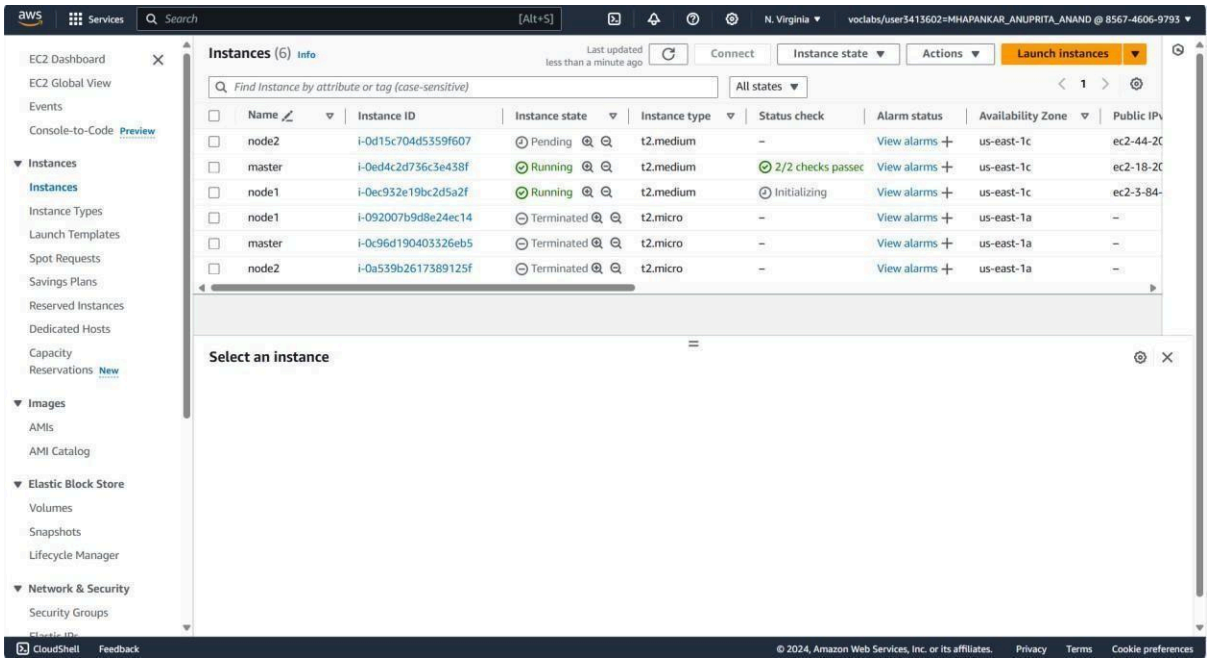
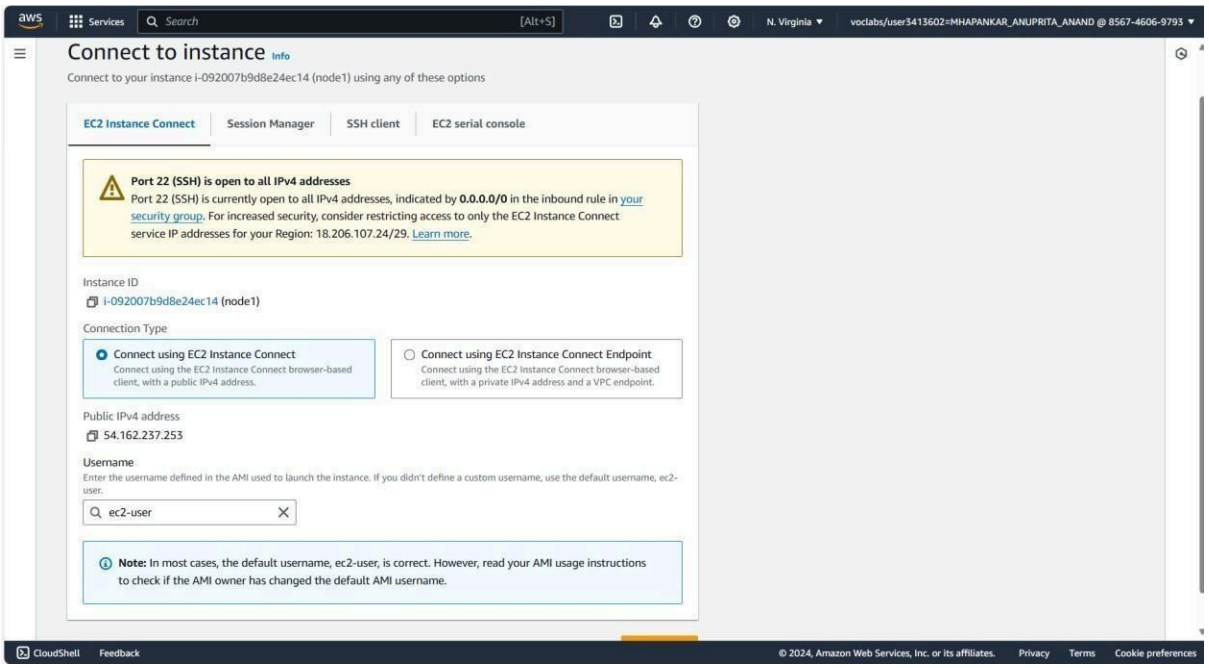
Advanced DevOps Experiment 3

Aim: To understand the Kubernetes Cluster Architecture, install and Spin Up a Kubernetes Cluster on Linux Machines/Cloud Platforms.

Step 1: Go to AWS Academia in services select EC2 and create 3 instance with instance type t2.medium and names as node1, node2 and master





Step 2: Select and connect each instance and run the following commands inside the console of each instance.

sudo su

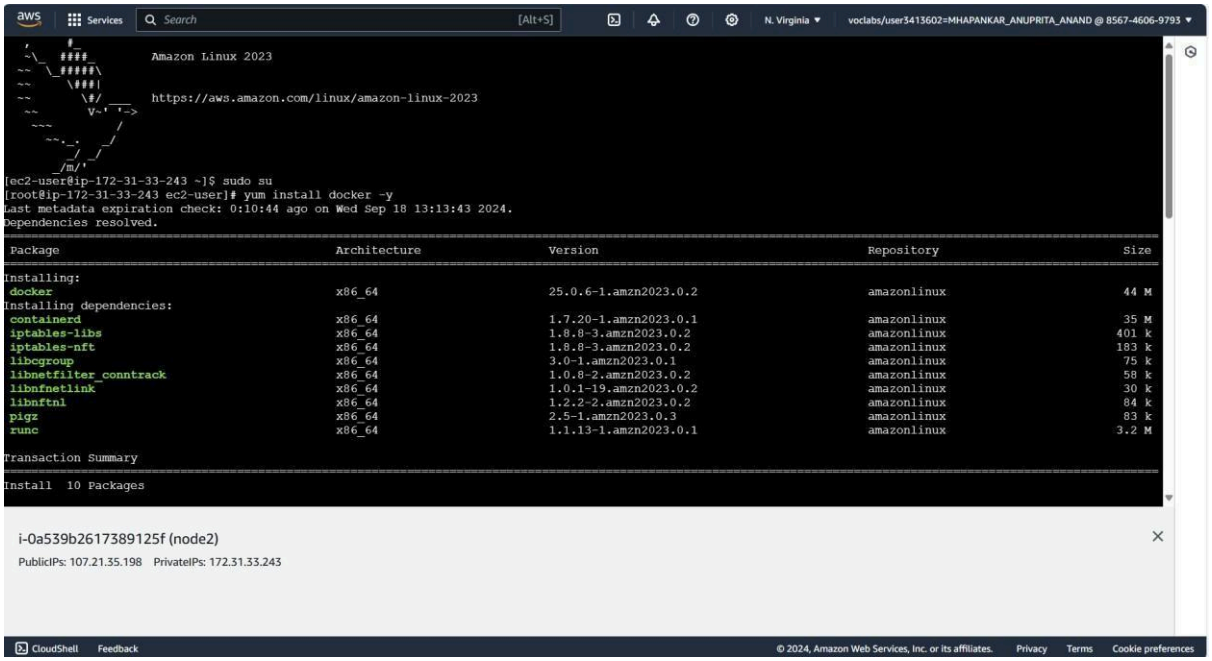
yum install docker -y

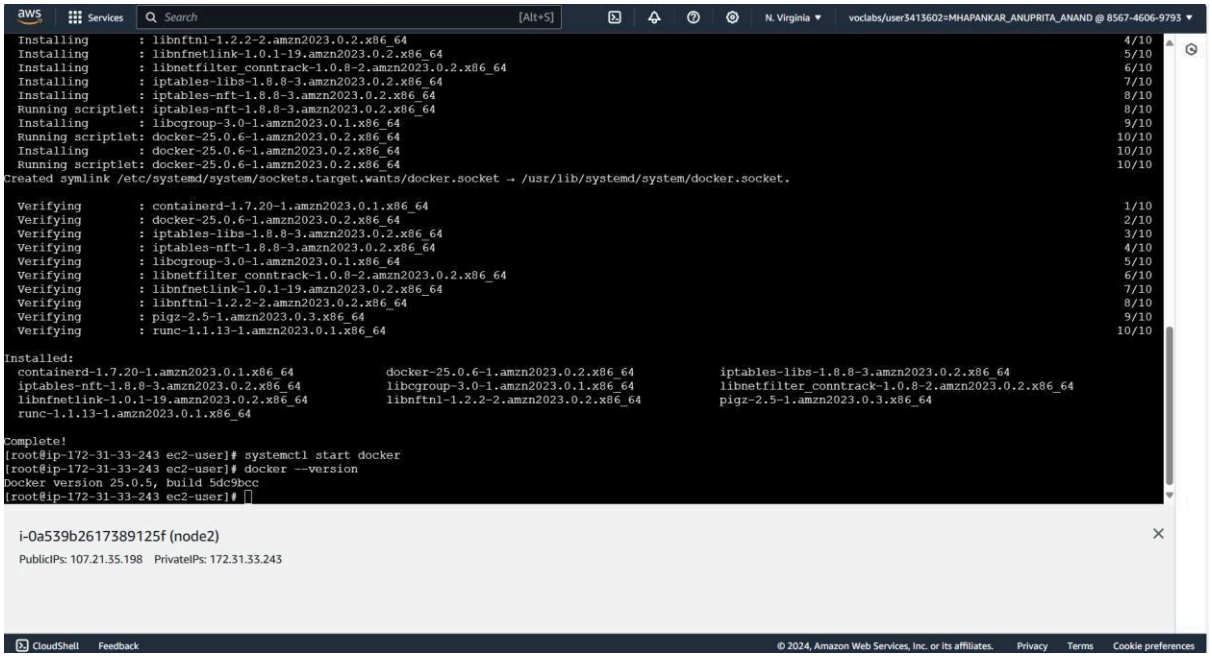
systemctl start

docker docker

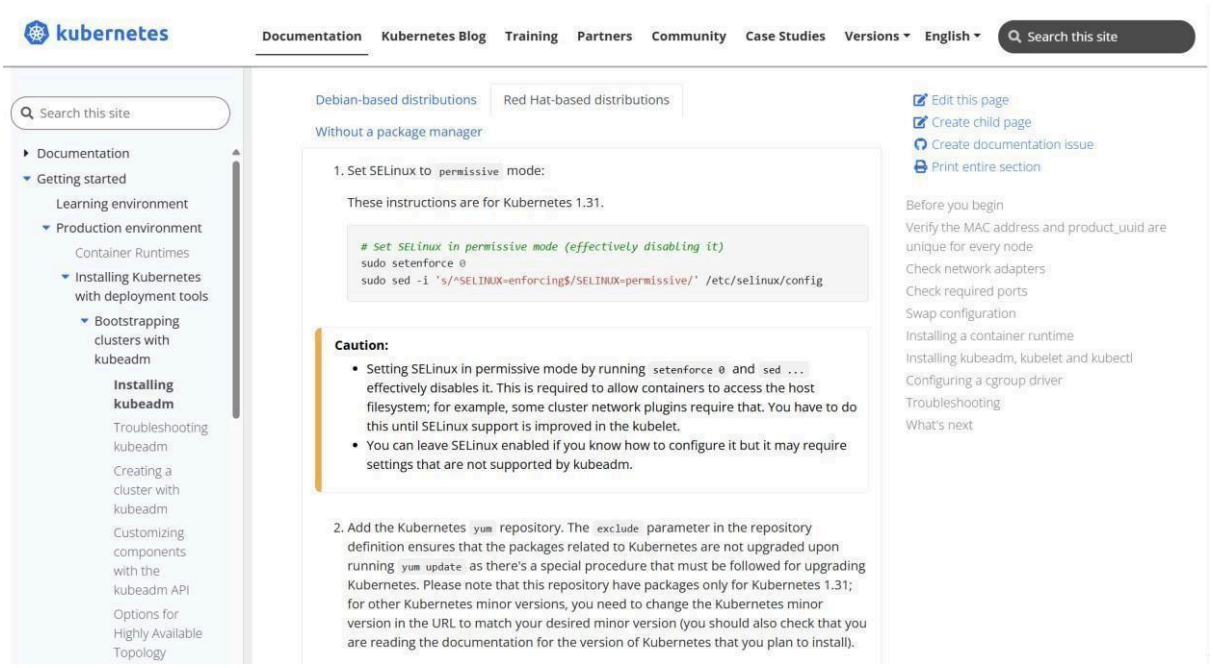
–version

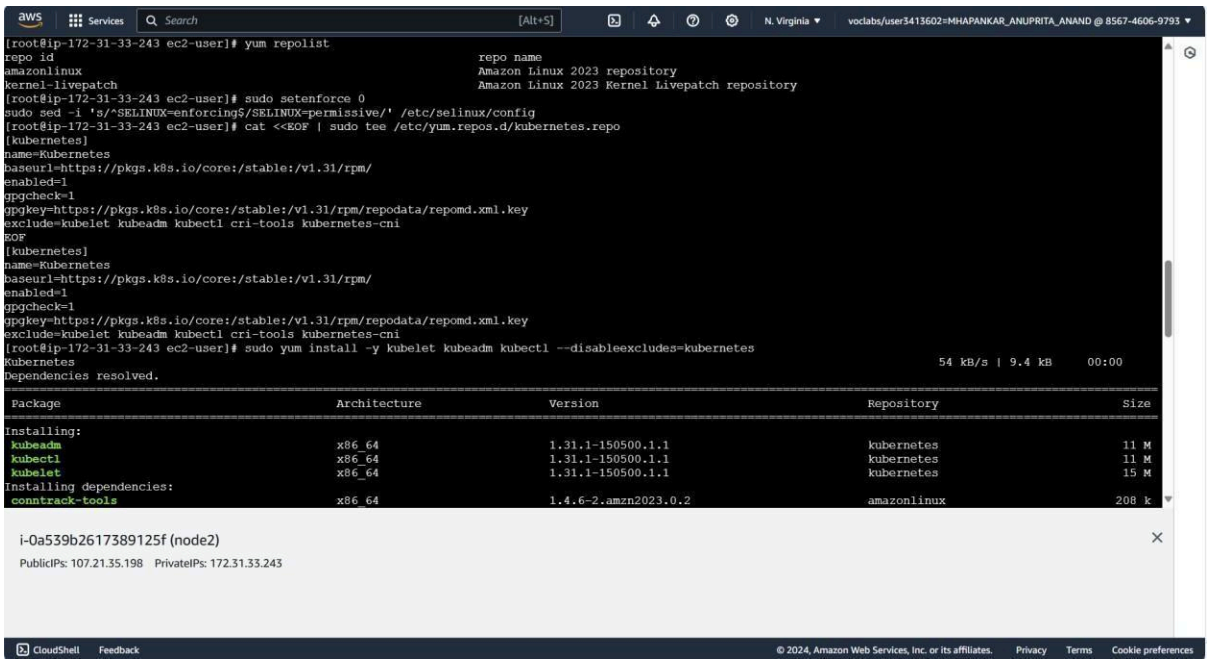
yum repolist

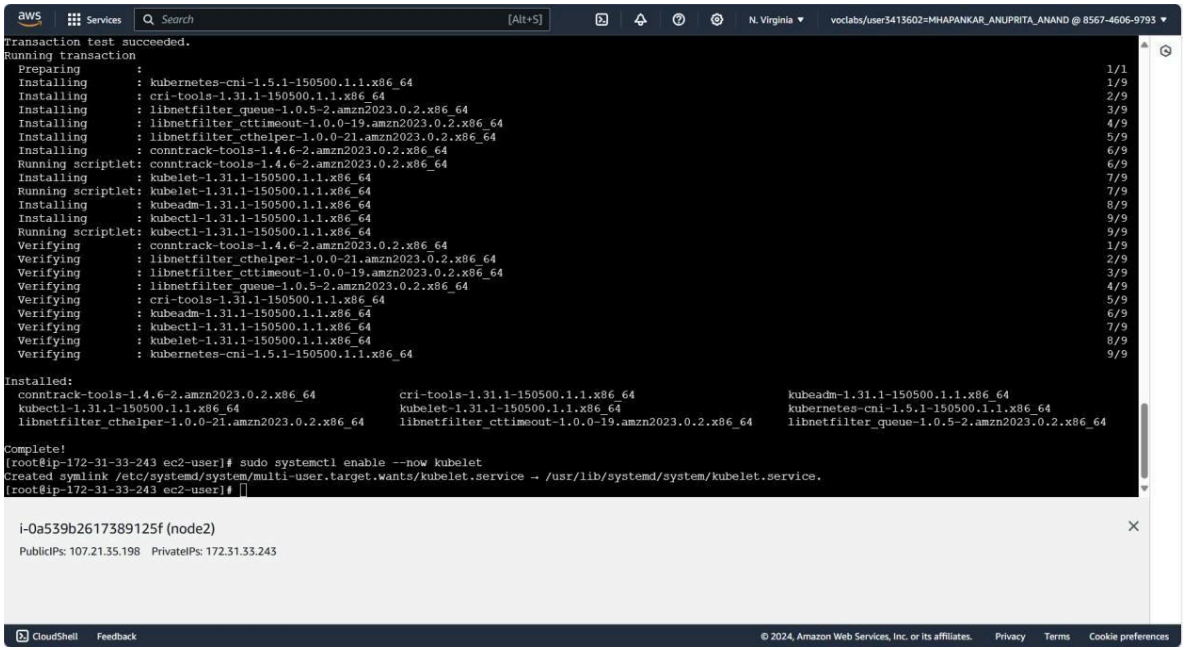




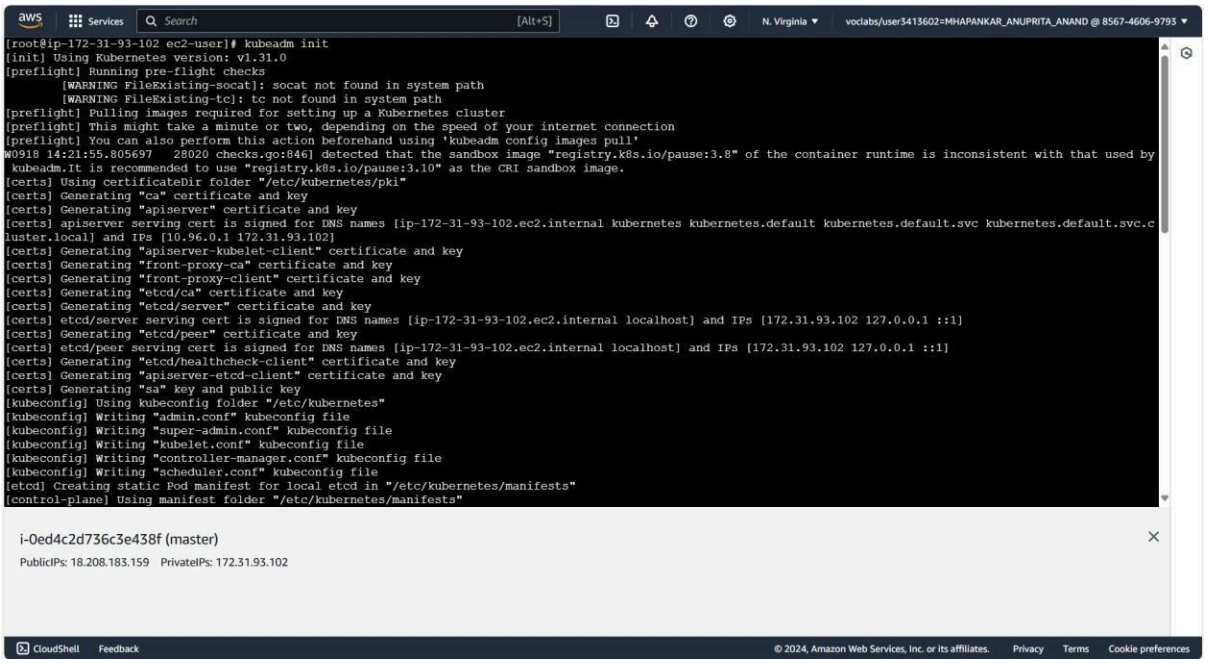
Step 3: Now, go to the following link https://kubernetes.io/docs/setup/production-environment/tools/kubeadm/install-kubeadm/ and scroll down and select Red-Hat based distributions tab copy all the commands on by one in each console of instance.


kubernetes
Documentation
Kubernetes Blog
Training
Partners
Community
Case Studies
Versions
English
Search this site
Search this site
Documentation
Getting started
Learning environment
Production environment
Container Runtimes
Installing Kubernetes with deployment tools
Bootstrapping clusters with kubeadm
Installing kubeadm
Troubleshooting kubeadm
Creating a cluster with kubeadm
Customizing components with the kubeadm API
Options for Highly Available Topology
Debian-based distributions
Red Hat-based distributions
Without a package manager
1. Set SELinux to permissive mode:
These instructions are for Kubernetes 1.31.
# Set SELinux in permissive mode (effectively disabling it)
sudo setenforce 0
sudo sed -i 's/^SELINUX=enforcing$/SELINUX=permissive/' /etc/selinux/config
Caution:
Setting SELinux in permissive mode by running setenforce 0 and sed ... effectively disables it. This is required to allow containers to access the host filesystem; for example, some cluster network plugins require that. You have to do this until SELinux support is improved in the kubelet.
You can leave SELinux enabled if you know how to configure it but it may require settings that are not supported by kubeadm.
2. Add the Kubernetes yum repository. The exclude parameter in the repository definition ensures that the packages related to Kubernetes are not upgraded upon running yum update as there's a special procedure that must be followed for upgrading Kubernetes. Please note that this repository have packages only for Kubernetes 1.31; for other Kubernetes minor versions, you need to change the Kubernetes minor version in the URL to match your desired minor version (you should also check that you are reading the documentation for the version of Kubernetes that you plan to install).
Edit this page
Create child page
Create documentation issue
Print entire section
Before you begin
Verify the MAC address and product_uuid are unique for every node
Check network adapters
Check required ports
Swap configuration
Installing a container runtime
Installing kubeadm, kubelet and kubectl
Configuring a cgroup driver
Troubleshooting
What's next


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793
[root@ip-172-31-33-243 ec2-user]# yum repolist
repo id repo name
amazonlinux Amazon Linux 2023 repository
kernel-livepatch Amazon Linux 2023 Kernel Livepatch repository
[root@ip-172-31-33-243 ec2-user]# sudo setenforce 0
sudo sed -i 's/^SELINUX=enforcing$/SELINUX=permissive/' /etc/selinux/config
[root@ip-172-31-33-243 ec2-user]# cat <<EOF | sudo tee /etc/yum.repos.d/kubernetes.repo
[kubernetes]
name=Kubernetes
baseurl=https://pkgs.k8s.io/core:/stable:/v1.31/rpm/
enabled=1
gpgcheck=1
gpgkey=https://pkgs.k8s.io/core:/stable:/v1.31/rpm/repodata/repomd.xml.key
exclude=kubelet kubeadm kubectl cri-tools kubernetes-cni
EOF
[kubernetes]
name=Kubernetes
baseurl=https://pkgs.k8s.io/core:/stable:/v1.31/rpm/
enabled=1
gpgcheck=1
gpgkey=https://pkgs.k8s.io/core:/stable:/v1.31/rpm/repodata/repomd.xml.key
exclude=kubelet kubeadm kubectl cri-tools kubernetes-cni
[root@ip-172-31-33-243 ec2-user]# sudo yum install -y kubelet kubeadm kubectl --disableexcludes=kubernetes
Kubernetes 54 kB/s | 9.4 kB 00:00
Dependencies resolved.
Package Architecture Version Repository Size
Installing:
kubeadm x86_64 1.31.1-150500.1.1 kubernetes 11 M
kubectl x86_64 1.31.1-150500.1.1 kubernetes 11 M
kubelet x86_64 1.31.1-150500.1.1 kubernetes 15 M
Installing dependencies:
conntrack-tools x86_64 1.4.6-2.amzn2023.0.2 amazonlinux 208 k
i-0a539b2617389125f (node2)
PublicIPs: 107.21.35.198 PrivateIPs: 172.31.33.243
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

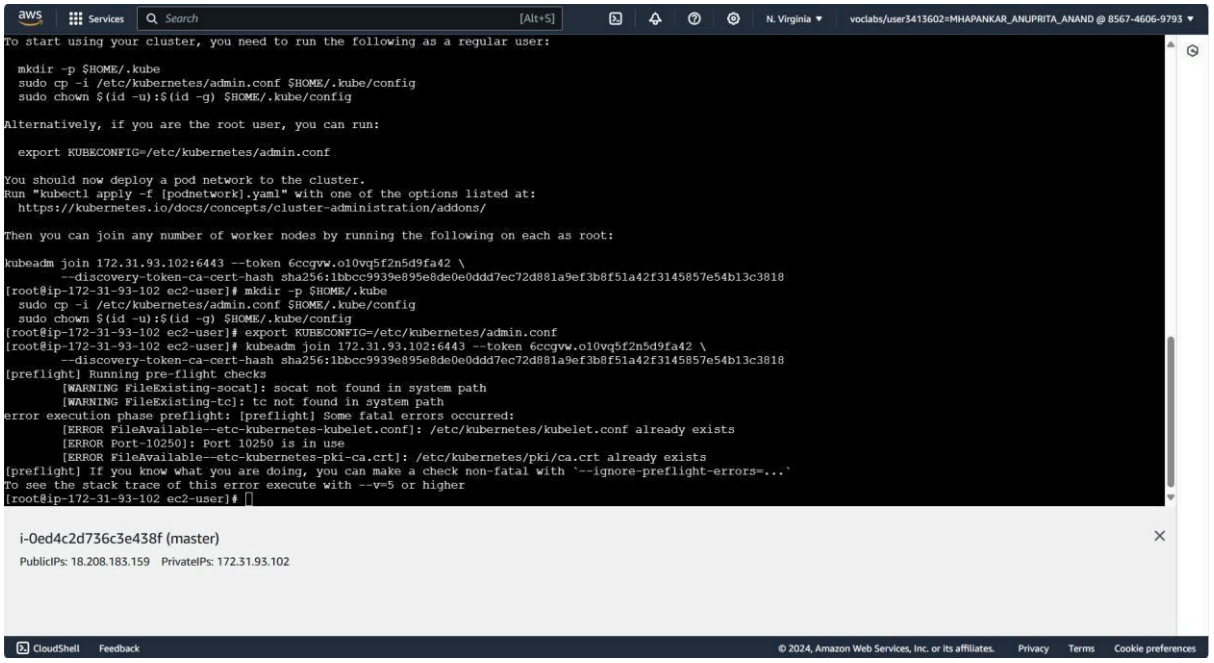

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793
Transaction test succeeded.
Running transaction
Preparing :
Installing : kubernetes-cni-1.5.1-150500.1.1.x86_64
Installing : cri-tools-1.31.1-150500.1.1.x86_64
Installing : libnetfilter_queue-1.0.5-2.amzn2023.0.2.x86_64
Installing : libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64
Installing : libnetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64
Installing : conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64
Running scriptlet: conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64
Installing : kubelet-1.31.1-150500.1.1.x86_64
Running scriptlet: kubelet-1.31.1-150500.1.1.x86_64
Installing : kubeadm-1.31.1-150500.1.1.x86_64
Installing : kubectl-1.31.1-150500.1.1.x86_64
Running scriptlet: kubectl-1.31.1-150500.1.1.x86_64
Verifying : conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64
Verifying : libnetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64
Verifying : libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64
Verifying : libnetfilter_queue-1.0.5-2.amzn2023.0.2.x86_64
Verifying : cri-tools-1.31.1-150500.1.1.x86_64
Verifying : kubeadm-1.31.1-150500.1.1.x86_64
Verifying : kubectl-1.31.1-150500.1.1.x86_64
Verifying : kubelet-1.31.1-150500.1.1.x86_64
Verifying : kubernetes-cni-1.5.1-150500.1.1.x86_64
Installed:
conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64 cri-tools-1.31.1-150500.1.1.x86_64 kubeadm-1.31.1-150500.1.1.x86_64
kubectl-1.31.1-150500.1.1.x86_64 kubelet-1.31.1-150500.1.1.x86_64 kubernetes-cni-1.5.1-150500.1.1.x86_64
libnetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64 libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64 libnetfilter_queue-1.0.5-2.amzn2023.0.2.x86_64
Complete!
[root@ip-172-31-33-243 ec2-user]# sudo systemctl enable --now kubelet
Created symlink /etc/systemd/system/multi-user.target.wants/kubelet.service → /usr/lib/systemd/system/kubelet.service.
[root@ip-172-31-33-243 ec2-user]#
i-0a539b2617389125f (node2)
PublicIPs: 107.21.35.198 PrivateIPs: 172.31.33.243
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 4: Now, run the following command in the mater instance -
kubeadm init

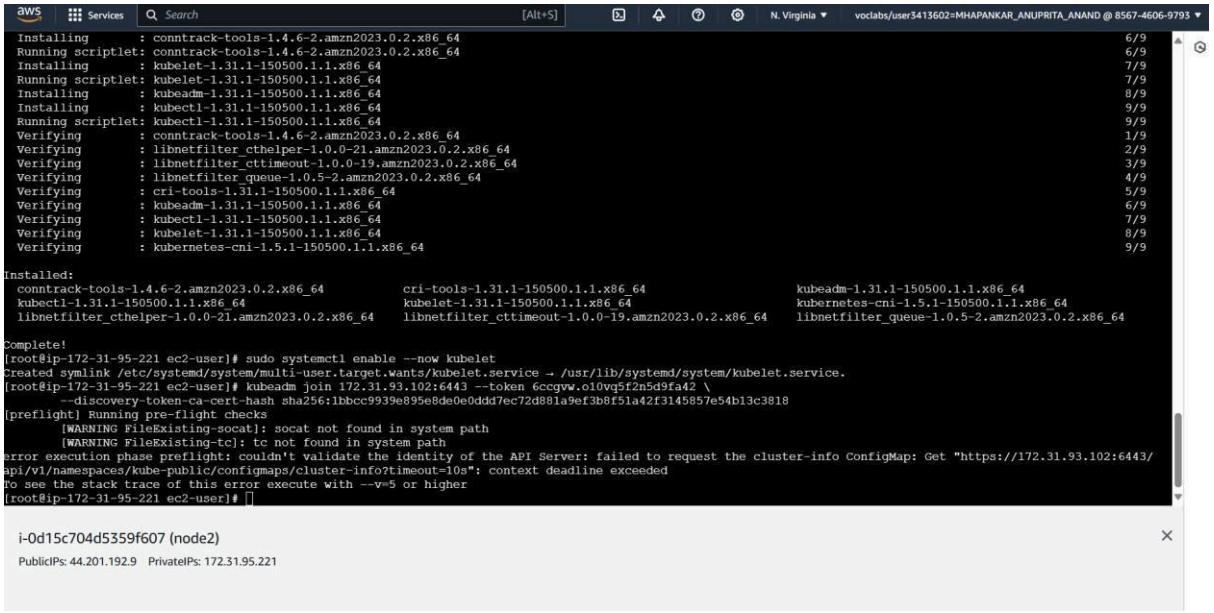


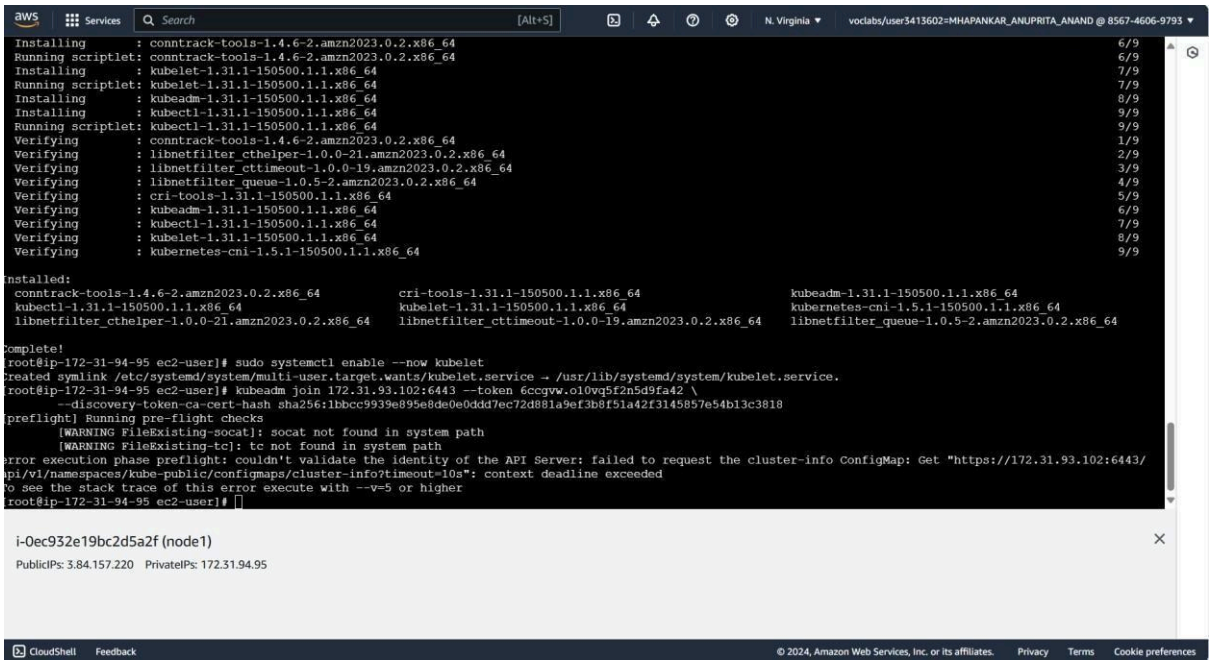
Step 5: Now, run the following commands in master instance's console –

a. mkdir -p $HOME/.kube
   sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
   sudo chown $(id -u):$(id -g) $HOME/.kube/config
b. export KUBECONFIG=/etc/kubernetes/admin.conf
c. kubeadm join 172.31.93.102:6443 --token 6ccgvw.o10vq5f2n5d9fa42 \
   --discovery-token-ca-cert-hash
   sha256:1bbcc9939e895e8de0e0ddd7ec72d881a9ef3b8f51a42f3145857e54b13c3818

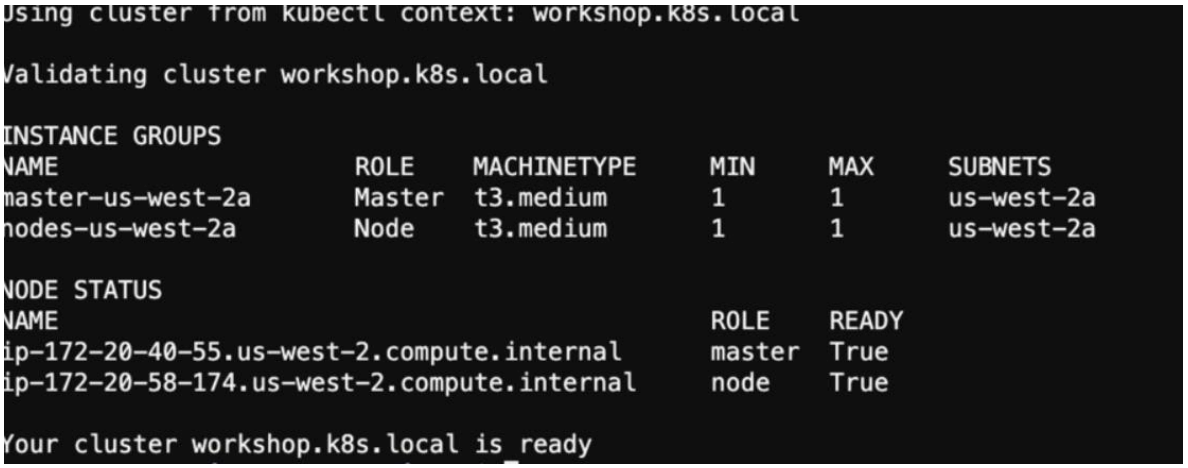


Step 6: Run this command in node1 and node2 -
kubeadm join 172.31.93.102:6443 --token 6ccgvw.o10vq5f2n5d9fa42 \
--discovery-token-ca-cert-hash sha256:1bbcc9939e895e8de0e0ddd7ec72d881a9ef3b8f51a42f3145857e54b13c3818





Step 7: Run the following command in master instance console -
kubectl get nodes

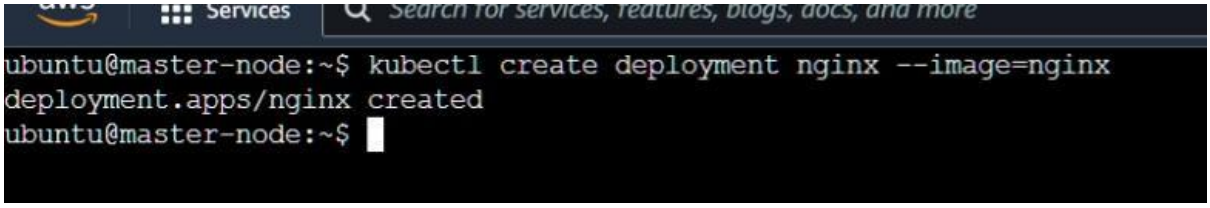


ADVANCE DEVOPS EXP 4

Aim :- To install Kubectl and execute Kubectl commands to manage the Kubernetes cluster and deploy Your First Kubernetes Application

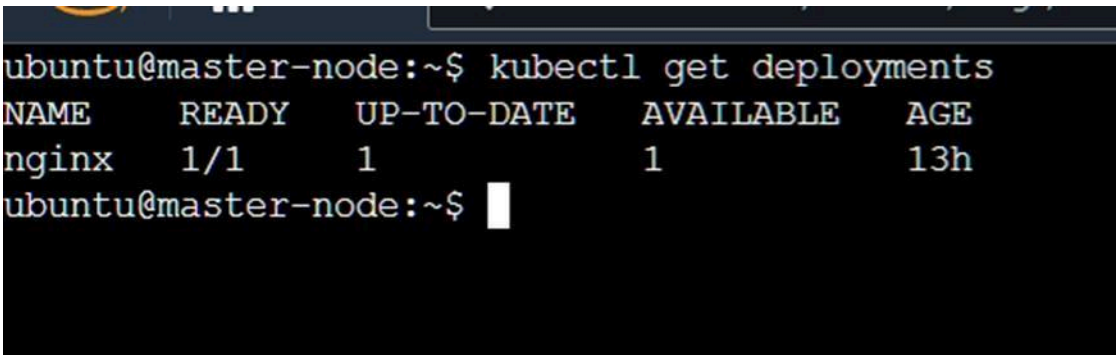
Step 1: As the cluster is up and running, we can deploy our nginx server on this cluster. Apply this deployment file using this command to create a deployment.

$kubectl create deployment nginx --image=nginx



Step 2: Verify the deployment using the command:

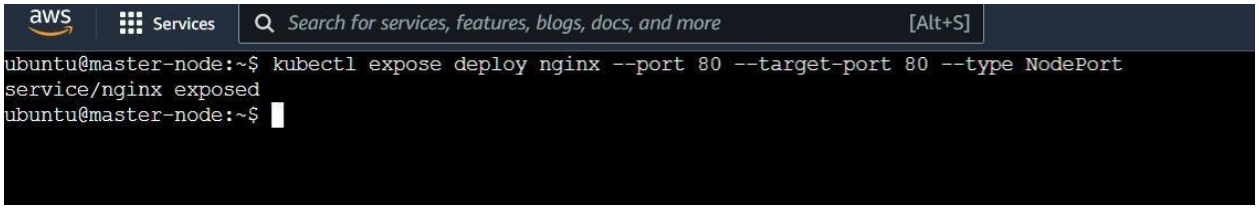
$kubectl get deployments



Step 3: Next, run the following command to create a service named nginx that will expose the app publicly. It will do so through a NodePort, a scheme that will make the pod accessible through an arbitrary port opened on each node of the cluster

with this service-type, Kubernetes will assign this service on ports on the **30000+** range.

