



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 Badgumar

Name of Student: Huzaifa Bubere

Student ID: 24204006

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 :

The screenshot shows the AWS Cloud9 interface. At the top, it says "Developer Tools" and "AWS Cloud9". Below that, it says "A cloud IDE for writing, running, and debugging code". There is a paragraph about AWS Cloud9 allowing you to write, run, and debug code with just a browser. On the right side, there is a button labeled "New AWS Cloud9 environment" with a "Create environment" button below it.

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

The screenshot shows the "Name environment" step of the AWS Cloud9 setup wizard. It has three tabs: Step 1 (Name environment), Step 2 (Configure settings), and Step 3 (Review). The "Name environment" tab is active. It has two sections: "Environment name and description". The "Name" section contains a text input field with "WebAppIDE" and a note that the name needs to be unique per user. The "Description - Optional" section contains a text input field with "Write a short description for your environment" and a note that it will appear on the environment's card in the dashboard.



5. Keep all the Default settings as shown in below then Click On next:

AWS Cloud9

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 explorations.

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.

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 setting of half an hour of inactivity to maximize savings.

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](#)

Network settings (advanced)

No tags associated with the resource.

You can add 50 more tags.

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



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



AWS Cloud9 X

AWS Cloud9 / Environments / Create environment

Step 1 Name environment

Step 2 Configure settings

Step 3 Review

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**

Code Anything (Ctrl+P) Welcome Developer Tools

AWS Cloud9

Welcome to your development environment

AWS Cloud9 allows you to write, run, and debug your code with just a browser. You can use the code editor, write code for AWS Lambda and Amazon API Gateway, or interact with others in real time, and much more.

Toolkit for AWS Cloud9

The AWS Toolkit for Cloud9 is an IDE extension that simplifies accessing and interacting with resources from services such as AWS Lambda, AWS CloudFormation, and AWS API Gateway. With the toolkit, developers can also develop, debug, and deploy applications using the AWS Serverless Application Model (SAM). [Learn more](#)

Support

If you have any questions or experience issues, refer to the documentation or reach us to get help.

Documentation Get Help Security Best Practices

We are creating your AWS Cloud9 environment. This can take a few minutes.

Main Theme: Editor Themes: More Settings...



A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



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

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

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

Add user

Set user details

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

User name*

[+ 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



9.Click on Create group To Add User In A Group And Give Permission To That 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.

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

Create policy **Filter policies** 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-AWSElasticBeanst...	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
AlexaForBusinessLifesizeDelegatedAcc...	AWS managed	None	Provide access to Lifesize AVS devices

Create group **Cancel**

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.



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



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	WebAppapsitgroup

Tags

No tags were added.

Cancel Previous Create user

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

Identity and Access Management (IAM) x

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.](#)

Dashboard

Access management ▼

- User groups selected
- 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

User groups (1) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

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:



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



Identity and Access Management (IAM) X

IAM > User groups > WebAppapsitgroup

WebAppapsitgroup

Delete

Edit

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.

Filter policies by property or policy name and press enter

< 1 > | @

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 4 matches

"Cloud9" X Clear filters

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

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



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



The screenshot shows the Cloud9 IDE interface. On the left, the AWS Explorer sidebar lists services like API Gateway, CloudFormation, ECR, Lambda functions, and S3. In the center, the AWS Toolkit - Quick Start panel displays a code editor with a file named 'app.js' containing Lambda function code. An orange arrow points from the 'AWS Explorer' label at the bottom left towards the AWS Explorer sidebar. Another orange arrow points from the 'AWS Explorer' label at the top left towards the AWS Explorer panel. A callout bubble labeled 'Inline Action' points to a line of code: 'exports.handler = async (event, context) => {'. At the bottom right of the code editor, 'Current Credentials' is displayed.

```
13 * Return doc: https://docs.aws.amazon.com/apigateway/latest/developerguide/set-up-lambda-proxy-format.html
14 * @returns (Object) object - API Gateway Lambda Proxy Output Format
15 *
16 */
17 exports.handler = async (event, context) => {
18   try {
19     const url = event['request']['url'];
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     }
28     catch (err) {
29       console.log(err);
30       return err;
31     }
32   };
33   return response;
34 }
```

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 Cloud9 IDE interface. On the left, the AWS Explorer sidebar lists services like API Gateway, CloudFormation, ECR, Lambda functions, and S3. In the center, the AWS Toolkit - Quick Start panel displays a code editor with a terminal window showing AWS CLI commands. An orange arrow points from the 'AWS Explorer' label at the bottom left towards the AWS Explorer sidebar. Another orange arrow points from the 'AWS Explorer' label at the top left towards the AWS Explorer panel. The terminal window shows the following output:

```
bash - "ip-172-31-10-50.ax" immediate (Javascript (br x +)
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": "2021-06-03T19:03:54Z",
        "UserId": "229296960472",
        "Arn": "arn:aws:iam::229296960472:root"
    ]
}
```

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



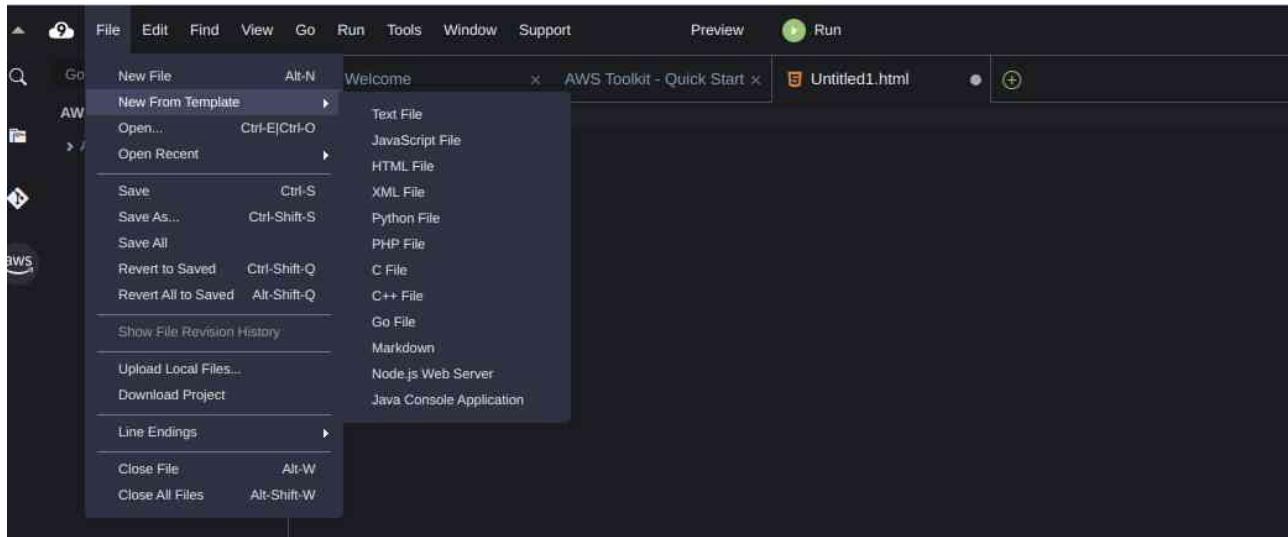
PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

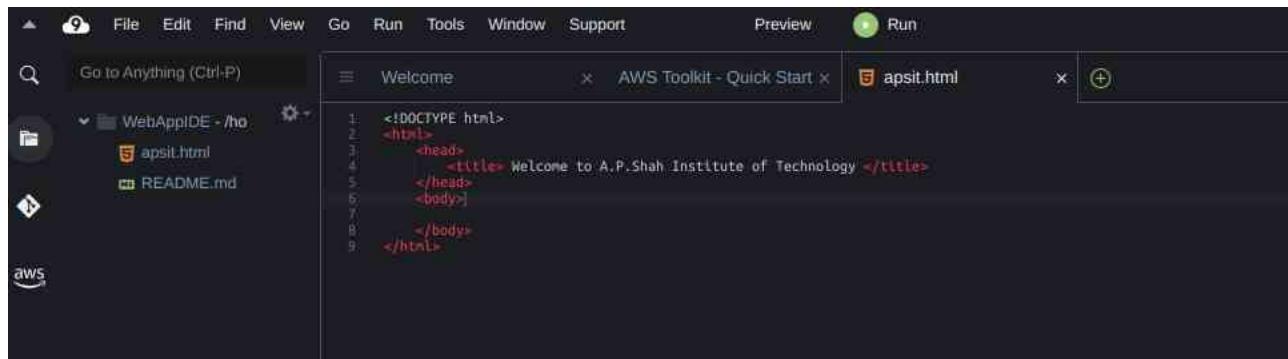


Department of Information Technology

(NBA Accredited)



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.



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

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

Next

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 'Your environments' (selected), 'Shared with you' (highlighted in orange), and 'Account environments'. Below that is a 'How-to guide'. The main area is titled 'AWS Cloud9 > Shared with you' and shows a single environment named 'WebAppIDE'. The environment details are: Type: EC2, Permissions: Read-write, Description: No description available, and Owner Arn: arn:aws:iam::229296960472:root. At the bottom of this card is a blue 'Open IDE' button. The overall interface is clean and modern, typical of AWS services.

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:

This screenshot shows the AWS Cloud9 IDE interface. The left side has a file browser with files like 'apsit.html', 'index.html', and 'README.md'. The main workspace shows the content of 'apsit.html', which includes a simple HTML structure with a title 'Welcome to A.P.Shah Institute of Technology'. The right side features a 'ENVIRONMENT MEMBERS' panel showing 'ReadWrite' access for two users: 'arn:aws:iam::229296960472:root' and 'You (online)'. There's also a 'GROUP CHAT' section where messages from 'root' and 'You' are displayed. The bottom part of the interface shows a terminal window with a bash prompt and some immediate Javascript output. The overall layout is designed for collaborative development and real-time communication.

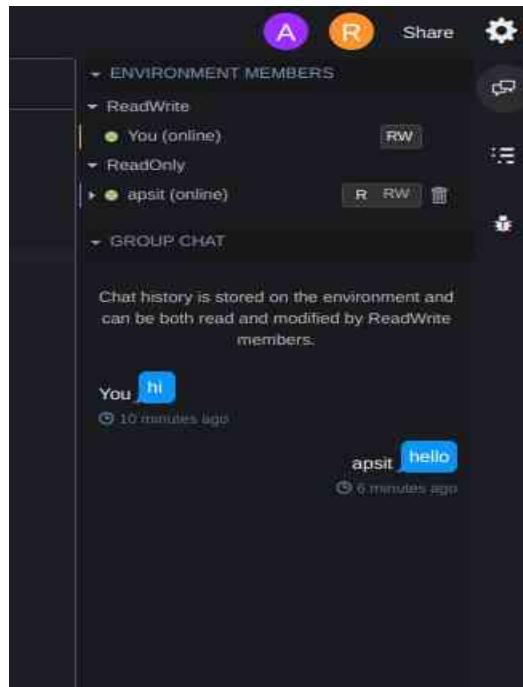


PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



The screenshot shows a terminal window with two panes. The left pane displays the contents of an 'apsit.html' file, which includes an HTML structure with a title and a 'Hello world!' message. The right pane shows AWS CloudWatch logs for a terminal session, with messages from 'You' and 'apsit'. The terminal prompt is 'bash ->'. The window title is 'WebAppIDE - AWS CloudWatch'.

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





PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



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: We Have Learned About benefits of Cloud Infrastructure and Setup AWS Cloud9 IDE, Launch AWS Cloud9 IDE and Perform Collaboration Demonstration With A Teammates. Also We Have Learned To Create User And User Group Also How To Add User To A User Group Was Learned.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Semester: V

Academic Year: 2021-22

Class / Branch: TE IT

Subject: Advanced Devops Lab (ADL)

Name of Instructor: Prof. Manjusha K.

Name of Student: Huzaifa Bubere

ID: 24204006

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.

The screenshot shows the AWS S3 console with the following details:

- General purpose buckets (1) [Info](#)**: Contains a single bucket named "store-build-venny".
- Actions**: Includes buttons for [Copy ARN](#), [Empty](#), [Delete](#), and [Create bucket](#).
- Buckets are containers for data stored in S3.**
- Search bar**: [Find buckets by name](#)
- Filtering**: Options to filter by [Name](#), [AWS Region](#), and [Creation date](#).
- Bucket Details**: Name: store-build-venny, Region: Asia Pacific (Mumbai) ap-south-1, Creation date: July 23, 2025, 10:53:47 (UTC+05:30).
- Account snapshot [Info](#)**: Updated daily. Provides visibility into storage usage and activity trends. Includes a [View dashboard](#) button.
- External access summary - new [Info](#)**: Updated daily. Helps identify bucket permissions for public access or access from other AWS accounts.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Elastic Beanstalk > Getting started

Create a web app

Create a new application and environment with a sample application or your own code. By creating an environment, you allow Amazon Elastic Beanstalk to manage Amazon Web Services resources and permissions on your behalf. [Learn more](#)

Application information

Application name Up to 100 Unicode characters, not including forward slash (/).

Application tags

Apply up to 50 tags. You can use tags to group and filter your resources. A tag is a key-value pair. The key must be unique within the resource and is case-sensitive. [Learn more](#)

Key	Value
EBS	CICD

[Add tag](#) 49 remaining

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

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

General purpose buckets (2) [Info](#)

Name	AWS Region	Creation date
development-bucket-pwa-venny	Asia Pacific (Mumbai) ap-south-1	July 23, 2025, 10:58:25 (UTC+05:30)
store-build-venny	Asia Pacific (Mumbai) ap-south-1	July 23, 2025, 10:53:47 (UTC+05:30)

Account snapshot [Info](#)
Updated daily [View dashboard](#)
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.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Manage default source credential

Source Provider

GitHub

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

Configuration

Source provider

GitHub

Primary repository

Venny-Hong/Car-pwa-deploy-
on-aws

Artifacts upload location

-

Service role

arn:aws:iam::863065069665:role/service-role/codebuild-pwa-codebuild-venny-service-role

Public builds

Disabled



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



▼ 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

store-build-venny X

development-bucket-pwa-venny

store-build-venny

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

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

Add source stage Info

Step 3 of 7

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

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](#) i

Repository



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1

Choose pipeline settings

Step 2

Add source stage

Step 3

Add build stage

Step 4

Add deploy stage

Step 5

Review

Add source stage Info

Source

Source provider

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

Amazon S3

Bucket

Q codepipeline-ap-south-1-48704463255 X

S3 object key

s3://awscodepipeline-demobucket-variables11/aws-codepipeline-s3-aws-codedeploy.

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

Change detection options

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

 Amazon CloudWatch Events (recommended)
Use Amazon CloudWatch Events to automatically start my pipeline when a change occurs **AWS CodePipeline**
Use AWS CodePipeline to check periodically for changes

Cancel

Previous

Next

Upload succeeded
View details below.

This information below will no longer be available once you navigate away from this page.

Summary		
Destination	Succeeded s3://awscodepipeline-demobucket-variables11	Failed 0 files, 0 B (0%)

Files and folders (7 Total, 12.2 KB)

Name	Type	Size	Status
LICENSE	-	10.6 KB	Succeeded
README.md	text/markdown	249.0 B	Succeeded
appspec.yml	application/x-yaml	359.0 B	Succeeded
index.html	text/html	782.0 B	Succeeded
install_dependencies	-	34.0 B	Succeeded
start_server	-	33.0 B	Succeeded
stop_server	-	105.0 B	Succeeded



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



Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1 Choose pipeline settings

Step 2 Add source stage

Step 3 Add build stage

Step 4 Add deploy stage

Step 5 Review

Add source stage Info

Source

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

Amazon S3

Bucket
codepipeline-ap-south-1-48704463255

S3 object key
s3://awscodepipeline-demobucket-variables11/aws-codepipeline-s3-aws-codedeploy

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

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

Amazon CloudWatch Events (recommended)
Use Amazon CloudWatch Events to automatically start my pipeline when a change occurs

AWS CodePipeline
Use AWS CodePipeline to check periodically for changes

Cancel **Previous** **Next**

aws Services ▾

Developer Tools **CodePipeline**

Source • CodeCommit
Artifacts • CodeArtifact
Build • CodeBuild
Deploy • CodeDeploy
Pipeline • CodePipeline

Getting started
Pipelines
Pipeline
History
Settings
Settings

Go to resource Feedback

Success Pipeline was saved successfully.

Success The most recent change will re-run through the pipeline. It might take a few moments for the status of the run to show in the pipeline view.

Source Succeeded
Pipeline execution ID: Da1f0e88-64e0-498e-ae02-72b865884a06

Source Amazon S3
Succeeded - 1 minute ago

Source: Amazon S3 version id: Apri0vY4ZworlP1vca1Tf2k5iTWFkdh

Deploy Succeeded
Pipeline execution ID: Da1f0e88-64e0-498e-ae02-72b865884a06

Deploy AWS Elastic Load Balancer
Succeeded - Just now

Source: Amazon S3 version id: Apri0vY4ZworlP1vca1Tf2k5iTWFkdh



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Conclusion

In this experiment, we successfully built and deployed a sample application using AWS CodePipeline. We created a deployment environment, uploaded the sample code to Amazon S3, and configured a pipeline to automate the deployment process. The pipeline retrieved the source code from S3 and deployed it to an Elastic Beanstalk environment. This demonstrated how AWS CodePipeline integrates with S3, Code Build, and Elastic Beanstalk to achieve continuous deployment, simplifying the release process and ensuring efficient application delivery.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)





PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)





PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)





PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)





PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)





PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Semester: V

Academic Year: 2021-22

Class / Branch: TE IT

Subject: Advanced Devops Lab (ADL)

Name of Instructor: Prof. Manjusha K.

Name of Student: Huzaifa Bubere

ID: 24204006

EXPERIMENT NO. 03

Aim: To deploy Sample Application on EC2 instance using AWS Code Deploy.

Static website hosting

- Disable
 Enable

Hosting type

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

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

Index document

Specify the home or default page of the website.

index.html

Error document - optional

This is returned when an error occurs.

error.html



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



← → ⌂ △ Not secure development-bucket-pwa-venny.s3-website.ap-south-1.amazonaws.com

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: DT17FNDF0SQP2BK0
- HostId: cBPs/uElpguM37my8lehnN/vAZtwp3MOyYUyvN4/yNEWLXSY2cLyApGV3NtVbSavLeNV0cROwK0=

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

Verify that it's you Relaunch to update

HOME CARS ABOUT SERVICES CONTACT

Car Zone

WE ARE WHEEL

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

545 VCC

READ MORE

Search by name

Brand

Model

Location

Year

Select Type Of Car

Price

0 USD 150000 USD

SEARCH



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Conclusion

In this experiment, we successfully built and deployed a sample application using AWS CodePipeline. We created a deployment environment, uploaded the sample code to Amazon S3, and configured a pipeline to automate the deployment process. The pipeline retrieved the source code from S3 and deployed it to an Elastic Beanstalk environment. This demonstrated how AWS CodePipeline integrates with S3, Code Build, and Elastic Beanstalk to achieve continuous deployment, simplifying the release process and ensuring efficient application delivery.



