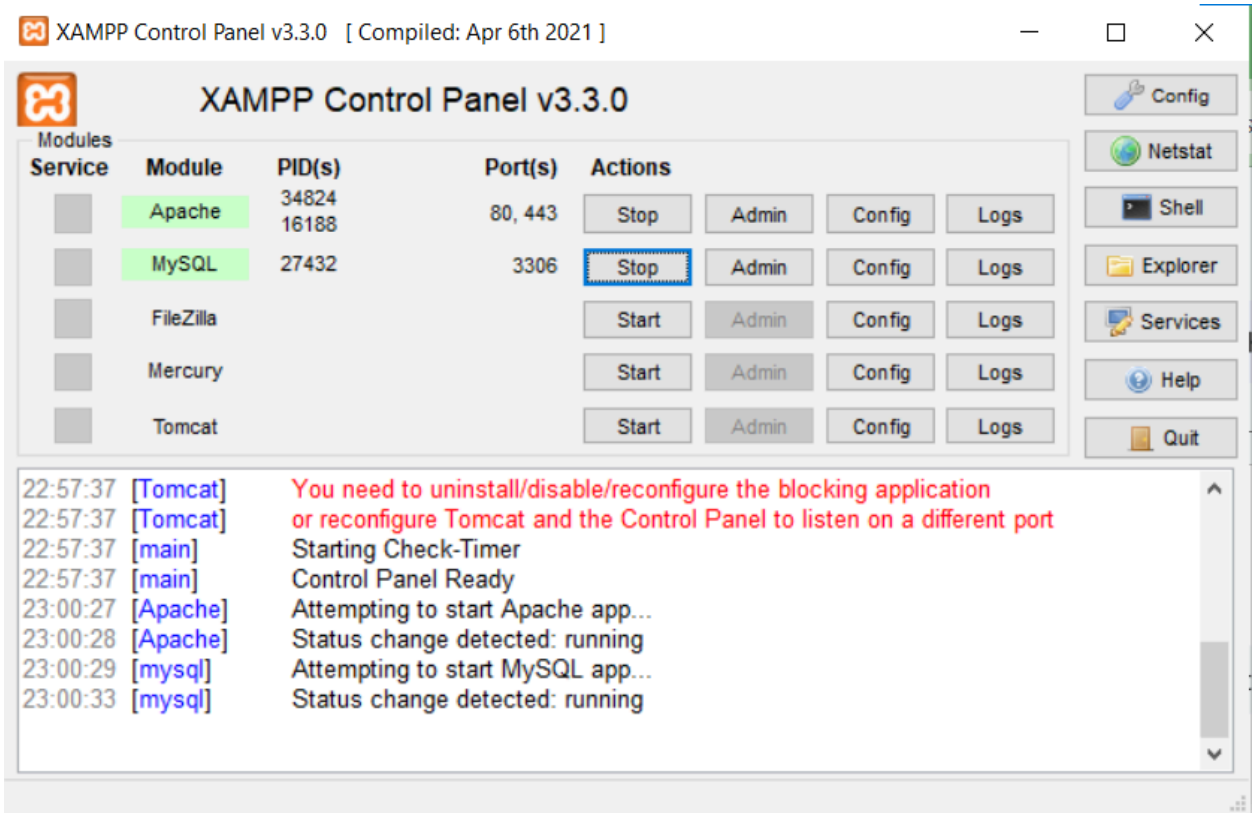
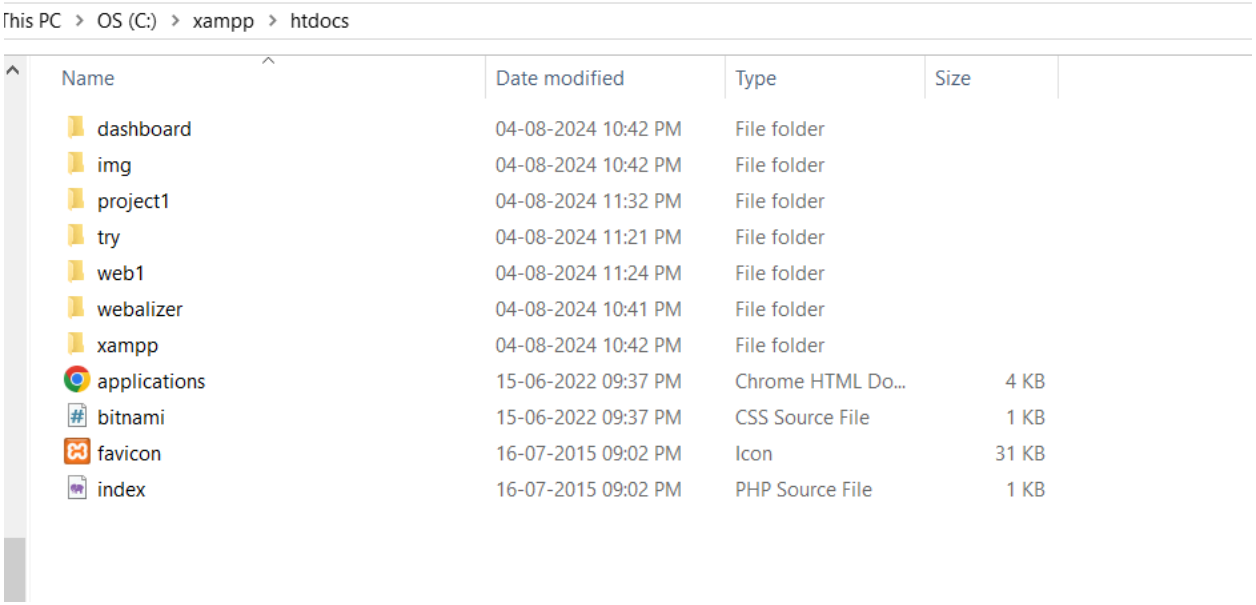
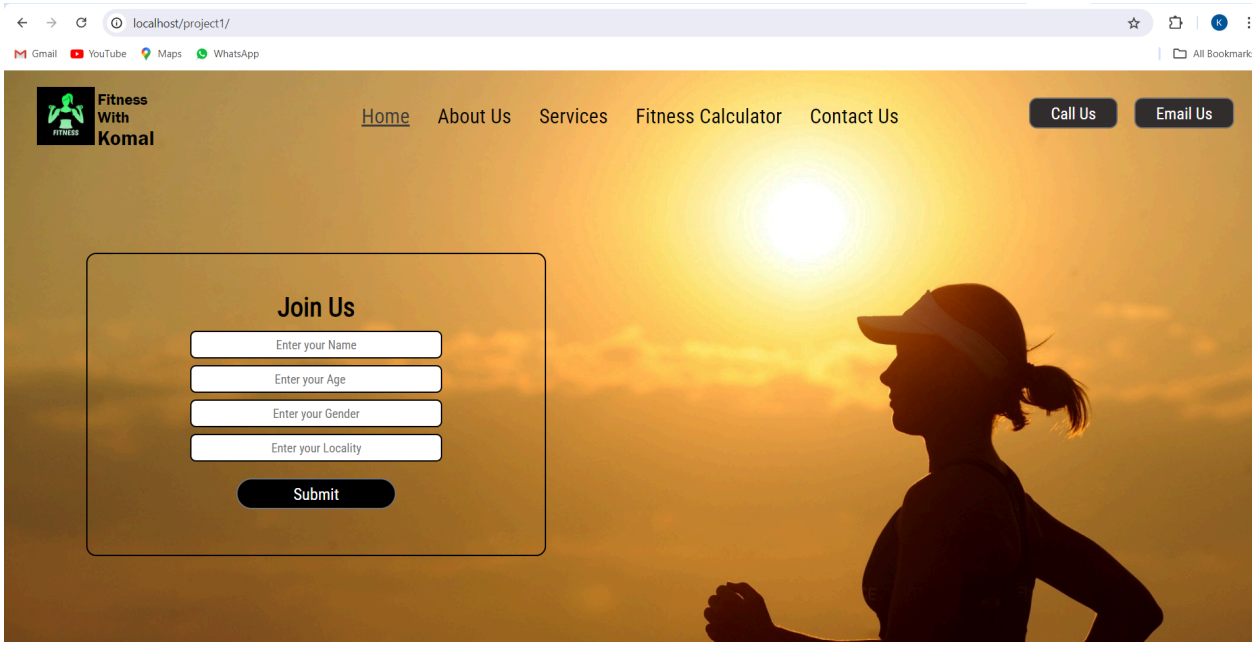
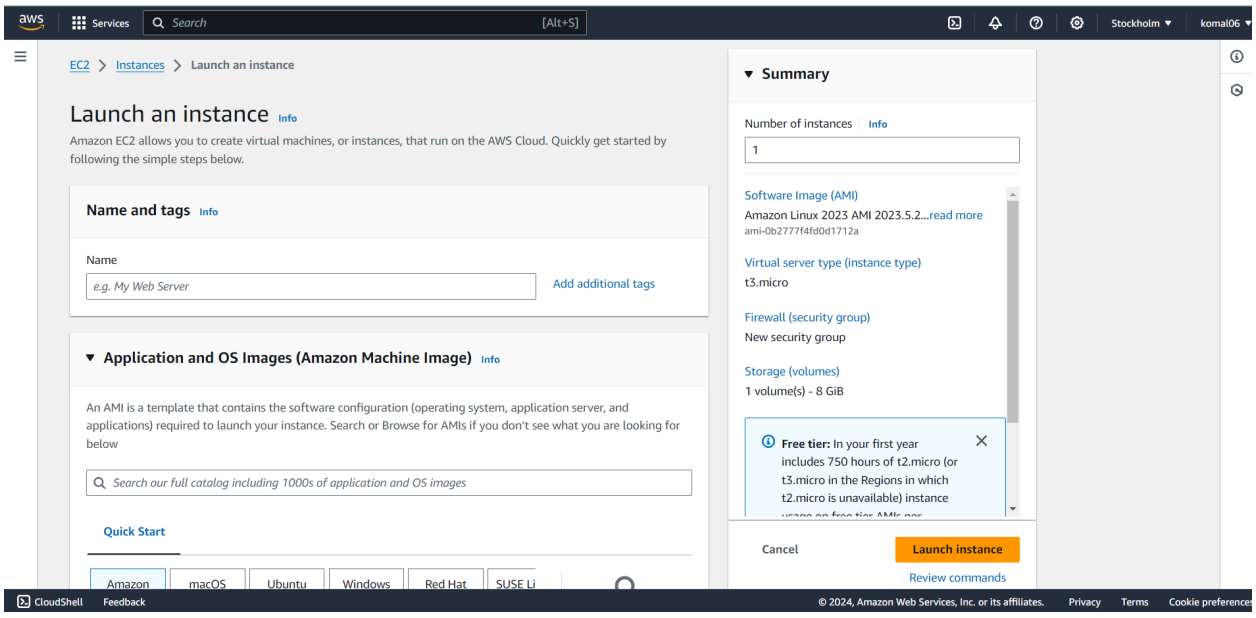
Experiment No. 1

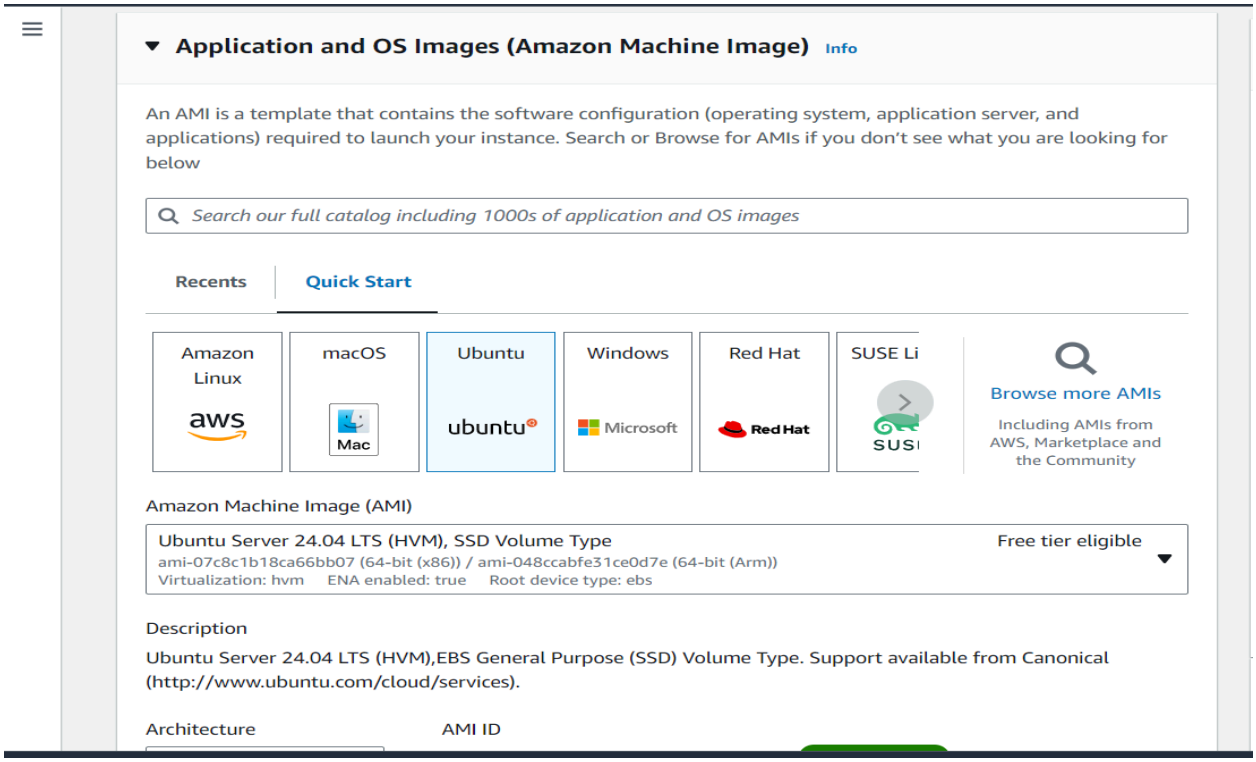


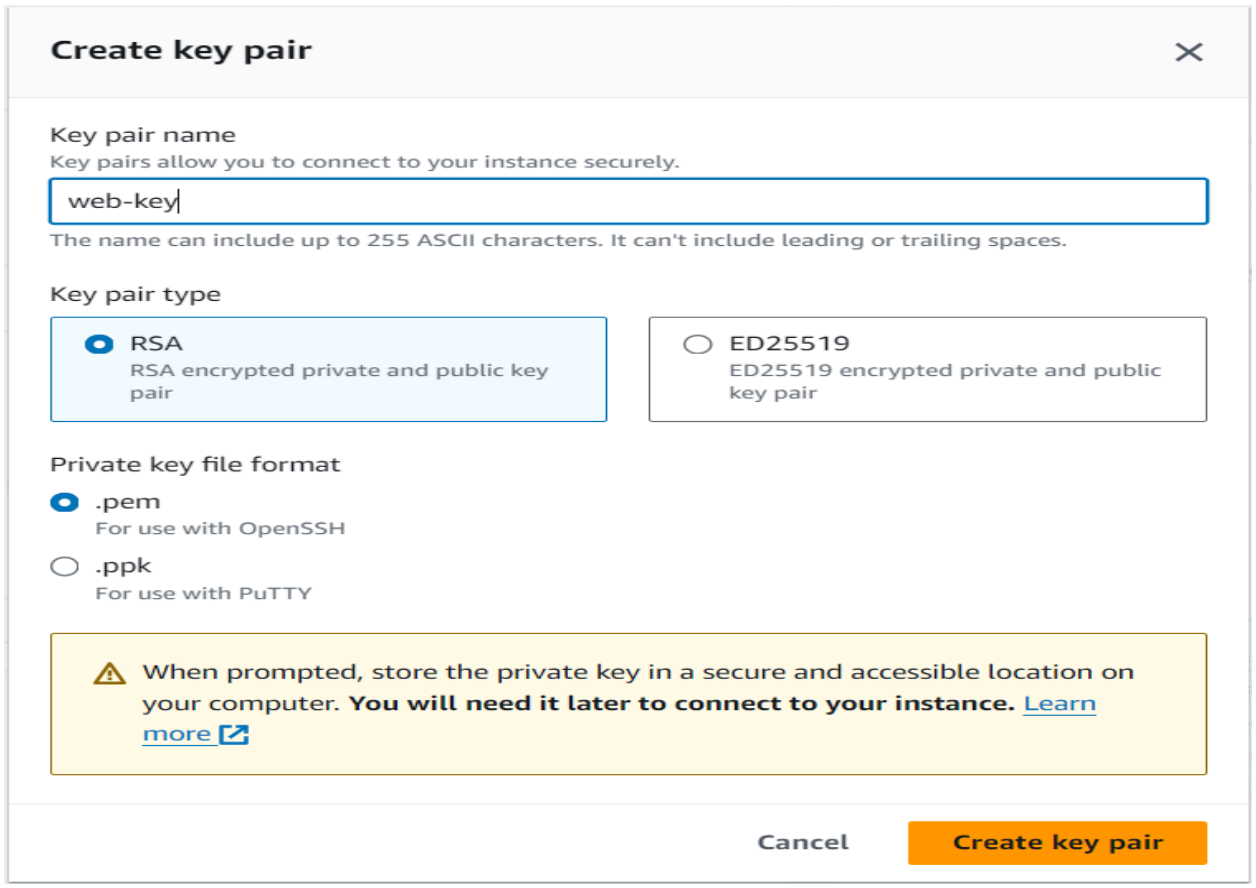


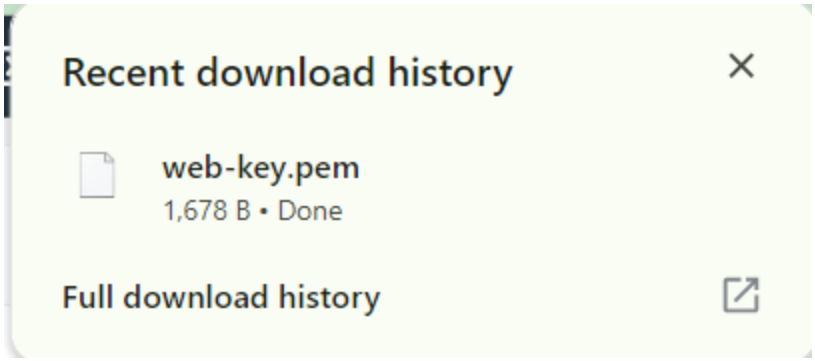


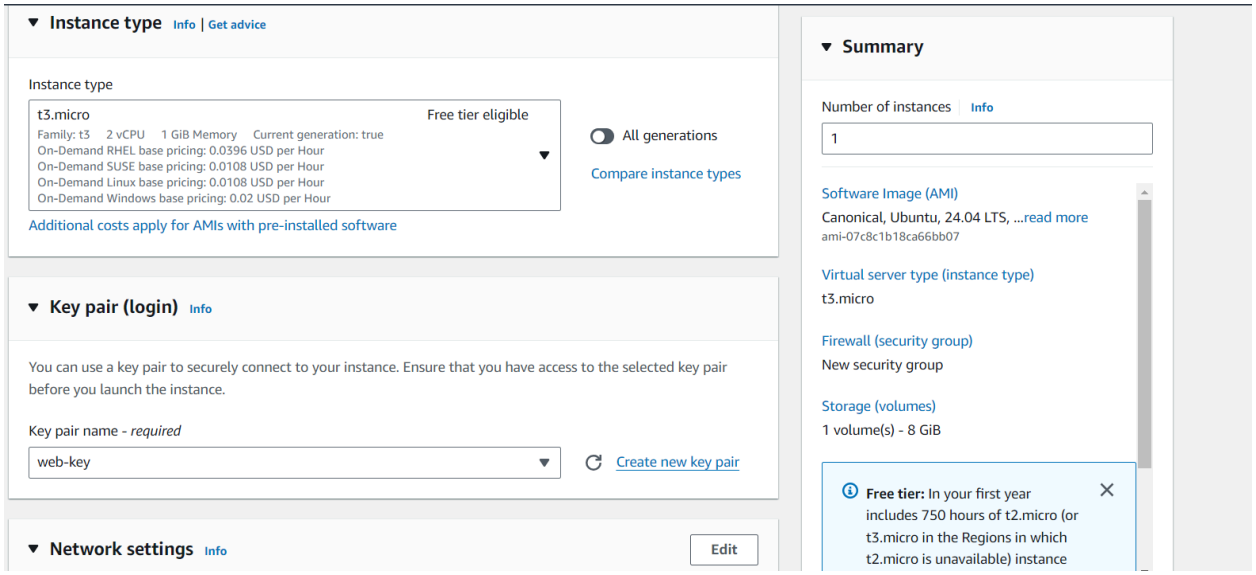
Hosting on AWS

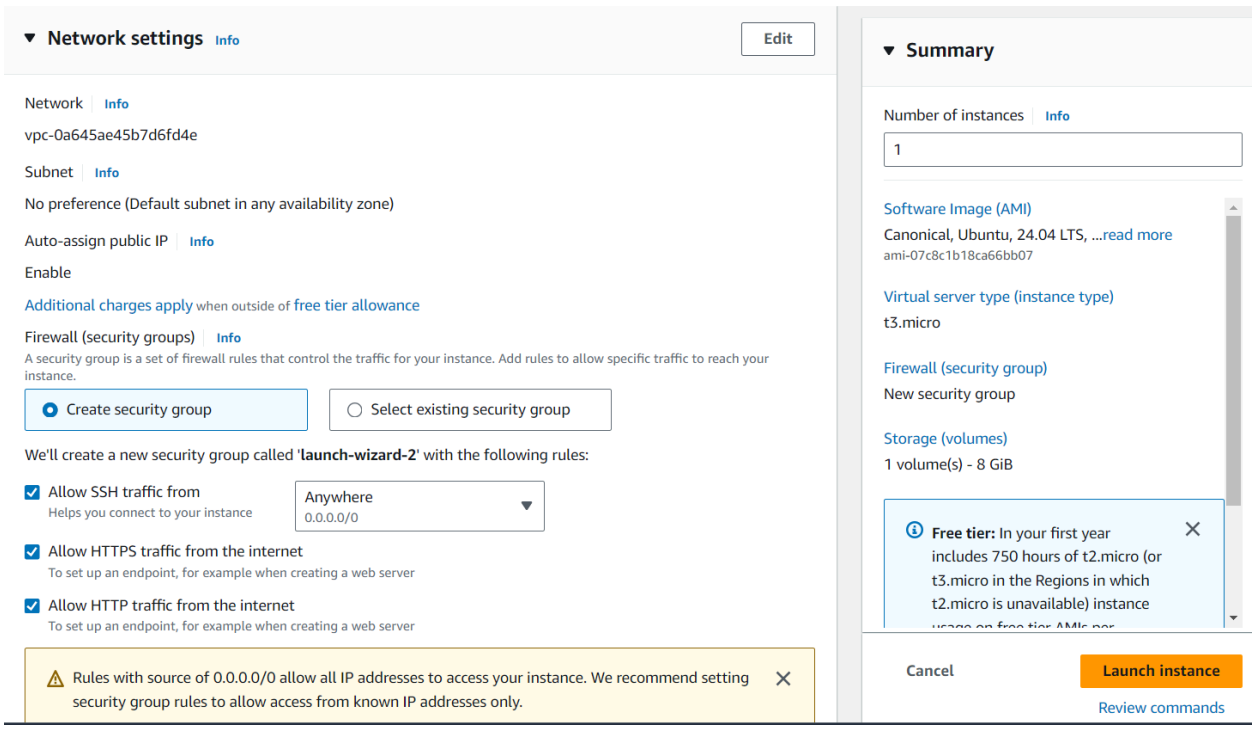


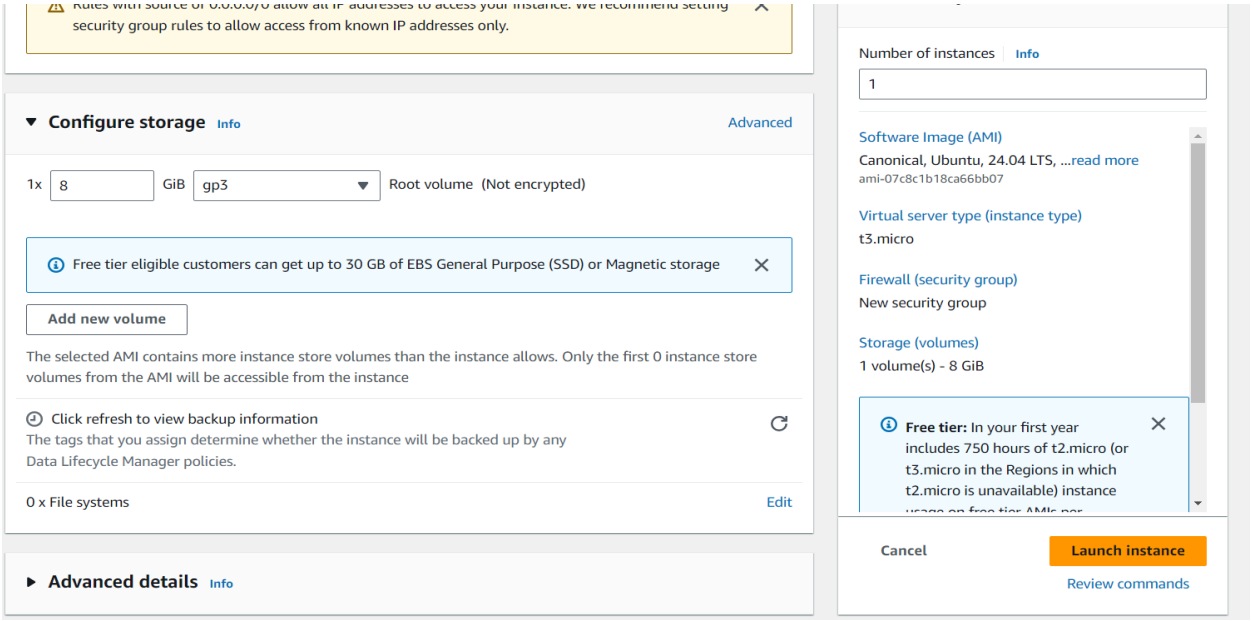

Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Li
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
Free tier eligible
ami-07c8c1b18ca66bb07 (64-bit (x86)) / ami-048ccabfe31ce0d7e (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs
Description
Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).
Architecture
AMI ID

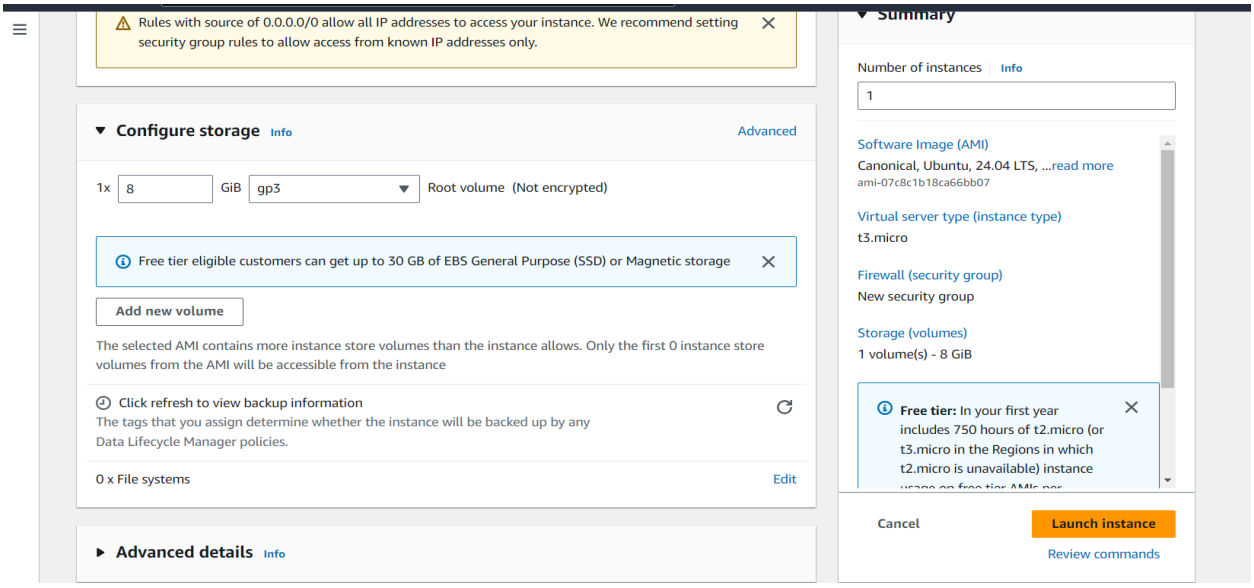

Create key pair
Key pair name
Key pairs allow you to connect to your instance securely.
web-key
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type
RSA
RSA encrypted private and public key pair
ED25519
ED25519 encrypted private and public key pair
Private key file format
.pem
For use with OpenSSH
.ppk
For use with PuTTY
When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. Learn more
Cancel
Create key pair

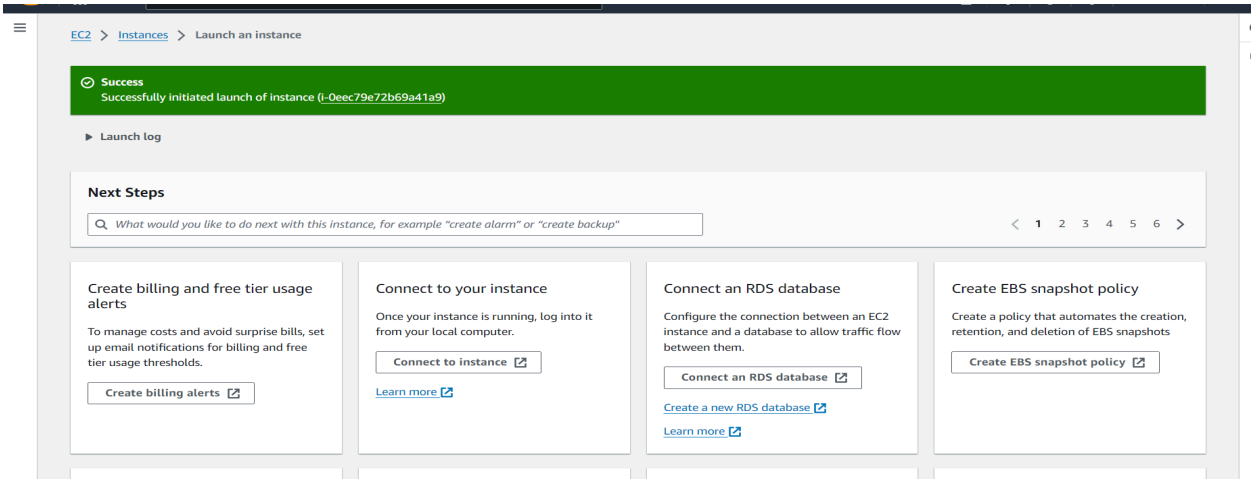

Recent download history
web-key.pem
1,678 B • Done
Full download history

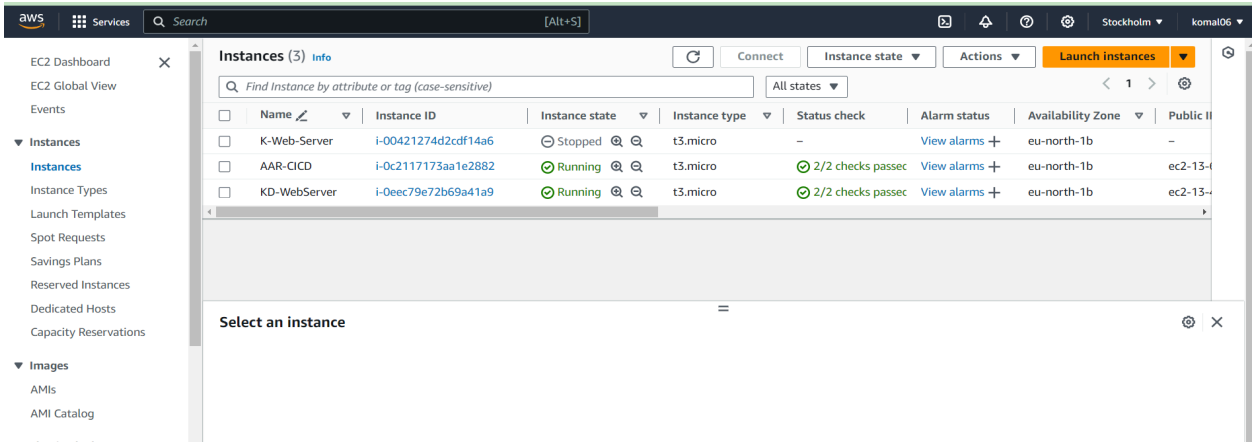

Instance type Info | Get advice
Instance type
t3.micro
Free tier eligible
Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand RHEL base pricing: 0.0396 USD per Hour
On-Demand SUSE base pricing: 0.0108 USD per Hour
On-Demand Linux base pricing: 0.0108 USD per Hour
On-Demand Windows base 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
web-key
Create new key pair
Network settings Info
Edit
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-07c8c1b18ca66bb07
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance

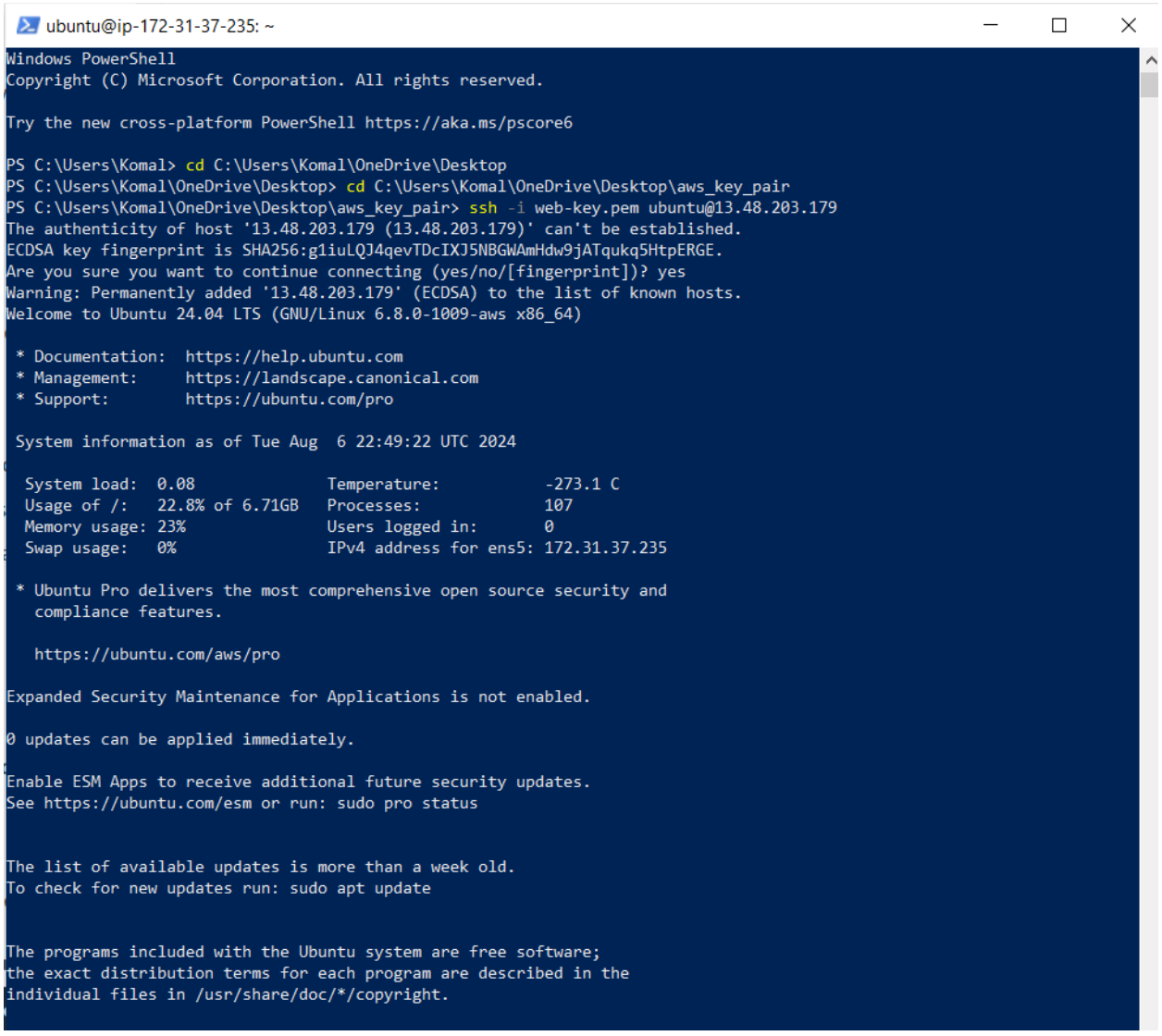

Network settings Info
Edit
Network Info
vpc-0a645ae45b7d6fd4e
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable
Additional charges apply when outside of free tier allowance
Firewall (security groups) Info
A security group is a set of firewall rules 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-2' 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.
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-07c8c1b18ca66bb07
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance
Cancel
Launch instance
Review commands

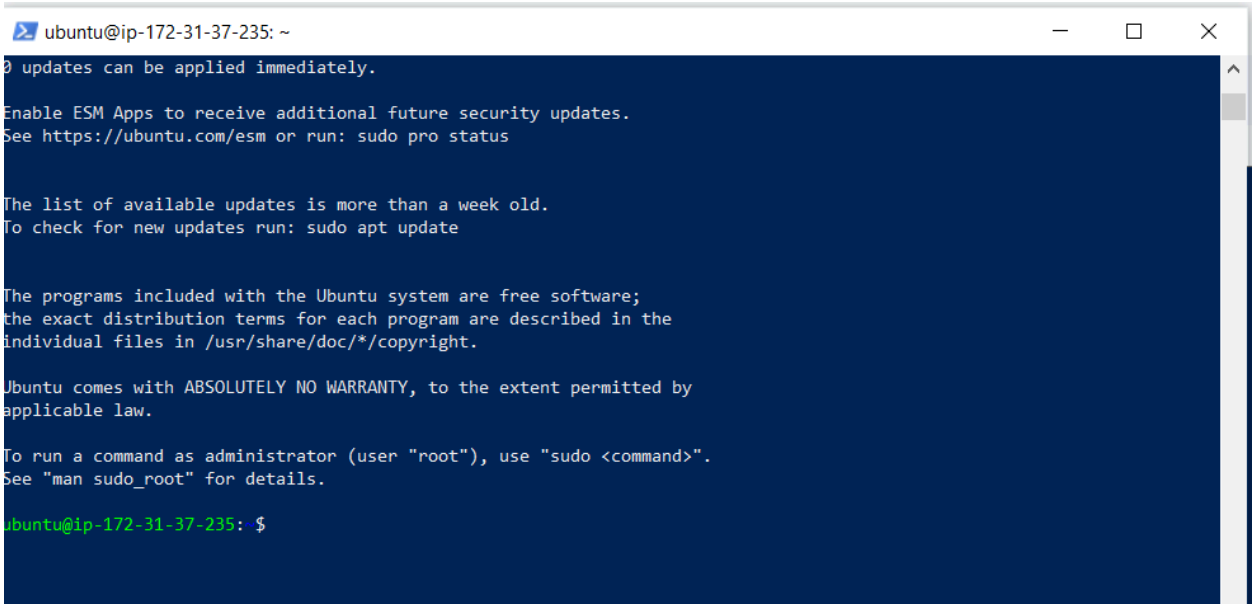

security group rules to allow access from known IP addresses only.
Configure storage Info
Advanced
1x 8 GiB gp3 Root volume (Not encrypted)
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage
Add new volume
The selected AMI contains more instance store volumes 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-07c8c1b18ca66bb07
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance
Cancel
Launch instance
Review commands

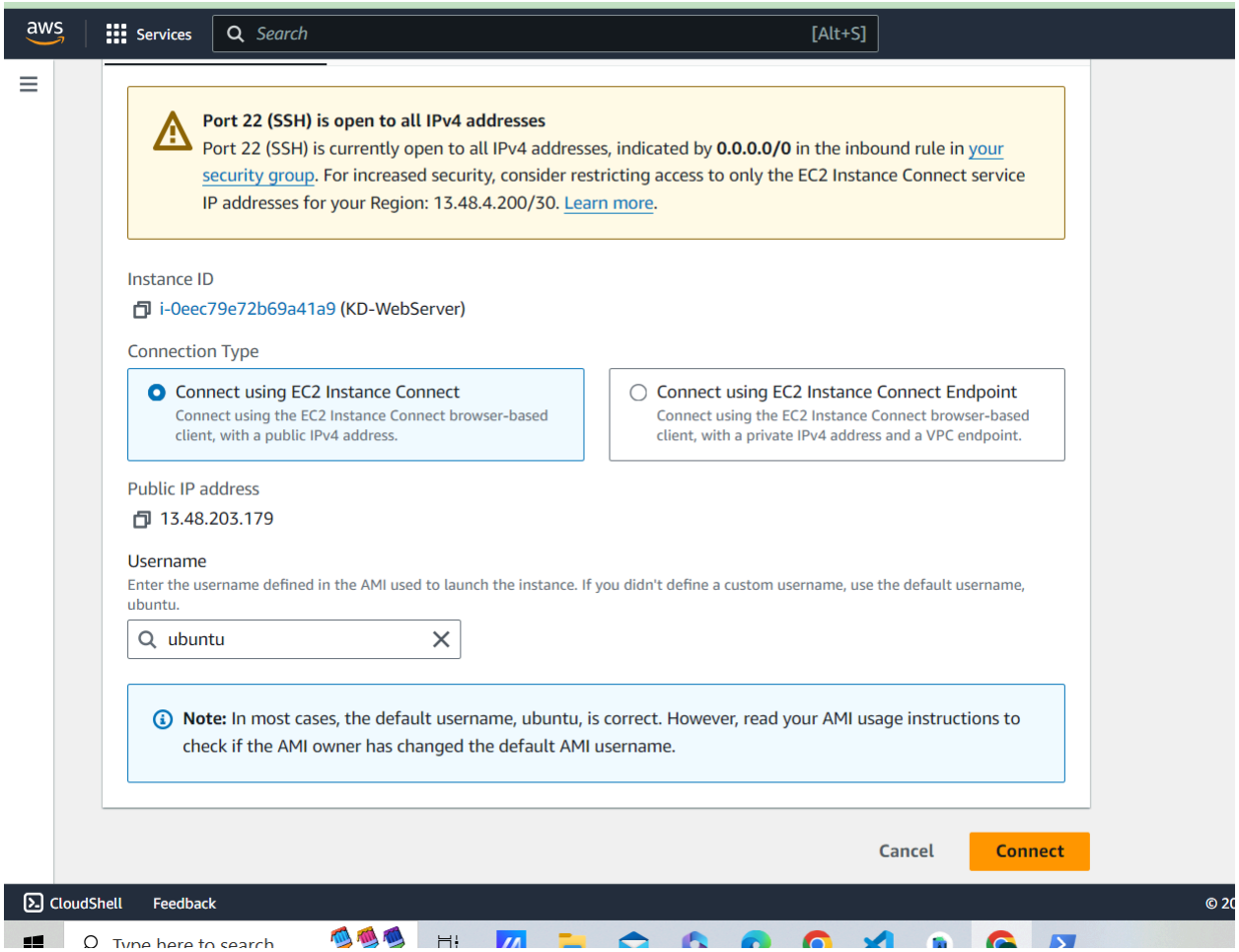

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Configure storage Info
Advanced
1x 8 GiB gp3 Root volume (Not encrypted)
Free tier eligible customers can get up to 30 GB of EBS General 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
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-07c8c1b18ca66bb07
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance
Cancel
Launch instance
Review commands

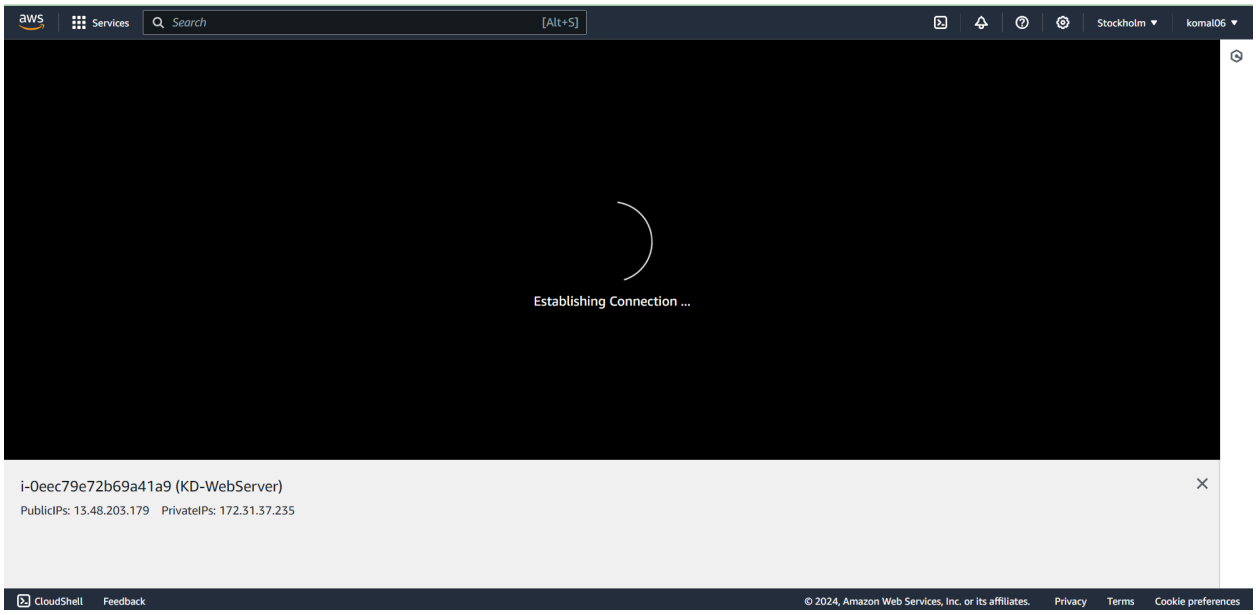

EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-0eec79e72b69a41a9)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
1 2 3 4 5 6
Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
Create billing alerts
Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more
Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy

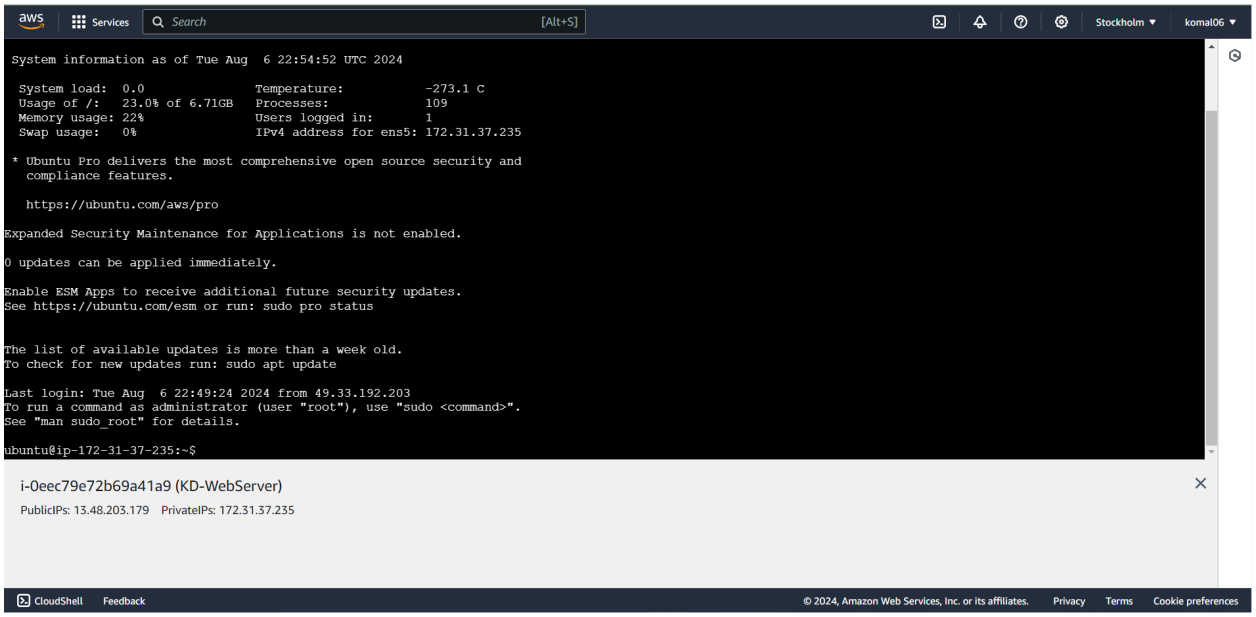

aws
Services
Search
[Alt+S]
Stockholm
komal06
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Instances (3) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
K-Web-Server
i-00421274d2cdf14a6
Stopped
t3.micro
View alarms
eu-north-1b
AAR-CICD
i-0c2117173aa1e2882
Running
t3.micro
2/2 checks passed
View alarms
eu-north-1b
KD-WebServer
i-0eec79e72b69a41a9
Running
t3.micro
2/2 checks passed
View alarms
eu-north-1b
Select an instance

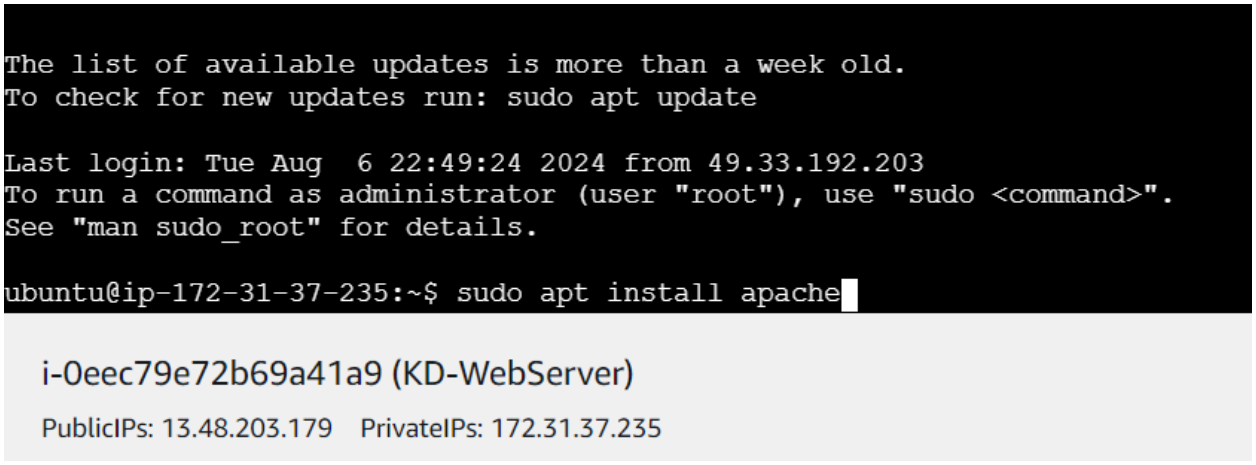

ubuntu@ip-172-31-37-235: ~
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\Komal> cd C:\Users\Komal\OneDrive\Desktop
PS C:\Users\Komal\OneDrive\Desktop> cd C:\Users\Komal\OneDrive\Desktop\aws_key_pair
PS C:\Users\Komal\OneDrive\Desktop\aws_key_pair> ssh -i web-key.pem ubuntu@13.48.203.179
The authenticity of host '13.48.203.179 (13.48.203.179)' can't be established.
ECDSA key fingerprint is SHA256:g1iuLQJ4qevTDcIXJ5NBGWAmHdw9jATqukq5HtpERGE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.48.203.179' (ECDSA) to the list of known hosts.
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 Tue Aug 6 22:49:22 UTC 2024
System load: 0.08
Usage of /: 22.8% of 6.71GB
Memory usage: 23%
Swap usage: 0%
Temperature: -273.1 C
Processes: 107
Users logged in: 0
IPv4 address for ens5: 172.31.37.235
* Ubuntu Pro delivers the most comprehensive open source security and compliance features.
https://ubuntu.com/aws/pro
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@ip-172-31-37-235: ~
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-172-31-37-235:~$


aws
Services
Search
[Alt+S]
Port 22 (SSH) is open to all IPv4 addresses
Port 22 (SSH) is currently open to all IPv4 addresses, indicated by 0.0.0.0/0 in the inbound rule in your security group. For increased security, consider restricting access to only the EC2 Instance Connect service IP addresses for your Region: 13.48.4.200/30. Learn more.
Instance ID
i-0eec79e72b69a41a9 (KD-WebServer)
Connection Type
Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.
Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.
Public IP address
13.48.203.179
Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ubuntu.
ubuntu
Note: In most cases, the default username, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.
Cancel
Connect
CloudShell
Feedback
Type here to search


aws
Services
Search
[Alt+S]
Stockholm
komal06
Establishing Connection ...
i-0eec79e72b69a41a9 (KD-WebServer)
PublicIPs: 13.48.203.179 PrivateIPs: 172.31.37.235
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Stockholm
komal06
System information as of Tue Aug 6 22:54:52 UTC 2024
System load: 0.0
Usage of /: 23.0% of 6.71GB
Memory usage: 22%
Swap usage: 0%
Temperature: -273.1 C
Processes: 109
Users logged in: 1
IPv4 address for ens5: 172.31.37.235
* Ubuntu Pro delivers the most comprehensive open source security and compliance features.
https://ubuntu.com/aws/pro
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
Last login: Tue Aug 6 22:49:24 2024 from 49.33.192.203
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ip-172-31-37-235:~$
i-0eec79e72b69a41a9 (KD-WebServer)
PublicIPs: 13.48.203.179 PrivateIPs: 172.31.37.235
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Tue Aug 6 22:49:24 2024 from 49.33.192.203
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ip-172-31-37-235:~$ sudo apt install apache
i-0eec79e72b69a41a9 (KD-WebServer)
PublicIPs: 13.48.203.179 PrivateIPs: 172.31.37.235

```
E: Unable to locate package apache
ubuntu@ip-172-31-37-235:~$ sudo apt install apache2
```

i-0eec79e72b69a41a9 (KD-WebServer)

PublicIPs: 13.48.203.179 PrivateIPs: 172.31.37.235

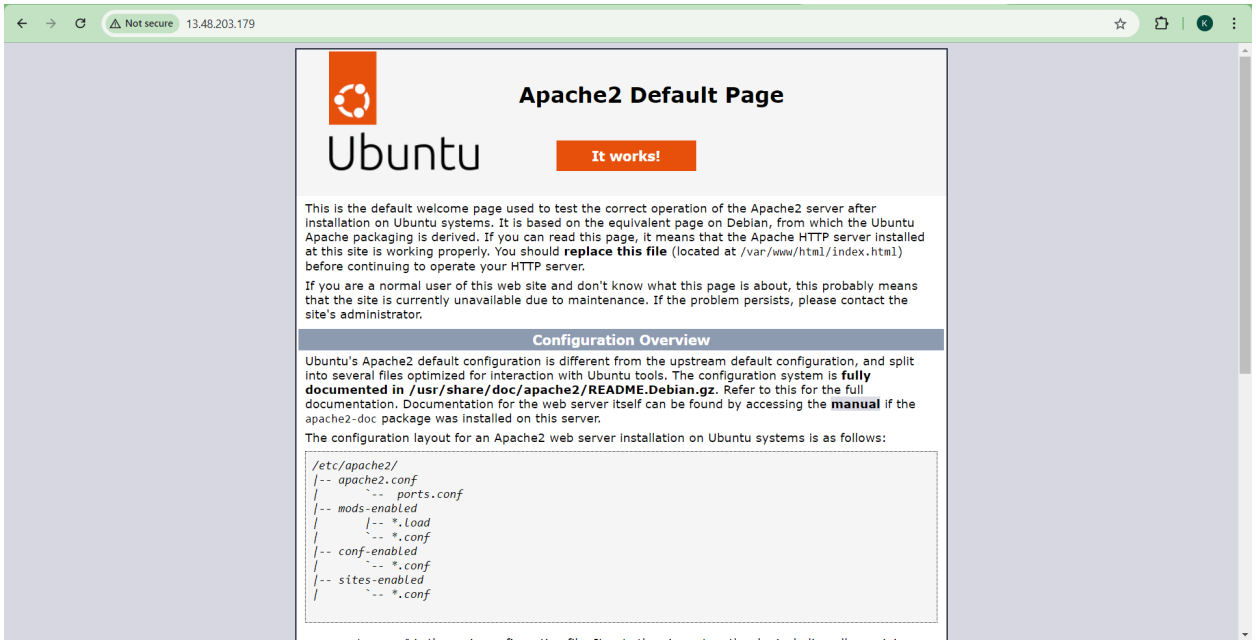
aws Services Search [Alt+S] Stockholm

```
0 upgraded, 10 newly installed, 0 to remove and 0 not upgraded.
Need to get 2080 kB of archives.
After this operation, 8091 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libapr1t64 amd64 1.7.2-3.1build2 [107 kB]
Get:2 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.1ubuntu7 [91.9 kB]
Get:3 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.3-1.1ubuntu7 [11.2 kB]
Get:4 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-ldap amd64 1.6.3-1.1ubuntu7 [9116 B]
Get:5 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 liblua5.4-0 amd64 5.4.6-3build2 [166 kB]
Ign:6 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-bin amd64 2.4.58-1ubuntu8.1
Ign:7 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-data all 2.4.58-1ubuntu8.1
Ign:8 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-utils amd64 2.4.58-1ubuntu8.1
Err:6 http://security.ubuntu.com/ubuntu noble-updates/main amd64 apache2-bin amd64 2.4.58-1ubuntu8.1
  404  Not Found [IP: 13.48.13.7 80]
Ign:9 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2 amd64 2.4.58-1ubuntu8.1
Get:10 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 ssl-cert all 1.1.2ubuntu1 [17.8 kB]
Err:7 http://security.ubuntu.com/ubuntu noble-updates/main amd64 apache2-data all 2.4.58-1ubuntu8.1
  404  Not Found [IP: 13.48.13.7 80]
Err:8 http://security.ubuntu.com/ubuntu noble-updates/main amd64 apache2-utils amd64 2.4.58-1ubuntu8.1
  404  Not Found [IP: 13.48.13.7 80]
Err:9 http://security.ubuntu.com/ubuntu noble-updates/main amd64 apache2 amd64 2.4.58-1ubuntu8.1
  404  Not Found [IP: 13.48.13.7 80]
Fetched 403 kB in 0s (1897 kB/s)
E: Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/a/apache2/apache2-bin_2.4.58-1ubuntu8.1_amd64.deb  404  Not Found [IP: 13.48.13.7 80]
E: Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/a/apache2/apache2-data_2.4.58-1ubuntu8.1_all.deb  404  Not Found [IP: 13.48.13.7 80]
E: Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/a/apache2/apache2-utils_2.4.58-1ubuntu8.1_amd64.deb  404  Not Found [IP: 13.48.13.7 80]
E: Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/a/apache2/apache2_2.4.58-1ubuntu8.1_amd64.deb  404  Not Found [IP: 13.48.13.7 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
ubuntu@ip-172-31-37-235:~$
```

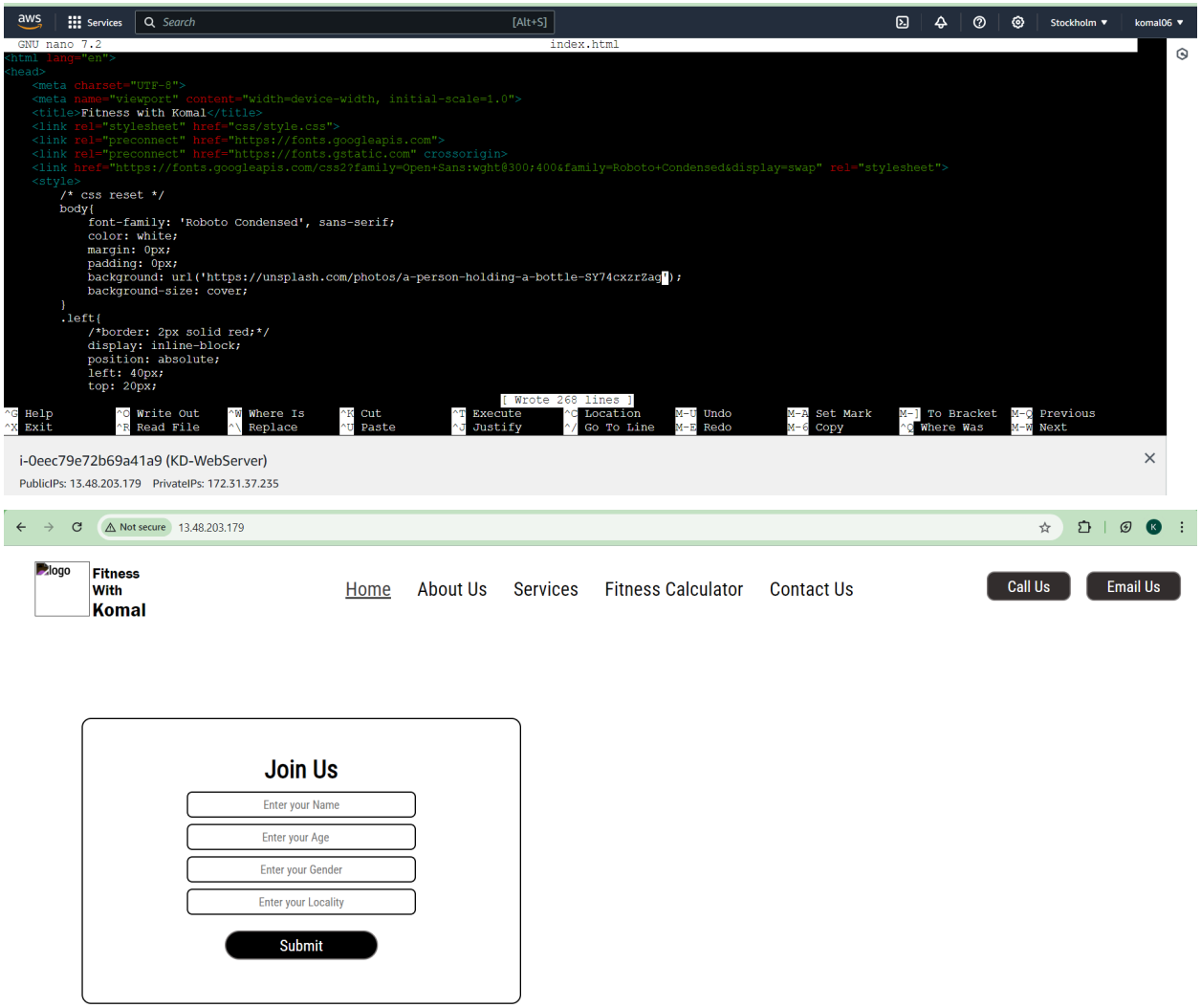
i-0eec79e72b69a41a9 (KD-WebServer)

PublicIPs: 13.48.203.179 PrivateIPs: 172.31.37.235

```
ubuntu@ip-172-31-37-235:~$ ^C
ubuntu@ip-172-31-37-235:~$ sudo apt-get update
Hit:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelea
Reading package lists... Done
ubuntu@ip-172-31-37-235:~$ sudo apt-get upgrade
Reading package lists... Done
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-37-235:~$ sudo apt-get install apache2
Reading package lists... Done
```



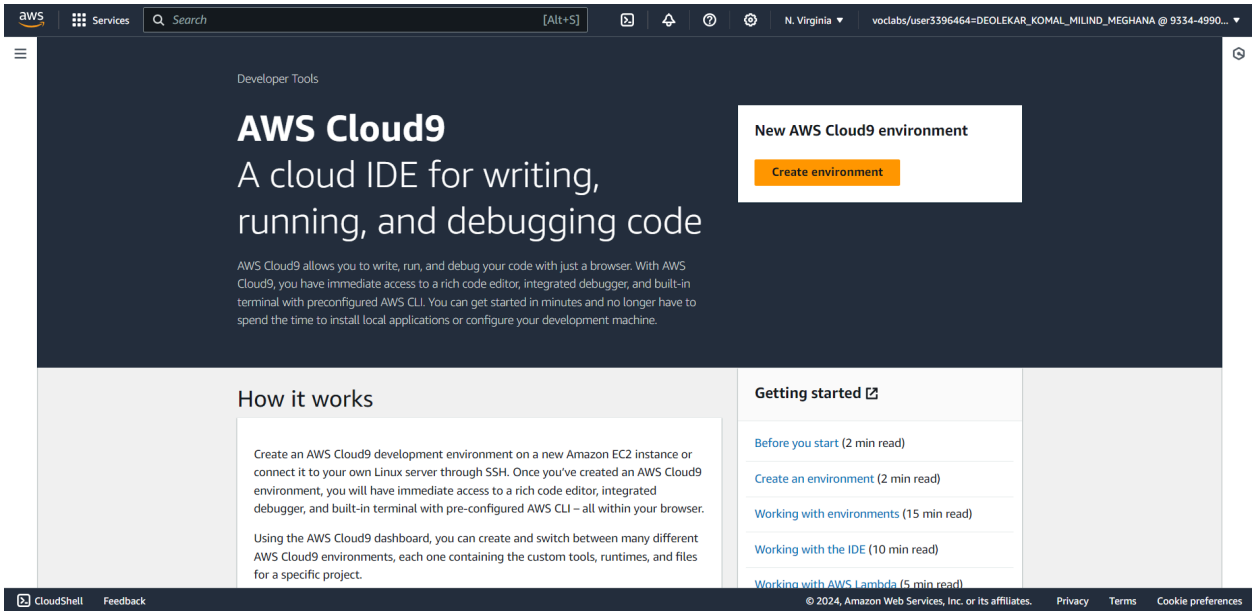

```
Last login: Tue Aug  6 22:54:53 2024 from 13.48.4.203
ubuntu@ip-172-31-37-235:~$ cd /var/www/html
ubuntu@ip-172-31-37-235:/var/www/html$ ls
index.html
ubuntu@ip-172-31-37-235:/var/www/html$ sodo rn index.html
Command 'sodo' not found, did you mean:
  command 'nodo' from snap nodo (master)
  command 'solo' from deb solo1-cli (0.1.1-4)
  command 'todo' from deb devtodo (0.1.20+git20200830.0ad52b0-3)
  command 'sudo' from deb sudo (1.9.14p2-1ubuntu1)
  command 'sudo' from deb sudo-ldap (1.9.14p2-1ubuntu1)
See 'snap info <snapname>' for additional versions.
ubuntu@ip-172-31-37-235:/var/www/html$ sudo rm index.html
ubuntu@ip-172-31-37-235:/var/www/html$
```

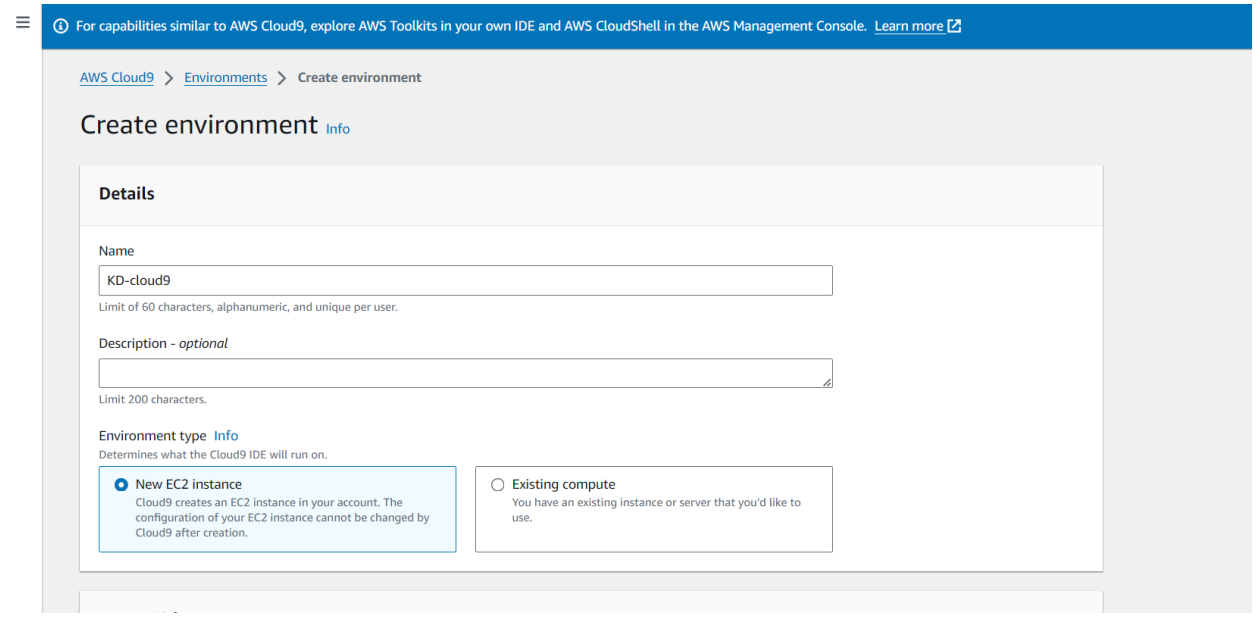

aws
Services
Search
[Alt+S]
Stockholm
komal06
GNU nano 7.2
index.html
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Fitness with Komal</title>
<link rel="stylesheet" href="css/style.css">
<link rel="preconnect" href="https://fonts.googleapis.com">
<link rel="preconnect" href="https://fonts.gstatic.com" crossorigin>
<link href="https://fonts.googleapis.com/css2?family=Open+Sans:wght@300;400&family=Roboto+Condensed&display=swap" rel="stylesheet">
<style>
/* css reset */
body{
font-family: 'Roboto Condensed', sans-serif;
color: white;
margin: 0px;
padding: 0px;
background: url('https://unsplash.com/photos/a-person-holding-a-bottle-SY74cxzrZag');
background-size: cover;
}
.left{
/*border: 2px solid red;*/
display: inline-block;
position: absolute;
left: 40px;
top: 20px;
[Wrote 268 lines]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was M-W Next
i-0eec79e72b69a41a9 (KD-WebServer)
PublicIPs: 13.48.203.179 PrivateIPs: 172.31.37.235

Not secure
13.48.203.179
logo
Fitness
With
Komal
Home
About Us
Services
Fitness Calculator
Contact Us
Call Us
Email Us

Join Us
Enter your Name
Enter your Age
Enter your Gender
Enter your Locality
Submit

Creating Cloud9 Environment





New EC2 instance

Instance type Info

The memory and CPU of the EC2 instance that will be created for Cloud9 to run on.

- (●) t2.micro (1 GiB RAM + 1 vCPU) — Free-tier eligible. Ideal for educational users and exploration.
- ( ) t3.small (2 GiB RAM + 2 vCPU) — Recommended for small web projects.
- ( ) m5.large (8 GiB RAM + 2 vCPU) — Recommended for production and most general-purpose development.
- ( ) Additional instance types — Explore additional instances to fit your need.

Platform Info

This will be installed on your EC2 instance. We recommend Amazon Linux 2023.

Amazon Linux 2

Timeout

How long Cloud9 can be inactive (no user input) before auto-hibernating. This helps prevent unnecessary charges.

30 minutes

Network settings Info

Connection

How your environment is accessed.

- ( ) AWS Systems Manager (SSM) — Accesses environment via SSM without opening inbound ports (no ingress).
- (●) Secure Shell (SSH) — Accesses environment directly via SSH, opens inbound ports.

