

## Experiment 01

a) To develop a website and host it on your local machine on a VM

The screenshot shows the AWS EC2 Dashboard in the US East (N. Virginia) Region. The left sidebar includes sections for EC2 Global View, Events, Console-to-Code, Instances, Images, and Elastic Block Store. The main area displays EC2 resources: 1 Instance (running), 1 Auto Scaling Group, 0 Capacity Reservations, 0 Dedicated Hosts, 1 Elastic IP, 1 Instance, 0 Key pairs, 0 Load balancers, 0 Placement groups, 2 Security groups, 0 Snapshots, and 1 Volumes.

In the center, there's a "Launch instance" section with a "Launch instance" button and a "Migrate a server" button. Below it, a note says "Note: Your instances will launch in the US East (N. Virginia) Region".

The "Service health" section shows "AWS Health Dashboard" and indicates "This service is operating normally".

The right sidebar contains sections for "EC2 Free Tier", "Account attributes", "Default VPC" (vpc-0fc2f3f7a22f1a71), "Settings" (Data protection and security, Zones, EC2 Serial Console, Default credit specification, EC2 console preferences), and "Additional information".

The bottom half of the screen shows a detailed view of launching an instance. It starts with a "Quick Start" tab and a "Recent" tab. Under "Amazon Machine Image (AMI)", it lists "Ubuntu Server 24.04 LTS (HVM), SSD Volume Type" (ami-04a81a99f5ec58529). The "Free tier eligible" status is shown. The "Description" section details "Ubuntu Server 24.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>)". The "Architecture" is set to "64-bit (x86)" and the "AMI ID" is "ami-04a81a99f5ec58529". A "Verified provider" badge is present.

The "Summary" section provides an overview of the launch configuration, including "Number of instances" (1), "Software Image (AMI)" (Canonical, Ubuntu, 24.04 LTS), "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 the "Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which you launch instances)." Buttons for "Cancel" and "Launch instance" are at the bottom.

**Configure storage**

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 24.04 LTS, ami-04a81a99f5ec58529

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

**Advanced details**

**Success**  
Successfully initiated launch of instance (i-0f3bd5bcbcc35b81a)

**Next Steps**

- Create billing and free tier usage alerts
- Connect to your instance
- Connect an RDS database
- Create EBS snapshot policy

**Instances (1/2)**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
Mynapp-env	i-0365889e6b3d22cdb	Running	t3.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-44-
<b>prathmesh_instance</b>	<b>i-0f3bd5bcbcc35b81a</b>	Running	t2.micro	Initializing	View alarms +	us-east-1b	ec2-54-

**i-0f3bd5bcbcc35b81a (vedant\_Instance)**

**Details**

Instance ID: i-0f3bd5bcbcc35b81a (vedant\_Instance)

Public IPv4 address: 54.159.13.162 | [open address](#)

Private IPv4 addresses: 172.31.33.103

IPv6 address: -

Instance state: Running

Private IP DNS name (IPv4 only): ec2-54-159-13-162.compute-1.amazonaws.com | [open address](#)

Hostname type:

AWS Services Search [Alt+S] ☰ ⓘ ⓘ ⓘ ⓘ

EC2 > Instances > i-0365889e6b3d22cdb > Connect to instance

## Connect to instance Info

Connect to your instance i-0365889e6b3d22cdb (Mynewapp-env) using any of these options

EC2 Instance Connect Session Manager SSH client EC2 serial console

**⚠ Port 22 (SSH) is not authorized**  
Port 22 (SSH) is currently not authorized by your security group. To use EC2 Instance Connect, you must authorize port 22 for the EC2 Instance Connect service IP addresses in your Region: 18.206.107.24/29.  
[Learn more.](#)

Instance ID [i-0365889e6b3d22cdb \(Mynewapp-env\)](#)

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 [44.205.155.152](#)

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, root.

```
supra>ssh -i "supra-key.pem" ubuntu@3.110.164.61
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1009-ams x86_64)

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

System information as of Mon Aug  5 14:53:57 UTC 2024

System load:  0.01      Processes:          105
Usage of /:   22.7% of 6.71GB  Users logged in:     0
Memory usage: 20%           IPv4 address for enX0: 172.31.6.34
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

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

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

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

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

```
ubuntu@ip-172-31-6-34:~$ sudo apt update && sudo apt upgrade -y
Get:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:5 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:6 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:8 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [381 kB]
Get:9 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:10 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:11 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.8 kB]
Get:12 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:13 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [317 kB]
Get:14 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [82.7 kB]
Get:15 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [5640 B]
Get:16 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [318 kB]
Get:17 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [133 kB]
Get:18 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [45.8 kB]
Get:19 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [12.5 kB]
Get:20 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [288 kB]
Get:21 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [48.7 kB]
Get:22 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 c-n-f Metadata [416 B]
Get:23 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [14.1 kB]
Get:24 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [3608 B]
Get:25 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [212 B]
Get:26 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [532 B]
Get:27 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Get:28 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 c-n-f Metadata [112 B]
Get:29 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Packages [10.3 kB]
Get:30 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe Translation-en [10.5 kB]
Get:31 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [17.6 kB]
Get:32 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 c-n-f Metadata [1816 B]
Get:33 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:34 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 c-n-f Metadata [116 B]
```

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-6-34:~$ sudo apt install apache2 -y
Reading package lists... Done
Building dependency tree... Done
Enabling module auth_basic.
Enabling module access_compat.
Enabling module authn_file.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 800-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /usr/lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /usr/lib/systemd/system/apache-htcacheclean
.service.
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.2) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Pending kernel upgrade!
```

```

*** System restart required ***
Last login: Mon Aug  5 14:53:58 2024 from 152.58.43.204
ubuntu@ip-172-31-6-34:~$ sudo mv /home/ubuntu/index.html /var/www/html/
ubuntu@ip-172-31-6-34:~$ sudo chown -R www-data:www-data /var/www/html
ubuntu@ip-172-31-6-34:~$ sudo nano /etc/apache2/sites-available/000-default.conf
ubuntu@ip-172-31-6-34:~$ sudo a2ensite 000-default.conf
Site 000-default already enabled
ubuntu@ip-172-31-6-34:~$ sudo systemctl restart apache2
ubuntu@ip-172-31-6-34:~$ sudo apt install certbot python3-certbot-apache
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  augeas-lenses libaugeas0 python3-acme python3-augeas
  python3-certbot python3-configargparse python3-icu
  python3-josepy python3-parsedatetime python3-rfc3339
Suggested packages:
  augeas-doc python-certbot-doc python3-certbot-nginx
  augeas-tools python-acme-doc python-certbot-apache-doc
The following NEW packages will be installed:
  augeas-lenses certbot libaugeas0 python3-acme python3-augeas
  python3-certbot python3-certbot-apache
...
Unpacking python3-parsedatetime (2.6-3) ...
Selecting previously unselected package python3-certbot.
Preparing to unpack .../00-python3-certbot_2.9.0-1_all.deb ...
Unpacking python3-certbot (2.9.0-1) ...
Selecting previously unselected package certbot.
Preparing to unpack .../09-certbot_2.9.0-1_all.deb ...
Unpacking certbot (2.9.0-1) ...
Selecting previously unselected package python3-certbot-apache.
Preparing to unpack .../10-python3-certbot-apache_2.9.0-1_all.deb ...
Unpacking python3-certbot-apache (2.9.0-1) ...
Selecting previously unselected package python3-icu.
Preparing to unpack .../11-python3-icu_2.12-1build2_amd64.deb ...
Unpacking python3-icu (2.12-1build2) ...

```

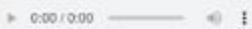


## DevSync

- [Home](#)
- [About Us](#)
- [Services](#)
- [Contact](#)

Welcome to DevSync

### Introduction



### Promotional Video



Prathamesh Palve  
D15A 32

## ADVANCE DEVOPS EXP-2

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

### Elastic Beanstalk:

The screenshot shows the 'Configure environment' step of the AWS Elastic Beanstalk setup wizard. The left sidebar lists steps: Step 1 (Configure environment), Step 2 (Configure service access), Step 3 - optional (Set up networking, database, and tags), Step 4 - optional (Configure instance traffic and scaling), Step 5 - optional (Configure updates, monitoring, and logging), and Step 6 (Review). The main area has four tabs: Environment tier, Application information, Environment information, and Platform.

- Environment tier:** Set to Web server environment. Description: Amazon Elastic Beanstalk has two types of environment tiers to support different types of web applications.
  - Web server environment: Run a website, web application, or web API that serves HTTP requests. [Learn more](#)
  - Worker environment: Run a worker application that processes long-running workloads on demand or performs tasks on a schedule. [Learn more](#)
- Application information:** Application name: myFirstApp. Maximum length of 100 characters.
- Environment information:** Environment name: MyFirstApp-env. Description: Choose the name, subdomain and description for your environment. These cannot be changed later.
  - Environment name: MyFirstApp-env
  - Domain: Leave blank for autogenerated value .eu-north-1.elasticbeanstalk.com [Check availability](#)
  - Environment description: (empty text area)
- Platform:** Platform type: Managed platform. Description: Platforms published and maintained by AWS.
  - Managed platform: Platforms published and maintained by AWS.
  - Custom platform: Platforms you publish and maintain yourself.

**Platform Info**

Platform type

Managed platform  
Platforms published and maintained by Amazon Elastic Beanstalk. Learn more [\[?\]](#)

Custom platform  
Platforms created and owned by you. This option is unavailable if you have no platforms.

Platform

PHP

Platform branch

PHP 8.3 running on 64bit Amazon Linux 2023

Platform version

4.3.2 (Recommended)

**Application code** [Info](#)

Sample application [us-east-1.console.aws.amazon.com/elasticbeanstalk/home?region=us-east-1#/create-environment](#)

WS Services Search [Alt+S] 80% - + (

Step 1 [Configure environment](#)

Step 2 [Configure service access](#)

Step 3 - optional [Set up networking, database, and tags](#)

Step 4 - optional [Configure instance traffic and scaling](#)

Step 5 - optional [Configure updates, monitoring, and logging](#)

Step 6 [Review](#)

**Configure service access** [Info](#)

Service access

IAM roles, assumed by Elastic Beanstalk as a service role, and EC2 instance profiles allow Elastic Beanstalk to create and manage your environment. Both the IAM role and instance profile must be attached to IAM managed policies that contain the required permissions. [Learn more \[?\]](#)

Service role

Create and use new service role

Use an existing service role

Existing service roles

Choose an existing IAM role for Elastic Beanstalk to assume as a service role. The existing IAM role must have the required IAM managed policies.

aws-elasticbeanstalk-service-role

EC2 key pair

Select an EC2 key pair to securely log in to your EC2 instances. [Learn more \[?\]](#)

newKey

EC2 instance profile

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

aws-elasticbeanstalk-ec2-role

[View permission details](#)

Cancel [Skip to review](#) [Previous](#) **Next**

Lifecycle	Log streaming	Allow URL fopen						
false	Deactivated	On						
Display errors	Document root	Max execution time						
Off	-	60						
Memory limit	Zlib output compression	Proxy server						
256M	Off	nginx						
Logs retention	Rotate logs	Update level						
7	Deactivated	minor						
X-Ray enabled								
Deactivated								
<b>Environment properties</b>								
<table border="1"> <thead> <tr> <th>Key</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2">No environment properties</td> </tr> <tr> <td colspan="2">There are no environment properties defined</td> </tr> </tbody> </table>			Key	Value	No environment properties		There are no environment properties defined	
Key	Value							
No environment properties								
There are no environment properties defined								
<input type="button" value="Cancel"/> <input type="button" value="Previous"/> <input type="button" value="Submit"/>								

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

https://eu-north-1.console.aws.amazon.com/elasticbeanstalk/home?region=eu-north-1#/environment/dashboard?environmentId=e-pma2pnpf3q

Elastic Beanstalk > Environments > New-app-env

**New-app-env** [Info]

**Environment overview**

Health	Environment ID
Ok	e-pma2pnpf3q
Domain	Application name
New-app-env.eba-wippim7w.eu-north-1.elasticbeanstalk.com	new-app

**Platform**

Platform
PHP 8.3 running on 64bit Amazon Linux 2023/4.3.2
Running version
-
Platform state
Supported

**Events** (12)

**Events**

Screenshot of the AWS CloudSearch results page for 'codeArtifact'.

The search results are categorized into Services and Features.

**Services** (32 results):

- Amazon Q Developer (Including Amazon CodeWhisperer) ☆
- CodeCommit ☆
- CodePipeline ☆
- AWS Signer ☆

**Features** (45 results):

- Full repository analysis (Amazon CodeGuru feature)
- Pull request code review

Left sidebar (Elastic Beanstalk environment details):

- Applications
- Environments
- Change history
- Application: vedantap (selected)
- Environment: Vedant (selected)
- Go to environment
- Configuration
- Events
- Health
- Logs
- Monitoring
- Alarms
- Managed updates
- Tasks

Bottom navigation bar:

- [Alt+S]
- Developer Tools > CodePipeline > Pipelines
- Introducing the new V2 pipeline type with improved release safety, pipeline triggers, parameterized pipelines, and a new billing model. Learn more [?]
- Pipelines Info
- Notify ▾
- View history
- Release change
- Delete pipeline
- Create pipeline

Name	Latest execution status	Latest source revisions	Latest execution started	Most recent executions
newpipeline (Type: V2   Execution mode: QUEUED)	Failed	Source – fb61b094 Update index.html	6 days ago	<a href="#">View details</a>

AWS Services Search [Alt+S] N. Virginia ▾ View

Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1 Choose pipeline settings Step 1 of 5

**Pipeline settings**

Pipeline name Enter the pipeline name. You cannot edit the pipeline name after it is created.  
vedant-pipeline No more than 100 characters

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

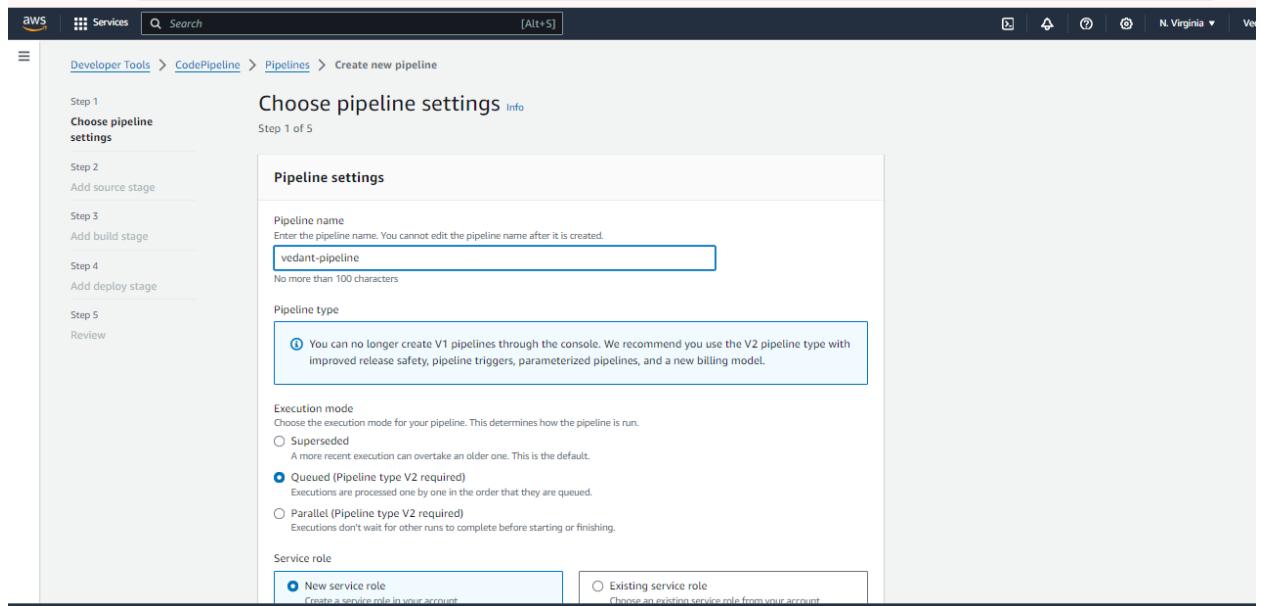
Execution mode Choose the execution mode for your pipeline. This determines how the pipeline is run.

Superseded A more recent execution can overtake an older one. This is the default.

Queued (Pipeline type V2 required) Executions are processed one by one in the order that they are queued.

Parallel (Pipeline type V2 required) Executions don't wait for other runs to complete before starting or finishing.

Service role **New service role** Create a service role in your account.  Existing service role Choose an existing service role from your account.



us-east-1.console.aws.amazon.com/codesuite/settings/connections/create/github... 🔎 ?region=us

aws Services N. Virginia VedantSanap

Developer Tools > Connections > Create connection

Beginning July 1, 2024, the console will create connections with codeconnections in the resource ARN. Resources with both service prefixes will continue to display in the console. [Learn more](#)

## Connect to GitHub

**GitHub connection settings** [Info](#)

Connection name

App installation - *optional*  
Install GitHub App to connect as a bot. Alternatively, leave it blank to connect as a GitHub user, which can be used in AWS CodeBuild projects.

or [Install a new app](#)

▶ Tags - *optional*

**Connect**

CloudShell Feedback Privacy Terms Cookie preferences © 2024, Amazon Web Services, Inc. or its affiliates. Default branch Default branch will be used only when pipeline execution starts from a different source or ma

Screenshot of the AWS CodePipeline console showing the creation of a new pipeline. The pipeline is currently at Step 2: Add source stage.

**Source**

Source provider: GitHub (Version 2)

**New GitHub version 2 (app-based) action**  
To add a GitHub version 2 action in CodePipeline, you create a connection, which uses GitHub Apps to access your repository. Use the options below to choose an existing connection or create a new one. Learn more

Connection: Choose an existing connection that you have already configured, or create a new one and then return to this task.  
arn:aws:codeconnections:us-east-1:314146309670:connection/7e91c9d2-bb X or Connect to GitHub

**Ready to connect**  
Your GitHub connection is ready for use.

Repository name: Choose a repository in your GitHub account.  
arn:aws:codepipeline-s3-codedeploy-linux-2.0 X

You can type or paste the group path to any project that the provided credentials can access. Use the format 'group/subgroup/project'.

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

**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.

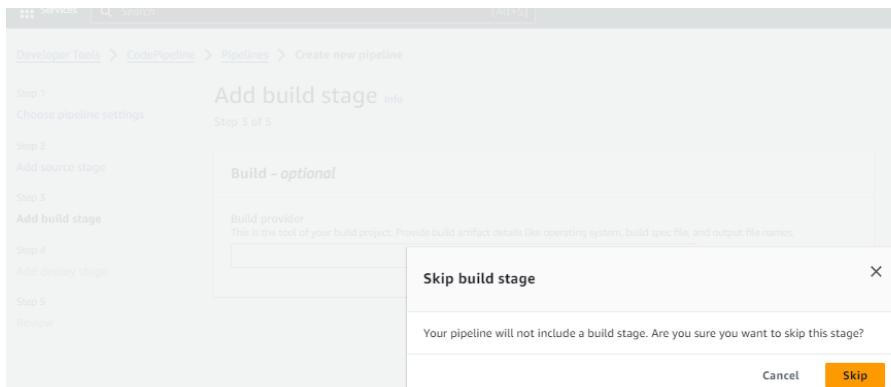
**Specify filter**  
Starts your pipeline on a specific filter and clones the exact commit. Pipeline type V2 is required.

**Do not detect changes**  
Don't automatically trigger the pipeline.

**Info:** You can add additional sources and triggers by editing the pipeline after it is created.

Cancel Previous Next

Feedback © 2024, Amazon Web Services, Inc. or its affiliates.



Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1 Choose pipeline settings Step 3 of 5

Step 2 Add source stage

Step 3 Add build stage

Step 4 Add deploy stage

Step 5 Review

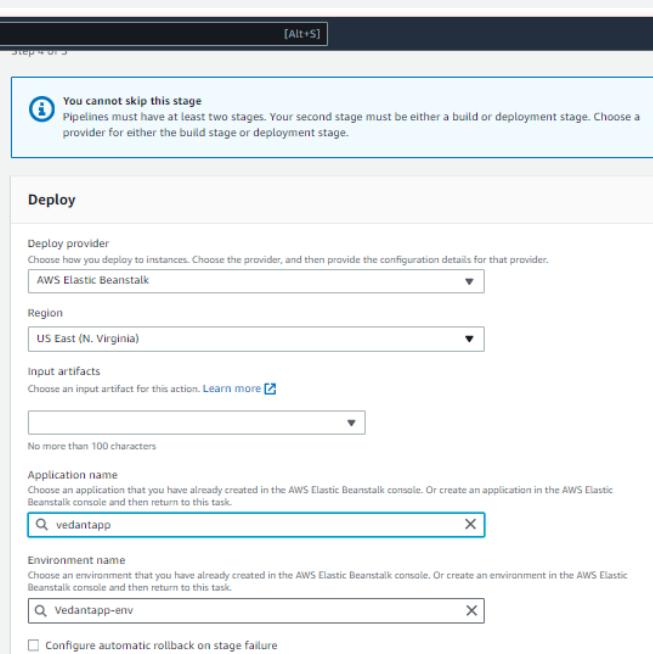
**Build - optional**

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

**Skip build stage**

Your pipeline will not include a build stage. Are you sure you want to skip this stage?

Cancel Skip

You cannot skip this stage

Pipelines must have at least two stages. Your second stage must be either a build or deployment stage. Choose a provider for either the build stage or deployment stage.

**Deploy**

Deploy provider Choose how you deploy to instances. Choose the provider, and then provide the configuration details for that provider.

AWS Elastic Beanstalk

Region US East (N. Virginia)

Input artifacts Choose an input artifact for this action. [Learn more](#)

No more than 100 characters

Application name Choose an application that you have already created in the AWS Elastic Beanstalk console. Or create an application in the AWS Elastic Beanstalk console and then return to this task.

vedantapp

Environment name Choose an environment that you have already created in the AWS Elastic Beanstalk console. Or create an environment in the AWS Elastic Beanstalk console and then return to this task.

Vedantapp-env

Configure automatic rollback on stage failure

Cancel Previous Next

us-east-1.console.aws.amazon.com/codesuite/codepipeline/pipeline/new?region=us-east-1

Trigger configuration  
You can add additional pipeline triggers after the pipeline is created.

Trigger type  
No filter

**Step 3: Add build stage**

Build action provider

Build stage  
No build

**Step 4: Add deploy stage**

Deploy action provider

Deploy action provider  
AWS Elastic Beanstalk

ApplicationName  
vedantapp

EnvironmentName  
Vedantapp-env

Configure automatic rollback on stage failure  
Disabled

Cancel Previous Create pipeline

The screenshot shows the 'Create Pipeline' wizard in the AWS CodePipeline console. In Step 4, a single stage named 'Deploy' is configured using the 'AWS Elastic Beanstalk' provider. The stage details include the application name 'vedantapp' and environment 'Vedantapp-env'. The stage status is 'Succeeded'. The 'Create pipeline' button is highlighted in orange at the bottom right.

Pipeline type: V2 Execution mode: QUEUED

**Source** Succeeded  
Pipeline execution ID: d20db24-22b8-4e0f-9e00-497633d23011

Source GitHub (Version 2) Succeeded 1 minute ago  
View details

Source Update index.html

**Deploy** Succeeded  
Pipeline execution ID: d20db24-22b8-4e0f-9e00-497633d23011

Deploy AWS Elastic Beanstalk Succeeded just now  
Start rollback

Disable transition

CloudShell Feedback

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

The screenshot shows the 'Pipeline details' page for the 'vedantapp' pipeline. The pipeline is currently in 'QUEUED' mode. It consists of two stages: 'Source' and 'Deploy'. The 'Source' stage is triggered by GitHub (Version 2) and has succeeded. The 'Deploy' stage is triggered by AWS Elastic Beanstalk and has also succeeded. There is a 'Start rollback' button available for the 'Deploy' stage. The pipeline is set to start a rollback if needed. The sidebar on the left provides navigation links for other AWS services like CodeBuild and CodeDeploy.

Screenshot of the AWS Elastic Beanstalk Environments page showing two environments: Mynewapp-env (terminated) and Vedantapp-env.

Environment name	Health	Application name	Platform	Domain	Running versions	Tier name	Date created
Mynewapp-env (terminated)	Unknown	MyNewApp	PHP 8.3 running on 64bit Amazon Linux 2 v2.9.11	Mynewapp-env.eba-pfz7h5nw...	-	WebServer	August 13, 2024 14:08...
Vedantapp-env	Ok	vedantapp	PHP 8.3 running on 64bit Amazon Linux 2 v2.9.11	Vedantapp-env.eba-5xm9gupn...	code-pipeline-172413...	WebServer	August 20, 2024 12:56...

The browser window shows a deployment success message:

# Congratulations!

You have successfully created a pipeline that retrieved this source application from an Amazon S3 bucket and deployed it to three Amazon EC2 instances using AWS CodeDeploy.

Updated Changes

## S3 Bucket :

Buckets are containers for data stored in S3.

### General configuration

AWS Region  
Europe (Stockholm) eu-north-1

Bucket type [Info](#)

General purpose  
Recommended for most use cases and access patterns.  
General purpose buckets are the original S3 bucket type.  
They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory - New  
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - *optional*  
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

### Object Ownership [Info](#)

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

**Files and folders (1 Total, 505.0 B)**

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	index.html	-	text/html

**Destination** [Info](#)

Destination  
<s3://vedantawsbucke>

▶ **Destination details**  
Bucket settings that impact new objects stored in the specified destination.

Feedback © 2024 Amazon Web Services

## Edit Block public access (bucket settings) [Info](#)

### Block public access (bucket settings)

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

**Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through *new* access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through *any* access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through *new* public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

## Object Ownership

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

ACLs disabled (recommended)

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

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



**Enabling ACLs turns off the bucket owner enforced setting for Object Ownership**

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

I acknowledge that ACLs will be restored.

