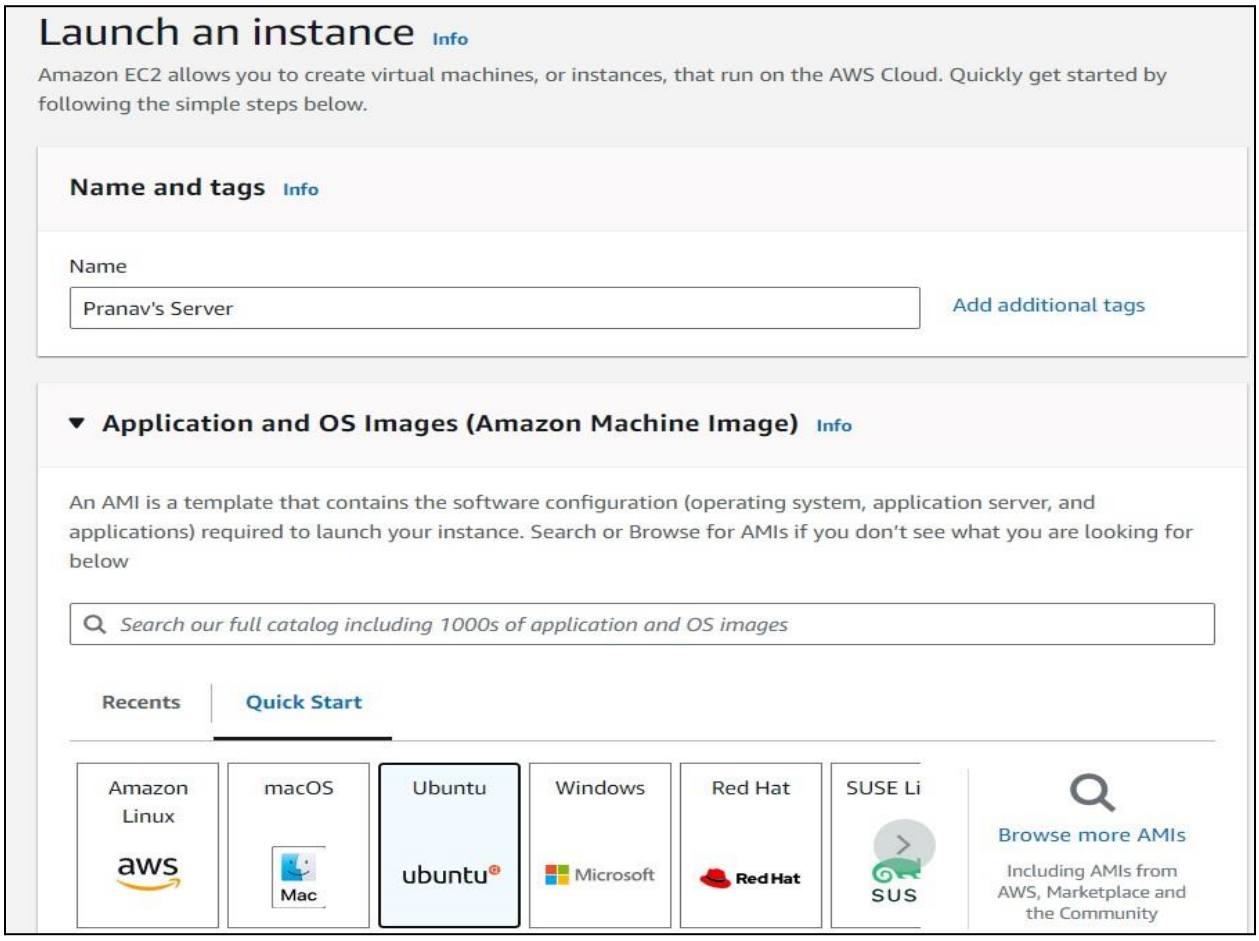
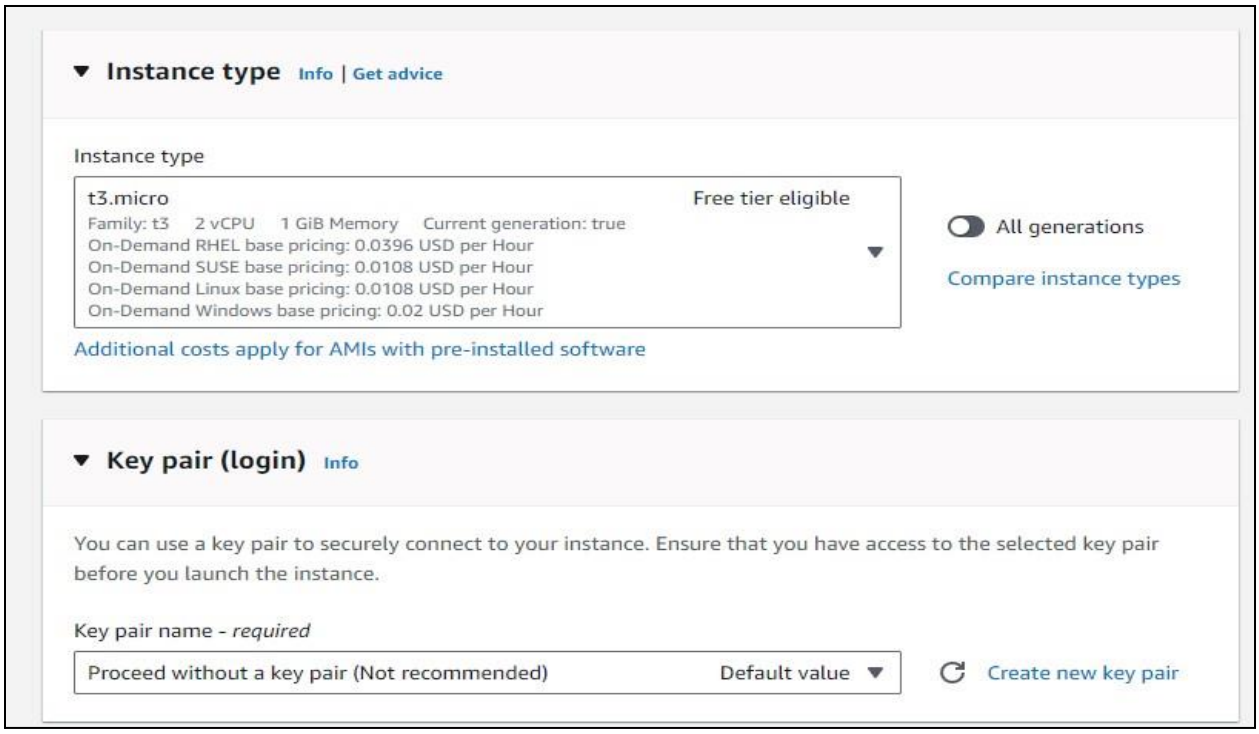
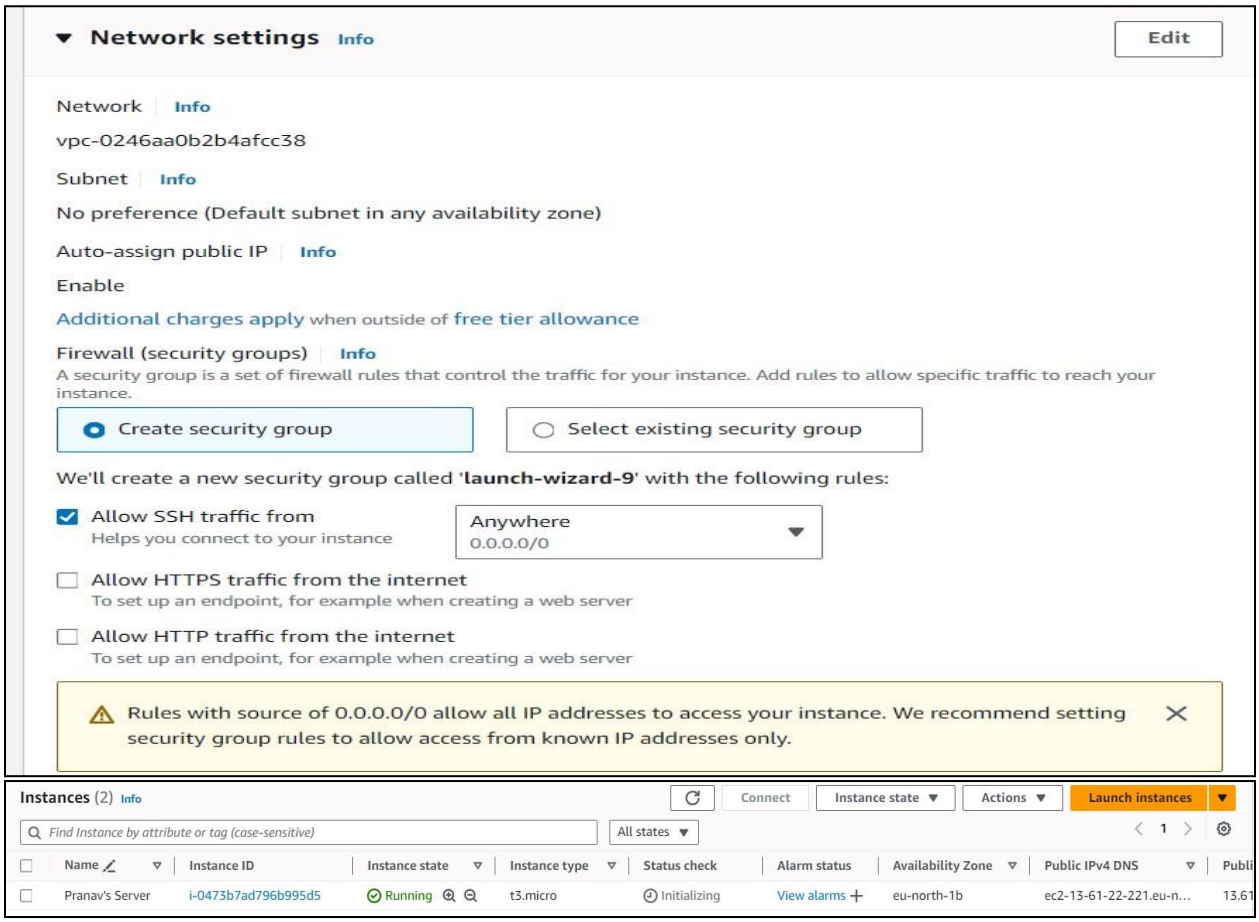
ADVANCE DEVOPS EXP-1

RIYA VARYANI **D15A/64**

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




Instance type Info | Get advice
Instance type
t3.micro
Free tier eligible
Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand RHEL base pricing: 0.0396 USD per Hour
On-Demand SUSE base pricing: 0.0108 USD per Hour
On-Demand Linux base pricing: 0.0108 USD per Hour
On-Demand Windows base pricing: 0.02 USD per Hour
All generations
Compare instance types
Additional costs apply for AMIs with pre-installed software
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
Proceed without a key pair (Not recommended)
Default value
Create new key pair


Network settings Info
Edit
Network Info
vpc-0246aa0b2b4afcc38
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-9' with the following rules:
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.

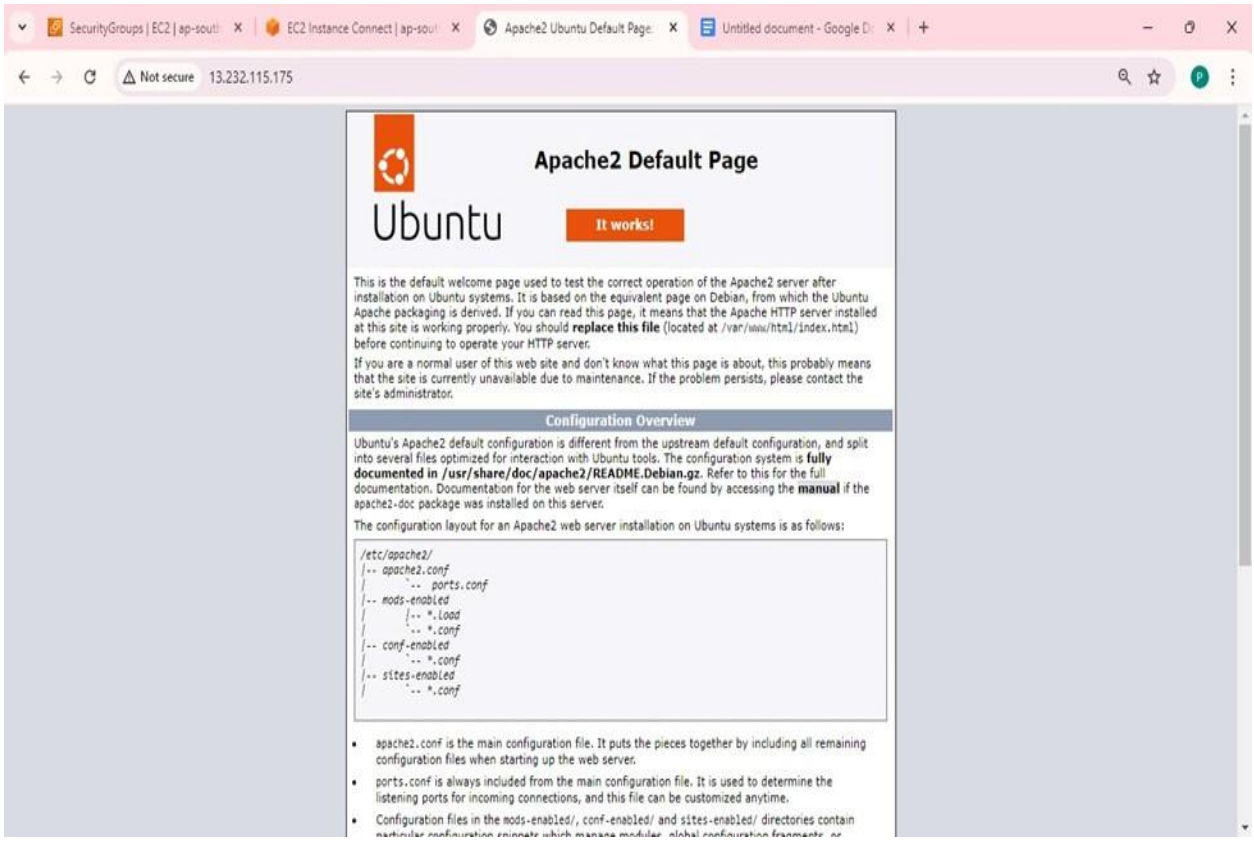
Instances (2) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Pranav's Server
i-0473b7ad796b995d5
Running
t3.micro
Initializing
View alarms
eu-north-1b
ec2-13-61-22-221.eu-n...

```
login as: ubuntu
Authenticating with public key "test-key"
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1009-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Mon Jul 29 17:28:10 UTC 2024

  System load:  0.02               Processes:             109
  Usage of /:   10.5% of 14.46GB   Users logged in:       0
  Memory usage: 20%                IPv4 address for enX0: 172.31.43.87
  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.
```

```
root@ip-172-31-43-87:/# apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.58-1ubuntu8.4).
0 upgraded, 0 newly installed, 0 to remove and 26 not upgraded.
root@ip-172-31-43-87:/#
```

```
root@ip-172-31-43-87:/# 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 2024-07-30 05:02:47 UTC; 12min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 494 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 527 (apache2)
      Tasks: 55 (limit: 1130)
     Memory: 8.3M (peak: 8.5M)
        CPU: 94ms
     CGroup: /system.slice/apache2.service
             ├─527 /usr/sbin/apache2 -k start
             ├─532 /usr/sbin/apache2 -k start
             └─533 /usr/sbin/apache2 -k start

Jul 30 05:02:45 ip-172-31-43-87 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jul 30 05:02:47 ip-172-31-43-87 systemd[1]: Started apache2.service - The Apache HTTP Server.
root@ip-172-31-43-87:/#
```

```
root@ip-172-31-43-87:/# cd /var/www/html/
root@ip-172-31-43-87:/var/www/html#
```

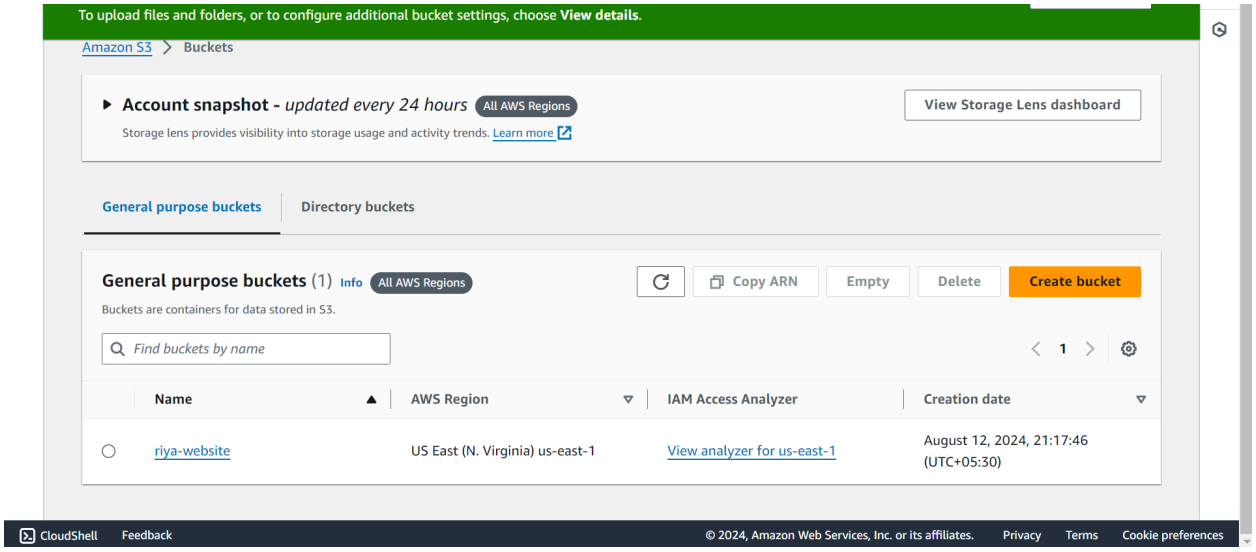


Experiment 2

Aim: To Build Your Application using AWS CodeBuild and Deploy on S3 / SEBS using AWS CodePipeline, deploy Sample Application on EC2 instance using AWS CodeDeploy.

Contents:

1. s3 bucket
2. ec2 instance
3. elastic beanstalk



Object Lock
Disabled

Requester pays Edit

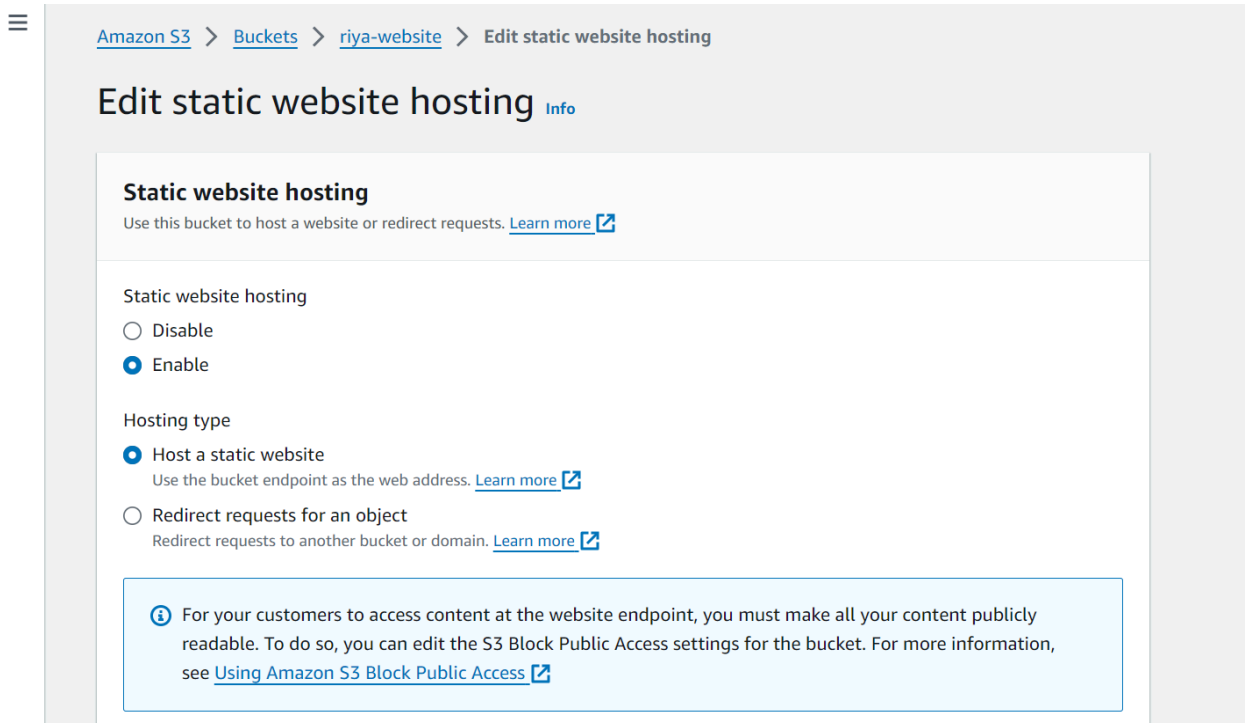
When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. Learn more

Requester pays
Disabled

Static website hosting Edit

Use this bucket to host a website or redirect requests. Learn more

Static website hosting
Disabled



see Using Amazon S3 Block Public Access

Index document

Specify the home or default page of the website.

index.html

Error document - *optional*

This is returned when an error occurs.

error.html

Redirection rules – *optional*

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more

1

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

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Cancel Save changes

aws Services Search [Alt+S] Stockholm Riya

Successfully edited public access

View details below.

Make public: status

Close

The information below will no longer be available after you navigate away from this page.

Summary

Source	Successfully edited public access	Failed to edit public access
s3://riya1-website/Html1/	3 objects, 9.7 KB	0 objects

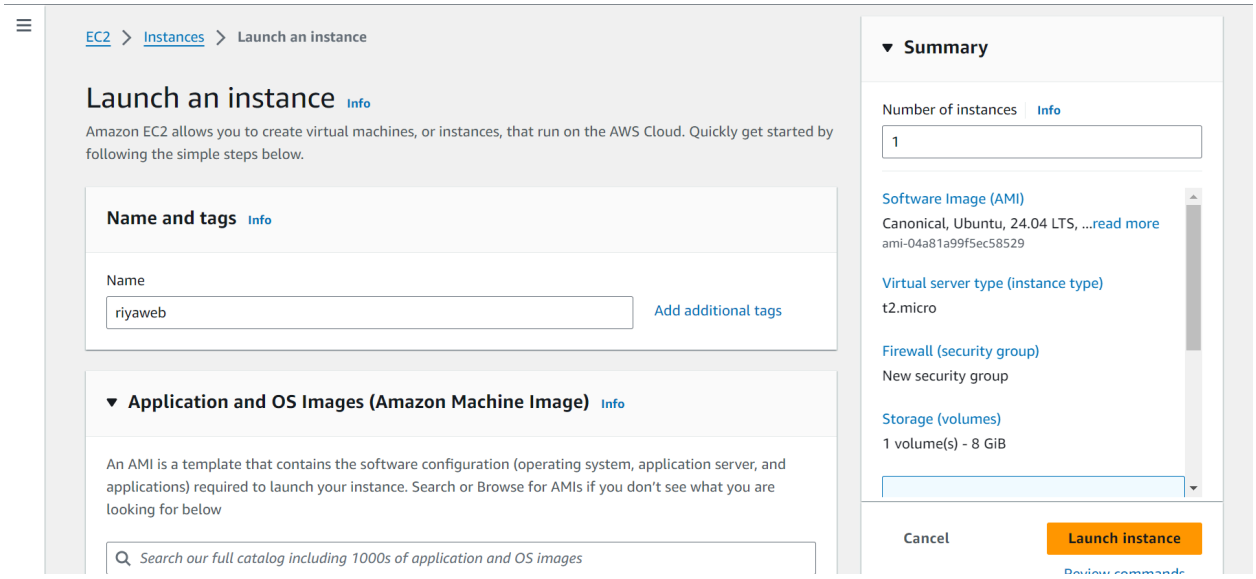
Welcome to Mess Company

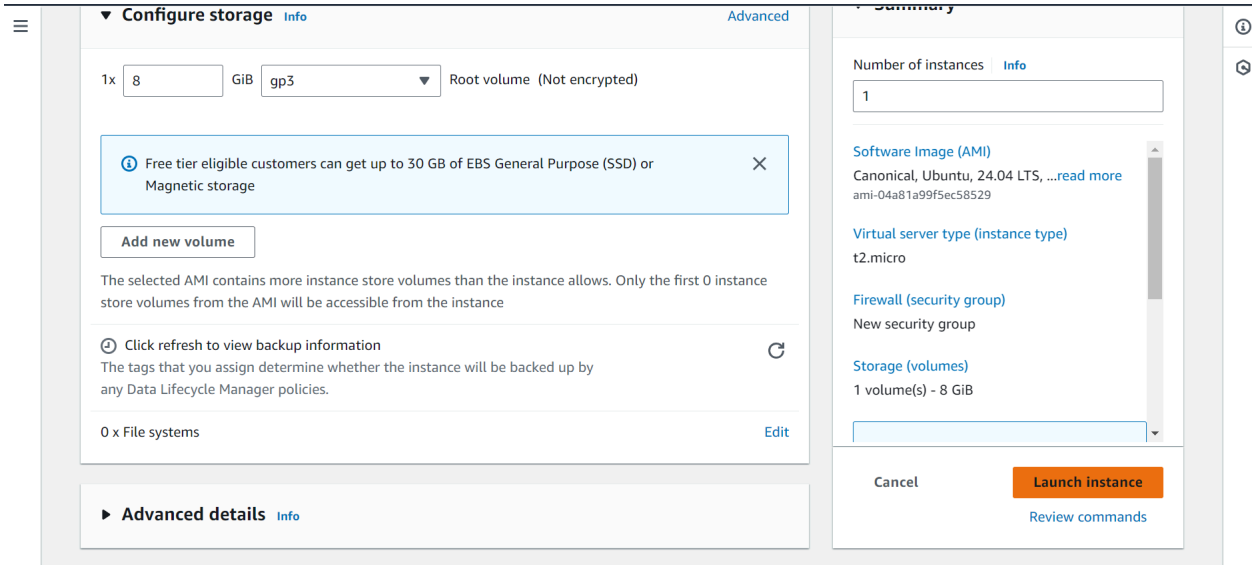
Company Details Our Services Our Meals

Our Services

- Custom Catering Services
- Home Cooked Meals
- Fresh Food
- Fruits, Salad, Milk

Using EC2 Instance


EC2 > Instances > Launch an instance
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
riyaweb
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
Search our full catalog including 1000s of application and OS images
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-04a81a99f5ec58529
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance


Configure storage Info
Advanced
1x 8 GiB gp3 Root volume (Not encrypted)
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage
Add new volume
The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance
Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.
0 x File systems
Edit
Advanced details Info
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-04a81a99f5ec58529
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands

Select an existing key pair or create a key pair

We noticed that you didn't select a key pair. If you want to be able to connect to your instance it is recommended that you create one or select an existing one.

- (•) Existing key pair
- ( ) Create new key pair
- ( ) Proceed without key pair

Key pair name

vockey

Cancel | Launch instance

▼ 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

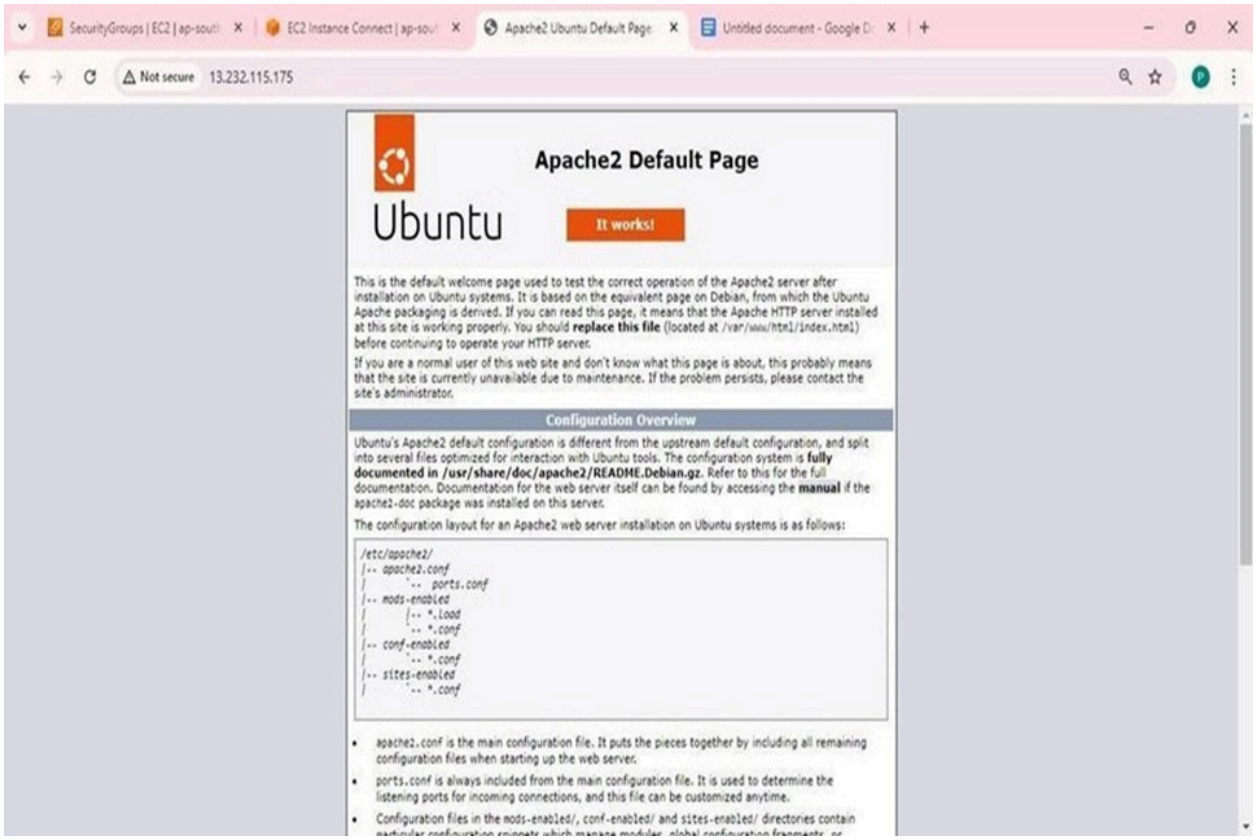
We'll create a new security group called '**launch-wizard-1**' with the following rules:

- [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

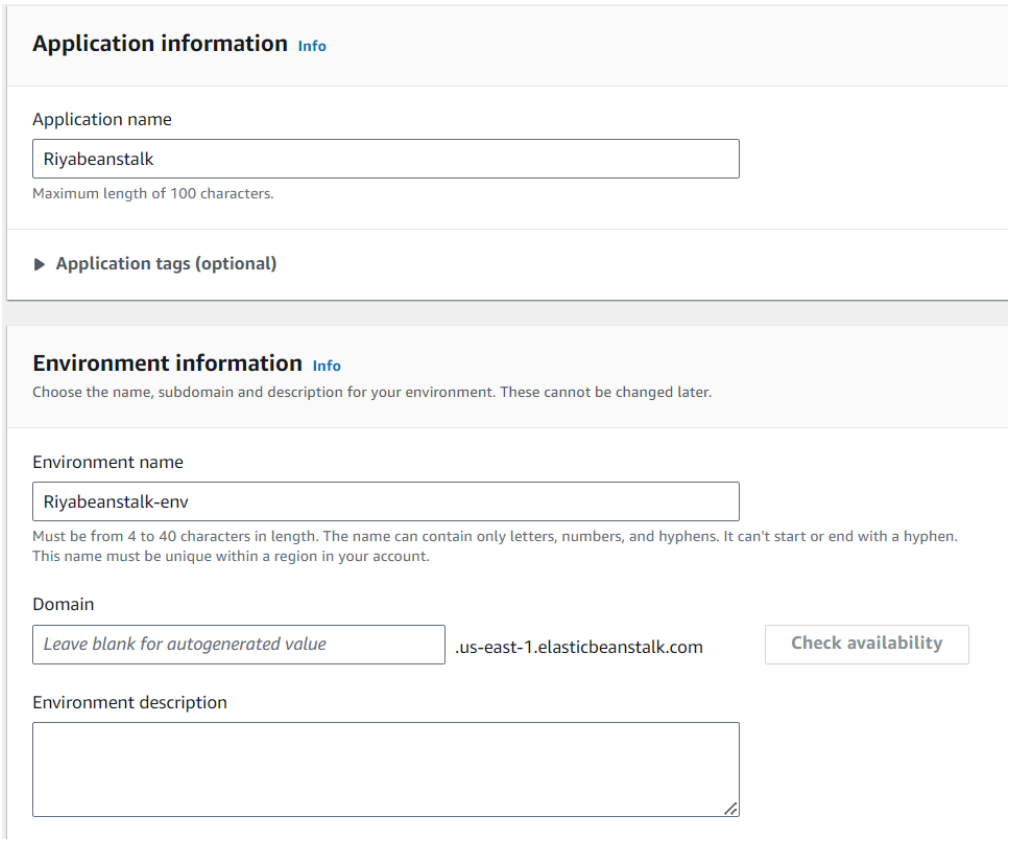
⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ✕

```
 * 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:~$
```

```
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:
```


SecurityGroups | EC2 | ap-south
EC2 Instance Connect | ap-sou
Apache2 Ubuntu Default Page
Untitled document - Google D
Not secure
13.232.115.175
Apache2 Default Page
Ubuntu
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain

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

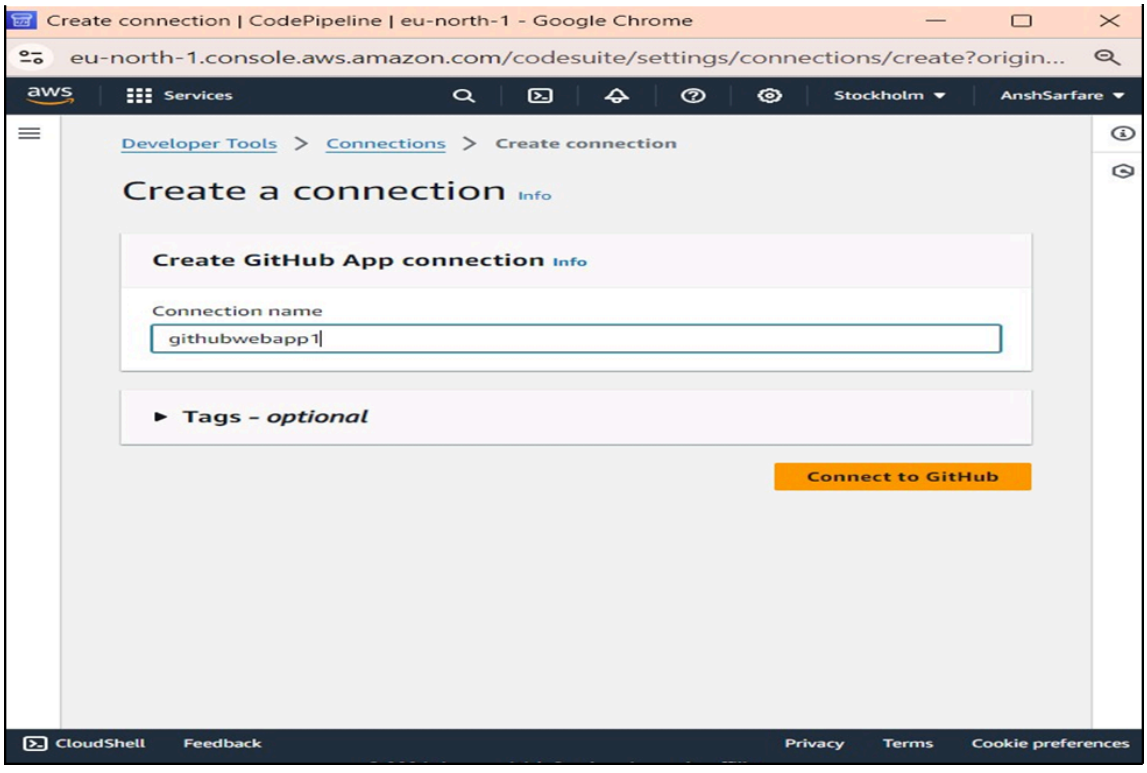
PHP 8.3 running on 64bit Amazon Linux 2023

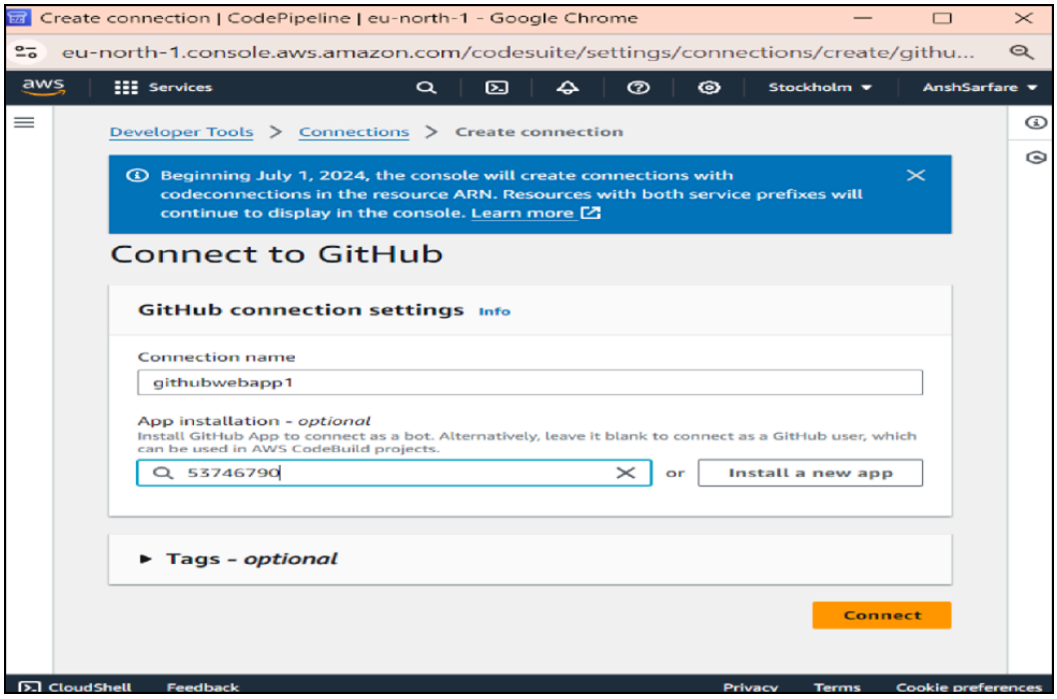
Platform version

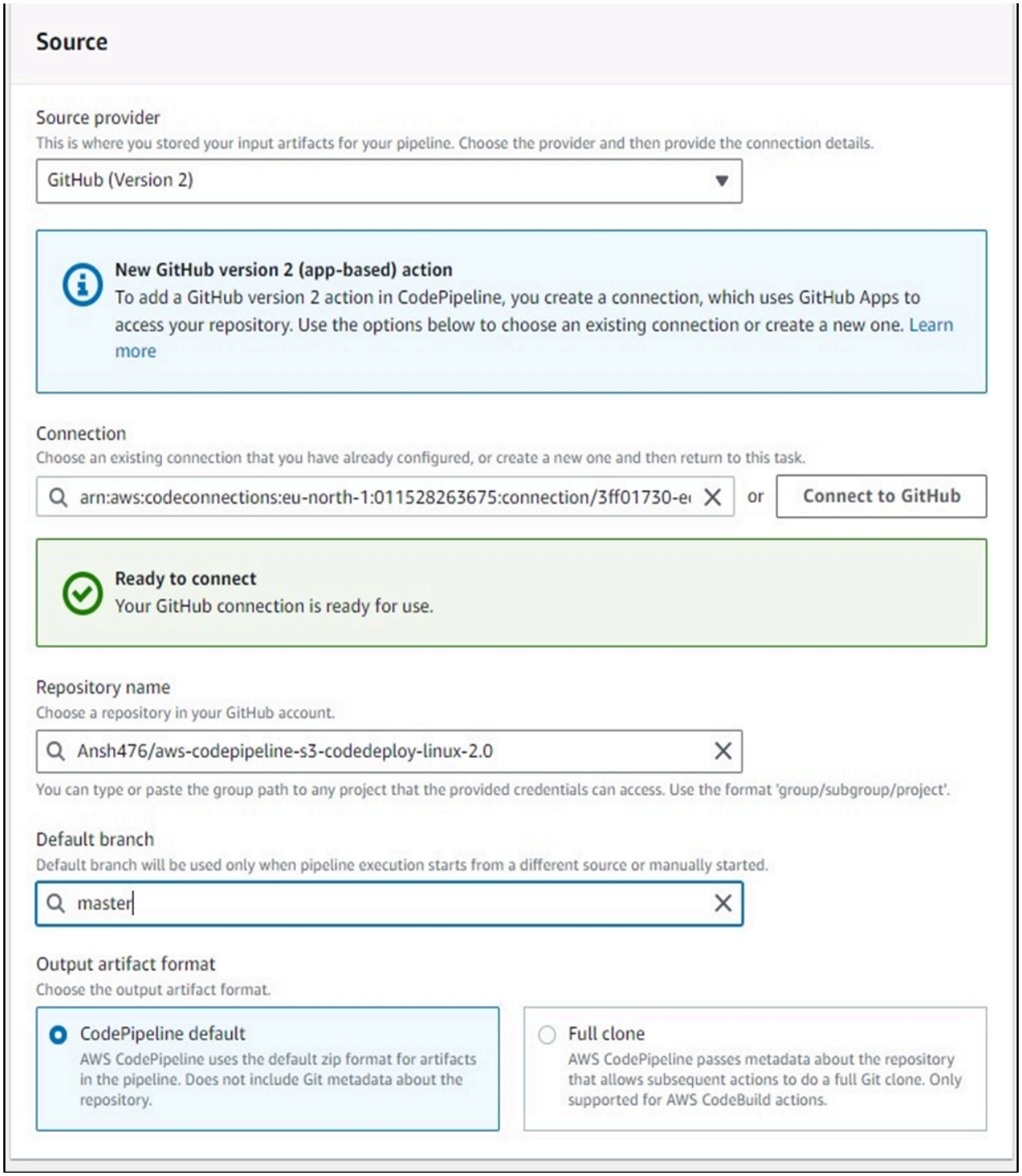
4.3.4 (Recommended)

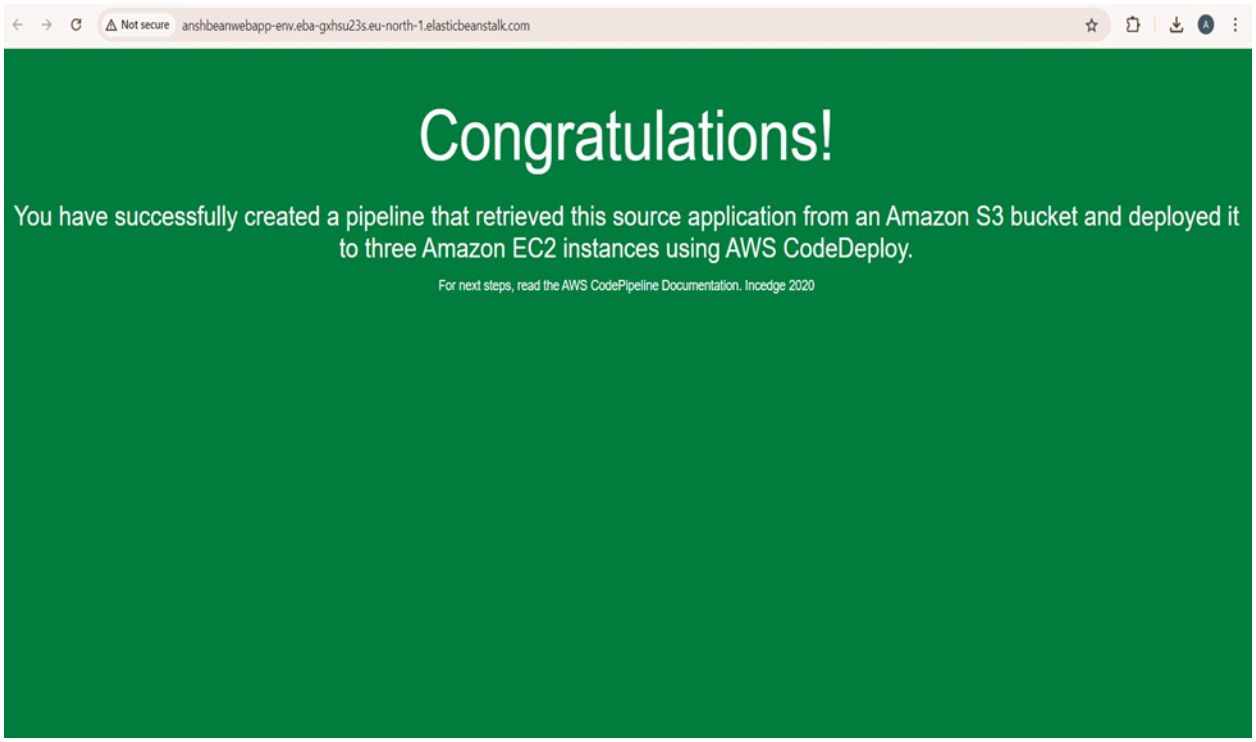
Application code Info

- (•) Sample application
- ( ) Existing version
  Application versions that you have uploaded.
- ( ) Upload your code
  Upload a source bundle from your computer or copy one from Amazon S3.




Create connection | CodePipeline | eu-north-1 - Google Chrome
eu-north-1.console.aws.amazon.com/codesuite/settings/connections/create/githu...
aws
Services
Stockholm
AnshSarfare
Developer Tools > Connections > Create connection
Beginning July 1, 2024, the console will create connections with codeconnections in the resource ARN. Resources with both service prefixes will continue to display in the console. Learn more
Connect to GitHub
GitHub connection settings Info
Connection name
githubwebapp1
App installation - optional
Install GitHub App to connect as a bot. Alternatively, leave it blank to connect as a GitHub user, which can be used in AWS CodeBuild projects.
53746790
or
Install a new app
Tags - optional
Connect
CloudShell
Feedback
Privacy
Terms
Cookie preferences


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-1:011528263675:connection/3ff01730-e
or
Connect to GitHub
Ready to connect
Your GitHub connection is ready for use.
Repository name
Choose a repository in your GitHub account.
Ansh476/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.


Not secure
anshbeanwebapp-env.eba-gxhsu23s.eu-north-1.elasticbeanstalk.com
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

Service role

- (•) Create and use new service role
- ( ) Use an existing service role

Service role name

Enter the name for an IAM role that Elastic Beanstalk will create to assume as a service role. Beanstalk will attach the required managed policies to it.

aws-elasticbeanstalk-service-role

View permission details

EC2 key pair

Select an EC2 key pair to securely log in to your EC2 instances. Learn more

riya

EC2 instance profile

Choose an IAM instance profile with managed policies that allow your EC2 instances to perform required operations.

View permission details

ADVANCE DEVOPS EXPERIMENT NO 3

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

Theory:

Container-based microservices architectures have revolutionized how development and operations teams test and deploy modern software. Containers allow companies to scale and deploy applications more efficiently, but they also introduce new challenges, adding complexity by creating a whole new infrastructure ecosystem. Today, both large and small software companies are deploying thousands of container instances daily. Managing this level of complexity at scale requires advanced tools. Enter Kubernetes. Originally developed by Google, Kubernetes is an open-source container orchestration platform designed to automate the deployment, scaling, and management of containerized applications. Kubernetes has quickly become the de facto standard for container orchestration and is the flagship project of the Cloud Native Computing Foundation (CNCF), supported by major players like Google, AWS, Microsoft, IBM, Intel, Cisco, and Red Hat. Kubernetes simplifies the deployment and operation of applications in a microservice architecture by providing an abstraction layer over a group of hosts. This allows development teams to deploy their applications while Kubernetes takes care of key tasks, including:

● Managing resource consumption by applications or teams
● Distributing application load evenly across the infrastructure
● Automatically load balancing requests across multiple instances of an application
● Monitoring resource usage to prevent applications from exceeding resource limits and automatically restarting them if needed
● Moving application instances between hosts when resources are low or if a host fails
● Automatically utilizing additional resources when new hosts are added to the cluster
● Facilitating canary deployments and rollbacks with ease

Necessary Requirements:

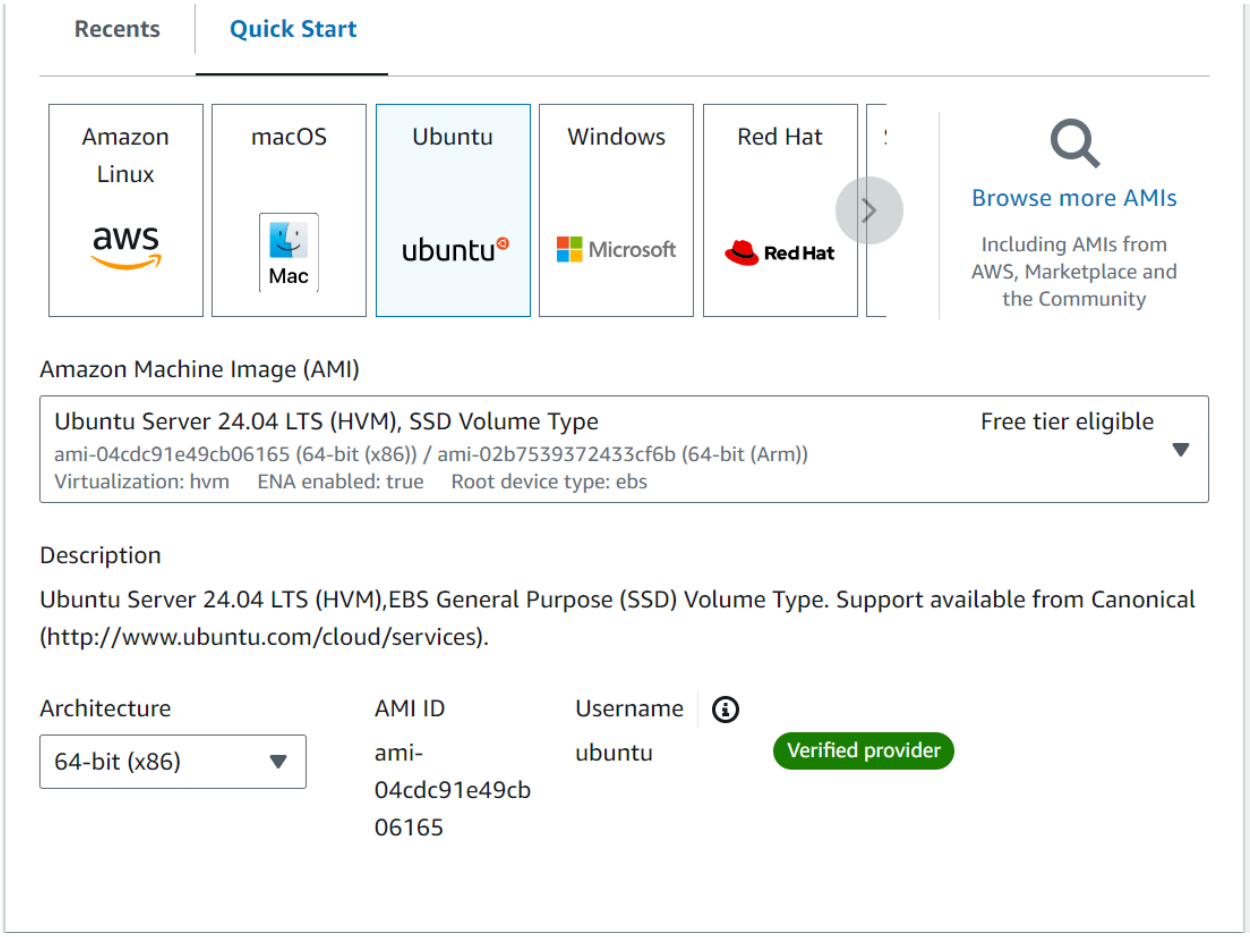
● EC2 Instance: The experiment required launching a t2.medium EC2 instance with 2 CPUs, as

Kubernetes demands sufficient resources for effective functioning.

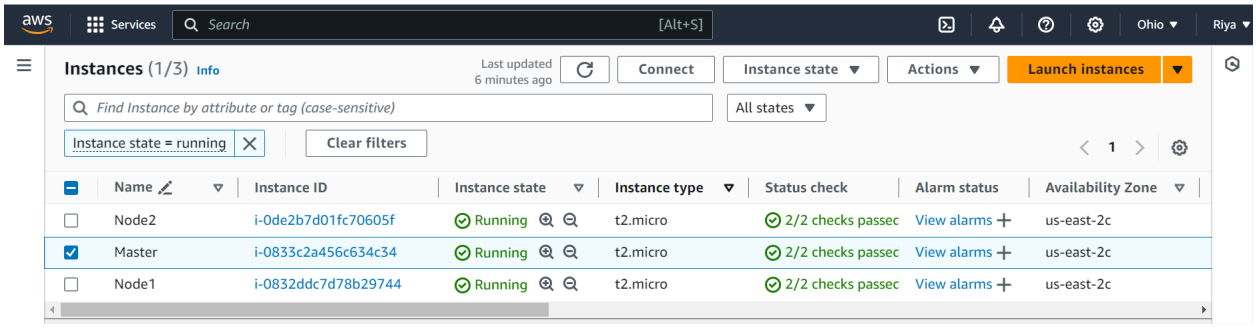
● Minimum Requirements:
○ Instance Type: t2.medium
○ CPUs: 2
○ Memory: Adequate for container orchestration.

This ensured that the Kubernetes cluster had the necessary resources to function smoothly.

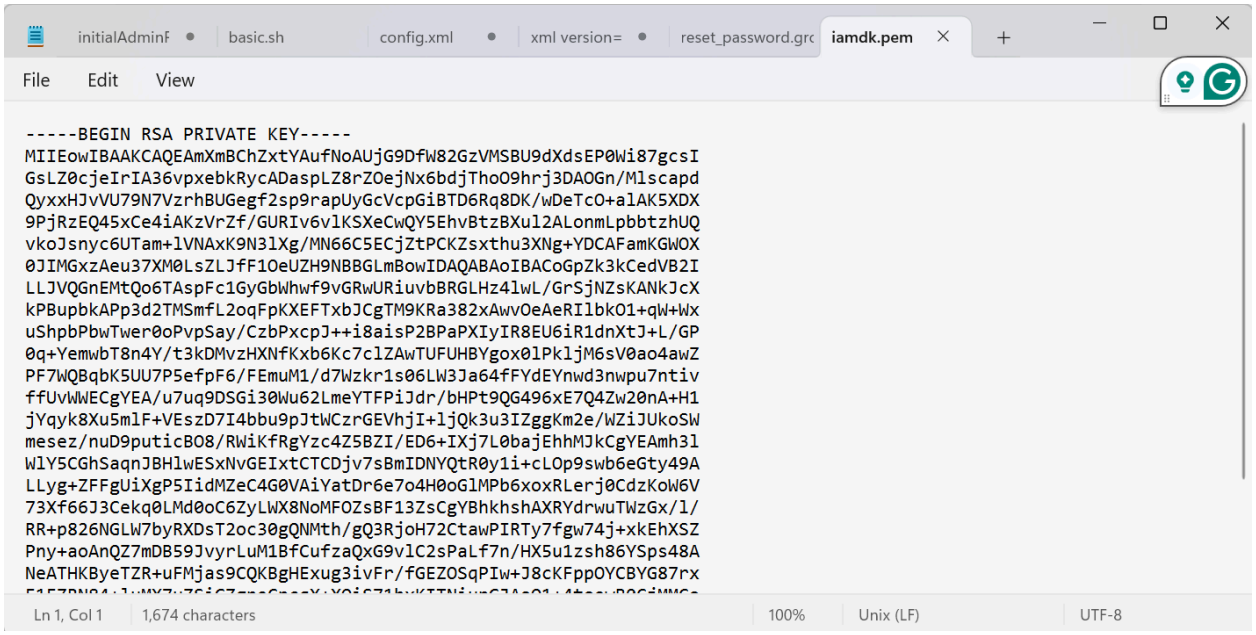
Step 1: Log in to your AWS Academy/personal account and launch 3 new Ec2 Instances. Select Ubuntu as AMI and t2.medium as Instance Type and create a key of type RSA with .pem extension and move the downloaded key to the new folder.We can use 3 Different keys or 1 common key also.
Note: A minimum of 2 CPUs are required so Please select t2.medium and do not forget to stop the instance after the experiment because it is not available in the free tier. Also Select Security groups from existing.



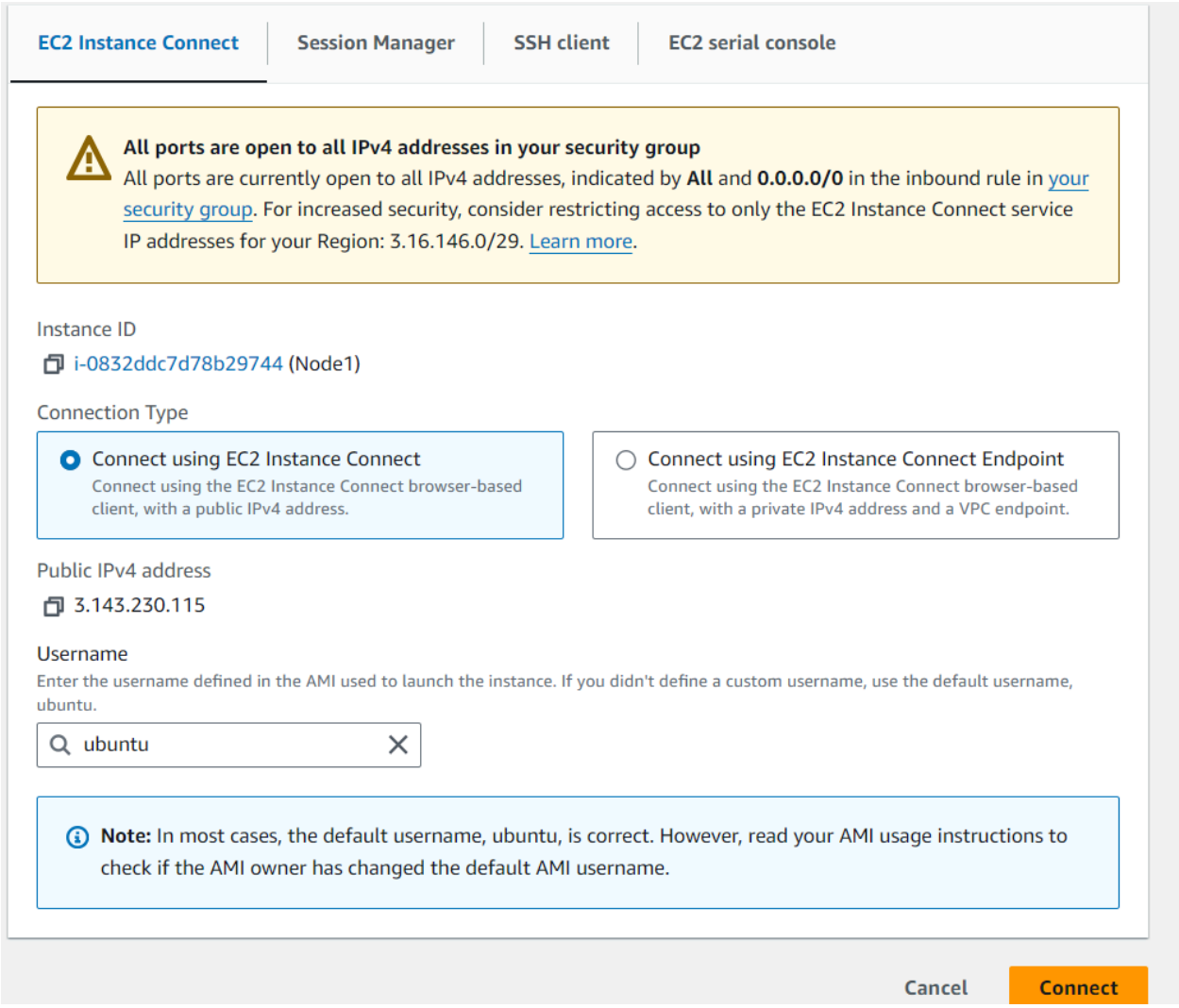
Step 2: After creating the instances click on Connect & connect all 3 instances and navigate to SSH Client.



Downloaded key:



Step 3: Now open the folder in the terminal 3 times for Master, Node1& Node 2 where our .pem key is stored and paste the Example command (starting with ssh -i .....) in the terminal.(ssh -i "Master_Ec2_Key.pem" ubuntu@ec2-54-196-129-215.compute-1.amazonaws.com)



Step 4: Run on Master,Node 1,and Node 2 the below commands to install and setup Docker in Master, Node1, and Node2.

sudo apt-get update

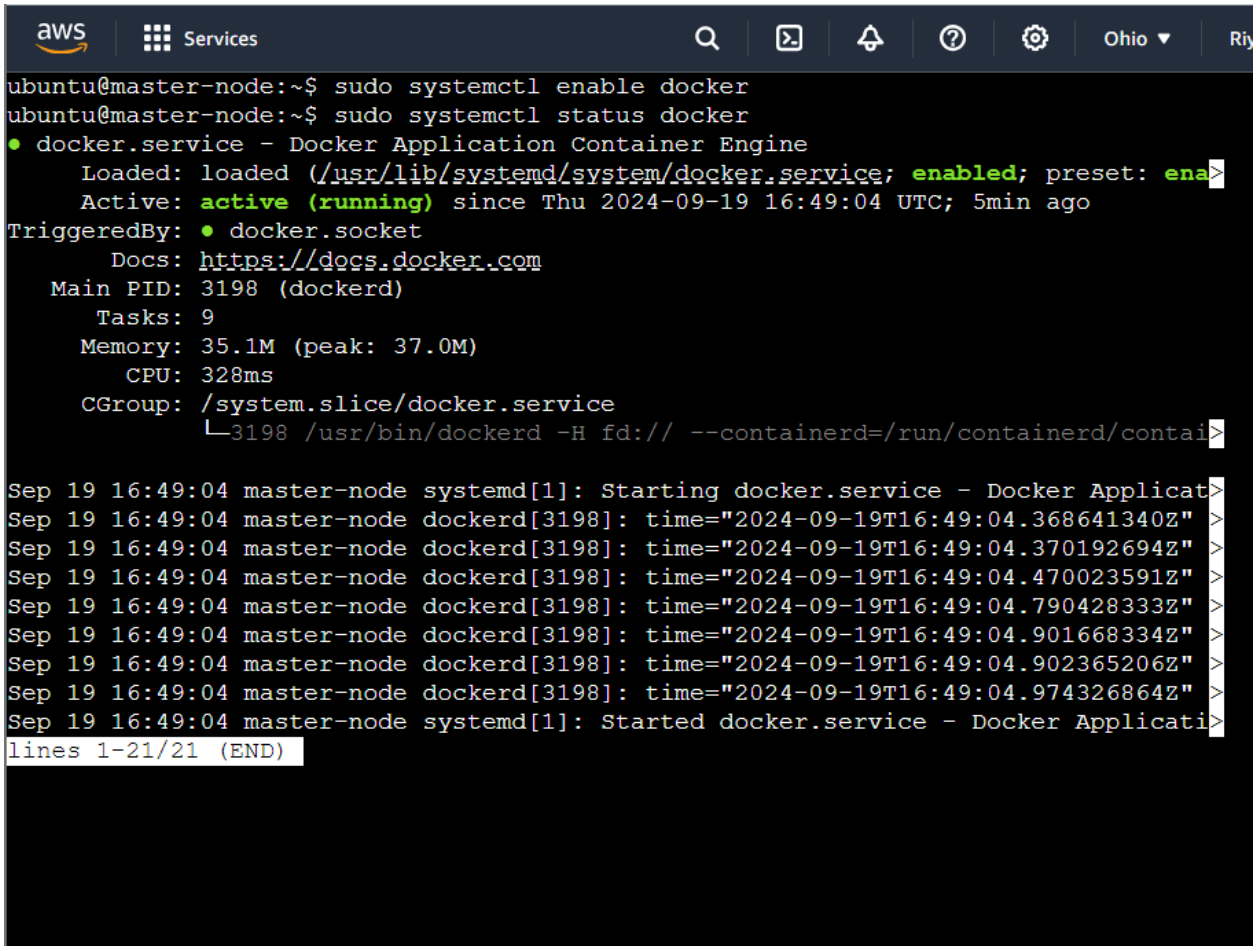
```
ubuntu@node2:~$ sudo apt-get update
Hit:1 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126
kB]
Get:3 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [12
6 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages
 [15.0 MB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [377 kB
]
Get:7 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en
 [5982 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [81.4 k
B]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [
4516 B]
Get:10 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [2
69 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [1
13 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components
[8632 B]
Get:13 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metad
ata [10.1 kB]
```

Sudo apt-get install docker.io

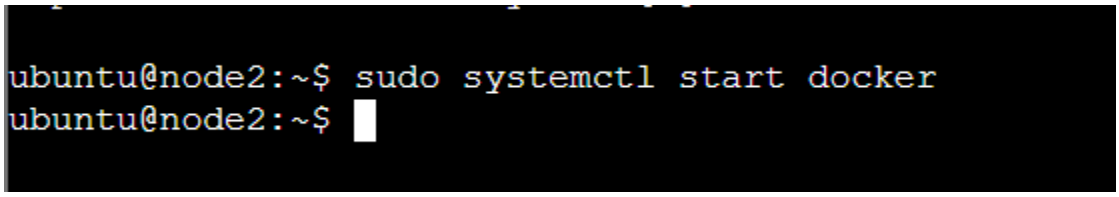
```
ubuntu@master-node:~$ sudo apt-get install docker.io
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bridge-utils containerd dns-root-data dnsmasq-base pigz runc ubuntu-fan
Suggested packages:
  ifupdown aufs-tools cgroupfs-mount | cgroup-lite debootstrap docker-buildx
  docker-compose-v2 docker-doc rinse zfs-fuse | zfsutils
The following NEW packages will be installed:
  bridge-utils containerd dns-root-data dnsmasq-base docker.io pigz runc
  ubuntu-fan
0 upgraded, 8 newly installed, 0 to remove and 139 not upgraded.
Need to get 76.8 MB of archives.
After this operation, 289 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 pigz am
64 2.8-1 [65.6 kB]
Get:2 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble/main amd64 bridge-util
 amd64 1.7.1-1ubuntu2 [33.9 kB]
Get:3 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 run
 amd64 1.1.12-0ubuntu3.1 [8599 kB]
Get:4 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 con
ainerd amd64 1.7.12-0ubuntu4.1 [38.6 MB]
Get:5 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble/main amd64 dns-root-da
a all 2023112702~willsync1 [4450 B]
Get:6 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble/main amd64 dnsmasq-bas
 amd64 2.90-2build2 [375 kB]
Get:7 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64
docker.io amd64 24.0.7-0ubuntu4.1 [29.1 MB]
Get:8 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 ubuntu-
an all 0.12.16 [35.2 kB]
```

Sudo systemctl enable docker

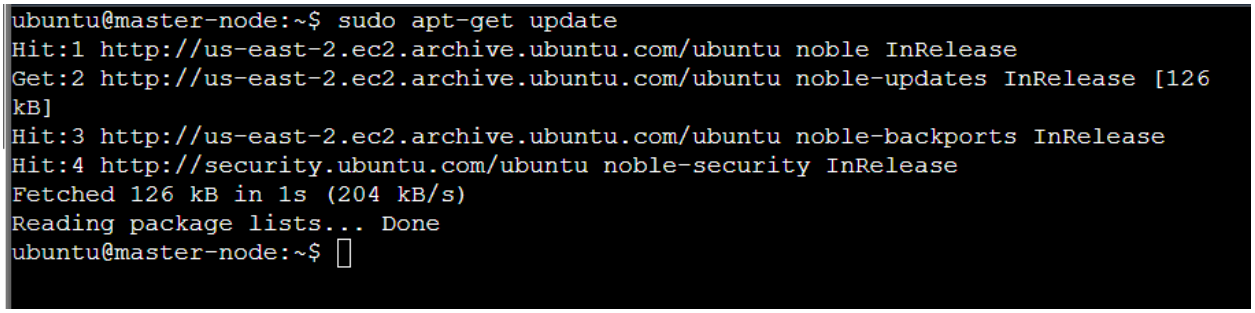
Sudo systemctl status docker



Sudo systemctl start docker



Step 5: Run the below command to install Kubernets.

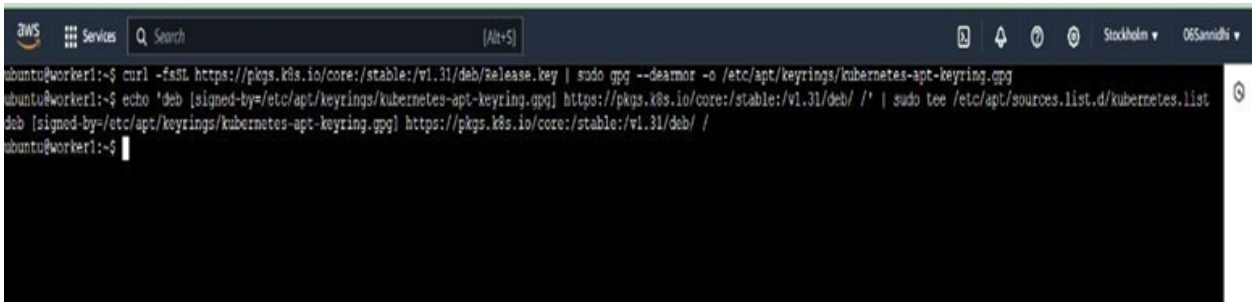


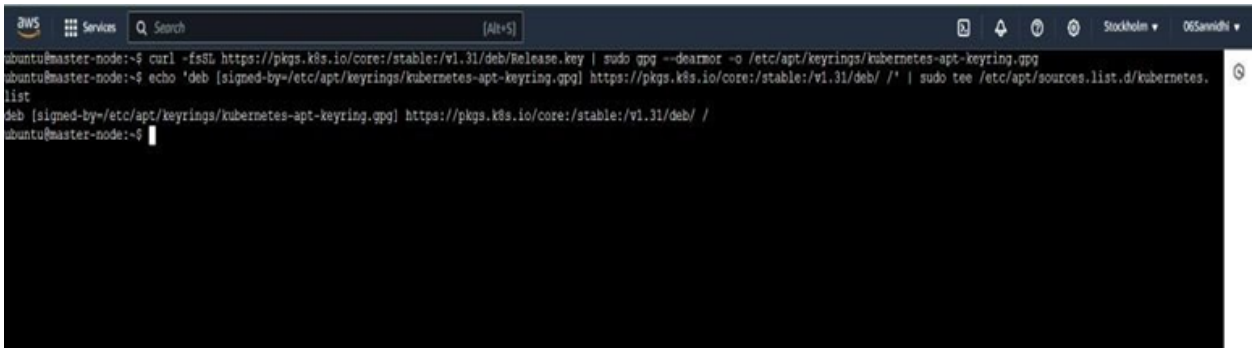
sudo apt-get install -y apt-transport-https ca-certificates curl

```
ubuntu@master-node:~$ sudo apt-get install -y apt-transport-https ca-certificates
curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ca-certificates is already the newest version (20240203).
ca-certificates set to manually installed.
The following additional packages will be installed:
  libcurl3t64-gnutls libcurl4t64
The following NEW packages will be installed:
  apt-transport-https
The following packages will be upgraded:
  curl libcurl3t64-gnutls libcurl4t64
3 upgraded, 1 newly installed, 0 to remove and 136 not upgraded.
Need to get 904 kB of archives.
After this operation, 38.9 kB of additional disk space will be used.
Get:1 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 apt-tran
sport-https all 2.7.14build2 [3974 B]
Get:2 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 curl
 amd64 8.5.0-2ubuntu10.4 [227 kB]
Get:3 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libc
url4t64 amd64 8.5.0-2ubuntu10.4 [341 kB]
Get:4 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libc
url3t64-gnutls amd64 8.5.0-2ubuntu10.4 [333 kB]
```

$ sudo curl -fsSLo /usr/share/keyrings/kubernetes-archive-keyring.gpg https://packages.cloud.google.com/apt/doc/apt-key.gpg
(download the google cloud public signing key)
(curl -fsSL https://pkgs.k8s.io/core:/stable:/v1.31/deb/Release.key | sudo gpg --dearmor -o /etc/apt/keyrings/kubernetes-apt-keyring.gpg)

$ echo "deb [signed-by=/usr/share/keyrings/kubernetes-archive-keyring.gpg] https://apt.kubernetes.io/ kubernetes-xenial main" | sudo tee/etc/apt/sources.list.d/kubernetes.list (add the Kubernetes apt repository:)
(echo "deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:/v1.31/deb/ /"
| sudo tee /etc/apt/sources.list.d/kubernetes.list
)

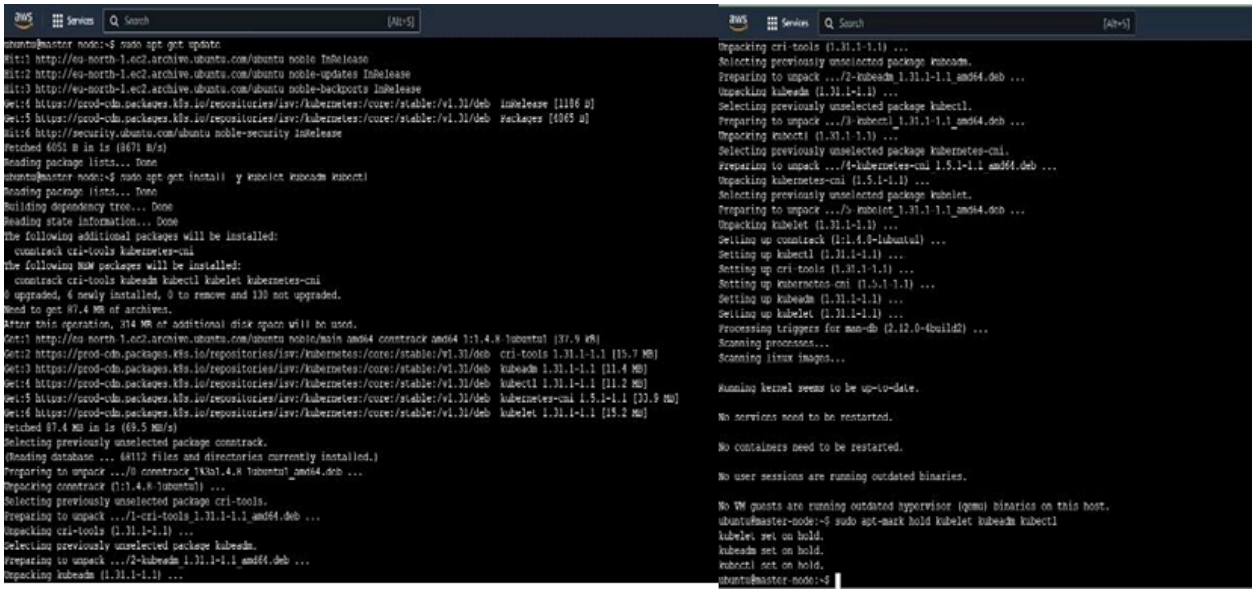


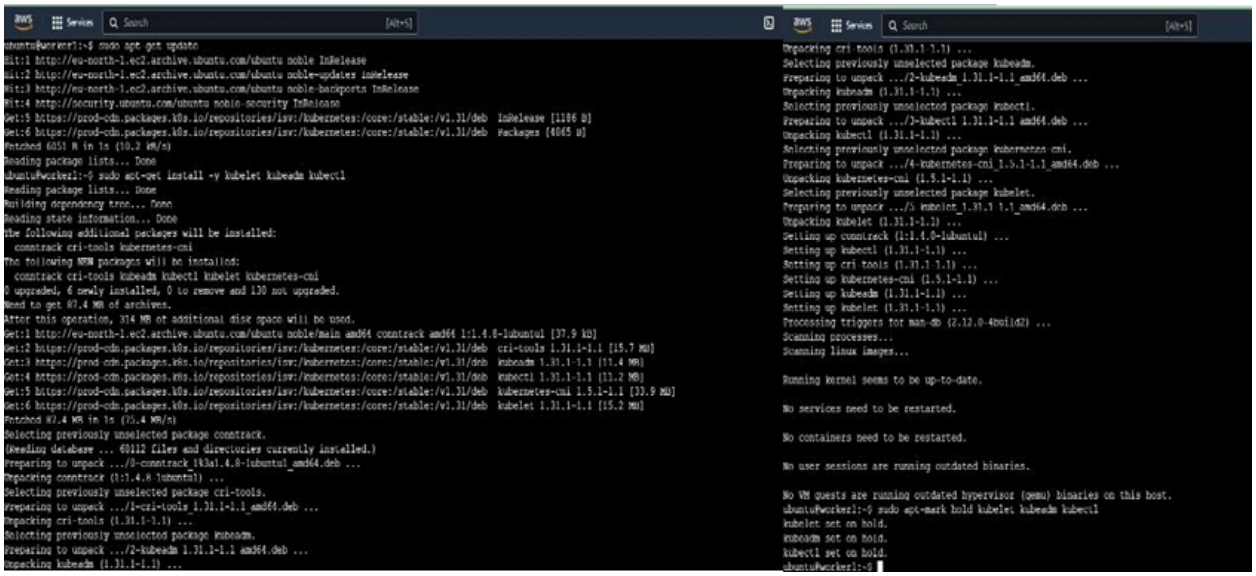


$ sudo apt-get update

$ sudo apt-get install -y kubelet kubeadm kubectl

$ sudo apt-mark hold kubelet kubeadm kubectl

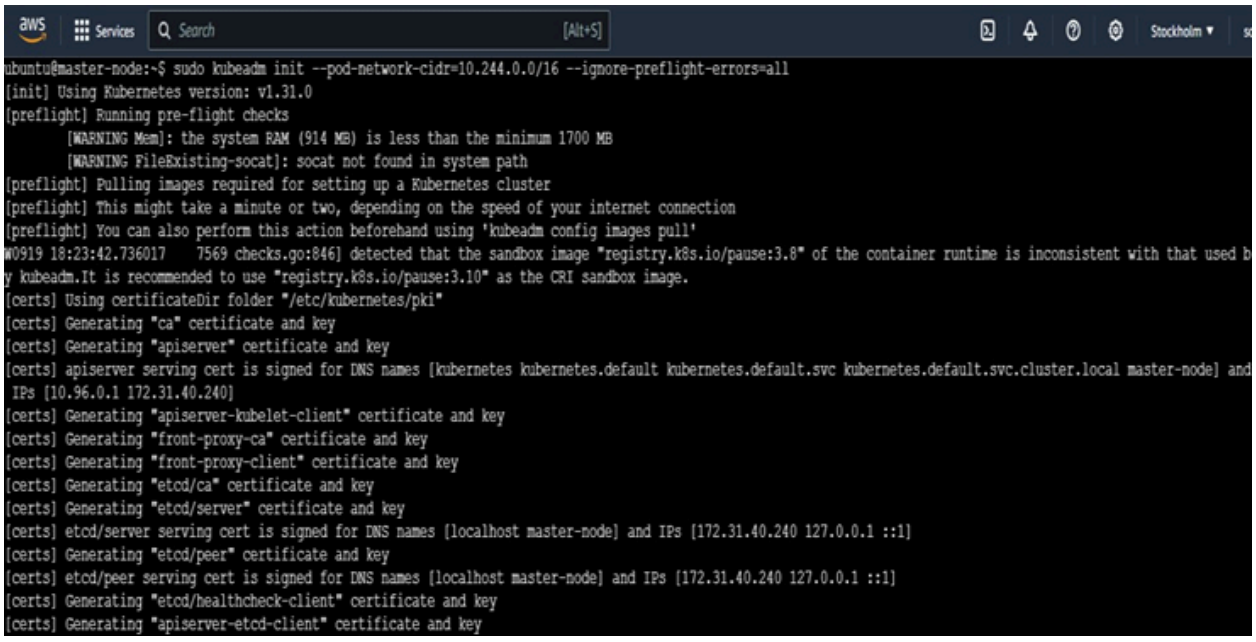




Kubernetes Deployment (master only)
Begin Kubernetes Deployment

$ sudo swapoff –a

Initialize Kubernetes on Master Node
$ sudo kubeadm init --pod-network-cidr=10.244.0.0/16--ignore- preflight- errors=all



Deploy Pod Network to Cluster

$ mkdir -p $HOME/.kube

$ sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config

$ sudo chown $(id -u):$(id -g) $HOME/.kube/config

$ kubectl apply -f https://raw.githubusercontent.com/coreos/flannel/master/Documentation/kube-flannel.yml

```
kubeadm join 172.31.40.240:6443 --token i0zoaj.tblkx57b8mg41aq3 \
        --discovery-token-ca-cert-hash sha256:b66cf6a507714d87b3012ab879b7af89f0d484df29bd6bccc7808e713a1c52fa
ubuntu@master-node:~$   mkdir -p $HOME/.kube
ubuntu@master-node:~$  sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
ubuntu@master-node:~$ sudo chown $(id -u):$(id -g) $HOME/.kube/config
ubuntu@master-node:~$ ^C
ubuntu@master-node:~$ kubectl apply -f https://github.com/flannel-io/flannel/releases/latest/download/kube-flannel.yml
namespace/kube-flannel created
serviceaccount/flannel created
clusterrole.rbac.authorization.k8s.io/flannel created
clusterrolebinding.rbac.authorization.k8s.io/flannel created
configmap/kube-flannel-cfg created
daemonset.apps/kube-flannel-ds created
ubuntu@master-node:~$
```

$ kubectl get pods --all-namespaces

```
ubuntu@master-node:~$ kubectl get pods --all-namespaces
NAMESPACE      NAME                                READY   STATUS             RESTARTS        AGE
kube-flannel   kube-flannel-ds-gmnqm               1/1     Running            0               4m57s
kube-system    coredns-7c65d6cfc9-bb6x4            1/1     Running            0               15m
kube-system    coredns-7c65d6cfc9-zfsvw            1/1     Running            0               15m
kube-system    etcd-master-node                    1/1     Running            0               15m
kube-system    kube-apiserver-master-node          1/1     Running            0               15m
kube-system    kube-controller-manager-master-node 1/1     Running            0               15m
kube-system    kube-proxy-k2ksj                    0/1     CrashLoopBackOff   6 (2m40s ago)   15m
kube-system    kube-scheduler-master-node          1/1     Running            0               15m
ubuntu@master-node:~$
```

Join Worker Node to Cluster (on worker node)

sudo kubeadm join 172.31.40.240:6443 --token i0zoaj.tblkx57b8mg41aq3 --discovery-token-ca-cert-hash

sha256:b66cf6a507714d87b3012ab879b7af89f0d484df29bd6bccc7808e713a1c52fa –ignore-preflight-errors=all

```
ubuntu@worker1:~$ sudo kubeadm join 172.31.40.240:6443 --token i0zoaj.tblkx57b8mg4lag3 --discovery-token-ca-cert-hash sha256:b66cf6a507714d87b3012ab879b7af89f0
4df29bd6bccc7808e713a1c52fa --ignore-preflight-errors=all
[preflight] Running pre-flight checks
        [WARNING FileExisting-socat]: socat not found in system path
[preflight] Reading configuration from the cluster...
[preflight] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
[kubelet-start] Writing kubelet configuration to file "/var/lib/kubelet/config.yaml"
[kubelet-start] Writing kubelet environment file with flags to file "/var/lib/kubelet/kubeadm-flags.env"
[kubelet-start] Starting the kubelet
[kubelet-check] Waiting for a healthy kubelet at http://127.0.0.1:10248/healthz. This can take up to 4m0s
[kubelet-check] The kubelet is healthy after 502.220002ms
[kubelet-start] Waiting for the kubelet to perform the TLS Bootstrap

This node has joined the cluster:
* Certificate signing request was sent to apiserver and a response was received.
* The Kubelet was informed of the new secure connection details.

Run 'kubectl get nodes' on the control-plane to see this node join the cluster.
```

$ kubectl get nodes (on master node)

```
aws | Services | Search [Alt+S]
ubuntu@master-node:~$ kubectl get pods --all-namespaces
NAMESPACE      NAME                                 READY   STATUS             RESTARTS        AGE
kube-flannel   kube-flannel-ds-gmnqm                1/1     Running            0               4m57s
kube-system    coredns-7c65d6cfc9-bb6x4             1/1     Running            0               15m
kube-system    coredns-7c65d6cfc9-zfsvw             1/1     Running            0               15m
kube-system    etcd-master-node                     1/1     Running            0               15m
kube-system    kube-apiserver-master-node           1/1     Running            0               15m
kube-system    kube-controller-manager-master-node  1/1     Running            0               15m
kube-system    kube-proxy-k2ksj                     0/1     CrashLoopBackOff   6 (2m40s ago)   15m
kube-system    kube-scheduler-master-node           1/1     Running            0               15m
ubuntu@master-node:~$ kubectl get nodes
NAME          STATUS   ROLES           AGE     VERSION
master-node   Ready    control-plane   39m     v1.31.1
worker1       Ready    <none>          9m44s   v1.31.1
ubuntu@master-node:~$
```

Conclusion

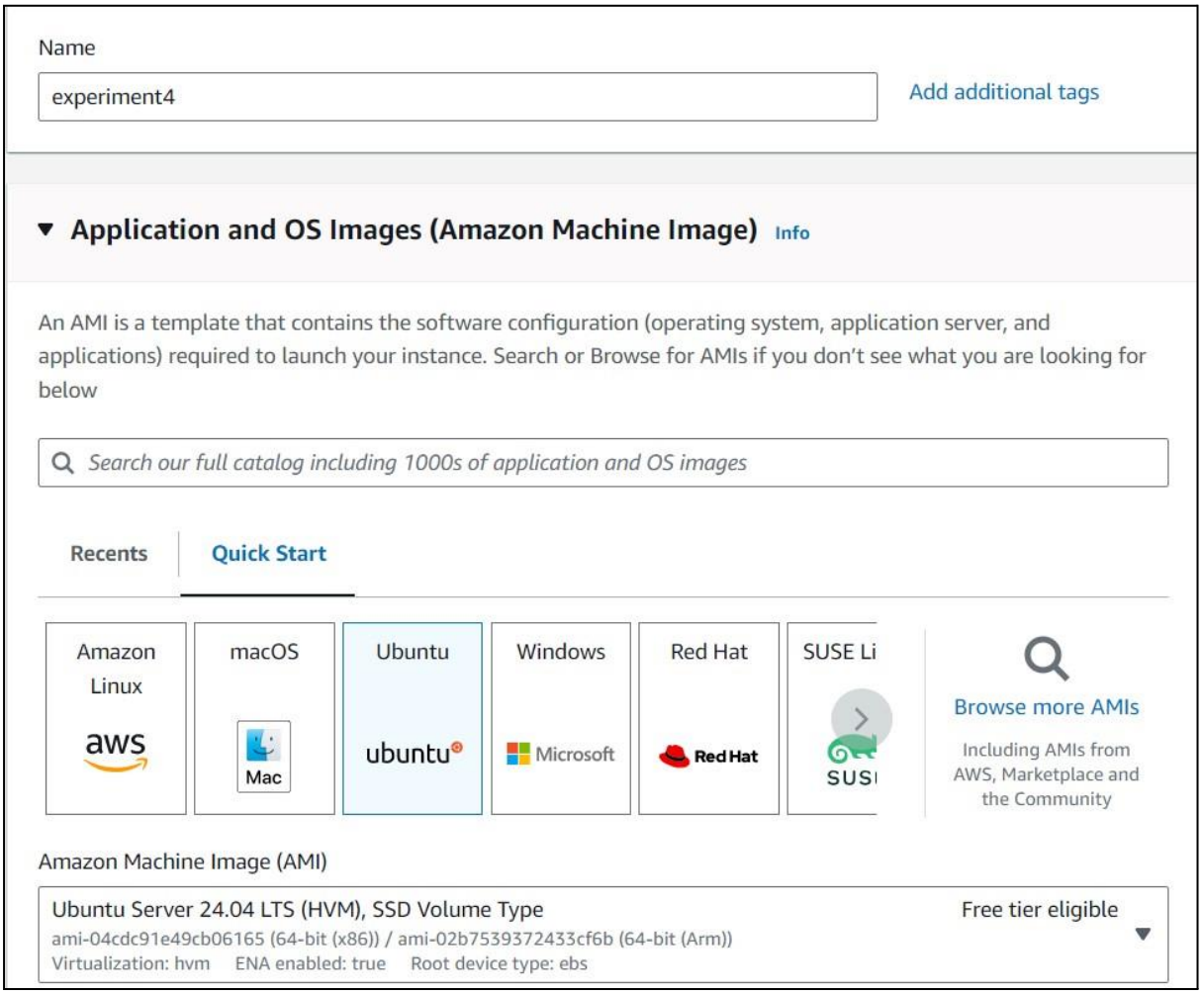
Successfully understood the Kubernetes cluster architecture and deployed a Kubernetes cluster on Linux machines/cloud platforms, demonstrating seamless setup and orchestration.

