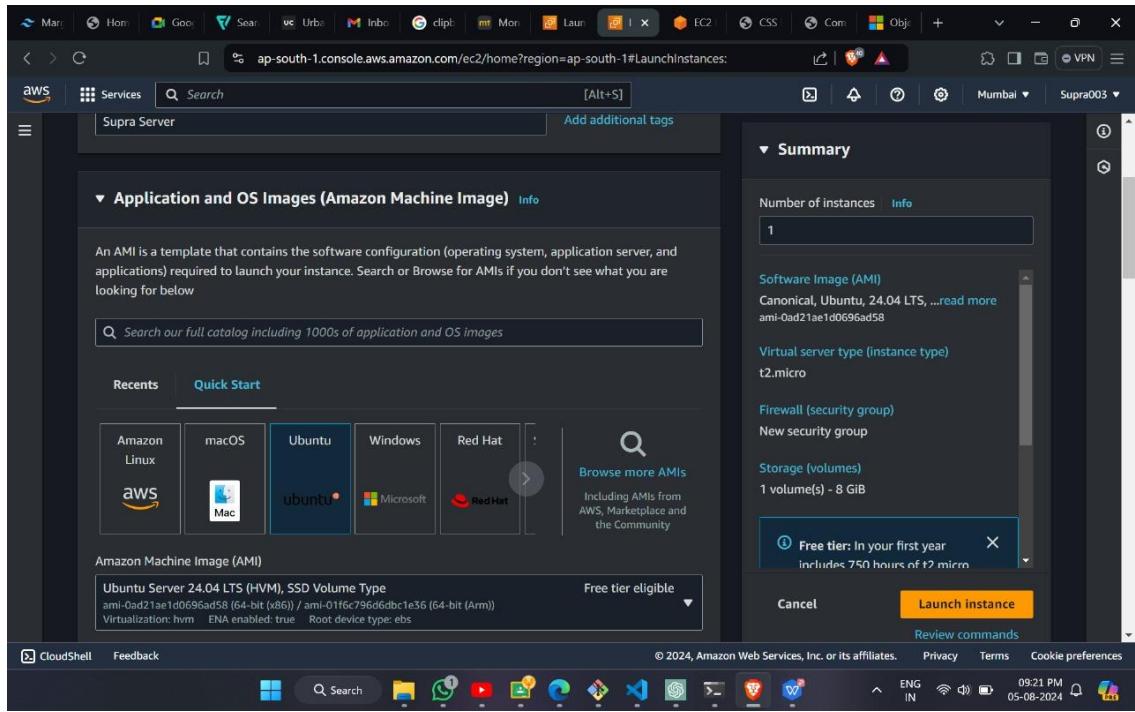


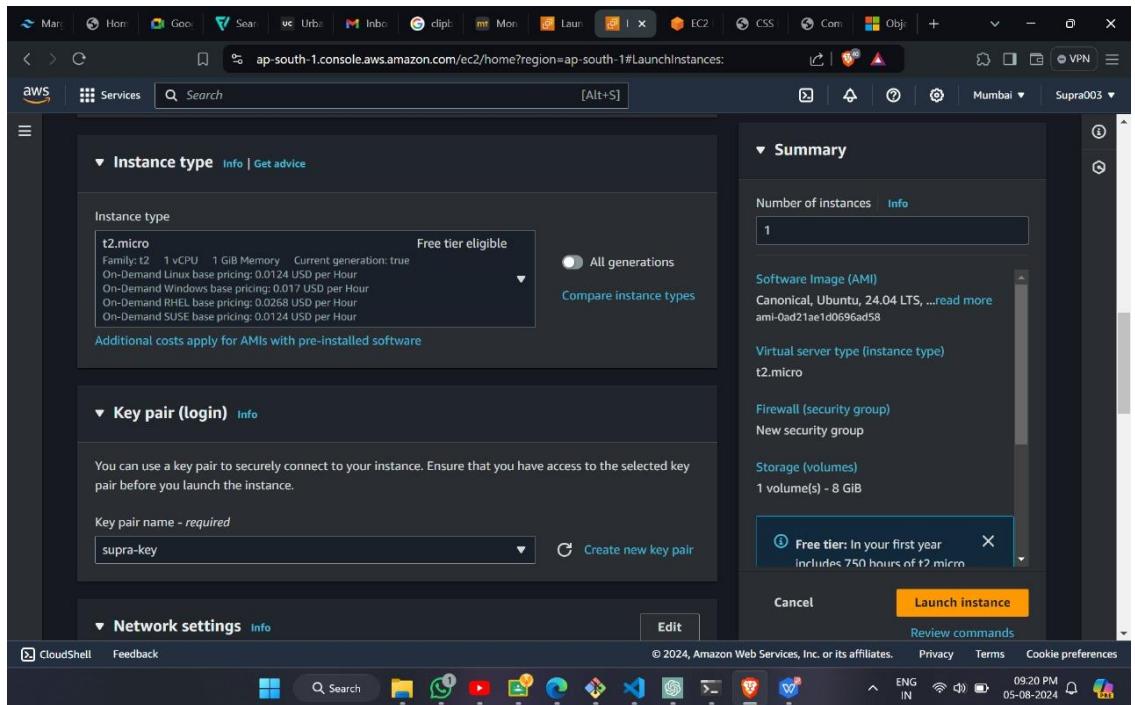
# Experiment 01

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

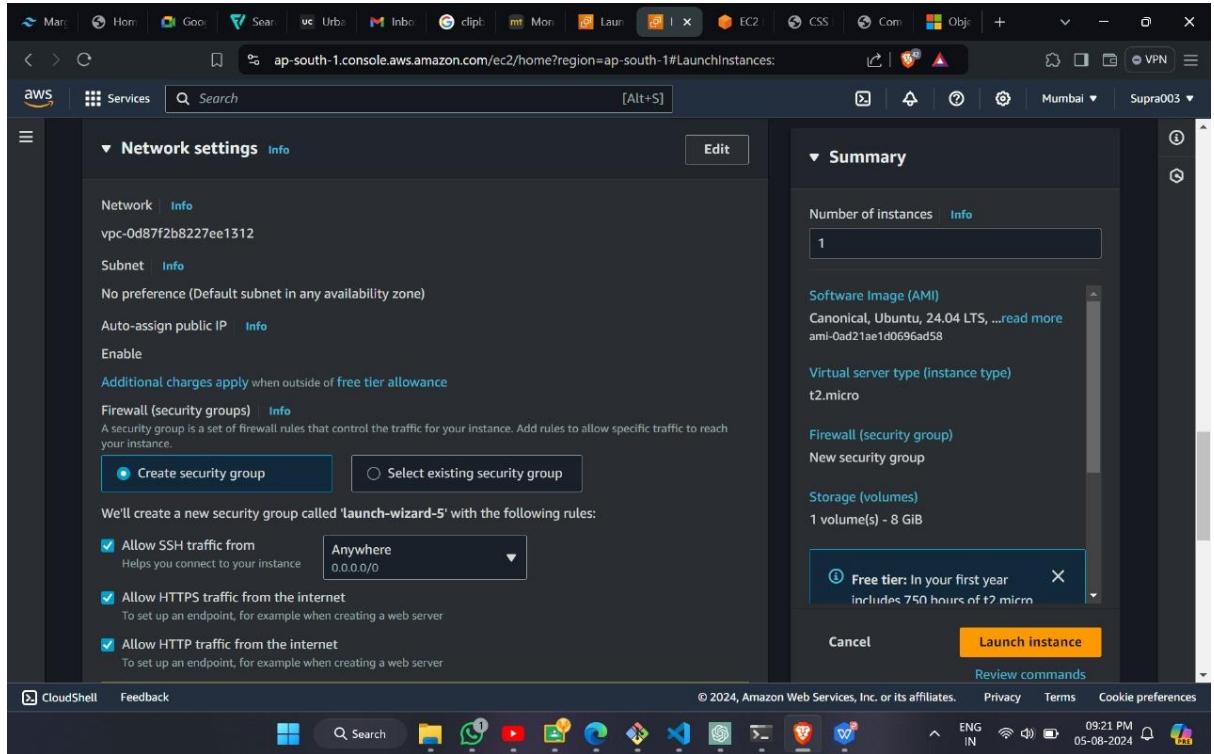
## 1. Give name to EC2 instance



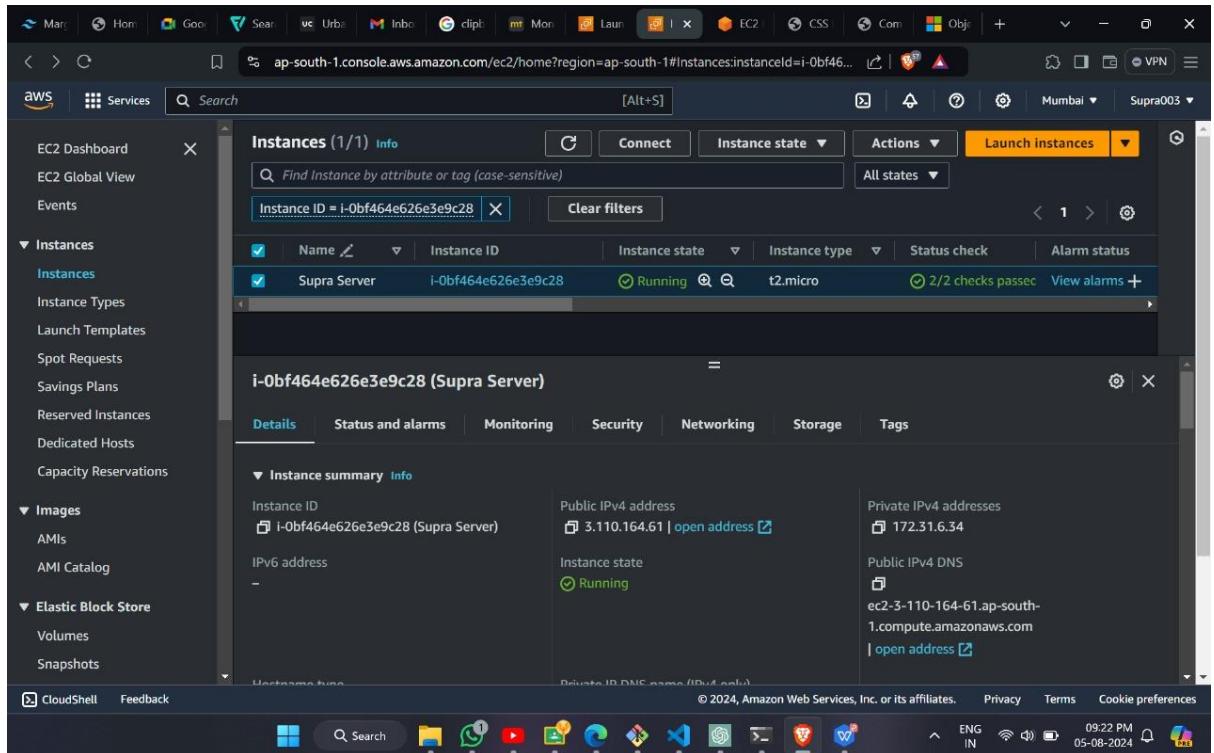
## 2. Create a key-pair login.



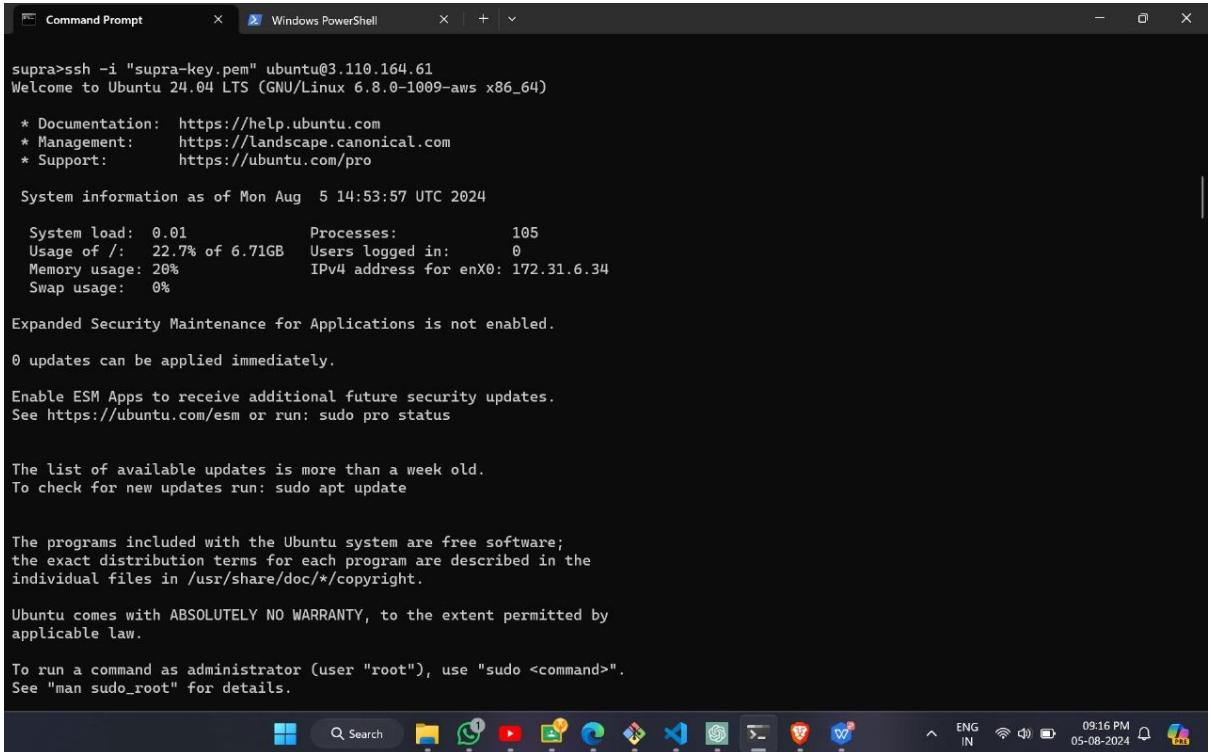
### 3. Edit network settings. And Launch Instance.



### 4. Instance successfully launched.



## 5. Create a virtual environment with key pair permission.



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

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

System information as of Mon 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

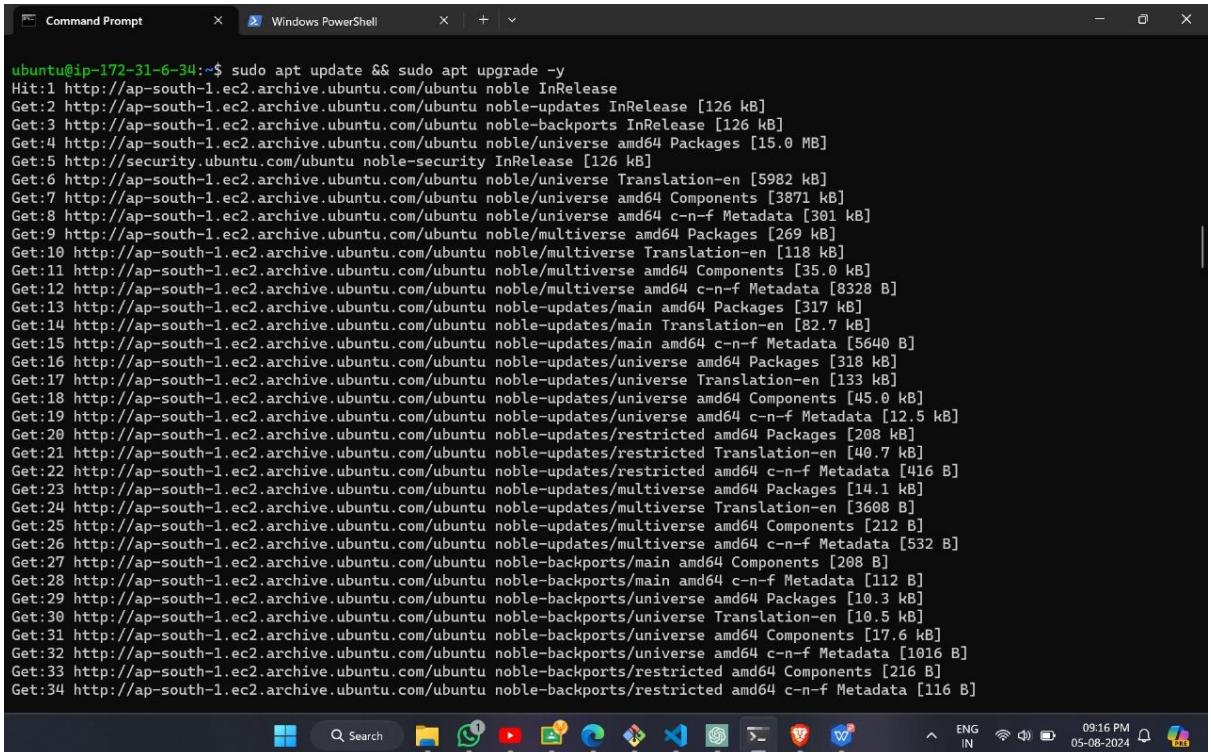
The list of available updates is more than a week old.
To check for new updates run: sudo apt update

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.

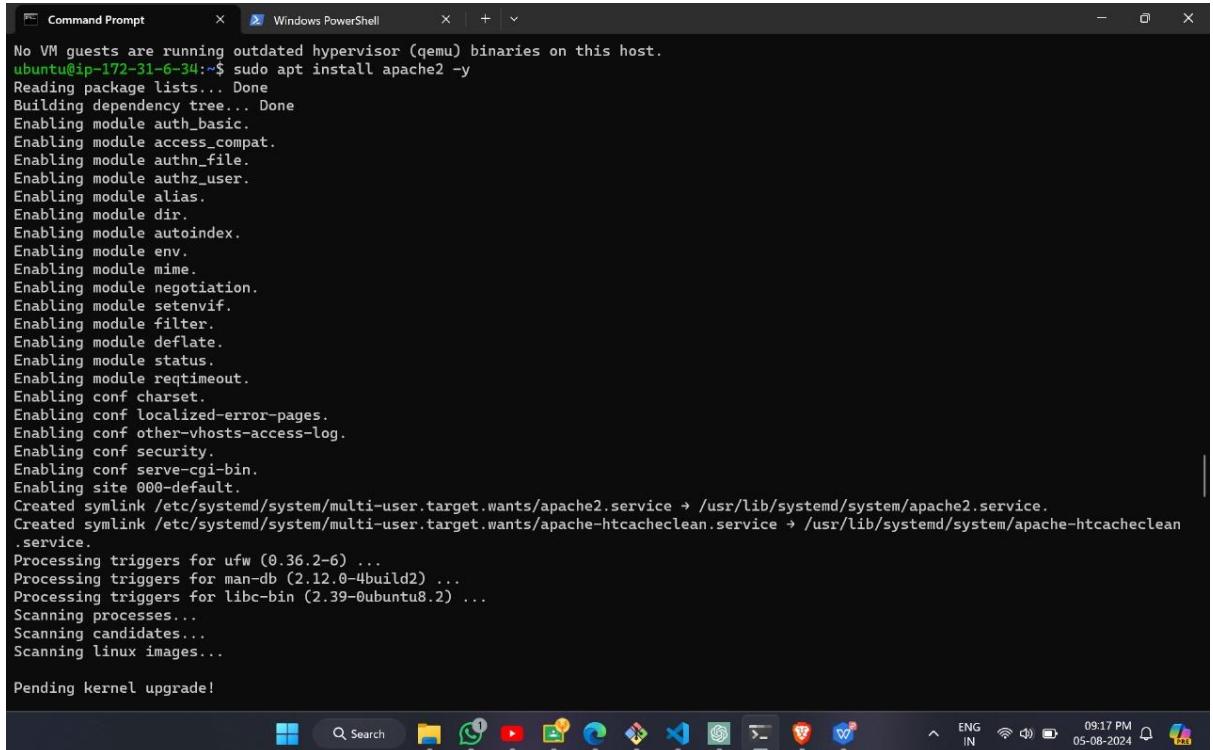
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

## 6. Install apache on virtual machine.



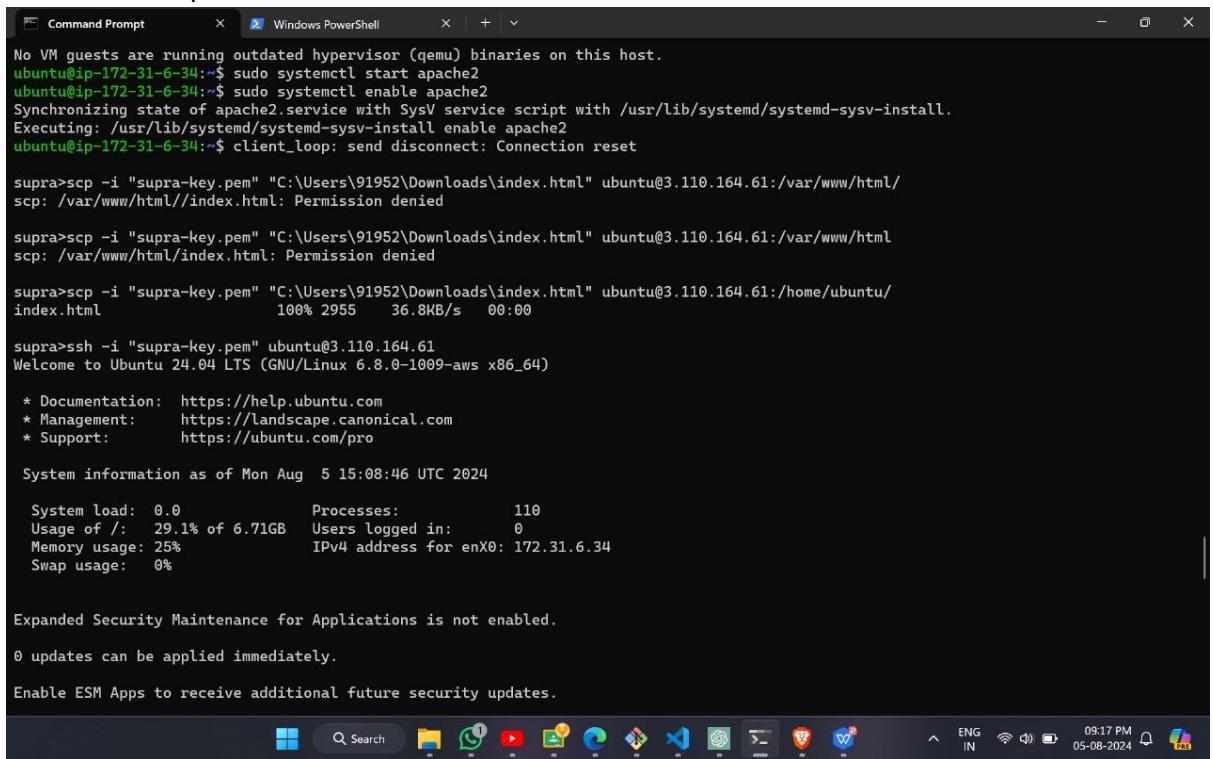
```
ubuntu@ip-172-31-6-34:~$ sudo apt update && sudo apt upgrade -y
Hit:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [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 [301 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 [35.0 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 [45.0 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 [208 kB]
Get:21 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu/noble-updates/restricted Translation-en [40.7 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 [1016 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]
```

## 7. Update and upgrade it.



```
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 000-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.  
.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!
```

## 8. Start the apache server.



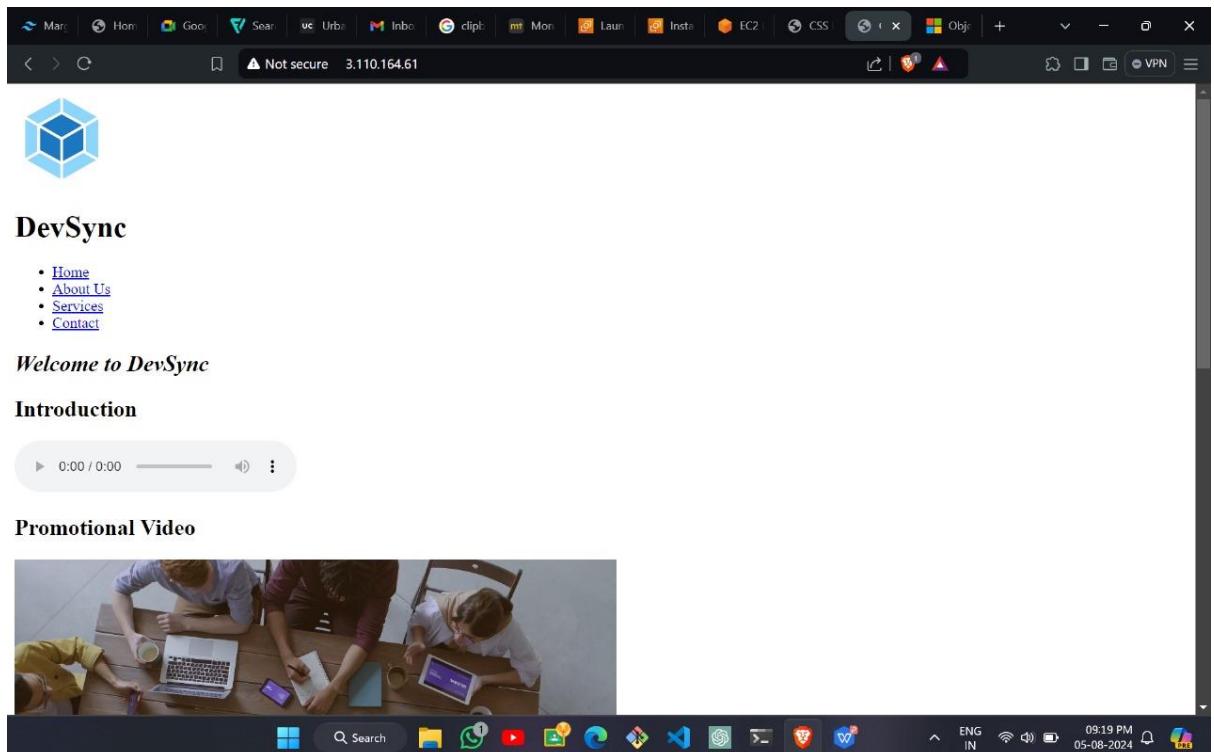
```
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
ubuntu@ip-172-31-6-34:~$ sudo systemctl start apache2  
ubuntu@ip-172-31-6-34:~$ sudo systemctl enable apache2  
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.  
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2  
ubuntu@ip-172-31-6-34:~$ client_loop: send disconnect: Connection reset  
  
supra>scp -i "supra-key.pem" "C:\Users\91952\Downloads\index.html" ubuntu@3.110.164.61:/var/www/html/  
scp: /var/www/html//index.html: Permission denied  
  
supra>scp -i "supra-key.pem" "C:\Users\91952\Downloads\index.html" ubuntu@3.110.164.61:/var/www/html  
scp: /var/www/html/index.html: Permission denied  
  
supra>scp -i "supra-key.pem" "C:\Users\91952\Downloads\index.html" ubuntu@3.110.164.61:/home/ubuntu/  
index.html  
    100% 2955      36.8KB/s   00:00  
  
supra>ssh -i "supra-key.pem" ubuntu@3.110.164.61  
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1009-aws x86_64)  
  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/pro  
  
System information as of Mon Aug  5 15:08:46 UTC 2024  
  
System load:  0.0          Processes:           110  
Usage of /:  29.1% of 6.71GB  Users logged in:     0  
Memory usage: 25%          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.
```

## 9. Give file location to be executed.

```
Command Prompt      Windows PowerShell      +      -      X
*** 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 apache
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 .../08-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) ...