▼ VPC settings Info

Amazon Virtual Private Cloud (VPC)

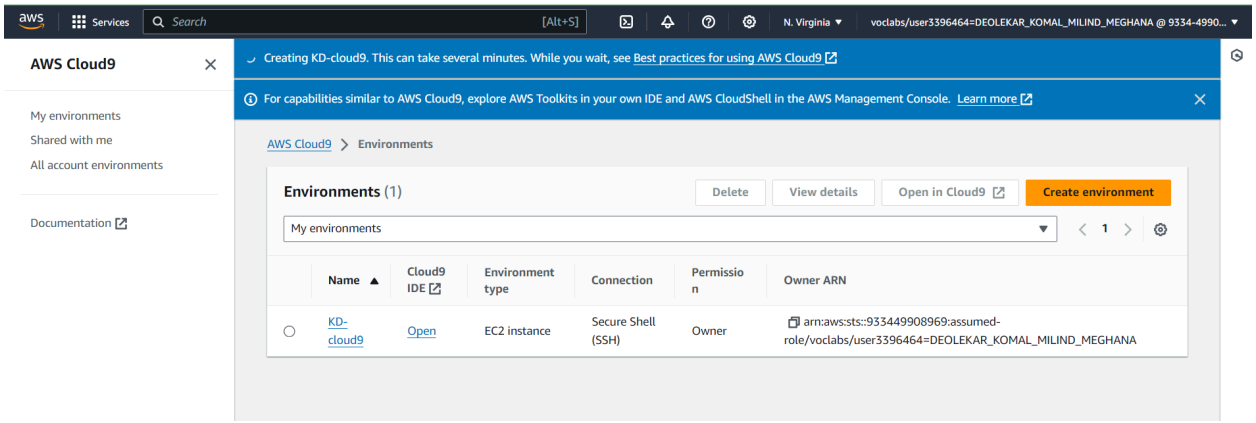
The VPC that your environment will access. To allow the AWS Cloud9 environment to connect to its EC2 instance, attach an internet gateway (IGW) to your VPC. Create new VPC

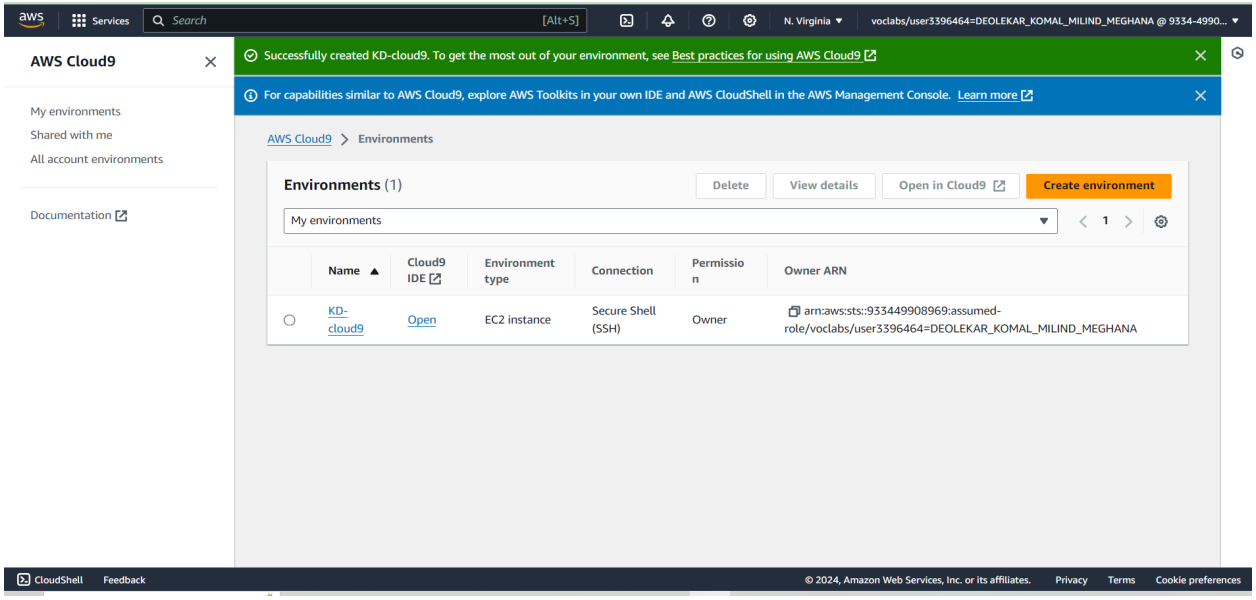
vpc-014f21aed2a85fb2e
Name -

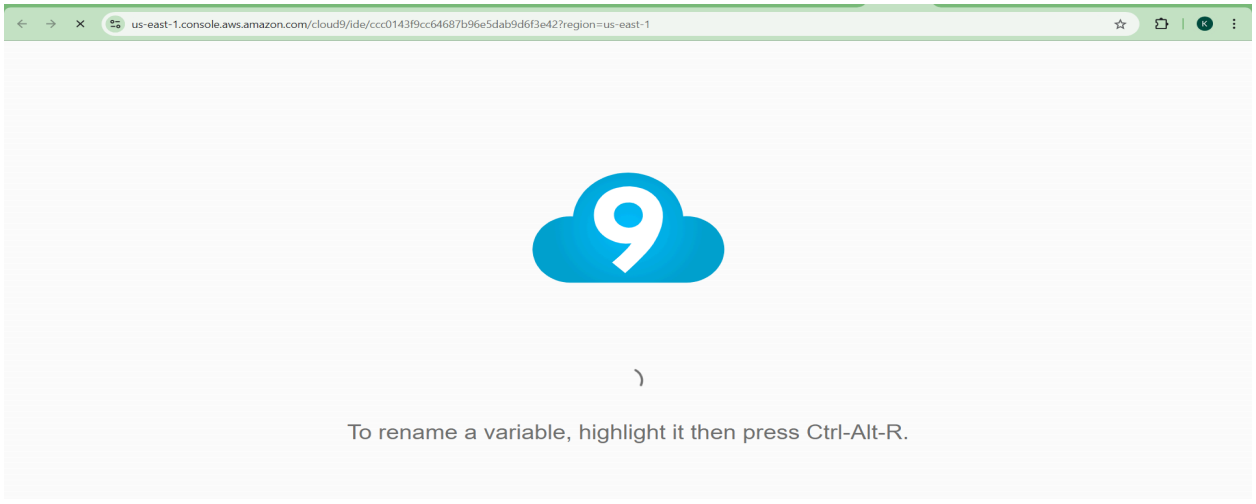
Subnet

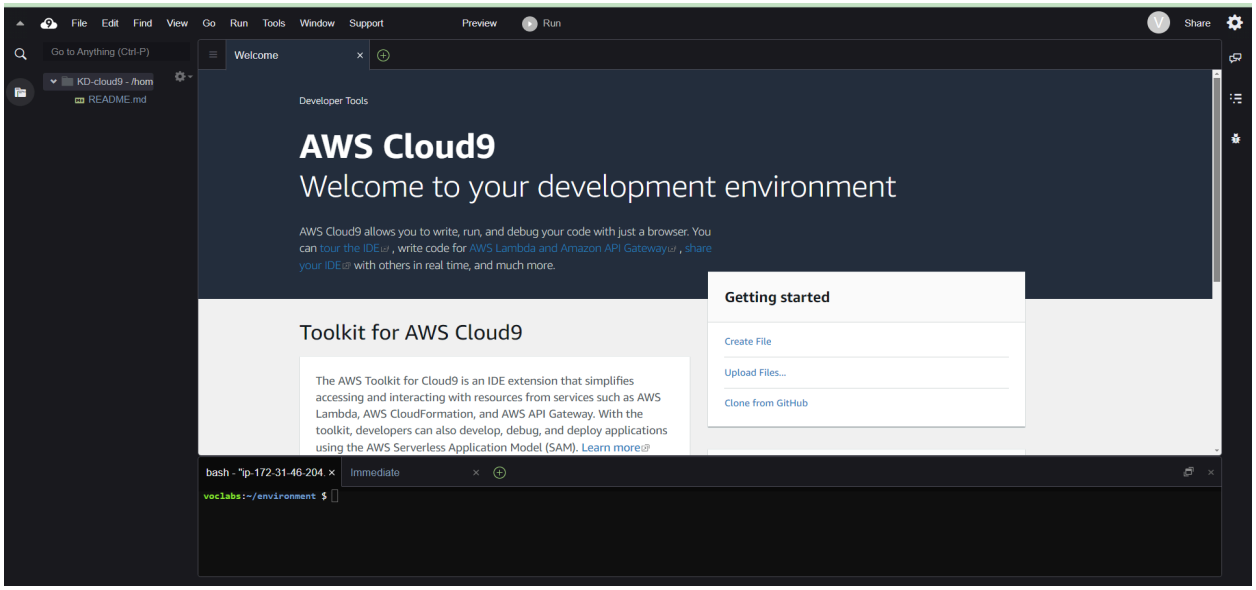
Used to setup your VPC configuration. To use a private subnet, select AWS Systems Manager (SSM) as the connection type. Create new subnet

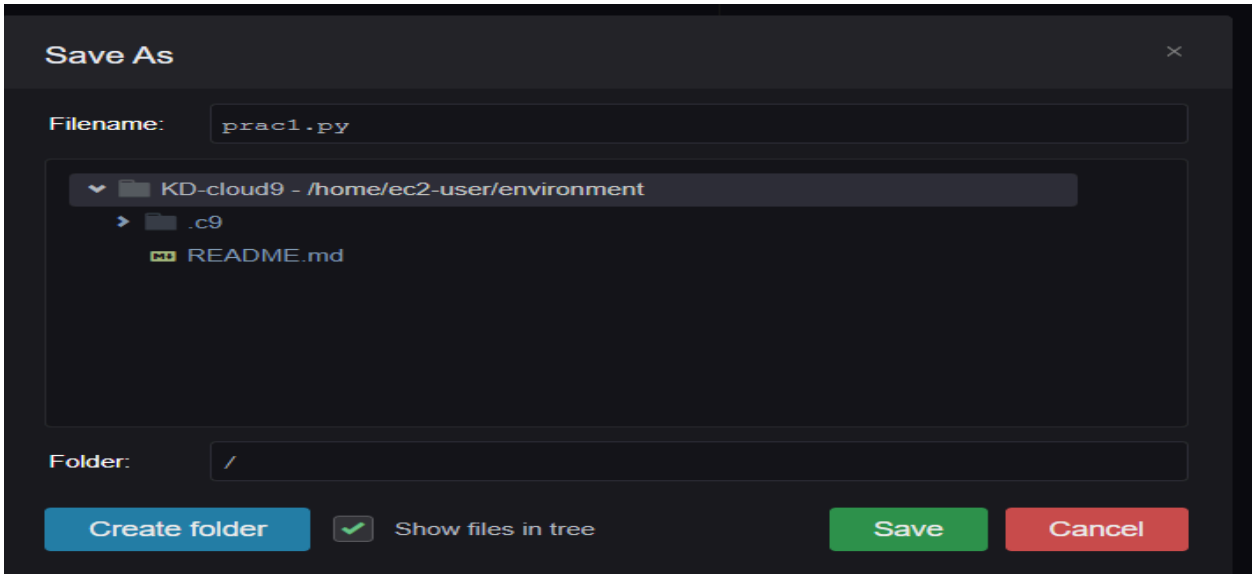
No preference
Uses default subnet in any Availability Zone

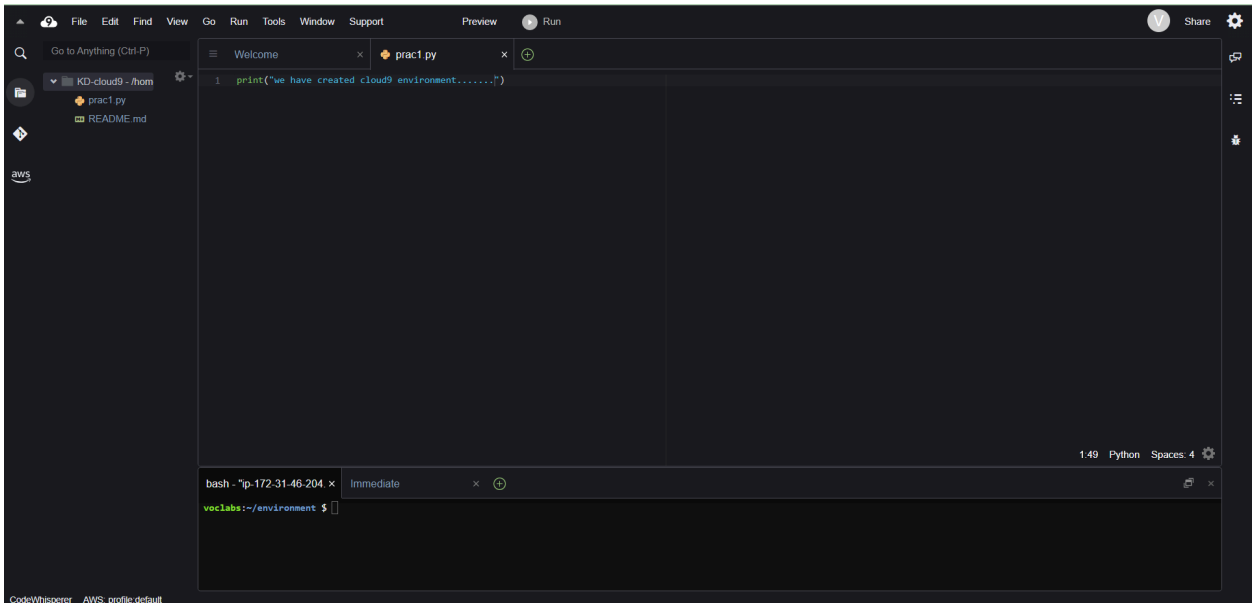


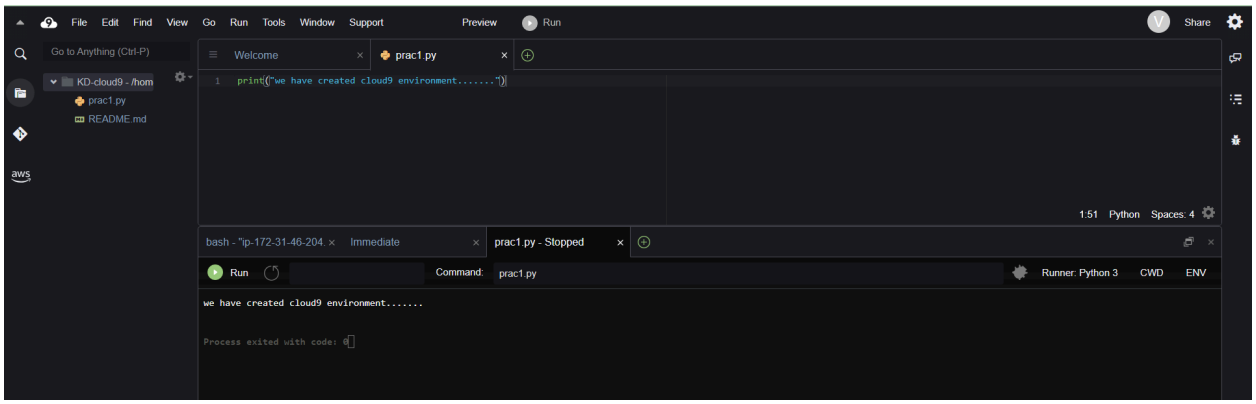

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3396464=DEOLEKAR_KOMAL_MILIND_MEGHANA @ 9334-4990...
AWS Cloud9
My environments
Shared with me
All account environments
Documentation
Successfully created KD-cloud9. To get the most out of your environment, see Best practices for using AWS Cloud9
For capabilities similar to AWS Cloud9, explore AWS Toolkits in your own IDE and AWS CloudShell in the AWS Management Console. Learn more
AWS Cloud9 > Environments
Environments (1)
Delete
View details
Open in Cloud9
Create environment
My environments
Name
Cloud9 IDE
Environment type
Connection
Permission
Owner ARN
KD-cloud9
Open
EC2 instance
Secure Shell (SSH)
Owner
arn:aws:sts::933449908969:assumed-role/voclabs/user3396464=DEOLEKAR_KOMAL_MILIND_MEGHANA
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

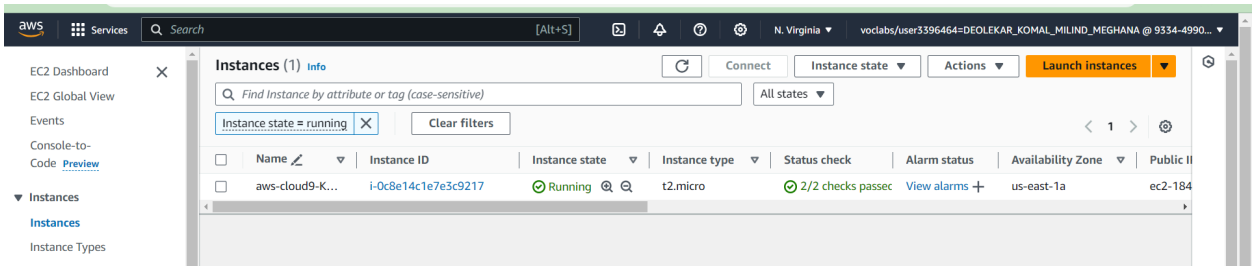

us-east-1.console.aws.amazon.com/cloud9/ide/ccc0143f9cc64687b96e5dab9d6f3e42?region=us-east-1
To rename a variable, highlight it then press Ctrl-Alt-R.


File
Edit
Find
View
Go
Run
Tools
Window
Support
Preview
Run
Share
Go to Anything (Ctrl-P)
KD-cloud9 - /hom
README.md
Welcome
Developer Tools
AWS Cloud9
Welcome to your development environment
AWS Cloud9 allows you to write, run, and debug your code with just a browser. You can tour the IDE, write code for AWS Lambda and Amazon API Gateway, share your IDE with others in real time, and much more.
Getting started
Create File
Upload Files...
Clone from GitHub
Toolkit for AWS Cloud9
The AWS Toolkit for Cloud9 is an IDE extension that simplifies accessing and interacting with resources from services such as AWS Lambda, AWS CloudFormation, and AWS API Gateway. With the toolkit, developers can also develop, debug, and deploy applications using the AWS Serverless Application Model (SAM). Learn more
bash - "ip-172-31-46-204. x
Immediate
voclabs:~/environment $


Save As
Filename:
prac1.py
KD-cloud9 - /home/ec2-user/environment
.c9
README.md
Folder:
/
Create folder
Show files in tree
Save
Cancel

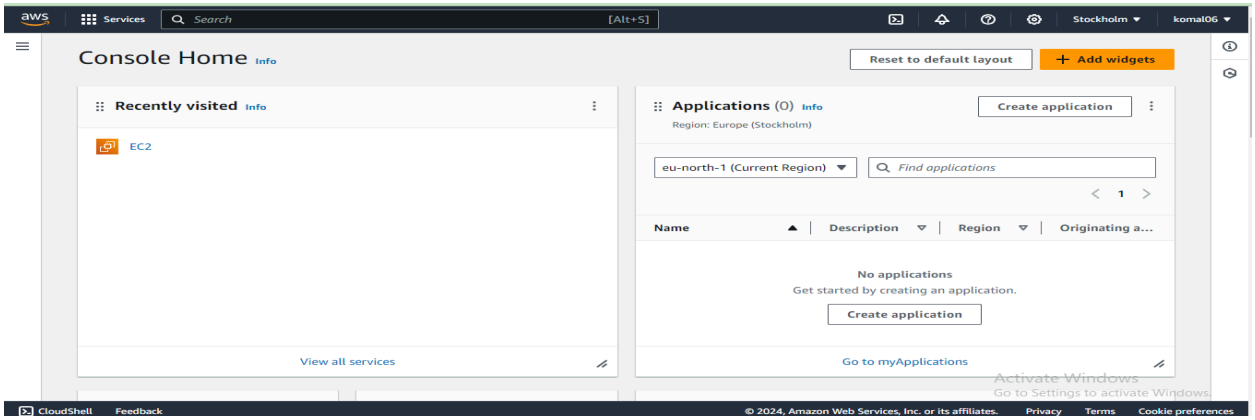

File Edit Find View Go Run Tools Window Support
Preview
Run
Share
Go to Anything (Ctrl-P)
Welcome
prac1.py
KD-cloud9 - /hom
prac1.py
README.md
print("we have created cloud9 environment.....")
1:49 Python Spaces: 4
bash - "ip-172-31-46-204.
Immediate
voclabs:~/environment $
CodeWhisperer AWS: profile:default

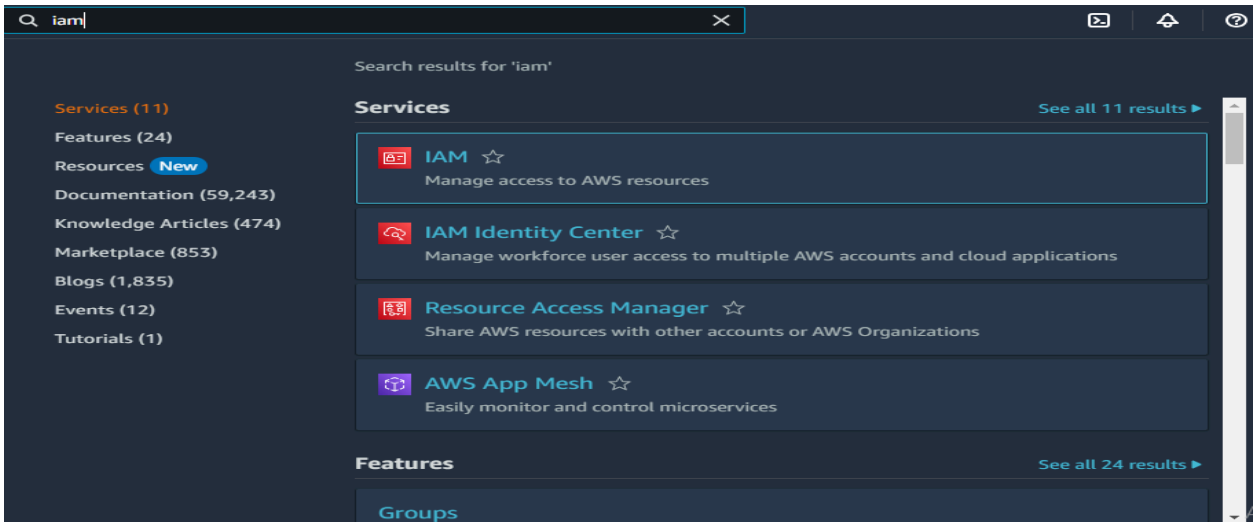

File Edit Find View Go Run Tools Window Support
Preview
Run
Share
Go to Anything (Ctrl-P)
Welcome
prac1.py
KD-cloud9 - /hom
prac1.py
README.md
print("we have created cloud9 environment.....")
1:51 Python Spaces: 4
bash - "ip-172-31-46-204.
Immediate
prac1.py - Stopped
Run
Command: prac1.py
Runner: Python 3
CWD
ENV
we have created cloud9 environment.....
Process exited with code: 0

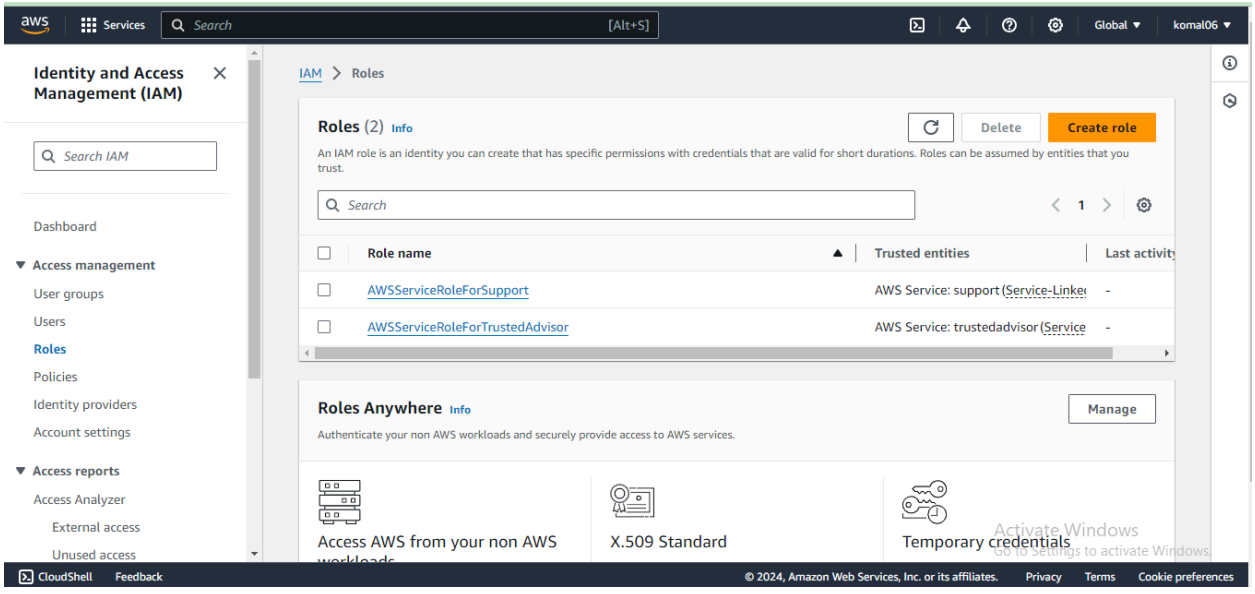

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3396464=DEOLEKAR_KOMAL_MILIND_MEGHANA @ 9334-4990...
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Instances (1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance state = running
Clear filters
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public I
aws-cloud9-K...
i-0c8e14c1e7e3c9217
Running
t2.micro
2/2 checks passec
View alarms
us-east-1a
ec2-184

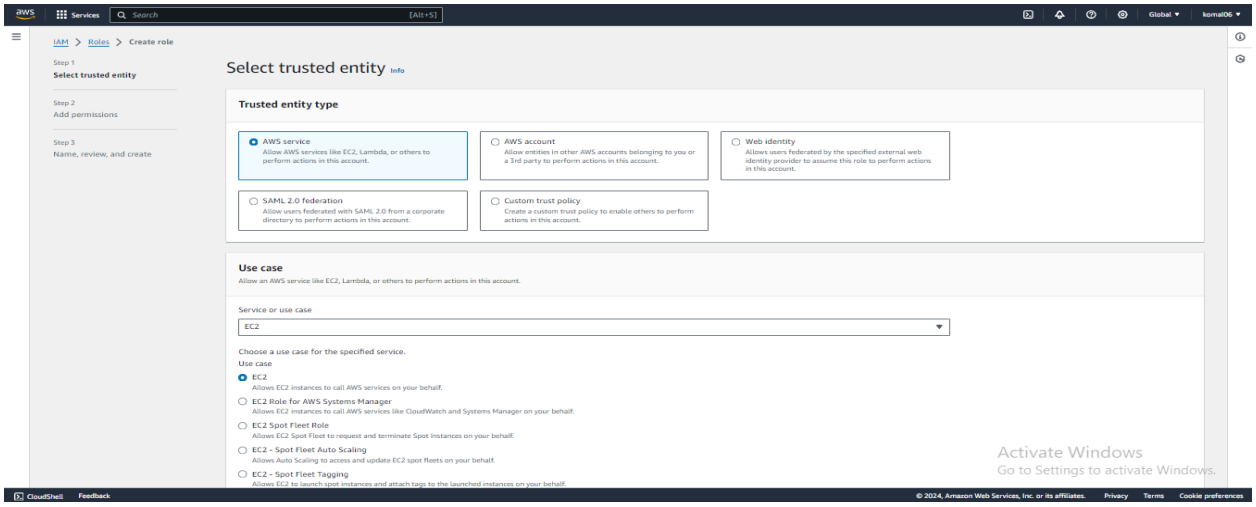
Experiment No.2

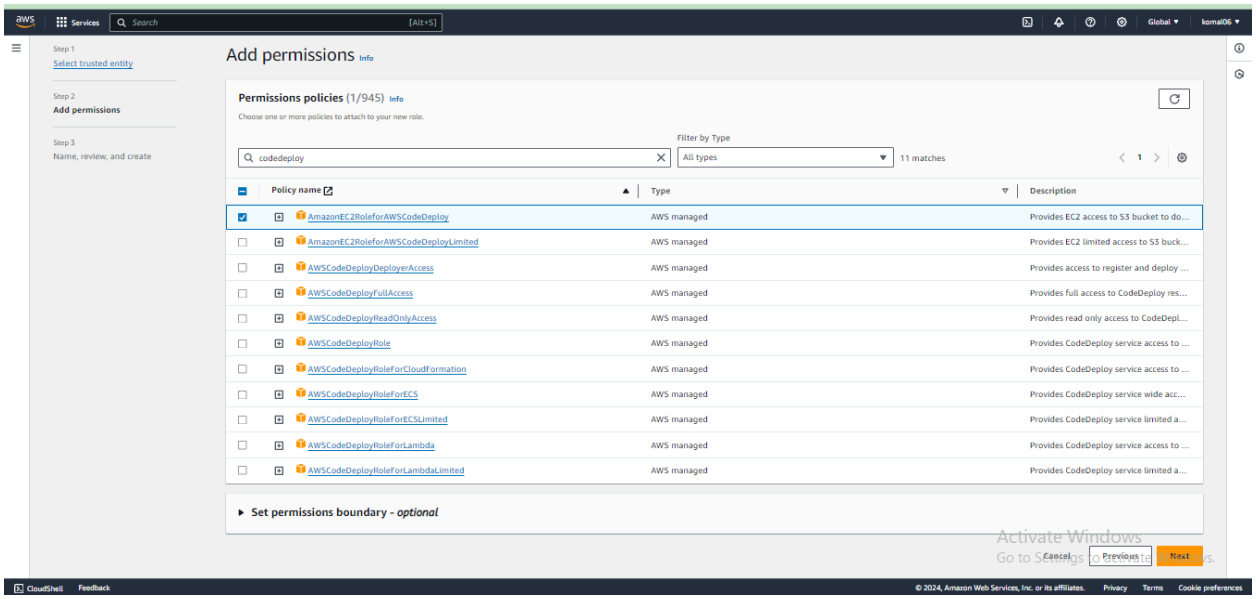
Creating Roles in AWS IAM for CI/CD pipeline setup

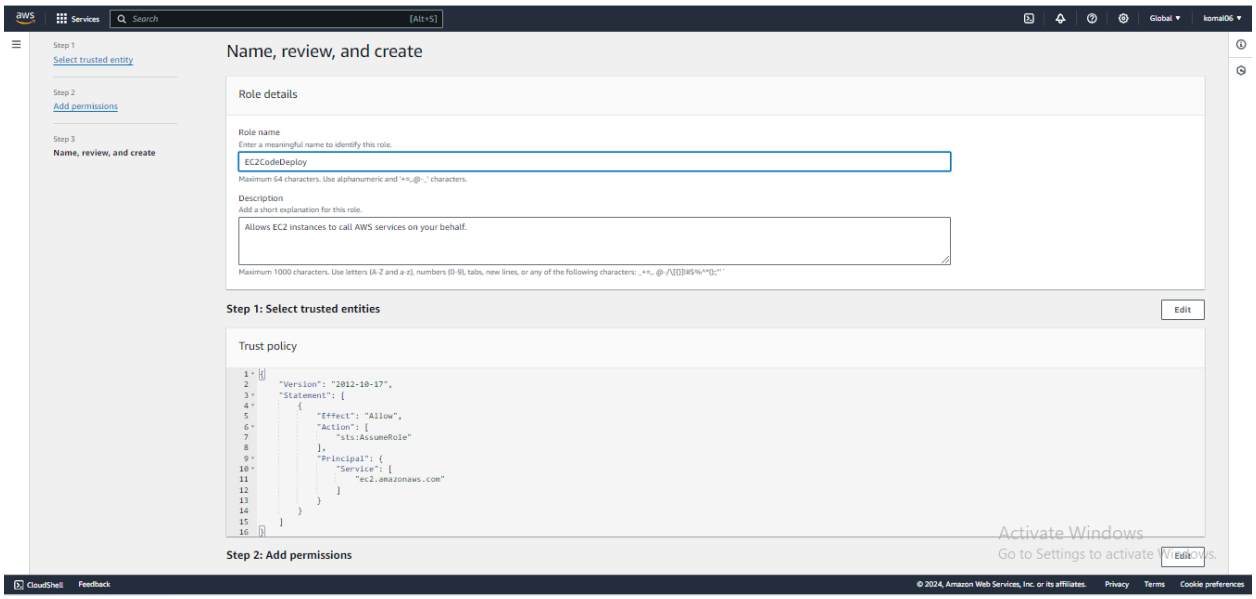


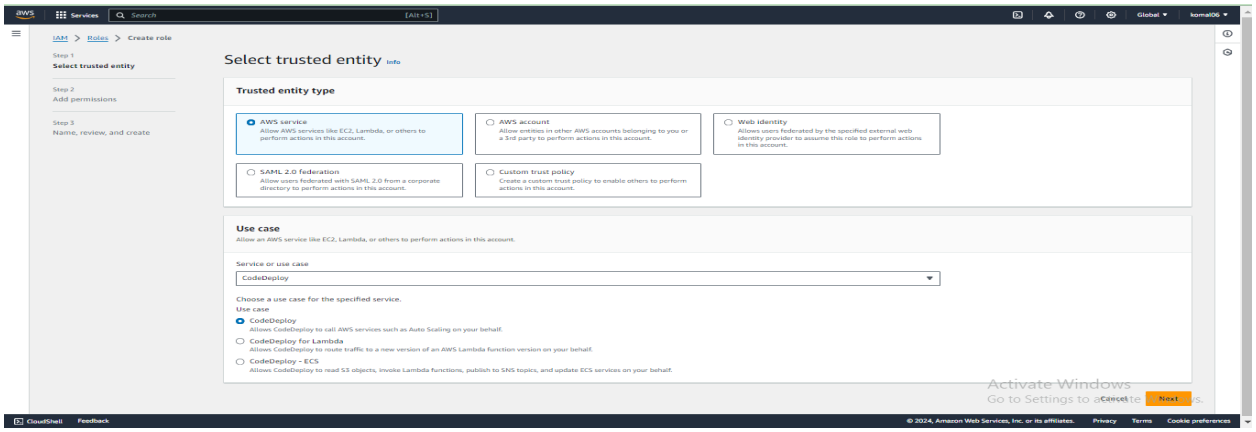


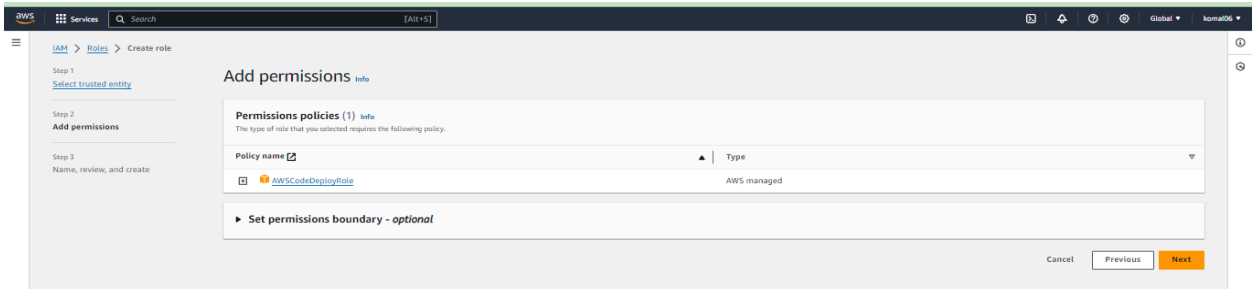


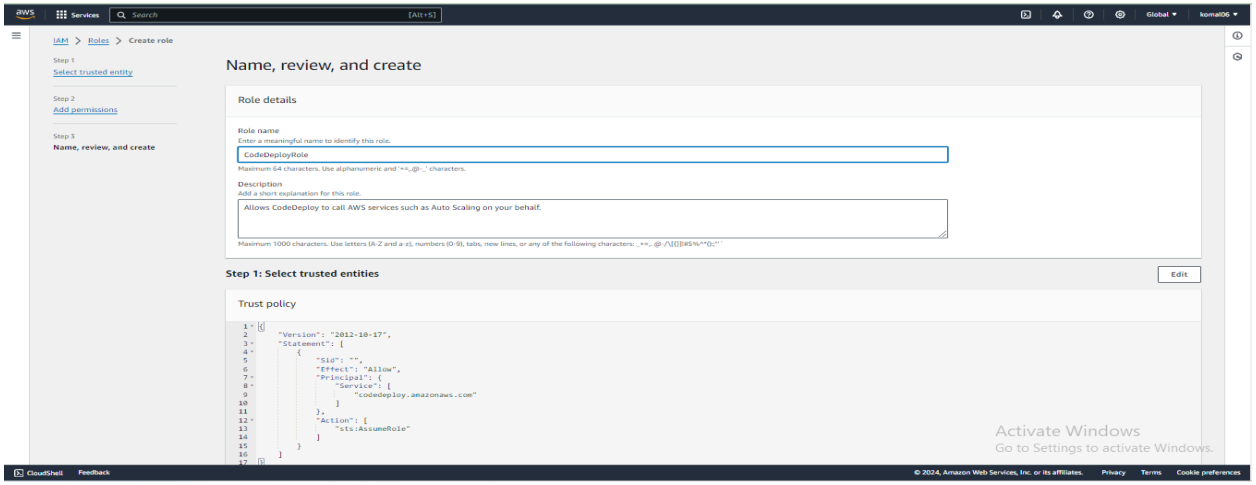

Select trusted entity
Trusted entity type
AWS service
AWS account
Web identity
SAML 2.0 federation
Custom trust policy
Use case
Service or use case
EC2
Choose a use case for the specified service.
EC2
EC2 Role for AWS Systems Manager
EC2 Spot Fleet Role
EC2 - Spot Fleet Auto Scaling
EC2 - Spot Fleet Tagging
Activate Windows
Go to Settings to activate Windows.

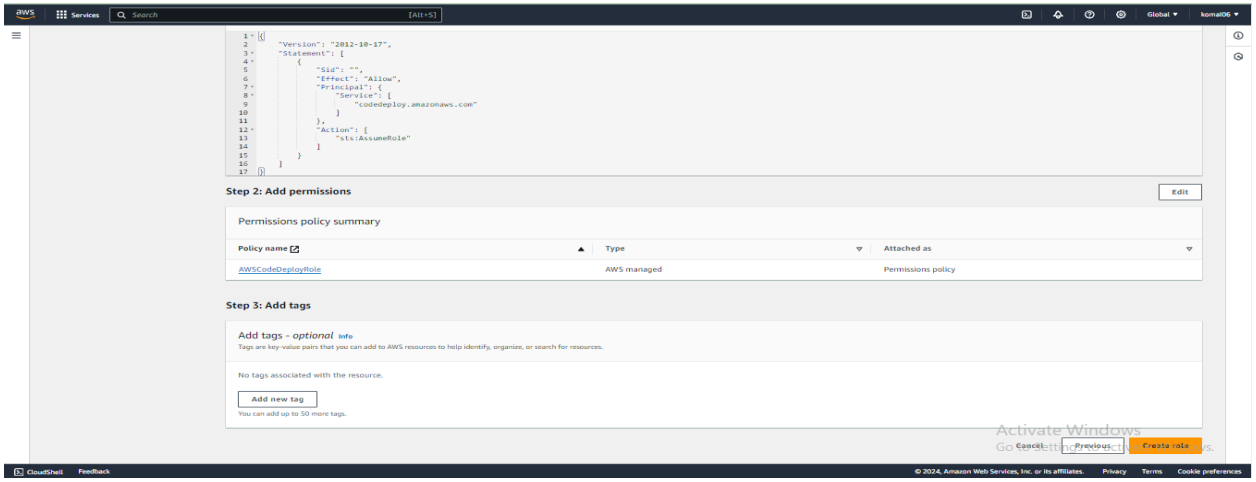

Add permissions
Permissions policies (1/945)
codedeploy
All types
11 matches
Policy name
Type
Description
AmazonEC2RoleforAWSCodeDeploy
AWS managed
Provides EC2 access to S3 bucket to do...
AmazonEC2RoleforAWSCodeDeployLimited
AWS managed
Provides EC2 limited access to S3 buck...
AWSCodeDeployDeployerAccess
AWS managed
Provides access to register and deploy ...
AWSCodeDeployFullAccess
AWS managed
Provides full access to CodeDeploy res...
AWSCodeDeployReadOnlyAccess
AWS managed
Provides read only access to CodeDepl...
AWSCodeDeployRole
AWS managed
Provides CodeDeploy service access to ...
AWSCodeDeployRoleForCloudFormation
AWS managed
Provides CodeDeploy service access to ...
AWSCodeDeployRoleForECS
AWS managed
Provides CodeDeploy service wide acc...
AWSCodeDeployRoleForECSLimited
AWS managed
Provides CodeDeploy service limited a...
AWSCodeDeployRoleForLambda
AWS managed
Provides CodeDeploy service access to ...
AWSCodeDeployRoleForLambdaLimited
AWS managed
Provides CodeDeploy service limited a...
Set permissions boundary - optional
Cancel
Previous
Next
Activate Windows

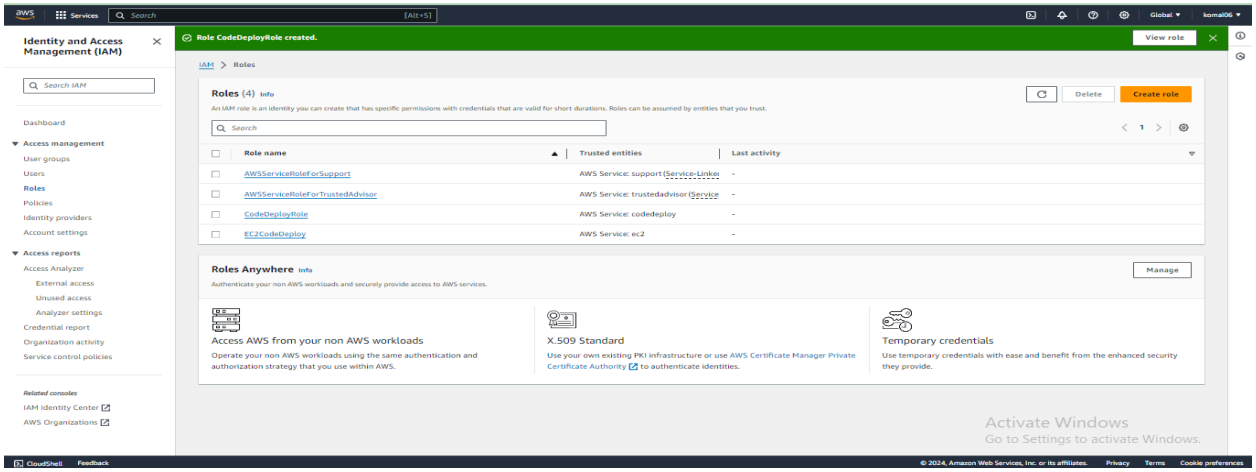

Name, review, and create
Role details
Role name
EC2CodeDeploy
Description
Allows EC2 instances to call AWS services on your behalf.
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"sts:AssumeRole"
],
"Principal": {
"Service": [
"ec2.amazonaws.com"
]
}
}
]
}
Step 2: Add permissions
Edit
Activate Windows


Select trusted entity
Trusted entity type
AWS service
AWS account
Web identity
SAML 2.0 federation
Custom trust policy
Use case
Service or use case
CodeDeploy
CodeDeploy
CodeDeploy for Lambda
CodeDeploy - ECS
Cancel
Next

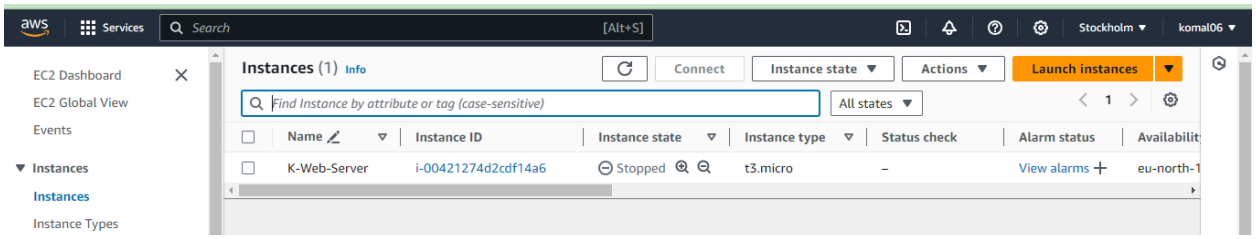

Add permissions
Permissions policies (1)
Policy name
Type
AWSCodeDeployRole
AWS managed
Set permissions boundary - optional
Cancel
Previous
Next

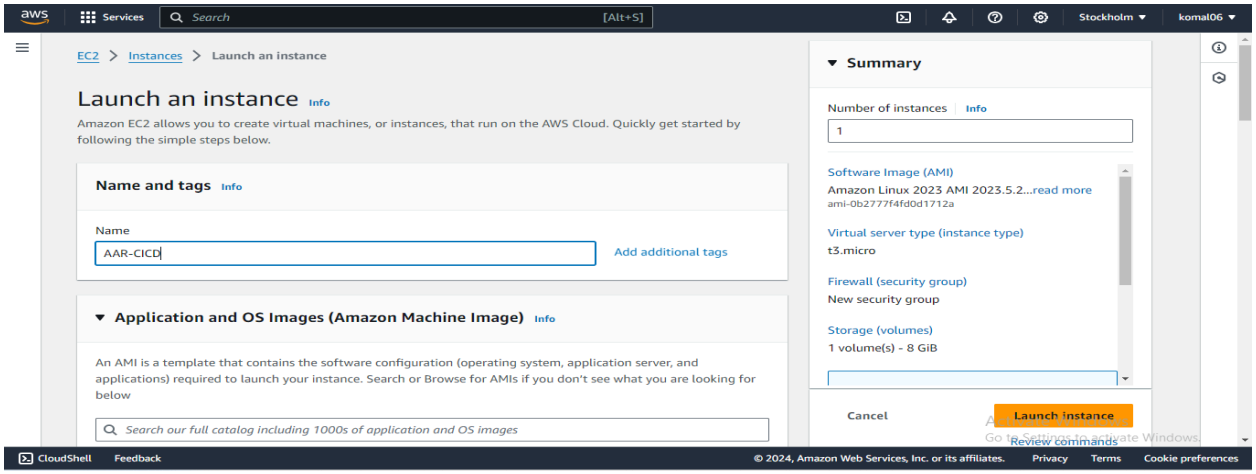

Name, review, and create
Role details
Role name
CodeDeployRole
Description
Allows CodeDeploy to call AWS services such as Auto Scaling on your behalf.
Step 1: Select trusted entities
Edit
Trust policy

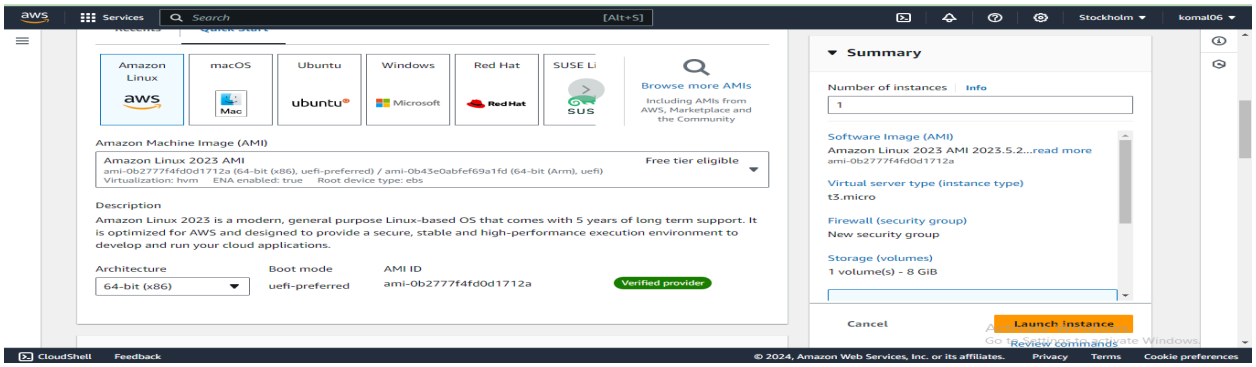

Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
AWSCodeDeployRole
AWS managed
Permissions policy
Step 3: Add tags
Add tags - optional
No tags associated with the resource.
Add new tag
Cancel
Previous
Create role

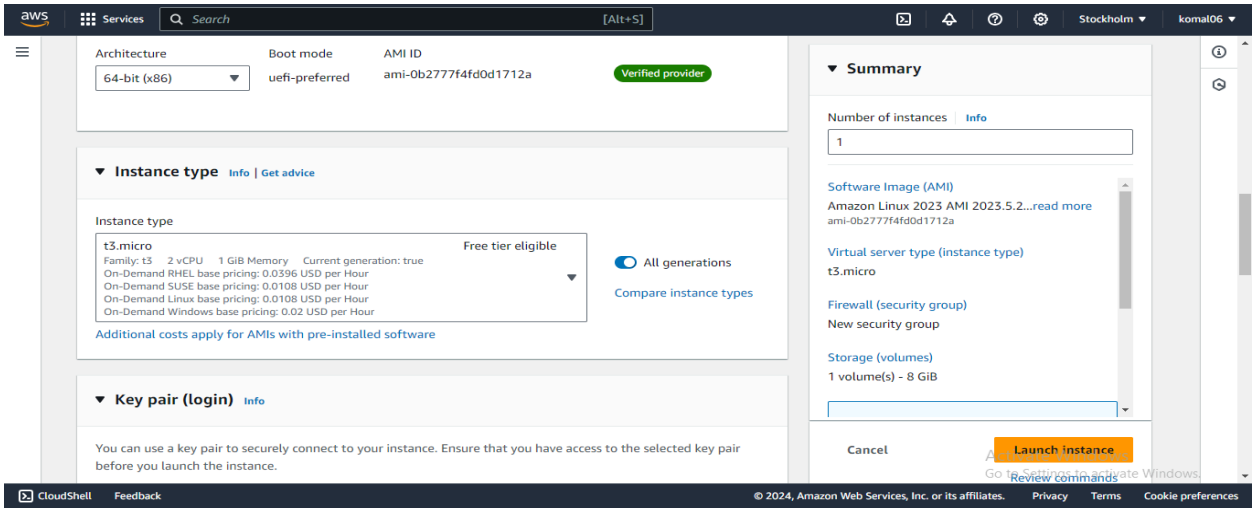


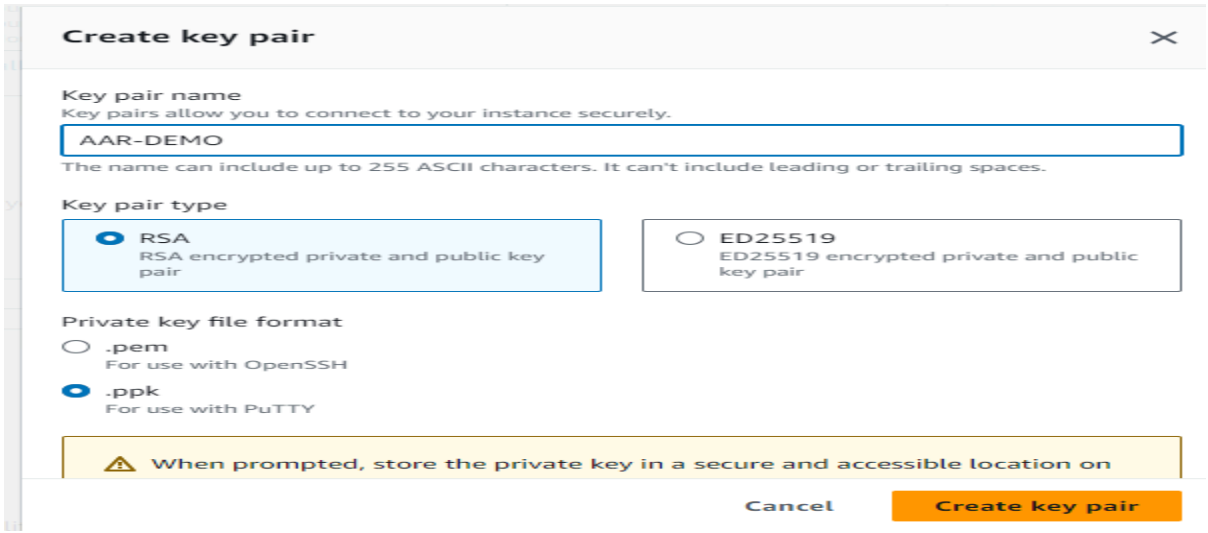
Launching EC2 Instace :

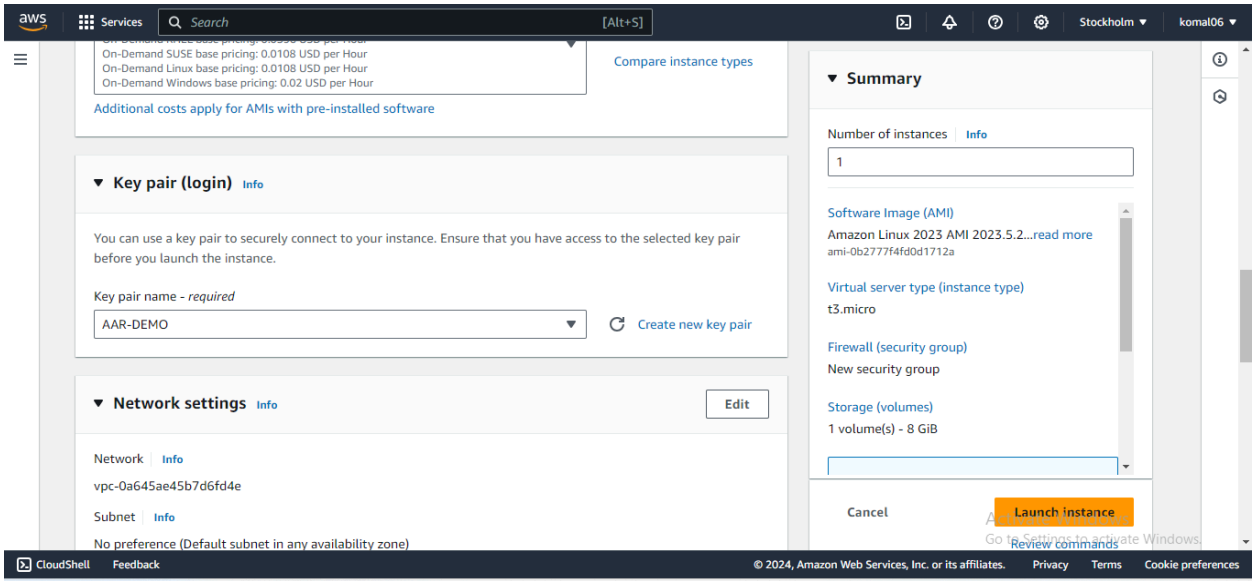


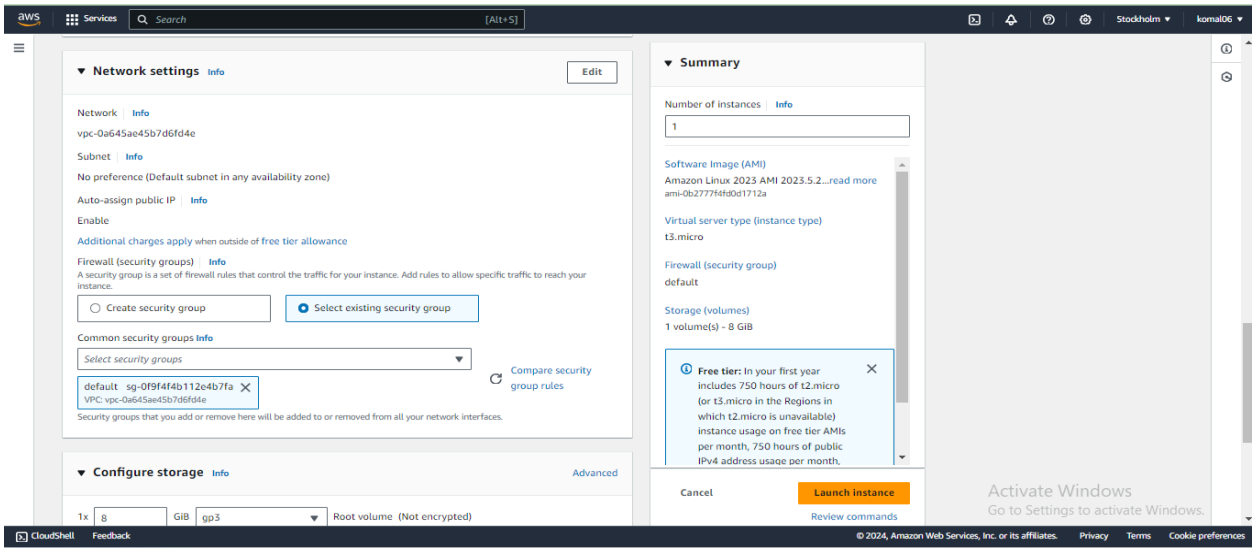


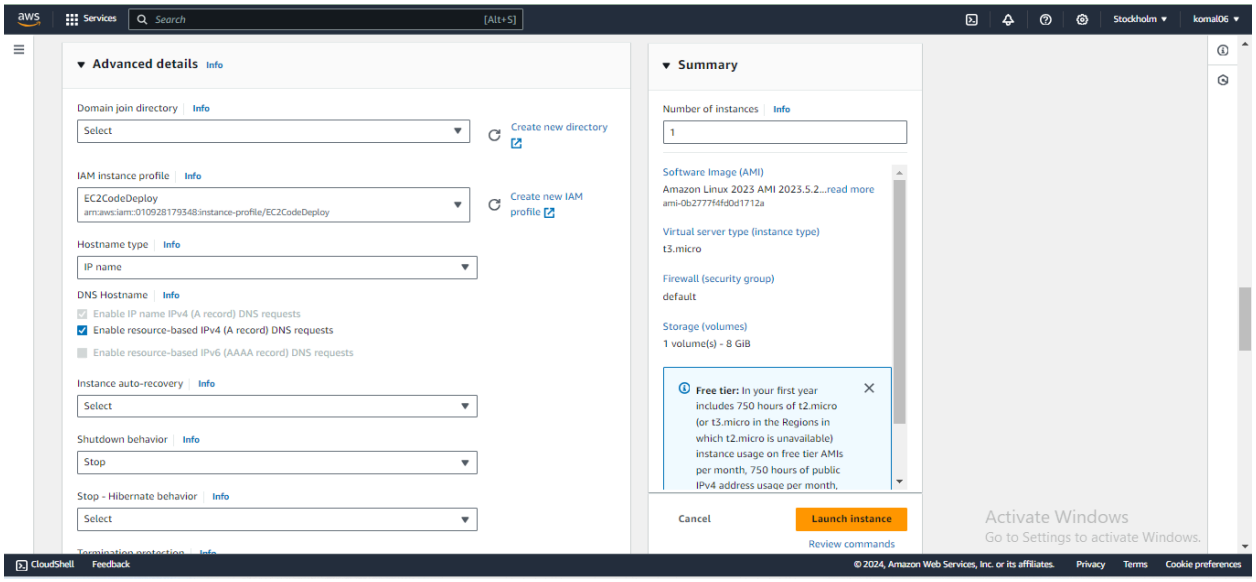


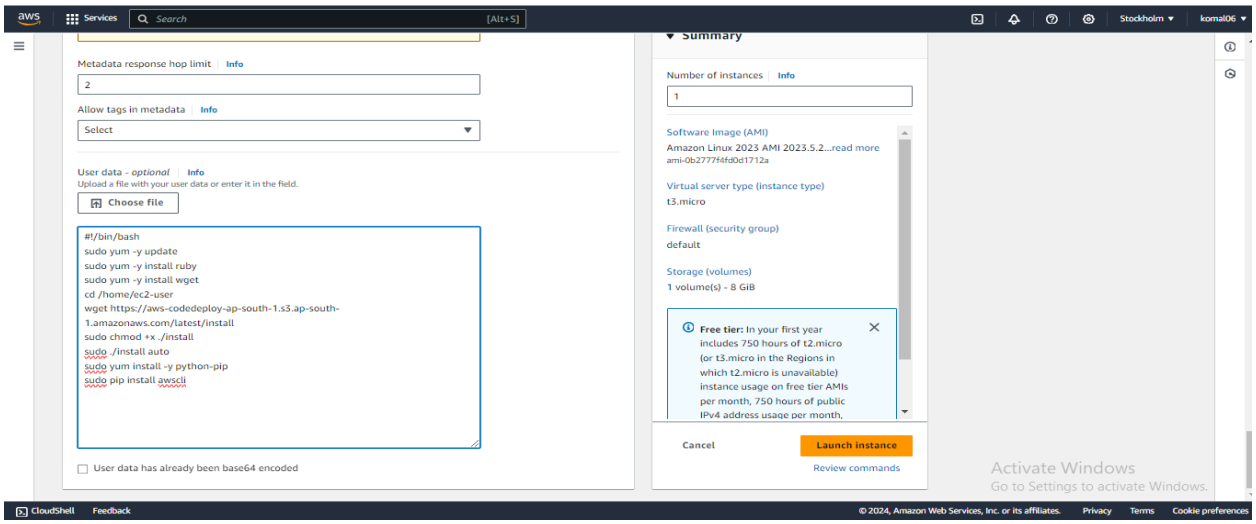

Services
Search
[Alt+S]
Stockholm
komal06
Architecture
64-bit (x86)
Boot mode
uefi-preferred
AMI ID
ami-0b2777f4fd0d1712a
Verified provider
Instance type Info | Get advice
Instance type
t3.micro
Free tier eligible
Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand RHEL base pricing: 0.0396 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.
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-0b2777f4fd0d1712a
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

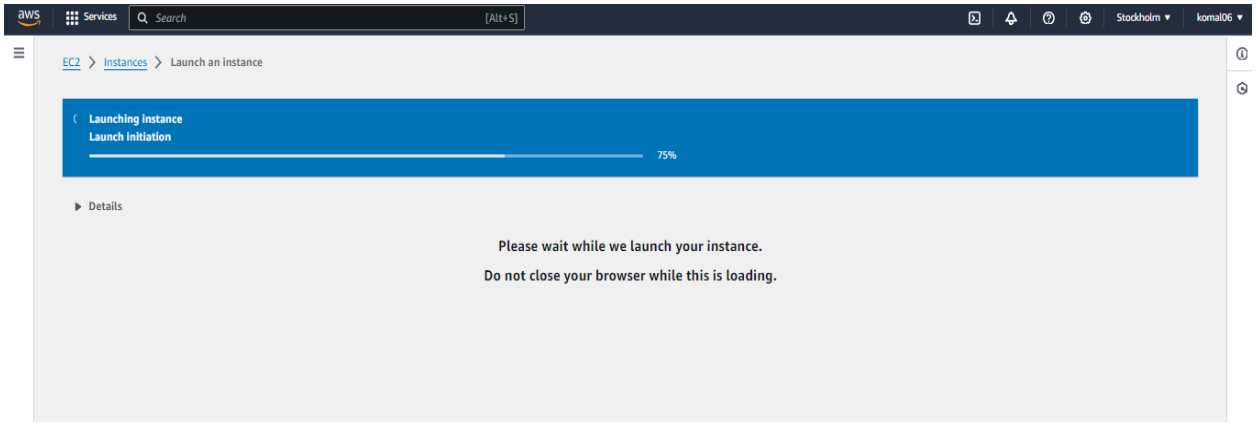

Create key pair
Key pair name
Key pairs allow you to connect to your instance securely.
AAR-DEMO
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type
RSA
RSA encrypted private and public key pair
ED25519
ED25519 encrypted private and public key pair
Private key file format
.pem
For use with OpenSSH
.ppk
For use with PuTTY
When prompted, store the private key in a secure and accessible location on
Cancel
Create key pair

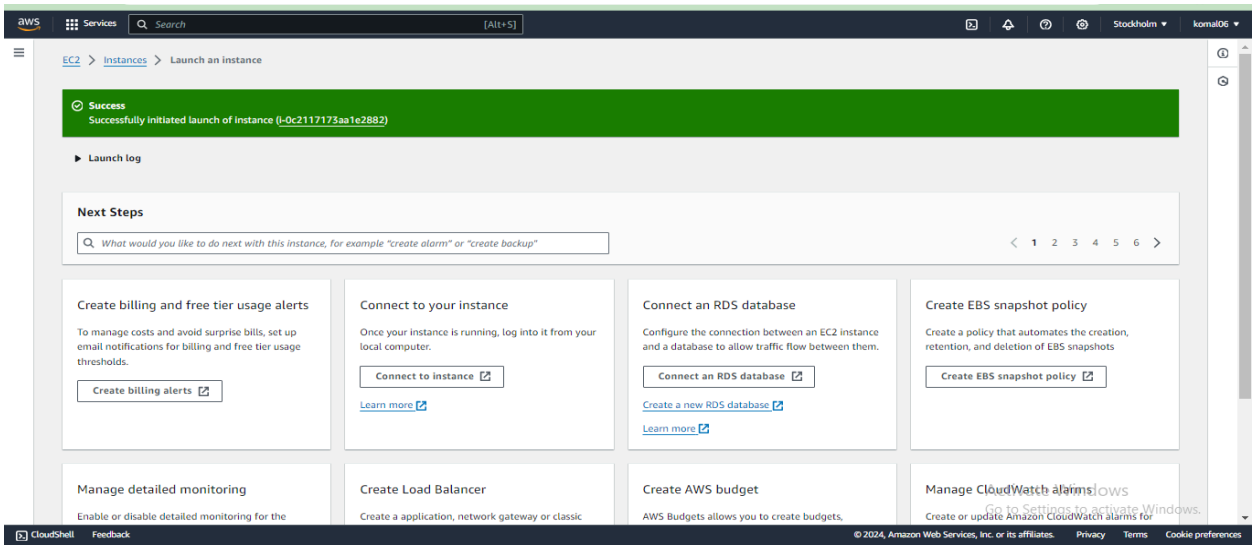

Services
Search
[Alt+S]
Stockholm
komal06
On-Demand SUSE base pricing: 0.0108 USD per Hour
On-Demand Linux base pricing: 0.0108 USD per Hour
On-Demand Windows base pricing: 0.02 USD per Hour
Compare instance types
Additional costs apply for AMIs with pre-installed software
Key pair (login) Info
You can 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
AAR-DEMO
Create new key pair
Network settings Info
Edit
Network Info
vpc-0a645ae45b7d6fd4e
Subnet Info
No preference (Default subnet in any availability zone)
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-0b2777f4fd0d1712a
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

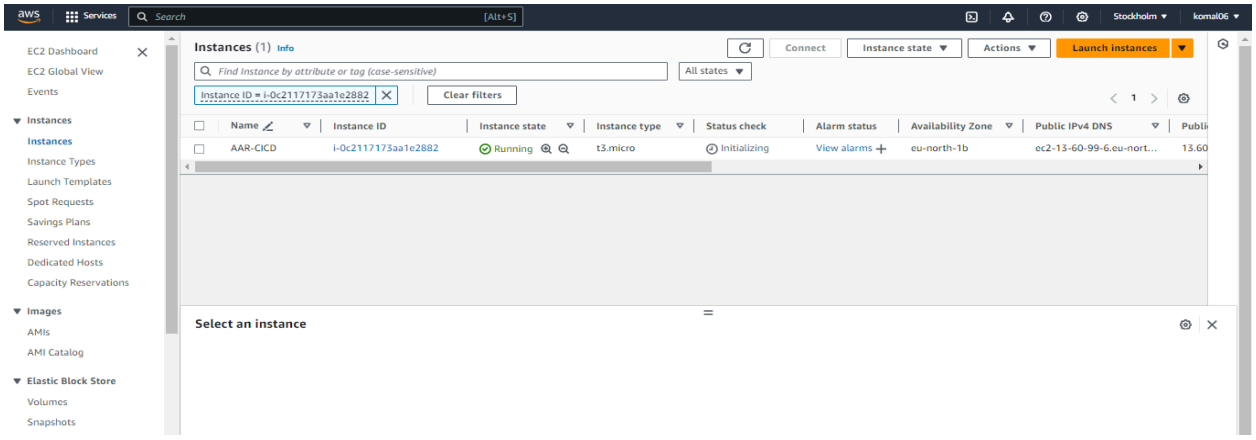

Network settings Info
Edit
Network Info
vpc-0a645ae45b7d6fd4e
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable
Additional charges apply when outside of free tier allowance
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Common security groups Info
Select security groups
default sg-0f9f4f4b112e4b7fa
VPC: vpc-0a645ae45b7d6fd4e
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Configure storage Info
Advanced
1x 8 GiB gp3 Root volume (Not encrypted)
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-0b2777f4fd0d1712a
Virtual server type (instance type)
t3.micro
Firewall (security group)
default
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month,
Cancel
Launch instance
Review commands
Activate Windows
Go to Settings to activate Windows.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Advanced details Info
Domain join directory Info
Select
Create new directory
IAM instance profile Info
EC2CodeDeploy
arn:aws:iam::010928179348:instance-profile/EC2CodeDeploy
Create new IAM profile
Hostname type Info
IP name
DNS Hostname Info
Enable IP name IPv4 (A record) DNS requests
Enable resource-based IPv4 (A record) DNS requests
Enable resource-based IPv6 (AAAA record) DNS requests
Instance auto-recovery Info
Select
Shutdown behavior Info
Stop
Stop - Hibernate behavior Info
Select
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-0b2777f4fd0d1712a
Virtual server type (instance type)
t3.micro
Firewall (security group)
default
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month,
Cancel
Launch instance
Review commands
Activate Windows
Go to Settings to activate Windows.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

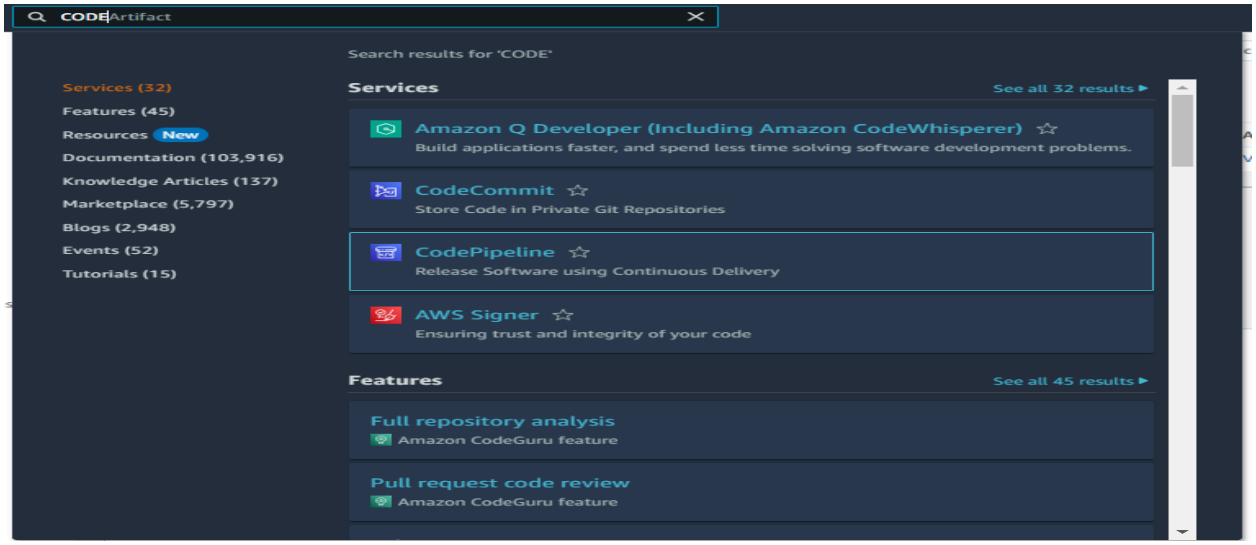

Metadata response hop limit Info
2
Allow tags in metadata Info
Select
User data - optional Info
Upload a file with your user data or enter it in the field.
Choose file
#!/bin/bash
sudo yum -y update
sudo yum -y install ruby
sudo yum -y install wget
cd /home/ec2-user
wget https://aws-codedeploy-ap-south-1.s3.ap-south-1.amazonaws.com/latest/install
sudo chmod +x ./install
sudo ./install auto
sudo yum install -y python-pip
sudo pip install awscli
User data has already been base64 encoded
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-0b2777f4fd0d1712a
Virtual server type (instance type)
t3.micro
Firewall (security group)
default
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month,
Cancel
Launch instance
Review commands
Activate Windows
Go to Settings to activate Windows.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

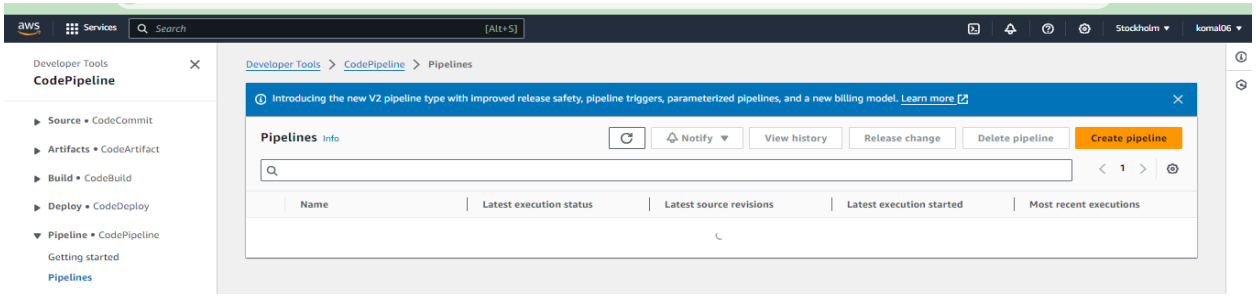

Services
Search
[Alt+S]
Stockholm
komal06
EC2 > Instances > Launch an instance
Launching instance
Launch initiation
75%
Details
Please wait while we launch your instance.
Do not close your browser while this is loading.

