

NAME:VAISHNAL MALI
DIV:D15A
ADVANCED DEV-OPS EXPERIMENT-01

AIM: To understand the benefits of Cloud Infrastructure and Setup AWS Cloud9 IDE, Launch AWS Cloud9 IDE and Perform Collaboration Demonstration.

Create Environment on cloud 9:

The screenshot shows the AWS Cloud9 interface. At the top, there's a search bar with 'CLOUD9' typed in. Below it, a sidebar lists recent services like IAM, ElastiCache, EC2, CodeBuild, and CloudWatch Metrics. The main area displays a search results page for 'CLOUD9' under 'Services'. It shows four items: 'Cloud9' (selected), 'Amazon CodeCatalyst', 'AWS Cloud Map', and 'AWS Deadline Cloud'. Below this, under 'Features', there's a single item 'Cloud WAN'. At the bottom, there's a detailed view of an environment named 'my-enviorment' with tabs for 'EC2 instance', 'Network settings', and 'Tags'. The 'EC2 instance' tab is selected, showing details like Name (my-enviorment), Description (-), Environment type (EC2 instance), Owner ARN (arn:aws:sts::262586457411:assumed-role/voclabs/user3402785=MALL_VAISHNAL_DILIP), Number of members (1), Status (Creating), and Lifecycle status (Creating). Buttons for 'Delete' and 'Open in Cloud9' are visible.

AWS Cloud9 > Environments > my-enviorment

my-enviorment

Delete Open in Cloud9

Details

| | | | | | |
|------------------|---------------|-------------------|--|------------------|----------|
| Name | my-enviorment | Owner ARN | arn:aws:sts::262586457411:assumed-role/voclabs/user3402785=MALL_VAISHNAL_DILIP | Status | Creating |
| Description | - | Number of members | 1 | Lifecycle status | Creating |
| Environment type | EC2 instance | | | | |

EC2 instance Network settings Tags

EC2 instance Manage EC2 instance

Searched for 'iam'

Search results for 'iam'

Services (11) See all 11 results ▶

Features (24)

Resources New

Documentation (59,458)

Knowledge Articles (467)

Marketplace (856)

Blogs (1,843)

Events (12)

Tutorials (1)

IAM Manage access to AWS resources

IAM Identity Center Manage workforce user access to multiple AWS accounts and cloud applications

Resource Access Manager Share AWS resources with other accounts or AWS Organizations

Identity and Access Management (IAM) IAM > Users

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Users (0) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Create user

No resources to display

User name: aryan

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), @ # \$ % ^ & * () _ + - (hyphen) - [] [] | '

Show password

Users must create a new password at next sign-in - Recommended

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

Activate Windows

User details

| | | |
|--------------------|--|-------------------------------|
| User name aryan | Console password type Custom password | Require password reset Yes |
|--------------------|--|-------------------------------|

Permissions summary

| Name | Type | Used as |
|-----------------------|-------------|--------------------|
| IAMUserChangePassword | AWS managed | Permissions policy |

Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)
You can add up to 50 more tags.

Add user to an existing group or create a new one. Adding groups is a best practice way to manage user permissions by job function. [Learn more](#)

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](#)

User name: aryanp

Console password type: None

Require password reset: No

Permissions summary

| Name | Type | Used as |
|--------------|------|---------|
| No resources | | |

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

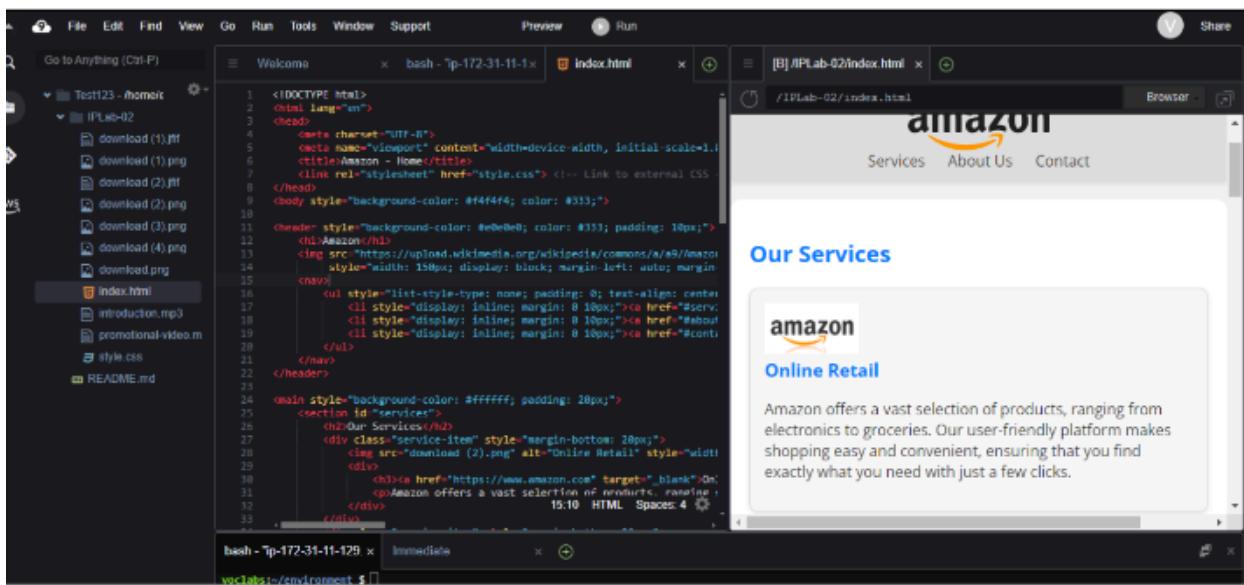
Cancel Previous Create user

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

For capabilities similar to AWS Cloud9, explore AWS Toolkits in your own IDE and AWS CloudShell in the AWS Management Console. Learn more

AWS Cloud9 > Environments

| Environments (1) | | | | | |
|----------------------------------|---------|----------------------|------------------|--------------------|------------|
| | Name | Cloud9 IDE | Environment type | Connection | Permission |
| <input checked="" type="radio"/> | Test123 | Open | EC2 instance | Secure Shell (SSH) | Owner |



EC2 INSTANCE :

EC2 > Instances > Launch an instance

Launch an instance Info

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

Name and tags Info

Name
Vaishnali 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

▼ Summary

Number of instances Info
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2... read more
ami-0ae8f15ae66fe8cda

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

Cancel **Launch instance**

Recents **Quick Start**

Amazon Linux  macOS  Ubuntu  Windows  Red Hat  SUSE Li 

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

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type Free tier eligible ▼

ami-04a81a99f5ec58529 (64-bit (x86)) / ami-0c14ff330901e49ff (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description
Ubuntu Server 24.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Architecture ▼ 64-bit (x86) **AMI ID** ami-04a81a99f5ec58529 **Verified provider**

Activate Windows
Go to Settings to acti

▼ Configure storage [Info](#)

[Advanced](#)

1x

8

GiB

gp3



Root volume (Not encrypted)

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

[Add new volume](#)

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

Click refresh to view backup information



The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

[Edit](#)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

vokey

[Create new key pair](#)

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

 All generations[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

▼ Network settings [Info](#)

Edit

Network [Info](#)

vpc-0eb15f74eb572c84e

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

[Additional charges apply](#) when outside of [free tier allowance](#)

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

We'll create a new security group called '[launch-wizard-3](#)' with the following rules:

Allow SSH traffic from

Helps you connect to your instance

Anywhere



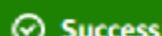
Allow HTTPS traffic from the internet

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

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



Successfully initiated launch of [instance \(i-0d949d3b5f417c6b6\)](#)