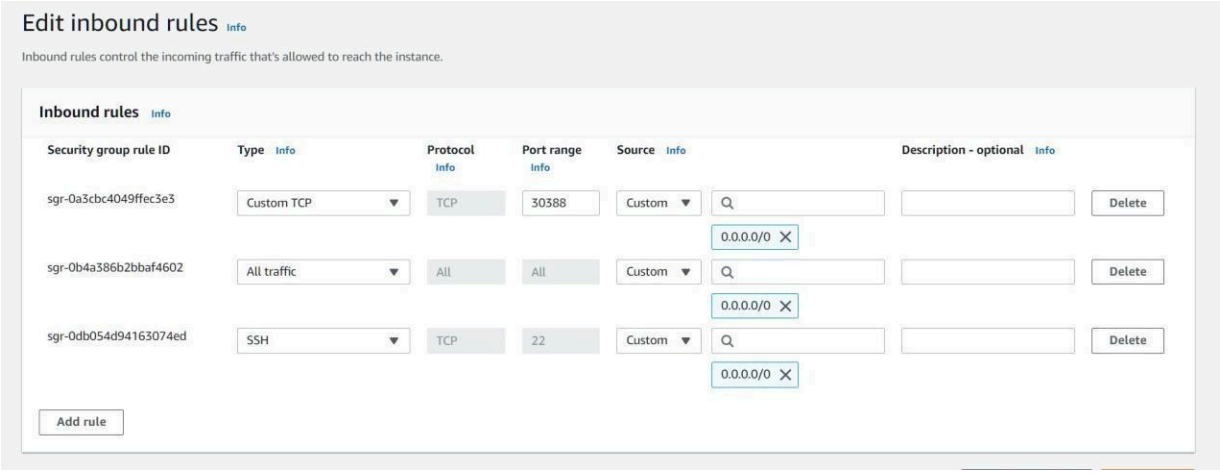
$kubectl expose deploy nginx --port 80 --target-port 80 --type NodePort



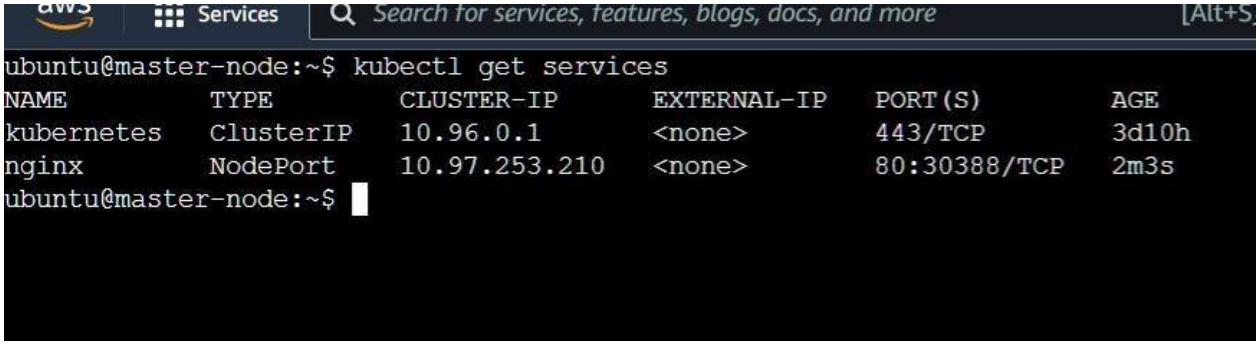
Step 4: Run this command to see a summary of the service and the ports exposed.

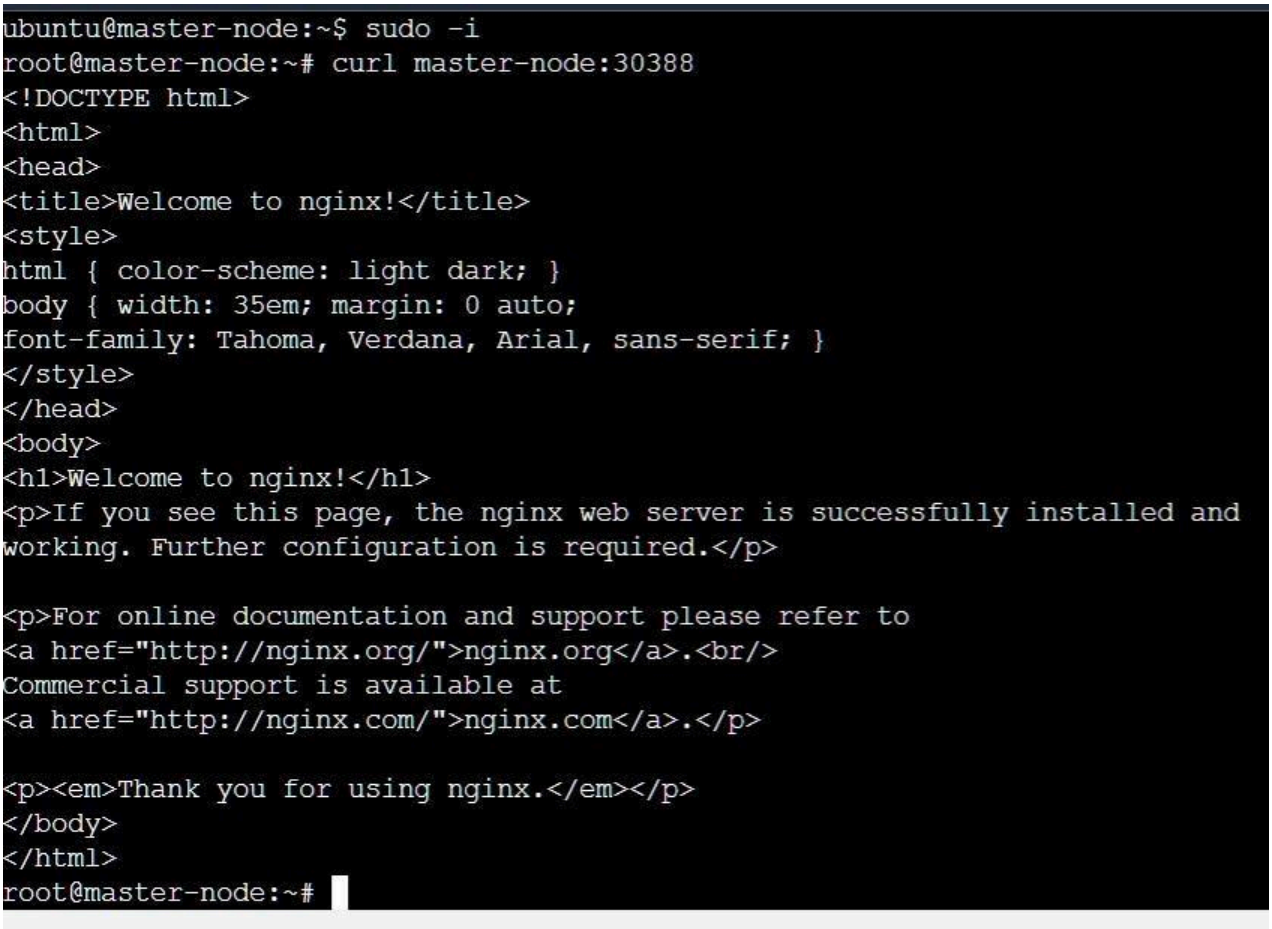
$kubectl get services

Step 5: Add the port which is displayed i.e. 30388 (in our case) in the inbound rules of the security group.



Step 6: Now you can verify that the Nginx page is reachable on all nodes using thecurl command.

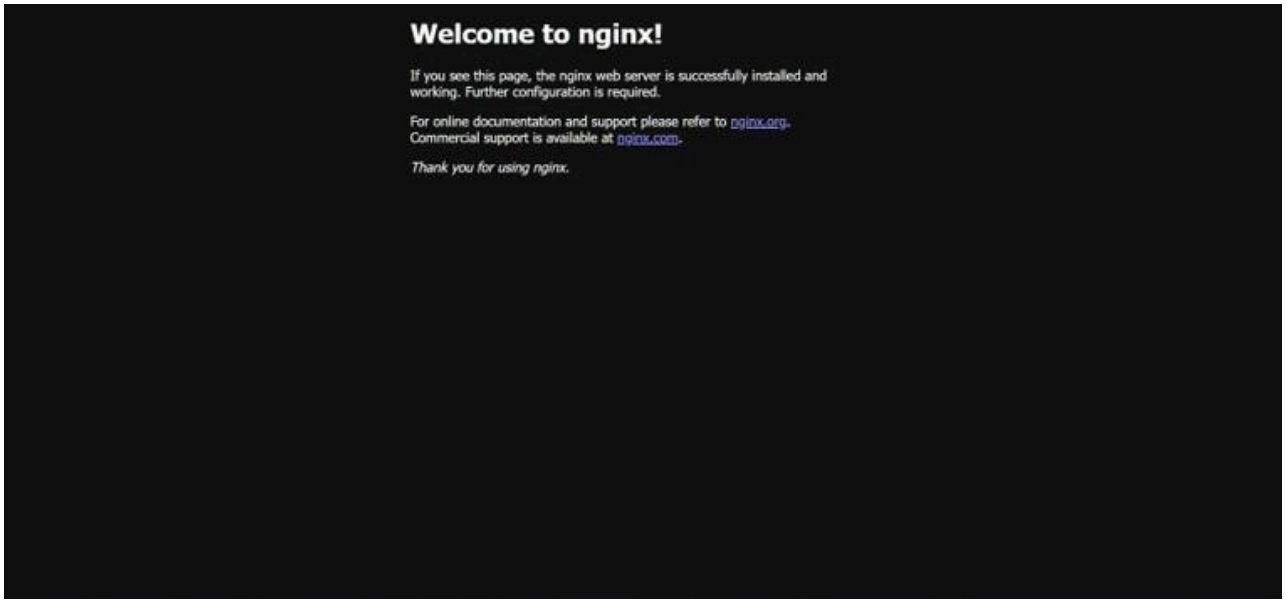




As you can see, the "**WELCOME TO NGINX!**" page can be reached.

Step 7: To test that everything is working, visithttp://worker_1_ip:nginx_port or http://worker_2_ip:nginx_port
through a browser on your local machine. You will see Nginx's familiar welcomepage.

http://52.90.129.234:30388

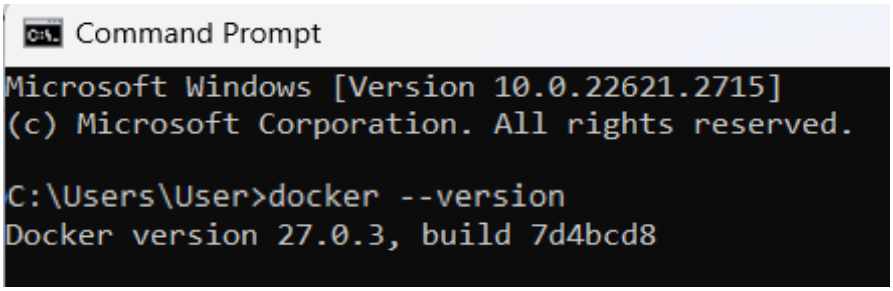


ADVANCE DEVOPS EXP 6

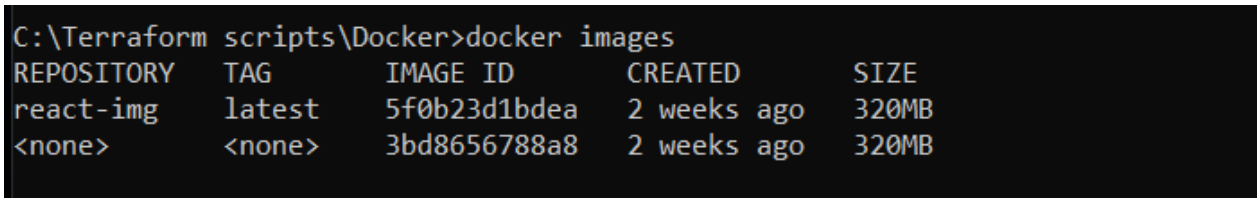
Vedang Wajge **D15A/66**

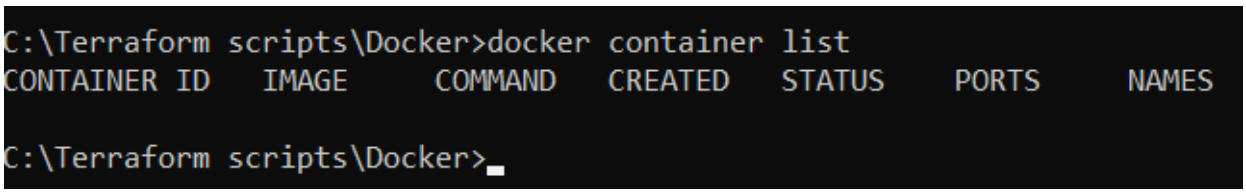
Aim:- To Build, change, and destroy AWS / GCP /Microsoft Azure/ DigitalOcean infrastructure Using Terraform. (S3 bucket or Docker) fdp

Docker Installation:



Before using terraform commands:





Code:

docker.tf

```
terraform {
        required_providers {
        docker = {
        source = "kreuzwerker/docker"
        version = "~> 3.0.1"
        }
    }
}
provider "docker" {
    host = "npipe:////.//pipe//docker_engine"
}
resource "docker_image" "nginx" {
    name = "nginx:latest"
    keep_locally = false
}
resource "docker_container" "nginx" {
    image = docker_image.nginx.image_id
    name = "tutorial"
    ports {
    internal = 80
    external = 8000
    }
}
```

Terraform Commands:

```
PS C:\Terraform scripts\Docker> terraform init
Initializing the backend...
Initializing provider plugins...
- Finding kreuzwerker/docker versions matching "~> 3.0.1"...
- Installing kreuzwerker/docker v3.0.2...
- Installed kreuzwerker/docker v3.0.2 (self-signed, key ID BD080C4571C6104C)
Partner and community providers are signed by their developers.
If you'd like to know more about provider signing, you can read about it here:
https://www.terraform.io/docs/cli/plugins/signing.html
Terraform has created a lock file .terraform.lock.hcl to record the provider
selections it made above. Include this file in your version control repository
so that Terraform can guarantee to make the same selections by default when
you run "terraform init" in the future.

Terraform has been successfully initialized!
```

```
PS C:\Terraform scripts\Docker> terraform plan

Terraform used the selected providers to generate the following execution plan. Resou
  + create

Terraform will perform the following actions:

  # docker_container.nginx will be created
  + resource "docker_container" "nginx" {
      + attach                                      = false
      + bridge                                      = (known after apply)
      + command                                     = (known after apply)
      + container_logs                              = (known after apply)
      + container_read_refresh_timeout_milliseconds = 15000
      + entrypoint                                  = (known after apply)
      + env                                         = (known after apply)
      + exit_code                                   = (known after apply)
      + hostname                                    = (known after apply)
      + id                                          = (known after apply)
```

```
PS C:\Terraform scripts\Docker> terraform apply

Terraform used the selected providers to generate the following execution plan.
  + create

Terraform will perform the following actions:

  # docker_container.nginx will be created
  + resource "docker_container" "nginx" {
      + attach                                      = false
      + bridge                                      = (known after apply)
      + command                                     = (known after apply)
      + container_logs                              = (known after apply)
      + container_read_refresh_timeout_milliseconds = 15000
```

```
  Enter a value: yes

docker_image.nginx: Creating...
docker_image.nginx: Still creating... [10s elapsed]
docker_image.nginx: Still creating... [20s elapsed]
docker_image.nginx: Still creating... [30s elapsed]
docker_image.nginx: Creation complete after 38s [id=sha256:5ef79149e0ec84a7a9f9284c3f91aa3c20608f8391f5445eabe92ef07dbda0
docker_container.nginx: Creating...
docker_container.nginx: Creation complete after 1s [id=19c3b26e694e3b26a5daa18288d68c790f0168d547f94171a49e3491bd173ae9]

Apply complete! Resources: 2 added, 0 changed, 0 destroyed.
PS C:\Terraform scripts\Docker>
```

After using Terraform commands:

```
C:\Terraform scripts\Docker>docker images
REPOSITORY   TAG       IMAGE ID       CREATED        SIZE
nginx        latest    5ef79149e0ec   12 days ago    188MB
react-img    latest    5f0b23d1bdea   2 weeks ago    320MB
<none>       <none>    3bd8656788a8   2 weeks ago    320MB
```

```
C:\Terraform scripts\Docker>docker container list
CONTAINER ID   IMAGE          COMMAND                  CREATED         STATUS             PORTS                   NAMES
19c3b26e694e   5ef79149e0ec   "/docker-entrypoint.…"   2 minutes ago   Up About a minute   0.0.0.0:8000->80/tcp   tutorial

C:\Terraform scripts\Docker>
```

To Delete the Containers created:

```
PS C:\Terraform scripts\Docker> terraform destroy
docker_image.nginx: Refreshing state... [id=sha256:5ef79149e0ec84a7a9f9284c3f91aa3c20608f8391f5445eabe92ef07dbda03
docker_container.nginx: Refreshing state... [id=19c3b26e694e3b26a5daa18288d68c790f0168d547f94171a49e3491bd173ae9]

Terraform used the selected providers to generate the following execution plan. Resource actions are indicated wit
  - destroy

Terraform will perform the following actions:

  # docker_container.nginx will be destroyed
  - resource "docker_container" "nginx" {
      - attach                                      = false -> null
      - command                                     = [
```

Vedang V. Wajge

D15A/66

Adv. Devops Assignment 1

Using S3 Bucket Video Streaming

a) Create an S3 bucket
Sign in to aws and select create bucket, enter appropriate name and choose region and for Block Public Access for this bucket, keep default settings. Choose Create Bucket

b) Upload a video to the S3 Bucket.
To upload a file to the bucket open the created bucket and on objects tab, choose upload, then select files and folders and Add Files. Select open and locate file then choose Upload.

c) Create a CloudFront origin access identity
To create a cloud Front OAI, sign in to the AWS Management Console, under the Security Section, choose Origin acces. Under the identities tab, choose Create origin access identity. Choose create.

d) Create a cloudfront distribution.
To use Cloud Front to serve and distribute the video in your S3 Bucket, you must create a Cloud Front distribution.

e) Access the S3 video through the CloudFront distribution with the custom domain name.
We can access this video through that custom URL created and SSL certificate for safety and security is also assigned.

Q.2 BMW and Hotstar on AWS Services.

→ On 15 Nov, 2023 when India was playi against New Zealand at the World Cup semifinal match in Wankhede Stadium i Mumbai more than 5 core people were watching the match on Hotstar apps on global level. AWS serves as the primary hosting provider for Disney. It relies on AWS as the backbone of their hosting, an provide details about the infrastructure, inclu the use of AWS instance during high impact events. It offers a scalable and reliable clou computing platform, and allow Disney to mana their infrastructure based on demand.

One of the best known names in the automotive industry, BMW Group has been providing premium driving experiences of millio of customers since 1916. Always at the forefront of innovation, it has now develope a groundbreaking In-Console Cloud Assistanc solution in collaboration with AWS. Part of the company's infrastructure optimization progra the ICCA is empowering BMW Group DevOps wit generative AI to boost performance and efficiency. With access to large language mod (LLM) and with data encrypted in transit an at rest - BMW Group can securely deliver high-quality connected mobility solutions.

Teacher's Sign.:

Kubernetes and how industries use it.

Kubernetes, commonly referred to K8's, it is like a manager for your computer programs. Imagine you have a bunch of different programs running on your computer. They need to work together, and sometimes you want to run more copies of a program when things get busy. This can be hard to do manually, like trying to juggle a lot of balls at once. Addidas is a globally renowned sportswear and athletic footwear company headquatered in Germany. Founded in 1949, it offers a wide range of sports-related product, collaborates with subsidiary brands like Rebok, focuses on innovation in athletic footwear technology, and maintains a strong global presence. Adidas is committed to sustainability and social responsibility.

Adidas stated "we started from the developer point of view"; and looked for ways to shorten the time it took to get a project up and running and into the adidas infrastructure, says Senior Director of Platform Engineering Fernando Cornago. They found the solution with containerization, agile development, continous delivery, and a cloud native platform that includes Kubernetes and Prometheus.

Q-4] What are Nagios and use in E-sevices.

→ Nagios is an Open Source IT system monitoring tool. It was designed to run on the Linux OS and can monitor devices running Linux, Windows and Unix OSes. Nagios software runs periodic checks on critical parameters of application, network server resources. Nagios can monitor memory use, disk use and microprocessor load, as well as the number of currently running processes.

Bitnetix with Nagios in an IT consulting organization which is into networking, datacenter, monitoring and Voice over IP, through their offerings, they make small business look big. Their solution help you managing customer relationships in a better way by increasing more engagement and improving their satisfaction. They say they are in business of communication, hence communicate right message to their customers at right time is very important for them.

Vedang V. Wajge

DISA / 66

Adv. Devops Assignment 2 04/03/24

1) Creating a REST API with serverless framework.

Creating Rest Api with serverless framework is an efficient way to deploy serverless applications that can scale automatically without managing servey.

i) Serverless framework : A powerful tool that deployment of services and serverless applications across various app cloud providers like Aws.

ii) Serverless Architecture: This design model allows developers to build applications without worrying about underlying infrastructure, enabling focus on code.

iii) Rest Api : Representational state transfer is architecture style for designing network applications.

Steps for creating Rest Apis for serverless framework:

1) Install serverless framework
2) Creating a Node.js serveless project.
3) Project structure define.
4) Create a Rest Api Resource
5) Deploy the Service.
6) Testing the API's.
7) Storing data in Dynamic DB's
8) Adding more functionalities : 'list all candidates', etc.
9) Aws IAM Permissions.
10) Monitoring and Maintanence.

Q-2] Case study for sonarQube.
Creating own profile in sonarqube for testing project quality. Use sonarqube to analyze your Github code. Install sonarlint in your intellij id and analyze java code. Analyze python project with sonarqube.

→ Sonarqube is an open source platform used for continuous inspection of code quality.

1) Profile updation/creation in sonarqube:
Quality profiles in sonarqube are essential configurations that define rules applied during code analysis. Each project has a quality profile for every supported language with default being 'sonarqube'.

2) Using sonarcloud to analyze Github code.
Sonarqube / sonar cloud is cloud based counterpart of sonar Qube that integrates directly with Github, BitBucket, Azure and Gitlab Repos. To get started with sonarcloud via Github sign up via sonarcloud setup, complete result can be viewed in both sonar-cloud & Github including security import issue.

3) Sonarlint in Java IDE:
Sonarlint is an IDE that performs on the fly code analysis as you write code. It helps developers detect bugs, security vulnerabilities and code smells directly in the development environment such as Intellij Idea or Ellipse

4] Analyzing Python Projects with SonarQube:
Sonarqube supports Python test coverage, reporting, but it requires third party too like coverage.py to generate the coverage port. To enable coverage adjust your blind process so that coverage tool runs before sonar scanner and ensures report.

5) Analyzing Node.js projects with Sonarqube.
For node.js project sonarqube can analyze Javascript and Typescript of code similar to the python setup you can configure sonarqube to analyze node.js projects by installing the appropriate.

At a large organization, your centralized operations team may get repetitive infrastructure requests. You can use Terraform to build a 'self-serve' infrastructure.
Terraform's self-serve infrastructure provides a powerful use case in large organizations.
i) Self serve infra: By using Terraform modules, you can create reusable and standardized infrastructure config. Module creation in Terraform, main.tf, variables.tf, and outputs.tf.
Also after module creation its standardization is equally important.
ii) Enabling self-service for Product Teams:
Create a self service or version control access and

and provide pre-configured Terraform workflows onboard and train product teams, and the most important RBAC (Role based Access Control) for preventing unauthorized Access

3] Automate Infrastruct Request via Ticketing systems:

Integrate Terraform Cloud or Terraform Enterpr connect terraform with the Ticketing system, automate approval workflows and monitor & log requests.

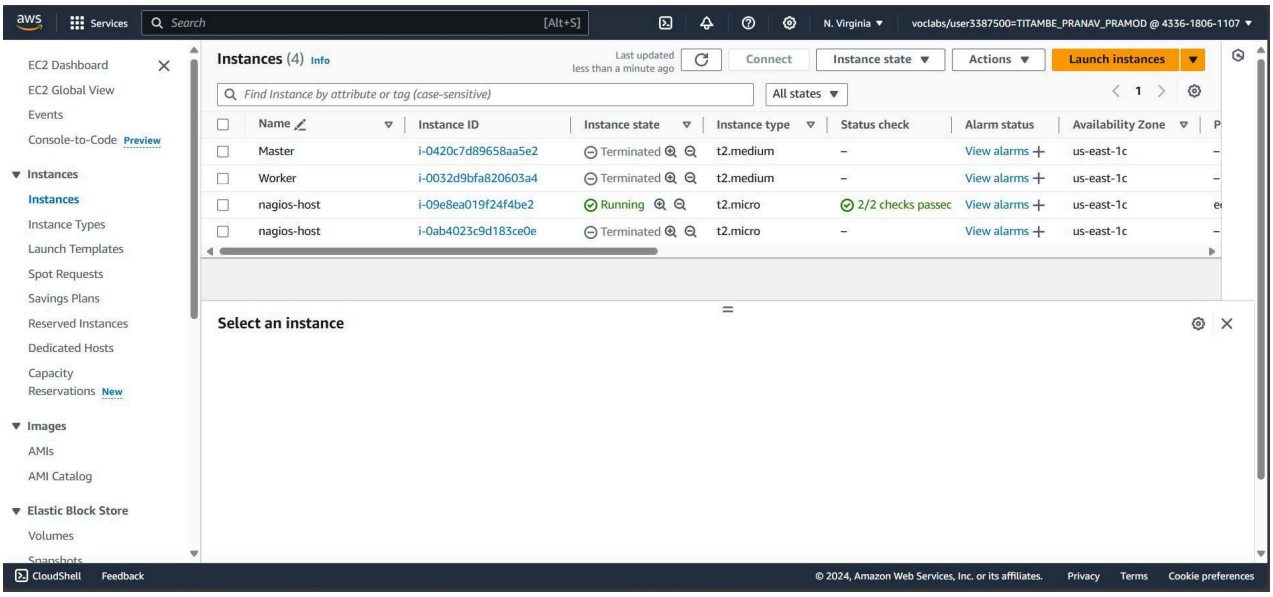
4] Workspaces setup for Environment Segregation.

To manage different environments, Terraform workspaces were set up. This ensured that teams could deploy the same infrastructure across different environments without overlap.

ADVANCE DEVOPS - 9

NAME - Vedang V. Wajge D15A 66

Create an EC2 instance at AWS



After this install following commands:-

```
sudo apt install apache2 libapache2-mod-php php php-gd libgd-dev
gcc make autoconf libssl-dev wget unzip bc gawk dc build-essential
snmp libnet-snmp-perl gettext -y
```

```
 System information as of Sat Sep 28 12:51:58 UTC 2024

  System load:  0.16              Processes:             106
  Usage of /:   10.6% of 14.46GB  Users logged in:       0
  Memory usage: 21%               IPv4 address for enX0: 172.31.89.161
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-89-161:~$ sudo apt update
```

```
ubuntu@ip-172-31-89-161:~$ sudo apt install apache2 php
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapache2-mod-php8.3 libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap
  libaprutil1t64 liblua5.4-0 php-common php8.3 php8.3-cli php8.3-common php8.3-opcache php8.3-readline ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser php-pear
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapache2-mod-php8.3 libapr1t64 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libaprutil1t64 liblua5.4-0 php php-common php8.3 php8.3-cli php8.3-common php8.3-opcache
  php8.3-readline ssl-cert
0 upgraded, 18 newly installed, 0 to remove and 143 not upgraded.
Need to get 6998 kB of archives.
After this operation, 30.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libapr1t64 amd64 1.7.2-3.1ubuntu0.1 [108 k
B]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.1ubuntu7 [91.9 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.3-1.1ubuntu7 [11
.2 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-ldap amd64 1.6.3-1.1ubuntu7 [9116 B]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 liblua5.4-0 amd64 5.4.6-3build2 [166 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-bin amd64 2.4.58-1ubuntu8.4 [1329
kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-data all 2.4.58-1ubuntu8.4 [163 kB
]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-utils amd64 2.4.58-1ubuntu8.4 [97.
1 kB]
```

```
ubuntu@ip-172-31-89-161:~$ sudo apt install gcc build-essential
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu bzip2 cpp cpp-13 cpp-13-x86-64-linux-gnu cpp-x86-64-linux-gnu
  dpkg dpkg-dev fakeroot fontconfig-config fonts-dejavu-core fonts-dejavu-mono g++ g++-13 g++-13-x86-64-linux-gnu
  g++-x86-64-linux-gnu gcc-13 gcc-13-base gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu libalgorithm-diff-perl
  libalgorithm-diff-xs-perl libalgorithm-merge-perl libaom3 libasan8 libatomic1 libbinutils libbz2-1.0 libc-bin
  libc-dev-bin libc-devtools libc6 libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libde265-0 libdeflate0
  libdpkg-perl libfakeroot libfile-fcntllock-perl libfontconfig1 libgcc-13-dev libgd3 libgomp1 libgprofng0
  libheif-plugin-aomdec libheif-plugin-aomenc libheif-plugin-libde265 libheif1 libhwasan0 libisl23 libitm1 libjbig0
  libjpeg-turbo8 libjpeg8 liblerc4 liblsan0 libmpc3 libquadmath0 libsframe1 libsharpyuv0 libstdc++-13-dev libtiff6
  libtsan2 libubsan1 libwebp7 libxpm4 linux-libc-dev linux-tools-common locales lto-disabled-list make manpages-dev
  rpcsvc-proto
Suggested packages:
  binutils-doc gprofng-gui bzip2-doc cpp-doc gcc-13-locales cpp-13-doc debsig-verify debian-keyring g++-multilib
  g++-13-multilib gcc-13-doc gcc-multilib autoconf automake libtool flex bison gdb gcc-doc gcc-13-multilib
  gdb-x86-64-linux-gnu glibc-doc libnss-nis libnss-nisplus bzr libgd-tools libheif-plugin-x265
  libheif-plugin-ffmpegdec libheif-plugin-jpegdec libheif-plugin-jpegenc libheif-plugin-j2kdec libheif-plugin-j2kenc
  libheif-plugin-rav1e libheif-plugin-svtenc libstdc++-13-doc make-doc
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential bzip2 cpp cpp-13 cpp-13-x86-64-linux-gnu
  cpp-x86-64-linux-gnu dpkg-dev fakeroot fontconfig-config fonts-dejavu-core fonts-dejavu-mono g++ g++-13
  g++-13-x86-64-linux-gnu g++-x86-64-linux-gnu gcc gcc-13 gcc-13-base gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu
  libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libaom3 libasan8 libatomic1 libbinutils
  libc-dev-bin libc-devtools libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libde265-0 libdeflate0 libdpkg-perl
  libfakeroot libfile-fcntllock-perl libfontconfig1 libgcc-13-dev libgd3 libgomp1 libgprofng0 libheif-plugin-aomdec
  libheif-plugin-aomenc libheif-plugin-libde265 libheif1 libhwasan0 libisl23 libitm1 libjbig0 libjpeg-turbo8 libjpeg8
  liblerc4 liblsan0 libmpc3 libquadmath0 libsframe1 libsharpyuv0 libstdc++-13-dev libtiff6 libtsan2 libubsan1 libwebp7
```

```
ubuntu@ip-172-31-89-161:~$ sudo apt install libgd-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libgd-dev is already the newest version (2.3.3-9ubuntu5).
0 upgraded, 0 newly installed, 0 to remove and 119 not upgraded.
ubuntu@ip-172-31-89-161:~$
```

Use this command to setup a new user called as nagios and adding it to nagcmd user group

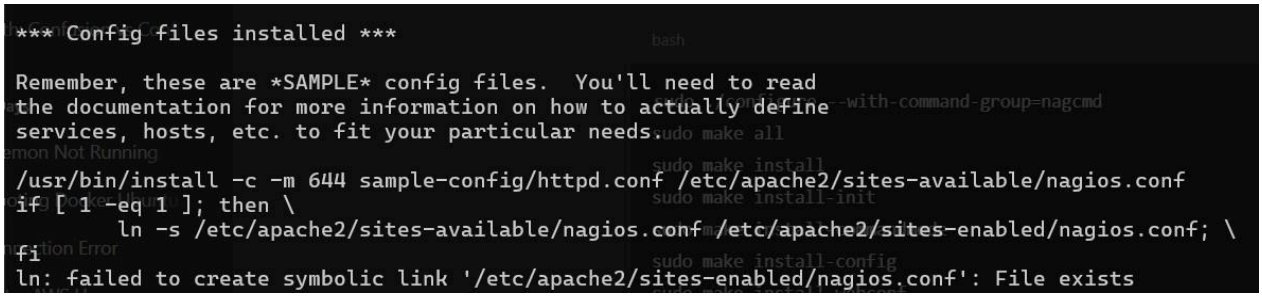
```
sudo useradd nagios
sudo groupadd nagcmd
sudo usermod -aG nagcmd nagios
sudo usermod -aG nagcmd www-data
```

Now download and install nagios core

```
cd
/tmp
wget
https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.
6. tar.gz
tar -zxvf nagios-*.tar.gz
cd nagios-4.4.6
```

Now compile and install nagios

```
sudo ./configure --with-command-group=nagcmd
sudo make all
sudo make install
sudo make install-init
sudo make install-commandmode
sudo make install-config
sudo make install-webconf
```



Now install Nagios plugins.

```
cd /tmp
wget
https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz tar
-zxvf nagios-plugins-*.tar.gz
cd nagios-plugins-2.3.3
sudo ./configure --with-nagios-user=nagios --with-nagios-group=nagios
sudo make
sudo make install
```

```
 GNU nano 7.2                          /usr/local/nagios/etc/objects/contacts.cfg *

# Just one contact defined by default - the Nagios admin (that's you)
# This contact definition inherits a lot of default values from the
# 'generic-contact' template which is defined elsewhere.

define contact {

    contact_name            nagiosadmin             ; Short name of user
    use                     generic-contact         ; Inherit default values from generic-contact template (defined abo>
    alias                   Nagios Admin            ; Full name of user
    email                   pranavtitambe04@gmail.com ; <****** CHANGE THIS TO YOUR EMAIL ADDRESS ******
}



################################################################################
#
# CONTACT GROUPS
#
################################################################################

# We only have one contact in this simple configuration file, so there is
# no need to create more than one contact group.

define contactgroup {

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy
```

Here by executing this command you need to set the password for ‘nagiosadmin’

```
sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

```
ubuntu@ip-172-31-89-161:/tmp/nagios-plugins-2.3.3$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
ubuntu@ip-172-31-89-161:/tmp/nagios-plugins-2.3.3$ sudo a2enmod rewrite
sudo a2enmod cgi
sudo systemctl restart apache2
Module rewrite already enabled
Module cgi already enabled
ubuntu@ip-172-31-89-161:/tmp/nagios-plugins-2.3.3$
```

Set proper permissions for the configuration:

```
sudo a2enmod rewrite
sudo a2enmod cgi
sudo systemctl restart apache2
```

```
ubuntu@ip-172-31-89-161:~$ sudo a2enmod rewrite
sudo a2enmod cgi
sudo systemctl restart apache2
Module rewrite already enabled
Module cgi already enabled
ubuntu@ip-172-31-89-161:~$
```

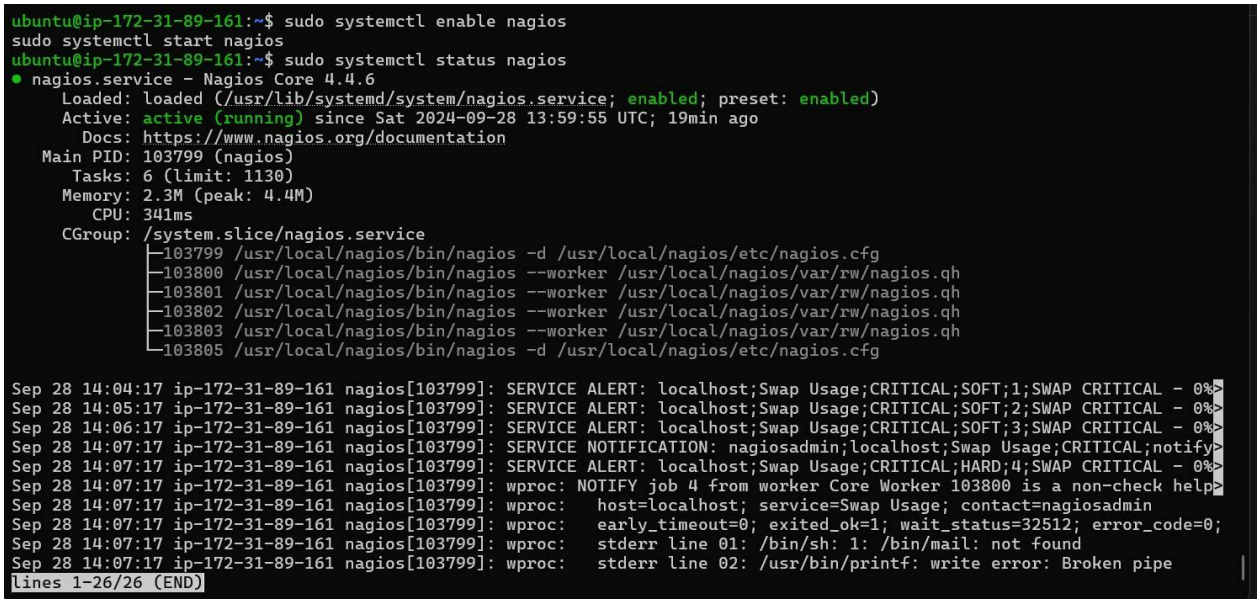
Ensure your firewall allows HTTP traffic (port 80):

```
sudo ufw allow Apache
sudo ufw reload
```

```
ubuntu@ip-172-31-89-161:~$ sudo ufw allow Apache
sudo ufw reload
Skipping adding existing rule
Skipping adding existing rule (v6)
Firewall not enabled (skipping reload)
ubuntu@ip-172-31-89-161:~$
```

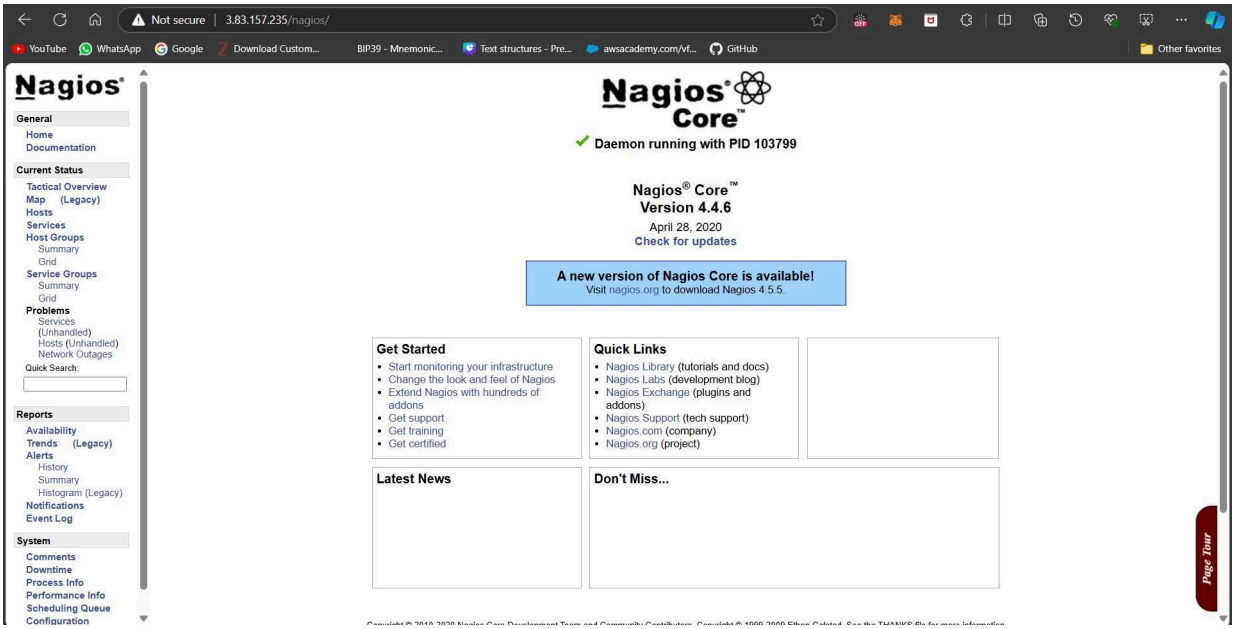
Starting the nagios services

```
sudo systemctl enable nagios
sudo systemctl start nagios
sudo systemctl status nagios
```



Here it will prompt to enter the username and password provide that we set earlier.
Go to your AWS EC2 dashboard and and copy the public ip address. The url should look like this

‘`http://<public-ip-address>/nagios`’

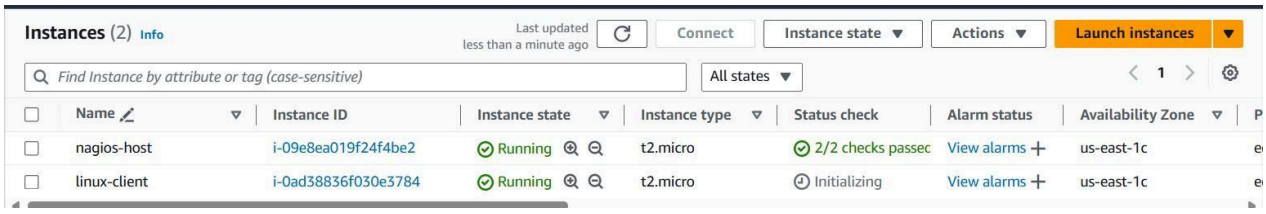

Not secure | 3.83.157.235/nagios/
YouTube
WhatsApp
Google
Download Custom...
BIP39 - Mnemonic...
Text structures - Pre...
awsacademy.com/vf...
GitHub
Other favorites
Nagios
General
Home
Documentation
Current Status
Tactical Overview
Map (Legacy)
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services (Unhandled)
Hosts (Unhandled)
Network Outages
Quick Search:
Reports
Availability
Trends (Legacy)
Alerts
History
Summary
Histogram (Legacy)
Notifications
Event Log
System
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Configuration
Nagios Core
Daemon running with PID 103799
Nagios® Core™
Version 4.4.6
April 28, 2020
Check for updates
A new version of Nagios Core is available!
Visit nagios.org to download Nagios 4.5.5.
Get Started
Start monitoring your infrastructure
Change the look and feel of Nagios
Extend Nagios with hundreds of addons
Get support
Get training
Get certified
Quick Links
Nagios Library (tutorials and docs)
Nagios Labs (development blog)
Nagios Exchange (plugins and addons)
Nagios Support (tech support)
Nagios.com (company)
Nagios.org (project)
Latest News
Don't Miss...
Page Tour

Check if the nagios service is running by executing following command

```
sudo systemctl status nagios
```

```
ubuntu@ip-172-31-89-161:~$ sudo systemctl status nagios
● nagios.service - Nagios Core 4.4.6
     Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-09-28 16:08:58 UTC; 1min 2s ago
       Docs: https://www.nagios.org/documentation
    Process: 15743 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
    Process: 15753 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
   Main PID: 15764 (nagios)
      Tasks: 6 (limit: 1130)
     Memory: 2.4M (peak: 3.2M)
        CPU: 29ms
     CGroup: /system.slice/nagios.service
             ├─15764 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─15765 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─15766 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─15767 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─15768 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─15769 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Sep 28 16:08:58 ip-172-31-89-161 nagios[15764]: qh: Socket '/usr/local/nagios/var/rw/nagios.qh' successfully initialized
Sep 28 16:08:58 ip-172-31-89-161 nagios[15764]: qh: core query handler registered
Sep 28 16:08:58 ip-172-31-89-161 nagios[15764]: qh: echo service query handler registered
Sep 28 16:08:58 ip-172-31-89-161 nagios[15764]: qh: help for the query handler registered
Sep 28 16:08:58 ip-172-31-89-161 nagios[15764]: wproc: Successfully registered manager as @wproc with query handler
Sep 28 16:08:58 ip-172-31-89-161 nagios[15764]: wproc: Registry request: name=Core Worker 15765;pid=15765
Sep 28 16:08:58 ip-172-31-89-161 nagios[15764]: wproc: Registry request: name=Core Worker 15766;pid=15766
Sep 28 16:08:58 ip-172-31-89-161 nagios[15764]: wproc: Registry request: name=Core Worker 15767;pid=15767
```

Now, create a new EC2 instance on AWS



Now perform the following commands on nagios-host EC2 instance.

On the server, run this command

```
ps -ef | grep nagios
```

```
ubuntu@ip-172-31-89-161:~$ ps -ef | grep nagios
nagios     15764       1  0 16:08 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios     15765   15764  0 16:08 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     15766   15764  0 16:08 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     15767   15764  0 16:08 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     15768   15764  0 16:08 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     15769   15764  0 16:08 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
ubuntu     15957    1342  0 16:13 pts/0    00:00:00 grep --color=auto nagios
ubuntu@ip-172-31-89-161:~$
```

Become a root user and create 2 folders

```
sudo su
mkdir /usr/local/nagios/etc/objects/monitorhosts
mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
```

```
ubuntu@ip-172-31-89-161:~$ sudo su
mkdir /usr/local/nagios/etc/objects/monitorhosts
mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
root@ip-172-31-89-161:/home/ubuntu#
```

Copy localhost.cfg file to the mentioned location

```
cp /usr/local/nagios/etc/objects/localhost.cfg
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts
```

```
root@ip-172-31-89-161:/usr/local/nagios/etc/objects# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
cp: cannot create regular file '/usr/local/nagios/etc/objects/monitorhosts/linuxhosts': No such file or directory
root@ip-172-31-89-161:/usr/local/nagios/etc/objects# sudo mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
root@ip-172-31-89-161:/usr/local/nagios/etc/objects# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
root@ip-172-31-89-161:/usr/local/nagios/etc/objects#
```

Open the nano editor for localhost.cfg file and make these changes. Add the Ip address of the linux-client for the address field.

