

Advanced DevOps Experiment-1

Sanket More

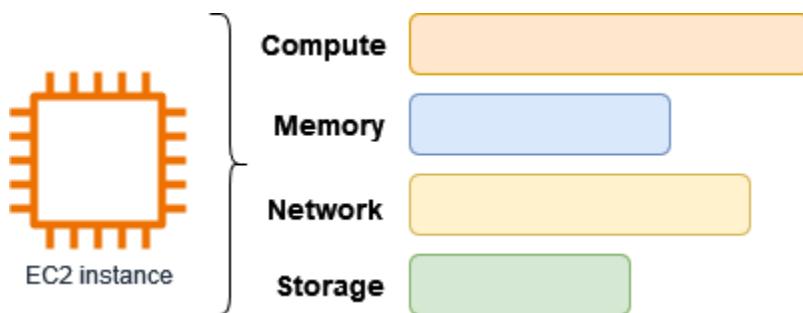
D15A 30

Aim: Using AWS CodePipeline, deploy Sample Application on EC2 instance using AWS CodeDeploy.

Theory:-

Amazon Elastic Compute Cloud (Amazon EC2) provides on-demand, scalable computing capacity in the Amazon Web Services (AWS) Cloud. Using Amazon EC2 reduces hardware costs so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. You can add capacity (scale up) to handle compute-heavy tasks, such as monthly or yearly processes, or spikes in website traffic. When usage decreases, you can reduce capacity (scale down) again.

An EC2 instance is a virtual server in the AWS Cloud. When you launch an EC2 instance, the instance type that you specify determines the hardware available to your instance. Each instance type offers a different balance of compute, memory, network, and storage resources. For more information, see the [Amazon EC2 Instance Types Guide](#).



Features of Amazon EC2

Amazon EC2 provides the following high-level features:

Instances

Virtual servers.

Amazon Machine Images (AMIs)

Preconfigured templates for your instances that package the components you need for your server (including the operating system and additional software).

Instance types

Various configurations of CPU, memory, storage, networking capacity, and graphics hardware for your instances.

Amazon EBS volumes

Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS).

Instance store volumes

Storage volumes for temporary data that is deleted when you stop, hibernate, or terminate your instance.

Key pairs

Secure login information for your instances. AWS stores the public key and you store the private key in a secure place.

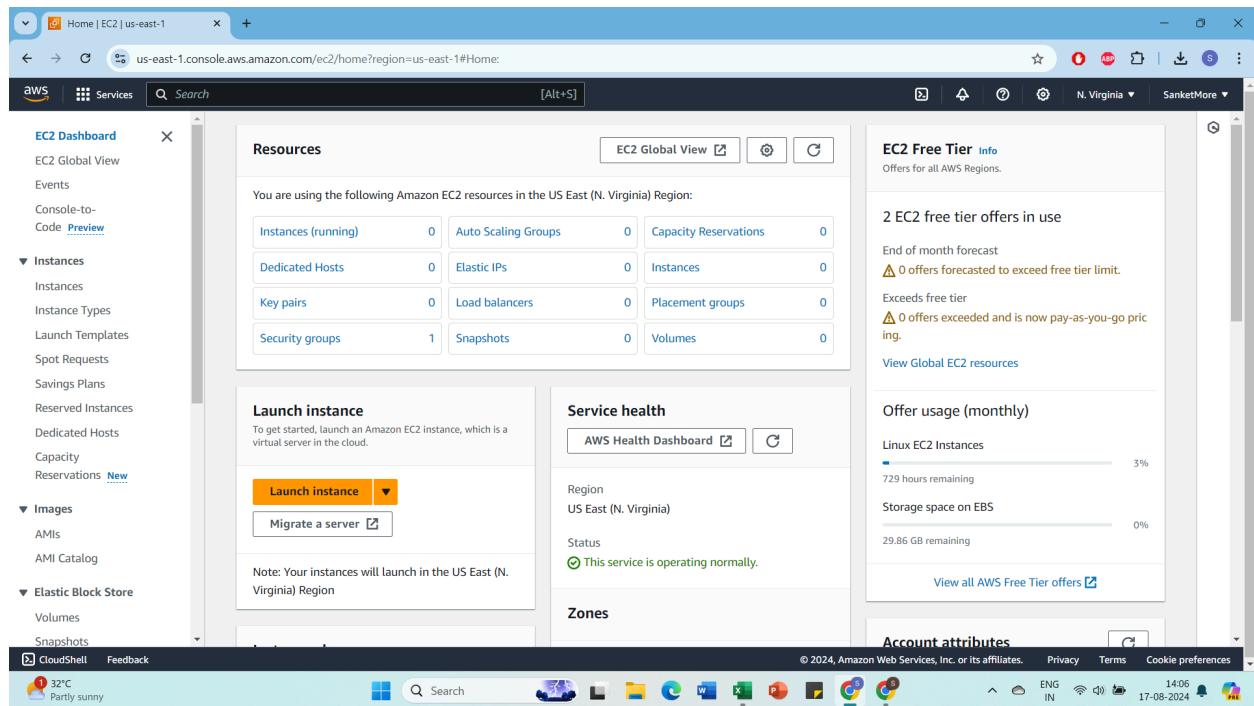
Security groups

A virtual firewall that allows you to specify the protocols, ports, and source IP ranges that can reach your instances, and the destination IP ranges to which your instances can connect.

Amazon EC2 supports the processing, storage, and transmission of credit card data by a merchant or service provider, and has been validated as being compliant with Payment Card Industry (PCI) Data Security Standard (DSS). For more information about PCI DSS, including how to request a copy of the AWS PCI Compliance Package, see [PCI DSS Level 1](#).

Implementation:-

EC2 Instance creation:



Launch an instance | EC2 | us-east-1

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

EC2 Services Search [Alt+S]

Amazon N. Virginia SanketMore

Instances Launch an instance

Launch an instance Info

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

Name and tags Info

Name: My_instance Add additional tags

Application and OS Images (Amazon Machine Image) Info

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

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

Quick Start

CloudShell Feedback 32°C Partly sunny © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 14:07 17-08-2024

Summary

Number of instances Info: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.5.2... read more
ami-0ae8f15ae6fe8cda

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

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

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch instance Review commands

Launch an instance | EC2 | us-east-1

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

EC2 Services Search [Alt+S]

Amazon N. Virginia SanketMore

CloudShell Feedback 32°C Partly sunny © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 14:08 17-08-2024

Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Li

AWS Mac ubuntu Microsoft Red Hat SUSE Li

Browse more AMIs Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible
ami-0ae8f15ae6fe8cda (64-bit (x86), uefi-preferred) / ami-0e36db3a3a535e401 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Architecture: 64-bit (x86) Boot mode: uefi-preferred AMI ID: ami-0ae8f15ae6fe8cda Verified provider

Instance type Info | Get advice

Summary

Number of instances Info: 1

Firewall (security group): New security group

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

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch instance Review commands

The screenshot shows the AWS CloudShell interface with two tabs open:

- Launch an instance | EC2 | us-east-1**: This tab displays the configuration for launching an EC2 instance. It includes sections for "Configure storage" (root volume of 8 GiB gp3), "Advanced details" (Free tier information), and a summary showing 1 instance launched. A tooltip for the Free tier provides details about usage included in the free tier.
- Course Invitation - 2022.sanket**: This tab shows the AWS Lambda function "Launch an instance" has been successfully executed, with the message "Successfully initiated launch of instance (i-058a79978ba0d38ae)". Below this, there is a "Next Steps" section with links to "Create billing and free tier usage alerts", "Connect to your instance", "Connect an RDS database", and "Create EBS snapshot policy".

The AWS CloudShell interface at the bottom of the screen also shows the Lambda function "Launch an instance" has been run successfully.

Screenshot of the AWS EC2 Instances page showing a single instance named "My-Website" (i-058a79978ba0d38ae) in the "Running" state.

The "Details" tab is selected, displaying the following information:

Instance ID	Public IPv4 address	Private IPv4 addresses
i-058a79978ba0d38ae (My-Website)	35.173.204.195 open address	172.31.36.30
IPv6 address	Instance state	Public IPv4 DNS
-	Running	ec2-35-173-204-195.compute-1.amazonaws.com

The "Connect" tab is selected in the main header, showing the following options:

- EC2 Instance Connect** (selected)
- Session Manager
- SSH client
- EC2 serial console

A warning message is displayed: "Port 22 (SSH) is open to all IPv4 addresses". It explains that 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](#).

Other tabs include "Status and alarms", "Monitoring", "Security", "Networking", "Storage", and "Tags".

CloudShell and Feedback buttons are visible at the bottom left. The status bar shows the date (08-08-2024), time (13:02), and location (N. Virginia). A weather icon indicates 31°C and mostly cloudy.

Static website hosting using EC2:-

```
See "man sudo_root" for details.

ubuntu@ip-172-31-41-61:~$ sudo su
root@ip-172-31-41-61:/home/ubuntu# sudo apt install
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@ip-172-31-41-61:/home/ubuntu# sudo apt-get update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [294 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [3768 B]
Get:9 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [250 kB]
Get:10 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [108 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [8632 B]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [9412 B]

Reading package lists... Done
root@ip-172-31-41-61:/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 libaprutil1 libaprutil1-db5 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libaprutil1 libaprutil1-db5 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 53 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]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-db5-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]

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-172-31-41-61:/home/ubuntu# systemctl status apache2
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
  Active: active (running) since Sun 2024-08-18 12:30:09 UTC; 30s ago
    Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2442 (apache2)
      Tasks: 55 (limit: 1130)
     Memory: 5.4M (peak: 5.7M)
        CPU: 40ms
       CGroup: /system.slice/apache2.service
           └─2442 /usr/sbin/apache2 -k start
              ├─2445 /usr/sbin/apache2 -k start
              └─2446 /usr/sbin/apache2 -k start

Aug 18 12:30:09 ip-172-31-41-61 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Aug 18 12:30:09 ip-172-31-41-61 systemd[1]: Started apache2.service - The Apache HTTP Server.
root@ip-172-31-41-61:/home/ubuntu# cd /var/www/html
root@ip-172-31-41-61:/var/www/html# 
```

EC2 > Security Groups > sg-0e7811c687e701e30 - launch-wizard-7

sg-0e7811c687e701e30 - launch-wizard-7

Actions ▾

Details

Security group name	Security group ID	Description	VPC ID
launch-wizard-7	sg-0e7811c687e701e30	launch-wizard-7 created 2024-08-18T11:25:33.225Z	vpc-08963bc0f8afcd789
Owner	Inbound rules count	Outbound rules count	
608111999703	1 Permission entry	1 Permission entry	

Inbound rules Outbound rules Tags

Inbound rules (1)

Search

C Manage tags Edit inbound rules

< 1 > ⚙

EC2 > Security Groups > sg-0896d82a58154b33d

sg-0896d82a58154b33d - launch-wizard-9

Actions ▾

Details

Security group name	Security group ID	Description	VPC ID
launch-wizard-9	sg-0896d82a58154b33d	launch-wizard-9 created 2024-08-18T12:21:13.480Z	vpc-08963bc0f8afcd789
Owner	Inbound rules count	Outbound rules count	
608111999703	3 Permission entries	1 Permission entry	

Inbound rules Outbound rules Tags

Inbound rules (3)

C Manage tags Edit inbound rules

Screenshot of the AWS VPC Security Group configuration page for launch-wizard-9.

Security group name	launch-wizard-9	Security group ID	sg-0896d82a58154b33d	Description	launch-wizard-9 created 2024-08-18T12:21:13.480Z	VPC ID	vpc-08963bc0f8afcd789
Owner	608111999703	Inbound rules count	3 Permission entries	Outbound rules count	1 Permission entry		

Navigation tabs: Inbound rules, Outbound rules (selected), Tags.

Outbound rules (1)

Search bar: Search

Name	Security group rule...	IP version	Type	Protocol
-	sgr-06dd7ee61f83e4e88	IPv4	All traffic	All

Browsing interface: Not secure 54.162.220.58

Apache2 Default Page

Ubuntu

It works!

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
```

DYNAMIC HOSTING ON EC2:

The screenshot shows the AWS CloudShell interface. At the top, there are several tabs: Course Invitation, Launch AWS Academy, Launch an instance, Instances | EC2, EC2 Instance Connect, moresaneket4003, and 35.173.204.195. The main area displays a terminal session on an Amazon Linux 2023 instance. The user has run the command `curl -I https://aws.amazon.com/linux/amazon-linux-2023`, which returns the expected headers for the Amazon Linux 2023 website.

```
[ec2-user@ip-172-31-36-30 ~]$ curl -I https://aws.amazon.com/linux/amazon-linux-2023
```

Below the terminal, the instance details are shown: i-058a79978ba0d38ae (My-Website), PublicIPs: 35.173.204.195, PrivateIPs: 172.31.36.30.

The screenshot shows the continuation of the AWS CloudShell session. The user runs `sudo su`, which fails because the command was not found. They then attempt to update the package manager and install httpd, but both commands fail due to requiring superuser privileges. Finally, they check the status of the httpd service and download a file from GitHub.

```
[ec2-user@ip-172-31-36-30 ~]$ sudo su
sudo: su: command not found
[ec2-user@ip-172-31-36-30 ~]$ yum update -y
Error: This command has to be run with superuser privileges (under the root user on most systems).
[ec2-user@ip-172-31-36-30 ~]$ yum install -y httpd
Error: This command has to be run with superuser privileges (under the root user on most systems).
[ec2-user@ip-172-31-36-30 ~]$ systemctl status httpd
Unit httpd.service could not be found.
[ec2-user@ip-172-31-36-30 ~]$ mkdir aws_assgl
[ec2-user@ip-172-31-36-30 ~]$ cd aws_assgl
[ec2-user@ip-172-31-36-30 aws_assgl]$ wget https://github.com/moresaneket4003/ip_Assignment_1.git
```

Below the terminal, the instance details are shown: i-058a79978ba0d38ae (My-Website), PublicIPs: 35.173.204.195, PrivateIPs: 172.31.36.30.

The screenshot shows the final state of the AWS CloudShell session. The user has completed the download of the GitHub repository to the /aws_assgl directory. The terminal window is closed, and the CloudShell interface is shown again with the same environment details at the bottom.

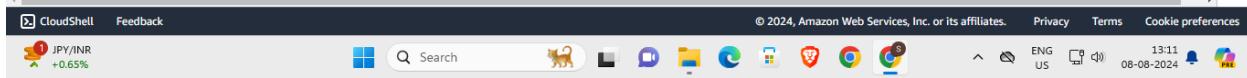
```
[ec2-user@ip-172-31-36-30 ~]$ yum update -y
Error: This command has to be run with superuser privileges (under the root user on most systems).
[ec2-user@ip-172-31-36-30 ~]$ yum install -y httpd
Error: This command has to be run with superuser privileges (under the root user on most systems).
[ec2-user@ip-172-31-36-30 ~]$ systemctl status httpd
Unit httpd.service could not be found.
[ec2-user@ip-172-31-36-30 ~]$ mkdir aws_assgl
[ec2-user@ip-172-31-36-30 ~]$ cd aws_assgl
[ec2-user@ip-172-31-36-30 aws_assgl]$ wget https://github.com/moresanket4003/ip_Assignment_1.git
--2024-08-08 07:41:09-- https://github.com/moresanket4003/ip_Assignment_1.git
Resolving github.com (github.com)... 140.82.113.3
Connecting to github.com (github.com)|140.82.113.3|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/moresanket4003/ip_Assignment_1 [following]
--2024-08-08 07:41:09-- https://github.com/moresanket4003/ip_Assignment_1
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'ip_Assignment_1.git'

ip_Assignment_1.git          [ <=>                               ] 253.04K  --.-KB/s   in 0.01s

2024-08-08 07:41:09 (18.2 MB/s) - 'ip_Assignment_1.git' saved [259108]
```

i-058a79978ba0d38ae (My-Website)

PublicIPs: 35.173.204.195 PrivateIPs: 172.31.36.30



```
[ec2-user@ip-172-31-36-30 ~]$ systemctl status httpd
Unit httpd.service could not be found.
[ec2-user@ip-172-31-36-30 ~]$ mkdir aws_assgl
[ec2-user@ip-172-31-36-30 ~]$ cd aws_assgl
[ec2-user@ip-172-31-36-30 aws_assgl]$ wget https://github.com/moresanket4003/ip_Assignment_1.git
--2024-08-08 07:41:09-- https://github.com/moresanket4003/ip_Assignment_1.git
Resolving github.com (github.com)... 140.82.113.3
Connecting to github.com (github.com)|140.82.113.3|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/moresanket4003/ip_Assignment_1 [following]
--2024-08-08 07:41:09-- https://github.com/moresanket4003/ip_Assignment_1
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'ip_Assignment_1.git'

ip_Assignment_1.git          [ <=>                               ] 253.04K  --.-KB/s   in 0.01s

2024-08-08 07:41:09 (18.2 MB/s) - 'ip_Assignment_1.git' saved [259108]

[ec2-user@ip-172-31-36-30 aws_assgl]$ ls -lrt
total 256
-rw-r--r--. 1 ec2-user ec2-user 259108 Aug  8 07:41 ip_Assignment_1.git
[ec2-user@ip-172-31-36-30 aws_assgl]$
```

i-058a79978ba0d38ae (My-Website)

PublicIPs: 35.173.204.195 PrivateIPs: 172.31.36.30



```
Course Invitation - 20 | Launch AWS Academy | Launch an instance | Instances | EC2 | us-east-1 | EC2 Instance Connect | moresaneket4003/ip_ | + | Error | us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-058a79978ba0d38ae&osUser=ec2-user&region=us-east-1&ssh... | S | Error | N. Virginia | vocabs/user3402836+MORE_SANKET_SATISH_@8774-7768-5784 |
```

2024-08-08 07:41:09 (18.2 MB/s) - 'ip_Assignment_1.git' saved [259108]

```
[ec2-user@ip-172-31-36-30 aws_assg1]$ ls -lrt
total 256
-rw-r--r--. 1 ec2-user ec2-user 259108 Aug 8 07:41 ip_Assignment_1.git
[ec2-user@ip-172-31-36-30 aws_assg1]$ wget https://github.com/moresaneket4003/ip_Assignment_1/archive/refs/heads/main.zip
--2024-08-08 07:51:14-- https://github.com/moresaneket4003/ip_Assignment_1/archive/refs/heads/main.zip
Resolving github.com (github.com)... 140.82.112.4
Connecting to github.com (github.com)|140.82.112.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/moresaneket4003/ip_Assignment_1/zip/refs/heads/main [following]
--2024-08-08 07:51:15-- https://codeload.github.com/moresaneket4003/ip_Assignment_1/zip/refs/heads/main
Resolving codeload.github.com (codeload.github.com)... 140.82.114.10
Connecting to codeload.github.com (codeload.github.com)|140.82.114.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: 'main.zip'

main.zip [ <=> ] 4.56M --.-KB/s in 0.05s
```



```
Course Invitation - 20 | Launch AWS Academy | Launch an instance | Instances | EC2 | us-east-1 | EC2 Instance Connect | moresaneket4003/ip_ | + | Error | us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-058a79978ba0d38ae&osUser=ec2-user&region=us-east-1&ssh... | S | Error | N. Virginia | vocabs/user3402836+MORE_SANKET_SATISH_@8774-7768-5784 |
```

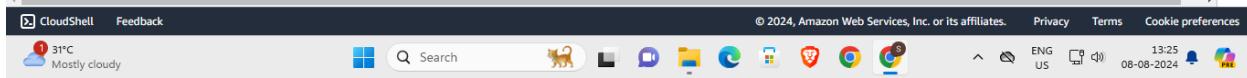
total 256
-rw-r--r--. 1 ec2-user ec2-user 259108 Aug 8 07:41 ip_Assignment_1.git
[ec2-user@ip-172-31-36-30 aws_assg1]\$ wget https://github.com/moresaneket4003/ip_Assignment_1/archive/refs/heads/main.zip
--2024-08-08 07:51:14-- https://github.com/moresaneket4003/ip_Assignment_1/archive/refs/heads/main.zip
Resolving github.com (github.com)... 140.82.112.4
Connecting to github.com (github.com)|140.82.112.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/moresaneket4003/ip_Assignment_1/zip/refs/heads/main [following]
--2024-08-08 07:51:15-- https://codeload.github.com/moresaneket4003/ip_Assignment_1/zip/refs/heads/main
Resolving codeload.github.com (codeload.github.com)... 140.82.114.10
Connecting to codeload.github.com (codeload.github.com)|140.82.114.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: 'main.zip'

main.zip [<=>] 4.56M --.-KB/s in 0.05s



```
[ec2-user@ip-172-31-36-30 aws_assgl]$ ls -lrt
total 4932
-rw-r--r--. 1 ec2-user ec2-user 259108 Aug  8 07:41 ip_Assignment_1.git
-rw-r--r--. 1 ec2-user ec2-user 4784447 Aug  8 07:51 main.zip
[ec2-user@ip-172-31-36-30 aws_assgl]$ unzip main.zip
Archive: main.zip
  creating: ip Assignment 1-main/
  inflating: ip Assignment 1-main/index.html
  inflating: ip Assignment 1-main/italian_recording1.mp4
  inflating: ip Assignment 1-main/menu_italian.jpg
[ec2-user@ip-172-31-36-30 aws_assgl]$ ls -lrt
total 4932
drwxr-xr-x. 2 ec2-user ec2-user    78 Aug  5 04:32 ip_Assignment_1-main
-rw-r--r--. 1 ec2-user ec2-user 259108 Aug  8 07:41 ip_Assignment_1.git
-rw-r--r--. 1 ec2-user ec2-user 4784447 Aug  8 07:51 main.zip
[ec2-user@ip-172-31-36-30 aws_assgl]$ cd^C
[ec2-user@ip-172-31-36-30 aws_assgl]$ cd ip_Assignment 1-main
[ec2-user@ip-172-31-36-30 ip_Assignment_1-main]$ ls -lrt
total 4788
-rw-r--r--. 1 ec2-user ec2-user 140394 Aug  5 04:32 menu_italian.jpg
-rw-r--r--. 1 ec2-user ec2-user 4746438 Aug  5 04:32 italian_recording1.mp4
-rw-r--r--. 1 ec2-user ec2-user 10887 Aug  5 04:32 index.html
[ec2-user@ip-172-31-36-30 ip_Assignment_1-main]$ 
```

i-058a79978ba0d38ae (My-Website)
PublicIPs: 35.173.204.195 PrivateIPs: 172.31.36.30



```
[ec2-user@ip-172-31-36-30 aws_assgl]$ ls -lrt
total 4932
-rw-r--r--. 1 root root 259108 Aug  8 08:03 ip_Assignment_1.git
-rw-r--r--. 1 root root 4784447 Aug  8 08:04 main.zip
[root@ip-172-31-36-30 aws_assgl]$ unzip main.zip
Archive: main.zip
  creating: ip Assignment 1-main/
  inflating: ip Assignment 1-main/index.html
  inflating: ip Assignment 1-main/italian_recording1.mp4
  inflating: ip Assignment 1-main/menu_italian.jpg
[root@ip-172-31-36-30 aws_assgl]$ ls -lrt
total 4932
drwxr-xr-x. 2 root root    78 Aug  5 04:32 ip_Assignment_1-main
-rw-r--r--. 1 root root 259108 Aug  8 08:03 ip_Assignment_1.git
-rw-r--r--. 1 root root 4784447 Aug  8 08:04 main.zip
[root@ip-172-31-36-30 aws_assgl]$ cd ip_Assignment 1-main
[root@ip-172-31-36-30 ip_Assignment_1-main]$ ls -lrt
total 4788
-rw-r--r--. 1 root root 140394 Aug  5 04:32 menu_italian.jpg
-rw-r--r--. 1 root root 4746438 Aug  5 04:32 italian_recording1.mp4
-rw-r--r--. 1 root root 10887 Aug  5 04:32 index.html
[root@ip-172-31-36-30 ip_Assignment_1-main]$ mv * /var/www/html
[root@ip-172-31-36-30 ip_Assignment_1-main]$ cd /var/www/html
[root@ip-172-31-36-30 html]$ 
```

i-058a79978ba0d38ae (My-Website)
PublicIPs: 35.173.204.195 PrivateIPs: 172.31.36.30



Course Invitations | Launch AWS | Launch an instance | Instances | EC2 Instances | moreanket@ip-172-31-36-30 | 172.31.36.30 | Restaurant Frontend | Error

us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-058a79978ba0d38ae&cosUser=ec2-user®ion=us-east-1&sshPort=... N. Virginia vocabs/user3402836+MORE_SANKET_SATISH_@ 8774-7768-5784

