

Experiment 1

Atharva Prabhu

D15A 43

1. Open AWS Academia and select launch instance

The image consists of three vertically stacked screenshots of the AWS Management Console.

Screenshot 1: AWS Cloud Home

This screenshot shows the AWS Cloud Home interface. On the left, there's a sidebar with "Recently visited" services (EC2, S3, Cloud9) and a "View all services" link. On the right, there's a section titled "Applications" with a "Create application" button and a message stating "No applications". Below it is a "Create application" button and a "Go to myApplications" link.

Screenshot 2: EC2 Dashboard

This screenshot shows the EC2 Dashboard. On the left, a sidebar lists "Instances", "Images", and "Launch Templates". The main area displays "Resources" with a grid of metrics: Instances (running) 2, Auto Scaling Groups 0, Capacity Reservations 0, Dedicated Hosts 0, Elastic IPs 0, Instances 2, Key pairs 1, Load balancers 0, Placement groups 0, Security groups 3, Snapshots 0, and Volumes 2. Below this is a "Launch instance" button and a "Service health" section with a "AWS Health Dashboard" link.

Screenshot 3: Instances

This screenshot shows the Instances page. On the left, a sidebar lists "Instances" (with "Instances" selected), "Image Catalog", and "Launch Templates". The main area shows "Instances (2)" with a table:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Available
aws-cloud9-At...	i-09717f2000b2e486f	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1
atharva	i-0401151b7a114184f	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1

2. Execute the following commands in the aws console.

Commands :

```
sudo su
sudo apt install
sudo apt-get update
apt install apache2
systemctl status apache2
cd /var/www/html/
```

```
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 Sun Aug 25 03:11:28 UTC 2024

System load: 0.09 Processes: 105
Usage of /: 23.4% of 6.71GB Users logged in: 0
Memory usage: 19% IPv4 address for enx0: 172.31.82.107
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

Last login: Thu Aug 22 05:23:58 2024 from 18.206.107.29
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-82-107:~$ sudo su
root@ip-172-31-82-107:/home/ubuntu# sudo apt install
Reading package lists... Done

i-0401151b7a114184f (atharva)
PublicIPs: 54.234.233.3 PrivateIPs: 172.31.82.107

Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@ip-172-31-82-107:/home/ubuntu# ^[[200-sudo apt-get update
sudo: command not found
root@ip-172-31-82-107:/home/ubuntu# ^[[200-sudo apt-get update
sudo: command not found
root@ip-172-31-82-107:/home/ubuntu# 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://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [323 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [463 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [114 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [7192 B]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [337 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [142 kB]
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [45.0 kB]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [13.6 kB]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [280 kB]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [54.8 kB]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 c-n-f Metadata [416 B]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [14.1 kB]

i-0401151b7a114184f (atharva)
PublicIPs: 54.234.233.3 PrivateIPs: 172.31.82.107
```

```
aws Services Search [Alt+S] N. Virginia v vodlabs/user3402849=PRABHU_ATHARVA_NILESH @ 9620-2110-487
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [3608 B]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [212 B]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [532 B]
Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 c-n-f Metadata [112 B]
Get:30 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Packages [10.3 kB]
Get:31 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe Translation-en [10.5 kB]
Get:32 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [17.6 kB]
Get:33 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 c-n-f Metadata [1016 B]
Get:34 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:35 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 c-n-f Metadata [116 B]
Get:36 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Get:37 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:38 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [73.3 kB]
Get:39 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4220 B]
Get:40 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [252 kB]
Get:41 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [103 kB]
Get:42 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [965 B]
Get:43 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [9756 B]
Get:44 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [280 kB]
Get:45 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 c-n-f Metadata [420 B]
Get:46 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [10.6 kB]
Get:47 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [2808 B]
Get:48 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Get:49 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [344 B]
Fetched 28.6 MB in 6s (5118 kB/s)
Reading package lists... Done
root@ip-172-31-82-107:/home/ubuntu# ^[[200~apt install apache2
apt: command not found
root@ip-172-31-82-107:/home/ubuntu# apt install apache2
Reading package lists... Done
```

i-0401151b7a114184f (atharva)

PublicIPs: 54.234.233.3 PrivateIPs: 172.31.82.107

```
aws Services Search [Alt+S] N. Virginia v vodlabs/user3402849=PRABHU_ATHARVA_NILESH @ 9620-2110-487
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libaprutil64 libaprutil11-dbd-sqlite3 libaprutil11-ldap libaprutil11t64 liblua5.4-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libaprutil64 libaprutil11-dbd-sqlite3 libaprutil11-ldap libaprutil11t64 liblua5.4-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 100 not upgraded.
Need to get 2083 kB of archives.
After this operation, 8094 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil64 amd64 1.7.2-3.1build2 [107 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil11t64 amd64 1.6.3-1.lubuntu7 [91.9 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil11-dbd-sqlite3 amd64 1.6.3-1.lubuntu7 [11.2 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil11-ldap amd64 1.6.3-1.lubuntu7 [9116 B]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 liblua5.4-0 amd64 5.4.6-3build2 [16 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 apache2-bin amd64 2.4.58-lubuntu8.4 [1329 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-data-all 2.4.58-lubuntu8.4 [163 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-utils amd64 2.4.58-lubuntu8.4 [97.1 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2 amd64 2.4.58-lubuntu8.4 [90.2 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 ssl-cert all 1.1.2ubuntul [17.8 kB]
Fetched 2083 kB in 0s (34.4 MB/s)
Preconfiguring packages...
Selecting previously unselected package libaprutil64:amd64.
(Reading database ... 67739 files and directories currently installed.)
Preparing to unpack .../0-libaprutil64_1.7.2-3.1build2_amd64.deb ...
Unpacking libaprutil64:amd64 (1.7.2-3.1build2) ...
Selecting previously unselected package libaprutil11t64:amd64.
Preparing to unpack .../1-libaprutil11t64_1.6.3-1.lubuntu7_amd64.deb ...
Unpacking libaprutil11t64:amd64 (1.6.3-1.lubuntu7) ...
Selecting previously unselected package libaprutil11-dbd-sqlite3:amd64.
```

i-0401151b7a114184f (atharva)

PublicIPs: 54.234.233.3 PrivateIPs: 172.31.82.107

AWS Services Search [Alt+S] N. Virginia v vclabs/user3402849=PRABHU_ATHARVA_NILESH @ 9620-2110

```

Preparing to unpack .../2-libaprutil1-dbd-sqlite3_1.6.3-1.lubuntu7_amd64.deb ...
Unpacking libaprutil1-dbd-sqlite3:amd64 (1.6.3-1.lubuntu7) ...
Selecting previously unselected package libaprutil1-dap:amd64.
Preparing to unpack .../3-libaprutil1-dap_1.6.3-1.lubuntu7_amd64.deb ...
Unpacking libaprutil1-dap:amd64 (1.6.3-1.lubuntu7) ...
Selecting previously unselected package liblua5.4-0:amd64.
Preparing to unpack .../4-liblua5.4-0_5.4.6-3build2_amd64.deb ...
Unpacking liblua5.4-0:amd64 (5.4.6-3build2) ...
Selecting previously unselected package apache2-bin.
Preparing to unpack .../5-apache2-bin_2.4.58-lubuntu8.4_amd64.deb ...
Unpacking apache2-bin (2.4.58-lubuntu8.4) ...
Selecting previously unselected package apache2-data.
Preparing to unpack .../6-apache2-data_2.4.58-lubuntu8.4_all.deb ...
Unpacking apache2-data (2.4.58-lubuntu8.4) ...
Selecting previously unselected package apache2-utils.
Preparing to unpack .../7-apache2-utils_2.4.58-lubuntu8.4_amd64.deb ...
Unpacking apache2-utils (2.4.58-lubuntu8.4) ...
Selecting previously unselected package apache2.
Preparing to unpack .../8-apache2_2.4.58-lubuntu8.4_amd64.deb ...
Unpacking apache2 (2.4.58-lubuntu8.4) ...
Selecting previously unselected package ssl-cert.
Preparing to unpack .../9-ssl-cert_1.1.2ubuntu1_all.deb ...
Unpacking ssl-cert (1.1.2ubuntu1) ...
Setting up ssl-cert (1.1.2ubuntu1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/ssl-cert.service → /usr/lib/systemd/system/ssl-cert.service.
Setting up libapr1t4:amd64 (1.7.2-3.lbuild2) ...
Setting up liblub1_4.0-0:amd64 (5.4.6-3build2) ...
Setting up apache2-data (2.4.58-lubuntu8.4) ...
Setting up libaprutil1t4:amd64 (1.6.3-1.lubuntu7) ...
Setting up libaprutil1-dap:amd64 (1.6.3-1.lubuntu7) ...
Setting up libaprutil1-dbd-sqlite3:amd64 (1.6.3-1.lubuntu7) ...
Setting up apache2-utils (2.4.58-lubuntu8.4) ...

i-0401151b7a114184f (atharva)
PublicIPs: 54.234.233.3 PrivateIPs: 172.31.82.107
```

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

AWS Services Search [Alt+S] N. Virginia v vclabs/user3402849=PRABHU_ATHARVA_NILESH @ 9620-2110-482

```

Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu0.2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@ip-172-31-92-107:/home/ubuntu# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Sun 2024-08-25 03:15:58 UTC; 1min 50s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Main PID: 2310 (apache2)
      Tasks: 55 (limit: 1130)
     Memory: 5.3M (peak: 5.4M)
        CPU: 41ms
       CGroup: /system.slice/apache2.service
           └─2310 /usr/sbin/apache2 -k start
              ├─2312 /usr/sbin/apache2 -k start
              ├─2313 /usr/sbin/apache2 -k start
              └─2314 /usr/sbin/apache2 -k start

Aug 25 03:15:58 ip-172-31-92-107 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Aug 25 03:15:58 ip-172-31-92-107 systemd[1]: Started apache2.service - The Apache HTTP Server.
root@ip-172-31-92-107:/home/ubuntu# cd /var/www/html/
root@ip-172-31-92-107:/var/www/html#
```

i-0401151b7a114184f (atharva)
PublicIPs: 54.234.233.3 PrivateIPs: 172.31.82.107

AWS Services Search [Alt+S] N. Virginia voclabs/user5402849=PRABHU_ATHARVA_NILESH @ 9620-2110-487

```
Setting up apache2 (2.4.58-1ubuntu0.4) ...
Enabling module mpm_event.
Enabling module authz_core.
Enabling module authz_host.
Enabling module authn_core.
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 deflate.
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-ghosts-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.
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu0.2) ...
Processing triggers for libcurl4-openssl-dev (4.8.0-1ubuntu0.1) ...
Scanning processes...
```

i-0401151b7a114184f (atharva)

Public IPs: 54.234.233.3 Private IPs: 172.31.82.107

3.Edit the inbound and outbound rules.

The screenshot shows two views of the AWS EC2 Security Groups interface for the security group "sg-027fc9d1716e3904f - launch-wizard-1".

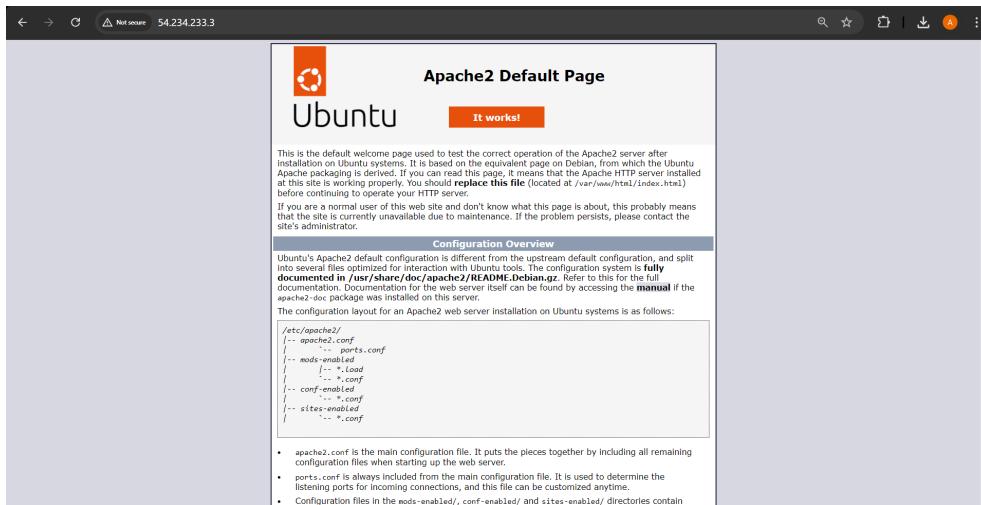
Top View (Inbound Rules):

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
-	sgr-0a294f7b728e86bb4	IPv4	HTTP	TCP	80	0.0.0.0/0

Bottom View (Outbound Rules):

Name	Security group rule...	IP version	Type	Protocol	Port range	Desti...
-	sgr-0875dd8762f2a189c	IPv4	HTTP	TCP	80	0.0.0.0/0

4. This is the hosted Static Website.



Static Site Hosting using S3 bucket

1. Visit S3 under the developer tools and create a Bucket. Click on the Edit Static Website Hosting under the properties tab

The screenshot shows the 'Edit static website hosting' configuration page for the 'atharva45554' bucket. The 'Static website hosting' section is enabled. Under 'Hosting type', 'Host a static website' is selected. A note indicates that for public access, content must be publicly readable. The 'Index document' field is set to 'index.html'. The 'Error document - optional' field contains '404.html'.

Amazon S3 > Buckets > atharva45554 > Edit static website hosting

Edit static website hosting Info

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

Static website hosting
 Disable
 Enable

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

ⓘ 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](#).

Index document
Specify the home or default page of the website.
index.html

Error document - *optional*
This is returned when an error occurs.
404.html

2. Upload a file

The screenshot shows the 'Upload: status' page after a file was uploaded successfully. The summary table shows 1 file uploaded (2.8 KB) with 100.00% success rate. The 'Files and folders' tab is selected, displaying a table with one entry: 'index.html' (2.8 KB, text/html, Succeeded).

Upload succeeded
View details below.

Upload: status

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

Summary		
Destination s3://atharva45554	Succeeded 1 file, 2.8 KB (100.00%)	Failed 0 files, 0 B (0%)

Files and folders (1 Total, 2.8 KB)

Name	Folder	Type	Size	Status	Error
index.html	-	text/html	2.8 KB	Succeeded	-

3. Click on the Edit block public access under the Permissions tab

The screenshot shows the 'Edit Block public access (bucket settings)' page. At the top, there's a breadcrumb navigation: 'Amazon S3 > Buckets > atharva45554 > Edit Block public access (bucket settings)'. Below the breadcrumb is the title 'Edit Block public access (bucket settings) Info'. A sub-section titled 'Block public access (bucket settings)' contains a detailed description of what public access is and how it can be blocked. It includes a link to 'Learn more'. Below this, there are five checkboxes for different types of access control:

- Block all public access**: Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
- Block public access to buckets and objects granted through new access control lists (ACLs)**: S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**: S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**: S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**: S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

At the bottom right, there are 'Cancel' and 'Save changes' buttons.

4. Click on Object Ownership under Permission Tab

≡ **Edit Object Ownership** Info

Object Ownership

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

ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

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

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

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

Object Ownership

Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

Object writer
The object writer remains the object owner.

ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#) ↗

Cancel **Save changes**

5. Select the file and click on Actions and select the option Make Public using ACL from the dropdown

Amazon S3 > Buckets > atharva45554

atharva45554 [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Objects (1) Info
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Name	Type	Last modified	Size
index.html	html	August 25, 2024, 09:59:25 (UTC+05:30)	2.8

Actions [Create folder](#) [Upload](#)

- [Download](#)
- [Copy S3 URI](#)
- [Copy URL](#)
- [Open](#)
- [Delete](#)
- [Actions ▾](#)
 - [Download as](#)
 - [Share with a presigned URL](#)
 - [Calculate total size](#)
 - [Copy](#)
 - [Move](#)
 - [Initiate restore](#)
 - [Query with S3 Select](#)
 - [Edit actions](#)
 - [Rename object](#)
 - [Edit storage class](#)
 - [Edit server-side encryption](#)
 - [Edit metadata](#)
 - [Edit tags](#)
 - [Make public using ACL](#)

6. Select on Make Public

Make public: status

[Close](#)

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

Summary

Source	Successfully edited public access	Failed to edit public access
s3://atharva45554	Successfully edited public access 1 object, 2.8 KB	Failed to edit public access 0 objects

[Failed to edit public access](#) [Configuration](#)

Failed to edit public access (0)

Name	Folder	Type	Last modified	Size	Error
No objects failed to edit					

7. Visit the domain and the website hosted.

atharva45554.s3.amazonaws.com/index.html

Custom T-Shirt Order Form

T-Shirt Details

Tagline on the Shirt: Enter your tagline | Color: Select a color | Size: Select a size | Quantity: | Delivery Date: dd-mm-yyyy

Delivery Details

Recipient's Name: | Address: | Email: | Phone Number: 1234567890

Any special instructions?

Additional Comments:

[Place Order](#) [Reset Form](#)

Cloud 9 IDE Site Hosting

Step 1: Create Environment

The screenshot shows the AWS Cloud9 interface. On the left, there's a sidebar with links for 'My environments', 'Shared with me', and 'All account environments'. Below that is a 'Documentation' link. The main area is titled 'Environments (1)' and shows a table with one row. The row contains the name 'Atharva@345', an 'Open' button, 'EC2 instance' as the connection type, and 'Secure Shell (SSH)' as the permission type. The owner is listed as 'Owner' with the ARN 'arn:aws:sts::962021104876:assumed-role/voclabs/user3402849=PRABHU_ATHARVA_NILESH'. At the top right of the main area, there are buttons for 'Delete', 'View details', 'Open in Cloud9', and 'Create environment'.

Step 2 :Open the Environment IDE and add the code and run the code

The screenshot shows the AWS Cloud9 IDE interface. The top navigation bar includes File, Edit, Find, View, Go, Run, Tools, Window, Support, Preview, and Run buttons. The main workspace has three tabs: 'Welcome', 'Untitled1.html', and 'Untitled1.py'. The 'Untitled1.py' tab contains the following Python code:

```
# Python3 program to add two numbers
num1 = 15
num2 = 12
# Adding two nos
sum = num1 + num2
# printing values
print("Sum of", num1, "and", num2, "is", sum)
```

Below the workspace is a terminal window with tabs for 'bash - ip-172-31-27-122.', 'Immediate (Javascript)', and 'Untitled1.py - Stopped'. The 'Untitled1.py' tab shows the output: 'Sum of 15 and 12 is 27'. The status bar at the bottom indicates '10:1 Python Spaces: 4'.

EXPERIMENT NO. 2

ATHARVA PRABHU

D15A 43

Step 1: create environment

The screenshot shows the 'Configure environment' wizard for creating a new environment. The left sidebar lists steps 1 through 6:

- Step 1: Configure environment
- Step 2: Configure service access
- Step 3 - optional: Set up networking, database, and tags
- Step 4 - optional: Configure instance traffic and scaling
- Step 5 - optional: Configure updates, monitoring, and logging
- Step 6: Review

The main content area is divided into three sections:

- Environment tier**: Set to Web server environment (selected).
Description: Amazon Elastic Beanstalk has two types of environment tiers to support different types of web applications.
 - Web server environment: Run a website, web application, or web API that serves HTTP requests. [Learn more](#)
 - Worker environment: Run a worker application that processes long-running workloads on demand or performs tasks on a schedule. [Learn more](#)
- Application information**: Application name: myapplication
Description: Maximum length of 100 characters.
Section: Application tags (optional)
- Environment information**: Environment name: Myapplication-env
Description: Choose the name, subdomain and description for your environment. These cannot be changed later.

Platform [Info](#)

Platform type

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

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

Platform

Python 

Platform branch

Python 3.11 running on 64bit Amazon Linux 2023 

Platform version

4.1.3 (Recommended) 

Application code [Info](#)

Sample application

Existing version
Application versions that you have uploaded.

Upload your code
Upload a source bundle from your computer or copy one from Amazon S3.