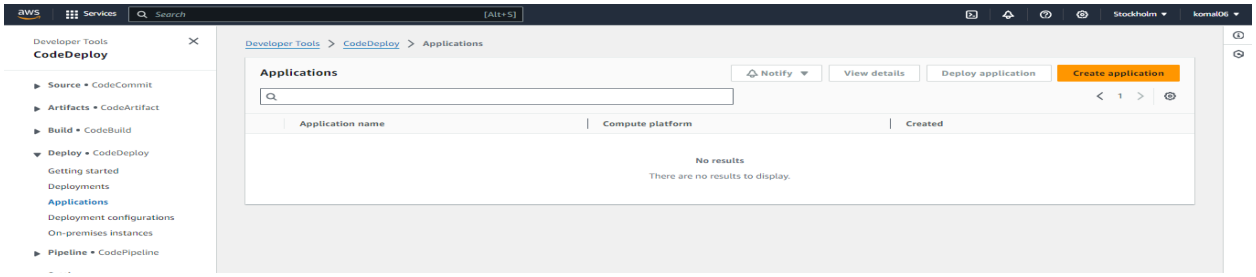

Services
Search
[Alt+S]
Stockholm
komal06
EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-0c2117173aa1e2882)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
Create billing alerts
Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more
Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy
Manage detailed monitoring
Enable or disable detailed monitoring for the
Create Load Balancer
Create a application, network gateway or classic
Create AWS budget
AWS Budgets allows you to create budgets,
Manage CloudWatch alarms
Create or update Amazon CloudWatch alarms for
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

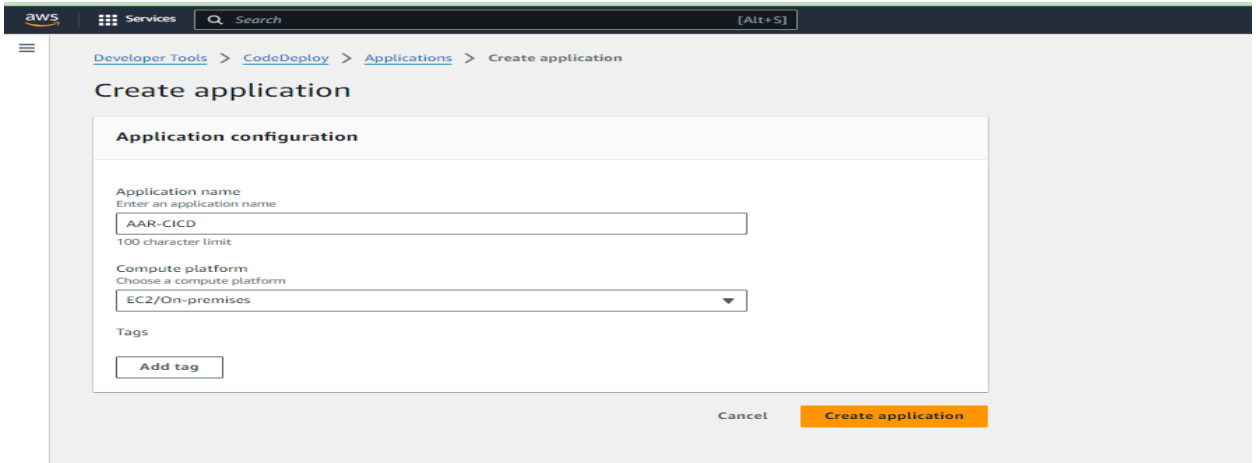

Services
Search
[Alt+S]
Stockholm
komal06
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Instances (1) Info
Connect
Instance state
Actions
Launch instances
Find instance by attribute or tag (case-sensitive)
All states
Instance ID = i-0c2117173aa1e2882
Clear filters
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
AAR-CICD
i-0c2117173aa1e2882
Running
t3.micro
Initializing
View alarms
eu-north-1b
ec2-13-60-99-6.eu-nort...
Select an instance

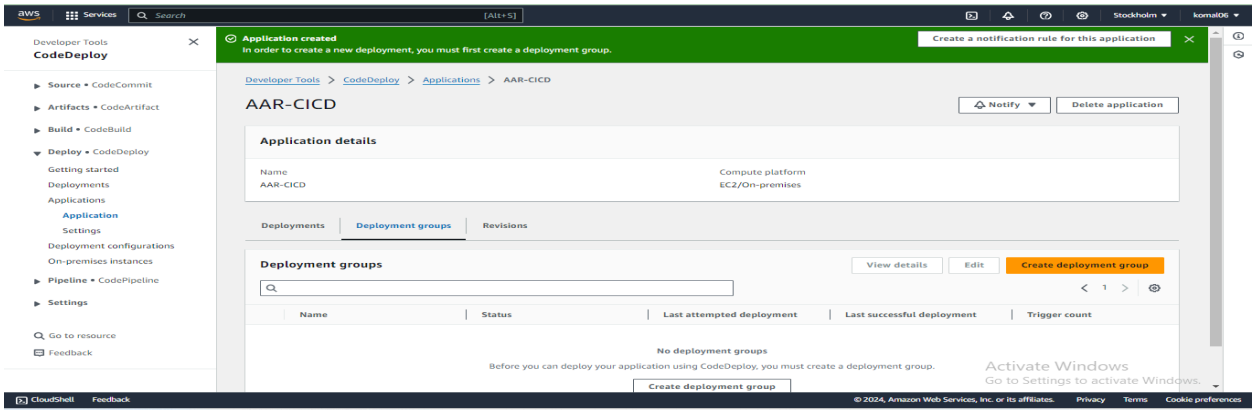
Setting up AWS CodePipeline :

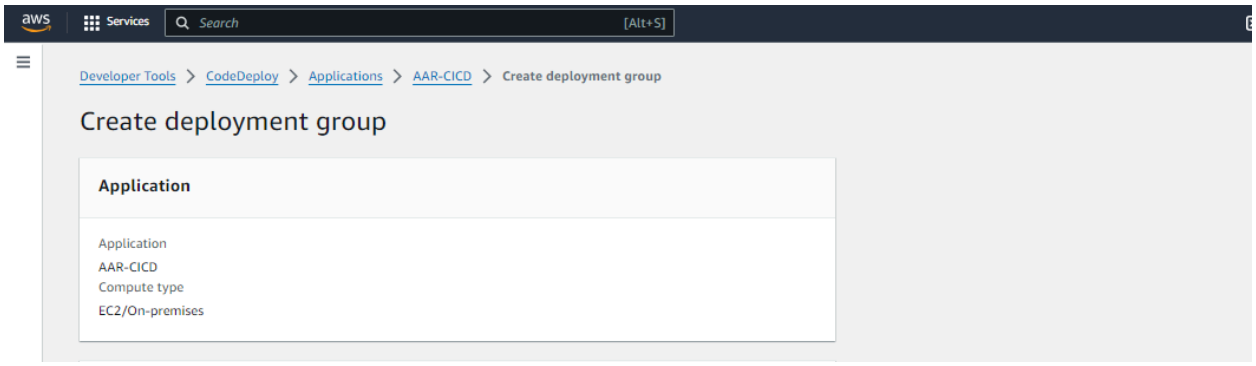


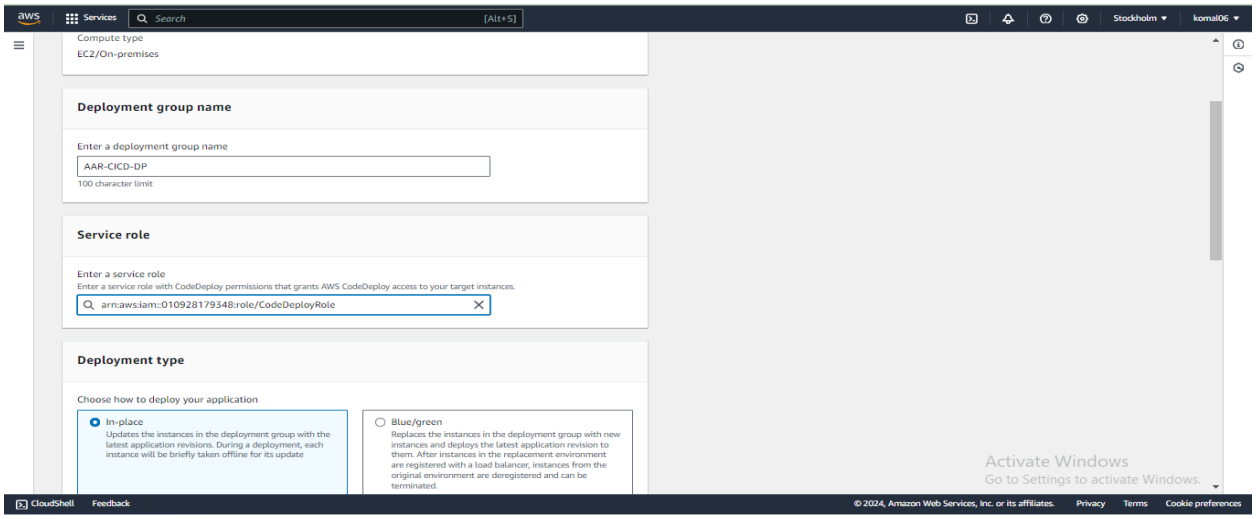


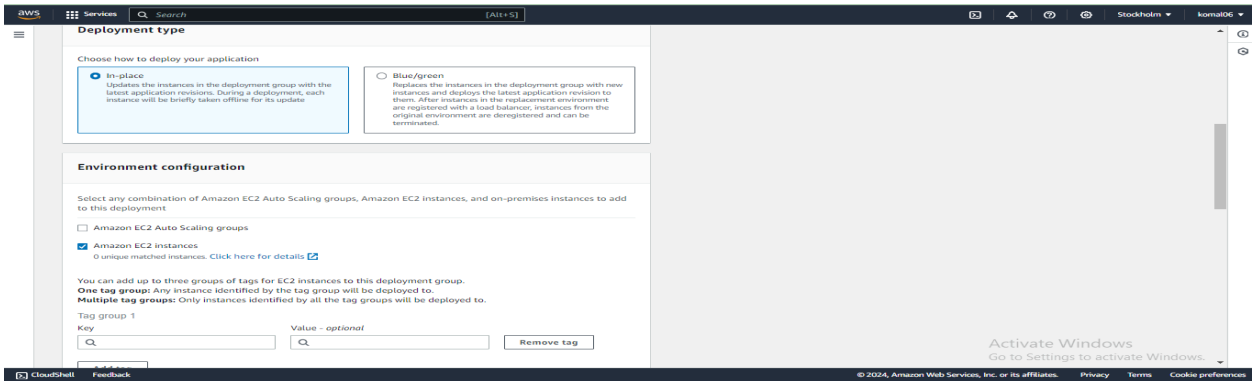


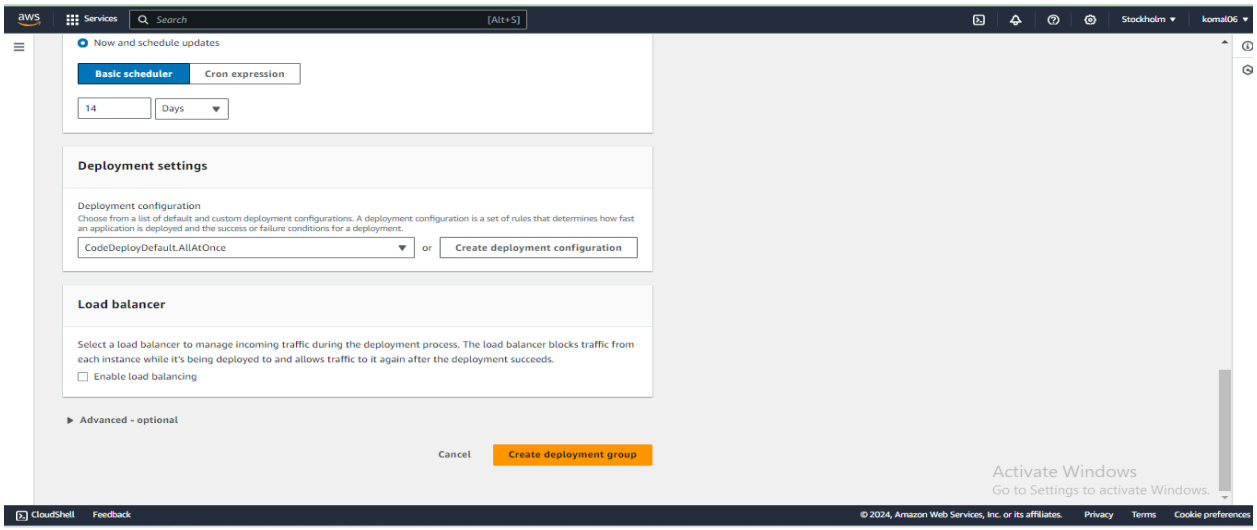


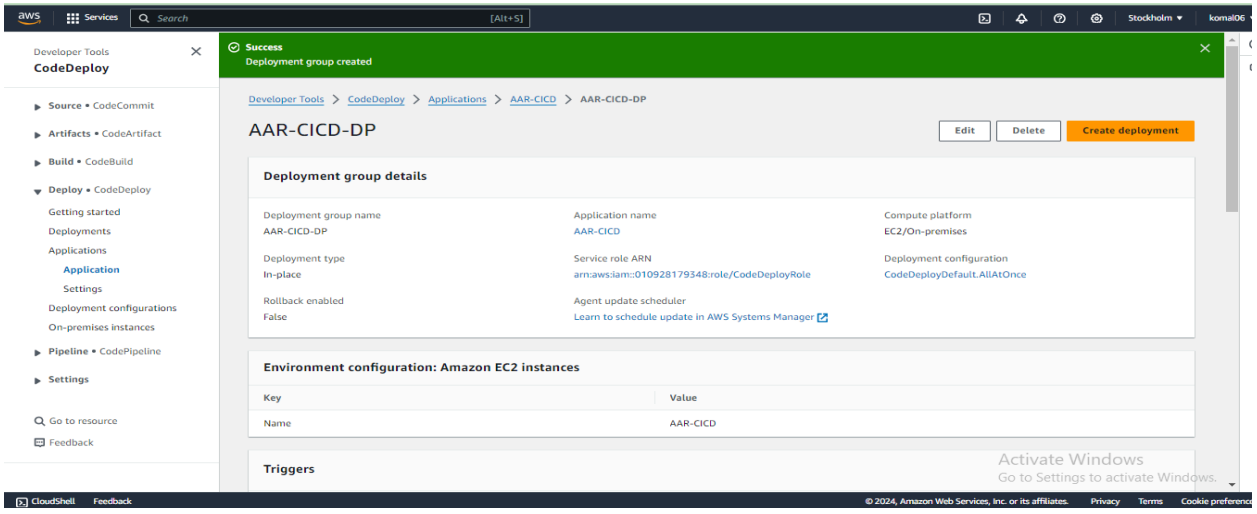

Application created
In order to create a new deployment, you must first create a deployment group.
Create a notification rule for this application
Developer Tools > CodeDeploy > Applications > AAR-CICD
AAR-CICD
Notify
Delete application
Application details
Name
AAR-CICD
Compute platform
EC2/On-premises
Deployments
Deployment groups
Revisions
Deployment groups
View details
Edit
Create deployment group
Name
Status
Last attempted deployment
Last successful deployment
Trigger count
No deployment groups
Before you can deploy your application using CodeDeploy, you must create a deployment group.
Create deployment group

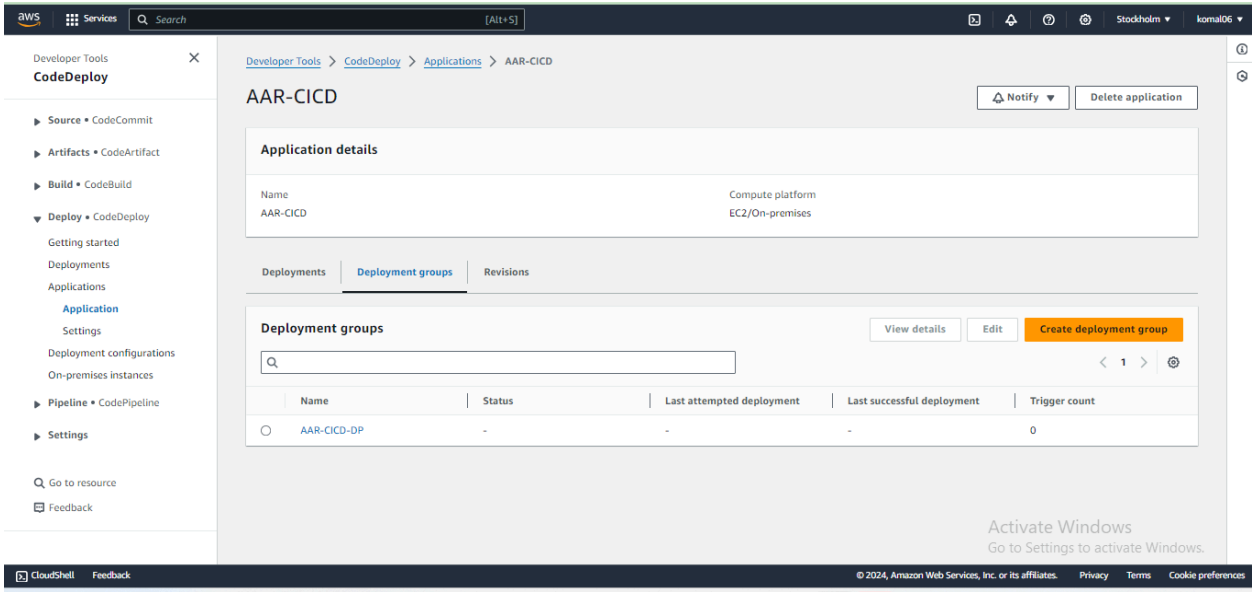

Developer Tools > CodeDeploy > Applications > AAR-CICD > Create deployment group
Create deployment group
Application
Application
AAR-CICD
Compute type
EC2/On-premises

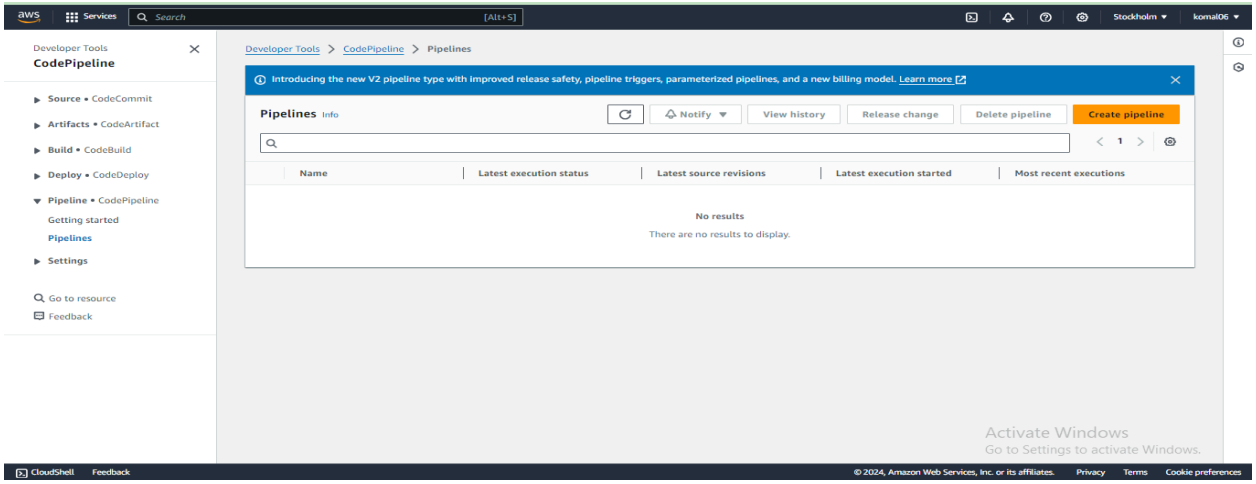

Compute type
EC2/On-premises
Deployment group name
Enter a deployment group name
AAR-CICD-DP
100 character limit
Service role
Enter a service role
Enter a service role with CodeDeploy permissions that grants AWS CodeDeploy access to your target instances.
arn:aws:iam::010928179348:role/CodeDeployRole
Deployment type
Choose how to deploy your application
In-place
Updates the instances in the deployment group with the latest application revisions. During a deployment, each instance will be briefly taken offline for its update
Blue/green
Replaces the instances in the deployment group with new instances and deploys the latest application revision to them. After instances in the replacement environment are registered with a load balancer, instances from the original environment are deregistered and can be terminated.

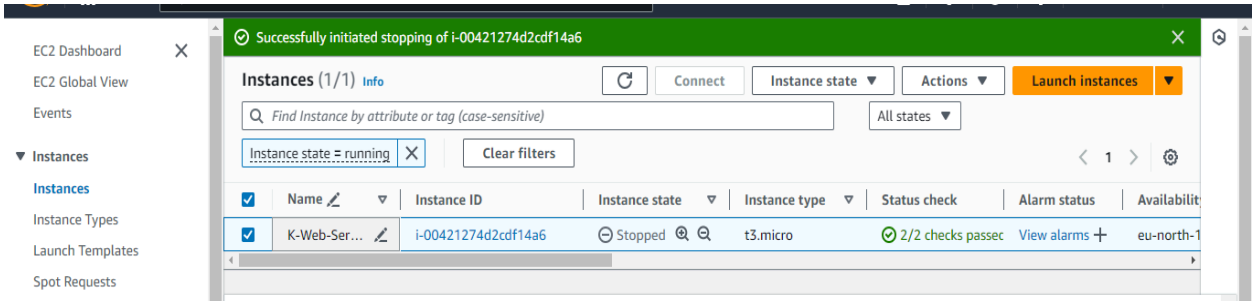

Deployment type
Choose how to deploy your application
In-place
Updates the instances in the deployment group with the latest application revisions. During a deployment, each instance will be briefly taken offline for its update
Blue/green
Replaces the instances in the deployment group with new instances and deploys the latest application revision to them. After instances in the replacement environment are registered with a load balancer, instances from the original environment are deregistered and can be terminated.
Environment configuration
Select any combination of Amazon EC2 Auto Scaling groups, Amazon EC2 instances, and on-premises instances to add to this deployment
Amazon EC2 Auto Scaling groups
Amazon EC2 instances
0 unique matched instances. Click here for details
You can add up to three groups of tags for EC2 instances to this deployment group.
One tag group: Any instance identified by the tag group will be deployed to.
Multiple tag groups: Only instances identified by all the tag groups will be deployed to.
Tag group 1
Key
Value - optional
Remove tag

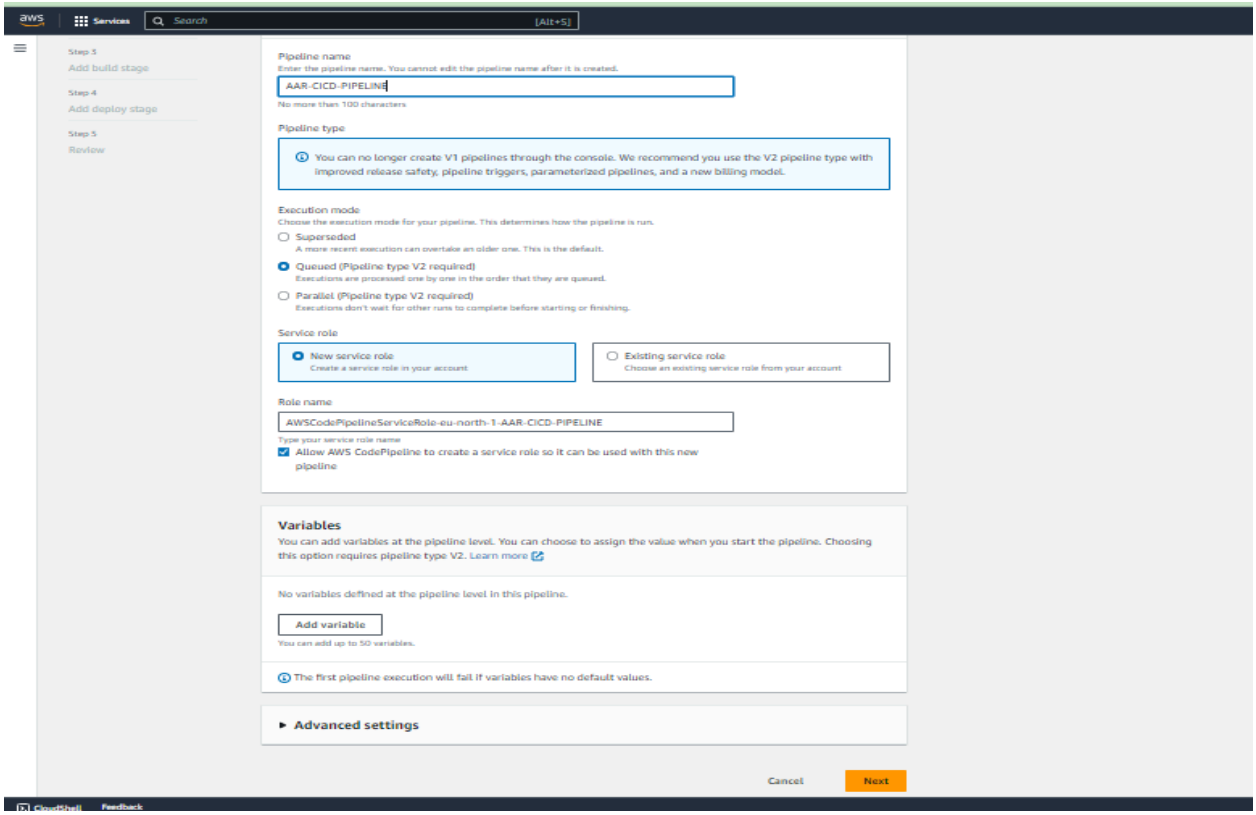

Now and schedule updates
Basic scheduler
Cron expression
14
Days
Deployment settings
Deployment configuration
Choose from a list of default and custom deployment configurations. A deployment configuration is a set of rules that determines how fast an application is deployed and the success or failure conditions for a deployment.
CodeDeployDefault.AllAtOnce
or
Create deployment configuration
Load balancer
Select a load balancer to manage incoming traffic during the deployment process. The load balancer blocks traffic from each instance while it's being deployed to and allows traffic to it again after the deployment succeeds.
Enable load balancing
Advanced - optional
Cancel
Create deployment group
Activate Windows
Go to Settings to activate Windows.

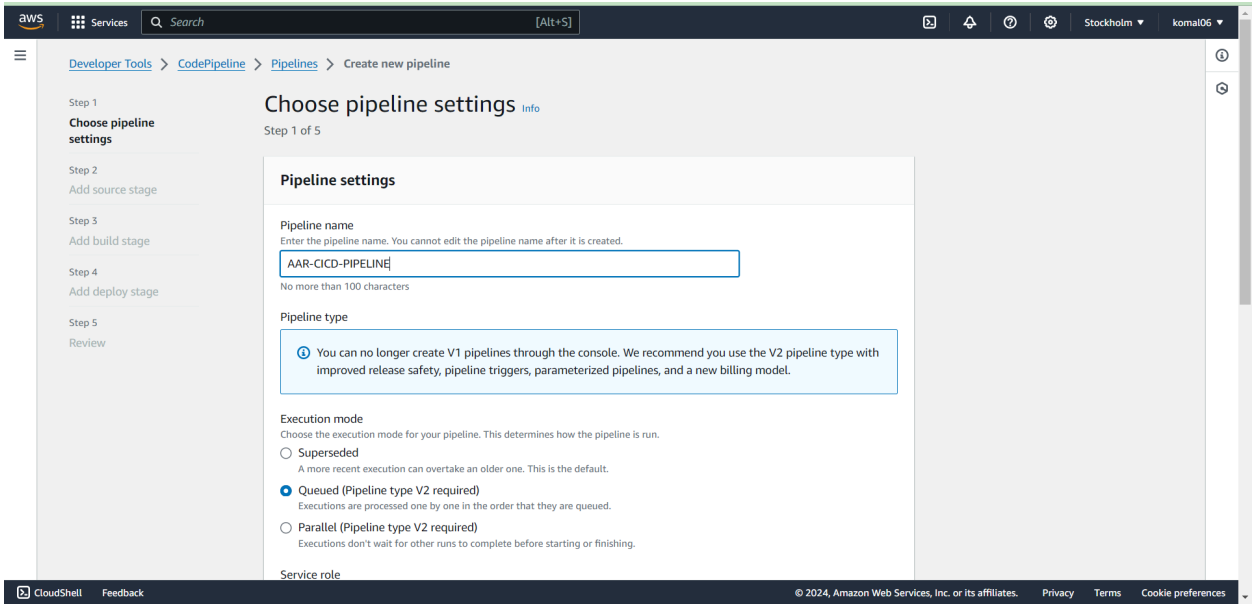

Success
Deployment group created
Developer Tools > CodeDeploy > Applications > AAR-CICD > AAR-CICD-DP
AAR-CICD-DP
Edit
Delete
Create deployment
Deployment group details
Deployment group name
AAR-CICD-DP
Application name
AAR-CICD
Compute platform
EC2/On-premises
Deployment type
In-place
Service role ARN
arn:aws:iam::010928179348:role/CodeDeployRole
Deployment configuration
CodeDeployDefault.AllAtOnce
Rollback enabled
False
Agent update scheduler
Learn to schedule update in AWS Systems Manager
Environment configuration: Amazon EC2 instances
Key
Value
Name
AAR-CICD
Triggers
Activate Windows
Go to Settings to activate Windows.

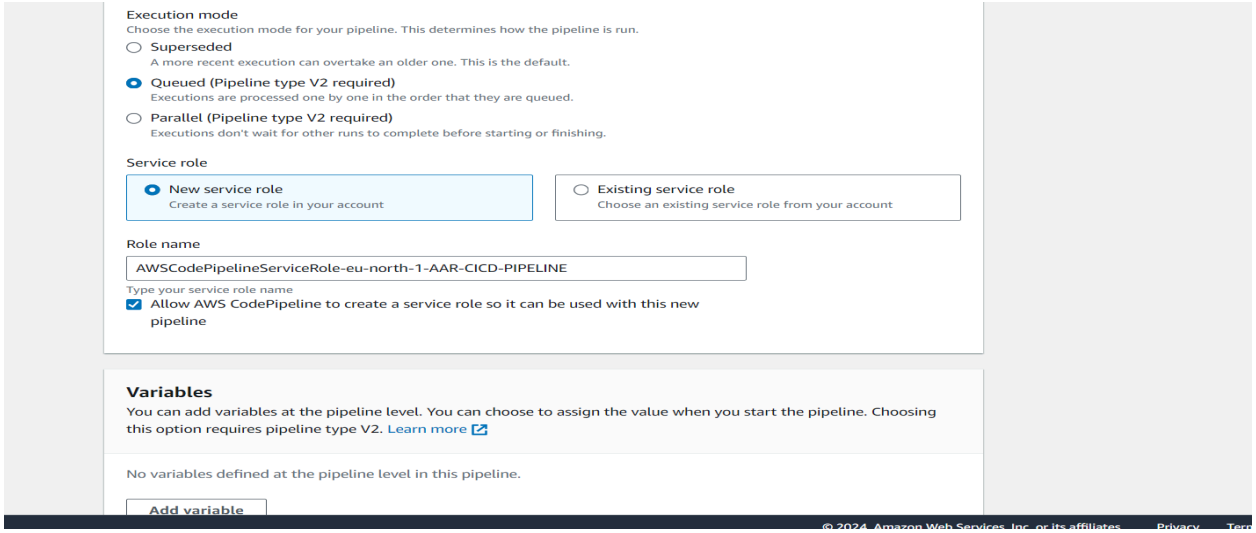

Developer Tools > CodeDeploy > Applications > AAR-CICD
AAR-CICD
Notify
Delete application
Application details
Name
AAR-CICD
Compute platform
EC2/On-premises
Deployments
Deployment groups
Revisions
Deployment groups
View details
Edit
Create deployment group
Name
Status
Last attempted deployment
Last successful deployment
Trigger count
AAR-CICD-DP
0
Activate Windows
Go to Settings to activate Windows.

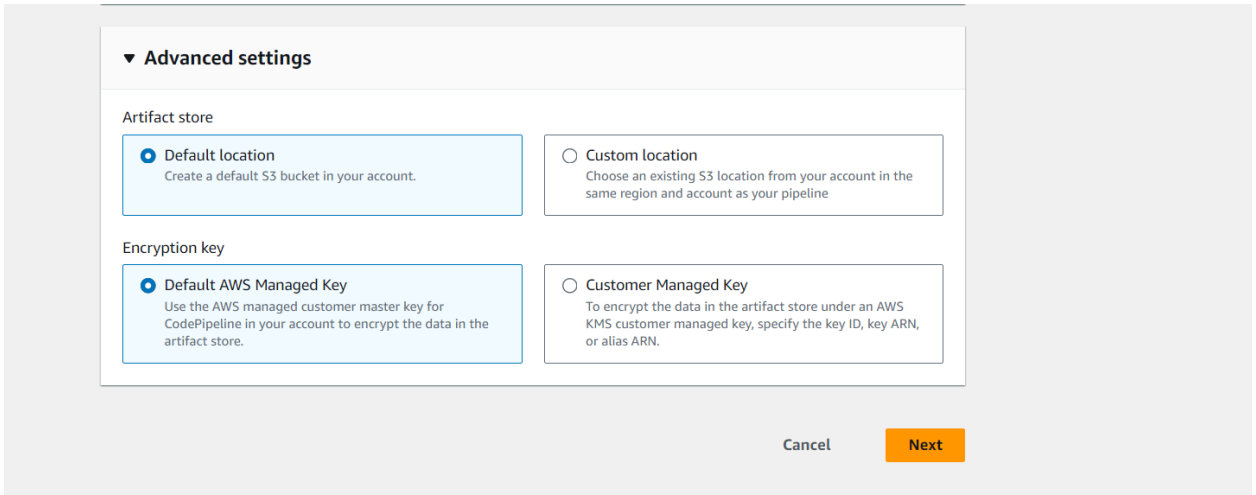

Developer Tools
CodePipeline
Source • CodeCommit
Artifacts • CodeArtifact
Build • CodeBuild
Deploy • CodeDeploy
Pipeline • CodePipeline
Getting started
Pipelines
Settings
Developer Tools > CodePipeline > Pipelines
Introducing the new V2 pipeline type with improved release safety, pipeline triggers, parameterized pipelines, and a new billing model. Learn more
Pipelines Info
Notify
View history
Release change
Delete pipeline
Create pipeline
Name
Latest execution status
Latest source revisions
Latest execution started
Most recent executions
No results
There are no results to display.
Activate Windows
Go to Settings to activate Windows.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

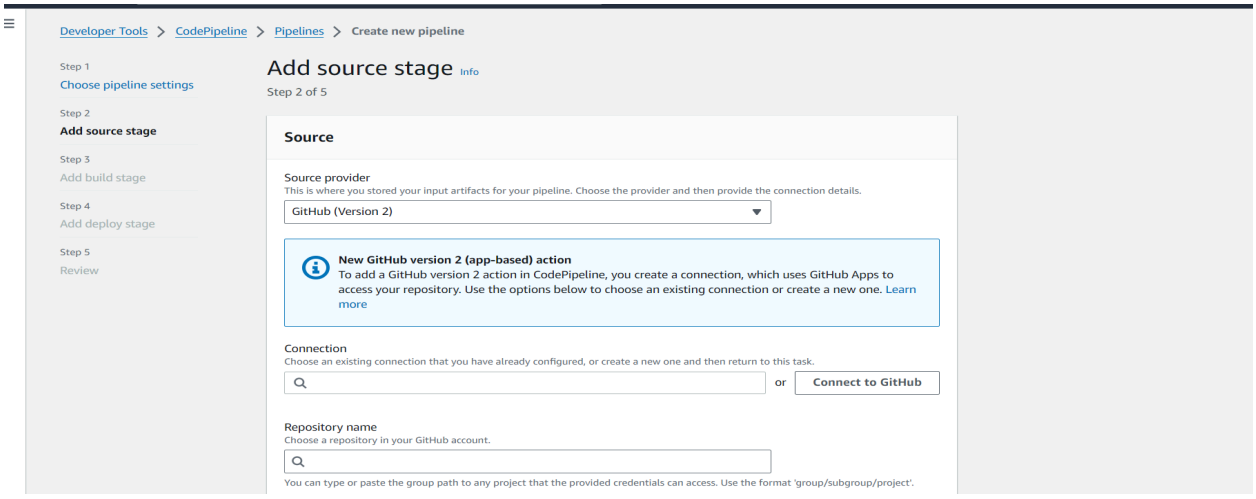

EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Successfully initiated stopping of i-00421274d2cdf14a6
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance state = running
Clear filters
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
K-Web-Ser...
i-00421274d2cdf14a6
Stopped
t3.micro
2/2 checks passed
View alarms
eu-north-1

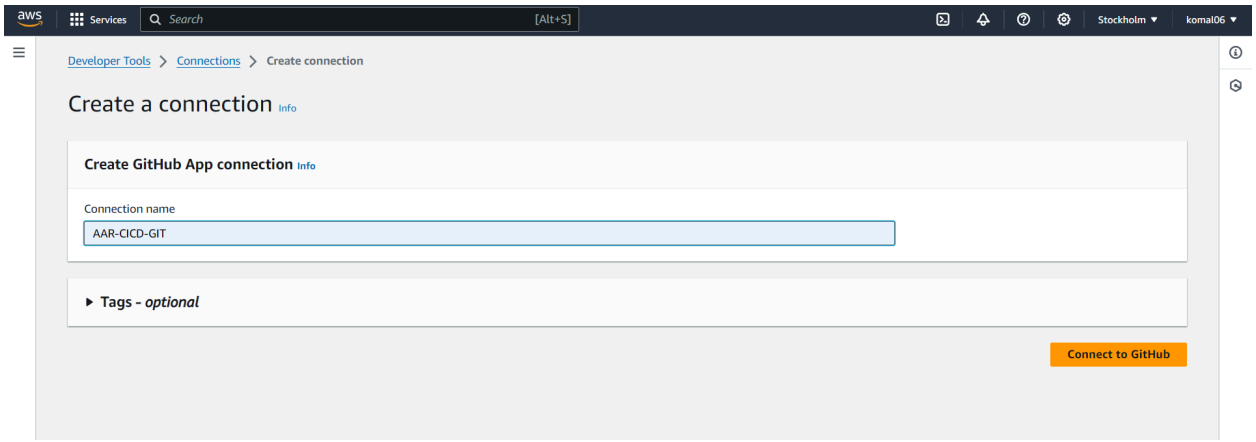

Step 3
Add build stage
Step 4
Add deploy stage
Step 5
Review
Pipeline name
Enter the pipeline name. You cannot edit the pipeline name after it is created.
AAR-CICD-PIPELINE
No more than 100 characters
Pipeline type
You can no longer create V1 pipelines through the console. We recommend you use the V2 pipeline type with improved release safety, pipeline triggers, parameterized pipelines, and a new billing model.
Execution mode
Choose the execution mode for your pipeline. This determines how the pipeline is run.
Superseded
A more recent execution can overtake an older one. This is the default.
Queued (Pipeline type V2 required)
Executions are processed one by one in the order that they are queued.
Parallel (Pipeline type V2 required)
Executions don't wait for other runs to complete before starting or finishing.
Service role
New service role
Create a service role in your account
Existing service role
Choose an existing service role from your account
Role name
AWSCodePipelineServiceRole-eu-north-1-AAR-CICD-PIPELINE
Type your service role name
Allow AWS CodePipeline to create a service role so it can be used with this new pipeline
Variables
You can add variables at the pipeline level. You can choose to assign the value when you start the pipeline. Choosing this option requires pipeline type V2. Learn more
No variables defined at the pipeline level in this pipeline.
Add variable
You can add up to 50 variables.
The first pipeline execution will fail if variables have no default values.
Advanced settings
Cancel
Next

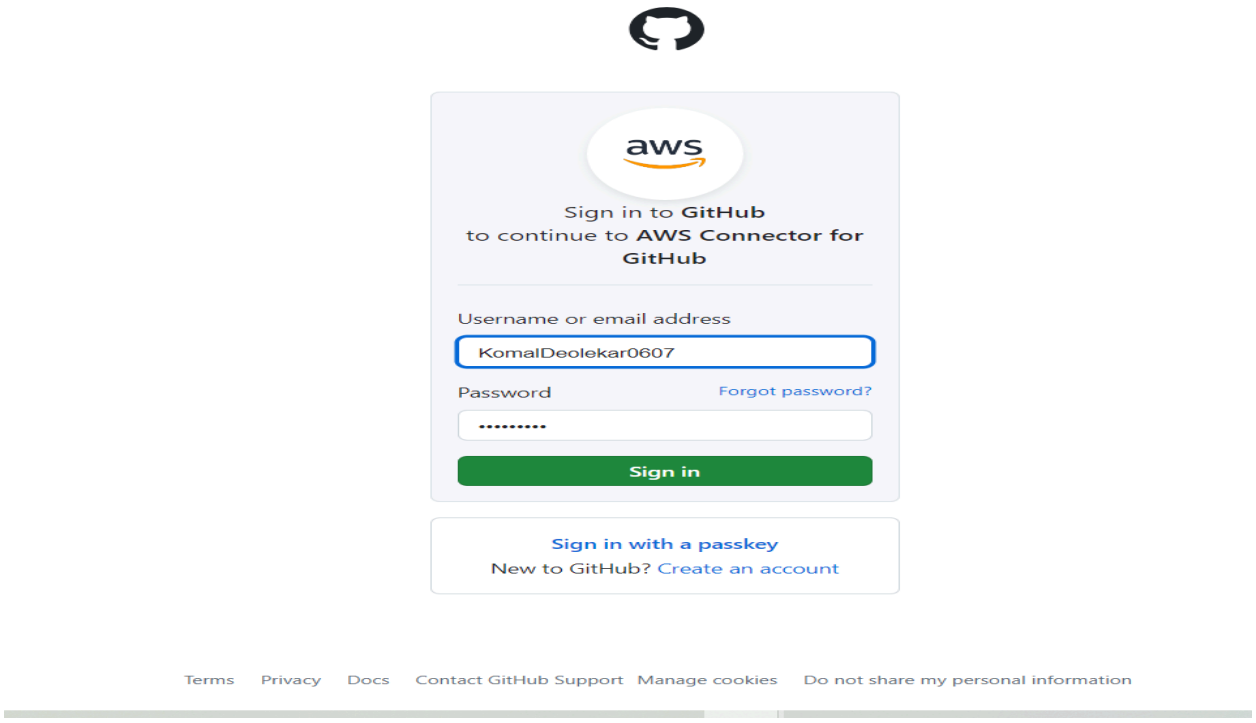

aws
Services
Search
[Alt+S]
Stockholm
komal06
Developer Tools > CodePipeline > Pipelines > Create new pipeline
Step 1
Choose pipeline settings
Step 2
Add source stage
Step 3
Add build stage
Step 4
Add deploy stage
Step 5
Review
Choose pipeline settings Info
Step 1 of 5
Pipeline settings
Pipeline name
Enter the pipeline name. You cannot edit the pipeline name after it is created.
AAR-CICD-PIPELINE
No more than 100 characters
Pipeline type
You can no longer create V1 pipelines through the console. We recommend you use the V2 pipeline type with improved release safety, pipeline triggers, parameterized pipelines, and a new billing model.
Execution mode
Choose the execution mode for your pipeline. This determines how the pipeline is run.
Superseded
A more recent execution can overtake an older one. This is the default.
Queued (Pipeline type V2 required)
Executions are processed one by one in the order that they are queued.
Parallel (Pipeline type V2 required)
Executions don't wait for other runs to complete before starting or finishing.
Service role
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

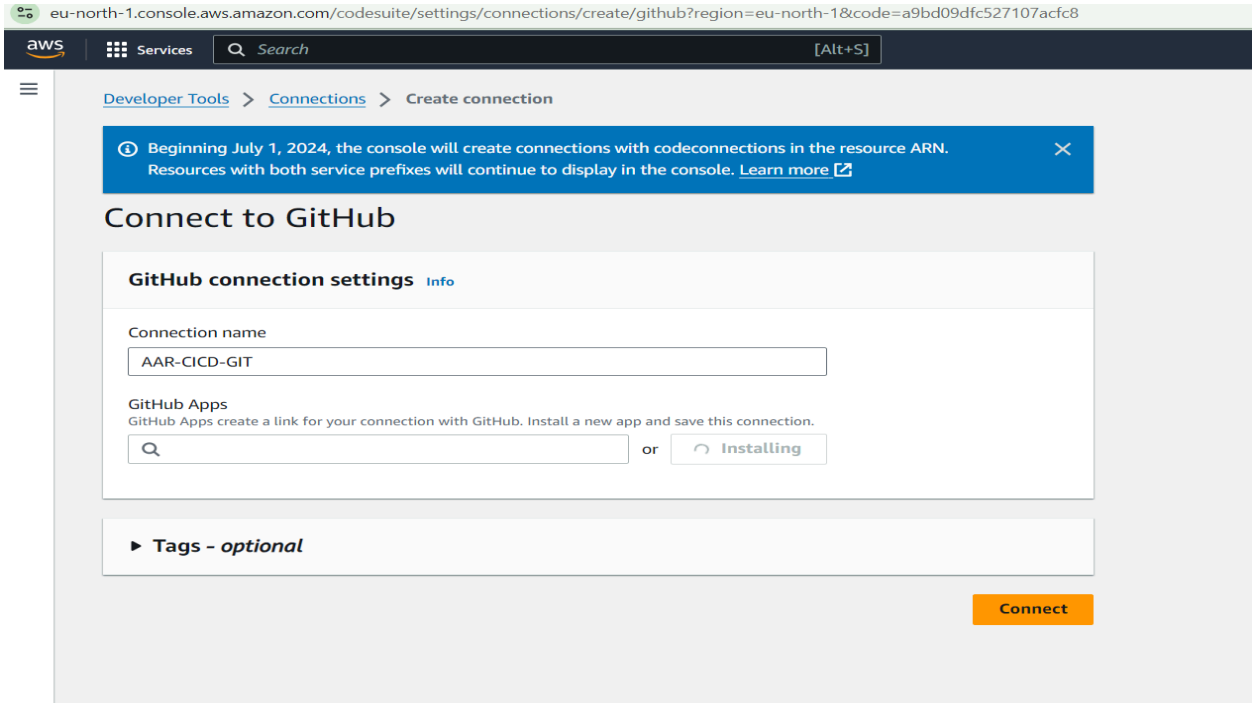

Execution mode
Choose the execution mode for your pipeline. This determines how the pipeline is run.
Superseded
A more recent execution can overtake an older one. This is the default.
Queued (Pipeline type V2 required)
Executions are processed one by one in the order that they are queued.
Parallel (Pipeline type V2 required)
Executions don't wait for other runs to complete before starting or finishing.
Service role
New service role
Create a service role in your account
Existing service role
Choose an existing service role from your account
Role name
AWSCodePipelineServiceRole-eu-north-1-AAR-CICD-PIPELINE
Type your service role name
Allow AWS CodePipeline to create a service role so it can be used with this new pipeline
Variables
You can add variables at the pipeline level. You can choose to assign the value when you start the pipeline. Choosing this option requires pipeline type V2. Learn more
No variables defined at the pipeline level in this pipeline.
Add variable

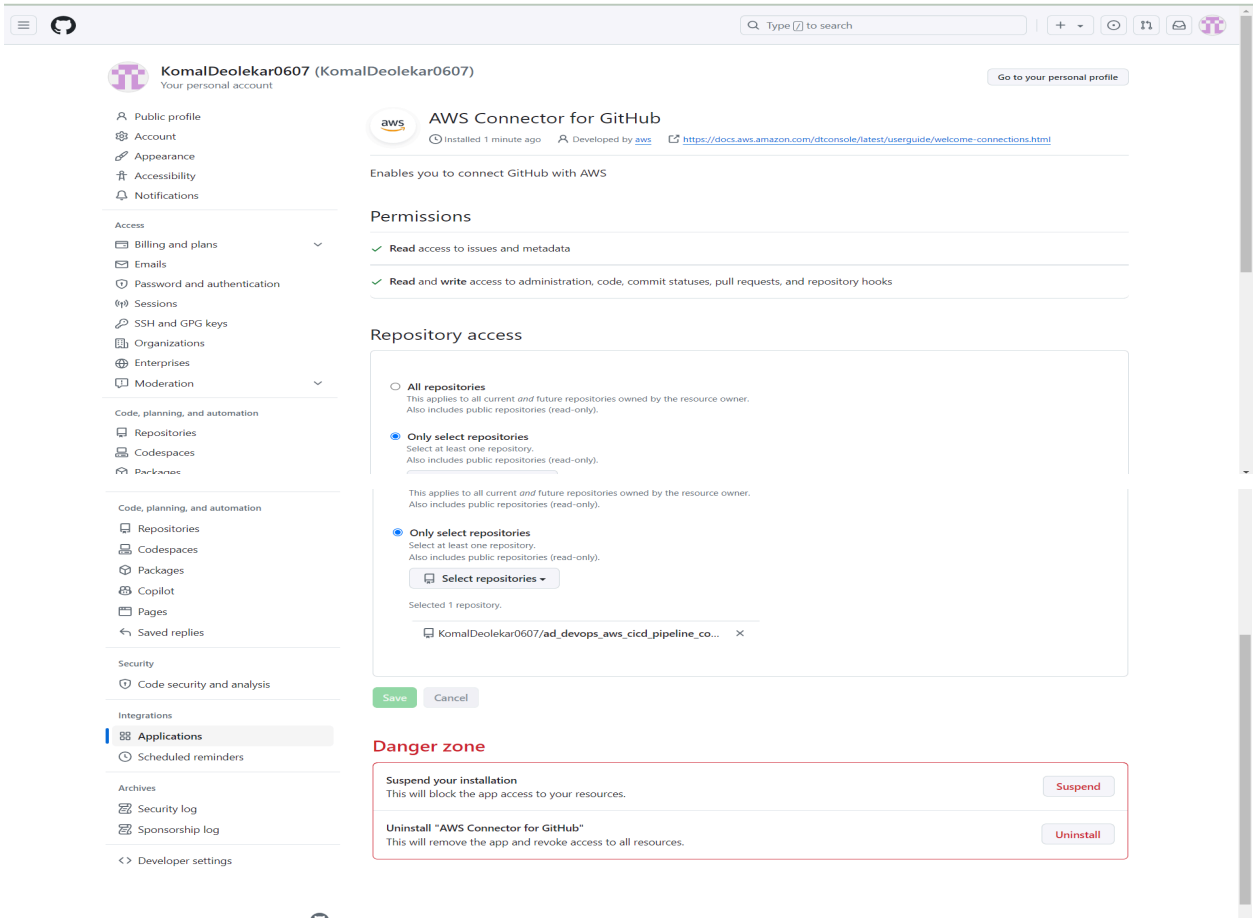

Advanced settings
Artifact store
Default location
Create a default S3 bucket in your account.
Custom location
Choose an existing S3 location from your account in the same region and account as your pipeline
Encryption key
Default AWS Managed Key
Use the AWS managed customer master key for CodePipeline in your account to encrypt the data in the artifact store.
Customer Managed Key
To encrypt the data in the artifact store under an AWS KMS customer managed key, specify the key ID, key ARN, or alias ARN.
Cancel
Next

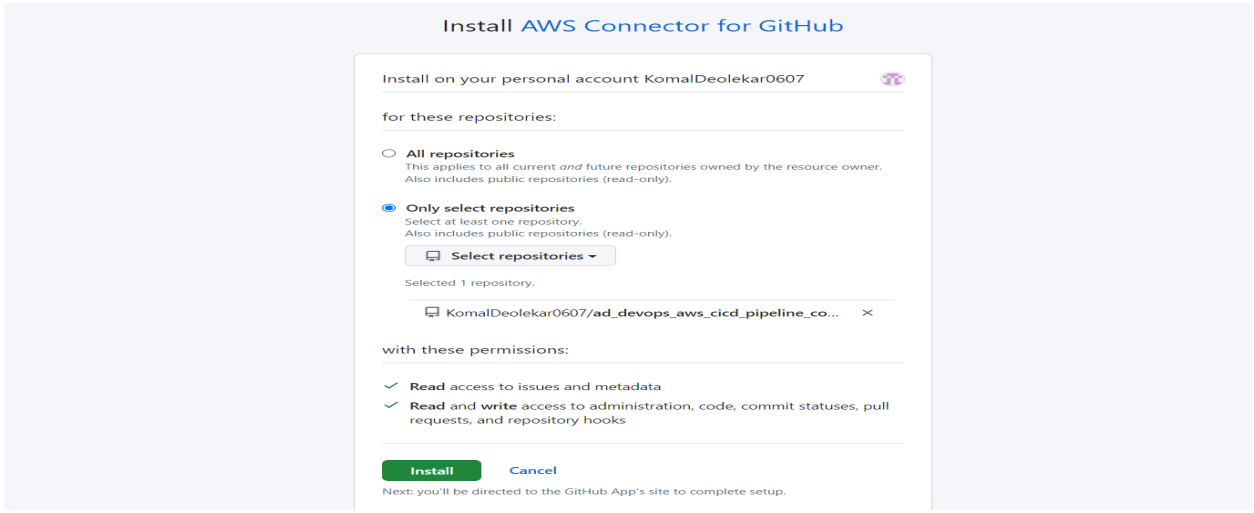

Developer Tools > CodePipeline > Pipelines > Create new pipeline
Step 1
Choose pipeline settings
Step 2
Add source stage
Step 3
Add build stage
Step 4
Add deploy stage
Step 5
Review
Add source stage Info
Step 2 of 5
Source
Source provider
This is where you stored your input artifacts for your pipeline. 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.
or
Connect to GitHub
Repository name
Choose a repository in your GitHub account.
You can type or paste the group path to any project that the provided credentials can access. Use the format 'group/subgroup/project'.

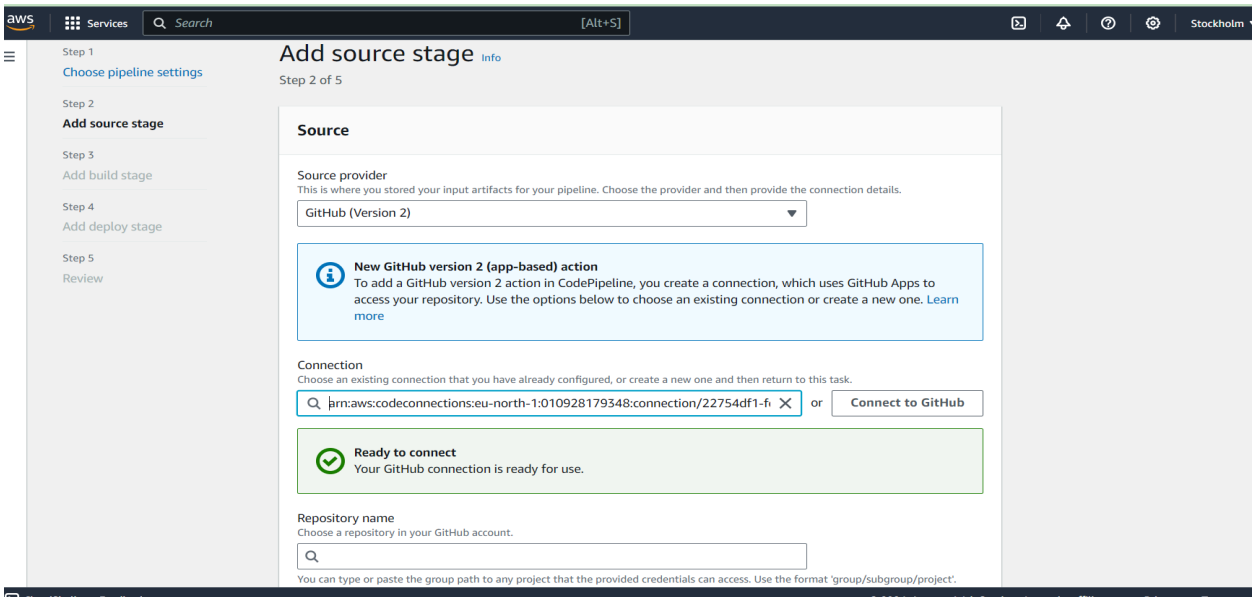

aws
Services
Search
[Alt+S]
Stockholm
komal06
Developer Tools > Connections > Create connection
Create a connection Info
Create GitHub App connection Info
Connection name
AAR-CICD-GIT
Tags - optional
Connect to GitHub

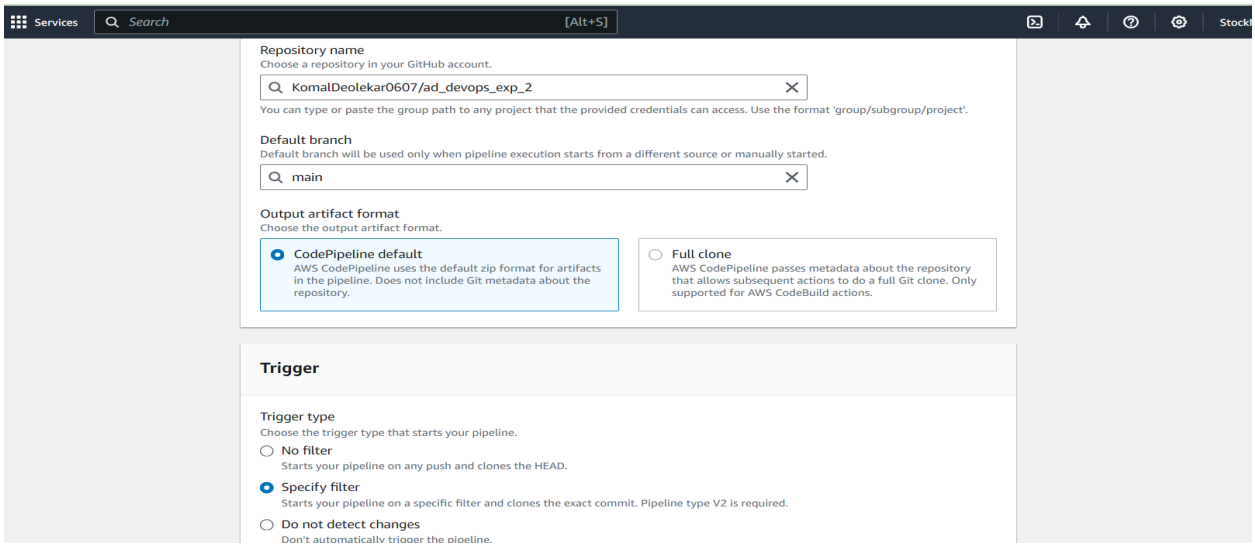

aws
Sign in to GitHub
to continue to AWS Connector for GitHub
Username or email address
KomalDeolekar0607
Password
Forgot password?
Sign in
Sign in with a passkey
New to GitHub? Create an account
Terms
Privacy
Docs
Contact GitHub Support
Manage cookies
Do not share my personal information

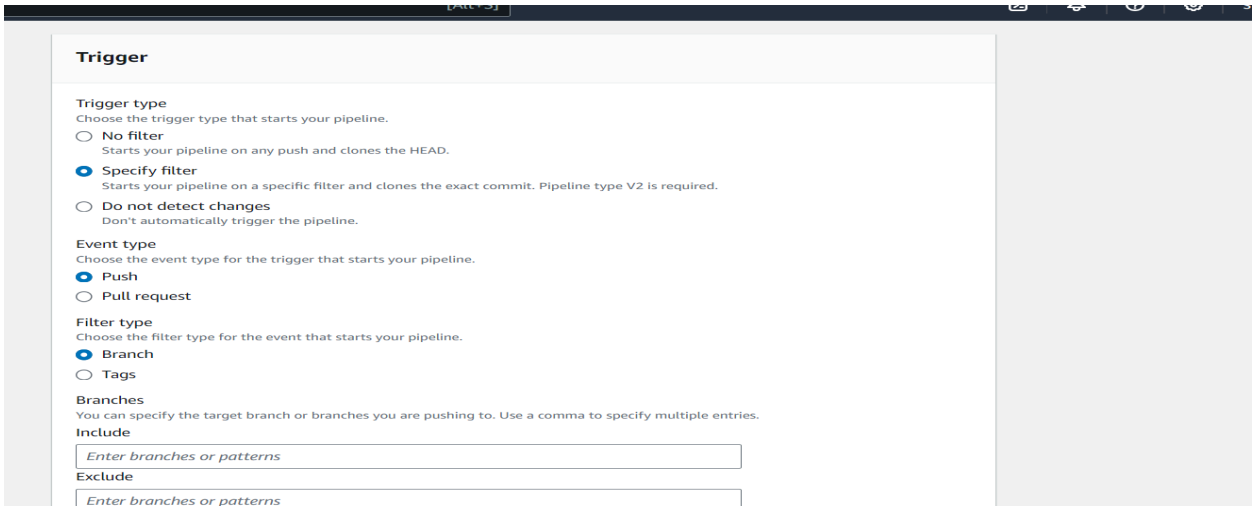

eu-north-1.console.aws.amazon.com/codesuite/settings/connections/create/github?region=eu-north-1&code=a9bd09dfc527107acfc8
aws
Services
Search
[Alt+S]
Developer Tools > Connections > Create connection
Beginning July 1, 2024, the console will create connections with codeconnections in the resource ARN.
Resources with both service prefixes will continue to display in the console. Learn more
Connect to GitHub
GitHub connection settings Info
Connection name
AAR-CICD-GIT
GitHub Apps
GitHub Apps create a link for your connection with GitHub. Install a new app and save this connection.
or
Installing
Tags - optional
Connect

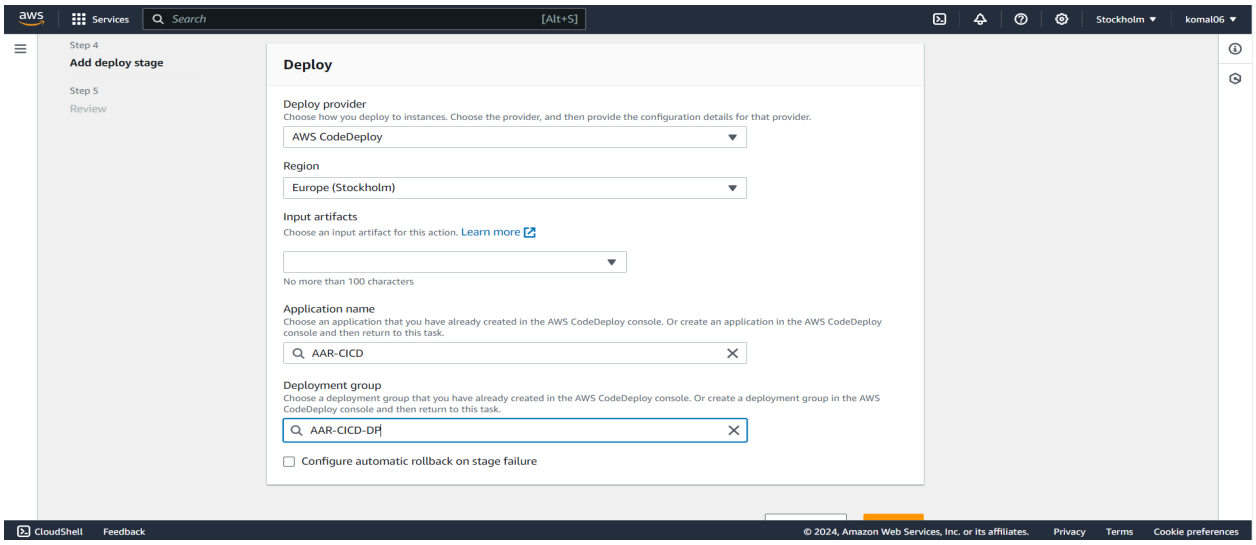

Type / to search
KomalDeolekar0607 (KomalDeolekar0607)
Your personal account
Go to your personal profile
Public profile
Account
Appearance
Accessibility
Notifications
Access
Billing and plans
Emails
Password and authentication
Sessions
SSH and GPG keys
Organizations
Enterprises
Moderation
Code, planning, and automation
Repositories
Codespaces
Packages
Copilot
Pages
Saved replies
Security
Code security and analysis
Integrations
Applications
Scheduled reminders
Archives
Security log
Sponsorship log
Developer settings
AWS Connector for GitHub
Installed 1 minute ago
Developed by aws
https://docs.aws.amazon.com/dtconsole/latest/userguide/welcome-connections.html
Enables you to connect GitHub with AWS
Permissions
Read access to issues and metadata
Read and write access to administration, code, commit statuses, pull requests, and repository hooks
Repository access
All repositories
This applies to all current and future repositories owned by the resource owner.
Also includes public repositories (read-only).
Only select repositories
Select at least one repository.
Also includes public repositories (read-only).
Select repositories
Selected 1 repository.
KomalDeolekar0607/ad_devops_aws_cicd_pipeline_co...
Save
Cancel
Danger zone
Suspend your installation
This will block the app access to your resources.
Suspend
Uninstall "AWS Connector for GitHub"
This will remove the app and revoke access to all resources.
Uninstall

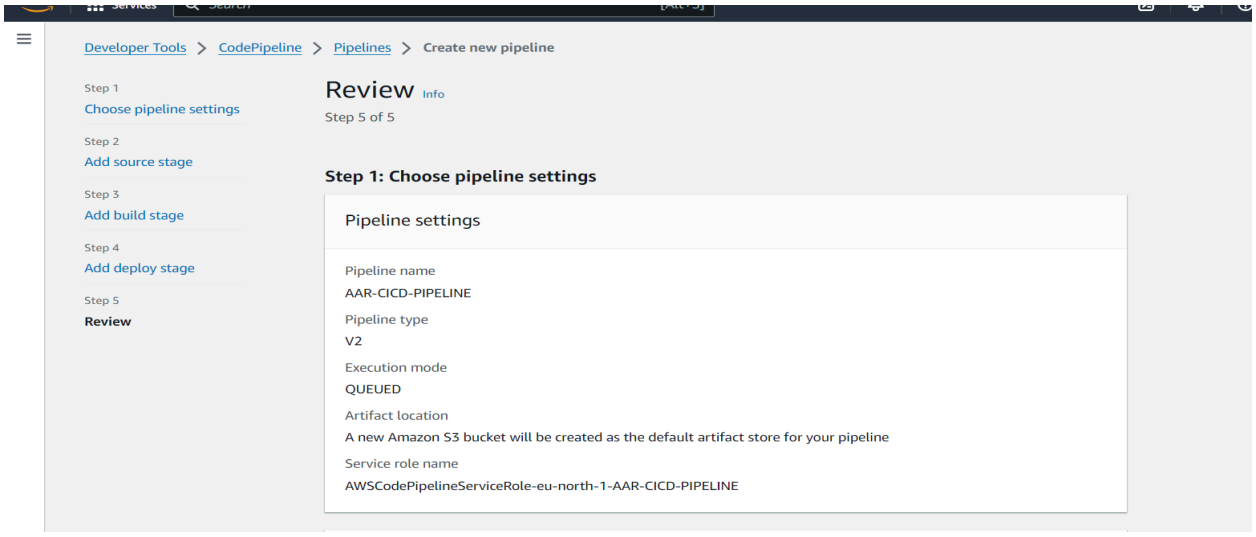

Install AWS Connector for GitHub
Install on your personal account KomalDeolekar0607
for these repositories:
All repositories
This applies to all current and future repositories owned by the resource owner.
Also includes public repositories (read-only).
Only select repositories
Select at least one repository.
Also includes public repositories (read-only).
Select repositories
Selected 1 repository.
KomalDeolekar0607/ad_devops_aws_cicd_pipeline_co...
with these permissions:
Read access to issues and metadata
Read and write access to administration, code, commit statuses, pull requests, and repository hooks
Install
Cancel
Next: you'll be directed to the GitHub App's site to complete setup.


aws
Services
Search
[Alt+S]
Stockholm
Step 1
Choose pipeline settings
Step 2
Add source stage
Step 3
Add build stage
Step 4
Add deploy stage
Step 5
Review
Add source stage Info
Step 2 of 5
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-1:010928179348:connection/22754df1-f
or
Connect to GitHub
Ready to connect
Your GitHub connection is ready for use.
Repository name
Choose a repository in your GitHub account.
You can type or paste the group path to any project that the provided credentials can access. Use the format 'group/subgroup/project'.

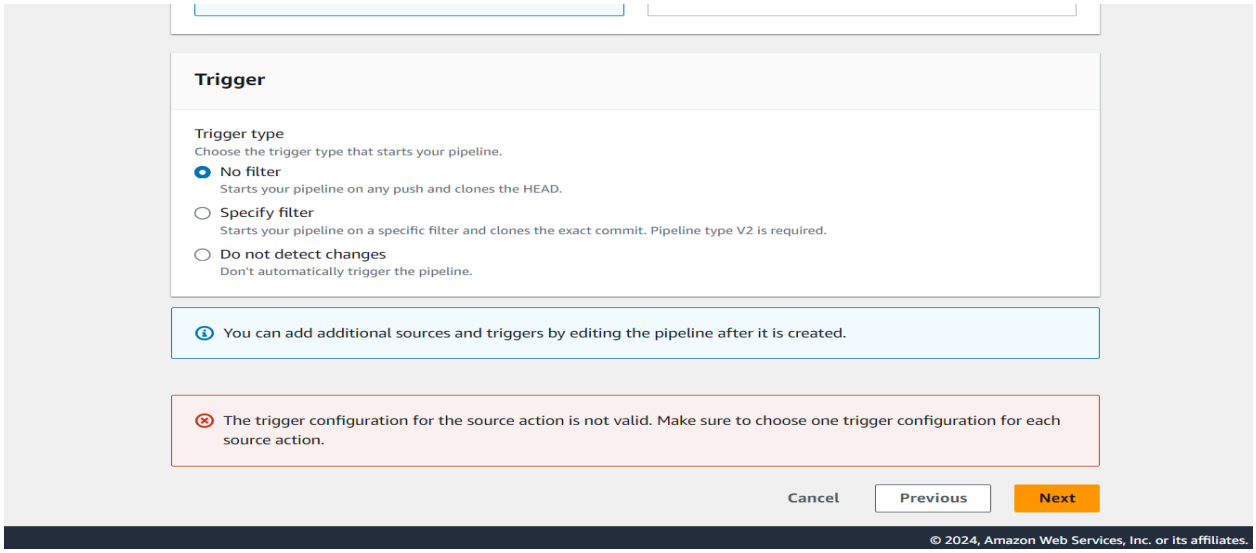

Services
Search
[Alt+S]
Repository name
Choose a repository in your GitHub account.
KomalDeolekar0607/ad_devops_exp_2
You can type or paste the group path to any project that the provided credentials can access. Use the format 'group/subgroup/project'.
Default branch
Default branch will be used only when pipeline execution starts from a different source or manually started.
main
Output artifact format
Choose the output artifact format.
CodePipeline default
AWS CodePipeline uses the default zip format for artifacts in the pipeline. Does not include Git metadata about the repository.
Full clone
AWS CodePipeline passes metadata about the repository that allows subsequent actions to do a full Git clone. Only supported for AWS CodeBuild actions.
Trigger
Trigger type
Choose the trigger type that starts your pipeline.
No filter
Starts your pipeline on any push and clones the HEAD.
Specify filter
Starts your pipeline on a specific filter and clones the exact commit. Pipeline type V2 is required.
Do not detect changes


Trigger
Trigger type
Choose the trigger type that starts your pipeline.
No filter
Starts your pipeline on any push and clones the HEAD.
Specify filter
Starts your pipeline on a specific filter and clones the exact commit. Pipeline type V2 is required.
Do not detect changes
Don't automatically trigger the pipeline.
Event type
Choose the event type for the trigger that starts your pipeline.
Push
Pull request
Filter type
Choose the filter type for the event that starts your pipeline.
Branch
Tags
Branches
You can specify the target branch or branches you are pushing to. Use a comma to specify multiple entries.
Include
Enter branches or patterns
Exclude
Enter branches or patterns

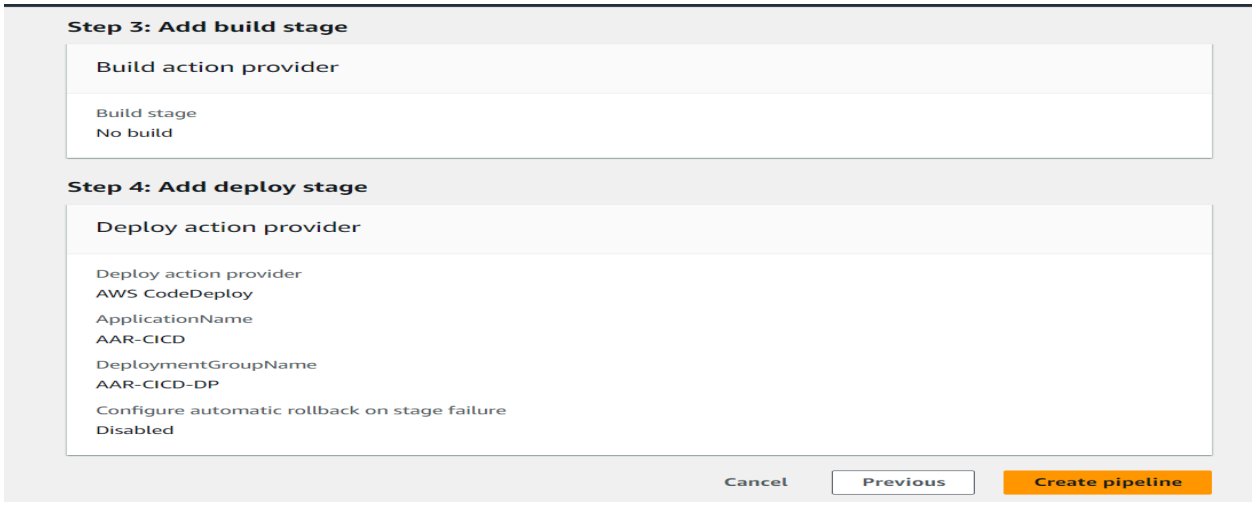

aws
Services
Search
[Alt+S]
Stockholm
komal06
Step 4
Add deploy stage
Step 5
Review
Deploy
Deploy provider
Choose how you deploy to instances. Choose the provider, and then provide the configuration details for that provider.
AWS CodeDeploy
Region
Europe (Stockholm)
Input artifacts
Choose an input artifact for this action. Learn more
No more than 100 characters
Application name
Choose an application that you have already created in the AWS CodeDeploy console. Or create an application in the AWS CodeDeploy console and then return to this task.
AAR-CICD
Deployment group
Choose a deployment group that you have already created in the AWS CodeDeploy console. Or create a deployment group in the AWS CodeDeploy console and then return to this task.
AAR-CICD-DP
Configure automatic rollback on stage failure
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

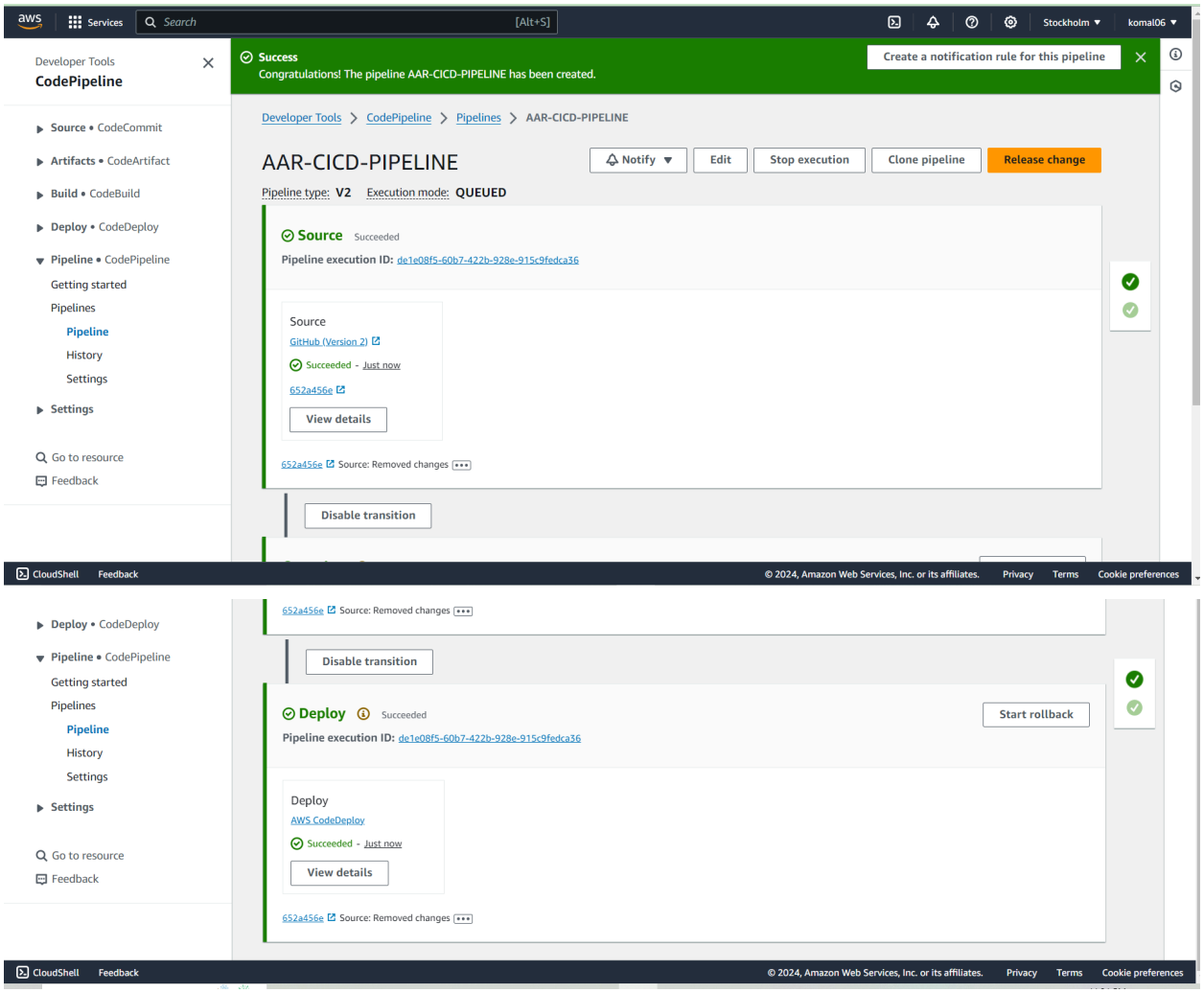

Developer Tools
CodePipeline
Pipelines
Create new pipeline
Step 1
Choose pipeline settings
Step 2
Add source stage
Step 3
Add build stage
Step 4
Add deploy stage
Step 5
Review
Review Info
Step 5 of 5
Step 1: Choose pipeline settings
Pipeline settings
Pipeline name
AAR-CICD-PIPELINE
Pipeline type
V2
Execution mode
QUEUED
Artifact location
A new Amazon S3 bucket will be created as the default artifact store for your pipeline
Service role name
AWSCodePipelineServiceRole-eu-north-1-AAR-CICD-PIPELINE


Step 2: Add source stage
Source action provider
Source action provider
GitHub (Version 2)
OutputArtifactFormat
CODE_ZIP
DetectChanges
false
ConnectionArn
arn:aws:codeconnections:eu-north-1:010928179348:connection/22754df1-fe9a-4b28-8f88-62eeef7233e2
FullRepositoryId
KomalDeolekar0607/ad_devops_exp_2
Default branch
main
Trigger configuration
You can add additional pipeline triggers after the pipeline is created.
Trigger type
Specify filter
© 2024, Amazon Web Services, Inc. or its affiliates.

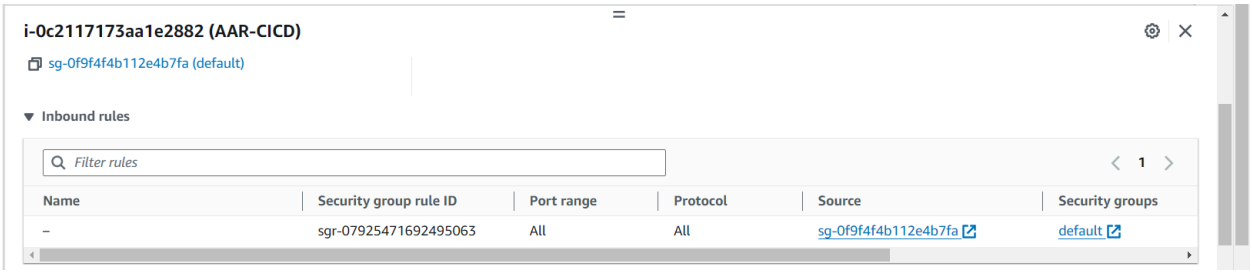

Trigger
Trigger type
Choose the trigger type that starts your pipeline.
No filter
Starts your pipeline on any push and clones the HEAD.
Specify filter
Starts your pipeline on a specific filter and clones the exact commit. Pipeline type V2 is required.
Do not detect changes
Don't automatically trigger the pipeline.
You can add additional sources and triggers by editing the pipeline after it is created.
The trigger configuration for the source action is not valid. Make sure to choose one trigger configuration for each source action.
Cancel
Previous
Next
© 2024, Amazon Web Services, Inc. or its affiliates.

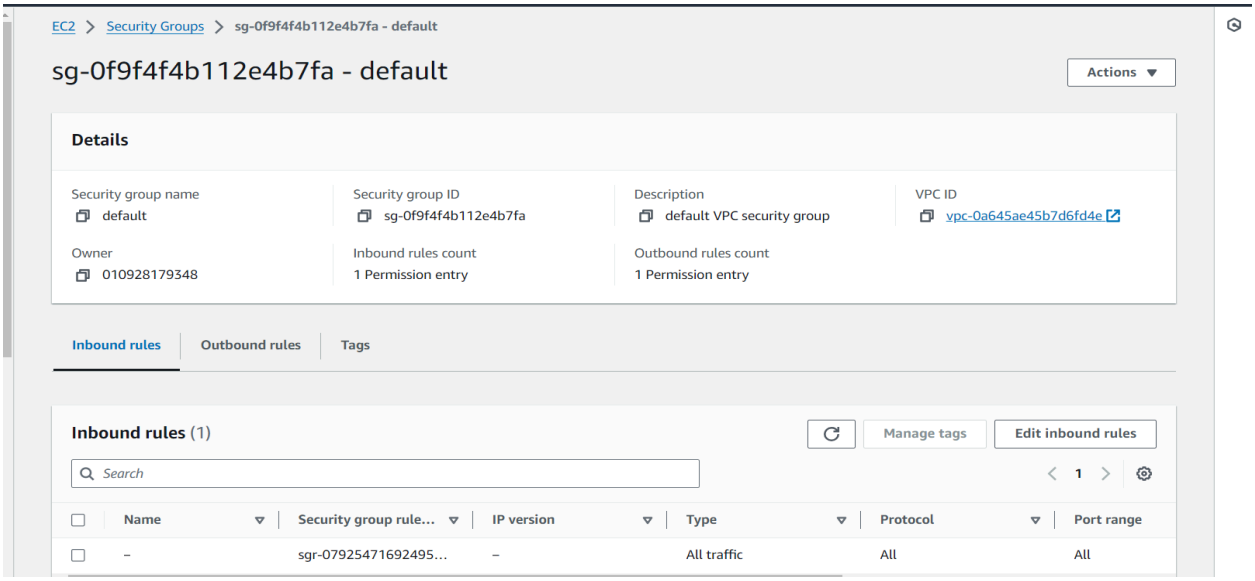

[Alt+S]
Step 2: Add source stage
Source action provider
Source action provider
GitHub (Version 2)
OutputArtifactFormat
CODE_ZIP
DetectChanges
true
ConnectionArn
arn:aws:codeconnections:eu-north-1:010928179348:connection/22754df1-fe9a-4b28-8f88-62eeef7233e2
FullRepositoryId
KomalDeolekar0607/ad_devops_exp_2
Default branch
main
Trigger configuration
You can add additional pipeline triggers after the pipeline is created.
Trigger type
No filter
© 2024, Amazon Web Services, Inc. or its affiliates.