## Object Ownership

Upload succeeded

[View details below.](#)

## Upload: status

[Close](#)

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

### Summary

Destination  
[s3://vedantawsbucke](#)

Succeeded

1 file, 505.0 B (100.00%)

Failed

0 files, 0 B (0%)

[Files and folders](#)

[Configuration](#)

**Files and folders (1 Total, 505.0 B)**

## Edit static website hosting Info

### Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

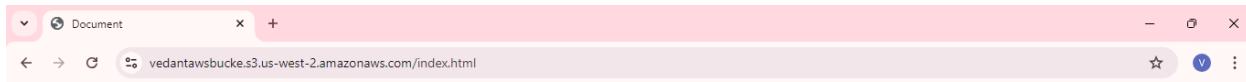
#### Static website hosting

- Disable  
 Enable

#### Hosting type

- Host a static website  
Use the bucket endpoint as the web address. [Learn more](#)  
 Redirect requests for an object  
Redirect requests to another bucket or domain. [Learn more](#)

**i** For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)



## Hello World

HEllo World Lorem ipsum dolor sit amet consectetur, adipisicing elit. Rem voluptatibus sint ipsam, iure eligendi velit laboriosam vitae nisi facilis ipsa recusandae nulla quia assumenda rerum quos, exercitationem doloribus consectetur voluptate.

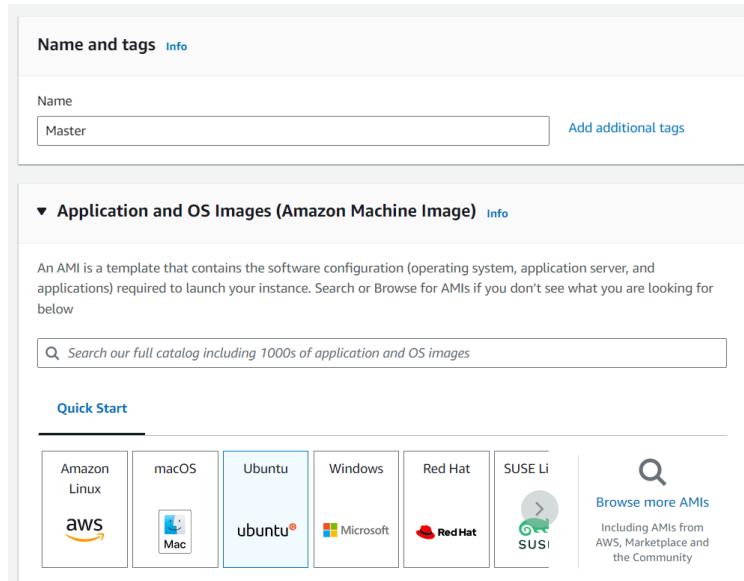


## Experiment No 3

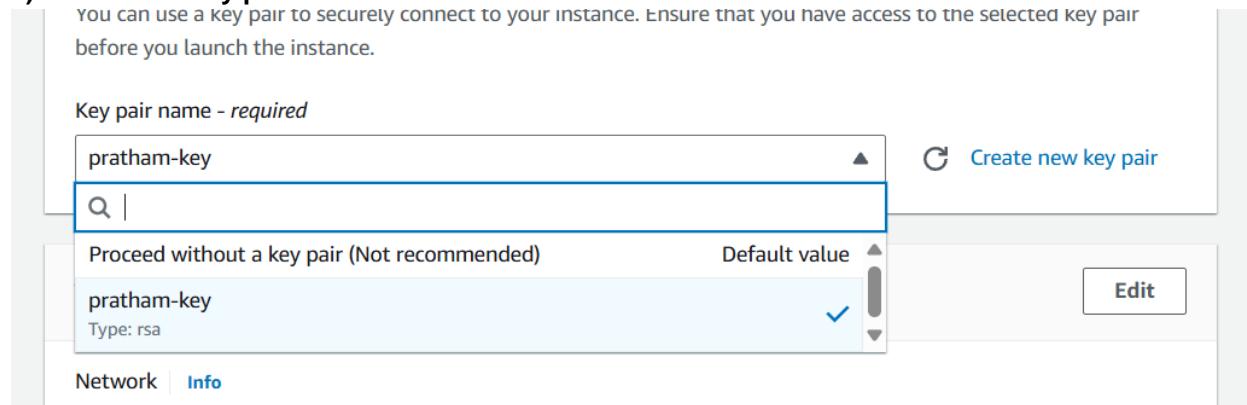
Prathamesh Palve  
D15A 32  
Batch B

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

### 1) Launch 2 EC2 instance and select Ubuntu in AMI



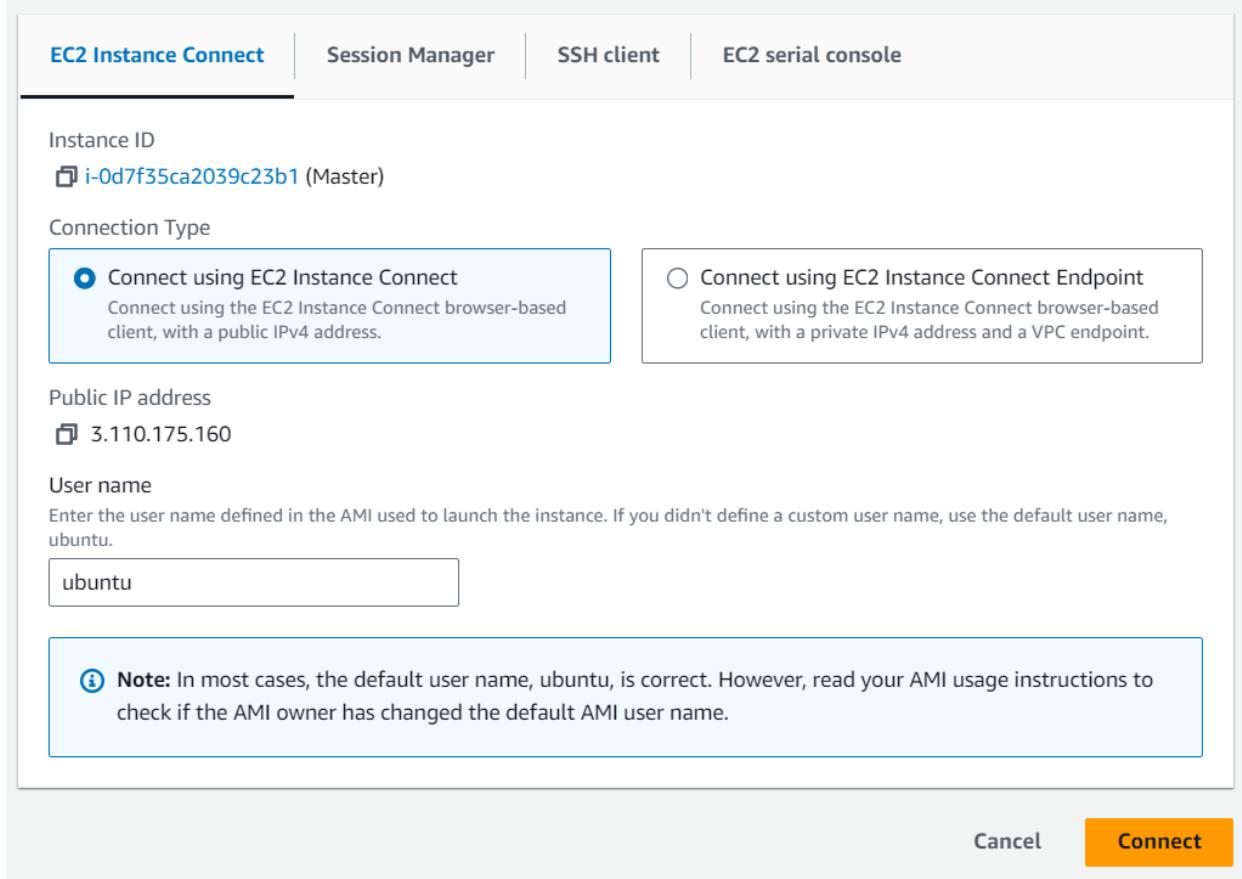
### 2) Create new key pair



- 3) In Security group select all checkbox and launch instance
- 4) Go to security group and edit inbound rules of both instance
- 5) Delete all the rules and add new rule with All traffic and Anywhere-IPv4

Inbound rules (1/1)							<input type="button" value="Edit inbound rules"/>
<input type="button" value="Filter security group rules"/>							<input type="button" value="Manage tags"/>
Name	Security group rule...	IP version	Type	Protocol	Port range		
<input checked="" type="checkbox"/> -	sgr-07c7275a5903c511f	IPv4	All traffic	All	All		

6) Now in running instances click on master instance and click on connect



8) Similarly connect the worker

9) Set hostname to master and worker respectively

```
ubuntu@ip-172-31-12-130:~$ sudo hostnamectl set-hostname master  
ubuntu@ip-172-31-12-130:~$
```

```
ubuntu@master:~$
```

```
ubuntu@worker:~$
```

10) Use command sudo apt-get update on both master and worker CLI

sudo apt-get update on both

```
Get:24 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [10.5 kB]
Get:25 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [388 B]
Get:26 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [1]
Get:27 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [24.3 kB]
Get:28 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [16.4 kB]
Get:29 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [644 B]
Get:30 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 c-n-f Metadata [1]
Get:31 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [765 kB]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [165 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [11.3 kB]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [826 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [133 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [536 B]
Get:37 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [781 kB]
Get:38 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [143 kB]
Get:39 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [16.7 kB]
Get:40 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [36.5 kB]
Get:41 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [7060 B]
Get:42 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-n-f Metadata [260 B]
Fetched 27.1 MB in 5s (5664 kB/s)
Reading package lists... Done
ubuntu@master:~$
```

## 11) Installing Docker on both CLI

```
sudo apt-get install docker.io on both
```

```
Done.
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /lib/systemd/system/docker.service.
Created symlink /etc/systemd/system/sockets.target.wants/docker.socket → /lib/systemd/system/docker.socket.
Processing triggers for dbus (1.12.20-2ubuntu4.1) ...
Processing triggers for man-db (2.10.2-1) ...
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@master:~$
```

## 12) Enable Docker on both CLI and check its status

```
sudo systemctl enable docker
```

```
sudo systemctl status docker on both
```

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@master:~$ sudo systemctl enable docker
ubuntu@master:~$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2023-09-17 17:23:49 UTC; 3min 30s ago
     Docs: https://docs.docker.com
 Main PID: 3050 (dockerd)
    Tasks: 7
   Memory: 33.2M
      CPU: 291ms
     CGroup: /system.slice/docker.service
             └─3050 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
```

**DOCKER INSTALLED SUCCESSFULLY**

## 13) Now for Installing Kubernetes (On both CLI)

```
sudo apt-get update
```

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

```
sudo apt-get install -y apt-transport-https ca-certificates curl
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt, it does not contain exactly one certificate or CRL
19 added, 6 removed; done.
Setting up libcurl4:amd64 (7.81.0-1ubuntu1.13) ...
Setting up curl (7.81.0-1ubuntu1.13) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
Processing triggers for ca-certificates (20230311ubuntu0.22.04.1) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
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@master:~$ 
```

#### 14) Download Google cloud public signing key

```
sudo curl -fsSLo /usr/share/keyrings/kubernetes-archive-keyring.gpg https://dl.k8s.io/apt/doc/apt-key.gpg
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@master:~$ sudo curl -fsSLo /usr/share/keyrings/kubernetes-archive-keyring.gpg https://dl.k8s.io/apt/doc/apt-key.gpg
ubuntu@master:~$ 
```

#### 15) Adding kubernetes apt repository

```
echo "deb [signed-by=/usr/share/keyrings/kubernetes-archive-keyring.gpg] https://apt.kubernetes.io/
kubernetes-xenial main" | sudo tee /etc/apt/sources.list.d/kubernetes.list
```

```
ubuntu@master:~$ echo "deb [signed-by=/usr/share/keyrings/kubernetes-archive-keyring.gpg] https://apt.kubernetes.io/ kubernetes-xenial main" | sudo tee /etc/apt/sources.list.d/kubernetes.list
deb [signed-by=/usr/share/keyrings/kubernetes-archive-keyring.gpg] https://apt.kubernetes.io/ kubernetes-xenial main
ubuntu@master:~$ 
```

#### 16) Run this 3 commands

```
sudo apt-get update
```

```
ubuntu@master:~$ sudo apt-get update
Hit:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Get:5 https://packages.cloud.google.com/apt kubernetes-xenial InRelease [8993 B]
Get:6 https://packages.cloud.google.com/apt kubernetes-xenial/main amd64 Packages [69.9 kB]
Fetched 78.9 kB in 1s (53.8 kB/s)
Reading package lists... Done
ubuntu@master:~$ 
```

```
sudo apt-get install -y kubelet kubeadm kubectl
```

```
Setting up conntrack (1:1.4.6-2build2) ...
Setting up kubectl (1.28.2-00) ...
Setting up ebtables (2.0.11-4build2) ...
Setting up socat (1.7.4.1-3ubuntu4) ...
Setting up cri-tools (1.26.0-00) ...
Setting up kubernetes-cni (1.2.0-00) ...
Setting up kubelet (1.28.2-00) ...
Created symlink /etc/systemd/system/multi-user.target.wants/kubelet.service → /lib/systemd/system/kubelet.service.
Setting up kubeadm (1.28.2-00) ...
Processing triggers for man-db (2.10.2-1) ...
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@master:~$ 
```

sudo apt-mark hold kubelet kubeadm kubectl

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

## KUBERNETES INSTALLED SUCCESSFULLY

### 17) Kubernetes Deployment

sudo swapoff -a

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

### 18) Initialize kubernetes on Master

sudo touch "/etc/docker/daemon.json"

sudo nano "/etc/docker/daemon.json" Run this command and copy paste this

```
{
"exec-opts": ["native.cgroupdriver=systemd"]
}
```

Then press ctrl + O and enter then ctrl + X

sudo cat "/etc/docker/daemon.json"

sudo systemctl daemon-reload

sudo systemctl restart docker

sudo systemctl restart kubelet

sudo kubeadm reset

```
ubuntu@master:~$ sudo touch "/etc/docker/daemon.json"
ubuntu@master:~$ sudo nano "/etc/docker/daemon.json" 
```

```
ubuntu@master:~$ sudo cat "/etc/docker/daemon.json"
{
    "exec-opts": ["native.cgroupdriver=systemd"],
    "log-driver": "json-file",
    "log-opt": {
        "max-size": "100m"
    },
    "storage-driver": "overlay2"
}
```

```
ubuntu@master:~$ sudo systemctl daemon-reload
ubuntu@master:~$ sudo systemctl restart docker
ubuntu@master:~$ sudo systemctl restart kubelet
ubuntu@master:~$ sudo kubeadm reset
W0917 18:15:57.371540    10839 preflight.go:56] [reset] WARNING: 0
[reset] Are you sure you want to proceed? [y/N]: y
[preflight] Running pre-flight checks
W0917 18:16:01.329044    10839 removeetcdmember.go:106] [reset] No
[reset] Deleted contents of the etcd data directory: /var/lib/etcd
[reset] Stopping the kubelet service
[reset] Unmounting mounted directories in "/var/lib/kubelet"
```

```
$ sudo kubeadm init --pod-network-cidr=10.244.0.0/16 --ignore-preflight-errors=all
ubuntu@master:~$ sudo kubeadm init --pod-network-cidr=10.244.0.0/16 --ignore-preflight-er
[init] Using Kubernetes version: v1.28.2
[preflight] Running pre-flight checks
    [WARNING NumCPU]: the number of available CPUs 1 is less than the required 2
    [WARNING Mem]: the system RAM (965 MB) is less than the minimum 1700 MB
[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 conn
[preflight] You can also perform this action in beforehand using 'kubeadm config images p
W0917 18:17:31.346348 10860 checks.go:835] detected that the sandbox image "registry.k8
    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 [kubernetes kubernetes.default kub
    172.31.12.130]
[certs] Generating "apiserver-kubelet-client" certificate and key
[certs] Generating "front-proxy-ca" certificate and key
[certs] Generating "front-proxy-client" certificate and key
[certs] Generating "etcd/ca" certificate and key
[certs] Generating "etcd/server" certificate and key
[certs] etcd/server serving cert is signed for DNS names [localhost master] and IPs [172.
[certs] Generating "etcd/peer" certificate and key
[certs] etcd/peer serving cert is signed for DNS names [localhost master] and IPs [172.31
[certs] Generating "etcd/healthcheck-client" certificate and key
[certs] Generating "apiserver-etcd-client" certificate and key
[certs] Generating "sa" key and public key
```

```
kubeadm join 172.31.12.130:6443 --token 67nba2.98zekjx1ogwtr29 --discovery-token-ca-cert-hash sha256:5d3403f5221016f77cbef1757a266467af45dc41b765ebe535f15ee058baf883
```

```
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 172.31.12.130:6443 --token 67nba2.98zekjx1ogwtrr29 \
--discovery-token-ca-cert-hash sha256:5d3403f5221016f77cb1757a266467af45dc41b765ebe535f15ee058baf883
ubuntu@master:~$ 
```

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

```
ubuntu@master:~$ kubectl apply -f https://github.com/flannel-io/flannel/releases/latest/download/kube-flannel.yml
namespace/kube-flannel created
serviceaccount/flannel created
clusterrole.rbac.authorization.k8s.io/flannel created
clusterrolebinding.rbac.authorization.k8s.io/flannel created
configmap/kube-flannel-cfg created
daemonset.apps/kube-flannel-ds created
ubuntu@master:~$ 
```

```
[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...
I0917 18:31:31.967826    11348 kubelet.go:220] [kubelet-start] preserving the crisocket information for the node
I0917 18:31:31.968119    11348 patchnode.go:31] [patchnode] Uploading the CRI Socket information "unix:///var/run/kubelet.sock" as an annotation
I0917 18:31:31.968407    11348 cert_rotation.go:137] Starting client certificate rotation controller
```

```
This node has joined the cluster:
```

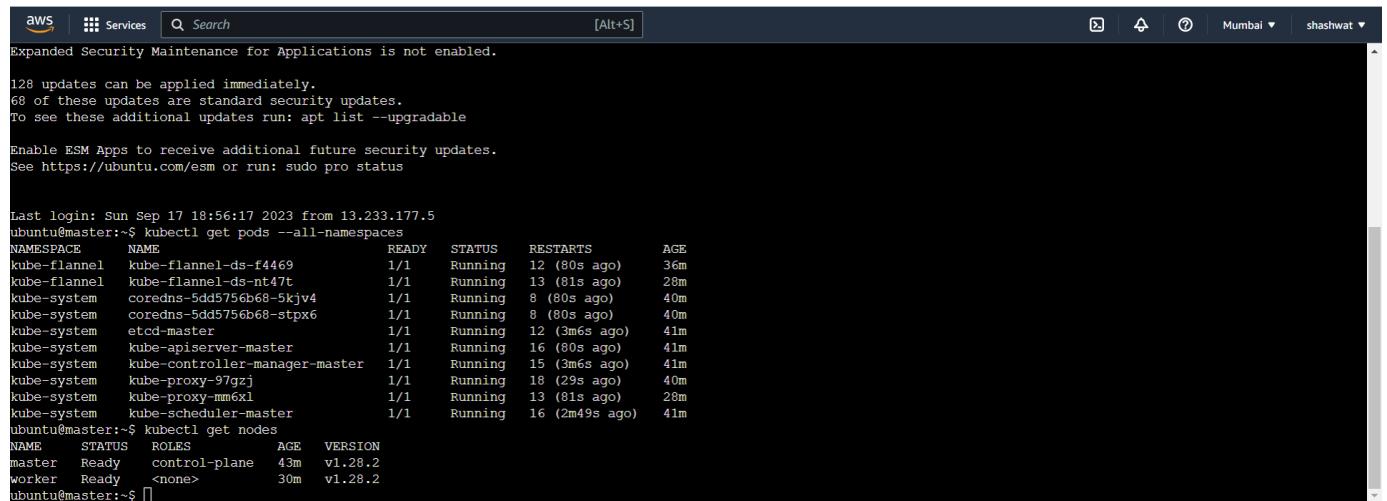
```
* Certificate signing request was sent to apiserver and a response was received.
* The Kubelet was informed of the new secure connection details.
```

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

```
ubuntu@worker:~$ 
```

```
ubuntu@master:~$ kubectl get pods --all-namespaces
The connection to the server 172.31.12.130:6443 was refused - did you specify the right host or port?
ubuntu@master:~$ 
```

```
ubuntu@master:~$ kubectl get nodes
NAME      STATUS      ROLES      AGE      VERSION
master    Ready       control-plane   24m     v1.28.2
worker    Ready       <none>        11m     v1.28.2
ubuntu@master:~$ 
```



The screenshot shows a terminal window within the AWS CloudShell interface. The terminal displays several commands related to Kubernetes and system updates:

```
Expanded Security Maintenance for Applications is not enabled.  
128 updates can be applied immediately.  
68 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
Last login: Sun Sep 17 18:56:17 2023 from 13.233.177.5  
ubuntu@master:~$ kubectl get pods --all-namespaces  
NAMESPACE     NAME           READY   STATUS    RESTARTS   AGE  
kube-flannel  kube-flannel-ds-f4469  1/1     Running  12 (80s ago)  36m  
kube-flannel  kube-flannel-ds-nt47t  1/1     Running  13 (81s ago)  28m  
kube-system   coredns-5dd5756b68-5kjv4  1/1     Running  8 (80s ago)  40m  
kube-system   coredns-5dd5756b68-stpx6  1/1     Running  8 (80s ago)  40m  
kube-system   etcd-master          1/1     Running  12 (3m6s ago)  41m  
kube-system   kube-apiserver-master  1/1     Running  16 (80s ago)  41m  
kube-system   kube-controller-manager-master  1/1     Running  15 (3m6s ago)  41m  
kube-system   kube-proxy-97gjz      1/1     Running  18 (29s ago)  40m  
kube-system   kube-proxy-mm6xl      1/1     Running  13 (81s ago)  28m  
kube-system   kube-scheduler-master  1/1     Running  16 (2m49s ago)  41m  
ubuntu@master:~$ kubectl get nodes  
NAME      STATUS  ROLES      AGE   VERSION  
master    Ready   control-plane  43m   v1.28.2  
worker   Ready   <none>    30m   v1.28.2  
ubuntu@master:~$
```

## Conclusion:

Thus we have understood the Kubernetes Cluster Architecture, installed and spun a Kubernetes Cluster on AWS Cloud Platform.

## Error:

The status of all namespaces was not showing running in the first try, but when I rebooted the master and worker instances it was successful.

## Experiment No 4

Prathamesh Palve  
D15A 32  
Batch B

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

- Running the application on the cluster

```
kubectl create deployment nginx --image=nginx
```

```
Last login: Sun Sep 17 18:58:53 2023 from 13.233.177.4
ubuntu@master:~$ kubectl create deployment nginx --image=nginx
deployment.apps/nginx created
ubuntu@master:~$ █
```

- Verifying the deployment using command

```
kubectl get deployments
```

```
ubuntu@master:~$ kubectl get deployments
NAME      READY    UP-TO-DATE   AVAILABLE   AGE
nginx     1/1      1           1           47s
ubuntu@master:~$ █
```

- Run the following command to create a service named nginx that will expose the app publicly.

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

```
ubuntu@master:~$ kubectl expose deploy nginx --port 80 --target-port 80 --type NodePort
service/nginx exposed
ubuntu@master:~$ █
```

- Run this command to see the summary of the service and ports exposed.

```
kubectl get services
```

```
ubuntu@master:~$ kubectl get services
NAME      TYPE        CLUSTER-IP   EXTERNAL-IP  PORT(S)          AGE
kubernetes  ClusterIP  10.96.0.1   <none>       443/TCP         4d14h
nginx      NodePort    10.103.96.233  <none>       80:30816/TCP   67s
ubuntu@master:~$ █
```

- Add the port which is displayed i.e 30816 (will differ for each device) in the inbound rules of the security group of the worker.

Inbound rules (2)						
	Name	Security group rule...	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-067c4ec19a6dc863c	IPv4	Custom TCP	TCP	30816
<input type="checkbox"/>	-	sgr-043a60f4b25fe2c26	IPv4	All traffic	All	

- We can verify that the nginx page is accessible on all nodes using curl command(Worker)

1. sudo su
2. curl worker:30816

```
Last login: Fri Sep 22 13:48:46 2023 from 13.233.177.4
ubuntu@worker:~$ sudo su
root@worker:/home/ubuntu# curl worker:30816
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>. <br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
root@worker:/home/ubuntu# 
```

**Open a new tab in browser and paste the public IP address followed by :port number (30816 in my case)**



## Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org).  
Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*

## Conclusion:

Thus, we have studied and implemented how to install Kubectl and execute Kubectl commands to manage the Kubernetes cluster and deploy.

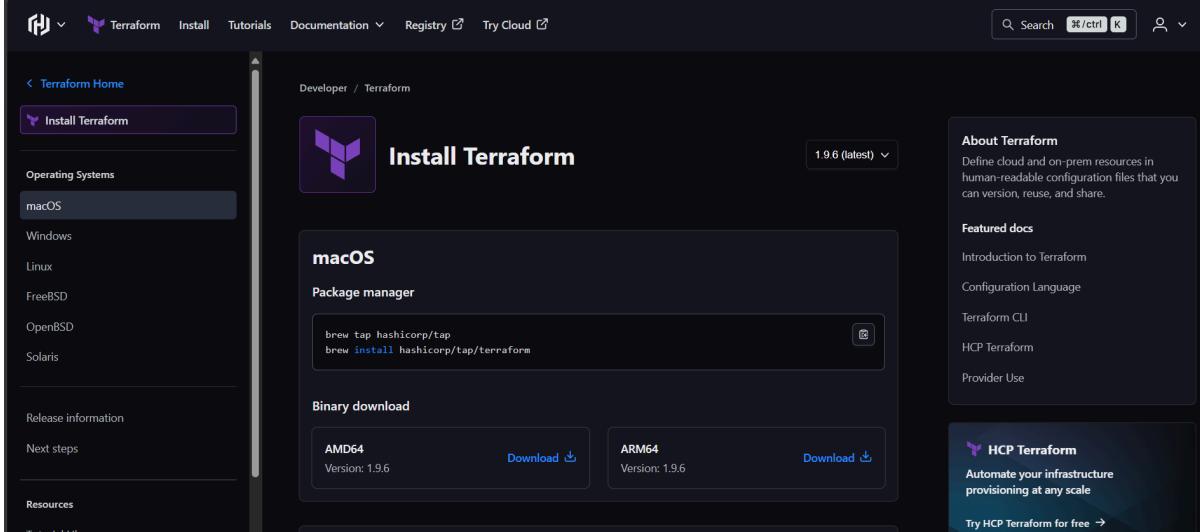
## Errors:

I was facing an error because I forgot to make changes in the security group of worker node.

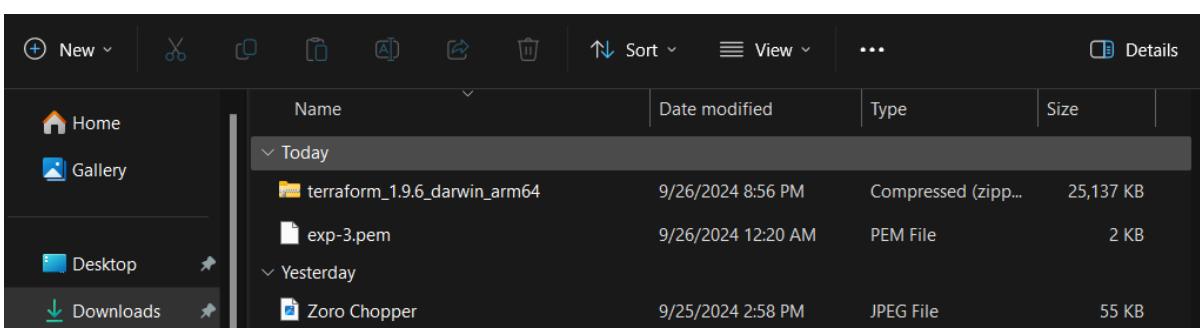
## Experiment-5 : Terraform

Aim : Installation and Configuration of Terraform in Windows

Step - 1 : Installing Terraform zip file

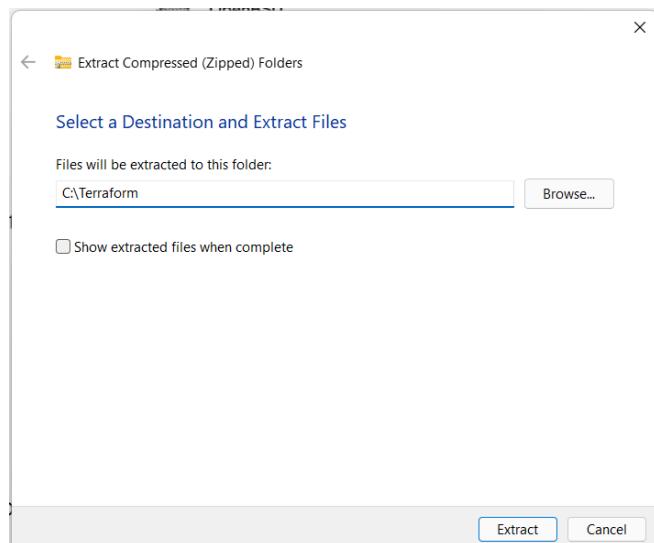


The screenshot shows the Terraform website's "Install Terraform" page for macOS. It features a "Package manager" section with the command `brew tap hashicorp/tap` and `brew install hashicorp/tap/terraform`, and a "Binary download" section for AMD64 and ARM64 architectures, both at version 1.9.6.

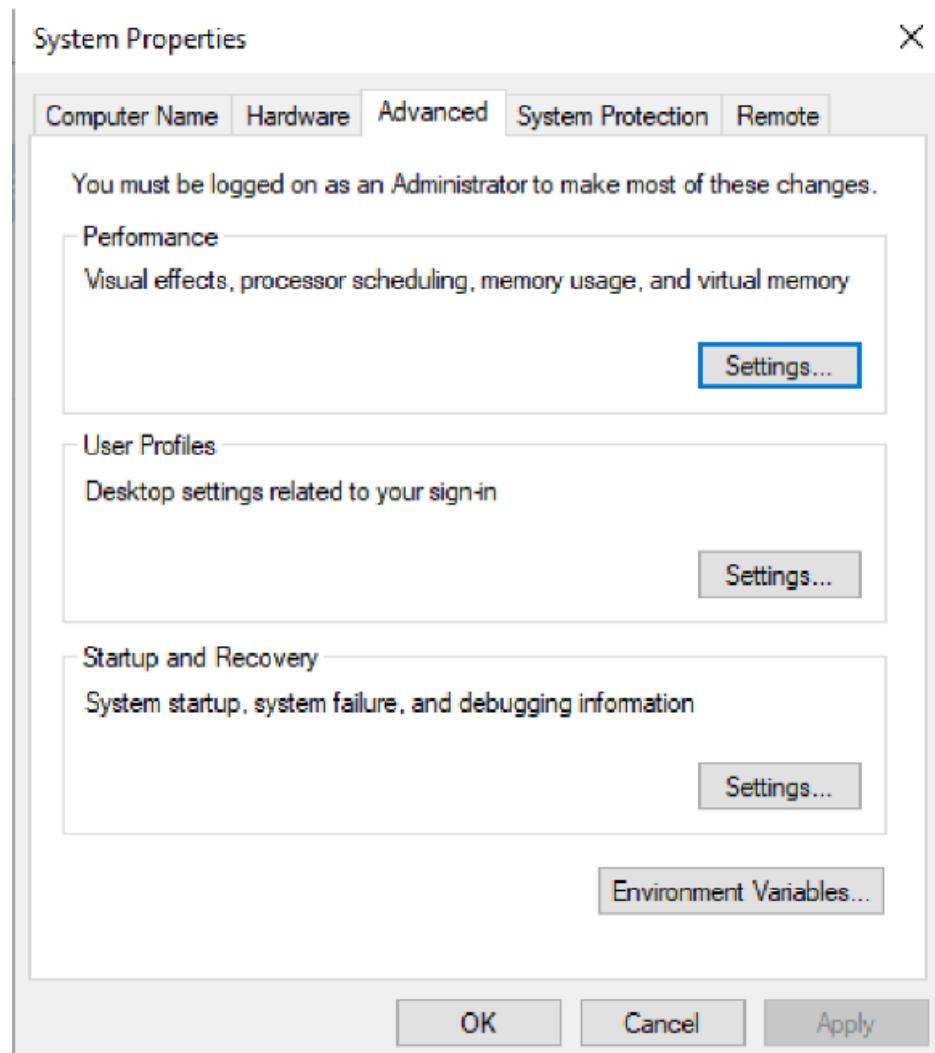
  


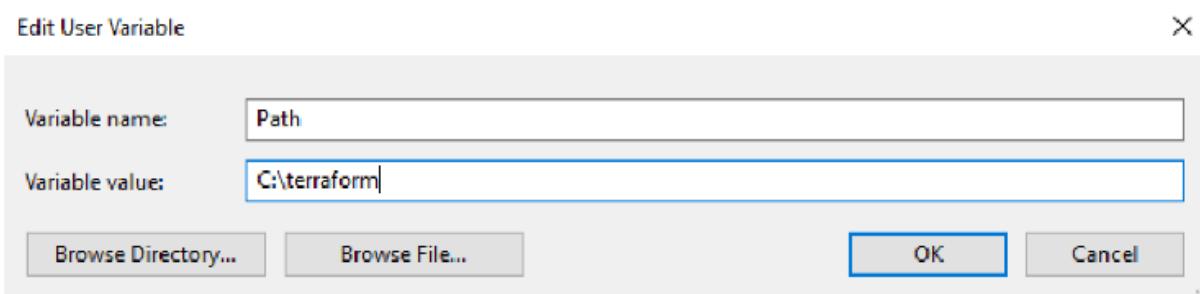
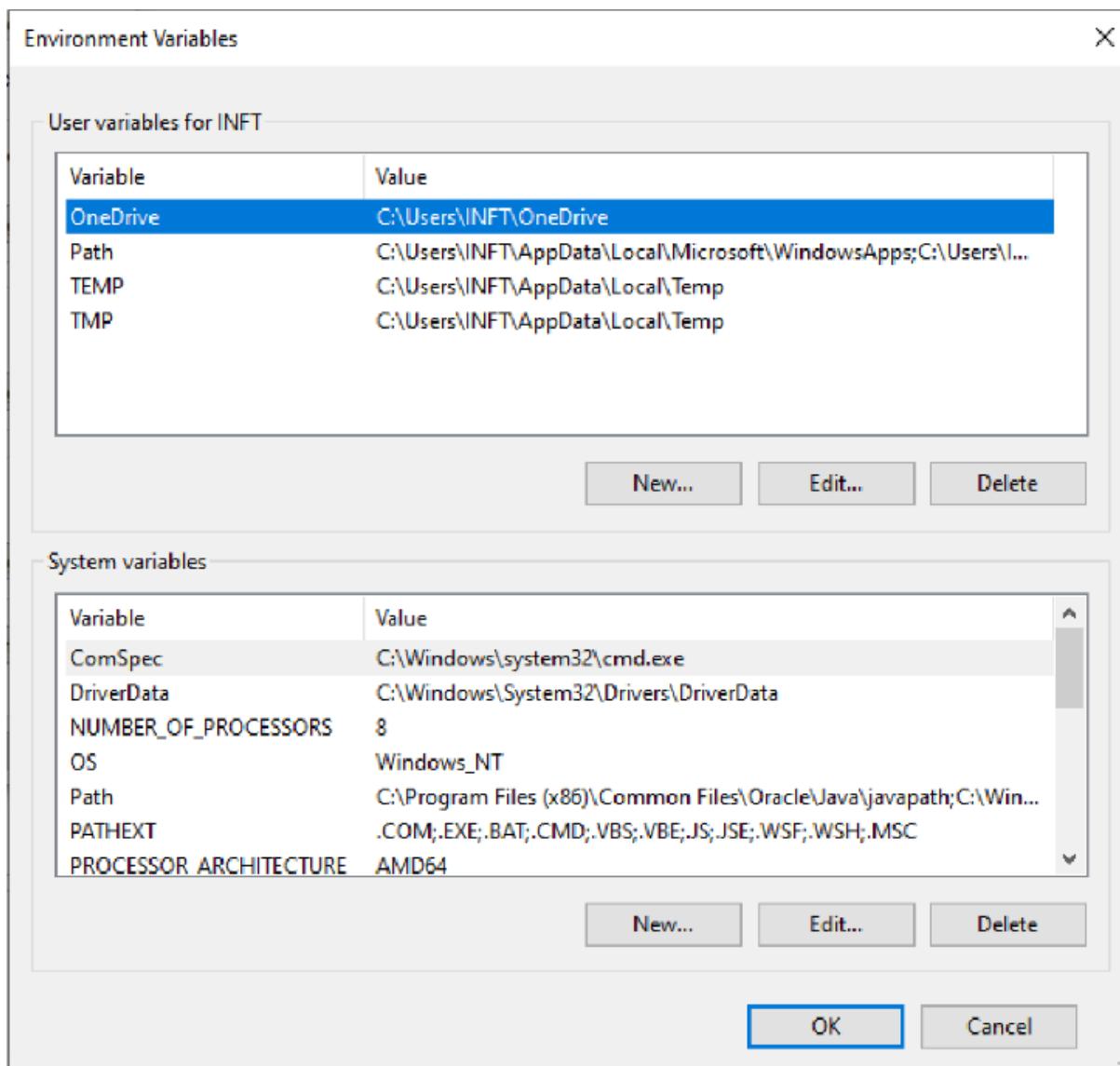
The screenshot shows the Windows File Explorer displaying the contents of the "Downloads" folder. It lists several files: "terraform\_1.9.6\_darwin\_arm64" (a compressed file), "exp-3.pem" (a PEM file), and "Zoro Chopper" (a JPEG file).

Step - 2 : extracting terraform from zip file



### Step - 3 : editing environment variables





#### Step 4 : opening windows powershell as admin



#### Step 5 : run terraform

```
Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> 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        Reformatted 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.

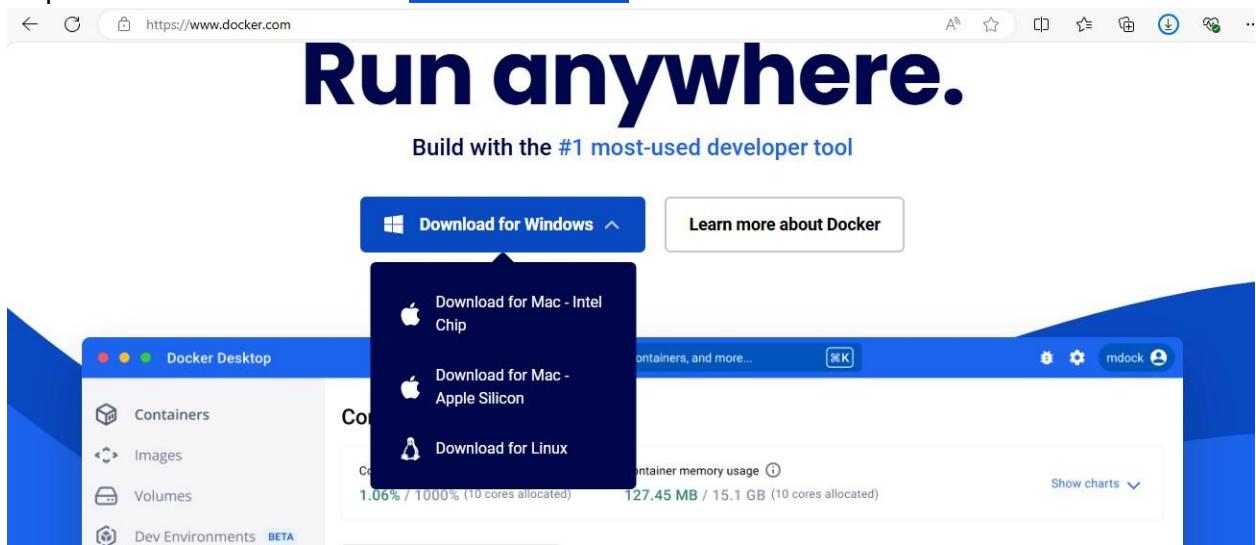
PS C:\WINDOWS\system32>
```

## Experiment 6

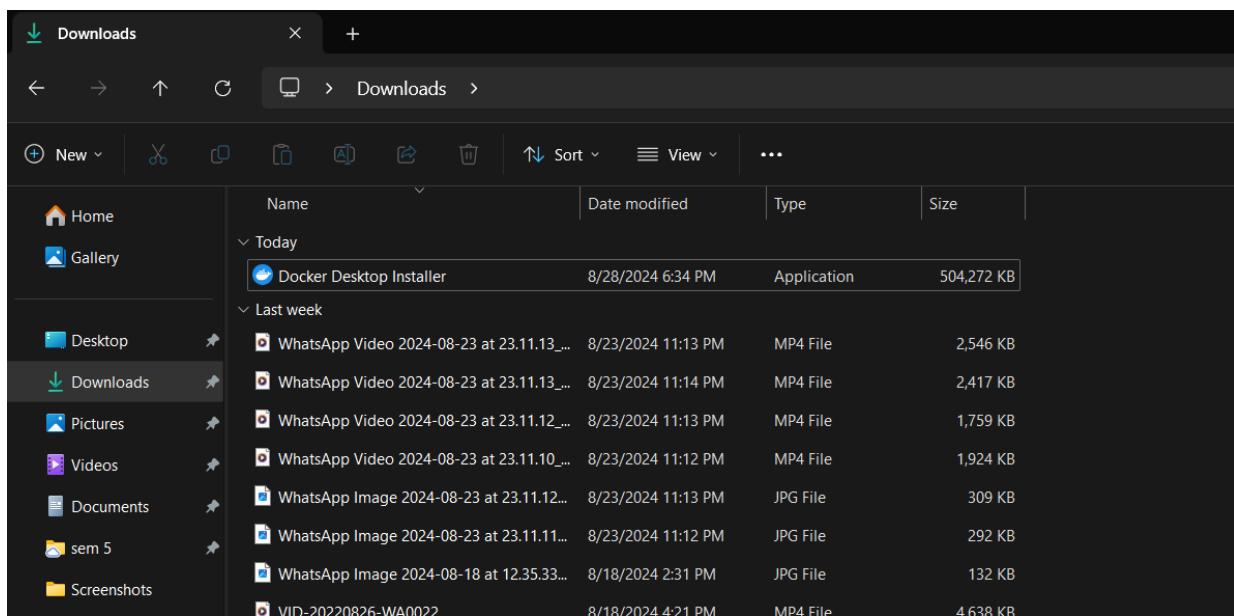
**Aim:**

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

Step 1: Download Docker from [www.docker.com](https://www.docker.com)



Step 2: The Docker is successfully downloaded. Now, run the docker installer and complete the installation.



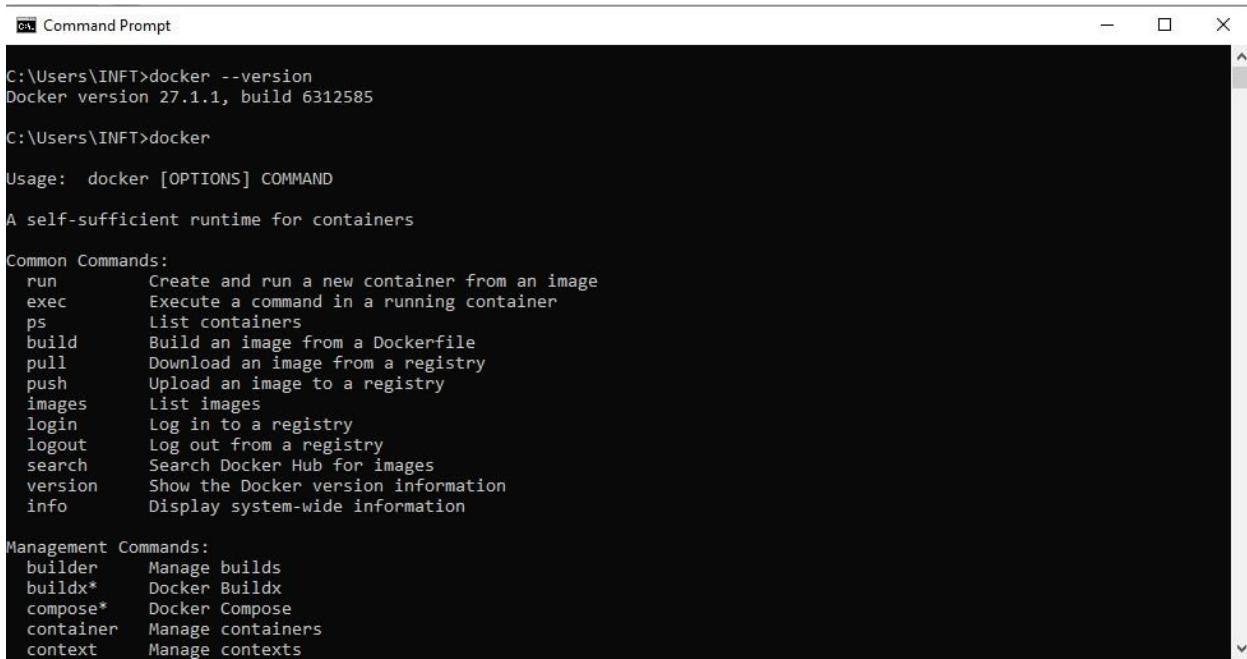


```
Unpacking file: resources/docker-desktop.iso  
Unpacking file: resources/ddvp.ico  
Unpacking file: resources/config-options.json  
Unpacking file: resources/componentsVersion.json  
Unpacking file: resources/bin/docker-compose  
Unpacking file: resources/bin/docker  
Unpacking file: resources/.gitignore  
Unpacking file: InstallerCli.pdb  
Unpacking file: InstallerCli.exe.config  
Unpacking file: frontend/vk_swiftshader_icd.json  
Unpacking file: frontend/v8_context_snapshot.bin  
Unpacking file: frontend/snapshot_blob.bin  
Unpacking file: frontend/resources/regedit/vbs/util.vbs  
Unpacking file: frontend/resources/regedit/vbs/regUtil.vbs
```



Close

Step 3: Open Command Prompt and run as administrator. Enter the command docker --version, to check whether the docker is successfully installed.



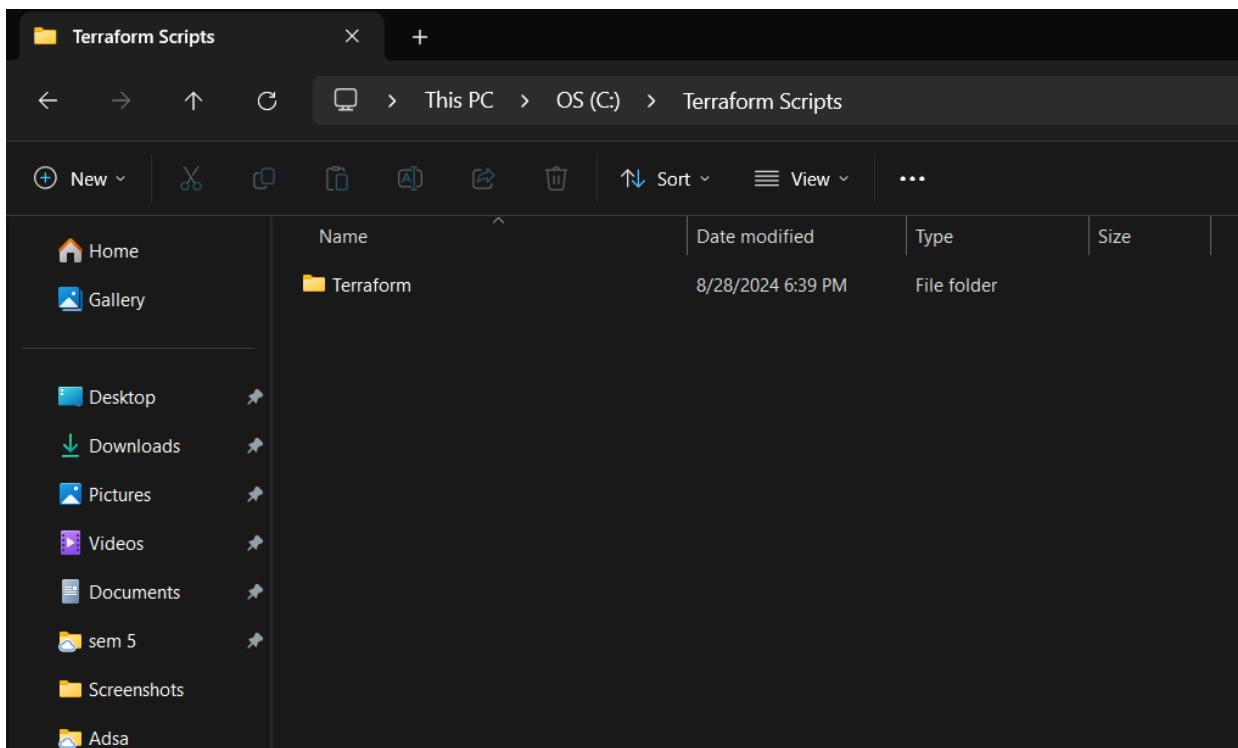
```
C:\Users\INFT>docker --version
Docker version 27.1.1, build 6312585

C:\Users\INFT>docker
Usage: docker [OPTIONS] COMMAND
A self-sufficient runtime for containers