```

## 10. Output of the code on local machine.



## Experiment 01-(a)

### Hosting a static website on Amazon S3

The image consists of three vertically stacked screenshots of a web browser displaying the AWS Management Console.

**Screenshot 1: General Configuration**

This screenshot shows the "Create bucket" page under the "Amazon S3 > Buckets" section. The "General configuration" tab is selected. The "Bucket name" field contains "suprabucket". A note below the field states: "Bucket name must be unique within the global namespace and follow the bucket naming rules. See [rules for bucket naming](#)".

**Screenshot 2: Advanced Settings**

This screenshot shows the "Advanced settings" tab. Under "Encryption type", "Server-side encryption with Amazon S3 managed keys (SSE-S3)" is selected. Under "Bucket Key", "Enable" is selected. A note says: "Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)".

**Screenshot 3: Confirmation and Next Steps**

This screenshot shows the confirmation step after creating the bucket. It displays a message: "After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings." At the bottom are "Cancel" and "Create bucket" buttons. The status bar at the bottom right shows the date and time: "13:39 13-08-2024".

Screenshot of the AWS S3 console showing the "Edit static website hosting" configuration for the "suprabucket2" bucket.

**Static website hosting**

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

**Static website hosting**

Disable  Enable

**Hosting type**

Host a static website Use the bucket endpoint as the web address. [Learn more](#)

Redirect requests for an object Redirect requests to another bucket or domain. [Learn more](#)

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

**Bucket policy**

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

**Bucket ARN**

arn:aws:s3:::suprabucket2

**Policy**

```
1▼ {
2  "Version": "2012-10-17",
3▼  "Statement": [
4▼    {
5      "Sid": "PublicReadGetObject",
6      "Effect": "Allow",
7      "Principal": "*",
8      "Action": "s3:GetObject",
9      "Resource": "arn:aws:s3:::suprabucket2|"
10     }
11   ]
12 }
```

**Edit statement**  
PublicReadGetObject [Remove](#)

**Add actions**

Choose a service

**Included**

S3

The screenshot shows the AWS S3 console with the URL [ap-south-1.console.aws.amazon.com/s3/buckets/suprabucket2?region=ap-south-1&bucketType=general&tab=permissions](https://ap-south-1.console.aws.amazon.com/s3/buckets/suprabucket2?region=ap-south-1&bucketType=general&tab=permissions). The browser tabs include D15 A..., suprab..., Hosting, 503 Ser..., Thank..., ChatG..., Install, New To..., New To..., Gmail, YouTube, Maps, India Scholarship 20..., and All Bookmarks. The AWS Services bar shows CloudShell and Feedback. The main content area displays a green success message: "Successfully edited bucket policy." Below this, the bucket name "suprabucket2" is shown with an "Info" link. The navigation bar includes Objects, Properties, Permissions (which is selected), Metrics, Management, and Access Points. The "Permissions overview" section contains an "Access finding" panel with a note about IAM external access analyzers and a link to "View analyzer for ap-south-1". The "Block public access (bucket settings)" section has an "Edit" button. A note states that public access is granted through ACLs, policies, or point policies, and recommends turning on "Block all public access". The footer includes links for CloudShell, Feedback, © 2024, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

The screenshot shows the AWS S3 console with the URL [ap-south-1.console.aws.amazon.com/s3/buckets/suprabucket2?region=ap-south-1&bucketType=general&tab=objects](https://ap-south-1.console.aws.amazon.com/s3/buckets/suprabucket2?region=ap-south-1&bucketType=general&tab=objects). The browser tabs and AWS Services bar are identical to the previous screenshot. The main content area shows the "Objects (0) Info" section. It features a toolbar with Copy S3 URI, Copy URL, Download, Open, Delete, Actions, Create folder, and Upload buttons. A search bar with "Find objects by prefix" and a pagination indicator (1) are also present. A table header for "Objects" includes columns for Name, Type, Last modified, Size, and Storage class. A message at the bottom states "No objects" and "You don't have any objects in this bucket." The footer includes CloudShell, Feedback, © 2024, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

Screenshot of the AWS S3 Upload interface showing the upload process for the file "index.html".

The browser address bar shows: ap-south-1.console.aws.amazon.com/s3/upload/suprabucket2?region=ap-south-1&bucketType=general

The AWS navigation bar includes: Services, Search, Mumbai, Supra003.

The breadcrumb navigation shows: Amazon S3 > Buckets > suprabucket2 > Upload.

## Upload Info

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

Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).

Files and folders (1 Total, 674.0 B)								
<small>All files and folders in this table will be uploaded.</small>								
<input type="button" value="Remove"/> <input type="button" value="Add files"/> <input type="button" value="Add folder"/>								
<input type="text" value="Find by name"/>								
<table border="1"><thead><tr><th>Name</th><th>Folder</th><th>Type</th></tr></thead><tbody><tr><td>index.html</td><td>-</td><td>text/html</td></tr></tbody></table>			Name	Folder	Type	index.html	-	text/html
Name	Folder	Type						
index.html	-	text/html						

**Destination:** [s3://suprabucket2](#)

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

**Upload succeeded**  
View details below.

### Upload: status

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

Summary		
Destination <a href="#">s3://suprabucket2</a>	Succeeded 1 file, 674.0 B (100.00%)	Failed 0 files, 0 B (0%)

[Files and folders](#) [Configuration](#)

**Files and folders (1 Total, 674.0 B)**

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

D15 A| suprabucket2 | Basic H | Hosting | 503 Se | Thank | ChatGF | Install | New To | New To | Gmail | Inbox | acs.am | acs.am | +

Gmail YouTube Maps India Scholarship 20...

Amazon S3 Services Search [Alt+S]

Buckets

- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

CloudShell Feedback

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

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

Requester pays  
Disabled

**Static website hosting**

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

Edit

Static website hosting  
Enabled

Hosting type  
Bucket hosting

Bucket website endpoint  
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)

<http://suprabucket2.s3-website.ap-south-1.amazonaws.com>

D15 A| suprabucket2 | Basic H | Hosting | 503 Se | Thank | ChatGF | Install | New To | New To | Gmail | Inbox | acs.am | acs.am | +

Gmail YouTube Maps India Scholarship 20...

Not secure suprabucket2.s3-website.ap-south-1.amazonaws.com

All Bookmarks

# Welcome to My Basic HTML Page

This is a paragraph of text on the page. HTML stands for HyperText Markup Language and is used to create the structure of web pages.

## Experiment 02

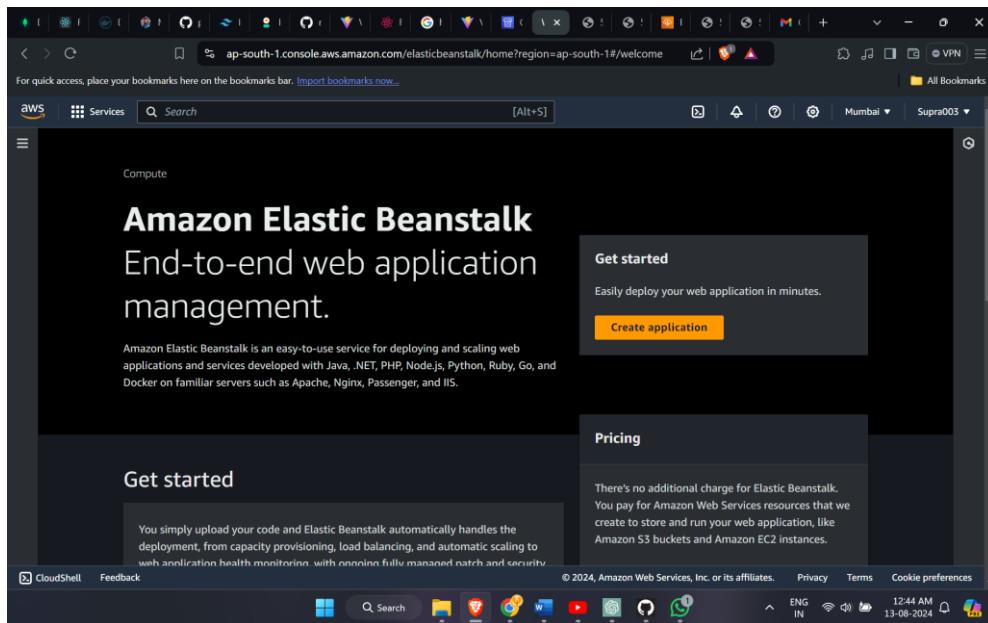
Name: Prajyot Shinde

Roll no: 57

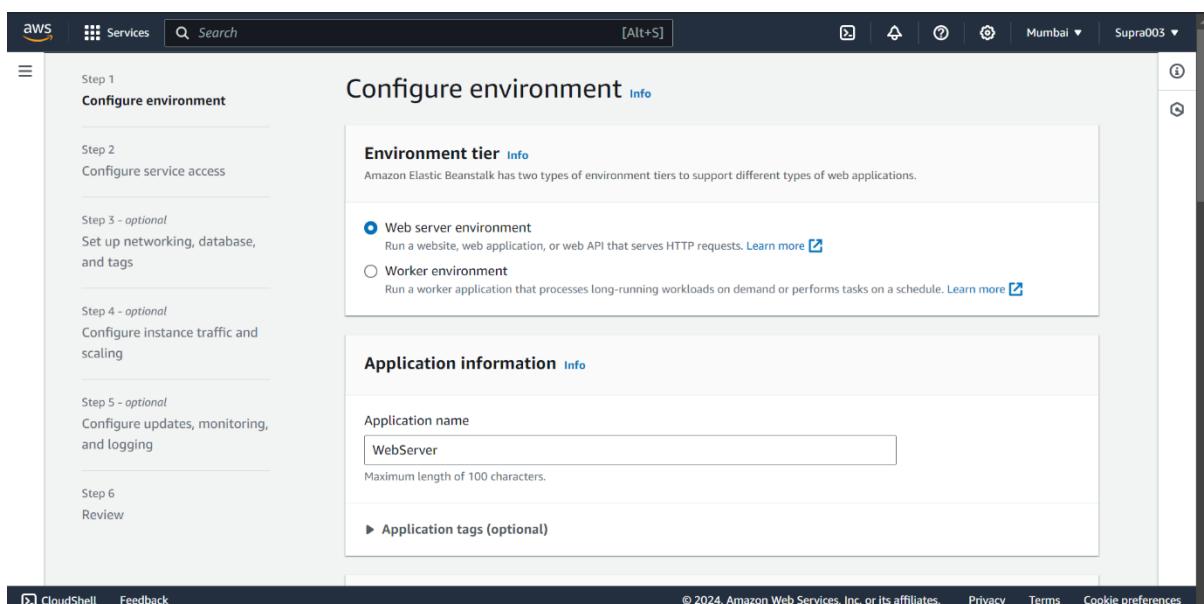
Aim: To Build Your Application using AWS CodeBuild and Deploy on S3 / SEBS using AWS CodePipeline, deploy Sample Application on EC2 instance using AWS CodeDeploy.

### Step-1: Beanstalk Deployment

1. Login to your AWS account and search for Elastic Beanstalk in the search box



2. Open up Elastic Beanstalk and name your web app.



3. Choose Python from the drop-down menu and then click Create Application.

The screenshot shows the 'Platform Info' configuration page. Under 'Platform type', the 'Managed platform' option is selected. The 'Platform' dropdown is set to 'PHP'. The 'Platform branch' dropdown shows 'PHP 8.3 running on 64bit Amazon Linux 2023'. The 'Platform version' dropdown shows '4.3.2 (Recommended)'. Below this, there is a section titled 'Application code' with a 'Info' link. At the bottom of the page, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates.' followed by 'Privacy', 'Terms', and 'Cookie preferences'.

4. Choose the proper options

The screenshot shows the 'Configure service access' step of the wizard. On the left, a 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 'Configure service access' step is currently selected. The main area is titled 'Service access' and contains instructions about IAM roles and EC2 instance profiles. It includes fields for 'Service role' (set to 'Use an existing service role' with 'aws-elasticbeanstalk-service-role' selected), 'EC2 key pair' (set to 'supra-key'), and 'EC2 instance profile' (set to 'elasticbeanstalk\_myEc2role'). At the bottom, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates.' followed by 'Privacy', 'Terms', and 'Cookie preferences'.

**VPC**

Launch your environment in a custom VPC instead of the default VPC. You can create a VPC and subnets in the VPC management console.

[Learn more](#)

vpc-0d87f2b8227ee1312 | (172.31.0.0/16)

[Create custom VPC](#)

**Instance settings**

Choose a subnet in each AZ for the instances that run your application. To avoid exposing your instances to the Internet, run your instances in private subnets and load balancer in public subnets. To run your load balancer and instances in the same public subnets, assign public IP addresses to the instances. [Learn more](#)

**Public IP address**

Assign a public IP address to the Amazon EC2 instances in your environment.

Activated

**Instance subnets**

Filter instance subnets

Availability Zone	Subnet	CIDR	Name
us-east-1a	sg-0d87f2b8227ee1312	172.31.0.0/16	vpc-0d87f2b8227ee1312

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

With the current setting, the environment enables only IAMDSV2.

Deactivated

**EC2 security groups**

Select security groups to control traffic.

EC2 security groups (7)

Filter security groups

Group name	Group ID	Name
awseb-e-d9kh68ppqn-stack-1	sg-0632048b6f88d4ddd	SupraApp-env-1
awseb-e-eczswppc8z-stack-1	sg-0de68df64bdffa855	WebApp02-env
default	sg-0a472ec49e7bb8a21	
launch-wizard-1	sg-01711621a355ca6a4	
launch-wizard-2	sg-048d55c094d22c63a	
launch-wizard-3	sg-0b5b28982c66cf258	
launch-wizard-4	sg-0d43e01a6548a50da	

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

**Review** [Info](#)

**Step 1: Configure environment**

[Edit](#)

**Environment information**

Environment tier	Application name
Web server environment	WebServer
Environment name	Application code
WebServer-env	Sample application
Platform	
arn:aws:elasticbeanstalk:ap-south-1:platform/PHP 8.3	
running on 64bit Amazon Linux 2023/4.3.2	

**Step 2: Configure service access**

[Edit](#)

**Service access** [Info](#)

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

**Instance log streaming to CloudWatch logs**

Configure the instances in your environment to stream logs to CloudWatch logs. You can set the retention to up to 10 years and configure Elastic Beanstalk to delete the logs when you terminate your environment. [Learn more](#)

**Log streaming**  
(standard CloudWatch charges apply.)

Activated

**Retention**

7

**Lifecycle**

Keep logs after terminating envir...

**Environment properties**

The following properties are passed in the application as environment properties. [Learn more](#)

No environment properties have been configured.

[Add environment property](#)

[Cancel](#) [Previous](#) [Next](#)

**Configure updates, monitoring, and logging - optional** [info](#)

**Monitoring** [info](#)

**Health reporting**

Enhanced health reporting provides free real-time application and operating system monitoring of the instances and other resources in your environment. The `EnvironmentHealth` custom metric is provided free with enhanced health reporting. Additional charges apply for each custom metric. For more information, see [Amazon CloudWatch Pricing](#)

**System**

Basic  
 Enhanced

**Health event streaming to CloudWatch Logs**

Configure Elastic Beanstalk to stream environment health events to CloudWatch Logs. You can set the retention up to a maximum of ten years and configure Elastic Beanstalk to delete the logs when you terminate your environment.

**Log streaming**

Activated (standard CloudWatch charges apply.)

**Retention**

7

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

## Step-2: Creating CodePipeline

Beanstalk creates a sample environment for you to deploy your application. By default, it creates an EC2 instance, a security group, an Auto Scaling group, an Amazon S3 Bucket, Amazon CloudWatch alarms and a domain name for your Application.

Create a CodePipeline and give pipeline name

The screenshot shows the 'Choose pipeline settings' step in the AWS CodePipeline console. On the left, a sidebar lists steps: Step 1 (Choose pipeline settings), Step 2 (Add source stage), Step 3 (Add build stage), Step 4 (Add deploy stage), and Step 5 (Review). The main area is titled 'Pipeline settings'. It has a 'Pipeline name' field containing 'WebServerPipe', a note about pipeline type (V2 recommended), and an 'Execution mode' section with 'Queued (Pipeline type V2 required)' selected. The bottom right shows copyright information: © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences.

Create a Github connection

The screenshot shows the 'Create a connection' step for GitHub in the AWS CodePipeline console. It's titled 'Create GitHub App connection'. A 'Connection name' field contains 'WebAppGitHub'. Below it is a 'Tags - optional' section and a 'Connect to GitHub' button. To the right, there's a note about actions and a progress bar indicating 'Connecting'. The bottom right shows copyright information: © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences.

Installed GitHub App - AWS Connector for GitHub - Brave

github.com/settings/installations/53728143

## Repository access

All repositories  
This applies to all current *and* future repositories owned by the resource owner.  
Also includes public repositories (read-only).

Only select repositories  
Select at least one repository.  
Also includes public repositories (read-only).

Select repositories ▾

Selected 1 repository.

prajyots60/aws-codepipeline-s3-codedeploy-linux-2.0

Save Cancel

## Danger zone

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

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 10:08 PM 17-08-2024

Create connection | CodePipeline | ap-south-1 - Brave

ap-south-1.console.aws.amazon.com/codesuite/settings/connections/create...

AWS Services More ▾

### Developer Tools > ... > 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](#)

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

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

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 10:08 PM 17-08-2024

Servicess Search [Alt+S] Mumbai Supra003

Step 1 Choose pipeline settings

Step 2 Add source stage

Step 3 Add build stage

Step 4 Add deploy stage

Step 5 Review

## Add source stage Info

### Step 2 of 5

#### Source

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

GitHub (Version 2)

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

Connection Choose an existing connection that you have already configured, or create a new one and then return to this task.

arn:aws:codeconnections:ap-south-1:01092822160:connection/38b1df1b-a X or [Connect to GitHub](#)

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

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

Servicess Search [Alt+S] Mumbai Supra003

#### Repository name

Choose a repository in your GitHub account.

prajots60/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**

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

## For deploy choose elastic beanstalk

The screenshot shows the 'Add deploy stage' step of an AWS Pipeline. The left sidebar lists steps: Step 1 (Choose pipeline settings), Step 2 (Add source stage), Step 3 (Add build stage), Step 4 (Add deploy stage), and Step 5 (Review). The main area is titled 'Deploy' and contains the 'Deploy provider' section. A message box states: '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.' Below this, the 'Deploy provider' dropdown is set to 'AWS Elastic Beanstalk'. Other fields include 'Region' (Asia Pacific (Mumbai)), 'Input artifacts' (SourceArtifact), 'Application name' (WebServer), and 'Environment name' (WebServer-env). A checkbox for 'Configure automatic rollback on stage failure' is checked. The bottom right corner shows copyright information: © 2024, Amazon Web Services, Inc. or its affiliates.

The screenshot shows the 'Step 4: Add deploy stage' step of an AWS Pipeline. The left sidebar lists steps: Step 1 (Choose pipeline settings), Step 2 (Add source stage), Step 3 (Add build stage), Step 4 (Add deploy stage), and Step 5 (Review). The main area is titled 'Step 4: Add deploy stage' and contains the 'Deploy action provider' section. It lists the following configuration: Deploy action provider (AWS Elastic Beanstalk), ApplicationName (WebServer), EnvironmentName (WebServer-env), and 'Configure automatic rollback on stage failure' (Enabled). At the bottom are 'Cancel', 'Previous', and 'Create pipeline' buttons. The bottom right corner shows copyright information: © 2024, Amazon Web Services, Inc. or its affiliates.

Make connection between code pipeline and beanstalk. And Green means successfully connected.