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: Huzaifa Bubere****Student ID: 24204006**

EXPERIMENT NO. 04

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

STEP 1: Check security group, delete all SG only keep default

The screenshot shows the AWS EC2 dashboard in the Asia Pacific (Mumbai) region. The left sidebar lists navigation options: EC2, Dashboard, Instances, Images, and Elastic Block Store. The main content area has three main sections: 'Resources' (listing 0 instances, 0 auto scaling groups, 0 capacity reservations, 0 dedicated hosts, 0 elastic IPs, 0 key pairs, 4 security groups, 0 load balancers, 0 snapshots, 0 instances, 0 placement groups, 0 volumes), 'Launch instance' (with 'Launch instance' and 'Migrate a server' buttons), and 'Service health' (showing 'AWS Health Dashboard' and status 'This service is operating normally'). On the right, there's a summary of 'EC2 cost' (date range: Past 6 months, credits remaining: \$159.93 USD, days remaining: 101), and a 'Cost (\$)' section.

Create 2 instance



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



Screenshot of the AWS EC2 Instances Launch screen:

The screenshot shows the AWS EC2 Instances Launch screen. At the top, it says "Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below." Below this, there's a "Name and tags" section where "Venny" is entered. The "Application and OS Images (Amazon Machine Image)" section lists various AMI categories like Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, and Debian. A specific Ubuntu Server 24.04 LTS (HVM) AMI is selected, showing details such as "ami-02d26659f082cf299 (64-bit (x86)) / ami-0890955e00bf0fd92 (64-bit (Arm))". The "Description" section notes that it's a "Ubuntu Server 24.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical [http://www.ubuntu.com/cloud/services]."

On the right side, there's a "Summary" panel with fields for "Number of instances" (set to 1), "Software image (AMI)" (selected as Canonical, Ubuntu, 24.04, amd64), "Virtual server type (instance type)" (selected as t3.micro), "Firewall (security group)" (selected as New security group), and "Storage (volumes)" (selected as 1 volume(s) - 8 GiB). At the bottom right are "Cancel" and "Launch" buttons.

Create key pair

Screenshot of the AWS EC2 Instances Launch screen with a modal for creating a key pair:

The main screen shows the "Instances" section with a selected instance type "t3.micro". The "Key pair (login)" section has "Key pair name" set to "Venny". The "Network settings" section includes "Network" (vpc-046725e34b5339937), "Subnet" (auto), and "Auto-assign public IP" (Enable). The "Firewall (security groups)" section notes that a security group is not yet created. A modal window titled "Create key pair" is open, asking for a "Key pair name" ("Venny") and a "Key pair type" (selected as "RSA"). It also asks for a "Private key file format" (.pem or .ppk) and provides a note about storing the private key securely. At the bottom of the modal are "Cancel" and "Create key pair" buttons.



Create security group and allow traffic

We'll create a new security group called 'launch-wizard-4' with the following rules:

- Allow SSH traffic from Anywhere
- Allow HTTPS traffic from the internet
- Allow HTTP traffic from the internet

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

Configure storage Info

Advanced

1x 16 GiB gp3 Root volume, 3000 IOPS, Not encrypted

Add new volume

The selected AMI contains instance store volumes, however the instance does not allow any instance store volumes. None of the instance store volumes from the AMI will be accessible from the instance.

Click refresh to view backup information

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

0 x File systems

Advanced details Info

Summary

Number of instances | [Info](#)

2

When launching more than 1 instance, consider [EC2 Auto Scaling](#)

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd64... [read more](#)

ami-02d26659fd32cf29

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 16 GiB

Cancel [Launch Inst...](#) Preview

Launch Instance

Launching instance
Creating security group rules

53%

Details

Please wait while we launch your instance.
Do not close your browser while this is loading.



Check security group of both instances

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like Dashboard, AWS Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, Elastic IPs, and Placement Groups. The main area displays a table titled 'Instances (1/2) Info' with two rows. The first row has Public IPv4 DNS as 'ec2-15-255-116-21.ap...', Public IPv4 as '13.233.116.21', and Security group name as 'launch-wizard-4'. The second row has Public IPv4 DNS as 'ec2-13-203-228-156.ap...', Public IPv4 as '13.203.228.156', and Security group name as 'launch-wizard-4'. Below the table, there's a detailed view for the instance 'i-093e044ed94c10e8c (Venny)'. It shows tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. Under the Details tab, it shows Instance ID 'i-093e044ed94c10e8c', Public IPv4 address '13.233.116.21', and Private IPv4 addresses.

Click on connect

The screenshot shows the 'Connect to instance' dialog box. At the top, it says 'Connect info' and 'Connect to an Instance using the browser-based client.' Below that, there are tabs for EC2 Instance Connect, Session Manager, SSH client, and EC2 serial console. The EC2 Instance Connect tab is selected. It shows the Instance ID 'i-093e044ed94c10e8c (Venny-master)' and a 'Connection type' section with two radio buttons: 'Connect using a Public IP' (selected) and 'Connect using a Private IP'. Under 'Public IPv4 address', it shows '13.233.116.21'. There's also a 'Username' field with 'ubuntu' typed in. At the bottom, a note says 'Note: In most cases, the default username, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.' There are 'Cancel' and 'Connect' buttons at the bottom right.

Sameway connect to slave-node



The screenshot shows the AWS EC2 Instance Connect interface. At the top, it says "Connect info" and "Connect to an Instance using the browser-based client." Below this, there are tabs for "EC2 Instance Connect", "Session Manager", "SSH client", and "EC2 serial console". The "EC2 Instance Connect" tab is selected. Under "Instance ID", it shows "i-0db14a051aadf501 (Venny-slave)". Under "Connection type", the "Public IPv4 address" option is selected, showing "13.203.228.156". There is also an option for "Private IP" which is not selected. The "Username" field contains "ubuntu". A note at the bottom says "Note: In most cases, the default username, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username." At the bottom right are "Cancel" and "Connect" buttons.

After Connecting

The screenshot shows a terminal window with a black background and white text. It starts with "Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.6-1811-aws x86_64)". It provides documentation, management, and support links. It then displays system information as of Wednesday, October 8, 2025, at 05:35:18 UTC. The system load is 0.08, memory usage is 22%, and swap usage is 0%. It shows 11.9% of 14.46GB used on the root partition. Processes: 110, Users logged in: 0, and an IPv4 address for ens5: 172.31.2.7. It then lists security updates, noting none are available. It encourages enabling ESM Apps for future updates. It notes that the list of available updates is more than a week old and suggests running sudo apt update. It includes a copyright notice from the Ubuntu project. Finally, it shows the user's details: "i-093e044ed94c10e8c (Venny-master)" and "PublicIPs: 15.233.116.21 PrivateIPs: 172.31.2.7".

Step 2:

Assign Unique Hostname for Each Server Node



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



\$ sudo hostnamectl set-hostname master-node

Than exit

Refresh

```
You are signed in as [REDACTED] Course: ITL504 Advanc... ADL_Exp4 (1).pdf Instances | EC2 | ap-south-1 | EC2 Instance Connect | EC2 Instance Connect | EC2 Instance Connect +  
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1811-aws x86_64)  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/pro  
System information as of Wed Oct 8 05:38:19 UTC 2025  
System load: 0.15 Temperature: -273.1 °C  
Usage of /: 12.6% of 14.46GB Processes: 113  
Memory usage: 22% Users logged in: 0  
Swap usage: 0% IPv4 address for ens5: 172.31.2.7  
Expanded Security Maintenance for Applications is not enabled.  
0 updates can be applied immediately.  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
Last login: Wed Oct 8 05:35:20 2025 from 13.233.177.3  
ubuntu@master-node:~$  
i-093e044ed94c10e8c (Venny-master)  
Public IPs: 15.235.116.21 Private IPs: 172.31.2.7
```

Next, set a worker node hostname by entering the following on the worker server:

\$ sudo hostnamectl set-hostname worker1

STEP 3: On both master and worker1

\$ sudo apt-get update

STEP 4: On both master and worker1



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



```
You are signed in as ... Course: ITL504 Advanc... ADL_Exp4 (1).pdf Instances | EC2 | ap-south-1 EC2 Instance Connect EC2 Instance Connect +  
aws Search [Alt+5] Asia Pacific (Mumbai) Account ID  
  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/pro  
  
System information as of Wed Oct 8 05:38:19 UTC 2025  
  
System load: 0.15 Temperature: -273.1 C  
Usage of /: 12.8% of 14.46GB Processes: 113  
Memory usage: 22% Users logged in: 0  
Swap usage: 0% IPv4 address for ens5: 172.31.2.7  
  
Expanded Security Maintenance for Applications is not enabled.  
0 updates can be applied immediately.  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
Last login: Wed Oct 8 05:35:20 2025 from 13.233.177.3  
ubuntu@master-node:~$ sudo apt-get update  
Hit:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble InRelease  
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]  
Get:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]  
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]  
Get:5 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]  
Get:6 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]  
Get:7 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]  
Get:8 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]  
Get:9 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]  
Get:10 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]  
Get:11 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]  
Get:12 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]  
  
i-093e044ed94c10e8c (Venny-master)  
Public IPs: 13.233.116.21 Private IPs: 172.31.2.7
```

```
You are signed in as ... Course: ITL504 Advanc... ADL_Exp4 (1).pdf Instances | EC2 | ap-south-1 EC2 Instance Connect EC2 Instance Connect +  
aws Search [Alt+5] Asia Pacific (Mumbai) Account ID  
  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/pro  
  
System information as of Wed Oct 8 05:38:27 UTC 2025  
  
System load: 0.0 Temperature: -273.1 C  
Usage of /: 12.8% of 14.46GB Processes: 112  
Memory usage: 22% Users logged in: 0  
Swap usage: 0% IPv4 address for ens5: 172.31.12.189  
  
Expanded Security Maintenance for Applications is not enabled.  
0 updates can be applied immediately.  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
Last login: Wed Oct 8 05:36:40 2025 from 13.233.177.4  
ubuntu@slave-node:~$ sudo apt-get update  
Hit:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble InRelease  
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]  
Get:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]  
Get:4 http://ap-south-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-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]  
Get:7 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]  
Get:8 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]  
Get:9 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]  
Get:10 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]  
Get:11 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]  
Get:12 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]  
  
i-0ddb14a051aadf501 (Venny-slave)  
Public IPs: 13.205.228.156 Private IPs: 172.31.12.189
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



```
Get:56 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [384 B]
Fetched 37.9 MB in 7s (5640 kB/s)
Reading package lists... Done
ubuntu@master-node:~$ sudo apt-get install docker.io
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:
  ifupdown autils cgroups-mount | cgroup-lite debootstrap docker-buildx docker-compose-v2 docker-doc rinse zfs-fuse | zfsutils
The Following NEW packages will be installed:
  bridge-utils containerd dns-root-data dnsmasq-base docker.io pigz runc ubuntu-fan
0 upgraded, 8 newly installed, 0 to remove and 41 not upgraded.
Need to get 75.9 MB of archives.
After this operation, 288 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 pigz amd64 2.8-1 [65.6 KB]
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu/noble/main amd64 bridge-utils amd64 1.7.1-1ubuntu2 [33.9 kB]
Get:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu/noble-updates/main amd64 runc amd64 1.8.0-0ubuntu2-24.04.1 [8748 kB]
Get:4 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu/noble-updates/main amd64 containerd amd64 1.7.28-0ubuntu1-24.04.1 [38.4 MB]
Get:5 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu/noble-updates/main amd64 dns-root-data all 2024071801-ubuntu0.24.04.1 [5918 B]
Get:6 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu/noble-updates/main amd64 dnsmasq-base amd64 2.90-2ubuntu0.1 [376 kB]
Get:7 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu/noble-updates/universe amd64 docker.io amd64 28.2.2-0ubuntu1-24.04.1 [28.3 MB]
Get:8 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu/noble-updates/universe amd64 ubuntu-fan all 0.12.16+24.04.1 [34.2 KB]
Fetched 75.9 MB in 1s (59.1 MB/s)
Preconfiguring packages ...
Selecting previously unselected package pigz.
(Reading database ... 73728 files and directories currently installed.)
Preparing to unpack .../0-pigz_2.8-1_amd64.deb ...
Unpacking pigz (2.8-1) ...
Selecting previously unselected package bridge-utils.
Preparing to unpack .../1-bridge-utils_1.7.1-1ubuntu2_amd64.deb ...
Unpacking bridge-utils (1.7.1-1ubuntu2) ...
Selecting previously unselected package runc.
Preparing to unpack .../2-runc_1.3.0-0ubuntu2-24.04.1_amd64.deb ...

```

i-093e044ed94c10e8c (Venny-master)
Public IPs: 13.233.116.21 Private IPs: 172.31.2.7

Install docker sudo apt-get install docker.io

STEP 5 :

Start and Enable Docker Set Docker to launch at boot by entering the following:

\$ sudo systemctl enable docker

\$ sudo systemctl status docker



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



```
You are signed in as ... Course: ITL504 Advanc... ADL_Exp4 (1).pdf Instances | EC2 | ap... EC2 Instance Connect EC2 Instance Connect +  
← → ⌂ ap-south-1.console.aws.amazon.com/ec2-instance-connect/sshd/home?region=ap-south-1&connType=standard&instanceId=i-0ddb14a051aadf501&osUser=ubuntu&sshPort=22&addressFa... Search [Alt+S] AWS Account ID: Asia Pacific (Mumbai)  
  
Get:56 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [384 B]  
Fetched 37.9 MB in 0s (6234 kB/s)  
Reading package lists... Done  
ubuntu@slave-node:~$ sudo apt-get install docker.io  
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:  
  ifupdown attrs-tools cgroups-mount | cgroup-lite debootstrap docker-buildx docker-compose-v2 docker-doc rinse zfs-fuse | zfsutils  
The following NEW packages will be installed:  
  bridge-utils containerd dns-root-data dnsmasq-base docker.io pigz runc ubuntu-fan  
0 upgraded, 8 newly installed, 0 to remove and 41 not upgraded.  
Need to get 75.9 MB of archives.  
After this operation, 288 MB of additional disk space will be used.  
Do you want to continue? [Y/n] Y  
Get:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 pigz amd64 2.8-1 [65.6 kB]  
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 bridge-utils amd64 1.7.1-1ubuntu2 [33.9 kB]  
Get:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 runc amd64 1.8.0-0ubuntu2-24.04.1 [8743 kB]  
Get:4 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 containerd amd64 1.7.28-0ubuntu1-24.04.1 [38.4 MB]  
Get:5 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 dns-root-data all 2024071801-ubuntu0.24.04.1 [5918 B]  
Get:6 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 dnsmasq-base amd64 2.90-2ubuntu0.1 [376 kB]  
Get:7 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 docker.io amd64 28.2.2-0ubuntu1-24.04.1 [28.3 MB]  
Get:8 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 ubuntu-fan all 0.12.16+24.04.1 [34.2 kB]  
Fetched 75.9 MB in 0s (81.7 MB/s)  
Preconfiguring packages ...  
Selecting previously unselected package pigz.  
(Reading database ... 73728 files and directories currently installed.)  
Preparing to unpack .../pigz_2.8-1_amd64.deb ...  
Unpacking pigz (2.8-1) ...  
Selecting previously unselected package bridge-utils.  
Preparing to unpack .../bridge-utils_1.7.1-1ubuntu2_amd64.deb ...  
Unpacking bridge-utils (1.7.1-1ubuntu2) ...  
Selecting previously unselected package runc.  
Preparing to unpack .../runc_1.3.0-0ubuntu2-24.04.1_amd64.deb ...  
  
i-0ddb14a051aadf501 (Venny-slave)  
PublicIPs: 13.203.228.156 PrivateIPs: 172.31.12.189  
  
  
The following packages were automatically installed and are no longer required:  
ubuntu@master-node:~$ sudo systemctl enable docker  
ubuntu@master-node:~$ sudo systemctl start docker  
ubuntu@master-node:~$  
  
i-093e044ed94c10e8c (Venny-master)  
PublicIPs: 13.235.116.21 PrivateIPs: 172.31.2.7  
  
  
ubuntu@slave-node:~$ sudo systemctl enable docker  
ubuntu@slave-node:~$ sudo systemctl start docker  
ubuntu@slave-node:~$  
  
i-0ddb14a051aadf501 (Venny-slave)  
PublicIPs: 13.203.228.156 PrivateIPs: 172.31.12.189
```

STEP 6 Install Kubernetes

<https://kubernetes.io/docs/setup/productionenvironment/tools/kubeadm/install-kubeadm/>



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



kubernetes.io/docs/setup/production-environment/tools/kubeadm/install-kubeadm/

kubernetes Documentation Kubernetes Blog Training Careers Partners Community Versions English Search this site

version. If you want to install a minor version other than v1.34, please see the installation guide for your desired minor version.

Debian-based distributions Red Hat-based distributions

Without a package manager

These instructions are for Kubernetes v1.34.

1. Update the apt package index and install packages needed to use the Kubernetes apt repository:

```
sudo apt-get update
# apt-transport-https may be a dummy package; if so, you can skip it
sudo apt-get install -y apt-transport-https ca-certificates curl
```

2. Download the public signing key for the Kubernetes package repositories. The same signing key is used for all repositories so you can disregard the version in the URL:

```
# If the directory '/etc/apt/keyrings' does not exist, it's likely that apt-transport-https was not installed
# sudo mkdir -p /etc/apt/keyrings
curl -fsSL https://pkgs.k8s.io/core:/stable:/v1.34/deb/Release | gpg --dearmor > /etc/apt/keyrings/kubernetes-keyring.gpg
```

Note:
In releases older than Debian 12 and Ubuntu 22.04, directory

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 (8.5.6-2ubuntu10.6).
curl set to manually installed.
gpg is already the newest version (2.4.4-2ubuntu17.3).
gpg set to manually installed.
The following NEW packages will be installed:
  apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 41 not upgraded.
Need to get 3970 B of archives.
After this operation, 36.0 kB of additional disk space will be used.
Get:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 apt-transport-https all 2.8.3 [3970 B]
Fetched 3978 B in 8s (291 kB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 72985 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.8.3_all.deb ...
Unpacking apt-transport-https (2.8.3) ...
Setting up apt-transport-https (2.8.3) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@master-node:~$
```

i-093e044ed94c10e8c (Venny-master)
PublicIP: 13.235.116.21 PrivateIP: 172.51.2.7



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY



Department of Information Technology

(NBA Accredited)

```
ubuntu@slave-node:~$ sudo systemctl start docker
ubuntu@slave-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 (8.5.0-2ubuntu18.6).
curl set to manually installed.
gpg is already the newest version (2.4.4-2ubuntu17.3).
gpg set to manually installed.
The following NEW packages will be installed:
  apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 41 not upgraded.
Need to get 3970 B of archives.
After this operation, 36.0 kB of additional disk space will be used.
Get:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 apt-transport-https all 2.8.3 [3970 B]
Fetched 3978 B in 8s (267 kB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 72085 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.8.3_all.deb ...
Unpacking apt-transport-https (2.8.3) ...
Setting up apt-transport-https (2.8.3) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@slave-node:~$
```

i-0ddb14a051aadf501 (Venny-slave)