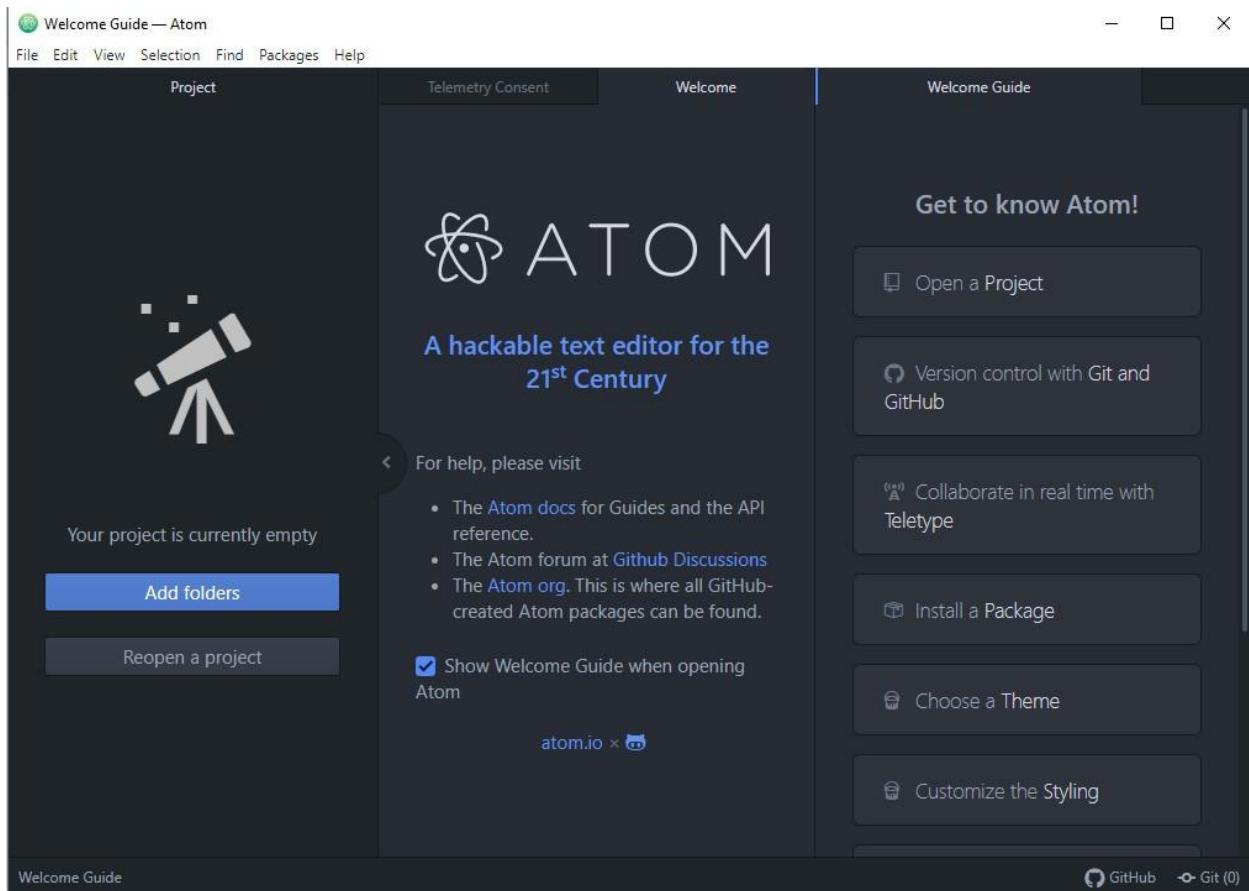
Common Commands:
  run      Create and run a new container from an image
  exec     Execute a command in a running container
  ps       List containers
  build    Build an image from a Dockerfile
  pull    Download an image from a registry
  push     Upload an image to a registry
  images   List images
  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
```

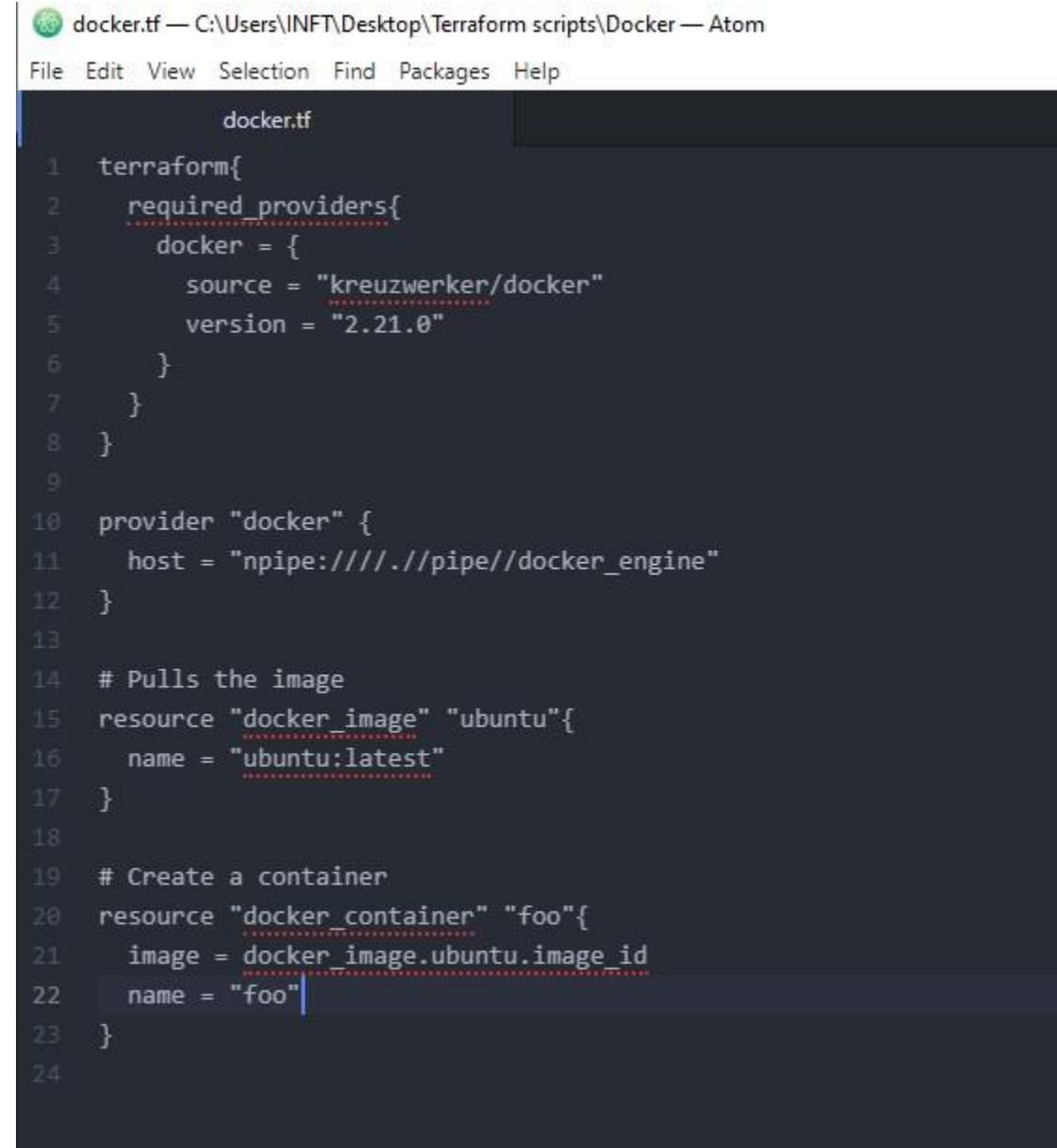
Step 4: Create a folder Terraform\_scripts and inside it create a folder named Docker.



## Step 5: Download Atom Editor.



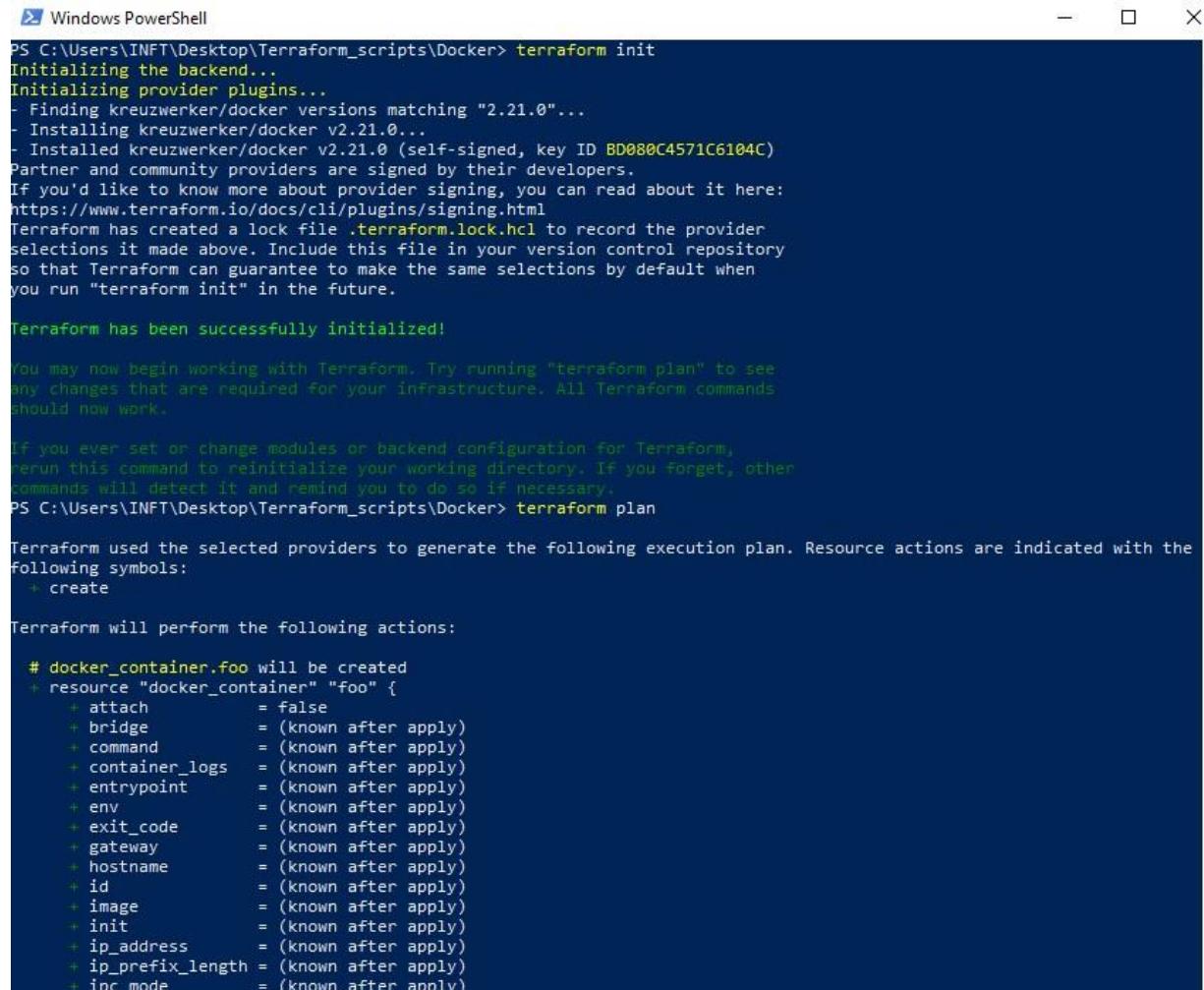
Step 6: Run the following script in the Atom Editor



The screenshot shows the Atom code editor interface with a dark theme. The title bar reads "docker.tf — C:\Users\INFT\Desktop\Terraform scripts\Docker — Atom". The menu bar includes File, Edit, View, Selection, Find, Packages, and Help. The main editor area displays a Terraform configuration file named "docker.tf". The code is as follows:

```
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 # Pulls the image  
15 resource "docker_image" "ubuntu"{  
16     name = "ubuntu:latest"  
17 }  
18  
19 # Create a container  
20 resource "docker_container" "foo"{  
21     image = docker_image.ubuntu.image_id  
22     name = "foo"  
23 }  
24
```

Step 7: Open Windows Explorer and run the following command terraform init, terraform plan, terraform apply, terraform destroy and docker images.



```
PS C:\Users\INFT\Desktop\Terraform_scripts\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\INFT\Desktop\Terraform_scripts\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.foo will be created
+ resource "docker_container" "foo" {
  + attach      = false
  + bridge      = (known after apply)
  + command     = (known after apply)
  + container_logs = (known after apply)
  + entrypoint   = (known after apply)
  + env         = (known after apply)
  + exit_code    = (known after apply)
  + gateway     = (known after apply)
  + hostname    = (known after apply)
  + id          = (known after apply)
  + image        = (known after apply)
  + init         = (known after apply)
  + ip_address   = (known after apply)
  + ip_prefix_length = (known after apply)
  + ipc_mode    = (known after apply)
```

```
Windows PowerShell
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\INFT\Desktop\Terraform_scripts\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.foo will be created
+ resource "docker_container" "foo" {
    + attach          = false
    + bridge          = (known after apply)
    + command         = (known after apply)
    + container_logs = (known after apply)
    + entrypoint      = (known after apply)
    + env             = (known after apply)
    + exit_code       = (known after apply)
    + gateway         = (known after apply)
    + hostname        = (known after apply)
    + id              = (known after apply)
    + image           = (known after apply)
    + init            = (known after apply)
    + ip_address      = (known after apply)
    + ip_prefix_length = (known after apply)
    + ipc_mode        = (known after apply)
    + log_driver      = (known after apply)
    + logs            = false
    + must_run        = true
    + name            = "foo"
    + network_data    = (known after apply)
    + read_only       = false
    + remove_volumes = true
    + restart         = "no"
    + rm              = false
    + runtime         = (known after apply)
    + 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.

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 11s [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c259&ubuntu:latest]
docker_container.foo: Creating...

Error: container exited immediately

with docker_container.foo,
on docker.tf line 20, in resource "docker_container" "foo":
20: resource "docker_container" "foo"{

PS C:\Users\INFT\Desktop\Terraform_scripts\Docker>
```

```
PS C:\Users\INFT\Desktop\Terraform_scripts\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:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598a" -> null
  image_id = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598a" -> null
  latest   = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598a" -> null
  name     = "ubuntu:latest" -> null
  repo_digest = "ubuntu@sha256:8a37d68f4f73ebf3d4efafbcf66379bf3728902a8038616808f04e34a9ab63ee" -> null
}

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

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

Enter a value: yes

docker_image.ubuntu: Destroying... [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]
docker_image.ubuntu: Destruction complete after 1s

Destroy complete! Resources: 1 destroyed.
PS C:\Users\INFT\Desktop\Terraform_scripts\Docker>
```

```
PS C:\Users\INFT\Desktop\Terraform_scripts\Docker> docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
PS C:\Users\INFT\Desktop\Terraform_scripts\Docker>
```

## Experiment No 7

### AIM: Installing SonarQube from the Docker Image

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

Sonarqube:latest

```
PS D:\Desktop\DockeFile> 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
44ba2882f8eb: Pull complete
2cabec57fa36: Pull complete
c20481384b6a: Pull complete
bf7b17ee74f8: Pull complete
38617faac714: Pull complete
b795b715553d: Pull complete
c5244f6c9231: Pull complete
Digest: sha256:1ffd122cfb37ce982289dc7f5d38bb702ba05af7b5a50f7cb077ae25e60b5b9a
Status: Downloaded newer image for sonarqube:latest
1442c4e613b25aaedec05c060f020a00802b1c6dbaa27e8c5c0dad4ed8fc1f76
```

The screenshot shows the Docker Hub 'Images' page. At the top, there are tabs for 'Local', 'Hub', 'Artifactory', and 'EARLY ACCESS'. Below the tabs, it says '715.97 MB / 0 Bytes in use 1 images'. A search bar is followed by a filter icon and a refresh icon. The main area shows a table with one row:

Name	Tag	Status	Created	Size	Actions
sonarqube bb91606199eb	latest	In use	17 days ago	715.97 MB	⋮

go to the SonarQube page by typing:

<http://localhost:9000/> on your browser.

**Installation is successful if you see this page**

The screenshot shows a web browser window with the address bar containing 'localhost:9000/sessions/new?return\_to=%2F'. The page title is 'Log in to SonarQube'. There are two input fields: one for 'admin' and one for a password (represented by asterisks). Below the fields are 'Log in' and 'Cancel' buttons.

## Update to new password

The screenshot shows the SonarQube interface for creating a new project. At the top, there's a navigation bar with links for Gmail, YouTube, Translate, and What's New in Dev... The main heading is "How do you want to create your project?". Below it, a note says: "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." A sub-note states: "First, you need to set up a DevOps platform configuration." There are four main import options: "Import from Azure DevOps" (Setup), "Import from Bitbucket Cloud" (Setup), "Import from Bitbucket Server" (Setup), "Import from GitHub" (Setup), and "Import from GitLab" (Setup). Below these, a link "Create project manually" is highlighted with a blue border.

## Create project manually: Here project name is “AdDevops”

This screenshot shows the first step of the manual project creation process. The title is "Create a local project". It asks for a "Project display name" (sonarqube-exp7) and a "Project key" (sonarqub-key-exp7). It also asks for a "Main branch name" (main). A note below says: "The name of your project's default branch [Learn More](#)". At the bottom are "Cancel" and "Next" buttons. A yellow warning box at the bottom left states: "⚠️ 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." The footer includes the message "SonarQube™ technology is powered by SonarSource SA", version information "Community Edition v18.6 (92116) ACTIVE", and links for "Community", "Documentation", "Plugins", and "Web API".

This screenshot shows the second step of the manual project creation process, titled "Set up project for Clean as You Code". It explains: "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](#)". It asks to "Choose the baseline for new code for this project". Three options are shown: 1. "Use the global setting" (radio button selected): "Previous version" (Any code that has changed since the previous version is considered new code. Recommended for projects following regular versions or releases). 2. "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), and "Reference branch" (Choose a branch as the baseline for the new code. Recommended for projects using feature branches). At the bottom are "Back" and "Create project" buttons.

## open Jenkins

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

### Plugins

The screenshot shows the Jenkins Plugin Manager interface. A search bar at the top contains the text "sonarqube". Below it, a table lists available plugins. The "SonarQube Scanner" plugin is highlighted with a checkmark in the "Install" column and is the first item in the list. The table has columns for "Install", "Name", and "Released". The "SonarQube Scanner" entry includes a brief description: "This plugin allows an easy integration of SonarQube, the open source platform for Continuous Inspection of code quality." At the bottom of the page, there are two buttons: "Install without restart" (highlighted in blue) and "Download now and install after restart".

### Download progress

#### Preparation

- Checking internet connectivity
- Checking update center connectivity
- Success

#### SSH server



#### Deploy to container



#### Loading plugin extensions



#### SonarQube Scanner



#### Loading plugin extensions



→ [Go back to the top page](#)

(you can start using the installed plugins right away)

→  Restart Jenkins when installation is complete and no jobs are running

## Under Jenkins ,

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

localhost:8080/manage/configure

Dashboard > Manage Jenkins > System >

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

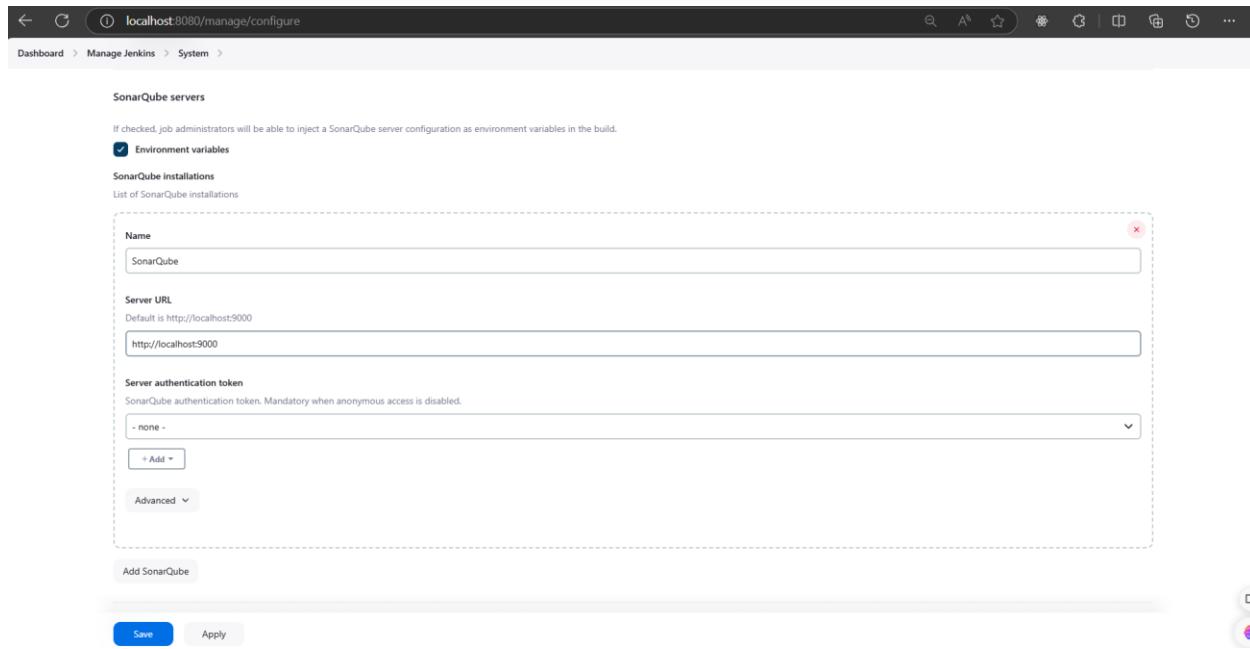
Server URL: Default is http://localhost:9000  
http://localhost:9000

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

Advanced ▾

Add SonarQube

Save Apply



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

**Choose the latest configuration and choose Install Automatically.**

localhost:8080/manage/configureTools/

Dashboard > Manage Jenkins > Tools

SonarQube Scanner installations

SonarQube Scanner installations ▾  Edited

Add SonarQube Scanner

SonarQube Scanner

Name: SonarQube

Install automatically ?

Install from Maven Central

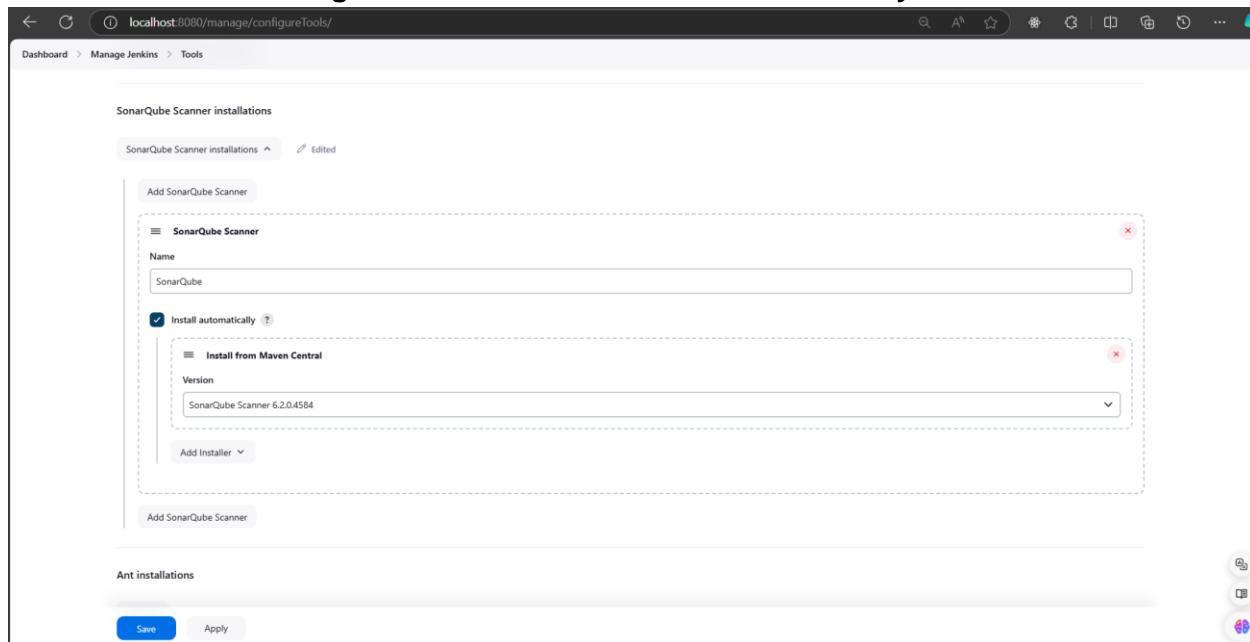
Version: SonarQube Scanner 6.2.0.4584

Add Installer ▾

Add SonarQube Scanner

Ant installations

Save Apply



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

The screenshot shows the Jenkins 'New Item' creation interface. At the top, there's a search bar with 'Search (CTRL+K)' and a user dropdown for 'Prathamesh Parmeshwar Patel'. Below the header, the URL is 'localhost:8080/view/all/newJob'. The main area is titled 'New Item' and has a sub-section 'Enter an item name' with the value 'adv DevOps exp-7'. A list of item types is shown: 'Freestyle project' (selected), 'Pipeline', 'Multi-configuration project', 'Folder', 'Multibranch Pipeline', and 'Organization Folder'. Each item type has a brief description. At the bottom right of the list are two buttons: 'OK' and 'Cancel'.

**Choose this GitHub repository in Source Code Management.**

[https://github.com/shazforiot/MSBuild\\_firstproject.git](https://github.com/shazforiot/MSBuild_firstproject.git)

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

sonar.projectKey=SonarQueue-key

sonar.login=admin

sonar.password=admin

sonar.hosturl=<http://localhost:9000/>

The screenshot shows the Jenkins 'Configuration' page for the 'adv DevOps exp-7' job. On the left, a sidebar lists configuration tabs: General (selected), Source Code Management, Build Triggers, Build Environment, Build Steps, and Post-build Actions. The 'General' tab contains a 'Description' field with the value 'adv DevOps exp - 7'. Below it are sections for 'Discard old builds' (unchecked) and 'GitHub project'. The 'GitHub project' section includes a 'Project url' field with the value 'https://github.com/shazforiot/MSBuild\_firstproject.git/'. There are also checkboxes for 'This project is parameterized', 'Throttle builds', and 'Execute concurrent builds if necessary'. The 'Advanced' section is collapsed. The 'Source Code Management' section at the bottom shows 'None' selected for Git, with a 'Repositories' field below it. At the very bottom are 'Save' and 'Apply' buttons.

Go to <http://localhost:9000/> and enter your previously created username.

**Go to Permissions and grant the Admin user Execute Permissions.**

Group	Administer System	Administrator	Execute Analysis	Create
sonar-administrators System administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
sonar-users Every authenticated user automatically belongs to this group	<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Anyone DEPRECATED Anybody who browses the application belongs to this group. If authentication is not enforced, assigned permissions also apply to non-authenticated users.	<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Administrator admin	<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

4 of 4 shown

**⚠️ 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.

**Build and Run:**

localhost:8080/job/adv%20DevOps%20exp-7/

# Jenkins

Dashboard > adv DevOps exp-7 >

Status: ✓ adv DevOps exp-7

Changes: adv DevOps exp - 7

Workspace

Build Now

Configure

Delete Project

GitHub

SonarQube

Rename

Permalinks

- Last build (#6), 1 hr 59 min ago
- Last stable build (#6), 1 hr 59 min ago
- Last successful build (#6), 1 hr 59 min ago
- Last failed build (#5), 2 hr 1 min ago
- Last unsuccessful build (#5), 2 hr 6 min ago
- Last completed build (#6), 1 hr 59 min ago

Build History

#	Date
#6	Sep 26, 2024, 12:08AM
#5	Sep 26, 2024, 12:00AM
#4	Sep 25, 2024, 11:37PM
#3	Sep 25, 2024, 11:37PM
#2	Sep 25, 2024, 11:36PM
#1	

localhost:8080/job/adv%20DevOps%20exp-7/6/

# Jenkins

Dashboard > adv DevOps exp-7 > #6

Status: ✓ #6 (Sep 26, 2024, 12:08:16 AM)

Changes

Console Output

Edit Build Information

Delete build '#6'

Timings

Git Build Data

Previous Build

Started by user Prathamesh parmeshwar palve

This run spent:

- 15 ms waiting;
- 27 sec build duration;
- 27 sec total from scheduled to completion.

Revision: f2bc042c04c6e72427c380bc4ee6d6fee7b49adf  
Repository: [https://github.com/shazforiot/MSBuild\\_firstproject.git](https://github.com/shazforiot/MSBuild_firstproject.git)  
refs/remotes/origin/master

</> No changes.

## Console Output:

localhost:8080/job/adv%20DevOps%20exp-7/6/console

## Jenkins

Dashboard > adv DevOps exp-7 > #6 > Console Output

**Console Output**

Status Changes Console Output Edit Build Information Delete build #6 Timings Git Build Data Previous Build

