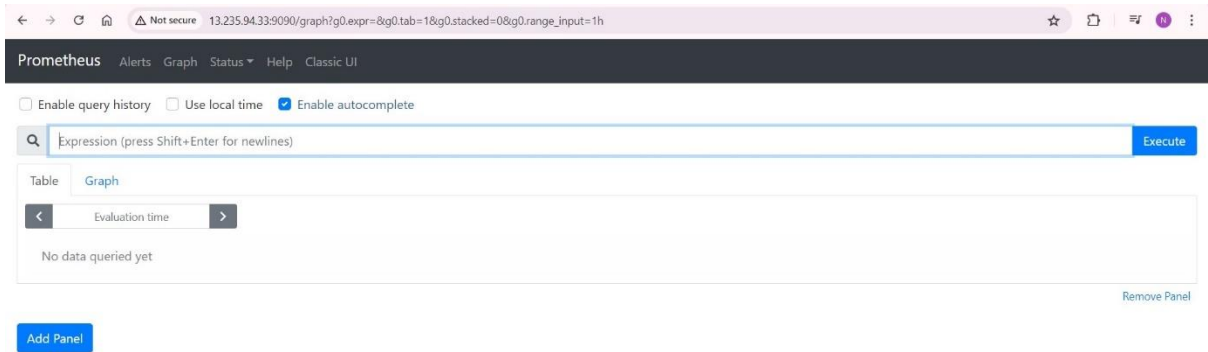
Monitoring Status: Cloudwatch Alarm:



Cloudwatch Metrics:



Prometheus and Grafana Status:



← → ↻ 🏠 ⚠ Not secure 13.235.94.33:9090/service-discovery ☆ 🗑 📄 📌 ⋮

Prometheus Alerts Graph Status ▾ Help Classic UI

Service Discovery

• prometheus (1 / 1 active targets)

prometheus [Show logs](#)

Discovered Labels

address	65.0.6.238:9100
metrics_path	/metrics
scheme	http
job	prometheus

Target Labels

instance	65.0.6.238:9100
job	prometheus

Target Server in which Application is running:

← → ↻ 🏠 ⚠ Not secure 13.235.94.33:9090/targets ☆ 🗑 📄 📌 ⋮

Prometheus Alerts Graph Status ▾ Help Classic UI

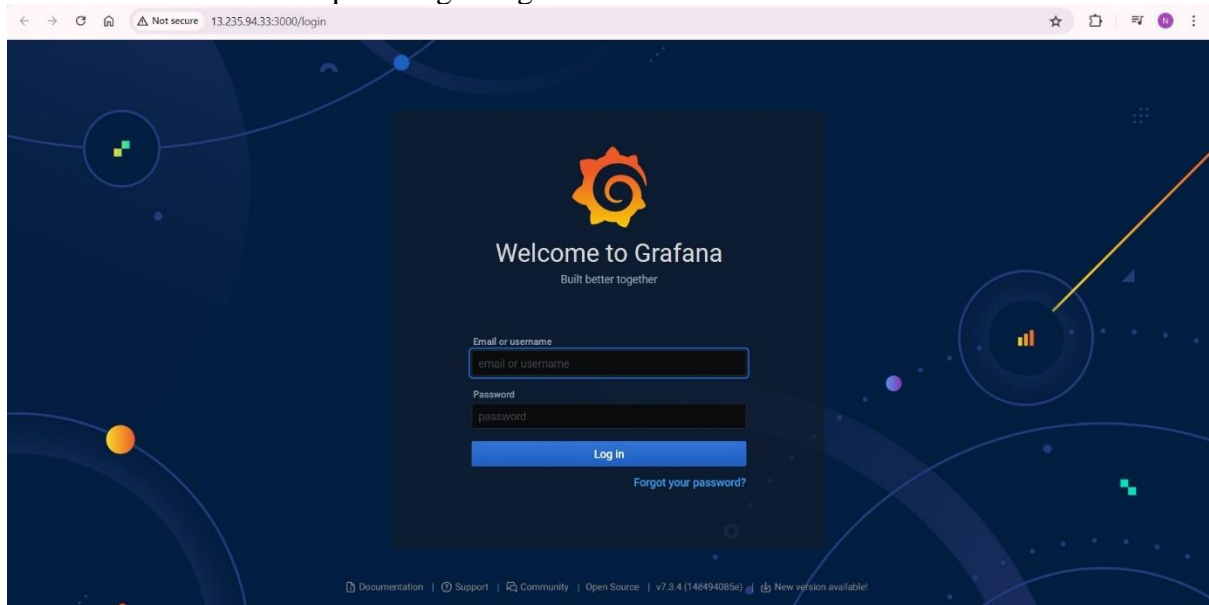
Targets

All Unhealthy

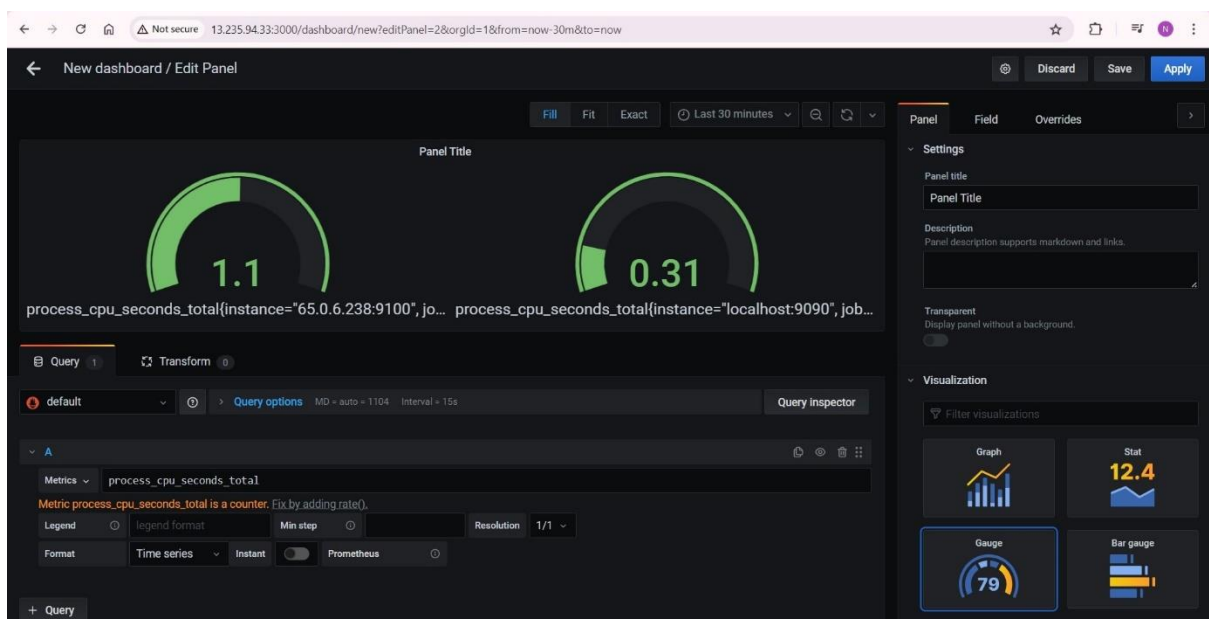
prometheus (1/1 up) [Show logs](#)

Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
http://65.0.6.238:9100/metrics	UP	instance="65.0.6.238:9100" job="prometheus"	-2.294s	30.226ms	

Grafana Visualization Report: Login Page:



CPU Utilization:



Memory Utilization:

