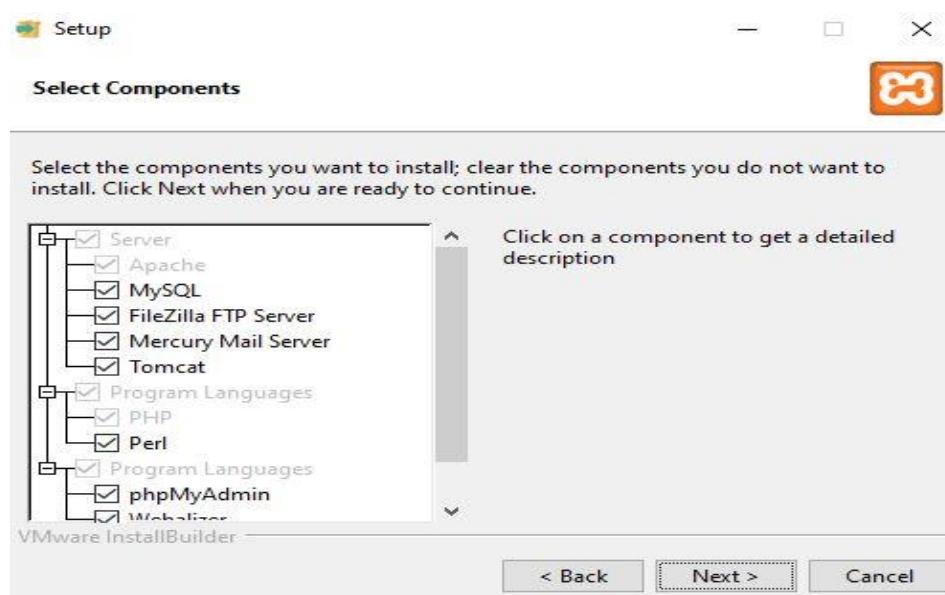
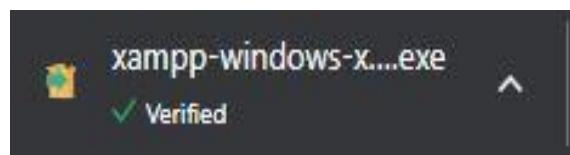
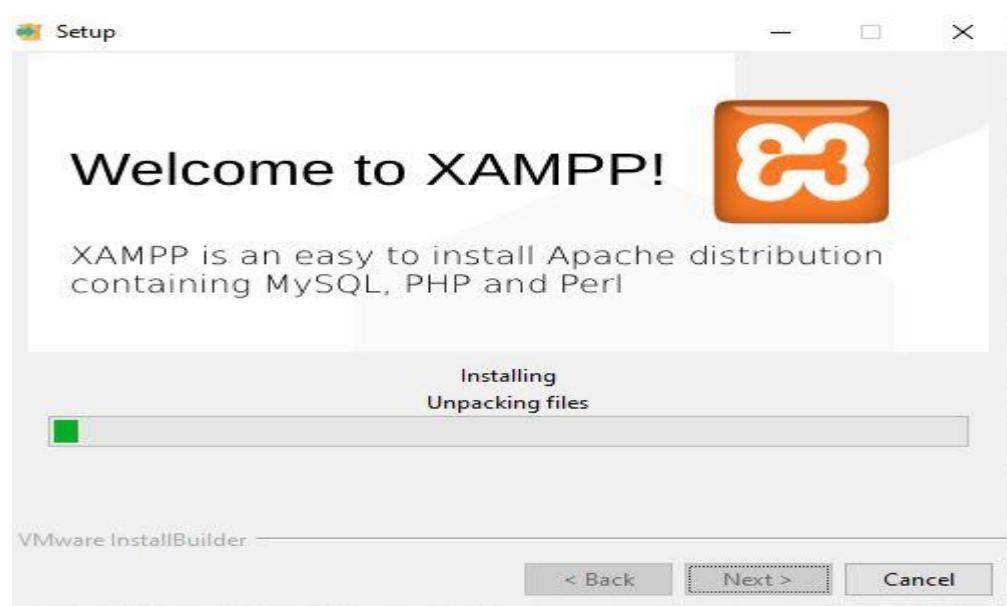
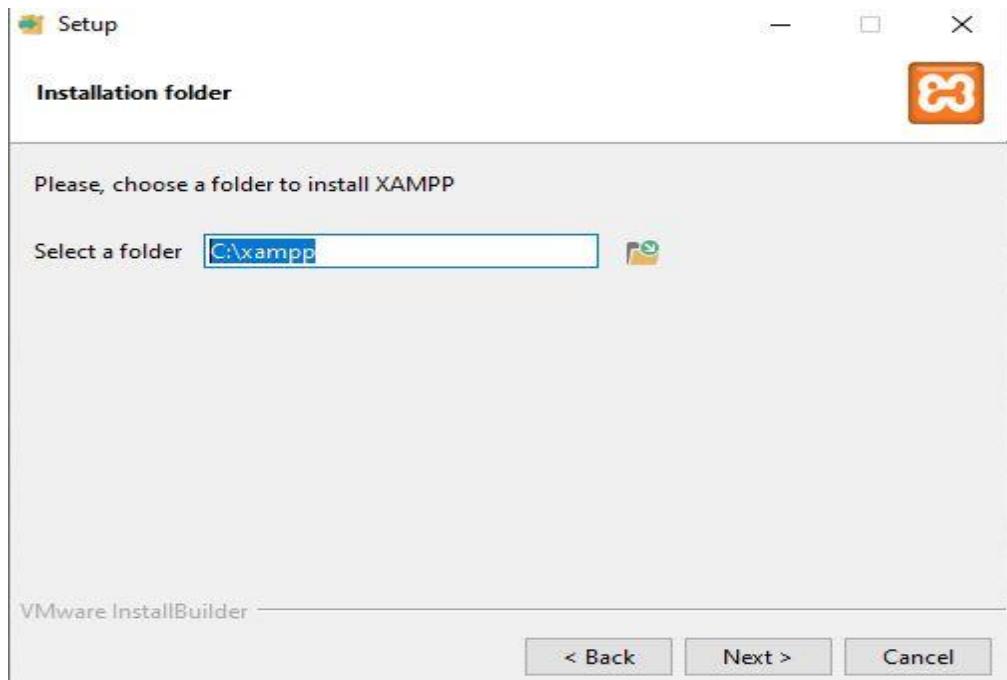


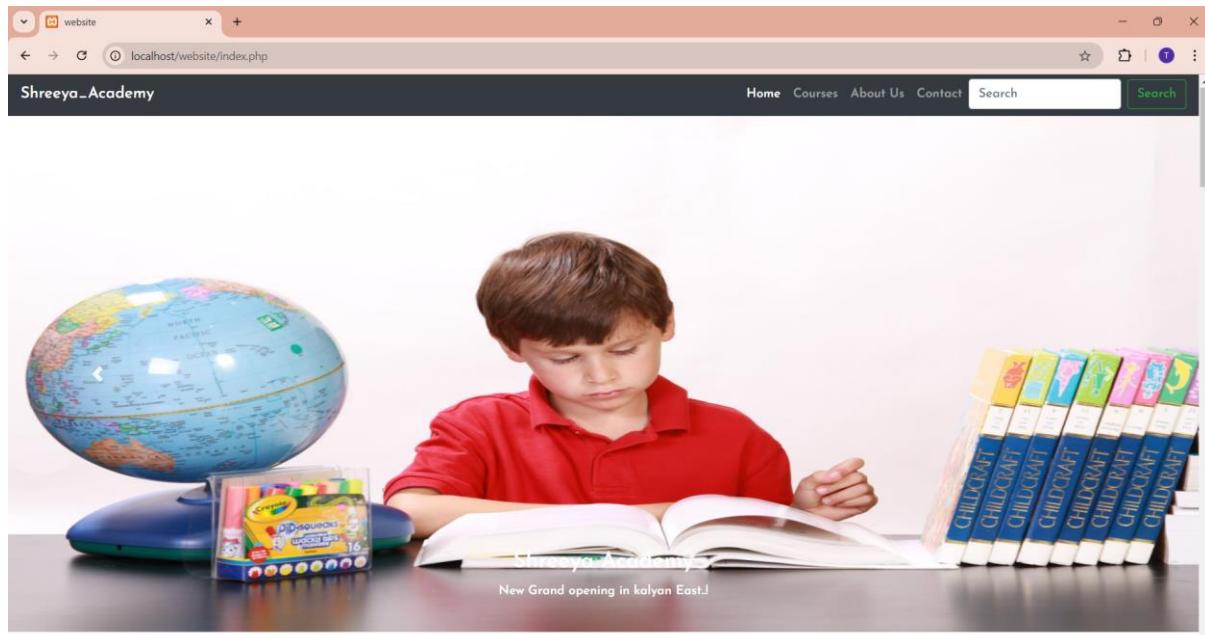
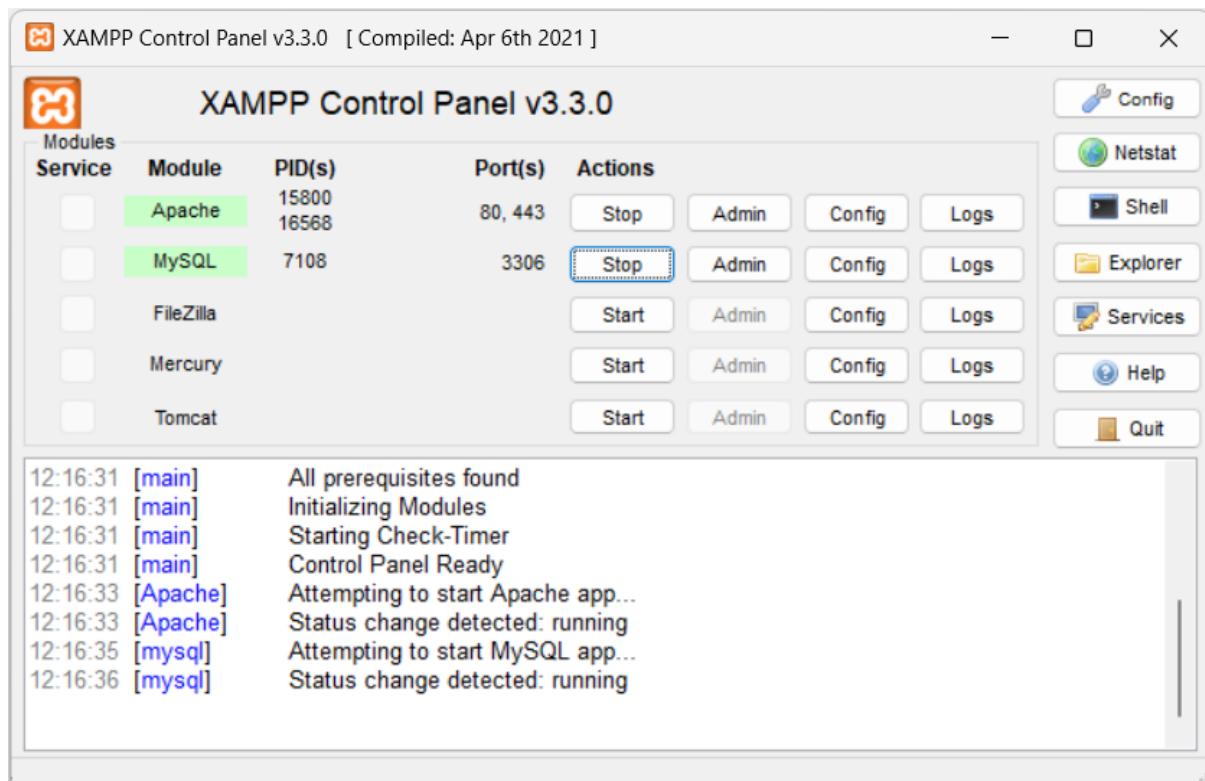
EXPERIMENT NO: - 01

Part 1: To develop a website and host it on your local machine on a VM

- Steps to host Website using Xampp Server







➤ Launching EC2 on AWS

The screenshot shows the AWS search interface with the query 'EC2'. The results page displays the 'Services' section, which includes the EC2 service card. The EC2 card is titled 'Virtual Servers in the Cloud' and lists 'Top features' such as Dashboard, Launch templates, Instances, Spot Instance requests, and Savings plans. Below the services section is a 'Features' section containing a 'Dashboard' card.

The screenshot shows the AWS EC2 Dashboard. On the left, there is a navigation sidebar with sections like EC2 Global View, Events, Console-to-Code, Instances, Images, and Elastic Block Store. The main area is titled 'Resources' and shows a summary of current resources: 0 Instances (running), 0 Auto Scaling Groups, 0 Dedicated Hosts, 0 Elastic IPs, 0 Instances, 1 Key pairs, 0 Load balancers, 0 Placement groups, 1 Security groups, 0 Snapshots, and 0 Volumes. To the right, there are sections for 'Account attributes' (Default VPC set to vpc-0d93715b8c7682b9a) and 'Explore AWS' (with links to AWS Health Dashboard, Service health, and Best Price-Performance with AWS Graviton2). A prominent 'Launch instance' button is located in the center-left of the dashboard.

The screenshot shows the AWS EC2 Instances page. The left sidebar includes links for EC2 Dashboard, EC2 Global View, Events, Console-to-Code Preview, Instances, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, Elastic IPs, Placement Groups, Key Pairs, and Network Interfaces. The main content area has a search bar and filters for Name, Instance ID, Instance state (set to running), Instance type, Status check, Alarm status, Availability Zone, and Public IP. A message says "No matching instances found". A modal window titled "Select an instance" is open, showing a single entry: "practical1". The bottom navigation bar includes cloudShell, Feedback, and links for 2024, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

The screenshot shows the AWS AMI selection page. The left sidebar has a three-line menu icon. The main content area includes sections for "Name and tags" (with a "practical1" input field and "Add additional tags" link), "Application and OS Images (Amazon Machine Image)" (with a search bar and a "Quick Start" section featuring logos for Amazon Linux, macOS, Ubuntu, Windows, Red Hat, and SUSE Linux), and "Browse more AMIs" (including AMIs from AWS, Marketplace, and the Community). On the right, a "Summary" section shows "Number of instances: 1". It also lists "Software Image (AMI)" (Canonical, Ubuntu, 24.04 LTS, ami-04a81a99f5ec58529), "Virtual server type (instance type)" (t2.micro), "Firewall (security group)" (New security group), and "Storage (volumes)" (1 volume(s) - 8 GiB). A callout box highlights a "Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which you launch)." At the bottom are "Cancel", "Launch instance" (in a blue button), and "Review commands". The top navigation bar includes AWS, Services, Search, and links for N. Virginia and the user vclabs/user3396433=GUNJAL_TEJAS.

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

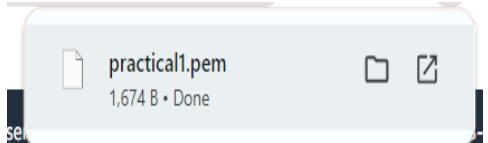
- RSA
RSA encrypted private and public key pair
- ED25519
ED25519 encrypted private and public key pair

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](#)



aws Services Search [Alt+S] N. Virginia v vocabs/user3396433=GUNJAL_TEJAS_DHONDIHAI_MANDA @ 4888-89

Network [Info](#)
vpc-0d95715b8c7682b9a

Subnet [Info](#)
No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)
Enable

Additional charges apply when outside of [free tier allowance](#)

Firewall (security groups) [Info](#)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

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

- Allow SSH traffic from 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. X

▼ Summary

Number of instances [Info](#)
1

Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...[read more](#)
ami-04a81a99f5ec58529

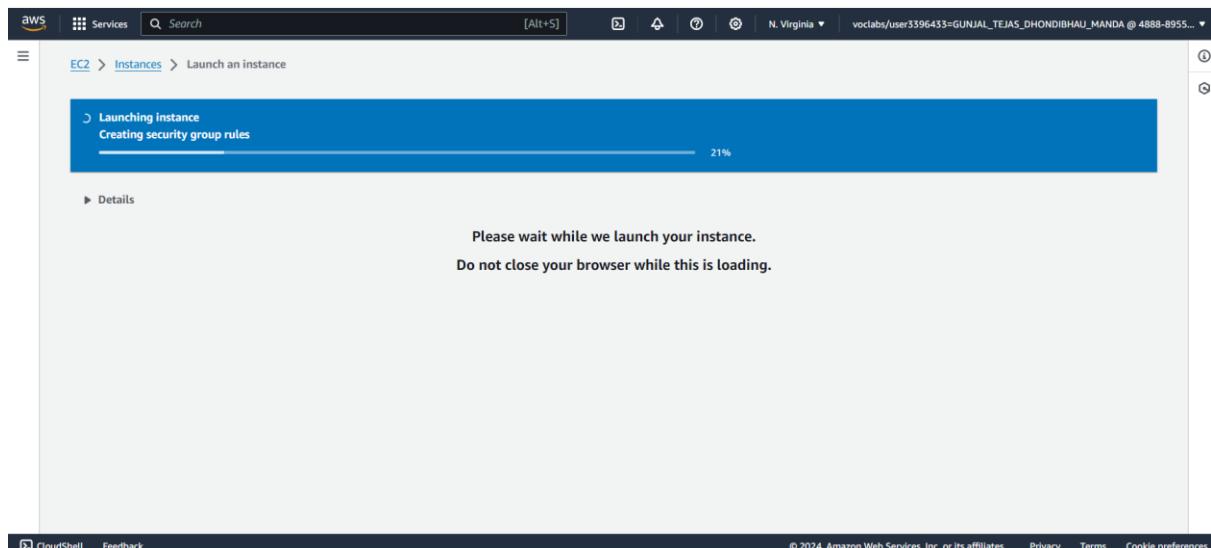
Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 30 GiB

ⓘ Free tier: In your first year includes 750 hours of t2.micro (or t2.micro in the Regions in which it's available).

[Cancel](#) [Launch instance](#) [Review commands](#)



Instances (1) Info

Find Instance by attribute or tag (case-sensitive)

Instance ID = i-0a05901d6f25b1800

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input type="checkbox"/>	practical1	i-0a05901d6f25b1800	Running	t2.micro	Initializing	<input type="button" value="View alarms"/>	us-east-1e	ec2-18-

Select an instance

Connect to instance Info

Connect to your instance i-0a05901d6f25b1800 (practical1) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console



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: 18.206.107.24/29. [Learn more](#).

Instance ID

i-0a05901d6f25b1800 (practical1)

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

18.208.119.124

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

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

```
ubuntu@ip-172-31-49-70:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/root       29G   1.6G   27G   6% /
tmpfs          479M     0  479M   0% /dev/shm
tmpfs          192M  868K  191M   1% /run
tmpfs          5.0M     0  5.0M   0% /run/lock
/dev/xvda16     881M   76M  744M  10% /boot
/dev/xvda15    105M   6.1M   99M   6% /boot/efi
tmpfs          96M   12K   96M   1% /run/user/1000
ubuntu@ip-172-31-49-70:~$ htop
ubuntu@ip-172-31-49-70:~$ ls
ubuntu@ip-172-31-49-70:~$ █
```

```
ubuntu@ip-172-31-49-70:-
[1] + 0000 Stopped                 htop
ubuntu@ip-172-31-49-70:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/root       29G   1.6G   27G   6% /
tmpfs          479M     0  479M   0% /dev/shm
tmpfs          192M  868K  191M   1% /run
tmpfs          5.0M     0  5.0M   0% /run/lock
/dev/xvda16     881M   76M  744M  10% /boot
/dev/xvda15    105M   6.1M   99M   6% /boot/efi
tmpfs          96M   12K   96M   1% /run/user/1000
ubuntu@ip-172-31-49-70:~$ htop
ubuntu@ip-172-31-49-70:~$ ls
ubuntu@ip-172-31-49-70:~$ █
```

```
ubuntu@ip-172-31-5-93:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libaprilt64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libaprilt64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 39 not upgraded.
Need to get 1680 kB/2083 kB of archives.
After this operation, 8094 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-bin amd64 2.4.58-1ubuntu8.4 [1329 kB]
Get:2 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-data all 2.4.58-1ubuntu8.4 [163 kB]
Get:3 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-utils amd64 2.4.58-1ubuntu8.4 [97.1 kB]
Get:4 http://us-east-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2 amd64 2.4.58-1ubuntu8.4 [90.2 kB]
Fetched 1680 kB in 0s (17.0 MB/s)
Preconfiguring packages ...
Selecting previously unselected package libaprilt64:amd64.
(Reading database ... 67739 files and directories currently installed.)
Preparing to unpack .../0-libaprilt64_1.7.2-3.1build2_amd64.deb ...
Unpacking libaprilt64:amd64 (1.7.2-3.1build2) ...
Selecting previously unselected package libaprutil1t64:amd64.
Preparing to unpack .../1-libaprutil1t64_1.6.3-1.lubuntu7_amd64.deb ...
```

```
Running kernel seems to be up-to-date.  
No services need to be restarted.  
No containers need to be restarted.  
No user sessions are running outdated binaries.  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
ubuntu@ip-172-31-5-93:~$ cd /var/www/html  
ubuntu@ip-172-31-5-93:/var/www/html$ ls  
index.html  
ubuntu@ip-172-31-5-93:/var/www/html$ sudo rm index.html  
ubuntu@ip-172-31-5-93:/var/www/html$ sudo nano indexxx.html  
ubuntu@ip-172-31-5-93:/var/www/html$ [ ]
```



Contact

username

Email address

Contact Number

comment

Submit

EXPERIMENT NO :- 02

AIM:- To Build Your Application using AWS CodeBuild and Deploy on S3 / SEBS using AWS Code Pipeline, deploy Sample Application on EC2 instance using AWS CodeDeploy.

- Creating two roles in AWS IAM for CI/CD pipeline setup

The screenshot shows the AWS Services search interface. The search bar at the top contains 'iam'. Below the search bar, there's a sidebar with various AWS service links. The main area displays search results for 'iam' under 'Services' and 'Features'.

Services (11)

- IAM: Manage access to AWS resources
- IAM Identity Center: Manage workforce user access to multiple AWS accounts and cloud applications
- Resource Access Manager: Share AWS resources with other accounts or AWS Organizations

Features (24)

- Groups: IAM feature

See all 11 results ▶ and **See all 24 results ▶**

The screenshot shows the IAM Dashboard. The left sidebar includes links for Identity and Access Management (IAM), Dashboard, Access management, Access reports, and Quick Links. The main dashboard area displays security recommendations, IAM resources (User groups: 0, Users: 0, Roles: 2, Policies: 0, Identity providers: 0), and a 'What's new' section. On the right side, there are sections for the AWS Account (Account ID: 010928184174, Account Alias: Create) and Tools.

Identity and Access Management (IAM)

Roles (2) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor	-

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

Step 2 Add permissions

Step 3 Name, review, and create

Trusted entity type

- AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- SAML 2.0 federation Allow users Federated with SAML 2.0 from a corporate directory to perform actions in this account.
- Custom trust policy Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

- EC2 Allows EC2 instances to call AWS services on your behalf.
- EC2 Role for AWS Systems Manager Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
- EC2 Spot Fleet Role Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
- EC2 - Spot Fleet Auto Scaling

IAM > Roles > Create role

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Add permissions Info

Permissions policies (1/945) Info

Choose one or more policies to attach to your new role.

Filter by Type

Policy name	Type	Description
<input checked="" type="checkbox"/> AmazonEC2RoleforAWSCodeDeploy	AWS managed	Provides EC2 access to S3 bucket to ...
<input type="checkbox"/> AmazonEC2RoleforAWSCodeDeployLimited	AWS managed	Provides EC2 limited access to S3 buck...
<input type="checkbox"/> AWSCodeDeployDeployerAccess	AWS managed	Provides access to register and deploy ...
<input type="checkbox"/> AWSCodeDeployFullAccess	AWS managed	Provides full access to CodeDeploy res...
<input type="checkbox"/> AWSCodeDeployReadOnlyAccess	AWS managed	Provides read only access to CodeDepl...
<input type="checkbox"/> AWSCodeDeployRole	AWS managed	Provides CodeDeploy service access to ...
<input type="checkbox"/> AWSCodeDeployRoleForCloudFormation	AWS managed	Provides CodeDeploy service access to ...
<input type="checkbox"/> AWSCodeDeployRoleForECS	AWS managed	Provides CodeDeploy service wide acc...
<input type="checkbox"/> AWSCodeDeployRoleForECSLimited	AWS managed	Provides CodeDeploy service limited a...
<input type="checkbox"/> AWSCodeDeployRoleForLambda	AWS managed	Provides CodeDeploy service access to ...

Role details

Role name: EC2CodeDeploy

Description: Allows EC2 instances to call AWS services on your behalf.

Step 1: Select trusted entities

Trust policy:

```

1 < [           "version": "2012-10-17",
2   "Statement": [
3     {
4       "Effect": "Allow",
5       "Action": [
6         "sts:AssumeRole"
7       ],
8       "Principal": [
9         "AWS:AmazonEC2"
10      ]
11    }
12  ]
13 ]
14 ]
15 ]

```

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Identity and Access Management (IAM)

Role EC2CodeDeploy created.

Roles (3) Info

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Link)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Link)	-
EC2CodeDeploy	AWS Service: ec2	-

Roles Anywhere Info

Access AWS from your non AWS workloads

X.509 Standard

Temporary credentials

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 3 Name, review, and create

AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account.

AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

Choose a use case for the specified service.
Use case

CodeDeploy Allows CodeDeploy to call AWS services such as Auto Scaling on your behalf.

CodeDeploy for Lambda Allows CodeDeploy to route traffic to a new version of an AWS Lambda function version on your behalf.

CodeDeploy - ECS Allows CodeDeploy to read S3 objects, invoke Lambda functions, publish to SNS topics, and update ECS services on your behalf.

Next

IAM > Roles > Create role

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Add permissions

Permissions policies (1) Info
The type of role that you selected requires the following policy.

Policy name	Type
<input checked="" type="checkbox"/> AWSCodeDeployRole	AWS managed

Set permissions boundary - optional

Next

CloudShell Feedback

Step 1: Select trusted entities

Role details

Role name
Enter a meaningful name to identify this role.

Description
Add a short explanation for this role.

Trust policy

```

1+ [{"Version": "2012-10-17", "Statement": [
2+   {"Sid": "", "Effect": "Allow", "Principal": {"Service": ["codedeploy.amazonaws.com"]}, "Action": ["sts:AssumeRole"]}], "Id": "ASIAQKJLH4PZGK3V3WQ", "Type": "AWS", "Arn": "arn:aws:iam::123456789012:role/CodeDeployRole", "CreateDate": "2024-01-15T10:00:00Z", "LastUsed": "2024-01-15T10:00:00Z", "UpdateDate": "2024-01-15T10:00:00Z", "VersionId": "1", "Version": "2012-10-17", "StatementCount": 1, "PolicySize": 1024, "AttachedPolicies": [], "AttachedGroups": []}
  
```

Next

➤ Launching & Setting up EC2 Instance for Deployment

Search results for 'EC'

Services (112)

- EC2
- Security Hub
- Security Lake
- Direct Connect

Features (293)

- Direct Connect gateways
- AWS Private CA Connector for Active Directory

Resources (New)

Knowledge Articles (1,942)

Marketplace (440)

Blogs (23,090)

Events (696)

Tutorials (90)

See all 112 results ►

See all 293 results ►

Instances (2) [Info](#)

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	practical	i-0bb4f0f6d6ff74928	Running	t2.micro	2/2 checks passed	View alarms +	us-east-2a
<input type="checkbox"/>	practical1	i-06b9eda49cc6d9226	Running	t2.micro	2/2 checks passed	View alarms +	us-east-2a

Select an instance

[CloudShell](#) [Feedback](#)

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: AAR-CICD

Application and OS Images (Amazon Machine Image)

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

Recent OS Images: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux Enterprise Server

Browse more AMIs Including AMIs from AWS Marketplace and the Community

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.5.2...read more ami-05c3dc660cb6907f0

Virtual server type (instance type): t2.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, 30 GiB of EBS storage, 2 million IOPS, 1 million requests, and 1 million API calls per month.

Cancel Launch instance Review commands

Instance type

t2.micro (Family: t2, 1 vCPU, 1 GiB Memory, Current generation: true) Free tier eligible

On-Demand Linux base pricing: 0.0116 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour

On-Demand Windows base pricing: 0.0162 USD per Hour

On-Demand RHEL base pricing: 0.026 USD per Hour

All generations Compare instance types

Additional costs apply for AMIs with pre-installed software

Key pair (login)

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

Network: info

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.5.2...read more ami-05c3dc660cb6907f0

Virtual server type (instance type): t2.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, 30 GiB of EBS storage, 2 million IOPS, 1 million requests, and 1 million API calls per month.

Cancel Launch instance Review commands

CloudShell Feedback

Network

vpc-008c238273e437b52

Subnet

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)

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-005e9d856101cf758 X VPC: vpc-008c238273e437b52

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

Advanced

1x 8 GiB gp3 Root volume (Not encrypted)

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.5.2...read more ami-05c3dc660cb6907f0

Virtual server type (instance type): t2.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, 30 GiB of EBS storage, 2 million IOPS, 1 million requests, and 1 million API calls per month.

Cancel Launch instance Review commands

Advanced details

Domain join directory: Select

IAM instance profile: EC2CodeDeploy (arn:aws:iam::010928184174:instance-profile/EC2CodeDeploy)

Hostname type: IP name

DNS Hostname: 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: Select

Shutdown behavior: Stop

Stop - Hibernate behavior: Select

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.5.2...read more
ami-05c3dc660cb6907f0

Virtual server type (instance type): t2.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

Launch instance

Number of instances: 2

Allow tags in metadata: Select

User data - optional: 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: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.5.2...read more
ami-05c3dc660cb6907f0

Virtual server type (instance type): t2.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

Launch instance

Success
Successfully initiated launch of instance (i-06ee810b4baa23bd8)

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](#)

- Creating an application and deployment group in AWS CodeDeploy

The screenshot shows the AWS Services search interface. The search bar at the top contains the text "CodeArtifact". Below the search bar, there is a sidebar with various service categories and their sub-options. The "Services" category is expanded, showing "Amazon Q Developer (Including Amazon CodeWhisperer)", "CodeCommit", "CodePipeline", and "AWS Signer". The "Features" category is also expanded, showing "Full repository analysis" and "Pull request code review". The footer of the page includes links for "CloudShell" and "Feedback", and a copyright notice for "© 2024, Amazon Web Services, Inc. or its affiliates."

The screenshot shows the AWS CodeDeploy Applications page. The left sidebar is titled "Developer Tools" and has a section for "CodeDeploy" which is expanded, showing "Source", "Artifacts", "Build", "Deploy", "Pipeline", and "Settings". Under "Deploy", there are links for "Getting started", "Deployments", and "Applications". The main content area is titled "Applications" and shows a table with columns for "Application name", "Compute platform", and "Created". A message at the bottom states "No results" and "There are no results to display." The footer of the page includes links for "CloudShell" and "Feedback", and a copyright notice for "© 2024, Amazon Web Services, Inc. or its affiliates.".

AWS Services Search [Alt+S] Ohio Tejas21

Developer Tools > CodeDeploy > Applications > Create application

Create application

Application configuration

Application name
Enter an application name
 100 character limit

Compute platform
Choose a compute platform

Tags

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [Alt+S] Ohio Tejas21

Developer Tools > CodeDeploy > Applications > AAR-CICD

AAR-CICD

Application details

Name	Compute platform
AAR-CICD	EC2/On-premises

Deployment groups

Name	Status	Last attempted deploy...	Last successful deploy...	Trigger count
No deployment groups				

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Create deployment group

Application

- Application: AAR-CI_CD
- Compute type: EC2/On-premises

Deployment group name

Enter a deployment group name: AAR-CI_CD-DP

Service role

Enter a service role: arn:aws:iam::010928184174:role/CodeDeployRole

Deployment type

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
1 unique matched instance. [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
Name	AAR-CI_CD

Add tag

Agent configuration with AWS Systems Manager

Complete the required prerequisites before AWS Systems Manager can install the CodeDeploy Agent. Make sure the AWS Systems Manager Agent is installed on all instances and attach the required IAM policies to them. [Learn more](#)

Install AWS CodeDeploy Agent

Never

Only once

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

- Setting up a CI/CD pipeline for deploying applications on EC2 using GitHub.

The screenshots show the AWS CodePipeline 'Create new pipeline' wizard, Step 1 of 5: Choose pipeline settings.

Pipeline settings:

- Pipeline name:** AAR-CI_CD_PIPELINE
- Pipeline type:** Queued (Pipeline type V2 required)
- Execution mode:** Superseded (radio button selected)
- Service role:** New service role (radio button selected)

Variables:

- No variables defined at the pipeline level in this pipeline.
- Add variable (button)
- The first pipeline execution will fail if variables have no default values.

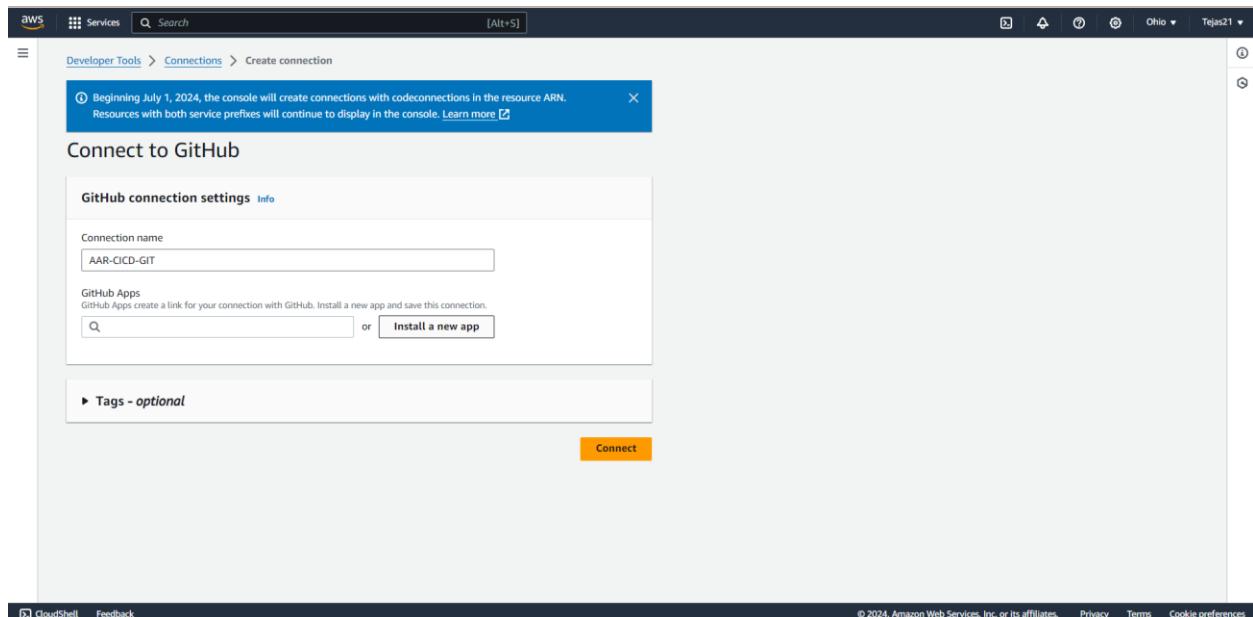
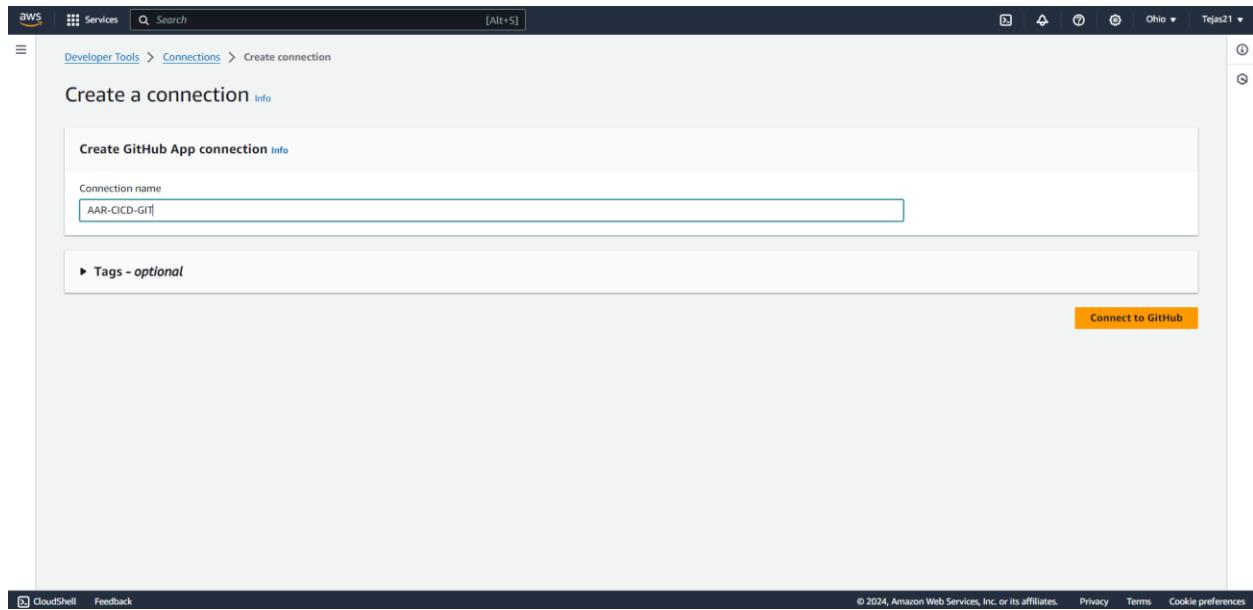
Advanced settings:

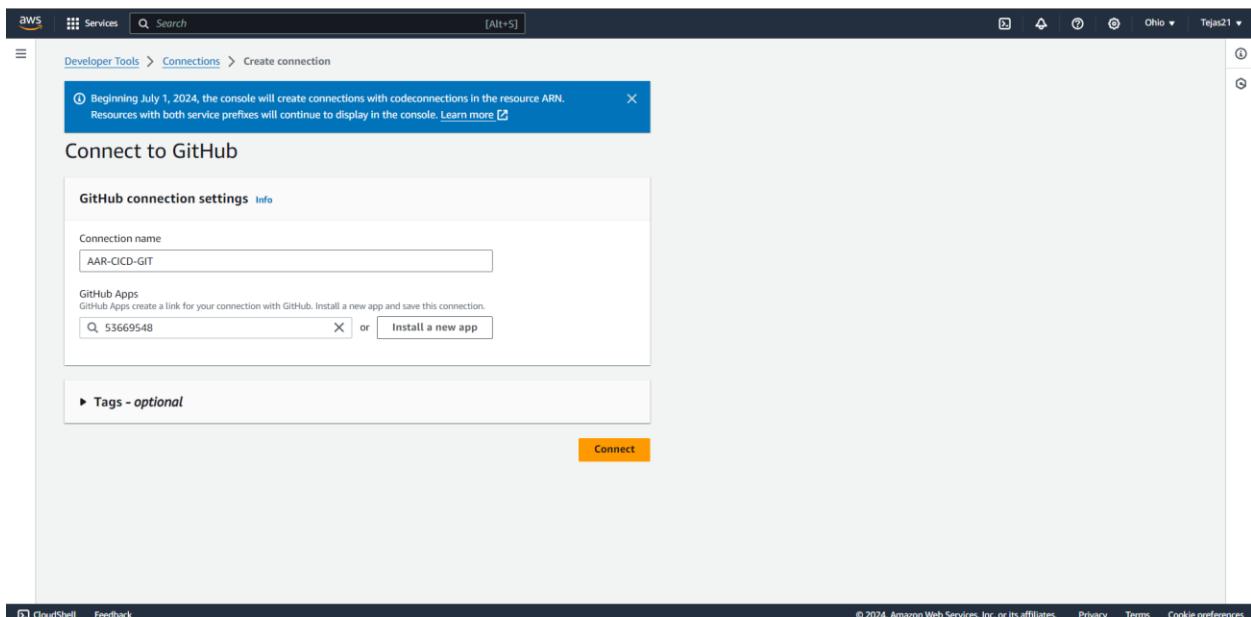
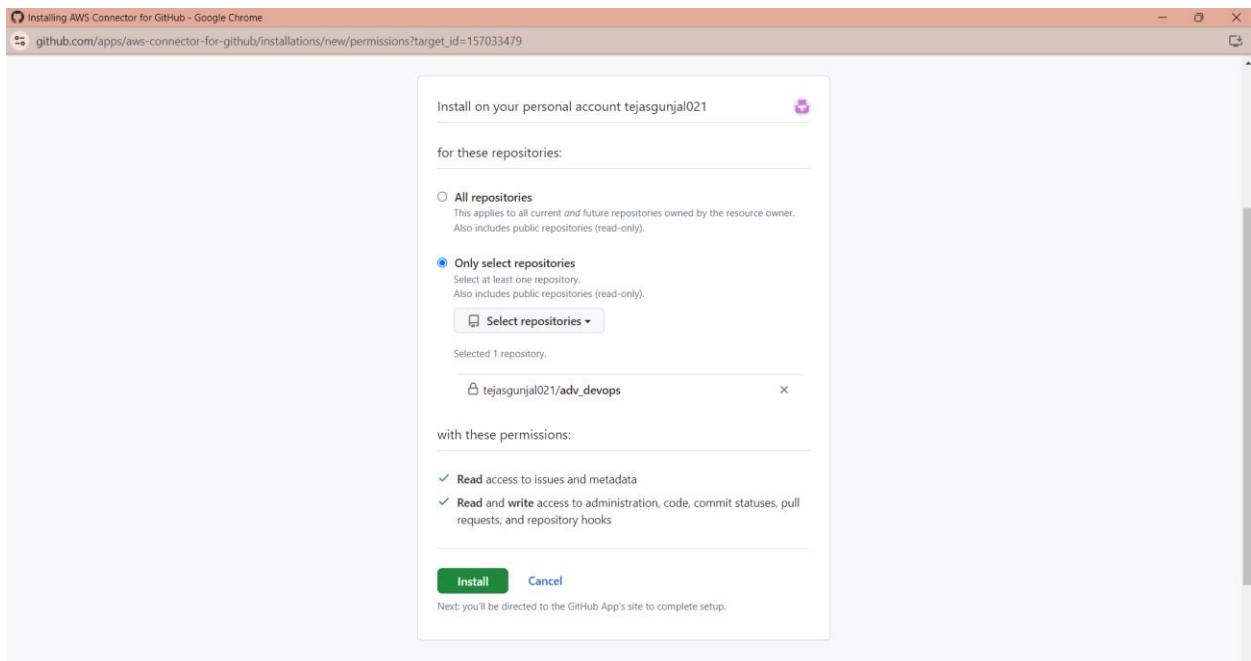
- Artifact store:** Default location (radio button selected)
- Encryption key:** Default AWS Managed Key (radio button selected)

Add source stage:

- Source provider:** GitHub (Version 2) (selected)
- 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:** Connect to GitHub (button)
- Repository name:** (input field)
- Default branch:** (input field)

- Connecting and setting up GitHub for CI/CD deployment on AWS CodeDeploy.