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

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

Step 2 : add your Ec2 key pair and instance profile

Configure service access Info

Service access

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

Service role

- Create and use new service role
 Use an existing service role

Existing service roles

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

▼C

EC2 key pair

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

▼C

EC2 instance profile

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

▼C

[View permission details](#)

Cancel

[Skip to review](#)

[Previous](#)

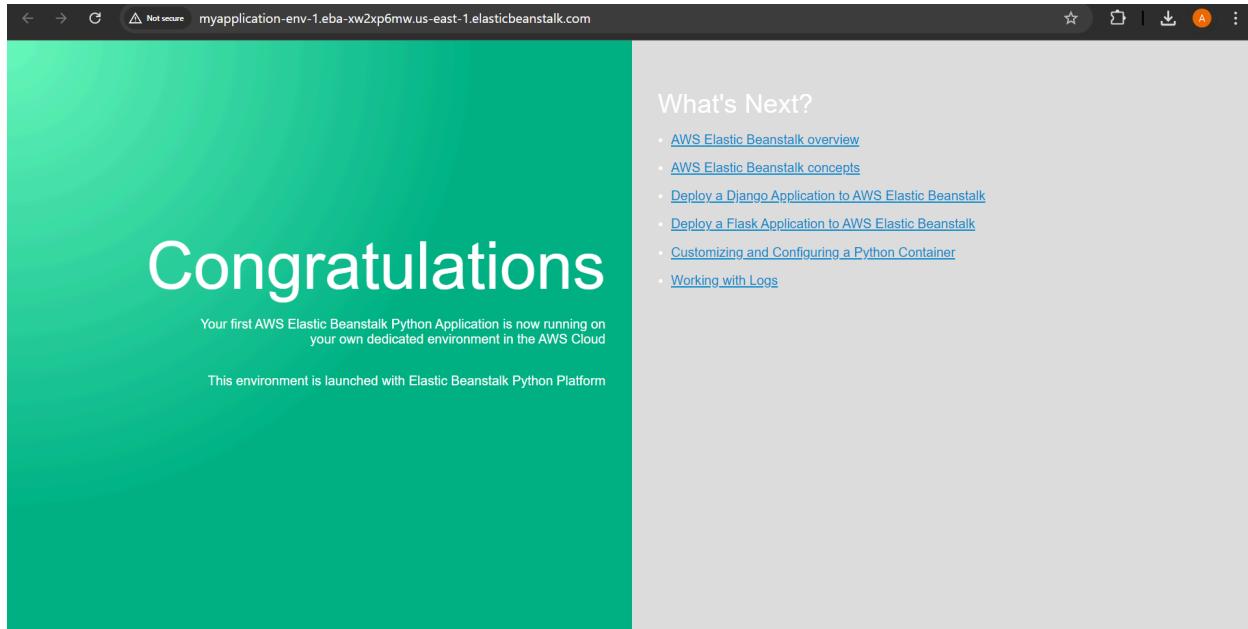
[Next](#)

Step 3 : add security config and review all settings

<p>Monitoring interval</p> <p>5 minute</p> <p>Instance metadata service (IMDS)</p> <p>Your environment's platform supports both IMDSv1 and IMDSv2. To enforce IMDSv2, deactivate IMDSv1. Learn more [?]</p> <p>IMDSv1</p> <p>With the current setting, the environment enables only IMDSv2.</p> <p><input checked="" type="checkbox"/> Deactivated</p> <p>EC2 security groups</p> <p>Select security groups to control traffic.</p> <p>EC2 security groups (2)</p> <table border="1"><thead><tr><th colspan="2">EC2 security groups (2)</th></tr><tr><th colspan="2"><input type="text"/> Filter security groups</th></tr><tr><th></th><th>Group name</th><th>Group ID</th><th>Name</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td>default</td><td>sg-0f6dae36cfa86246b</td><td></td></tr><tr><td><input checked="" type="checkbox"/></td><td>launch-wizard-1</td><td>sg-0ddee33c2cc66868</td><td></td></tr></tbody></table>	EC2 security groups (2)		<input type="text"/> Filter security groups			Group name	Group ID	Name	<input type="checkbox"/>	default	sg-0f6dae36cfa86246b		<input checked="" type="checkbox"/>	launch-wizard-1	sg-0ddee33c2cc66868		
EC2 security groups (2)																	
<input type="text"/> Filter security groups																	
	Group name	Group ID	Name														
<input type="checkbox"/>	default	sg-0f6dae36cfa86246b															
<input checked="" type="checkbox"/>	launch-wizard-1	sg-0ddee33c2cc66868															

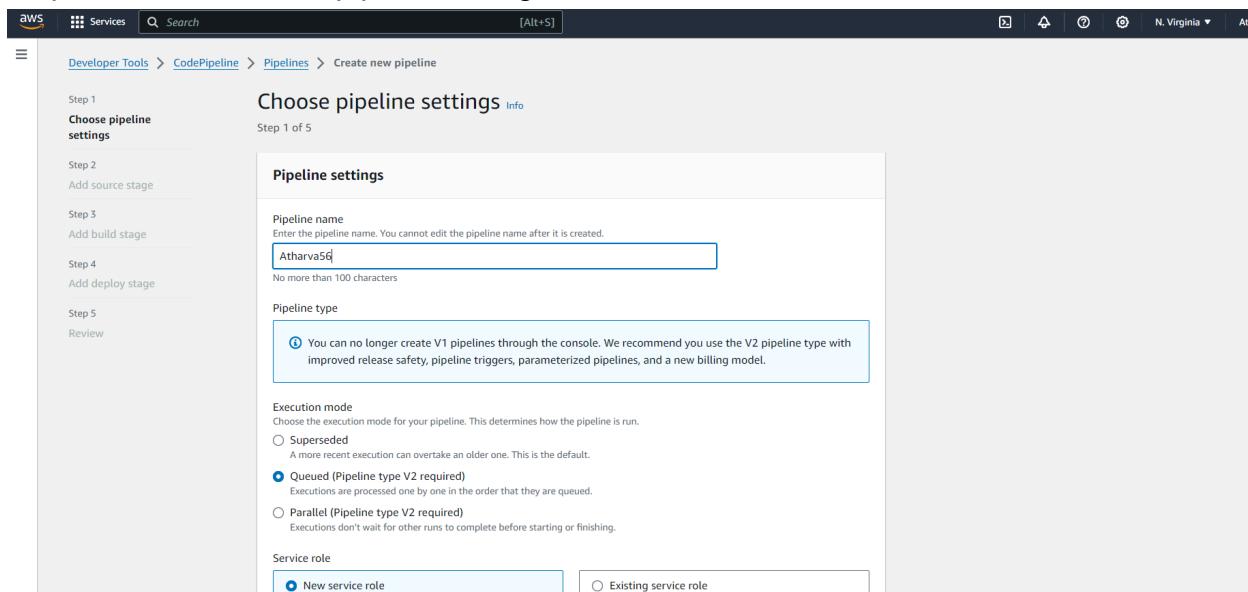
<p>Step 1 Configure environment</p> <hr/> <p>Step 2 Configure service access</p> <hr/> <p>Step 3 - optional Set up networking, database, and tags</p> <hr/> <p>Step 4 - optional Configure instance traffic and scaling</p> <hr/> <p>Step 5 - optional Configure updates, monitoring, and logging</p> <hr/> <p>Step 6 Review</p>	<p>Review Info</p> <p>Step 1: Configure environment Edit</p> <p>Environment information</p> <table><tr><td>Environment tier</td><td>Application name</td></tr><tr><td>Web server environment</td><td>myapplication</td></tr><tr><td>Environment name</td><td>Application code</td></tr><tr><td>Myapplication-env</td><td>Sample application</td></tr><tr><td>Platform</td><td></td></tr><tr><td>arn:aws:elasticbeanstalk:us-east-1::platform/Python 3.11</td><td></td></tr><tr><td>running on 64bit Amazon Linux 2023/4.1.3</td><td></td></tr></table> <p>Step 2: Configure service access Edit</p> <p>Service access Info</p> <p>Configure the service role and EC2 instance profile that Elastic Beanstalk uses to manage your environment. Choose an EC2 key pair to securely log in to your EC2 instances.</p> <table><tr><td>Service role</td><td>EC2 key pair</td><td>EC2 instance profile</td></tr><tr><td>arn:aws:iam::396913710384:role/aws-elasticbeanstalk-service-role</td><td>vockey</td><td>aws-elasticbeanstalk-ec2-role</td></tr></table>	Environment tier	Application name	Web server environment	myapplication	Environment name	Application code	Myapplication-env	Sample application	Platform		arn:aws:elasticbeanstalk:us-east-1::platform/Python 3.11		running on 64bit Amazon Linux 2023/4.1.3		Service role	EC2 key pair	EC2 instance profile	arn:aws:iam::396913710384:role/aws-elasticbeanstalk-service-role	vockey	aws-elasticbeanstalk-ec2-role
Environment tier	Application name																				
Web server environment	myapplication																				
Environment name	Application code																				
Myapplication-env	Sample application																				
Platform																					
arn:aws:elasticbeanstalk:us-east-1::platform/Python 3.11																					
running on 64bit Amazon Linux 2023/4.1.3																					
Service role	EC2 key pair	EC2 instance profile																			
arn:aws:iam::396913710384:role/aws-elasticbeanstalk-service-role	vockey	aws-elasticbeanstalk-ec2-role																			

Step 4 : Beanstalk environment is created



Pipeline Creation

Step 1 : click on create pipeline and give name



Step 2 : Add Your github account and add the file to add to pipeline deployment

The screenshot shows the 'Create new pipeline' wizard at Step 2 of 5, specifically the 'Add source stage' step. The left sidebar lists steps 1 through 5: 'Choose pipeline settings', 'Add source stage' (selected), 'Add build stage', 'Add deploy stage', and 'Review'. The main panel title is 'Add source stage' with an 'info' link. It displays a 'Source' provider dropdown set to 'GitHub (Version 1)' with a 'Connected' status message and a green success notification: 'You have successfully configured the action with the provider.' A blue info box warns that the GitHub (Version 1) action is not recommended due to OAuth app usage, suggesting the GitHub (Version 2) action instead. Below these, fields for 'Repository' (set to 'atharva2125/experiment1') and 'Branch' (set to 'main') are shown. Under 'Change detection options', two radio button options are available: 'GitHub webhooks (recommended)' (selected) and 'AWS CodePipeline'. At the bottom right are 'Cancel', 'Previous', and 'Next' buttons, with 'Next' being orange.

Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1
Choose pipeline settings

Step 2
Add source stage

Step 3
Add build stage

Step 4
Add deploy stage

Step 5
Review

Add source stage [Info](#)

Step 2 of 5

Source

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

GitHub (Version 1)

Grant AWS CodePipeline access to your GitHub repository. This allows AWS CodePipeline to upload commits from GitHub to your pipeline.

Connected

You have successfully configured the action with the provider. [X](#)

i **The GitHub (Version 1) action is not recommended**
The selected action uses OAuth apps to access your GitHub repository. This is no longer the recommended method. Instead, choose the GitHub (Version 2) action to access your repository by creating a connection. Connections use GitHub Apps to manage authentication and can be shared with other resources. [Learn more](#)

Repository

atharva2125/experiment1 [X](#)

Branch

main [X](#)

Change detection options
Choose a detection mode to automatically start your pipeline when a change occurs in the source code.

GitHub webhooks (recommended)
Use webhooks in GitHub to automatically start my pipeline when a change occurs

AWS CodePipeline
Use AWS CodePipeline to check periodically for changes

Cancel Previous **Next**

Step 3 : Add deploy config choosing the elastic beanstalk

Step 4
Add deploy stage

Step 5
Review

Deploy

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

AWS Elastic Beanstalk ▾

Region
US East (N. Virginia) ▾

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

No more than 100 characters

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

myapplication

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

Myapplication-env-1

Configure automatic rollback on stage failure

Cancel Previous **Next**

Step 5 : view the pipeline build and deployment

Atharva56

Pipeline type: V2 Execution mode: QUEUED

Source Succeeded
Pipeline execution ID: [09b793a3-71f9-4fc8-8bc7-9374f2d5a2e9](#)

Source
[GitHub \(Version_1\)](#)
 Succeeded - Just now
[bbc38add](#)
[View details](#)

[bbc38add](#) Source: first commit

[Disable transition](#)

Deploy In progress
Pipeline execution ID: [09b793a3-71f9-4fc8-8bc7-9374f2d5a2e9](#)

Step 6 : Check the deployed website at beanstalk link



Pixel Perfect

About
Services
Contact

Pixel Perfect is company which transform your digital vision into reality.

creative by profession

graphic design | web development | mobile app development | ux/ui design

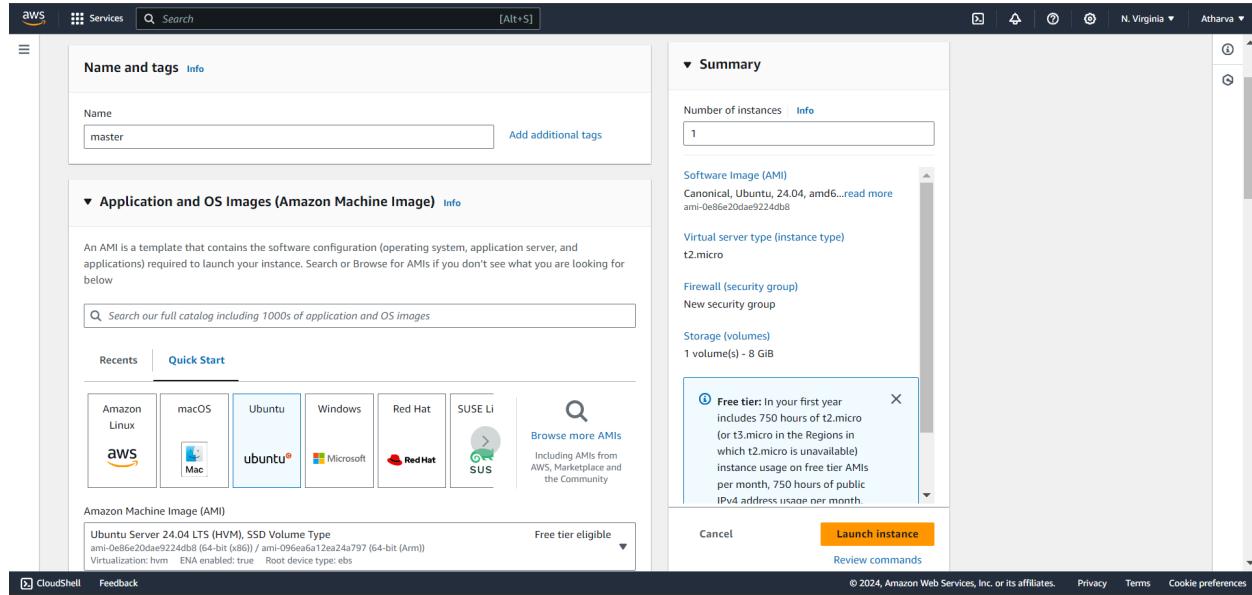
Watch Our Promotional Video



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

Step 1:Prerequisites

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



1.2 Proceed with the following settings and create a new key pair as follows(use the same key pair for all the three nodes)

AWS Services Search [Alt+S] Mumbai Atharva

Name and tags [Info](#)

Name Add additional tags

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

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

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux

Browse more AMIs Including AMIs from AWS Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type ami-0522ab6e1ddc705 (64-bit (x86)) / ami-0000791baef666add5 (64-bit (Arm)) Free tier eligible Virtualization: hvm ENA enabled: true Root device type: ebs

Summary

Number of instances [Info](#) 1

Software Image (AMI) Canonical, Ubuntu, 24.04, amd64... [read more](#) ami-0522ab6e1ddc705

Virtual server type (instance type) t2.micro

Firewall (security group) New security group

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

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month

Cancel Launch instance

The screenshot shows the AWS Lambda console with the following details:

- Function name:** HelloWorld
- Runtime:** Python 3.8
- Description:** A simple Lambda function that prints "Hello World" to the CloudWatch logs.
- Code entry type:** Lambda provided
- Code:** (Not visible in the screenshot)
- Environment:** (Not visible in the screenshot)
- Logs:** CloudWatch Logs
- Test:** Test
- Deployment:** Deploy
- Logs:** CloudWatch Logs

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.
 The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

RSA RSA encrypted private and public key pair

ED25519 ED25519 encrypted private and public key pair

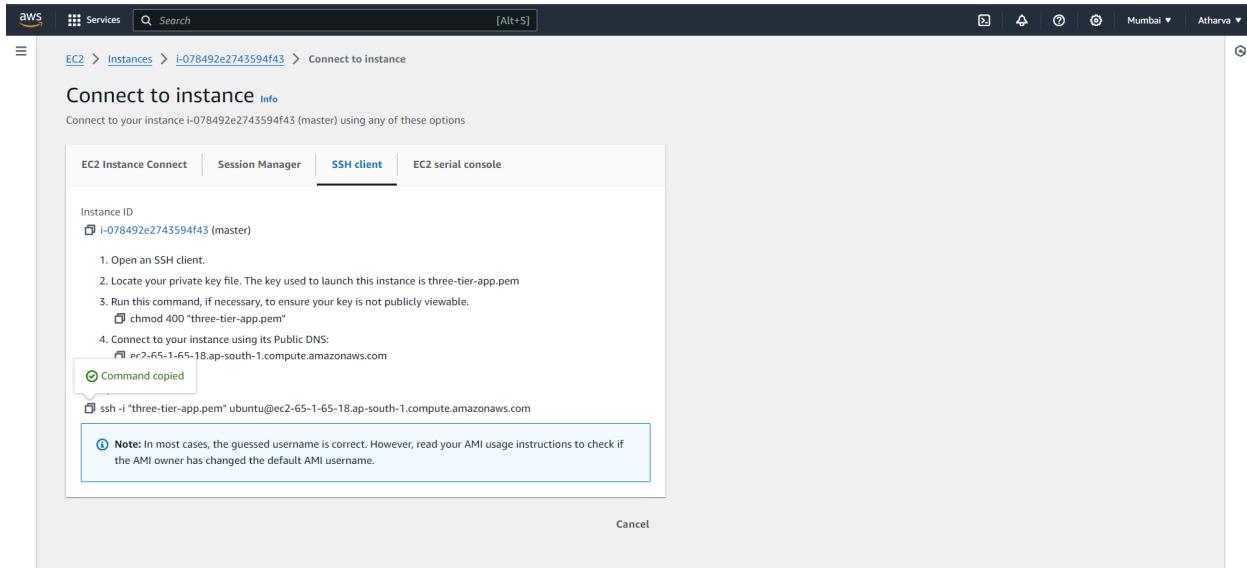
Private key file format

.pem For use with OpenSSH

.ppk For use with PuTTY

⚠️ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

Cancel Create key pair



1.3 Add port 6443 in each security group

The screenshot shows the 'Inbound rules' section of the AWS Security Groups page. It lists two rules:

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-0cf20b6a9f8501fc6	Custom TCP	TCP	6443	Custom	0.0.0.0/0
sgr-0e02c88e6fce1b710	SSH	TCP	22	Custom	0.0.0.0/0

At the bottom left is a 'Add rule' button.

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

```
C:\Users\Atharva\Downloads>ssh -i "three-tier-app.pem" ubuntu@ec2-65-1-65-18.ap-south-1.compute.amazonaws.com
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1012-aws x86_64)

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

System information as of Sat Sep 21 10:50:19 UTC 2024

 System load:  0.11           Processes:      115
 Usage of /:   22.9% of 6.71GB  Users logged in:  0
 Memory usage: 5%            IPv4 address for enX0: 172.31.46.220
 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

Last login: Sat Sep 21 10:44:19 2024 from 49.36.97.186
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

Step 2: Run the following commands on both the master and worker nodes to prepare them for kubeadm.

```
# disable swap
sudo swapoff -a
```

```
# Create the .conf file to load the modules at bootup
cat <<EOF | sudo tee /etc/modules-load.d/k8s.conf
overlay
br_netfilter
EOF
```

```
sudo modprobe overlay
sudo modprobe br_netfilter
```

```
# sysctl params required by setup, params persist across reboots
cat <<EOF | sudo tee /etc/sysctl.d/k8s.conf
net.bridge.bridge-nf-call-iptables = 1
net.bridge.bridge-nf-call-ip6tables = 1
net.ipv4.ip_forward = 1
EOF
```

```
# Apply sysctl params without reboot
sudo sysctl --system
```

```
## Install CRI-O Runtime
sudo apt-get update -y
sudo apt-get install -y software-properties-common curl apt-transport-https
ca-certificates gpg

sudo curl -fsSL https://pkgs.k8s.io/addons:/cri-o:/prerelease:/main/deb/Release.key | 
sudo gpg --dearmor -o /etc/apt/keyrings/cri-o-apt-keyring.gpg
echo "deb [signed-by=/etc/apt/keyrings/cri-o-apt-keyring.gpg]
https://pkgs.k8s.io/addons:/cri-o:/prerelease:/main/deb/ /" | sudo tee
/etc/apt/sources.list.d/cri-o.list

sudo apt-get update -y
sudo apt-get install -y cri-o

sudo systemctl daemon-reload
sudo systemctl enable crio --now
sudo systemctl start crio.service

echo "CRI runtime installed successfully"

# Add Kubernetes APT repository and install required packages
curl -fsSL https://pkgs.k8s.io/core:/stable:/v1.29/deb/Release.key | sudo gpg --dearmor
-o /etc/apt/keyrings/kubernetes-apt-keyring.gpg
echo 'deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg]
https://pkgs.k8s.io/core:/stable:/v1.29/deb/ /' | sudo tee
/etc/apt/sources.list.d/kubernetes.list

sudo apt-get update -y
sudo apt-get install -y kubelet="1.29.0-*" kubectl="1.29.0-*" kubeadm="1.29.0-*"
sudo apt-get update -y
sudo apt-get install -y jq

sudo systemctl enable --now kubelet
sudo systemctl start kubelet
```

```

ubuntu@ip-172-31-46-220:~$ # disable swap
sudo swapoff -a

# Create the .conf file to load the modules at bootup
cat <<EOF | sudo tee /etc/modules-load.d/k8s.conf
overlay
br_netfilter
EOF

sudo modprobe overlay
sudo modprobe br_netfilter

# sysctl params required by setup, params persist across reboots
cat <<EOF | sudo tee /etc/sysctl.d/k8s.conf
net.bridge.bridge-nf-call-iptables = 1
net.bridge.bridge-nf-call-ip6tables = 1
net.ipv4.ip_forward = 1
EOF

# Apply sysctl params without reboot
sudo sysctl --system

## Install CRIU Runtime
sudo apt-get update -y
sudo apt-get install -y software-properties-common curl apt-transport-https ca-certificates gpg

sudo curl -fsSL https://pkgs.k8s.io/addons:/cri-o:/prerelease:/main/deb/Release.key | sudo gpg --dearmor -o /etc/apt/keyrings/cri-o-apt-keyring.gpg
echo "deb [signed-by=/etc/apt/keyrings/cri-o-apt-keyring.gpg] https://pkgs.k8s.io/addons:/cri-o:/prerelease:/main/deb/ /" | sudo tee /etc/apt/sources.list.d/crio.list
sudo apt-get update -y
sudo apt-get install cri-o=1.29.0-0k8s.io-00000000000000000000000000000000