```
nano
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/localhost.cfg
```

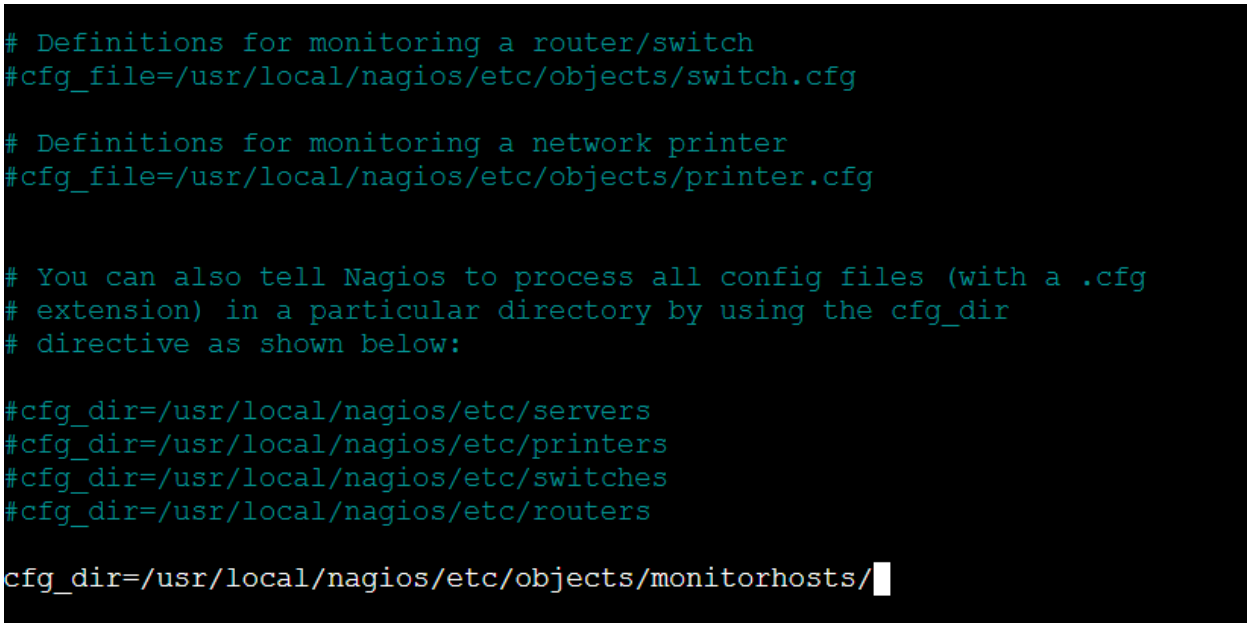
```
  GNU nano 7.2                                        /usr/local/nagios/et
##############################################################################
#
# HOST DEFINITION
#
##############################################################################

# Define a host for the local machine

define host {

    use                     linux-server            ; Name of host te
                                                    ; This host defin
                                                    ; in (or inherite
    host_name               linuxserver
    alias                   linuxserver
    address                 52.207.253.18
}



##############################################################################
#
# HOST GROUP DEFINITION

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Ex
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Ju
```

Note - Here replace hostname with linuxserver

```
nano /usr/local/nagios/etc/nagios.cfg
```

Add the following line to the nagios.cfg file

```
cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/
```



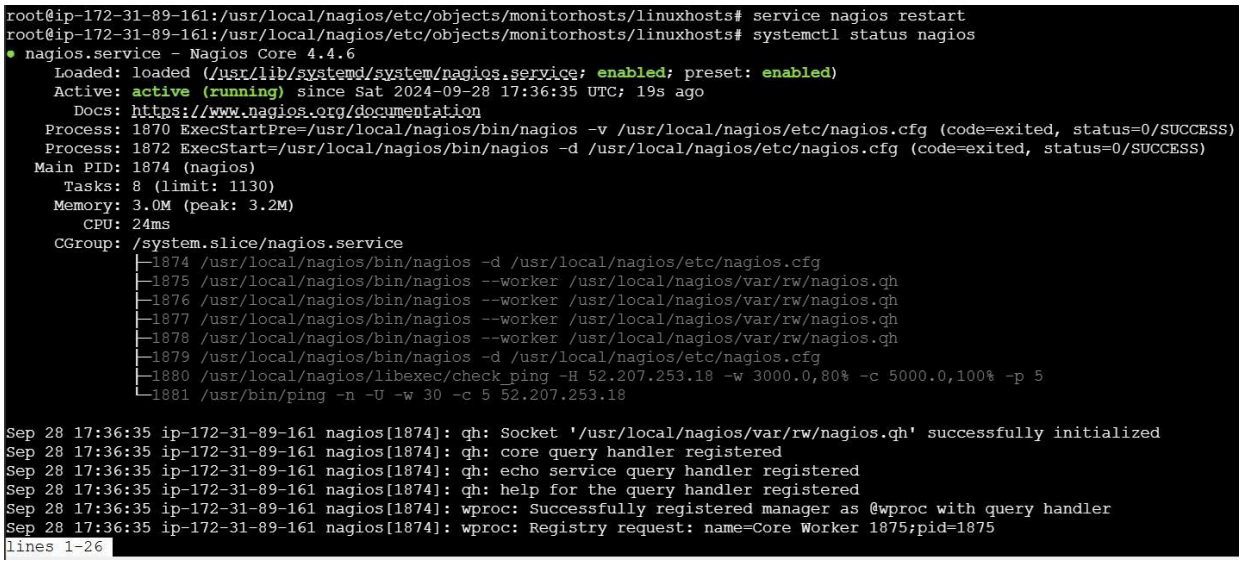
After making the changes in nagios.cfg file now check validate the file by typing the following command in the terminal.

```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

```
License: GPL

Website: https://www.nagios.org
Reading configuration data...
   Read main config file okay...
   Read object config files okay...

Running pre-flight check on configuration data...

Checking objects...
        Checked 16 services.
        Checked 2 hosts.
        Checked 2 host groups.
        Checked 0 service groups.
        Checked 1 contacts.
        Checked 1 contact groups.
        Checked 24 commands.
        Checked 5 time periods.
        Checked 0 host escalations.
        Checked 0 service escalations.
Checking for circular paths...
        Checked 2 hosts
        Checked 0 service dependencies
        Checked 0 host dependencies
        Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
root@ip-172-31-89-161:/usr/local/nagios/etc/objects/monitorhosts/linuxhosts#
```

Now restart the service by using this command

```
service nagios restart
```



Now using this command update the apt repository of ubuntu (linux-client), install gcc, nagios-nrpe-server and nagios-plugin

```
sudo apt update -y
sudo apt install gcc -y
sudo apt install -y nagios-nrpe-server nagios-plugins
```

Now open nrpe.cfg file and add the ip address of the nagios host as shown. To open the nrpe.cfg file copy this command.

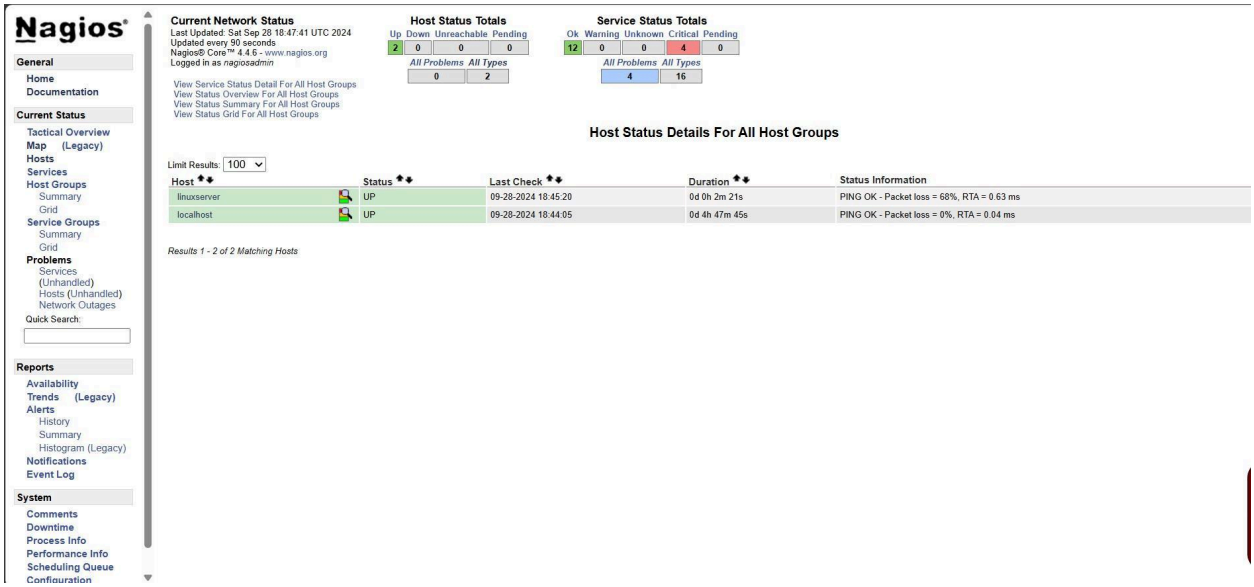
```
sudo nano /etc/nagios/nrpe.cfg
```

```
# Supported.
#
# Note: The daemon only does rudimentary checkin
# address.  I would highly recommend adding entr
# file to allow only the specified host to conne
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is runnin

allowed_hosts=127.0.0.1,54.167.169.0


# COMMAND ARGUMENT PROCESSING
# This option determines whether or not the NRPE
# to specify arguments to commands that are exec
# if the daemon was configured with the --enable
# option.
```

Now restart nrpe server by using this command

```
sudo systemctl restart nagios-nrpe-server
```

Now, check nagios dashboard, you should see linuxserver up and running, if not check security groups of the EC2 instances.

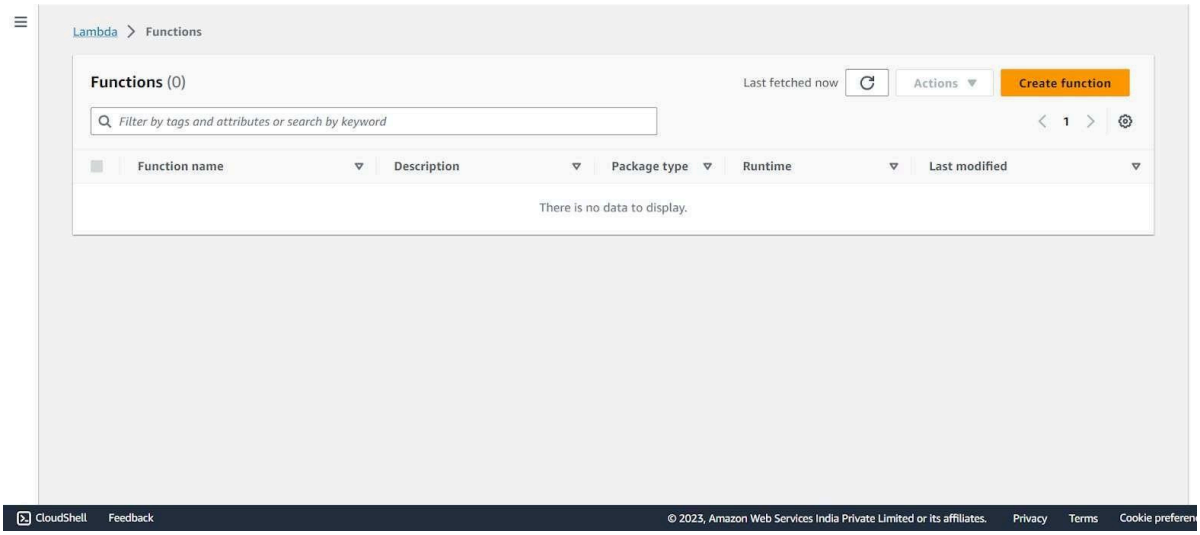


Experiment No 11

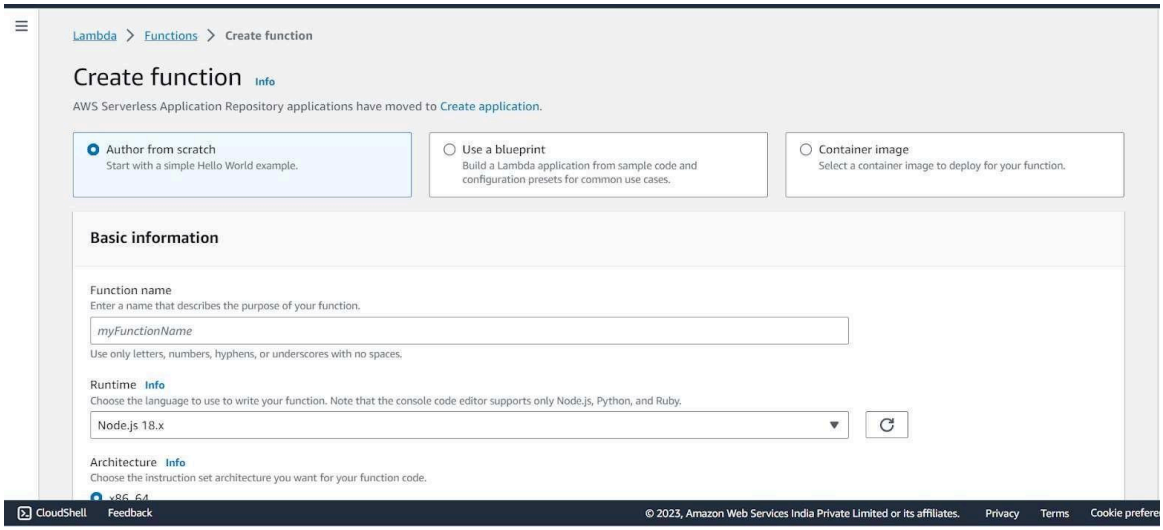
AIM: To understand AWS Lambda, its workflow, various functions and create your first Lambda functions using Python / Java / Nodejs.

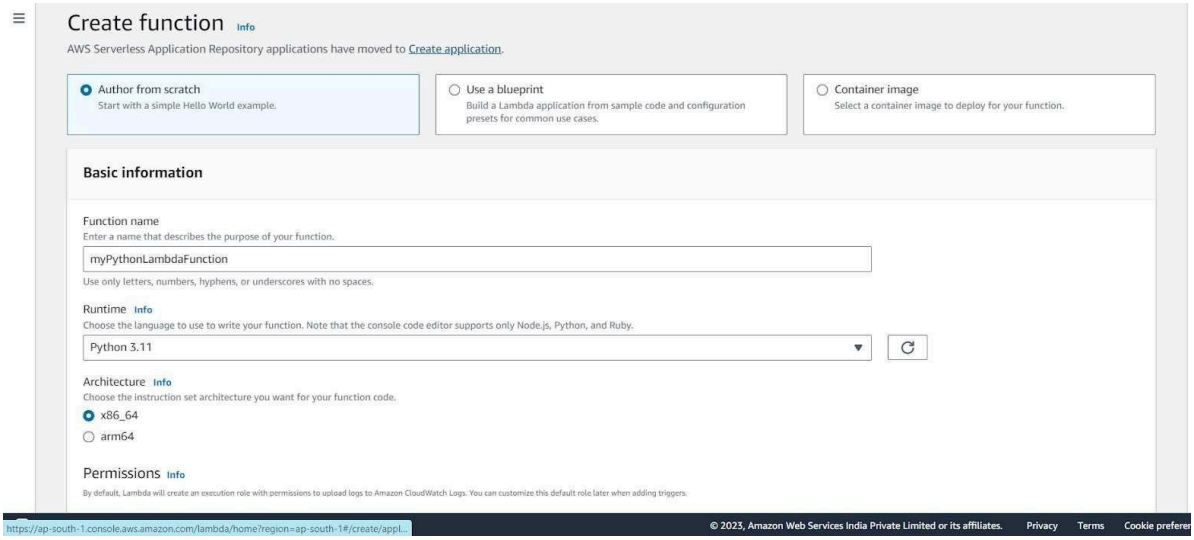
Steps to create an AWS Lambda function

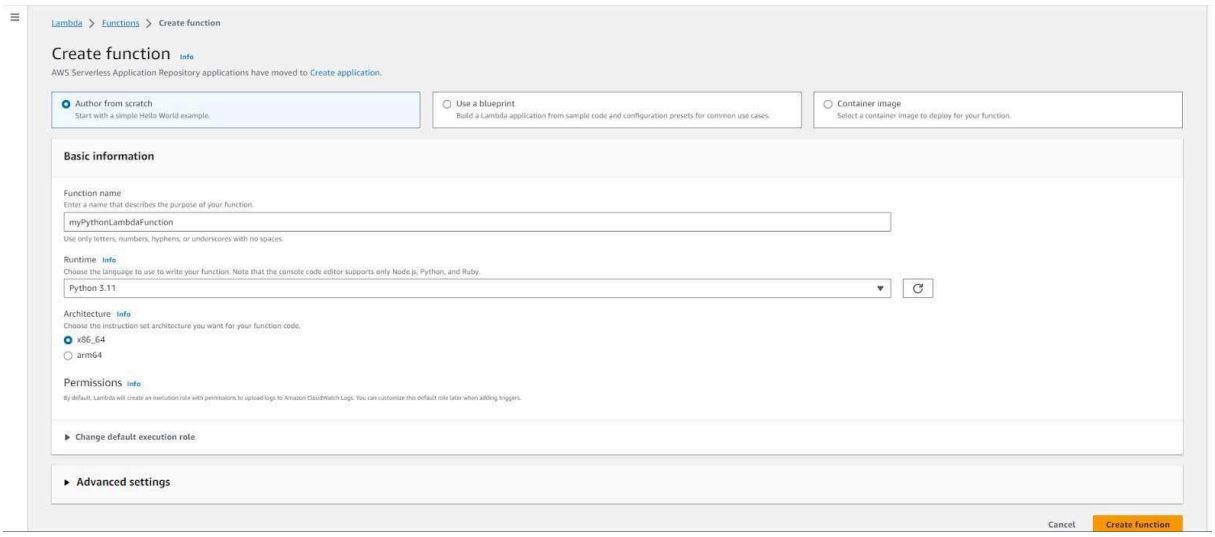
Step 1:Open up the Lambda Console and click on the Create button.
Be mindful of where you create your functions since Lambda is region-dependent.



2. Choose to create a function from scratch or use a blueprint, i.e templates defined by AWS for you with all configuration presets required for the most common use cases. Then, choose a runtime env for your function, under the dropdown, you can see all the options AWS supports, Python, Nodejs, .NET and Java being the most popular ones. After that, choose to create a new role with basic Lambda permissions if you don't have an existing one.

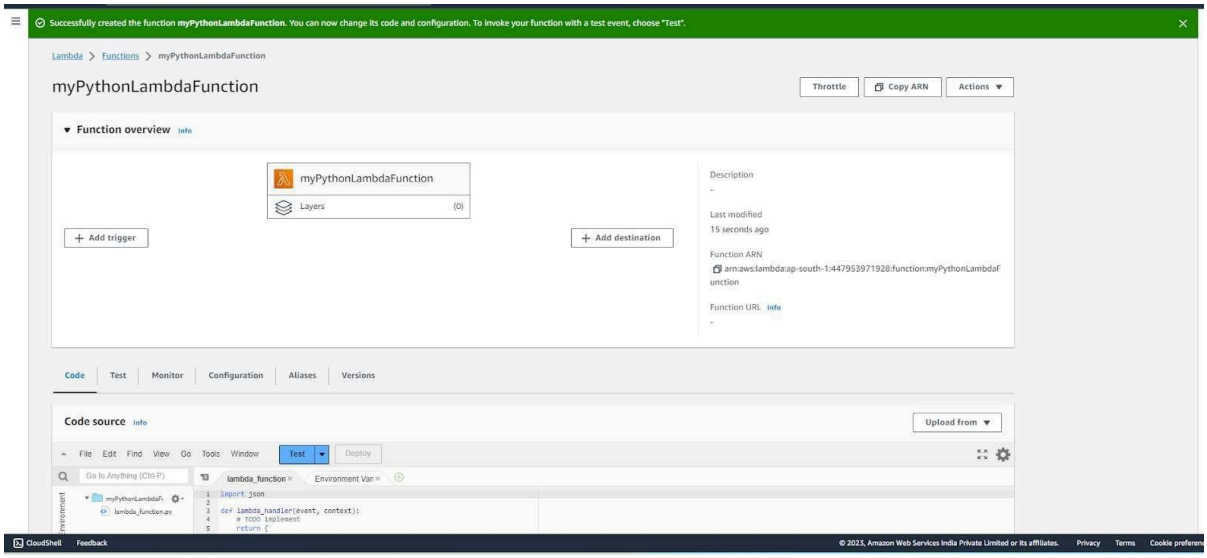


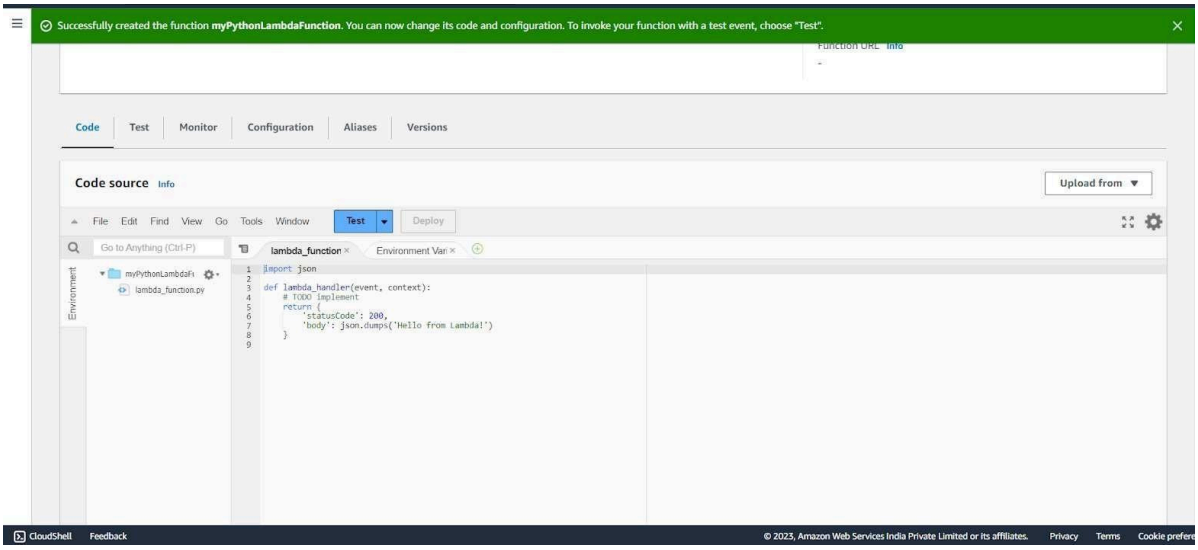




Click on the Create button.

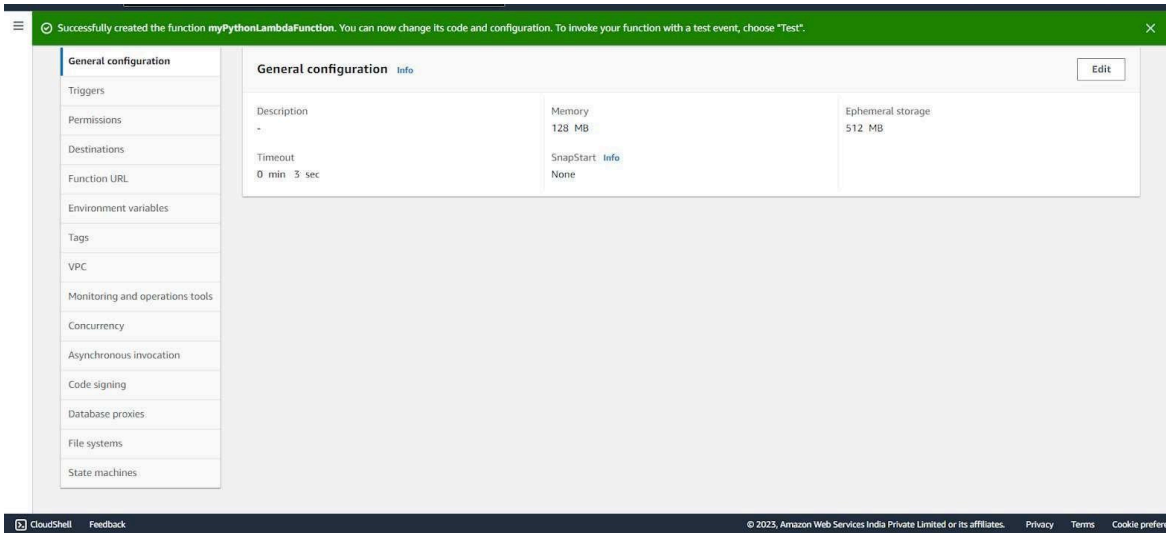
3. This process will take a while to finish and after that, you'll get a message that your function was successfully created.

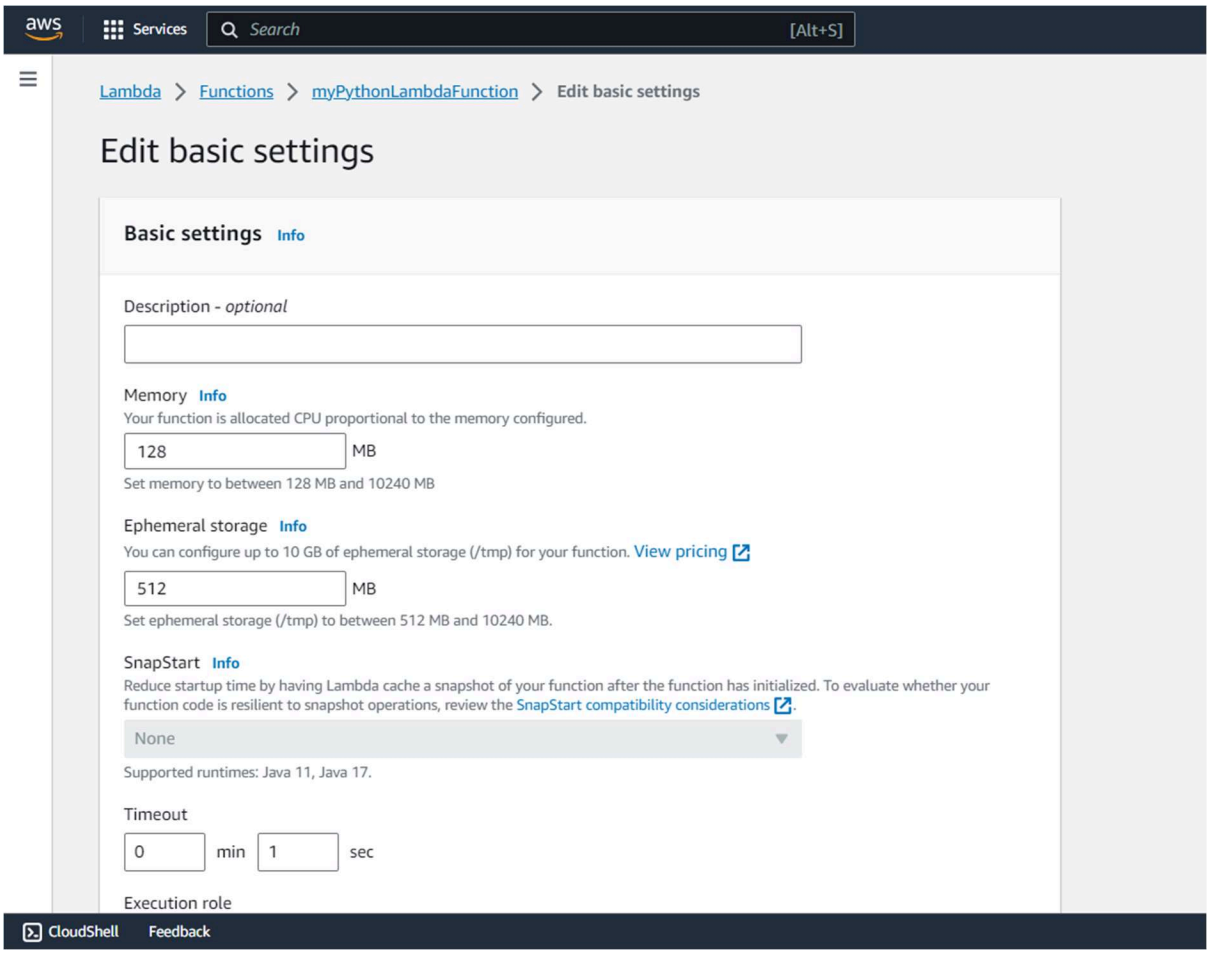




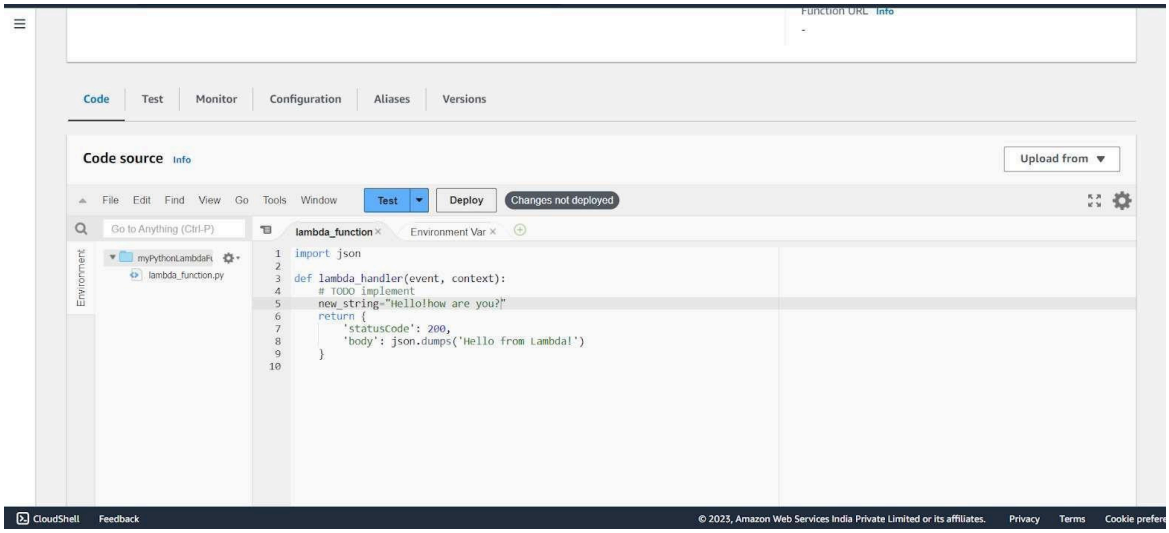
4. To change the configuration, open up the Configuration tab and under General Configuration, choose Edit.

Here, you can enter a description and change Memory and Timeout. I've changed the Timeout period to 1 sec since that is sufficient for now.

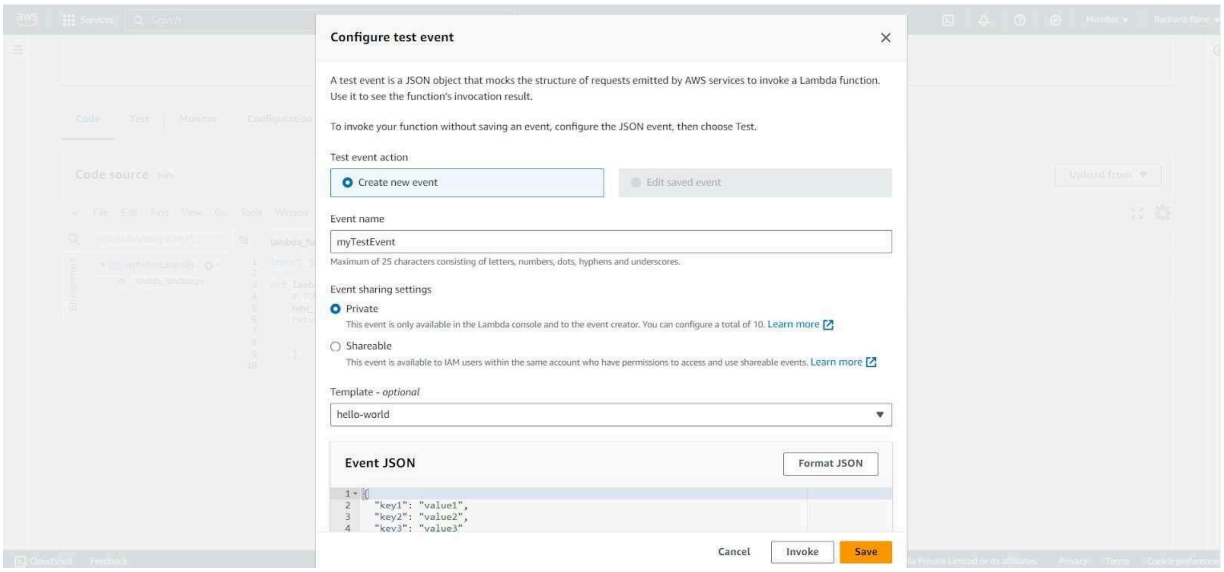




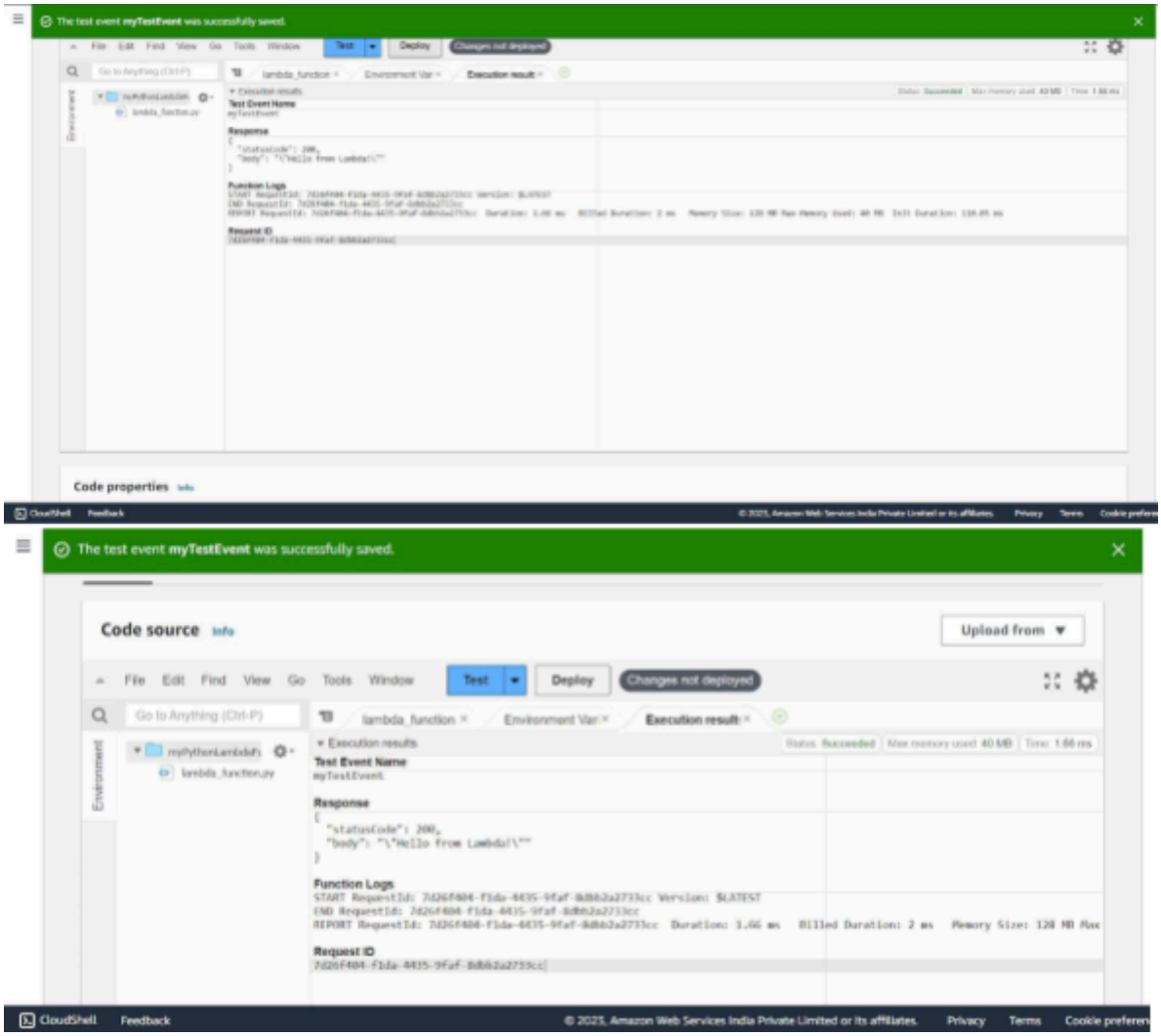
5. You can make changes to your function inside the code editor. You can also upload a zip file of your function or upload one from an S3 bucket if needed.
Press Ctrl + S to save the file and click Deploy to deploy the changes.