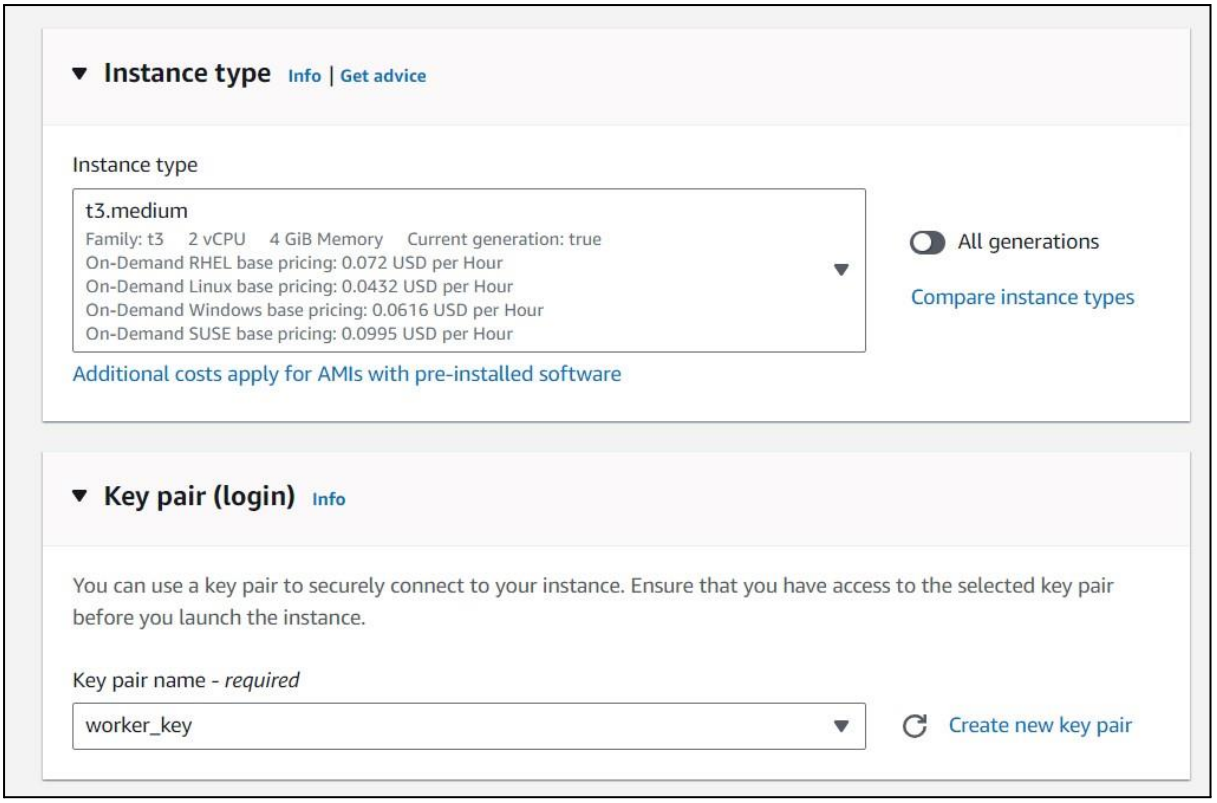
Riya Varyani
D15A - 64

Experiment 4

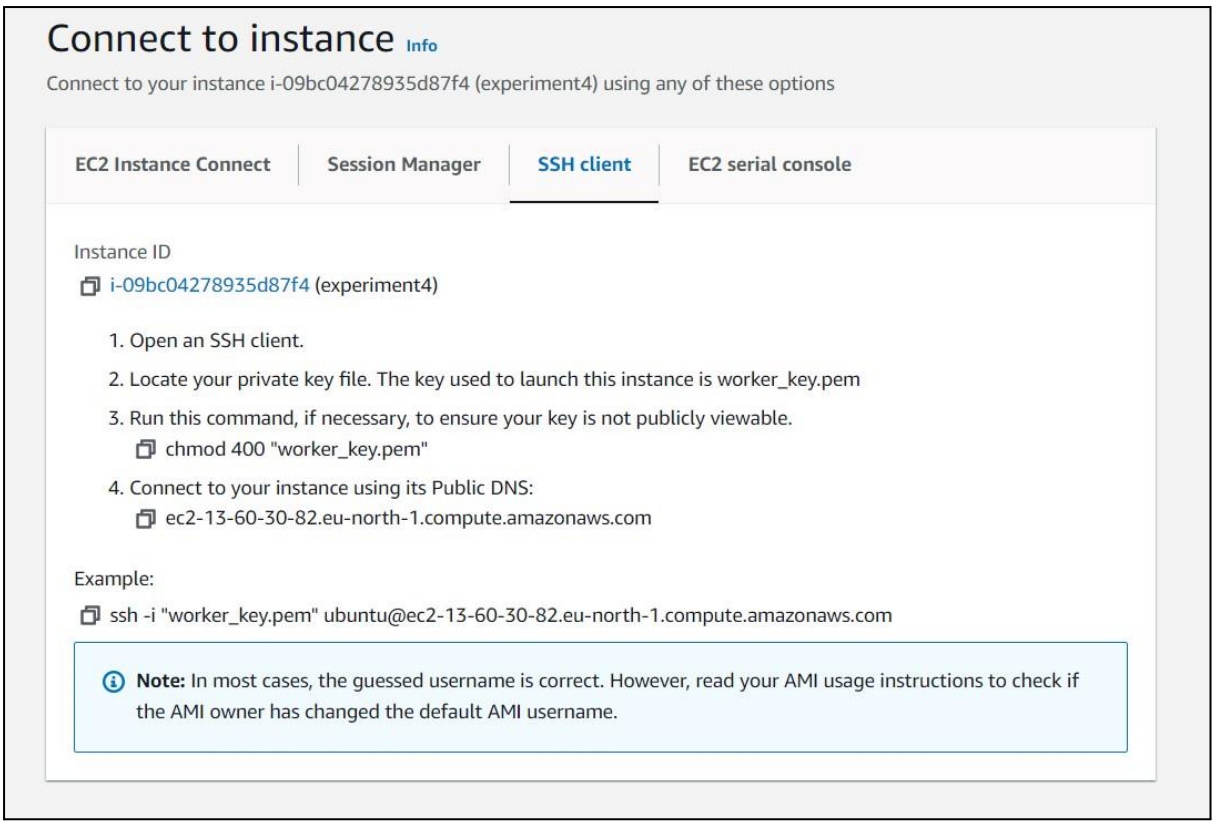
Aim: To install Kubectl and execute Kubectl commands to manage the Kubernetes cluster and deploy Your First Kubernetes Application.

Step 1: Log in to your AWS Academy/personal account and launch a new Ec2 Instance. Select Ubuntu as AMI and t2.medium as Instance Type, create a key of type RSA with .pem extension, and move the downloaded key to the new folder




Instance type Info | Get advice
Instance type
t3.medium
Family: t3 2 vCPU 4 GiB Memory Current generation: true
On-Demand RHEL base pricing: 0.072 USD per Hour
On-Demand Linux base pricing: 0.0432 USD per Hour
On-Demand Windows base pricing: 0.0616 USD per Hour
On-Demand SUSE base pricing: 0.0995 USD per Hour
All generations
Compare instance types
Additional costs apply for AMIs with pre-installed software
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
worker_key
Create new key pair


EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-09bc04278935d87f4)
Launch log



Step 3: Now open the folder in the terminal where our .pem key is stored and paste the Example command

```
PS C:\Users\siddi\downloads> cd exp4
PS C:\Users\siddi\downloads\exp4> ssh -i "worker_key.pem" ubuntu@ec2-13-60-3
0-82.eu-north-1.compute.amazonaws.com
The authenticity of host 'ec2-13-60-30-82.eu-north-1.compute.amazonaws.com (
64:ff9b::d3c:1e52)' can't be established.
ED25519 key fingerprint is SHA256:poqkTnWc7IrjE4zQbuKp8iPtPdLEF+pM5aZMfdtY9L
o.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-60-30-82.eu-north-1.compute.amazonaws.com
' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1012-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Tue Sep 24 18:53:42 UTC 2024

  System load:  0.11              Temperature:           -273.1 C
  Usage of /:   22.8% of 6.71GB   Processes:             112
  Memory usage: 5%                Users logged in:       0
  Swap usage:   0%                IPv4 address for ens5: 172.31.37.243
```

Step 4: Run the below commands to install and setup Docker. curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add - curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo tee /etc/apt/trusted.gpg.d/docker.gpg

> /dev/null sudo add-apt-repository "deb [arch=amd64]
https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable"

```
ubuntu@ip-172-31-37-243:~$ curl -fsSL https://download.docker.com/linux/ubun
tu/gpg | sudo apt-key add -
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo tee
/etc/apt/trusted.gpg.d/docker.gpg > /dev/null
sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/
ubuntu
$(lsb_release -cs) stable"
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instea
d (see apt-key(8)).
OK
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFit2ioBEADhWpZ8/wvZ6hUTiXOwQHXMAlaFHcPH9hAtr4F1y2+OYdbtMuth
lqqwp028AqyY+PRfVMtSYMbjuQuu5byyKR01BbqYhuS3jtqQmljZ/bJvXqnmiVXh
38UuLa+z077PxyxQhu5BbqntTPQMfiyqEiU+BKbq2WmANUKQf+1AmZY/IruOXbnq
L4C1+gJ8vfmXQt99npCaxEjaNRVYfOS8QcixNzHUYnb6emjlANyEVlZzeqo7XKl7
UrwV5inawTSzWNvtjEjj4nJL8NsLwscpLPQUhTQ+7BbQXAwAmeHCUTQIvvWXqw0N
cmhh4HgeQscQHYgOJjjDVfoY5MucvglbIgCqfzAHW9jxmRL4qbMZj+b1XoePEtht
ku4bIQN1X5P07fNWzlgaRL5Z4POXDDZTlIQ/El58j9kp4bnWRCJW0lya+f8ocodo
vZZ+Doi+fy4D5ZGrL4XEcIQP/Lv5uFyf+kQtl/94VFYVJOleAv8W92KdgDkhTcTD
G7c0tIkVEKNUq48b3aQ64NOZQW7fVjfoKwEZdOqPE72Pa45jrZzvUFxSpdiNk2tZ
XYukHjlxxEgBdC/J3cMMNRE1F4NCA3ApfV1Y7/hTeOnmDuDYwr9/obA8t016Yljj
```

```
on-en [2808 B]
Get:51 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Com
ponents [208 B]
Get:52 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n
-f Metadata [344 B]
Fetched 29.1 MB in 5s (5866 kB/s)
Reading package lists... Done
W: https://download.docker.com/linux/ubuntu/dists/noble/InRelease: Key is st
ored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATI
ON section in apt-key(8) for details.
ubuntu@ip-172-31-37-243:~$
```

sudo apt-get update sudo apt-
get install -y docker-ce

```
ubuntu@ip-172-31-37-243:~$ sudo apt-get update
sudo apt-get install -y docker-ce
Hit:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates InReleas
e
Hit:3 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRele
ase
Hit:4 https://download.docker.com/linux/ubuntu noble InRelease
Hit:5 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
W: https://download.docker.com/linux/ubuntu/dists/noble/InRelease: Key is st
ored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATI
ON section in apt-key(8) for details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

```
Setting up docker-ce (5:27.3.1-1~ubuntu.24.04~noble) ...
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service →
 /usr/lib/systemd/system/docker.service.
Created symlink /etc/systemd/system/sockets.target.wants/docker.socket → /us
r/lib/systemd/system/docker.socket.
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-37-243:~$
```

sudo mkdir -p /etc/docker cat <<EOF | sudo
tee /etc/docker/daemon.json
{
"exec-opts": ["native.cgroupdriver=systemd"]
}
EOF

```
ubuntu@ip-172-31-37-243:~$ sudo mkdir -p /etc/docker
cat <<EOF | sudo tee /etc/docker/daemon.json
{
"exec-opts": ["native.cgroupdriver=systemd"]
}
EOF
{
"exec-opts": ["native.cgroupdriver=systemd"]
}
ubuntu@ip-172-31-37-243:~$
```

sudo systemctl enable docker
sudo systemctl daemon-reload
sudo systemctl restart docker

```
ubuntu@ip-172-31-37-243:~$ sudo systemctl enable docker
sudo systemctl daemon-reload
sudo systemctl restart docker
Synchronizing state of docker.service with SysV service script with /usr/lib
/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable docker
ubuntu@ip-172-31-37-243:~$
```

Step 5: Run the below command to install Kubernets.
curl -fsSL https://pkgs.k8s.io/core:/stable:/v1.31/deb/Release.key | sudo gpg --dearmor -o

/etc/apt/keyrings/kubernetes-apt-keyring.gpg echo 'deb

[signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg]

https://pkgs.k8s.io/core:/stable:/v1.31/deb/ /' | sudo tee

/etc/apt/sources.list.d/kubernetes.list

```
ubuntu@ip-172-31-37-243:~$ curl -fsSL https://pkgs.k8s.io/core:/stable:/v1.3
1/deb/Release.key | sudo gpg --dearmor -o
/etc/apt/keyrings/kubernetes-apt-keyring.gpg
echo 'deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg]
https://pkgs.k8s.io/core:/stable:/v1.31/deb/ /' | sudo tee /etc/apt/sources.
list.d/kubernetes.list
gpg: missing argument for option "-o"
-bash: /etc/apt/keyrings/kubernetes-apt-keyring.gpg: No such file or directo
ry
deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg]
https://pkgs.k8s.io/core:/stable:/v1.31/deb/ /
ubuntu@ip-172-31-37-243:~$
```

Error:

```
ubuntu@ip-172-31-37-243:~$ sudo apt-get update
sudo apt-get install -y kubelet kubeadm kubectl
sudo apt-mark hold kubelet kubeadm kubectl
E: Malformed entry 1 in list file /etc/apt/sources.list.d/kubernetes.list (U
RI)
E: The list of sources could not be read.
E: Malformed entry 1 in list file /etc/apt/sources.list.d/kubernetes.list (U
RI)
E: The list of sources could not be read.
E: Malformed entry 1 in list file /etc/apt/sources.list.d/kubernetes.list (U
RI)
E: The list of sources could not be read.
```

```
ubuntu@ip-172-31-37-243:~$ sudo mkdir -p /etc/apt/keyrings
ubuntu@ip-172-31-37-243:~$ curl -fsSL https://pkgs.k8s.io/core:/stable:/v1.3
1/deb/Release.key | sudo gpg --dearmor -o
/etc/apt/keyrings/kubernetes-apt-keyring.gpg
echo 'deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg]
https://pkgs.k8s.io/core:/stable:/v1.31/deb/ /' | sudo tee /etc/apt/sources.
list.d/kubernetes.list
gpg: missing argument for option "-o"
-bash: /etc/apt/keyrings/kubernetes-apt-keyring.gpg: No such file or directo
ry
deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg]
https://pkgs.k8s.io/core:/stable:/v1.31/deb/ /
ubuntu@ip-172-31-37-243:~$ sudo apt-get update
sudo apt-get install -y kubelet kubeadm kubectl
sudo apt-mark hold kubelet kubeadm kubectl
E: Malformed entry 1 in list file /etc/apt/sources.list.d/kubernetes.list (U
RI)
E: The list of sources could not be read.
E: Malformed entry 1 in list file /etc/apt/sources.list.d/kubernetes.list (U
RI)
E: The list of sources could not be read.
E: Malformed entry 1 in list file /etc/apt/sources.list.d/kubernetes.list (U
RI)
E: The list of sources could not be read.
ubuntu@ip-172-31-37-243:~$ sudo mkdir -p /etc/apt/keyrings
ubuntu@ip-172-31-37-243:~$ curl -fsSL https://pkgs.k8s.io/core:/stable:/v1.3
1/deb/Release.key | sudo gpg --dearmor -o /etc/apt/keyrings/kubernetes-apt-k
eyring.gpg
ubuntu@ip-172-31-37-243:~$ echo "deb [signed-by=/etc/apt/keyrings/kubernetes
-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:/v1.31/deb/ /" | sudo tee
 /etc/apt/sources.list.d/kubernetes.list
deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8
s.io/core:/stable:/v1.31/deb/ /
ubuntu@ip-172-31-37-243:~$ sudo apt-get update
Hit:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates InReleas
e
Hit:3 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRele
ase
```

```
ubuntu@ip-172-31-37-243:~$ sudo apt-get install -y kubelet kubeadm kubectl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  conntrack cri-tools kubernetes-cni
The following NEW packages will be installed:
  conntrack cri-tools kubeadm kubectl kubelet kubernetes-cni
0 upgraded, 6 newly installed, 0 to remove and 139 not upgraded.
Need to get 87.4 MB of archives.
After this operation, 314 MB of additional disk space will be used.
Get:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 connt
rack amd64 1:1.4.8-1ubuntu1 [37.9 kB]
Get:2 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/s
table:/v1.31/deb  cri-tools 1.31.1-1.1 [15.7 MB]
Get:3 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/s
table:/v1.31/deb  kubeadm 1.31.1-1.1 [11.4 MB]
Get:4 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/s
table:/v1.31/deb  kubectl 1.31.1-1.1 [11.2 MB]
Get:5 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/s
table:/v1.31/deb  kubernetes-cni 1.5.1-1.1 [33.9 MB]
Get:6 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/s
table:/v1.31/deb  kubelet 1.31.1-1.1 [15.2 MB]
Fetched 87.4 MB in 1s (78.5 MB/s)
Selecting previously unselected package conntrack.
(Reading database ... 68007 files and directories currently installed.)
Preparing to unpack .../0-conntrack_1%3a1.4.8-1ubuntu1_amd64.deb ...
Unpacking conntrack (1:1.4.8-1ubuntu1) ...
Selecting previously unselected package cri-tools.
Preparing to unpack .../1-cri-tools_1.31.1-1.1_amd64.deb ...
Unpacking cri-tools (1.31.1-1.1) ...
Selecting previously unselected package kubeadm.
Preparing to unpack .../2-kubeadm_1.31.1-1.1_amd64.deb ...
Unpacking kubeadm (1.31.1-1.1) ...
Selecting previously unselected package kubectl.
Setting up kubeadm (1.31.1-1.1) ...
Setting up kubelet (1.31.1-1.1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-37-243:~$ sudo apt-mark hold kubelet kubeadm kubectl
kubelet set on hold.
kubeadm set on hold.
kubectl set on hold.
ubuntu@ip-172-31-37-243:~$
```

sudo systemctl enable --now kubelet sudo kubeadm
init --pod-network-cidr=10.244.0.0/16

```
ubuntu@ip-172-31-37-243:~$ sudo systemctl enable --now kubelet
sudo kubeadm init --pod-network-cidr=10.244.0.0/16
[init] Using Kubernetes version: v1.31.0
[preflight] Running pre-flight checks
W0924 19:06:55.141347    4241 checks.go:1080] [preflight] WARNING: Couldn't
create the interface used for talking to the container runtime: failed to cr
eate new CRI runtime service: validate service connection: validate CRI v1 r
untime API for endpoint "unix:///var/run/containerd/containerd.sock": rpc er
ror: code = Unimplemented desc = unknown service runtime.v1.RuntimeService
        [WARNING FileExisting-socat]: socat not found in system path
[preflight] Pulling images required for setting up a Kubernetes cluster
[preflight] This might take a minute or two, depending on the speed of your
internet connection
[preflight] You can also perform this action beforehand using 'kubeadm confi
g images pull'
error execution phase preflight: [preflight] Some fatal errors occurred:
failed to create new CRI runtime service: validate service connection: valid
ate CRI v1 runtime API for endpoint "unix:///var/run/containerd/containerd.s
ock": rpc error: code = Unimplemented desc = unknown service runtime.v1.Runt
imeService[preflight] If you know what you are doing, you can make a check n
on-fatal with `--ignore-preflight-errors=...`
To see the stack trace of this error execute with --v=5 or higher
ubuntu@ip-172-31-37-243:~$
```

sudo apt-get install -y containerd

```
ubuntu@ip-172-31-37-243:~$ sudo apt-get install -y containerd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  docker-buildx-plugin docker-ce-cli docker-ce-rootless-extras
  docker-compose-plugin libltdl7 libslirp0 pigz slirp4netns
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  runc
The following packages will be REMOVED:
  containerd.io docker-ce
The following NEW packages will be installed:
  containerd runc
0 upgraded, 2 newly installed, 2 to remove and 139 not upgraded.
Need to get 47.2 MB of archives.
After this operation, 53.1 MB disk space will be freed.
Get:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 runc amd64 1.1.12-0ubuntu3.1 [8599 kB]
Get:2 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 containerd amd64 1.7.12-0ubuntu4.1 [38.6 MB]
Fetched 47.2 MB in 1s (81.0 MB/s)
(Reading database ... 68064 files and directories currently installed.)
Removing docker-ce (5:27.3.1-1~ubuntu.24.04~noble) ...
Removing containerd.io (1.7.22-1) ...
Selecting previously unselected package runc.
(Reading database ... 68044 files and directories currently installed.)
Preparing to unpack .../runc_1.1.12-0ubuntu3.1_amd64.deb ...
Unpacking runc (1.1.12-0ubuntu3.1) ...
Selecting previously unselected package containerd.
Preparing to unpack .../containerd_1.7.12-0ubuntu4.1_amd64.deb ...
Unpacking containerd (1.7.12-0ubuntu4.1) ...
Setting up runc (1.1.12-0ubuntu3.1) ...
Setting up containerd (1.7.12-0ubuntu4.1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...
```

sudo mkdir -p /etc/containerd sudo containerd config default | sudo
tee /etc/containerd/config.toml

```
ubuntu@ip-172-31-37-243:~$ sudo mkdir -p /etc/containerd
sudo containerd config default | sudo tee /etc/containerd/config.toml
disabled_plugins = []
imports = []
oom_score = 0
plugin_dir = ""
required_plugins = []
root = "/var/lib/containerd"
state = "/run/containerd"
temp = ""
version = 2

[cgroup]
  path = ""

[debug]
  address = ""
  format = ""
  gid = 0
  level = ""
  uid = 0
```

```
[timeouts]
  "io.containerd.timeout.bolt.open" = "0s"
  "io.containerd.timeout.metrics.shimstats" = "2s"
  "io.containerd.timeout.shim.cleanup" = "5s"
  "io.containerd.timeout.shim.load" = "5s"
  "io.containerd.timeout.shim.shutdown" = "3s"
  "io.containerd.timeout.task.state" = "2s"

[ttrpc]
  address = ""
  gid = 0
  uid = 0
ubuntu@ip-172-31-37-243:~$
```

sudo systemctl restart containerd
sudo systemctl enable containerd
sudo systemctl status containerd

```
ubuntu@ip-172-31-37-243:~$ sudo systemctl restart containerd
sudo systemctl enable containerd
sudo systemctl status containerd
● containerd.service - containerd container runtime
     Loaded: loaded (/usr/lib/systemd/system/containerd.service; enabled; p>
     Active: active (running) since Tue 2024-09-24 19:09:13 UTC; 325ms ago
       Docs: https://containerd.io
   Main PID: 4718 (containerd)
      Tasks: 8
     Memory: 13.2M (peak: 13.8M)
        CPU: 73ms
     CGroup: /system.slice/containerd.service
             └─4718 /usr/bin/containerd

Sep 24 19:09:13 ip-172-31-37-243 containerd[4718]: time="2024-09-24T19:09:1>
Sep 24 19:09:13 ip-172-31-37-243 containerd[4718]: time="2024-09-24T19:09:1>
Sep 24 19:09:13 ip-172-31-37-243 containerd[4718]: time="2024-09-24T19:09:1>
Sep 24 19:09:13 ip-172-31-37-243 containerd[4718]: time="2024-09-24T19:09:1>
Sep 24 19:09:13 ip-172-31-37-243 containerd[4718]: time="2024-09-24T19:09:1>
Sep 24 19:09:13 ip-172-31-37-243 containerd[4718]: time="2024-09-24T19:09:1>
Sep 24 19:09:13 ip-172-31-37-243 containerd[4718]: time="2024-09-24T19:09:1>
Sep 24 19:09:13 ip-172-31-37-243 containerd[4718]: time="2024-09-24T19:09:1>
Sep 24 19:09:13 ip-172-31-37-243 systemd[1]: Started containerd.service - c>
Sep 24 19:09:13 ip-172-31-37-243 containerd[4718]: time="2024-09-24T19:09:1>
lines 1-21/21 (END)
● containerd.service - containerd container runtime
     Loaded: loaded (/usr/lib/systemd/system/containerd.service; enabled; preset: enabled)
     Active: active (running) since Tue 2024-09-24 19:09:13 UTC; 325ms ago
       Docs: https://containerd.io
   Main PID: 4718 (containerd)
      Tasks: 8
     Memory: 13.2M (peak: 13.8M)
        CPU: 73ms
     CGroup: /system.slice/containerd.service
             └─4718 /usr/bin/containerd
```

sudo apt-get install -y socat

```
ubuntu@ip-172-31-37-243:~$ sudo apt-get install -y socat
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  docker-buildx-plugin docker-ce-cli docker-ce-rootless-extras docker-compose-plugin libltdl7 libslirp0 pigz slirp4netns
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  socat
0 upgraded, 1 newly installed, 0 to remove and 139 not upgraded.
Need to get 374 kB of archives.
After this operation, 1649 kB of additional disk space will be used.
Get:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 socat amd64 1.8.0.0-4build3 [374 kB]
Fetched 374 kB in 0s (22.1 MB/s)
Selecting previously unselected package socat.
(Reading database ... 68108 files and directories currently installed.)
Preparing to unpack .../socat_1.8.0.0-4build3_amd64.deb ...
Unpacking socat (1.8.0.0-4build3) ...
Setting up socat (1.8.0.0-4build3) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-37-243:~$ |
```

Step 6: Initialize the Kubecluster sudo kubeadm init --pod-network-cidr=10.244.0.0/16

```
ubuntu@ip-172-31-37-243:~$ sudo kubeadm init --pod-network-cidr=10.244.0.0/1
6
[init] Using Kubernetes version: v1.31.0
[preflight] Running pre-flight checks
[preflight] Pulling images required for setting up a Kubernetes cluster
[preflight] This might take a minute or two, depending on the speed of your
internet connection
[preflight] You can also perform this action beforehand using 'kubeadm confi
g images pull'
W0924 19:12:15.863783    5009 checks.go:846] detected that the sandbox image
 "registry.k8s.io/pause:3.8" of the container runtime is inconsistent with t
hat used by kubeadm.It is recommended to use "registry.k8s.io/pause:3.10" as
 the CRI sandbox image.
[certs] Using certificateDir folder "/etc/kubernetes/pki"
[certs] Generating "ca" certificate and key
[certs] Generating "apiserver" certificate and key
[certs] apiserver serving cert is signed for DNS names [ip-172-31-37-243 kub
ernetes kubernetes.default kubernetes.default.svc kubernetes.default.svc.clu
ster.local] and IPs [10.96.0.1 172.31.37.243]
[certs] Generating "apiserver-kubelet-client" certificate and key
[certs] Generating "front-proxy-ca" certificate and key
[certs] Generating "front-proxy-client" certificate and key
[certs] Generating "etcd/ca" certificate and key
[certs] Generating "etcd/server" certificate and key
[certs] etcd/server serving cert is signed for DNS names [ip-172-31-37-243 l
ocalhost] and IPs [172.31.37.243 127.0.0.1 ::1]
[certs] Generating "etcd/peer" certificate and key
[certs] etcd/peer serving cert is signed for DNS names [ip-172-31-37-243 loc
alhost] and IPs [172.31.37.243 127.0.0.1 ::1]
[certs] Generating "etcd/healthcheck-client" certificate and key
[certs] Generating "apiserver-etcd-client" certificate and key
[certs] Generating "sa" key and public key
[kubeconfig] Using kubeconfig folder "/etc/kubernetes"
[kubeconfig] Writing "admin.conf" kubeconfig file
[kubeconfig] Writing "super-admin.conf" kubeconfig file
[kubeconfig] Writing "kubelet.conf" kubeconfig file
[kubeconfig] Writing "controller-manager.conf" kubeconfig file
[kubeconfig] Writing "scheduler.conf" kubeconfig file
[etcd] Creating static Pod manifest for local etcd in "/etc/kubernetes/manif
ests"
```

```
Your Kubernetes control-plane has initialized successfully!

To start using your cluster, you need to run the following as a regular user
:

  mkdir -p $HOME/.kube
  sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
  sudo chown $(id -u):$(id -g) $HOME/.kube/config

Alternatively, if you are the root user, you can run:

  export KUBECONFIG=/etc/kubernetes/admin.conf

You should now deploy a pod network to the cluster.
Run "kubectl apply -f [podnetwork].yaml" with one of the options listed at:
  https://kubernetes.io/docs/concepts/cluster-administration/addons/

Then you can join any number of worker nodes by running the following on eac
h as root:

kubeadm join 172.31.37.243:6443 --token 83t146.gii8h4xivxue1bio \
        --discovery-token-ca-cert-hash sha256:d3833aa042f888a0a506ff97a41023
c5524cd0e0b533ba00adb635a5eff723d9
ubuntu@ip-172-31-37-243:~$
```

Copy the mkdir and chown commands from the top and execute them.
mkdir -p $HOME/.kube sudo cp -i /etc/kubernetes/admin.conf
$HOME/.kube/config sudo chown $(id -u):$(id -g)
$HOME/.kube/config

```
ubuntu@ip-172-31-37-243:~$ mkdir -p $HOME/.kube
sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
sudo chown $(id -u):$(id -g) $HOME/.kube/config
ubuntu@ip-172-31-37-243:~$
```

Add a common networking plugin called flannel as mentioned in the code.
kubectl apply -f
https://raw.githubusercontent.com/coreos/flannel/master/Documentation/kube-flannel.yml

```
ubuntu@ip-172-31-37-243:~$ kubectl apply -f https://raw.githubusercontent.co
m/coreos/flannel/master/Documentation/kube-flannel.yml
namespace/kube-flannel created
clusterrole.rbac.authorization.k8s.io/flannel created
clusterrolebinding.rbac.authorization.k8s.io/flannel created
serviceaccount/flannel created
configmap/kube-flannel-cfg created
daemonset.apps/kube-flannel-ds created
ubuntu@ip-172-31-37-243:~$
```

Step 7: Now that 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 apply -f https://k8s.io/examples/application/deployment.yaml

```
ubuntu@ip-172-31-37-243:~$ kubectl apply -f https://k8s.io/examples/applicat
ion/deployment.yaml
deployment.apps/nginx-deployment created
ubuntu@ip-172-31-37-243:~$
```

kubectl get pods
POD_NAME=$(kubectl get pods -l app=nginx -o jsonpath="{.items[0].metadata.name}")
kubectl port-forward $POD_NAME 8081:80

kubectl taint nodes --all node-role.kubernetes.io/control-plane-node/ip-172-31-20-171 untainted kubectl get nodes

```
ubuntu@ip-172-31-37-243:~$ kubectl get pods
NAME                              READY   STATUS    RESTARTS   AGE
nginx-deployment-d556bf558-ptclv   0/1     Pending   0          55s
nginx-deployment-d556bf558-rsgxw   0/1     Pending   0          55s
ubuntu@ip-172-31-37-243:~$ POD_NAME=$(kubectl get pods -l app=nginx -o jsonp
ath="{.items[0].metadata.name}")
ubuntu@ip-172-31-37-243:~$ kubectl port-forward $POD_NAME 8080:80
error: unable to forward port because pod is not running. Current status=Pen
ding
ubuntu@ip-172-31-37-243:~$ kubectl taint nodes --all node-role.kubernetes.io
/control-plane-node/ip-172-31-20-171 untainted
error: at least one taint update is required
ubuntu@ip-172-31-37-243:~$ kubectl get nodes
NAME               STATUS   ROLES           AGE   VERSION
ip-172-31-37-243   Ready    control-plane   10m   v1.31.1
ubuntu@ip-172-31-37-243:~$ kubectl taint nodes --all node-role.kubernetes.io
/control-plane-
node/ip-172-31-37-243 untainted
ubuntu@ip-172-31-37-243:~$ kubectl get nodes
NAME               STATUS   ROLES           AGE   VERSION
ip-172-31-37-243   Ready    control-plane   10m   v1.31.1
ubuntu@ip-172-31-37-243:~$
```

```
ubuntu@ip-172-31-37-243:~$ kubectl get pods
NAME                              READY   STATUS    RESTARTS   AGE
nginx-deployment-d556bf558-ptclv   1/1     Running   0          8m32s
nginx-deployment-d556bf558-rsgxw   1/1     Running   0          8m32s
ubuntu@ip-172-31-37-243:~$
```

```
ubuntu@ip-172-31-37-243:~$ POD_NAME=$(kubectl get pods -l app=nginx -o jsonp
ath="{.items[0].metadata.name}")
```

```
ubuntu@ip-172-31-37-243:~$ kubectl port-forward $POD_NAME 8081:80
Forwarding from 127.0.0.1:8081 -> 80
Forwarding from [::1]:8081 -> 80
Forwarding from 127.0.0.1:8081 -> 80
Forwarding from [::1]:8081 -> 80
```

Step 8: Verify your deployment Open up a new terminal and ssh to your EC2 instance. Then, use this curl command to check if the Nginx server is running. curl --head http://127.0.0.1:8080

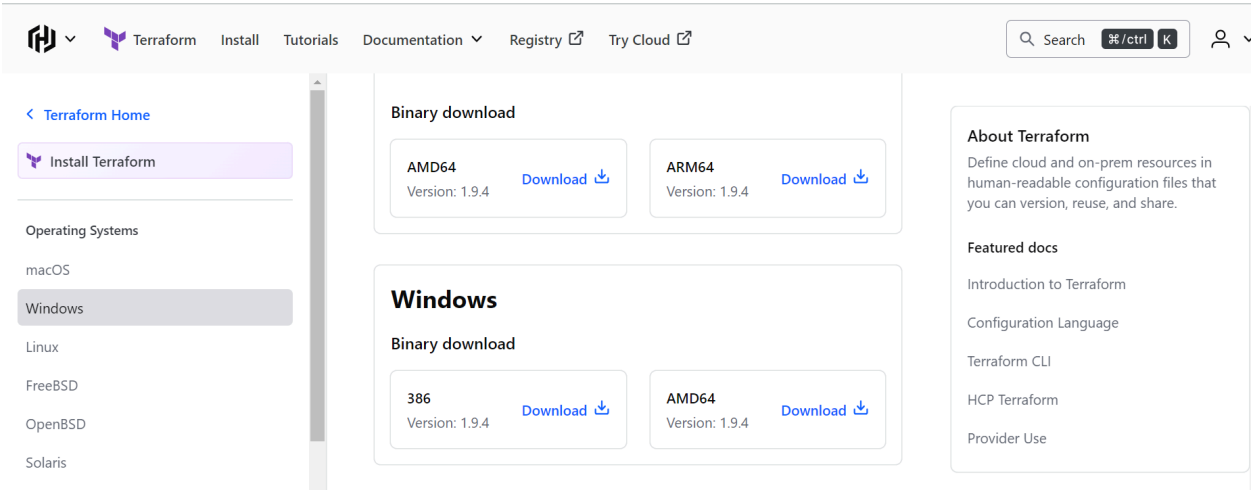
```
PS C:\Users\siddi\downloads\exp4> ssh -i "worker_key.pem" ubuntu@ec2-13-60-3
0-82.eu-north-1.compute.amazonaws.com
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1012-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Tue Sep 24 19:52:47 UTC 2024

  System load:  0.01              Temperature:           -273.1 C
  Usage of /:   55.5% of 6.71GB   Processes:             149
  Memory usage: 20%               Users logged in:       1
  Swap usage:   0%                IPv4 address for ens5: 172.31.37.243


Expanded Security Maintenance for Applications is not enabled.

143 updates can be applied immediately.
41 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

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


Last login: Tue Sep 24 19:41:15 2024 from 152.57.249.67
ubuntu@ip-172-31-37-243:~$ curl --head http://127.0.0.1:8080
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Tue, 24 Sep 2024 19:53:04 GMT
Content-Type: text/html
Content-Length: 612
Last-Modified: Tue, 04 Dec 2018 14:44:49 GMT
Connection: keep-alive
ETag: "5c0692e1-264"
Accept-Ranges: bytes