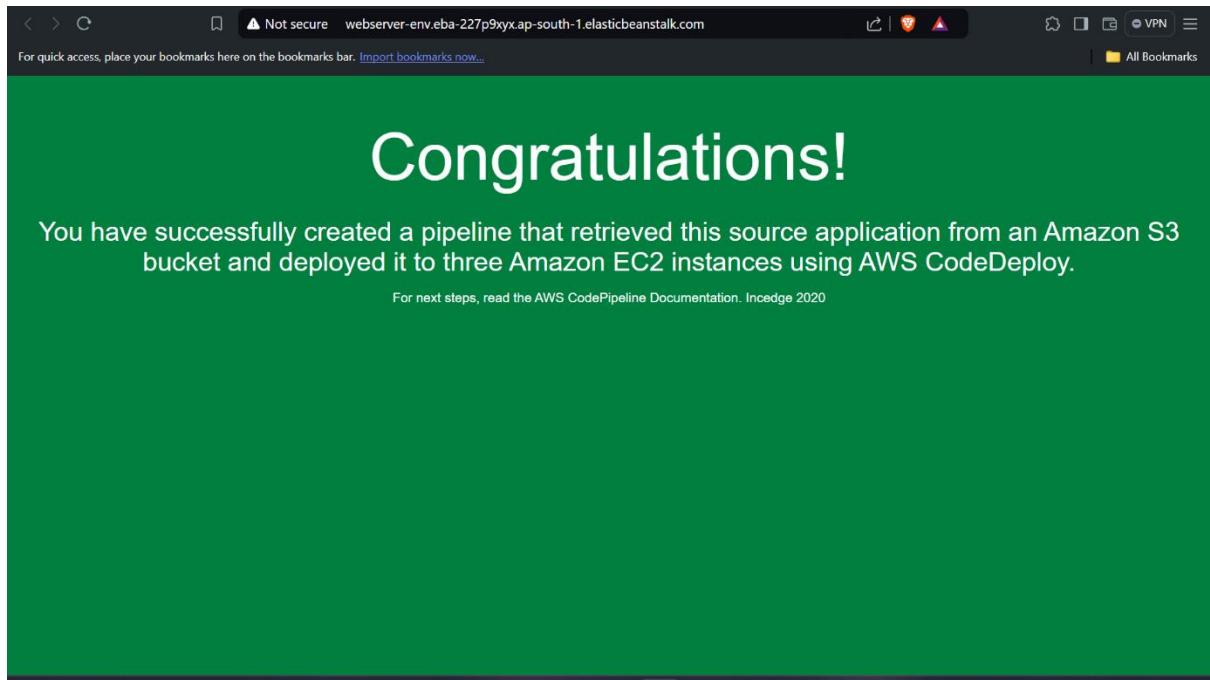
The screenshot shows the AWS CodePipeline console for a pipeline named "WebServerPipe". The pipeline type is V2 and the execution mode is QUEUED. The execution ID is `8e246baaf-dfb7-463f-925d-7d5d2ee71640`. The pipeline consists of two stages: "Source" and "Deploy". The "Source" stage is succeeded, showing a GitHub commit from "Supra003" with a timestamp of "1 minute ago". The "Deploy" stage is also succeeded, showing an AWS Elastic Beanstalk deployment with a timestamp of "Just now". Both stages have green checkmarks indicating successful completion. The pipeline status is overall SUCCEEDED.

Click on domain to view your hosting site

The screenshot shows the AWS Elastic Beanstalk console for an application named "WebServer". The application has one environment named "WebServer-env". The environment details are as follows:

Environment name	Health	Date created	Domain	Running vers
WebServer-env	Green	August 17, 2024 22:00:00	WebServer-env.eba-227p9xyx...	code-pipeline

The environment status is Green, indicating successful deployment. The URL for the environment is listed at the bottom of the page: <https://ap-south-1.console.aws.amazon.com/elasticbeanstalk/home?region=ap-south-1#>.



## Experiment 01-(a)

### Hosting a static website on Amazon S3

The image consists of three vertically stacked screenshots of a web browser displaying the AWS Management Console.

**Screenshot 1: General Configuration**

This screenshot shows the "Create bucket" page under the "Amazon S3 > Buckets" section. The "General configuration" tab is selected. The "Bucket name" field contains "suprabucket". A note below the field states: "Bucket name must be unique within the global namespace and follow the bucket naming rules. See [rules for bucket naming](#)".

**Screenshot 2: Advanced Settings**

This screenshot shows the "Advanced settings" tab. Under "Encryption type", "Server-side encryption with Amazon S3 managed keys (SSE-S3)" is selected. Under "Bucket Key", "Enable" is selected. A note says: "Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)".

**Screenshot 3: Confirmation and Next Steps**

This screenshot shows the confirmation step after creating the bucket. It displays a message: "After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings." At the bottom are "Cancel" and "Create bucket" buttons. The status bar at the bottom right shows the date and time: "13:39 13-08-2024".

Screenshot of the AWS S3 console showing the "Edit static website hosting" configuration for the "suprabucket2" bucket.

**Static website hosting**

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

**Static website hosting**

Disable  Enable

**Hosting type**

Host a static website Use the bucket endpoint as the web address. [Learn more](#)

Redirect requests for an object Redirect requests to another bucket or domain. [Learn more](#)

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

**Bucket policy**

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

**Bucket ARN**

arn:aws:s3:::suprabucket2

**Policy**

```
1▼ {
2  "Version": "2012-10-17",
3▼  "Statement": [
4▼    {
5      "Sid": "PublicReadGetObject",
6      "Effect": "Allow",
7      "Principal": "*",
8      "Action": "s3:GetObject",
9      "Resource": "arn:aws:s3:::suprabucket2|"
10     }
11   ]
12 }
```

**Edit statement**  
PublicReadGetObject [Remove](#)

**Add actions**

Choose a service

**Included**

S3

Screenshot of the AWS S3 Bucket Permissions Overview page for 'suprabucket2'.

The top navigation bar shows the URL: ap-south-1.console.aws.amazon.com/s3/buckets/suprabucket2?region=ap-south-1&bucketType=general&tab=permissions

The main content area displays a success message: "Successfully edited bucket policy."

The navigation bar below the title bar includes: Objects, Properties, **Permissions**, Metrics, Management, Access Points.

The "Permissions overview" section contains:

- Access finding: "Access findings are provided by IAM external access analyzers. Learn more about How IAM analyzer findings work." with a link.
- Block public access (bucket settings): A button labeled "Edit". Below it, a note states: "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."

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

Screenshot of the AWS S3 Bucket Objects page for 'suprabucket2'.

The top navigation bar shows the URL: ap-south-1.console.aws.amazon.com/s3/buckets/suprabucket2?region=ap-south-1&bucketType=general&tab=objects

The main content area displays a message: "No objects" and "You don't have any objects in this bucket."

The navigation bar below the title bar includes: Objects, Properties, Permissions, Metrics, Management, Access Points.

The "Objects (0) Info" section contains:

- Actions: Copy S3 URI, Copy URL, Download, Open, Delete, Actions, Create folder, Upload.
- Search bar: "Find objects by prefix".
- Table headers: Name, Type, Last modified, Size, Storage class.

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

Screenshot of the AWS S3 Upload interface showing the upload process for the file "index.html".

The browser address bar shows: ap-south-1.console.aws.amazon.com/s3/upload/suprabucket2?region=ap-south-1&bucketType=general

The AWS navigation bar includes: Services, Search [Alt+S], Mumbai, Supra003.

The breadcrumb navigation shows: Amazon S3 > Buckets > suprabucket2 > Upload.

## Upload Info

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

Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).

**Files and folders (1 Total, 674.0 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**

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

**Upload succeeded**

View details below.

### Upload: status

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

#### Summary

Destination	Succeeded	Failed
s3://suprabucket2	<span style="color: green;">✔ 1 file, 674.0 B (100.00%)</span>	<span style="color: gray;">✖ 0 files, 0 B (0%)</span>

[Files and folders](#) [Configuration](#)

**Files and folders (1 Total, 674.0 B)**

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

The screenshot shows the AWS S3 console with the URL [ap-south-1.console.aws.amazon.com/s3/buckets/suprabucket2?region=ap-south-1&bucketType=general&tab=properties](https://ap-south-1.console.aws.amazon.com/s3/buckets/suprabucket2?region=ap-south-1&bucketType=general&tab=properties). The left sidebar includes links for Buckets, Storage Lens, and Block Public Access settings. The main content area displays the 'Requester pays' setting as 'Disabled' and the 'Static website hosting' section as 'Enabled' with 'Bucket hosting' selected. A note about the bucket endpoint is present.

The screenshot shows a web browser window with the URL <http://suprabucket2.s3-website.ap-south-1.amazonaws.com>. The page title is "Welcome to My Basic HTML Page". The content of the page is a single paragraph: "This is a paragraph of text on the page. HTML stands for HyperText Markup Language and is used to create the structure of web pages."

## ADVANCE DEVOPS EXP-3

Name : Prajyot Shinde

Roll No : 57

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

**Step 1:** Create 2 Security Groups for Master and Nodes and add the following inbound rules in those groups:

The screenshot shows the 'Launch an instance' wizard in the AWS EC2 console. The current step is 'Name and tags'. A single instance is selected. The 'Name' field contains 'Master'. Other fields include 'Add additional tags' and a search bar for AMIs. On the right, the 'Summary' pane shows the configuration: 1 instance, Canonical Ubuntu 24.04 AMI, t2.medium instance type, New security group, and 1 volume (8 GiB). Buttons for 'Cancel', 'Launch instance', and 'Review commands' are at the bottom.

Generate a key pair for the same:

The screenshot shows the 'Launch an instance' wizard in the AWS EC2 console. The current step is 'Key pair (login)'. A key pair named 'master-key' is selected. Other steps shown are 'Instance type' (t2.medium) and 'Network settings'. The 'Summary' pane on the right remains the same as the previous screenshot, showing 1 instance, Canonical Ubuntu 24.04 AMI, t2.medium instance type, New security group, and 1 volume (8 GiB). Buttons for 'Cancel', 'Launch instance', and 'Review commands' are at the bottom.

<input type="checkbox"/> node 2	i-05c78ee26bbc9b179	Pending		t2.medium	-	<a href="#">View alarms</a>	ap-south-1a	ec2-13-20
<input type="checkbox"/> node 1	i-0b1270d945da2029e	Running		t2.medium	Initializing	<a href="#">View alarms</a>	ap-south-1a	ec2-13-23
<input type="checkbox"/> Master	i-0f13653cf3d300e3	Running		t2.medium	2/2 checks passed	<a href="#">View alarms</a>	ap-south-1a	ec2-13-20

## Step2:

Open Master and node on EC2 terminal:

```

ubuntu@ip-172-31-91-198:~$ sudo apt-get update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [377 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [81.6 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4528 B]
Get:9 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [270 kB]
Get:10 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [113 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [8632 B]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [10.1 kB]
Get:13 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [353 kB]
Get:14 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [68.1 kB]
Get:15 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 c-n-f Metadata [428 B]
Get:16 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [10.9 kB]
Get:17 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [2808 B]
Get:18 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Get:19 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [344 B]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]

i-05b0173781636f4ff (Master)
PublicIPs: 44.201.176.188 PrivateIPs: 172.31.91.198

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

```

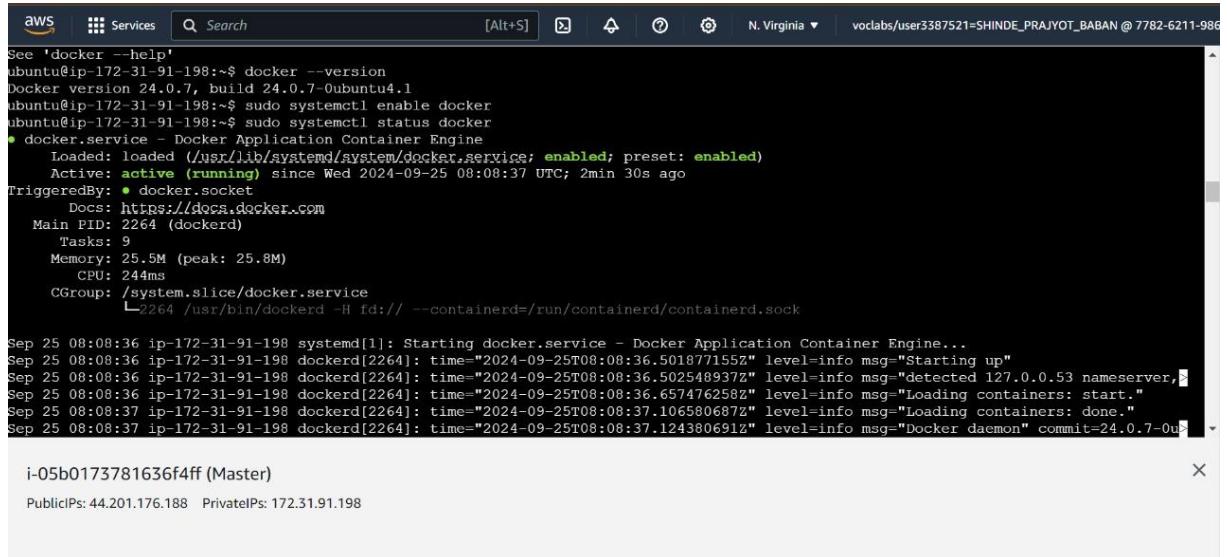
ubuntu@ip-172-31-80-216:~\$ sudo apt-get update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [377 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [81.6 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4528 B]
Get:10 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [270 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [113 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [8632 B]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:14 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [10.1 kB]
Get:15 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [353 kB]
Get:16 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [68.1 kB]
Get:17 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 c-n-f Metadata [428 B]
Get:18 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [10.9 kB]
Get:19 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [2808 B]
Get:20 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Get:21 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [344 B]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]

i-0c11fef84f9ef24a2 (node)
PublicIPs: 3.85.160.47 PrivateIPs: 172.31.80.216

## Step 3:

### Install Docker

```
ubuntu@ip-172-31-91-198:~$ sudo apt-get install docker.io
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bridge-utils containerd dns-root-data dnsmasq-base pigz runc ubuntu-fan
Suggested packages:
  ifupdown aufs-tools cgroupfs-mount | cgroup-lite debootstrap docker-buildx docker-compose-v2 docker-doc rinse zfs-fuse | zfsutils
The following NEW packages will be installed:
  bridge-utils containerd dns-root-data dnsmasq-base docker.io pigz runc ubuntu-fan
0 upgraded, 8 newly installed, 0 to remove and 139 not upgraded.
Need to get 76.8 MB of archives.
After this operation, 289 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```



The screenshot shows a CloudWatch Metrics interface with the following details:

- Region:** N. Virginia
- User:** vodlabs/user3387521=SHINDE\_PRAJYOT\_BABAN @ 7782-6211-986
- Service:** Docker
- Filter:** docker --help
- Logs:** The log output shows the installation of Docker version 24.0.7 and its configuration as a system service.
- Log Stream:** i-05b0173781636f4ff (Master)
- Metrics:** PublicIPs: 44.201.176.188 PrivateIPs: 172.31.91.198

```
See 'docker --help'
ubuntu@ip-172-31-91-198:~$ docker --version
Docker version 24.0.7, build 24.0.7-0ubuntu4.1
ubuntu@ip-172-31-91-198:~$ sudo systemctl enable docker
ubuntu@ip-172-31-91-198:~$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: enabled)
     Active: active (running) since Wed 2024-09-25 08:08:37 UTC; 2min 30s ago
TriggeredBy: ● docker.socket
  Docs: https://docs.docker.com
 Main PID: 2264 (dockerd)
    Tasks: 9
   Memory: 25.5M (peak: 25.8M)
      CPU: 244ms
     CGroup: /system.slice/docker.service
             └─2264 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock

Sep 25 08:08:36 ip-172-31-91-198 systemd[1]: Starting docker.service - Docker Application Container Engine...
Sep 25 08:08:36 ip-172-31-91-198 dockerd[2264]: time="2024-09-25T08:08:36.501877155Z" level=info msg="Starting up"
Sep 25 08:08:36 ip-172-31-91-198 dockerd[2264]: time="2024-09-25T08:08:36.502549937Z" level=info msg="detected 127.0.0.53 nameserver, using it as the default gateway"
Sep 25 08:08:36 ip-172-31-91-198 dockerd[2264]: time="2024-09-25T08:08:36.657476258Z" level=info msg="Loading containers: start."
Sep 25 08:08:37 ip-172-31-91-198 dockerd[2264]: time="2024-09-25T08:08:37.106580687Z" level=info msg="Loading containers: done."
Sep 25 08:08:37 ip-172-31-91-198 dockerd[2264]: time="2024-09-25T08:08:37.124380691Z" level=info msg="Docker daemon" commit=24.0.7-0up
```

## Step 4:

### Install kubeadm, kubelet, kubectl:

```
aws Services Search [Alt+S] N. Virginia v vocabs/user3387521=SHINDE_PRAJYOT_BABAN @ 7782-6211-986
ubuntu@ip-172-31-91-198:~$ sudo apt-get update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
ubuntu@ip-172-31-91-198:~$ sudo apt-get install -y apt-transport-https ca-certificates curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ca-certificates is already the newest version (20240203).
ca-certificates set to manually installed.
The following additional packages will be installed:
  libcurl3t64-gnutls libcurl4t64
The following NEW packages will be installed:
  apt-transport-https
The following packages will be upgraded:
  curl libcurl3t64-gnutls libcurl4t64
3 upgraded, 1 newly installed, 0 to remove and 136 not upgraded.
Need to get 904 kB of archives.
After this operation, 38.9 kB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 apt-transport-https all 2.7.14build2 [3974 B]
```

```
aws Services Search [Alt+S] N. Virginia v vocabs/user3387521=SHINDE_PRAJYOT_BABAN @ 7782-6211-986
ubuntu@ip-172-31-91-198:~$ sudo apt-get update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
ubuntu@ip-172-31-91-198:~$ sudo apt-get install -y apt-transport-https ca-certificates curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ca-certificates is already the newest version (20240203).
ca-certificates set to manually installed.
The following additional packages will be installed:
  libcurl3t64-gnutls libcurl4t64
The following NEW packages will be installed:
  apt-transport-https
The following packages will be upgraded:
  curl libcurl3t64-gnutls libcurl4t64
3 upgraded, 1 newly installed, 0 to remove and 136 not upgraded.
Need to get 904 kB of archives.
After this operation, 38.9 kB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 apt-transport-https all 2.7.14build2 [3974 B]
```

```
aws Services Search [Alt+S] N. Virginia v vocabs/user3387521=SHINDE_PRAJYOT_BABAN @ 7782-6211-986
Processing triggers for libc-bin (2.39-0ubuntu8.2) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...
  systemctl restart packagekit.service

No containers need to be restarted.

No user sessions are running outdated binaries.

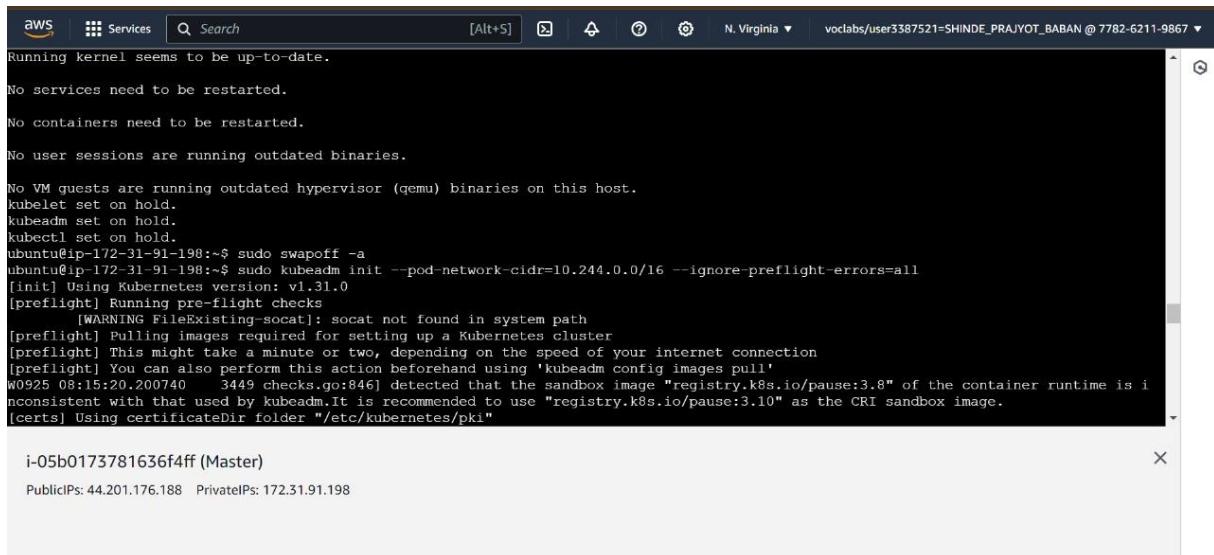
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-91-198:~$ curl -fsSL https://pkgs.k8s.io/core:/stable:/v1.31/deb/Release.key | sudo gpg --dearmor -o /etc/apt/keyrings/kubernetes-apt-keyring.gpg
ubuntu@ip-172-31-91-198:~$ echo 'deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:/v1.31/deb/' | sudo tee /etc/apt/sources.list.d/kubernetes.list
deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:/v1.31/deb/
ubuntu@ip-172-31-91-198:~$ sudo apt-get update
sudo apt-get install -y kubelet kubeadm kubectl
sudo apt-mark hold kubelet kubeadm kubectl
```

i-05b0173781636f4ff (Master)

PublicIPs: 44.201.176.188 PrivateIPs: 172.31.91.198

## Step5:

Disable Swap (Kubernetes requires swap to be off):



```
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.  
kubelet set on hold.  
kubeadm set on hold.  
kubectl set on hold.  
ubuntu@ip-172-31-91-198:~$ sudo swapoff -a  
ubuntu@ip-172-31-91-198:~$ sudo kubeadm init --pod-network-cidr=10.244.0.0/16 --ignore-preflight-errors=all  
[init] Using Kubernetes version: v1.31.0  
[preflight] Running pre-flight checks  
[WARNING FileExisting-socat]: socat not found in system path  
[preflight] Pulling images required for setting up a Kubernetes cluster  
[preflight] This might take a minute or two, depending on the speed of your internet connection  
[preflight] You can also perform this action beforehand using 'kubeadm config images pull'  
W0925 08:15:20.200740    3449 checks.go:846] detected that the sandbox image "registry.k8s.io/pause:3.8" of the container runtime is inconsistent with that used by kubelet. It is recommended to use "registry.k8s.io/pause:3.10" as the CRI sandbox image.  
[certs] Using certificateDir folder "/etc/kubernetes/pki"  
  
i-05b0173781636f4ff (Master)  
PublicIPs: 44.201.176.188 PrivateIPs: 172.31.91.198
```

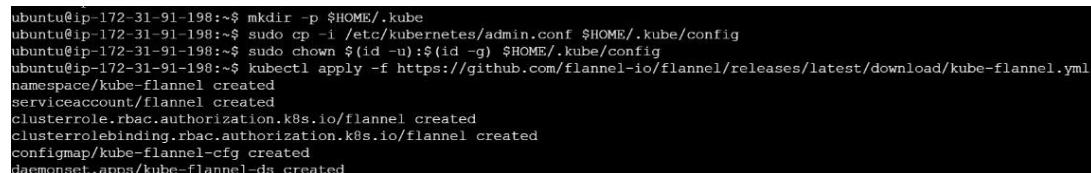
## Step 6:

**Initialize the Kubernetes Cluster on Master Node On the master node:** sudo

```
kubeadm init --pod-network-cidr=10.244.0.0/16
```

Set up kubectl on the master node:

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



```
ubuntu@ip-172-31-91-198:~$ mkdir -p $HOME/.kube  
ubuntu@ip-172-31-91-198:~$ sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config  
ubuntu@ip-172-31-91-198:~$ sudo chown $(id -u):$(id -g) $HOME/.kube/config  
ubuntu@ip-172-31-91-198:~$ 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
```

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 172.31.91.198:6443 --token 22ilrn.r4quqbb6kojruvxz \
--discovery-token-ca-cert-hash sha256:e0e897036572a9d7b7d82e441ee532a17499a55de8dee37e788e2b3e798a62ea
ubuntu@ip-172-31-91-198:~$ ^C
ubuntu@ip-172-31-91-198:~$ mkdir -p $HOME/.kube
```

NAMESPACE	NAME	READY	STATUS
RESTARTS	AGE		
kube-flannel	kube-flannel-ds-qmgdh	1/1	Running
0	3m47s		
kube-system	coredns-7c65d6cf9-42w2x	1/1	Running
0	9m56s		
kube-system	coredns-7c65d6cf9-8ctb6	1/1	Running
0	9m56s		
kube-system	etcd-maste-node	1/1	Running
0	10m		
kube-system	kube-apiserver-maste-node	1/1	Running
0	10m		
kube-system	kube-controller-manager-maste-node	1/1	Running
0	10m		
kube-system	kube-proxy-5g6gj	0/1	CrashLoopBackoff
7 (78s ago)	9m57s		
kube-system	kube-scheduler-maste-node	1/1	Running
0	10m		

## Step 7:

Join Worker Nodes to the Cluster On the worker nodes, run the command provided by the master node during initialization:

```
ubuntu@maste-node:~$ sudo kubeadm join 172.31.32.117:6443 --token t2jpj2.rauz0s7fimwpdo4a --discovery-token-ca-cert-hash sha256:b9cf34dd1cff8161d84586cd50b
```

## Step 8:

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

```
ubuntu@ip-172-31-91-198:~$ kubectl get nodes
NAME           STATUS    ROLES     AGE     VERSION
ip-172-31-80-216   Ready    <none>    14s    v1.31.1
ip-172-31-91-198   Ready    control-plane 3m35s   v1.31.1
```

## ADVANCE DEVOPS EXP 4

Name :- Prajyot Shinde

Roll no :- 57

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

**Step 1:** As the cluster is up and running, we can deploy our nginx server on this cluster.

```
ubuntu@ip-172-31-91-198:~$ kubectl get nodes
NAME           STATUS    ROLES     AGE      VERSION
ip-172-31-80-216   Ready    <none>    14s    v1.31.1
ip-172-31-91-198   Ready    control-plane   3m35s   v1.31.1
```

Apply this deployment file using this command to create a deployment.