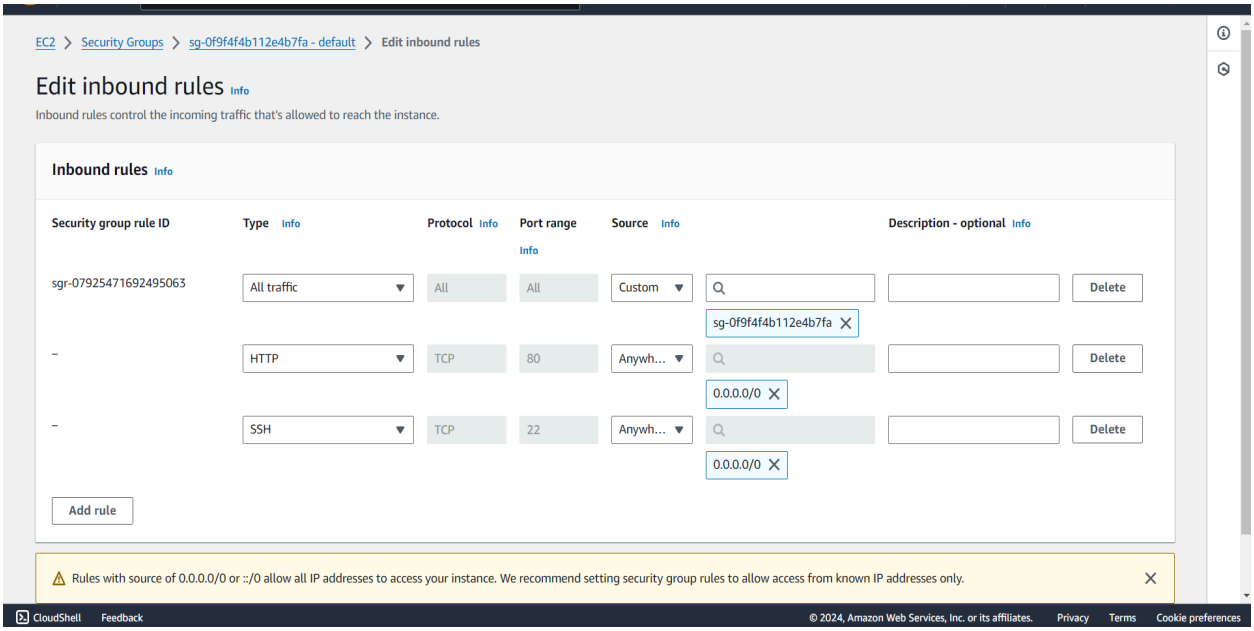

Step 3: Add build stage
Build action provider
Build stage
No build
Step 4: Add deploy stage
Deploy action provider
Deploy action provider
AWS CodeDeploy
ApplicationName
AAR-CICD
DeploymentGroupName
AAR-CICD-DP
Configure automatic rollback on stage failure
Disabled
Cancel
Previous
Create pipeline

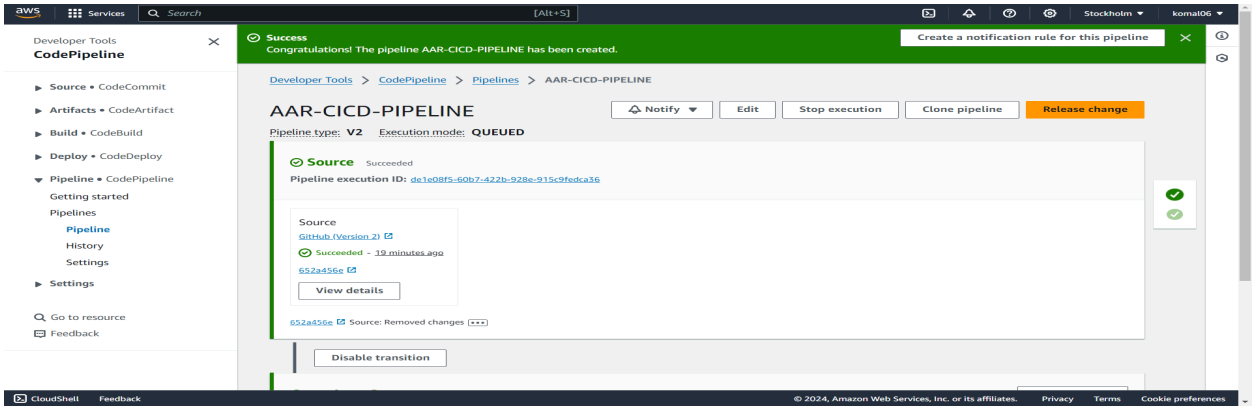

Developer Tools
CodePipeline
Success
Congratulations! The pipeline AAR-CICD-PIPELINE has been created.
Create a notification rule for this pipeline
Developer Tools > CodePipeline > Pipelines > AAR-CICD-PIPELINE
AAR-CICD-PIPELINE
Notify
Edit
Stop execution
Clone pipeline
Release change
Pipeline type: V2
Execution mode: QUEUED
Source
Succeeded
Pipeline execution ID: de1e08f5-60b7-422b-928e-915c9fedca36
Source
GitHub (Version 2)
Succeeded - Just now
652a456e
View details
652a456e Source: Removed changes
Disable transition
Source • CodeCommit
Artifacts • CodeArtifact
Build • CodeBuild
Deploy • CodeDeploy
Pipeline • CodePipeline
Getting started
Pipelines
Pipeline
History
Settings
Settings
Go to resource
Feedback
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

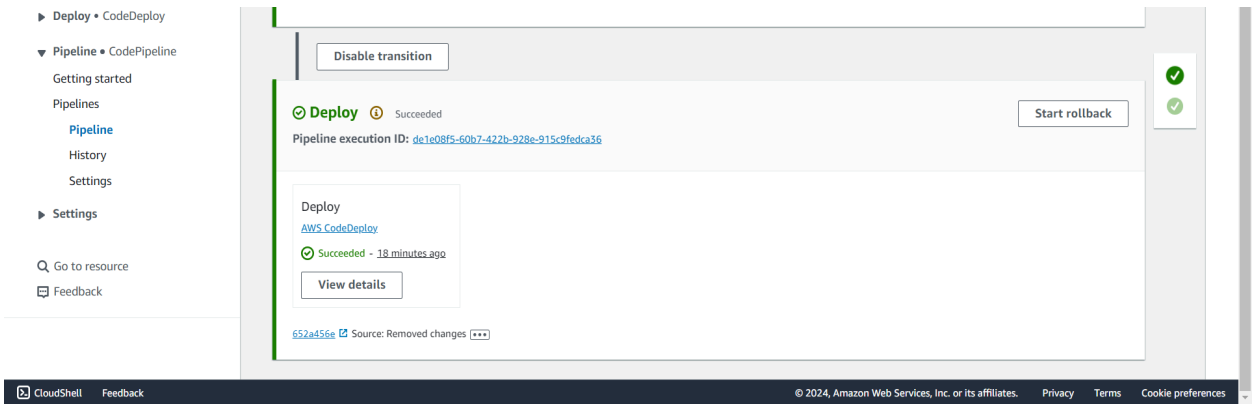
652a456e Source: Removed changes
Disable transition
Deploy
Succeeded
Start rollback
Pipeline execution ID: de1e08f5-60b7-422b-928e-915c9fedca36
Deploy
AWS CodeDeploy
Succeeded - Just now
View details
652a456e Source: Removed changes
Deploy • CodeDeploy
Pipeline • CodePipeline
Getting started
Pipelines
Pipeline
History
Settings
Settings
Go to resource
Feedback
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

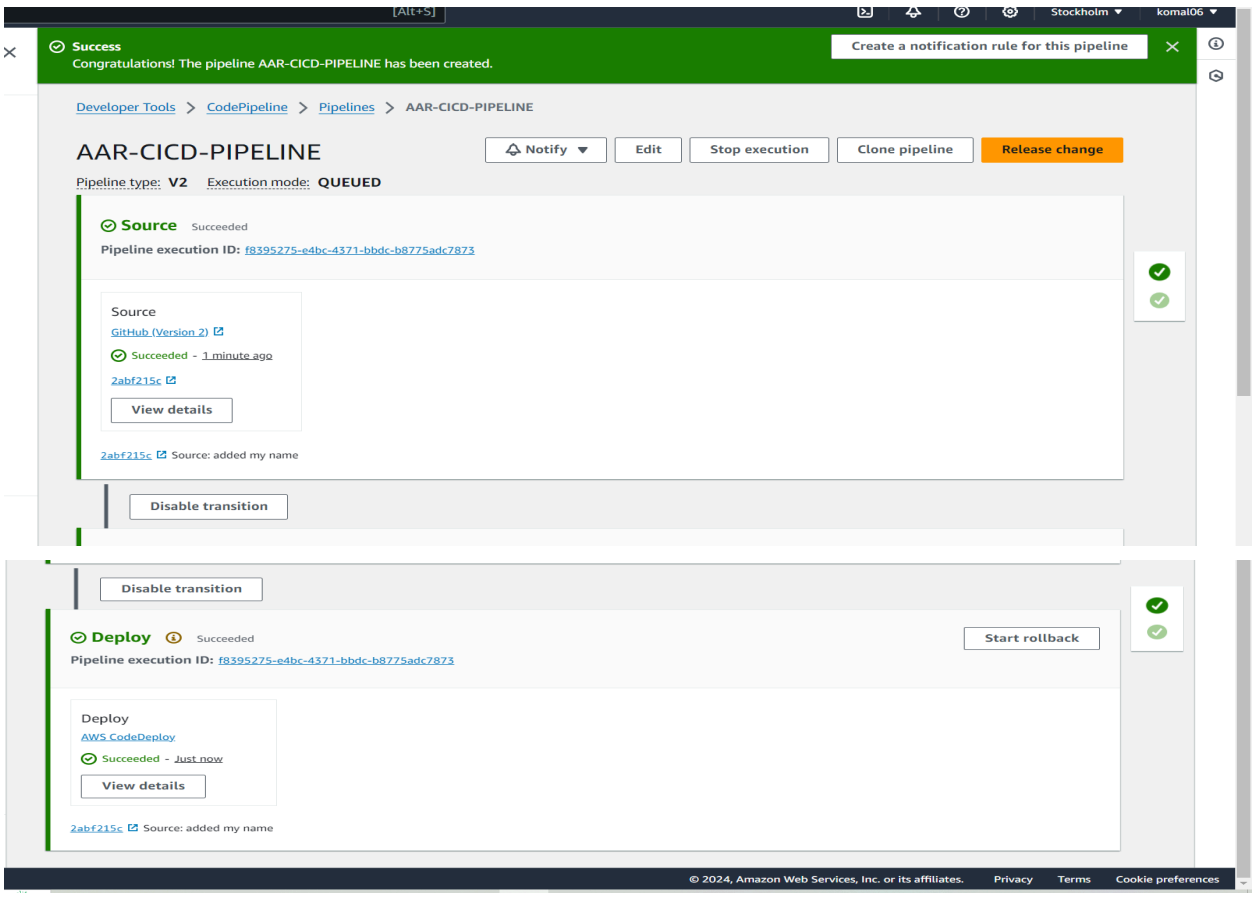

i-0c2117173aa1e2882 (AAR-CICD)
sg-0f9f4f4b112e4b7fa (default)
Inbound rules
Filter rules
1
Name
Security group rule ID
Port range
Protocol
Source
Security groups
–
sgr-07925471692495063
All
All
sg-0f9f4f4b112e4b7fa
default


EC2 > Security Groups > sg-0f9f4f4b112e4b7fa - default
sg-0f9f4f4b112e4b7fa - default
Actions
Details
Security group name
default
Security group ID
sg-0f9f4f4b112e4b7fa
Description
default VPC security group
VPC ID
vpc-0a645ae45b7d6fd4e
Owner
010928179348
Inbound rules count
1 Permission entry
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Tags
Inbound rules (1)
Manage tags
Edit inbound rules
Search
1
Name
Security group rule...
IP version
Type
Protocol
Port range
–
sgr-07925471692495...
–
All traffic
All
All


EC2 > Security Groups > sg-0f9f4f4b112e4b7fa - default > Edit inbound rules
Edit inbound rules
Info
Inbound rules control the incoming traffic that's allowed to reach the instance.
Inbound rules
Info
Security group rule ID
Type
Info
Protocol
Info
Port range
Info
Source
Info
Description - optional
Info
sgr-07925471692495063
All traffic
All
All
Custom
sg-0f9f4f4b112e4b7fa
Delete
–
HTTP
TCP
80
Anywh...
0.0.0.0/0
Delete
–
SSH
TCP
22
Anywh...
0.0.0.0/0
Delete
Add rule
Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Developer Tools
CodePipeline
Source • CodeCommit
Artifacts • CodeArtifact
Build • CodeBuild
Deploy • CodeDeploy
Pipeline • CodePipeline
Getting started
Pipelines
Pipeline
History
Settings
Settings
Go to resource
Feedback
Success
Congratulations! The pipeline AAR-CICD-PIPELINE has been created.
Create a notification rule for this pipeline
Developer Tools > CodePipeline > Pipelines > AAR-CICD-PIPELINE
AAR-CICD-PIPELINE
Notify
Edit
Stop execution
Clone pipeline
Release change
Pipeline type: V2
Execution mode: QUEUED
Source
Succeeded
Pipeline execution ID: de1e08f5-60b7-422b-928e-915c9fedca36
Source
GitHub (Version 2)
Succeeded - 19 minutes ago
652a456e
View details
652a456e Source: Removed changes
Disable transition
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Deploy • CodeDeploy
Pipeline • CodePipeline
Getting started
Pipelines
Pipeline
History
Settings
Settings
Go to resource
Feedback
Disable transition
Deploy
Succeeded
Start rollback
Pipeline execution ID: de1e08f5-60b7-422b-928e-915c9fedca36
Deploy
AWS CodeDeploy
Succeeded - 18 minutes ago
View details
652a456e Source: Removed changes
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

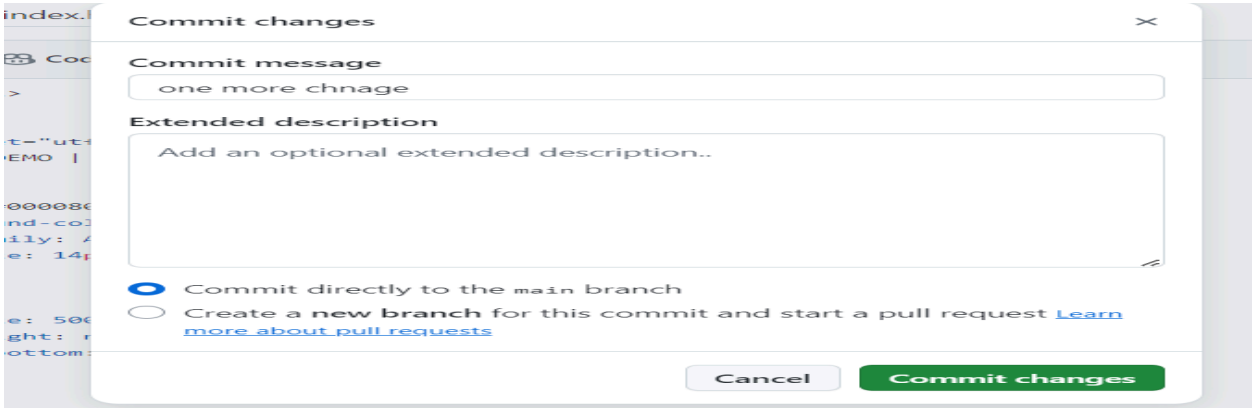

Success
Congratulations! The pipeline AAR-CICD-PIPELINE has been created.
Create a notification rule for this pipeline
Developer Tools > CodePipeline > Pipelines > AAR-CICD-PIPELINE
AAR-CICD-PIPELINE
Notify
Edit
Stop execution
Clone pipeline
Release change
Pipeline type: V2
Execution mode: QUEUED
Source
Succeeded
Pipeline execution ID: f8395275-e4bc-4371-bbdc-b8775adc7873
Source
GitHub (Version 2)
Succeeded - 1 minute ago
2abf215c
View details
2abf215c Source: added my name
Disable transition
Disable transition
Deploy
Succeeded
Start rollback
Pipeline execution ID: f8395275-e4bc-4371-bbdc-b8775adc7873
Deploy
AWS CodeDeploy
Succeeded - Just now
View details
2abf215c Source: added my name
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

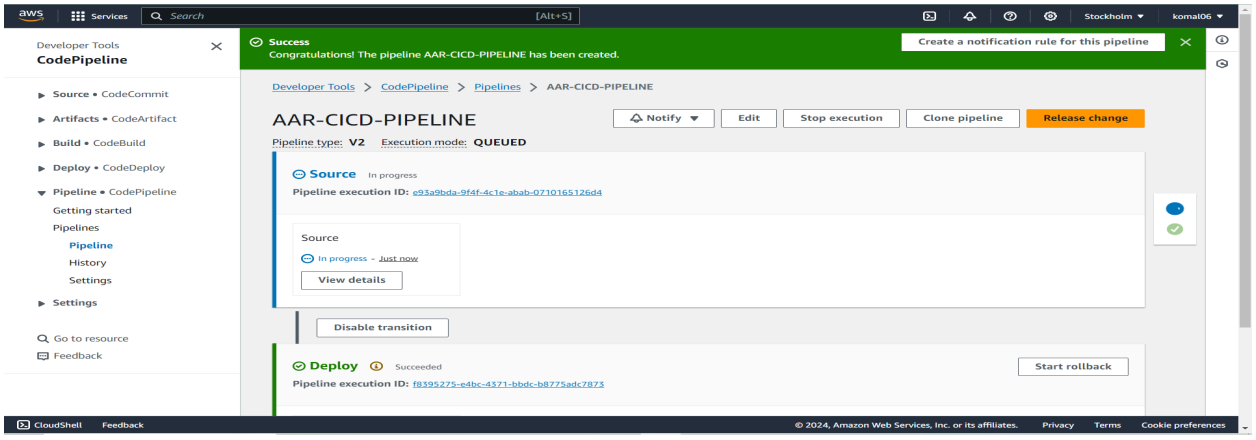
Congratulations Komal!!!

Welcome to AAR SOURCE| Ram Hemareddy

This application was deployed using AWS CodeDeploy.

For next steps, read the AWS CodeDeploy Documentation.





Congratulations Komal!!!

Welcome to AAR SOURCE| Ram Hemareddy | Komal

This application was deployed using AWS CodeDeploy.

For next steps, read the AWS CodeDeploy Documentation.

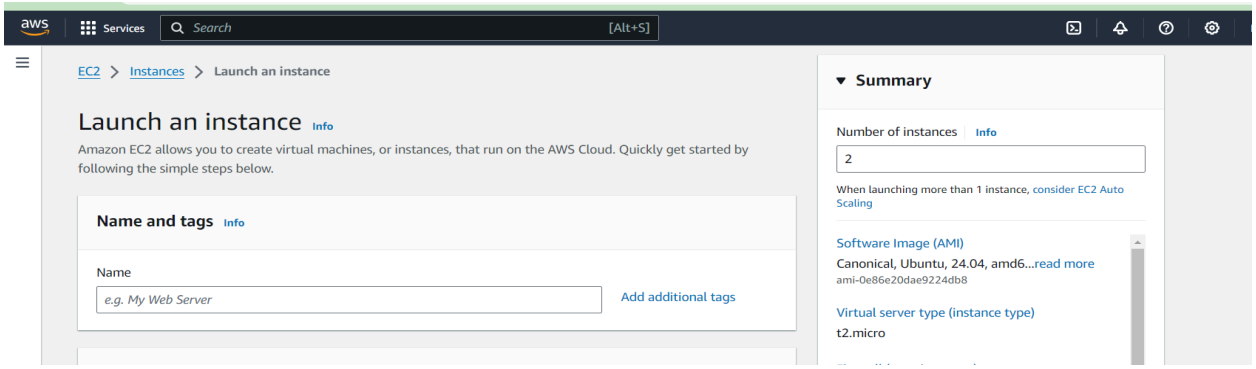
Experiment No. 3

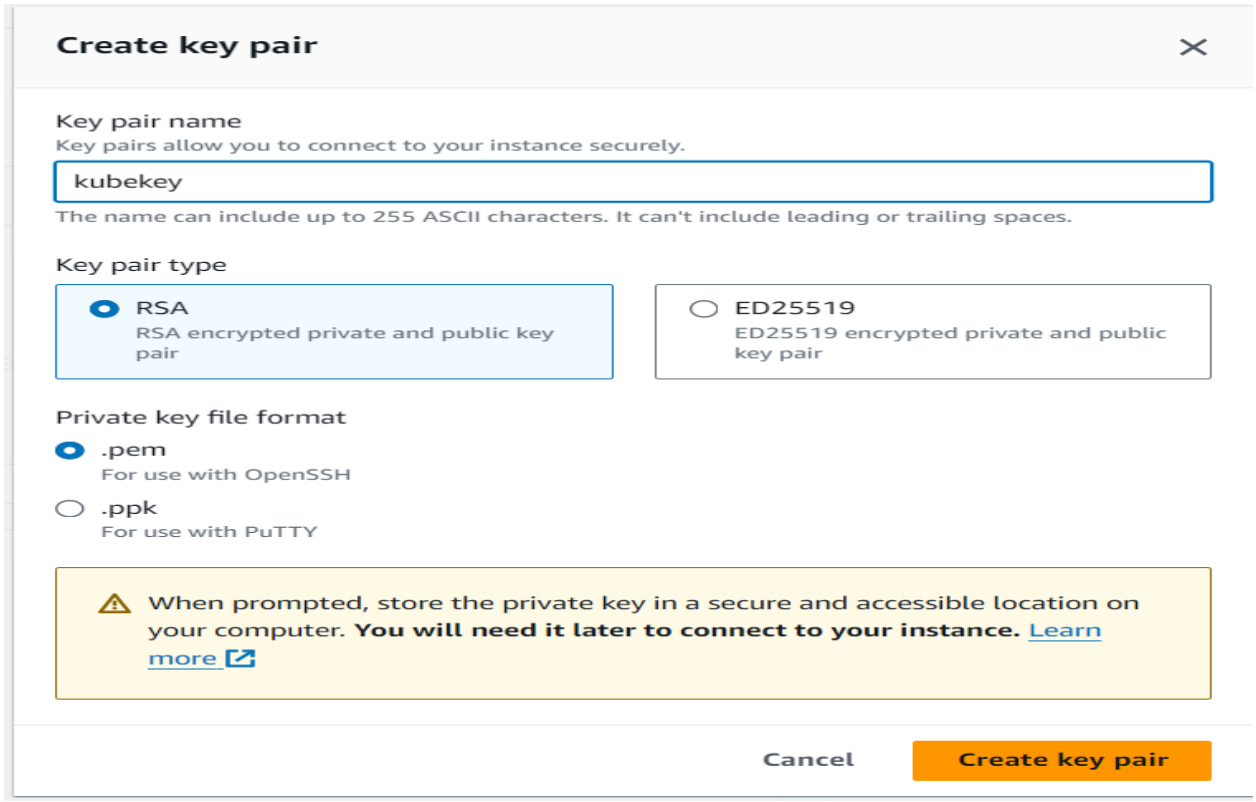
AIM : To understand the Kubernetes Cluster Architecture, Install and Spin Up a Kubernetes Cluster on Linux Machines/Cloud Platforms.

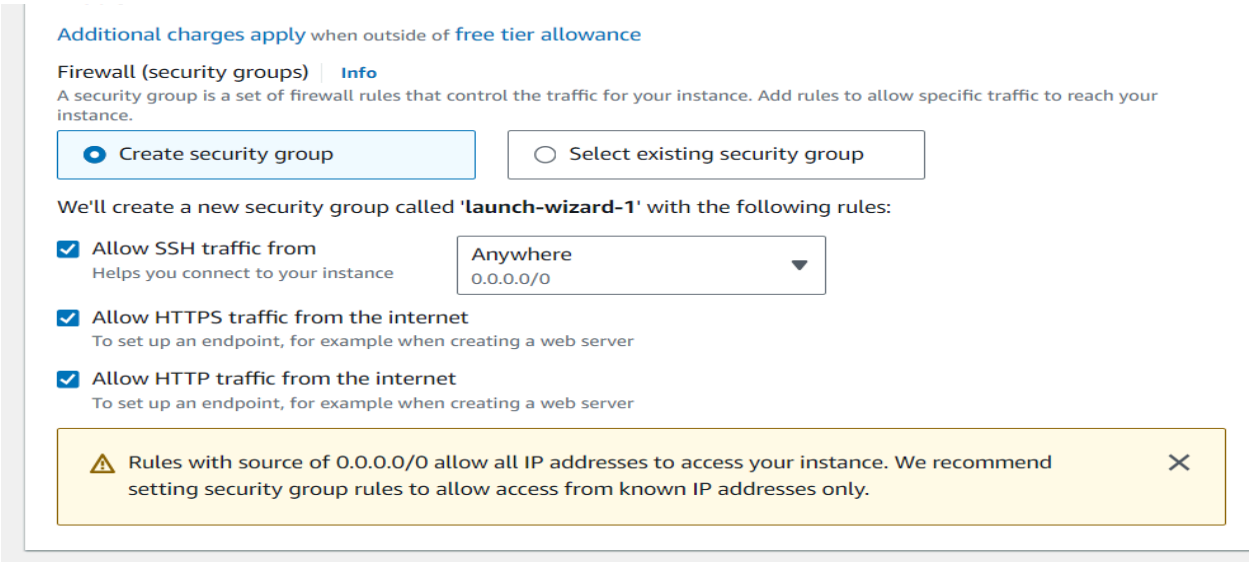
Steps :

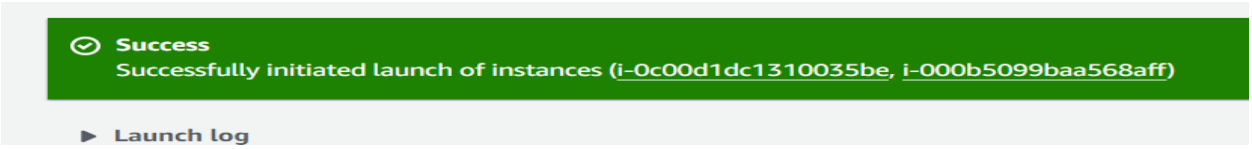
Step1 : First delete all security groups so that no conflict will occur

Step2 : Create 2 EC2 instances one for master and one for worker node
(you can write number of instances 2 so 2 instances will get create with same configuration)

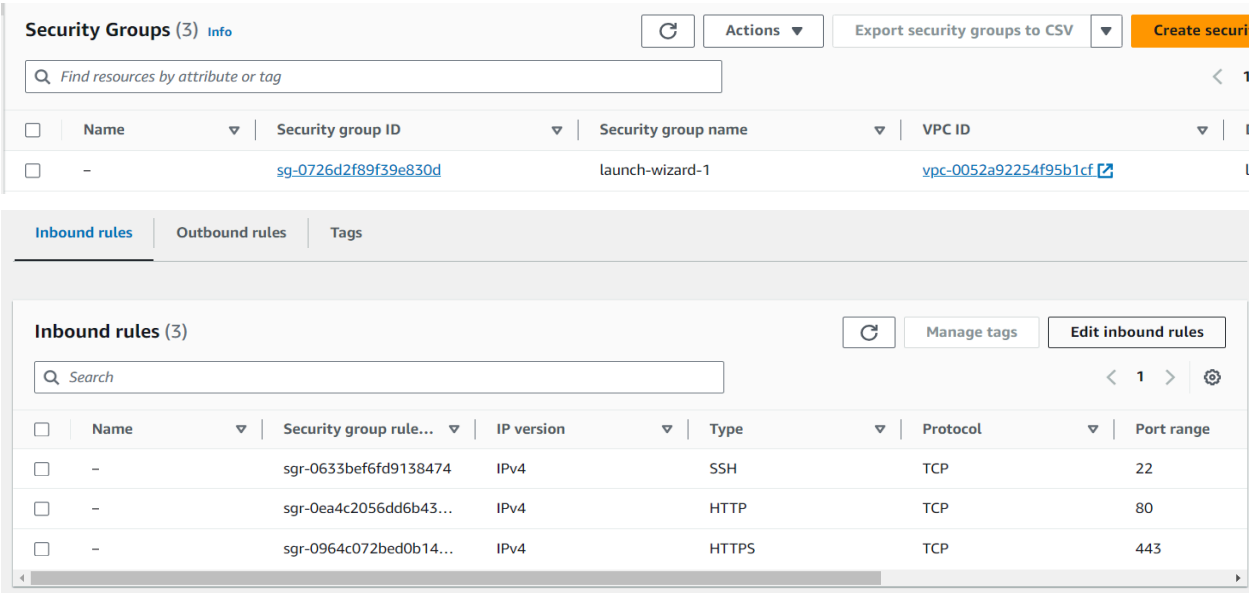




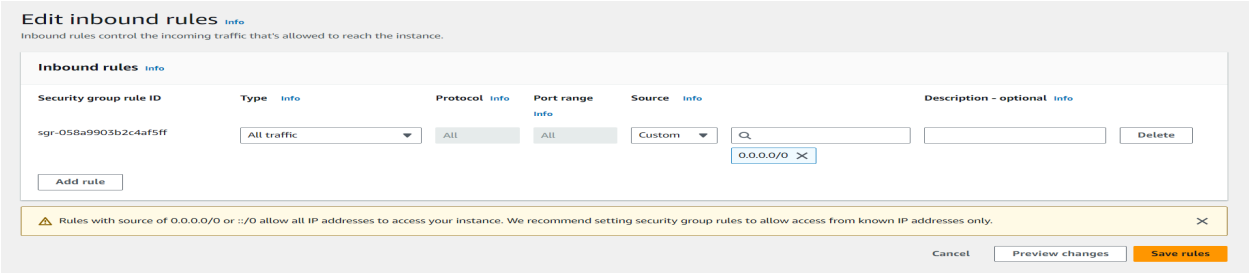




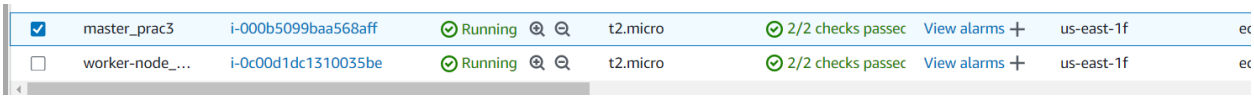
Step3 : Now the security group which we specified while creating instances we will be able to see that in security groups

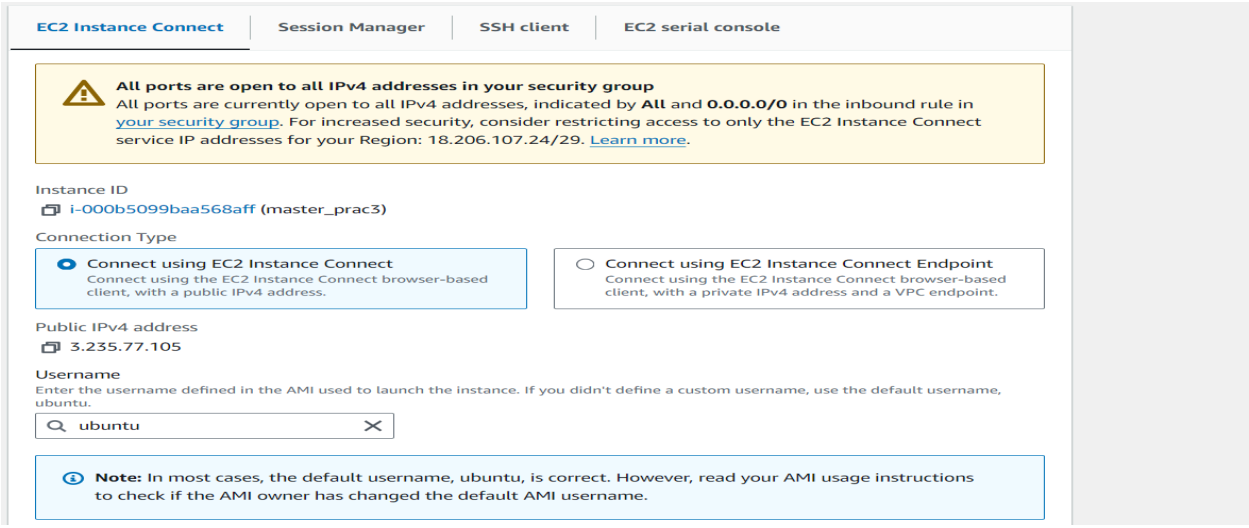


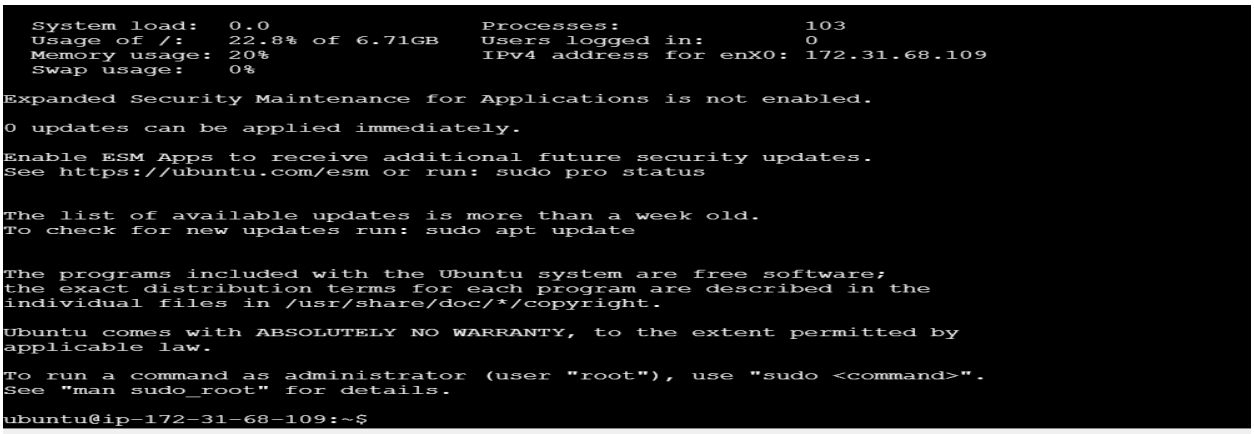
Step4 : Then click on edit inbound rules delete all rules and add new rule by selecting all traffic in type and by allowing all ipv4 ports for communication (by this we can be able to communicate with all ports) and then save

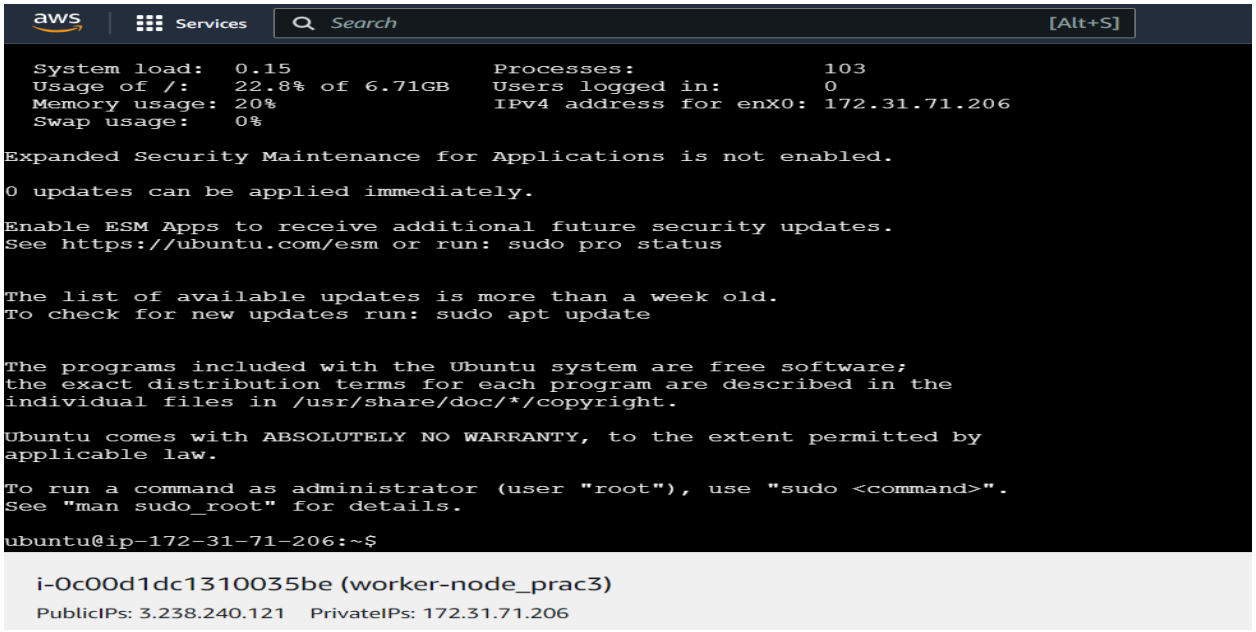


Step5 : Then connect both of the instances by selecting the instance and click on connect individually. (so they will connect to their ec2 instance connect)

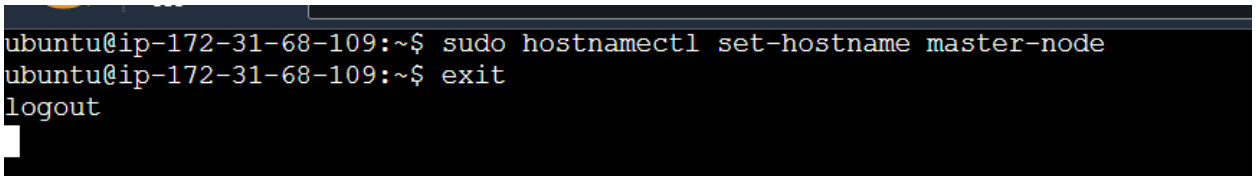


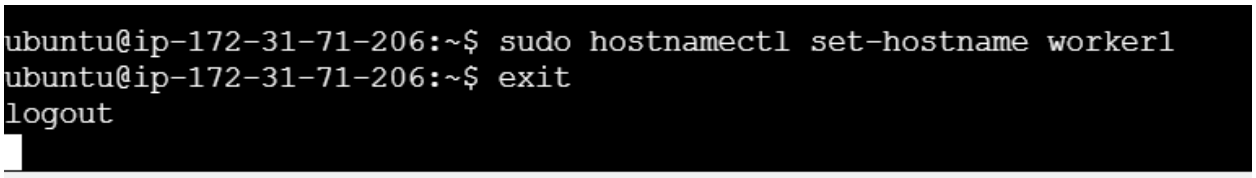






Step6 : Then give name to nodes as master and worker for identification





Then execute below commands in both the instances

Step7 : Update packet manager

Step8 : Install docker on all nodes

```
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-com
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 133 not upgraded.
```

Step9 : Enable the docker and check its status

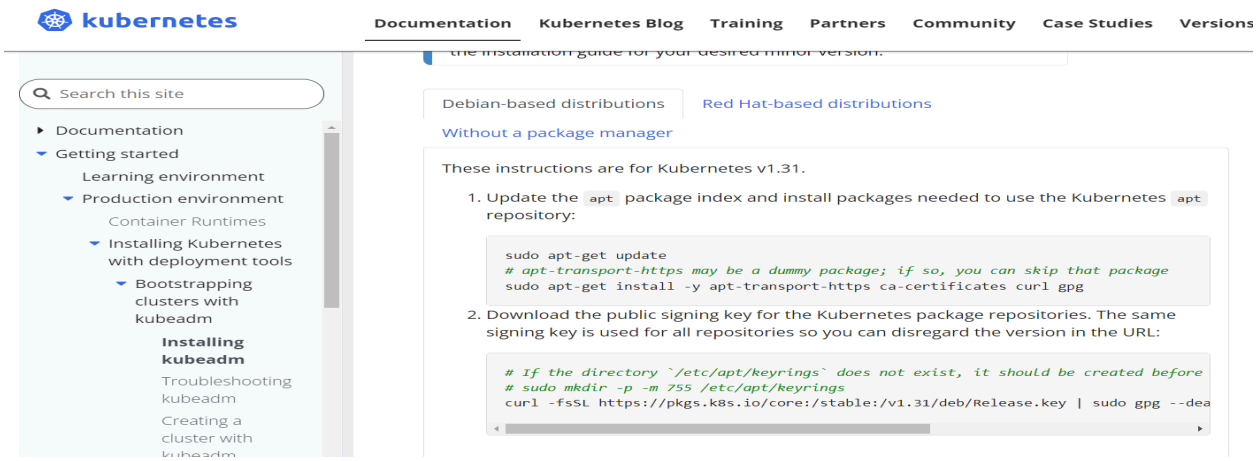
```
ubuntu@master-node:~$ sudo systemctl enable docker
ubuntu@master-node:~$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: enabled)
     Active: active (running) since Mon 2024-09-16 02:36:41 UTC; 1min 55s ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 2681 (dockerd)
      Tasks: 7
     Memory: 33.0M (peak: 33.4M)
        CPU: 287ms
     CGroup: /system.slice/docker.service
             └─2681 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock

Sep 16 02:36:39 master-node systemd[1]: Starting docker.service - Docker Application Container Engine...
Sep 16 02:36:39 master-node dockerd[2681]: time="2024-09-16T02:36:39.994142271Z" level=info msg="Starting up"
Sep 16 02:36:39 master-node dockerd[2681]: time="2024-09-16T02:36:39.996175763Z" level=info msg="detected 127.0
Sep 16 02:36:40 master-node dockerd[2681]: time="2024-09-16T02:36:40.081459452Z" level=info msg="Loading contai
Sep 16 02:36:40 master-node dockerd[2681]: time="2024-09-16T02:36:40.430490054Z" level=info msg="Loading contai
Sep 16 02:36:41 master-node dockerd[2681]: time="2024-09-16T02:36:41.583873984Z" level=info msg="Docker daemon"
Sep 16 02:36:41 master-node dockerd[2681]: time="2024-09-16T02:36:41.584439056Z" level=info msg="Daemon has com
Sep 16 02:36:41 master-node dockerd[2681]: time="2024-09-16T02:36:41.639977888Z" level=info msg="API listen on
Sep 16 02:36:41 master-node systemd[1]: Started docker.service - Docker Application Container Engine.
lines 1-21/21 (END)
```

Step10 : Also start the docker

```
ubuntu@master-node:~$ sudo systemctl start docker
ubuntu@master-node:~$
```

Now search kubeadm for installing kubernetes and other required packages and refer the document

Step11 : Update the apt package index and install packages needed to use the Kubernetes apt repository for creating repository for kubernetes



```
ubuntu@master-node:~$ sudo apt-get update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
ubuntu@master-node:~$
```

i-000b5099baa568aff (master_prac3)

PublicIPs: 3.235.77.105 PrivateIPs: 172.31.68.109

```
ubuntu@master-node:~$ sudo apt-get install -y apt-transport-https ca-certificates curl gpg
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.
gpg is already the newest version (2.4.4-2ubuntu17).
gpg set to manually installed.
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 130 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-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 apt-transport-https all
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 curl amd64 8.5.0-2ub
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libcurl4t64 amd64 8.
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libcurl3t64-gnutls a
```

Step12 : Download the public signing key for the Kubernetes package repositories. The same signing key is used for all repositories so you can disregard the version in the URL

```
ubuntu@master-node:~$ curl -fsSL https://pkgs.k8s.io/core:/stable:/v1.31/deb/Release.key | sudo gpg --dearmor -o /etc/apt/keyrings/kubernetes-apt-keyring.gpg
ubuntu@master-node:~$ ^C
ubuntu@master-node:~$ echo 'deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:/v1.31/deb/ /' | sudo tee /etc/apt/sourc
es.list.d/kubernetes.list
deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:/v1.31/deb/ /
ubuntu@master-node:~$
```

Step13 : Update the apt package index

```
ubuntu@master-node:~$ sudo apt-get update
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
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports
Hit:5 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:4 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes
Get:6 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes
Fetched 132 kB in 1s (175 kB/s)
Reading package lists... Done
ubuntu@master-node:~$
```

Step14 : Then install kubelet kubeadm and kubectl

```
ubuntu@master-node:~$ 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 130 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://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 conntrack am
Get:2 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:
Get:3 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:
Get:4 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:
Get:5 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:
Get:6 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:
Fetched 87.4 MB in 1s (76.2 MB/s)
Selecting previously unselected package conntrack.
(Reading database ... 68112 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) ...
```

pin their version

```
ubuntu@master-node:~$ sudo apt-mark hold kubelet kubeadm kubectl
kubelet set on hold.
kubeadm set on hold.
kubectl set on hold.
ubuntu@master-node:~$
```

Step15 : Disable swap memory

```
ubuntu@master-node:~$ sudo swapoff -a
ubuntu@master-node:~$
```

Now follow below steps only on master node

Step16 : Initialize the kubernetes cluster on master node

```
ubuntu@master-node:~$ sudo kubeadm init --pod-network-cidr=10.244.0.0/16 --ignore-preflight-errors=all
[init] Using Kubernetes version: v1.31.0
[preflight] Running pre-flight checks
        [WARNING NumCPU]: the number of available CPUs 1 is less than the required 2
        [WARNING Mem]: the system RAM (957 MB) is less than the minimum 1700 MB
        [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 config images pull'
W0916 14:42:02.662037   21099 checks.go:846] detected that the sandbox image "registry.k8s.io/pause:3.8" of the container runtime
y 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 [kubernetes kubernetes.default kubernetes.default.svc kubernetes.default.
 IPs [10.96.0.1 172.31.68.109]
[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 [localhost master-node] and IPs [172.31.68.109 127.0.0.1 ::1]
[certs] Generating "etcd/peer" certificate and key
[certs] etcd/peer serving cert is signed for DNS names [localhost master-node] and IPs [172.31.68.109 127.0.0.1 ::1]
```

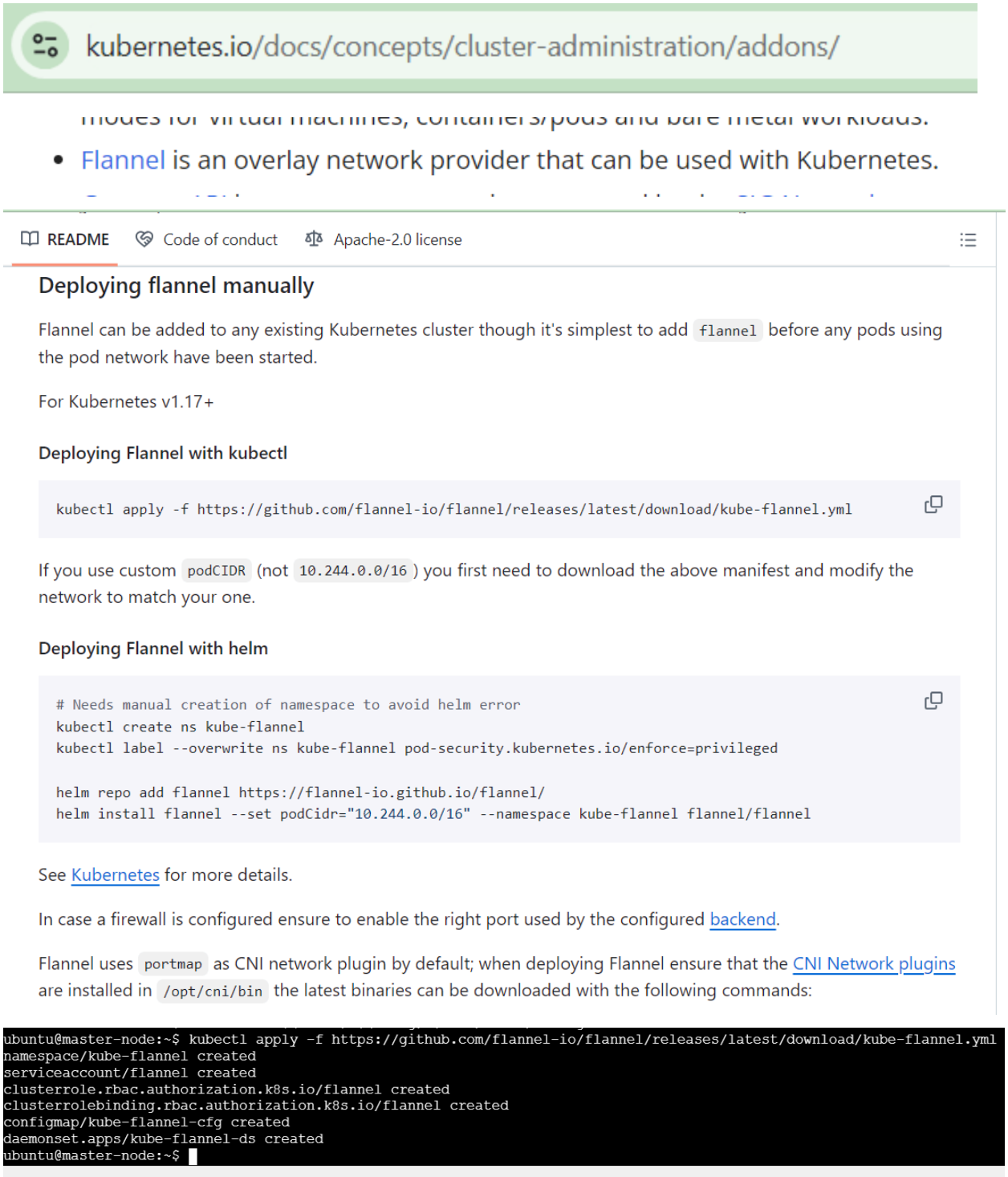
```
Your Kubernetes control-plane has initialized successfully!

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 each as root:

kubeadm join 172.31.68.109:6443 --token c8r2s0.hi8hsx8dt6td1sjf \
        --discovery-token-ca-cert-hash sha256:64987e22fa379fd818cb9a21d2075c7c148a4e1ece07951c8639b0ead0450af5
ubuntu@master-node:~$
```

Here we get the join command to run on worker node. Copy the join command and keep it in a notepad, we'll need it later.

Step17 : To make kubectl work for your non-root user, run these commands
Set up kubectl on master node

```
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) $HOME/.kube/config
ubuntu@master-node:~$
```

Step18 : To enable communication between pods, install a pod network plugin like flannel or calico
(This is needed for communication between pods or containers)
add a common networking plugin called flammel file as written
(this will deploy flannel with kubectl)



Now run below command only on worker node

Step19 : Then run the join command on worker node which we copied when we executed init command on master

run in worker node with sudo(for access)

(this will join the worker node with master)a

```
ubuntu@worker1:~$ sudo kubeadm join 172.31.68.109:6443 --token c8r2s0.hi8hsx8dt6td1sjf --discovery-token-ca-cert-has
e1ece07951c8639b0ead0450af5 --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 1.002781661s
[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.

ubuntu@worker1:~$
```

Step20 : Verify the cluster once the worker node joins , check the status on the master node

```
ubuntu@master-node:~$ kubectl get nodes
NAME          STATUS   ROLES           AGE   VERSION
master-node   Ready    control-plane   22m   v1.31.1
worker1       Ready    <none>          47s   v1.31.1
ubuntu@master-node:~$
```

```
ubuntu@master-node:~$ kubectl get pods --all-namespaces
NAMESPACE      NAME                                  READY   STATUS             RESTARTS        AGE
kube-flannel   kube-flannel-ds-2944s                 1/1     Running            0               32m
kube-flannel   kube-flannel-ds-t77qg                 1/1     Running            0               23m
kube-system    coredns-7c65d6cfc9-2tk7z              1/1     Running            0               45m
kube-system    coredns-7c65d6cfc9-vn7xh              1/1     Running            0               45m
kube-system    etcd-master-node                      1/1     Running            0               45m
kube-system    kube-apiserver-master-node            1/1     Running            0               45m
kube-system    kube-controller-manager-master-node   1/1     Running            0               45m
kube-system    kube-proxy-5wprn                      0/1     CrashLoopBackOff   11 (27s ago)    45m
kube-system    kube-proxy-6cx84                      0/1     CrashLoopBackOff   7 (4m4s ago)    23m
kube-system    kube-scheduler-master-node            1/1     Running            0               45m
ubuntu@master-node:~$
```

i-000b5099baa568aff (master_prac3)

PublicIPs: 3.235.77.105 PrivateIPs: 172.31.68.109

```
ubuntu@master-node:~$ kubectl get pods --all-namespaces
NAMESPACE      NAME                                  READY   STATUS             RESTARTS         AGE
kube-flannel   kube-flannel-ds-2944s                 1/1     Running            0                34m
kube-flannel   kube-flannel-ds-t77qg                 1/1     Running            0                25m
kube-system    coredns-7c65d6cfc9-2tk7z              1/1     Running            0                47m
kube-system    coredns-7c65d6cfc9-vn7xh              1/1     Running            0                47m
kube-system    etcd-master-node                      1/1     Running            0                47m
kube-system    kube-apiserver-master-node            1/1     Running            0                47m
kube-system    kube-controller-manager-master-node   1/1     Running            0                47m
kube-system    kube-proxy-5wprn                      0/1     CrashLoopBackOff   11 (2m36s ago)   47m
kube-system    kube-proxy-6cx84                      1/1     Running            8 (6m13s ago)    25m
kube-system    kube-scheduler-master-node            1/1     Running            0                47m
```

EXPERIMENT NO.4

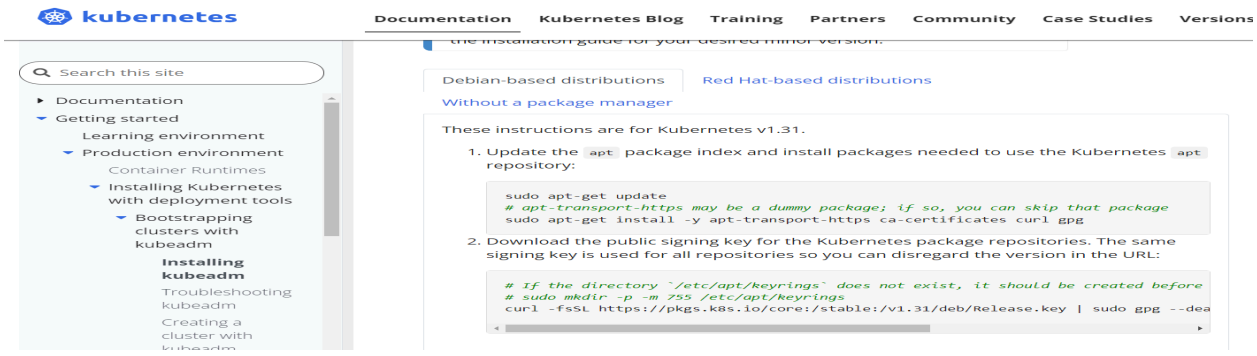
AIM : To install Kubectl and execute Kubectl commands to manage the Kubernetes cluster and deploy Your First Kubernetes Application.

Steps :

Step1 : Create EC2 instance on aws and connect it also configure security groups to communicate with all ports

Now search kubeadm for installing kubernetes and other required packages and refer the document

Step2 : Update the apt package index and install packages needed to use the Kubernetes apt repository for creating repository for kubernetes




```
ubuntu@master-node:~$ sudo apt-get update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
ubuntu@master-node:~$
```

i-000b5099baa568aff (master_prac3)
PublicIPs: 3.235.77.105 PrivateIPs: 172.31.68.109

Install required packages for HTTPS and certificate transport

```
ubuntu@master-node:~$ sudo apt-get install -y apt-transport-https ca-certificates curl gpg
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.
gpg is already the newest version (2.4.4-2ubuntu17).
gpg set to manually installed.
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 130 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-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 apt-transport-https all
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 curl amd64 8.5.0-2ub
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libcurl4t64 amd64 8.
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libcurl3t64-gnutls a
```

Step3 : Download the public signing key for the Kubernetes package repositories. The same signing key is used for all repositories so you can disregard the version in the URL
Add the GPG ley & make repository for kubernetes

```
ubuntu@master-node:~$ curl -fsSL https://pkgs.k8s.io/core:/stable:/v1.31/deb/Release.key | sudo gpg --dearmor -o /etc/apt/keyrings/kubernetes-apt-keyring.gpg
ubuntu@master-node:~$ ^C
ubuntu@master-node:~$ echo 'deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:/v1.31/deb/ /' | sudo tee /etc/apt/sourc
es.list.d/kubernetes.list
deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:/v1.31/deb/ /
ubuntu@master-node:~$
```

Step4 : Update the apt package index

```
ubuntu@master-node:~$ sudo apt-get update
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
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports
Hit:5 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:4 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:
Get:6 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:
Fetched 132 kB in 1s (175 kB/s)
Reading package lists... Done
ubuntu@master-node:~$
```

Step5 : Then install kubelet kubeadm and kubectl

```
ubuntu@master-node:~$ 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 130 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://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 conntrack am
Get:2 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:
Get:3 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:
Get:4 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:
Get:5 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:
Get:6 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:
Fetched 87.4 MB in 1s (76.2 MB/s)
Selecting previously unselected package conntrack.
(Reading database ... 68112 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) ...
```

pin their version

```
ubuntu@master-node:~$ sudo apt-mark hold kubelet kubeadm kubectl
kubelet set on hold.
kubeadm set on hold.
kubectl set on hold.
ubuntu@master-node:~$
```

Step6 : Disable swap memory

```
ubuntu@master-node:~$ sudo swapoff -a
ubuntu@master-node:~$
```

Step7 : Initialize the kubernetes cluster on master node

```
ubuntu@master-node:~$ sudo kubeadm init --pod-network-cidr=10.244.0.0/16 --ignore-preflight-errors=all
[init] Using Kubernetes version: v1.31.0
[preflight] Running pre-flight checks
        [WARNING NumCPU]: the number of available CPUs 1 is less than the required 2
        [WARNING Mem]: the system RAM (957 MB) is less than the minimum 1700 MB
        [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 config images pull'
W0916 14:42:02.662037   21099 checks.go:846] detected that the sandbox image "registry.k8s.io/pause:3.8" of the container runtime
y 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 [kubernetes kubernetes.default kubernetes.default.svc kubernetes.default.
 IPs [10.96.0.1 172.31.68.109]
[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 [localhost master-node] and IPs [172.31.68.109 127.0.0.1 ::1]
[certs] Generating "etcd/peer" certificate and key
[certs] etcd/peer serving cert is signed for DNS names [localhost master-node] and IPs [172.31.68.109 127.0.0.1 ::1]
```

```
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 each as root:

kubeadm join 172.31.68.109:6443 --token c8r2s0.hi8hsx8dt6td1sjf \
        --discovery-token-ca-cert-hash sha256:64987e22fa379fd818cb9a21d2075c7c148a4e1ece07951c8639b0ead0450af5
ubuntu@master-node:~$
```

Step8 : To make kubectl work for your non-root user, run these commands

Set up kubectl on master node

```
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) $HOME/.kube/config
ubuntu@master-node:~$
```

Step9 : To enable communication between pods, install a pod network plugin like flannel or calico


```
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:~$
```

Step10 : Then run the join command on worker node which we got in init command of master

```
ubuntu@worker1:~$ sudo kubeadm join 172.31.68.109:6443 --token c8r2s0.hi8hsx8dt6td1sjf --discovery-token-ca-cert-has
e1ece07951c8639b0ead0450af5 --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 1.002781661s
[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.

ubuntu@worker1:~$
```

Step11 : Verify the cluster once the worker node joins , check the status on the master node

```
ubuntu@master-node:~$ kubectl get nodes
NAME           STATUS   ROLES           AGE   VERSION
master-node    Ready    control-plane   22m   v1.31.1
worker1        Ready    <none>          47s   v1.31.1
ubuntu@master-node:~$
```

Deploying application on kubernetes

Step12 : search this in web and copy the code which is present on that page

kubernetes.io/docs/concepts/workloads/controllers/deployment/

controllers/nginx-deployment.yaml

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  labels:
    app: nginx
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx:1.14.2
        ports:
        - containerPort: 80
```

Step13 : In node create one file deploy.yaml with the help of nano editor and paste that code inside it.

```
ubuntu@master-node:~$ sudo nano deploy.yaml
```

```
  GNU nano 7.2
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  labels:
    app: nginx
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx:1.14.2
        ports:
        - containerPort: 80

^G Help          ^O Write Out     ^W Where Is      ^K
^X Exit          ^R Read File     ^\ Replace       ^U
```

```
File Name to Write: deploy.yaml
^G Help                  M-D DOS Format           M-A Append               M-
^C Cancel                M-M Mac Format           M-P Prepend              ^
```

Then to save Ctrl+o enter and ctrl+x to exit the editor

Step14 : Deploy the application

Use kubectl to create deployment from the yaml file

```
ubuntu@master-node:~$ kubectl create -f deploy.yaml
deployment.apps/nginx-deployment created
ubuntu@master-node:~$
```

Step15 : Verify the deployment , check the status of your deployment

```
ubuntu@master-node:~$ kubectl get deploy
NAME               READY   UP-TO-DATE   AVAILABLE   AGE
nginx-deployment   3/3     3            3           2m35s
ubuntu@master-node:~$
```

i-000b5099baa568aff (master_prac3)

Step16 : Now expose the deployment

kubectl expose deployment.apps/nginx-deployment --type="LoadBalancer"

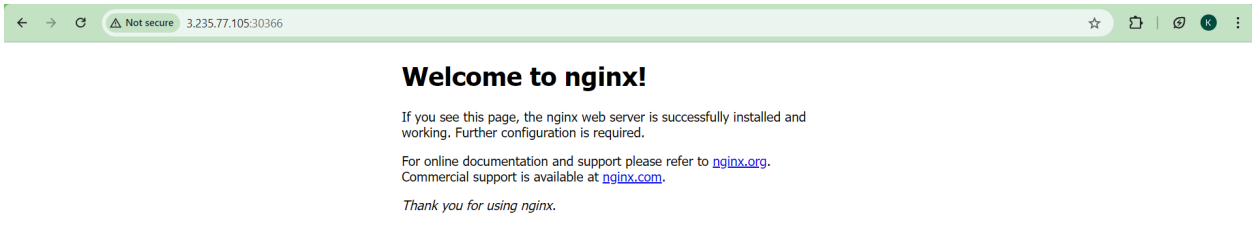
```
ubuntu@master-node:~$ kubectl expose deployment.apps/nginx-deployment --type="LoadBalancer"
service/nginx-deployment exposed
ubuntu@master-node:~$
```

Step17 : Check status of the service

```
ubuntu@master-node:~$ kubectl get svc
NAME               TYPE           CLUSTER-IP       EXTERNAL-IP   PORT(S)        AGE
kubernetes         ClusterIP      10.96.0.1        <none>        443/TCP        74m
nginx-deployment   LoadBalancer   10.109.172.152   <pending>     80:30366/TCP   90s
ubuntu@master-node:~$
```

Step18 : paste the ip public ip address of the ec2 instance we are working and then colon (:) and port number of the service here it is 30366 and the enter

Done your application has deployed

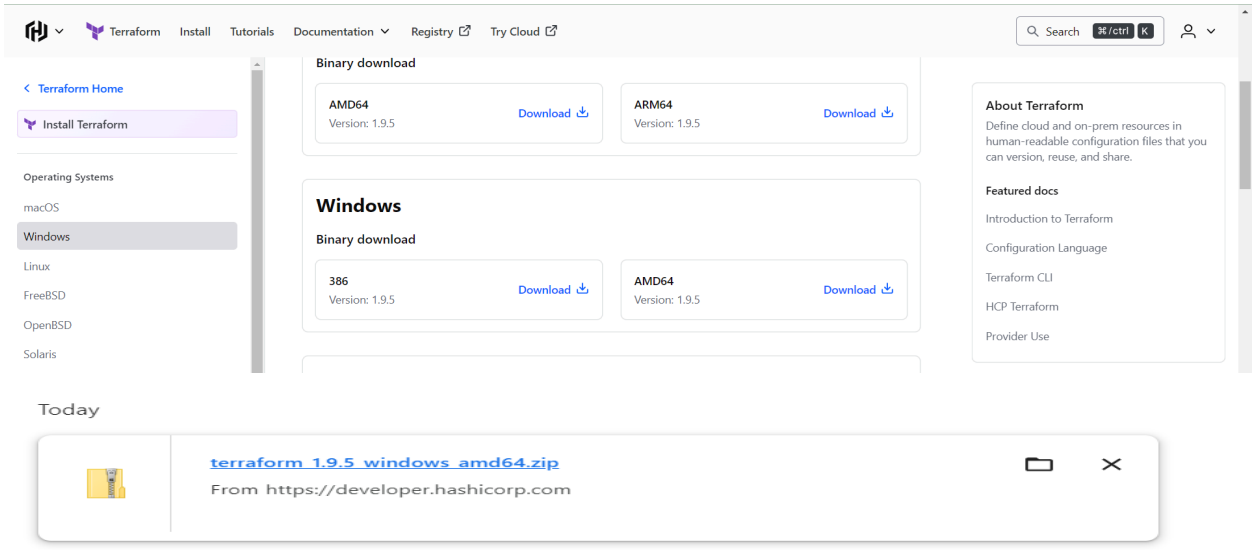


Experiment No. 5

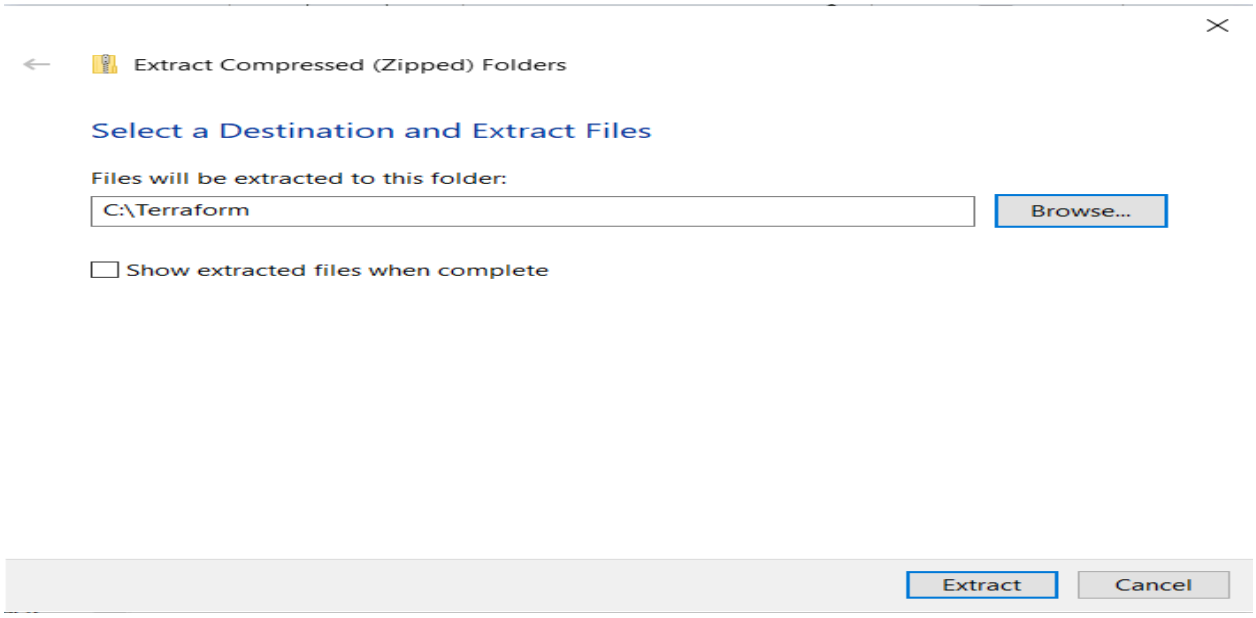
Installation and Configuration of Terraform in Windows

Step 1: Download terraform

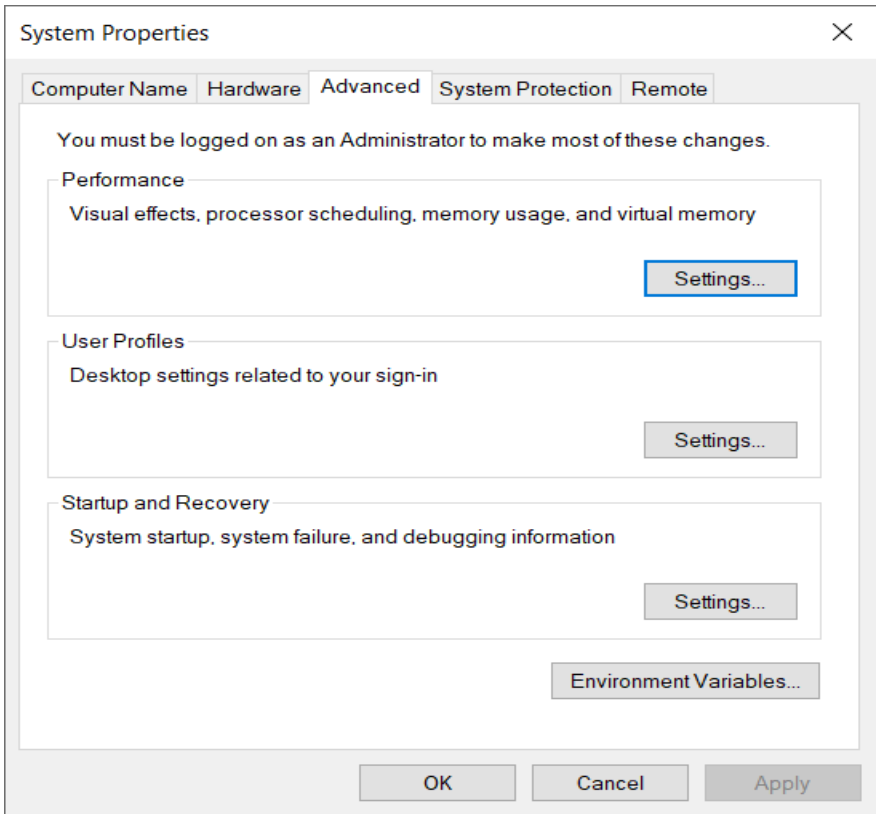
First Download the Terraform Cli Utility for windows from terraforms official website
website:https://www.terraform.io/downloads.html
Select the Operating System Windows followed by either 32bit or 64 bit based on your OS type.

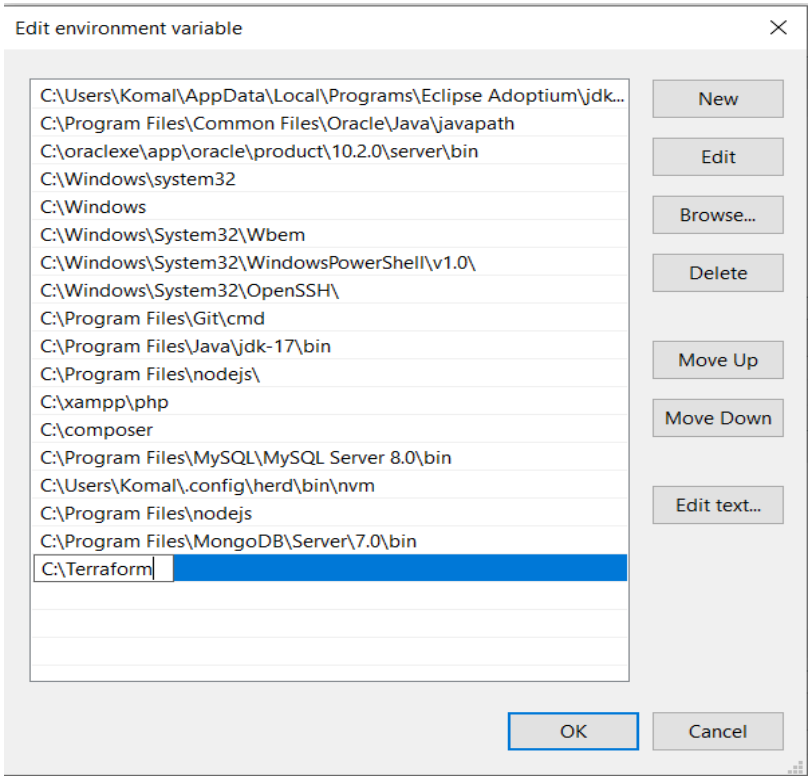


Step 2: Extract the downloaded setup file Terraform.exe in C:\Terraform directory



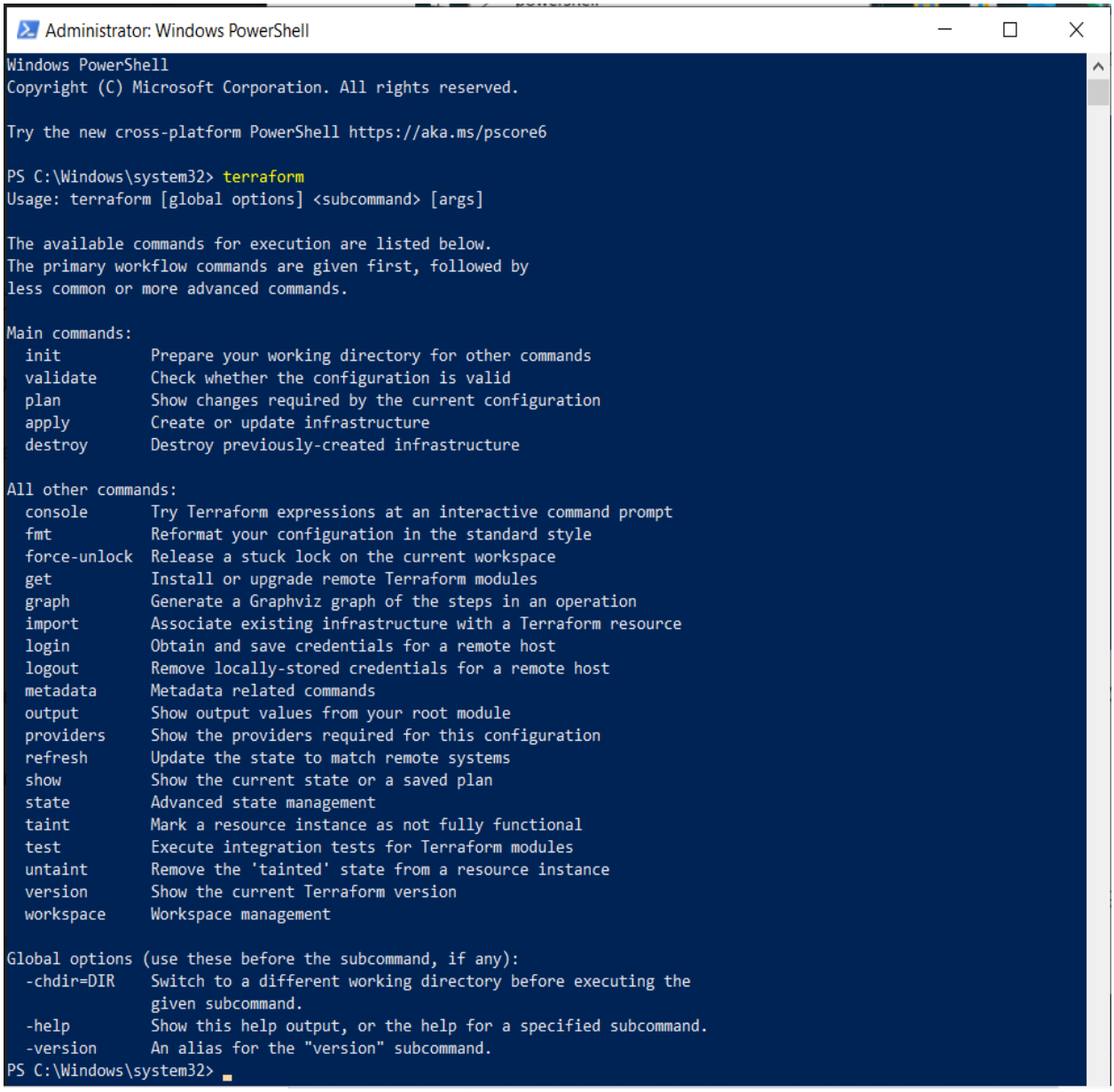
Step 3: Set the System path for Terraform in Environment Variables





Step 4: Open PowerShell with Admin Access

Step 5 : Open Terraform in PowerShell and check its functionality



```
PS C:\Windows\system32> terraform --version
Terraform v1.9.5
on windows_amd64
```

```
C:\Terraform>terraform --version
Terraform v1.9.5
on windows_amd64
```

EXPERIMENT NO. 6

AIM : A. Creating docker image using terraform

B. Creating S3 Bucket using terraform

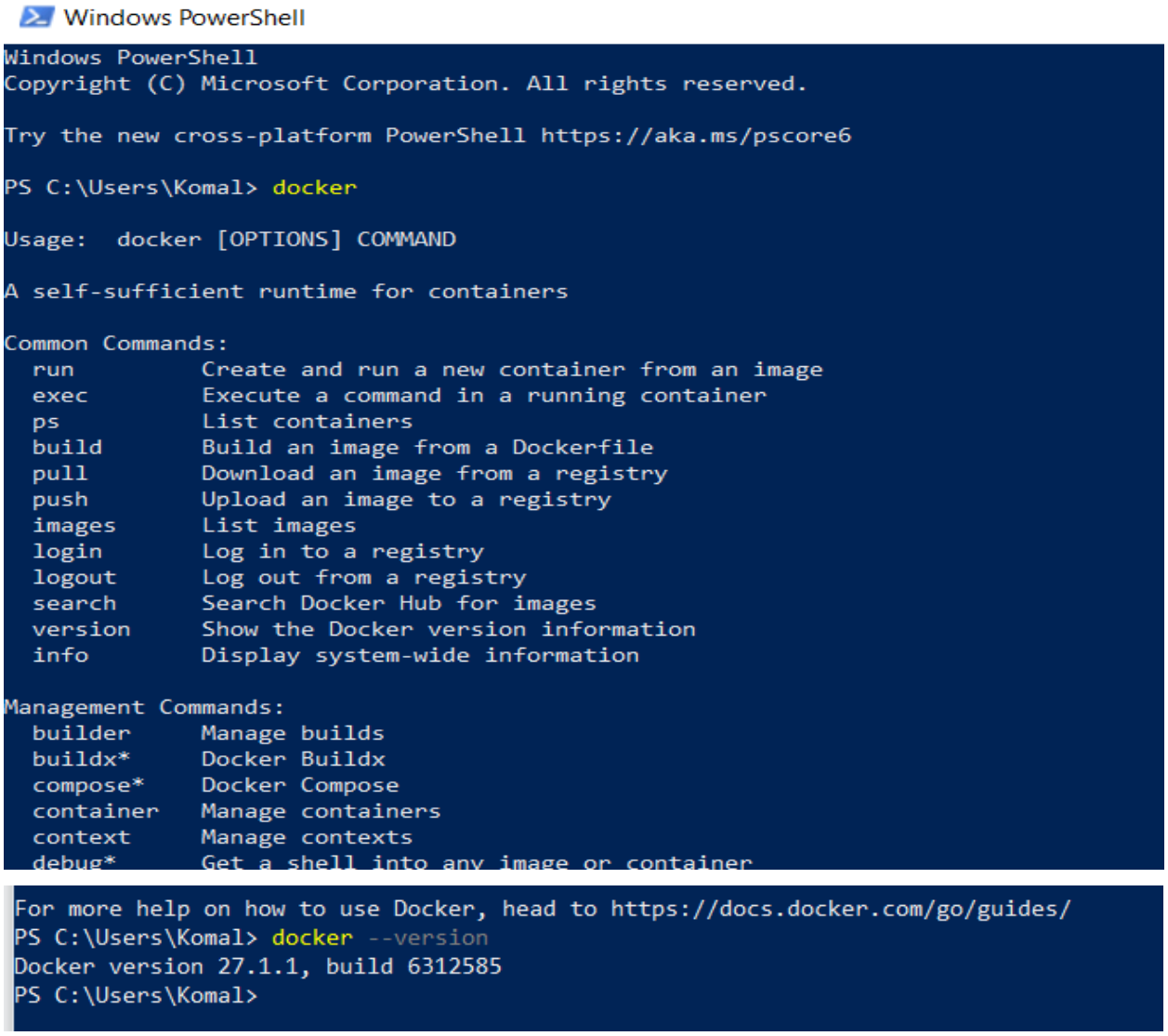
Steps :

A. Creating docker image using terraform

Prerequisite:

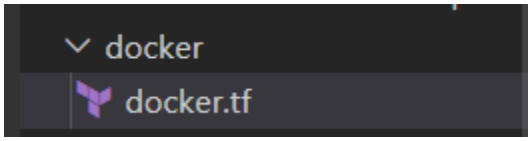
1) Download and Install Docker Desktop from https://www.docker.com/

Step1 : Check the docker functionality

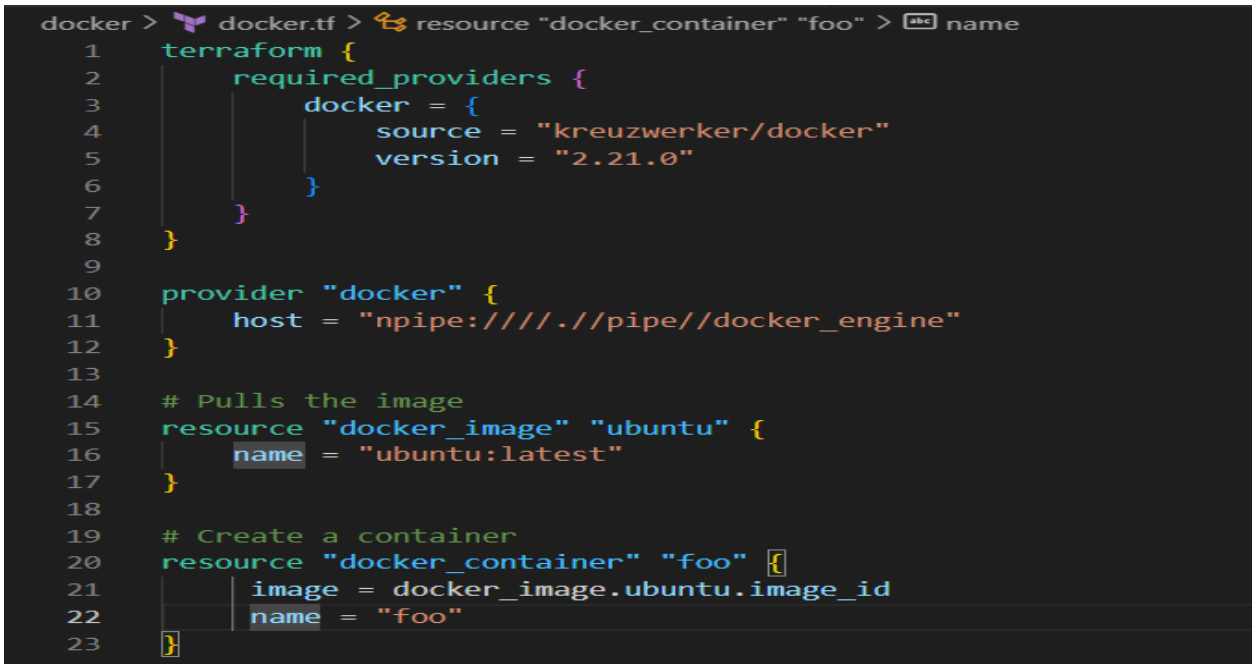


Now, create a folder in which we save our different types of scripts which will be further used in this experiment.

Step2 : Firstly create a new folder named ‘Docker’ in the ‘TerraformScripts’ folder. Then create a new docker.tf file and write the following contents into it to create a Ubuntu Linux container.