6. Click on Test and you can change the configuration, like so. If you do not have anything in the request body, it is important to specify two curly braces as valid JSON, so make sure they are there.



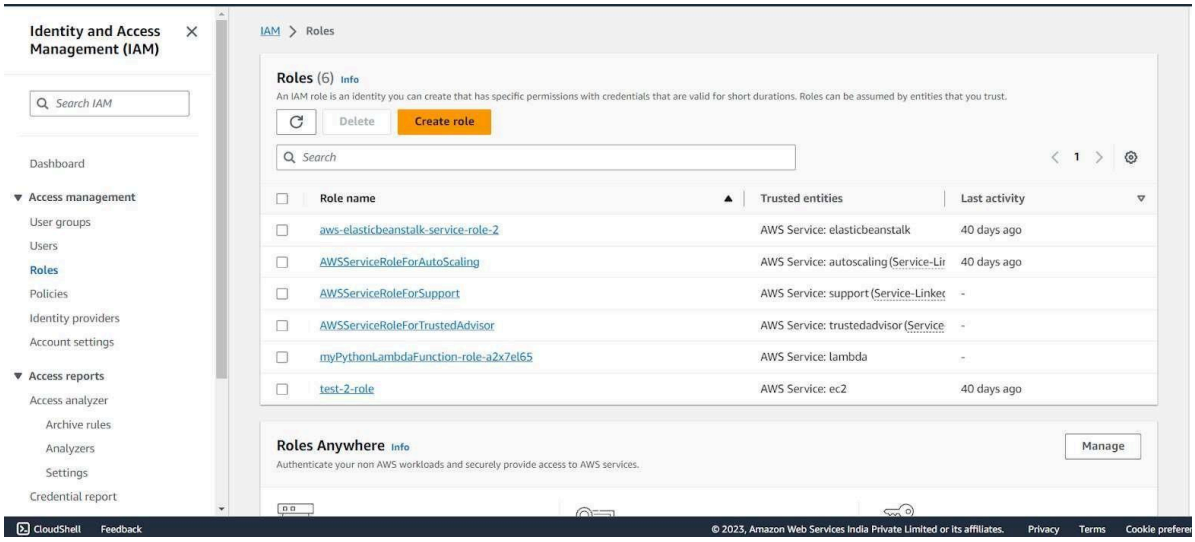
7. Now click on Test and you should be able to see the results.



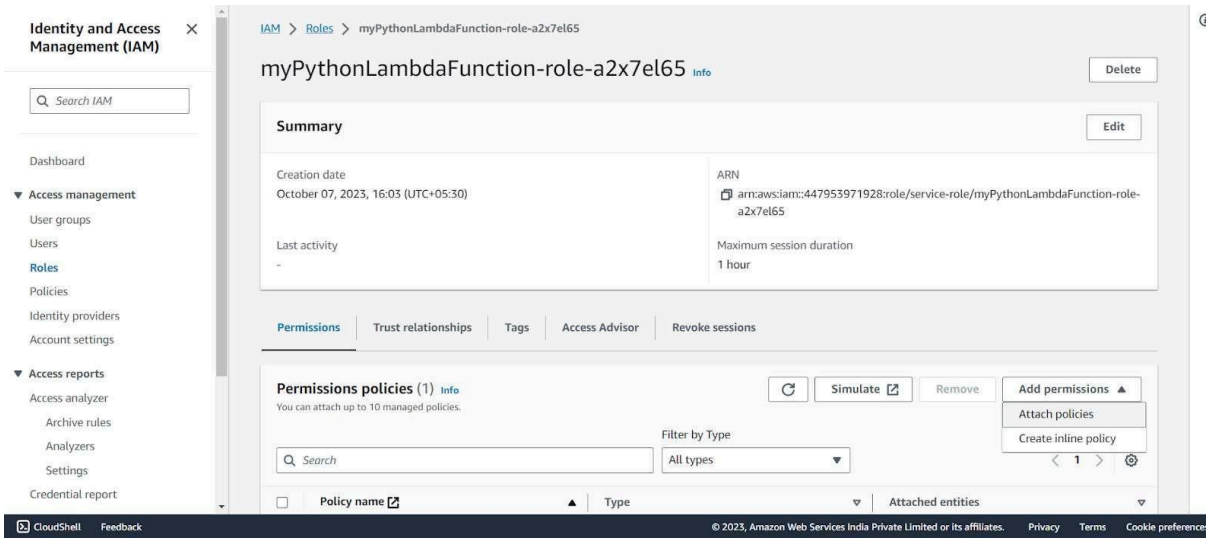
Conclusion: Thus, we understood AWS Lambda, its workflow, various functions and created our first Lambda functions using Python / Java / Nodejs.

Experiment No 12

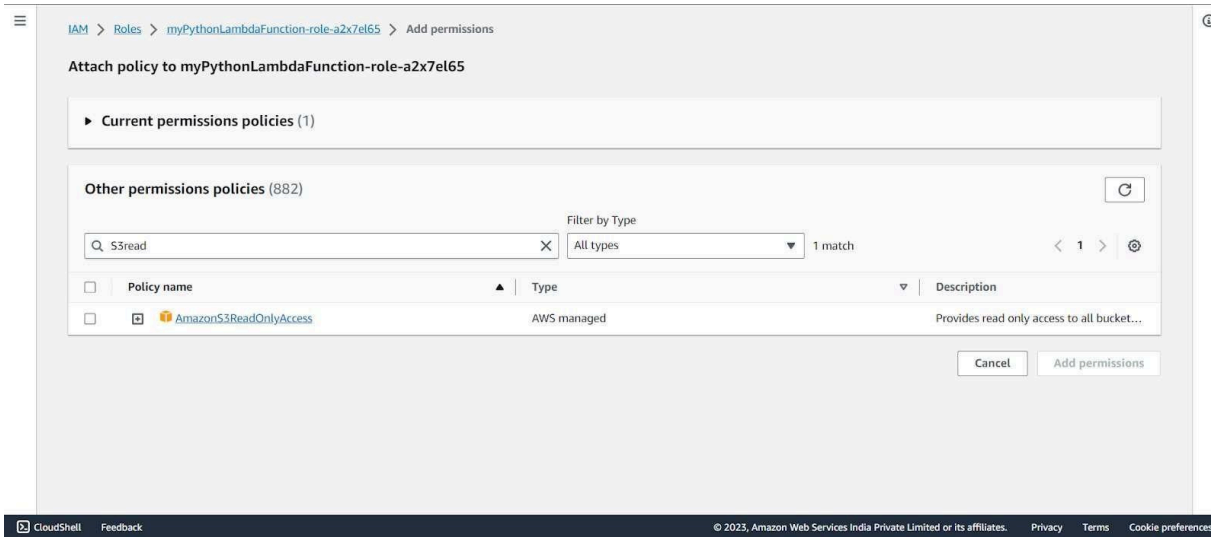
Step 1: Open up the IAM Console and under Roles, choose the Role we previously created for the Python Lambda Function (You can find your role name configuration of your Lambda function).



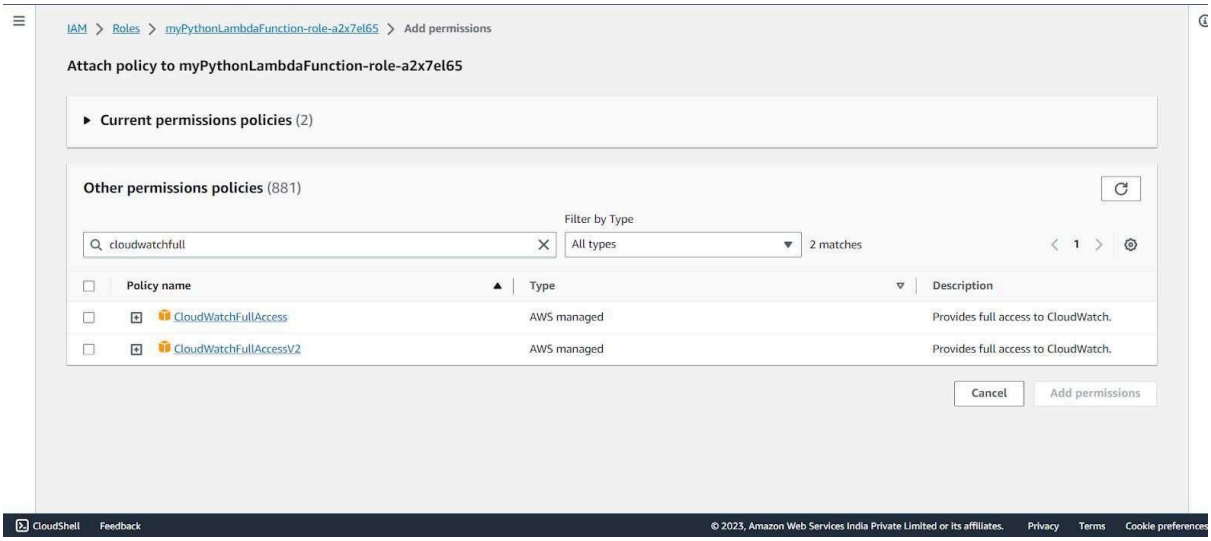
Step 2: Under Attach Policies, add S3-ReadOnly and CloudWatchFull permissions to this role.



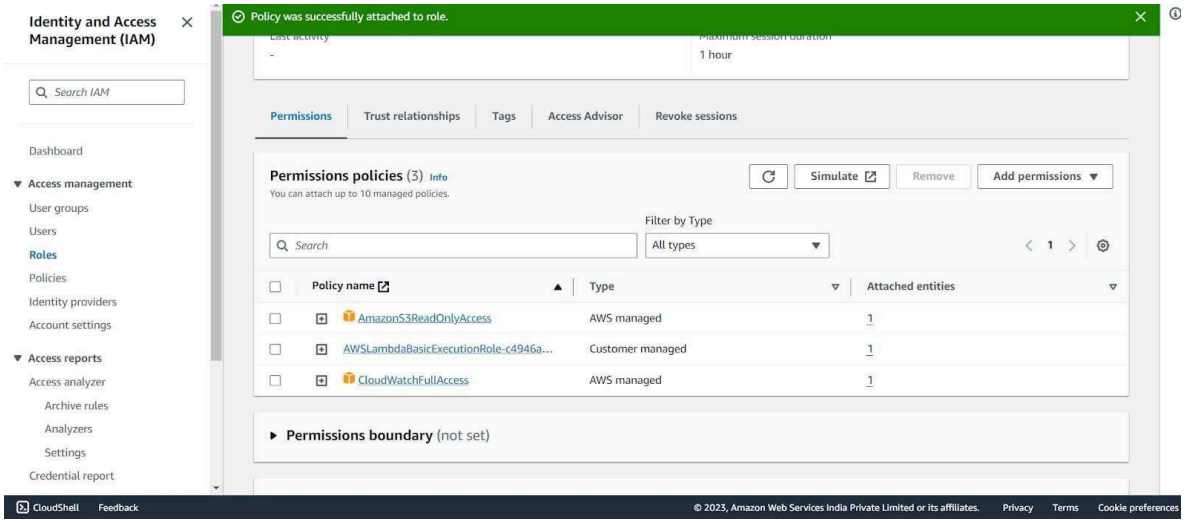
S3-ReadOnly



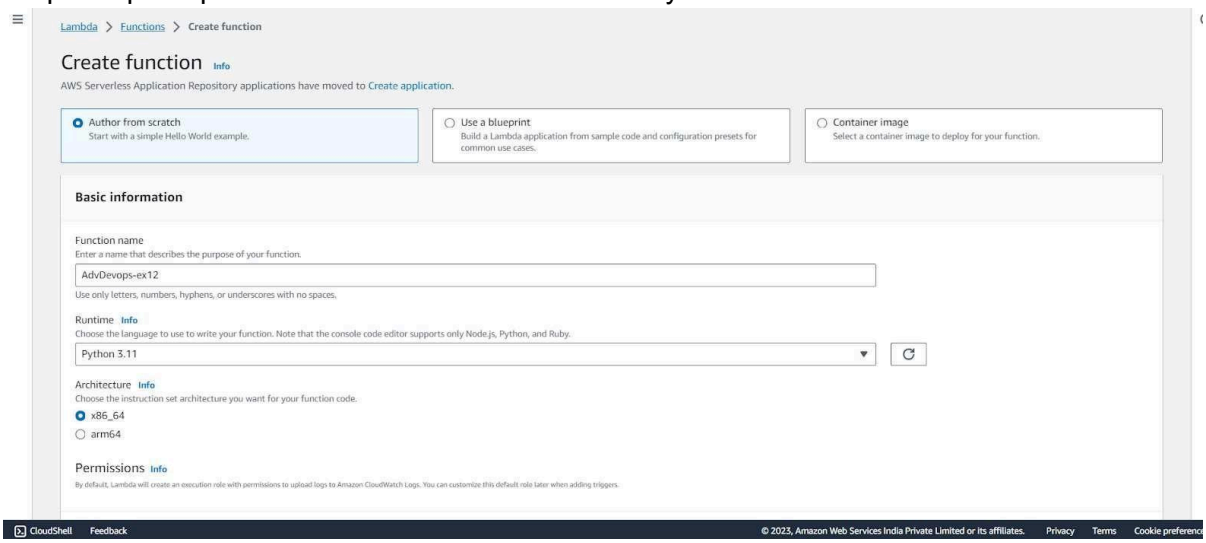
CloudWatchFull



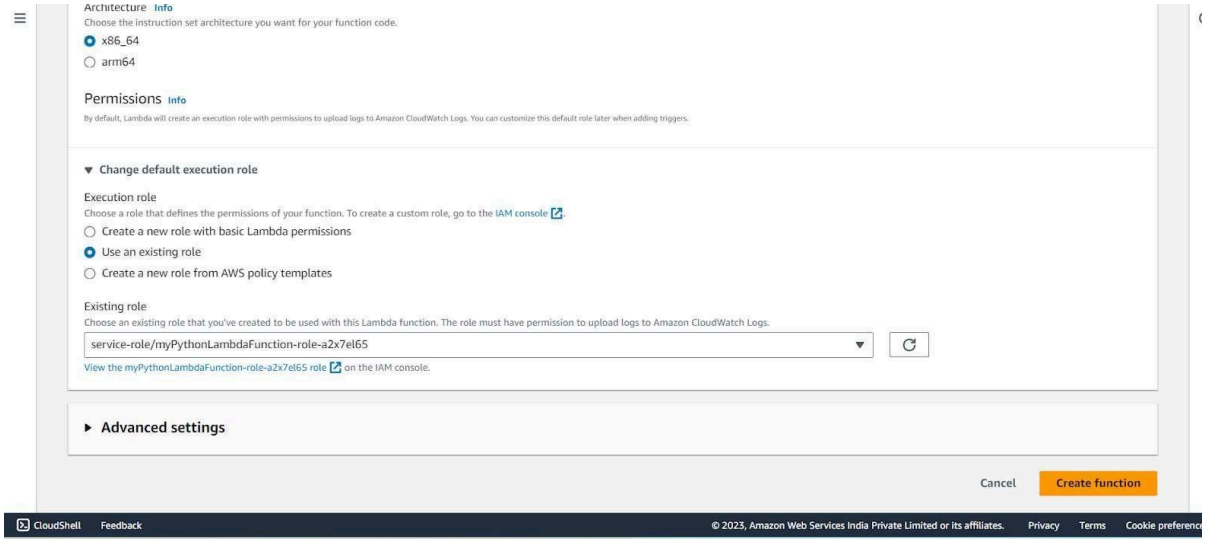
After successful attachment of policy you will see something like this you will be able to see the updated policies.



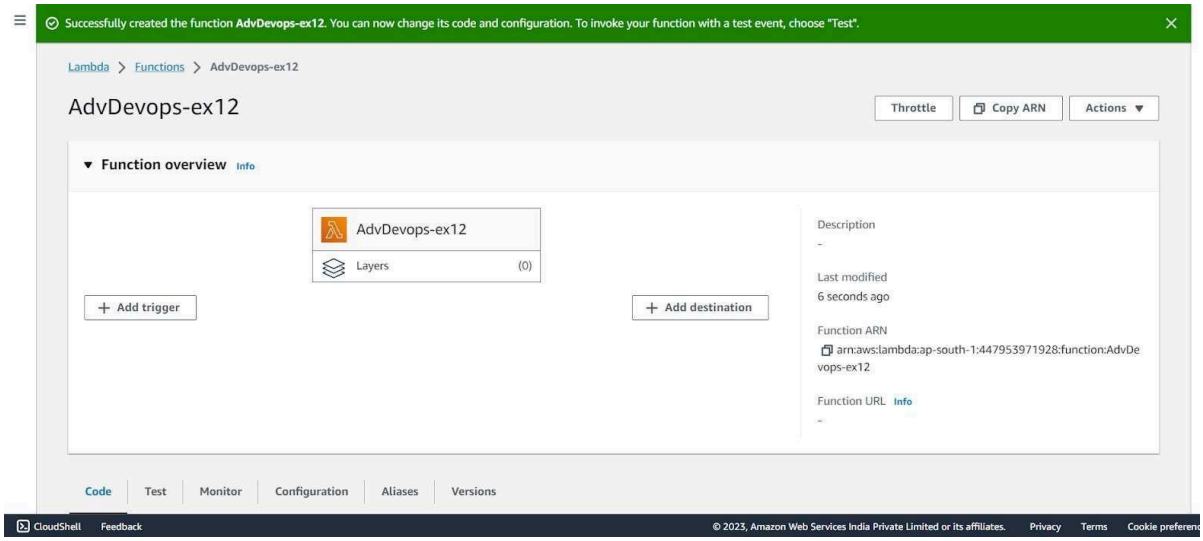
Step 3: Open up AWS Lambda and create a new Python function.



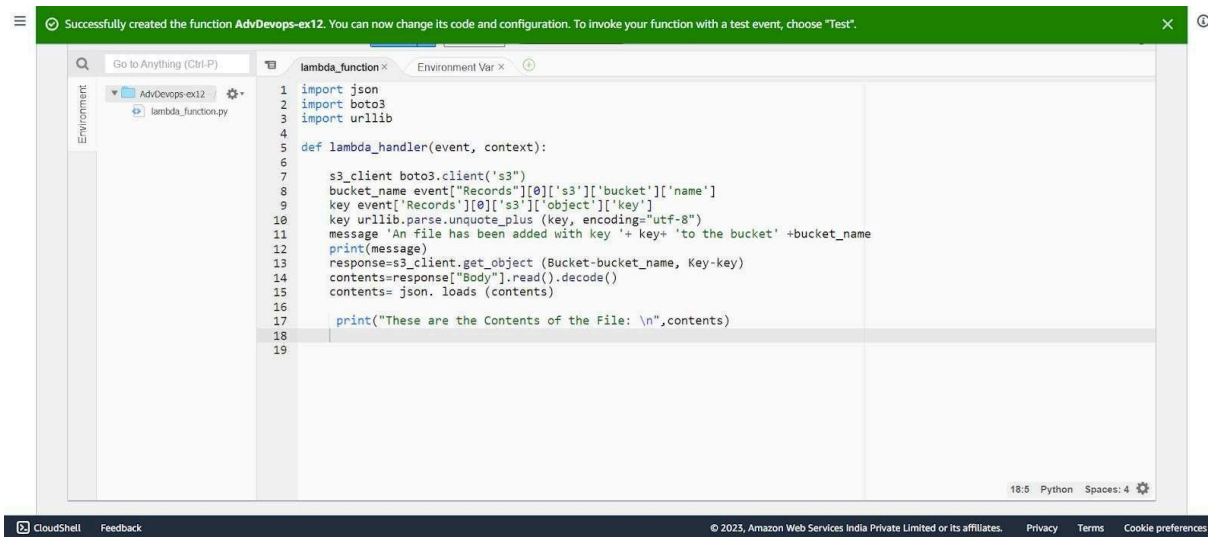
Under Execution Role, choose the existing role, then select the one which was previously created and to which we just added permissions.



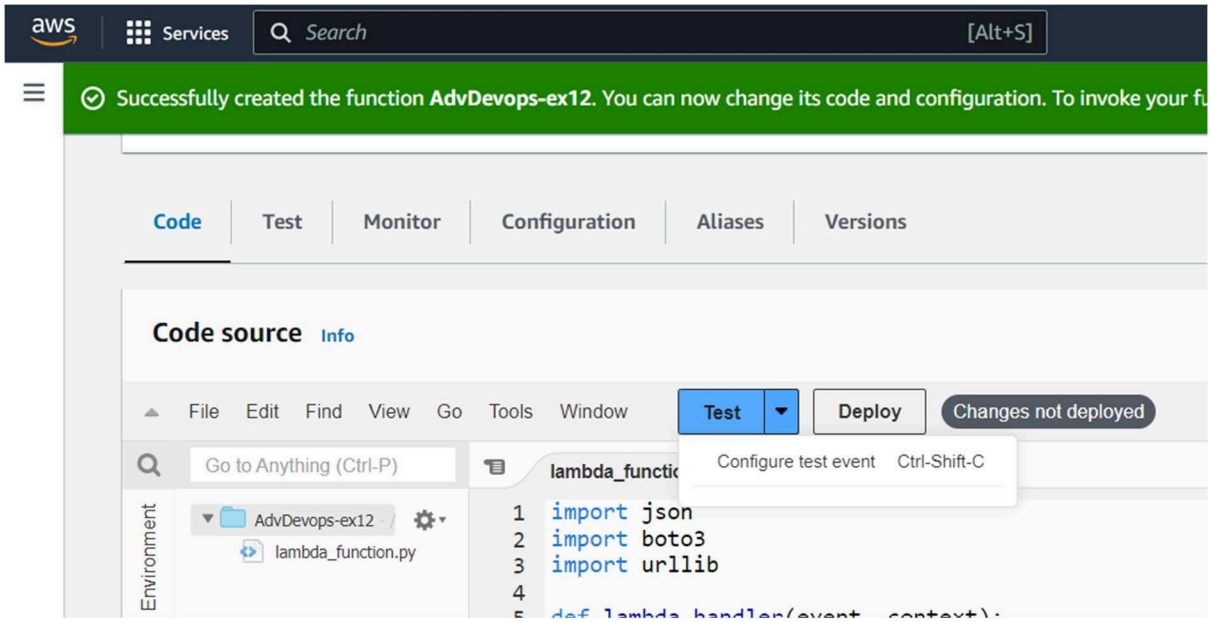
Step 4: The function is up and running.

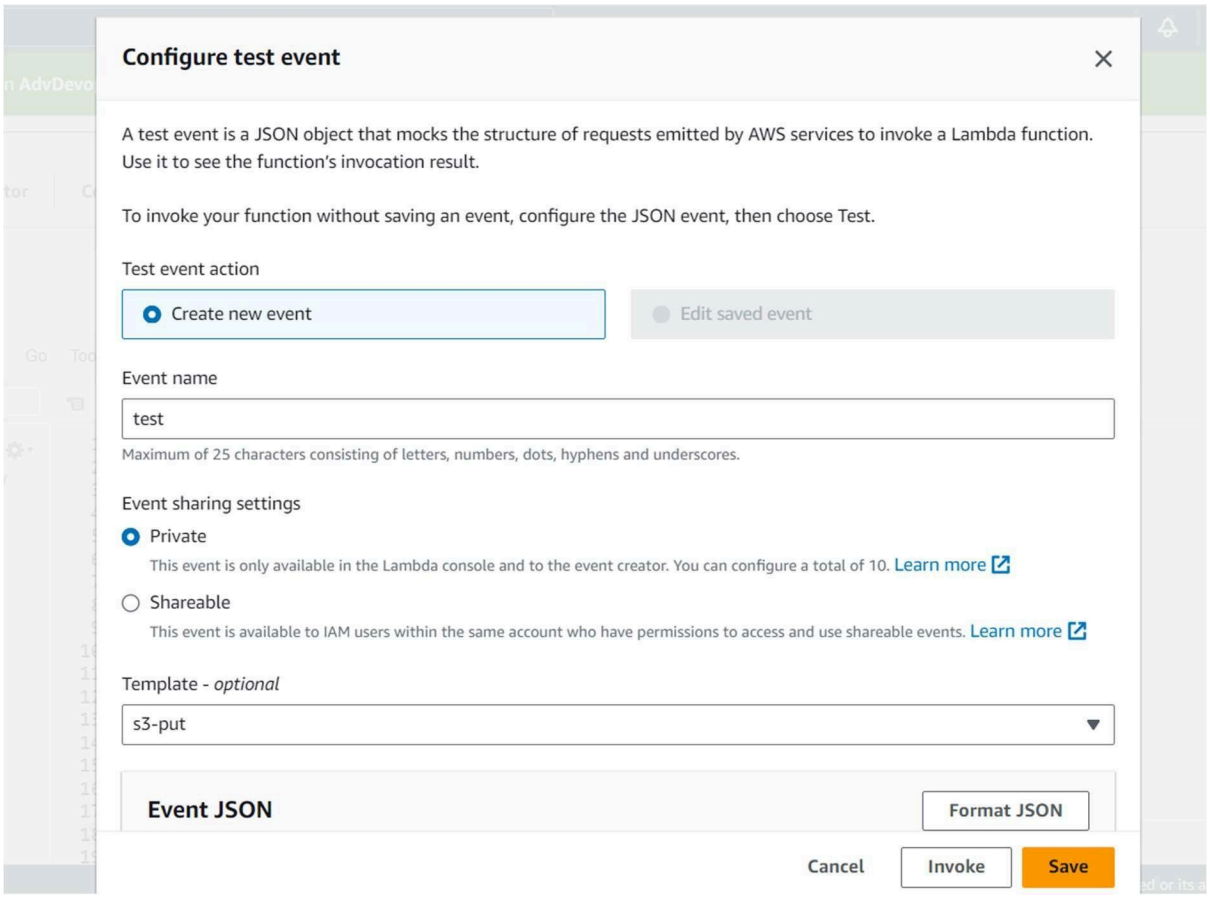


Step 5: Make the following changes to the function and click on the deploy button. This code basically logs a message and logs the contents of a JSON file which is uploaded to an S3 Bucket and then deploy the code.



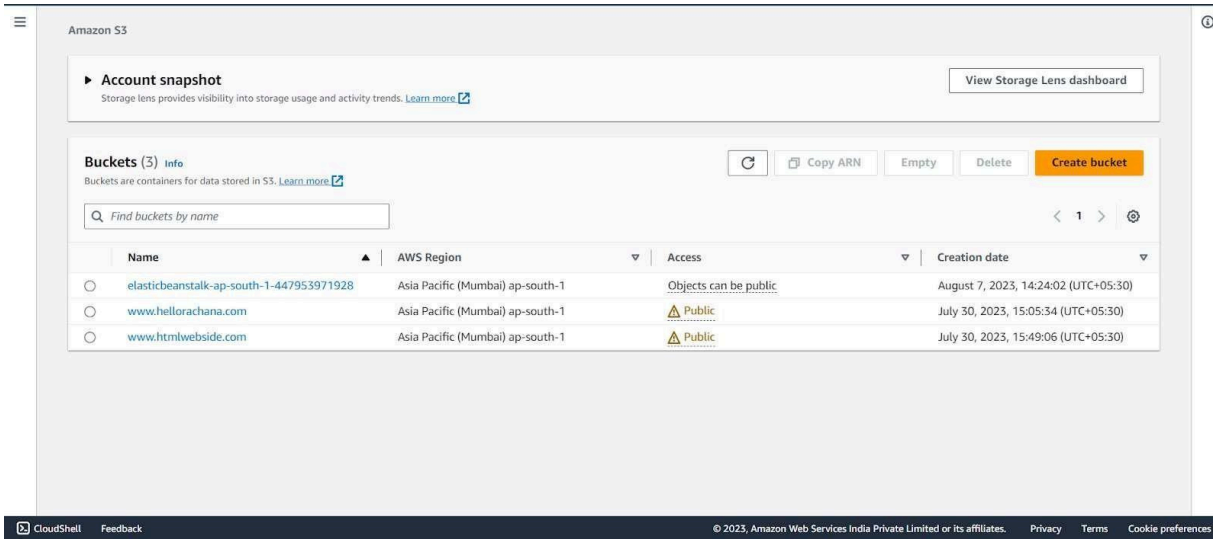
Step 6: Click on Test and choose the ‘S3 Put’ Template.



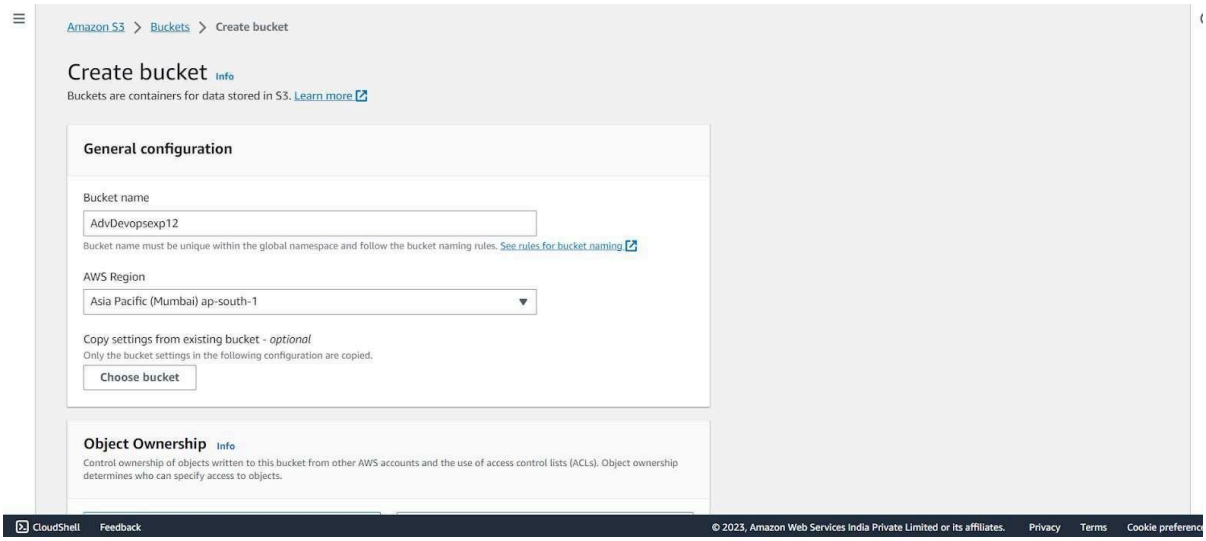


And Save it.

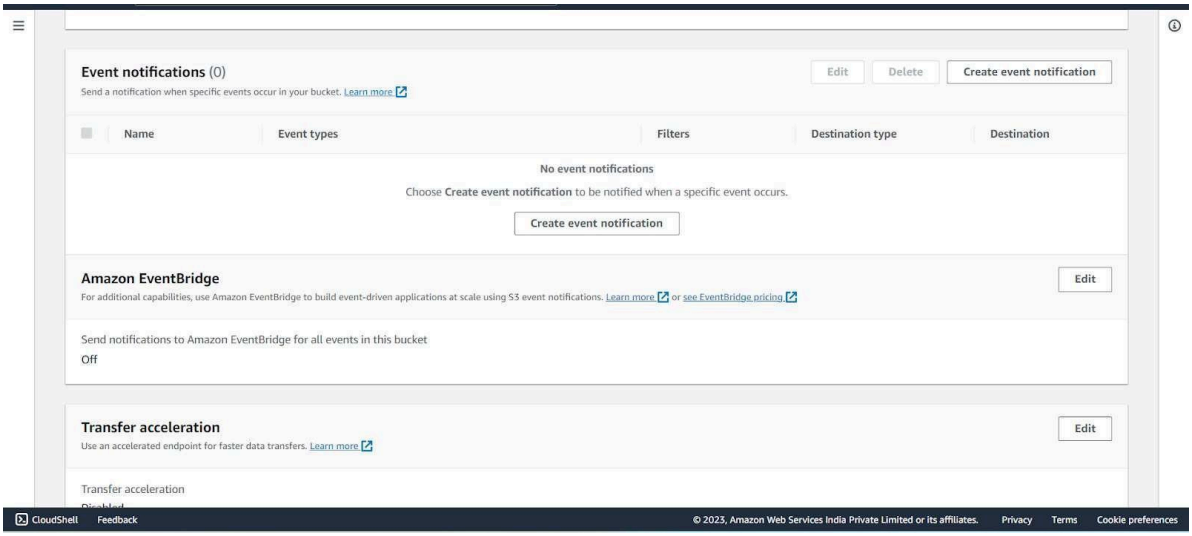
Step 7: Open up the S3 Console and create a new bucket.



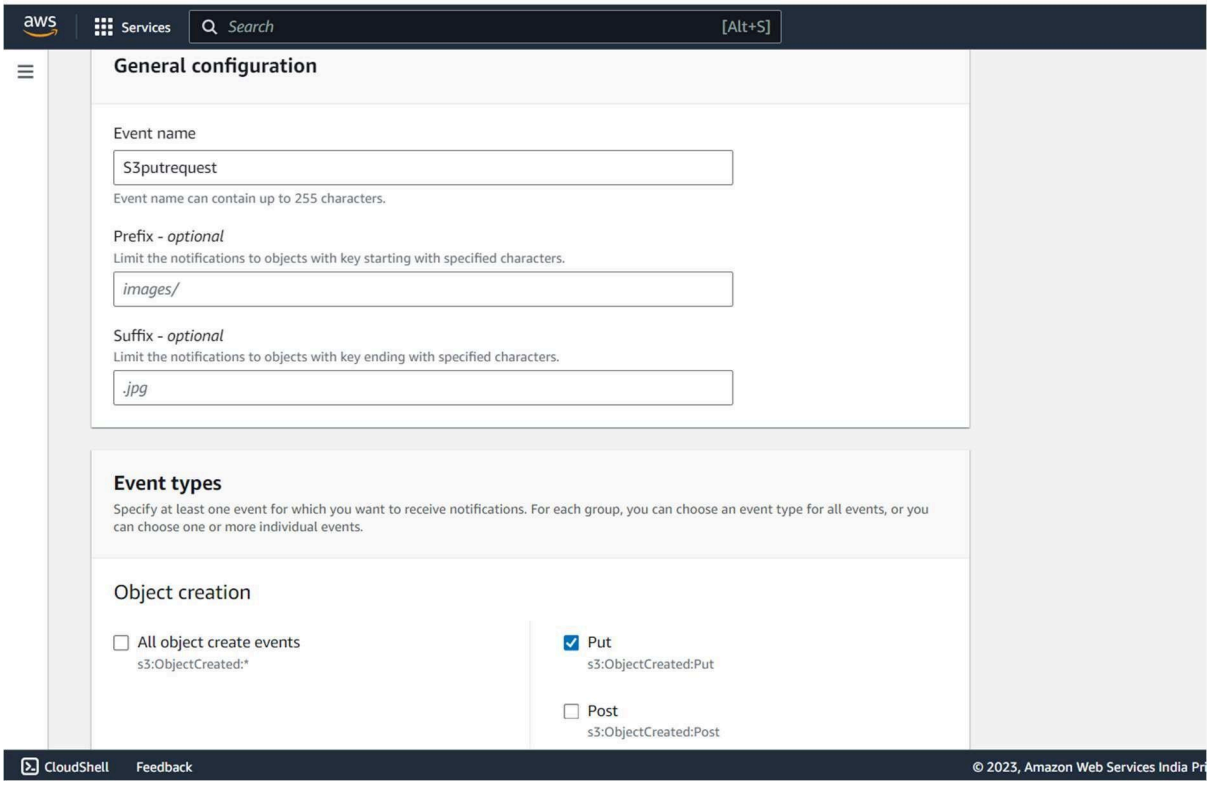
Step 8: With all general settings, create the bucket in the same region as the function.



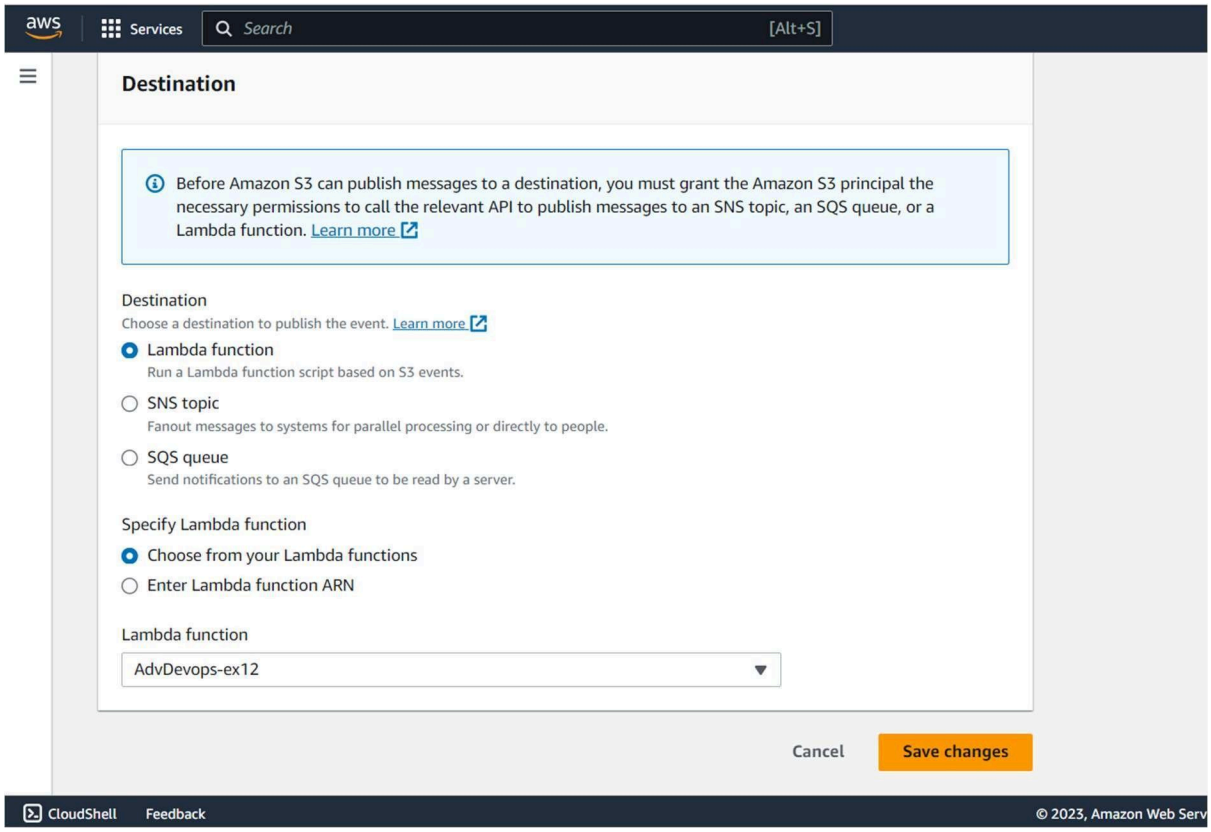
Step 9: Click on the created bucket and under properties, look for events.



