

Experiment 1

Aim:

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

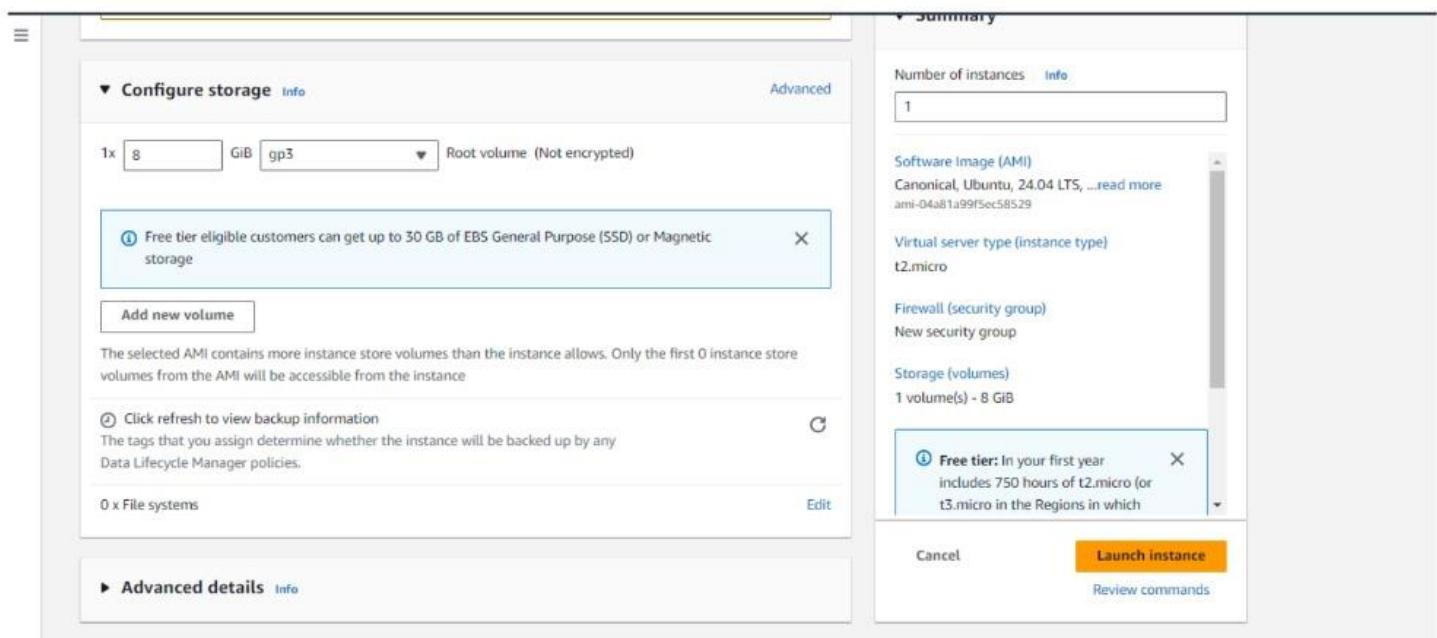
1. Open AWS Academia and select launch instance

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with navigation links like 'Instances', 'Images', and 'Elastic Block Store'. The main area has a 'Resources' summary table and a 'Launch instance' section. The 'Launch instance' section contains a large orange 'Launch instance' button. To the right, there's a sidebar titled 'EC2 Free Tier Info' with a link to 'View all AWS Free Tier offers'. Below that is an 'Account attributes' section with a 'Default VPC' dropdown set to 'vpc-0fc2f3f7a22f1a71'. There are also sections for 'Settings' (Data protection and security, Zones, EC2 Serial Console, Default credit specification, EC2 console preferences) and 'Additional information'.

2. Select Ubuntu

The screenshot shows the AWS Lambda console. It features a 'Quick Start' section with various operating system icons (Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE L). Below this is a search bar and a 'Browse more AMIs' link. A specific 'Ubuntu Server 24.04 LTS (HVM), SSD Volume Type' AMI is selected, showing its details: AMI ID 'ami-04a81a99f5ec58529', Virtualization type 'hvm', ENA enabled 'true', and Root device type 'ebs'. The 'Free tier eligible' status is indicated. The 'Summary' section on the right shows 'Number of instances: 1', 'Software Image (AMI): Canonical, Ubuntu, 24.04 LTS', 'Virtual server type (instance type): t2.micro', 'Firewall (security group): New security group', and 'Storage (volumes): 1 volume(s) - 8 GiB'. A note about the free tier is present. At the bottom, there are 'Cancel' and 'Launch instance' buttons.

3. Set the configuration



4. 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 disabled due to load higher than 1.0

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

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

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

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

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

ubuntu@ip-172-31-17-139:~$ sudo su
root@ip-172-31-17-139:/home/ubuntu# sudo apt install
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
root@ip-172-31-17-139:/home/ubuntu# i-0f7cedaab7d390e14 (My Web Server)
PublicIPs: 3.91.6.193 PrivateIPs: 172.31.17.139
```

```
aws Services Search [Alt+S] N. Virginia vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
root@ip-172-31-17-139:/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://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [265 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [63.3 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [3668 B]
Get:10 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [247 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [107 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [8632 B]
Get:13 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [9220 B]
Get:14 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [208 kB]
Get:15 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [40.7 kB]
Get:16 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 c-n-f Metadata [420 B]
Get:17 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [10.6 kB]
Get:18 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [2808 B]
Get:19 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Get:20 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [344 B]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [318 kB]
Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [82.9 kB]
Get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [5676 B]
Get:30 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [319 kB]
Get:31 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [134 kB]
Get:32 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [45.0 kB]
Get:33 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [12.6 kB]
Get:34 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [208 kB]
aws Services Search [Alt+S] N. Virginia vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
Get:34 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [208 kB]
Get:35 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [40.7 kB]
Get:36 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 c-n-f Metadata [416 B]
Get:37 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [14.1 kB]
Get:38 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [3608 B]
Get:39 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [212 B]
Get:40 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [532 B]
Get:41 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Get:42 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 c-n-f Metadata [112 B]
Get:43 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Packages [10.3 kB]
Get:44 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe Translation-en [10.5 kB]
Get:45 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [17.6 kB]
Get:46 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 c-n-f Metadata [1016 B]
Get:47 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:48 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 c-n-f Metadata [116 B]
Get:49 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Get:50 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 c-n-f Metadata [116 B]
Fetched 28.2 MB in 6s (5073 kB/s)
Reading package lists... Done
root@ip-172-31-17-139:/home/ubuntu# apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-db-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblbu5.4-0 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 libapr1t64 libaprutil1-db-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblbu5.4-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 42 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 libapr1t64 amd64 1.7.2-3.1build2 [107 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.lubuntu7 [91.9 kB]
```

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

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 libapr1t64 amd64 1.7.2-3.1build2 [107 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.lubuntu7 [91.9 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-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 libaprutil1-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 [166 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/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 (25.8 MB/s)
Preconfiguring packages ...
Selecting previously unselected package libapr1t64:amd64.
(Reading database ... 67739 files and directories currently installed.)
Preparing to unpack .../0-libapr1t64_1.7.2-3.1build2_amd64.deb ...
Unpacking libapr1t64:amd64 (1.7.2-3.1build2) ...
Selecting previously unselected package libaprutil1t64:amd64.
Preparing to unpack .../1-libaprutil1t64_1.6.3-1.lubuntu7_amd64.deb ...
Unpacking libaprutil1t64:amd64 (1.6.3-1.lubuntu7) ...
Selecting previously unselected package libaprutil1-dbd-sqlite3:amd64.
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-ldap:amd64.
Preparing to unpack .../3-libaprutil1-ldap_1.6.3-1.lubuntu7_amd64.deb ...
Unpacking libaprutil1-ldap: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 ...

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

Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /usr/lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /usr/lib/systemd/system/apache-htcacheclean.service.
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.2) ...
Scanning processes...
Scanning 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-172-31-17-139:/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 Wed 2024-08-07 14:32:03 UTC; 32s ago
 Docs: https://httpd.apache.org/docs/2.4/
 Main PID: 2487 (apache2)
 Tasks: 55 (limit: 1130)
 Memory: 5.4M (peak: 5.6M)
 CPU: 37ms
 CGroup: /system.slice/apache2.service
 ├─2487 /usr/sbin/apache2 -k start
 ├─2490 /usr/sbin/apache2 -k start
 └─2491 /usr/sbin/apache2 -k start

Aug 07 14:32:03 ip-172-31-17-139 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Aug 07 14:32:03 ip-172-31-17-139 systemd[1]: Started apache2.service - The Apache HTTP Server.
root@ip-172-31-17-139:/home/ubuntu# cd /var/www/html/
root@ip-172-31-17-139:/var/www/html# []

5. Edit the inbound and outbound rules.

Screenshot of the AWS EC2 Security Groups Details page for security group sg-0501f07360e1dce47 - launch-wizard-1.

Details

Security group name launch-wizard-1	Security group ID sg-0501f07360e1dce47	Description launch-wizard-1 created 2024-08-07T14:21:19.108Z	VPC ID vpc-0ec7dea564d6f7acf
Owner 856746069793	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules (1)

Name	Security group rule...	IP version	Type	Protocol	Port range
-	sgr-09fa8639sec8777e3	IPv4	HTTP	TCP	80

Screenshot of the AWS EC2 Security Groups Details page for security group sg-0501f07360e1dce47 - launch-wizard-1.

Details

Security group name launch-wizard-1	Security group ID sg-0501f07360e1dce47	Description launch-wizard-1 created 2024-08-07T14:21:19.108Z	VPC ID vpc-0ec7dea564d6f7acf
Owner 856746069793	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Outbound rules (1)

Name	Security group rule...	IP version	Type	Protocol	Port range
-	sgr-0cc59fd03e24266	IPv4	HTTP	TCP	80

6. This is the hosted Static Website.

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   '-- ports.conf
|-- mods-enabled
|   '-- *.Load
|   '-- *.conf
|-- conf-enabled
|   '-- *.conf
|-- sites-enabled
|   '-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain

Using S3

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

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.

error.html

Redirection rules - optional

2. Upload a file

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, a search bar, and account information for 'N. Virginia' and 'AnupritaMhapankar'. Below the navigation is a breadcrumb trail: 'Amazon S3 > Buckets > anubucke'. The main content area has a title 'anubucke [Info](#)'. A horizontal menu bar below the title includes 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is selected, showing a table of objects. The table has columns for 'Name', 'Type', 'Last modified', 'Size', and 'Storage class'. One object, 'index.html', is listed: Name is 'index.html', Type is 'html', Last modified is 'August 22, 2024, 21:13:21 (UTC+05:30)', Size is '259.0 B', and Storage class is 'Standard'. Action buttons at the top of the table include 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'.

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 navigation bar with the AWS logo, 'Services' dropdown, a search bar, and account information for 'N. Virginia' and 'AnupritaMhapankar'. Below the navigation is a breadcrumb trail: 'Amazon S3 > Buckets > anubucke > Edit Block public access (bucket settings)'. The main content area has a title 'Edit Block public access (bucket settings) [Info](#)'. A section titled 'Block public access (bucket settings)' contains a note about how public access is granted through access control lists (ACLs), bucket policies, access point policies, or all. It says turning 'Block all public access' on is the same as turning on all four settings below. The settings listed are: 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public access and cross-account access to buckets and objects through any public bucket or access point policies'. At the bottom of the page are 'Cancel' and 'Save changes' buttons.

4. Click on Object Ownership under Permission Tab

S Services Search [Alt+S] N. Virginia AnupritaMhapankar

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

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

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

S Services Search [Alt+S] N. Virginia AnupritaMhapankar

Amazon S3 > Buckets > anubucke

anubucke [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, your

Find objects by prefix

Name	Type	Last modified	Size
<input checked="" type="checkbox"/> index.html	html	August 22, 2024, 21:13:21 (UTC+05:30)	

Actions ▾ Create folder

Download as [Learn more](#)

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

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

6. Select on Make Public

The screenshot shows the 'Amazon S3 > Buckets > anubucke > Make public' interface. A yellow warning box states: 'When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.' Below it, a table lists 'Specified objects' with one item: 'index.html' (html, August 22, 2024, 21:13:21 (UTC+05:30), 259.0 B). Buttons for 'Cancel' and 'Make public' are at the bottom.

7. Visit the domain and the website hosted.

The screenshot shows a web browser window with the URL 'https://anubucke.s3.amazonaws.com/index.html'. The page content is 'Hello World. This is Anuprita Mhapankar'.

Dynamic Hosting :

Step 1: Clone the following Github repository

Code

About

Define a data property on an object. Will fall back to assignment in an engine without descriptors.

Tags

- javascript
- data
- object
- ecmascript
- property
- enumerable
- configurable
- accessor
- define
- writable

Readme

MIT license

Code of conduct

Security policy

Activity

4 stars

2 watching

0 forks

Report repository

Releases

7 tags

Step 2: Open Console and run the following command

```
root@ip-172-31-55-145:/home/ubuntu/dynamic/dyanamic_site# npm i
( ) :: reify:define-data-property: http fetch GET 200 https://registry.npmjs.org/define-data-prop
added 93 packages, and audited 94 packages in 3s

16 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
root@ip-172-31-55-145:/home/ubuntu/dynamic/dyanamic_site# npm start

