



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Semester: V

Academic Year: 2023-24

Class / Branch: TE IT

Subject: Advanced Devops Lab (ADL)

Name of Instructor: Prof. Vishal Badgumar

Name of Student: Sanket B. Bhoir

Student ID: 24204022

EXPERIMENT NO. 01

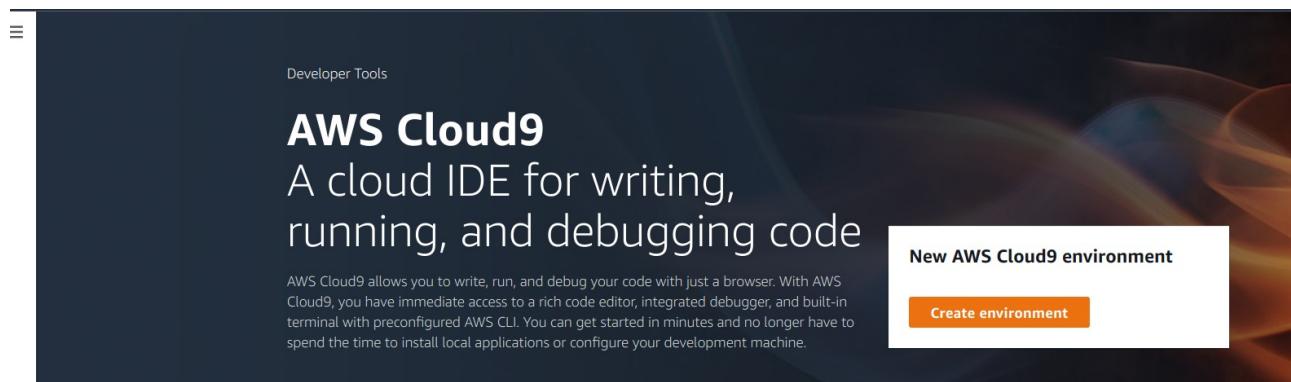
Aim: To understand the benefits of Cloud Infrastructure and Setup AWS Cloud9 IDE, Launch AWS Cloud9 IDE and Perform Collaboration Demonstration.

Steps:

1. Login with your AWS account.

2. Navigate to Cloud 9 service from Developer tools section as below:

3. Click on Create Environment :



4. Provide name for the Environment (WebAppIDE) and click on next.

AWS Cloud9 > Environments > Create environment

Step 1 Name environment

Step 2 Configure settings

Step 3 Review

Name environment

Environment name and description

Name
The name needs to be unique per user. You can update it at any time in your environment settings.

Limit: 60 characters

Description - Optional
This will appear on your environment's card in your dashboard. You can update it at any time in your environment settings.

Limit: 200 characters

Cancel **Next step**



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



5. Keep all the Default settings as shown in below:

AWS Cloud9 ×

Your environments Shared with you Account environments How-to guide

AWS Cloud9 > Environments > Create environment

Step 1 Name environment Step 2 Configure settings Step 3 Review

Configure settings

Environment settings

Environment type Info
Run your environment in a new EC2 instance or an existing server. With EC2 instances, you can connect directly through Secure Shell (SSH) or connect via AWS Systems Manager (without opening inbound ports).

Create a new EC2 instance for environment (direct access)
Launch a new instance in this region that your environment can access directly via SSH.

Create a new no-ingress EC2 instance for environment (access via Systems Manager)
Launch a new instance in this region that your environment can access through Systems Manager.

Create and run in remote server (SSH connection)
Configure the secure connection to the remote server for your environment.

Instance type
 t2.micro (1 GiB RAM + 1 vCPU)
Free-tier eligible. Ideal for educational users and exploration.

t3.small (2 GiB RAM + 2 vCPU)
Recommended for small-sized web projects.

m5.large (8 GiB RAM + 2 vCPU)
Recommended for production and general-purpose development.

Other instance type
Select an instance type.

t3.nano

Platform
 Amazon Linux 2 (recommended)

Amazon Linux AMI

Ubuntu Server 18.04 LTS

Cost-saving setting
Choose a predetermined amount of time to auto-hibernate your environment and prevent unnecessary charges. We recommend a hibernation settings of half an hour of no activity to maximize savings.
After 30 minutes (default)

IAM role
AWS Cloud9 creates a service-linked role for you. This allows AWS Cloud9 to call other AWS services on your behalf. You can delete the role from the AWS IAM console once you no longer have any AWS Cloud9 environments. [Learn more](#)

AWSServiceRoleForAWSCloud9

Network settings (advanced)

No tags associated with the resource.

Add new tag
You can add 50 more tags.

Cancel Previous step Next step



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



6. Review the Environment name and Settings and click on Create Environment:

AWS Cloud9 X AWS Cloud9 > Environments > Create environment

Step 1 Name environment Review

Step 2 Configure settings

Step 3 Review

Environment name and settings

Name: WebAppIDE

Description: No description provided

Environment type: EC2

Instance type: t2.micro

Subnet:

Platform: Amazon Linux 2 (recommended)

Cost-saving settings: After 30 minutes (default)

IAM role: AWSServiceRoleForAWSCloud9 (generated)

We recommend the following best practices for using your AWS Cloud9 environment

- Use [source control and backup](#) your environment frequently. AWS Cloud9 does not perform automatic backups.
- Perform regular [updates of software](#) on your environment. AWS Cloud9 does not perform automatic updates on your behalf.
- Turn on [AWS CloudTrail in your AWS account](#) to track activity in your environment. [Learn more](#)
- Only share your environment with [trusted users](#). Sharing your environment may put your AWS access credentials at risk. [Learn more](#)

Cancel Previous step **Create environment**

It will take few minutes to create aws instance for your Cloud 9 Environment.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



7. Till that time open IAM Identity and Access Management in order to Add user In other tab.

8. Add user provide manual password if you want and click on Next permission tab.



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* apsit

[+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type*

Programmatic access

Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

AWS Management Console access

Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*

Autogenerated password

Custom password

Show password

Require password reset

User must create a new password at next sign-in

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

* Required

[Cancel](#)

[Next: Permissions](#)

9.

Click on Create group

Add user

1

▼ Set permissions



Add user to group



Copy permissions from existing user



Attach existing policies directly



[Get started with groups](#)

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job access, or your custom permissions. Get started by creating a group. [Learn more](#)

[Create group](#)

► Set permissions boundary

10. Provide group name and click on create group.



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. [Learn more](#)

Group name: WebAppspsitgroup

Create policy Refresh

Filter policies Search Showing 669 results

Policy name	Type	Used as	Description
AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissions while explicitly allowing direct access to resources.
AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permissions. Explicitly allows developers and administrators...
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to related AWS Services
AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
AlexaForBusinessLifesizeDelegatedAccess	AWS managed	None	Provide access to Lifesize AVS devices

Cancel Create group

11. After that group is created click on next if u want to provide tag else click on Review for user settings and click on create user as shown in fig.

Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	apsit
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	WebAppspsitgroup

Tags

No tags were added.

Cancel Previous Create user

12. Now close that window and Navigate to user Groups from left pane in IAM.



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Identity and Access Management (IAM)

- Dashboard
- Access management
 - User groups
 - Users
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
 - Credential report
 - Organization activity
 - Service control policies (SCPs)

Introducing the new User groups experience
We've redesigned the User groups experience to make it easier to use. [Let us know what you think.](#)

IAM > User groups

User groups (1) [Info](#)
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time
WebAppapsitgroup	1 ..	Not defined	4 minutes ago

13. click on your group name which you have created and navigate to permission tab as shown:

Identity and Access Management (IAM)

- Dashboard
- Access management
 - User groups
 - Users
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
 - Credential report
 - Organization activity
 - Service control policies (SCPs)

IAM > User groups > WebAppapsitgroup

WebAppapsitgroup

Delete

Summary

User group name	Creation time	ARN
WebAppapsitgroup	July 07, 2021, 12:07 (UTC+05:30)	arn:aws:iam::229296960472:group/WebAppapsitgroup

Users **Permissions** Access advisor

Permissions policies (0) Info
You can attach up to 10 managed policies.

Policy Name	Type	Attached entities
No resources to display		

14. Now click on Add permission and select Attach Policy after that search for Cloud9 related policy and select Awscloud9EnviornmentMember policy and add it.

Other permission policies (Selected 1/669) [Info](#)
You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Filter policies by property or policy name and press enter

"Cloud9"

Policy Name	Type	Attached entities
<input checked="" type="checkbox"/> AWSCloud9EnvironmentMember	AWS managed	0
<input type="checkbox"/> AWSCloud9Administrator	AWS managed	0
<input type="checkbox"/> AWSCloud9User	AWS managed	0
<input type="checkbox"/> AWSCloud9SSMInstanceProfile	AWS managed	0

[Cancel](#) [Add permissions](#)



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



15. now we move towards our cloud9 IDE Enviorment tab it shows as shown :

The screenshot shows the AWS Toolkit interface within a Cloud9 IDE. On the left, the AWS Explorer sidebar is open, showing regions like Europe (Ireland) and US West (Oregon). In the center, a code editor window displays a JavaScript file named 'app.js' with the following content:

```
13 * Return doc: https://docs.aws.amazon.com/apigateway/latest/developerguide/set-up-lambda-proxy.html
14 * @returns {Object} object - API Gateway Lambda Proxy Output Format
15 *
16 */
17 Add Debug Configuration
18 exports.handler = async (event, context) => {
19   try {
20     // const ret = await axios(url);
21     response = {
22       'statusCode': 200,
23       'body': JSON.stringify({
24         message: 'Hello world',
25         // location: ret.data.trim()
26       })
27     } catch (err) {
28       console.log(err);
29       return err;
30     }
31   }
32   return response;
33 };
34 }
```

Annotations in the screenshot include:

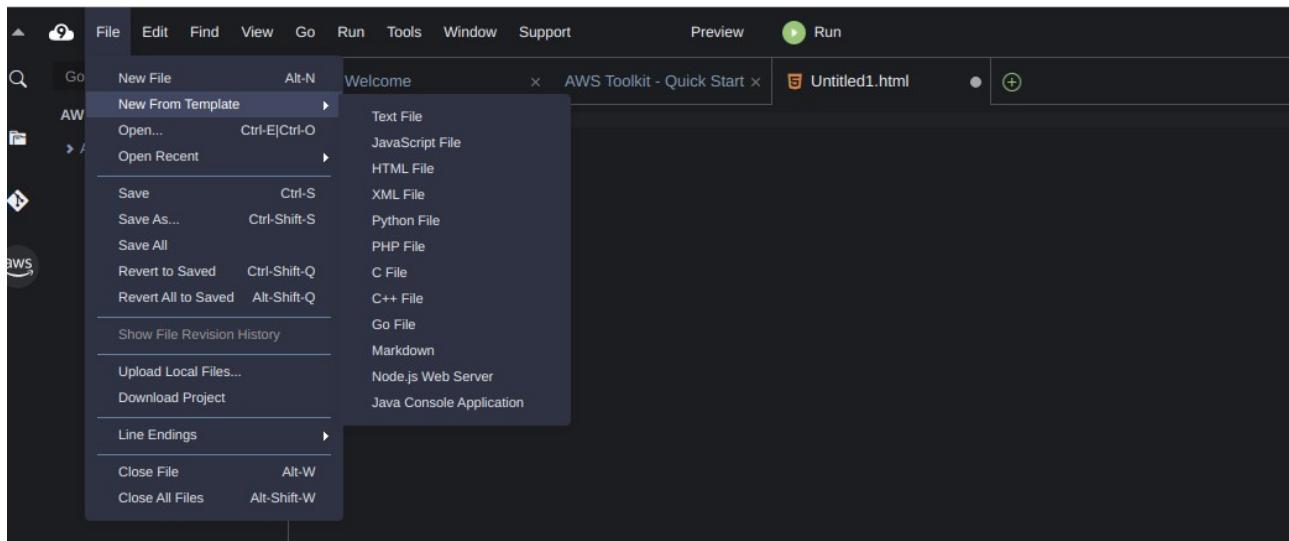
- An orange arrow points from the text "AWS Explorer" to the AWS Explorer sidebar.
- An orange arrow points from the text "AWS Explorer" to the AWS icon in the top-left corner of the interface.
- A yellow arrow points from the text "AWS Explorer" to the AWS icon in the bottom-left corner of the interface.
- A red arrow points from the text "Inline Action" to the word "Add Debug Configuration" in the code.
- A yellow arrow points from the text "Current Credentials" to the "Current Credentials" status bar at the bottom right.

16. If you check at bottom side Cloud9 IDE also giving you and aws CLI for command operations: as we here checked git version, iam user details and so on...

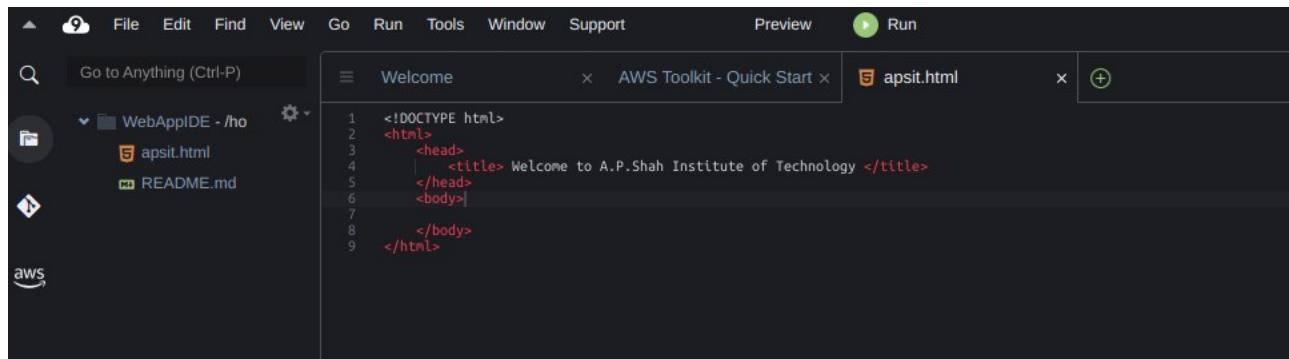
The screenshot shows the AWS Toolkit interface within a Cloud9 IDE. On the left, the AWS Explorer sidebar is open, showing regions like Asia Pacific (Mumbai). In the center, a terminal window titled "bash - ip-172-31-10-50.a x" shows the following AWS CLI commands and their outputs:

```
ec2-user:~/environment $ git --version
git version 2.23.4
ec2-user:~/environment $ aws iam get-user
{
  "User": {
    "PasswordLastUsed": "2021-07-07T05:34:24Z",
    "CreateDate": "2021-06-03T18:03:54Z",
    "UserId": "229296960472",
    "Arn": "arn:aws:iam::229296960472:root"
  }
}
```

17. Now we will setup collaborative enviorment Click on File you can create new file or choose from template, here m opting html file to collaborate.



18. Edit html file and save it



19. now in order to share this file to collaborate with other members of your team click on Share option on Right Pane and username which you created in IAM before into Invite members and enable permission as RW (Read and Write) and click on Done. Click OK for Security warning.



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Share this environment

Links to share

Environment: <https://ap-south-1.console.aws.amazon.com/cloud9/ide/77a623f05f68>

Application: 15.206.205.29

Security warning

Allowing ReadWrite access to your environment may put your AWS security credentials at risk

Do you trust this person with your AWS security credentials and full access to all files in your environment?

[Details and advanced options](#)

Don't show me this notification again

Don't allow members to save their tab state

Invite Members

apsit R RW

Invite an existing IAM user or [create a new user](#)

6:11 HTML Spa

20. Now Open your Browsers Incognito Window and login with IAM user which you configured before.



Sign in

Root user

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

IAM user

User within an account that performs daily tasks. [Learn more](#)

Account ID (12 digits) or account alias

229296960472

Remember this account

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

New to AWS? [Create a new AWS account](#)



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



21. After Successful login with IAM user open Cloud9 service from dashboard services and click on shared with you enviornment to collaborate.

The screenshot shows the AWS Cloud9 interface. On the left, there's a sidebar with links for 'Your environments', 'Shared with you' (which is highlighted in orange), and 'Account environments'. Below that is a 'How-to guide'. The main area is titled 'AWS Cloud9 > Shared with you'. It lists 'Shared with you (1)'. The environment is named 'WebAppIDE'. It shows the following details:

- Type: EC2
- Permissions: Read-write
- Description: No description available
- Owner Arn: arn:aws:iam::229296960472:root

A large 'Open IDE' button is located at the bottom of this card.

22. Click on Open IDE you will same interface as your other member have to collaborate in real time, also you all within team can do group chats as shown below:

The screenshot shows the AWS Cloud9 IDE interface. The left side has a file tree with 'apsit.html' selected, showing its content:

```
<!DOCTYPE html>
<html>
<head>
<title> Welcome to A.P.Shah Institute of Technology </title>
</head>
<body>
hello mumbai!
</body>
</html>
```

The right side of the interface includes:

- A toolbar with File, Edit, Find, View, Go, Run, Tools, Window, Support, Preview, and Run buttons.
- An 'ENVIRONMENT MEMBERS' section showing two members: 'arn:aws:iam::229296960472:root' (ReadWrite) and 'You (online)' (ReadWrite).
- A 'GROUP CHAT' section with a message from 'root' to 'You'.
- A status bar at the bottom showing '7:13 HTML Spaces: 4'.



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



```
<!DOCTYPE html>
<html>
<head>
<title> Welcome to A.P.Shah Institute of Technology </title>
</head>
<body>
hello mundo!
</body>
```

```
aws: profile.default
bash *ip-172-31-10-50.x Immediate (JavaScript) (b x)
ec2-user:~/environment $ git config --global user.email vishalbadgur
ec2-user:~/environment $
```



PARSHVANATH CHARITABLE TRUST'S

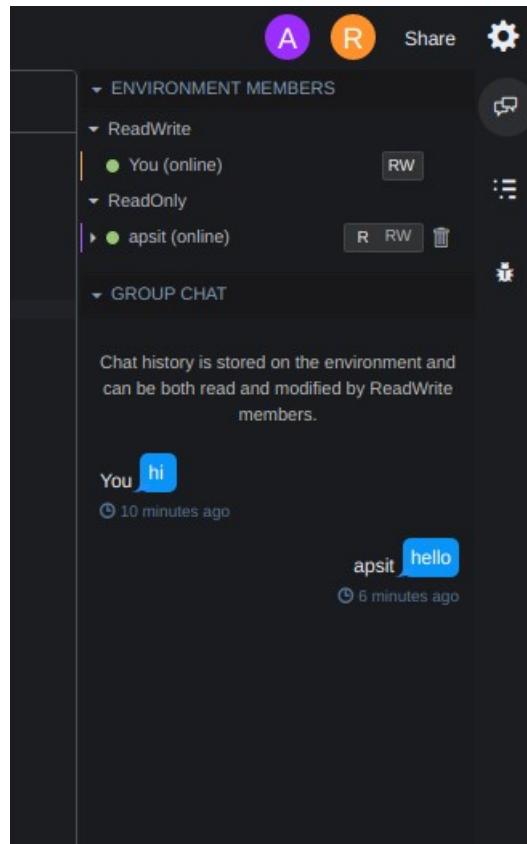
A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



23. you can also explore settings where you can update permissions of your temmates as from RW to R only or you can remove user too.



For more info related to AWS-Cloud 9 you all can refer following Docs.

<https://docs.aws.amazon.com/cloud9/latest/user-guide/aws-cloud9-ug.pdf>

Conclusion:

I successfully created Cloud9 instance also created one user and one group then I added user to group and to the cloud9 instance.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)

**Semester: V****Academic Year: 2025-26****Class / Branch: TE IT****Subject: Advanced Devops Lab (ADL)****Name of Instructor: Prof. Vishal Badgujar****Name of Student: Sanket B. Bhoir****Student ID: 24204022**

EXPERIMENT NO. 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.

Step 1:

The screenshot shows the 'Create bucket' wizard in the AWS S3 console. The 'General configuration' section is selected. Under 'Bucket type', the 'General purpose' option is chosen, with a note explaining it's recommended for most use cases. The 'Bucket name' field contains 'store-build-artifact-sanket'. The 'Copy settings from existing bucket - optional' section is present but empty. The 'Format: s3://bucket/prefix' placeholder is visible at the bottom.