ubuntu@ip-172-31-37-243:~$
```

Riya Varyani D15A 64

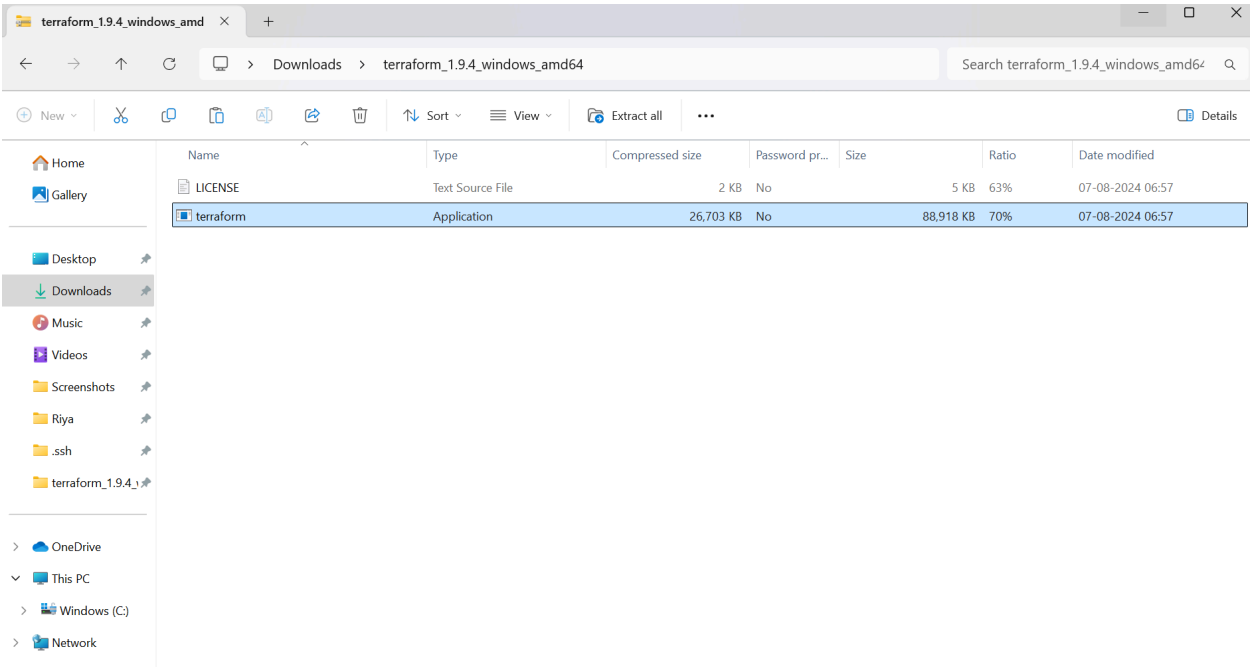
ADVANCE DEVOPS EXPERIMENT NO 5

A) Installation and Configuration of Terraform in Windows

Step 1: Download terraform

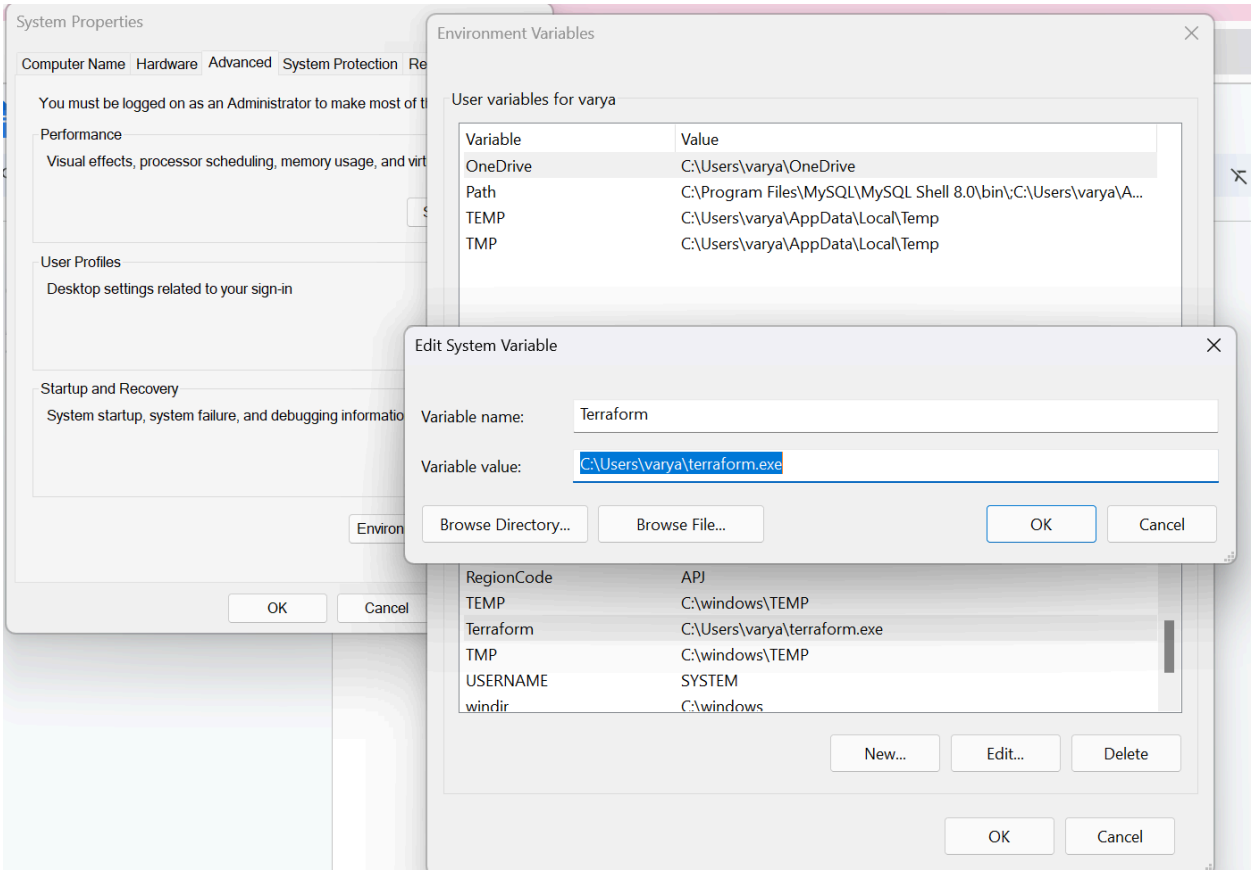


Step 2: Extract the downloaded setup file Terraform.exe in C:\Terraform directory

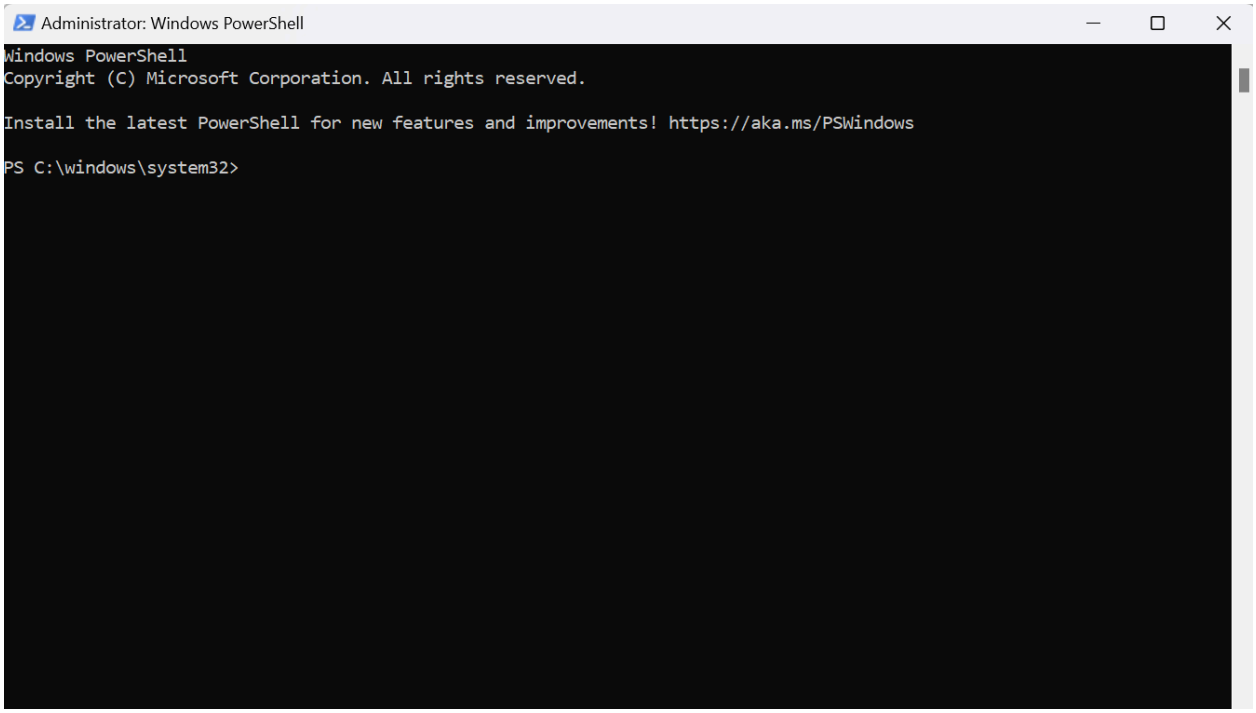


Step 3: Set the System path for Terraform in Environment Variables

Riya Varyani D15A 64

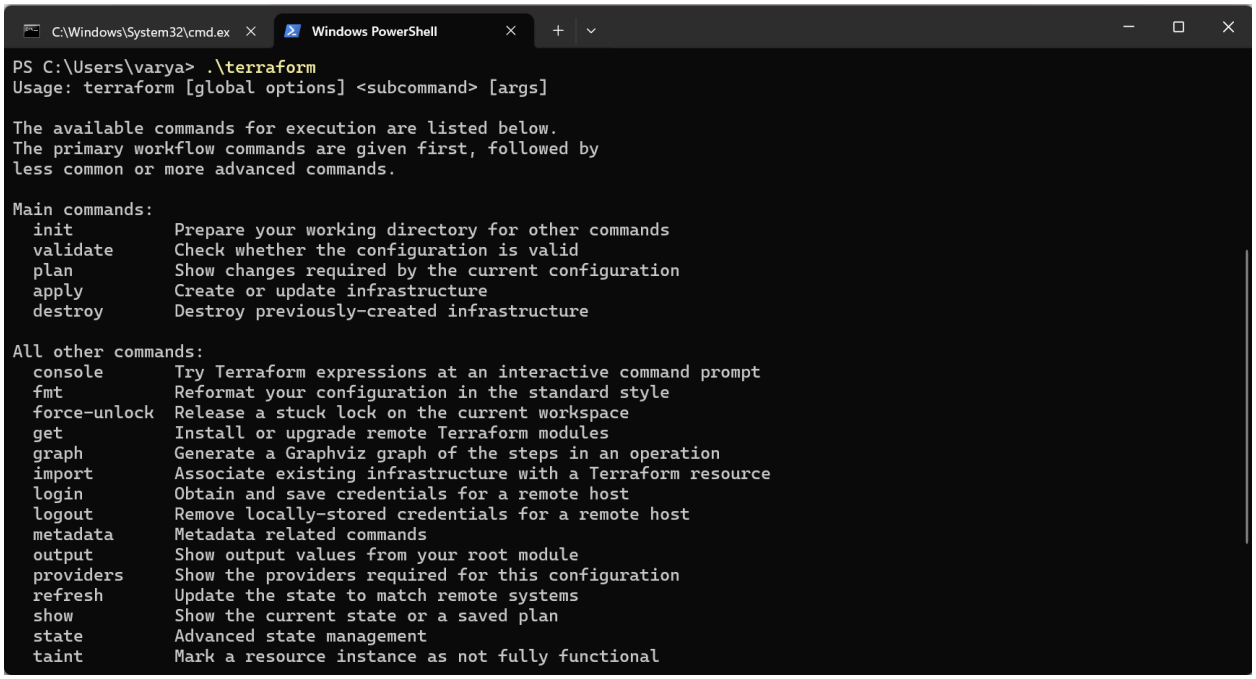


Step 4: Open PowerShell with Admin Access



Step 5 : Open Terraform in PowerShell and check its functionality

Riya Varyani D15A 64



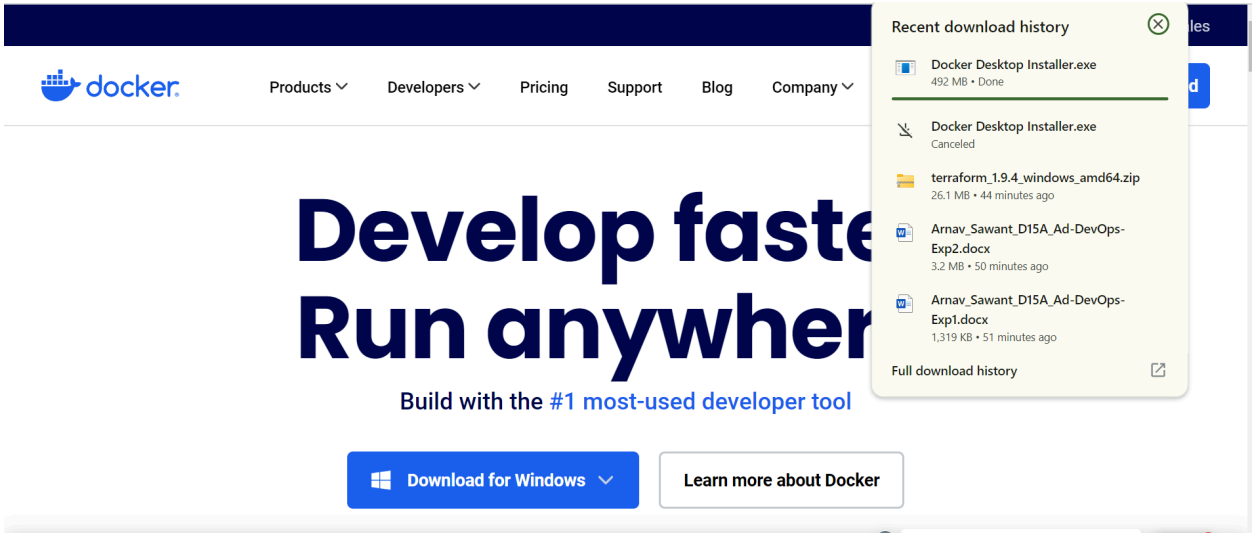
RIYA VARYANI D15A 64

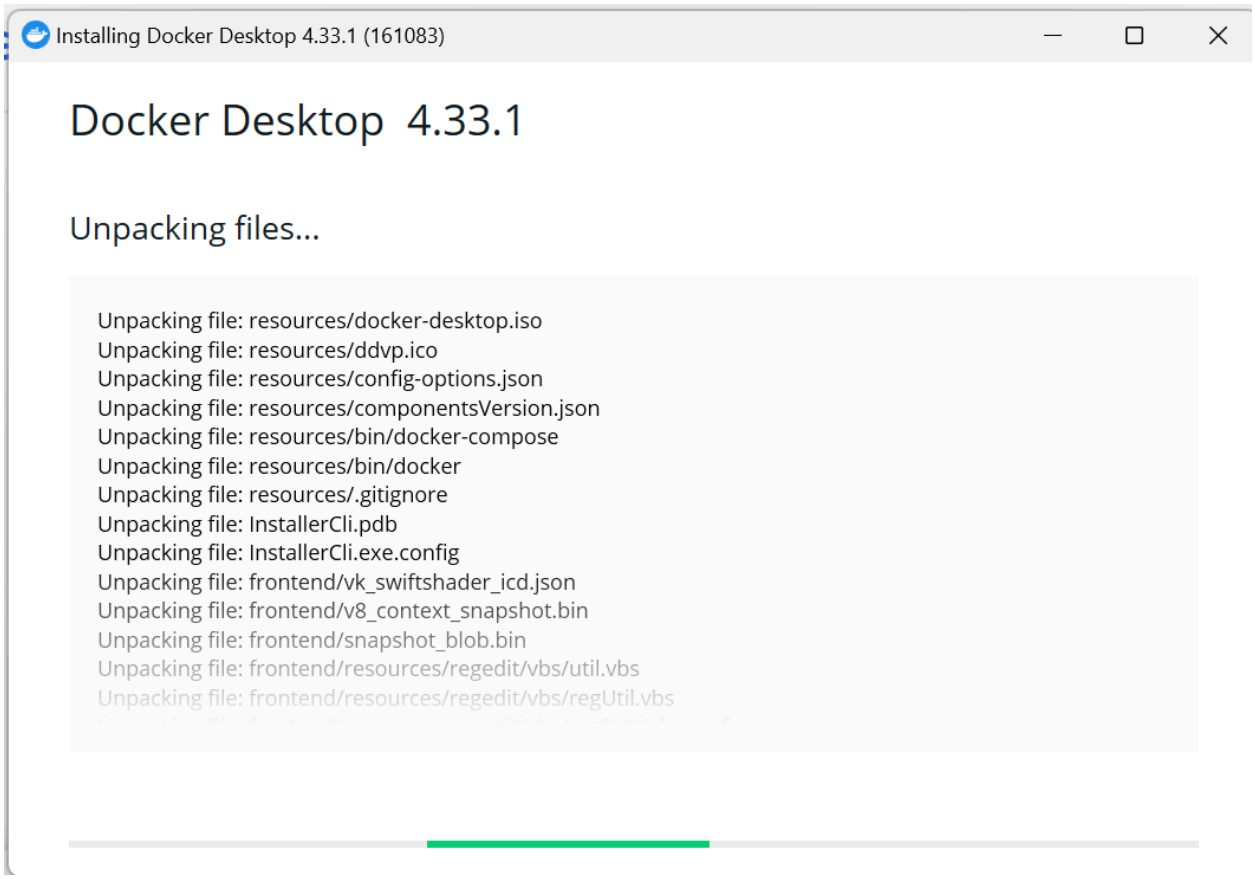
ADVANCE DEVOPS EXPERIMENT NO 6

A. Creating docker image using terraform

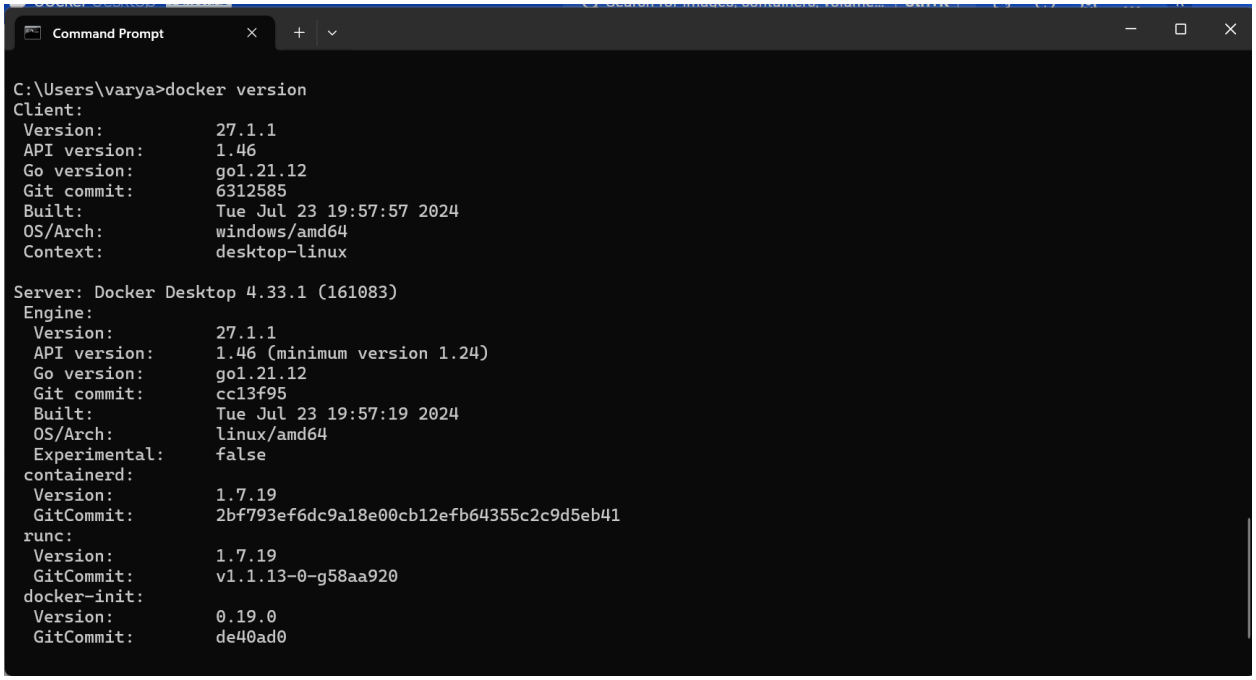
1) Download and Install Docker Desktop from https://www.docker.com/

Step 1: Check the docker functionality





RIYA VARYANI D15A 64



Now, create a folder named ‘Terraform Scripts’ in which we save our different types of
scripts which will be further used in this experiment.

Step 2: Firstly create a new folder named ‘Docker’ in the ‘TerraformScripts’ folder. Then
create a new dteocker.tf file using Atom editor and write the followingcontents into it to
create a Ubuntu Linux container.

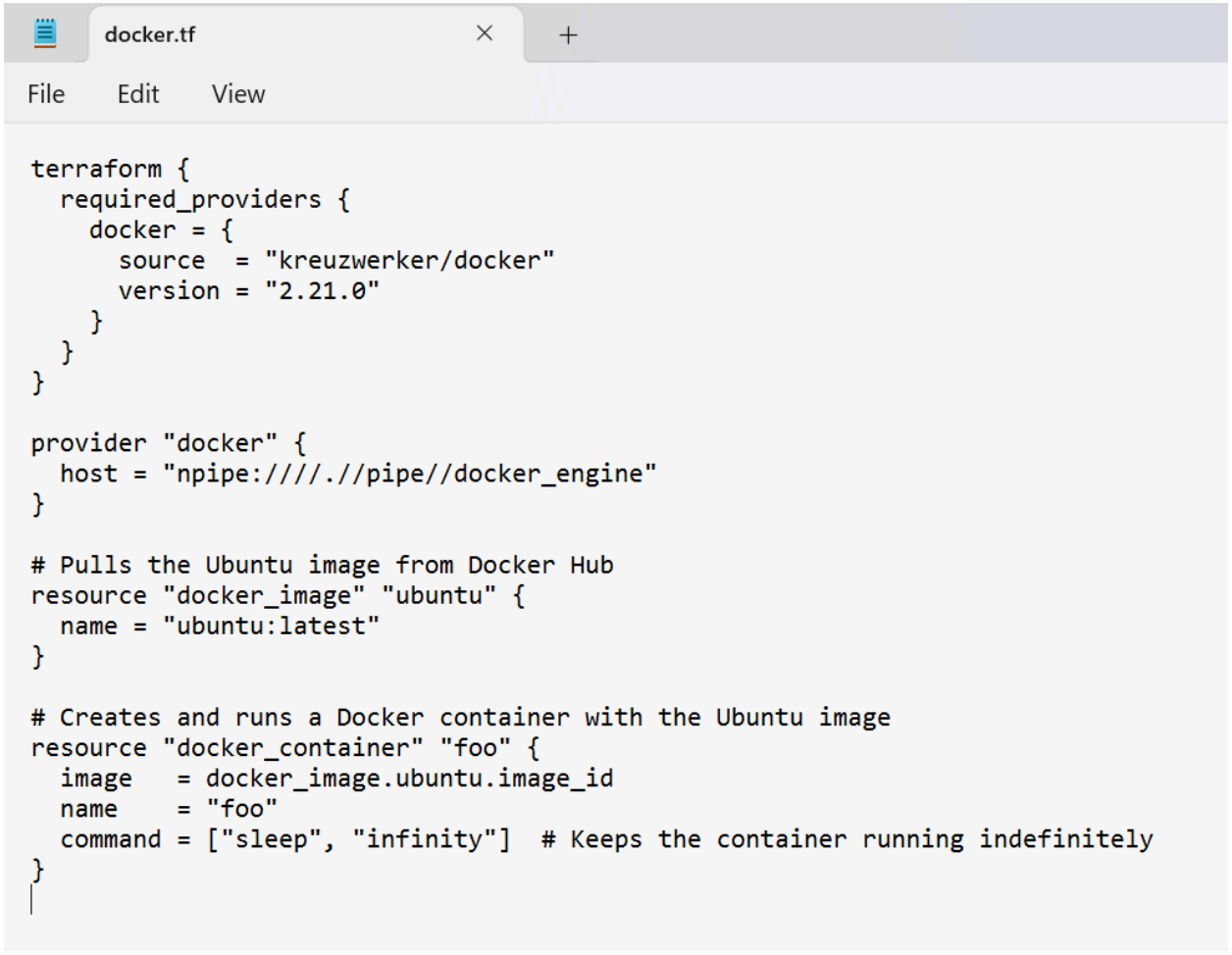
Script:

terraform

```
{ required_providers
{docker = {
source = "kreuzwerker/docker"
version = "2.21.0"
}
}
}
provider "docker" {
host = "npipe:////.//pipe//docker_engine"
}
```

RIYA VARYANI D15A 64

```
# Pulls the image
resource "docker_image" "ubuntu"
{name = "ubuntu:latest"
}
# Create a container
resource "docker_container" "foo"
{ image =
docker_image.ubuntu.image_idname =
"foo"
}
```



Step 3: Execute Terraform Init command to initialize the resources.

RIYA VARYANI D15A 64

```
C:\Users\varya>cd C:\Users\varya\TerraformScripts\Docker

C:\Users\varya\TerraformScripts\Docker>terraform init
Initializing the backend...
Initializing provider plugins...
- Reusing previous version of kreuzwerker/docker from the depend
ency lock file
- Using previously-installed kreuzwerker/docker v2.21.0

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform
 plan" to see
any changes that are required for your infrastructure. All Terra
form commands
should now work.

If you ever set or change modules or backend configuration for T
erraform,
rerun this command to reinitialize your working directory. If yo
u forget, other
commands will detect it and remind you to do so if necessary.
```

Step 4: Execute Terraform plan to see the available resources

```
C:\Users\varya\TerraformScripts\Docker>terraform plan
docker_image.ubuntu: Refreshing state... [id=sha256:edbfe74c41f8
a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:lates
t]

Terraform used the selected providers to generate the following
execution plan. Resource actions are indicated with the
following symbols:
  + create

Terraform will perform the following actions:

  # docker_container.foo will be created
  + resource "docker_container" "foo" {
      + attach           = false
      + bridge           = (known after apply)
      + command          = [
          + "sleep",
          + "infinity",
        ]
      + container_logs   = (known after apply)
      + entrypoint       = (known after apply)
      + env              = (known after apply)
      + exit_code        = (known after apply)
      + gateway          = (known after apply)
      + hostname         = (known after apply)
      + id               = (known after apply)
```

RIYA VARYANI D15A 64

Step 5: Execute Terraform apply to apply the configuration, which will automatically
create and run the Ubuntu Linux container based on our configuration.
Using command :
“terraform apply”

```
C:\Users\varya\TerraformScripts\Docker>terraform apply
docker_image.ubuntu: Refreshing state... [id=sha256:edbfe74c41f8
a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:lates
t]

Terraform used the selected providers to generate the following
execution plan. Resource actions are indicated with the
following symbols:
  + create

Terraform will perform the following actions:

  # docker_container.foo will be created
  + resource "docker_container" "foo" {
      + attach           = false
      + bridge           = (known after apply)
      + command          = [
          + "sleep",
          + "infinity",
        ]
```

Docker images, Before Executing Apply step:

```
C:\Users\varya\TerraformScripts\Docker>docker images
REPOSITORY   TAG       IMAGE ID       CREATED       SIZE
ubuntu       latest    edbfe74c41f8   2 weeks ago   78.1MB
```

Step 6: Execute Terraform destroy to delete the configuration, which will automatically
delete the Ubuntu Container.

RIYA VARYANI D15A 64

```
C:\Users\varya\TerraformScripts\Docker>terraform destroy
docker_image.ubuntu: Refreshing state... [id=sha256:edbfe74c41f8
a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:lates
t]
docker_container.foo: Refreshing state... [id=1dcd9c4a8bbccf62fe
a18099efddb1af6fdcf0a85deab004c503949cb7d16554]

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

Terraform will perform the following actions:

  # docker_container.foo will be destroyed
  - resource "docker_container" "foo" {
```

Docker images After Executing Destroy step

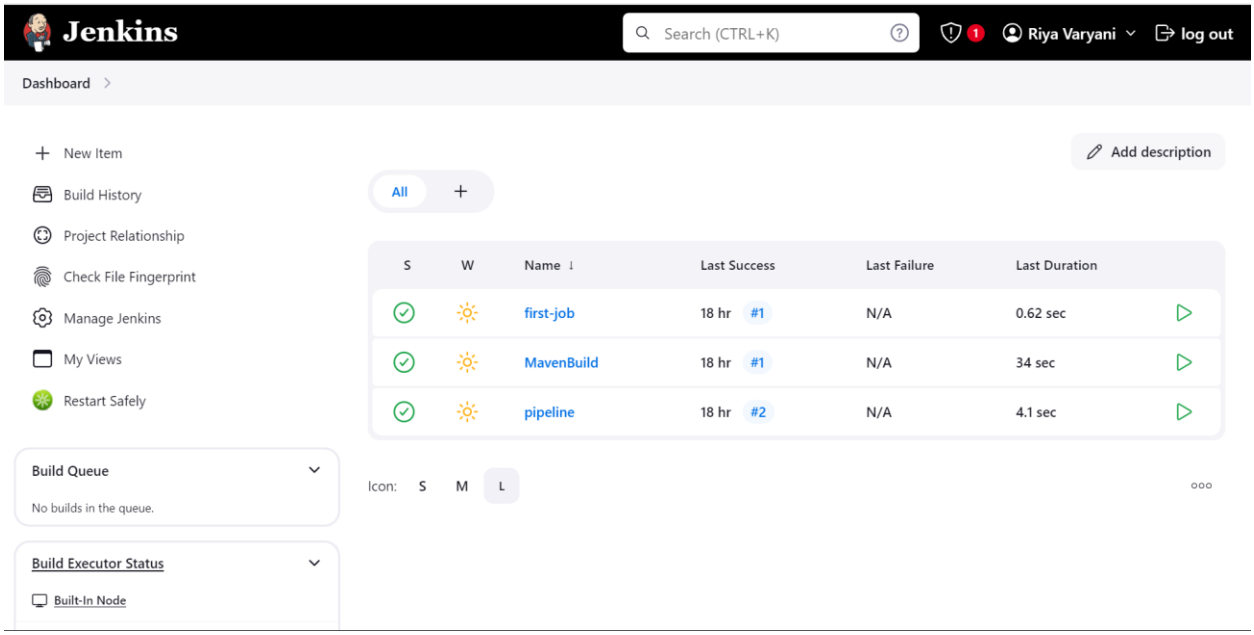
```
C:\Users\varya\TerraformScripts\Docker>docker images
REPOSITORY   TAG       IMAGE ID   CREATED   SIZE
```

ADVANCE DEVOPS EXP-7

RIYA VARYANI **D15A/64**

Aim: To understand Static Analysis SAST process and learn to integrate Jenkins SAST to SonarQube/GitLab.

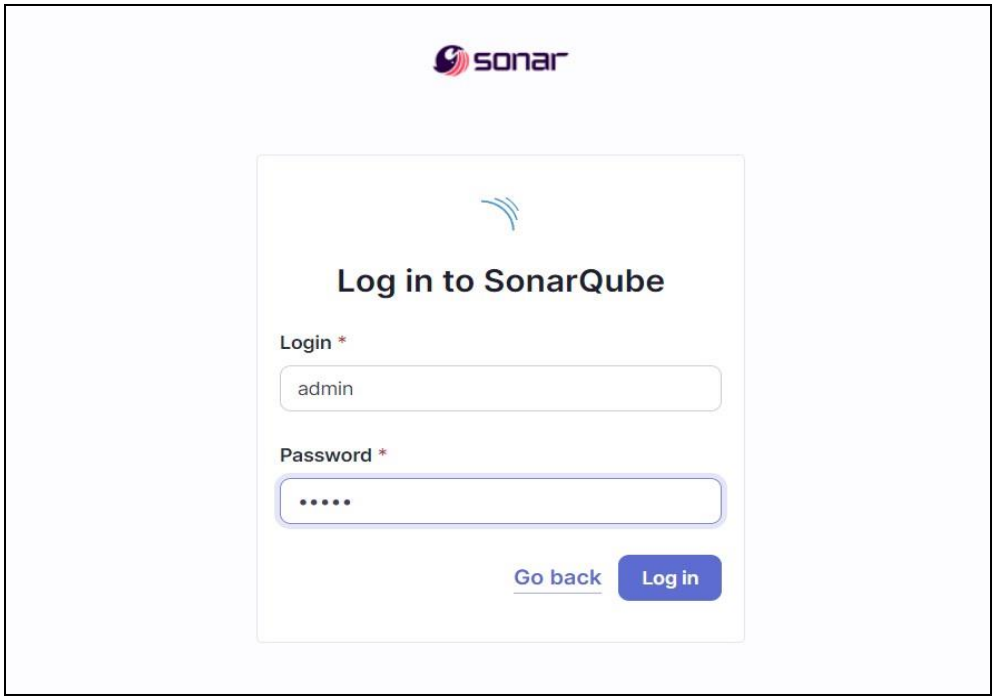
Step-1: Open up Jenkins Dashboard on localhost, port 8080 or whichever port it is at for you.



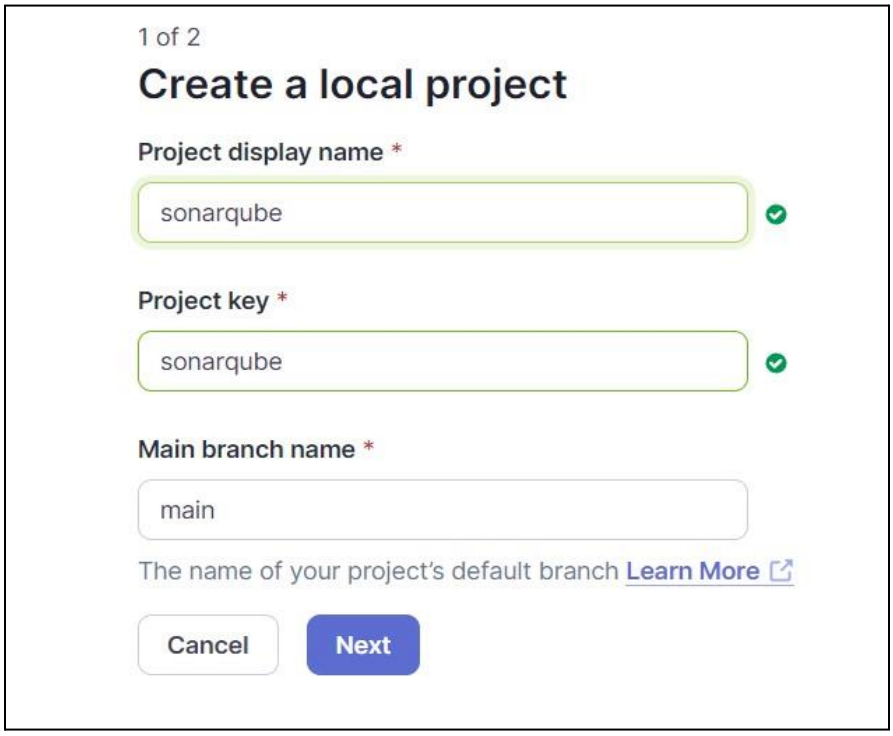
Step-2: Run SonarQube in a Docker container using this command :- a]docker -v b] docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest

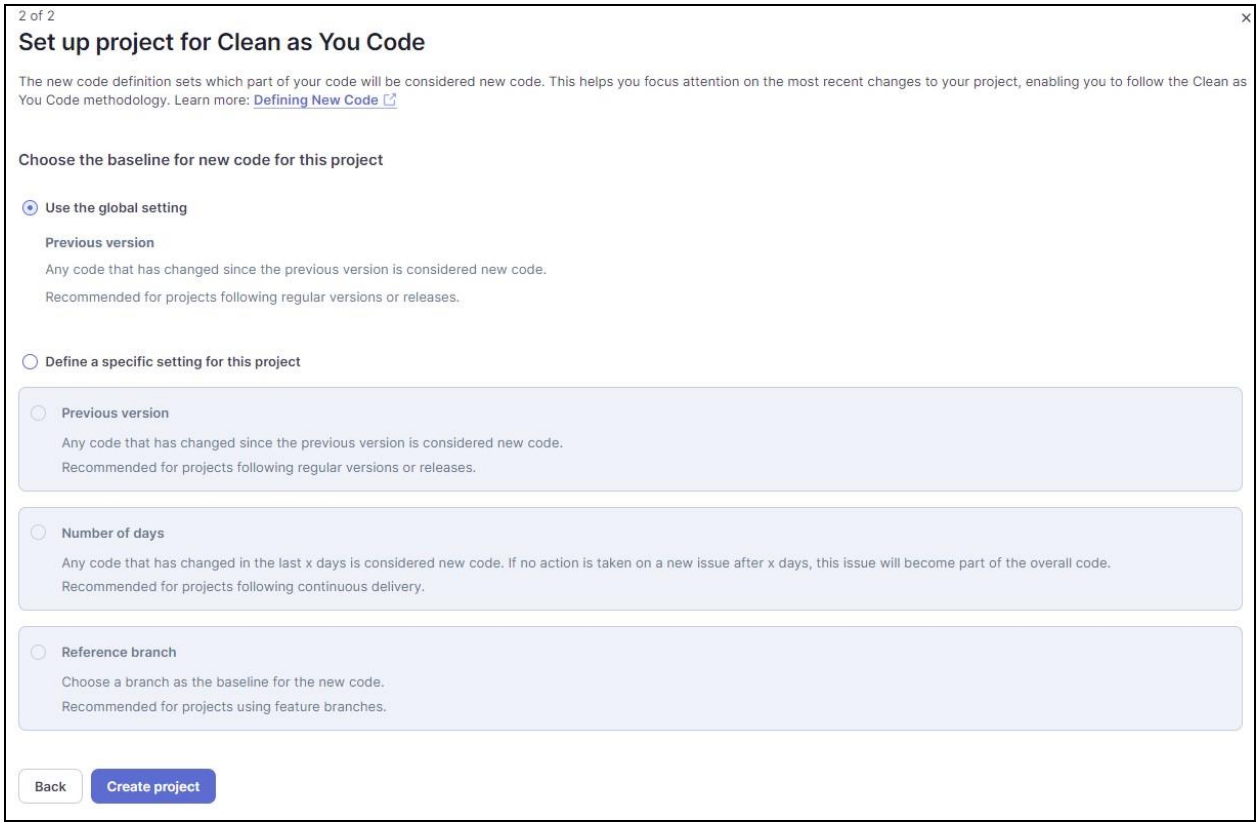
```
C:\Users\varya>docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
7478e0ac0f23: Pull complete
90a925ab929a: Pull complete
7d9a34308537: Pull complete
80338217a4ab: Pull complete
1a5fd5c7e184: Pull complete
7b87d6fa783d: Pull complete
bd819c9b5ead: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Downloaded newer image for sonarqube:latest
b186ed1336af1631917ede88ae9f1d4d688ccd35cc77eb5bfd47b1764967a2c6