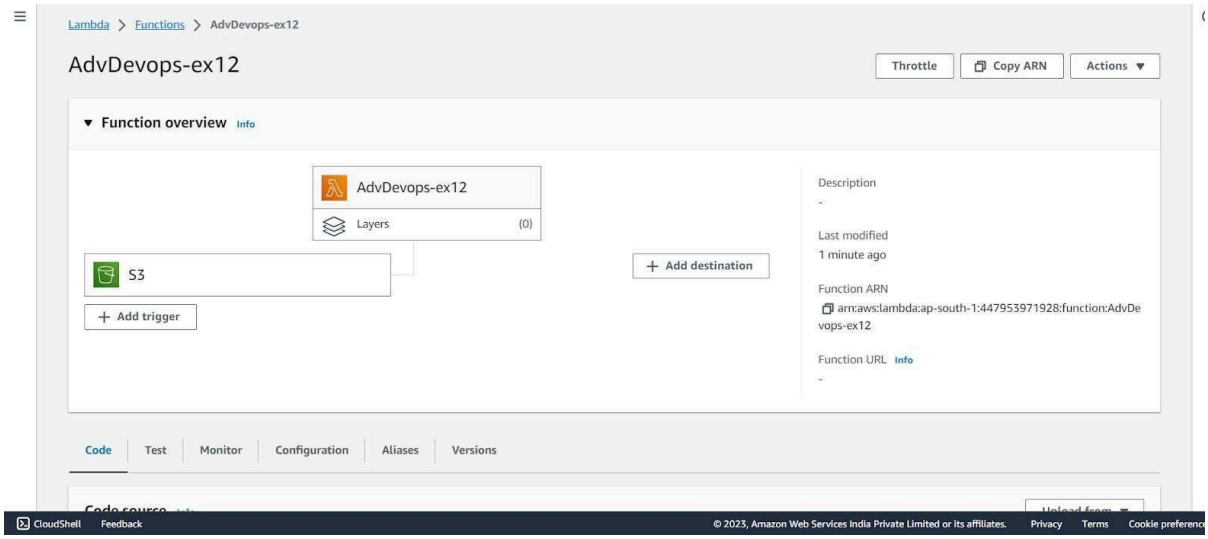
Click on Create Event Notification.
Step 10: Mention an event name and check Put under event types.



Choose Lambda function as destination and choose your lambda function and save the changes.

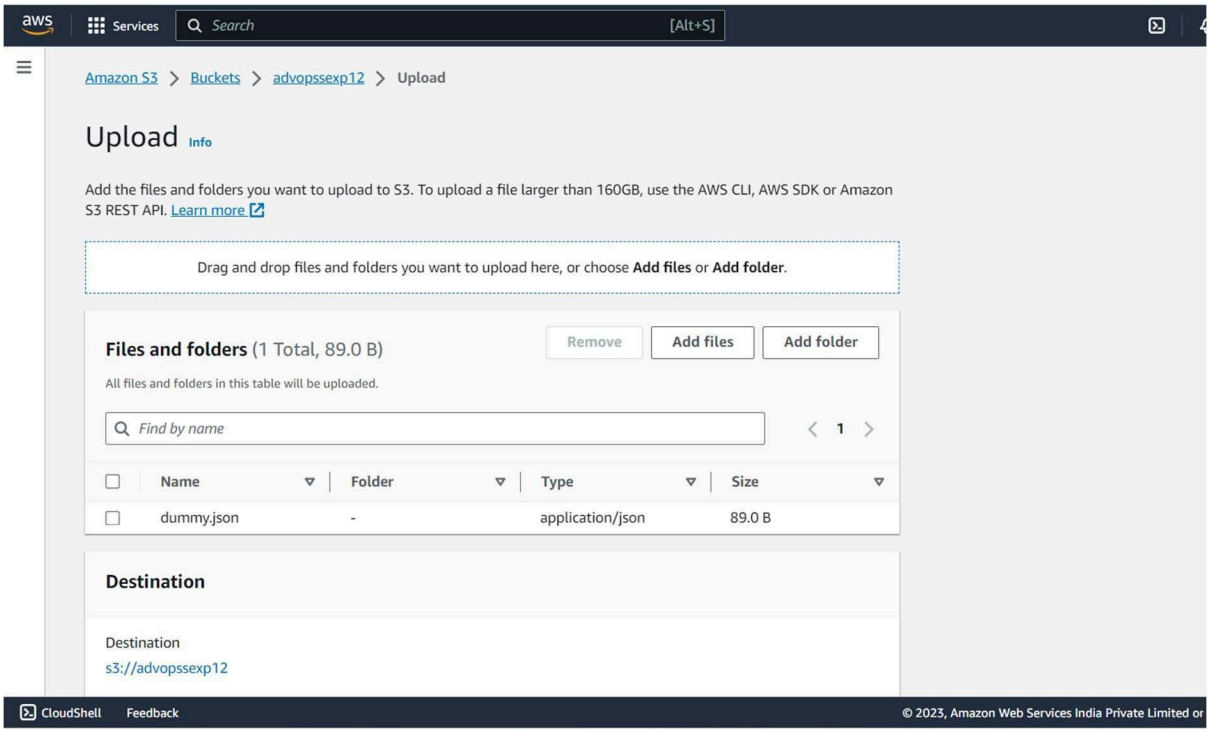


Step 11: Refresh the Lambda function console and you should be able to see an S3 Trigger in the overview.

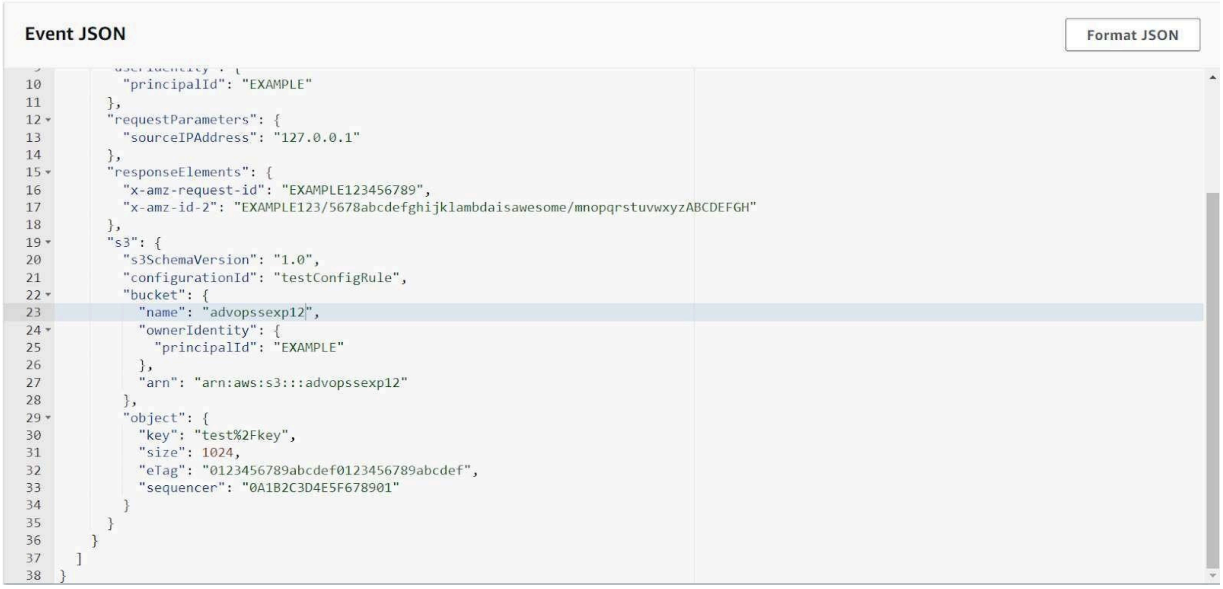


Step 12: Now, create a dummy JSON file locally.

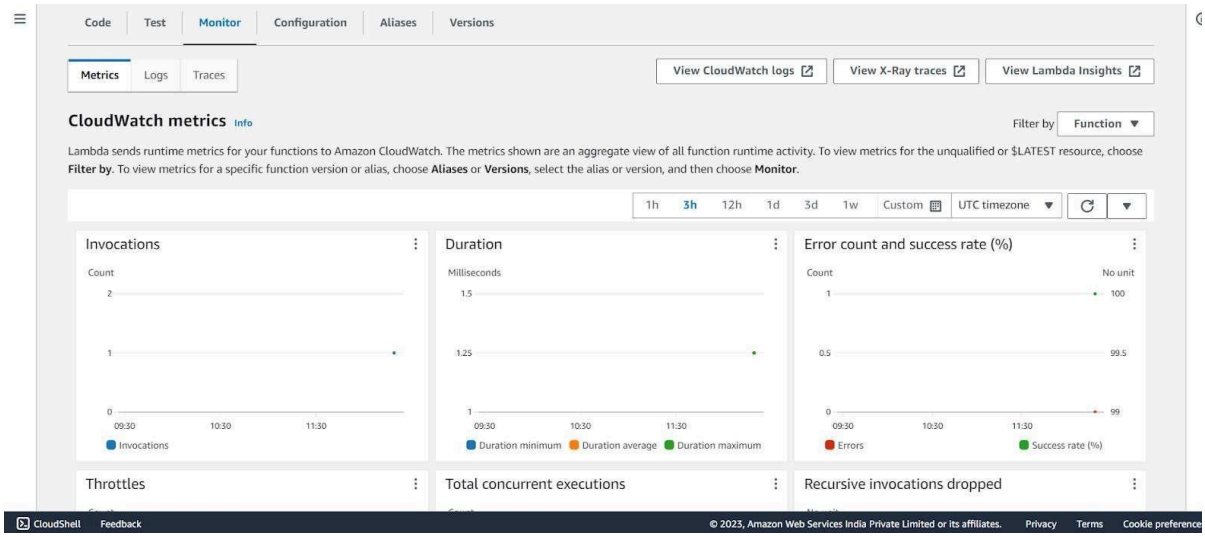
Step 13: Go back to your S3 Bucket and click on Add Files to upload a new file.
Step 14: Select the dummy data file from your computer and click Upload.



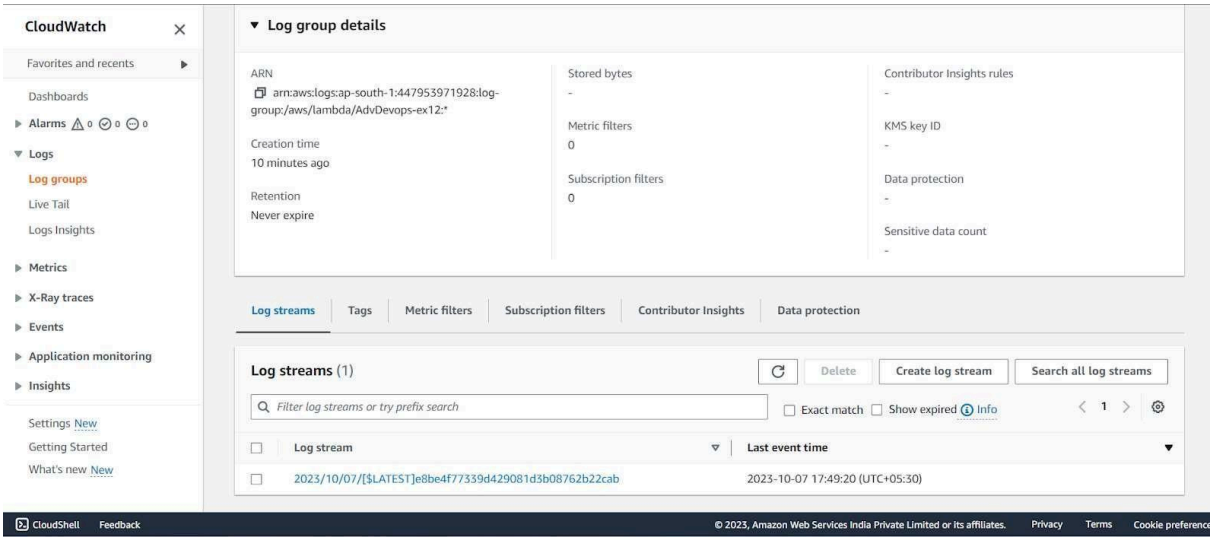
Step 15: After this make the necessary changes in the Test configuration file which we created it previously by replacing the Bucket Name and the ARN of Bucket.



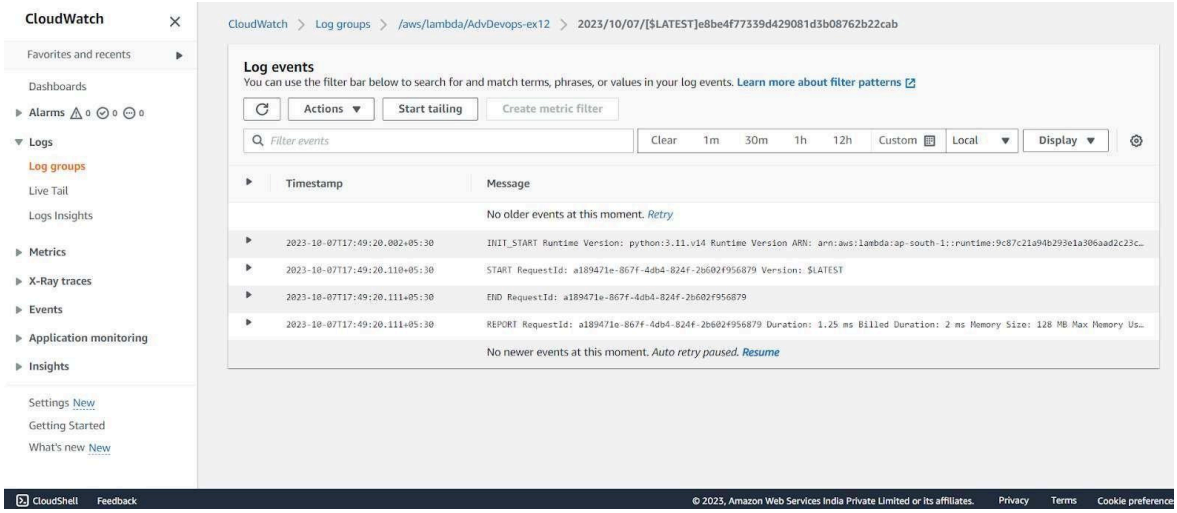
Step 16: Go back to your Lambda function , Refresh it and check the Monitor tab.



Under Log streams, click on View logs in Cloudwatch to check the Function logs.



Step 17: Click on this log Stream that was created to view what was logged by your function.

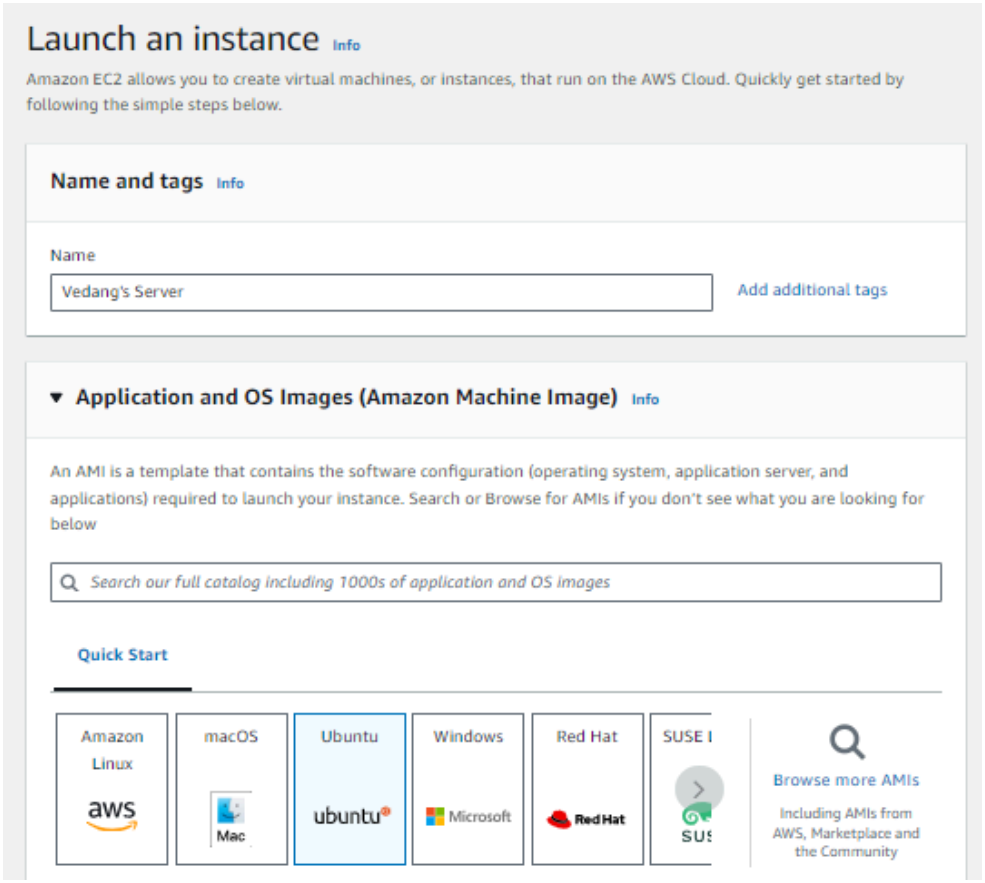


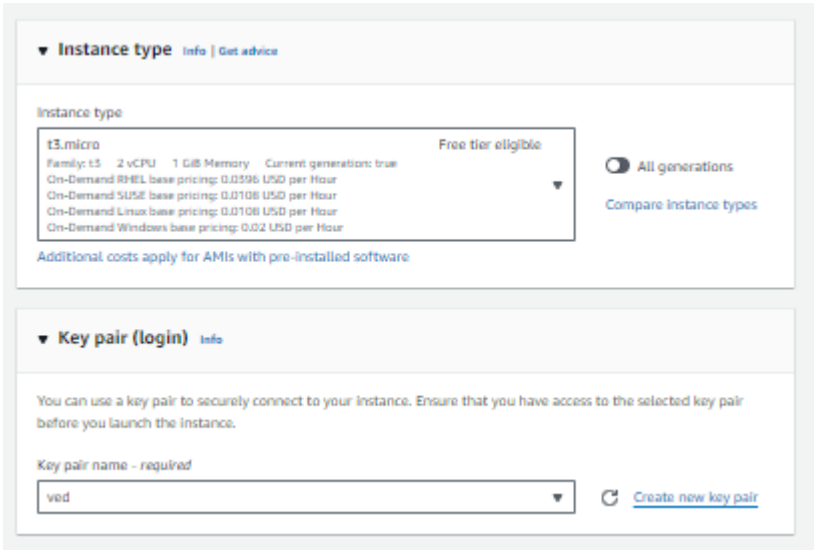
Conclusion: Thus, we have created a Lambda function which logs “An Image has been added” once you add an object to a specific bucket in S3.

ADVANCE DEVOPS EXP-1

Vedang Wajge **D15A/66**

Aim: To understand the benefits of Cloud infrastructure and Setup AWS Cloud9 IDE, Launch AWS Cloud9 IDE and and Perform Collaboration Demonstration.





Network settings Info

Edit

Network | Info

vpc-0775017352e40f883

Subnet | Info

No preference (Default subnet in any availability zone)

Auto-assign public IP | Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) | Info

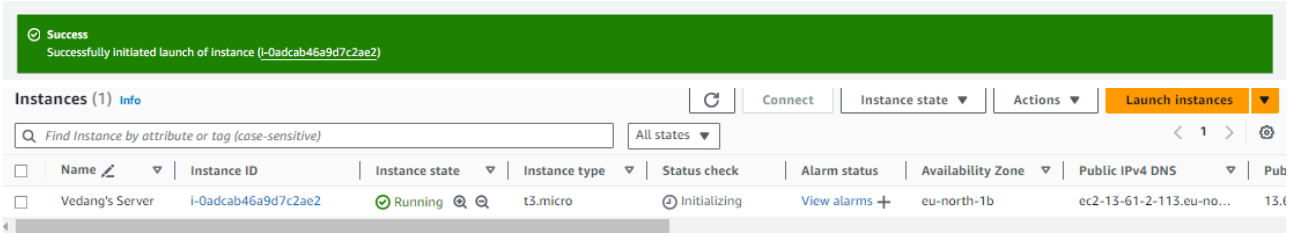
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

- (•) Create security group
- ( ) Select existing security group

We'll create a new security group called '**launch-wizard-1**' with the following rules:

- [x] Allow SSH traffic from
  Helps you connect to your instance
  Anywhere
  0.0.0.0/0
- [ ] Allow HTTPS traffic from the internet
  To set up an endpoint, for example when creating a web server
- [ ] Allow HTTP traffic from the internet
  To set up an endpoint, for example when creating a web server

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




```
 * Support:        https://ubuntu.com/pro

 System information as of Tue Aug 20 07:27:04 UTC 2024

  System load:  0.17              Temperature:           -273.1 C
  Usage of /:   22.7% of 6.71GB   Processes:             112
  Memory usage: 24%               Users logged in:       0
  Swap usage:   0%                IPv4 address for ens5: 172.31.37.143

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-37-143:~$
```

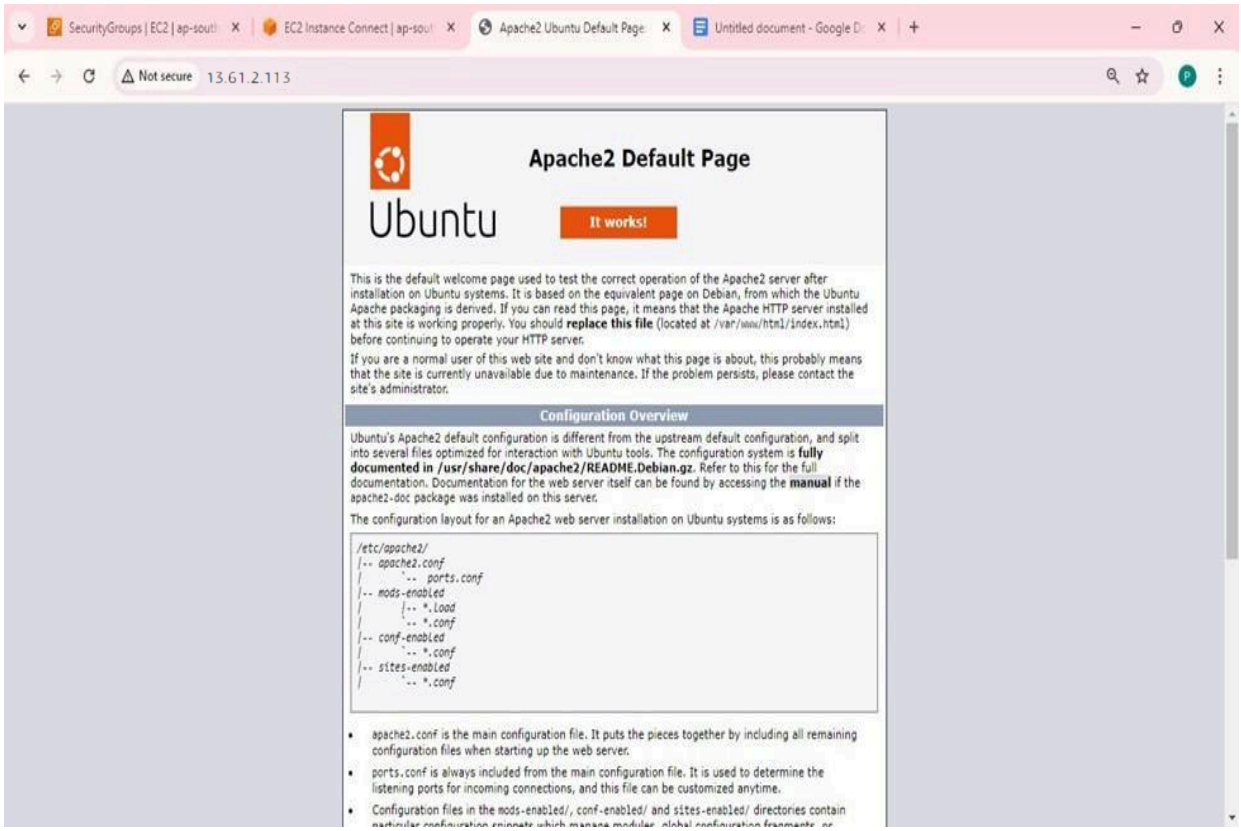
i-0adcab46a9d7c2ae2 (Vedang's Server)

PublicIPs: 13.61.2.113 PrivateIPs: 172.31.37.143

```
root@ip-172-31-37-143:/home/ubuntu# apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
```

```
root@ip-172-31-37-143:/home/ubuntu# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Tue 2024-08-20 07:28:04 UTC; 2min 10s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2454 (apache2)
      Tasks: 55 (limit: 1078)
     Memory: 5.5M (peak: 5.9M)
        CPU: 45ms
     CGroup: /system.slice/apache2.service
             ├─2454 /usr/sbin/apache2 -k start
             ├─2456 /usr/sbin/apache2 -k start
             └─2458 /usr/sbin/apache2 -k start
```

```
root@ip-172-31-37-143:/home/ubuntu# cd /var/www/html
root@ip-172-31-37-143:/var/www/html# /var/www/html
bash: /var/www/html: Is a directory
root@ip-172-31-37-143:/var/www/html#
```

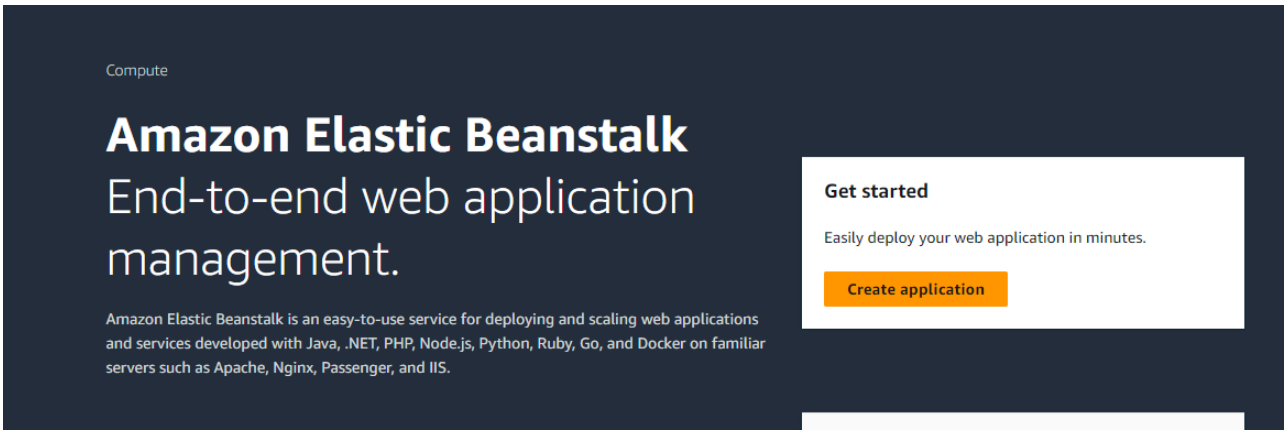


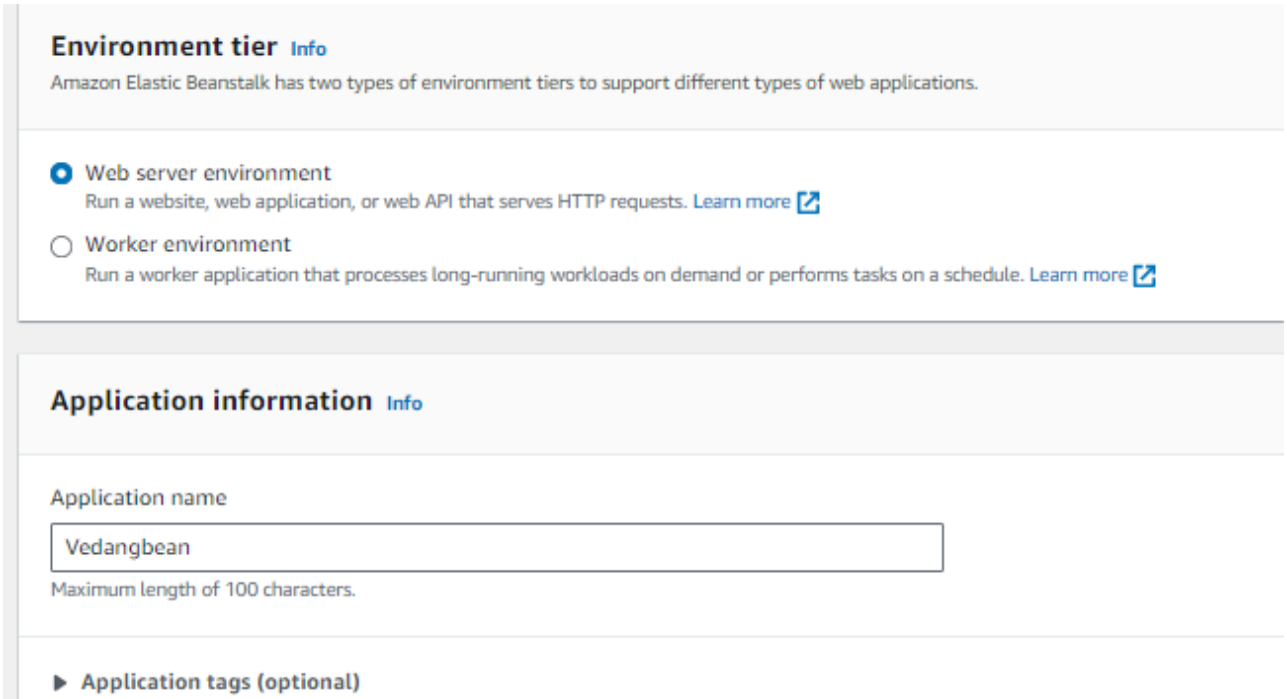
ADVANCE DEVOPS EXP-2

Vedang Wajge D15A/66

Aim: To build your application using AWS Codebuild and deploy on S3 using AWS CodePipeline deploy sample application on EC2 instance using AWS codedeploy.

Code and Output :
Using elastic beanstalk:





Platform Info

Platform type

- Managed platform
  Platforms published and maintained by Amazon Elastic Beanstalk. Learn more
- Custom platform
  Platforms created and owned by you. This option is unavailable if you have no platforms.

Platform

PHP

Platform branch

PHP 8.3 running on 64bit Amazon Linux 2023

Platform version

4.3.2 (Recommended)

Environment properties

Key	Value

No environment properties

There are no environment properties defined

Cancel | Previous | Submit

Vedangbean-env Info

Actions | Upload and deploy

Environment overview

Health
Unknown

Environment ID
e-vbejiswjbp

Domain
–

Application name
Vedangbean

Platform

Change version

Platform
PHP 8.3 running on 64bit Amazon Linux 2023/4.3.2

Running version
–

Platform state
Supported

Developer Tools > CodePipeline > Pipelines

Introducing the new V2 pipeline type with improved release safety, pipeline triggers, parameterized pipelines, and a new billing model. Learn more

Pipelines Info

Notify | View history | Release change | Delete pipeline | Create pipeline

Name	Latest execution status	Latest source revisions	Latest execution started	Most recent executions

No results

There are no results to display.

a

Choose pipeline settings Info

Step 1 of 5

Pipeline settings

Pipeline name

Enter the pipeline name. You cannot edit the pipeline name after it is created.

vedangpipeline

No more than 100 characters

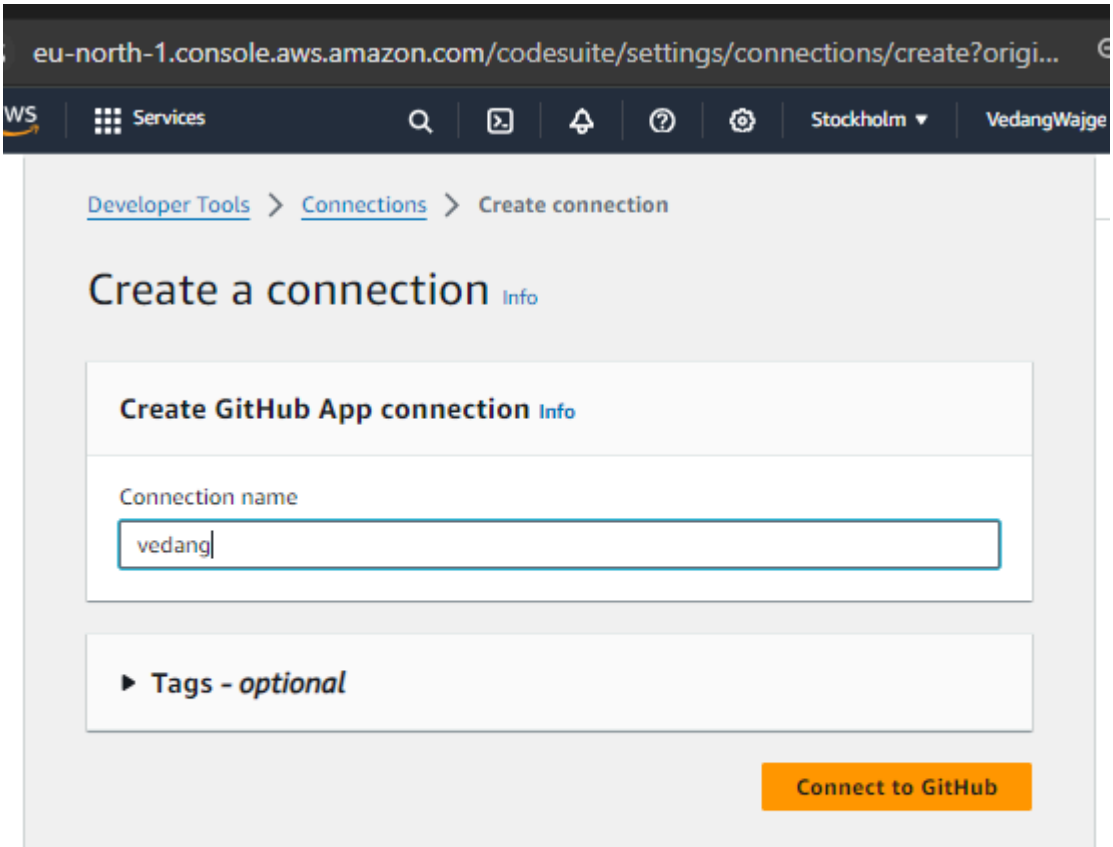
Pipeline type

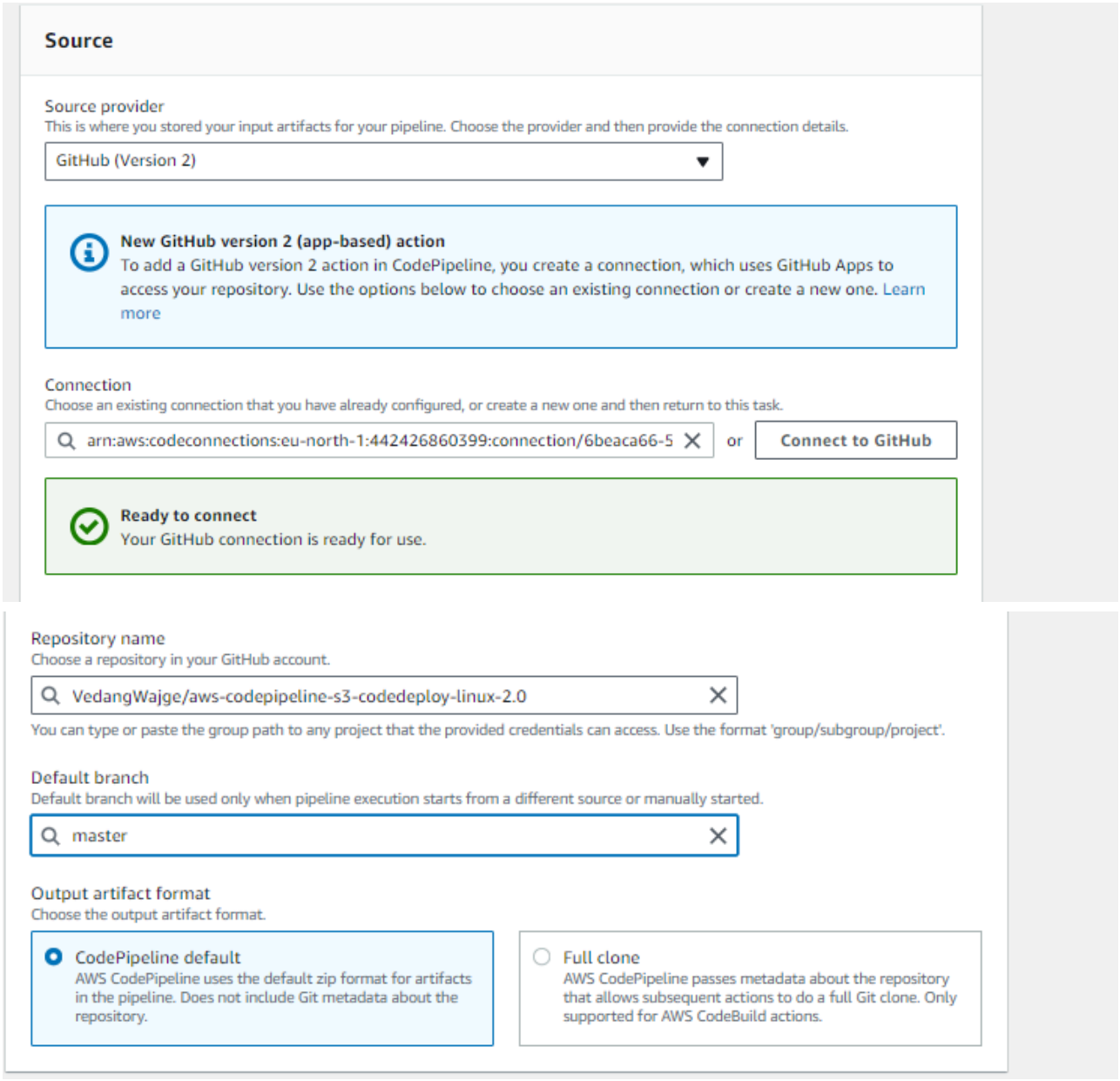
You can no longer create V1 pipelines through the console. We recommend you use the V2 pipeline type with improved release safety, pipeline triggers, parameterized pipelines, and a new billing model.

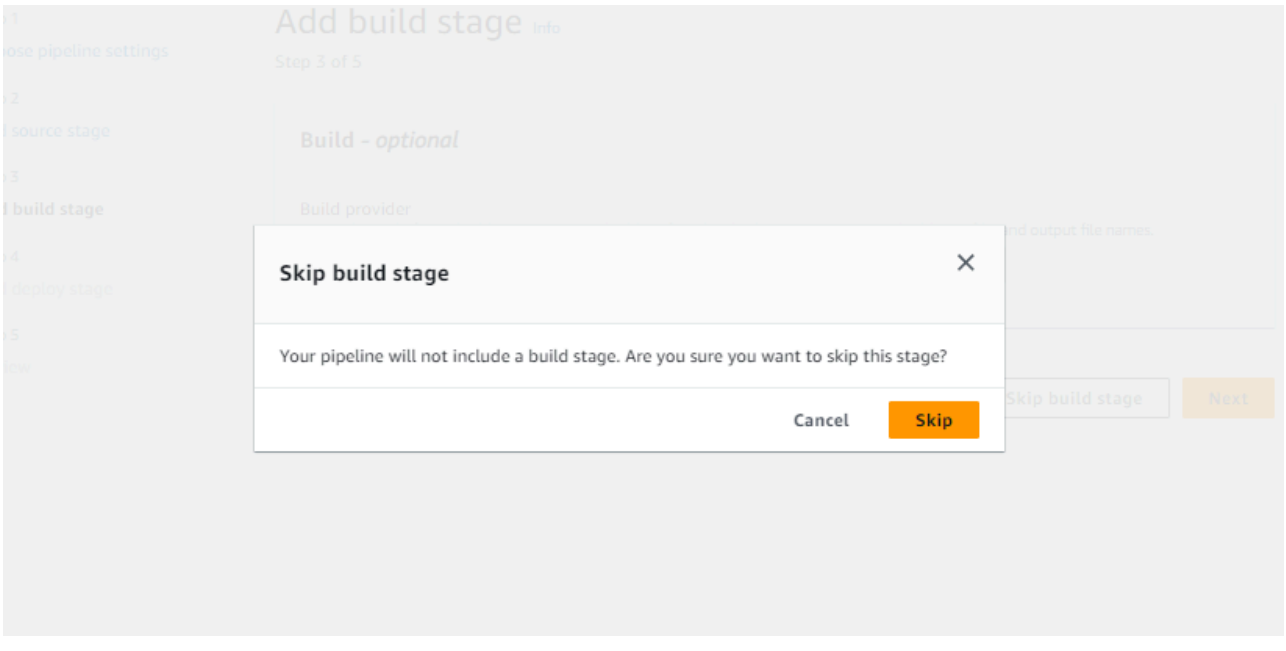
Execution mode

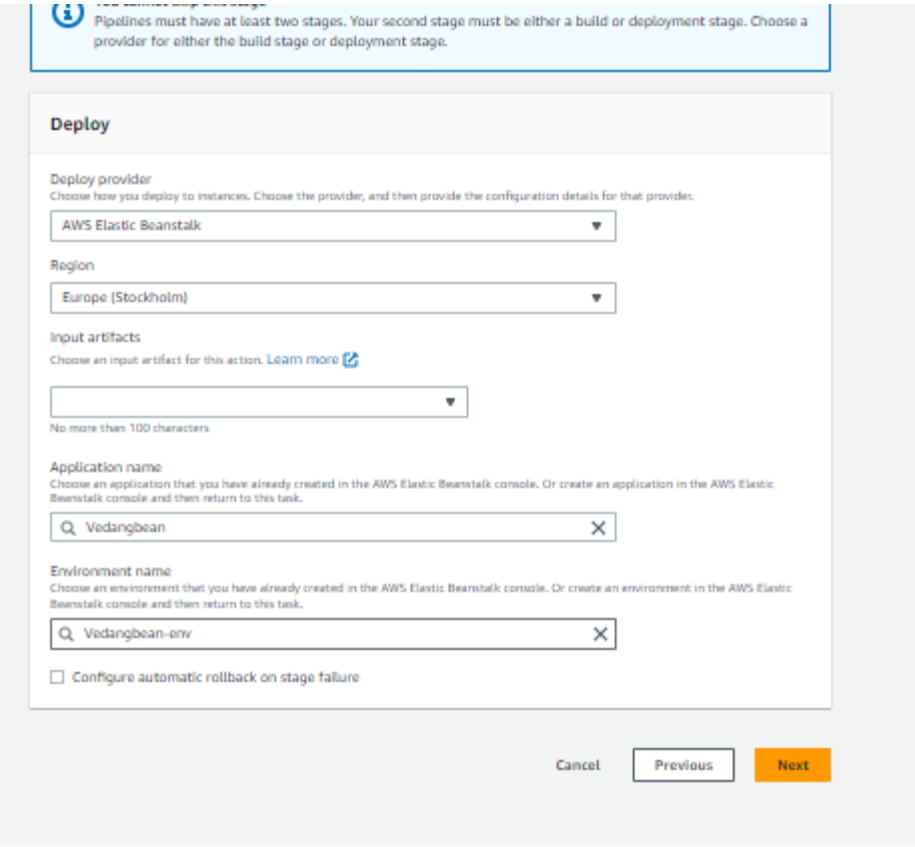
Choose the execution mode for your pipeline. This determines how the pipeline is run.