▼ Launch log

Initializing requests

Succeeded

Creating security groups

Succeeded

Creating security group
rules

Succeeded

Launch initiation

Succeeded



Ubuntu

Apache2 Default Page

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
```

NAME:VAISHNAL MALI

DIV:D15A

ADVANCED DEV-OPS EXPERIMENT-02

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

Elastic Beanstalk

The screenshot shows the AWS Management Console search results for 'elastic beanstalk'. The search bar at the top contains the query. Below it, the 'Services' section is expanded, showing 12 results. The first result is 'Elastic Beanstalk' with the description 'Run and Manage Web Apps'. To the right of the search results, there's a sidebar with a 'Create application' button and other navigation options. The left sidebar shows recent activity and various AWS service links.

The screenshot shows the Amazon Elastic Beanstalk landing page. The main heading is 'Amazon Elastic Beanstalk' with the subtitle 'End-to-end web application management.'. A 'Get started' button is prominently displayed, along with a description: 'Easily deploy your web application in minutes.' Below this, there's a 'Create application' button. On the right side, there's a 'Pricing' section with a note: 'There's no additional charge for Elastic Beanstalk. You pay for Amazon Web Services resources that we create to store and run your web application, like Amazon S3 buckets and Amazon EC2 instances.' At the bottom, there's a 'Get started' section with a note: 'You simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, and automatic scaling to web application.'

Screenshot of the AWS Elastic Beanstalk configuration interface showing the "Configure environment" step.

The sidebar on the left lists steps:

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

The main content area shows the "Configure environment" step with the following sections:

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: Vaishnal27

Maximum length of 100 characters.

▶ Application tags (optional)

Screenshot of the AWS Elastic Beanstalk configuration interface showing the "Platform" section.

Platform Info

Platform type:

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

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

Platform:

Python

Platform branch:

Python 3.11 running on 64bit Amazon Linux 2023

Platform version:

4.1.3 (Recommended)

Application code [Info](#)

Sample application

Existing version
Application versions that you have uploaded.

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

Presets [Info](#)

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

Configuration presets

Single instance (free tier eligible)

Single instance (using spot instance)

High availability

High availability (using spot and on-demand instances)

Custom configuration

Activate Window
[Cancel](#) [Next](#) [Go to Settings](#)

Search results for 'iam'

Services (11)

- Features (24)
- Resources [New](#)
- Documentation (59,485)
- Knowledge Articles (461)
- Marketplace (860)
- Blogs (1,844)
- Events (12)
- Tutorials (1)

Services [See all 11 results ▶](#)

- IAM** ☆ Manage access to AWS resources
- IAM Identity Center** ☆ Manage workforce user access to multiple AWS accounts and cloud applications
- Resource Access Manager** ☆ Share AWS resources with other accounts or AWS Organizations
- AWS App Mesh** ☆ Easily monitor and control microservices

Features [See all 24 results ▶](#)

AWS Services Search [Alt+S] Global ▾ Vaishnal ▾

IAM > Roles > Create role

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Select trusted entity Info

Trusted entity type

AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account.

AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

EC2 Allows EC2 instances to call AWS services on your behalf.

EC2 Role for AWS Systems Manager Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

EC2 Spot Fleet Role Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

EC2 - Spot Fleet Auto Scaling Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

EC2 - Spot Fleet Tagging Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

EC2 - Spot Instances Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

EC2 - Spot Fleet Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

Activate Windows
Go to Settings to activate Windows

| Filter by Type | | | |
|-------------------------------------|---|-------------|--|
| | <input type="text" value="beanstalk"/> X | All types | 14 matches |
| | Policy name | Type | Description |
| <input type="checkbox"/> |  AdministratorAccess-AWS... | AWS managed | Grants account administrative permissions. Explicitly allows developers and administrators to... |
| <input type="checkbox"/> |  AWSElasticBeanstalkCust... | AWS managed | Provide the instance in your custom platform builder environment permission to launch EC... |
| <input type="checkbox"/> |  AWSElasticBeanstalkEnha... | AWS managed | AWS Elastic Beanstalk Service policy for Health Monitoring system |
| <input type="checkbox"/> |  AWSElasticBeanstalkMan... | AWS managed | This policy is for the AWS Elastic Beanstalk service role used to perform managed updates o... |
| <input checked="" type="checkbox"/> |  AWSElasticBeanstalkMulti... | AWS managed | Provide the instances in your multicontainer Docker environment access to use the Amazon ... |
| <input type="checkbox"/> |  AWSElasticBeanstalkRead... | AWS managed | Grants read-only permissions. Explicitly allows operators to gain direct access to retrieve inf... |
| <input type="checkbox"/> |  AWSElasticBeanstalkRole... | AWS managed | AWSElasticBeanstalkRoleCore (Elastic Beanstalk operations role) Allows core operation of a ... |
| <input type="checkbox"/> |  AWSElasticBeanstalkRole... | AWS managed | (Elastic Beanstalk operations role) Allows an environment to manage Amazon CloudWatch L... |
| <input type="checkbox"/> |  AWSElasticBeanstalkRole... | AWS managed | (Elastic Beanstalk operations role) Allows a multicontainer Docker environment to manage ... |
| <input type="checkbox"/> |  AWSElasticBeanstalkRole... | AWS managed | (Elastic Beanstalk operations role) Allows an environment to integrate an Amazon RDS insta... |
| <input type="checkbox"/> |  AWSElasticBeanstalkRole... | AWS managed | (Elastic Beanstalk operations role) Allows an environment to enable Amazon SNS topic inte... |
| <input type="checkbox"/> |  AWSElasticBeanstalkRole... | AWS managed | (Elastic Beanstalk operations role) Allows a worker environment tier to create an Amazon D... |
| <input checked="" type="checkbox"/> |  AWSElasticBeanstalkWeb... | AWS managed | Provide the instances in your web server environment access to upload log files to Amazon S3. |
| <input checked="" type="checkbox"/> |  AWSElasticBeanstalkWor... | AWS managed | Provide the instances in your worker environment access to upload log files to Amazon S3, t... |

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

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

Description
Add a short explanation for this role.

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

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.



EC2 key pair

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



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](#)

Elastic Beanstalk > [Environments](#) > Vaishnal27-env

Vaishnal27-env [Info](#)



[Actions](#)

[Upload and deploy](#)

Environment overview

Health
⌚ Pending

Environment ID
✉ e-5gujkvgkpa

Domain
-

Application name
Vaishnal27

Platform

[Change version](#)

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

Running version
-

Platform state
☑ Supported

Q cloud formation X

Search results for 'cloud formation'

Services (66)

Features (110)

Resources New

Documentation (116,209)

Knowledge Articles (1,064)

Marketplace (724)

Blogs (10,144)

Events (374)

Tutorials (26)

Services

CloudFormation ☆ Create and Manage Resources with Templates

Application Composer ☆ Visually design and build modern applications quickly

Athena ☆ Serverless interactive analytics service

AWS Supply Chain ☆ Supply chain management application to manage your supply chain systems.

See all 66 results ►

Features

IaC Generator

See all 110 results ►

This screenshot shows the AWS CloudFormation search results. The sidebar on the left lists various categories such as Services, Features, and Resources. The main area displays four recommended services: CloudFormation, Application Composer, Athena, and AWS Supply Chain, each with a brief description and a star icon. Below these, there's a section for 'Features' with one item, 'IaC Generator'.

CloudFormation > Stacks

Stacks (1)

C Delete Update Stack actions ▾ Create stack ▾

Filter status

Filter by stack name Active View nested < 1 >

| Stack name | Status | Created time | Description |
|--------------------------|-----------------|------------------------------|---|
| awseb-e-5gujkvgkpa-stack | CREATE_COMPLETE | 2024-08-21 17:42:52 UTC+0530 | AWS Elastic Beanstalk environment (Name: 'Vaishnal27-env' ID: '5gujkvgkpa') |

This screenshot shows the 'Stacks' page within the CloudFormation service. It displays a single stack named 'awseb-e-5gujkvgkpa-stack' which has completed its creation ('CREATE_COMPLETE'). The stack was created on 2024-08-21 at 17:42:52 UTC+0530. The description indicates it's an AWS Elastic Beanstalk environment.

Instances (1) Info Last updated less than a minute ago C Connect Instance state ▾ Actions ▾ Launch instances ▾

Find Instance by attribute or tag (case-sensitive) All states ▾

Instance state = running X Clear filters < 1 >

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability |
|----------------|---------------------|----------------|---------------|-------------------|---------------|--------------|
| Vaishnal27-env | i-09ae763ea6085e5d4 | Running | t3.micro | 2/2 checks passed | View alarms + | eu-north-1 |

This screenshot shows the 'Instances' page within the EC2 service. It displays a single instance named 'Vaishnal27-env' with the instance ID 'i-09ae763ea6085e5d4'. The instance is currently running ('Running') and is of type 't3.micro'. It has passed 2 out of 2 status checks and has no active alarms. The instance is located in the 'eu-north-1' region.



Not secure

vaishnal27-env.eba-db3ivsyg.eu-north-1.elasticbeanstalk.com



Congratulations

Your first AWS Elastic Beanstalk Python Application is now running on your own dedicated environment in the AWS Cloud

This environment is launched with Elastic Beanstalk Python Platform

What's Next?

- [AWS Elastic Beanstalk overview](#)
- [AWS Elastic Beanstalk concepts](#)
- [Deploy a Django Application to AWS Elastic Beanstalk](#)
- [Deploy a Flask Application to AWS Elastic Beanstalk](#)
- [Customizing and Configuring a Python Container](#)
- [Working with Logs](#)

Activate Windows
Go to Settings to activate Windows.

Code Deployment using Codepipeline

The screenshot shows the AWS search interface with the query 'codepipeline'. The results are categorized into Services, Resources, and Documentation.

- Services (1)**: CodePipeline
- Resources (New)**: Documentation (1,463), Knowledge Articles (4), Marketplace (1), Blogs (103), Tutorials (1).
- Documentation (1,463)**: Introducing resource search, CodePipeline tutorials, User Guide.

A sidebar on the left shows navigation for Elastic Beanstalk and the current environment 'Vaishnal'. A right-hand panel displays deployment options like 'Upload and deploy' and 'Change version'.

The screenshot shows the 'Pipelines' page under 'Developer Tools > CodePipeline > Pipelines'.

A banner at the top informs about the new V2 pipeline type: "Introducing the new V2 pipeline type with improved release safety, pipeline triggers, parameterized pipelines, and a new billing model." with a "Learn more" link.

The main interface includes:

- Header buttons: Pipelines (Info), Refresh, Notify, View history, Release change, Delete pipeline, Create pipeline.
- Search bar.
- Table headers: Name, Latest execution status, Latest source revisions, Latest execution started, Most recent executions.
- Message: "No results" and "There are no results to display."

Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1
Choose pipeline settings Info

Step 2
Add source stage

Step 3
Add build stage

Step 4
Add deploy stage

Step 5
Review

Pipeline settings

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

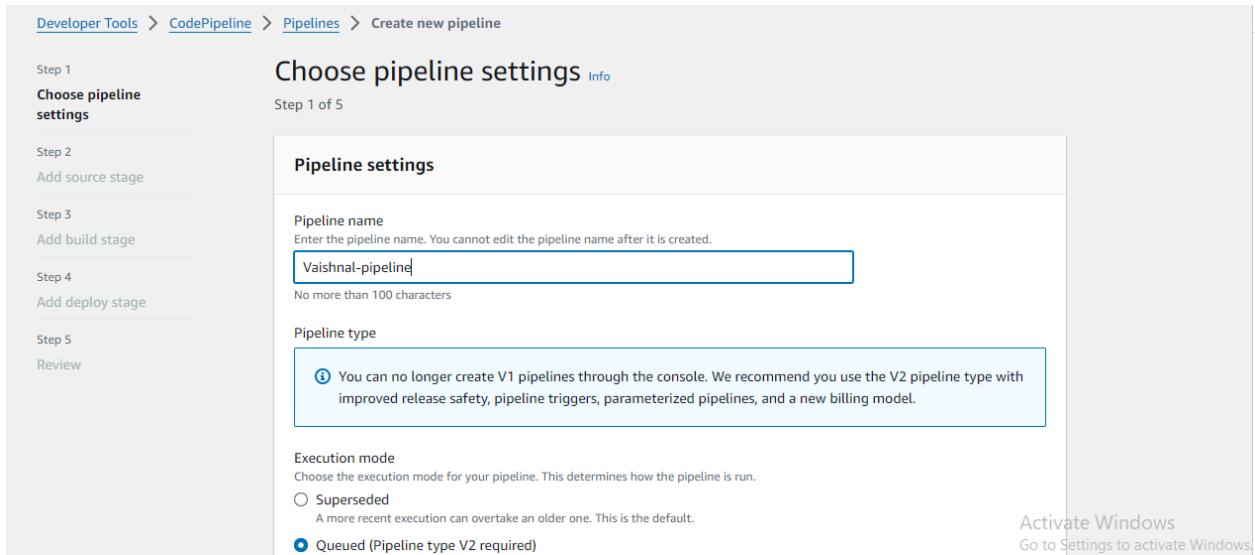
Pipeline type

ⓘ 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.

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

Queued (Pipeline type V2 required)

Activate Windows
Go to Settings to activate Windows.



Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1
Choose pipeline settings Info

Step 2
Add source stage Info

Step 3
Add build stage

Step 4
Add deploy stage

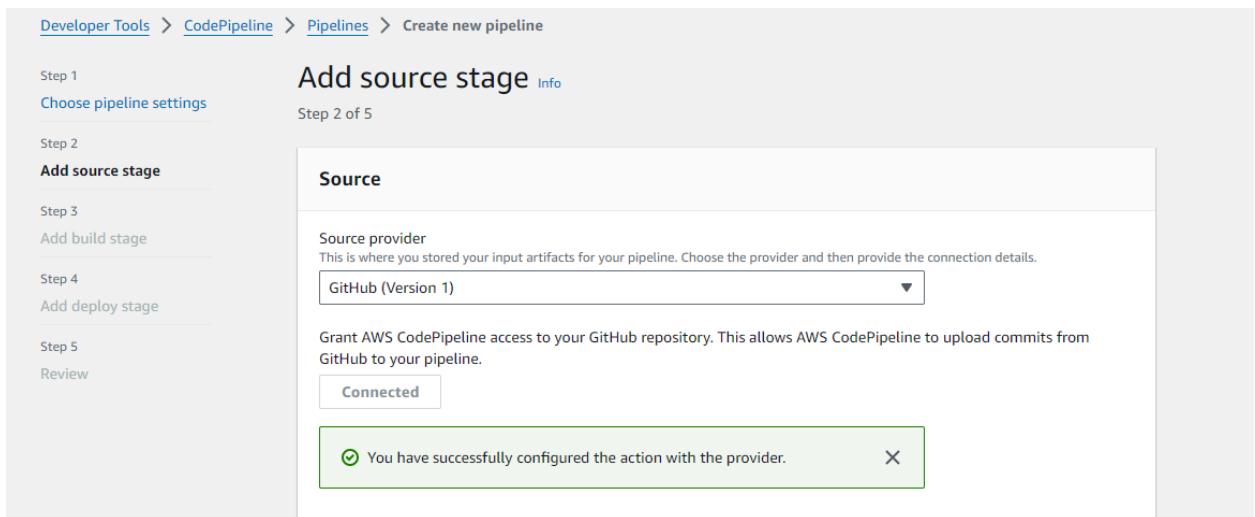
Step 5
Review

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.

ⓘ You have successfully configured the action with the provider. X



Repository

Branch

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

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

AWS CodePipeline
Use AWS CodePipeline to check periodically for changes

Cancel Previous Next

Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1 Choose pipeline settings

Step 2 Add source stage

Step 3 Add build stage

Step 4 Add deploy stage

Step 5 Review

Add build stage Info

Step 3 of 5

Build - optional

Build provider

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

Cancel Previous Skip build stage Next

Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1 Choose pipeline settings

Step 2 Add source stage

Step 3 Add build stage

Step 4 Add deploy stage

Step 5 Review

Add deploy stage Info

Step 4 of 5

i 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)

Cancel Previous Next

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.

 Vaishnal27 X**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.

 Vaishnal27-env X

Vaishnal27-env

[Cancel](#)[Previous](#)[Next](#)[Developer Tools](#) > [CodePipeline](#) > [Pipelines](#) > Create new pipeline**Review** Info

Step 5 of 5

Step 1
[Choose pipeline settings](#)Step 2
[Add source stage](#)

Step 3

[Add build stage](#)

Step 4

[Add deploy stage](#)

Step 5

[Review](#)**Step 1: Choose pipeline settings****Pipeline settings**

Pipeline name

Vaishnal-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-Vaishnal-pipeline

Activate Windows

Go to [Settings](#) to activate Windows

Screenshot of the AWS CodePipeline console showing a successful pipeline creation.

Success
Congratulations! The pipeline Vaishnal-pipeline has been created.

Create a notification rule for this pipeline

Developer Tools > CodePipeline > Pipelines > Vaishnal-pipeline

Vaishnal-pipeline

Pipeline type: V2 Execution mode: QUEUED

Source Succeeded
Pipeline execution ID: 914dbdae-9746-43a0-917c-96f15484b6e0

Source GitHub (Version 1) Succeeded - Just now 2f65ba7d View details

Notify Edit Stop execution Clone pipeline Release change

Not secure vaishnal27-env.eba-db3ivsyg.eu-north-1.elasticbeanstalk.com

Service Samurai

Home About Us Services Portfolio Blog Careers Contact

Welcome to Service Samurai

Innovating the future with cutting-edge technology products.

Explore Our Services

Our Story

Activate Windows
Go to Settings to activate Windows.

Code Deployment Using S3 Bucket :

The screenshot shows the AWS search interface with the query 's3'. The results page displays the 'Services' section, where the 'S3' service card is prominently featured. The card includes the service name, a star icon, and a brief description: 'Scalable Storage in the Cloud'. Below the main card, there are other service cards for 'S3 Glacier', 'AWS Snow Family', and 'Storage Gateway'. To the right of the main search results, there is a sidebar titled 'Create environment' which lists recent environments, including 'Vaishnal27-env'. The top navigation bar shows the AWS logo, the 'Services' menu, and the current region 'Stockholm'.

The screenshot shows the 'Create bucket' wizard in the AWS S3 console. The title bar indicates the user is in the 'Amazon S3 > Buckets > Create bucket' section. The main form is titled 'General configuration'. Under 'AWS Region', it shows 'Europe (Stockholm) eu-north-1'. Under 'Bucket type', the 'General purpose' option is selected, with a note explaining it's recommended for most use cases. The 'Bucket name' field contains 'vaishnal27'. A note below the field states that the name must be unique within the global namespace and follows naming rules, with a link to 'See rules for bucket naming'. At the bottom of the form, there are sections for 'Copy settings from existing bucket - optional' and a note that only specific settings are copied. The footer of the page includes links for 'CloudShell', 'Feedback', and copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates.' and links to 'Privacy', 'Terms', and 'Cookie preferences'. On the right side of the page, there is a sidebar with the text 'Activate Windows' and a link to 'Go to Settings to activate Windows'.

AWS Services Search [Alt+S] Stockholm Vaishnai ⓘ ⓘ

Object Ownership Info

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

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

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

Object Ownership
Bucket owner enforced

Block Public Access settings for this bucket

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

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

Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access

Activate Windows
Go to Settings to activate Windows.

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

AWS Services Search [Alt+S] Stockholm Vaishnai ⓘ ⓘ

Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

Server-side encryption with Amazon S3 managed keys (SSE-S3)

Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

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](#)

Disable
 Enable

Advanced settings

ⓘ After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Activate Windows
Go to Settings to activate Windows.

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

aws Services Search [Alt+S] Stockholm Vaishnal

Successfully created bucket "vaishnal27"
To upload files and folders, or to configure additional bucket settings, choose View details.

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

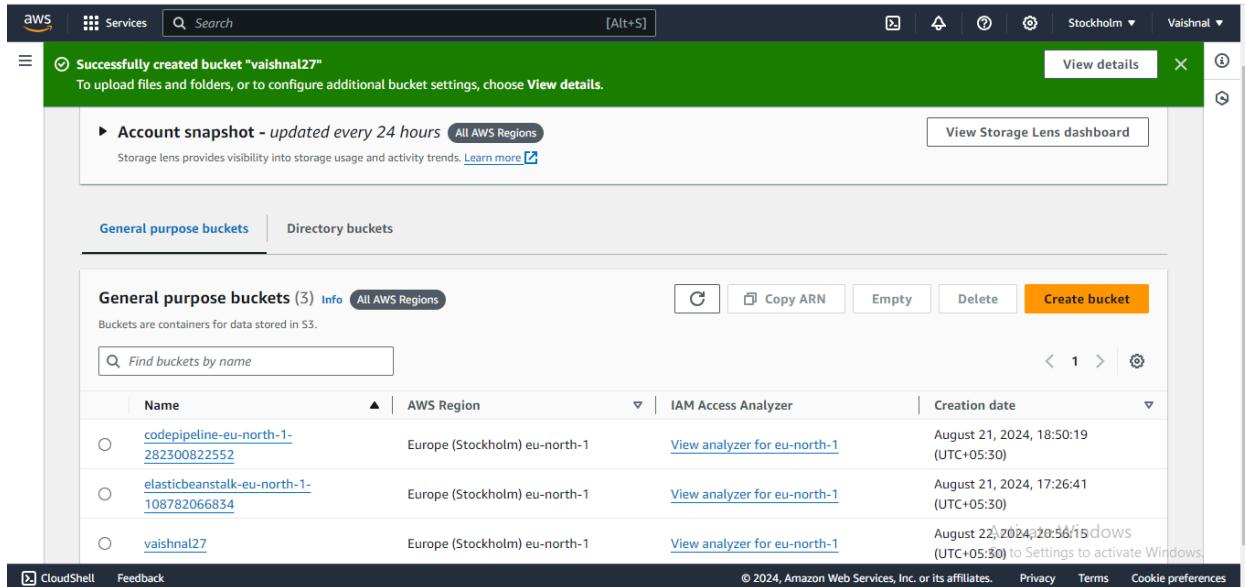
General purpose buckets Directory buckets

General purpose buckets (3) Info All AWS Regions

Buckets are containers for data stored in S3.

| Name | AWS Region | IAM Access Analyzer | Creation date |
|--|-------------------------------|--|--|
| codepipeline-eu-north-1-282300822552 | Europe (Stockholm) eu-north-1 | View analyzer for eu-north-1 | August 21, 2024, 18:50:19 (UTC+05:30) |
| elasticbeanstalk-eu-north-1-108782066834 | Europe (Stockholm) eu-north-1 | View analyzer for eu-north-1 | August 21, 2024, 17:26:41 (UTC+05:30) |
| vaishnal27 | Europe (Stockholm) eu-north-1 | View analyzer for eu-north-1 | August 22, 2024, 12:56:15 (UTC+05:30) Go to Settings to activate Windows |

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



aws Services Search [Alt+S] Stockholm Vaishnal

Amazon S3 > Buckets > vaishnal27 > 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.

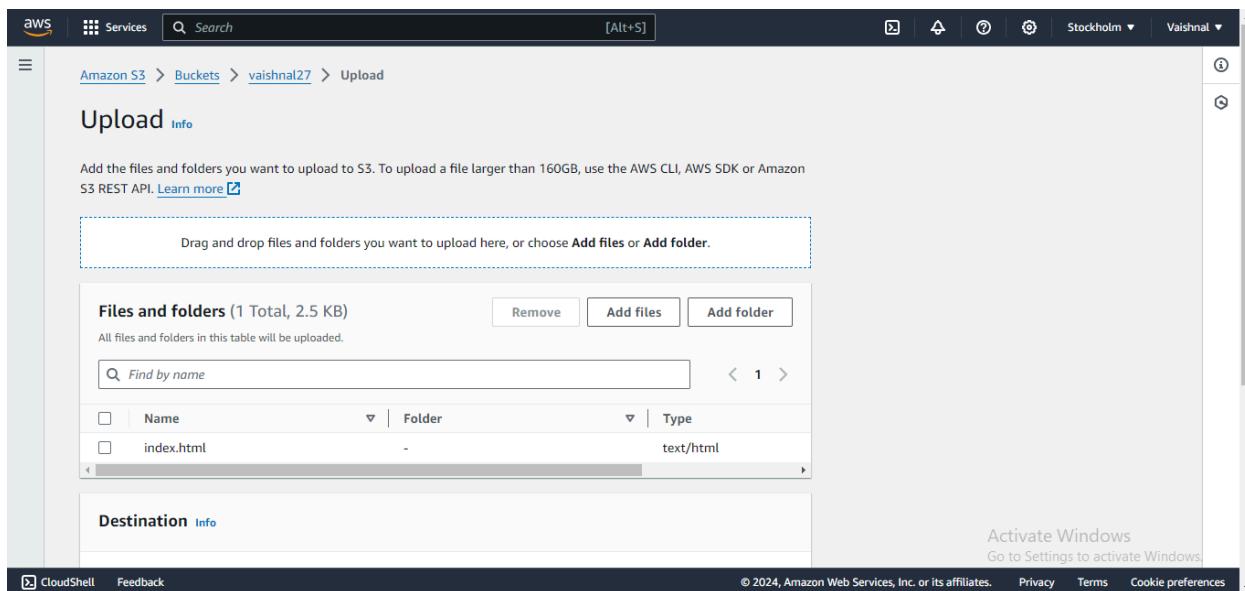
Files and folders (1 Total, 2.5 KB)
All files and folders in this table will be uploaded.

| Name | Folder | Type |
|----------------------------|--------|-----------|
| index.html | - | text/html |

Destination Info

Activate Windows
Go to Settings to activate Windows

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



Upload succeeded

View details below.

Summary

| Destination | Succeeded | Failed |
|-----------------|--------------------------|-------------------|
| s3://vaishnal27 | 1 file, 2.5 KB (100.00%) | 0 files, 0 B (0%) |

Files and folders (1 Total, 2.5 KB)

| Name | Folder | Type | Size | Status | Error |
|------------|--------|-----------|--------|-----------|-------|
| index.html | - | text/html | 2.5 KB | Succeeded | - |

Activate Windows
Go to Settings to activate Windows

Amazon S3

Buckets

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

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

CloudShell Feedback

Amazon S3 > Buckets > vaishnal27 > index.html

index.html Info

[Copy S3 URI](#) [Download](#) [Open](#) [Object actions](#)

Properties [Permissions](#) [Versions](#)

Object overview

| | |
|---|---|
| Owner | S3 URI |
| 2a2d4731449a9a279eef4456196a2cf4eb9ffa8e7796cbbac73abfe103264d2 | s3://vaishnal27/index.html |
| AWS Region | Amazon Resource Name (ARN) |
| Europe (Stockholm) eu-north-1 | arn:aws:s3:::vaishnal27/index.html |
| Last modified | Entity tag (Etag) |
| August 22, 2024, 21:04:51 (UTC+05:30) | c07652731061bfca2575fa2fde413cdb |
| Size | Object URL |
| 2.5 KB | https://vaishnal27.s3.eu-north-1.amazonaws.com/index.html |

Activate Windows
Go to Settings to activate Windows

Static website hosting

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

Static website hosting

Disabled

Edit

Activate Windows

The screenshot shows the 'Edit static website hosting' configuration page for a bucket named 'vaishnal27'. The left sidebar includes links for Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings for this account, and Storage Lens (Dashboards, Storage Lens groups, AWS Organizations settings). The main content area has tabs for 'Static website hosting' (selected), 'Static website hosting' (Info), 'Static website hosting' (Edit), and 'Static website hosting' (Metrics). Under 'Static website hosting', the 'Enable' radio button is selected. Under 'Hosting type', the 'Host a static website' radio button is selected. A note below states: 'For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access.' The bottom navigation bar includes CloudShell, Feedback, Activate Windows (Go to Settings to activate Windows), and links for Privacy, Terms, and Cookie preferences.

Index document

Specify the home or default page of the website.

index.html

Error document - *optional*

This is returned when an error occurs.

error.html

Redirection rules – *optional*

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

The screenshot shows the 'Permissions overview' page for a bucket named 'vaishnal27'. The left sidebar includes links for Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings for this account, and Storage Lens (Dashboards, Storage Lens groups, AWS Organizations settings). The top navigation bar has tabs for Objects, Properties, Permissions (selected), Metrics, Management, and Access Points. The main content area features a 'Permissions overview' section with 'Access finding' (Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#)) and a 'Block public access (bucket settings)' section. In the 'Block public access' section, 'Block all public access' is set to 'On'. There is an 'Edit' button next to the settings. A note below states: 'Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases.' The bottom navigation bar includes CloudShell, Feedback, Activate Windows (Go to Settings to activate Windows), and links for Privacy, Terms, and Cookie preferences.

AWS Services Search [Alt+S] Stockholm Vaishnal

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

Block Public Access settings for this account

Storage Lens Dashboards Storage Lens groups AWS Organizations settings

CloudShell Feedback

Amazon S3 > Buckets > vaishnal27 > Edit Block public access (bucket settings)

Edit Block public access (bucket settings) Info

Block public access (bucket settings)

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

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

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

Activate Windows Go to Settings to activate Windows.

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

can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit Block public access (bucket settings) X

⚠️ Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter *confirm* in the field.

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Cancel **Confirm**

Object Ownership Info

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

Object Ownership
Bucket owner enforced
ACLs are disabled. All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

Edit

Edit Object Ownership

Object Ownership

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

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

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

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

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

I acknowledge that ACLs will be restored.

Object Ownership

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

Object writer
The object writer remains the object owner.

Activate Windows
Go to Settings to activate Windows.

vaishnal27

Objects

Actions

Upload

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

Find objects by prefix

Show versions

| Name | Type | Last modified | Size |
|------------|------|---------------------------------------|------|
| index.html | html | August 22, 2024, 21:04:51 (UTC+05:30) | |

Actions

- Initiate restore
- Query with S3 Select
- Edit actions**
- Rename object
- Edit storage class
- Edit server-side encryption
- Edit metadata
- Edit tags

Activate Windows
Go to Settings to activate Windows.

Make public Info

The make public action enables public read access in the object access control list (ACL) settings. [Learn more](#).

⚠ When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.

Specified objects

Find objects by name

| Name | Type | Last modified | Size |
|--|------|---------------------------------------|--------|
|  index.html | html | August 22, 2024, 21:04:51 (UTC+05:30) | 2.5 KB |

Cancel

Make public

⌚ Successfully edited public access
View details below.

Make public: status

[Close](#)

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

Summary

Source
s3://vaishnal27

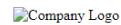
Successfully edited public access
⌚ 1 object, 2.5 KB

Failed to edit public access
⌚ 0 objects

← → ⌂ vaishnal27.s3.eu-north-1.amazonaws.com/index.html



Welcome to Service Samurai



Company Details

| | |
|---------------------|--|
| Name | Service Samurai |
| Address | 123 Business Ave, Suite 100, City, Country |
| Contact Information | (123) 456-7890 contact@servicesamurai.com |
| Description | Service Samurai provides top-notch services in technology solutions, including consulting, development, and support. |

Our Services

- Consulting Services 
- Software Development 
- Technical Support 
- IT Infrastructure Management 

Introduction Audio

▶ 0:00 / 0:00 ⏸ :

Promotional Video

Activate Windows
Go to Settings to activate Windows.

NAME:VAISHNAL MALI

DIV:D15A

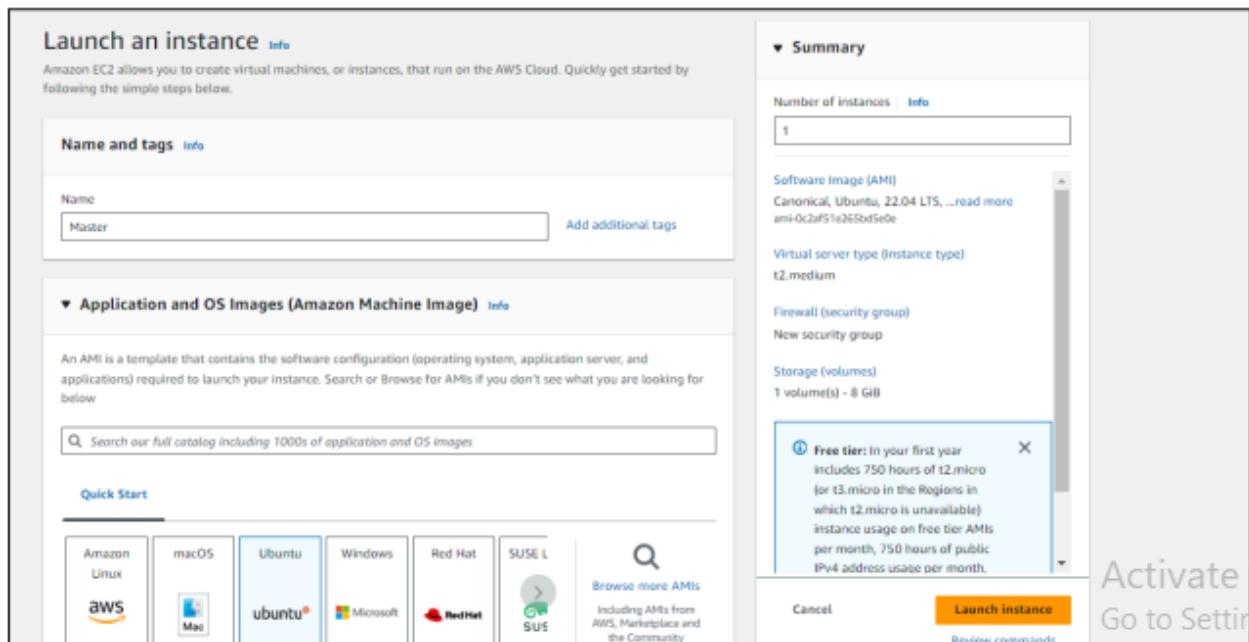
ROLL NO. :27

ADVANCED DEV-OPS EXPERIMENT-03

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

Step 1:Prerequisites

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



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

The screenshot shows the AWS Lambda 'Create Function' configuration interface. It includes sections for 'Instance type', 'Key pair (login)', and 'Network settings'.

Instance type: t2.medium
Family: t2 2 vCPU 4 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0496 USD per Hour
On-Demand Windows base pricing: 0.0676 USD per Hour
On-Demand RHEL base pricing: 0.0784 USD per Hour
On-Demand SUSE base pricing: 0.1496 USD per Hour

Key pair (login): Key pair name - required: two-tier-app-k8s | Create new key pair

Network settings: Network: vpc-04007898e59a6979f | Edit | Activate | Go to Settings

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

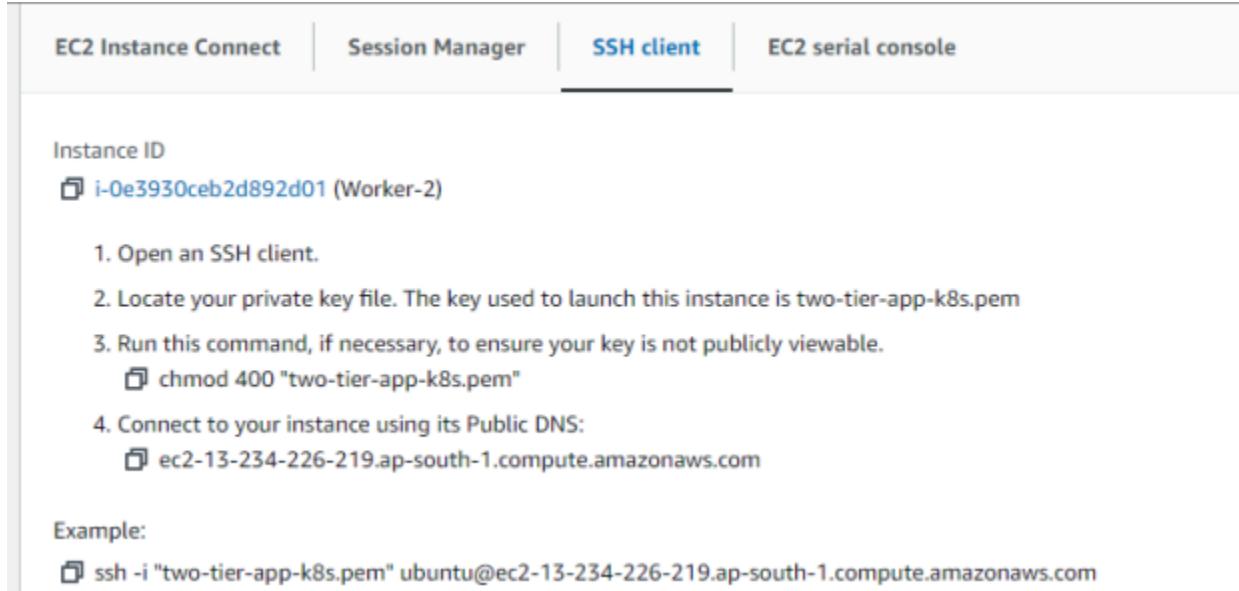
- .pem
For use with OpenSSH
- .ppk
For use with PuTTY

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

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

| Instances (1/3) Info | | | | | | | | | |
|--|---------------------|--|---------------|--|--------------|--------------------------|-----------------|-----------|--|
| Last updated C Connect Instance state 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 | Public IPv4 DNS | Public IP | |
| Worker-2 | i-0e3930ccb2d892d01 | Running View details Edit | t2.medium | 2/2 checks passed View alarms + | ap-south-1a | ec2-13-234-226-219.ap... | 13.234.22 | | |
| Worker-1 | i-0d16e01d1824e0e3a | Running View details Edit | t2.medium | 2/2 checks passed View alarms + | ap-south-1a | ec2-65-0-104-95.ap-so... | 65.0.104. | | |
| <input checked="" type="checkbox"/> Master | i-0tae3d388db90ad73 | Running View details Edit | t2.medium | 2/2 checks passed View alarms + | ap-south-1a | ec2-13-232-36-34.ap-s... | 13.232.36 | | |

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



Instance ID
i-0e3930ceb2d892d01 (Worker-2)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is two-tier-app-k8s.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 "two-tier-app-k8s.pem"
4. Connect to your instance using its Public DNS:
ec2-13-234-226-219.ap-south-1.compute.amazonaws.com

Example:

```
ssh -i "two-tier-app-k8s.pem" ubuntu@ec2-13-234-226-219.ap-south-1.compute.amazonaws.com
```

```
acer@TMP214-53 MINGW64 ~/Downloads
$ ssh -i "two-tier-app-k8s.pem" ubuntu@ec2-13-232-36-34.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-13-232-36-34.ap-south-1.compute.amazonaws.com (13.232.36.34)' can't be established.
ED25519 key fingerprint is SHA256:uVGEO+FWYefj60j0ft70Sralv8NrzEi/IwxAtBY+EPE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-232-36-34.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1022-aws x86_64)

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

System information as of Wed Sep 11 14:07:10 UTC 2024

System Load: 0.0          Processes:      106
Usage of /: 20.7% of 7.57GB  Users logged in:  0
Memory usage: 5%           IPv4 address for eth0: 172.31.45.227
Swap usage:  0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

Activ

Step 2:Prepare Nodes

2.1. Update the package manager on all nodes: sudo apt-get update && sudo apt-get upgrade -y

```
ubuntu@ip-172-31-22-29:~$ sudo apt-get update && sudo apt-get upgrade -y
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.

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

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

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

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

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

ubuntu@ip-172-31-22-29:~$ sudo apt-get update && sudo apt-get upgrade -y
```

```
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:5 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8372 B]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2023 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [352 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [17.8 kB]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [2437 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [419 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted a
```

2.2. Disable Swap (Kubernetes requires swap to be off):

```
ubuntu@ip-172-31-22-29:~$ sudo swapoff -a
sudo sed -i '/ swap / s/^/#/' /etc/fstab
```

2.3. Load necessary kernel modules for networking and iptables:

```
ubuntu@ip-172-31-22-29:~$ cat <<EOF | sudo tee /etc/modules-load.d/k8s.conf
overlay
br_netfilter
EOF
sudo modprobe overlay
sudo modprobe br_netfilter
overlay
br_netfilter
```

2.4. Configure sysctl settings for Kubernetes networking:

```
ubuntu@ip-172-31-22-29:~$ cat <<EOF | sudo tee /etc/modules-load.d/k8s.conf
overlay
br_netfilter
EOF
sudo modprobe overlay
sudo modprobe br_netfilter
overlay
br_netfilter
ubuntu@ip-172-31-22-29:~$ cat <<EOF | sudo tee /etc/sysctl.d/k8s.conf
net.bridge.bridge-nf-call-ip6tables = 1
net.bridge.bridge-nf-call-iptables = 1
EOF
sudo sysctl --system
net.bridge.bridge-nf-call-ip6tables = 1
net.bridge.bridge-nf-call-iptables = 1
# Applying /etc/sysctl.d/10-console-messages.conf ...
kernel.printk = 4 4 1 7
# Applying /etc/sysctl.d/10-ipv6-privacy.conf ...
net.ipv6.conf.all.use_tempaddr = 2
net.ipv6.conf.default.use_tempaddr = 2
# Applying /etc/sysctl.d/10-kernel-hardening.conf ...
kernel.kptr_restrict = 1
```

Step 3: Install Docker-Kubernetes uses container runtimes like Docker.

Install Docker on all nodes.

Run following commands

```
sudo apt-get update
sudo apt-get install -y apt-transport-https ca-certificates curl
software-properties-common
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
sudo add-apt-repository "deb [arch=amd64]
https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable"
sudo apt-get update
sudo apt-get install -y docker-ce docker-ce-cli containerd.io
```

```
ubuntu@ip-172-31-22-29:~$ sudo apt-get update
sudo apt-get install -y apt-transport-https ca-certificates curl software-properties-common
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable"
sudo apt-get update
sudo apt-get install -y docker-ce docker-ce-cli containerd.io
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Fetched 129 kB in 1s (241 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).
ca-certificates set to manually installed.
curl is already the newest version (7.81.0-1ubuntu1.17).
curl set to manually installed.
software-properties-common is already the newest version (0.99.22.9).
software-properties-common set to manually installed.
```

Configure Docker for Kubernetes:

```
ubuntu@ip-172-31-22-29:~$ cat <<EOF | sudo tee /etc/docker/daemon.json
{
  "exec-opts": ["native.cgroupdriver=systemd"],
  "log-driver": "json-file",
  "log-opt": {
    "max-size": "100m"
  },
  "storage-driver": "overlay2"
}
EOF
sudo systemctl restart docker
{
  "exec-opts": ["native.cgroupdriver=systemd"],
  "log-driver": "json-file",
  "log-opt": {
    "max-size": "100m"
  },
  "storage-driver": "overlay2"
}
```

Step 4: Install kubeadm, kubelet, kubectl

Install Kubernetes tools on all nodes.