Source

Source provider
This is where you stored your input artifacts for your pipeline. Choose the provider and then provide the connection details.

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](#)

Ready to connect
Your GitHub connection is ready for use.

Repository name
Choose a repository in your GitHub account.

Default branch
Default branch will be used only when pipeline execution starts from a different source or manually started.

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
Does not 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

Add build stage

Step 1 **Choose pipeline settings**
Step 2 **Add source stage**
Step 3 **Add build stage**
Step 4 **Add deploy stage**
Step 5 **Review**

Build - optional

Build provider
This is the tool of your build project. Provide build artifact details like operating system, build spec file, and output file names.

[Cancel](#) [Previous](#) [Skip build stage](#) [Next](#)

Add build stage

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
US East (Ohio)

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.
Q AAR-CI_CD

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.
Q AAR-CI_CD-DP

Configure automatic rollback on stage failure

Cancel **Previous** **Next**

Step 3: Add build stage

Build action provider
No build

Step 4: Add deploy stage

Deploy action provider

Deploy action provider
AWS CodeDeploy
ApplicationName
AAR-CI_CD
DeploymentGroupName
AAR-CI_CD-DP
Configure automatic rollback on stage failure
Disabled

Cancel **Previous** **Create pipeline**

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-CI_CD-PIPELINE has been created.

AAR-CI_CD-PIPELINE

Pipeline type: V2 Execution mode: QUEUED

Source Succeeded
Pipeline execution ID: 79f449a3-8c99-4865-acd6-4b44c7b71275

Source
GitHub (Version 2) [\[?\]](#)
Succeeded - Just now
abfb677d [\[?\]](#)

View details

Disable transition

Deploy Failed
Pipeline execution ID: 79f449a3-8c99-4865-acd6-4b44c7b71275

Start rollback **Retry stage** **Retry failed actions**

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with links like EC2 Dashboard, EC2 Global View, Events, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, and Elastic IPs. The main content area shows an instance named 'IMDSv2 Required'. It has tabs for Details, Status and alarms, Monitoring, Security (which is selected), Networking, Storage, and Tags. Under the Security tab, there's a 'Security details' section with IAM Role (EC2CodeDeploy), Owner ID (010928184174), and Launch time (Sat Aug 10 2024 23:02:07 GMT+0530 (India Standard Time)). Below that is a 'Inbound rules' section with a table:

Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sgr-0d969b954754bdd69	All	All	sg-005e9d856101cf758	default

There's also an 'Outbound rules' section with a similar table:

Name	Security group rule ID	Port range	Protocol	Destination	Security groups
-	sgr-00b02179951be2472	All	All	0.0.0.0/0	default

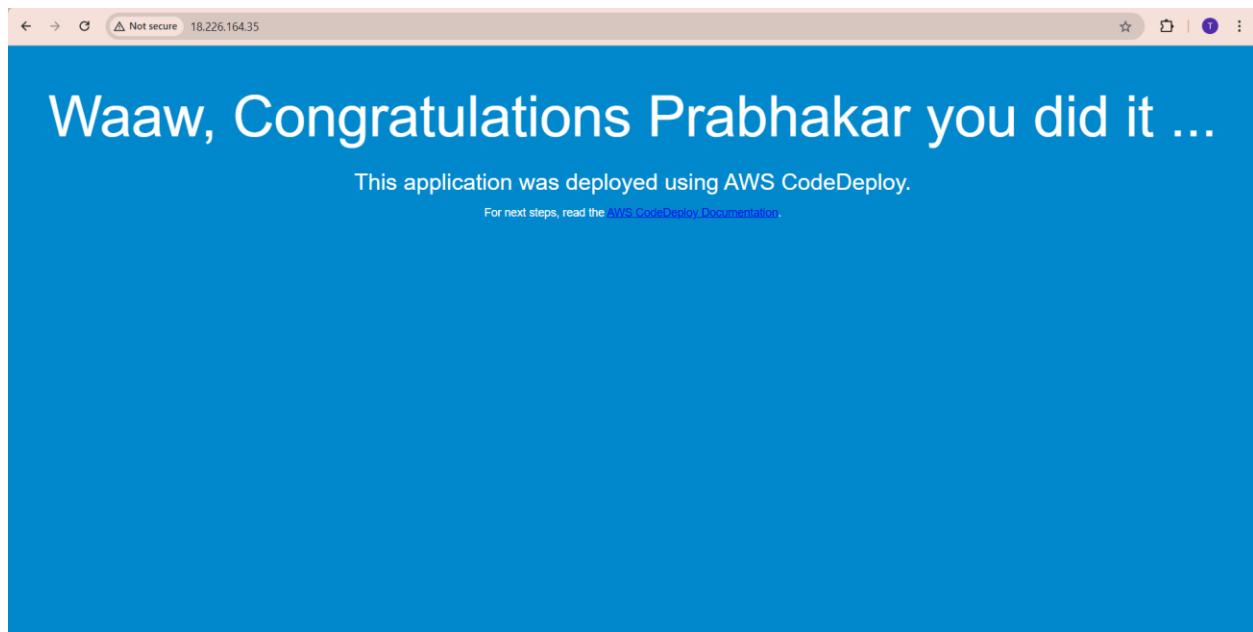
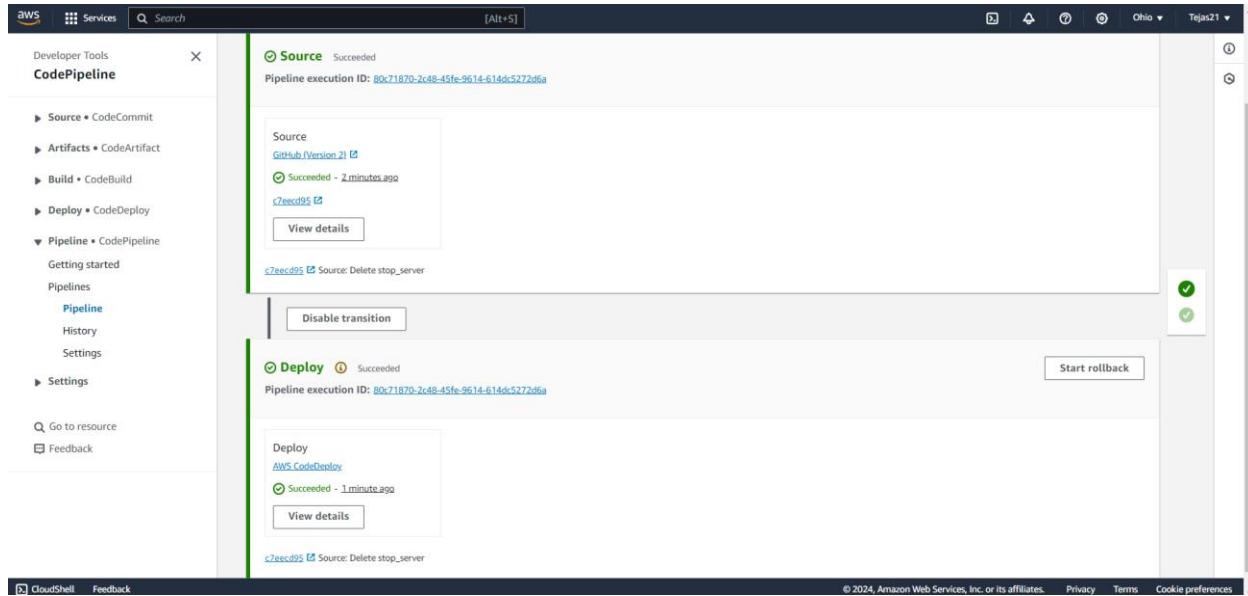
At the bottom, there's a URL bar with the address https://us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#SecurityGroups:securityGroupDetails=sg-005e9d856101cf758, and a footer with links for Privacy, Terms, and Cookie preferences.

The screenshot shows the 'Edit inbound rules' page for the security group 'sg-005e9d856101cf758 - default'. The top navigation bar includes links for EC2, Security Groups, and the current page 'sg-005e9d856101cf758 - default > Edit inbound rules'. Below the navigation is a heading 'Edit inbound rules' with a 'Info' link. A note says 'Inbound rules control the incoming traffic that's allowed to reach the instance.'

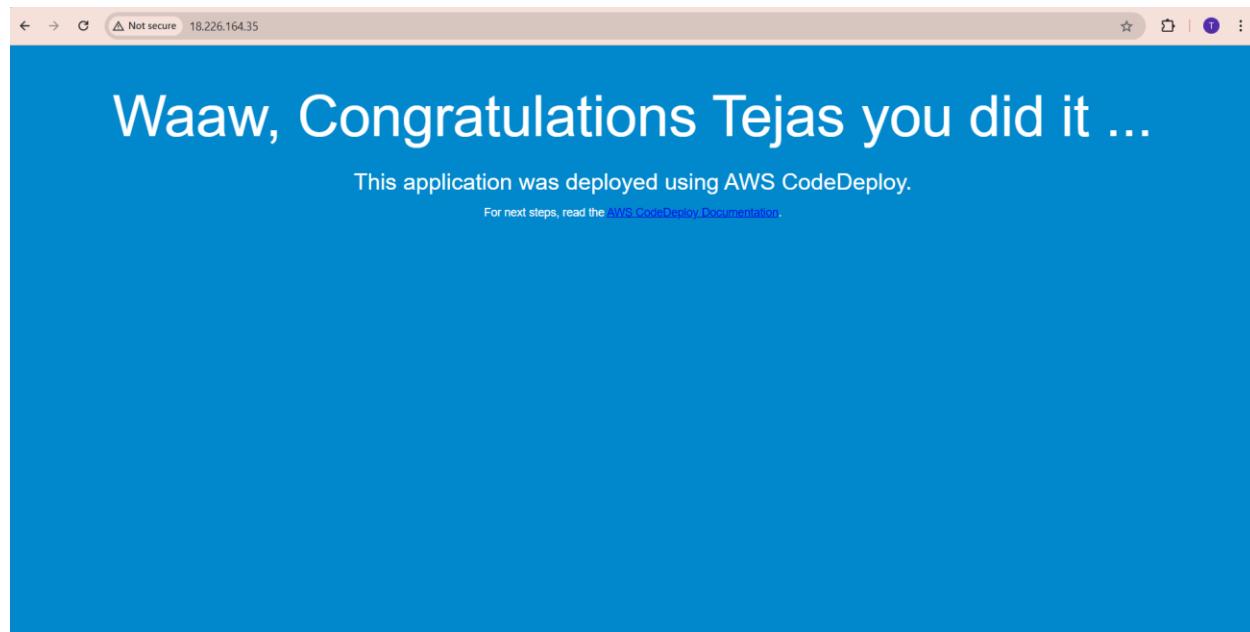
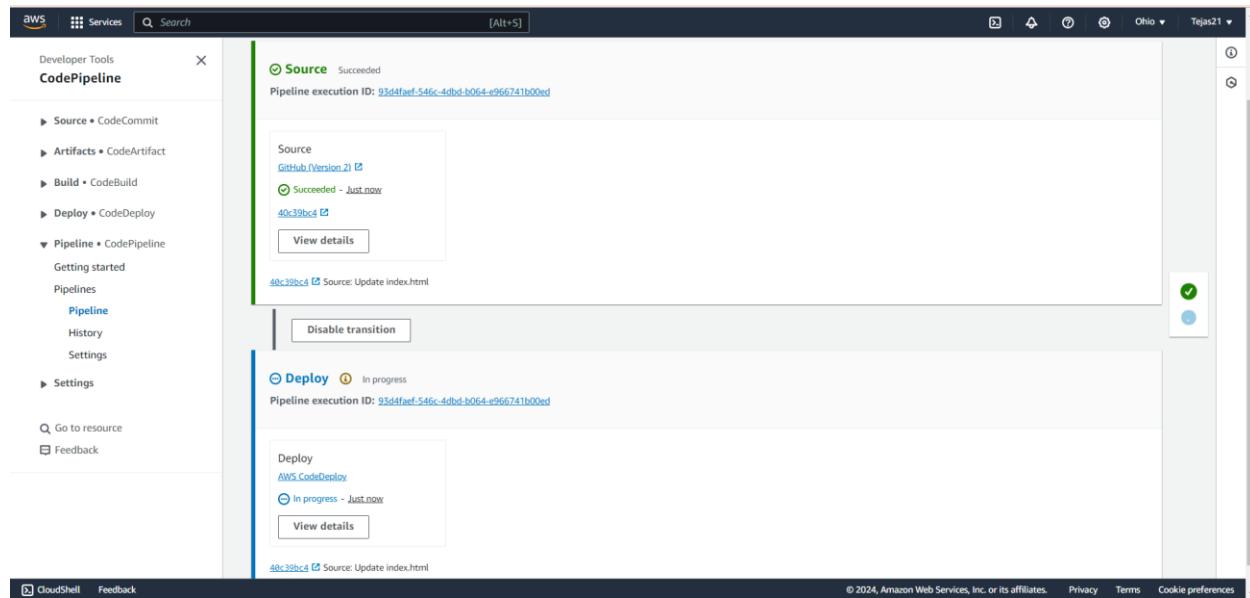
The main area is titled 'Inbound rules' with an 'Info' link. It shows three existing rules:

- Rule 1: Type: All traffic, Protocol: All, Port range: All, Source: Custom, Destination: sg-005e9d856101cf758. This row has a 'Delete' button.
- Rule 2: Type: HTTP, Protocol: TCP, Port range: 80, Source: Anywhere..., Destination: 0.0.0.0/0. This row has a 'Delete' button.
- Rule 3: Type: SSH, Protocol: TCP, Port range: 22, Source: Anywhere..., Destination: 0.0.0.0/0. This row has a 'Delete' button.

Below the rules is a 'Add rule' button. A warning message in a yellow box says: '⚠️ 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.' At the bottom are 'Cancel', 'Preview changes', and a highlighted 'Save rules' button. The footer includes links for cloudShell, Feedback, and standard AWS footer links for Privacy, Terms, and Cookie preferences.



- After committing changes in GitHub, the pipeline automatically starts deploying the updates, and the changes are applied without any manual intervention.



EXPERIMENT NO: - 03

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

Understanding Kubernetes Cluster Architecture

Introduction: -

Kubernetes is an open-source platform used to deploy and maintain a group of containers in a virtualized environment. In practice, Kubernetes is most commonly used alongside Docker for better control and implementation of containerized applications. Containerized applications “bundle” applications together with all its files, libraries, and packages required for it to run reliably and efficiently on different platforms. However, it operates at the container level rather than at the hardware level.

The name Kubernetes is derived from a Greek term meaning ‘helmsman’ or ‘pilot.’ True to this word, Kubernetes provides the guiding force for developer platforms to transition from virtual machines (VMs) to containers and the statically scheduled to the dynamically scheduled. This means no more manual integration and configuration when you move from a testing environment to an actual production environment or from on-premise to the cloud! The Kubernetes logical compute environment offers common services to all the applications in the cluster as part of the ecosystem for the software to run consistently.

Features of Kubernetes

- Automates various manual processes and controls server hosting and launching
- Manages containers offer security, and networking and storage services
- Monitors and continuously checks the health of nodes and containers
- Automates rollback for changes that go wrong
- Mounts and adds a storage system to run apps

Purpose of Kubernetes

The primary purpose of Kubernetes is to enable developers to write and deploy applications that can run seamlessly across multiple operating environments. Traditionally, application performance and deployment were tightly coupled to specific infrastructures, often requiring adherence to cloud provider-specific constructs and back-end storage systems. This dependency resulted in infrastructure lock-in, limiting flexibility and scalability.

Kubernetes addresses this challenge by abstracting the underlying infrastructure, allowing developers to deploy cloud-native applications in containers without restrictions. This means applications can be managed and scaled consistently across different environments—be it in the cloud, on-premises, or in hybrid setups—providing true infrastructure independence and operational flexibility.

Working of Kubernetes

Before exploring how Kubernetes operates, it's essential to grasp the concept of containers and their significance in modern application development. A container is a small, lightweight virtual machine (VM) that does not have device drivers and shares its operating system among the applications. It is a good way to bundle and run applications in a production environment. However, you need to manage these containers in a proper way so that there is no downtime. This is where Kubernetes comes to the rescue.

Kubernetes works as a “container orchestration system” that manages the lifecycle of containerized applications and automates the deployment of several containers. Containers running the same applications are usually grouped together into Pods. There can be one or multiple containers in a single Pod and each of them shares the same IP address and resources such as memory and storage. By grouping the containers in this manner, Kubernetes eliminates the need to cram multiple functionalities in one single container. There is a dedicated container orchestrator which supervises these groups and ensures that they operate correctly.

Kubernetes in DevOps

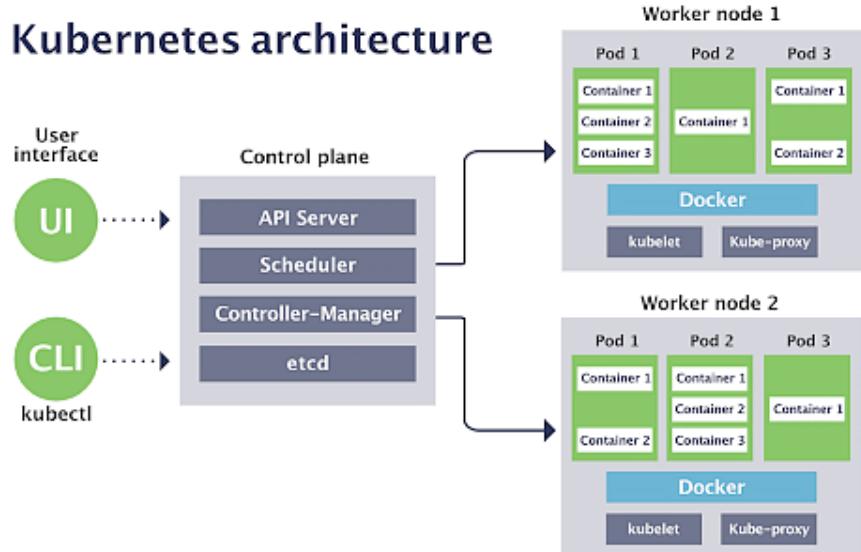
Kubernetes is more than just a container orchestration tool; it's a powerful enabler of DevOps practices. By bridging the gap between IT operations and development, Kubernetes fosters a collaborative DevOps environment, ensuring that software and its dependencies are shared seamlessly across different environments.

Kubernetes facilitates various stages of the software lifecycle, enhancing the build-test-deploy timeline:

- **Developer Environment:** Helps run software consistently in any setting, ensuring that applications behave the same across different environments.
- **QA/Testing Process:** Coordinates pipelines between test and production environments, streamlining the testing process.
- **Sys-Admin:** Once configured, Kubernetes runs anything, simplifying system administration tasks.
- **Operations:** Provides a comprehensive solution for building, shipping, and scaling software, making operations smoother and more efficient.

Kubernetes Cluster Architecture

A Kubernetes cluster consists of a set of worker machines, called nodes, that run containerized applications. The cluster is managed by a control plane, which is responsible for maintaining the desired state of the cluster, such as which applications are running and where they are running.



Control Plane: The control plane is the brain of the Kubernetes cluster, responsible for managing the desired state of the cluster, making decisions on scheduling, and responding to cluster events.

- **API Server:** The API server acts as the front-end for the Kubernetes control plane. It exposes the Kubernetes API, which is used by both internal components and external users (via CLI or UI) to communicate with the cluster.
- **Scheduler:** The scheduler is responsible for assigning newly created pods to nodes in the cluster. It evaluates the resource requirements of the pods against the available resources on the nodes, ensuring optimal placement.
- **Controller Manager:** This component runs various controllers that manage the state of the cluster. For example, it ensures that the number of pod replicas matches the desired configuration and handles node failures.
- **etcd:** A key-value store that holds all the configuration data for the Kubernetes cluster, including the current state and the desired state of the objects in the cluster. It is essential for maintaining cluster consistency and recovery.

Worker Nodes: Worker nodes are the machines where the application workloads run. Each worker node contains the services necessary to run pods and communicate with the control plane.

- **Kubelet:** The kubelet is an agent that runs on each worker node. It ensures that containers are running in a pod as expected by the control plane. It communicates with the API server to receive instructions and report back the status of the node and its workloads.
- **Kube-proxy:** Kube-proxy is a network proxy that runs on each worker node. It manages the networking for the pods, ensuring that each pod can communicate with others, both within and outside the cluster.
- **Docker (or other container runtimes):** Docker is the container runtime that runs and manages the containers on the worker nodes. It pulls container images from a registry, starts and stops containers, and manages container storage and networking.

User Interfaces: Users interact with the Kubernetes cluster through two primary interfaces:

- **UI (User Interface):** A graphical interface that provides an easy way to manage and monitor the cluster.
- **CLI (Command-Line Interface, e.g., kubectl):** A more powerful tool for managing the cluster, allowing users to interact with the API server directly via command-line commands.

This architecture allows Kubernetes to abstract away the underlying infrastructure, providing a consistent and scalable environment for deploying and managing containerized applications across different environments.

Conclusion: -

In conclusion, Kubernetes is a powerful, open-source platform that automates the deployment and management of containerized applications. Its architecture ensures seamless operation across diverse environments, promoting flexibility and scalability. By abstracting the underlying infrastructure and supporting DevOps practices, Kubernetes enhances the software development lifecycle. This results in streamlined operations, reduced downtime, and consistent application performance.

Install and Spin Up a Kubernetes Cluster on Linux Machines/Cloud Platforms.

- Create 3 EC2 instances, one for the master node and two for the worker nodes

The screenshot shows the AWS CloudFormation Launch Wizard Step 2. It includes sections for Instance type (t2.medium), Key pair (kubernetes_cluster), and Network settings (vpc-0d93715b8c7682b9a). A callout box highlights the 'Free tier' information: 'In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance'.

The screenshot shows the AWS CloudFormation Launch Wizard Step 3. It focuses on configuring security group rules. A callout box provides a warning: '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.'

The screenshot shows the AWS CloudWatch Metrics dashboard. It displays a table of terminated EC2 instances, including columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, and Public IP. The instances listed are master, worker-1, and worker-2, all of which were terminated successfully.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IP
master	i-04e60dd4f6abefca6	Running	t2.medium	Initializing	View alarms +	us-east-1b	ec2-44-222-207-187.co...	44.222.2
worker-1	i-04e6f01c6f2e6cd68	Running	t2.medium	Initializing	View alarms +	us-east-1b	ec2-54-146-243-168.co...	54.146.2
worker-2	i-0825e9af4a2bfa3cb	Running	t2.medium	Initializing	View alarms +	us-east-1b	ec2-3-80-70-36.comput...	3.80.70.3

- After the instances have been created, copy the text given in the example part of each of the three instances into git bash.

EC2 > Instances > i-0e65e6b3d1a332a44 > Connect to instance

Connect to instance Info

Connect to your instance i-0e65e6b3d1a332a44 (master) using any of these options

EC2 Instance Connect | **Session Manager** | **SSH client** | **EC2 serial console**

Instance ID
i-0e65e6b3d1a332a44 (master)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is kubernetes_cluster.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 "kubernetes_cluster.pem"
4. Connect to your instance using its Public DNS:
ec2-54-211-197-39.compute-1.amazonaws.com

Example:
ssh -i "kubernetes_cluster.pem" ubuntu@ec2-54-211-197-39.compute-1.amazonaws.com

Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Cancel

```
ubuntu@ip-172-31-29-63: ~
Microsoft Windows [Version 10.0.22631.4112]
(c) Microsoft Corporation. All rights reserved.

C:\Users\TEJAS\Downloads>ssh -i "kubernetes_cluster.pem" ubuntu@ec2-54-211-197-39.compute-1.amazonaws.com
The authenticity of host 'ec2-54-211-197-39.compute-1.amazonaws.com (54.211.197.39)' can't be established.
ED25519 key fingerprint is SHA256:E7RRK6LxQFHSmWLb8zgsskyIdj0YXpInW0B08/5vnA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-211-197-39.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1022-aws x86_64)

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

System information as of Sun Sep 15 17:48:58 UTC 2024

 System load:  0.28      Processes:           115
 Usage of /:   20.7% of  7.57GB   Users logged in:     0
 Memory usage: 5%          IPv4 address for eth0: 172.31.29.63
 Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.
```

- Update the package manager on all nodes:

```
ubuntu@ip-172-31-29-63: ~
$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1806 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8372 B]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2023 kB]
Get:13 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [295 kB]
Get:14 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [13.3 kB]
Get:15 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [2377 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [352 kB]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [17.8 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [2437 kB]
Get:19 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [409 kB]
Get:20 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [584 B]
Get:21 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [902 kB]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [419 kB]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [616 B]
```

➤ Installing Required Packages for HTTPS and Certificate Transport on Ubuntu

```
ubuntu@ip-172-31-29-63:~$ sudo apt-get install -y apt-transport-https ca-certificates curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ca-certificates is already the newest version (20230311ubuntu0.22.04.1).
ca-certificates set to manually installed.
The following NEW packages will be installed:
  apt-transport-https
The following packages will be upgraded:
  curl libcurl4
2 upgraded, 1 newly installed, 0 to remove and 67 not upgraded.
Need to get 485 kB of archives.
After this operation, 170 kB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 apt-transport-https all 2.4.13 [1510 B]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 curl amd64 7.81.0-1ubuntu1.17 [194 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libcurl4 amd64 7.81.0-1ubuntu1.17 [290 kB]
Fetched 485 kB in 0s (17.3 MB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 65320 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.4.13_all.deb ...
Unpacking apt-transport-https (2.4.13) ...
Preparing to unpack .../curl_7.81.0-1ubuntu1.17_amd64.deb ...
Unpacking curl (7.81.0-1ubuntu1.17) over (7.81.0-1ubuntu1.16) ...
```

➤ Installing Docker on Ubuntu

```
ubuntu@ip-172-31-29-63:~$ sudo apt install docker.io -y
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-doc rinse zfs-fuse | zfsutils
The following NEW packages will be installed:
  bridge-utils containerd dns-root-data dnsmasq-base docker.io pigz runc ubuntu-fan
0 upgraded, 8 newly installed, 0 to remove and 67 not upgraded.
Need to get 75.5 MB of archives.
After this operation, 284 MB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 pigz amd64 2.6-1 [63.6 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 bridge-utils amd64 1.7-1ubuntu3 [34.4 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 runc amd64 1.1.12-0ubuntu2~22.04.1 [8405 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 containerd amd64 1.7.12-0ubuntu2~22.04.1 [37.8 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 dns-root-data all 2023112702~ubuntu0.22.04.1 [5136 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 dnsmasq-base amd64 2.90-0ubuntu0.22.04.1 [374 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 docker.io amd64 24.0.7-0ubuntu2~22.04.
```

➤ Enabling Docker and Disabling Swap on Ubuntu

```
ubuntu@ip-172-31-29-63:~$ sudo systemctl enable --now docker
ubuntu@ip-172-31-29-63:~$ sudo swapoff -a
```

➤ Load necessary kernel modules for networking and iptables:

```
ubuntu@ip-172-31-29-63:~$ cat <<EOF | sudo tee /etc/modules-load.d/k8s.conf
overlay
br_netfilter
EOF
overlay
br_netfilter
ubuntu@ip-172-31-29-63:~$ sudo modprobe overlay
sudo modprobe br_netfilter
```

➤ Configure sysctl settings for Kubernetes networking:

```
ubuntu@ip-172-31-29-63:~$ cat <<EOF | sudo tee /etc/sysctl.d/k8s.conf
net.bridge.bridge-nf-call-iptables = 1
net.bridge.bridge-nf-call-ip6tables = 1
net.ipv4.ip_forward = 1
EOF
net.bridge.bridge-nf-call-iptables = 1
net.bridge.bridge-nf-call-ip6tables = 1
net.ipv4.ip_forward = 1

ubuntu@ip-172-31-29-63:~$ sudo sysctl --system
* Applying /etc/sysctl.d/10-console-messages.conf ...
kernel.printk = 4 4 1 7
* Applying /etc/sysctl.d/10-ipv6-privacy.conf ...
net.ipv6.conf.all.use_tempaddr = 2
net.ipv6.conf.default.use_tempaddr = 2
* Applying /etc/sysctl.d/10-kernel-hardening.conf ...
kernel.kptr_restrict = 1
* Applying /etc/sysctl.d/10-magic-sysrq.conf ...
kernel.sysrq = 176
* Applying /etc/sysctl.d/10-network-security.conf ...
net.ipv4.conf.default.rp_filter = 2
net.ipv4.conf.all.rp_filter = 2
* Applying /etc/sysctl.d/10-ptrace.conf ...
kernel.yama.ptrace_scope = 1
* Applying /etc/sysctl.d/10-zero-page.conf ...
vm.mmap_min_addr = 65536
* Applying /etc/sysctl.d/50-cloudimg-settings.conf ...
net.ipv4.neigh.default.gc_thresh2 = 15360
net.ipv4.neigh.default.gc_thresh3 = 16384
net.netfilter.nf_conntrack_max = 1048576
* Applying /usr/lib/sysctl.d/50-default.conf ...
kernel.core_uses_pid = 1
net.ipv4.conf.default.rp_filter = 2
```

➤ Install Kubernetes tools on all nodes.

```
ubuntu@ip-172-31-29-63:~$ curl -fsSL https://pkgs.k8s.io/core:/stable:/v1.29/deb/Release.key | sudo gpg --dearmor -o /etc/apt/keyrings/kubernetes-apt-keyring.gpg
echo 'deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:/v1.29/deb/ /' | sudo tee /etc/apt/sources.list.d/kubernetes.list
deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:/v1.29/deb/ /

ubuntu@ip-172-31-29-63:~$ sudo apt-get update -y
sudo apt-get install -y kubelet="1.29.0-*" kubectl="1.29.0-*" kubeadm="1.29.0-*"
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Get:5 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:/v1.29/deb InRelease [1189 B]
Get:6 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:/v1.29/deb Packages [14.0 kB]
Fetched 15.1 kB in 0s (31.9 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Selected version '1.29.0-1.1' (isv:kubernetes:core:stable:v1.29:pkgs.k8s.io [amd64]) for 'kubelet'
Selected version '1.29.0-1.1' (isv:kubernetes:core:stable:v1.29:pkgs.k8s.io [amd64]) for 'kubectl'
Selected version '1.29.0-1.1' (isv:kubernetes:core:stable:v1.29:pkgs.k8s.io [amd64]) for 'kubeadm'
The following additional packages will be installed:
  conntrack cri-tools ebtables kubernetes-cni socat
The following NEW packages will be installed:

ubuntu@ip-172-31-29-63:~$ sudo apt-mark hold kubelet kubeadm kubectl
kubelet set on hold.
kubeadm set on hold.
kubectl set on hold.
```

ONLY ON MASTER NODE

➤ Initialize the Kubernetes Cluster on Master Node

```
ubuntu@ip-172-31-29-63:~$ sudo kubeadm init --pod-network-cidr=10.244.0.0/16
I0915 17:58:19.113429    3356 version.go:256] remote version is much newer: v1.31.0; falling back to: stable-1.29
[init] Using Kubernetes version: v1.29.8
[preflight] Running pre-flight checks
[preflight] Pulling images required for setting up a Kubernetes cluster
[preflight] This might take a minute or two, depending on the speed of your internet connection
[preflight] You can also perform this action in beforehand using 'kubeadm config images pull'
W0915 17:58:28.696218    3356 checks.go:835] detected that the sandbox image "registry.k8s.io/pause:3.8" of the container runtime is inconsistent with that used by kubeadm. It is recommended that using "registry.k8s.io/pause:3.9" as the CRI sandbox image.
[certs] Using certificateDir folder "/etc/kubernetes/pki"
[certs] Generating "ca" certificate and key
[certs] Generating "apiserver" certificate and key
[certs] apiserver serving cert is signed for DNS names [ip-172-31-29-63 kubernetes kubernetes.default kubernetes.default.svc kubernetes.default.svc.cluster.local] and IPs [10.96.0.1 172.31.29.63]
[certs] Generating "apiserver-kubelet-client" certificate and key
[certs] Generating "front-proxy-ca" certificate and key
[certs] Generating "front-proxy-client" certificate and key
[certs] Generating "etcd/ca" certificate and key
[certs] Generating "etcd/server" certificate and key
[certs] etcd/server serving cert is signed for DNS names [ip-172-31-29-63 localhost] and IPs [172.31.29.63 127.0.0.1 ::1]
[certs] Generating "etcd/peer" certificate and key
[certs] etcd/peer serving cert is signed for DNS names [ip-172-31-29-63 localhost] and IPs [172.31.29.63 127.0.0.1 ::1]
```

```
ubuntu@ip-172-31-29-63:~$ 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 172.31.29.63:6443 --token 05rvqu.66v5246nmoe81d5e \
--discovery-token-ca-cert-hash sha256:ff6e3056ea0d41a598919b1be9dbe765739c40a5aa6d37b5e4cbc45b1256c1c7
```

➤ Set up kubectl on the master node

```
ubuntu@ip-172-31-29-63:~$ mkdir -p $HOME/.kube
sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
sudo chown $(id -u):$(id -g) $HOME/.kube/config
```

```
ubuntu@ip-172-31-29-63:~$ kubectl get nodes
NAME           STATUS      ROLES   AGE     VERSION
ip-172-31-29-63   NotReady   control-plane   3m      v1.29.0
ubuntu@ip-172-31-29-63:~$ |
```

➤ To enable communication between pods, install a pod network plugin like Flannel or Calico

```
ubuntu@ip-172-31-29-63:~$ sudo systemctl restart kubelet
ubuntu@ip-172-31-29-63:~$ mkdir -p $HOME/.kube
sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
sudo chown $(id -u):$(id -g) $HOME/.kube/config
cp: overwrite '/home/ubuntu/.kube/config'? y
ubuntu@ip-172-31-29-63:~$ kubectl apply -f https://raw.githubusercontent.com/coreos/flannel/master/Documentation/kube-flannel.yml
namespace/kube-flannel created
clusterrole.rbac.authorization.k8s.io/flannel created
clusterrolebinding.rbac.authorization.k8s.io/flannel created
serviceaccount/flannel created
configmap/kube-flannel-cfg created
daemonset.apps/kube-flannel-ds created
ubuntu@ip-172-31-29-63:~$ |

ubuntu@ip-172-31-29-63:~$ kubeadm token create --print-join-command
kubeadm join 172.31.29.63:6443 --token avprdu.7xw3ox1x6l9w6zf9 --discovery-token-ca-cert-hash sha256:ff6e3056ea0d41a598919b1be9dbe765739c40a5aa6d37b5e4cbc45b1256c1c7
ubuntu@ip-172-31-29-63:~$ |
```

ONLY ON WORKER NODES

- Join Worker Nodes to the Cluster

```
ubuntu@ip-172-31-20-115:~$ sudo kubeadm reset pre-flight checks
W0915 18:24:16.207647    3366 preflight.go:56] [reset] WARNING: Changes made to this host by 'kubeadm init' or 'kubeadm
join' will be reverted.
[reset] Are you sure you want to proceed? [y/N]: y
[preflight] Running pre-flight checks
W0915 18:24:24.608981    3366 removeetcdmember.go:106] [reset] No kubeadm config, using etcd pod spec to get data direct
ory
[reset] Deleted contents of the etcd data directory: /var/lib/etcd
[reset] Stopping the kubelet service
[reset] Unmounting mounted directories in "/var/lib/kubelet"
[reset] Deleting contents of directories: [/etc/kubernetes/manifests /var/lib/kubelet /etc/kubernetes/pki]
[reset] Deleting files: [/etc/kubernetes/admin.conf /etc/kubernetes/super-admin.conf /etc/kubernetes/kubelet.conf /etc/k
ubernetes/bootstrap-kubelet.conf /etc/kubernetes/controller-manager.conf /etc/kubernetes/scheduler.conf]

The reset process does not clean CNI configuration. To do so, you must remove /etc/cni/net.d

The reset process does not reset or clean up iptables rules or IPVS tables.
If you wish to reset iptables, you must do so manually by using the "iptables" command.

If your cluster was setup to utilize IPVS, run ipvsadm --clear (or similar)
to reset your system's IPVS tables.
```