PublicIPs: 13.205.228.156 PrivateIPs: 172.51.12.189

Signining key

```
curl is already the newest version (8.5.0-2ubuntu18.6).
curl set to manually installed.
gpg is already the newest version (2.4.4-2ubuntu17.3).
gpg set to manually installed.
The following NEW packages will be installed:
  apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 41 not upgraded.
Need to get 3970 B of archives.
After this operation, 36.9 kB of additional disk space will be used.
Get:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 apt-transport-https all 2.8.3 [3970 B]
Fetched 3978 B in 8s (267 kB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 72085 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.8.3_all.deb ...
Unpacking apt-transport-https (2.8.3) ...
Setting up apt-transport-https (2.8.3) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@slave-node:~$ curl -fsSL https://pkgs.k8s.io/core/stable:/v1.34/deb/Release.key | sudo gpg --dearmor -o /etc/apt/keyrings/kubernetes-apt-keyring.gpg
ubuntu@slave-node:~$ sudo apt-get update
Hit:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
ubuntu@slave-node:~$
```

i-0ddb14a051aadf501 (Venny-slave)

PublicIPs: 13.205.228.156 PrivateIPs: 172.51.12.189



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



```
Preparing to unpack .../2-kubeadm_1.34.1-1.1_amd64.deb ...
Unpacking kubeadm (1.34.1-1.1) ...
Selecting previously unselected package kubelet.
Preparing to unpack .../3-kubelet_1.34.1-1.1_amd64.deb ...
Unpacking kubelet (1.34.1-1.1) ...
Selecting previously unselected package kubernetes-cni.
Preparing to unpack .../4-kubernetes-cni_1.7.1-1.1_amd64.deb ...
Unpacking kubernetes-cni (1.7.1-1.1) ...
Selecting previously unselected package kubelet.
Preparing to unpack .../5-kubelet_1.34.1-1.1_amd64.deb ...
Unpacking kubelet (1.34.1-1.1) ...
Setting up conntrack (1:1.4.8-1ubuntu1) ...
Setting up kubelet (1.34.1-1.1) ...
Setting up cri-tools (1.34.0-1.1) ...
Setting up kubernetes-cni (1.7.1-1.1) ...
Setting up kubeadm (1.34.1-1.1) ...
Setting up kubelet (1.34.1-1.1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@master-node:$ sudo apt-mark hold kubelet kubeadm kubelet
kubelet set on hold.
kubeadm set on hold.
kubelet set on hold.
ubuntu@master-node:$ sudo systemctl enable --now kubelet
ubuntu@master-node:$ 
```

i-093e044ed94c10e8c (Venny-master)

PublicIPs: 13.235.116.21 PrivateIPs: 172.51.2.7

```
Preparing to unpack .../2-kubeadm_1.34.1-1.1_amd64.deb ...
Unpacking kubeadm (1.34.1-1.1) ...
Selecting previously unselected package kubelet.
Preparing to unpack .../3-kubelet_1.34.1-1.1_amd64.deb ...
Unpacking kubelet (1.34.1-1.1) ...
Selecting previously unselected package kubernetes-cni.
Preparing to unpack .../4-kubernetes-cni_1.7.1-1.1_amd64.deb ...
Unpacking kubernetes-cni (1.7.1-1.1) ...
Selecting previously unselected package kubelet.
Preparing to unpack .../5-kubelet_1.34.1-1.1_amd64.deb ...
Unpacking kubelet (1.34.1-1.1) ...
Setting up conntrack (1:1.4.8-1ubuntu1) ...
Setting up kubelet (1.34.1-1.1) ...
Setting up cri-tools (1.34.0-1.1) ...
Setting up kubernetes-cni (1.7.1-1.1) ...
Setting up kubeadm (1.34.1-1.1) ...
Setting up kubelet (1.34.1-1.1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@slave-node:$ sudo apt-mark hold kubelet kubeadm kubelet
kubelet set on hold.
kubeadm set on hold.
kubelet set on hold.
ubuntu@slave-node:$ sudo systemctl enable --now kubelet
ubuntu@slave-node:$ 
```

i-0ddb14a051aadf501 (Venny-slave)

PublicIPs: 13.205.228.156 PrivateIPs: 172.51.12.189



```
[mark-control-plane] Marking the node master-node as control-plane by adding the taints [node-role.kubernetes.io/control-plane:NoSchedule]
[bootstrap-token] Using token: myqun.v9g6jkkjkbjw6
[bootstrap-token] Configuring bootstrap tokens, cluster-info ConfigMap, RBAC Roles
[bootstrap-token] Configured RBAC rules to allow Node Bootstrap tokens to get nodes
[bootstrap-token] Configured RBAC rules to allow Node Bootstrap tokens to post CSRs in order for nodes to get long term certificate credentials
[bootstrap-token] Configured RBAC rules to allow the csrapprover controller automatically approve CSRs from a Node Bootstrap Token
[bootstrap-token] Configured RBAC rules to allow certificate rotation for all node client certificates in the cluster
[bootstrap-token] Creating the "cluster-info" ConfigMap in the "kube-public" namespace
[kubelet-finalize] Updating "/etc/kubernetes/kubelet.conf" to point to a rotatable kubelet client certificate and key
[addons] Applied essential addon: CoreDNS
[addons] Applied essential addon: kube-proxy

Your Kubernetes control-plane has initialized successfully!

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

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

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

export KUBECONFIG=/etc/kubernetes/admin.conf

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

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

kubeadm join 172.31.2.7:6443 --token myqun.v9g6jkkjkbjw6 \
    --discovery-token-ca-cert-hash sha256:cc2a2f007456923054ba829e890ecb20c241a52aecb6a0b868b91181a3ec5be3
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) $HOME/.kube/config
ubuntu@master-node:~$ 
```

i-093e044ed94c10e8c (Venny-master)

PublicIPs: 15.235.116.21 PrivateIPs: 172.51.2.7

STEP 10 Copy weblink from masternode <https://kubernetes.io/docs/concepts/cluster-administration/addons/>

kubernetes Documentation Kubernetes Blog Training Careers Partners Community Versions English Search

KubeCon + CloudNativeCon 2025
join us for four days of incredible opportunities to collaborate, learn and share with the cloud native community.
Buy your ticket now! 10 - 13 November | Atlanta, Georgia

Kubernetes Documentation / Concepts / Cluster Administration / Installing Addons

Installing Addons

Note: This section links to third party projects that provide functionality required by Kubernetes. The Kubernetes project authors aren't responsible for these projects, which are listed alphabetically. To add a project to this list, read the [content guide](#) before submitting a change. [More information.](#)

Add-ons extend the functionality of Kubernetes.

This page lists some of the available add-ons and links to their respective installation instructions. The list does not try to be exhaustive.

Networking and Network Policy

Edit this page
 Third party content advice
 Create child page
 Create an issue
 Print entire section

Networking and Network Policy
Service Discovery
Visualization & Control
Infrastructure
Instrumentation
Legacy Add-ons



goto flannel copy this command and paste on master

Deploying flannel manually

Flannel can be added to any existing Kubernetes cluster though it's simplest to add `flannel` before any pods using the pod network have been started.

For Kubernetes v1.17+

Deploying Flannel with kubectl

```
kubectl apply -f https://github.com/flannel-io/flannel/releases/latest/download/kube-flannel.yaml
```

If you use custom `podCIDR` (not `10.244.0.0/16`) you first need to download the above manifest and modify the network to match your one.

Deploying Flannel with helm

```
# Needs manual creation of namespace to avoid helm error
kubectl create ns kube-flannel
kubectl label --overwrite ns kube-flannel pod-security.kubernetes.io/enforce=privileged

helm repo add flannel https://flannel.io.github.io/flannel/
helm install flannel --set podCidr="10.244.0.0/16" --namespace kube-flannel flannel/flannel
```

See [Kubernetes](#) for more details.

In case a firewall is configured ensure to enable the right port used by the configured [backend](#).

Flannel uses `portmap` as CNI network plugin by default; when deploying Flannel ensure that the [CNI Network plugins](#) are installed in `/opt/cni/bin` the latest binaries can be downloaded with the following commands:

Conclusion: In this experiment We Have Learnt About Kubernetes Cluster Architecture, install and Spin Up a Kubernetes Cluster on Linux Machines/Cloud Platforms.



Semester: V
Academic Year: 2025-26
Class / Branch: TE IT
Subject: Advanced Devops Lab (ADL)
Name of Instructor: Prof. Vishal Badgujar

Name of Student: Huzaifa Bubere
Student ID: 24204006

EXPERIMENT NO. 05

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

Terraform Installation Steps on Ubuntu18.04

Step: 1 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 Terraform installation page on developer.hashicorp.com/terraform/install. The left sidebar lists operating systems: macOS, Windows, Linux (selected), FreeBSD, OpenBSD, Solaris, Release information, and Next steps. The main content area shows a terminal window titled "Ubuntu/Debian" with the command to add the HashiCorp GPG key and update the apt repository. Below this is a "Binary download" section for Linux, showing links for 386, AMD64, ARM, and ARM64 architectures, each with a "Download" button. A note at the bottom encourages users to complete a tutorial to learn how to install and verify HashiCorp tools. The right sidebar contains sections for "About Terraform" (defining it as a tool for managing cloud and on-prem resources), "Featured docs" (Introduction to Terraform, Configuration Language, Terraform CLI, HCP Terraform, Provider Use), and a "HCP Terraform" section (Automate your infrastructure provisioning at any scale).



Step:2 unzip the archive by using below command

```
nagios@apsit-HP-280-Pro-G6-Microtower-PC:~/Downloads$ unzip terraform_1.12.2_linux_amd64.zip
Archive:  terraform_1.12.2_linux_amd64.zip
  inflating: LICENSE.txt
  inflating: terraform
```

The archive will extract a single binary called **terraform**.

Step 3: Change the directory to unzipped folder

```
nagios@apsit-HP-280-Pro-G6-Microtower-PC:~/Downloads$ cd terraform_1.12.2_linux_amd64
nagios@apsit-HP-280-Pro-G6-Microtower-PC:~/Downloads/terraform_1.12.2_linux_amd64$
```

and Move the **terraform** binary to a directory included in your system's PATH in my case *usr/local/bin*/

Step 4: To check whether Terraform is installed, run:

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/Downloads/terraform_1.12.2_linux_amd64$ sudo mv terraform /usr/local/bin/
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/Downloads/terraform_1.12.2_linux_amd64$ terraform -v
Terraform v1.12.2
on linux_amd64
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/Downloads/terraform_1.12.2_linux_amd64$
```

Conclusion: In This Experiment We have Learnt About Terraform lifecycle, core concepts/terminologies and install it on a Linux Machine.



Semester: V
Academic Year: 2022-23
Class / Branch: TE IT
Subject: Advanced Devops Lab (ADL)
Name of Instructor: Prof. Vishal Badgujar

Name of Student: Huzaifa Bubere
Student ID: 24204006

EXPERIMENT NO. 06

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

Pre-requisites:

1. Install the AWS CLI version 2 on Linux

Follow these steps from the command line to install the AWS CLI on Linux.

Install curl on linux

```
apsit@apsit-HP-280-Pro-G6-Mictrotower-PC:~/Downloads/terraform_1.12.2_linux_amd64$ 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).
0 upgraded, 0 newly installed, 0 to remove and 59 not upgraded.
apsit@apsit-HP-280-Pro-G6-Mictrotower-PC:~/Downloads/terraform_1.12.2_linux_amd64$
```

```
apsit@apsit:~$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
```

```
apsit@apsit-HP-280-Pro-G6-Mictrotower-PC:~/Downloads/terraform_1.12.2_linux_amd64$ sudo curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
% Total    % Received % Xferd  Average Speed   Time     Time      Current
          Dload  Upload Total   Spent   Left Speed
100 59.0M  100 59.0M    0     0  6899K  0:00:08  0:00:08 --:--:-- 11.2M
apsit@apsit-HP-280-Pro-G6-Mictrotower-PC:~/Downloads/terraform_1.12.2_linux_amd64$
```

```
apsit@apsit:~$ sudo apt install unzip
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/Downloads/terraform_1.12.2_linux_amd64$ sudo apt install unzip
Reading package lists... Done
Building dependency tree
Reading state information... Done
unzip is already the newest version (6.0-21ubuntui.2).
0 upgraded, 0 newly installed, 0 to remove and 59 not upgraded.
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/Downloads/terraform_1.12.2_linux_amd64$
```

apsit@apsit:~\$ sudo unzip awscliv2.zip

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/Downloads/terraform_1.12.2_linux_amd64$ sudo unzip awscliv2.zip
Archive: awscliv2.zip
  creating: aws/
  creating: aws/dist/
  inflating: aws/THIRD_PARTY_LICENSES
  inflating: aws/README.md
  inflating: aws/install
  creating: aws/dist/awscli/
  creating: aws/dist/dateutil/
  creating: aws/dist/docutils/
  creating: aws/dist/lib-dynload/
  creating: aws/dist/prompt_toolkit-3.0.51.dist-info/
  creating: aws/dist/wheel-0.45.1.dist-info/
```

apsit@apsit:~\$ sudo ./aws/install

apsit@apsit:~\$ aws --version

it should display the below output.

aws-cli/2.1.29 Python/3.8.8 Linux/5.4.0-1038-aws exe/x86_64.ubuntu.18 prompt/off



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



Department of Information Technology

(NBA Accredited)

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/Downloads/terraform_1.12.2_linux_amd64$ sudo ./aws/install
Found preexisting AWS CLI installation: /usr/local/aws-cli/v2/current. Please rerun install script with --update flag.
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/Downloads/terraform_1.12.2_linux_amd64$ aws --version
aws-cli/2.13.12 Python/3.11.4 Linux/5.4.0-158-generic exe/x86_64 ubuntu.18 prompt/off
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/Downloads/terraform_1.12.2_linux_amd64$
```

2. Create a new access key if you don't have one. Make sure you download the keys in your local machine.

Login to AWS console, click on username and go to My security credentials.

The screenshot shows the AWS IAM 'My security credentials' page. On the left, there's a sidebar with options like Roles, Policies, Identity providers, Account settings, Root access management, Access reports, Access Analyzer, Credential report, Organization activity, Service control policies, and Resource control policies. The main area has two sections: 'Multi-factor authentication (MFA)' (0) and 'Access keys' (1). The 'Multi-factor authentication' section has a table with columns Type, Identifier, and Certificate. There's a button labeled 'Assign MFA device'. The 'Access keys' section has a table with columns Access key ID, Created on, and Access key last used. One row is shown in the table. On the right side, there's a 'Free plan status' section showing Credits remaining (\$140.00 USD) and Days remaining (166 days), along with links to Account ID (1255-8227-1444), Account, Organization, Service Quotas, Billing and Cost Management, and Security credentials. At the bottom right, there's a 'Turn on multi-session support' button.



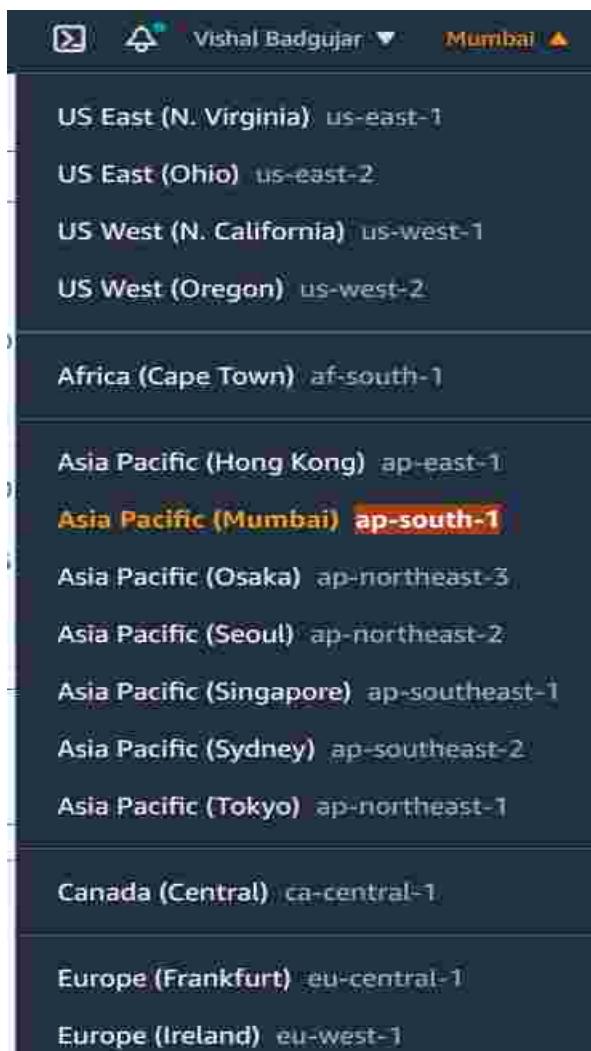
Continue on security credentials, click on access keys

Perform below commands in Linux where you have installed Terraform

First setup your access keys, secret keys and region code locally.

apsit@apsit:~\$aws configure

You can check region as shown in below image :





```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/Downloads/terraform_1.12.2_linux_amd64$ aws configure
AWS Access Key ID [*****NM34]: AKIAR2PKJMPKNOIWRU7Z
AWS Secret Access Key [*****fleU]: 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
Default region name [us-east-1]: ap-south-1
Default output format [None]:
```

Create one Directory for Terraform project in which all files of terraform we can save

```
apsit@apsit:~$ cd ~
apsit@apsit:~$ mkdir project-terraform
apsit@apsit:~$ cd project-terraform
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/Downloads/terraform_1.12.2_linux_amd64$ cd
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ mkdir project-terraform
mkdir: cannot create directory 'project-terraform': File exists
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ mkdir projects-terraform
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ cd projects-terraform
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/projects-terraform$ █
```

Create Terraform Files

[vishal@apsit:~\\$ sudo nano variables.tf](#)

The screenshot shows the AWS Management Console with the EC2 service selected. The main content area displays information about virtual servers in the cloud, mentioning the broadest and deepest compute platform with over 600 instance types. Below this, a section titled 'Benefits and features' highlights the ultimate scalability and control of EC2, stating it offers fully resizable compute capacity. It also lists several key benefits: highest level of control, widest variety of server size options, widest availability of operating systems, and global scalability.

In order to provide key name in variables first create key pair as shown:

chnology | APSIT



Give name to key pair file as **terraform**

The screenshot shows the 'Create key pair' form on the AWS EC2 website. The 'Name' field is filled with 'terraform'. The 'Key pair type' section shows 'RSA' selected. Under 'Private key file format', '.pem' is selected. There are no tags added. At the bottom right are 'Cancel' and 'Create' buttons.

Name: terraform
Key pair type: RSA
Private key file format: .pem
Tags - optional: No tags associated with the resource.
Add new tag
Cancel Create



Key pair is generated

The screenshot shows the AWS Management Console with the AWS Lambda service selected. On the left, a navigation pane lists services like EC2, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs), and Network Interfaces. The 'Key Pairs' link under 'Network & Security' is highlighted in blue. The main content area displays a green success message: 'Successfully created key pair'. Below it is a table titled 'Key pairs (1) Info' with one item listed:

Name	Type	Created	Fingerprint	ID
terraform	rsa	2025/06/06 11:27 GMT+5:30	c9:88:4a:ff:f3:f9:1c:28:dd:7c:45:55:a...	key

Use your Region and Key name in variable.tf as shown and provide instance type which you want to create.