4.1. Add Kubernetes APT repository:

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

4.2. Install kubeadm, kubelet, and kubectl:

```
ubuntu@ip-172-31-22-29:~$ sudo apt-get update
sudo apt-get install -y kubelet kubeadm kubectl
sudo apt-mark hold kubelet kubeadm kubectl
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease
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
```

Step 5: Initialize the Kubernetes Cluster on Master Node

On the master node: sudo kubeadm init --pod-network-cidr=10.244.0.0/16

```
ubuntu@ip-172-31-22-29:~$ sudo kubeadm init --pod-network-cidr=10.244.0.0/16 --v=5
Found multiple CRI endpoints on the host. Please define which one do you wish to
use by setting the 'criSocket' field in the kubeadm configuration file: unix://
/var/run/containerd/containerd.sock, unix:///var/run/crio/crio.sock
k8s.io/kubernetes/cmd/kubeadm/app/util/runtime.detectCRISocketImpl
    cmd/kubeadm/app/util/runtime/runtime.go:167
k8s.io/kubernetes/cmd/kubeadm/app/util/runtime.DetectCRISocket
    cmd/kubeadm/app/util/runtime/runtime.go:175
k8s.io/kubernetes/cmd/kubeadm/app/util/config.SetNodeRegistrationDynamicDefaults
    cmd/kubeadm/app/util/config/initconfiguration.go:118
k8s.io/kubernetes/cmd/kubeadm/app/util/config.SetInitDynamicDefaults
    cmd/kubeadm/app/util/config/initconfiguration.go:64
k8s.io/kubernetes/cmd/kubeadm/app/util/config.DefaultedInitConfiguration
    cmd/kubeadm/app/util/config/initconfiguration.go:248
k8s.io/kubernetes/cmd/kubeadm/app/util/config.LoadOrDefaultInitConfiguration
    cmd/kubeadm/app/util/config/initconfiguration.go:282
k8s.io/kubernetes/cmd/kubeadm/app/cmd.newInitData
    cmd/kubeadm/app/cmd/init.go:319
k8s.io/kubernetes/cmd/kubeadm/app/cmd.newCmdInit.func3
    cmd/kubeadm/app/cmd/init.go:170
k8s.io/kubernetes/cmd/kubeadm/app/cmd/phases/workflow.(*Runner).InitData
    cmd/kubeadm/app/cmd/phases/workflow/runner.go:183
k8s.io/kubernetes/cmd/kubeadm/app/cmd.newCmdInit.func1
```

5.1. Set up kubectl on the master node:

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

```
ubuntu@ip-172-31-22-29:~$ sudo kubeadm config images pull  
sudo kubeadm init  
mkdir -p "$HOME"/.kube  
sudo cp -i /etc/kubernetes/admin.conf "$HOME"/.kube/config  
sudo chown "$(id -u):$(id -g)" "$HOME"/.kube/config  
  
# Network Plugin = calico  
kubectl apply -f https://raw.githubusercontent.com/projectcalico/calico/v3.26.0/manifests/calico.yaml  
  
kubeadm token create --print-join-command --v=5  
Found multiple CRI endpoints on the host. Please define which one do you wish to use by setting the 'criSocket' field in the kubeadm configuration file: unix:///var/run/containerd/c  
uck, unix:///var/run/crio/crio.sock  
To see the stack trace of this error execute with --v=5 or higher  
Found multiple CRI endpoints on the host. Please define which one do you wish to use by setting the 'criSocket' field in the kubeadm configuration file: unix:///var/run/containerd/c  
uck, unix:///var/run/crio/crio.sock
```

Step 6: Install a Pod Network

Add-on To enable communication between pods, install a pod network plugin like Flannel or Calico.

Install Flannel: kubectl apply -f

```
ubuntu@ip-172-31-22-29:~$ kubectl apply -f https://raw.githubusercontent.com/coreos/flannel/master/documentation/kube-flannel.yml --validate=false  
E0913 15:35:04.261458 19259 memcache.go:265] couldn't get current server API group list: Get "http://localhost:8080/api?timeout=32s": dial tcp 127.0.0.1:808  
E0913 15:35:04.261902 19259 memcache.go:265] couldn't get current server API group list: Get "http://localhost:8080/api?timeout=32s": dial tcp 127.0.0.1:808  
E0913 15:35:04.263424 19259 memcache.go:265] couldn't get current server API group list: Get "http://localhost:8080/api?timeout=32s": dial tcp 127.0.0.1:808  
E0913 15:35:04.263799 19259 memcache.go:265] couldn't get current server API group list: Get "http://localhost:8080/api?timeout=32s": dial tcp 127.0.0.1:808  
E0913 15:35:04.265840 19259 memcache.go:265] couldn't get current server API group list: Get "http://localhost:8080/api?timeout=32s": dial tcp 127.0.0.1:808  
E0913 15:35:04.266524 19259 memcache.go:265] couldn't get current server API group list: Get "http://localhost:8080/api?timeout=32s": dial tcp 127.0.0.1:808  
unable to recognize "https://raw.githubusercontent.com/coreos/flannel/master/Documentation/kube-flannel.yml": Get "http://localhost:8080/api?timeout=32s": dia
```

Step 7: Join Worker Nodes to the Cluster On the worker nodes run :

```
sudo kubeadm join :6443 --token --discovery-token-ca-cert-hash sha256:
```

```
clusterrolebinding.rbac.authorization.k8s.io/calico-cni-plugin created  
daemonset.apps/calico-node created  
deployment.apps/calico-kube-controllers created  
kubeadm join 172.31.62.216:6443 --token br7fe5.hq28adbmnlmu17ky --discovery-token-ca-cert-hash sha256:2bc469a8d14fbeb0f879328d2b416fad  
32b29a8505d3f448b98703fff3b014d9
```

Step 8: Verify the Cluster

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

```
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:~$ |
```

NAME:VAISHNAL MALI

DIV:D15A

ROLL NO. :27

ADVANCED DEV-OPS EXPERIMENT-04

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

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
[...]
ubuntu@ip-172-31-22-29:~$ sudo apt-get install -y apt-transport-https ca-certificates curl
[...]
ubuntu@ip-172-31-22-29:~$ curl https://72.21.14.14:443/ | gpg --keyring /usr/share/keyrings/kubernetes-archive-keyring.gpg --verify kubernetes-archive-keyring.gpg
[...]
ubuntu@ip-172-31-22-29:~$ curl https://72.21.14.14:443/ | gpg --keyring /usr/share/keyrings/kubernetes-archive-keyring.gpg --verify kubernetes-archive-keyring.gpg
[...]
```

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:~$ curl https://72.21.14.14:443/ | gpg --keyring /usr/share/keyrings/kubernetes-archive-keyring.gpg --verify kubernetes-archive-keyring.gpg
[...]
```

3. Add the Kubernetes repository:

```
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
[...]
ubuntu@ip-172-31-22-29:~$ curl https://72.21.14.14:443/ | gpg --keyring /usr/share/keyrings/kubernetes-archive-keyring.gpg --verify kubernetes-archive-keyring.gpg
[...]
```

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.
```

Step 2: Deploying Your Application on Kubernetes

2.1 Set up Kubernetes Cluster

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:

```
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:

```
ubuntu@ip-172-31-45-227: ~
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
```

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/ :
```

```
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
```

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>



NAME:VAISHNAL MALI

DIV:D15A

ADVANCED DEV-OPS EXPERIMENT-05

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

Step 1: Go to the website [Terraform.io](https://www.terraform.io/) and install terraform from there. Select the AMD64 option for windows.

The screenshot shows the Terraform.io website's "Install Terraform" section. At the top right, a dropdown menu shows "1.9.5 (latest)".

macOS

Package manager

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

Binary download

| | | | |
|-------------------------|----------------------------|-------------------------|----------------------------|
| AMD64 Version: 1.9.5 | Download ↓ | ARM64 Version: 1.9.5 | Download ↓ |
|-------------------------|----------------------------|-------------------------|----------------------------|

About Terraform
Define cloud and on-prem resources in human-readable configuration files that you can version, reuse, and share.

Featured docs

- Introduction to Terraform
- Configuration Language
- Terraform CLI
- HCP Terraform
- Provider Use

HCP Terraform
Automate your infrastructure

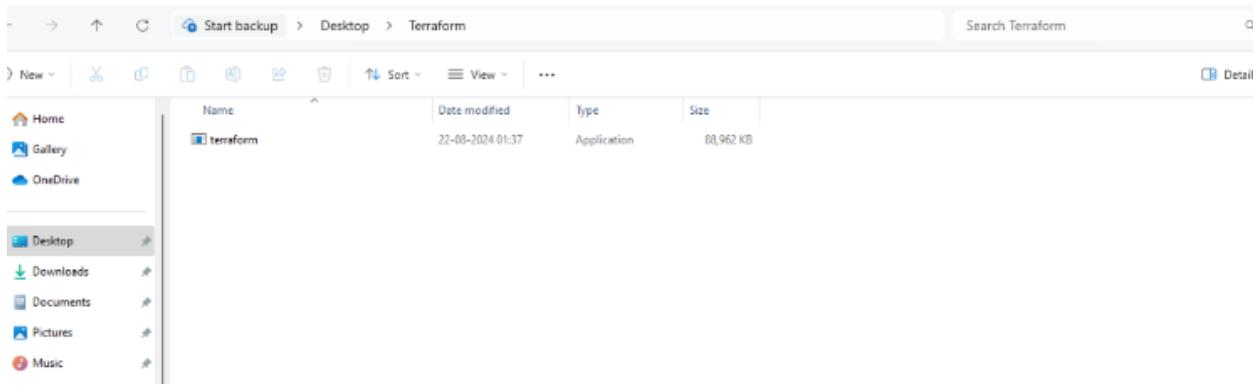
The screenshot shows the Terraform.io website's "Windows" section under the "Binary download" heading.

| | | | |
|-----------------------|----------------------------|-------------------------|----------------------------|
| 386 Version: 1.9.5 | Download ↓ | AMD64 Version: 1.9.5 | Download ↓ |
|-----------------------|----------------------------|-------------------------|----------------------------|

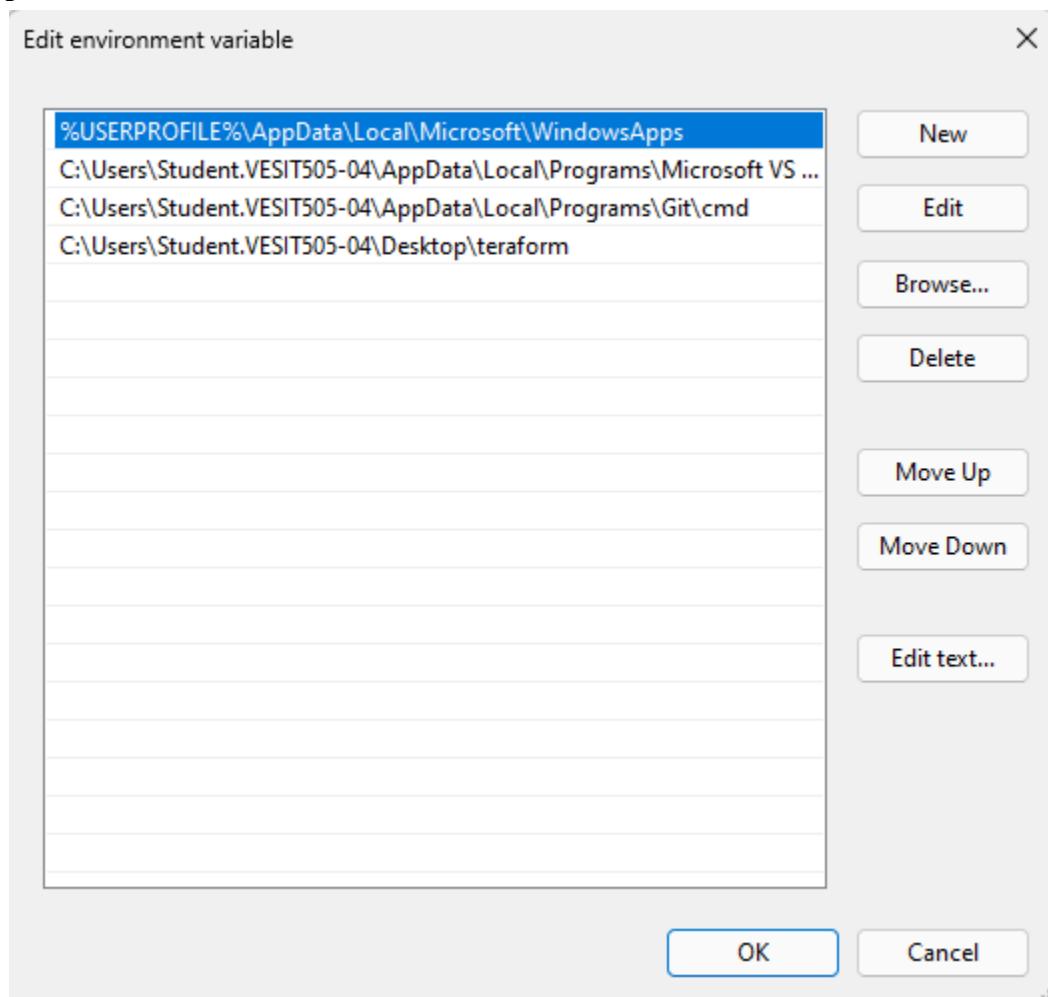
Step 2: Go to the zip file where terraform is installed.

| Name | Date modified | Type | Size |
|-----------|------------------|-------------|-----------|
| terraform | 22-08-2024 14:09 | Application | 88,962 KB |

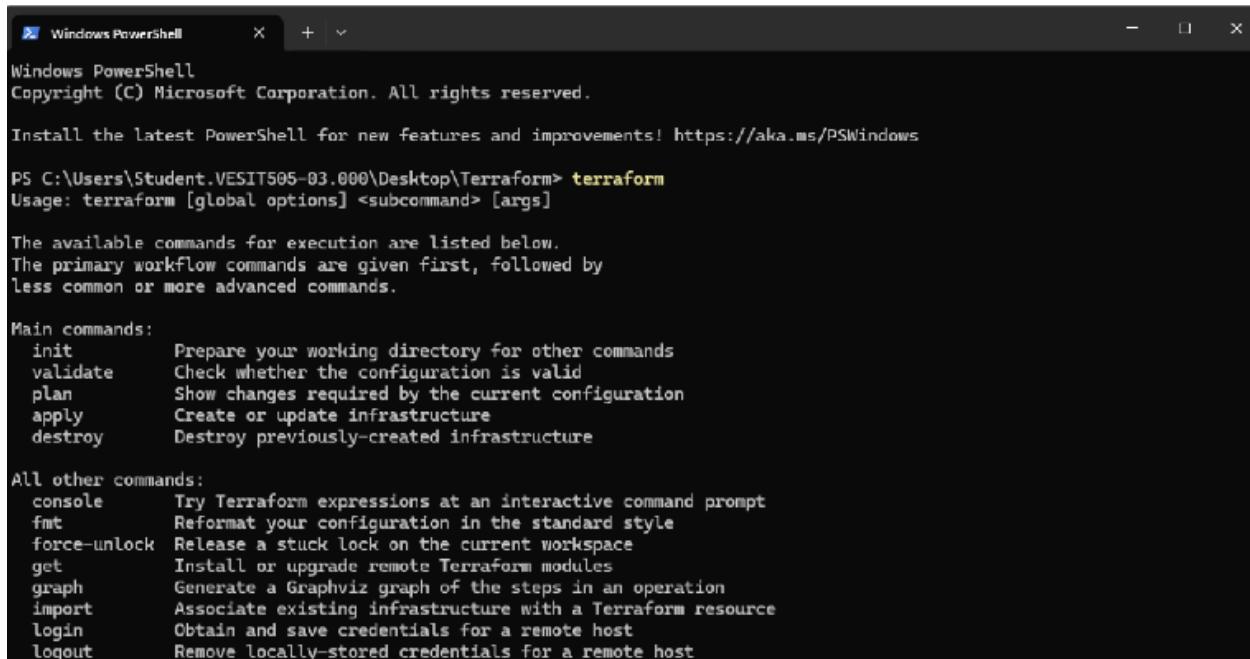
Step 3: Since the entire file is zip create the folder on desktop copy the terraform file there.



Step 4: Now go to search bar and edit environmental variable copy the folder path and paste it in enviormrntal variable.



Step 5: Now go to folder where we install terraform and open it in powershell.type command terraform and hit enter after that check the version of terraform.



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

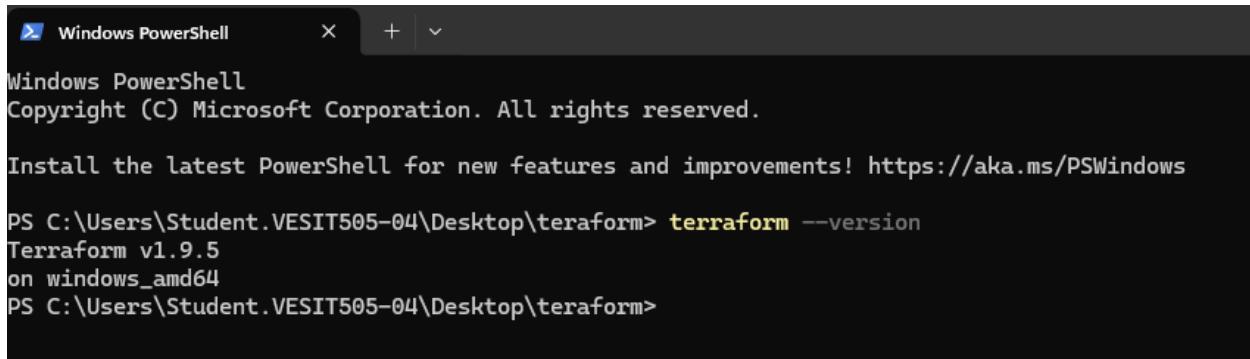
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Student.VESIT505-03.000\Desktop\Terraform> terraform
Usage: terraform [global options] <subcommand> [args]

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

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

All other commands:
  console    Try Terraform expressions at an interactive command prompt
  fmt        Reformat your configuration in the standard style
  force-unlock Release a stuck lock on the current workspace
  get        Install or upgrade remote Terraform modules
  graph      Generate a Graphviz graph of the steps in an operation
  import     Associate existing infrastructure with a Terraform resource
  login      Obtain and save credentials for a remote host
  logout     Remove locally-stored credentials for a remote host
```



```
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\Student.VESIT505-04\Desktop\terraform> terraform --version
Terraform v1.9.5
on windows_amd64
PS C:\Users\Student.VESIT505-04\Desktop\terraform>
```

NAME:VAISHNAL MALI

DIV:D15A

ADVANCED DEV-OPS EXPERIMENT-06

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

Implementation:

A. Creating docker image using terraform

Prerequisite:

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

Step 1: Check the docker functionality

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

C:\Users\Admin>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 (Docker Inc., v0.11.2-desktop.5)
  compose*  Docker Compose (Docker Inc., v2.22.0-desktop.2)
  container  Manage containers
  context   Manage contexts
  dev*     Docker Dev Environments (Docker Inc., v0.1.0)
```

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

Step 2: Firstly create a new folder named ‘Docker’ in the ‘TerraformScripts’ folder. Then create a new docker.tf file using Atom editor and write the following contents into it to create a Ubuntu Linux container

```
❶ Welcome ❷ terraform.tf X
Docker > ❸ terraform.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 image
15 resource "docker_image" "ubuntu" {
16   name = "ubuntu:latest"
17 }
18
19 # Create a container
20 resource "docker_container" "foo" {
21   image = docker_image.ubuntu.image_id
22   name  = "foo"
23   command = ["sleep", "3600"]
24 }
```

Step 3: Execute Terraform Init command to initialize the resource

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

Terraform has been successfully initialized!

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

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

Step 4: Execute Terraform plan to see the available resources

```
PS C:\Users\Admin\Desktop\Terraform Scripts\docker> terraform plan

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

Terraform will perform the following actions:

# docker_container.foo will be created
+ resource "docker_container" "foo" {
    + attach          = false
    + bridge          = (known after apply)
    + command         = [
        + "sleep",
        + "3600",
    ]
    + container_logs = (known after apply)
    + entrypoint      = (known after apply)
    + env             = (known after apply)
    + exit_code       = (known after apply)
    + gateway         = (known after apply)
    + hostname        = (known after apply)
    + id              = (known after apply)
    + image           = (known after apply)
    + init            = (known after apply)
    + ip_address      = (known after apply)
    + ip_prefix_length = (known after apply)
    + ipc_mode        = (known after apply)
    + log_driver      = (known after apply)
    + logs            = false
    + must_run        = true
    + name            = "foo"
    + network_data   = (known after apply)
    + read_only       = false
    + remove_volumes = true
    + restart         = "no"
    + rm              = false
}
```

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

+ healthcheck (known after apply)

+ labels (known after apply)
}

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

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

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

```
PS C:\Users\Admin\Desktop\Terraform Scripts\docker> terraform apply

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

Terraform will perform the following actions:

# docker_container.foo will be created
+ resource "docker_container" "foo" {
    + attach          = false
    + bridge          = (known after apply)
    + command         = [
        + "sleep",
        + "3600",
    ]
    + container_logs = (known after apply)
    + entrypoint      = (known after apply)
    + env             = (known after apply)
    + exit_code       = (known after apply)
    + gateway         = (known after apply)
    + hostname        = (known after apply)
    + id              = (known after apply)
    + image           = (known after apply)
    + init            = (known after apply)
    + ip_address      = (known after apply)
    + ip_prefix_length = (known after apply)
    + ipc_mode        = (known after apply)
    + log_driver       = (known after apply)
    + logs            = false
}
```

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

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

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

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

Enter a value: yes

docker_image.ubuntu: Creating...
docker_image.ubuntu: Still creating... [10s elapsed]
docker_image.ubuntu: Creation complete after 12s [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]
docker_container.foo: Creating...
docker_container.foo: Creation complete after 3s [id=9cd9e799109022c4cfa1545e449894948a72460b66ca2e468f933bc2b650255]

Apply complete! Resources: 2 added, 0 changed, 0 destroyed.
```

Docker images, Before Executing Apply step:

| REPOSITORY | TAG | IMAGE ID | CREATED | SIZE |
|------------|-----|----------|---------|------|
|------------|-----|----------|---------|------|

Docker images, After Executing Apply step:

| REPOSITORY | TAG | IMAGE ID | CREATED | SIZE |
|------------|--------|--------------|-------------|--------|
| ubuntu | latest | edbfe74c41f8 | 3 weeks ago | 78.1MB |

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

```
PS C:\Users\Admin\Desktop\Terraform Scripts\docker> terraform destroy
docker_image.ubuntu: Refreshing state... [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]
docker_container.foo: Refreshing state... [id=9dc9e799109022c4cfa1545e449894948a72460b66ca2e468f933bc2b650255]

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          = [
        - "sleep",
        - "3600",
    ] -> 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         = "9dc9e799109" -> null
    - id               = "9dc9e799109022c4cfa1545e449894948a72460b66ca2e468f933bc2b650255" -> 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
    - log_opts           = {} -> null
    - logs              = false -> null
}
```

```

    - ip_address          = "172.17.0.2"
    - ip_prefix_length    = 16
    - network_name        = "bridge"
    # (2 unchanged attributes hidden)
  },
] -> null
- network_mode      = "default" -> null
- privileged        = false -> null
- publish_all_ports = false -> null
- read_only         = false -> null
- remove_volumes   = true -> null
- restart           = "no" -> null
- rm                = false -> null
- runtime           = "runc" -> null
- security_opts     = [] -> null
- shm_size          = 64 -> null
- start              = true -> null
- stdin_open         = false -> null
- stop_timeout       = 0 -> null
- storage_opts      = {} -> null
- sysctls            = {} -> null
- tmpfs              = {} -> null
- tty                = false -> null
# (8 unchanged attributes hidden)
}

# 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=9dc9e799109022c4cfa1545e449894948a72460b66ca2e468f933bc2b650255]
docker_container.foo: Destruction complete after 0s
docker_image.ubuntu: Destroying... [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]
docker_image.ubuntu: Destruction complete after 1s

```

Destroy complete! Resources: 2 destroyed.