# OverlayFS and BRIDGE_NF call-iptables/ip6tables modules
# These modules are required for kubelet to work with CRIU
# They are loaded via /etc/modules-load.d/k8s.conf
# They are also loaded via /etc/init.d/crio
# They are also loaded via /etc/cron.d/crio

# OverlayFS module
# This module is required for kubelet to work with CRIU
# It is loaded via /etc/modules-load.d/k8s.conf
# It is also loaded via /etc/init.d/crio
# It is also loaded via /etc/cron.d/crio

# BRIDGE_NF call-iptables module
# This module is required for kubelet to work with CRIU
# It is loaded via /etc/modules-load.d/k8s.conf
# It is also loaded via /etc/init.d/crio
# It is also loaded via /etc/cron.d/crio

# BRIDGE_NF call-ip6tables module
# This module is required for kubelet to work with CRIU
# It is loaded via /etc/modules-load.d/k8s.conf
# It is also loaded via /etc/init.d/crio
# It is also loaded via /etc/cron.d/crio

# net.ipv4.ip_forward module
# This module is required for kubelet to work with CRIU
# It is loaded via /etc/modules-load.d/k8s.conf
# It is also loaded via /etc/init.d/crio
# It is also loaded via /etc/cron.d/crio

# kernel-hardening module
# This module is required for kubelet to work with CRIU
# It is loaded via /etc/modules-load.d/k8s.conf
# It is also loaded via /etc/init.d/crio
# It is also loaded via /etc/cron.d/crio

# magic-sysrq module
# This module is required for kubelet to work with CRIU
# It is loaded via /etc/modules-load.d/k8s.conf
# It is also loaded via /etc/init.d/crio
# It is also loaded via /etc/cron.d/crio

# map-count module
# This module is required for kubelet to work with CRIU
# It is loaded via /etc/modules-load.d/k8s.conf
# It is also loaded via /etc/init.d/crio
# It is also loaded via /etc/cron.d/crio

# network-security module
# This module is required for kubelet to work with CRIU
# It is loaded via /etc/modules-load.d/k8s.conf
# It is also loaded via /etc/init.d/crio
# It is also loaded via /etc/cron.d/crio

# ptrace module
# This module is required for kubelet to work with CRIU
# It is loaded via /etc/modules-load.d/k8s.conf
# It is also loaded via /etc/init.d/crio
# It is also loaded via /etc/cron.d/crio

# cloudimg-ipv6 module
# This module is required for kubelet to work with CRIU
# It is loaded via /etc/modules-load.d/k8s.conf
# It is also loaded via /etc/init.d/crio
# It is also loaded via /etc/cron.d/crio

# pid-max module
# This module is required for kubelet to work with CRIU
# It is loaded via /etc/modules-load.d/k8s.conf
# It is also loaded via /etc/init.d/crio
# It is also loaded via /etc/cron.d/crio

# protect-links module
# This module is required for kubelet to work with CRIU
# It is loaded via /etc/modules-load.d/k8s.conf
# It is also loaded via /etc/init.d/crio
# It is also loaded via /etc/cron.d/crio

# sysctl module
# This module is required for kubelet to work with CRIU
# It is loaded via /etc/modules-load.d/k8s.conf
# It is also loaded via /etc/init.d/crio
# It is also loaded via /etc/cron.d/crio

# Applying /usr/lib/sysctl.d/10-apply-messages.conf ...
# Applying /etc/sysctl.d/10-console-messages.conf ...
# Applying /etc/sysctl.d/10-ipv6-privacy.conf ...
# Applying /etc/sysctl.d/10-kernel-hardening.conf ...
# Applying /etc/sysctl.d/10-magic-sysrq.conf ...
# Applying /etc/sysctl.d/10-map-count.conf ...
# Applying /etc/sysctl.d/10-network-security.conf ...
# Applying /etc/sysctl.d/10-ptrace.conf ...
# Applying /etc/sysctl.d/10-protect-links.conf ...
# Applying /etc/sysctl.d/99-cloudimg-ipv6.conf ...
# Applying /etc/lib/sysctl.d/99-pid-max.conf ...
# Applying /etc/lib/sysctl.d/99-protect-links.conf ...
# Applying /usr/lib/sysctl.d/99-protect-links.conf ...
# Applying /etc/sysctl.d/99-sysctl.com ...

```

Step3: Run the above command only on master node

sudo kubeadm config images pull

sudo kubeadm init

```

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

```

```

# Network Plugin = calico
kubectl apply -f
https://raw.githubusercontent.com/projectcalico/calico/v3.26.0/manifests/calico.yaml

```

kubeadm token create --print-join-command

```

ubuntu@ip-172-31-46-220:~$ sudo kubeadm config images pull
sudo kubeadm init
mkdir -p "$HOME"/.kube
sudo cp -i /etc/kubernetes/admin.conf "$HOME"/.kube/config
sudo chown "$(id -u)": "$(id -g)" "$HOME"/.kube/config

# Network Plugin = calico
kubectl apply -f https://raw.githubusercontent.com/projectcalico/calico/v3.26.0/manifests/calico.yaml

kubeadm token create --print-join-command
W0921 11:12:21.776389 3863 version.go:256] remote version is much newer: v1.31.0; falling back to: stable-1.29
[config/images] Pulled registry.k8s.io/kube-apiserver:v1.29.9
[config/images] Pulled registry.k8s.io/kube-controller-manager:v1.29.9
[config/images] Pulled registry.k8s.io/kube-scheduler:v1.29.9
[config/images] Pulled registry.k8s.io/kube-proxy:v1.29.9
[config/images] Pulled registry.k8s.io/coredns/coredns:v1.11.1
[config/images] Pulled registry.k8s.io/pause:3.9
[config/images] Pulled registry.k8s.io/etcd:v3.5.10-0
W0921 11:12:41.958409 4304 version.go:256] remote version is much newer: v1.31.0; falling back to: stable-1.29
[join] Using Kubernetes version v1.29.9
[preflight] Running pre-flight checks
[preflight] Pulling images required for setting up a Kubernetes cluster
[preflight] This might take a minute or two, depending on the speed of your internet connection
[preflight] You can also perform this action in beforehand using 'kubeadm config images pull'
W0921 11:12:41.763411 4304 checks.go:835] detected that the sandbox image "registry.k8s.io/pause:3.10" of the container runtime is inconsistent with that used by kubeadm. It is recommended that using "registry.k8s.io/pause:3.9" as the CRI sandbox image.
[certs] Generating "apiserver" certificate and key
[certs] Generating "apiserver" certificate and key
[certs] apiserver serving cert is signed for DNS names [ip-172-31-46-220 kubernetes kubernetes.default kubernetes.default.svc kubernetes.default.svc.cluster.local] and IPs [10.96.0.1 172.31.46.220]
[certs] Generating "apiserver-kubelet-client" certificate and key
[certs] Generating "front-proxy-ca" certificate and key
[certs] Generating "front-proxy-client" certificate and key
[certs] Generating "etcd/ca" certificate and key
[certs] Generating "etcd/server" certificate and key
[certs] Generating "etcd-peer" certificate and key
[certs] etcd/peer serving cert is signed for DNS names [ip-172-31-46-220 localhost] and IPs [172.31.46.220 127.0.0.1 ::1]
[certs] Generating "etcd/healthcheck-client" certificate and key
[certs] Generating "apiserver-etcd-client" certificate and key
[certs] Generating "sa" key and public key
[kubeconfig] Using kubeconfig folder "/etc/kubernetes"
[kubeconfig] Writing "admin.conf" kubeconfig file
[kubeconfig] Writing "super-admin.conf" kubeconfig file
[kubeconfig] Writing "etcd-peer.conf" kubeconfig file
[kubeconfig] Writing "controller-manager.conf" kubeconfig file
[kubeconfig] Writing "scheduler.conf" kubeconfig file
[etcd] Creating static Pod manifest for local etcd in "/etc/kubernetes/manifests"

```

You will get kubeadm token, Copy it.

Step 4: Run the above command only on worker nodes

sudo kubeadm reset pre-flight checks
 sudo your-token --v=5

```

ubuntu@ip-172-31-36-212:~$ sudo kubeadm reset pre-flight checks
W0921 11:14:17.713669 3933 preflight.go:56] [reset] WARNING: Changes made to this host by 'kubeadm init' or 'kubeadm join' will be reverted.
[reset] Are you sure you want to proceed? [y/N]: yes
[preflight] Running pre-flight checks
W0921 11:14:28.535200 3933 removeetcdmember.go:106] [reset] No kubeadm config, using etcd pod spec to get data directory
[reset] Deleted contents of the etcd data directory: /var/lib/etcd
[reset] Stopping the kubelet service
[reset] Deleting mounted directories in "/var/lib/kubelet"
[reset] Deleting contents of directories: /etc/kubernetes/manifests /var/lib/kubelet /etc/kubernetes/pki
[reset] Deleting files: [/etc/kubernetes/admin.conf /etc/kubernetes/super-admin.conf /etc/kubernetes/kubelet.conf /etc/kubernetes/bootstrap-kubelet.conf /etc/kubernetes/controller-manager.conf /etc/kubernetes/scheduler.conf]

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

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

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

The reset process does not clean your kubeconfig files and you must remove them manually.

```

```

ubuntu@ip-172-31-36-212:~$ sudo kubeadm join 172.31.46.220:6443 --token k4psyh.ns1g1yett9he59kd4 --discovery-token-ca-cert-hash sha256:80e7e9abf8f31f0333a9d2f7a680d6bd961267ae45cf71bada8de069d4a292e --v=5
I0921 11:28:31.063878 4097 join.go:413] [preflight] found NodeName empty; using OS hostname as NodeName
I0921 11:28:31.063885 4097 initConfiguration.go:122] detected and using CRI socket: unix:///var/run/crio/crio.sock
[preflight] Running pre-flight checks
I0921 11:28:31.064142 4097 preFlight.go:93] [preflight] Running general checks
I0921 11:28:31.064183 4097 checks.go:280] validating the existence of file /etc/kubernetes/kubelet.conf
I0921 11:28:31.064287 4097 checks.go:280] validating the existence of file /etc/kubernetes/bootstrap-kubelet.conf
I0921 11:28:31.064219 4097 checks.go:184] validating the container runtime
I0921 11:28:31.089669 4097 checks.go:639] validating whether swap is enabled or not
I0921 11:28:31.089763 4097 checks.go:280] validating the presence of executable crictl
I0921 11:28:31.089799 4097 checks.go:370] validating the presence of executable cointtrack
I0921 11:28:31.089810 4097 checks.go:370] validating the presence of executable dmesg
I0921 11:28:31.089818 4097 checks.go:370] validating the presence of executable iptables
I0921 11:28:31.089870 4097 checks.go:370] validating the presence of executable mount
I0921 11:28:31.089897 4097 checks.go:370] validating the presence of executable nsenter
I0921 11:28:31.089919 4097 checks.go:370] validating the presence of executable ebttables
I0921 11:28:31.089954 4097 checks.go:370] validating the presence of executable ethtool
I0921 11:28:31.089977 4097 checks.go:370] validating the presence of executable socat
I0921 11:28:31.089996 4097 checks.go:370] validating the presence of executable tc
I0921 11:28:31.089911 4097 checks.go:370] validating the presence of executable touch
I0921 11:28:31.089953 4097 checks.go:370] validating the presence of executable curl
I0921 11:28:31.183935 4097 checks.go:401] checking whether the given node name is valid and reachable using net.LookupHost
I0921 11:28:31.185638 4097 checks.go:685] validating Kubelet version
I0921 11:28:31.162593 4097 checks.go:130] validating if the "kubelet" service is enabled and active
I0921 11:28:31.176512 4097 checks.go:283] validating availability of port 10259
I0921 11:28:31.176737 4097 checks.go:280] validating the existence of file /etc/kubernetes/pki/ca.crt
I0921 11:28:31.176765 4097 checks.go:430] validating if the connectivity type is via proxy or direct
I0921 11:28:31.176893 4097 checks.go:329] validating the contents of file /proc/sys/net/bridge/bridge-nf-call-iptables
I0921 11:28:31.176909 4097 checks.go:329] validating the contents of file /proc/sys/net/ipv4/ip_forward
I0921 11:28:31.176983 4097 checks.go:521] [preflight] Discovering cluster info
I0921 11:28:31.176987 4097 token.go:481] [discovery] Created cluster-info discovery client, requesting info from "172.31.46.220:6443"
I0921 11:28:31.187676 4097 token.go:118] [discovery] Requesting info from "172.31.46.220:6443" again to validate TLS against the pinned public key
I0921 11:28:31.194531 4097 token.go:135] [discovery] Cluster info signature and contents are valid and TLS certificate validates against pinned roots, will use API Server "172.31.46.220:6443"
I0921 11:28:31.194608 4097 discovery.go:52] [discovery] Using provided TLSBootstrapToken as authentication credentials for the join process
I0921 11:28:31.194622 4097 join.go:546] [preflight] Fetching init configuration
I0921 11:28:31.194629 4097 join.go:592] [preflight] Retrieving KubeConfig objects
[preflight] Retrieving configuration for the cluster
[preflight] If you look at this config file with 'kubectl -n kube-system get cm kubeade-config -o yaml'
I0921 11:28:31.281989 4097 kubeProxy.go:58] attempting to download the KubeProxyConfiguration from ConfigMap "kube-proxy"
I0921 11:28:31.285146 4097 kubelet.go:74] attempting to download the KubeletConfiguration from ConfigMap "kubelet-config"
I0921 11:28:31.289379 4097 initConfiguration.go:114] skip CRI socket detection, fill with the default CRI socket unix:///var/run/containerd/containerd.sock
I0921 11:28:31.289595 4097 interface.go:432] Looking for default routes with IPv4 addresses
I0921 11:28:31.289617 4097 interface.go:437] Default route transits interface "enX0"
I0921 11:28:31.289751 4097 interface.go:289] Interface enX0 is up
I0921 11:28:31.289839 4097 interface.go:259] Interface enX0 has 2 addresses : [172.31.36.212/20 fe80::75:41ff:fea5:aefb1/64].
I0921 11:28:31.289840 4097 interface.go:260] Checking addr: 172.31.36.212/20.
I0921 11:28:31.289829 4097 interface.go:231] IP found 172.31.36.212
I0921 11:28:31.289848 4097 interface.go:263] Found valid IPv4 address 172.31.36.212 for interface "enX0".
I0921 11:28:31.289849 4097 interface.go:443] Found active IP 172.31.36.212
I0921 11:28:31.215982 4097 preflight.go:184] [preflight] Running configuration dependant checks
I0921 11:28:31.215928 4097 controlplaneprepare.go:225] [download-certs] Skipping certs download

```

Step5: Run the given command to verify cluster creation

kubectl get nodes

ubuntu@ip-172-31-46-220:~\$ kubectl get nodes				
NAME	STATUS	ROLES	AGE	VERSION
ip-172-31-36-212	Ready	<none>	47s	v1.29.0
ip-172-31-46-220	Ready	control-plane	16m	v1.29.0
ip-172-31-47-26	Ready	<none>	29s	v1.29.0

Step 1: Deploying Your Application on Kubernetes

1.1 Set up Kubernetes Cluster

1. If you haven't already set up a Kubernetes cluster (e.g., with kubeadm), use minikube or any managed Kubernetes service (like EKS, GKE, etc.) to get a cluster running.

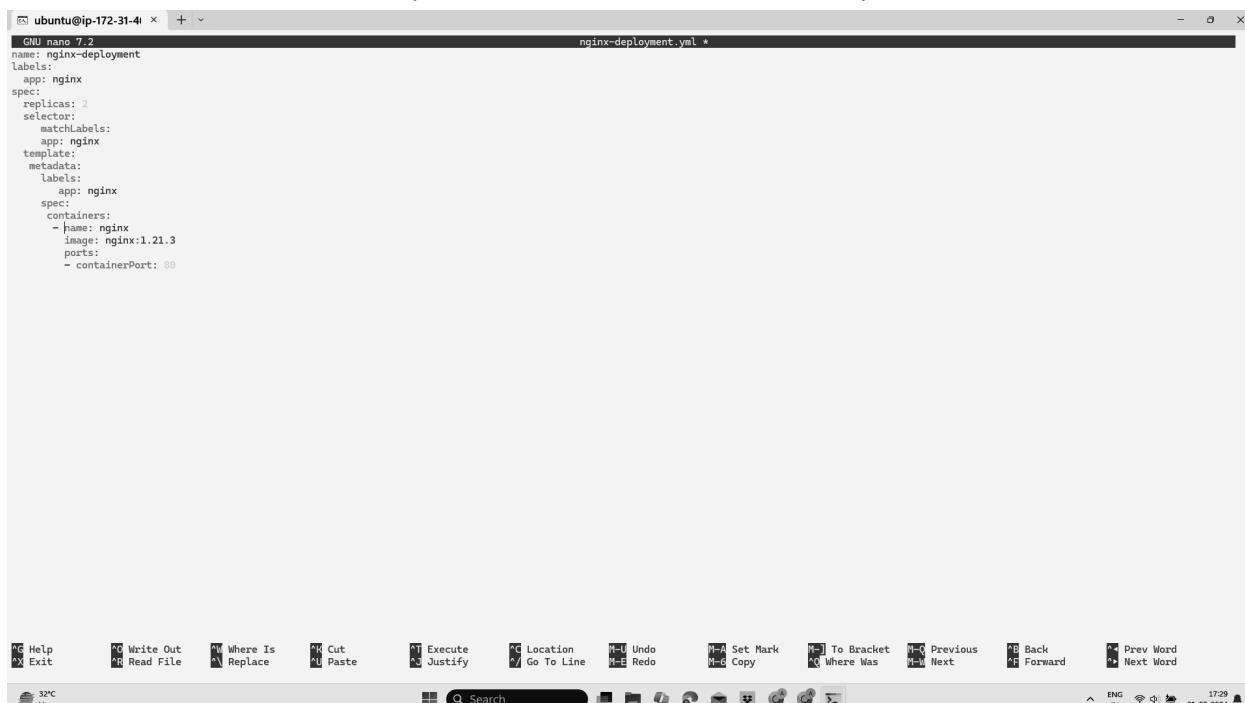
2. Once your cluster is ready, verify the nodes:

kubectl get nodes

```
ubuntu@ip-172-31-46-220:~$ kubectl get nodes
NAME           STATUS    ROLES      AGE     VERSION
ip-172-31-36-212   Ready    <none>    47s    v1.29.0
ip-172-31-46-220   Ready    control-plane   16m    v1.29.0
ip-172-31-47-26   Ready    <none>    29s    v1.29.0
```

Step 2: Create the Deployment YAML file

a) Create the YAML file: Use a text editor to create a file named nginx-deployment.yaml
Add the Deployment Configuration: Copy and paste the following YAML content into the file. Save and exit the editor (Press Ctrl+X, then Y, and Enter).



```
GNU nano 7.2                               nginx-deployment.yaml *
name: nginx-deployment
labels:
  app: nginx
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
        - name: nginx
          image: nginx:1.21.3
          ports:
            - containerPort: 80
```

Step 3:Create the Service YAML File

a) Create the YAML File: Create another file named nginx-service.yaml Add the Service Configuration: Copy and paste the following YAML content into the file given below



```
GNU nano 7.2
apiVersion: v1
kind: Service
metadata:
  name: nginx-server
spec:
  selector:
    app: nginx
  ports:
    - protocol: TCP
      port: 80
      targetport: 80
  type: loadbalancer
```

Step 4:Apply the YAML Files a) Deploy the Application: Use kubectl to create the Deployment and Service from the YAML files. Verify the Deployment: Check the status of your Deployment,Pods and Services. Describe the deployment(Extra)

```
ubuntu@ip-172-31-46-220:~$ kubectl apply -f nginx-deployment.yaml
deployment.apps/nginx-deployment created
```

```
ubuntu@ip-172-31-46-220:~$ kubectl apply -f nginx-service.yaml
service/nginx-server created
```

Step 5:Ensure Service is Running 6.1 Verify Service: Run the following command to check the services running in your cluster: Kubectl get deployment Kubectl get pods kubectl get service

```
error: the server doesn't have a resource type "deployments"
ubuntu@ip-172-31-46-220:~$ kubectl get deployments
NAME          READY   UP-TO-DATE   AVAILABLE   AGE
nginx-deployment  3/3     3           3           7m27s
```

```
ubuntu@ip-172-31-46-220:~$ kubectl get services
NAME      TYPE      CLUSTER-IP      EXTERNAL-IP      PORT(S)      AGE
kubernetes  ClusterIP  10.96.0.1      <none>        443/TCP      85m
nginx-server  LoadBalancer  10.111.218.213  <pending>      80:30798/TCP  110s
```

Step 6: Forward the Service Port to Your Local Machine kubectl port-forward allows you to forward a port from your local machine to a port on a service running in the Kubernetes cluster.

1. Forward the Service Port: Use the following command to forward a local port to the service's target port. kubectl port-forward service/ :

This command will forward local port 8080 on your machine to port 80 of the service nginx-service running inside the cluster.