```
GNU nano 2.9.3                                         variables.tf

variable "aws_region" {
  description = "The AWS region to create things in."
  default     = "ap-south-1"
}

variable "key_name" {
  description = "SSH keys to connect to ec2 instance"
  default     = "terraform"
}

variable "instance_type" {
  description = "instance type for ec2"
  default     = "t2.micro"
}
```

After creating variable terraform file note down the AMI ID of instance which u want to create which we will use to configure our instance in main.tf file.



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



The screenshot shows the AWS EC2 'Launch an instance' wizard. In the left sidebar, the path 'EC2 > Instances > Launch an instance' is visible. The main area displays a grid of Linux AMIs, with the 'Ubuntu Server 24.04 LTS (HVM), SSD Volume Type' AMI selected. This AMI is highlighted with a yellow border and labeled 'Free tier eligible'. To the right, a 'Summary' section is expanded, showing details like the instance type (t3.micro), security group (New security group), and storage (1 volume(s) - 8 GiB). At the bottom right of the summary section are 'Cancel' and 'Launch' buttons.

Now create main.tf file:

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/projects-terraform$ sudo nano main.tf
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/projects-terraform$
```



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

Department of Information Technology

(NBA Accredited)



```
provider "aws" {
```

```
    region = var.aws_region
```

```
}
```

```
#Create security group with firewall rules
```

```
resource "aws_security_group" "security_jenkins_port" {
```

```
    name      = "security_jenkins_port"
```

```
    description = "security group for jenkins"
```

```
    ingress {
```

```
        from_port  = 8080
```

```
        to_port    = 8080
```

```
        protocol   = "tcp"
```

```
        cidr_blocks = ["0.0.0.0/0"]
```

```
}
```

```
    ingress {
```

```
        from_port  = 22
```

```
        to_port    = 22
```

```
        protocol   = "tcp"
```

```
        cidr_blocks = ["0.0.0.0/0"]
```

```
}
```

```
# outbound from Jenkins server
```

```
    egress {
```

```
        from_port  = 0
```

```
        to_port    = 65535
```



```
protocol = "tcp"  
cidr_blocks = ["0.0.0.0/0"]  
}
```

```
tags= {  
    Name = "security_jenkins_port"  
}  
}
```

```
resource "aws_instance" "myFirstInstance" {  
    ami      = "ami-0f918f7e67a3323f0"  
    key_name = var.key_name  
    instance_type = var.instance_type  
    security_groups= [ "security_jenkins_port"]  
    tags= {  
        Name = "jenkins_instance"  
    }  
}
```

Put AMI-ID in above highlighted space and Now execute the below command:

you should see like below screenshot.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/projects-terraform$ terraform init
Initializing the backend...
Initializing provider plugins...
- Finding latest version of hashicorp/aws...
- Installing hashicorp/aws v6.7.0...
- Installed hashicorp/aws v6.7.0 (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.
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/projects-terraform$
```

Execute the below command

the above command will show how many resources will be added.
Plan: 3 to add, 0 to change, 0 to destroy.

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/projects-terraform$ 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-0f918f7e07a3323f0"
    + 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)
    + get_password_data                 = false
    + host_id                            = (known after apply)
    + host_resource_group_arn            = (known after apply)
    + iam_instance_profile               = (known after apply)
    + id                                 = (known after apply)
    + instance_initiated_shutdown_behavior = (known after apply)
    + instance_lifecycle                = (known after apply)
    + instance_state                     = (known after apply)
    + instance_type                      = "t2.micro"
    + ipv6_address_count                = (known after apply)
    + ipv6_addresses                     = (known after apply)
    + key_name                           = "terraform"
    + monitoring                         = (known after apply)
    + outpost_arn                        = (known after apply)
    + password_data                      = (known after apply)
    + placement_group                    = (known after apply)
    + placement_partition_number         = (known after apply)
    + primary_network_interface_id      = (known after apply)
    + private_dns                         = (known after apply)
    + private_ip                          = (known after apply)
    + public_dns                          = (known after apply)
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



```
      }
+ vpc_id          = (known after apply)
}

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

Execute the below command



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



```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~/projects-terraform$ terraform apply

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

Terraform will perform the following actions:

# aws_instance.myFirstInstance will be created
+ resource "aws_instance" "myFirstInstance" {
    + ami                                = "ami-0f918f7e07a3323f0"
    + 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)
    + get_password_data                = false
    + host_id                            = (known after apply)
    + host_resource_group_arn           = (known after apply)
    + iam_instance_profile              = (known after apply)
    + id                                 = (known after apply)
    + instance_initiated_shutdown_behavior = (known after apply)
    + instance_lifecycle                = (known after apply)
    + instance_state                   = (known after apply)
    + instance_type                     = "t2.micro"
    + ipv6_address_count                = (known after apply)
    + ipv6_addresses                    = (known after apply)
    + key_name                           = "terraform"
    + monitoring                         = (known after apply)
    + outpost_arn                        = (known after apply)
    + password_data                     = (known after apply)
    + placement_group                   = (known after apply)
```

Provide the value as Yes for applying terraform

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

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

Enter a value: yes
```



Plan: 3 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

Apply complete! Resources: 3 added, 0 changed, 0 destroyed.

Now login to EC2 console, to see the new instances up and running, you can see Jenkins_instance is up and running which we deploy from terraform.

You can also check the security group resource details which you created from terraform :

Terraform destroy

you can also destroy or delete your instance by using terraform destroy command :

```
vishal@apsit:~/project-terraform$ terraform destroy
```

Now you can see instance which you created by using terraform is deleted successfully from aws console also you can check it will removed successfully:



The screenshot shows the AWS CloudFormation Instances page. The left sidebar has a 'EC2' section with 'Instances' selected. The main area displays a table titled 'Instances (1)'. The table contains one row with the following details:

Name	Instance ID	Instance State	Instance Type	Health Check	Alarm Status
jenkins_instance	i-01234567890123456	Running	t2.micro	Passing	Normal

Below the table, a modal window titled 'Select an instance' is open, showing the same instance information.

All the Resources including Security groups, EC2 instances using terraform will be deleted. In this way we can automate infrastructure set up using terraform in aws cloud.

Conclusion: In this Experiment We have Learnt About Build, change, and destroy AWS infrastructure Using Terraform.



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: Huzaifa Bubere

Student ID: 24204006

EXPERIMENT NO. 07

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

Steps:

- 1) Install and configure a Jenkins and SonarQube CICD environment using Docker containers.
- 2) Configure Jenkins with the SonarQube Scanner plugin for automated static code analysis.

```
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ wget -q -O - https://pkg.jenkins.io/debian-stable/jenkins.io.key | sudo apt-key add -
[sudo] password for apsit:
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo sh -c 'echo deb http://pkg.jenkins.io/debian-stable binary/ > /etc/apt/sources.list.d/jenkins.list'
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo apt update
E: Invalid operation update.
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo apt update
Ign:1 https://pkg.jenkins.io/debian-stable binary/ InRelease
Get:2 https://pkg.jenkins.io/debian-stable binary/ Release [2,044 B]
Get:3 https://pkg.jenkins.io/debian-stable binary/ Release.gpg [833 B]
Get:4 https://dl.google.com/linux/chrome/deb stable InRelease [1,825 B]
Get:5 https://pkg.jenkins.io/debian-stable binary/ Packages [29.7 kB]
Get:6 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,214 B]
Get:7 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:8 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:9 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [54.6 kB]
Get:11 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
```



```
Preparing to unpack .../jenkins_2.516.3_all.deb ...
Unpacking jenkins (2.516.3) over (2.516.2) ...
Setting up jenkins (2.516.3) ...
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo systemctl start jenkins
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo systemctl status jenkins
● jenkins.service - Jenkins Continuous Integration Server
   Loaded: loaded (/lib/systemd/system/jenkins.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2025-09-18 10:52:06 IST; 38s ago
       Main PID: 5883 (java)
          Tasks: 72 (limit: 9050)
         Memory: 936.2M
            CPU: 21.796s
           CGroup: /system.slice/jenkins.service
               └─ 5883 /usr/bin/java -Djava.awt.headless=true -jar /usr/share/java/jenklns.war --webroot=/var/cache/jenkins/war --httpPort=8080

Sep 18 10:52:00 apsit@HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: [LF]> This may also be found at: /var/lib/jenkins/secrets/initialAdminPassword
Sep 18 10:52:00 apsit@HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: [LF]>
Sep 18 10:52:00 apsit@HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: [LF]> ****
Sep 18 10:52:00 apsit@HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: [LF]> ****
Sep 18 10:52:00 apsit@HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: [LF]> ****
Sep 18 10:52:06 apsit@HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: 2025-09-18 05:22:06.041+0000 [id=57]      INFO      jenkins.InitReactorRunner$1#onAttainE>
Sep 18 10:52:06 apsit@HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: 2025-09-18 05:22:06.053+0000 [id=33]      INFO      hudson.lifecycle.Lifecycle#onReady: JB
Sep 18 10:52:06 apsit@HP-Pro-Tower-280-G9-E-PCI-Desktop-PC systemd[1]: Started Jenkins Continuous Integration Server.
Sep 18 10:52:07 apsit@HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: 2025-09-18 05:22:07.972+0000 [id=98]      INFO      h.m.DownloadService$Downloadable#load>
Sep 18 10:52:07 apsit@HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: 2025-09-18 05:22:07.973+0000 [id=98]      INFO      hudson.util.Retrier#start: Performed >
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo ufw allow 8080
Rules updated
Rules updated (v6)
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ ^[[200-sudo cat /var/lib/jenkins/secrets/initialAdminPassword
sudo: command not found
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo cat /var/lib/jenkins/secrets/initialAdminPassword
90ac065b1344cd5b878cd461b39f50a
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ ^C
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ docker run -d -p 9000:9000 sonarqube
Command 'docker' not found, but can be installed with:
sudo snap install docker      # version 28.1.1+1, or
sudo apt install docker.io    # version 27.5.1~ubuntu3-22.04.2
sudo apt install podman-docker # version 3.4.4+ds1~ubuntu1.22.04.3
See 'snap info docker' for additional versions.
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo snap install docker
[sudo] password for apsit:
docker 28.1.1+1 from Canonical** installed
WARNING: There is 1 new warning. See 'snap warnings'.
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ ^C
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo apt-get install docker
```

1) Install and configure a Jenkins and SonarQube CICD environment using Docker containers.

Installation of Jenkins

The version of Jenkins included with the default Ubuntu packages is often behind the latest available version from the project itself. To take advantage of the latest fixes and features, you can use the project-maintained packages to install Jenkins.

```
manjusha@apsit:~$ wget -q -O -  
https://pkg.jenkins.io/debian-stable/jenkins.io.key | sudo apt-key add -
```

When the key is added, the system will return OK. Next, append the Debian package repository address to the server's sources.list:

```
manjusha@apsit:~$ sudo sh -c 'echo deb http://pkg.jenkins.io/debian-stable
```



The screenshot shows a web browser window with the URL `localhost:8080/login?from=%2F`. The title bar says "Getting Started". The main content is titled "Unlock Jenkins". It instructs the user to ensure Jenkins is securely set up by an administrator, who has written a password to the log ([not sure where to find it?](#)) and this file on the server: `/var/lib/jenkins/secrets/initialAdminPassword`. It asks the user to copy the password from either location and paste it into a text input field labeled "Administrator password". A "Continue" button is at the bottom right.

The screenshot shows a web browser window with the URL `localhost:8080`. The title bar says "Getting Started". The main content is titled "Getting Started". It displays a table of Jenkins plugins and their status:

✓ Folders	✓ OWASP Markup Formatter	✓ Build Timeout	✓ Credentials Binding	✗ commons-lang3 %3.x Jenkins API
✗ Timestamper	✗ Workspace Cleanup	✗ Ant	✗ Gradle	✗ Icons API
✗ Pipeline	✗ GitHub Branch Source	✗ Pipeline: GitHub Groovy Libraries	✗ Pipeline Graph View	✗ Jenkins Markup Formatter
✗ Git	✗ SSH Build Agents	✗ Matrix Authorization Strategy	✗ LDAP	✗ ASN API
✗ Email Extension	✗ Mailer	✗ Dark Theme		✗ JSON Path API

On the right side of the table, there is a detailed list of Jenkins API endpoints:

- common-lang3 %3.x Jenkins API
- Icons API
- Jenkins Markup Formatter
- ASN API
- JSON Path API
- Structs
- Pipeline: Step API
- Commons-Text API
- Tolken API
- Build Timeout
- Boomerang API
- Credentials

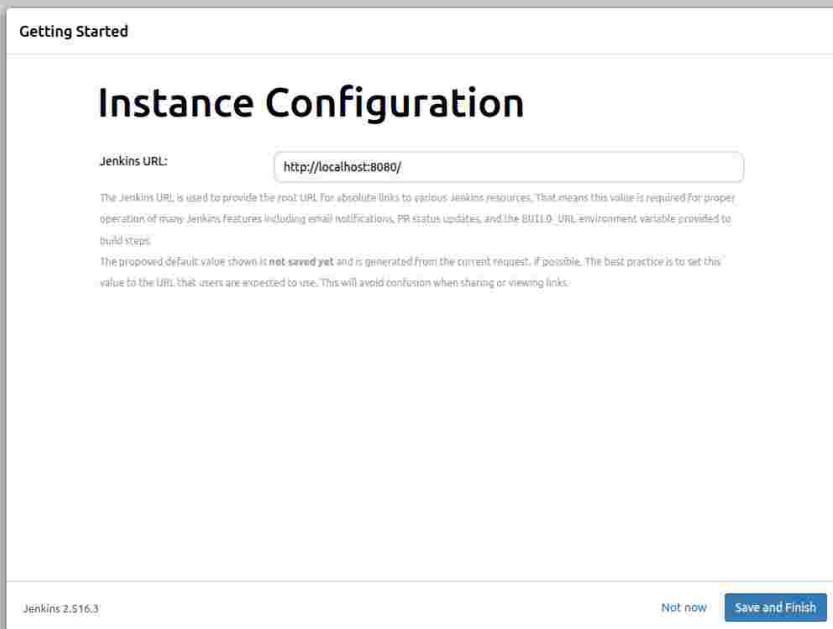
At the bottom left, it says "Jenkins 2.516.3".



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



When the installation is complete, you will be prompted to set up the first administrative user. It's possible to skip this step and continue as admin using the initial password we used above, but we'll take a moment to create the user.



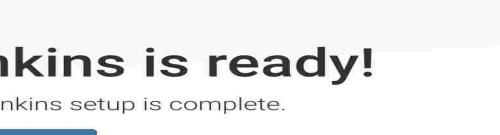
Jenkins URL:

The Jenkins URL is used to provide the root URL for absolute links to various Jenkins resources. That means this value is required for proper operation of many Jenkins features including email notifications, PR status updates, and the BUILD_URL environment variable provided to build steps.
The proposed default value shown is **not saved yet** and is generated from the current request, if possible. The best practice is to set this value to the URL that users are expected to use. This will avoid confusion when sharing or viewing links.

Jenkins 2.516.3 Not now Save and Finish

After confirming the appropriate information, click Save and Finish. You will see a confirmation page confirming that "Jenkins is Ready!"

Click Start using Jenkins to visit the main Jenkins dashboard:



Getting Started

Jenkins is ready!

Your Jenkins setup is complete.

[Start using Jenkins](#)



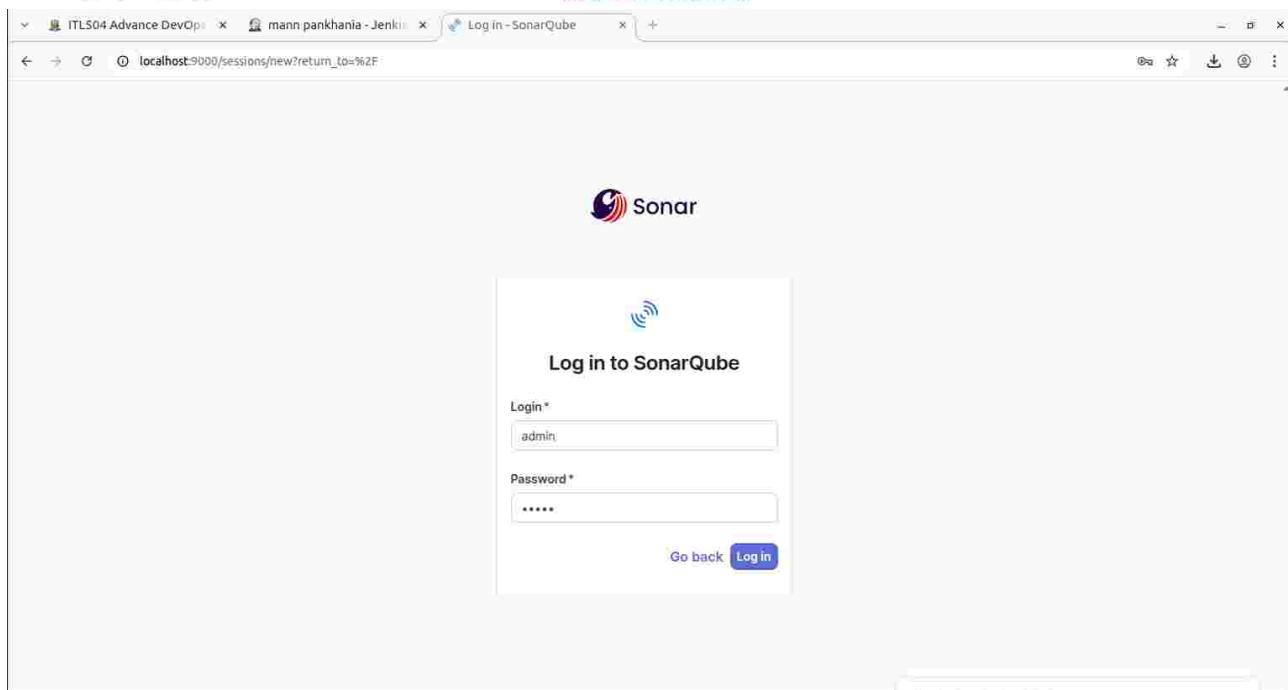
SonarQube Setup

Before proceeding with the integration, we will setup SonarQube Instance. we are using SonarQube Docker Container.