> hosting-dynamic-website@1.0.0 start
> nodemon index.js

[nodemon] 3.1.4
[nodemon] to restart at any time, enter `rs`
[nodemon] watching path(s): ***!
[nodemon] watching extensions: js,mjs,cjs,json
[nodemon] starting `node index.js`
Server is running on port 3000
```

Step 3: Install necessary packages and run the website on port number 3000.

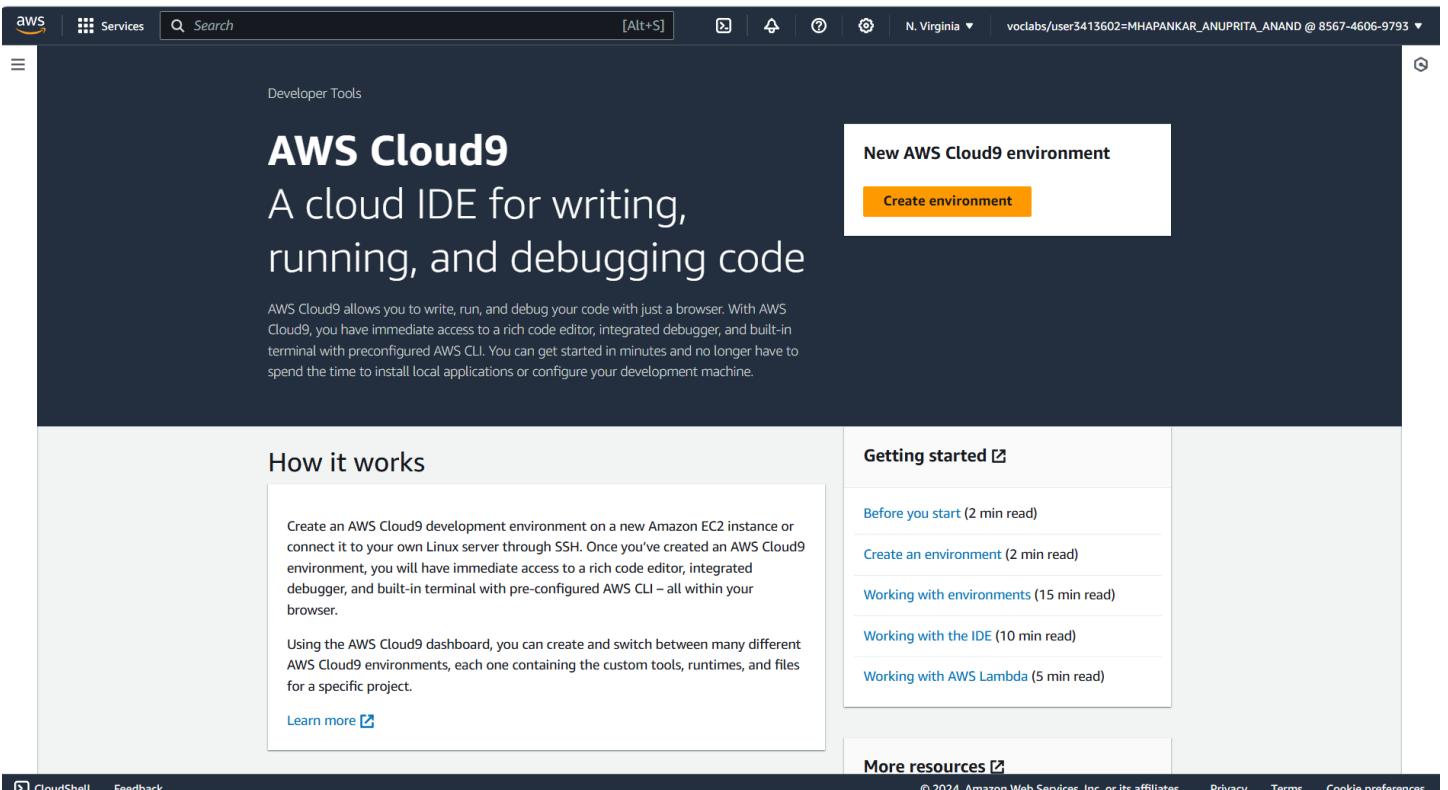
Not secure 54.237.31.193:3000

Hey this is Dynamic Website.

Hey this is about page.

IDE Hosting :

Step 1: Go to AWS Academy and open AWS Cloud9 from developer Tools.



The screenshot shows the AWS Cloud9 landing page within the AWS Developer Tools. At the top right, there's a 'Create environment' button. Below it, a section titled 'How it works' explains the process of creating an AWS Cloud9 development environment. To the right, a 'Getting started' sidebar lists several learning paths: 'Before you start' (2 min read), 'Create an environment' (2 min read), 'Working with environments' (15 min read), 'Working with the IDE' (10 min read), and 'Working with AWS Lambda' (5 min read). At the bottom, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates.' followed by 'Privacy', 'Terms', and 'Cookie preferences'.

Step 2: Create a environment

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

AWS Cloud9 > Environments > Create environment

Create environment Info

Details

Name Limit of 60 characters, alphanumeric, and unique per user.

Description - *optional* Limit 200 characters.

Environment type Info
Determines what the Cloud9 IDE will run on.

New EC2 instance Cloud9 creates an EC2 instance in your account. The configuration of your EC2 instance cannot be changed by Cloud9 after creation.

Existing compute You have an existing instance or server that you'd like to use.

New EC2 instance

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

t2.micro (1 GiB RAM + 1 vCPU)
Free-tier eligible. Ideal for small web applications.

t3.small (2 GiB RAM + 2 vCPU)
Recommended for small web applications.

m5.large (8 GiB RAM + 2 vCPU)
Recommended for production and mission-critical workloads.

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

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

How long Cloud9 can be inactive (no user input) before data monitoring runs help prevent unnecessary charges.

30 minutes ▾

Network settings Info

Connection
How your environment is accessed.

AWS Systems Manager (SSM)
Accesses environment via SSM without opening inbound ports (no ingress).

Secure Shell (SSH)
Accesses environment directly via SSH, opens inbound ports.

▶ VPC settings Info

▶ Tags - *optional* Info
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

The following IAM resources will be created in your account

- **AWSServiceRoleForAWSCloud9** - AWS Cloud9 creates a service-linked role for you. This allows AWS Cloud9 to call other AWS services on your behalf. You can delete the role from the AWS IAM console once you no longer have any AWS Cloud9 environments. [Learn more](#)
- **AWSCloud9SSMAccessRole** and **AWSCloud9SSMInstanceProfile** - A service role and an instance profile are automatically created if Cloud9 accesses its EC2 instance through AWS Systems Manager. If your environments no longer require EC2 instances that block incoming traffic, you can delete these roles using the AWS IAM console. [Learn more](#)

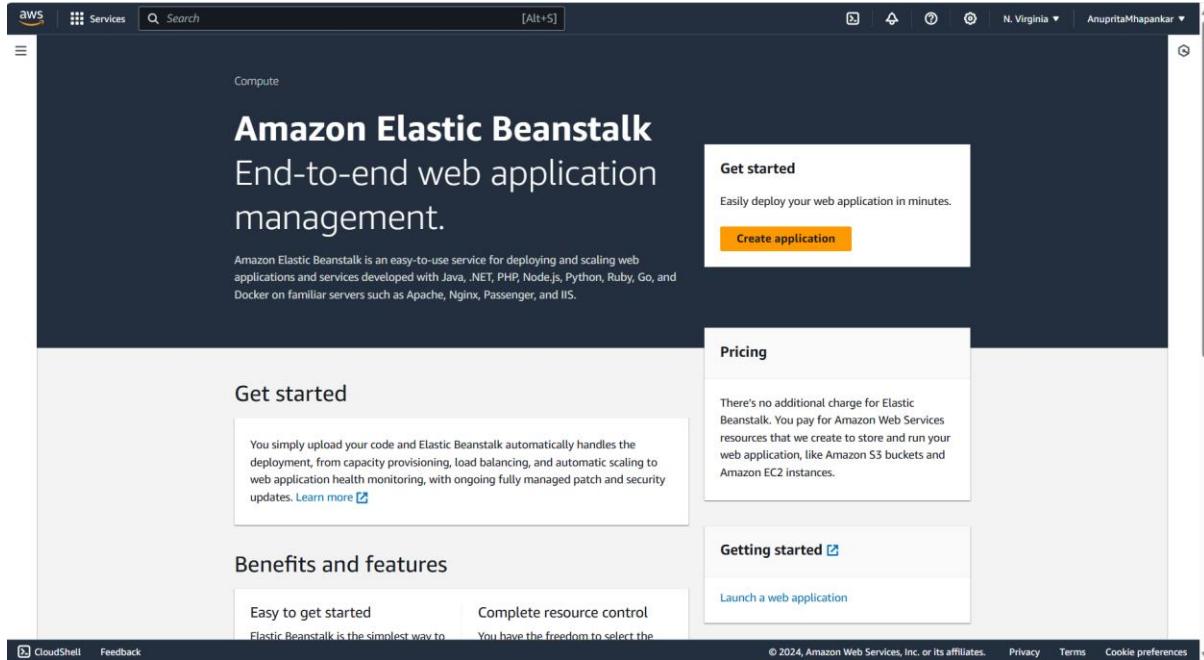
Cancel **Create**

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

Experiment 2

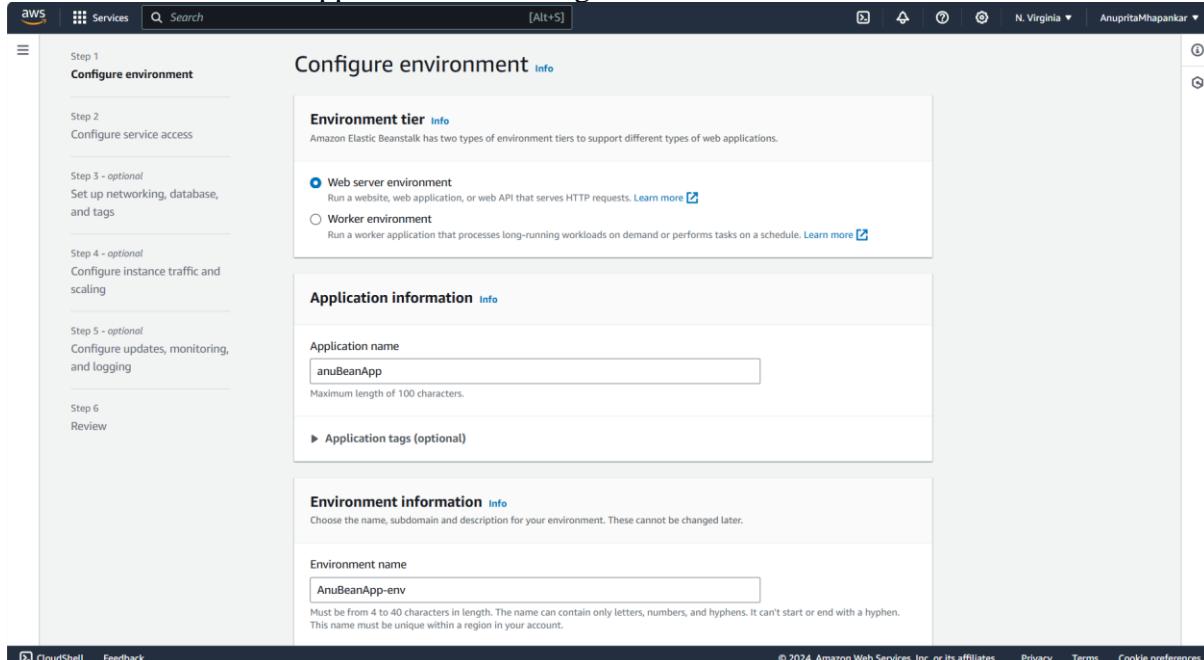
Using Beanstalk

1. Search Elastic Beanstalk from Developer Tools



The screenshot shows the AWS Elastic Beanstalk landing page. At the top, there's a search bar and a 'Get started' button. Below the header, the title 'Amazon Elastic Beanstalk' and subtitle 'End-to-end web application management.' are displayed. A brief description of the service follows. On the left, there's a 'Get started' section with a box containing text about uploading code. On the right, there are sections for 'Pricing' (no additional charge), 'Getting started' (with a 'Launch a web application' button), and 'Benefits and features' (listing 'Easy to get started' and 'Complete resource control'). The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, and Copyright information.

2. Click on create application and configure the environment



The screenshot shows the 'Configure environment' step of the AWS Elastic Beanstalk setup wizard. On the left, a sidebar lists steps: Step 1 (Configure environment), Step 2 (Configure service access), Step 3 - optional (Set up networking, database, and tags), Step 4 - optional (Configure instance traffic and scaling), Step 5 - optional (Configure updates, monitoring, and logging), and Step 6 (Review). The main area is titled 'Configure environment'. It contains three sections: 'Environment tier' (selected 'Web server environment'), 'Application information' (application name 'anuBeanApp'), and 'Environment information' (environment name 'AnuBeanApp-env'). Each section has a detailed description and validation rules. The bottom of the page includes standard AWS navigation links.

3. Choose PHP from the dropdown menu and click next

Platform type

- Managed platform Platforms published and maintained by Amazon Elastic Beanstalk. [Learn more](#)
- Custom platform Platforms created and owned by you. This option is unavailable if you have no platforms.

Platform

PHP

Platform branch

PHP 8.3 running on 64bit Amazon Linux 2023

Platform version

4.3.2 (Recommended)

Application code

- 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.

Presets

Start from a preset that matches your use case or choose custom configuration to unset recommended values and use the service's default

4. From the dropdown menu select the key pair and instance profile

Step 1 [Configure environment](#)

Step 2 **Configure service access**

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

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

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

Step 6 [Review](#)

Configure service access [Info](#)

Service access

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

Service role

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

Service role name

Enter the name for an IAM role that Elastic Beanstalk will create to assume as a service role. Beanstalk will attach the required managed policies to it.

aws-elasticbeanstalk-service-role

[View permission details](#)

EC2 key pair

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

myKey

[View permission details](#)

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

5. Review the changes made and click on Submit

The screenshot shows the AWS Lambda configuration interface. In the 'Environment properties' section, there is a table with one row and two columns. The first column is 'Key' and the second is 'Value'. The key is 'No environment properties' and the value is 'There are no environment properties defined'. At the bottom right of the configuration screen, there are 'Cancel', 'Previous', and 'Submit' buttons.

Pipeline Creation :

1. Fork a github repo for aws codepipeline.

The screenshot shows a GitHub repository page for 'aws-codepipeline-s3-codedeploy-linux-2.0'. The repository has 20 commits, 445 forks, and 4 stars. The repository description is: 'Use this sample when creating a simple pipeline in AWS CodePipeline while following the Simple Pipeline Walkthrough tutorial.' The repository includes files like README.md, CONTRIBUTING.md, LICENSE, and app-specification.yml. On the right side, there are sections for 'About', 'Releases', and 'Packages'.

2. Go to developer tools and select CodePipeline and create a new pipeline

The screenshot shows the AWS CodePipeline Pipelines page. The left sidebar has a tree view with 'Source' (CodeCommit), 'Artifacts' (CodeArtifact), 'Build' (CodeBuild), 'Deploy' (CodeDeploy), and 'Pipeline' (CodePipeline). Under Pipeline, 'Getting started' is expanded, showing 'Pipelines' (selected) and 'Settings'. Below the sidebar are links for 'Go to resource' and 'Feedback'. The main content area shows a banner about the new V2 pipeline type. A search bar and filter buttons ('Notify', 'View history', 'Release change', 'Delete pipeline') are at the top. A large button labeled 'Create pipeline' is prominent. Below is a table with columns: Name, Latest execution status, Latest source revisions, Latest execution started, and Most recent executions. A message 'No results' indicates there are no pipelines to display.

3. Name your pipeline and select the desired service role

The screenshot shows the 'Pipeline settings' step of creating a new pipeline. On the left, a sidebar lists steps: Step 2 (Add source stage), Step 3 (Add build stage), Step 4 (Add deploy stage), Step 5 (Review). The main area is titled 'Pipeline settings'. It shows a 'Pipeline name' input field containing 'anupritaPipelineNew'. Below it is a note: 'You can no longer create V1 pipelines through the console. We recommend you use the V2 pipeline type with improved release safety, pipeline triggers, parameterized pipelines, and a new billing model.' Under 'Execution mode', the 'Queued (Pipeline type V2 required)' option is selected. Under 'Service role', the 'New service role' option is selected, with a sub-note: 'Create a service role in your account'. A 'Role name' input field contains 'AWSCodePipelineServiceRole-us-east-1-anupritaPipelineNew'. A checkbox 'Allow AWS CodePipeline to create a service role so it can be used with this new pipeline' is checked. The bottom of the page includes standard AWS footer links: CloudShell, Feedback, © 2024, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

S | Services | Search [Alt+S] | N. Virginia | AnupritaMhapankar | ⓘ | ⓘ

Service role

New service role
Create a service role in your account

Existing service role
Choose an existing service role from your account

Role name

AWSCodePipelineServiceRole-us-east-1-anupritaPipeline

Type your service role name

Allow AWS CodePipeline to create a service role so it can be used with this new pipeline

Variables

You can add variables at the pipeline level. You can choose to assign the value when you start the pipeline. Choosing this option requires pipeline type V2. [Learn more](#)

No variables defined at the pipeline level in this pipeline.

Add variable
You can add up to 50 variables.

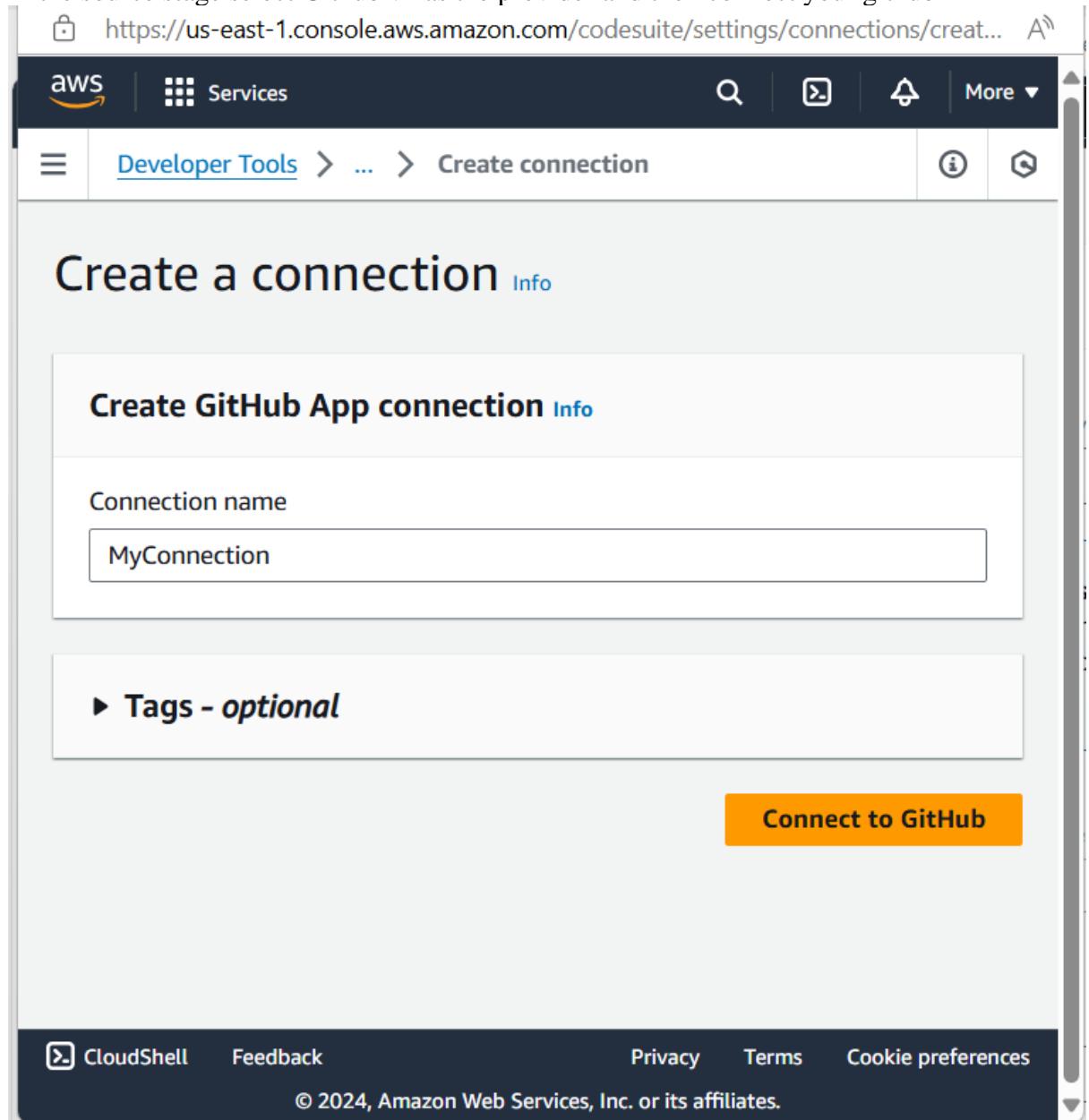
Info The first pipeline execution will fail if variables have no default values.

Advanced settings

Cancel **Next**

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

4. In the source stage select Github v2 as the provider and then connect your github

A screenshot of the AWS CodeSuite interface showing the 'Create a connection' page for creating a GitHub App connection. The URL in the address bar is https://us-east-1.console.aws.amazon.com/codesuite/settings/connections/create... . The top navigation bar includes the AWS logo, Services, search, and more options. The breadcrumb navigation shows 'Developer Tools > ... > Create connection'. The main title is 'Create a connection' with an 'Info' link. Below it, the specific section title is 'Create GitHub App connection' with an 'Info' link. A 'Connection name' input field contains 'MyConnection'. A 'Tags - optional' section is present. At the bottom right is a large orange 'Connect to GitHub' button. The footer includes links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences, along with a copyright notice: © 2024, Amazon Web Services, Inc. or its affiliates.

Authorize AWS Connector for GitHub - Personal - Microsoft Edge

https://github.com/login/oauth/authorize?client_id=lv1.ab636337c58c3ec...

AWS Connector for GitHub by **Amazon Web Services** would like permission to:

-  Verify your GitHub identity (Anuprita579)
-  Know which resources you can access
-  Act on your behalf
 - [Learn more](#)

[Learn more about AWS Connector for GitHub](#)

[Cancel](#) **Authorize AWS Connector for GitHub**

Authorizing will redirect to
<https://redirect.codestar.aws>

 Not owned or operated by GitHub

 Created 4 years ago



<https://github.com/apps/aws-connector-for-github/installations/new/personal>



Install AWS Connector for GitHub

Install on your personal account Anuprita Mhapankar 

for these repositories:

All repositories

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

Only select repositories

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

with these permissions:

- Read** access to issues and metadata
- Read and write** access to administration, code, commit statuses, pull

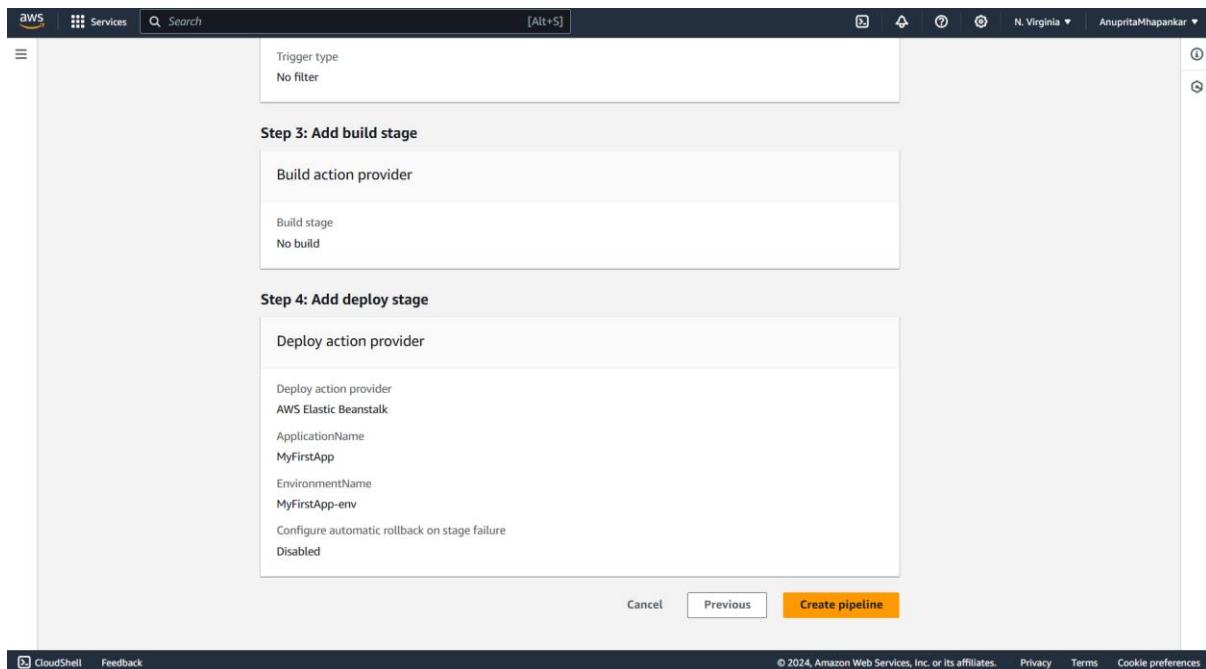
5. Once the connection is established from the drop down menu select the repository and the branch

The screenshot shows the 'Add GitHub action' configuration screen. It includes a note about GitHub version 2 actions, a search bar for connections, and a message indicating the GitHub connection is ready to use. Fields for Repository name (Anuprita579/aws-codepipeline-s3-codedeploy-linux-2.0) and Default branch (master) are filled out. The 'Output artifact format' section shows 'CodePipeline default' selected.

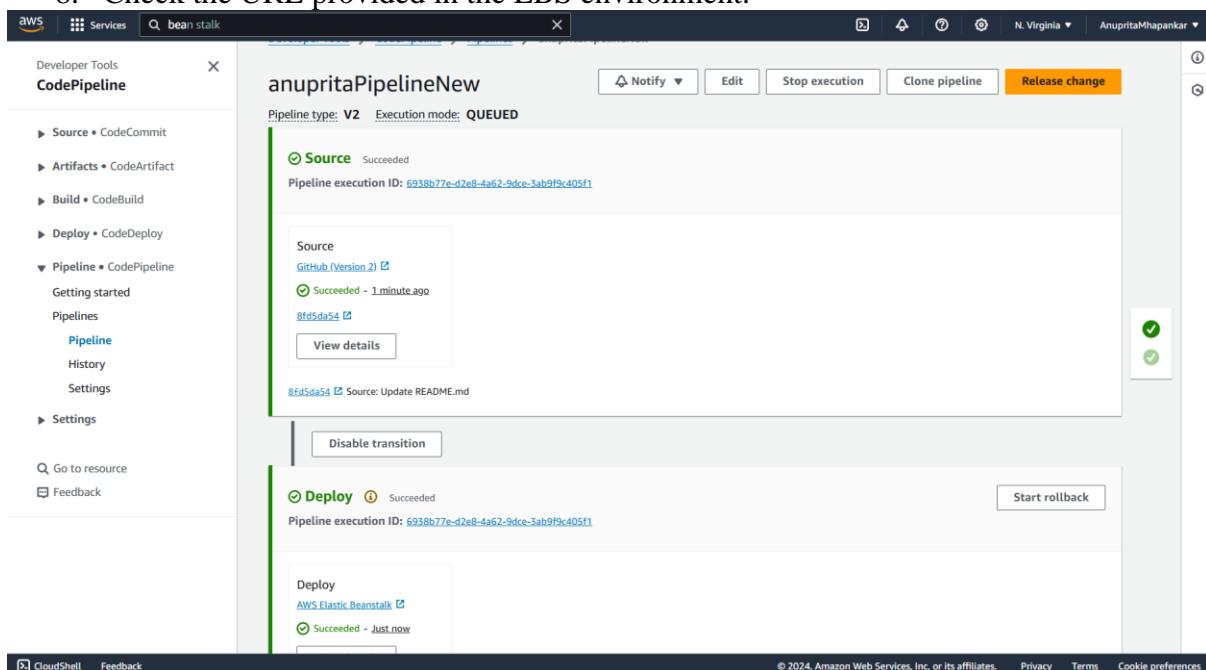
6. Skip the build stage

The screenshot shows the 'Add deploy stage' configuration screen. It includes a 'Deploy' provider dropdown set to 'AWS Elastic Beanstalk', a region dropdown set to 'US East (N. Virginia)', and an input artifact dropdown set to 'SourceArtifact'. The 'Application name' field contains 'myBeanApp' and the 'Environment name' field contains 'MyBeanApp-env'. A checkbox for 'Configure automatic rollback on stage failure' is present. Navigation buttons 'Cancel', 'Previous', and 'Next' are at the bottom.

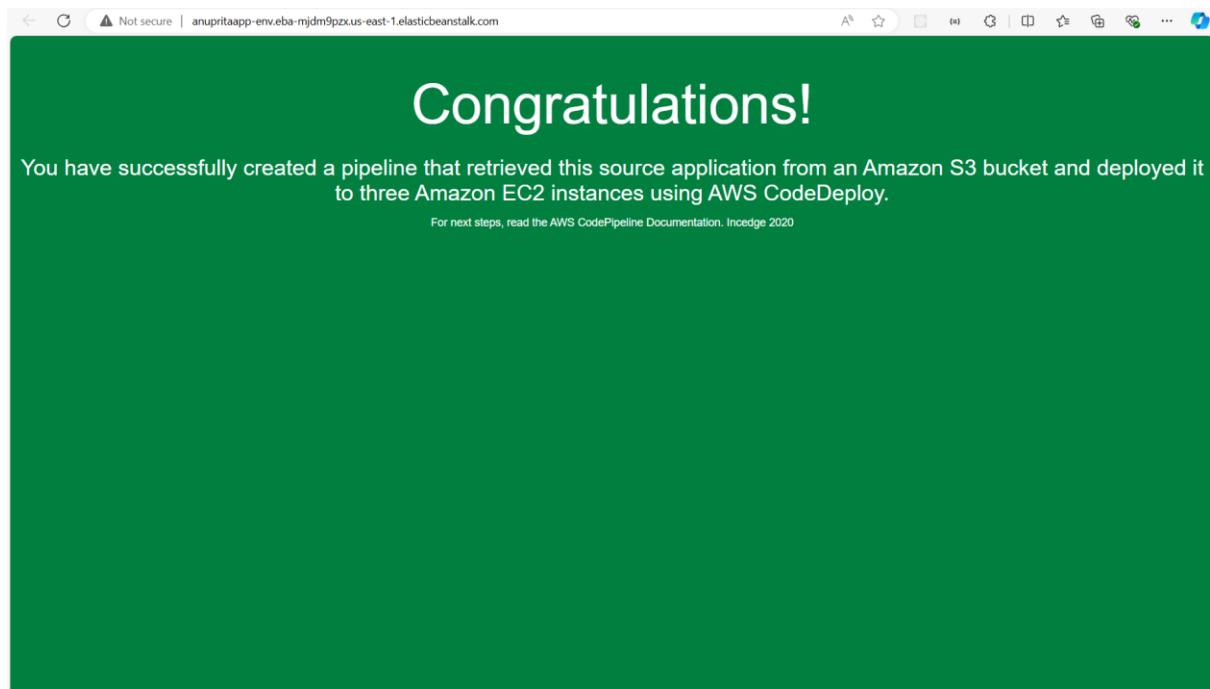
7. Review the settings and click on create pipeline



8. Check the URL provided in the EBS environment.



9. The website is hosted from the forked repo in our beanstalk environment



10. Now, Edit index.html file and then commit the changes

Commit changes ×

Commit message

Update index.html

Extended description

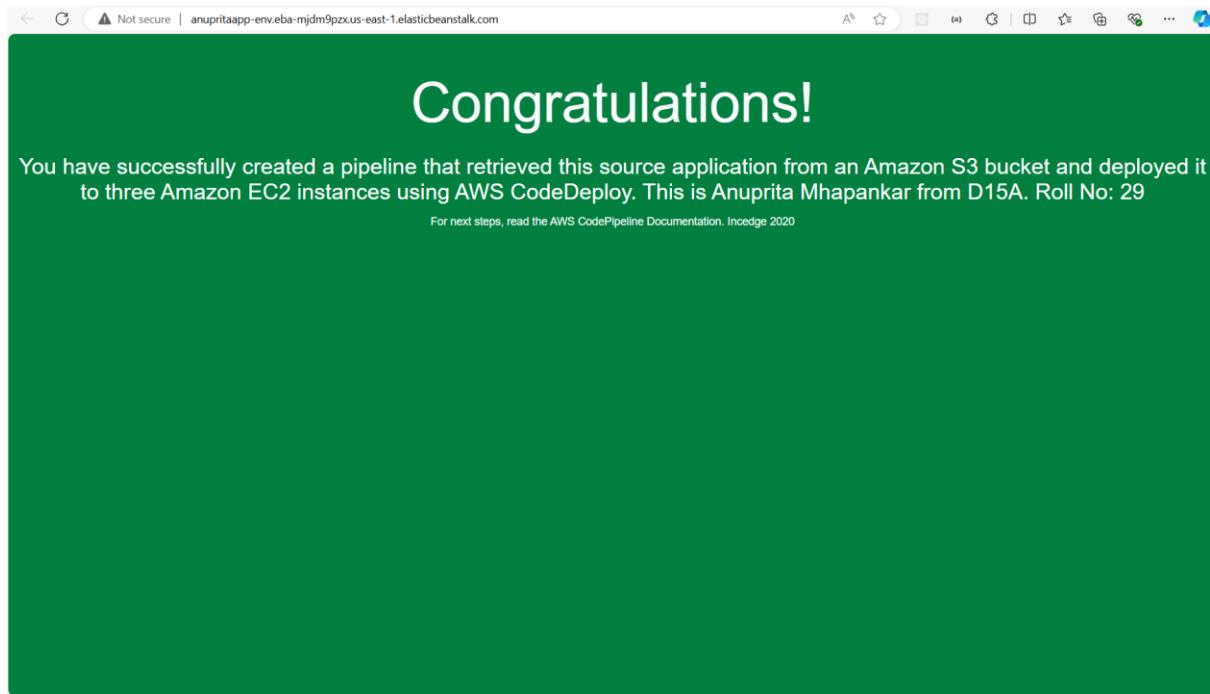
Add an optional extended description..

Commit directly to the `master` branch

Create a **new branch** for this commit and start a pull request [Learn more about pull requests](#)

Cancel Commit changes

11. Visit the deployed link again, the changes will be reflected in the website.



Advanced DevOps Experiment 3

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

Step 1: Go to AWS Academia in services select EC2 and create 3 instance with instance type t2.medium and names as node1, node2 and master

The screenshot shows the AWS EC2 Dashboard. The left sidebar includes sections for Services, Events, Instances (with a preview link), Capacity, Reservations, Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs), CloudShell, and Feedback. The main content area displays a table titled "Instances (6) Info" with the following data:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
node2	i-0d15c704d5359f607	Pending	t2.medium	-	View alarms +	us-east-1c	ec2-44-20
master	i-0ed4c2d736c3e438f	Running	t2.medium	2/2 checks passed	View alarms +	us-east-1c	ec2-18-20
node1	i-0ec932e19bc2d5a2f	Running	t2.medium	Initializing	View alarms +	us-east-1c	ec2-3-84-
node1	i-092007bd8be24ec14	Terminated	t2.micro	-	View alarms +	us-east-1a	-
master	i-0c96d190403326eb5	Terminated	t2.micro	-	View alarms +	us-east-1a	-
node2	i-0a539b2617389125f	Terminated	t2.micro	-	View alarms +	us-east-1a	-

A modal window titled "Select an instance" is open at the bottom, showing a list of instances: node2, master, node1, node1, master, and node2.

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

Connect to instance Info

Connect to your instance i-092007b9d8e24ec14 (node1) using any of these options

EC2 Instance Connect Session Manager SSH client EC2 serial console

⚠ Port 22 (SSH) is open to all IPv4 addresses

Port 22 (SSH) is currently open to all IPv4 addresses, indicated by **0.0.0.0/0** in the inbound rule in [your security group](#). For increased security, consider restricting access to only the EC2 Instance Connect service IP addresses for your Region: 18.206.107.24/29. [Learn more](#).

Instance ID

Connection Type

Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

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

Public IPv4 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.

Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Step 2: Select and connect each instance and run the following commands inside the console of each instance.

sudo su

```
yum install docker -v
```

systemctl start docker

docker –version

yum repolist

Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

```
[ec2-user@ip-172-31-33-243 ~]$ sudo su
[root@ip-172-31-33-243 ec2-user]# yum install docker -y
Last metadata expiration check: 0:10:44 ago on Wed Sep 18 13:13:43 2024.
Dependencies resolved.

Transaction Summary
Install 10 Packages
```

i-0a539b2617389125f (node2)

Public IPs: 107.21.35.198 Private IPs: 172.31.33.243

CloudShell Feedback

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

```
Installing : libnftnl-1.2.2-2.amzn2023.0.2.x86_64 4/10
Installing : libnftnlink-1.0.1-19.amzn2023.0.2.x86_64 5/10
Installing : libnftfilter_conntrack-1.0.8-2.amzn2023.0.2.x86_64 6/10
Installing : iptables-libs-1.8.8-3.amzn2023.0.2.x86_64 7/10
Installing : iptables-nft-1.8.8-3.amzn2023.0.2.x86_64 8/10
Running scriptlet: iptables-nft-1.8.8-3.amzn2023.0.2.x86_64 8/10
Installing : libcgroup-3.0-1.amzn2023.0.1.x86_64 9/10
Running scriptlet: docker-25.0-6-1.amzn2023.0.2.x86_64 10/10
Installing : docker-25.0-6-1.amzn2023.0.2.x86_64 10/10
Running scriptlet: docker-25.0-6-1.amzn2023.0.2.x86_64 10/10
Created symlink /etc/systemd/system/sockets.target.wants/docker.socket --> /usr/lib/systemd/system/docker.socket.

Verifying : containerd-1.7.20-1.amzn2023.0.1.x86_64 1/10
Verifying : docker-25.0-6-1.amzn2023.0.2.x86_64 2/10
Verifying : iptables-libs-1.8.8-3.amzn2023.0.2.x86_64 3/10
Verifying : iptables-nft-1.8.8-3.amzn2023.0.2.x86_64 4/10
Verifying : libcgroup-3.0-1.amzn2023.0.1.x86_64 5/10
Verifying : libnftfilter_conntrack-1.0.8-2.amzn2023.0.2.x86_64 6/10
Verifying : libnftnlink-1.0.1-19.amzn2023.0.2.x86_64 7/10
Verifying : libnftnlink-1.2.2-2.amzn2023.0.2.x86_64 8/10
Verifying : pigz-2.5-1.amzn2023.0.3.x86_64 9/10
Verifying : runc-1.1.13-1.amzn2023.0.1.x86_64 10/10

Installed:
containerd-1.7.20-1.amzn2023.0.1.x86_64 docker-25.0-6-1.amzn2023.0.2.x86_64
iptables-nft-1.8.8-3.amzn2023.0.2.x86_64 libcgroup-3.0-1.amzn2023.0.1.x86_64
libnftnlink-1.0.1-19.amzn2023.0.2.x86_64 libnftnlink-1.2.2-2.amzn2023.0.2.x86_64
runc-1.1.13-1.amzn2023.0.1.x86_64 pigz-2.5-1.amzn2023.0.3.x86_64

Complete!
[root@ip-172-31-33-243 ec2-user]# systemctl start docker
[root@ip-172-31-33-243 ec2-user]# docker --version
Docker version 25.0.5, build 5dc9bec
[root@ip-172-31-33-243 ec2-user]#
```

i-0a539b2617389125f (node2)

Public IPs: 107.21.35.198 Private IPs: 172.31.33.243

CloudShell Feedback

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

Step 3: Now, go to the following link <https://kubernetes.io/docs/setup/production-environment/tools/kubeadm/install-kubeadm/> and scroll down and select Red-Hat based distributions tab copy all the commands on by one in each console of instance.

Search this site	
Documentation	
Getting started	
Learning environment	
Production environment	
Container Runtimes	
Installing Kubernetes with deployment tools	
Bootstrapping clusters with kubeadm	
Installing kubeadm	
Troubleshooting kubeadm	
Creating a cluster with kubeadm	
Customizing components with the kubeadm API	
Options for Highly Available Topology	

Debian-based distributions Red Hat-based distributions

Without a package manager

1. Set SELinux to `permissive` mode:

These instructions are for Kubernetes 1.31.