```
ubuntu@ip-172-31-46-220:~$ kubectl describe deployments
Name:           nginx-deployment
Namespace:      default
CreationTimestamp: Sat, 21 Sep 2024 12:30:54 +0000
Labels:          app=nginx
Annotations:    deployment.kubernetes.io/revision: 1
Selector:        app=nginx
Replicas:       3 desired | 3 updated | 3 total | 3 available | 0 unavailable
StrategyType:   RollingUpdate
MinReadySeconds: 0
RollingUpdateStrategy: 25% max unavailable, 25% max surge
Pod Template:
  Labels:  app=nginx
  Containers:
    nginx:
      Image:      nginx:1.16
      Port:       80/TCP
      Host Port:  80/TCP
      Environment: <none>
      Mounts:     <none>
      Volumes:    <none>
  Conditions:
    Type     Status  Reason
    ----  -----
    Available  True    MinimumReplicasAvailable
    Progressing  True    NewReplicaSetAvailable
  OldReplicaSets: <none>
  NewReplicaSet:  nginx-deployment-854bc88786 (3/3 replicas created)
Events:
  Type     Reason          Age   From            Message
  ----  -----  --  --  -----
  Normal  ScalingReplicaSet 11m  deployment-controller  Scaled up replica set nginx-deployment-854bc88786 to 3
```

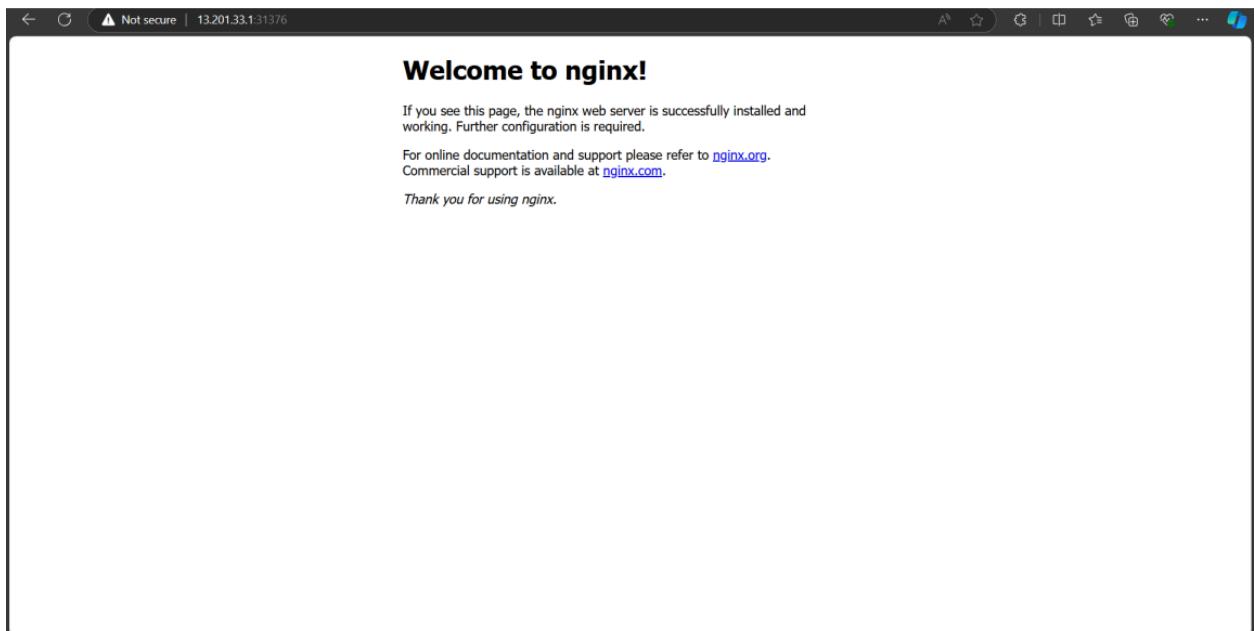
2. This means port forwarding is now active, and any traffic to localhost:8080 will be routed to the nginx-service on port 80.

```
ubuntu@ip-172-31-46-220:~$ kubectl port-forward service/nginx-server 8080:80
```

Step 7:

Access the Application Locally

1. Open a Web Browser: Now open your web browser and go to the following URL:
<http://localhost:8080> You should see the application (in this case, Nginx) that you have deployed running in the Kubernetes cluster, served locally via port 8080. In case the port 8080 is unavailable, try using a different port like 8081



Advance devops Exp:5

Atharva Prabhu

D15 A-43

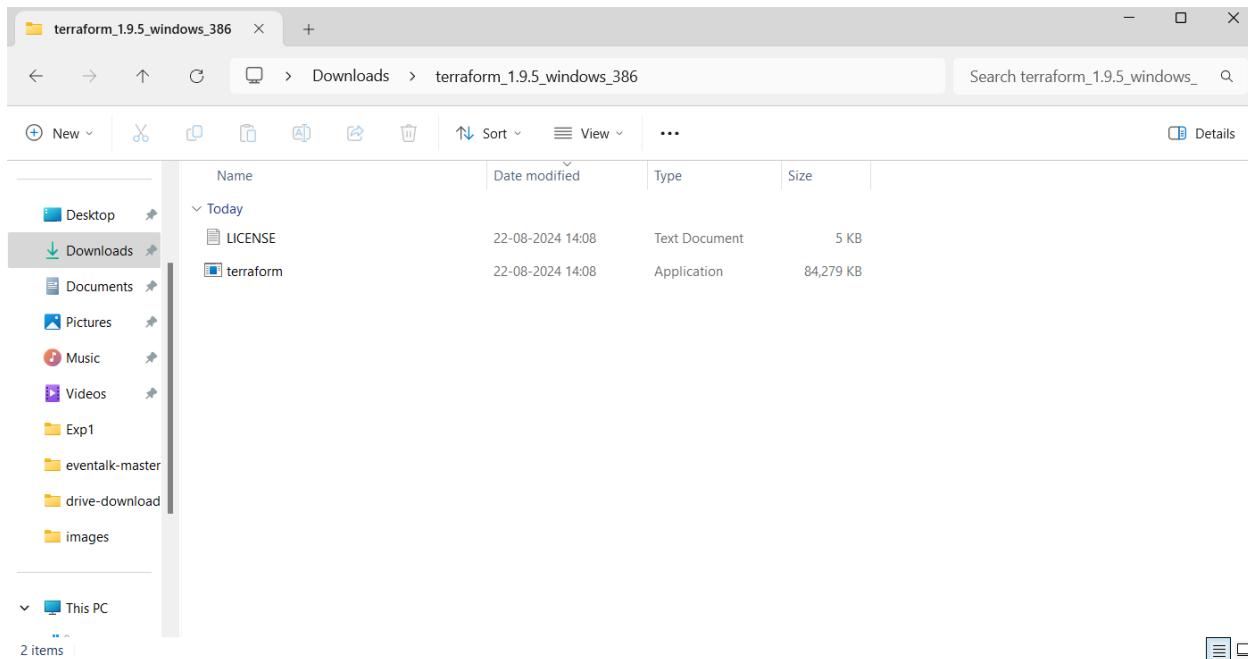
Aim: To understand terraform lifecycle, core concepts/terminologies and install it on a linux machine and windows

Step1: Download Terraform from the official website

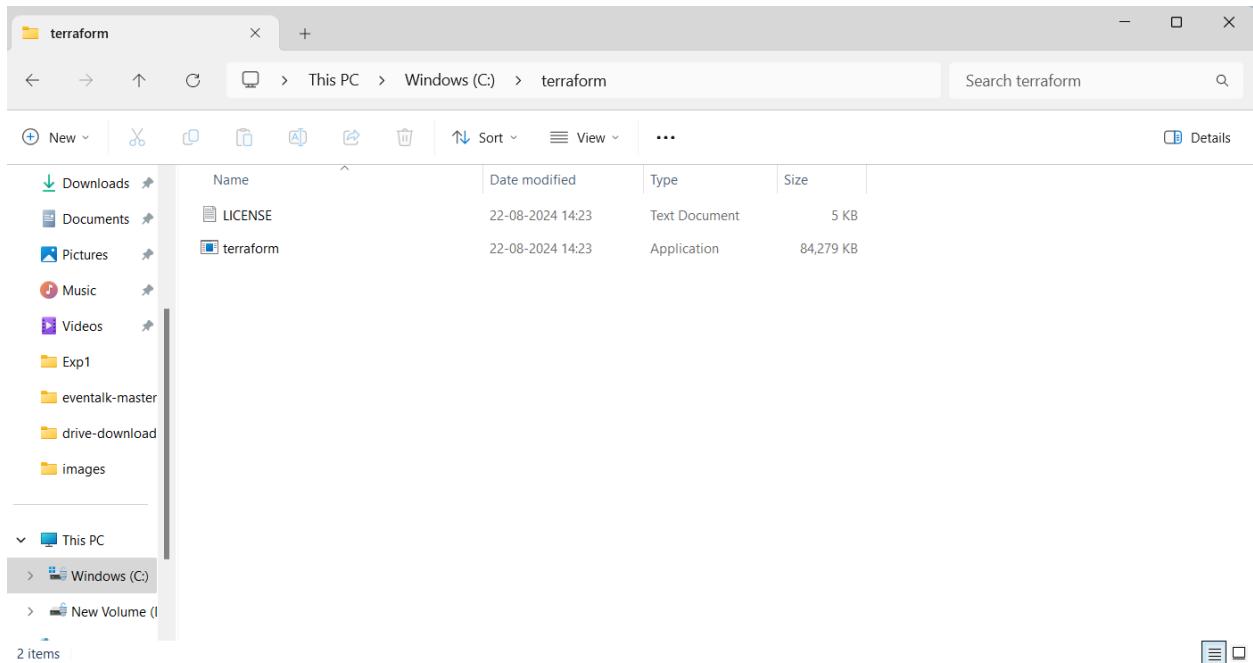
The screenshot shows the HashiCorp Terraform website's 'Install Terraform' page for macOS. The left sidebar has 'macOS' selected under 'Operating Systems'. The main content area shows the 'macOS' section with a package manager section containing a terminal command:

```
brew tap hashicorp/tap
brew install hashicorp/tap/terraform
```

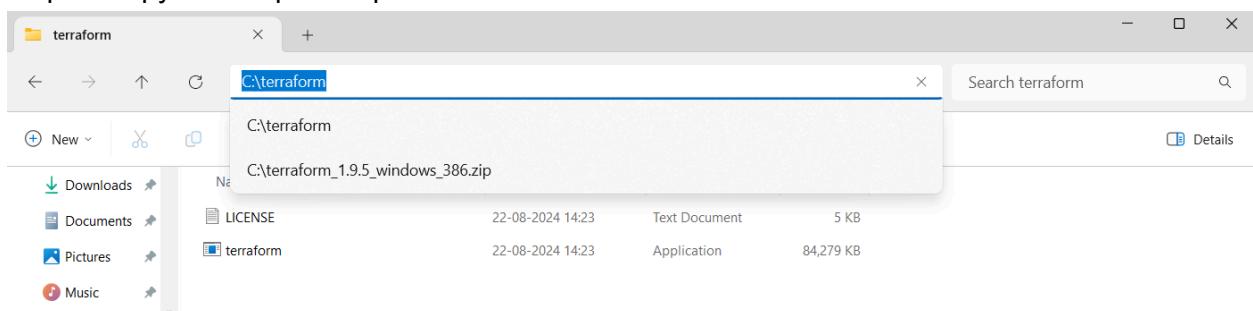
and a binary download section with links for AMD64 and ARM64 versions. The right sidebar contains sections for 'About Terraform', 'Featured docs', and 'HCP Terraform'.



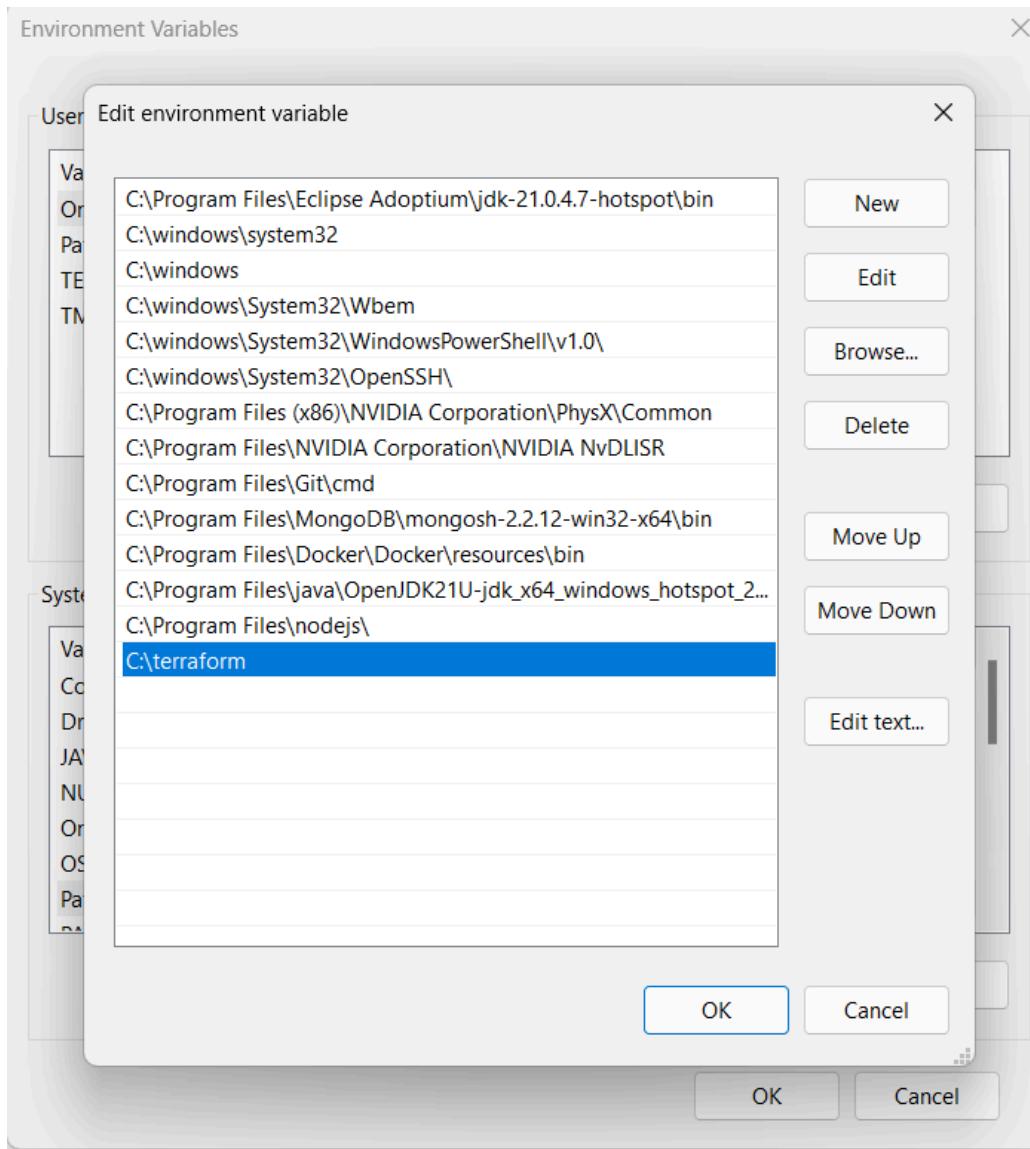
Step 2: Copy and extract Terraform from the downloads and paste it in the C drive



Step 3: Copy the file path to paste in the environment variables



Step 4: Set the environment variables for terraform



Step 5: Check whether the terraform is installed

```
Microsoft Windows [Version 10.0.22631.4037]
(c) Microsoft Corporation. All rights reserved.

C:\Users\navan>terraform --version
Terraform v1.9.5
on windows_386
```

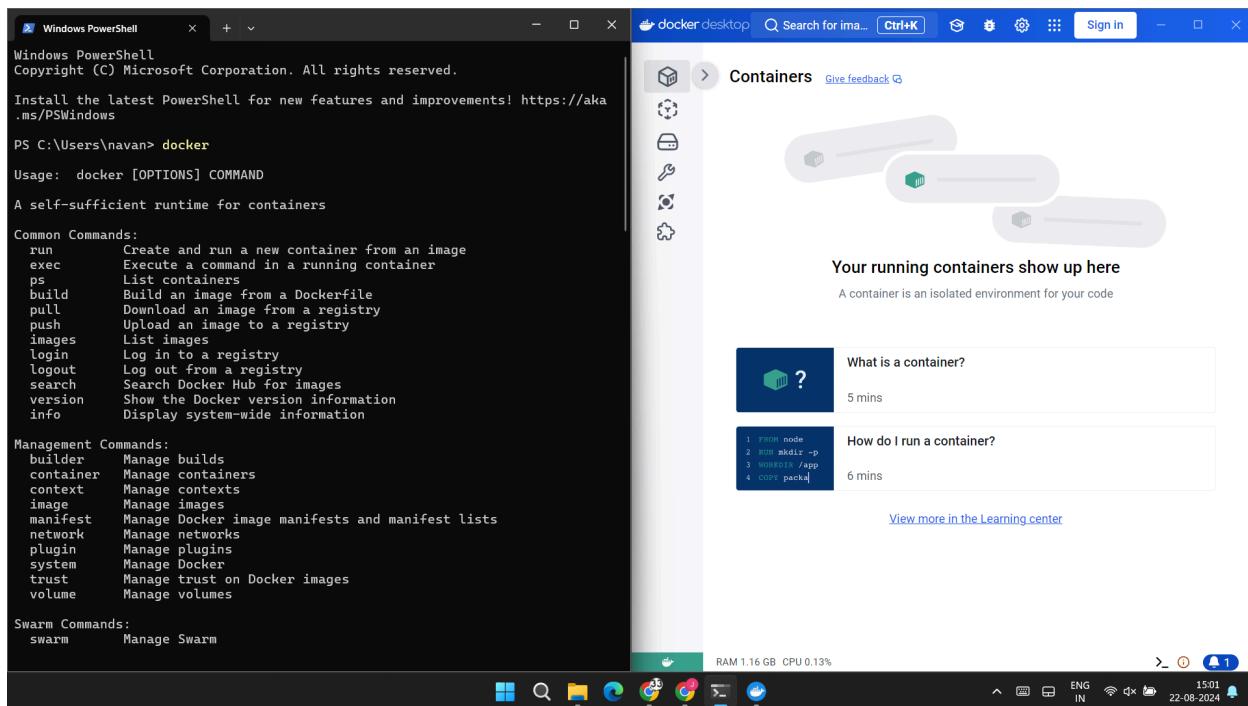
Advance Devops Experiment 6

Atharva Prabhu

D15 A-43

Aim: Creating docker image using Terraform

Step 1: Install docker Desktop after installation check the functionality



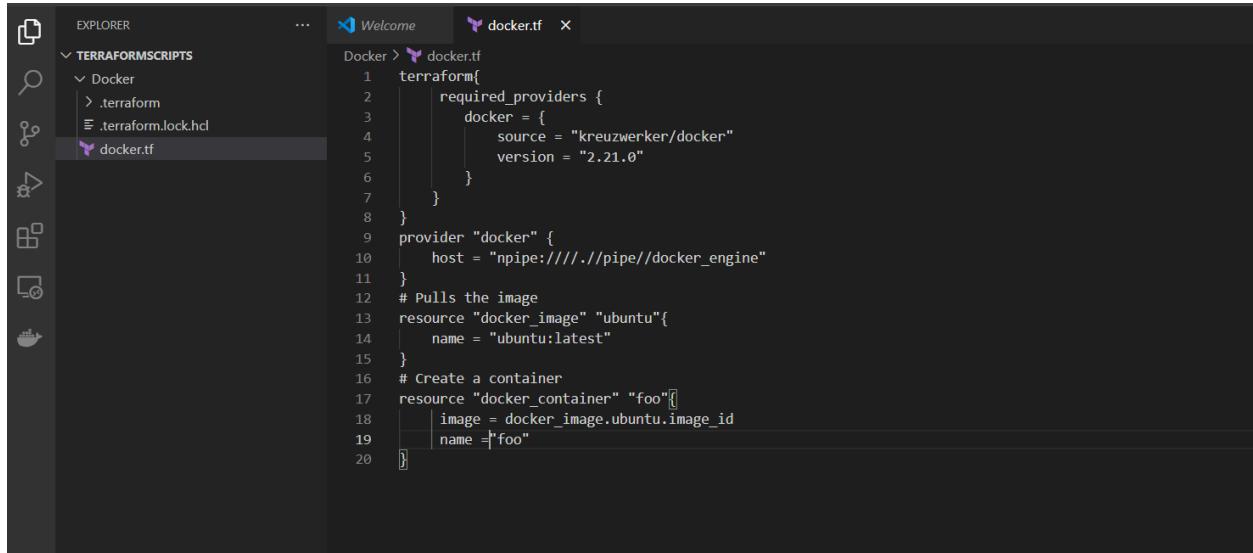
```
PS C:\Users\navan> docker --version
Docker version 27.0.3, build 7d4bcd8
PS C:\Users\navan>
```

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 = "2.21.0"
        }
    }
    provider "docker" {
        host = "npipe:///./pipe//docker_engine"
    }
    # Pulls the image
    resource "docker_image" "ubuntu"{
        name = "ubuntu:latest"
    }
    # Create a container
    resource "docker_container" "foo"{
        image = docker_image.ubuntu.image_id
        name ="foo"
    }
}
```



Step 3: Execute terraform init command to initialize the resources

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

Terraform has been successfully initialized!

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

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

C:\Users\navan\Desktop\TerraformScripts\Docker>
```

Step 4: Execute Terraform plan to see the available resources

```
C:\Users\navan\Desktop\TerraformScripts\Docker>terraform plan
Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the
following symbols:
+ create

Terraform will perform the following actions:

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

```

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

+ healthcheck (known after apply)

+ labels (known after apply)
}

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

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

Note: You didn't use the -out option to save this plan, so Terraform can't guarantee to take exactly these actions if you run "terraform apply" now.

C:\Users\navan\Desktop\TerraformScripts\Docker>

```

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

```

}
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 10s [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]
docker_container.foo: Creating...