PS C:\Users\Admin\Desktop\Terraform Scripts\docker> []

Docker images After Executing Destroy step

| REPOSITORY | TAG | IMAGE ID | CREATED | SIZE |
|------------|-----|----------|---------|------|
|------------|-----|----------|---------|------|

ADVANCE DEVOPS EXP 7

Name:VAISHNAL MALI
Class:D15A
Roll No:27

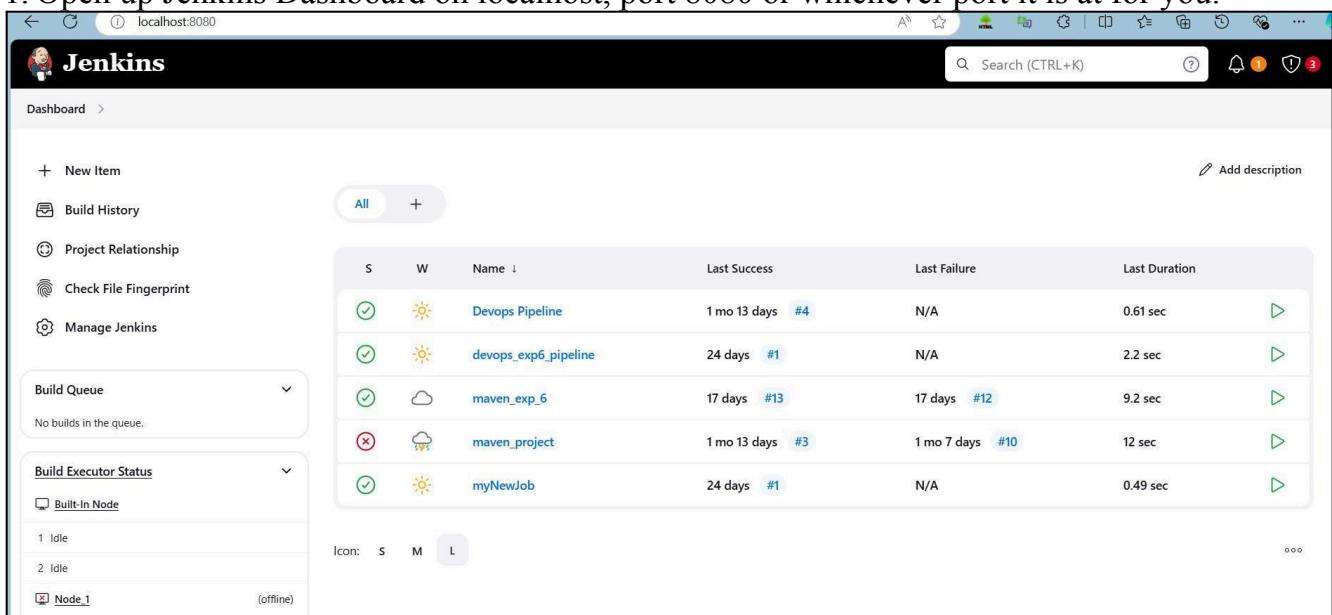
Aim: To understand Static Analysis SAST process and learn to integrate Jenkins SAST to SonarQube/GitLab.

Integrating Jenkins with SonarQube:

- Jenkins installed
- Docker Installed (for SonarQube)
- SonarQube Docker Image

Steps to integrate Jenkins with SonarQube

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



The screenshot shows the Jenkins dashboard at localhost:8080. On the left, there's a sidebar with links for 'New Item', 'Build History', 'Project Relationship', 'Check File Fingerprint', and 'Manage Jenkins'. Below these are sections for 'Build Queue' (empty) and 'Build Executor Status' (two idle nodes: 'Node_1' and 'Node_2'). The main area displays a table of build jobs:

| S | W | Name | Last Success | Last Failure | Last Duration |
|---|----|----------------------|-----------------|-----------------|---------------|
| ✓ | ☀️ | Devops Pipeline | 1 mo 13 days #4 | N/A | 0.61 sec |
| ✓ | ☀️ | devops_exp6_pipeline | 24 days #1 | N/A | 2.2 sec |
| ✓ | ☁️ | maven_exp_6 | 17 days #13 | 17 days #12 | 9.2 sec |
| ✗ | ☁️ | maven_project | 1 mo 13 days #3 | 1 mo 7 days #10 | 12 sec |
| ✓ | ☀️ | myNewJob | 24 days #1 | N/A | 0.49 sec |

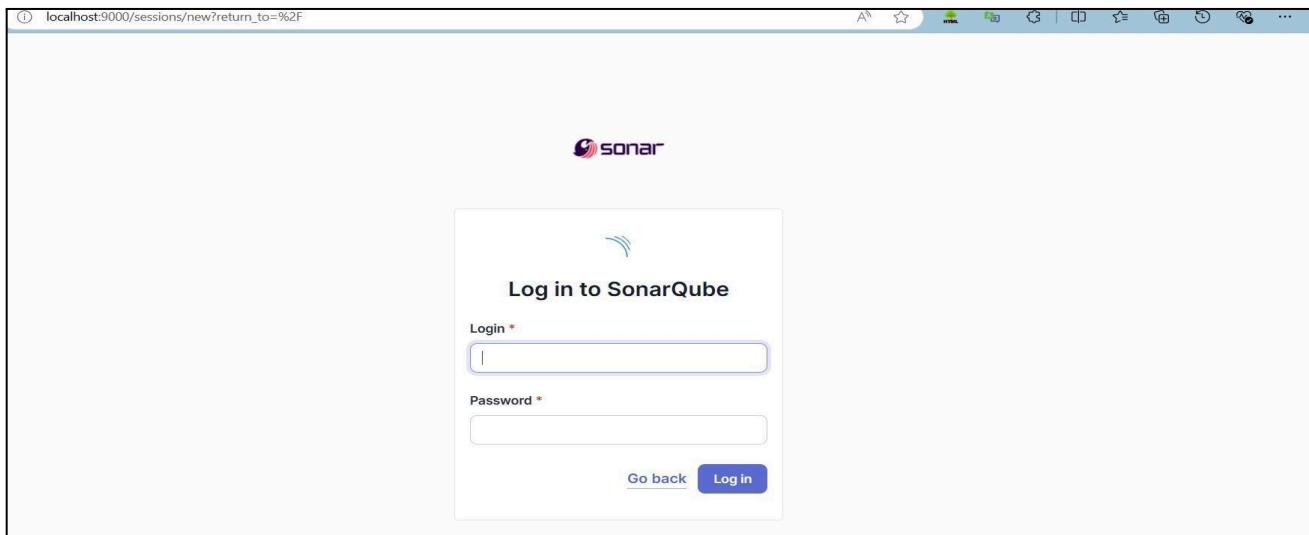
2. Run SonarQube in a Docker container using this command -
`docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest`

```
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>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
e54bd5b0b0df29bd00176c14e08bdc56d7fac6b45ba606f0a30c522fc3fe93da

C:\Windows\System32>
```

- Once the container is up and running, you can check the status of SonarQube at localhost port 9000.



- Login to SonarQube using username admin and password admin.

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 manual project in SonarQube with the name sonarqube

1 of 2

Create a local project

Project display name *
adv_devops_7_sonarqube

Project key *
adv_devops_7_sonarqube

Main branch name *
main

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

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 relevant changes. 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 be considered new code.
Recommended for projects following continuous delivery.

Setup the project and come back to Jenkins Dashboard.

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

The screenshot shows the Jenkins 'Plugins' page. On the left, there's a sidebar with links: 'Updates' (25), 'Available plugins', 'Installed plugins', 'Advanced settings', and 'Download progress' (which is selected). The main area is titled 'Download progress' and shows the 'Preparation' step completed with three green checkmarks: 'Checking internet connectivity', 'Checking update center connectivity', and 'Success'. Below that, under 'SonarQube Scanner', it shows 'Success' next to both 'Loading plugin extensions' and another green checkmark. At the bottom, there are two buttons: one pointing to 'Go back to the top page' with the note '(you can start using the installed plugins right away)', and another with a checkbox labeled 'Restart Jenkins when installation is complete and no jobs are running'.

6. Under Jenkins 'Manage Jenkins' then go to 'system', scroll and look for **SonarQube Servers**

and enter the details.

Enter the Server Authentication token if needed.

In SonarQube installations: Under **Name** add <project name of sonarqube>, here we have named it as **adv_devops_7_sonarqube**

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

The screenshot shows the 'SonarQube servers' configuration page. It has several sections: 'Environment variables' (unchecked), 'SonarQube installations' (list of installations), 'Name' (input field containing 'adv_devops_7_sonarqube'), 'Server URL' (input field containing 'https://localhost:9000'), 'Server authentication token' (dropdown menu showing '- none -' and a '+ Add' button), and an 'Advanced' dropdown menu at the bottom.

7. Search for SonarQube Scanner under Global Tool Configuration.

Choose the latest configuration and choose Install automatically.

Dashboard > Manage Jenkins > Tools

The screenshot shows the Jenkins 'Manage Jenkins' interface under the 'Tools' section. It includes sections for 'Gradle installations', 'SonarScanner for MSBuild installations', 'SonarQube Scanner installations', and 'Ant installations'. Each section has a 'Add [Tool]' button.

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

The screenshot shows the 'SonarQube Scanner installations' configuration screen. It allows adding a new scanner with a name (e.g., 'sonarqube_exp7') and the 'Install automatically' checkbox selected. A sub-section for 'Install from Maven Central' shows the version 'SonarQube Scanner 6.1.0.4477'.

8. After the configuration, create a New Item in Jenkins, choose a freestyle project.

The screenshot shows the Jenkins 'New Item' creation dialog. In the top left, there is a text input field containing 'adv_devops_exp7' with the placeholder '» Required field'. Below this, a list of project types is shown in cards:

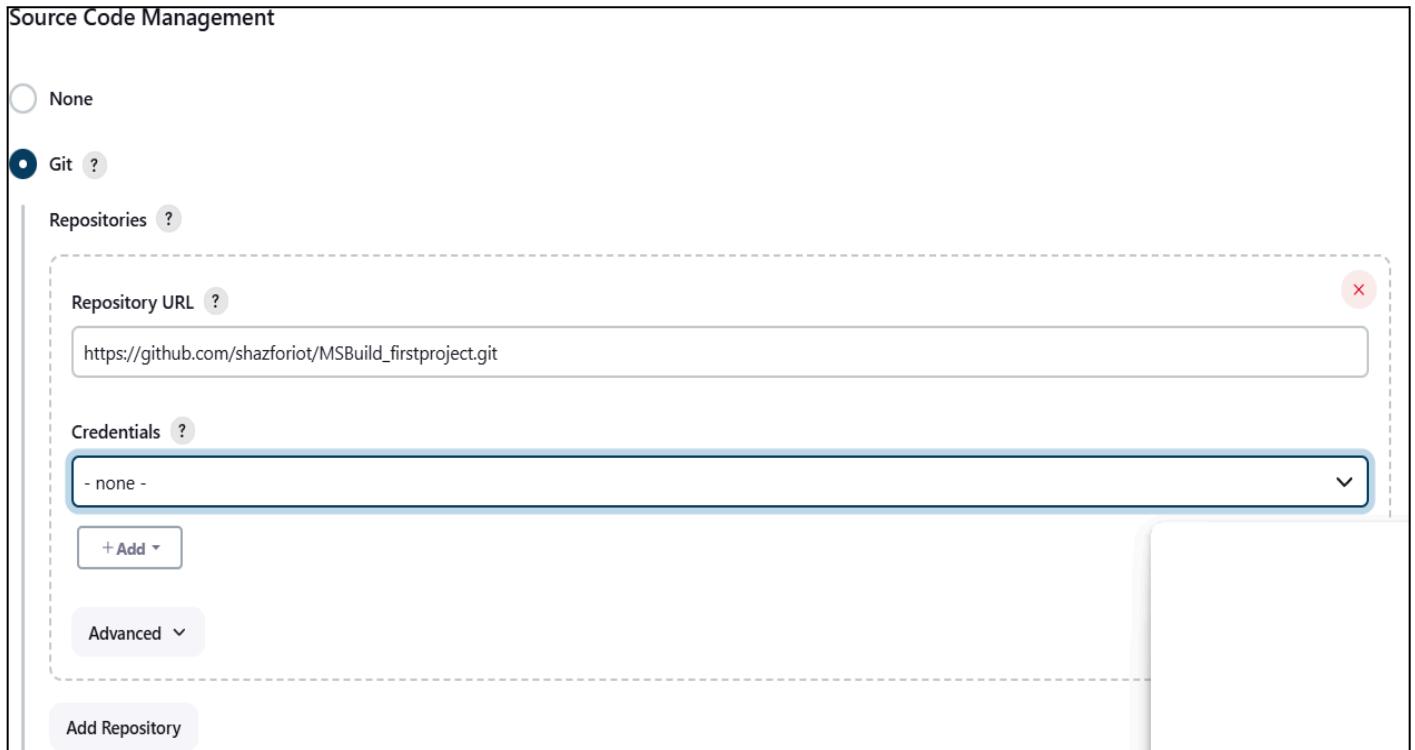
- Freestyle project**: Classic, general-purpose job type that checks out from up to one SCM, executes build steps serially, followed by post-build steps like archiving artifacts and sending email notifications.
- Maven project**: Build a maven project. Jenkins takes advantage of your POM files and drastically reduces the configuration.
- Pipeline**: Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.
- Multi-configuration project**: Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.
- Folder**: Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.

At the bottom left is a blue 'OK' button, and at the bottom right is a link labeled 'branch Pipeline'.

9. Choose this GitHub repository in Source Code Management.

https://github.com/shazforiot/MSBuild_firstproject.git

It is a sample hello-world project with no vulnerabilities and issues, just to test the integration.



10. Under Select project → Configuration → Build steps → Execute SonarQube Scanner, enter these Analysis properties. Mention the SonarQube Project Key, Login, Password, Source path and Host URL.

Configure

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

Build Environment

Filter

- Execute SonarCube Scanner
- Execute Windows batch command
- Execute shell
- Invoke Ant
- Invoke Gradle script
- Invoke top-level Maven targets
- Run with timeout
- Set build status to "pending" on GitHub commit
- SonarScanner for MSBuild - Begin Analysis
- SonarScanner for MSBuild - End Analysis

Add build step ^

Post-build Actions

Execute SonarQube Scanner

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

Path to project properties ?
[Empty input field]

Analysis properties ?
sonar.projectKey=adv_devops_7_sonarqube
sonar.host.url=http://localhost:9000
sonar.login=admin
sonar.sources=.

Additional arguments ?
[Empty input field]

JVM Options ?
[Empty input field]

Then save

Status **adv_devops_exp7** Add description Disable Project

- </> Changes
- Workspace
- Build Now
- Configure
- Delete Project
- SonarQube
- Rename

SonarQube Permalinks

- Last build (#2), 1 day 20 hr ago
- Last stable build (#2), 1 day 20 hr ago
- Last successful build (#2), 1 day 20 hr ago
- Last completed build (#2), 1 day 20 hr ago

11. Go to http://localhost:9000/<user_name>/permissions and allow Execute Permissions to the Admin user

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.

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

4 of 4 shown

IF CONSOLE OUTPUT FAILED:

Step 1: Generate a New Authentication Token in SonarQube

1. Login to SonarQube:

- Open your browser and go to **http://localhost:9000**.
- Log in with your admin credentials (default username is **admin**, and the password is either **admin** or your custom password if it was changed).

2. Generate a New Token:

- Click on your **username** in the top-right corner of the SonarQube dashboard.
- Select **My Account** from the dropdown menu.
- Go to the **Security** tab.
- Under **Generate Tokens**, type a name for the token (e.g., "Jenkins-SonarQube").
- Click **Generate**.
- Copy the token and save it securely. You will need it in Jenkins.

Step 2: Update the Token in Jenkins

1. Go to Jenkins Dashboard:

- Open Jenkins and log in with your credentials.

2. Configure the Jenkins Job:

- Go to the job that is running the SonarQube scanner ([adv_devops_exp⁷](#)).
- Click **Configure**.

3. Update the SonarQube Token:

- In the SonarQube analysis configuration (either in the pipeline script or under "Build" section, depending on your job type), update the **sonar.login** parameter with the new token.

Execute SonarQube Scanner

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

Path to project properties ?
[Empty text area]

Analysis properties ?
sonar.projectKey=adv_devops_7_sonarqube
sonar.host.url=http://localhost:9000
-Dsonar.login=sq...
sonar.sources=.

Additional arguments ?
[Empty text area]

JVM Options ?
[Empty text area]

12. Run the Jenkins build.

Status ✓ adv_devops_exp7

- </> Changes
- Workspace
- ▷ Build Now
- ⚙ Configure
- >Delete Project

SonarQube

Permalinks

- Last build (#10), 19 sec ago
- Last stable build (#10), 19 sec ago
- Last successful build (#10), 19 sec ago
- Last failed build (#8), 22 min ago
- Last unsuccessful build (#8), 22 min ago
- Last completed build (#10), 19 sec ago

Build History trend ▾

Filter... /

#10 Sep 18, 2024, 2:36PM

Add description Disable Project

Check the console Output

Dashboard > adv_devops_exp7 > #10 > Console Output

Status ✓ Console Output

- </> Changes
- Console Output
- View as plain text
- Edit Build Information
- Delete build '#10'
- Timings

Started by user unknown or anonymous
Running as SYSTEM
Building on the built-in node in workspace C:\ProgramData\Jenkins\jenkins\workspace\adv_devops_exp7
The recommended git tool is: NONE
No credentials specified

```
> git.exe rev-parse --resolve-git-dir C:\ProgramData\Jenkins\jenkins\workspace\adv_devops_exp7\.git # timeout=10
Fetching changes from the remote Git repository
> git.exe config remote.origin.url https://github.com/shazforiot/MSBuild_firstproject # timeout=10
Fetching upstream changes from https://github.com/shazforiot/MSBuild_firstproject
> git.exe --version # timeout=10
> git --version # 'git version 2.46.0.windows.1'
```

13. Once the build is complete, check project on SonarQube

The screenshot shows the SonarQube interface for the project 'adv_devops_7.sonarqube'. The top navigation bar includes links for Projects, Issues, Rules, Quality Profiles, Quality Gates, Administration, More, and a search bar. Below the navigation is a breadcrumb trail: star icon → adv_devops_7.sonarqube / main. A dropdown menu for 'main' is open, showing options like 'Switch to', 'Edit', 'Delete', and 'Archive'. The main content area is titled 'Overview' and displays the following information:

- Status:** Quality Gate ✓ Passed
- Last analysis:** 5 minutes ago
- Warnings:** The last analysis has warnings. [See details](#)
- Code Types:** New Code (light gray), Overall Code (white)
- Metrics:** Security, Reliability, Maintainability

ADVANCE DEVOPS EXP 8

Name: Vaishnal Dilip Mali

Class: D15A

Roll No: 27

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

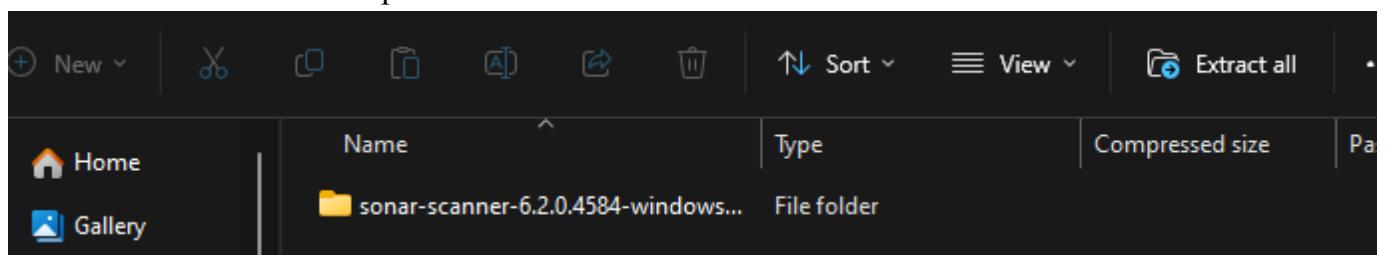
Step 1: Download sonar scanner

<https://docs.sonarsource.com/sonarqube/latest/analyzing-source-code/scanners/sonarscan>

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

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

Extract the downloaded zip file in a folder.



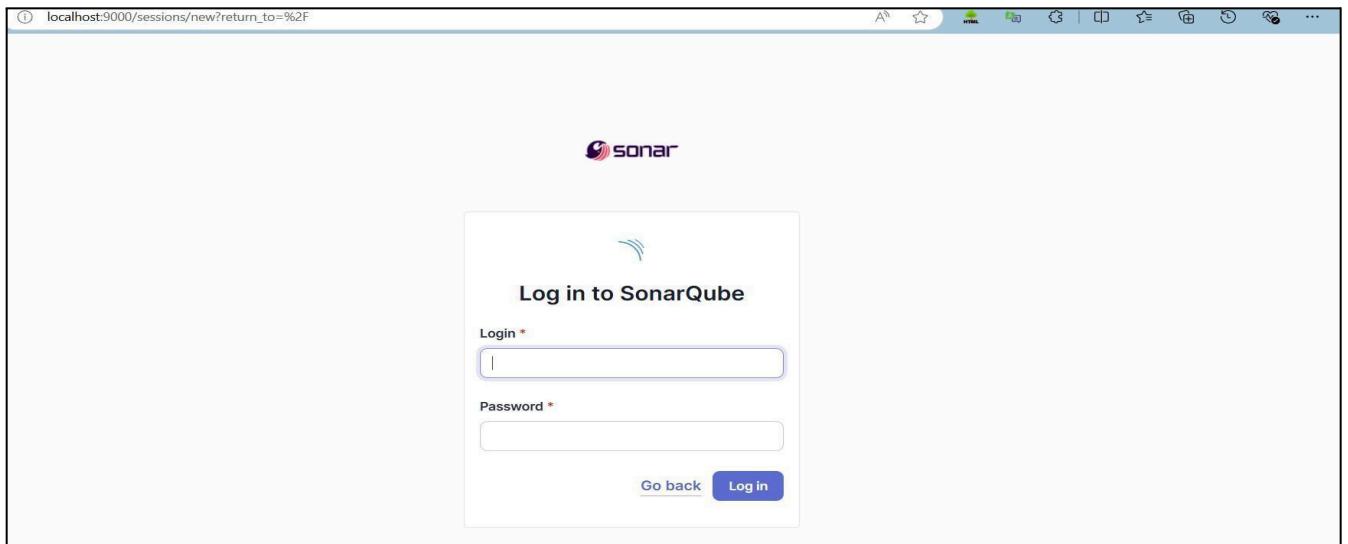
1. Install sonarqube image

Command: **docker pull**

sonarqube

```
C:\Windows\System32>docker pull sonarqube
Using default tag: latest
latest: Pulling from library/sonarqube
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Image is up to date for sonarqube:latest
docker.io/library/sonarqube:latest
```

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



SonarQube at localhost port 9000.

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

A screenshot of the SonarQube interface after logging in. The top navigation bar includes 'Projects', 'Issues', 'Rules', 'Quality Profiles', 'Quality Gates', 'Administration', 'More', and a search icon. The main content area is titled 'How do you want to create your project?'. It lists several import options: 'Import from Azure DevOps' (Setup), 'Import from Bitbucket Cloud' (Setup), 'Import from Bitbucket Server' (Setup), 'Import from GitHub' (Setup), and 'Import from GitLab' (Setup). At the bottom, there is a button labeled 'Create a local project'.

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

1 of 2

Create a local project

Project display name *

Project key *

Main branch name *

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

[Cancel](#)

[Next](#)

2 of 2

Set up project for Clean as You Code

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

Choose the baseline for new code for this project

Use the global setting

Previous version

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

Define a specific setting for this project

Previous version

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

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

The screenshot shows the Jenkins dashboard with the following details:

- Left sidebar:** Includes links for "New Item", "Build History", "Project Relationship", "Check File Fingerprint", and "Manage Jenkins".
- Build Queue:** Shows "No builds in the queue."
- Build Executor Status:** Shows 1 Idle and 2 Idle nodes, with one node labeled "(offline)".
- Central Table:** Displays a list of build jobs with columns: S (Status), W (Last Success), Name, Last Success, Last Failure, and Last Duration.

| S | W | Name | Last Success | Last Failure | Last Duration |
|-----------------|------------|----------------------|-----------------|-----------------|---------------|
| Green checkmark | Sun icon | Devops Pipeline | 1 mo 13 days #4 | N/A | 0.61 sec |
| Green checkmark | Sun icon | devops_exp6_pipeline | 24 days #1 | N/A | 2.2 sec |
| Green checkmark | Cloud icon | maven_exp_6 | 17 days #13 | 17 days #12 | 9.2 sec |
| Red X | Cloud icon | maven_project | 1 mo 13 days #3 | 1 mo 7 days #10 | 12 sec |
| Green checkmark | Sun icon | myNewJob | 24 days #1 | N/A | 0.49 sec |
- Bottom:** Icon selection buttons for S, M, and L.