```
[root@ip-172-31-36-30 ip_Assignment_1-main]# ls -lrt
total 4788
-rw-r--r--. 1 root root 140394 Aug 5 04:32 menu_italian.jpg
-rw-r--r--. 1 root root 4746438 Aug 5 04:32 italian_recording1.mp4
-rw-r--r--. 1 root root 10887 Aug 5 04:32 index.html
[root@ip-172-31-36-30 ip_Assignment_1-main]# mv * /var/www/html/
mv: overwrite '/var/www/html/index.html'?
mv: overwrite '/var/www/html/italian_recording1.mp4'?
mv: overwrite '/var/www/html/menu_italian.jpg'?
[root@ip-172-31-36-30 ip_Assignment_1-main]# cd /var/www/html
[root@ip-172-31-36-30 html]# ls -lrt
total 4788
-rw-r--r--. 1 root root 140394 Aug 5 04:32 menu_italian.jpg
-rw-r--r--. 1 root root 4746438 Aug 5 04:32 italian_recording1.mp4
-rw-r--r--. 1 root root 10887 Aug 5 04:32 index.html
[root@ip-172-31-36-30 html]# systemctl status httpd
● httpd.service - The Apache HTTP Server
    Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
      Active: inactive (dead)
        Docs: man:httpd.service(8)
[root@ip-172-31-36-30 html]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@ip-172-31-36-30 html]# systemctl start httpd
[root@ip-172-31-36-30 html]# 
```

i-058a79978ba0d38ae (My-Website)

PublicIPs: 35.173.204.195 PrivateIPs: 172.31.36.30

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 14:37 08-08-2024

Course Invitations | Launch AWS | Launch an instance | Instances | EC2 Instances | moreanket@ip-172-31-36-30 | 172.31.36.30 | Restaurant Frontend | Error

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances: N. Virginia vocabs/user3402836+MORE_SANKET_SATISH_@ 8774-7768-5784

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 14:37 08-08-2024

Instances (1/1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
My-Website	i-058a79978ba0d38ae	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1c

i-058a79978ba0d38ae (My-Website)

- s copied
- 35.173.204.195 [Public IP]
- VPC ID: vpc-01ae12dcbe2a5aeb9
- AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations.
- Subnet ID: subnet-0c208f956e5d78d6a
- Auto Scaling Group name: -
- IAM Role: -
- Instance ARN: -
- IMDSv2 Required

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 14:37 08-08-2024

Inbound security group rules successfully modified on security group (sg-02b121f0bd66ade84 | launch-wizard-2)

Security Groups (3) info

Name	Security group ID	Security group name	VPC ID
-	sg-02b121f0bd66ade84	launch-wizard-2	vpc-01ae12dcbe2a5aeb9
-	sg-0a0160a47f50d0f2	default	vpc-01ae12dcbe2a5aeb9
-	sg-027d77b5cc42040b	Launch wizard-1	vpc-01ae12dcbe2a5aeb9

Inbound rules (3)

Name	Security group rule...	IP version	Type	Protocol
sgr-0e6522ac562f26628	SSH	TCP	22	Cust... 0.0.0.0/0
sgr-08d998234f9b3b741	HTTP	TCP	80	Cust... 0.0.0.0/0
sgr-0b658bfd4a867c65f	HTTPS	TCP	443	Cust... 0.0.0.0/0

Edit inbound rules

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

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-0e6522ac562f26628	SSH	TCP	22	Cust... 0.0.0.0/0	
sgr-08d998234f9b3b741	HTTP	TCP	80	Cust... 0.0.0.0/0	
sgr-0b658bfd4a867c65f	HTTPS	TCP	443	Cust... 0.0.0.0/0	

The screenshot shows a web browser window with the following details:

- Address Bar:** Shows the URL `35.173.204.195` and a "Not secure" warning.
- Content Area:**
 - Logo:** A white square containing a green spoon, a grey fork, and a red knife.
 - Text:** "ITALIAN" in large bold letters, "FOOD" in smaller letters below it.
 - Section:** "Restaurant Reservation Portal".
 - Navigation:** Links for "Home", "Menu", "Reservation", and "Contact Us".
 - Offer Section:** "Special Offers" with links for "Happy Hour" and "Weekend Special".
 - Welcome Message:** "Welcome to Italian Food, where the essence of Italy comes alive in every dish. Nestled in the heart of Thane, our restaurant offers a delightful escape to the enchanting".
- Taskbar:** Shows the Windows Start button, a search bar, pinned icons for File Explorer, Edge, File History, Task View, and Google Chrome, system tray icons for battery, signal, and volume, and a date/time indicator (14:37, 08-08-2024).

STATIC WEBSITE HOSTING USING S3 BUCKET:

The screenshot shows the AWS S3 'Create bucket' wizard in three sequential steps:

- Step 1: General configuration**
 - AWS Region:** Europe (Stockholm) eu-north-1
 - Bucket type:** General purpose (Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.)
 - Bucket name:** Sanket_Bucket_1
 - Copy settings from existing bucket - optional:** Only the bucket settings in the following configuration are copied.
- Step 2: Default encryption**
 - Encryption type:** Server-side encryption with Amazon S3 managed keys (SSE-S3)
 - Bucket Key:** Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)
 - Bucket Key status:** Enable
- Step 3: Advanced settings**
 - Note:** After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Buttons at the bottom: Cancel, Create bucket

S3 buckets | S3 | eu-north-1

eu-north-1.console.aws.amazon.com/s3/buckets?region=eu-north-1&bucketType=general

Services Search [Alt+S]

Amazon S3 > Buckets

Successfully created bucket "sanket-bucket1"
To upload files and folders, or to configure additional bucket settings, choose View details.

View details

Amazon S3 > Buckets

▶ Account snapshot - updated every 24 hours All AWS Regions

Storage lens provides visibility into storage usage and activity trends. Learn more

View Storage Lens dashboard

General purpose buckets (2) Info All AWS Regions

Buckets are containers for data stored in S3.

Find buckets by name

Name AWS Region IAM Access Analyzer Creation date

Name	AWS Region	IAM Access Analyzer	Creation date
elasticbeanstalk-eu-north-1-869935102438	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	August 15, 2024, 16:27:46 (UTC+05:30)
sanket-bucket1	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	August 19, 2024, 17:22:35 (UTC+05:30)

CloudShell Feedback

31°C Mostly cloudy

Search

eu-north-1.console.aws.amazon.com/s3/upload/sanket-bucket1?region=eu-north-1&bucketType=general

Services Search [Alt+S]

Upload objects - S3 bucket sanket-bucket1

All files and folders in this table will be uploaded.

Find by name

Name	Folder	Type
pic1.jpg		image/jpeg

Files and folders (2 Total, 47.8 KB)

Remove Add files Add folder

Destination Info

Destination s3://sanket-bucket1

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

Permissions Grant public access and access to other AWS accounts.

Properties Specify storage class, encryption settings, tags, and more.

Cancel Upload

CloudShell Feedback

31°C Mostly cloudy

Search

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

ENG IN 17:22 19-08-2024

Upload objects - S3 bucket sanketbucket1

eu-north-1.console.aws.amazon.com/s3/upload/sanket-bucket1?region=eu-north-1&bucketType=general

Amazon S3 > Buckets > sanket-bucket1 > Upload

Upload

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

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

Files and folders (2 Total, 47.8 KB)		
All files and folders in this table will be uploaded.		
<input type="text"/> Find by name		
<input type="checkbox"/>	Name	Folder
<input type="checkbox"/>	index21.html	text/html
<input type="checkbox"/>	pic1.jpg	image/jpeg

Destination

CloudShell Feedback

31°C Mostly cloudy

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

ENG IN 17:23 19-08-2024

Upload objects - S3 bucket sanketbucket1

eu-north-1.console.aws.amazon.com/s3/upload/sanket-bucket1?region=eu-north-1&bucketType=general

Amazon S3 > Buckets > sanket-bucket1 > Upload

Upload succeeded

View details below.

Summary

Destination	Succeeded	Failed
s3://sanket-bucket1	2 files, 47.8 KB (100.00%)	0 files, 0 B (0%)

Files and folders Configuration

Files and folders (2 Total, 47.8 KB)

Files and folders (2 Total, 47.8 KB)						
<input type="text"/> Find by name						
Name	Folder	Type	Size	Status	Error	
index21.htm...	-	text/html	3.8 KB	Successed	-	
pic1.jpg	-	image/jpeg	44.0 KB	Successed	-	

CloudShell Feedback

31°C Mostly cloudy

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

ENG IN 17:24 19-08-2024

The screenshot shows the AWS S3 console interface. At the top, the URL is eu-north-1.console.aws.amazon.com/s3/buckets/sanket-bucket1?region=eu-north-1&bucketType=general&tab=objects. Below the header, there's a navigation bar with 'Amazon S3' and 'Buckets'. The main area is titled 'sanket-bucket1' with an 'Info' link. A horizontal menu bar includes 'Objects' (which is selected), 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' section displays a table with two rows:

	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	index21.html	html	August 19, 2024, 17:24:08 (UTC+05:30)	3.8 KB	Standard
<input type="checkbox"/>	pic1.jpg	jpg	August 19, 2024, 17:24:09 (UTC+05:30)	44.0 KB	Standard

The screenshot shows a web browser window with a custom T-shirt order form. The URL is sanket-bucket1.s3.eu-north-1.amazonaws.com/index21.html?response-content-disposition=inline&X-Amz-Security-Token=IQoJb3jPZ2luX2VjEDwaCmV1LW5vcnRoLTEiRjBEAh... The page has a header with 'CloudShell' and 'Feedback' buttons, weather information (31°C, Mostly cloudy), and a search bar. The main content is a form with several sections:

- T-shirt Customization**: Fields for Tagline on the Shirt (text input), Color (dropdown), Size (dropdown), Quantity (input: 1), and Delivery Date (date input).
- Delivery Details**: Fields for Recipient's Name, Address, Email, and Phone Number.
- Order Summary**: Total Cost (\$20.00) and Shipping Method (dropdown).
- Additional Comments**: A text area for entering additional comments or special requests.

At the bottom are 'Place Order' and 'Reset Form' buttons.



CLOUD 9 HOSTING:

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.

AWS Cloud9 > Environments > SnehalEnv

SnehalEnv

[Delete](#) [Open in Cloud9](#)

Details [Edit](#)

Name SnehalEnv	Owner ARN <code>arn:aws:sts::608111999703:assumed-role/voclabs/user3402712-PATIL_SHRAVANI_ANIL</code>	Status Ready
Description -	Number of members 1	Lifecycle status Created
Environment type EC2 instance		

Creating SnehalEnv. This can take several minutes. While you wait, see [Best practices for using AWS Cloud9](#).

For capabilities similar to AWS Cloud9, explore AWS Toolkits in your own IDE and AWS CloudShell in the AWS Management Console. [Find out more](#)

AWS Cloud9 > Environments

Environments (1)

Name	Cloud9 IDE	Environment type	Connection	Permission	Owner ARN
SnehalEnv	Open	EC2 instance	Secure Shell (SSH)	Owner	arn:aws:sts::608111999703:assumed-role/voclabs/user3402712=PATIL_SHRAVANI_ANIL

Go to Anything (Ctrl-P)

SnehalEnv - /home

cloud9.html

README.md

Welcome

AWS Cloud9

Welcome to your development environment

AWS Cloud9 allows you to write, run, and debug your code with just a browser. You can [tour the IDE](#), write code for [AWS Lambda](#) and [Amazon API Gateway](#), share your IDE with others in real time, and much more.

Developer Tools

Getting started

Create File

Upload Files...

Toolkit for AWS Cloud9

bash - 172.31.42.231.x Immediate

voclabs:~/environment \$

User details

User name

Snehal

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

Provide user access to the AWS Management Console - optional

If you're providing console access to a person, it's a **best practice** [to manage their access in IAM Identity Center](#).

Console password

Autogenerated password

You can view the password after you create the user.

Custom password

Enter a custom password for the user.

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _ + - (hyphen) = [] { } | '

Permissions options

Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.



Get started with groups

Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

[Create group](#)

► Set permissions boundary - optional

[Cancel](#)

[Previous](#)

[Next](#)

Create user group

X

Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

User group name

Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+,.,@-_ ' characters.

Permissions policies (952)



Create policy

Filter by Type

All ty... ▾

< 1 2 3 4 5 6 7 ... 48 >



Policy name	Type	Use...	Description
AdministratorAccess	AWS managed	Permis...	Provides full access to AWS services an...
AdministratorAcce...	AWS managed	None	Grants account administrative permis...
AdministratorAcce...	AWS managed	None	Grants account administrative permis...
AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaFo...
AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusiness ...
AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to A...
AlexaForBusinessLi...	AWS managed	None	Provide access to Lifesize AVS devices
AlexaForBusinessP...	AWS managed	None	Provide access to Poly AVS devices
AlexaForBusinessR...	AWS managed	None	Provide read only access to AlexaForB...
AmazonAPIGatewa...	AWS managed	None	Provides full access to create/edit/delete...
AmazonACService...	AWS managed	None	Provides full access to invoke AWS Lambda

Cancel

Create user group

Advanced DevOps Experiment-2

Sanket More

D15A 30

Aim: Using AWS CodePipeline, deploy Sample Application on Elastic BeanStalk using AWS CodeDeploy.

Theory:-

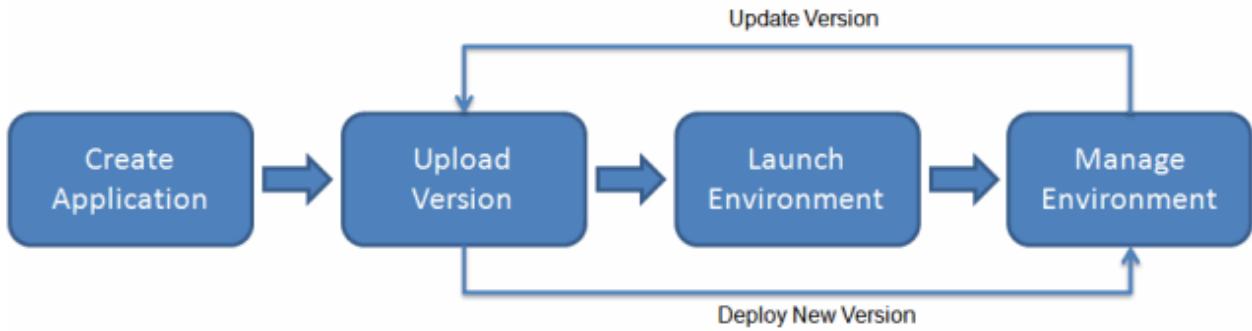
With Elastic Beanstalk you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications. Amazon Web Services (AWS) comprises over one hundred services, each of which exposes an area of functionality. While the variety of services offers flexibility for how you want to manage your AWS infrastructure, it can be challenging to figure out which services to use and how to provision them. Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

Elastic Beanstalk supports applications developed in Go, Java, .NET, Node.js, PHP, Python, and Ruby. Elastic Beanstalk also supports Docker platforms. With Docker containers you can choose your own programming language and application dependencies that may not be supported by the other Elastic Beanstalk platforms. When you deploy your application, Elastic Beanstalk builds the selected supported platform version and provisions one or more AWS resources, such as Amazon EC2 instances, to run your application.

You can interact with Elastic Beanstalk by using the Elastic Beanstalk console, the AWS Command Line Interface (AWS CLI), or eb, a high-level CLI designed specifically for Elastic Beanstalk.

You can also perform most deployment tasks, such as changing the size of your fleet of Amazon EC2 instances or monitoring your application, directly from the Elastic Beanstalk web interface (console). To use Elastic Beanstalk, you create an application, upload an application version in the form of an application source bundle (for example, a Java .war file) to Elastic Beanstalk, and then provide some information about the application. Elastic Beanstalk automatically launches an environment and creates and configures the AWS resources needed to run your code. After

your environment is launched, you can then manage your environment and deploy new application versions. The following diagram illustrates the workflow of Elastic Beanstalk.



After you create and deploy your application, information about the application—including metrics, events, and environment status—is available through the Elastic Beanstalk console, APIs, or Command Line Interfaces, including the unified AWS CLI.

Implementation:-

Deploying basic web page on Elastic Beanstalk

The screenshot shows the 'Welcome | Elastic Beanstalk' page. The header includes tabs for 'Compute', 'Mobile', 'Machine Learning', 'Serverless', and 'CloudWatch'. Below the header, the main content features the 'Amazon Elastic Beanstalk' logo and the tagline 'End-to-end web application management.' A 'Get started' section explains the service's purpose: 'Easily deploy your web application in minutes.' It includes a 'Create application' button. Another 'Get started' section provides instructions for deployment. A 'Pricing' section states there's no additional charge for Elastic Beanstalk. At the bottom, there's a 'Getting started' link and a footer with links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences. The footer also shows system status icons and the date 15-08-2024.

Configure environment | Elastic eu-north-1.console.aws.amazon.com/elasticbeanstalk/home?region=eu-north-1#/create-environment

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 environment Info

Environment tier Info
Amazon Elastic Beanstalk has two types of environment tiers to support different types of web applications.

Web server environment
Run a website, web application, or web API that serves HTTP requests. [Learn more](#)

Worker environment
Run a worker application that processes long-running workloads on demand or performs tasks on a schedule. [Learn more](#)

Application information Info

Application name

Maximum length of 100 characters.

Application tags (optional)

Environment information Info
Choose the name, subdomain and description for your environment. These cannot be changed later.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 16:26 15-08-2024

Configure environment | Elastic eu-north-1.console.aws.amazon.com/elasticbeanstalk/home?region=eu-north-1#/create-environment

Step 6 Review

Maximum length of 100 characters.

Application tags (optional)

Environment information Info
Choose the name, subdomain and description for your environment. These cannot be changed later.

Environment name
 SanketApplication30-env
Must be from 4 to 40 characters in length. The name can contain only letters, numbers, and hyphens. It can't start or end with a hyphen. This name must be unique within a region in your account.

Domain
 Leave blank for autogenerated value .eu-north-1.elasticbeanstalk.com Check availability

Environment description

Platform Info

Platform type
 Managed platform

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 16:27 15-08-2024

Configure environment | Elastic Beanstalk | How to migrate from AWS CloudFormation

eu-north-1.console.aws.amazon.com/elasticbeanstalk/home?region=eu-north-1#/create-environment

Services Search [Alt+S]

Platform type

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

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

Platform

Python

Platform branch

Python 3.11 running on 64bit Amazon Linux 2023

Platform version

4.1.3 (Recommended)

Application code [Info](#)

Sample application

Existing version Application versions that you have uploaded.

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

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

Wi - SA in 3 hours ENG IN 16:36 15-08-2024

Configure service access | Elastic Beanstalk | How to migrate from AWS CloudFormation

eu-north-1.console.aws.amazon.com/elasticbeanstalk/home?region=eu-north-1#/create-environment

Services Search [Alt+S]

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

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](#)

Choose a key pair

[View permission details](#)

EC2 instance profile

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

[View permission details](#)

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

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

Wi - SA in 3 hours ENG IN 16:38 15-08-2024

Set up networking, database, and tags - optional

Virtual Private Cloud (VPC)

VPC
Launch your environment in a custom VPC instead of the default VPC. You can create a VPC and subnets in the VPC management console.
Learn more [\[Link\]](#)

vpc-09fa2c756cb7c77a5 | (172.31.0.0/16)

Create custom VPC [\[Link\]](#)

Instance settings

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

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

Activated

Instance subnets

Filter instance subnets

Availability Zone	Subnet	CIDR	Name
<input checked="" type="checkbox"/> eu-north-1c	subnet-03ae3ef60...	172.31.0.0/20	
<input checked="" type="checkbox"/> eu-north-1a	subnet-0d32b416...	172.31.16.0/20	
<input type="checkbox"/> eu-north-1b	subnet-0d6e656ff...	172.31.32.0/20	

Database info
Integrate an RDS SQL database with your environment. Learn more [\[Link\]](#)

Database subnets

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences Feels hotter Now ENG IN 16:39 15-08-2024 Stockholm SanktMore

Set up networking, database, and tags - optional

Virtual Private Cloud (VPC)

VPC
Launch your environment in a custom VPC instead of the default VPC. You can create a VPC and subnets in the VPC management console.
Learn more [\[Link\]](#)

scaling

Instance settings

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

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

Activated

Instance subnets

Filter instance subnets

Availability Zone	Subnet	CIDR	Name
<input checked="" type="checkbox"/> eu-north-1c	subnet-03ae3ef60...	172.31.0.0/20	
<input checked="" type="checkbox"/> eu-north-1a	subnet-0d32b416...	172.31.16.0/20	
<input type="checkbox"/> eu-north-1b	subnet-0d6e656ff...	172.31.32.0/20	

Database info
Integrate an RDS SQL database with your environment. Learn more [\[Link\]](#)

Database subnets

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences Feels hotter Now ENG IN 16:39 15-08-2024 Stockholm SanktMore

Configure instance traffic and scaling - optional

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

Instances Info

Configure the Amazon EC2 instances that run your application.

Root volume (boot device)

Root volume type: (Container default)

Size: 8 GB

IOPS: 100 IOPS

Throughput: 125 MiB/s

Amazon CloudWatch monitoring

The time interval between when metrics are reported from the EC2 instances

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 31°C Partly sunny Search Stockholm SanktMore

Configure instance traffic and scaling - optional

eu-north-1.console.aws.amazon.com/elasticbeanstalk/home?region=eu-north-1#/create-environment

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 31°C Partly sunny Search Stockholm SanktMore

Amazon CloudWatch monitoring

The time interval between when metrics are reported from the EC2 instances

Monitoring interval: 5 minute

Instance metadata service (IMDS)

Your environment's platform supports both IMDSv1 and IMDSv2. To enforce IMDSv2, deactivate IMDSv1. Learn more

IMDSv1: With the current setting, the environment enables only IMDSv2.
Deactivated

EC2 security groups

Select security groups to control traffic.

EC2 security groups (1)

Filter security groups

Group name	Group ID	Name
default	sg-026f1dc59cf2f7707	

Capacity Info

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 31°C Partly sunny Search Stockholm SanktMore

Configure updates, monitoring

eu-north-1.console.aws.amazon.com/elasticbeanstalk/home?region=eu-north-1#/create-environment

Rotating updates and deployments

Application deployments
Choose how Amazon Elastic Beanstalk propagates source code changes and software configuration updates. [Learn more](#)

Deployment policy
 All at once

Batch size type
 Percentage
 Fixed

Deployment batch size
100
% instances at a time

Configuration updates
Changes to virtual machine settings and VPC configuration trigger rolling updates to replace the instances in your environment without downtime. [Learn more](#)

Rolling update type
 Deactivated

Deployment preferences
Customize health check requirements and deployment timeouts.

Ignore health check
Don't fail deployments due to health check failures.

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

Configure instance traffic and scaling

eu-north-1.console.aws.amazon.com/elasticbeanstalk/home?region=eu-north-1#/create-environment

Auto scaling group

Environment type
Select a single-instance or load-balanced environment. You can develop and test an application in a single-instance environment to save costs and then upgrade to a load-balanced environment when the application is ready for production. [Learn more](#)

Single instance

Instances
1 Min
1 Max

Fleet composition
Spot instances are launched at the lowest available price. [Learn more](#)

On-Demand instance
 Spot instance

Maximum spot price
The maximum price per instance-hour, in USD, that you're willing to pay for a Spot Instance. Setting a custom price limits your chances to fulfill your target capacity using Spot Instances.

Default
 Set your maximum price

On-Demand base
The minimum number of On-Demand Instances that your Auto Scaling group provisions before considering Spot Instances as your environment scales out.

0

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

Configure environment - review

eu-north-1.console.aws.amazon.com/elasticbeanstalk/home?region=eu-north-1#/create-environment

aws Services Search [Alt+S]

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

Review Info

Step 1: Configure environment

Environment information

Environment tier	Application name
Web server environment	Sanket_Application_30
Environment name	Application code
SanketApplication30-env	Sample application
Platform	arm:aws:elasticbeanstalk:eu-north-1::platform/Python 3.11 running on 64bit Amazon Linux 2023/4.1.3

Step 2: Configure service access

Service access Info

Configure the service role and EC2 instance profile that Elastic Beanstalk uses to manage your environment. Choose an EC2 key pair to securely log in to your EC2 instances.

Service role EC2 instance profile

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

Wi - SA in 3 hours ENG IN 16:56 15-08-2024

Configure updates, monitoring, and logging - optional

eu-north-1.console.aws.amazon.com/elasticbeanstalk/home?region=eu-north-1#/create-environment

aws Services Search [Alt+S]

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 updates, monitoring, and logging - optional Info

Monitoring Info

Health reporting

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

System

Basic
 Enhanced

Health event streaming to CloudWatch Logs

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

Log streaming

Activated (standard CloudWatch charges apply.)

Retention

7

Lifecycle

Keep logs after terminating environment

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

31°C Partly sunny ENG IN 16:55 15-08-2024

Screenshot of the AWS Elastic Beanstalk Environment overview page for SanketApplication30-env.

The page shows the following details:

- Health:** Unknown
- Environment ID:** e-8dxvvdjawj
- Domain:** -
- Application name:** Sanket_Application_30

Platform: Python 3.11 running on 64bit Amazon Linux 2023/4.1.3

Events: (2) Info

Configuration:

Key	Value
PYTHONPATH	/var/app/venv/staging-LQM1lest/bin

Submit button.

Configure service access | Elastic Beanstalk | Create role | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles/create

AWS Services Search [Alt+S]

Global SanketMore

<input type="checkbox"/>	AWS-ElasticBeanstalkCustomPlatform...	AWS managed	Provide the instance in your custom pl...
<input type="checkbox"/>	AWS-ElasticBeanstalkEnhancedHealth	AWS managed	AWS Elastic Beanstalk Service policy f...
<input type="checkbox"/>	AWS-ElasticBeanstalkManagedUpdates...	AWS managed	This policy is for the AWS Elastic Beans...
<input checked="" type="checkbox"/>	AWS-ElasticBeanstalkMulticontainerDoc...	AWS managed	Provide the instances in your multicon...
<input type="checkbox"/>	AWS-ElasticBeanstalkReadOnly	AWS managed	Grants read-only permissions. Explicit...
<input type="checkbox"/>	AWS-ElasticBeanstalkRoleCore	AWS managed	AWS-ElasticBeanstalkRoleCore (Elastic ...
<input type="checkbox"/>	AWS-ElasticBeanstalkRoleCWL	AWS managed	(Elastic Beanstalk operations role) Allo...
<input type="checkbox"/>	AWS-ElasticBeanstalkRoleECS	AWS managed	(Elastic Beanstalk operations role) Allo...
<input type="checkbox"/>	AWS-ElasticBeanstalkRoleRDS	AWS managed	(Elastic Beanstalk operations role) Allo...
<input type="checkbox"/>	AWS-ElasticBeanstalkRoleSNS	AWS managed	(Elastic Beanstalk operations role) Allo...
<input type="checkbox"/>	AWS-ElasticBeanstalkRoleWorkerTier	AWS managed	(Elastic Beanstalk operations role) Allo...
<input checked="" type="checkbox"/>	AWS-ElasticBeanstalkWebTier	AWS managed	Provide the instances in your web serv...
<input checked="" type="checkbox"/>	AWS-ElasticBeanstalkWorkerTier	AWS managed	Provide the instances in your worker e...

▶ Set permissions boundary - optional

Cancel Previous Next

CloudShell Feedback

31°C Partly sunny

Search

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 17-21 15-08-2024

Configure service access | Elastic Beanstalk | Create role | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles/create?trustedEntityType=AWS_SERVICE&selectedService=EC2&selectedUseCase=EC2

AWS Services Search [Alt+S]

Global SanketMore

IAM > Roles > Create role

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Add permissions [Info](#)

Permissions policies (946) [Info](#)

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

Filter by Type All types 14 matches

Policy name Type Description

Policy name	Type	Description
AdministratorAccess-AWSElasticBeans...	AWS managed	Grants account administrative permis...
AWS-ElasticBeanstalkCustomPlatform...	AWS managed	Provide the instance in your custom pl...
AWS-ElasticBeanstalkEnhancedHealth	AWS managed	AWS Elastic Beanstalk Service policy f...
AWS-ElasticBeanstalkManagedUpdates...	AWS managed	This policy is for the AWS Elastic Beans...
AWS-ElasticBeanstalkMulticontainerDoc...	AWS managed	Provide the instances in your multicon...
AWS-ElasticBeanstalkReadOnly	AWS managed	Grants read-only permissions. Explicit...
AWS-ElasticBeanstalkRoleCore	AWS managed	AWS-ElasticBeanstalkRoleCore (Elastic ...
AWS-ElasticBeanstalkRoleCWL	AWS managed	(Elastic Beanstalk operations role) Allo...
AWS-ElasticBeanstalkRoleECS	AWS managed	(Elastic Beanstalk operations role) Allo...
AWS-ElasticBeanstalkRoleRDS	AWS managed	(Elastic Beanstalk operations role) Allo...
AWS-ElasticBeanstalkRoleSNS	AWS managed	(Elastic Beanstalk operations role) Allo...
AWS-ElasticBeanstalkRoleWorkerTier	AWS managed	(Elastic Beanstalk operations role) Allo...
AWS-ElasticBeanstalkWebTier	AWS managed	Provide the instances in your web serv...
AWS-ElasticBeanstalkWorkerTier	AWS managed	Provide the instances in your worker e...

CloudShell Feedback

31°C Partly sunny

Search

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 17-20 15-08-2024

Configure service access | Elastic Beanstalk **Create role | IAM | Global**

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles/create?trustedEntityType=AWS_SERVICE&selectedService=EC2&policies=arn%3Aa...

aws Services Search [Alt+S]

Step 2 Add permissions

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
aws-beanstalk-ec2-sanket

Maximum 64 characters. Use alphanumeric and '+-_@.' characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: +-_@[]!#\$%^&`~`

Step 1: Select trusted entities **Edit**

Trust policy

```

1 "Version": "2012-10-17",
2 "Statement": [
3     {
4         "Effect": "Allow",
5         "Action": [
6             "sts:AssumeRole"
7         ],
8         "Principal": [
9             "arn:aws:iam::123456789012:root"
10        ]
11    }
]
  
```

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

31°C Partly sunny **CloudShell Feedback** **CloudShell Feedback** © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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

Configure service access | Elastic Beanstalk **Roles | IAM | Global**

eu-north-1.console.aws.amazon.com/elasticbeanstalk/home?region=eu-north-1#/create-environment

aws Services Search [Alt+S]

Configure environment

Step 2 Configure service access

Step 3 - optional Set up networking, database, and tags

Step 4 - optional Configure instance traffic and scaling

Step 5 - optional Configure updates, monitoring, and logging

Step 6 Review

Configure service access **Info**

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

Service role
 Create and use new service role
 Use an existing service role
Existing service roles
Choose an existing IAM role for Elastic Beanstalk to assume as a service role. The existing IAM role must have the required IAM managed policies.
aws-elasticbeanstalk-service-role

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

EC2 instance profile
Choose an IAM instance profile with managed policies that allow your EC2 instances to perform required operations.
aws-beanstalk-ec2-sanket

View permission details

Cancel Skip to review Previous Next

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

NED - USA Live **CloudShell Feedback** **CloudShell Feedback** © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS CloudFormation search results for 'cloud fo'.

Elastic Beanstalk

- Applications
- Environments
- Change history
- Application: 30SAN**
 - Application version
 - Saved configurations
- Environment: 30SAN**
 - Go to environment
 - Configuration
 - Events
 - Health
 - Logs
 - Monitoring
 - Alarms
 - Managed updates
 - Tags

Services (120)

CloudFormation Create and Manage Resources with Templates

Top features: StackSets, IaC Generator, Stacks, Exports, Application Composer

Application Composer Visually design and build modern applications quickly

AWS Well-Architected Tool Use AWS Well-Architected Tool to learn best practices, measure, and improve your workloads

Features

IaC Generator, **CloudFormation feature**

Designer, **CloudFormation feature**

Using elasticbeanstalk-eu-north-1-869955102438 as Amazon S3 storage bucket for

CloudShell Feedback August 15, 2024 17:24:38 (UTC+5:30) INFO © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 17:25 15-08-2024

Screenshot of the IAM Roles page showing the role 'aws-beanstalk-ec2-sanket' created.

Identity and Access Management (IAM)

- Dashboard
- Access management**
 - User groups
 - Users
 - Roles**
 - Policies
 - Identity providers
 - Account settings
- Access reports**
 - Access Analyzer
 - External access
 - Unused access
 - Analyzer settings
 - Credential report
 - Organization activity

Role aws-beanstalk-ec2-sanket created.

Roles (4) Info

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

Role name	Trusted entities	Last activity
aws-beanstalk-ec2-sanket	AWS Service: ec2	-
aws-elasticbeanstalk-service-role	AWS Service: elasticbeanstalk	-
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linker)	-

Roles Anywhere

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

Access AWS from your non AWS workloads

X.509 Standard

Temporary credentials

CloudShell Feedback NED - USA Live August 15, 2024 17:23 (UTC+5:30) INFO © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 17:25 15-08-2024

Screenshot of the AWS CloudFormation console showing the creation of a new stack named "awseb-e-22vv2jtenw-stack". The "Template" tab displays the CloudFormation template JSON:

```
{ "Outputs": {}, "AWSTemplateFormatVersion": "2010-09-09", "Parameters": { "numThreads": { "NoEcho": "true", "Type": "Number", "Description": "The number of threads to create to handle requests in each daemon process.", "Default": 15 }, "InstanceTypeFamily": { "NoEcho": "true", "Type": "String", "Description": "WebServer EC2 instance type family" }, "LogPublicationControl": { "NoEcho": "true", "Type": "String" } }, "Resources": {} }
```

The "Events" tab shows two INFO-level events related to the environment creation:

Time	Type	Details
August 15, 2024 17:24:38 (UTC+5:30)	INFO	Using elasticbeanstalk-eu-north-1-869935102438 as Amazon S3 storage bucket for environment data.
August 15, 2024 17:24:37 (UTC+5:30)	INFO	createEnvironment is starting.

Screenshot of the AWS CloudFormation console showing the Environment overview - events page. The left sidebar shows the CloudFormation navigation menu with the 'Stacks' section selected. The main content area displays a table of stacks, showing one stack named 'awseb-e-22vv2jtenw-stack' in 'CREATE_IN_PROGRESS' status, created on 2024-08-15 at 17:24:43 UTC+0530. The description indicates it's an AWS Elastic Beanstalk environment (Name: '3OSAN-env' Id: 'e-22vv2jtenw').

Screenshot of the AWS Application Composer console showing the 'CloudFormation – Stack awseb-e-22vv2jtenw-stack' page. The left sidebar shows the Application Composer navigation menu with the 'Resources' section selected. The main content area displays a canvas with several standard components: 'AWSEBAutoScalingLaunchConfiguration', 'AWSEBInstanceLaunchWaitHandle', 'AWSEBEIP', 'AWSEBBeanstalkMetadata', and 'AWSEBInstanceLaunchWaitCondition'. A dotted line connects the 'AWSEBAutoScalingLaunchConfiguration' and 'AWSEBInstanceLaunchWaitHandle' components, indicating they are connected in the template.

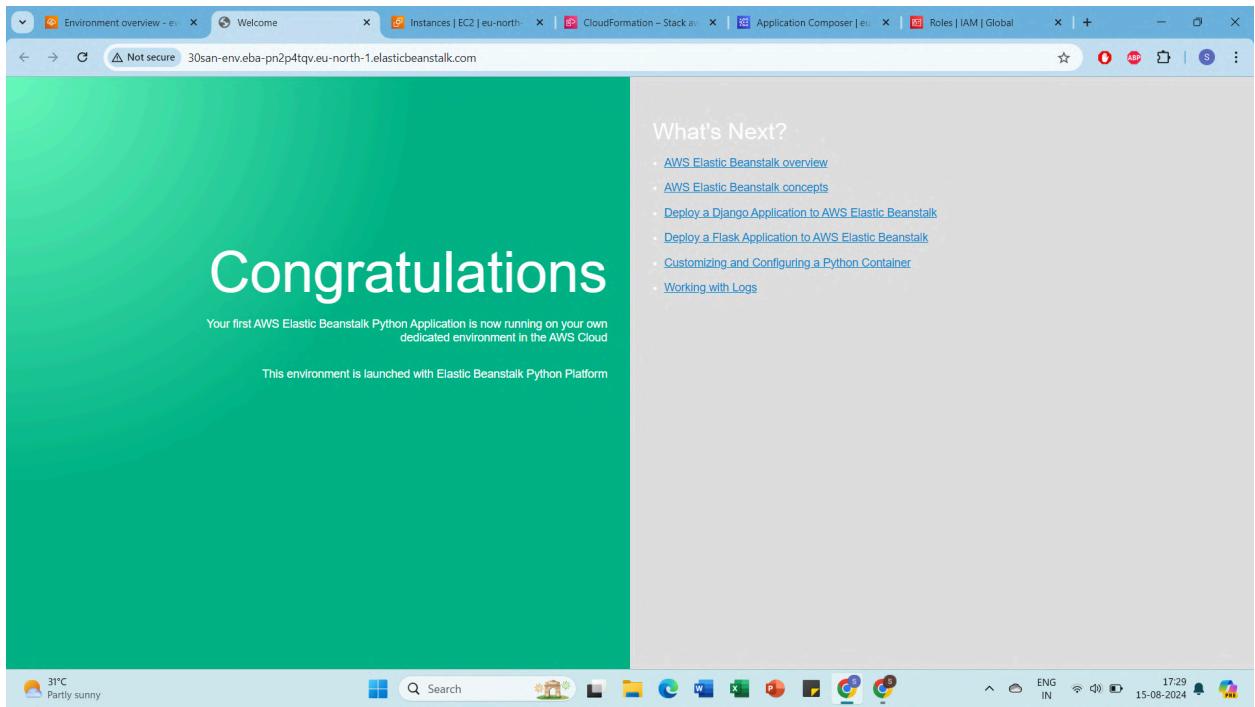
Screenshot of the AWS CloudFormation console showing the environment overview for the 'events' stack. The search bar at the top has 'ec2' typed into it.

The main pane displays the 'Services' section, specifically the EC2 service, which is highlighted. Other services listed include EC2 Image Builder and Recycle Bin.

The sidebar on the left shows the navigation menu for the Elastic Beanstalk service, with sections for Applications, Environments, Change history, Application: 30SAN, Environment: 30SAN, and CloudShell.

Below the main pane, a modal window titled 'Select an instance' is open, showing a table of running instances. One instance is selected: '30SAN-env' (Instance ID: i-0e5554a951cee2f53, Instance state: Running, Instance type: t3.micro, Status check: 2/2 checks passed, Alarm status: eu-north-1c, Public IP: ec2-13-49-).

The bottom of the screen shows the standard AWS navigation bar with links for CloudShell, Feedback, and various AWS services like S3, Lambda, and CloudWatch.



Code Deployment using Codepipeline:

The screenshot shows the AWS search interface with the query "codepipeline". The results are categorized under "Services" and "Documentation".

Services (1)

- CodePipeline

Documentation (1,463)

- CodePipeline tutorials
- Troubleshooting CodePipeline
- AWS CodePipeline

Resources (New)

Pipelines

Settings

Search results for 'codepipeline'

Introducing resource search

Enable to show cross-region resources for your account in search results. Takes less than 5 minutes to set up.

Dismiss **Go to Resource Explorer**

See all 1,463 results ▶

Create pipeline

CloudShell Feedback

Hot weather Now

Search

ENG IN 16:17 21-08-2024

The screenshot shows the AWS CodePipeline Pipelines list page. It displays a single pipeline entry:

Pipelines

Create pipeline

No results

There are no results to display.

CloudShell Feedback

Hot weather Now

Search

ENG IN 16:17 21-08-2024

Create new pipeline | CodePipeline

eu-north-1.console.aws.amazon.com/codesuite/codepipeline/pipeline/new?region=eu-north-1

Developer Tools > CodePipeline > Pipelines > Create new pipeline

Choose pipeline settings Info

Step 1 of 5

Pipeline settings

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

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

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

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

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

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

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 32°C Mostly cloudy ENG IN 16:19 21-08-2024

Create new pipeline | CodePipeline

eu-north-1.console.aws.amazon.com/codesuite/codepipeline/pipeline/new?region=eu-north-1

Developer Tools > CodePipeline > Pipelines > Create new pipeline

Add source stage Info

Step 2 of 5

Source

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

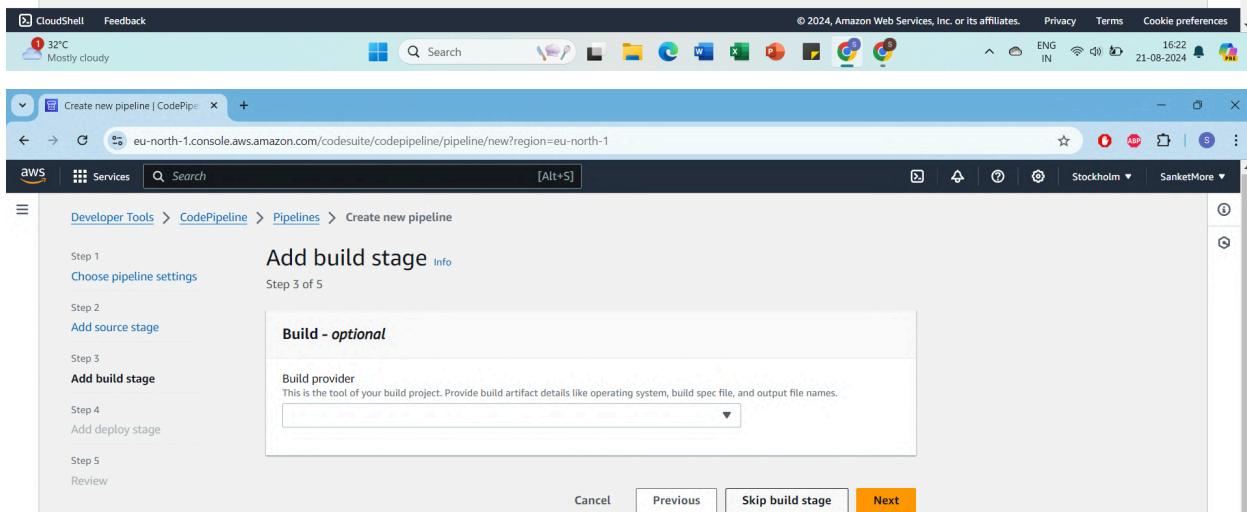
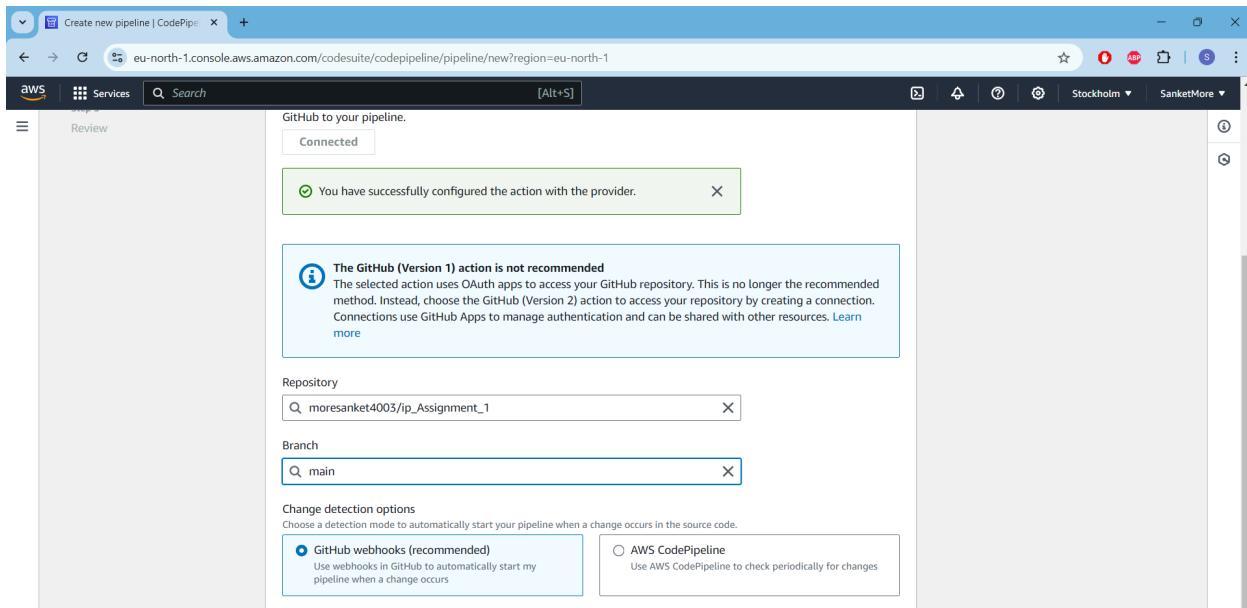
Grant AWS CodePipeline access to your GitHub repository. This allows AWS CodePipeline to upload commits from GitHub to your pipeline.

Connected

You have successfully configured the action with the provider.

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

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences USD/INR +0.16% 16:22 21-08-2024



Create new pipeline | CodePipeline

eu-north-1.console.aws.amazon.com/codesuite/codepipeline/pipeline/new?region=eu-north-1

Step 1 Choose pipeline settings

Step 2 Add source stage

Step 3 Add build stage

Step 4 Add deploy stage

Step 5 Review

Add deploy stage Info Step 4 of 5

You cannot skip this stage

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

Deploy

Deploy provider

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

AWS Elastic Beanstalk

Region

Europe (Stockholm)

Input artifacts

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

No more than 100 characters

Application name

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

Q 30SAN

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 16:25 21-08-2024

Create new pipeline | CodePipeline

eu-north-1.console.aws.amazon.com/codesuite/codepipeline/pipeline/new?region=eu-north-1

Step 5 Review

Deploy provider

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

AWS Elastic Beanstalk

Region

Europe (Stockholm)

Input artifacts

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

No more than 100 characters

Application name

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

Q 30SAN

Environment name

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

Q 30SAN-env

30SAN-env

Cancel Previous Next

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 16:25 21-08-2024

Create new pipeline | CodePipeline

eu-north-1.console.aws.amazon.com/codesuite/codepipeline/pipeline/new?region=eu-north-1

Developer Tools Services Search [Alt+S]

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

Review info Step 5 of 5

Step 1: Choose pipeline settings

Pipeline settings

Pipeline name: sanket_pipeline

Pipeline type: V2

Execution mode: QUEUED

Artifact location: A new Amazon S3 bucket will be created as the default artifact store for your pipeline

Service role name: AWSCodePipelineServiceRole-eu-north-1-sanket_pipeline

Variables

CloudShell Feedback 32°C Mostly cloudy © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 16:25 21-08-2024

sanket_pipeline | CodePipeline

eu-north-1.console.aws.amazon.com/codesuite/codepipeline/pipelines/sanket_pipeline/view?region=eu-north-1

Developer Tools Services Search [Alt+S]

Developer Tools > CodePipeline > Pipelines > sanket_pipeline

sanket_pipeline

Pipeline type: V2 Execution mode: QUEUED

Source In progress Pipeline execution ID: bc5c9237-6052-4a17-abde-05e781029825

Source GitHub (Version_1) In progress - Just now View details

Disable transition

Deploy Didn't Run Start rollback

CloudShell Feedback PAK - BAN Live © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 16:26 21-08-2024



Restaurant Reservation Portal

[Home](#) [Menu](#) [Reservation](#) [Contact Us](#)

Special Offers

- Happy Hour
- Weekend Special

Home

Welcome to Italian Food, where the essence of Italy comes alive in every dish. Nestled in the heart of Thane, our restaurant offers a delightful escape to the enchanting landscapes and rich culinary traditions of Italy. From our handmade pasta to our wood-fired pizzas, each meal is crafted with passion, using the freshest ingredients and time-honored recipes passed down through generations. Whether you're enjoying a romantic dinner, a family gathering, or a special celebration, La Dolce Vita promises an unforgettable dining experience filled with warmth, flavor, and Italian hospitality.



Advanced DevOps Experiment - 3

Sanket More

D15A 30

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

Implementation:-

Creating Instance using Amazon Linux

The screenshot shows the 'Launch an instance' wizard in the AWS Management Console. The process is divided into several steps:

- Step 1: Name and tags**
Name: Master
Software Image (AMI): Canonical, Ubuntu, 22.04 LTS, ami-0c2af51e265bd5e0e
- Step 2: Application and OS Images (Amazon Machine Image)**
Virtual server type (instance type): t2.medium
Firewall (security group): New security group
Storage (volumes): 1 volume(s) - 8 GiB
- Step 3: Instance type**
Selected: t3.xlarge
Family: t3 - 4 vCPU 16 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.1728 USD per Hour
On-Demand Windows base pricing: 0.2464 USD per Hour
On-Demand SUSE base pricing: 0.2291 USD per Hour
On-Demand RHEL base pricing: 0.2304 USD per Hour
Additional costs apply for AMIs with pre-installed software
Options: All generations, Compare instance types
- Step 4: Key pair (login)**
Key pair name - required: Select
Create new key pair

A summary sidebar on the right indicates 1 instance and a free tier offer: "Free tier: In your first year".

Create key pair

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

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

Key pair type

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

Private key file format

- .pem
For use with OpenSSH
- .ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on

[Cancel](#) [Create key pair](#)

Instances (4) Info							
		Last updated less than a minute ago		Connect	Instance state ▾	Actions ▾	Launch instances ▾
<input type="text"/> Find Instance by attribute or tag (case-sensitive) All states ▾							
□	Name ↴	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone ▾
□	30SAN-env	i-06dae01fd646e93ba	Running Q Q	t3.micro	3/3 checks passed	View alarms +	eu-north-1a
□	Master	i-05e71d31a2d0b9a11	Stopped Q Q	t3.xlarge	-	View alarms +	eu-north-1a
□	node1	i-0065bd5c032d2fda0	Stopped Q Q	t3.xlarge	-	View alarms +	eu-north-1b
□	node2	i-095cb5930eba6bee4	Stopped Q Q	t3.xlarge	-	View alarms +	eu-north-1b

Create security group

Select existing security group

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

Allow SSH traffic from

Helps you connect to your instance

Anywhere
0.0.0.0/0

Allow HTTPs traffic from the internet

To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

▼ Configure storage [Info](#)

[Advanced](#)

1x

30



GiB gp2



Root volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage



[Add new volume](#)

0 x File systems

[Edit](#)

Add rules of 'All traffic' to your instances

Security group rule ID	Type	Info	Protocol	Info	Port range	Info	Source	Info	Description - optional	Info
------------------------	------	----------------------	----------	----------------------	------------	----------------------	--------	----------------------	------------------------	----------------------

sgr-0dadf365271495e2e

HTTPS

TCP

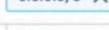
443

Custom



Q

0.0.0.0/0



Del

ete

sgr-0fdc139bb1e69104e

HTTP

TCP

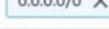
80

Custom



Q

0.0.0.0/0



Del

ete

sgr-07f8c2683ddfd0c8b

SSH

TCP

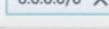
22

Custom



Q

0.0.0.0/0



Del

ete

-

All traffic

All

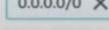
All

Anywh...



Q

0.0.0.0/0

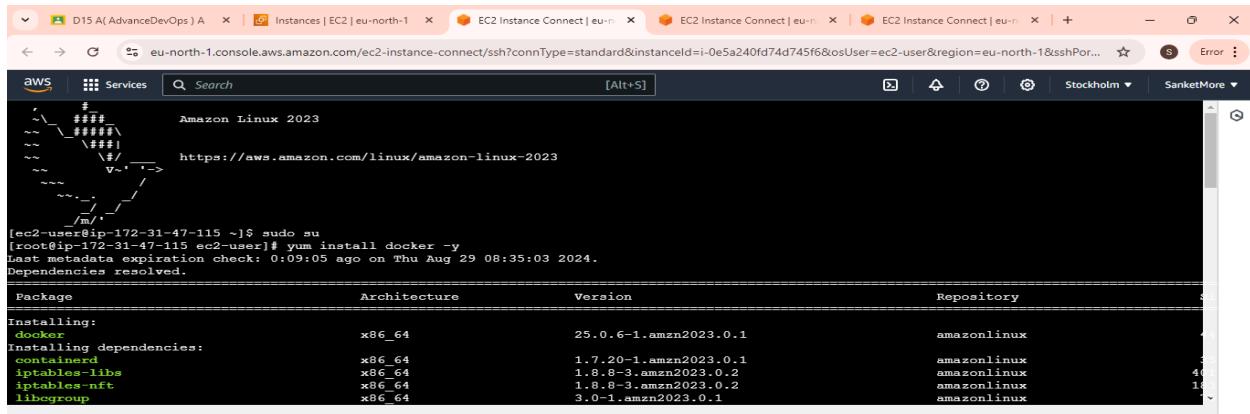


Del

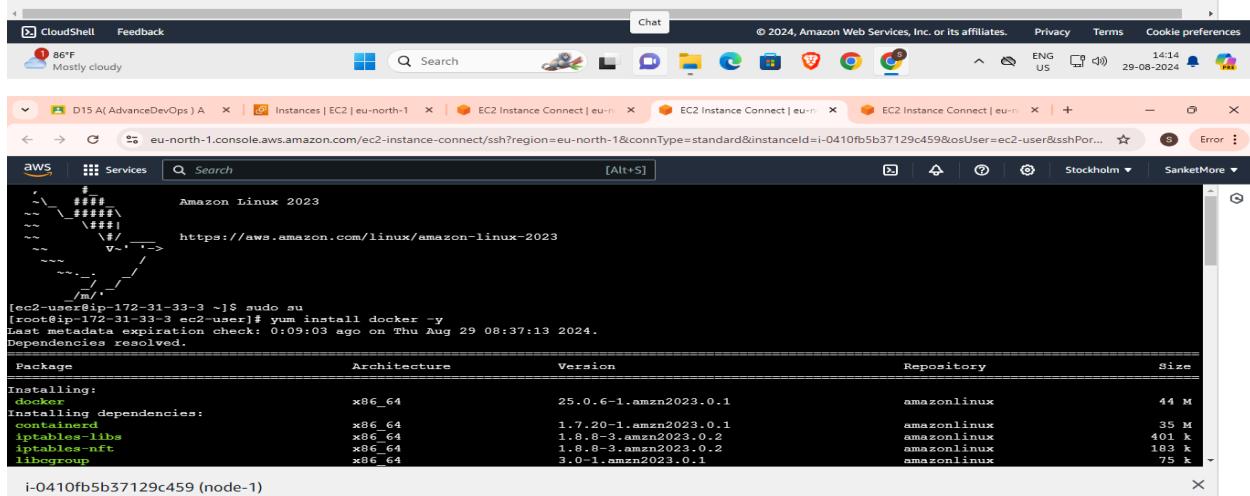
ete

[Add rule](#)

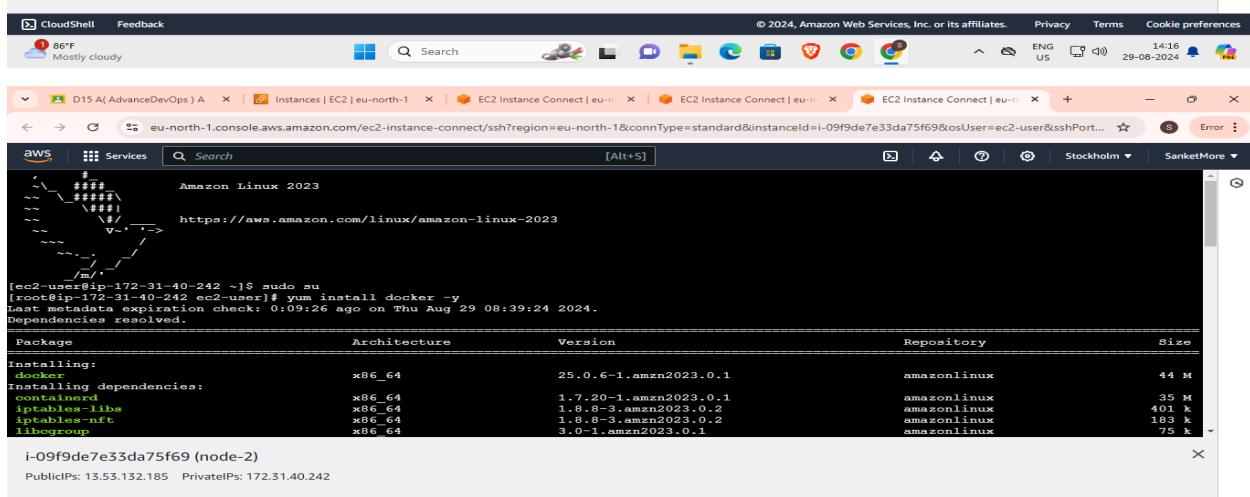
Installing Docker:-



```
[ec2-user@ip-172-31-47-115 ~]$ sudo su
[root@ip-172-31-47-115 ec2-user]# yum install docker -y
Last metadata expiration check: 0:09:05 ago on Thu Aug 29 08:35:03 2024.
Dependencies resolved.
Package           Architecture Version      Repository
Installing:
docker             x86_64      25.0.6-1.amzn2023.0.1  amazonlinux
Installing dependencies:
containerd          x86_64      1.7.20-1.amzn2023.0.1  amazonlinux
iptables-libc       x86_64      1.8.8-3.amzn2023.0.2  amazonlinux
iptables-nft        x86_64      1.8.8-3.amzn2023.0.2  amazonlinux
libcgroup           x86_64      3.0-1.amzn2023.0.1   amazonlinux
i-0e5a240fd74d745f6 (Master)
Public IPs: 13.60.196.238 Private IPs: 172.31.47.115
```



```
[ec2-user@ip-172-31-33-3 ~]$ sudo su
[root@ip-172-31-33-3 ec2-user]# yum install docker -y
Last metadata expiration check: 0:09:03 ago on Thu Aug 29 08:37:13 2024.
Dependencies resolved.
Package           Architecture Version      Repository
Installing:
docker             x86_64      25.0.6-1.amzn2023.0.1  amazonlinux
Installing dependencies:
containerd          x86_64      1.7.20-1.amzn2023.0.1  amazonlinux
iptables-libc       x86_64      1.8.8-3.amzn2023.0.2  amazonlinux
iptables-nft        x86_64      1.8.8-3.amzn2023.0.2  amazonlinux
libcgroup           x86_64      3.0-1.amzn2023.0.1   amazonlinux
i-0410fb5b37129c459 (node-1)
Public IPs: 13.60.191.4 Private IPs: 172.31.33.3
```



```
[ec2-user@ip-172-31-40-242 ~]$ sudo su
[root@ip-172-31-40-242 ec2-user]# yum install docker -y
Last metadata expiration check: 0:09:26 ago on Thu Aug 29 08:39:24 2024.
Dependencies resolved.
Package           Architecture Version      Repository
Installing:
docker             x86_64      25.0.6-1.amzn2023.0.1  amazonlinux
Installing dependencies:
containerd          x86_64      1.7.20-1.amzn2023.0.1  amazonlinux
iptables-libc       x86_64      1.8.8-3.amzn2023.0.2  amazonlinux
iptables-nft        x86_64      1.8.8-3.amzn2023.0.2  amazonlinux
libcgroup           x86_64      3.0-1.amzn2023.0.1   amazonlinux
i-05f9de7e33da75f69 (node-2)
Public IPs: 13.53.132.185 Private IPs: 172.31.40.242
```

Installing Kubernetes:-

The screenshot shows a web browser window with multiple tabs open, including one for 'Installing kubeadm'. The main content is the Kubernetes documentation page for 'Installing kubeadm'. The sidebar on the left contains links for Documentation, Getting started, Production environment, and a detailed section on 'Installing Kubernetes with deployment tools' which includes 'Booting clusters with kubeadm'. The main content area has a heading '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.' Below this is a code snippet:

```
# This overwrites any existing configuration in /etc/yum.repos.d/kubernetes.repo
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/repodata/repomd.xml.key
exclude=kubelet kubeadm kubectl cri-tools kubernetes-cni
EOF
```

Below the code snippet, there's a section titled '3. Install kubelet, kubeadm and kubectl:' with the command:

```
sudo yum install -y kubelet kubeadm kubectl --disableexcludes=kubernetes
```

On the right side of the page, there are links for 'Edit this page', 'Create child page', 'Create documentation issue', and 'Print entire section'. Below these links is a sidebar with links for 'Before you begin', 'Verify the MAC address and product_uuid are unique for every node', 'Check network adapters', 'Check required ports', 'Installing a container runtime', 'Installing kubeadm, kubelet and kubectl', 'Configuring a cgroup driver', 'Troubleshooting', and 'What's next'.

```
[root@ip-172-31-47-115 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/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/repodata/repomd.xml.key
exclude=kubelet kubeadm kubectl cri-tools kubernetes-cni
[root@ip-172-31-47-115 ec2-user]# sudo yum install -y kubelet kubeadm kubectl --disableexcludes=kubernetes
Kubernetes
Dependencies resolved.
```

```
Complete!
[root@ip-172-31-47-115 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-172-31-47-115 ec2-user]# i-0e5a240fd74d745f6 (Master)
PublicIPs: 13.60.196.238 PrivateIPs: 172.31.47.115
```

```

Installed:
conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64
kubeadm-1.31.0-150500.1.1.x86_64
kubelet-1.31.0-150500.1.1.x86_64
libnetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64
libnetfilter_queue-1.0.5-2.amzn2023.0.2.x86_64
cri-tools-1.31.1-150500.1.1.x86_64
kubectl-1.31.0-150500.1.1.x86_64
kubernetes-cni-1.5.0-150500.2.1.x86_64
libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64
socat-1.7.4.2-1.amzn2023.0.2.x86_64

Complete!
[root@ip-172-31-33-3 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-172-31-33-3 ec2-user]# 

i-0410fb5b37129c459 (node-1)
PublicIPs: 13.60.191.4 PrivateIPs: 172.31.33.3

```

```

Installed:
conntrack-tools-1.4.6-2.amzn2023.0.2.x86_64
kubeadm-1.31.0-150500.1.1.x86_64
kubelet-1.31.0-150500.1.1.x86_64
libnetfilter_cthelper-1.0.0-21.amzn2023.0.2.x86_64
libnetfilter_queue-1.0.5-2.amzn2023.0.2.x86_64
cri-tools-1.31.1-150500.1.1.x86_64
kubectl-1.31.0-150500.1.1.x86_64
kubernetes-cni-1.5.0-150500.2.1.x86_64
libnetfilter_cttimeout-1.0.0-19.amzn2023.0.2.x86_64
socat-1.7.4.2-1.amzn2023.0.2.x86_64

Complete!
[root@ip-172-31-40-242 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-172-31-40-242 ec2-user]# 

i-09f9de7e33da75f69 (node-2)
PublicIPs: 13.53.132.185 PrivateIPs: 172.31.40.242

```

Initializing Kubeadm:-

```

[root@ip-172-31-37-74 ec2-user]# kubeadm init
[init] Using Kubernetes version: v1.31.0
[preflight] Running pre-flight checks
  [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'
W0911 06:06:02.983804      2545 checks.go:846] detected that the sandbox image "registry.k8s.io/pause:3.8" of t
y 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

Your Kubernetes control-plane has initialized successfully!

To start using your cluster, you need to run the following as a regular user:

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

Alternatively, if you are the root user, you can run:

export KUBECONFIG=/etc/kubernetes/admin.conf

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

Then you can join any number of worker nodes by running the following on each as root:

kubeadm join 172.31.25.144:6443 --token kw6rp8.mi1vmqzveqzzeifs \
    --discovery-token-ca-cert-hash sha256:e2285a0bb9324e4ebd564331961c506c7c8172e4639c81d5d89c86a47f0ad842
[root@ip-172-31-25-144 ec2-user]# 

```

```

[root@master ~]# mkdir -p $HOME/.kube
[root@master ~]# sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
[root@master ~]# sudo chown $(id -u):$(id -g) $HOME/.kube/config
[root@master ~]# export KUBECONFIG=/etc/kubernetes/admin.conf

```

Creating the kubernetes nodes by copying the link in the workers:-

```
[root@worker ~]# systemctl enable docker
[root@worker ~]# systemctl enable kubelet
Created symlink from /etc/systemd/system/multi-user.target.wants/kubelet.service to /usr/lib/systemd/system/kubelet.service.
[root@worker ~]# systemctl restart docker kubelet
[root@worker ~]# kubeadm join 172.31.46.167:6443 --token d47j51.2ejotl12hbxm5tys \
>           --discovery-token-ca-cert-hash sha256:a5511cfbd8b2b8bd69f15e7ad4247c34e1e2218b448a3a36509c0bb15b6f8d43
```

Installing the Calico file:-

The screenshot shows the Project Calico website's 'Install Calico' page for Kubernetes. It features a sidebar with options like 'About', 'Install Calico' (selected), 'Kubernetes' (expanded), 'Managed public cloud', 'Self-managed public cloud', 'Self-managed on-premises', and 'Install Calico for on-premises'. The main content area has a note about Typha scaling, a 'Quickstart' section with three bullet points, and a 'Install Calico with Kubernetes API datastore, 50 nodes or less' section with two steps. Step 1 shows a curl command to download the manifest. Step 2 notes that if using pod CIDR 192.168.0.0/16, it should be skipped as Calico will automatically detect the CIDR. A sidebar on the right lists links for 'Big picture', 'Value', 'Concepts', 'Calico operator', 'Calico manifests', 'Before you begin...', 'How to', and 'Next steps'.