Step 2:

The screenshot shows the 'Buckets' page in the AWS S3 console. The 'General purpose buckets' tab is active. A single bucket, 'store-build-artifact-sanket', is listed. The bucket details show it was created on July 22, 2025, at 15:37:06 (UTC+05:30) in the 'Asia Pacific (Mumbai) ap-south-1' region. The bucket name is highlighted in blue.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 3:

The screenshot shows the 'Create bucket' page in the AWS S3 console. Under 'Object Ownership', it says 'Bucket owner enforced'. In the 'Block Public Access settings for this bucket' section, there are five checkboxes: 'Block all public access' (unchecked), 'Block public access to buckets and objects granted through new access control lists (ACLs)' (unchecked), 'Block public access to buckets and objects granted through any access control lists (ACLs)' (unchecked), 'Block public access to buckets and objects granted through new public bucket or access point policies' (unchecked), and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies' (unchecked). Below these, a note states: '⚠️ Turning off block all public access might result in this bucket and the objects within becoming public. AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.' A checkbox at the bottom is checked, stating: 'I acknowledge that the current settings might result in this bucket and the objects within becoming public.' The URL in the address bar is 'Amazon S3 > Buckets > Create bucket'.

Step 4:

The screenshot shows the 'Buckets' page in the AWS S3 console. A green banner at the top says 'Successfully created bucket "deployment-bucket-pwa-sanket"'. Below it, a message says 'To upload files and folders, or to configure additional bucket settings, choose View details.' Under 'General purpose buckets', there are two buckets listed: 'deployment-bucket-pwa-sanket' (created July 22, 2025) and 'store-build-artifact-sanket' (created July 22, 2025). The 'Create bucket' button is visible at the top right. The URL in the address bar is 'Amazon S3 > Buckets'.

Step 5:

The screenshot shows the 'Build projects' page in the AWS CodeBuild console. At the top, there are buttons for 'Build projects' (Info), 'Actions', 'Create trigger', 'View details', 'Debug build', 'Start build', and 'Create project'. Below is a search bar and a dropdown for 'Your projects'. A table header includes columns for 'Name', 'Source provider', 'Repository', 'Latest build status', 'Description', and 'Last Modified'. A message at the bottom center says 'No results' and 'There are no results to display.' The URL in the address bar is 'Developer Tools > CodeBuild > Build projects'.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 6:

Create a new fork

A fork is a copy of a repository. Forking a repository allows you to freely experiment with changes without affecting the original project. [View existing forks.](#)

Required fields are marked with an asterisk (*).

Owner *



Repository name *

/ Car-pwa-deploy-on-aws

Car-pwa-deploy-on-aws is available.

By default, forks are named the same as their upstream repository. You can customize the name to distinguish it further.

Description (optional)

Copy the master branch only

Contribute back to iamdkcoder/Car-pwa-deploy-on-aws by adding your own branch. [Learn more.](#)

i You are creating a fork in your personal account.

Create fork

Step 7:

Manage default source credential

Source Provider



Credential type

GitHub App

Connect project to GitHub using
an AWS managed GitHub App

Personal access token

Connect project to GitHub using
a personal access token

OAuth app

Connect project to GitHub using
an OAuth app

Service

Secrets Manager (recommended)

Use Secrets Manager to store token

CodeBuild

Use CodeBuild managed token

Connect to GitHub



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Step 8:

Authorize application - Google Chrome

github.com/login/oauth/authorize?client_id=9859b46d0db8987e9a94&scope=r...

Authorize AWS CodeBuild (Mumbai)

AWS CodeBuild (Mumbai) by aws-codesuite wants to access your Sanketbhoir03 account

Organization webhooks Admin access

Organizations and teams Read-only access

Repositories Public and private

Cancel Authorize aws-codesuite

Authorizing will redirect to <https://ap-south-1.console.aws.amazon.com>

Step 9:

Source 1 - Primary

Source provider

GitHub

Credential

Your account is successfully connected through OAuth using CodeBuild managed token. [Manage account credentials](#).

Use override credentials for this project only

Repository

Repository In my GitHub account Public repository GitHub scoped webhook

https://github.com/Sanketbhoir03/Car-pwa-deploy-on-aws.git

Source version - optional info

Enter a pull request, branch, commit ID, tag, or reference and a commit ID.

► Additional configuration

Git clone depth, Git submodules, Build status config



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 10:

▼ Environment

Provisioning model [Info](#)

On-demand
Automatically provision build infrastructure in response to new builds.

Reserved capacity
Use a dedicated fleet of instances for builds. A fleet's compute and environment type will be used for the project.

Environment Image

Managed image
Use an Image managed by AWS CodeBuild

Custom image
Specify a Docker image

Compute

EC2
Optimized for flexibility during action runs

Lambda
Optimized for speed and minimizes the start up time of workflow actions

Running mode

Container
Running on Docker container

Instance
Running on EC2 instance directly

Operating system

Amazon Linux

Step 11:

Operating system

Amazon Linux

Runtime(s)

Base

Image

aws/codebuild/ami/amazonlinux-x86_64-base:latest

Service role

New service role
Create a service role in your account

Existing service role
Choose an existing service role from your account

Role name

codebuild-pwa-codebuild-sanket-service-role

Type your service role name

► Additional configuration

Timeout, privileged, certificate, VPC, compute type, environment variables, file systems, auto-retry, registry credential



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 12:

▼ Buildspec

Build specifications

Insert build commands

Store build commands as build project configuration

Use a buildspec file

Store build commands in a YAML-formatted buildspec file

Buildspec name - *optional*

By default, CodeBuild looks for a file named buildspec.yml in the source code root directory. If your buildspec file uses a different name or location, enter its path from the source root here (for example, buildspec-two.yml or configuration/buildspec.yml).

buildspec.yml

▼ Batch configuration

You can run a group of builds as a single execution. Batch configuration is also available in advanced option when starting build.

Define batch configuration - *optional*

You can also define or override batch configuration when starting a build batch.

Step 13:

▼ Logs

CloudWatch

CloudWatch logs - *optional*

Checking this option will upload build output logs to CloudWatch.

Group name - *optional*

aws/codebuild/pwa-codebuild-sanket

The group name of the logs in CloudWatch Logs. The log group name will be /aws/codebuild/<project-name> by default.

Stream name prefix - *optional*

The prefix of the stream name of the CloudWatch Logs.

S3

S3 logs - *optional*

Checking this option will upload build output logs to S3.

Cancel

Create build project



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 14:

Project created
You have successfully created the following project: pwa-codebuild-sanket

Create a notification rule for this project X

Developer Tools > CodeBuild > Build projects > pwa-codebuild-sanket

pwa-codebuild-sanket

Actions ▾ Create trigger Edit Clone Debug build Start build with overrides Start build

Configuration

Source provider	Primary repository	Artifacts upload location	Service role
GitHub	Sanketbhoir03/Car-pwa-deploy-on-aws [2]	-	arn:aws:iam::158018605139:role/service-role/codebuild-pwa-codebuild-sanket-service-role
Public builds	Disabled		

Build history Batch history Project details Build triggers Metrics Debug sessions

Conclusion:

In this topic, I learned how to automate the build, test, and deployment of applications using AWS CodeBuild and AWS CodePipeline. I gained practical experience deploying to Amazon S3/SEBS and utilizing AWS CodeDeploy to deploy a sample application onto an EC2 instance.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)

**Semester: V****Academic Year: 2025-26****Class / Branch: TE IT****Subject: Advanced Devops Lab (ADL)****Name of Instructor: Prof. Vishal Badgujar****Name of Student: Sanket B. Bhoir****Student ID: 24204022**

EXPERIMENT NO. 03

Aim: To deploy sample application using EC2 instance using AWS Code Deploy**Step 1:**

The screenshot shows the 'Create bucket' step in the AWS S3 console. Under 'General configuration', the 'AWS Region' is set to 'Asia Pacific (Mumbai) ap-south-1'. The 'Bucket type' section has 'General purpose' selected, with a note about redundancy across Availability Zones. The 'Bucket name' field contains 'store-build-artifact-sanket'. Below it, there's a note about bucket naming rules and a 'Choose bucket' button for copying settings from another bucket.

Step 2:

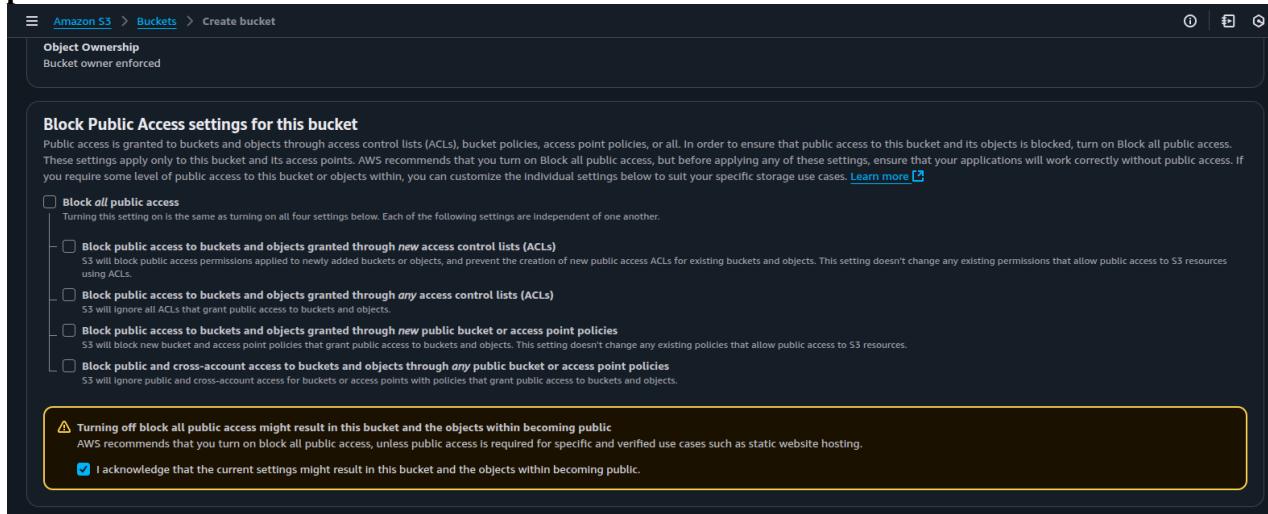
The screenshot shows the 'General purpose buckets' list in the AWS S3 console. It displays one bucket named 'store-build-artifact-sanket' created on July 22, 2025. The bucket is in the 'ap-south-1' region. The page includes filters for 'Name', 'AWS Region', and 'Creation date'.



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)

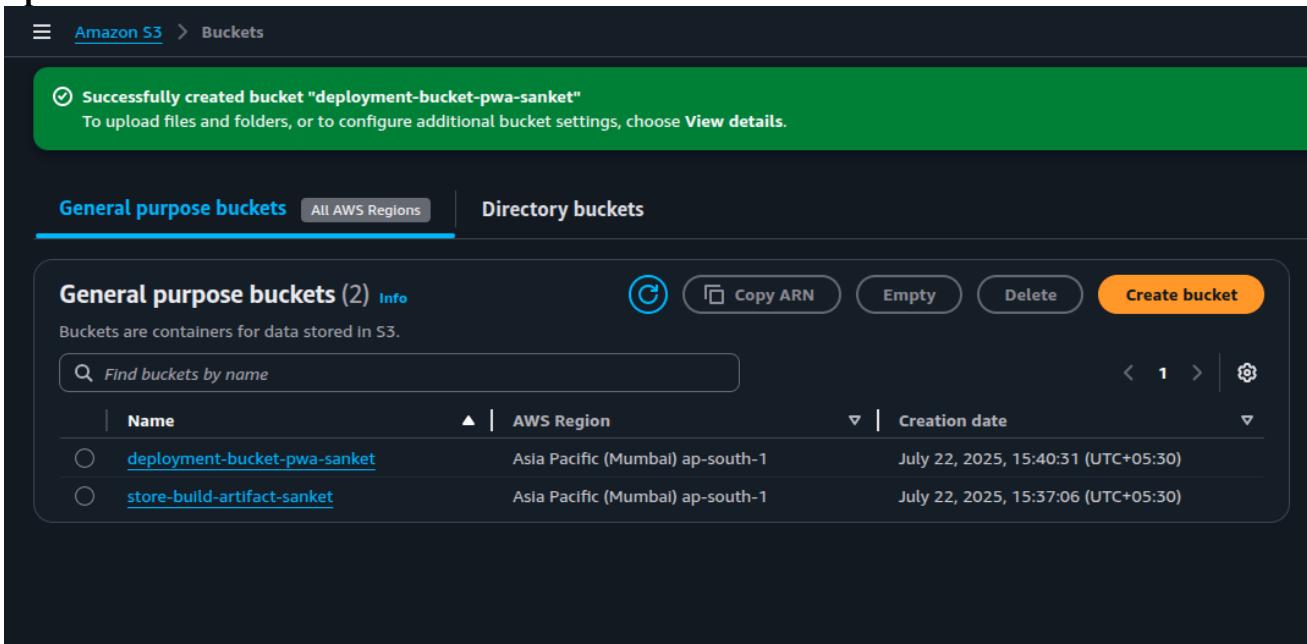


Step 3:



The screenshot shows the 'Block Public Access settings for this bucket' section in the AWS S3 console. It includes a note about public access being granted through various mechanisms like ACLs and policies. It features several checkboxes for enabling different types of public access, with 'Block all public access' being the primary option. A warning message at the bottom states that turning off block all public access might result in the bucket becoming public, and a checkbox is present for acknowledging this risk.

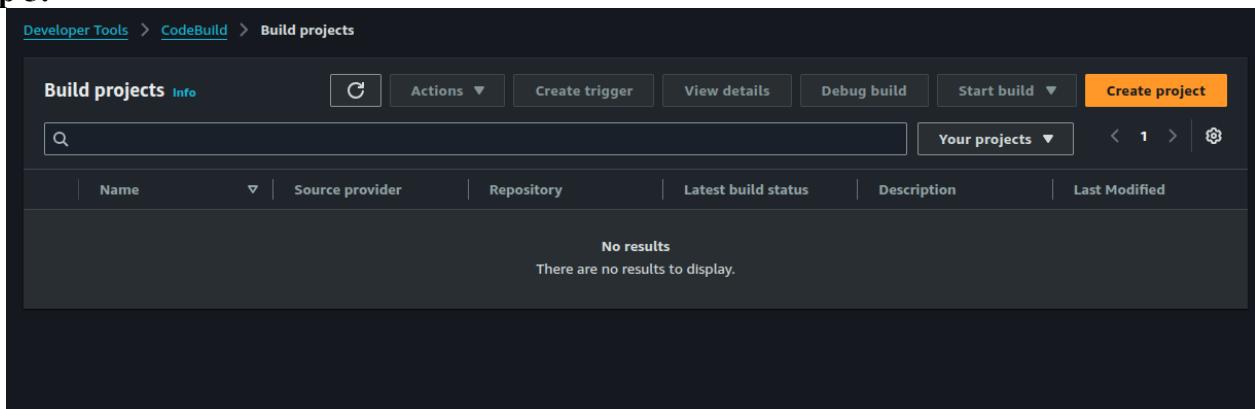
Step 4:



The screenshot shows the 'General purpose buckets' list in the AWS S3 console. It displays two buckets: 'deployment-bucket-pwa-sanket' and 'store-build-artifact-sanket'. The 'deployment-bucket-pwa-sanket' was created on July 22, 2025, at 15:40:31 UTC+05:30. The 'Create bucket' button is visible at the top right of the list.

Name	AWS Region	Creation date
deployment-bucket-pwa-sanket	Asia Pacific (Mumbai) ap-south-1	July 22, 2025, 15:40:31 (UTC+05:30)
store-build-artifact-sanket	Asia Pacific (Mumbai) ap-south-1	July 22, 2025, 15:37:06 (UTC+05:30)

Step 5:



The screenshot shows the 'Build projects' list in the AWS CodeBuild console. It displays no results, indicating there are no build projects currently listed. The interface includes a search bar, project status filters, and columns for Name, Source provider, Repository, Latest build status, Description, and Last Modified.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 6:

Create a new fork

A fork is a copy of a repository. Forking a repository allows you to freely experiment with changes without affecting the original project. [View existing forks.](#)

Required fields are marked with an asterisk (*).

Owner *



Repository name *

/ Car-pwa-deploy-on-aws

Car-pwa-deploy-on-aws is available.

By default, forks are named the same as their upstream repository. You can customize the name to distinguish it further.

Description (optional)

Copy the master branch only

Contribute back to iamdkcoder/Car-pwa-deploy-on-aws by adding your own branch. [Learn more.](#)

i You are creating a fork in your personal account.

Create fork

Step 7:

Manage default source credential

Source Provider



Credential type

GitHub App

Connect project to GitHub using
an AWS managed GitHub App

Personal access token

Connect project to GitHub using
a personal access token

OAuth app

Connect project to GitHub using
an OAuth app

Service

Secrets Manager (recommended)

Use Secrets Manager to store token

CodeBuild

Use CodeBuild managed token

Connect to GitHub



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Step 8:

Authorize application - Google Chrome

github.com/login/oauth/authorize?client_id=9859b46d0db8987e9a94&scope=r...

Authorize AWS CodeBuild (Mumbai)

AWS CodeBuild (Mumbai) by aws-codesuite wants to access your Sanketbhoir03 account

Organization webhooks Admin access

Organizations and teams Read-only access

Repositories Public and private

Cancel Authorize aws-codesuite

Authorizing will redirect to <https://ap-south-1.console.aws.amazon.com>

Step 9:

Source 1 - Primary

Source provider

GitHub

Credential

Your account is successfully connected through OAuth using CodeBuild managed token. [Manage account credentials](#).

Use override credentials for this project only

Repository

Repository In my GitHub account Public repository GitHub scoped webhook

https://github.com/Sanketbhoir03/Car-pwa-deploy-on-aws.git

Source version - optional info

Enter a pull request, branch, commit ID, tag, or reference and a commit ID.

► Additional configuration

Git clone depth, Git submodules, Build status config



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 10:

▼ Environment

Provisioning model [Info](#)

On-demand
Automatically provision build infrastructure in response to new builds.

Reserved capacity
Use a dedicated fleet of instances for builds. A fleet's compute and environment type will be used for the project.

Environment Image

Managed image
Use an Image managed by AWS CodeBuild

Custom image
Specify a Docker image

Compute

EC2
Optimized for flexibility during action runs

Lambda
Optimized for speed and minimizes the start up time of workflow actions

Running mode

Container
Running on Docker container

Instance
Running on EC2 instance directly

Operating system

Amazon Linux

Step 11:

Operating system

Amazon Linux

Runtime(s)

Base

Image

aws/codebuild/ami/amazonlinux-x86_64-base:latest

Service role

New service role
Create a service role in your account

Existing service role
Choose an existing service role from your account

Role name

codebuild-pwa-codebuild-sanket-service-role

Type your service role name

► Additional configuration

Timeout, privileged, certificate, VPC, compute type, environment variables, file systems, auto-retry, registry credential



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 12:

▼ Buildspec

Build specifications

Insert build commands

Store build commands as build project configuration

Use a buildspec file

Store build commands in a YAML-formatted buildspec file

Buildspec name - *optional*

By default, CodeBuild looks for a file named buildspec.yml in the source code root directory. If your buildspec file uses a different name or location, enter its path from the source root here (for example, buildspec-two.yml or configuration/buildspec.yml).

buildspec.yml

▼ Batch configuration

You can run a group of builds as a single execution. Batch configuration is also available in advanced option when starting build.

Define batch configuration - *optional*

You can also define or override batch configuration when starting a build batch.

Step 13:

▼ Logs

CloudWatch

CloudWatch logs - *optional*

Checking this option will upload build output logs to CloudWatch.

Group name - *optional*

aws/codebuild/pwa-codebuild-sanket

The group name of the logs in CloudWatch Logs. The log group name will be /aws/codebuild/<project-name> by default.

Stream name prefix - *optional*

The prefix of the stream name of the CloudWatch Logs.

S3

S3 logs - *optional*

Checking this option will upload build output logs to S3.