```

Started by user Prathamesh parmeshwar pale
Running as SYSTEM
Building in workspace C:\ProgramData\Jenkins\jenkins\workspace\SonarQube
The recommended git tool is: NONE
No credentials specified
> git.exe rev-parse --resolve-git-dir C:\ProgramData\Jenkins\jenkins\workspace\SonarQube\.git # timeout=10
Fetching changes from the remote git repository
> git.exe config remote.origin.url https://github.com/shazforiot/MSBuild_FirstProject.git # timeout=10
Fetching upstream changes from https://github.com/shazforiot/MSBuild_FirstProject.git
> git.exe -version # timeout=10
> git --version # git version 2.46.2.windows.1"
> git.exe fetch --tags --force --progress .. https://github.com/shazforiot/MSBuild_FirstProject.git +refs/heads/*:refs/remotes/origin/* # timeout=10
> git.exe rev-parse "refs/remotes/origin/master^{commit}" # timeout=10
Checking out Revision f2bc042c0d6e72427c300cae6d6fee7b49adf (refs/remotes/origin/master)
> git.exe config core.sparsecheckout # timeout=10
> git.exe checkout -f f2bc042c0d6e72427c300cae6d6fee7b49adf # timeout=10
Commit message: "updated"
> git.exe rev-list --no-walk f2bc042c0d6e72427c300cae6d6fee7b49adf # timeout=10
Injecting SonarQube environment variables using the configuration: SonarQube
[SonarQube] $ C:\ProgramData\Jenkins\jenkins\tools\hudson.plugins.sonar.SonarRunnerInstallation\SonarQube\bin\sonar-scanner.bat -Dsonar.host.url=http://localhost:9080 -Dsonar.projectKey=sonarqube -Dsonar.projectName=sonarqube-key -Dsonar.host.url=http://localhost:9080 -Dsonar.login=admin -Dsonar.password=$PaIve#08 -Dsonar.projectBaseDir=C:\ProgramData\Jenkins\jenkins\workspace\SonarQube
00:08:18.621 WARN Property 'sonar.host.url' with value 'https://localhost:9080' is overridden with value 'http://localhost:9080'
00:08:18.669 INFO Scanner configuration file: C:\ProgramData\Jenkins\jenkins\tools\hudson.plugins.sonar.SonarRunnerInstallation\SonarQube\bin..\conf\sonar-scanner.properties
00:08:18.672 INFO Project root configuration file: NONE
00:08:18.689 INFO SonarScanner CLI 6.2.0.4584
00:08:18.691 INFO Java 22.0.2 Oracle Corporation (64-bit)
00:08:18.696 INFO Windows 11 10.0 amd64
00:08:18.720 INFO User cache: C:\Windows\system2\config\systemprofile\sonar\cache
00:08:19.348 INFO JRE provisioning: os(windows), arch(amd64)
00:08:22.136 INFO Communicating with SonarQube Server 10.6.0.92116
00:08:22.802 INFO Starting SonarScanner Engine...
00:08:22.802 INFO Java 17.0.11 Eclipse Adoptium (64-bit)

```

localhost:8080/job/adv%20DevOps%20exp-7/6/console

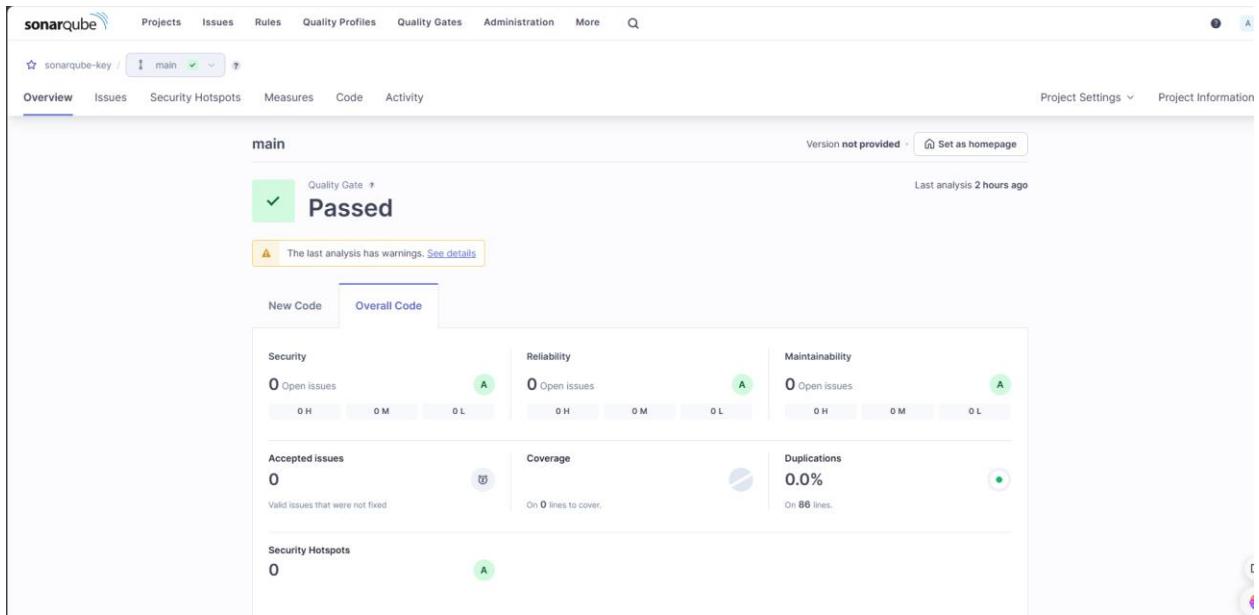
Dashboard > adv DevOps exp-7 > #6 > Console Output

```

00:08:42.039 INFO Using git CLI to retrieve untracked files
00:08:42.103 INFO Analyzing language associated files and files included via "sonar.text.inclusions" that are tracked by git
00:08:42.148 INFO 14 source files to be analyzed
00:08:42.322 INFO 14/14 source files have been analyzed
00:08:42.323 INFO Sensor TextAndSecretsSensor [text] (done) | time=91ms
00:08:42.329 INFO -----
00:08:42.417 INFO Sensor C# [csharp]
00:08:42.419 WARN Your project contains C# files which cannot be analyzed with the scanner you are using. To analyze C# or VB.NET, you must use the SonarScanner for .NET 5.x or higher, see https://reindet.sonarsource.com/doc/install-configure-scanner-msbuild.html
00:08:42.419 INFO Sensor C# [csharp] (done) | time=0ms
00:08:42.419 INFO Sensor Analysis Warnings Import [csharp]
00:08:42.419 INFO Sensor Analysis Warnings Import [csharp] (done) | time=0ms
00:08:42.419 INFO Sensor C# File Caching Sensor [csharp]
00:08:42.419 WARN Incremental PR analysis: Could not determine common base path, cache will not be computed. Consider setting 'sonar.projectBaseDir' property.
00:08:42.419 INFO Sensor C# File Caching Sensor [csharp] (done) | time=1ms
00:08:42.420 INFO Sensor Zero Coverage Sensor
00:08:42.427 INFO Sensor Zero Coverage Sensor (done) | time=8ms
00:08:42.429 INFO SCN Publisher SCM provider for this project is: git
00:08:42.430 INFO SCN Publisher 4 source files to be analyzed
00:08:42.455 INFO SCN Publisher 4/4 source files have been analyzed (done) | time=425ms
00:08:42.457 INFO CPD Executor Calculating CPD for 0 files
00:08:42.458 INFO CPD Executor CPD calculation finished (done) | time=0ms
00:08:42.463 INFO SCN revision ID 'f2bc042c0d6e72427c300cae6d6fee7b49adf'
00:08:43.105 INFO Analysis report generated in 99ms, dir size:199.9 kB
00:08:43.142 INFO Analysis report compressed in 24ms, zip size:22.3 kB
00:08:43.681 INFO Analysis report uploaded in 53ms
00:08:43.683 INFO ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9080/dashboard?id=sonarqube
00:08:43.684 INFO Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
00:08:43.684 INFO More about the report processing at http://localhost:9080/api/ce/taskId=5ba2c6da-d3cb-4ec3-9088-308ad22f8670
00:08:43.709 INFO Analysis total time: 17.889 s
00:08:43.703 INFO SonarScanner Engine completed successfully
00:08:43.778 INFO EXECUTION SUCCESS
00:08:43.782 INFO Total time: 25.150s
Finished: SUCCESS

```

Project on sonarqube:



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

## Experiment 8

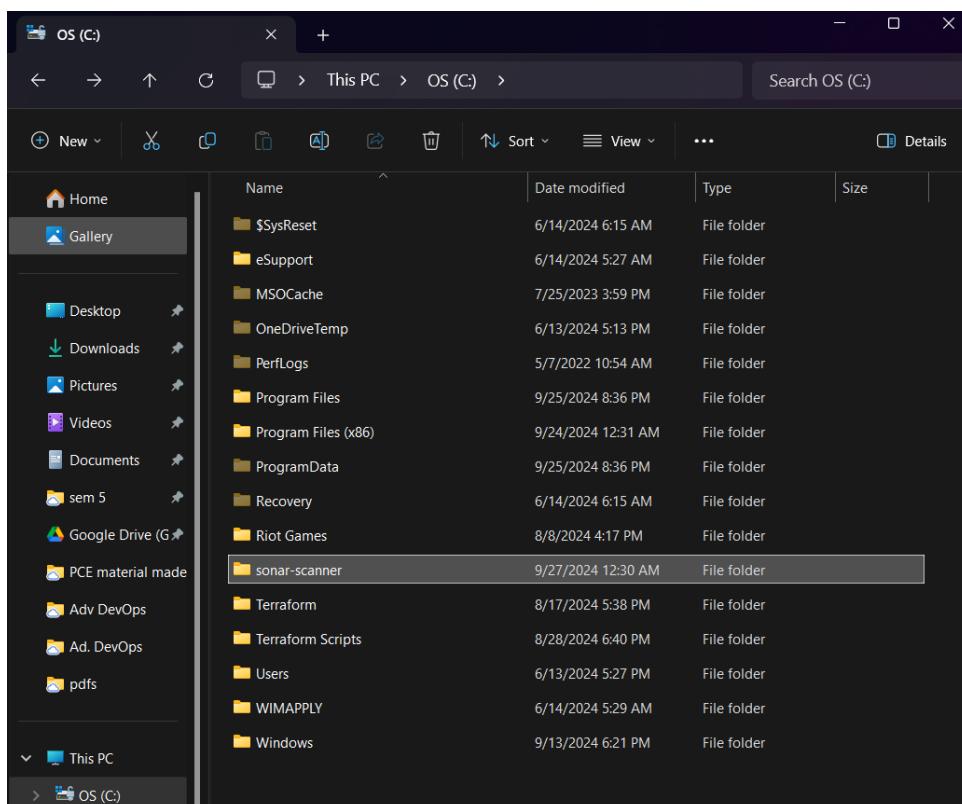
Aim: Create a Jenkins CICD Pipeline with SonarQube / GitLab Integration to perform a static analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web /Java / Python application.

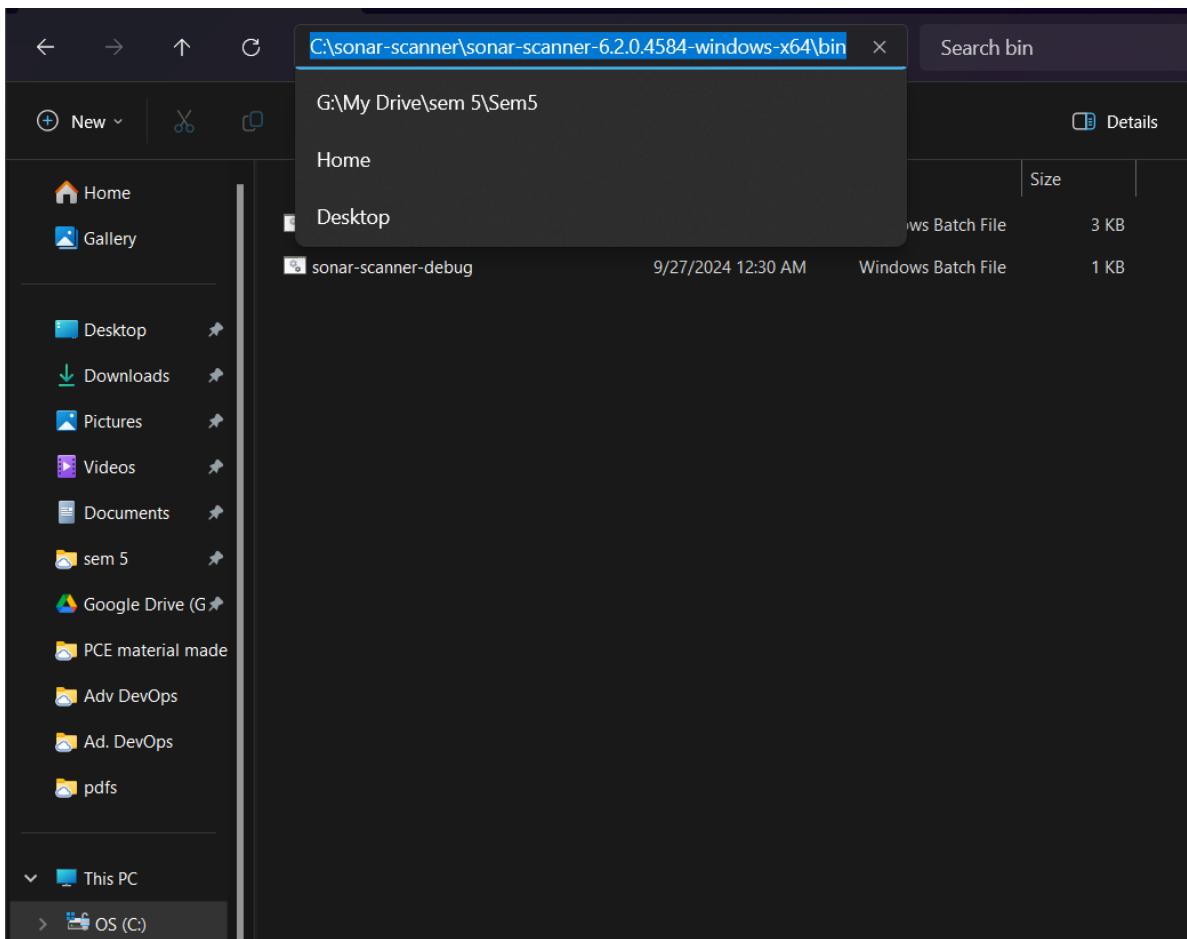
Step 1 : Visit the following link to download the SonarScanner CLI -

<https://docs.sonarsource.com/sonarqube/latest/analyzing-source-code/scanners/sonarscanner/> and then click on Windows x-64 to download the zip file.

The screenshot shows the SonarScanner CLI documentation page. The left sidebar contains navigation links for SonarQube, Docs 10.6, and various scanner-related topics like Server installation and setup, Analyzing source code, Scanners, and Analysis parameters. The main content area displays the SonarScanner CLI section, which includes a release note for version 6.2, a note about running on checked-out code, and a "Configuring your project" section. A "START FREE" button is visible in the top right corner.

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





Step 3: Open Command Prompt and run as administrator and run the following commands –

```
cd C:\sonar-scanner\sonar-scanner-6.2.0.4584-windows-x64\bin dir
```

```
sonar-scanner.bat
```

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

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

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

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

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

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

New Item

Enter an item name  
SonarQube Pipeline

Select an item type

**Pipeline** Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

**Freestyle project** Classic, general-purpose job type that checks out from up to one SCM, executes build steps serially, followed by post-build steps like archiving artifacts and sending email notifications.

**Multi-configuration project** Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.

**Folder** Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.

OK

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

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

Then click on the save button.

**Configure**

General

Advanced Project Options

Pipeline

**Definition**

Pipeline script

```

1+ node {
2+   stage('Cloning the Github Repo') {
3+     git 'https://github.com/shazfioriot/GOL.git'
4+   }
5+   stage('SonarQube analysis') {
6+     withSonarQubeEnv('sonarqube') {
7+       sh "D:\\sonar\\scanner\\sonar-scanner-6.2.0.4584-windows-x64\\bin\\sonar-scanner.bat" +
8+         "-DSonar.login=admin" +
9+         "-DSonar.password=d5P4lve@00" +
10+        "-DSonar.projectKey=sonarqube" +
11+        "-DSonar.exclusions=vendor/**,resources/**/*.*.java" +
12+        "-DSonar.host.url=http://192.168.1.40:9000"
13+     }
14+   }
15+ }
16+

```

 Use Groovy Sandbox ?

Pipeline Syntax

Save

Apply

REST API Jenkins 2.462.2

Step 6: Now, click on Build Now and the build is successful.

**Jenkins**

Dashboard > SonarQube Pipeline >

## SonarQube Pipeline

Status: ✓ Permalinks: [Add description](#)

[Changes](#) [Build Now](#) [Configure](#) [Delete Pipeline](#) [SonarQube](#) [Stages](#) [Rename](#) [Pipeline Syntax](#)

**Build History** trend ▾

- Last build (#8), 23 min ago
- Last stable build (#8), 23 min ago
- Last successful build (#8), 23 min ago
- Last failed build (#6), 1 hr 1 min ago
- Last unsuccessful build (#7), 31 min ago
- Last completed build (#8), 23 min ago

Build #8: Sep 27, 2024, 2:00 AM | Sep 27, 2024, 1:52 AM

**Jenkins**

Dashboard > SonarQube Pipeline > #8

## Console Output

Status: ✓ Changes: [Console Output](#) [Edit Build Information](#) [Delete build #8](#) [Timings](#) [Git Build Data](#) [Pipeline Overview](#) [Pipeline Console](#) [Replay](#) [Pipeline Steps](#) [Workspaces](#) [Previous Build](#)

Skipping 4,246 KB. [Full Log](#)

```

02:06:47.449 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 789. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 512. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 248. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 886. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 249. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 662. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 615. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 664. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 913. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 810. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 668. Keep only the first 100 references.
02:06:47.449 WARN Too many duplication references on file gameoflife-

```

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

The screenshot shows the SonarQube dashboard for the 'main' project. At the top, it displays '683k Lines of Code - Version not provided'. A prominent green 'Passed' badge indicates the analysis has passed. Below this, there's a message about not letting issues accumulate and a 'Take the Tour' button. The dashboard is divided into sections: 'New Code' and 'Overall Code'. Under 'New Code', it shows '0 New issues' and '0 Accepted issues'. Under 'Overall Code', it shows 'Coverage' at 0%, 'Duplications' at 0%, and 'Security Hotspots' at 0%. The last analysis was performed 25 minutes ago.

This screenshot shows the SonarQube dashboard with a more detailed view of the quality gate. It includes metrics for Security, Reliability, and Maintainability. Security has 0 open issues (0 H, 0 M, 0 L). Reliability has 68k open issues (0 H, 47k M, 21k L). Maintainability has 164k open issues (7 H, 143k M, 21k L). Other sections like Accepted issues, Coverage, Duplications, and Security Hotspots are also displayed with their respective counts and details. The last analysis was performed 26 minutes ago.

## Experiment No 9

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

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

The screenshot shows the AWS Management Console interface for the EC2 service. A success message at the top says "Successfully initiated starting of i-0c718840b8064ab08". Below it, the "Instances" table lists one instance: "nagios-host" (Instance ID: i-0c718840b8064ab08, Status: Running, Type: t2.micro, Subnet: us-east-1a, Public IP: ec2-3-88-22-82.compute.amazonaws.com). The table includes columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, Public IPv4 IP, and Elastic IP.

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

The screenshot shows the "Inbound rules" table for a security group. It lists seven rules allowing traffic from anywhere (0.0.0.0/0) on various ports and protocols. The rules include:
 

- HTTP (TCP port 80) - All ICMP - IPv6
- All ICMP - IPv6
- HTTPS (TCP port 443) - All
- All traffic (All) - All
- SSH (TCP port 22) - 0.0.0.0/0
- Custom TCP (TCP port 5666) - 0.0.0.0/0
- All ICMP - IPv4

### 3. SSH into Your EC2 instance or simply use EC2 Instance Connect from the browser.

```

ec2-user@ip-172-31-92-100: ~ + -
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

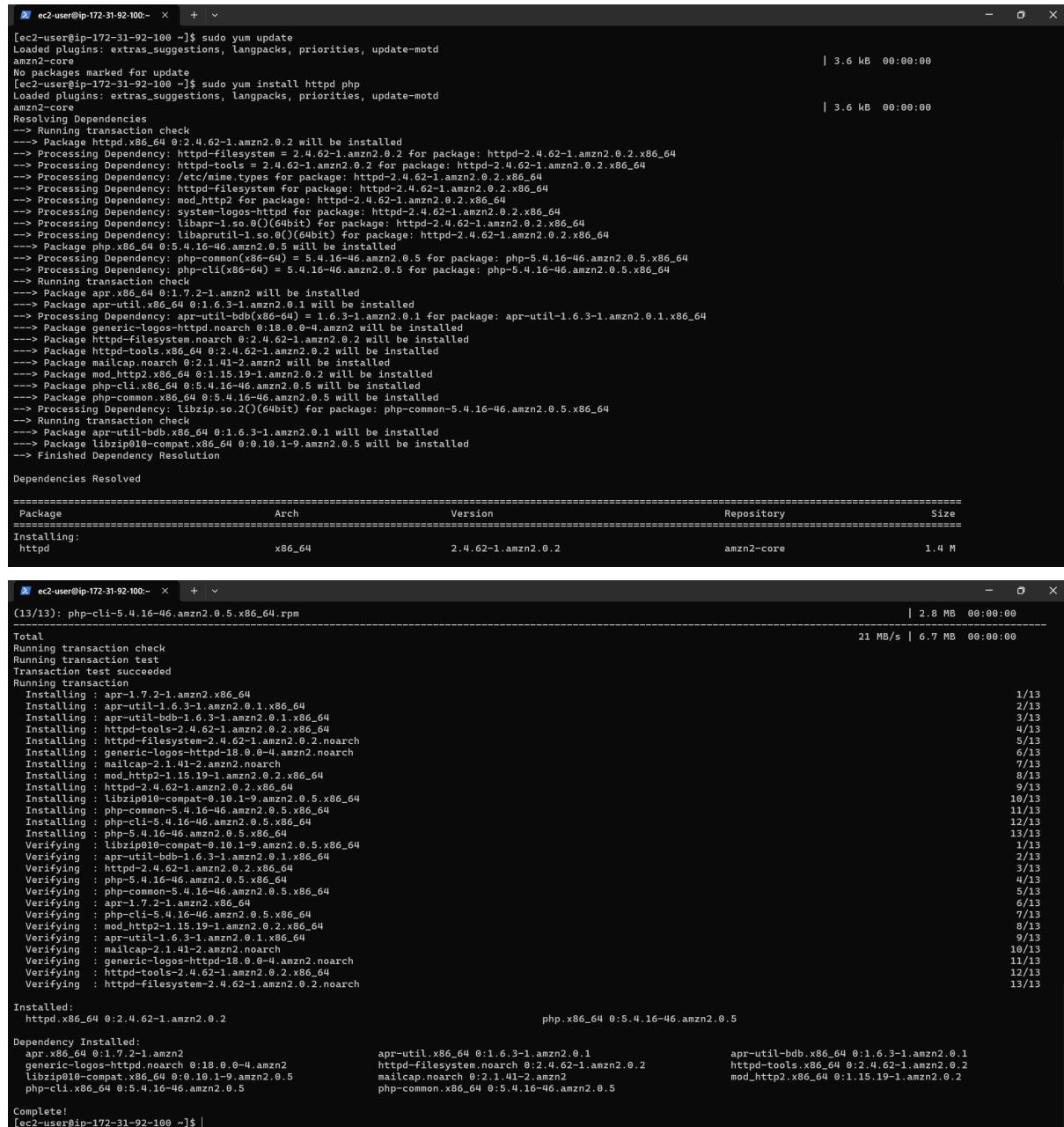
PS C:\Users\prath> cd .\Desktop\
PS C:\Users\prath\Desktop> cd '\adv DevOps temp\' 
PS C:\Users\prath\Desktop\adv DevOps temp> chmod 400 your-key-pair.pem
/usr/bin/chmod: cannot access 'your-key-pair.pem': No such file or directory
PS C:\Users\prath\Desktop\adv DevOps temp> chmod 400 exp-9.pem
PS C:\Users\prath\Desktop\adv DevOps temp> ssh -i "exp-9.pem" ec2-user@44.202.40.68
The authenticity of host '44.202.40.68 (44.202.40.68)' can't be established.
ED25519 key fingerprint is SHA256:rtnyRksavxfOalsjWpTk6bevj7n0U7Htvs3NhFA9/50.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '44.202.40.68' (ED25519) to the list of known hosts.