```

Docker images,before Executing Apply step:

```

C:\Users\navan\Desktop\TerraformScripts\Docker>docker images
REPOSITORY      TAG          IMAGE ID      CREATED        SIZE
ubuntu          latest        edbfe74c41f8  2 weeks ago   78.1MB
node            20-alpine    e2997a3fdff8  4 weeks ago   133MB

```

```
docker_image.ubuntu: Refreshing state... [id=sha256:edbfe74c41f8a3501ce542e137cf28e  
3e6df8c9d66519b6ad761c2598aubuntu:latest]
```

Note: Objects have changed outside of Terraform

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

```
# docker_image.ubuntu has been deleted
- resource "docker_image" "ubuntu" {
    id          = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6  
2598aubuntu:latest"
    - image_id   = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6  
2598a" -> null
    name        = "ubuntu:latest"
    # (2 unchanged attributes hidden)
}
```

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

Step 6: Execute Terraform destroy to delete the configuration, which will automatically delete the ubuntu container.

```
C:\Users\navan\Desktop\TerraformScripts\Docker>terraform destroy
docker_image.ubuntu: Refreshing state... [id=sha256:edbfe74c41f8a3501ce542e137cf28e  
3e6df8c9d66519b6ad761c2598aubuntu: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" -> n  
    - 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:
```

```
C:\Windows\System32\cmd.e > 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

```
C:\Users\navan\Desktop\TerraformScripts\Docker>docker images
REPOSITORY      TAG          IMAGE ID      CREATED        SIZE
node            20-alpine    e2997a3fdff8  5 weeks ago   133MB
```

Atharva Prabhu
D15A 43

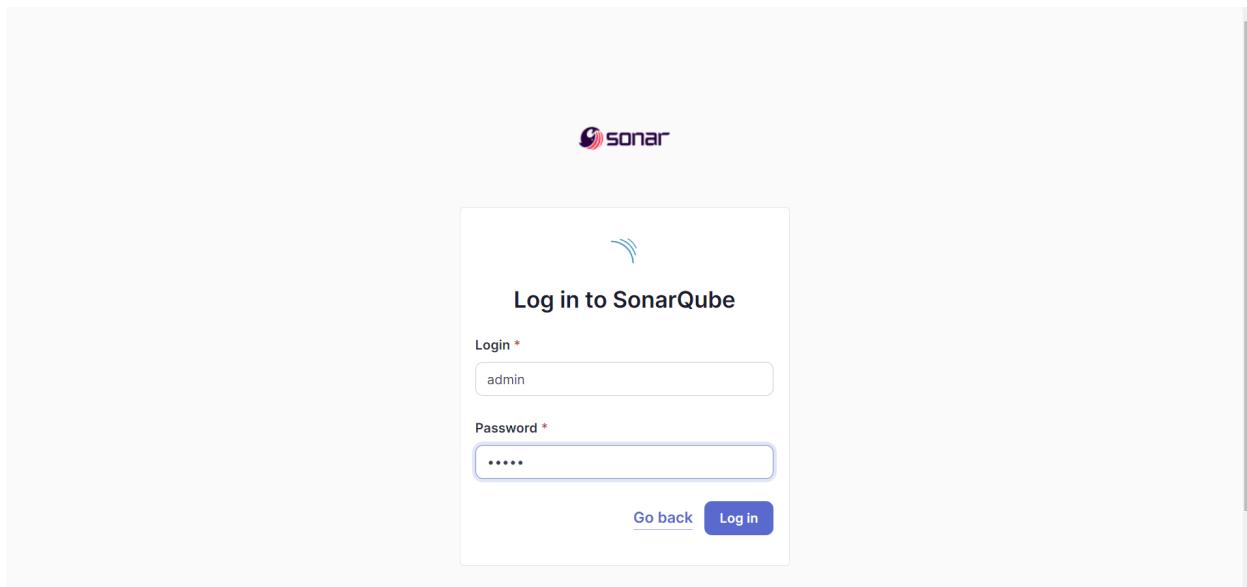
EXPERIMENT 7

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

Step 1: Open Windows PowerShell and run the following command – docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
sonarqube:latest WARNING: Run the following command only once

```
C:\Users\Atharva\OneDrive\Desktop\docker>docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
7478e0acd0f23: Pull complete
90a925ab929a: Pull complete
7d9a34308537: Pull complete
80338217a4ab: Pull complete
1a5fd5c7e184: Pull complete
7b87d6fa783d: Pull complete
bd819c9b5ead: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Downloaded newer image for sonarqube:latest
bc8a095e5c3155db49536b93661f49be9a4d3eff42237d7f162d1d67a01cd78f
```

Step 2: Visit <http://localhost:9000/> to open SonarQube. Login with username: admin and password: admin.



Step 3: Click on create a local project and name the project as sonarqube-test and key as sonarqube-test and click on the next button. In the next step select the “Use the global setting” option and click on create project.

sonarqube

Projects Issues Rules Quality Profiles Quality Gates Administration More Q

1 of 2

Create a local project

Project display name *

Project key *

Main branch name *

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

[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 most recent changes to your project, enabling you to follow the Clean as You Code methodology. Learn more: [Defining New Code](#)

Choose the baseline for new code for this project

Use the global setting

Previous version

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

Define a specific setting for this project

Previous version

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

Step 4: Open Jenkins using <http://localhost:8080/> and select Manage Jenkins, then select the Plugins and select available plugins from sidebar and search for SonarQube Scanner and install it. Once installed you can view the installed plugin in installed plugins section in sidebar.

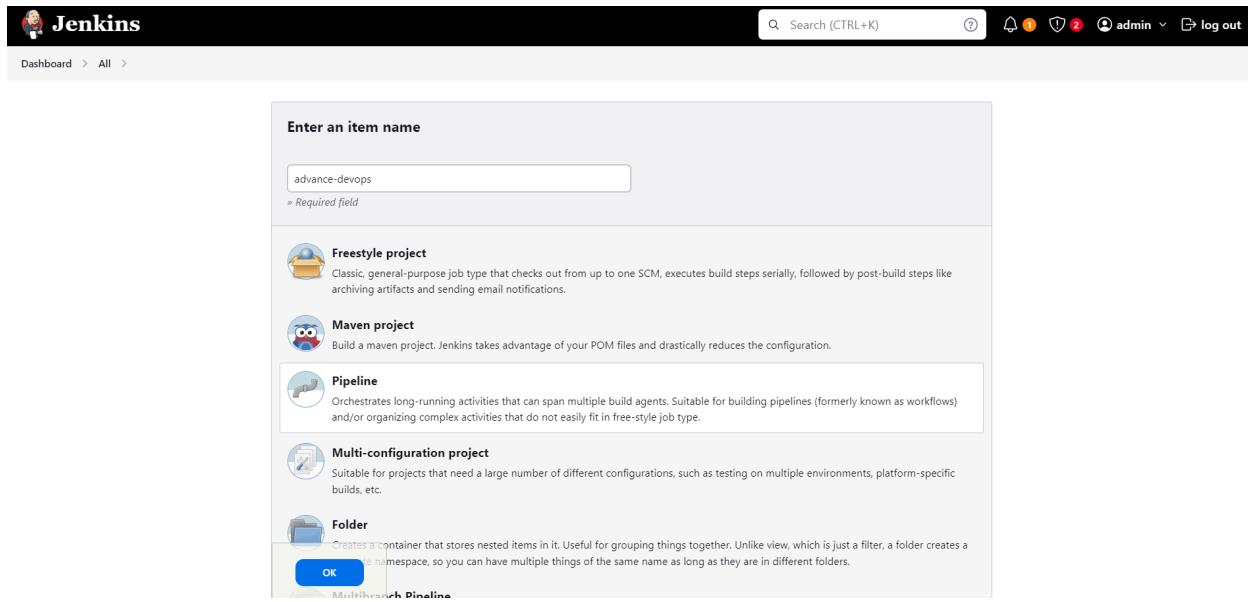
The screenshot shows the Jenkins Plugins page. In the top navigation bar, there are links for Dashboard, Manage Jenkins, and Plugins. The Plugins section is selected. A search bar at the top right contains the text "Sonar". Below the search bar, there are tabs for Updates, Available plugins, Installed plugins (which is selected), and Advanced settings. A table lists the "SonarQube Scanner for Jenkins" plugin, version 2.17.2. The table columns are Name, Version, Description, Enabled, and Actions. The plugin is described as allowing an easy integration of SonarQube for continuous inspection of code quality. It has a status of "Enabled" and a "Report an issue with this plugin" link. At the bottom of the page, there are links for REST API and Jenkins 2.452.3.

Step 5: Select Manage Jenkins, then select the System and then scroll down to SonarQube Server. Name the server as sonarqube and set the server url as http://localhost:9000/ then click on save.

Step 6: Go to Jenkins Dashboard and select Manage Jenkins, then select the Tools and then scroll down to SonarQube Scanner installations. Name the sonarqube scanner as sonarqubescanner and select install automatically then click on save.

The screenshot shows the Jenkins Manage Jenkins > System configuration page. Under the "SonarQube servers" section, there is a note that if checked, job administrators will be able to inject a SonarQube server configuration as environment variables in the build. A checkbox labeled "Environment variables" is checked. Below this, there is a "SonarQube installations" section with a "List of SonarQube installations" table. The table has one row with the following fields: Name (sonarqube), Server URL (http://localhost:9000), and Server authentication token (sonarexp). There is also an "Advanced" dropdown and buttons for "Save" and "Apply".

Step 7: Go to Jenkins dashboard and click on New Item and select Freestyle project and name it as SonarQube and then click on ok.



Step 8: For configuration, Select git and paste the following git repository in the repository url.
https://github.com/shazforiot/MSBuild_firstproject This is a simple Hello world project Step 9: Under the Build steps select “Execute SonarQube Scanner” option and under Analysis Properties write the following - sonar.projectKey, sonar.login, sonar.password, sonar.hosturl. Then click on the save button.

JDK ?
JDK to be used for this SonarQube analysis
(Inherit From Job)

Path to project properties ?
[empty input field]

Analysis properties ?
sonar.projectKey=advdevops7
sonar.projectName=advdevops7
sonar.sources=srcDir1,srcDir2
sonar.tests=src/test/java
sonar.sources=src/main/java
sonar.language=java
sonar.projectVersion=1.0

Additional arguments ?
[empty input field]

JVM Options ?
[empty input field]

Save Apply

Step 10: Visit <http://localhost:9000/admin/permissions> and select the Users tab and for Administrator select the checkbox Execute Analysis.

The screenshot shows the 'Users' tab in the Project Settings. There are four rows: 'sonar-administrators' (System administrators), 'sonar-users' (Every authenticated user automatically belongs to this group), 'Administrator admin' (highlighted in blue), and 'Anyone DEPRECATED' (Anybody who browses the application belongs to this group). The 'Execute Analysis' column has checkboxes for each row. For 'Administrator admin', the checkbox is checked. For the other three rows, it is unchecked. A note below 'Anyone' says: 'Anybody who browses the application belongs to this group. If authentication is not enforced, assigned permissions also apply to non-authenticated users.' At the bottom, it says '4 of 4 shown'.

Step 11: Now, come back to Jenkins and click on Build Now. The build is success.

The screenshot shows the Jenkins project page for 'sonarqube-2'. The status is 'Status' (green checkmark) and 'Build Now' is available. On the right, there's a 'SonarQube Quality Gate' section showing 'adadvdevops7' with a 'Passed' status and 'server-side processing' with a 'Success' status. Below it are 'Permalinks' and a 'Build History' section showing a single build (#1) from Sep 26, 2024, 11:16 AM, with links for 'Atom feed for all' and 'Atom feed for failures'.

Step 12: Visit the following URL to see the result -
<http://localhost:9000/dashboard?id=sonarqubetest&codeScope=overall>

main

124 Lines of Code · Version 1.0 · Set as homepage

Quality Gate Passed

Last analysis 11 minutes ago

The last analysis has warnings. [See details](#)

New Code Overall Code

Security 0 Open issues 0 H 0 M 0 L	Reliability 0 Open issues 0 H 0 M 0 L	Maintainability 1 Open issues 0 H 1 M 0 L
Accepted issues 0 <small>Valid issues that were not fixed</small>	Coverage 0.0% <small>On 26 lines to cover.</small>	Duplications 0.0% <small>On 167 lines.</small>

ADVANCE DEVOPS EXP 8

Name:Atharva Prabhu

Class:D15A

Roll No:43

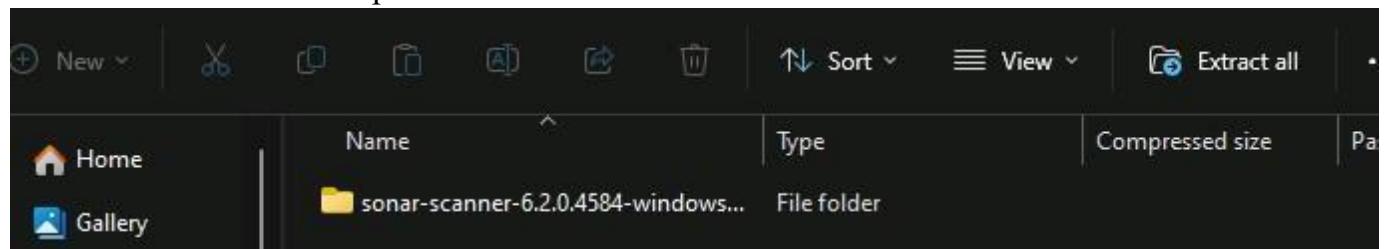
Aim: Create a Jenkins CICD Pipeline with SonarQube / GitLab Integration to perform a static analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web / Java / Python application.

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. 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 "Homepage", "Try out SonarQube", "Server installation and setup", "Analyzing source code" (which is expanded), "Project analysis setup", "Scanners" (which is expanded), and "Scanner environment", "SonarScanner CLI", "SonarQube extension for Azure DevOps", "SonarQube extension for Jenkins", "SonarScanner .NET", and "SonarScanner for Maven". The main content area features a section for "SonarScanner" and "Issue Tracker", with a "Show more" link. Below this is a "6.1" section from "2024-06-27" that includes links for "macOS and Linux AArch64 distributions", "Download scanner for: Linux x64", "Linux AArch64", "Windows x64", "macOS x64", "macOS AArch64", "Docker Any (Requires a pre-installed JVM)", and "Release notes". At the bottom, there is a note about the SonarScanner CLI being the scanner to use when there is no specific scanner for your build system, and another note about ARM architecture support.

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

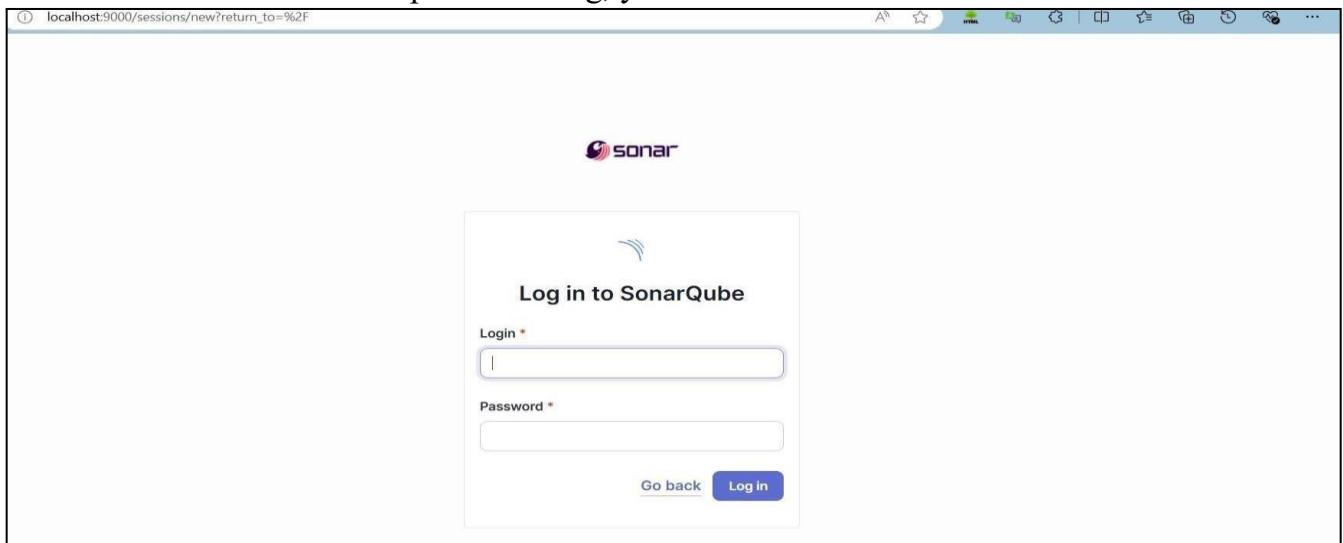
Extract the downloaded zip file in a folder.



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 with the following details:

- Left sidebar:**
 - + New Item
 - Build History
 - Project Relationship
 - Check File Fingerprint
 - Manage Jenkins
 - My Views
- Top right:** Search (CTRL+K), Help, User: Soham Satpute, Log Out
- Main area:** A table listing projects:

S	W	Name	Last Success	Last Failure	Last Duration
✓	☀️	mn	7 days 10 hr #1	N/A	2.6 sec
⌚	☀️	my-app-pipeline	28 days log	N/A	8.8 sec
✓	☀️	my-Maven	28 days #1	N/A	1 min 37 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 with the following details:

- Left sidebar:** Updates (25), Available plugins (selected), Installed plugins, Advanced settings
- Search bar:** sonarq
- Available plugins section:**

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

- Left sidebar:** Updates (25), Available plugins (selected), Installed plugins, Advanced settings, Download progress (selected)
- Right panel:**

Download progress

Preparation:

 - Checking internet connectivity
 - Checking update center connectivity
 - Success

SonarQube Scanner: Success
Loading plugin extensions: Success

→ Go back to the top page
(you can start using the installed plugins right away)
→ 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 Servers** and enter the details.

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.

Name

Server URL

Default is <http://localhost:9000>

Server authentication token

SonarQube authentication token. Mandatory when anonymous access is disabled.

- none -

+ Add ▾

Advanced ▾

Choose the latest configuration and choose Install automatically.

Dashboard > Manage Jenkins > Tools

Dashboard > Manage Jenkins > Tools

Add Git ▾

Gradle installations

Add Gradle

SonarScanner for MSBuild installations

Add SonarScanner for MSBuild

SonarQube Scanner installations

Add SonarQube Scanner

Ant installations

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.

Dashboard > All > New Item

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_Jenkins>') {
        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.

The screenshot shows the Jenkins Pipeline Configuration screen. The pipeline script is defined as a Pipeline script:

```

node {
    stage('Cloning the GitHub Repo') {
        git 'https://github.com/shazforiot/GOL.git'
    }

    stage('SonarQube analysis') {
        withSonarQubeEnv('sonarqube') {
            bat """
                "%C:/Users/Atharva_Prabhu/Downloads/sonar-scanner-cl1-6.2.0.4584-windows-x64/sonar-scanner-6.2.0.4584-windows-x64/bin/sonar-scanner" \
                -Dsonar.projectKey=Pipeline \
                -Dsonar.sources=. \
                -Dsonar.exclusions=**/*.java \
                -Dsonar.host.url=http://localhost:9000 \
                -Dsonar.login=admin \
                -Dsonar.password=admin10
            """
        }
    }
}

```

The "Pipeline Syntax" section indicates that "Use Groovy Sandbox" is checked. At the bottom, there are "Save" and "Apply" buttons.

The screenshot shows the Jenkins Pipeline Stage View for the 'sonarpipe' pipeline. The pipeline consists of several stages:

- Cloning the GitHub Repo**: Duration 3s
- SonarQube analysis**: Duration 52s
- Stage #23**: Duration 3s, Status: Success
- Stage #22**: Duration 4s, Status: Failed (failed)
- Stage #21**: Duration 3s, Status: Failed (failed)
- Stage #20**: Duration 2s, Status: Failed (failed)

Average stage times: (Average full run time: ~6min 30s)

Build History (trend):

- #23 Oct 03, 09:11 AM
- (X) #22 Oct 03, 09:09 AM

11.Check console

The screenshot shows the Jenkins Pipeline Console Output for build #23. The output window displays the following log entries:

```

Skipping 4,247 KB.. Full Log
09:17:22.526 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/testelement/AbstractScopedAssertion.html for block at line 17. Keep only the first 100 references.
09:17:22.526 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/testelement/AbstractScopedAssertion.html for block at line 529. Keep only the first 100 references.
09:17:22.526 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/testelement/AbstractScopedAssertion.html for block at line 75. Keep only the first 100 references.
09:17:22.526 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/parser/HTMLParseError.html for block at line 232. Keep only the first 100 references.
09:17:22.526 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/parser/HTMLParseError.html for block at line 353. Keep only the first 100 references.
09:17:22.526 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/parser/HTMLParseError.html for block at line 17. Keep only the first 100 references.
09:17:22.526 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/parser/HTMLParseError.html for block at line 232. Keep only the first 100 references.
09:17:22.526 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/parser/HTMLParseError.html for block at line 355. Keep only the first 100 references.
09:17:22.526 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/parser/HTMLParseError.html for block at line 32. Keep only the first 100 references.

```

12.Now, check the project in SonarQube:

Sonarqube-test / main ?

Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information

Quality Gate **Passed** Last analysis 26 minutes ago

The last analysis has warnings. See details

New Code Overall Code

New Code: Since September 26, 2024 Started 4 days ago

New issues Accepted issues

0 0

Required = 0 Valid issues that were not fixed

Coverage Duplications Security Hotspots

0 A

This screenshot shows the Sonarqube Quality Gate dashboard for the 'main' branch. It displays a green 'Passed' status with a checkmark icon. A warning message indicates there are warnings in the latest analysis, with a 'See details' link. The dashboard is divided into 'New Code' and 'Overall Code' sections. Under 'New Code', it shows 'New Code: Since September 26, 2024 Started 4 days ago'. Metrics include 'New issues' (0), 'Accepted issues' (0), 'Coverage' (0), 'Duplications' (0), and 'Security Hotspots' (0). A note says 'Required = 0' for New issues and 'Valid issues that were not fixed' for Accepted issues. The overall status is 'Passed'.

13. code problems consistency:

My Issues All

Bulk Change Select issues ▾ Navigate to issue ▾ 210,549 issues 3135d effort

Filters gameoflife-acceptance-tests/Dockerfile

Issues in new code

Clean Code Attribute

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

Software Quality

Use a specific version tag for the image. Intentionality Maintainability Open Not assigned L1 - 5min effort - 4 years ago - Code Smell - Major

Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. Intentionality Maintainability Open Not assigned L12 - 5min effort - 4 years ago - Code Smell - Major

Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. Intentionality Maintainability Open Not assigned No tags +

This screenshot shows the Sonarqube Issues page for the 'gameoflife-acceptance-tests/Dockerfile' file. It lists issues categorized by 'Clean Code Attribute' (Consistency, Intentionality, Adaptability, Responsibility) and 'Software Quality'. The 'Intentionality' attribute has three specific issues listed: 1. 'Use a specific version tag for the image.' (L1 - 5min effort - 4 years ago - Code Smell - Major), 2. 'Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.' (L12 - 5min effort - 4 years ago - Code Smell - Major), and 3. Another instance of 'Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.' (No tags +). The interface includes filters, bulk change options, and navigation controls.

14. Intentionality:

The screenshot shows a software interface for managing code issues. On the left, there's a sidebar with 'My Issues' and 'All' buttons, and a 'Filters' section. Under 'Clean Code Attribute', 'Intentionality' is selected, showing 14k issues. Below it are 'Consistency' (197k), 'Adaptability' (0), and 'Responsibility' (0). A note says 'Issues in new code'. At the bottom of the sidebar, there's a link 'Add to selection Ctrl + click'. The main area displays code smells for 'gameoflife-acceptance-tests/Dockerfile'. There are three items listed:

- Use a specific version tag for the image. Intentionality
Maintainability
Open Not assigned L1 • 5min effort • 4 years ago • ⚡ Code Smell • ⚡ Major
- Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. Intentionality
Maintainability
Open Not assigned L12 • 5min effort • 4 years ago • ⚡ Code Smell • ⚡ Major
- Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. Intentionality
Maintainability
Open Not assigned No tags + L12 • 5min effort • 4 years ago • ⚡ Code Smell • ⚡ Major

15.Bugs

The screenshot shows a software interface for managing bugs. On the left, there's a sidebar with 'Software Quality' (Security: 0, Reliability: 14k, Maintainability: 0), 'Severity' (with a question mark), and 'Type'. 'Bug' is selected, showing 14k issues. Below it are 'Vulnerability' (0) and 'Code Smell' (268). A note says 'Add to selection Ctrl + click'. The main area displays bugs for 'gameoflife-core/build/reports/tests/all-tests.html'. There are two items listed:

- Add "lang" and/or "xml:lang" attributes to this "<html>" element. Intentionality
Reliability
Open Not assigned L1 • 2min effort • 4 years ago • ⚡ Bug • ⚡ Major
- Add "<th>" headers to this "<table>". Intentionality
Reliability
Open Not assigned L9 • 2min effort • 4 years ago • ⚡ Bug • ⚡ Major

Below this, it says 'gameoflife-core/build/reports/tests/allclasses-frame.html'.

⚠️ Embedded database should be used for evaluation purposes only

Code smells:

Sonarqube-test / main

Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information

Type: 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 (selected) accessibility wcag2-a

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 accessibility wcag2-a

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 LGPL v3 Community Documentation Plugins Web API

Duplications:

Sonarqube-test / main

Overview Issues Security Hotspots Measures 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%

The chart displays a scatter plot where the x-axis represents 'Duplicated Lines' (ranging from 0 to 2,000+) and the y-axis represents 'Duplicated Blocks' (ranging from 0 to 2,000+). The data points are represented by blue bubbles of varying sizes, indicating the volume of duplicated code. A large cluster of bubbles is centered around 1,400-1,500 duplicated lines and 1,400-1,500 duplicated blocks. Another significant bubble is located at approximately 1,300 duplicated lines and 2,000 duplicated blocks.

localhost:9000/component_measures?metric=Duplications&id=Sonarqube-test#

Cyclomatic Complexities:

The screenshot shows the SonarQube interface for the project 'Sonarqube-test'. The main navigation bar includes 'Overview', 'Issues', 'Security Hotspots', 'Measures' (which is selected), 'Code', and 'Activity'. On the right, there are 'Project Settings' and 'Project Information' dropdowns. The left sidebar displays various code metrics: Duplicated Blocks (0), Overall Code, Density (50.6%), Duplicated Lines (384,007), Duplicated Blocks (42,799), and Duplicated Files (979). Below these are sections for 'Size', 'Complexity' (selected), and 'Issues'. The 'Complexity' section shows a total of 1,112 cyclomatic complexities. The right panel shows a tree view of the project structure under 'Sonarqube-test', with 'gameoflife-acceptance-tests', 'gameoflife-build', 'gameoflife-core' (18 files), 'gameoflife-deploy', and 'gameoflife-web' (1,094 files). A message at the top right indicates 'New Code: Since September 26, 2024'.

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

Experiment 9

Atharva Prabhu

D15A 43

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

Step 1: Create an EC2 Instance and name it as nagios-host

The screenshot shows the AWS EC2 'Launch an instance' wizard. In the 'Name and tags' step, the instance name is set to 'nagios-host'. In the 'Application and OS Images (Amazon Machine Image)' step, the 'Amazon Linux 2023 AMI' is selected. On the right, a summary panel shows 1 instance being launched, using the Amazon Linux 2023 AMI, t2.micro instance type, and a new security group. A tooltip for the 'Free tier' indicates it covers 750 hours of t2.micro usage per month. At the bottom, there are 'Cancel', 'Launch instance', and 'Review commands' buttons.

Step 2: Under the security groups, click on edit inbound rules and set as shown in the figure below

Inbound rules (6)										
<input type="button" value="Search"/> Manage tags <input type="button" value="Edit inbound rules"/>										
	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description		
<input type="checkbox"/>	-	sgr-08fd8adc13683e0a	IPv4	HTTPS	TCP	443	0.0.0.0/0	-		
<input type="checkbox"/>	-	sgr-058fcfed777849588b	IPv4	HTTP	TCP	80	0.0.0.0/0	-		
<input type="checkbox"/>	-	sgr-0dc6f270d7dc50b7	IPv4	All traffic	All	All	0.0.0.0/0	-		
<input type="checkbox"/>	-	sgr-0af2fa8d1584e888c	IPv4	SSH	TCP	22	0.0.0.0/0	-		
<input type="checkbox"/>	-	sgr-04bc8aca5d0aa8c78	IPv4	All ICMP - IPv6	IPv6 ICMP	All	0.0.0.0/0	-		
<input type="checkbox"/>	-	sgr-02c0cdd35c5a31f9f	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	-		

Step 3: Then select the instance nagios-host and then connect the instance.

Services Search [Alt+S] N. Virginia v vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾

EC2 > Instances > i-025f1d18f7c8a8cda > Connect to instance

Connect to instance Info

Connect to your instance i-025f1d18f7c8a8cda (nagios-host) using any of these options

EC2 Instance Connect Session Manager SSH client EC2 serial console

⚠ All ports are open to all IPv4 addresses in your security group
All ports are currently open to all IPv4 addresses, indicated by All and 0.0.0.0/0 in the inbound rule in your **security group**. For increased security, consider restricting access to only the EC2 Instance Connect service IP addresses for your Region: 18.206.107.24/29. [Learn more](#).

Instance ID

Connection Type Connect using EC2 Instance Connect Connect using the EC2 Instance Connect browser-based client, with a public IPv4 or IPv6 address. Connect using EC2 Instance Connect Endpoint Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IPv4 address IPv6 address

Username Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.

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

Step 3: Now, run the following commands -

sudo su

sudo yum update

sudo yum install httpd php

sudo yum install gcc glibc glibc-common

sudo yum install gd gd-devel

```
[ec2-user@ip-172-31-13-171 ~]$ sudo yum update -y
sudo yum install -y httpd php
sudo yum install -y gcc glibc glibc-common
sudo yum install -y gd gd-devel
Last metadata expiration check: 0:04:14 ago on Thu Oct  3 12:58:05 2024.
```

WARNING:
A newer release of "Amazon Linux" is available.

Available Versions:

Version 2023.5.20241001:
Run the following command to upgrade to 2023.5.20241001:

dnf upgrade --releasever=2023.5.20241001

Please notes:
<https://docs.aws.amazon.com/linux/al2023/release-notes/relnotes-2023.5.20241001.html>

Dependencies resolved.
Nothing to do.
Complete!
Last metadata expiration check: 0:04:14 ago on Thu Oct 3 12:58:05 2024.
Dependencies resolved.

Package	Architecture	Version	Repository	Size
Installing:				
httpd	x86_64	2.4.62-1.amzn2023	amazonlinux	48 k
php8.3	x86_64	8.3.10-1.amzn2023.0.1	amazonlinux	10 k
Installing dependencies:				
apr	x86_64	1.7.2-2.amzn2023.0.2	amazonlinux	129 k
apr-util	x86_64	1.6.3-1.amzn2023.0.1	amazonlinux	98 k
generic-logos-httdp	noarch	18.0.0-12.amzn2023.0.3	amazonlinux	19 k
httpd	x86_64	2.4.62-1.amzn2023	amazonlinux	14 k
httpd-filesystem	noarch	2.4.62-1.amzn2023	amazonlinux	14 k
httpd-tools	x86_64	2.4.62-1.amzn2023	amazonlinux	81 k
libiconv	x86_64	1.0.9-4.amzn2023.0.2	amazonlinux	315 k

Step 4: Create a new nagios user with its password.

```
sudo adduser -m nagios
sudo passwd nagios
sudo groupadd nagcmd
sudo usermod -a -G nagcmd nagios
sudo usermod -a -G nagcmd apache
```

```
[ec2-user@ip-172-31-13-171 ~]$ sudo groupadd nagcmd
[ec2-user@ip-172-31-13-171 ~]$ sudo usermod -aG nagcmd nagios
[ec2-user@ip-172-31-13-171 ~]$ sudo usermod -aG nagcmd apache
[ec2-user@ip-172-31-13-171 ~]$ mkdir ~/downloads
cd ~/downloads
[ec2-user@ip-172-31-13-171 downloads]$ wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz
--2024-10-03 13:05:44-- 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:feff:45ce
Connecting to assets.nagios.com (assets.nagios.com)|45.79.49.120|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11333414 (11M) [application/x-gzip]
Saving to: "nagios-4.4.6.tar.gz"

nagios-4.4.6.tar.gz          100%[=====]  10.81M  2.44MB/s   in 5.1s
2024-10-03 13:05:50 (2.14 MB/s) - 'nagios-4.4.6.tar.gz' saved [11333414/11333414]

--2024-10-03 13:05:50-- https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz
Resolving nagios-plugins.org (nagios-plugins.org)... 45.56.123.251
Connecting to nagios-plugins.org (nagios-plugins.org)|45.56.123.251|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2782610 (2.7M) [application/x-gzip]
Saving to: "nagios-plugins-2.3.3.tar.gz"

nagios-plugins-2.3.3.tar.gz      100%[=====]  2.65M  832KB/s   in 3.3s
2024-10-03 13:05:54 (832 KB/s) - 'nagios-plugins-2.3.3.tar.gz' saved [2782610/2782610]
```

Step 5: Now, run the following commands -

```
mkdir ~/downloads  
cd ~/downloads  
wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz  
wget http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz  
tar zxvf nagios-4.0.8.tar.gz
```

```
[root@ip-172-31-93-157 ec2-user]# mkdir ~/downloads  
[root@ip-172-31-93-157 ec2-user]# cd ~/downloads  
[root@ip-172-31-93-157 downloads]# wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz  
wget: missing URL  
Usage: wget [OPTION]... [URL]...  
Try 'wget --help' for more options.  
bash: http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.: No such file or directory  
bash: gz: command not found  
[root@ip-172-31-93-157 downloads]# wget http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz  
--2024-09-30 17:00:06-- http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz  
Resolving nagios-plugins.org (nagios-plugins.org)... 45.56.123.251  
Connecting to nagios-plugins.org (nagios-plugins.org)|45.56.123.251|:80... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 2659772 (2.5M) [application/x-gzip]  
Saving to: "nagios-plugins-2.0.3.tar.gz"  
  
nagios-plugins-2.0.3.tar.gz      100%[=====]   2.54M  6.16MB/s    in 0.4s  
2024-09-30 17:00:07 (6.16 MB/s) - 'nagios-plugins-2.0.3.tar.gz' saved [2659772/2659772]  
  
[root@ip-172-31-93-157 downloads]# tar zxvf nagios-4.0.8.tar.gz  
tar (child): nagios-4.0.8.tar.gz: Cannot open: No such file or directory  
tar (child): Error is not recoverable: exiting now  
tar: Child returned status 2  
tar: Error is not recoverable: exiting now  
[root@ip-172-31-93-157 downloads]#
```

i-025f1d18f7c8a8cda (nagios-host)
Public IPs: 3.86.198.73 Private IPs: 172.31.93.157

To resolve the error run the following commands -

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

```
aws Services Search [Alt+S] N. Virginia vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
root@ip-172-31-93-157 ~# wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz
--2024-09-30 17:03:04-- http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz
Resolving prdownloads.sourceforge.net (prdownloads.sourceforge.net) ... 204.68.111.105
Connecting to prdownloads.sourceforge.net (prdownloads.sourceforge.net)|204.68.111.105|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz [following]
--2024-09-30 17:03:04-- http://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz
Resolving downloads.sourceforge.net (downloads.sourceforge.net) ... 204.68.111.105
Reusing existing connection to prdownloads.sourceforge.net:80.
HTTP request sent, awaiting response... 302 Found
Location: http://versaweb.dl.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz?viafsf=1 [following]
--2024-09-30 17:03:04-- http://versaweb.dl.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz?viafsf=1
Resolving versaweb.dl.sourceforge.net (versaweb.dl.sourceforge.net) ... 162.251.232.173
Connecting to versaweb.dl.sourceforge.net (versaweb.dl.sourceforge.net)|162.251.232.173|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1805059 (1.7M) [application/x-xzzip]
Saving to: 'nagios-4.0.8.tar.gz'

nagios-4.0.8.tar.gz          100%[=====]   1.72M  2.21MB/s  in 0.8s

2024-09-30 17:03:05 (2.21 MB/s) - 'nagios-4.0.8.tar.gz' saved [1805059/1805059]

--2024-09-30 17:03:05-- http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz
Resolving nagios-plugins.org (nagios-plugins.org) ... 45.56.123.251
Connecting to nagios-plugins.org (nagios-plugins.org)|45.56.123.251|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2659772 (2.5M) [application/x-xzzip]
Saving to: 'nagios-plugins-2.0.3.tar.gz.l1'

nagios-plugins-2.0.3.tar.gz.l1    100%[=====]   2.54M  7.26MB/s  in 0.3s

2024-09-30 17:03:05 (7.26 MB/s) - 'nagios-plugins-2.0.3.tar.gz.l1' saved [2659772/2659772]
```

i-025f1d18f7c8a8cda (nagios-host)

PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

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

```
aws Services Search [Alt+S] N. Virginia vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
nagios-plugins-2.0.3/plugins-scripts/check_ifoperstatus.pl
nagios-plugins-2.0.3/plugins-scripts/Makefile.am
nagios-plugins-2.0.3/plugins-scripts/subst.in
nagios-plugins-2.0.3/plugins-scripts/check_breeze.pl
nagios-plugins-2.0.3/plugins-scripts/check_log.sh
nagios-plugins-2.0.3/plugins-scripts/check_flexlm.pl
nagios-plugins-2.0.3/plugins-scripts/check_rpc.pl
nagios-plugins-2.0.3/plugins-scripts/check_oracle.sh
nagios-plugins-2.0.3/plugins-scripts/utils.pm.in
nagios-plugins-2.0.3/plugins-scripts/check_disk_smb.pl
nagios-plugins-2.0.3/plugins-scripts/t/
nagios-plugins-2.0.3/plugins-scripts/t/check_ifoperstatus.t
nagios-plugins-2.0.3/plugins-scripts/t/check_rpc.t
nagios-plugins-2.0.3/plugins-scripts/t/check_file_age.t
nagios-plugins-2.0.3/plugins-scripts/t/check_disk_smb.t
nagios-plugins-2.0.3/plugins-scripts/t/check_ifstatus.t
nagios-plugins-2.0.3/plugins-scripts/t/utils.t
nagios-plugins-2.0.3/plugins-scripts/check_mailq.pl
nagios-plugins-2.0.3/plugins-scripts/check_wave.pl
nagios-plugins-2.0.3/plugins-scripts/check_ircd.pl
nagios-plugins-2.0.3/plugins-scripts/utils.sh.in
nagios-plugins-2.0.3/plugins-scripts/check_ifstatus.pl
nagios-plugins-2.0.3/plugins-scripts/check_sensors.sh
nagios-plugins-2.0.3/pkg/
nagios-plugins-2.0.3/pkg/fedora/
nagios-plugins-2.0.3/pkg/fedora/requirements
nagios-plugins-2.0.3/pkg/solaris/
nagios-plugins-2.0.3/pkg/solaris/preinstall
nagios-plugins-2.0.3/pkg/solaris/solpkgs
nagios-plugins-2.0.3/pkg/solaris/pkinfo.in
nagios-plugins-2.0.3/pkg/solaris/pkinfo
nagios-plugins-2.0.3/pkg/redhat/
nagios-plugins-2.0.3/pkg/redhat/requirements
[root@ip-172-31-93-157 ~]#
```

i-025f1d18f7c8a8cda (nagios-host)

PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

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