```
# Set SELinux in permissive mode (effectively disabling it)
sudo setenforce 0
sudo sed -i 's/^SELINUX=enforcing$/SELINUX=permissive/' /etc/selinux/config
```

Caution:

- Setting SELinux in permissive mode by running `setenforce 0` and `sed ...` effectively disables it. This is required to allow containers to access the host filesystem; for example, some cluster network plugins require that. You have to do this until SELinux support is improved in the kubelet.
- You can leave SELinux enabled if you know how to configure it but it may require settings that are not supported by kubeadm.

2. Add the Kubernetes `yum` repository. The `exclude` parameter in the repository definition ensures that the packages related to Kubernetes are not upgraded upon running `yum update` as there's a special procedure that must be followed for upgrading Kubernetes. Please note that this repository have packages only for Kubernetes 1.31; for other Kubernetes minor versions, you need to change the Kubernetes minor version in the URL to match your desired minor version (you should also check that you are reading the documentation for the version of Kubernetes that you plan to install).

 Edit this page Create child page Create documentation issue Print entire section

Before you begin

Verify the MAC address and product_uuid are unique for every node

Check network adapters

Check required ports

Swap configuration

Installing a container runtime

Installing kubeadm, kubelet and kubectl

Configuring a cgroup driver

Troubleshooting

What's next

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

```
[root@ip-172-31-33-243 ec2-user]# yum repolist
repo id                                repo name
amazonlinux                             Amazon Linux 2023 repository
kernel-livelpatch                        Amazon Linux 2023 Kernel Livepatch repository
[root@ip-172-31-33-243 ec2-user]# sudo setenforce 0
sudo sed -i 's/^SELINUX=enforcing$/SELINUX=permissive/' /etc/selinux/config
[root@ip-172-31-33-243 ec2-user]# cat <>EOF | sudo tee /etc/yum.repos.d/kubernetes.repo
[kubernetes]
name=kubernetes
baseurl=https://pkgs.k8s.io/core:/stable:/v1.31/rpm/
enabled=1
gpgcheck=1
gpgkey=https://pkgs.k8s.io/core:/stable:/v1.31/rpm/repo/repodata/repomd.xml.key
exclude=kubelet kubeadm kubectl cri-tools kubernetes-cni
EOF
[kubernetes]
name=kubernetes
baseurl=https://pkgs.k8s.io/core:/stable:/v1.31/rpm/
enabled=1
gpgcheck=1
gpgkey=https://pkgs.k8s.io/core:/stable:/v1.31/rpm/repo/repodata/repomd.xml.key
exclude=kubelet kubeadm kubectl cri-tools kubernetes-cni
[root@ip-172-31-33-243 ec2-user]# sudo yum install -y kubelet kubeadm kubectl --disableexcludes=kubernetes
Kubernetes
Dependencies resolved.

Transaction Summary
  0 installed, 0 updated, 0 removed
  0 packages skipped due to local repos
  0 transactions total

Total download size: 0
Installed size: 0
Dependencies resolved.

Package          Architecture Version      Repository  Size
Installing:
  kubelet          x86_64      1.31.1-150500.1.1           kubernetes   11 M
  kubeadm         x86_64      1.31.1-150500.1.1           kubernetes   11 M
  kubectl          x86_64      1.31.1-150500.1.1           kubernetes   15 M
Installing dependencies:
  conntrack-tools x86_64      1.4.6-2.amzn2023.0.2.x86_64    amazonlinux  208 k
Dependencies resolved.

i-0a539b2617389125f (node2)
PublicIPs: 107.21.35.198 PrivateIPs: 172.31.33.243
```

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

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

```
Transaction test succeeded.
Running transaction
Preparing :
  kubelet-cni-1.5.1-150500.1.1.x86_64
Installing : cri-tools-1.31.1-150500.1.1.x86_64
Installing : libnetfilter_cttimeout-1.0.5-2.amzn2023.0.2.x86_64
Installing : libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64
Installing : libnetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64
Installing : conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64
Running scriptlet: conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64
Installing : kubelet-1.31.1-150500.1.1.x86_64
Running scriptlet: kubelet-1.31.1-150500.1.1.x86_64
Installing : kubeadm-1.31.1-150500.1.1.x86_64
Installing : kubectl-1.31.1-150500.1.1.x86_64
Running scriptlet: kubeadm-1.31.1-150500.1.1.x86_64
Verifying   : conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64
Verifying   : libnetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64
Verifying   : libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64
Verifying   : libnetfilter_cttimeout-1.0.5-2.amzn2023.0.2.x86_64
Verifying   : cri-tools-1.31.1-150500.1.1.x86_64
Verifying   : kubeadm-1.31.1-150500.1.1.x86_64
Verifying   : kubectl-1.31.1-150500.1.1.x86_64
Verifying   : kubelet-1.31.1-150500.1.1.x86_64
Verifying   : kubelet-cni-1.5.1-150500.1.1.x86_64
Complete!
[root@ip-172-31-33-243 ec2-user]# sudo systemctl enable --now kubelet
Created symlink /etc/systemd/system/multi-user.target.wants/kubelet.service → /usr/lib/systemd/system/kubelet.service.
[root@ip-172-31-33-243 ec2-user]# []
```

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

Step 4: Now, run the following command in the master instance -
kubeadm init

```
[root@ip-172-31-93-102 ec2-user]# kubeadm init
[init] Using Kubernetes version: v1.31.0
[preflight] Running pre-flight checks
[WARNING FileExisting-socat]: socat not found in system path
[WARNING FileExisting-tc]: tc not found in system path
[preflight] Pulling images required for setting up a Kubernetes cluster
[preflight] This might take a minute or two, depending on the speed of your internet connection
[preflight] You can also perform this action beforehand using 'kubeadm config images pull'
W0918 14:21:55.805697    28020 checks.go:94] detected that the sandbox image "registry.k8s.io/pause:3.8" of the container runtime is inconsistent with that used by kubeadm. It is recommended to use "registry.k8s.io/pause:3.10" as the CRI Sandbox Image.
[certs] Using certificateDir folder "/etc/kubernetes/pki"
[certs] Generating "ca" certificate and key
[certs] Generating "apiserver" certificate and key
[certs] apiserver serving cert is signed for DNS names [ip-172-31-93-102.ec2.internal kubernetes kubernetes.default kubernetes.default.svc kubernetes.default.svc.cluster.local] and IPs [10.96.0.1 172.31.93.102]
[certs] Generating "apiserver-kubelet-client" certificate and key
[certs] Generating "front-proxy-ca" certificate and key
[certs] Generating "front-proxy-client" certificate and key
[certs] Generating "etcd/ca" certificate and key
[certs] Generating "etcd/server" certificate and key
[certs] etcd/server serving cert is signed for DNS names [ip-172-31-93-102.ec2.internal localhost] and IPs [172.31.93.102 127.0.0.1 :1]
[certs] Generating "etcd/peer" certificate and key
[certs] etcd/peer serving cert is signed for DNS names [ip-172-31-93-102.ec2.internal localhost] and IPs [172.31.93.102 127.0.0.1 :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 "kubelet.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"
[control-plane] Using manifest folder "/etc/kubernetes/manifests"
```

i-0ed4c2d736c3e438f (master)
PublicIPs: 18.208.183.159 PrivateIPs: 172.31.93.102

Step 5: Now, run the following commands in master instance's console –

- a. mkdir -p \$HOME/.kube
sudo cp -i /etc/kubernetes/admin.conf \$HOME/.kube/config
sudo chown \$(id -u):\$(id -g) \$HOME/.kube/config
- b. export KUBECONFIG=/etc/kubernetes/admin.conf
- c. kubeadm join 172.31.93.102:6443 --token 6ccgvw.o10vq5f2n5d9fa42 \
--discovery-token-ca-cert-hash
sha256:1bbcc9939e895e8de0e0ddd7ec72d881a9ef3b8f51a42f3145857e54b13c3818

```
To start using your cluster, you need to run the following as a regular user:  
mkdir -p $HOME/.kube  
sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config  
sudo chown $(id -u):$(id -g) $HOME/.kube/config  
Alternatively, if you are the root user, you can run:  
export KUBECONFIG=/etc/kubernetes/admin.conf  
You should now deploy a pod network to the cluster.  
Run "kubectl apply -f [podnetwork].yaml" with one of the options listed at:  
https://kubernetes.io/docs/concepts/cluster-administration/addons/  
Then you can join any number of worker nodes by running the following on each as root:  
kubeadm join 172.31.93.102:6443 --token 6ccgvw.o10vq5f2n5d9fa42 \  
--discovery-token-ca-cert-hash sha256:1bbcc9939e895e8de0e0ddd7ec72d881a9ef3b8f51a42f3145857e54b13c3818  
(root@ip-172-31-93-102 ec2-user) # mkdir -p $HOME/.kube  
(root@ip-172-31-93-102 ec2-user) # sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config  
(root@ip-172-31-93-102 ec2-user) # sudo chown $(id -u):$(id -g) $HOME/.kube/config  
(root@ip-172-31-93-102 ec2-user) # export KUBECONFIG=/etc/kubernetes/admin.conf  
(root@ip-172-31-93-102 ec2-user) # kubeadm join 172.31.93.102:6443 --token 6ccgvw.o10vq5f2n5d9fa42 \  
--discovery-token-ca-cert-hash sha256:1bbcc9939e895e8de0e0ddd7ec72d881a9ef3b8f51a42f3145857e54b13c3818  
(preflight) Running pre-flight checks  
[WARNING FileExisting-socat]: socat not found in system path  
[WARNING FileExisting-tc]: tc not found in system path  
error execution phase preflight: [preflight] Some fatal errors occurred:  
[ERROR FileAvailable--etc-kubernetes-kubelet.conf]: /etc/kubernetes/kubelet.conf already exists  
[ERROR Port-10250]: Port 10250 is in use  
[ERROR FileAvailable--etc-kubernetes-pki-ca.crt]: /etc/kubernetes/pki/ca.crt already exists  
(preflight) If you know what you are doing, you can make a check non-fatal with '--ignore-preflight-errors=...'  
to see the stack trace of this error execute with --v=5 or higher  
(root@ip-172-31-93-102 ec2-user) # []
```

i-0ed4c2d736c3e438f (master)
PublicIPs: 18.208.183.159 PrivateIPs: 172.31.93.102

Step 6: Run this command in node1 and node2 -

```
kubeadm join 172.31.93.102:6443 --token 6ccgvw.o10vq5f2n5d9fa42 \  
--discovery-token-ca-cert-hash sha256:1bbcc9939e895e8de0e0ddd7ec72d881a9ef3b8f51a42f3145857e54b13c3818
```

```

aws Services Search [Alt+S] N. Virginia vodlabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
Installing : conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64 6/9
Running scriptlet: conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64 6/9
Installing : kubelet-1.31.1-150500.1.1.x86_64 7/9
Running scriptlet: kubelet-1.31.1-150500.1.1.x86_64 7/9
Installing : kubeadm-1.31.1-150500.1.1.x86_64 8/9
Installing : kubectl-1.31.1-150500.1.1.x86_64 9/9
Running scriptlet: kubectl-1.31.1-150500.1.1.x86_64 9/9
Verifying : conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64 1/9
Verifying : libmetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64 2/9
Verifying : libmetfilter_queue-1.0.5-2.amzn2023.0.2.x86_64 3/9
Verifying : cri-tools-1.31.1-150500.1.1.x86_64 4/9
Verifying : kubeadm-1.31.1-150500.1.1.x86_64 5/9
Verifying : kubectl-1.31.1-150500.1.1.x86_64 6/9
Verifying : kubelet-1.31.1-150500.1.1.x86_64 7/9
Verifying : kubernetes-cni-1.5.1-150500.1.1.x86_64 8/9
Verifying : libmetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64 9/9
Complete!
[root@ip-172-31-95-221 ec2-user]# sudo systemctl enable --now kubelet
Created symlink /etc/systemd/system/multi-user.target.wants/kubelet.service → /usr/lib/systemd/system/kubelet.service.
[root@ip-172-31-95-221 ec2-user]# kubeadm join 172.31.93.102:6443 --token 6ccgw.010vqf2n5d9fa42 \
--discovery-token-ca-cert-hash sha256:lbbcc9939e895e8de0e0ddd7ec72d881a9ef3b8f51a42f3145857e54b13c3818
[preflight] Running pre-flight checks
[WARNING FileExisting-socat]: socat not found in system path
[WARNING FileExisting-tc]: tc not found in system path
error execution phase preflight: couldn't validate the identity of the API Server: failed to request the cluster-info ConfigMap: Get "https://172.31.93.102:6443/api/v1/namespaces/kube-public/configmaps/cluster-info?timeout=10s": context deadline exceeded
To see the stack trace of this error execute with --v=5 or higher
[root@ip-172-31-95-221 ec2-user]# 

```

i-0d15c704d5359f607 (node2)

PublicIPs: 44.201.192.9 PrivatelPs: 172.31.95.221

```

aws Services Search [Alt+S] N. Virginia vodlabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
Installing : conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64 6/9
Running scriptlet: conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64 6/9
Installing : kubelet-1.31.1-150500.1.1.x86_64 7/9
Running scriptlet: kubelet-1.31.1-150500.1.1.x86_64 7/9
Installing : kubeadm-1.31.1-150500.1.1.x86_64 8/9
Installing : kubectl-1.31.1-150500.1.1.x86_64 9/9
Running scriptlet: kubectl-1.31.1-150500.1.1.x86_64 9/9
Verifying : conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64 1/9
Verifying : libmetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64 2/9
Verifying : libmetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64 3/9
Verifying : libmetfilter_queue-1.0.5-2.amzn2023.0.2.x86_64 4/9
Verifying : cri-tools-1.31.1-150500.1.1.x86_64 5/9
Verifying : kubeadm-1.31.1-150500.1.1.x86_64 6/9
Verifying : kubectl-1.31.1-150500.1.1.x86_64 7/9
Verifying : kubelet-1.31.1-150500.1.1.x86_64 8/9
Verifying : kubernetes-cni-1.5.1-150500.1.1.x86_64 9/9
installed:
conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64      cri-tools-1.31.1-150500.1.1.x86_64      kubeadm-1.31.1-150500.1.1.x86_64
kubectl-1.31.1-150500.1.1.x86_64                 kubelet-1.31.1-150500.1.1.x86_64      kubernetes-cni-1.5.1-150500.1.1.x86_64
libmetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64 libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64 libmetfilter_queue-1.0.5-2.amzn2023.0.2.x86_64
complete!
root@ip-172-31-94-95 ec2-user]# sudo systemctl enable --now kubelet
Created symlink /etc/systemd/system/multi-user.target.wants/kubelet.service → /usr/lib/systemd/system/kubelet.service.
root@ip-172-31-94-95 ec2-user]# kubeadm join 172.31.93.102:6443 --token 6ccgw.010vqf2n5d9fa42 \
--discovery-token-ca-cert-hash sha256:bbcc9939e895e8de0e0ddd7ec72d881a9ef3b8f51a42f3145857e54b13c3818
[preflight] Running pre-flight checks
[WARNING FileExisting-socat]: socat not found in system path
[WARNING FileExisting-tc]: tc not found in system path
error execution phase preflight: couldn't validate the identity of the API Server: failed to request the cluster-info ConfigMap: Get "https://172.31.93.102:6443/api/v1/namespaces/kube-public/configmaps/cluster-info?timeout=10s": context deadline exceeded
To see the stack trace of this error execute with --v=5 or higher
root@ip-172-31-94-95 ec2-user]# 

```

i-0ec932e19bc2d5a2f (node1)

PublicIPs: 3.84.157.220 PrivatelPs: 172.31.94.95

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

Step 7: Run the following command in master instance console -
kubectl get nodes

```

aws Services Search [Alt+S] N. Virginia vodlabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
[root@ip-172-31-81-4 ec2-user]# kubectl get nodes
NAME          STATUS    ROLES   AGE     VERSION
ip-172-31-81-4.ec2.internal   NotReady   control-plane   26m   v1.31.1
[root@ip-172-31-81-4 ec2-user]# kubectl get nodes
NAME          STATUS    ROLES   AGE     VERSION
ip-172-31-81-4.ec2.internal   NotReady   control-plane   26m   v1.31.1
ip-172-31-94-95.ec2.internal   NotReady   <none>        17s   v1.31.1
ip-172-31-95-221.ec2.internal   NotReady   <none>        13s   v1.31.1
[root@ip-172-31-81-4 ec2-user]#

```

Experiment 4

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

Step 1: Go to AWS Academia in services select EC2 and create 3 instance with instance type t2.medium and names as node1, node2 and master

The screenshot shows the AWS EC2 Instances page. The left sidebar includes options like EC2 Dashboard, EC2 Global View, Events, Console-to-Code, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity, Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, CloudShell, and Feedback. The main content area displays a table of instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
node2	i-0d15c704d5359f607	Pending	t2.medium	-	View alarms	us-east-1c	ec2-44-20-
master	i-0ed4cc2d736c3e43bf	Running	t2.medium	2/2 checks passed	View alarms	us-east-1c	ec2-18-20-
node1	i-0ec932e19bc2d5a2f	Running	t2.medium	Initializing	View alarms	us-east-1c	ec2-3-84-
node1	i-092007b9d8e24ec14	Terminated	t2.micro	-	View alarms	us-east-1a	-
master	i-0c96d190403326eb5	Terminated	t2.micro	-	View alarms	us-east-1a	-
node2	i-0a539b2617389125f	Terminated	t2.micro	-	View alarms	us-east-1a	-

Below the table, a modal window titled "Select an instance" is open, showing the same list of instances.

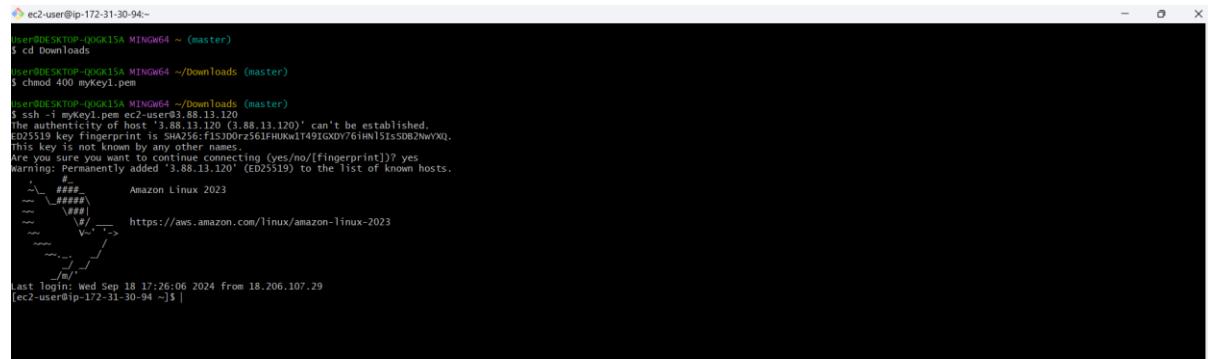
The screenshot shows the "Connect to instance" page for instance i-092007b9d8e24ec14 (node1). The top navigation bar includes Services, Search, and the AWS logo. The main content area has tabs for EC2 Instance Connect, Session Manager, SSH client, and EC2 serial console. A warning message states: "Port 22 (SSH) is open to all IPv4 addresses. Port 22 (SSH) is currently open to all IPv4 addresses, indicated by 0.0.0.0/0 in the inbound rule in your security group. For increased security, consider restricting access to only the EC2 Instance Connect service IP addresses for your Region: 18.206.107.24/29. [Learn more](#)". Below this, there are fields for Instance ID (i-092007b9d8e24ec14 (node1)), Connection Type (radio buttons for "Connect using EC2 Instance Connect" and "Connect using EC2 Instance Connect Endpoint"), Public IPv4 address (54.162.237.253), Username (ec2-user), and a Note section: "Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username." The bottom of the page includes CloudShell, Feedback, and standard footer links.

Step 2: Create a new key pair and name it as myKey1 and download as .pem file. Then, open command prompt and go to the directory where the key is downloaded and run the following command

chmod 400 myKey1.pem

```
ssh -i myKey1.pem ec2-user@3.88.13.120
```

Repeat the steps for node1, master and node2



```
ec2-user@ip-172-31-30-94:~  
user@DESKTOP-QQK15A MINGW64 ~ (master)  
$ cd Downloads  
user@DESKTOP-QQK15A MINGW64 ~/Downloads (master)  
$ chmod 400 mykey1.pem  
user@DESKTOP-QQK15A MINGW64 ~/Downloads (master)  
$ ssh -i mykey1.pem ec2-user@3.88.13.120  
The authenticity of host '3.88.13.120' (3.88.13.120) can't be established.  
ED25519 key fingerprint is SHA256:F150D7C236FMUkW1t491GxDYf6IHN15isSD82NwyQJ.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '3.88.13.120' (ED25519) to the list of known hosts.  
      .### Amazon Linux 2023  
      .###\###/  
      .### \###/  
      .###   #/  
      .###     V-- https://aws.amazon.com/linux/amazon-linux-2023  
      .###       /  
      .###     /  
      .###   /  
      .### /  
      .###/  
Last login: Wed Sep 18 17:26:06 2024 From 18.206.107.29  
[ec2-user@ip-172-31-30-94 ~]$ |
```

Step 3: Select and connect each instance and run the following commands inside the console of each instance.

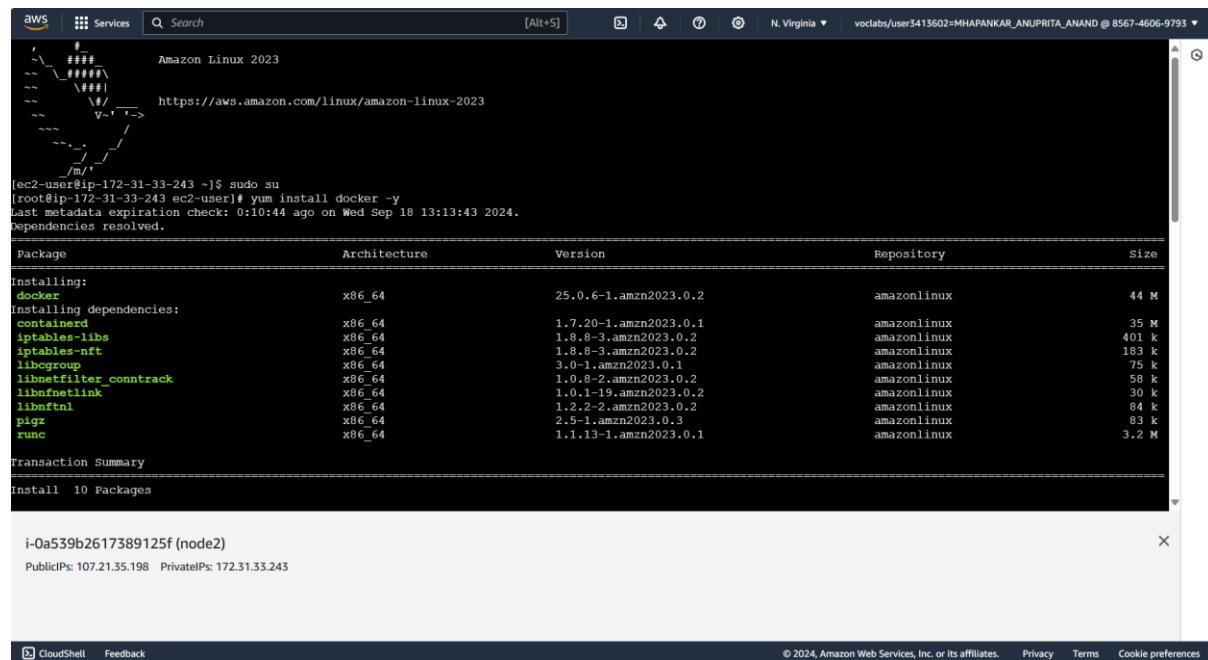
```
sudo su
```

```
yum install docker -y
```

```
systemctl start docker
```

```
docker --version
```

```
yum repolist
```



```
Amazon Linux 2023  
https://aws.amazon.com/linux/amazon-linux-2023  
[ec2-user@ip-172-31-33-243 ~]$ sudo su  
[root@ip-172-31-33-243 ec2-user]# yum install docker -y  
Last metadata expiration check: 0:10:44 ago on Wed Sep 18 13:13:43 2024.  
Dependencies resolved.  
Transaction Summary  
=====  
Install  10 Packages  


| Package                  | Architecture | Version               | Repository  | Size  |
|--------------------------|--------------|-----------------------|-------------|-------|
| Installing:              |              |                       |             |       |
| docker                   | x86_64       | 25.0.6-1.amzn2023.0.2 | amazonlinux | 44 M  |
| Installing dependencies: |              |                       |             |       |
| containerd               | x86_64       | 1.7.20-1.amzn2023.0.1 | amazonlinux | 35 M  |
| iptables-libc            | x86_64       | 1.8.8-3.amzn2023.0.2  | amazonlinux | 401 k |
| iptables-nft             | x86_64       | 1.8.8-3.amzn2023.0.2  | amazonlinux | 183 k |
| liblroup                 | x86_64       | 3.0-1.amzn2023.0.1    | amazonlinux | 75 k  |
| libnetfilter_conntrack   | x86_64       | 1.0.8-2.amzn2023.0.2  | amazonlinux | 58 k  |
| libnetfilter_ip          | x86_64       | 1.0.1-19.amzn2023.0.2 | amazonlinux | 30 k  |
| libnftnl                 | x86_64       | 1.2.2-2.amzn2023.0.2  | amazonlinux | 84 k  |
| pigr                     | x86_64       | 2.5-1.amzn2023.0.3    | amazonlinux | 83 k  |
| runc                     | x86_64       | 1.1.13-1.amzn2023.0.1 | amazonlinux | 3.2 M |

  
i-0a539b2617389125f (node2)  
PublicIPs: 107.21.35.198 PrivateIPs: 172.31.33.243  
  
CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
```

```

Installing : libnftnl-1.2.2-2.amzn2023.0.2.x86_64
Installing : libnetlink-1.0.1-19.amzn2023.0.2.x86_64
Installing : libnetfilter_conntrack-1.0.8-2.amzn2023.0.2.x86_64
Installing : iptables-libs-1.8.8-3.amzn2023.0.2.x86_64
Installing : iptables-nft-1.8.8-3.amzn2023.0.2.x86_64
Running scriptlet: iptables-nft-1.8.8-3.amzn2023.0.2.x86_64
Installing : libcgroup-3.0-1.amzn2023.0.1.x86_64
Running scriptlet: docker-25.0.6-1.amzn2023.0.2.x86_64
Installing : docker-25.0.6-1.amzn2023.0.2.x86_64
Running scriptlet: docker-25.0.6-1.amzn2023.0.2.x86_64
Created symlink /etc/systemd/system/sockets.target.wants/docker.socket → /usr/lib/systemd/system/docker.socket.