C:\Users\varya>
```

Step-3: Once the container is up and running, you can check the status of SonarQube at localhost port 9000. The login id is “admin” and the password is also “admin”.

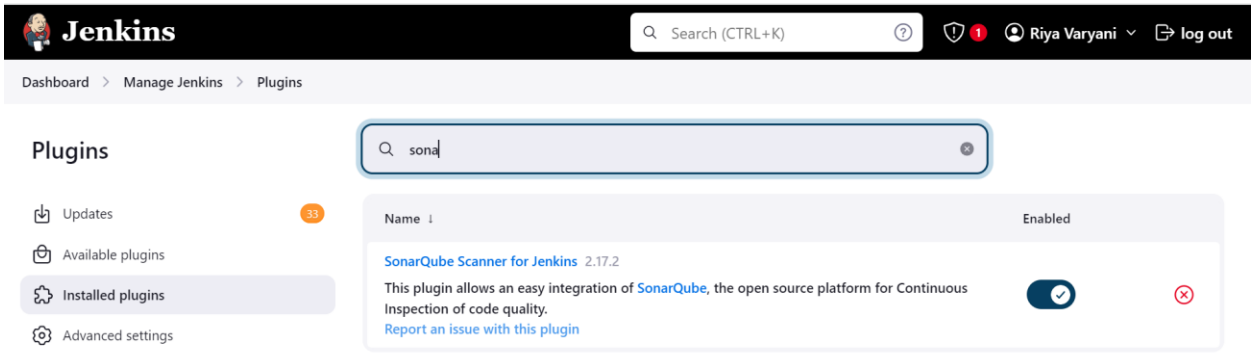


Step-4: Create a local project in SonarQube with the name sonarqube

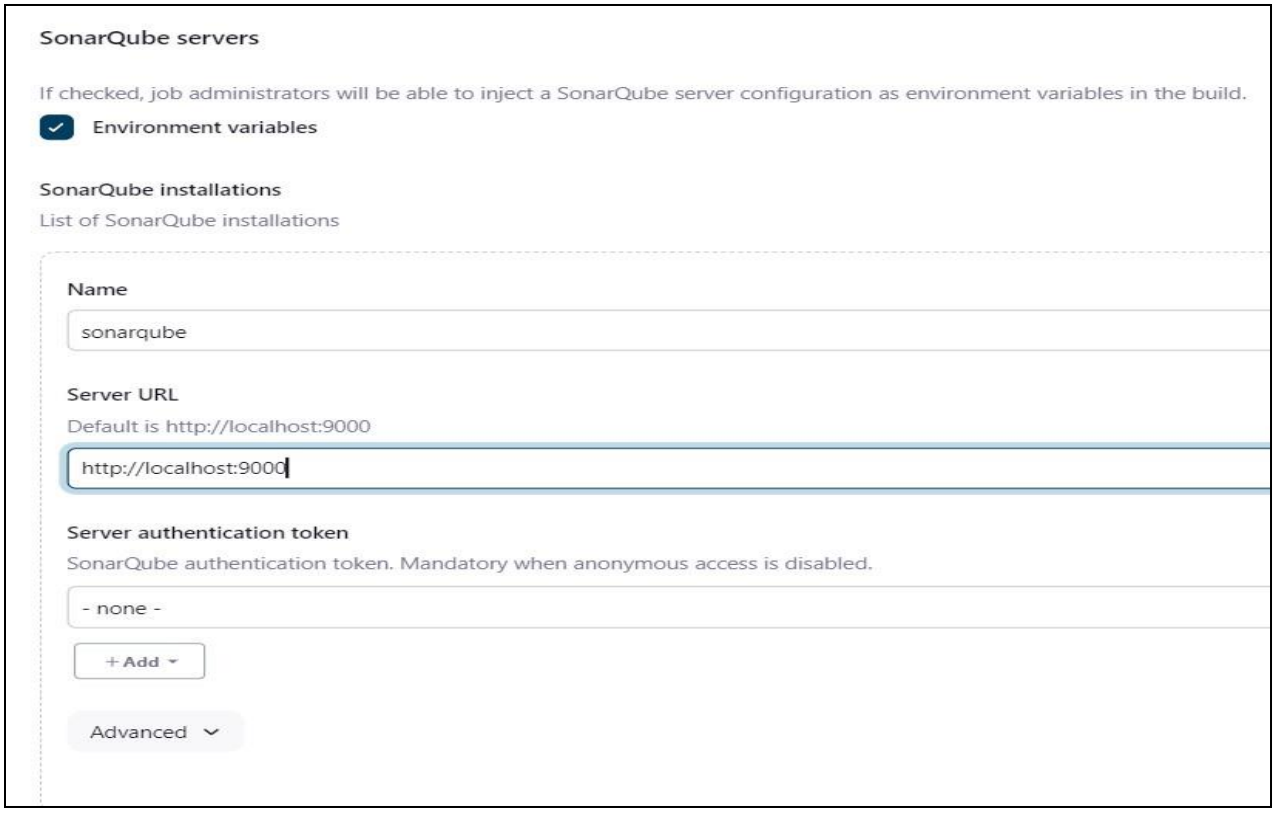




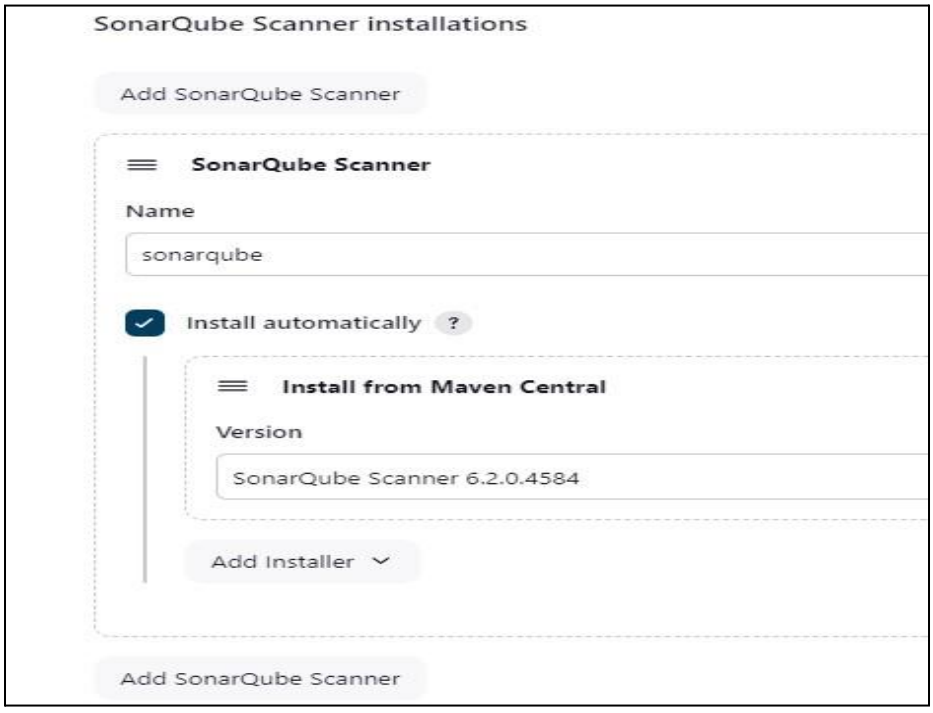
Step-5: Setup the project and come back to Jenkins Dashboard. Go to Manage Jenkins → Plugins and search for SonarQube Scanner in Available Plugins and install it.



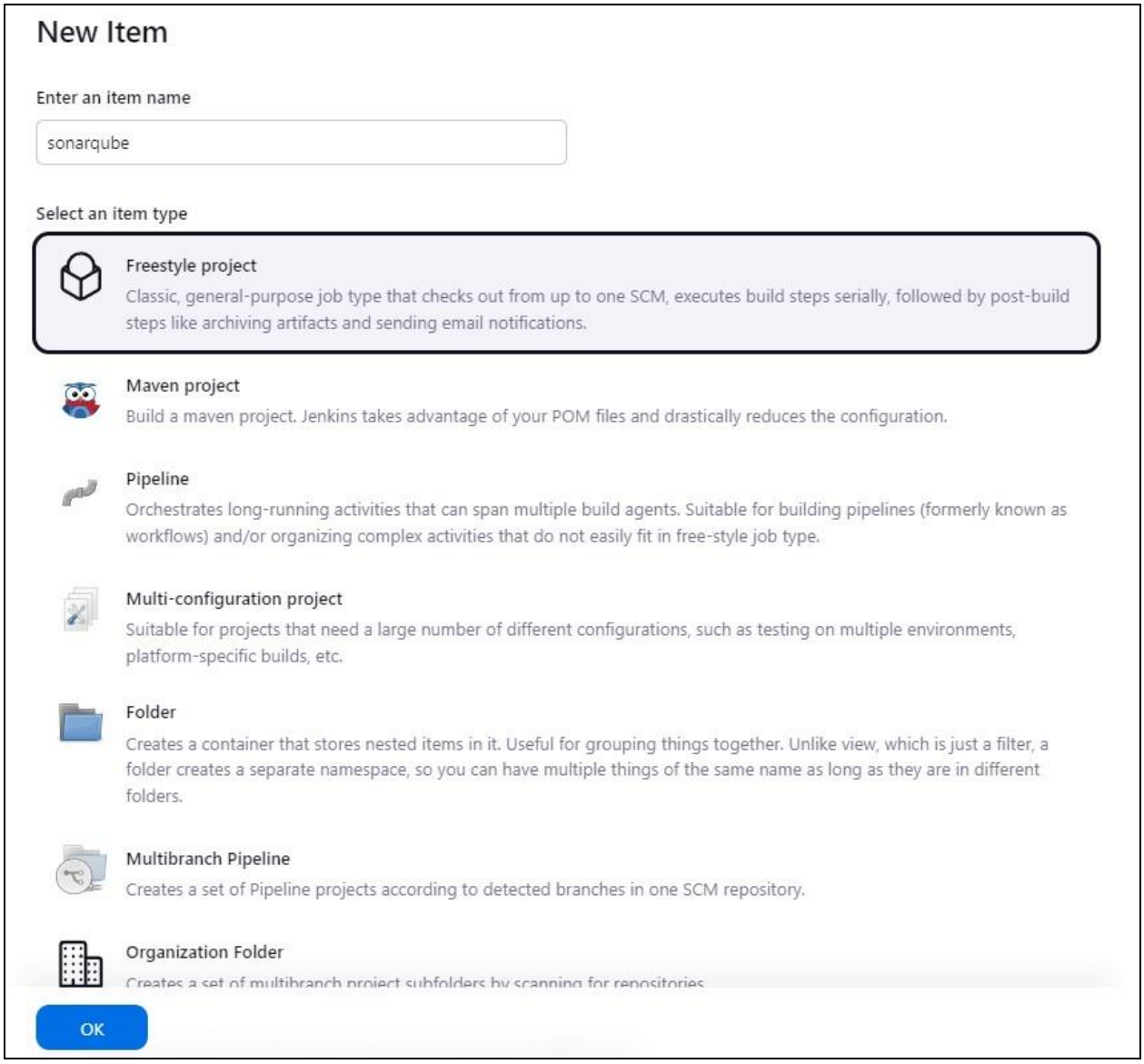
Step-6: Under 'Manage Jenkins → System', look for SonarQube Servers and enter these details. Name : sonarqube, Server URL : http://localhost:9000



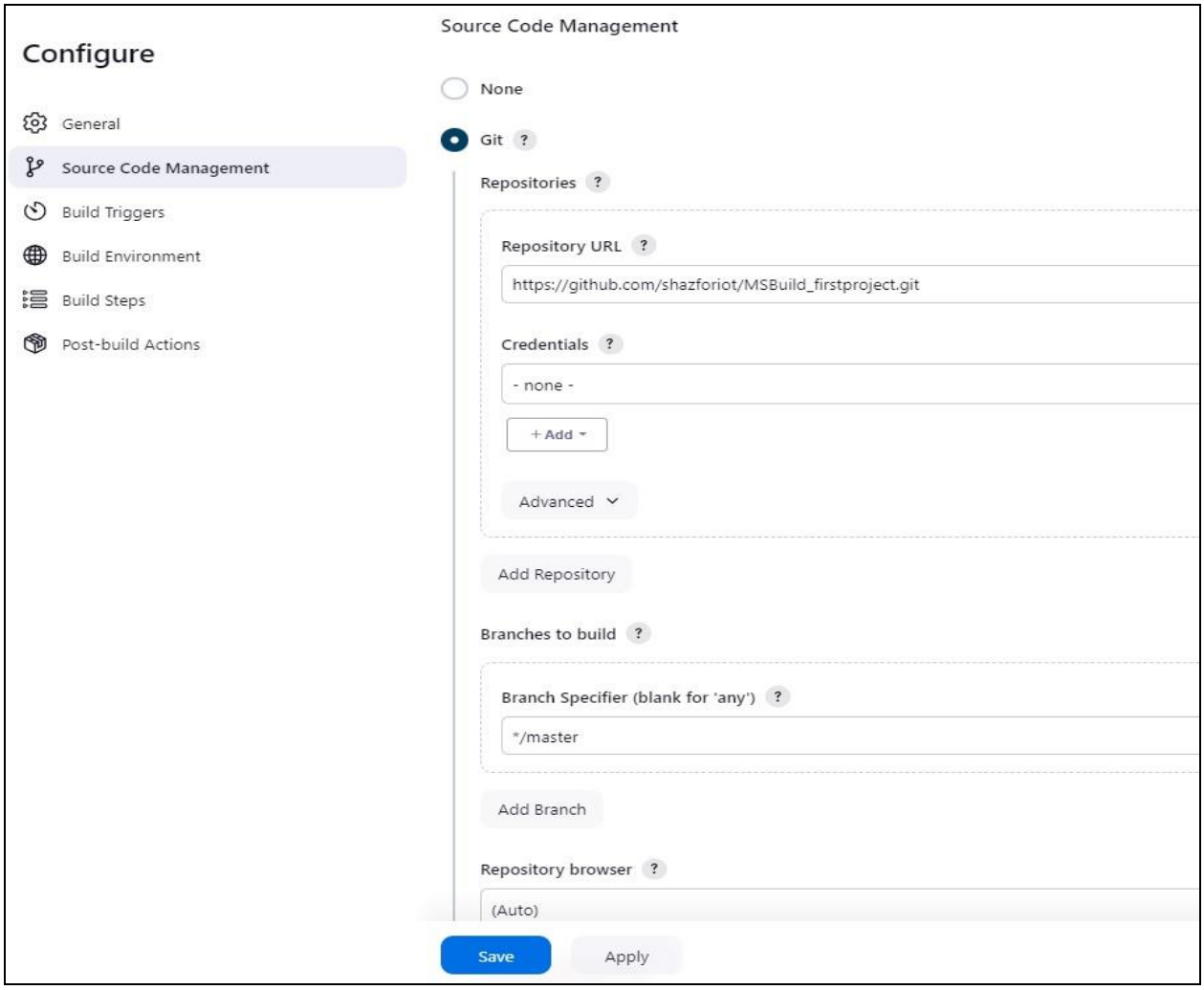
Step-7: Search for SonarQube Scanner under Global Tool Configuration. Choose the latest configuration and choose Install automatically. Manage Jeknins → Tools → SonarQube Scanner Installation.



Step-8: After the configuration, create a New Item in Jenkins, choose a freestyle project named sonarqube.



Step-9: Choose this GitHub repository in Source Code Management. https://github.com/shazforiot/MSBuild_firstproject.git . It is a sample hello-world project with no vulnerabilities and issues, just to test the integration.



Step-10: Under Build-> Execute SonarQube Scanner, enter these Analysis Properties. Mention the SonarQube Project Key, Login, Password, Source path and Host URL.

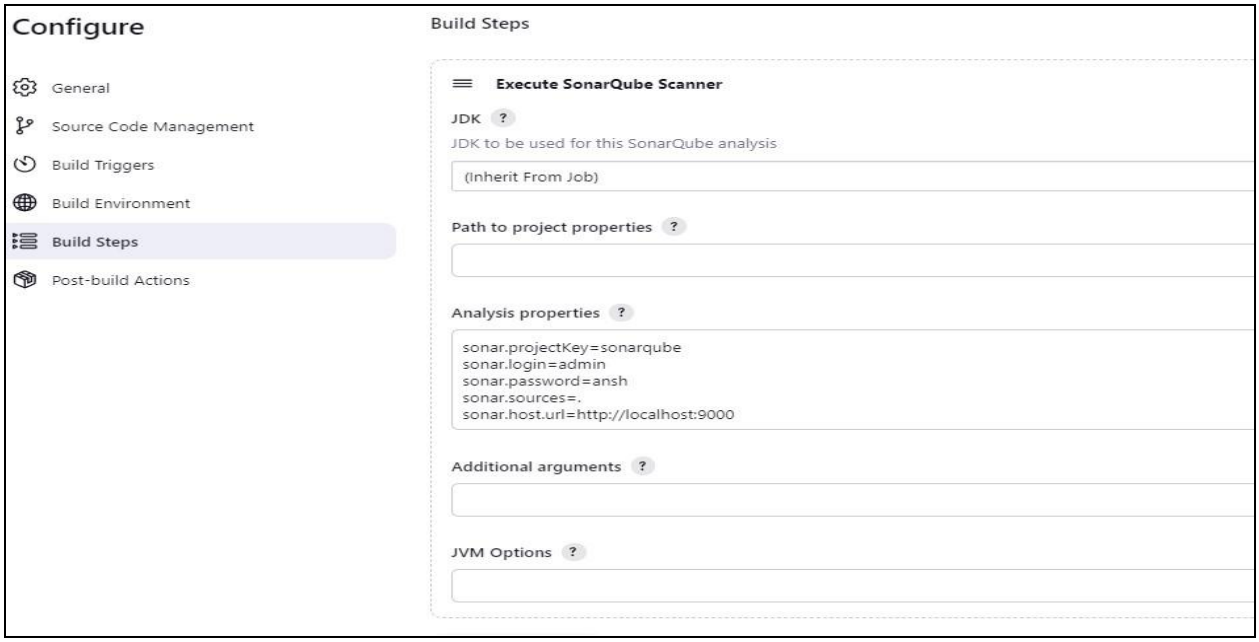
sonar.projectKey=sonarqube

sonar.login=admin

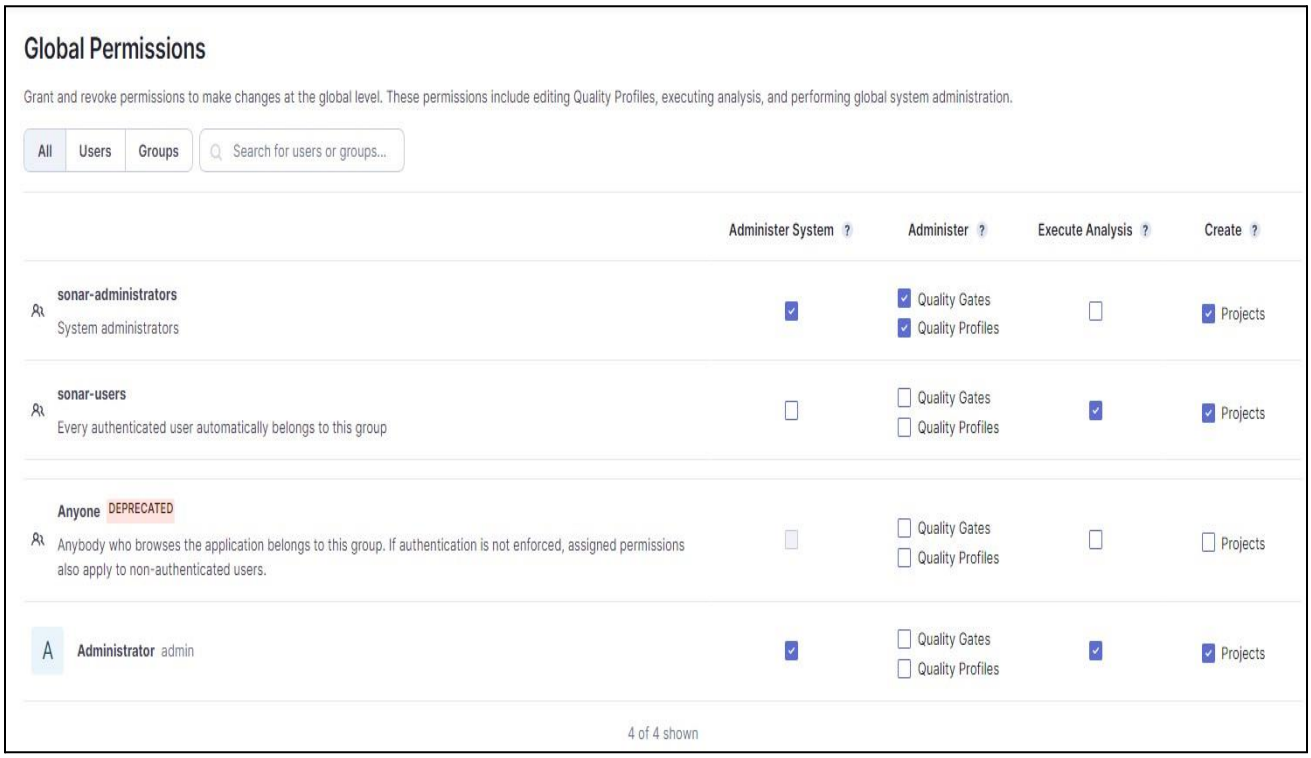
sonar.password=riya 123

sonar.sources=.

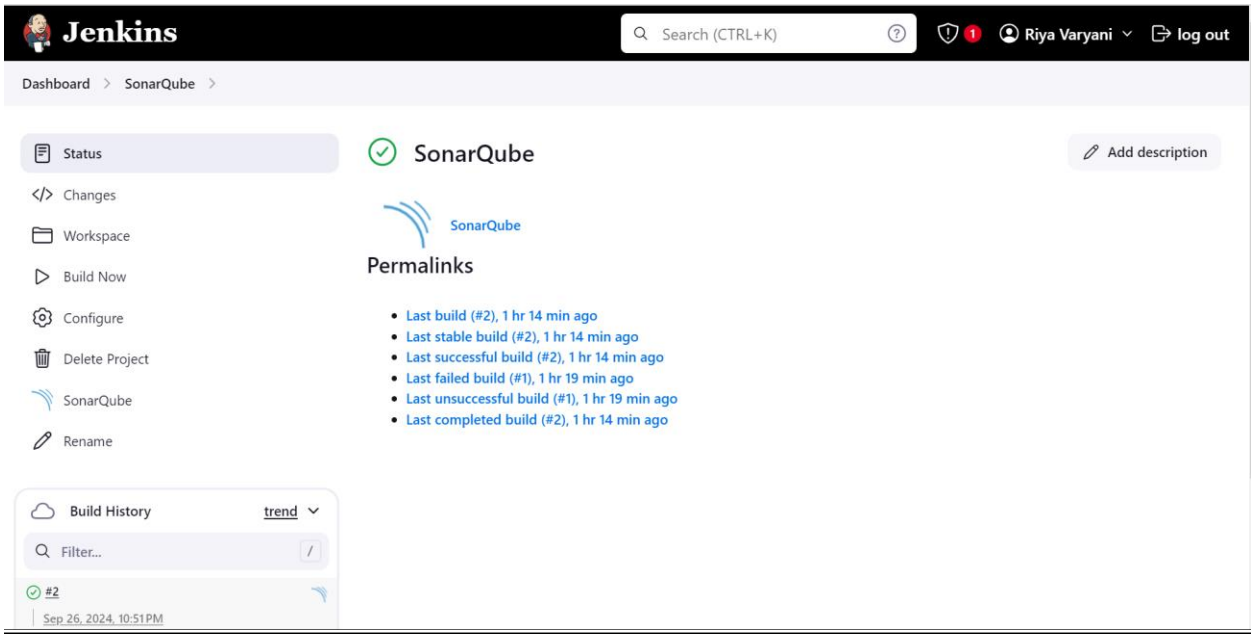
sonar.host.url=http://localhost:9000

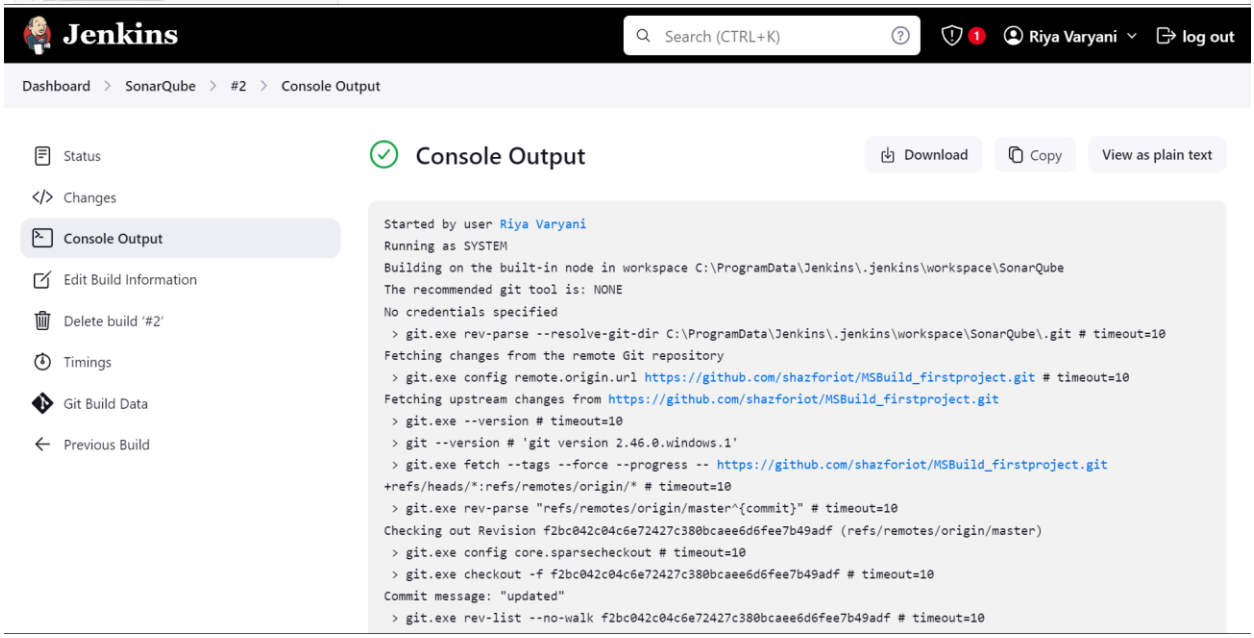


Step-11: Go to http://localhost:9000/admin/permissions and allow Execute Permissions to the Admin user.

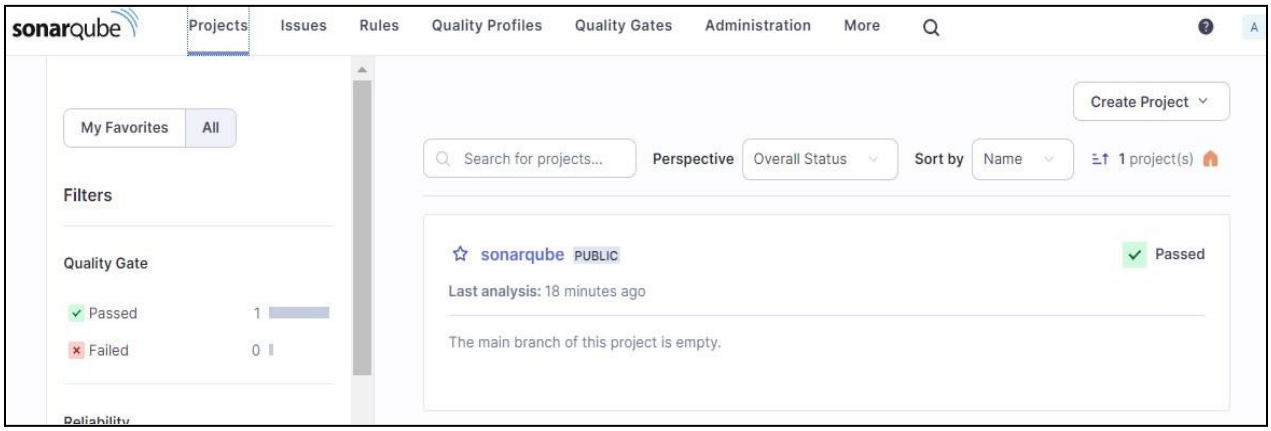


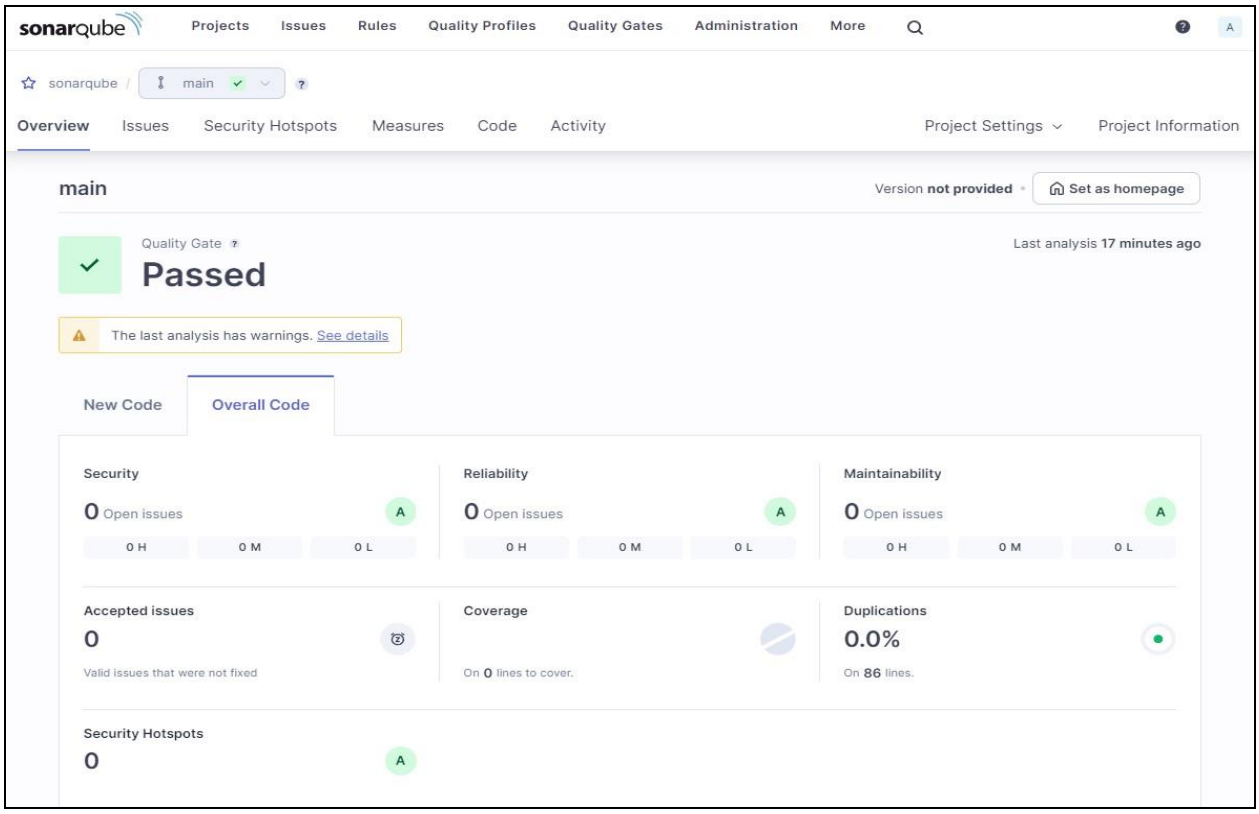
Step-12: Run The Build and check the console output.


Jenkins
Search (CTRL+K)
Riya Varyani
log out
Dashboard > SonarQube >
Status
Changes
Workspace
Build Now
Configure
Delete Project
SonarQube
Rename
SonarQube
Add description
SonarQube
Permalinks
Last build (#2), 1 hr 14 min ago
Last stable build (#2), 1 hr 14 min ago
Last successful build (#2), 1 hr 14 min ago
Last failed build (#1), 1 hr 19 min ago
Last unsuccessful build (#1), 1 hr 19 min ago
Last completed build (#2), 1 hr 14 min ago
Build History
trend
Filter...
#2
Sep 26, 2024, 10:51 PM


Jenkins
Search (CTRL+K)
Riya Varyani
log out
Dashboard > SonarQube > #2 > Console Output
Status
Changes
Console Output
Edit Build Information
Delete build '#2'
Timings
Git Build Data
Previous Build
Console Output
Download
Copy
View as plain text
Started by user Riya Varyani
Running as SYSTEM
Building on the built-in node in workspace C:\ProgramData\Jenkins\.jenkins\workspace\SonarQube
The recommended git tool is: NONE
No credentials specified
> git.exe rev-parse --resolve-git-dir C:\ProgramData\Jenkins\.jenkins\workspace\SonarQube\.git # timeout=10
Fetching changes from the remote Git repository
> git.exe config remote.origin.url https://github.com/shazforiot/MSBuild_firstproject.git # timeout=10
Fetching upstream changes from https://github.com/shazforiot/MSBuild_firstproject.git
> git.exe --version # timeout=10
> git --version # 'git version 2.46.0.windows.1'
> git.exe fetch --tags --force --progress -- https://github.com/shazforiot/MSBuild_firstproject.git
+refs/heads/*:refs/remotes/origin/* # timeout=10
> git.exe rev-parse "refs/remotes/origin/master^{commit}" # timeout=10
Checking out Revision f2bc042c04c6e72427c380bcaee6d6fee7b49adf (refs/remotes/origin/master)
> git.exe config core.sparsecheckout # timeout=10
> git.exe checkout -f f2bc042c04c6e72427c380bcaee6d6fee7b49adf # timeout=10
Commit message: "updated"
> git.exe rev-list --no-walk f2bc042c04c6e72427c380bcaee6d6fee7b49adf # timeout=10

Step-13: Once the build is complete, check the project in SonarQube.



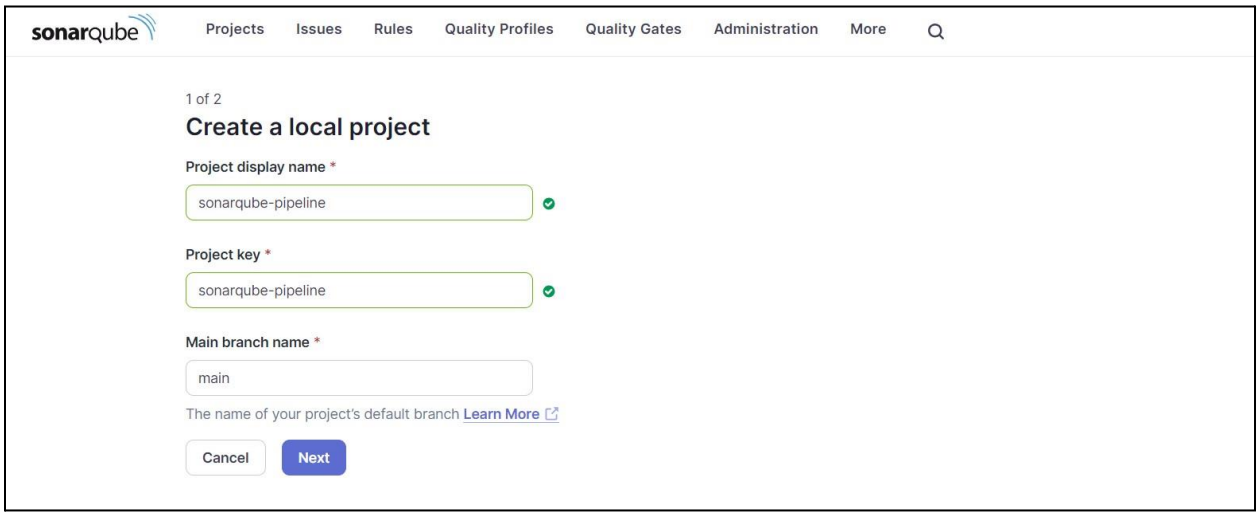

sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
sonarqube / main
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Project Information
main
Version not provided
Set as homepage
Quality Gate
Passed
Last analysis 17 minutes ago
The last analysis has warnings. See details
New Code
Overall Code
Security
0 Open issues
A
0 H
0 M
0 L
Reliability
0 Open issues
A
0 H
0 M
0 L
Maintainability
0 Open issues
A
0 H
0 M
0 L
Accepted issues
0
Valid issues that were not fixed
Coverage
On 0 lines to cover.
Duplications
0.0%
On 86 lines.
Security Hotspots
0
A

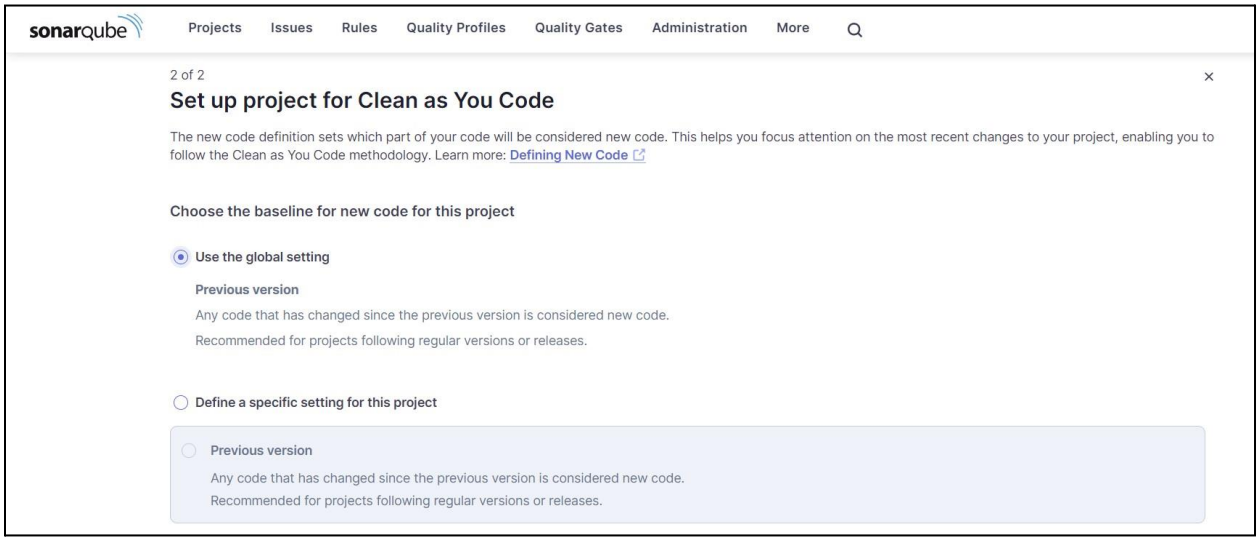
Riya Varyani
D15A Roll: 64

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.

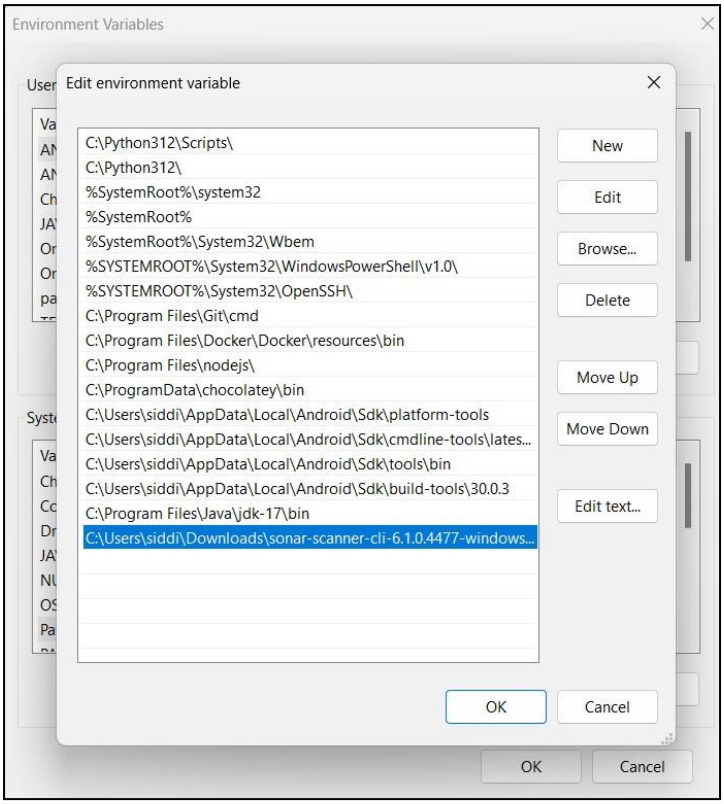
Step 1: Log in to sonarqube portal and create a local project.



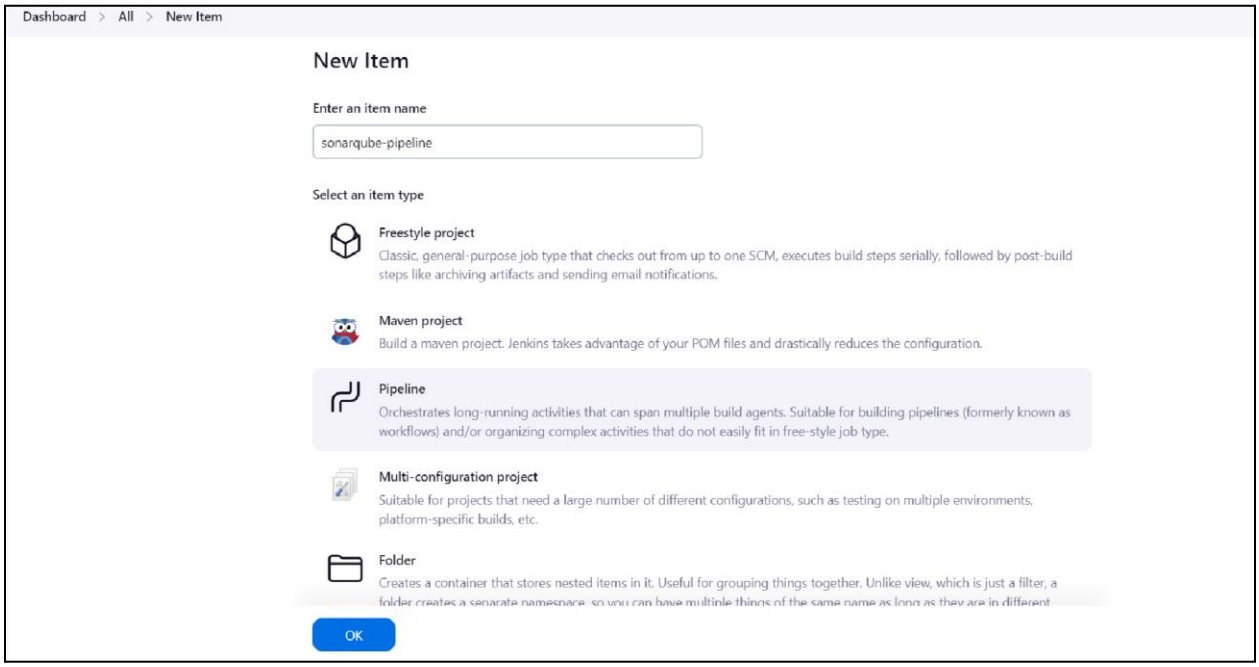


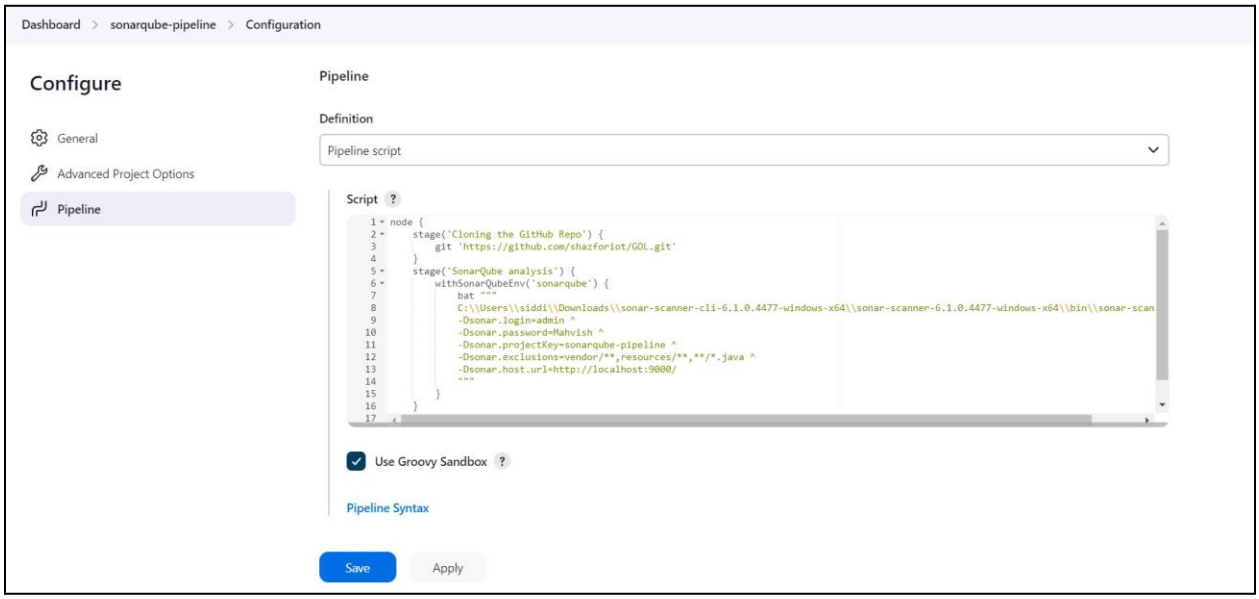
Step 2: Go to download sonarscanner to download sonar scanner

After the download is complete, extract the file and copy the path to bin folder
Go to environment variables, system variables and click on path Add a new path, paste the path copied earlier.

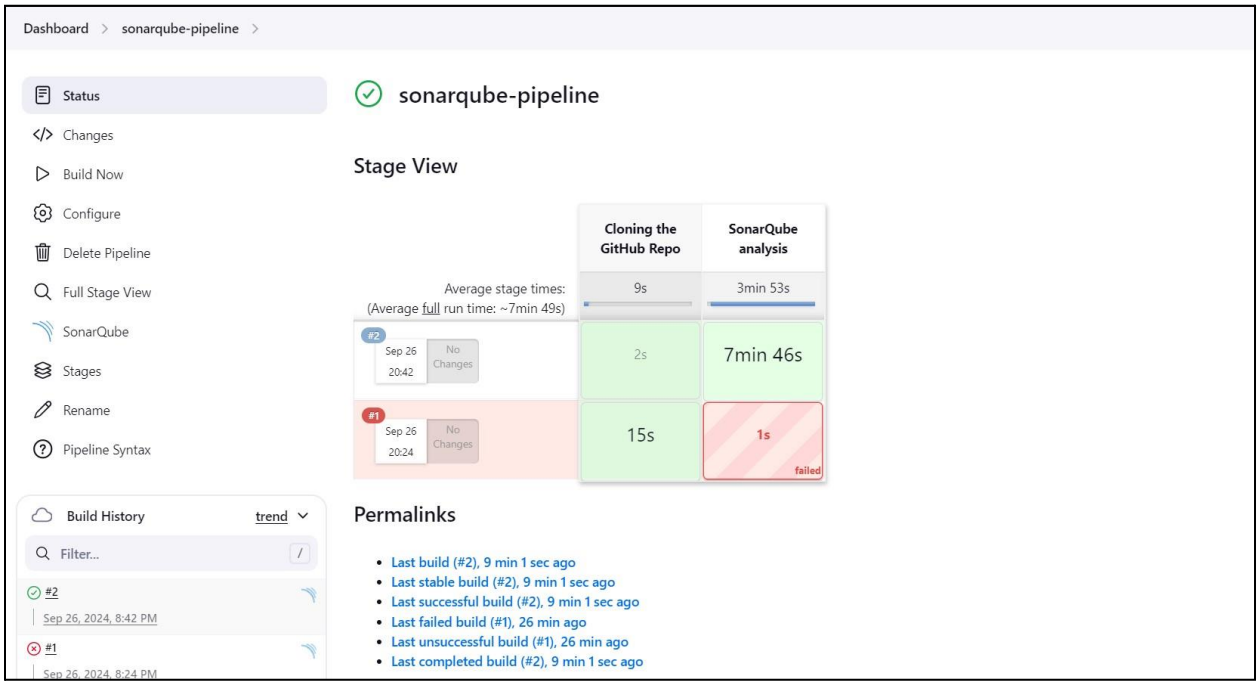


Step 3: Create a New Item in Jenkins, choose Pipeline.

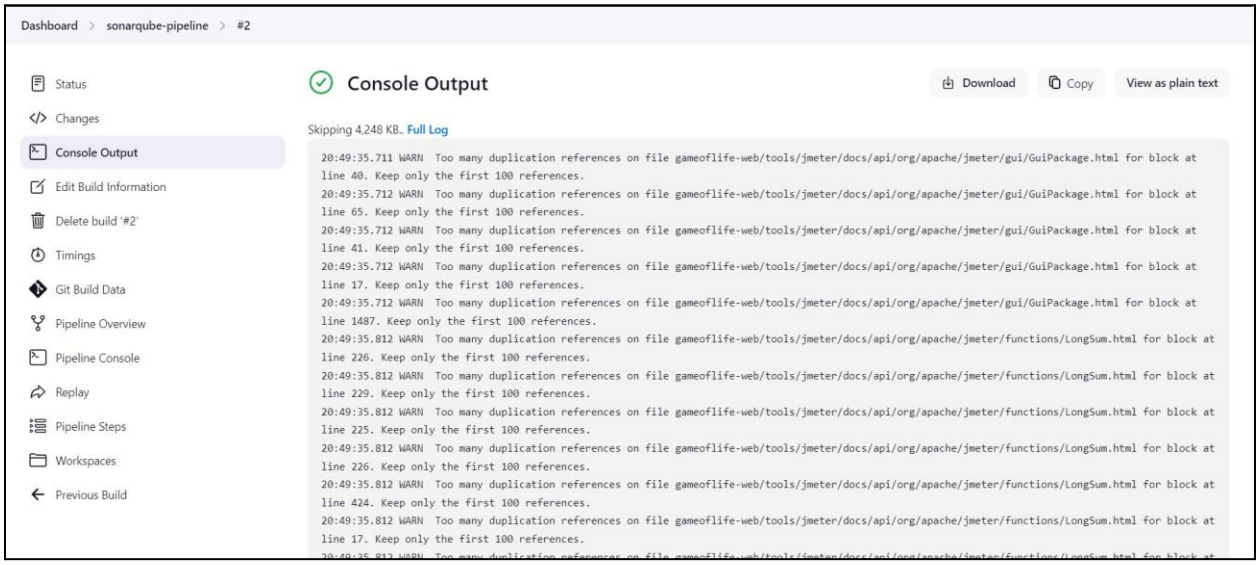




Step 4: Save the pipeline and build it.

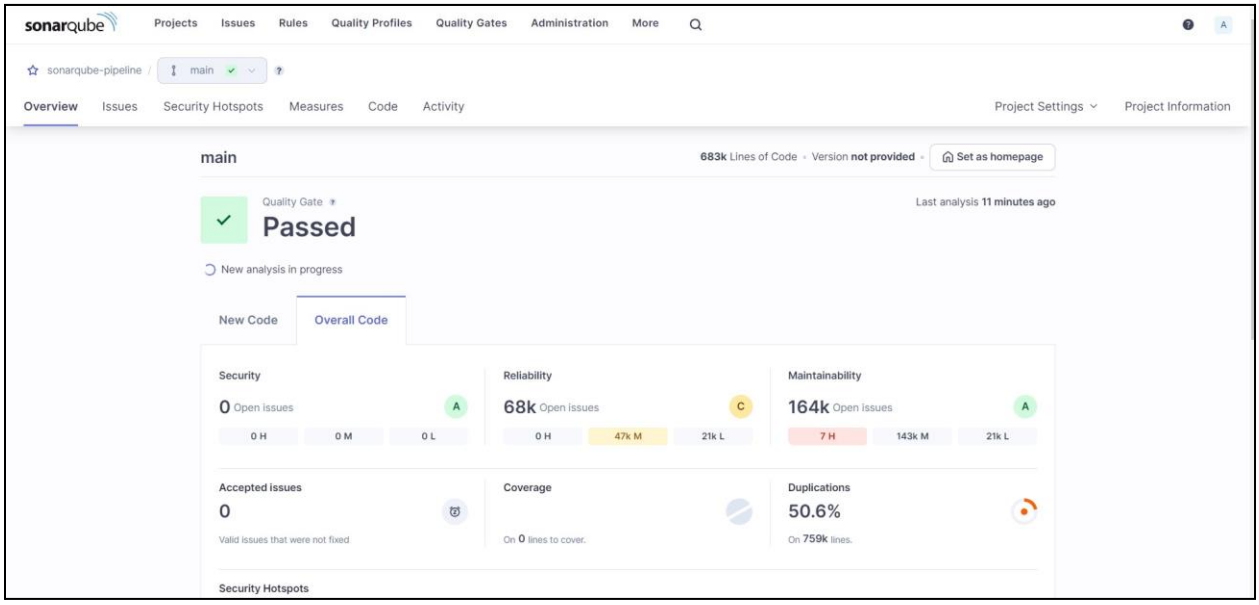


Console output:

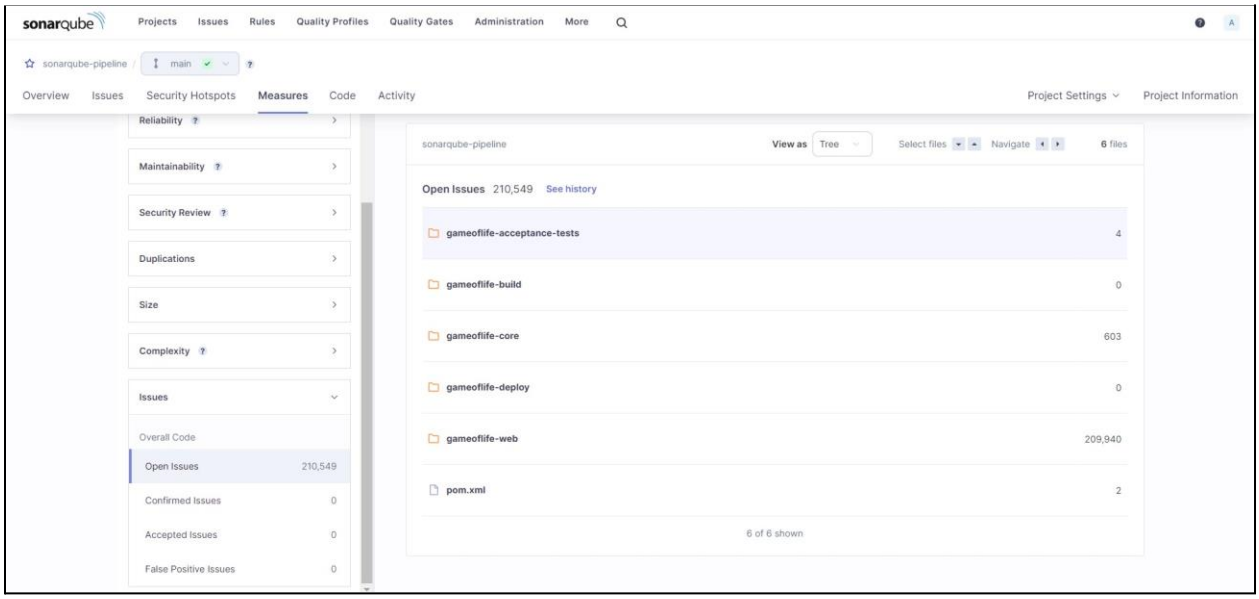


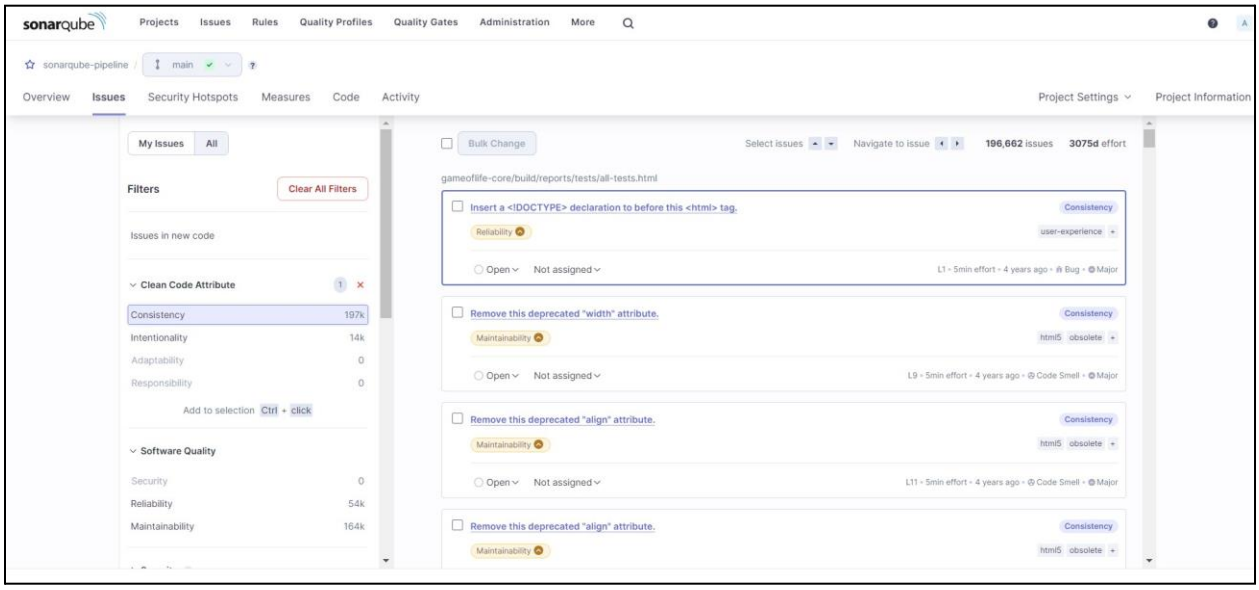
```
20:50:01.832 INFO  ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=sonarqube-pipeline
20:50:01.832 INFO  Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
20:50:01.832 INFO  More about the report processing at http://localhost:9000/api/ce/task?id=159a9d05-1f5f-4e17-bd27-3643a32a836a
20:50:12.108 INFO  Analysis total time: 7:37.235 s
20:50:12.110 INFO  SonarScanner Engine completed successfully
20:50:12.849 INFO  EXECUTION SUCCESS
20:50:12.851 INFO  Total time: 7:44.878s
[Pipeline] }
[Pipeline] // withSonarQubeEnv
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