- On the worker nodes, run the command provided by the master node during initialization . It looks something like this: sudo kubeadm join :6443 --token --discovery-token-ca-cert- hash sha256:

```
ubuntu@ip-172-31-20-115:~$ sudo kubeadm join 172.31.29.63:6443 --token avprdu.7xw3ox1x6l9w6zfw --discovery-token-ca-cer
t-hash sha256:ff6e3056ea0d41a598919b1be9dbe765739c40a5aa6d37b5e4cbc45b1256c1c7 --v=5
I0915 18:26:15.816542    3382 join.go:413] [preflight] found NodeName empty; using OS hostname as NodeName
I0915 18:26:15.816650    3382 initconfiguration.go:122] detected and using CRI socket: unix:///var/run/containerd/contai
nerd.sock
[preflight] Running pre-flight checks
I0915 18:26:15.816686    3382 preflight.go:93] [preflight] Running general checks
I0915 18:26:15.816765    3382 checks.go:280] validating the existence of file /etc/kubernetes/kubelet.conf
I0915 18:26:15.816774    3382 checks.go:280] validating the existence of file /etc/kubernetes/bootstrap-kubelet.conf
I0915 18:26:15.816784    3382 checks.go:104] validating the container runtime
I0915 18:26:15.833043    3382 checks.go:639] validating whether swap is enabled or not
I0915 18:26:15.833129    3382 checks.go:370] validating the presence of executable crictl
I0915 18:26:15.833152    3382 checks.go:370] validating the presence of executable conctrack
I0915 18:26:15.833171    3382 checks.go:370] validating the presence of executable ip
I0915 18:26:15.833203    3382 checks.go:370] validating the presence of executable iptables
I0915 18:26:15.833227    3382 checks.go:370] validating the presence of executable mount
I0915 18:26:15.833242    3382 checks.go:370] validating the presence of executable nsenter
I0915 18:26:15.833276    3382 checks.go:370] validating the presence of executable ebtables
I0915 18:26:15.833292    3382 checks.go:370] validating the presence of executable ethtool
I0915 18:26:15.833320    3382 checks.go:370] validating the presence of executable socat
I0915 18:26:15.833340    3382 checks.go:370] validating the presence of executable tc

ootstrap-kubelet.conf
I0915 18:26:15.933343    3382 kubelet.go:136] [kubelet-start] writing CA certificate at /etc/kubernetes/pki/ca.crt
I0915 18:26:15.933723    3382 kubelet.go:157] [kubelet-start] Checking for an existing Node in the cluster with name "ip
-172-31-20-115" and status "Ready"
I0915 18:26:15.936219    3382 kubelet.go:172] [kubelet-start] Stopping the kubelet
[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-start] Waiting for the kubelet to perform the TLS Bootstrap...
I0915 18:26:17.103583    3382 cert_rotation.go:137] Starting client certificate rotation controller
I0915 18:26:17.104245    3382 kubelet.go:220] [kubelet-start] preserving the crisocket information for the node
I0915 18:26:17.104261    3382 patchnode.go:31] [patchnode] Uploading the CRI Socket information "unix:///var/run/contain
erd/containerd.sock" to the Node API object "ip-172-31-20-115" as an annotation

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@ip-172-31-20-115:~$ |
```

➤ Verify the Cluster

Once the worker node joins, check the status on the master node

```
ubuntu@ip-172-31-29-63:~$ kubectl get nodes
NAME      STATUS   ROLES     AGE   VERSION
ip-172-31-20-115 Ready    <none>   27m   v1.29.0
ip-172-31-20-200 Ready    <none>   24m   v1.29.0
ip-172-31-29-63  Ready    control-plane  55m   v1.29.0
ubuntu@ip-172-31-29-63:~$ |
```

EXPERIMENT NO: - 04

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

➤ Install Kubectl on Ubuntu

Installing Required Packages for HTTPS and Certificate Transport on Ubuntu

```
ubuntu@ip-172-31-29-63:~$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1806 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8372 B]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2023 kB]
Get:13 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [295 kB]
Get:14 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [13.3 kB]
Get:15 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [2377 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [352 kB]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [17.8 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [2437 kB]
Get:19 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [409 kB]
Get:20 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [584 B]
Get:21 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [902 kB]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [419 kB]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [616 B]
```

```
ubuntu@ip-172-31-29-63:~$ sudo apt-get install -y apt-transport-https ca-certificates curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ca-certificates is already the newest version (20230311ubuntu0.22.04.1).
ca-certificates set to manually installed.
The following NEW packages will be installed:
  apt-transport-https
The following packages will be upgraded:
  curl libcurl4
2 upgraded, 1 newly installed, 0 to remove and 67 not upgraded.
Need to get 485 kB of archives.
After this operation, 170 kB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 apt-transport-https all 2.4.13 [1510 B]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 curl amd64 7.81.0-1ubuntu1.17 [194 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libcurl4 amd64 7.81.0-1ubuntu1.17 [290 kB]
Fetched 485 kB in 0s (17.3 MB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 65320 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.4.13_all.deb ...
Unpacking apt-transport-https (2.4.13) ...
Preparing to unpack .../curl_7.81.0-1ubuntu1.17_amd64.deb ...
Unpacking curl (7.81.0-1ubuntu1.17) over (7.81.0-1ubuntu1.16) ...
```

Add the GPG key & repository for Kubernetes

```
ubuntu@ip-172-31-29-63:~$ curl -fsSL https://pkgs.k8s.io/core:/stable:/v1.29/deb/Release.key | sudo gpg --dearmor -o /etc/apt/keyrings/kubernetes-apt-keyring.gpg
echo 'deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:/v1.29/deb/ /' | sudo tee /etc/apt/sources.list.d/kubernetes.list
deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:/v1.29/deb/ /
```

Configure sysctl settings for Kubernetes networking

```
ubuntu@ip-172-31-29-63:~$ sudo sysctl --system
* Applying /etc/sysctl.d/10-console-messages.conf ...
kernel.printk = 4 4 1 7
* Applying /etc/sysctl.d/10-ipv6-privacy.conf ...
net.ipv6.conf.all.use_tempaddr = 2
net.ipv6.conf.default.use_tempaddr = 2
* Applying /etc/sysctl.d/10-kernel-hardening.conf ...
kernel.kptr_restrict = 1
* Applying /etc/sysctl.d/10-magic-sysrq.conf ...
kernel.sysrq = 176
* Applying /etc/sysctl.d/10-network-security.conf ...
net.ipv4.conf.default.rp_filter = 2
net.ipv4.conf.all.rp_filter = 2
* Applying /etc/sysctl.d/10-ptrace.conf ...
kernel.yama.ptrace_scope = 1
* Applying /etc/sysctl.d/10-zero-page.conf ...
vm.mmap_min_addr = 65536
* Applying /etc/sysctl.d/50-cloudimg-settings.conf ...
net.ipv4.neigh.default.gc_thresh2 = 15360
net.ipv4.neigh.default.gc_thresh3 = 16384
net.netfilter.nf_conntrack_max = 1048576
* Applying /usr/lib/sysctl.d/50-default.conf ...
kernel.core_uses_pid = 1
net.ipv4.conf.default.rp_filter = 2
```

Install Kubernetes tools on all nodes.

```
ubuntu@ip-172-31-29-63:~$ sudo apt-get update -
sudo apt-get install -y kubelet="1.29.0-*" kubectl="1.29.0-*" kubeadm="1.29.0-*"
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Get:5 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:/v1.29/deb InRelease [1189 B]
Get:6 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:/v1.29/deb Packages [14.0 kB]
Fetched 15.1 kB in 0s (31.9 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Selected version '1.29.0-1.1' (isv:kubernetes:core:stable:v1.29:pkgs.k8s.io [amd64]) for 'kubelet'
Selected version '1.29.0-1.1' (isv:kubernetes:core:stable:v1.29:pkgs.k8s.io [amd64]) for 'kubectl'
Selected version '1.29.0-1.1' (isv:kubernetes:core:stable:v1.29:pkgs.k8s.io [amd64]) for 'kubeadm'
The following additional packages will be installed:
  conntrack cri-tools ebtables kubernetes-cni socat
The following NEW packages will be installed:
```

➤ Set up Kubernetes Cluster

If you haven't already set up a Kubernetes cluster (e.g., with kubeadm), use minikube or any managed Kubernetes service (like EKS, GKE, etc.) to get a cluster running. Once your cluster is ready, verify the nodes: kubectl get nodes

```
ubuntu@ip-172-31-29-63:~$ kubectl get nodes
NAME      STATUS   ROLES      AGE     VERSION
ip-172-31-20-115 Ready    <none>    27m    v1.29.0
ip-172-31-20-200 Ready    <none>    24m    v1.29.0
ip-172-31-29-63  Ready    control-plane  55m    v1.29.0
ubuntu@ip-172-31-29-63:~$ |
```

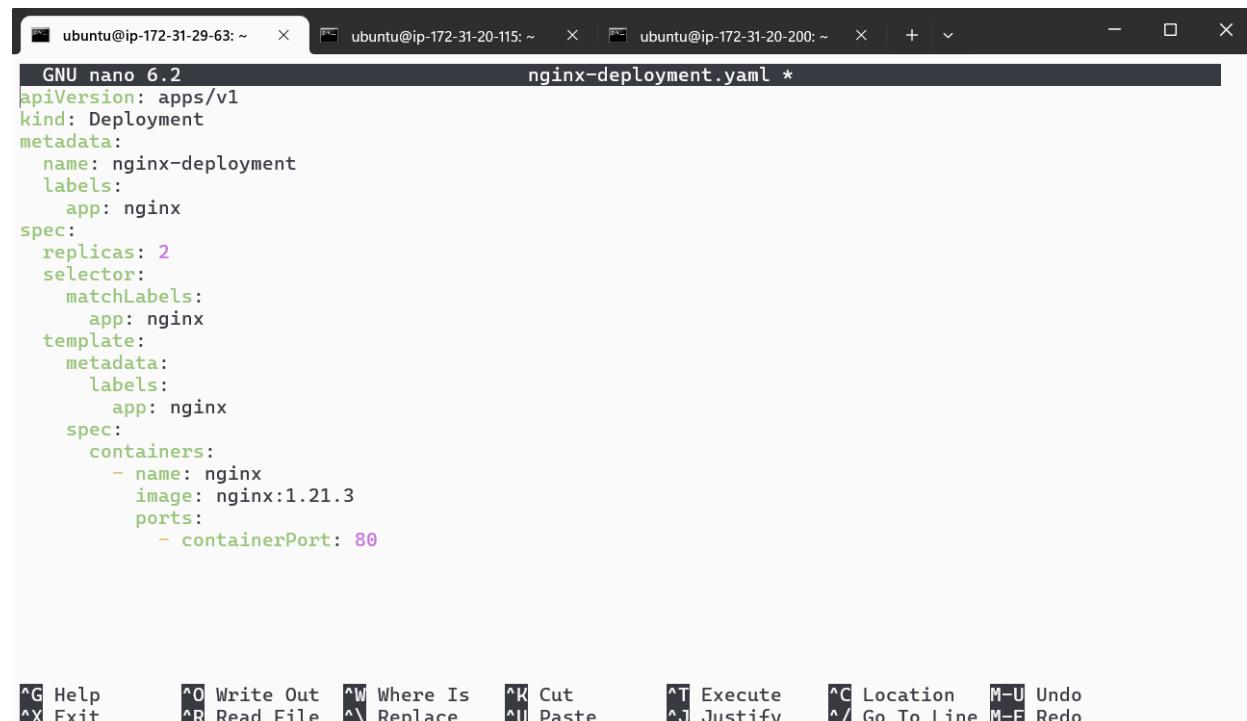
➤ Deploying Your Application on Kubernetes

Create the Deployment YAML file

Create the YAML file: Use a text editor to create a file named nginx-deployment.yaml

```
ubuntu@ip-172-31-29-63:~$ nano nginx-deployment.yaml
ubuntu@ip-172-31-29-63:~$ |
```

Add the Deployment Configuration: Copy and paste the following YAML content into the file. Save and exit the editor (Press Ctrl+X, then Y, and Enter).



```
GNU nano 6.2                                     nginx-deployment.yaml *
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  labels:
    app: nginx
spec:
  replicas: 2
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
        - name: nginx
          image: nginx:1.21.3
          ports:
            - containerPort: 80
```

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

Create the Service YAML File: Create another file named nginx-service.yaml

```
ubuntu@ip-172-31-29-63:~$ nano nginx-service.yaml
ubuntu@ip-172-31-29-63:~$ |
```

Add the Service Configuration: Copy and paste the following YAML content into the file given below.

```

ubuntu@ip-172-31-29-63:~$ nano nginx-service.yaml
GNU nano 6.2
apiVersion:v1
kind: Service
metadata:
  name:nginx-service
spec:
  selector:
    app: nginx
  ports:
    - protocol: TCP
      port: 80
      targetPort: 80
  type: LoadBalancer

```

Deploy the Application: Use kubectl to create the Deployment and Service from the YAML files.

```
ubuntu@ip-172-31-29-63:~$ kubectl apply -f nginx-deployment.yaml --validate=false
deployment.apps/nginx-deployment created
```

```
ubuntu@ip-172-31-29-63:~$ kubectl apply -f nginx-service.yaml --validate=false
service/nginx-service created
ubuntu@ip-172-31-29-63:~$ |
```

Verify the Deployment: Check the status of your Deployment, Pods and Services

```
ubuntu@ip-172-31-29-63:~$ kubectl get deployments
NAME          READY   UP-TO-DATE   AVAILABLE   AGE
nginx-deployment   1/2       2           1          9m25s
ubuntu@ip-172-31-29-63:~$ kubectl get pods
NAME                           READY   STATUS    RESTARTS   AGE
nginx-deployment-6b4d6fdbf-6w4bm   1/1     Running   4 (98s ago)   9m18s
nginx-deployment-6b4d6fdbf-bhcwm   1/1     Running   4 (70s ago)   9m18s
ubuntu@ip-172-31-29-63:~$ kubectl get services
NAME          TYPE      CLUSTER-IP   EXTERNAL-IP   PORT(S)   AGE
kubernetes   ClusterIP  10.96.0.1   <none>        443/TCP   111m
nginx-service   LoadBalancer  10.110.88.111   <pending>    80:30132/TCP   110s
ubuntu@ip-172-31-29-63:~$ |
```

Describe the deployment

```
ubuntu@ip-172-31-29-63:~$ kubectl get deployments
NAME      READY   UP-TO-DATE   AVAILABLE   AGE
nginx-deployment  2/2     2          2           11m
ubuntu@ip-172-31-29-63:~$ kubectl describe deployment
Name:            nginx-deployment
Namespace:       default
CreationTimestamp: Sun, 15 Sep 2024 19:39:41 +0000
Labels:          app=nginx
Annotations:    deployment.kubernetes.io/revision: 1
Selector:        app=nginx
Replicas:       2 desired | 2 updated | 2 total | 1 available | 1 unavailable
StrategyType:   RollingUpdate
MinReadySeconds: 0
RollingUpdateStrategy: 25% max unavailable, 25% max surge
Pod Template:
  Labels:  app=nginx
  Containers:
    nginx:
      Image:      nginx:1.21.3
      Port:       80/TCP
      Host Port:  0/TCP
      Environment: <none>
      Mounts:      <none>
      Volumes:     <none>
  Conditions:
    Type        Status  Reason
    ----        ----   -----
    Progressing  True    NewReplicaSetAvailable
    Available   False   MinimumReplicasUnavailable
OldReplicaSets: <none>
NewReplicaSet:  nginx-deployment-6b4d6fdbf (2/2 replicas created)
Events:
  Type      Reason     Age   From           Message
  ----      ----     --   --   -----
  Normal   ScalingReplicaSet  11m  deployment-controller  Scaled up replica set nginx-deployment-6b4d6fdbf to 2
ubuntu@ip-172-31-29-63:~$ |
```

Verify Service: Run the following command to check the services running in your cluster:

```
ubuntu@ip-172-31-29-63:~$ kubectl get service
NAME      TYPE      CLUSTER-IP      EXTERNAL-IP      PORT(S)      AGE
kubernetes  ClusterIP  10.96.0.1    <none>        443/TCP      114m
nginx-service  LoadBalancer  10.110.88.111  <pending>    80:30132/TCP  4m59s
ubuntu@ip-172-31-29-63:~$ |
```

Forward the Service Port to Your Local Machine

```
ubuntu@ip-172-31-45-227:~$ kubectl port-forward service/nginx-service 8080:80
Forwarding from 127.0.0.1:8080 -> 80
Forwarding from [::1]:8080 -> 80
```

```
ubuntu@ip-172-31-45-227:~$ kubectl port-forward service/nginx-service 8080:80
Forwarding from 127.0.0.1:8080 -> 80
Forwarding from [::1]:8080 -> 80
^Cubuntu@ip-172-31-45-227:~$ kubectl port-forward service/nginx-service 8081:8080
Forwarding from 127.0.0.1:8081 -> 80
Forwarding from [::1]:8081 -> 80
^Cubuntu@ip-172-31-45-227:~$ kubectl get pods
NAME                  READY   STATUS    RESTARTS   AGE
nginx-deployment-776b8fd845-k9cx4  1/1     Running   0          113m
ubuntu@ip-172-31-45-227:~$ kubectl logs nginx-deployment-776b8fd845-k9cx4
/docker-entrypoint.sh: /docker-entrypoint.d/ is not empty, will attempt to perform configuration
/docker-entrypoint.sh: Looking for shell scripts in /docker-entrypoint.d/
/docker-entrypoint.sh: Launching /docker-entrypoint.d/10-listen-on-ipv6-by-default.sh
10-listen-on-ipv6-by-default.sh: info: Getting the checksum of /etc/nginx/conf.d/default.conf
10-listen-on-ipv6-by-default.sh: info: Enabled listen on IPv6 in /etc/nginx/conf.d/default.conf
/docker-entrypoint.sh: Sourcing /docker-entrypoint.d/15-local-resolvers.envsh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/20-envsubst-on-templates.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/30-tune-worker-processes.sh
/docker-entrypoint.sh: Configuration complete; ready for start up
2024/09/12 06:35:51 [notice] 1#1: using the "epoll" event method
2024/09/12 06:35:51 [notice] 1#1: nginx/1.27.1
2024/09/12 06:35:51 [notice] 1#1: built by gcc 12.2.0 (Debian 12.2.0-14)
2024/09/12 06:35:51 [notice] 1#1: OS: Linux 6.5.0-1022-aws
2024/09/12 06:35:51 [notice] 1#1: getrlimit(RLIMIT_NOFILE): 1048576:1048576
2024/09/12 06:35:51 [notice] 1#1: start worker processes
2024/09/12 06:35:51 [notice] 1#1: start worker process 24
2024/09/12 06:35:51 [notice] 1#1: start worker process 25
```

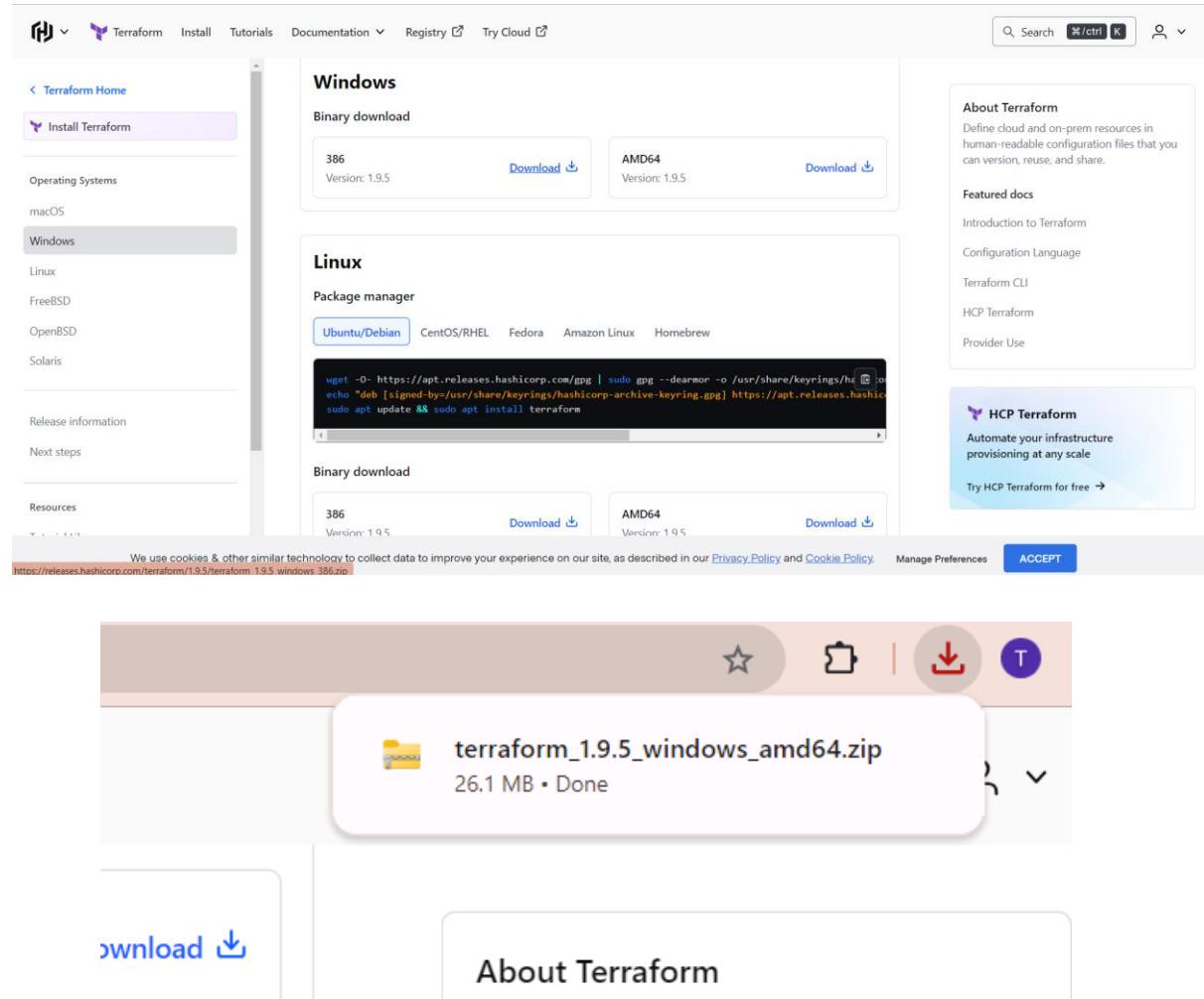
Access the Application Locally

Open a Web Browser: Now open your web browser and go to the following URL:
http://localhost:8080 You should see the application (in this case, Nginx) that you have deployed running in the Kubernetes cluster, served locally via port 8080.

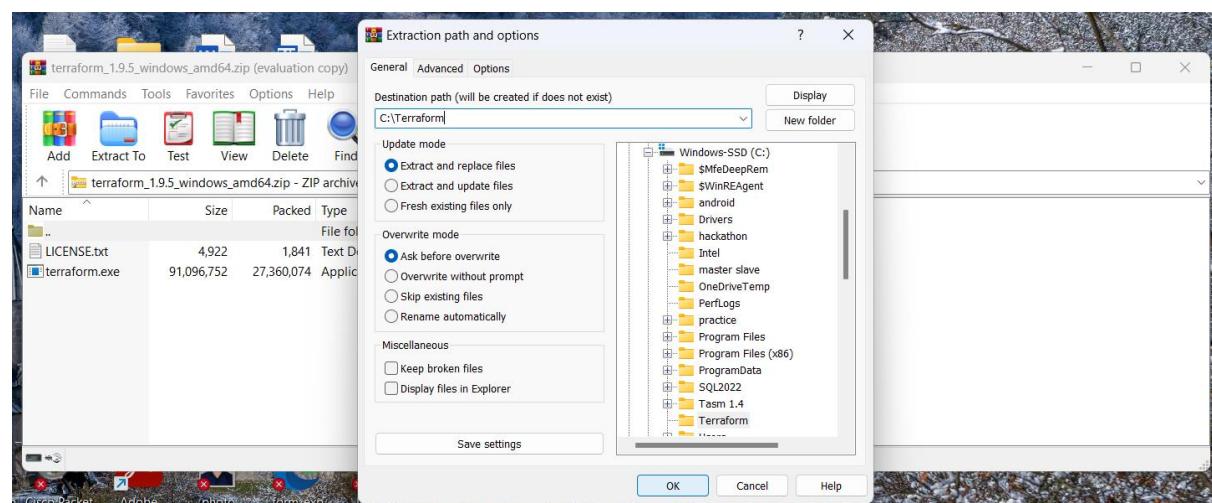


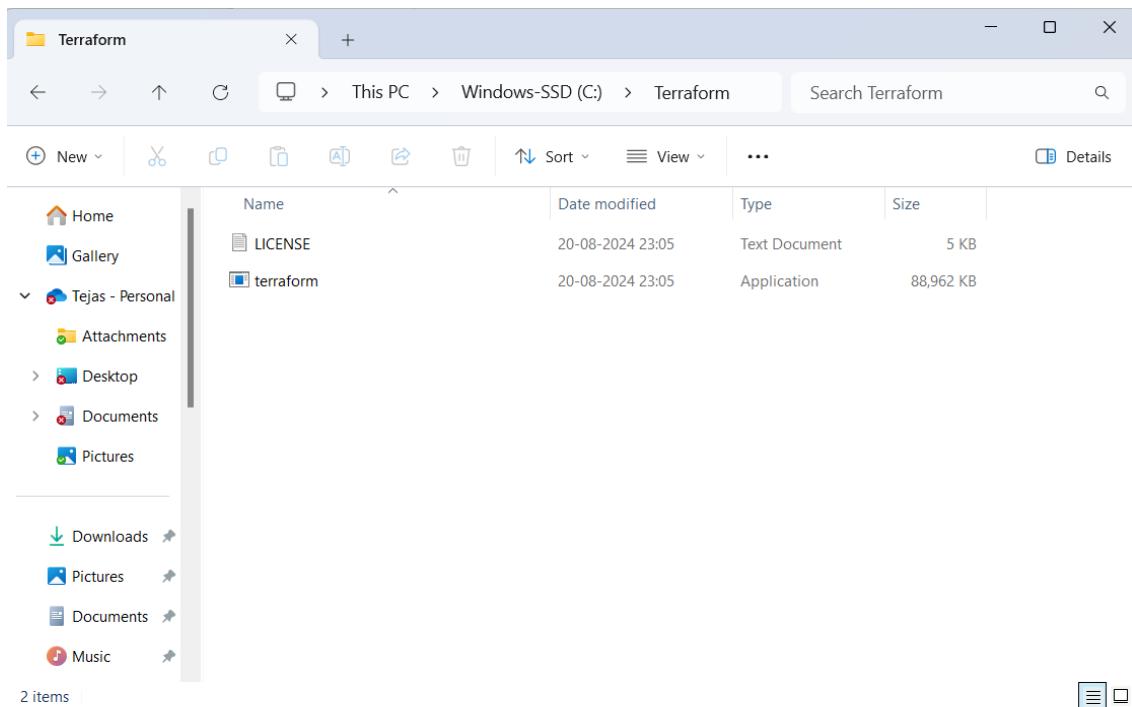
EXPERIMENT NO: - 05

➤ **Terraform installation on Windows**

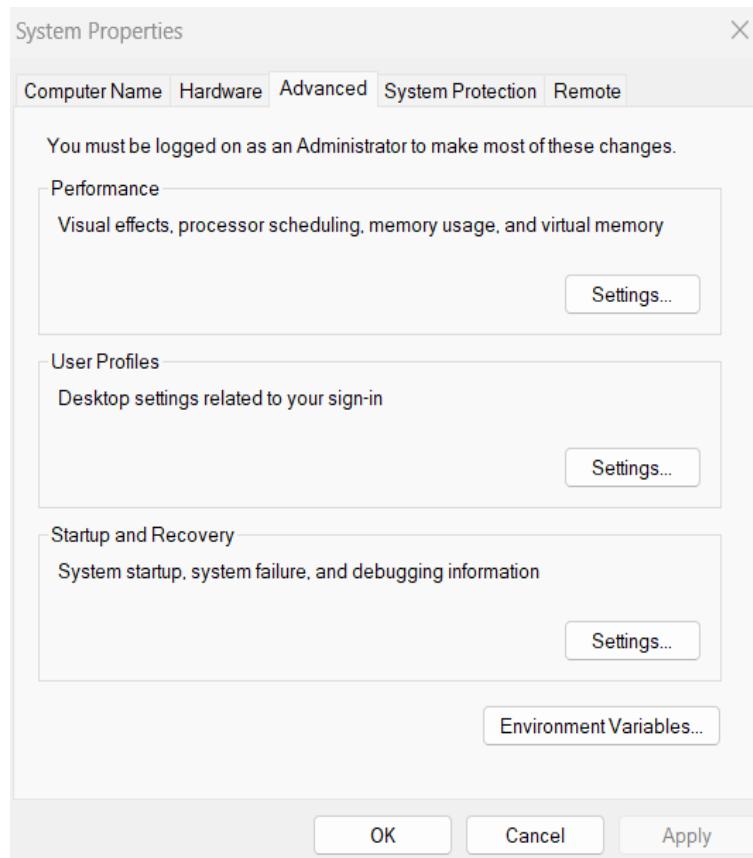


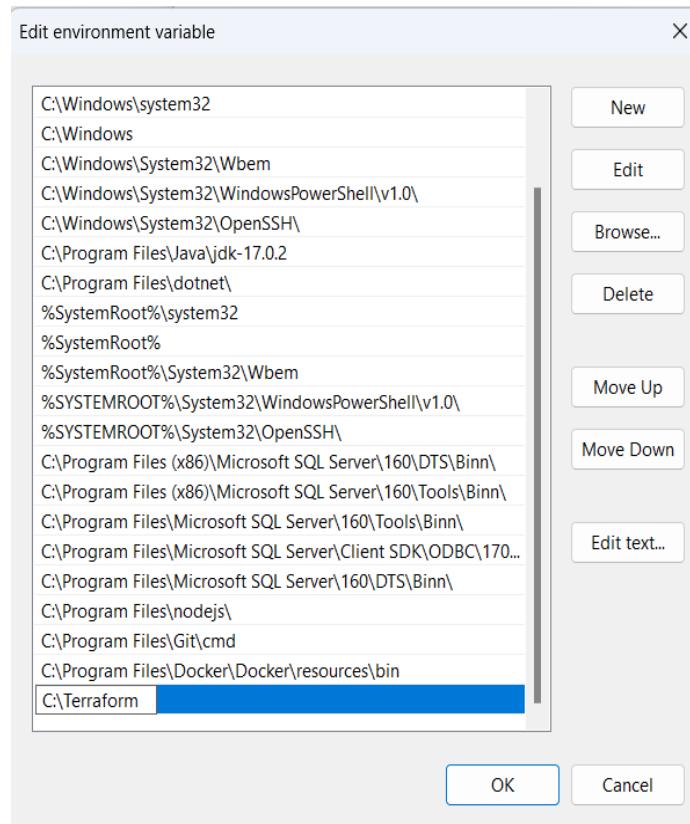
➤ Extract the downloaded setup file Terraform.exe in C:\Terraform directory





➤ Set the System path for Terraform in Environment Variables





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

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

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

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

Global options (use these before the subcommand, if any):
  -chdir=DIR  Switch to a different working directory before executing the
              given subcommand.
  -help       Show this help output, or the help for a specified subcommand.
  -version    An alias for the "version" subcommand.
```

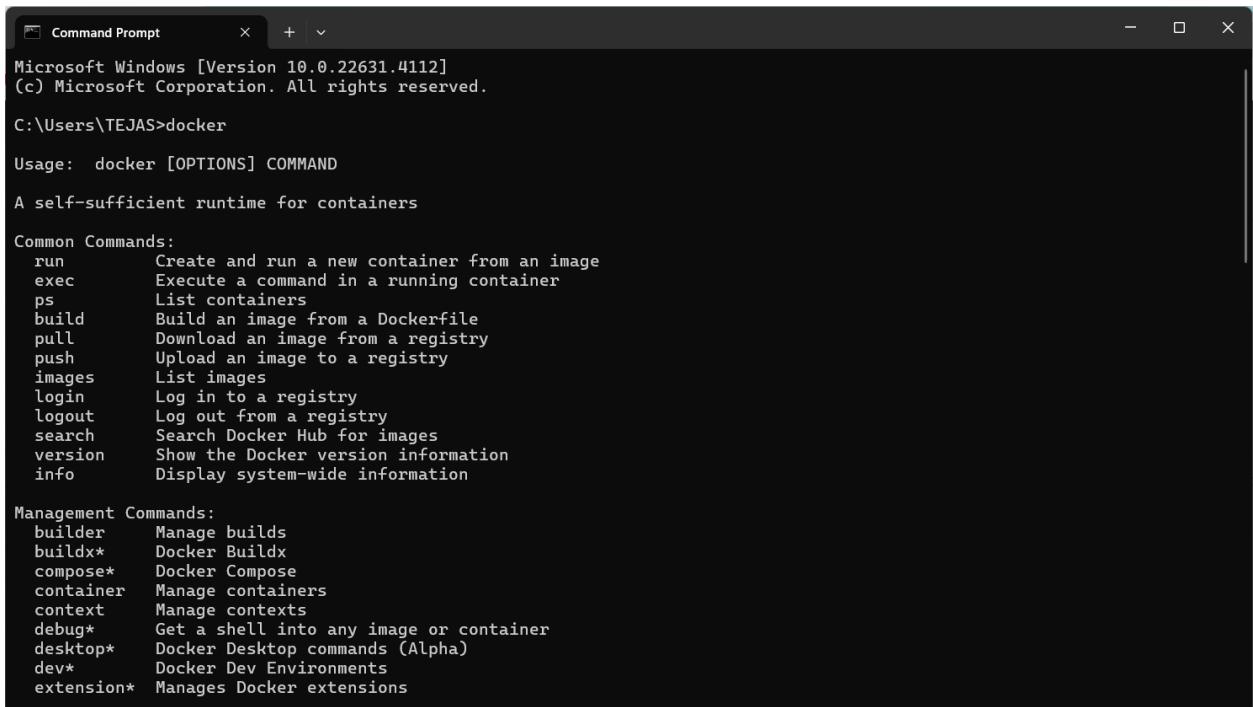
```
PS C:\Users\TEJAS> terraform --version
Terraform v1.9.5
on windows_amd64
PS C:\Users\TEJAS> docker --version
Docker version 27.0.3, build 7d4bcd8
PS C:\Users\TEJAS> |
```

EXPERIMENT NO: - 06

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

A] Create Docker Image using Terraform

- Checking the Docker Functionality



```
Command Prompt      X + ▾
Microsoft Windows [Version 10.0.22631.4112]
(c) Microsoft Corporation. All rights reserved.

C:\Users\TEJAS>docker

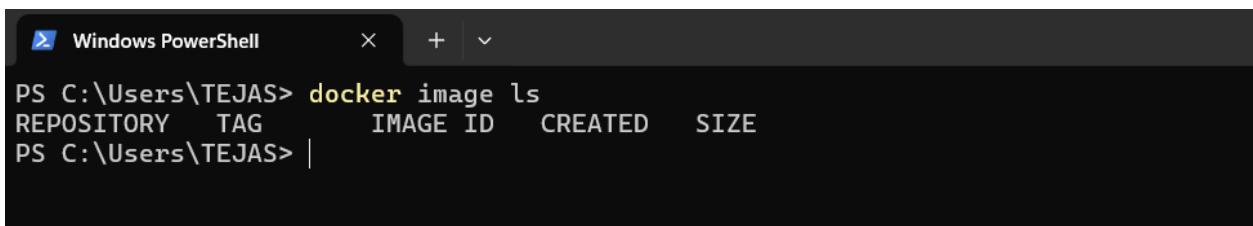
Usage: docker [OPTIONS] COMMAND
      A self-sufficient runtime for containers

Common Commands:
  run      Create and run a new container from an image
  exec    Execute a command in a running container
  ps       List containers
  build   Build an image from a Dockerfile
  pull    Download an image from a registry
  push    Upload an image to a registry
  images   List images
  login   Log in to a registry
  logout  Log out from a registry
  search   Search Docker Hub for images
  version  Show the Docker version information
  info     Display system-wide information

Management Commands:
  builder  Manage builds
  buildx*  Docker Buildx
  compose*  Docker Compose
  container  Manage containers
  context   Manage contexts
  debug*   Get a shell into any image or container
  desktop* Docker Desktop commands (Alpha)
  dev*    Docker Dev Environments
  extension* Manages Docker extensions
```

```
C:\Users\TEJAS>docker --version
Docker version 27.1.1, build 6312585
```

```
C:\Users\TEJAS>
```



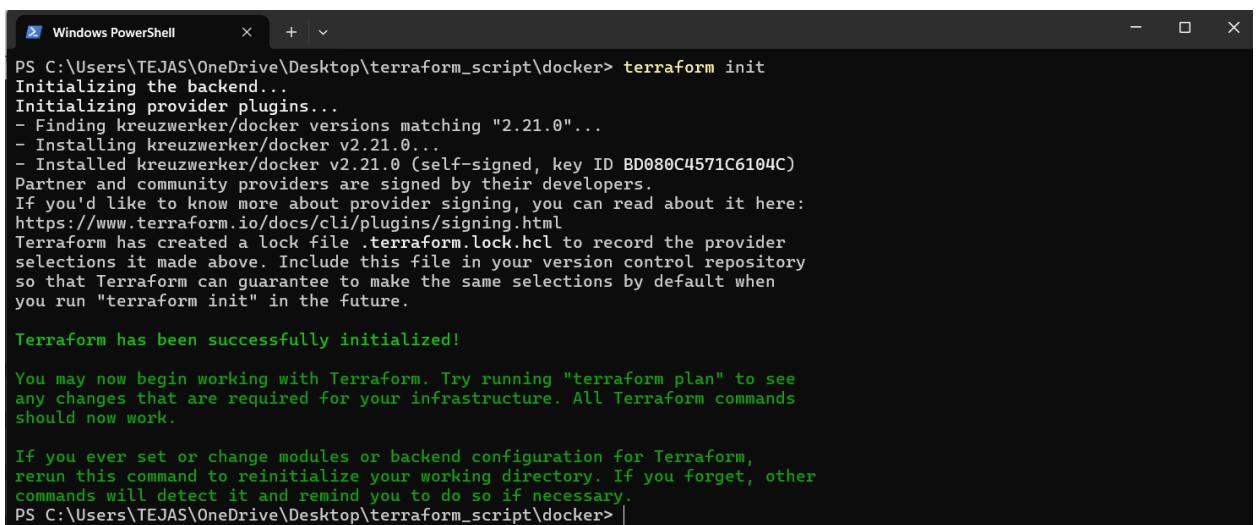
```
Windows PowerShell      X + ▾
PS C:\Users\TEJAS> docker image ls
REPOSITORY TAG IMAGE ID CREATED SIZE
PS C:\Users\TEJAS> |
```

➤ Creation of docker.tf file

Create a folder named ‘Terraform Scripts’ in which we save our different types of scripts. Then, create a new folder named ‘Docker’ in the ‘TerraformScripts’ folder. Then create a new docker.tf file to create a Ubuntu Linux container.

```
⚡ docker.tf > ...
1  terraform {
2    required_providers {
3      docker = {
4        source  = "kreuzwerker/docker"
5        version = "2.21.0"
6      }
7    }
8  }
9
10 provider "docker" {
11   host = "npipe:///./pipe/docker_engine"
12 }
13
14 resource "docker_image" "ubuntu" {
15   name = "ubuntu:latest"
16 }
17
18 resource "docker_container" "practical6" {
19   image = docker_image.ubuntu.image_id
20   name  = "practical6"
21 }
22 |
```

➤ Execute Terraform Init command to initialize the resources



```
PS C:\Users\TEJAS\OneDrive\Desktop\terraform_script\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.
PS C:\Users\TEJAS\OneDrive\Desktop\terraform_script\docker> |
```

- Execute Terraform plan to see the available resources

```
PS C:\Users\TEJAS\OneDrive\Desktop\terraform_script\docker> terraform plan

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.practical6 will be created
+ resource "docker_container" "practical6" {
    + 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              = "practical6"
    + network_data     = (known after apply)
    + read_only         = false
    + remove_volumes   = true
    + restart            = "no"
    + rm                = false
}
```

```
+ remove_volumes = true
+ restart        = "no"
+ rm             = false
+ runtime         = (known after apply)
+ security_opts  = (known after apply)
+ shm_size        = (known after apply)
+ start           = true
+ stdin_open      = false
+ stop_signal     = (known after apply)
+ stop_timeout    = (known after apply)
+ tty              = false

+ healthcheck (known after apply)

+ labels (known after apply)
}

# 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)
}

Plan: 2 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 these actions if
you run "terraform apply" now.
PS C:\Users\TEJAS\OneDrive\Desktop\terraform_script\docker> |
```

- Execute Terraform apply to apply the configuration, which will automatically create and run the Ubuntu Linux container based on our configuration.