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

```
ubuntu@ip-172-31-91-198:~$ kubectl create deployment nginx --image=nginx
deployment.apps/nginx created
```

**Step 2:** Verify the deployment using the command:

```
$kubectl get deployments
```

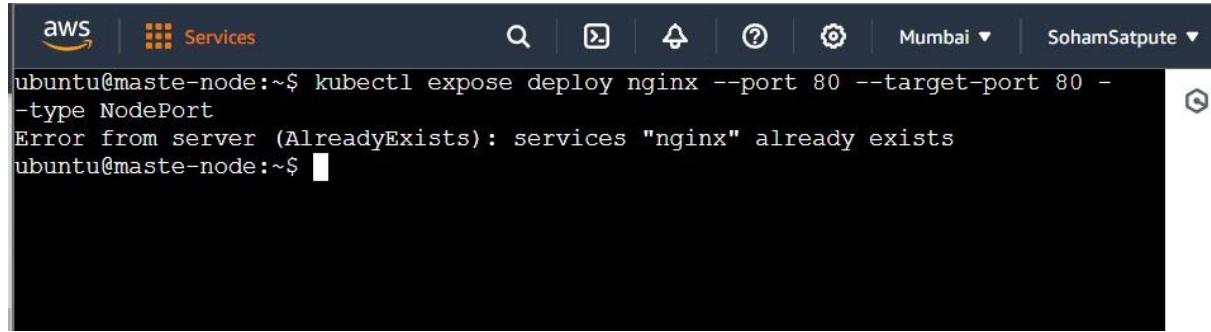
```

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@ip-172-31-91-198:~$ kubectl get nodes
NAME           STATUS    ROLES   AGE     VERSION
ip-172-31-80-216 Ready    <none>  14s    v1.31.1
ip-172-31-91-198 Ready    control-plane   3m35s   v1.31.1
ubuntu@ip-172-31-91-198:~$ kubectl create deployment nginx --image=nginx
deployment.apps/nginx created
ubuntu@ip-172-31-91-198:~$ kubectl get deployments
NAME      READY   UP-TO-DATE   AVAILABLE   AGE
nginx   1/1     1           1           28s
ubuntu@ip-172-31-91-198:~$ kubectl expose deploy nginx --port 80 --target-port 80 --type NodePort
service/nginx exposed
ubuntu@ip-172-31-91-198:~$ kubectl get services
NAME        TYPE      CLUSTER-IP   EXTERNAL-IP   PORT(S)        AGE
kubernetes  ClusterIP  10.96.0.1   <none>       443/TCP      6m6s
nginx       NodePort   10.110.120.152 <none>       80:31122/TCP  24s
ubuntu@ip-172-31-91-198:~$ ^C
ubuntu@ip-172-31-91-198:~$ 
```

i-05b0173781636f4ff (Master)  
PublicIPs: 44.201.176.188 PrivateIPs: 172.31.91.198

**Step 3:** Next, run the following command to create a service named nginx that will expose the app publicly. It will do so through a NodePort, a scheme that will make the pod accessible through an arbitrary port opened on each node of the cluster with this service type, Kubernetes will assign this service on ports on the **30000+** range.

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



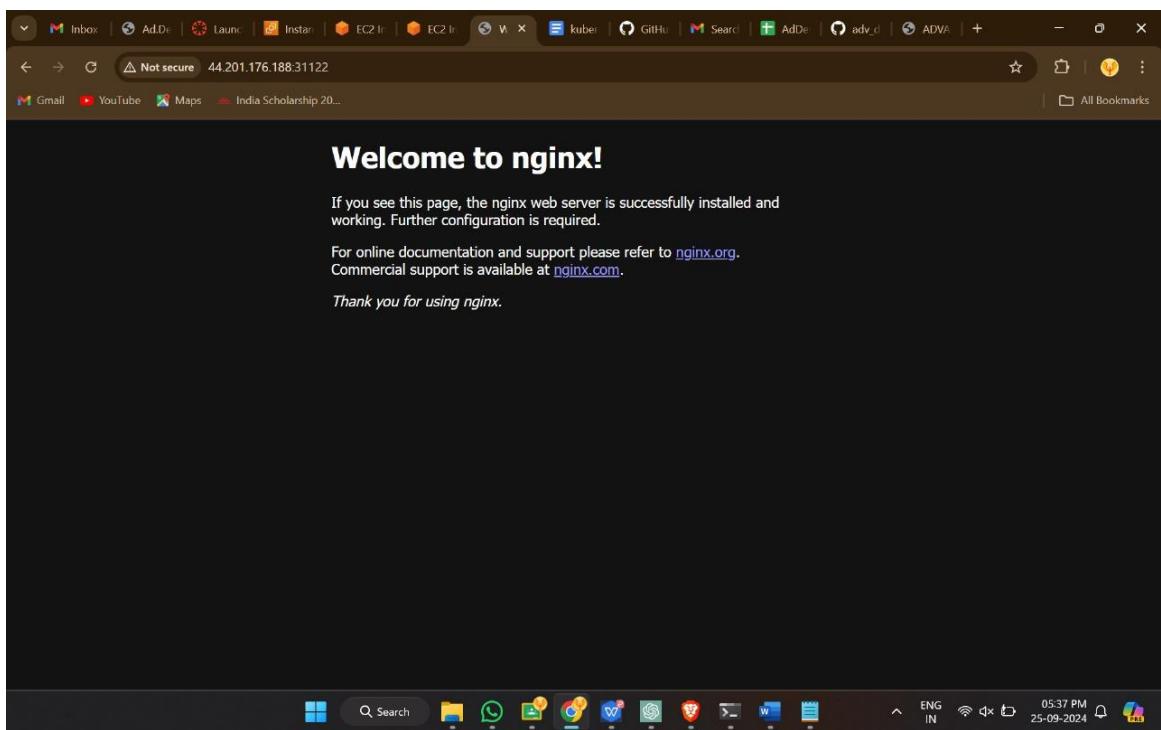
```
aws | Services | 🔍 | 🚧 | ⓘ | ⚙️ | Mumbai | SohamSatpute | ⓘ
ubuntu@maste-node:~$ kubectl expose deploy nginx --port 80 --target-port 80 -type NodePort
Error from server (AlreadyExists): services "nginx" already exists
ubuntu@maste-node:~$
```

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

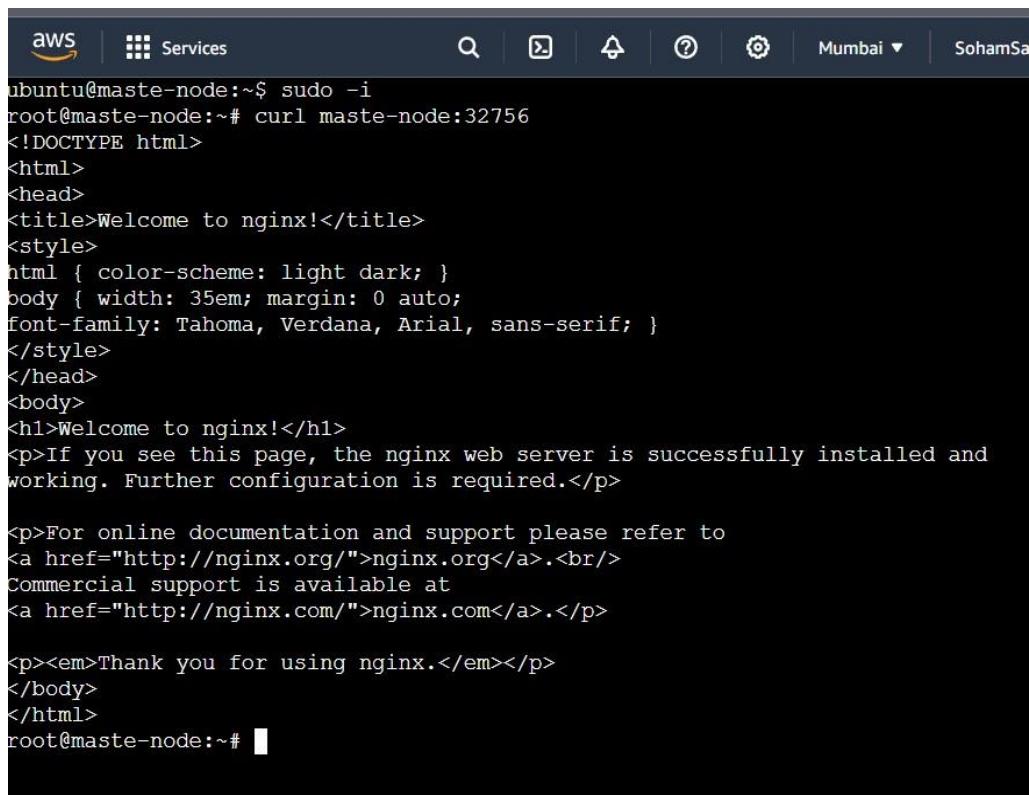
\$kubectl get services

```
ubuntu@ip-172-31-91-198:~$ kubectl get services
NAME      TYPE      CLUSTER-IP      EXTERNAL-IP      PORT(S)      AGE
kubernetes   ClusterIP   10.96.0.1      <none>        443/TCP      6m6s
nginx      NodePort    10.110.120.152   <none>        80:32756/TCP   24s
```

**Step 5:** Add the port which is displayed i.e. 32756(in our case ) in the inbound rules of the security group.



**Step 6:** Now you can verify that the Nginx page is reachable on all nodes using the curl command. As you can see, the “WELCOME TO NGINX!” page can be reached.



The screenshot shows a terminal window within the AWS CloudWatch interface. The terminal title is "ubuntu@maste-node:~\$". The user runs the command "sudo -i" and then "curl maste-node:32756". The response is the standard Nginx welcome page HTML code, indicating successful installation.

```
ubuntu@maste-node:~$ sudo -i
root@maste-node:~# curl maste-node:32756
<!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@maste-node:~#
```

**Step 7:** To test that everything is working, visit [http://worker\\_1\\_ip:nginx\\_port](http://worker_1_ip:nginx_port) or [http://worker\\_2\\_ip:nginx\\_port](http://worker_2_ip:nginx_port) through a browser on your local machine. You will see Nginx's familiar welcomepage.

<http://13.127.63.136:32756/>



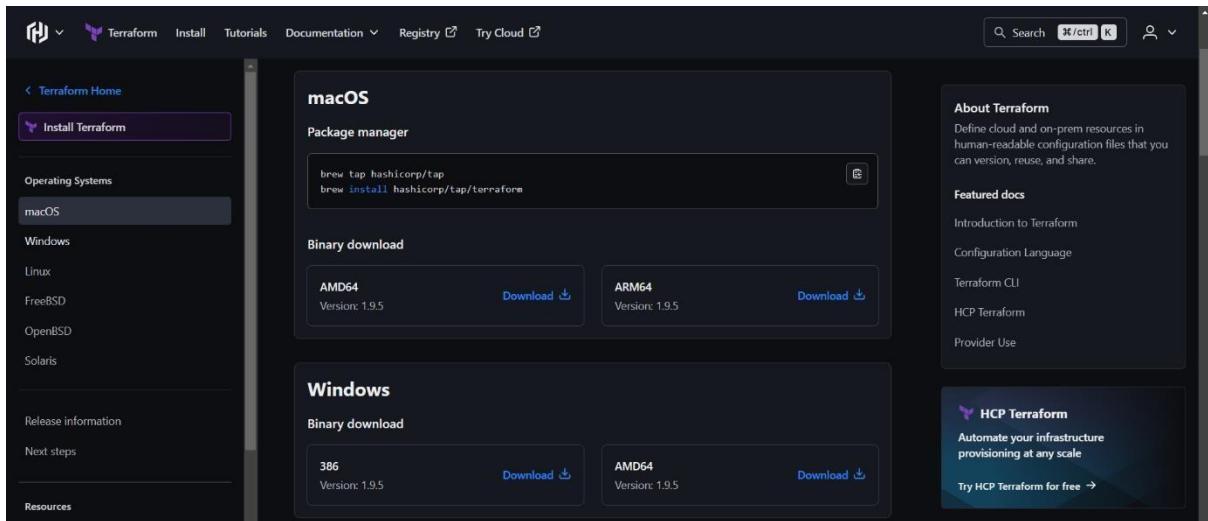
# Experiment no 5

Name :Prajyot Shinde

Roll no :- 57/D15A

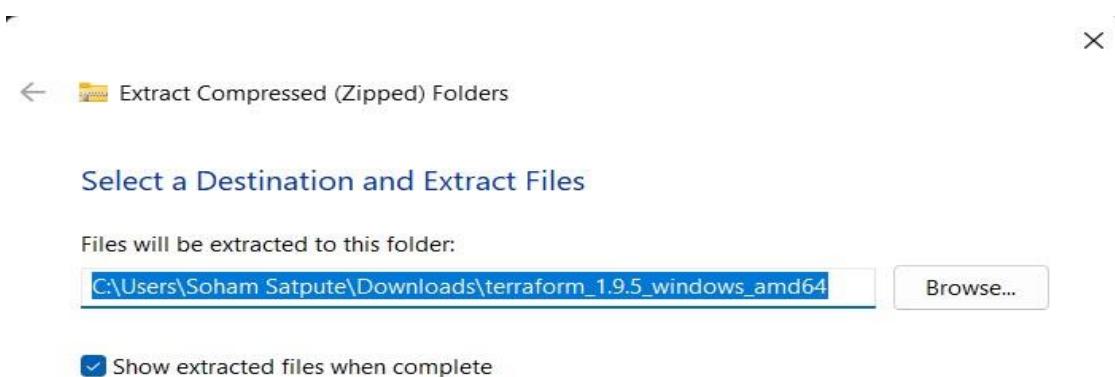
**Aim :-**Installation and Configuration of Terraform in Windows

**Installation for Windows :-**



**Step1:** In your Downloads, right-click on the downloaded Terraform binary file and select "**Extract All**" .

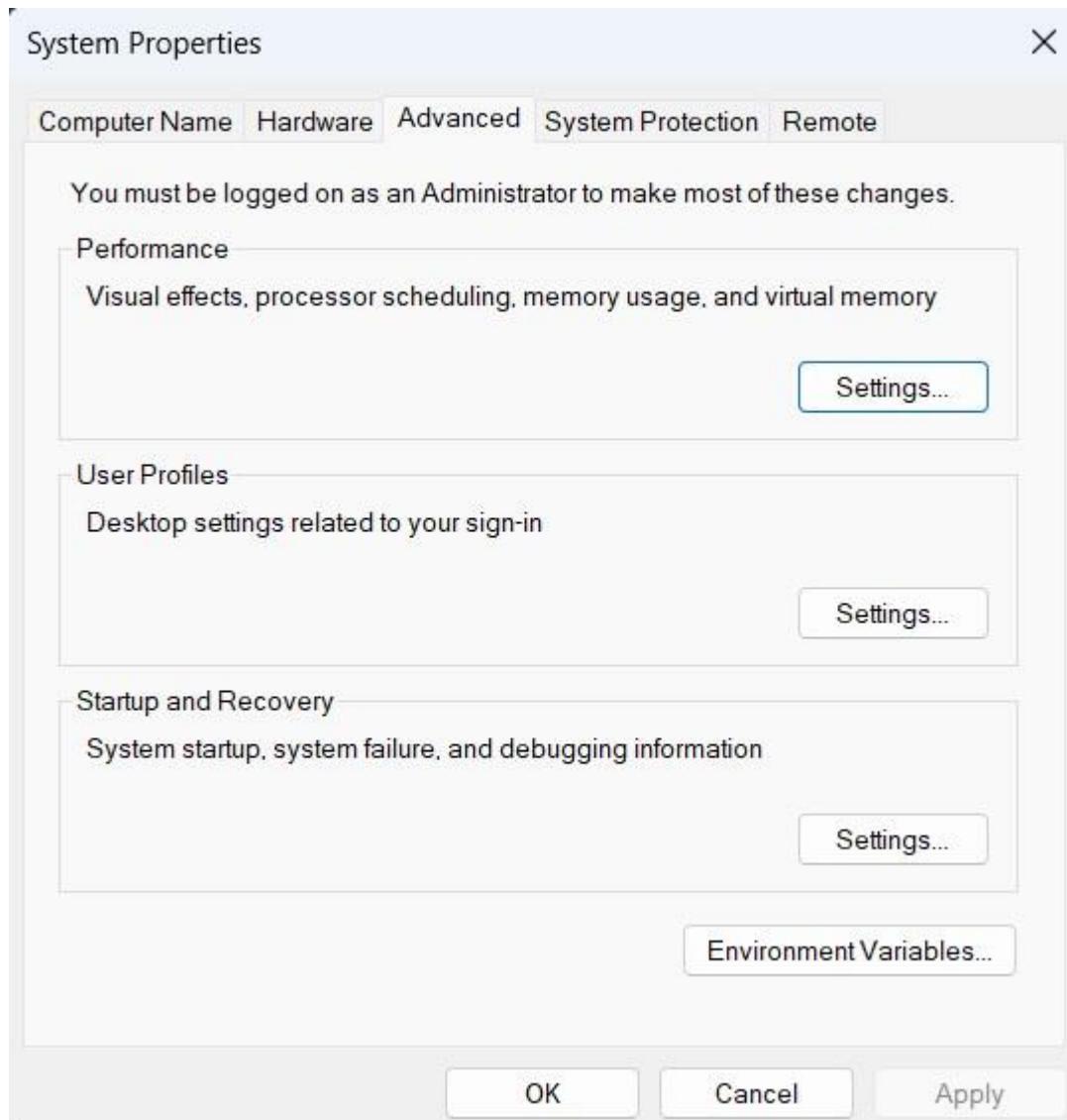
The following window will pop up:



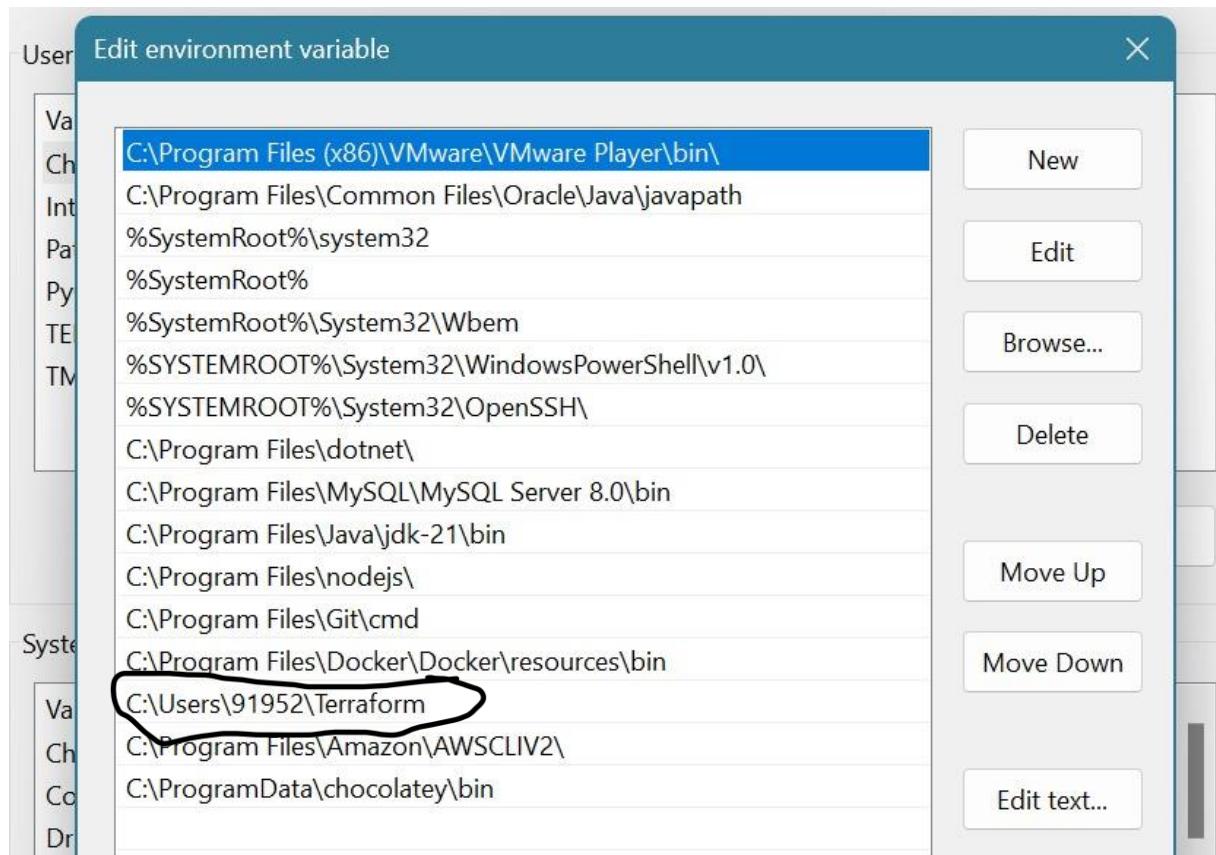
## Step 2 :

Set Terraform Path to System Environment Variables

Click on the “**Environment variables**” in the system properties:



### Step 3: Set the path



**Step 4:** Navigate to the folder path C:\terraform in a new command prompt window and type the terraform -version to verify the installed version.

```
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\91952>
```

**Step 5:** To see more Terraform commands, you can simply type terraform in the terminal.

```
Administrator: Windows Pow X + ▾
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\91952> terraform
Usage: terraform [global options] <subcommand> [args]

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

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

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



ENG IN 04:07 PM 20-08-2024

# Experiment no 6

Name :- Prajyot Shinde

Roll\_No :- 57

Aim :-

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

## Part A:Creating docker image using terraform

### Prerequisite:

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

### Step 1:Check Docker functionality

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

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

Management Commands:
  builder  Manage builds
  buildx*  Docker Buildx
  compose*  Docker Compose
  container  Manage containers
  context   Manage contexts
  debug*   Get a shell into any image or container
  desktop* Docker Desktop commands (Alpha)
  dev*    Docker Dev Environments
  extension* Manages Docker extensions
  feedback* Provide feedback, right in your terminal!
  image    Manage images
  init*   Creates Docker-related starter files for your project
  manifest Manage Docker image manifests and manifest lists
  network  Manage networks
  plugin   Manage plugins
  sbom*   View the packaged-based Software Bill Of Materials (SBOM) for an image
  scout*  Docker Scout
  system   Manage Docker
```

Check for the docker version with the following command

```
PS C:\Users\bhagy> docker --version
Docker version 27.1.1, build 6312585
PS C:\Users\bhagy> |
```

Now, create a folder named ‘Terraform Scripts’ in which we save our different types of scripts which will be further used in this experiment. Step 2: Firstly create a new folder named

‘Docker’ in the ‘TerraformScripts’ folder. Then create a new docker.tf file using Atom editor and write the following contents into it to create a Ubuntu Linux container.