Verifying : containerd-1.7.20-1.amzn2023.0.1.x86_64
Verifying : docker-25.0.6-1.amzn2023.0.2.x86_64
Verifying : iptables-libs-1.8.8-3.amzn2023.0.2.x86_64
Verifying : iptables-nft-1.8.8-3.amzn2023.0.2.x86_64
Verifying : libcgroup-3.0-1.amzn2023.0.1.x86_64
Verifying : libnetfilter_conntrack-1.0.8-2.amzn2023.0.2.x86_64
Verifying : libnftnl-1.2.2-2.amzn2023.0.2.x86_64
Verifying : ping-2.5-1.amzn2023.0.3.x86_64
Verifying : runc-1.1.15-1.amzn2023.0.1.x86_64

Installed:
containerd-1.7.20-1.amzn2023.0.1.x86_64
iptables-libs-1.8.8-3.amzn2023.0.2.x86_64
libnetlink-1.0.1-19.amzn2023.0.2.x86_64
runc-1.1.15-1.amzn2023.0.1.x86_64

Complete!
[root@ip-172-31-33-243 ec2-user]# systemctl start docker
[root@ip-172-31-33-243 ec2-user]# docker --version
Docker version 25.0.5, build 5dc9bcc
[root@ip-172-31-33-243 ec2-user]# [REDACTED]

```

i-0a539b2617389125f (node2)
PublicIPs: 107.21.35.198 PrivateIPs: 172.31.33.243

Step 4: Now, go to the following link <https://kubernetes.io/docs/setup/production-environment/tools/kubeadm/install-kubeadm/> and scroll down and select Red-Hat based distributions tab copy all the commands on by one in each console of instance.

Documentation Kubernetes Blog Training Partners Community Case Studies Versions ▾ English ▾ Search this site

Debian-based distributions Red Hat-based distributions

Without a package manager

1. Set SELinux to `permissive` mode:

These instructions are for Kubernetes 1.31.

```
# Set SELinux in permissive mode (effectively disabling it)
sudo setenforce 0
sudo sed -i '/^SELINUX=enforcing$/ SELINUX=permissive/' /etc/selinux/config
```

Caution:

- Setting SELinux in permissive mode by running `setenforce 0` and `sed ...` effectively disables it. This is required to allow containers to access the host filesystem; for example, some cluster network plugins require that. You have to do this until SELinux support is improved in the kubelet.
- You can leave SELinux enabled if you know how to configure it but it may require settings that are not supported by kubeadm.

2. Add the Kubernetes `yum` repository. The `exclude` parameter in the repository definition ensures that the packages related to Kubernetes are not upgraded upon running `yum update` as there's a special procedure that must be followed for upgrading Kubernetes. Please note that this repository have packages only for Kubernetes 1.31; for other Kubernetes minor versions, you need to change the Kubernetes minor version in the URL to match your desired minor version (you should also check that you are reading the documentation for the version of Kubernetes that you plan to install).

Before you begin
Verify the MAC address and product_uuid are unique for every node
Check network adapters
Check required ports
Swap configuration
Installing a container runtime
Installing kubeadm, kubelet and kubectl
Configuring a cgroup driver
Troubleshooting
What's next

```

aws Services Search [Alt+S] N. Virginia vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
[root@ip-172-31-33-243 ec2-user]# yum repolist
repo id repo name
amazonlinux Amazon Linux 2023 repository
kernel-livelpatch Amazon Linux 2023 Kernel Livepatch repository
[root@ip-172-31-33-243 ec2-user]# sudo setenforce 0
sudo sed -i '/^SELINUX=enforcing$/SELINUX=permissive/' /etc/selinux/config
[root@ip-172-31-33-243 ec2-user]# cat <<EOF | sudo tee /etc/yum.repos.d/kubernetes.repo
[kubernetes]
name=Kubernetes
baseurl=https://pkgs.k8s.io/core/stable:v1.31/rpm/
enabled=1
gpgcheck=1
gpgkey=https://pkgs.k8s.io/core/stable:v1.31/rpm/repo/repomd.xml.key
exclude=kubelet kubeadm kubectl cri-tools kubernetes-cni
EOF
(kubernetes)
name=Kubernetes
baseurl=https://pkgs.k8s.io/core/stable:v1.31/rpm/
enabled=1
gpgcheck=1
gpgkey=https://pkgs.k8s.io/core/stable:v1.31/rpm/repo/repomd.xml.key
exclude=kubelet kubeadm kubectl cri-tools kubernetes-cni
[root@ip-172-31-33-243 ec2-user]# sudo yum install -y kubelet kubeadm kubectl --disableexcludes=kubernetes
Dependencies resolved.
54 kB/s | 9.4 kB 00:00
[Package Architecture Version Repository Size]
Installing:
kubeadm x86_64 1.31.1-150500.1.1 kubernetes 11 M
kubectl x86_64 1.31.1-150500.1.1 kubernetes 11 M
kubelet x86_64 1.31.1-150500.1.1 kubernetes 15 M
Installing dependencies:
comctrack-tools x86_64 1.4.6-2.amzn2023.0.2 amazonlinux 208 k
i-0a539b2617389125f (node2)
PublicIPs: 107.21.35.198 PrivateIPs: 172.31.33.243

```

```

CloudShell Feedback © 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 ▾
Transaction test succeeded.
Running transaction
Preparing : 1/1
Installing : kubernetes-cni-1.5.1-150500.1.1.x86_64 1/9
              cri-tools-1.31.1-150500.1.1.x86_64 2/9
              libnetfilter_queue-1.0.5-2.amzn2023.0.2.x86_64 3/9
              libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64 4/9
              libnetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64 5/9
              comctrack-tools-1.4.6-2.amzn2023.0.2.x86_64 6/9
Running scriptlet: comctrack-tools-1.4.6-2.amzn2023.0.2.x86_64 6/9
Installing : kubelet-1.31.1-150500.1.1.x86_64 7/9
Running scriptlet: kubelet-1.31.1-150500.1.1.x86_64 7/9
Installing : kubeadm-1.31.1-150500.1.1.x86_64 8/9
Installing : kubectl-1.31.1-150500.1.1.x86_64 9/9
Running scriptlet: kubectl-1.31.1-150500.1.1.x86_64 9/9
Verifying : comctrack-tools-1.4.6-2.amzn2023.0.2.x86_64 1/9
Verifying : libnetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64 2/9
Verifying : libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64 3/9
Verifying : libnetfilter_queue-1.0.5-2.amzn2023.0.2.x86_64 4/9
Verifying : cri-tools-1.31.1-150500.1.1.x86_64 5/9
Verifying : kubeadm-1.31.1-150500.1.1.x86_64 6/9
Verifying : kubectl-1.31.1-150500.1.1.x86_64 7/9
Verifying : kubelet-1.31.1-150500.1.1.x86_64 8/9
Verifying : kubernetes-cni-1.5.1-150500.1.1.x86_64 9/9
Installed:
comctrack-tools-1.4.6-2.amzn2023.0.2.x86_64      cri-tools-1.31.1-150500.1.1.x86_64      kubeadm-1.31.1-150500.1.1.x86_64
kubectl-1.31.1-150500.1.1.x86_64                kubelet-1.31.1-150500.1.1.x86_64      kubernetes-cni-1.5.1-150500.1.1.x86_64
libnetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64 libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64  libnetfilter_queue-1.0.5-2.amzn2023.0.2.x86_64
Complete!
[root@ip-172-31-33-243 ec2-user]# sudo systemctl enable --now kubelet
Created symlink /etc/systemd/system/multi-user.target.wants/kubelet.service → /usr/lib/systemd/system/kubelet.service.
[root@ip-172-31-33-243 ec2-user]# []
i-0a539b2617389125f (node2)
PublicIPs: 107.21.35.198 PrivateIPs: 172.31.33.243

```

Step 5: Now, run the following command in the master instance -
kubeadm init

```

[root@ip-172-31-93-102 ec2-user]# kubeadm init
[init] Using Kubernetes version: v1.31.0
[preflight] Running pre-flight checks
  [WARNING FileExisting-socat]: socat not found in system path
  [WARNING FileExisting-tc]: tc not found in system path
[preflight] Pulling images required for setting up a Kubernetes cluster
[preflight] This might take a minute or two, depending on the speed of your internet connection
[preflight] You can also perform this action beforehand using 'kubeadm config images pull'
W0918 14:21:55.805697 28020 checks.go:846] detected that the sandbox image "registry.k8s.io/pause:3.8" of the container runtime is inconsistent with that used by kubeadm. It is recommended to use "registry.k8s.io/pause:3.10" as the CRI sandbox image.
[certs] Using certificatebir folder "/etc/kubernetes/pki"
[certs] Generating "ca" certificate and key
[certs] Generating "apiserver" certificate and key
[certs] apiserver serving cert is signed for DNS names [ip-172-31-93-102.ec2.internal kubernetes kubernetes.default kubernetes.default.svc kubernetes.default.svc.cluster.local] and IPs [10.96.0.1 172.31.93.102]
[certs] Generating "apiserver-kubelet-client" certificate and key
[certs] Generating "front-proxy-ca" certificate and key
[certs] Generating "front-proxy-client" certificate and key
[certs] Generating "etcd/ca" certificate and key
[certs] Generating "etcd/server" certificate and key
[certs] etcd/server serving cert is signed for DNS names [ip-172-31-93-102.ec2.internal localhost] and IPs [172.31.93.102 127.0.0.1 ::1]
[certs] Generating "etcd/peer" certificate and key
[certs] etcd/peer serving cert is signed for DNS names [ip-172-31-93-102.ec2.internal localhost] and IPs [172.31.93.102 127.0.0.1 ::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 "kubelet.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"
[control-plane] Using manifest folder "/etc/kubernetes/manifests"

i-0ed4c2d736c3e438f (master)
PublicIPs: 18.208.183.159 PrivateIPs: 172.31.93.102

```

Step 6: Now, run the following commands in master instance's console –

- `mkdir -p $HOME/.kube`
`sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config`
`sudo chown $(id -u):$(id -g) $HOME/.kube/config`
- `export KUBECONFIG=/etc/kubernetes/admin.conf`
- `kubeadm join 172.31.93.102:6443 --token 6ccgvw.o10vq5f2n5d9fa42 \`
`--discovery-token-ca-cert-hash sha256:1bbcc9939e895e8de0e0ddd7ec72d881a9ef3b8f51a42f3145857e54b13c3818`

```

To start using your cluster, you need to run the following as a regular user:
mkdir -p $HOME/.kube
sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
sudo chown $(id -u):$(id -g) $HOME/.kube/config

Alternatively, if you are the root user, you can run:
export KUBECONFIG=/etc/kubernetes/admin.conf

You should now deploy a pod network to the cluster.
Run "kubectl apply -f [podnetwork].yaml" with one of the options listed at:
  https://kubernetes.io/docs/concepts/cluster-administration/addons/

Then you can join any number of worker nodes by running the following on each as root:
kubeadm join 172.31.93.102:6443 --token 6ccgvw.o10vq5f2n5d9fa42 \
  --discovery-token-ca-cert-hash sha256:1bbcc9939e895e8de0e0ddd7ec72d881a9ef3b8f51a42f3145857e54b13c3818
[root@ip-172-31-93-102 ec2-user]# mkdir -p $HOME/.kube
sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
sudo chown $(id -u):$(id -g) $HOME/.kube/config
[root@ip-172-31-93-102 ec2-user]# export KUBECONFIG=/etc/kubernetes/admin.conf
[root@ip-172-31-93-102 ec2-user]# kubeadm join 172.31.93.102:6443 --token 6ccgvw.o10vq5f2n5d9fa42 \
  --discovery-token-ca-cert-hash sha256:1bbcc9939e895e8de0e0ddd7ec72d881a9ef3b8f51a42f3145857e54b13c3818
[preflight] Running pre-flight checks
  [WARNING FileExisting-socat]: socat not found in system path
  [WARNING FileExisting-tc]: tc not found in system path
error execution phase preflight: [preflight] Some fatal errors occurred:
  [ERROR FileAvailable--etc-kubernetes-kubelet.conf]: /etc/kubernetes/kubelet.conf already exists
  [ERROR Port-10250]: Port 10250 is in use
  [ERROR FileAvailable--etc-kubernetes-pki-ca.crt]: /etc/kubernetes/pki/ca.crt already exists
[preflight] If you know what you are doing, you can make a check non-fatal with '--ignore-preflight-errors=...'
To see the stack trace of this error execute with --v=5 or higher
[root@ip-172-31-93-102 ec2-user]# 

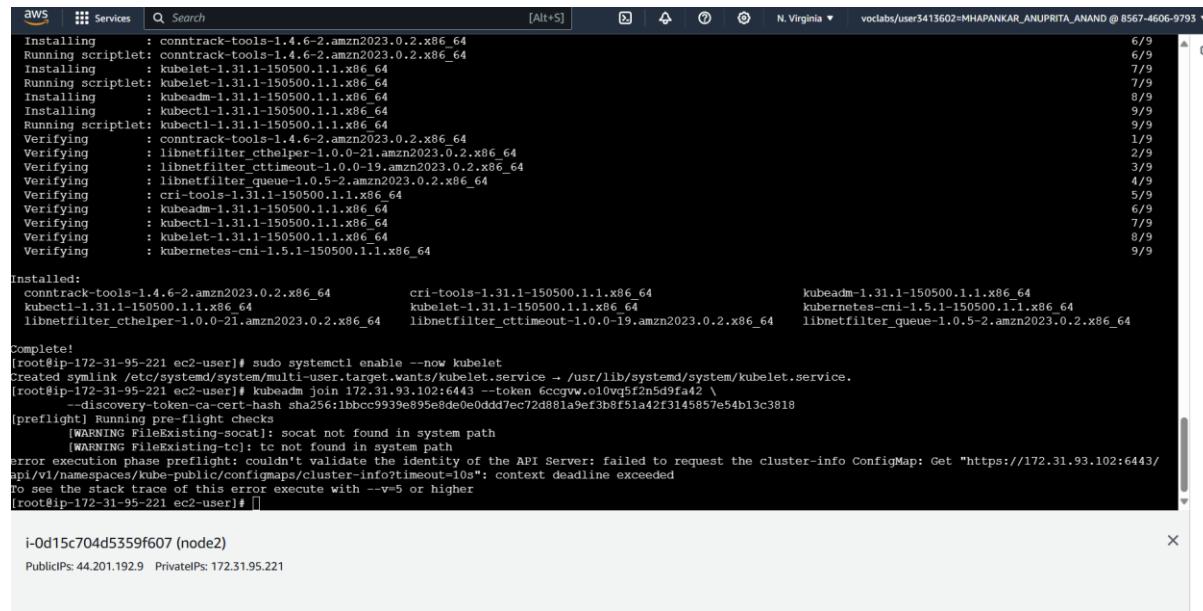
i-0ed4c2d736c3e438f (master)
PublicIPs: 18.208.183.159 PrivateIPs: 172.31.93.102

```

Step 7: Run this command in node1 and node2 -

`kubeadm join 172.31.93.102:6443 --token 6ccgvw.o10vq5f2n5d9fa42 \`

--discovery-token-ca-cert-hash
sha256:1bbcc9939e895e8de0e0ddd7ec72d881a9ef3b8f51a42f3145857e54b13c3818



```

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

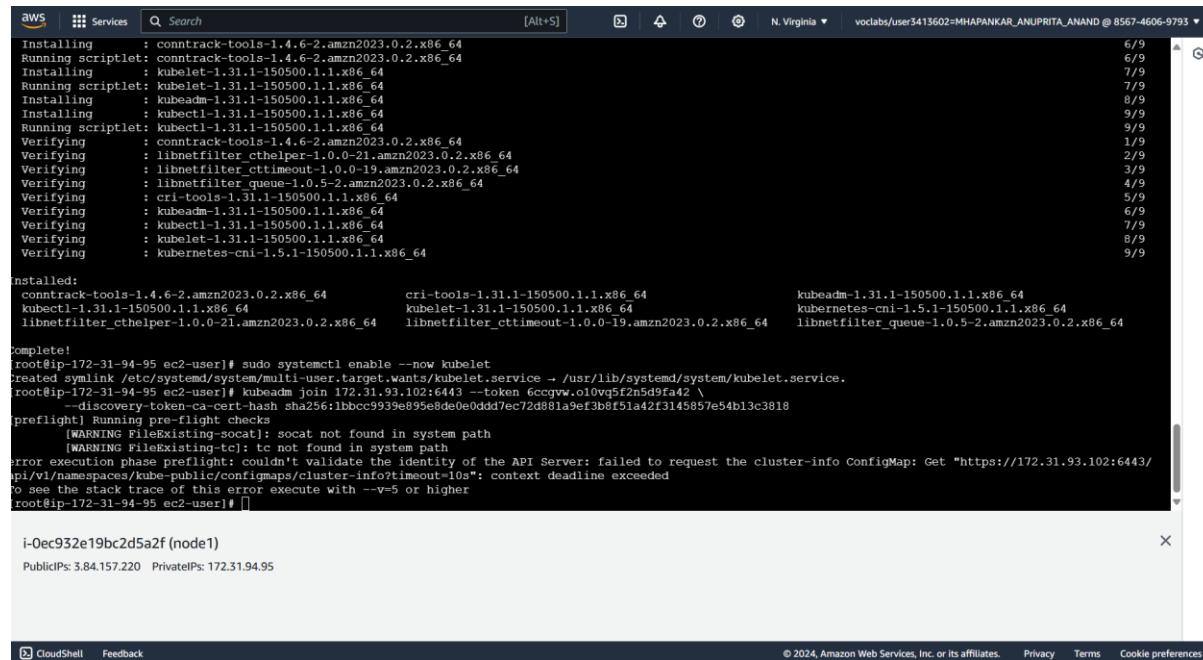
Installing : conctrack-tools-1.4.6-2.amzn2023.0.2.x86_64          6/9
Running scriptlet: conctrack-tools-1.4.6-2.amzn2023.0.2.x86_64  6/9
Installing : kubelet-1.31.1-150500.1.1.x86_64                  7/9
Running scriptlet: kubelet-1.31.1-150500.1.1.x86_64          7/9
Installing : kubeadm-1.31.1-150500.1.1.x86_64                8/9
Installing : kubectl-1.31.1-150500.1.1.x86_64                 9/9
Running scriptlet: kubectl-1.31.1-150500.1.1.x86_64          9/9
Verifying   : conctrack-tools-1.4.6-2.amzn2023.0.2.x86_64      1/9
Verifying   : libnetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64 2/9
Verifying   : libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64 3/9
Verifying   : libnetfilter_ctqueue-1.0.5-2.amzn2023.0.2.x86_64   4/9
Verifying   : cri-tools-1.31.1-150500.1.1.x86_64              5/9
Verifying   : kubeadm-1.31.1-150500.1.1.x86_64                6/9
Verifying   : kubectl-1.31.1-150500.1.1.x86_64                 7/9
Verifying   : kubelet-1.31.1-150500.1.1.x86_64                8/9
Verifying   : kubernetes-cni-1.5.1-150500.1.1.x86_64          9/9

Installed:
conctrack-tools-1.4.6-2.amzn2023.0.2.x86_64      cri-tools-1.31.1-150500.1.1.x86_64      kubeadm-1.31.1-150500.1.1.x86_64
kubectl-1.31.1-150500.1.1.x86_64                 kubelet-1.31.1-150500.1.1.x86_64       kubernetes-cni-1.5.1-150500.1.1.x86_64
libnetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64 libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64 libnetfilter_ctqueue-1.0.5-2.amzn2023.0.2.x86_64

complete!
[root@ip-172-31-95-221 ec2-user]# sudo systemctl enable --now kubelet
Created symlink /etc/systemd/system/multi-user.target.wants/kubelet.service → /usr/lib/systemd/system/kubelet.service.
[root@ip-172-31-95-221 ec2-user]# kubeadm join 172.31.93.102:6443 --token 6ccgw.o10vg5f2n5df9fa42 \
--discovery-token-ca-cert-hash sha256:1bbcc9939e895e8de0e0ddd7ec72d881a9ef3b8f51a42f3145857e54b13c3818
[preflight] Running pre-flight checks
[WARNING FileExisting-socat]: socat not found in system path
[WARNING FileExisting-tc]: tc not found in system path
error execution phase preflight: couldn't validate the identity of the API Server: failed to request the cluster-info ConfigMap: Get "https://172.31.93.102:6443/api/v1/namespaces/kube-public/configmaps/cluster-info?timeout=10s": context deadline exceeded
To see the stack trace of this error execute with --v=5 or higher
[root@ip-172-31-95-221 ec2-user]# []

i-0d15c704d5359f607 (node2)
PublicIPs: 44.201.192.9 PrivateIPs: 172.31.95.221

```



```

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

Installing : conctrack-tools-1.4.6-2.amzn2023.0.2.x86_64          6/9
Running scriptlet: conctrack-tools-1.4.6-2.amzn2023.0.2.x86_64  6/9
Installing : kubelet-1.31.1-150500.1.1.x86_64                  7/9
Running scriptlet: kubelet-1.31.1-150500.1.1.x86_64          7/9
Installing : kubeadm-1.31.1-150500.1.1.x86_64                8/9
Installing : kubectl-1.31.1-150500.1.1.x86_64                 9/9
Running scriptlet: kubectl-1.31.1-150500.1.1.x86_64          9/9
Verifying   : conctrack-tools-1.4.6-2.amzn2023.0.2.x86_64      1/9
Verifying   : libnetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64 2/9
Verifying   : libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64 3/9
Verifying   : libnetfilter_ctqueue-1.0.5-2.amzn2023.0.2.x86_64   4/9
Verifying   : cri-tools-1.31.1-150500.1.1.x86_64              5/9
Verifying   : kubeadm-1.31.1-150500.1.1.x86_64                6/9
Verifying   : kubectl-1.31.1-150500.1.1.x86_64                 7/9
Verifying   : kubelet-1.31.1-150500.1.1.x86_64                8/9
Verifying   : kubernetes-cni-1.5.1-150500.1.1.x86_64          9/9

Installed:
conctrack-tools-1.4.6-2.amzn2023.0.2.x86_64      cri-tools-1.31.1-150500.1.1.x86_64      kubeadm-1.31.1-150500.1.1.x86_64
kubelet-1.31.1-150500.1.1.x86_64                 kubelet-1.31.1-150500.1.1.x86_64       kubernetes-cni-1.5.1-150500.1.1.x86_64
libnetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64 libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64 libnetfilter_ctqueue-1.0.5-2.amzn2023.0.2.x86_64

complete!
[root@ip-172-31-94-95 ec2-user]# sudo systemctl enable --now kubelet
Created symlink /etc/systemd/system/multi-user.target.wants/kubelet.service → /usr/lib/systemd/system/kubelet.service.
[root@ip-172-31-94-95 ec2-user]# kubeadm join 172.31.93.102:6443 --token 6ccgw.o10vg5f2n5df9fa42 \
--discovery-token-ca-cert-hash sha256:i0ec932e19bc2d5a2f
[preflight] Running pre-flight checks
[WARNING FileExisting-socat]: socat not found in system path
[WARNING FileExisting-tc]: tc not found in system path
error execution phase preflight: couldn't validate the identity of the API Server: failed to request the cluster-info ConfigMap: Get "https://172.31.93.102:6443/api/v1/namespaces/kube-public/configmaps/cluster-info?timeout=10s": context deadline exceeded
To see the stack trace of this error execute with --v=5 or higher
[root@ip-172-31-94-95 ec2-user]# []

i-0ec932e19bc2d5a2f (node1)
PublicIPs: 3.84.157.220 PrivateIPs: 172.31.94.95

```

Step 8: Run the following command in master instance console -
kubectl get nodes

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

```
RWS Services Search [Alt+S] N. Virginia variable/user/S41560-MHAPANKAR_ANUPRITA_ANAND@8567-4B06-9793

[root@ip-172-31-81-4 ec2-user]# kubectl get nodes
NAME          STATUS    ROLES     AGE      VERSION
ip-172-31-81-4.ec2.internal   NotReady   control-plane   26m   v1.31.1
[root@ip-172-31-81-4 ec2-user]# kubectl get nodes
NAME          STATUS    ROLES     AGE      VERSION
ip-172-31-81-4.ec2.internal   NotReady   control-plane   26m   v1.31.1
ip-172-31-94-95.ec2.internal NotReady   <none>    179s  v1.31.1
ip-172-31-95-21.ec2.internal  NotReady   <none>    135s  v1.31.1
[root@ip-172-31-81-4 ec2-user]#
```

Step 9: Once the cluster is set up and running, deploy an Nginx application:

```
kubectl apply -f https://k8s.io/examples/application/deployment.yaml
```

Forward the Nginx service to your localhost so that you can access it using the following command

```
kubectl port-forward deployment/nginx-deployment 8080:80
```

```
deployment.yaml x
C:\Users\...\Downloads> deployment.yaml
1 apiVersion: apps/v1
2 kind: Deployment
3 metadata:
4   name: nginx-deployment
5 spec:
6   selector:
7     matchLabels:
8       app: nginx
9   replicas: 2 # tells deployment to run 2 pods matching the template
10  template:
11    metadata:
12      labels:
13        app: nginx
14    spec:
15      containers:
16        - name: nginx
17          image: nginx:1.14.2
18          ports:
19            - containerPort: 80
20
```

Step 10: In a new terminal of Git Bash, run:

```
curl --head http://127.0.0.1:8080
```

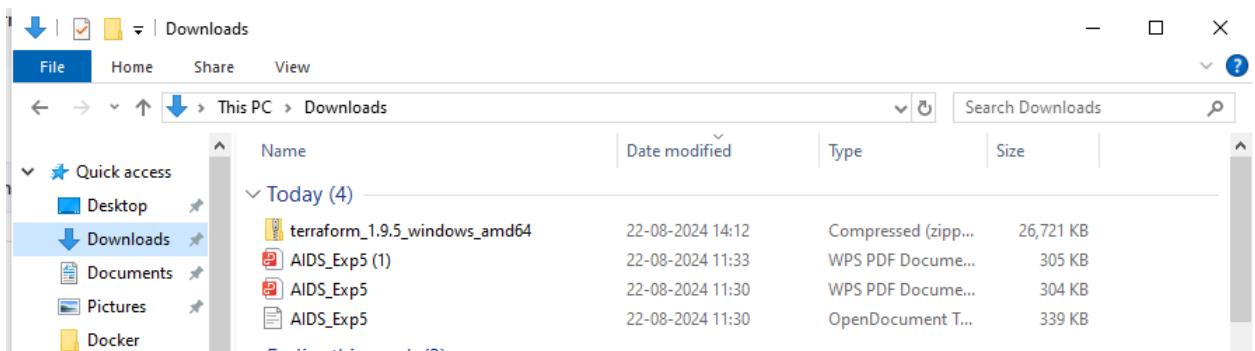
Step 11: The website is live

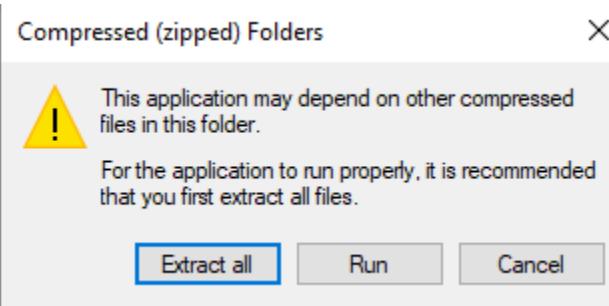
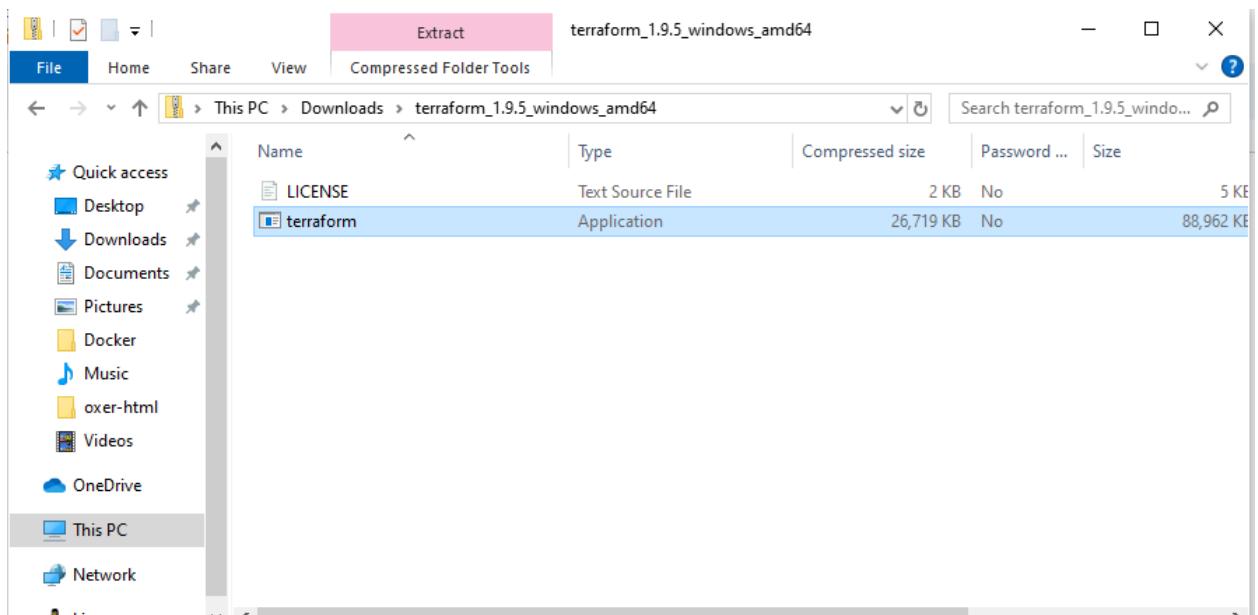


Experiment 5 : Terraform

Aim : Installation and Configuration of Terraform in Windows

The screenshot shows the HashiCorp Terraform website at <https://developer.hashicorp.com/terraform/install>. The left sidebar has a 'Windows' category selected. The main content area shows 'Binary download' options for 386 and AMD64 architectures, both at version 1.9.5. Below this, the 'Linux' section shows package manager links for Ubuntu/Debian, CentOS/RHEL, Fedora, Amazon Linux, and Homebrew. A terminal window displays the command to install Terraform on Ubuntu/Debian.





X

←  Extract Compressed (Zipped) Folders

Select a Destination and Extract Files

Files will be extracted to this folder:

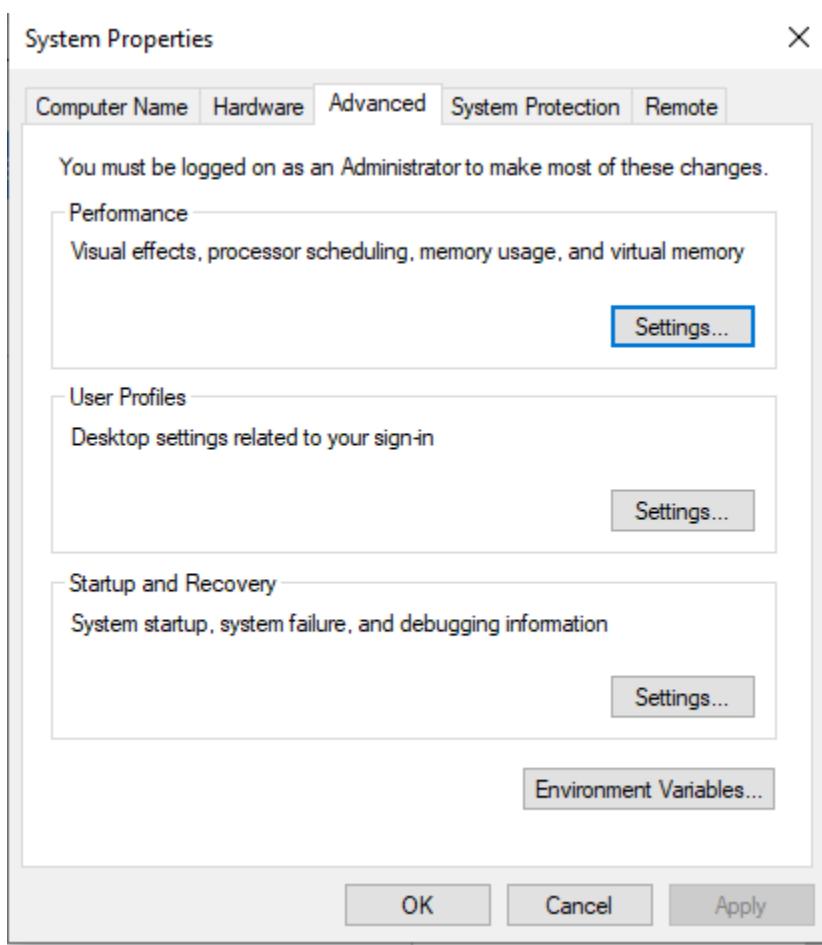
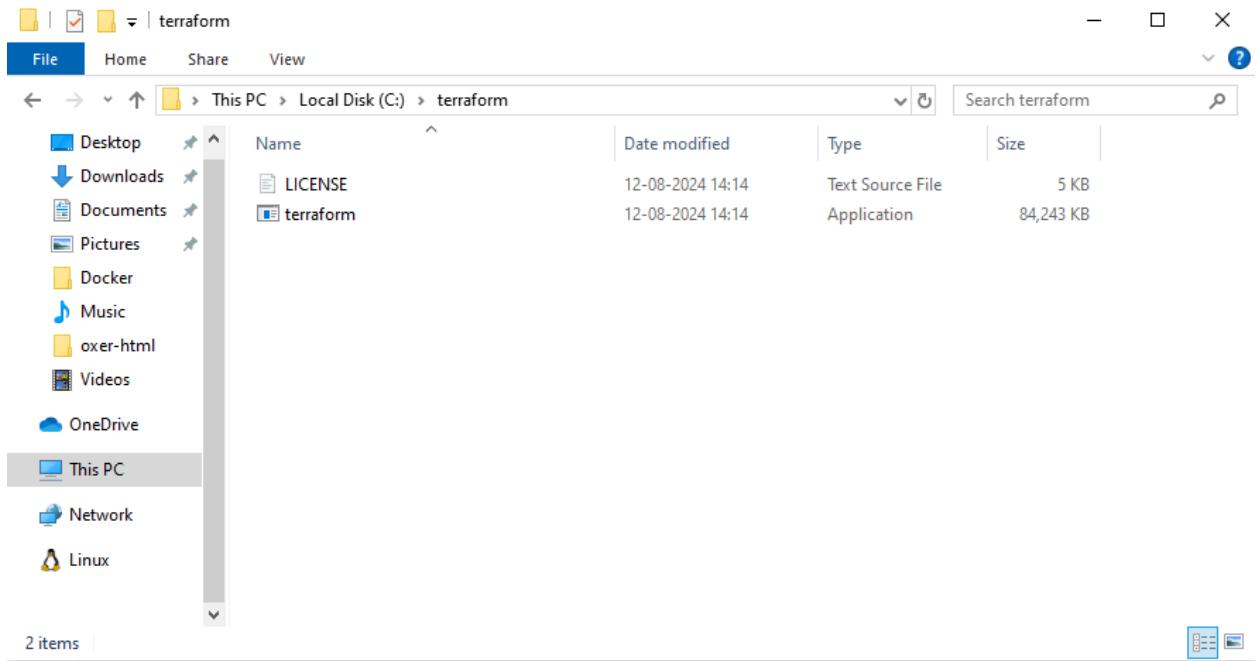
C:\Users\INFT\Downloads\terraform_1.9.5_windows_amd64

[Browse...](#)

Show extracted files when complete

[Extract](#)

[Cancel](#)



User variables for INFT	
Variable	Value
OneDrive	C:\Users\INFT\OneDrive
Path	C:\Users\INFT\AppData\Local\Microsoft\WindowsApps;C:\Users\I...
TEMP	C:\Users\INFT\AppData\Local\Temp
TMP	C:\Users\INFT\AppData\Local\Temp

New... Edit... Delete

System variables	
Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
NUMBER_OF_PROCESSORS	8
OS	Windows_NT
Path	C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\Win...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	AMD64

New... Edit... Delete

OK Cancel

Edit User Variable

Variable name:	<input type="text" value="Path"/>
Variable value:	<input type="text" value="C:\terraform"/>
<input type="button" value="Browse Directory..."/>	<input type="button" value="Browse File..."/>
	<input type="button" value="OK"/> <input type="button" value="Cancel"/>

Administrator: Windows PowerShell

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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> terraform
Usage: terraform [global options] <subcommand> [args]

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

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

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

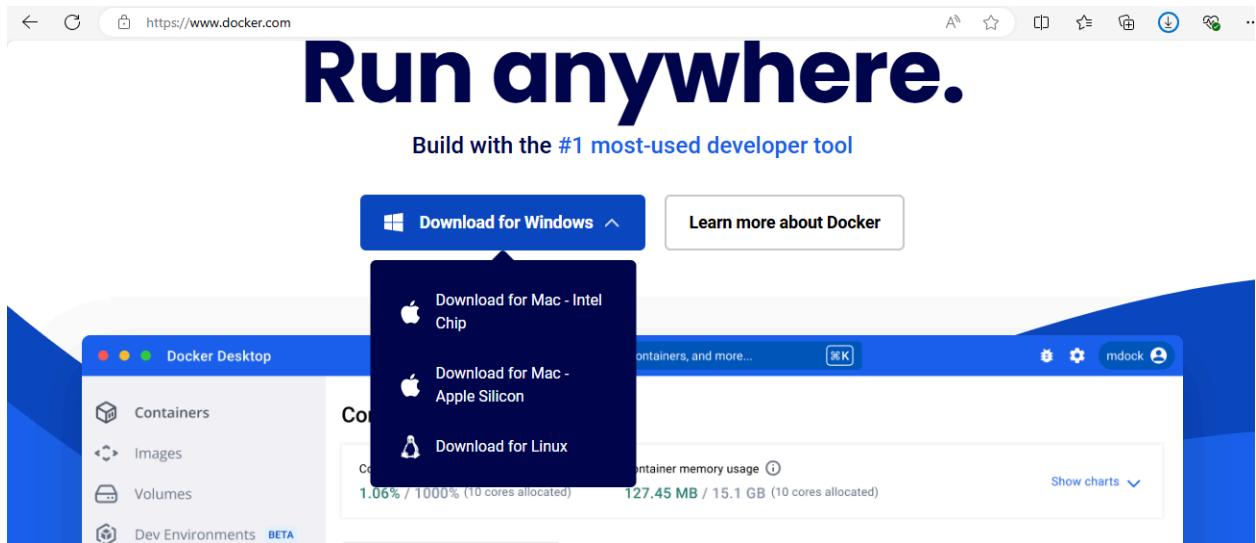
Global options (use these before the subcommand, if any):
  -chdir=DIR  Switch to a different working directory before executing the
              given subcommand.
  -help       Show this help output, or the help for a specified subcommand.
  -version    An alias for the "version" subcommand.
PS C:\Windows\system32>
```

Experiment 6

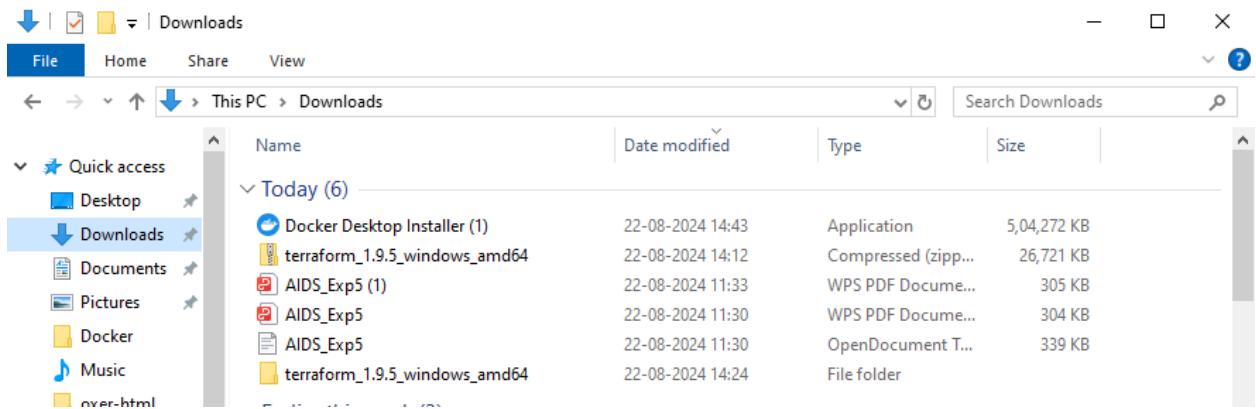
Aim:

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

Step 1: Download Docker from www.docker.com



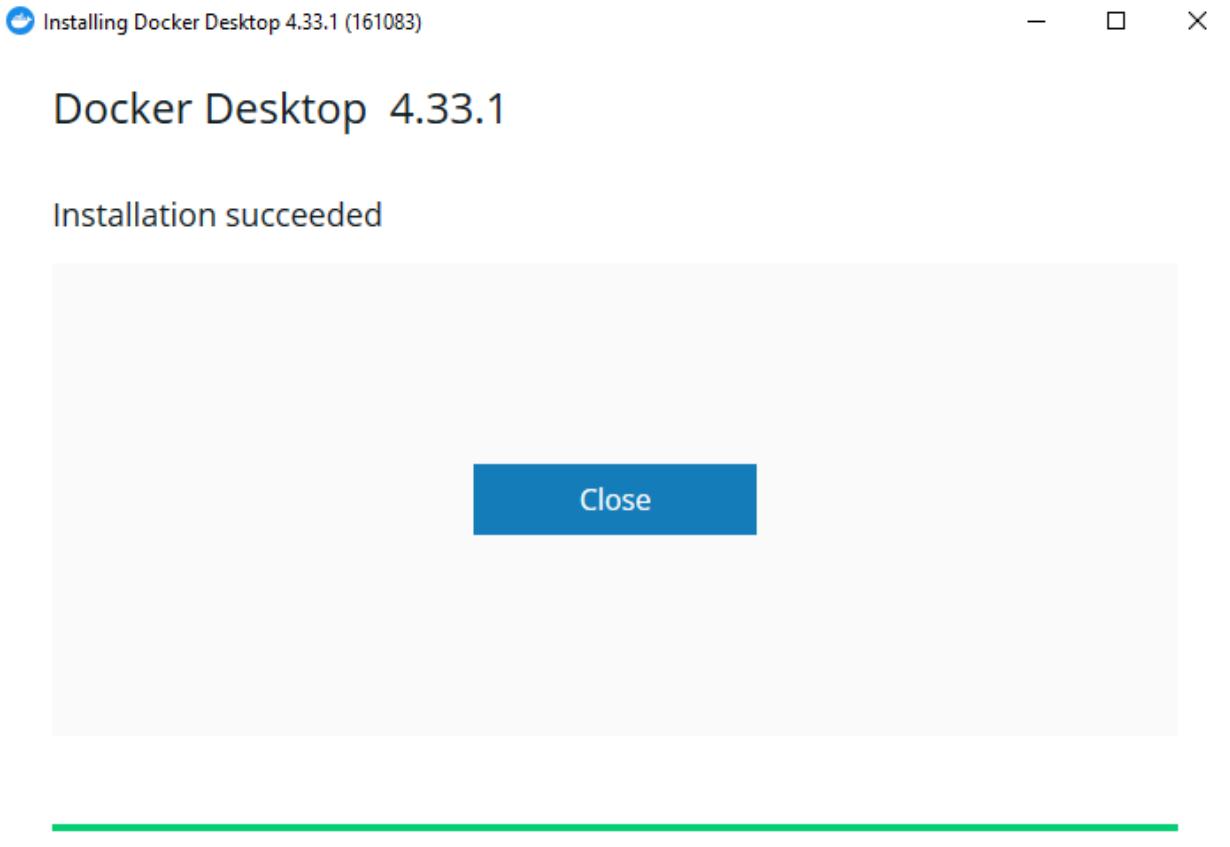
Step 2: The Docker is successfully downloaded. Now, run the docker installer and complete the installation.



Docker Desktop 4.33.1

Unpacking files...

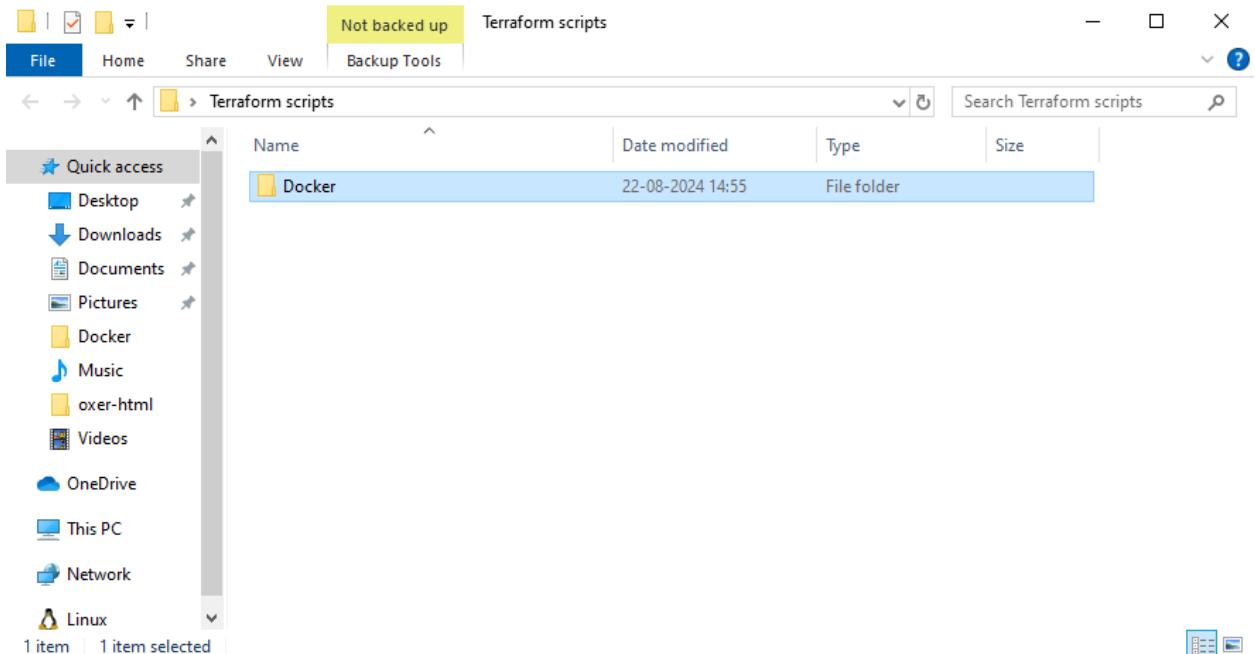
```
Unpacking file: resources/docker-desktop.iso
Unpacking file: resources/ddvp.ico
Unpacking file: resources/config-options.json
Unpacking file: resources/componentsVersion.json
Unpacking file: resources/bin/docker-compose
Unpacking file: resources/bin/docker
Unpacking file: resources/.gitignore
Unpacking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



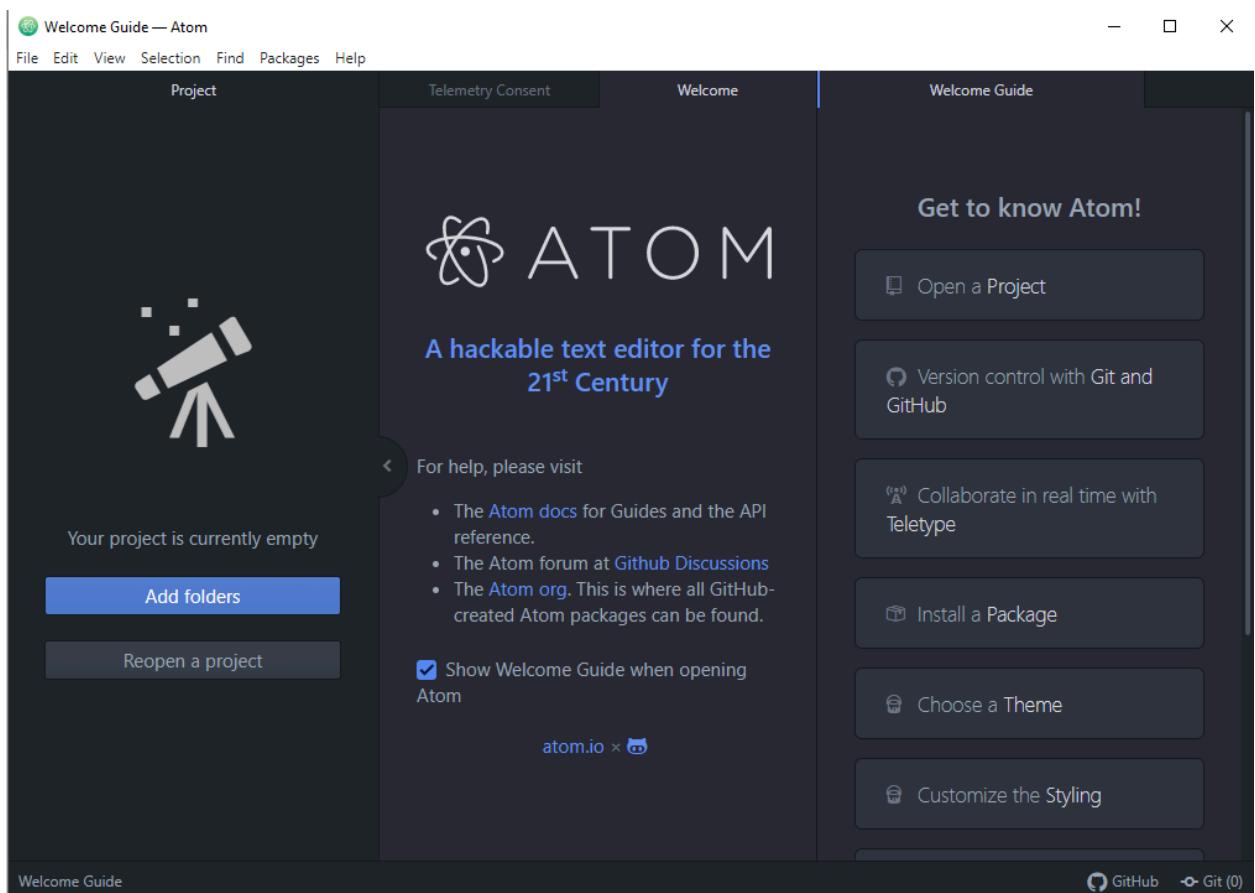
Step 3: Open Command Prompt and run as administrator. Enter the command docker –version, to check whether the docker is successfully installed.

A screenshot of a Windows Command Prompt window titled "Command Prompt". The window shows the output of the "docker --version" command, which displays "Docker version 27.1.1, build 6312585". Below this, the "Usage" and "Common Commands" sections of the Docker documentation are displayed. The "Common Commands" section lists commands like "run", "exec", "ps", "build", "pull", "push", "images", "login", "logout", "search", "version", and "info" with their descriptions. The "Management Commands" section lists "builder", "buildx*", "compose*", "container", and "context" with their descriptions. The window has a standard Windows title bar with minimize, maximize, and close buttons.

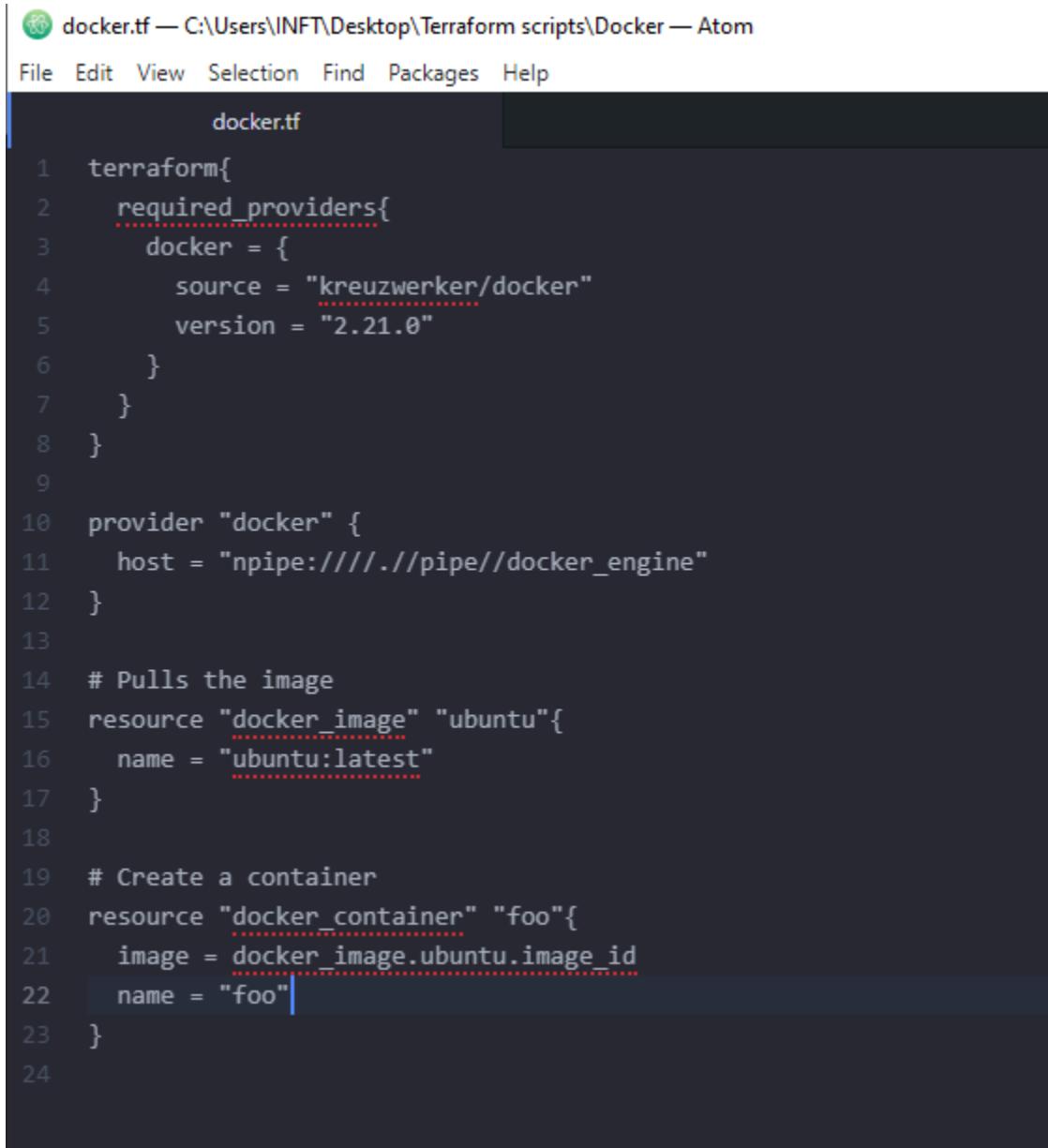
Step 4: Create a folder Terraform_scripts and inside it create a folder named Docker.



Step 5: Download Atom Editor.



Step 6: Run the following script in the Atom Editor



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