```

PS C:\Users\TEJAS\OneDrive\Desktop\terraform_script\docker> 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:

# docker_container.practical6 will be created
+ resource "docker_container" "practical6" {
    + 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               = "practical6"
    + network_data        = (known after apply)
    + read_only           = false
    + remove_volumes      = true
    + restart             = "no"
    + rm                  = false
}

```

```

+ start           = true
+ stdin_open       = false
+ stop_signal      = (known after apply)
+ stop_timeout     = (known after apply)
+ tty              = false

+ healthcheck (known after apply)

+ labels (known after apply)
}

# 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)
}

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

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_image.ubuntu: Creating...
docker_image.ubuntu: Still creating... [10s elapsed]
docker_image.ubuntu: Creation complete after 13s [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2
598aubuntu:latest]
docker_container.practical6: Creating...

```

- Docker images, Before Executing Apply step:

```
PS C:\Users\TEJAS> docker image ls
REPOSITORY      TAG      IMAGE ID      CREATED      SIZE
PS C:\Users\TEJAS> |
```

- Docker images, After Executing Apply step:

```
PS C:\Users\TEJAS\OneDrive\Desktop\terraform_script\docker> docker images
REPOSITORY      TAG      IMAGE ID      CREATED      SIZE
ubuntu          latest   edbfe74c41f8   6 weeks ago  78.1MB
PS C:\Users\TEJAS\OneDrive\Desktop\terraform_script\docker> |
```

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

```
PS C:\Users\TEJAS\OneDrive\Desktop\terraform_script\docker> terraform destroy
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:
- destroy

Terraform will perform the following actions:

# docker_image.ubuntu will be destroyed
- resource "docker_image" "ubuntu" {
    - id           = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest"
    - image_id     = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598a"
    - latest       = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598a"
    - 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 0s

Destroy complete! Resources: 1 destroyed.
PS C:\Users\TEJAS\OneDrive\Desktop\terraform_script\docker> |
```

- Docker images After Executing Destroy step

```
Destroy complete! Resources: 1 destroyed.
PS C:\Users\TEJAS\OneDrive\Desktop\terraform_script\docker> docker images
REPOSITORY      TAG      IMAGE ID      CREATED      SIZE
PS C:\Users\TEJAS\OneDrive\Desktop\terraform_script\docker> |
```

B] Creating S3 Bucket using terraform.

- Write a Terraform Script in Atom for creating S3 Bucket on Amazon AWS

```
aws-s3 > 🎨 main.tf > ...
  1  terraform {
  2    required_providers {
  3      aws = {
  4        source = "hashicorp/aws"
  5        version = "5.64.0"
  6      }
  7      random = {
  8        source = "hashicorp/random"
  9        version = "3.6.2"
 10      }
 11    }
 12  }

 13
 14  resource "random_id" "rand_id"{
 15    byte_length = 8
 16  }

 17
 18  resource "aws_s3_bucket" "demo-bucket" {
 19    bucket = "demo-bucket-${random_id.rand_id.hex}"
 20  }

 21
 22  resource "aws_s3_object" "bucket-data" {
 23    bucket = aws_s3_bucket.demo-bucket.bucket
 24    source = "./myfile.txt"
 25    key = "newfile.txt"
 26  }
```

- Create a new provider.tf file

```
aws-s3 > 🎨 provider.tf > ...
  1  provider "aws" {
  2    access_key = "ASTAXDVAJUCAHHPBYALZ"
  3    secret_key = "kdP24c5nfLccbuwQe49jBthzJc4RefZBns6t6J8y"
  4    token = "TQoJb3jpZ2luX2vje3f//////////wEaCXVzLXd130tMiJIJIMEYCIQCSj3i5FhAaZU/xRQHF5L2DoNBiAuOG0PAemX7fcCn2bwIhAPIRX10U0Af6Bz3Qs7oX8Cnpn62XK7LhDo3/u4vx66juKsACMD//////////wEQABoMNDg4ODg5NTU3MTU4TgZPDJggqUyZ9njLwq1AK1v6HhX0V2hev/w51dDaiTqa9/1Tgriv1VofAfozhohRcK5yuOah05IXYGothTERbx8N1n018fQFBqn1/DB/pEMSk02xh/SPYBrdu1aHSvLuV/86LPqZzJ0wTS41Tn+16f16PyhM4kZtbPTPiXhAjZGJuVNYzrPbe6t6lhGsw/Rsv51B91HEjyVyy7LDQsXvz+YX4ie5Dt09+Xbxh+HMMAp2+GucNkQOKRg+IkdkRPf5njOHJ818h3xQD72tIGmWwXZgbHrobKI5zVkKFzMseofXImgj1h1Zq8zGof9KOUIxdinvRpFzH+FhYPV/cCEMLjE8MleurcdlRna5E7PdAg3k7F8FnMAFcU4qck9uhQCJooowq2yRtwy6nAghyr0X3yVQrc1EWk3j6Hb5MOJC41Tme7fNTs5HyKfdVSFUGzkrzojspeSepbn/YnI1OaadFZCEbY4ayUfsSEhMnKHyzd185xewRnp8kZTKSdxWzqyuTjoi/dL1vfq0B5jPSdJ4J0v453YIsyZmXRnldh8AnYg2zAyw3kc5CdipQLDEti37zP20nciYcA10y+iF+e3Cw/vcgFR08="
  5    region = "us-east-1"
  6  }
  7  \end{code}
```

➤ Execute Terraform Init command to initialize the resources

```
PS C:\Users\TEJAS\OneDrive\Desktop\SEM 5 VESIT\Terraform practical>
cd aws-s3
PS C:\Users\TEJAS\OneDrive\Desktop\SEM 5 VESIT\Terraform practical\aws-s3> terraform init
Initializing the backend...
Initializing provider plugins...
- Reusing previous version of hashicorp/aws from the dependency lock file
- Reusing previous version of hashicorp/random from the dependency lock file
- Using previously-installed hashicorp/aws v5.64.0
- Using previously-installed hashicorp/random v3.6.2

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.
PS C:\Users\TEJAS\OneDrive\Desktop\SEM 5 VESIT\Terraform practical\aws-s3>
```

➤ Execute Terraform plan to see the available resources

```
PS C:\Users\TEJAS\OneDrive\Desktop\SEM 5 VESIT\Terraform practical\aws-s3> terraform plan
random_id.rand_id: Refreshing state... [id=mW9L9tLf-c]
aws_s3_bucket.demo-bucket: Refreshing state... [id=demo-bucket-98c27d2fdb4b7fe7]
aws_s3_object.bucket-data: Refreshing state... [id=newfile.txt]

Note: Objects have changed outside of Terraform

Terraform detected the following changes made outside of Terraform since the last "terraform apply" which may have affected this plan:

# aws_s3_bucket.demo-bucket has been deleted
- resource "aws_s3_bucket" "demo-bucket" {
  - bucket           = "demo-bucket-98c27d2fdb4b7fe7" -> null
  id                 = "demo-bucket-98c27d2fdb4b7fe7"
  # (12 unchanged attributes hidden)

  # (3 unchanged blocks hidden)
}

Unless you have made equivalent changes to your configuration, or ignored the relevant attributes using ignore_changes, the following plan may include actions to
undo or respond to these changes.

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                   = "demo-bucket-98c27d2fdb4b7fe7"
  + bucket_domain_name       = (known after apply)
  + bucket_prefix             = (known after apply)
  + bucketRegionalDomainName = (known after apply)
  + force_destroy             = false
}
```

```

+ replication_configuration (known after apply)
+ server_side_encryption_configuration (known after apply)
+ versioning (known after apply)
+ website (known after apply)
}

# aws_s3_object.bucket-data will be created
+ resource "aws_s3_object" "bucket-data" {
  + acl           = (known after apply)
  + arn           = (known after apply)
  + bucket        = "demo-bucket-98c27d2fdb4b7fe7"
  + bucket_key_enabled = (known after apply)
  + checksum_crc32 = (known after apply)
  + checksum_crc32c = (known after apply)
  + checksum_sha1 = (known after apply)
  + checksum_sha256 = (known after apply)
  + content_type = (known after apply)
  + etag          = (known after apply)
  + force_destroy = false
  + id            = (known after apply)
  + key           = "newfile.txt"
  + kms_key_id   = (known after apply)
  + server_side_encryption = (known after apply)
  + source        = "./myfile.txt"
  + storage_class = (known after apply)
  + tags_all     = (known after apply)
  + version_id   = (known after apply)
}

```

Plan: 2 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 these actions if you run `"terraform apply"` now.
PS C:\Users\TEJAS\OneDrive\Desktop\SEM 5 VESIT\Terraform practical\aws-s3> |

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

```

PS C:\Users\TEJAS\OneDrive\Desktop\SEM 5 VESIT\Terraform practical\aws-s3> terraform apply
random_id.rand_id: Refreshing state... [id=mMD99tLf-c]
aws_s3_bucket.demo-bucket: Refreshing state... [id=demo-bucket-98c27d2fdb4b7fe7]
aws_s3_object.bucket-data: Refreshing state... [id=newfile.txt]

```

Note: objects have changed outside of Terraform

Terraform detected the following changes made outside of Terraform since the last `"terraform apply"` which may have affected this plan:

```

# aws_s3_bucket.demo-bucket has been deleted
- resource "aws_s3_bucket" "demo-bucket" {
  - bucket           = "demo-bucket-98c27d2fdb4b7fe7" -> null
  id                = "demo-bucket-98c27d2fdb4b7fe7"
  # (12 unchanged attributes hidden)

  # (3 unchanged blocks hidden)
}

```

Unless you have made equivalent changes to your configuration, or ignored the relevant attributes using `ignore_changes`, the following plan may include actions to undo or respond to these changes.

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                   = "demo-bucket-98c27d2fdb4b7fe7"
  + bucket_domain_name       = (known after apply)
  + bucket_prefix             = (known after apply)
  + bucketRegionalDomainName = (known after apply)
  + force_destroy             = false
}

```

```
# aws_s3_object.bucket-data will be created
+ resource "aws_s3_object" "bucket-data" {
    + acl           = (known after apply)
    + arn           = (known after apply)
    + bucket        = "demo-bucket-98c27d2fdb4b7fe7"
    + bucket_key_enabled = (known after apply)
    + checksum_crc32 = (known after apply)
    + checksum_sha1 = (known after apply)
    + checksum_sha256 = (known after apply)
    + content_type = (known after apply)
    + etag          = (known after apply)
    + force_destroy = false
    + id            = (known after apply)
    + key           = "newfile.txt"
    + kms_key_id   = (known after apply)
    + server_side_encryption = (known after apply)
    + source         = "./myfile.txt"
    + storage_class = (known after apply)
    + tags_all      = (known after apply)
    + version_id    = (known after apply)
}

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

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

aws_s3_bucket.demo-bucket: Creating...
aws_s3_bucket.demo-bucket: Creation complete after 7s [id=demo-bucket-98c27d2fdb4b7fe7]
aws_s3_object.bucket-data: Creating...
aws_s3_object.bucket-data: Creation complete after 2s [id=newfile.txt]

Apply complete! Resources: 2 added, 0 changed, 0 destroyed.
PS C:\Users\TEJAS\OneDrive\Desktop\SEM 5 VESIT\Terraform practical\aws-s3>
```

➤ AWS S3bucket dashboard, Before Executing Apply command:

The screenshot shows the AWS S3 service dashboard. On the left, there's a sidebar with navigation links like 'Buckets', 'Access Grants', 'Access Points', etc. The main area displays an 'Account snapshot' with an update frequency of 'updated every 24 hours'. Below it, under 'General purpose buckets', there is one entry:

Name	AWS Region	IAM Access Analyzer	Creation date
mywebapp-bucket-f58273e0c7a54302	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 24, 2024, 16:24:08 (UTC+05:30)

- AWS S3 Bucket dashboard, After Executing Apply step:

The screenshot shows the AWS S3 service dashboard. On the left, there's a sidebar with options like Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings, Storage Lens, Dashboards, Storage Lens groups, and AWS Organizations settings. A Feature spotlight section is also present. The main area is titled "Amazon S3" and "Amazon S3". It features an "Account snapshot - updated every 24 hours" section with a link to "All AWS Regions" and a "Storage lens provides visibility into storage usage and activity trends. Learn more" link. Below this is a tab bar with "General purpose buckets" (selected) and "Directory buckets". A table lists "General purpose buckets (2)" with columns for Name, AWS Region, IAM Access Analyzer, and Creation date. The first bucket, "demo-bucket-12059a75f2ba9934", was created on September 14, 2024, at 20:47:16 (UTC+05:30). The second bucket, "mywebapp-bucket-f58273e0c7a54302", was created on August 24, 2024, at 16:24:08 (UTC+05:30). Buttons for "Copy ARN", "Empty", "Delete", and "Create bucket" are available at the top of the table. The URL in the address bar is <https://us-east-1.console.aws.amazon.com/s3/buckets/demo-bucket-12059a75f2ba9934?region=us-east-1>.

- Execute Terraform destroy to delete the configuration, which will automatically delete the bucket

```
PS C:\Users\TEJAS\OneDrive\Desktop\SEM 5 VESIT\Teraform practical\aws-s3> terraform destroy
random_id.rand_id: Refreshing state... [id=mMJ9L9tf-c]
aws_s3_bucket.demo-bucket: Refreshing state... [id=demo-bucket-98c27d2fdb4b7fe7]
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-98c27d2fdb4b7fe7" -> null
    - bucket = "demo-bucket-98c27d2fdb4b7fe7" -> null
    - bucket_domain_name = "demo-bucket-98c27d2fdb4b7fe7.s3.us-east-1.amazonaws.com" -> null
    - bucketRegionalDomainName = "demo-bucket-98c27d2fdb4b7fe7.s3.us-east-1.amazonaws.com" -> null
    - force_destroy = false -> null
    - hostedZoneId = "Z3AQ8STGFYJSTF" -> null
    - id = "demo-bucket-98c27d2fdb4b7fe7" -> null
    - objectLockEnabled = false -> null
    - region = "us-east-1" -> null
    - requestPayer = "BucketOwner" -> null
    - tags = "{}" -> null
    - tags_all = "{}" -> null
    # (3 unchanged attributes hidden)

    - grant {
        - id = "89f191669ac713a2d0a157aa4176d8ce16adda216e3bafb6e7f0811cb559dca" -> null
        - permissions = [
            - "FULL_CONTROL",
        ] -> null
        - type = "CanonicalUser" -> null
        # (1 unchanged attribute hidden)
    }

    - serverSideEncryptionConfiguration {
        - rule {
            - bucketKeyEnabled = false -> null
            - applyServerSideEncryptionByDefault {
                - sseAlgorithm = "AES256" -> null
            }
        }
    }
}
```

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

```
aws_s3_object.bucket-data: Destroying... [id=newfile.txt]
aws_s3_object.bucket-data: Destruction complete after 1s
aws_s3_bucket.demo-bucket: Destroying... [id=demo-bucket-98c27d2fdb4b7fe7]
aws_s3_bucket.demo-bucket: Destruction complete after 1s
random_id.rand_id: Destroying... [id=mMJ9L9tLf-c]
random_id.rand_id: Destruction complete after 0s
```

Destroy complete! Resources: 3 destroyed.

PS C:\Users\TEJAS\OneDrive\Desktop\SEM 5 VESIT\Teraform practical\aws-s3>

- AWS S3 Bucket dashboard, After Executing Destroy step:

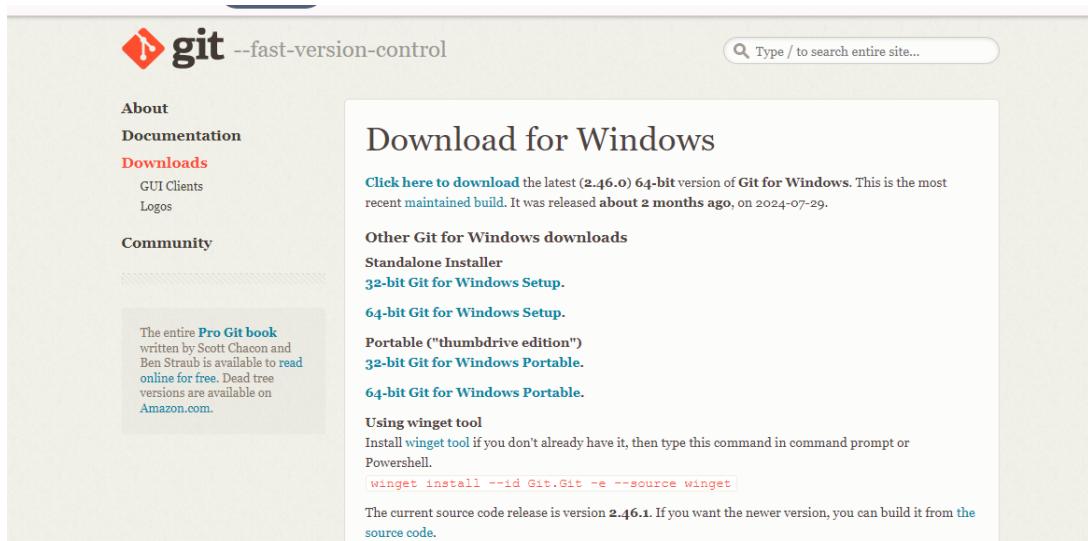
The screenshot shows the AWS S3 service dashboard. On the left, there's a sidebar with options like Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings, Storage Lens, Dashboards, Storage Lens groups, and AWS Organizations settings. A 'Feature spotlight' section is also present. The main content area is titled 'Amazon S3' and shows an 'Account snapshot - updated every 24 hours'. It includes a 'View Storage Lens dashboard' button. Below this, there are tabs for 'General purpose buckets' and 'Directory buckets', with 'General purpose buckets' currently selected. It displays a table with one item:

Name	AWS Region	IAM Access Analyzer	Creation date
mywebapp-bucket-f5b273e0c7a54302	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 24, 2024, 16:24:08 (UTC+05:30)

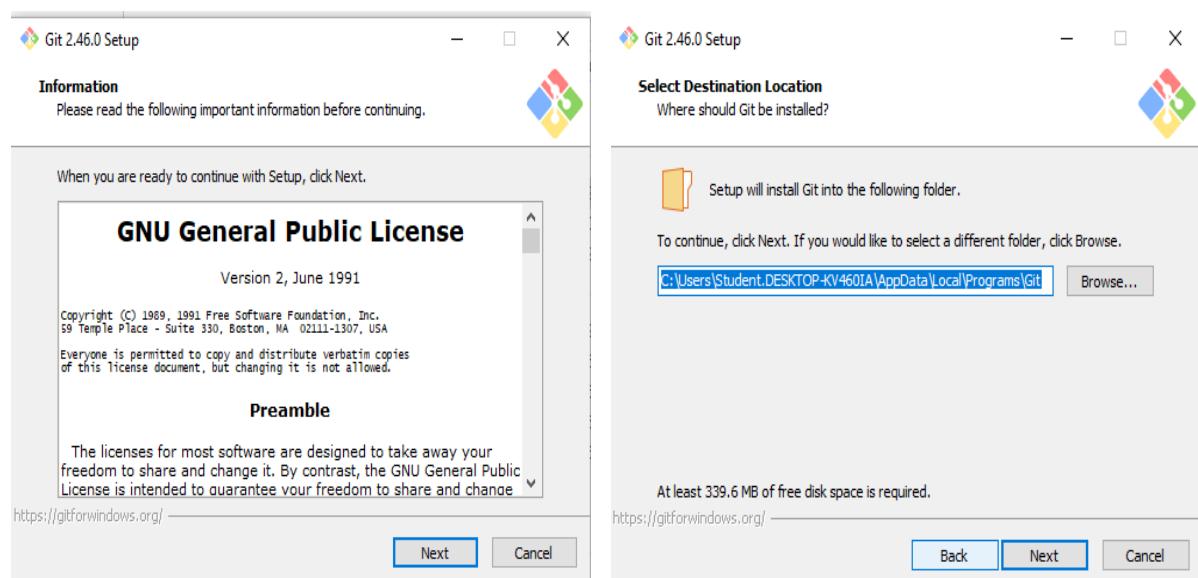
EXPERIMENT NO: - 07

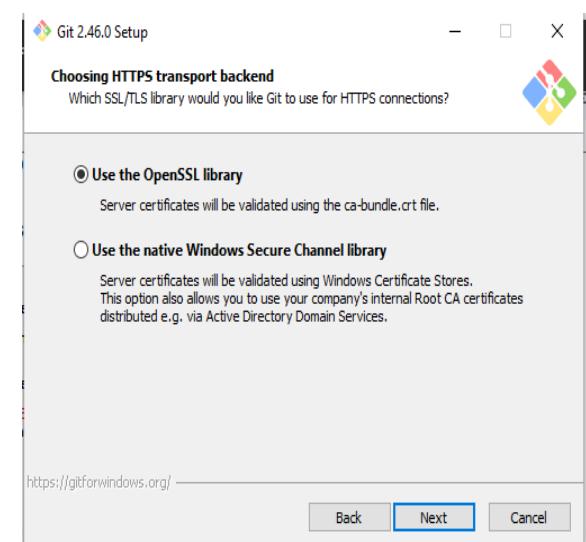
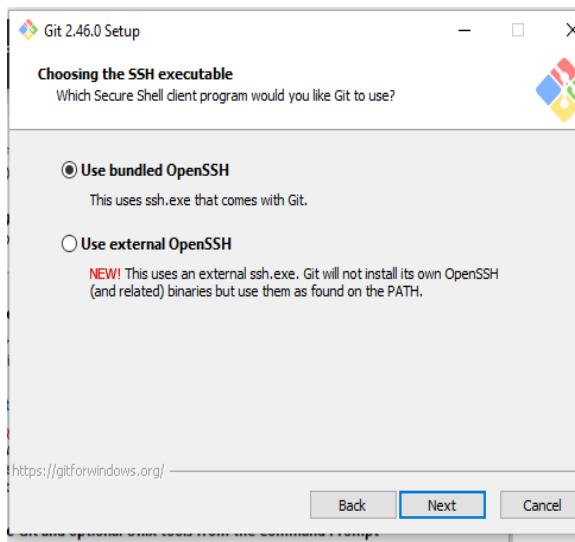
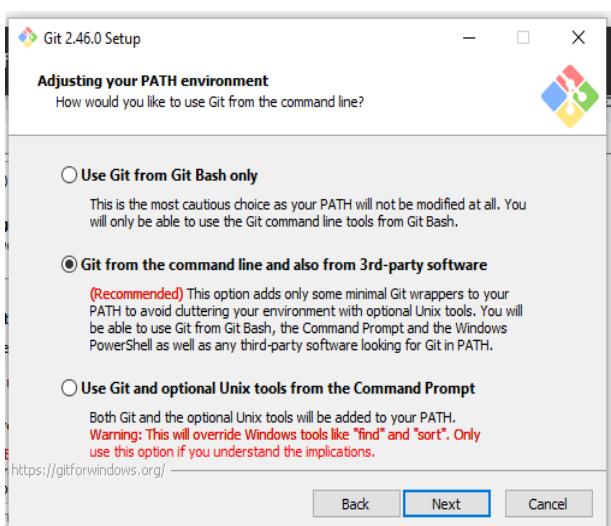
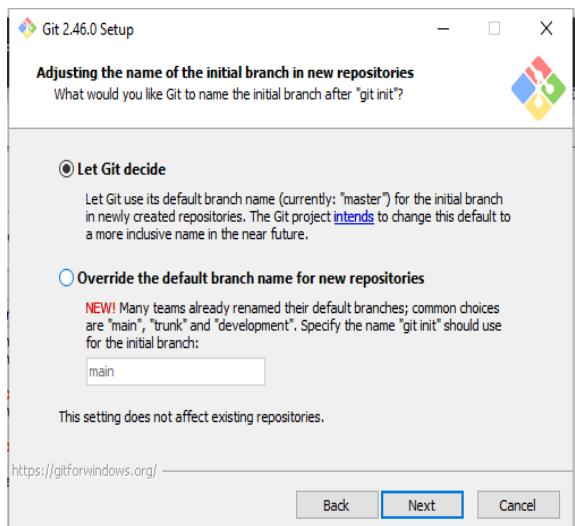
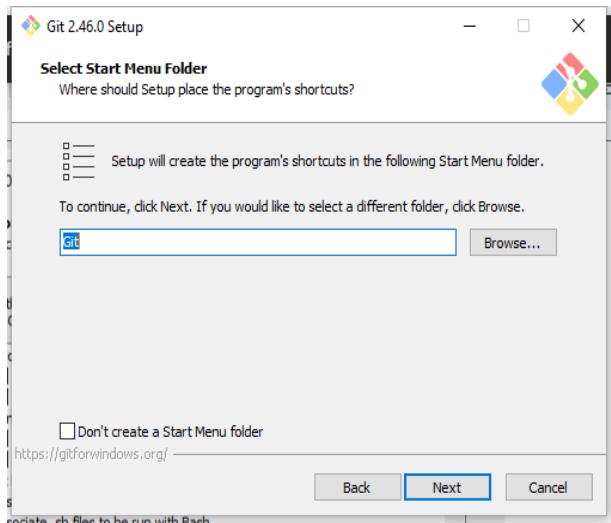
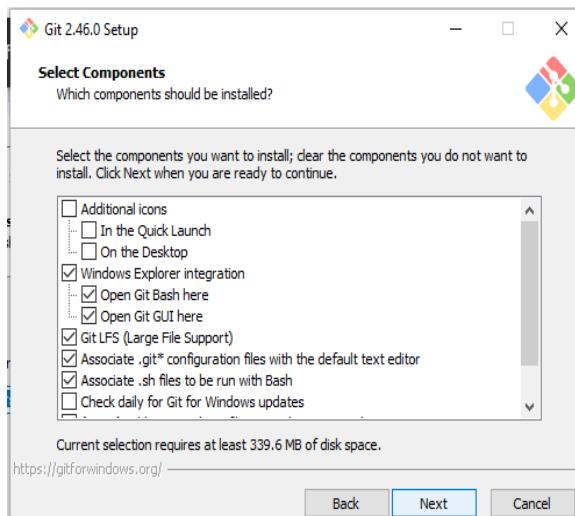
AIM:- To understand Static Analysis SAST process and learn to integrate Jenkins SAST to SonarQube/GitLab

➤ GIT Installation

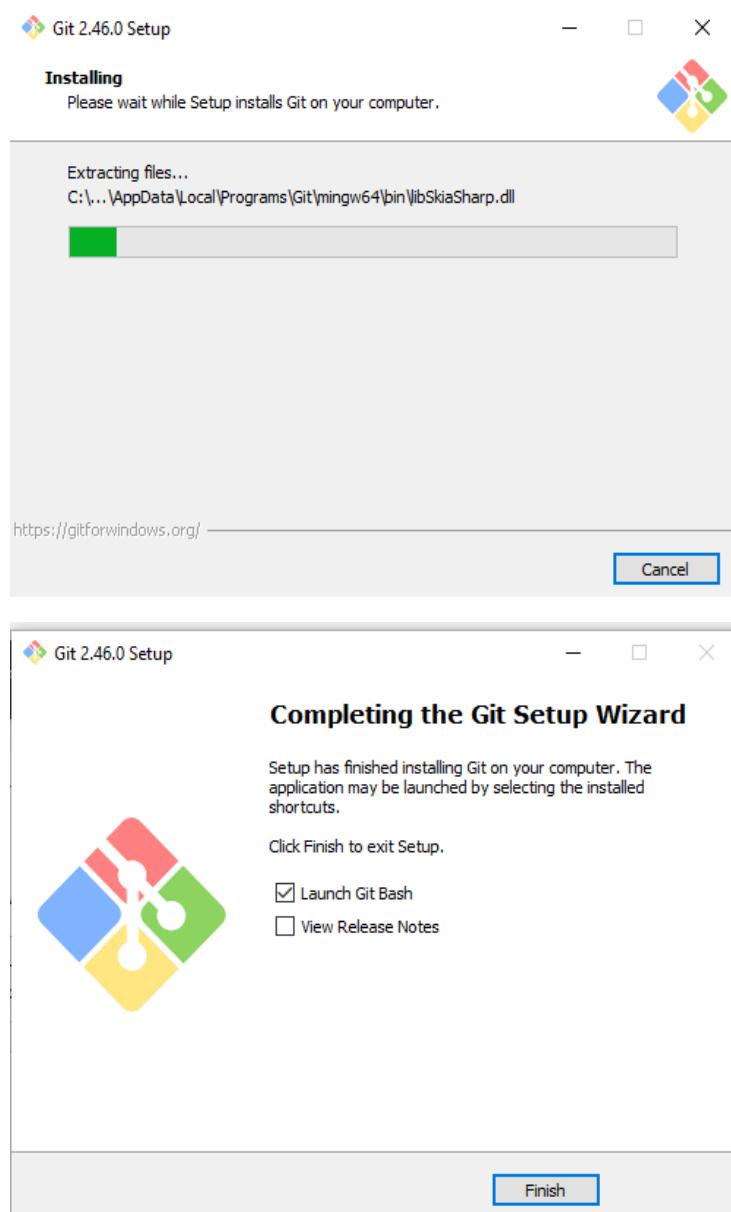


Select Installation for Windows setup and set up the destination for GIT installation.





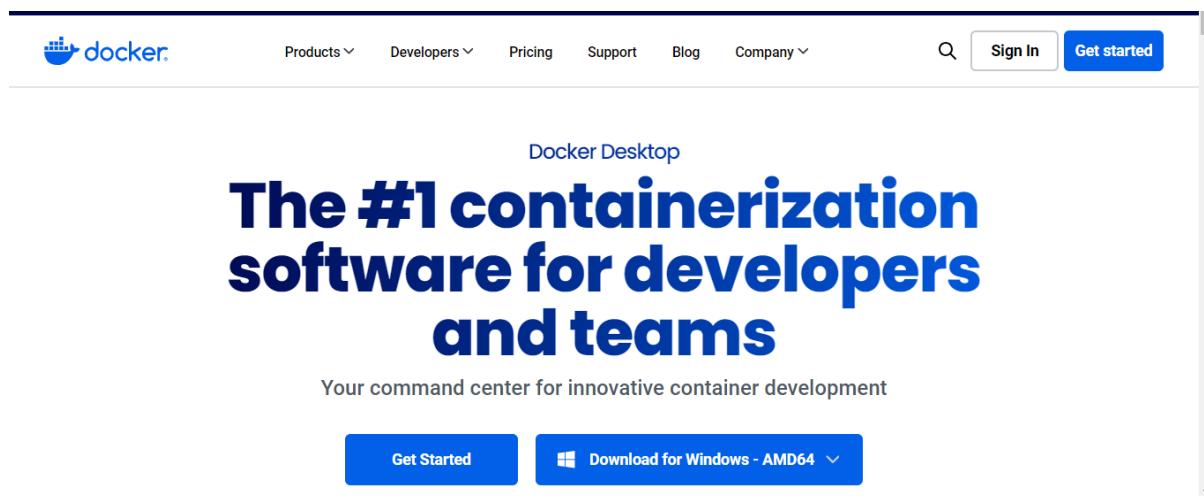
After all such configurations, Git installation is started



After Installation, Git Bash is launched

```
MINGW64:/c/Users/Student.DESKTOP-KV460IA
Student@DESKTOP-KV460IA MINGW64 ~
$ |
```

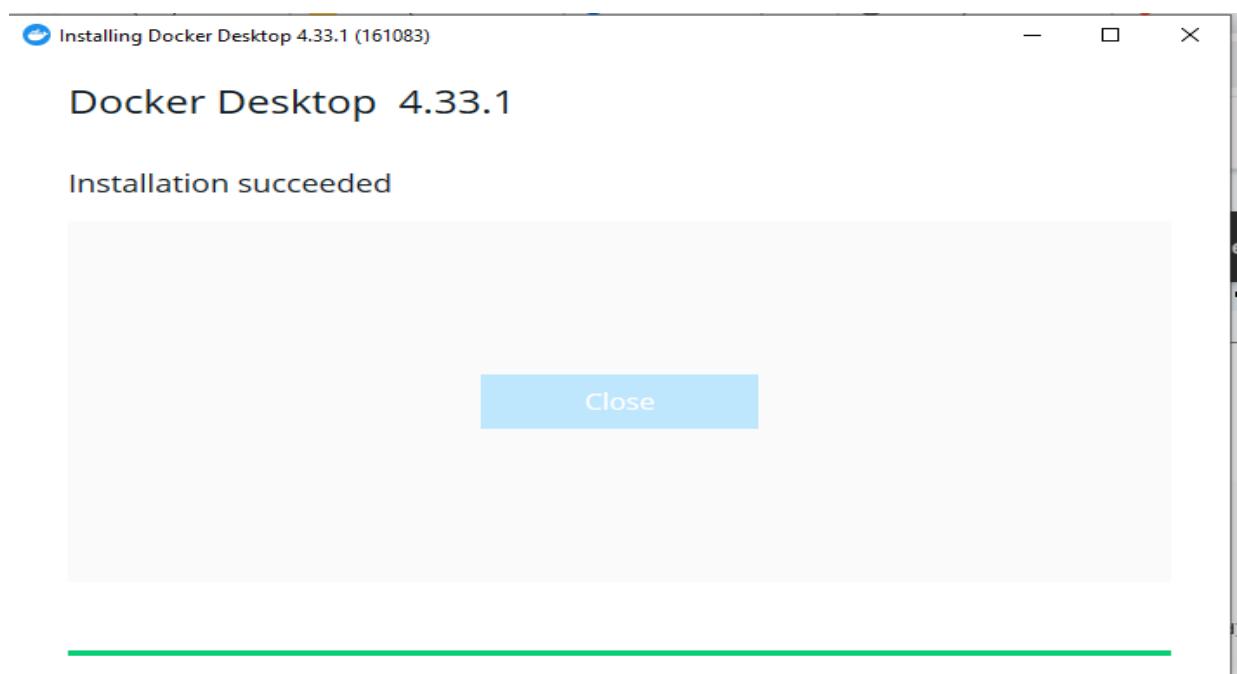
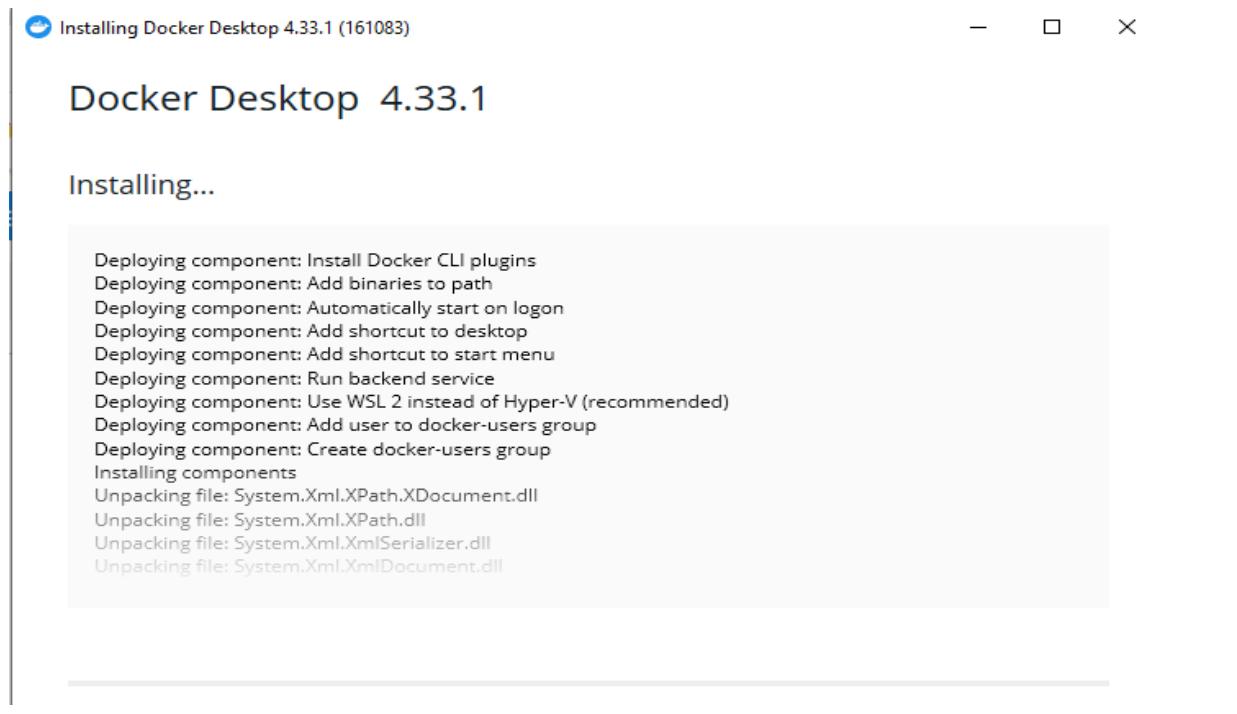
➤ Docker Installation



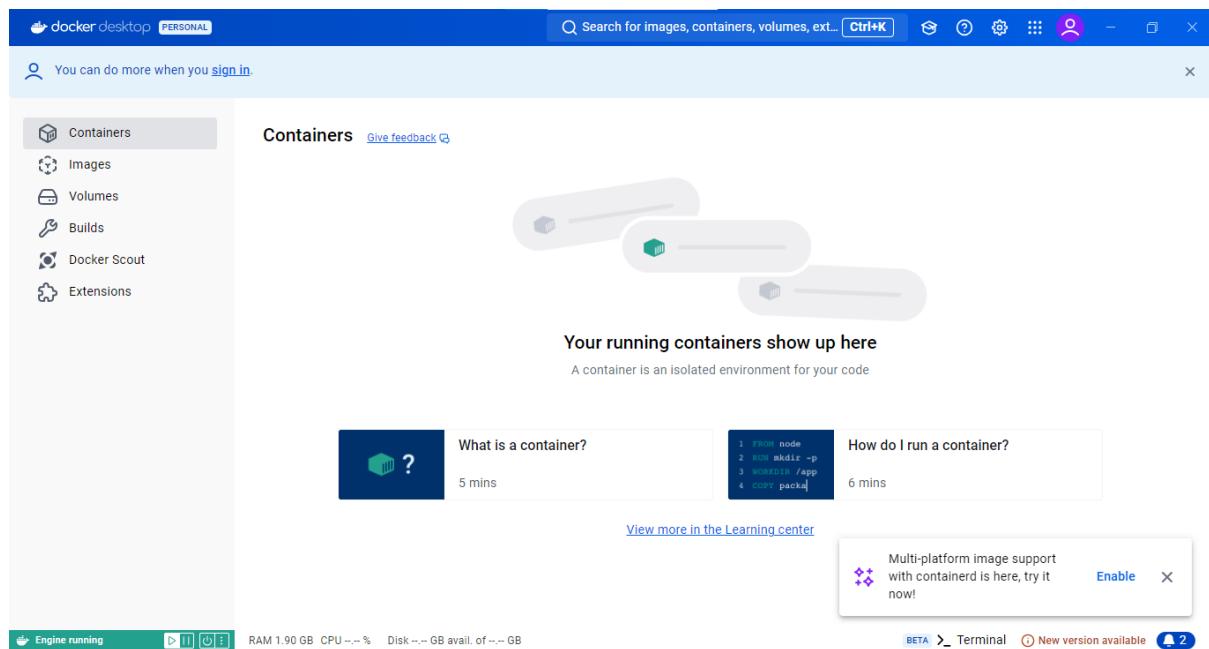
The screenshot shows the Docker Desktop landing page. At the top, there's a navigation bar with the Docker logo, a search icon, and links for 'Sign In' and 'Get started'. Below the header, the text 'Docker Desktop' is followed by a large, bold headline: 'The #1 containerization software for developers and teams'. Underneath the headline, it says 'Your command center for innovative container development'. At the bottom of the main content area, there are two buttons: 'Get Started' and 'Download for Windows - AMD64'.