**Script:-**

```
terraform {
  required_providers {
    docker = {
      source  = "kreuzwerker/docker"
      version = "2.25.0"
    }
  }
}
```

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

```
resource "docker_image" "ubuntu" {
  name = "ubuntu:latest"
}
```

```
resource "docker_container" "foo" {
  image  = docker_image.ubuntu.image_id
  name   = "foo"  command = ["sleep",
  "3600"]
}
```

```
VS Code
docker.tf
1  terraform {
2      required_providers {
3          docker = {
4              source  = "kreuzwerker/docker"
5              version = "2.25.0"
6          }
7      }
8  }
9
10 provider "docker" {
11     host = "npipe://./pipe//docker_engine"
12 }
13
14 resource "docker_image" "ubuntu" {
15     name = "ubuntu:latest"
16 }
17
18 resource "docker_container" "foo" {
19     image  = docker_image.ubuntu.image_id
20     name   = "foo"
21     command = ["sleep", "3600"]
22 }
23
```

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

```
PS E:\terraform_1.9.5_windows_386\Docker> terraform init
Initializing the backend...
Initializing provider plugins...
- Finding kreuzwerker/docker versions matching "~> 2.13"...
- Installing kreuzwerker/docker v2.25.0...
- Installed kreuzwerker/docker v2.25.0 (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
```

### Step 4: Execute Terraform plan to see the available resources

```
PS E:\terraform_1.9.5_windows_386\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)
    + container_read_refresh_timeout_milliseconds = 15000
    + 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                           = true
    + start                             = false
    + stdin_open                         = (known after apply)
    + stop_signal                        = (known after apply)
```

**Step 5 :** Type `terraform apply` to apply changes .

```

PS E:\terraform_1.9.5_windows_386\ 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)
    + container_read_refresh_timeout_milliseconds = 15000
    + 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)
}

# 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: Creation complete after 8s [id=sha256:edbf74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:1
at test]
docker_container.foo: Creating...

```

In 22 Col 1 Spaces: 4 UFT-8 CR LF Terraform Prettier

## Docker images , Before Executing Apply Step

```

PS E:\terraform_1.9.5_windows_386\ Docker> docker images
REPOSITORY TAG IMAGE ID CREATED SIZE

```

## Docker images , After Executing Apply Step

```

PS E:\terraform_1.9.5_windows_386\ Docker> docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
ubuntu latest edbf74c41f8 3 weeks ago 78.1MB

```

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

```
PS E:\terraform_1.9.5_windows_386\ Docker> terraform destroy
docker_image.ubuntu: Refreshing state... [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]

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

Terraform will perform the following actions:

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

Destroy complete! Resources: 1 destroyed.
```

## Docker images After Executing Destroy step

```
PS E:\terraform_1.9.5_windows_386\ Docker> docker images
REPOSITORY      TAG          IMAGE ID      CREATED      SIZE
```

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

### **Theory:**

Static application security testing (SAST), or static analysis, is a testing methodology that analyzes source code to find security vulnerabilities that make your organization's applications susceptible to attack. SAST scans an application before the code is compiled. It's also known as white box testing.

### **What problems does SAST solve?**

**SAST** takes place very early in the software development life cycle (SDLC) as it does not require a working application and can take place without code being executed. It helps developers identify vulnerabilities in the initial stages of development and quickly resolve issues without breaking builds or passing on vulnerabilities to the final release of the application.

**SAST** tools give developers real-time feedback as they code, helping them fix issues before they pass the code to the next phase of the SDLC. This prevents security-related issues from being considered an afterthought. SAST tools also provide graphical representations of the issues found, from source to sink. These help you navigate the code easier. Some tools point out the exact location of vulnerabilities and highlight the risky code. Tools can also provide in-depth guidance on how to fix issues and the best place in the code to fix them, without requiring deep security domain expertise. It's important to note that SAST tools must be run on the application on a regular basis, such as during daily/monthly builds, every time code is checked in, or during a code release.

### **Why is SAST important?**

Developers dramatically outnumber security staff. It can be challenging for an organization to find the resources to perform code reviews on even a fraction of its applications. A key strength of SAST tools is the ability to analyze 100% of the codebase. Additionally, they are much faster than manual secure code reviews performed by humans. These tools can scan millions of lines of code in a matter of minutes. SAST tools automatically identify critical vulnerabilities—such as buffer overflows, SQL injection, cross-site scripting, and others—with high confidence.

Thus, integrating static analysis into the SDLC can yield dramatic results in the overall quality of the code developed.

### **What are the key steps to run SAST effectively?**

There are six simple steps needed to perform SAST efficiently in organizations that have a very large number of applications built with different languages, frameworks, and platforms.

1. Finalize the tool. Select a static analysis tool that can perform code reviews of applications written in the programming languages you use. The tool should also be able to comprehend the underlying framework used by your software.
2. Create the scanning infrastructure, and deploy the tool. This step involves handling the licensing requirements, setting up access control and authorization, and procuring the resources required (e.g., servers and databases) to deploy the tool.
3. Customize the tool. Fine-tune the tool to suit the needs of the organization. For example, you might configure it to reduce false positives or find additional security vulnerabilities by writing new rules or updating existing ones. Integrate the tool into the build environment, create dashboards for tracking scan results, and build custom reports.
4. Prioritize and onboard applications. Once the tool is ready, onboard your applications. If you have a large number of applications, prioritize the high-risk applications to scan first. Eventually, all your applications should be onboarded and scanned regularly, with application scans synced with release cycles, daily or monthly builds, or code check-ins.
5. Analyze scan results. This step involves triaging the results of the scan to remove false positives. Once the set of issues is finalized, they should be tracked and provided to the deployment teams for proper and timely remediation.

6. Provide governance and training. Proper governance ensures that your development teams are employing the scanning tools properly. The software

security touchpoints should be present within the SDLC. SAST should be incorporated as part of your application development and deployment process.

### **Integrating Jenkins with SonarQube: Windows installation**

Step 1 Install JDK 1.8

Step 2 download and install  
jenkins

**installing-the-default-jre-**

**jdk** Step 1 Install JDK 1.8  
sudo apt-get install openjdk-  
8-jre sudo apt install default-  
jre /

### **how-to-install-jenkins-on-ubuntu-20-04**

### **Open SSH**

#### **Prerequisites:**

- Jenkins installed
- Docker Installed (for SonarQube)

(sudo apt-get install docker-ce=5:20.10.15~3-0~ubuntu-jammy docker-ce-  
cli=5:20.10.15~3-0~ubuntu-jammy containerd.io docker-compose-plugin)

- SonarQube Docker Image

```
C:\Users\91952>docker run -d --name sonarqube -p 9000:9000 sonarqube  
0392bc54d6d9ecd3e651c04433976aae2ab159b63bc07776b81a03ebf6e754b5
```

```
C:\Users\91952>docker image ls
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
postgres	latest	026d0ab72b34	7 weeks ago	611MB
sonarqube	latest	72e9feec7124	2 months ago	1.92GB

```
C:\Users\91952>
```

The screenshot shows a web browser window with the SonarQube interface. At the top, there is a navigation bar with links for Projects, Issues, Rules, Quality Profiles, Quality Gates, Administration, More, and a search bar. Below the navigation bar, the main content area displays a form for creating a new project. The form fields include:

- Project display name \*: sonarqube-test
- Project key \*: sonarqube-test
- Main branch name \*: main

Below the form, a warning message in a yellow box 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." There are "Cancel" and "Next" buttons at the bottom of the form.

# Prajyot Shinde 57/D15A

Ok so go to Jenkins dashboard and then go to Manage Jenkins then plugins , install plugins and then install “sonarqube scanner”

The screenshot shows the Jenkins Plugins page. The left sidebar has tabs for Updates (29), Available plugins, **Installed plugins**, and Advanced settings. The right panel shows a search bar and a list of installed plugins:

- Script Security 1.341.vc\_201904-414006 (Enabled)
- SnakeYAML API 2.2-111.vc6598e30cc65 (Enabled)
- SonarQube Scanner for Jenkins 2.17.2** (Enabled) - This plugin allows an easy integration of SonarQube, the open source platform for Continuous Inspection of code quality.
- SSH Build Agents plugin 2.973.v0fa\_8c0dea\_f9f (Enabled)
- SSH Credentials Plugin 343.v884f71d78167 (Enabled)

The screenshot shows the Jenkins Plugins page with a search bar containing "sona". The left sidebar is identical to the previous screenshot. The right panel shows the SonarQube Scanner plugin listed in the search results:

Name	Enabled
SonarQube Scanner for Jenkins 2.17.2	Enabled

At the bottom, there are links for REST API and Jenkins 2.462.2.

# Prajyot Shinde 57/D15A

Dashboard > Manage Jenkins > System >

SonarQube installations

List of SonarQube installations

Name: sonarqube

Server URL: http://localhost:9000

Server authentication token: - none -

Save Apply

Jenkins

Search (CTRL+K) ? 🔍 1 ⚡ 1 Prajyot Shinde log out

Dashboard > All > New Item

## New Item

Enter an item name: Sonarube

Select an item 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.
- Maven project**  
Build a maven project. Jenkins takes advantage of your POM files and drastically reduces the configuration.
- 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.

OK

# Prajyot Shinde 57/D15A

Dashboard > sonarQube > Configuration

## Configure

### Source Code Management

- General
- Source Code Management**
- Build Triggers
- Build Environment
- Build Steps
- Post-build Actions

None

Git [?](#)

#### Repositories [?](#)

##### Repository URL [?](#)

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

##### Credentials [?](#)

- none -

[+ Add](#) ▾

[Save](#)

[Apply](#)

Dashboard > sonarQube2 > Configuration

## Configure

### (INHERITED FROM SONARQUBE)

- General
- Source Code Management
- Build Triggers
- Build Environment
- Build Steps**
- Post-build Actions

#### Path to project properties [?](#)

#### Analysis properties [?](#)

```
sonar.projectKey=sonarqube  
sonar.login=sqp_018cb0bf9d002dc6c6c3f278248d119e5c2e0ab  
sonar.sources=HelloWorldCore  
sonar.host.url=http://localhost:9000
```

#### Additional arguments [?](#)

#### JVM Options [?](#)

[Save](#)

[Apply](#)

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration More Q ? A

## Administration

Configuration ▾ Security ▾ Projects ▾ System Marketplace

Administrator System [?](#) Administer System [?](#) Execute Analysis [?](#) Create [?](#)

A **sonar-administrators**  
System administrators



Quality Gates  
 Quality Profiles



Projects

A **sonar-users**  
Every authenticated user automatically belongs to this group



Quality Gates  
 Quality Profiles



Projects

A **Anyone DEPRECATED**  
Anybody who browses the application belongs to this group. If authentication is not enforced, assigned permissions also apply to non-authenticated users.



Quality Gates  
 Quality Profiles



Projects

A **Administrator admin**



Quality Gates  
 Quality Profiles



Projects

After 3 failures finally there was 4th success which is shown down below in image

The screenshot shows the Jenkins interface for the 'SonarQube' project. The top navigation bar includes links for 'Dashboard', 'SonarQube', 'Status' (which is currently selected), 'Changes', 'Workspace', 'Build Now', 'Configure', 'Delete Project', 'SonarQube', and 'Rename'. The main content area displays the 'SonarQube' project status with a green checkmark icon and the text 'SonarQube'. Below this is a 'Permalinks' section with a SonarQube logo. A list of builds is provided:

- Last build (#4), 1 min 45 sec ago
- Last stable build (#4), 1 min 45 sec ago
- Last successful build (#4), 1 min 45 sec ago
- Last failed build (#3), 16 min ago
- Last unsuccessful build (#3), 16 min ago
- Last completed build (#4), 1 min 45 sec ago

Below this is a 'Build History' section with a table showing two entries:

Build #	Date
#4	Sep 27, 2024, 3:25 PM
#3	Sep 27, 2024, 3:10 PM

The screenshot shows the Jenkins interface for the 'SonarQube' project, specifically for build #4. The top navigation bar includes links for 'Dashboard', 'SonarQube', '#4', and 'Console Output' (which is currently selected). The left sidebar shows options like 'Status', 'Changes', 'Console Output' (selected), 'Edit Build Information', 'Delete build #4', 'Timings', 'Git Build Data', and 'Previous Build'. The main content area displays the 'Console Output' for build #4. It starts with the message 'Started by user Prajyot Shinde' and continues with the Jenkins build process logs:

```
Started by user Prajyot Shinde
Running as SYSTEM
Building on the built-in node in workspace C:\ProgramData\Jenkins\.jenkins\workspace\SonarQube
The recommended git tool is: NONE
No credentials specified
> git.exe rev-parse --resolve-git-dir C:\ProgramData\Jenkins\.jenkins\workspace\SonarQube\.git # timeout=10
Fetching changes from the remote Git repository
> git.exe config remote.origin.url https://github.com/shazforiot/MSBuild_firstproject.git # timeout=10
Fetching upstream changes from https://github.com/shazforiot/MSBuild_firstproject.git
> git.exe --version # timeout=10
> git --version # 'git version 2.45.2.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 f2bc042c04c6e72427c380bcae6d6fee7b49adf (refs/remotes/origin/master)
> git.exe config core.sparsecheckout # timeout=10
> git.exe checkout -f f2bc042c04c6e72427c380bcae6d6fee7b49adf # timeout=10
Commit message: "updated"
> git.exe rev-list --no-walk f2bc042c04c6e72427c380bcae6d6fee7b49adf # timeout=10
Unpacking https://repo1.maven.org/maven2/org/sonarsource/scanner/cli/sonar-scanner-cli/6.2.0.4584/sonar-scanner-cli-6.2.0.4584.zip to
C:\ProgramData\Jenkins\.jenkins\tools\hudson.plugins.sonar.SonarRunnerInstallation\null on Jenkins
[sonarQube] $ C:\ProgramData\Jenkins\.jenkins\tools\hudson.plugins.sonar.SonarRunnerInstallation\null\bin\sonar-scanner.bat -
-Dsonar.host.url=http://localhost:9000 -Dsonar.projectKey=sonarqube-test -Dsonar.login=admin -Dsonar.host.url=http://localhost:9000 -
```

# Prajyot Shinde 57/D15A

The screenshot shows the SonarQube web interface for the project 'sonarqube-test / main'. The top navigation bar includes links for Projects, Issues, Rules, Quality Profiles, Quality Gates, Administration, More, and a search bar. The main content area displays a 'Quality Gate' status as 'Passed' (indicated by a green checkmark icon). A message states 'The last analysis has warnings. See details'. Below this, there are two tabs: 'New Code' (selected) and 'Overall Code'. The 'Overall Code' section contains six metrics: Security (0 Open issues, A grade), Reliability (0 Open issues, A grade), Maintainability (0 Open issues, A grade), Accepted issues (0), Coverage (represented by a blue progress bar), and Duplications (0.0%). The right side of the interface shows 'Project Settings' and 'Project Information' with a note about the 'Last analysis 3 minutes ago'.

## ADVANCE DEVOPS EXP 8

NAME: PRAJYOT SHINDE 57 / D15A

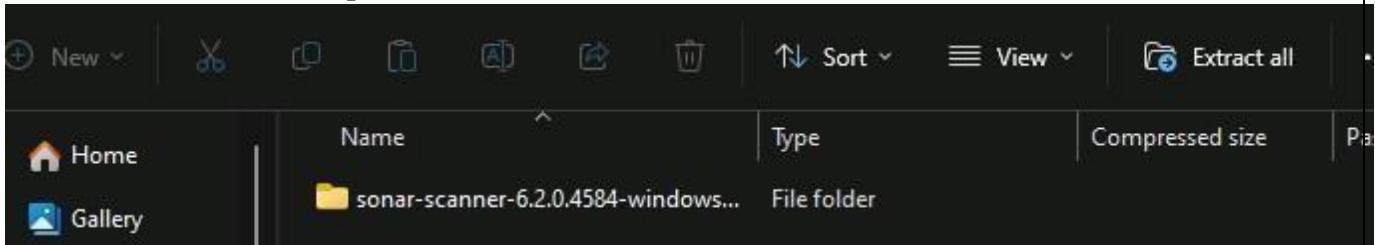
**Aim:** Create a Jenkins CICD Pipeline with SonarQube / GitLab Integration to perform a static analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web / Java / Python application.

**Step 1: Download sonar scanner** <https://docs.sonarsource.com/sonarqube/latest/analyzing-source-code/scanners/sonarscan>

The screenshot shows a web browser displaying the SonarScanner CLI documentation page. The URL in the address bar is <https://docs.sonarsource.com/sonarqube/latest/analyzing-source-code/scanners/sonarscan>. The page title is "SonarScanner CLI". On the left, there is a sidebar with navigation links for SonarQube and Docs 10.6, including "Homepage", "Try out SonarQube", "Server installation and setup", "Analyzing source code" (with "SonarQube analysis overview" and "Project analysis setup" sub-links), "Scanners", "Scanner environment", "SonarScanner CLI", "SonarQube extension for Azure DevOps", "SonarQube extension for Jenkins", "SonarScanner for .NET", and "SonarScanner for Maven". The main content area features a card for version 6.1, which was released on 2024-06-27. It mentions "macOS and Linux AArch64 distributions" and provides download links for "Linux x64", "Linux AArch64", "Windows x64", "macOS x64", "macOS AArch64", and "Docker Any (Requires a pre-installed JVM)". Below the card, release notes and a note about ARM support are displayed.

ner/ Visit this link and download the sonarqube scanner CLI.

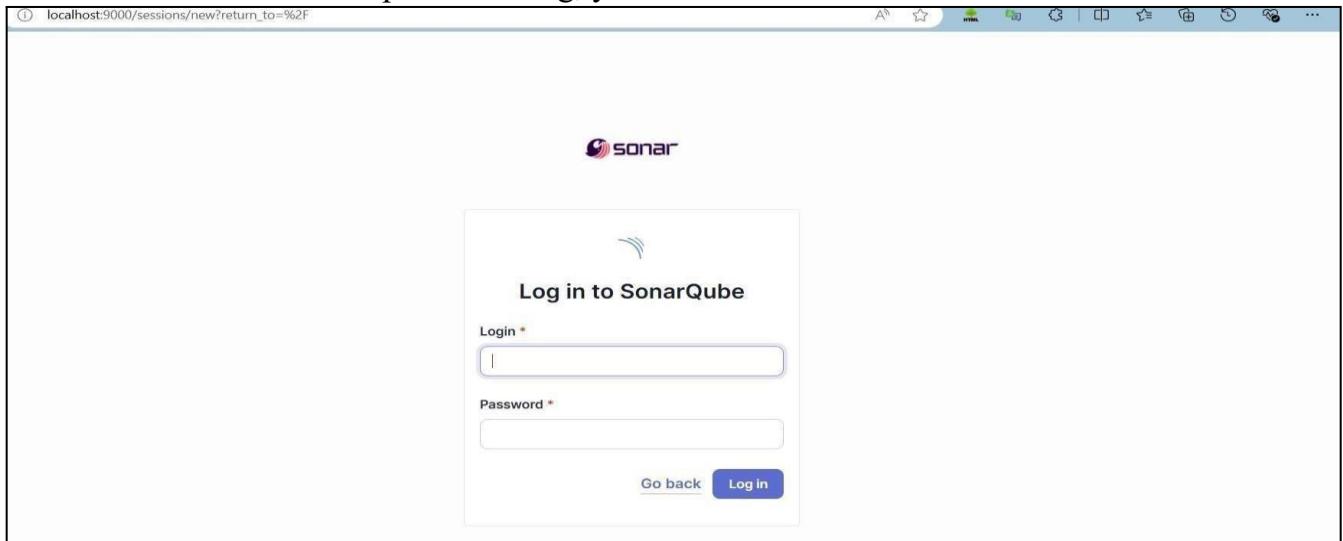
Extract the downloaded zip file in a folder.



1. Install sonarqube image Command: **docker pull sonarqube**

```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindc
PS C:\Users\Soham Satpute> docker pull sonarqube
Using default tag: latest
latest: Pulling from library/sonarqube
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Image is up to date for sonarqube:latest
docker.io/library/sonarqube:latest
```

2. Once the container is up and running, you can check the status of



SonarQube at localhost port 9000.

3. Login to SonarQube using username admin and password admin.

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration More Q

How do you want to create your project?

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

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

Import from Azure DevOps Setup Import from Bitbucket Cloud Setup Import from Bitbucket Server Setup

Import from GitHub Setup Import from GitLab Setup

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

Create a local project

4. Create a manual project in SonarQube with the name sonarqube

1 of 2

## Create a local project

Project display name \*

Sonarqube-test



Project key \*

Sonarqube-test



Main branch name \*

main

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

2 of 2

## Set up project for Clean as You Code

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

Choose the baseline for new code for this project

Use the global setting

Previous version

Any code that has changed since the previous version is considered new code.

Recommended for projects following regular versions or releases.

Define a specific setting for this project

Previous version

Any code that has changed since the previous version is considered new code.

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

The screenshot shows the Jenkins dashboard. On the left, there's a sidebar with links like 'New Item', 'Build History', 'Project Relationship', 'Check File Fingerprint', 'Manage Jenkins', and 'My Views'. Below these are two expandable sections: 'Build Queue' (No builds in the queue) and 'Build Executor Status' (1 Idle, 2 Idle). The main area displays a table of projects with columns: S (Status), W (Icon), Name, Last Success, Last Failure, and Last Duration. The projects listed are:

S	W	Name	Last Success	Last Failure	Last Duration
✓	☀️	DevOps Pipeline	2 mo 1 day #3	N/A	2.6 sec
✓	☀️	first-job	1 mo 5 days #4	N/A	1.6 sec
...	☀️	Git_Job	N/A	N/A	N/A
✗	🌧️	Maven-Project1	N/A	1 mo 5 days #5	2.7 sec
✗	☁️	my maven	2 mo 1 day #3	2 mo 1 day #5	12 sec
✓	☀️	My-Maven	2 hr 16 min #5	N/A	56 sec

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

The screenshot shows the Jenkins 'Manage Jenkins > Plugins' page. The search bar contains 'sonarq'. The results table shows one plugin entry:

Install	Name	Released
<input type="checkbox"/>	SonarQube Scanner 2.17.2	6 mo 29 days ago

Details for the SonarQube Scanner plugin:

- External Site/Tool Integrations
- Build Reports
- This plugin allows an easy integration of SonarQube, the open source platform for Continuous Inspection of code quality.

The screenshot shows the Jenkins 'Manage Jenkins > Plugins' page with the 'Download progress' tab selected. The table shows the progress of the SonarQube Scanner plugin download:

Preparation	
• Checking internet connectivity	
• Checking update center connectivity	
• Success	

Success messages:

- SonarQube Scanner: Success
- Loading plugin extensions: Success

Buttons at the bottom:

- 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

- 7.Under Jenkins ‘Manage Jenkins’ then go to ‘system’, scroll and look for SonarQube

The screenshot shows the Jenkins configuration interface for tools. Under the 'SonarQube' section, the 'Name' field is set to 'sonarqube'. The 'Server URL' field contains 'http://localhost:9000', with a note that it's the default. The 'Server authentication token' dropdown is set to '- none -', and there is a '+ Add' button. An 'Advanced' dropdown menu is partially visible.

**Servers** and enter the details.

The screenshot shows the Jenkins configuration interface for tools. It lists several sections: 'Gradle installations' (with an 'Add Gradle' button), 'SonarScanner for MSBuild installations' (with an 'Add SonarScanner for MSBuild' button), 'SonarQube Scanner installations' (with an 'Add SonarQube Scanner' button), and 'Ant installations'. The 'SonarQube Scanner installations' section is currently active.

Enter the Server Authentication token if needed.

In SonarQube installations: Under **Name** add <project name of sonarqube> for me  
**adv\_devops\_7\_sonarqube**

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

8. Search for SonarQube Scanner under Global Tool Configuration.  
 Choose the latest configuration and choose Install automatically.

**Dashboard > Manage Jenkins > Tools**

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

## 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

Save

Apply

9. After configuration, create a New Item → choose a pipeline project.

## New Item

Enter an item name

AdDevops-8

Select an item 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.



## Maven project

Build a maven project. Jenkins takes advantage of your POM files and drastically reduces the configuration.



## 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.



## Multi-configuration project

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

OK

10. Under Pipeline script, enter the following:

```
node {  
    stage('Cloning the GitHub Repo') { git  
        'https://github.com/shazforiot/GOL.git'  
    } stage('SonarQube  
  
analysis') {  
  
    withSonarQubeEnv('<Name_of_SonarQube_environment_on_Jenk  
i ns>') { sh """"  
        <PATH_TO SONARQUBE_SCANNER_FOLDER>/bin/sonar-scanner \  
        -D sonar.login=<SonarQube_USERNAME> \  
        -D sonar.password=<SonarQube_PASSWORD> \  
        -D sonar.projectKey=<Project_KEY> \  
        -D sonar.exclusions=vendor/**,resources/**,**/*.java \  
        -D sonar.host.url=<SonarQube_URL>(default: http://localhost:9000/)  
        """"  
    }  
}  
}
```

It is a java sample project which has a lot of repetitions and issues that will be detected by SonarQube.

Jenkins

Search (CTRL+K)

Prajyot Shinde log out

Dashboard > SonarQube-Pipeline >

Status SonarQube-Pipeline Add description

</> Changes

Build Now

Configure

Delete Pipeline

Full Stage View

SonarQube

Stages

Rename

Pipeline Syntax

Build History trend

Average stage times:  
Average full run time: ~1min

Cloning the GitHub Repo	SonarQube analysis	Declarative: Post Actions
2s	1min 53s	393ms
1s	11min 54s	
1s	144ms	failed
1s	1min 29s	426ms

#14 Sep 30 15:07 No Changes 56s 1s 11min 54s

#13 Sep 30 15:05 No Changes 1s 144ms failed

#12 Sep 30 14:56 No Changes 1s 1min 29s 426ms

## 11.Check console

Jenkins

Search (CTRL+K)

Prajyot Shinde log out

Dashboard > SonarQube-Pipeline > #14

Status Console Output Full Log

</> Changes

Console Output

View as plain text

Edit Build Information

Delete build #14'

Timings

Git Build Data

Pipeline Overview

Pipeline Console

Replay

Pipeline Steps

```
Skipping 4,248 KB.. Full Log
15:16:52.071 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 798. Keep only the first 100 references.
15:16:52.071 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 810. Keep only the first 100 references.
15:16:52.071 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 823. Keep only the first 100 references.
15:16:52.071 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 844. Keep only the first 100 references.
15:16:52.071 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 509. Keep only the first 100 references.
15:16:52.071 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 1065. Keep only the first 100 references.
15:16:52.072 WARN Too many duplication references on file gameoflife-
```

## 12.Now, check the project in SonarQube:

SonarQube Projects Issues Rules Quality Profiles Quality Gates Administration More ? A

sonarqube-test / main ?

Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information

main 683k Lines of Code Version not provided Set as homepage Last analysis 8 hours ago

Quality Gate Passed

New Code Overall Code

Security 0 Open issues A

Reliability 68k Open issues C

Maintainability 164k Open issues A

## 13.code problems consistency:

My Issues All Bulk Change Select issues Navigate to issue 210,549 issues 3135d effort

Filters

Issues in new code

Clean Code Attribute

- Consistency 197k
- Intentionality 14k
- Adaptability 0
- Responsibility 0

Software Quality

gameoflife-acceptance-tests/Dockerfile

Use a specific version tag for the image. Intentionality Maintainability No tags

Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. Intentionality Maintainability No tags

## 14. Intentionality:

The screenshot shows the SonarQube interface for the project "gameoflife-acceptance-tests/Dockerfile". The left sidebar displays various code attribute filters, including "Intentionality" which is selected and highlighted in blue. The main panel lists three specific issues under the "Intentionality" category:

- Issue 1: "Use a specific version tag for the image." (Maintainability) - Status: Open
- Issue 2: "Surround this variable with double quotes; otherwise, it can lead to unexpected behavior." (Maintainability) - Status: Open
- Issue 3: "Surround this variable with double quotes; otherwise, it can lead to unexpected behavior." (Maintainability) - Status: Open

At the top right, the statistics are shown as 13,887 issues and 59d effort.

## 15. Bugs

The screenshot shows the SonarQube interface for the project "gameoflife-core/build/reports/all-tests.html". The left sidebar displays various software quality and bug filters, with "Bug" selected and highlighted in blue. The main panel lists two specific bugs under the "Bug" category:

- Issue 1: "Add "lang" and/or "xml:lang" attributes to this "<html>" element." (Reliability) - Status: Open
- Issue 2: "Add "<th>" headers to this "<table>". (Reliability) - Status: Open

At the top right, the statistics are shown as 13,619 issues and 56d effort. A warning message at the bottom states: "Embedded database should be used for evaluation purposes only".

## Code smells:

SonarQube-test / main

Issues

Overview Security Hotspots Measures Code Activity Project Settings Project Information

Type: 1 Bug: 14k Vulnerability: 0 Code Smell: 253

Add to selection Ctrl + click

Scope

Status

Security Category

gameoflife-web/tools/jmeter/printable\_docs/building.html

Add an "alt" attribute to this image. Intentionality Reliability Open Not assigned L29 + 5min effort ~ 4 years ago Code Smell Minor

gameoflife-web/tools/jmeter/printable\_docs/changes.html

Add an "alt" attribute to this image. Intentionality Reliability Open Not assigned L31 + 5min effort ~ 4 years ago Code Smell Minor

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

SonarQube™ technology is powered by SonarSource SA

Community Edition v10.6 (92116) ACTIVE GPL v3 Community Documentation Plugins Web API

## Duplications:

SonarQube-test / main

Measures

Overview Issues Security Hotspots Code Activity Project Settings Project Information

Coverage

Duplications

Overview New Code Duplicated Lines: 0 Duplicated Blocks: 0 Overall Code Density: 50.6% Duplicated Lines: 384,007

Duplications Overview (Only showing data for the first 500 files)  
See the data presented on this chart as a list

Size: Duplicated Blocks

Zoom: 100%

Duplicated Lines

localhost:9000/component\_measures?metric=Duplications&id=SonarQube-test#

## Cyclomatic Complexities:

The screenshot shows the SonarQube interface for the project "Sonarqube-test". The top navigation bar includes links for Overview, Issues, Security Hotspots, Measures (which is the active tab), Code, and Activity. On the right, there are Project Settings and Project Information options. The main content area is divided into two sections: a sidebar on the left and a detailed view on the right.

**Measures Sidebar Data:**

Measure	Value
Duplicated Blocks	0
Overall Code	
Density	50.6%
Duplicated Lines	384,007
Duplicated Blocks	42,799
Duplicated Files	979

**Complexity Sidebar Data:**

Complexity Type	Value
Cyclomatic Complexity	1,112

**Issues Sidebar Data:**

Issue Type	Count
Issues	>

**Main View Data (Cyclomatic Complexity):**

Category	Complexity	Last Updated
Sonarqube-test	1,112	See history
gameoflife-acceptance-tests	—	
gameoflife-build	—	
gameoflife-core	18	
gameoflife-deploy	—	
gameoflife-web	1,094	

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

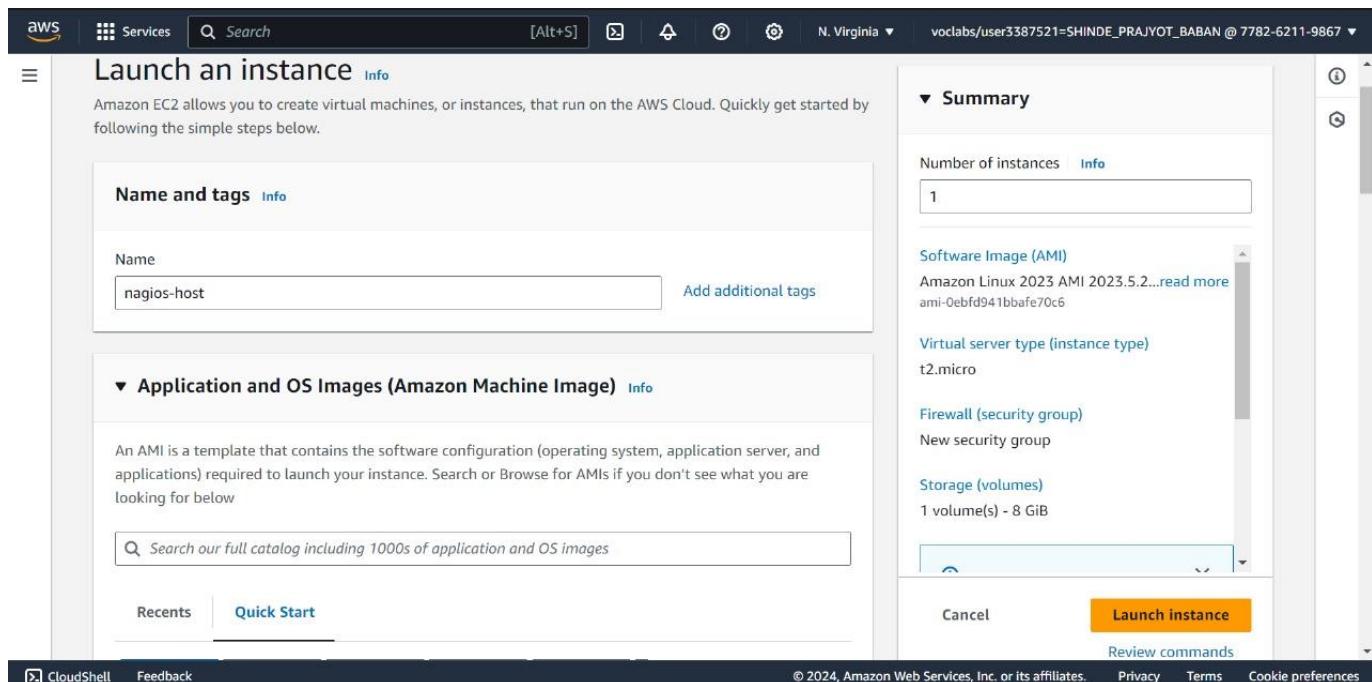
## ADVANCE DEVOPS EXP 9

Name :- Prajyot Shinde

Roll no :- 57

**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



### 2. Configure Security Group

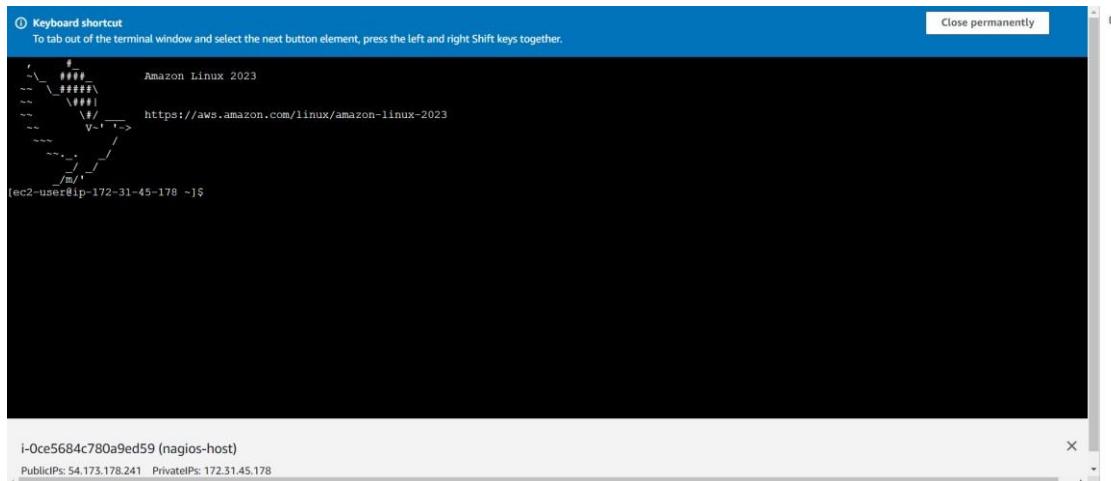
- Ensure HTTP, HTTPS, SSH, and ICMP are open from everywhere.
- Edit the inbound rules of the specified Security Group

Inbound rules

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-00d59807a11e25687	All ICMP - IPv4	ICMP	All	Custom	Q. 0.0.0.0/0 X
sgr-0ae620ec0b187c4a7	All traffic	All	All	Custom	Q. 0.0.0.0/0 X
sgr-0775d4388ffe14db6	SSH	TCP	22	Custom	Q. 0.0.0.0/0 X
sgr-0ebadedcb97cb60fc	HTTP	TCP	80	Custom	Q. 0.0.0.0/0 X
sgr-08985e0020306b273	HTTPS	TCP	443	Custom	Q. 0.0.0.0/0 X

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

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



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

```
[ec2-user@ip-172-31-40-254 ~]$ sudo yum update
Last metadata expiration check: 0:01:31 ago on Wed Oct  2 05:48:47 2024.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-172-31-40-254 ~]$
```

sudo yum install httpd php

```
[ec2-user@ip-172-31-40-254 ~]$ sudo yum install httpd php
Last metadata expiration check: 0:01:59 ago on Wed Oct 2 05:48:47 2024.
Dependencies resolved.
=====
| Package           | Architecture | Version      | Repository | Size
|=====|
| Installing:
|   httpd          | x86_64       | 2.4.62-1.amzn2023
|   php8.3         | x86_64       | 8.3.10-1.amzn2023.0.1
| Installing dependencies:
|   apr            | x86_64       | 1.7.2-2.amzn2023.0.2
|   apr-util        | x86_64       | 1.6.3-1.amzn2023.0.1
|   generic-logos-httpd | noarch     | 18.0.0-12.amzn2023.0.3
|   httpd-core      | x86_64       | 2.4.62-1.amzn2023
|   httpd-filesystem | noarch     | 2.4.62-1.amzn2023
|   httpd-tools      | x86_64       | 2.4.62-1.amzn2023
|   libbrotli        | x86_64       | 1.0.9-4.amzn2023.0.2
|   libbsd           | x86_64       | 1.0.19-4.amzn2023
|   libxml2          | x86_64       | 1.1.34-5.amzn2023.0.2
|   mailcap          | noarch     | 2.1.49-3.amzn2023.0.3
|   nginx-filesystem | noarch     | 1:1.24.0-1.amzn2023.0.4
|   php8.3-cli       | x86_64       | 8.3.10-1.amzn2023.0.1
|   php8.3-common    | x86_64       | 8.3.10-1.amzn2023.0.1
|   php8.3-process   | x86_64       | 8.3.10-1.amzn2023.0.1
|=====
| Repository | Size
| amazonlinux | 48 M
| amazonlinux | 10 M
| amazonlinux | 129 M
| amazonlinux | 98 M
| amazonlinux | 19 M
| amazonlinux | 1.4 M
| amazonlinux | 14 M
| amazonlinux | 81 M
| amazonlinux | 315 M
| amazonlinux | 176 M
| amazonlinux | 241 M
| amazonlinux | 33 M
| amazonlinux | 9.8 M
| amazonlinux | 3.7 M
| amazonlinux | 737 M
| amazonlinux | 45 M
```

sudo yum install gcc glibc glibc-common

```
[ec2-user@ip-172-31-40-254 ~]$ sudo yum install gcc glibc glibc-common
Last metadata expiration check: 0:02:41 ago on Wed Oct 2 05:48:47 2024.
Package glibc-2.34-52.amzn2023.0.11.x86_64 is already installed.
Package glibc-common-2.34-52.amzn2023.0.11.x86_64 is already installed.
Dependencies resolved.
=====
| Package           | Architecture | Version      | Repository | Size
|=====|
| Installing:
|   gcc             | x86_64       | 11.4.1-2.amzn2023.0.2
| Installing dependencies:
|   annobin-docs    | noarch     | 10.93-1.amzn2023.0.1
|   annobin-plugin-gcc | x86_64       | 10.93-1.amzn2023.0.1
|   cpp             | x86_64       | 11.4.1-2.amzn2023.0.2
|   gc              | x86_64       | 8.0.4-5.amzn2023.0.2
|   glibc-devel     | x86_64       | 2.34-52.amzn2023.0.11
|   glibc-headers-x86 | noarch     | 2.34-52.amzn2023.0.11
|   guile22        | x86_64       | 2.2.7-2.amzn2023.0.3
|   kernel-headers  | x86_64       | 6.1.109-118.189.amzn2023
|   libmpc          | x86_64       | 1.2.1-2.amzn2023.0.2
|   libtool-ltdl    | x86_64       | 2.4.7-1.amzn2023.0.3
|   libxcrypt-devel | x86_64       | 4.4.33-7.amzn2023
|   make            | x86_64       | 1:4.3-5.amzn2023.0.2
|=====
| Repository | Size
| amazonlinux | 32 M
| amazonlinux | 92 M
| amazonlinux | 887 M
| amazonlinux | 10 M
| amazonlinux | 105 M
| amazonlinux | 27 M
| amazonlinux | 427 M
| amazonlinux | 6.4 M
| amazonlinux | 1.4 M
| amazonlinux | 62 M
| amazonlinux | 38 M
| amazonlinux | 32 M
| amazonlinux | 534 M
```

Transaction Summary

sudo yum install gd gd-devel

```
[ec2-user@ip-172-31-40-254 ~]$ sudo yum install gd gd-devel
Last metadata expiration check: 0:03:46 ago on Wed Oct 2 05:48:47 2024.
Dependencies resolved.
=====
| Package           | Architecture | Version      | Repository | Size
|=====|
| Installing:
|   gd              | x86_64       | 2.3.3-5.amzn2023.0.3
|   gd-devel        | x86_64       | 2.3.3-5.amzn2023.0.3
| Installing dependencies:
|   brotli          | x86_64       | 1.0.9-4.amzn2023.0.2
|   brotli-devel    | x86_64       | 1.0.9-4.amzn2023.0.2
|   bzlib2-devel    | x86_64       | 1.0.8-6.amzn2023.0.2
|   cairo           | x86_64       | 1.17.6-6.amzn2023.0.1
|   cmake-filesystem | x86_64       | 3.22.2-1.amzn2023.0.4
|   fontconfig      | x86_64       | 2.13.94-2.amzn2023.0.2
|   fontconfig-devel | x86_64       | 2.13.94-2.amzn2023.0.2
|   fonts-filesystem | noarch     | 1:2.0.5-12.amzn2023.0.2
|   freetype         | x86_64       | 2.13.2-5.amzn2023.0.1
|   freetype-devel   | x86_64       | 2.13.2-5.amzn2023.0.1
|   glibc-devel      | x86_64       | 2.74.7-689.amzn2023.0.2
|   google-noto-fonts-common | noarch     | 20201206-2.amzn2023.0.2
|   google-noto-sans-vf-fonts | noarch     | 20201206-2.amzn2023.0.2
|   graphite2         | x86_64       | 1.3.14-7.amzn2023.0.2
|   graphite2-devel   | x86_64       | 1.3.14-7.amzn2023.0.2
|   harfbuzz          | x86_64       | 7.0.0-2.amzn2023.0.1
|   harfbuzz-devel    | x86_64       | 7.0.0-2.amzn2023.0.1
|   harfbuzz-icu      | x86_64       | 7.0.0-2.amzn2023.0.1
|=====
| Repository | Size
| amazonlinux | 139 M
| amazonlinux | 38 M
| amazonlinux | 314 M
| amazonlinux | 31 M
| amazonlinux | 214 M
| amazonlinux | 684 M
| amazonlinux | 16 M
| amazonlinux | 128 M
| amazonlinux | 9.5 M
| amazonlinux | 423 M
| amazonlinux | 912 M
| amazonlinux | 496 M
| amazonlinux | 15 M
| amazonlinux | 492 M
| amazonlinux | 97 M
| amazonlinux | 21 M
| amazonlinux | 868 M
| amazonlinux | 404 M
| amazonlinux | 18 M
```

**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-172-31-40-254 ~]$ sudo adduser -m nagios
[ec2-user@ip-172-31-40-254 ~]$ sudo passwd nagios
Changing password for user nagios.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[ec2-user@ip-172-31-40-254 ~]$
```

## 6. Create a new user group sudo groupadd nagcmd

```
[ec2-user@ip-172-31-40-254 ~]$ sudo groupadd nagcmd  
[ec2-user@ip-172-31-40-254 ~]$ █
```

## 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-172-31-40-254 ~]$ sudo groupadd nagcmd  
[ec2-user@ip-172-31-40-254 ~]$ sudo usermod -a -G nagcmd nagios  
sudo usermod -a -G nagcmd apache  
[ec2-user@ip-172-31-40-254 ~]$ █
```

## 8. Create a new directory for Nagios downloads mkdir ~/downloads cd ~/downloads

```
[ec2-user@ip-172-31-40-254 ~]$ mkdir ~/downloads  
cd ~/downloads  
[ec2-user@ip-172-31-40-254 downloads]$ █
```

## 9. Use wget to download the source zip files.

Wget <https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz> wget

```
[ec2-user@ip-172-31-40-254 downloads]$ Wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz  
wget: https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz  
-bash: Wget: command not found  
--2024-10-02 06:15:45-- https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz  
Resolving nagios-plugins.org (nagios-plugins.org)... 45.56.123.251  
Connecting to nagios-plugins.org (nagios-plugins.org)|45.56.123.251|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 2782610 (2.7M) [application/x-gzip]  
Saving to: 'nagios-plugins-2.3.3.tar.gz'  
  
nagios-plugins-2.3.3.tar.gz          0%[=====]  
nagios-plugins-2.3.3.tar.gz      23%[=====>]  
nagios-plugins-2.3.3.tar.gz    100%[=====>]  632.00K 3.02MB/s  
                                         ==>] 2.65M 8.10MB/s   in 0.3s  
  
2024-10-02 06:15:46 (8.10 MB/s) - 'nagios-plugins-2.3.3.tar.gz' saved [2782610/2782610]  
[ec2-user@ip-172-31-40-254 downloads]$ █
```

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

```
[ec2-user@ip-172-31-40-254 downloads]$ wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz  
wget: https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz  
Resolving assets.nagios.com (assets.nagios.com)... 45.79.49.120, 2600:3c00:f03c:92ff:fe17:4cce  
Connecting to assets.nagios.com (assets.nagios.com)|45.79.49.120|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 11333414 (11M) [application/x-gzip]  
Saving to: 'nagios-4.4.6.tar.gz'  
  
nagios-4.4.6.tar.gz          0%[=====]  
nagios-4.4.6.tar.gz      4%[==>]  
nagios-4.4.6.tar.gz    30%[=====>]  
nagios-4.4.6.tar.gz    63%[=====>]  
nagios-4.4.6.tar.gz    96%[=====>]  
nagios-4.4.6.tar.gz  100%[=====>]  495.62K 2.40MB/s  
                                         ==>] 3.26M 7.99MB/s  
                                         ==>] 6.91M 11.0MB/s  
                                         ==>] 10.46M 12.6MB/s  
                                         ==>] 10.81M 12.9MB/s   in 0.8s  
  
2024-10-02 06:17:25 (12.9 MB/s) - 'nagios-4.4.6.tar.gz' saved [11333414/11333414]  
[ec2-user@ip-172-31-40-254 downloads]$ █
```

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

```
tar zxvf nagios-4.4.6.tar.gz cd  
nagios-4.4.6
```

```
[ec2-user@ip-172-31-40-254 downloads]$ tar zxvf nagios-4.4.6.tar.gz
nagios-4.4.6/
nagios-4.4.6/.gitignore
nagios-4.4.6/.travis.yml
nagios-4.4.6/CONTRIBUTING.md
nagios-4.4.6/Changelog
nagios-4.4.6/INSTALLING
nagios-4.4.6/LEGAL
nagios-4.4.6/LICENSE
nagios-4.4.6/Makefile.in
nagios-4.4.6/README.md
nagios-4.4.6/THANKS
nagios-4.4.6/UPGRADING
nagios-4.4.6/aclocal.m4
nagios-4.4.6/autoconf-macros/
nagios-4.4.6/autoconf-macros/.gitignore
nagios-4.4.6/autoconf-macros/CHANGELOG.md
nagios-4.4.6/autoconf-macros/LICENSE
nagios-4.4.6/autoconf-macros/LICENSE.md
nagios-4.4.6/autoconf-macros/README.md
nagios-4.4.6/autoconf-macros/add_group_user
nagios-4.4.6/autoconf-macros/ax_nagios_get_distrib
nagios-4.4.6/autoconf-macros/ax_nagios_get_files
nagios-4.4.6/autoconf-macros/ax_nagios_get_inetd
nagios-4.4.6/autoconf-macros/ax_nagios_get_init
nagios-4.4.6/autoconf-macros/ax_nagios_get_os
nagios-4.4.6/autoconf-macros/ax_nagios_get_paths
nagios-4.4.6/autoconf-macros/ax_nagios_get_ssl
nagios-4.4.6/base/
nagios-4.4.6/base/.gitignore
nagios-4.4.6/base/Makefile.in
nagios-4.4.6/base/broker.c
```

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

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