```
1 terraform{  
2   required_providers{  
3     docker = {  
4       source = "kreuzwerker/docker"  
5       version = "2.21.0"  
6     }  
7   }  
8 }  
9  
10 provider "docker" {  
11   host = "npipe://./pipe/docker_engine"  
12 }  
13  
14 # Pulls the image  
15 resource "docker_image" "ubuntu"{  
16   name = "ubuntu:latest"  
17 }  
18  
19 # Create a container  
20 resource "docker_container" "foo"{  
21   image = docker_image.ubuntu.image_id  
22   name = "foo"  
23 }  
24
```

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

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

Terraform has been successfully initialized!

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

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
PS C:\Users\INFT\Desktop\Terraform_scripts\Docker> terraform plan

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

Terraform will perform the following actions:

# docker_container.foo will be created
+ resource "docker_container" "foo" {
  + attach          = false
  + bridge          = (known after apply)
  + command         = (known after apply)
  + container_logs = (known after apply)
  + entrypoint      = (known after apply)
  + env             = (known after apply)
  + exit_code       = (known after apply)
  + gateway         = (known after apply)
  + hostname        = (known after apply)
  + id              = (known after apply)
  + image           = (known after apply)
  + init            = (known after apply)
  + ip_address      = (known after apply)
  + ip_prefix_length = (known after apply)
  + ipc_mode        = (known after apply)
```

```
Windows PowerShell
Note: You didn't use the -out option to save this plan, so Terraform can't guarantee to take exactly these actions if you run "terraform apply" now.
PS C:\Users\INFT\Desktop\Terraform_scripts\Docker> terraform apply

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

Terraform will perform the following actions:

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

    + healthcheck (known after apply)

    + labels (known after apply)
}

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

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

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

Enter a value: yes

docker_image.ubuntu: Creating...
docker_image.ubuntu: Still creating... [10s elapsed]
docker_image.ubuntu: Creation complete after 11s [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598@ubuntu:latest]
docker_container.foo: Creating...

Error: container exited immediately

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

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

```
PS C:\Users\INFT\Desktop\Terraform_scripts\Docker> terraform destroy
docker_image.ubuntu: Refreshing state... [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]

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

Terraform will perform the following actions:

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

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

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

Enter a value: yes

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

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

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

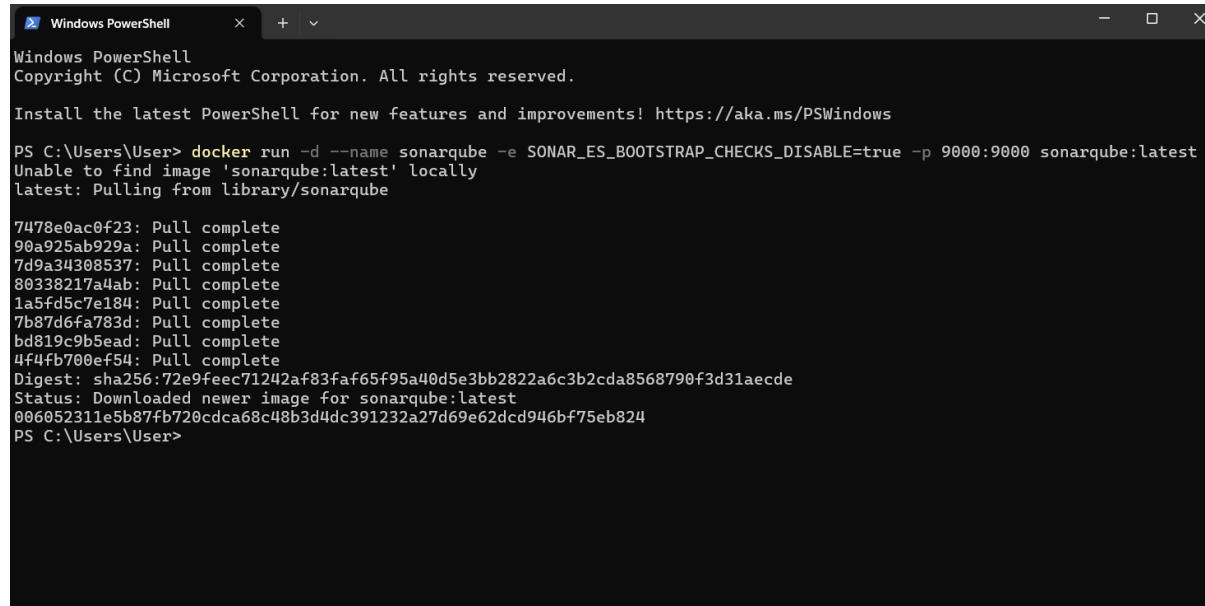
EXPERIMENT 7

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
```

WARNING: Run the following command only once



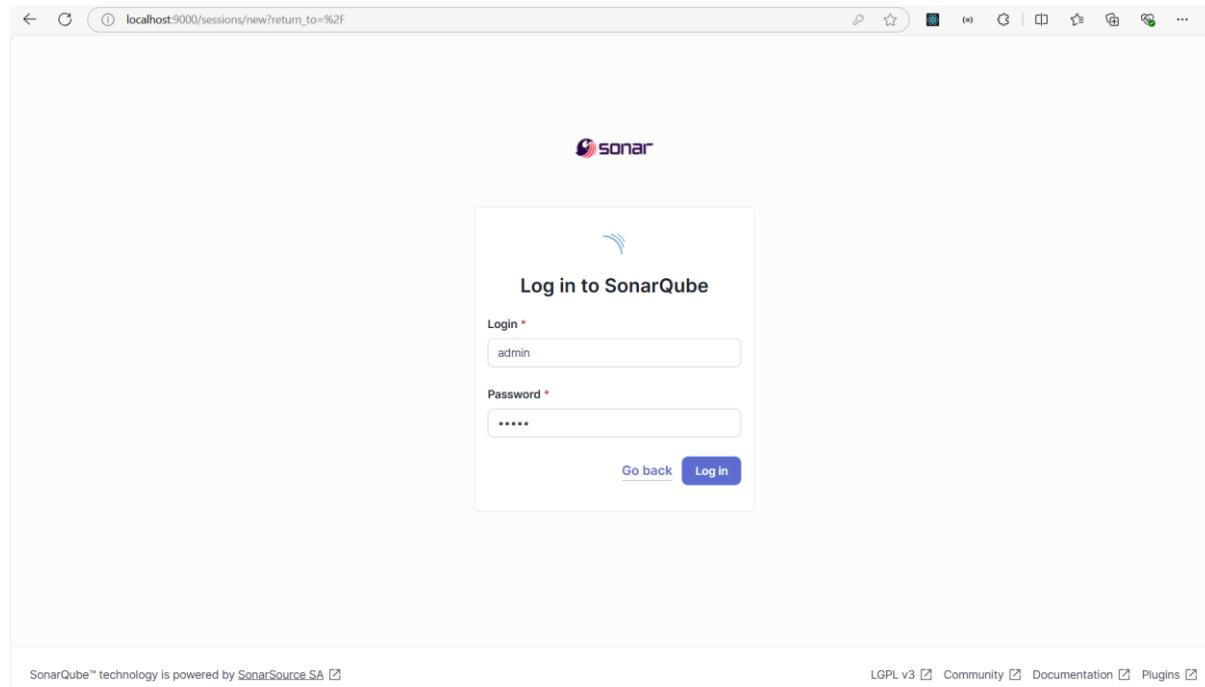
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\User> docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube

7478e0ac0f23: Pull complete
90a925ab929a: Pull complete
7d9a34308537: Pull complete
80338217a4ab: Pull complete
1a5fd5c7e184: Pull complete
7b87d6fa783d: Pull complete
bd819c9b5ead: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Downloaded newer image for sonarqube:latest
006052311e5b87fb720cdca68c48b3d4dc391232a27d69e62cd946bf75eb824
PS C:\Users\User>
```

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.

localhost:9000/projects/create

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

⚠️ 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](#)

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

⚠️ 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](#)

2 of 2

Set up project for Clean as You Code

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

Choose the baseline for new code for this project

Use the global setting

Previous version

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

Recommended for projects following regular versions or releases.

Define a specific setting for this project

Previous version

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

Recommended for projects following regular versions or releases.

Number of days

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

Recommended for projects following continuous delivery.

Reference branch

Choose a branch as the baseline for the new code.

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 Manage Jenkins interface. The left sidebar includes links for New Item, Build History, Project Relationship, Check File Fingerprint, Manage Jenkins (selected), My Views, Build Queue, Build Executor Status (with Built-In Node, 1 idle, 2 idle, and 1 Slave (offline)), and System Configuration (with System, Tools, Nodes, Clouds, and Appearance). The main content area displays a message about a new Jenkins version (2.462.2) available for download, a warning about the built-in node being a security issue, and a list of published warnings for Jenkins 2.452.3 core and libraries, mentioning multiple security vulnerabilities in Jenkins 2.470 and earlier, LTS 2.452.3 and earlier. A blue button allows upgrading automatically. The Plugins section on the right shows 29 available plugins, with SonarQube Scanner listed as one of them.

The screenshot shows the Jenkins Plugins page. A search bar at the top contains the text "sona". On the left, a sidebar lists "Updates", "Available plugins", "Installed plugins" (which is selected and highlighted in grey), and "Advanced settings". The main content area displays the "SonarQube Scanner for Jenkins 2.17.2" plugin, which is described as enabling easy integration with SonarQube for code quality inspection. The plugin is marked as "Enabled" with a green checkmark icon and has a red "Uninstall" button. At the bottom right 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.

The screenshot shows the Jenkins Manage Jenkins page. The left sidebar includes options like "New Item", "Build History", "Project Relationship", "Check File Fingerprint", "Manage Jenkins" (selected), and "My Views". The main content area is titled "Manage Jenkins" and features a "System Configuration" section. It includes links for "System" (Configure global settings and paths), "Tools" (Configure tools, their locations and automatic installers), "Nodes" (Add, remove, control and monitor various nodes), "Clouds" (Add, remove, and configure cloud instances), "Plugins" (Add, remove, disable or enable plugins), and "Appearance" (Configure the look and feel of Jenkins). A message at the top indicates a new version of Jenkins (2.462.2) is available for download, with a "Or Upgrade Automatically" button. Another message below discusses a security issue with the built-in node. The URL "localhost:8080/manage/configure" is visible at the bottom left.

SonarQube servers

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

Environment variables

SonarQube installations

List of SonarQube installations

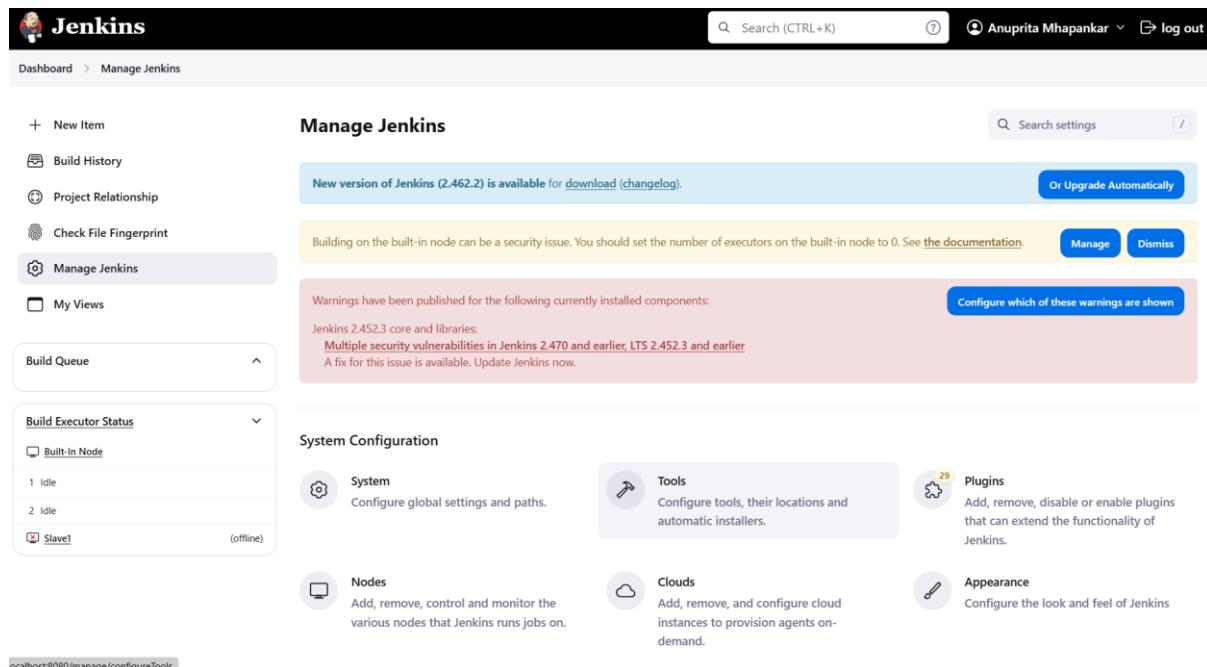
Name

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

Server authentication token
SonarQube authentication token. Mandatory when anonymous access is disabled.

[Advanced](#)

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 interface. On the left, there's a sidebar with links like New Item, Build History, Project Relationship, Check File Fingerprint, Manage Jenkins (which is selected), My Views, and Build Queue. The main area is titled "Manage Jenkins". It features a "System Configuration" section with several tabs: "System" (selected), "Tools", "Nodes", "Clouds", "Plugins" (with a count of 29), and "Appearance". A prominent message at the top says "New version of Jenkins (2.462.2) is available for download (changelog)." Below it, another message about security vulnerabilities in Jenkins 2.452.3 is displayed. The "Tools" tab under System Configuration is currently active, showing options to configure tools, their locations, and automatic installers.

SonarScanner for MSBuild installations

[Add SonarScanner for MSBuild](#)

SonarQube Scanner installations

[Add SonarQube Scanner](#)

SonarQube Scanner

Name

sonarqubescanner

 Install automatically ?

Install from Maven Central

Version

SonarQube Scanner 6.2.0.4584

[Add Installer](#)[Save](#)[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.

Enter an item name

SonarQube > Required field

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.

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

Multibranch Pipeline
OK Creates a set of Pipeline projects according to detected branches in one SCM repository.

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

Configure

Source Code Management

None

Git [?](#)

Repositories [?](#)

Repository URL [?](#)
https://github.com/shazfiori/MSBuild_firstproject.git

Credentials [?](#)
- none -

+ Add [?](#)

Advanced [?](#)

Add Repository

Branches to build [?](#)

Branch Specifier (blank for 'any') [?](#)
*/master

Save **Apply**

Step 9: Under the Build steps select “Execute SonarQube Scanner” option and under Analysis Properties write the following -

sonar.projectKey=sonarqube-test

sonar.login=admin

sonar.password=sonarqube

sonar.hosturl=http://sonarqube:9000

Then click on the save button.

Configure

Build Steps

General

Source Code Management

Build Triggers

Build Environment

Build Steps [?](#)

Post-build Actions

Execute SonarQube Scanner

JDK [?](#)
(Inherit From Job)

Path to project properties [?](#)

Analysis properties [?](#)
sonar.projectKey=sonarqube-test
sonar.login=admin
sonar.password=sonarqube
sonar.hosturl=http://sonarqube:9000

Additional arguments [?](#)

JVM Options [?](#)

Save **Apply**

SonarQube

Add description

Disable Project

Build History trend

No builds

Atom feed for all Atom feed for failures

REST API Jenkins 2.452.3

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

sonarqube

Projects Issues Rules Quality Profiles Quality Gates Administration More Q

Administration

Configuration Security Projects System Marketplace

Global Permissions

Grant and revoke permissions to make changes at the global level. These permissions include editing Quality Profiles, executing analysis, and performing global system administration.

All Users Groups Search for users or groups...

Administrator admin

Administer System Administer Execute Analysis Create

Quality Gates Quality Profiles Projects

1 of 1 shown

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

SonarQube™ technology is powered by SonarSource SA Community Edition v10.6 (92116) ACTIVE LGPL v3 Community Documentation Plugins Web API

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

Jenkins

Dashboard > SonarQube > #4 > Console Output

Status Changes Console Output View as plain text Edit Build Information Delete build #4 Timings Git Build Data Previous Build

Console Output

Started by user Anuprita Mhapankar
Running as SYSTEM
Building on the built-in node in workspace C:\ProgramData\Jenkins\jenkins\workspace\SonarQube
The recommended git tool is: NONE
No credentials specified
> git.exe rev-parse --resolve-git-dir C:\ProgramData\Jenkins\jenkins\workspace\SonarQube\.git # timeout=10
Fetching changes from the remote Git repository
> git.exe config remote.origin.url https://github.com/shazforiot/MSBuild_firstproject.git # timeout=10
Fetching upstream changes from https://github.com/shazforiot/MSBuild_firstproject.git
> git.exe --version # timeout=10
> git --version # "git version 2.41.0.windows.3"
> git.exe fetch --tags --force --progress -- https://github.com/shazforiot/MSBuild_firstproject.git +refs/heads/*:refs/remotes/origin/* # timeout=10
> git.exe rev-parse "refs/remotes/origin/master^{commit}" # timeout=10
Checking out Revision f2bc042c04c6e72427c380bcae6d6fee7b49adf (refs/remotes/origin/master)
> git.exe config core.sparsecheckout # timeout=10
> git.exe checkout -f f2bc042c04c6e72427c380bcae6d6fee7b49adf # timeout=10
Commit message: "updated"
> git.exe rev-list --no-walk f2bc042c04c6e72427c380bcae6d6fee7b49adf # timeout=10
[SonarQube] \$ C:\ProgramData\Jenkins\jenkins\tools\hudson.plugins.sonar.SonarRunnerInstallation\sonarqubescanner\bin\sonar-scanner.bat -Dsonar.host.url=http://localhost:9000 -Dsonar.projectKey=sonarqube-test -Dsonar.login=admin -Dsonar.hosturl=http://sonarqube:9000 -Dsonar.password=sonarqube -Dsonar.projectBaseDir=C:\ProgramData\Jenkins\jenkins\workspace\SonarQube
18:40:04.147 INFO Scanner configuration file:
C:\ProgramData\Jenkins\jenkins\tools\hudson.plugins.sonar.SonarRunnerInstallation\sonarqubescanner\bin..\conf\sonar-scanner.properties
18:40:04.152 INFO Project root configuration file: NONE
18:40:04.175 INFO SonarScanner CLI 6.20.4.4584
18:40:04.177 INFO Java 21.0.4 Eclipse Adoptium (64-bit)
18:40:04.184 INFO Windows 11 10.0 amd64

Dashboard > SonarQube > #4 > Console Output

```
18:40:41.286 INFO ----- Run sensors on project
18:40:41.484 INFO Sensor C# [csharp]
18:40:41.485 WARN Your project contains C# files which cannot be analyzed with the scanner you are using. To analyze C#
SonarScanner for .NET 5.x or higher, see https://redirect.sonarsource.com/doc/install-configure-scanner-msbuild.html
18:40:41.485 INFO Sensor C# [csharp] (done) | time=2ms
18:40:41.486 INFO Sensor Analysis Warnings import [csharp]
18:40:41.488 INFO Sensor Analysis Warnings import [csharp] (done) | time=2ms
18:40:41.488 INFO Sensor # File Caching Sensor [csharp]
18:40:41.489 WARN Incremental PR analysis: Could not determine common base path, cache will not be computed. Consider
'sonar.projectBaseDir' property.
18:40:41.490 INFO Sensor C# File Caching Sensor [csharp] (done) | time=1ms
18:40:41.491 INFO Sensor Zero Coverage Sensor
18:40:41.508 INFO Sensor Zero Coverage Sensor (done) | time=19ms
18:40:41.514 INFO SCM Publisher SCM provider for this project is: git
18:40:41.517 INFO SCM Publisher 4 source files to be analyzed
18:40:42.309 INFO SCM Publisher 4/4 source files have been analyzed (done) | time=791ms
18:40:42.317 INFO CPD Executor Calculating CPD for 0 files
18:40:42.318 INFO CPD Executor CPD calculation finished (done) | time=0ms
18:40:42.326 INFO SCM revision ID 'f2bc042c04c6e72427c380bcae6d6fee7b49adf'
18:40:42.522 INFO Analysis report generated in 181ms, dir size=201.1 kB
18:40:42.588 INFO Analysis report compressed in 63ms, zip size=22.3 kB
18:40:42.876 INFO Analysis report uploaded in 283ms
18:40:42.880 INFO ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=sonarqube-test
18:40:42.881 INFO Note that you will be able to access the updated dashboard once the server has processed the submitte
18:40:42.882 INFO More about the report processing at http://localhost:9000/api/ce/task?id=d10eb30d-ebdd-4bb2-b564-0aa
18:40:42.916 INFO Analysis total time: 25.189 s
18:40:42.926 INFO SonarScanner Engine completed successfully
18:40:43.027 INFO EXECUTION SUCCESS
18:40:43.029 INFO Total time: 38.885s
Finished: SUCCESS
```

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

localhost:9000/dashboard?id=sonarqube-test&codeScope=overall

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration More

main / main ?

Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information

main

Quality Gate * Passed Version not provided Set as homepage Last analysis 14 minutes ago

New Code Overall Code

Security Reliability Maintainability

0 Open issues 0 Open issues 0 Open issues

0 H 0 M 0 L A 0 H 0 M 0 L A 0 H 0 M 0 L A

Accepted issues Coverage Duplications

0 Valid issues that were not fixed On 0 lines to cover. On 86 lines. 0.0%

Security Hotspots

The dashboard displays a green 'Passed' status for the quality gate. It shows zero open issues for security, reliability, and maintainability. There are zero accepted issues, zero coverage, and zero duplications. A note at the top says 'The last analysis has warnings. See details'.

Experiment 8

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

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

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

The screenshot shows the 'SonarScanner CLI' page under the 'Analyzing source code' section. The left sidebar includes links for 'Homepage', 'Try out SonarQube', 'Server installation and setup', 'Analyzing source code' (with 'SonarQube analysis overview', 'Project analysis setup', 'Scanners' (selected), 'Scanner environment', 'SonarScanner CLI', 'SonarQube extension for Azure DevOps', 'SonarQube extension for Jenkins', 'SonarScanner for .NET', 'SonarScanner for Maven', 'SonarScanner for Gradle', 'SonarScanner for NPM', 'SonarScanner for Ant (Deprecated)', 'SonarScanner for Python (Beta)', 'Analysis parameters', 'Languages', 'Test coverage', and 'Importing external issues'). The main content area displays version 6.2 (2024-09-17) with a note about supporting PKCS12 truststore generated with OpenSSL. It lists supported platforms: Linux x64, Linux AArch64, Windows x64, macOS x64, macOS AArch64, Docker, and Any (Requires a pre-installed JVM). Below this is a 'Release notes' section. A callout box highlights that SonarScanners run on checked-out code. To the right, a 'On this page' sidebar lists various configuration and usage topics. The URL in the address bar is https://binaries.sonarsource.com/Distribution/sonar-scanner-cli/sonar-scanner-cli-6.2.0.4584-windows-x64.zip?_gl=1/w3exrs*_qd1_au#MTUyMDY5NDYzMS4xNzI3MjczNDM5*_qa#NTAzMjA1Mzc2IjE3MjcyNzMoMzk1_ga_9/Z0GZ5TC6*MTCyNzI3MzQzO54xJEuMTCyNzI3OTAxNS4yM...