#_
~\_\####_      Amazon Linux 2
~~\_\#####\
~~\###|      AL2 End of Life is 2025-06-30.
~~\#/--->
~~\`~'-->
~~\`/          A newer version of Amazon Linux is available!
~~\`/`/        Amazon Linux 2023, GA and supported until 2028-03-15.
~/m/          https://aws.amazon.com/linux/amazon-linux-2023/
[ec2-user@ip-172-31-92-100 ~]$ |

```

#### 4. Update the package indices and install the following packages using yum

```
sudo yum update
sudo yum install httpd php
sudo yum install gcc glibc glibc-common
sudo yum install gd gd-devel
```



```
[ec2-user@ip-172-31-92-100: ~]$ sudo yum update
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
No packages marked for update
[ec2-user@ip-172-31-92-100: ~]$ sudo yum install httpd php
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
Resolving Dependencies
--> Package httpd.x86_64 0:2.4.62-1.amzn2.0.2 will be installed
--> Processing Dependency: httpd-filesystem = 2.4.62-1.amzn2.0.2 for package: httpd-2.4.62-1.amzn2.0.2.x86_64
--> Processing Dependency: httpd-tools = 2.4.62-1.amzn2.0.2 for package: httpd-2.4.62-1.amzn2.0.2.x86_64
--> Processing Dependency: /etc/mime.types for package: httpd-2.4.62-1.amzn2.0.2.x86_64
--> Processing Dependency: httpd-tools.x86_64 for package: httpd-2.4.62-1.amzn2.0.2.x86_64
--> Processing Dependency: system-devel-httdp for package: httpd-2.4.62-1.amzn2.0.2.x86_64
--> Processing Dependency: libapr-1.so.0((64bit)) for package: httpd-2.4.62-1.amzn2.0.2.x86_64
--> Processing Dependency: libaprutil-1.so.0((64bit)) for package: httpd-2.4.62-1.amzn2.0.2.x86_64
--> Package php.x86_64 0:5.4.16-46.amzn2.0.5 will be installed
--> Processing Dependency: php-common(x86-64) = 5.4.16-46.amzn2.0.5 for package: php-5.4.16-46.amzn2.0.5.x86_64
--> Processing Dependency: php-cli(x86-64) = 5.4.16-46.amzn2.0.5 for package: php-5.4.16-46.amzn2.0.5.x86_64
--> Running transaction check
--> Package apr.x86_64 0:1.7.2-1.amzn2 will be installed
--> Package apr-util.x86_64 0:1.6.3-1.amzn2.0.1 will be installed
--> Processing Dependency: apr-util-bdb(x86-64) = 1.6.3-1.amzn2.0.1 for package: apr-util-1.6.3-1.amzn2.0.1.x86_64
--> Package generic-logos-httdp.noarch 0:18.0.0-4.amzn2 will be installed
--> Package httpd-filesystem.noarch 0:2.4.62-1.amzn2.0.2 will be installed
--> Package httpd-tools.x86_64 0:2.4.62-1.amzn2.0.2 will be installed
--> Package mailcap.noarch 0:2.1.41-2.amzn2 will be installed
--> Package mod_http2.x86_64 0:1.15.19-1.amzn2.0.2 will be installed
--> Package php-common.x86_64 0:5.4.16-46.amzn2.0.5 will be installed
--> Processing Dependency: libzip.so.0((64bit)) for package: php-common-5.4.16-46.amzn2.0.5.x86_64
--> Running transaction check
--> Package apr-util-bdb.x86_64 0:1.6.3-1.amzn2.0.1 will be installed
--> Package libzip010-compat.x86_64 0:0.10.1-9.amzn2.0.5 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package           Arch      Version            Repository        Size
=====
Installing:     httpd      x86_64   2.4.62-1.amzn2.0.2      amzn2-core       1.4 M

=====
[ec2-user@ip-172-31-92-100: ~]$ (13/13): php-cli-5.4.16-46.amzn2.0.5.x86_64.rpm
Total                                         | 2.8 MB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : apr-1.7.2-1.amzn2.x86_64
  Installing : apr-util-1.6.3-1.amzn2.0.1.x86_64
  Installing : apr-util-bdb-1.6.3-1.amzn2.0.1.x86_64
  Installing : httpd-tools-2.4.62-1.amzn2.0.2.x86_64
  Installing : httpd-filesystem-2.4.62-1.amzn2.0.2.noarch
  Installing : generic-logos-httdp-18.0.0-4.amzn2.noarch
  Installing : mailcap-2.1.41-2.amzn2.noarch
  Installing : mod_http2-1.15.19-1.amzn2.0.2.x86_64
  Installing : httpd-2.4.62-1.amzn2.0.2.x86_64
  Installing : libzip010-compat-0.10.1-9.amzn2.0.5.x86_64
  Installing : php-common-5.4.16-46.amzn2.0.5.x86_64
  Installing : php-cli-5.4.16-46.amzn2.0.5.x86_64
  Installing : php-5.4.16-46.amzn2.0.5.x86_64
  Verifying  : libzip010-compat-0.10.1-9.amzn2.0.5.x86_64
  Verifying  : apr-util-bdb-1.6.3-1.amzn2.0.1.x86_64
  Verifying  : httpd-2.4.62-1.amzn2.0.2.x86_64
  Verifying  : libzip010-compat-0.10.1-9.amzn2.0.5.x86_64
  Verifying  : php-common-5.4.16-46.amzn2.0.5.x86_64
  Verifying  : php-5.4.16-46.amzn2.0.5.x86_64
  Verifying  : php-cli-5.4.16-46.amzn2.0.5.x86_64
  Verifying  : mod_http2-1.15.19-1.amzn2.0.2.x86_64
  Verifying  : apr-util-1.6.3-1.amzn2.0.1.x86_64
  Verifying  : mailcap-2.1.41-2.amzn2.noarch
  Verifying  : generic-logos-httdp-18.0.0-4.amzn2.noarch
  Verifying  : httpd-tools-2.4.62-1.amzn2.0.2.x86_64
  Verifying  : httpd-filesystem-2.4.62-1.amzn2.0.2.noarch

Installed:
  httpd.x86_64 0:2.4.62-1.amzn2.0.2

Dependency Installed:
  apr.x86_64 0:1.7.2-1.amzn2
  generic-logos-httdp.noarch 0:18.0.0-4.amzn2
  libzip010-compat.x86_64 0:0.10.1-9.amzn2.0.5
  php-cli.x86_64 0:5.4.16-46.amzn2.0.5

Complete!
[ec2-user@ip-172-31-92-100 ~]$
```

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

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

```
[ec2-user@ip-172-31-92-100 ~]$ sudo adduser -m nagios  
adduser: user 'nagios' already exists  
[ec2-user@ip-172-31-92-100 ~]$ sudo passwd nagios  
Changing password for user nagios.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[ec2-user@ip-172-31-92-100 ~]$ |
```

6. Create a new user group

```
sudo groupadd nagcmd
```

7. Use these commands so that you don't have to use sudo for Apache and Nagios

```
sudo usermod -a -G nagcmd nagios  
sudo usermod -a -G nagcmd apache
```

```
[ec2-user@ip-172-31-92-100 ~]$ sudo groupadd nagcmd  
[ec2-user@ip-172-31-92-100 ~]$ sudo usermod -a -G nagcmd nagios  
[ec2-user@ip-172-31-92-100 ~]$ sudo usermod -a -G nagcmd apache  
[ec2-user@ip-172-31-92-100 ~]$ mkdir ~/downloads
```

8. Create a new directory for Nagios downloads

```
mkdir ~/downloads  
cd ~/downloads
```

```
[ec2-user@ip-172-31-92-100 ~]$ mkdir ~/downloads  
[ec2-user@ip-172-31-92-100 ~]$ cd ~/downloads
```

9. Use wget to download the source zip files.

```
wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz  
gz  
wget http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz
```

```
[ec2-user@ip-172-31-92-100 downloads]$ wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz  
--2024-09-29 20:39:25-- http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz  
Resolving prdownloads.sourceforge.net (prdownloads.sourceforge.net)... 204.68.111.105  
Connecting to prdownloads.sourceforge.net (prdownloads.sourceforge.net)|204.68.111.105|:80... connected.  
HTTP request sent, awaiting response... 301 Moved Permanently  
Location: http://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz [following]
```

```
[ec2-user@ip-172-31-92-100 ~]$ sudo groupadd nagcmd
[ec2-user@ip-172-31-92-100 ~]$ sudo usermod -a -G nagcmd nagios
[ec2-user@ip-172-31-92-100 ~]$ sudo usermod -a -G nagcmd apache
[ec2-user@ip-172-31-92-100 ~]$ mkdir ~/downloads
[ec2-user@ip-172-31-92-100 ~]$ cd ~/downloads
[ec2-user@ip-172-31-92-100 downloads]$ wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz
--2024-09-29 20:39:25-- http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz
Resolving prdownloads.sourceforge.net (prdownloads.sourceforge.net)... 204.68.111.105
Connecting to prdownloads.sourceforge.net (prdownloads.sourceforge.net)|204.68.111.105|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://versaweb.dl.sourceforge.net/project/nagios/nagios-4/x/nagios-4.0.8/nagios-4.0.8.tar.gz [following]
--2024-09-29 20:39:25-- http://versaweb.dl.sourceforge.net/project/nagios/nagios-4/x/nagios-4.0.8/nagios-4.0.8.tar.gz?viafs=1
Resolving versaweb.dl.sourceforge.net (versaweb.dl.sourceforge.net)... 162.251.232.173
Connecting to versaweb.dl.sourceforge.net (versaweb.dl.sourceforge.net)|162.251.232.173|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1805059 (1.7M) [application/x-gzip]
Saving to: 'nagios-4.0.8.tar.gz'

100%[=====] 1,805,059  3.53MB/s  in 0.5s

2024-09-29 20:39:26 (3.53 MB/s) - 'nagios-4.0.8.tar.gz' saved [1805059/1805059]

[ec2-user@ip-172-31-92-100 downloads]$ wget http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz
--2024-09-29 20:39:26-- http://nagios-plugins.org/download/nagios-plugins-2.0.3.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|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2659772 (2.5M) [application/x-gzip]
Saving to: 'nagios-plugins-2.0.3.tar.gz'

100%[=====] 2,659,772  6.77MB/s  in 0.4s

2024-09-29 20:39:26 (6.77 MB/s) - 'nagios-plugins-2.0.3.tar.gz' saved [2659772/2659772]

[ec2-user@ip-172-31-92-100 downloads]$
```

## 10. Use tar to unzip and change to that directory.

`tar zxvf nagios-4.0.8.tar.gz`

```
[ec2-user@ip-172-31-92-100 downloads]$ tar zxvf nagios-4.0.8.tar.gz
nagios-4.0.8/
nagios-4.0.8/.gitignore
nagios-4.0.8/Changelog
nagios-4.0.8/INSTALLING
nagios-4.0.8/LEGAL
nagios-4.0.8/LICENSE
nagios-4.0.8/Makefile.in
nagios-4.0.8/README
nagios-4.0.8/README.asciidoc
nagios-4.0.8/THANKS
nagios-4.0.8/UPGRADING
nagios-4.0.8/base/
nagios-4.0.8/base/.gitignore
nagios-4.0.8/base/Makefile.in
nagios-4.0.8/base/broker.c
nagios-4.0.8/base/checks.c
```

## 11. Run the configuration script with the same group name you previously created.

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

```
[ec2-user@ip-172-31-92-100 downloads]$ cd nagios-4.0.8
[ec2-user@ip-172-31-92-100 nagios-4.0.8]$ ./configure --with-command-group=nagcmd
checking for a BSD-compatible install... /usr/bin/install -c
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
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 for strip... /usr/bin/strip
checking how to run the C preprocessor... gcc -E
```

## 12. Compile the source code.

make all

```
[ec2-user@ip-172-31-92-100 nagios-4.0.8]$ make all
cd ./base && make
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/base'
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nagios.o nagios.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o broker.o broker.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nebmods.o nebmods.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o ../common/shared.o ../common/shared.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nerd.o nerd.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o query-handler.o query-handler.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o workers.o workers.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o checks.o checks.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o config.o config.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o commands.o commands.c
commands.c: In function 'process_passive_service_check':
commands.c:2247:12: warning: assignment discards 'const' qualifier from pointer target type [-Wdiscarded-qualifiers]
    cr.source = command_worker.source_name;
           ^
commands.c: In function 'process_passive_host_check':
commands.c:2339:12: warning: assignment discards 'const' qualifier from pointer target type [-Wdiscarded-qualifiers]
    cr.source = command_worker.source_name;
           ^
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o events.o events.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o flapping.o flapping.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o logging.o logging.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o macros-base.o ../common/macros.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o netutils.o netutils.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o notifications.o notifications.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o sehandlers.o sehandlers.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o utils.o utils.c
utils.c: In function 'get_matching_timerange':
utils.c:1117:6: warning: assuming signed overflow does not occur when assuming that (X + c) >= X is always true [-Wstrict-overflow]
    if((midnight + 84800 >= start_time && (midnight <= end_time || start_time > end_time)) || (midnight <= end_time && start_time > end_time))
           ^
utils.c: In function 'process_check_result_queue':
utils.c:2038:38: warning: 'snprintf' output may be truncated before the last format character [-Wformat-truncation=]
    sprintf(file, sizeof(file), "%s/%s", dirname, dirfile->d_name);
           ^
utils.c:2038:3: note: 'sprintf' output 2 or more bytes (assuming 257) into a destination of size 256
    sprintf(file, sizeof(file), "%s/%s", dirname, dirfile->d_name);
           ^
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o retention-base.o sretention.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o xretention-base.o ../xdata/xrddefault.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o comments-base.o ../common/comments.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o xcomments-base.o ../xdata/xcddefault.c
```

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

sudo make install  
sudo make install-init  
sudo make install-config  
sudo make install-commandmode

```
[ec2-user@ip-172-31-92-100 nagios-4.0.8]$ sudo make install
cd ./base && make install
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/base'
make install-basic
make[2]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/base'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/bin
/usr/bin/install -c -m 774 -o nagios -g nagios nagios /usr/local/nagios/bin
/usr/bin/install -c -m 774 -o nagios -g nagios nagiosstats /usr/local/nagios/bin
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-4.0.8/base'
make strip-post-install
make[2]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/base'
/usr/bin/strip /usr/local/nagios/bin/nagios
/usr/bin/strip /usr/local/nagios/bin/nagiosstats
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-4.0.8/base'
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-4.0.8/base'
cd ./cgi && make install
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/cgi'
make install-basic
make[2]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/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 -m 775 -o nagios -g nagios $file /usr/local/nagios/sbin; \
done
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-4.0.8/cgi'
make strip-post-install
make[2]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/cgi'
for file in * cgi; do \  
done
```

\*\*\* Support Notes \*\*\*\*\*

If you have questions about configuring or running Nagios, please make sure that you:

- Look at the sample config files
- Read the documentation on the Nagios Library at:  
<http://library.nagios.com>

before you post a question to one of the mailing lists. Also make sure to include pertinent information that could help others help you. This might include:

- What version of Nagios you are using
- What version of the plugins you are using
- Relevant snippets from your config files
- Relevant error messages from the Nagios log file

For more information on obtaining support for Nagios, visit:

<http://support.nagios.com>

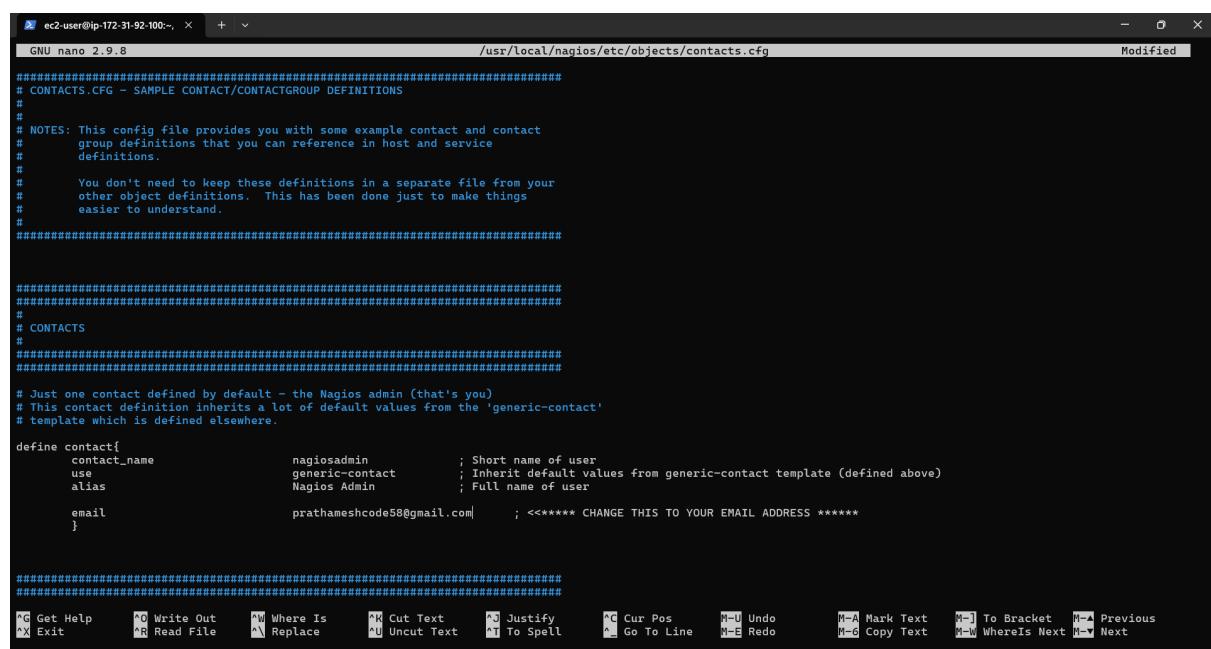
\*\*\*\*\*

Enjoy.

#### 14. Edit the config file and change the email address.

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

```
[ec2-user@ip-172-31-92-100 nagios-4.0.8]$ sudo nano /usr/local/nagios/etc/objects/contacts.cfg
```



```
GNU nano 2.9.8                               /usr/local/nagios/etc/objects/contacts.cfg                         Modified

#####
# 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                prathameshcode58@gmail.com; <***** CHANGE THIS TO YOUR EMAIL ADDRESS *****
}

#####
#G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo   M-A Mark Text   M-] To Bracket   M-^ Previous
^X Exit      ^R Read File   ^X Replace    ^U Uncut Text  ^I To Spell    ^A Go To Line  M-E Redo    M-G Copy Text   M-W WhereIs Next M-` Next
```

```
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                prathameshcode58@gmail.com; <***** CHANGE THIS TO YOUR EMAIL ADDRESS *****
}
```

15. Configure the web interface.

```
sudo make install-webconf
```

```
[ec2-user@ip-172-31-92-100 nagios-4.0.8]$ sudo make install-webconf  
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/httpd/conf.d/nagios.conf  
  
*** Nagios/Apache conf file installed ***
```

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

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

```
[ec2-user@ip-172-31-92-100 nagios-4.0.8]$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin  
New password:  
Re-type new password:  
Adding password for user nagiosadmin
```

17. Restart Apache

```
sudo service httpd restart
```

```
[ec2-user@ip-172-31-92-100 nagios-4.0.8]$ sudo service httpd restart  
Redirecting to /bin/systemctl restart httpd.service
```

19. Compile and install plugins

```
cd nagios-plugins-2.0.3
```

```
[ec2-user@ip-172-31-92-100 nagios-4.0.8]$ cd ~/downloads  
[ec2-user@ip-172-31-92-100 downloads]$ tar zxvf nagios-plugins-2.0.3.tar.gz  
nagios-plugins-2.0.3/  
nagios-plugins-2.0.3/perlmods/  
nagios-plugins-2.0.3/perlmods/Config-Tiny-2.14.tar.gz  
nagios-plugins-2.0.3/perlmods/parent-0.226.tar.gz  
nagios-plugins-2.0.3/perlmods/Test-Simple-0.98.tar.gz  
nagios-plugins-2.0.3/perlmods/Makefile.in  
nagios-plugins-2.0.3/perlmods/version-0.9903.tar.gz  
nagios-plugins-2.0.3/perlmods/Makefile.am  
nagios-plugins-2.0.3/perlmods/Module-Runtime-0.013.tar.gz  
nagios-plugins-2.0.3/perlmods/Module-Metadata-1.000014.tar.gz  
nagios-plugins-2.0.3/perlmods/Params-Validate-1.08.tar.gz  
nagios-plugins-2.0.3/perlmods/Class-Accessor-0.34.tar.gz  
nagios-plugins-2.0.3/perlmods/Try-Tiny-0.18.tar.gz  
nagios-plugins-2.0.3/perlmods/Module-Implementation-0.07.tar.gz  
nagios-plugins-2.0.3/perlmods/Makefile
```

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

```
make
```

```
sudo make install
```

```
[ec2-user@ip-172-31-92-100 downloads]$ cd nagios-plugins-2.0.3  
[ec2-user@ip-172-31-92-100 nagios-plugins-2.0.3]$ ./configure --with-nagios-user=nagios --with-nagios-group=nagios  
checking for a BSD-compatible install... /usr/bin/install -c  
checking whether build environment is sane... yes  
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p  
checking for gawk... gawk  
checking whether make sets $(MAKE)... yes  
checking whether to disable maintainer-specific portions of Makefiles... yes  
checking build system type... x86_64-unknown-linux-gnu  
checking host system type... x86_64-unknown-linux-gnu
```

## 20. Start Nagios

Add Nagios to the list of system services

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

```
[ec2-user@ip-172-31-92-100 nagios-plugins-2.0.3]$ sudo chkconfig --add nagios  
[ec2-user@ip-172-31-92-100 nagios-plugins-2.0.3]$ sudo chkconfig nagios on  
[ec2-user@ip-172-31-92-100 nagios-plugins-2.0.3]$ sudo service nagios start|
```

## Verify the sample configuration files

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

```
[ec2-user@ip-172-31-92-100 nagios-plugins-2.0.3]$ sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg  
  
Nagios Core 4.0.8  
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors  
Copyright (c) 1999-2009 Ethan Galstad  
Last Modified: 08-12-2014  
License: GPL  
  
Website: http://www.nagios.org  
Reading configuration data...  
  Read main config file okay...  
  Read object config files okay...  
  
Running pre-flight check on configuration data...  
  
Checking objects...  
  Checked 8 services.  
  Checked 1 hosts.  
  Checked 1 host groups.  
  Checked 0 service groups.  
  Checked 1 contacts.  
  Checked 1 contact groups.  
  Checked 24 commands.  
  Checked 5 time periods.  
  Checked 0 host escalations.  
  Checked 0 service escalations.  
Checking for circular paths...  
  Checked 1 hosts  
  Checked 0 service dependencies  
  Checked 0 host dependencies  
  Checked 5 timeperiods  
Checking global event handlers...  
Checking obsessive compulsive processor commands...  
Checking misc settings...  
  
Total Warnings: 0  
Total Errors: 0  
  
Things look okay - No serious problems were detected during the pre-flight check  
[ec2-user@ip-172-31-92-100 nagios-plugins-2.0.3]$ |
```

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

```
Total Warnings: 0  
Total Errors: 0  
  
Things look okay - No serious problems were detected during the pre-flight check  
[ec2-user@ip-172-31-92-100 nagios-plugins-2.0.3]$ |
```

```
sudo service nagios start
```

```
[ec2-user@ip-172-31-92-100 nagios-plugins-2.0.3]$ sudo service nagios start  
Starting nagios (via systemctl): [ OK ]
```

## 21. Check the status of Nagios

```
sudo systemctl status nagios
```

```
[ec2-user@ip-172-31-92-100 nagios-plugins-2.0.3]$ sudo systemctl status nagios
● nagios.service - LSB: Starts and stops the Nagios monitoring server
  Loaded: loaded (/etc/rc.d/init.d/nagios; bad; vendor preset: disabled)
  Active: active (running) since Sun 2024-09-29 21:06:29 UTC; 44min ago
    Docs: man:systemd-sysv-generator(8)
 Process: 22314 ExecStart=/etc/rc.d/init.d/nagios start (code=exited, status=0/SUCCESS)
 CGroup: /system.slice/nagios.service
         ├─22335 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
         ├─22337 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
         ├─22338 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
         ├─22339 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
         ├─22340 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
         └─22341 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

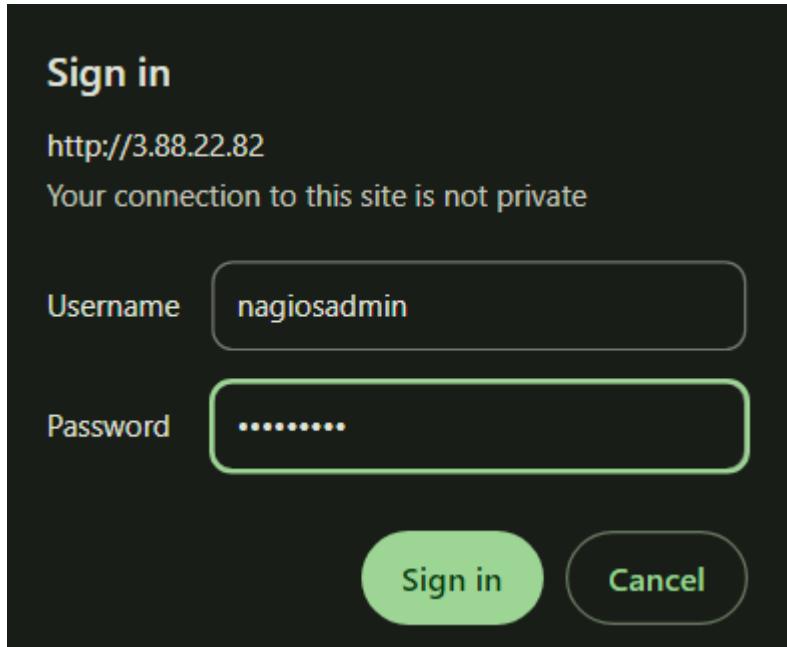
Sep 29 21:11:21 ip-172-31-92-100.ec2.internal nagios[22335]: SERVICE ALERT: localhost;HTTP;WARNING;HARD;4;HTTP WA...
Sep 29 21:11:51 ip-172-31-92-100.ec2.internal nagios[22335]: SERVICE ALERT: localhost;Swap Usage;CRITICAL;SOFT;2;...
Sep 29 21:12:51 ip-172-31-92-100.ec2.internal nagios[22335]: SERVICE ALERT: localhost;Swap Usage;CRITICAL;SOFT;3;...
Sep 29 21:13:51 ip-172-31-92-100.ec2.internal nagios[22335]: SERVICE ALERT: localhost;Swap Usage;CRITICAL;HARD;4;...
Sep 29 21:13:51 ip-172-31-92-100.ec2.internal nagios[22335]: SERVICE NOTIFICATION: nagiosadmin;localhost;Swap Us...
Sep 29 21:13:51 ip-172-31-92-100.ec2.internal nagios[22335]: wproc: NOTIFY job 6 from worker Core Worker 22340 is ...
Sep 29 21:13:51 ip-172-31-92-100.ec2.internal nagios[22335]: wproc: host=localhost; service=Swap Usage; contact...
Sep 29 21:13:51 ip-172-31-92-100.ec2.internal nagios[22335]: wproc: early_timeout=0; exited_ok=1; wait_status=3;...
Sep 29 21:13:51 ip-172-31-92-100.ec2.internal nagios[22335]: wproc: stderr line 01: /bin/sh: /bin/mail: No such ...
Sep 29 21:13:51 ip-172-31-92-100.ec2.internal nagios[22335]: wproc: stderr line 02: /usr/bin/printf: write error: ...
Hint: Some lines were ellipsized, use -l to show in full.
```

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

The screenshot shows the AWS EC2 Instances page. A specific instance, "i-0c718840b8064ab08 (nagios-host)", is selected. The instance summary table includes the following details:

Instance summary for i-0c718840b8064ab08 (nagios-host)		Actions	
Updated less than a minute ago		<a href="#">Connect</a>	Instance state ▾
Instance ID i-0c718840b8064ab08 (nagios-host)	Public IPv4 address 3.88.22.82   <a href="#">open address</a>	Private IPv4 addresses 172.31.92.100	
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-3-88-22-82.compute-1.amazonaws.com   <a href="#">open address</a>	
Hostname type IP name: ip-172-31-92-100.ec2.internal	Private IP DNS name (IPv4 only) ip-172-31-92-100.ec2.internal	Elastic IP addresses -	
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	AWS Compute Optimizer finding <a href="#">Opt-in to AWS Compute Optimizer for recommendation</a>	
Auto-assigned IP address 3.88.22.82 [Public IP]	VPC ID vpc-08d8d23aa994554c8		

23. Open up your browser and look for [http://<your\\_public\\_ip\\_address>/nagios](http://<your_public_ip_address>/nagios)



A screenshot of the Nagios Core dashboard. The top navigation bar shows 'Not secure | 3.88.22.82/nagios/'. The main header says 'Nagios® Core™ Version 4.0.8 August 12, 2014 Check for updates'. A blue banner at the top right says 'A new version of Nagios Core is available! Visit nagios.org to download Nagios 4.5.5'. The left sidebar has sections for General (Home, Documentation), Current Status (Tactical Overview, Map, Hosts, Services, Host Groups, Grid, Service Groups, Problems, Services, Reports), and System (Comments, Downtime, Process Info, Performance Info, Scheduling Queue, Configuration). The main content area includes 'Get Started' (with links to monitoring infrastructure, look-and-feel, addons, support, training, certification), 'Latest News' (with links to Nagios Plugins 2.0.2, GitHub, and Core 4.0.6), and 'Don't Miss...' (with links to Nagios World Conference 2014 registration and information). The bottom footer contains copyright and license information.

## Experiment No 10

Prerequisites: AWS Free Tier, Nagios Server running on Amazon Linux Machine.