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

The screenshot shows the Jenkins Manage Jenkins > Plugins page with the following details:

- Left sidebar:** Includes links for "Updates" (25), "Available plugins" (selected), "Installed plugins", and "Advanced settings".
- Search Bar:** Contains the search term "sonarq".
- Table:** Shows the "SonarQube Scanner" plugin information.

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

Details for the SonarQube Scanner plugin:
This plugin allows an easy integration of SonarQube, the open source platform for Continuous Inspection of code quality.

The screenshot shows the Jenkins Manage Jenkins > Plugins > Download progress page with the following details:

- Left sidebar:** Includes links for "Updates" (25), "Available plugins" (selected), "Installed plugins", and "Advanced settings".
- Section:** "Download progress" (selected).
- Preparation:** A bulleted list of steps:
 - Checking internet connectivity
 - Checking update center connectivity
 - Success
- Progress:** Shows the status of the SonarQube Scanner download:

| Task | Status |
|---------------------------|---------|
| SonarQube Scanner | Success |
| Loading plugin extensions | Success |
- Buttons:**
 - [Go back to the top page](#) (you can start using the installed plugins right away)
 - [Restart Jenkins when installation is complete and no jobs are running](#)

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

and enter the details.

Enter the Server Authentication token if needed.

In SonarQube installations: Under **Name** add <project name of sonarqube> for me
adv_devops_7_sonarqube

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



The screenshot shows the Jenkins configuration interface for SonarQube servers. It includes fields for Name (sonarqube), Server URL (http://localhost:9000), and a dropdown for Server authentication token (set to - none -). There are also 'Add' and 'Advanced' buttons.

| | |
|-----------------------------|---|
| Name | sonarqube |
| Server URL | Default is http://localhost:9000 http://localhost:9000 |
| Server authentication token | - none - + Add Advanced |

8. Search for SonarQube Scanner under Global Tool Configuration.

Choose the latest configuration and choose Install automatically.

Dashboard > Manage Jenkins > Tools

The screenshot shows the Jenkins 'Tools' configuration page. It includes sections for 'Add Git', 'Gradle installations' (with an 'Add Gradle' button), 'SonarScanner for MSBuild installations' (with an 'Add SonarScanner for MSBuild' button), 'SonarQube Scanner installations' (with an 'Add SonarQube Scanner' button), and 'Ant installations'. The 'SonarQube Scanner' section is currently selected.

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

The screenshot shows the 'SonarQube Scanner' configuration dialog. It includes fields for 'Name' (set to 'sonarqube_exp8'), 'Install automatically' (checked), 'Install from Maven Central' (with 'Version' set to 'SonarQube Scanner 6.2.0.4584'), and an 'Add Installer' button. At the bottom is a large 'Add SonarQube Scanner' button.

Check the “Install automatically” option.

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

New Item

Enter an item name
adv_devops_exp8

Select an item type

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

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

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

OK

10. Under Pipeline script, enter the following:

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

}

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

Definition

Pipeline script

Script ?

```
1 node {  
2 stage('Cloning the GitHub Repo') {  
3 git 'https://github.com/shazforiot/GOL.git'  
4 }  
5  
6 stage('SonarQube analysis') { withSonarQubeEnv('<Name_of_SonarQube_environment_on_Jenkins>') {  
7 sh """  
8 <PATH_TO SONARQUBE_SCANNER_FOLDER>/bin/sonar-scanner \  
9 -D sonar.login=admin \  
10 -D sonar.password=admin> \  
11 -D sonar.projectKey=sonarqube \  
12 -D sonar.exclusions=vendor/**,resources/**,**/*.java \  
13 -D sonar.host.url=http://localhost:9000  
14 """  
15 }  
16 }  
17 }  
18 }
```

Use Groovy Sandbox ?

[Pipeline Syntax](#)

11. Build project

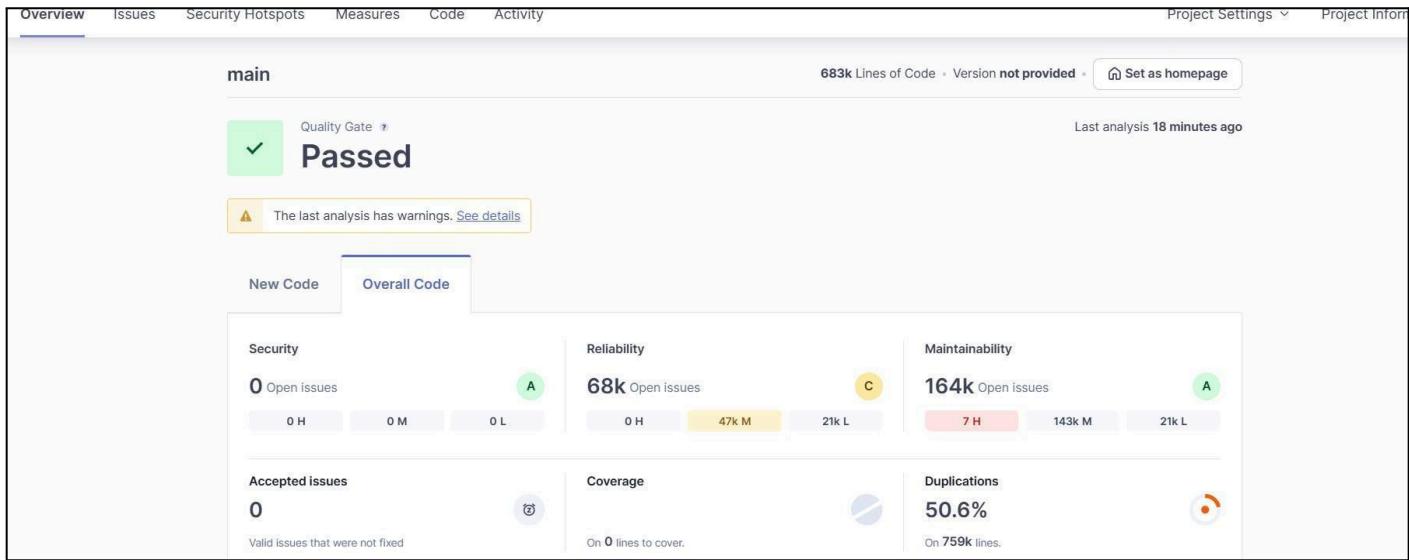
The screenshot shows the Jenkins Pipeline interface for a build named "adv_devops_exp8". On the left, there's a sidebar with various options like Status, Changes, Build Now, Configure, Delete Pipeline, Full Stage View, SonarQube, Stages, Rename, and Pipeline Syntax. Below that is a "Build History" section showing three builds (#9, #8, #7) with their status and timestamps. The main area is titled "Stage View" and displays a grid of stages. The first stage, "Cloning the GitHub Repo", took 3s and is green. The second stage, "SonarQube analysis", took 40s and failed, indicated by a red background and the word "failed". The third stage, which appears to be a JMeter test, took 120ms and failed, also indicated by a red background and the word "failed". The overall average stage time is 6min 2s.

12. Check console

The screenshot shows the Jenkins Console Output for the same build. The sidebar includes Status, Changes, Console Output (which is selected), View as plain text, Edit Build Information, Delete build '#9', Timings, Git Build Data, Pipeline Overview, Pipeline Console, Replay, Pipeline Steps, Workspaces, and Previous Build. The main content area shows the console log starting with a warning about duplicate references in a JMeter documentation file. The log continues with several similar warnings at different line numbers, indicating a repetitive issue in the codebase being tested.

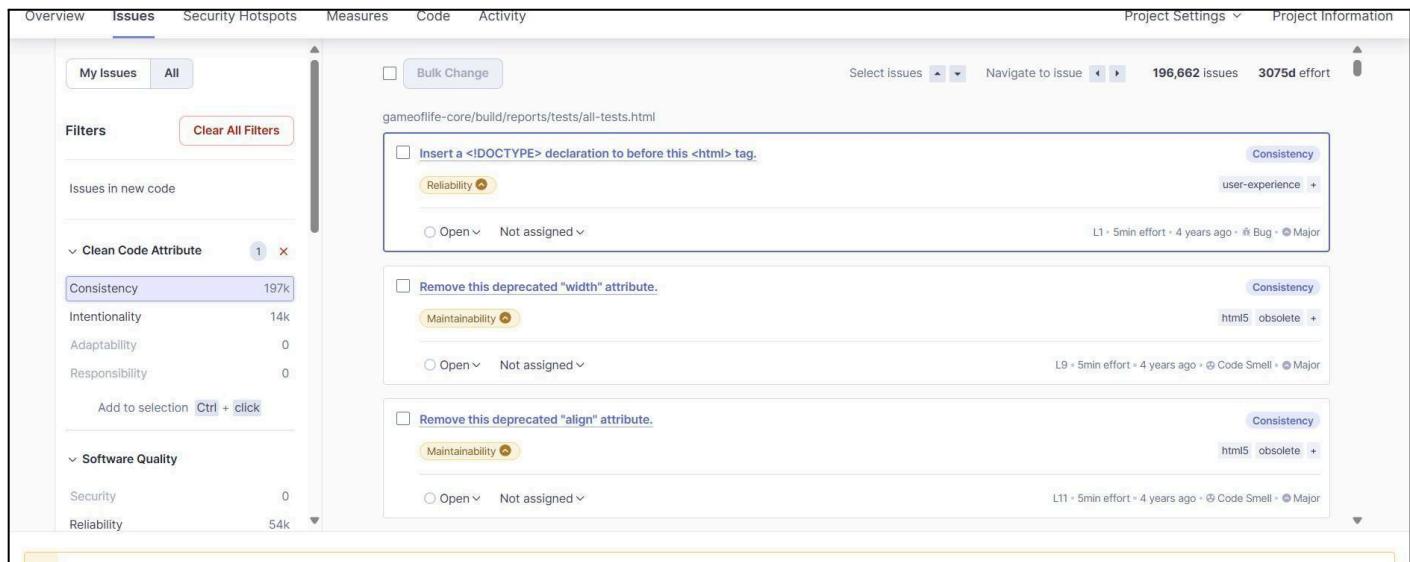
```
Skipping 4,246 KB.. Full Log
16:19:49.751 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 512. Keep only the first 100 references.
16:19:49.751 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 248. Keep only the first 100 references.
16:19:49.751 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 886. Keep only the first 100 references.
16:19:49.751 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 249. Keep only the first 100 references.
16:19:49.751 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 662. Keep only the first 100 references.
16:19:49.751 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 615. Keep only the first 100 references.
16:19:49.751 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 664. Keep only the first 100 references.
16:19:49.751 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 913. Keep only the first 100 references.
16:19:49.752 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 810. Keep only the first 100 references.
16:19:49.752 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 668. Keep only the first 100 references.
16:19:49.752 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 548. Keep only the first 100 references.
16:19:49.752 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 543. Keep only the first 100 references.
16:19:49.752 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line 152. Keep only the first 100 references.
16:19:49.752 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
```

13. Now, check the project in SonarQube



14. Code Problems

• Consistency



● Intentionality

The screenshot shows a software interface for managing code quality and security. At the top, there are tabs for Overview, Issues, Security Hotspots, Measures, Code, and Activity. The Issues tab is selected. In the top right corner, it says "Project Settings" and "Project Information". Below the tabs, there are buttons for "My Issues" and "All". A "Bulk Change" button is available, along with "Select issues" and "Navigate to issue" buttons. It also displays "13,887 issues" and "59d effort".

The main area is titled "gameoflife-acceptance-tests/Dockerfile". On the left, there's a sidebar with "Filters" and a "Clear All Filters" button. It lists "Issues in new code" and categories under "Clean Code Attribute":

- Consistency: 197k
- Intentionality: 14k (selected)
- Adaptability: 0
- Responsibility: 0

An "Add to selection" button with "Ctrl + click" instructions is present. Below this, there are sections for "Software Quality" and "Reliability", both with 0 issues.

The main content area shows three specific issues:

- Use a specific version tag for the image.** (Intentionality)
Maintainability
Open Not assigned L1 - 5min effort 4 years ago ⚡ Code Smell ⚡ Major
- Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.** (Intentionality)
Maintainability
Open Not assigned L12 - 5min effort 4 years ago ⚡ Code Smell ⚡ Major
- Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.** (Intentionality)
Maintainability
Open Not assigned L12 - 5min effort 4 years ago ⚡ Code Smell ⚡ Major

Bugs

The screenshot shows a list of three bugs for the 'gameoflife-core' project:

- Bug 1:** "Add 'lang' and/or "xml:lang" attributes to this "<html>" element". Status: Open, Not assigned. Intentionality: accessibility wcag2-a. Effort: L1 = 2min effort, 4 years ago. Type: Bug, Major.
- Bug 2:** "Insert a <!DOCTYPE> declaration to before this <html> tag.". Status: Open, Not assigned. Intentionality: user-experience. Effort: L1 = 5min effort, 4 years ago. Type: Bug, Major.
- Bug 3:** "Add "<th>" headers to this "<table>". Status: Open, Not assigned. Intentionality: accessibility wcag2-a. Effort: L9 = 2min effort, 4 years ago. Type: Bug, Major.

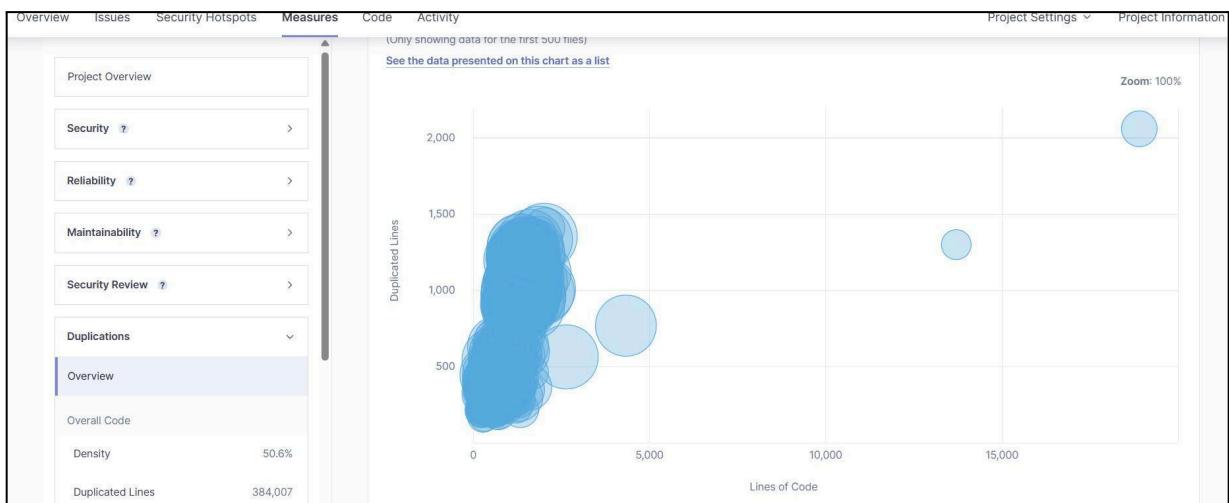
Code Smells

The screenshot shows a list of code smells for the 'gameoflife-acceptance-tests/Dockerfile' file:

- Code Smell 1:** "Use a specific version tag for the image.". Status: Open, Not assigned. Intentionality: No tags. Effort: L1 = 5min effort, 4 years ago. Type: Code Smell, Major.
- Code Smell 2:** "Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.". Status: Open, Not assigned. Intentionality: No tags. Effort: L12 = 5min effort, 4 years ago. Type: Code Smell, Major.
- Code Smell 3:** "Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.". Status: Open, Not assigned. Intentionality: No tags. Effort: L12 = 5min effort, 4 years ago. Type: Code Smell, Major.

On the left, there are filters for 'Clean Code Attribute' (Consistency, Intentionality, Adaptability, Responsibility) and 'Software Quality' (Security, Reliability, Maintainability).

Duplications



- Cyclomatic Complexities

The screenshot shows the SonarQube interface for the 'gameoflife' project. The top navigation bar includes 'Overview', 'Issues', 'Security Hotspots', 'Measures' (which is selected), 'Code', and 'Activity'. On the right, there are 'Project Settings' and 'Project Information' dropdowns. The main content area is titled 'Cyclomatic Complexity 1,112 See history'. It lists six components with their respective cyclomatic complexity counts: 'gameoflife-acceptance-tests' (18), 'gameoflife-build' (18), 'gameoflife-core' (18), 'gameoflife-deploy' (18), 'gameoflife-web' (1,094), and 'pom.xml' (18). A note at the bottom indicates '6 of 6 shown'. On the left, a sidebar lists various metrics: Security, Reliability, Maintainability, Security Review, Duplications, Size, Complexity (selected), and Cyclomatic Complexity (1,112).

| Component | Cyclomatic Complexity |
|-----------------------------|-----------------------|
| gameoflife-acceptance-tests | 18 |
| gameoflife-build | 18 |
| gameoflife-core | 18 |
| gameoflife-deploy | 18 |
| gameoflife-web | 1,094 |
| pom.xml | 18 |

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

ADVANCE DEVOPS EXPERIMENT 9

Name: Vaishnal Dilip Mali

Class: D15A

Roll No: 27

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

Step 1: Create an Amazon Linux EC2 instance and name it as nagios-host

| Instances (1) Info | | Last updated 1 minute ago | Connect | Instance state ▾ | Actions ▾ | Launch instances ▾ | Edit filters |
|------------------------------------|-------------|---|---|------------------|---------------------------|------------------------------------|------------------------------|
| | | <input type="text"/> Find Instance by attribute or tag (case-sensitive) | | All states ▾ | | | |
| <input type="checkbox"/> | Name ▾ | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability zone |
| <input type="checkbox"/> | nagios-host | i-08373a53cb8045f0a | Running Details Logs | t2.micro | Initializing | View alarms + | ap-south-1 |

Step 2: Edit the following inbound rules of the specified security groups and ensure HTTP, HTTPS, SSH, ICMP are accessible from anywhere

| Inbound rules (7) | | | | | | Edit | Manage tags | Edit inbound rules |
|-------------------|--------------------------|------------|-----------------|-----------|------------|------------------------|-----------------------------|------------------------------------|
| | | | | | | Search | | |
| ▼ | Security group rule... ▾ | IP version | Type | Protocol | Port range | | | |
| | sgr-0842dcf237958c987 | IPv4 | HTTPS | TCP | 443 | | | |
| | sgr-0e3b5fe756fe77f0a | IPv4 | All traffic | All | All | | | |
| | sgr-07c7572562bdb3... | IPv4 | Custom TCP | TCP | 0 | | | |
| | sgr-07882e9275b39c4... | IPv4 | HTTP | TCP | 80 | | | |
| | sgr-08540b31df42cc513 | IPv4 | All ICMP - IPv4 | ICMP | All | | | |
| | sgr-0dcbe24f99412dcfb | IPv6 | Custom TCP | TCP | 0 | | | |
| | sgr-09ccae5af38c85345 | IPv6 | All ICMP - IPv6 | IPv6 ICMP | All | | | |

Step 3: Connect to your EC2 instance via the connect option available in EC2 instances menu

```
[ec2-user@ip-172-31-33-14 ~]$ sudo yum install httpd php
Last metadata expiration check: 0:19:23 ago on Thu Sep 26 08:42:17 2024.
Dependencies resolved.
```

| Package | Architecture | Version | Repository | Size |
|---------------------------------|--------------|------------------------|-------------|-------|
| Installing: | | | | |
| httpd | x86_64 | 2.4.62-1.amzn2023 | amazonlinux | 48 k |
| php8.3 | x86_64 | 8.3.10-1.amzn2023.0.1 | amazonlinux | 10 k |
| Installing dependencies: | | | | |
| apr | x86_64 | 1.7.2-2.amzn2023.0.2 | amazonlinux | 129 k |
| apr-util | x86_64 | 1.6.3-1.amzn2023.0.1 | amazonlinux | 98 k |
| generic-logos-httpd | noarch | 18.0.0-12.amzn2023.0.3 | amazonlinux | 19 k |
| httpd-core | x86_64 | 2.4.62-1.amzn2023 | amazonlinux | 1.4 M |
| httpd-filesystem | noarch | 2.4.62-1.amzn2023 | amazonlinux | 14 k |
| httpd-tools | x86_64 | 2.4.62-1.amzn2023 | amazonlinux | 81 k |
| libbrotli | x86_64 | 1.0.9-4.amzn2023.0.2 | amazonlinux | 315 k |
| libsodium | x86_64 | 1.0.19-4.amzn2023 | amazonlinux | 176 k |
| libxslt | x86_64 | 1.1.34-5.amzn2023.0.2 | amazonlinux | 241 k |
| mod_wsgi | noarch | 2.1.49-2.amzn2023.0.3 | amazonlinux | 33 k |

Step 4: Update and install the required packages

Use the following commands:

sudo yum update

sudo yum install httpd php

sudo yum install gcc glibc glibc-common

sudo yum install gd gd-devel

```
[ec2-user@ip-172-31-33-14 ~]$ sudo yum install gcc glibc glibc-common
Last metadata expiration check: 0:20:32 ago on Thu Sep 26 08:42:17 2024.
Package glibc-2.34-52.amzn2023.0.11.x86_64 is already installed.
Package glibc-common-2.34-52.amzn2023.0.11.x86_64 is already installed.
Dependencies resolved.
```

| Package | Architecture | Version | Repository | Size |
|---------------------------------|--------------|--------------------------|-------------|-------|
| Installing: | | | | |
| gcc | x86_64 | 11.4.1-2.amzn2023.0.2 | amazonlinux | 32 M |
| Installing dependencies: | | | | |
| annobin-docs | noarch | 10.93-1.amzn2023.0.1 | amazonlinux | 92 k |
| annobin-plugin-gcc | x86_64 | 10.93-1.amzn2023.0.1 | amazonlinux | 887 k |
| cpp | x86_64 | 11.4.1-2.amzn2023.0.2 | amazonlinux | 10 M |
| gc | x86_64 | 8.0.4-5.amzn2023.0.2 | amazonlinux | 105 k |
| glibc-devel | x86_64 | 2.34-52.amzn2023.0.11 | amazonlinux | 27 k |
| glibc-headers-x86 | noarch | 2.34-52.amzn2023.0.11 | amazonlinux | 427 k |
| guile22 | x86_64 | 2.2.7-2.amzn2023.0.3 | amazonlinux | 6.4 M |
| kernel-headers | x86_64 | 6.1.109-118.189.amzn2023 | amazonlinux | 1.4 M |
| libomp | x86_64 | 1.2.1-2.amzn2023.0.2 | amazonlinux | 62 k |
| libtool-ltdl | x86_64 | 2.4.7-1.amzn2023.0.3 | amazonlinux | 38 k |
| libxml2-devel | x86_64 | 4.4.33-7.amzn2023 | amazonlinux | 32 k |

```
[ec2-user@ip-172-31-33-14 ~]$ sudo yum install gd gd-devel
Last metadata expiration check: 0:21:27 ago on Thu Sep 26 08:42:17 2024.
Dependencies resolved.
```

| Package | Architecture | Version | Repository | Size |
|---------------------------------|--------------|-------------------------|-------------|-------|
| Installing: | | | | |
| gd | x86_64 | 2.3.3-5.amzn2023.0.3 | amazonlinux | 139 k |
| gd-devel | x86_64 | 2.3.3-5.amzn2023.0.3 | amazonlinux | 38 k |
| Installing dependencies: | | | | |
| brotli | x86_64 | 1.0.9-4.amzn2023.0.2 | amazonlinux | 314 k |
| brotli-devel | x86_64 | 1.0.9-4.amzn2023.0.2 | amazonlinux | 31 k |
| bzip2-devel | x86_64 | 1.0.8-6.amzn2023.0.2 | amazonlinux | 214 k |
| cairo | x86_64 | 1.17.6-2.amzn2023.0.1 | amazonlinux | 684 k |
| cmake-filesystem | x86_64 | 3.22.2-1.amzn2023.0.4 | amazonlinux | 16 k |
| fontconfig | x86_64 | 2.13.94-2.amzn2023.0.2 | amazonlinux | 273 k |
| fontconfig-devel | x86_64 | 2.13.94-2.amzn2023.0.2 | amazonlinux | 128 k |
| fnts-filesystem | noarch | 1:2.0.5-12.amzn2023.0.2 | amazonlinux | 9.5 k |
| freetype | x86_64 | 2.12.3-5.amzn2023.0.1 | amazonlinux | 422 k |

Step 5: Create a new nagios user by writing the following commands

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

```
Complete!  
[ec2-user@ip-172-31-33-14 ~]$ sudo adduser -m nagios  
[ec2-user@ip-172-31-33-14 ~]$ sudo passwd nagios  
Changing password for user nagios.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[ec2-user@ip-172-31-33-14 ~]$ █
```