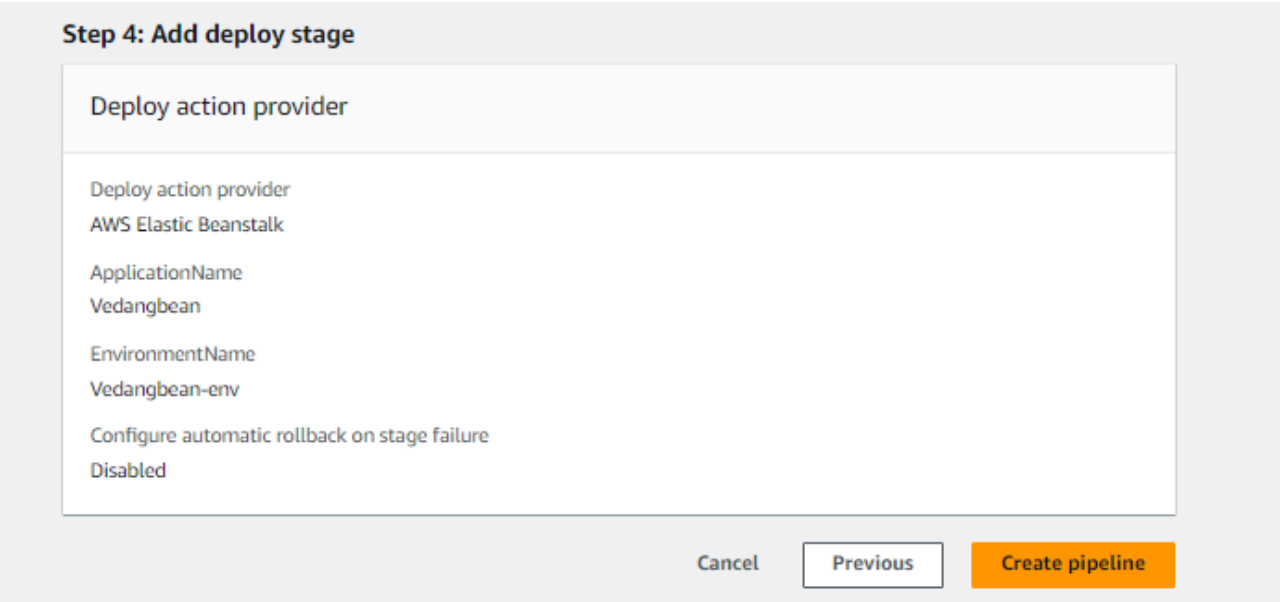
- ○ Superseded
  A more recent execution can overtake an older one. This is the default.
- ◉ Queued (Pipeline type V2 required)
  Executions are processed one by one in the order that they are queued.
- ○ Parallel (Pipeline type V2 required)
  Executions don't wait for other runs to complete before starting or finishing.

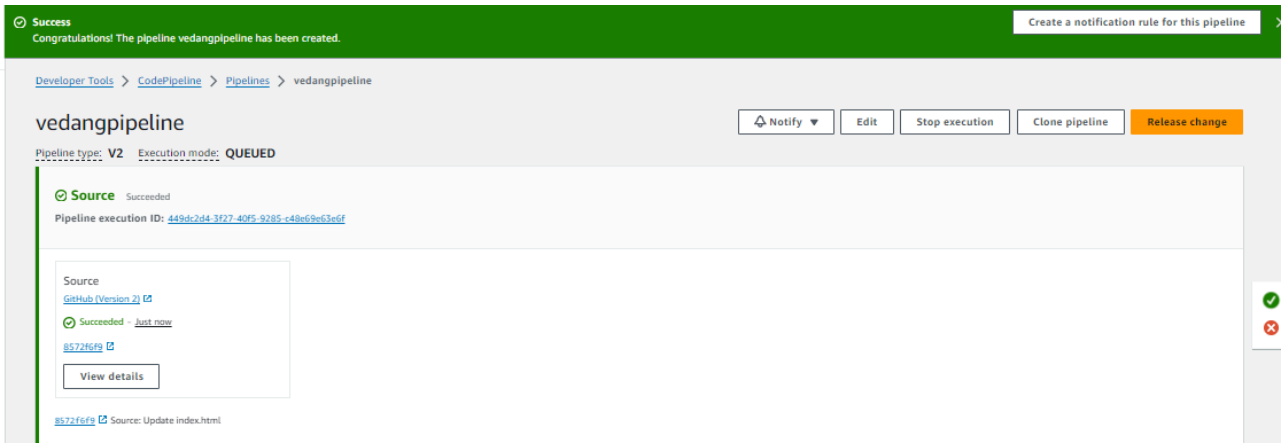


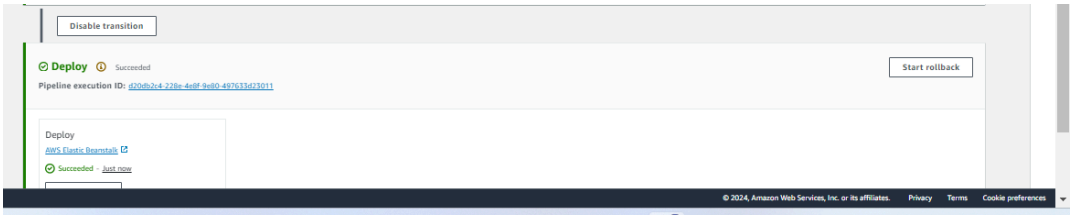

Source
Source provider
This is where you stored your input artifacts for your pipeline. Choose the provider and then provide the connection details.
GitHub (Version 2)
New GitHub version 2 (app-based) action
To add a GitHub version 2 action in CodePipeline, you create a connection, which uses GitHub Apps to access your repository. Use the options below to choose an existing connection or create a new one. Learn more
Connection
Choose an existing connection that you have already configured, or create a new one and then return to this task.
arn:aws:codeconnections:eu-north-1:442426860399:connection/6beaca66-5
or
Connect to GitHub
Ready to connect
Your GitHub connection is ready for use.
Repository name
Choose a repository in your GitHub account.
VedangWajge/aws-codepipeline-s3-codedeploy-linux-2.0
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.
master
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.

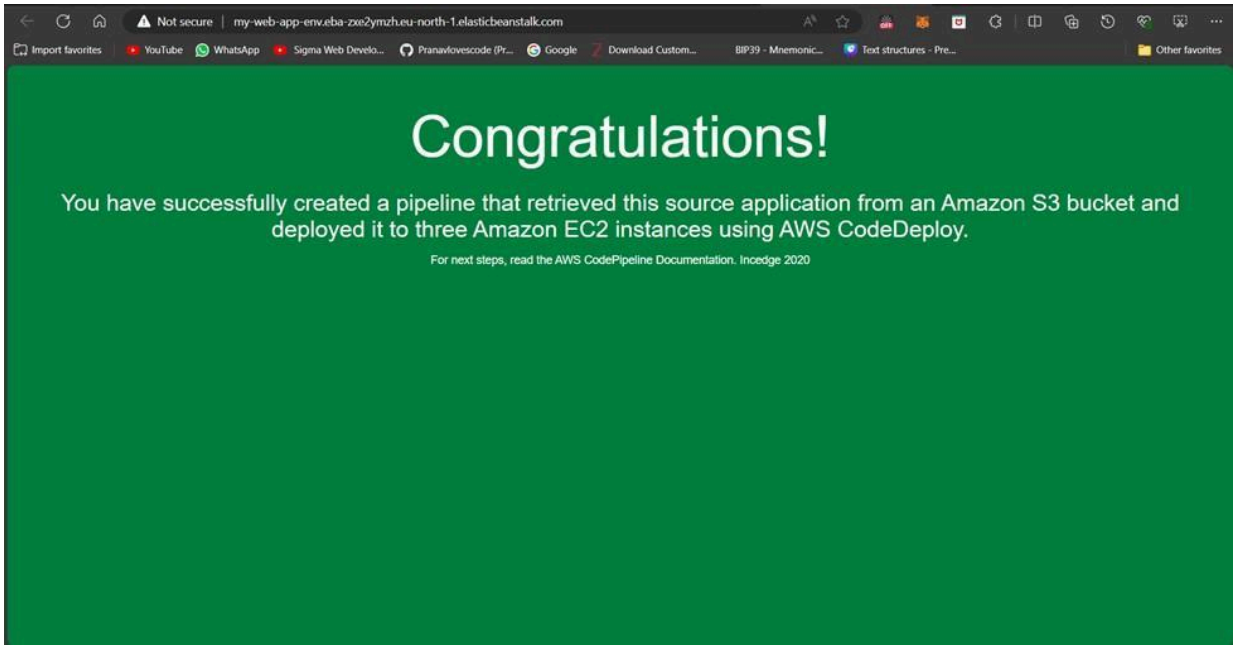

Add build stage
Step 3 of 5
Build - optional
Skip build stage
Your pipeline will not include a build stage. Are you sure you want to skip this stage?
Cancel
Skip
Next


Pipelines must have at least two stages. Your second stage must be either a build or deployment stage. Choose a provider for either the build stage or deployment stage.
Deploy
Deploy provider
Choose how you deploy to instances. Choose the provider, and then provide the configuration details for that provider.
AWS Elastic Beanstalk
Region
Europe (Stockholm)
Input artifacts
Choose an input artifact for this action. Learn more
No more than 100 characters
Application name
Choose an application that you have already created in the AWS Elastic Beanstalk console. Or create an application in the AWS Elastic Beanstalk console and then return to this task.
Vedangbean
Environment name
Choose an environment that you have already created in the AWS Elastic Beanstalk console. Or create an environment in the AWS Elastic Beanstalk console and then return to this task.
Vedangbean-env
Configure automatic rollback on stage failure
Cancel
Previous
Next

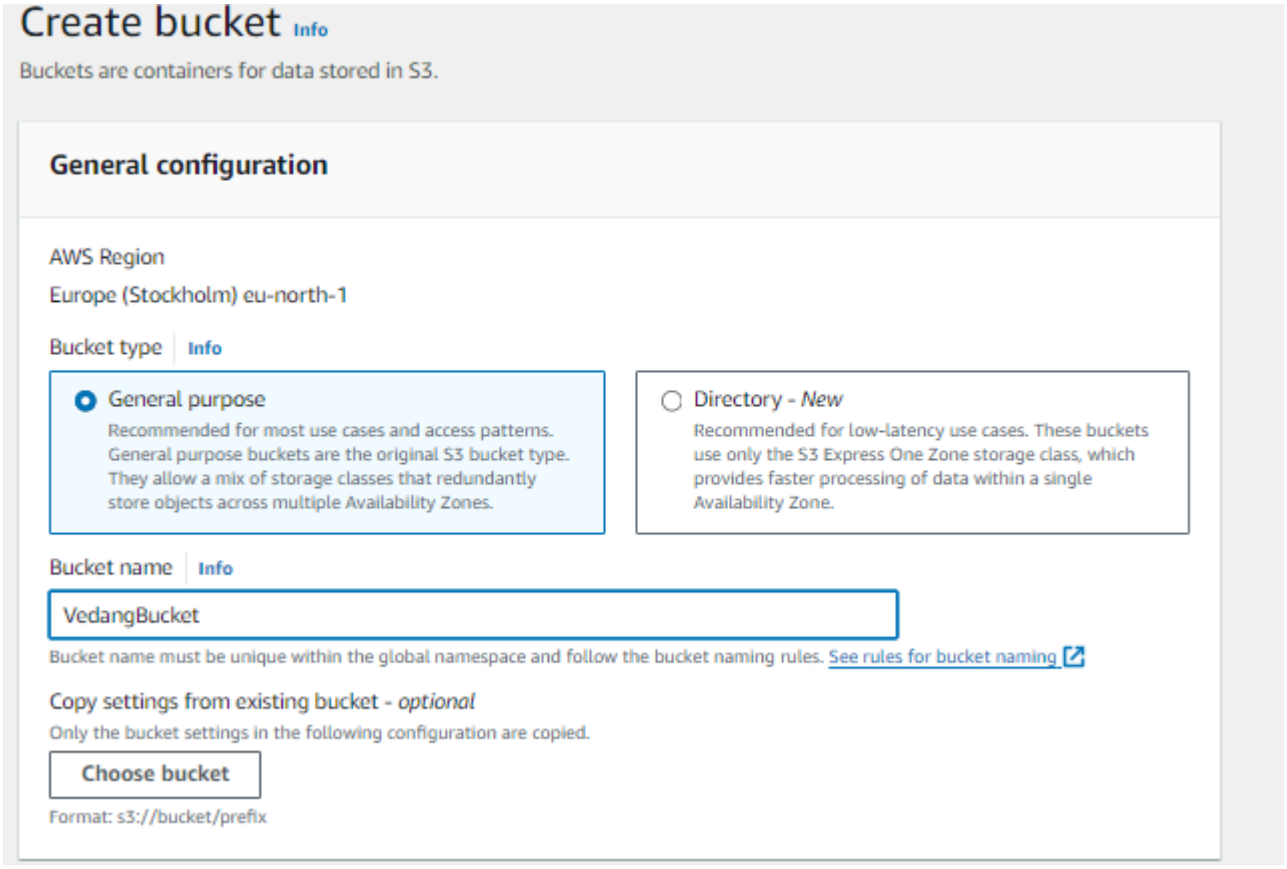

Step 4: Add deploy stage
Deploy action provider
Deploy action provider
AWS Elastic Beanstalk
ApplicationName
Vedangbean
EnvironmentName
Vedangbean-env
Configure automatic rollback on stage failure
Disabled
Cancel
Previous
Create pipeline

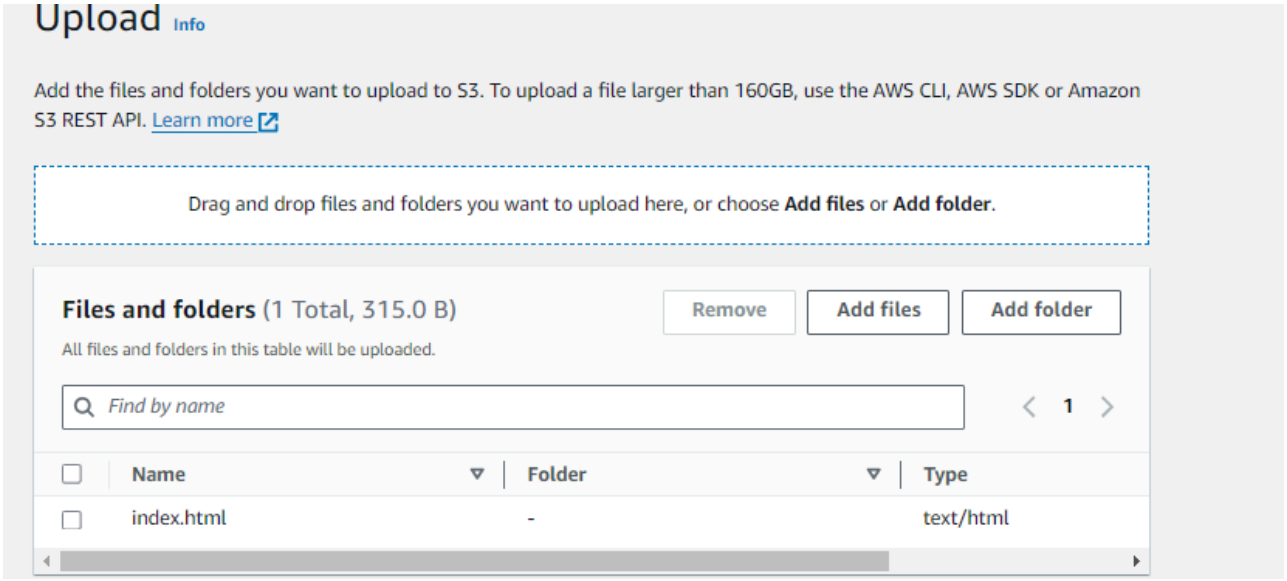

Success
Congratulations! The pipeline vedangpipeline has been created.
Create a notification rule for this pipeline
Developer Tools > CodePipeline > Pipelines > vedangpipeline
vedangpipeline
Notify
Edit
Stop execution
Clone pipeline
Release change
Pipeline type: V2
Execution mode: QUEUED
Source
Succeeded
Pipeline execution ID: 449dc2d4-3f27-40f5-9285-c48e69e63e6f
Source
GitHub (Version 2)
Succeeded - Just now
8572f6f9
View details
8572f6f9 Source: Update index.html


Disable transition
Deploy
Succeeded
Start rollback
Pipeline execution ID: d20db2c4-228e-4e8f-9e80-497633d23011
Deploy
AWS Elastic Beanstalk
Succeeded - Just now
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Not secure | my-web-app-env.eba-zxe2ymzh.eu-north-1.elasticbeanstalk.com
Import favorites
YouTube
WhatsApp
Sigma Web Develo...
Pranavlovescode (Pr...
Google
Download Custom...
BIP39 - Mnemonic...
Text structures - Pre...
Other favorites
Congratulations!
You have successfully created a pipeline that retrieved this source application from an Amazon S3 bucket and deployed it to three Amazon EC2 instances using AWS CodeDeploy.
For next steps, read the AWS CodePipeline Documentation. Incedge 2020

Using S3 Bucket:





Edit Block public access (bucket settings) Info

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

- ☐ **Block *all* public access**
  Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
  - ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
    S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
  - ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
    S3 will ignore all ACLs that grant public access to buckets and objects.
  - ☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
    S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
  - ☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**

Object Ownership

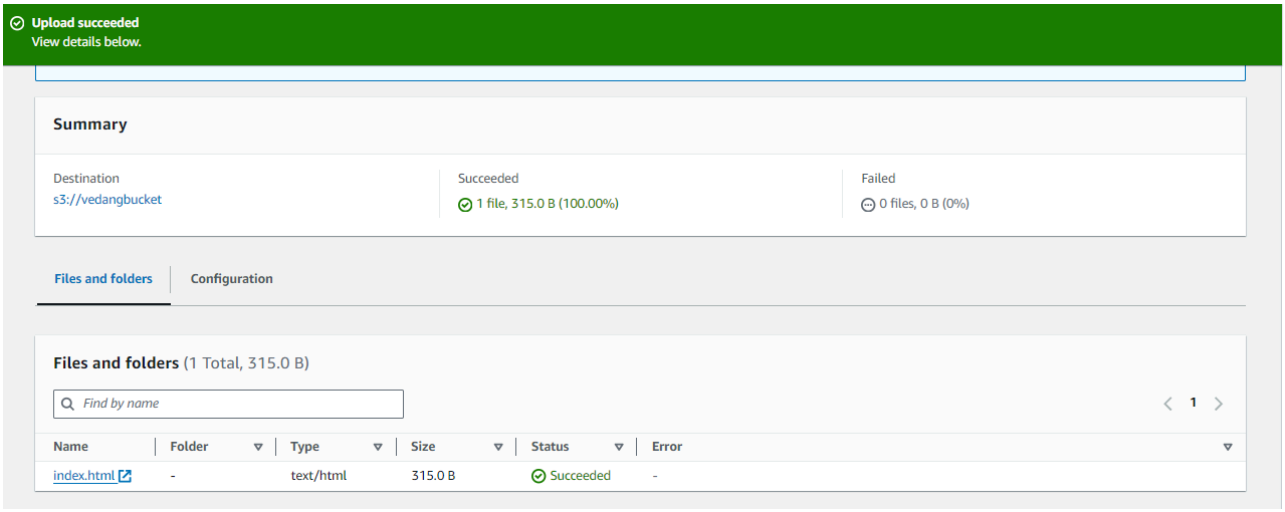
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

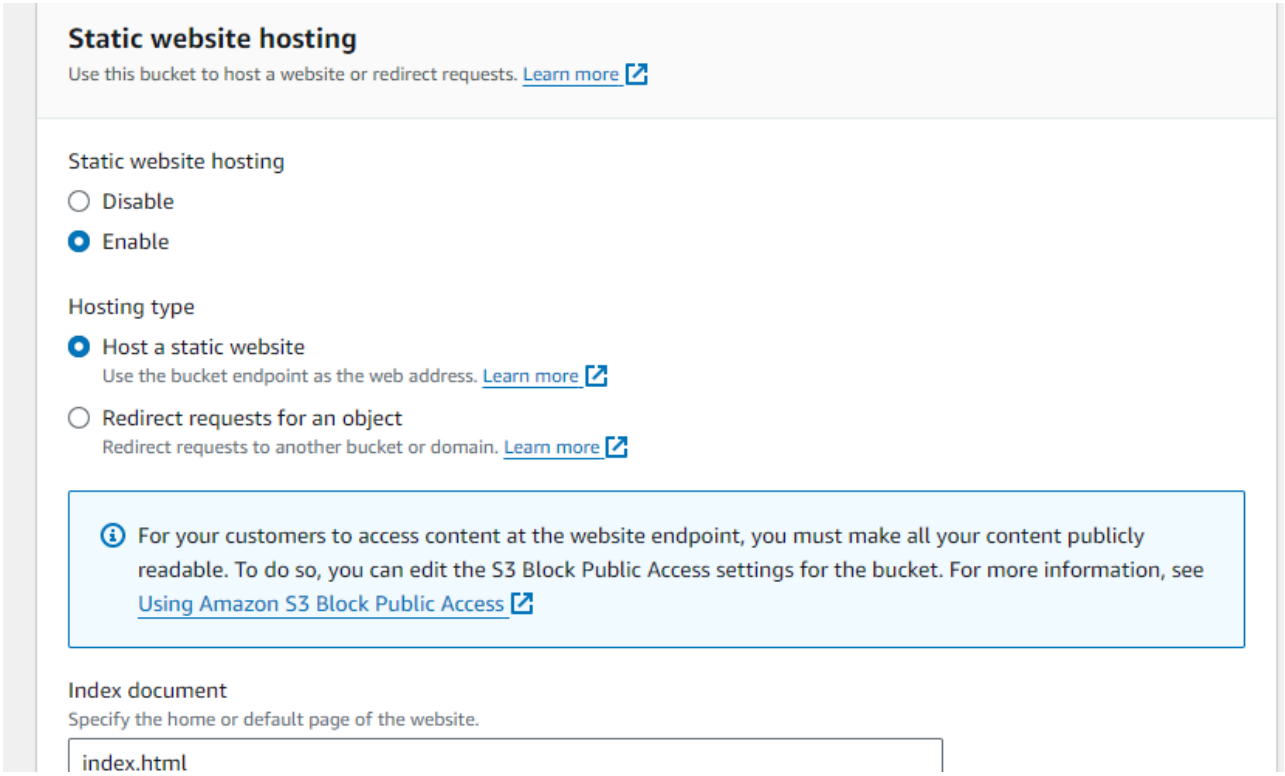
- ○ ACLs disabled (recommended)
  All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
- ◉ ACLs enabled
  Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

⚠ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

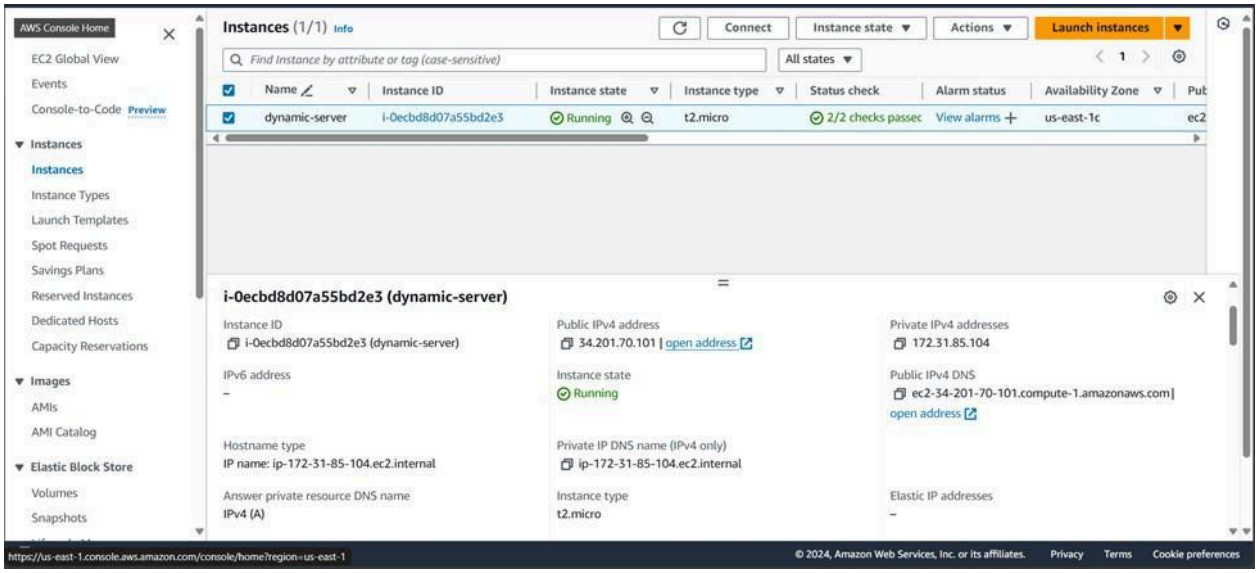
⚠ **Enabling ACLs turns off the bucket owner enforced setting for Object Ownership**
Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.

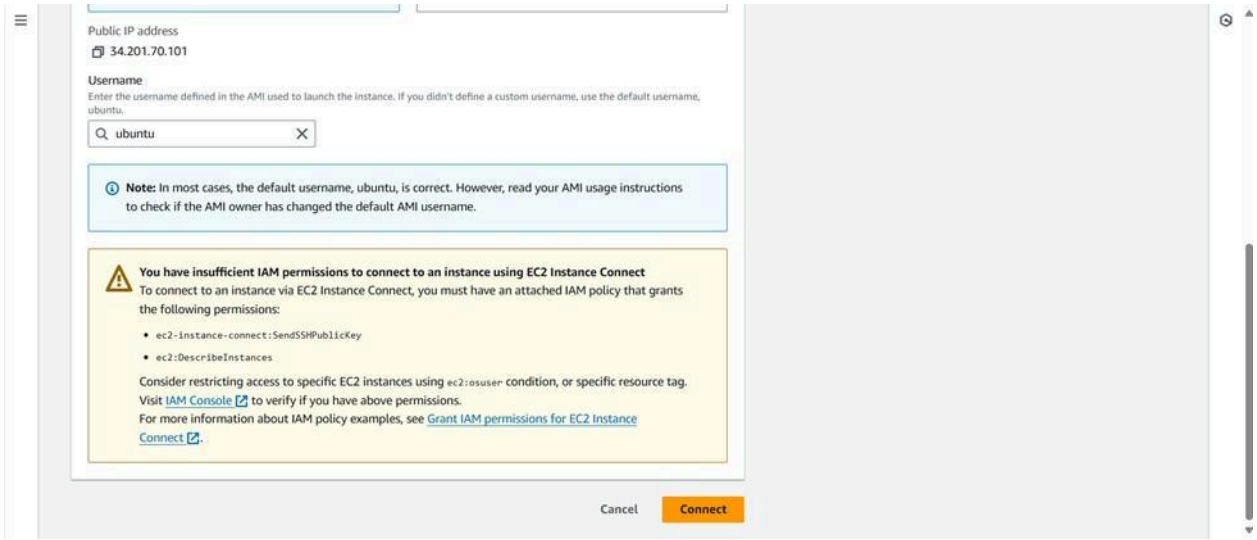
☑ I acknowledge that ACLs will be restored.


Upload succeeded
View details below.
Summary
Destination
s3://vedangbucket
Succeeded
1 file, 315.0 B (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 Total, 315.0 B)
Find by name
1
Name
Folder
Type
Size
Status
Error
index.html
-
text/html
315.0 B
Succeeded
-


Static website hosting
Use this bucket to host a website or redirect requests. Learn more
Static website hosting
Disable
Enable
Hosting type
Host a static website
Use the bucket endpoint as the web address. Learn more
Redirect requests for an object
Redirect requests to another bucket or domain. Learn more
For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access
Index document
Specify the home or default page of the website.
index.html

Using EC2:

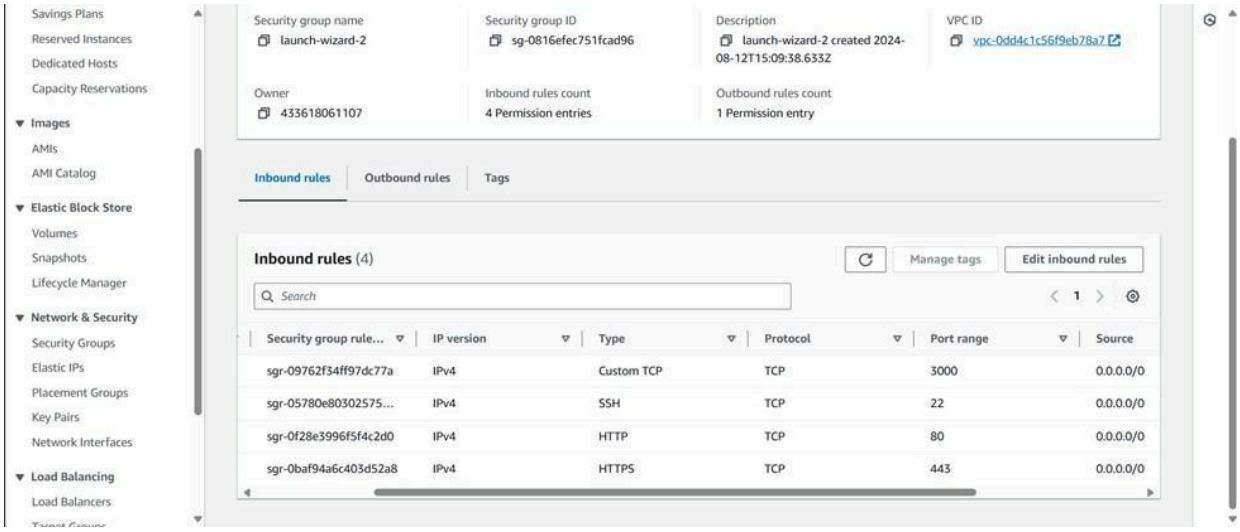


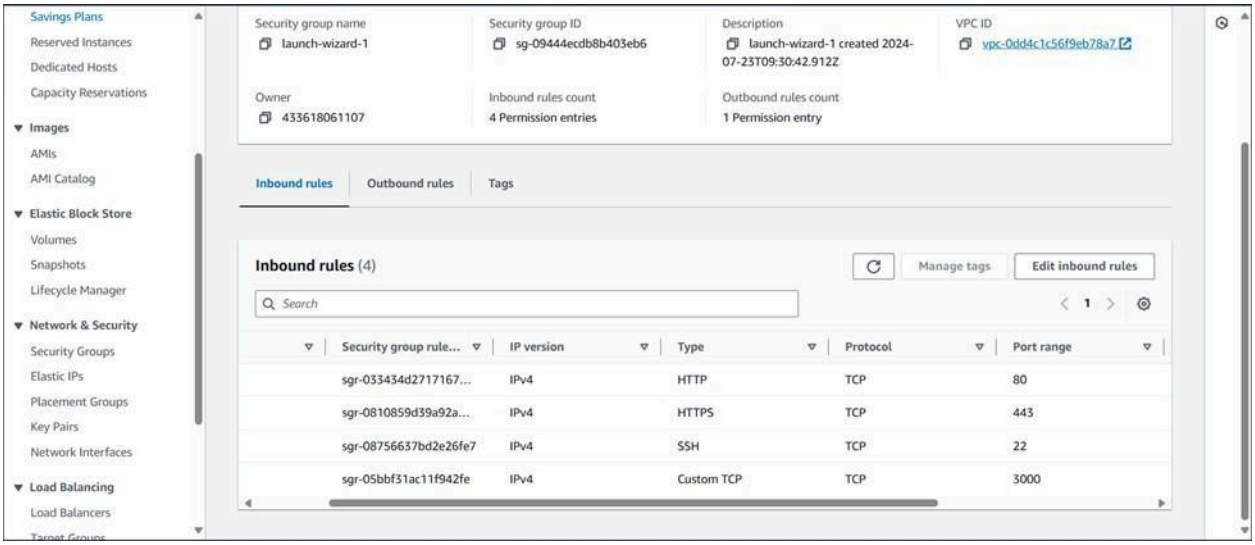



```
ubuntu@ip-172-31-85-104:~$ pwd
/home/ubuntu
ubuntu@ip-172-31-85-104:~$ mkdir pranav
ubuntu@ip-172-31-85-104:~$ cd pranav
ubuntu@ip-172-31-85-104:~/pranav$ git clone https://github.com/Pranavlovescode/Dynamic-website-hosting-sample.git
Cloning into 'Dynamic-website-hosting-sample'...
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 6 (delta 0), reused 6 (delta 0), pack-reused 0
Receiving objects: 100% (6/6), 11.16 KiB | 5.58 MiB/s, done.
```

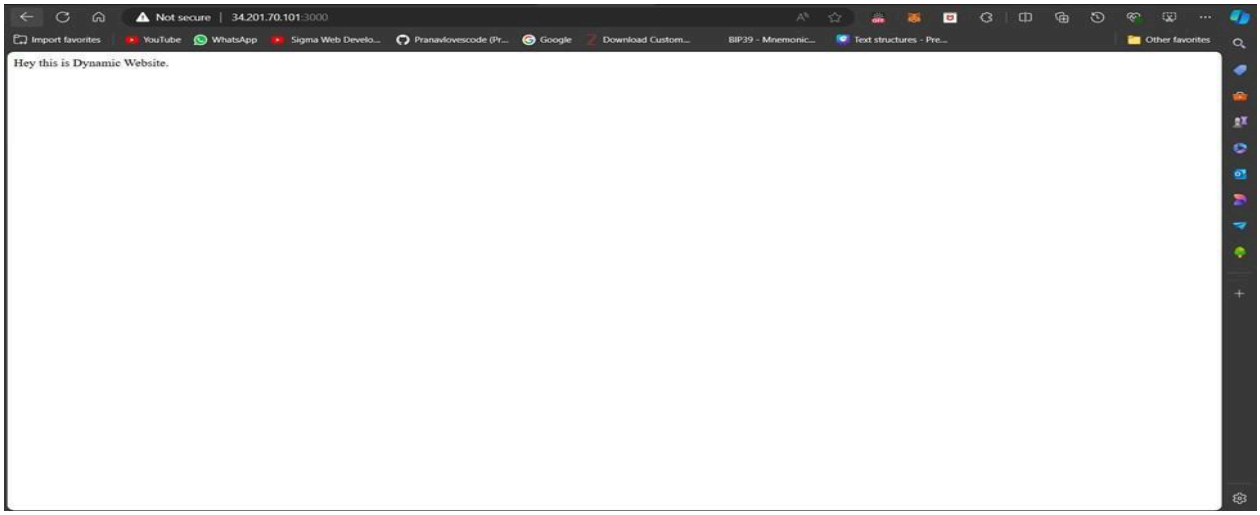
```
ubuntu@ip-172-31-85-104:~/pranav$ ls
Dynamic-website-hosting-sample
ubuntu@ip-172-31-85-104:~/pranav$ cd Dynamic-website-hosting-sample/
ubuntu@ip-172-31-85-104:~/pranav/Dynamic-website-hosting-sample$ ls
index.js  package-lock.json  package.json
ubuntu@ip-172-31-85-104:~/pranav/Dynamic-website-hosting-sample$ npm i

added 93 packages, and audited 94 packages in 3s

16 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
npm notice
npm notice New patch version of npm available! 10.8.1 -> 10.8.2
npm notice Changelog: https://github.com/npm/cli/releases/tag/v10.8.2
npm notice To update run: npm install -g npm@10.8.2
npm notice
```

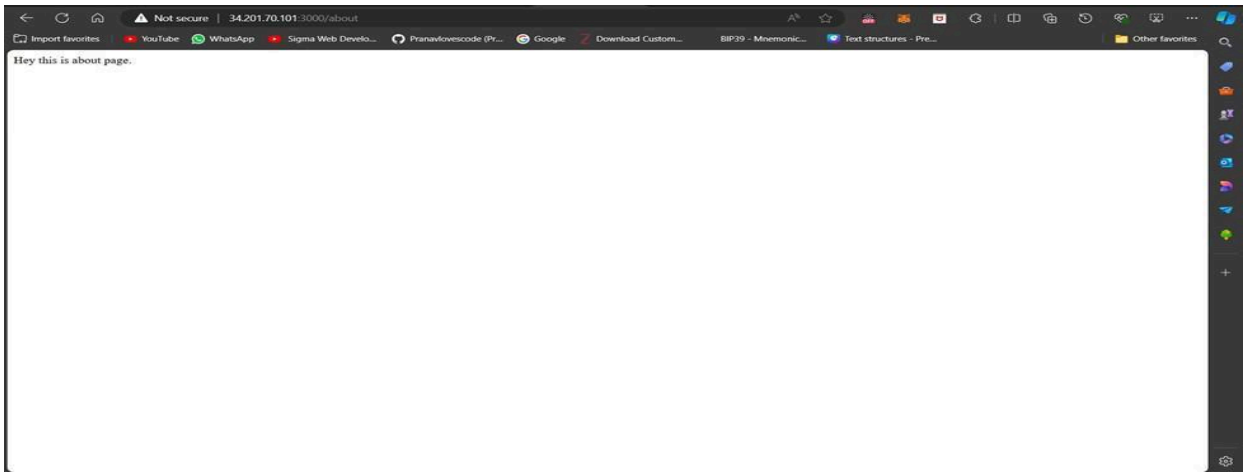
```
ubuntu@ip-172-31-85-104:~/pranav/Dynamic-website-hosting-sample$ npm start

> hosting-dynamic-website@1.0.0 start
> nodemon index.js

[nodemon] 3.1.4
[nodemon] to restart at any time, enter `rs`
[nodemon] watching path(s): *.*
[nodemon] watching extensions: js,mjs,cjs,json
[nodemon] starting `node index.js`
Server is running on port 3000
```




Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Load Balancing
Load Balancers
Security group name
launch-wizard-1
Security group ID
sg-09444ecdb8b403eb6
Description
launch-wizard-1 created 2024-07-23T09:30:42.912Z
VPC ID
vpc-0dd4c1c56f9eb78a7
Owner
433618061107
Inbound rules count
4 Permission entries
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Tags
Inbound rules (4)
Manage tags
Edit inbound rules
Search
Security group rule...
IP version
Type
Protocol
Port range
sgr-033434d2717167...
IPv4
HTTP
TCP
80
sgr-0810859d39a92a...
IPv4
HTTPS
TCP
443
sgr-08756637bd2e26fe7
IPv4
SSH
TCP
22
sgr-05bbf31ac11f942fe
IPv4
Custom TCP
TCP
3000

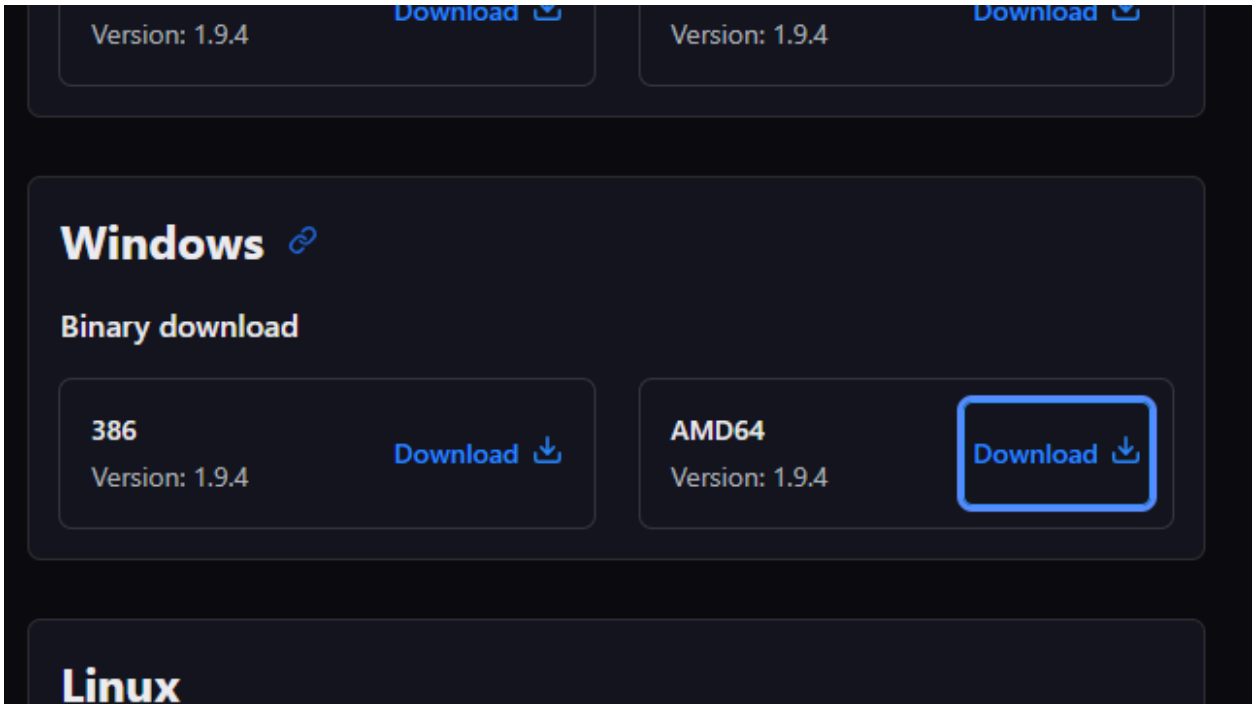
Hosting:

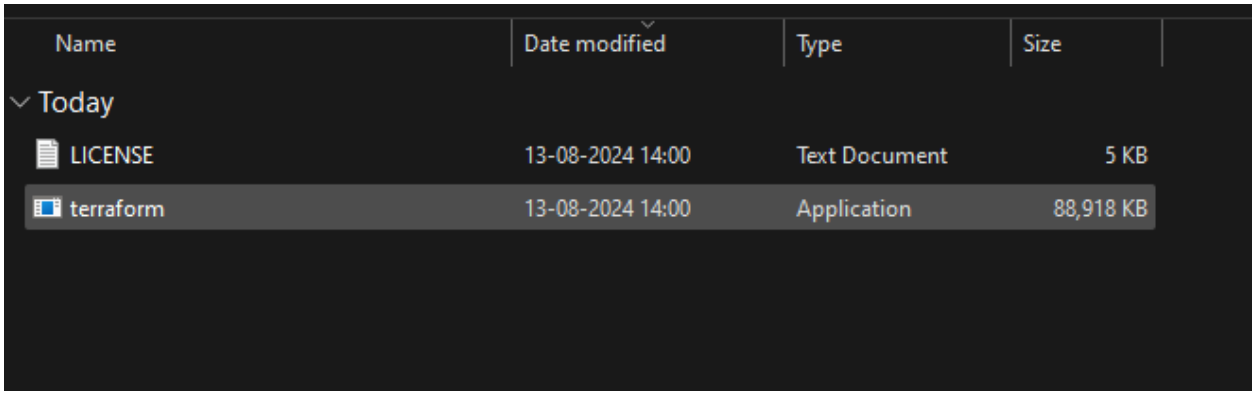

Not secure | 34.201.70.101:3000
Hey this is Dynamic Website.