```
aws Services Search [Alt+S] N. Virginia vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
nagios-plugins-2.0.3/plugins-scripts/Makefile.am
nagios-plugins-2.0.3/plugins-scripts/subst.in
nagios-plugins-2.0.3/plugins-scripts/check_breeze.pl
nagios-plugins-2.0.3/plugins-scripts/check_log.sh
nagios-plugins-2.0.3/plugins-scripts/check_flexlm.pl
nagios-plugins-2.0.3/plugins-scripts/check_rpc.pl
nagios-plugins-2.0.3/plugins-scripts/check_oracle.sh
nagios-plugins-2.0.3/plugins-scripts/utils.pm.in
nagios-plugins-2.0.3/plugins-scripts/check_disk_smb.pl
nagios-plugins-2.0.3/plugins-scripts/t/
nagios-plugins-2.0.3/plugins-scripts/t/check_ifoperstatus.t
nagios-plugins-2.0.3/plugins-scripts/t/check_rpc.t
nagios-plugins-2.0.3/plugins-scripts/t/check_file_age.t
nagios-plugins-2.0.3/plugins-scripts/t/check_disk_smb.t
nagios-plugins-2.0.3/plugins-scripts/t/check_ifstatus.t
nagios-plugins-2.0.3/plugins-scripts/t/utils.t
nagios-plugins-2.0.3/plugins-scripts/check_mailq.pl
nagios-plugins-2.0.3/plugins-scripts/check_wave.pl
nagios-plugins-2.0.3/plugins-scripts/check_ircd.pl
nagios-plugins-2.0.3/plugins-scripts/utils.sh.in
nagios-plugins-2.0.3/plugins-scripts/check_ifstatus.pl
nagios-plugins-2.0.3/plugins-scripts/check_sensors.sh
nagios-plugins-2.0.3/pkg/
nagios-plugins-2.0.3/pkg/fedora/
nagios-plugins-2.0.3/pkg/fedora/requirements
nagios-plugins-2.0.3/pkg/solaris/
nagios-plugins-2.0.3/pkg/solaris/preinstall
nagios-plugins-2.0.3/pkg/solaris/solpkgs
nagios-plugins-2.0.3/pkg/solaris/pkinfo.in
nagios-plugins-2.0.3/pkg/solaris/pkinfo
nagios-plugins-2.0.3/pkg/redhat/
nagios-plugins-2.0.3/pkg/redhat/requirements
[root@ip-172-31-93-157 ~]# cd nagios-4.0.8
[root@ip-172-31-93-157 nagios-4.0.8]#
```

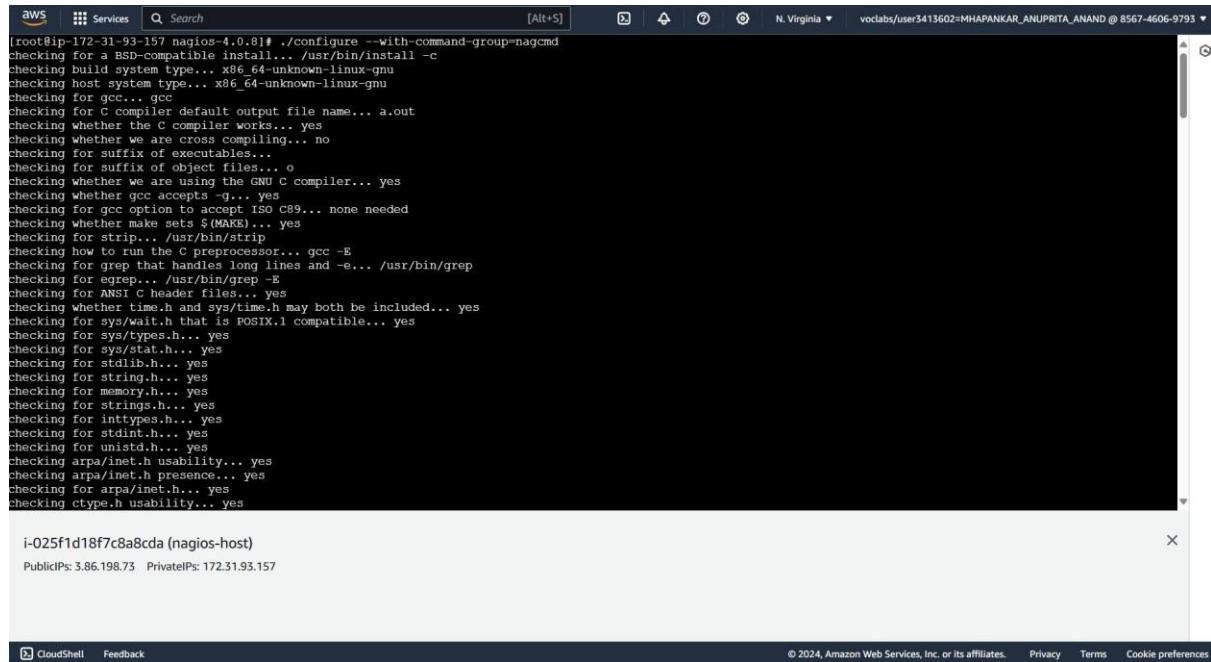
i-025f1d18f7c8a8cda (nagios-host)

PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

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

Step 6: Now to run the configuration script run the following command.

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

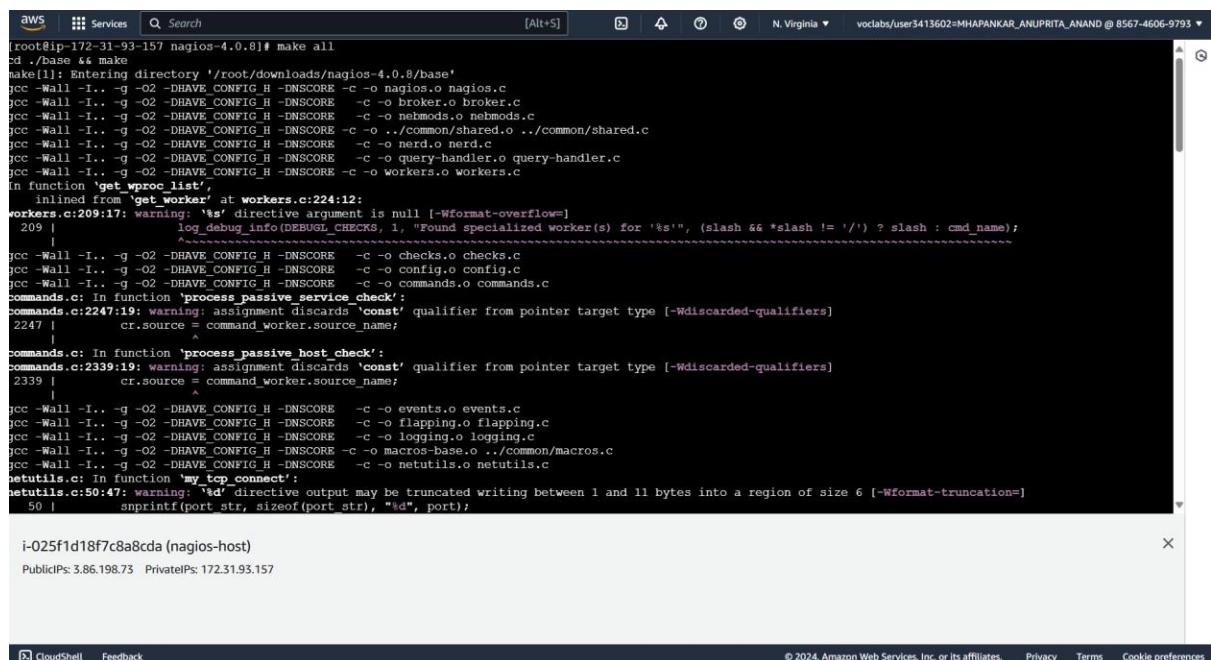


```
[root@ip-172-31-93-157 nagios-4.0.8]# ./configure --with-command-group=nagcmd
checking for a BSD-compatible install... /usr/bin/install -c
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -q... yes
checking for gcc option to accept ISO C89... none needed
checking whether make sets ${MAKE}... yes
checking for strip... /usr/bin/stripl
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 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... yes
checking ctype.h usability... yes
```

i-025f1d18f7c8a8cda (nagios-host)
PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

Step 7: Now, to compile the source code run the following command -

```
make all
```



```
[root@ip-172-31-93-157 nagios-4.0.8]# make all
cd ./base && make
make[1]: Entering directory '/root/downloads/nagios-4.0.8/base'
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nagios.o nagios.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o broker.o broker.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nebmods.o nebmods.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o ./common/shared.o ./common/shared.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nerd.o nerd.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o query-handler.o query-handler.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o workers.o workers.c
In function 'get_wproc_list':
  inlined from 'get_worker' at workers.c:224:12:
workers.c:209:17: warning: `*s' directive argument is null [-Wformat-overflow=]
  209 |     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
commands.c: In function 'process_passive_service_check':
commands.c:2247:19: warning: assignment discards 'const' qualifier from pointer target type [-Wdiscarded-qualifiers]
  2247 |     cr.source = command_worker.source_name;
  |     ^
commands.c: In function 'process_passive_host_check':
commands.c:2339:19: warning: assignment discards 'const' qualifier from pointer target type [-Wdiscarded-qualifiers]
  2339 |     cr.source = command_worker.source_name;
  |     ^
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o events.o events.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o flapping.o flapping.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o logging.o logging.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o macros-base.o ./common/macros.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o netutils.o netutils.c
netutils.c: In function 'my_tcp_connect':
netutils.c:50:47: warning: `*sd' directive output may be truncated writing between 1 and 11 bytes into a region of size 6 [-Wformat-truncation=]
  50 |     snprintf(port_str, sizeof(port_str), "%d", port);
```

i-025f1d18f7c8a8cda (nagios-host)
PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

```
aws Services Search [Alt+S] N. Virginia v vclabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
[roo...@ip-172-31-93-157 nagios-4.0.8]# sudo make install
cd ./base && make install
make[1]: Entering directory '/root/downloads/nagios-4.0.8/base'
make install-basic
make[2]: Entering directory '/root/downloads/nagios-4.0.8/base'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/bin
/usr/bin/install -c -m 774 -o nagios -g nagios nagios /usr/local/nagios/bin
/usr/bin/install -c -m 774 -o nagios -g nagios nagiosstats /usr/local/nagios/bin
make[2]: Leaving directory '/root/downloads/nagios-4.0.8/base'
make strip-post-install
make[2]: Entering directory '/root/downloads/nagios-4.0.8/base'
/usr/bin/strip /usr/local/nagios/bin/nagios
/usr/bin/strip /usr/local/nagios/bin/nagiosstats
make[2]: Leaving directory '/root/downloads/nagios-4.0.8/base'
make[1]: Leaving directory '/root/downloads/nagios-4.0.8/base'
cd ./cgi && make install
make[1]: Entering directory '/root/downloads/nagios-4.0.8/cgi'
make install-basic
make[2]: Entering directory '/root/downloads/nagios-4.0.8/cgi'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/sbin
for file in *.cgi; do \
    /usr/bin/install -c -m 775 -o nagios -g nagios $file /usr/local/nagios/sbin; \
done
/usr/bin/install: cannot stat '*.cgi': No such file or directory
make[2]: *** [Makefile:205: install-basic] Error 1
make[2]: Leaving directory '/root/downloads/nagios-4.0.8/cgi'
make[1]: *** [Makefile:197: install] Error 2
make[1]: Leaving directory '/root/downloads/nagios-4.0.8/cgi'
make: *** [Makefile:235: install] Error 2
[roo...@ip-172-31-93-157 nagios-4.0.8]# sudo make install-init
/usr/bin/install -c -m 755 -d -o root -g root /etc/rc.d/init.d/nagios
/usr/bin/install -c -m 755 -o root -g root daemon-init /etc/rc.d/init.d/nagios
*** Init script installed ***
```

i-025f1d18f7c8a8cda (nagios-host)

Public IPs: 3.86.198.73 Private IPs: 172.31.93.157

```
CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
aws Services Search [Alt+S] N. Virginia v vclabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
[roo...@ip-172-31-93-157 nagios-4.0.8]# sudo make install-init
/usr/bin/install -c -m 755 -d -o root -g root /etc/rc.d/init.d/nagios
/usr/bin/install -c -m 755 -o root -g root daemon-init /etc/rc.d/init.d/nagios
*** Init script installed ***
[roo...@ip-172-31-93-157 nagios-4.0.8]# sudo make install-config
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc
/usr/bin/install -c -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.cgi /usr/local/nagios/etc/cgi.cgi
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/cgi.cgi /usr/local/nagios/etc/resource.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object.cfg /usr/local/nagios/etc/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/timerperiods.cfg /usr/local/nagios/etc/objects/timerperiods.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/localhost.cfg /usr/local/nagios/etc/objects/localhost.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/windows.cfg /usr/local/nagios/etc/objects/windows.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/printer.cfg /usr/local/nagios/etc/objects/printer.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/switc...cfg /usr/local/nagios/etc/objects/switc...cfg
*** Config files installed ***
Remember, these are *SAMPLE* config files. You'll need to read the documentation for more information on how to actually define services, hosts, etc. to fit your particular needs.
[roo...@ip-172-31-93-157 nagios-4.0.8]# sudo make install-commandmode
/usr/bin/install -c -m 775 -o nagios -g nagcmd -d /usr/local/nagios/var/rw
chmod g+s /usr/local/nagios/var/rw
*** External command directory configured ***
[roo...@ip-172-31-93-157 nagios-4.0.8]#
```

i-025f1d18f7c8a8cda (nagios-host)

Public IPs: 3.86.198.73 Private IPs: 172.31.93.157

To resolve the errors run the following commands -

sudo yum install -y gcc glibc glibc-common gd gd-devel make net-snmp openssl-devel

rm -rf nagios-4.0.8

cd ~/downloads/nagios-4.4.6

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

make all

sudo make install

```

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.

[root@ip-172-31-93-157 nagios-4.4.6]#

```

```

GNU nano 5.8
/usr/local/nagios/etc/objects/contacts.cfg
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                2022.anuprita.mhapankar@ves.ac.in   ; <<***** 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{
    contactgroup_name    admins
    alias               Nagios Administrators
    members             nagiosadmin
}

i-025f1d18f7c8a8cda (nagios-host)
PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

```

Step 9: Now run the following commands –

```

sudo make install-webconf
sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
sudo service httpd restart
cd ~/downloads
tar zxvf nagios-plugins-2.0.3.tar.gz

```

```
aws Services Search [Alt+S] N. Virginia v occlabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
- 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.

[root@ip-172-31-93-157 nagios-4.4.6]# sudo nano /usr/local/nagios/etc/objects/contacts.cfg
[root@ip-172-31-93-157 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 ***
[root@ip-172-31-93-157 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
[root@ip-172-31-93-157 nagios-4.4.6]# i-025f1d18f7c8a8cda (nagios-host)
PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157
```

```
CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
aws Services Search [Alt+S] N. Virginia v occlabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
[root@ip-172-31-93-157 nagios-4.4.6]# sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@ip-172-31-93-157 nagios-4.4.6]# cd ~/downloads
tar zxfv nagios-plugins-2.0.3.tar.gz
nagios-plugins-2.0.3/
nagios-plugins-2.0.3/perlmods/
nagios-plugins-2.0.3/perlmods/Config-Tiny-2.14.tar.gz
nagios-plugins-2.0.3/perlmods/parent-0.226.tar.gz
nagios-plugins-2.0.3/perlmods/test-Simple-0.98.tar.gz
nagios-plugins-2.0.3/perlmods/Makefile.in
nagios-plugins-2.0.3/perlmods/version-0.9903.tar.gz
nagios-plugins-2.0.3/perlmods/Makefile.am
nagios-plugins-2.0.3/perlmods/Module-Runtime-0.013.tar.gz
nagios-plugins-2.0.3/perlmods/Module-Metadata-1.00014.tar.gz
nagios-plugins-2.0.3/perlmods/Params-Validate-1.08.tar.gz
nagios-plugins-2.0.3/perlmods/Class-Accessor-0.34.tar.gz
nagios-plugins-2.0.3/perlmods/try-tiny-0.18.tar.gz
nagios-plugins-2.0.3/perlmods/Module-Implementation-0.07.tar.gz
nagios-plugins-2.0.3/perlmods/Makefile
nagios-plugins-2.0.3/perlmods/Perl-OSType-1.003.tar.gz
nagios-plugins-2.0.3/perlmods/install_order
nagios-plugins-2.0.3/perlmods/Nagios_Plugin-0.36.tar.gz
nagios-plugins-2.0.3/perlmods/Math_Calc_Units-1.07.tar.gz
nagios-plugins-2.0.3/perlmods/Module-Build-0.4007.tar.gz
nagios-plugins-2.0.3/ABOUT-NLS
nagios-plugins-2.0.3/configure.ac
nagios-plugins-2.0.3/Makefile.in
nagios-plugins-2.0.3/config.h.in
nagios-plugins-2.0.3/Changelog
nagios-plugins-2.0.3/AUTHORS
nagios-plugins-2.0.3/lib/
nagios-plugins-2.0.3/lib/parse_ini.h
nagios-plugins-2.0.3/lib/extr(opts.c
nagios-plugins-2.0.3/lib/Makefile.in
```

i-025f1d18f7c8a8cda (nagios-host)
PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

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

Step 10: Compile and install plugins

```
cd nagios-plugins-2.0.3
./configure --with-nagios-user=nagios --with-nagios-group=nagios
make
sudo make install
```

```

/usr/bin/install -c -o nagios -g nagios check_dhcp /usr/local/nagios/libexec/check_dhcp
chmod root /usr/local/nagios/libexec/check_dhcp
chmod ug-rx,u+s /usr/local/nagios/libexec/check_dhcp
/usr/bin/install -c -o nagios -g nagios check_icmp /usr/local/nagios/libexec/check_icmp
chmod root /usr/local/nagios/libexec/check_icmp
chmod ug-rx,u+s /usr/local/nagios/libexec/check_icmp
take[2]: Nothing to be done for 'install-data-am'.
take[2]: Leaving directory '/root/downloads/nagios-plugins-2.0.3/plugins-root'
take[1]: Leaving directory '/root/downloads/nagios-plugins-2.0.3/plugins-root'
taking install in po
take[1]: Entering directory '/root/downloads/nagios-plugins-2.0.3/po'
/usr/bin/mkdir -p /usr/local/nagios/share/gettext/po; \
installing fr.qm as /usr/local/nagios/share/locale/fr/LC_MESSAGES/nagios-plugins.mo
installing de.qm as /usr/local/nagios/share/locale/de/LC_MESSAGES/nagios-plugins.mo
if test "nagios-plugins" = "gettext-tools"; then \
/usr/bin/mkdir -p /usr/local/nagios/share/gettext/po; \
for file in Makefile.in.in remove-potcdate.sin Makevars.template; do \
/usr/bin/install -c -o nagios -g nagios -m 644 ./${file} \
/usr/local/nagios/share/gettext/po/${file}; \
done; \
for file in Makevars; do \
rm -f /usr/local/nagios/share/gettext/po/${file}; \
done; \
else \
: ; \
fi
take[1]: Leaving directory '/root/downloads/nagios-plugins-2.0.3/po'
take[1]: Entering directory '/root/downloads/nagios-plugins-2.0.3'
take[2]: Entering directory '/root/downloads/nagios-plugins-2.0.3'
take[2]: Nothing to be done for 'install-exec-am'.
take[2]: Nothing to be done for 'install-data-am'.
take[2]: Leaving directory '/root/downloads/nagios-plugins-2.0.3'
take[1]: Leaving directory '/root/downloads/nagios-plugins-2.0.3'
root@ip-172-31-93-157 nagios-plugins-2.0.3]#

```

i-025f1d18f7c8a8cda (nagios-host)
PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

Step 11: To start nagios run the following commands –
sudo chkconfig --add nagios

sudo chkconfig nagios on

Verify using the following command -

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

```

root@ip-172-31-93-157 nagios-plugins-2.0.3]# sudo chkconfig --add nagios
root@ip-172-31-93-157 nagios-plugins-2.0.3]# sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

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

Website: https://www.nagios.org
Reading configuration data...
Read main config file okay...
WARNING: The normal check_interval attribute is deprecated and will be removed in future versions. Please use check_interval instead.
WARNING: The retry_check_interval attribute is deprecated and will be removed in future versions. Please use retry_interval instead.
WARNING: The normal check_interval attribute is deprecated and will be removed in future versions. Please use check_interval instead.
WARNING: The retry_check_interval attribute is deprecated and will be removed in future versions. Please use retry_interval instead.
Read object config files okay...

running pre-flight check on configuration data...

Checking objects...
Checked 8 services.
Checked 1 hosts.
Checked 1 host groups.
Checked 0 service groups.
Checked 1 contacts.
Checked 1 contact groups.
Checked 24 commands.
Checked 5 time periods.
Checked 0 host escalations.
Checked 0 service escalations.
Checking for circular paths...
Checked 1 hosts


```

i-025f1d18f7c8a8cda (nagios-host)
PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

If there are no errors run the following command –

sudo service nagios start

aws Services Search [Alt+S] N. Virginia vocabs/user3413602:MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793

WARNING: The `retry_check_interval` attribute is deprecated and will be removed in future versions. Please use `retry_interval` instead.

WARNING: The `normal_check_interval` attribute is deprecated and will be removed in future versions. Please use `check_interval` instead.

WARNING: The `retry_check_interval` attribute is deprecated and will be removed in future versions. Please use `retry_interval` instead.

Read object config files okay...

Running pre-flight check on configuration data...

Checking objects...

Checked 8 services.

Checked 1 hosts.

Checked 1 host groups.

Checked 0 service groups.

Checked 1 contacts.

Checked 1 contact groups.

Checked 24 commands.

Checked 5 time periods.

Checked 0 host escalations.

Checked 0 service escalations.

Checking for circular paths...

Checked 1 hosts.

Checked 0 service dependencies.

Checked 0 host dependencies.

Checked 5 timperiods.

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-172-31-93-157 nagios-plugins-2.0.3]# sudo service nagios start
Starting nagios (via systemctl): [ OK ]
[root@ip-172-31-93-157 nagios-plugins-2.0.3]#
```

i-025f1d18f7c8a8cda (nagios-host)

PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

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

Check status using the following command -

`sudo systemctl status nagios`

```
[ec2-user@ip-172-31-13-171 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 Thu 2024-10-03 13:18:35 UTC; 13s ago
     Docs: https://www.nagios.org/documentation
 Process: 67878 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
 Process: 67879 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
Main PID: 67880 (nagios)
   Tasks: 6 (limit: 1112)
      Memory: 2.0M
        CPU: 18ms
       CGroup: /system.slice/nagios.service
           ├─67880 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
           ├─67881 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
           ├─67882 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
           ├─67883 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
           ├─67884 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
           └─67885 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Oct 03 13:18:35 ip-172-31-13-171.ap-south-1.compute.internal nagios[67880]: qh: Socket '/usr/local/nagios/var/rw/nagios.gh' successfully initialized
Oct 03 13:18:35 ip-172-31-13-171.ap-south-1.compute.internal nagios[67880]: qh: core query handler registered
Oct 03 13:18:35 ip-172-31-13-171.ap-south-1.compute.internal nagios[67880]: qh: echo service query handler registered
Oct 03 13:18:35 ip-172-31-13-171.ap-south-1.compute.internal nagios[67880]: qh: help for the query handler registered
Oct 03 13:18:35 ip-172-31-13-171.ap-south-1.compute.internal nagios[67880]: wproc: Successfully registered manager as @wproc with query handler
Oct 03 13:18:35 ip-172-31-13-171.ap-south-1.compute.internal nagios[67880]: wproc: Registry request: name=Core Worker 67884;pid=67884
Oct 03 13:18:35 ip-172-31-13-171.ap-south-1.compute.internal nagios[67880]: wproc: Registry request: name=Core Worker 67883;pid=67883
Oct 03 13:18:35 ip-172-31-13-171.ap-south-1.compute.internal nagios[67880]: wproc: Registry request: name=Core Worker 67882;pid=67882
Oct 03 13:18:35 ip-172-31-13-171.ap-south-1.compute.internal nagios[67880]: wproc: Registry request: name=Core Worker 67881;pid=67881
Oct 03 13:18:36 ip-172-31-13-171.ap-south-1.compute.internal nagios[67880]: Successfully launched command file worker with pid 67885
[ec2-user@ip-172-31-13-171 nagios-plugins-2.3.3]$
```

Step 12: Go to EC2 instance and copy the public IP address of the instance

aws Services Search [Alt+S] Mumbai Atharva

EC Dashboard EC2 Global View Events Instances (1/1) Info Last updated 19 minutes ago Connect Instance state Actions Launch instances

Instances

Name: nagios-host Instance ID: i-09980e5ace4d37d9a Instance state: Running Status check: 2/2 checks passed Alarm status: View alarms Availability Zone: ap-south-1b Public IPv4 DNS: ec2-3-111-58-159.ap-s... Public IPv4 IP: 3.111.58.159 Elastic IP:

i-09980e5ace4d37d9a (nagios-host)

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary Info

Instance ID: i-09980e5ace4d37d9a (nagios-host) Public IPv4 address: 3.111.58.159 | open address

IPv6 address: - Instance state: Running Private IP DNS name (IPv4 only): ip-172-31-13-171.ap-south-1.compute.internal

Hostname type: IP name: ip-172-31-13-171.ap-south-1.compute.internal Answer private resource DNS name: IPv4 (A) Instance type: t2.micro

Auto-assigned IP address: VPC ID: Elastic IP addresses: - AWS Compute Optimizer finding: -

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

Step 13: Now visit http://<your_public_ip_address>/nagios Enter correct credentials and then you will see this page.