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

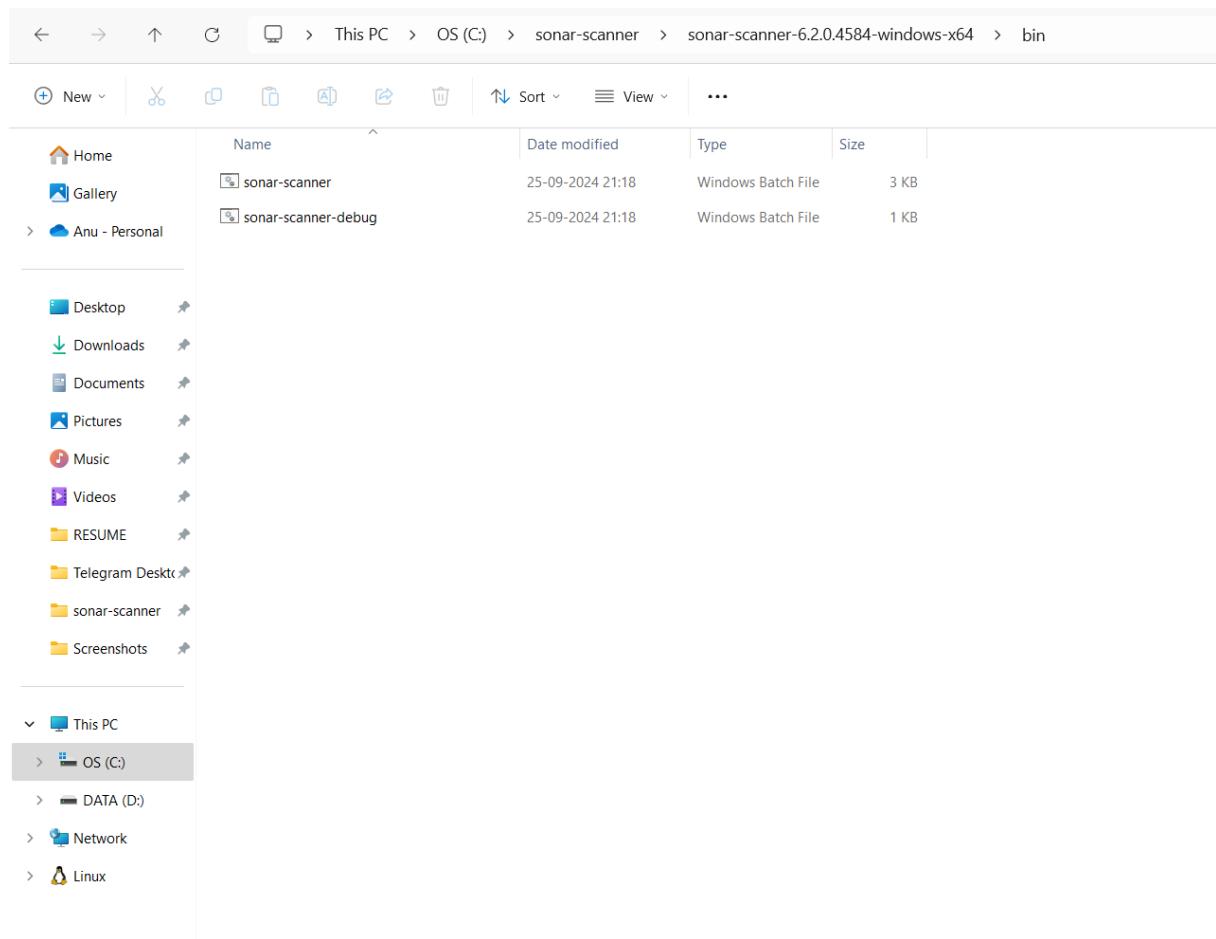
The screenshot shows a Windows File Explorer window with the path 'This PC > OS (C:)'. The 'sonar-scanner' folder is selected. The details pane on the right shows the following information for the 'sonar-scanner' folder:

Details	Type
File location	C:\
Date modified	25-09-2024 21:16

The contents of the 'sonar-scanner' folder are listed in the main pane:

Name	Date modified	Type
data	26-11-2023 16:28	File folder
dell	07-05-2023 12:31	File folder
Drivers	07-10-2022 03:08	File folder
e-logo	04-12-2022 20:02	File folder
ghcup	22-07-2023 18:02	File folder
kubectl	13-11-2023 10:20	File folder
MinGW	24-10-2022 11:26	File folder
msys64	24-10-2022 10:51	File folder
PerfLogs	07-05-2022 10:54	File folder
Program Files	25-09-2024 21:28	File folder
Program Files (x86)	18-07-2024 20:15	File folder
tools	22-07-2023 18:24	File folder
Users	24-10-2022 04:17	File folder
Windows	15-09-2024 10:56	File folder
xampp	24-09-2023 20:52	File folder
sonar-scanner	25-09-2024 21:16	File folder

At the bottom left, it says '17 items 1 item selected'.



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

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

dir

sonar-scanner.bat

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

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

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

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

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

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

Enter an item name

SonarQube Pipeline

> Required field



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.



Folder

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



Branch Pipeline

OK Create a set of Pipeline projects according to detected branches in one SCM repository.

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

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

stage('SonarQube analysis') {
    withSonarQubeEnv('sonarqube') {
        bat "C:/sonar-scanner/sonar-scanner-6.2.0.4584-windows-x64/bin/sonar-scanner.bat \
            -D sonar.login=admin \
            -D sonar.password=sonarqube \
            -D sonar.projectKey=sonarqube-test \
            -D sonar.exclusions=vendor/**,resources/**,*/*.java \
            -D sonar.host.url=http://127.0.0.1:9000/"
    }
}
```

Then click on the save button.

Configure

General

Advanced Project Options

Pipeline

Pipeline**Definition**

Pipeline script

Script ?

```

1+ node {
2+   stage('Cloning the GitHub Repo') {
3+     git 'https://github.com/shazforiot/MSBuild_firstproject.git'
4+   }
5+   stage('SonarQube analysis') {
6+     withSonarQubeEnv('sonarqube') {
7+       Bat "C:/sonar-scanner/sonar-scanner-6.2.0.4584-windows-x64/bin/sonar-scanner.bat" \
8+           -D sonar.login=admin \
9+           -D sonar.password=sonarqube \
10+          -D sonar.projectKey=sonarqube-test \
11+          -D sonar.host.url=http://127.0.0.1:9000/ \
12+          -D sonar.host.url=http://127.0.0.1:9000/"
13+     }
14+   }
15+ }
16

```

 Use Groovy Sandbox ?

Pipeline Syntax

Save**Apply**

REST API Jenkins 2.452.3

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

Jenkins

Dashboard > SonarQube Pipeline >

SonarQube Pipeline

Status Changes Build Now Configure Delete Pipeline Full Stage View SonarQube Stages Rename Pipeline Syntax Add description Disable Project

Stage View

Average stage times: (Average full run time: ~22s)

	Cloning the GitHub Repo	SonarQube analysis
#10 Sep 25 21:55	No Changes	1s
#9 Sep 25 21:52	No Changes	19s
#8 Sep 25 21:43	No Changes	1s
#7 Sep 25 21:33	No Changes	1s

Build History trend ▾

- #10 Sep 25, 2024, 9:55 PM
- #9 Sep 25, 2024, 9:52 PM
- #8

```

21:56:16.244 INFO ----- Run sensors on project
21:56:16.428 INFO Sensor C# [csharp]
21:56:16.429 WARN Your project contains C# files which cannot be analyzed with the scanner you are using. To analyze C# or VB.NET, you must use the SonarScanner for .NET 5.x or higher, see https://redirect.sonarsource.com/doc/install-configure-scanner-msbuild.html
21:56:16.429 INFO Sensor C# [csharp] (done) | time=1ms
21:56:16.430 INFO Sensor Analysis Warnings import [csharp]
21:56:16.432 INFO Sensor Analysis Warnings import [csharp] (done) | time=2ms
21:56:16.432 INFO Sensor C# File Caching Sensor [csharp]
21:56:16.432 WARN Incremental PR analysis: Could not determine common base path, cache will not be computed. Consider setting 'sonar.projectBaseDir' property.
21:56:16.432 INFO Sensor C# File Caching Sensor [csharp] (done) | time=1ms
21:56:16.433 INFO Sensor Zero Coverage Sensor
21:56:16.450 INFO Sensor Zero Coverage Sensor (done) | time=16ms
21:56:16.494 INFO CPU Executor Calculating CPD for 0 files
21:56:16.494 INFO CPU Executor CPD calculation finished (done) | time=0ms
21:56:16.530 INFO SCM revision ID 'f2bc042c04c6e72427c380bcaeedd6fee7b49adf'
21:56:16.704 INFO Analysis report generated in 178ms, dir size=200.5 kB
21:56:16.773 INFO Analysis report compressed in 68ms, zip size=21.9 kB
21:56:16.930 INFO Analysis report uploaded in 155ms
21:56:16.931 INFO ANALYSIS SUCCESSFUL, you can find the results at: http://127.0.0.1:9000/dashboard?id=sonarqube-test
21:56:16.931 INFO Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
21:56:16.932 INFO More about the report processing at http://127.0.0.1:9000/api/ce/task?id=af67fb15-719a-4b23-8f38-5edc7a765dae
21:56:16.940 INFO Analysis total time: 16.723 s
21:56:16.943 INFO SonarScanner Engine completed successfully
21:56:17.042 INFO EXECUTION SUCCESS
21:56:17.044 INFO Total time: 19.574s
[Pipeline]
[Pipeline] // withSonarQubeEnv
[Pipeline]
[Pipeline] // stage
[Pipeline]
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS

```

Step 7: Now, visit <http://127.0.0.1:9000/dashboard?id=sonarqube-test> to see the result.

The screenshot shows the SonarQube dashboard for the 'sonarqube-test' project. The main header includes the SonarQube logo, navigation links for Projects, Issues, Rules, Quality Profiles, Quality Gates, Administration, More, and a search bar. Below the header, there's a breadcrumb trail showing the project name and a dropdown menu. The main content area features a large green 'Passed' status indicator with a checkmark icon. A yellow warning box indicates that the last analysis has warnings, with a 'See details' link. The dashboard is divided into several sections: 'Quality Gate' (Passed), 'New Code' (0 Open issues), 'Overall Code' (selected), 'Security' (0 Open issues), 'Reliability' (0 Open issues), 'Maintainability' (0 Open issues), 'Accepted issues' (0), 'Coverage' (0.0%), 'Duplications' (0.0%), and 'Security Hotspots' (0). The 'Overall Code' section also displays metrics for hours (0 H), minutes (0 M), and lines (0 L).

127.0.0.1:9000/dashboard?id=sonarqube-test&codeScope=overall

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration More Q

sonarqube-test / main ?

Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information

Learn how to improve your code base by cleaning only new code.

Take the Tour Not now

Quality Gate Passed Last analysis 45 minutes ago

The last analysis has warnings. See details

New Code Overall Code

Security	Reliability	Maintainability
0 Open issues 0 H 0 M 0 L	68k Open issues 0 H 47k M 21k L	164k Open issues 7 H 143k M 21k L
Accepted issues 0 Valid issues that were not fixed	Coverage On 0 lines to cover.	Duplications 50.6% On 759k lines.

Security Hotspots

Experiment 9

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 Instances page. On the left, there's a navigation sidebar with links like EC2 Dashboard, EC2 Global View, Events, and various instance-related options. The main area displays a table of instances. One row is selected, showing details for an instance named "nagios-host" with the ID "i-033ee56b96fef8322". The instance is listed as "Running" with an "Initializing" status check. It's located in the "us-east-1c" availability zone and has a public IP of "ec2-44-21-225-236.compute-1.amazonaws.com". Below the table, a detailed view for the selected instance is shown, including sections for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. The "Details" tab is active, displaying the instance summary and its configuration.

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

The screenshot shows the AWS Security Groups page. The left sidebar includes links for EC2 Dashboard, EC2 Global View, Events, and various security-related options. The main content area shows a security group named "launch-wizard-13" with a description of "created 2024-09-30T16:37:21.185Z". It lists 7 inbound rules and 1 outbound rule. The "Inbound rules" tab is selected, showing a table of rules. The rules include various ports and protocols such as Custom TCP (port 5666), HTTPS (port 443), SSH (port 22), HTTP (port 80), All traffic (port All), IPv6 ICMP (port All), and ICMP (port All). The "Edit inbound rules" button is visible at the top right of the rule table.

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

AWS Services Search [Alt+S] N. Virginia 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 [i-025f1d18f7c8a8cda](#) (nagios-host)

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 [3.86.198.73](#)

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

Amazon Linux 2023

https://aws.amazon.com/linux/amazon-linux-2023

```
(ec2-user@ip-172-31-93-157 ~)$ sudo su
[root@ip-172-31-93-157 ec2-user]# sudo yum update
Last metadata expiration check: 0:11:38 ago on Mon Sep 30 16:39:07 2024.
Dependencies resolved.
Nothing to do.
Nothing to do.
Complete!
[root@ip-172-31-93-157 ec2-user]# sudo yum install httpd php
Last metadata expiration check: 0:11:51 ago on Mon Sep 30 16:39:07 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-core	x86_64	2.4.62-1.amzn2023	amazonlinux	1.4 M
httpd-filesystem	noarch	2.4.62-1.amzn2023	amazonlinux	14 k
httpd-tools	x86_64	2.4.62-1.amzn2023	amazonlinux	81 k
libbrotli	x86_64	1.0.9-4.amzn2023.0.2	amazonlinux	315 k
libsodium	x86_64	1.0.19-4.amzn2023	amazonlinux	176 k

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 vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
php8.3-xml-0.3.10-1.amzn2023.0.1.x86_64
Complete!
[root@ip-172-31-93-157 ec2-user]# sudo yum install gcc glibc glibc-common
Last metadata expiration check: 0:12:22 ago on Mon Sep 30 16:39:07 2024.
Package glibc-2.34-52.amzn2023.0.11.x86_64 is already installed.
Package glibc-common-2.34-52.amzn2023.0.11.x86_64 is already installed.
Dependencies resolved.
Transaction Summary
Install 13 Packages
Total download size: 52 M
Installed size: 168 M
Is this ok [y/N]: y

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 vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
Complete!
[root@ip-172-31-93-157 ec2-user]# sudo yum install gd gd-devel
Last metadata expiration check: 0:13:10 ago on Mon Sep 30 16:39:07 2024.
Dependencies resolved.
Transaction Summary
Install 30 Packages
Total download size: 1.39 G
Installed size: 3.86 G
Is this ok [y/N]: y

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

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

```

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

[root@ip-172-31-93-157 ec2-user]# sudo adduser -m nagios
[root@ip-172-31-93-157 ec2-user]# sudo passwd nagios
Changing password for user nagios.
New password:
Re-type new password:
passwd: all authentication tokens updated successfully.
[root@ip-172-31-93-157 ec2-user]# sudo groupadd nagcmd
[root@ip-172-31-93-157 ec2-user]# sudo usermod -a -G nagcmd nagios
[root@ip-172-31-93-157 ec2-user]# sudo usermod -a -G nagcmd apache
[root@ip-172-31-93-157 ec2-user]#
```

i-025f1d18f7c8a8cda (nagios-host) X

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 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
```

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

[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) X

PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

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

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 downloads]# 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...
HTTP request sent, awaiting response... 302 Found
Location: http://versaweb.dl.sourceforge.net/project/nagios/nagios-4.0.8/nagios-4.0.8.tar.gz?viafs=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?viafs=1
Resolving versaweb.dl.sourceforge.net (versaweb.dl.sourceforge.net)... 162.251.232.173
Connecting to versaweb.dl.sourceforge.net (versaweb.dl.sourceforge.net)|162.251.232.173:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1805059 (1.7M) [application/x-gzip]
Saving to: 'nagios-4.0.8.tar.gz'

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-gzip]
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

```
CloudShell Feedback Search [Alt+S] N. Virginia vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793
aws Services
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_flexim.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_agt.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/solpkg
nagios-plugins-2.0.3/pkg/solaris/pkginfo.in
nagios-plugins-2.0.3/pkg/solaris/pkginfo
nagios-plugins-2.0.3/pkg/redhat/
nagios-plugins-2.0.3/pkg/redhat/requirements
[root@ip-172-31-93-157 downloads]# ]
```

i-025f1d18f7c8a8cda (nagios-host)

PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

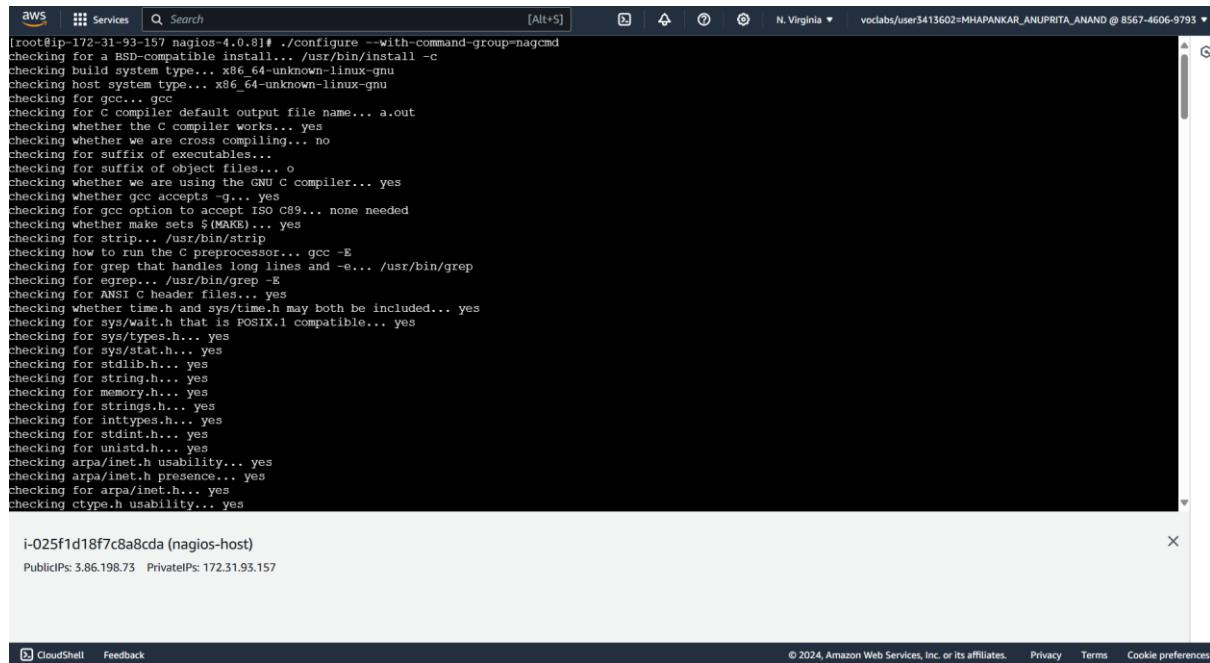
```
CloudShell Feedback Search [Alt+S] N. Virginia vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793
aws Services
nagios-plugins-2.0.3/plugins-scripts/Makefile.am
nagios-plugins-2.0.3/plugins-scripts/subst.in
nagios-plugins-2.0.3/plugins-scripts/check_breeze.pl
nagios-plugins-2.0.3/plugins-scripts/check_log.sh
nagios-plugins-2.0.3/plugins-scripts/check_flexim.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.rn.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_agt.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/solpkg
nagios-plugins-2.0.3/pkg/solaris/pkginfo.in
nagios-plugins-2.0.3/pkg/solaris/pkginfo
nagios-plugins-2.0.3/pkg/redhat/
nagios-plugins-2.0.3/pkg/redhat/requirements
[root@ip-172-31-93-157 downloads]# 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

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

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



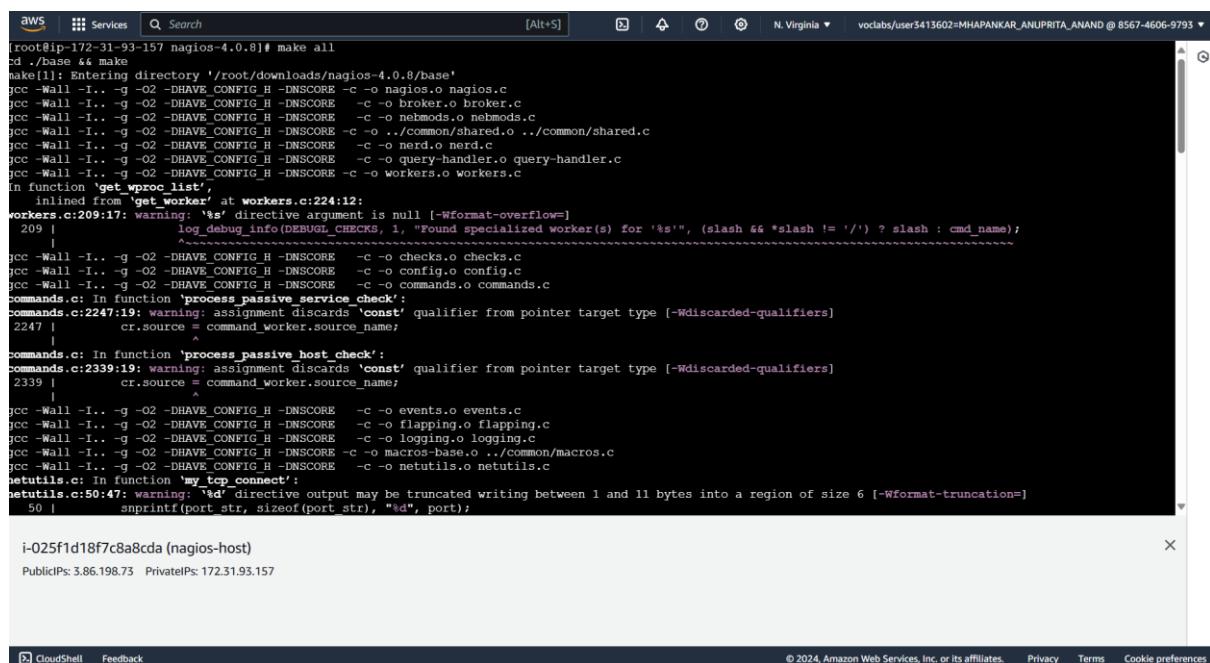
```
aws Services Search [Alt+S] N. Virginia vclabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793
root@ip-172-31-93-157 nagios-4.0.8# ./configure --with-command-group=nagcmd
checking for a BSD-compatible install... /usr/bin/install -c
checking build system type... x86_64-unknown-linux-gnu
checking 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 -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether make sets ${MAKE}... yes
checking for strip... /usr/bin/strip
checking how to run the C preprocessor... gcc -E
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
checking ctype.h presence... yes
```

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

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

```
make all
```



```
aws Services Search [Alt+S] N. Virginia vclabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793
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 nelmods.o nelmods.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: '%d' directive output may be truncated writing between 1 and 11 bytes into a region of size 6 [-Wformat-truncation=]
  50 |     sprintf(port_str, sizeof(port_str), "%d", port);
```

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 voclabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
[root@ip-172-31-93-157 nagios-4.0.8]# sudo make install
cd ./base ss 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 *.cfg; do \
/usr/bin/install -c -m 775 -o nagios -g nagios $file /usr/local/nagios/sbin; \
done
/usr/bin/install: cannot stat '**.cfg': 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
[root@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
/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)

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 voclabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
[root@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
/usr/bin/install -c -m 755 -o root -g root daemon-init /etc/rc.d/init.d/nagios
*** Init script installed ***

```

```

[root@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 -b -m 664 -o nagios -g nagios sample-config/nagios.cfg /usr/local/nagios/etc/nagios.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/cgi.cfg /usr/local/nagios/etc/cgi.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/resource.cfg /usr/local/nagios/etc/resource.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/templates.cfg /usr/local/nagios/etc/objects/templates.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/commands.cfg /usr/local/nagios/etc/objects/commands.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/contacts.cfg /usr/local/nagios/etc/objects/contacts.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/timperiods.cfg /usr/local/nagios/etc/objects/timperiods.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/swtch.cfg /usr/local/nagios/etc/objects/swtch.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.

```

[root@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 ***

```

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

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

```

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

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]#

```

```

aws Services Search [Alt+S] /usr/local/nagios/etc/objects/contacts.cfg N. Virginia vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793
GNU nano 5.8
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 voclabs/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 [ $? -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 voclabs/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 xvzf nagios-plugins-2.0.3.tar.gz
nagios-plugins-2.0.3/
nagios-plugins-2.0.3/perlmods/
nagios-plugins-2.0.3/perlmods/Config-Tiny-2.14.tar.gz
nagios-plugins-2.0.3/perlmods/parent-0.226.tar.gz
nagios-plugins-2.0.3/perlmods/test-Simple-0.98.tar.gz
nagios-plugins-2.0.3/perlmods/Makefile.in
nagios-plugins-2.0.3/perlmods/version-0.9903.tar.gz
nagios-plugins-2.0.3/perlmods/Makefile.am
nagios-plugins-2.0.3/perlmods/Module-Runtime-0.013.tar.gz
nagios-plugins-2.0.3/perlmods/Module-Metadata-1.000014.tar.gz
nagios-plugins-2.0.3/perlmods/Params-Validate-1.08.tar.gz
nagios-plugins-2.0.3/perlmods/Class-Accessor-0.34.tar.gz
nagios-plugins-2.0.3/perlmods/try-Tiny-0.18.tar.gz
nagios-plugins-2.0.3/perlmods/Module-Implementation-0.07.tar.gz
nagios-plugins-2.0.3/perlmods/Makefile
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
```

```

aws Services Search [Alt+S] N. Virginia voclabs/user3413602:MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793
/usr/bin/install -c -o nagios -g nagios check_dhcp /usr/local/nagios/libexec/check_dhcp
chmod ug-rx,ut+ws /usr/local/nagios/libexec/check_dhcp
/usr/bin/install -c -o nagios -g nagios check_icmp /usr/local/nagios/libexec/check_icmp
chmod ug-rx,ut+ws /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]: Nothing to be done for 'install-exec-am'.
take[1]: Leaving directory '/root/downloads/nagios-plugins-2.0.3/plugins-root'
take[1]: Entering directory '/root/downloads/nagios-plugins-2.0.3/po'
/usr/bin/mkdir -p /usr/local/nagios/share/gettext/po/
installing fr.gmo as /usr/local/nagios/share/locale/fr/LC_MESSAGES/nagios-plugins.mo
installing de.gmo as /usr/local/nagios/share/locale/de/LC_MESSAGES/nagios-plugins.mo
if test "nagios-plugins" != "gettext-tools"; then \
  /usr/bin/mkdir -p /usr/local/nagios/share/gettext/po; \
  for file in Makefile.in.in remove-potcdate.sm Makevars.template; do \
    rm -f /usr/local/nagios/share/gettext/po/$file; \
  done; \
else \
  :; \
fi
done; \
for file in Makevars; do \
  rm -f /usr/local/nagios/share/gettext/po/$file; \
done; \
done; \
done; \
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]: 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

```

aws Services Search [Alt+S] N. Virginia voclabs/user3413602:MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793
[root@ip-172-31-93-157 nagios-plugins-2.0.3]# sudo chkconfig --add nagios
sudo chkconfig nagios on
[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

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

Check status using the following command -
sudo systemctl status nagios

```

aws Services Search [Alt+S] N. Virginia vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793
[root@ip-172-31-93-157 nagios-plugins-2.0.3]# sudo systemctl status nagios
● nagios.service - LSB: Starts and stops the Nagios monitoring server
   Loaded: loaded (/etc/rc.d/init.d/nagios; generated)
   Active: active (running) since Mon 2024-09-30 10:02:27 UTC; 42s ago
     Docs: man:systemctl(1)
   Process: 79969 ExecStart=/etc/rc.d/init.d/nagios start (code=exited, status=0/SUCCESS)
   Tasks: 6 (limit: 1112)
   Memory: 2.2M
      CPU: 52ms
      CPU: 52ms
     CGroup: /system.slice/nagios.service
             ├─80009 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─80011 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─80012 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─80013 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─80014 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─80037 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Sep 30 10:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Successfully registered manager as @wproc with query handler
Sep 30 10:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80011;pid=80011
Sep 30 10:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80014;pid=80014
Sep 30 10:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80013;pid=80013
Sep 30 10:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80012;pid=80012
Sep 30 10:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The normal_check_interval attribute is deprecated and will be removed in future versions. Please use Check_interval instead.
Sep 30 10:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The retry_check_interval attribute is deprecated and will be removed in future versions. Please use retry_interval instead.
Sep 30 10:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The normal_check_interval attribute is deprecated and will be removed in future versions. Please use Check_interval instead.
Sep 30 10:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The retry_check_interval attribute is deprecated and will be removed in future versions. Please use retry_interval instead.
Sep 30 10:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: Successfully launched command file worker with pid 80037
lines: 1-26/26 (END)

```

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

Screenshot of the AWS EC2 Instances page showing a single instance named "nagios-host" (i-025f1d18f7c8a8cda) in the "Running" state. The instance type is t2.micro, and it has 2/2 checks passed. It is located in the us-east-1c availability zone with a public IP of ec2-3-86-172-31-93-157.compute-1.amazonaws.com.