```
terraform {
  required_providers {
    docker = {
      source = "kreuzwerker/docker"
      version = "2.21.0"
    }
  }
}

provider "docker" {
  host =
"npipe:////.//pipe//docker_engine"
}

# Pulls the image
resource "docker_image" "ubuntu" {
  name = "ubuntu:latest"
}

# Create a container
resource "docker_container" "foo" {
   image = docker_image.ubuntu.image_id
   name = "foo"
}
```



Step3 : Execute Terraform Init command to initialize the resources

```
C:\Users\Komal\OneDrive\Desktop\terraform-workshop\docker>terraform init
Initializing the backend...
Initializing provider plugins...
- Finding kreuzwerker/docker versions matching "2.21.0"...
- Installing kreuzwerker/docker v2.21.0...
- Installed kreuzwerker/docker v2.21.0 (self-signed, key ID BD080C4571C6104C)
Partner and community providers are signed by their developers.
If you'd like to know more about provider signing, you can read about it here:
https://www.terraform.io/docs/cli/plugins/signing.html
Terraform has created a lock file .terraform.lock.hcl to record the provider
selections it made above. Include this file in your version control repository
so that Terraform can guarantee to make the same selections by default when
you run "terraform init" in the future.

Terraform has been successfully initialized!

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

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

C:\Users\Komal\OneDrive\Desktop\terraform-workshop\docker>
```

Step4 : Execute Terraform plan to see the available resources

```
C:\Users\Komal\OneDrive\Desktop\terraform-workshop\docker>terraform plan

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

Terraform will perform the following actions:

  # docker_container.foo will be created
  + resource "docker_container" "foo" {
      + attach            = false
      + bridge            = (known after apply)
      + command           = (known after apply)
      + 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)
      + image             = (known after apply)
      + init              = (known after apply)
      + ip_address        = (known after apply)
      + ip_prefix_length  = (known after apply)
      + ipc_mode          = (known after apply)
      + log_driver        = (known after apply)
      + logs              = false
      + must_run          = true
      + name              = "foo"
      + network_data      = (known after apply)
      + read_only         = false
      + remove_volumes    = true
      + restart           = "no"
      + rm                = false
      + runtime           = (known after apply)
```

```
# docker_image.ubuntu will be created

# docker_image.ubuntu will be created
+ resource "docker_image" "ubuntu" {
    + id          = (known after apply)
    + image_id    = (known after apply)
    + latest      = (known after apply)
    + name        = "ubuntu:latest"
    + output      = (known after apply)
    + repo_digest = (known after apply)
  }

lan: 2 to add, 0 to change, 0 to destroy.

ote: You didn't use the -out option to save this plan, so Terraform can't guarantee

:\Users\Komal\OneDrive\Desktop\terraform-workshop\docker>
```

Step5 : 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\Komal\OneDrive\Desktop\terraform-workshop\docker>terraform apply
docker_image.ubuntu: Refreshing state... [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]

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          = (known after apply)
      + 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)
```

```
Do you want to perform these actions?
  Terraform will perform the actions described above.
  Only 'yes' will be accepted to approve.

  Enter a value: yes

docker_container.foo: Creating...
docker_container.foo: Creation complete after 10s [id=5fb1f8f65af6b6320bc40523149a31ff42441bdb9b103705178e271d620501bb]

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.

C:\Users\Komal\OneDrive\Desktop\terraform-workshop\docker>
```

Docker images, Before Executing Apply step:

```
C:\Users\Komal\OneDrive\Desktop\terraform-workshop\docker>docker images
REPOSITORY   TAG       IMAGE ID   CREATED   SIZE
```

Docker images, After Executing Apply step:

```
C:\Users\Komal\OneDrive\Desktop\terraform-workshop\docker>docker images
REPOSITORY   TAG       IMAGE ID       CREATED       SIZE
ubuntu       latest    edbfe74c41f8   6 weeks ago   78.1MB
```

Step6 : Execute Terraform destroy to delete the configuration, which will automatically delete the Ubuntu Container.

```
C:\Users\Komal\OneDrive\Desktop\terraform-workshop\docker>terraform destroy
docker_image.ubuntu: Refreshing state... [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]
docker_container.foo: Refreshing state... [id=5fb1f8f65af6b6320bc40523149a31ff42441bdb9b103705178e271d620501bb]

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

Terraform will perform the following actions:

  # docker_image.ubuntu will be destroyed
  - resource "docker_image" "ubuntu" {
      - id          = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest" -> null
      - image_id    = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598a" -> null
      - latest      = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598a" -> null
      - name        = "ubuntu:latest" -> null
      - repo_digest = "ubuntu@sha256:8a37d68f4f73ebf3d4efafbcf66379bf3728902a8038616808f04e34a9ab63ee" -> null
    }

Plan: 0 to add, 0 to change, 1 to destroy.

Do you really want to destroy all resources?
  Terraform will destroy all your managed infrastructure, as shown above.
  There is no undo. Only 'yes' will be accepted to confirm.

  Enter a value: yes

docker_image.ubuntu: Destroying... [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]
docker_image.ubuntu: Destruction complete after 5s

Destroy complete! Resources: 1 destroyed.
```

Docker images After Executing Destroy step

```
C:\Users\Komal\OneDrive\Desktop\terraform-workshop\docker>docker images
REPOSITORY   TAG       IMAGE ID   CREATED   SIZE
```

B. Creating S3 Bucket using terraform

Prerequisite:

1) Install Editor for Writing the Scripts like Atom

2) Must have an AWS Access Key ID and Secret Access Key

Step1 : Go to aws academy and start lab and then click on aws details to get the details
Now make the Variables capital (select text shift+ctrl+p transform uppercase)

```
set AWS_ACCESS_KEY_ID=ASIA5SVPTILUR5DRZTJR
set AWS_SECRET_ACCESS_KEY=hV6QshjZR0S7YABsSF4v4yfrrCPM4flO+B0VehYn
set AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEPX//////////wEaCXVzLXdlc3QtMiJGMEQCIHbThRX3auCOhxlwg3AUAaITQT0q0U+INd/
mZEgIuTp9AiB7BC5L3vEVKfjFVJytC7U4BZ33GxGQgIwKTJDqbWGfsSq3AgguEAEaDDkzMzQ0OTkwODk2OSIMkZ6YIvYdnEgYRZWgKpQCKKGrVXGPzSlxQdeO7lSOUnqzDnuPW5yf50snf
ycprzLF0rN5phb1lID8u1LIURlL1Fj4tOr3AbzhnUrhNs8yttxPvSariIMJv4480L88VR9t0llRhf36IZDpDUiN0N3XfWz+JbvPAHYHS1jUdo9QcHRUqG0/
Q7ZVQN061nMDOOGUJR1y8UxSGtJ6j2CukNzLbrQ1KsQ8pdYgJKQNC84CiiMqyGx/Fyk4PIUKFdGPmf87OaC9zvi/
SclELuTWvXQ19BWIUDxNyELtoC7ogUNCk4za1iSv0X8YgecfuZSD0j7rD471yihhhH0sUl6SFiuYG/6XarRTYqlzJO2l/JQsdVQwqXHqmN6xMzwLp5ttdtlgSqI0MMyAprcGOp4B
+OhgGYKbQAOJtstvwncOWkyVOeJjDNNnih6HDhsynD3bfkN6X74nb/arxT4ADB35qNe5CtCGJSgpAihNQGAdOS4yD
+rudofJXYskTzwSJsCZb5PLU0DJi5wTcG6mgz1bupvXGotX6N91OoWWOBG6/cs15lZIrPD/4oK/NR6UYuN25HMykRZl1Cf22bOO51mRX2/O8WjbwkD4TfVsj/s=P
```

Step2 : Then write set at the start of three of them then paste them into cmd of the same folder and enter

```
C:\Users\Komal\OneDrive\Desktop\terraform-workshop>^Zset AWS_ACCESS_KEY_ID=ASIA5SVPTILUR5DRZTJR
C:\Users\Komal\OneDrive\Desktop\terraform-workshop>set AWS_SECRET_ACCESS_KEY=hV6QshjZR0S7YABsSF4v4yfrrCPM4flO+B0VehYn

C:\Users\Komal\OneDrive\Desktop\terraform-workshop>set AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEPX//////////wEaCXVzLXdlc3QtMiJGMEQCIHbThRX3auCOhxlwg3AUAaITQT
7BC5L3vEVKfjFVJytC7U4BZ33GxGQgIwKTJDqbWGfsSq3AgguEAEaDDkzMzQ0OTkwODk2OSIMkZ6YIvYdnEgYRZWgKpQCKKGrVXGPzSlxQdeO7lSOUnqzDnuPW5yf50snfycprzLF0rN5phb1lID8u1
hNs8yttxPvSariIMJv4480L88VR9t0llRhf36IZDpDUiN0N3XfWz+JbvPAHYHS1jUdo9QcHRUqG0/Q7ZVQN061nMDOOGUJR1y8UxSGtJ6j2CukNzLbrQ1KsQ8pdYgJKQNC84CiiMqyGx/Fyk4PIUKFd
WvXQ19BWIUDxNyELtoC7ogUNCk4za1iSv0X8YgecfuZSD0j7rD471yihhhH0sUl6SFiuYG/6XarRTYqlzJO2l/JQsdVQwqXHqmN6xMzwLp5ttdtlgSqI0MMyAprcGOp4B+OhgGYKbQAOJtstvwncOWk
bfkN6X74nb/arxT4ADB35qNe5CtCGJSgpAihNQGAdOS4yD+rudofJXYskTzwSJsCZb5PLU0DJi5wTcG6mgz1bupvXGotX6N91OoWWOBG6/cs15lZIrPD/4oK/NR6UYuN25HMykRZl1Cf22bOO51mRX2

C:\Users\Komal\OneDrive\Desktop\terraform-workshop>
```

Step3 : Then create provider.tf file and paste that three values like these also add region

```
aws-s3-exp-6 > provider.tf > ...
1  provider "aws" {
2      access_key = "ASIA5SVPTILUR5DRZTJR"
3      secret_key = "hV6QshjZR0S7YABsSF4v4yfrrCPM4flO+B0VehYn"
4      token = "IQoJb3JpZ2luX2VjEPX//////////wEaCXVzLXdlc3QtMiJGMEQCIHbThRX3auCOhxlwg3AUAaITQT0q0U+INd/
       mZEgIuTp9AiB7BC5L3vEVKfjFVJytC7U4BZ33GxGQgIwKTJDqbWGfsSq3AgguEAEaDDkzMzQ0OTkwODk2OSIMkZ6YIvYdnEgYRZWgKpQCKKGrVXGPzSlxQdeO7lSOUnqzDnuPW5yf5
       0snfycprzLF0rN5phb1lID8u1LIURlL1Fj4tOr3AbzhnUrhNs8yttxPvSariIMJv4480L88VR9t0llRhf36IZDpDUiN0N3XfWz+JbvPAHYHS1jUdo9QcHRUqG0/
       Q7ZVQN061nMDOOGUJR1y8UxSGtJ6j2CukNzLbrQ1KsQ8pdYgJKQNC84CiiMqyGx/Fyk4PIUKFdGPmf87OaC9zvi/
       SclELuTWvXQ19BWIUDxNyELtoC7ogUNCk4za1iSv0X8YgecfuZSD0j7rD471yihhhH0sUl6SFiuYG/6XarRTYqlzJO2l/JQsdVQwqXHqmN6xMzwLp5ttdtlgSqI0MMyAprcGOp4B
       +OhgGYKbQAOJtstvwncOWkyVOeJjDNNnih6HDhsynD3bfkN6X74nb/arxT4ADB35qNe5CtCGJSgpAihNQGAdOS4yD
       +rudofJXYskTzwSJsCZb5PLU0DJi5wTcG6mgz1bupvXGotX6N91OoWWOBG6/cs15lZIrPD/4oK/NR6UYuN25HMykRZl1Cf22bOO51mRX2/O8WjbwkD4TfVsj/s="
5      region = "us-east-1"
6  }
7
8
```

Step4 : Create main.tf file for writing script and paste the below content

```
terraform {
 required_providers {
  aws = {
   source = "hashicorp/aws"
   version = "5.64.0"
  }
  random = {
   source = "hashicorp/random"
   version = "3.6.2"
  }
 }
}

resource "random_id" "rand_id" {
  byte_length = 8
}

#demo-bucket is the name for resource not a bucket name and s3 bucket name should be unique everytime
resource "aws_s3_bucket" "demo-bucket" {
   bucket = "demo-bucket-${random_id.rand_id.hex}"
}

resource "aws_s3_object" "bucket-data" {
 bucket = aws_s3_bucket.demo-bucket.bucket
 source = "./myfile.txt"
 key = "newfile.txt"
}
```

Also create myfile.txt file as we have mentioned it in code and write something in that because we are storing that file in s3 bucket

Step5 : Now go to that folder in command prompt and Execute Terraform Init command to initialize the resources

```
C:\Users\Komal\OneDrive\Desktop\terraform-workshop\aws-s3-exp-6>terraform init
Initializing the backend...
Initializing provider plugins...
- Finding hashicorp/aws versions matching "5.64.0"...
- Finding hashicorp/random versions matching "3.6.2"...
- Installing hashicorp/aws v5.64.0...
- Installed hashicorp/aws v5.64.0 (signed by HashiCorp)
- Installing hashicorp/random v3.6.2...
- Installed hashicorp/random v3.6.2 (signed by HashiCorp)
Terraform has created a lock file .terraform.lock.hcl to record the provider
selections it made above. Include this file in your version control repository
so that Terraform can guarantee to make the same selections by default when
you run "terraform init" in the future.

Terraform has been successfully initialized!

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

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

C:\Users\Komal\OneDrive\Desktop\terraform-workshop\aws-s3-exp-6>
```

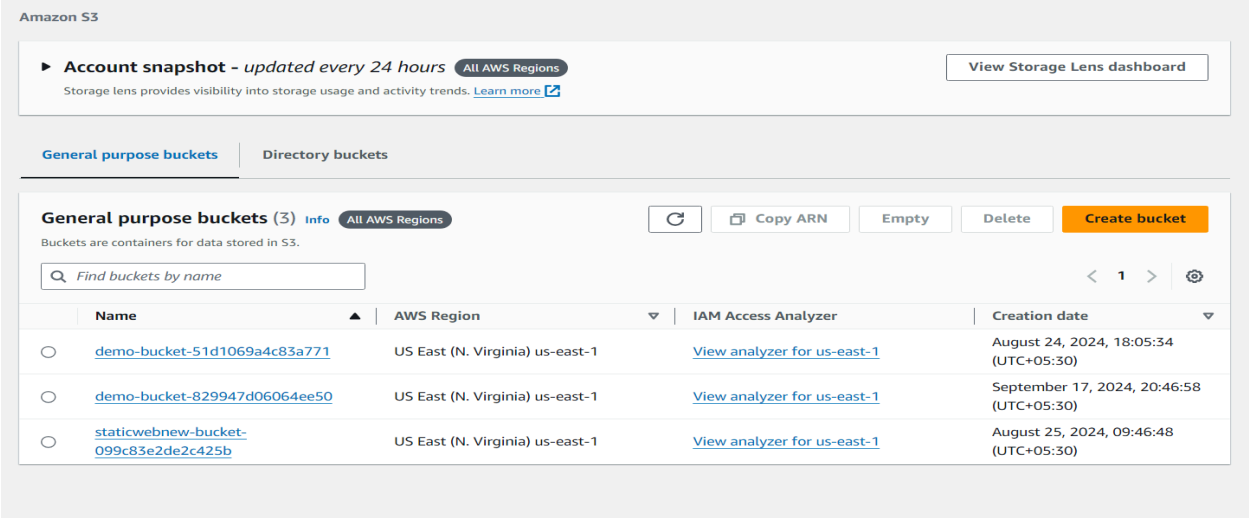
Step6 : Execute Terraform plan to see the available resources

```
C:\Users\Komal\OneDrive\Desktop\terraform-workshop\aws-s3-exp-6>terraform plan

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

Terraform will perform the following actions:

  # aws_s3_bucket.demo-bucket will be created
  + resource "aws_s3_bucket" "demo-bucket" {
      + acceleration_status         = (known after apply)
      + acl                         = (known after apply)
      + arn                         = (known after apply)
      + bucket                      = (known after apply)
      + bucket_domain_name          = (known after apply)
      + bucket_prefix               = (known after apply)
      + bucket_regional_domain_name = (known after apply)
      + force_destroy               = false
      + hosted_zone_id              = (known after apply)
      + id                          = (known after apply)
      + object_lock_enabled         = (known after apply)
      + policy                      = (known after apply)
      + region                      = (known after apply)
      + request_payer               = (known after apply)
      + tags_all                    = (known after apply)
      + website_domain              = (known after apply)
      + website_endpoint            = (known after apply)
    }

Plan: 3 to add, 0 to change, 0 to destroy.

Note: You didn't use the -out option to save this plan, so Terraform can't guarantee to take exactly th

C:\Users\Komal\OneDrive\Desktop\terraform-workshop\aws-s3-exp-6>terraform apply
```

Step7 : Execute Terraform apply to apply the configuration, which will automatically create an S3 bucket based on our configuration.

```
C:\Users\Komal\OneDrive\Desktop\terraform-workshop\aws-s3-exp-6>terraform apply

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:

  # aws_s3_bucket.demo-bucket will be created
  + resource "aws_s3_bucket" "demo-bucket" {
      + acceleration_status         = (known after apply)
      + acl                         = (known after apply)
      + arn                         = (known after apply)
      + bucket                      = (known after apply)
      + bucket_domain_name          = (known after apply)
      + bucket_prefix               = (known after apply)
      + bucket_regional_domain_name = (known after apply)
      + force_destroy               = false
      + hosted_zone_id              = (known after apply)
      + id                          = (known after apply)
      + object_lock_enabled         = (known after apply)
      + policy                      = (known after apply)
```

AWS S3 Bucket dashboard, After Executing Apply step:

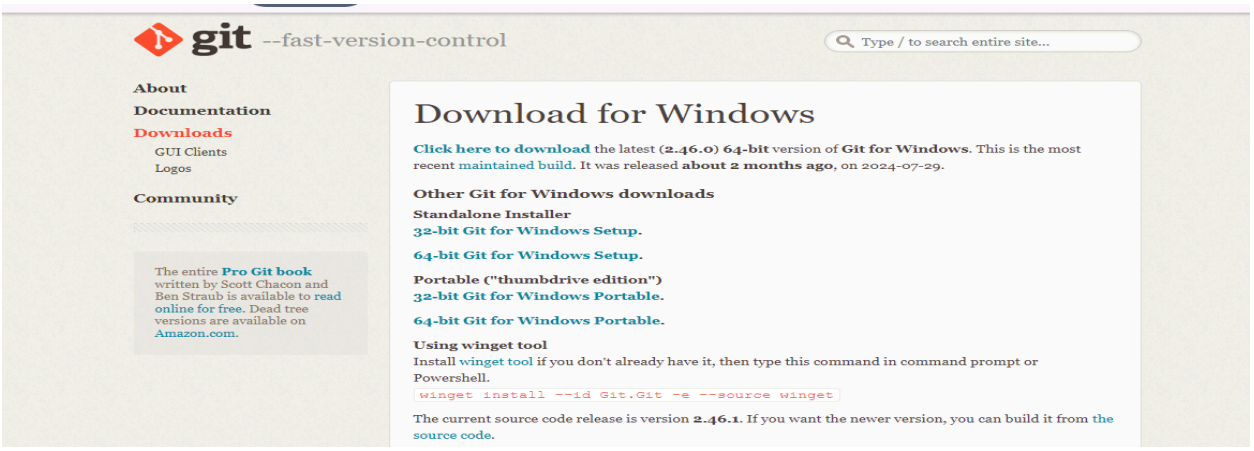


Step8 : 6: Execute Terraform destroy to delete the configuration, which will automatically delete an EC2 instance

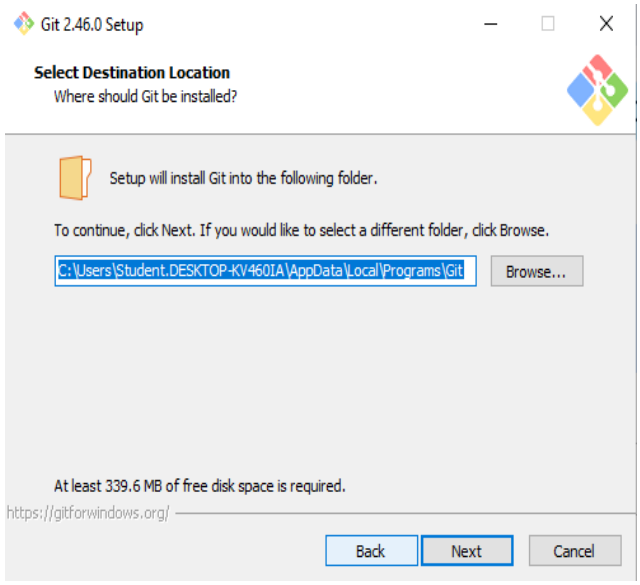
```
C:\Users\Komal\OneDrive\Desktop\terraform-workshop\aws-s3-exp-6>terraform destroy
random_id.rand_id: Refreshing state... [id=gplH0GBk7lA]
aws_s3_bucket.demo-bucket: Refreshing state... [id=demo-bucket-829947d06064ee50]
aws_s3_object.bucket-data: Refreshing state... [id=newfile.txt]

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:

  # aws_s3_bucket.demo-bucket will be destroyed
  - resource "aws_s3_bucket" "demo-bucket" {
      - arn                         = "arn:aws:s3:::demo-bucket-829947d06064ee50" -> null
      - bucket                      = "demo-bucket-829947d06064ee50" -> null
      - bucket_domain_name          = "demo-bucket-829947d06064ee50.s3.amazonaws.com" -> null
      - bucket_regional_domain_name = "demo-bucket-829947d06064ee50.s3.us-east-1.amazonaws.com" -> null
      - force_destroy               = false -> null
      - hosted_zone_id              = "Z3AQBSTGFYJSTF" -> null
      - id                          = "demo-bucket-829947d06064ee50" -> null
      - object_lock_enabled         = false -> null
```

Experiment No. 7

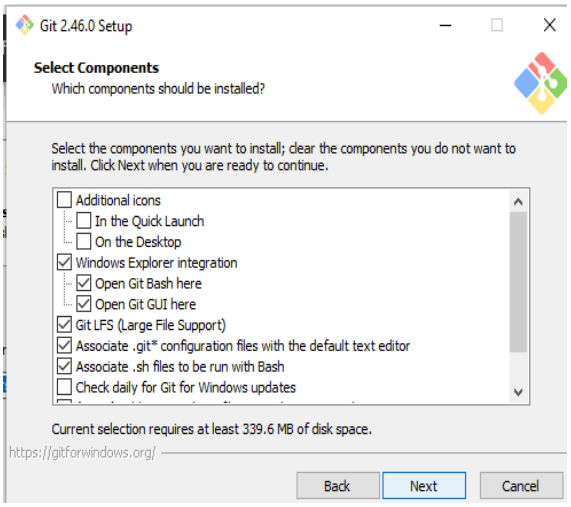
Git Installation

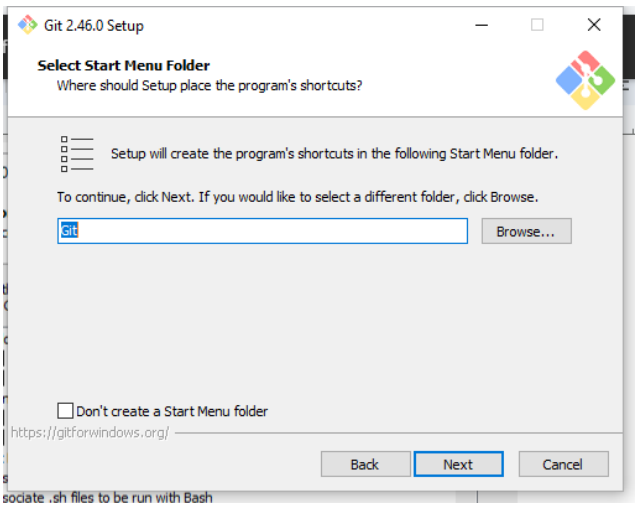


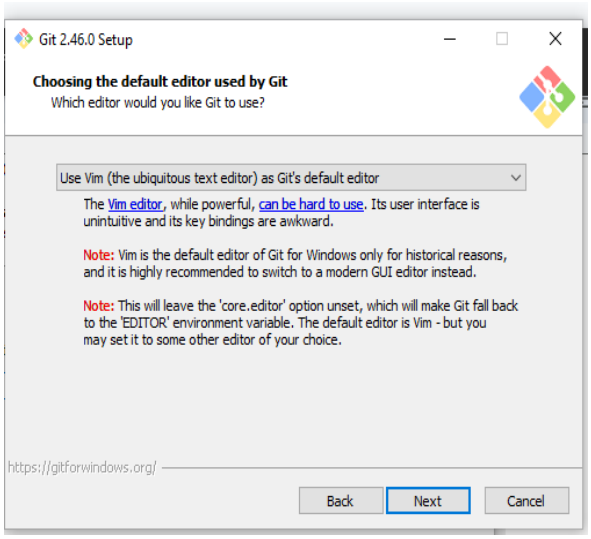
Select Installation for Windows setup and set up the destination for GIT installation.

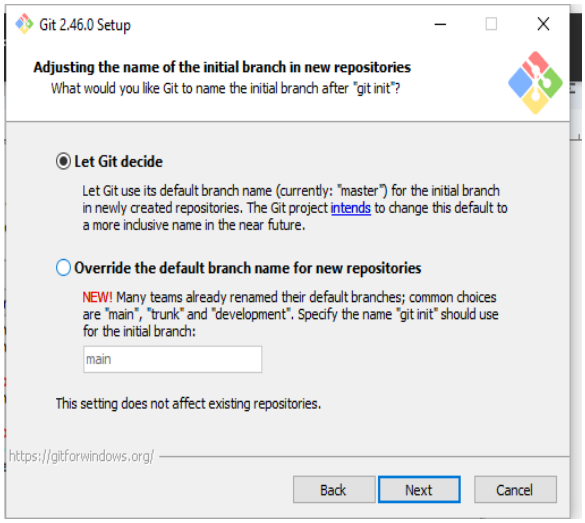


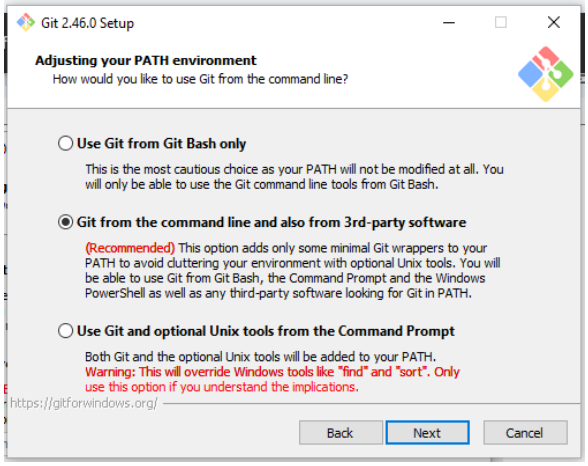
Configure or select as given below

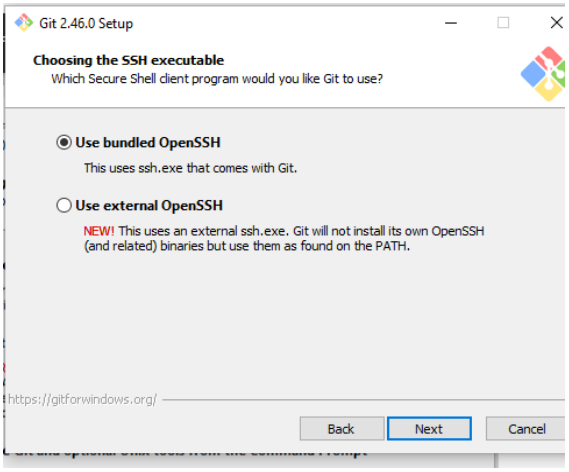


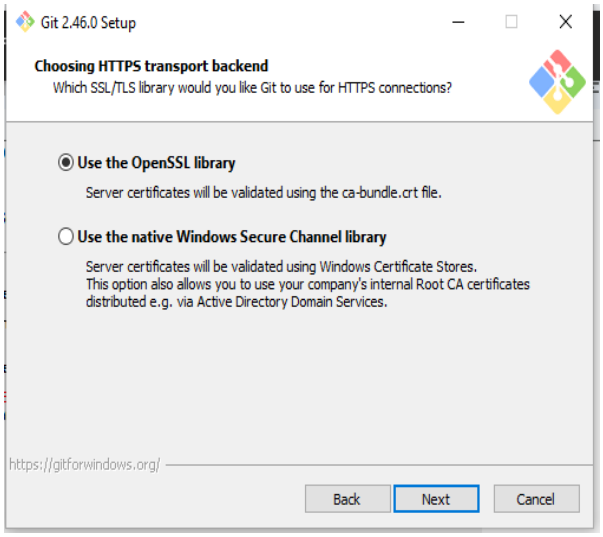


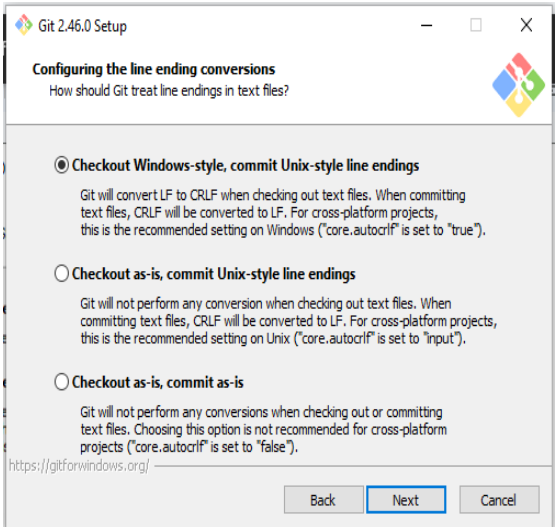

Git 2.46.0 Setup
Choosing the default editor used by Git
Which editor would you like Git to use?
Use Vim (the ubiquitous text editor) as Git's default editor
The Vim editor, while powerful, can be hard to use. Its user interface is unintuitive and its key bindings are awkward.
Note: Vim is the default editor of Git for Windows only for historical reasons, and it is highly recommended to switch to a modern GUI editor instead.
Note: This will leave the 'core.editor' option unset, which will make Git fall back to the 'EDITOR' environment variable. The default editor is Vim - but you may set it to some other editor of your choice.
https://gitforwindows.org/
Back
Next
Cancel

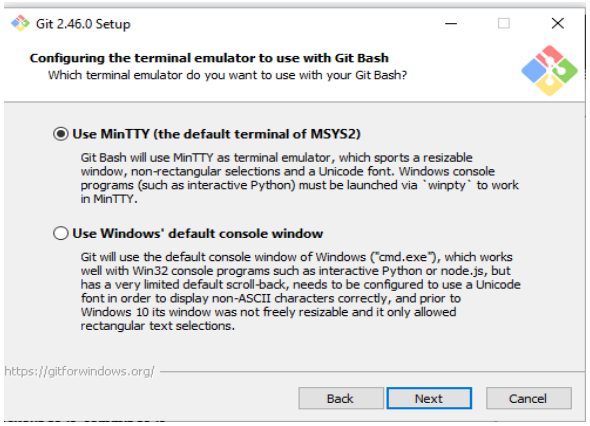

Git 2.46.0 Setup
Adjusting the name of the initial branch in new repositories
What would you like Git to name the initial branch after "git init"?
Let Git decide
Let Git use its default branch name (currently: "master") for the initial branch in newly created repositories. The Git project intends to change this default to a more inclusive name in the near future.
Override the default branch name for new repositories
NEW! Many teams already renamed their default branches; common choices are "main", "trunk" and "development". Specify the name "git init" should use for the initial branch:
main
This setting does not affect existing repositories.
https://gitforwindows.org/
Back
Next
Cancel

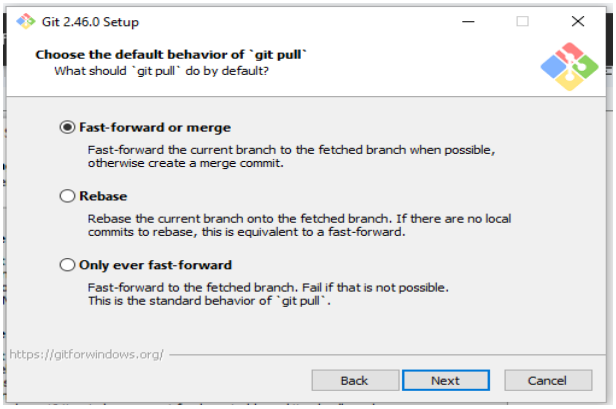

Git 2.46.0 Setup
Adjusting your PATH environment
How would you like to use Git from the command line?
Use Git from Git Bash only
This is the most cautious choice as your PATH will not be modified at all. You will only be able to use the Git command line tools from Git Bash.
Git from the command line and also from 3rd-party software
(Recommended) This option adds only some minimal Git wrappers to your PATH to avoid cluttering your environment with optional Unix tools. You will be able to use Git from Git Bash, the Command Prompt and the Windows PowerShell as well as any third-party software looking for Git in PATH.
Use Git and optional Unix tools from the Command Prompt
Both Git and the optional Unix tools will be added to your PATH.
Warning: This will override Windows tools like "find" and "sort". Only use this option if you understand the implications.
https://gitforwindows.org/
Back
Next
Cancel

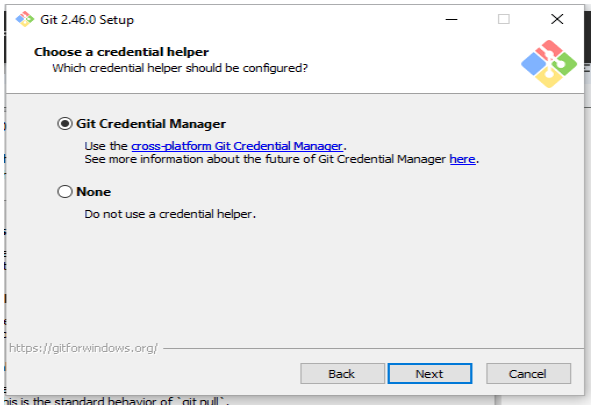

Git 2.46.0 Setup
Choosing the SSH executable
Which Secure Shell client program would you like Git to use?
Use bundled OpenSSH
This uses ssh.exe that comes with Git.
Use external OpenSSH
NEW! This uses an external ssh.exe. Git will not install its own OpenSSH (and related) binaries but use them as found on the PATH.
https://gitforwindows.org/
Back
Next
Cancel

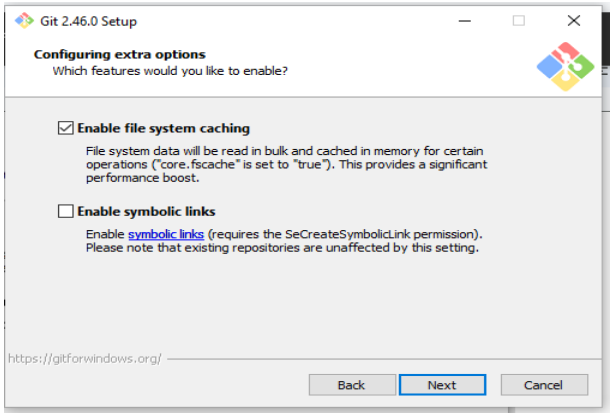

Git 2.46.0 Setup
Choosing HTTPS transport backend
Which SSL/TLS library would you like Git to use for HTTPS connections?
Use the OpenSSL library
Server certificates will be validated using the ca-bundle.crt file.
Use the native Windows Secure Channel library
Server certificates will be validated using Windows Certificate Stores. This option also allows you to use your company's internal Root CA certificates distributed e.g. via Active Directory Domain Services.
https://gitforwindows.org/
Back
Next
Cancel

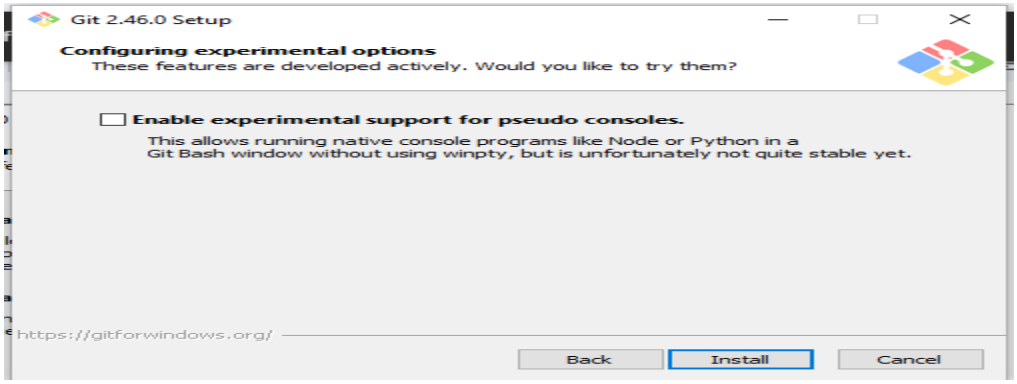

Git 2.46.0 Setup
Configuring the line ending conversions
How should Git treat line endings in text files?
Checkout Windows-style, commit Unix-style line endings
Git will convert LF to CRLF when checking out text files. When committing text files, CRLF will be converted to LF. For cross-platform projects, this is the recommended setting on Windows ("core.autocrlf" is set to "true").
Checkout as-is, commit Unix-style line endings
Git will not perform any conversion when checking out text files. When committing text files, CRLF will be converted to LF. For cross-platform projects, this is the recommended setting on Unix ("core.autocrlf" is set to "input").
Checkout as-is, commit as-is
Git will not perform any conversions when checking out or committing text files. Choosing this option is not recommended for cross-platform projects ("core.autocrlf" is set to "false").
https://gitforwindows.org/
Back
Next
Cancel



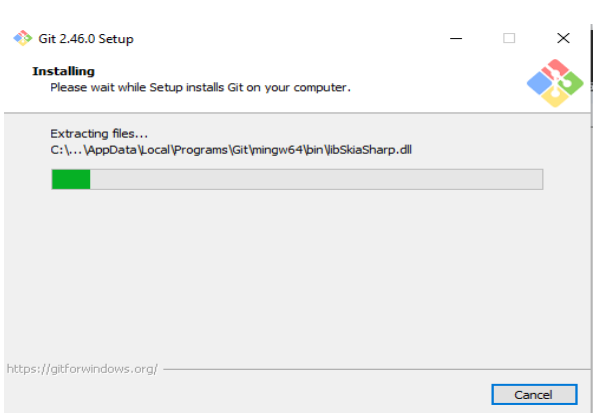


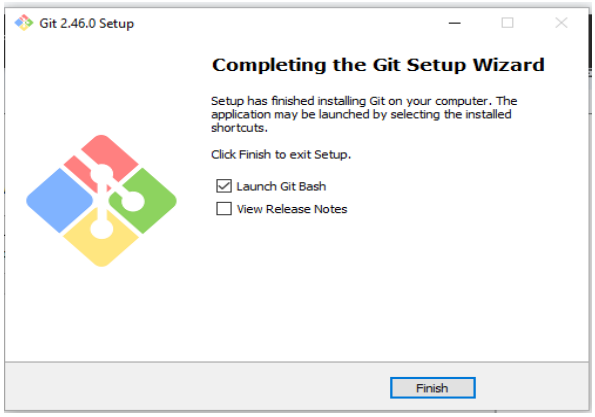




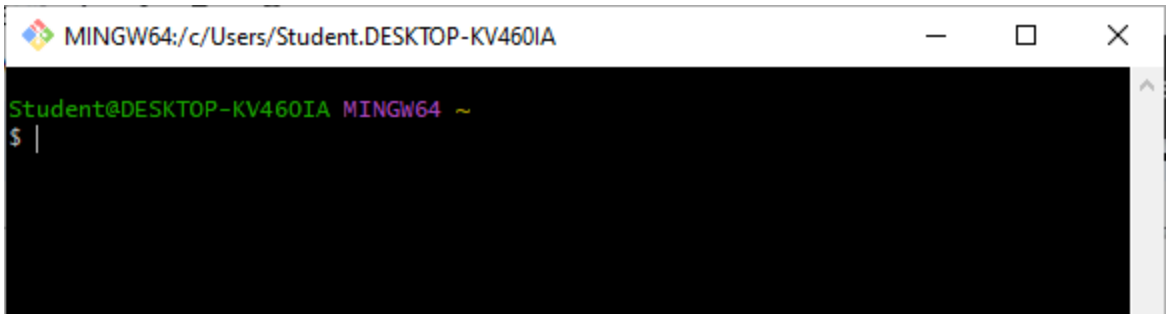


After all such configurations, Git installation is started



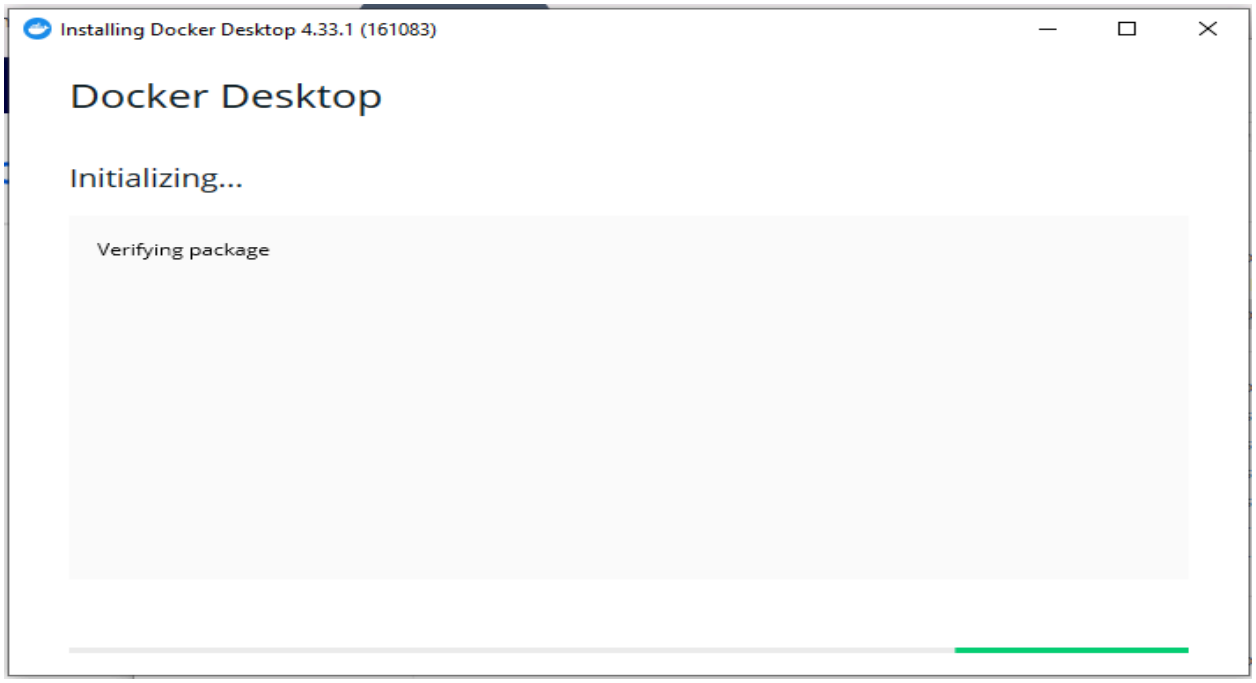


After Installation, Git Bash is launched

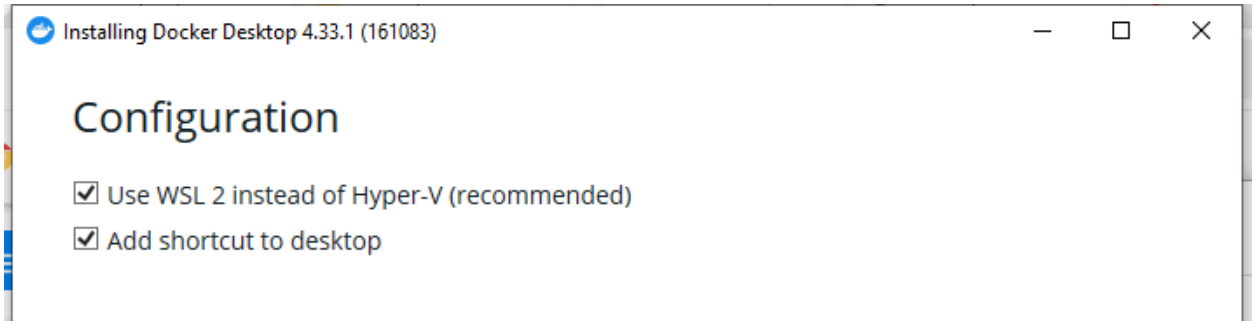


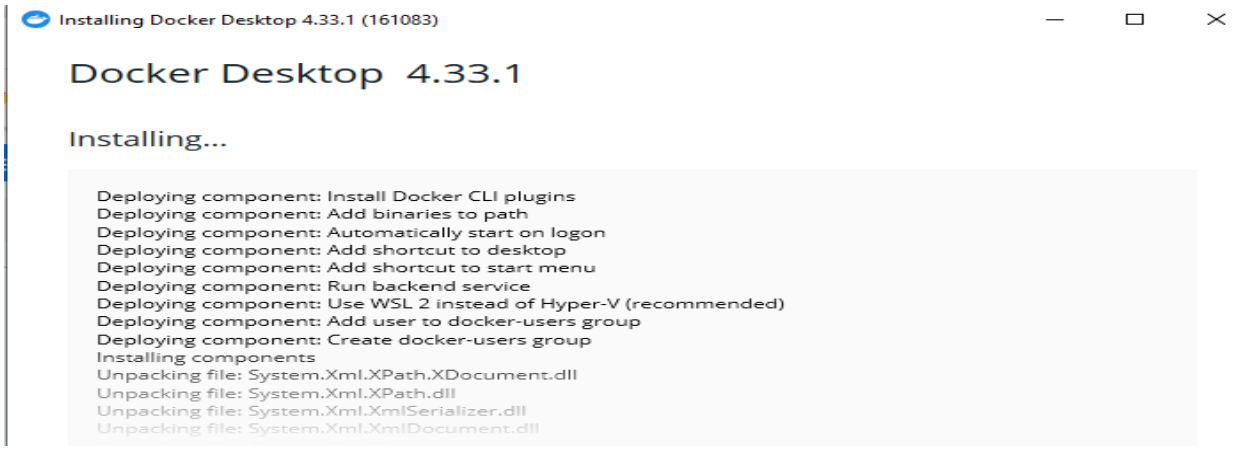
Docker Installation

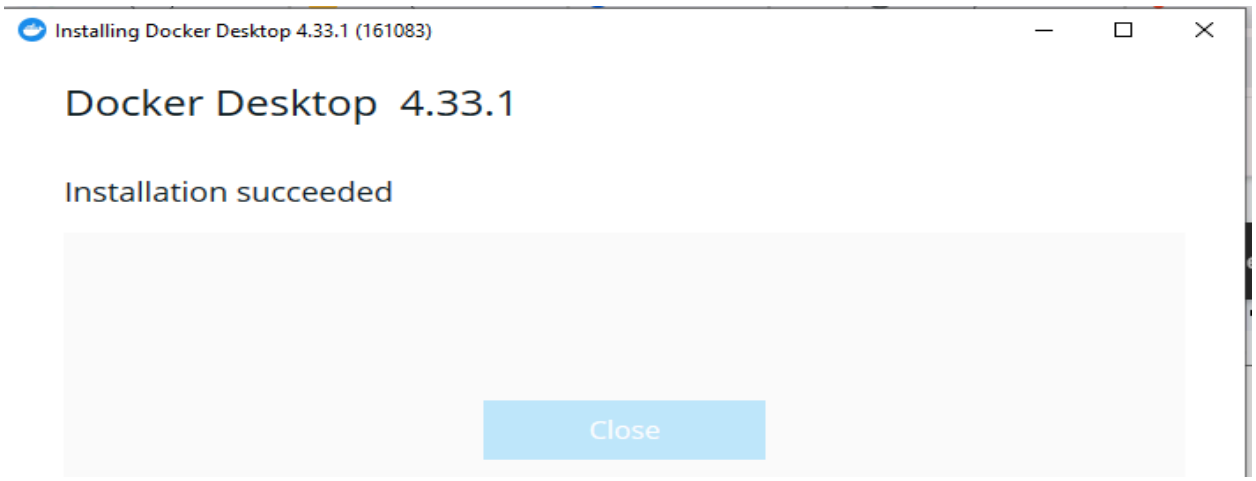
Go to docker website



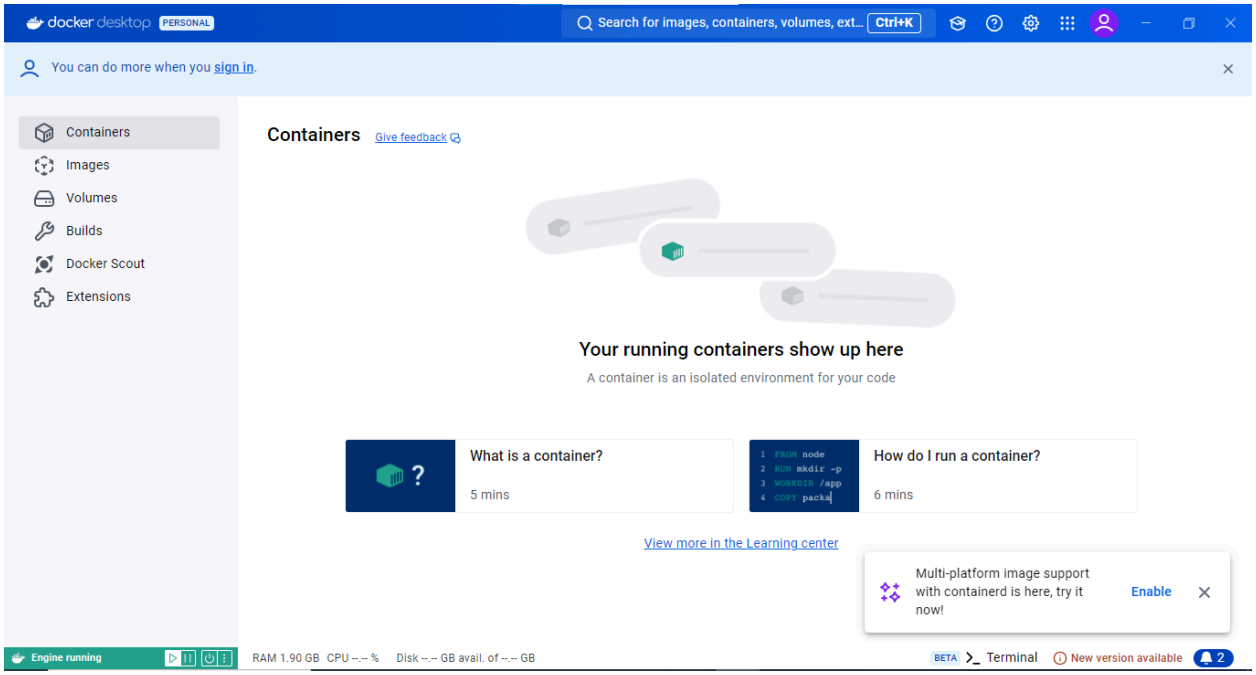
Enable WSL2 in order to work the docker correctly



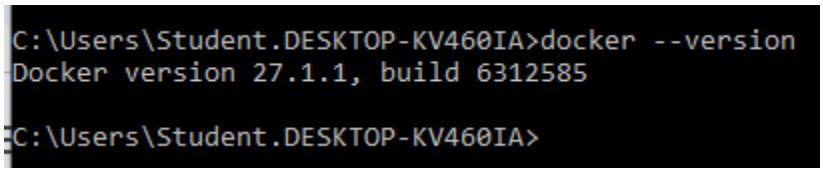




After Docker is installed, homepage will look like these



We can ensure whether docker is downloaded successfully or not by command "docker –version"

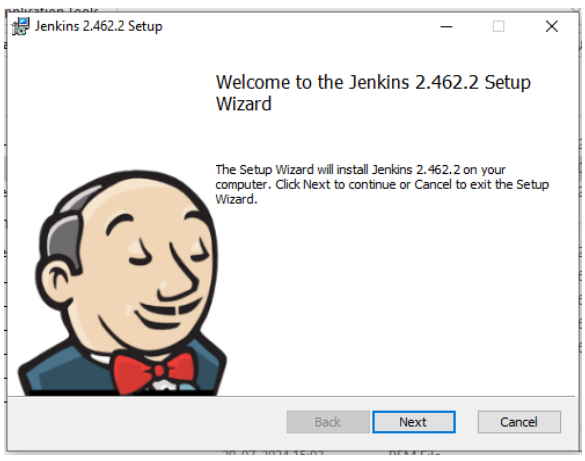


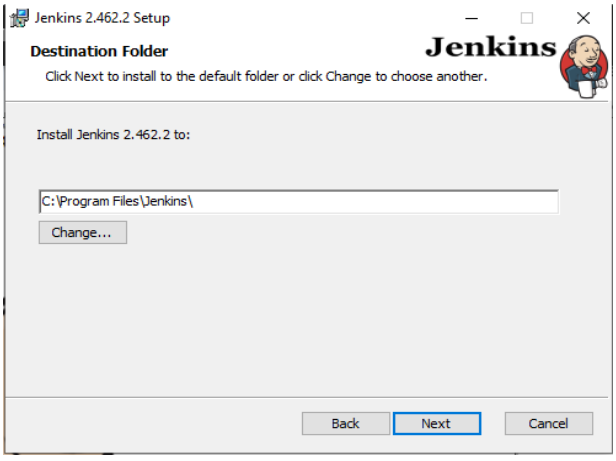
Jenkins Installation

Install JDK first then go for Jenkins installation (mostly prefered 17 - 20)

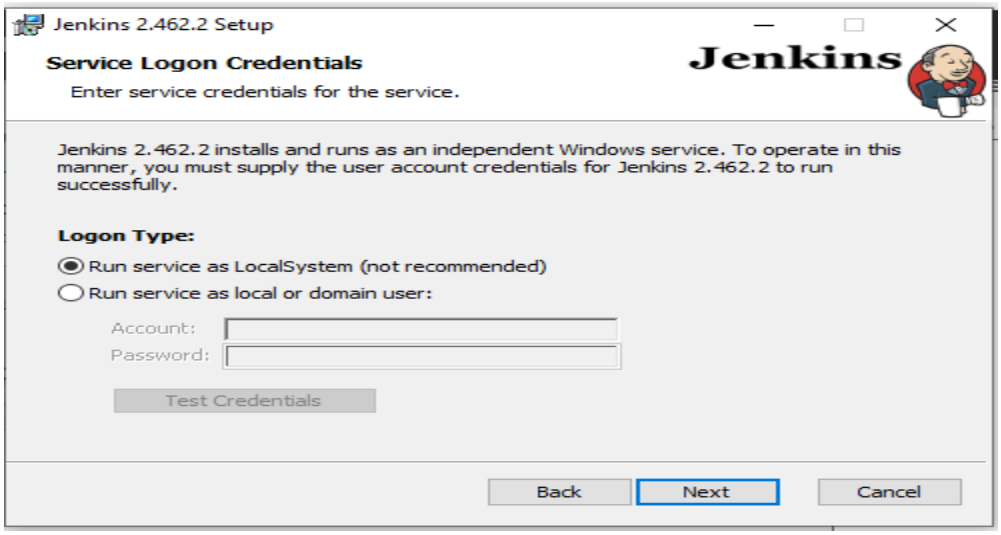
Launch the Jenkins exe file downloaded

Set the path for Jenkins all workspaces and jobs

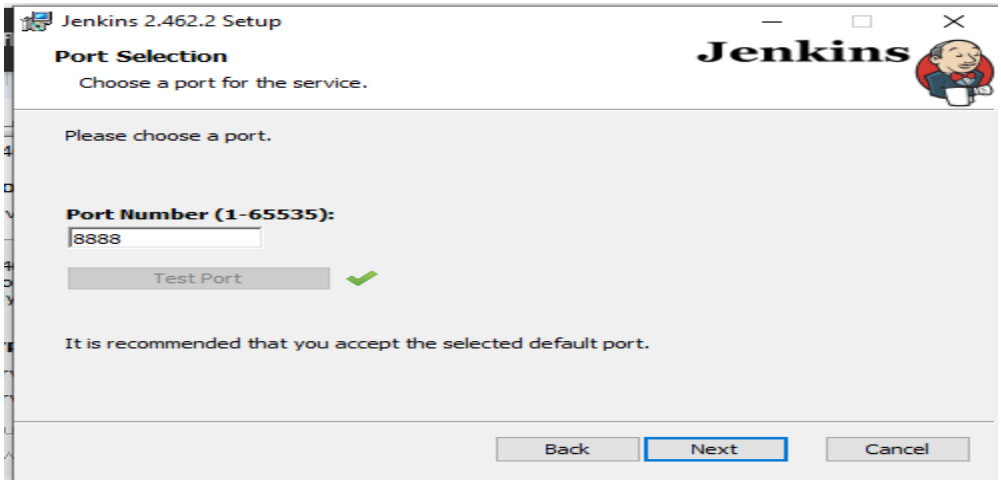




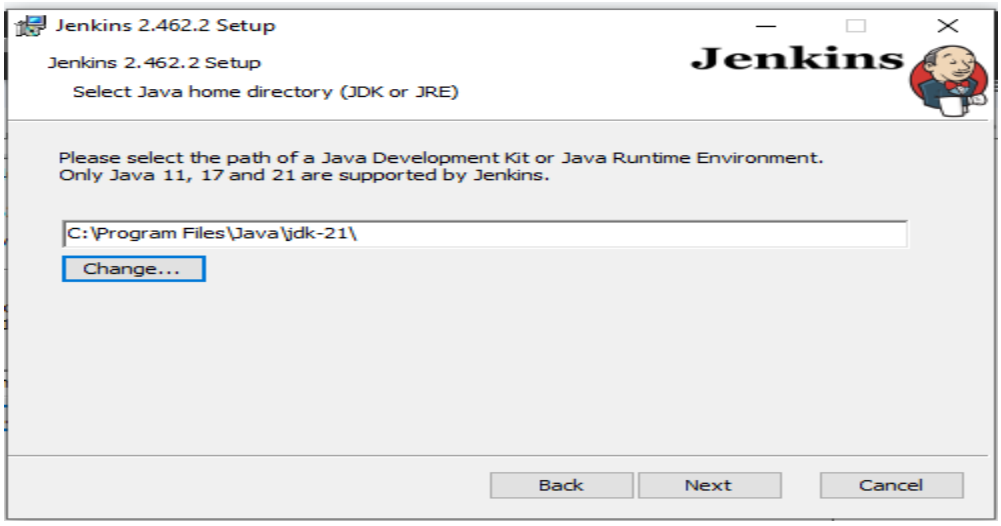
Select “Run service as a LocalSystem” to start Jenkins locally

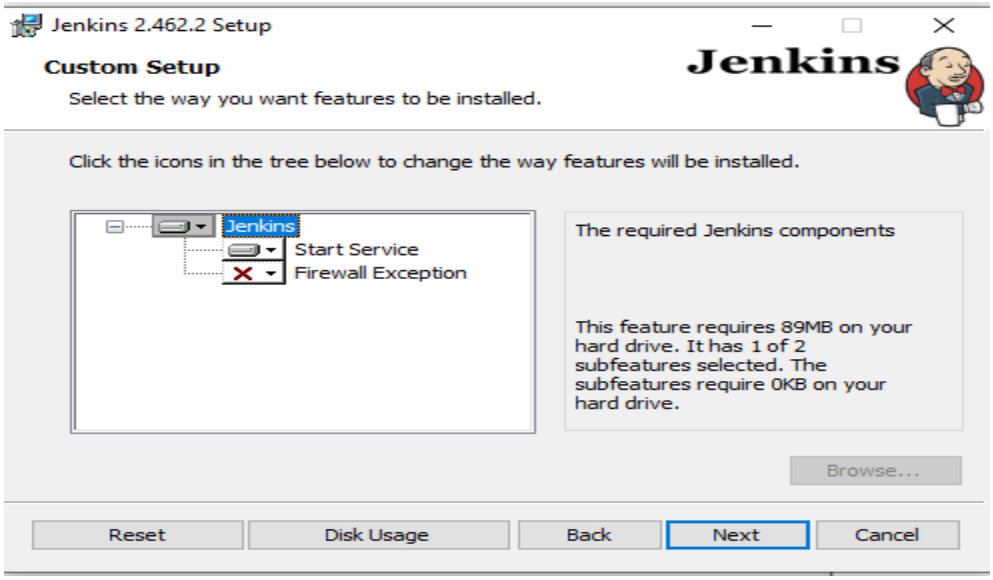


Choose a port on which you want Jenkins to work.(By default it is 8080)

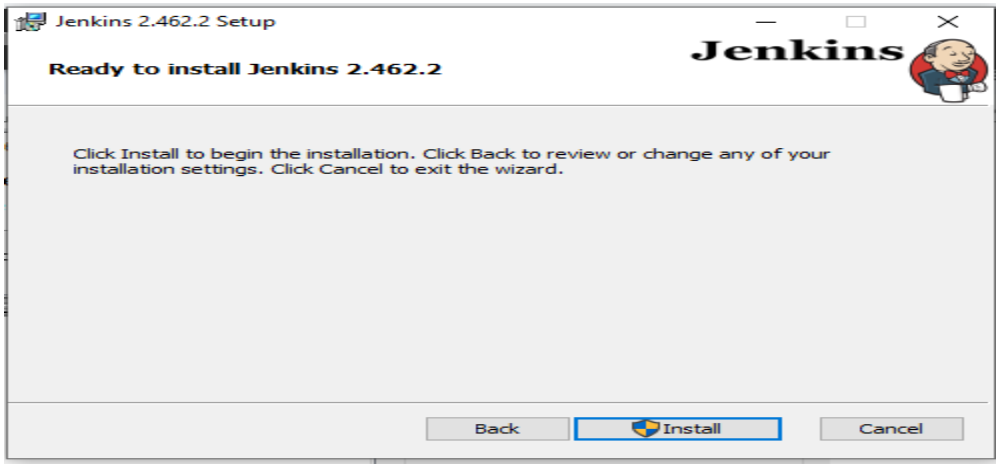


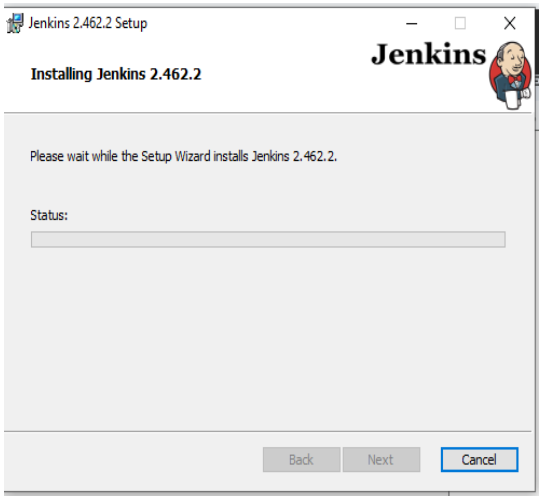
Set up the latest Java directory (mostly preferred 17/ 21)

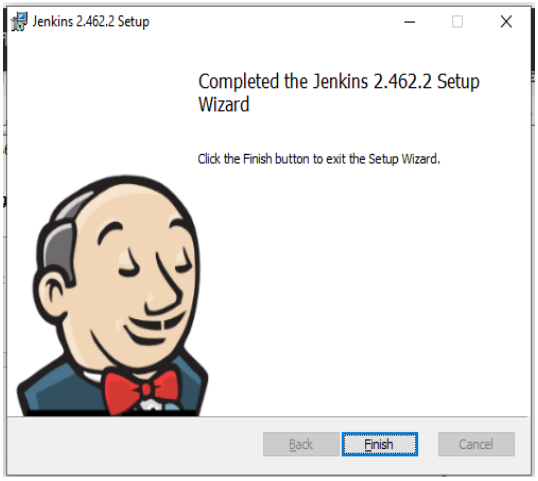




Click Install to begin the installation process

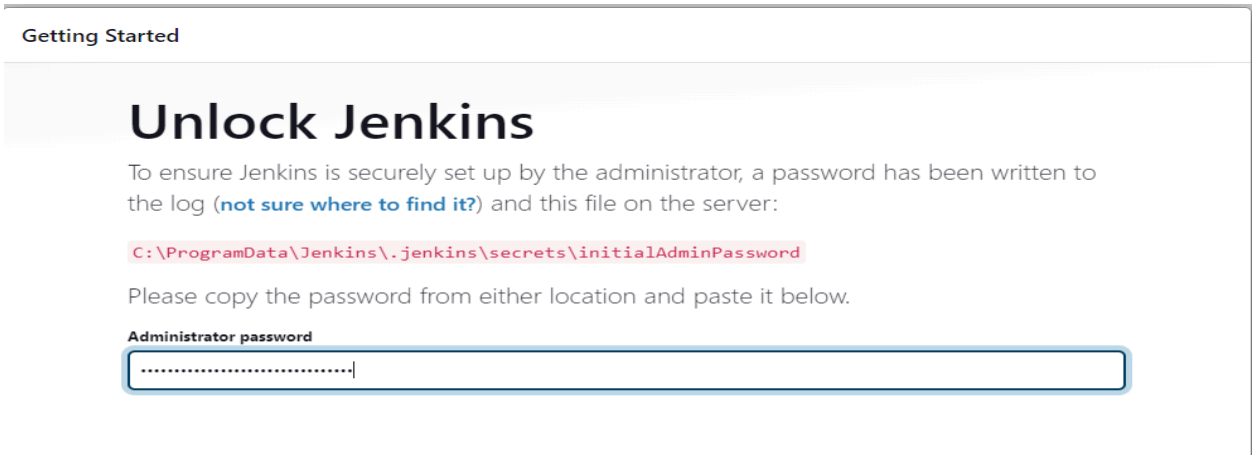




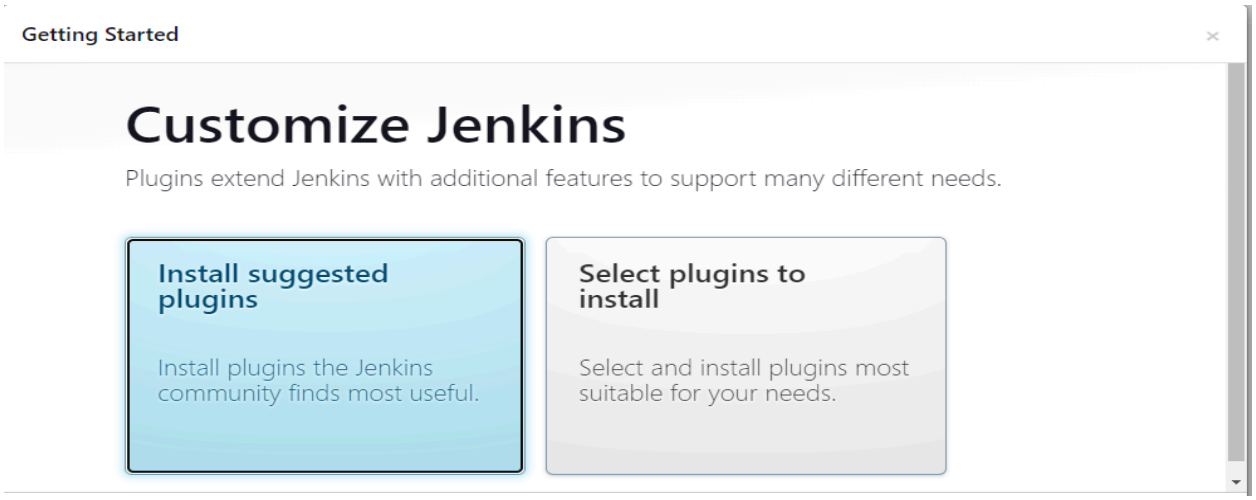


Installation completed

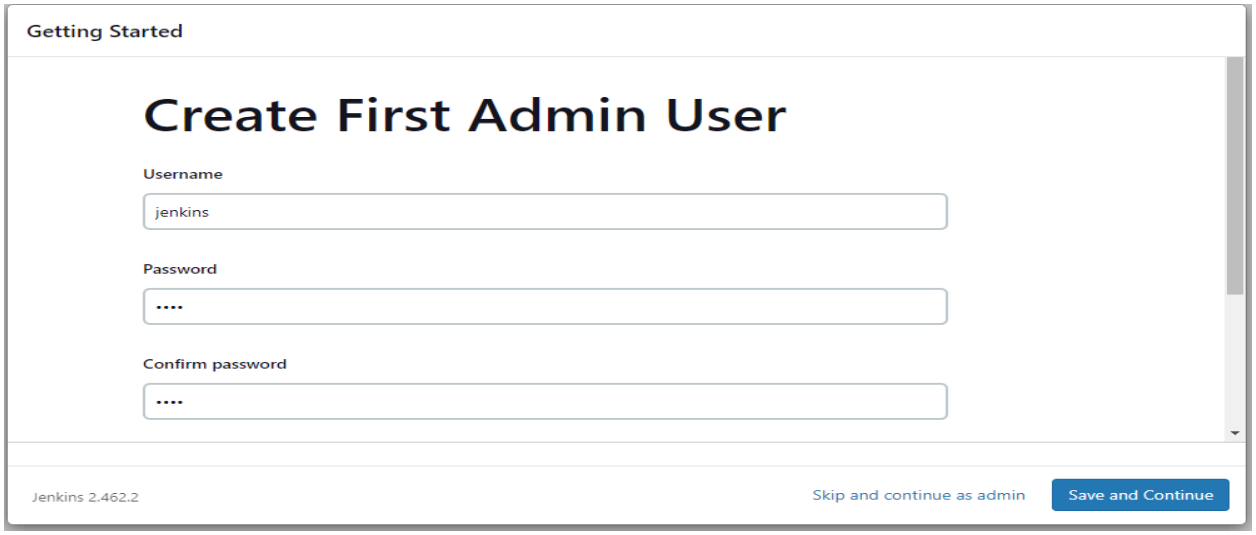
Once it is installed, go to http://localhost:<port_number_you_have_set> , where we first need to setup the Jenkins

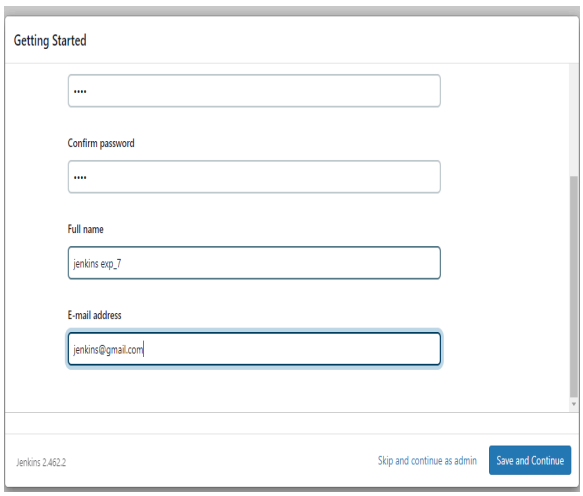


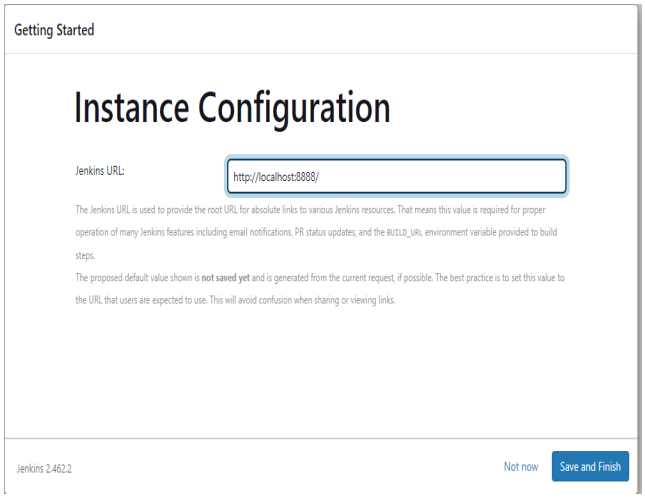
Install selected plugins, which will install all necessary plugins during installation only

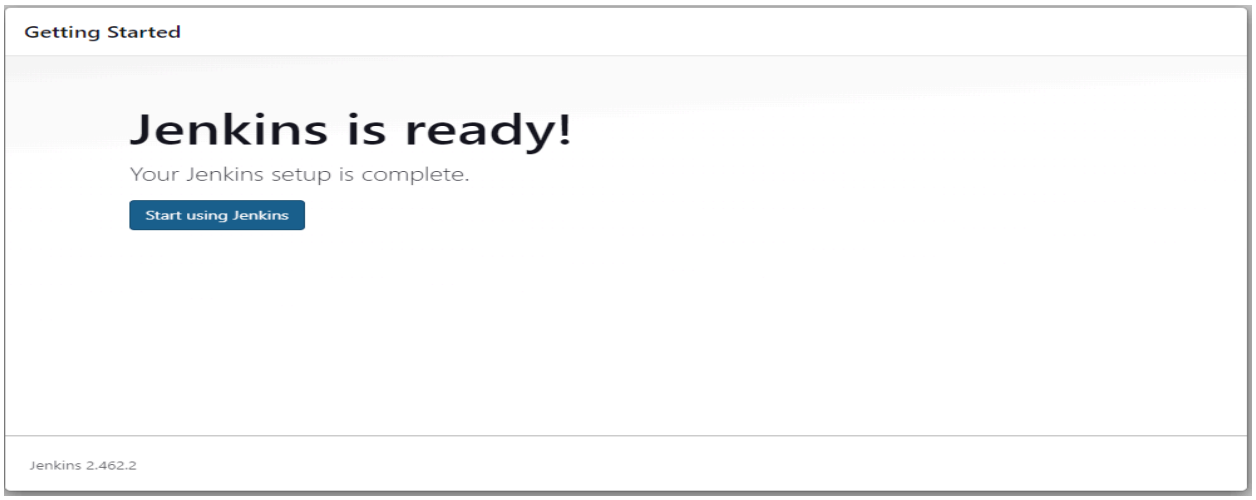


Set up the configuration details

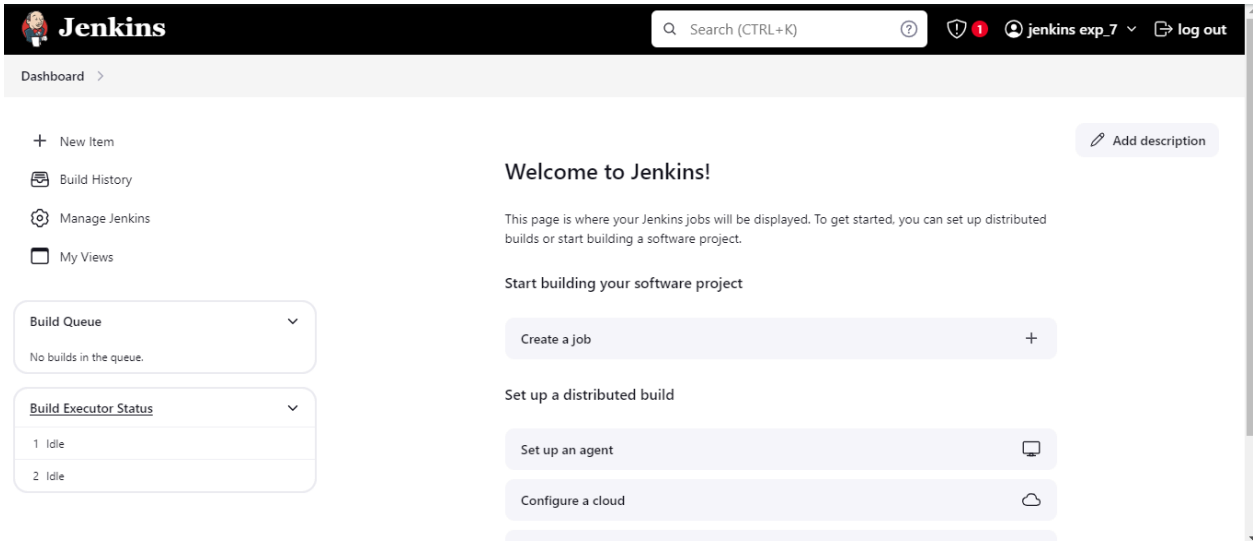








Once, all the setup is ready, you can login with your credentials



Prerequisites:
- **Jenkins installed**
- **Docker Installed (for SonarQube)**
- **SonarQube Docker Image**

Steps to integrate Jenkins with SonarQube

Open up Jenkins Dashboard on localhost, port 8081 or whichever port it is at for you.