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”

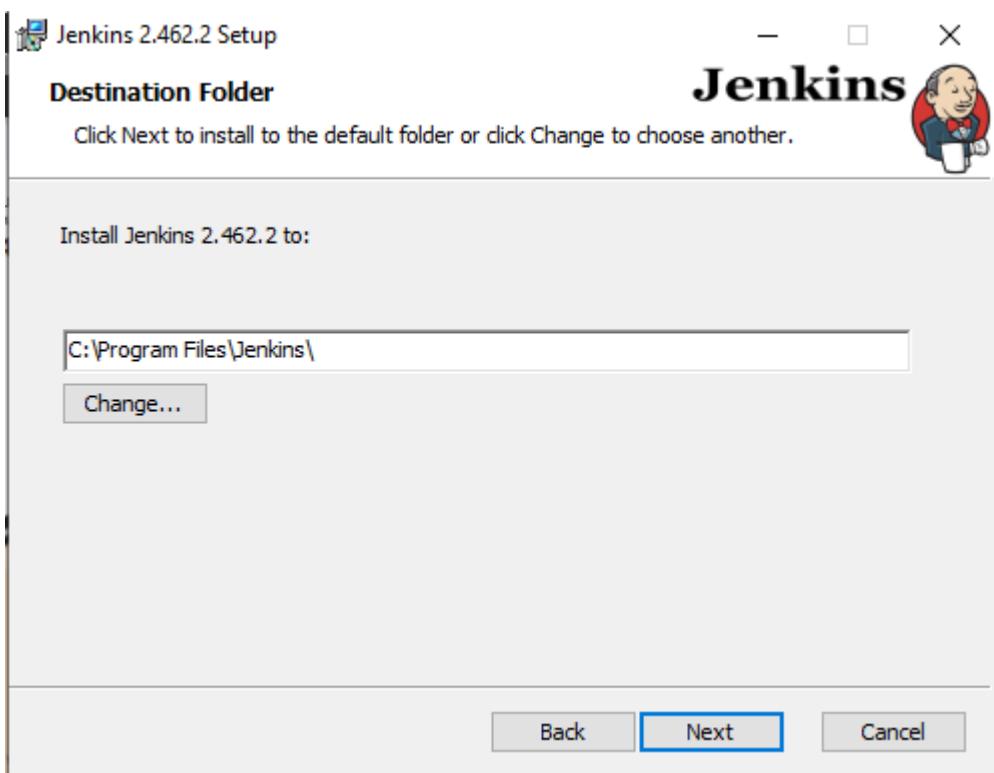
```
C:\Users\Student.DESKTOP-KV460IA>docker --version
Docker version 27.1.1, build 6312585
C:\Users\Student.DESKTOP-KV460IA>
```

➤ Jenkins Installation

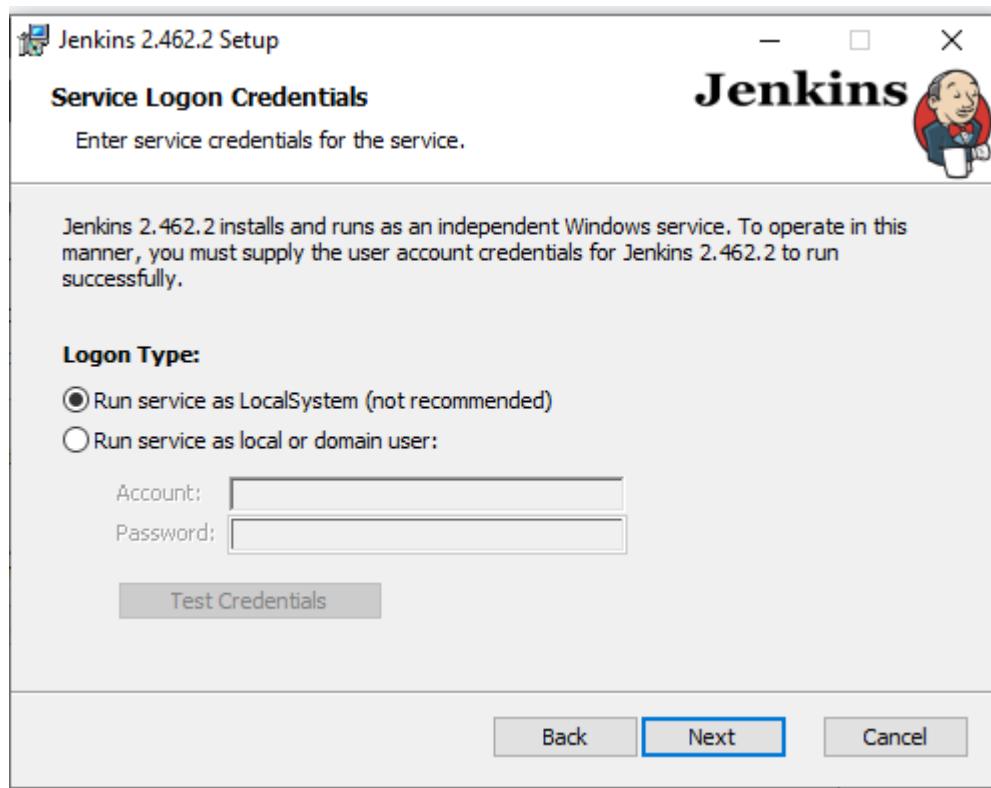
Launch the Jenkins exe file downloaded



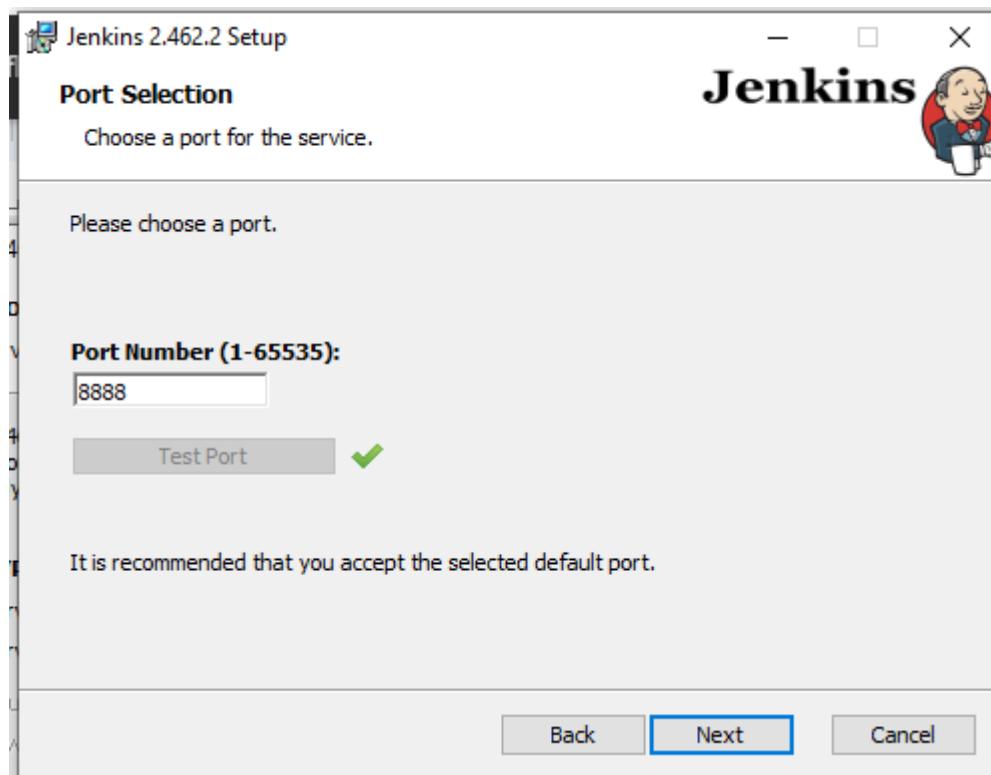
Set the path for Jenkins all workspaces and jobs



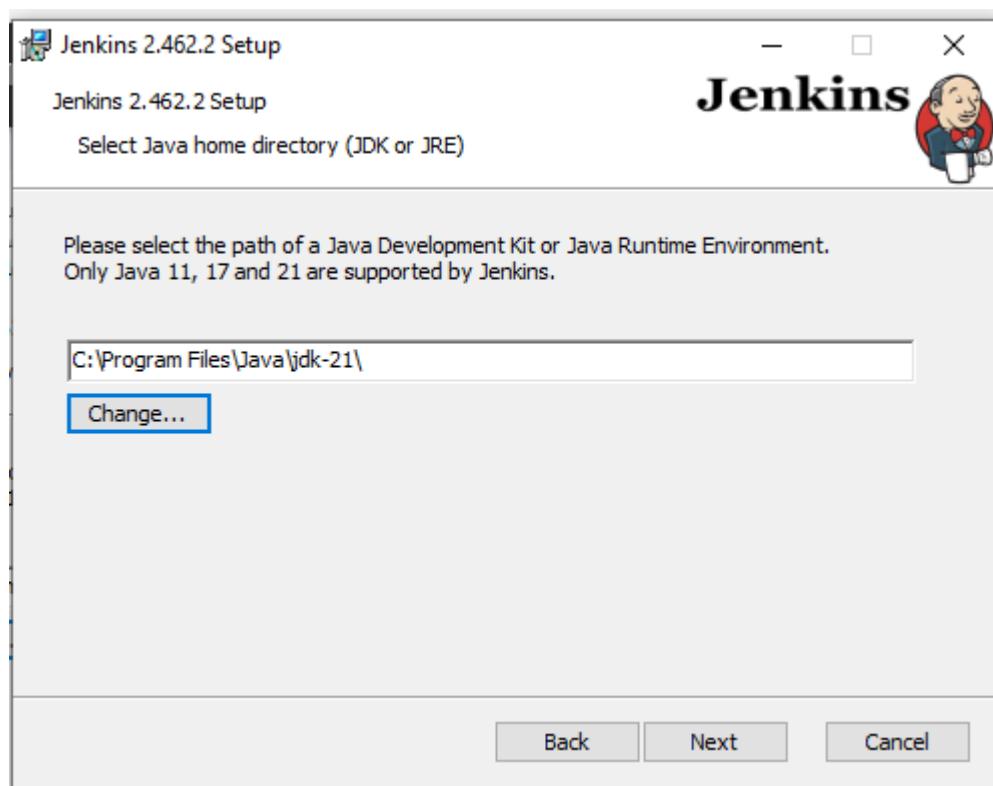
Select “Run service as a LocalSystem” to start Jenkins locally



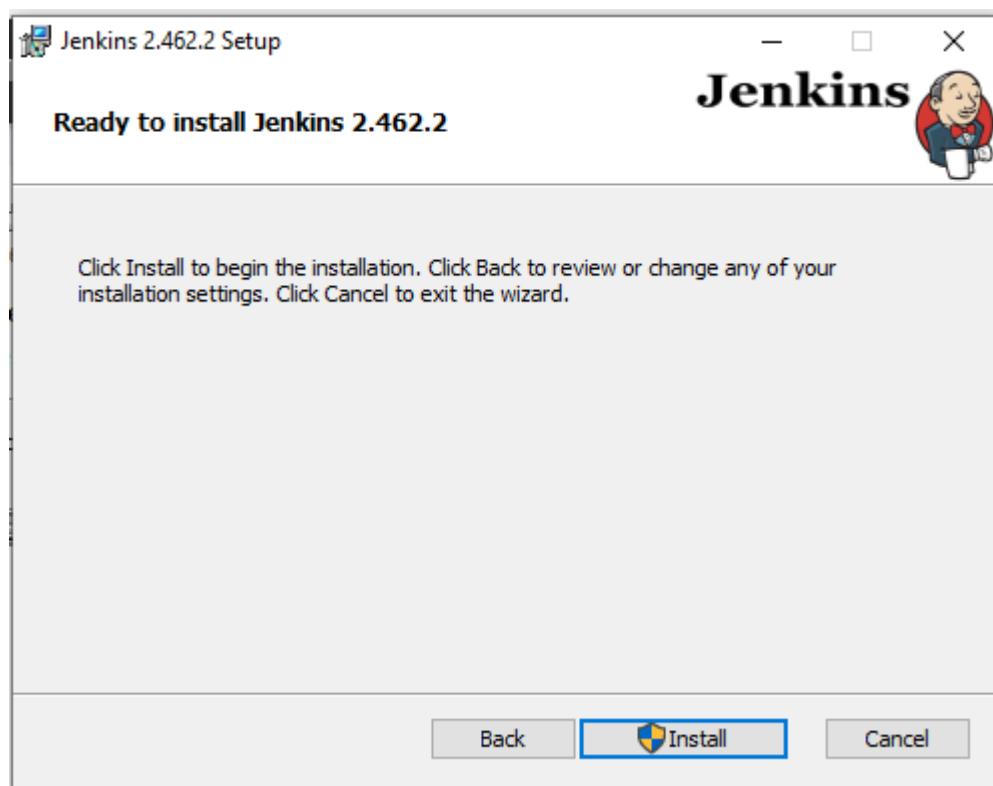
Choose a port on which you want Jenkins to work.(By default it is 8080)

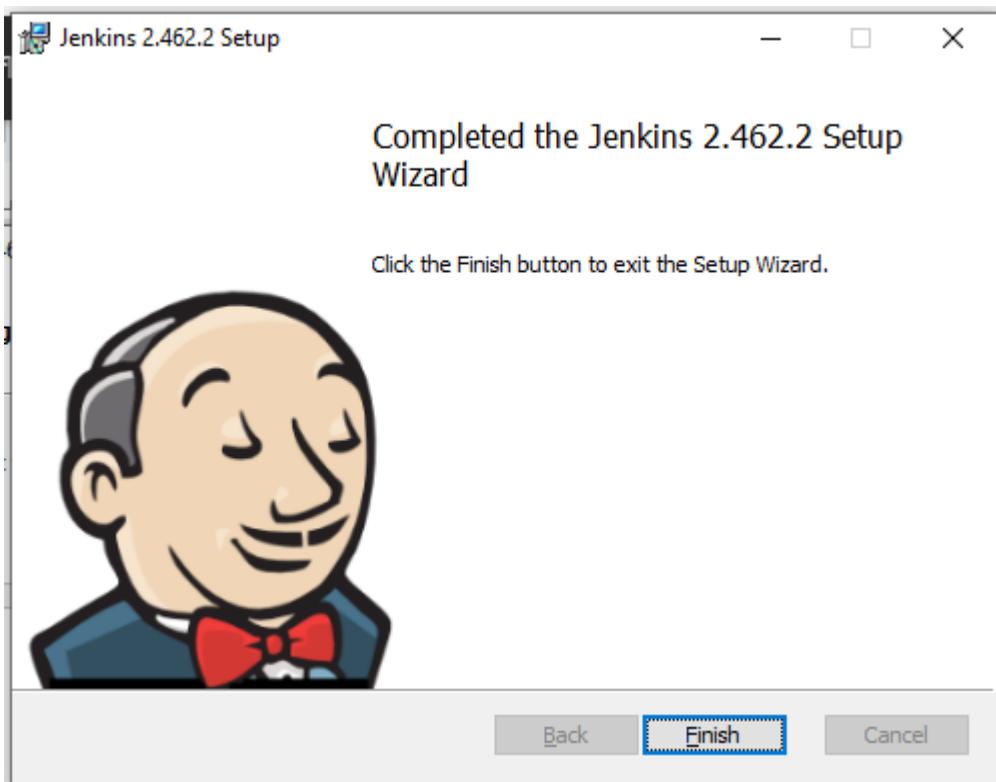


Set up the latest Java directory



Click Install to begin the installation process





Once it is installed, go to <http://localhost:8888>, where we first need to setup the Jenkins

Getting Started

Unlock Jenkins

To ensure Jenkins is securely set up by the administrator, a password has been written to the log ([not sure where to find it?](#)) and this file on the server:

`C:\ProgramData\Jenkins\.jenkins\secrets\initialAdminPassword`

Please copy the password from either location and paste it below.

Administrator password

.....

Continue

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

Getting Started

Customize Jenkins

Plugins extend Jenkins with additional features to support many different needs.

Install suggested plugins

Install plugins the Jenkins community finds most useful.

Select plugins to install

Select and install plugins most suitable for your needs.

Jenkins 2.462.2

Set up the configuration details

Getting Started

Create First Admin User

Username

jenkins

Password

....

Confirm password

....

Jenkins 2.462.2

Skip and continue as admin

Save and Continue

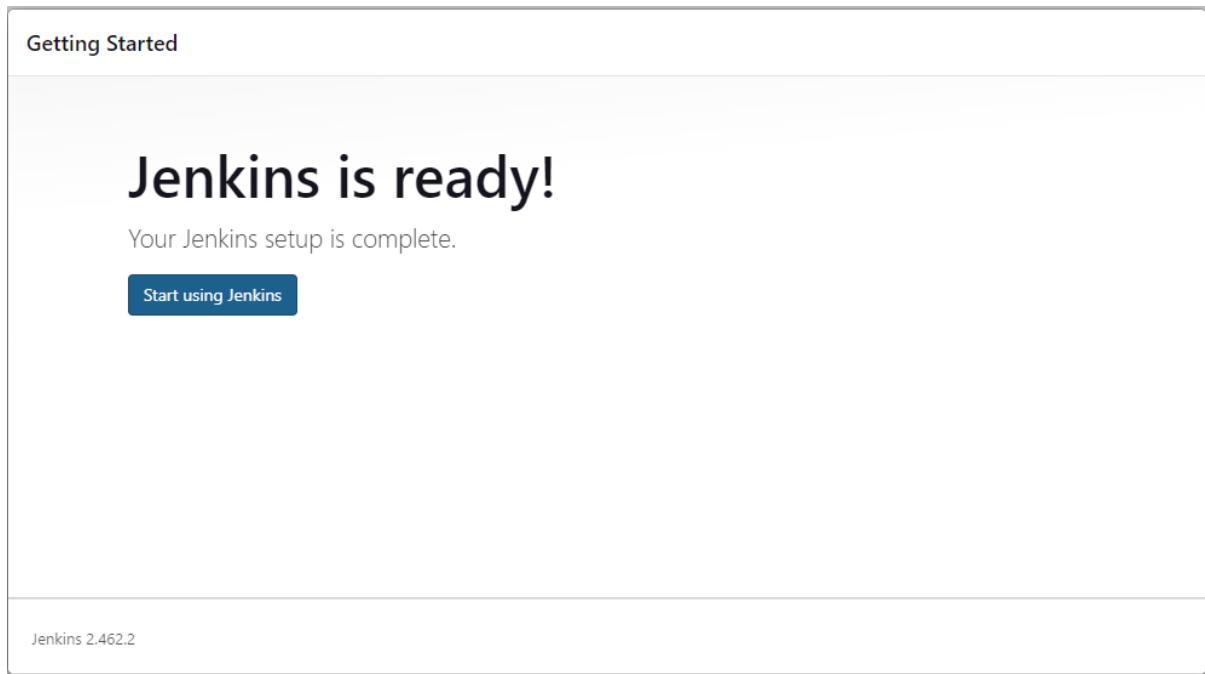
Getting Started

Jenkins is ready!

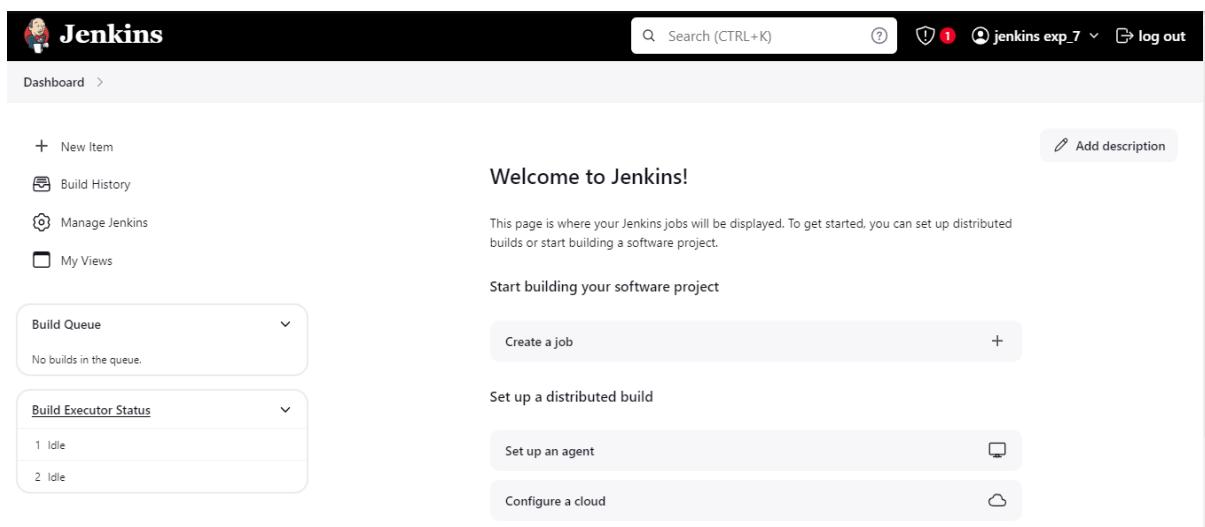
Your Jenkins setup is complete.

[Start using Jenkins](#)

Jenkins 2.462.2



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

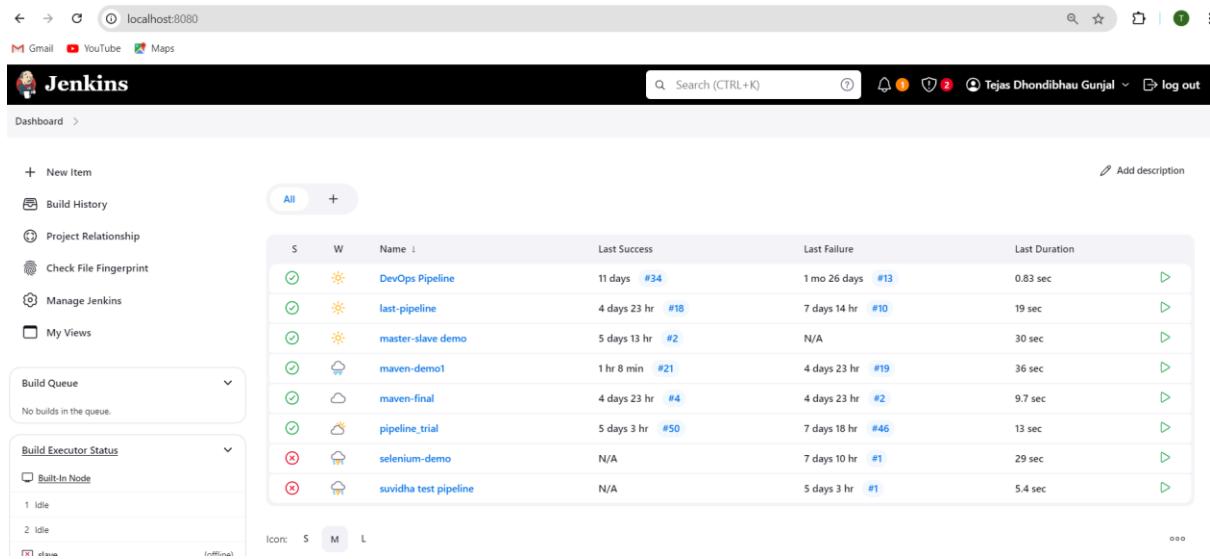


The screenshot shows the Jenkins dashboard after login. At the top, there's a navigation bar with the Jenkins logo, a search bar, and user information ('jenkins exp_7'). Below the header, a 'Welcome to Jenkins!' message is displayed with a note about setting up jobs. The main area has several sections: 'Build Queue' (empty), 'Build Executor Status' (2 Idle), 'Start building your software project' (with a 'Create a job' button), 'Set up a distributed build' (with 'Set up an agent' and 'Configure a cloud' buttons), and other management links like 'New Item', 'Build History', and 'Manage Jenkins'.

EXPERIMENT NO: - 08

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

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

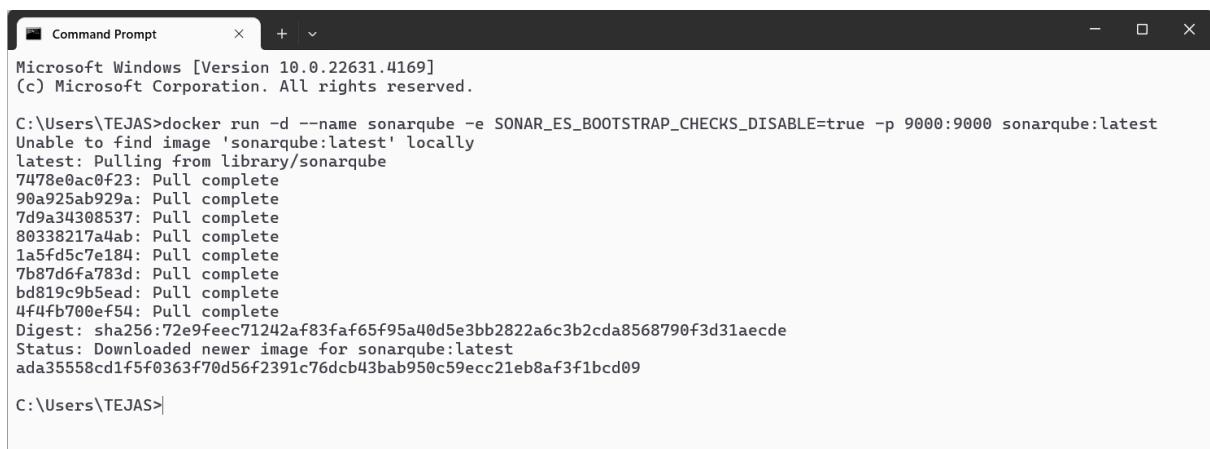


The screenshot shows the Jenkins dashboard at localhost:8080. The left sidebar includes links for 'New Item', 'Build History', 'Project Relationship', 'Check File Fingerprint', 'Manage Jenkins', and 'My Views'. Under 'Build Queue' and 'Build Executor Status', there are no builds in the queue and 2 idle nodes respectively. The main area displays a table of pipelines:

S	W	Name	Last Success	Last Failure	Last Duration
✓	☀️	DevOps Pipeline	11 days #34	1 mo 26 days #13	0.83 sec
✓	☀️	last-pipeline	4 days 23 hr #18	7 days 14 hr #10	19 sec
✓	☀️	master-slave demo	5 days 13 hr #2	N/A	30 sec
✓	☁️	maven-demo1	1 hr 8 min #21	4 days 23 hr #19	36 sec
✓	☁️	maven-final	4 days 23 hr #4	4 days 23 hr #2	9.7 sec
✓	☁️	pipeline_trial	5 days 3 hr #50	7 days 18 hr #46	13 sec
✗	☁️	selenium-demo	N/A	7 days 10 hr #1	29 sec
✗	☁️	suvidha test pipeline	N/A	5 days 3 hr #1	5.4 sec

- 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
```

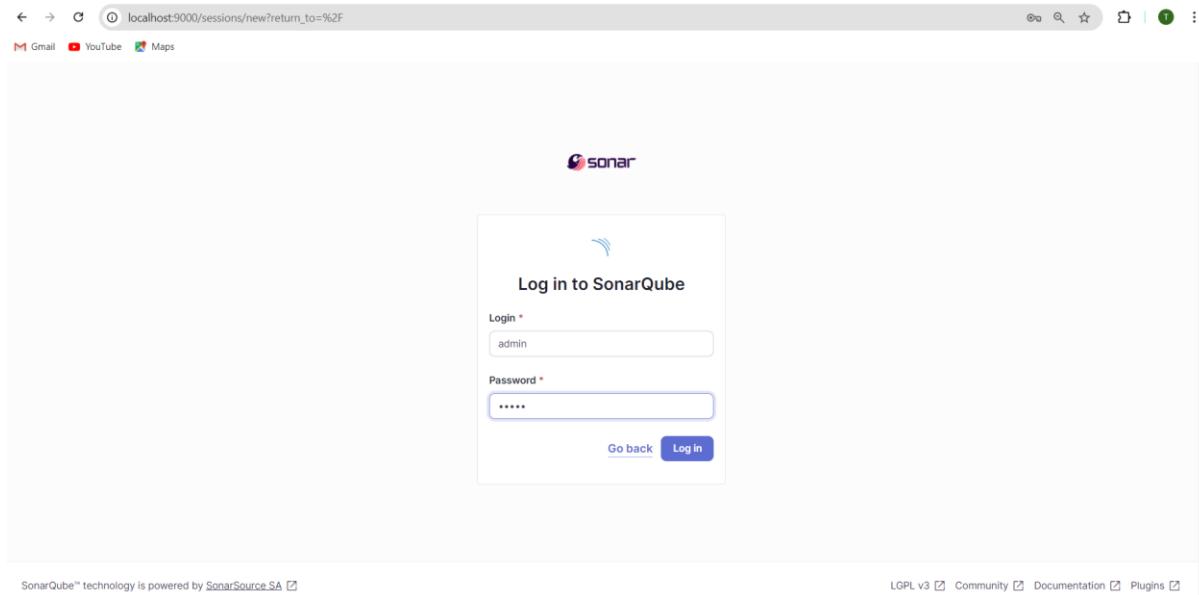


```
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. All rights reserved.

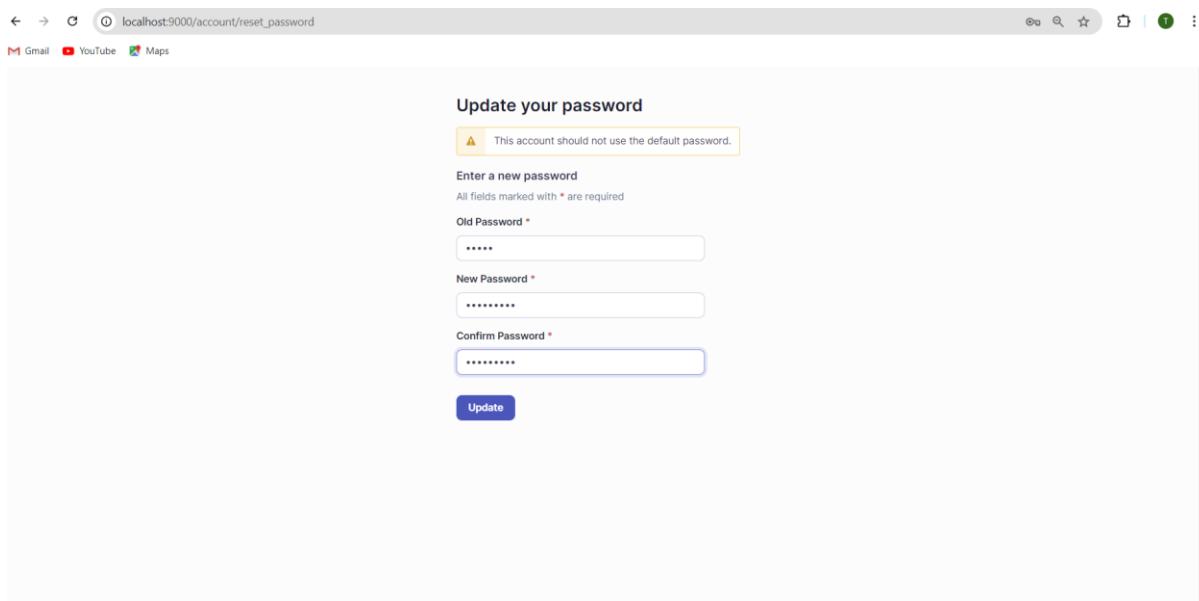
C:\Users\TEJAS>docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
7478e0ac0f23: Pull complete
90a925ab929a: Pull complete
7d9a34308537: Pull complete
80338217a4ab: Pull complete
1a5fd5c7e184: Pull complete
7b87d6fa783d: Pull complete
bd819c9b5ead: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Downloaded newer image for sonarqube:latest
ada35558cd1f5f0363f70d56f2391c76dc43bab950c59ecc21eb8af3f1bcd09

C:\Users\TEJAS>
```

- 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.



- It also gives an option to update the password, for the security purposes



How do you want to create your project?

Do you want to benefit from all of SonarQube's features (like repository import and Pull Request decoration)? Create your project from your favorite DevOps platform.

First, you need to set up a DevOps platform configuration.

Are you just testing or have an advanced use-case? Create a local project.

⚠️ Embedded database should be used for evaluation purposes only
The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.

SonarQube™ technology is powered by SonarSource SA [\[\]](#)

Community Edition v10.6 (92116) ACTIVE [\[\]](#) LGPL V3 [\[\]](#) Community [\[\]](#) Documentation [\[\]](#) Plugins [\[\]](#) Web API [\[\]](#)

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

1 of 2

Create a local project

Project display name *

✓

Project key *

✓

Main branch name *

The name of your project's default branch [Learn More](#)

- Setup the project and come back to Jenkins Dashboard.

2 of 2

Set up project for Clean as You Code

The new code definition sets which part of your code will be considered new code. This helps you focus attention on the most recent changes to your project, enabling you to follow the Clean as You Code methodology. Learn more: [Defining New Code](#)

Choose the baseline for new code for this project

Use the global setting

Previous version
Any code that has changed since the previous version is considered new code.
Recommended for projects following regular versions or releases.

Define a specific setting for this project

Previous version
Any code that has changed since the previous version is considered new code.
Recommended for projects following regular versions or releases.

Number of days
Any code that has changed in the last x days is considered new code. If no action is taken on a new issue after x days, this issue will become part of the overall code.
Recommended for projects following continuous delivery.

Reference branch

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

Dashboard > Manage Jenkins > Plugins

Plugins

Updates 27

Available plugins

Installed plugins

Advanced settings

Q Sonarqube Scanner

Install Name : SonarQube Scanner 2.17.2 Released

External Site/Tool Integrations Build Reports 7 mo 12 days ago

This plugin allows an easy integration of SonarQube, the open source platform for Continuous Inspection of code quality.

Dashboard > Manage Jenkins > Plugins

Plugins

Updates 25

Available plugins

Installed plugins

Advanced settings

Download progress

Preparation

- Checking internet connectivity
- Checking update center connectivity
- Success

SonarQube Scanner Success

Loading plugin extensions Success

→ Go back to the top page
(you can start using the installed plugins right away)

- Under Jenkins ‘Manage Jenkins’ then go to ‘system’, scroll and look for SonarQube Servers and enter the details. Enter the Server Authentication token if needed.

Dashboard > Manage Jenkins > System >

SonarQube installations
List of SonarQube installations

Name: sonarqube

Server URL: Default is <http://localhost:9000>
http://localhost:9000

Server authentication token:
SonarQube authentication token. Mandatory when anonymous access is disabled.
- none -
+ Add ▾

Advanced ▾

Add SonarQube

Save Apply

- Search for SonarQube Scanner under Global Tool Configuration. Choose the latest configuration and choose Install automatically. Dashboard > Manage Jenkins > Tools

Dashboard > Manage Jenkins > Tools

Gradle installations
Add Gradle

SonarScanner for MSBuild installations
Add SonarScanner for MSBuild

SonarQube Scanner installations
Add SonarQube Scanner

Ant installations
Add Ant

Maven installations
Save Apply

- Check the “Install automatically” option. → Under name any name as identifier → Check the “Install automatically” option.

SonarQube Scanner installations

Add SonarQube Scanner

SonarQube Scanner

Name: sonarqube_exp8

Install automatically ?

Install from Maven Central

Version: SonarQube Scanner 6.2.0.4584

Add Installer ▾

Add SonarQube Scanner

Save Apply

- Generating a token on sonarqubes for authentication [optional]

Analysis Method > Locally

Analyze your project

We initialized your project on SonarQube, now it's up to you to launch analyses!

1 Provide a token

Token name ? Analyze "sonarqube-test"

Expires in 90 days

Please note that this token will only allow you to analyze the current project. If you want to use the same token to analyze multiple projects, you need to generate a global token in your [user account](#). See the [documentation](#) for more information.

The token is used to identify you when an analysis is performed. If it has been compromised, you can revoke it at any point in time in your [user account](#).

- Copy the token you get here and save it securely as we would need it in Jenkins.

Analysis Method > Locally

Analyze your project

We initialized your project on SonarQube, now it's up to you to launch analyses!

1 Provide a token

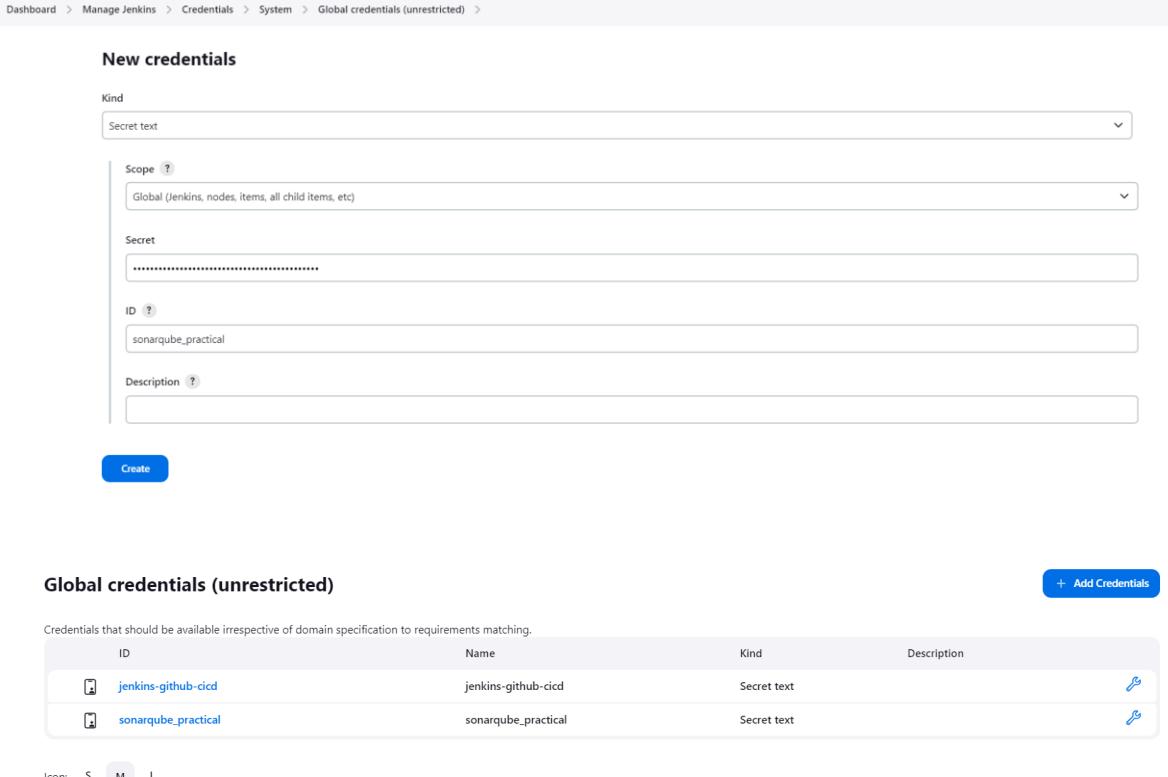
Analyze "sonarqube-test": sqp_35944e83f22ae4380284e2ff1e40e2ddf63a1706 

The token is used to identify you when an analysis is performed. If it has been compromised, you can revoke it at any point in time in your [user account](#).

[Continue](#)

- Update the Token in Jenkins

Click on global under the domains part of Stores scoped to Jenkins section. Further click on add credentials. Proceed with the following details. Make sure to copy the token generated earlier in sonarqube and give any suitable name as the ID.



The screenshot shows the Jenkins 'Global credentials (unrestricted)' page. A new credential is being created with the following details:

- Kind:** Secret text
- Scope:** Global (Jenkins, nodes, items, all child items, etc)
- Secret:** (redacted)
- ID:** sonarqube_practical
- Description:** (empty)

A blue 'Create' button is visible at the bottom left of the form.

Below the form, the 'Global credentials (unrestricted)' table lists two existing credentials:

ID	Name	Kind	Description
jenkins-github-cicd	jenkins-github-cicd	Secret text	
sonarqube_practical	sonarqube_practical	Secret text	

At the bottom left of the table, there are size icons: S, M, L.

- Now go to Manage Jenkins—>System—>SonarQube servers and proceed with the following details. Reference the authentication token generated in the previous step.

SonarQube servers

If checked, job administrators will be able to inject a SonarQube server configuration as environment variables in the build.

Environment variables

SonarQube installations

List of SonarQube installations

Name	sonarqube
Server URL	Default is http://localhost:9000 http://localhost:9000
Server authentication token	SonarQube authentication token. Mandatory when anonymous access is disabled. sonarqube_practical
+ Add	
Advanced	
Save	Apply

- After configuration, create a New Item → choose a pipeline project
Under Pipeline script, enter the following:
It is a java sample project which has a lot of repetitions and issues that will be detected by SonarQube.

Dashboard > sonarqube_practical > Configuration

Pipeline

Configure

General

Advanced Project Options

Pipeline

Definition

Pipeline script