Cancel

Create build project



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 14:

The screenshot shows the AWS CodeBuild console. At the top, a green banner indicates "Project created" with the message "You have successfully created the following project: pwa-codebuild-sanket". Below this, the navigation path is "Developer Tools > CodeBuild > Build projects > pwa-codebuild-sanket". The main title is "pwa-codebuild-sanket". Below the title are several action buttons: "Actions", "Create trigger", "Edit", "Clone", "Debug build", "Start build with overrides", and "Start build" (which is highlighted in orange). A large section titled "Configuration" displays the following details:

Source provider GitHub	Primary repository Sanketbhoir03/Car-pwa-deploy-on-aws	Artifacts upload location -	Service role arn:aws:iam::158018605139:role/service-role/codebuild-pwa-codebuild-sanket-service-role
Public builds Disabled			

Below the configuration are links for "Build history", "Batch history", "Project details", "Build triggers", "Metrics", and "Debug sessions".

Step 15:

The screenshot shows the AWS CodePipeline console. The navigation path is "Developer Tools > CodePipeline > Pipelines". The main title is "Pipelines". Below the title are several buttons: "Info", "C" (refresh), "View history", "Release change", "Delete pipeline", and "Create pipeline" (which is highlighted in orange). There is also a search bar and a pagination indicator showing page 1 of 1. A message "No results" is displayed with the subtext "There are no results to display."

Step 16:

The screenshot shows the "Pipeline settings" page for a new pipeline. The pipeline name is "pwa-pipeline-sanket". The execution mode is set to "Queued". The service role is configured to "New service role" with the role name "AWSCodePipelineServiceRole-ap-south-1-pwa-pipeline-sanket". A checkbox "Allow AWS CodePipeline to create a service role so it can be used with this new pipeline" is checked.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 17:

▼ Advanced settings
Configure artifact store location, encryption settings, and pipeline variables for your pipeline.

Artifact store

Default location
Create a default S3 bucket in your account.

Custom location
Choose an existing S3 location from your account in the same region and account as your pipeline

Bucket
 X

Encryption key

Default AWS Managed Key
Use the AWS managed customer master key for CodePipeline in your account to encrypt the data in the artifact store.

Customer Managed Key
To encrypt the data in the artifact store under an AWS KMS customer managed key, specify the key ID, key ARN, or alias ARN.

Variables
You can add variables at the pipeline level. You can choose to assign the value when you start the pipeline. [Learn more](#)

No variables defined at the pipeline level in this pipeline.

Add variable
You can add up to 50 variables.

Step 18:

Source

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

▾

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

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

Enable automatic retry on stage failure

[Cancel](#) | [Previous](#)



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 19:

Authorize AWS CodePipeline (Mumbai)

AWS CodePipeline (Mumbai) by [aws-codesuite](#)
wants to access your [Sanketbhoir03](#) account

Repository webhooks and services
Admin access

Repositories
Public and private

Cancel Authorize aws-codesuite

Authorizing will redirect to
<https://ap-south-1.console.aws.amazon.com>

Not owned or operated by GitHub
Created 9 years ago

Step 20:

Source

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

GitHub (via OAuth app)

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

Connected

You have successfully configured the action with the provider. X



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 21:

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

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

Repository
 X

Branch
 X

Enable automatic retry on stage failure

Step 22:

Add build stage Info

Step 4 of 7

Build - optional

Build provider
Choose the tool you want to use to run build commands and specify artifacts for your build action.

Commands Other build providers

▼

Project name
Choose a build project that you have already created in the AWS CodeBuild console. Or create a build project in the AWS CodeBuild console and then return to this task.

X or [Create project](#)

Define buildspec override - *optional*
Buildspec file or definition that overrides the latest one defined in the build project, for this build only.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 23:

Environment variables - *optional*
Choose the key, value, and type for your CodeBuild environment variables. In the value field, you can reference variables generated by CodePipeline. [Learn more](#)

[Add environment variable](#)

Build type

Single build
Triggers a single build.

Batch build
Triggers multiple builds as a single execution.

Region

Asia Pacific (Mumbai) ▾

Input artifacts

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

SourceArtifact X
Defined by: Source

Enable automatic retry on stage failure

[Cancel](#) [Previous](#) [Skip build stage](#) [Next](#)

Step 24:

Deploy - *optional*

Deploy provider
Choose how you want to deploy your application or content. Choose the provider, and then provide the configuration details for that provider.

Amazon S3 ▾

Region

Asia Pacific (Mumbai) ▾

Input artifacts

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

BuildArtifact X
Defined by: Build

No more than 100 characters

Bucket

Q deployment-bucket-pwa-sanket X

S3 object key

Enter the object key. You can include a file path without the delimiter character (/) at the beginning. Include the file extension. Example: SampleApp.zip



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 25:

Step 6: Add deploy stage

Deploy action provider

Deploy action provider
Amazon S3

Extract
true

BucketName
deployment-bucket-pwa-sanket

Configure automatic rollback on stage failure
Enabled

Enable automatic retry on stage failure
Disabled

Cancel Previous Create pipeline

Step 26:

Success
Congratulations! The pipeline pwa-pipeline-sanket has been created.

Developer Tools > CodePipeline > Pipelines > pwa-pipeline-sanket

pwa-pipeline-sanket

Edit Stop execution Create trigger Clone pipeline Release change

Pipeline Executions Triggers Settings Tags Stage

Step 27:

Developer Tools > CodeBuild > Build projects > pwa-codebuild-sanket > pwa-codebuild-sanket:f5ed5bb6-fa60-464f-93e9-6f91459224f9

pwa-codebuild-sanket:f5ed5bb6-fa60-464f-93e9-6f91459224f9

Stop build Debug build Retry build

Build status

Status	Initiator	Build ARN	Resolved source version
Failed	codepipeline/pwa-pipeline-sanket	arn:aws:codebuild:ap-south-1:158018605139:build/pwa-codebuild-sanket:f5ed5bb6-fa60-464f-93e9-6f91459224f9	e96963323cf1d3d811e61c397af2cff50d65e8c4

Start time End time Build number

Jul 22, 2025 4:19 PM (UTC+5:30) Jul 22, 2025 4:19 PM (UTC+5:30) 2

Build logs Phase details Reports Environment variables Build details Resource utilization

Department of Information Technology | AP SIT



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Step 28:

Other permissions policies (1/1068)

Policy name	Type	Description
AmazonDMSRedshiftS3Role	AWS managed	Provides access to manage S3 settings...
AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t...
AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	Provides AWS Lambda functions permil...
AmazonS3OutpostsFullAccess	AWS managed	Provides full access to Amazon S3 on ...
AmazonS3OutpostsReadOnlyAccess	AWS managed	Provides read only access to Amazon S...

Step 29:

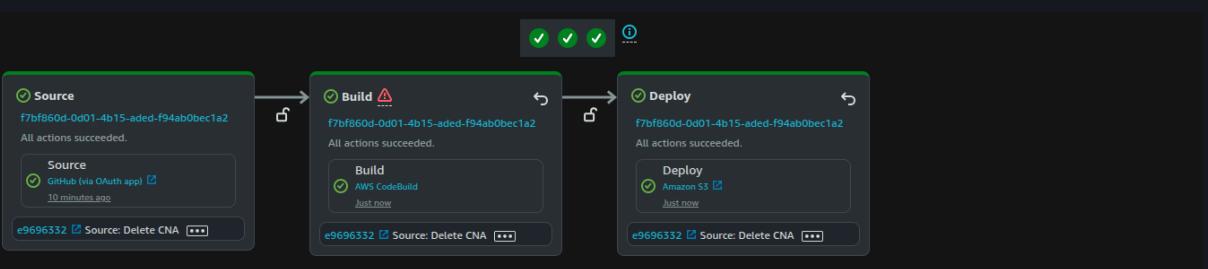
Success
Stage Build successfully retried

Developer Tools > CodePipeline > Pipelines > pwa-pipeline-sanket

pwa-pipeline-sanket

Edit Stop execution Create trigger Clone pipeline Release change

Pipeline Executions Triggers Settings Tags Stage



Step 30:

Policy was successfully attached to role.

Permissions Trust relationships Tags Last Accessed Revoke sessions

Permissions policies (2) [Info](#)

You can attach up to 10 managed policies.

Policy name	Type	Attached entities
AmazonS3FullAccess	AWS managed	1
CodeBuildBasePolicy-pwa-codebuild-sanket-a...	Customer managed	1



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 31:

Amazon S3 > Buckets > deployment-bucket-pwa-sanket > Edit static website hosting

Edit static website hosting

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

Static website hosting
 Disable
 Enable

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

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

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

Step 32:

Amazon S3 > Buckets > deployment-bucket-pwa-sanket

Successfully edited static website hosting.

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)

Bucket Key
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)
Enabled

Step 33:

Edit bucket policy [Info](#)

Bucket policy

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

Bucket ARN
arn:aws:s3:::deployment-bucket-pwa-sanket

Policy

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Sid": "PublicReadGetObject",  
6             "Effect": "Allow",  
7             "Principal": "",  
8             "Action": [  
9                 "s3:GetObject"  
10            ],  
11             "Resource": [  
12                 "arn:aws:s3:::deployment-bucket-pwa-sanket/*"  
13             ]  
14         }  
15     ]  
16 }
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 34:

Successfully edited bucket policy.

Bucket policy

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

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "PublicReadGetObject",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "s3:GetObject",  
      "Resource": "arn:aws:s3:::deployment-bucket-pwa-sanket/*"  
    }  
  ]  
}
```

[Edit](#) [Delete](#) [Copy](#)

Step 35:

+55-4XX-634-7071 info@themevessel.com Mon - Sun: 8:00am - 6:00pm

Car Zone

HOME CARS ABOUT SERVICES CONTACT

EXPLORE YOUR DREAM CAR

Allow us to guide you through the innovative stress free approach in finding your dream car.

READ MORE

Search by name

Brand

Model

Location

Year

Select Type Of Car

Price
0 USD 150000 USD

SEARCH

Conclusion:

In this topic, I learned how to automate the build, test, and deployment of applications using AWS CodeBuild and AWS CodePipeline. I gained practical experience deploying to Amazon S3/SEBS and utilizing AWS CodeDeploy to deploy a sample application onto an EC2 instance.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)

**Semester:V****Academic Year: 2025-26****Class / Branch: TE IT****Subject: Advanced DevOps Lab (ADL)****Name of Instructor: Prof. Vishal Badgujar****Name of Student:Sanket B. Bhoir****Student ID: 24204022**

EXPERIMENT NO. 04

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

Step1:

The screenshot shows the AWS EC2 Instances page with the 'Launch an instance' button selected. In the 'Name' field, 'sanket' is entered. Under 'Application and OS Images (Amazon Machine Image)', the 'Quick Start' tab is selected, showing various OS options like Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, and Debian. An Ubuntu Server 24.04 LTS (HVM) AMI is selected. On the right, the 'Summary' section shows 1 instance being launched. The 'Software Image (AMI)' is Canonical, Ubuntu, 24.04, amd64. The 'Virtual server type (instance type)' is set to t2.micro. The 'Storage (volumes)' section indicates 1 volume(s) - 8 GiB. A note about the free tier is displayed: 'Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage for t3.micro where t2.micro isn't eligible'. At the bottom, there are 'Cancel', 'Launch instance', and 'Preview code' buttons.

Step2:

The screenshot shows the 'Create key pair' dialog box. In the 'Key pair name' field, 'sb' is entered. Below it, a note states: '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.' Under 'Key pair type', the 'RSA' option is selected. Another option, 'ED25519', is also available. In the 'Private key file format', the '.pem' option is selected, with a note: 'For use with OpenSSH'. The '.ppk' option is also listed, 'For use with PuTTY'. A warning message at the bottom left says: 'When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. Learn more [?]'.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 3:

The screenshot shows the 'Configure security group' step of the AWS EC2 instance launch wizard. It includes fields for Subnet (vpc-0223dc77f3ac862c1), Auto-assign public IP (Enabled), and Firewall (security groups) (Create security group selected). Below these, it lists rules for SSH, HTTPS, and HTTP traffic. At the bottom, it shows storage configuration (1x 16 GiB gp3 volume).

Step4:

The screenshot shows the 'Summary' step of the AWS EC2 instance launch wizard. It displays the following details:
Number of instances: 2
Software Image (AMI): Canonical, Ubuntu, 24.04, amd64...
Virtual server type (instance type): t2.micro
Firewall (security group): New security group
Storage (volumes): 1 volume(s) - 16 GiB
At the bottom are 'Cancel', 'Launch instance' (highlighted in orange), and 'Preview code' buttons.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 5:

EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instances (i-0b43dba4ee85b2e52, i-0abe57059201bf0ec)

▶ Launch log

Step 6:

EC2 > Instances

Instances (2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
sanket	i-0abe57059201bf0ec	Running	t2.micro	Initializing	View alarms +	ap-southeast-1b	ec2-54-179-176-83.aj
sanket	i-0b43dba4ee85b2e52	Running	t2.micro	Initializing	View alarms +	ap-southeast-1b	ec2-13-215-178-44.aj

Step 7:

Instances (2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
master	i-0abe57059201bf0ec	Running	t2.micro	Initializing	View alarms +	ap-southeast-1b	ec2-54-179-176-83.aj
slave	i-0b43dba4ee85b2e52	Running	t2.micro	Initializing	View alarms +	ap-southeast-1b	ec2-13-215-178-44.aj

Step 8:

```
ubuntu@master-node:~$
```

```
ubuntu@slave-node:~$
```

Step 9:

```
ubuntu@master-node:~$ sudo apt-get update
Hit:1 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:5 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY



Department of Information Technology

(NBA Accredited)

Step 10:

```
ubuntu@master-node:~$ sudo apt-get install docker.io -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bridge-utils containerd dns-root-data dnsmasq-base pigz runc ubuntu-fan
Suggested packages:
```

Step 11:

```
ubuntu@master-node:~$ sudo systemctl enable docker
ubuntu@master-node:~$ sudo systemctl start docker
ubuntu@master-node:~$ sudo apt-get install -y apt-transport-https ca-certificates curl gpg
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ca-certificates is already the newest version (20240203).
ca-certificates set to manually installed.
curl is already the newest version (8.5.0-2ubuntu10.6).
curl set to manually installed.
gpg is already the newest version (2.4.4-2ubuntu17.3).
gpg set to manually installed.
```

Step 12:

```
ubuntu@master-node:~$ sudo apt-get install -y kubelet kubeadm kubectl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  conntrack cri-tools kubernetes-cni
The following NEW packages will be installed:
  conntrack cri-tools kubeadm kubectl kubelet kubernetes-cni
0 upgraded, 6 newly installed, 0 to remove and 41 not upgraded.
Need to get 93.9 MB of archives.
After this operation, 333 MB of additional disk space will be used.
```

Step 13:

```
ubuntu@master-node:~$ sudo apt-mark hold kubelet kubeadm kubectl
kubelet set on hold.
kubeadm set on hold.
kubectl set on hold.
ubuntu@master-node:~$ sudo systemctl enable --now kubelet
ubuntu@master-node:~$ sudo kubeadm init --pod-network-cidr=10.244.0.0/16 --ignore-preflight-errors=all
[kubelet] Using Kubernetes version: v1.34.1
[preflight] Running pre-flight checks
  [WARNING NumCPU]: the number of available CPUs 1 is less than the required 2
  [WARNING Mem]: the system RAM (957 MB) is less than the minimum 1700 MB
[preflight] Pulling images required for setting up a Kubernetes cluster
[preflight] This might take a minute or two, depending on the speed of your internet connection
[preflight] You can also perform this action beforehand using 'kubeadm config images pull'
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY



Department of Information Technology

(NBA Accredited)

Step 14:

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

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

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

```
export KUBECONFIG=/etc/kubernetes/admin.conf
```

You should now deploy a pod network to the cluster.

Run "kubectl apply -f [podnetwork].yaml" with one of the options listed at:

<https://kubernetes.io/docs/concepts/cluster-administration/addons/>

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

```
kubeadm join 172.31.24.248:6443 --token 42re52.lx5kazbumjyr97ba \
--discovery-token-ca-cert-hash sha256:e11f2ad4603ae8724ebb091f33d64d60678cebf9c24037618867076cd1ca2966
ubuntu@master-node:~$ mkdir -p $HOME/.kube
ubuntu@master-node:~$ sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
ubuntu@master-node:~$ sudo chown $(id -u):$(id -g) $HOME/.kube/config
ubuntu@master-node:~$ kubectl apply -f https://github.com/flannel-io/flannel/releases/latest/download/kube-flannel.yaml
namespace/kube-flannel created
serviceaccount/flannel created
clusterrole.rbac.authorization.k8s.io/flannel created
clusterrolebinding.rbac.authorization.k8s.io/flannel created
configmap/kube-flannel-cfg created
daemonset.apps/kube-flannel-ds created
```

Step 15:

```
ubuntu@master-node:~$ sudo kubeadm join 172.31.24.248:6443 --token 42re52.lx5kazbumjyr97ba --discovery-token-ca-cert-hash sha256:e11f2ad4603ae8724ebb091f33d64d60678cebf9c24037618867076cd1ca2966 --ignore-preflight-errors=all
[preflight] Running pre-flight checks
```

Step 16:

Instances (2) Info		Last updated 2 minutes ago	Connect	Instance state ▾	Actions ▾	Launch instances	▼	
				All states ▾				
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
<input type="checkbox"/>	master	i-0abe57059201bf0ec	Terminated	t2.micro	-	View alarms +	ap-southeast-1b	-
<input type="checkbox"/>	slave	i-0b45dba4ee85b2e52	Terminated	t2.micro	-	View alarms +	ap-southeast-1b	-

Conclusion:

A Kubernetes cluster is a powerful system built on a Control Plane (managing the cluster state) and Worker Nodes (running containerized apps). Deploying a cluster successfully validates this architecture, establishing a scalable and resilient foundation for modern application orchestration.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)

**Semester:V****Academic Year: 2025-26****Class/Branch: TE IT****Subject: Advanced DevOps Lab (ADL)****Name of Instructor: Prof. Vishal Badgujar****Name of Student:Sanket B. Bhoir****Student ID: 24204022**

EXPERIMENT NO. 05

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

Step 01: Terraform uses HashiCorp Configuration Language (HCL) to manage environments of Operators and Infrastructure teams. To download go to site <https://www.terraform.io/downloads.html> Select the appropriate package for your operating system and architecture

The screenshot shows the HashiCorp Terraform website's "Install" section for Linux. On the left, a sidebar lists operating systems: macOS, Windows, Linux (selected), FreeBSD, OpenBSD, Solaris, Release information, Next steps, and Resources. The main content area has tabs for Ubuntu/Debian, CentOS/RHEL, Fedora 40, Fedora 41, Amazon Linux, and Homebrew. Under the Ubuntu/Debian tab, a terminal window shows the command: `wget -O - https://apt.releases.hashicorp.com/gpg | sudo gpg --dearmor -o /usr/share/keyrings/hashicorp-archive-keyring.gpg`. Below this, there are four download buttons: "386 Version: 1.12.2 Download", "AMD64 Version: 1.12.2 Download", "ARM Version: 1.12.2 Download", and "ARM64 Version: 1.12.2 Download". At the bottom, a "Note" box states: "Complete this [tutorial](#) to learn how to install and verify HashiCorp tools on any Linux distribution, and create a custom Linux container with verified HashiCorp tools."

Step 02: Change the directory to unzipped folder

```
psit@psit-HP-ProDesk-600-G4-PCI-MT:~$ cd Downloads
psit@psit-HP-ProDesk-600-G4-PCI-MT:~/Downloads$ cd terraform_1.12.2_linux_amd64
```

Step 03: Move the terraform binary to a directory included in your system's PATH in my case usr/local/bin/ and check if Terraform is installed or not.

```
psit@psit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/terraform_1.12.2_linux_amd64$ sudo mv terraform /usr/local/bin
[sudo] password for psit:
psit@psit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/terraform_1.12.2_linux_amd64$ terraform -v
Terraform v1.12.2
on linux_amd64
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Conclusion:

I learned the basic concepts of Terraform, including its core components and how it works. I also successfully installed Terraform on a Linux machine. This helped me understand how Terraform is used to manage and automate infrastructure easily.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)

**Semester:V****Academic Year: 2025-26****Class/Branch: TE IT****Subject: Advanced DevOps Lab (ADL)****Name of Instructor: Prof. Vishal Badgujar****Name of Student:Sanket B. Bhoir****Student ID: 24204022**

EXPERIMENT NO. 06

Aim: To Build, change, and destroy AWS infrastructure Using Terraform.