```
[root@master ~]# curl https://raw.githubusercontent.com/projectcalico/calico/v3.24.1/manifests/calico.yaml -o
% Total    % Received % Xferd  Average Speed   Time     Time      Current
          Dload  Upload Total Spent   Left Speed
100  229k  100  229k    0     0  175k      0  0:00:01  0:00:01 ---:--:--  176k
[root@master ~]#
[root@master ~]# kubectl apply -f calico.yaml
poddisruptionbudget.policy/calico-kube-controllers created
serviceaccount/calico-kube-controllers created
serviceaccount/calico-node created
configmap/calico-config created
customresourcedefinition.apiextensions.k8s.io/bgpconfigurations.crd.projectcalico.org created
customresourcedefinition.apiextensions.k8s.io/bgppeers.crd.projectcalico.org created
customresourcedefinition.apiextensions.k8s.io/blockaffinities.crd.projectcalico.org created
```

```
Every 2.0s: kubectl get pods -A

NAMESPACE     NAME             READY   STATUS        RESTARTS   AGE
kube-system   calico-kube-controllers-58dbc876ff-nnprd  0/1    ContainerCreating  0          29s
kube-system   calico-node-bs95w   0/1    Init:2/3     0          29s
kube-system   calico-node-hplqt  0/1    Init:2/3     0          29s
kube-system   coredns-565d847f94-prsps  0/1    ContainerCreating  0          6m7s
kube-system   coredns-565d847f94-qrg48  0/1    ContainerCreating  0          6m6s
kube-system   etcd-master       1/1    Running       0          6m14s
kube-system   kube-apiserver-master  1/1    Running       0          6m12s
kube-system   kube-controller-manager-master  1/1    Running       0          6m11s
kube-system   kube-proxy-v2kxq    1/1    Running       0          2m31s
kube-system   kube-proxy-w8nn7    1/1    Running       0          6m7s
kube-system   kube-scheduler-master  1/1    Running       0          6m13s
```

Nodes Created:

Every 2.0s: kubectl get nodes				
NAME	STATUS	ROLES	AGE	VERSION
ip-172-31-85-89.ec2.internal	Ready	control-plane	3m39s	v1.26.0
ip-172-31-89-46.ec2.internal	Ready	<none>	119s	v1.26.0
ip-172-31-94-70.ec2.internal	Ready	<none>	112s	v1.26.0

ADVANCE DEVOPS EXP 4

Sanket More

D15A 30

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

Step 1: Install Kubectl on Ubuntu

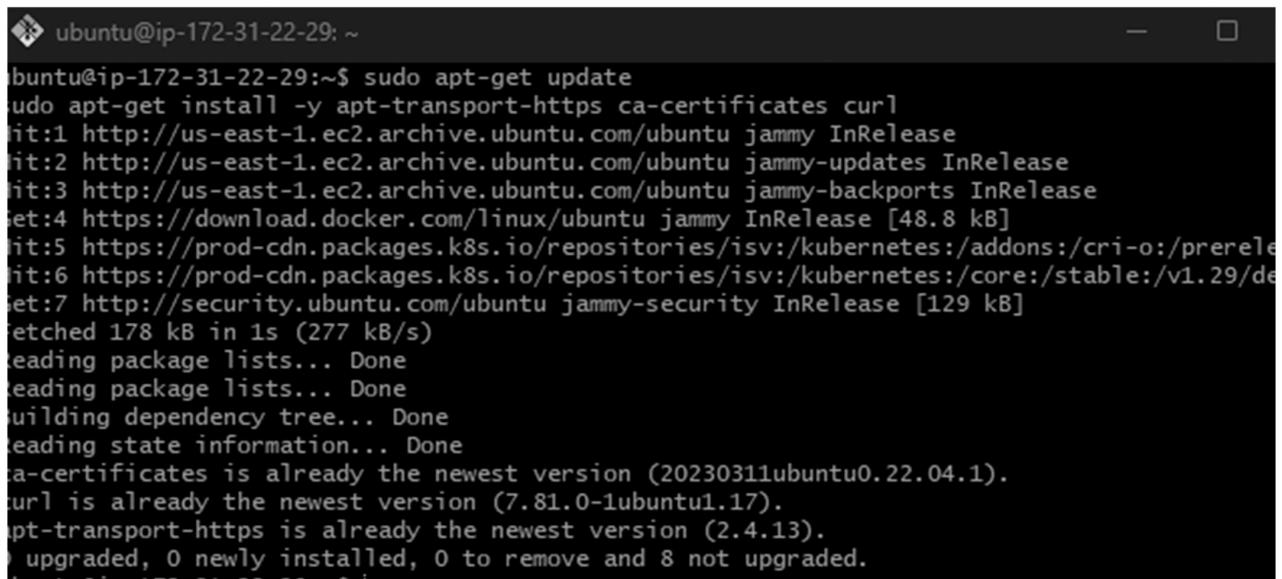
1.1 Add Kubernetes APT repository

First, add the Kubernetes repository to your system.

1. Install prerequisites:

```
sudo apt-get update
```

```
sudo apt-get install -y apt-transport-https ca-certificates curl
```



```
ubuntu@ip-172-31-22-29:~$ sudo apt-get update
[sudo] password for ubuntu:
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:4 https://download.docker.com/linux/ubuntu jammy InRelease [48.8 kB]
Get:5 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/addons:/cri-o:/prerelease
Get:6 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:/v1.29/debian
Get:7 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Fetched 178 kB in 1s (277 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ca-certificates is already the newest version (20230311ubuntu0.22.04.1).
curl is already the newest version (7.81.0-1ubuntu1.17).
apt-transport-https is already the newest version (2.4.13).
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
[11:51:17 21-03-2023]
```

2. Add the GPG key for Kubernetes:

```
sudo curl -fsSLo  
/usr/share/keyrings/kubernetes-archive-keyring.gpg  
https://packages.cloud.google.com/apt/doc/apt-key.gpg
```

```
ubuntu@ip-172-31-22-29:~$ sudo curl -fsSLo /usr/share/keyrings/kubernetes-archive-keyring.gpg  
https://packages.cloud.google.com/apt/doc/apt-key.gpg
```

3. Add the Kubernetes repository:

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

```
ubuntu@ip-172-31-22-29:~$ echo "deb [signed-by=/usr/share/keyrings/kubernetes-archive-keyring.gpg]
https://apt.kubernetes.io/ kubernetes-focal main" | sudo tee /etc/apt/sources.list.d/kubernetes.list
deb [signed-by=/usr/share/keyrings/kubernetes-archive-keyring.gpg] https://apt.kubernetes.io/
kubernetes-focal main
```

1.2 Install

kubectl Now install

kubectl: sudo

apt-get update

sudo apt-get install -y kubectl

```
ubuntu@ip-172-31-22-29:~$ sudo apt-get update
sudo apt-get install -y kubectl
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:5 https://download.docker.com/linux/ubuntu jammy InRelease
Hit:6 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/addons:/cri-o:/prerelease:/main/deb InRelease
Ign:7 https://packages.cloud.google.com/apt kubernetes-focal InRelease
Err:8 https://packages.cloud.google.com/apt kubernetes-focal Release
  404 Not Found [IP: 172.253.62.138 443]
Reading package lists... Done
E: The repository 'https://apt.kubernetes.io kubernetes-focal Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
kubectl is already the newest version (1.29.0-1.1).
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
```

Verify the installation(extra):

kubectl version --client

```
ubuntu@ip-172-31-22-29:~$ kubectl version --client
Client Version: v1.29.0
Kustomize Version: v5.0.4-0.20230601165947-6ce0bf390ce3
```

Step 2: Deploying Your Application on Kubernetes

2.1 Set up Kubernetes Cluster

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

```
ubuntu@ip-172-31-45-227:~$ kubectl get nodes
NAME           STATUS   ROLES      AGE    VERSION
ip-172-31-43-211   Ready    <none>    50s   v1.29.0
ip-172-31-45-13   Ready    <none>    34s   v1.29.0
ip-172-31-45-227   Ready    control-plane  5m17s  v1.29.0
ubuntu@ip-172-31-45-227:~$ |
```

Step 3: Create the Deployment YAML file

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

```
ubuntu@ip-172-31-45-227:~$ nano nginx-deployment.yaml
```

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

```
ubuntu@ip-172-31-45-227: ~
GNU nano 6.2                                     nginx-deployment.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  labels:
    app: nginx
spec:
  replicas: 2
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx:1.21.3
        ports:
        - containerPort: 80
```

Step 4:Create the Service YAML File

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

```
ubuntu@ip-172-31-45-227:~$ nano nginx-service.yaml
```

- b) Add the Service Configuration: Copy and paste the following YAML content into the file given below

```
ubuntu@ip-172-31-45-227:~$ nano nginx-service.yaml
GNU nano 6.2
nginx-service.yaml *
apiVersion: v1
kind: Service
metadata:
  name: nginx-service
spec:
  selector:
    app: nginx
  ports:
    - protocol: TCP
      port: 80
      targetPort: 80
  type: LoadBalancer
```

Step 5: Apply the YAML Files

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

```
ubuntu@ip-172-31-45-227:~$ kubectl apply -f nginx-deployment.yaml
kubectl apply -f nginx-service.yaml
deployment.apps/nginx-deployment created
service/nginx-service created
```

- b) Verify the Deployment: Check the status of your Deployment, Pods and Services.

```
ubuntu@ip-172-31-45-227:~$ kubectl get deployments
kubectl get pods
kubectl get services
NAME           READY   UP-TO-DATE   AVAILABLE   AGE
nginx-deployment   2/2     2           2          40s
NAME                  READY   STATUS    RESTARTS   AGE
nginx-deployment-6b4d6fdbf-6k84m   1/1     Running   0          40s
nginx-deployment-6b4d6fdbf-9d8j6   1/1     Running   0          40s
NAME            TYPE        CLUSTER-IP      EXTERNAL-IP    PORT(S)         AGE
kubernetes      ClusterIP   10.96.0.1    <none>        443/TCP       40m
nginx-service   LoadBalancer 10.106.182.152 <pending>     80:32317/TCP   40s
```

Describe the deployment(Extra)

```
ubuntu@ip-172-31-45-227:~$ kubectl get deployments
NAME           READY   UP-TO-DATE   AVAILABLE   AGE
nginx-deployment 1/1     1            1           14h
ubuntu@ip-172-31-45-227:~$ kubectl describe deployment
Name:            nginx-deployment
Namespace:       default
CreationTimestamp:  Wed, 11 Sep 2024 17:16:17 +0000
Labels:          <none>
Annotations:    deployment.kubernetes.io/revision: 2
Selector:        app=nginx
Replicas:        1 desired | 1 updated | 1 total | 1 available | 0 unavailable
StrategyType:   RollingUpdate
MinReadySeconds: 0
RollingUpdateStrategy: 25% max unavailable, 25% max surge
Pod Template:
  Labels:  app=nginx
  Containers:
    nginx:
      Image:      nginx:latest
      Port:       80/TCP
      Host Port:  0/TCP
      Environment: <none>
      Mounts:
        /usr/share/nginx/html from website-volume (rw)
  Volumes:
    website-volume:
      Type:      ConfigMap (a volume populated by a ConfigMap)
      Name:      nginx-website
      Optional:  false
Conditions:
  Type    Status  Reason
  ----  -----
  Available  True    MinimumReplicasAvailable
  Progressing  True    NewReplicaSetAvailable
OldReplicaSets:  nginx-deployment-6b4d6fdbf (0/0 replicas created)
NewReplicaSet:   nginx-deployment-776b8fd845 (1/1 replicas created)
Events:          <none>
```

Step 6:Ensure Service is Running

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

```
kubectl get service
```

```
ubuntu@ip-172-31-45-227:~$ kubectl get service
NAME      TYPE      CLUSTER-IP      EXTERNAL-IP      PORT(S)      AGE
kubernetes  ClusterIP  10.96.0.1      <none>        443/TCP      16h
nginx     NodePort   10.106.0.176    <none>        80:32618/TCP  76m
nginx-service  NodePort   10.106.182.152    <none>        80:30007/TCP  15h
nginx2     NodePort   10.99.32.156    <none>        80:31421/TCP  8s
```

Step 7:Forward the Service Port to Your Local Machine

kubectl port-forward allows you to forward a port from your local machine to a port on a service running in the Kubernetes cluster.

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

```
kubectl port-forward service/<service-name> <local-port>:<service-port>
```

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

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

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

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

Step 8: Access the Application Locally

1. **Open a Web Browser:** Now open your web browser and go to the following URL:

http://localhost:8080

You should see the application (in this case, Nginx) that you have deployed running in the Kubernetes cluster, served locally via port 8080.

In case the port 8080 is unavailable, try using a different port like 8081



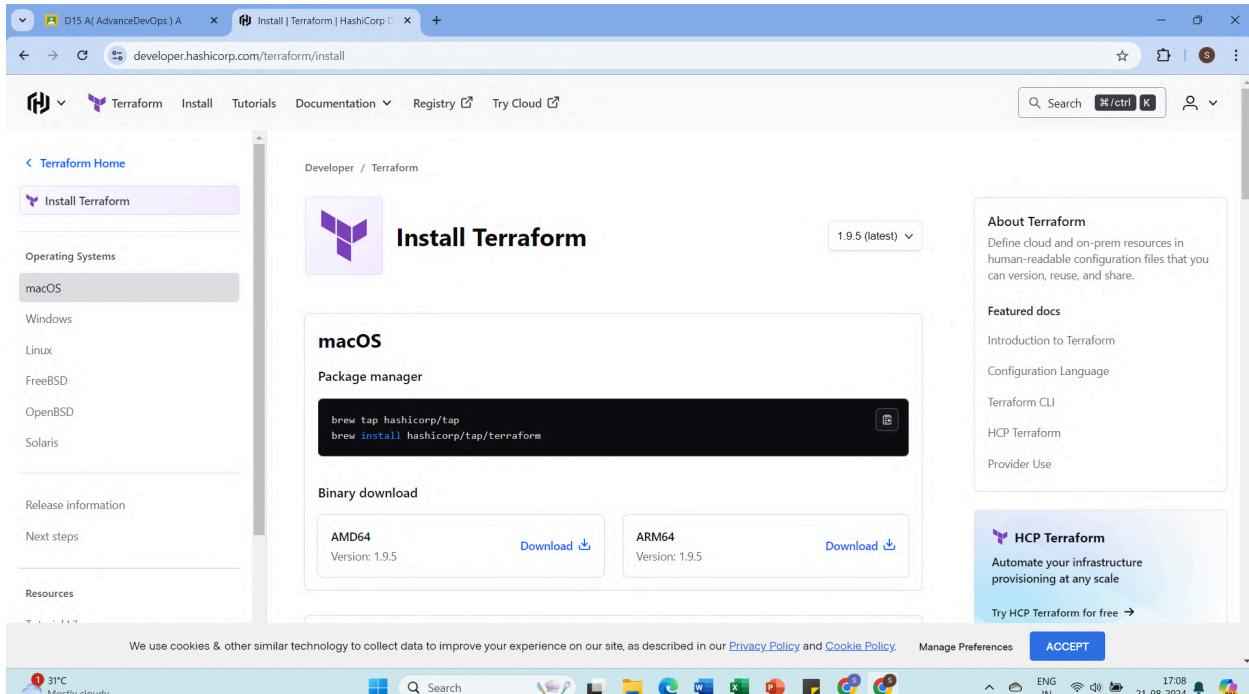
Advanced DevOps Experiment-5

Sanket More

D15A 30

Aim: To understand terraform lifecycle, core concepts/terminologies and install it on a Linux Machine and Windows.

Implementation:-

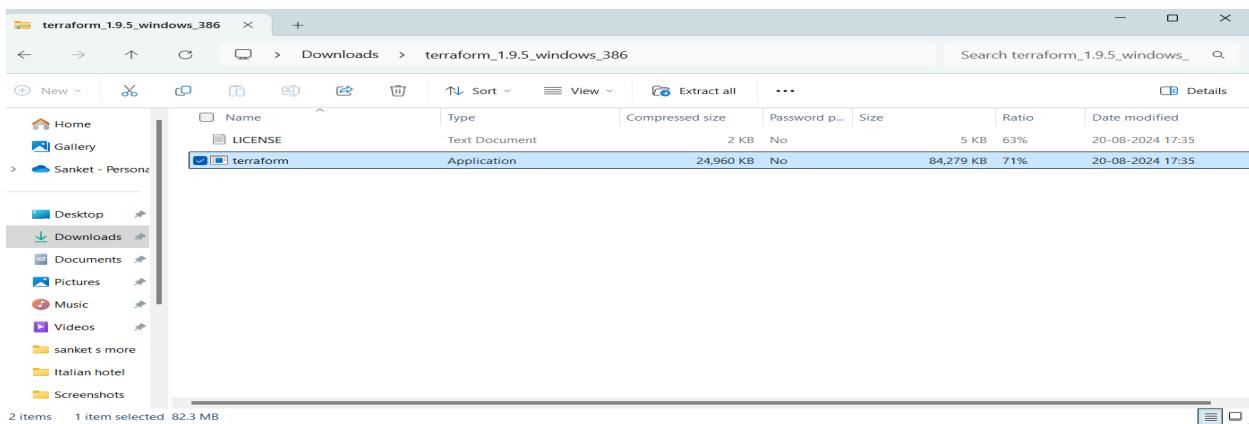


The screenshot shows the HashiCorp Terraform website's "Install Terraform" page for macOS. On the left, there's a sidebar with "Install Terraform" selected. The main content area has a heading "Install Terraform" with a "macOS" section. It contains "Package manager" instructions for Homebrew:

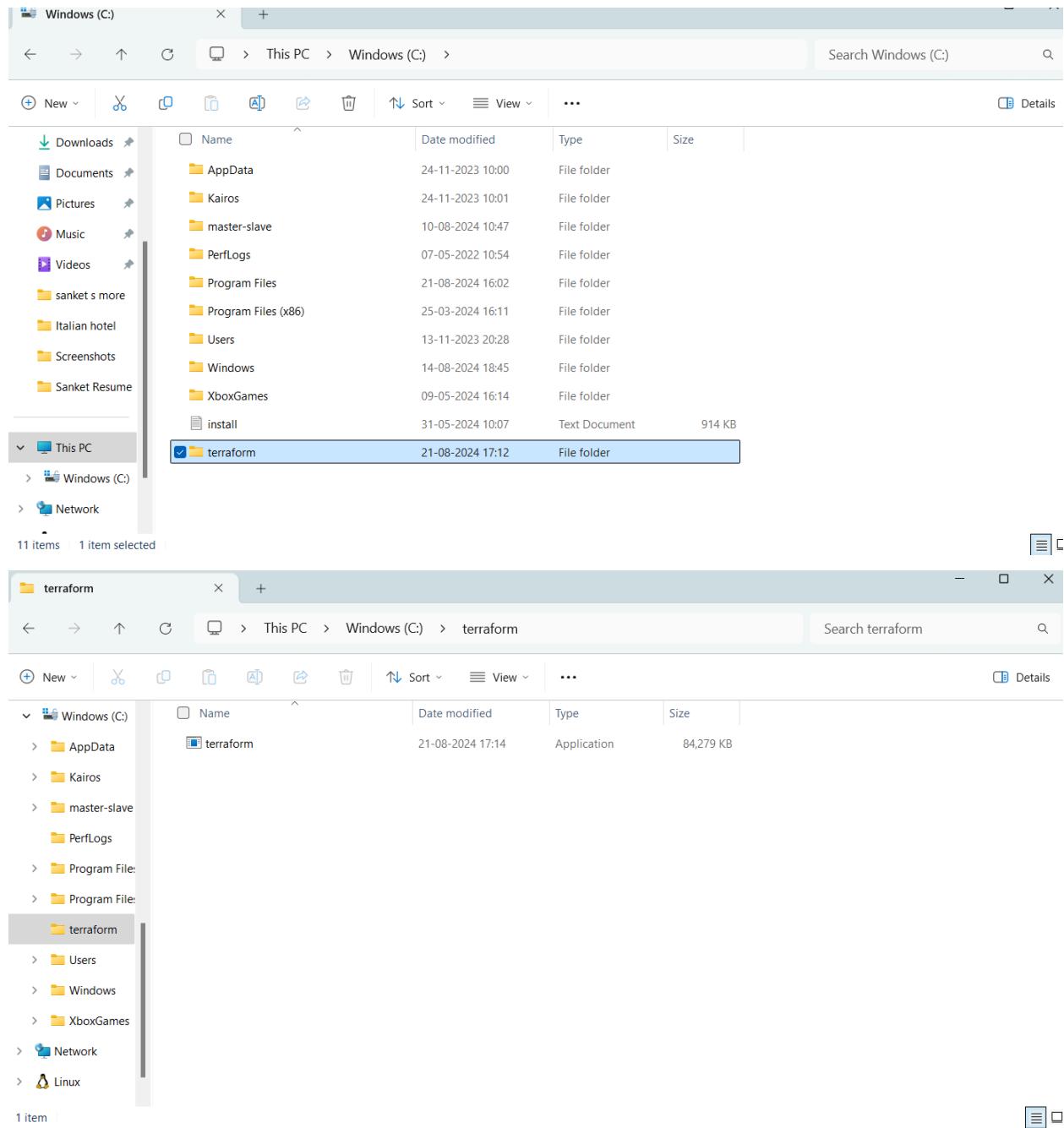
```
brew tap hashicorp/tap
brew install hashicorp/tap/terraform
```

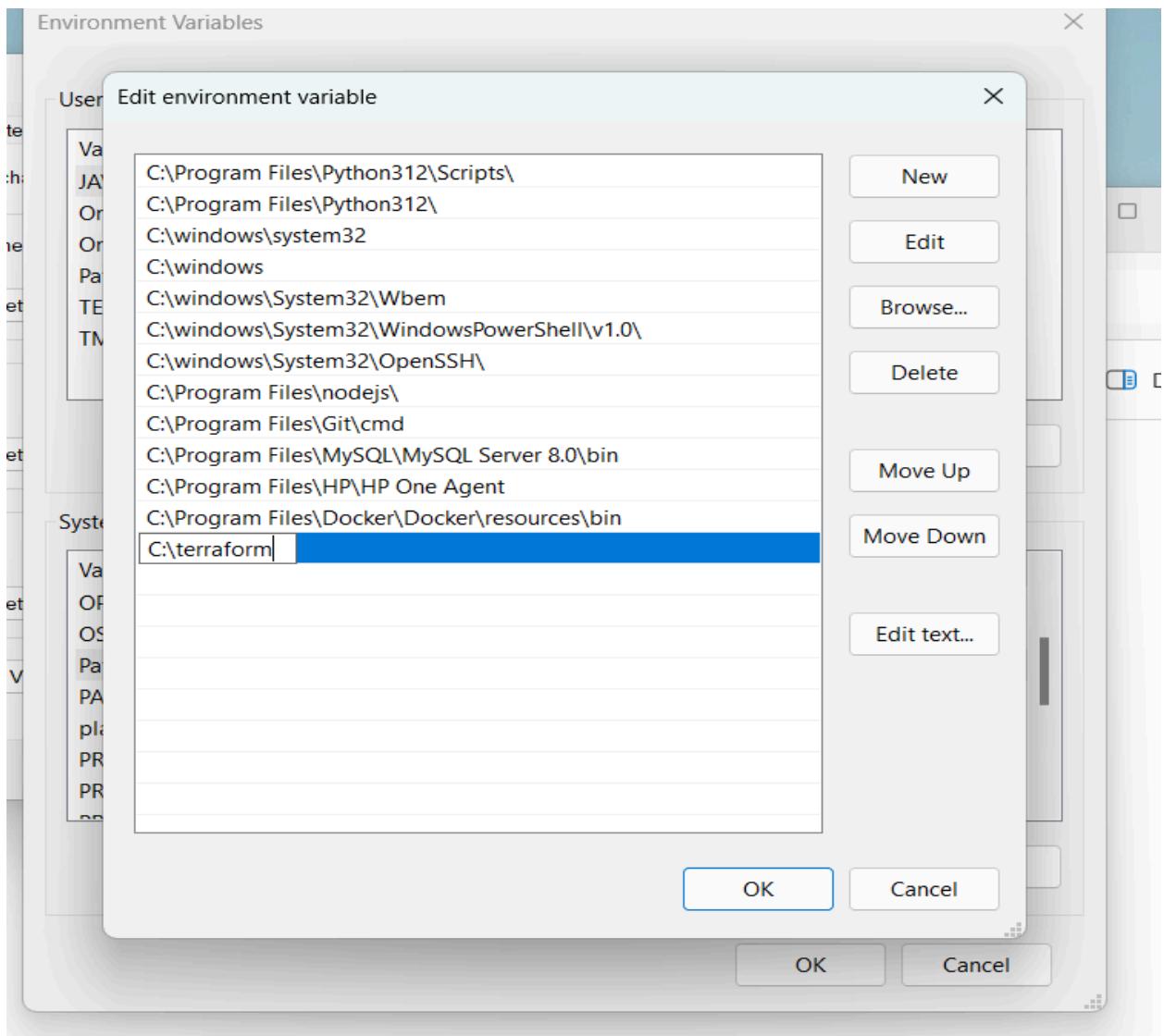
It also provides "Binary download" links for "AMD64" and "ARM64" architectures, both labeled "Version: 1.9.5".

On the right, there's a sidebar titled "About Terraform" with a brief description and links to "Featured docs" like "Introduction to Terraform" and "Configuration Language". Below that is a "HCP Terraform" section with a "Try HCP Terraform for free" button.



The screenshot shows a Windows File Explorer window titled "terraform_1.9.5_windows_386" in the "Downloads" folder. It lists two files: "LICENSE" (Text Document, 2 KB, 5 KB, 63%, 20-08-2024 17:35) and "terraform" (Application, 24,960 KB, 84,279 KB, 71%, 20-08-2024 17:35).





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

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

```
C:\Users\Sanket More>
```

AdvDevOps Lab 6

Sanket More

D15A 30

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

Part A: Creating docker image using terraform

1. Install docker

```
C:\Users\Sanket More>docker

Usage: docker [OPTIONS] COMMAND

A self-sufficient runtime for containers

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

Management Commands:
  builder      Manage builds
  buildx*      Docker Buildx
  checkpoint   Manage checkpoints
  compose*     Docker Compose
  container    Manage containers
  context      Manage contexts
```

```
C:\Users\Sanket More>docker --version
Docker version 27.0.3, build 7d4bcd8
```

2. Create a new folder Docker, inside it, create a file docker.tf

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

3. Terraform init

```
C:\Users\siddi\OneDrive\Desktop\lab-works\terraform_scripts>cd Docker  
C:\Users\siddi\OneDrive\Desktop\lab-works\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.
```

4. Terraform plan

```
C:\Users\siddi\OneDrive\Desktop\lab-works\terraform_scripts\ Docker>terraform plan  
Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with  
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)
```

```

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

+ healthcheck   (known after apply)

+ labels (known after apply)
}

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

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

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

```

5. Check docker images before applying

```
C:\Users\siddi\OneDrive\Desktop\lab-works\terraform_scripts\Docker>docker images
REPOSITORY      TAG      IMAGE ID      CREATED      SIZE
react-img      latest    619c9b7a9ac5  2 weeks ago  320MB
```

```
C:\Users\siddi\OneDrive\Desktop\lab-works\terraform_scripts\Docker>
```

6. Terraform apply

```
C:\Users\siddi\OneDrive\Desktop\lab-works\terraform_scripts\Docker>terraform apply
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:
+ create

Terraform will perform the following actions:

# docker_container.foo will be created
+ resource "docker_container" "foo" {
  + attach          = false
  + bridge         = (known after apply)
  + command        = [
    + "tail",
    + "-f",
    + "/dev/null",
  ]
  + container_logs = (known after apply)
  + entrypoint     = (known after apply)
```

```

+ logs          = false
+ must_run     = true
+ name         = "foo"
+ network_data = (known after apply)
+ read_only    = false
+ remove_volumes = true
+ restart      = "no"
+ rm           = false
+ runtime       = (known after apply)
+ security_opts = (known after apply)
+ shm_size      = (known after apply)
+ start         = true
+ stdin_open    = false
+ stop_signal   = (known after apply)
+ stop_timeout  = (known after apply)
+ tty           = false

+ healthcheck (known after apply)
+ labels (known after apply)
}

Plan: 1 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_container.foo: Creating...
docker_container.foo: Creation complete after 1s [id=af0512641b95dfece26fa5f29deafb8a8d56bd8b9878a246f46bd694e961e5b5]

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.

C:\Users\siddi\OneDrive\Desktop\lab-works\terraform_scripts\Docker>

```

7. Docker images after apply

```

C:\Users\siddi\OneDrive\Desktop\lab-works\terraform_scripts\Docker>docker images
REPOSITORY      TAG      IMAGE ID      CREATED      SIZE
react-img      latest   619c9b7a9ac5  2 weeks ago  320MB
ubuntu          latest   edbfe74c41f8  3 weeks ago  78.1MB

```

8. Terraform destroy

```
C:\Users\siddi\OneDrive\Desktop\lab-works\terraform_scripts\Docker>terraform destroy
docker_image.ubuntu: Refreshing state... [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]
docker_container.foo: Refreshing state... [id=af0512641b95dfece26fa5f29deafb8a8d56bd8b9878a246f46bd694e961e5b5]

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_container.foo will be destroyed
- resource "docker_container" "foo" {
  - attach = false -> null
  - command = [
    - "tail",
    - "-f",
    - "/dev/null",
  ] -> null
  - cpu_shares = 0 -> null
  - dns = [] -> null
  - dns_opts = [] -> null
  - dns_search = [] -> null
  - entrypoint = [] -> null
  - env = [] -> null
  - gateway = "172.17.0.1" -> null
  - group_add = [] -> null
  - hostname = "af0512641b95" -> null
  - id = "af0512641b95dfece26fa5f29deafb8a8d56bd8b9878a246f46bd694e961e5b5" -> null
  - image = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598a" -> null
  - init = false -> null
  - ip_address = "172.17.0.2" -> null
  - ip_prefix_length = 16 -> null
  - ipc_mode = "private" -> null
  - links = [] -> null
  - log_driver = "json-file" -> null
}
```

```
# docker_image.ubuntu will be destroyed
- resource "docker_image" "ubuntu" {
  - id = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest" -> null
  - image_id = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598a" -> null
  - latest = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598a" -> null
  - name = "ubuntu:latest" -> null
  - repo_digest = "ubuntu@sha256:8a37d68f4f73ebf3d4efafbcf66379bf3728902a8038616808f04e34a9ab63ee" -> null
}

Plan: 0 to add, 0 to change, 2 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_container.foo: Destroying... [id=af0512641b95dfece26fa5f29deafb8a8d56bd8b9878a246f46bd694e961e5b5]
docker_container.foo: Destruction complete after 1s
docker_image.ubuntu: Destroying... [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]
docker_image.ubuntu: Destruction complete after 0s

Destroy complete! Resources: 2 destroyed.