```

1 + node {
2     stage('Cloning the GitHub Repo') {
3         git 'https://github.com/shafzforlot/GOL.git'
4     }
5     stage('SonarQube analysis') {
6         withSonarQubeEnv('sonarqube') {
7             bat """
8                 docker run --rm ^
9                 -e SONAR_HOST_URL=http://172.28.160.1:9000 ^
10                -v $WORKSPACE.replace("\\\\","\\\\\\\\"):/usr/src ^
11                sonar-project.properties ^
12                -Dsonar.projectKey=sonarqube-test ^
13                -Dsonar.sources=.^ ^
14                -Dsonar.exclusions=**/*.java,vendor/*,resources ^
15                -Dsonar.login=admin ^
16                -Dsonar.password=t ^
17                ...
18            """
19        }
20    }
}

```

Use Groovy Sandbox

Pipeline Syntax

[Save](#) [Apply](#)

➤ Build project

Dashboard > sonarqube_practical >

Status **sonarqube_practical**

- </> Changes
- ▷ Build Now
- ⚙ Configure
- >Delete Pipeline
- Full Stage View
- Stages
- Rename
- Pipeline Syntax

Stage View

	Cloning the GitHub Repo	SonarQube analysis
Average stage times: (Average full run time: ~9min 36s)	1s	1min 25s
#21 Sep 29, 2024, 4:34 PM 16:34 No Changes	1s	9min 34s
#20 Sep 29, 2024, 4:26 PM 16:26 No Changes	1s	1min 9s failed
#19 Sep 29, 2024, 4:26 PM 16:24 No Changes	2s	1min 6s failed
#18 Sep 29, 2024, 4:26 PM 16:23 No Changes	1s	1min 6s

➤ Check Console

Dashboard > sonarqube_practical > #21

Status **Console Output**

- </> Changes
- Console Output
- View as plain text
- Edit Build Information
- Delete build #21
- Timings
- Git Build Data
- Pipeline Overview
- Pipeline Console
- Replay
- Pipeline Steps
- Workspaces
- ← Previous Build

```
Started by user Tejas Dhondibhai Gunjal
[Pipeline] Start of Pipeline
[Pipeline] node
Running on Jenkins in C:\ProgramData\Jenkins\.jenkins\workspace\sonarqube_practical
[Pipeline] {
[Pipeline] stage
[Pipeline] { (Cloning the GitHub Repo)
[Pipeline] git
The recommended git tool is: NONE
No credentials specified
> git.exe rev-parse --resolve-git-dir C:\ProgramData\Jenkins\.jenkins\workspace\sonarqube_practical\.git # timeout=10
Fetching changes from the remote Git repository
> git.exe config remote.origin.url https://github.com/shazforiot/GOL.git # timeout=10
Fetching upstream changes from https://github.com/shazforiot/GOL.git
> git.exe --version # timeout=10
> git -v --version # git version 2.46.0.windows.1'
> git.exe fetch --tags --force --progress -- https://github.com/shazforiot/GOL.git +refs/heads/*:refs/remotes/origin/* # timeout=10
> git.exe rev-parse "refs/remotes/origin/master^{commit}" # timeout=10
Checking out Revision ba799ba7e1b576f04a4612322b0412c5e6e1e5e4 (refs/remotes/origin/master)
> git.exe config core.sparsecheckout # timeout=10
> git.exe checkout -f ba799ba7e1b576f04a4612322b0412c5e6e1e5e4 # timeout=10
> git.exe branch -a -v --no-abbrev # timeout=10
> git.exe branch -D master # timeout=10
> git.exe checkout -b master ba799ba7e1b576f04a4612322b0412c5e6e1e5e4 # timeout=10
Commit message: "Update Jenkinsfile"
> git.exe rev-list --no-walk ba799ba7e1b576f04a4612322b0412c5e6e1e5e4 # timeout=10
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
```

Dashboard > sonarqube_practical > #21

Status **Console Output**

- </> Changes
- Console Output
- View as plain text
- Edit Build Information
- Delete build #21
- Timings
- Git Build Data
- Pipeline Overview
- Pipeline Console
- Replay
- Pipeline Steps
- Workspaces
- ← Previous Build

```
Started by user Tejas Dhondibhai Gunjal
[Pipeline] Start of Pipeline
[Pipeline] node
Running on Jenkins in C:\ProgramData\Jenkins\.jenkins\workspace\sonarqube_practical
[Pipeline] {
[Pipeline] stage
[Pipeline] { (Cloning the GitHub Repo)
[Pipeline] git
The recommended git tool is: NONE
No credentials specified
> git.exe rev-parse --resolve-git-dir C:\ProgramData\Jenkins\.jenkins\workspace\sonarqube_practical\.git # timeout=10
Fetching changes from the remote Git repository
> git.exe config remote.origin.url https://github.com/shazforiot/GOL.git # timeout=10
Fetching upstream changes from https://github.com/shazforiot/GOL.git
> git.exe --version # timeout=10
> git -v --version # git version 2.46.0.windows.1'
> git.exe fetch --tags --force --progress -- https://github.com/shazforiot/GOL.git +refs/heads/*:refs/remotes/origin/* # timeout=10
> git.exe rev-parse "refs/remotes/origin/master^{commit}" # timeout=10
Checking out Revision ba799ba7e1b576f04a4612322b0412c5e6e1e5e4 (refs/remotes/origin/master)
> git.exe config core.sparsecheckout # timeout=10
> git.exe checkout -f ba799ba7e1b576f04a4612322b0412c5e6e1e5e4 # timeout=10
> git.exe branch -a -v --no-abbrev # timeout=10
> git.exe branch -D master # timeout=10
> git.exe checkout -b master ba799ba7e1b576f04a4612322b0412c5e6e1e5e4 # timeout=10
Commit message: "Update Jenkinsfile"
> git.exe rev-list --no-walk ba799ba7e1b576f04a4612322b0412c5e6e1e5e4 # timeout=10
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
```

➤ Now, check the project in SonarQube

SonarQube Overview for sonarqube-test project.

- Security:** 0 Open issues
- Reliability:** 68k Open issues
- Maintainability:** 164k Open issues
- Accepted issues:** 0
- Coverage:** 50.6%
- Duplications:** 50.6%
- Security Hotspots:** 3

➤ Code Problems

Consistency

SonarQube Issues page for sonarqube-test project, filtered by Consistency.

- Issues in new code:**
 - Insert a <!DOCTYPE> declaration to before this <html> tag. (Consistency, user-experience)
 - Remove this deprecated "width" attribute. (Consistency, html5 obsolete)
 - Remove this deprecated "align" attribute. (Consistency, html5 obsolete)

Intentionality

SonarQube Issues page for sonarqube-test project, filtered by Intentionality.

- Issues in new code:**
 - Use a specific version tag for the image. (Intentionality, No tags)
 - Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. (Intentionality, No tags)
 - Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. (Intentionality, No tags)

Bugs

SonarQube Projects Issues Rules Quality Profiles Quality Gates Administration More Q

sonarqube-test / main

Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information

Issues in new code

Bulk Change Select issues Navigate to issue 13,872 issues 59d effort

Clean Code Attribute

- Consistency 54k
- Intentionality 14k
- Adaptability 0
- Responsibility 0

Add to selection Ctrl + click

Software Quality

- Security 0
- Reliability 14k
- Maintainability 15

Add to selection Ctrl + click

gameoflife-core/build/reports/tests/all-tests.html

Add "lang" and/or "xml:lang" attributes to this "<html>" element Intentionality Reliability Open - Not assigned L1 - 2min effort - 4 years ago - Bug - Major accessibility wcag2-a

Add "<th>" headers to this "<table>". Intentionality Reliability Open - Not assigned L9 - 2min effort - 4 years ago - Bug - Major accessibility wcag2-a

gameoflife-core/build/reports/tests/allclasses-frame.html

Add "lang" and/or "xml:lang" attributes to this "<html>" element Intentionality Reliability Open - Not assigned L1 - 2min effort - 4 years ago - Bug - Major accessibility wcag2-a

Code Smells

SonarQube Projects Issues Rules Quality Profiles Quality Gates Administration More Q

sonarqube-test / main

Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information

Issues in new code

Bulk Change Select issues Navigate to issue 15 issues 44min effort

Clean Code Attribute

- Consistency 164k
- Intentionality 15
- Adaptability 0
- Responsibility 0

Add to selection Ctrl + click

Software Quality

- Security 0
- Reliability 14k
- Maintainability 15

Add to selection Ctrl + click

gameoflife-acceptance-tests/Dockerfile

Use a specific version tag for the image. Intentionality Maintainability Open - Not assigned L1 - 5min effort - 4 years ago - Code Smell - Major No tags

Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. Intentionality Maintainability Open - Not assigned L12 - 5min effort - 4 years ago - Code Smell - Major No tags

Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. Intentionality Maintainability Open - Not assigned L17 - 5min effort - 4 years ago - Code Smell - Major No tags

Reliability

SonarQube Projects Issues Rules Quality Profiles Quality Gates Administration More Q

sonarqube-test / main

Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information

Overall Code

Issues 0 Rating A Remediation Effort 0

Reliability

Overview

Overall Code

Issues 67624 Rating C Remediation Effort 1426d

Maintainability

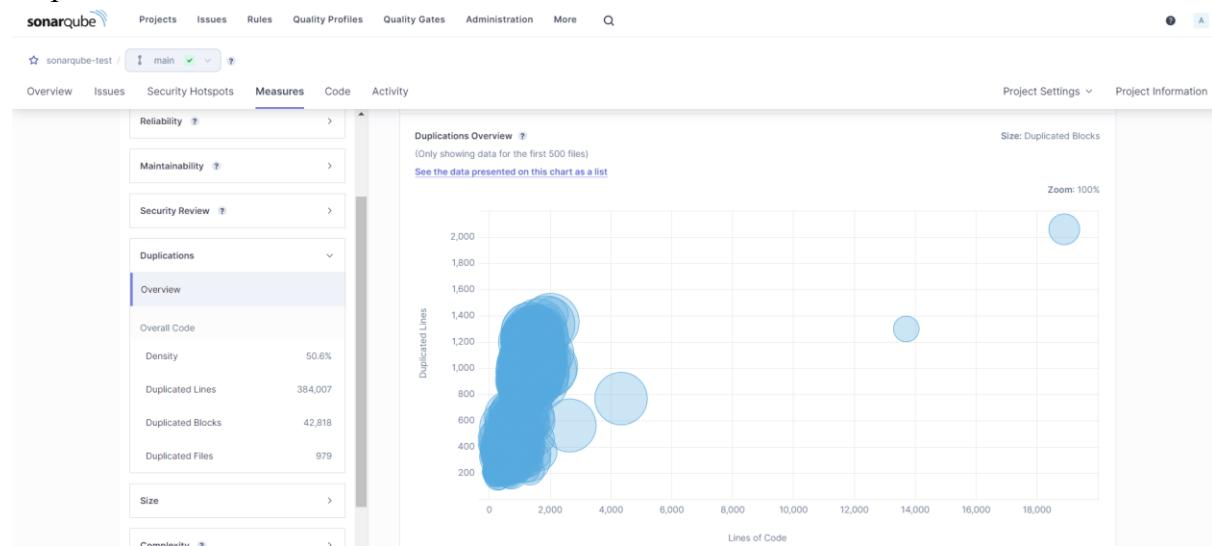
Security Review

Reliability Overview (Only showing data for the first 500 files) See the data presented on this chart as a list Color: Reliability Rating Size: Bugs Zoom: 184% Reset

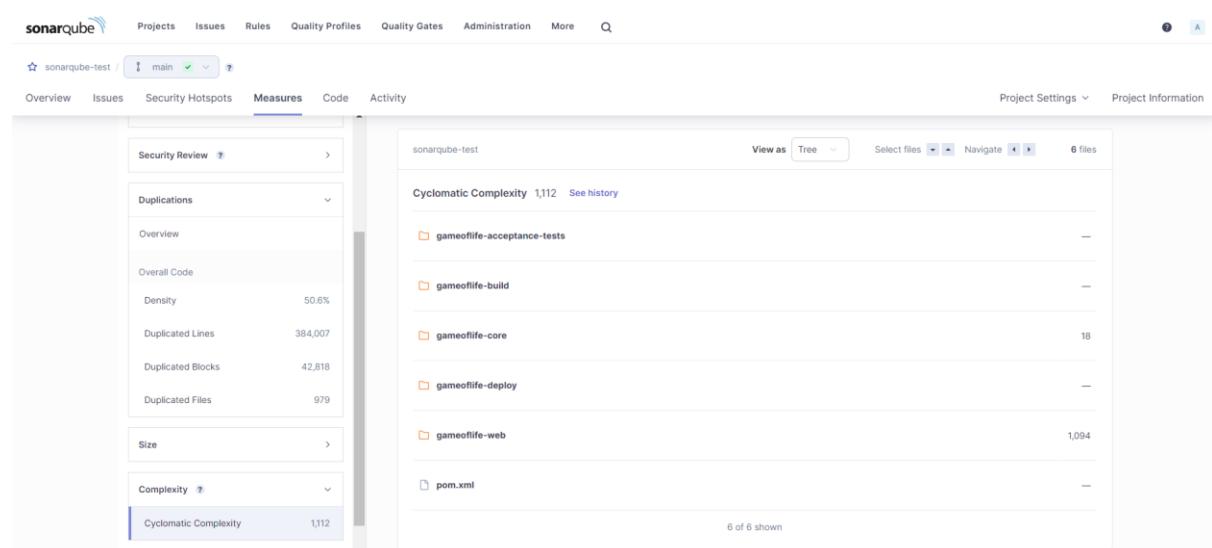
Reliability Remediation Effort

Lines of Code

Duplications



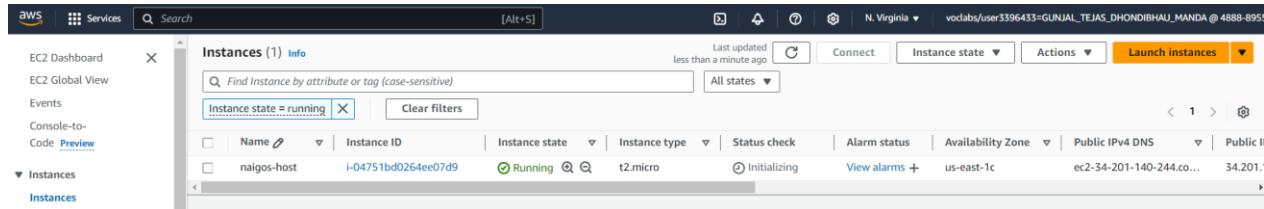
Cyclomatic Complexities



EXPERIMENT NO :- 09

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

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



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

Inbound rules (7)							<input type="button" value="C"/>	Manage tags	Edit inbound rules
	Name	Security group rule...	IP version	Type	Protocol	Port range		Source	
<input type="checkbox"/>	-	sgr-02a9f3b07b74c6b99	IPv4	All traffic	All	All		0.0.0.0/0	
<input type="checkbox"/>	-	sgr-06bc1bda1cab4310b	IPv4	HTTP	TCP	80		0.0.0.0/0	
<input type="checkbox"/>	-	sgr-0326ed648d9ec08...	IPv4	Custom TCP	TCP	0		0.0.0.0/0	
<input type="checkbox"/>	-	sgr-0d9f700fbeef6cd54	IPv6	Custom TCP	TCP	0		::/0	
<input type="checkbox"/>	-	sgr-09de549ee0cd724...	IPv4	All ICMP - IPv4	ICMP	All		0.0.0.0/0	
<input type="checkbox"/>	-	sgr-06a0c86195a574ae2	IPv4	HTTPS	TCP	443		0.0.0.0/0	
<input type="checkbox"/>	-	sgr-0ee64d6378e641b...	IPv4	All ICMP - IPv6	IPv6 ICMP	All		0.0.0.0/0	

- Connect to your EC2 instance via the connect option available in EC2 instances menu. After that command prompt will be started.

```

aws | Services | Search [Alt+S]
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-172-31-46-179 ~]$ sudo yum install httpd php
Last metadata expiration check: 0:07:53 ago on Sun Oct 6 15:35:40 2024.
Dependencies resolved.

```

➤ Update and install the required packages

```
sudo yum install httpd php
```

Package	Architecture	Version	Repository	S
Installing:				
httpd	x86_64	2.4.62-1.amzn2023	amazonlinux	4
php8.3	x86_64	8.3.10-1.amzn2023.0.1	amazonlinux	1
Installing dependencies:				
apr	x86_64	1.7.2-2.amzn2023.0.2	amazonlinux	12
apr-util	x86_64	1.6.3-1.amzn2023.0.1	amazonlinux	9
generic-logos-httdp	noarch	18.0.0-12.amzn2023.0.3	amazonlinux	1
httpd-core	x86_64	2.4.62-1.amzn2023	amazonlinux	1.
httpd-filesystem	noarch	2.4.62-1.amzn2023	amazonlinux	1
httpd-tools	x86_64	2.4.62-1.amzn2023	amazonlinux	8
libbrotli	x86_64	1.0.9-4.amzn2023.0.2	amazonlinux	31
libsodium	x86_64	1.0.19-4.amzn2023	amazonlinux	17
libsxtl	x86_64	1.1.34-5.amzn2023.0.2	amazonlinux	24
mailcap	noarch	2.1.49-3.amzn2023.0.3	amazonlinux	3
nginx-filesystem	noarch	1:1.24.0-1.amzn2023.0.4	amazonlinux	9.
php8.3-cli	x86_64	8.3.10-1.amzn2023.0.1	amazonlinux	3.
php8.3-common	x86_64	8.3.10-1.amzn2023.0.1	amazonlinux	73
php8.3-process	x86_64	8.3.10-1.amzn2023.0.1	amazonlinux	4
php8.3-xml	x86_64	8.3.10-1.amzn2023.0.1	amazonlinux	15
Installing weak dependencies:				
apr-util-openssl	x86_64	1.6.3-1.amzn2023.0.1	amazonlinux	1
mod http2	x86_64	2.0.27-1.amzn2023.0.3	amazonlinux	16
mod lua	x86_64	2.4.62-1.amzn2023	amazonlinux	6
mod fpm	x86_64	8.3.10-1.amzn2023.0.1	amazonlinux	1.

```
sudo yum install gcc glibc glibc-common
```

Package	Architecture	Version	Repository	S
Installing:				
gcc	x86_64	11.4.1-2.amzn2023.0.2	amazonlinux	3
Installing dependencies:				
annobin-docs	noarch	10.93-1.amzn2023.0.1	amazonlinux	9
annobin-plugin-gcc	x86_64	10.93-1.amzn2023.0.1	amazonlinux	88
cpp	x86_64	11.4.1-2.amzn2023.0.2	amazonlinux	1
gc	x86_64	8.0.4-5.amzn2023.0.2	amazonlinux	10
glibc-devel	x86_64	2.34-52.amzn2023.0.11	amazonlinux	2
glibc-headers-x86	noarch	2.34-52.amzn2023.0.11	amazonlinux	42
guile22	x86_64	2.2.7-2.amzn2023.0.3	amazonlinux	6
kernel-headers	x86_64	6.1.109-118.199.amzn2023	amazonlinux	1.
libmpc	x86_64	1.2.1-2.amzn2023.0.2	amazonlinux	6
libtool-ltdl	x86_64	2.4.7-1.amzn2023.0.3	amazonlinux	3
libxcrypt-devel	x86_64	4.4.33-7.amzn2023	amazonlinux	3
make	x86_64	1:4.3-5.amzn2023.0.2	amazonlinux	53
Transaction Summary				
Install 13 Packages				
Total download size: 52 M				
Installed size: 168 M				
Is this ok [y/N]: y				

```
sudo yum install gd gd-devel
```

Package	Architecture	Version	Repository	S
Installing:				
gd	x86_64	2.3.3-5.amzn2023.0.3	amazonlinux	13
gd-devel	x86_64	2.3.3-5.amzn2023.0.3	amazonlinux	3
Installing dependencies:				
brotli	x86_64	1.0.9-4.amzn2023.0.2	amazonlinux	31
brotli-devel	x86_64	1.0.9-4.amzn2023.0.2	amazonlinux	3
bzip2-devel	x86_64	1.0.8-6.amzn2023.0.2	amazonlinux	21
cairo	x86_64	1.17.6-2.amzn2023.0.1	amazonlinux	68
cmake-filesystem	x86_64	3.22.2-1.amzn2023.0.4	amazonlinux	1
fontconfig	x86_64	2.13.94-2.amzn2023.0.2	amazonlinux	27
fontconfig-devel	x86_64	2.13.94-2.amzn2023.0.2	amazonlinux	12
fonts-filesystem	noarch	1:2.0.5-12.amzn2023.0.2	amazonlinux	9.
freetype	x86_64	2.13.2-5.amzn2023.0.1	amazonlinux	42
freetype-devel	x86_64	2.13.2-5.amzn2023.0.1	amazonlinux	91
glib2-devel	x86_64	2.74.7-699.amzn2023.0.2	amazonlinux	48
google-noto-fonts-common	noarch	20201206-2.amzn2023.0.2	amazonlinux	1
google-noto-sans-vf-fonts	noarch	20201206-2.amzn2023.0.2	amazonlinux	49
graphite2	x86_64	1.3.14-7.amzn2023.0.2	amazonlinux	9
graphite2-devel	x86_64	1.3.14-7.amzn2023.0.2	amazonlinux	2
harfbuzz	x86_64	7.0.0-2.amzn2023.0.1	amazonlinux	86
harfbuzz-devel	x86_64	7.0.0-2.amzn2023.0.1	amazonlinux	40
harfbuzz-icu	x86_64	7.0.0-2.amzn2023.0.1	amazonlinux	1
jbigkit-libs	x86_64	2.1-21.amzn2023.0.2	amazonlinux	5
langpacks-core-font-en	noarch	3.0-21.amzn2023.0.4	amazonlinux	1
libICE	x86_64	1.0.10-6.amzn2023.0.2	amazonlinux	7

```

Verifying : sysprof-capture-devel-3.40.1-2.amzn2023.0.2.x86_64
Verifying : xml-common-0.6.3-56.amzn2023.0.2.noarch
Verifying : xorg-x11proto-devel-2021.4-1.amzn2023.0.2.noarch
Verifying : xz-devel-5.2.5-9.amzn2023.0.2.x86_64
Verifying : zlib-devel-1.2.11-33.amzn2023.0.5.x86_64

Installed:
brotli-1.0.9-4.amzn2023.0.2.x86_64
cairo-1.17.6-2.amzn2023.0.1.x86_64
fontconfig-devel-2.13.94-2.amzn2023.0.2.x86_64
freetype-devel-2.13.2-3.amzn2023.0.1.x86_64
glib2-devel-2.74.7-69.amzn2023.0.2.x86_64
graphite2-devel-1.3.14-7.amzn2023.0.2.x86_64
harfbuzz-devel-7.0.0-1.amzn2023.0.1.x86_64
lambdocks-core-font-enc-0.2-1.amzn2023.0.4.noarch
libX11-1.7.2-3.amzn2023.0.1.x86_64
libX11-xcb-1.2-3.amzn2023.0.2.x86_64
libXext-1.3.4-1.amzn2023.0.2.x86_64
libXinerama-0.9.10-14.amzn2023.0.1.x86_64
libXrender-1.4.4-1.amzn2023.0.1.x86_64
libXtiff-devel-3.4.4-2.amzn2023.0.5.x86_64
libzipng-2.1.6-37-10.amzn2023.0.6.x86_64
libzepo-devel-3.4-3.amzn2023.0.3.x86_64
libwebp-1.2.4-1.amzn2023.0.6.x86_64
libxcb-devel-1.13.1-7.amzn2023.0.2.x86_64
pcre2-utf16-10.40-1.amzn2023.0.3.x86_64
sysprof-capture-devel-3.40.1-2.amzn2023.0.2.x86_64
xz-devel-5.2.5-9.amzn2023.0.2.x86_64

bzip2-devel-1.0.8-6.amzn2023.0.2.x86_64
fontconfig-2.13.94-2.amzn2023.0.2.x86_64
freetype-2.13.2-5.amzn2023.0.1.x86_64
gd-devel-3.3.5.amzn2023.0.3.x86_64
google-noto-fonts-complete-2021206-2.amzn2023.0.2.noarch
graphite2-devel-1.3.14-7.amzn2023.0.2.x86_64
harfbuzz-7.0.0-2.amzn2023.0.3.x86_64
jbigkit-l1bs-2.1-21.amzn2023.0.2.x86_64
libBOM-1.2.3-8.amzn2023.0.2.x86_64
libX11-devel-1.7.2-3.amzn2023.0.4.x86_64
libXau-1.0.9-6.amzn2023.0.2.x86_64
libXpm-1.5.15-2.amzn2023.0.3.x86_64
libXt-1.2.0-4.amzn2023.0.3.x86_64
libXt-1.7.amzn2023.0.3.x86_64
libXtiff-3.4-2.amzn2023.0.5.x86_64
libzipng-turbo-devel-2.1.4-2.amzn2023.0.6.x86_64
libzepo-devel-1.6.37-10.amzn2023.0.6.x86_64
libzepo-devel-3.4-5.amzn2023.0.2.x86_64
libwebp-devel-1.2.4-1.amzn2023.0.6.x86_64
libxcb-devel-2.10.4-1.amzn2023.0.6.x86_64
pcre2-utf32-10.40-1.amzn2023.0.3.x86_64
xml-common-0.6.3-56.amzn2023.0.2.noarch
zlib-devel-1.2.11-33.amzn2023.0.5.x86_64

Complete!
[ec2-user@ip-172-31-46-179 ~]$ 

```

- Create a new nagios user by writing the following commands


```
sudo adduser -m nagios
sudo passwd nagios
```

```

[ec2-user@ip-172-31-46-179 ~]$ sudo adduser -m nagios
[ec2-user@ip-172-31-46-179 ~]$ sudo passwd nagios
Changing password for user nagios.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[ec2-user@ip-172-31-46-179 ~]$ 

```

- Create a new user group using sudo groupadd nagcmd and add users to the group using the following commands

```

[ec2-user@ip-172-31-46-179 ~]$ sudo usermod -a -G nagcmd nagios
usermod: group 'nagcmd' does not exist
[ec2-user@ip-172-31-46-179 ~]$ sudo groupadd nagcmd
[ec2-user@ip-172-31-46-179 ~]$ sudo usermod -a -G nagcmd naigod
usermod: user 'naigod' does not exist
[ec2-user@ip-172-31-46-179 ~]$ sudo usermod -a -G nagcmd naigos
[ec2-user@ip-172-31-46-179 ~]$ sudo usermod -a -G nagcmd apache
[ec2-user@ip-172-31-46-179 ~]$ 

```

- Create a directory for Nagios downloads using the following commands and Also download Nagios and plugin source files


```
wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz
wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz
```

```

[ec2-user@ip-172-31-46-179 ~]$ mkdir downloads
[ec2-user@ip-172-31-46-179 ~]$ cd downloads
[ec2-user@ip-172-31-46-179 ~]$ wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz
--2024-10-06 16:03:26-- 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:fe7:45ce
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 11.0MB/s   in 1.0s

2024-10-06 16:03:27 (11.0 MB/s) - 'nagios-4.4.6.tar.gz' saved [11333414/11333414]

--2024-10-06 16:03:27-- 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 7.08MB/s   in 0.4s

2024-10-06 16:03:28 (7.08 MB/s) - 'nagios-plugins-2.3.3.tar.gz' saved [2782610/2782610]

[ec2-user@ip-172-31-46-179 downloads]$ 

```

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

```
[ec2-user@ip-172-31-46-179 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
nagios-4.4.6/autoconf-macros/ax_nagios_get_os
nagios-4.4.6/autoconf-macros/ax_nagios_get_paths
nagios-4.4.6/autoconf-macros/ax_nagios_get_ssl
nagios-4.4.6/base/
nagios-4.4.6/base/.gitignore
nagios-4.4.6/base/Makefile.in
```

- Listing out all the files present in the nagios directory

```
[ec2-user@ip-172-31-46-179 nagios-4.4.6]$ ls -l
total 704
-rw-r--r--. 1 ec2-user ec2-user 6291 Apr 28 2020 CONTRIBUTING.md
-rw-r--r--. 1 ec2-user ec2-user 32590 Apr 28 2020 Changelog
-rw-r--r--. 1 ec2-user ec2-user 422 Apr 28 2020 INSTALLING
-rw-r--r--. 1 ec2-user ec2-user 841 Apr 28 2020 LICENSE
-rw-r--r--. 1 ec2-user ec2-user 18002 Apr 28 2020 LICENSE
-rw-r--r--. 1 ec2-user ec2-user 16506 Apr 28 2020 Makefile.in
-rw-r--r--. 1 ec2-user ec2-user 3395 Apr 28 2020 README.md
-rw-r--r--. 1 ec2-user ec2-user 5832 Apr 28 2020 THANKS
-rw-r--r--. 1 ec2-user ec2-user 643 Apr 28 2020 UPGRADING
-rwxr-xr-x. 1 ec2-user ec2-user 346 Apr 28 2020 aclocal.m4
drwxr-xr-x. 2 ec2-user ec2-user 16384 Apr 28 2020 autoconf-macros
drwxr-xr-x. 2 ec2-user ec2-user 16384 Apr 28 2020 base
drwxr-xr-x. 2 ec2-user ec2-user 16384 Apr 28 2020 cgi
drwxr-xr-x. 2 ec2-user ec2-user 148 Apr 28 2020 common
-rwxr-xr-x. 1 ec2-user ec2-user 43765 Apr 28 2020 config.guess
-rwxr-xr-x. 1 ec2-user ec2-user 36345 Apr 28 2020 config.sub
-rwxr-xr-x. 1 ec2-user ec2-user 246354 Apr 28 2020 configure
-rw-r--r--. 1 ec2-user ec2-user 29812 Apr 28 2020 configure.ac
drwxr-xr-x. 5 ec2-user ec2-user 16384 Apr 28 2020 contrib
drwxr-xr-x. 2 ec2-user ec2-user 129 Apr 28 2020 docs
-rw-r--r--. 1 ec2-user ec2-user 886 Apr 28 2020 doxy.conf
-rwxr-xr-x. 1 ec2-user ec2-user 7025 Apr 28 2020 functions
drwxr-xr-x. 11 ec2-user ec2-user 16384 Apr 28 2020 html
drwxr-xr-x. 2 ec2-user ec2-user 16384 Apr 28 2020 include
-rwxr-xr-x. 1 ec2-user ec2-user 77 Apr 28 2020 indent-all.sh
-rwxr-xr-x. 1 ec2-user ec2-user 161 Apr 28 2020 indent.sh
-rwxr-xr-x. 1 ec2-user ec2-user 5869 Apr 28 2020 install-sh
drwxr-xr-x. 2 ec2-user ec2-user 16384 Apr 28 2020 lib
-rwxr-xr-x. 1 ec2-user ec2-user 461 Apr 28 2020 make-tarball
```

- Then run the configuration script with the following command

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

```
[ec2-user@ip-172-31-46-179 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
checking for string.h... yes
checking for memory.h... yes
checking for strings.h... yes
checking for inttypes.h... yes
checking for stdint.h... yes
checking for unistd.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.

```
[ec2-user@ip-172-31-46-179 nagios-4.4.6]$
```

- Compile the source code with the following commands make all

```
inflating: dist/css/bootstrap-theme.css
inflating: dist/css/bootstrap-theme.min.css.map
inflating: dist/css/bootstrap-theme.css.map
inflating: dist/css/bootstrap.min.css
inflating: dist/css/bootstrap-theme.min.css
inflating: dist/css/bootstrap.css
mkdir -p d3
(cd d3 && unzip -u ../d3-3.5.17.zip)
Archive: ./d3-3.5.17.zip
inflating: bower.json
inflating: d3.js
inflating: d3.min.js
inflating: LICENSE
inflating: README.md
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-4.4.6/html'
if [ xyes = xyes ]; then \
    cd ./module && make; \
fi
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.4.6/module'
gcc -I.. -fPIC -g -O2 -DHAVE_CONFIG_H -o helloworld.o helloworld.c -shared
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-4.4.6/module'
cd ./worker && make all
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.4.6/worker'
cd ./ping && make all
make[2]: Entering directory '/home/ec2-user/downloads/nagios-4.4.6/worker/ping'
gcc -I../../include -I ../../ -g -O2 -DHAVE_CONFIG_H -o worker-ping worker-ping.c -L ../../lib -l nagios
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-4.4.6/worker/ping'
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-4.4.6/worker'

*** Compile finished ***
```

- Install binaries,init script and sample config files

sudo make install

```
nagios:x:1002:1003::/home/nagios:/bin/bash
[ec2-user@ip-172-31-46-179 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 /usr/local/nagios/bin
/usr/bin/install -c -s -m 774 -o nagios -g nagios nagiosstats /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
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/images
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/images/logos
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/includes
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/ssi
```

sudo make install-init

sudo make install-config

```
[ec2-user@ip-172-31-46-179 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/switc.cfg /usr/local/nagios/etc/objects/switc.cfg

*** Config files installed ***
Remember, these are *SAMPLE* config files. You'll need to read
the documentation for more information on how to actually define
services, hosts, etc. to fit your particular needs.
```

sudo make install-commandmode

```
[ec2-user@ip-172-31-46-179 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-172-31-46-179 nagios-4.4.6]$
```

➤ Edit the Config File to Change the Email Address

```
#####
# CONTACTS.CFG - SAMPLE CONTACT/CONTACTGROUP DEFINITIONS
#
#
# NOTES: This config file provides you with some example contact and contact
# group definitions that you can reference in host and service
# definitions.
#
# You don't need to keep these definitions in a separate file from your
# other object definitions. This has been done just to make things
# easier to understand.
#
#####
#
# CONTACTS
#
#
# Just one contact defined by default - the Nagios admin (that's you)
# This contact definition inherits a lot of default values from the
# 'generic-contact' template which is defined elsewhere.

define contact {
    contact_name      nagiosadmin          ; Short name of user
    use               generic-contact       ; Inherit default values from generic-contact template (defined above)
    alias             Nagios Admin         ; Full name of user
    email             tejasgunjal021@gmail.com ; <***** CHANGE THIS TO YOUR EMAIL ADDRESS *****

}

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

[ Read 51 lines ]
^G Help           ^C Write Out        ^W Where Is        ^K Cut            ^T Execute        [ Location        M-U Undo
^X Exit           ^R Read File         ^\ Replace         ^U Paste          ^J Justify        ^/ Go To Line     M-E Redo
                                         M-A Set Mark      M-J To
                                         M-G Copy          ^Q Wher
```

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

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

define contact {
    contact_name      nagiosadmin          ; Short name of user
    use               generic-contact       ; Inherit default values from generic-contact template (defined above)
    alias             Nagios Admin         ; Full name of user
    email             tejasgunjal021@gmail.com ; <***** CHANGE THIS TO YOUR EMAIL ADDRESS *****

}

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

[ Wrote 51 lines ]
^G Help           ^C Write Out        ^W Where Is        ^K Cut            ^T Execute        [ Location        M-U Undo
^X Exit           ^R Read File         ^\ Replace         ^U Paste          ^J Justify        ^/ Go To Line     M-E Redo
                                         M-A Set Mark      M-J To
                                         M-G Copy          ^Q Wher
```

➤ Extract the Plugins Source File

```
[ec2-user@ip-172-31-46-179 nagios-4.4.6]$ cd ..
[ec2-user@ip-172-31-46-179 downloads]$ tar zxfv 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
nagios-plugins-2.3.3/Makefile.in
nagios-plugins-2.3.3/config.h.in
nagios-plugins-2.3.3/ChangeLog
nagios-plugins-2.3.3/AUTHORS
nagios-plugins-2.3.3/lib/
nagios-plugins-2.3.3/lib/parse_ini.h
```

➤ Create a Nagios Admin Account

```
[ec2-user@ip-172-31-46-179 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-172-31-46-179 nagios-4.4.6]$
```

➤ Compile and Install Plugins

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

```
[ec2-user@ip-172-31-46-179 nagios-4.4.6]$ configure --with-nagios-user=nagios --with-nagios-group=nagios
make
-bash: configure: command not found
Please supply a command line argument (i.e. 'make all'). Other targets are:
  nagios  cgi contrib modules workers
  test
  install           install-base
  install-cgis      install-html
  install-webconf   install-config
  install-init      install-daemoninit
  install-commandmode install-groups-users
  install-exfoliation  install-classicui
  install-basic     install-unstripped
  fullinstall
  clean
[ec2-user@ip-172-31-46-179 nagios-4.4.6]$
```

➤ Start Nagios

```
sudo chkconfig --add nagios
```

```
sudo chkconfig nagios on
```

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

```
sudo systemctl start nagios
```

```
[ec2-user@ip-172-31-46-179 nagios-4.4.6]$ sudo chkconfig --add nagios
sudo chkconfig nagios on
sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
sudo systemctl start nagios
error reading information on service nagios: No such file or directory
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.