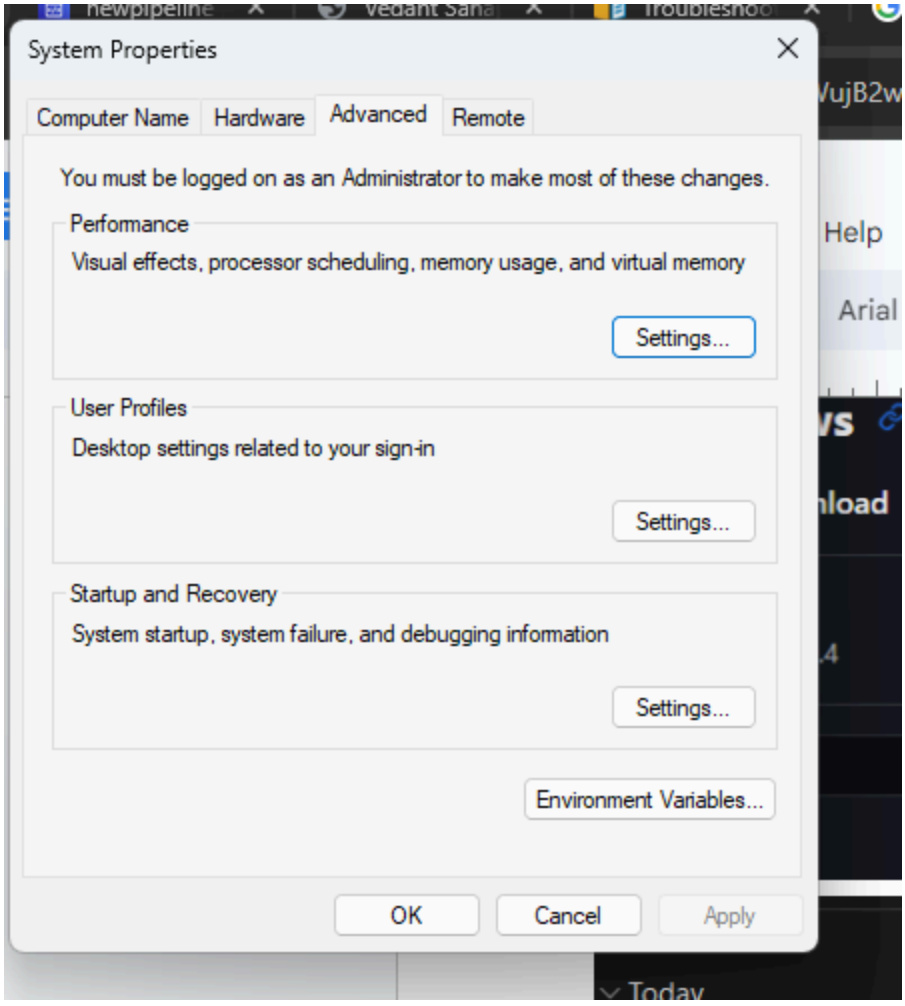

Not secure | 34.201.70.101:3000/about
Hey this is about page.

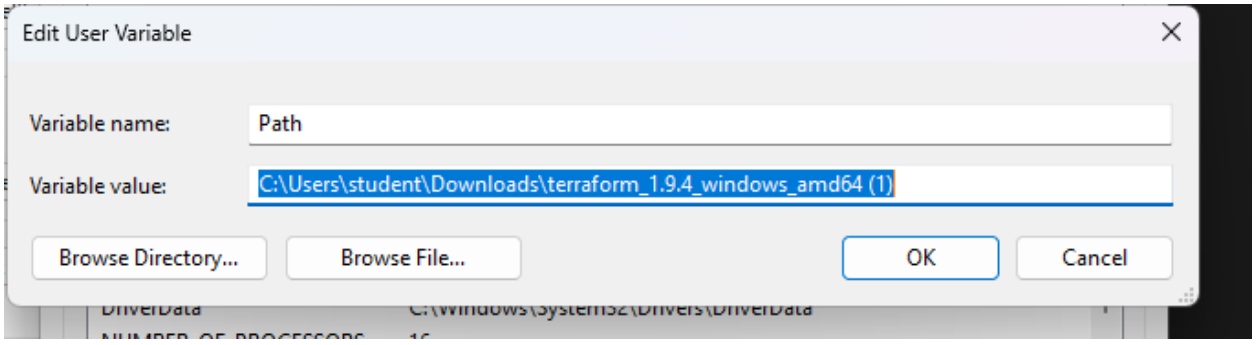
ADVANCE DEVOPS EXP-5

Vedang Wajge **D15A/66**






System Properties
Computer Name
Hardware
Advanced
Remote
You must be logged on as an Administrator to make most of these changes.
Performance
Visual effects, processor scheduling, memory usage, and virtual memory
Settings...
User Profiles
Desktop settings related to your sign-in
Settings...
Startup and Recovery
System startup, system failure, and debugging information
Settings...
Environment Variables...
OK
Cancel
Apply


Edit User Variable
Variable name:
Path
Variable value:
C:\Users\student\Downloads\terraform_1.9.4_windows_amd64 (1)
Browse Directory...
Browse File...
OK
Cancel


Windows PowerShell
System
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar

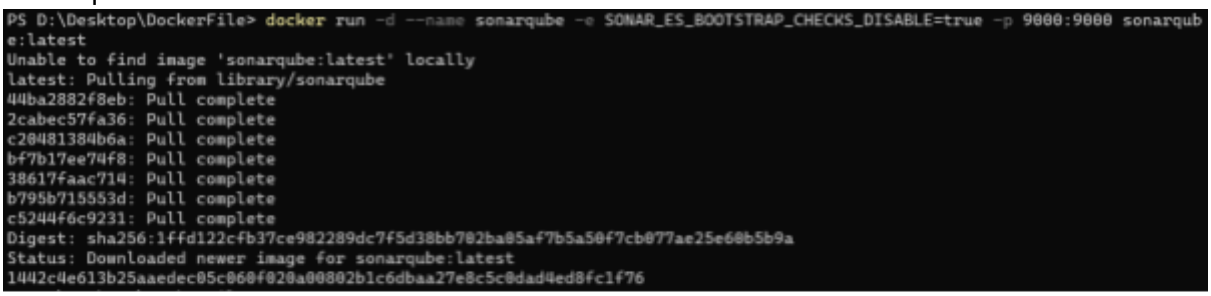
```
PS C:\Users\student> terraform
Usage: terraform [global options] <subcommand> [args]

The available commands for execution are listed below.
The primary workflow commands are given first, followed by
less common or more advanced commands.

Main commands:
  init          Prepare your working directory for other commands
  validate      Check whether the configuration is valid
  plan          Show changes required by the current configuration
  apply         Create or update infrastructure
  destroy       Destroy previously-created infrastructure

All other commands:
  console       Try Terraform expressions at an interactive command prompt
  fmt           Reformat your configuration in the standard style
  force-unlock  Release a stuck lock on the current workspace
  get           Install or upgrade remote Terraform modules
  graph         Generate a Graphviz graph of the steps in an operation
  import        Associate existing infrastructure with a Terraform resource
  login         Obtain and save credentials for a remote host
  logout        Remove locally-stored credentials for a remote host
  metadata      Metadata related commands
  output        Show output values from your root module
  providers     Show the providers required for this configuration
  refresh       Update the state to match remote systems
  show          Show the current state or a saved plan
  state         Advanced state management
  taint         Mark a resource instance as not fully functional
  test          Execute integration tests for Terraform modules
  untaint       Remove the 'tainted' state from a resource instance
  version       Show the current Terraform version
```

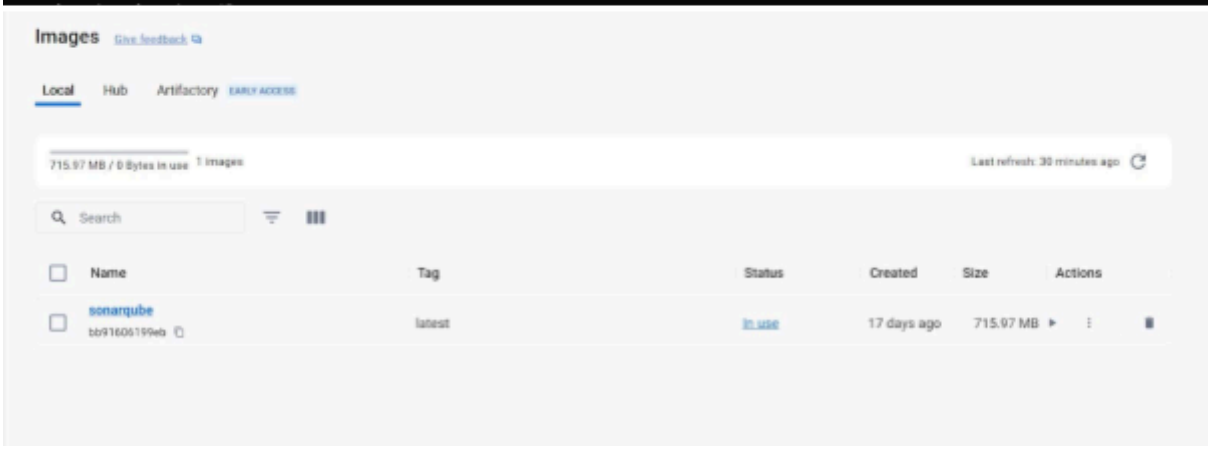
Vedang Wajge **D15A** **66**

Experiment No 7

AIM: Installing SonarQube from the Docker Image

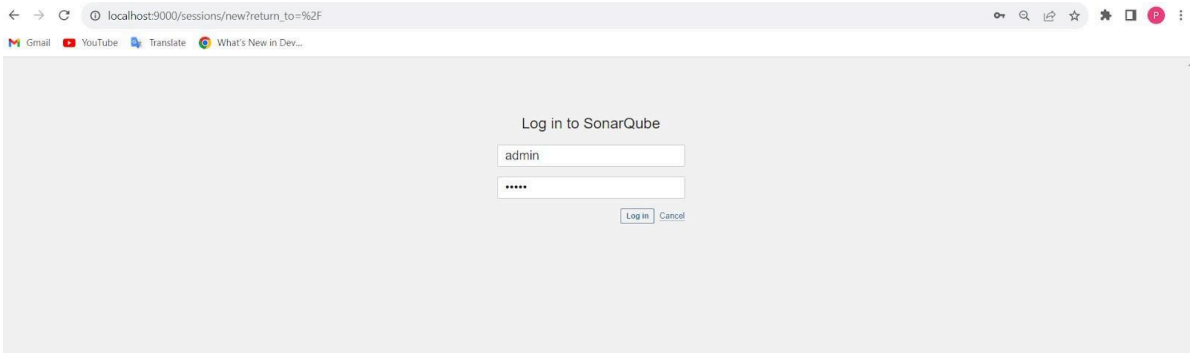
$ docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000
Sonarqube:latest



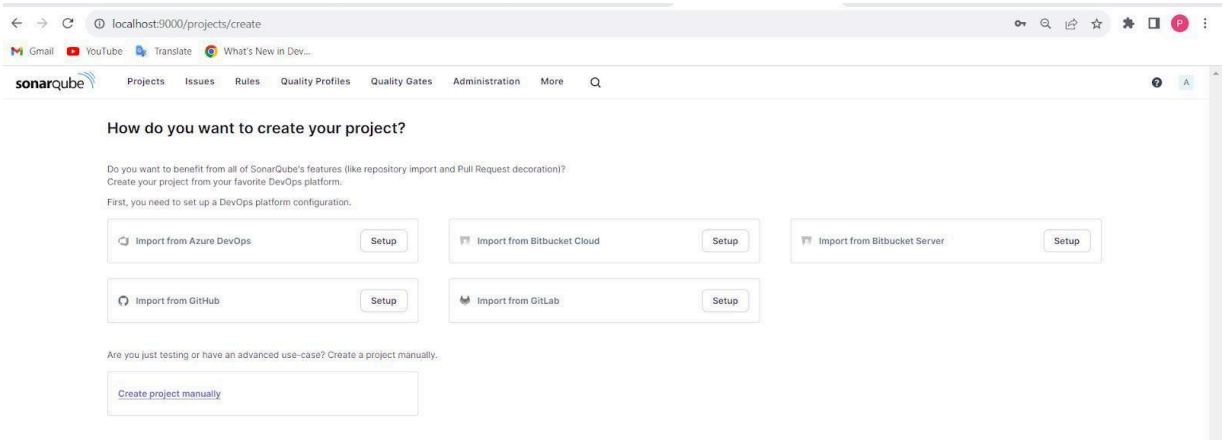


go to the SonarQube page by typing:
http://localhost:9000/ on your browser.

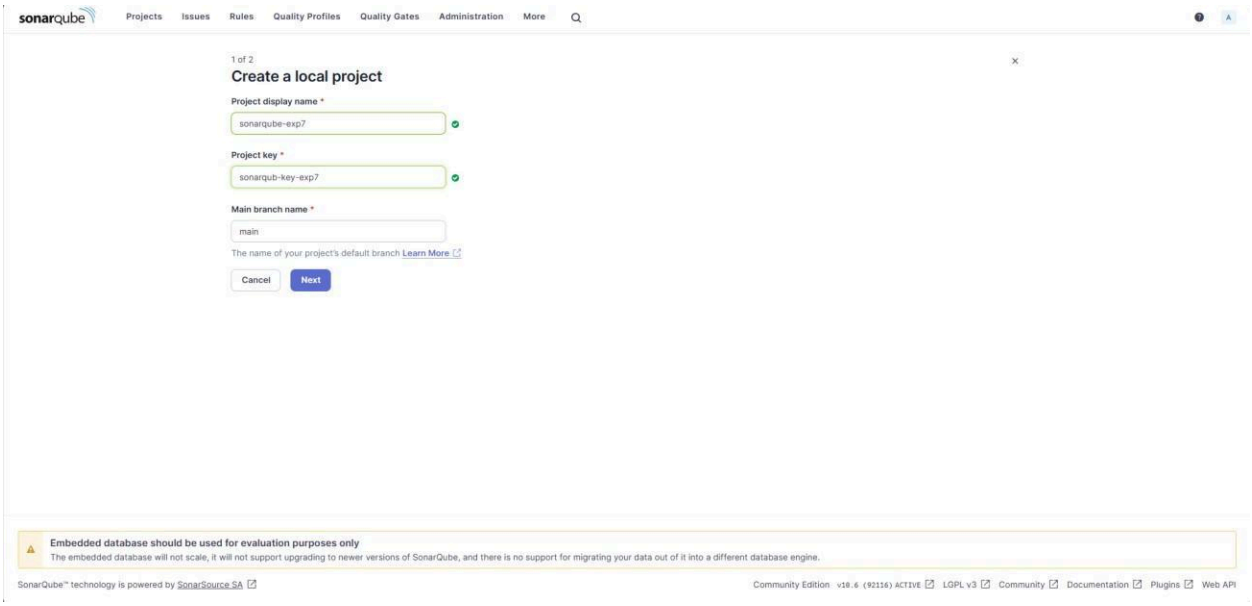
Installation is successful if you see this page

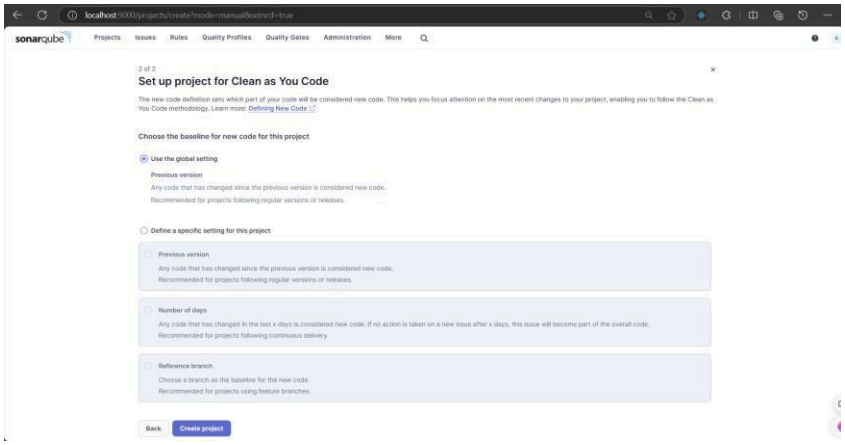


Update to new password

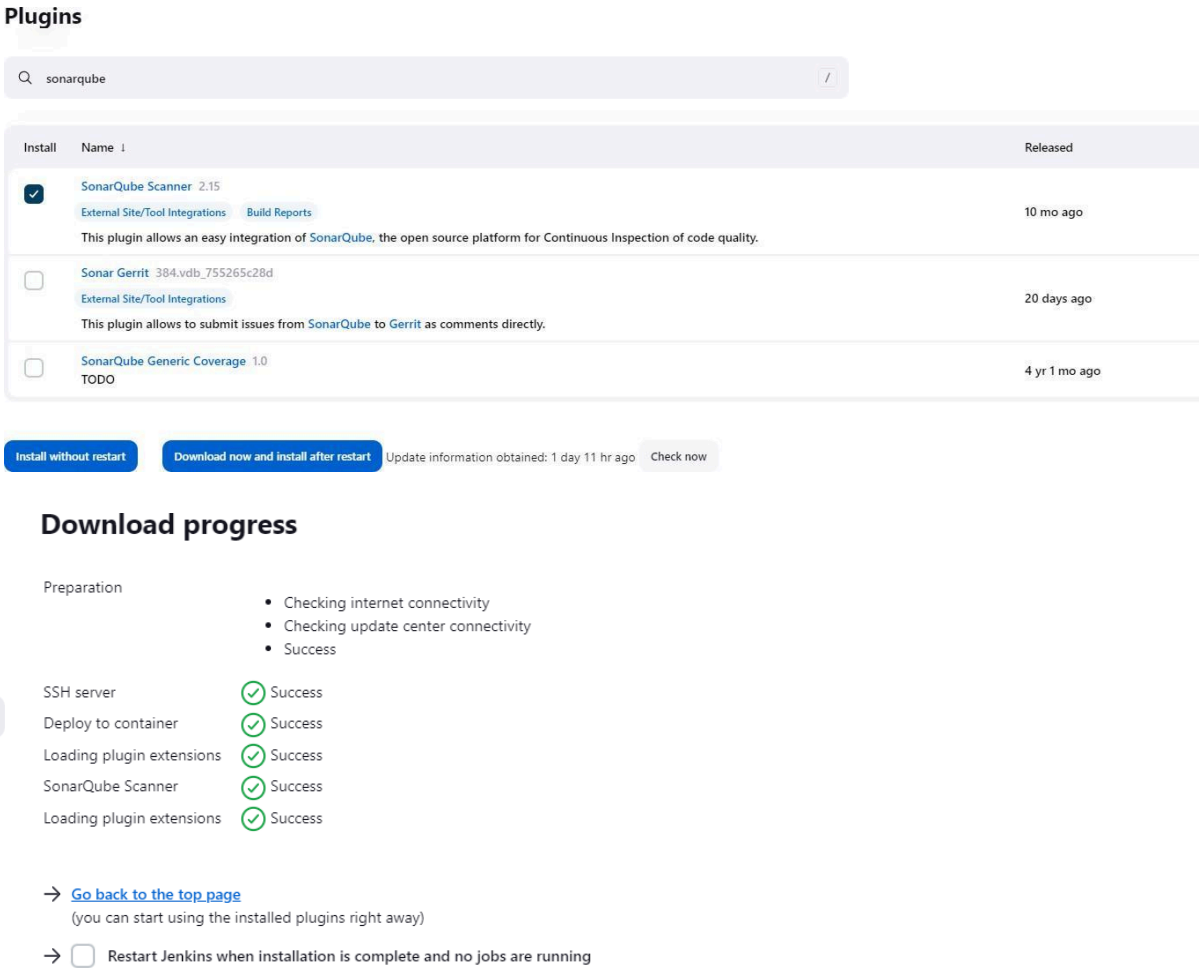


Create project manually: Here project name is “AdDevops”

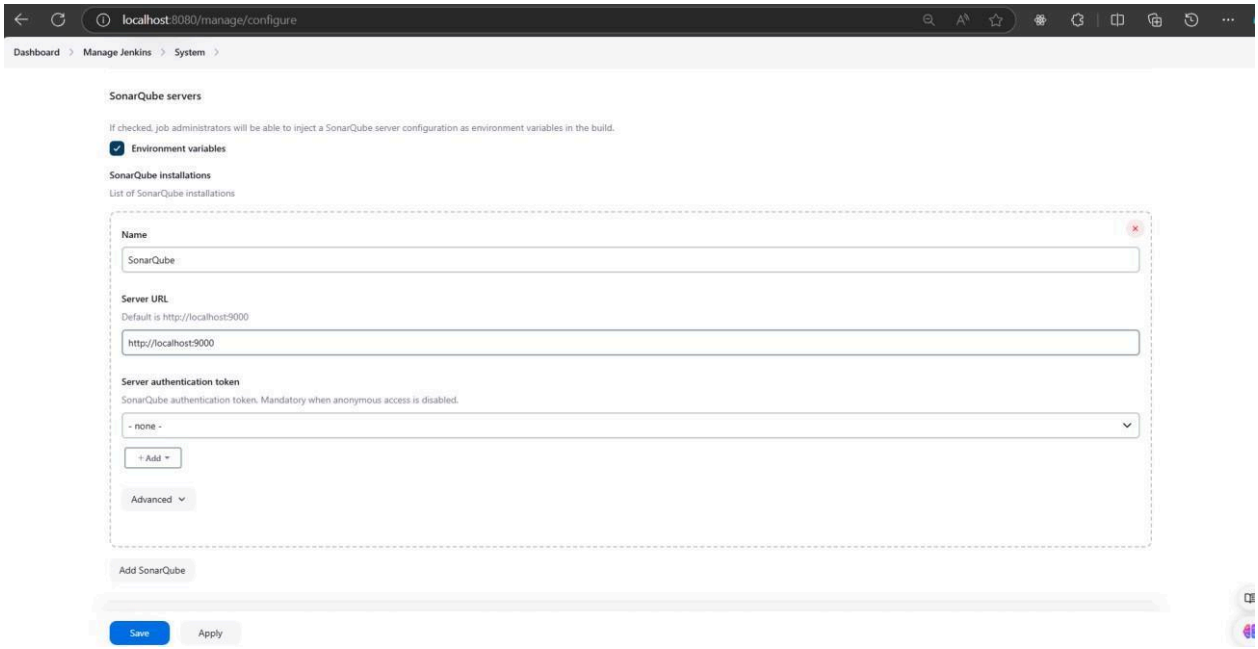




open Jenkins
Go to Dashboard ->Manage Jenkins -> Plugin Manager and search for SonarQube Scanner under Available plugins for Jenkins and install without restart.

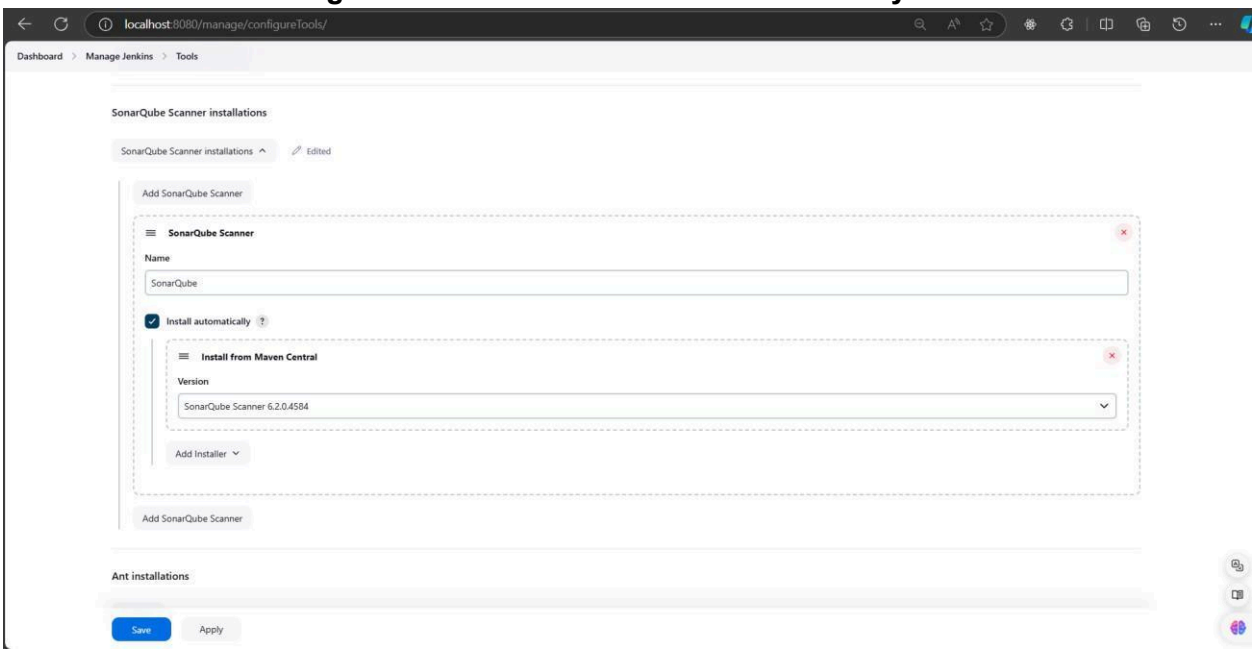


Under Jenkins ,
Dashboard -> Manage Jenkins -> Configure System ,
Look for SonarQube Servers and enter the details. Enter the Server Authentication Token if needed.

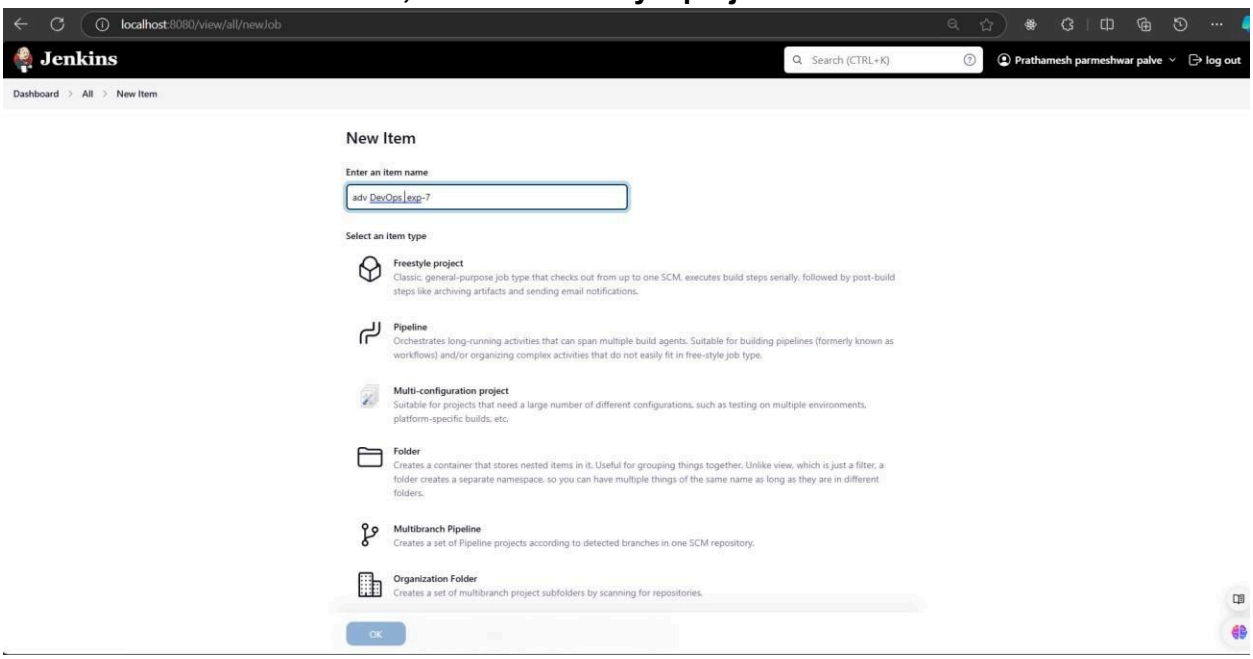


Search SonarQube Scanner under Dashboard -> Manage Jenkins -> Global Tool Configuration.

Choose the latest configuration and choose Install Automatically.

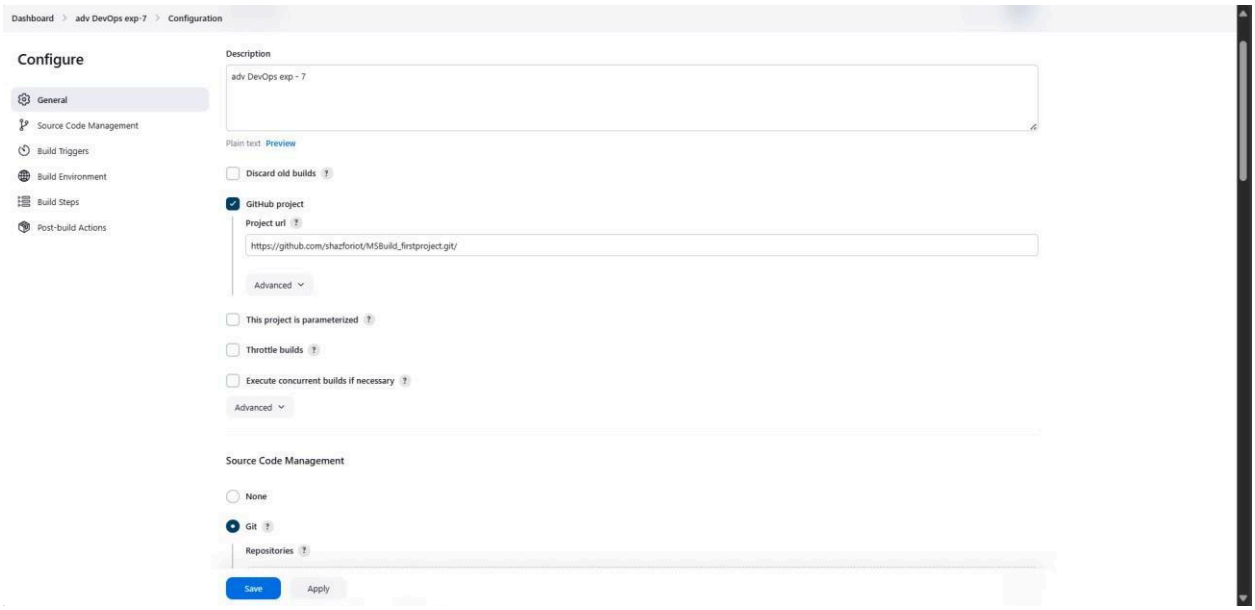


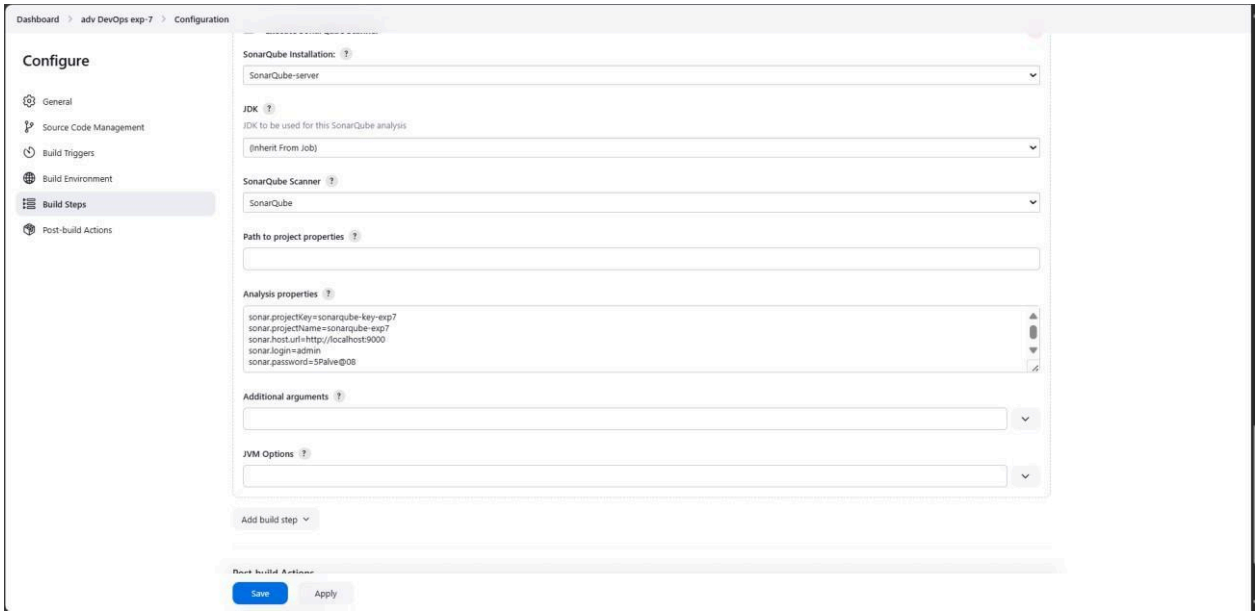
create a New Item in Jenkins, choose a freestyle project.