```
manjusha@apsit:~$ docker run -d -p 9000:9000 sonarqube
```

```
Processing triggers for libc-bin (0.1ubuntu0.21) ...
root@ubuntu:/home/manasi# docker run -d -p 9000:9000 sonarqube
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
9621f1afde84: Pull complete
1220b1fb64e6: Pull complete
f0a3b7127ede: Pull complete
Digest: sha256:9ca40ae23bb2228a6c4cc8c20de41fcd72a8ed7358331b4bd5910cd20dcee995
Status: Downloaded newer image for sonarqube:latest
ed54d42e5aa9a31f212c204e48e47b80e63478abbf7960ce65c6c56a99a35e24
root@ubuntu:/home/manasi#
```

In the above command, we are forwarding port 9000 of the container to the port 9000 of the host machine as SonarQube is will run on port 9000. Then, from the browser, enter <http://localhost:9000>. After That, you will see the SonarQube is running. Then, login using default credentials (admin:admin).



Generate User Token

Now, we need to get the SonarQube user token to make connection between Jenkins and SonarQube. For the same, go to **Administration > User > My Account > Security** and then, from the bottom of the page you can create new tokens by clicking the Generate Button. Copy the Token and keep it safe.

C96798e9bd081e117189b516c868ddb7d87ee785 SonarQube



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



localhost:9000/account/security

Embedded database should be used for evaluation purposes only. It doesn't support scaling, upgrading to a new SonarQube Server version, or migration to another database engine. [Learn more](#).

SonarQube community Projects Issues Rules Quality Profiles Quality Gates Administration More

A Administrator

Profile Security Notifications Projects

or the user login. This will increase the security of your installation by not letting your analysis user's password going through your network.

Generate Tokens

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

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

sqa_cd59e2f0502dd4390bc2b05e7d98031d6bf0c514

Name	Type	Project	Last use	Created	Expiration
sonarqube	Global		Never	September 18, 2025	October 18, 2025

Enter a new password

Old Password *



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



localhost:8080/manage/pluginManager/available

Jenkins / Manage Jenkins / Plugins

Plugins

Updates Available plugins Installed plugins Advanced settings Download progress

Search: sonar

Install

Install	Name	Released	Health
<input checked="" type="checkbox"/>	SonarQube Scanner 2.18	7 mo 22 days ago	84
<input type="checkbox"/>	Sonar Quality Gates 3.52.vdcab_d7994fb_6	6 mo 27 days ago	100
<input type="checkbox"/>	Quality Gates 2.5	9 yr 4 mo ago	42
<input type="checkbox"/>	Sonargraph Integration 5.0.2	2 yr 3 mo ago	88
<input type="checkbox"/>	CodeSonar 3.6.0		

localhost:8080/manage/pluginManager/updates/

Jenkins / Manage Jenkins / Plugins

Plugins

Updates Available plugins Installed plugins Advanced settings Download progress

Download progress

Preparation

- Checking internet connectivity
- Checking update center connectivity
- Success

commons-lang3 v3.x Jenkins API	Success
Ionicons API	Success
Folders	Success
OWASP Markup Formatter	Success
ASM API	Success
JSON Path API	Success
Structs	Success
Pipeline: Step API	Success
commons-text API	Success
Token Macro	Success
Build Timeout	Success
bouncycastle API	Success
Credentials	Success
Plain Credentials	Success
Variant	Success
SSH Credentials	Success
Credentials Binding	Success
SCM API	Success
Pipeline: API	Success
Timestamper	Success



The screenshot shows the Jenkins Global credentials (unrestricted) page. The URL is localhost:8080/manage/credentials/store/system/domain/_/. The page displays a single credential entry:

ID	Name	Kind	Description
19d0431c-f106-486a-95fb-426e3b2344f2	19d0431c-f106-486a-95fb-426e3b2344f2	Username with password	

Icon: S M L

REST API Jenkins 2.516.3

2) Configure Jenkins with the SonarQube Scanner plugin for automated static code analysis.

Jenkins Setup for SonarQube

Before all, we need to install the SonarQube Scanner plugin in Jenkins. For the same, go to **Manage Jenkins > Plugin Manager > Available**. From here, type SonarQube Scanner then select and install.



Tool Configuration SonarQube Scanner

Now, we need to configure the Jenkins plugin for SonarQube Scanner to make a connection with the SonarQube Instance. For that, got to **Manage Jenkins > Configure System > SonarQube Server**. Then, Add SonarQube. In this, give the Installation Name, Server URL then Add the Authentication token in the Jenkins Credential Manager and select the same in the configuration.

The screenshot shows the Jenkins 'SonarQube servers' configuration page. It includes sections for 'Environment variables', 'SonarQube installations' (with fields for 'Name' set to 'SonarQube' and 'Server URL' set to 'http://localhost:9000'), and 'Server authentication token' (with a dropdown set to 'sonarqube' and a 'Add' button). A note at the bottom states: 'SonarQube authentication token. Mandatory when anonymous access is disabled.'

Then, we need to set-up the SonarQube Scanner to scan the source code in the various stage. For the same, go to **Manage Jenkins > Global Tool Configuration > SonarQube Scanner**. Then, Click **Add SonarQube Scanner Button**. From there, give some name of the scanner type and **Add Installer** of your choice. In this case, I have selected SonarQube Scanner from Maven Central.



SonarQube Scanner

SonarQube Scanner installations

Add SonarQube Scanner

SonarQube Scanner

Name

SonarQube

Install automatically

Install from Maven Central

Version

SonarQube Scanner 4.6.2.2472 ▾

Add Installer ▾

SonarQube Scanner in Jenkins Pipeline

Now, It's time to integrate the SonarQube Scanner in the Jenkins Pipeline. For the same, we are going to add one more stage in the Jenkinsfile called SonarQube and inside that, I am adding the following settings and code.



Screenshot of Jenkins Pipeline configuration:

The pipeline script is defined as follows:

```
node {
    stage('cloning from GIT'){
        git branch: 'main',credentialsId: 'GIT_REPO', url: 'https://github.com/vishal003/jenkins-sonarqube.git'
    }
}
```

The "Use Groovy Sandbox" checkbox is checked.

Buttons at the bottom: Advanced, Save, Apply.

Enter an item name

General Build Triggers Advanced Project Options Pipeline

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/

Folder ?

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.



Github Configuration in Jenkins Pipeline

Pipeline

Definition

Pipeline script

Script

```
1 node
2 [
3   stage('clonning from GIT'){
4     git branch: 'main', credentialsId: 'GIT_REPO', url: 'https://github.com/vishal003/jenkins-sonarqube.git'
5   }
6 ]
7
```

Git Clonning into Jenkins

ITL504 Advance DevOps x sonarqube #1 Console - Security - My Account - +

localhost:8080/job/sonarqube/fastBuild/console

Jenkins sonarqube #1

Status Changes Console Output Edit Build Information Delete build #1 Timings Git Build Data Pipeline Overview Replay Pipeline Steps Workspaces

Console Output

Started by user manan_pankhania
(Pipeline) Start of Pipeline
(Pipeline) node
Running on Jenkins in /var/lib/jenkins/workspace/sonarqube
(Pipeline) {
(Pipeline) stage
(Pipeline) ['clonning from GIT'
(Pipeline) git
The recommended git tool is: NONE
Warning: CredentialId "GIT_REPO" could not be found.
Cloning the remote Git repository
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 2.34.1'
> git fetch --tags --force --progress -- https://github.com/vishal003/jenkins-sonarqube.git +refs/heads/*:refs/remotes/origin/* # timeout=10
> 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 80c34f481be25f7733e50784c2f763909884ed90 (refs/remotes/origin/main)
> git config core.sparsecheckout # timeout=10
> git checkout -f 80c34f481be25f7733e50784c2f763909884ed90 # timeout=10
> git branch -a -v --no-abbrev # timeout=10
> git checkout -b main 80c34f481be25f7733e50784c2f763909884ed90 # timeout=10
Commit message: "Update README.md"
First time build. Skipping changelog.
(Pipeline) }
(Pipeline) // stage
(Pipeline) }
(Pipeline) // node
(Pipeline) End of Pipeline

Finished: SUCCESS

Successfully Build Github Repository in Jenkins



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Conclusion: In This Experiment We Have Learnt About Static Analysis SAST process and learn to integrate Jenkins SAST to SonarQube/GitLab.



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-C

Subject: Advanced Devops Lab (ADL)

Name of Instructor: Prof. Vishal Badgujar

Name of Student: Huzaifa Bubere

Student ID: 24204006

EXPERIMENT NO. 08

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

Steps:

- 1) Install and configure a Jenkins and SonarQube CICD environment using Docker containers.
- 2) Configure Jenkins with the SonarQube Scanner plugin for automated static code analysis.

```
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ wget -q -O - https://pkg.jenkins.io/debian-stable/jenkins.io.key | sudo apt-key add -
[sudo] password for apsit:
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo sh -c 'echo deb http://pkg.jenkins.io/debian-stable binary/ > /etc/apt/sources.list.d/jenkins.list'
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo apt update-
E: Invalid operation update-
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo apt update
Ign:1 https://pkg.jenkins.io/debian-stable binary/ InRelease
Get:2 https://pkg.jenkins.io/debian-stable binary/ Release [2,044 B]
Get:3 https://pkg.jenkins.io/debian-stable binary/ Release.gpg [833 B]
Get:4 https://dl.google.com/linux/chrome/deb stable InRelease [1,825 B]
Get:5 https://pkg.jenkins.io/debian-stable binary/ Packages [29.7 kB]
Get:6 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,214 B]
Get:7 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:8 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:9 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [54.6 kB]
Get:11 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
```



```
Preparing to unpack .../jenkins_2.516.3_all.deb ...
Unpacking jenkins (2.516.3) over (2.516.2) ...
Setting up jenkins (2.516.3) ...
apt@aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo systemctl start jenkins
apt@aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo systemctl status jenkins
● jenkins.service - Jenkins Continuous Integration Server
   Loaded: loaded (/lib/systemd/system/jenkins.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2025-09-18 10:52:06 IST; 38s ago
     Main PID: 5883 (java)
        Tasks: 72 (limit: 9050)
       Memory: 936.2M
          CPU: 21.796s
         CGroup: /system.slice/jenkins.service
             └─5883 /usr/bin/java -Djava.awt.headless=true -jar /usr/share/java/jenklns.war --webroot=/var/cache/jenkins/war --httpPort=8080

Sep 18 10:52:00 aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: [LF]> This may also be found at: /var/lib/jenkins/secrets/initialAdminPassword
Sep 18 10:52:00 aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: [LF]>
Sep 18 10:52:00 aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: [LF]> ****
Sep 18 10:52:00 aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: 2025-09-18 05:22:06.041+0000 [id=57]      INFO    jenkins.InitReactorRunner$1#onAttaines
Sep 18 10:52:00 aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: 2025-09-18 05:22:06.053+0000 [id=33]      INFO    hudson.lifecycle.Lifecycle$OnReady: J
Sep 18 10:52:00 aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: Started Jenkins Continuous Integration Server.
Sep 18 10:52:07 aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: 2025-09-18 05:22:07.972+0000 [id=98]      INFO    h.m.DownloadService$Downloadable#load>
Sep 18 10:52:07 aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC jenkins[5883]: 2025-09-18 05:22:07.973+0000 [id=98]      INFO    hudson.util.Retrier#start: Performed >
apt@aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo ufw allow 8080
Rules updated
Rules updated (v6)
apt@aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ [[2020-sudo cat /var/lib/jenkins/secrets/initialAdminPassword
sudo: command not found
apt@aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo cat /var/lib/jenkins/secrets/initialAdminPassword
90ac0665b1344dc5b878cd461b39f50a
apt@aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ mc
apt@aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ docker run -d -p 9080:9000 sonarqube
command 'docker' not found, but can be installed with:
sudo snap install docker      # version 28.1.1+1, or
sudo apt install docker.io    # version 27.5.1~ubuntu32-22.04.2
sudo apt install podman-docker # version 3.4.4+ds1~ubuntu11.22.04.3
See 'snap info docker' for additional versions.
apt@aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo snap install docker
[sudo] password for aptis:
docker 28.1.1+1 from Canonical** installed
WARNING: There is a new warning. See 'snap warnings'.
apt@aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ mc
apt@aptis-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: $ sudo apt-get install docker
```

1) Install and configure a Jenkins and SonarQube CICD environment using Docker containers.

Installation of Jenkins

The version of Jenkins included with the default Ubuntu packages is often behind the latest available version from the project itself. To take advantage of the latest fixes and features, you can use the project-maintained packages to install Jenkins.

```
manjusha@apsit:~$ wget -q -O -  
https://pkg.jenkins.io/debian-stable/jenkins.io.key | sudo apt-key add -
```

When the key is added, the system will return OK. Next, append the Debian package repository address to the server's sources.list:

```
manjusha@apsit:~$ sudo sh -c 'echo deb http://pkg.jenkins.io/debian-stable
```

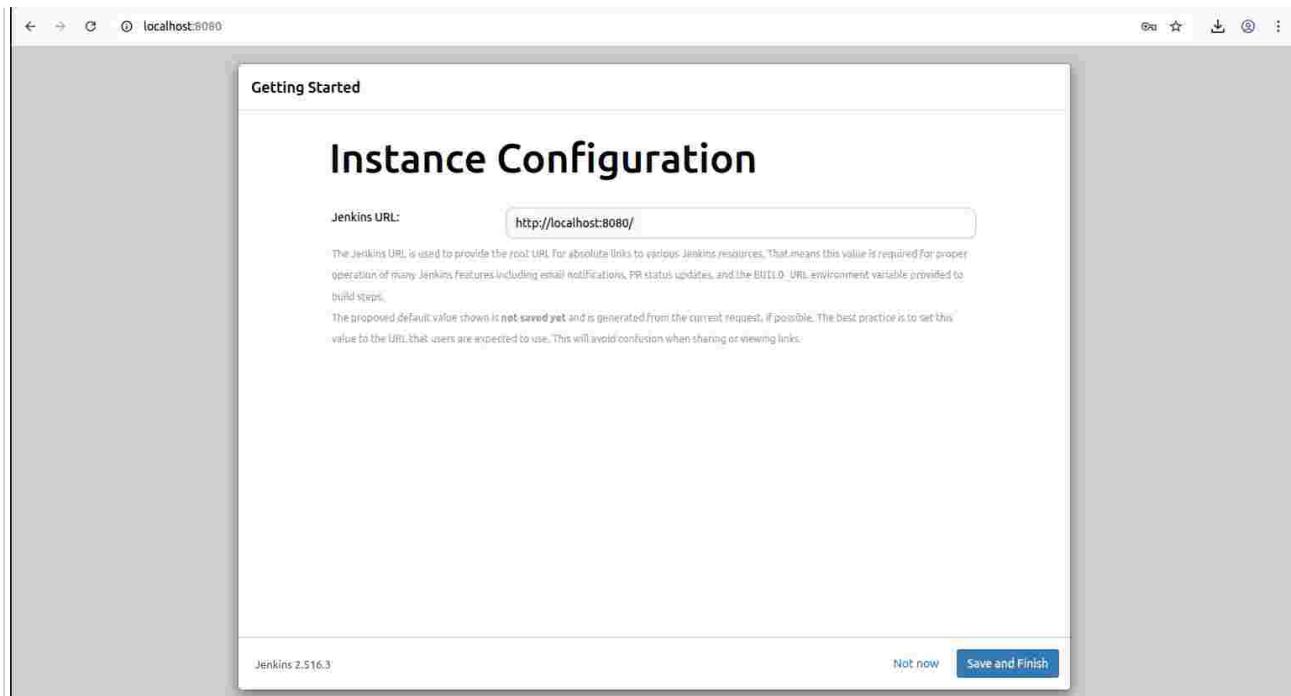


The screenshot shows a web browser window for Jenkins at localhost:8080/login?from=%2F. The title bar says "Getting Started". The main content is titled "Unlock Jenkins". It instructs the user that a password has been written to the log and this file on the server, located at /var/lib/jenkins/secrets/initialAdminPassword. It asks the user to copy the password from either location and paste it into a text input field labeled "Administrator password". A "Continue" button is at the bottom right.

The screenshot shows a web browser window for Jenkins at localhost:8080. The title bar says "Getting Started". The main content is titled "Getting Started". It displays a grid of Jenkins plugins with checkboxes. The visible rows include Folders, OWASP Markup Formatter, Build Timeout, Credentials Binding, commons-lang3 %3.x Jenkins API, Icons API, Folders, Pipeline, GitHub Branch Source, Ant, Gradle, Pipeline: GitHub Groovy Libraries, Pipeline Graph View, Pipeline: Step API, Pipeline: Text API, Pipeline: Token Macro API, Pipeline: Timeout API, Pipeline: buildscript API, Pipeline: Credentials, Git, SSH Build Agents, Matrix Authorization Strategy, LDAP, and Dark Theme. A tooltip for the "Folders" plugin indicates it is a required dependency. At the bottom, it says "Jenkins 2.516.3".



When the installation is complete, you will be prompted to set up the first administrative user. It's possible to skip this step and continue as admin using the initial password we used above, but we'll take a moment to create the user.



Getting Started

Instance Configuration

Jenkins URL:

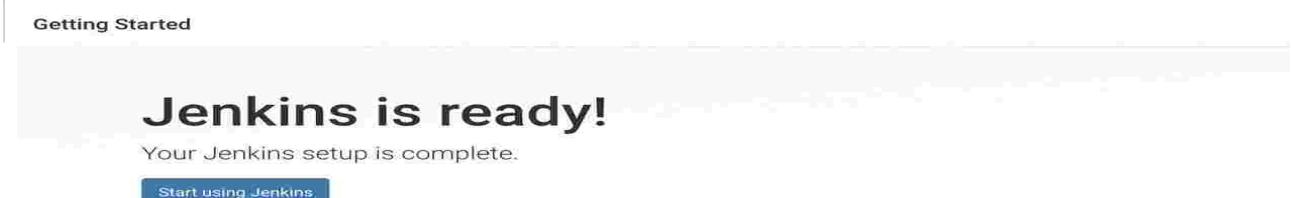
The Jenkins URL is used to provide the root URL for absolute links to various Jenkins resources. That means this value is required for proper operation of many Jenkins features including email notifications, PR status updates, and the BUILD_URL environment variable provided to build steps.

The proposed default value shown is **not saved yet** and is generated from the current request, if possible. The best practice is to set this value to the URL that users are expected to use. This will avoid confusion when sharing or viewing links.

Jenkins 2.516.3 Not now Save and Finish

After confirming the appropriate information, click Save and Finish. You will see a confirmation page confirming that “Jenkins is Ready!”:

Click Start using Jenkins to visit the main Jenkins dashboard:



Getting Started

Jenkins is ready!

Your Jenkins setup is complete.

[Start using Jenkins](#)



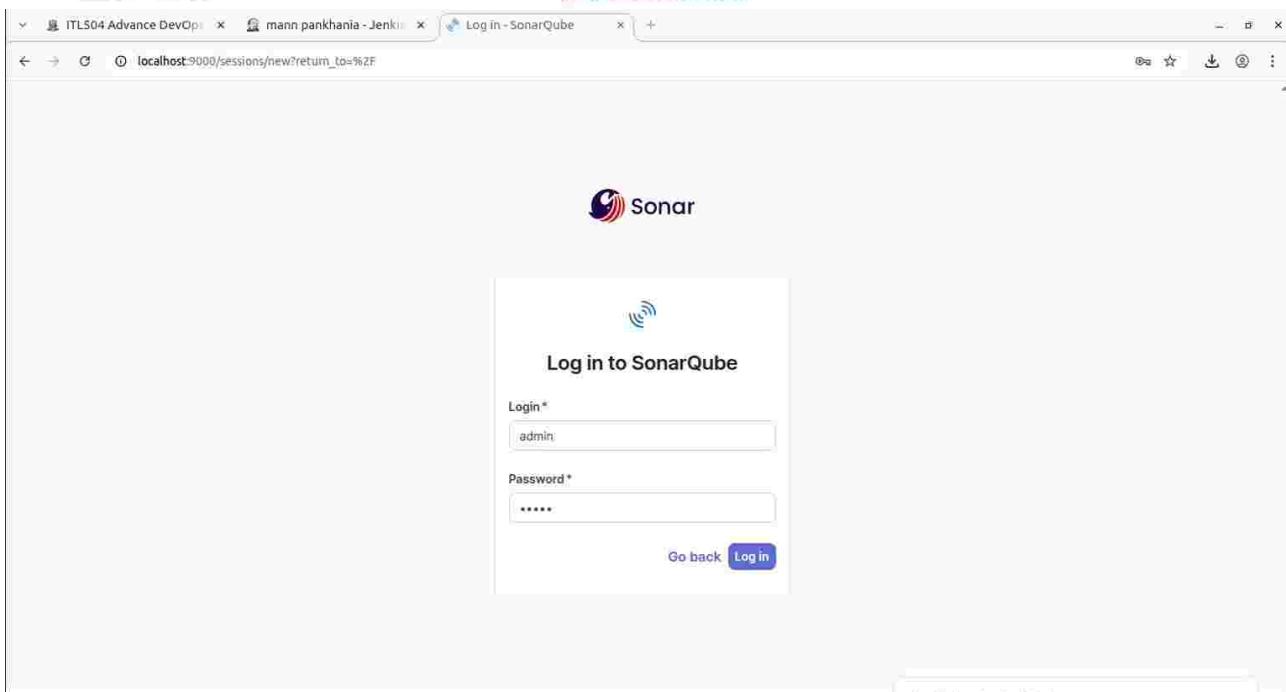
SonarQube Setup

Before proceeding with the integration, we will setup SonarQube Instance. we are using SonarQube Docker Container.