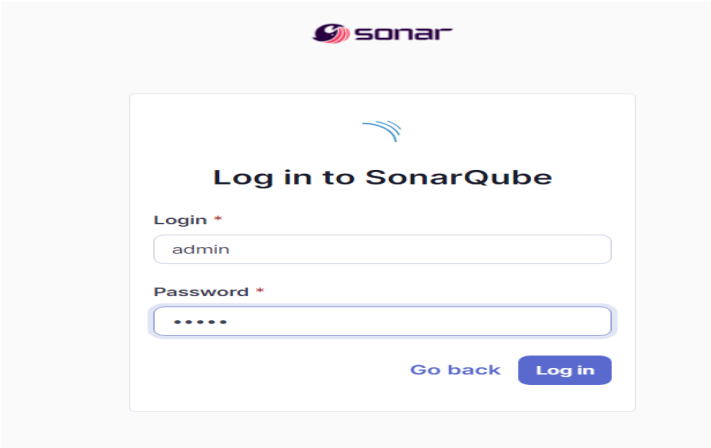
Run SonarQube in a Docker container using this command -
docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest

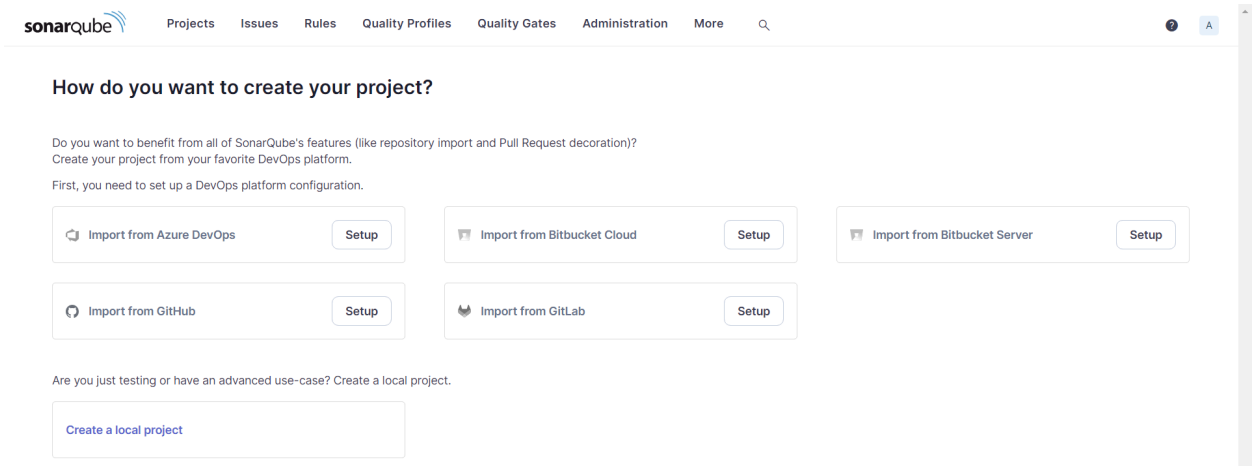
Warning: run above command only once

```
PS C:\Users\Komal> docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
Unable to find image 'sonarqube:latest' locally
```

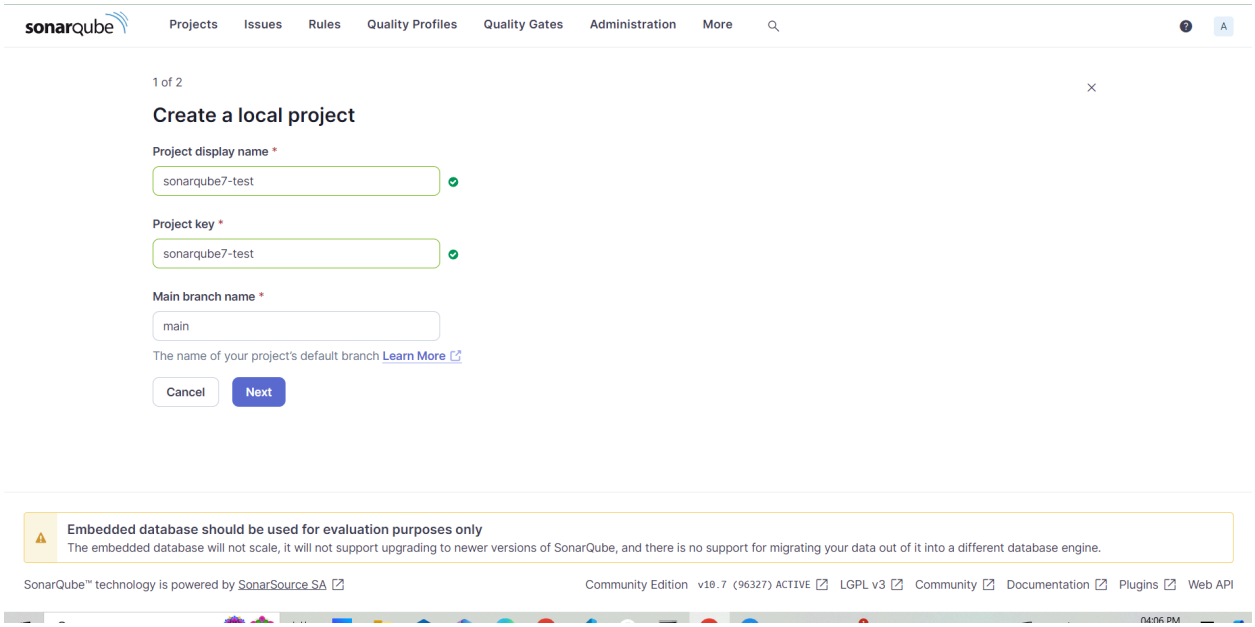
```
PS C:\Users\Komal> docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
7478e0ac0f23: Downloading [============>                                      ]  8.417MB/30.44MB
90a925ab929a: Downloading [==================================>                ]  9.321MB/12.87MB
7d9a34308537: Downloading [==========>                                        ]  9.521MB/47.28MB
80338217a4ab: Waiting
1a5fd5c7e184: Waiting
fbe03067fd0d: Waiting
8f68213fa028: Waiting
4f4fb700ef54: Waiting
```

Once the container is up and running, you can check the status of SonarQube at localhost port 9000.
Login to SonarQube using username admin and password admin.

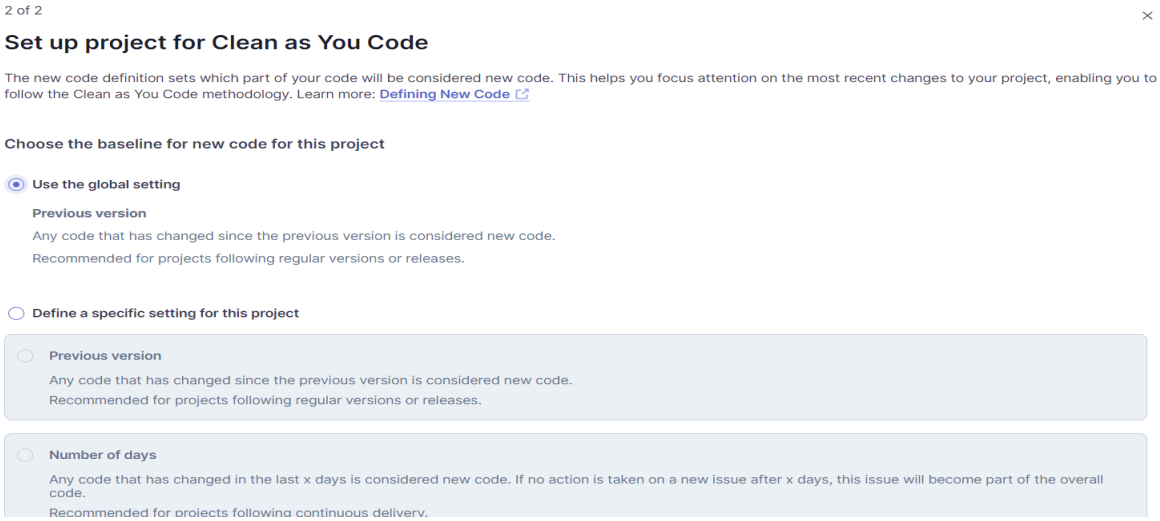




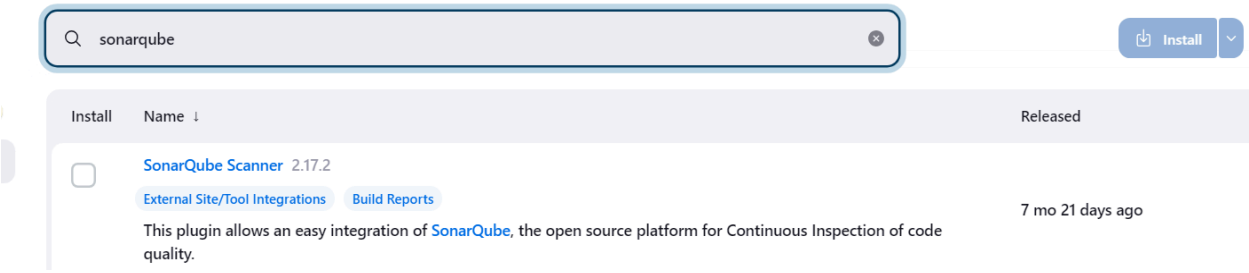
Create a manual project in SonarQube with the name sonarqube7-test



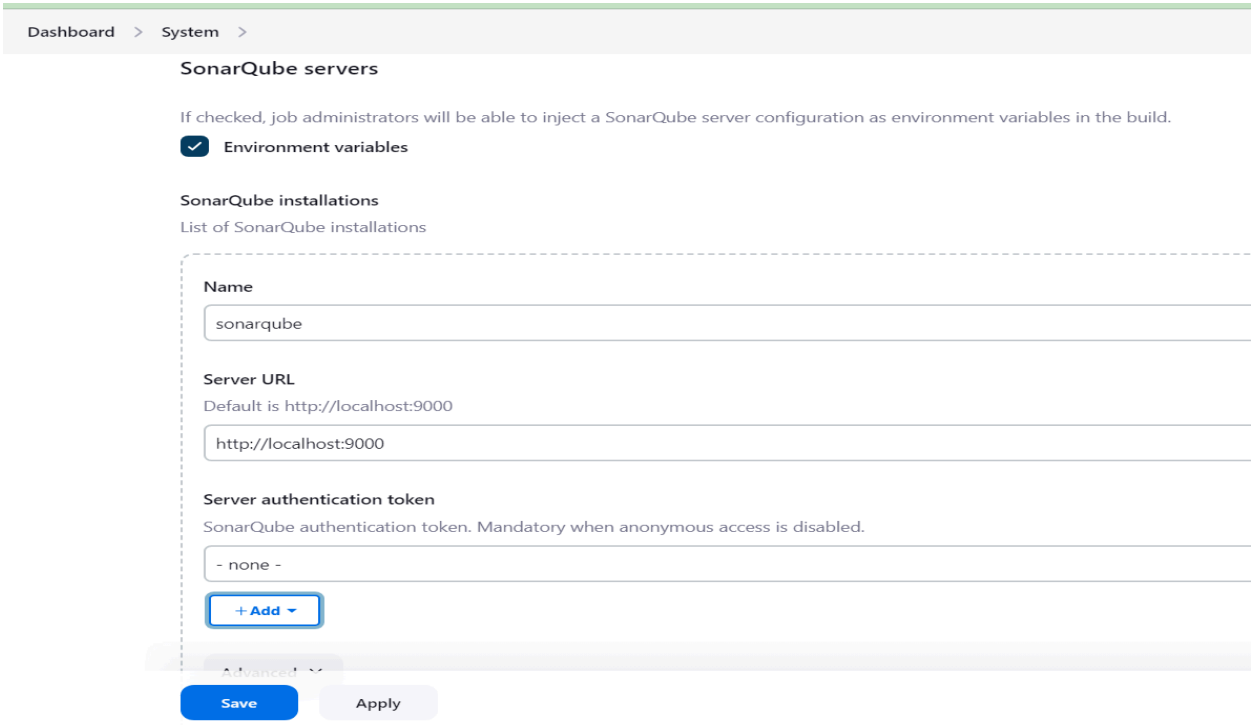
Setup the project and come back to Jenkins Dashboard.

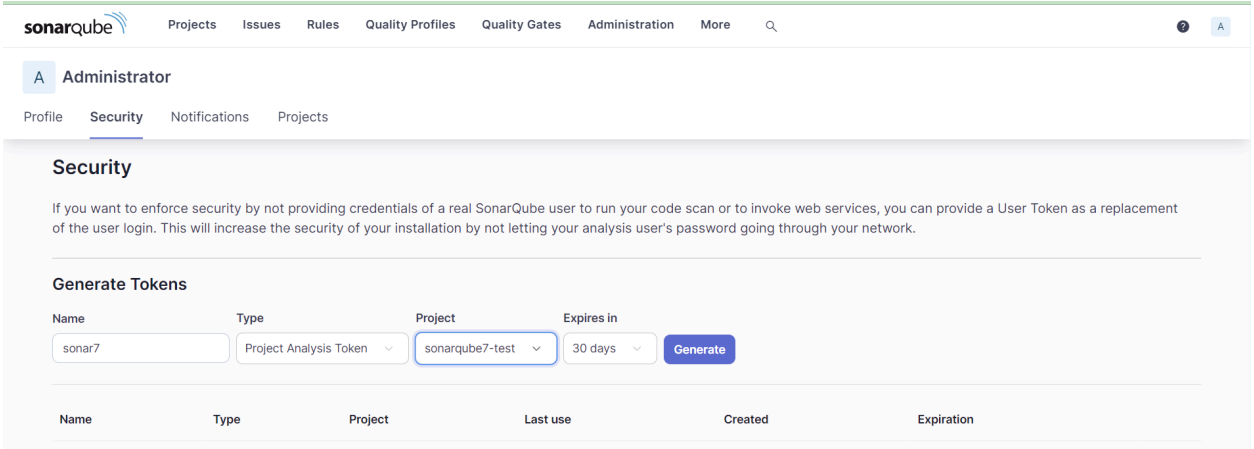


Go to Manage Jenkins and search for SonarQube Scanner for Jenkins and install it.

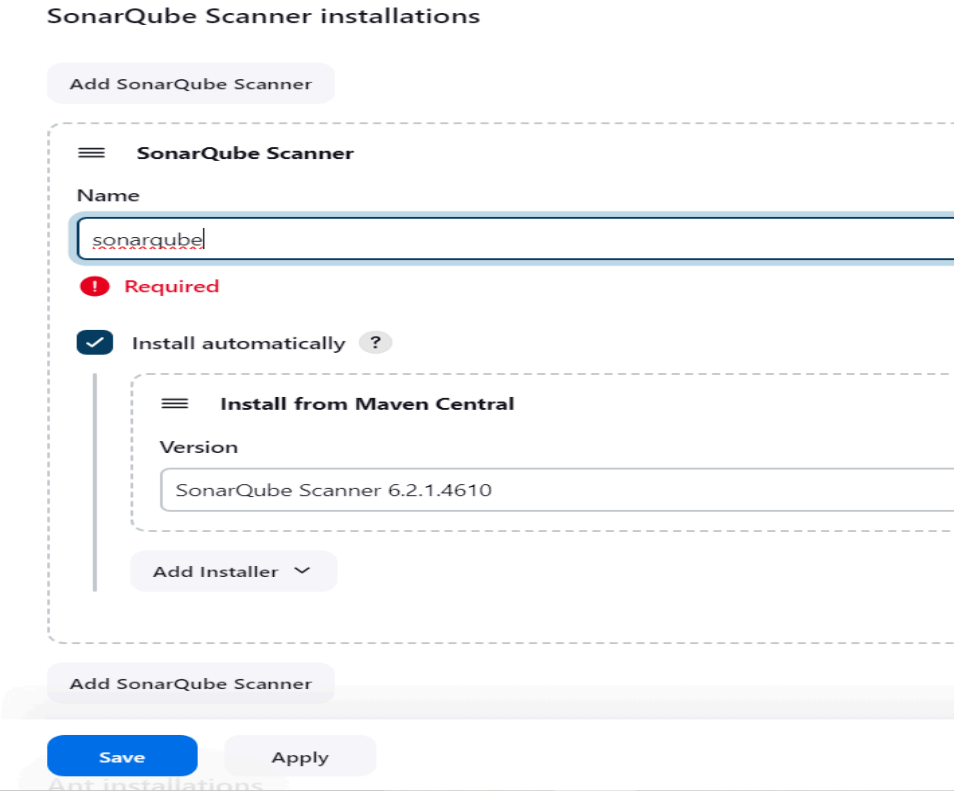


Under Jenkins 'Configure System', look for SonarQube Servers and enter the details. Enter the Server Authentication token if needed.

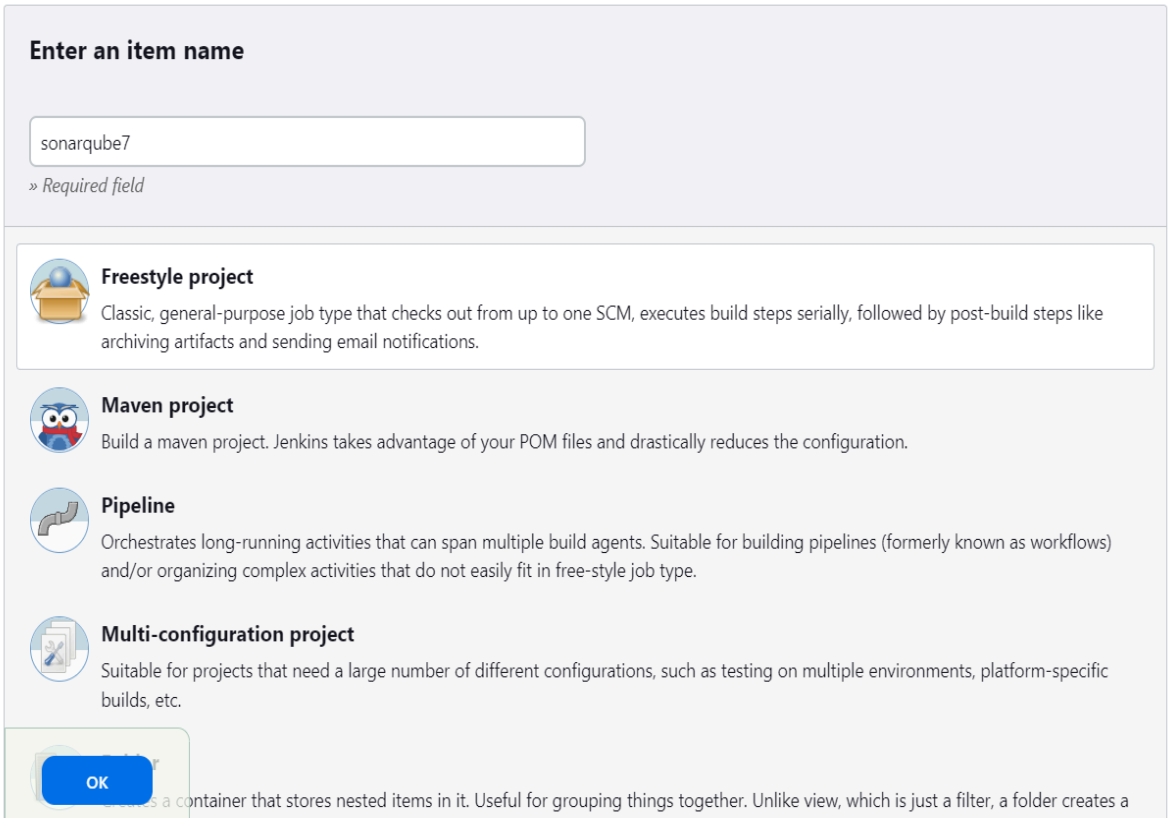




Under sonarqube scanner installation add the name and version



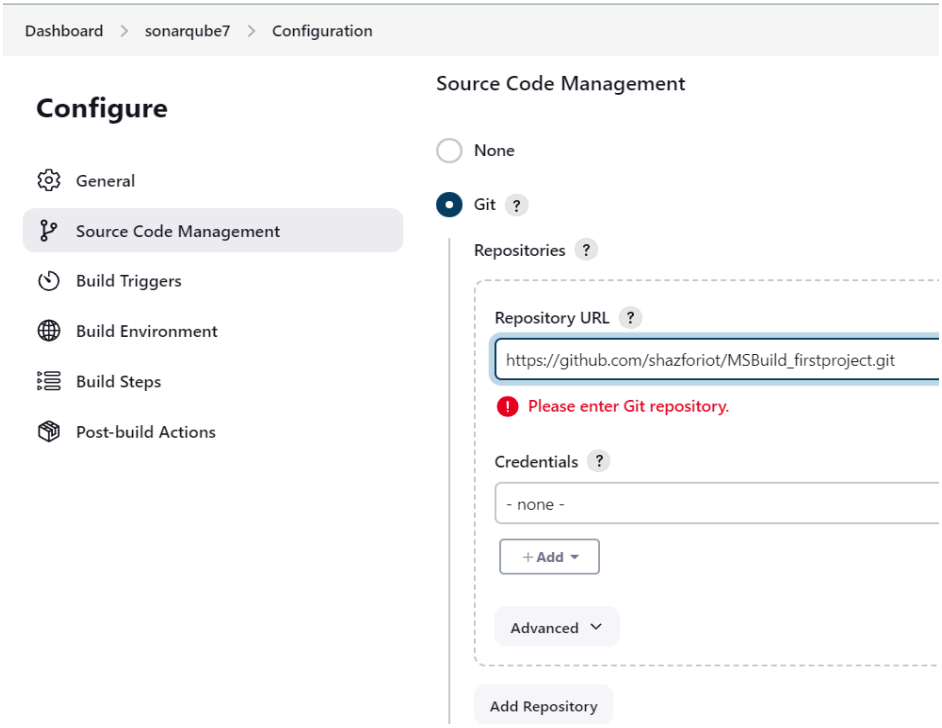
After the configuration, create a New Item in Jenkins, choose a freestyle project.



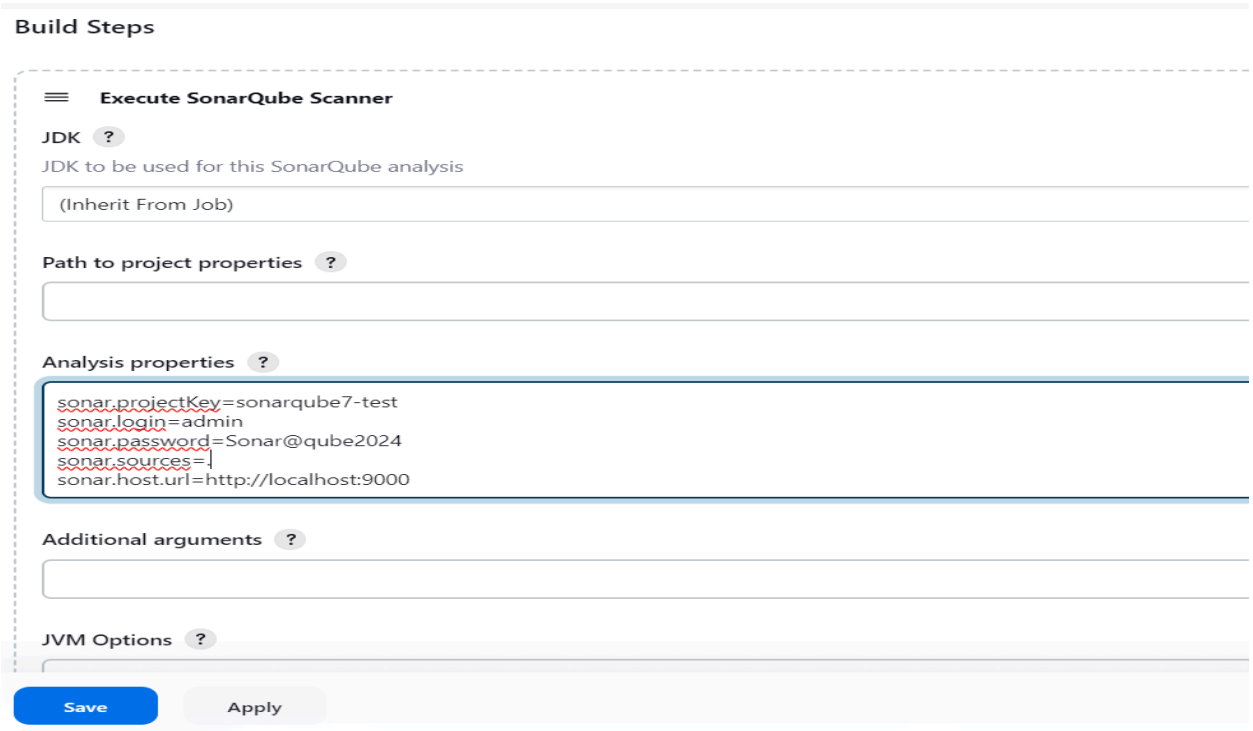
Choose this GitHub repository in Source Code Management.

https://github.com/shazforiot/MSBuild_firstproject.git

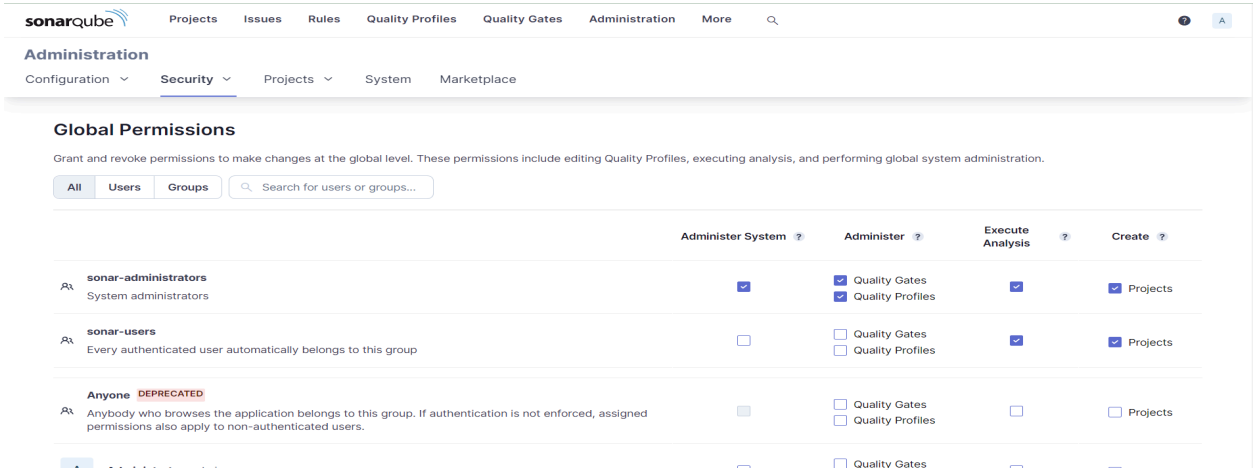
It is a sample hello-world project with no vulnerabilities and issues, just to test



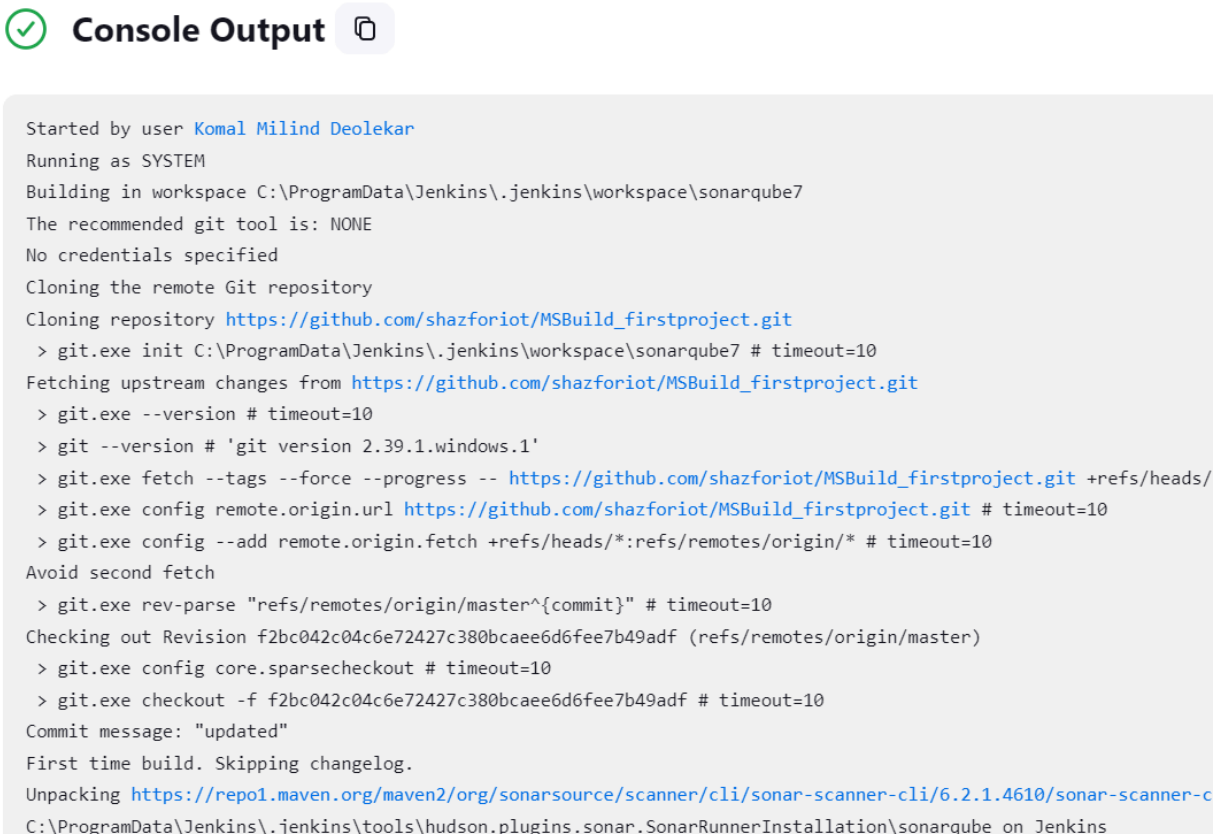
Under Build-> Execute SonarQube Scanner, enter these Analysis properties. Mention the SonarQube Project Key, Login, Password, Source path and Host URL.



Go to http://localhost:9000/<user_name>/permissions and allow Execute Permissions to the Admin user.

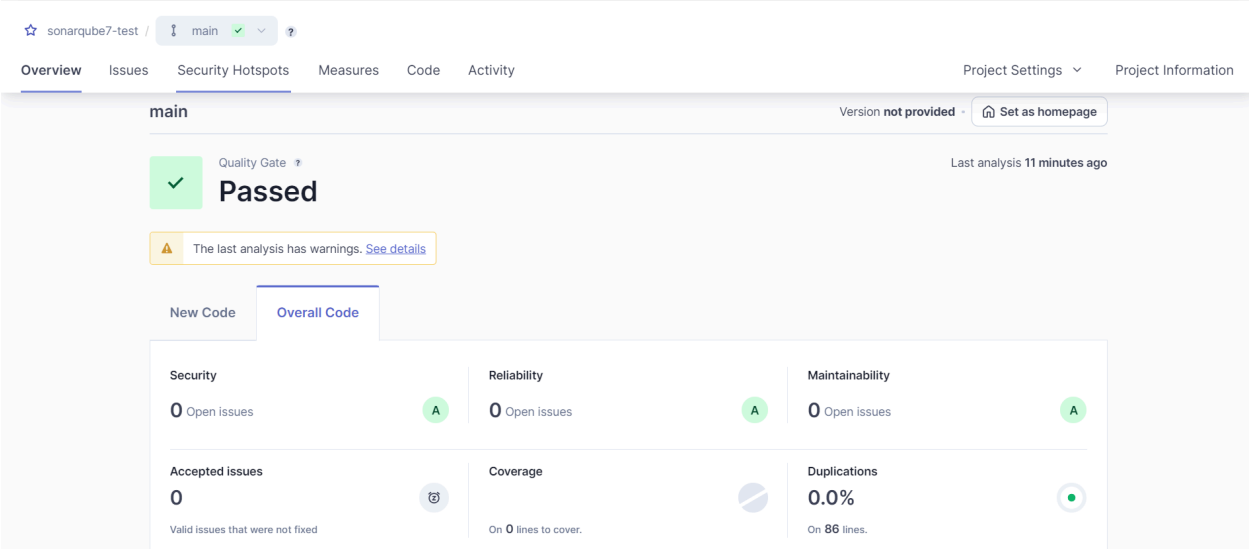


Run The Build.
Check the console output.



```
16:45:27.379 INFO  Sensor C# File Caching Sensor [csharp] (done) | time=0ms
16:45:27.379 INFO  Sensor Zero Coverage Sensor
16:45:27.396 INFO  Sensor Zero Coverage Sensor (done) | time=33ms
16:45:27.396 INFO  SCM Publisher SCM provider for this project is: git
16:45:27.396 INFO  SCM Publisher 4 source files to be analyzed
16:45:30.089 INFO  SCM Publisher 4/4 source files have been analyzed (done) | time=2692ms
16:45:30.094 INFO  CPD Executor Calculating CPD for 0 files
16:45:30.096 INFO  CPD Executor CPD calculation finished (done) | time=0ms
16:45:30.145 INFO  SCM revision ID 'f2bc042c04c6e72427c380bcaee6d6fee7b49adf'
16:45:31.663 INFO  Analysis report generated in 534ms, dir size=224.5 kB
16:45:31.928 INFO  Analysis report compressed in 182ms, zip size=24.0 kB
16:45:33.012 INFO  Analysis report uploaded in 1083ms
16:45:33.012 INFO  ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=sonarqube7-test
16:45:33.012 INFO  Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
16:45:33.012 INFO  More about the report processing at http://localhost:9000/api/ce/task?id=82df79fb-1bd4-48b3-91fb-93afa78d4ea6
16:45:33.045 INFO  Analysis total time: 2:24.886 s
16:45:33.096 INFO  SonarScanner Engine completed successfully
16:45:33.255 INFO  EXECUTION SUCCESS
16:45:33.258 INFO  Total time: 4:15.033s
Finished: SUCCESS
```

Once the build is complete, check the project in SonarQube.



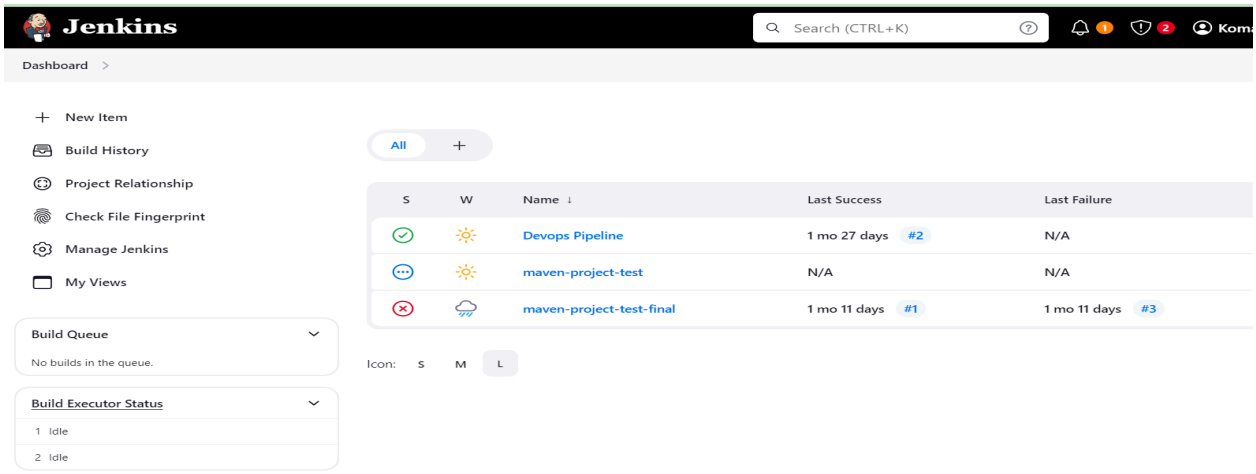
In this way, we have integrated Jenkins with SonarQube for SAST.

Experiment No. 8

Prerequisites

- **Jenkins installed on your machine.**
- **Docker installed to run SonarQube.**
- **SonarQube installed via Docker.**

Open up Jenkins Dashboard on localhost, port 8080 or on the port you have configured



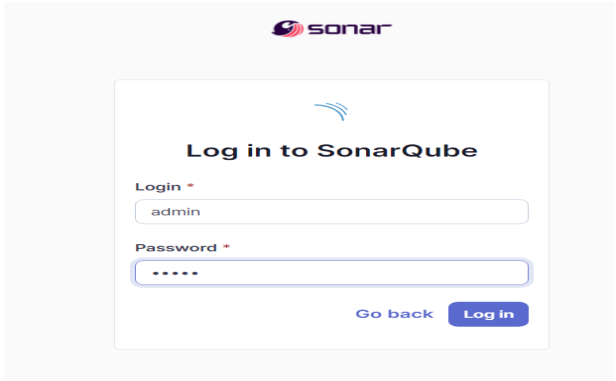
Run SonarQube in a Docker container using command:

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

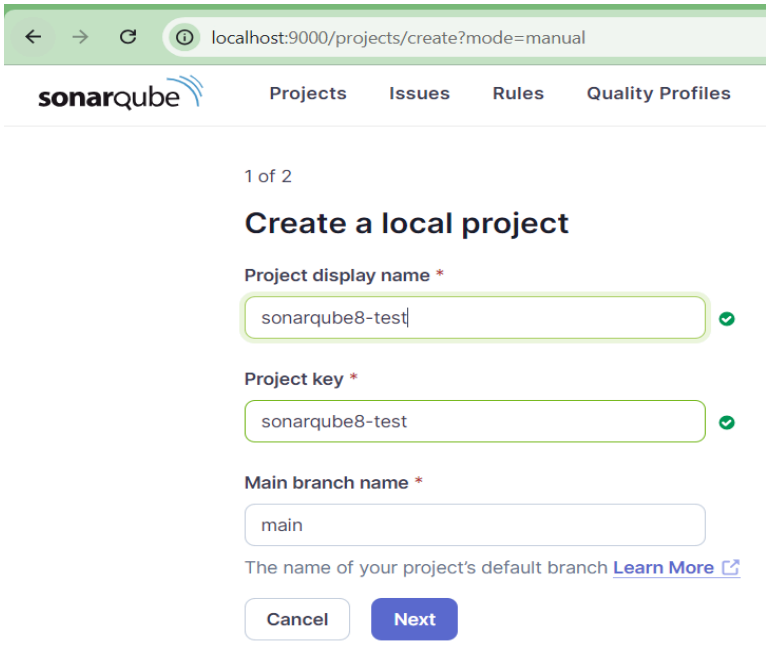
```
PS C:\Users\Komal> docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
7478e0ac0f23: Downloading [============>                                      ]  8.417MB/30.44MB
90a925ab929a: Downloading [==================================>                ]  9.321MB/12.87MB
7d9a34308537: Downloading [==========>                                        ]  9.521MB/47.28MB
80338217a4ab: Waiting
1a5fd5c7e184: Waiting
fbe03067fd0d: Waiting
8f68213fa028: Waiting
4f4fb700ef54: Waiting
```

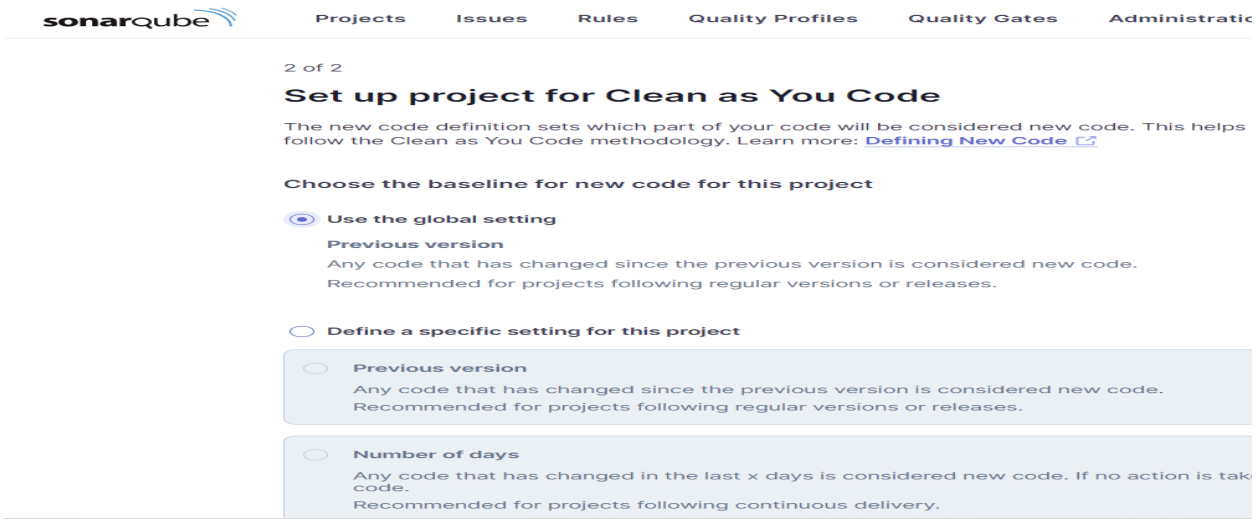
Once the container is up and running, you can check the status of SonarQube at localhost port 9000.

Login to SonarQube with your credentials.



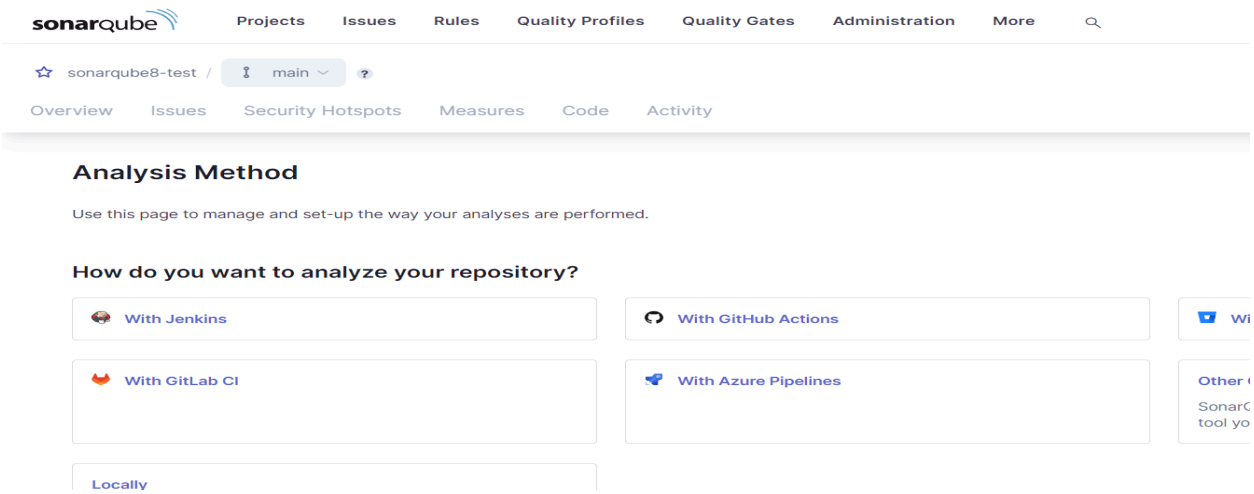
Create a manual project in SonarQube with the name sonarqube8-test





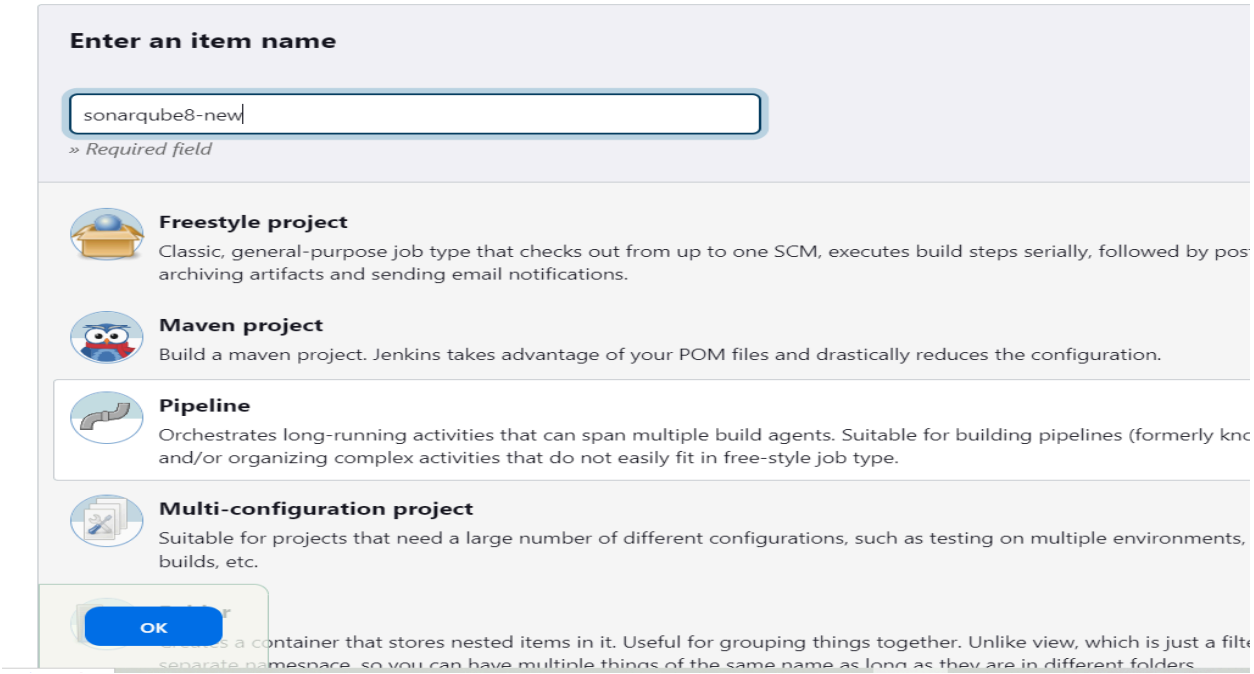
Generate SonarQube Token

- **Go to My Account > Security > Generate Tokens.**
- **Copy the generated token for later use**



Create a Jenkins Pipeline

• Go to Jenkins Dashboard, click New Item, and select Pipeline.

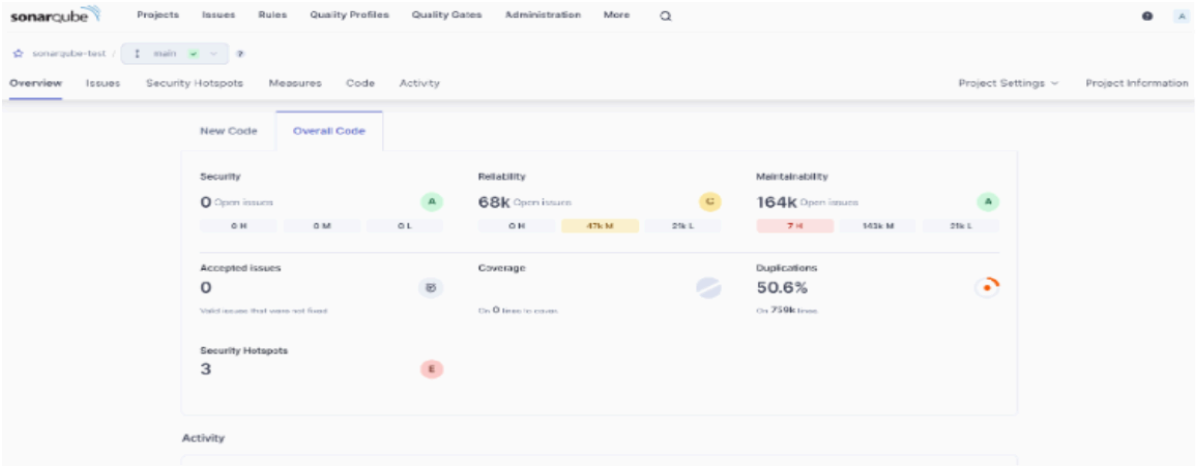



```
docker network create sonarnet
node {
stage('Cloning the GitHub Repo') {
git 'https://github.com/shazforiot/GOL.git'
}
stage('SonarQube analysis') {
withSonarQubeEnv('sonarqube') {
sh """
docker run --rm --network host \
-e SONAR_HOST_URL=http://<ip_address>:9000 \
-e SONAR_LOGIN=admin \
```

```
-e SONAR_PASSWORD=<Sonarqube_password> \
-e SONAR_PROJECT_KEY=sonarqube8-test \
-v ${WORKSPACE.replace('\\', '/')}:/usr/src \
sonarsource/sonar-scanner-cli \
-Dsonar.projectKey=sonarqube8-test \
-Dsonar.exclusions=vendor/**,resources/**,**/*.java \
-Dsonar.login=admin \
-Dsonar.password=<Sonarqube_password>
"""
}
}
}
```

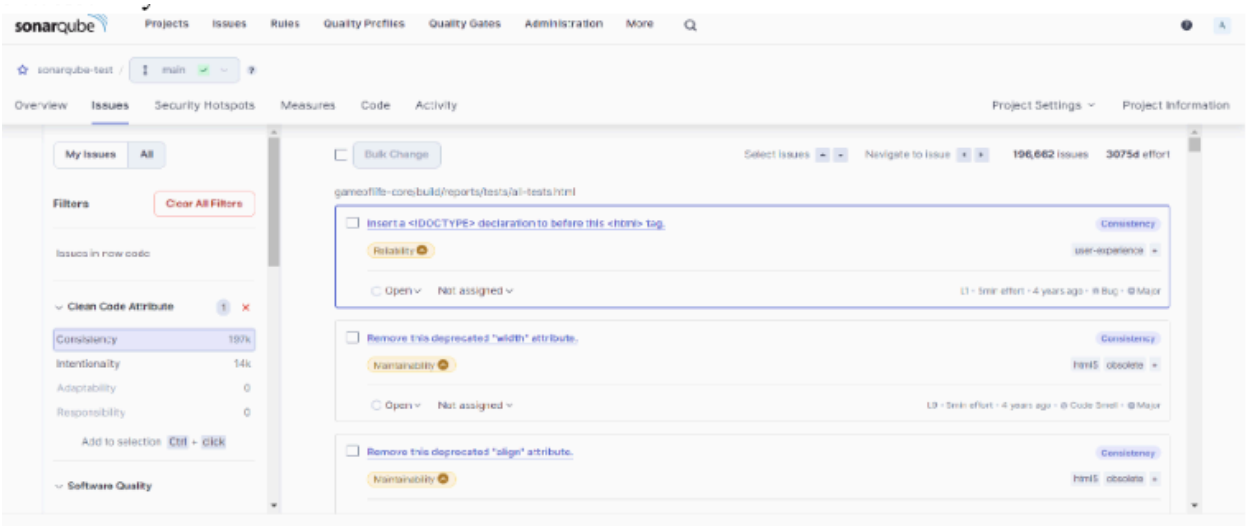
Build project

Now, check the project in SonarQube

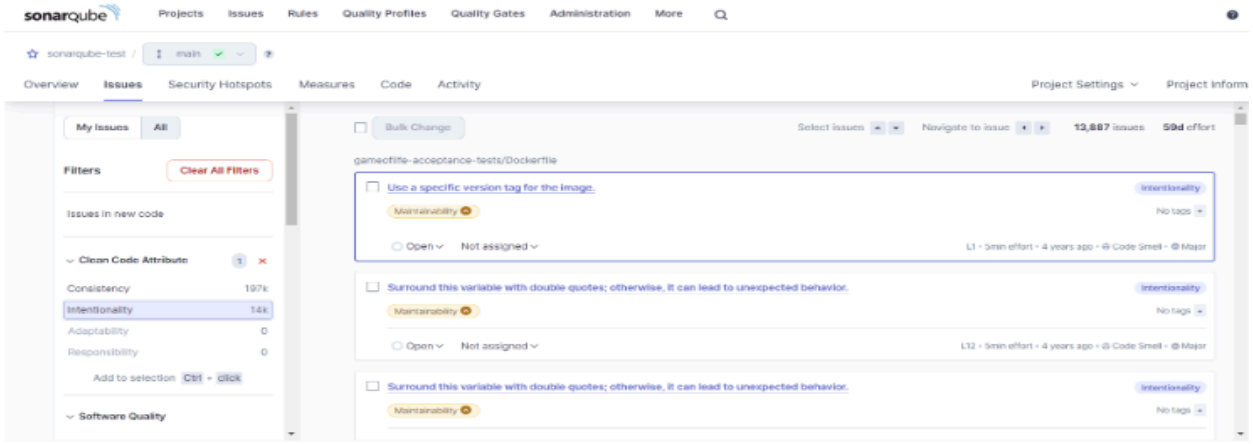


Code Problems

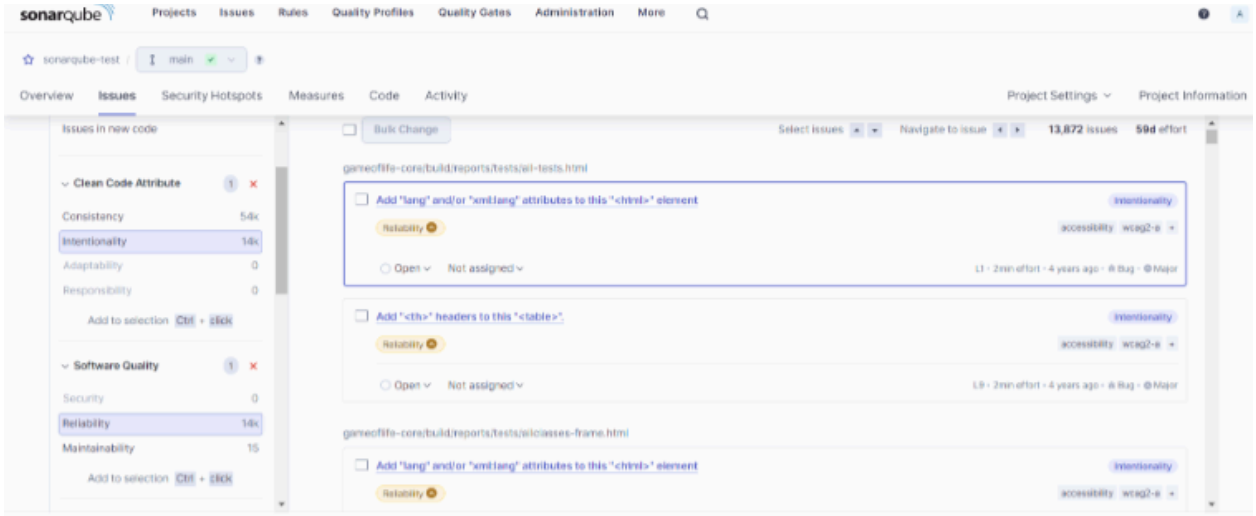
Consistency :



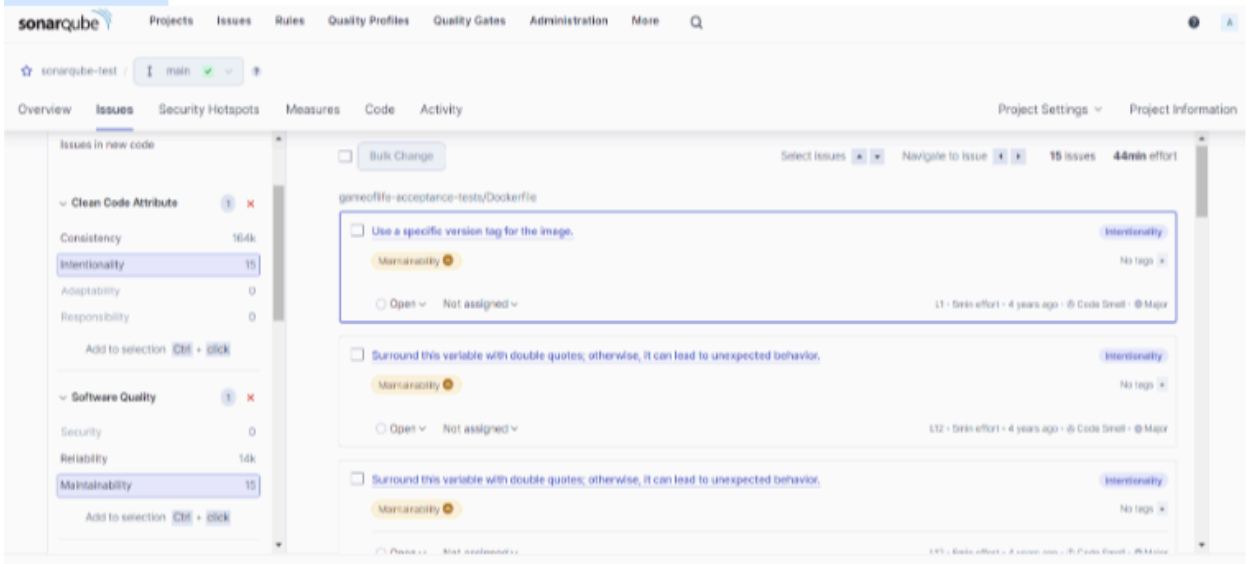
Intentionality :



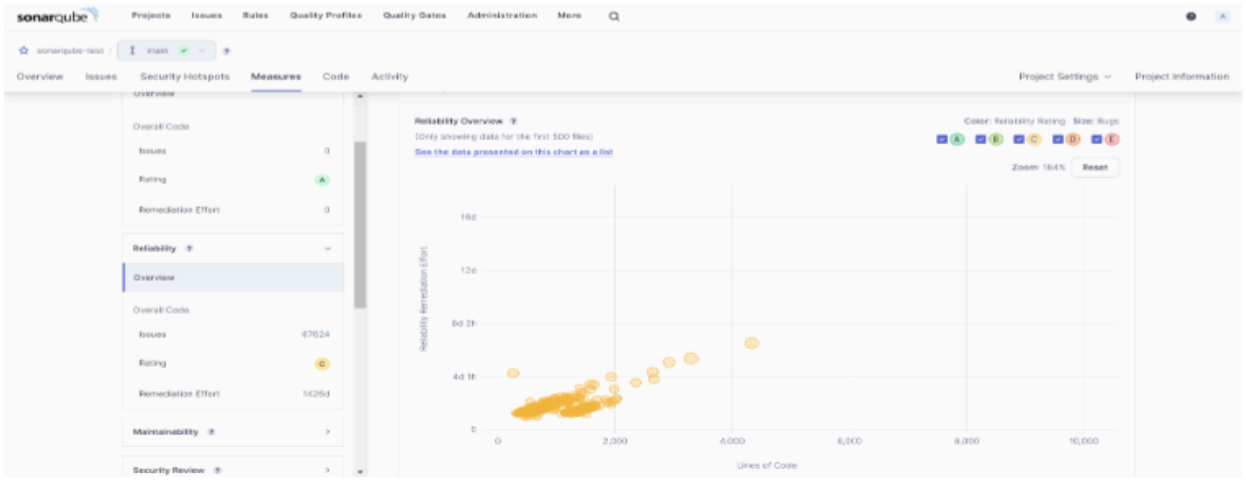
Bugs :



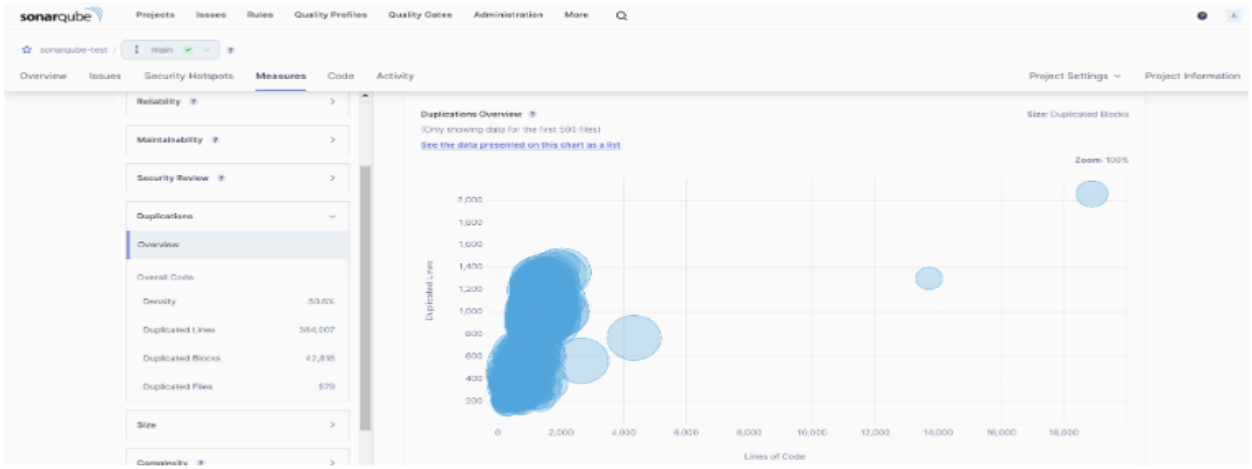
Code Smells :



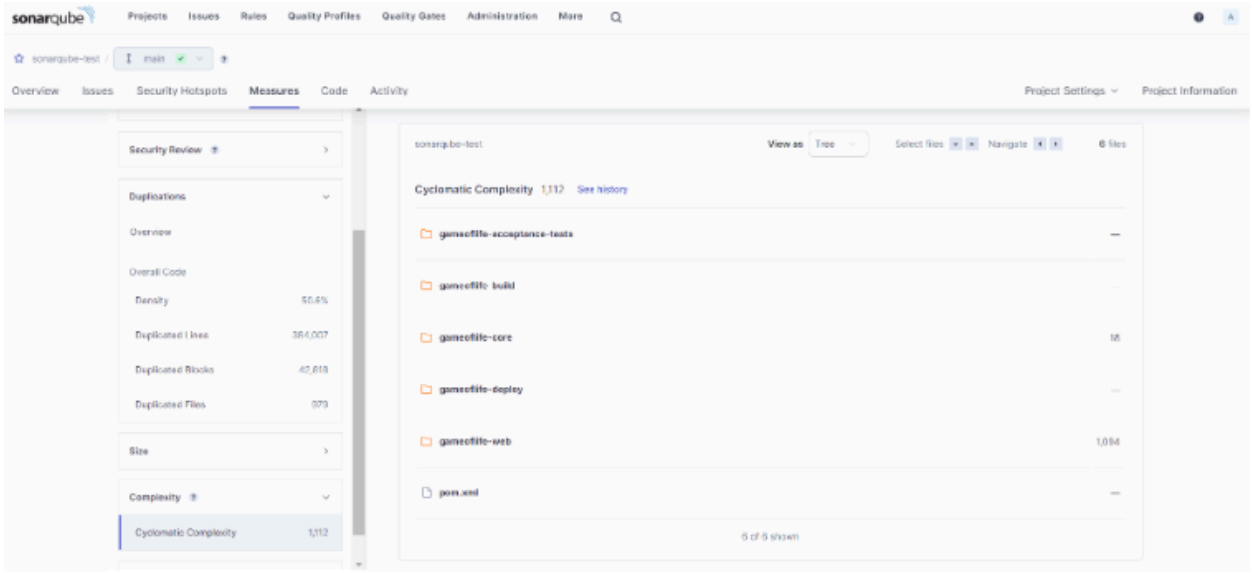
Reliability :



Duplications :



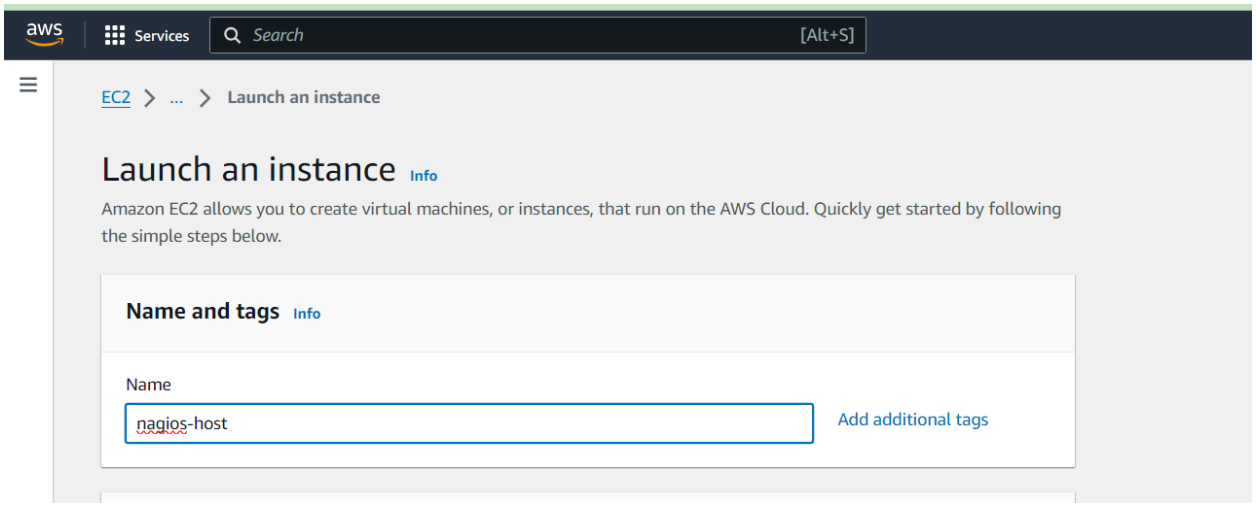
Cyclomatic Complexities :

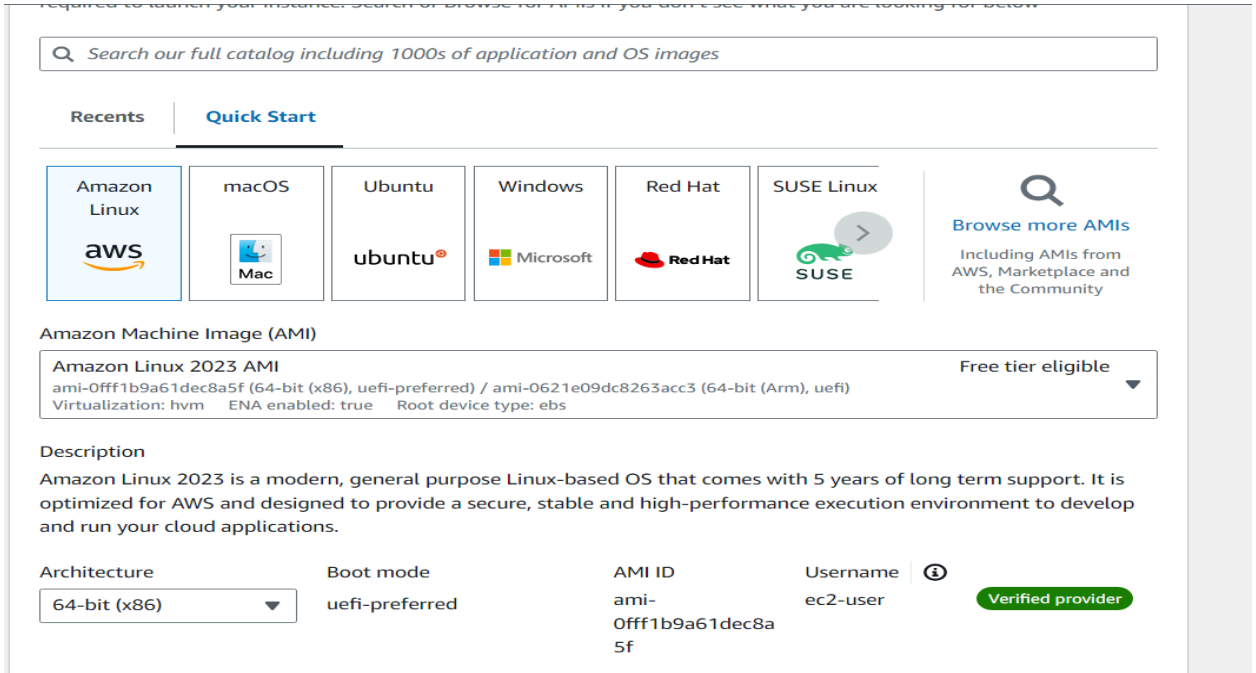


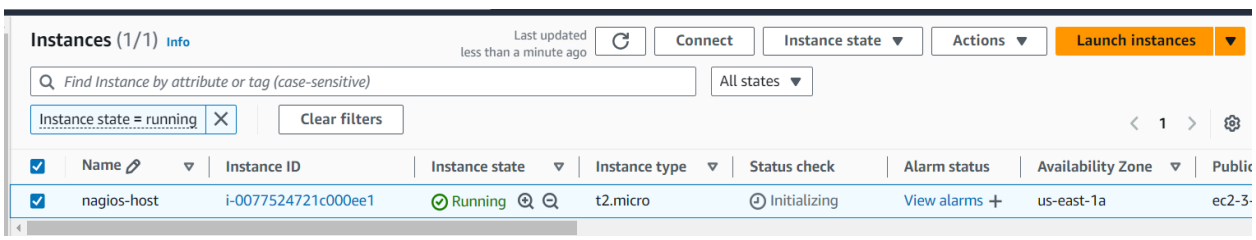
Experiment No. 9

Prerequisites: AWS Free Tier

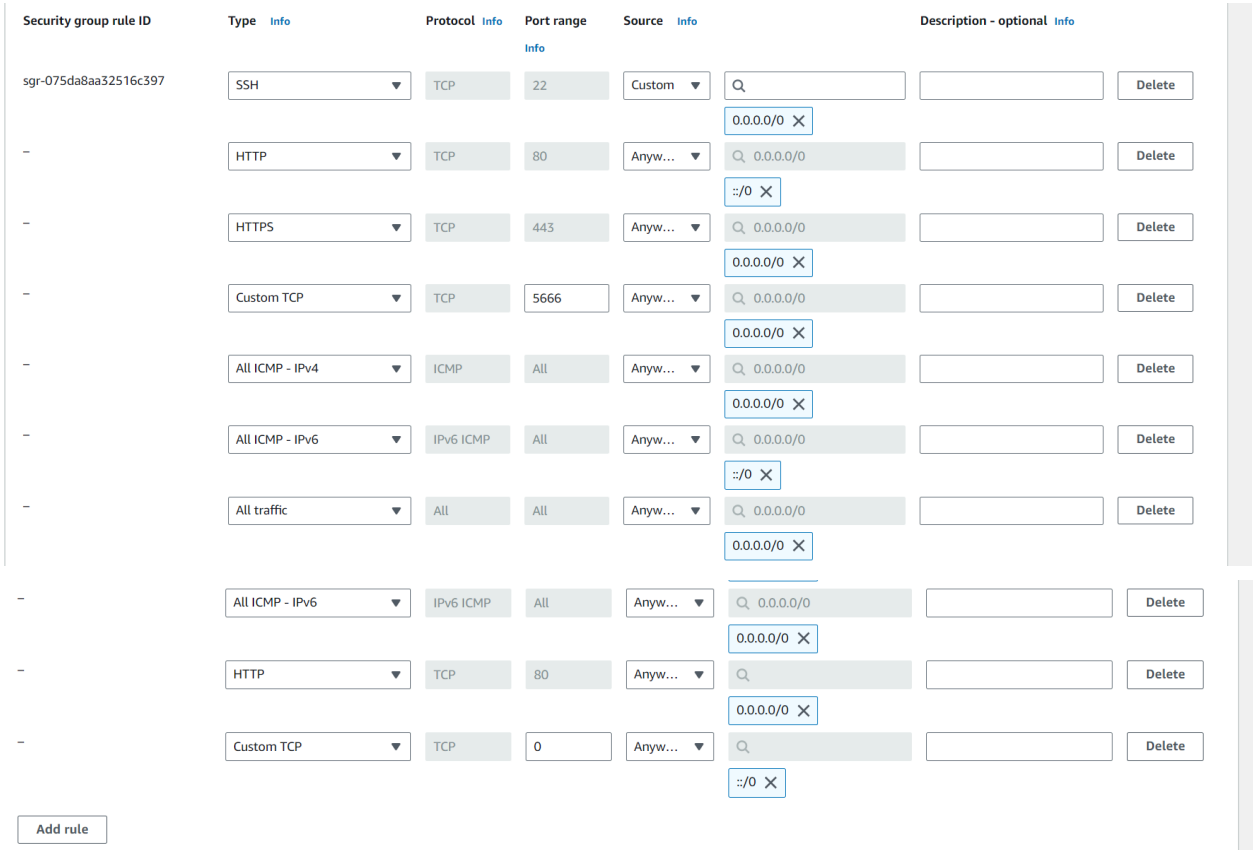
Create an Amazon Linux EC2 Instance in AWS and name it - nagios-host







Under Security Group, make sure HTTP, HTTPS, SSH, ICMP are open from everywhere.



Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-075da8aa32516c397	SSH	TCP	22	Custom	0.0.0.0/0		Delete
–	HTTP	TCP	80	Anyw…	::/0		Delete
–	HTTPS	TCP	443	Anyw…	0.0.0.0/0		Delete
–	Custom TCP	TCP	5666	Anyw…	0.0.0.0/0		Delete
–	All ICMP - IPv4	ICMP	All	Anyw…	0.0.0.0/0		Delete
–	All ICMP - IPv6	IPv6 ICMP	All	Anyw…	::/0		Delete
–	All traffic	All	All	Anyw…	0.0.0.0/0		Delete
–	All ICMP - IPv6	IPv6 ICMP	All	Anyw…	0.0.0.0/0		Delete
–	HTTP	TCP	80	Anyw…	0.0.0.0/0		Delete
–	Custom TCP	TCP	0	Anyw…	::/0		Delete

Add rule

You have to edit the inbound rules of the specified Security Group for this.