Step 6: Create a new user group using **sudo groupadd nagcmd** and

Add users to the group using the following commands:

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

```
Complete!  
[ec2-user@ip-172-31-33-14 ~]$ sudo adduser -m nagios  
[ec2-user@ip-172-31-33-14 ~]$ sudo passwd nagios  
Changing password for user nagios.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[ec2-user@ip-172-31-33-14 ~]$ sudo groupadd nagcmd  
[ec2-user@ip-172-31-33-14 ~]$ sudo usermod -a -G nagcmd nagios  
[ec2-user@ip-172-31-33-14 ~]$ sudo usermod -a -G nagcmd apache  
[ec2-user@ip-172-31-33-14 ~]$ mkdir downloads  
[ec2-user@ip-172-31-33-14 ~]$ cd downloads  
[ec2-user@ip-172-31-33-14 downloads]$ wget https://sourceforge.net/projects/nagios/files/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz/download?use_mirror=excellmedia  
--2024-09-26 09:15:54-- https://sourceforge.net/projects/nagios/files/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz/download?use_mirror=excellmedia  
a  
Resolving sourceforge.net (sourceforge.net)... 172.64.150.145, 104.18.37.111, 2606:4700:4400::6812:256f, ...  
Connecting to sourceforge.net (sourceforge.net)|172.64.150.145|:443... connected.  
HTTP request sent, awaiting response... 302 Found  
Location: https://downloads.sourceforge.net/project/nagios/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz?ts=gAAAAABm9S2KLFW7LwD1QAJ2jNzqmSJwAPA1mQ-eAYK8z5Nmrv ifVkhbsV-qOfPsLUyICC6yvdHu6UeeIyvNzsVGUTir9BeQ%3D%3D&use_mirror=excellmedia&r= [following]
```

Step 7: Create a directory for Nagios downloads using the following commands-

Commands -

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

Also download Nagios and plugin source files

Commands -

```
wget  
https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz  
wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz
```

```

Connecting to prdownloads.sourceforge.net (prdownloads.sourceforge.net)|204.68.111.105|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz [following]
--2024-09-26 09:38:43-- https://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz
Resolving downloads.sourceforge.net (downloads.sourceforge.net)... 204.68.111.105
Connecting to downloads.sourceforge.net (downloads.sourceforge.net)|204.68.111.105|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://excellmedia.dl.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz?viasf=1 [following]
--2024-09-26 09:38:45-- https://excellmedia.dl.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz?viasf=1
Resolving excellmedia.dl.sourceforge.net (excellmedia.dl.sourceforge.net)... 202.153.32.19, 2401:fb00:0:1fe:8000::5
Connecting to excellmedia.dl.sourceforge.net (excellmedia.dl.sourceforge.net)|202.153.32.19|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1805059 (1.7M) [application/x-gzip]
Saving to: 'nagios-4.0.8.tar.gz'

nagios-4.0.8.tar.gz          100%[=====] 1.72M 8.14MB/s   in 0.2s

2024-09-26 09:38:45 (8.14 MB/s) - 'nagios-4.0.8.tar.gz' saved [1805059/1805059]

[ec2-user@ip-172-31-33-14 downloads]$ ls
'download?use_mirror=excellmedia'  nagios-4.0.8.tar.gz
[ec2-user@ip-172-31-33-14 downloads]$ tar -xzf nagios-4.0.8.tar.gz
[ec2-user@ip-172-31-33-14 downloads]$ []

```

Step 8-Extract the nagios source file with the following commands

tar zxvf nagios-4.4.6.tar.gz

cd nagios-4.4.6

Then run the configuration script with the following command

/configure --with-command-group=nagcmd

```

Nagios user/group: nagios,nagios
Command user/group: nagios,nagcmd
Event Broker: yes
Install ${prefix}: /usr/local/nagios
Install ${includedir}: /usr/local/nagios/include/nagios
Lock file: ${prefix}/var/nagios.lock
Check result directory: ${prefix}/var/spool/checkresults
Init directory: /etc/rc.d/init.d
Apache conf.d directory: /etc/httpd/conf.d
Mail program: /bin/mail
Host OS: linux-gnu
IOBroker Method: epoll

```

Web Interface Options:

```

-----  

HTML URL: http://localhost/nagios/  

CGI URL: http://localhost/nagios/cgi-bin/  

Traceroute (used by WAP): /usr/bin/traceroute

```

Review the options above for accuracy. If they look okay,
type 'make all' to compile the main program and CGIs.

```
[ec2-user@ip-172-31-33-14 nagios-4.0.8]$ ]
```

Step 9-Compile the source code with the following commands
make all

```
[ec2-user@ip-172-31-33-14 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(DEBUGL_CHECKS, 1, "Found specialized worker(s) for '%s'", (slash && *slash != '/') ? slash : cmd name);
    |         ^~~~~~
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o checks.o checks.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o config.o config.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o commands.o commands.c
commands.c: In function 'process_passive_service_check':
commands.c:2247:19: warning: assignment discards 'const' qualifier from pointer target type [-Wdiscarded-qualifiers]
```

Step 10-Install binaries,init script and sample config files

Commands -

./sudo make install

sudo make install-init

sudo make install-config

sudo make install-commandmode

```
*** Config files installed ***

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

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

*** External command directory configured ***

[ec2-user@ip-172-31-33-14 nagios-4.0.8]$ ]
```

Step 11-Edit the Config File to Change the Email Address

Commands -

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

- Change the email address in the contacts.cfg file to your preferred email

Step 12-Configure the Web Interface

Commands -

sudo make install-webconf

```

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

    email                nagios@localhost ; <<***** CHANGE THIS TO YOUR EMAIL ADDRESS *****

}

# we only have one contact in this simple configuration file, so there is

```

File: /usr/local/nagios/etc/objects/contacts.cfg

Step 13-Create a Nagios Admin Account

Commands -

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

- You will be prompted to enter and confirm the password for the nagiosadmin user

```

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

    email                vaishnal16305@gmail.com ; <<***** CHANGE THIS TO YOUR EMAIL ADDRESS *****

}

# we only have one contact in this simple configuration file, so there is

```

File: /usr/local/nagios/etc/objects/contacts.cfg

Step 14-. Extract the Plugins Source File

Commands -

cd ~/downloads

tar zxvf nagios-plugins-2.3.3.tar.gz

cd nagios-plugins-2.3.3

```

*** External command directory configured ***

[ec2-user@ip-172-31-33-14 nagios-4.0.8]$ sudo nano /usr/local/nagios/etc/objects/contacts.cfg
[ec2-user@ip-172-31-33-14 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 ***

```

Step 15-19. Compile and Install Plugins

Commands -

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

```
make
```

```
sudo make install
```

```
[ec2-user@ip-172-31-33-14 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
```

Step 16-Start Nagios

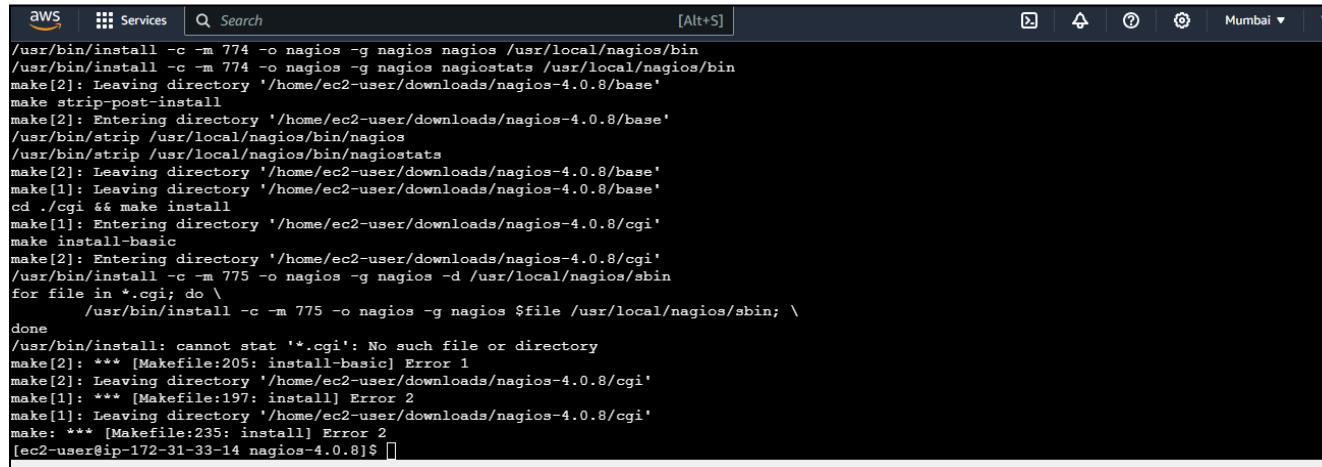
Commands -

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

```
sudo chkconfig nagios on
```

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

```
sudo systemctl start nagios
```



```
/usr/bin/install -c -m 774 -o nagios -g nagios nagios /usr/local/nagios/bin
/usr/bin/install -c -m 774 -o nagios -g nagios nagiosstats /usr/local/nagios/bin
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-4.0.8/base'
make strip-post-install
make[2]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/base'
/usr/bin/strip /usr/local/nagios/bin/nagios
/usr/bin/strip /usr/local/nagios/bin/nagiosstats
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-4.0.8/base'
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-4.0.8/base'
cd ./cgi && make install
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/cgi'
make install-basic
make[2]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/cgi'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/sbin
for file in *.cgi; do \
    /usr/bin/install -c -m 775 -o nagios -g nagios $file /usr/local/nagios/sbin; \
done
/usr/bin/install: cannot stat '*.cgi': No such file or directory
make[2]: *** [Makefile:205: install-basic] Error 1
make[2]: Leaving directory '/home/ec2-user/downloads/nagios-4.0.8/cgi'
make[1]: *** [Makefile:197: install] Error 2
make[1]: Leaving directory '/home/ec2-user/downloads/nagios-4.0.8/cgi'
make: *** [Makefile:235: install] Error 2
[ec2-user@ip-172-31-33-14 nagios-4.0.8]$
```

Step 17-Access Nagios Web Interface

- Copy the Public IP address of your EC2 instance.
- Open your browser and navigate to <http://nagios>.
- Enter the username nagiosadmin and the password you set in Step 16.

Nagios® Core™



Unable to get process status

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

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

General

- [Home](#)
- [Documentation](#)

Current Status

- [Tactical Overview](#)
- [Map \(Legacy\)](#)
- [Hosts](#)
- [Services](#)
- [Host Groups](#)
 - [Summary](#)
 - [Grid](#)
- [Service Groups](#)
 - [Summary](#)
 - [Grid](#)
- Problems**
- [Services \(Unhandled\)](#)
- [Hosts \(Unhandled\)](#)
- [Network Outages](#)

Quick Search:

Reports

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

Get Started

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

Quick Links

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

Latest News

Don't Miss...

ADVANCE DEVOPS EXPERIMENT 10

Name: Vaishnal Dilip Mali

Class: D15A

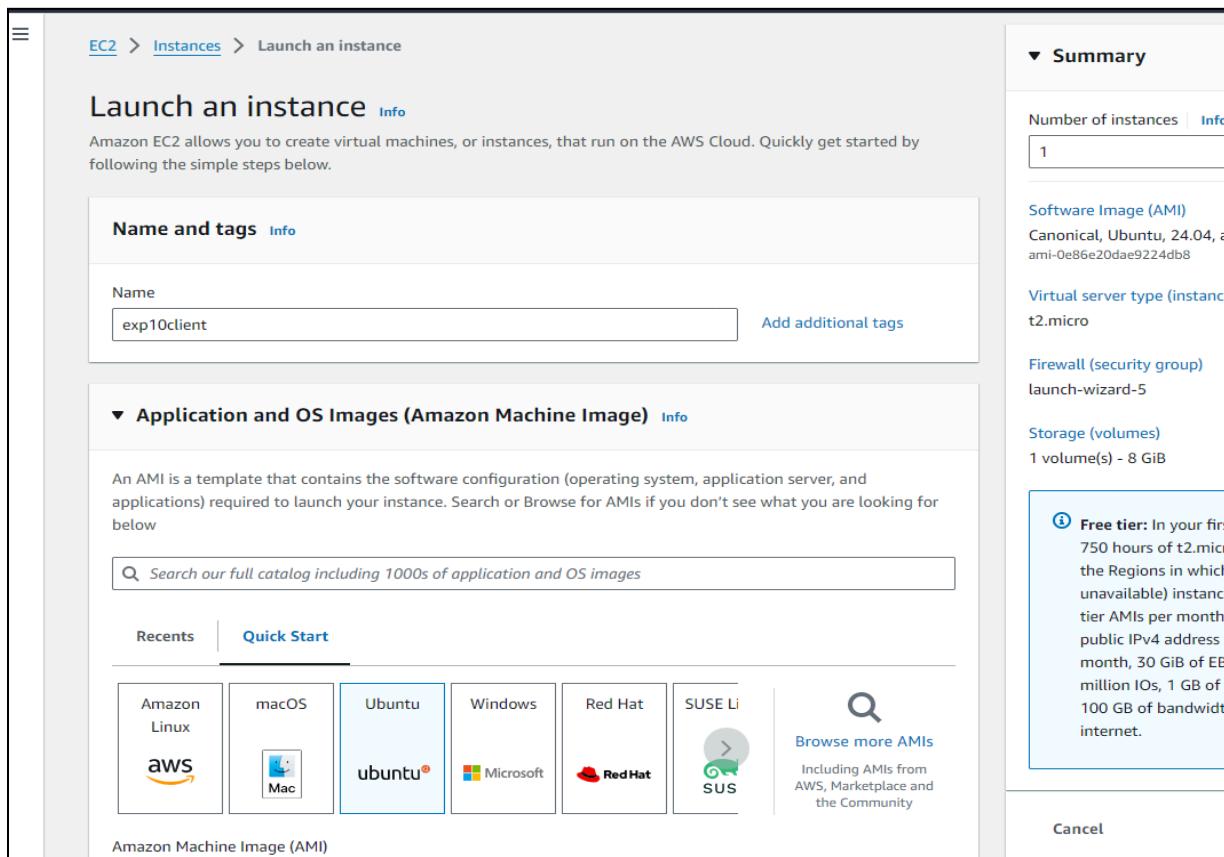
Roll No: 27

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

1) Launch an instance

Launch an ec2 instance.

Select Ubuntu as the os give a meaningful name of the instance.



Select the same security group as given in exp9.

▼ 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

Recents [Quick Start](#)

[Browse more AMIs](#) Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-0e86e20dae9224db8 (64-bit (x86)) / ami-096ea6a12ea24a797 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description
Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Architecture: 64-bit (x86) ▾ AMI ID: ami-0e86e20dae9224db8 Username: ubuntu Verified provider

▼ Summary

Number of instances: 1

Software Images: Canonical, Ubuntu, Red Hat, SUSE Linux

Virtual server type: t2.micro

Firewall (security group): launch-wizard-1

Storage (volume): 1 volume(s) - 8 GB

Free tier: 750 hours in the Region, unavailability tier AMI, public IP per month, million API requests, 100 GB internet bandwidth

[Cancel](#)

Make sure to select the same key-pair login used in the exp9 machine.

Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

[Create new key pair](#)

Network settings [Info](#)

[Edit](#)

Network [Info](#)
vpc-07b6966cbfba88ee3

Subnet [Info](#)
No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of [free tier allowance](#)

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Common security groups [Info](#)

Select security groups [▼](#)

Software Canonical, ami-0e86e20

Virtual service t2.micro

Firewall (security group) launch-wiz

Storage (volume) 1 volume(s)

Free tier 750 hours the unanticipated tier public monitoring mill 100 integrated

Cancel

click on launch instance.

Now connect with this client machine using the ssh through your terminal(open a new terminal in your local machine and we will need both of the terminals open)

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS |
|------------------|---------------------|----------------------|---------------|--------------------------------|-------------------------------|-------------------|-------------------------|
| Master | i-0ab175e9c60cc3a23 | Running | t2.micro | 2/2 checks passed | View alarms + | us-east-1b | ec2-3-82-156-160.com... |
| node-1 | i-08ad30b7114767ca2 | Running | t2.micro | 2/2 checks passed | View alarms + | us-east-1b | ec2-3-85-110-80.comp... |
| node-2 | i-03c70d364fb762af5 | Running | t2.micro | 2/2 checks passed | View alarms + | us-east-1b | ec2-54-226-209-38.co... |
| nagios_host_e... | i-0820376be204a7fcf | Running | t2.micro | 2/2 checks passed | View alarms + | us-east-1b | ec2-54-224-175-95.co... |
| exp10client | i-0994ca5a178801a54 | Running | t2.micro | Initializing | View alarms + | us-east-1b | ec2-54-173-58-143.co... |

EC2 > Instances > i-0994ca5a178801a54 > Connect to instance

Connect to instance Info

Connect to your instance i-0994ca5a178801a54 (exp10client) using any of these options

EC2 Instance Connect | Session Manager | **SSH client** | EC2 serial console

Instance ID
i-0994ca5a178801a54 (exp10client)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is nagios_exp_9.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 "nagios_exp_9.pem"
4. Connect to your instance using its Public DNS:
ec2-54-173-58-143.compute-1.amazonaws.com

Command copied

ssh -i "nagios_exp_9.pem" ubuntu@ec2-54-173-58-143.compute-1.amazonaws.com

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

Cancel

Note to change the path of the .pem file.

```
Host Client
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\Lenovo> ssh -i "C:\Users\Lenovo\Downloads\nagios_exp_9.pem" ubuntu@ec2-54-173-58-143.compute-1.amazonaws.com

The authenticity of host 'ec2-54-173-58-143.compute-1.amazonaws.com (54.173.58.143)' can't be established.
ED25519 key fingerprint is SHA256:IA3XH7f011spk084wDcZFmqRgNn0iJZ7itI2pBMmHP4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-173-58-143.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1012-aws x86_64)

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

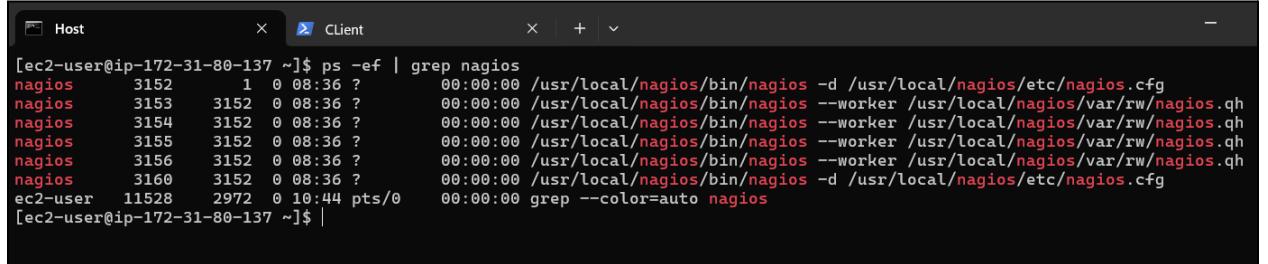
System information as of Sat Sep 28 10:43:28 UTC 2024

System load:  0.01      Processes:          107
Usage of /:   22.8% of 6.71GB  Users logged in:     0
Memory usage: 19%           IPv4 address for enX0: 172.31.82.77
```

2) Go to nagios host machine (Host machine)

Perform the following commands

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



```
[ec2-user@ip-172-31-80-137 ~]$ ps -ef | grep nagios
nagios    3152     1  0 08:36 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios    3153   3152  0 08:36 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios    3154   3152  0 08:36 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios    3155   3152  0 08:36 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios    3156   3152  0 08:36 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios    3160   3152  0 08:36 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
ec2-user  11528  2972  0 10:44 pts/0    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-80-137 ~]$
```

```
sudo su
```

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

```
[root@ip-172-31-80-137 ec2-user]# mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
[root@ip-172-31-80-137 ec2-user]# ls
```

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

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

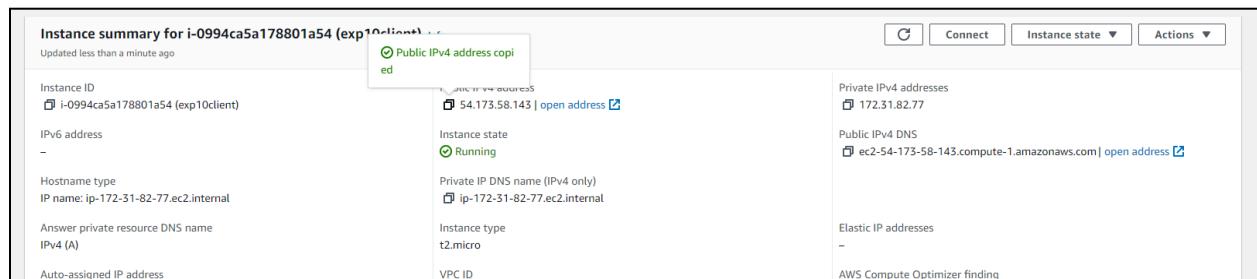
```
[root@ip-172-31-80-137 ec2-user]# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
```

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

```
[root@ip-172-31-80-137 ec2-user]# nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
```

Change hostname and alias to linuxserver

Change address to public ip address of client instance (Ubuntu instance) you can get the ip address by clicking on the instance id on the instances section there you will get the public ipv4 address



```

# HOST DEFINITION
#
#####
# Define a host for the local machine

define host {
    use          linux-server           ; Name of host template to use
                                         ; This host definition will in>
                                         ; in (or inherited by) the lin>
    host_name    linuxserver
    alias        linuxserver
    address     54.173.58.143
}

```

Change hostgroup_name to linux-servers1

```

# Define an optional hostgroup for Linux machines

define hostgroup {
    hostgroup_name      linux-servers1      ; The name of the hostgroup
    alias               Linux Servers        ; Long name of the group
    members             localhost           ; Comma separated list of host>
}
|
```

Change the occurrences of hostname further in the document from localhost to linuxserver
example like:

| | |
|------------------|------------------|
| host_name | localhost |
|------------------|------------------|

changed to

| | | |
|----------------------------|---------------------------------------|-----------------------------------|
| define service { | local-service | ; Name of service template |
| use | linuxserver | |
| host_name | | |
| service_description | PING | |
| check_command | check_ping!100.0,20%!500.0,60% | |

This is the last one

```

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

```

now ctrl+O and enter to save and then ctrl+X for exiting.
 Open nagios configuration file and add the line shown below
 nano /usr/local/nagios/etc/nagios.cfg

```
[root@ip-172-31-80-137 ec2-user]# nano /usr/local/nagios/etc/nagios.cfg
```

##Add this line below the opened nano interface where similar lines are commented.

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

```

GNU nano 5.8                               /usr/local/nagios/etc/nagios.cfg
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

# You can specify individual object config files as shown below:
:cfg_file=/usr/local/nagios/etc/objects/commands.cfg
:cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
:cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
:cfg_file=/usr/local/nagios/etc/objects/templates.cfg

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

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

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

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

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

:cfg_dir=/usr/local/nagios/etc/servers
:cfg_dir=/usr/local/nagios/etc/printers
:cfg_dir=/usr/local/nagios/etc/switches
:cfg_dir=/usr/local/nagios/etc/routers
:cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/

# OBJECT CACHE FILE
# This option determines where object definitions are cached when
# Nagios starts/restarts. The SCIs read object definitions from
# the cache instead of reading them from disk.
:cache_dir=/tmp/nagios_cache

```

ctrl+o and enter for saving and ctrl+x to exit nano editor.

Verify configuration files

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

```
[root@ip-172-31-80-137 ec2-user]# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

```
Nagios Core 4.5.5
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2024-09-17
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 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-172-31-80-137 ec2-user]# |
```

Restart nagios service.

```
service nagios restart
```

```
Things look okay - No serious problems were detected during the pre-flight check
[root@ip-172-31-80-137 ec2-user]# service nagios restart
Redirecting to /bin/systemctl restart nagios.service
[root@ip-172-31-80-137 ec2-user]# |
```

- 3) Go to client machine (ubuntu machine)

Perform the following commands

```
sudo apt update -y
```

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

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

```
ubuntu@ip-172-31-82-77:~$ sudo apt update -y
sudo apt install gcc -y
sudo apt install -y nagios-nrpe-server nagios-plugins
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]

Running kernel seems to be up-to-date.

Restarting services...

Service restarts being deferred:
/etc/needrestart/restart.d/dbus.service
systemctl restart getty@tty1.service
systemctl restart networkd-dispatcher.service
systemctl restart serial-getty@ttyS0.service
systemctl restart systemd-logind.service
systemctl restart unattended-upgrades.service

No containers need to be restarted.