```
[ec2-user@ip-172-31-40-254 nagios-4.4.6]$ ./configure --with-command-group=nagcmd
checking for a BSD-compatible install... /usr/bin/install -c
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether make sets $MAKE... yes
checking whether ln -s works... yes
checking for strip... /usr/bin/strip
checking how to run the C preprocessor... gcc -E
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for ANSI C header files... yes
checking whether time.h and sys/time.h may both be included... yes
checking for sys/wait.h that is POSIX.1 compatible... yes
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
checking for string.h... yes
checking for memory.h... yes
checking for strings.h... yes
checking for inttypes.h... yes
checking for stdint.h... yes
checking for unistd.h... yes
checking arpa/inet.h usability... yes
checking arpa/inet.h presence... yes
checking for arpa/inet.h...
```

## 12. Compile the source code.

make all

```
[ec2-user@ip-172-31-40-254 nagios-4.4.6]$ make all
cd ./base && make
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.4.6/base'
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nagios.o nagios.c
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o broker.o broker.c
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nebmods.o nebmods.c
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o ../common/shared.o ../common/shared.c
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o query-handler.o query-handler.c
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o workers.o workers.c
In function 'get_wproc_list',
  inlined from 'get_worker' at workers.c:277:12:
workers.c:253:17: warning: `*s' directive argument is null [-Wformat-overflows=]
  253 |     log_debug_info(DEBUGL_CHECKS, 1, "Found specialized worker(s) for '%s'", (slash && *slash != '/') ? slash : cmd_name);
   |     ^
   |     ~~~~~
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o checks.o checks.c
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o config.o config.c
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o commands.o commands.c
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o events.o events.c
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o flapping.o flapping.c
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o logging.o logging.c
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o macros-base.o ../common/macros.c
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o netutils.o netutils.c
netutils.c: In function 'my_tcp_connect':
netutils.c:50:47: warning: `*d' directive output may be truncated writing between 1 and 11 bytes into a region of size 6 [-Wformat-truncation=]
  50 |     sprintf(port_str, sizeof(port_str), "%d", port);
   |     ^
   |     ~~~
netutils.c:50:46: note: directive argument in the range [-2147483648, 65535]
  50 |     sprintf(port_str, sizeof(port_str), "%d", port);
   |     ^
   |     ~~~
netutils.c:50:9: note: `sprintf' output between 2 and 12 bytes into a destination of size 6
  50 |     sprintf(port_str, sizeof(port_str), "%d", port);
   |     ^
   |     ~~~
gcc -Wall -I... -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o notifications.o notifications.c
```

```

make install-classicui
  - This installs the classic theme for the Nagios
    web interface

**** 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:
    https://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:
  https://support.nagios.com
*****
Enjoy.

```

### **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-172-31-40-254 nagios-4.4.6]$ ./sudo make install
sudo make install-init
sudo make install-config
sudo make install-commandmode
-bash: ./sudo: No such file or directory
/usr/bin/install -c -m 755 -o root -g root /lib/systemd/system
/usr/bin/install -c -m 755 -o nagios -g nagios -d /usr/local/nagios/etc
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc/objects
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/nagios.cfg /usr/local/nagios/etc/nagios.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/cgi.cfg /usr/local/nagios/etc/cgi.cfg
/usr/bin/install -c -b -m 660 -o nagios -g nagios sample-config/resource.cfg /usr/local/nagios/etc/resource.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/templates.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/commands.cfg /usr/local/nagios/etc/objects/commands.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/contacts.cfg /usr/local/nagios/etc/objects/contacts.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/timeperiods.cfg /usr/local/nagios/etc/objects/timeperiods.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/localhost.cfg /usr/local/nagios/etc/objects/localhost.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/windows.cfg /usr/local/nagios/etc/objects/windows.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/printer.cfg /usr/local/nagios/etc/objects/printer.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/switch.cfg /usr/local/nagios/etc/objects/switch.cfg

*** Config files installed ***

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

/usr/bin/install -c -m 775 -o nagios -g nagcmd -d /usr/local/nagios/var/rw
chmod g+s /usr/local/nagios/var/rw

*** External command directory configured ***

```

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

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

```

GNU nano 5.8                               /usr/local/nagios/etc/objects/contacts.cfg
just one contact defined by default - the Nagios admin (that's you)
This contact definition inherits a lot of default values from the
'generic-contact' template which is defined elsewhere.

define contact {
    contact_name      nagiosadmin          ; Short name of user
    use               generic-contact       ; Inherit default values from generic-contact template (defined above)
    alias             Nagios Admin        ; Full name of user
    email            bhaiyeshpatil0702@gmail.com; <<***** CHANGE THIS TO YOUR EMAIL ADDRESS *****

}

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

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

define contactgroup {
    #G Help      ^C Write Out   ^W Where Is   ^K Cut           ^X Execute   ^L Location   M-U Undo   M-A Set Mark   M-I To Bracket   M-X Previous
    ^X Exit      ^R Read File   ^X Replace   ^V Paste         ^J Justify   ^G Go To Line  M-Z Redo   M-C Copy      M-S Where Was   M-W Next
}

```

## 15. Configure the web interface.

sudo make install-webconf

```
[ec2-user@ip-172-31-40-254 nagios-4.4.6]$ sudo make install-webconf
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/httpd/conf.d/nagios.conf
if [ 0 -eq 1 ]; then \
    ln -s /etc/httpd/conf.d/nagios.conf /etc/apache2/sites-enabled/nagios.conf; \
fi

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

[ec2-user@ip-172-31-40-254 nagios-4.4.6]$
```

## 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-172-31-40-254 nagios-4.4.6]$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
[ec2-user@ip-172-31-40-254 nagios-4.4.6]$
```

## 17. Restart Apache sudo systemctl restart httpd

```
Adding password for user nagiosadmin
[ec2-user@ip-172-31-40-254 nagios-4.4.6]$ sudo systemctl restart httpd
[ec2-user@ip-172-31-40-254 nagios-4.4.6]$
```

cd ~/downloads tar zxvf nagios-

plugins-2.3.3.tar.gz cd nagios-

plugins-2.3.3

```
[ec2-user@ip-172-31-40-254 nagios-4.4.6]$ sudo systemctl restart httpd
[ec2-user@ip-172-31-40-254 nagios-4.4.6]$ cd ~/downloads
tar zxvf nagios-plugins-2.3.3.tar.gz
cd nagios-plugins-2.3.3
nagios-plugins-2.3.3/
nagios-plugins-2.3.3/perlmod/
nagios-plugins-2.3.3/perlmod/Config-Tiny-2.14.tar.gz
nagios-plugins-2.3.3/perlmod/parent-0.226.tar.gz
nagios-plugins-2.3.3/perlmod/test-strict-0.98.tar.gz
nagios-plugins-2.3.3/perlmod/Makefile.in
nagios-plugins-2.3.3/perlmod/version-0.9903.tar.gz
nagios-plugins-2.3.3/perlmod/Makefile.am
nagios-plugins-2.3.3/perlmod/Module-Runtime-0.013.tar.gz
nagios-plugins-2.3.3/perlmod/Module-Metadata-1.000014.tar.gz
nagios-plugins-2.3.3/perlmod/Params-Validate-1.08.tar.gz
nagios-plugins-2.3.3/perlmod/Class-Accessor-0.34.tar.gz
nagios-plugins-2.3.3/perlmod/Try-Tiny-0.18.tar.gz
nagios-plugins-2.3.3/perlmod/Module-Implementation-0.07.tar.gz
nagios-plugins-2.3.3/perlmod/Makefile
nagios-plugins-2.3.3/perlmod/Perl-OStype-1.003.tar.gz
nagios-plugins-2.3.3/perlmod/install_order
nagios-plugins-2.3.3/perlmod/nagios-Plugin-0.36.tar.gz
nagios-plugins-2.3.3/perlmod/Math-Calc-Units-1.07.tar.gz
nagios-plugins-2.3.3/perlmod/Module-Build-0.4007.tar.gz
nagios-plugins-2.3.3/ABOUT-NLS
nagios-plugins-2.3.3/configure.ac
nagios-plugins-2.3.3/Makefile.in
nagios-plugins-2.3.3/config.h.in
nagios-plugins-2.3.3/Changelog
nagios-plugins-2.3.3/AUTHORS
nagios-plugins-2.3.3/lib/
nagios-plugins-2.3.3/lib/parse_ini.h
nagios-plugins-2.3.3/lib/extr_opts.c
nagios-plugins-2.3.3/lib/Makefile.in
```

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

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

```
group=nagios make sudo make install
```

```
[ec2-user@ip-172-31-80-22 nagios-plugins-2.3.3]$ ./configure --with-nagios-user=nagios --with-nagios-group=nagios
make
sudo make install
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
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 for style of include used by make... GNU
checking dependency style of gcc... gcc3
checking how to run the C preprocessor... gcc -E
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... (none) [using this grep]
```

## 19. Compile and install plugins sudo chkconfig --add nagios sudo

```
chkconfig nagios on
```

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

```
systemctl start nagios
```

```
[ec2-user@ip-172-31-80-22 nagios-plugins-2.3.3]$ sudo chkconfig --add nagios
sudo chkconfig nagios on
sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
sudo systemctl start nagios
error reading information on service nagios: No such file or directory
Note: Forwarding request to 'systemctl enable nagios.service'.
Created symlink /etc/systemd/system/multi-user.target.wants/nagios.service → /usr/lib/systemd/system/nagios.service.

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

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

Running pre-flight check on configuration data...

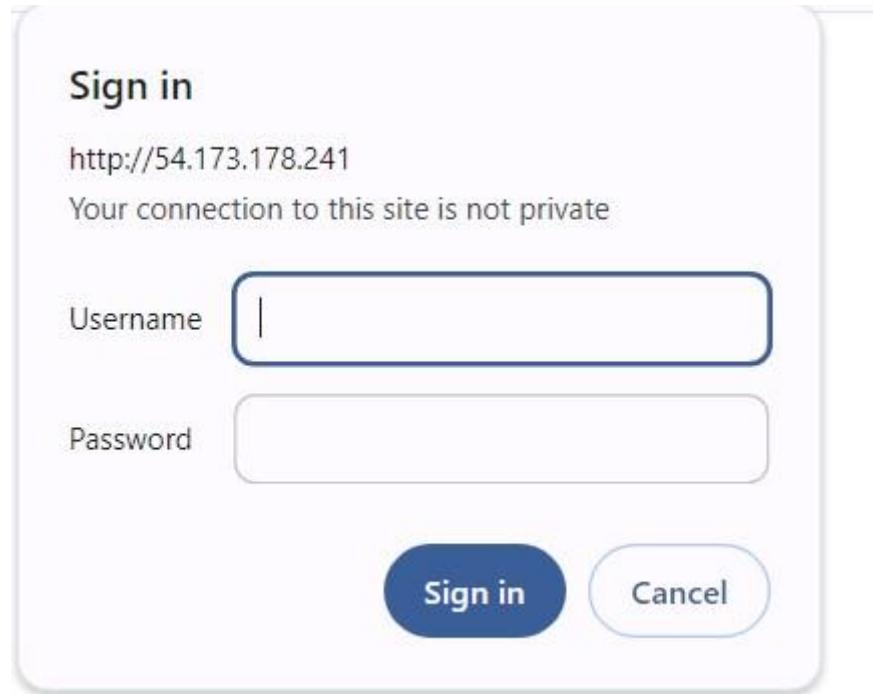
Checking objects...
  Checked 8 services.
  Checked 1 hosts.
  Checked 1 host groups.
```

## 20. Check the status of Nagios

```
Things look okay - No serious problems were detected during the pre-flight check
ec2-user@ip-172-31-45-178 nagios-plugins-2.3.3$ sudo systemctl status nagios
nagios.service - Nagios Core 4.4.6
   Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
     Active: active (running) since Wed 2024-10-02 05:37:36 UTC; 14s ago
       Docs: https://www.nagios.org/documentation
    Process: 67990 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
   Main PID: 67992 (nagios)
      Tasks: 6 (limit: 1112)
        Memory: 2.0M
          CPU: 16ms
         CGroup: /system.slice/nagios.service
             └─67992 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
                  ├─67993 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
                  ├─67994 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
                  ├─67995 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
                  ├─67996 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
                  └─67997 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Oct 02 05:37:36 ip-172-31-45-178.ec2.internal nagios[67992]: qh: Socket '/usr/local/nagios/var/rw/nagios.qh' successfully initialized
Oct 02 05:37:36 ip-172-31-45-178.ec2.internal nagios[67992]: qh: core query handler registered
```

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



Not secure 54.173.178.241/nagios/

# Nagios® Core™

✓ Daemon running with PID 67992

**Nagios® Core™**  
Version 4.4.6  
April 28, 2020  
[Check for updates](#)

A new version of Nagios Core is available!  
Visit [nagios.org](#) to download Nagios 4.5.5.

**General**

- Home
- Documentation

**Current Status**

- Tactical Overview
- Maps (Legacy)
- Hosts
- Services
- Host Groups
- Summary
- Grid
- Service Groups
- Summary
- Grid

**Problems**

- Services
- (Unhandled)
- Events (Unhandled)
- Network Outages

**Quick Search:**

**Reports**

- Availability
- Trends (Legacy)
- Alarms
- History
- Summary
- Histogram (Legacy)
- Notifications
- Event Log

**System**

- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue
- Configuration

**Get Started**

- Start monitoring your infrastructure
- Change the look and feel of Nagios
- Extend Nagios with hundreds of addons
- Get support
- Get training
- Get certified

**Quick Links**

- Nagios Library (tutorials and docs)
- Nagios Labs (development blog)
- Nagios Exchange (plugins and addons)
- Nagios Support (tech support)
- Nagios.com (company)
- Nagios.org (project)

**Latest News**

**Don't Miss...**

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

Page Tour

# Advance DevOps Exp 10

Name:- Prajyot Shinde

Roll :- 57

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

## Procedure:-

**Check if the nagios service is running by executing following command**      sudo systemctl status nagios

```
ubuntu@ip-172-31-89-161:~$ sudo systemctl status nagios
● nagios.service - Nagios Core 4.4.6
   Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: enabled)
   Active: active (running) since Sat 2024-09-28 16:08:58 UTC; 1min 25 ago
     Docs: https://www.nagios.org/documentation
 Process: 15743 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
 Process: 15753 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
 Main PID: 15764 (nagios)
   Tasks: 6 (limit: 1130)
  Memory: 2.4M (peak: 3.2M)
    CPU: 29ms
   CGroup: /system.slice/nagios.service
           ├─15764 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
           ├─15765 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─15766 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─15767 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─15768 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           └─15769 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

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

**Now, create a new EC2 instance on AWS**

Instances (2) <small>Info</small>		Last updated less than a minute ago	Connect	Instance state	Actions	Launch instances
				All states		
<input type="checkbox"/>	Name ↴	Instance ID	Instance state	Instance type	Status check	Alarm status
<input type="checkbox"/>	nagios-host	i-09e8ea019f24f4be2	<span>Running</span> ⓘ ⓘ	t2.micro	<span>2/2 checks passed</span> ⓘ	<a href="#">View alarms</a> +
<input type="checkbox"/>	linux-client	i-0ad38836f030e3784	<span>Running</span> ⓘ ⓘ	t2.micro	<span>Initializing</span> ⓘ	<a href="#">View alarms</a> +

**Now perform the following commands on nagios-host EC2 instance. On the server, run this command**

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

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

Sudo su

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

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

**Copy localhost.cfg file to the mentioned location**

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

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

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

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

```

GNU nano 7.2                                     /usr/local/nagios/etc/nagios.cfg
#####
#
# HOST DEFINITION
#
#####
# Define a host for the local machine

define host {

    use          linux-server ; Name of host template
                  ; This host definition
                  ; is (or inherits) from the "linux-server" template

    host_name    linuxserver
    alias        linuxserver
    address      52.207.253.18
}

#####
#
# HOST GROUP DEFINITION

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

```

**Note - Here replace hostname with linuxserver**

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

**Add the following line to the nagios.cfg file**

cfg\_dir=/usr/local/nagios/etc/objects/monitorhosts/

```

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

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

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

#cfg_dir=/usr/local/nagios/etc/servers
#cfg_dir=/usr/local/nagios/etc/printers
#cfg_dir=/usr/local/nagios/etc-switches
#cfg_dir=/usr/local/nagios/etc/routers

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

```

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

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

```
License: GPL

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

Running pre-flight check on configuration data...

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

Total Warnings: 0
Total Errors: 0

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

**Now restart the service by using this command**

```
service nagios restart
```

```

root@ip-172-31-89-161:/usr/local/nagios/etc/objects/monitorhosts/linuxhosts# service nagios restart
root@ip-172-31-89-161:/usr/local/nagios/etc/objects/monitorhosts/linuxhosts# systemctl status nagios
● nagios.service - Nagios Core 4.4.6
   Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: enabled)
   Active: active (running) since Sat 2024-09-28 17:36:35 UTC; 19s ago
     Docs: https://www.nagios.org/documentation
 Process: 1870 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
 Process: 1872 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
 Main PID: 1874 (nagios)
   Tasks: 8 (limit: 1130)
  Memory: 3.0M (peak: 3.2M)
    CPU: 24ms
   CGroup: /system.slice/nagios.service
           ├─1874 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
           ├─1875 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─1876 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─1877 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─1878 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─1879 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
           ├─1880 /usr/local/nagios/libexec/check_ping -H 52.207.253.18 -w 3000.0,80% -c 5000.0,100% -p 5
           └─1881 /usr/bin/ping -n -U -w 30 -c 5 52.207.253.18

Sep 28 17:36:35 ip-172-31-89-161 nagios[1874]: qh: Socket '/usr/local/nagios/var/rw/nagios.qh' successfully initialized
Sep 28 17:36:35 ip-172-31-89-161 nagios[1874]: qh: core query handler registered
Sep 28 17:36:35 ip-172-31-89-161 nagios[1874]: qh: echo service query handler registered
Sep 28 17:36:35 ip-172-31-89-161 nagios[1874]: qh: help for the query handler registered
Sep 28 17:36:35 ip-172-31-89-161 nagios[1874]: wproc: Successfully registered manager as @wproc with query handler
Sep 28 17:36:35 ip-172-31-89-161 nagios[1874]: wproc: Registry request: name=Core Worker 1875;pid=1875
lines 1-26

```

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

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

```

# Supported.
#
# Note: The daemon only does rudimentary checking
# address. I would highly recommend adding entr
# file to allow only the specified host to connect
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running
# in a chroot environment.
allowed_hosts=127.0.0.1,54.167.169.0

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

```

sudo nano /etc/nagios/nrpe.cfg

**Now restart nrpe server by using this command**

sudo systemctl restart nagios-nrpe-server

Now, check nagios dashboard, you should see linuxserver up and running, if not

The screenshot shows the Nagios 4.4.6 dashboard at the URL 3.87.228.45/nagios/. The interface includes a left sidebar with navigation links for General, Current Status, Problems, Reports, and System. The main content area displays the "Host Status Details For All Host Groups" table, which lists two hosts: "linuxserver" and "localhost", both marked as "UP". The table includes columns for Host, Status, Last Check, Duration, and Status Information. Above the table are two summary boxes: "Host Status Totals" and "Service Status Totals", each showing counts for Up, Down, Unreachable, Pending, Ok, Warning, Unknown, Critical, and Pending states.

Host	Status	Last Check	Duration	Status Information
linuxserver	UP	10-08-2024 08:17:49	0d 0h 20m 45s	PING OK - Packet loss = 0%, RTA = 1.89 ms
localhost	UP	10-08-2024 08:15:19	6d 22h 26m 7s	PING OK - Packet loss = 0%, RTA = 0.03 ms

## **Experiment 11**

**PRAJYOT SHINDE 57 D15A**

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

Theory:

### **AWS Lambda**

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

The concept of “serverless” computing refers to not needing to maintain your own servers to run these functions. AWS Lambda is a fully managed service that takes care of all the infrastructure for you. And so “serverless” doesn’t mean that there are no servers involved: it just means that the servers, the operating systems, the network layer and the rest of the infrastructure have already been taken care of so that you can focus on writing application code.

### **Features of AWS Lambda**

- AWS Lambda easily scales the infrastructure without any additional configuration. It reduces the operational work involved.
- It offers multiple options like AWS S3, CloudWatch, DynamoDB, API Gateway, Kinesis, CodeCommit, and many more to trigger an event.
- You don’t need to invest upfront. You pay only for the memory used by the lambda function and minimal cost on the number of requests hence cost-efficient.
- AWS Lambda is secure. It uses AWS IAM to define all the roles and security policies.
- It offers fault tolerance for both services running the code and the function. You do not have to worry about the application down.

### **Packaging Functions**

Lambda functions need to be packaged and sent to AWS. This is usually a process of compressing the function and all its dependencies and uploading it to an S3 bucket.

And letting AWS know that you want to use this package when a specific event takes place. To help us with this process we use the Serverless Stack Framework (SST). We'll go over this in detail later on in this guide.

### **Execution Model**

The container (and the resources used by it) that runs our function is managed completely by AWS. It is brought up when an event takes place and is turned off if it is not being used. If additional requests are made while the original event is being served, a new container is brought up to serve a request. This means that if we are undergoing a usage spike, the cloud provider simply creates multiple instances of the container with our function to serve those requests.

This has some interesting implications. Firstly, our functions are effectively stateless. Secondly, each request (or event) is served by a single instance of a Lambda function. This means that you are not going to be handling concurrent requests in your code.

AWS brings up a container whenever there is a new request. It does make some optimizations here. It will hang on to the container for a few minutes (5 - 15mins depending on the load) so it can respond to subsequent requests without a cold start.

### **Stateless Functions**

The above execution model makes Lambda functions effectively stateless. This means that every time your Lambda function is triggered by an event it is invoked in a completely new environment. You don't have access to the execution context of the previous event.

However, due to the optimization noted above, the actual Lambda function is invoked only once per container instantiation. Recall that our functions are run inside containers. So when a function is first invoked, all the code in our handler function gets executed and the handler function gets invoked. If the container is still available for subsequent requests, your function will get invoked and not the code around it.

For example, the `createNewDbConnection` method below is called once per container instantiation and not every time the Lambda function is invoked. The `myHandler` function on the other hand is called on every invocation.

### **Common Use Cases for Lambda**

Due to Lambda's architecture, it can deliver great benefits over traditional cloud computing setups for applications where:

1. Individual tasks run for a short time;
2. Each task is generally self-contained;
3. There is a large difference between the lowest and highest levels in the workload of the application.

Some of the most common use cases for AWS Lambda that fit these criteria are: Scalable APIs. When building APIs using AWS Lambda, one execution of a Lambda function can serve a single HTTP request. Different parts of the API can be routed to different Lambda functions via Amazon API Gateway. AWS Lambda automatically scales individual functions according to

the demand for them, so different parts of your API can scale differently according to current usage levels. This allows for cost-effective and flexible API setups.

Data processing. Lambda functions are optimized for event-based data processing. It is easy to integrate AWS Lambda with data sources like Amazon DynamoDB and trigger a Lambda function for specific kinds of data events. For example, you could employ Lambda to do some work every time an item in DynamoDB is created or updated, thus making it a good fit for things like notifications, counters and analytics.

Steps to create an AWS Lambda function

**Step 1:** Create a Lambda Function

1. Choose a Function Creation Method:

Select Author from scratch.

2. Configure the Function:

Function name: Enter a name for your function (e.g., MyFirstLambda).

Runtime: Choose Python 3.x (the latest available version).

Permissions: Choose Create a new role with basic Lambda permissions (this creates a role with the necessary permissions).

3. Click on Create function.

Lambda > Functions > Create function

## Create function Info

Choose one of the following options to create your function.

- 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 Info  
Enter a name that describes the purpose of your function.  
Myfirstlambda

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 3.12

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

## Step 2: Write Your Lambda Function Code

In the Function code section, you will see a code editor. Replace the default code with the following Python code:

```
python Copy code def lambda_handler(event,  
context): # This function returns a greeting  
message name = event.get('name', 'World')  
return {  
    'statusCode': 200, 'body': fHello,  
    '{name}!'  
}
```

This function reads a name from the event and returns a greeting message. If no name is provided, it defaults to "World".

The screenshot shows the AWS Lambda console interface. At the top, a green success message says: "Successfully created the function Myfirstlambda. You can now change its code and configuration. To invoke your function with a test event, choose 'Test'." Below this, the function name "Myfirstlambda" is displayed. The "Code source" tab is active, showing the following Python code:

```

1 def lambda_handler(event, context):
2     # This function returns a greeting message
3     name = event.get('name', 'World')
4     return {
5         'statusCode': 200,
6         'body': f'Hello, {name}!'
7     }

```

### Step3: 1. Configure a Test Event:

Click on the Test button.

In the Configure test event dialog, give your event a name (e.g., TestEvent). Replace the default JSON with the following:

```
{
  "name": "Lambda User"
}
```

### 2. Run the Test:

Click on the Test button again to execute your Lambda function.

You should see the execution results below the code editor, including the response: json

```

Copy code
{
  "statusCode": 200,
  "body": "Hello, Lambda User!"
}

```

**Configure test event**

A test event is a JSON object that mocks the structure of requests emitted by AWS services to invoke a Lambda function. Use it to see the function's invocation result.

To invoke your function without saving an event, configure the JSON event, then choose Test.

Test event action

Create new event     Edit saved event

Event name

TestEvent

Maximum of 25 characters consisting of letters, numbers, dots, hyphens and underscores.

Event sharing settings

Private  
This event is only available in the Lambda console and to the event creator. You can configure a total of 10. [Learn more](#)

Shareable  
This event is available to IAM users within the same account who have permissions to access and use shareable events. [Learn more](#)

Template - optional

hello-world

**Event JSON**

Format JSON

```

1 * {   "name": "Lambda User"
2   }
3 }
4

```

Cancel    **Invoke**    Save

**Code**    **Test**    Monitor    Configuration    Aliases    Versions

**Code source**    Info

File    Edit    Find    View    Go    Tools    Window    **Test**    Deploy    Changes not deployed

Go to Anything (Ctrl-P)

Environment

lambda\_function    Environment Var    Execution result

Myfirstlambda /

lambda\_function.py

Execution results

Test Event Name

TestEvent

Response

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

Function Logs

START RequestId: 36449800-5b8a-496e-83f6-7de19be2aa3c Version: \$LATEST  
 END RequestId: 36449800-5b8a-496e-83f6-7de19be2aa3c  
 REPORT RequestId: 36449800-5b8a-496e-83f6-7de19be2aa3c Duration: 2.08 ms    Billed Duration: 3 ms    Mem

Request ID

36449800-5b8a-496e-83f6-7de19be2aa3c

## Conclusion:

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

## Adv. DevOps Exp. 12

Prajyot Shinde

D15A - 57

### Step 1: Open the IAM (user)

The screenshot shows the AWS IAM Roles page. On the left, there's a sidebar with navigation links like Dashboard, Access management, and Access reports. The main area displays a table of roles with columns for Role name, Trusted entities, and Last activity. The roles listed are: `any-elasticbeanstalk-service-role-2`, `AWSServiceRoleForAutoScaling`, `AWSServiceRoleForSupport`, `AWSServiceRoleForTrustedAdvisor`, `myPythonLambdaFunction-role-a2x7el65`, and `test-2-role`. The last activity for most roles is 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 (October 07, 2023), ARN, and last activity. Below it is a Permissions tab where you can manage policies. A modal window is open over the page, specifically the "Permissions policies" section, which lists one policy: `arn:aws:iam::447953971928:role/service-role/myPythonLambdaFunction-role-a2x7el65`. The modal has buttons for "Add permissions" (with "Attach policies" selected) and "Create inline policy".

S3-ReadOnly

The screenshot shows the 'Add permissions' dialog in the AWS IAM console. The URL is [IAM > Roles > myPythonLambdaFunction-role-a2x7el65 > Add permissions](#). The title is 'Attach policy to myPythonLambdaFunction-role-a2x7el65'. The 'Current permissions policies (1)' section is collapsed. The 'Other permissions policies (882)' section is expanded, showing a search bar with 'S3read' and a filter 'All types'. One result, 'AmazonS3ReadOnlyAccess', is listed as 'AWS managed' with a description: 'Provides read only access to all bucket...'. At the bottom are 'Cancel' and 'Add permissions' buttons.

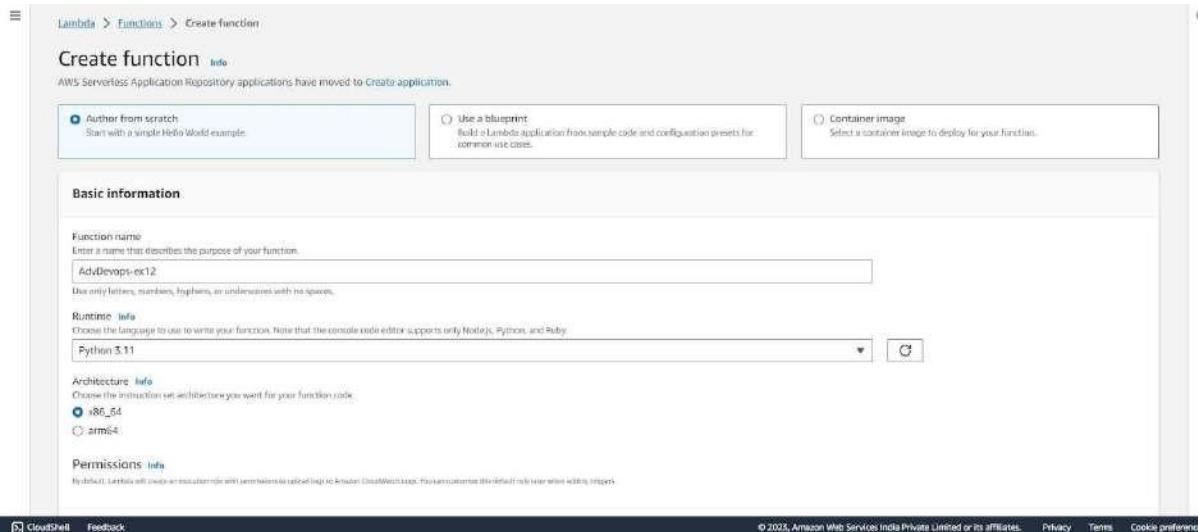
## CloudWatchFull

The screenshot shows the 'Add permissions' dialog in the AWS IAM console. The URL is [IAM > Roles > myPythonLambdaFunction-role-a2x7el65 > Add permissions](#). The title is 'Attach policy to myPythonLambdaFunction-role-a2x7el65'. The 'Current permissions policies (2)' section is collapsed. The 'Other permissions policies (881)' section is expanded, showing a search bar with 'cloudwatchfull' and a filter 'All types'. Two results, 'CloudWatchFullAccess' and 'CloudWatchFullAccessV2', are listed as 'AWS managed' with descriptions: 'Provides full access to CloudWatch.' and 'Provides full access to CloudWatch.' respectively. At the bottom are 'Cancel' and 'Add permissions' buttons.

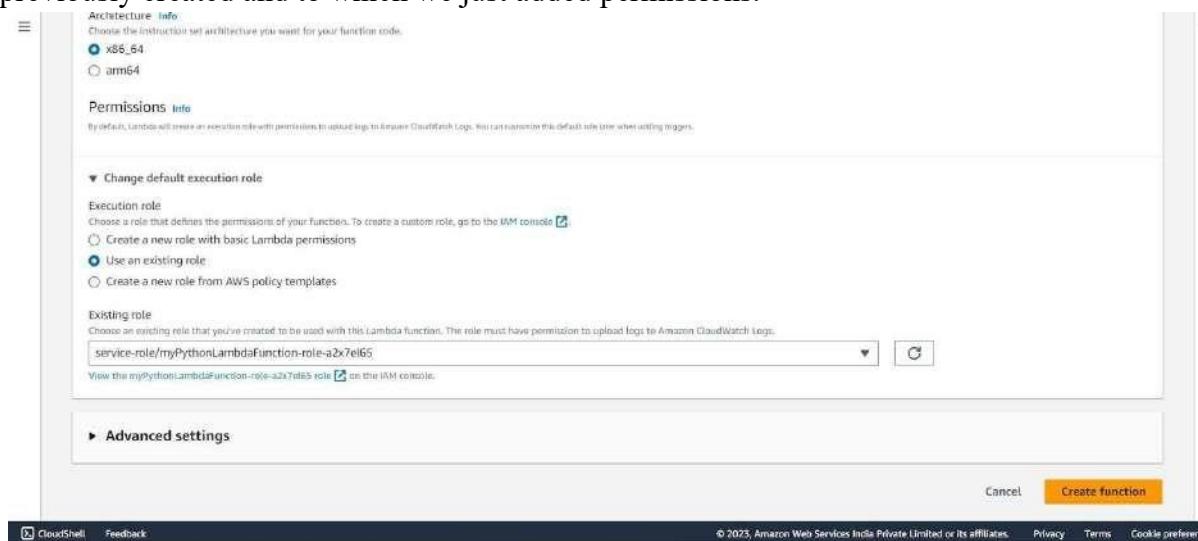
After successful attachment of policy you will see something like this you will be able to see the updated policies.

The screenshot shows the 'Permissions' tab in the AWS IAM console. The URL is [Identity and Access Management \(IAM\)](#). A green banner at the top says 'Policy was successfully attached to role.' Below it is a message 'Last modified: 1 hour ago'. The 'Permissions' tab is selected. The 'Permissions policies (3)' section shows three policies: 'AmazonS3ReadOnlyAccess' (AWS managed), 'AWSLambdaBasicExecutionRole' (Customer managed), and 'CloudWatchFullAccess' (AWS managed). Each policy has a checkbox, a type indicator, and an 'Attached entities' column showing '1'. At the bottom is a 'Permissions boundary (not set)' section.

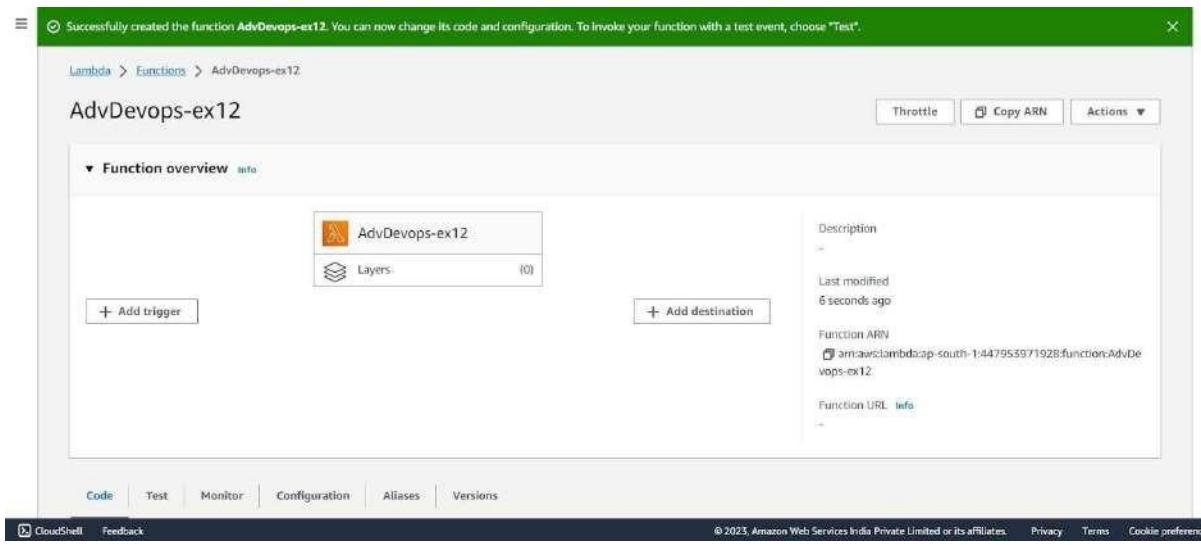
### Step 3: Open up AWS Lambda and create a new Python function.



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



Step 4: The function is up and running.



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

```
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 = 'An 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 code is a Python script named 'lambda\_function.py'. It uses the boto3 library to interact with the S3 service. The script defines a single function, 'lambda\_handler', which takes 'event' and 'context' as parameters. Inside the function, it retrieves the name of the bucket and the key of the uploaded file from the event. It then prints a message indicating the file has been added. It uses the 'urllib.parse.unquote\_plus' method to decode the key. It then gets the object from the S3 bucket using the 'get\_object' method. The response is a dictionary containing a 'Body' key, which is read and decoded. Finally, the contents are printed to the console.

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

The screenshot shows the AWS Lambda console interface. At the top, a green banner indicates that a function has been successfully created. Below the banner, the navigation bar includes tabs for Code, Test, Monitor, Configuration, Aliases, and Versions. The 'Code' tab is selected, showing the 'Code source' section with a file browser. A file named 'lambda\_function.py' is open, displaying Python code for a Lambda function:

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

Below the code editor is a modal window titled 'Configure test event'. The modal provides instructions for creating a test event and includes fields for 'Test event action' (radio buttons for 'Create new event' and 'Edit saved event', with 'Create new event' selected), 'Event name' (text input field containing 'test'), and 'Event sharing settings' (radio buttons for 'Private' and 'Shareable', with 'Private' selected). The 'Event JSON' section contains a dropdown menu set to 's3-put' and a 'Format JSON' button. At the bottom of the modal are 'Cancel', 'Invoke', and 'Save' buttons.

And Save it.

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

The screenshot shows the Amazon S3 buckets list page. At the top, there's an 'Account snapshot' section with a link to 'View Storage Lens dashboard'. Below it, a table lists three buckets:

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, 15:05:54 (UTC+05:30)
www.htmlwebside.com	Asia Pacific (Mumbai) ap-south-1	Public	July 30, 2023, 15:49:06 (UTC+05:30)

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.' followed by 'Privacy', 'Terms', and 'Cookie preferences'.

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

The screenshot shows the 'Create bucket' wizard in the 'General configuration' step. The 'Bucket name' field contains 'AdvDevopsexp12'. The 'AWS Region' dropdown is set to 'Asia Pacific (Mumbai) ap-south-1'. There's also a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button. At the bottom, there's an 'Object Ownership' section with a note about controlling object ownership and access control lists (ACLs). The footer includes links for 'CloudShell', 'Feedback', and copyright information: '© 2023, Amazon Web Services India Private Limited or its affiliates.' followed by 'Privacy', 'Terms', and '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](#)

Name	Event types	Filters	Destination type	Destination
		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 policies](#).

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

Click on Create Event Notification.

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

**General configuration**

**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

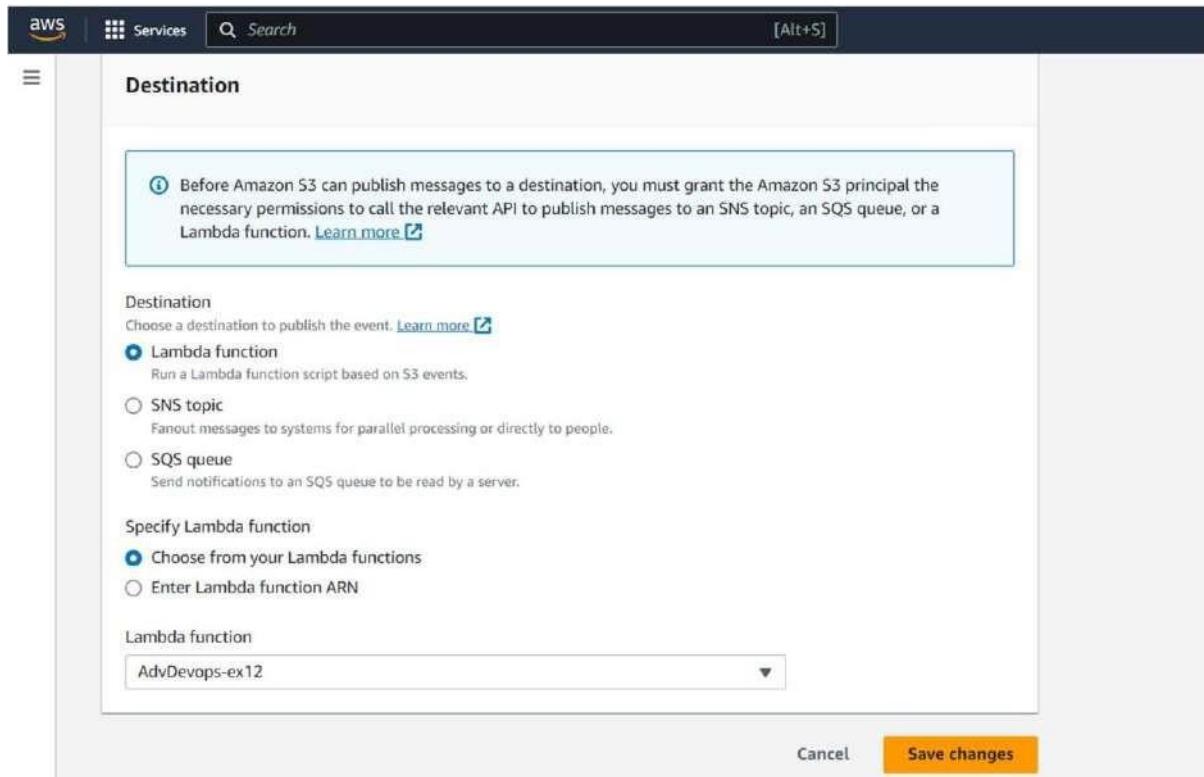
**Event types**  
Specify at least one event for which you want to receive notifications. For each group, you can choose an event type for all events, or you can choose one or more individual events.

**Object creation**

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

Post  
s3:ObjectCreated:Post

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



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

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

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

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

The screenshot shows the AWS S3 'Upload' interface. At the top, the navigation bar includes 'Services' and a search bar. Below the navigation, the path 'Amazon S3 > Buckets > advopssexp12 > Upload' is displayed. The main area is titled 'Upload' with a 'Info' link. A note at the top 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.' Below this is a large dashed box with the placeholder text 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' Underneath is a table titled 'Files and folders (1 Total, 89.0 B)' containing one item: 'dummy.json'. The table has columns for Name, Folder, Type, and Size. The file 'dummy.json' is listed as application/json, 89.0 B. There are 'Remove', 'Add files', and 'Add folder' buttons above the table. A search bar labeled 'Find by name' is present. The 'Destination' section shows 'Destination' set to 's3://advopssexp12'. At the bottom, there are 'CloudShell' and 'Feedback' links, 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 the AWS Lambda 'Event JSON' editor. The JSON code is as follows:

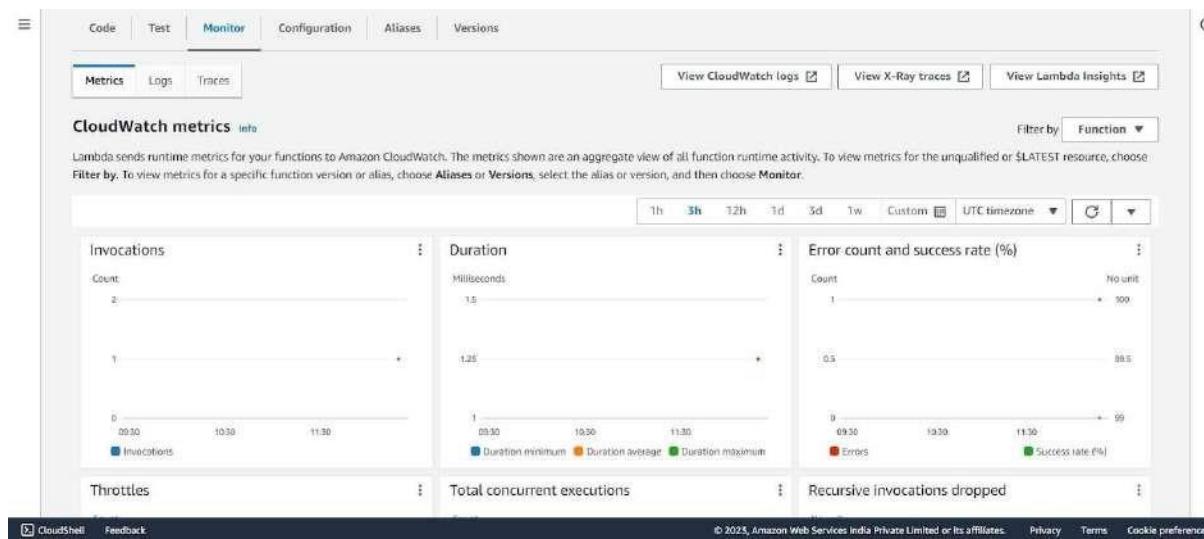
```

10     "principalId": "EXAMPLE"
11   },
12   "requestParameters": {
13     "sourceIPAddress": "127.0.0.1"
14   },
15   "responseElements": {
16     "x-amz-request-id": "EXAMPLE123456789",
17     "x-amz-id-2": "EXAMPLE123/5678abcdefghijklmnaqrstuvwxyzABCDEFGHIJKLMN"
18   },
19   "s3": {
20     "s3SchemaVersion": "1.0",
21     "configurationId": "testConfigRule",
22     "bucket": {
23       "name": "advopssexp12",
24       "ownerIdentity": {
25         "principalId": "EXAMPLE"
26       },
27       "arn": "arn:aws:s3:::advopssexp12"
28     },
29     "object": {
30       "key": "test%2Fkey",
31       "size": 1024,
32       "eTag": "0123456789abcdef0123456789abcdef",
33       "sequencer": "0A1B2C3D4E5F678901"
34     }
35   }
36 }
37 ]
38 }

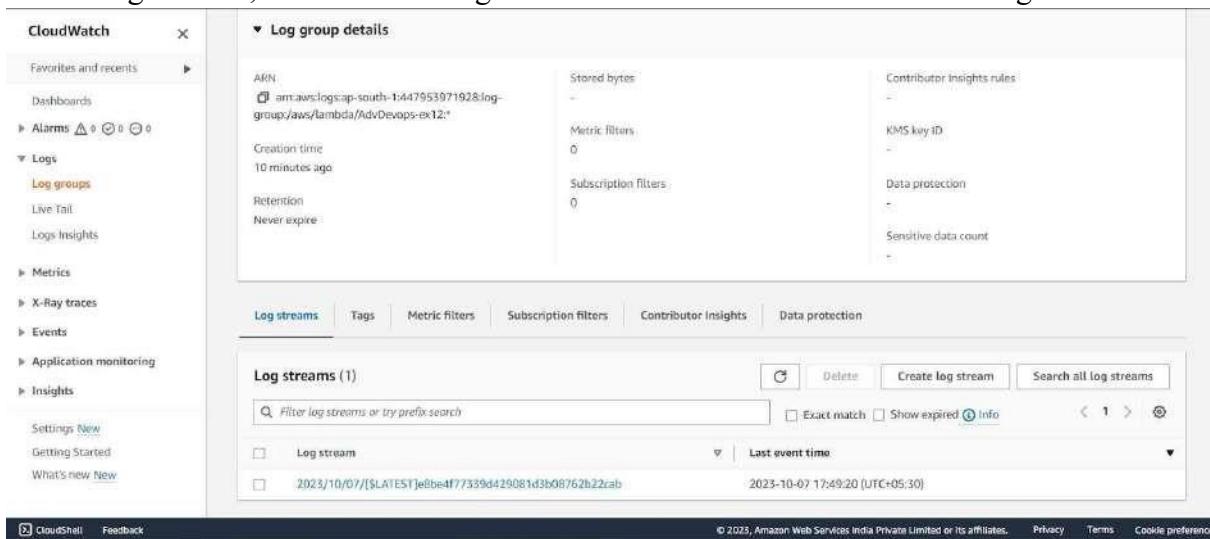
```

At the top right of the editor is a 'Format JSON' button. The code is highlighted with line numbers from 10 to 38.

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.

The screenshot shows the AWS CloudWatch Logs interface. On the left, there's a navigation sidebar with options like Favorites and recent, Dashboards, Alarms, Logs (selected), Log groups, Log Anomalies, Live Tail, Logs Insights, Contributor Insights, Metrics, X-Ray traces, Events, Application Signals (New), Network monitoring, Insights, Settings, and Getting Started. At the bottom of the sidebar are CloudShell and Feedback links. The main area displays a log group path: CloudWatch > Log groups > /aws/lambda/Lambda-Func > 2024/10/11/[...LATEST]aff54e3f606143548ec12e1f2f25a4df. Below this, a section titled "Log events" shows a table with columns for "Timestamp" and "Message". The table contains several log entries, each starting with a timestamp (e.g., 2024-10-11T05:23:33.473Z) followed by a log message. The messages include INIT\_START, START, END, and REPORT requests for a Lambda function. The interface includes a search bar, filter buttons (Clear, 1m, 30m, 1h, 12h, Custom, UTC timezone), and display settings (Display, Show more). At the bottom right, there are links for © 2024, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

**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.