```
manjusha@apsit:~$docker run -d -p 9000:9000 sonarqube
```

```
Processing triggers for libc-bin (0.100.0-21) ...
root@ubuntu:/home/manasi# docker run -d -p 9000:9000 sonarqube
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
9621f1afde84: Pull complete
1220b1fb64e6: Pull complete
f0a3b7127ede: Pull complete
Digest: sha256:9ca40ae23bb2228a6c4cc8c20de41fc72a8ed7358331b4bd5910cd20dcee995
Status: Downloaded newer image for sonarqube:latest
ed54d42e5aa9a31f212c204e48e47b80e63478abb7960ce65c6c56a99a35e24
root@ubuntu:/home/manasi#
```

In the above command, we are forwarding port 9000 of the container to the port 9000 of the host machine as SonarQube is will run on port 9000. Then, from the browser, enter <http://localhost:9000>. After That, you will see the SonarQube is running. Then, login using default credentials (admin:admin).



Generate User Token

Now, we need to get the SonarQube user token to make connection between Jenkins and SonarQube. For the same, go to **Administration > User > My Account > Security** and then, from the bottom of the page you can create new tokens by clicking the Generate Button. Copy the Token and keep it safe.

C96798e9bd081e117189b516c868ddb7d87ee785 SonarQube



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



localhost:9000/account/security

Embedded database should be used for evaluation purposes only. It doesn't support scaling, upgrading to a new SonarQube Server version, or migration to another database engine. [Learn more](#).

SonarQube community Projects Issues Rules Quality Profiles Quality Gates Administration More

A Administrator

Profile Security Notifications Projects

of the user login. This will increase the security of your installation by not letting your analysis user's password going through your network.

Generate Tokens

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

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

sqa_cd59e2f0502dd4390bc2b05e7d98031d6bf0c514 [Copy](#)

Name	Type	Project	Last use	Created	Expiration
sonarqube	Global		Never	September 18, 2025	October 18, 2025

Enter a new password

Old Password *

Revoke



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



localhost:8080/manage/pluginManager/available

Jenkins / Manage Jenkins / Plugins

Plugins

Updates Available plugins Installed plugins Advanced settings Download progress

Search: sonar

Install

Install	Name	Released	Health
<input checked="" type="checkbox"/>	SonarQube Scanner 2.18	7 mo 22 days ago	84
<input type="checkbox"/>	Sonar Quality Gates 3.52.vdcab_d7994fb_6	6 mo 27 days ago	100
<input type="checkbox"/>	Quality Gates 2.5	9 yr 4 mo ago	42
<input type="checkbox"/>	Sonargraph Integration 5.0.2	2 yr 3 mo ago	88
<input type="checkbox"/>	CodeSonar 3.6.0		

localhost:8080/manage/pluginManager/updates/

Jenkins / Manage Jenkins / Plugins

Plugins

Updates Available plugins Installed plugins Advanced settings Download progress

Download progress

Preparation

- Checking internet connectivity
- Checking update center connectivity
- Success

commons-lang3 v3.x Jenkins API	Success
Ionicons API	Success
Folders	Success
OWASP Markup Formatter	Success
ASM API	Success
JSON Path API	Success
Structs	Success
Pipeline: Step API	Success
commons-text API	Success
Token Macro	Success
Build Timeout	Success
bouncycastle API	Success
Credentials	Success
Plain Credentials	Success
Variant	Success
SSH Credentials	Success
Credentials Binding	Success
SCM API	Success
Pipeline: API	Success
Timestamper	Success



The screenshot shows the Jenkins Global credentials (unrestricted) page. At the top, there are navigation links for Jenkins, Manage Jenkins, Credentials, System, and Global credentials (unrestricted). A search bar and other global navigation icons are also present. The main content area is titled "Global credentials (unrestricted)" and contains a table with one row of data. The table columns are ID, Name, Kind, and Description. The single row shows an ID of "19d0431c-f106-486a-95fb-426e3b2344f2", a Name of "19d0431c-f106-486a-95fb-426e3b2344f2", a Kind of "Username with password", and a Description of "Username with password". There is a blue "Add Credentials" button at the top right of the table. Below the table, there is a "Icon:" section with "S", "M", and "L" options. At the bottom right of the page, there are links for "REST API" and "Jenkins 2.516.3".

ID	Name	Kind	Description
19d0431c-f106-486a-95fb-426e3b2344f2	19d0431c-f106-486a-95fb-426e3b2344f2	Username with password	Username with password

2) Configure Jenkins with the SonarQube Scanner plugin for automated static code analysis.

Jenkins Setup for SonarQube

Before all, we need to install the SonarQube Scanner plugin in Jenkins. For the same, go to **Manage Jenkins > Plugin Manager > Available**. From here, type SonarQube Scanner then select and install.



Tool Configuration SonarQube Scanner

Now, we need to configure the Jenkins plugin for SonarQube Scanner to make a connection with the SonarQube Instance. For that, got to **Manage Jenkins > Configure System > SonarQube Server**. Then, Add SonarQube. In this, give the Installation Name, Server URL then Add the Authentication token in the Jenkins Credential Manager and select the same in the configuration.

The screenshot shows the Jenkins 'SonarQube servers' configuration page. It includes sections for 'Environment variables', 'SonarQube installations' (with fields for 'Name' set to 'SonarQube' and 'Server URL' set to 'http://localhost:9000'), and 'Server authentication token' (with a dropdown set to 'sonarqube' and a 'Add' button). A note at the bottom states: 'SonarQube authentication token. Mandatory when anonymous access is disabled.'

Then, we need to set-up the SonarQube Scanner to scan the source code in the various stage. For the same, go to **Manage Jenkins > Global Tool Configuration > SonarQube Scanner**. Then, Click **Add SonarQube Scanner Button**. From there, give some name of the scanner type and **Add Installer** of your choice. In this case, I have selected SonarQube Scanner from Maven Central.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



SonarQube Scanner

SonarQube Scanner installations

Add SonarQube Scanner

SonarQube Scanner

Name

SonarQube

Install automatically

Install from Maven Central

Version

SonarQube Scanner 4.6.2.2472 ▾

Add Installer ▾

SonarQube Scanner in Jenkins Pipeline

Now, It's time to integrate the SonarQube Scanner in the Jenkins Pipeline. For the same, we are going to add one more stage in the Jenkinsfile called SonarQube and inside that, I am adding the following settings and code.



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



The screenshot shows the Jenkins Pipeline configuration page. The pipeline script is defined as follows:

```
node {
    stage('cloning from GIT'){
        git branch: 'main',credentialsId: 'GIT_REPO', url: 'https://github.com/vishal003/jenkins-sonarqube.git'
    }
}
```

Below the script, there is a checkbox labeled "Use Groovy Sandbox" which is checked. At the bottom of the pipeline section, there are "Save" and "Apply" buttons.

The screenshot shows the Jenkins Pipeline job configuration page for a GitHub project. The job is named "Hello Pipeline job". The "General" tab is selected. The "Description" field contains the text "Hello Pipeline job". Under the "GitHub project" section, the "Project url" is set to "https://github.com/vishal003/jenkins-sonarqube/". There are several checkboxes at the bottom left: "Discard old builds", "Do not allow concurrent builds", "Do not allow the pipeline to resume if the controller restarts", and "GitHub project", which is checked. The "OK" button is visible at the bottom right.

IT



Github Configuration in Jenkins Pipeline

Pipeline

Definition

Pipeline script

Script

```
1 node
2 [
3   stage('cloning from GIT'){
4     git branch: 'main', credentialsId: 'GIT_REPO', url: 'https://github.com/vishal083/jenkins-sonarqube.git'
5   }
6 ]
7
```

Git Clonning into Jenkins

ITL504 Advance DevOps x sonarqube #1 Console - Security - My Account - +

localhost:8080/job/sonarqube/lastBuild/console

Jenkins sonarqube #1

Status Changes Console Output Edit Build Information Delete build #1 Timings Git Build Data Pipeline Overview Reply Pipeline Steps Workspaces

Console Output

Started by user name penkharia
(Pipeline) Start of Pipeline
(Pipeline) node
Running on Jenkins in /var/lib/jenkins/workspace/sonarqube
(Pipeline) {
(Pipeline) stage
(Pipeline) [cloning from GIT]
(Pipeline) git
The recommended git tool is: NONE
Warning: CredentialId "GIT_REPO" could not be found.
Cloning the remote Git repository
Cloning repository https://github.com/vishal083/jenkins-sonarqube.git
> git init /var/lib/jenkins/workspace/sonarqube # timeout=10
Fetching upstream changes from https://github.com/vishal083/jenkins-sonarqube.git
> git --version # timeout=10
> git -version # git version 2.34.1'
> git fetch --tags --force --progress -- https://github.com/vishal083/jenkins-sonarqube.git +refs/heads/*:refs/remotes/origin/* # timeout=10
> git config remote.origin.url https://github.com/vishal083/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 88c34f481be25f7733e50784c2f763909884ed90 (refs/remotes/origin/main)
> git config core.sparsecheckout # timeout=10
> git checkout -f 88c34f481be25f7733e50784c2f763909884ed90 # timeout=10
> git branch -a -v --no-abbrev # timeout=10
> git checkout -b main 88c34f481be25f7733e50784c2f763909884ed90 # timeout=10
Commit message: "Update README.md"
First time build. Skipping changelog.
(Pipeline) }
(Pipeline) // stage
(Pipeline) }
(Pipeline) // node
(Pipeline) End of Pipeline

Finished: SUCCESS

Successfully Build Github Repository in Jenkins



Conclusion:

In this experiment, we learnt and understood how to create a Jenkins CICD Pipeline with SonarQube / GitLab Integration to perform a static analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web / Java / Python application.



PARSHVANATH CHARITABLE TRUST

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

[NBA Accredited]



Academic Year: 2022-23 Semester: V Class / Branch: TE IT

Subject: Advanced Devops Lab (ADL)

Subject Lab Incharge: Prof. Manjusha K.

Name: Huzaifa Bubere

Student Id: 24204006

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.

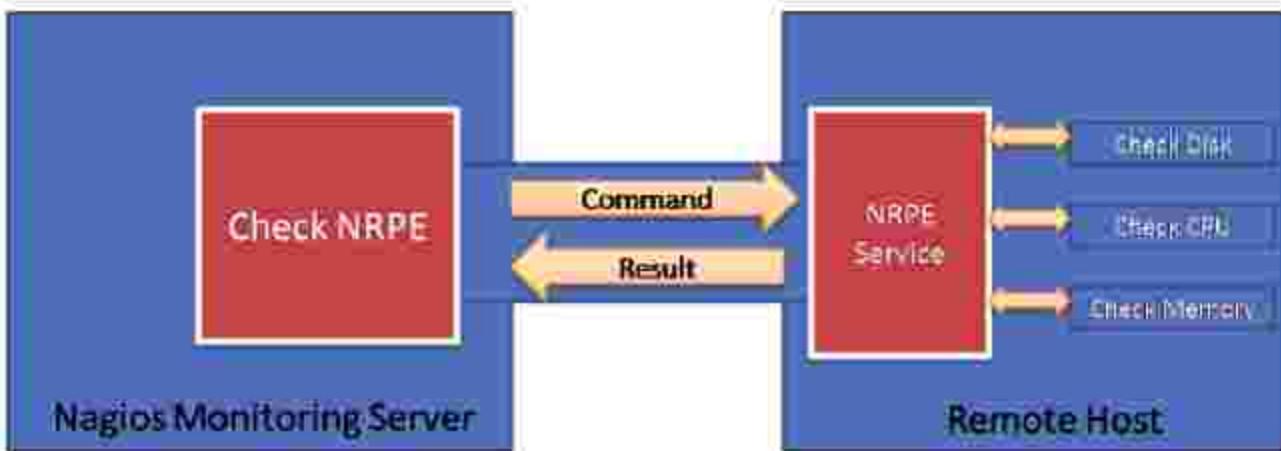
Theory:

Continuous monitoring is a process to detect, report, respond all the attacks which occur in its infrastructure. Once the application is deployed into the server, the role of continuous monitoring comes in to play. The entire process is all about taking care of the company's infrastructure and respond appropriately.

Why We Need Nagios tool?

Here, are the important reasons to use Nagios monitoring tool:

- Detects all types of network or server issues
 - Helps you to find the root cause of the problem which allows you to get the permanent solution to the problem
 - Active monitoring of your entire infrastructure and business processes
 - Allows you to monitors and troubleshoot server performance issues
 - Helps you to plan for infrastructure upgrades before outdated systems create failures
 - You can maintain the security and availability of the service
 - Automatically fix problems in a panic situation
- Nagios is the most popular, open source, powerful monitoring system for any kind of infrastructure. It enables organizations to identify and resolve IT infrastructure problems before they affect critical business processes. Nagios has the capability of monitoring application, services, entire IT infrastructure.
- NRPE is known as Nagios Remote Plugin Executor. The NRPE add-on is designed to execute plugins on remote Nix systems. In this setup, NRPE daemon is installed on the remote system to which services need to monitor through Nagios server.
- NRPE runs as a daemon on remote systems and waits for Nagios requests. When Nagios server needs to check the status of any resources or applications to that remote host, sends and commands signal, which command definition is stored on NRPE service. NRPE takes Nagios server request and execute the command on the local system and sends the result back to Nagios.



1. Pre-requisites:

First requirement is to install Apache and PHP first. Use the following commands to complete it. And use commands to install required packages for Nagios.

```
nagios@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo apt-get install wget build-essential unzip openssl libssl-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
build-essential is already the newest version (1:2.8ubuntu1.1).
wget is already the newest version (1:2.0.3-1ubuntu2.1).
The following packages were automatically installed and are no longer required:
  libgcc1:i386 libhttp-parser2.7.1 libssl1.0.0
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libc-bin libc-dev-bin libc6 libc6:i386 libc6-dbg libc6-dev libc6-i386 libcrypt-dev libcrypti libcrypti:i386 libfido2-1 libgssapi-krb5-2 libicu66
  libkrypto3 libkrb5-3 libkrb5support0 libnhttp2-14 libnode-dev libnode64 libssl1.1 libuv libuv-dev locales manpages-dev node-gyp node-semver nodejs
  openssh-client openssh-server openssh-sftp-server
Suggested packages:
  glibc-doc glibc-doc:i386 locales:i386 krb5-user libssl-doc keychain libpam-ssh monkeysphere ssh-askpass molly-guard
Recommended packages:
  libidn2-0 libidn2-0:i386
The following packages will be REMOVED:
  libssl1.0-dev nodejs-dev
The following NEW packages will be installed:
  libcbor0.6 libcrypt-dev libcrypti libcrypti:i386 libfido2-1 libicu66 libnode-dev libnode64 libssl-dev
The following packages will be upgraded:
  libc-bin libc-dev-bin libc6 libc6:i386 libc6-dbg libc6-dev libc6-i386 libgssapi-krb5-2 libkrypto3 libkrb5-3 libkrb5support0 libnhttp2-14 libssl1.1 libuv
  libuv-dev locales manpages-dev node-gyp node-semver nodejs openssh-client openssh-server openssh-sftp-server openssl unzip
25 upgraded, 9 newly installed, 2 to remove and 1830 not upgraded.
Need to get 22.4 MB/58.4 MB of archives.
After this operation, 40.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main i386 libcrypti 1:4.4.10-1ubuntu4 [98.9 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libcbor0.6 amd64 0.6.0-0ubuntu1 [21.1 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libfido2-1 amd64 1.3.1-1ubuntu2 [47.9 kB]
```

2 – Create Nagios User

Create a new user account for Nagios in your system and assign a password

```
nagios@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo adduser venny
Adding user 'venny' ...
Adding new group 'venny' (1004) ...
Adding new user 'venny' (1003) with group 'venny' ...
Creating home directory '/home/venny' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for venny
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
nagios@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo groupadd vennycmd
nagios@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo usermod -a -G vennycmd venny
nagios@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo usermod -a -G vennycmd www-data
nagios@apsit-HP-280-Pro-G6-Microtower-PC:~$
```

Step 3 – Install Nagios Core Service

After installing required dependencies and adding user accounts and Nagios core installation. Download latest Nagios core service from the official site.

```
nagios@apsit-HP-280-Pro-G6-Mictrotower-PC:~$ cd /opt/
nagios@apsit-HP-280-Pro-G6-Mictrotower-PC:/opt$ sudo wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.3.tar.gz
--2025-09-24 11:04:54-- https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.3.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: 11302228 (11M) [application/x-gzip]
Saving to: 'nagios-4.4.3.tar.gz.1'

nagios-4.4.3.tar.gz.1          100%[=====] 10.78M 2.48MB/s   in 4.3s

2025-09-24 11:04:59 (2.48 MB/s) - 'nagios-4.4.3.tar.gz.1' saved [11302228/11302228]

nagios@apsit-HP-280-Pro-G6-Mictrotower-PC:/opt$ sudo tar xzf nagios-4.4.3.tar.gz
nagios@apsit-HP-280-Pro-G6-Mictrotower-PC:/opt$ cd nagios-4.4.3
nagios@apsit-HP-280-Pro-G6-Mictrotower-PC:/opt/nagios-4.4.3$ sudo ./configure --with-command-group=vennycmd
checking for a BSD-compatible install... /usr/bin/install -c
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
```

```
nagios@apsit-HP-280-Pro-G6-Mictrotower-PC:/opt/nagios-4.4.3$ sudo make all
cd ./base && make
make[1]: Entering directory '/opt/nagios-4.4.3/base'
make -C ./lib
make[2]: Entering directory '/opt/nagios-4.4.3/lib'
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c queue.c -o queue.o
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c kvvec.c -o kvvec.o
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c iocache.c -o iocache.o
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c lobroker.c -o lobroker.o
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c bitmap.c -o bitmap.o
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c dkhash.c -o dkhash.o
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c runcmd.c -o runcmd.o
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c nsutils.c -o nsutils.o
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c fanout.c -o fanout.o
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c pqueue.c -o pqueue.o
gcc -Wall -g -O2 -DHAVE_CONFIG_H -c worker.c -o worker.o
worker.c: In function 'enter_worker':
```

```
nagios@apsit-HP-280-Pro-G6-Mictrotower-PC:/opt/nagios-4.4.3$ sudo 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
nagios@apsit-HP-280-Pro-G6-Mictrotower-PC:/opt/nagios-4.4.3$ sudo 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
*** Init script installed ***
nagios@apsit-HP-280-Pro-G6-Mictrotower-PC:/opt/nagios-4.4.3$ sudo make install-config
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc/objects
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/nagios.cfg /usr/local/nagios/etc/nagios.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/cgi.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/timerperiods.cfg /usr/local/nagios/etc/objects/timerperiods.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/localhost.cfg /usr/local/nagios/etc/objects/localhost.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/windows.cfg /usr/local/nagios/etc/objects/windows.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/printer.cfg /usr/local/nagios/etc/objects/printer.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/switch.cfg /usr/local/nagios/etc/objects/switch.cfg
```

```
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ sudo make install-commandmode
/usr/bin/install -c -m 775 -o nagios -g vennycmd -d /usr/local/nagios/var/rw
chmod g+s /usr/local/nagios/var/rw

*** External command directory configured ***

nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ sudo make install-exfoliation

*** Exfoliation theme installed ***
NOTE: Use 'make install-classicui' to revert to classic Nagios theme
```

Now copy event handlers scripts under libexec directory. These binaries provides multiple events triggers for your Nagios web interface.