User sessions running outdated binaries:
ubuntu @ session #1: sshd[990,1101]
ubuntu @ user manager service: systemd[996]

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-82-77:~$ |
```

Open the nrpe.cfg file in nano editor

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

Under allowed_hosts, add the nagios host ip address (public)

```
# You can either supply a username or a UID.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd.
nrpe_user=nagios

#
# NRPE GROUP
# This determines the effective group that the NRPE daemon should run as.
# You can either supply a group name or a GID.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd.
nrpe_group=nagios

#
# ALLOWED HOST ADDRESSES
# This is an optional comma-delimited list of IP address or hostnames
# that are allowed to talk to the NRPE daemon. Network addresses with a bit
# (i.e. 192.168.1.0/24) are also supported. Hostname wildcards are not currently
# supported.
#
# Note: The daemon only does rudimentary checking of the client's IP
# address. I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd.
allowed_hosts=127.0.0.1,54.224.175.95

#
# COMMAND ARGUMENT PROCESSING
# This option determines whether or not the NRPE daemon will allow clients
```

again save and exit the nano editor.

4) Go to nagios dashboard and click on hosts

The screenshot shows the Nagios Core dashboard. On the left, there's a sidebar with links for General, Current Status, Problems, Reports, and System. The 'Current Status' section is expanded, showing links for Tactical Overview, Map, Hosts, Services, Host Groups, and Service Groups. The main content area features the Nagios Core logo and a message indicating the daemon is running with PID 13935. Below this, it displays 'Nagios® Core™ Version 4.5.5' and the date 'September 17, 2024'. A 'Check for updates' button is present. The dashboard is divided into several boxes: 'Get Started' (with bullet points like 'Start monitoring your infrastructure'), 'Latest News' (empty), 'Don't Miss...' (empty), and 'Quick Links' (with links to Nagios Library, Nagios Labs, Nagios Exchange, Nagios Support, Nagios.com, and Nagios.org). At the bottom, there's a copyright notice and a 'Nagios' footer.

Click on hosts

This screenshot shows the 'Tactical Overview' page under the 'Current Status' section. It contains a sidebar with links for Hosts, Services, and Host Groups. The main area is currently empty, showing a light gray background.

5) Click on linux server

Nagios®

Current Network Status

Last Updated: Sat Sep 28 11:33:24 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.5.5 - www.nagios.org
Logged in as nagiosadmin

Host Status Totals

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

Service Status Totals

| Ok | Warning | Unknown | Critical | Pending |
|--------------|-----------|---------|----------|---------|
| 12 | 1 | 0 | 3 | 0 |
| All Problems | All Types | | | |
| 4 | 16 | | | |

Host Status Details For All Host Groups

Limit Results: 100 ▾

| Host | Status | Last Check | Duration | Status Information |
|-------------|--------|---------------------|--------------|---|
| linuxserver | UP | 09-28-2024 11:29:10 | 0d 0h 8m 36s | PING OK - Packet loss = 0%, RTA = 1.18 ms |
| localhost | UP | 09-28-2024 11:32:18 | 0d 3h 53m 7s | PING OK - Packet loss = 0%, RTA = 0.03 ms |

Results 1 - 2 of 2 Matching Hosts

Reports

- Availability
- Trends
- Alerts
- History
- Summary
- Histogram
- Notifications
- Event Log

Nagios®

General

Home Documentation

Current Status

Tactical Overview Map Hosts Services Host Groups Summary Grid Service Groups Summary Grid Problems Services (Unhandled) Hosts (Unhandled) Network Outages Quick Search:

Reports

- Availability
- Trends
- Alerts
- History
- Summary
- Histogram
- Notifications
- Event Log

System

Comments Downtime Process Info Performance Info Scheduling Queue Configuration

Host Information

Last Updated: Sat Sep 28 11:33:24 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.5.5 - www.nagios.org
Logged in as nagiosadmin

Host
linuxserver
(linuxserver)

Member of
No hostgroups

54.173.58.143

Host State Information

| | |
|-------------------------------------|---|
| Host Status: | UP (for 0d 0h 8m 51s) |
| Status Information: | PING OK - Packet loss = 0%, RTA = 1.18 ms |
| Performance Data: | rta=1.18400ms;3000.000000;5000.000000;0.000000 pl=0%;80,100,100 |
| Current Attempt: | 1/10 (HARD state) |
| Last Check Time: | 09-28-2024 11:29:10 |
| Check Type: | ACTIVE |
| Check Latency / Duration: | 0.00 - 0.005 seconds |
| Next Scheduled Active Check: | 09-28-2024 11:34:10 |
| Last State Change: | 09-28-2024 11:24:48 |
| Last Notification: | N/A (notification 0) |
| Is This Host Flapping? | NO (0.00% state change) |
| In Scheduled Downtime? | NO |
| Last Update: | 09-28-2024 11:33:37 (0d 0h 0m 2s ago) |

Host Commands

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

Host Comments

Add a new comment

| Entry Time | Author | Comment | Comment ID | Persistent | Type | Expires | Actions |
|--|--------|---------|------------|------------|------|---------|---------|
| This host has no comments associated with it | | | | | | | |

6) Click on nagios services

Documentation

Current Status

Tactical Overview

Map

Hosts

Services

Host Groups

 Summary

 Grid

Service Groups

Nagios*

Current Network Status

Last Updated Sat Sep 29 11:33:58 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.5.5 - www.nagios.org
Logged in as [nagiosadmin](#)

General

- [Home](#)
- [Documentation](#)

Current Status

Tactical Overview

Map

Hosts

Services

Host Groups

 Summary

 Grid

Service Groups

Host Status Totals

| | | | |
|----|------|-------------|---------|
| Up | Down | Unreachable | Pending |
| 2 | 0 | 0 | 0 |

All Problems All Types

| | |
|---|---|
| 0 | 2 |
|---|---|

Service Status Totals

| | | | | |
|----|---------|---------|----------|---------|
| Ok | Warning | Unknown | Critical | Pending |
| 12 | 1 | 0 | 3 | 0 |

All Problems All Types

| | |
|---|----|
| 4 | 16 |
|---|----|

Service Status Details For All Hosts

Limit Results: 100

| Host | Service | Status | Last Check | Duration | Attempt | Status Information |
|-----------------|---|--|---------------------|---------------|--|---|
| linuxserver | Current Load | OK | 09-28-2024 11:30:25 | 0d 0h 8m 33s | 1/4 | OK - load average: 0.01, 0.00, 0.00 |
| | Current Users | OK | 09-28-2024 11:31:03 | 0d 0h 7m 55s | 1/4 | USERS OK - 2 users currently logged in |
| localhost | HTTP | CRITICAL | 09-28-2024 11:29:40 | 0d 0h 4m 18s | 4/4 | connect to address 54.173.58.143 and port 80: Connection refused |
| | PING | OK | 09-28-2024 11:32:18 | 0d 0h 6m 40s | 1/4 | PING OK - Packet loss = 0%, RTA = 1.03 ms |
| | Root Partition | OK | 09-28-2024 11:32:55 | 0d 0h 6m 3s | 1/4 | DISK OK - free space / 6105 MB (75.23% inode=98%) |
| | SSH | CRITICAL | 09-28-2024 11:33:33 | 0d 0h 5m 25s | 1/4 | SSH OK - OpenSSH_9.6p1 Ubuntu-Subuntu13.4 (protocol 2.0) |
| | Swap Usage | CRITICAL | 09-28-2024 11:32:10 | 0d 0h 1m 48s | 4/4 | SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size. |
| | Total Processes | OK | 09-28-2024 11:29:48 | 0d 0h 9m 10s+ | 1/4 | PROCS OK - 37 processes with STATE = R/Z/D/T |
| | Current Load | OK | 09-28-2024 11:29:39 | 0d 3h 53m 5s | 1/4 | OK - load average: 0.02, 0.01, 0.00 |
| | Current Users | OK | 09-28-2024 11:30:17 | 0d 3h 52m 27s | 1/4 | USERS OK - 2 users currently logged in |
| HTTP | WARNING | 09-28-2024 11:29:46 | 0d 2h 49m 12s | 4/4 | HTTP WARNING: HTTP/1.1 403 Forbidden - 319 bytes in 0.001 second response time | |
| | PING | OK | 09-28-2024 11:31:32 | 0d 3h 5m 12s | 1/4 | PING OK - Packet loss = 0%, RTA = 0.03 ms |
| | Root Partition | OK | 09-28-2024 11:32:09 | 0d 3h 50m 35s | 1/4 | DISK OK - free space / 6105 MB (75.23% inode=98%) |
| | SSH | CRITICAL | 09-28-2024 11:32:47 | 0d 3h 49m 57s | 1/4 | SSH OK - OpenSSH_9.7 (protocol 2.0) |
| | Swap Usage | CRITICAL | 09-28-2024 11:31:24 | 0d 3h 12m 34s | 4/4 | SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size. |
| Total Processes | OK | 09-28-2024 11:29:02 | 0d 3h 14m 56s | 1/4 | PROCS OK - 37 processes with STATE = R/Z/D/T | |

Results 1 - 16 of 16 Matching Services

Reports

- [Availability](#)
- [Trends](#)
- [Alerts](#)
- History
- Downtime
- Histogram

Notifications

Event Log

System

Comments

Adv. DevOps Exp. 11

Vaishnal Mali

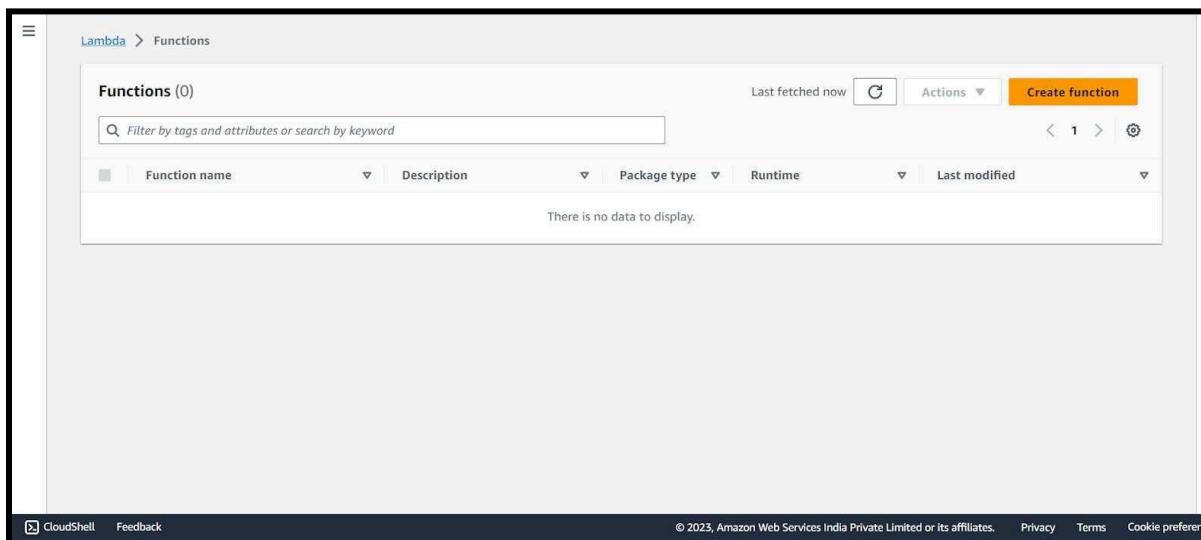
D15A - 27

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

Steps to create an AWS Lambda function

Step 1: Open up the Lambda Console and click on the Create button.

Be mindful of where you create your functions since Lambda is region-dependent.



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

Lambda > Functions > Create function

Create function Info

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

Author from scratch
Start with a simple Hello World example.

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

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

Basic information

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

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

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

Architecture Info
Choose the instruction set architecture you want for your function code.
 x86_64
 arm64

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

Lambda > Functions > Create function Info

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

Author from scratch
Start with a simple Hello World example.

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

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

Basic information

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

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

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

Architecture Info
Choose the instruction set architecture you want for your function code.
 x86_64
 arm64

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

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

Lambda > Functions > Create function

Create function Info

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

Author from scratch
Start with a simple Hello World example.

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

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

Basic information

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

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

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

Architecture Info
Choose the instruction set architecture you want for your function code.
 x86_64
 arm64

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

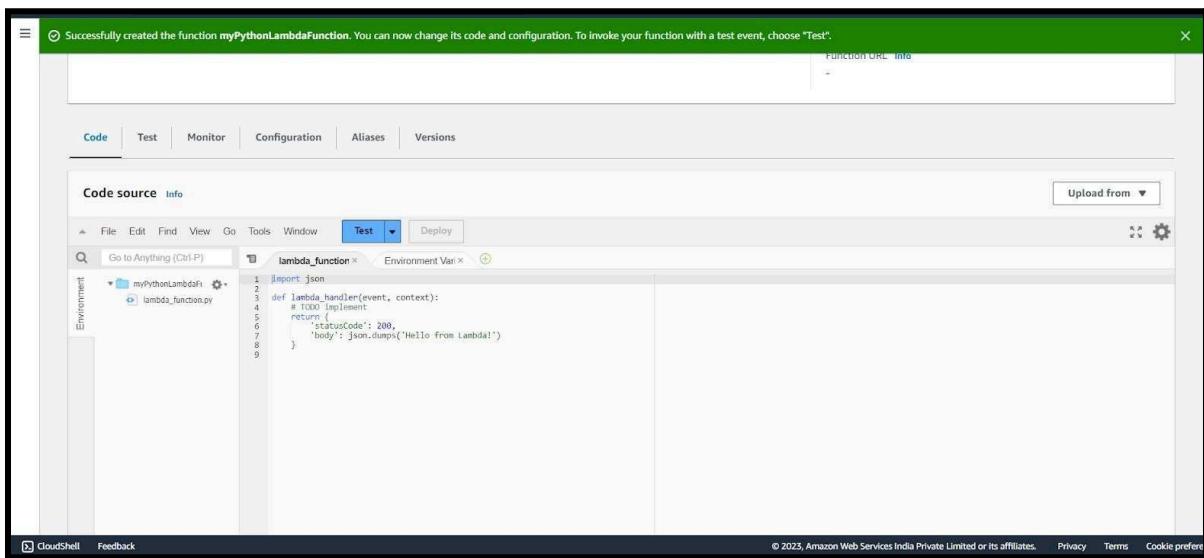
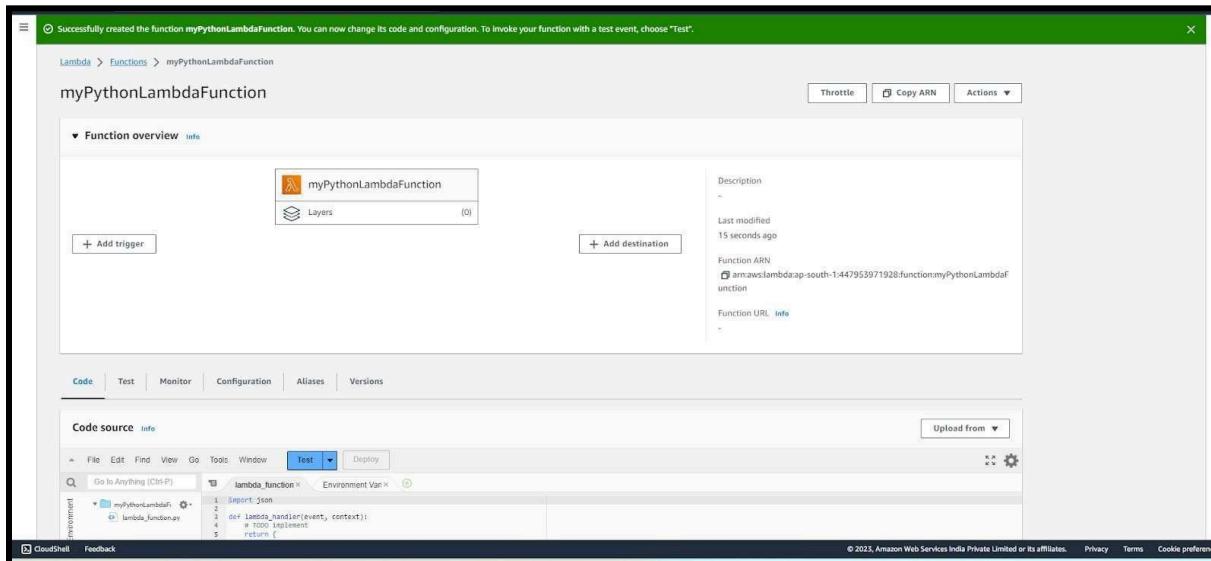
[Change default execution role](#)

[Advanced settings](#)

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

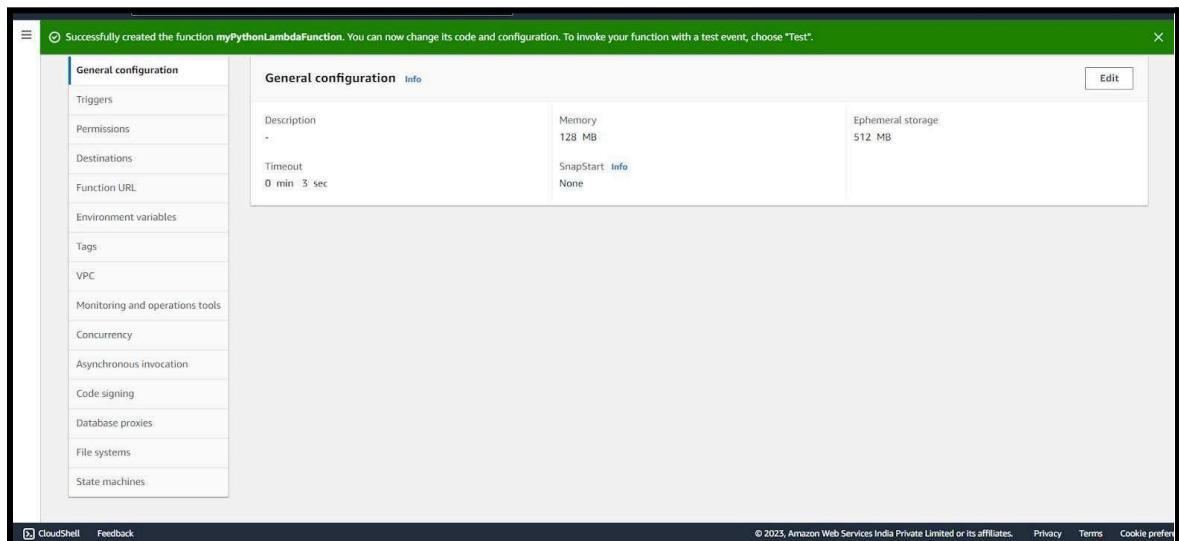
Click on the Create button.

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



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

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



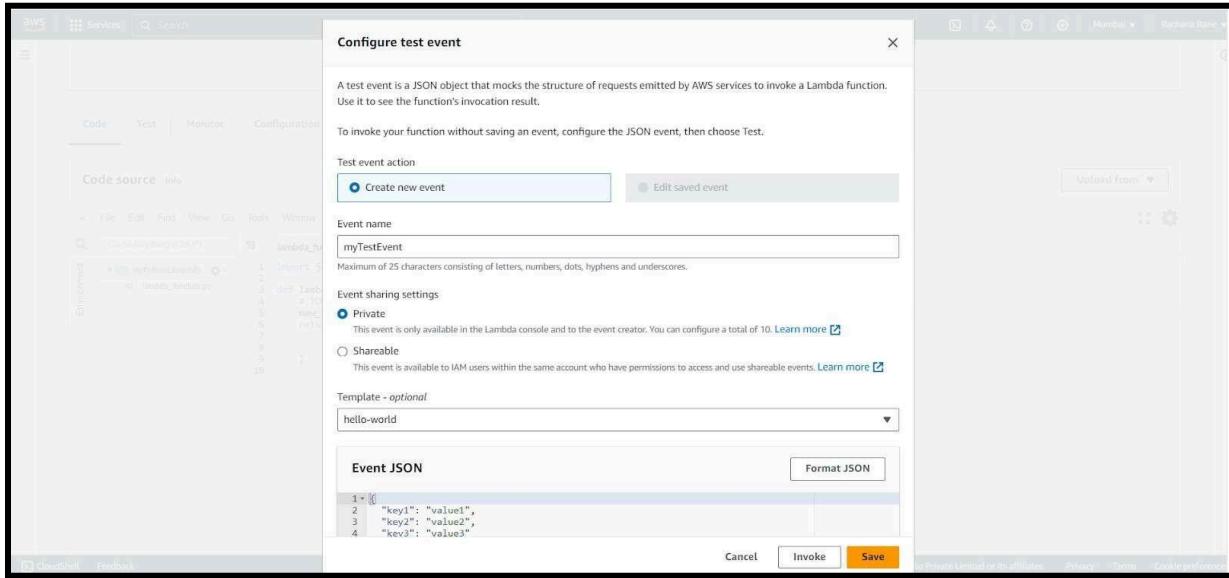
The screenshot shows the 'Edit basic settings' page for the 'myPythonLambdaFunction'. The title bar includes the AWS logo, Services menu, a search bar, and a keyboard shortcut [Alt+S]. The navigation path is Lambda > Functions > myPythonLambdaFunction > Edit basic settings. The main content area is titled 'Edit basic settings' and contains the 'Basic settings' tab. It includes fields for Description (empty), Memory (128 MB), Ephemeral storage (512 MB), SnapStart (None), and Timeout (0 min 1 sec). The 'Execution role' section is partially visible at the bottom. The footer includes CloudShell and Feedback links.

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