C:\Users\siddi\OneDrive\Desktop\lab-works\terraform_scripts\Docker>
```

9. Docker images after apply

```
C:\Users\siddi\OneDrive\Desktop\lab-works\terraform_scripts\Docker>docker images
REPOSITORY      TAG      IMAGE ID      CREATED      SIZE
react-img      latest   619c9b7a9ac5   2 weeks ago   320MB

C:\Users\siddi\OneDrive\Desktop\lab-works\terraform_scripts\Docker>
```

Part B:Terraform and S3 -

Step 1: Create access keys and secret key for IAM user

AWS account.

Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

Other
Your use case is not listed here.

⚠ Alternative recommended
Assign an IAM role to compute resources like EC2 instances or Lambda functions to automatically supply temporary credentials to enable access. [Learn more](#)

Step 2 : Type below code in main.tf in editor for aws and terraform connection and environment creation .

Code -

```
terraform {  
  required_providers {  
    aws = {  
      source = "hashicorp/aws"  
      version = "~> 5.0"  
    }  
  }  
}  
  
# Configure the AWS Provider  
  
provider "aws" {  
  region = "us-east-1"
```

```

access_key = ""

secret_key = ""

}

resource "aws_s3_bucket" "bucket" {

bucket = "bucket-pranav-123"

tags = {

Name = "My bucket"

}

}

```

```

s3 > 🐾 main.tf
1  terraform {
2    required_providers {
3      aws = {
4        source  = "hashicorp/aws"
5        version = "~> 5.0"
6      }
7    }
8  }
9
10 # Configure the AWS Provider
11 provider "aws" {
12   region = "us-east-1"
13   access_key = ""
14   secret_key = ""
15 }
16
17
18
19 resource "aws_s3_bucket" "bucket" {
20   bucket = "bucket-pranav-123"
21
22   tags = {
23     Name = "My bucket"
24
25   }
26 }
27

```

Step 3 : Type terraform init command in powershell.

```
(base) PS C:\Users\sbpol\Documents\terraform_scripts\docker\s3> terraform init
Initializing the backend...
Initializing provider plugins...
- Finding hashicorp/aws versions matching "~> 5.0"...
- Installing hashicorp/aws v5.63.1...
- Installed hashicorp/aws v5.63.1 (signed by HashiCorp)
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.
(base) PS C:\Users\sbpol\Documents\terraform_scripts\docker\s3>
```

Step 4 : Type terraform plan command in powershell.

```
(base) PS C:\Users\sbpol\Documents\terraform_scripts\docker\s3> 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:

# aws_s3_bucket.terr will be created
+ resource "aws_s3_bucket" "terr" {
    + acceleration_status      = (known after apply)
    + acl                      = (known after apply)
    + arn                      = (known after apply)
    + bucket                   = "my-tf-test-bucket"
    + bucket_domain_name       = (known after apply)
    + bucket_prefix             = (known after apply)
    + bucketRegionalDomainName = (known after apply)
    + force_destroy             = false
    + hosted_zone_id           = (known after apply)
    + id                       = (known after apply)
    + object_lock_enabled       = (known after apply)
    + policy                   = (known after apply)
    + region                   = (known after apply)
    + request_payer             = (known after apply)
    + tags                     = {
        + "Environment" = "Dev"
        + "Name"        = "My bucket"
    }
    + tags_all                 = {
        + "Environment" = "Dev"
        + "Name"        = "My bucket"
    }
    + website_domain           = (known after apply)
    + website_endpoint          = (known after apply)
    + cors_rule (known after apply)
    + grant (known after apply)
    + lifecycle_rule (known after apply)
    + logging (known after apply)
```

Step 5 : Type terraform apply command in powershell.

```
    }
+ tags_all          = {
  + "Name" = "My bucket"
}
+ website_domain      = (known after apply)
+ website_endpoint     = (known after apply)

+ cors_rule (known after apply)
+ grant (known after apply)
+ lifecycle_rule (known after apply)
+ logging (known after apply)
+ object_lock_configuration (known after apply)
+ replication_configuration (known after apply)
+ server_side_encryption_configuration (known after apply)
+ versioning (known after apply)
+ website (known after apply)
}

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

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

Enter a value: yes

aws_s3_bucket.bucket: Creating...
aws_s3_bucket.bucket: Creation complete after 5s [id=bucket-pranav-123]

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.
```

```
    }
+ tags_all          = {
  + "Name" = "My bucket"
}
+ website_domain      = (known after apply)
+ website_endpoint     = (known after apply)

+ cors_rule (known after apply)
+ grant (known after apply)
+ lifecycle_rule (known after apply)
+ logging (known after apply)
+ object_lock_configuration (known after apply)
+ replication_configuration (known after apply)
+ server_side_encryption_configuration (known after apply)
+ versioning (known after apply)
+ website (known after apply)
}

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

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

Enter a value: yes

aws_s3_bucket.bucket: Creating...
aws_s3_bucket.bucket: Creation complete after 5s [id=bucket-pranav-123]

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.
```

Step 6 : AWS s3 before and after the bucket creation using terraform.

BEFORE -

General purpose buckets (3) Info All AWS Regions			
Buckets are containers for data stored in S3.			
Name		AWS Region	IAM Access Analyzer
<input type="radio"/>	codepipeline-eu-north-1-21903055499	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1
<input type="radio"/>	elasticbeanstalk-eu-north-1-869935102438	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1

AFTER -

General purpose buckets (3) Info All AWS Regions			
Buckets are containers for data stored in S3.			
Name		AWS Region	IAM Access Analyzer
<input type="radio"/>	codepipeline-eu-north-1-21903055499	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1
<input type="radio"/>	elasticbeanstalk-eu-north-1-869935102438	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1
<input type="radio"/>	sanket-bucket1	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1

Step 7 : Upload file to the bucket using terraform .

CODE -

```
terraform {  
    required_providers {  
        aws = {  
            source = "hashicorp/aws"  
            version = "~> 5.0"{}  
        }  
    }  
    # Configure the AWS Provider  
    provider "aws" {  
        region = "us-east-1"  
        access_key = ""  
        secret_key = ""}  
        resource "aws_s3_bucket" "bucket" {  
            bucket = "bucket-pranav-123"  
            tags = {  
                Name = "My bucket"}  
        }
```

```

resource "aws_s3_bucket_object" "file" {

bucket = aws_s3_bucket.bucket.id

key = "hello.txt"

source = "C:/Users/sbpol/Documents/terraform_scripts/docker/s3/hello.txt"}


resource "aws_s3_bucket" "bucket" {
  bucket = "bucket-pranav-123"

  tags = {
    Name = "My bucket"
  }
}

resource "aws_s3_bucket_object" "file" {
  bucket = aws_s3_bucket.bucket.id
  key    = "hello.txt"
  source = "C:/Users/sbpol/Documents/terraform_scripts/docker/s3/hello.txt"
}

```

Step 8 : Terraform plan and apply command to apply the changes for file .

```

(base) PS C:\Users\sbpol\Documents\terraform_scripts\docker\s3> terraform plan
aws_s3_bucket.bucket: Refreshing state... [id=bucket-pranav-123]

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

Terraform will perform the following actions:

# aws_s3_bucket_object.file will be created
+ resource "aws_s3_bucket_object" "file" {
  + acl          = "private"
  + arn          = (known after apply)
  + bucket       = "bucket-pranav-123"
  + bucket_key_enabled = (known after apply)
  + content_type = (known after apply)
  + etag         = (known after apply)
  + force_destroy = false
  + id           = (known after apply)
  + key          = "hello.txt"
  + kms_key_id   = (known after apply)
  + server_side_encryption = (known after apply)
  + source        = "C:/Users/sbpol/Documents/terraform_scripts/docker/s3/hello.txt"
  + storage_class = (known after apply)
  + tags_all     = (known after apply)
  + version_id   = (known after apply)
}

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

Warning: Deprecated Resource
  with aws_s3_bucket_object.file,
  on main.tf line 28, in resource "aws_s3_bucket_object" "file":
  28: resource "aws_s3_bucket_object" "file" {
    use the aws_s3_object resource instead
  (and one more similar warning elsewhere)

```

```
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.
(base) PS C:\Users\sbpol\Documents\terraform_scripts\docker\s3> terraform apply
aws_s3_bucket.bucket: Refreshing state... [id=bucket-pranav-123]

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

Terraform will perform the following actions:

# aws_s3_bucket_object.file will be created
+ resource "aws_s3_bucket_object" "file" {
    + acl           = "private"
    + arn           = "(known after apply)"
    + bucket        = "bucket-pranav-123"
    + bucket_key_enabled = "(known after apply)"
    + content_type   = "(known after apply)"
    + etag          = "(known after apply)"
    + force_destroy  = false
    + id            = "(known after apply)"
    + key           = "hello.txt"
    + kms_key_id    = "(known after apply)"
    + server_side_encryption = "(known after apply)"
    + source         = "C:/Users/sbpol/Documents/terraform_scripts/docker/s3/hello.txt"
    + storage_class  = "(known after apply)"
    + tags_all      = "(known after apply)"
    + version_id    = "(known after apply)"
}

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

Warning: Deprecated Resource
with aws_s3_bucket_object.file,
on main.tf line 28, in resource "aws_s3_bucket_object" "file":
28: resource "aws_s3_bucket_object" "file" {

use the aws_s3_object resource instead
(and one more similar warning elsewhere)
```

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

Enter a value: yes

aws_s3_bucket_object.file: Creating...
aws_s3_bucket_object.file: Creation complete after 1s [id=hello.txt]

Warning: Deprecated Resource
with aws_s3_bucket_object.file,
on main.tf line 28, in resource "aws_s3_bucket_object" "file":
28: resource "aws_s3_bucket_object" "file" {

use the aws_s3_object resource instead

Warning: Argument is deprecated
with aws_s3_bucket_object.file,
on main.tf line 29, in resource "aws_s3_bucket_object" "file":
29:   bucket = aws_s3_bucket.bucket.id

Use the aws_s3_object resource instead
(and one more similar warning elsewhere)

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.
(base) PS C:\Users\sbpol\Documents\terraform_scripts\docker\s3>
```

Step 9 : s3 bucket before and after execution of upload

Name	Type	Last modified	Size	Storage class
index21.html	html	August 19, 2024, 17:24:08 (UTC+05:30)	3.8 KB	Standard
pic1.jpg	jpg	August 19, 2024, 17:24:09 (UTC+05:30)	44.0 KB	Standard

Step 10 : Terraform destroy command to destroy the s3 bucket.

```
(base) PS C:\Users\sbpol\Documents\terraform_scripts\docker\s3> terraform destroy
aws_s3_bucket.bucket: Refreshing state... [id=bucket-pranav-123]
aws_s3_bucket_object.file: Refreshing state... [id=hello.txt]

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

Terraform will perform the following actions:

# aws_s3_bucket.bucket will be destroyed
- resource "aws_s3_bucket" "bucket" {
    - arn                  = "arn:aws:s3:::bucket-pranav-123" -> null
    - bucket               = "bucket-pranav-123" -> null
    - bucket_domain_name   = "bucket-pranav-123.s3.amazonaws.com" -> null
    - bucketRegionalDomainName = "bucket-pranav-123.s3.us-east-1.amazonaws.com" -> null
    - force_destroy         = false -> null
    - hosted_zone_id       = "Z3AQBSTGFYJSTF" -> null
    - id                   = "bucket-pranav-123" -> null
    - object_lock_enabled  = false -> null
    - region               = "us-east-1" -> null
    - request_payer        = "BucketOwner" -> null
    - tags                 = {
        - "Name" = "My bucket"
    } -> null
    - tags_all              = {
        - "Name" = "My bucket"
    } -> null
    # (3 unchanged attributes hidden)

    - grant {
        - id          = "10def03d73e09d8adda11bfe68e632f70a83a37758b74ea6e933dafd0250c850" -> null
        - permissions = [
            - "FULL_CONTROL",
        ] -> null
        - type        = "CanonicalUser" -> null
        # (1 unchanged attribute hidden)
    }

    - server_side_encryption_configuration {
```

```
        }
    }

- versioning {
  - enabled      = false -> null
  - mfa_delete   = false -> null
}
}

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

Warning: Deprecated Resource
with aws_s3_bucket_object.file,
on main.tf line 28, in resource "aws_s3_bucket_object" "file":
28: resource "aws_s3_bucket_object" "file" {

use the aws_s3_object resource instead

Warning: Argument is deprecated
with aws_s3_bucket_object.file,
on main.tf line 30, in resource "aws_s3_bucket_object" "file":
30:   key      = "hello.txt"

Use the aws_s3_object resource instead

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

Enter a value: yes

aws_s3_bucket.bucket: Destroying... [id=bucket-pranav-123]
aws_s3_bucket.bucket: Destruction complete after 1s

Destroy complete! Resources: 1 destroyed.
(base) PS C:\Users\sbpol\Documents\terraform_scripts\docker\s3>
```

EXPERIMENT 7

Sanket More

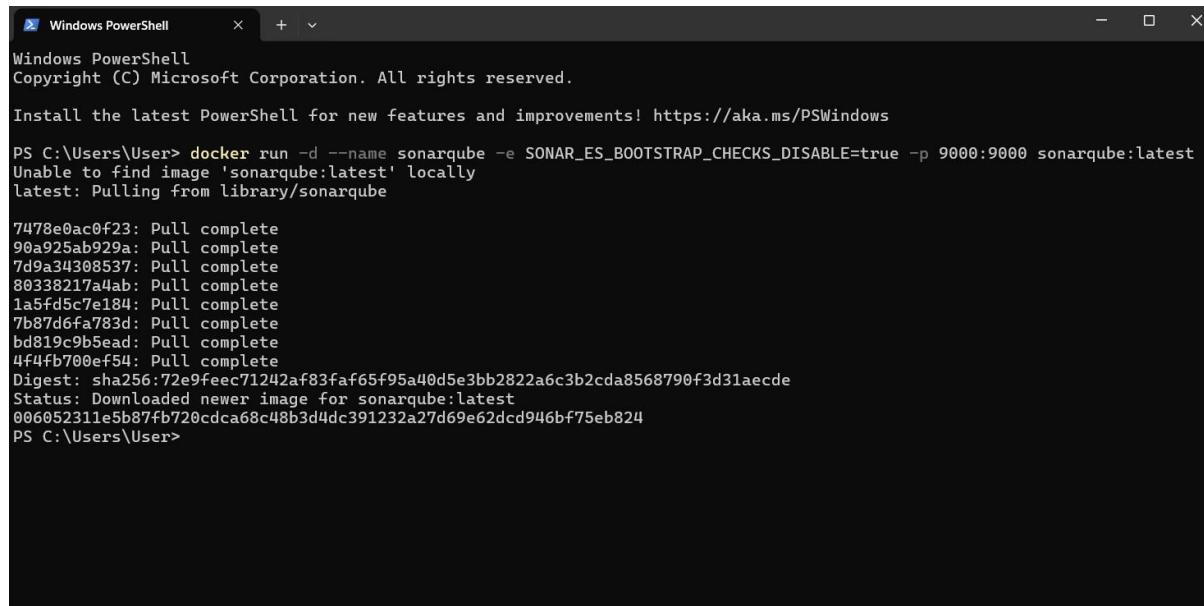
D15A 30

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

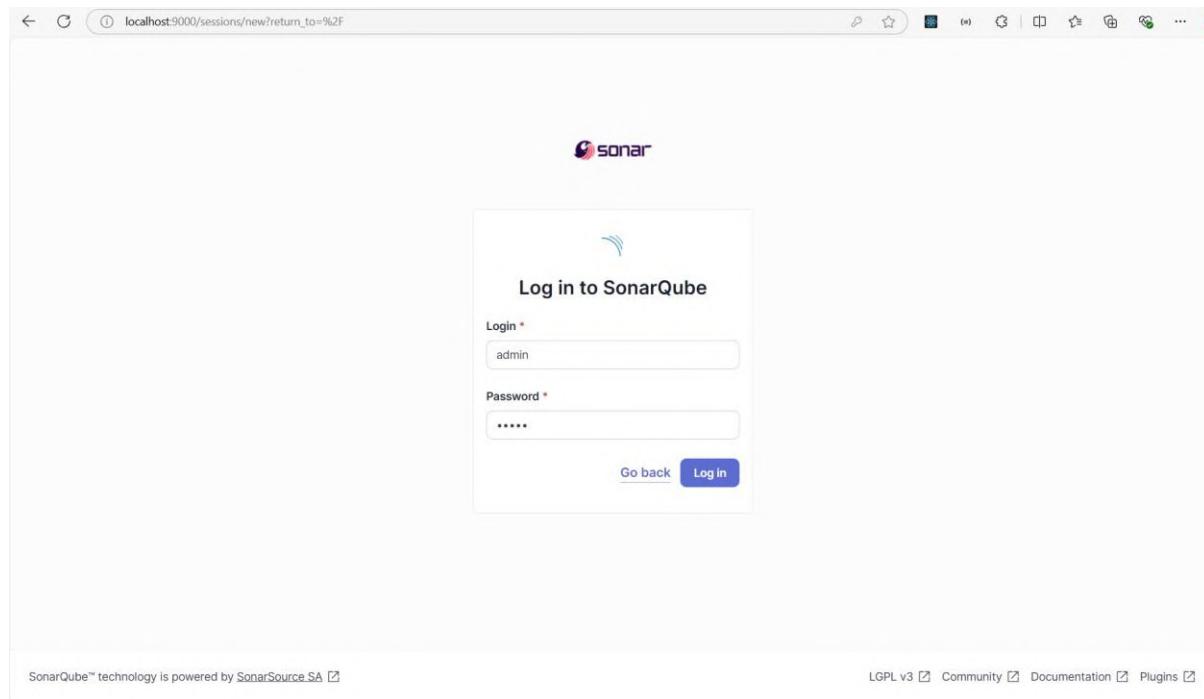


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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
006052311e5b87fb720cdca68c48b3d4dc391232a27d69e62dc946bf75eb824
PS C:\Users\User>
```

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



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

LGPL v3 ▾ Community ▾ Documentation ▾ Plugins ▾

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 Import from Bitbucket Cloud Import from Bitbucket Server

Import from GitHub Import from GitLab

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 Documentation Web API

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 Documentation 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.

Recommended for projects using feature branches.

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.

Dashboard > Manage Jenkins

Manage Jenkins

New version of Jenkins (2.462.2) is available for download (changelog). [Or Upgrade Automatically](#)

Building on the built-in node can be a security issue. You should set the number of executors on the built-in node to 0. See [the documentation](#). [Manage](#) [Dismiss](#)

Warnings have been published for the following currently installed components:

Jenkins 2.452.3 core and libraries:
[Multiple security vulnerabilities in Jenkins 2.470 and earlier, LTS 2.452.3 and earlier](#)
A fix for this issue is available. Update Jenkins now.

[Configure which of these warnings are shown](#)

System Configuration

- System**: Configure global settings and paths.
- Tools**: Configure tools, their locations and automatic installers.
- Nodes**: Add, remove, control and monitor the various nodes that Jenkins runs jobs on.
- Clouds**: Add, remove, and configure cloud instances to provision agents on-demand.
- Plugins**: ²⁹ Add, remove, disable or enable plugins that can extend the functionality of Jenkins.
- Appearance**: Configure the look and feel of Jenkins

localhost:8080/manage/pluginManager

Dashboard > Manage Jenkins > Plugins

The screenshot shows the Jenkins 'Plugins' page. A search bar at the top contains the text 'sonar'. Below it, a sidebar on the left lists 'Updates', 'Available plugins', 'Installed plugins' (which is selected), and 'Advanced settings'. The main content area displays a single plugin entry: 'SonarQube Scanner for Jenkins 2.17.2'. The entry includes a description: 'This plugin allows an easy integration of SonarQube, the open source platform for Continuous Inspection of code quality.', a 'Report an issue with this plugin' link, and two buttons: a blue 'Enabled' button with a checkmark and a red 'Disabled' button with a crossed-out circle.

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.

Dashboard > Manage Jenkins

The screenshot shows the Jenkins 'Manage Jenkins' page. On the left, there's a sidebar with links like 'New Item', 'Build History', 'Project Relationship', 'Check File Fingerprint', 'Manage Jenkins' (which is selected), and 'My Views'. Below this is a 'Build Queue' section. The main content area is titled 'Manage Jenkins' and features several status and configuration sections. One section says 'New version of Jenkins (2.462.2) is available for download (changelog)' with a 'Or Upgrade Automatically' button. Another section about built-in nodes has 'Manage' and 'Dismiss' buttons. A warning about security vulnerabilities in Jenkins 2.452.3 core and libraries has a 'Configure which of these warnings are shown' button. The 'System Configuration' section contains links for 'System', 'Tools', 'Nodes', 'Clouds', 'Plugins' (with a count of 29), and 'Appearance'. The 'Build Executor Status' sidebar shows 1 idle node named 'Slave1' (offline). The URL in the address bar is 'localhost:8080/manage/configure'.

SonarQube servers

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

Environment variables

SonarQube installations

List of SonarQube installations

Name
sonarqube

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

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.

+ New Item

Build History

Project Relationship

Check File Fingerprint

Manage Jenkins

My Views

Build Queue

Build Executor Status

Built-In Node

1 Idle

2 Idle

Slave1

Manage Jenkins

Search settings /

New version of Jenkins (2.462.2) is available for [download \(changelog\)](#).

[Or Upgrade Automatically](#)

Building on the built-in node can be a security issue. You should set the number of executors on the built-in node to 0. See [the documentation](#).

[Manage](#)

[Dismiss](#)

Warnings have been published for the following currently installed components:

Jenkins 2.452.3 core and libraries:
[Multiple security vulnerabilities in Jenkins 2.470 and earlier, LTS 2.452.3 and earlier](#)
 A fix for this issue is available. Update Jenkins now.

[Configure which of these warnings are shown](#)

System Configuration

System

Configure global settings and paths.

Tools

Configure tools, their locations and automatic installers.

 Plugins 29

Add, remove, disable or enable plugins that can extend the functionality of Jenkins.

Nodes

Add, remove, control and monitor the various nodes that Jenkins runs jobs on.

Clouds

Add, remove, and configure cloud instances to provision agents on-demand.

Appearance

Configure the look and feel of Jenkins

SonarScanner for MSBuild installations

[Add SonarScanner for MSBuild](#)

SonarQube Scanner installations

[Add SonarQube Scanner](#)

SonarQube Scanner

Name: sonarqubescanner

Install automatically ?

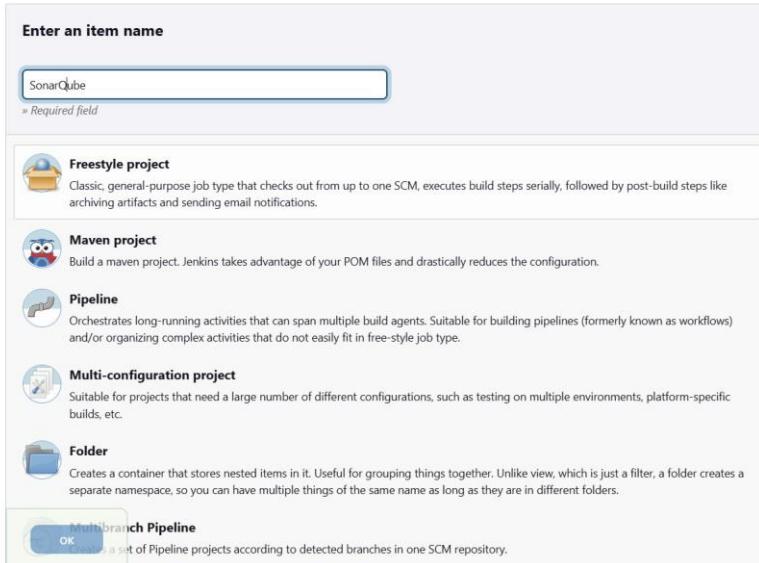
Install from Maven Central

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.



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**

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

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**

JDK to be used for this SonarQube analysis

(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**

Dashboard > SonarQube >

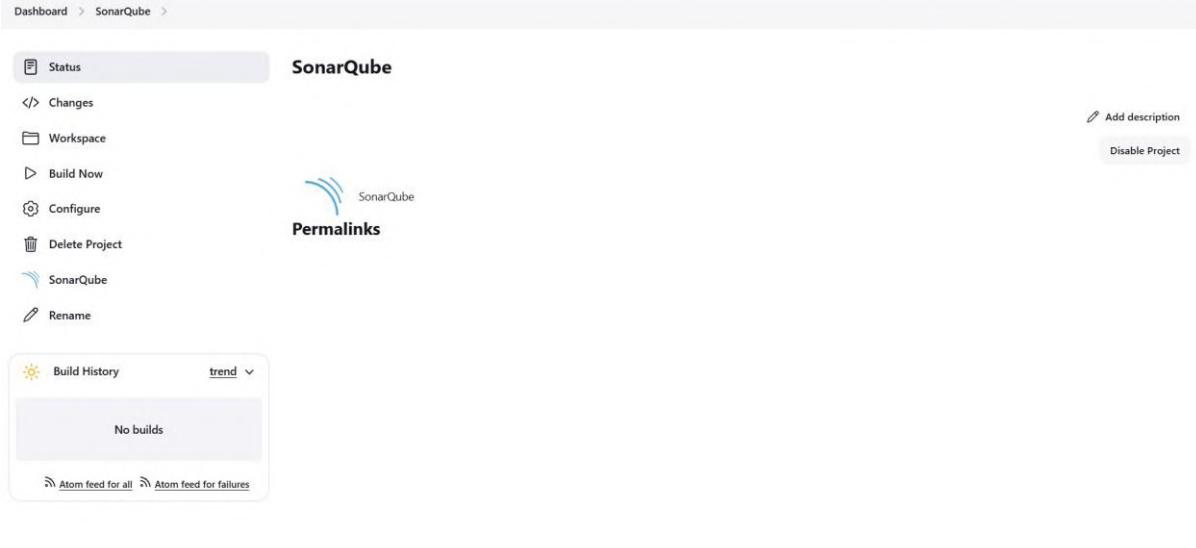
SonarQube

Status Changes Workspace Build Now Configure Delete Project SonarQube Rename

Permalinks

Build History trend ▾ No builds Atom feed for all Atom feed for failures

Add description Disable Project 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.

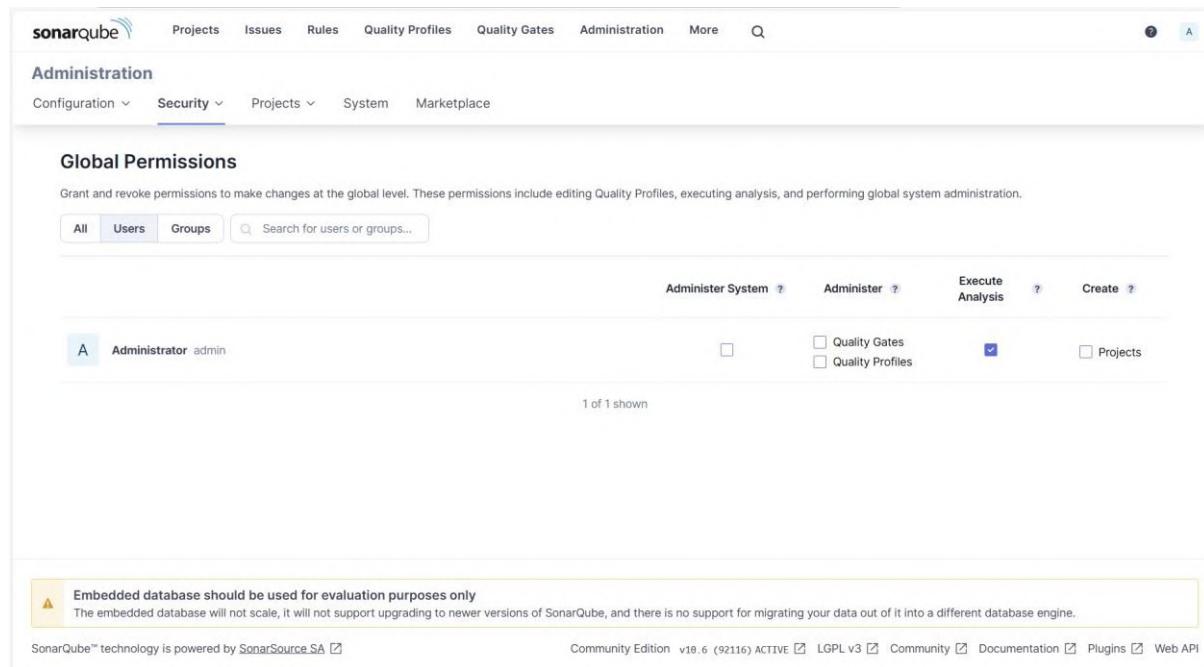
All Users Groups Search for users or groups...

Administrator System ? Administer ? Execute Analysis ? Create ?

Administrator	admin	<input type="checkbox"/>	<input type="checkbox"/> Quality Gates	<input checked="" type="checkbox"/> Quality Profiles	<input type="checkbox"/> 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 GPL v3 Community Documentation Plugins Web API



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

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 6.2.0.4584
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# 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
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 C# File Caching Sensor [csharp]
18:40:41.489 WARN Incremental PR analysis: Could not determine common base path, cache will not be computed. Consider setting
'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 submitted analysis report
18:40:42.882 INFO More about the report processing at http://localhost:9000/api/ce/task?id=d10eb30d-ebdd-4bb2-b564-0aa4ea71b0f2
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

```

REST API Jenkins 2.452.3

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 Q ?

sonarqube-test / main ?

Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information

main Version not provided Set as homepage Last analysis 14 minutes ago

Quality Gate Passed

The last analysis has warnings. See details

New Code Overall Code

Security	Reliability	Maintainability
0 Open issues (A)	0 Open issues (A)	0 Open issues (A)
0 H 0 M 0 L	0 H 0 M 0 L	0 H 0 M 0 L

Accepted issues	Coverage	Duplications
0 (2)	On 0 lines to cover.	0.0% (86)

Security Hotspots

This screenshot shows the SonarQube dashboard for the 'main' branch of the 'sonarqube-test' project. The top navigation bar includes links for Projects, Issues, Rules, Quality Profiles, Quality Gates, Administration, More, and a search bar. The dashboard header displays the project name, a green 'Passed' status for the quality gate, and the last analysis time (14 minutes ago). A prominent message indicates there are warnings in the latest analysis. Below this, two tabs are shown: 'New Code' and 'Overall Code', with 'Overall Code' being selected. The main content area is divided into three columns: Security, Reliability, and Maintainability, each showing zero open issues with an 'A' grade. Below these are sections for Accepted issues (0), Coverage (0.0%), and Duplications (0.0% on 86 lines). A 'Security Hotspots' section is also present at the bottom. The overall interface is clean and modern, using a light color palette and large, legible typography.

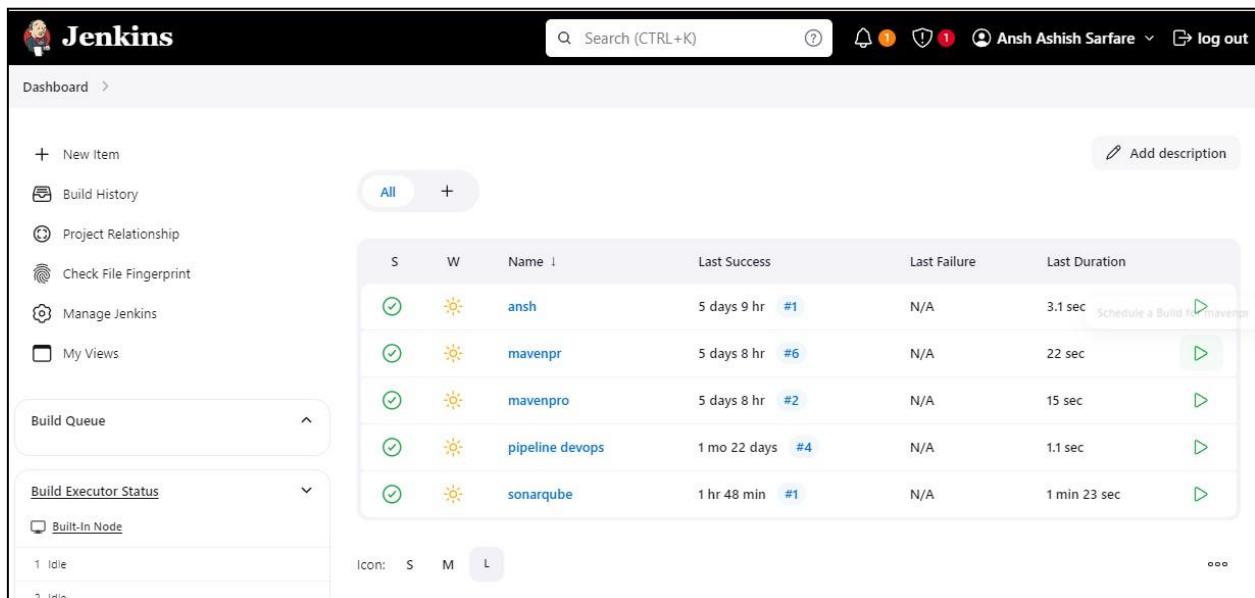
ADVANCE DEVOPS EXP-8

Sanket More

D15A 30

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: Open up Jenkins Dashboard on localhost, port 8080 or whichever port it is atfor you.



The screenshot shows the Jenkins dashboard with the following details:

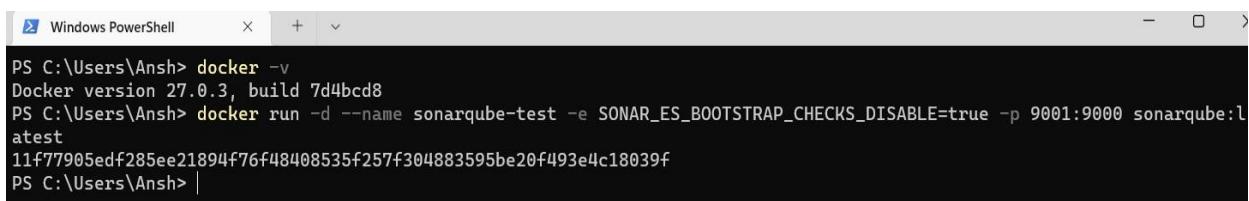
- Left Sidebar:** Includes links for "New Item", "Build History", "Project Relationship", "Check File Fingerprint", "Manage Jenkins", and "My Views".
- Build Queue:** Shows 1 idle node.
- Build Executor Status:** Shows 2 idle nodes.
- Central View:** A table listing Jenkins projects:

S	W	Name ↓	Last Success	Last Failure	Last Duration
✓	☀️	ansh	5 days 9 hr #1	N/A	3.1 sec
✓	☀️	mavenpr	5 days 8 hr #6	N/A	22 sec
✓	☀️	mavenpro	5 days 8 hr #2	N/A	15 sec
✓	☀️	pipeline devops	1 mo 22 days #4	N/A	1.1 sec
✓	☀️	sonarqube	1 hr 48 min #1	N/A	1 min 23 sec

Step-2: Run SonarQube in a Docker container using this command :- a]docker -vb]

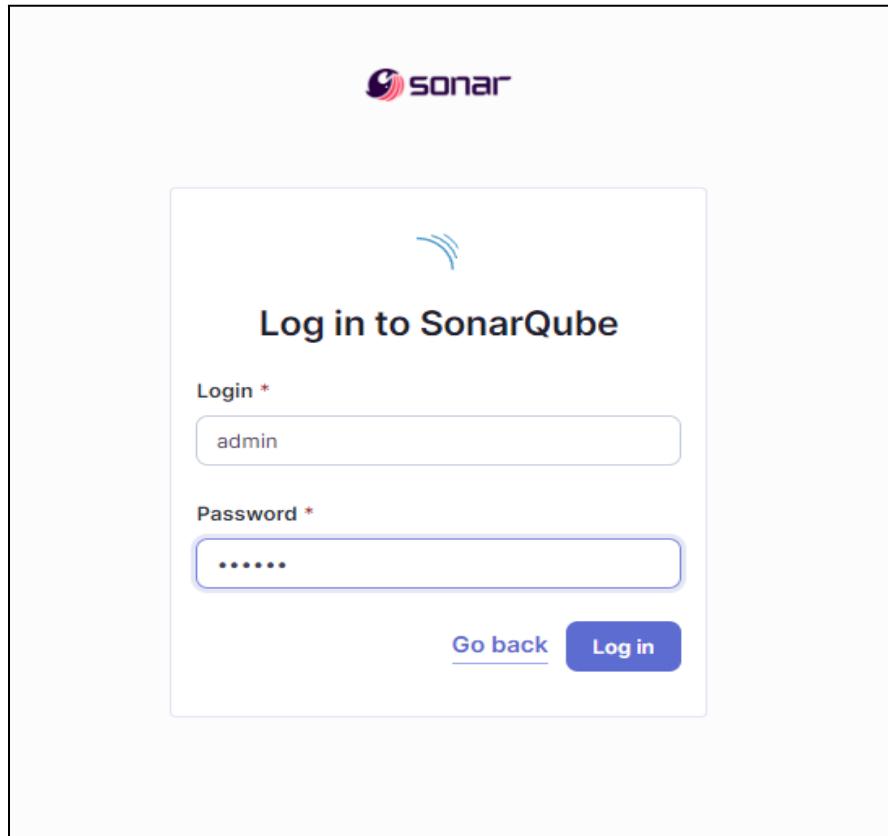
```
docker run -d --name sonarqube-test -e
```

```
SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9001:9000 sonarqube:latest
```



```
PS C:\Users\Ansh> docker -v
Docker version 27.0.3, build 7d4bcd8
PS C:\Users\Ansh> docker run -d --name sonarqube-test -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9001:9000 sonarqube:latest
11f77905edf285ee21894f76f48408535f257f304883595be20f493e4c18039f
PS C:\Users\Ansh>
```

Step-3: Once the container is up and running, you can check the status of SonarQbeat on localhost port 9001. The login id is “admin” and the password is also “ansh16”.



Step-4: Create a local project in SonarQube with the name sonarqube-test.

1 of 2

Create a local project

Project display name *

 ✓

Project key *

 ✓

Main branch name *

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

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

Step-5: Setup the project and come back to Jenkins Dashboard.

The screenshot shows the 'Set up project for Clean as You Code' configuration page. At the top, it says '2 of 2' and 'Set up project for Clean as You Code'. Below that, a note states: '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'.

Under the heading 'Choose the baseline for new code for this project', there are two options:

- 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.
 - Recommended for projects using feature branches.

At the bottom, there are 'Back' and 'Create project' buttons.

Step-6: Create a New Item in Jenkins, choose Pipeline.

The screenshot shows the Jenkins 'New Item' creation page. The title is 'New Item'. A search bar at the top right contains 'Search (CTRL+K)'. On the left, a sidebar shows 'Dashboard > All > New Item'.

The main area is titled 'New Item' and contains a form to 'Enter an item name' with the value 'sonarqube-test'.

Below the form, a section titled 'Select an item type' lists several options:

- Freestyle project
 - Icon: A cube.
 - Description: 'Freestyle project'.
 - Text: '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
 - Icon: An owl.
 - Description: 'Maven project'.
 - Text: 'Build a maven project. Jenkins takes advantage of your POM files and drastically reduces the configuration.'
- Pipeline
 - Icon: A gear.
 - Description: 'Pipeline'.
 - Text: '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
 - Icon: A document with a gear.
 - Description: 'Multi-configuration project'.
 - Text: 'Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.'
- Folder
 - Icon: A folder.
 - Description: 'Folder'.
 - Text: '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
 - Icon: A pipeline icon.
 - Description: 'Multibranch Pipeline'.
 - Text: 'Creates a set of Pipeline projects according to detected branches in one SCM repository.'
- Organization Folder
 - Icon: A folder with multiple subfolders.
 - Description: 'Organization Folder'.
 - Text: 'Creates a set of multibranch project subfolders by scanning for repositories.'

Step-7: Under Pipeline Script, enter the following -

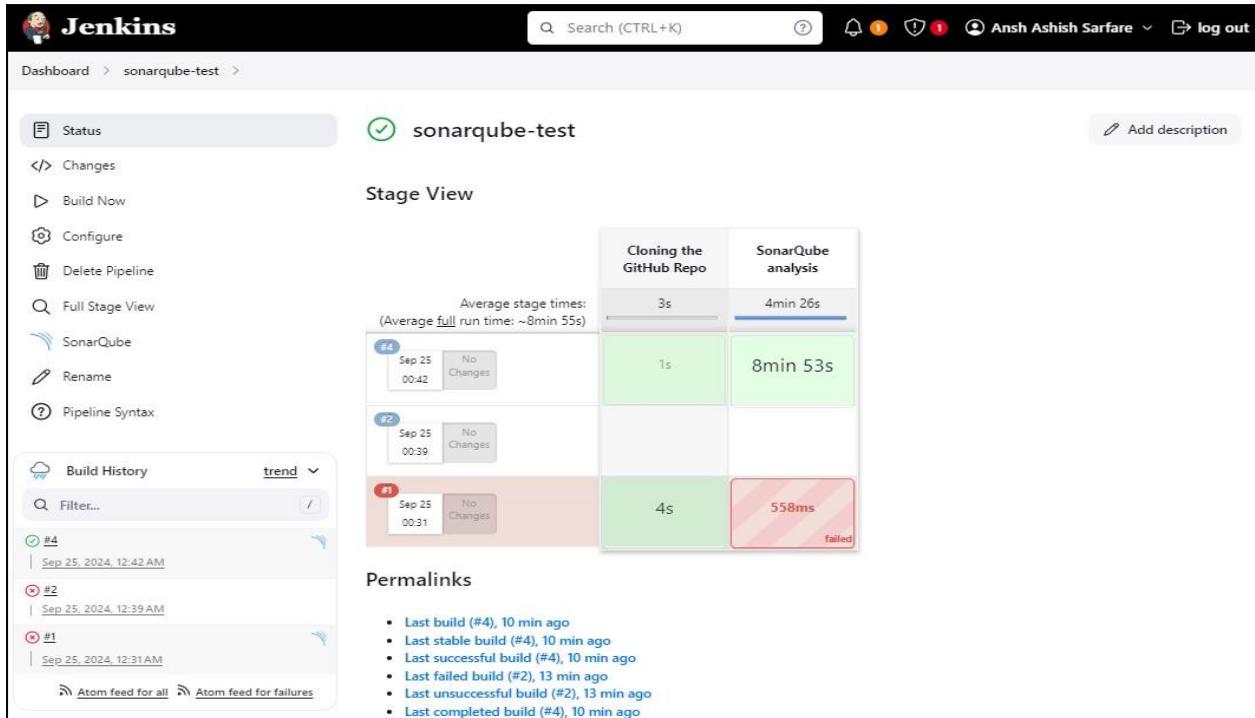
```
node {  
    stage('Cloning the GitHub Repo')  
    {  
        git 'https://github.com/shazforiot/GOL.git'  
    }  
    stage('SonarQube analysis') {  
        withSonarQubeEnv('sonarqube') {bat  
            "C:\\Users\\Ansh\\Downloads\\sonar-scanner-cli-6.1.0.4477-windows-x64\\sonar-scanner-6.1.0. 4477-  
            windows-x64\\bin\\sonar-scanner.bat \  
            -D sonar.login=admin \  
            -D sonar.password=ansh16 \  
            -D sonar.projectKey=sonarqube-test \  
            -D sonar.exclusions=vendor/**,resources/**,**/*.java \  
            -D sonar.host.url=http://localhost:9001/"  
        }  
    }  
}
```

The screenshot shows the Jenkins Pipeline configuration interface. The top navigation bar has 'Pipeline' selected. Below it, the 'Definition' section is set to 'Pipeline script'. The main area contains a code editor with the Groovy script from the previous step. A checkbox labeled 'Use Groovy Sandbox' is checked. At the bottom, there are 'Save' and 'Apply' buttons.

```
1+ node {  
2+     stage('Cloning the GitHub Repo') {  
3+         git 'https://github.com/shazforiot/GOL.git'  
4+     }  
5+     stage('SonarQube analysis') {  
6+         withSonarQubeEnv('sonarqube') {  
7+             bat ***  
8+                 C:/Users/Ansh/Downloads/sonar-scanner-cli-6.1.0.4477-windows-x64/sonar-scanner-6.1.0.4477-windows-x64/bin/sonar-scanner.bat ^  
9+                 -D sonar.login=admin ^  
10+                -D sonar.password=ansh16 ^  
11+                -D sonar.projectKey=sonarqube-test ^  
12+                -D sonar.exclusions=vendor/**,resources/**,**/*.java ^  
13+                -D sonar.host.url=http://127.0.0.1:9001/  
14+            ***  
15+        }  
16+    }  
17+ }
```

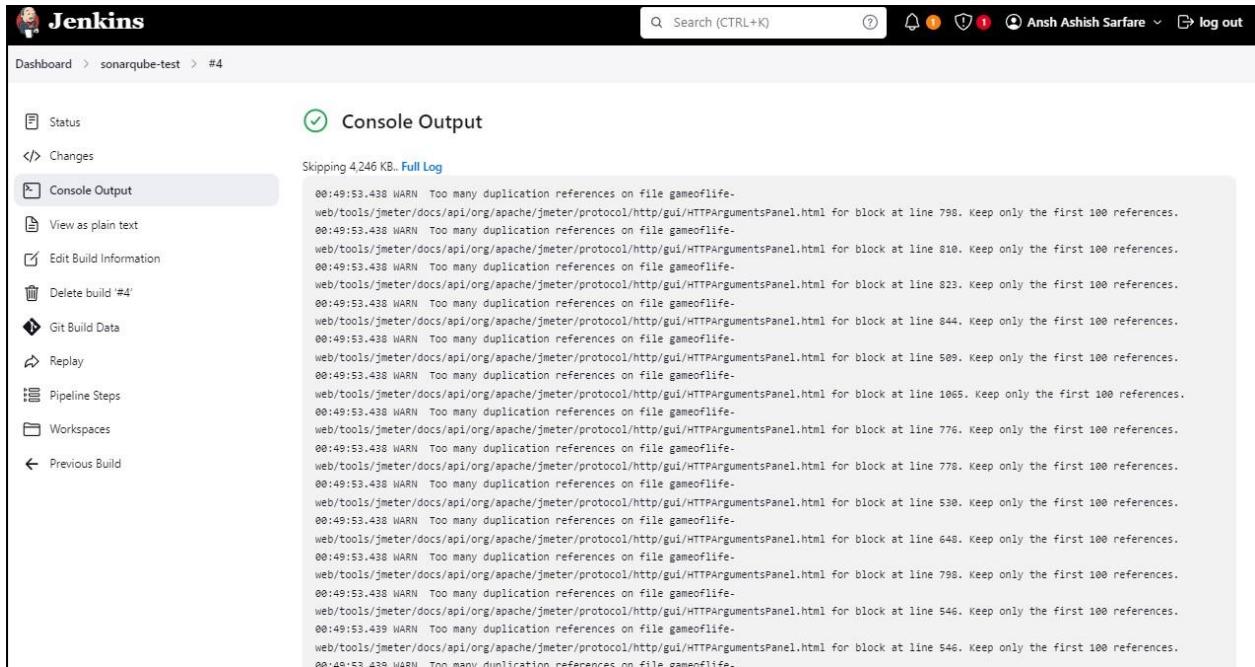
It is a java sample project which has a lot of repetitions and issues that will be detected by SonarQube.

Step-8: Run The Build and check the console output:



The screenshot shows the Jenkins Pipeline interface for the 'sonarqube-test' pipeline. On the left, there's a sidebar with various Jenkins-related links like Status, Changes, Build Now, Configure, Delete Pipeline, Full Stage View, SonarQube, Rename, and Pipeline Syntax. Below that is the 'Build History' section, which lists three builds: #4 (Sep 25, 2024, 12:42 AM), #2 (Sep 25, 2024, 12:39 AM), and #1 (Sep 25, 2024, 12:31 AM). At the bottom of the history are links for 'Atom feed for all' and 'Atom feed for failures'. The main area is titled 'Stage View' and displays two stages: 'Cloning the GitHub Repo' (3s) and 'SonarQube analysis' (4min 26s). The 'SonarQube analysis' stage is shown in a grid with three rows. Row 1 (Build #4) shows a green bar for the SonarQube analysis step with a duration of 8min 53s. Row 2 (Build #2) shows a green bar for the SonarQube analysis step with a duration of 558ms. Row 3 (Build #1) shows a red bar for the SonarQube analysis step with a duration of 558ms and the status 'failed'. Below the stage view is a 'Permalinks' section with a list of recent builds.

- Last build (#4), 10 min ago
- Last stable build (#4), 10 min ago
- Last successful build (#4), 10 min ago
- Last failed build (#2), 13 min ago
- Last unsuccessful build (#2), 13 min ago
- Last completed build (#4), 10 min ago



The screenshot shows the Jenkins Pipeline interface for build #4 of the 'sonarqube-test' pipeline. The left sidebar includes links for Status, Changes, Console Output (which is selected), View as plain text, Edit Build Information, Delete build #4, Git Build Data, Replay, Pipeline Steps, Workspaces, and Previous Build. The main content area is titled 'Console Output' and shows the start of the log: 'Skipping 4246 KB. Full Log'. The log itself consists of multiple lines of warning messages from the SonarQube analysis process, all related to duplicate references in files like gameoflife-. The messages are timestamped at 00:49:53.438 and mention 'Too many duplication references' in various JMeter protocol files.

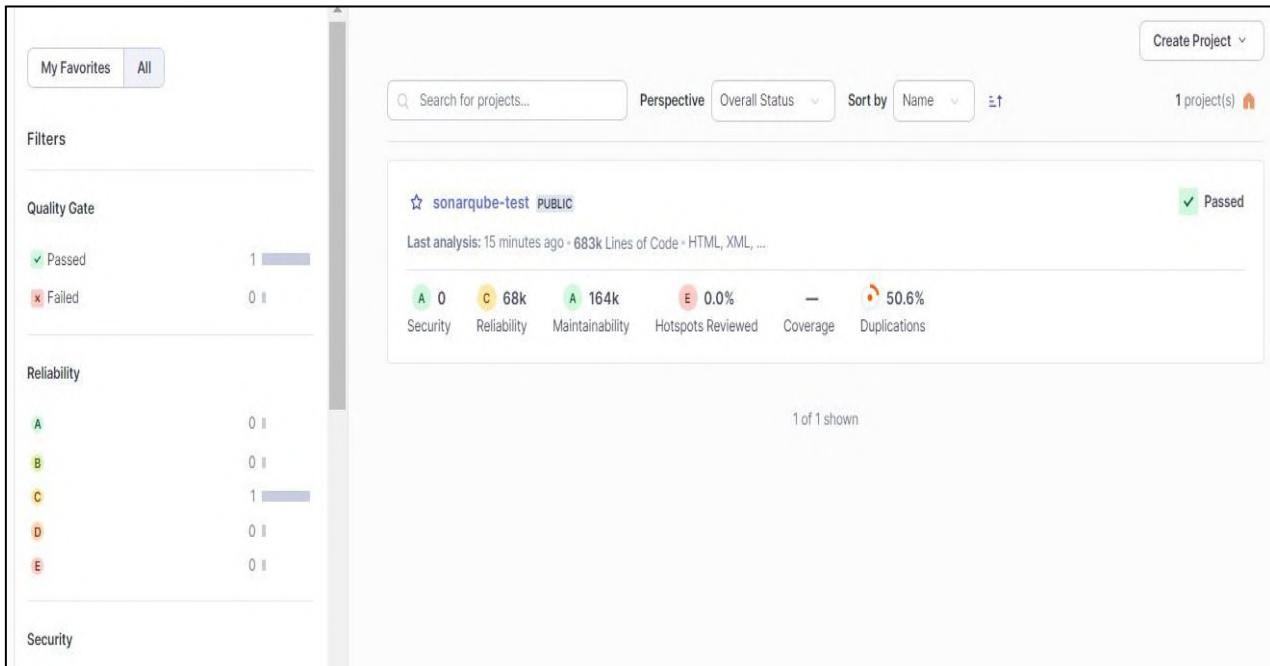
```
00:49:53.438 WARN Too many duplication references on file gameoflife-.  
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 798. Keep only the first 100 references.  
00:49:53.438 WARN Too many duplication references on file gameoflife-.  
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 810. Keep only the first 100 references.  
00:49:53.438 WARN Too many duplication references on file gameoflife-.  
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 823. Keep only the first 100 references.  
00:49:53.438 WARN Too many duplication references on file gameoflife-.  
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 844. Keep only the first 100 references.  
00:49:53.438 WARN Too many duplication references on file gameoflife-.  
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 860. Keep only the first 100 references.  
00:49:53.438 WARN Too many duplication references on file gameoflife-.  
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 1065. Keep only the first 100 references.  
00:49:53.438 WARN Too many duplication references on file gameoflife-.  
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 776. Keep only the first 100 references.  
00:49:53.438 WARN Too many duplication references on file gameoflife-.  
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 778. Keep only the first 100 references.  
00:49:53.438 WARN Too many duplication references on file gameoflife-.  
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 530. Keep only the first 100 references.  
00:49:53.438 WARN Too many duplication references on file gameoflife-.  
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 648. Keep only the first 100 references.  
00:49:53.438 WARN Too many duplication references on file gameoflife-.  
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 798. Keep only the first 100 references.  
00:49:53.439 WARN Too many duplication references on file gameoflife-.  
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 546. Keep only the first 100 references.  
00:49:53.439 WARN Too many duplication references on file gameoflife-.  
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 546. Keep only the first 100 references.  
00:49:53.439 WARN Too many duplication references on file gameoflife-.
```

```

00:49:56.323 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 31. Keep only the first 100 references
00:49:56.323 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 177. Keep only the first 100 references
00:49:56.323 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 180. Keep only the first 100 references
00:49:56.323 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 65. Keep only the first 100 references
00:49:56.323 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 349. Keep only the first 100 references
00:49:56.323 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 40. Keep only the first 100 references
00:49:56.323 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 75. Keep only the first 100 references
00:49:56.323 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 41. Keep only the first 100 references
00:49:56.324 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 17. Keep only the first 100 references
00:49:56.324 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 296. Keep only the first 100 references
00:49:56.324 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 75. Keep only the first 100 references
00:49:56.324 INFO SCM revision ID 'ba7990a7e1b576f04a4612322b0412c5e6e1e5e4'
00:51:38.402 INFO Analysis report generated in 2893ms, dir size=127.2 MB
00:51:40.652 INFO Analysis report compressed in 10210ms, zip size=29.6 MB
00:51:44.098 INFO Analysis report uploaded in 3444ms
00:51:44.101 INFO ANALYSIS SUCCESSFUL, you can find the results at: http://127.0.0.1:9001/dashboard?id=sonarqube-test
00:51:44.101 INFO Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
00:51:44.101 INFO More about the report processing at http://127.0.0.1:9001/api/ce/task?id=22b0b5c1-635d-4c1b-8d62-99d4ce4567b9
00:51:53.341 INFO Analysis total time: 8:44.093 s
00:51:53.349 INFO SonarScanner Engine completed successfully
00:51:54.059 INFO EXECUTION SUCCESS
00:51:54.071 INFO Total time: 8:51.363s
[Pipeline]
[Pipeline] // withSonarQubeEnv
[Pipeline]
[Pipeline] // stage
[Pipeline]
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS

```

Step-9: After that, check the project in SonarQube.



The screenshot shows the SonarQube main dashboard for the 'main' project. The top navigation bar includes Quality Profiles, Quality Gates, Administration, More, and a search bar. Below the navigation is a breadcrumb trail: Issues > Code > Activity. The main content area starts with a 'Quality Gate' section showing a green checkmark and the word 'Passed'. A yellow warning box indicates there are warnings, with a link to 'See details'. Below this are sections for New Code and Overall Code, followed by detailed metrics for Security, Reliability, and Maintainability. The Security section shows 0 Open issues (0 H, 0 M, 0 L). The Reliability section shows 68k Open issues (0 H, 47k M, 21k L). The Maintainability section shows 164k Open issues (7 H, 143k M, 21k L). Other sections include Accepted issues (0), Coverage (On 0 lines to cover), and Duplications (50.6% on 759k lines). At the bottom, there's an 'Activity' section and a dropdown menu for 'Issues'.

Step-10: Under different tabs, check all different issues with the code.

Code Problems

Code issues:

The screenshot shows the SonarQube interface with the 'sonarqube-test' project selected. The top navigation bar includes Projects, Issues, Rules, Quality Profiles, Quality Gates, Administration, More, and a search bar. Below the navigation is a breadcrumb trail: sonarqube-test / main. The main content area has tabs for Overview, Issues, Security Hotspots, Measures (which is active), Code, and Activity. On the right, there are buttons for Project Settings and Project Information. The left sidebar has a 'Project Overview' section with links for Security, Reliability, Overview, Overall Code, Issues (67624), Rating, Remediation Effort (1426d), Maintainability, Security Review, and Duplications. The right panel displays a list of issues under 'sonarqube-test' with 'View as' options (Tree, Select files, Navigate). The list includes: gameoflife-acceptance-tests (0), gameoflife-build (0), gameoflife-core (172), gameoflife-deploy (0), gameoflife-web (67452), and pom.xml (0). At the bottom, it says '6 of 6 shown'.

Consistency:

The screenshot shows the SonarQube Issues page for the project 'sonarqube-test / main'. The 'Issues' tab is selected. On the left, a sidebar shows filters for 'Clean Code Attribute' (selected 'Consistency'), 'Software Quality', 'Severity', and 'Type'. The main area displays several issues under the file 'gameoflife-core/build/reports/tests/all-tests.html'. Each issue has a checkbox, a title, a severity level (e.g., Reliability, Maintainability), and a detailed description. The 'Consistency' filter is highlighted in blue.

Issue Type	Title	Severity	Description
Consistency	Insert a <!DOCTYPE> declaration to before this <html> tag.	Reliability	L1 = 5min effort = 4 years ago ~ ⚙ Bug ~ ⚙ Major
Maintainability	Remove this deprecated "width" attribute.	Maintainability	L9 = 5min effort = 4 years ago ~ ⚙ Code Smell ~ ⚙ Major
Maintainability	Remove this deprecated "align" attribute.	Maintainability	L11 = 5min effort = 4 years ago ~ ⚙ Code Smell ~ ⚙ Major
Maintainability	Remove this deprecated "size" attribute.	Maintainability	L12 = 5min effort = 4 years ago ~ ⚙ Code Smell ~ ⚙ Major

Intentionally:

The screenshot shows the SonarQube Issues page for the project 'sonarqube-test / main'. The 'Issues' tab is selected. The sidebar shows filters for 'Clean Code Attribute' (selected 'Intentionality'), 'Software Quality', 'Severity', and 'Type'. The main area displays several issues under the file 'gameoflife-acceptance-tests/Dockerfile'. Each issue has a checkbox, a title, a severity level (e.g., Maintainability), and a detailed description. The 'Intentionality' filter is highlighted in blue.

Issue Type	Title	Severity	Description
Maintainability	Use a specific version tag for the image.	Maintainability	L1 = 5min effort = 4 years ago ~ ⚙ Code Smell ~ ⚙ Major
Maintainability	Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.	Maintainability	L12 = 5min effort = 4 years ago ~ ⚙ Code Smell ~ ⚙ Major
Maintainability	Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.	Maintainability	L12 = 5min effort = 4 years ago ~ ⚙ Code Smell ~ ⚙ Major
Maintainability	Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.	Maintainability	L13 = 5min effort = 4 years ago ~ ⚙ Code Smell ~ ⚙ Major

Reliability:

The screenshot shows the SonarQube Issues page for the project 'sonarqube-test'. The 'Issues' tab is selected. On the left, the 'Filters' sidebar is open, showing categories like 'Clean Code Attribute', 'Software Quality', 'Severity', and 'Type'. Under 'Type', 'Reliability' is selected. The main panel displays several code smell issues found in files like 'gameoflife-core/build/reports/tests/all-tests.html' and 'gameoflife-core/build/reports/tests/allclasses-frame.html'. Each issue has a checkbox, a title, an 'Intentionality' button (labeled 'Reliability'), and a status dropdown ('Open' or 'Not assigned'). Below each issue, there is a timestamp and severity information.