Step 01: Install the AWS CLI version 2 on Linux

```
psit@psit-HP-ProDesk-600-G4-PCI-MT:~$ sudo apt-get install curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
curl is already the newest version (7.58.0-2ubuntu3.24).
The following packages were automatically installed and are no longer required:
  gyp javascript-common libhttp-parser2.7.1 libjs-async libjs-inherits libjs-jquery libjs-node-uuid libjs-underscore libssl1.0-dev libuv1-dev
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
```

Step 02: Create a new access key. Make sure you download the keys in your local machine.

The screenshot shows the AWS IAM Access Keys page. At the top, there is a heading "Access keys (0)" and a "Create access key" button. Below this, a message states "Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time." A "Learn more" link is provided. The main table has columns: Access key ID, Created on, Access key last used, Region last used, Service last used, and Status. A note below the table says "No access keys" and advises against using long-term credentials like access keys. It also provides a "Create access key" button.

The screenshot shows the "Create access key" wizard, Step 2: "Retrieve access key". The title is "Access key". It says, "If you lose or forget your secret access key, you cannot recover it later. However, you can create a new access key any time." There are two fields: "Access key" (containing "AKIASJSV5ESBJR22TYEXK") and "Secret access key" (containing a redacted string). Below this is a section titled "Access key best practices" with a bulleted list: "Never store your access key in plain text, in a code repository, or in code.", "Disable or delete access key when no longer needed.", "Enable least-privilege permissions.", and "Rotate access keys regularly.". A note at the bottom says, "For more details about managing access keys, see the [best practices for managing AWS access keys](#)".



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Access keys (1)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

[Actions ▾](#)[Create access key](#)

Access key ID	Created on	Access key last used	Region last used	Service last used	Status
AKIASJSVESBJR22TYEXK	1 minute ago	None	N/A	N/A	Active

Step 03:

```
psit@psit-HP-ProDesk-600-G4-PCI-MT:~/awscliv2$ aws configure
AWS Access Key ID [*****KFIK]: AKIASJSVESBJR22TYEXK
AWS Secret Access Key [*****DjFh]: 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
Default region name [ap-south-1]: ap-south-1
Default output format [None]:
```

Step 04:

Key pairs Info		Actions ▾	Create key pair
<input type="text"/> Find Key Pair by attribute or tag			
<input type="checkbox"/>	Name	Type	Created
No key pairs to display			

Create key pair [Info](#)

Key pair
A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

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

Key pair type [Info](#)
 RSA ED25519

Private key file format
 .pem For use with OpenSSH
 .ppk For use with PuTTY

Tags - optional
No tags associated with the resource.
[Add new tag](#)
You can add up to 50 more tags.

Successfully created key pair ×

Key pairs (1) Info		Actions ▾	Create key pair
<input type="text"/> Find Key Pair by attribute or tag			
<input type="checkbox"/>	Name	Type	Created

terraform rsa 2025/08/12 15:41 GMT+5:30 51:51:66:5c:63:da:19:a3:cb:bb:ef:03:2d:e8:87:7c... key-Off920...



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 05:

```
psit@psit-HP-ProDesk-600-G4-PCI-MT:~/awscliv2$ cd
psit@psit-HP-ProDesk-600-G4-PCI-MT:~$ cd Downloads
psit@psit-HP-ProDesk-600-G4-PCI-MT:~/Downloads$ mkdir sanket
psit@psit-HP-ProDesk-600-G4-PCI-MT:~/Downloads$ cd sanket
psit@psit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/sanket$ sudo nano variables.tf
psit@psit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/sanket$ sudo nano main.tf
psit@psit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/sanket$ terraform init
Initializing the backend...
Initializing provider plugins...
- Finding latest version of hashicorp/aws...
- Installing hashicorp/aws v6.8.0...
- Installed hashicorp/aws v6.8.0 (signed by HashiCorp)
Terraform has created a lock file .terraform.lock.hcl to record the provider
selections it made above. Include this file in your version control repository
so that Terraform can guarantee to make the same selections by default when
you run "terraform init" in the future.

Terraform has been successfully initialized!

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

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

Step 06:

```
psit@psit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/sanket$ terraform plan
Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the following symbols:
+ create

Terraform will perform the following actions:

# aws_instance.myFirstInstance will be created
+ resource "aws_instance" "myFirstInstance" {
    + ami                                = "ami-0f918f7e67a3323f0"
    + arn                                = (known after apply)
    + associate_public_ip_address        = (known after apply)
    + availability_zone                  = (known after apply)
    + disable_api_stop                   = (known after apply)
    + disable_api_termination            = (known after apply)
    + ebs_optimized                      = (known after apply)
    + enable_primary_ipv6                = (known after apply)
    + force_destroy                      = false
    + get_password_data                 = false
    + tags_all                           = {
        + "Name" = "security_jenkins_port"
    }
    + vpc_id                            = (known after apply)
}

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



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY



Department of Information Technology

(NBA Accredited)

Step 07:

```
psit@psit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/sanket$ terraform apply
aws_security_group.security_jenkins_port: Refreshing state... [id=sg-0c54809cf6231414]

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

Terraform will perform the following actions:

# aws_instance.myFirstInstance will be created
+ resource "aws_instance" "myFirstInstance" {
    + ami                               = "ami-0f918f7e67a3323f0"
    + arn                             = (known after apply)
    + associate_public_ip_address      = (known after apply)

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

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

Enter a value: yes

aws_instance.myFirstInstance: Creating...
aws_instance.myFirstInstance: Still creating... [00m10s elapsed]
aws_instance.myFirstInstance: Still creating... [00m20s elapsed]
aws_instance.myFirstInstance: Creation complete after 21s [id=i-0d39009e8edd100eb]

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

Step 08:

The screenshot shows the AWS EC2 Instances page. On the left sidebar, under the 'Instances' section, 'Instances' is selected. In the main content area, there is a table titled 'Instances (1)'. It shows one instance: 'jenkins_Instance' with ID 'i-0d39009e8edd100eb', which is currently 'Running'. The table includes columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. The Public IPv4 DNS is listed as 'ec2-65-0-89-29.ap-southeast-1.amazonaws.com'.

Step 09:

```
psit@psit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/sanket$ terraform destroy
aws_security_group.security_jenkins_port: Refreshing state... [id=sg-0c54809cf6231414]
aws_instance.myFirstInstance: Refreshing state... [id=i-0d39009e8edd100eb]

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

Enter a value: yes

aws_security_group.security_jenkins_port: Destroying... [id=sg-0c54809cf6231414]
aws_instance.myFirstInstance: Destroying... [id=i-0d39009e8edd100eb]
aws_security_group.security_jenkins_port: Still destroying... [id=sg-0c54809cf6231414, 00m10s elapsed]
aws_instance.myFirstInstance: Still destroying... [id=i-0d39009e8edd100eb, 00m10s elapsed]
aws_security_group.security_jenkins_port: Still destroying... [id=sg-0c54809cf6231414, 00m20s elapsed]
aws_instance.myFirstInstance: Still destroying... [id=i-0d39009e8edd100eb, 00m20s elapsed]
aws_instance.myFirstInstance: Destruction complete after 30s
aws_security_group.security_jenkins_port: Still destroying... [id=sg-0c54809cf6231414, 00m30s elapsed]
aws_security_group.security_jenkins_port: Destruction complete after 37s

Destroy complete! Resources: 2 destroyed.
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 10:

The screenshot shows the AWS EC2 Instances page. The sidebar on the left is titled 'EC2' and includes 'Dashboard', 'EC2 Global View', 'Events', and a expanded 'Instances' section with 'Instances', 'Instance Types', and 'Launch Templates'. The main content area has a header 'Instances (1) Info' with filters for 'Name', 'Instance ID', 'Instance state', 'Instance type', 'Status check', 'Alarm status', 'Availability Zone', and 'Public IPv4 DNS'. A search bar says 'Find Instance by attribute or tag (case-sensitive)' and a dropdown says 'All states'. Below the header is a table with one row: Jenkins_Instance (I-0d39009e8edd100eb), Terminated, t2.micro, - (Status check), View alarms +, ap-south-1a (Availability Zone), and - (Public IPv4 DNS). A status bar at the bottom says 'Last updated less than a minute ago'.

The screenshot shows the AWS EC2 Instances page after the instance has been terminated. The main content area has a green success message 'Successfully initiated termination (deletion) of I-0d39009e8edd100eb'. The table below shows the same instance information as the previous screenshot, but the 'Status check' column now shows a red minus sign, indicating the instance is no longer active.

Conclusion:

By writing configuration files, I successfully created an EC2 instance on command line interface using Access key and Key-pair.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Semester:V

Academic Year: 2025-26

Class/Branch: TE IT

Subject: Advanced DevOps Lab (ADL)

Name of Instructor: Prof. Vishal Badgujar

Name of Student:Sanket B. Bhoir

Student ID: 24204022

EXPERIMENT NO. 07

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

Step 01:

The screenshot shows the Jenkins dashboard at localhost:8080. The page title is "Welcome to Jenkins!". It features a sidebar with links for "New Item", "Build History", "Build Queue" (which shows "No builds in the queue."), and "Build Executor Status" (which shows "0/2"). The main content area has sections for "Start building your software project" (with a "Create a job" button) and "Set up a distributed build" (with links for "Set up an agent", "Configure a cloud", and "Learn more about distributed builds"). At the bottom right, there are links for "REST API" and "Jenkins 2.516.2".

Step 02:

```
psit@psit-HP-ProDesk-600-G4-PCI-MT:~$ sudo docker run -d -p 9000:9000 sonarqube
[sudo] password for psit:
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
76249c7cd503: Pull complete
f706b5aed643: Pull complete
929e753abe01: Pull complete
9eb9a8044837: Pull complete
5d5a1fad7028: Pull complete
47f8c849269d: Pull complete
e869ea04c9ac: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:963c88705b11923b205ebc9101c9031104b9af6c46a2c124e8bade6e9f2dcc83
Status: Downloaded newer image for sonarqube:latest
9cab89a636042675bf550eaa37cfbb2fc43d3c40843708504297f5d42ef218ec
psit@psit-HP-ProDesk-600-G4-PCI-MT:~$ |
```



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Step 03:

Log in to SonarQube

Login *

Password *

Go back **Log in**

Step 04:

Generate Tokens

Name	Type	Expires in	
jenkin	User Token	No expiration	Generate

Step 05:

Token : squ_f4146403d695680c1dda4199e7e7c09767666817

Generate Tokens

Name	Type	Expires in	
Enter Token Name	Select Token Type	30 days	Generate

New token "jenkin" has been created. Make sure you copy it now, you won't be able to see it again!

squ_f4146403d695680c1dda4199e7e7c09767666817

Name	Type	Project	Last use	Created	Expiration
jenkin	User		Never	September 9, 2025	-



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Step 06:

The screenshot shows the Jenkins plugin manager interface. A search bar at the top contains the text "sonarQube". Below it, a table lists three available plugins:

Install	Name	Released	Health
<input checked="" type="checkbox"/>	SonarQube Scanner 2.18	7 mo 13 days ago	84
<input type="checkbox"/>	Sonar Gerrit 388.v9b_f1cb_e42306	1 yr 3 mo ago	86
<input type="checkbox"/>	SonarQube Generic Coverage 1.0	6 yr 1 mo ago	76

The "SonarQube Scanner" plugin is selected and has a green checkmark in the "Install" column.

Step 07:

The screenshot shows the Jenkins global tool configuration page for SonarQube installations. It displays a single entry for "SonarQube" with the following details:

- Name:** SonarQube
- Server URL:** http://localhost:9000
- Server authentication token:** - none - (dropdown menu)
- Add SonarQube** button
- Save** and **Apply** buttons at the bottom



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 08:

Jenkins Credentials Provider: Jenkins

Add Credentials

Domain

Global credentials (unrestricted)

Kind

Secret text

Scope ?

Global (Jenkins, nodes, items, all child items, etc)

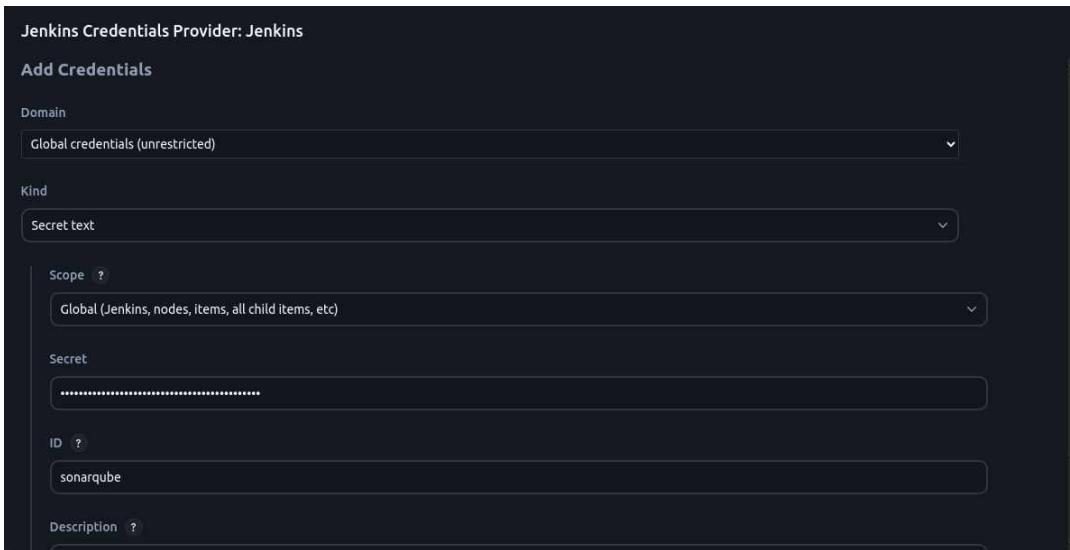
Secret

.....

ID ?

sonarqube

Description ?



Step 09:

SonarQube installations

List of SonarQube installations

Name

SonarQube

Server URL

Default is http://localhost:9000

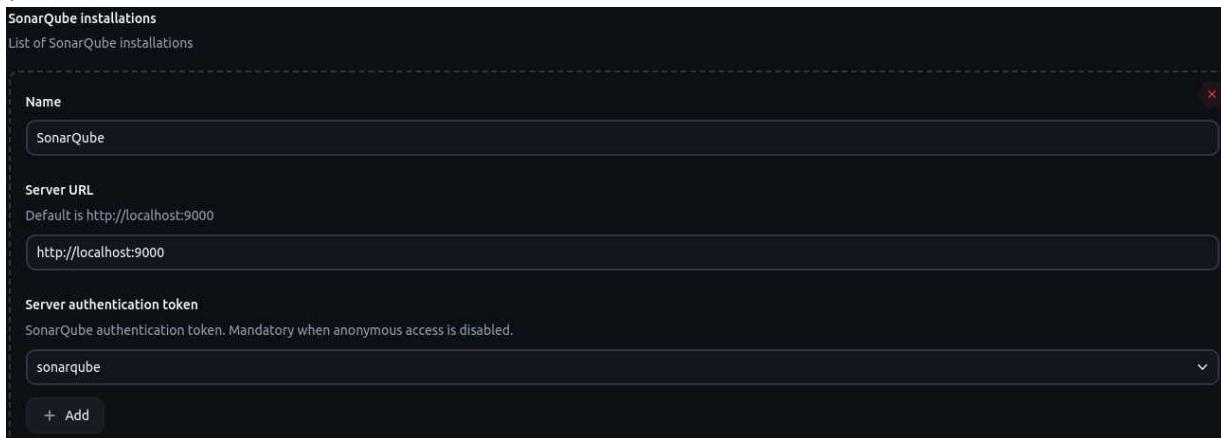
http://localhost:9000

Server authentication token

SonarQube authentication token. Mandatory when anonymous access is disabled.

sonarqube

+ Add



Step 10:

SonarQube Scanner installations

Add SonarQube Scanner

SonarQube Scanner

Name

SonarQube

Install automatically ?

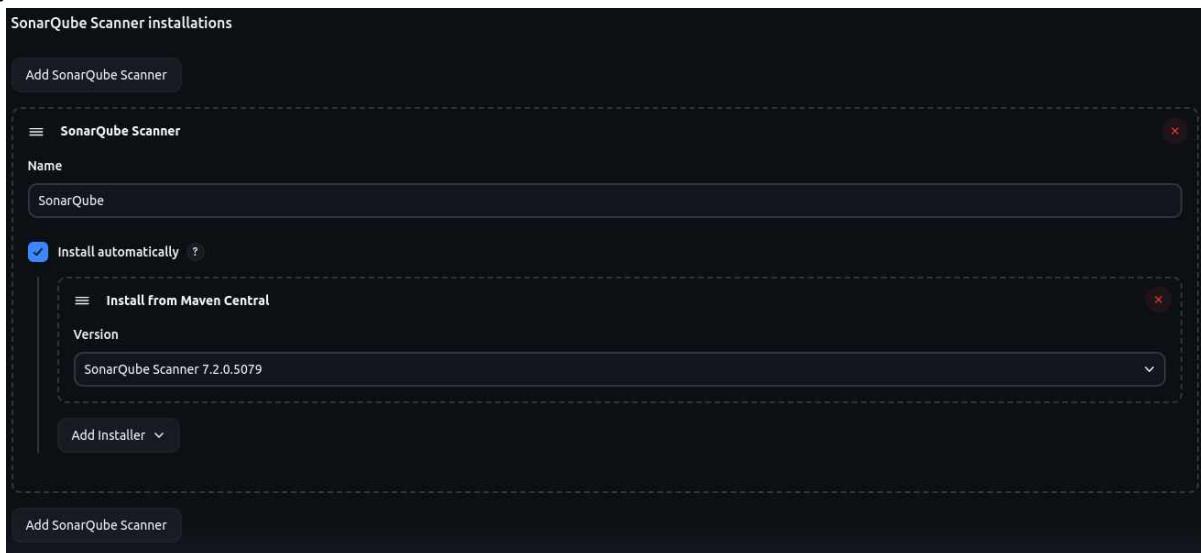
Install from Maven Central

Version

SonarQube Scanner 7.2.0.5079

Add Installer

Add SonarQube Scanner





PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 11:

New Item

Enter an item name
SonarQube

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.
- Pipeline**
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.
- Multi-configuration project**
Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.
- Folder**
Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a Folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.
- Multibranch Pipeline**

OK

Step 12:

General

Enabled

Description
Hello pipeline job

Plain text [Preview](#)

Discard old builds ?

Do not allow concurrent builds

Do not allow the pipeline to resume if the controller restarts

GitHub project

Project url ?
<https://github.com/vishal003/jenkins-sonarqube/>

Advanced ▾

Pipeline speed/durability override ?

Save Apply



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Step 13:

Definition

Pipeline script

```
Script ?  
try sample Pipeline...  
1 node  
2 {  
3   stage('cloning from GIT'){  
4     git branch: 'main', credentialsId: 'GIT_REPO', url: 'https://github.com/vishal003/jenkins-sonarqube.git'  
5   }  
6 }
```

Use Groovy Sandbox ?