```
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ sudo cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ sudo chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers
chown: missing operand after 'nagios:nagios/usr/local/nagios/libexec/eventhandlers'
Try 'chown --help' for more information.
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ sudo chown -R venny:nagios /usr/local/nagios/libexec/eventhandlers
chown: missing operand after 'venny:nagios/usr/local/nagios/libexec/eventhandlers'
Try 'chown --help' for more information.
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ sudo chown -R venny:nagios /usr/local/nagios/libexec/eventhandlers
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ sudo chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$
```

Step 4 – Setup Apache with Authentication

Now create an Apache configuration file for your Nagios server as below:

Add below lines to nagios.conf file.

To setup apache authentication for user nagiosadmin

```
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ sudo a2enconf nagios
Conf nagios already enabled
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ sudo a2enmod cgi rewrite
Module cgi already enabled
Module rewrite already enabled
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ sudo service apache2 restart
Job for apache2.service failed because the control process exited with error code.
See "systemctl status apache2.service" and "journalctl -xe" for details.
```

Step 5 – Installing Nagios Plugins

After installing and configuring Nagios core service, Download latest nagios-plugins source and install using following commands.

```
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ sudo tar xzf nagios-plugins-2.2.1.tar.gz
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ cd nagios-plugins-2.2.1
-bash: cd: nagios-plugins-2.2.1: No such file or directory
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ ls
aclocal.m4      common    configure   doxy.conf   indent.sh    LICENSE     module      pkginfo    subst     THANKS     xdata
autoconf-macros config.guess  configure.ac  functions   INSTALLING  Makefile   nagios-plugins-2.2.1  pkgInfo.in  subst.in  t-tap
base           config.log   contrib       html        install-sh  Makefile.in  nagios-plugins-2.2.1.tar.gz README.md  t          update-version
cgt            config.status  CONTRIBUTING.MD include    LEGAL      make-tarball  nagios.spec  sample-config  tap      UPGRADING
changelog      config.sub   docs         indent-all.sh lib        mpackage    nagios.sysconfig  startup   test      worker
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ cd nagios-plugins-2.2.1
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3$ ./configure --with-nagios-user=nagios --with-nagios-group=nagios
configure: WARNING: unrecognized options: --with-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... /bin/mkdir -p
checking for gawk... no
checking for mawk
checking whether make sets $(MAKE)... yes
checking whether to disable maintainer-specific portions of Makefiles... yes
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking for gcc... gcc
checking for C compiler default output file name... a.out
```

Step 6 – Verify Settings

Use the Nagios commands to verify the Nagios installation and configuration file. After successfully verify start the Nagios core service.

```
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
Nagios Core 4.4.3
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2019-01-15
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
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo service nagios start
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ █
```

Step 7 – Access Nagios Web Interface

Access your nagios setup by access nagios server using hostname or ip address followed by /nagios. http://127.0.0.1/nagios/

Prompting for Apache Authentication Password –

username: nagiosadmin

Password : 123456 (which you enter while configuration)

Nagios After login screen –

The screenshot shows the Nagios Core 4.4.3 web interface. At the top right, there is a browser header with the URL "127.0.0.1/nagios/" and a "Verify that it's you" button. The main title "Nagios® Core™" is displayed with a gear icon. Below the title, a green checkmark indicates "Daemon running with PID 1559".

The left sidebar contains several navigation sections:

- General**: Home, Documentation.
- Current Status**: Tactical Overview, Map (Legacy), Hosts, Services, Host Groups, Summary, Grid, Service Groups, Summary, Grid.
- Problems**: Services (Unhandled), Hosts (Unhandled), Network Outages.
- Reports**: Availability, Trends (Legacy), Alerts, History, Summary, Histogram (Legacy), Notifications, Event Log.
- System**: Comments, Downtime, Process Info, Performance Info, Scheduling Queue, Configuration.

The main content area includes:

- Get Started**: A list of links to start monitoring infrastructure, change look and feel, extend with addons, get support, training, and certification.
- Nagios® Core™ Version 4.4.3**: Release date January 15, 2019, and a link to "Check for updates".
- Quick Links**: Nagios Library (tutorials and docs), Nagios Labs (development blog), Nagios Exchange (plugins and addons), Nagios Support (tech support), Nagios.com (company), Nagios.org (project).
- Latest News**: A placeholder section.
- Don't Miss...**: A placeholder section.

At the bottom, there is a copyright notice: "Copyright © 2010-2019 Nagios Core Development Team and Community Contributors. Copyright © 1999-2009 Ethan Galstad. See the THANKS file for more information on contributors." and a note about the GNU General Public License. Logos for "Nagios Core" and "SOURCEFORGE.NET" are at the bottom right.

Conclusion: We have successfully installed and configured Nagios Monitoring Server core service in our system now we need to install NRPE on all remote Linux systems to monitor with Nagios



PARIBHANAJI CHARITABLE TRUST

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

[NBA Accredited]



Academic Year: 2025-26 Semester: V Class / Branch: TE IT

Subject: Advanced Devops Lab (ADL)

Subject Lab Incharge: Prof Vishal Badgujar.

Name: Huzaifa Bubere

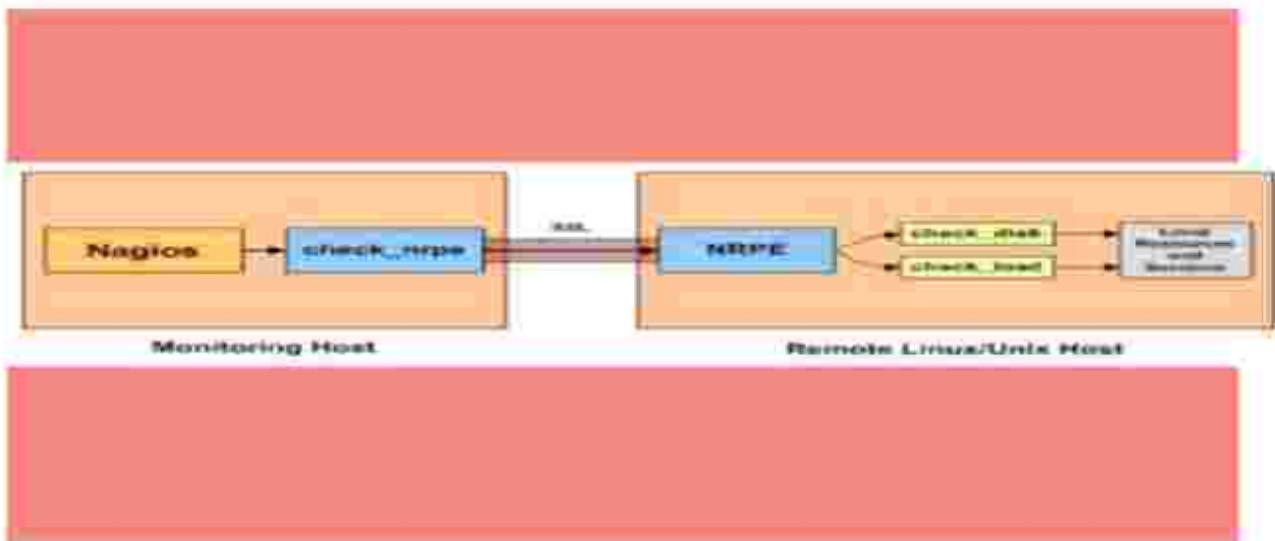
Student Id: 24204006

EXPERIMENT NO. 10

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

Theory:

Monitoring remote Linux/Unix hosts is to use the NRPE addon. NRPE allows you to execute plugins on remote Linux/Unix hosts. This is useful if you need to monitor local resources/attributes like disk usage, CPU load, memory usage, etc. on a remote host.



Note: To perform this experiment Experiment 9 is pre-requisite where we have configured Nagios on Linux System. Here In this Experiment we will Add a Linux Host to Nagios for Monitoring purpose.

Step 1 – Configure NRPE on Linux Host:

Follow the below steps to install and configure NRPE on client machine and check connectivity with Nagios server.

```
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo apt-get install nagios-nrpe-server nagios-plugins
Reading package lists... Done
Building dependency tree
Reading state information... Done
nagios-nrpe-server is already the newest version (4.0.0-2ubuntu1).
nagios-plugins is already the newest version (2.2-3ubuntu3.18.04.1).
The following packages were automatically installed and are no longer required:
  libgcc1:i386 libhttp-parser2.7.1 libssl1.0.0
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1829 not upgraded.
```

Step 1.2 – Configure NRPE

After successfully installing NRPE service, Edit nrpe configuration file /etc/nagios/nrpe.cfg in your favorite editor and add your nagios service ip in allowed hosts.

```
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo nano /etc/nagios/nrpe.cfg
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo /etc/init.d/nagios-nrpe-server restart
[ ok ] Restarting nagios-nrpe-server (via systemctl): nagios-nrpe-server.service.
```

allowed_hosts=127.0.0.1, 192.168.86.13, 192.168.86.30

After making above changes in nrpe configuration file, Lets restart NRPE service as per your system

Step 1.3 – Verify Connectivity from Nagios

Now run the below command from Nagios server to make sure your nagios is able to connect nrpe client on remote Linux system. Here 192.168.86.13 is your remote Linux system ip.

```
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ /usr/lib/nagios/plugins/check_nrpe -H 192.168.86.13
NRPE v4.0.0
```

Step 2 – Add Linux Host in Nagios

First create a configuration file using below values. for example you Linux hosts ip is . We also need to define a service with host. So add a ping check service, which will continuously check that host is up or not.

```
# -----
# Host definition
# -----
define host {
    use          linux-server
    host_name    Linux_Host_001
    alias        Linux Host 001
    address      192.168.86.13
```

```

register      1
}

# -----
# Service definition (PING check)
# -----

define service {
    use          generic-service
    host_name    Linux_Host_001
    service_description  PING
    check_command   check_ping!100.0,20%!500.0,60%
    max_check_attempts  2
    check_interval   2
    retry_interval   2
    check_period     24x7
    check_freshness   1
    contact_groups   admins
    notification_interval  2
    notification_period  24x7
    notifications_enabled  1
    register        1
}

```

Now verify configuration files using following command. If there are no errors found in configuration, restart nagios service.

```

nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo service nagios restart
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo service nagios start
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
htpasswd: password verification error
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users venny
New password:
Re-type new password:
Adding password for user venny
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo systemctl restart apache2
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo systemctl restart nagios
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo systemctl restart apache2
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo service nagios start
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ cat /usr/local/nagios/etc/htpasswd.users
venny:$apr1$CAKWL7hSvGtferrAxXlRXCX0e4Fg6.
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo nano /usr/local/nagios/etc/cgi.cfg
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo systemctl restart nagios
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo systemctl restart apache2
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ ls /etc/apache2/conf-available/
    charset.conf  javascript-common.conf  nagios.conf  other-vhosts-access-log.conf  serve-cgi-bin.conf
    gitweb.conf  localized-error-pages.conf  'nagios.conf.wq1'  security.conf
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo nano /etc/apache2/conf-available/nagios.conf
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo a2enconf nagios
Conf nagios already enabled
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo a2enmod cgi
Module cgi already enabled
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo systemctl restart apache2
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ sudo service nagios start
nagios@apsit-HP-280-Pro-G6-Microtower-PC:/opt/nagios-4.4.3/nagios-plugins-2.2.1$ █

```

Step 3 – Check Host in Nagios Web Interface

Open your Nagios web interface and check for new Linux hosts added in Nagios core service.

The screenshot shows the Nagios web interface at the URL `127.0.0.1/nagios/`. The main dashboard displays current network status, host status totals (1 Up, 0 Down, 0 Unreachable, 0 Pending), and service status totals (8 Ok, 0 Warning, 0 Unknown, 0 Critical, 0 Pending). On the right, a table titled "Host Status Details For All Host Groups" lists one host: "inc01host" (Status: UP, Last Check: 08-25-2025 11:20:47, Duration: 367d 4h 49m 48s, Status Information: PING OK - Packet loss = 0%, RTA = 0.07 ms). The left sidebar includes links for General, Home, Documentation, Current Status, Host Groups, Service Groups, Problems, Reports, and System.

127.0.0.1/nagios/

Nagios®

General

- Home
- Documentation

Current Status

- Tactical Overview
- Map (Legacy)
- Hosts
- Services
- Host Groups
- Summary
- Grid
- Service Groups
- Summary
- Grid
- Problems
- Services (Unhandled)
- Hosts (Unhandled)
- Network Outages

Quick Search:

Reports

- Availability
- Trends (Legacy)
- Alerts
- History
- Summary
- Histogram (Legacy)
- Notifications
- Event Log

System

- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue
- Configuration

Host Information

Last Updated: Thu Sep 25 11:22:37 IST 2025
 Updated every 90 seconds
 Nagios® Core™ 4.4.3 - www.nagios.org
 Logged in as vermy

Host
localhost
(localhost)

Member of
linux-servers

127.0.0.1

Host State Information

Host Status:	UP (for 367d 4h 50m 22s)
Status Information:	PING OK - Packet loss = 0%, RTA = 0.07 ms.
Performance Data:	rta=0.070000ms;3000.000000;5000.000000;0.000000 p=0%;80;100;0
Current Attempt:	1/10 (HARD state)
Last Check Time:	09-25-2025 11:20:47
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 4.100 seconds
Next Scheduled Active Check:	09-25-2025 11:25:47
Last State Change:	09-23-2024 08:32:15
Last Notification:	N/A (notification 0)
Is This Host Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	09-25-2025 11:22:29 (0d 0h 0m 8s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	ENABLED
Flap Detection:	ENABLED

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: We have successfully perform Port, Service monitoring, Linux server monitoring using Nagios.



Semester: V

Academic Year: 2022-23

Class / Branch: TE IT

Subject: Advanced Devops Lab (ADL)

Name of Instructor: Prof. Vishal Badgujar

Name of Student: Huzaifa Bubere
Student ID: 24204006

EXPERIMENT NO. 11

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

Steps: First Lambda functions using Python

1. Open Aws Console and search for Lambda Service and open home screen of Lambda.

2. Choose region in which you need to create Lambda function as it is region specific.

The screenshot shows the AWS Lambda service home page. The left sidebar is collapsed, showing options like CloudWatch Logs, Favorites and Dashboards, AI Operations, Alarms, Metrics, Application Monitoring (APM), Network Monitoring, Insights, and Settings. The main content area has two sections: 'Services' and 'Features'. Under 'Services', there are cards for Security Lake, Lambda, and ElastiCache. Under 'Features', there are cards for Launch templates (EC2 feature), Replays (Amazon EventBridge feature), and Alarms (CloudWatch feature). At the bottom left, there's a question 'Were these results helpful?' with 'Yes' and 'No' buttons. On the right, the 'Logs' tab is active, showing the Lambda logs for a function named 'lambdafunction'. The logs include entries for runtime initialization, incoming events, and a file upload event. The top right corner shows the region as 'Asia Pacific (Mumbai)' and the user as 'Huzaifa Bubere'.



3. Create sum as a Lambda Function in Python Language so select latest version of Python and choose role with basic Lambda Permission to allow cloudwatch for monitoring.

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.
- Browse serverless app repository
Deploy a sample Lambda application from the AWS Serverless Application Repository.

Basic information

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

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

Runtime Info
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.
Python 3.8

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

4. Lambda sum function is created successfully

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

Function overview Info

Diagram **Template**

Sum
Layers (0)

+ Add trigger + Add destination

Description
-

Last modified
32 seconds ago

Function ARN
arn:aws:lambda:ap-south-1:125582271444:function:Sum

Function URL Info
-

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

Code source Info

Open in Visual Studio Code Upload from

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



Write a sample python code for sum of two numbers:

The screenshot shows the AWS Lambda console interface. On the left, the function 'Sum' is selected. The code editor contains the following Python code:

```
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 right side of the screen shows a 'Create new test event' dialog. The 'Event Name' field is set to 'MyTest'. The 'Event sharing settings' section has 'Private' selected. The 'Template - optional' dropdown shows 'MyTest'. The 'Event JSON' field contains a simple JSON object:

```
1 {
2 }
```

A message at the bottom of the dialog says 'Test event is saved successfully.'

6. Configure Test Event in Json Format

The screenshot shows the AWS Lambda console interface. The function 'Sum' is selected. The code editor contains the same Python code as before. The right side of the screen shows the 'Edit test event' dialog. The 'Event Name' field is set to 'MyTest'. The 'Event JSON' field contains the following JSON object:

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

A message at the bottom of the dialog says 'Test event is saved successfully.'

Write a sample Second sample python Code:



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



Configure Test Event

If condition met returns a value as apsits

The screenshot shows the AWS Lambda console interface. On the left, the Lambda function 'Sum' is selected. In the center, the code editor displays a Python file named 'sum.py' with the following content:

```
import json
def lambda_handler(event, context):
    if event["name"] == "ABC":
        return "Hello ABC"
```

To the right of the code editor, there is an 'Edit test event' panel. It contains a JSON input field for defining the test event. The 'Event Name' is set to 'MyTest1'. The JSON input shows:

```
{"name": "ABC"}
```

Below the JSON input, the 'Response' field shows the output: "Hello ABC". At the bottom of the panel, there are tabs for PROBLEMS, OUTPUT, CODE REFERENCE LOG, and TERMINAL, along with an Execution Results dropdown.

On the far right, there is a sidebar titled 'Tutorials' with a section for 'Create a simple web app'. It includes a list of steps and a 'Start tutorial' button.

Conclusion: Write your own findings.