SSH into Your EC2 instance or simply use EC2 Instance Connect from the browser.
Update the package indices and install the following packages using yum
sudo yum update -y
sudo yum install -y httpd php

```
[ec2-user@ip-172-31-45-197 ~]$ sudo yum update -y
Last metadata expiration check: 0:39:01 ago on Sun Oct 13 14:23:12 2024.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-172-31-45-197 ~]$ sudo yum install -y httpd php
Last metadata expiration check: 0:42:37 ago on Sun Oct 13 14:23:12 2024.
Dependencies resolved.
```

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

```
Installed:
  apr-1.7.2-2.amzn2023.0.2.x86_64                  apr-util-1.6.3-1.amzn2023.0.1.x86_64          apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64
  generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch  httpd-2.4.62-1.amzn2023.x86_64              httpd-core-2.4.62-1.amzn2023.x86_64
  httpd-filesystem-2.4.62-1.amzn2023.noarch        httpd-tools-2.4.62-1.amzn2023.x86_64          libbrotli-1.0.9-4.amzn2023.0.2.x86_64
  libsodium-1.0.19-4.amzn2023.x86_64               libxslt-1.1.34-5.amzn2023.0.2.x86_64          mailcap-2.1.49-3.amzn2023.0.3.noarch
  mod_http2-2.0.27-1.amzn2023.0.3.x86_64           mod_lua-2.4.62-1.amzn2023.x86_64              nginx-filesystem-1:1.24.0-1.amzn2023.0.4.noarch
  php8.3-8.3.10-1.amzn2023.0.1.x86_64              php8.3-cli-8.3.10-1.amzn2023.0.1.x86_64       php8.3-common-8.3.10-1.amzn2023.0.1.x86_64
  php8.3-fpm-8.3.10-1.amzn2023.0.1.x86_64          php8.3-mbstring-8.3.10-1.amzn2023.0.1.x86_64  php8.3-opcache-8.3.10-1.amzn2023.0.1.x86_64
  php8.3-pdo-8.3.10-1.amzn2023.0.1.x86_64          php8.3-process-8.3.10-1.amzn2023.0.1.x86_64   php8.3-sodium-8.3.10-1.amzn2023.0.1.x86_64
  php8.3-xml-8.3.10-1.amzn2023.0.1.x86_64

Complete!
[ec2-user@ip-172-31-45-197 ~]$
```

sudo yum install -y gcc glibc glibc-common

```
[ec2-user@ip-172-31-45-197 ~]$ sudo yum install -y gcc glibc glibc-common
Last metadata expiration check: 0:43:39 ago on Sun Oct 13 14:23:12 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
Installing:			
gcc	x86_64	11.4.1-2.amzn2023.0.2	amazonlinux
Installing dependencies:			
annobin-docs	noarch	10.93-1.amzn2023.0.1	amazonlinux
annobin-plugin-gcc	x86_64	10.93-1.amzn2023.0.1	amazonlinux
cpp	x86_64	11.4.1-2.amzn2023.0.2	amazonlinux
gc	x86_64	8.0.4-5.amzn2023.0.2	amazonlinux
glibc-devel	x86_64	2.34-52.amzn2023.0.11	amazonlinux
glibc-headers-x86	noarch	2.34-52.amzn2023.0.11	amazonlinux
guile22	x86_64	2.2.7-2.amzn2023.0.3	amazonlinux
kernel-headers	x86_64	6.1.109-118.189.amzn2023	amazonlinux
libmpc	x86_64	1.2.1-2.amzn2023.0.2	amazonlinux
libtool-ltdl	x86_64	2.4.7-1.amzn2023.0.3	amazonlinux
libxcrypt-devel	x86_64	4.4.33-7.amzn2023	amazonlinux
make	x86_64	1:4.3-5.amzn2023.0.2	amazonlinux

Transaction Summary

```
Installed:
  annobin-docs-10.93-1.amzn2023.0.1.noarch          annobin-plugin-gcc-10.93-1.amzn2023.0.1.x86_64   cpp-11.4.1-2.amzn2023.0.2.x86_64
  gc-8.0.4-5.amzn2023.0.2.x86_64                    gcc-11.4.1-2.amzn2023.0.2.x86_64                 glibc-devel-2.34-52.amzn2023.0.11.x86_64
  glibc-headers-x86-2.34-52.amzn2023.0.11.noarch    guile22-2.2.7-2.amzn2023.0.3.x86_64              kernel-headers-6.1.109-118.189.amzn2023.x86_64
  libmpc-1.2.1-2.amzn2023.0.2.x86_64                libtool-ltdl-2.4.7-1.amzn2023.0.3.x86_64         libxcrypt-devel-4.4.33-7.amzn2023.x86_64
  make-1:4.3-5.amzn2023.0.2.x86_64

Complete!
[ec2-user@ip-172-31-45-197 ~]$
```

sudo yum install -y gd gd-devel

```
[ec2-user@ip-172-31-45-197 ~]$ sudo yum install -y gd gd-devel
Last metadata expiration check: 0:44:42 ago on Sun Oct 13 14:23:12 2024.
Dependencies resolved.
```

Package	Architecture	Version	Repository
Installing:			
gd	x86_64	2.3.3-5.amzn2023.0.3	amazonlinux
gd-devel	x86_64	2.3.3-5.amzn2023.0.3	amazonlinux
Installing dependencies:			
brotli	x86_64	1.0.9-4.amzn2023.0.2	amazonlinux
brotli-devel	x86_64	1.0.9-4.amzn2023.0.2	amazonlinux
bzip2-devel	x86_64	1.0.8-6.amzn2023.0.2	amazonlinux
cairo	x86_64	1.17.6-2.amzn2023.0.1	amazonlinux
cmake-filesystem	x86_64	3.22.2-1.amzn2023.0.4	amazonlinux
fontconfig	x86_64	2.13.94-2.amzn2023.0.2	amazonlinux
fontconfig-devel	x86_64	2.13.94-2.amzn2023.0.2	amazonlinux
fonts-filesystem	noarch	1:2.0.5-12.amzn2023.0.2	amazonlinux
freetype	x86_64	2.13.2-5.amzn2023.0.1	amazonlinux
freetype-devel	x86_64	2.13.2-5.amzn2023.0.1	amazonlinux
glib2-devel	x86_64	2.74.7-689.amzn2023.0.2	amazonlinux
google-noto-fonts-common	noarch	20201206-2.amzn2023.0.2	amazonlinux
google-noto-sans-vf-fonts	noarch	20201206-2.amzn2023.0.2	amazonlinux
graphite2	x86_64	1.3.14-7.amzn2023.0.2	amazonlinux
graphite2-devel	x86_64	1.3.14-7.amzn2023.0.2	amazonlinux
harfbuzz	x86_64	7.0.0-2.amzn2023.0.1	amazonlinux
harfbuzz-devel	x86_64	7.0.0-2.amzn2023.0.1	amazonlinux

Create a new Nagios User with its password. You'll have to enter the password twice for

confirmation.
sudo adduser -m nagios
sudo passwd nagios

```
[ec2-user@ip-172-31-45-197 ~]$ sudo useradd -m nagios
[ec2-user@ip-172-31-45-197 ~]$ sudo passwd nagios
Changing password for user nagios.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[ec2-user@ip-172-31-45-197 ~]$
```

Create a new user group
sudo groupadd nagcmd

```
[ec2-user@ip-172-31-45-197 ~]$ sudo groupadd nagcmd
[ec2-user@ip-172-31-45-197 ~]$
```

Use these commands so that you don't have to use sudo for Apache and Nagios
sudo usermod -a -G nagcmd nagios
sudo usermod -a -G nagcmd apache

```
[ec2-user@ip-172-31-45-197 ~]$ sudo usermod -a -G nagcmd nagios
sudo usermod -a -G nagcmd apache
[ec2-user@ip-172-31-45-197 ~]$
```

Create a new directory for Nagios downloads
mkdir ~/downloads
cd ~/downloads

```
[ec2-user@ip-172-31-45-197 ~]$ mkdir ~/downloads
[ec2-user@ip-172-31-45-197 ~]$ cd ~/downloads
[ec2-user@ip-172-31-45-197 downloads]$
```

Use wget to download the source zip files.
Wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz

```
[ec2-user@ip-172-31-45-197 downloads]$ Wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz
-bash: Wget: command not found
[ec2-user@ip-172-31-45-197 downloads]$ wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz
--2024-10-13 15:17:15--  https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz
Resolving assets.nagios.com (assets.nagios.com)... 45.79.49.120, 2600:3c00::f03c:92ff:fef7:45ce
Connecting to assets.nagios.com (assets.nagios.com)|45.79.49.120|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11333414 (11M) [application/x-gzip]
Saving to: 'nagios-4.4.6.tar.gz'

nagios-4.4.6.tar.gz                 100%[=============================================================================>]  10.81M  15.2MB/s    in 0.7s

2024-10-13 15:17:16 (15.2 MB/s) - 'nagios-4.4.6.tar.gz' saved [11333414/11333414]
```

wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz

```
[ec2-user@ip-172-31-45-197 downloads]$ wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz
--2024-10-13 15:17:35--  https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz
Resolving nagios-plugins.org (nagios-plugins.org)... 45.56.123.251
Connecting to nagios-plugins.org (nagios-plugins.org)|45.56.123.251|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2782610 (2.7M) [application/x-gzip]
Saving to: 'nagios-plugins-2.3.3.tar.gz'

nagios-plugins-2.3.3.tar.gz           100%[=============================================================================>]   2.65M  4.26MB/s    in 0.6s

2024-10-13 15:17:35 (4.26 MB/s) - 'nagios-plugins-2.3.3.tar.gz' saved [2782610/2782610]

[ec2-user@ip-172-31-45-197 downloads]$
```

Extract the Nagios Source File
tar zxvf nagios-4.4.6.tar.gz

```
[ec2-user@ip-172-31-45-197 downloads]$ tar zxvf nagios-4.4.6.tar.gz
nagios-4.4.6/
nagios-4.4.6/.gitignore
nagios-4.4.6/.travis.yml
nagios-4.4.6/CONTRIBUTING.md
nagios-4.4.6/Changelog
nagios-4.4.6/INSTALLING
nagios-4.4.6/LEGAL
nagios-4.4.6/LICENSE
nagios-4.4.6/Makefile.in
nagios-4.4.6/README.md
nagios-4.4.6/THANKS
nagios-4.4.6/UPGRADING
nagios-4.4.6/aclocal.m4
nagios-4.4.6/autoconf-macros/
nagios-4.4.6/autoconf-macros/.gitignore
nagios-4.4.6/autoconf-macros/CHANGELOG.md
nagios-4.4.6/autoconf-macros/LICENSE
nagios-4.4.6/autoconf-macros/LICENSE.md
nagios-4.4.6/autoconf-macros/README.md
nagios-4.4.6/autoconf-macros/add_group_user
nagios-4.4.6/autoconf-macros/ax_nagios_get_distrib
nagios-4.4.6/autoconf-macros/ax_nagios_get_files
nagios-4.4.6/autoconf-macros/ax_nagios_get_inetd
nagios-4.4.6/autoconf-macros/ax_nagios_get_init
```

cd nagios-4.4.6

```
[ec2-user@ip-172-31-45-197 downloads]$ cd nagios-4.4.6
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$
```

Run the Configuration Script

./configure --with-command-group=nagcmd

```
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$ ./configure --with-command-group=nagcmd
checking for a BSD-compatible install... /usr/bin/install -c
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether make sets $(MAKE)... yes
checking whether ln -s works... yes
checking for strip... /usr/bin/strip
checking how to run the C preprocessor... gcc -E
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for ANSI C header files... yes
checking whether time.h and sys/time.h may both be included... yes
checking for sys/wait.h that is POSIX.1 compatible... yes
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
```

```
*** Configuration summary for nagios 4.4.6 2020-04-28 ***:

 General Options:
 -------------------------
        Nagios executable:  nagios
        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:  /run/nagios.lock
   Check result directory:  /usr/local/nagios/var/spool/checkresults
           Init directory:  /lib/systemd/system
  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.
```

Compile the source code.

make all

```
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$ make all
cd ./base && make
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.4.6/base'
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nagios.o nagios.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE   -c -o broker.o broker.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE   -c -o nebmods.o nebmods.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o ../common/shared.o ../common/shared.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE   -c -o query-handler.o query-handler.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o workers.o workers.c
In function 'get_wproc_list',
    inlined from 'get_worker' at workers.c:277:12:
workers.c:253:17: warning: '%s' directive argument is null [-Wformat-overflow=]
  253 |                 log_debug_info(DEBUGL_CHECKS, 1, "Found specialized worker(s) for '
      |                 ^~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE   -c -o checks.o checks.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE   -c -o config.o config.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE   -c -o commands.o commands.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE   -c -o events.o events.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE   -c -o flapping.o flapping.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE   -c -o logging.o logging.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o macros-base.o ../common/macros.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE   -c -o netutils.o netutils.c
netutils.c: In function 'my_tcp_connect':
netutils.c:50:47: warning: '%d' directive output may be truncated writing between 1 and 11 b
   50 |         snprintf(port_str, sizeof(port_str), "%d", port);
```

i-0077524721c000ee1 (nagios-host)

Install binaries, init script and sample config files. Lastly, set permissions on the external command directory.

sudo make install

```
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$ sudo make install
cd ./base && make install
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.4.6/base'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/bin
/usr/bin/install -c -s -m 774 -o nagios -g nagios nagios /usr/local/nagios/bin
/usr/bin/install -c -s -m 774 -o nagios -g nagios nagiostats /usr/local/nagios/bin
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-4.4.6/base'
cd ./cgi && make install
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.4.6/cgi'
make install-basic
make[2]: Entering directory '/home/ec2-user/downloads/nagios-4.4.6/cgi'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/sbin
for file in *.cgi; do \
        /usr/bin/install -c -s -m 775 -o nagios -g nagios $file /usr/local/nagios/sbin; \
done
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-4.4.6/cgi'
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-4.4.6/cgi'
cd ./html && make install
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.4.6/html'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/media
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/stylesheets
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/contexthelp
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/docs
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/docs/images
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/js
```

sudo make install-init

```
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$ sudo make install-init
/usr/bin/install -c -m 755 -d -o root -g root /lib/systemd/system
/usr/bin/install -c -m 755 -o root -g root startup/default-service /lib/systemd/system/nagios.service
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$
```

i-0077524721c000ee1 (nagios-host)

sudo make install-config

```
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$ sudo make install-config
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc/objects
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/nagios.cfg /usr/local/nagios/etc/nagios.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/cgi.cfg /usr/local/nagios/etc/cgi.cfg
/usr/bin/install -c -b -m 660 -o nagios -g nagios sample-config/resource.cfg /usr/local/nagios/etc/resource.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/templates.cfg /usr/local/nagios/etc/objects/templates.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/commands.cfg /usr/local/nagios/etc/objects/commands.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/contacts.cfg /usr/local/nagios/etc/objects/contacts.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/timeperiods.cfg /usr/local/nagios/etc/objects/timeperiods.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/localhost.cfg /usr/local/nagios/etc/objects/localhost.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/windows.cfg /usr/local/nagios/etc/objects/windows.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/printer.cfg /usr/local/nagios/etc/objects/printer.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/switch.cfg /usr/local/nagios/etc/objects/switch.cfg

*** Config files installed ***

Remember, these are *SAMPLE* config files.  You'll need to read
```

sudo make install-commandmode

```
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$ sudo make install-commandmode
/usr/bin/install -c -m 775 -o nagios -g nagcmd -d /usr/local/nagios/var/rw
chmod g+s /usr/local/nagios/var/rw

*** External command directory configured ***

[ec2-user@ip-172-31-45-197 nagios-4.4.6]$
```

Edit the config file and change the email address.

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

```
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$ sudo nano /usr/local/nagios/etc/objects/contacts.cfg
```

Configure the web interface.

sudo make install-webconf

```
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$ sudo make install-webconf
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/httpd/conf.d/nagios.conf
if [ 0 -eq 1 ]; then \
        ln -s /etc/httpd/conf.d/nagios.conf /etc/apache2/sites-enabled/nagios.conf; \
fi

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

[ec2-user@ip-172-31-45-197 nagios-4.4.6]$
```

Create a nagiosadmin account for nagios login along with password. You'll have to specify the password twice.

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

```
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$
```

CloudShell Feedback © 2024, Amazo

Restart Apache

sudo service httpd restart

```
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$ sudo systemctl restart httpd
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$
```

CloudShell Feedback

Go back to the downloads folder and unzip the plugins zip file.

cd ~/downloads

tar zxvf nagios-plugins-2.0.3.tar.gz

```
[ec2-user@ip-172-31-45-197 nagios-4.4.6]$ cd ~/downloads
[ec2-user@ip-172-31-45-197 downloads]$ tar zxvf nagios-plugins-2.3.3.tar.gz
nagios-plugins-2.3.3/
nagios-plugins-2.3.3/perlmods/
nagios-plugins-2.3.3/perlmods/Config-Tiny-2.14.tar.gz
nagios-plugins-2.3.3/perlmods/parent-0.226.tar.gz
nagios-plugins-2.3.3/perlmods/Test-Simple-0.98.tar.gz
nagios-plugins-2.3.3/perlmods/Makefile.in
nagios-plugins-2.3.3/perlmods/version-0.9903.tar.gz
nagios-plugins-2.3.3/perlmods/Makefile.am
nagios-plugins-2.3.3/perlmods/Module-Runtime-0.013.tar.gz
nagios-plugins-2.3.3/perlmods/Module-Metadata-1.000014.tar.gz
nagios-plugins-2.3.3/perlmods/Params-Validate-1.08.tar.gz
nagios-plugins-2.3.3/perlmods/Class-Accessor-0.34.tar.gz
nagios-plugins-2.3.3/perlmods/Try-Tiny-0.18.tar.gz
nagios-plugins-2.3.3/perlmods/Module-Implementation-0.07.tar.gz
nagios-plugins-2.3.3/perlmods/Makefile
nagios-plugins-2.3.3/perlmods/Perl-OSType-1.003.tar.gz
nagios-plugins-2.3.3/perlmods/install_order
nagios-plugins-2.3.3/perlmods/Nagios-Plugin-0.36.tar.gz
nagios-plugins-2.3.3/perlmods/Math-Calc-Units-1.07.tar.gz
nagios-plugins-2.3.3/perlmods/Module-Build-0.4007.tar.gz
nagios-plugins-2.3.3/ABOUT-NLS
nagios-plugins-2.3.3/configure.ac
```

Compile and install plugins

cd nagios-plugins-2.0.3

```
[ec2-user@ip-172-31-45-197 downloads]$ cd nagios-plugins-2.3.3/
[ec2-user@ip-172-31-45-197 nagios-plugins-2.3.3]$
```

./configure --with-nagios-user=nagios --with-nagios-group=nagios

```
--enable-perl-modules: no
                  --with-cgiurl: /nagios/cgi-bin
              --with-trusted-path: /usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/
                  --enable-libtap: no
configure: creating ./config.status
config.status: creating gl/Makefile
config.status: creating nagios-plugins.spec
config.status: creating tools/build_perl_modules
config.status: creating Makefile
config.status: creating tap/Makefile
config.status: creating lib/Makefile
config.status: creating plugins/Makefile
config.status: creating lib/tests/Makefile
config.status: creating plugins-root/Makefile
config.status: creating plugins-scripts/Makefile
config.status: creating plugins-scripts/utils.pm
config.status: creating plugins-scripts/utils.sh
config.status: creating perlmods/Makefile
config.status: creating test.pl
config.status: creating pkg/solaris/pkginfo
config.status: creating po/Makefile.in
config.status: creating config.h
config.status: config.h is unchanged
config.status: executing depfiles commands
config.status: executing libtool commands
config.status: executing po-directories commands
config.status: creating po/POTFILES
config.status: creating po/Makefile
```

make

```
resolv -lpthread -ldl
gcc -DLOCALEDIR=\"/usr/local/nagios/share/locale\" -DHAVE_CONFIG_H -I. -I..  -
g -O2 -MT check_icmp.o -MD -MP -MF .deps/check_icmp.Tpo -c -o check_icmp.o che
mv -f .deps/check_icmp.Tpo .deps/check_icmp.Po
/bin/sh ../libtool --tag=CC   --mode=link gcc -DNP_VERSION='"2.3.3"' -g -O2  -
iosplug.a ../gl/libgnu.a  -lresolv -lresolv  -lpthread -ldl
libtool: link: gcc -DNP_VERSION=\"2.3.3\" -g -O2 -o check_icmp check_icmp.o ..
resolv -lpthread -ldl
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-plugins-2.3.3/plug
Making all in po
make[2]: Entering directory '/home/ec2-user/downloads/nagios-plugins-2.3.3/po'
make[2]: Nothing to be done for 'all'.
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-plugins-2.3.3/po'
make[2]: Entering directory '/home/ec2-user/downloads/nagios-plugins-2.3.3'
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-plugins-2.3.3'
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-plugins-2.3.3'
```

sudo make install

```
 chmod ug=rx,u+s /usr/local/nagios/libexec/check_icmp
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-plugins-2.3.3/plugins-root'
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-plugins-2.3.3/plugins-root'
Making install in po
make[1]: Entering directory '/home/ec2-user/downloads/nagios-plugins-2.3.3/po'
/usr/bin/mkdir -p /usr/local/nagios/share
installing fr.gmo as /usr/local/nagios/share/locale/fr/LC_MESSAGES/nagios-plugins.mo
installing de.gmo as /usr/local/nagios/share/locale/de/LC_MESSAGES/nagios-plugins.mo
if test "nagios-plugins" = "gettext-tools"; then \
  /usr/bin/mkdir -p /usr/local/nagios/share/gettext/po; \
  for file in Makefile.in.in remove-potcdate.sin    Makevars.template; do \
    /usr/bin/install -c -o nagios -g nagios -m 644 ./$file \
                  /usr/local/nagios/share/gettext/po/$file; \
  done; \
  for file in Makevars; do \
    rm -f /usr/local/nagios/share/gettext/po/$file; \
  done; \
else \
  : ; \
fi
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-plugins-2.3.3/po'
make[1]: Entering directory '/home/ec2-user/downloads/nagios-plugins-2.3.3'
make[2]: Entering directory '/home/ec2-user/downloads/nagios-plugins-2.3.3'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-plugins-2.3.3'
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-plugins-2.3.3'
```

Start Nagios

Add Nagios to the list of system services

sudo chkconfig --add nagios

```
[ec2-user@ip-172-31-45-197 nagios-plugins-2.3.3]$ sudo chkconfig --add nagios
error reading information on service nagios: No such file or directory
```

sudo chkconfig nagios on

```
[ec2-user@ip-172-31-45-197 nagios-plugins-2.3.3]$ sudo chkconfig nagios on
Note: Forwarding request to 'systemctl enable nagios.service'.
Created symlink /etc/systemd/system/multi-user.target.wants/nagios.service → /usr/lib/systemd/system/nagios.service.
```

Verify the sample configuration files

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

```
[ec2-user@ip-172-31-45-197 nagios-plugins-2.3.3]$ 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...
   Read object config files okay...

Running pre-flight check on configuration data...

Checking objects...
        Checked 8 services.
        Checked 1 hosts.
        Checked 1 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 1 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
```

If there are no errors, you can go ahead and start Nagios.

sudo service nagios start

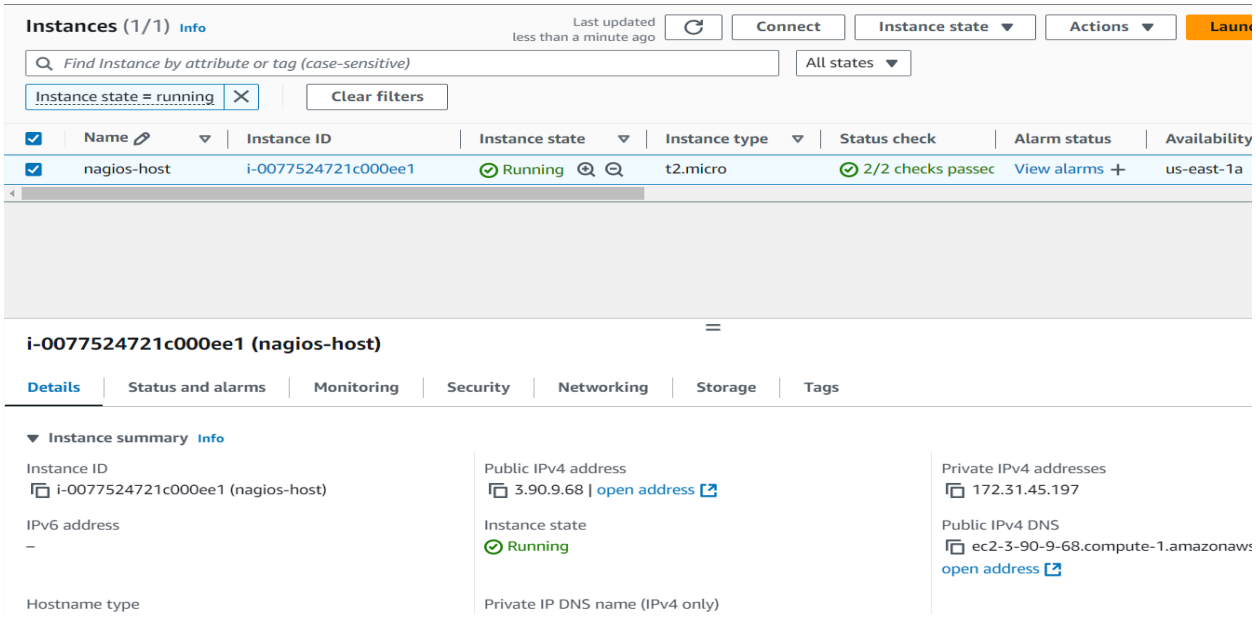
```
[ec2-user@ip-172-31-45-197 nagios-plugins-2.3.3]$ sudo systemctl start nagios
[ec2-user@ip-172-31-45-197 nagios-plugins-2.3.3]$
```

Check the status of Nagios

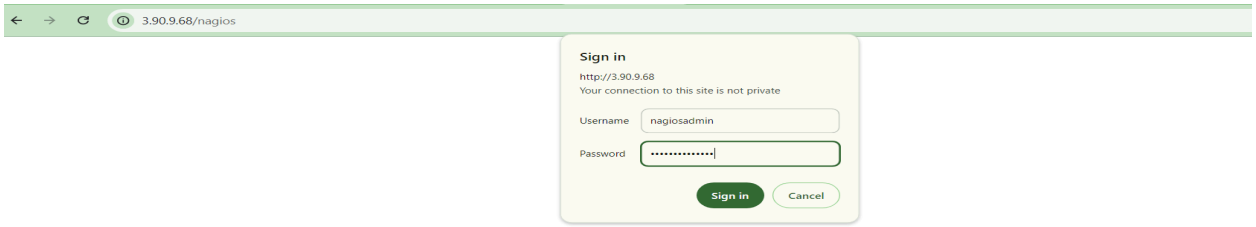
sudo systemctl status nagios

```
[ec2-user@ip-172-31-45-197 nagios-plugins-2.3.3]$ sudo systemctl status nagios
● nagios.service - Nagios Core 4.4.6
     Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
     Active: active (running) since Sun 2024-10-13 15:51:41 UTC; 18s ago
       Docs: https://www.nagios.org/documentation
    Process: 70507 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
    Process: 70508 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
   Main PID: 70509 (nagios)
      Tasks: 6 (limit: 1112)
     Memory: 2.0M
        CPU: 16ms
     CGroup: /system.slice/nagios.service
             ├─70509 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─70510 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─70511 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─70512 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─70513 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─70514 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Oct 13 15:51:41 ip-172-31-45-197.ec2.internal nagios[70509]: qh: Socket '/usr/local/nagios/var/rw/nagios.qh' successfully initialized
Oct 13 15:51:41 ip-172-31-45-197.ec2.internal nagios[70509]: qh: core query handler registered
Oct 13 15:51:41 ip-172-31-45-197.ec2.internal nagios[70509]: qh: echo service query handler registered
Oct 13 15:51:41 ip-172-31-45-197.ec2.internal nagios[70509]: qh: help for the query handler registered
Oct 13 15:51:41 ip-172-31-45-197.ec2.internal nagios[70509]: wproc: Successfully registered manager as @wproc with query handler
Oct 13 15:51:41 ip-172-31-45-197.ec2.internal nagios[70509]: wproc: Registry request: name=Core Worker 70510;pid=70510
Oct 13 15:51:41 ip-172-31-45-197.ec2.internal nagios[70509]: wproc: Registry request: name=Core Worker 70513;pid=70513
Oct 13 15:51:41 ip-172-31-45-197.ec2.internal nagios[70509]: wproc: Registry request: name=Core Worker 70512;pid=70512
Oct 13 15:51:41 ip-172-31-45-197.ec2.internal nagios[70509]: wproc: Registry request: name=Core Worker 70511;pid=70511
Oct 13 15:51:41 ip-172-31-45-197.ec2.internal nagios[70509]: Successfully launched command file worker with pid 70514
lines 1-28
```

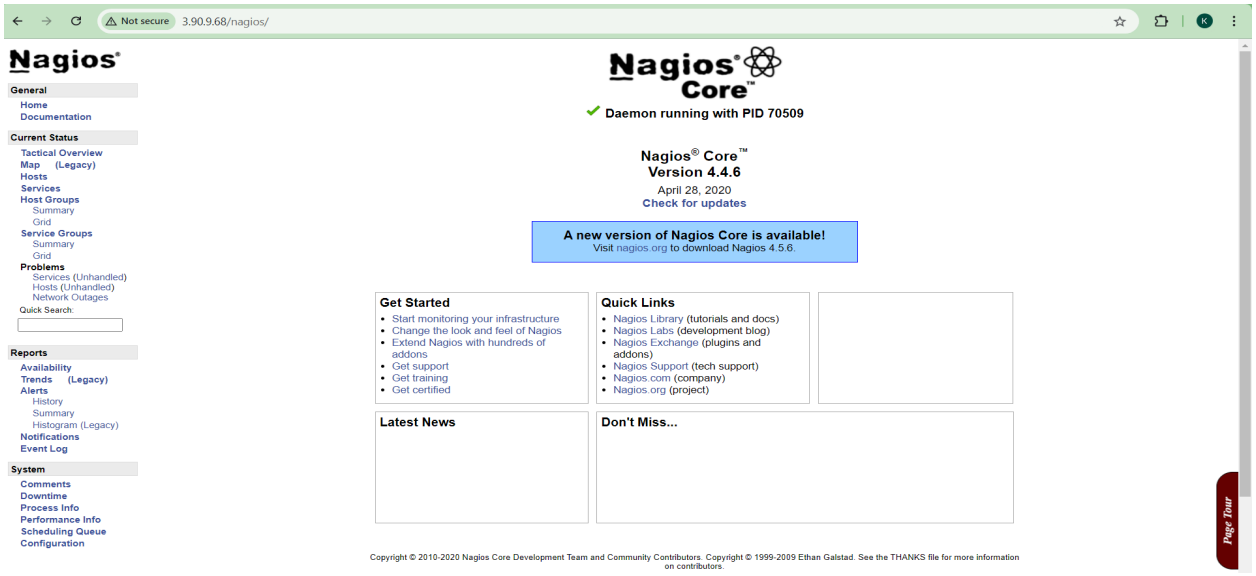
Go back to EC2 Console and copy the Public IP address of this instance



Open up your browser and look for http://<your_public_ip_address>/nagios



Enter username as nagiosadmin and password which you set
After entering the correct credentials, you will see this page.



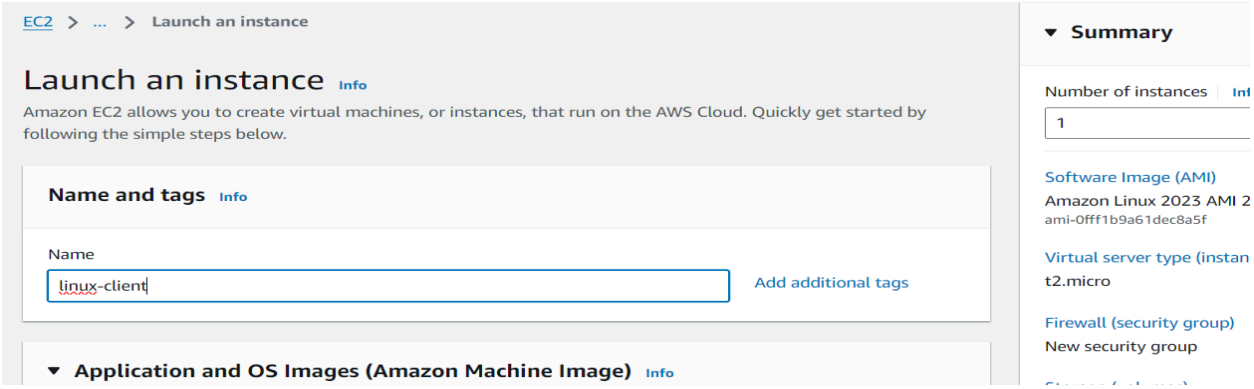
This means that Nagios was correctly installed and configured with its plugins so far.

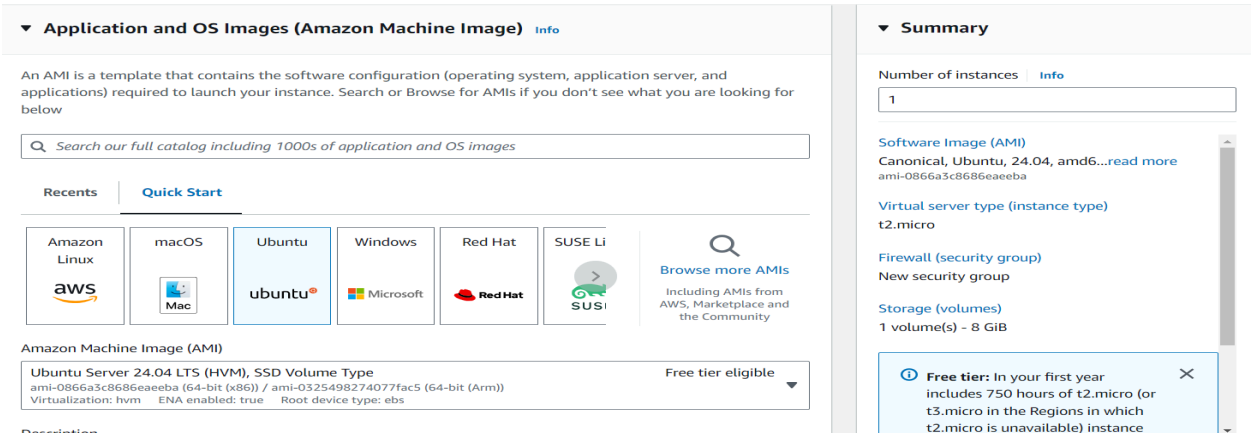
Experiment No. 10

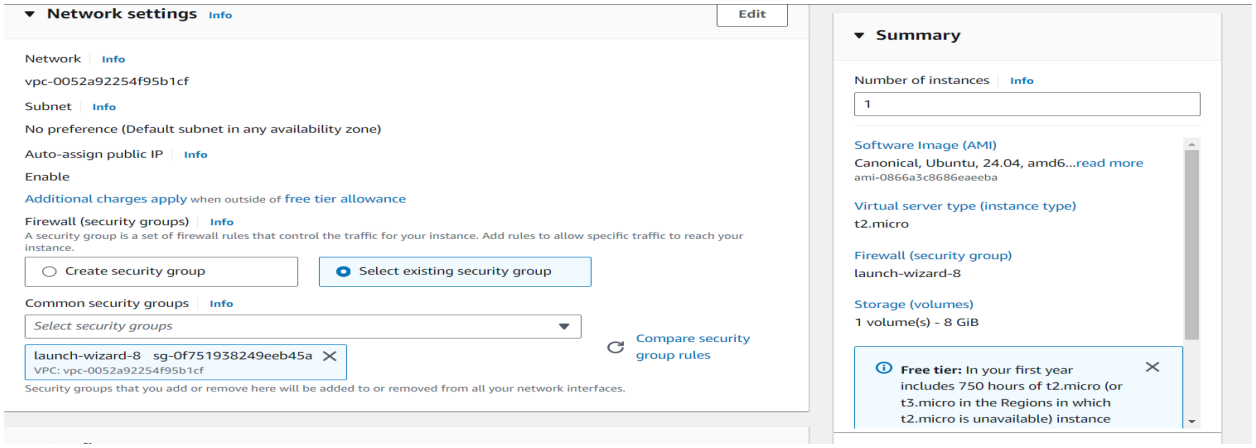
Prerequisites: AWS Free Tier, Nagios Server running on Amazon Linux Machine.
To Confirm that Nagios is running on the server side, run this sudo systemctl status nagios on the “NAGIOS HOST”.

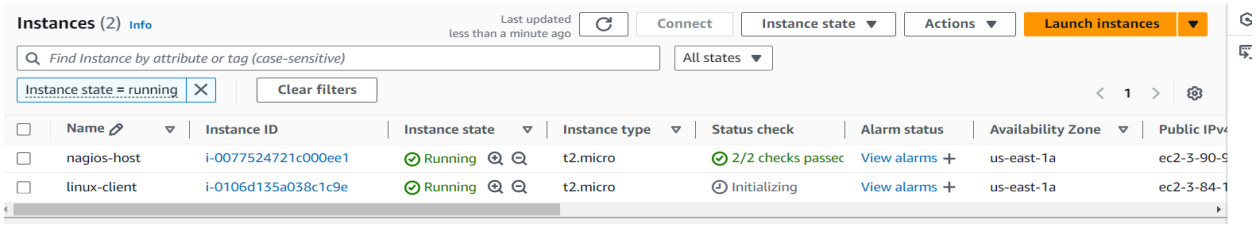
```
[ec2-user@ip-172-31-45-197 nagios-plugins-2.3.3]$ sudo systemctl status nagios
● nagios.service - Nagios Core 4.4.6
     Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
     Active: active (running) since Sun 2024-10-13 15:51:41 UTC; 11min ago
       Docs: https://www.nagios.org/documentation
    Process: 70507 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited,
    Process: 70508 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, sta
   Main PID: 70509 (nagios)
      Tasks: 6 (limit: 1112)
     Memory: 3.1M
        CPU: 174ms
     CGroup: /system.slice/nagios.service
             ├─70509 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─70510 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─70511 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─70512 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─70513 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─70514 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Oct 13 15:56:33 ip-172-31-45-197.ec2.internal nagios[70509]: SERVICE ALERT: localhost;HTTP;WARNING;HARD;4;HTTP
Oct 13 15:57:03 ip-172-31-45-197.ec2.internal nagios[70509]: SERVICE ALERT: localhost;Swap Usage;CRITICAL;SOFT;
Oct 13 15:58:03 ip-172-31-45-197.ec2.internal nagios[70509]: SERVICE ALERT: localhost;Swap Usage;CRITICAL;SOFT;
Oct 13 15:59:03 ip-172-31-45-197.ec2.internal nagios[70509]: SERVICE NOTIFICATION: nagiosadmin;localhost;Swap U
Oct 13 15:59:03 ip-172-31-45-197.ec2.internal nagios[70509]: SERVICE ALERT: localhost;Swap Usage;CRITICAL;HARD;
Oct 13 15:59:03 ip-172-31-45-197.ec2.internal nagios[70509]: wproc: NOTIFY job 4 from worker Core Worker 70511
Oct 13 15:59:03 ip-172-31-45-197.ec2.internal nagios[70509]: wproc:   host=localhost; service=Swap Usage; conta
Oct 13 15:59:03 ip-172-31-45-197.ec2.internal nagios[70509]: wproc:   early_timeout=0; exited_ok=1; wait_status
Oct 13 15:59:03 ip-172-31-45-197.ec2.internal nagios[70509]: wproc:   stderr line 01: /bin/sh: line 1: /bin/mai
Oct 13 15:59:03 ip-172-31-45-197.ec2.internal nagios[70509]: wproc:   stderr line 02: /usr/bin/printf: write er
lines 1-28
```

You can proceed if you get this message.
Before we begin,
To monitor a Linux machine, create an Ubuntu 20.04 server EC2 Instance in AWS. Provide it with the same security group as the Nagios Host and name it ‘linux-client’ alongside the host.









For now, leave this machine as is, and go back to your nagios HOST machine.

On the server, run this command

ps -ef | grep nagios

```
[ec2-user@ip-172-31-45-197 ~]$ ps -ef | grep nagios
nagios     70509       1  0 15:51 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios     70510   70509  0 15:51 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     70511   70509  0 15:51 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     70512   70509  0 15:51 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     70513   70509  0 15:51 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     70514   70509  0 15:51 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
ec2-user   72416   72322  0 16:18 pts/0    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-45-197 ~]$
```

Become a root user and create 2 folders

sudo su

mkdir /usr/local/nagios/etc/objects/monitorhosts

mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts

```
[ec2-user@ip-172-31-45-197 ~]$ sudo su
[root@ip-172-31-45-197 ec2-user]# mkdir /usr/local/nagios/etc/objects/monitorhosts
[root@ip-172-31-45-197 ec2-user]# mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
[root@ip-172-31-45-197 ec2-user]#
```

i-0077524721c000ee1 (nagios-host)

PublicIPs: 3.90.9.68 PrivateIPs: 172.31.45.197

Copy the sample localhost.cfg file to linuxhost folder

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

```
[root@ip-172-31-45-197 ec2-user]# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
[root@ip-172-31-45-197 ec2-user]#
```

Open linuxserver.cfg using nano and make the following changes

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

Change the hostname to linuxserver (EVERYWHERE ON THE FILE)

Change address to the public IP address of your LINUX CLIENT.

```
[root@ip-172-31-45-197 ec2-user]# nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
```

```
  GNU nano 5.8                                  /usr/local/nagios/etc/objects/monitorhosts/linux
##############################################################################
# LOCALHOST.CFG - SAMPLE OBJECT CONFIG FILE FOR MONITORING THIS MACHINE
#
#
# NOTE: This config file is intended to serve as an *extremely* simple
#       example of how you can create configuration entries to monitor
#       the local (Linux) machine.
#
##############################################################################



##############################################################################
#
# HOST DEFINITION
#
##############################################################################
```

```
##############################################################################
#
# HOST DEFINITION
#
##############################################################################

# Define a host for the local machine

define host {

    use                     linux-server            ; Name of host template to use
                                                    ; This host definition will inherit all variables that are defined
                                                    ; in (or inherited by) the linux-server host template definition.
    host_name               linuxserver
    alias                   linuxserver
    address                 3.84.142.31
}
```

```
##############################################################################
#
# SERVICE DEFINITIONS
#
##############################################################################

# Define a service to "ping" the local machine

define service {

    use                     local-service           ; Name of service template to use
    host_name               linuxserver
    service_description     PING
    check_command           check_ping!100.0,20%!500.0,60%
}
```

```
# Define a service to check the disk space of the root partition
# on the local machine.  Warning if < 20% free, critical if
# < 10% free space on partition.

define service {

    use                     local-service           ; Name of service template to use
    host_name               linuxserver
    service_description     Root Partition
    check_command           check_local_disk!20%!10%!/
}



# Define a service to check the number of currently logged in
# users on the local machine.  Warning if > 20 users, critical
# if > 50 users.

define service {

    use                     local-service           ; Name of service template to use
    host_name               linuxserver
    service_description     Current Users
    check_command           check_local_users!20!50
}
```

```
# Define a service to check the number of currently running procs
# on the local machine.  Warning if > 250 processes, critical if
# > 400 processes.

define service {

    use                     local-service           ; Name of service template to use
    host_name               linuxserver
    service_description     Total Processes
    check_command           check_local_procs!250!400!RSZDT
}



# Define a service to check the load on the local machine.

define service {

    use                     local-service           ; Name of service template to use
    host_name               linuxserver
    service_description     Current Load
    check_command           check_local_load!5.0,4.0,3.0!10.0,6.0,4.0
}
```

```
  GNU nano 5.8                          /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linux
# Define a service to check the swap usage the local machine.
# Critical if less than 10% of swap is free, warning if less than 20% is free

define service {

    use                     local-service           ; Name of service template to use
    host_name               linuxserver
    service_description     Swap Usage
    check_command           check_local_swap!20%!10%
}



# Define a service to check SSH on the local machine.
# Disable notifications for this service by default, as not all users may have SSH enabled.

define service {

    use                     local-service           ; Name of service template to use
    host_name               linuxserver
    service_description     SSH
    check_command           check_ssh
    notifications_enabled   0
}
```

```
# Define a service to check HTTP on the local machine.
# Disable notifications for this service by default, as not all users may have HTTP enabled.

define service {

    use                     local-service           ; Name of service template to use
    host_name               linuxserver
    service_description     HTTP
    check_command           check_http
    notifications_enabled   0
}
```

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

# Define an optional hostgroup for Linux machines

define hostgroup {

    hostgroup_name          linux-servers1          ; The name of the hostgroup
    alias                   Linux Servers           ; Long name of the group
    members                 localhost               ; Comma separated list of hosts that belong to this group
}
```

Change hostgroup_name under hostgroup to linux-servers1

```
  GNU nano 5.8                          /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
###############################################################################
#
# HOST GROUP DEFINITION
#
###############################################################################

# Define an optional hostgroup for Linux machines

define hostgroup {

    hostgroup_name          linux-servers1          ; The name of the hostgroup
    alias                   Linux Servers           ; Long name of the group
    members                 linuxserver             ; Comma separated list of hosts that belong to this group
}
```

Everywhere else on the file, change the hostname to linuxserver instead of localhost.

Open the Nagios Config file and add the following line

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

```
[root@ip-172-31-45-197 ec2-user]# nano /usr/local/nagios/etc/nagios.cfg
```

##Add this line

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

```
  GNU nano 5.8                                                          /usr/
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# Definitions for monitoring a Windows machine
#cfg_file=/usr/local/nagios/etc/objects/windows.cfg

# Definitions for monitoring a router/switch
#cfg_file=/usr/local/nagios/etc/objects/switch.cfg

# Definitions for monitoring a network printer
#cfg_file=/usr/local/nagios/etc/objects/printer.cfg


# You can also tell Nagios to process all config files (with a .cfg
# extension) in a particular directory by using the cfg_dir
# directive as shown below:

#cfg_dir=/usr/local/nagios/etc/servers
#cfg_dir=/usr/local/nagios/etc/printers
#cfg_dir=/usr/local/nagios/etc/switches
#cfg_dir=/usr/local/nagios/etc/routers
cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/
```

Verify the configuration files

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

```
[root@ip-172-31-45-197 ec2-user]# sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

```
[root@ip-172-31-45-197 ec2-user]# 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...
   Read object config files okay...

Running pre-flight check on configuration data...

Checking objects...
        Checked 16 services.
        Checked 2 hosts.
        Checked 2 host groups.
        Checked 0 service groups.
        Checked 1 contacts.
        Checked 1 contact groups.
        Checked 24 commands.
        Checked 5 time periods.
        Checked 0 host escalations.
        Checked 0 service escalations.
```

```
Checking for circular paths...
        Checked 2 hosts
        Checked 0 service dependencies
        Checked 0 host dependencies
        Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

You are good to go if there are no errors.

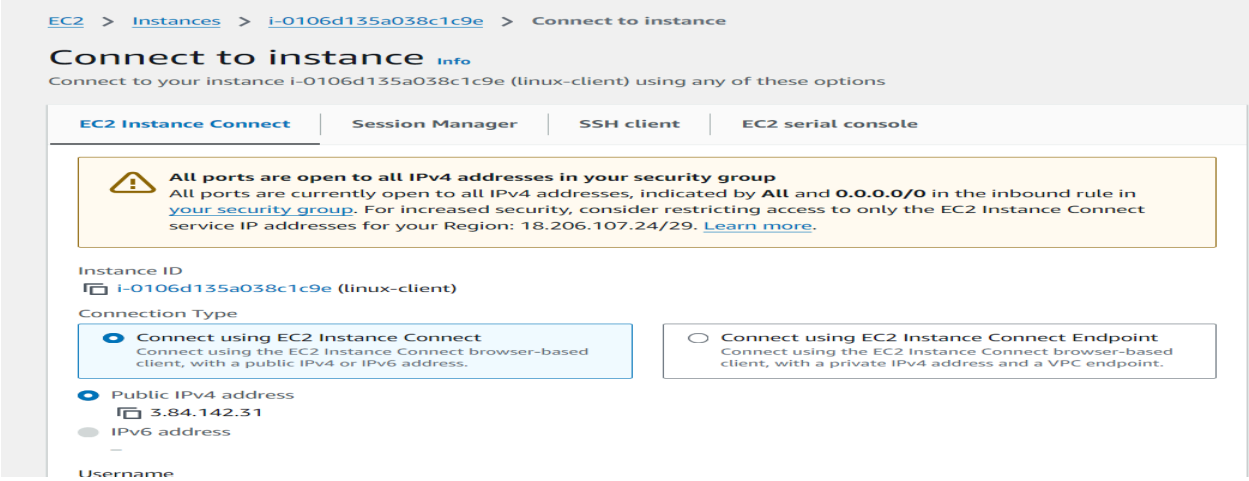
Restart the nagios service

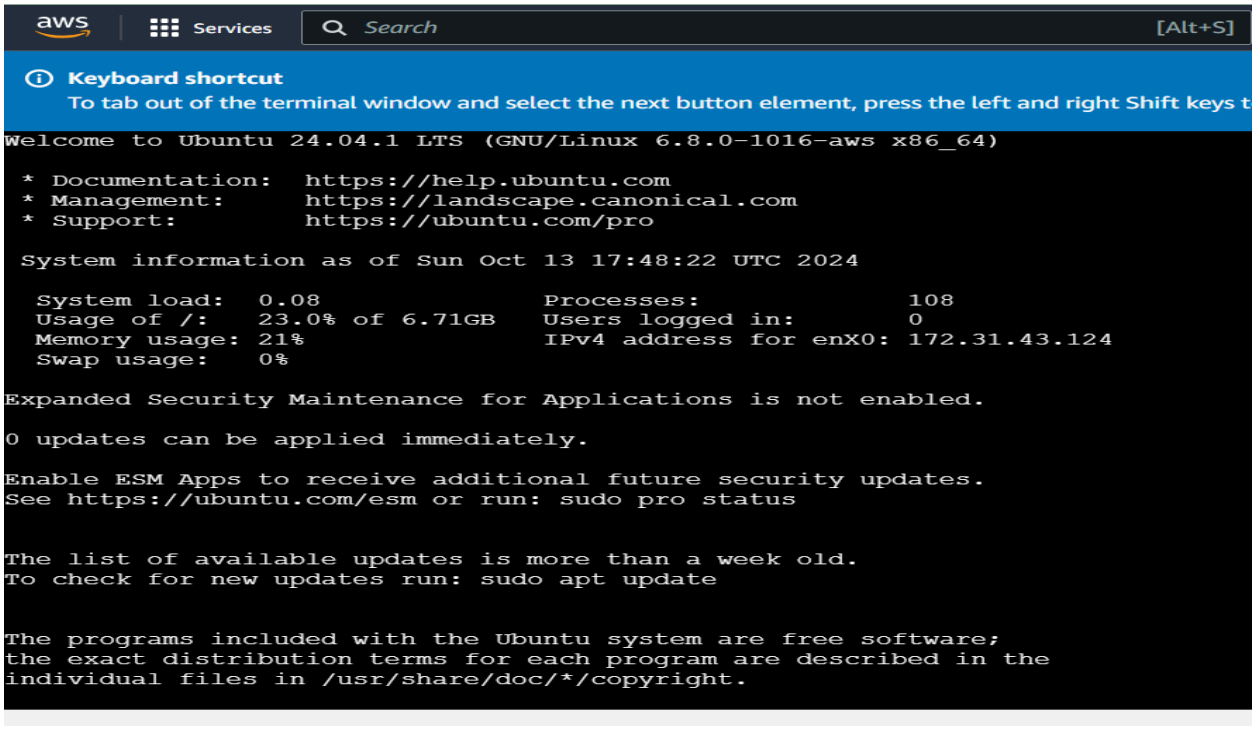
service nagios restart

```
[root@ip-172-31-45-197 ec2-user]# service nagios restart
Redirecting to /bin/systemctl restart nagios.service
[root@ip-172-31-45-197 ec2-user]#
```

Now it is time to switch to the client machine.

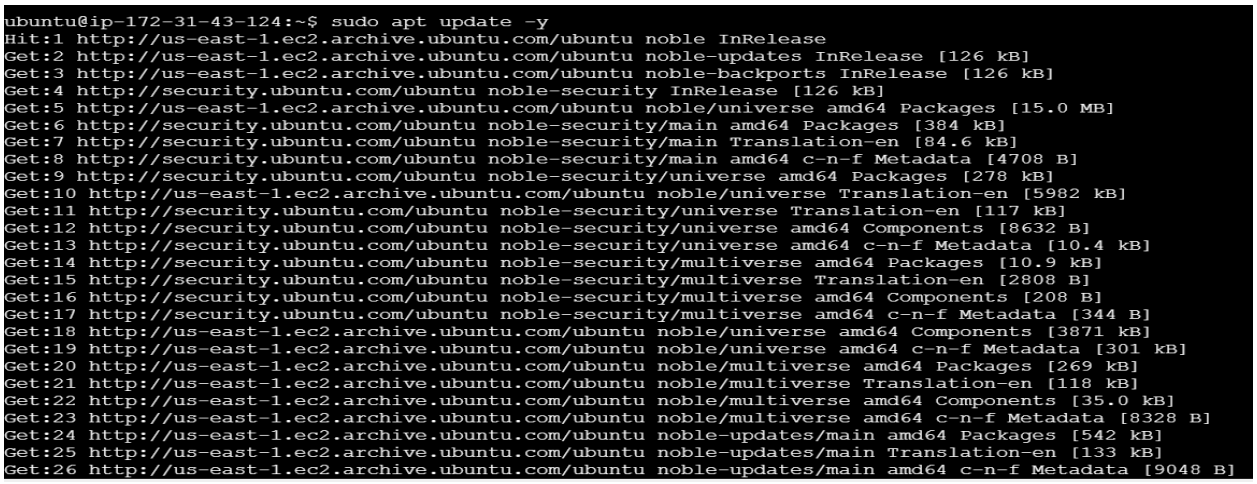
SSH into the machine or simply use the EC2 Instance Connect feature.

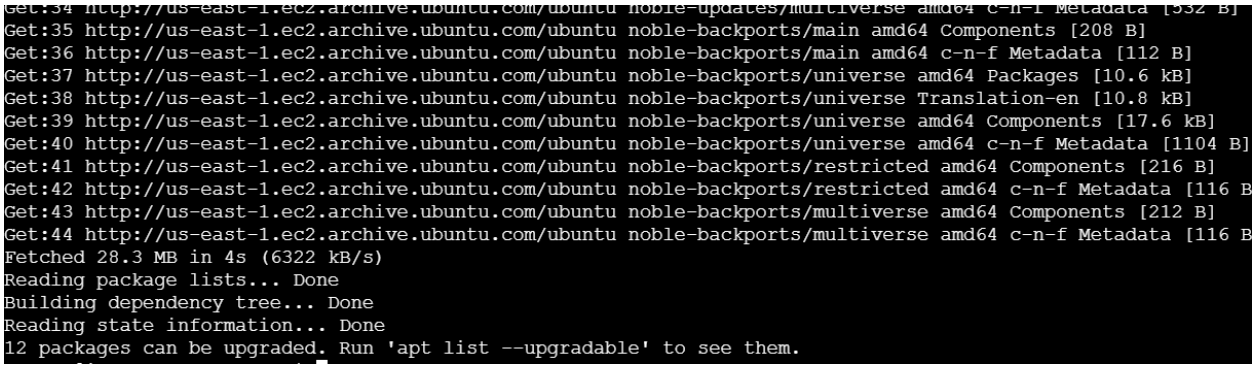




Make a package index update and install gcc, nagios-nrpe-server and the plugins.

sudo apt update -y





sudo apt install gcc -y

```
ubuntu@ip-172-31-43-124:~$ sudo apt install gcc -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu cpp cpp-13 cpp-13-x86-64-linux-gnu cpp-x86-64-linu
  fonts-dejavu-mono gcc-13 gcc-13-base gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu libaom3 libasan8 li
  libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libde265-0 libdeflate0 libfontconfig1 libgcc-13
  libheif-plugin-aomenc libheif-plugin-libde265 libheif1 libhwasan0 libis123 libitm1 libjbig0 libjpeg-t
  libsframe1 libsharpyuv0 libtiff6 libtsan2 libubsan1 libwebp7 libxpm4 linux-libc-dev manpages-dev rpcs
Suggested packages:
  binutils-doc gprofng-gui cpp-doc gcc-13-locales cpp-13-doc gcc-multilib make autoconf automake libtoo
  gdb-x86-64-linux-gnu glibc-doc libgd-tools libheif-plugin-x265 libheif-plugin-ffmpegdec libheif-plugi
  libheif-plugin-j2kenc libheif-plugin-rav1e libheif-plugin-svtenc
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu cpp cpp-13 cpp-13-x86-64-linux-gnu cpp-x86-64-linu
  fonts-dejavu-mono gcc gcc-13 gcc-13-base gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu libaom3 libasan
  libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libde265-0 libdeflate0 libfontconfig1 libgcc-13
  libheif-plugin-aomenc libheif-plugin-libde265 libheif1 libhwasan0 libis123 libitm1 libjbig0 libjpeg-t
  libsframe1 libsharpyuv0 libtiff6 libtsan2 libubsan1 libwebp7 libxpm4 linux-libc-dev manpages-dev rpcs
0 upgraded, 57 newly installed, 0 to remove and 12 not upgraded.
Need to get 62.8 MB of archives.
After this operation, 222 MB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 binutils-common amd64 2.42-4ubunt
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libsframe1 amd64 2.42-4ubuntu2 [1
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libbinutils amd64 2.42-4ubuntu2 [
Processing triggers for sgml-base (1.31) ...
Setting up libfontconfig1:amd64 (2.15.0-1.1ubuntu2) ...
Setting up libgd3:amd64 (2.3.3-9ubuntu5) ...
Setting up libc-devtools (2.39-0ubuntu8.3) ...
Processing triggers for libc-bin (2.39-0ubuntu8.3) ...
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.
```

sudo apt install -y nagios-nrpe-server nagios-plugins

```
ubuntu@ip-172-31-43-124:~$ sudo apt install -y nagios-nrpe-server nagios-plugins
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'monitoring-plugins' instead of 'nagios-plugins'
The following additional packages will be installed:
  libavahi-client3 libavahi-common-data libavahi-common3 libcups2t64 libdbi1t64 libldb2 libmysqlclient21 libnet-snmp-perl libpq5 libradc
  libsnmp-base libsnmp40t64 libtalloc2 libtdb1 libtevent0t64 liburiparser1 libwbclient0 monitoring-plugins-basic monitoring-plugins-comm
  monitoring-plugins-standard mysql-common python3-gpg python3-ldb python3-markdown python3-samba python3-talloc python3-tdb rpcbind sam
  samba-common-bin samba-dsdb-modules samba-libs smbclient snmp
Suggested packages:
  cups-common libcrypt-des-perl libdigest-hmac-perl libio-socket-inet6-perl snmp-mibs-downloader icinga2 nagios-plugins-contrib fping po
  | exim4-daemon-heavy | exim4-daemon-light qstat xinetd | inetd python-markdown-doc heimdal-clients python3-dnspython cifs-utils
The following NEW packages will be installed:
  libavahi-client3 libavahi-common-data libavahi-common3 libcups2t64 libdbi1t64 libldb2 libmysqlclient21 libnet-snmp-perl libpq5 libradc
  libsnmp-base libsnmp40t64 libtalloc2 libtdb1 libtevent0t64 liburiparser1 libwbclient0 monitoring-plugins monitoring-plugins-basic moni
  monitoring-plugins-standard mysql-common nagios-nrpe-server python3-gpg python3-ldb python3-markdown python3-samba python3-talloc pyth
  samba-common samba-common-bin samba-dsdb-modules samba-libs smbclient snmp
0 upgraded, 37 newly installed, 0 to remove and 12 not upgraded.
Need to get 16.1 MB of archives.
After this operation, 72.0 MB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 nagios-nrpe-server amd64 4.1.0-1ubuntu3 [356 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 rpcbind amd64 1.2.6-7ubuntu2 [46.5 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libavahi-common-data amd64 0.8-13ubuntu6 [29.7 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libavahi-common3 amd64 0.8-13ubuntu6 [23.3 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libavahi-client3 amd64 0.8-13ubuntu6 [26.8 kB]
```

Open nrpe.cfg file to make changes.

sudo nano /etc/nagios/nrpe.cfg

Under allowed_hosts, add your nagios host IP address like so

```
ubuntu@ip-172-31-43-124:~$ sudo nano /etc/nagios/nrpe.cfg
```

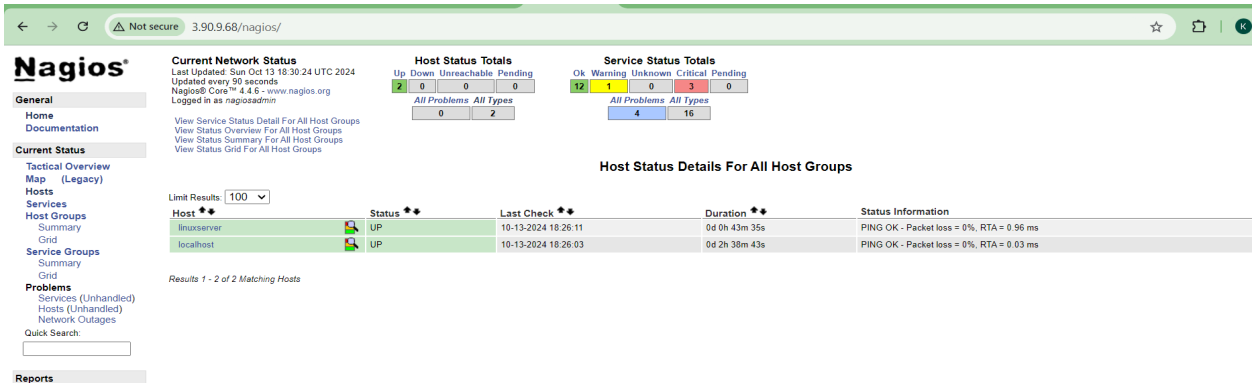
```
  GNU nano 7.2                                                /etc/nagios/nrpe.cfg *
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd

nrpe_group=nagios



# ALLOWED HOST ADDRESSES
# This is an optional comma-delimited list of IP address or hostnames
# that are allowed to talk to the NRPE daemon. Network addresses with a bit mask
# (i.e. 192.168.1.0/24) are also supported. Hostname wildcards are not currently
# supported.
#
# 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=127.0.0.1,3.90.9.68
```

Restart the NRPE server

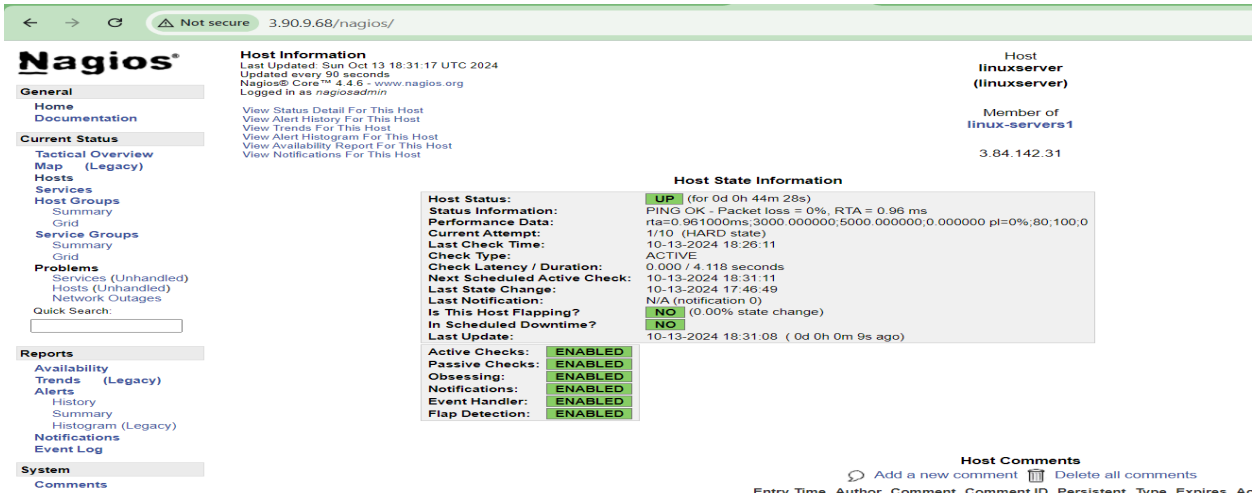
sudo systemctl restart nagios-nrpe-server

```
ubuntu@ip-172-31-43-124:~$ sudo systemctl restart nagios-nrpe-server
ubuntu@ip-172-31-43-124:~$
```

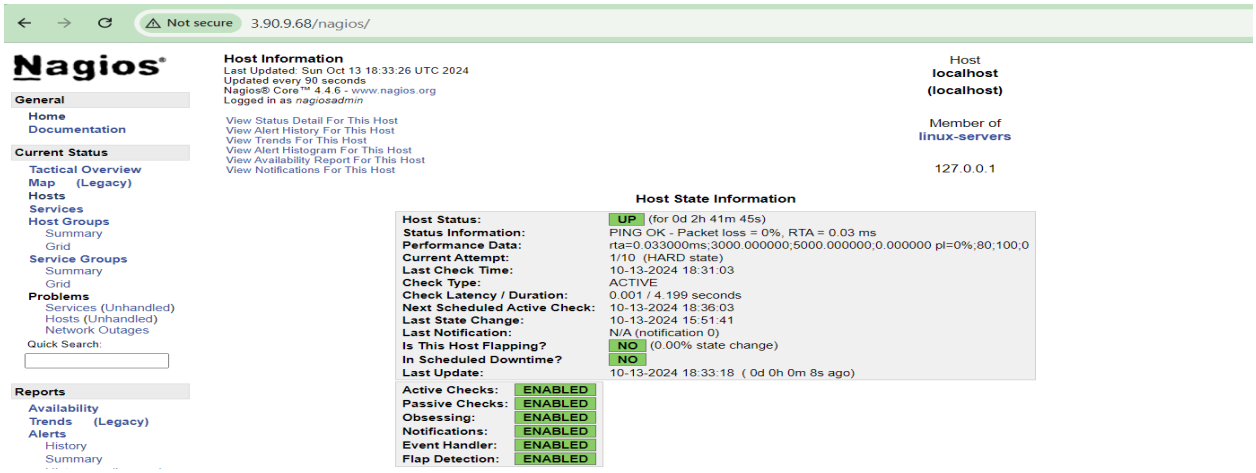
Now, check your nagios dashboard and you'll see a new host being added.
Click on Hosts.



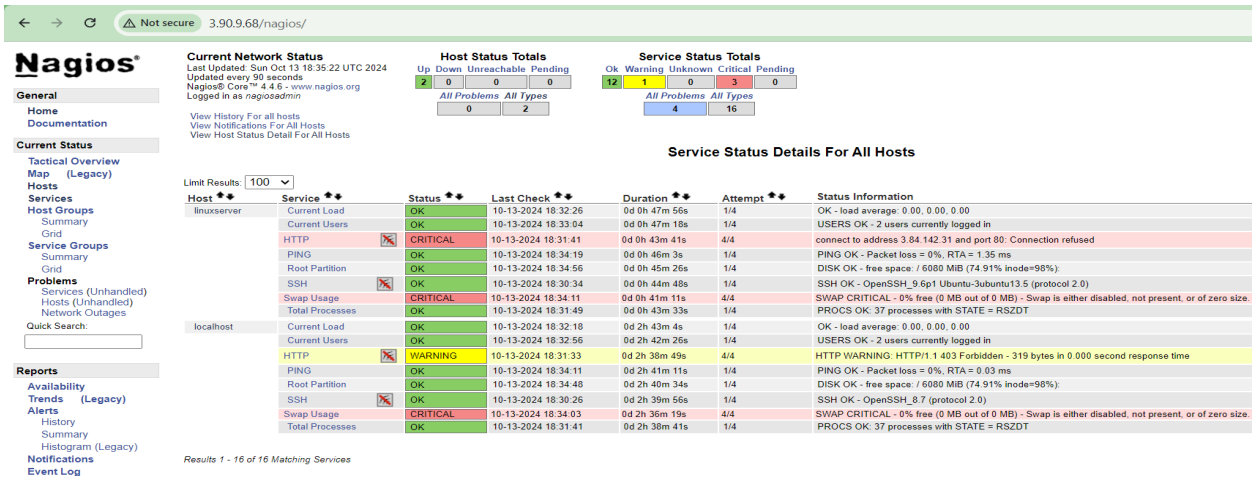
Click on linuxserver to see the host details



Click on localhost to see the host details

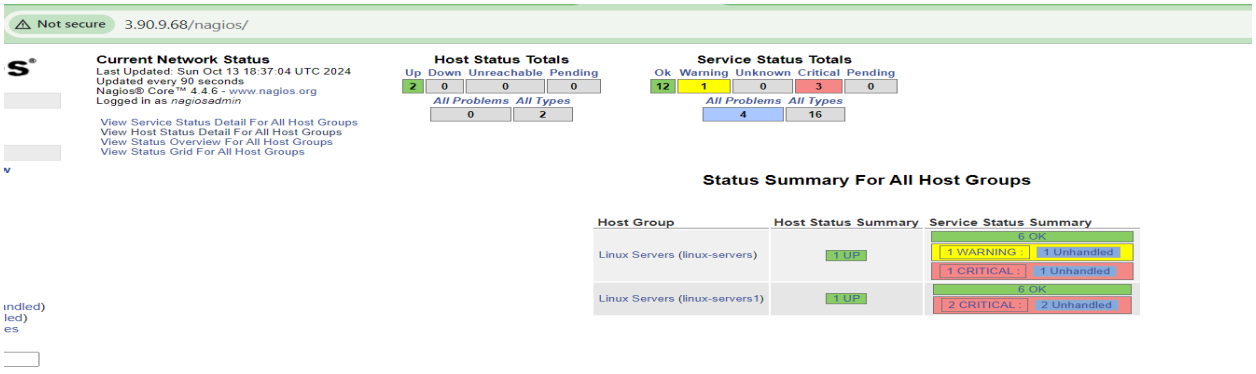


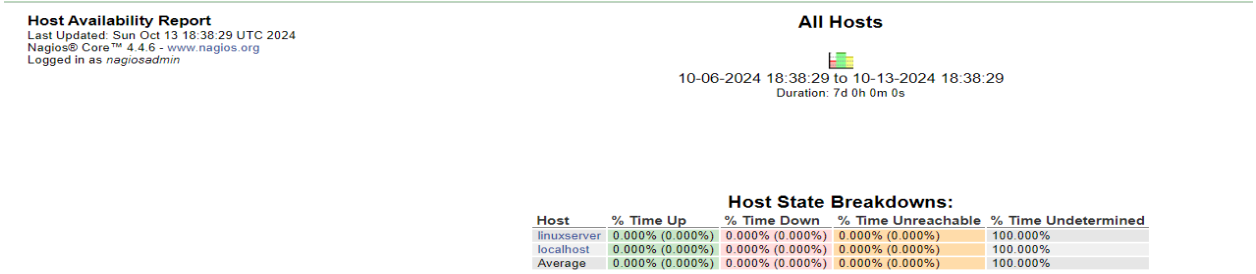
You can click Services to see all services and ports being monitored.