Pipeline Syntax

Save Apply

Step 14:

Jenkins / SonarQube

Status

</> Changes
▷ Build Now
⚙ Configure
🗑 Delete Pipeline
GitHub
☰ Stages
✍ Rename
Pipeline Syntax

SonarQube

Hello pipeline job

Permalinks

Builds

Today
#1 16:19



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY



Department of Information Technology

(NBA Accredited)

Step 15:

Jenkins / SonarQube / #1

Replay Pipeline Steps Workspaces

```
Cloning repository https://github.com/vishal003/jenkins-sonarqube.git
> git init /var/lib/jenkins/workspace/SonarQube # timeout=10
Fetching upstream changes from https://github.com/vishal003/jenkins-sonarqube.git
> git --version # timeout=10
> git --version # 'git version 2.17.1'
> git fetch --tags --progress -- https://github.com/vishal003/jenkins-sonarqube.git +refs/head
> git config remote.origin.url https://github.com/vishal003/jenkins-sonarqube.git # timeout=10
> git config --add remote.origin.fetch +refs/heads/*:refs/remotes/origin/* # timeout=10
Avoid second fetch
> git rev-parse refs/remotes/origin/main^{commit} # timeout=10
Checking out Revision 80c34f4818e25f7733e50784c2f7639d9884ed90 (refs/remotes/origin/main)
> git config core.sparsecheckout # timeout=10
> git checkout -f 80c34f4818e25f7733e50784c2f7639d9884ed90 # timeout=10
> git branch -a -v --no-abbrev # timeout=10
> git checkout -b main 80c34f4818e25f7733e50784c2f7639d9884ed90 # timeout=10
Commit message: "Update README.md"
First time build. Skipping changelog.
[Pipeline] 
[Pipeline] // stage
[Pipeline] 
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

Conclusion:

Thus we have successfully installed Jenkins and SonarQube and I have created for pipeline for CI with Jenkins and SonarQube using GitHub repository



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Semester: V

Academic Year: 2025-26

Class / Branch: TE IT

Subject: Advanced DevOps Lab (ADL)

Name of Instructor: Prof. Vishal Badgujar

Name of Student: Sanket B. Bhoir

Student ID: 24204022

EXPERIMENT NO. 08

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

Step 01:

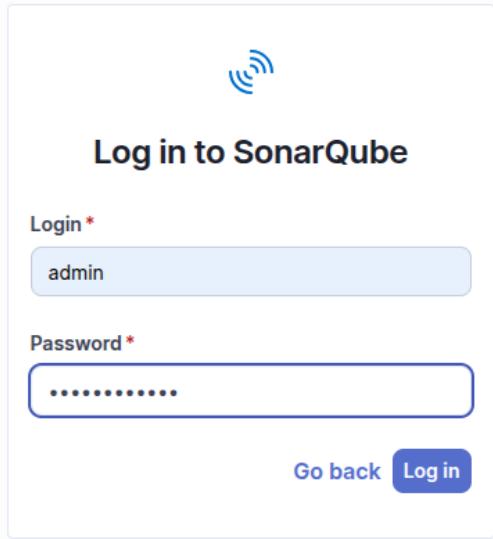
The screenshot shows the Jenkins dashboard at localhost:8080. The main header says "Welcome to Jenkins!". Below it, a message states: "This page is where your Jenkins jobs will be displayed. To get started, you can set up distributed builds or start building a software project." There are several buttons and links: "Start building your software project" (with "Create a job" and "+"), "Set up a distributed build" (with "Set up an agent", "Configure a cloud", and "Learn more about distributed builds"). On the left sidebar, there are links for "New item", "Build History", "Build Queue" (which shows "No builds in the queue."), and "Build Executor Status" (which shows "0/2"). At the bottom right, it says "REST API" and "Jenkins 2.516.2".

Step 02:

```
psit@psit-HP-ProDesk-600-G4-PCI-MT:~$ sudo docker run -d -p 9000:9000 sonarqube
[sudo] password for psit:
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
76249c7cd503: Pull complete
f706b5aed643: Pull complete
929e753abe01: Pull complete
9eb9a8044837: Pull complete
5d5a1fad7028: Pull complete
47f8c849269d: Pull complete
e869ea04c9ac: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:963c88705b11923b205ebc9101c9031104b9af6c46a2c124e8bade6e9f2dcc83
Status: Downloaded newer image for sonarqube:latest
9cab89a636042675bf550eaa37cfbb2fc43d3c40843708504297f5d42ef218ec
psit@psit-HP-ProDesk-600-G4-PCI-MT:~$ |
```



Step 03:



The SonarQube login screen displays a placeholder token 'soanrqube' in a large text area above the login fields. The placeholder is enclosed in a light gray box with a green checkmark icon and the text 'New token "soanrqube" has been created. Make sure you copy it now, you won't be able to see it again!'. Below the placeholder, there is a text input field containing 'sqa_413efd821ca53afa4a9f535265cca8d28016c9f6' with a copy icon next to it.

Log in to SonarQube

Login *

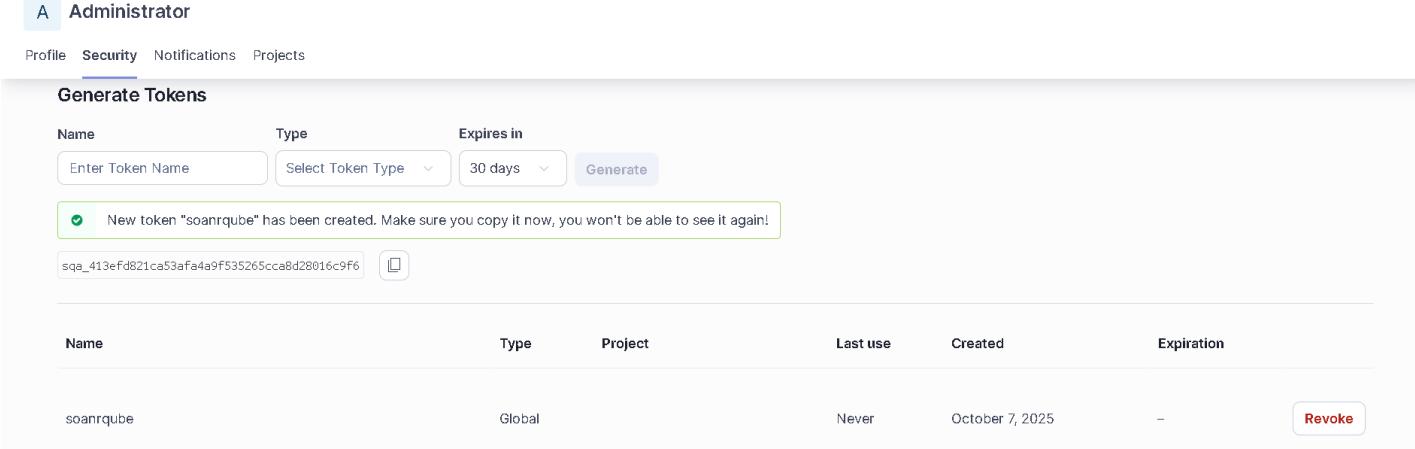
admin

Password *

.....

Go back Log in

Step 04:



The screenshot shows the 'Generate Tokens' section of the SonarQube interface. It includes fields for 'Name', 'Type' (set to 'Select Token Type'), and 'Expires in' (set to '30 days'). A 'Generate' button is present. A success message indicates a new token 'soanrqube' has been created. The token value 'sqa_413efd821ca53afa4a9f535265cca8d28016c9f6' is displayed with a copy icon. A table lists existing tokens, showing one entry for 'soanrqube' with details: Type 'Global', Last use 'Never', Created 'October 7, 2025', and an 'Expiration' column with a red 'Revoke' link.

Name	Type	Project	Last use	Created	Expiration
soanrqube	Global		Never	October 7, 2025	Revoke



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Step 05:

Jenkins / Manage Jenkins / Plugins

Plugins

Updates Available plugins Installed plugins Advanced settings Download progress

Search: sonarqube

Install Name Released Health

Install	Name	Released	Health
<input checked="" type="checkbox"/>	SonarQube Scanner 2.18	External Site/Tool Integrations Build Reports	8 mo 12 days ago 84
<input type="checkbox"/>	Sonar Gerrit 388.v9b_f1db_e42306	External Site/Tool Integrations	1 yr 4 mo ago 86
<input type="checkbox"/>	SonarQube Generic Coverage 1.0	TODO	6 yr 2 mo ago 76

Step 06:

Jenkins / Manage Jenkins / Credentials

Credentials

T	P	Store	Domain	ID	Name
		System	(global)	SonarQube	SonarQube

Stores scoped to Jenkins

P	Store	Domains
	System	(global)

Icon: S M L

SonarQube installations

List of SonarQube installations

Name: SonarQube

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

Server URL: <http://3.1.20.130:9000>

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

Server authentication token: SonarQube

Advanced ▾

Save Apply



Step 07:

New Item

Enter an item name

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.

 **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.

 **OK**

Step 08:

Configure

-  General
-  Triggers
-  Pipeline
-  Advanced

Plain text [Preview](#)

Discard old builds [?](#)

Do not allow concurrent builds

Do not allow the pipeline to resume if the controller restarts

GitHub project

Project url [?](#)

<https://github.com/Sanketbhoir03/jenkins-sonarqube/>

Step 09:

Pipeline

Define your Pipeline using Groovy directly or pull it from source control.

Definition

Pipeline script

```
Script ?  
try sample Pipeline...  
  
1 v pipeline {  
2   agent any  
3   tools {  
4     maven 'M3'  
5   }  
6   stages {  
7     stage('Cloning from GIT') {  
8       steps {  
9         git branch: 'main', url: 'http://github.com/Sanketbhoir03/jenkins-sonarqube.git'  
10      }  
11    }  
12    stage('SonarQube Analysis') {  
13      steps {  
14        withSonarQubeEnv('sonarQube') {  
15        }  
16      }  
17    }  
18  }  
19}  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
3310  
3311  
3312  
3313  
3314  
3315  
3316  
3317  
3318  
3319  
3320  
3321  
3322  
3323  
3324  
3325  
3326  
3327  
3328  
3329  
3330  
3331  
3332  
3333  
3334  
3335  
3336  
3337  
3338  
3339  
33310  
33311  
33312  
33313  
33314  
33315  
33316  
33317  
33318  
33319  
33320  
33321  
33322  
33323  
33324  
33325  
33326  
33327  
33328  
33329  
33330  
33331  
33332  
33333  
33334  
33335  
33336  
33337  
33338  
33339  
333310  
333311  
333312  
333313  
333314  
333315  
333316  
333317  
333318  
333319  
333320  
333321  
333322  
333323  
333324  
333325  
333326  
333327  
333328  
333329  
333330  
333331  
333332  
333333  
333334  
333335  
333336  
333337  
333338  
333339  
3333310  
3333311  
3333312  
3333313  
3333314  
3333315  
3333316  
3333317  
3333318  
3333319  
3333320  
3333321  
3333322  
3333323  
3333324  
3333325  
3333326  
3333327  
3333328  
3333329  
3333330  
3333331  
3333332  
3333333  
3333334  
3333335  
3333336  
3333337  
3333338  
3333339  
33333310  
33333311  
33333312  
33333313  
33333314  
33333315  
33333316  
33333317  
33333318  
33333319  
33333320  
33333321  
33333322  
33333323  
33333324  
33333325  
33333326  
33333327  
33333328  
33333329  
33333330  
33333331  
33333332  
33333333  
33333334  
33333335  
33333336  
33333337  
33333338  
33333339  
333333310  
333333311  
333333312  
333333313  
333333314  
333333315  
333333316  
333333317  
333333318  
333333319  
333333320  
333333321  
333333322  
333333323  
333333324  
333333325  
333333326  
333333327  
333333328  
333333329  
333333330  
333333331  
333333332  
333333333  
333333334  
333333335  
333333336  
333333337  
333333338  
333333339  
3333333310  
3333333311  
3333333312  
3333333313  
3333333314  
3333333315  
3333333316  
3333333317  
3333333318  
3333333319  
3333333320  
3333333321  
3333333322  
3333333323  
3333333324  
3333333325  
3333333326  
3333333327  
3333333328  
3333333329  
3333333330  
3333333331  
3333333332  
3333333333  
3333333334  
3333333335  
3333333336  
3333333337  
3333333338  
3333333339  
33333333310  
33333333311  
33333333312  
33333333313  
33333333314  
33333333315  
33333333316  
33333333317  
33333333318  
33333333319  
33333333320  
33333333321  
33333333322  
33333333323  
33333333324  
33333333325  
33333333326  
33333333327  
33333333328  
33333333329  
33333333330  
33333333331  
33333333332  
33333333333  
33333333334  
33333333335  
33333333336  
33333333337  
33333333338  
33333333339  
333333333310  
333333333311  
333333333312  
333333333313  
333333333314  
333333333315  
333333333316  
333333333317  
333333333318  
333333333319  
333333333320  
333333333321  
333333333322  
333333333323  
333333333324  
333333333325  
333333333326  
333333333327  
333333333328  
333333333329  
333333333330  
333333333331  
333333333332  
333333333333  
333333333334  
333333333335  
333333333336  
333333333337  
333333333338  
333333333339  
3333333333310  
3333333333311  
3333333333312  
3333333333313  
3333333333314  
3333333333315  
3333333333316  
3333333333317  
3333333333318  
3333333333319  
3333333333320  
3333333333321  
3333333333322  
3333333333323  
3333333333324  
3333333333325  
3333333333326  
3333333333327  
3333333333328  
3333333333329  
3333333333330  
3333333333331  
3333333333332  
3333333333333  
3333333333334  
3333333333335  
3333333333336  
3333333333337  
3333333333338  
3333333333339  
33333333333310  
33333333333311  
33333333333312  
33333333333313  
33333333333314  
33333333333315  
33333333333316  
33333333333317  
33333333333318  
33333333333319  
33333333333320  
33333333333321  
33333333333322  
33333333333323  
33333333333324  
33333333333325  
33333333333326  
33333333333327  
33333333333328  
33333333333329  
33333333333330  
33333333333331  
33333333333332  
33333333333333  
33333333333334  
33333333333335  
33333333333336  
33333333333337  
33333333333338  
33333333333339  
333333333333310  
333333333333311  
333333333333312  
333333333333313  
333333333333314  
333333333333315  
333333333333316  
333333333333317  
333333333333318  
333333333333319  
333333333333320  
333333333333321  
333333333333322  
333333333333323  
333333333333324  
333333333333325  
333333333333326  
333333333333327  
333333333333328  
333333333333329  
333333333333330  
333333333333331  
333333333333332  
333333333333333  
333333333333334  
333333333333335  
333333333333336  
333333333333337  
333333333333338  
333333333333339  
3333333333333310  
3333333333333311  
3333333333333312  
3333333333333313  
3333333333333314  
3333333333333315  
3333333333333316  
3333333333333317  
3333333333333318  
3333333333333319  
3333333333333320  
3333333333333321  
3333333333333322  
3333333333333323  
3333333333333324  
3333333333333325  
3333333333333326  
3333333333333327  
3333333333333328  
3333333333333329  
3333333333333330  
3333333333333331  
3333333333333332  
3333333333333333  
3333333333333334  
3333333333333335  
3333333333333336  
3333333333333337  
3333333333333338  
3333333333333339  
33333333333333310  
33333333333333311  
33333333333333312  
33333333333333313  
33333333333333314  
33333333333333315  
33333333333333316  
33333333333333317  
33333333333333318  
33333333333333319  
33333333333333320  
33333333333333321  
33333333333333322  
33333333333333323  
33333333333333324  
33333333333333325  
33333333333333326  
33333333333333327  
33333333333333328  
33333333333333329  
33333333333333330  
33333333333333331  
33333333333333332  
33333333333333333  
33333333333333334  
33333333333333335  
33333333333333336  
33333333333333337  
33333333333333338  
33333333333333339  
333333333333333310  
333333333333333311  
333333333333333312  
333333333333333313  
333333333333333314  
333333333333333315  
333333333333333316  
333333333333333317  
333333333333333318  
333333333333333319  
333333333333333320  
333333333333333321  
333333333333333322  
333333333333333323  
333333333333333324  
333333333333333325  
333333333333333326  
333333333333333327  
333333333333333328  
333333333333333329  
333333333333333330  
333333333333333331  
333333333333333332  
333333333333333333  
333333333333333334  
333333333333333335  
333333333333333336  
333333333333333337  
333333333333333338  
333333333333333339  
3333333333333333310  
3333333333333333311  
3333333333333333312  
3333333333333333313  
3333333333333333314  
3333333333333333315  
3333333333333333316  
3333333333333333317  
3333333333333333318  
3333333333333333319  
3333333333333333320  
3333333333333333321  
3333333333333333322  
3333333333333333323  
3333333333333333324  
3333333333333333325  
3333333333333333326  
3333333333333333327  
3333333333333333328  
3333333333333333329  
3333333333333333330  
3333333333333333331  
3333333333333333332  
3333333333333333333  
3333333333333333334  
3333333333333333335  
3333333333333333336  
3333333333333333337  
3333333333333333338  
3333333333333333339  
33333333333333333310  
33333333333333333311  
33333333333333333312  
33333333333333333313  
33333333333333333314  
33333333333333333315  
33333333333333333316  
33333333333333333317  
33333333333333333318  
33333333333333333319  
33333333333333333320  
33333333333333333321  
33333333333333333322  
33333333333333333323  
33333333333333333324  
33333333333333333325  
33333333333333333326  
33333333333333333327  
33333333333333333328  
33333333333333333329  
33333333333333333330  
33333333333333333331  
33333333333333333332  
33333333333333333333  
33333333333333333334  
33333333333333333335  
33333333333333333336  
33333333333333333337  
33333333333333333338  
33333333333333333339  
333333333333333333310  
333333333333333333311  
333333333333333333312  
333333333333333333313  
333333333333333333314  
333333333333333333315  
333333333333333333316  
333333333333333333317  
333333333333333333318  
333333333333333333319  
333333333333333333320  
333333333333333333321  
333333333333333333322  
333333333333333333323  
333333333333333333324  
333333333333333333325  
333333333333333333326  
333333333333333333327  
333333333333333333328  
333333333333333333329  
333333333333333333330  
333333333333333333331  
333333333333333333332  
333333333333333333333  
333333333333333333334  
333333333333333333335  
333333333333333333336  
333333333333333333337  
333333333333333333338  
333333333333333333339  
3333333333333333333310  
3333333333333333333311  
3333333333333333333312  
3333333333333333333313  
3333333333333333333314  
3333333333333333333315  
3333333333333333333316  
3333333333333333333317  
3333333333333333333318  
3333333333333333333319  
3333333333333333333320  
3333333333333333333321  
3333333333333333333322  
3333333333333333333323  
3333333333333333333324  
3333333333333333333325  
3333333333333333333326  
3333333333333333333327  
3333333333333333333328  
3333333333333333333329  
3333333333333333333330  
3333333333333333333331  
3333333333333333333332  
3333333333333333333333  
3333333333333333333334  
3333333333333333333335  
3333333333333333333336  
3333333333333333333337  
3333333333333333333338  
3333333333333333333339  
33333333333333333333310  
33333333333333333333311  
33333333333333333333312  
33333333333333333333313  
33333333333333333333314  
33333333333333333333315  
33333333333333333333316  
33333333333333333333317  
33333333333333333333318  
33333333333333333333319  
33333333333333333333320  
33333333333333333333321  
33333333333333333333322  
33333333333333333333323  
33333333333333333333324  
33333333333333333333325  
33333333333333333333326  
33333333333333333333327  
33333333333333333333328  
33333333333333333333329  
33333333333333333333330  
33333333333333333333331  
33333333333333333333332  
33333333333333333333333  
33333333333333333333334  
33333333333333333333335  
33333333333333333333336  
33333333333333333333337  
33333333333333333333338  
33333333333333333333339  
333333333333333333333310  
333333333333333333333311  
333333333333333333333312  
333333333333333333333313  
333333333333333333333314  
333333333333333333333315  
333333333333333333333316  
333333333333333333333317  
333333333333333333333318  
333333333333333333333319  
333333333333333333333320  
333333333333333333333321  
333333333333333333333322  
333333333333333333333323  
333333333333333333333324  
333333333333333333333325  
333333333333333333333326  
333333333333333333333327  
333333333333333333333328  
333333333333333333333329  
333333333333333333333330  
333333333333333333333331  
333333333333333333333332  
333333333333333333333333  
333333333333333333333334  
333333333333333333333335  
333333333333333333333336  
333333333333333333333337  
333333333333333333333338  
333333333333333333333339  
3333333333333333333333310  
3333333333333333333333311  
3333333333333333333333312  
3333333333333333333333313  
3333333333333333333333314  
3333333333333333333333315  
3333333333333333333333316  
3333333333333333333333317  
3333333333333333333333318  
3333333333333333333333319  
3333333333333333333333320  
3333333333333333333333321  
3333333333333333333333322  
3333333333333333333333323  
3333333333333333333333324  
3333333333333333333333325  
3333333333333333333333326  
3333333333333333333333327  
3333333333333333333333328  

```



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Step 10:



Jenkins / SonarQube / #9 / Console Output

- Status
- Changes
- Console Output
- Edit Build Information
- Delete build '#9'
- Timings
- Git Build Data
- Pipeline Overview
- Restart from Stage
- Replay
- Pipeline Steps
- Workspaces
- Previous Build

Console Output

```
Started by user Sanket B. Bhoir
[Pipeline] Start of Pipeline
[Pipeline] node
Running on Jenkins in /var/lib/jenkins/workspace/SonarQube
[Pipeline] {
[Pipeline] stage
[Pipeline] { (Declarative: Tool Install)
[Pipeline] tool
[Pipeline] envVarsForTool
[Pipeline] }
[Pipeline] // stage
[Pipeline] withEnv
[Pipeline] {
[Pipeline] stage
[Pipeline] { (Cloning from GIT)
[Pipeline] tool
[Pipeline] envVarsForTool
[Pipeline] withEnv
[Pipeline] {
[Pipeline] git
The recommended git tool is: NONE
No credentials specified
> git rev-parse --resolve-git-dir /var/lib/jenkins/workspace/SonarQube/.git # timeout=10
```

```
[INFO] Analysis report compressed in 29ms, zip size=33.1 kB
[INFO] Analysis report uploaded in 598ms
[INFO] ANALYSIS SUCCESSFUL, you can find the results at: http://3.1.20.130:9000/dashboard?id=com.sonarqube.example%3Asonarqube-maven-example
[INFO] Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
[INFO] More about the report processing at http://3.1.20.130:9000/api/ce/task?id=e7655e1f-3b8a-49f9-a936-b36a2fbb4826
[INFO] Analysis total time: 9.066 s
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
[INFO] Total time: 23.707 s
[INFO] Finished at: 2025-10-08T14:53:12Z
[INFO] -----
[Pipeline] }
[Pipeline] // withSonarQubeEnv
[Pipeline] }
[Pipeline] // dir
[Pipeline] }
[Pipeline] // withEnv
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // withEnv
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Step 11:

SonarQube community Projects Issues Rules Quality Profiles Quality Gates Administration More ▾

Example of basic Maven project to integrate with SonarQube Bind project / main ✓ ?