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

Screenshot of the Nagios Core 4.4.6 dashboard. The main header shows "Nagios® Core™ Version 4.4.6" and "April 28, 2020". A blue box at the top right says "A new version of Nagios Core is available! Visit nagios.org to download Nagios 4.5.5." The left sidebar includes links for General, Current Status, Problems, Reports, and System. The main content area features sections for "Get Started" (with bullet points like "Start monitoring your infrastructure" and "Extend Nagios with hundreds of addons"), "Quick Links" (with links to Nagios Library, Labs, Exchange, Support, and more), "Latest News" (empty), and "Don't Miss..." (empty). The bottom of the page includes copyright information and logos for Nagios and SourceForge.NET.

Experiment 10

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

Step 1: Initially confirm that Nagios is running on the server side. For this run the following command -

sudo systemctl status nagios
on the nagios-host instance.

```
aws Services Search [Alt+S] N. Virginia vociabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793
root@ip-172-31-93-157:~# sudo systemctl status nagios
● nagios.service - LSB: Starts and stops the Nagios monitoring server
   Loaded: loaded (/etc/rc.d/init.d/nagios)
   Active: active (running) since Mon 2024-09-30 18:02:27 UTC; 42s ago
     Docs: man:/etc/init.d/SVNV-88967030.0
   Process: 79969 execStart=/etc/rc.d/init.d/nagios start (code=exited, status=0/SUCCESS)
   Tasks: 6 (limit: 1112)
   Memory: 2.2M
      CPU: 52ms
     CGroup: /system.slice/nagios.service
             └─80009 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
               ├─80011 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
               ├─80012 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
               ├─80013 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
               ├─80014 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
               └─80037 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Successfully registered manager as /proc with query handler
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80011/pid=80011
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80014/pid=80014
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80013/pid=80013
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80012/pid=80012
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The normal_check_interval attribute is deprecated and will be removed in future versions. Please use retry_check_interval instead.
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The retry_check_interval attribute is deprecated and will be removed in future versions. Please use normal_check_interval instead.
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The normal_check_interval attribute is deprecated and will be removed in future versions. Please use retry_check_interval instead.
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: Successfully launched command file worker with pid 80037
lines: 1-26/26 (END)
```

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

Step 2: Once confirmed, make another instance with the same security group as that of nagios-host.
For now, leave this machine as it is, and go back to your nagios-host machine.

Inbound rules (7)						
<input type="button" value="C"/> <input type="button" value="Manage tags"/> <input type="button" value="Edit inbound rules"/>						
<input type="text" value="Search"/> < 1 > 						
Name	Security group rule...	IP version	Type	Protocol	Port range	
-	sgr-01439baf13aca75fa	IPv6	All ICMP - IPv6	IPv6 ICMP	All	
-	sgr-07d8ce2ac9f5e6a92	IPv4	All traffic	All	All	
-	sgr-071fd6724622dd2...	IPv4	HTTPS	TCP	443	
-	sgr-0e47c6681768287...	IPv4	SSH	TCP	22	
-	sgr-0f594249495210d...	IPv4	Custom TCP	TCP	5666	
-	sgr-07b7ba4fe05f14614	IPv4	HTTP	TCP	80	
-	sgr-0fcfb4849f80ee0409	IPv4	All ICMP - IPv4	ICMP	All	

Step 3: Now run the following command -

ps -ef | grep nagios

```

aws Services Search [Alt+S] N. Virginia v vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
Active: active (running) since Mon 2024-09-30 18:02:27 UTC; 42s ago
  Docs: man:sysdig-sysv-runqsp(8)
Process: 79569 ExecStart=/etc/rc.d/init.d/nagios start (code=exited, status=0/SUCCESS)
 Tasks: 6 (limit: 1112)
Memory: 2.2M
 CPU: 52ms
 cgroup: /system.slice/nagios.service
└─80009 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
   ├─80011 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
   ├─80012 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
   ├─80013 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
   ├─80014 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
   └─80037 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Successfully registered manager as @wproc with query handler
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80011;pid=80011
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80014;pid=80014
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80013;pid=80013
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80012;pid=80012
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The normal check_interval attribute is deprecated and will be removed in future versions. Please use retry_interval instead.
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The retry_check_interval attribute is deprecated and will be removed in future versions. Please use retry_interval instead.
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The normal check_interval attribute is deprecated and will be removed in future versions. Please use retry_interval instead.
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: Successfully launched command file worker with pid 80037
[root@ip-172-31-93-157 nagios-plugins-2.0.3]# ps -ef | grep nagios
nagios 80009 1 0 18:02 ? 0:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios 80011 80009 0 18:02 ? 0:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
nagios 80012 80009 0 18:02 ? 0:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
nagios 80013 80009 0 18:02 ? 0:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
nagios 80014 80009 0 18:02 ? 0:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
nagios 80037 80009 0 18:02 ? 0:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
root 81960 3110 0 18:35 pts/1 0:00:00 grep --color=auto nagios
[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 4: Now, run the following commands -

```

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

```

```

aws Services Search [Alt+S] N. Virginia v vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793 ▾
root@ip-172-31-93-157 nagios-plugins-2.0.3]# sudo su
root@ip-172-31-93-157 nagios-plugins-2.0.3]# mkdir /usr/local/nagios/etc/objects/monitorhosts
root@ip-172-31-93-157 nagios-plugins-2.0.3]# mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
root@ip-172-31-93-157 nagios-plugins-2.0.3]# cp /usr/local/nagios/etc/objects/localhost.cfg
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
cp: missing destination file operand after '/usr/local/nagios/etc/objects/localhost.cfg'
try 'cp --help' for more information.
ash: /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg: No such file or directory
root@ip-172-31-93-157 nagios-plugins-2.0.3]# nano
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
ash: /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg: No such file or directory
root@ip-172-31-93-157 nagios-plugins-2.0.3]# cp /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
cp: missing destination file operand after '/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg'
try 'cp --help' for more information.
root@ip-172-31-93-157 nagios-plugins-2.0.3]# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
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 5: Open linuxserver.cfg using the the following command -

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

Change the hostname to linuxserver (EVERYWHERE ON THE FILE)

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

Change hostgroup_name under hostgroup to linux-servers1

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

```
#####
# 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      linux-server
    alias          linux-server
    address        3.95.202.23
}
```

^X Help ^C Write Out ^W Where Is ^K Cut ^E Execute ^A Location M-U Undo M-D Set Mark M-L To Bracket M-C Previous
^M Exit ^R Read File ^V Replace ^U Paste ^J Justify ^I Go To Line M-B Redo M-Q Copy ^Q Where Was M-N Next

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

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

```
check_command check_local_swap!20!0
```

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

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

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

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

^X Help ^C Write Out ^W Where Is ^K Cut ^E Execute ^A Location M-U Undo M-D Set Mark M-L To Bracket M-C Previous
^M Exit ^R Read File ^V Replace ^U Paste ^J Justify ^I Go To Line M-B Redo M-Q Copy ^Q Where Was M-N Next

i-025f1d18f7c8a8cda (nagios-host)

Public IPs: 3.86.198.73 Private IPs: 172.31.93.157

Step 6: Open Nagios config file and add the following line -
nano /usr/local/nagios/etc/nagios.cfg

Then add this line -

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

```

GNU nano 5.8
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

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

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

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

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

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

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

^G Help      ^Q Write Out   ^M Where Is   ^F Cut        ^T Execute    ^L Location   M-U Undo   M-D Set Mark   M-I To Bracket M-S Previous
^X Exit      ^R Read File   ^V Replace    ^U Paste      ^J Justify    ^G Go To Line M-E Redo   M-C Copy      M-Q Where Was  M-N Next

```

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

Step 8: Verify configuration files using the following command -
sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

If there are no errors, run the following command -
sudo service nagios start

```

aws Services Search [Alt+S] N. Virginia v vocabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793
[root@ip-172-31-93-157 nagios-plugins-2.0.3]# nano /usr/local/nagios/etc/nagios.cfg
[root@ip-172-31-93-157 nagios-plugins-2.0.3]# nano /usr/local/nagios/etc/nagios.cfg
[root@ip-172-31-93-157 nagios-plugins-2.0.3]# /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.
Error: Could not find any host matching 'linuxserver' (config file '/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg', starting on line 45)
Error: Could not expand members specified in hostgroup (config file '/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg', starting on line 45)
  Error processing object config files!

***> One or more problems was encountered while processing the config files...

Check your configuration file(s) to ensure that they contain valid
directives and data definitions. If you are upgrading from a previous
version of Nagios, you should be aware that some variables/definitions
may have been removed or modified in this version. Make sure to read
the HTML documentation regarding the config files, as well as the
"What's New" section to find out what has changed.

[root@ip-172-31-93-157 nagios-plugins-2.0.3]# []

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

```

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

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

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

Step 9: After entering the correct credentials, you will see this page.

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

Instances (1/1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
nagios-host	i-025f1d18f7c8a8cda	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1c	ec2-3-86-

i-025f1d18f7c8a8cda (nagios-host)

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary

- Instance ID: i-025f1d18f7c8a8cda (nagios-host)
- IPv6 address: -
- Hostname type: IP name: ip-172-31-93-157.ec2.internal
- Answer private resource DNS name: -
- Public IPv4 address copied: 3.86.198.73 | open address
- Private IP DNS name (IPv4 only): ip-172-31-93-157.ec2.internal
- Instance state: Running
- Instance type: t2.micro
- Elastic IP addresses: -

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

Not secure 3.86.198.73/nagios/

Nagios®

Current Network Status

Last Updated: Mon Sep 30 19:13:49 UTC 2024
 Nagios® Core™ 4.4.6 - www.nagios.org
 Logged in as nagiosadmin

[View Service Status Details For All Host Groups](#)
[View Status Overview For All Host Groups](#)
[View Status Summary For All Host Groups](#)
[View Status Grid For All Host Groups](#)

Host Status Totals

Up	Down	Unreachable	Pending
2	0	0	0
All Problems	All Types		
0	2		

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
6	1	0	1	8
All Problems	All Types			
2	16			

Host Status Details For All Host Groups

Limit Results: 100 ▾

Host *	Status *♦	Last Check *♦	Duration *♦	Status Information
linuxserver	UP	09-30-2024 19:13:16	0d 0h 0m 33s+	PING OK - Packet loss = 0%, RTA = 1.82 ms
localhost	UP	09-30-2024 19:01:49	0d 1h 11m 22s	PING OK - Packet loss = 0%, RTA = 0.04 ms

Results 1 - 2 of 2 Matching Hosts

Current Status

- [General Overview](#)
- [Map \(Legacy\)](#)
- [Hosts](#)
- [Services](#)
- [Host Groups](#)
 - Summary
 - Grid
- [Service Groups](#)
 - Summary
 - Grid
- [Problems](#)
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages
- [Quick Search:](#)

Reports

- [Availability](#)
- [Trends \(Legacy\)](#)
- [Alerts](#)
- [History](#)
- [Summary](#)
- [Histogram \(Legacy\)](#)
- [Notifications](#)
- [Event Log](#)

System

- [Comments](#)
- [Downtime](#)
- [Process Info](#)
- [Performance Info](#)
- [Scheduling Queue](#)
- [Configuration](#)

Experiment 11

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

Step1: Open up the Lambda Console and click on the Create button.

The screenshot shows the AWS Lambda console interface. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, search bar, and account information ('N. Virginia' and 'voclabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793'). Below the navigation is a sidebar with a 'Lambda' icon and the text 'Functions (5)'. The main area displays a table of functions with columns: Function name, Description, Package type, Runtime, and Last modified. Each row has a checkbox and a link to the function details. The last modified column shows '2 months ago' for all functions. At the bottom of the table are navigation arrows and a refresh icon. A large orange 'Create function' button is located at the top right of the main content area. The footer contains links for CloudShell, Feedback, and copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates.' followed by Privacy, Terms, and Cookie preferences.

Step 2: Create a function and name it and select the runtime environment as Python 3.12 and for the role select the existing role LabRole.

The screenshot shows the 'Create function' wizard. The first step, 'Choose one of the following options to create your function.', has three options: 'Author from scratch' (selected), 'Use a blueprint', and 'Container image'. The second step, 'Basic information', includes fields for 'Function name' (with placeholder 'Enter a name that describes the purpose of your function.' and input field 'lambdaanuprita'), 'Runtime' (with dropdown 'Python 3.12' selected), and 'Architecture' (with link 'Info'). The footer contains CloudShell, Feedback, and copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates.' followed by Privacy, Terms, and Cookie preferences.

S | Services | Search | [Alt+S] | N. Virginia | vclabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793

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

▼ Change default execution role

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).

Create a new role with basic Lambda permissions
 Use an existing role
 Create a new role from AWS policy templates

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

LabRole  

View the LabRole role [on the IAM console](#).

► Advanced settings

Cancel **Create function**

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

aws | Services | Search | [Alt+S] | N. Virginia | vclabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793

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

Lambda > Functions > lambdaanuprita

lambdaanuprita

Throttle  Actions ▾

▼ Function overview [Info](#)

Diagram [Template](#)

 lambdaanuprita
 Layers (0)

+ Add trigger 

Description
-

Last modified
11 seconds ago

Function ARN
 arn:aws:lambda:us-east-1:856746069793:function:lambdaanuprita

Function URL [Info](#)
-

Export to Application Composer 

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

Step 3: Scroll down to the code source section and then visit Configuration section and click on edit.

aws | Services | Search | [Alt+S] | N. Virginia | vclabs/user3413602=MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793

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

Code source [Info](#)

File Edit Find View Go Tools Window Test Deploy

Upload from ▾

Environment

Go to Anything (Ctrl-P) lambda_function Environment Var

lambdaanuprita lambda_function.py

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

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

Step 4: Make the following changes and then click on the save button.

Step 5: Scroll down to the code source section and then visit Test section. Create a new event and then name the event. Now, click on Test.

Successfully updated the function lambdaanuprita.

Code Test Monitor Configuration Aliases Versions

Test event Info

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

anupritaevent

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](#)

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

Successfully updated the function lambdaanuprita.

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 "key1": "value1",
3 "key2": "value2",
4 "key3": "value3"
5]

Format JSON

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

Step 6: The test results are as shown below.

The test event anupritaevent was successfully saved.

Code Source Info

File Edit Find View Go Tools Window Test Deploy

Execution result

Execution results

Test Event Name (unsaved) test event Status: Succeeded Max memory used: 32 MB Time: 1.98 ms

Response

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

Function Logs

```
START RequestId: efa4b7a6-4876-4478-bcfb-e304307119f8 Version: $LATEST
END RequestId: efa4b7a6-4876-4478-bcfb-e304307119f8
REPORT RequestId: efa4b7a6-4876-4478-bcfb-e304307119f8 Duration: 1.98 ms Billed Duration: 2 ms Memory Size: 128 MB Max Memory Used: 32 MB
```

Request ID efa4b7a6-4876-4478-bcfb-e304307119f8

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

Experiment 12

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

Step 1: Create a S3 bucket that will store the objects and will act as the trigger source for the Lambda function.

The screenshot shows the AWS S3 service page. On the left, there's a large banner with the text "Amazon S3" and "Store and retrieve any amount of data from anywhere". Below the banner, a section titled "How it works" features a placeholder image of a cloud with a camera icon. To the right of this, a "Create a bucket" call-to-action box contains the text: "Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored." At the bottom of this box is a prominent orange "Create bucket" button. The footer of the page includes standard AWS links like CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

This screenshot shows the "Create bucket" configuration page. The top navigation bar includes "Amazon S3 > Buckets > Create bucket". The main form is titled "Create bucket" with an "Info" link. It asks for a "Bucket name" (set to "anupritalambdabucket") and provides a note about unique naming. Below this, there's a section for "Copy settings from existing bucket - optional" with a note that only the bucket settings in the configuration are copied. The "General configuration" section includes fields for "AWS Region" (set to "US East (N. Virginia) us-east-1") and "Bucket type" (with "General purpose" selected). There are two options: "General purpose" (selected) and "Directory". The "General purpose" option is described as recommended for most use cases and access patterns, mentioning S3 Express One Zone storage class and redundancy across multiple Availability Zones. The "Directory" option is described as recommended for low-latency use cases, using only the S3 Express One Zone storage class. The footer of the page includes standard AWS links like CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

This screenshot shows the confirmation of a successfully created bucket. A green header bar says "Successfully created bucket 'anupritalambdabucket'". Below it, a message says "To upload files and folders, or to configure additional bucket settings, choose View details." The main content area shows the "Account snapshot - updated every 24 hours" and a "View Storage Lens dashboard" button. Under "General purpose buckets", there is one entry: "anupritalambdabucket" (1). This entry includes a "C" icon, "Copy ARN", "Empty", "Delete", and a "Create bucket" button. Below this is a search bar and a table with columns: Name, AWS Region, IAM Access Analyzer, and Creation date. The table shows one row for "anupritalambdabucket". The footer of the page includes standard AWS links like CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

Step 2: Now, create a Lambda function using AWS Lambda's console and choose the runtime environment as Python.

The screenshot shows the 'Create function' wizard in the AWS Lambda console. The 'Author from scratch' option is selected. In the 'Basic information' section, the function name is set to 'anupritaimageloader'. The runtime is chosen as 'Python 3.12'. The architecture is set to 'Lambda@edge'. At the bottom, there are links for CloudShell, Feedback, and navigation icons.

The screenshot shows the 'Function overview' page for the 'anupritaimageloader' function. The function name is displayed at the top. On the left, there is a 'Diagram' tab showing a single function icon labeled 'anupritaimageloader' and a 'Layers' section with '(0)'. On the right, there is a 'Description' section with fields for 'Last modified' (12 seconds ago), 'Function ARN' (arn:aws:lambda:us-east-1:856746069793:function:anupritaimageloader), and 'Function URL' (Info). At the bottom, there are links for CloudShell, Feedback, and navigation icons.

Step 3: Add the following code to set up the trigger.

The screenshot shows the code editor for the 'anupritaimageloader' function. The 'Code' tab is selected. The code in the editor is:

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

At the top, there are tabs for Code, Test, Monitor, Configuration, Aliases, and Versions. There are also buttons for Test, Deploy, and Changes not deployed. On the left, there is an Environment sidebar. At the bottom, there are links for CloudShell, Feedback, and navigation icons.

Step 4: Link the S3 bucket to the Lambda function by setting up a trigger.

AWS Services Search [Alt+S] N. Virginia v vclabs/user3413602-MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793

Lambda > Add triggers

Add trigger

Trigger configuration Info

S3 aws asynchronous storage

Bucket Choose or enter the ARN of an S3 bucket that serves as the event source. The bucket must be in the same region as the function.

s3/anupritalambdabucket

Bucket region: us-east-1

Event types Select the events that you want to trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.

All object create events

Prefix - optional Enter a single optional prefix to limit the notifications to objects with keys that start with matching characters. Any [special characters](#) must be URL encoded.

e.g. images/

Suffix - optional Enter a single optional suffix to limit the notifications to objects with keys that end with matching characters. Any [special characters](#) must be URL encoded.

e.g. jpg

Recursive invocation If your function writes objects to an S3 bucket, ensure that you are using different S3 buckets for input and output. Writing to the same bucket increases the risk of creating a recursive invocation, which can result in increased Lambda usage and increased costs. [Learn more](#)

I acknowledge that using the same S3 bucket for both input and output is not recommended and that this configuration can cause recursive invocations, increased Lambda usage, and increased costs.

Lambda will add the necessary permissions for AWS S3 to invoke your Lambda function from this trigger. [Learn more](#) about the Lambda permissions model.

Cancel

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

All object create events

Prefix - optional Enter a single optional prefix to limit the notifications to objects with keys that start with matching characters. Any [special characters](#) must be URL encoded.

e.g. images/

Suffix - optional Enter a single optional suffix to limit the notifications to objects with keys that end with matching characters. Any [special characters](#) must be URL encoded.

e.g. jpg

Recursive invocation If your function writes objects to an S3 bucket, ensure that you are using different S3 buckets for input and output. Writing to the same bucket increases the risk of creating a recursive invocation, which can result in increased Lambda usage and increased costs. [Learn more](#)

I acknowledge that using the same S3 bucket for both input and output is not recommended and that this configuration can cause recursive invocations, increased Lambda usage, and increased costs.

Lambda will add the necessary permissions for AWS S3 to invoke your Lambda function from this trigger. [Learn more](#) about the Lambda permissions model.

Cancel

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

Lambda > Functions > anupritaimageloader

anupritaimageloader

The trigger anupritalambdabucket was successfully added to function anupritaimageloader. The function is now receiving events from the trigger.

Function overview Export to Application Composer

Diagram

anupritaimageloader

S3

Description -

Last modified 11 minutes ago

Function ARN arn:aws:lambda:us-east-1:856746069793:function:anupritaimageloader

Function URL

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

The screenshot shows the AWS Lambda Configuration page. On the left, a sidebar lists options like General configuration, Triggers, Permissions, Destinations, Function URL, Environment variables, Tags, VPC, RDS databases, Monitoring and operations tools, and Concurrency and recursion detection. The 'Triggers' option is selected. The main panel displays a 'Triggers (1) info' section with a table. The table has one row for 'Trigger' with a checkbox, a file icon, and the name '53: anupralambdabucket'. Below the table is a 'Details' link. At the top of the main panel are buttons for 'C' (Copy), 'Fix errors', 'Edit', 'Delete', and 'Add trigger'. A search bar at the top says 'Find triggers'.

Step 5: Setup the required permissions.

The screenshot shows the AWS Lambda Configuration page. The sidebar shows the 'Permissions' option is selected. The main panel has a 'Execution role' section with a 'Role name' field containing 'LabRole'. Below it is a 'Resource summary' section with a warning message: 'User: arn:aws:sts::856746069793:assumed-role/voclabs/user3413602-MHAPANKAR_ANUPRITA_ANAND is not authorized to perform: iam:GetPolicy on resource: policy arnaws:iam::856746069793:policy/c127334a3201310l7262874t1w856746069793-VocLabPolicy2-r1u3cL4wT61 with an explicit deny in an identity-based policy'. There is also a 'Resource-based policy statements (1) info' section with a table and a 'View policy', 'Edit', 'Delete', and 'Add permissions' button.

The screenshot shows the AWS Lambda Configuration page. The sidebar shows the 'Permissions' option is selected. The main panel has a 'Resource-based policy statements (1) info' section with a table. The table has one row for 'lambda-77a4339c-2...', with columns for Statement ID, Principal, PrincipalOrgID, Conditions, and Action. The principal is 's3.amazonaws.com'. The conditions are 'StringEquals, ArnLike'. The action is 'lambda:InvokeFunction'. Below the table is an 'Auditing and compliance' section with a note about AWS CloudTrail logging invocations for auditing.

Step 6: 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.

Screenshot of the AWS S3 console showing the bucket 'anupritalambdabucket'. The left sidebar shows various AWS services like Access Grants, Object Lambda Access Points, and Storage Lens. The main area displays the 'Objects' tab with 0 objects. Buttons for 'Create folder' and 'Upload' are present. A note says 'No objects' and 'You don't have any objects in this bucket.' The bottom navigation bar includes CloudShell and Feedback.

Screenshot of the AWS S3 console showing the 'Upload' interface for the 'anupritalambdabucket'. It shows a dashed box for dragging files, a table of files (1 Total, 77.9 KB) including 'image.png', and a 'Destination' section. The bottom navigation bar includes CloudShell and Feedback.

Screenshot of the AWS S3 console showing the results of the upload. A green header bar says 'Upload succeeded'. The 'Summary' table shows 1 file uploaded successfully. The 'Files and folders' table lists 'image.png' with a status of 'Succeeded'. The bottom navigation bar includes CloudShell and Feedback.

AWS Services Search [Alt+S] N. Virginia vclabs/user3413602-MHAPANKAR_ANUPRITA_ANAND @ 8567-4606-9793

CloudWatch X

Favorites and recent

CloudWatch

Log groups

Log Anomalies

Live Tail

Logs Insights

Contributor Insights

Metrics

X-Ray traces

Events

Application Signals New

Network monitoring

CloudShell Feedback

CloudWatch > Log groups > /aws/lambda/anupritaimageloader > 2024/10/03/[LATEST]0a6fc5cf1df4b1bb2dc48e6d2640982

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Filter events - press enter to search 1m 1h UTC timezone Display

Timestamp	Message
No older events at this moment. Retry	
2024-10-03T09:38:34.628Z	INIT_START Runtime Version: python:3.12.v36 Runtime Version ARN: arn:aws:lambda:us-east-1::runtime:1...
2024-10-03T09:38:34.731Z	START RequestId: 65b9c8c2-fd60-42b1-b8cd-839a9acaba0d Version: \$LATEST
2024-10-03T09:38:34.733Z	END RequestId: 65b9c8c2-fd60-42b1-b8cd-839a9acaba0d Duration: 1.70 ms Billed Duration: 2 ms Memor...
2024-10-03T09:38:34.733Z	REPORT RequestId: 65b9c8c2-fd60-42b1-b8cd-839a9acaba0d Duration: 1.70 ms Billed Duration: 2 ms Memor...
No newer events at this moment. Auto retry paused. Resume	

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