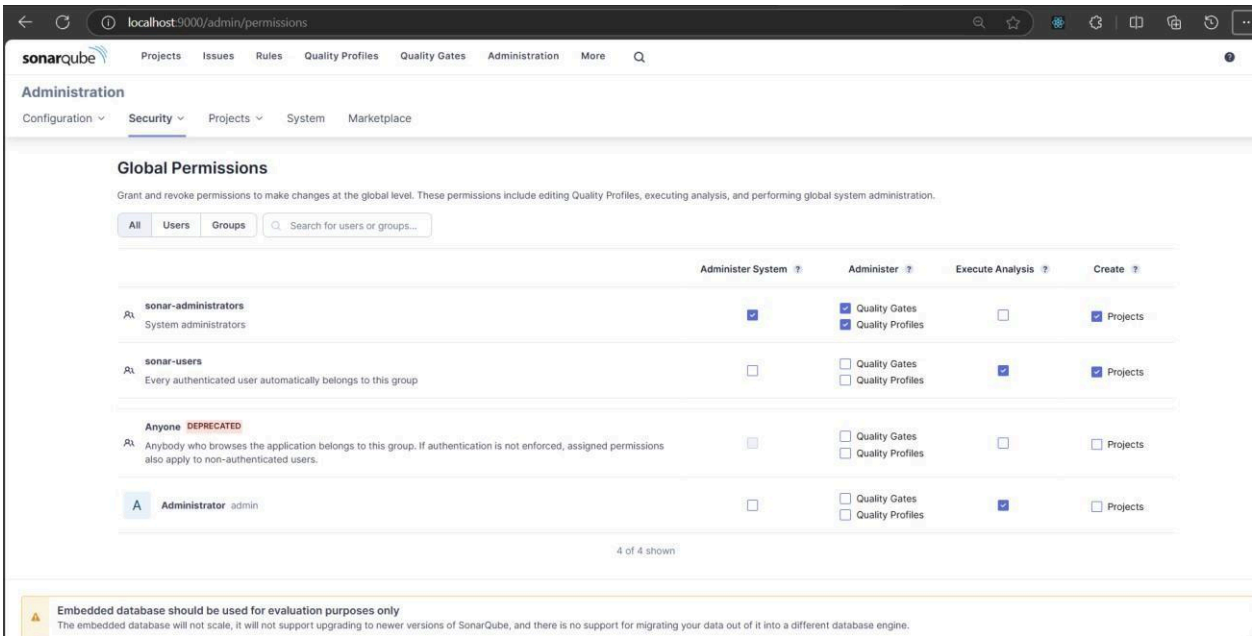
Choose this GitHub repository in Source Code Management.
https://github.com/shazforiot/MSBuild_firstproject.git

Under Build ->Execute SonarQube Scanner, enter these Analysis properties. Mention the SonarQube Project Key, Login, Password, and Host URL.
sonar.projectKey=SonarQueue-key
sonar.login=admin
sonar.password=admin
sonar.hosturl=http://localhost:9000/

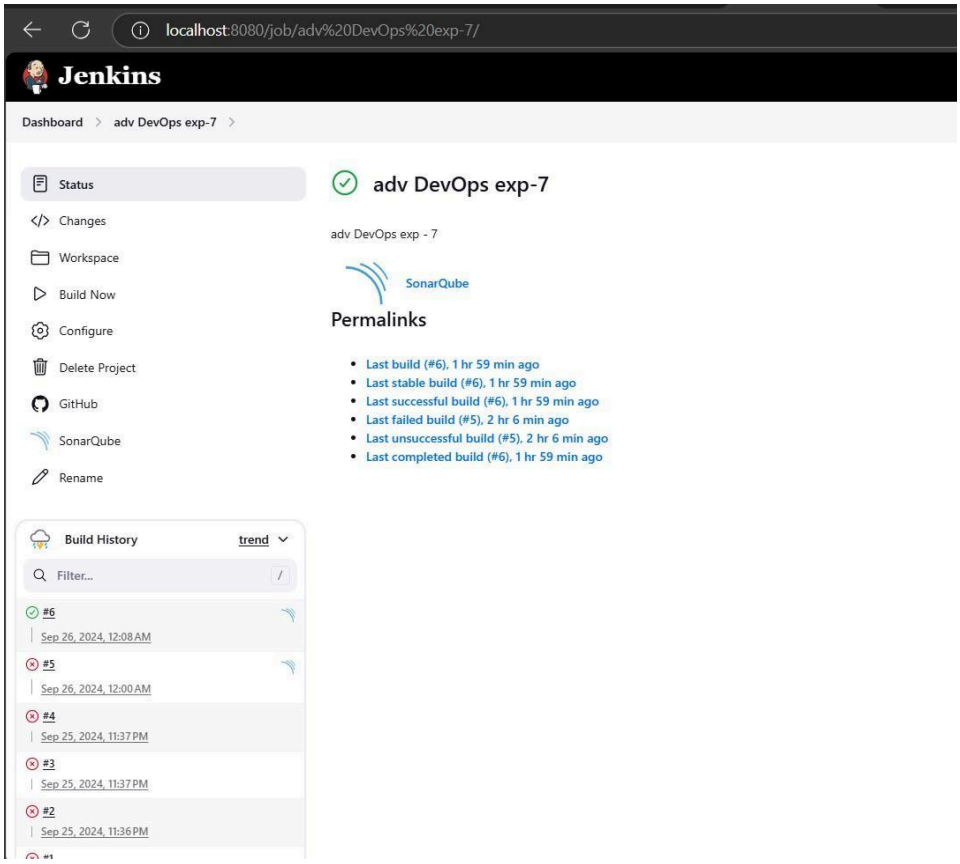


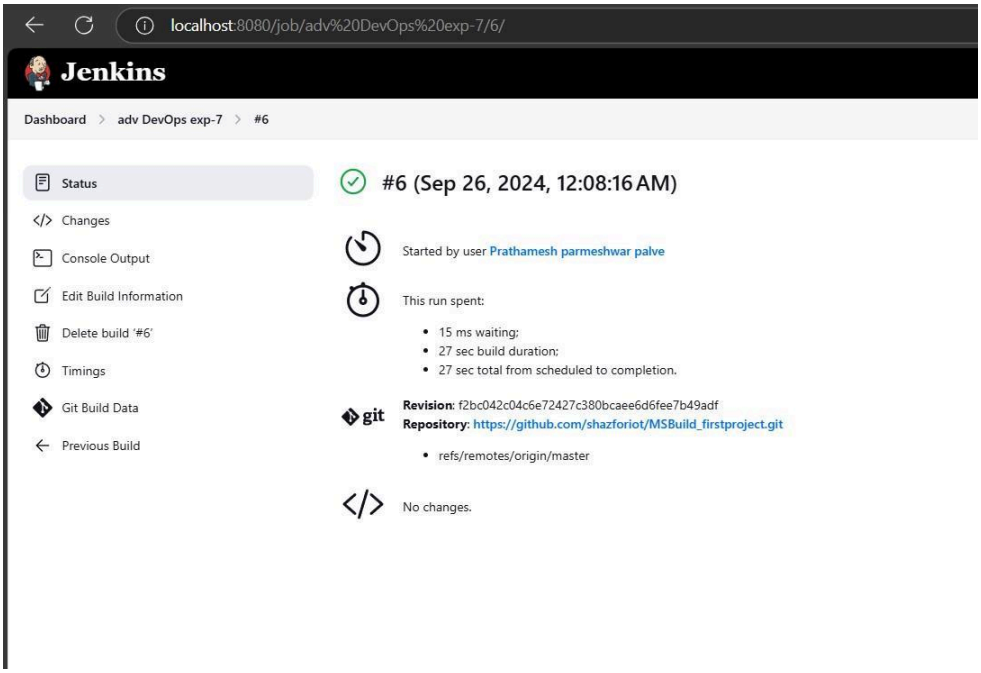


Go to http://localhost:9000/ and enter your previously created username.
Go to Permissions and grant the Admin user Execute Permissions.

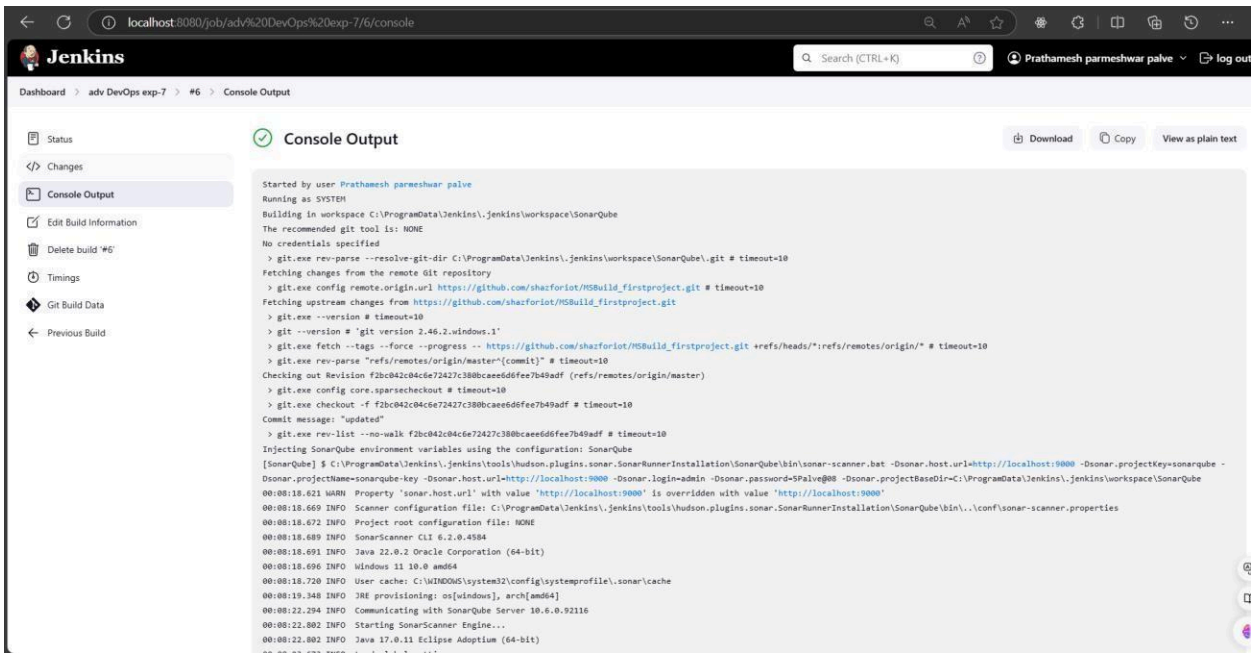


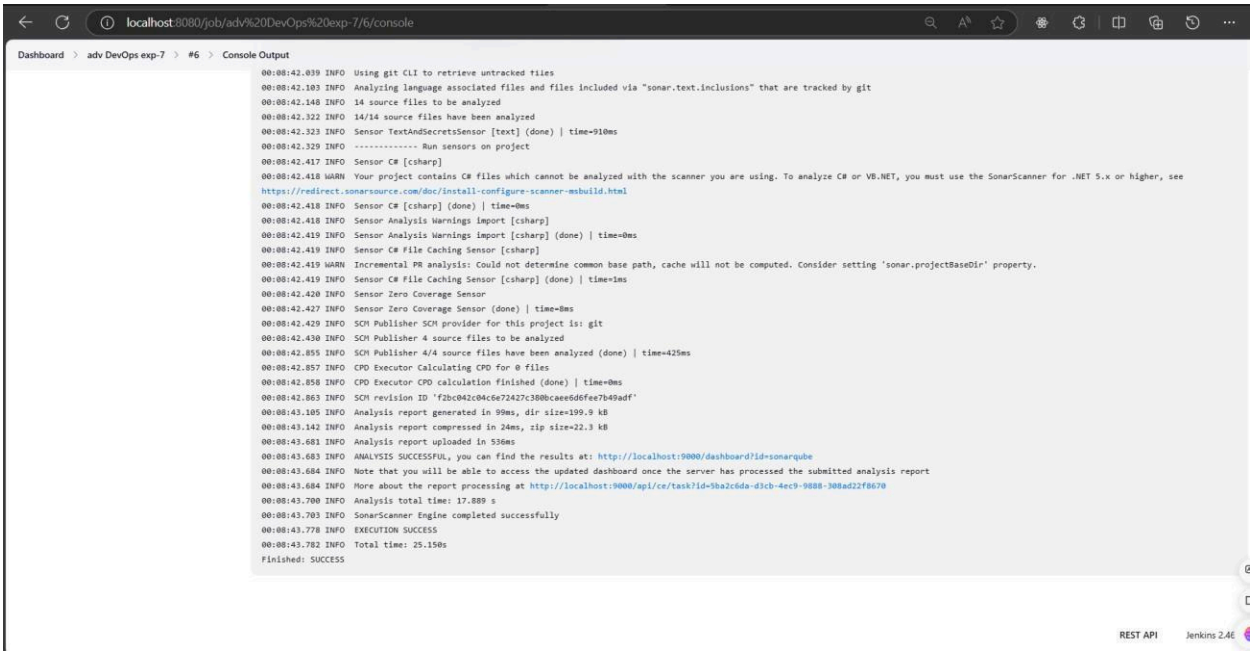
Build and Run:



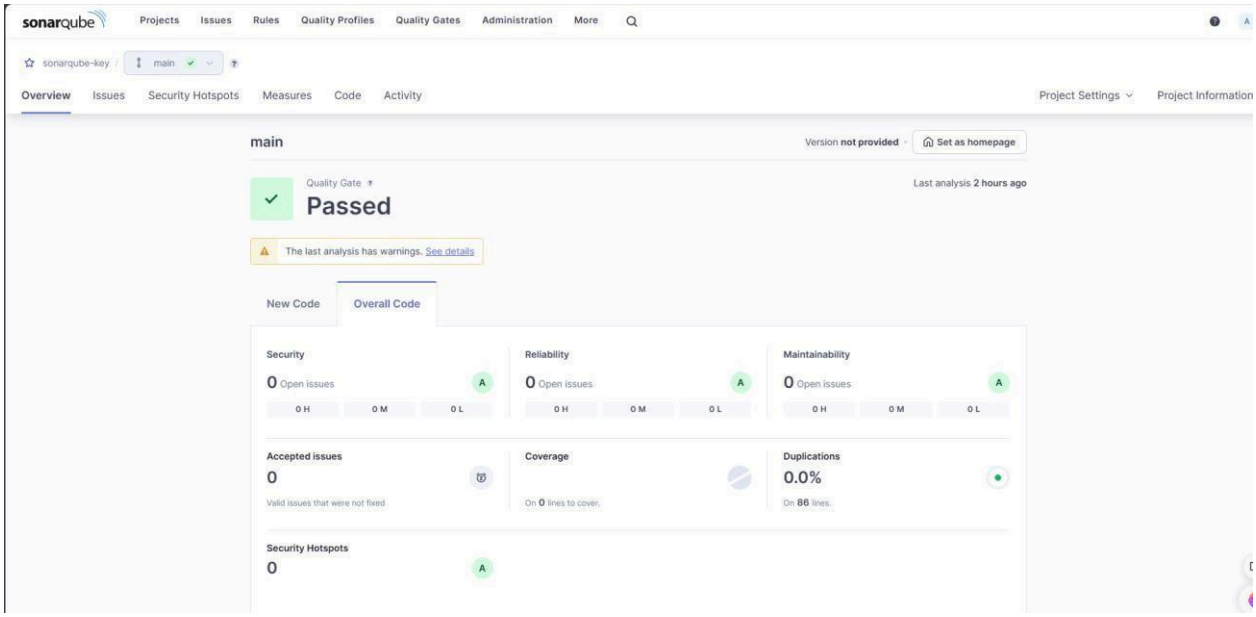


Console Output:





Project on sonarqube:



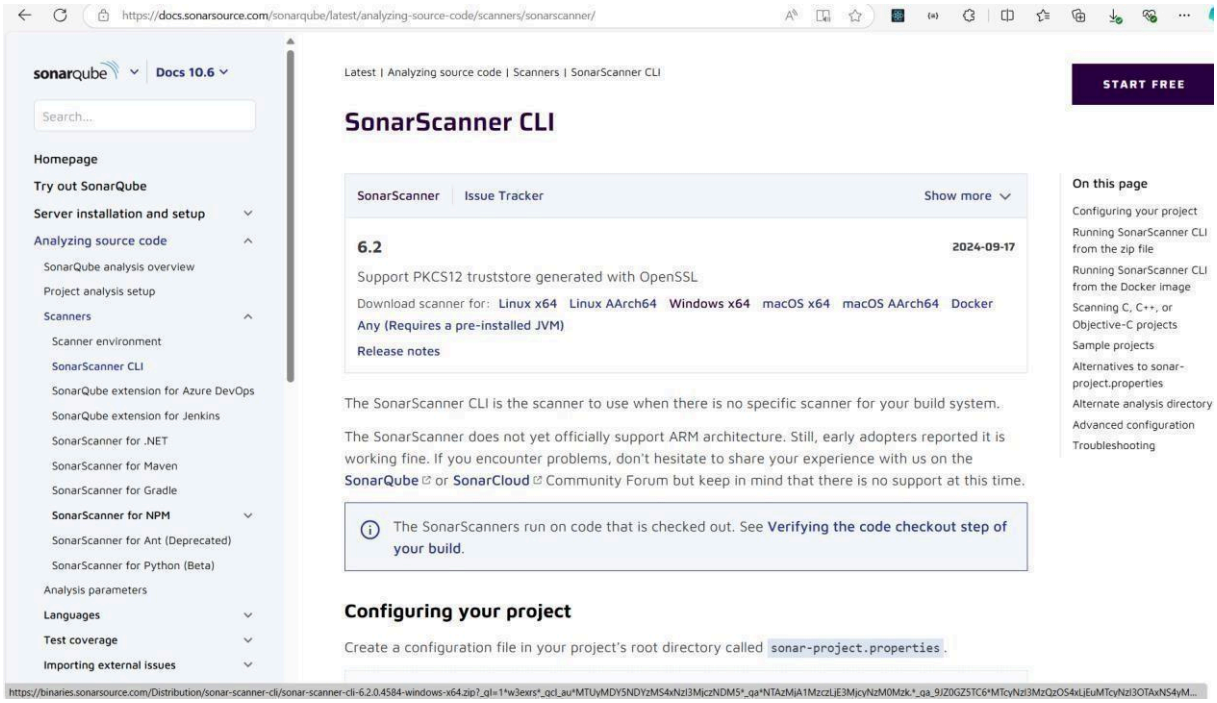
Conclusion: Thus, we have successfully installed SonarQube from Docker image.

Vedang Wajge **D15A** **66**

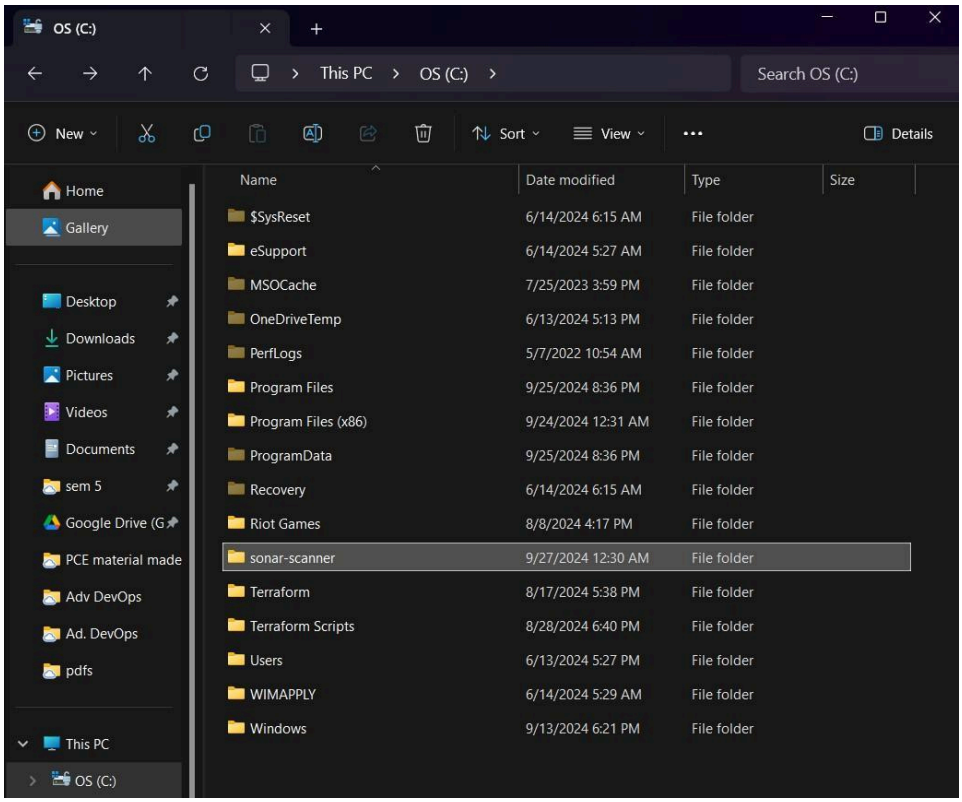
Experiment 8

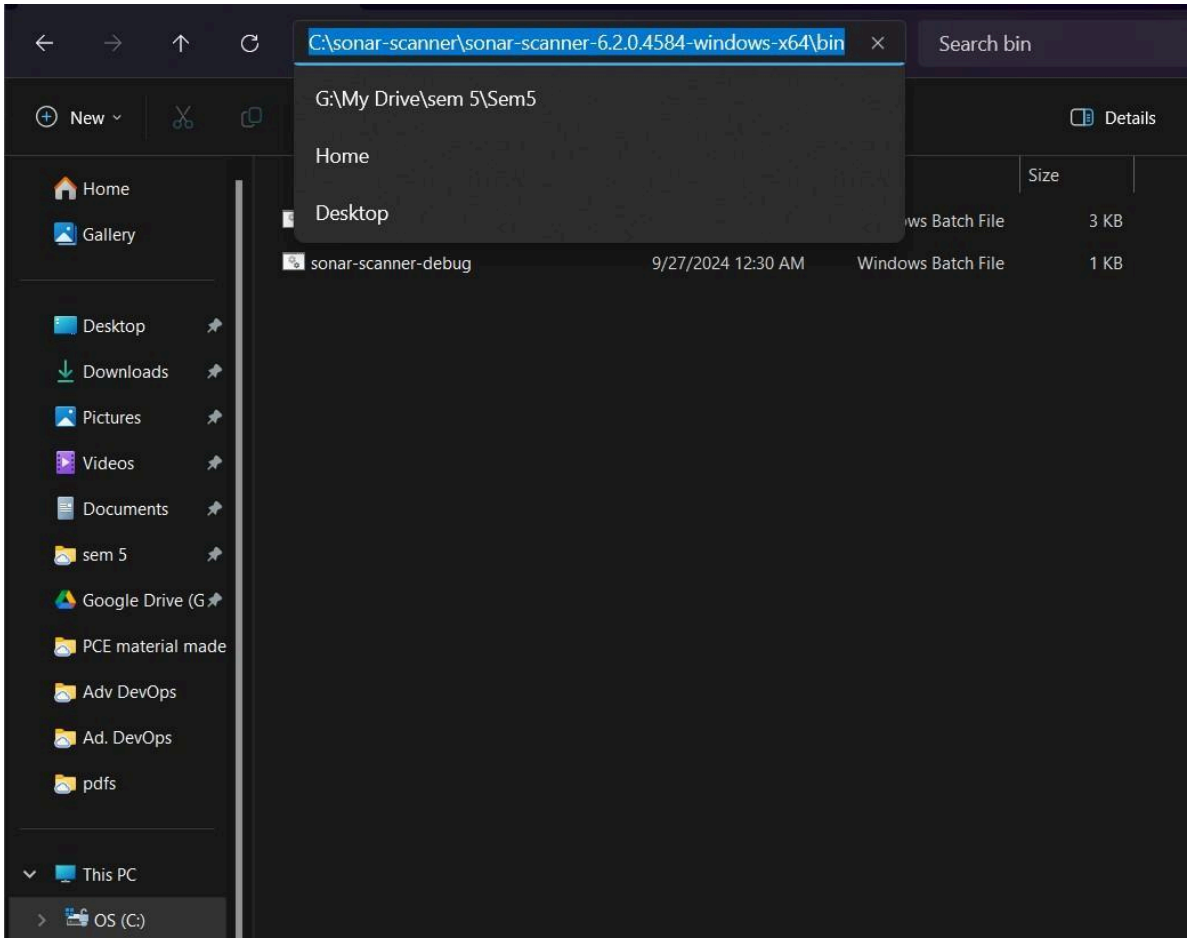
Aim: Create a Jenkins CICD Pipeline with SonarQube / GitLab Integration to perform a static analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web /Java / Python application.

Step 1 : Visit the following link to download the SonarScanner CLI - https://docs.sonarsource.com/sonarqube/latest/analyzing-source-code/scanners/sonarscanner/ and then click on Windows x-64 to download the zip file.

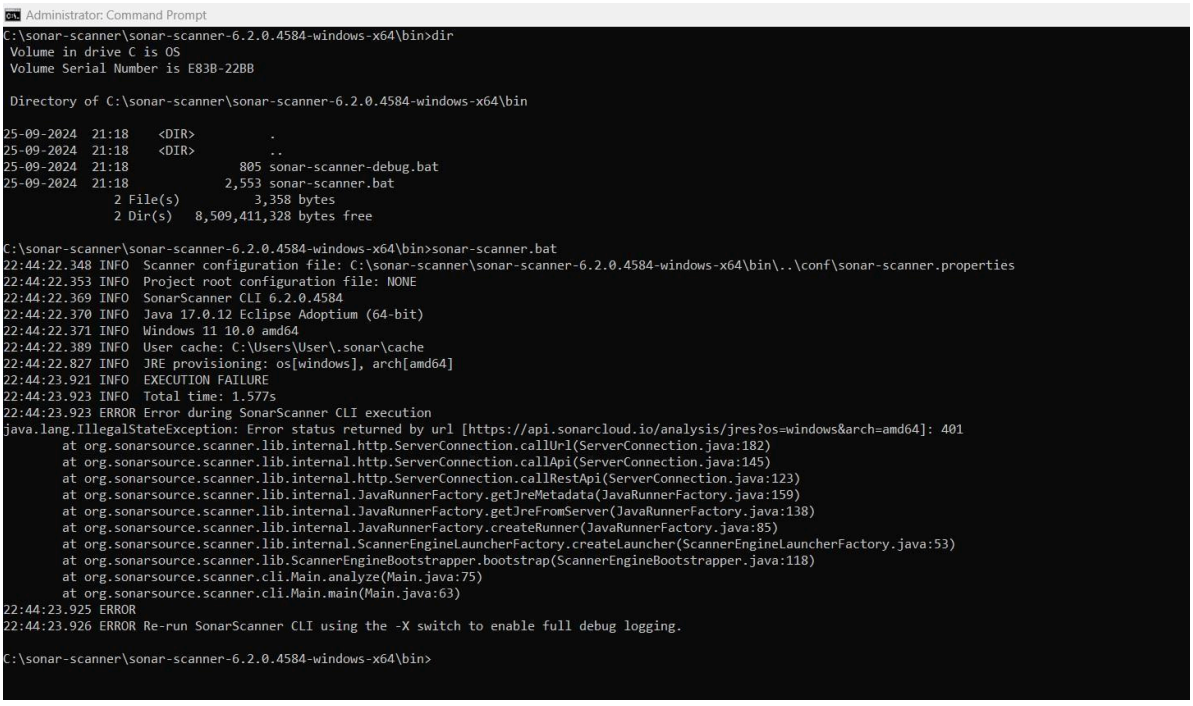


Step 2: Extract the content in C drive and name the folder sonar-scanner



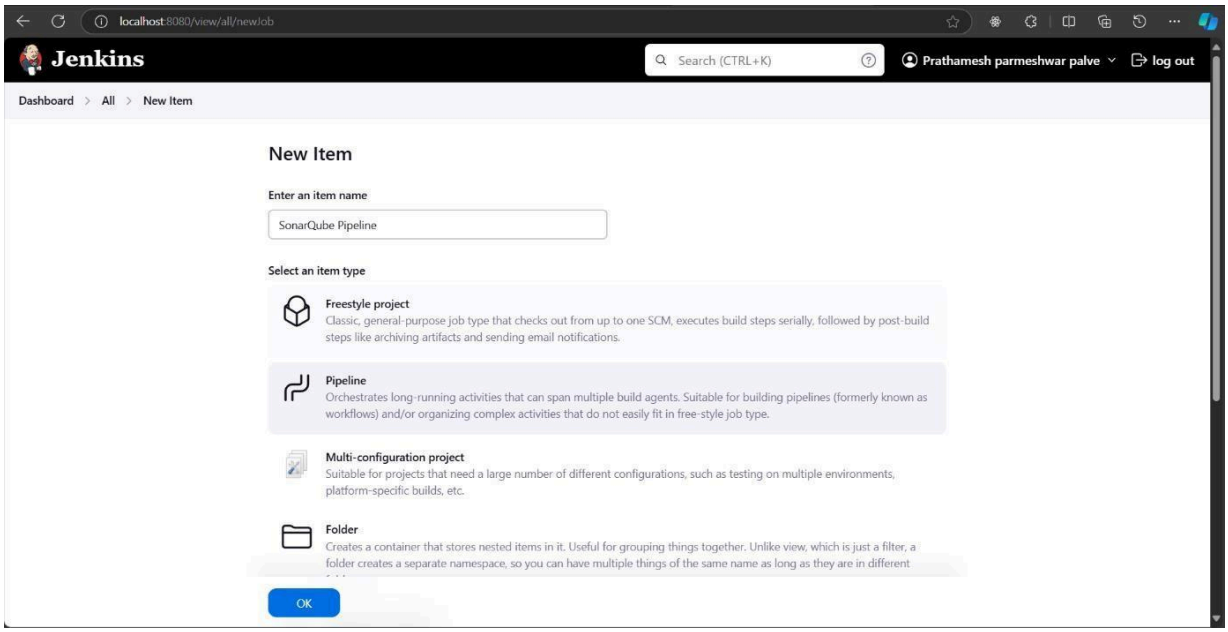


Step 3: Open Command Prompt and run as administrator and run the following commands –
cd C:\sonar-scanner\sonar-scanner-6.2.0.4584-windows-x64\bin dir
sonar-scanner.bat



```
Administrator: Command Prompt
C:\sonar-scanner\sonar-scanner-6.2.0.4584-windows-x64\bin>dir
 Volume in drive C is OS
 Volume Serial Number is E83B-22BB

 Directory of C:\sonar-scanner\sonar-scanner-6.2.0.4584-windows-x64\bin

25-09-2024  21:18    <DIR>          .
25-09-2024  21:18    <DIR>          ..
25-09-2024  21:18               805 sonar-scanner-debug.bat
25-09-2024  21:18             2,553 sonar-scanner.bat
               2 File(s)          3,358 bytes
               2 Dir(s)   8,509,411,328 bytes free

C:\sonar-scanner\sonar-scanner-6.2.0.4584-windows-x64\bin>sonar-scanner.bat
22:44:22.348 INFO  Scanner configuration file: C:\sonar-scanner\sonar-scanner-6.2.0.4584-windows-x64\bin\..\conf\sonar-scanner.properties
22:44:22.353 INFO  Project root configuration file: NONE
22:44:22.369 INFO  SonarScanner CLI 6.2.0.4584
22:44:22.370 INFO  Java 17.0.12 Eclipse Adoptium (64-bit)
22:44:22.371 INFO  Windows 11 10.0 amd64
22:44:22.389 INFO  User cache: C:\Users\User\.sonar\cache
22:44:22.827 INFO  JRE provisioning: os[windows], arch[amd64]
22:44:23.921 INFO  EXECUTION FAILURE
22:44:23.923 INFO  Total time: 1.577s
22:44:23.923 ERROR Error during SonarScanner CLI execution
java.lang.IllegalStateException: Error status returned by url [https://api.sonarcloud.io/analysis/jres?os=windows&arch=amd64]: 401
        at org.sonarsource.scanner.lib.internal.http.ServerConnection.callUrl(ServerConnection.java:182)
        at org.sonarsource.scanner.lib.internal.http.ServerConnection.callApi(ServerConnection.java:145)
        at org.sonarsource.scanner.lib.internal.http.ServerConnection.callRestApi(ServerConnection.java:123)
        at org.sonarsource.scanner.lib.internal.JavaRunnerFactory.getJreMetadata(JavaRunnerFactory.java:159)
        at org.sonarsource.scanner.lib.internal.JavaRunnerFactory.getJreFromServer(JavaRunnerFactory.java:138)
        at org.sonarsource.scanner.lib.internal.JavaRunnerFactory.createRunner(JavaRunnerFactory.java:85)
        at org.sonarsource.scanner.lib.internal.ScannerEngineLauncherFactory.createLauncher(ScannerEngineLauncherFactory.java:53)
        at org.sonarsource.scanner.lib.ScannerEngineBootstrapper.bootstrap(ScannerEngineBootstrapper.java:118)
        at org.sonarsource.scanner.cli.Main.analyze(Main.java:75)
        at org.sonarsource.scanner.cli.Main.main(Main.java:63)
22:44:23.925 ERROR
22:44:23.926 ERROR Re-run SonarScanner CLI using the -X switch to enable full debug logging.

C:\sonar-scanner\sonar-scanner-6.2.0.4584-windows-x64\bin>
```

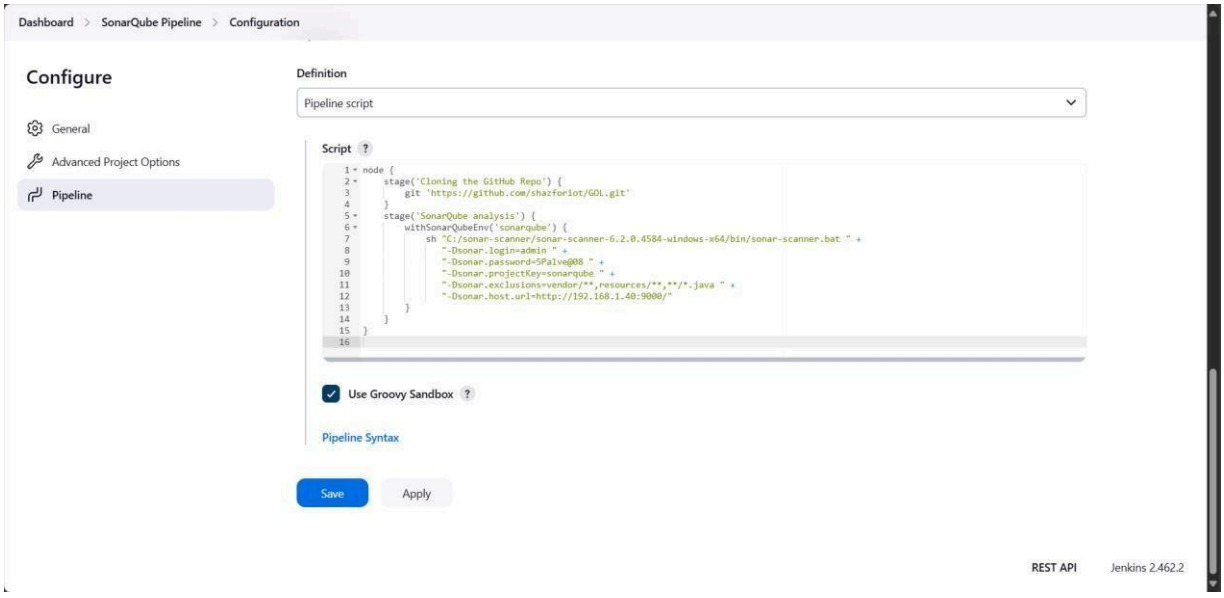
Step 4: Open Jenkins and create a pipeline and name the pipeline SonarQube Pipeline and then click on okay.

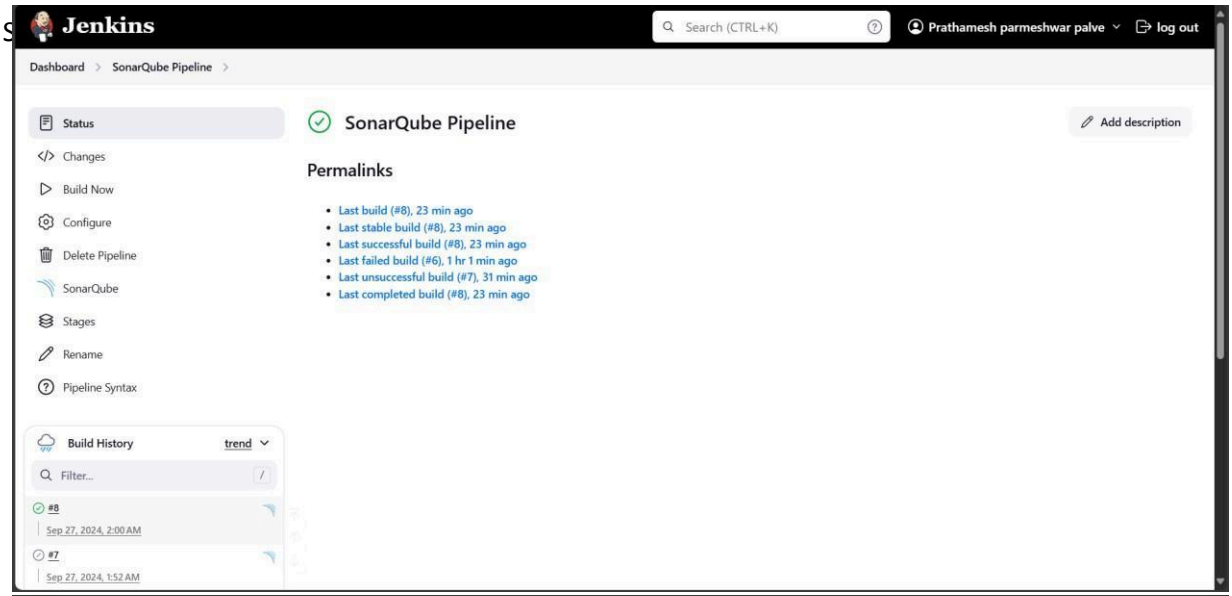


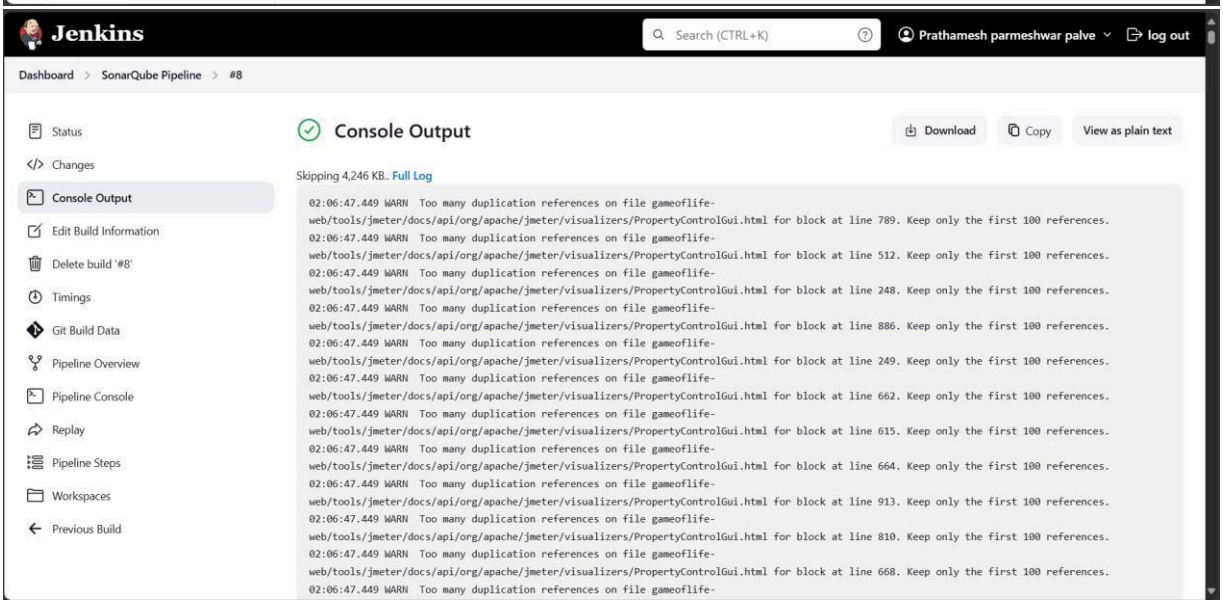
Step 5: In the configuration, under the Pipeline Section write the following Pipeline Script -

```
node {
    stage('Cloning the GitHub Repo') {
        git 'https://github.com/shazforiot/GOL.git'
    }
    stage('SonarQube analysis') {
        withSonarQubeEnv('sonarqube') {
            sh "C:/sonar-scanner/sonar-scanner-6.2.0.4584-windows-x64/bin/sonar-
scanner.bat " +
                "-Dsonar.login=admin " +
                "-Dsonar.password=5Palve@08 " +
                "-Dsonar.projectKey=sonarqube " +
                "-Dsonar.exclusions=vendor/**,resources/**,**/*.java " +
                "-Dsonar.host.url=http://192.168.1.40:9000/"
        }
    }
}
```

Then click on the save button.


Dashboard > SonarQube Pipeline > Configuration
Configure
General
Advanced Project Options
Pipeline
Definition
Pipeline script
Script
node {
stage('Cloning the GitHub Repo') {
git 'https://github.com/shazforiot/GOL.git'
}
stage('SonarQube analysis') {
withSonarQubeEnv('sonarqube') {
sh "C:/sonar-scanner/sonar-scanner-6.2.0.4584-windows-x64/bin/sonar-scanner.bat " +
"-Dsonar.login=admin " +
"-Dsonar.password=5Palve@08 " +
"-Dsonar.projectKey=sonarqube " +
"-Dsonar.exclusions=vendor/**,resources/**,**/*.java " +
"-Dsonar.host.url=http://192.168.1.40:9000/"
}
}
}
Use Groovy Sandbox
Pipeline Syntax
Save
Apply
REST API
Jenkins 2.462.2


Jenkins
Search (CTRL+K)
Prathamesh parmeshwar palve
log out
Dashboard > SonarQube Pipeline >
Status
Changes
Build Now
Configure
Delete Pipeline
SonarQube
Stages
Rename
Pipeline Syntax
Build History
trend
Filter...
#8
Sep 27, 2024, 2:00 AM
#7
Sep 27, 2024, 1:52 AM
SonarQube Pipeline
Add description
Permalinks
Last build (#8), 23 min ago
Last stable build (#8), 23 min ago
Last successful build (#8), 23 min ago
Last failed build (#6), 1 hr 1 min ago
Last unsuccessful build (#7), 31 min ago
Last completed build (#8), 23 min ago


Jenkins
Search (CTRL+K)
Prathamesh parmeshwar palve
log out
Dashboard > SonarQube Pipeline > #8
Status
Changes
Console Output
Edit Build Information
Delete build '#8'
Timings
Git Build Data
Pipeline Overview
Pipeline Console
Replay
Pipeline Steps
Workspaces
Previous Build
Console Output
Download
Copy
View as plain text
Skipping 4,246 KB.. Full Log
02:06:47.449 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 789. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 512. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 248. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 886. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 249. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 662. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 615. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 664. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 913. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 810. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 668. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-

Step 7: Now, visit http:// 192.168.1.40:9000/dashboard?id=sonarqube to see the result.