Overview Issues Security Hotspots Code Measures Activity Project Settings ▾ Project Information

main 92 Lines of Code • Version 1.0-SNAPSHOT • Set as homepage Last analysis 5 minutes ago

Quality Gate ⓘ **Passed**

New Code Overall Code

Security	Reliability	Maintainability
0 Open issues	0 Open issues	5 Open issues
Accepted issues	Coverage	Duplications
0	0.0%	0.0%
Valid issues that were not fixed	On 4 lines to cover.	On 115 lines.

Security Hotspots 0

Activity

Graph type Issues There isn't enough data to generate an activity graph.

October 8, 2025 at 8:23 PM 1.0-SNAPSHOT Quality Gate: Passed

First analysis: 5 Issues • 0.0% Coverage • 0.0% Duplications

[See full history of analyses](#)

Conclusion:

By integrating Jenkins and SonarQube, this experiment successfully built a CI/CD pipeline that automates static code analysis. This process automatically detects bugs, vulnerabilities, and code smells in the Java application , providing developers with rapid feedback to improve code quality and security early in the development lifecycle.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY



Department of Information Technology

(NBA Accredited)

Semester: V**Academic Year: 2025-26****Class / Branch: TE IT****Subject: Advanced DevOps Lab (ADL)****Name of Instructor: Prof. Vishal Badgujar****Name of Student: Sanket B. Bhoir****Student ID: 24204022**

EXPERIMENT NO. 09

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

Step 01:

```
ubuntu@ip-172-31-38-63:~$ sudo su
root@ip-172-31-38-63:/home/ubuntu# sudo apt-get update
Hit:1 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:5 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:6 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:8 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:9 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:10 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
```

Step 02:

```
root@ip-172-31-38-63:/home/ubuntu# sudo apt-get install wget build-essential unzip openssl libssl-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wget is already the newest version (1.21.4-1ubuntu4.1).
wget set to manually installed.
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu bzip2 cpp cpp-13 cpp-13-x86-64-linux-gnu cpp-x86-64-
  fonts-dejavu-core fonts-dejavu-mono g++ g++-13 g++-13-x86-64-linux-gnu g++-x86-64-linux-gnu gcc gcc-13
```

Step 03:

```
root@ip-172-31-38-63:/home/ubuntu# sudo apt-get install apache2 php libapache2-mod-php php-gd libgd-dev
libapache2-mod-php php-gd libgd-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils bzip2-doc libaom-dev libapache2-mod-php8.3 libapr1t64 libaprutil1-dbd-sqlite3 libap
  libbz2-dev libdav1d-dev libde265-dev libdeflate-dev libexpat1-dev libfontconfig-dev libfreetype-dev libheif-dev
  libjpeg-turbo8-dev libjpeg8-dev liblerc-dev liblua5.4-0 liblzma-dev libpkcconf3 libpng-dev libpng-tools libpthread-stubs0-
  libtiffxx6 libvpx-dev libvpx9 libwebp-dev libwebpdecoder3 libwebpdemux2 libwebpmux3 libx11-dev libx265-199 libx265-dev li
  libxpm-dev libzstd-dev php-common php8.3 php8.3-cli php8.3-common php8.3-gd php8.3-opcache php8.3-readline pkgconf pkgcon
  xorg-sgml-doctools xtrans-dev zlib1g-dev
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser php-pear freetype2-doc liblzma-doc libx11-doc lib
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 04:

```
root@ip-172-31-38-63:/home/ubuntu# sudo adduser nagios
info: Adding user `nagios' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `nagios' (1001) ...
info: Adding new user `nagios' (1001) with group `nagios (1001)' ...
info: Creating home directory `/home/nagios' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for nagios
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
info: Adding new user `nagios' to supplemental / extra groups `users' ...
info: Adding user `nagios' to group `users' ...
```

```
root@ip-172-31-38-63:/home/ubuntu# sudo groupadd nagcmd
root@ip-172-31-38-63:/home/ubuntu# $sudo usermod -a -G nagcmd nagios
root@ip-172-31-38-63:/home/ubuntu# sudo usermod -a -G nagcmd www-data
```

Step 05:

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# cd /tmp
root@ip-172-31-38-63:/tmp# wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.5.2.tar.gz
--2025-10-05 11:00:33-- https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.5.2.tar.gz
Resolving assets.nagios.com (assets.nagios.com)... 45.79.49.120, 2600:3c00::f03c:92ff:fe7:45ce
Connecting to assets.nagios.com (assets.nagios.com)|45.79.49.120|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11540257 (11M) [application/x-gzip]
Saving to: `nagios-4.5.2.tar.gz.1'

nagios-4.5.2.tar.gz.1                                         27%[=====>
```

Step 06:

```
root@ip-172-31-38-63:/tmp# tar xzf nagios-4.5.2.tar.gz
root@ip-172-31-38-63:/tmp# cd nagios-4.5.2
root@ip-172-31-38-63:/tmp/nagios-4.5.2# ./configure --with-command-group=nagcmd
```

```
General Options:
-----
Nagios executable: nagios
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: /run/nagios.lock
Check result directory: /usr/local/nagios/var/spool/checkresults
Init directory: /lib/systemd/system
Apache conf.d directory: /etc/apache2/sites-available
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):
```

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



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 07:

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# make all
cd ./base && make
make[1]: Entering directory '/tmp/nagios-4.5.2/base'
```

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# make install
cd ./base && make install
make[1]: Entering directory '/tmp/nagios-4.5.2/base'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/bin
/usr/bin/install -c -s -m 774 -o nagios -g nagios nagios /usr/local/nagios/bin
/usr/bin/install -c -s -m 774 -o nagios -g nagios nagiostats /usr/local/nagios/bin
make[1]: Leaving directory '/tmp/nagios-4.5.2/base'
cd ./cgi && make install
make[1]: Entering directory '/tmp/nagios-4.5.2/cgi'
make install-basic
```

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# make install-init
/usr/bin/install -c -m 755 -d -o root -g root /lib/systemd/system
/usr/bin/install -c -m 755 -o root -g root startup/default-service /lib/systemd/system/nagios.service
root@ip-172-31-38-63:/tmp/nagios-4.5.2# make install-daemoninit
/usr/bin/install -c -m 755 -d -o root -g root /lib/systemd/system
/usr/bin/install -c -m 755 -o root -g root startup/default-service /lib/systemd/system/nagios.service
Created symlink /etc/systemd/system/multi-user.target.wants/nagios.service → /usr/lib/systemd/system/nagios.service.

*** Init script installed ***
```

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# make install-config
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc/objects
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/nagios.cfg /usr/local/nagios/etc/nagios.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/cgi.cfg /usr/local/nagios/etc/cgi.cfg
/usr/bin/install -c -b -m 660 -o nagios -g nagios sample-config/resource.cfg /usr/local/nagios/etc/resource.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/templates.cfg /usr/local/nagios/etc/objects/templates.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/commands.cfg /usr/local/nagios/etc/objects/commands.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/contacts.cfg /usr/local/nagios/etc/objects/contacts.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/timeperiods.cfg /usr/local/nagios/etc/objects/timeperiods.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/localhost.cfg /usr/local/nagios/etc/objects/localhost.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/windows.cfg /usr/local/nagios/etc/objects/windows.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/printer.cfg /usr/local/nagios/etc/objects/printer.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/switch.cfg /usr/local/nagios/etc/objects/switch.cfg

*** Config files installed ***

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

Step 08:

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# make install-commandmode
/usr/bin/install -c -m 775 -o nagios -g nagcmd -d /usr/local/nagios/var/rw
chmod g+s /usr/local/nagios/var/rw

*** External command directory configured ***

root@ip-172-31-38-63:/tmp/nagios-4.5.2# make install-classicui

*** Classic theme installed ***
NOTE: Use 'make install-exfoliation' to use new Nagios theme

root@ip-172-31-38-63:/tmp/nagios-4.5.2#
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY



Department of Information Technology

(NBA Accredited)

Step 09:

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# sudo make install-webconf
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sites-available/nagios.conf
if [ 1 -eq 1 ]; then \
    ln -s /etc/apache2/sites-available/nagios.conf /etc/apache2/sites-enabled/nagios.conf; \
fi

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

root@ip-172-31-38-63:/tmp/nagios-4.5.2# sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
root@ip-172-31-38-63:/tmp/nagios-4.5.2# sudo a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
    systemctl restart apache2
root@ip-172-31-38-63:/tmp/nagios-4.5.2# sudo a2enmod cgi
Enabling module cgi.
To activate the new configuration, you need to run:
    systemctl restart apache2
root@ip-172-31-38-63:/tmp/nagios-4.5.2# sudo systemctl restart apache2
```

Step 10:

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# cd /tmp
root@ip-172-31-38-63:/tmp# wget https://nagios-plugins.org/download/nagios-plugins-2.4.8.tar.gz
--2025-10-05 11:09:28-- https://nagios-plugins.org/download/nagios-plugins-2.4.8.tar.gz
Resolving nagios-plugins.org (nagios-plugins.org)... 45.56.123.251
Connecting to nagios-plugins.org (nagios-plugins.org)|45.56.123.251|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2744359 (2.6M) [application/x-gzip]
Saving to: 'nagios-plugins-2.4.8.tar.gz'

nagios-plugins-2.4.8.tar.gz          100%[=====] 2744359  2.6M/s
2025-10-05 11:09:31 (1.64 MB/s) - 'nagios-plugins-2.4.8.tar.gz' saved [2744359/2744359]

root@ip-172-31-38-63:/tmp# tar xzf nagios-plugins-2.4.8.tar.gz
root@ip-172-31-38-63:/tmp# cd nagios-plugins-2.4.8
root@ip-172-31-38-63:/tmp/nagios-plugins-2.4.8# ./configure --with-nagios-user=nagios --with-nagios-group=nagios
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... gawk
```

```
root@ip-172-31-38-63:/tmp/nagios-plugins-2.4.8# make
```

```
root@ip-172-31-38-63:/tmp/nagios-plugins-2.4.8# make install
```

Step 11:

```
root@ip-172-31-38-63:/tmp/nagios-plugins-2.4.8# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Nagios Core 4.5.2
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2024-04-30
License: GPL

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



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Running pre-flight check on configuration data...

Checking objects...

```
Checked 8 services.  
Checked 1 hosts.  
Checked 1 host groups.  
Checked 0 service groups.  
Checked 1 contacts.  
Checked 1 contact groups.  
Checked 24 commands.  
Checked 5 time periods.  
Checked 0 host escalations.  
Checked 0 service escalations.
```

Checking for circular paths...

```
Checked 1 hosts  
Checked 0 service dependencies  
Checked 0 host dependencies  
Checked 5 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

Step 12:



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY



Department of Information Technology

(NBA Accredited)

Conclusion:

This experiment documented the procedure for installing the Nagios Core monitoring system. The final outcome demonstrates that using the latest stable software versions for both Nagios Core and its plugins is a critical factor for ensuring compatibility with a modern operating system's libraries and build environment.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY



Department of Information Technology

(NBA Accredited)

Semester: V**Academic Year: 2025-26****Class / Branch: TE IT****Subject: Advanced DevOps Lab (ADL)****Name of Instructor: Prof. Vishal Badgujar****Name of Student: Sanket B. Bhoir****Student ID: 24204022**

EXPERIMENT NO. 10

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

Step 01: On Nagios Server :

```
ubuntu@ip-172-31-38-63:~$ sudo su
root@ip-172-31-38-63:/home/ubuntu# sudo apt-get update
Hit:1 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:5 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:6 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:8 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:9 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:10 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
```

Step 02:

```
root@ip-172-31-38-63:/home/ubuntu# sudo apt-get install wget build-essential unzip openssl libssl-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wget is already the newest version (1.21.4-1ubuntu4.1).
wget set to manually installed.
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu bzip2 cpp cpp-13 cpp-13-x86-64-linux-gnu cpp-x86-64-
  fonts-dejavu-core fonts-dejavu-mono g++ g++-13 g++-13-x86-64-linux-gnu g++-x86-64-linux-gnu gcc gcc-13
```

Step 03:

```
root@ip-172-31-38-63:/home/ubuntu# sudo apt-get install apache2 php libapache2-mod-php php-gd libgd-dev
libapache2-mod-php php-gd libgd-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils bzip2-doc libaom-dev libapache2-mod-php8.3 libapr1t64 libaprutil1-dbd-sqlite3 libap
  libbz2-dev libdav1d-dev libde265-dev libdeflate-dev libexpat1-dev libfontconfig-dev libfreetype-dev libheif-dev
  libjpeg-turbo8-dev libjpeg8-dev liblrc-dev liblua5.4-0 liblzma-dev libpkcconf3 libpng-dev libpng-tools libpthread-stubs0-
  libtiffxx6 libvpx-dev libvpx9 libwebp-dev libwebpdecoder3 libwebpdemux2 libwebpmux3 libx11-dev libx265-199 libx265-dev li
  libxpm-dev libzstd-dev php-common php8.3 php8.3-cli php8.3-common php8.3-gd php8.3-opcache php8.3-readline pkgconf pkgcon
  xorg-sgml-doctools xtrans-dev zlib1g-dev
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser php-pear freetype2-doc liblzma-doc libx11-doc lib
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY



Department of Information Technology

(NBA Accredited)

Step 04:

```
root@ip-172-31-38-63:/home/ubuntu# sudo adduser nagios
info: Adding user `nagios' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `nagios' (1001) ...
info: Adding new user `nagios' (1001) with group `nagios (1001)' ...
info: Creating home directory `/home/nagios' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for nagios
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
info: Adding new user `nagios' to supplemental / extra groups `users' ...
info: Adding user `nagios' to group `users' ...
```

```
root@ip-172-31-38-63:/home/ubuntu# sudo groupadd nagcmd
root@ip-172-31-38-63:/home/ubuntu# $sudo usermod -a -G nagcmd nagios
root@ip-172-31-38-63:/home/ubuntu# sudo usermod -a -G nagcmd www-data
```

Step 05:

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# cd /tmp
root@ip-172-31-38-63:/tmp# wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.5.2.tar.gz
--2025-10-05 11:00:33-- https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.5.2.tar.gz
Resolving assets.nagios.com (assets.nagios.com)... 45.79.49.120, 2600:3c00::f03c:92ff:fe7:45ce
Connecting to assets.nagios.com (assets.nagios.com)|45.79.49.120|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11540257 (11M) [application/x-gzip]
Saving to: `nagios-4.5.2.tar.gz.1'

nagios-4.5.2.tar.gz.1                                         27%[=====>]
```

Step 06:

```
root@ip-172-31-38-63:/tmp# tar xzf nagios-4.5.2.tar.gz
root@ip-172-31-38-63:/tmp# cd nagios-4.5.2
root@ip-172-31-38-63:/tmp/nagios-4.5.2# ./configure --with-command-group=nagcmd
```

```
General Options:
-----
Nagios executable: nagios
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: /run/nagios.lock
Check result directory: /usr/local/nagios/var/spool/checkresults
Init directory: /lib/systemd/system
Apache conf.d directory: /etc/apache2/sites-available
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):
```

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



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 07:

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# make all
cd ./base && make
make[1]: Entering directory '/tmp/nagios-4.5.2/base'
```

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# make install
cd ./base && make install
make[1]: Entering directory '/tmp/nagios-4.5.2/base'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/bin
/usr/bin/install -c -s -m 774 -o nagios -g nagios nagios /usr/local/nagios/bin
/usr/bin/install -c -s -m 774 -o nagios -g nagios nagiostats /usr/local/nagios/bin
make[1]: Leaving directory '/tmp/nagios-4.5.2/base'
cd ./cgi && make install
make[1]: Entering directory '/tmp/nagios-4.5.2/cgi'
make install-basic
```

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# make install-init
/usr/bin/install -c -m 755 -d -o root -g root /lib/systemd/system
/usr/bin/install -c -m 755 -o root -g root startup/default-service /lib/systemd/system/nagios.service
root@ip-172-31-38-63:/tmp/nagios-4.5.2# make install-daemoninit
/usr/bin/install -c -m 755 -d -o root -g root /lib/systemd/system
/usr/bin/install -c -m 755 -o root -g root startup/default-service /lib/systemd/system/nagios.service
Created symlink /etc/systemd/system/multi-user.target.wants/nagios.service → /usr/lib/systemd/system/nagios.service.

*** Init script installed ***
```

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# make install-config
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc/objects
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/nagios.cfg /usr/local/nagios/etc/nagios.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/cgi.cfg /usr/local/nagios/etc/cgi.cfg
/usr/bin/install -c -b -m 660 -o nagios -g nagios sample-config/resource.cfg /usr/local/nagios/etc/resource.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/templates.cfg /usr/local/nagios/etc/objects/templates.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/commands.cfg /usr/local/nagios/etc/objects/commands.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/contacts.cfg /usr/local/nagios/etc/objects/contacts.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/timeperiods.cfg /usr/local/nagios/etc/objects/timeperiods.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/localhost.cfg /usr/local/nagios/etc/objects/localhost.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/windows.cfg /usr/local/nagios/etc/objects/windows.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/printer.cfg /usr/local/nagios/etc/objects/printer.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/switch.cfg /usr/local/nagios/etc/objects/switch.cfg

*** Config files installed ***

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

Step 08:

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# make install-commandmode
/usr/bin/install -c -m 775 -o nagios -g nagcmd -d /usr/local/nagios/var/rw
chmod g+s /usr/local/nagios/var/rw

*** External command directory configured ***

root@ip-172-31-38-63:/tmp/nagios-4.5.2# make install-classicui

*** Classic theme installed ***
NOTE: Use 'make install-exfoliation' to use new Nagios theme

root@ip-172-31-38-63:/tmp/nagios-4.5.2#
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY



Department of Information Technology

(NBA Accredited)

Step 09:

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# sudo make install-webconf
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sites-available/nagios.conf
if [ 1 -eq 1 ]; then \
    ln -s /etc/apache2/sites-available/nagios.conf /etc/apache2/sites-enabled/nagios.conf; \
fi

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

root@ip-172-31-38-63:/tmp/nagios-4.5.2# sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
root@ip-172-31-38-63:/tmp/nagios-4.5.2# sudo a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
    systemctl restart apache2
root@ip-172-31-38-63:/tmp/nagios-4.5.2# sudo a2enmod cgi
Enabling module cgi.
To activate the new configuration, you need to run:
    systemctl restart apache2
root@ip-172-31-38-63:/tmp/nagios-4.5.2# sudo systemctl restart apache2
```

Step 10:

```
root@ip-172-31-38-63:/tmp/nagios-4.5.2# cd /tmp
root@ip-172-31-38-63:/tmp# wget https://nagios-plugins.org/download/nagios-plugins-2.4.8.tar.gz
--2025-10-05 11:09:28-- https://nagios-plugins.org/download/nagios-plugins-2.4.8.tar.gz
Resolving nagios-plugins.org (nagios-plugins.org)... 45.56.123.251
Connecting to nagios-plugins.org (nagios-plugins.org)|45.56.123.251|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2744359 (2.6M) [application/x-gzip]
Saving to: 'nagios-plugins-2.4.8.tar.gz'

nagios-plugins-2.4.8.tar.gz          100%[=====] 2744359  2.6M/s
2025-10-05 11:09:31 (1.64 MB/s) - 'nagios-plugins-2.4.8.tar.gz' saved [2744359/2744359]

root@ip-172-31-38-63:/tmp# tar xzf nagios-plugins-2.4.8.tar.gz
root@ip-172-31-38-63:/tmp# cd nagios-plugins-2.4.8
root@ip-172-31-38-63:/tmp/nagios-plugins-2.4.8# ./configure --with-nagios-user=nagios --with-nagios-group=nagios
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... gawk
```

```
root@ip-172-31-38-63:/tmp/nagios-plugins-2.4.8# make
```

```
root@ip-172-31-38-63:/tmp/nagios-plugins-2.4.8# make install
```

Step 11:

```
root@ip-172-31-38-63:/tmp/nagios-plugins-2.4.8# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Nagios Core 4.5.2
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2024-04-30
License: GPL

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



PARTHVNATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Running pre-flight check on configuration data...