```
PS C:\Users\prath\Desktop\adv DevOps temp> ssh -i "exp-9.pem" ec2-user@3.88.22.82
Last login: Sun Sep 29 20:48:36 2024 from 111.125.237.191
      _#
     ~\_ #####_          Amazon Linux 2
     ~~ \_\#####\_
     ~~   \###|          AL2 End of Life is 2025-06-30.
     ~~   \#/  __-
     ~~    V~' '-->
     ~~~   /          A newer version of Amazon Linux is available!
     ~~.. /          Amazon Linux 2023, GA and supported until 2028-03-15.
     _/_ /          https://aws.amazon.com/linux/amazon-linux-2023/
     _/m/'
```

1. To Confirm that Nagios is running on the server side, run this

```
sudo systemctl status nagios
on the "NAGIOS HOST".
```

```
[ec2-user@ip-172-31-92-100 ~]$ sudo systemctl status nagios
● nagios.service - LSB: Starts and stops the Nagios monitoring server
  Loaded: loaded (/etc/rc.d/init.d/nagios; bad; vendor preset: disabled)
  Active: active (running) since Sun 2024-09-29 21:06:29 UTC; 1h 5min ago
    Docs: man:systemd-sysv-generator(8)
 Process: 22314 ExecStart=/etc/rc.d/init.d/nagios start (code=exited, status=0/SUCCESS)
 CGroup: /system.slice/nagios.service
         └─22335 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─22337 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─22338 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─22339 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─22340 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─22341 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
```

2. Before we begin,

To monitor a Linux machine, create an Ubuntu 20.04 server EC2 Instance in AWS.

[EC2](#) > [Instances](#) > Launch an instance

## Launch an instance [Info](#)

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

**Name and tags [Info](#)**

Name  Add additional tags

**Application and OS Images (Amazon Machine Image) [Info](#)**

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Recents [Quick Start](#)

[Amazon Linux](#) [macOS](#) [Ubuntu](#) [Windows](#) [Red Hat](#) [SUSE LI](#) [Browse more AMIs](#) Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

**Summary**

Number of instances [Info](#)

**Software Image (AMI)**  
Canonical, Ubuntu, 24.04, amd6... [read more](#)  
ami-0e86e20dae9224db8

**Virtual server type (instance type)**  
t2.micro

**Firewall (security group)**  
New security group

**Storage (volumes)**  
1 volume(s) - 8 GiB

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

Provide it with the same security group as the Nagios Host and name it 'linux-client' alongside the host.

[EC2](#) > [Security Groups](#) > [sg-06deb7f2c1721e7f9 - launch-wizard-6](#) > Edit inbound rules

### Edit inbound rules [Info](#)

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

Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
sgr-087a61b54d2e7f783	HTTP	TCP	80	Custom	<input type="text" value="0.0.0.0/0"/> <a href="#">Delete</a>
sgr-0059f7887de571348	SSH	TCP	22	Custom	<input type="text" value="0.0.0.0/0"/> <a href="#">Delete</a>
sgr-011c932cb461bee7f	All ICMP - IPv4	ICMP	All	Custom	<input type="text" value="0.0.0.0/0"/> <a href="#">Delete</a>
sgr-008061b040cbfa8cd	HTTPS	TCP	443	Custom	<input type="text" value="0.0.0.0/0"/> <a href="#">Delete</a>

[Add rule](#)

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. [X](#)

[Cancel](#) [Preview changes](#) [Save rules](#)

**Instances (2) [Info](#)**

	Name <a href="#">Info</a>	Instance ID	Instance state <a href="#">Info</a>	Instance type <a href="#">Info</a>	Status check	Alarm status	Availability Zone <a href="#">Info</a>	Public IPv4 DNS	Public IPv4 ... <a href="#">Info</a>	Elastic IP
<input type="checkbox"/>	nagios-host	i-0c718840b8064ab08	<span style="color: green;">Running</span> <a href="#">View details</a> <a href="#">Logs</a>	t2.micro	<span style="color: green;">2/2 checks passed</span> <a href="#">View alarms</a> +	<span style="color: green;">OK</span>	us-east-1a	ec2-3-88-22-82.comput...	3.88.22.82	-
<input type="checkbox"/>	linux-client	i-0199595de1fa040d7	<span style="color: green;">Running</span> <a href="#">View details</a> <a href="#">Logs</a>	t2.micro	<span style="color: yellow;">Initializing</span> <a href="#">View alarms</a> +	<span style="color: yellow;">WARN</span>	us-east-1a	ec2-44-211-159-102.co...	44.211.159.102	-

### 3. On the server, run this command

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

```
[ec2-user@ip-172-31-92-100 ~]$ ps -ef | grep nagios
nagios  22335  1  0 21:06 ?    00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios  22337 22335  0 21:06 ?    00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios  22338 22335  0 21:06 ?    00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios  22339 22335  0 21:06 ?    00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios  22340 22335  0 21:06 ?    00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios  22341 22335  0 21:06 ?    00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
[ec2-user@ip-172-31-92-100 ~]$ ps -ef | grep --color=auto nagios
```

### 4. Become a root user and create 2 folders

```
sudo su
```

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

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

```
[ec2-user@ip-172-31-92-100 ~]$ sudo su
[root@ip-172-31-92-100 ec2-user]# mkdir /usr/local/nagios/etc/objects/monitorhosts
[root@ip-172-31-92-100 ec2-user]# mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
[root@ip-172-31-92-100 ec2-user]#
```

### 5. Copy the sample localhost.cfg file to linuxhost folder

```
cp
```

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

```
[ec2-user@ip-172-31-92-100 ~]$ sudo su
[root@ip-172-31-92-100 ec2-user]# mkdir /usr/local/nagios/etc/objects/monitorhosts
[root@ip-172-31-92-100 ec2-user]# mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
[root@ip-172-31-92-100 ec2-user]# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
[root@ip-172-31-92-100 ~]#
```

### 6. Open linuxserver.cfg using nano and make the following changes

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

Change the hostname to linuxserver (EVERYWHERE ON THE FILE)

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

```
# 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      44.211.159.102
}
```

Change hostgroup\_name under hostgroup to linux-servers1

```
# Define an optional hostgroup for Linux machines
define hostgroup{
    hostgroup_name  linux-servers1 ; The name of the hostgroup
    alias          Linux Servers ; Long name of the group
    members        linuxserver    ; Comma separated list of hosts that belong to this group
}
```

7. Open the Nagios Config file and add the following line

```
nano /usr/local/nagios/etc/nagios.cfg  
##Add this line  
cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/
```

GNU nano 2.9.8

/usr/local/nagios/etc/nagios..

```
# OBJECT CONFIGURATION FILE(S)  
# These are the object configuration files in which you define hosts,  
# host groups, contacts, contact groups, services, etc.  
# You can split your object definitions across several config files  
# if you wish (as shown below), or keep them all in a single config file.  
  
# You can specify individual object config files as shown below:  
cfg_file=/usr/local/nagios/etc/objects/commands.cfg  
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg  
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg  
cfg_file=/usr/local/nagios/etc/objects/templates.cfg  
  
# Definitions for monitoring the local (Linux) host  
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg  
cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/  
  
# 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
```

8. Verify the configuration files

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

```
Checking objects...  
    Checked 11 services.  
    Checked 2 hosts.  
    Checked 2 host groups.  
    Checked 0 service groups.  
    Checked 1 contacts.  
    Checked 1 contact groups.  
    Checked 24 commands.  
    Checked 5 time periods.  
    Checked 0 host escalations.  
    Checked 0 service escalations.  
Checking for circular paths...  
    Checked 2 hosts  
    Checked 0 service dependencies  
    Checked 0 host dependencies  
    Checked 5 timeperiods  
Checking global event handlers...  
Checking obsessive compulsive processor commands...  
Checking misc settings...  
  
Total Warnings: 0  
Total Errors: 0  
  
Things look okay - No serious problems were detected during the pre-flight check  
[root@ip-172-31-92-100 ec2-user]# |
```

## 9. Restart the nagios service

```
service nagios restart
```

```
[root@ip-172-31-92-100 ec2-user]# service nagios restart
Restarting nagios (via systemctl): [ OK ]
[root@ip-172-31-92-100 ec2-user]# |
```

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

```
PS C:\Users\prath\Desktop\adv DevOps temp> ssh -i "exp-10.pem" ubuntu@44.211.159.102
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1012-aws x86_64)

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

System information as of Sun Sep 29 22:50:12 UTC 2024

System load:  0.0          Processes:           104
Usage of /:   22.7% of 6.71GB  Users logged in:    0
Memory usage: 20%          IPv4 address for enX0: 172.31.93.79
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

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

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

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

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

ubuntu@ip-172-31-93-79:~$ |
```

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

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

```
Get:43 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe
Get:44 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe
Get:45 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe
Get:46 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe
Get:47 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted
Get:48 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted
Get:49 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse
Get:50 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse
Fetched 29.1 MB in 6s (5068 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
143 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
ubuntu@ip-172-31-93-79:~$ sudo apt install gcc nagios-nrpe-server nagios-plugins -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'monitoring-plugins' instead of 'nagios-plugins'
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu cpp cpp-13 cpp-13-x86-64-linux-gnu
  gcc-13 gcc-13-base gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu libaom3 libasan8 lib
  libc-bin libc-dev-bin libc-devtools libc6 libc6-dev libcc1-0 libcrypt-dev libctf-nob
```

12. Open nrpe.cfg file to make changes.

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

Under allowed\_hosts, add your nagios host IP address like so

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

# ALLOWED HOST ADDRESSES
# This is an optional comma-delimited list of IP address or hostnames
# that are allowed to talk to the NRPE daemon. Network addresses with a bit mask
# (i.e. 192.168.1.0/24) are also supported. Hostname wildcards are not currently
# supported.
#
# Note: The daemon only does rudimentary checking of the client's IP
# address. I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd
allowed_hosts=127.0.0.1,3.88.22.82
```

13. Restart the NRPE server

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

```
ubuntu@ip-172-31-93-79:~$ sudo systemctl restart nagios-nrpe-server|
```

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

The screenshot shows the Nagios Core 4.0.8 dashboard. At the top right, a green checkmark indicates "Daemon running with PID 31464". Below it, the version information "Nagios® Core™ Version 4.0.8" and the date "August 12, 2014" are displayed, along with a link to "Check for updates". A blue banner at the top center says "A new version of Nagios Core is available! Visit nagios.org to download Nagios 4.5.5". On the left sidebar, under "Current Status", "Tactical Overview" is selected. In the main content area, there are several boxes: "Get Started" (with bullet points like "Start monitoring your infrastructure"), "Quick Links" (with links to Nagios Library, Labs, Exchange, Support, and the project), "Latest News" (with bullet points about Nagios Plugins 2.0.2, Projects moved to GitHub, and Core 4.0.6), and "Don't Miss..." (with a link to the Nagios World Conference). At the bottom, a note states: "Copyright © 2010-2014 Nagios Core Development Team and Community Contributors. Copyright © 1999-2009 Ethan Galstad. See the THANKS file for more information on contributors." and "Nagios Core is licensed under the GNU General Public License and is provided AS IS with NO WARRANTY OF ANY KIND, INCLUDING THE WARRANTY OF DESIGN, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. Nagios, Nagios Core and the Nagios logo are registered trademarks of Ethan Galstad."

The screenshot shows the Nagios Core 4.0.8 dashboard with the "Tactical Overview" selected in the sidebar. In the main content area, there are three status summary boxes: "Current Network Status" (last updated Sep 29 23:12:55 UTC 2024, updated every 90 seconds, Nagios Core 4.0.8 - www.nagios.org), "Host Status Totals" (Up: 2, Down: 0, Unreachable: 0, Pending: 0), and "Service Status Totals" (Ok: 9, Warning: 1, Unknown: 0, Critical: 1, Pending: 0). Below these is a table titled "Host Status Details For All Host Groups". The table has columns: Host, Status, Last Check, Duration, and Status Information. It shows two hosts: "linuxserver" (UP, last checked 09-29-2024 23:12:39, duration 0d 0h 0m 12s, status PING OK - Packet loss = 0%, RTA = 1.03 ms) and "localhost" (UP, last checked 09-29-2024 23:11:20, duration 0d 2h 5m 49s, status PING OK - Packet loss = 0%, RTA = 0.03 ms). A note below the table says "Results 1 - 2 of 2 Matching Hosts".

## 15. Click on linuxserver to see the host details

**Host Information**

Last Updated: Sun Sep 29 23:13:18 UTC 2024  
Updated every 90 seconds  
Nagios® Core™ 4.0.8 - www.nagios.org  
Logged in as **nagiosadmin**

**Host**  
**linuxserver**  
(**linuxserver**)

**Member of**  
**linux-servers1**

**View Status Detail For This Host**  
**View Alert History For This Host**  
**View Trends For This Host**  
**View Alert Histogram For This Host**  
**View Availability Report For This Host**  
**View Notifications For This Host**

**IP Address:** 44.211.159.102

**Host State Information**

<b>Host Status:</b>	<b>UP</b> (for 0d 0h 0m 35s)
<b>Status Information:</b>	PING OK - Packet loss = 0%, RTA = 1.03 ms
<b>Performance Data:</b>	rta=1.031000ms;3000.000000;5000.000000;0.000000 pl=%;80;100;0
<b>Current Attempt:</b>	1/10 (HARD state)
<b>Last Check Time:</b>	09-29-2024 23:12:39
<b>Check Type:</b>	ACTIVE
<b>Check Latency / Duration:</b>	0.000 / 0.021 seconds
<b>Next Scheduled Active Check:</b>	09-29-2024 23:17:43
<b>Last State Change:</b>	09-29-2024 23:12:43
<b>Last Notification:</b>	N/A (notification 0)
<b>Is This Host Flapping?</b>	<b>NO</b> (5.25% state change)
<b>In Scheduled Downtime?</b>	<b>NO</b>
<b>Last Update:</b>	09-29-2024 23:13:17 ( 0d 0h 0m 1s ago)

**Active Checks:** **ENABLED**  
**Passive Checks:** **ENABLED**  
**Obsessing:** **ENABLED**  
**Notifications:** **ENABLED**  
**Event Handler:** **ENABLED**  
**Flap Detection:** **ENABLED**

**Host Commands**

- Locate host on map
- Disable active checks of this host
- Re-schedule the next check of this host
- Submit passive check result for this host
- Stop accepting passive checks for this host
- Stop obsessing over this host
- Disable notifications for this host
- Send custom host notification
- Schedule downtime for this host
- Schedule downtime for all services on this host
- Disable notifications for all services on this host
- Enable notifications for all services on this host
- Schedule a check of all services on this host
- Disable checks of all services on this host
- Enable checks of all services on this host
- Disable event handler for this host
- Disable flap detection for this host

**Host Comments**

Add a new comment | Delete all comments

**Current Network Status**

Last Updated: Sun Sep 29 23:13:34 UTC 2024  
Updated every 90 seconds  
Nagios® Core™ 4.0.8 - www.nagios.org  
Logged in as **nagiosadmin**

**Host Status Totals**

Up	2
Down	0
Unreachable	0
Pending	0

All Problems All Types

**Service Status Totals**

Ok	9
Warning	1
Unknown	0
Critical	1
Pending	0

All Problems All Types

**Service Status Details For All Hosts**

Host	Service	Status	Last Check	Duration	Attempt	Status Information
linuxserver	Current Users	OK	09-29-2024 23:12:39	0d 0h 25m 55s	1/4	USERS OK - 2 users currently logged in
	SSH	OK	09-29-2024 23:08:34	0d 0h 25m 0s	1/4	SSH OK - OpenSSH_9_6p1 Ubuntu-3ubuntu13.4 (protocol 2.0)
	Total Processes	OK	09-29-2024 23:09:22	0d 0h 24m 6s	1/4	PROCS OK - 31 processes with STATE = RSZDT
localhost	Current Load	OK	09-29-2024 23:12:05	0d 2h 6m 28s	1/4	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	09-29-2024 23:12:43	0d 2h 5m 50s	1/4	USERS OK - 2 users currently logged in
	HTTP	WARNING	09-29-2024 23:11:20	0d 2h 5m 13s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 3932 bytes in 0.000 second response time
	PING	OK	09-29-2024 23:08:58	0d 2h 4m 35s	1/4	PING OK - Packet loss = 0%, RTA = 0.03 ms
	Root Partition	OK	09-29-2024 23:09:35	0d 2h 3m 58s	1/4	DISK OK - free space: 6101 MB (74% inode=98%)
	SSH	OK	09-29-2024 23:10:13	0d 2h 3m 20s	1/4	SSH OK - OpenSSH_7.4 (protocol 2.0)
	Swap Usage	CRITICAL	09-29-2024 23:08:50	0d 2h 2m 43s	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	09-29-2024 23:11:28	0d 2h 2m 5s	1/4	PROCS OK - 31 processes with STATE = RSZDT

Results 1 - 11 of 11 Matching Services

## Experiment No 11

Prathamesh Palve  
D15A 32

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

### Steps to create an AWS Lambda function

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

The screenshot shows the AWS Lambda Functions page. At the top, there is a breadcrumb navigation: Lambda > Functions. Below the breadcrumb, there is a search bar labeled "Filter by tags and attributes or search by keyword". To the right of the search bar are buttons for "Last fetched now", "Actions", and a prominent orange "Create function" button. Below the search bar is a table header with columns: "Function name", "Description", "Package type", "Runtime", and "Last modified". A message "There is no data to display." is centered below the table. At the bottom of the page, there are links for "CloudShell", "Feedback", and copyright information: "© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences".

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

Lambda > Functions > Create function

### Create function Info

AWS Serverless Application Repository applications have moved to [Create application](#).

Author from scratch  
Start with a simple Hello World example.

Use a blueprint  
Build a Lambda application from sample code and configuration presets for common use cases.

Container image  
Select a container image to deploy for your function.

#### Basic information

Function name  
Enter a name that describes the purpose of your function.  
`myFunctionName`

Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info  
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.  
`Node.js 18.x`

Architecture Info  
Choose the instruction set architecture you want for your function code.  
 x86\_64

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Lambda > Functions > Create function Info

AWS Serverless Application Repository applications have moved to [Create application](#).

Author from scratch  
Start with a simple Hello World example.

Use a blueprint  
Build a Lambda application from sample code and configuration presets for common use cases.

Container image  
Select a container image to deploy for your function.

#### Basic information

Function name  
Enter a name that describes the purpose of your function.  
`myPythonLambdaFunction`

Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info  
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.  
`Python 3.11`

Architecture Info  
Choose the instruction set architecture you want for your function code.  
 x86\_64

arm64

#### Permissions Info

By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

https://ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/create/app... © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Lambda > Functions > Create function

### Create function Info

AWS Serverless Application Repository applications have moved to [Create application](#).

Author from scratch  
Start with a simple Hello World example.

Use a blueprint  
Build a Lambda application from sample code and configuration presets for common use cases.

Container image  
Select a container image to deploy for your function.

#### Basic information

Function name  
Enter a name that describes the purpose of your function.  
`myPythonLambdaFunction`

Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info  
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.  
`Python 3.11`

Architecture Info  
Choose the instruction set architecture you want for your function code.  
 x86\_64

arm64

#### Permissions Info

By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

Change default execution role

Advanced settings

Create function Cancel

Click on the Create button.

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

The screenshot shows the AWS Lambda Function Overview page for a function named "myPythonLambdaFunction". At the top, a green banner indicates "Successfully created the function myPythonLambdaFunction. You can now change its code and configuration. To invoke your function with a test event, choose "Test". The main interface includes tabs for "Code", "Test", "Monitor", "Configuration", "Aliases", and "Versions". Under the "Code" tab, there is a code editor window titled "lambda\_function" showing the following Python code:

```
1 import json
2
3 def lambda_handler(event, context):
4     # TODO Implement
5     return {
6         'statusCode': 200,
7         'body': json.dumps('Hello from Lambda!')
8     }
```

This screenshot shows the same Lambda function overview page after changes have been made. The code editor window now displays the following updated Python code:

```
1 import json
2
3 def lambda_handler(event, context):
4     # TODO Implement
5     return {
6         'statusCode': 200,
7         'body': json.dumps('Hello from Lambda!')
8     }
```

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

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

Successfully created the function `myPythonLambdaFunction`. You can now change its code and configuration. To invoke your function with a test event, choose "Test".

<b>General configuration</b>	<b>General configuration</b> <small>Info</small>	<small>Edit</small>
Triggers	Description -	Memory 128 MB
Permissions	Timeout 0 min 3 sec	Ephemeral storage 512 MB
Destinations	SnapStart <small>Info</small> None	
Function URL		
Environment variables		
Tags		
VPC		
Monitoring and operations tools		
Concurrency		
Asynchronous invocation		
Code signing		
Database proxies		
File systems		
State machines		

cloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

**Services**  [Alt+S]

Lambda > Functions > [myPythonLambdaFunction](#) > Edit basic settings

## Edit basic settings

<b>Basic settings</b> <small>Info</small>
Description – optional
<input type="text"/>
<b>Memory</b> <small>Info</small>
Your function is allocated CPU proportional to the memory configured.
<input type="text" value="128"/> MB
Set memory to between 128 MB and 10240 MB
<b>Ephemeral storage</b> <small>Info</small>
You can configure up to 10 GB of ephemeral storage (/tmp) for your function. <a href="#">View pricing</a>
<input type="text" value="512"/> MB
Set ephemeral storage (/tmp) to between 512 MB and 10240 MB.
<b>SnapStart</b> <small>Info</small>
Reduce startup time by having Lambda cache a snapshot of your function after the function has initialized. To evaluate whether your function code is resilient to snapshot operations, review the <a href="#">SnapStart compatibility considerations</a> .
<input type="text" value="None"/>
Supported runtimes: Java 11, Java 17.
<b>Timeout</b>
<input type="text" value="0"/> min <input type="text" value="1"/> sec
<b>Execution role</b>

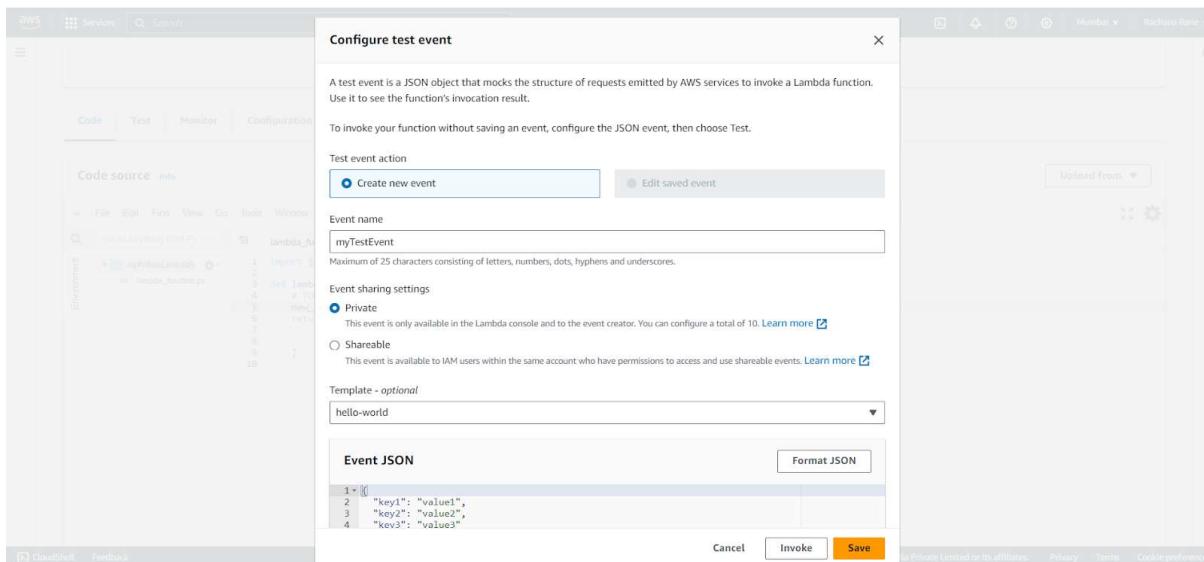
5. You can make changes to your function inside the code editor. You can also upload a zip file of your function or upload one from an S3 bucket if needed.  
Press Ctrl + S to save the file and click Deploy to deploy the changes.