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.
```

```

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
Total Errors: 0

Things look okay - No serious problems were detected during the pre-flight check
[ec2-user@ip-172-31-46-179 nagios-4.4.6]$

```

➤ Verify the sample configuration files

```

[ec2-user@ip-172-31-46-179 nagios-4.4.6]$ 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

```

➤ If there are no errors, you can go ahead and start Nagios and Check the status of Nagios

```

[ec2-user@ip-172-31-46-179 nagios-4.4.6]$ sudo service nagios start
Redirecting to /bin/systemctl start nagios.service
[ec2-user@ip-172-31-46-179 nagios-4.4.6]$ 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 2024-10-06 16:37:12 UTC; 1h 47min ago
     Docs: https://www.nagios.org/documentation
 Main PID: 49199 (nagios)
   Tasks: 8 (limit: 1112)
    Memory: 3.7M
      CPU: 1.379s
     CGroup: /system.slice/nagios.service
             └─49199 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
                 ├─49200 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
                 ├─49201 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
                 ├─49202 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
                 ├─49203 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
                 ├─49204 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
                 ├─73692 /usr/local/nagios/libexec/check_ping -H 127.0.0.1 -w 100.0,20% -c 500.0,60% -p 5
                 └─73693 /usr/bin/ping -n -U -w 10 -c 5 127.0.0.1

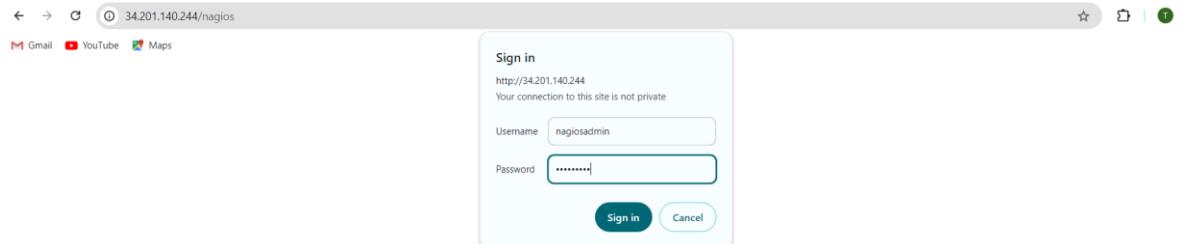
Oct 06 16:58:27 ip-172-31-46-179.ec2.internal nagios[49199]: SERVICE ALERT: localhost;Current Users:OK;SOFT;1;USERS OK - 1 users currently logged in
Oct 06 16:59:46 ip-172-31-46-179.ec2.internal nagios[49199]: SERVICE ALERT: localhost;PING:OK;SOFT;1;PING OK - Packet loss = 0%, RTA = 0.04 ms
Oct 06 17:37:12 ip-172-31-46-179.ec2.internal nagios[49199]: Auto-save of retention data completed successfully.
Oct 06 17:56:34 ip-172-31-46-179.ec2.internal nagios[49199]: SERVICE NOTIFICATION: nagiosadmin;localhost;Swap Usage:CRITICAL;notify-service-by-email;SWP
Oct 06 17:56:34 ip-172-31-46-179.ec2.internal nagios[49199]: wproc: NOTIFY job 38 from worker Core Worker 49202 is a non-check helper but exited with re
Oct 06 17:56:34 ip-172-31-46-179.ec2.internal nagios[49199]: wproc: host=localhost; service=Swap Usage; contact=nagiosadmin
Oct 06 17:56:34 ip-172-31-46-179.ec2.internal nagios[49199]: wproc: early_timeout=0; exited_ok=1; wait_status=32512; error_code=0;
Oct 06 17:56:34 ip-172-31-46-179.ec2.internal nagios[49199]: wproc: stderr line 01: /bin/sh: line 1: /bin/mail: No such file or directory

```

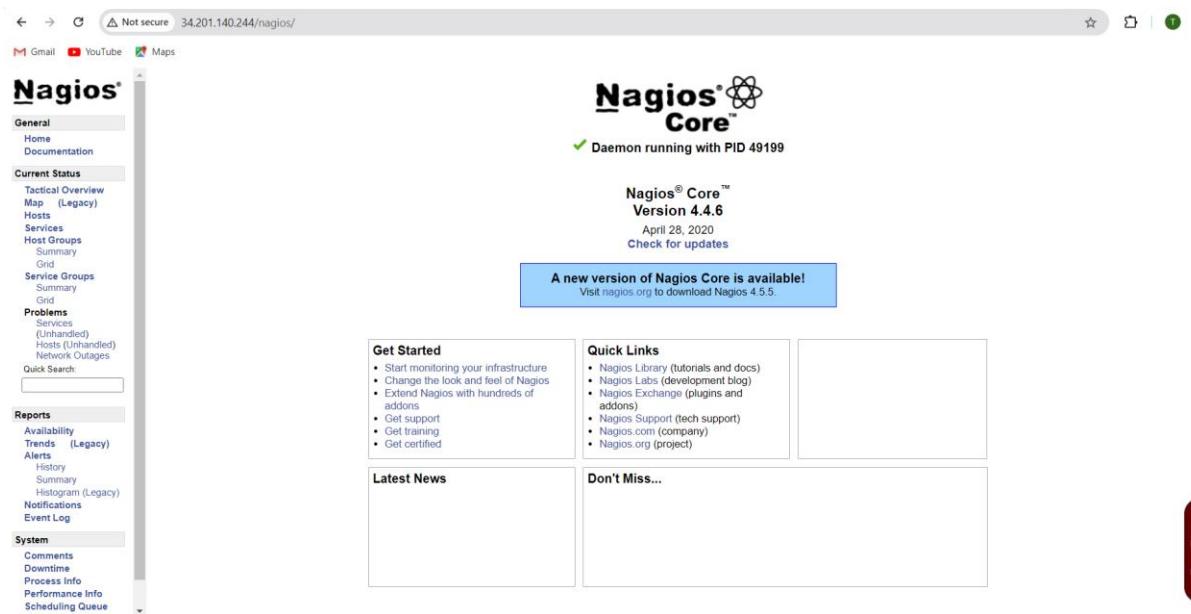
➤ Access Nagios Web Interface

Copy the Public IP address of your EC2 instance.
Open your browser and navigate to <http://nagios>.

➤ Enter username as nagiosadmin and password you set



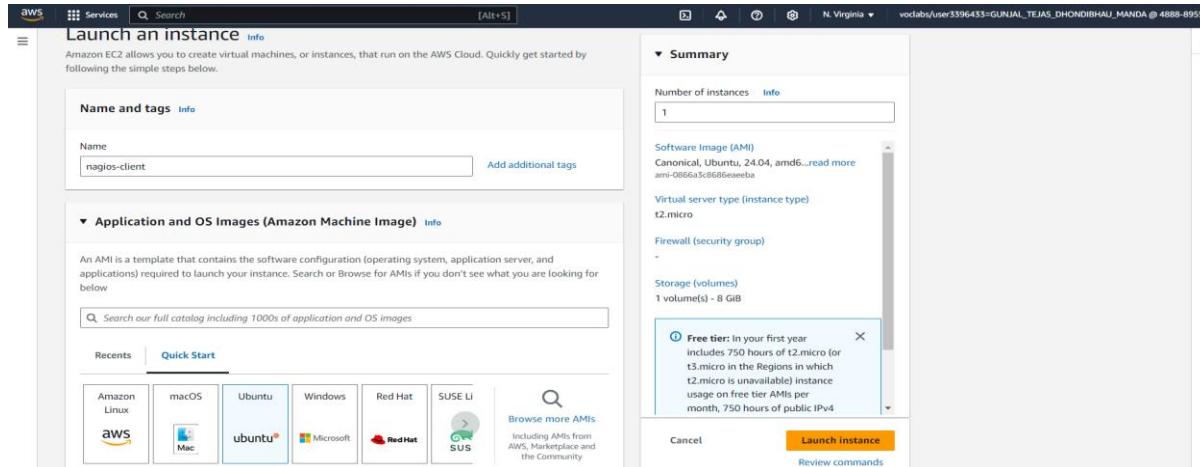
➤ After sign in, this page will be displayed.
This means that Nagios was correctly installed and configured with its plugins so far.



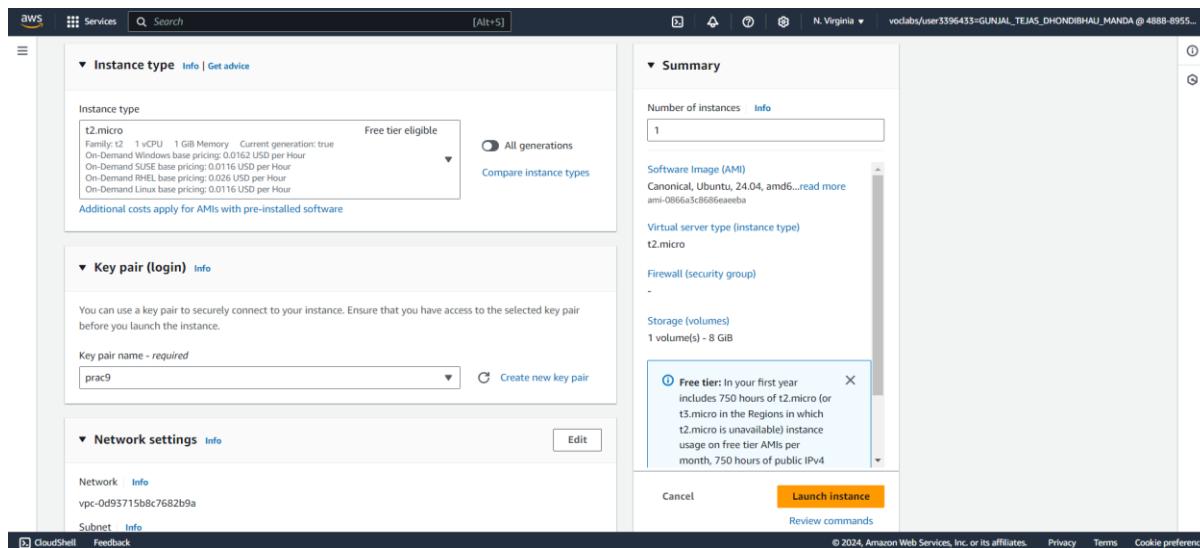
EXPERIMENT NO: - 10

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

- Launch an instance



- Select Ubuntu as the os give a meaningful name of the instance.
Make sure to select the same key-pair login used in the prac9 machine



- Click on launch instance.

The screenshot shows the AWS EC2 Launch Instance wizard. In the 'Network settings' section, it shows a VPC (vpc-0d93715bb8c7682b9a) and a subnet (No preference). Under 'Configure storage', a 1x 8 GiB gp3 volume is selected as the root volume. In the 'Summary' step, it shows 1 instance and 1 volume (8 GiB). A tooltip for the 'Free tier' is displayed, stating: '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, 30 GB of EBS storage, 2 million IOPS, 1 GB of snapshots, and 100 GB of bandwidth to the internet.' A large orange 'Launch instance' button is visible at the bottom right.

Attribute	Value
Number of instances	1
Storage (volumes)	1 volume(s) - 8 GiB

Instances (2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IP
naigos-host	i-04751bd0264ee07d9	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1c	ec2-3-80-236-69.compute...	3.80.236
naigos-client	i-0f5fd467f2577ca3f	Running	t2.micro	Initializing	View alarms +	us-east-1c	ec2-54-145-178-15.compute...	54.145.1

- Now connect with this client machine using the ssh through your terminal(open a new terminal in your local machine and we will need both of the terminals open)

The screenshot shows the 'Connect to instance' dialog for the instance i-0f5fd467f2577ca3f (nagios-client). It provides instructions for connecting via SSH, including opening an SSH client, locating a private key file (prac9.pem), running chmod 400 on it, and connecting to its Public DNS (ec2-54-145-178-15.compute-1.amazonaws.com). A note at the bottom states: 'Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.' A 'Cancel' button is at the bottom right.

- Nagios Host

The screenshot shows a terminal window titled 'Nagios Host'. The command entered is: `C:\Users\TEJAS>ssh -i "C:\Users\TEJAS\Downloads\prac9.pem" ec2-user@ec2-3-80-236-69.compute-1.amazonaws.com`. The response shows the Amazon Linux 2023 logo and the URL `https://aws.amazon.com/linux/amazon-linux-2023`. At the bottom, it says 'Last login: Mon Oct 7 13:03:39 2024 from 120.88.190.21'.

```
C:\Users\TEJAS>ssh -i "C:\Users\TEJAS\Downloads\prac9.pem" ec2-user@ec2-3-80-236-69.compute-1.amazonaws.com
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
Last login: Mon Oct 7 13:03:39 2024 from 120.88.190.21
```

- Note to change the path of the .pem file.

```
C:\Users\TEJAS>ssh -i "C:\Users\TEJAS\Downloads\prac9.pem" ubuntu@ec2-23-20-116-3.compute-1.amazonaws.com
The authenticity of host 'ec2-23-20-116-3.compute-1.amazonaws.com (23.20.116.3)' can't be established.
ED25519 key fingerprint is SHA256:xxysTigWzQlhqj1JboIduB2W/+mVHHycTGpqaSb5uo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-23-20-116-3.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

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

System information as of Mon Oct 7 13:19:03 UTC 2024

 System load: 0.59      Processes:          106
 Usage of /: 22.9% of 6.71GB  Users logged in:    0
 Memory usage: 22%          IPv4 address for enX0: 172.31.46.217
 Swap usage:  0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

The list of available updates is more than a week old.
```

- Go to nagios host machine (Host machine) & Perform the following commands

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

```
[ec2-user@ip-172-31-46-179 ~]$ ps -ef | grep nagios
nagios   3420      1  0 12:40 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios   3421     3420  0 12:40 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios   3422     3420  0 12:40 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios   3423     3420  0 12:40 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios   3424     3420  0 12:40 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios   3425     3420  0 12:40 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
ec2-user  10340   9541  0 13:20 pts/0    00:00:00 grep --color=auto nagios
```

```
sudo su
```

```
mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
```

```
[ec2-user@ip-172-31-46-179 ~]$ sudo su
[root@ip-172-31-46-179 ec2-user]# mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
[root@ip-172-31-46-179 ec2-user]# ls
downloads nagios-4.4.6 nagios-4.4.6.tar.gz nagios-plugins-2.3.3.tar.gz
```

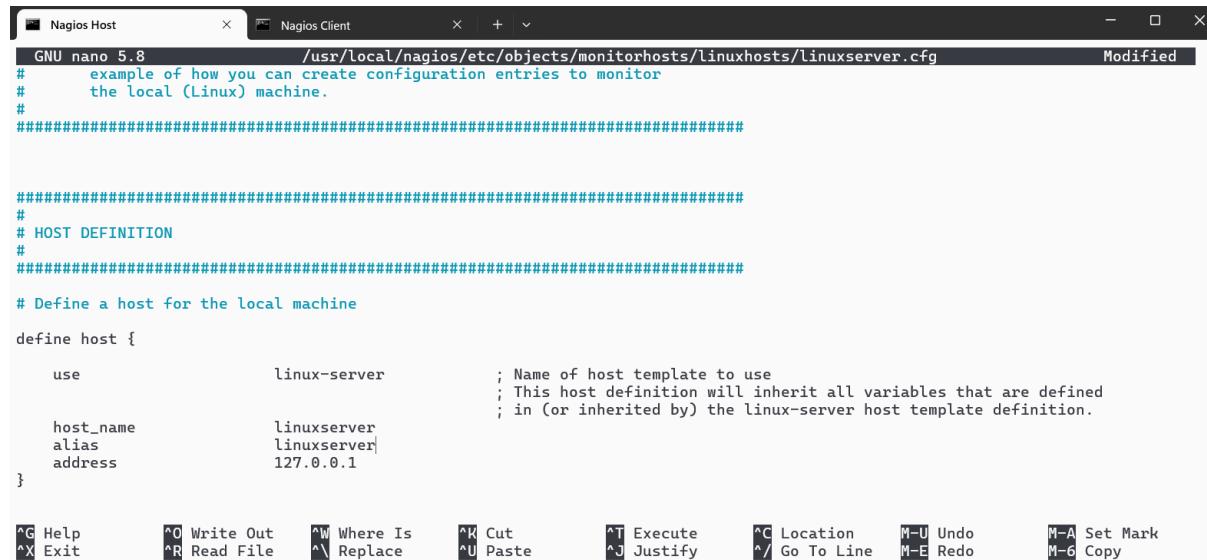
```
cp /usr/local/nagios/etc/objects/localhost.cfg
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
```

```
[root@ip-172-31-46-179 ec2-user]# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
```

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

```
[root@ip-172-31-46-179 ec2-user]# nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
[root@ip-172-31-46-179 ec2-user]# |
```

- Change hostname and alias to linuxserver Change address to public ip address of client instance (Ubuntu instance)



```

GNU nano 5.8          /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg      Modified
# example of how you can create configuration entries to monitor
# the local (Linux) machine.
#
#####
#
# HOST DEFINITION
#
#####
# Define a host for the local machine

define host {

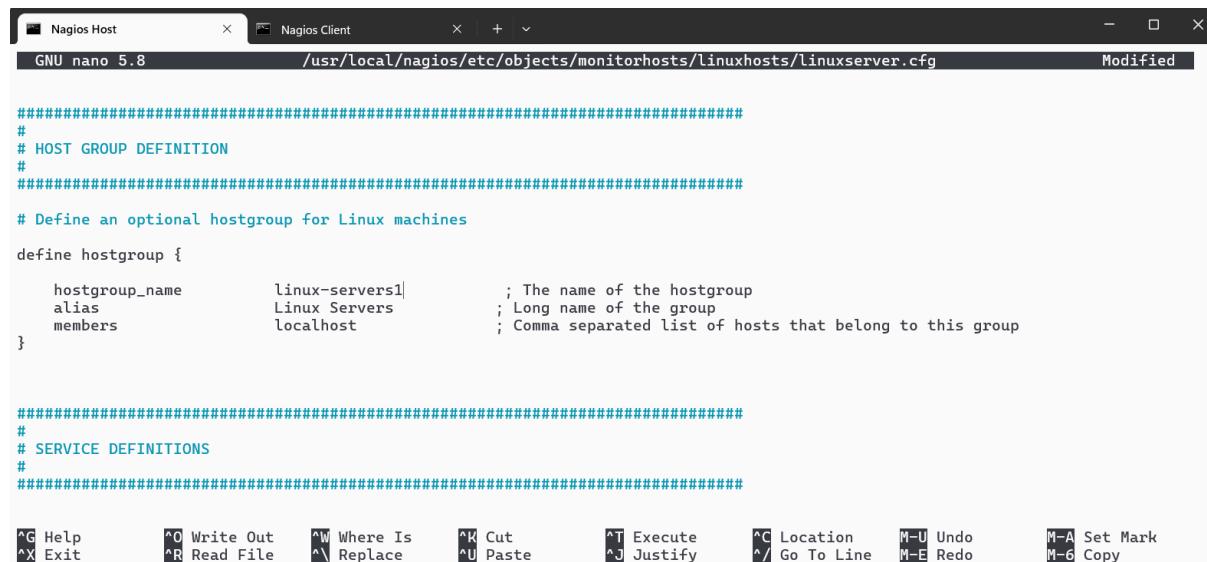
    use            linux-server           ; Name of host template to use
                           ; This host definition will inherit all variables that are defined
                           ; in (or inherited by) the linux-server host template definition.

    host_name      linuxserver
    alias          linuxserver
    address        127.0.0.1
}

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

```

- Change hostgroup_name to linux-servers1



```

GNU nano 5.8          /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg      Modified
#####
#
# 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
}

#####
#
# SERVICE DEFINITIONS
#
#####

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

```

- Change the occurrences of hostname further in the document from localhost to linuxserver

```

Nagios Host      Nagios Client
GNU nano 5.8      /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg Modified
alias           Linux Servers ; Long name of the group
members          localhost    ; Comma separated list of hosts that belong to this group
}

#####
#
# 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

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

#####
#
# 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 HTTP
    check_command  check_http
    notification_enabled 0
}

# Define a service to check the disk space of the root partition

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

```

- Open nagios configuration file and add the line shown below
`cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/`

```

Nagios Host      Nagios Client
GNU nano 5.8      /usr/local/nagios/etc/nagios.cfg Modified
# Definitions for monitoring the local (Linux) host
: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/

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

```

➤ Verify configuration files

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

```
[root@ip-172-31-46-179 ec2-user]# /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
```

```
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
Total Errors: 0

Things look okay - No serious problems were detected during the pre-flight check
[root@ip-172-31-46-179 ec2-user]#
```

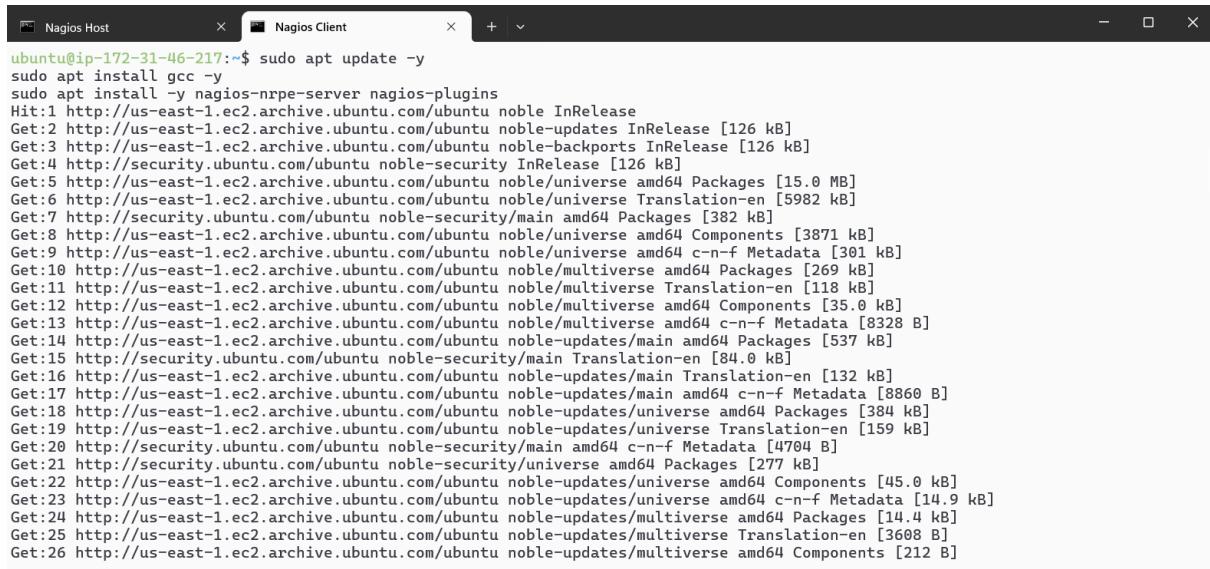
➤ Restart nagios service.

```
service nagios restart
```

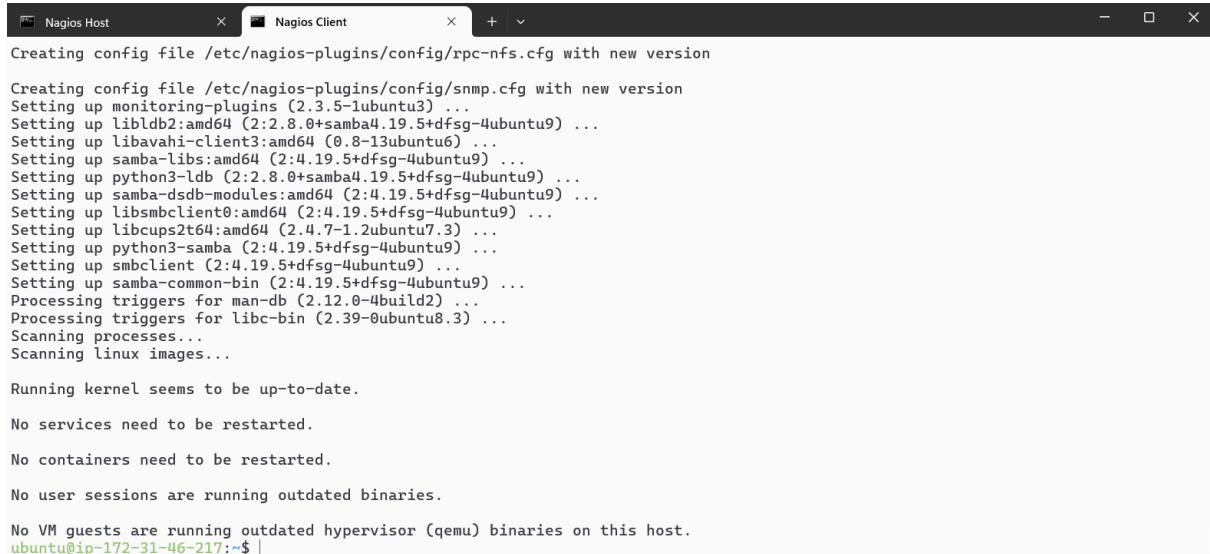
```
[root@ip-172-31-46-179 ec2-user]# service nagios restart
Redirecting to /bin/systemctl restart nagios.service
[root@ip-172-31-46-179 ec2-user]# |
```

- Go to client machine (ubuntu machine) & Perform the following commands

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



```
ubuntu@ip-172-31-46-217:~$ sudo apt update -y
[sudo] password for ubuntu:
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [382 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Translation-en [118 kB]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [537 kB]
Get:15 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [84.0 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [132 kB]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [8860 B]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [384 kB]
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [159 kB]
Get:20 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4704 B]
Get:21 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [277 kB]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [45.0 kB]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [14.9 kB]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [14.4 kB]
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [3608 B]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [212 B]
```



```
Creating config file /etc/nagios-plugins/config/rpc-nfs.cfg with new version
Creating config file /etc/nagios-plugins/config/snmp.cfg with new version
Setting up monitoring-plugins (2.3.5-1ubuntu3) ...
Setting up liblbd2:amd64 (2:2.8.0+samba4.19.5+dfsg-4ubuntu9) ...
Setting up libavahi-client3:amd64 (0.8-13ubuntu6) ...
Setting up samba-libs:amd64 (2:4.19.5+dfsg-4ubuntu9) ...
Setting up python3-ldbc (2:2.8.0+samba4.19.5+dfsg-4ubuntu9) ...
Setting up samba-dsdb-modules:amd64 (2:4.19.5+dfsg-4ubuntu9) ...
Setting up lib smbclient0:amd64 (2:4.19.5+dfsg-4ubuntu9) ...
Setting up libcups2t64:amd64 (2:4.7-1.2ubuntu7.3) ...
Setting up python3-samba (2:4.19.5+dfsg-4ubuntu9) ...
Setting up smbclient (2:4.19.5+dfsg-4ubuntu9) ...
Setting up samba-common-bin (2:4.19.5+dfsg-4ubuntu9) ...
Processing triggers for man-db (2.12.0-4build2) ...
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.

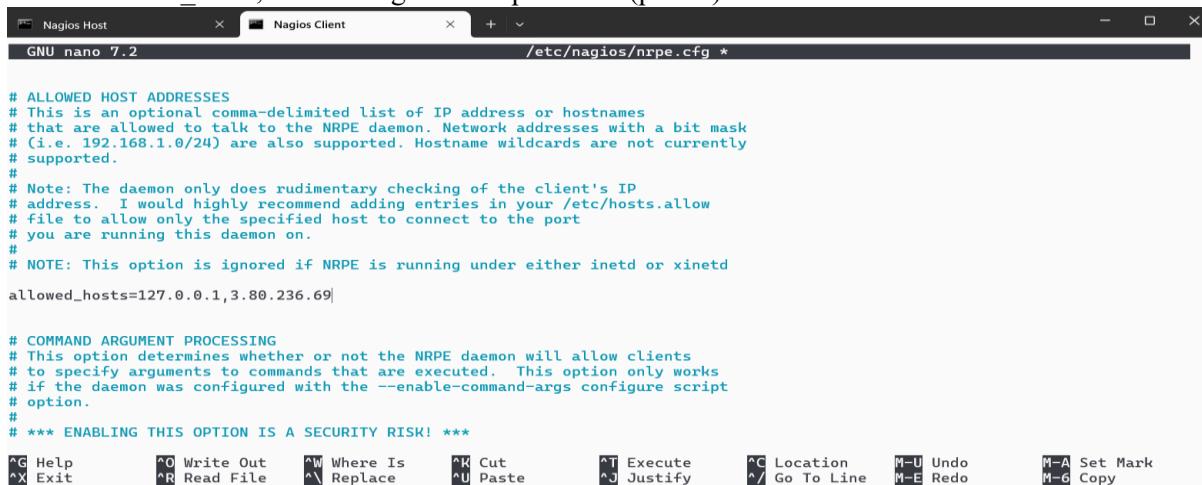
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-46-217:~$ |
```

- Open the nrpe.cfg file in nano editor

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

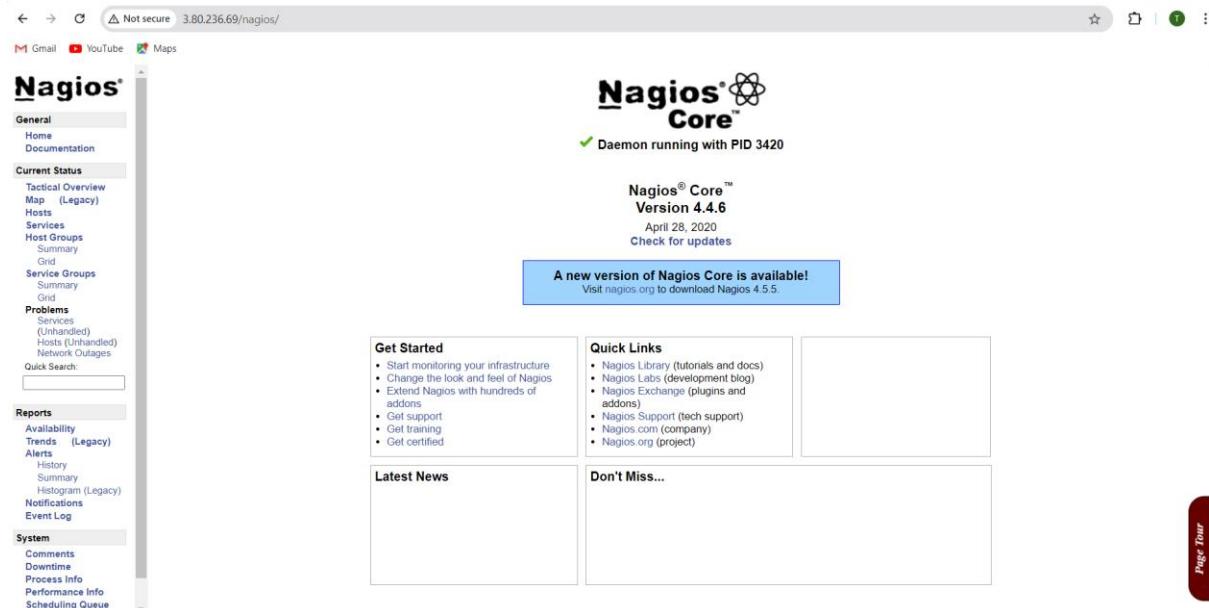
Under allowed_hosts, add the nagios host ip address (public)



```
# 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=127.0.0.1,3.80.236.69