File	Issue Title	Intentionality	Status	Timestamp	Severity
gameoflife-core/build/reports/tests/all-tests.html	Add "lang" and/or "xml:lang" attributes to this "<html>" element	Reliability	Open	L1 + 2min effort + 4 years ago	Bug
gameoflife-core/build/reports/tests/alltests.html	Add "<th>" headers to this "<table>"	Reliability	Open	L9 + 2min effort + 4 years ago	Bug
gameoflife-core/build/reports/tests/allclasses-frame.html	Add "lang" and/or "xml:lang" attributes to this "<html>" element	Reliability	Open	L1 + 2min effort + 4 years ago	Bug
gameoflife-core/build/reports/tests/allclasses-frame.html	Add "<th>" headers to this "<table>"	Reliability	Open	L9 + 2min effort + 4 years ago	Bug

Code smells:

The screenshot shows the SonarQube Issues page for the project 'sonarqube-test'. The 'Issues' tab is selected. The 'Filters' sidebar is open, showing categories like 'Clean Code Attribute', 'Software Quality', 'Severity', 'Type', 'Scope', 'Status', 'Security Category', and 'Creation Date'. Under 'Type', 'Code Smell' is selected. The main panel displays code smell issues found in files such as 'gameoflife-acceptance-tests/Dockerfile', 'gameoflife-core/...', and 'gameoflife-core/.../com/wakaleo/gameoflife/domain/0_WhenYouCreateACell.html'. Each issue has a checkbox, a title, an 'Intentionality' button (labeled 'Maintainability'), and a status dropdown ('Open' or 'Not assigned'). Below each issue, there is a timestamp and severity information.

File	Issue Title	Intentionality	Status	Timestamp	Severity
gameoflife-acceptance-tests/Dockerfile	Use a specific version tag for the image.	Maintainability	Open	L1 + 5min effort + 4 years ago	Code Smell
gameoflife-core/...	Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.	Maintainability	Open	L12 + 5min effort + 4 years ago	Code Smell
gameoflife-core/.../com/wakaleo/gameoflife/domain/0_WhenYouCreateACell.html	Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.	Maintainability	Open	L13 + 5min effort + 4 years ago	Code Smell

Security hotspot:

The screenshot shows the SonarQube interface for a project named "sonarqube-test". The "Security Hotspots" tab is selected. A prominent alert states: "The tomcat image runs with root as the default user. Make sure it is safe here." Below this, a status box says "To review". To the right, detailed information is provided: "Review priority: Medium", "Category: Permission", and "Assignee: Not assigned". A "Review" button is available. Below the alert, a code snippet from a Dockerfile is shown, highlighting the line "FROM tomcat:9.0-jre8". The Dockerfile also includes "RUN rm -rf /usr/local/tomcat/webapps/*", "COPY target/gameoflife.war /usr/local/tomcat/webapps/ROOT.war", "EXPOSE 8080", and "CMD ["catalina.sh", "run"]".

Duplicates:

The screenshot shows the SonarQube interface for the same project, with the "Measures" tab selected. On the left, a sidebar displays various metrics: Overall Code (Security Hotspots: 3), Rating (E), Security Hotspots Reviewed (0.0%), and Duplications (Density: 50.6%, Duplication Lines: 384,007). The main panel shows a tree view of the project structure under "sonarqube-test". The "gameoflife-web" module has the highest duplication density at 50.9% (383,633 lines). Other modules like "gameoflife-core" and "gameoflife-deploy" show lower densities. A summary at the bottom indicates 6 of 6 files are shown.

Size:

The screenshot shows the SonarQube interface for the project 'sonarqube-test'. The left sidebar has tabs for 'Overview', 'Issues', 'Security Hotspots', 'Measures' (selected), 'Code', and 'Activity'. The right panel displays 'Lines of Code' statistics for the project, showing a total of 682,883 lines across 6 files. The breakdown by file type is: HTML (678k), XML (4.7k), JSP (332), CSS (110), Docker (19). Below this, a tree view shows the directory structure: gameoflife-acceptance-tests (164), gameoflife-build (368), gameoflife-core (3,675), gameoflife-deploy (69), gameoflife-web (678,148), and pom.xml (459).

File Type	Count
HTML	678k
XML	4.7k
JSP	332
CSS	110
Docker	19

File	Size
gameoflife-acceptance-tests	164
gameoflife-build	368
gameoflife-core	3,675
gameoflife-deploy	69
gameoflife-web	678,148
pom.xml	459

Complexity:

The screenshot shows the SonarQube interface for the project 'sonarqube-test'. The left sidebar has tabs for 'Overview', 'Issues', 'Security Hotspots', 'Measures' (selected), 'Code', and 'Activity'. The right panel displays 'Cyclomatic Complexity' statistics for the project, showing a total of 1,112 across 6 files. The breakdown by file type is: gameoflife-acceptance-tests (—), gameoflife-build (—), gameoflife-core (18), gameoflife-deploy (—), gameoflife-web (1,094), and pom.xml (—). Below this, a tree view shows the directory structure.

File	Complexity
gameoflife-acceptance-tests	—
gameoflife-build	—
gameoflife-core	18
gameoflife-deploy	—
gameoflife-web	1,094
pom.xml	—

Advanced DevOps Exp-9

Sanket More

D15A 30

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

Procedure:-

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

The screenshot shows the 'Name and tags' section of the AWS EC2 'Launch an instance' wizard. The 'Name' field contains 'Nagios-host'. There is also a link to 'Add additional tags'.

The screenshot shows the 'Instance type' section of the AWS EC2 'Launch an instance' wizard. The selected instance type is 't3.medium'. A detailed description of the instance type is provided, including family information, On-Demand base pricing, and supported operating systems. A note at the bottom states: 'Additional costs apply for AMIs with pre-installed software'. There are also links to 'All generations' and 'Compare instance types'.

Create security group

Select existing security group

We'll create a new security group called '**launch-wizard-12**' with the following rules:

Allow SSH traffic from

Helps you connect to your instance

Anywhere

0.0.0.0/0

Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like EC2 Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, and more. The main area is titled 'Instances (1/2) Info' and shows two instances: '30SAN-env' (i-089082d105bc9beeb) and 'Nagios-host' (i-0a27c2927b0cf759c). Both instances are listed as 'Running' with 't3.micro' or 't3.medium' instance types. The 'Nagios-host' instance is selected. The interface includes filters, actions, and launch instance buttons.

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

Inbound rules

Filter rules				
Security group rule ID	Port range	Protocol	Source	Security groups
sgr-06686cfa6d7b1a5f4	22	TCP	0.0.0.0/0	launch-wizard-12
sgr-0363cd569b0833531	All	ICMP	0.0.0.0/0	launch-wizard-12
sgr-08e17bfcc6b1db134	All	ICMPV6	0.0.0.0/0	launch-wizard-12
sgr-0bcfba9b932c07675	443	TCP	0.0.0.0/0	launch-wizard-12
sgr-0c3c8b0e7955d214f	All	All	0.0.0.0/0	launch-wizard-12
sgr-0d52c1a72b565f94f	80	TCP	0.0.0.0/0	launch-wizard-12
sgr-0e7f6952648554c1a	0	TCP	0.0.0.0/0	launch-wizard-12

Step 3: Now, run the following commands -

```
sudo su sudo yum update
```

```
sudo yum install httpd php
```

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

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

```
[ec2-user@ip-172-31-16-211 ~]$ sudo yum install httpd php
Last metadata expiration check: 0:04:23 ago on Sun Sep 29 04:05:53 2024.
Dependencies resolved.
```

Package	Architecture	Version
Installing:		
httpd	x86_64	2.4.62-1.amzn2023
php8.3	x86_64	8.3.10-1.amzn2023.0.1
Installing dependencies:		
apr	x86_64	1.7.2-2.amzn2023.0.2
apr-util	x86_64	1.6.3-1.amzn2023.0.1

```
[ec2-user@ip-172-31-16-211 ~]$ sudo yum install gcc glibc glibc-common
Last metadata expiration check: 0:04:54 ago on Sun Sep 29 04:05:53 2024.
Package glibc-2.34-52.amzn2023.0.11.x86_64 is already installed.
Package glibc-common-2.34-52.amzn2023.0.11.x86_64 is already installed.
Dependencies resolved.
```

Package	Architecture	Version
Installing:		
gcc	x86_64	11.4.1-2.amzn2023.0.2
Installing dependencies:		
annobin-docs	noarch	10.93-1.amzn2023.0.1
annobin-plugin-gcc	x86_64	10.93-1.amzn2023.0.1
cpp	x86_64	11.4.1-2.amzn2023.0.2

```
[ec2-user@ip-172-31-16-211 ~]$ sudo yum install gd gd-devel
Last metadata expiration check: 0:05:21 ago on Sun Sep 29 04:05:53 2024.
Dependencies resolved.
```

Package	Architecture	Version
Installing:		
gd	x86_64	2.3.3-5.amzn2023.0.3
gd-devel	x86_64	2.3.3-5.amzn2023.0.3
Installing dependencies:		

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

```
sudo adduser -m nagios
```

```
sudo passwd nagios
```

```
sudo groupadd nagcmd
```

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

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

```
[ec2-user@ip-172-31-16-211 ~]$ sudo adduser -m nagios
[ec2-user@ip-172-31-16-211 ~]$ sudo passwd nagios
Changing password for user nagios.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

```
[ec2-user@ip-172-31-16-211 ~]$ sudo groupadd nagcmd
[ec2-user@ip-172-31-16-211 ~]$ sudo usermod -a -G nagcmd nagios
[ec2-user@ip-172-31-16-211 ~]$ sudo usermod -a -G nagcmd apache
```

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
```

```
[ec2-user@ip-172-31-16-211 ~]$ mkdir ~/downloads
[ec2-user@ip-172-31-16-211 ~]$ cd ~/downloads
[ec2-user@ip-172-31-16-211 downloads]$ 
```

```
[ec2-user@ip-172-31-16-211 downloads]$ wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz
--2024-09-29 04:17:09--  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]
--2024-09-29 04:17:10--  http://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz

```

```
[ec2-user@ip-172-31-16-211 downloads]$ wget http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz
--2024-09-29 04:17:25--  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  1.68MB/s    in 1.5s

2024-09-29 04:17:27 (1.68 MB/s) - 'nagios-plugins-2.0.3.tar.gz' saved [2659772/2659772]
```

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

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

```
[ec2-user@ip-172-31-16-211 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
```

**Step 7: Now, to compile the source code run the following command - make all
sudo make install**

sudo make install-in

sudo make install-con

sudo make install-comm

© 2010 The McGraw-Hill Companies, Inc. All rights reserved.

```
[ec2-user@ip-172-31-16-211 nagios-4.0.8]$ make all
cd ./base && make
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/base'
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nagios.o nagios.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o broker.o broker.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nebmods.o nebmods.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o ..//common/shared.o ..//common/shared.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nerd.o nerd.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o query-handler.o query-handler.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o workers.o workers.c
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(DEBUG_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':
```

```
c2-user@ip-172-31-16-211 nagios-4.0.8]$ cd ./base/..//common/shared
collect2: error: ld returned 1 exit status
make[1]: *** [Makefile:177: archivejson.cgi] Error 1
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-4.0.8/base'
make: *** [Makefile:72: all] Error 2
[ec2-user@ip-172-31-16-211 nagios-4.0.8]$ 
```

```
ec2-user@ip-172-31-16-211 nagios-4.0.8]$ cd ./cgi
collect2: error: ld returned 1 exit status
make[1]: *** [Makefile:177: archivejson.cgi] Error 1
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-4.0.8/cgi'
make: *** [Makefile:72: all] Error 2
[ec2-user@ip-172-31-16-211 nagios-4.0.8]$ 
```

```
[ec2-user@ip-172-31-16-211 nagios-4.0.8]$ sudo make install
cd ./base && make install
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/base'
make install-basic
make[2]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/base'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/bin
/usr/bin/install -c -m 774 -o nagios -g nagios nagios /usr/local/nagios/bin
/usr/bin/install -c -m 774 -o nagios -g nagios nagiostats /usr/local/nagios/bin
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-4.0.8/base'
make strip-post-install
make[2]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/base'
/usr/bin/strip /usr/local/nagios/bin/nagios
/usr/bin/strip /usr/local/nagios/bin/nagiostats
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-4.0.8/base'
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-4.0.8/base'
cd ./cgi && make install
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/cgi'
make install-basic
make[2]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/cgi'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/sbin
for file in *.cgi; do \
    /usr/bin/install -c -m 775 -o nagios -g nagios $file /usr/local/nagios/sbin; \
done
/usr/bin/install: cannot stat '*.cgi': No such file or directory
make[2]: *** [Makefile:205: install-basic] Error 1
```

```
[ec2-user@ip-172-31-16-211 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 ***

[ec2-user@ip-172-31-16-211 nagios-4.0.8]$ █
```

```
[ec2-user@ip-172-31-16-211 nagios-4.0.8]$ sudo make install-config
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc/objects
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/nagios.cfg /usr/local/nagios/etc/nagios.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/cgi.cgi /usr/local/nagios/etc/cgi.cgi
/usr/bin/install -c -b -m 660 -o nagios -g nagios sample-config/resource.cfg /usr/local/nagios/etc/resource.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/templates.cfg /usr/local/nagios/etc/objects/templates.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/commands.cfg /usr/local/nagios/etc/objects/commands.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/contacts.cfg /usr/local/nagios/etc/objects/contacts.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/timeperiods.cfg /usr/local/nagios/etc/objects/timeperiods.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/localhost.cfg /usr/local/nagios/etc/objects/localhost.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/windows.cfg /usr/local/nagios/etc/objects/windows.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/printer.cfg /usr/local/nagios/etc/objects/printer.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/switch.cfg /usr/local/nagios/etc/objects/switch.cfg

*** Config files installed ***

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

[ec2-user@ip-172-31-16-211 nagios-4.0.8]$ █
```

```
[ec2-user@ip-172-31-16-211 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 ***

[ec2-user@ip-172-31-16-211 nagios-4.0.8]$ █
```

Step 8: Edit the config file and change the email address. sudo nano /usr/local/nagios/etc/objects/contacts.cfg

```
GNU nano 5.8                                         /usr/local/nagios/etc/objects/contacts.cfg

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

define contact{
    contact_name          nagiosadmin      ; Short name of user
    use                   generic-contact   ; Inherit default values from generic-contact template (defined
    alias                 Nagios Admin    ; Full name of user

    email                moresanket3004@gmail.com ; <<***** CHANGE THIS TO YOUR EMAIL ADDRESS *****

}

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

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

```
[ec2-user@ip-172-31-16-211 nagios-4.0.8]$ sudo make install-webconf
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/httpd/conf.d/nagios.conf

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

```
[ec2-user@ip-172-31-16-211 nagios-4.0.8]$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
[ec2-user@ip-172-31-16-211 nagios-4.0.8]$ 
```

```
[ec2-user@ip-172-31-16-211 nagios-4.0.8]$ sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[ec2-user@ip-172-31-16-211 nagios-4.0.8]$ 
```

```
[ec2-user@ip-172-31-16-211 nagios-4.0.8]$ cd ~/downloads
[ec2-user@ip-172-31-16-211 downloads]$ tar zxvf nagios-plugins-2.0.3.tar.gz
nagios-plugins-2.0.3/
nagios-plugins-2.0.3/perlmods/
nagios-plugins-2.0.3/perlmods/Config-Tiny-2.14.tar.gz
nagios-plugins-2.0.3/perlmods/parent-0.226.tar.gz
nagios-plugins-2.0.3/perlmods/Test-Simple-0.98.tar.gz
nagios-plugins-2.0.3/perlmods/Makefile.in
nagios-plugins-2.0.3/perlmods/version-0.9903.tar.gz
nagios-plugins-2.0.3/perlmods/Makefile.am
nagios-plugins-2.0.3/perlmods/Module-Runtime-0.013.tar.gz
nagios-plugins-2.0.3/perlmods/Module-Metadata-1.000014.tar.gz
nagios-plugins-2.0.3/perlmods/Params-Validate-1.08.tar.gz
nagios-plugins-2.0.3/perlmods/Class-Accessor-0.34.tar.gz
nagios-plugins-2.0.3/perlmods/Try-Tiny-0.18.tar.gz
```

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
```

```
[ec2-user@ip-172-31-16-211 nagios-plugins-2.0.3]$ ./configure --with-nagios-user=nagios --with-nagios-group=nagios
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking whether to disable maintainer-specific portions of Makefiles... yes
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
```

```
[ec2-user@ip-172-31-16-211 nagios-plugins-2.0.3]$ sudo make install
```

```
make install-exec-hook
make[3]: Entering directory '/home/ec2-user/downloads/nagios-plugins-2.0.3/plugins'
cd /usr/local/nagios/libexec && \
for i in check_ftp check_imap check_ntp check_pop check_udp check_clamd ; do rm -f $i; ln -s check_ldap $i; done
make[3]: Leaving directory '/home/ec2-user/downloads/nagios-plugins-2.0.3/plugins'
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-plugins-2.0.3/plugins'
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-plugins-2.0.3/plugins'
Making install in plugins-scripts
make[1]: Entering directory '/home/ec2-user/downloads/nagios-plugins-2.0.3/plugins-scripts'
make[2]: Entering directory '/home/ec2-user/downloads/nagios-plugins-2.0.3/plugins-scripts'
test -z "/usr/local/nagios/libexec" || /usr/bin/mkdir -p "/usr/local/nagios/libexec"
/usr/bin/install -c -o nagios -g nagios check_breeze check_disk_smb check_flexlm check_ircd
check_ifoperstatus check_mailq check_file_age utils.sh utils.pm '/usr/local/nagios/libexec'
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-plugins-2.0.3/plugins-scripts'
```

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
```

```
[ec2-user@ip-172-31-16-211 nagios-plugins-2.0.3]$ sudo chkconfig --add nagios
[ec2-user@ip-172-31-16-211 nagios-plugins-2.0.3]$ sudo chkconfig nagios on
[ec2-user@ip-172-31-16-211 nagios-plugins-2.0.3]$ █
```

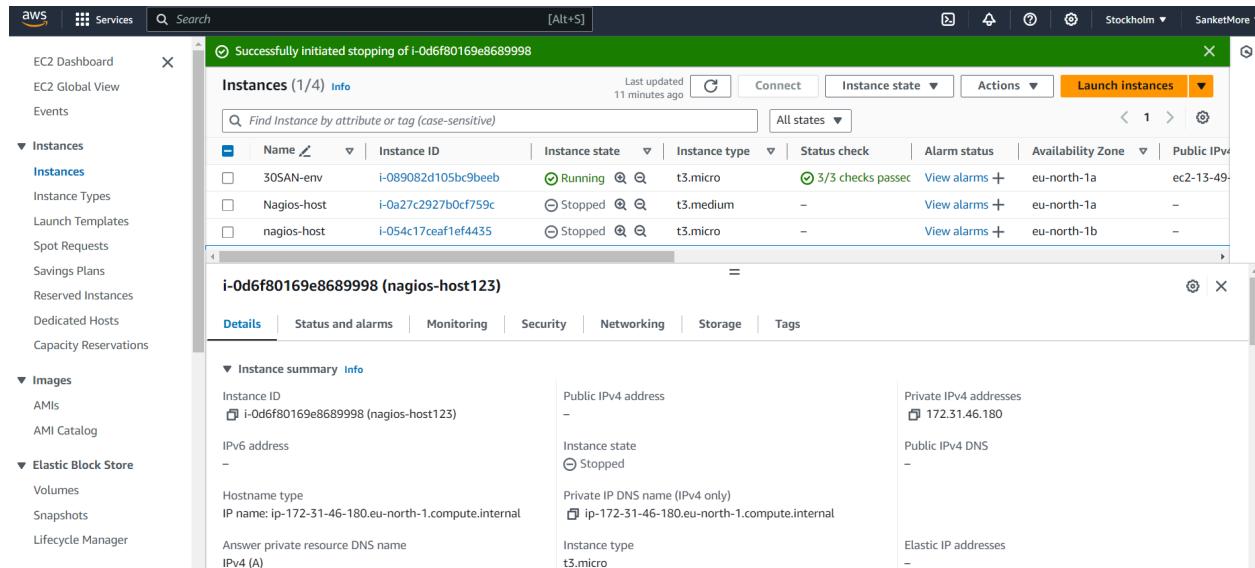
```
[ec2-user@ip-172-31-16-211 nagios-plugins-2.0.3]$ sudo chkconfig --add nagios
[ec2-user@ip-172-31-16-211 nagios-plugins-2.0.3]$ sudo chkconfig nagios on
[ec2-user@ip-172-31-16-211 nagios-plugins-2.0.3]$ sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Nagios Core 4.0.8
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 08-12-2014
License: GPL

Website: http://www.nagios.org
Reading configuration data...
Error in configuration file '/usr/local/nagios/etc/nagios.cfg' - Line 452 (Check result path '/usr/local/nagios/var/spool/checkresults' is not a valid directory
    Error processing main config file!
[ec2-user@ip-172-31-16-211 nagios-plugins-2.0.3]$ █
```

```
[ec2-user@ip-172-31-16-211 nagios-plugins-2.0.3]$ sudo service nagios start
Starting nagios (via systemctl): [ OK ]
```

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



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

The image shows a web browser window with two screenshots of the Nagios Core interface.

The top screenshot shows a "Sign in" dialog box. The URL in the address bar is 51.20.118.97/nagios. The dialog box contains:

- Sign in
- http://51.20.118.97
- Your connection to this site is not private
- Username: nagiosadmin
- Password: [redacted]
- Sign in button
- Cancel button

The bottom screenshot shows the main Nagios Core dashboard for "localhost". The URL in the address bar is localhost/nagios/. The dashboard includes:

- Nagios Core logo
- A message: "✓ Daemon running with PID 13119"
- Nagios Core Version 4.4.3, released on January 15, 2019. A "Check for updates" link is present.
- Links to other Nagios products:
 - Nagios XI: Easy Configuration Advanced Reporting Download
 - Nagios Log Server: Monitor and analyze logs from anywhere Download
 - Nagios Network Analyzer: Real-time netflow and bandwidth analysis Download
- A "Tour" button in the bottom right corner.

Advance DevOps Exp – 10

Sanket More

D15A 30

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

Procedure:-

Check if the nagios service is running by executing following command

```
ubuntu@ip-172-31-89-161:~$ sudo systemctl status nagios
● nagios.service - Nagios Core 4.4.6
   Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: enabled)
   Active: active (running) since Sat 2024-09-28 16:08:58 UTC; 1min 2s ago
     Docs: https://www.nagios.org/documentation
 Process: 15743 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
 Process: 15753 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
Main PID: 15764 (nagios)
   Tasks: 6 (limit: 1130)
  Memory: 2.4M (peak: 3.2M)
    CPU: 29ms
   CGroup: /system.slice/nagios.service
           ├─15764 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
           ├─15765 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─15766 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─15767 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─15768 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           └─15769 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

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

sudo systemctl status nagios

Now, create a new EC2 instance on AWS

Instances (2) Info							
		Last updated less than a minute ago		Actions		Launch instances	
		Find Instance by attribute or tag (case-sensitive)		All states			
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	nagios-host	i-09e8ea019f24f4be2	Running	Q Q	t2.micro	2/2 checks passed	View alarms +
<input type="checkbox"/>	linux-client	i-0ad38836f030e3784	Running	Q Q	t2.micro	Initializing	View alarms +

Now perform the following commands on nagios-host EC2 instance.

On the server, run this command

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

ps -ef | grep nagios

Become a root user and create 2 folders

sudo su

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

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

Copy localhost.cfg file to the mentioned location

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

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

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

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

```
nano
```

```
GNU nano 7.2                                     /usr/local/nagios/et  
#####  
#  
# HOST DEFINITION  
#  
#####  
  
# Define a host for the local machine  
  
define host {  
  
    use          linux-server ; Name of host template  
    ; This host definition is (or inherits) all  
    ; from the 'linux-server' template  
  
    host_name    linuxserver  
    alias        linuxserver  
    address      52.207.253.18  
}  
  
#####  
#  
# HOST GROUP DEFINITION  
  
^G Help      ^O Write Out     ^W Where Is      ^K Cut      ^T Exit  
^X Exit      ^R Read File     ^\ Replace      ^U Paste     ^J Ju  
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/localhost.cfg
```

Note - Here replace hostname with linuxserver

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

Add the following line to the nagios.cfg file

```
# 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/
```

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

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

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

```
License: GPL

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

Running pre-flight check on configuration data...

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

Total Warnings: 0
Total Errors: 0

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

Now restart the service by using this command

```

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

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

```

service nagios restart

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

sudo apt update -y

sudo apt install gcc -y

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

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

```

# supported.

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

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

```

sudo nano /etc/nagios/nrpe.cfg

Now restart nrpe server by using this command
 sudo systemctl restart nagios-nrpe-server

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

The screenshot shows the Nagios interface. On the left, there's a sidebar with links for General, Current Status, Problems, Reports, and System. The main area displays the "Current Network Status" with a summary table and three status bars: Host Status Totals, Service Status Totals, and a larger Host Status Details For All Host Groups table.

Host Status Totals			
Up	Down	Unreachable	Pending
2	0	0	0

Service Status Totals			
Ok	Warning	Unknown	Critical
12	0	0	4

Host Status Details For All Host Groups				
Host	Status	Last Check	Duration	Status Information
linuxserver	UP	09-28-2024 18:45:20	0d 0h 2m 21s	PING OK - Packet loss = 68%, RTA = 0.63 ms
localhost	UP	09-28-2024 18:44:05	0d 4h 47m 45s	PING OK - Packet loss = 0%, RTA = 0.04 ms

Results 1 - 2 of 2 Matching Hosts

check security groups of the EC2 instances.

Advanced DevOps Exp-11

Sanket More

D15A 30

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

Theory:-

AWS Lambda

AWS Lambda is a serverless computing service provided by Amazon Web Services

(AWS). Users of AWS Lambda create functions, self-contained applications written in one

of the supported languages and runtimes, and upload them to AWS Lambda, which executes those functions in an efficient and flexible manner. The Lambda functions can

perform any kind of computing task, from serving web pages and processing streams of data to call APIs and integrate with other AWS services.

The concept of “serverless” computing refers to not needing to maintain your own servers to run these functions. AWS Lambda is a fully managed service that takes care of all the infrastructure for you.

Features of AWS Lambda

- AWS Lambda easily scales the infrastructure without any additional configuration. It

reduces the operational work involved.

- It offers multiple options like AWS S3, CloudWatch, DynamoDB, API Gateway, Kinesis,

CodeCommit, and many more to trigger an event.

- You don't need to invest upfront. You pay only for the memory used by the lambda

function and minimal cost on the number of requests hence cost-efficient.

- AWS Lambda is secure. It uses AWS IAM to define all the roles and security policies.

- It offers fault tolerance for both services running the code and the function. You do not have to worry about the application down.

Packaging Functions

Lambda functions need to be packaged and sent to AWS. This is usually a process of compressing the function and all its dependencies and uploading it to an S3 bucket. And letting AWS know that you want to use this package when a specific event takes place.

To help us with this process we use the Serverless Stack Framework (SST). We'll go over this in detail later on in this guide.

Execution Model

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

This has some interesting implications. Firstly, our functions are effectively stateless. Secondly, each request (or event) is served by a single instance of a Lambda function. This means that you are not going to be handling concurrent requests in your code. AWS brings up a container whenever there is a new request. It does make some optimizations here. It will hang on to the container for a few minutes (5 - 15 mins depending on the load) so it can respond to subsequent requests without a cold start.

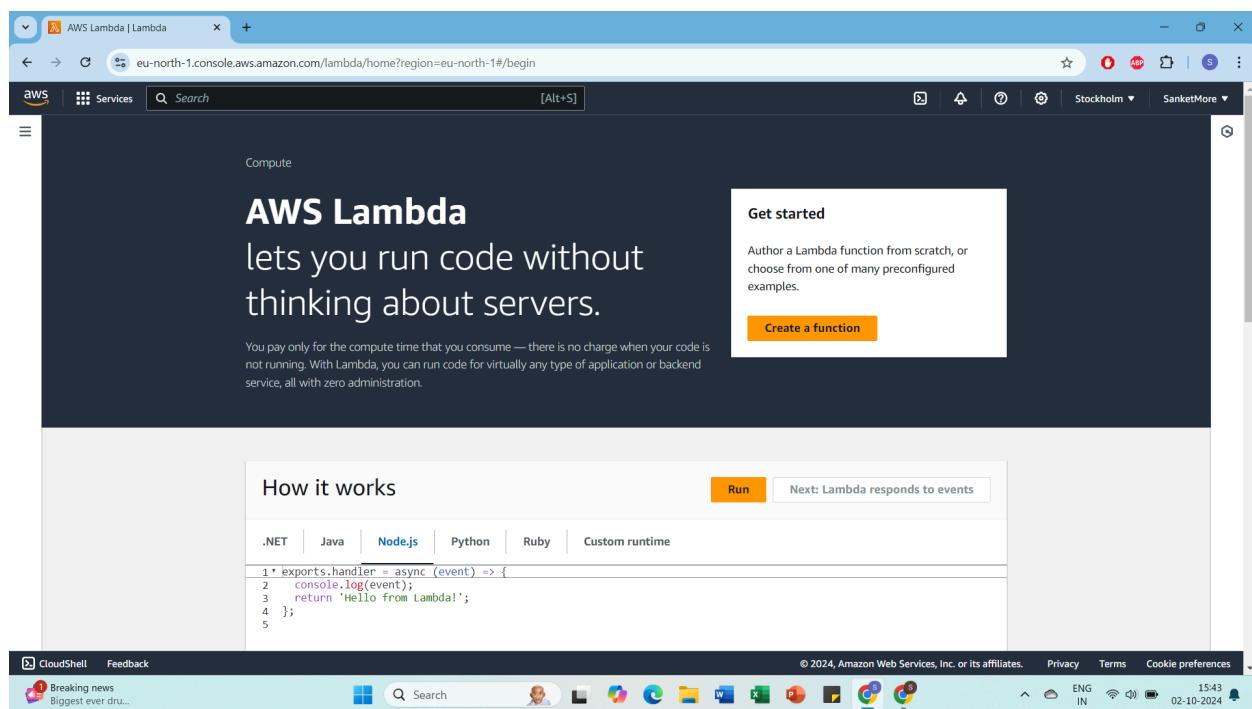
Stateless Functions

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

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

Procedure:-

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



2. Choose to create a function from scratch or use a blueprint, i.e templates defined by AWS for you with all configuration presets required for the most common use cases.