The screenshot shows the AWS Lambda function editor. The top navigation bar includes tabs for Code, Test, Monitor, Configuration, Aliases, and Versions. The Code tab is selected. Below the tabs is a toolbar with File, Edit, Find, View, Go, Tools, Window, Test (with a dropdown arrow), Deploy, and a status message 'Changes not deployed'. To the right of the toolbar is an 'Upload from' button and a gear icon. The main area is titled 'Code source' with an 'Info' link. It contains a code editor with Python code for a lambda function:

```
1 import json
2
3 def lambda_handler(event, context):
4     # TODO implement
5     new_string="Hello! how are you?"
6     return {
7         'statusCode': 200,
8         'body': json.dumps('Hello from Lambda!')
9     }
10
```

On the left, there's an 'Environment' sidebar with a 'myPythonLambdaEnv' environment listed, containing a 'lambda\_function.py' file. At the bottom of the editor are CloudShell and Feedback links.

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



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

The screenshot displays two side-by-side views of the AWS Lambda console. The top view shows the 'Execution result' tab for a test event named 'myTestEvent'. The response body is a JSON object with 'statusCode' 200 and 'body' '\"Hello from Lambda!\"'. The bottom view shows the 'Code source' tab, which includes the 'Execution result' tab. Both tabs show the same successful execution details: Status Succeeded, Max memory used: 40 MB, Time: 1.66 ms.

**Execution result**

Test Event Name  
myTestEvent

Response

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

Function Logs

```
START RequestId: 7d26f404-f1da-4435-9faf-8dbb2a2733cc Version: $LATEST
END RequestId: 7d26f404-f1da-4435-9faf-8dbb2a2733cc
REPORT RequestId: 7d26f404-f1da-4435-9faf-8dbb2a2733cc Duration: 1.66 ms Billed Duration: 2 ms Memory Size: 128 MB Max Memory Used: 40 MB Init Duration: 110.05 ms
RequestID
7d26f404-f1da-4435-9faf-8dbb2a2733cc
```

**Code properties** Info

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

**Execution result**

Test Event Name  
myTestEvent

Response

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

Function Logs

```
START RequestId: 7d26f404-f1da-4435-9faf-8dbb2a2733cc Version: $LATEST
END RequestId: 7d26f404-f1da-4435-9faf-8dbb2a2733cc
REPORT RequestId: 7d26f404-f1da-4435-9faf-8dbb2a2733cc Duration: 1.66 ms Billed Duration: 2 ms Memory Size: 128 MB Max Memory Used: 40 MB Init Duration: 110.05 ms
RequestID
7d26f404-f1da-4435-9faf-8dbb2a2733cc
```

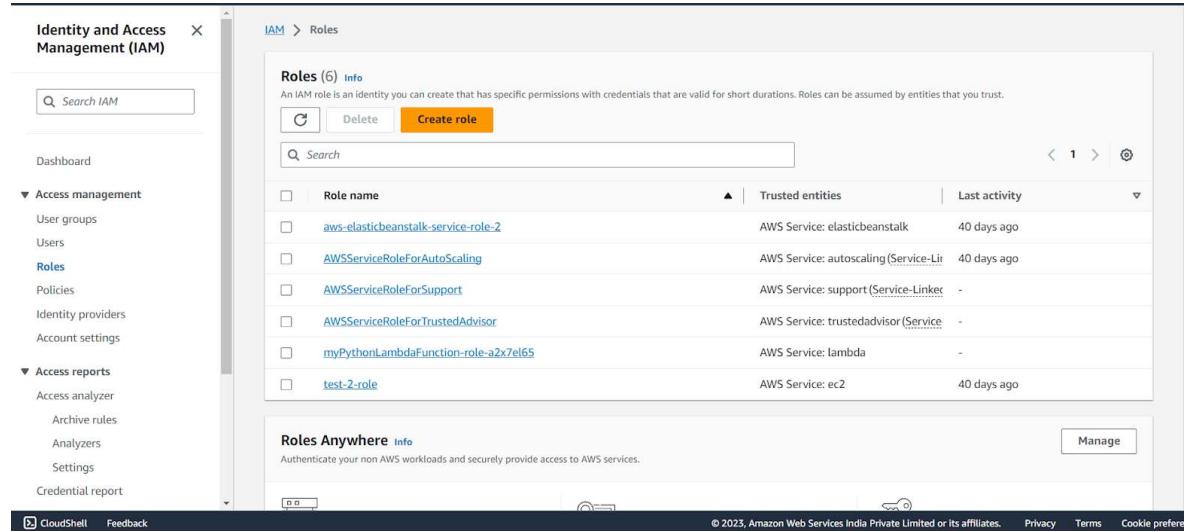
CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

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

## Experiment No 12

Prathamesh Palve  
D15A 32

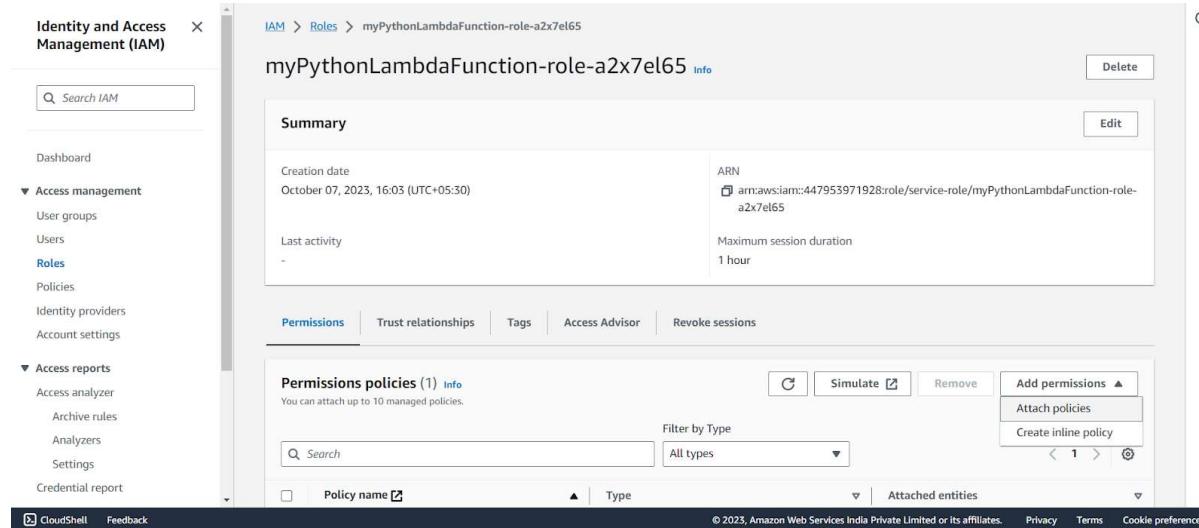
Step 1: Open up the IAM Console and under Roles, choose the Role we previously created for the Python Lambda Function (You can find your role name configuration of your Lambda function).



The screenshot shows the AWS IAM Roles page. On the left, there's a sidebar with navigation links like Dashboard, Access management, and Roles. The main area displays a table of roles with columns for Role name, Trusted entities, and Last activity. One role, "myPythonLambdaFunction-role-a2x7el65", is highlighted in blue.

Role name	Trusted entities	Last activity
aws-elasticbeanstalk-service-role-2	AWS Service: elasticbeanstalk	40 days ago
AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Li...	40 days ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linker...	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service...	-
myPythonLambdaFunction-role-a2x7el65	AWS Service: Lambda	-
test-2-role	AWS Service: ec2	40 days ago

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



The screenshot shows the detailed view of the "myPythonLambdaFunction-role-a2x7el65" role. It includes a Summary section with creation date and ARN, and a Permissions tab where a policy named "S3-ReadOnly" is attached. A context menu is open over the "Add permissions" button, showing options like "Attach policies" and "Create inline policy".

S3-ReadOnly

IAM > Roles > myPythonLambdaFunction-role-a2x7el65 > Add permissions

Attach policy to myPythonLambdaFunction-role-a2x7el65

▶ Current permissions policies (1)

Other permissions policies (882)

Filter by Type: All types, 1 match

Policy name	Type	Description
<input type="checkbox"/> <a href="#">AmazonS3ReadOnlyAccess</a>	AWS managed	Provides read only access to all bucket...

[Cancel](#) [Add permissions](#)

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

## CloudWatchFull

IAM > Roles > myPythonLambdaFunction-role-a2x7el65 > Add permissions

Attach policy to myPythonLambdaFunction-role-a2x7el65

▶ Current permissions policies (2)

Other permissions policies (881)

Filter by Type: All types, 2 matches

Policy name	Type	Description
<input type="checkbox"/> <a href="#">CloudWatchFullAccess</a>	AWS managed	Provides full access to CloudWatch.
<input type="checkbox"/> <a href="#">CloudWatchFullAccessV2</a>	AWS managed	Provides full access to CloudWatch.

[Cancel](#) [Add permissions](#)

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

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

Identity and Access Management (IAM)

Search IAM

Last activity: - Maximum session duration: 1 hour

Permissions Trust relationships Tags Access Advisor Revoke sessions

Policy was successfully attached to role.

Permissions policies (3) Info You can attach up to 10 managed policies.

Filter by Type: All types

Policy name	Type	Attached entities
<input type="checkbox"/> <a href="#">AmazonS3ReadOnlyAccess</a>	AWS managed	1
<input type="checkbox"/> <a href="#">AWSLambdaBasicExecutionRole-c4946a...</a>	Customer managed	1
<input type="checkbox"/> <a href="#">CloudWatchFullAccess</a>	AWS managed	1

▶ Permissions boundary (not set)

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

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

Lambda > Functions > Create function

Create function [Info](#)  
AWS Serverless Application Repository applications have moved to [Create application](#).

Author from scratch  
Start with a simple Hello World example.

Use a blueprint  
Build a Lambda application from sample code and configuration presets for common use cases.

Container image  
Select a container image to deploy for your function.

**Basic information**

Function name  
Enter a name that describes the purpose of your function.

Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime [Info](#)  
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.  
 [C](#)

Architecture [Info](#)  
Choose the instruction set architecture you want for your function code.  
 x86\_64  
 arm64

Permissions [Info](#)  
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

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

© 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preference](#)

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

Architecture [Info](#)  
Choose the instruction set architecture you want for your function code.  
 x86\_64  
 arm64

Permissions [Info](#)  
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

▼ Change default execution role

Execution role  
Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).  
 Create a new role with basic Lambda permissions  
 Use an existing role  
 Create a new role from AWS policy templates

Existing role  
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.  
 [C](#)

View the [myPythonLambdaFunction-role-a2x7el65 role](#) on the IAM console.

► Advanced settings

[Cancel](#) [Create function](#)

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

© 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preference](#)

Step 4: The function is up and running.

The screenshot shows the AWS Lambda Function Overview page for a function named 'AdvDevops-ex12'. At the top, a green banner indicates success: 'Successfully created the function AdvDevops-ex12. You can now change its code and configuration. To invoke your function with a test event, choose "Test".' Below the banner, the function name 'AdvDevops-ex12' is displayed with a small Lambda icon. A 'Layers' section shows '(0)'. On the right, there are buttons for 'Throttle', 'Copy ARN', and 'Actions'. Under the main title, there's a 'Function overview' section with a 'Layers' button and a '+ Add destination' button. To the right, detailed information is shown: 'Description' (empty), 'Last modified' (6 seconds ago), 'Function ARN' (arn:aws:lambda:ap-south-1:447953971928:function:AdvDevops-ex12), and 'Function URL' (info). At the bottom, navigation tabs include 'Code' (selected), 'Test', 'Monitor', 'Configuration', 'Aliases', and 'Versions'. The footer includes links for CloudShell, Feedback, and copyright information: '© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences'.

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

The screenshot shows the AWS Lambda Code Editor for the 'lambda\_function' of the 'AdvDevops-ex12' function. The editor displays Python code for a Lambda function named 'lambda\_handler'. The code imports json, boto3, and urllib, and defines a lambda\_handler function that processes S3 events. It prints a message when a file is added to a bucket and logs the contents of a JSON file uploaded to the bucket. The code editor interface includes tabs for 'Environment', 'lambda\_function', 'Environment Var', and 'lambda\_function.py'. The code itself is as follows:

```
1 import json
2 import boto3
3 import urllib
4
5 def lambda_handler(event, context):
6
7     s3_client = boto3.client('s3')
8     bucket_name = event['Records'][0]['s3']['bucket']['name']
9     key = event['Records'][0]['s3']['object']['key']
10    key_urlib.parse.unquote_plus(key, encoding='utf-8')
11    message = 'A file has been added with key ' + key + ' to the bucket ' + bucket_name
12    print(message)
13    response = s3_client.get_object(Bucket=bucket_name, Key=key)
14    contents = response['Body'].read().decode()
15    contents = json.loads(contents)
16
17    print("These are the Contents of the File: \n", contents)
18
19
```

The footer of the editor includes links for CloudShell, Feedback, and copyright information: '© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences'.

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

Screenshot of the AWS Lambda console showing the creation of a new function named "AdvDevops-ex12".

The "Code" tab is selected, displaying the code source in a code editor:

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

A modal window titled "Configure test event" is open, showing the configuration for a test event:

- Test event action:** Create new event (selected)
- Event name:** test
- Event sharing settings:** Private (selected)
- Template - optional:** s3-put
- Event JSON:** (Empty field)

Buttons at the bottom of the modal include: Cancel, Invoke, and Save.

And Save it.

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

Amazon S3

▶ Account snapshot  
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

Buckets (3) [Info](#)  
Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

Name	AWS Region	Access	Creation date
elasticbeanstalk-ap-south-1-447953971928	Asia Pacific (Mumbai) ap-south-1	Objects can be public	August 7, 2023, 14:24:02 (UTC+05:30)
www.hellorachana.com	Asia Pacific (Mumbai) ap-south-1	⚠️ Public	July 30, 2023, 15:05:34 (UTC+05:30)
www.htmlwebsite.com	Asia Pacific (Mumbai) ap-south-1	⚠️ Public	July 30, 2023, 15:49:06 (UTC+05:30)

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

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

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)  
Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name: AdvDevopsexp12  
Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

AWS Region: Asia Pacific (Mumbai) ap-south-1

Copy settings from existing bucket - optional  
Only the bucket settings in the following configuration are copied.  
[Choose bucket](#)

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

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

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

Event notifications (0)  
Send a notification when specific events occur in your bucket. [Learn more](#)

No event notifications  
Choose [Create event notification](#) to be notified when a specific event occurs.  
[Create event notification](#)

Amazon EventBridge  
For additional capabilities, use Amazon EventBridge to build event-driven applications at scale using S3 event notifications. [Learn more](#) or see [EventBridge pricing](#)

Send notifications to Amazon EventBridge for all events in this bucket  
Off

Transfer acceleration  
Use an accelerated endpoint for faster data transfers. [Learn more](#)

Transfer acceleration  
Disabled

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Click on Create Event Notification.

Step 10: Mention an event name and check Put under event types.

The screenshot shows the 'General configuration' section with an 'Event name' field containing 'S3putrequest'. Below it, there are optional fields for 'Prefix' (containing 'images/') and 'Suffix' (containing '.jpg'). The 'Event types' section shows 'Put' checked under 'Object creation'. At the bottom, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2023, Amazon Web Services India Private Limited'.

Event name  
S3putrequest

Event name can contain up to 255 characters.

Prefix - optional  
Limit the notifications to objects with key starting with specified characters.  
images/

Suffix - optional  
Limit the notifications to objects with key ending with specified characters.  
.jpg

**Event types**  
Specify at least one event for which you want to receive notifications. For each group, you can choose an event type for all events, or you can choose one or more individual events.

All object create events  
s3:ObjectCreated:  
 Put  
s3:ObjectCreated:Put

Post  
s3:ObjectCreated:Post

CloudShell Feedback © 2023, Amazon Web Services India Private Limited

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

The screenshot shows the 'Destination' section. It includes a note about granting permissions to publish messages. Under 'Destination', 'Lambda function' is selected. In the 'Specify Lambda function' section, 'Choose from your Lambda functions' is selected. The 'Lambda function' dropdown contains 'AdvDevops-ex12'. At the bottom, there are 'Cancel' and 'Save changes' buttons.

Before Amazon S3 can publish messages to a destination, you must grant the Amazon S3 principal the necessary permissions to call the relevant API to publish messages to an SNS topic, an SQS queue, or a Lambda function. [Learn more](#)

**Destination**  
Choose a destination to publish the event. [Learn more](#)

**Lambda function**  
Run a Lambda function script based on S3 events.

**SNS topic**  
Fanout messages to systems for parallel processing or directly to people.

**SQS queue**  
Send notifications to an SQS queue to be read by a server.

Specify Lambda function

Choose from your Lambda functions

Enter Lambda function ARN

Lambda function  
AdvDevops-ex12

Cancel Save changes

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

The screenshot shows the AWS Lambda Functions overview for the function 'AdvDevops-ex12'. In the 'Triggers' section, there is one entry for 'S3'. Below the triggers, there are buttons for 'Add destination' and 'Add trigger'. To the right, there are sections for 'Description', 'Last modified' (1 minute ago), 'Function ARN' (arn:aws:lambda:ap-south-1:447953971928:function:AdvDevops-ex12), and 'Function URL' (Info). At the bottom, there are tabs for 'Code', 'Test', 'Monitor', 'Configuration', 'Aliases', and 'Versions'. A CloudShell tab is open at the bottom left.

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

```
{ } dummy.json X
{ } dummy.json > ...
1   {
2     "firstname" : "Shashwat",
3     "lastname" : "Tripathi",
4     "gender" : "Male",
5     "age": 19
6 }
```

Step 13: Go back to your S3 Bucket and click on Add Files to upload a new file.

Step 14: Select the dummy data file from your computer and click Upload.

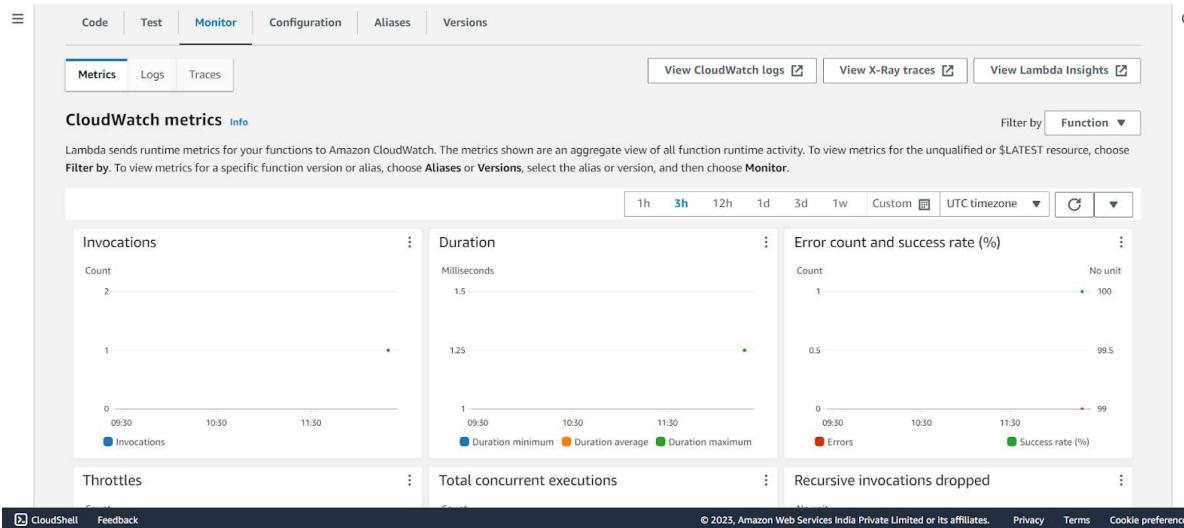
The screenshot shows the AWS S3 'Upload' interface. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, a search bar, and keyboard shortcut '[Alt+S]'. Below the navigation is a breadcrumb trail: 'Amazon S3 > Buckets > advopssexp12 > Upload'. The main title is 'Upload' with an 'Info' link. A note below says: 'Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)'.

A large dashed box area is labeled 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' Below this is a table titled 'Files and folders (1 Total, 89.0 B)'. It contains one item: 'dummy.json' (application/json, 89.0 B). There are 'Remove', 'Add files', and 'Add folder' buttons above the table. A search bar 'Find by name' is also present. The 'Destination' section shows 'Destination s3://advopssexp12'. At the bottom, there are links for 'CloudShell' and 'Feedback', and a copyright notice: '© 2023, Amazon Web Services India Private Limited or its affiliates'.

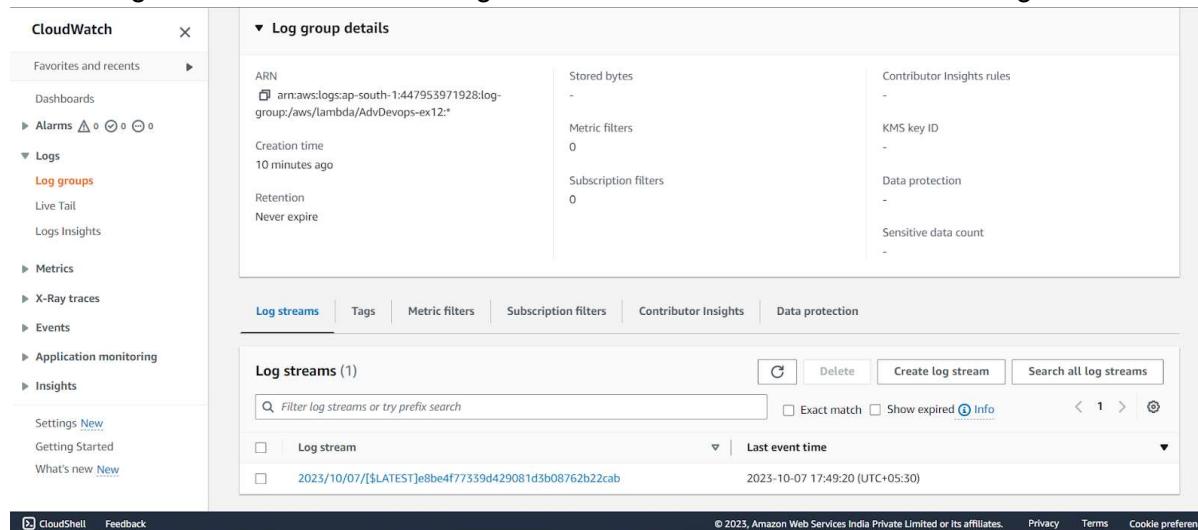
**Step 15:** After this make the necessary changes in the Test configuration file which we created it previously by replacing the Bucket Name and the ARN of Bucket.

The screenshot shows a JSON editor with the title 'Event JSON' and a 'Format JSON' button. The JSON code is a test event for a Lambda function. It includes line numbers from 10 to 38. The code defines a principalId ('EXAMPLE'), request parameters ('sourceIPAddress: "127.0.0.1"'), response elements ('x-amz-request-id: "EXAMPLE123456789", x-amz-id-2: "EXAMPLE123/5678abcdefghijklambdaisawesome/mnopqrstuvwxyzABCDEFGHIJ"'), and an S3 object ('s3: { s3SchemaVersion: "1.0", configurationId: "testConfigRule", bucket: { name: "advopssexp12", ownerIdentity: { principalId: "EXAMPLE" }, arn: "arn:aws:s3:::advopssexp12" }, object: { key: "test%2Fkey", size: 1024, eTag: "0123456789abcdef0123456789abcdef", sequencer: "0A1B2C3D4E5F678901" } } }').

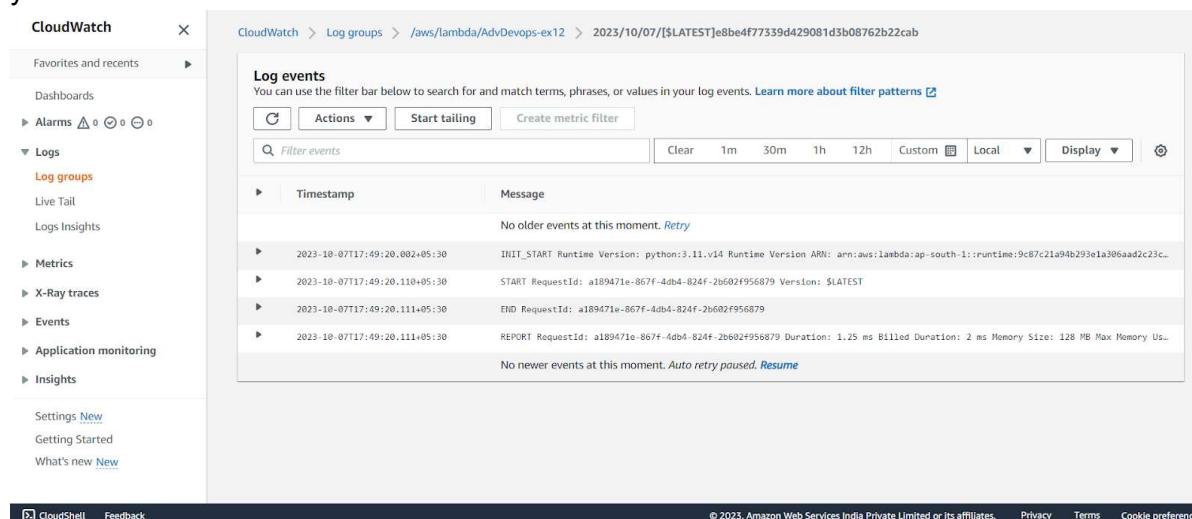
**Step 16:** Go back to your Lambda function , Refresh it and check the Monitor tab.



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



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



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