```
import json

def lambda_handler(event, context):
    # TODO implement
    new_string="Hello! how are you?"
    return {
        'statusCode': 200,
        'body': json.dumps('Hello from Lambda!')
    }
```

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



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

The test event myTestEvent was successfully saved.

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

Go to Anything (Ctrl-P) lambda_function Environment Var Execution result

Execution results Test Event Name myTestEvent

Response

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

Function Logs

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

Code properties Info

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

The test event myTestEvent was successfully saved.

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

Go to Anything (Ctrl-P) lambda_function Environment Var Execution result

Execution results Test Event Name myTestEvent

Response

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

Function Logs

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

Code source Info Upload from

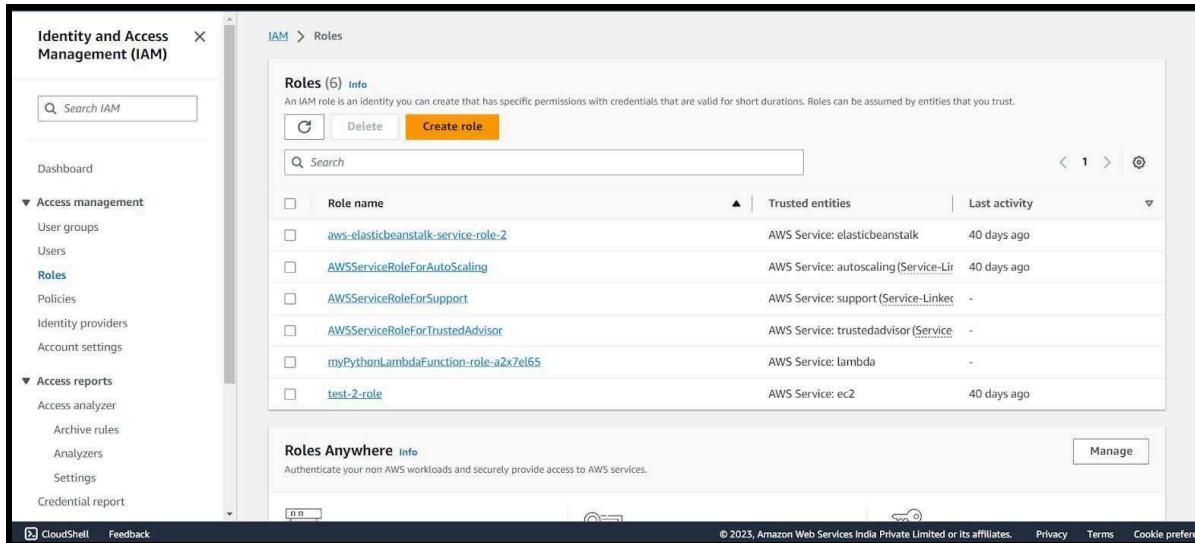
CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Adv. DevOps Exp. 12

Vaishnal Mali
D15A - 27

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

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

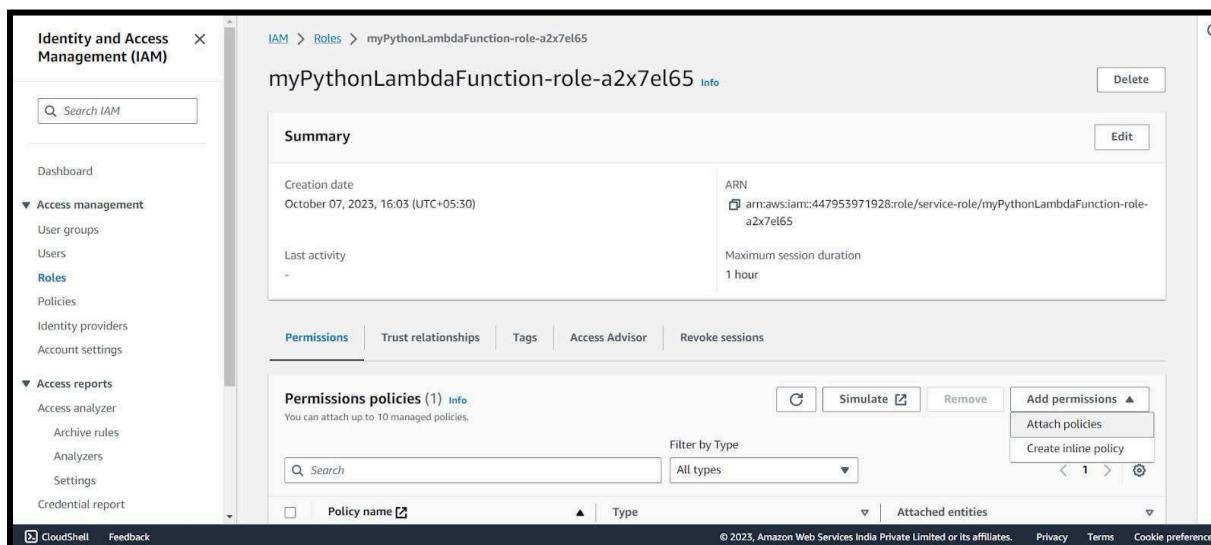


The screenshot shows the AWS IAM Roles page. On the left, there's a navigation sidebar with options like Dashboard, User groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, and Credential report. The main area is titled "Roles (6) Info" and contains a table with the following data:

| Role name | Trusted entities | Last activity |
|--------------------------------------|--|---------------|
| aws-elasticbeanstalk-service-role-2 | AWS Service: elasticbeanstalk | 40 days ago |
| AWSServiceRoleForAutoScaling | AWS Service: autoscaling (Service-Linker) | 40 days ago |
| AWSServiceRoleForSupport | AWS Service: support (Service-Linker) | - |
| AWSServiceRoleForTrustedAdvisor | AWS Service: trustedadvisor (Service-Linker) | - |
| myPythonLambdaFunction-role-a2x7el65 | AWS Service: lambda | - |
| test_2_role | AWS Service: ec2 | 40 days ago |

Below the table, there's a section titled "Roles Anywhere" with a "Manage" button.

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



The screenshot shows the "myPythonLambdaFunction-role-a2x7el65" role details page. The left sidebar is identical to the previous screenshot. The main area has a "Summary" section with information like Creation date (October 07, 2023, 16:05 (UTC+05:30)), Last activity (-), ARN (arn:aws:iam::447953971928:role/service-role/myPythonLambdaFunction-role-a2x7el65), and Maximum session duration (1 hour). Below the summary is a "Permissions" tab. The "Permissions policies" section shows one policy attached: "arn:aws:iam::447953971928:role/service-role/myPythonLambdaFunction-role-a2x7el65". There are buttons for "Add permissions" (with options for "Attach policies" and "Create inline policy"), "Simulate", and "Remove". A search bar and filter dropdown are also present.

S3-ReadOnly

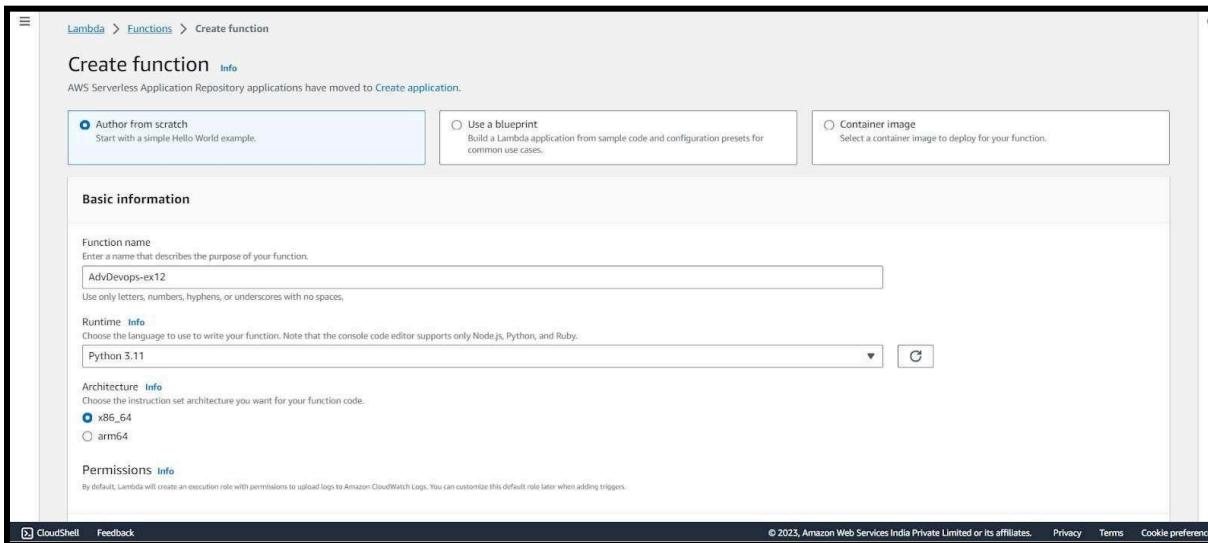
The screenshot shows the 'Add permissions' dialog in the AWS IAM console. The 'Other permissions policies' section is displayed, filtered by 'S3read'. A single policy, 'AmazonS3ReadOnlyAccess', is listed under 'AWS managed'. The description indicates it provides 'Provides read only access to all bucket...'. At the bottom right are 'Cancel' and 'Add permissions' buttons.

The screenshot shows the 'Add permissions' dialog in the AWS IAM console. The 'Other permissions policies' section is displayed, filtered by 'cloudwatchfull'. Two policies are listed under 'AWS managed': 'CloudWatchFullAccess' and 'CloudWatchFullAccessV2'. Both policies provide 'Provides full access to CloudWatch.'. At the bottom right are 'Cancel' and 'Add permissions' buttons.

CloudWatchFull

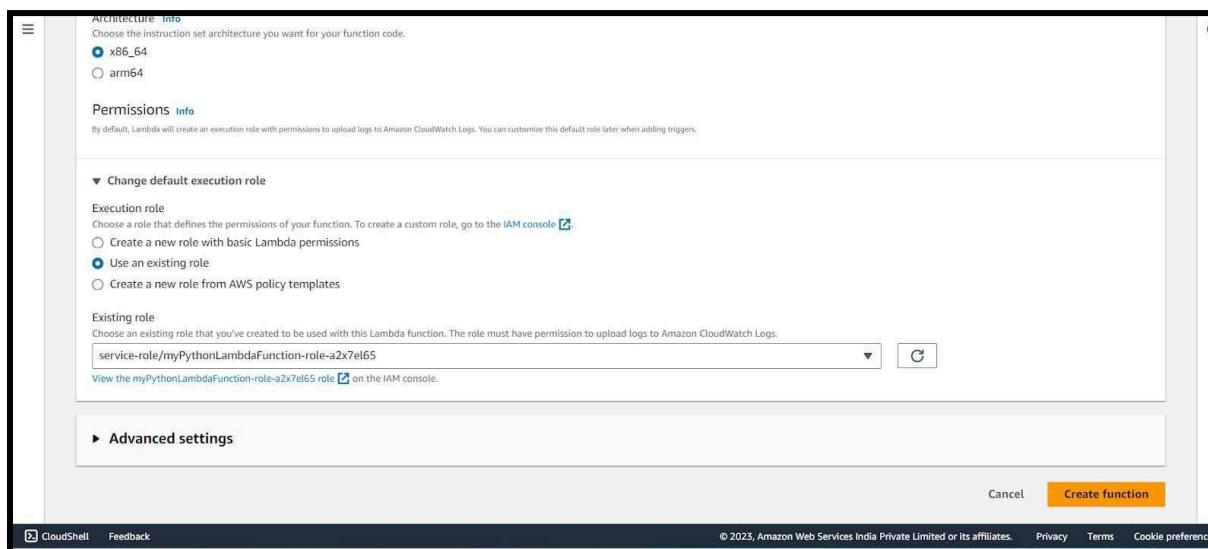
After successful attachment of policy you will see something like this you will be able to see the updated policies.

The screenshot shows the 'Permissions' tab in the AWS IAM console. A green banner at the top states 'Policy was successfully attached to role.' Below it, the 'Permissions policies' section shows three policies attached to the role: 'AmazonS3ReadOnlyAccess', 'AWSLambdaBasicExecutionRole-c4946a...', and 'CloudWatchFullAccess'. The 'Attached entities' column shows the count '1' for each. At the bottom left is a 'Permissions boundary' section labeled '(not set)'. The bottom right includes standard copyright and footer links.

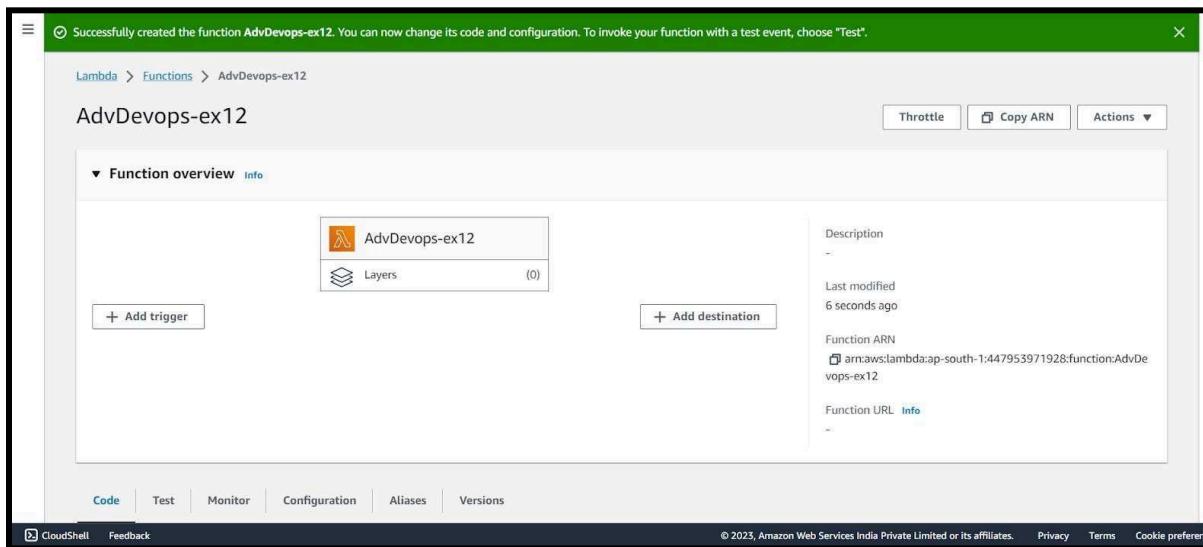


Step 3: Open up AWS Lambda and create a new Python function.

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



Step 4: The function is up and running.



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

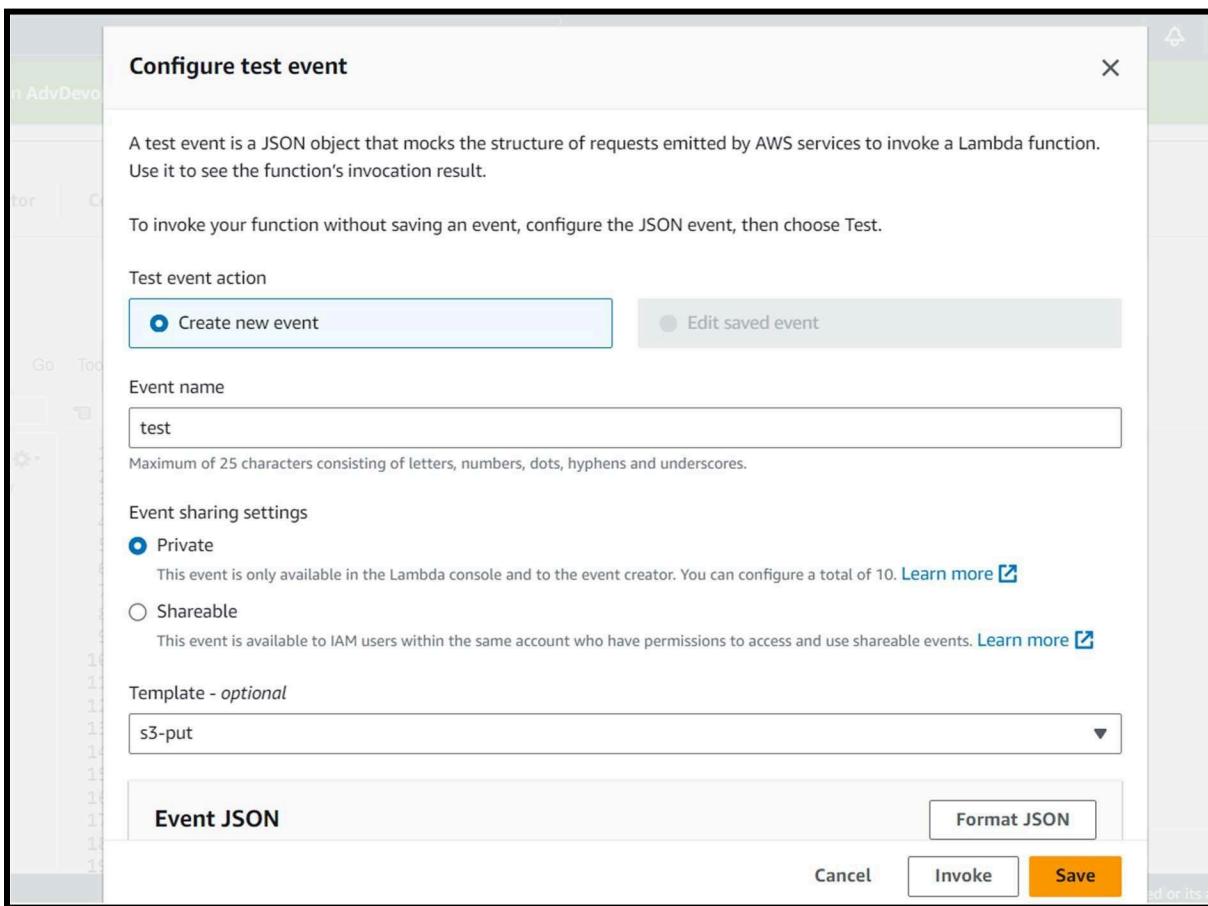
```
1 import json
2 import boto3
3 import urllib
4
5 def lambda_handler(event, context):
6
7     s3_client = boto3.client('s3')
8     bucket_name = event['Records'][0]['s3']['bucket']['name']
9     key = event['Records'][0]['s3']['object']['key']
10    key = urllib.parse.unquote_plus(key, encoding='utf-8')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

The screenshot shows the AWS Lambda code editor. The left sidebar shows the environment and a file tree with "lambda_function.py" selected. The main area displays the Python code for the lambda function. The code imports json, boto3, and urllib, defines a lambda_handler function, and processes an S3 event to log a message and print the contents of a JSON file. The status bar at the bottom indicates "18:5 Python Spaces: 4".

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

The screenshot shows the AWS Lambda console interface. At the top, a green banner indicates that the function 'AdvDevops-ex12' has been successfully created. Below the banner, there are tabs for 'Code', 'Test', 'Monitor', 'Configuration', 'Aliases', and 'Versions'. The 'Code' tab is selected. In the main area, there's a 'Code source' section with an 'Info' button. A file browser window is open, showing a folder named 'AdvDevops-ex12' containing a file 'lambda_function.py'. The code editor shows the following Python code:

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



And Save it.

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

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

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

Bucket name: AdvDevopsexp12
AWS Region: Asia Pacific (Mumbai) ap-south-1

Event notifications (0)
No event notifications
Choose Create event notification to be notified when a specific event occurs.
Create event notification

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

Transfer acceleration
Edit

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

Click on Create Event Notification.

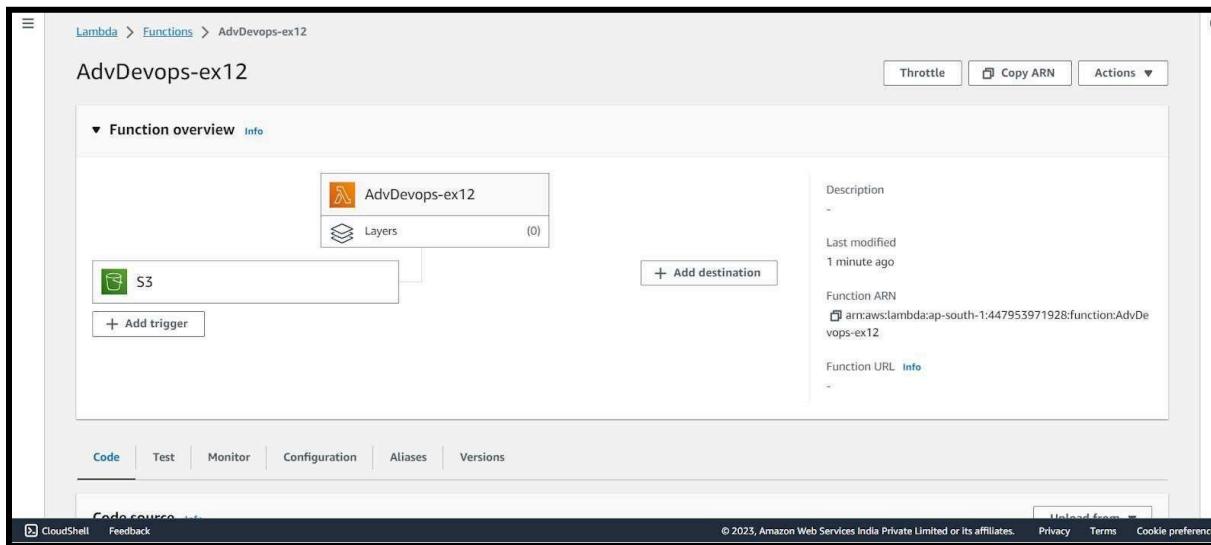
The screenshot shows the 'General configuration' section of the AWS S3 Event Notifications setup. It includes fields for 'Event name' (S3putrequest), 'Prefix - optional' (images/), and 'Suffix - optional' (.jpg). Below this, the 'Event types' section is shown, with the 'Put' option (s3:ObjectCreated:Put) checked. Other options like 'Post' (s3:ObjectCreated:Post) and 'All object create events' (s3:ObjectCreated:*) are available but unchecked. The bottom of the screen shows standard AWS navigation links (CloudShell, Feedback) and a copyright notice (© 2023, Amazon Web Services India Private Limited).

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

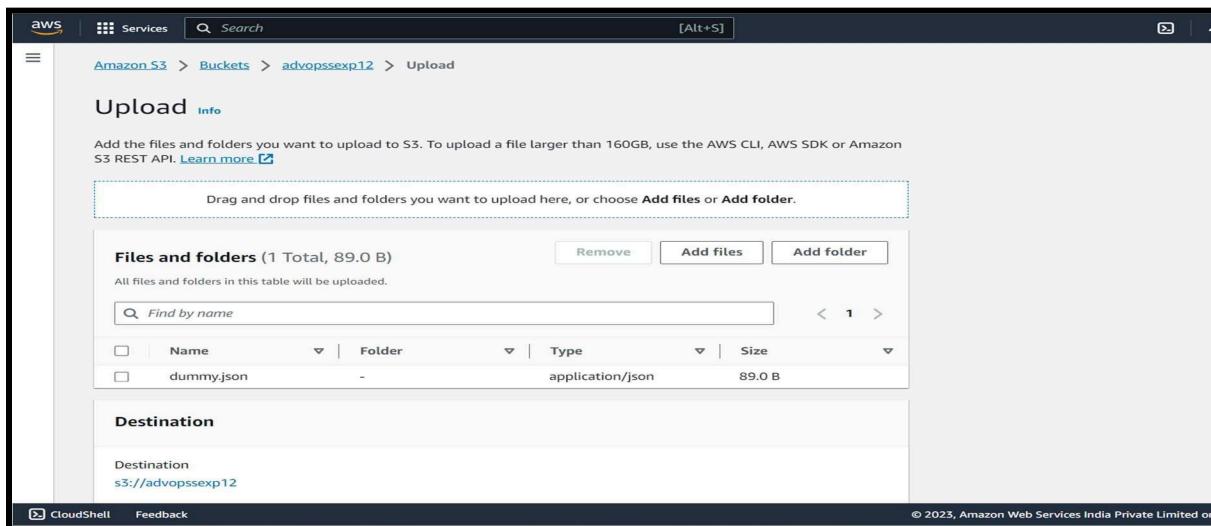
Choose Lambda function as destination and choose your lambda function and save the changes.

The screenshot shows the 'Destination' configuration step. A note states that before publishing messages, permissions must be granted to the Amazon S3 principal. It lists three destination options: 'Lambda function' (selected), 'SNS topic', and 'SQS queue'. Under 'Specify Lambda function', the option 'Choose from your Lambda functions' is selected. A dropdown menu shows the Lambda function 'AdvDevops-ex12'. At the bottom right are 'Cancel' and 'Save changes' buttons.

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



Step 12: Go back to your S3 Bucket and click on Add Files to upload a new file. Select the dummy data file from



from your computer and click Upload.

Step 13: After this make the necessary changes in the Test configuration file which we created it previously by replacing the Bucket Name and the ARN of Bucket.



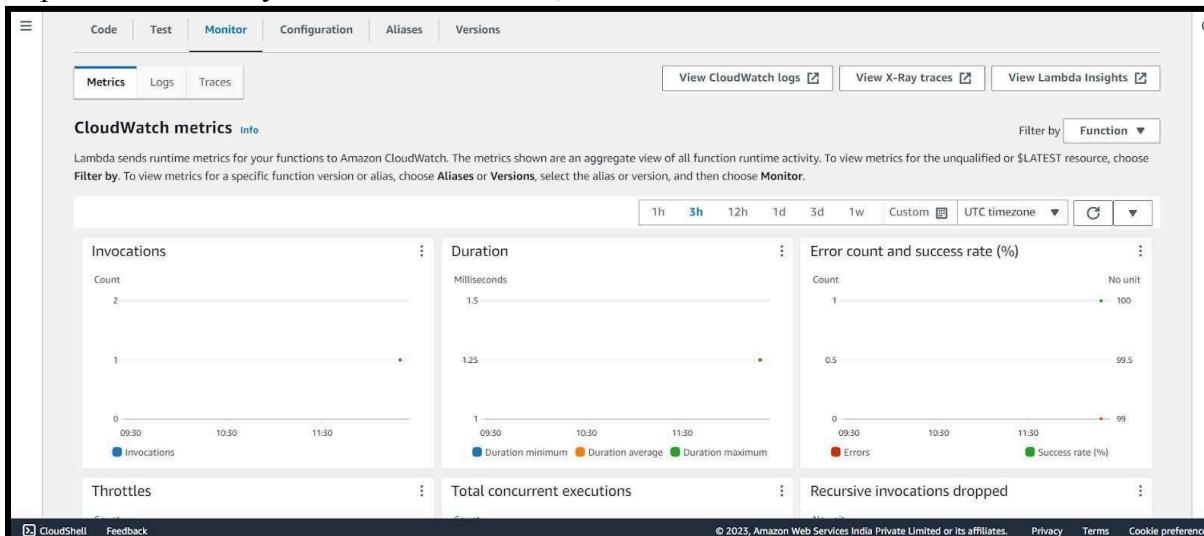
```

Event JSON
Format JSON

10  "principalId": "EXAMPLE"
11 },
12 "requestParameters": {
13   "sourceIPAddress": "127.0.0.1"
14 },
15 "responseElements": {
16   "x-amz-request-id": "EXAMPLE123456789",
17   "x-amz-id-2": "EXAMPLE123/5678abcdefghijklmabcdaisawesome/mnopqrstuvwxyzABCDEFGHIJ"
18 },
19 "s3": {
20   "S3SchemaVersion": "1.0",
21   "configurationId": "testConfigRule",
22   "bucket": {
23     "name": "advopssexp12",
24     "ownerIdentity": {
25       "principalId": "EXAMPLE"
26     },
27     "arn": "arn:aws:s3:::advopssexp12"
28   },
29   "object": {
30     "key": "test%2Fkey",
31     "size": 1024,
32     "eTag": "0123456789abcdef0123456789abcdef",
33     "sequencer": "0A1B2C3D4E5F678901"
34   }
35 }
36 ]
37 }
38 ]

```

Step 14: Go back to your Lambda function , Refresh it and ch



Check the Monitor tab.

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

Step 15: Click on this log Stream that was created to view what was logged by your function.