# COMMAND ARGUMENT PROCESSING
# This option determines whether or not the NRPE daemon will allow clients
# to specify arguments to commands that are executed. This option only works
# if the daemon was configured with the --enable-command-args configure script
# option.
#
# *** ENABLING THIS OPTION IS A SECURITY RISK! ***
```

- Go to nagios dashboard



- Click on hosts



➤ Click on linux server

➤ Click on nagios services

Nagios®

Current Network Status

Last Updated: Sat Sep 29 11:33:58 UTC 2024
Updated every 50 seconds
Nagios® Core™ 4.5.5 - www.nagios.org
Logged in as nagiosadmin

Host Status Totals

Up	Down	Unreachable	Pending
2	0	0	0

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
12	1	0	3	0

Service Status Details For All Hosts

Limit Results: 100 ▾

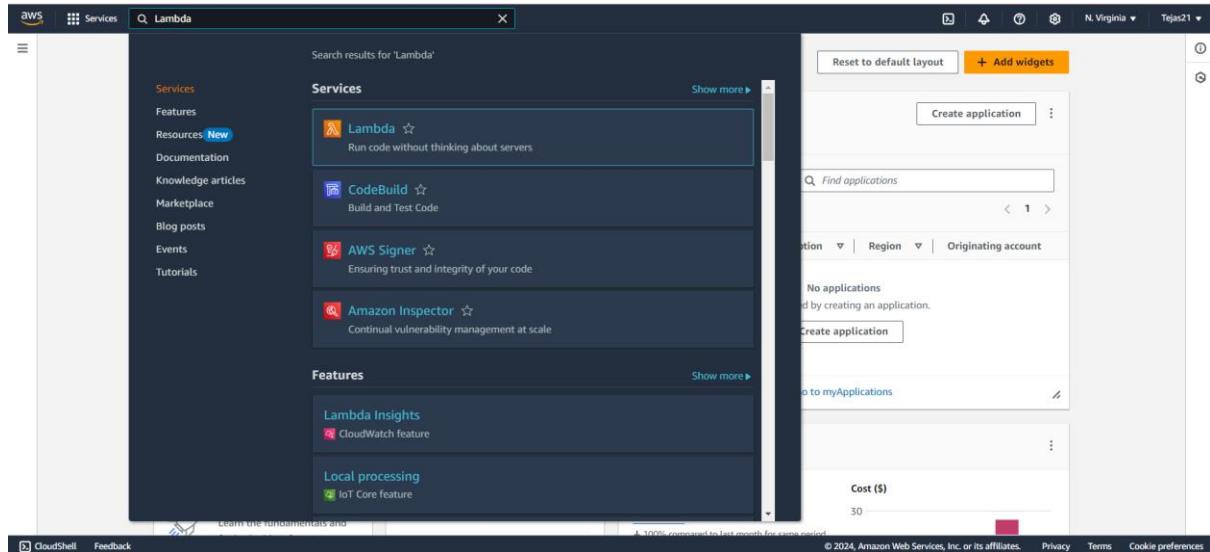
Host **	Service **	Status **	Last Check **	Duration **	Attempt **	Status Information
linusserver	Current Load	OK	09-28-2024 11:30:25	0d 0h 8m 33s	1/4	OK - load average: 0.91, 0.08, 0.00
	Current Users	OK	09-28-2024 11:31:03	0d 0h 7m 55s	1/4	USERS OK - 2 users currently logged in
	HTTP	CRITICAL	09-28-2024 11:29:40	0d 0h 4m 18s	4/4	connect to address 54.173.58.143 and port 80: Connection refused
	PING	OK	09-28-2024 11:32:18	0d 0h 6m 40s	1/4	PING OK - Packet loss = 0%, RTA = 1.03 ms
	Root Partition	OK	09-28-2024 11:32:55	0d 0h 6m 3s	1/4	DISK OK - free space: / 6105 MB (75.23% mode=98%)
	SSH	OK	09-28-2024 11:33:33	0d 0h 5m 25s	1/4	SSH OK - OpenSSH_8.6-p1 Ubuntu-Subuntu13.4 (protocol 2.0)
	Swap Usage	CRITICAL	09-28-2024 11:32:10	0d 0h 1m 48s	4/4	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.
	Total Processes	OK	09-28-2024 11:29:48	0d 0h 9m 10s+	1/4	PROCS OK, 37 processes with STATE = RSZDT
localhost	Current Load	OK	09-28-2024 11:29:39	0d 3h 53m 5s	1/4	OK - load average: 0.02, 0.01, 0.00
	Current Users	OK	09-28-2024 11:30:17	0d 3h 52m 27s	1/4	USERS OK - 2 users currently logged in
	HTTP	WARNING	09-28-2024 11:29:46	0d 2h 49m 12s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 319 bytes in 0.001 second response time
	PING	OK	09-28-2024 11:31:32	0d 3h 51m 12s	1/4	PING OK - Packet loss = 0%, RTA = 0.03 ms
	Root Partition	OK	09-28-2024 11:32:09	0d 3h 50m 35s	1/4	DISK OK - free space: / 6105 MB (75.23% mode=98%)
	SSH	OK	09-28-2024 11:32:47	0d 3h 49m 57s	1/4	SSH OK - OpenSSH_8.7 (protocol 2.0)
	Swap Usage	CRITICAL	09-28-2024 11:31:24	0d 3h 12m 34s	4/4	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.
	Total Processes	OK	09-28-2024 11:29:02	0d 3h 14m 56s	1/4	PROCS OK, 37 processes with STATE = RSZDT

Results 1 - 16 of 16 Matching Services

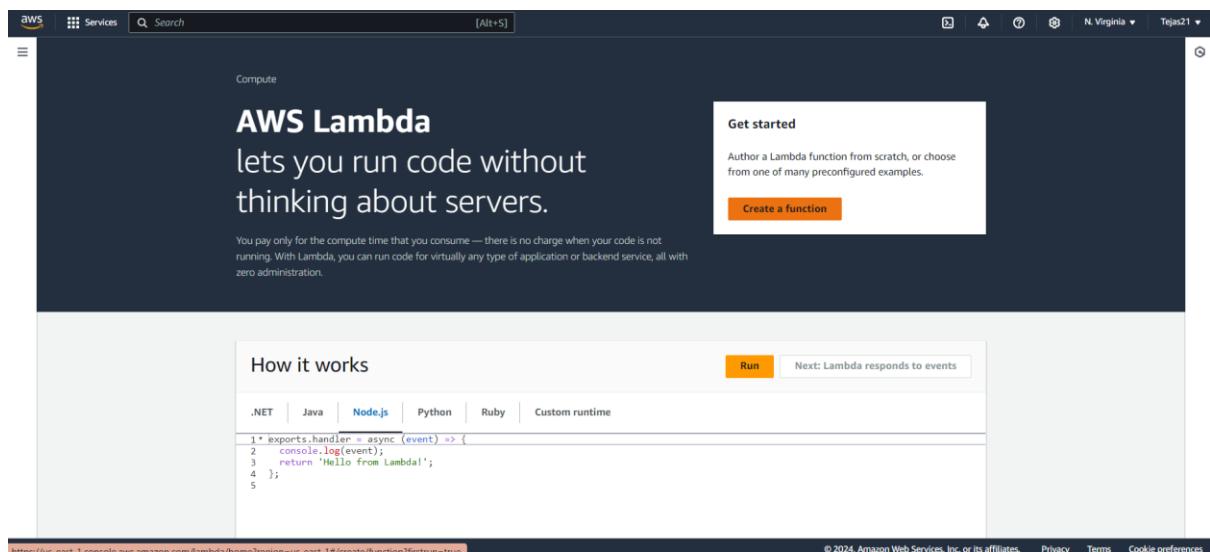
EXPERIMENT NO: - 11

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

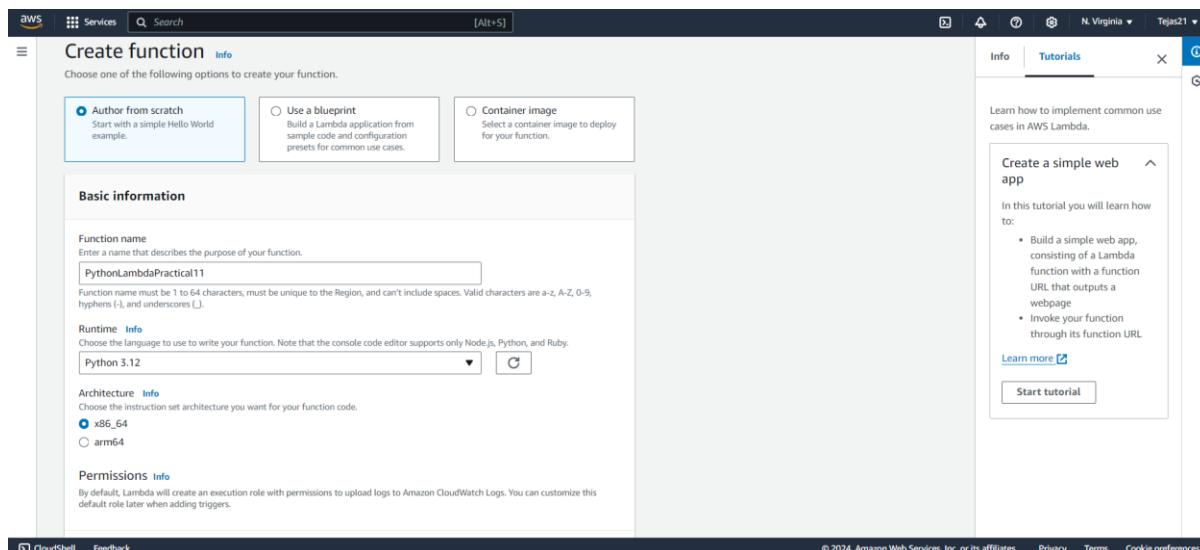
- Open Lambda to create an AWS Lambda function



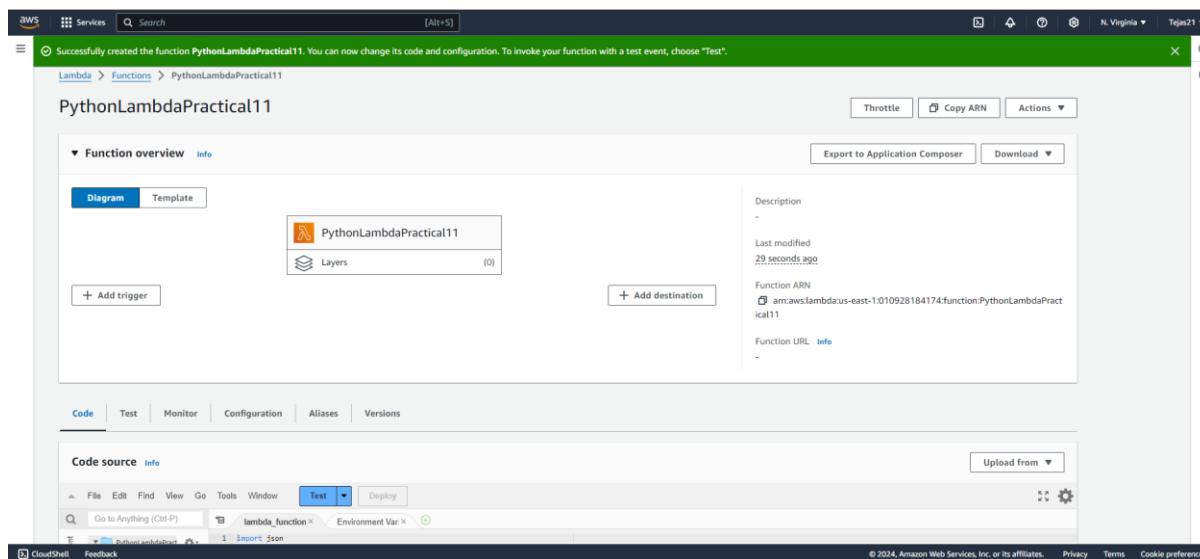
- Open up the Lambda Console and click on the Create button.

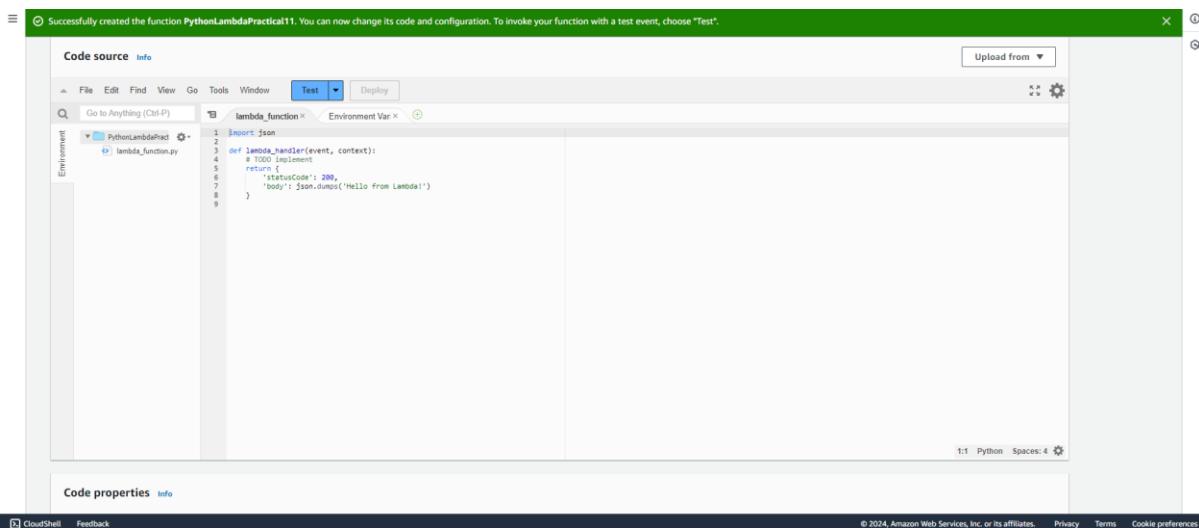


- Choose to create a function from scratch or use a blueprint, i.e templates defined by AWS for you with all configuration presets required for the most common use cases. Then, choose a runtime env for your function, under the dropdown, you can see all the options AWS supports, Python, Nodejs, .NET and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

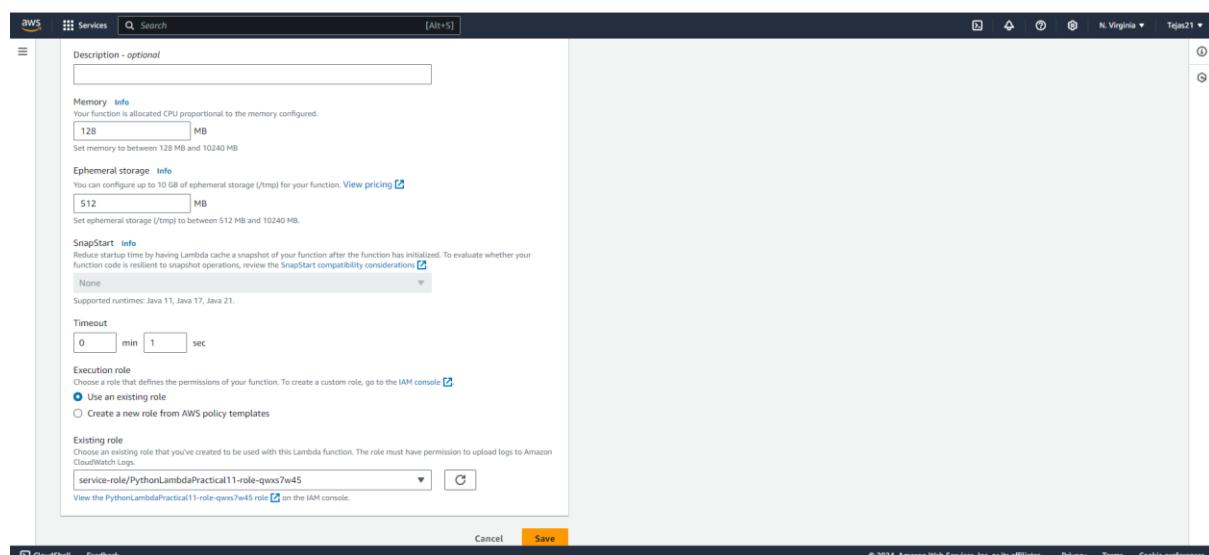
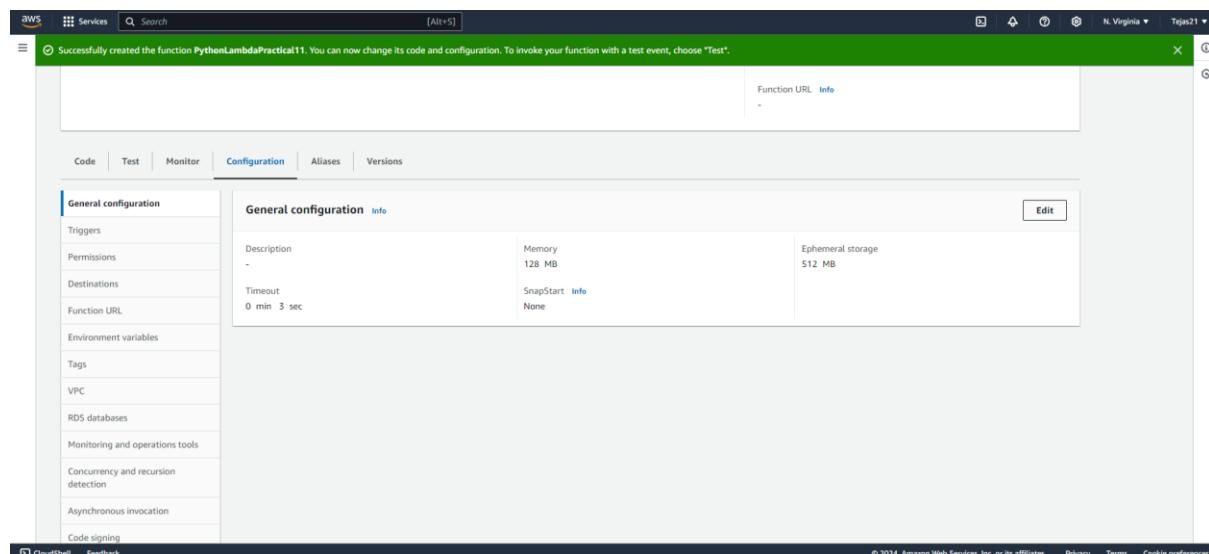


- Function is successfully created

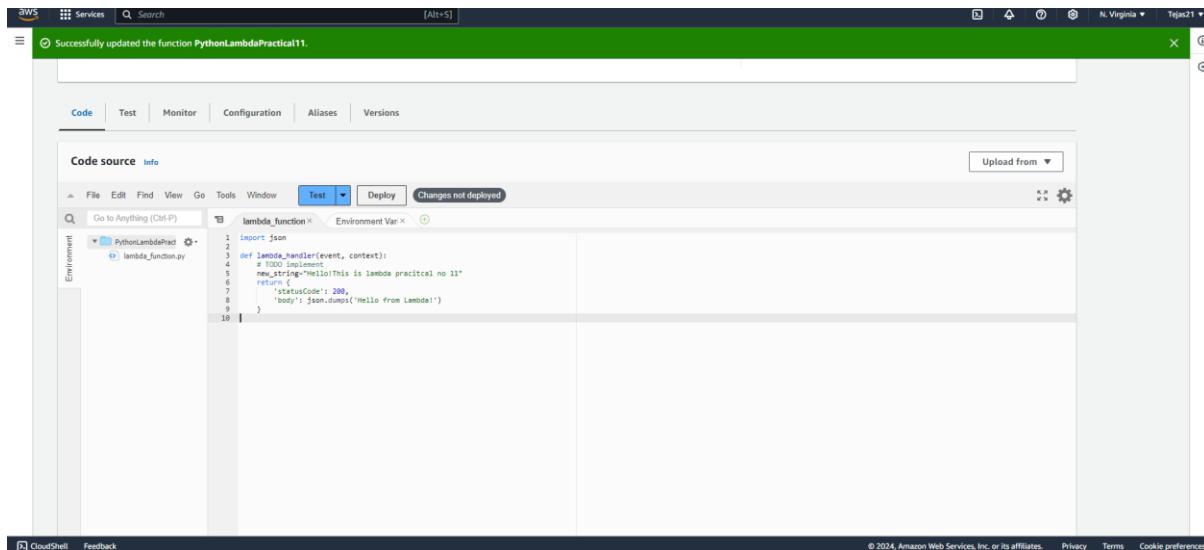




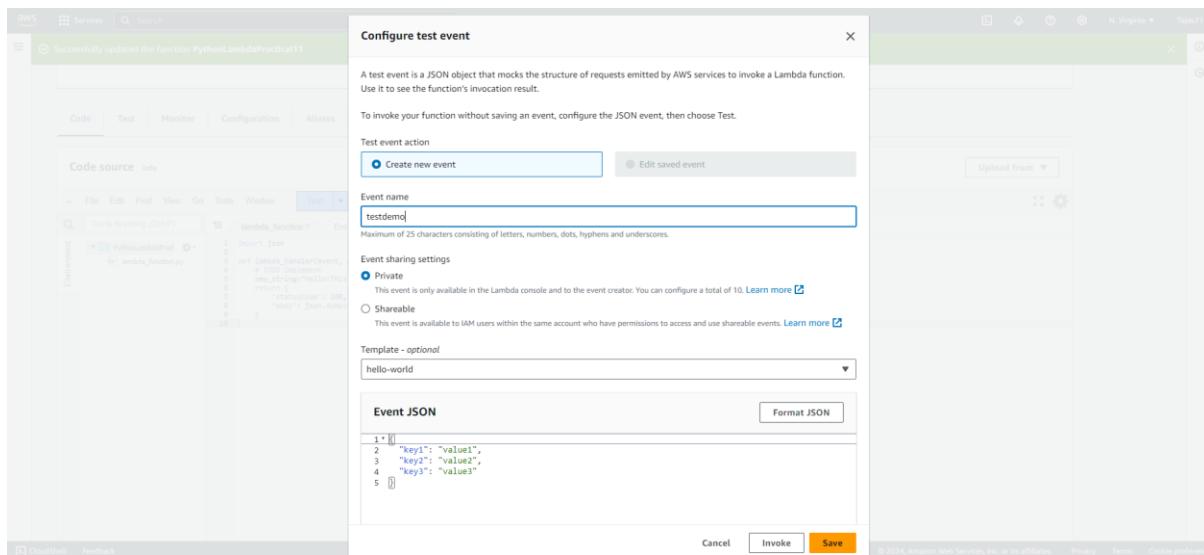
- To change the configuration, open up the Configuration tab and under General Configuration, choose Edit. Here, you can enter a description and change Memory and Timeout. I've changed the Timeout period to 1 sec since that is sufficient for now.



- 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 and you should be able to see the results

The screenshot shows the AWS Lambda console interface. At the top, there are tabs for Code, Test, Monitor, Configuration, Aliases, and Versions. The Code tab is selected. Below the tabs, there are buttons for File, Edit, Find, View, Go, Tools, Window, Test (which is currently selected), Deploy, and a status message indicating "Changes not deployed". To the right of the status message is an "Upload from" button.

The main area displays the "Execution result" for a test event named "testEvent". The response object is shown as:

```
Response
{
  "statusCode": 200,
  "body": "Hello from Lambda!"
}
```

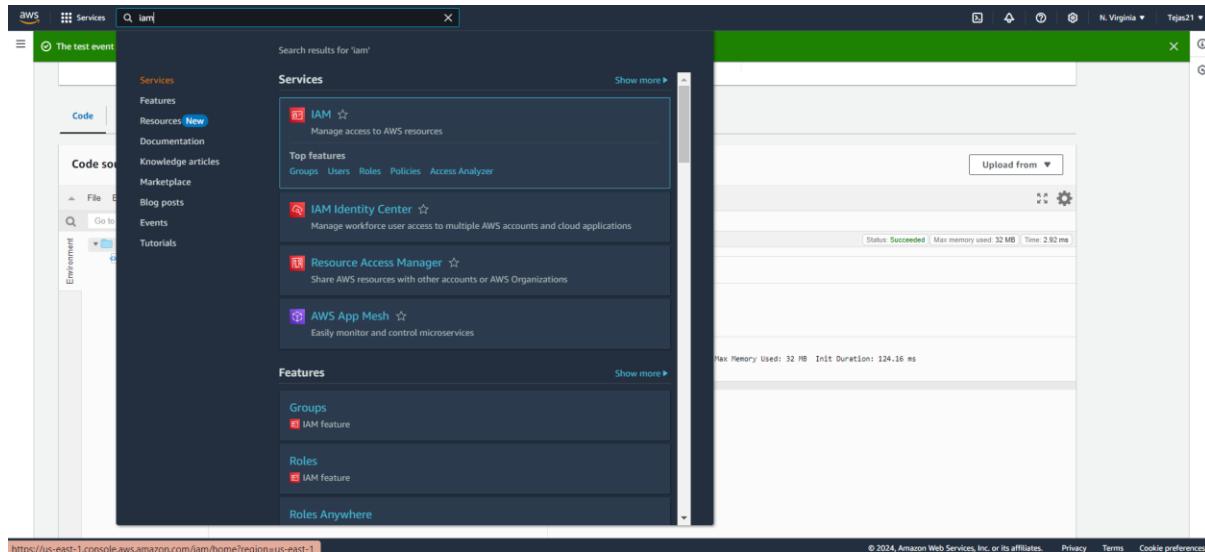
Below the response, the "Function Logs" section shows the following log entries:

```
START RequestId: c1138474-7d39-49ed-9b07-99d320d74b28 Version: $LATEST
END RequestId: c1138474-7d39-49ed-9b07-99d320d74b28
REPORT RequestId: c1138474-7d39-49ed-9b07-99d320d74b28 Duration: 2.92 ms Billed Duration: 3 ms Memory Size: 128 MB Max Memory Used: 32 MB Init Duration: 124.16 ms
Request ID
c1138474-7d39-49ed-9b07-99d320d74b28
```

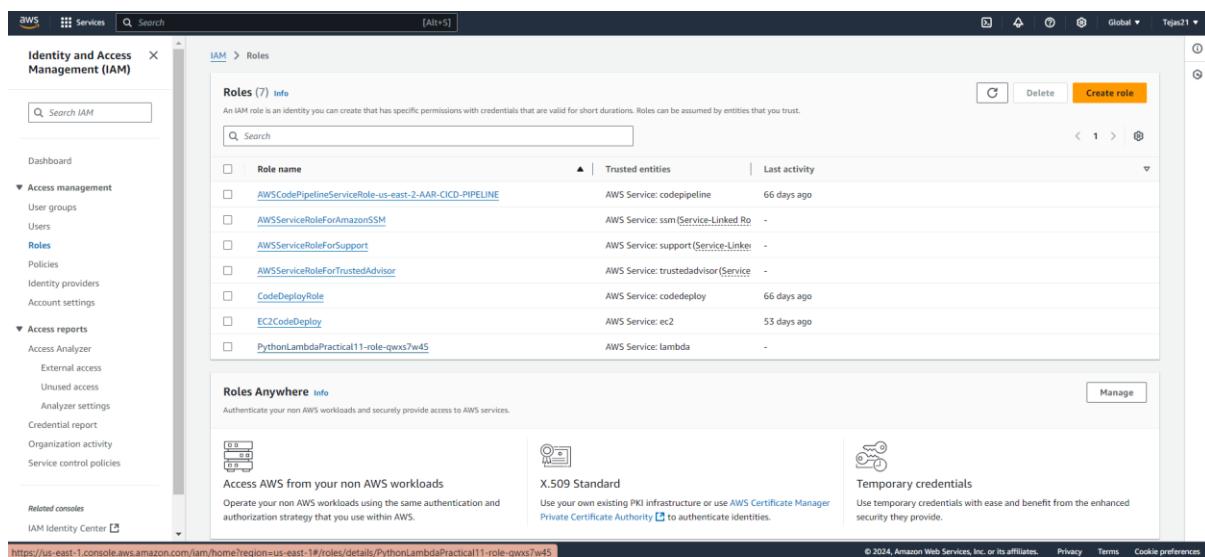
EXPERIMENT NO: - 12

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

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

The screenshot shows the AWS IAM Roles page. On the left, the navigation menu includes 'Identity and Access Management (IAM)', 'Access management' (with 'Roles' selected), 'Policies', 'Identity providers', and 'Account settings'. Under 'Access reports', it lists 'Access Analyzer', 'External access', 'Unused access', 'Analyzer settings', 'Credential report', 'Organization activity', and 'Service control policies'. 'Related consoles' include 'IAM Identity Center' and 'CloudShell'. The main content area displays the 'PythonLambdaPractical11-role-qwxs7w45' role. The 'Summary' tab shows creation date (October 17, 2024, 19:10 UTC+05:30), last activity (none), ARN (arn:aws:iam::010928184174:role/service-role/PythonLambdaPractical11-role-qwxs7w45), and maximum session duration (1 hour). The 'Permissions' tab is selected, showing 'Permissions policies (1) Info'. It lists one policy: 'AWSLambdaBasicExecutionRole-f05e2480-c296-4722-996b-...', which is 'Customer managed'. Below this is a 'Permissions boundary (not set)' section. At the bottom right, there are buttons for 'Simulate', 'Remove', and 'Add permissions'.

- S3-ReadOnly

The screenshot shows the 'Add permissions' dialog for the 'PythonLambdaPractical11-role-qwxs7w45' role. The 'Current permissions policies (1)' section shows one policy: 'AmazonS3ReadonlyAccess'. The 'Other permissions policies (1/956)' section has a search bar 'Q S3RE' and a filter 'Filter by Type All types'. It lists two policies: 'AmazonS3ReadonlyAccess' (selected) and 'AWSBackupServiceRolePolicyForS3Restore'. At the bottom right are 'Cancel' and 'Add permissions' buttons.

- CloudWatchFull

The screenshot shows the 'Add permissions' dialog for the 'PythonLambdaPractical11-role-qwxs7w45' role. The 'Current permissions policies (2)' section shows two policies: 'AmazonS3ReadonlyAccess' and 'CloudWatchFullAccess'. The 'Other permissions policies (1/955)' section has a search bar 'Q CLOUDWATCHFU' and a filter 'Filter by Type All types'. It lists two policies: 'CloudWatchFullAccess' (selected) and 'CloudWatchFullAccessV2'. At the bottom right are 'Cancel' and 'Add permissions' buttons.

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

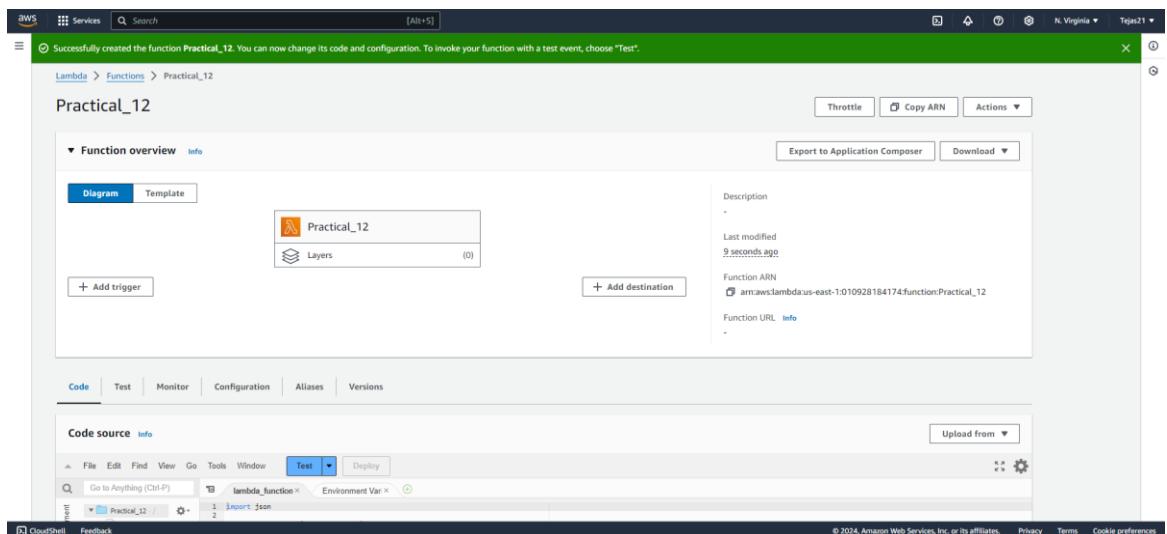
The screenshot shows the AWS IAM Permissions page. A green banner at the top says "Policy was successfully attached to role." Below it, the ARN of the policy is listed: arn:aws:iam::010928184174:role/service-role/PythonLambdaPractical11-role-qwxs7w45. The maximum session duration is set to 1 hour. The "Permissions policies" section shows three policies attached to the role: AmazonS3ReadOnlyAccess, AWSLambdaBasicExecutionRole, and CloudWatchFullAccess. The "Permissions boundary" and "Generate policy based on CloudTrail events" sections are also visible.

- 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.

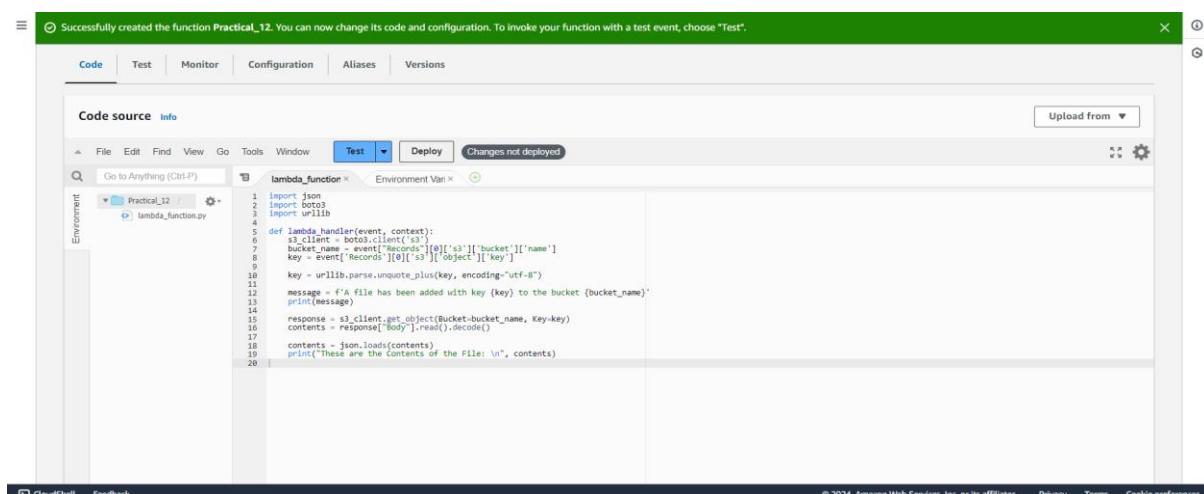
The screenshot shows the AWS Lambda "Create function" page. It has three options for creating a function: "Author from scratch" (selected), "Use a blueprint", and "Container image". The "Basic information" section includes fields for "Function name" (Practical_12), "Runtime" (Python 3.12), "Architecture" (x86_64), and "Permissions" (Info). The "Permissions" section notes that Lambda will create an execution role with CloudWatch Logs permissions. The "Change default execution role" button is visible.

The screenshot shows the AWS Lambda "Create function" page with more detailed configuration. It includes sections for "Runtime" (Python 3.12), "Architecture" (x86_64), "Permissions" (Info), "Execution role" (using the service-role/PythonLambdaPractical11-role-qwxs7w45 role), and "Additional Configurations". The "Create function" button is highlighted.

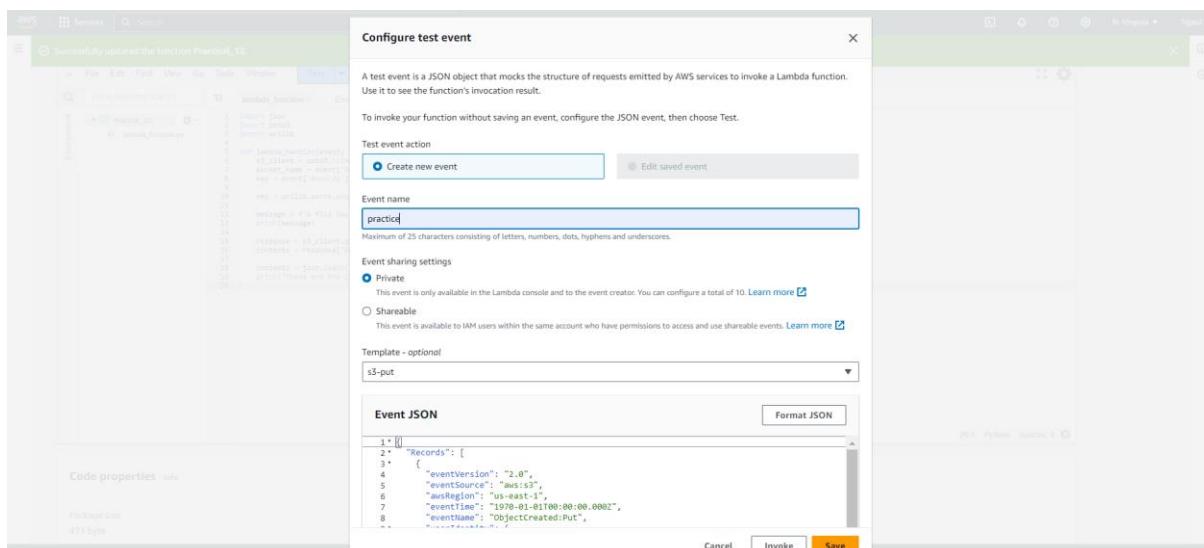
- The function is now successfully created and running



- 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.



- Open up the S3 Console and create a new bucket.

The screenshot shows the AWS S3 Buckets page. At the top, there's a search bar and a 'Create bucket' button. Below the search bar, there are tabs for 'General purpose buckets' and 'Directory buckets'. Under the 'General purpose buckets' tab, it says 'General purpose buckets (1) info All AWS Regions'. A note states 'Buckets are containers for data stored in S3.' There's a search bar labeled 'Find buckets by name'. Below the search bar, there's a table with columns: Name, AWS Region, IAM Access Analyzer, and Creation date. The single bucket listed is 'codepipeline-us-east-2-518101101971' from the 'us-east-2' region, created on August 11, 2024, at 00:30:08 (UTC+05:30). Action buttons for each row include 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'.

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

The screenshot shows the 'Create bucket' wizard. It starts with a 'Create bucket' step. The next step is 'General configuration'. In this step, the 'AWS Region' is set to 'US East (N. Virginia) us-east-1'. The 'Bucket type' is set to 'General purpose', which is described as recommended for most user cases and access patterns. The bucket name is 'advedevopsxp12'. The 'Object Ownership' section shows 'ACLs disabled (recommended)' selected. Other options like 'CloudWatch Metrics' and 'CloudWatch Metrics Insights' are also available. At the bottom, there are buttons for 'Choose bucket' and 'Create bucket'.

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

The screenshot shows the 'Event notifications' section of the S3 bucket properties. It displays a message 'No data events to display.' and a 'Configure in CloudTrail' button. Below this, there's a table for 'Event notifications (0)'. The table has columns: Name, Event types, Filters, Destination type, and Destination. A note says 'No event notification' and 'Choose Create event notification to be notified when a specific event occurs.' A 'Create event notification' button is present. Other sections visible include 'Amazon EventBridge' (with a note about using it for event-driven applications), 'Transfer acceleration' (with a note about using an accelerated endpoint for faster data transfers), and 'Object Lock' (with a note about preventing objects from being deleted or overwritten). At the bottom, there are buttons for 'Edit' and 'Create event notification'.

- Mention an event name and check Put under event types.

The screenshot shows the 'Create event notification' configuration page. In the 'Event name' field, 'S3putrequest' is entered. Under 'Prefix - optional', 'images/' is listed. Under 'Suffix - optional', '.jpg' is listed. In the 'Event types' section, the 'Put' checkbox is checked, while 'All object create events' and 'Post' are unchecked. The status bar at the bottom right indicates '© 2024, Amazon Web Services, Inc. or its affiliates.' and includes links for Privacy, Terms, and Cookie preferences.

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

The screenshot shows the 'Intelligent-Tiering' configuration page. Under 'Destination', the 'Lambda function' radio button is selected. A dropdown menu shows 'Practical_12' as the chosen function. The status bar at the bottom right indicates '© 2024, Amazon Web Services, Inc. or its affiliates.' and includes links for Privacy, Terms, and Cookie preferences.

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

The screenshot shows the 'Practical_12' Lambda function overview. In the 'Function overview' section, an 'S3' trigger is visible. The 'Code source' tab is active, showing the function code in a code editor:

```

    1 import base64
    2 import boto3
    3 import urllib
    4
    5 def lambda_handler(event, context):

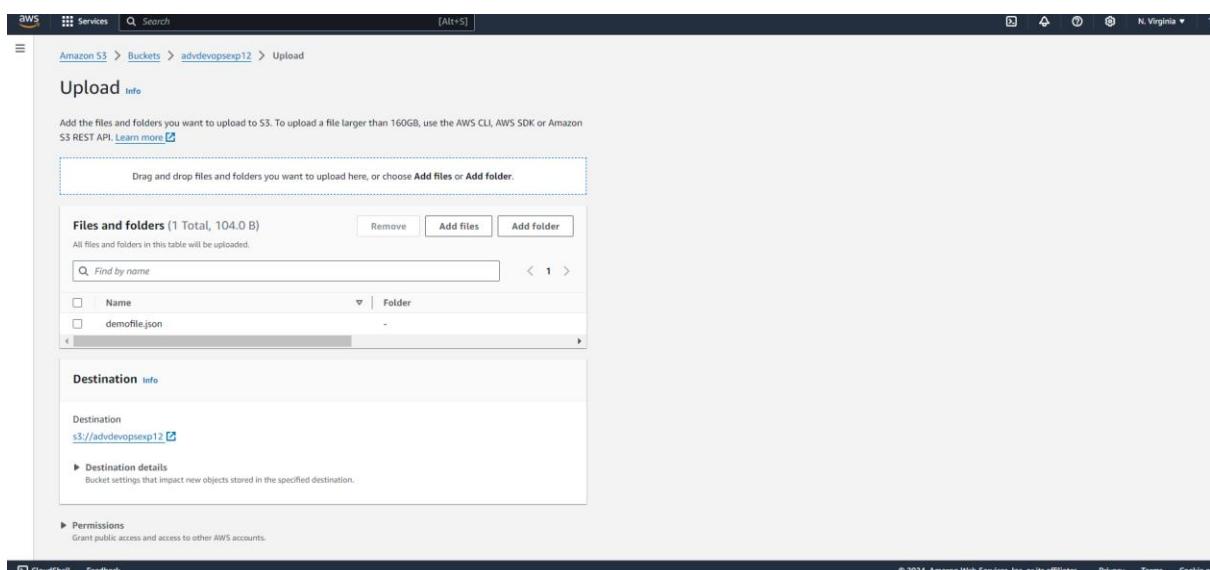
```

The status bar at the bottom right indicates '© 2024, Amazon Web Services, Inc. or its affiliates.' and includes links for Privacy, Terms, and Cookie preferences.

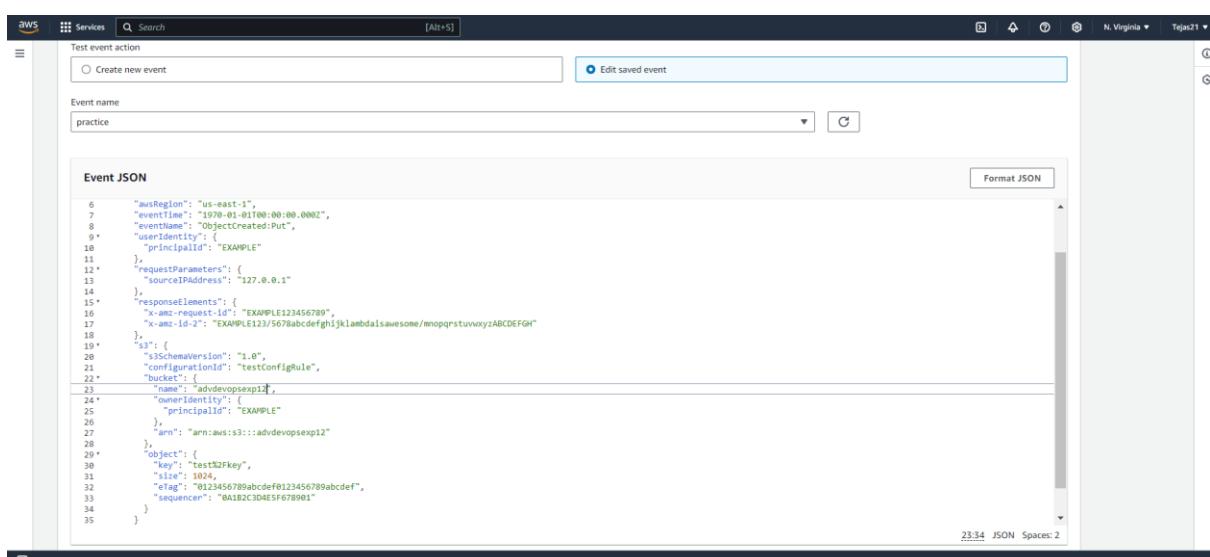
- Now, create a demofile JSON file locally.

```
{
  "firstname": "TEJAS",
  "lastname": "GUNJAL",
  "gender": "Male",
  "age": "20"
}
```

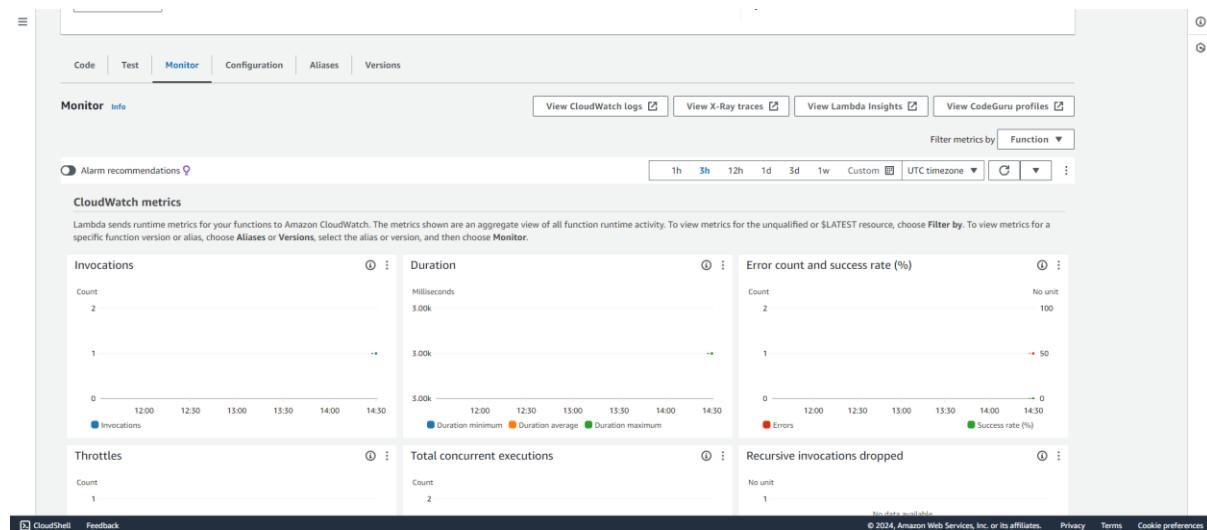
- Go back to your S3 Bucket and click on Add Files to upload a new file. Select the demofile data file from your computer and click Upload.



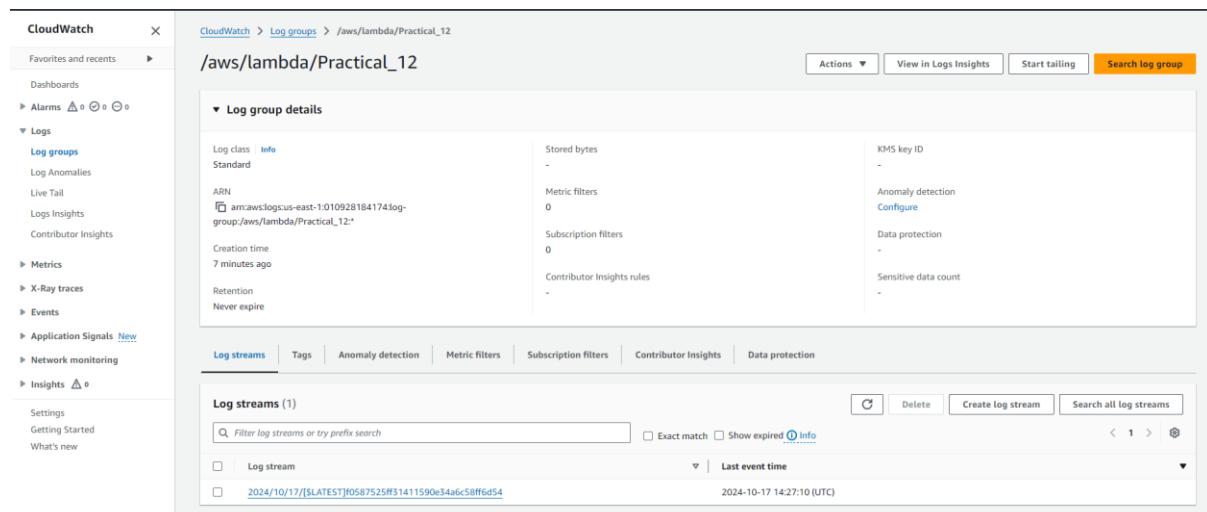
- After this make the necessary changes in the Test configuration file which we created it previously by replacing the Bucket Name and the ARN of Bucket.



- 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.