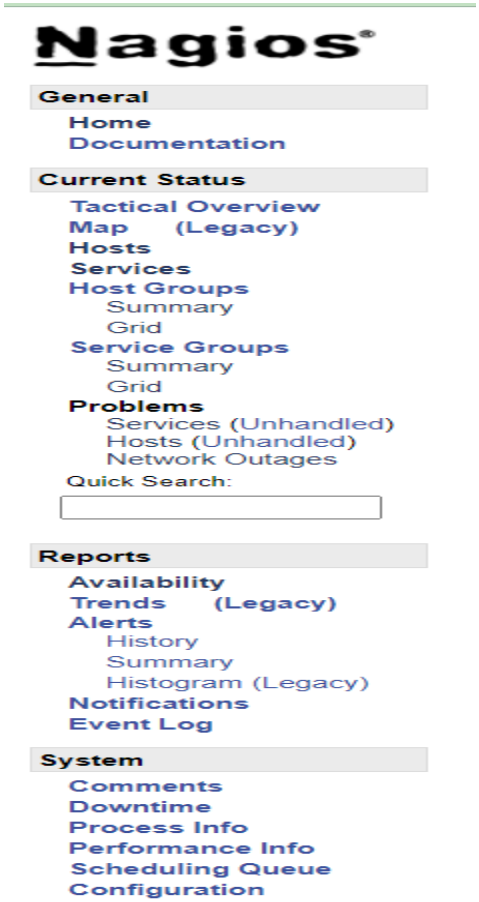


As you can see, we have our linuxserver up and running. It is showing critical status on HTTP due to permission errors and swap because there is no partition created.
In this case, we have monitored -
Servers: 1 linux server
Services: swap
Ports: 22, 80 (ssh, http)
Processes: User status, Current load, total processes, root partition, etc.

summary

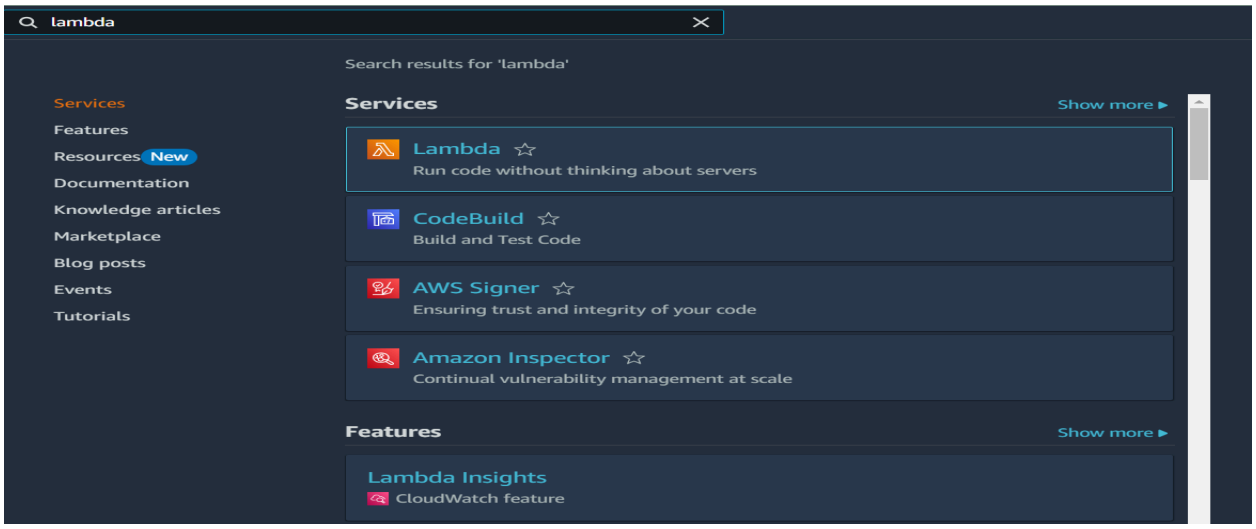

Not secure
3.90.9.68/nagios/
Current Network Status
Last Updated: Sun Oct 13 18:37:04 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.4.6 - www.nagios.org
Logged in as nagiosadmin
View Service Status Detail For All Host Groups
View Host Status Detail For All Host Groups
View Status Overview For All 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
12 1 0 3 0
All Problems All Types
4 16
Status Summary For All Host Groups
Host Group
Host Status Summary
Service Status Summary
Linux Servers (linux-servers)
1 UP
6 OK
1 WARNING : 1 Unhandled
1 CRITICAL : 1 Unhandled
Linux Servers (linux-servers1)
1 UP
6 OK
2 CRITICAL : 2 Unhandled


Host Availability Report
Last Updated: Sun Oct 13 18:38:29 UTC 2024
Nagios® Core™ 4.4.6 - www.nagios.org
Logged in as nagiosadmin
All Hosts
10-06-2024 18:38:29 to 10-13-2024 18:38:29
Duration: 7d 0h 0m 0s
Host State Breakdowns:
Host
% Time Up
% Time Down
% Time Unreachable
% Time Undetermined
linuxserver 0.000% (0.000%) 0.000% (0.000%) 0.000% (0.000%) 100.000%
localhost 0.000% (0.000%) 0.000% (0.000%) 0.000% (0.000%) 100.000%
Average 0.000% (0.000%) 0.000% (0.000%) 0.000% (0.000%) 100.000%

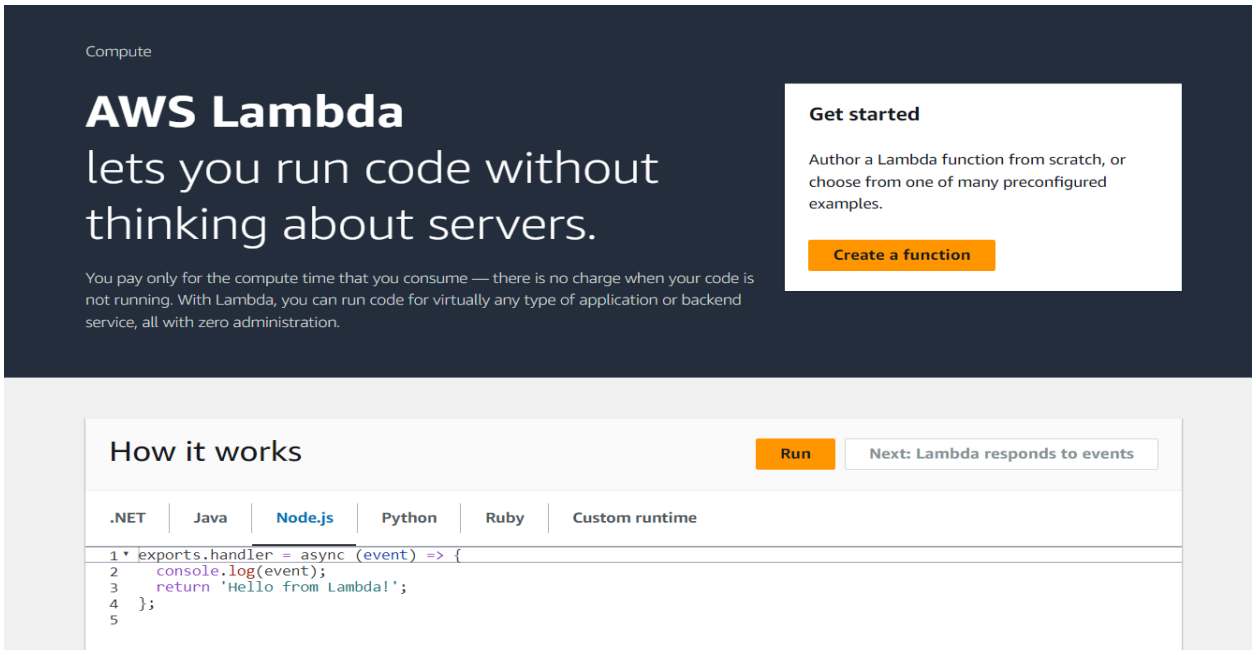

Nagios
General
Home
Documentation
Current Status
Tactical Overview
Map (Legacy)
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services (Unhandled)
Hosts (Unhandled)
Network Outages
Quick Search:
Reports
Availability
Trends (Legacy)
Alerts
History
Summary
Histogram (Legacy)
Notifications
Event Log
System
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Configuration

Experiment No. 11

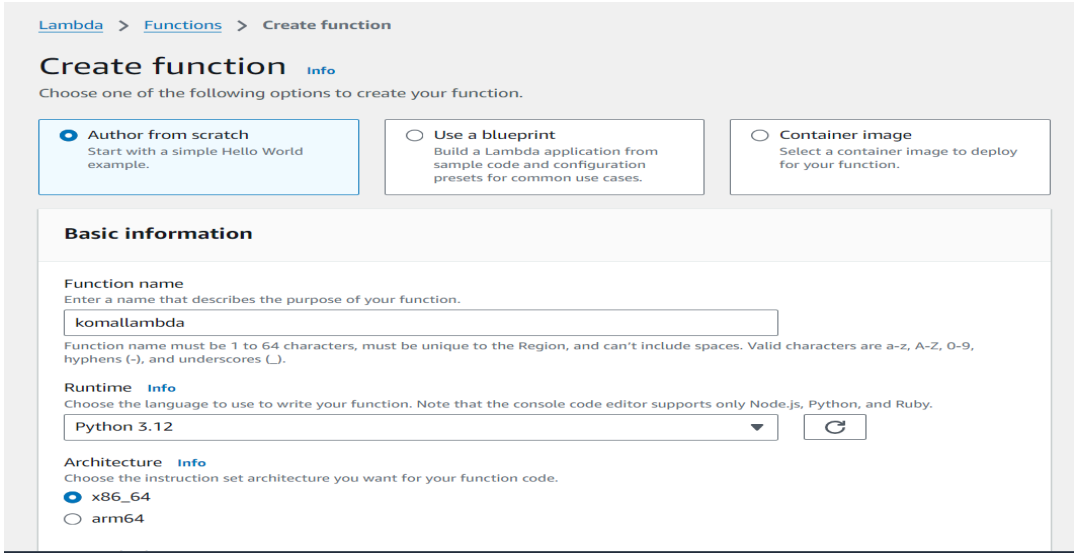
Open Lambda to create an AWS Lambda function

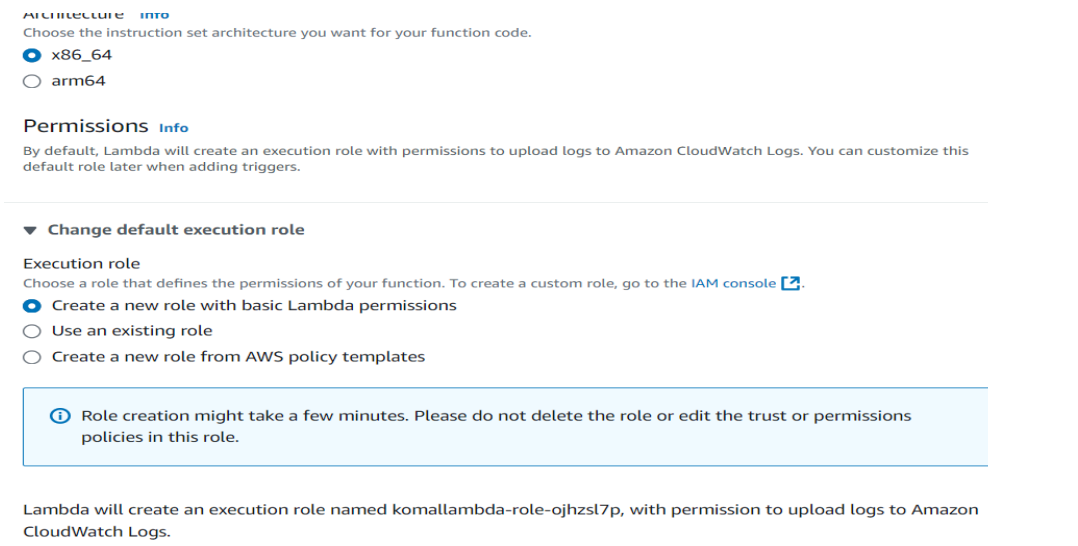


Open up the Lambda Console and click on the Create button.

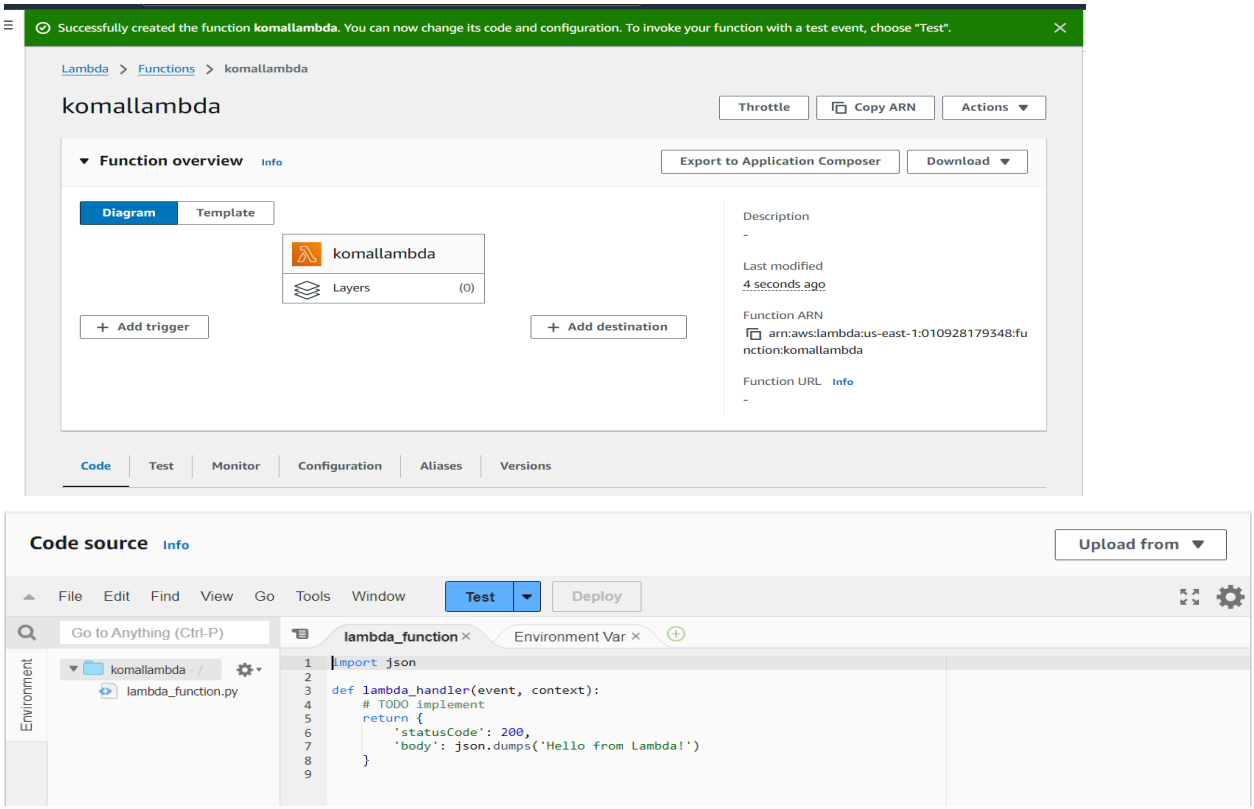


Choose to create a function from scratch or use a blueprint, i.e templates defined by AWS for you with all configuration presets required for the most common use cases. Then, choose a runtime env for your function, under the dropdown, you can see all the options AWS supports, Python, Nodejs, .NET and 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.

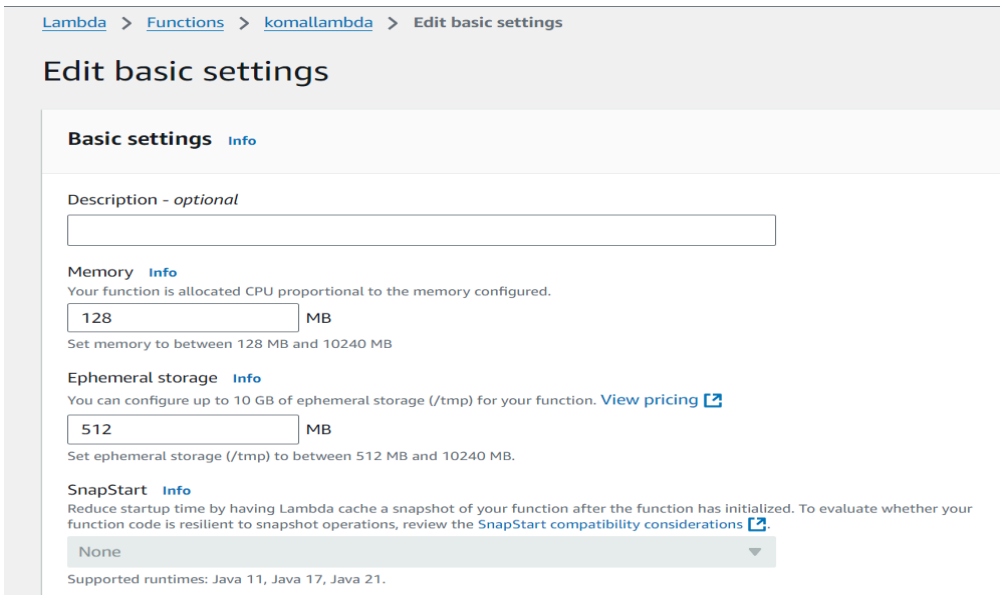


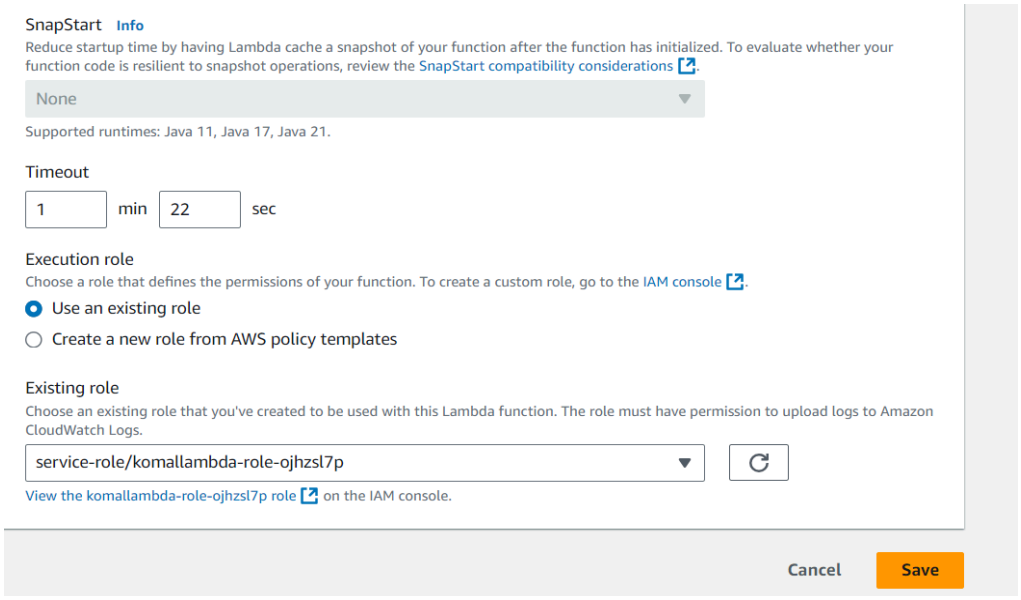


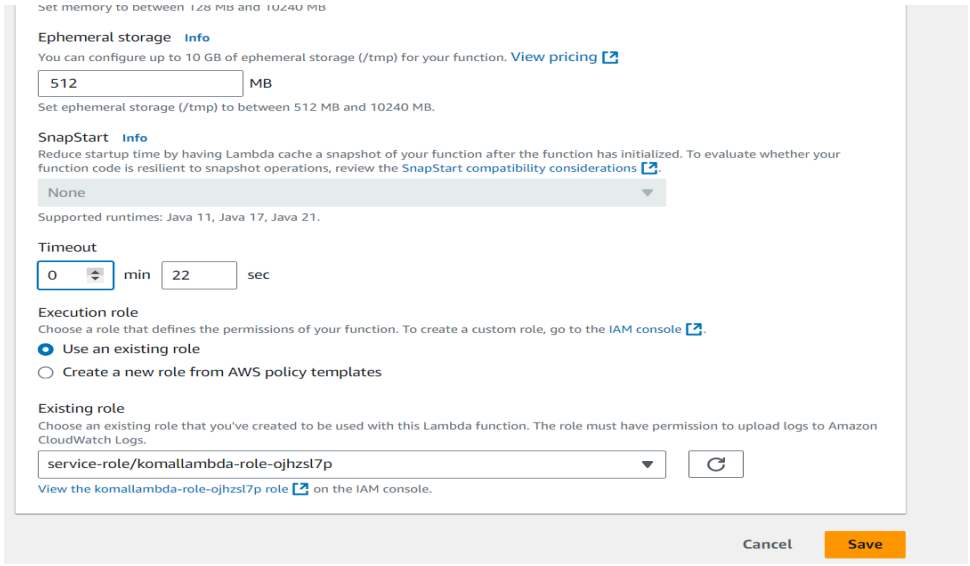
Function is successfully created



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 22 sec since that is sufficient for now.

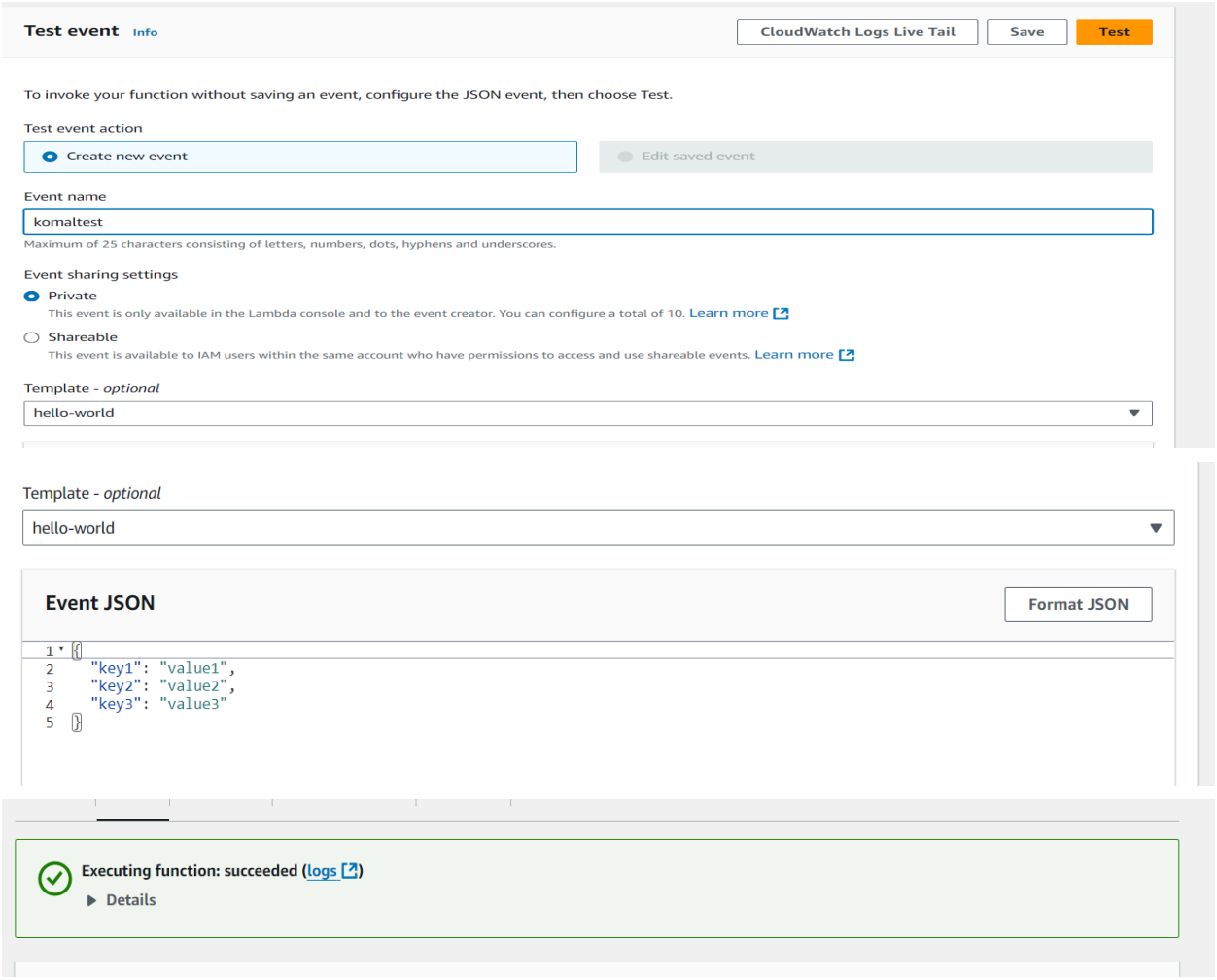




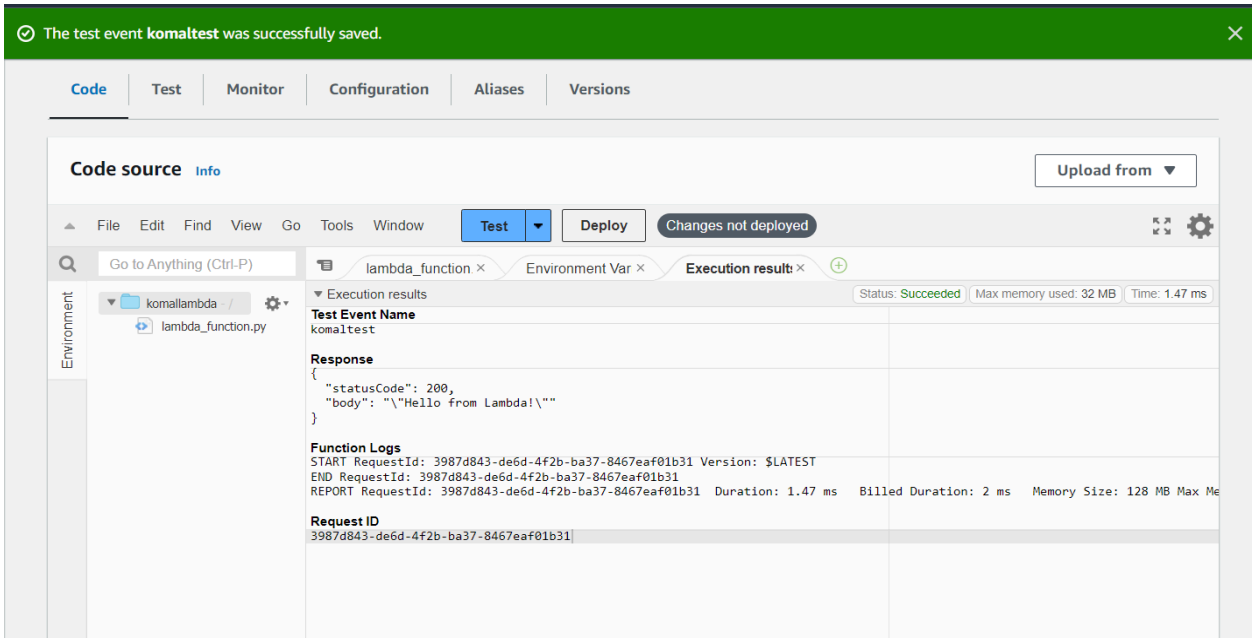


You can make changes to your function inside the code editor. You can also upload a zip file of your function or upload one from an S3 bucket if needed. Press Ctrl + S to save the file and click Deploy to deploy the changes.

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.

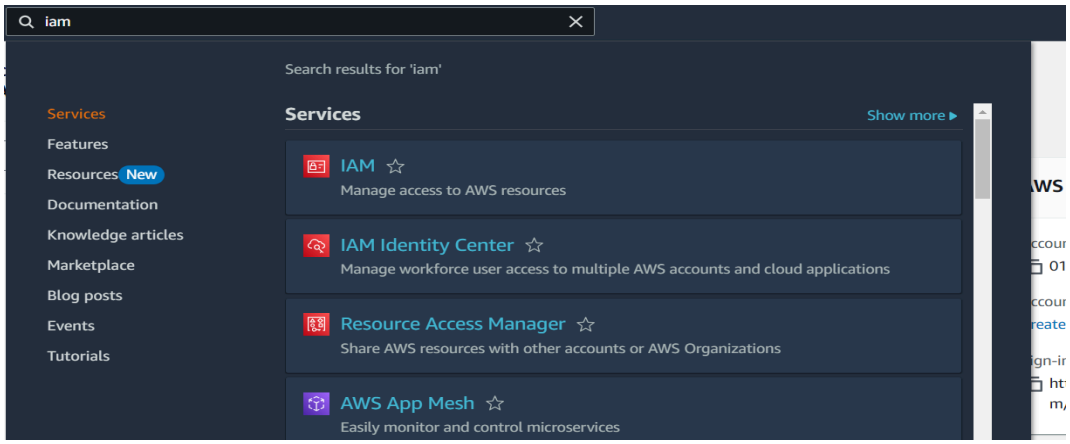


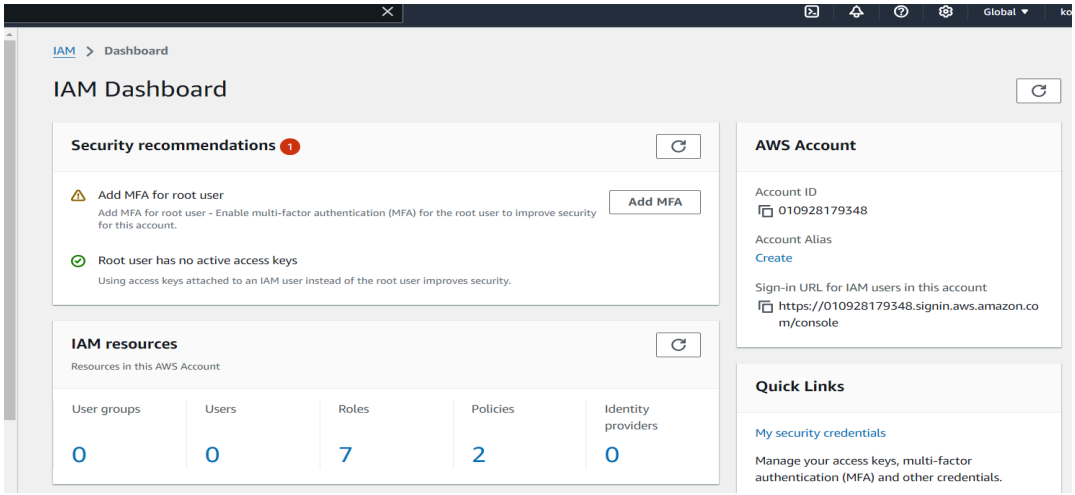
Click on Test arrow and select your event and then test and you should be able to see the results


The test event komaltest was successfully saved.
Code
Test
Monitor
Configuration
Aliases
Versions
Code source Info
Upload from
File Edit Find View Go Tools Window
Test
Deploy
Changes not deployed
Go to Anything (Ctrl-P)
lambda_function
Environment Var
Execution result
Environment
komallambda
lambda_function.py
Execution results
Status: Succeeded
Max memory used: 32 MB
Time: 1.47 ms
Test Event Name
komaltest
Response
{
"statusCode": 200,
"body": "\"Hello from Lambda!\""
}
Function Logs
START RequestId: 3987d843-de6d-4f2b-ba37-8467eaf01b31 Version: $LATEST
END RequestId: 3987d843-de6d-4f2b-ba37-8467eaf01b31
REPORT RequestId: 3987d843-de6d-4f2b-ba37-8467eaf01b31 Duration: 1.47 ms Billed Duration: 2 ms Memory Size: 128 MB Max Me
Request ID
3987d843-de6d-4f2b-ba37-8467eaf01b31

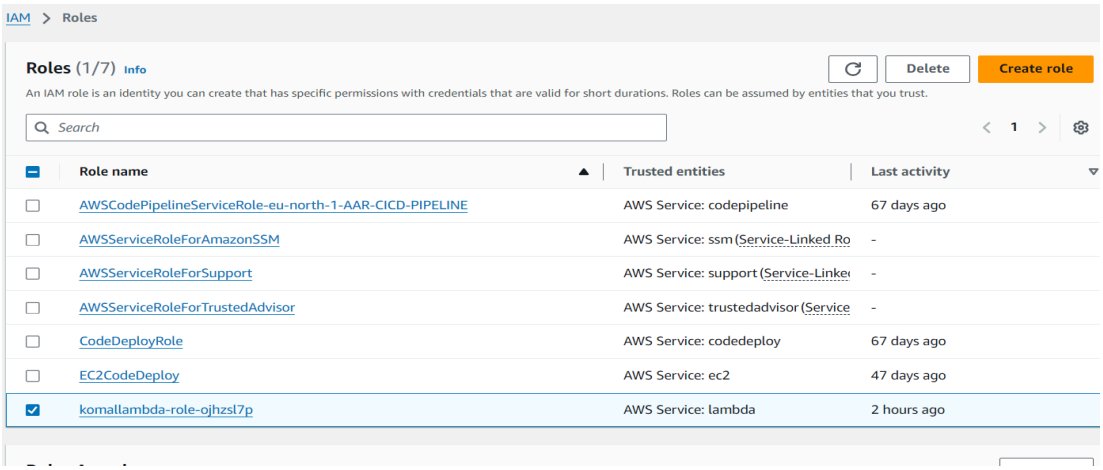
Experiment No. 12

Select an IAM services

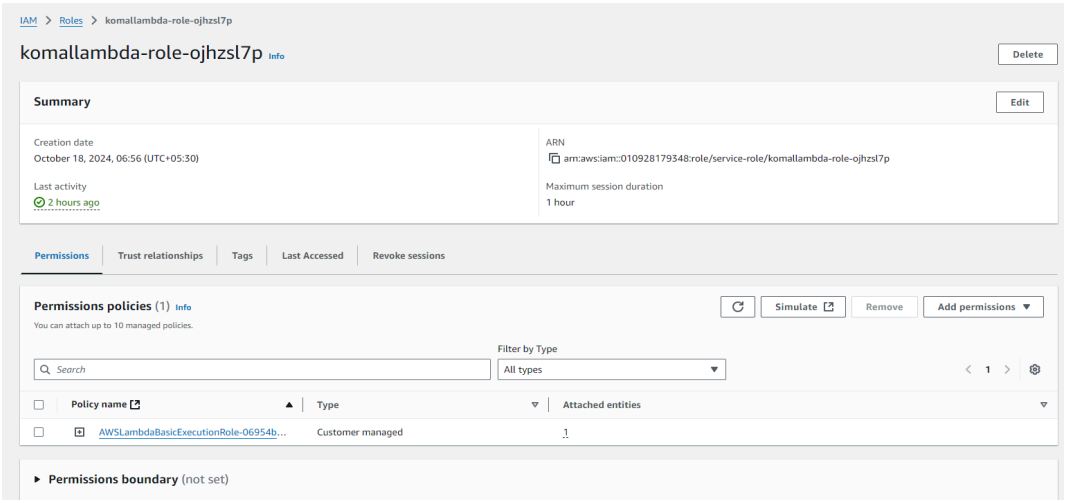




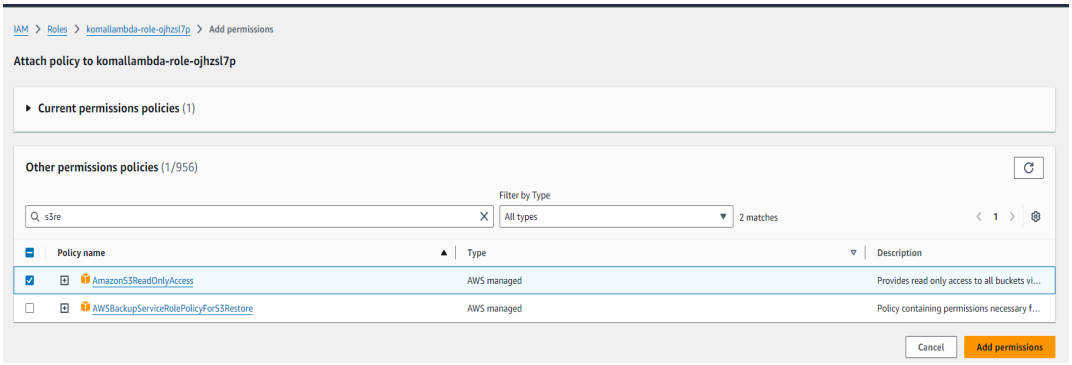
Open up the IAM Console and under Roles, choose the Role we previously created for the Python Lambda Function (You can find your role name configuration of your Lambda function).



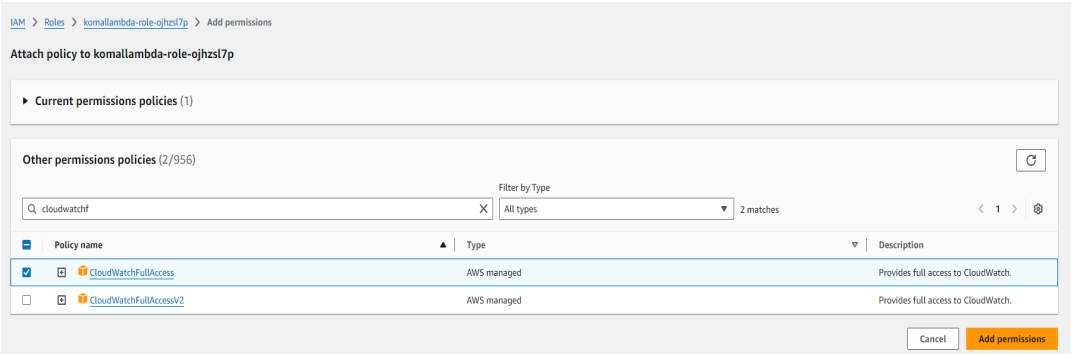
Under Add permissions select Attach Policies, add S3-ReadOnly and CloudWatchFull permissions to this role.



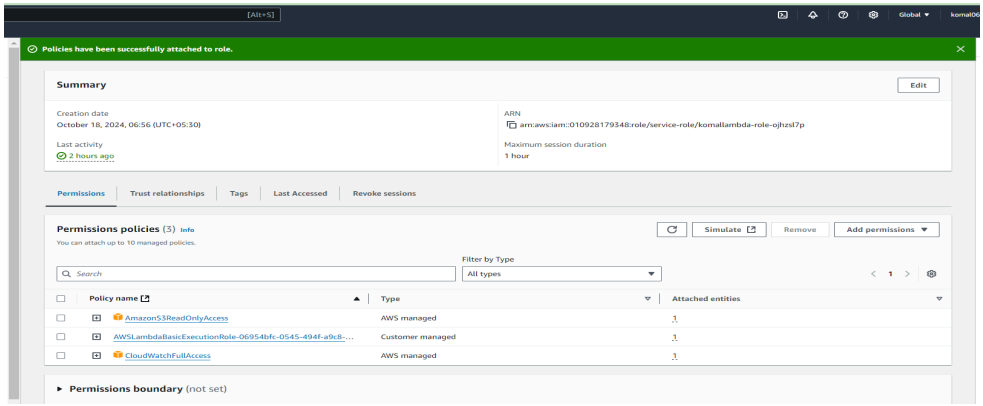
S3-ReadOnly



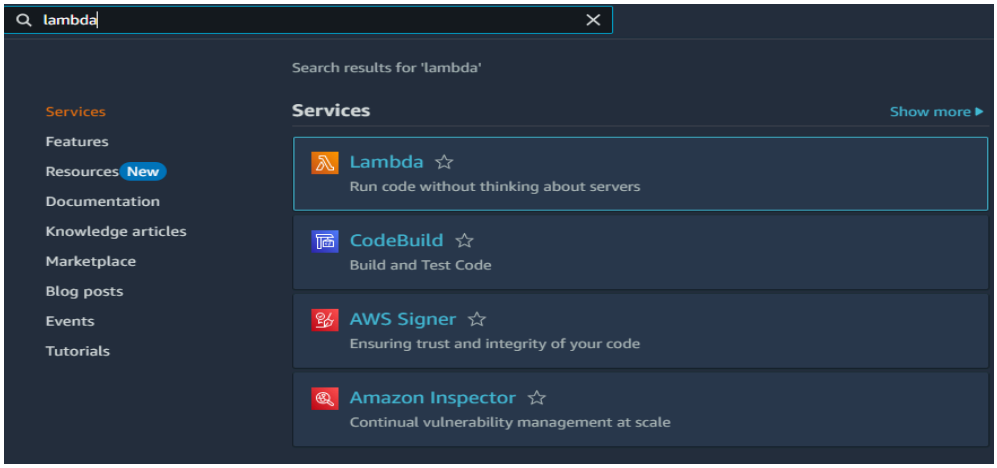
CloudWatchFull

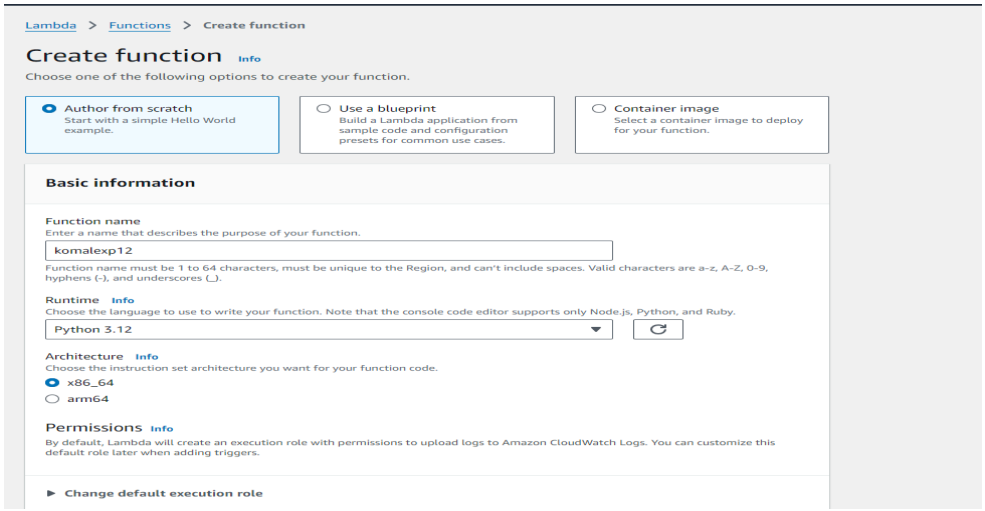


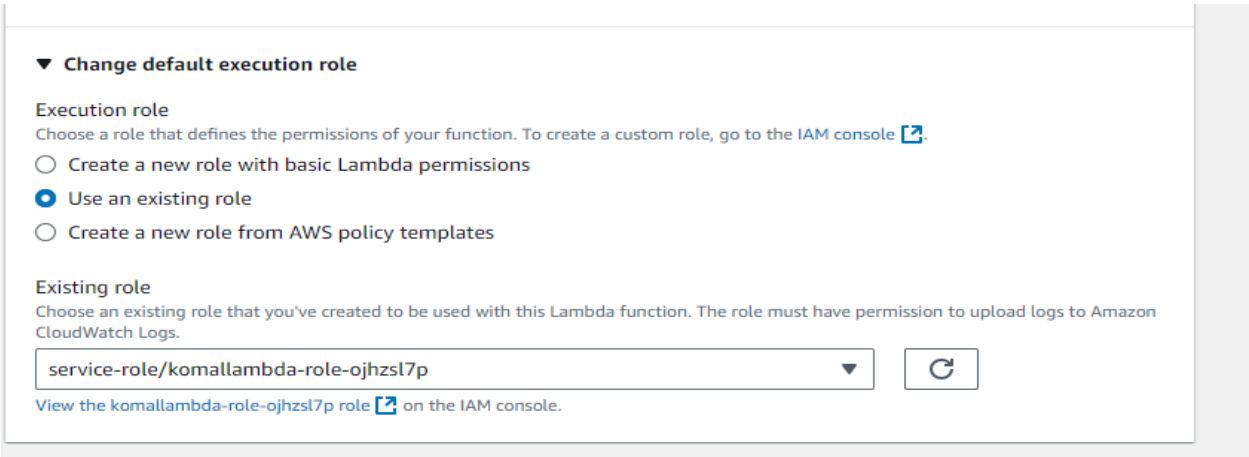
After successful attachment of policy you will see something like this you will be able to see the updated policies.



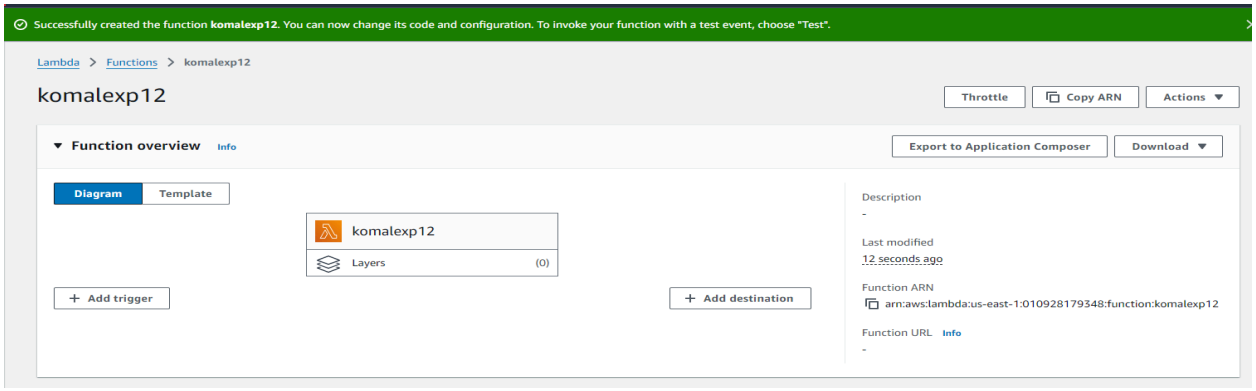
Open up AWS Lambda and create a new Python function. Under Execution Role, choose the existing role, then select the one which was previously created and to which we just added permissions.



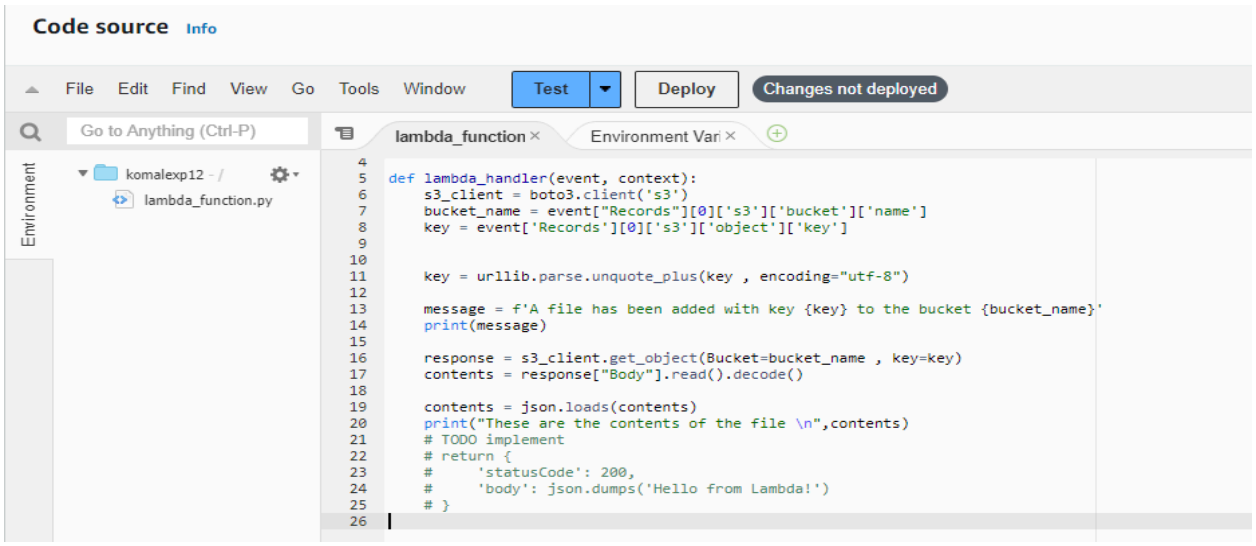




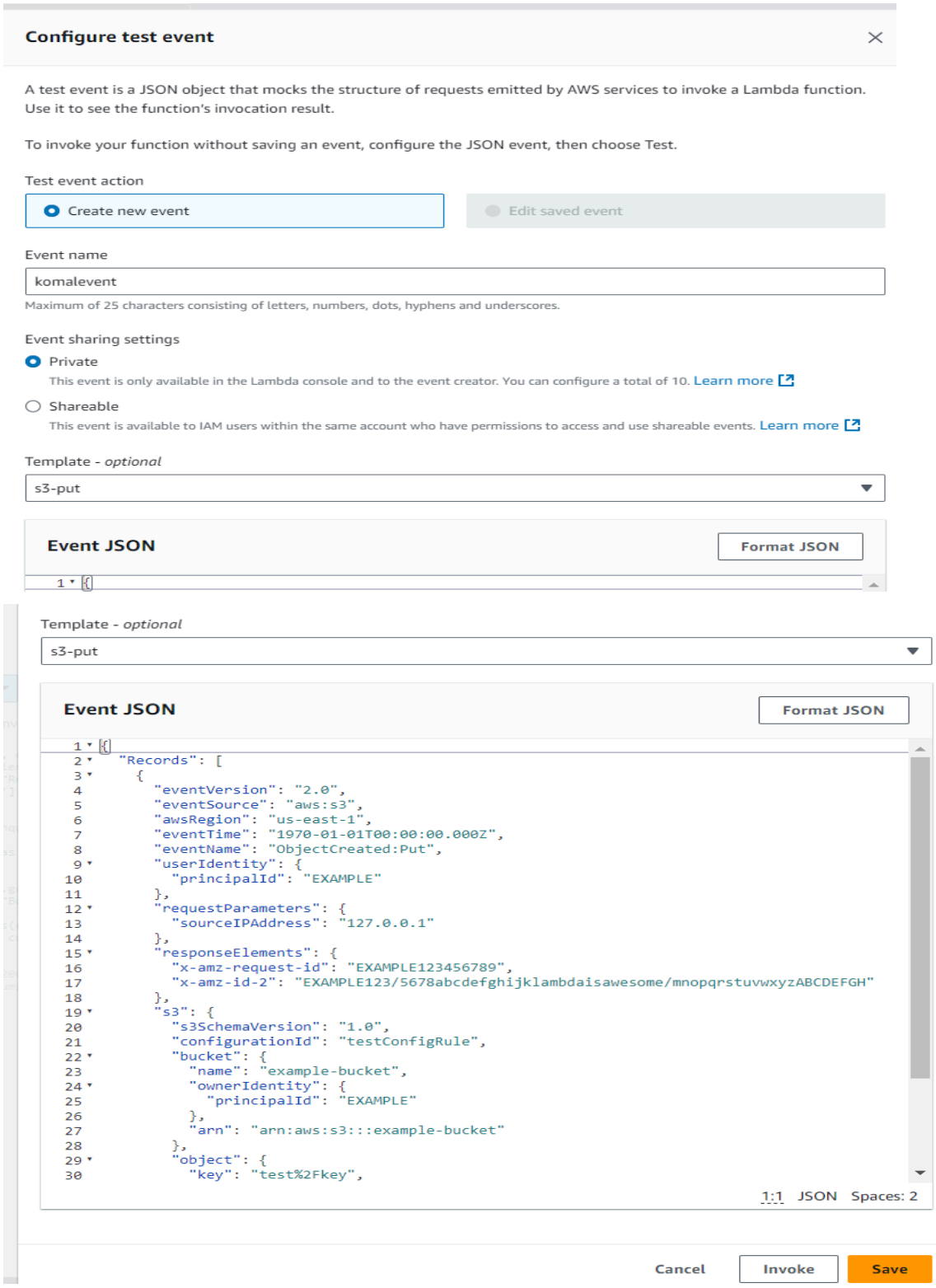
The function is now successfully created and running

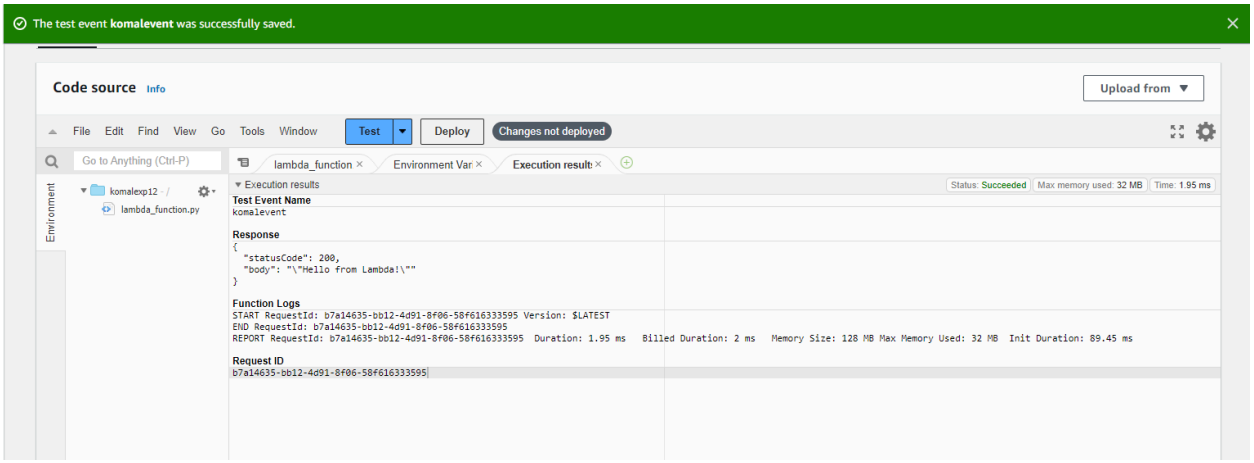


Make the following changes to the function and click on the deploy button. This code basically logs a message and logs the contents of a JSON file which is uploaded to an S3 Bucket and then deploy the code.

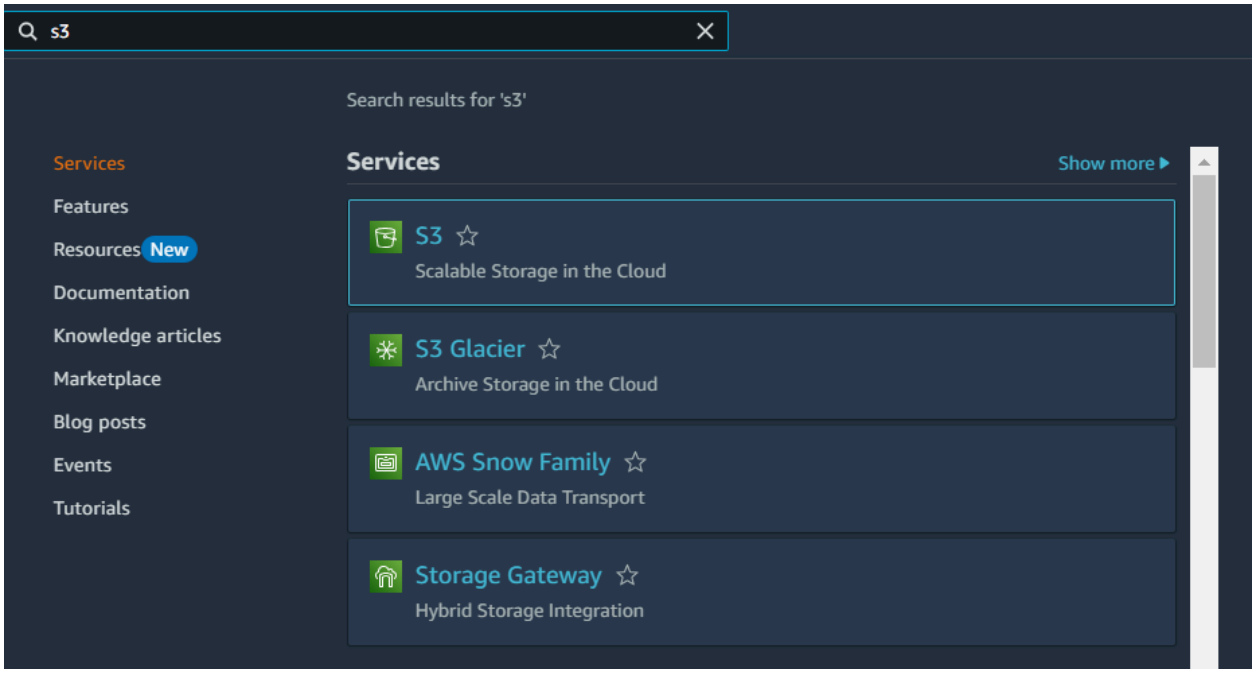


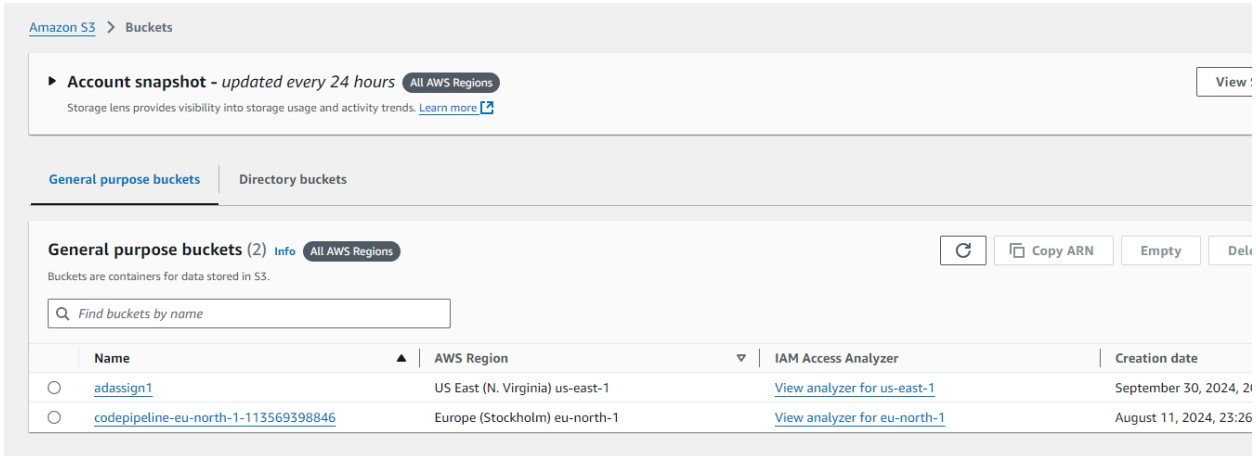
Click on Test and choose the ‘S3 Put’ Template.


Configure test event
A test event is a JSON object that mocks the structure of requests emitted by AWS services to invoke a Lambda function. Use it to see the function's invocation result.
To invoke your function without saving an event, configure the JSON event, then choose Test.
Test event action
Create new event
Edit saved event
Event name
komalevent
Maximum of 25 characters consisting of letters, numbers, dots, hyphens and underscores.
Event sharing settings
Private
This event is only available in the Lambda console and to the event creator. You can configure a total of 10. Learn more
Shareable
This event is available to IAM users within the same account who have permissions to access and use shareable events. Learn more
Template - optional
s3-put
Event JSON
Format JSON
1 {
Template - optional
s3-put
Event JSON
Format JSON
{
"Records": [
{
"eventVersion": "2.0",
"eventSource": "aws:s3",
"awsRegion": "us-east-1",
"eventTime": "1970-01-01T00:00:00.000Z",
"eventName": "ObjectCreated:Put",
"userIdentity": {
"principalId": "EXAMPLE"
},
"requestParameters": {
"sourceIPAddress": "127.0.0.1"
},
"responseElements": {
"x-amz-request-id": "EXAMPLE123456789",
"x-amz-id-2": "EXAMPLE123/5678abcdefghijklambdaisawesome/mnopqrstuvwxyzABCDEFGH"
},
"s3": {
"s3SchemaVersion": "1.0",
"configurationId": "testConfigRule",
"bucket": {
"name": "example-bucket",
"ownerIdentity": {
"principalId": "EXAMPLE"
},
"arn": "arn:aws:s3:::example-bucket"
},
"object": {
"key": "test%2Fkey",
1:1 JSON Spaces: 2
Cancel
Invoke
Save

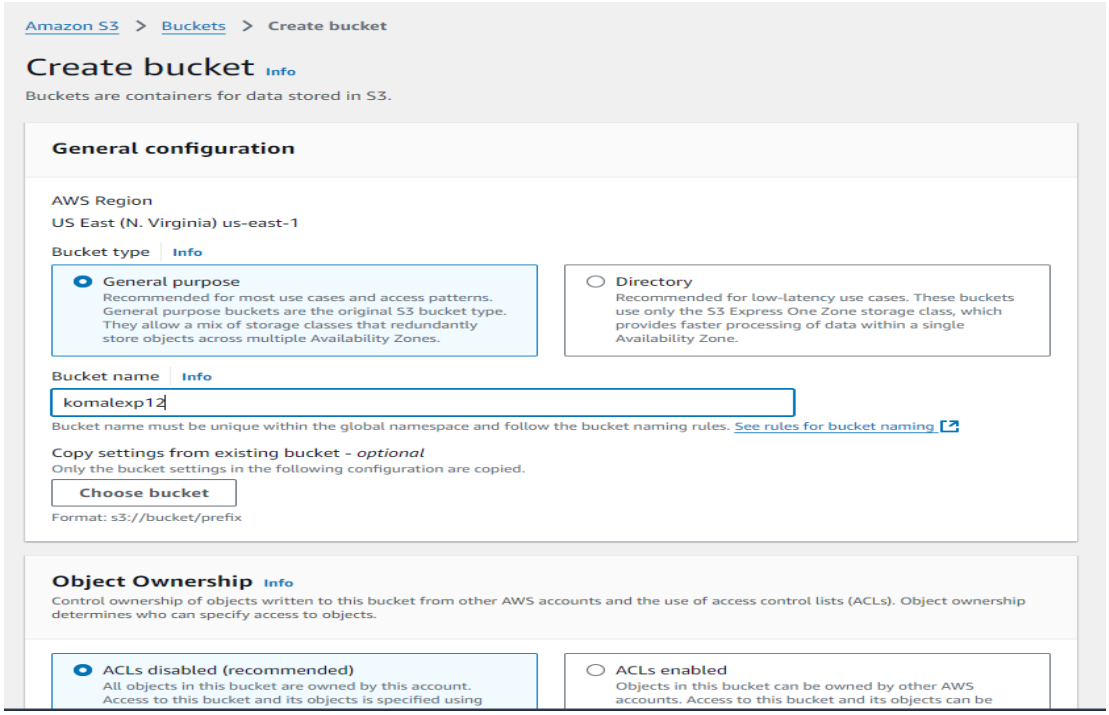


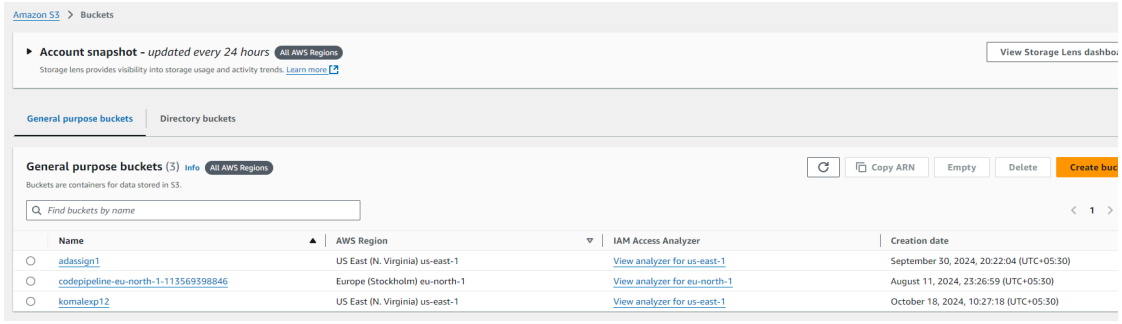
Open up the S3 Console and create a new bucket.



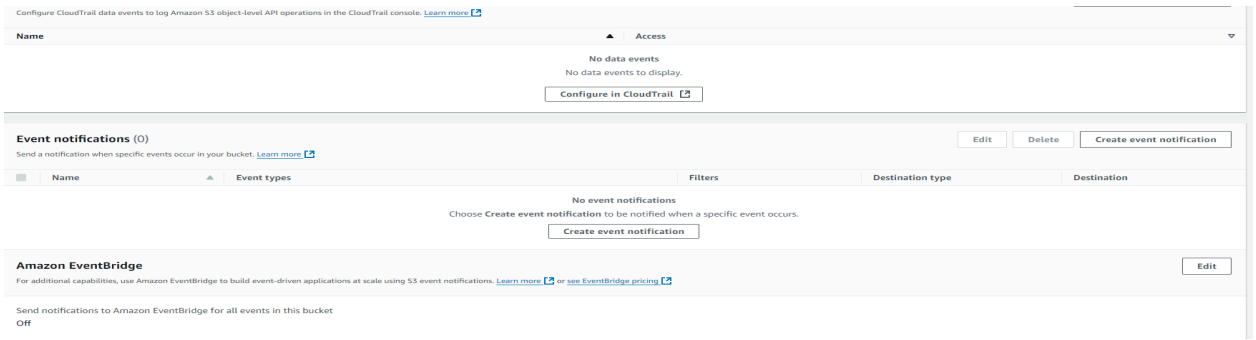


With all general settings, create the bucket in the same region as the function.

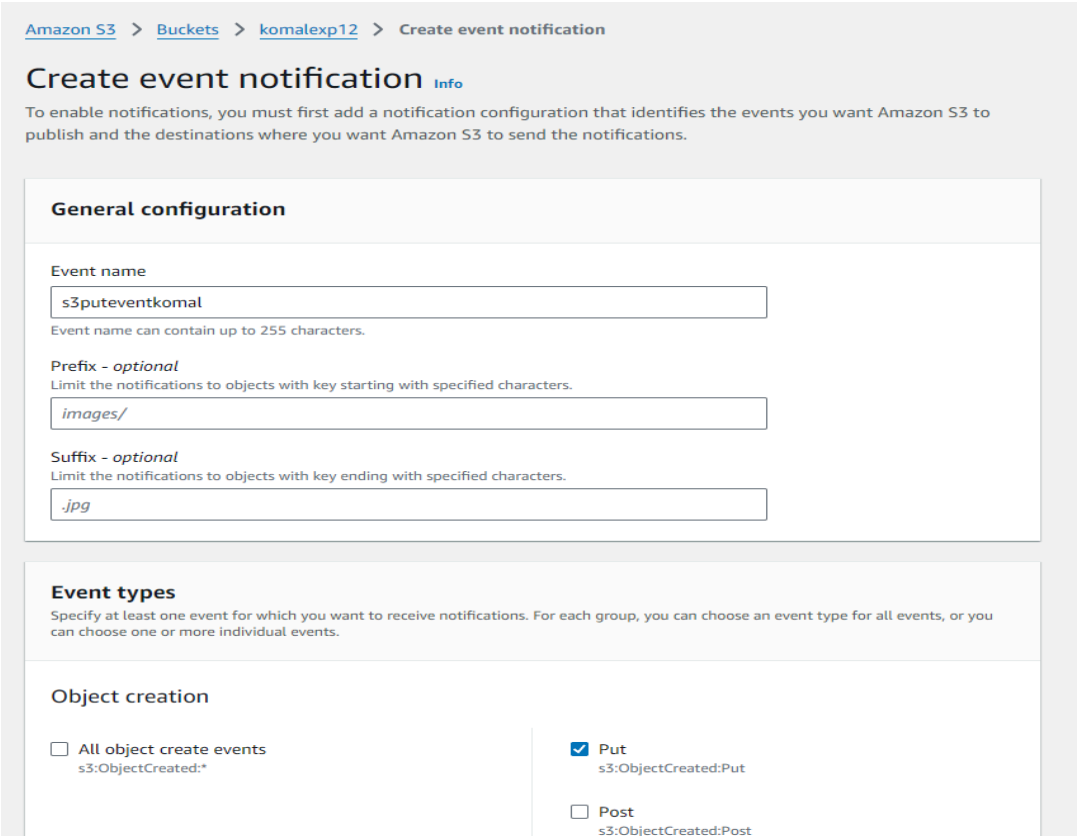




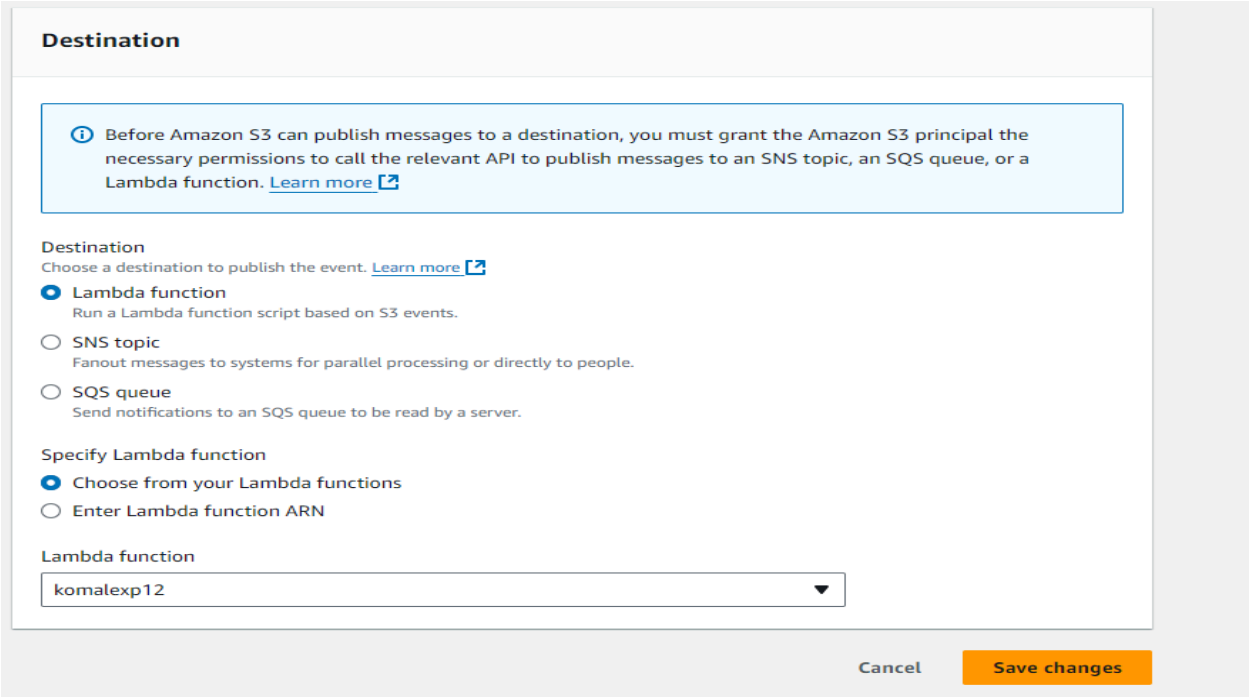
Click on the created bucket and under properties, look for events. Click on Create Event Notification.



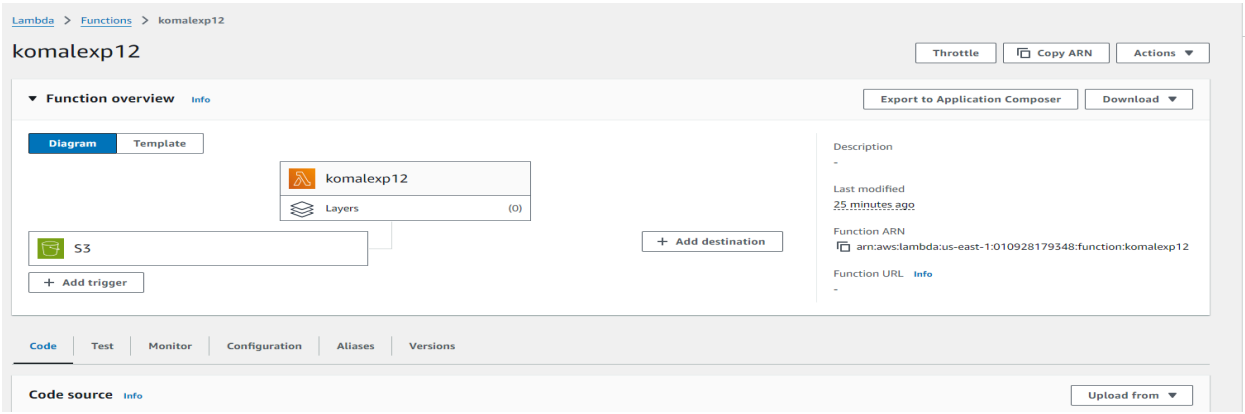
Mention an event name and check Put under event types.



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

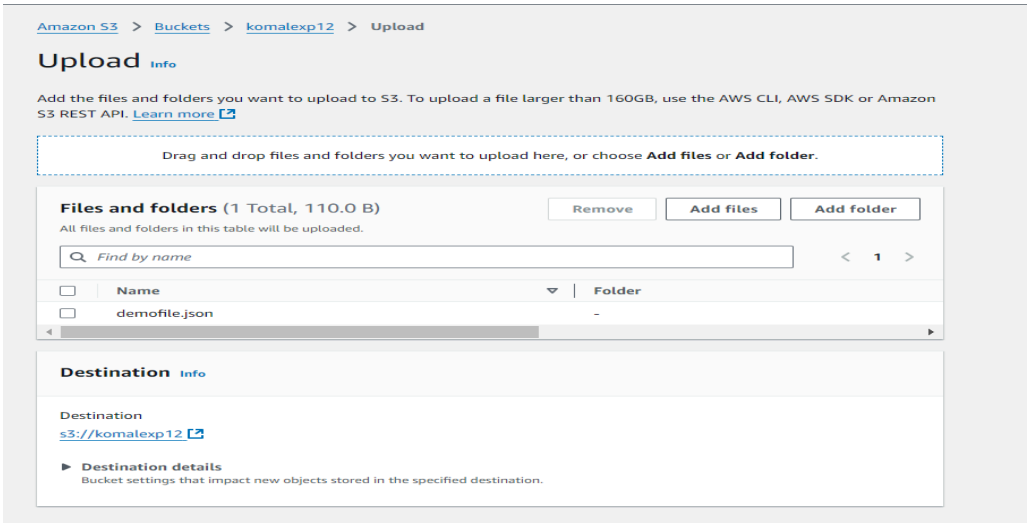


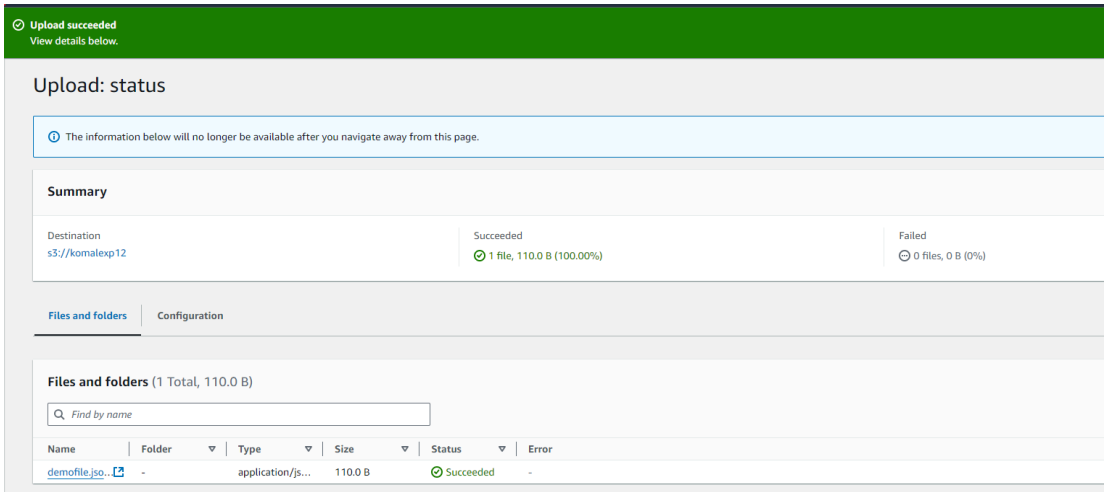
Refresh the Lambda function console and you should be able to see an S3 Trigger in the overview.



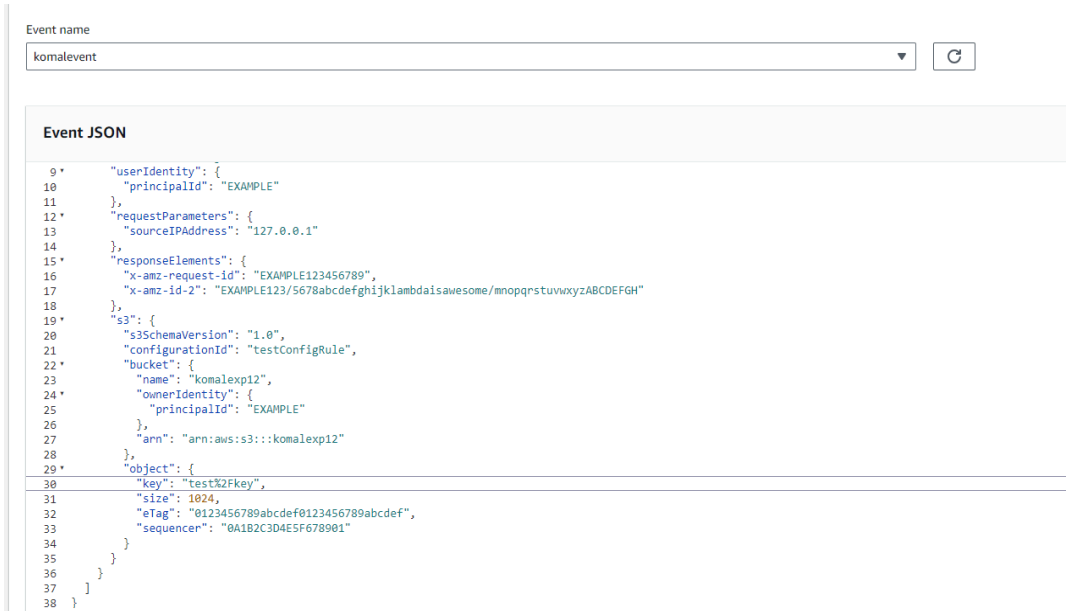
Now, create a demofile JSON file locally.

Go back to your S3 Bucket and click on Add Files to upload a new file. Select the demofile data file from your computer and click Upload.

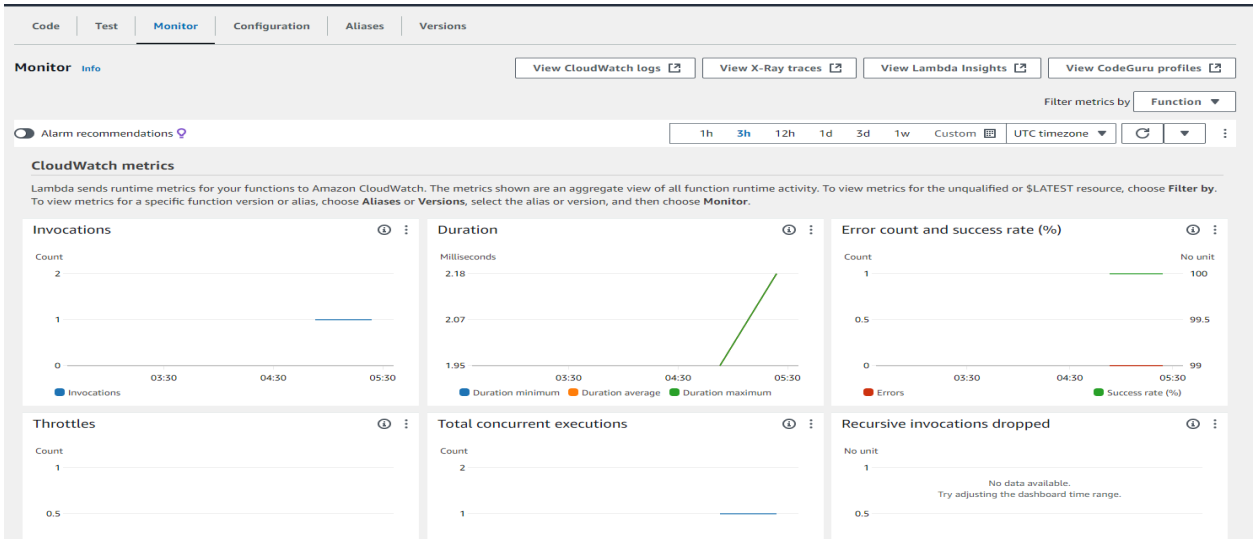




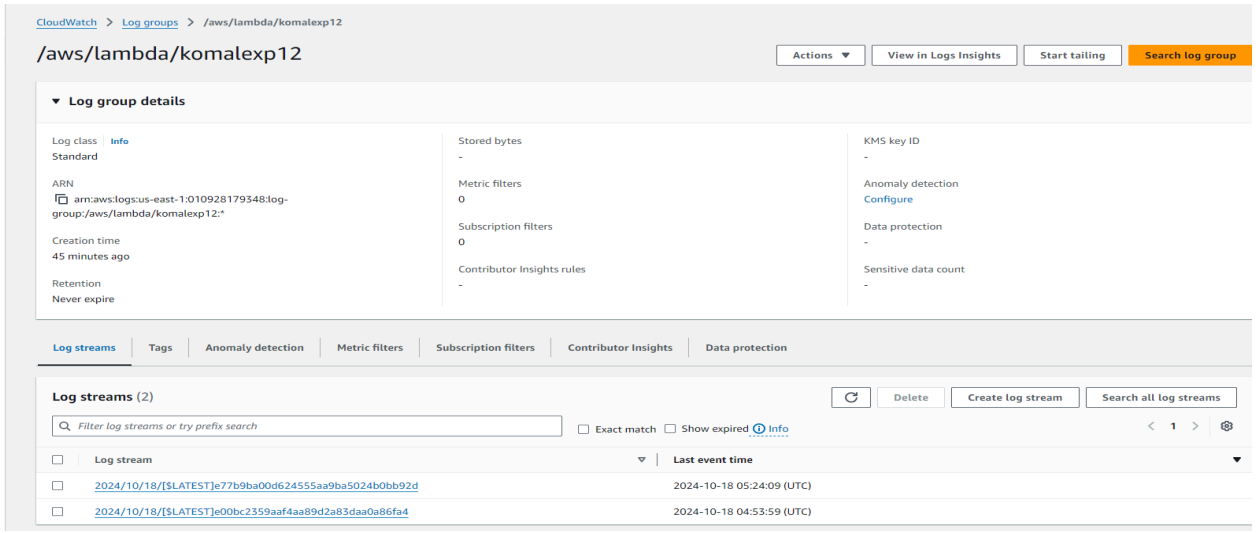
After this make the necessary changes in the Test configuration file which we created it previously by replacing the Bucket Name and the ARN of Bucket.



Go back to your Lambda function , Refresh it and check the Monitor tab



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



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