Then, choose a runtime env for your function, under the dropdown, you can see all the options AWS supports, Python, Nodejs, .NET and Java being the most popular ones. After that, choose to create a new role with basic Lambda permissions if you don't have an existing one.

The screenshot shows the AWS Lambda 'Create function' wizard. At the top, there's a navigation bar with the AWS logo, 'Services' (selected), a search bar, and a keyboard shortcut [Alt+S]. Below the navigation bar, the path is shown as 'Lambda > Functions > Create function'. The main title is 'Create function' with an 'Info' link. A sub-instruction says 'Choose one of the following options to create your function.' There are four options:

- Author from scratch**
Start with a simple Hello World example.
- Use a blueprint**
Build a Lambda application from sample code and configuration presets for common use cases.
- Container image**
Select a container image to deploy for your function.
- Browse serverless app repository**
Deploy a sample Lambda application from the AWS Serverless Application Repository.

Below these options is a section titled 'Basic information'.

Function name:
Enter a name that describes the purpose of your function.
Use only letters, numbers, hyphens, or underscores with no spaces.

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

Architecture: [Info](#)
Choose the instruction set architecture you want for your function code.

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

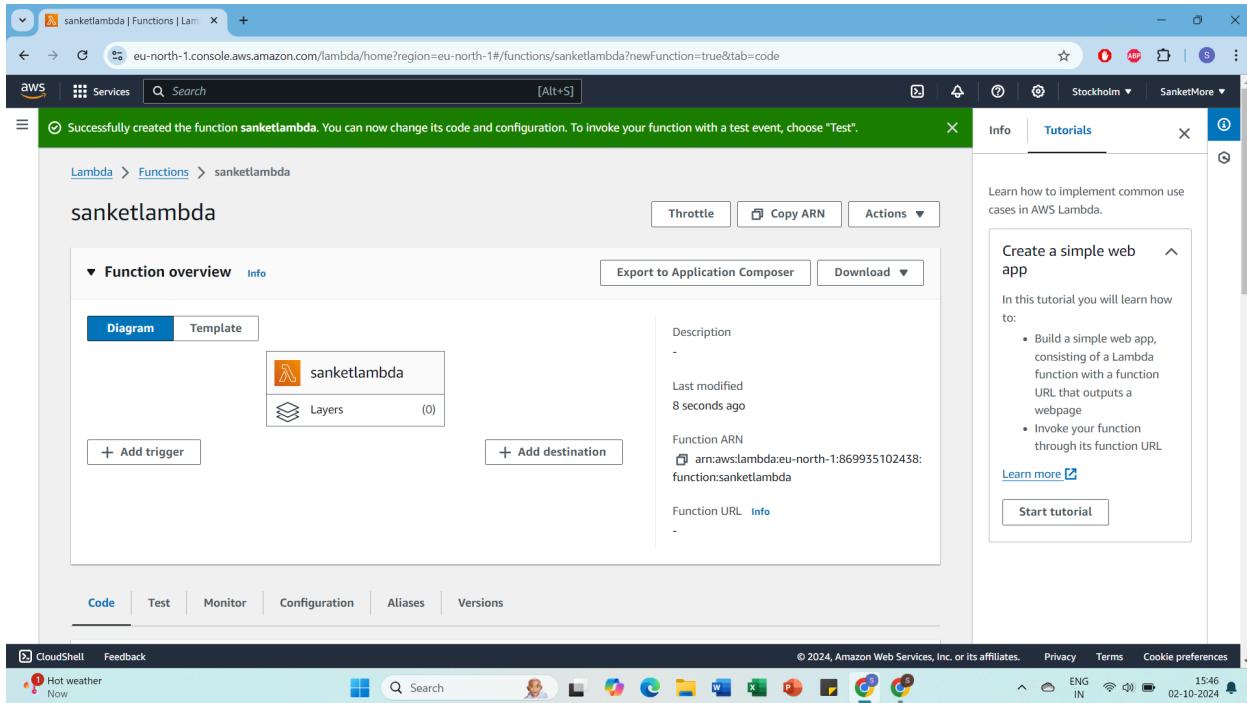
Use an existing role

Create a new role from AWS policy templates

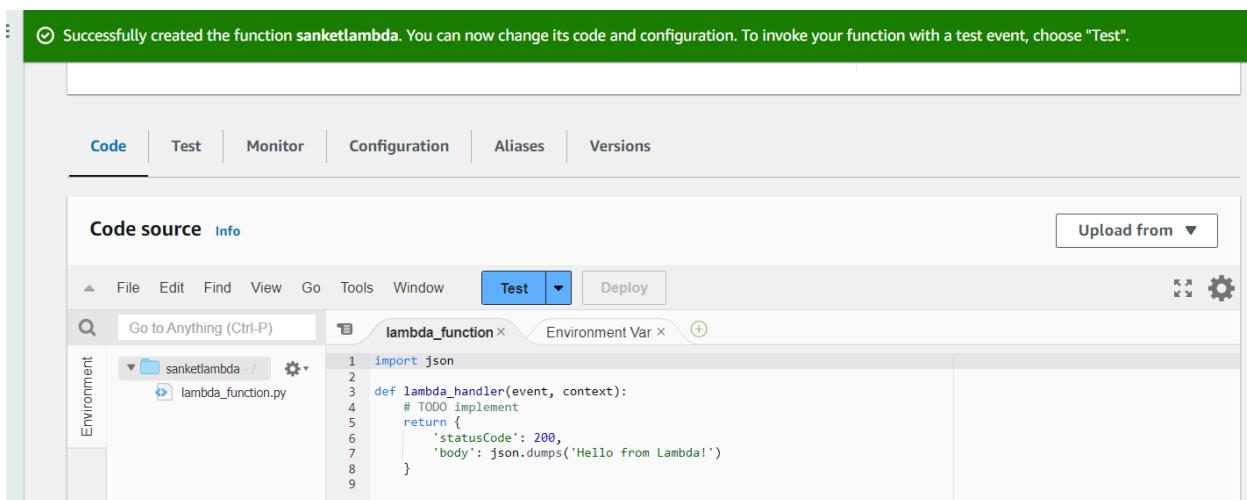
Role creation might take a few minutes. Please do not delete the role or edit the trust or permissions policies in this role.

Lambda will create an execution role named sanketlambda-role-aqbvjl1, with permission to upload logs to Amazon CloudWatch Logs.

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



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



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

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

The screenshot shows the AWS Lambda console. A green success message at the top states: "Successfully created the function sanketlambda. You can now change its code and configuration. To invoke your function with a test event, choose "Test".". Below this, the "Configuration" tab is selected in the navigation bar. On the left, a sidebar menu has "General configuration" selected. The main area displays "General configuration" settings:

General configuration		
Description	Memory	Ephemeral storage
-	128 MB	512 MB
Timeout	SnapStart	
0 min 3 sec	Info	None

An "Edit" button is located in the top right corner of the configuration table.

This screenshot shows the "Edit" view for the "General configuration" of the "sanketlambda" function. It includes fields for "Description", "Memory", "Ephemeral storage", "Timeout" (set to 1 second), and "SnapStart". The "SnapStart" section notes that it reduces startup time by caching snapshots. The "Timeout" section allows setting between 0 and 10240 seconds. The "Execution role" section lets users choose an existing role or create a new one from AWS policy templates. The "Existing role" section lists roles like "LambdaBasicExecutionRole" and "AWSLambdaBasicExecutionRole".

The screenshot shows the AWS Lambda console after updating the function. A green success message at the top states: "Successfully updated the function sanketlambda.". Below this, the "Configuration" tab is selected in the navigation bar. The "General configuration" table shows the updated settings:

General configuration		
Description	Memory	Ephemeral storage
-	128 MB	512 MB
Timeout	SnapStart	
0 min 1 sec	Info	None

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

The screenshot shows the 'Test event' configuration page. At the top, there are 'Save' and 'Test' buttons. Below them, a note says: 'To invoke your function without saving an event, configure the JSON event, then choose Test.' Under 'Test event action', the 'Create new event' option is selected. The 'Event name' field contains 'sanketevent'. In the 'Event sharing settings' section, 'Private' is selected. The 'Template - optional' dropdown shows 'hello-world'. Below this, another 'Template - optional' section also shows 'hello-world'. On the right side, there is an 'Event JSON' editor with the following JSON code:

```
1 [ ]  
2   "key1": "value1",  
3   "key2": "value2",  
4   "key3": "value3"  
5 [ ]
```

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

The screenshot shows the AWS Lambda function configuration page. At the top, a green success message says: 'The test event sanketevent was successfully saved.' Below it, tabs for 'Code', 'Test', 'Monitor', 'Configuration', 'Aliases', and 'Versions' are visible, with 'Test' being the active tab. The 'Code source' section shows the 'lambda_function.py' file with the following code:

```
def lambda_handler(event, context):  
    """  
    This function takes a single string and returns the string  
    surrounded by quotes.  
    """  
    return {  
        "statusCode": 200,  
        "body": ("Hello from Lambda!")  
    }
```

The 'Execution result' section shows the test event details and the successful execution results:

Test Event Name	Status	Max memory used	Time
(unsaved) test event	Succeeded	32 MB	196 ms

Below the execution results, the 'Function Logs' section displays the log output:

```
START RequestId: 9308aa8a-986f-43d9-alce-2c182fa3cf55 Version: $LATEST  
END RequestId: 9308aa8a-986f-43d9-alce-2c182fa3cf55  
REPORT RequestId: 9308aa8a-986f-43d9-alce-2c182fa3cf55 Duration: 1.98 ms Billed Duration: 2 ms Memory Size: 128 MB Max Mem
```

The 'Request ID' is listed as 9308aa8a-986f-43d9-alce-2c182fa3cf55.

Advanced DevOps Exp-12

Sanket More

D15A 30

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

Theory:

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

Workflow:

1. Create an S3 Bucket:

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

2. Create the Lambda Function:

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

3. Set Up Permissions:

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

4. Configure S3 Trigger:

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

5. Test the Setup:

- 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.

Procedure:-

1. Create an S3 bucket of the same location as that of the Lambda function

The screenshot shows the 'Create bucket' wizard in the AWS S3 console. The 'General configuration' step is selected. The 'AWS Region' is set to 'Europe (Stockholm) eu-north-1'. The 'Bucket type' section shows two options: 'General purpose' (selected) and 'Directory'. The 'Bucket name' field contains 'sanketbucket123'. Below it, a note states: 'Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)'.

The screenshot shows the 'sanketbucket123' bucket details page in the AWS S3 console. The top navigation bar includes 'Services' and 'Search' fields, and the location 'Stockholm'. The main content area shows the 'Objects' tab selected. A table header for 'Objects' includes columns for 'Name', 'Type', 'Last modified', 'Size', and 'Storage class'. A message at the bottom of the table states: 'No objects' and 'You don't have any objects in this bucket.' A large 'Upload' button is located at the bottom of the table.

The screenshot shows the 'Create function' wizard in the AWS Lambda console. The top navigation bar includes the AWS logo, 'Services' dropdown, a search bar, and a keyboard shortcut '[Alt+S]'. The main title 'Create function' has an 'Info' link. Below it, a sub-instruction says 'Choose one of the following options to create your function.' Four options are listed in boxes:

- Author from scratch: Start with a simple Hello World example.
- Use a blueprint: Build a Lambda application from sample code and configuration presets for common use cases.
- Container image: Select a container image to deploy for your function.
- Browse serverless app repository: Deploy a sample Lambda application from the AWS Serverless Application Repository.

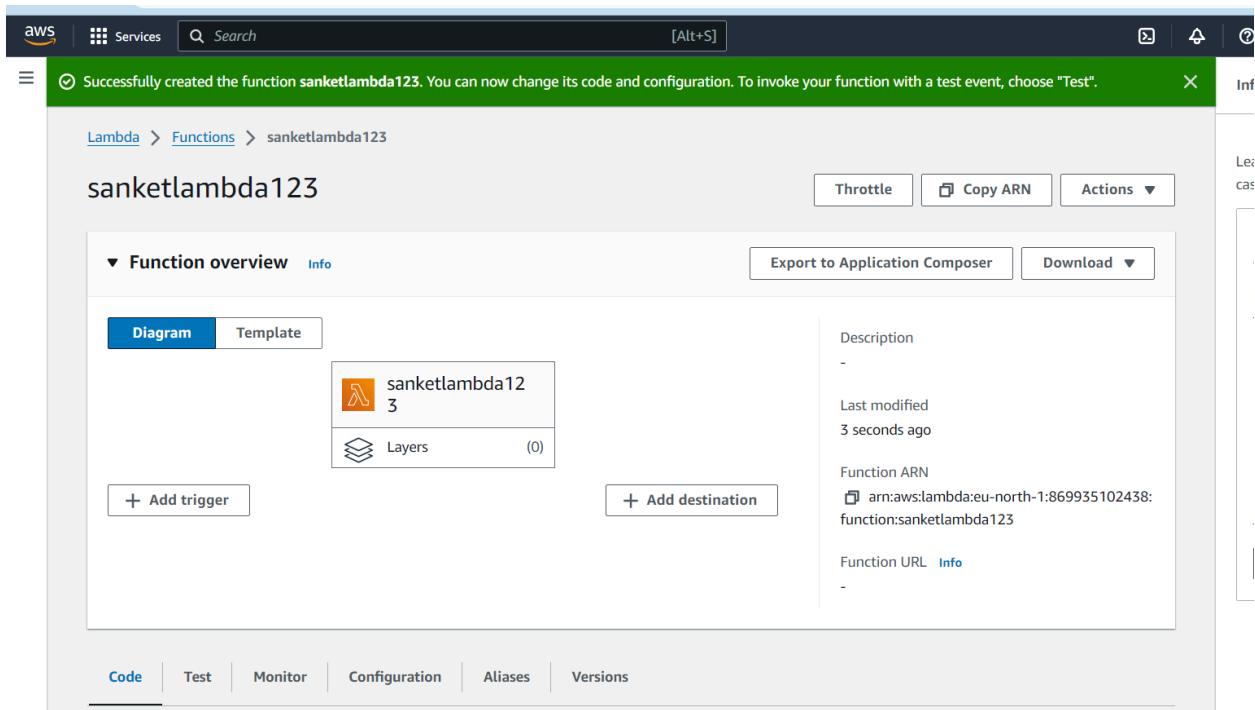
The 'Basic information' step is active. It contains the following fields:

- Function name**: A text input field containing 'sanketlambda123'. A placeholder says 'Enter a name that describes the purpose of your function.' and a note says 'Use only letters, numbers, hyphens, or underscores with no spaces.'
- Runtime**: A dropdown menu set to 'Python 3.12'. A note says 'Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.'
- Architecture**: A dropdown menu set to 'x86_64'. A note says 'Choose the instruction set architecture you want for your function code.'

2. Add roles while creating the Lambda function and give permissions for accessing the S3 bucket

This screenshot shows the 'Change default execution role' step. It includes the following sections:

- Execution role**: A note says 'Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console [link].'
 - Create a new role with basic Lambda permissions
 - Use an existing role
 - Create a new role from AWS policy templates
- Role creation note**: A callout box says 'Role creation might take a few minutes. Please do not delete the role or edit the trust or permissions policies in this role.'
- Role name**: A text input field containing 'sanketrole'. A placeholder says 'Enter a name for your new role.' and a note says 'Use only letters, numbers, hyphens, or underscores with no spaces.'
- Policy templates - optional**: A note says 'Choose one or more policy templates.' A dropdown menu is shown, with a note 'Amazon S3 object read-only permissions X S3' highlighted at the bottom.



3. After creating the Lambda function copy a code available on the internet which allows the Lambda function to access the S3 bucket contents.

```
import json
import urllib.parse
import boto3

print('Loading function')

s3 = boto3.client('s3')

def lambda_handler(event, context):
    #print("Received event: " + json.dumps(event, indent=2))

    # Get the object from the event and show its content type
    bucket = event['Records'][0]['s3']['bucket']['name']
    key = urllib.parse.unquote_plus(event['Records'][0]['s3']['object']['key'],
                                    encoding='utf-8')
    try:
        response = s3.get_object(Bucket=bucket, Key=key)
        print("CONTENT TYPE: " + response['ContentType'])
        return response['ContentType']
    except Exception as e:
        print(e)
        print('Error getting object {} from bucket {}. Make sure they exist and your bucket is in the same region as this function.'.format(key, bucket))
        raise e
```

Successfully updated the function sanketlambda123.

Code Test Monitor Configuration Aliases Versions

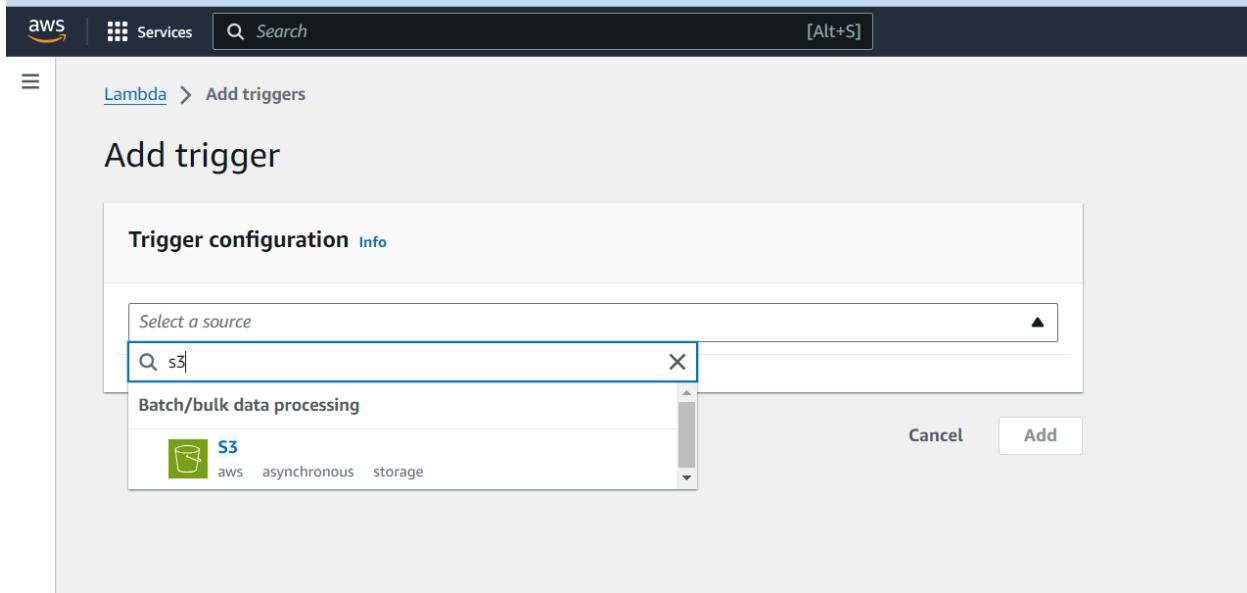
Code source Info Upload from ▾

File Edit Find View Go Tools Window Test Deploy

λ Environment λ lambda_function Environment Var +

```
1 import json
2 import urllib.parse
3 import boto3
4
5 print('Loading function')
6
7 s3 = boto3.client('s3')
8
9
10 def lambda_handler(event, context):
11     #print("Received event: " + json.dumps(event, indent=2))
12
13     # Get the object from the event and show its content type
14     bucket = event['Records'][0]['s3']['bucket']['name']
15     key = urllib.parse.unquote_plus(event['Records'][0]['s3']['object']['key'], encoding='utf-8')
16     try:
17         response = s3.get_object(Bucket=bucket, Key=key)
18         print("CONTENT TYPE: " + response['ContentType'])
19         return response['ContentType']
20     except Exception as e:
21         print(e)
22         print('Error getting object {} from bucket {}. Make sure they exist and your bucket is in the same region as the Lambda function.'.format(key, bucket))
23         raise e
24
```

4. Add a trigger to the Lambda function so any changes in the S3 bucket will be first visible to the user.



aws | Services | Search [Alt+S]

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/sanketbucket123

Bucket region: eu-north-1

Event types
Select the events that you want to have 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/

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.

Lambda > Functions > sanketlambda123

sanketlambda123

Throttle Copy ARN Actions ▾

The trigger sanketbucket123 was successfully added to function sanketlambda123. The function is now receiving events from the trigger. X

Function overview Info Export to Application Composer Download ▾

Diagram Template

sanketlambda123

Layers (0)

S3 + Add destination

+ Add trigger

Description

Last modified 5 minutes ago

Function ARN arn:aws:lambda:eu-north-1:869935102438:function:sanketlambda123

Function URL Info

Code Test Monitor Configuration Aliases Versions

This screenshot shows the AWS Lambda Function Overview page for the function 'sanketlambda123'. At the top, there's a success message: 'The trigger sanketbucket123 was successfully added to function sanketlambda123. The function is now receiving events from the trigger.' Below this, the 'Function overview' section is expanded, showing a diagram where an 'S3' bucket is connected to the function. The function itself has a count of 3. On the right side of the overview, there are sections for 'Description', 'Last modified' (5 minutes ago), 'Function ARN' (arn:aws:lambda:eu-north-1:869935102438:function:sanketlambda123), and 'Function URL'. At the bottom of the overview, there are tabs for Code, Test, Monitor, Configuration (which is selected), Aliases, and Versions.

5. In the event notification of the S3 bucket we can see that it has been connected to the Lambda function .

No data events to display.

Configure in CloudTrail

Event notifications (1)

Send a notification when specific events occur in your bucket. Learn more

Edit Delete Create event notification

Name	Event types	Filters	Destination type	Destination
905f180d-6a25-4474-941b-66671d74e4cd	All object create events	-	Lambda function	sanketlambda123

Amazon EventBridge

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

Edit

Send notifications to Amazon EventBridge for all events in this bucket

Off

This screenshot shows the 'Event notifications' section for an S3 bucket. It displays one notification rule named '905f180d-6a25-4474-941b-66671d74e4cd', which triggers 'All object create events' to a 'Lambda function' destination named 'sanketlambda123'. There are also sections for 'Amazon EventBridge' and a note about sending notifications to EventBridge. The 'Edit' button is visible next to the notification rule.

Managed policy AWSLambdaBasicExecutionRole-8a94e813-c025-4185-8c68-137a8a145ce0.statement.1

Resource-based policy document

```
1 Version: "2012-10-17",
2   "Id": "default",
3   "Statement": [
4     {
5       "Sid": "lambda-f873ffbb0-bb23-44ff-a3a8-08ebd4e381d2",
6       "Effect": "Allow",
7       "Principal": {
8         "Service": "s3.amazonaws.com"
9       },
10      "Action": "lambda:InvokeFunction",
11      "Resource": "arn:aws:lambda:eu-north-1:869935102438:function:sanketlambda123",
12      "Condition": {
13        "StringEquals": {
14          "AWS:SourceAccount": "869935102438"
15        },
16        "ArnLike": {
17          "AWS:SourceArn": "arn:aws:s3:::sanketbucket123"
18        }
19      }
20    }
21  ]
22 ]
23 
```

1:1 JSON Spaces: 2

Close

6. Upload a photo to the S3 bucket

Amazon S3 > Buckets > sanketbucket123 > Upload

Upload Info

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

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

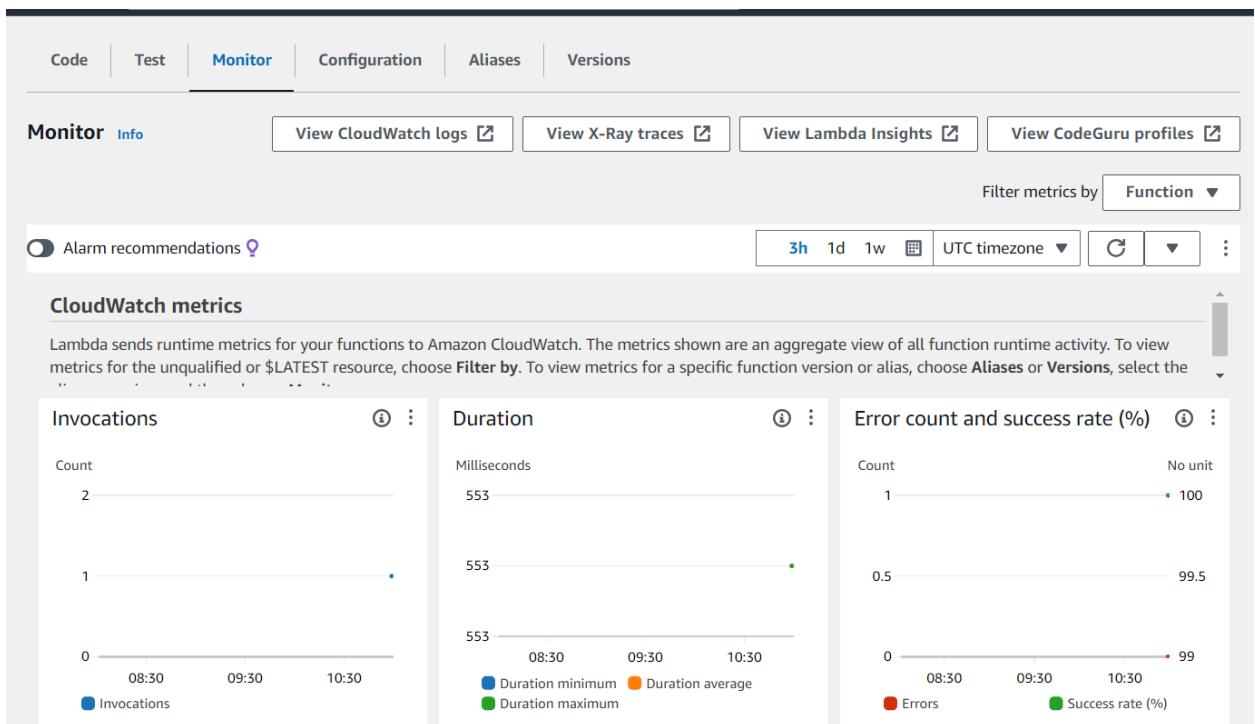
Files and folders (1 Total, 78.6 KB)		Remove	Add files	Add folder
All files and folders in this table will be uploaded.				
<input type="text"/> <small>Find by name</small>		<small>< 1 ></small>		
<input type="checkbox"/>	Name	Folder	Type	
<input type="checkbox"/>	sanket more photo 1.jpeg	-	image/jpeg	

Destination Info

Destination
<s3://sanketbucket123>

The screenshot shows the AWS Lambda console interface. At the top, there's a green header bar with the message "Upload succeeded" and "View details below." Below this, a note says "The information below will no longer be available after you navigate away from this page." The main section is titled "Summary" and shows the destination as "s3://sanketbucket123". It indicates 1 file succeeded (78.6 KB) and 0 files failed (0 B). Below the summary, there are tabs for "Files and folders" (selected) and "Configuration". Under "Files and folders", it shows 1 total item: "sanket more ..." which is an image/jpeg file of size 78.6 KB and status "Succeeded".

7. Now run the function and in the cloud watch logs of AWS you can see the message printed and all the other details of the working of the Lambda function.



AWS Services Search [Alt+S]

CloudWatch

Favorites and recent Dashboards Alarms 0 Log Anomalies Live Tail Logs Insights Contributor Insights Metrics X-Ray traces Events Application Signals New Network monitoring Insights

CloudWatch > Log groups > /aws/lambda/sanketlambda123

/aws/lambda/sanketlambda123 Actions View in Logs Insights Start tailing Search log group

Log group details

Log class: Info Standard	Stored bytes:	KMS key ID:
ARN: arn:aws:logs:eu-north-1:869935102438:log-group:/aws/lambda/sanketlambda123:*	Metric filters: 0	Anomaly detection: Configure
Creation time: 3 minutes ago	Subscription filters: 0	Data protection:
Retention: Never expire	Contributor Insights rules:	Sensitive data count:

Log streams Tags Anomaly detection Metric filters Subscription filters Contributor Insights Data protection

This screenshot shows the AWS CloudWatch Log Groups page. On the left, there's a navigation sidebar with links for various AWS services like CloudWatch Metrics and X-Ray. The main content area shows a log group named '/aws/lambda/sanketlambda123'. It displays basic information such as log class (Info), ARN, creation time, and retention period. There are tabs at the bottom for 'Log streams', 'Tags', 'Anomaly detection', 'Metric filters', 'Subscription filters', 'Contributor Insights', and 'Data protection'.

AWS Services Search [Alt+S]

CloudWatch

Favorites and recent Dashboards Alarms 0 Log Anomalies Live Tail Logs Insights Contributor Insights Metrics X-Ray traces Events Application Signals New Network monitoring Insights Settings

CloudWatch > Log groups > /aws/lambda/sanketlambda123 > 2024/10/02[\$LATEST]8ed57b1dccf54ab8b05688935ed748db

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 Clear 1m 30m 1h 12h Custom UTC timezone Display

Timestamp	Message
2024-10-02T10:59:36.409Z	INIT_START Runtime Version: python:3.12.v36 Runtime Version ARN: arn:aws:lambda:eu-north-1::runtime:188d9ca2e2714ff5637bd2bb..
2024-10-02T10:59:36.801Z	Loading function
2024-10-02T10:59:37.172Z	START RequestId: df929631-f73a-46eb-8a07-56f2f4a810c8 Version: \$LATEST
2024-10-02T10:59:37.718Z	CONTENT TYPE: image/jpeg
2024-10-02T10:59:37.725Z	END RequestId: df929631-f73a-46eb-8a07-56f2f4a810c8
2024-10-02T10:59:37.725Z	REPORT RequestId: df929631-f73a-46eb-8a07-56f2f4a810c8 Duration: 552.91 ms Billed Duration: 553 ms Memory Size: 128 MB Max. M..

No newer events at this moment. Auto retry paused. [Resume](#)

This screenshot shows the AWS CloudWatch Log Events page. It lists log events for the '/aws/lambda/sanketlambda123' log group. The events are timestamped and show the initialization of the Lambda function, loading of the function, the start of a request, the content type of the response, and the end of the request. The interface includes a search bar and a filter bar at the top, and a table for displaying the log events.