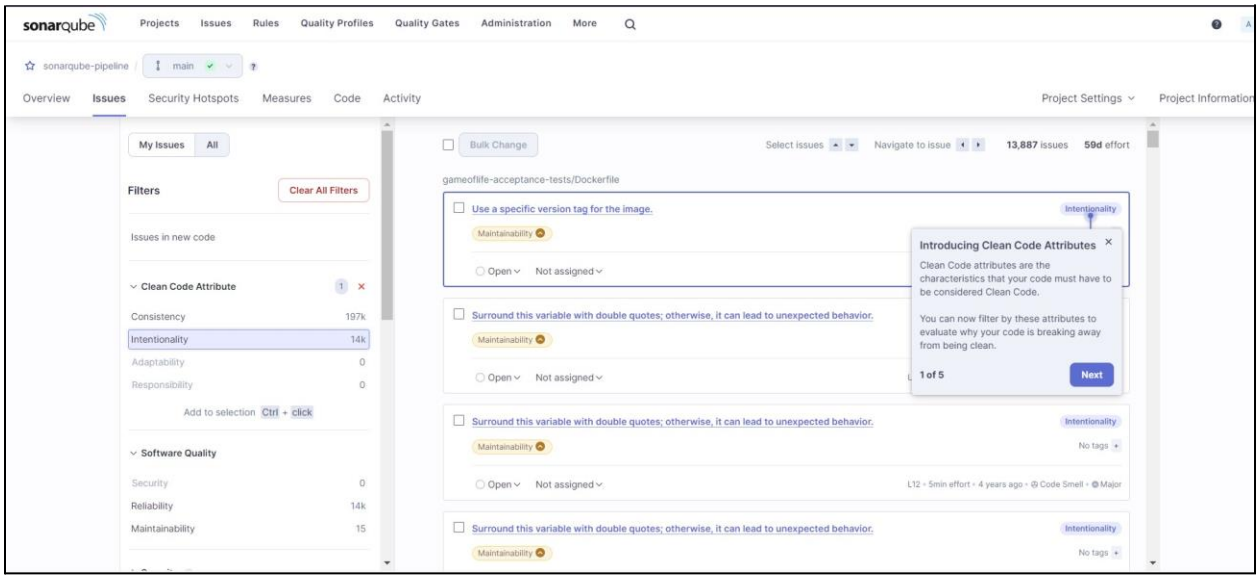
Step 5: After that, check the project in SonarQube

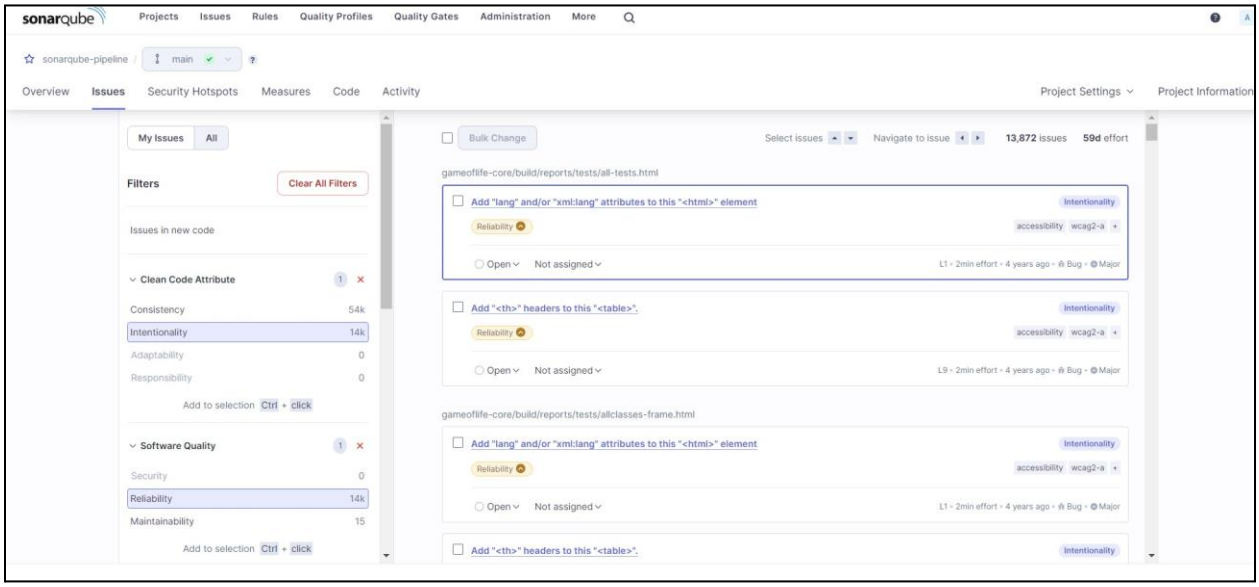


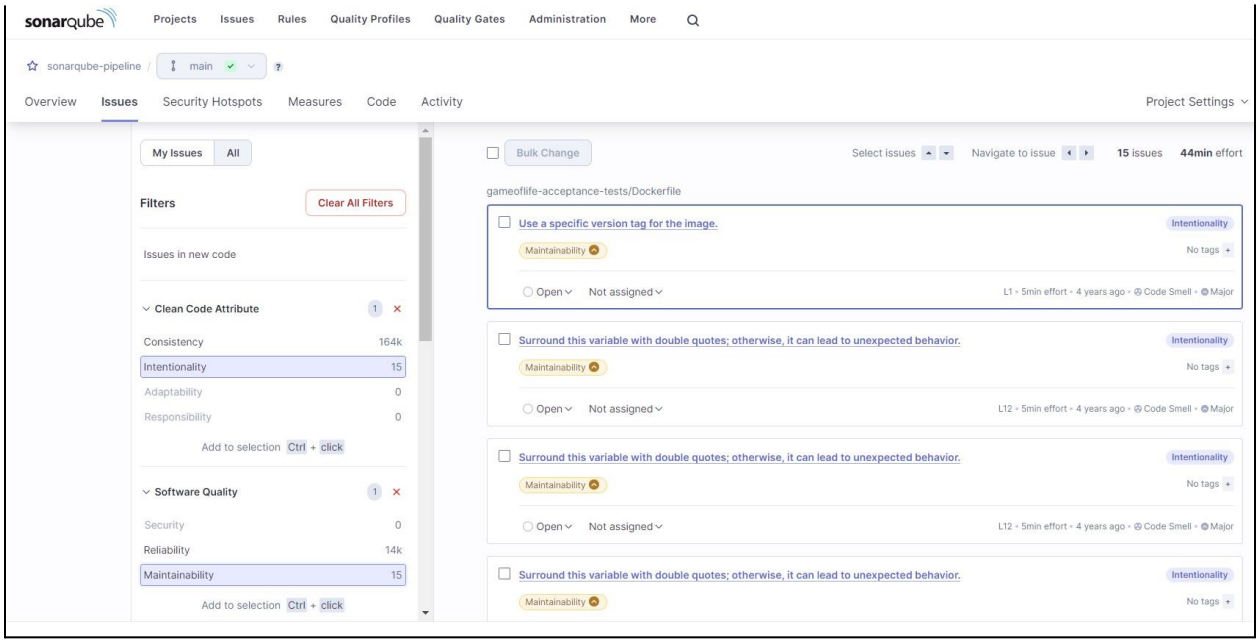
Under different tabs, check all different issues with the code.

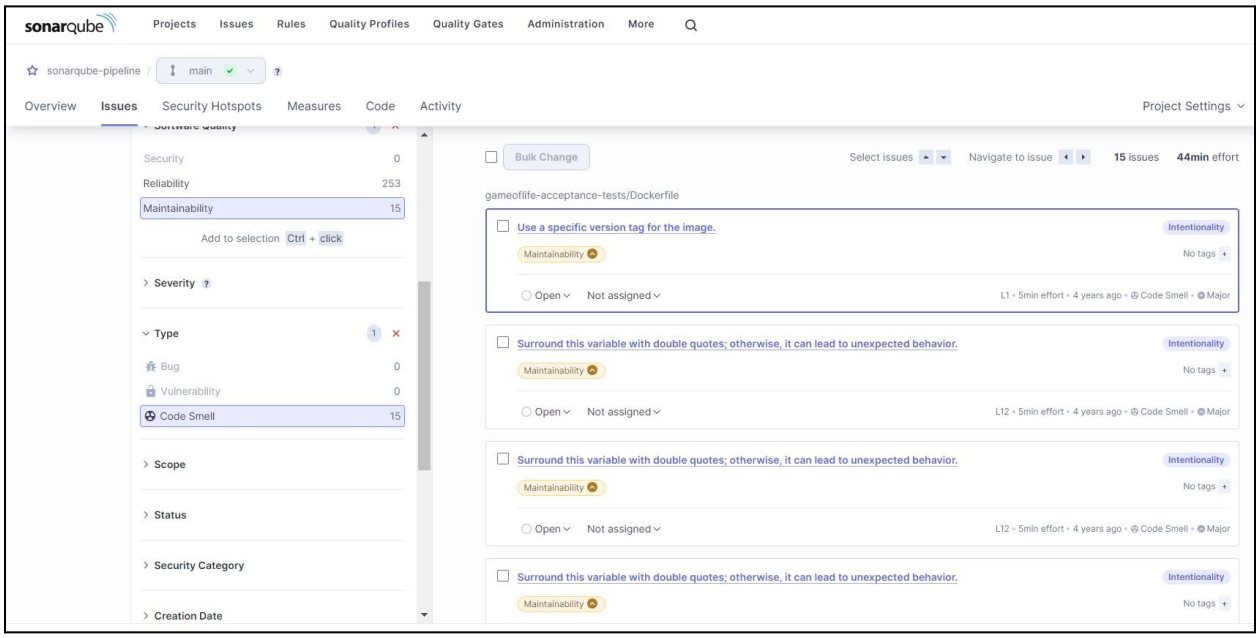

sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
sonarqube-pipeline
main
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Project Information
Reliability
Maintainability
Security Review
Duplications
Size
Complexity
Issues
Overall Code
Open Issues 210,549
Confirmed Issues 0
Accepted Issues 0
False Positive Issues 0
sonarqube-pipeline
View as Tree
Select files
Navigate
6 files
Open Issues 210,549
See history
gameoflife-acceptance-tests 4
gameoflife-build 0
gameoflife-core 603
gameoflife-deploy 0
gameoflife-web 209,940
pom.xml 2
6 of 6 shown

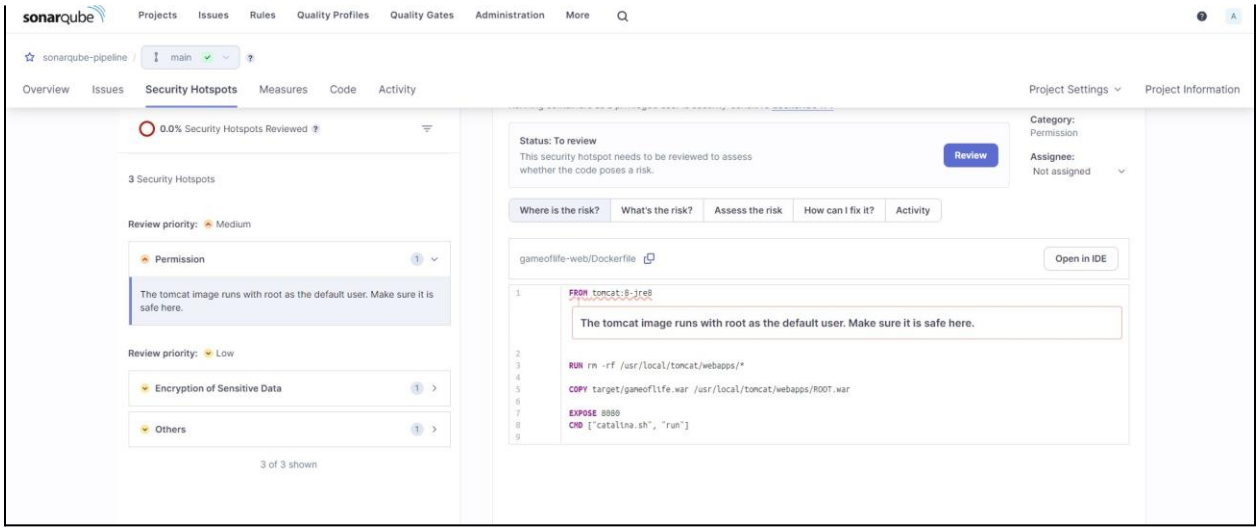

sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
sonarqube-pipeline
main
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Project Information
My Issues
All
Filters
Clear All Filters
Issues in new code
Clean Code Attribute
Consistency 197k
Intentionality 14k
Adaptability 0
Responsibility 0
Add to selection Ctrl + click
Software Quality
Security 0
Reliability 54k
Maintainability 164k
Bulk Change
Select issues
Navigate to issue
196,662 issues
3075d effort
gameoflife-core/build/reports/tests/all-tests.html
Insert a <!DOCTYPE> declaration to before this <html> tag.
Consistency
Reliability
user-experience
Open
Not assigned
L1 · 5min effort · 4 years ago · Bug · Major
Remove this deprecated "width" attribute.
Consistency
Maintainability
html5 obsolete
Open
Not assigned
L9 · 5min effort · 4 years ago · Code Smell · Major
Remove this deprecated "align" attribute.
Consistency
Maintainability
html5 obsolete
Open
Not assigned
L11 · 5min effort · 4 years ago · Code Smell · Major
Remove this deprecated "align" attribute.
Consistency
Maintainability
html5 obsolete

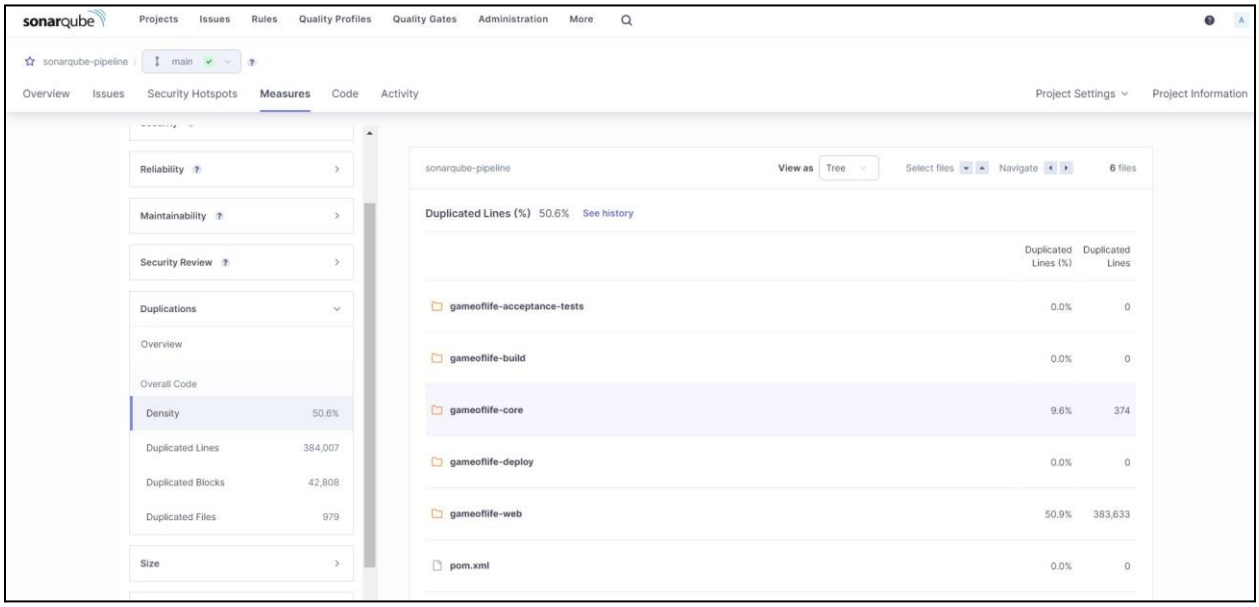

sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
sonarqube-pipeline
main
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Project Information
My Issues
All
Filters
Clear All Filters
Issues in new code
Clean Code Attribute
Consistency 197k
Intentionality 14k
Adaptability 0
Responsibility 0
Add to selection Ctrl + click
Software Quality
Security 0
Reliability 14k
Maintainability 15
Bulk Change
Select issues
Navigate to issue
13,887 issues
59d effort
gameoflife-acceptance-tests/Dockerfile
Use a specific version tag for the image.
Intentionality
Maintainability
Open
Not assigned
Introducing Clean Code Attributes
Clean Code attributes are the characteristics that your code must have to be considered Clean Code.
You can now filter by these attributes to evaluate why your code is breaking away from being clean.
1 of 5
Next
Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.
No tags
L12 • 5min effort • 4 years ago • Code Smell • Major

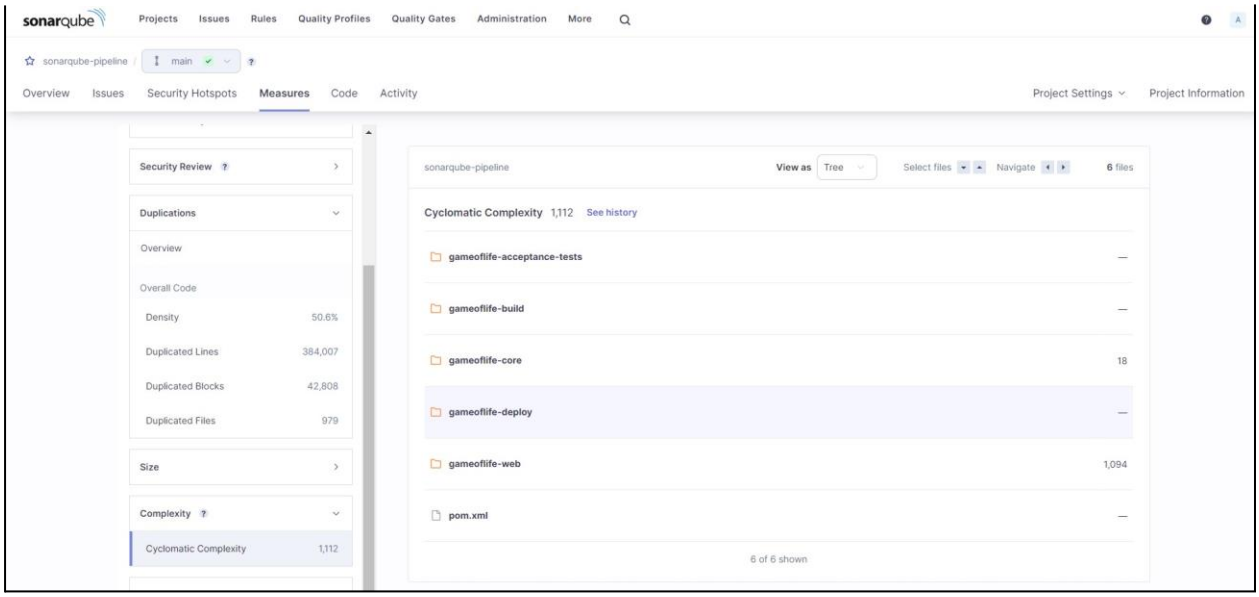

sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
sonarqube-pipeline
main
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Project Information
My Issues
All
Filters
Clear All Filters
Issues in new code
Clean Code Attribute
Consistency 54k
Intentionality 14k
Adaptability 0
Responsibility 0
Add to selection Ctrl + click
Software Quality
Security 0
Reliability 14k
Maintainability 15
Bulk Change
Select issues
Navigate to issue
13,872 issues
59d effort
gameoflife-core/build/reports/tests/all-tests.html
Add "lang" and/or "xml:lang" attributes to this "<html>" element
Intentionality
Reliability
accessibility wcag2-a
Open
Not assigned
L1 • 2min effort • 4 years ago • Bug • Major
Add "<th>" headers to this "<table>".
L9 • 2min effort • 4 years ago • Bug • Major
gameoflife-core/build/reports/tests/allclasses-frame.html


sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
sonarqube-pipeline
main
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
My Issues
All
Filters
Clear All Filters
Issues in new code
Clean Code Attribute
Consistency 164k
Intentionality 15
Adaptability 0
Responsibility 0
Add to selection Ctrl + click
Software Quality
Security 0
Reliability 14k
Maintainability 15
Add to selection Ctrl + click
Bulk Change
Select issues
Navigate to issue
15 issues
44min effort
gameoflife-acceptance-tests/Dockerfile
Use a specific version tag for the image.
Intentionality
Maintainability
No tags
Open
Not assigned
L1 • 5min effort • 4 years ago • Code Smell • Major
Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.
Intentionality
Maintainability
No tags
Open
Not assigned
L12 • 5min effort • 4 years ago • Code Smell • Major
Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.
Intentionality
Maintainability
No tags
Open
Not assigned
L12 • 5min effort • 4 years ago • Code Smell • Major
Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.
Intentionality
Maintainability
No tags


sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
sonarqube-pipeline
main
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Security 0
Reliability 253
Maintainability 15
Add to selection Ctrl + click
Severity
Type
Bug 0
Vulnerability 0
Code Smell 15
Scope
Status
Security Category
Creation Date
Bulk Change
Select issues
Navigate to issue
15 issues
44min effort
gameoflife-acceptance-tests/Dockerfile
Use a specific version tag for the image.
Intentionality
Maintainability
No tags
Open
Not assigned
L1 • 5min effort • 4 years ago • Code Smell • Major
Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.
Intentionality
Maintainability
No tags
Open
Not assigned
L12 • 5min effort • 4 years ago • Code Smell • Major
Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.
Intentionality
Maintainability
No tags
Open
Not assigned
L12 • 5min effort • 4 years ago • Code Smell • Major
Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.
Intentionality
Maintainability
No tags


sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
sonarqube-pipeline
main
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Project Information
0.0% Security Hotspots Reviewed
3 Security Hotspots
Review priority: Medium
Permission
The tomcat image runs with root as the default user. Make sure it is safe here.
Review priority: Low
Encryption of Sensitive Data
Others
3 of 3 shown
Status: To review
This security hotspot needs to be reviewed to assess whether the code poses a risk.
Review
Category:
Permission
Assignee:
Not assigned
Where is the risk?
What's the risk?
Assess the risk
How can I fix it?
Activity
gameoflife-web/Dockerfile
Open in IDE
FROM tomcat:8-jre8
The tomcat image runs with root as the default user. Make sure it is safe here.
RUN rm -rf /usr/local/tomcat/webapps/*
COPY target/gameoflife.war /usr/local/tomcat/webapps/ROOT.war
EXPOSE 8080
CMD ["catalina.sh", "run"]


sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
sonarqube-pipeline
main
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Project Information
Reliability
Maintainability
Security Review
Duplications
Overview
Overall Code
Density 50.6%
Duplicated Lines 384,007
Duplicated Blocks 42,808
Duplicated Files 979
Size
sonarqube-pipeline
View as Tree
Select files
Navigate
6 files
Duplicated Lines (%) 50.6%
See history
Duplicated Lines (%)
Duplicated Lines
gameoflife-acceptance-tests 0.0% 0
gameoflife-build 0.0% 0
gameoflife-core 9.6% 374
gameoflife-deploy 0.0% 0
gameoflife-web 50.9% 383,633
pom.xml 0.0% 0

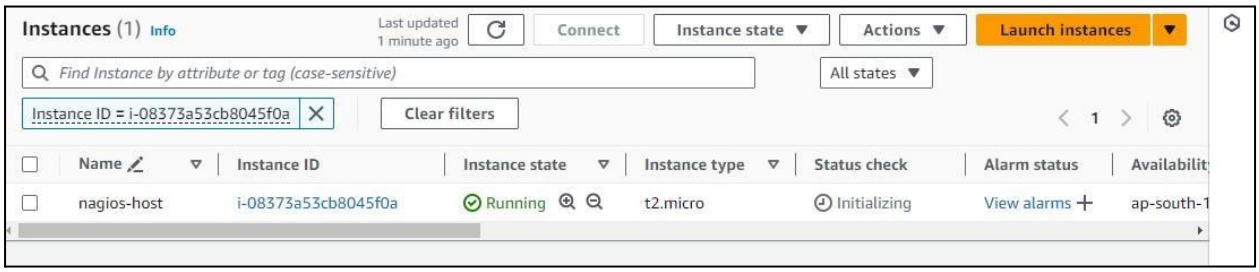

sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
sonarqube-pipeline
main
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Project Information
Security Review
Duplications
Overview
Overall Code
Density 50.6%
Duplicated Lines 384,007
Duplicated Blocks 42,808
Duplicated Files 979
Size
Complexity
Cyclomatic Complexity 1,112
sonarqube-pipeline
View as Tree
Select files
Navigate
6 files
Cyclomatic Complexity 1,112 See history
gameoflife-acceptance-tests —
gameoflife-build —
gameoflife-core 18
gameoflife-deploy —
gameoflife-web 1,094
pom.xml —
6 of 6 shown

ADVANCE DEVOPS EXPERIMENT 9

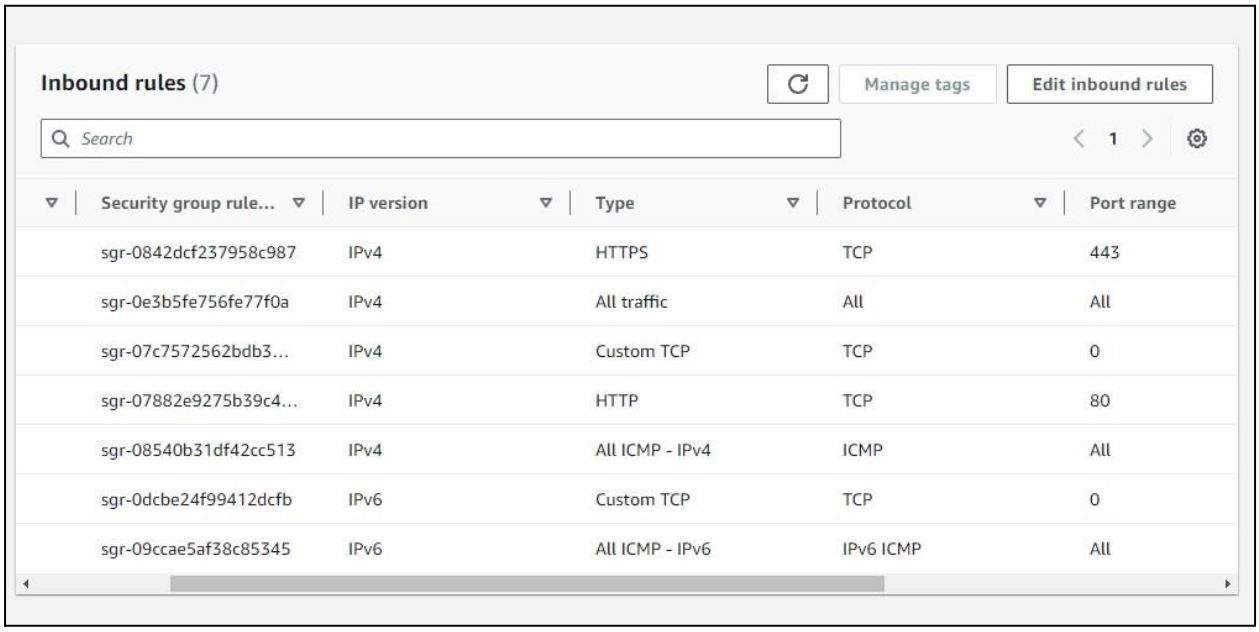
Name:Riya Varyani
Class:D15A
Roll No:64

Aim:To Understand Continuous monitoring and Installation and configuration of Nagios Core, Nagios Plugins and NRPE (Nagios Remote Plugin Executor) on Linux Machine

Step 1: Create an Amazon Linux EC2 instance and name it as nagios-host



Step 2: Edit the following inbound rules of the specified security groups and ensure HTTP.HTTPS,SSH,ICMP are accessible from anywhere



Step 3:Connect to your EC2 instance via the connect option available in EC2 instances menu

```
[ec2-user@ip-172-31-33-14 ~]$ sudo yum install httpd php
Last metadata expiration check: 0:19:23 ago on Thu Sep 26 08:42:17 2024.
Dependencies resolved.
```

Package	Architecture	Version	Repository	Size
Installing:				
httpd	x86_64	2.4.62-1.amzn2023	amazonlinux	48 k
php8.3	x86_64	8.3.10-1.amzn2023.0.1	amazonlinux	10 k
Installing dependencies:				
apr	x86_64	1.7.2-2.amzn2023.0.2	amazonlinux	129 k
apr-util	x86_64	1.6.3-1.amzn2023.0.1	amazonlinux	98 k
generic-logos-httpd	noarch	18.0.0-12.amzn2023.0.3	amazonlinux	19 k
httpd-core	x86_64	2.4.62-1.amzn2023	amazonlinux	1.4 M
httpd-filesystem	noarch	2.4.62-1.amzn2023	amazonlinux	14 k
httpd-tools	x86_64	2.4.62-1.amzn2023	amazonlinux	81 k
libbrotli	x86_64	1.0.9-4.amzn2023.0.2	amazonlinux	315 k
libsodium	x86_64	1.0.19-4.amzn2023	amazonlinux	176 k
libxslt	x86_64	1.1.34-5.amzn2023.0.2	amazonlinux	241 k
mailcap	noarch	2.1.49-3.amzn2023.0.3	amazonlinux	33 k

Step 4: Update and install the required packages Use the following commands: **sudo yum update sudo yum install httpd php sudo yum install gcc glibc glibc-common sudo yum install gd gd-devel**

```
[ec2-user@ip-172-31-33-14 ~]$ sudo yum install gcc glibc glibc-common
Last metadata expiration check: 0:20:32 ago on Thu Sep 26 08:42:17 2024.
Package glibc-2.34-52.amzn2023.0.11.x86_64 is already installed.
Package glibc-common-2.34-52.amzn2023.0.11.x86_64 is already installed.
Dependencies resolved.
```

Package	Architecture	Version	Repository	Size
Installing:				
gcc	x86_64	11.4.1-2.amzn2023.0.2	amazonlinux	32 M
Installing dependencies:				
annobin-docs	noarch	10.93-1.amzn2023.0.1	amazonlinux	92 k
annobin-plugin-gcc	x86_64	10.93-1.amzn2023.0.1	amazonlinux	887 k
cpp	x86_64	11.4.1-2.amzn2023.0.2	amazonlinux	10 M
gc	x86_64	8.0.4-5.amzn2023.0.2	amazonlinux	105 k
glibc-devel	x86_64	2.34-52.amzn2023.0.11	amazonlinux	27 k
glibc-headers-x86	noarch	2.34-52.amzn2023.0.11	amazonlinux	427 k
guile22	x86_64	2.2.7-2.amzn2023.0.3	amazonlinux	6.4 M
kernel-headers	x86_64	6.1.109-118.189.amzn2023	amazonlinux	1.4 M
libmpc	x86_64	1.2.1-2.amzn2023.0.2	amazonlinux	62 k
libtool-ltdl	x86_64	2.4.7-1.amzn2023.0.3	amazonlinux	38 k
libxcrypt-devel	x86_64	4.4.33-7.amzn2023	amazonlinux	32 k

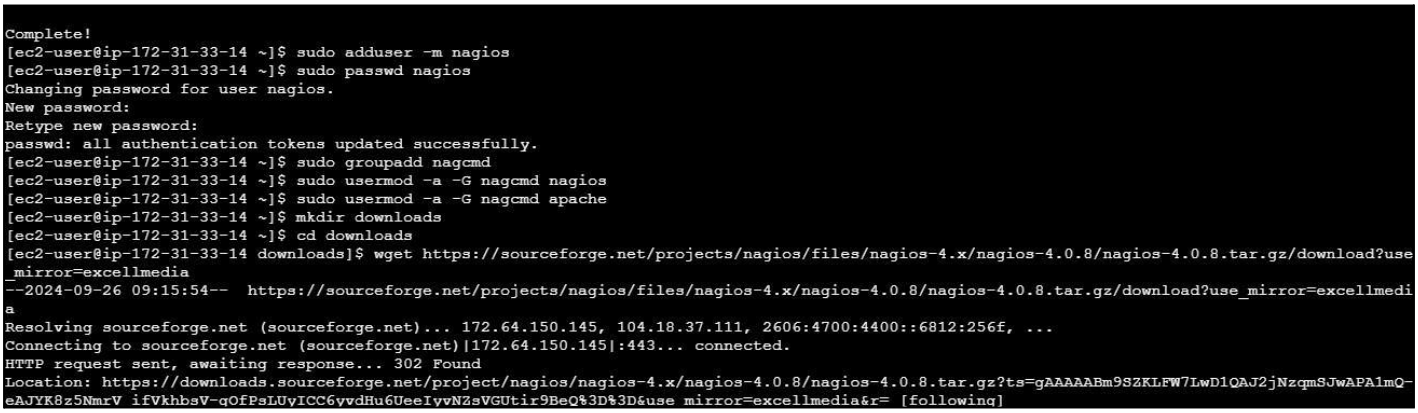
```
[ec2-user@ip-172-31-33-14 ~]$ sudo yum install gd gd-devel
Last metadata expiration check: 0:21:27 ago on Thu Sep 26 08:42:17 2024.
Dependencies resolved.
```

Package	Architecture	Version	Repository	Size
Installing:				
gd	x86_64	2.3.3-5.amzn2023.0.3	amazonlinux	139 k
gd-devel	x86_64	2.3.3-5.amzn2023.0.3	amazonlinux	38 k
Installing dependencies:				
brotli	x86_64	1.0.9-4.amzn2023.0.2	amazonlinux	314 k
brotli-devel	x86_64	1.0.9-4.amzn2023.0.2	amazonlinux	31 k
bzip2-devel	x86_64	1.0.8-6.amzn2023.0.2	amazonlinux	214 k
cairo	x86_64	1.17.6-2.amzn2023.0.1	amazonlinux	684 k
cmake-filesystem	x86_64	3.22.2-1.amzn2023.0.4	amazonlinux	16 k
fontconfig	x86_64	2.13.94-2.amzn2023.0.2	amazonlinux	273 k
fontconfig-devel	x86_64	2.13.94-2.amzn2023.0.2	amazonlinux	128 k
fonts-filesystem	noarch	1:2.0.5-12.amzn2023.0.2	amazonlinux	9.5 k
freetype	x86_64	2.13.2-5.amzn2023.0.1	amazonlinux	423 k

Step 5:Create a new nagios user by writing the following commands **sudo adduser -m nagios sudo passwd nagios**

```
Complete!
[ec2-user@ip-172-31-33-14 ~]$ sudo adduser -m nagios
[ec2-user@ip-172-31-33-14 ~]$ sudo passwd nagios
Changing password for user nagios.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[ec2-user@ip-172-31-33-14 ~]$
```

Step 6: Create a new user group using **sudo groupadd nagcmd** and
Add users to the group using the following commands:
sudo usermod -a -G nagcmd nagios
sudo usermod -a -G nagcmd apache



Step 7: Create a directory for Nagios downloads using the following commands-
Commands - **mkdir ~/downloads**
cd ~/downloads

Also download Nagios and plugin source files
Commands - **wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz**

```
Connecting to prdownloads.sourceforge.net (prdownloads.sourceforge.net)|204.68.111.105|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz [following]
--2024-09-26 09:38:43--  https://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz
Resolving downloads.sourceforge.net (downloads.sourceforge.net)... 204.68.111.105
Connecting to downloads.sourceforge.net (downloads.sourceforge.net)|204.68.111.105|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://excellmedia.dl.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz?viasf=1 [following]
--2024-09-26 09:38:45--  https://excellmedia.dl.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz?viasf=1
Resolving excellmedia.dl.sourceforge.net (excellmedia.dl.sourceforge.net)... 202.153.32.19, 2401:fb00:0:1fe:8000::5
Connecting to excellmedia.dl.sourceforge.net (excellmedia.dl.sourceforge.net)|202.153.32.19|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1805059 (1.7M) [application/x-gzip]
Saving to: 'nagios-4.0.8.tar.gz'

nagios-4.0.8.tar.gz                 100%[=================================================================>]   1.72M  8.14MB/s    in 0.2s

2024-09-26 09:38:45 (8.14 MB/s) - 'nagios-4.0.8.tar.gz' saved [1805059/1805059]

[ec2-user@ip-172-31-33-14 downloads]$ ls
'download?use_mirror=excellmedia'   nagios-4.0.8.tar.gz
[ec2-user@ip-172-31-33-14 downloads]$ tar -xzf nagios-4.0.8.tar.gz
[ec2-user@ip-172-31-33-14 downloads]$
```

Step 8-Extract the nagios source file with the following commands
tar zxvf nagios-4.4.6.tar.gz cd nagios-4.4.6

Then run the configuration script with the following command
/configure --with-command-group=nagcmd

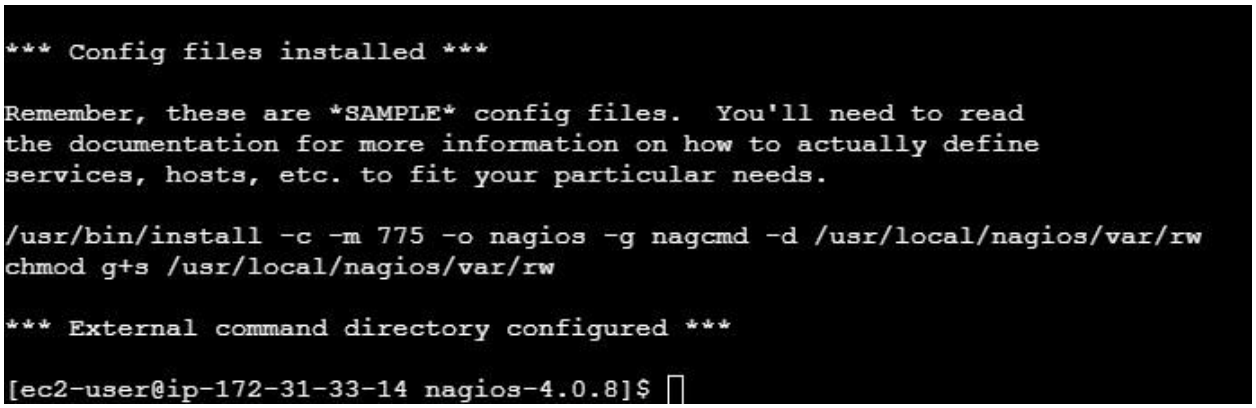
```
        Nagios user/group:  nagios,nagios
       Command user/group:  nagios,nagcmd
             Event Broker:  yes
        Install ${prefix}:  /usr/local/nagios
    Install ${includedir}:  /usr/local/nagios/include/nagios
                Lock file:  ${prefix}/var/nagios.lock
   Check result directory:  ${prefix}/var/spool/checkresults
           Init directory:  /etc/rc.d/init.d
  Apache conf.d directory:  /etc/httpd/conf.d
             Mail program:  /bin/mail
                  Host OS:  linux-gnu
          IOBroker Method:  epoll

 Web Interface Options:
 ------------------------
                HTML URL:  http://localhost/nagios/
                 CGI URL:  http://localhost/nagios/cgi-bin/
 Traceroute (used by WAP):  /usr/bin/traceroute


Review the options above for accuracy.  If they look okay,
type 'make all' to compile the main program and CGIs.

[ec2-user@ip-172-31-33-14 nagios-4.0.8]$
```

Step 9-Compile the source code with the following commands make all

Step 10-Install binaries,init script and sample config files

Commands -

./sudo make install sudo make install-init sudo make install-config sudo make install-commandmode



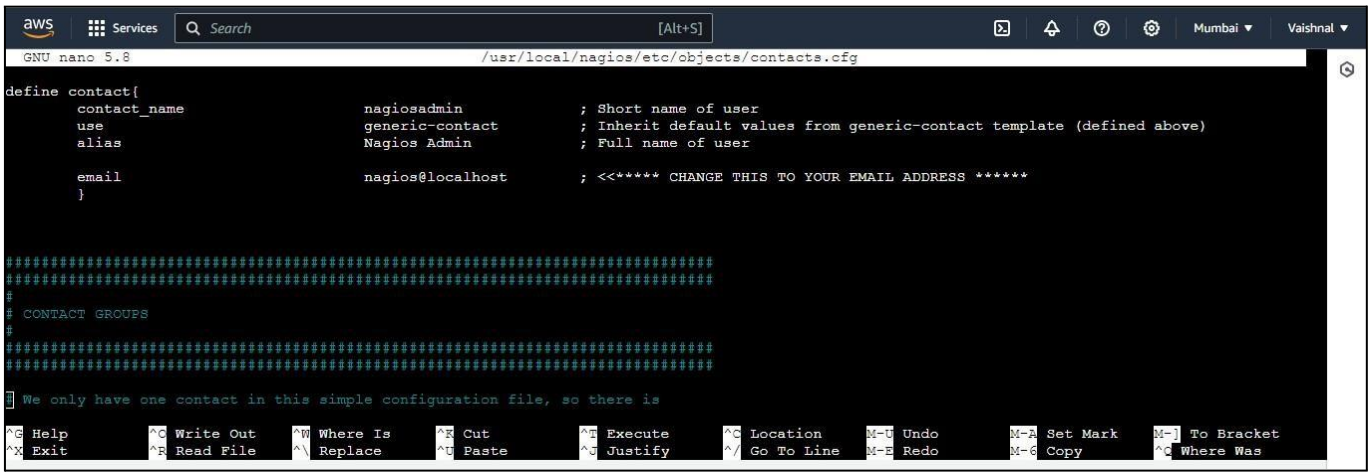
Step 11-Edit the Config File to Change the Email Address Commands -

sudo nano /usr/local/nagios/etc/objects/contacts.cfg

● Change the email address in the contacts.cfg file to your preferred email

Step 12-Configure the Web Interface

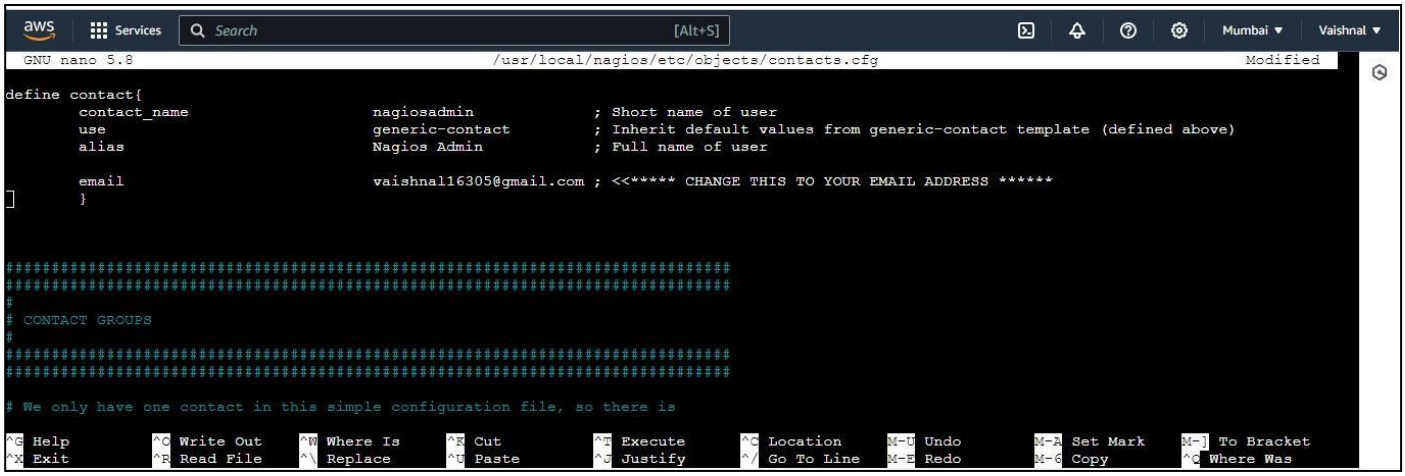
Commands - **sudo make install-webconf**



Step 13-Create a Nagios Admin Account

Commands -

sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin ● You will be prompted to enter and confirm the password for the nagiosadmin user



Step 14-. Extract the Plugins Source File

Commands - **cd**

~/downloads

tar zxvf nagios-plugins-2.3.3.tar.gz

cd nagios-plugins-2.3.3

```
*** External command directory configured ***

[ec2-user@ip-172-31-33-14 nagios-4.0.8]$ sudo nano /usr/local/nagios/etc/objects/contacts.cfg
[ec2-user@ip-172-31-33-14 nagios-4.0.8]$ sudo make install-webconf
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/httpd/conf.d/nagios.conf

*** Nagios/Apache conf file installed ***
```

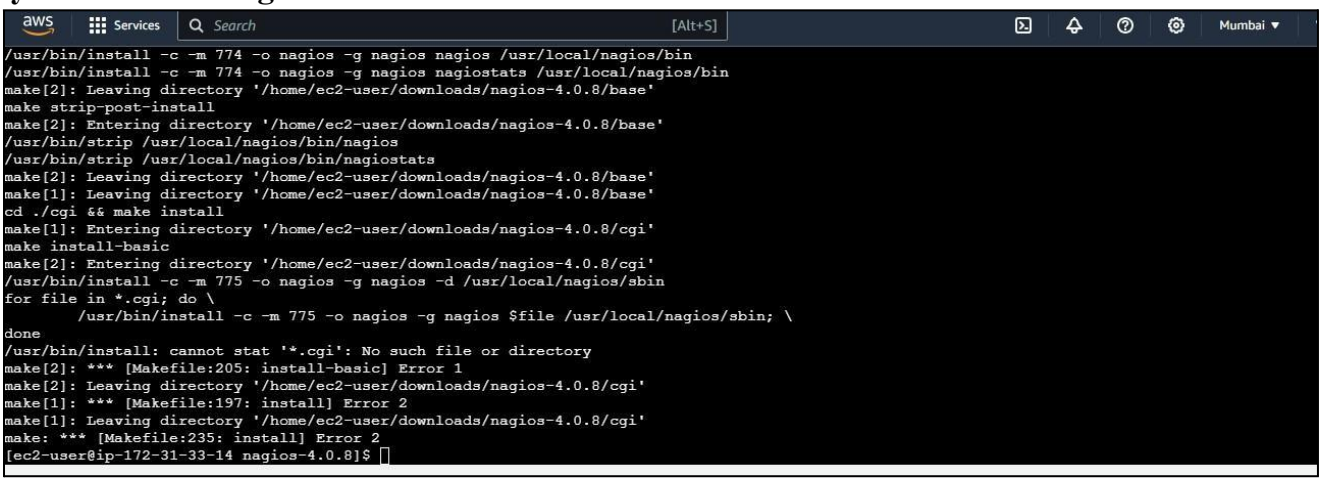
Step 15-19. Compile and Install Plugins

Commands -

./configure --with-nagios-user=nagios --with-nagios-group=nagios make
sudo make install

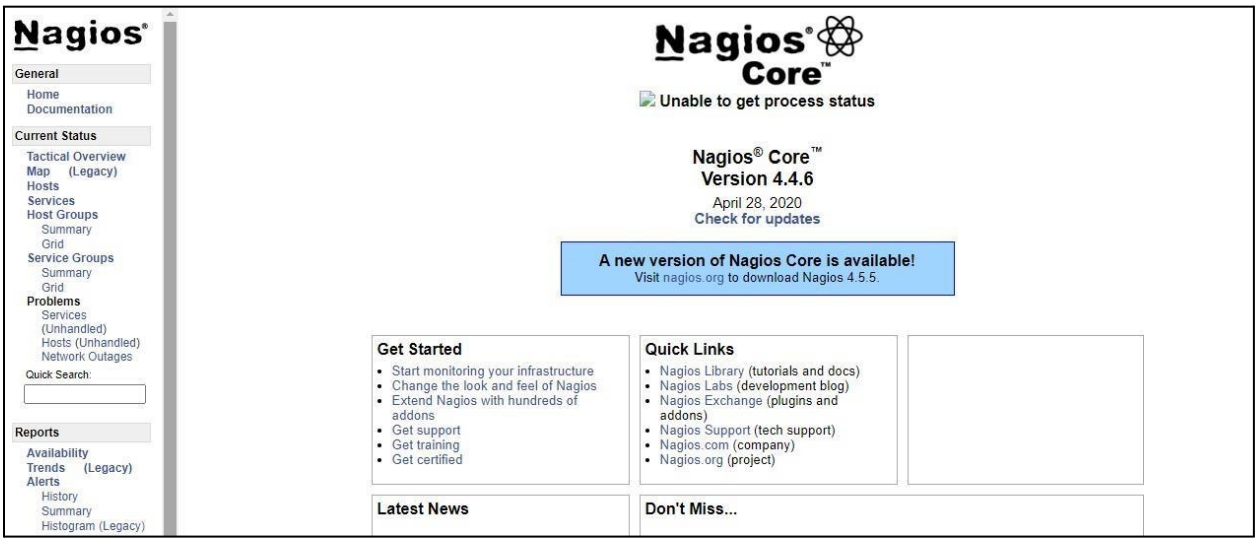
```
[ec2-user@ip-172-31-33-14 nagios-4.0.8]$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
```

Step 16-Start Nagios
Commands - **sudo chkconfig**
--add nagios sudo chkconfig
nagios on
sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg sudo
systemctl start nagios



Step 17-Access Nagios Web Interface

- Copy the Public IP address of your EC2 instance.
- Open your browser and navigate to http:///nagios.
- Enter the username nagiosadmin and the password you set in Step 16.