Checking objects...

```
Checked 8 services.  
Checked 1 hosts.  
Checked 1 host groups.  
Checked 0 service groups.  
Checked 1 contacts.  
Checked 1 contact groups.  
Checked 24 commands.  
Checked 5 time periods.  
Checked 0 host escalations.  
Checked 0 service escalations.
```

Checking for circular paths...

```
Checked 1 hosts  
Checked 0 service dependencies  
Checked 0 host dependencies  
Checked 5 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

Step 12:



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY



Department of Information Technology

(NBA Accredited)

Step 13: On Remote Host:

```
ubuntu@ip-172-31-21-219:~$ sudo su
root@ip-172-31-21-219:/home/ubuntu# apt update
Hit:1 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:5 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
```

Step 14:

```
root@ip-172-31-21-219:/home/ubuntu# sudo apt install -y nagios-nrpe-server nagios-plugins
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'monitoring-plugins' instead of 'nagios-plugins'
The following additional packages will be installed:
  libavahi-client3 libavahi-common-data libavahi-common3 libcups2t64 libdbi1t64 libldb2 lib
  libsnmp-base libsnmp40t64 libtalloc2 libtdb1 libtevent0t64 liburiparser1 libwbclient0 md
  monitoring-plugins-standard mysql-common python3-gpg python3-ldb python3-markdown python
  samba-dsdb-modules samba-libs smbclient snmp
```

Step 15:

```
GNU nano 7.2
allowed_hosts=127.0.0.1,::1,172.31.38.63
/etc/nagios/nrpe.cfg *
```

EC2 > Security Groups > sg-0c22d0ba317348f88 - launch-wizard-6 > Edit inbound rules

Edit inbound rules Info

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

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-0b2598ce5bc7c909c	HTTP	TCP	80	Custom	0.0.0.0/0
sgr-04089b24c49371e54	SSH	TCP	22	Custom	0.0.0.0/0
sgr-07f7f6e1f6894b60b	HTTPS	TCP	443	Custom	0.0.0.0/0
-	Custom TCP	TCP	5666	Custom	172.31.38.63/32

[Add rule](#)

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

```
root@ip-172-31-21-219:/home/ubuntu# nano /etc/nagios/nrpe.cfg
root@ip-172-31-21-219:/home/ubuntu# sudo systemctl restart nagios-nrpe-server
root@ip-172-31-21-219:/home/ubuntu# sudo systemctl enable nagios-nrpe-server
Synchronizing state of nagios-nrpe-server.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable nagios-nrpe-server
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY



Department of Information Technology

(NBA Accredited)

Step 16: On Nagios Server

```
root@ip-172-31-38-63:/tmp/nagios-plugins-2.4.8# /usr/lib/nagios/plugins/check_nrpe -H 172.31.21.219
NRPE v4.1.0
```

```
GNU nano 7.2
define host {
    use                 linux-server
    host_name          my-remote-ec2
    alias              Remote EC2 Instance
    address            172.31.21.219
}

define service {
    use                 local-service
    host_name          my-remote-ec2
    service_description PING
    check_command      check_ping!100.0,20%1500.0,60%
}
```

Step 17:

```
root@ip-172-31-38-63:/tmp/nagios-plugins-2.4.8# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
Nagios Core 4.5.2
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2024-04-30
License: GPL

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

Running pre-flight check on configuration data...
Checking objects...
  Checked 8 services.
  Checked 1 hosts.
  Checked 1 host groups.
  Checked 0 service groups.
  Checked 1 contacts.
  Checked 1 contact groups.
  Checked 24 commands.
  Checked 5 time periods.
  Checked 0 host escalations.
  Checked 0 service escalations.
Checking for circular paths...
  Checked 1 hosts
  Checked 0 service dependencies
  Checked 0 host dependencies
  Checked 5 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-172-31-38-63:/tmp/nagios-plugins-2.4.8# sudo systemctl restart nagios
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY**Department of Information Technology**

(NBA Accredited)

**Step 18:**

Nagios®

Current Network Status
Last Updated: Sun Oct 5 12:49:58 UTC 2025
Updated every 90 seconds
Nagios® Core™ 4.5.2 - www.nagios.org
Logged in as nagiosadmin

Host Status Totals

Up	Down	Unreachable	Pending
2	0	0	0

All Problems All Types

All Problems	All Types
0	2

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
2	0	0	3	0

All Problems All Types

All Problems	All Types
3	11

Host Status Details For All Host Groups
Limit Results: 100 ▾

Host **	Status **	Last Check **	Duration **	Status Information
RemoteHost	UP	10-05-2025 12:47:50	0d 0h 7m 8s	PING OK - Packet loss = 0%, RTA = 0.04 ms
my-remote-ec2	UP	10-05-2025 12:48:35	0d 0h 6m 23s	PING OK - Packet loss = 0%, RTA = 1.41 ms

Results 1 - 2 of 2 Matching Hosts

Nagios®

General

Host Information
Last Updated: Sun Oct 5 12:50:32 UTC 2025
Updated every 90 seconds
Nagios® Core™ 4.5.2 - www.nagios.org
Logged in as nagiosadmin

Host
Remote EC2 Instance (my-remote-ec2)

Member of
No hostgroups
172.31.21.219

Host State Information

Host Status:	UP (for 0d 0h 6m 57s)
Status Information:	PING OK - Packet loss = 0%, RTA = 1.41 ms
Performance Data:	rta=1.407000ms;3000.000000;5000.000000;0.000000 pl=%;80;100;0
Current Attempt:	1/10 (HARD state)
Last Check Time:	10-05-2025 12:48:35
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 4.018 seconds
Next Scheduled Active Check:	10-05-2025 12:53:35
Last State Change:	10-05-2025 12:43:35
Last Notification:	N/A (notification 0)
Is This Host Flapping?	NO (5.46% state change)
In Scheduled Downtime?	NO
Last Update:	10-05-2025 12:50:30 (0d 0h 0m 2s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	ENABLED
Flap Detection:	ENABLED

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](#) [Delete all comments](#)

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

Conclusion:

This experiment successfully established a Nagios monitoring environment. The procedure involved configuring Nagios Core to monitor both the local server and a remote Linux host using the NRPE agent. Key tasks included installing plugins, defining check commands, and correctly configuring firewall rules. The final result is a functional monitoring system that actively checks the health and status of both servers as intended.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Semester: V

Academic Year: 2022-23

Class / Branch: TE IT

Subject: Advanced Devops Lab (ADL)

Name of Instructor: Prof. Vishal Badgujar

Name of Student: Sanket B. Bhoir

Student ID: 24204022

EXPERIMENT NO. 11

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

Step 1:

Compute

AWS Lambda

lets you run code without thinking about servers.

You pay only for the compute time that you consume — there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or backend service, all with zero administration.

Get started

Author a Lambda function from scratch, or choose from one of many preconfigured examples.

Create a function

Step 2:

Create function Info

Choose one of the following options to create your function.

Author from scratch
Start with a simple Hello World example.

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

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

Basic information

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

Function name must be 1 to 64 characters, must be unique to the Region, and can't include spaces. Valid characters are a-z, A-Z, 0-9, hyphens (-), and underscores (_).

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

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

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.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 3:

▼ Change default execution role

Execution role

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

Create a new role with basic Lambda permissions

Use an existing role

Create a new role from AWS policy templates

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

Lambda will create an execution role named sum-role-95c3tdb8, with permission to upload logs to Amazon CloudWatch Logs.

Step 4:

Lambda > Functions > sum

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

sum

Throttle Copy ARN Actions ▾

Function overview Info

Diagram Template

sum Layers (0)

+ Add trigger + Add destination

Description

Last modified 22 seconds ago

Function ARN arn:aws:lambda:ap-south-1:158018605139:function:sum

Function URL | Info

Code Test Monitor Configuration Aliases Versions

Step 5:

Code source Info

Open in Visual Studio Code Upload from ▾

EXPLORER

SUM

lambda_function.py

```
1 import json
2
3 def lambda_handler(event, context):
4     first_number = 100
5     second_number = 200
6     sum first_number + second_number
7
8     return sum
```

DEPLOY [UNDEPLOYED CHANGES]

You have undeployed changes.

Deploy (Ctrl+Shift+U) Test (Ctrl+Shift+I)

TEST EVENTS [NONE SELECTED]



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 6:

Test event Info

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

Test event action

Create new event Edit saved event

Event name
sanket-apsit
Maximum of 25 characters consisting of letters, numbers, dots, hyphens and underscores.

Event sharing settings

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

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

Template - optional
Hello World ▼ ⟳

Event JSON Format JSON

Step 7:

Template - optional
Hello World ▼ ⟳

Event JSON Format JSON Copy

1: []
2: []
3: []

3:2 JSON

Step 8:

Code Test Monitor Configuration Aliases Versions

Executing function: succeeded ([Logs](#))
▶ Details

Test event Info

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

CloudWatch Logs Live Tail Save Test



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 9:

The screenshot shows the AWS Lambda function configuration in the AWS Toolkit for VS Code. The code in `lambda_function.py` adds two numbers. The deployment section shows an undeployed change, with 'Deploy' and 'Test' buttons. The test events section shows a selected event named 'sanket-apsit'. The execution results show a successful test run with status 200, body "Hello from Lambda!", and detailed logs.

```
import json

def lambda_handler(event, context):
    first_number = 100
    second_number = 200
    sum = first_number + second_number
    return sum
```

Status: Succeeded
Test Event Name: sanket-apsit

Response:

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

Function Logs:

```
START RequestId: d142c061-ed64-4f62-970a-30d93d54d0d5 Version: $LATEST
END RequestId: d142c061-ed64-4f62-970a-30d93d54d0d5
REPORT RequestId: d142c061-ed64-4f62-970a-30d93d54d0d5 Duration: 1.03 ms Billed Duration: 2 ms
Memory Size: 128 MB Max Memory Used: 31 MB
```

Step 10:

The screenshot shows the AWS Lambda function configuration in the AWS Toolkit for VS Code. The code remains the same as in Step 9. The deployment section shows a successful update with 'Deploy' and 'Test' buttons. The test events section shows a selected event named 'sanket-apsit'. The execution results show a successful test run with status 300, and detailed logs.

```
import json

def lambda_handler(event, context):
    first_number = 100
    second_number = 200
    sum = first_number + second_number
    return sum
```

Status: Succeeded
Test Event Name: sanket-apsit

Response:

```
300
```

Function Logs:

```
START RequestId: 9b9af1f1-ca15-463c-87a8-0091db74220e Version: $LATEST
END RequestId: 9b9af1f1-ca15-463c-87a8-0091db74220e
REPORT RequestId: 9b9af1f1-ca15-463c-87a8-0091db74220e Duration: 1.15 ms Billed Duration: 2 ms
Memory Size: 128 MB Max Memory Used: 31 MB Init Duration: 66.18 ms
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 11:

```
def lambda_handler(event, context):
    if event['name'] == "sanket":
        return "apsit"
```

Step 12:

Successfully updated the function sum.

Executing function: succeeded ([Logs](#))
▶ Details

Test event [Info](#)

To Invoke your function without saving an event, modify the event, then choose Test. Lambda uses the modified event to invoke your function, but does not overwrite the original event until you choose Save.

Test event action

Create new event Edit saved event

Event name

sanket-apsit [Edit](#)

Event JSON

```
1: {
2:   "name": "sanket"
3: }
```

[Format JSON](#) [Copy](#)



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 13:

```
def lambda_handler(event, context):
    if event["name"] == "sanket":
        return "apsit"
```

Conclusion:

We explored AWS Lambda, understood its workflow, and learned how it enables serverless computing. We also created our first Lambda functions using Python and Node.js, gaining hands-on experience with its capabilities.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Semester: V

Academic Year: 2022-23

Class / Branch: TE IT

Subject: Advanced Devops Lab (ADL)

Name of Instructor: Prof. Vishal Badgujar

Name of Student: Sanket B. Bhoir

Student ID: 24204022

EXPERIMENT NO. 12

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

Step 1:

Compute

AWS Lambda

lets you run code without thinking about servers.

You pay only for the compute time that you consume — there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or backend service, all with zero administration.

Get started

Author a Lambda function from scratch, or choose from one of many preconfigured examples.

Create a function

Step 2:

Create function Info

Choose one of the following options to create your function.

Author from scratch
Start with a simple Hello World example.

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

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

Basic information

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

Function name must be 1 to 64 characters, must be unique to the Region, and can't include spaces. Valid characters are a-z, A-Z, 0-9, hyphens (-), and underscores (_).

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

Python 3.9 ▼

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

arm64

x86_64

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.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 3:

The screenshot shows the AWS Lambda 'Create New Function' wizard. Under the 'Execution role' section, the 'Create a new role with basic Lambda permissions' option is selected. A note below states: 'Role creation might take a few minutes. Do not delete the role or edit the trust or permissions policies in this role.' A message at the bottom indicates: 'Lambda will create an execution role named sum-role-95c3tdb8, with permission to upload logs to Amazon CloudWatch Logs.'

Step 4:

The screenshot shows the AWS Lambda function overview for 'sum'. It displays a green success message: 'Successfully created the function sum. You can now change its code and configuration. To invoke your function with a test event, choose "Test".' The function details include: Name: sum, Description: -, Last modified: 22 seconds ago, Function ARN: arn:aws:lambda:ap-south-1:158018605139:function:sum, and Function URL: -.

Step 5:

The screenshot shows the AWS Lambda code editor for the 'lambda_function.py' file. The code is as follows:

```
1 import json
2
3 def lambda_handler(event, context):
4     first_number = 100
5     second_number = 200
6     sum first_number + second_number
7
8     return sum
```

The interface includes an 'EXPLORER' sidebar showing the file structure, and a 'DEPLOY [UNDEPLOYED CHANGES]' section with 'Deploy (Ctrl+Shift+U)' and 'Test (Ctrl+Shift+I)' buttons.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 6:

Test event Info

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

Test event action

Create new event Edit saved event

Event name
sanket-apsit
Maximum of 25 characters consisting of letters, numbers, dots, hyphens and underscores.

Event sharing settings

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

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

Template - optional
Hello World ▼ ⟳

Event JSON Format JSON

Step 7:

Template - optional
Hello World ▼ ⟳

Event JSON Format JSON Copy

1: []
2: []
3: []

3:2 JSON

Step 8:

Code Test Monitor Configuration Aliases Versions

Executing function: succeeded ([Logs](#))
▶ Details

Test event Info

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

CloudWatch Logs Live Tail Save Test



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 9:

The screenshot shows the AWS Lambda function configuration in Visual Studio Code. The code editor displays a Python file named `lambda_function.py` with the following content:

```
1 import json
2
3 def lambda_handler(event, context):
4     first_number = 100
5     second_number = 200
6     sum = first_number + second_number
7     return sum
8
```

The sidebar on the left shows the project structure under `SUM`, with `lambda_function.py` selected. Below it, the `TEST EVENTS` section is expanded, showing a saved event named `sanket-apsit`. The main panel shows the deployment status as "Succeeded" with the test event name `sanket-apsit`. The response body is displayed as:

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

Function Logs show the execution details:

```
START RequestId: d142c061-ed64-4f62-970a-30d93d54d0d5 Version: $LATEST
END RequestId: d142c061-ed64-4f62-970a-30d93d54d0d5
REPORT RequestId: d142c061-ed64-4f62-970a-30d93d54d0d5 Duration: 1.03 ms Billed Duration: 2 ms
Memory Size: 128 MB Max Memory Used: 31 MB
```

Step 10:

The screenshot shows the AWS Lambda function configuration in Visual Studio Code. The code editor displays the same `lambda_function.py` file as in Step 9. The sidebar shows the project structure under `SUM`. The `TEST EVENTS` section is expanded, showing a saved event named `sanket-apsit`. The main panel shows the deployment status as "Succeeded" with the test event name `sanket-apsit`. The response body is displayed as:

```
300
```

Function Logs show the execution details:

```
START RequestId: 9b9af1f1-ca15-463c-87a8-0091db74220e Version: $LATEST
END RequestId: 9b9af1f1-ca15-463c-87a8-0091db74220e
REPORT RequestId: 9b9af1f1-ca15-463c-87a8-0091db74220e Duration: 1.15 ms Billed Duration: 2 ms
Memory Size: 128 MB Max Memory Used: 31 MB Init Duration: 66.18 ms
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 11:

```
def lambda_handler(event, context):
    if event['name'] == "sanket":
        return "apsit"
```

Step 12:

Successfully updated the function sum.

Executing function: succeeded ([Logs](#))
▶ Details

Test event [Info](#)

To Invoke your function without saving an event, modify the event, then choose Test. Lambda uses the modified event to invoke your function, but does not overwrite the original event until you choose Save.

Test event action

Create new event Edit saved event

Event name

sanket-apsit [Edit](#)

Event JSON

```
1: {
2:   "name": "sanket"
3: }
```

[Format JSON](#) [Copy](#)



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 13:

The screenshot shows the AWS Lambda function code editor. The code file is named `lambda_function.py` and contains the following Python code:

```
def lambda_handler(event, context):
    if event["name"] == "sanket":
        return "apsit"
```

The status bar at the bottom indicates the status is **Succeeded**, the test event is **sanket-apsit**, and the response is **"apsit"**. There are also buttons for **Deploy** and **Test**.

Step 14:

The screenshot shows the AWS S3 'Create bucket' configuration page. The 'General configuration' section is selected. The 'Bucket name' field is set to `lambda-sanket`. The 'Bucket type' dropdown has the 'General purpose' option selected. The 'AWS Region' is set to Asia Pacific (Mumbai) ap-south-1. The 'Copy settings from existing bucket - optional' section shows a 'Choose bucket' button and a note that only bucket settings will be copied. The 'Object Ownership' section is partially visible at the bottom.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 15:

Successfully created bucket "lambda-sanket". To upload files and folders, or to configure additional bucket settings, choose [View details](#).

[View details](#) X

[General purpose buckets](#) All AWS Regions [Directory buckets](#)

General purpose buckets (1) [Info](#)
Buckets are containers for data stored in S3.

[Find](#)

Name	AWS Region	Creation date
lambda-sanket	Asia Pacific (Mumbai) ap-south-1	July 29, 2025, 15:46:26 (UTC+05:30)

Account snapshot [Info](#)
Updated daily

Storage Lens provides visibility into storage usage and activity trends.

External access summary - new [Info](#)
Updated daily

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

Step 16:

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

Lambda

Choose a use case for the specified service.

Use case

Lambda
Allows Lambda functions to call AWS services on your behalf.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 17:

Add permissions [Info](#)

Permissions policies (3/1070) [Info](#)

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

Filter by Type

Policy name	Type	Description
<input type="checkbox"/> AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	Provides AWS Lambda functions perm...
<input type="checkbox"/> AmazonSageMakerPartnerServiceCatalogProducts...	AWS managed	Service role policy used by the AWS La...
<input type="checkbox"/> AmazonSageMakerServiceCatalogProductsLambd...	AWS managed	Service role policy used by the AWS La...
<input type="checkbox"/> AWSCodeDeployRoleForLambda	AWS managed	Provides CodeDeploy service access to ...
<input type="checkbox"/> AWSCodeDeployRoleForLambdaLimited	AWS managed	Provides CodeDeploy service limited a...
<input type="checkbox"/> AWSDeepLensLambdaFunctionAccessPolicy	AWS managed	This policy specifies permissions requir...
<input checked="" type="checkbox"/> AWSLambda_FullAccess	AWS managed	Grants full access to AWS Lambda serv...
<input type="checkbox"/> AWSLambda_ReadOnlyAccess	AWS managed	Grants read-only access to AWS Lamb...
<input type="checkbox"/> AWSLambdaBasicExecutionRole	AWS managed	Provides write permissions to CloudW...

Step 18:

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: _+=,. @-/\[\{\}\]!#\$%^&*()::;"`



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 19:

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy
AWSLambda_FullAccess	AWS managed	Permissions policy
CloudWatchFullAccess	AWS managed	Permissions policy

Step 3: Add tags

Add tags - optional Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create role](#)

Step 20:

⌚ Role apsit-lambda created.

Roles (6) Info

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

Search

Role name	Trusted entities	Last activity
apsit-lambda	AWS Service: lambda	-
AWSCodePipelineServiceRole-ap-south-1-pwa-pipeline-sanket	AWS Service: codepipeline	6 days ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linker)	-
codebuild-pwa-codebuild-sanket-service-role	AWS Service: codebuild	6 days ago
sum-role-95c3tdb8	AWS Service: lambda	19 minutes ago



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 21:

Lambda > Functions > Create function

Create function Info

Choose one of the following options to create your function.

- Author from scratch
Start with a simple Hello World example.
- Use a blueprint
Build a Lambda application from sample code and configuration presets for common use cases.
- Container Image
Select a container image to deploy for your function.

Basic information

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

Function name must be 1 to 64 characters, must be unique to the Region, and can't include spaces. Valid characters are a-z, A-Z, 0-9, hyphens (-), and underscores (_).

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

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

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.

Step 22:

Lambda > Functions > Create function

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

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

▼ Change default execution role

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).
 Create a new role with basic Lambda permissions
 Use an existing role
 Create a new role from AWS policy templates

Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.
 ▼ C
View the apsit-lambda role [on the IAM console](#).

► Additional configurations
Use additional configurations to set up code signing, function URL, tags, and Amazon VPC access for your function.

Cancel Create function



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 23:

Successfully created the function **lambdawiths3-sanket**. You can now change its code and configuration. To invoke your function with a test event, choose "Test".

lambdawiths3-sanket

Function overview Info

Description
-

Last modified
12 seconds ago

Function ARN
`arn:aws:lambda:ap-south-1:158018605139:function:lambdawiths3-sanket`

Function URL Info

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

Step 24:

Lambda > Add triggers

aws asynchronous storage

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

X C

Bucket region: ap-south-1

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

All object create events X

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

e.g. `Images/`

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

`.png`

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

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

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



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 25:

The trigger lambda-sanket was successfully added to function lambdawiths3-sanket. The function is now receiving events from the trigger.

Function overview [Info](#)

[Diagram](#) [Template](#)

lambdawiths3-sanket

S3

[+ Add destination](#)

[+ Add trigger](#)

Description
-

Last modified
4 minutes ago

Function ARN
arn:aws:lambda:ap-south-1:158018605139:function:lambdawiths3-sanket

Function URL [Info](#)
-

Step 26:

```
JS index.mjs x
JS index.mjs > handler
1 export const handler = async (event, context) => {
2   console.log("Incoming Event:", event);
3   if (!event.Records || event.Records.length === 0) {
4     const errorMessage = "No records found in the event.";
5     console.log(errorMessage);
6     return errorMessage;
7   }
8   const bucket = event.Records[0].s3.bucket.name;
9   const filename = decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/g, ''));
10  const message = `An Image has been added - ${bucket} -> ${filename}`;
11  console.log(message);
12
13  return message;
14}
15
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 27:

lambda-sanket [Info](#)

Objects Properties Permissions Metrics Management Access Points

Objects (0) [C](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [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 bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix ✖ 1 ↗ ⚙

Name	Type	Last modified	Size	Storage class
No objects You don't have any objects in this bucket.				

[Upload](#)

Step 28:

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 SDKs 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 (0) [Remove](#) [Add files](#) [Add folder](#)

All files and folders in this table will be uploaded.

Find by name ✖ 1 ↗ ⚙

Name	Folder	Type	Size
No files or folders You have not chosen any files or folders to upload.			

Destination [Info](#)

Destination <s3://lambda-sanket>

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

[CloudShell](#) [Feedback](#) © 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Step 29:

Amazon S3 > Buckets > lambda-sanket > 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 SDKs 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, 72.2 KB)			
All files and folders in this table will be uploaded.			
<input type="text"/> Find by name			
Name	Folder	Type	Size
14.png	-	image/png	72.2 KB

Destination Info

Destination
s3://lambda-sanket

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

Step 30:

Upload succeeded
For more information, see the [Files and folders](#) table.

Upload: status

After you navigate away from this page, the following information is no longer available.

Summary		Succeeded		Failed	
Destination	s3://lambda-sanket	Succeeded	1 file, 72.2 KB (100.00%)	Failed	0 files, 0 B (0%)
Files and folders	Configuration				

Files and folders (1 total, 72.2 KB)

Files and folders (1 total, 72.2 KB)					
<input type="text"/> Find by name					
Name	Folder	Type	Size	Status	Error
14.png	-	image/png	72.2 KB	✓ Succeeded	-



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Step 31:

CloudWatch > Log groups > /aws/lambda/lambdawiths3bucket > 2021/08/03/[\${LATEST}]0f36a60d46ca40078172fc11de9d735f

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

[View as text](#)

Filter events Clear 1m

▶	Timestamp	Message
No older events at this moment. Retry		
▶	2021-08-03T12:01:00.069+05:30	START RequestId: ae43508a-8eb7-4b08-8fa1-841814d597c1 Version: \$LATEST
▶	2021-08-03T12:01:00.098+05:30	2021-08-03T06:31:00.097Z ae43508a-8eb7-4b08-8fa1-841814d597c1 INFO Incoming Event: { Records: [{ eventVersion: '2.1', eventSource: 'aws:s3', awsRegion: 'ap-south-1', s3: { objectKey: 'apsit_logo.jpg', bucket: 'lambdawiths3', size: 128 } }] }
▼	2021-08-03T12:01:00.098+05:30	2021-08-03T06:31:00.098Z ae43508a-8eb7-4b08-8fa1-841814d597c1 INFO An Image has been added - lambdawiths3 -> apsit_logo.jpg
	2021-08-03T06:31:00.098Z	ae43508a-8eb7-4b08-8fa1-841814d597c1 INFO An Image has been added - lambdawiths3 -> apsit_logo.jpg
▶	2021-08-03T12:01:00.119+05:30	END RequestId: ae43508a-8eb7-4b08-8fa1-841814d597c1
▶	2021-08-03T12:01:00.119+05:30	REPORT RequestId: ae43508a-8eb7-4b08-8fa1-841814d597c1 Duration: 49.40 ms Billed Duration: 50 ms Memory Size: 128 MB Max Memory Used: 65 MB Init Duration: 155.37 ms
No newer events at this moment. Auto retry paused. Resume		

Conclusion:

In this experiment, we created a Lambda function that automatically logs “An Image has been added” whenever a new object is uploaded to a specific S3 bucket, demonstrating event-driven automation using AWS services.



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology
(NBA Accredited)



Semester: V

Academic Year: 2024-25

Class / Branch: TE IT

Subject: Advanced DevOps Lab (ADL)

Name of Instructor: Prof. Vishal Badgujar

Name of Student: Sanket B. Bhoir

Student ID: 24204022

EXPERIMENT NO. 13

Aim: To demonstrate working of cloud launcher to launch the web application and Manage and Monitor the Application.

Theory:

To demonstrate the working of **Google Cloud Launcher (Google Cloud Marketplace)** to launch a web application, the purpose of this lab is to deploy a web application using a pre-configured environment from the Google Cloud Marketplace and

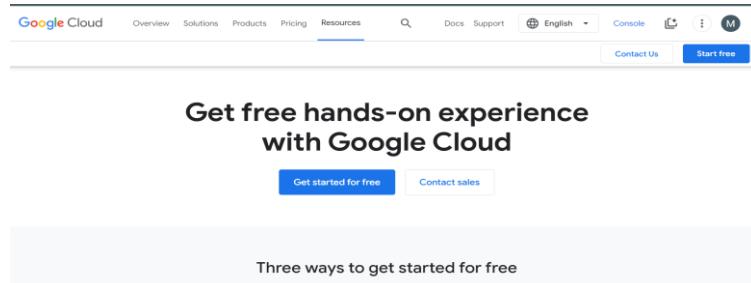
Prerequisites

- A **Google Cloud Platform (GCP)** account.
- **Billing enabled** on your GCP account (to avoid deployment restrictions).
- Basic knowledge of **web applications** (e.g., web servers, databases).
- Familiarity with the **Google Cloud Console**.

Step 1: Setting Up Your GCP Account

1. Login to Google Cloud Console:

- Visit the Google Cloud Console.
- Sign in using your Google account credentials.





PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Try Google Cloud for free

Step 1 of 2 Account Information



M.N. Kashikar
mnkashikar@apsit.edu.in

SWITCH ACCOUNT

Country

India

By using this application, you agree to the [Google Cloud Platform Terms](#), [Supplemental Free Trial Terms](#), and [any applicable services and APIs Terms](#) of Service.

AGREE & CONTINUE

Access to all Google Cloud products

Get everything you need to build and run your apps, websites and services, including Firebase and the Google Maps API.

\$300 credit for free

Put Google Cloud to work with \$300 in credit to spend over the next 90 days.

No autocharge after free trial ends

We ask you for your credit card to make sure you are not a robot. If you use a credit or debit card, you won't be charged unless you manually activate your full account.

The screenshot shows the Google Cloud sign-up process. On the left, under 'Step 1 of 2 Account Information', a user named M.N. Kashikar is selected, and the country is set to India. There is a note about agreeing to the terms of service. On the right, under 'Step 2 of 2 Payment Information', the user is creating a payments profile for an organization named 'apsit'. It also shows options for adding a credit or debit card and a note about autocharge after the free trial ends.

Create a New Project:

- Click on the **project drop-down** on the top-left corner of the console.
- Select **New Project**.
- Name the project (e.g., "Cloud Launcher Demo") and select your billing account.
- Click **Create**



Google Cloud Platform

New Project

You have 22 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)

[MANAGE QUOTAS](#)

Project name *

The name is required.

Location * No organization [BROWSE](#)

Parent organization or folder

[CREATE](#) [CANCEL](#)

Google Cloud Platform My First Project

Search products and resources

HOME PROJECT DASHBOARD ACTIVITY RECOMMENDATIONS

How Google Cloud is helping during COVID-19 [Learn more](#)

Project info

Project name: My First Project
Project ID: modern-alloy-278318
Project number: 920237031190

Add people to this project

do to project settings

Resources

BigQuery 1 dataset

Trace

No trace data from the past 7 days
Get started with Trace

Getting Started

RPI Explore and enable APIs

Select a project

NEW PROJECT

Name	ID
My First Project	modern-alloy-278318
IoT Cloud Tutorial	iot-cloud-tutorial
Simple Project	m2m-test-project
My Project 15338	data-exe-293614

CANCEL OPEN

Step 2: Navigating Google Cloud Marketplace

1. Open Google Cloud Marketplace:
 - o In the left-hand menu, navigate to Marketplace.
 - o This section allows you to find pre-configured solutions such as WordPress, LAMP stack, or Django, as well as other web application frameworks and services.
2. Search for a Web Application:
 - o Use the search bar in the Marketplace to find a web application you want to deploy. For this demo, let's deploy a simple **WordPress** instance.
 - o Type "**WordPress**" and select the official package from the search results.



The top screenshot shows the Google Cloud Platform dashboard with the 'Marketplace' tab selected. The 'Project info' section displays the following details:

Project name	Qode
Project ID	qode-293008
Project number	879250284347

The bottom screenshot shows a search results page for 'wordpress' in the Google Cloud Platform Marketplace. The results include:

- Plesk WordPress Edition PREMIUM
- Premium WordPress
- WordPress 5 on PHP 7
- WordPress with NGINX and SSL Certified by Bitnami and Automattic
- WordPress on LEMP 7 Max Performance
- WordPress
- Plesk on CentOS - BYOL - Website & WordPress Platform

Step 3: Deploying the Web Application

1. **Launch the WordPress App:**
 - On the WordPress product page, click **Launch on Compute Engine**.
 - You'll be taken to a page to configure the deployment.
2. **Configure Deployment Settings:**
 - Choose the **zone** where you want to deploy the application (e.g., us-central1).
 - Select the **machine type** (e.g., e2-small) which will allocate the appropriate CPU and memory resources.
 - Disk type:** Choose either the default **Persistent Disk** or **SSD** (for faster performance).
 - Networking:** Leave the default networking settings, or create a new Virtual Private Cloud (VPC) if necessary.
3. **Click Deploy:**



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



- After selecting your settings, click **Deploy** to start the process. GCP will automatically create the necessary infrastructure, including a virtual machine (VM), storage, and network configuration.

The screenshot shows the Google Cloud Platform interface for deploying a WordPress website. At the top, there's a blue header bar with the text "Google Cloud Platform" and "WordPress website". Below the header, the main content area has a title "WordPress" with a "Google Click to Deploy" badge. It describes WordPress as a "Web publishing platform for building multiple blogs and websites". There are two buttons at the bottom: "LAUNCH" (which is highlighted with a red box) and "VIEW PAST DEPLOYMENTS". Below these buttons are tabs for "OVERVIEW", "PRICING", and "SUPPORT". Under the "OVERVIEW" tab, there's an "Overview" section stating that WordPress is a software application used to create websites and blogs, with a "Learn more" link. There's also an "About Google Click to Deploy" section mentioning it runs on Google Compute Engine and is a single VM type. The "Additional details" section includes "Runs on: Google Compute Engine", "Type: Virtual machines, Single VM", and "Last updated: 4/6/22".

The screenshot shows the "Enable required APIs" step for a new WordPress deployment. The top navigation bar is identical to the previous screenshot. The main content area has a title "Enable required APIs" with a note: "The following APIs are required to deploy a VM product from Marketplace". It lists three APIs: "Compute Engine API", "Cloud Deployment Manager V2 API", and "Cloud Runtime Configuration API", each with a status indicator "Not enabled". At the bottom of the modal are two buttons: "ENABLE" (highlighted with a red box) and "SEND FEEDBACK".



The screenshot shows the Google Cloud Platform interface for deploying a new WordPress website. It includes sections for setting up source IP ranges for HTTP and HTTPS traffic, enabling Stackdriver monitoring and logging, and accepting the GCP Marketplace Terms of Service. A prominent blue 'DEPLOY' button is highlighted with a red box.

Step 4: Accessing the Web Application

1. Monitor Deployment Progress:

See the progress of the deployment in the Google Cloud Console. This includes setting up the virtual machine, installing WordPress, and configuring the environment.

2. Get the External IP Address:

Once deployment is complete, go to the **VM instances** page from the left-hand menu under **Compute Engine**.

Locate the deployed WordPress instance, and note the **External IP Address** assigned to the VM.

3. Access the Web Application:

- Open a new browser tab and navigate to the External IP address you noted.
- You should see the WordPress installation page, where you can set up the site (e.g., language, admin credential)

Step 5: Configuring the Web Application

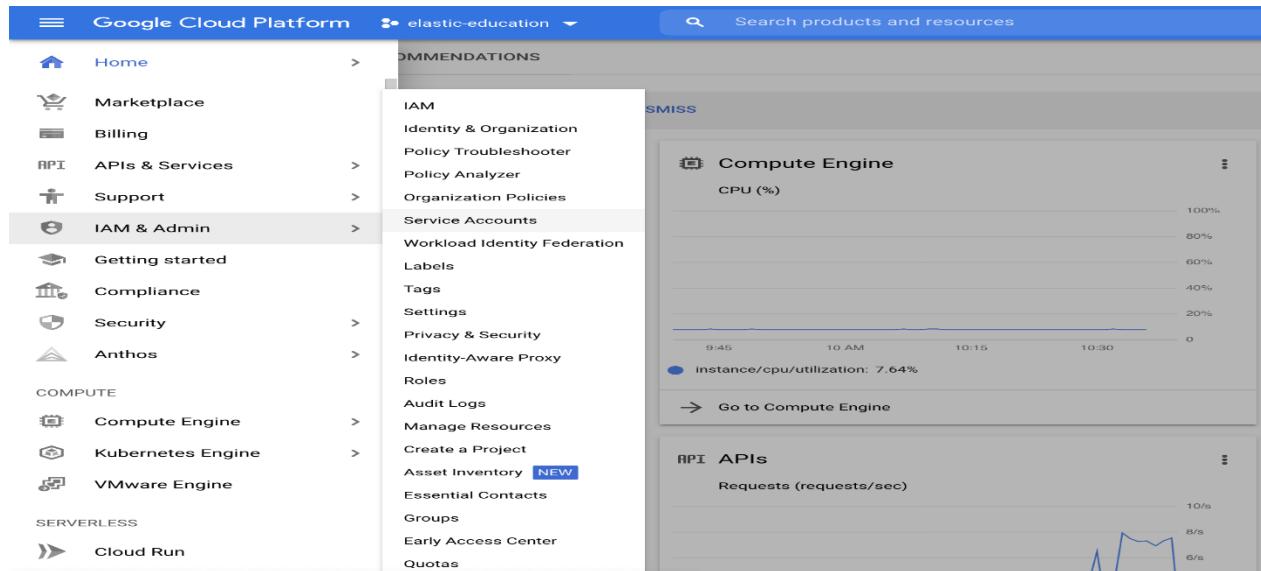
1. Set Up WordPress:

- Follow the on-screen instructions to complete the WordPress setup.
- Choose your site's title, create an admin username, and password.
- After setup, log in to the WordPress admin panel to customize your site.



2. Explore the Admin Dashboard:

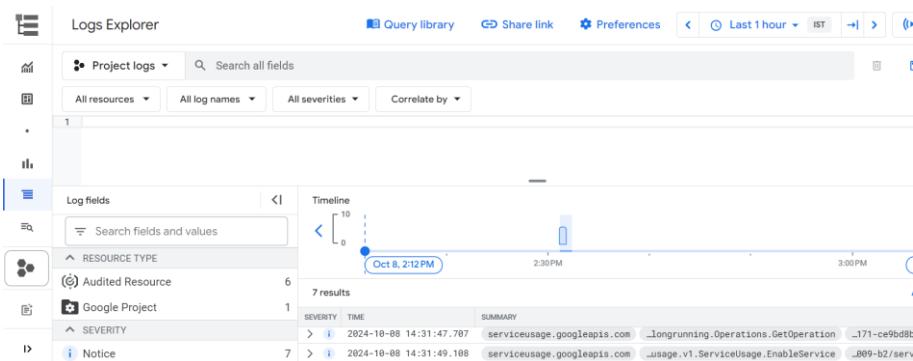
- Once logged in, explore the admin dashboard where you can add new content, change the theme, or install plugins.



Step 6: Manage and Monitor the Application

1. View Logs and Performance:

- Go to the **Operations** menu in the Cloud Console and select **Logs Explorer**.
- This allows you to view real-time logs from the web server, which can be useful for troubleshooting and monitoring application performance.





2. Scaling and Auto-healing:

- Discuss how you can modify the configuration to enable auto-scaling and high availability.
- For advanced users, demonstrate how to enable **Cloud Monitoring** and **Alerting** to get notified if the web server is under heavy load or goes down.

Step 7: Clean Up Resources

1. Delete Resources:

- To avoid unnecessary billing charges, delete the resources you created after the lab.
- Go to **Compute Engine > VM Instances**, and select the instance you deployed (WordPress).
- Click **Delete** to remove the virtual machine and associated resources.

2. Verify Billing:

- Check your **billing dashboard** to ensure there are no active resources still incurring charges.

Conclusion:

Thus we have deployed a WordPress instance, accessed it through the web, and explored management and monitoring functionalities within GCP.