The screenshot shows the Nagios Core 4.4.6 web interface. At the top, it displays the Nagios Core logo and a green checkmark indicating "Daemon running with PID 80009". Below this, the version information "Nagios® Core™ Version 4.4.6 April 28, 2020 Check for updates" is shown. A blue banner at the top right says "A new version of Nagios Core is available! Visit nagios.org to download Nagios 4.5.5." On the left, there's a sidebar with links for General (Home, Documentation), Current Status (Tactical Overview, Map (Legacy), Hosts, Services, Host Groups, Grid, Service Groups, Summary), Problems (Services (Unhandled), Hosts (Unhandled), Network Outages), Quick Search, Reports (Availability, Trends (Legacy), Alerts, History, Summary, Histogram (Legacy), Notifications, Event Log), and System (Comments, Done queue, Process Info, Performance Info, Scheduling Queue, Configuration). The main content area has sections for "Get Started" (with a bulleted list of steps), "Quick Links" (with links to Nagios Library, Nagios Labs, Nagios Exchange, Nagios Support, Nagios.com, and Nagios.org), "Latest News" (empty), and "Don't Miss..." (empty). At the bottom, there's a copyright notice, a Nagios logo, and a SourceForge.NET link. A vertical "Page Down" scroll bar is visible on the right side of the browser window.

ADVANCE DEVOPS EXP-10

ATHARVA PRABHU
D15A 43

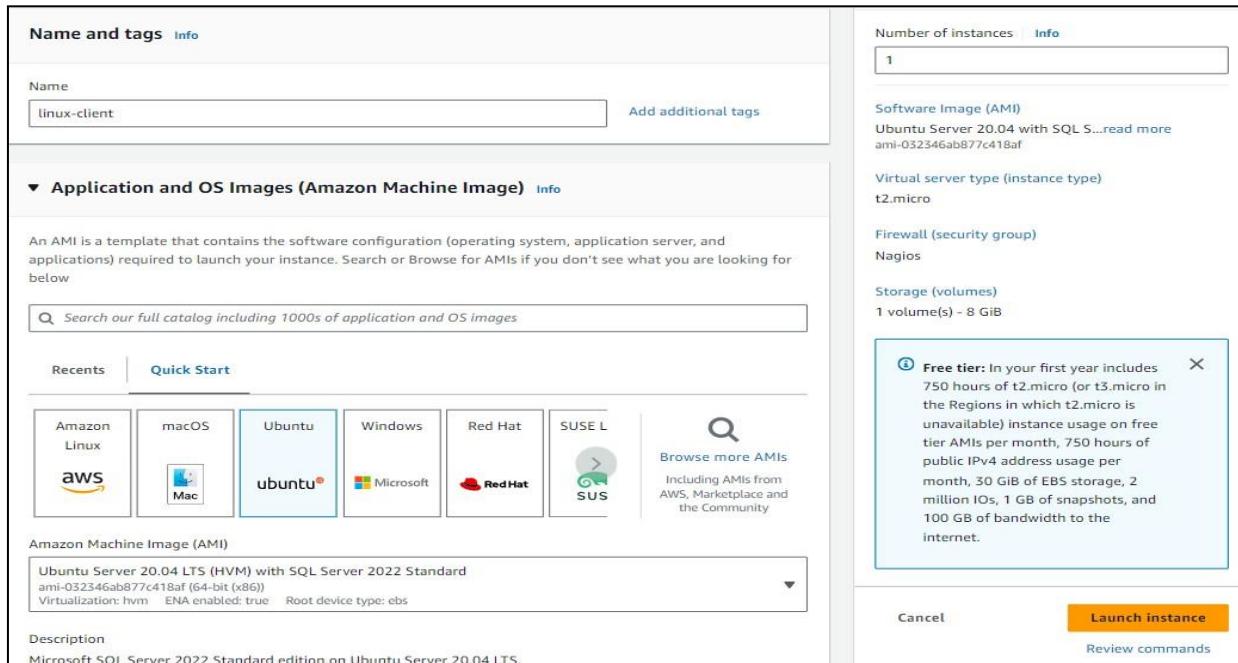
Aim: To perform Port, Service monitoring, Windows/Linux server monitoring using Nagios.

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

```
[ec2-user@ip-172-31-90-152 nagios-plugins-2.3.3]$ cd
[ec2-user@ip-172-31-90-152 ~]$ sudo systemctl restart nagios
[ec2-user@ip-172-31-90-152 ~]$ sudo systemctl status nagios
● nagios.service - Nagios Core 4.5.5
   Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
     Active: active (running) since Mon 2024-09-30 19:41:36 UTC; 7s ago
       Docs: https://www.nagios.org/documentation
   Process: 80238 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
  Process: 80239 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
 Main PID: 80240 (nagios)
    Tasks: 6 (limit: 1112)
   Memory: 4.0M
      CPU: 15ms
     CGroup: /system.slice/nagios.service
             ├─80240 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─80241 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─80242 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─80243 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─80244 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─80245 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: qh: Socket '/usr/local/nagios/var/rw/nagios.qh' successfully initialized
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: qh: core query handler registered
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: qh: echo service query handler registered
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: qh: help for the query handler registered
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Successfully registered manager as @wproc with query handler
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80244;pid=80244
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80243;pid=80243
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80242;pid=80242
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80241;pid=80241
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: Successfully launched command file worker with pid 80245
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: qh: core query handler registered
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: qh: echo service query handler registered
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: qh: help for the query handler registered
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Successfully registered manager as @wproc with query handler
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80244;pid=80244
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80243;pid=80243
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80242;pid=80242
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80241;pid=80241
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: Successfully launched command file worker with pid 80245
```

Step-2. Create an Ubuntu 20.04 Server EC2 Instance



Step-3: Verify Nagios Process on the Server

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

Step-4: Become Root User and Create Directories-

sudo su , mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
and to copy the same config file- cp /usr/local/nagios/etc/objects/localhost.cfg,
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg

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

i-0ae1aae975bae3b7a (nagios-host)

Step-5: Edit the Configuration File

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

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

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

# Define a host for the local machine

define host {

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

    host_name    linuxserver
    alias        linuxserver
    address     35.174.139.220
}

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

# Define an optional hostgroup for Linux machines

define hostgroup {

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

[Read 157 lines]

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

Step-6: Update Nagios Configuration

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

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

```
# 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/
```

Step-7: Verify Configuration Files

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

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

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

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

Running pre-flight check on configuration data...

Checking objects...
  Checked 8 services.
  Checked 2 hosts.
  Checked 2 host groups.
  Checked 0 service groups.
  Checked 1 contacts.
  Checked 1 contact groups.
  Checked 24 commands.
  Checked 5 time periods.
  Checked 0 host escalations.
  Checked 0 service escalations.
Checking for circular paths...
  Checked 2 hosts
  Checked 0 service dependencies
  Checked 0 host dependencies
  Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors: 0
```

Step-8: Restart Nagios Service

```
sudo systemctl restart nagios
```

Step-9: SSH into the Client Machine

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

Step-10: Update Package Index and Install Required Packages

```
sudo apt update -y
```

```
sudo apt install gcc -y
```

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

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

Step-11: Edit NRPE Configuration File

Commands -

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

Add your Nagios host IP address under allowed_hosts:

```
allowed_hosts=<Nagios_Host_IP>
```

```
# Note: The daemon only does rudimentary checking of the client's IP
# address. I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd
allowed_hosts=127.0.0.1,35.174.139.220

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

Step-12: Restart NRPE Server

Commands -

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

Step-13:Check Nagios Dashboard

Open your browser and navigate to http://<Nagios_Host_IP>/nagios.

Log in with nagiosadmin and the password you set earlier.

You should see the new host linuxserver added.

Click on Hosts to see the host details.

Click on Services to see all services and ports being monitored

Nagios® Core™

✓ Daemon running with PID 71172

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

A new version of Nagios Core is available!
Visit nagios.org to download Nagios 4.5.5.

Get Started <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Nagios Library (tutorials and docs) • Nagios Labs (development blog) • Nagios Exchange (plugins and addons) • Nagios Support (tech support) • Nagios.com (company) • Nagios.org (project) 	
Latest News	Don't Miss...	

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

Nagios®

Current Network Status
Last Updated: Mon Sep 30 21:16:41 UTC 2024
Updated every 30 seconds
Nagios® Core™ 4.4.6 - www.nagios.org
Logged in as nagiosadmin

General
Home Documentation

Current Status
Tactical Overview
Map (Legacy)
Hosts Services Host Groups Service Groups Problems Services (Unhandled) Hosts (Unhandled) Network Outages Quick Search:

Host Status Totals Up Down Unreachable Pending 2 0 0 0 All Problems All Types 0 2	Service Status Totals Ok Warning Unknown Critical Pending 6 1 0 1 0 All Problems All Types 2 8	
--	---	--

Host Status Details For All Host Groups

Host **	Status ***	Last Check ***	Duration ***	Status Information
linuxserver	UP	09-30-2024 21:14:52	0d 0h 1m 49s	PING OK - Packet loss = 0%, RTA = 0.98 ms
localhost	UP	09-30-2024 21:14:01	0d 0h 47m 2s	PING OK - Packet loss = 0%, RTA = 0.04 ms

Results 1 - 2 of 2 Matching Hosts

Current Network Status
Last Updated: Mon Sep 30 21:21:11 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.4.6 - www.nagios.org
Logged in as nagiosadmin

Host Status Totals
Up Down Unreachable Pending
2 0 0 0
All Problems All Types
0 2

Service Status Totals
Ok Warning Unknown Critical Pending
6 1 0 1 0
All Problems All Types
2 8

Service Status Details For All Hosts

Host **	Service ***	Status ***	Last Check ***	Duration ***	Attempt ***	Status Information
localhost	Current Load	OK	09-30-2024 21:20:16	0d 0h 50m 55s	1/4	OK - load average: 0.00, 0.00, 0.00
localhost	Current Users	OK	09-30-2024 21:20:54	0d 0h 50m 17s	1/4	USERS OK - 1 users currently logged in
HTTP		WARNING	09-30-2024 21:19:31	0d 0h 46m 40s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 319 bytes in 0.001 second response time
PING		OK	09-30-2024 21:17:09	0d 0h 49m 2s	1/4	PING OK - Packet loss = 0%, RTA = 0.04 ms
Root Partition		OK	09-30-2024 21:17:46	0d 0h 48m 25s	1/4	DISK OK - free space / 6080 MB (74.91% inode=98%);
SSH		OK	09-30-2024 21:18:24	0d 0h 47m 47s	1/4	SSH OK - OpenSSH_8.7 (protocol 2.0)
Swap Usage		CRITICAL	09-30-2024 21:17:01	0d 0h 44m 10s	4/4	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.
Total Processes		OK	09-30-2024 21:19:39	0d 0h 46m 32s	1/4	PROCS OK - 36 processes with STATE = RSZDT

Results 1 - 8 of 8 Matching Services

Experiment 11

Atharva Prabhu

D15A 43

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.

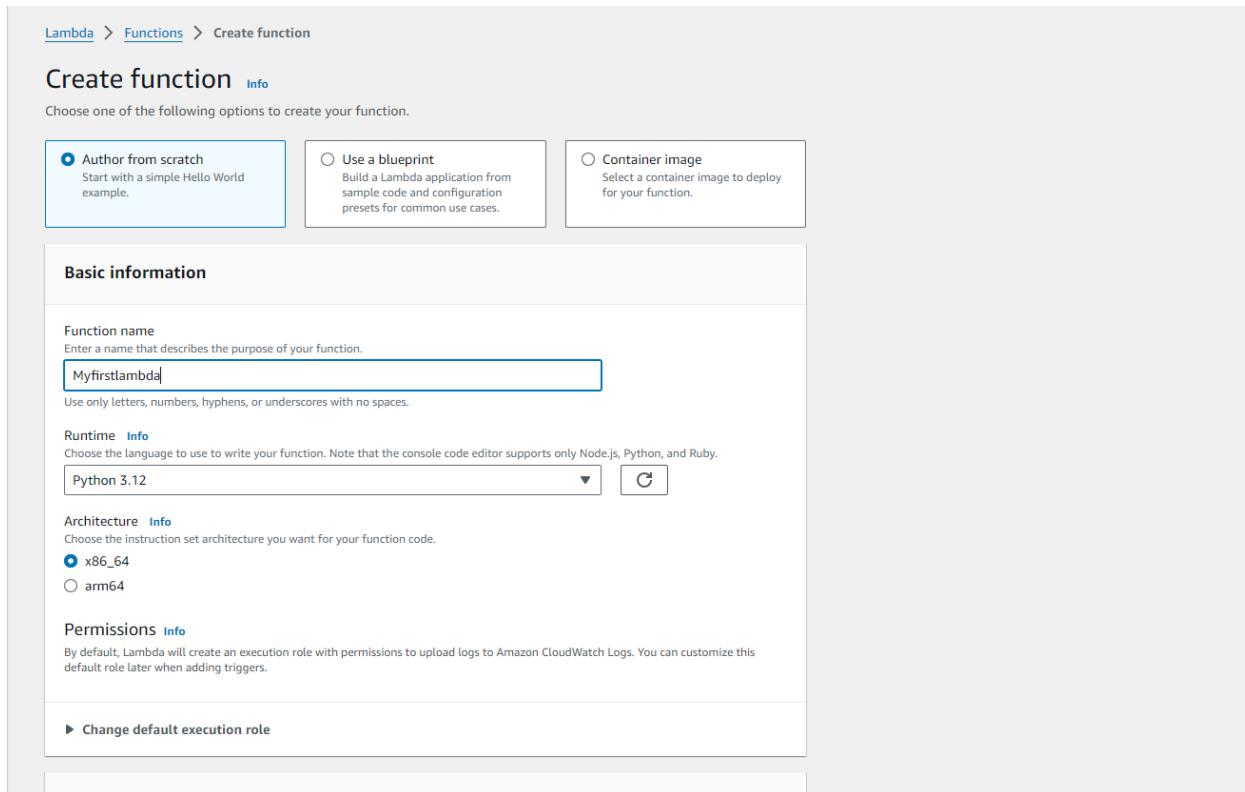
2. Configure the Function:

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.



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': f'Hello, {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 banner indicates: "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" tab is selected, 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

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

Format JSON

Cancel Invoke Save

The screenshot shows the AWS Lambda console interface. At the top, there are tabs for Code, Test, Monitor, Configuration, Aliases, and Versions. The 'Code' tab is currently selected. Below the tabs, there's a 'Code source' section with an 'Info' link. A navigation bar includes File, Edit, Find, View, Go, Tools, Window, Test (which is highlighted in blue), Deploy, and a status message 'Changes not deployed'. On the left, there's a sidebar with an 'Environment' tab selected. The main area shows a file tree with 'Myfirstlambda - /' and 'lambda_function.py'. Under 'Execution results', there's a 'Test Event Name' dropdown set to 'TestEvent'. The 'Response' section displays the following JSON:

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

Below this, the 'Function Logs' section shows the following log output:



```
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 Memory Size: 128 MB
```



The 'Request ID' is highlighted in the log output.


```

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. The workflow of AWS Lambda involves defining a function with specific logic, configuring triggers that will invoke the function, and setting permissions to control access. Lambda supports multiple programming languages, including Python, Java, and Node.js, enabling developers to choose the best fit for their applications. Creating your first Lambda function is straightforward: you write the code, define triggers, and deploy, allowing you to quickly build and run applications without the overhead of managing infrastructure. This simplicity and flexibility make AWS Lambda an excellent tool for building modern, event-driven applications.

EXPERIMENT NO - 12

ATHARVA PRABHU D15A 43

Aim: To create a Lambda function which will log “[An Image has been added](#)” once you add an object to a specific bucket in S3

Theory:

AWS Lambda and S3 Integration: AWS Lambda allows you to execute code in response to various events, including those triggered by Amazon S3. When an object is added to an S3 bucket, it can trigger a Lambda function to execute, allowing for event-driven processing without managing servers.

Workflow:

1. Create an S3 Bucket:

- o First, create an S3 bucket that will store the objects. This bucket will act as the trigger source for the Lambda function.

2. Create the Lambda Function:

- o Set up a new Lambda function using AWS Lambda’s console. You can choose a runtime environment like Python, Node.js, or Java.
- o Write code that logs a message like “An Image has been added” when triggered.

3. Set Up Permissions:

- o Ensure that the Lambda function has the necessary permissions to access S3. You can do this by attaching an IAM role with policies that allow reading from the bucket and writing logs to CloudWatch.

4. Configure S3 Trigger:

- o Link the S3 bucket to the Lambda function by setting up a trigger. Specify that the function should be triggered when an object is created in the bucket (e.g., when an image is uploaded).

5. Test the Setup:

- o Upload an object (e.g., an image) to the S3 bucket to test the trigger. The Lambda function should execute and log the message “An Image has been added” in AWS CloudWatch Logs.

Outcomes:

The screenshot shows the 'Create bucket' configuration page in the AWS S3 console. The 'General configuration' section is visible, showing the AWS Region set to 'Europe (Stockholm) eu-north-1'. Under 'Bucket type', 'General purpose' is selected. A bucket name 'exp12buck' is entered in the 'Bucket name' field. The 'Copy settings from existing bucket - optional' section is present, with a 'Choose bucket' button and a note about the format: 'Format: s3://bucket/prefix'.

The screenshot shows the 'Functions' page in the AWS Lambda console. A function named 'lambdafunc' is listed. A success message states: 'The trigger exp12buck was successfully added to function lambdafunc. The function is now receiving events from the trigger.' The 'Function overview' section shows the function's configuration, including its ARN: arn:aws:lambda:eu-north-1:026090558619:function:lambdafunc. The 'Configuration' tab is selected at the bottom. On the right side, there is a 'Tutorials' sidebar with a 'Create a simple web app' section and a 'Start tutorial' button.

The screenshot shows the AWS Lambda function configuration interface. At the top, there is a code editor window titled "lambda_function" containing Python code for a Lambda function. Below the code editor is a navigation bar with tabs: "Code", "Test", "Monitor", "Configuration" (which is selected), "Aliases", and "Versions".

In the main content area, under the "Configuration" tab, there is a "Triggers" section. It shows one trigger named "S3: exp12buck" which is associated with the ARN "arn:aws:s3:::exp12buck". A "Details" link is also present next to the trigger name.

To the right of the triggers section, there is a "Tutorials" sidebar. The "Create a simple web app" tutorial is currently selected. The sidebar includes a brief description of the tutorial, a list of steps, and a "Start tutorial" button.

The bottom of the interface shows the standard AWS navigation bar with links for CloudShell, Feedback, and various AWS services like S3, Lambda, and CloudWatch. The status bar at the bottom right indicates the date and time as "03-10-2024 14:31".

```
1 import json
2
3 def lambda_handler(event, context):
4     # Extract bucket name and object key from the event
5     bucket_name = event['Records'][0]['s3']['bucket']['name']
6     object_key = event['Records'][0]['s3']['object']['key']
7
8     # Log a message
9     print(f"An Image has been added to the bucket {bucket_name}: {object_key}")
10
11    return {
12        'statusCode': 200,
13        'body': json.dumps('Log entry created successfully')
14    }
15
```

The screenshot shows the AWS S3 console interface. At the top, a green banner displays the message "Upload succeeded". Below this, a summary table shows the destination as "s3://exp12buck" and the status as "Succeeded" with "1 file, 41.0 KB (100.00%)". A note below the summary states: "The information below will no longer be available after you navigate away from this page." Under the "Files and folders" tab, a table lists one file: "pngwing.co..." which is an image/png file of size 41.0 KB and status "Succeeded". The AWS CloudShell icon is visible at the bottom left, and the system tray at the bottom right shows the date and time as 03-10-2024.

The screenshot shows the AWS CloudWatch Log Events interface. The left sidebar navigation includes "CloudWatch" (selected), "Services", "Search", and "CloudShell". Under "Logs", "Log groups" is selected, showing a log group for "/aws/lambda/MyfirstLambda" with log events for the date 2024/10/09. The log events table has columns for "Timestamp" and "Message". The messages show Lambda startup and execution details, such as "INIT START Runtime Version: python3.12-v36" and "REPORT RequestId: c556902f-24f7-42e5-80a7-9f68e414ec19 Duration: 2.13 ms Billed Duration: 3 ms Memory Size: 128 MB Max Memory Used: 32 MB Init Duration: 88.18 ms".

Conclusion:

Integrating AWS Lambda with S3 allows for real-time, automated processing of events such as file uploads. In this example, a Lambda function is configured to log a message whenever an image is added to a specific S3 bucket.