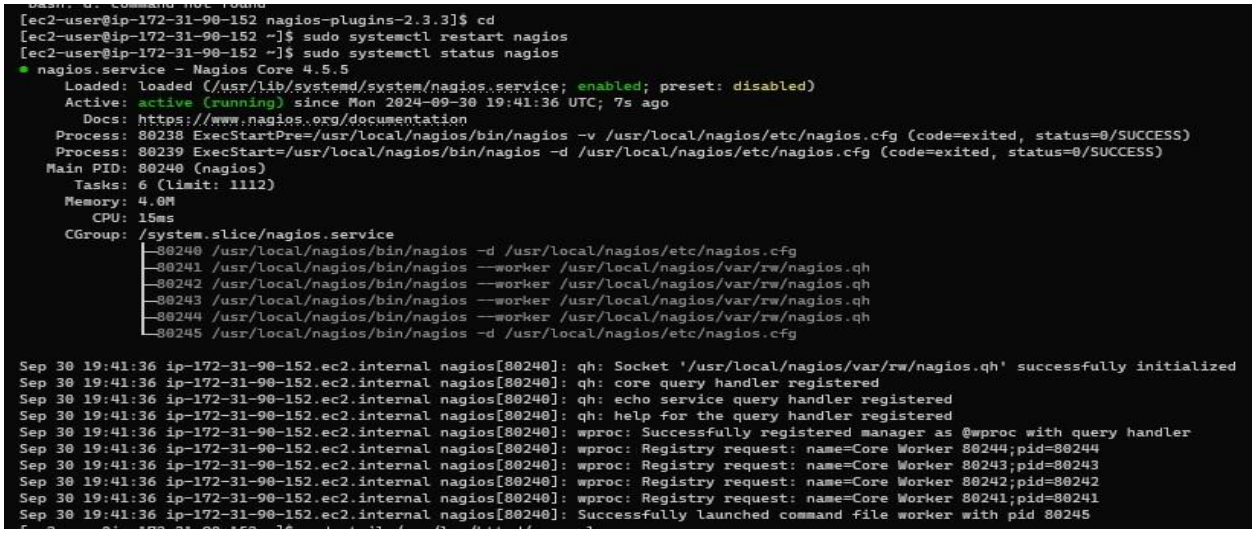

Nagios
General
Home
Documentation
Current Status
Tactical Overview
Map (Legacy)
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services (Unhandled)
Hosts (Unhandled)
Network Outages
Quick Search:
Reports
Availability
Trends (Legacy)
Alerts
History
Summary
Histogram (Legacy)
Nagios® Core™
Unable to get process status
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...

ADVANCE DEVOPS EXP-10

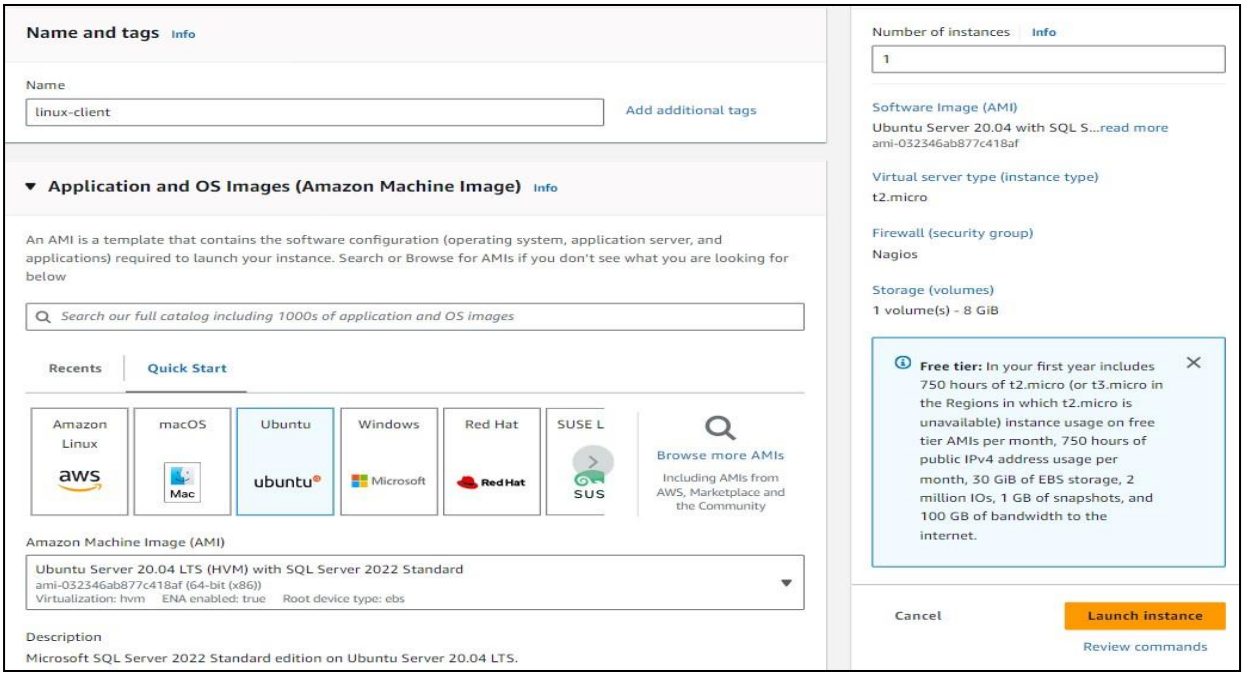
Riya Varyani **D15A/64**

Aim: To perform Port, Service monitoring, Windows/Linux server monitoring using Nagios.

Step-1. Confirm Nagios is Running on the Server. sudo systemctl status nagios Proceed if you see that Nagios is active and running.



Step-2. Create an Ubuntu 20.04 Server EC2 Instance



Step-3: Verify Nagios Process on the Server

```
[ec2-user@ip-172-31-80-215 nagios-plugins-2.3.3]$ ps -ef | grep nagios
nagios     68654       1  0 20:29 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios     68655   68654  0 20:29 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     68656   68654  0 20:29 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     68657   68654  0 20:29 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     68658   68654  0 20:29 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     68659   68654  0 20:29 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
ec2-user   69588   26447  0 20:44 pts/0    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-80-215 nagios-plugins-2.3.3]$
```

Step-4: Become Root User and Create Directoriessudo su , mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts **and to copy the same config file**- cp /usr/local/nagios/etc/objects/localhost.cfg, /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg

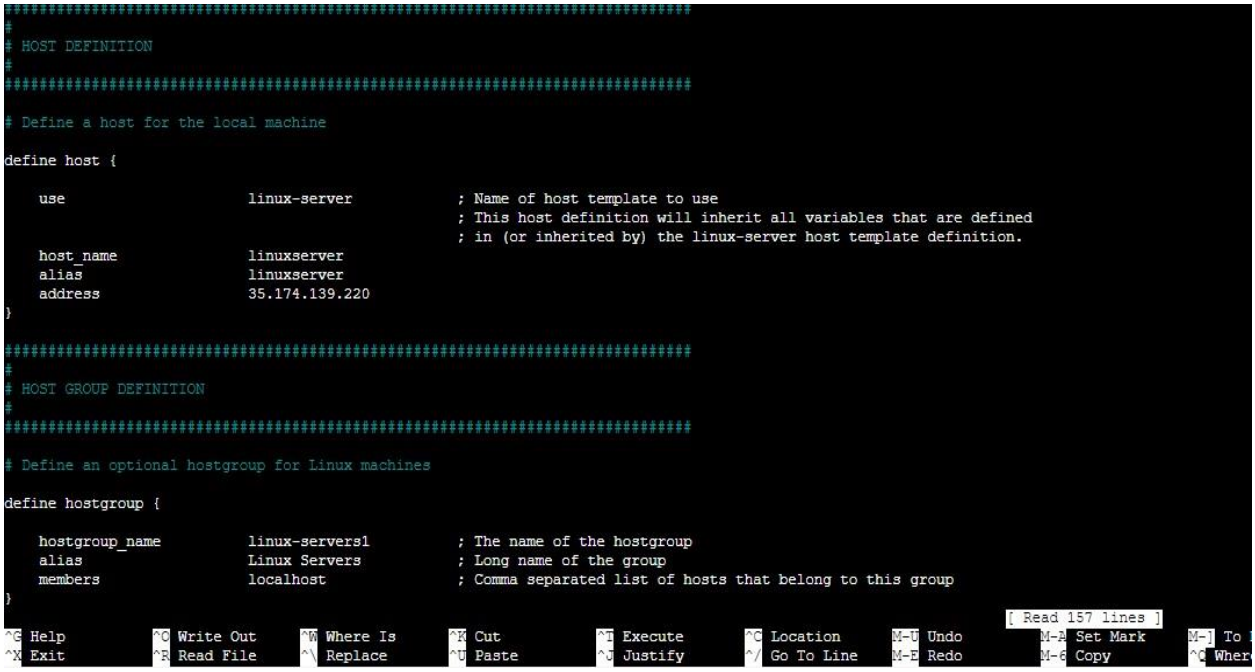
```
[ec2-user@ip-172-31-80-215 nagios-plugins-2.3.3]$ sudo su
[root@ip-172-31-80-215 nagios-plugins-2.3.3]# mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
[root@ip-172-31-80-215 nagios-plugins-2.3.3]# cp /usr/local/nagios/etc/objects/localhost.cfg
cp: missing destination file operand after '/usr/local/nagios/etc/objects/localhost.cfg'
Try 'cp --help' for more information.
[root@ip-172-31-80-215 nagios-plugins-2.3.3]# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
[root@ip-172-31-80-215 nagios-plugins-2.3.3]#
```

i-0ae1aae975bae3b7a (nagios-host)

Step-5: Edit the Configuration File

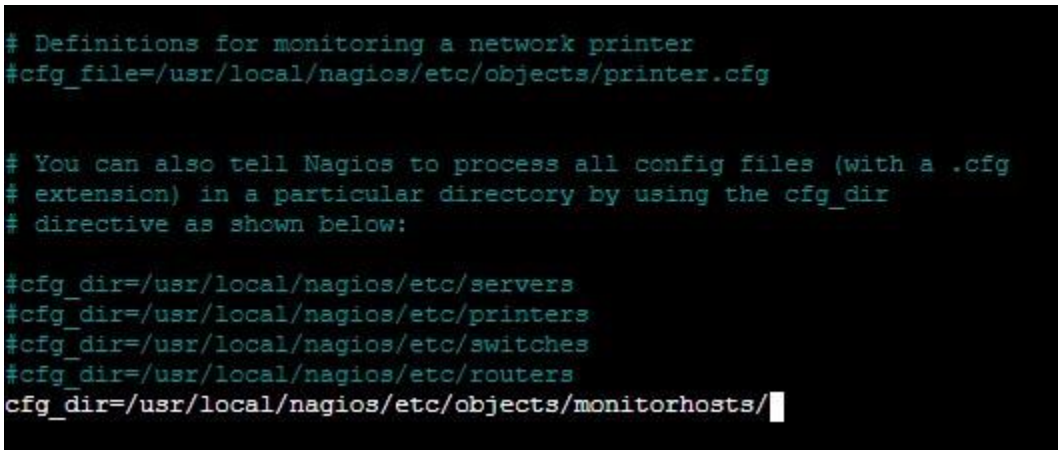
sudo nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg

- Change hostname to linuxserver everywhere in the file ●Change address to the public IP address of your linux-client.
- Change host_group name under hostgroup to linux_server



Step-6: Update Nagios Configuration sudo nano /usr/local/nagios/etc/nagios.cfg

Add the command - cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/



Step-7: Verify Configuration Files sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

```
[ec2-user@ip-172-31-80-215 ~]$ sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Nagios Core 4.4.6
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2020-04-28
License: GPL

Website: https://www.nagios.org
Reading configuration data...
   Read main config file okay...
Warning: Duplicate definition found for service 'HTTP' on host 'localhost' (config file '/usr/local/nagios/etc/objects/localhost.cfg'
Warning: Duplicate definition found for service 'SSH' on host 'localhost' (config file '/usr/local/nagios/etc/objects/localhost.cfg',
Warning: Duplicate definition found for service 'Swap Usage' on host 'localhost' (config file '/usr/local/nagios/etc/objects/localhos
Warning: Duplicate definition found for service 'Current Load' on host 'localhost' (config file '/usr/local/nagios/etc/objects/localh
Warning: Duplicate definition found for service 'Total Processes' on host 'localhost' (config file '/usr/local/nagios/etc/objects/loc
Warning: Duplicate definition found for service 'Current Users' on host 'localhost' (config file '/usr/local/nagios/etc/objects/local
Warning: Duplicate definition found for service 'Root Partition' on host 'localhost' (config file '/usr/local/nagios/etc/objects/loca
Warning: Duplicate definition found for service 'PING' on host 'localhost' (config file '/usr/local/nagios/etc/objects/localhost.cfg'
   Read object config files okay...

Running pre-flight check on configuration data...

Checking objects...
        Checked 8 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
```

Step-8: Restart Nagios Service sudo
systemctl restart nagios

Step-9:. SSH into the Client Machine

Use SSH or EC2 Instance Connect to access the `linux-client`.

Step-10: Update Package Index and Install Required Packages sudo
apt update -y sudo apt install gcc -y
sudo apt install -y nagios-nrpe-server nagios-plugins

```
ubuntu@ip-172-31-86-24:~$ sudo apt update -y
sudo apt install gcc -y
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:5 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [380 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [83.1 kB]
Get:10 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4560 B]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [274 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [535 kB]
Get:18 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [116 kB]
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [130 kB]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [8652 B]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [379 kB]
```

Step-11: Edit NRPE Configuration File

Commands -

sudo nano /etc/nagios/nrpe.cfg

Add your Nagios host IP address under `allowed_hosts`:

`allowed_hosts=<Nagios_Host_IP>`

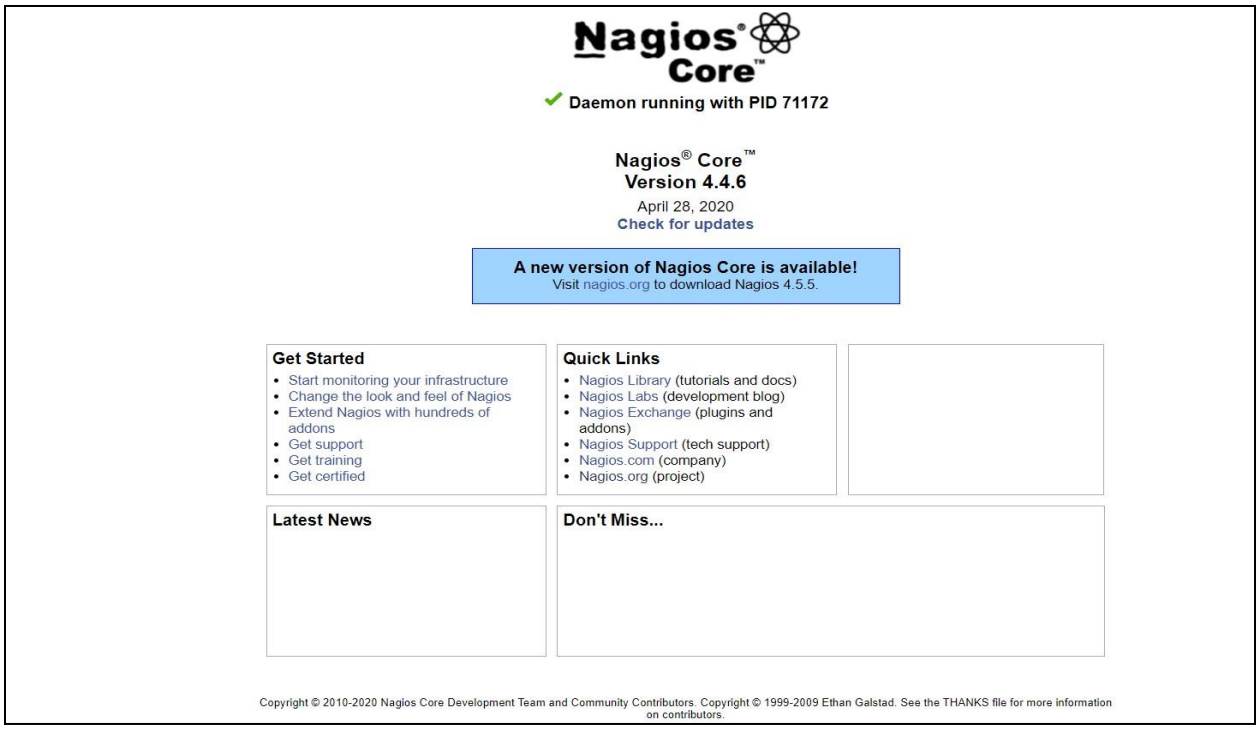
```
#
# Note: The daemon only does rudimentary checking of the client's IP
# address.  I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd

allowed_hosts=127.0.0.1,35.174.139.220



# COMMAND ARGUMENT PROCESSING
# This option determines whether or not the NRPE daemon will allow clients
# to specify arguments to commands that are executed.  This option only works
# if the daemon was configured with the --enable-command-args configure script
# option.
#
# *** ENABLING THIS OPTION IS A SECURITY RISK! ***
# Read the SECURITY file for information on some of the security implications
# of enabling this variable.
#
# Values: 0=do not allow arguments, 1=allow command arguments

dont_blame_nrpe=0
```

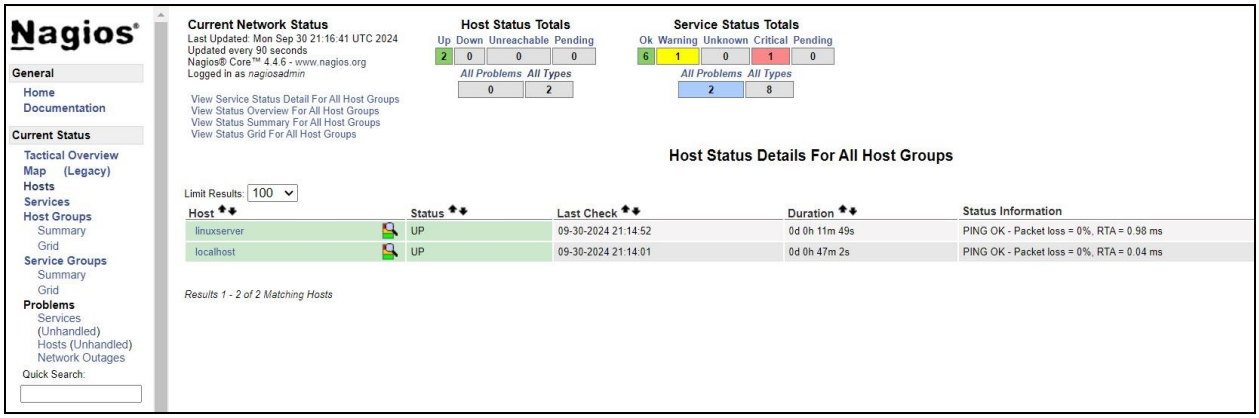
Step-12: Restart NRPE Server

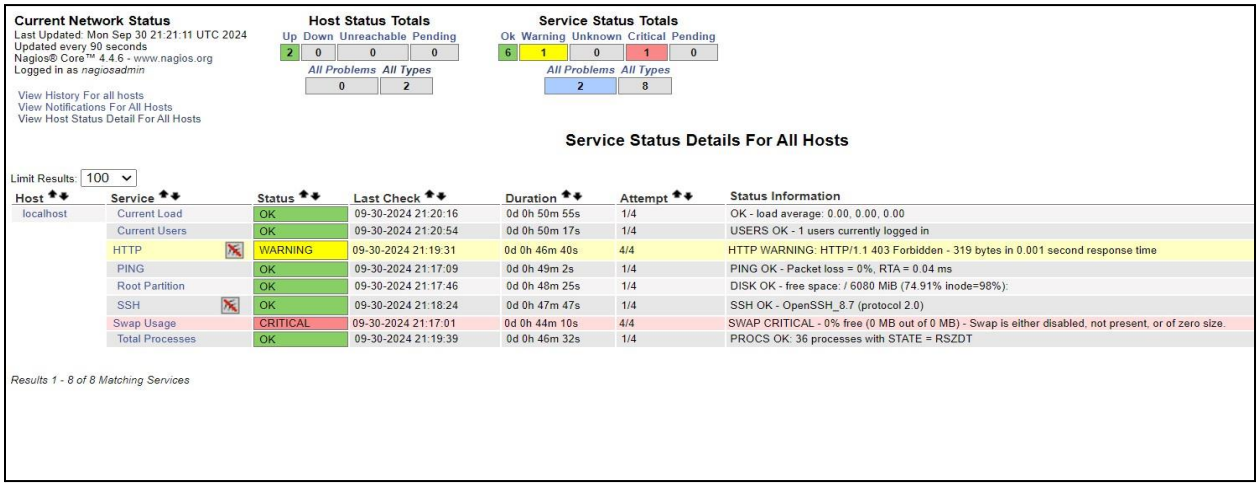
Commands -
sudo systemctl restart nagios-nrpe-server

Step-13: Check Nagios Dashboard

Open your browser and navigate to http://<Nagios_Host_IP>/nagios.
Log in with nagiosadmin and the password you set earlier.
You should see the new host linuxserver added.
Click on Hosts to see the host details.
Click on Services to see all services and ports being monitored


Nagios Core
Daemon running with PID 71172
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...
Copyright © 2010-2020 Nagios Core Development Team and Community Contributors. Copyright © 1999-2009 Ethan Galstad. See the THANKS file for more information on contributors.


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:
Current Network Status
Last Updated: Mon Sep 30 21:16:41 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.4.6 - www.nagios.org
Logged in as nagiosadmin
View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups
Host Status Totals
Up Down Unreachable Pending
2 0 0 0
All Problems All Types
0 2
Service Status Totals
Ok Warning Unknown Critical Pending
6 1 0 1 0
All Problems All Types
2 8
Host Status Details For All Host Groups
Limit Results: 100
Host
Status
Last Check
Duration
Status Information
linuxserver
UP
09-30-2024 21:14:52
0d 0h 11m 49s
PING OK - Packet loss = 0%, RTA = 0.98 ms
localhost
UP
09-30-2024 21:14:01
0d 0h 47m 2s
PING OK - Packet loss = 0%, RTA = 0.04 ms
Results 1 - 2 of 2 Matching Hosts


Current Network Status
Last Updated: Mon Sep 30 21:21:11 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.4.6 - www.nagios.org
Logged in as nagiosadmin
View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts
Host Status Totals
Up Down Unreachable Pending
2 0 0 0
All Problems All Types
0 2
Service Status Totals
Ok Warning Unknown Critical Pending
6 1 0 1 0
All Problems All Types
2 8
Service Status Details For All Hosts
Limit Results: 100
Host
Service
Status
Last Check
Duration
Attempt
Status Information
localhost
Current Load
OK
09-30-2024 21:20:16
0d 0h 50m 55s
1/4
OK - load average: 0.00, 0.00, 0.00
Current Users
OK
09-30-2024 21:20:54
0d 0h 50m 17s
1/4
USERS OK - 1 users currently logged in
HTTP
WARNING
09-30-2024 21:19:31
0d 0h 46m 40s
4/4
HTTP WARNING: HTTP/1.1 403 Forbidden - 319 bytes in 0.001 second response time
PING
OK
09-30-2024 21:17:09
0d 0h 49m 2s
1/4
PING OK - Packet loss = 0%, RTA = 0.04 ms
Root Partition
OK
09-30-2024 21:17:46
0d 0h 48m 25s
1/4
DISK OK - free space: / 6080 MiB (74.91% inode=98%):
SSH
OK
09-30-2024 21:18:24
0d 0h 47m 47s
1/4
SSH OK - OpenSSH_8.7 (protocol 2.0)
Swap Usage
CRITICAL
09-30-2024 21:17:01
0d 0h 44m 10s
4/4
SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.
Total Processes
OK
09-30-2024 21:19:39
0d 0h 46m 32s
1/4
PROCS OK: 36 processes with STATE = RSZDT
Results 1 - 8 of 8 Matching Services

Advance Devops-11

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

Theory:

AWS Lambda

AWS Lambda is a serverless computing service provided by Amazon Web Services (AWS). Users of AWS Lambda create functions, self-contained applications written in one of the supported languages and runtimes, and upload them to AWS Lambda, which executes those functions in an efficient and flexible manner.The Lambda functions can perform any kind of computing task, from serving web pages and processing streams of data to calling APIs and integrating with other AWS services.

The concept of "serverless" computing refers to not needing to maintain your own servers to run these functions. AWS Lambda is a fully managed service that takes care of all the infrastructure

for you. And so "serverless" doesn't mean that there are no servers involved: it just means that the servers, the operating systems, the network layer and the rest of the infrastructure have already been taken care of so that you can focus on writing application code.

Features of AWS Lambda

- AWS Lambda easily scales the infrastructure without any additional configuration. It reduces the operational work involved.
- It offers multiple options like AWS S3, CloudWatch, DynamoDB, API Gateway,

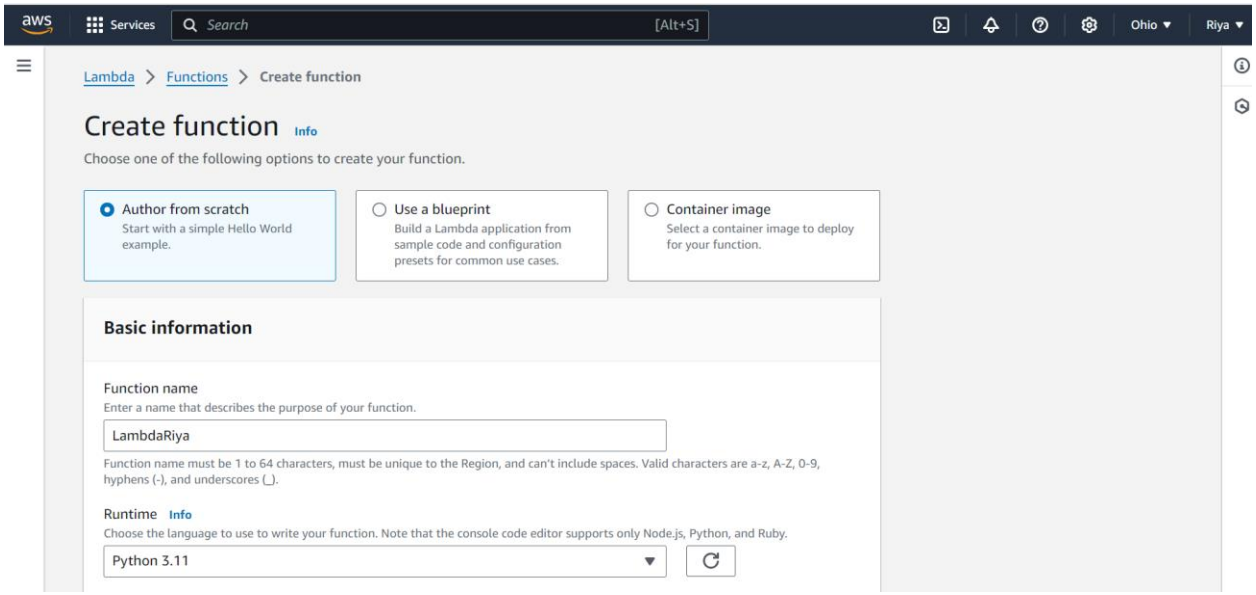
Kinesis,

CodeCommit, and many more to trigger an event.

- You don't need to invest upfront. You pay only for the memory used by the lambda function and minimal cost on the number of requests hence cost-efficient.
- AWS Lambda is secure. It uses AWS IAM to define all the roles and security policies.
  - It offers fault tolerance for both services running the code and the function. You do not have to worry about the application down.

Steps to create an AWS Lambda function

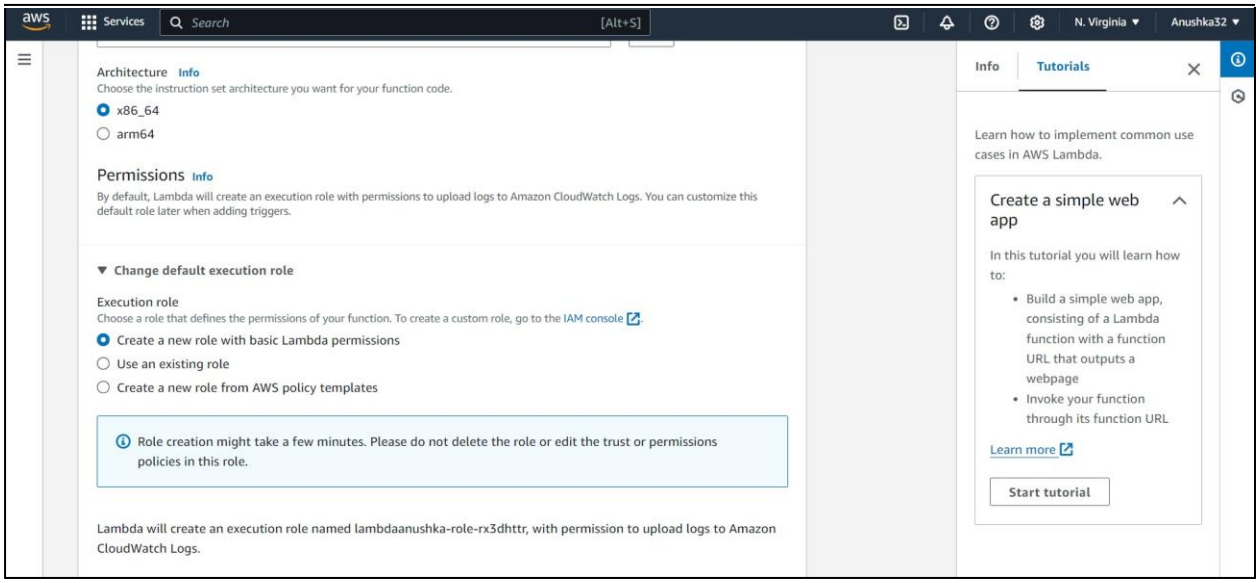
1. Open up the Lambda Console and click on the Create button. Be mindful of where you create your functions since Lambda is region-dependent.

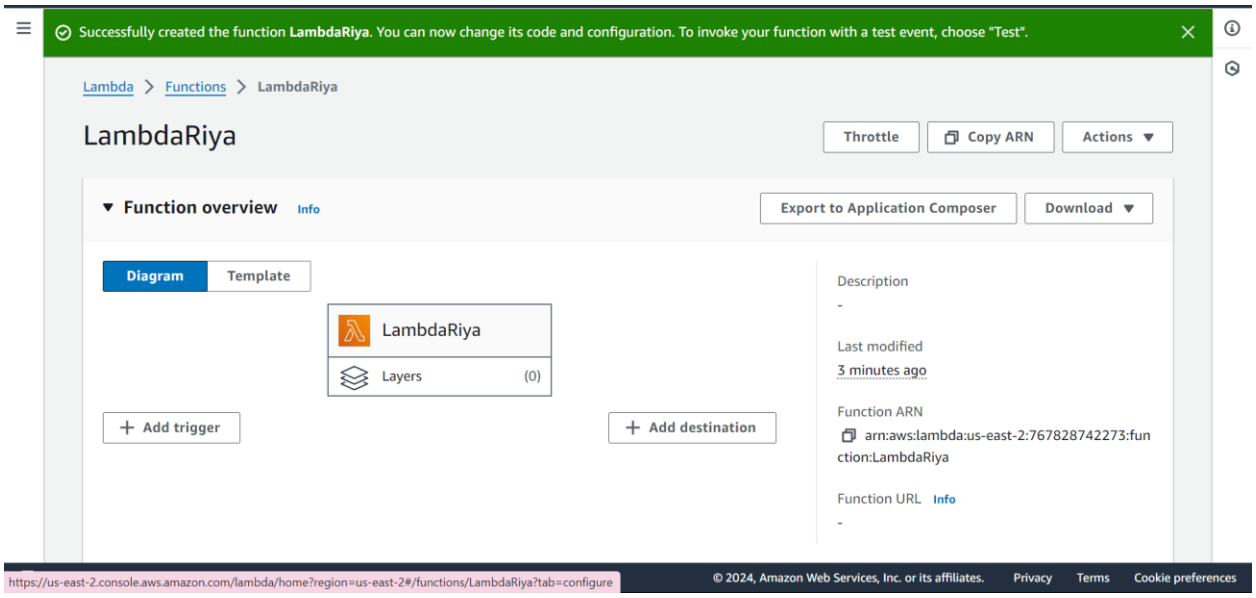


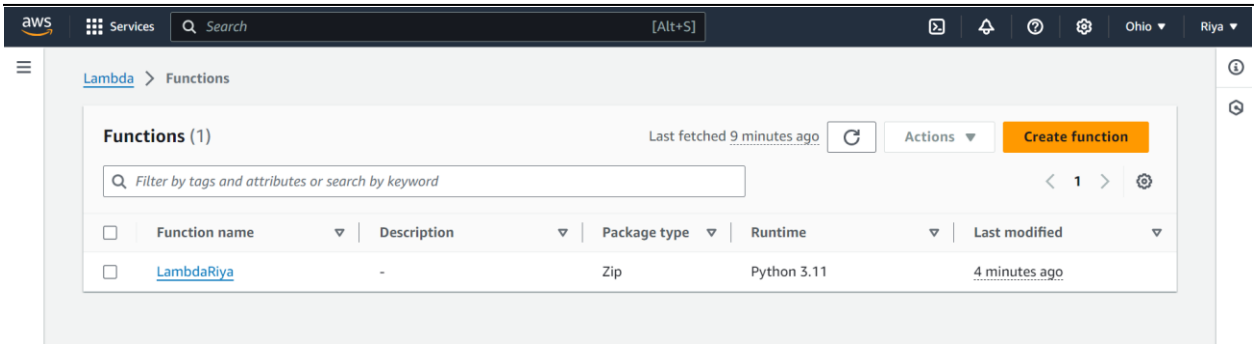
2. Choose to create a function from scratch or use a blueprint, i.e templates defined by AWS for you with all configuration presets required for the most common use cases.

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.

Riya Varyani D15A 64

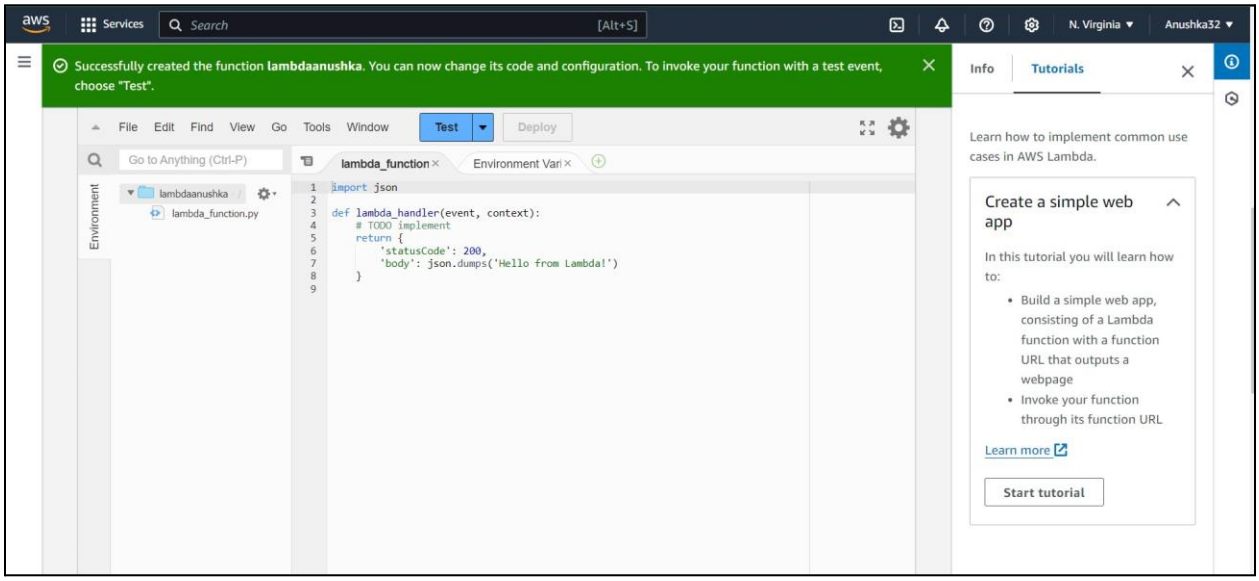


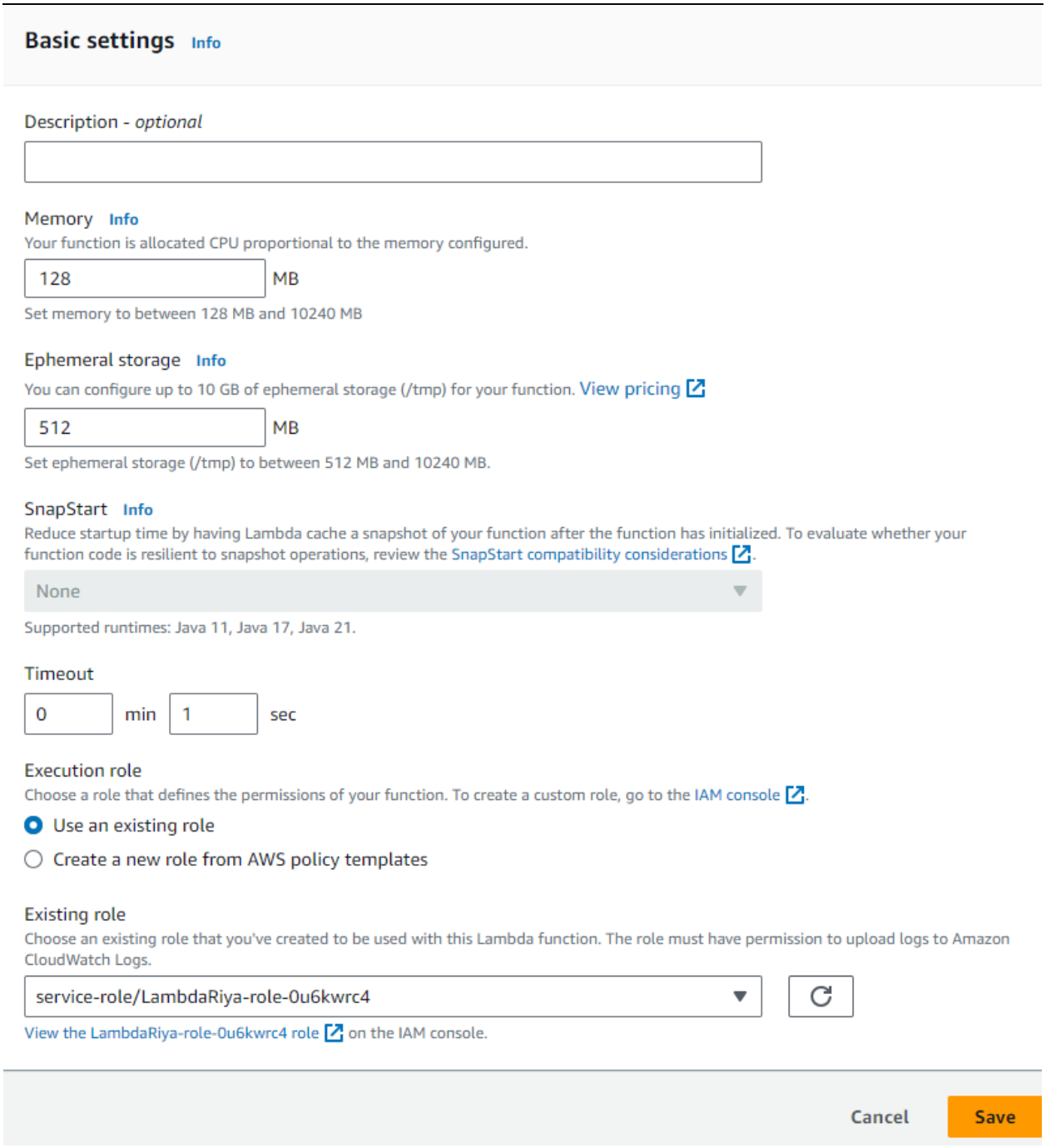




Click on the Create button.

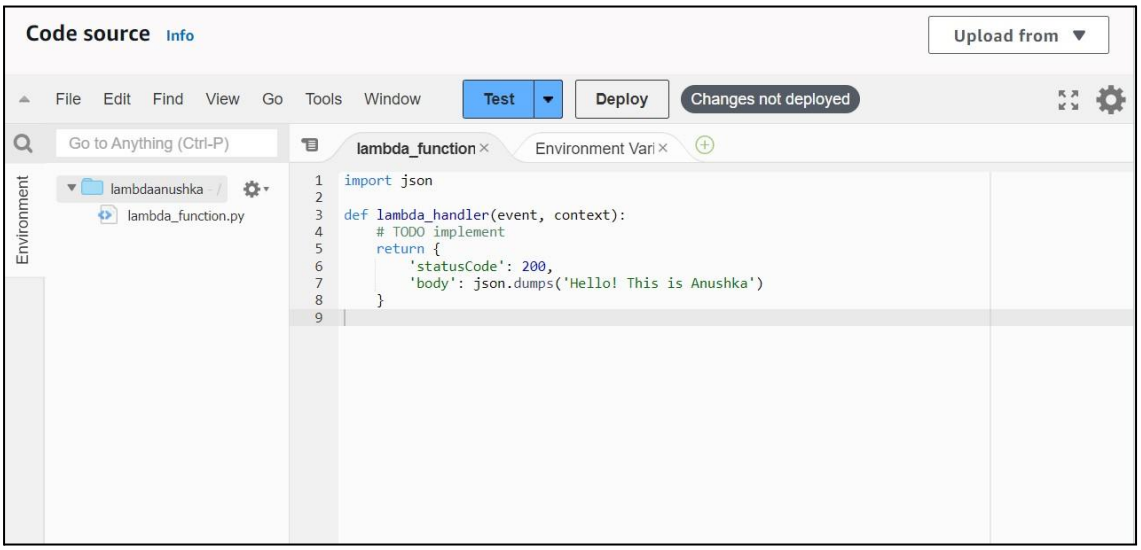
3. This process will take a while to finish and after that, you'll get a message that your function was successfully created.





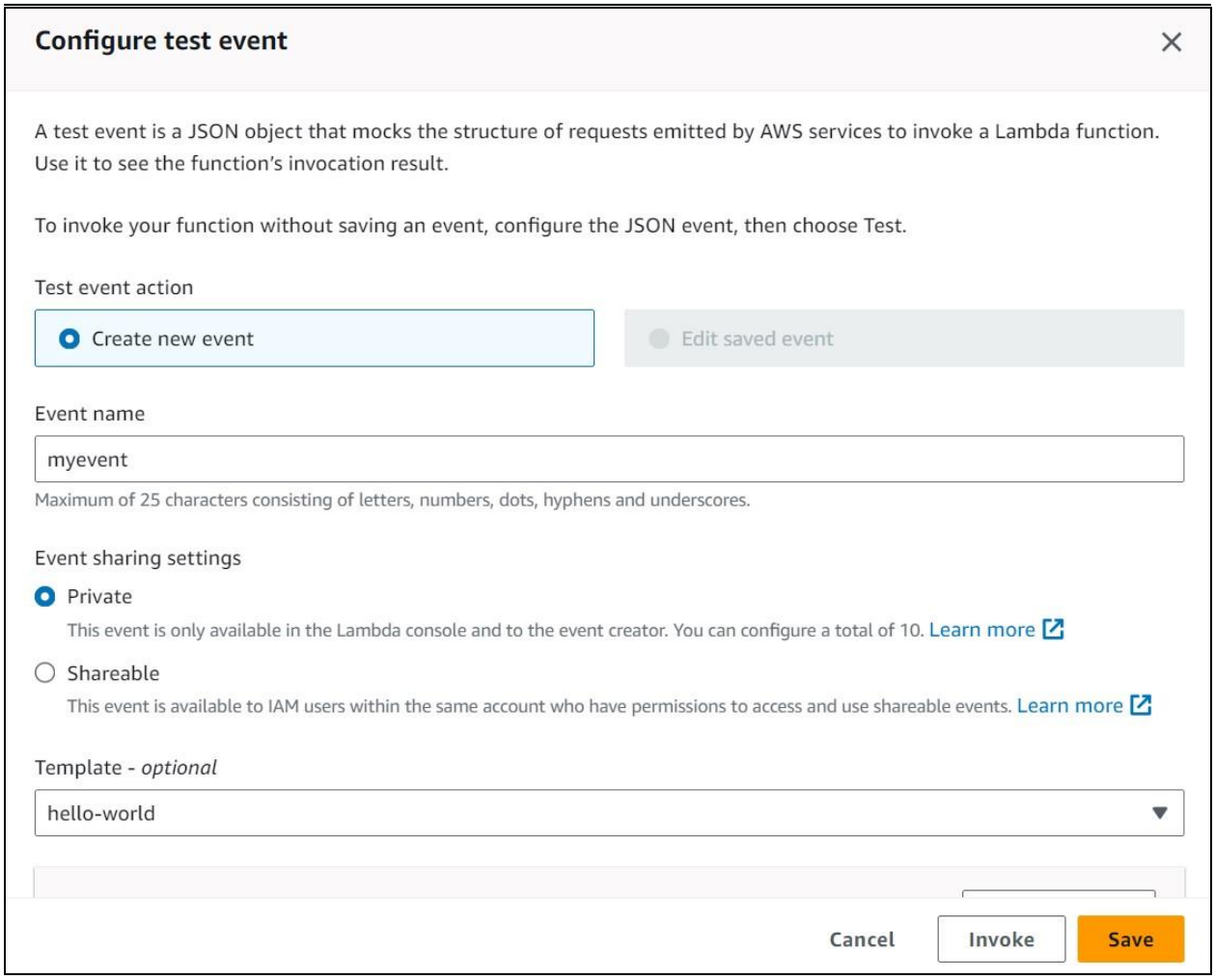
4. To change the configuration, open up the Configuration tab and under General Configuration, choose Edit.

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.



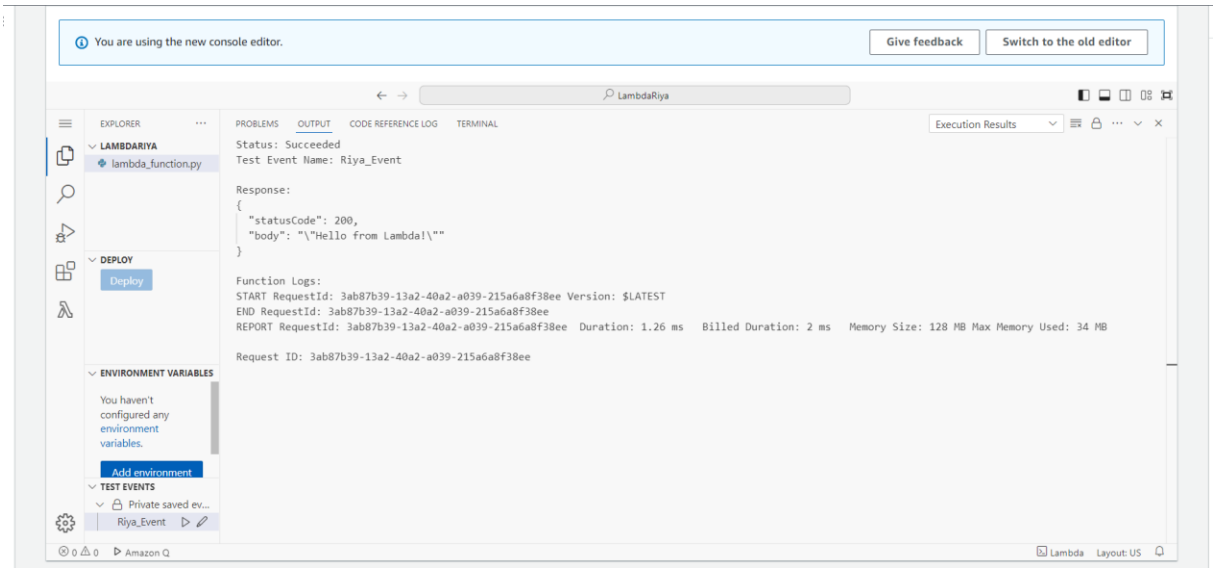
5. You can make changes to your function inside the code editor. You can also upload a zip file of your function or upload one from an S3 bucket if needed.

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:

AWS Lambda is a serverless computing service that allows you to run code without managing servers, making it highly scalable, cost-effective, and easy to use. It automatically manages the compute resources, executes your code in response to specific events such as API calls, file uploads, or database updates, and scales based on the demand.

ADVANCE DEVOPS EXP-12

Riya Varyani **D15A/64**

Aim: To create a Lambda function which will log “An image has been added” once you add an object to a specific bucket in S3.

Step 1: Login to your AWS Personal account. Now open S3 from services and click on create S3 bucket and create a bucket.

Step 2: Now Give a name to the Bucket, select general purpose project and deselect the Block public access and keep other this to default.

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

US East (Ohio) us-east-2

Bucket name Info

RiyaBucket

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

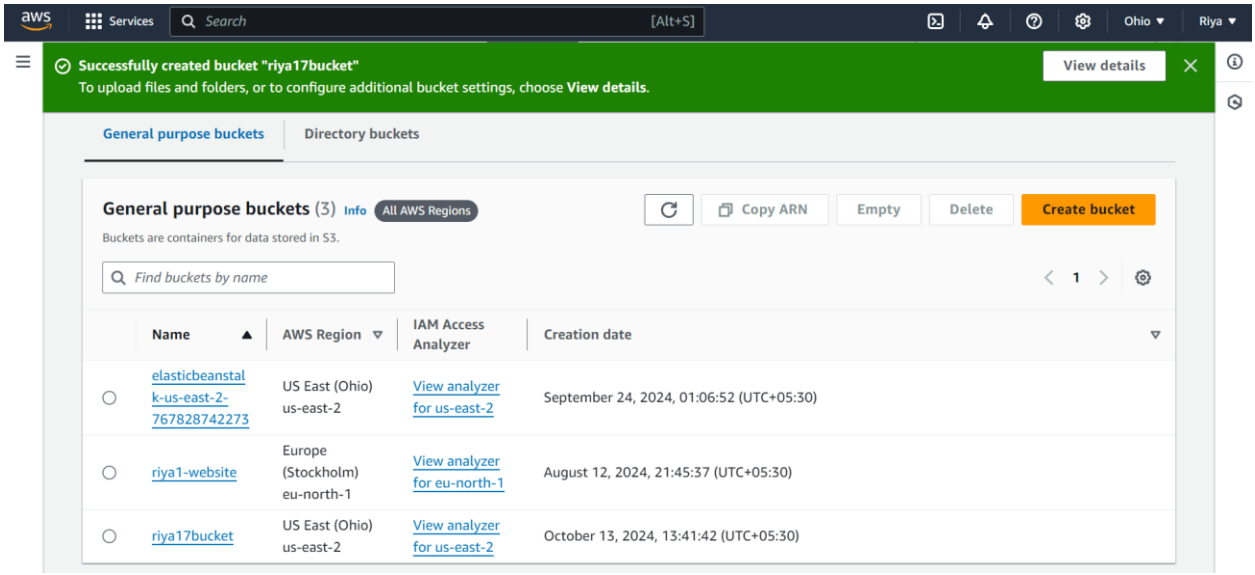
Object Ownership Info

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.

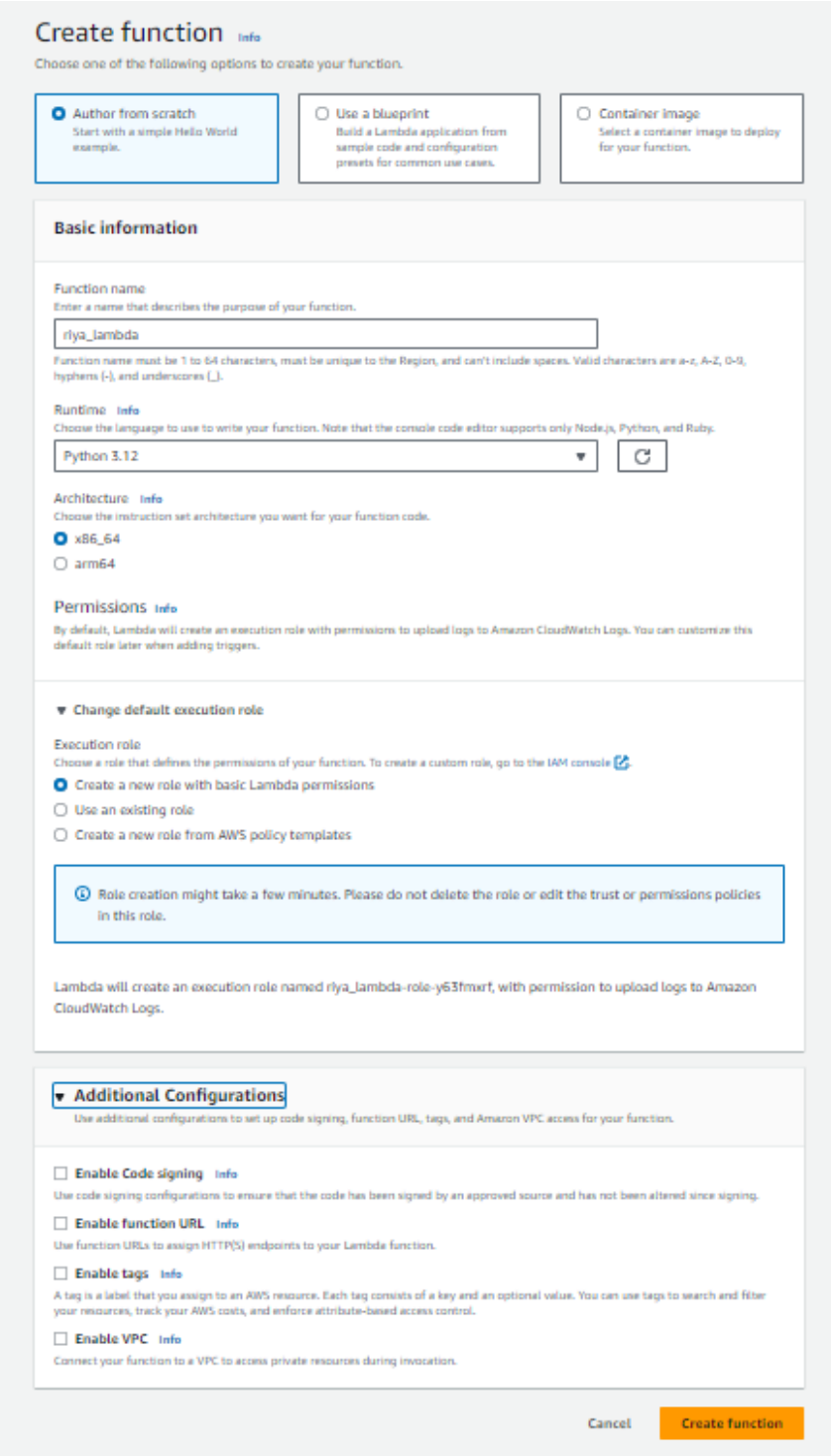
- (●) ACLs disabled (recommended)
  All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
- ( ) ACLs enabled
  Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using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

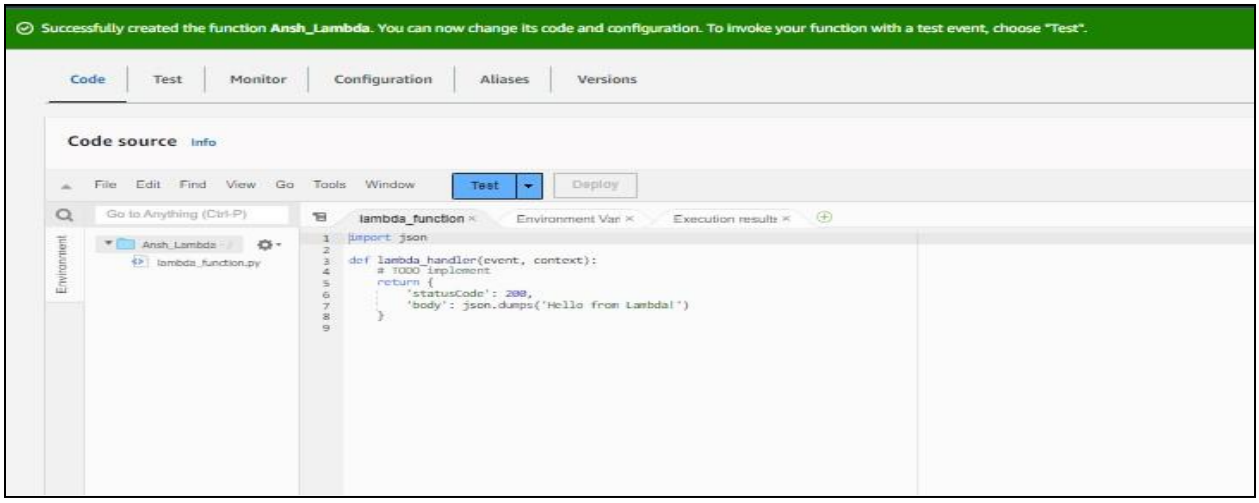
Object Ownership

Bucket owner enforced

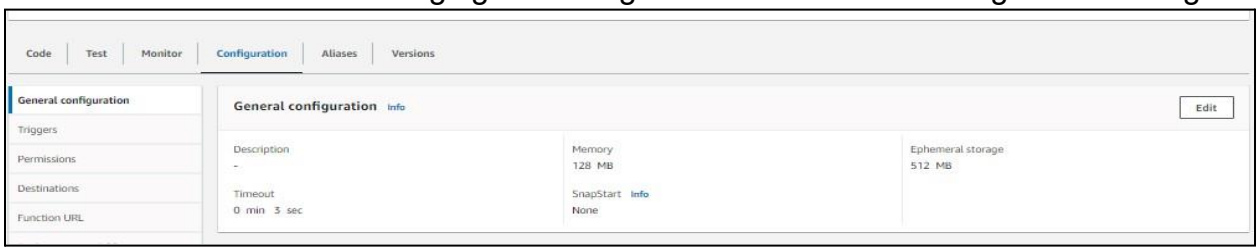

aws
Services
Search
[Alt+S]
Ohio
Riya
Successfully created bucket "riya17bucket"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
General purpose buckets
Directory buckets
General purpose buckets (3) Info All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
1
Name
AWS Region
IAM Access Analyzer
Creation date
elasticbeanstalk-us-east-2-767828742273
US East (Ohio) us-east-2
View analyzer for us-east-2
September 24, 2024, 01:06:52 (UTC+05:30)
riya1-website
Europe (Stockholm) eu-north-1
View analyzer for eu-north-1
August 12, 2024, 21:45:37 (UTC+05:30)
riya17bucket
US East (Ohio) us-east-2
View analyzer for us-east-2
October 13, 2024, 13:41:42 (UTC+05:30)

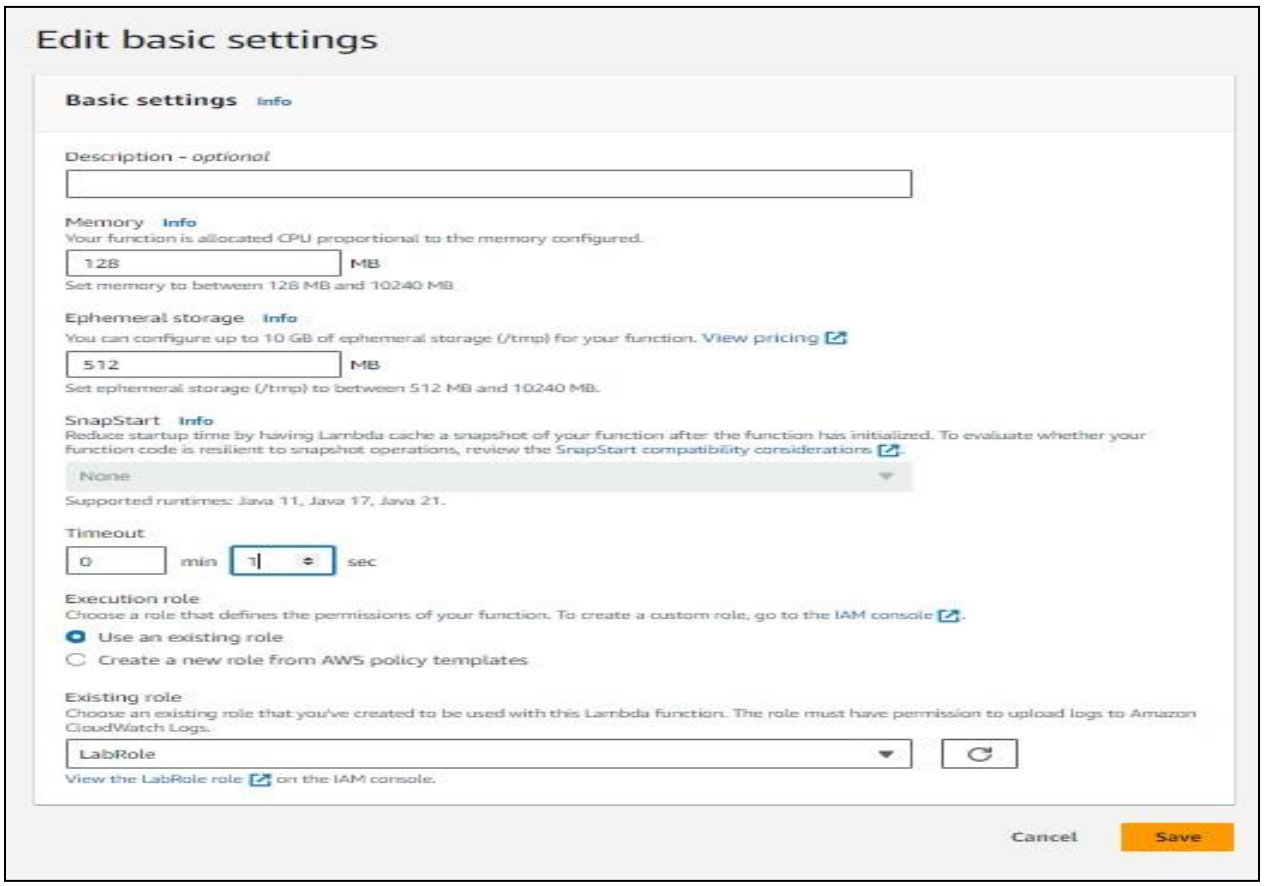
Step 3: Open lambda console and click on create function button.Give a name to your Lambda function, Select the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby. So will select Python 3.12
, Architecture as x86, and existing Execution role



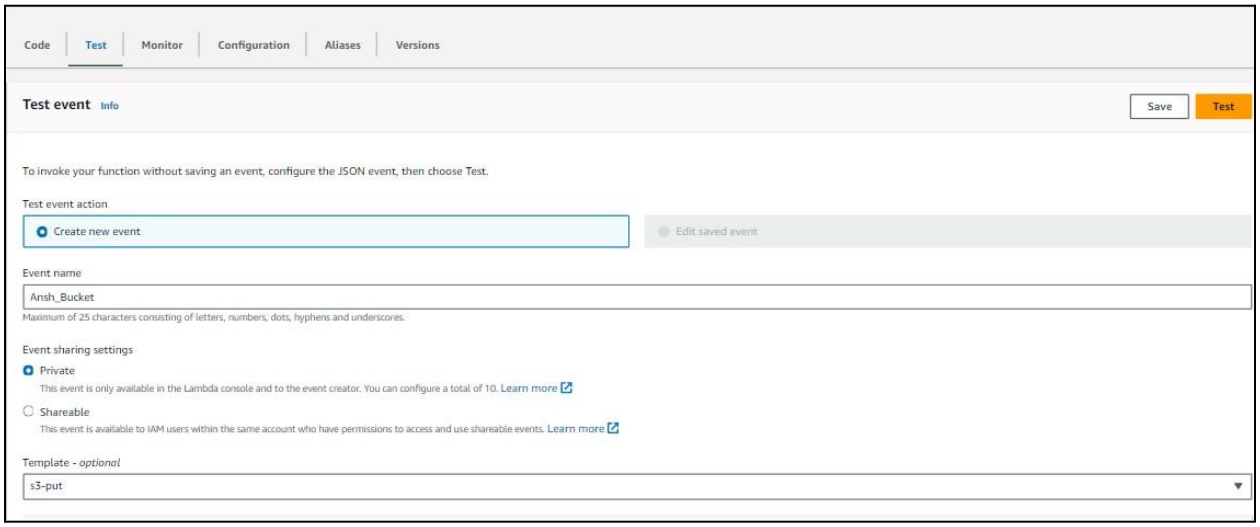


So See or Edit the basic settings go to configuration then click on edit general setting.

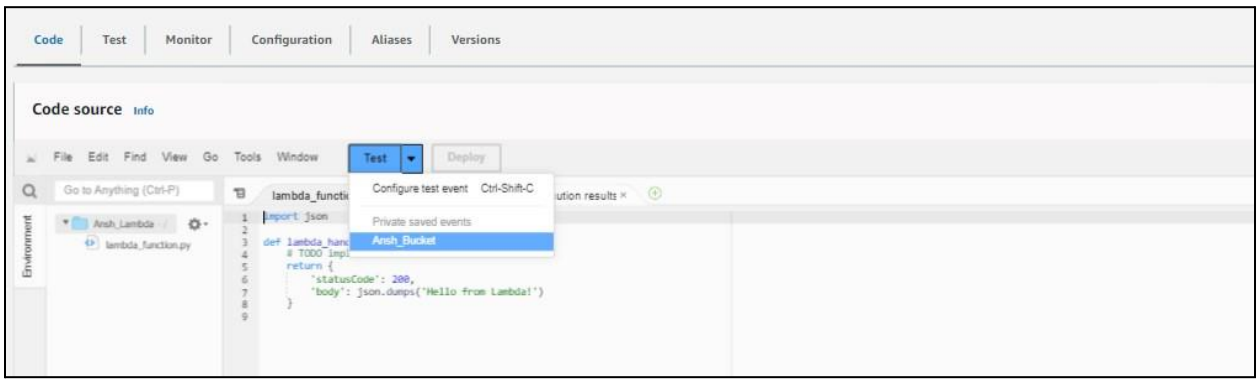




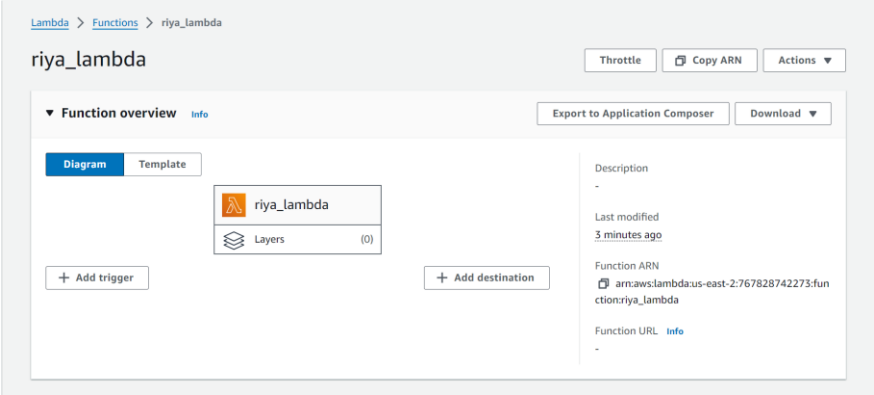
Step 4: Now Click on the Test tab then select Create a new event, give a name to the event and select Event Sharing to private, and select s3 put template.



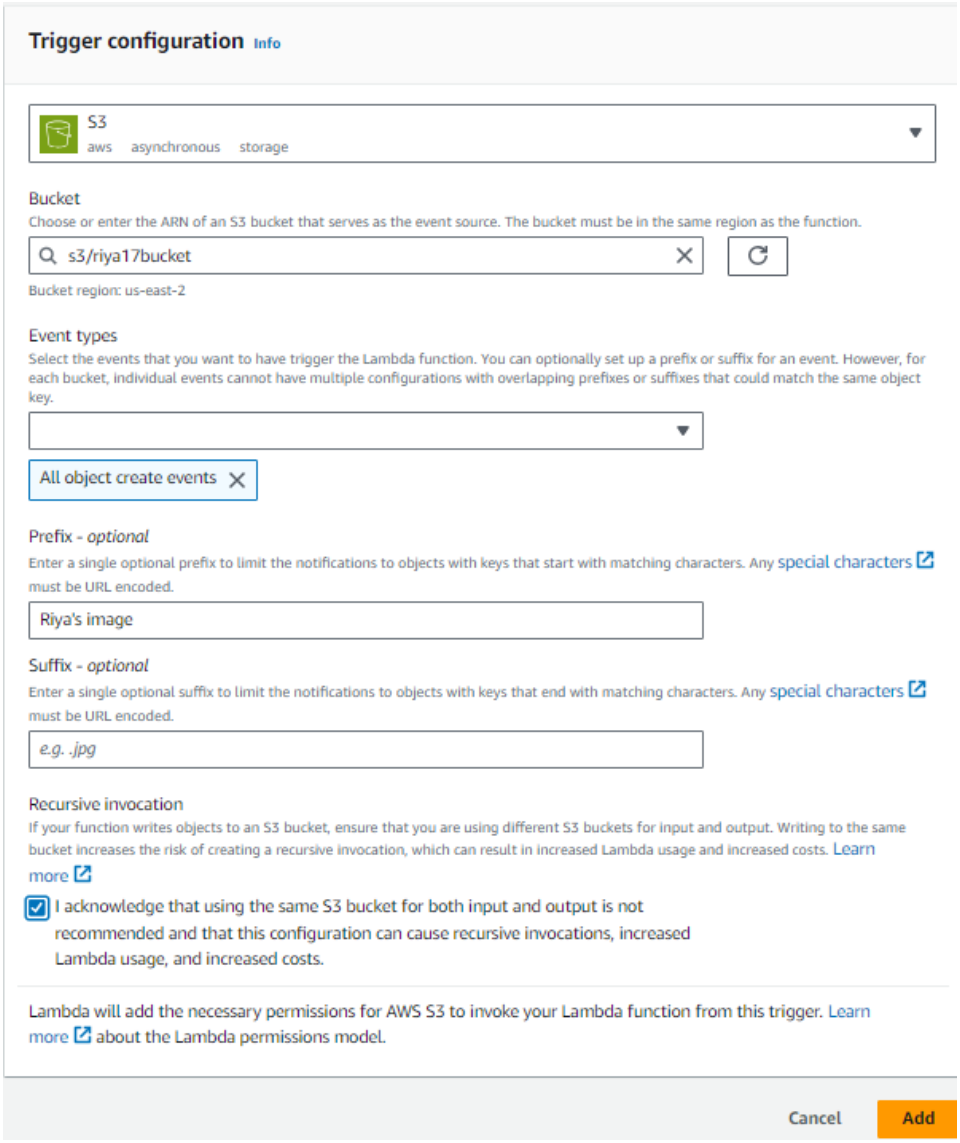
Step 5: Now In Code section select the created event from the dropdown .

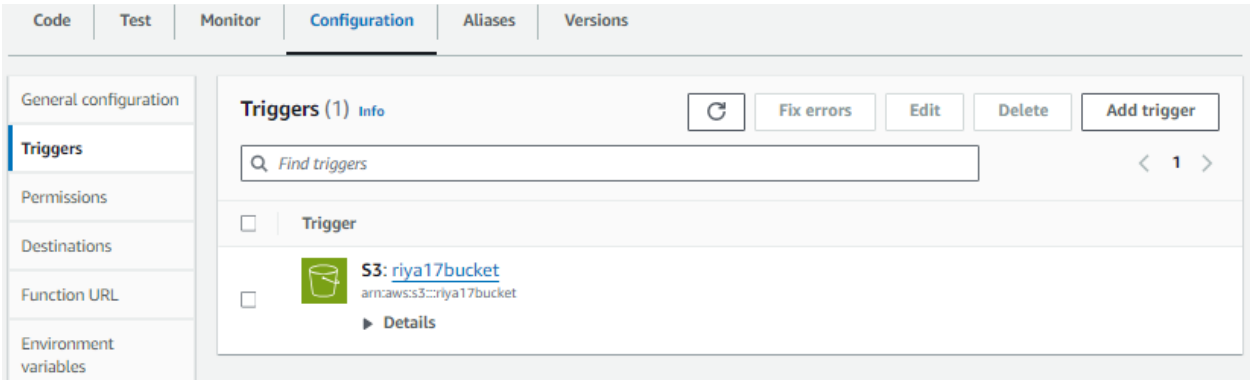


Step 6: Now In the Lambda function click on add tigger.

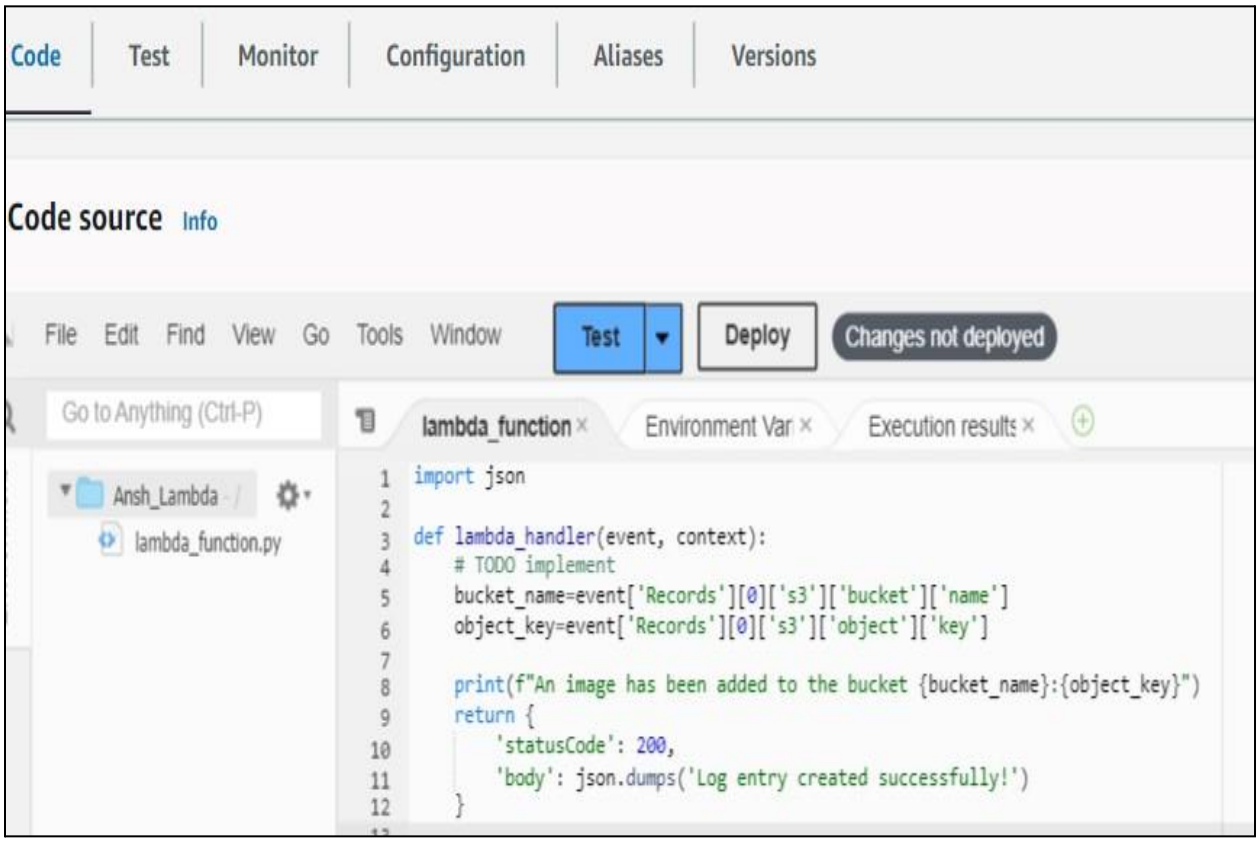


Now select the source as S3 then select the bucket name from the dropdown, keep other things to default and also you can add prefix to image.





Step 7: Now Write code that logs a message like “An Image has been added” when triggered. Save the file and click on deploy



Step 8: Now upload any image to the bucket

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (1 Total, 26.6 KB)

Remove | Add files | Add folder

All files and folders in this table will be uploaded.

Find by name

1

Name	Folder	Type	Size
Screenshot 2…	-	image/png	26.6 KB

Destination Info

Destination

s3://riya17bucket

▶ **Destination details**

Bucket settings that impact new objects stored in the specified destination.

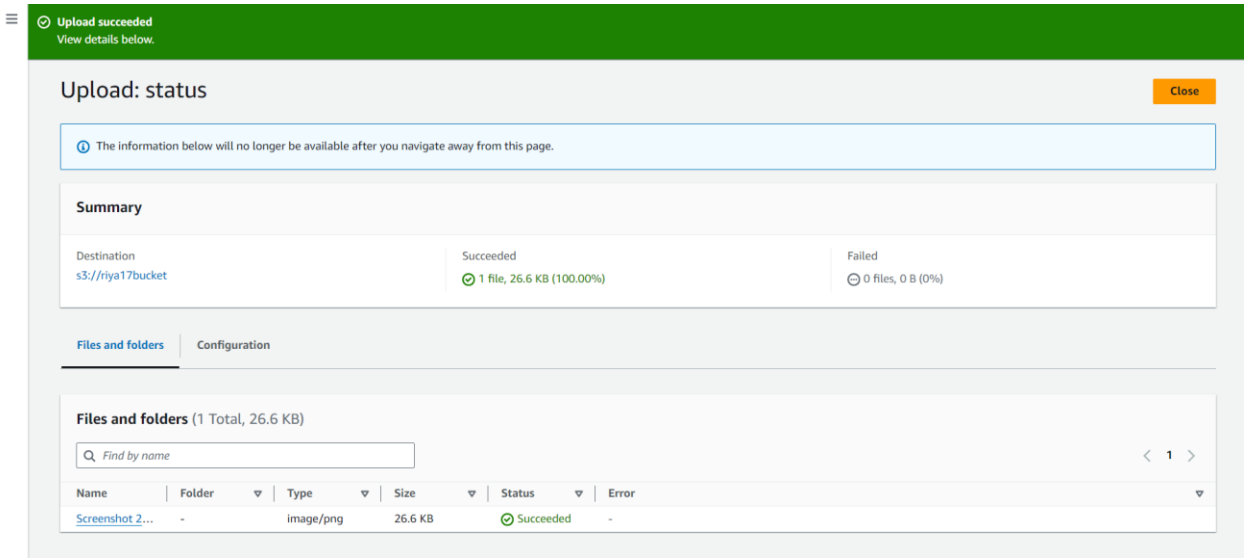
▶ **Permissions**

Grant public access and access to other AWS accounts.

▶ **Properties**

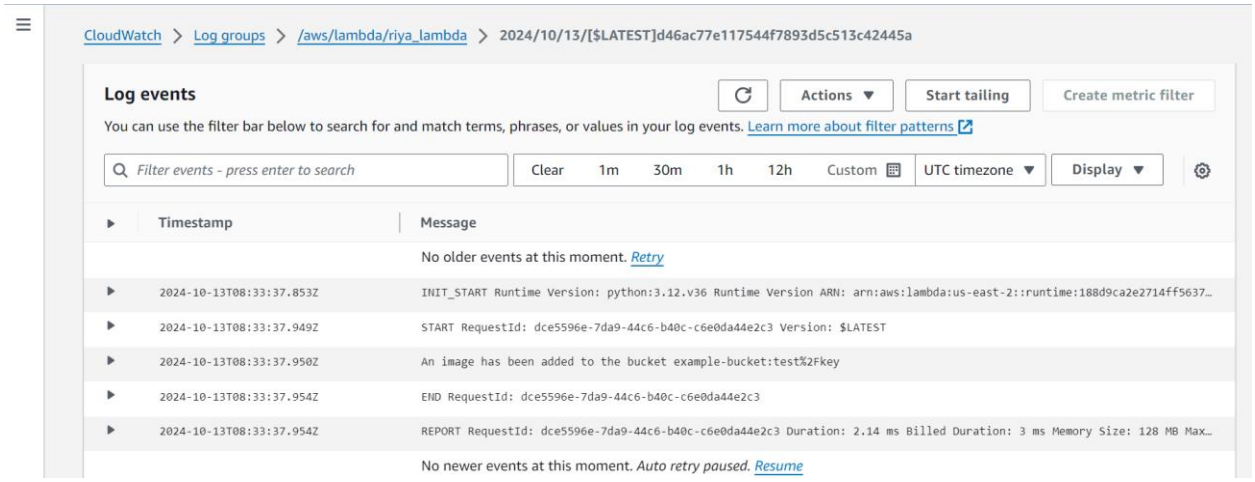
Specify storage class, encryption settings, tags, and more.

Cancel | Upload



Step 10: Now to click on test in lambda to check whether it is giving log when image is added to S3.

Step 11: Now Lets see the log on Cloud watch.To see it go to monitor section and then click on view cloudwatch logs.


CloudWatch > Log groups > /aws/lambda/riya_lambda > 2024/10/13/[$LATEST]d46ac77e117544f7893d5c513c42445a
Log events
Actions
Start tailing
Create metric filter
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns
Filter events - press enter to search
Clear
1m
30m
1h
12h
Custom
UTC timezone
Display
Timestamp
Message
No older events at this moment. Retry
2024-10-13T08:33:37.853Z INIT_START Runtime Version: python:3.12.v36 Runtime Version ARN: arn:aws:lambda:us-east-2::runtime:188d9ca2e2714ff5637…
2024-10-13T08:33:37.949Z START RequestId: dce5596e-7da9-44c6-b40c-c6e0da44e2c3 Version: $LATEST
2024-10-13T08:33:37.950Z An image has been added to the bucket example-bucket:test%2Fkey
2024-10-13T08:33:37.954Z END RequestId: dce5596e-7da9-44c6-b40c-c6e0da44e2c3
2024-10-13T08:33:37.954Z REPORT RequestId: dce5596e-7da9-44c6-b40c-c6e0da44e2c3 Duration: 2.14 ms Billed Duration: 3 ms Memory Size: 128 MB Max…
No newer events at this moment. Auto retry paused. Resume