Semester: V

Academic Year: 2022-23

Class / Branch: TE IT

Subject: Advanced Devops Lab (ADL)

Name of Instructor: Prof. Vishal Badgujar

Name of Student: Huzaifa Bubere

Student ID: 24204006

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

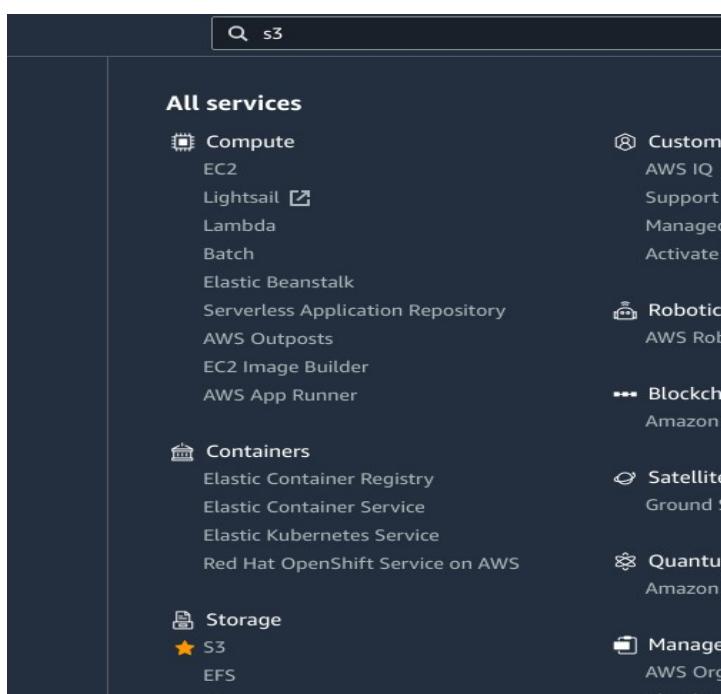
Theory:

Creating S3 Bucket

Let us start first by creating a s3 bucket in AWS console using the steps given below –

Step 1

Go to Amazon services and click **S3** in storage section as highlighted in the image given below –





Step 2

Click **S3** storage and **Create bucket** which will store the files uploaded.

The screenshot shows the Amazon S3 console. At the top left is the 'Amazon S3' logo. Below it is a section titled 'Account snapshot' with a link to 'View Storage Lens dashboard'. The main area is titled 'Buckets (3) Info' with a note that buckets are containers for data stored in S3. A 'Create bucket' button is prominently displayed at the top right of this section. Below this, there's a search bar and a toolbar with icons for refresh, copy ARN, empty, delete, and create bucket.

Step 3

Once you click Create bucket button, you can see a screen as follows –

Step 4

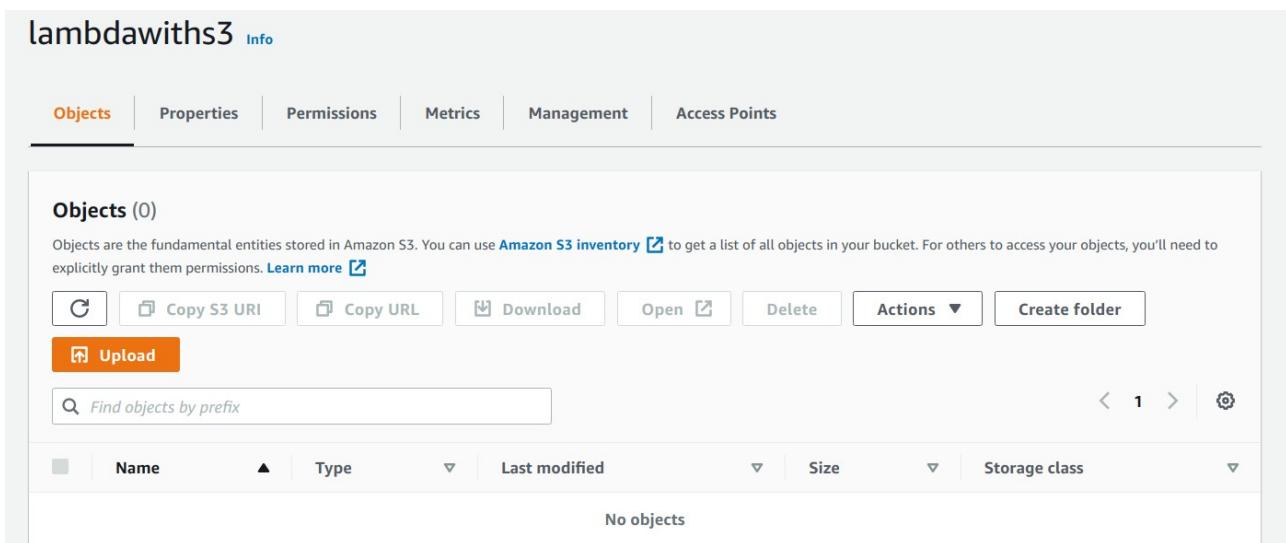
Enter the details Bucket name, Select the Region and click Create button at the bottom left side. Thus, we have created bucket with name :

The screenshot shows the Amazon S3 console after a bucket has been created. A green banner at the top states 'Successfully created bucket "lamdawiths3bh"' with a link to 'View details'. Below this, the 'General purpose buckets' section shows one bucket named 'lamdawiths3bh' in the 'Name' column, located in the 'Asia Pacific (Mumbai)' region. The 'Creation date' is listed as July 31, 2025, 11:19:02 (UTC+05:30). To the right, there are sections for 'Account snapshot' and 'External access summary - new'. The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, and cookie preferences.



Step 5

Now, click the bucket name and it will ask you to upload files as shown below –



Thus, we are done with bucket creation in S3.

Create Role that Works with S3 and Lambda

To create role that works with S3 and Lambda, please follow the Steps given below –

Step 1

Go to AWS services and select IAM as shown below –



Search results for 'iam'

Services

16) IAM Manage access to AWS resources

27)

Features See all 11 results ►

Step 2

Now, click **IAM -> Roles** as shown below –

IAM > Roles

Roles (18) 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

1

Create role

Step 3

Now, click **Create role** and choose the services that will use this role. Select Lambda and click **Permission** button.



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



Create role

1 2 3 4

Select type of trusted entity

AWS service EC2, Lambda and others	Another AWS account Belonging to you or 3rd party	Web identity Cognito or any OpenID provider	SAML 2.0 federation Your corporate directory
---------------------------------------	--	--	---

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose a use case

Common use cases

EC2

Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

API Gateway	CodeBuild	EMR Containers	IoT SiteWise	RDS
AWS Backup	CodeDeploy	ElastiCache	IoT Things Graph	Redshift
AWS Chatbot	CodeGuru	Elastic Beanstalk	KMS	Rekognition
AWS Marketplace	CodeStar Notifications	Elastic Container Registry	Kinesis	RoboMaker
AWS Support	Comprehend	Elastic Container Service	Lake Formation	S3
Amplify	Config	Elastic Transcoder	Lambda	SMS
AppStream 2.0	Connect	Elastic Load Balancing	Lex	SNS
AppSync	DMS	EventBridge	License Manager	SWF
Application Auto Scaling	Data Lifecycle Manager	Forecast	MQ	SageMaker
Application Discovery	Data Pipeline	GameLift	Machine Learning	Security Hub

* Required

Cancel

Next: Permissions

Step 4

Add the permission from below and click Review.

AmazonS3FullAccess, AWSLambdaFullAccess and CloudWatchFullAccess.

Step 5

Observe that we have chosen the following permissions –



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



Observe that the Policies that we have selected are **AmazonS3FullAccess**, **AWSLambdaFullAccess** and **CloudWatchFullAccess**.

The screenshot shows the AWS IAM Roles page. A green banner at the top indicates that the role 'lambdawiths3_H' has been created. The main table lists five roles, including the newly created one. The table columns are 'Role name', 'Trusted entities', and 'Last activity'. The newly created role 'lambdawiths3_H' is listed under 'AWS Service: lambda' with a timestamp of '15 minutes ago'. Below the table, there are sections for 'Roles Anywhere', 'Access AWS from your non AWS workloads', 'X.509 Standard', and 'Temporary credentials'.

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linked)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-
lambdawiths3_H	AWS Service: lambda	-
lambdawiths3-H	AWS Service: lambda	-
Sum-role-2jn00euc	AWS Service: lambda	15 minutes ago

Step 6

Now, enter the Role name, Role description and click Create Role button at the bottom.

Thus, our role named lambdawiths3service is created.

Create Lambda function and Add S3 Trigger

In this section, let us see how to create a Lambda function and add a S3 trigger to it. For this purpose, you will have to follow the Steps given below –

Step 1

Go to AWS Services and select Lambda as shown below –



The screenshot shows a search interface with a search bar containing 'Lambda'. Below it, a list of services is displayed under the heading 'Services'. The first item is 'Lambda' with the subtext 'Run Code without Thinking about Servers'. There is also a link 'See all 5 results ▶' and a vertical scroll bar.

Step 2

Click **Lambda** and follow the process for adding **Name**. Choose the **Runtime**, **Role** etc. and create the function. The Lambda function that we have created is shown in the screenshot below –

The screenshot shows the 'Create function' wizard. It starts with a choice between 'Author from scratch' (selected) and 'Use a blueprint'. The 'Basic information' section follows, where the function name is set to 'lambdawiths3bucket'. The 'Runtime' is chosen as 'Node.js 14.x'. In the 'Permissions' section, the default execution role is being changed. Under 'Execution role', the 'Use an existing role' option is selected, and the role 'lambdawiths3service' is chosen. The bottom part of the screenshot shows the 'Existing role' section, which lists the same role.



Step 3

Now let us add the S3 trigger.

S
t
e
p

4

Choose the trigger from above and add the details as shown below –

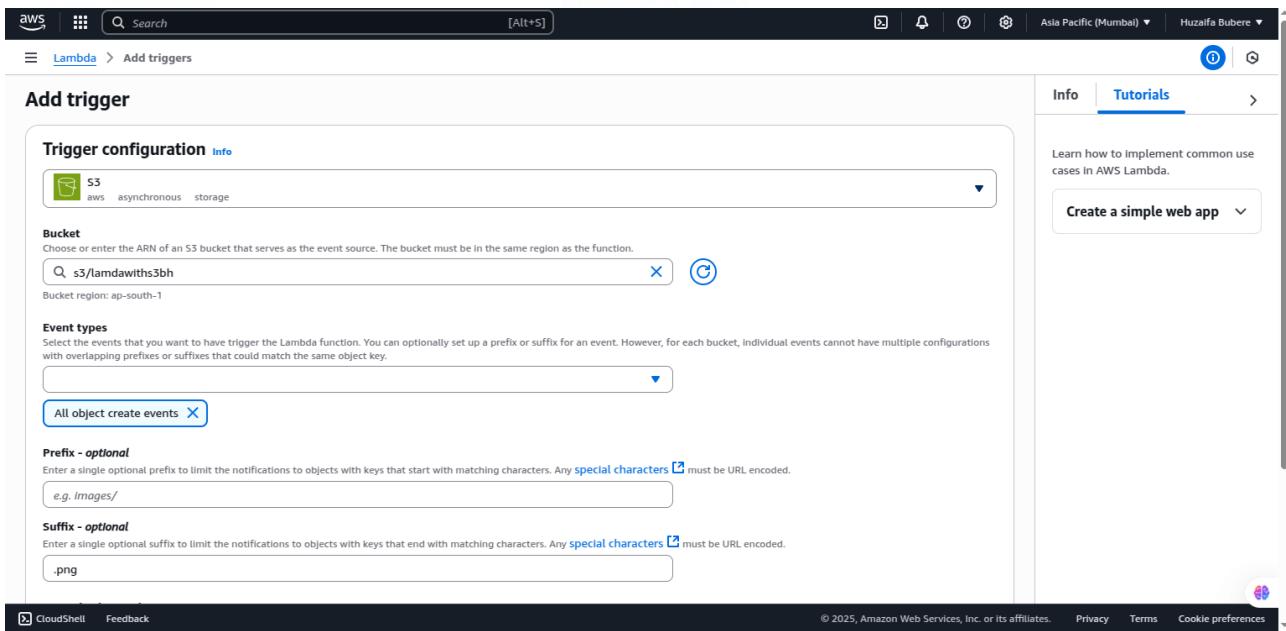
You can add Prefix and File pattern which are used to filter the files added. For Example, to trigger lambda only for .jpg images. as we need to trigger Lambda for all jpg image files uploaded. Click Add button to add the trigger.

Step 5

You can find the the trigger display for the Lambda function as shown below –



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

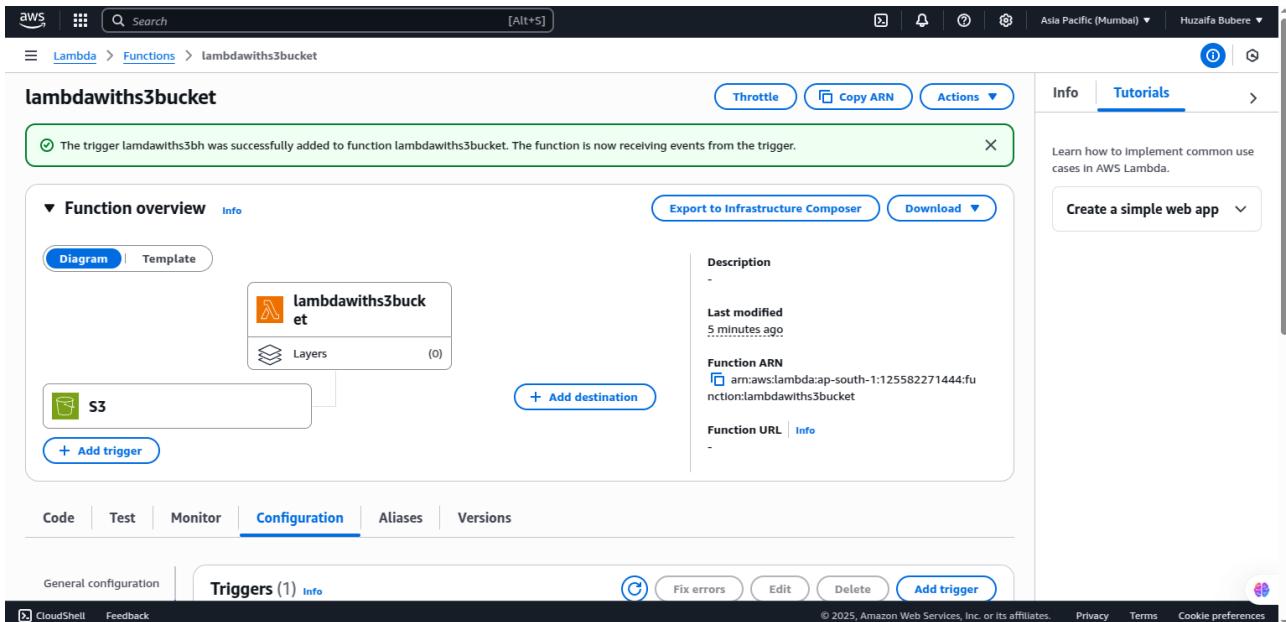


The screenshot shows the 'Trigger configuration' page for an AWS Lambda function. The 'Event types' section is set to 'All object create events'. Under 'Prefix - optional', there is a field with 'e.g. Images/'. Under 'Suffix - optional', there is a field with '.png'. The right sidebar features a 'Tutorials' section with a link to 'Create a simple web app'.

Step 6

Let's add the details for the aws lambda function. Here, we will use the online editor to add our code and use nodejs as the runtime environment.

To trigger S3 with AWS Lambda, we will have to use S3 event in the code as shown below

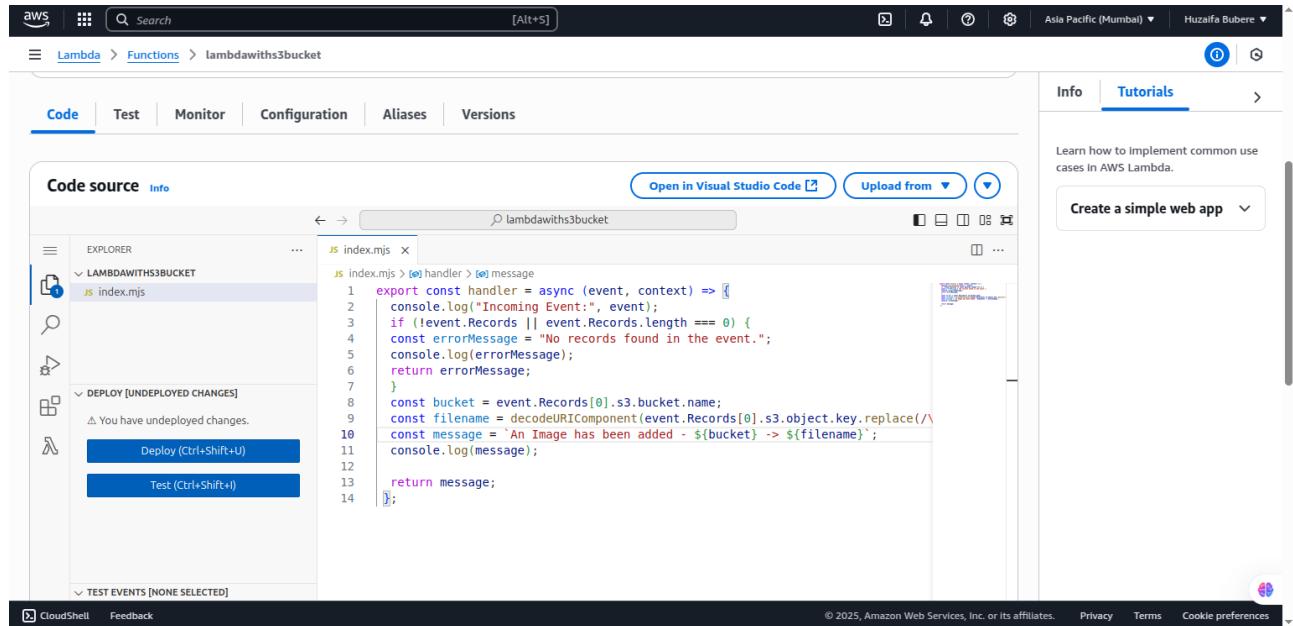


The screenshot shows the AWS Lambda function configuration for 'lambdawiths3bucket'. It displays a success message: 'The trigger lambdawiths3bh was successfully added to function lambdawiths3bucket. The function is now receiving events from the trigger.' The 'Configuration' tab is selected, showing the trigger details: 'lambdawiths3bucket' (Function ARN), 'S3' (Event source), and '+ Add destination'. The 'Triggers (1)' section shows the added trigger. The right sidebar includes a 'Tutorials' section with a link to 'Create a simple web app'.



Step 7:

let us save the changes and test the lambda function with S3upload.



The screenshot shows the AWS Lambda console interface. The top navigation bar includes 'AWS' and a search bar. Below it, the path 'Lambda > Functions > lambdawiths3bucket' is visible. The main area has tabs for 'Code', 'Test', 'Monitor', 'Configuration', 'Aliases', and 'Versions'. The 'Code' tab is selected, showing the 'Code source' section. On the left, there's an 'EXPLORER' sidebar with a tree view showing a folder 'LAMBDAWITHS3BUCKET' containing 'index.mjs'. The main editor window displays the following JavaScript code:

```
index.mjs
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};
```

Below the editor, there are buttons for 'Deploy (Ctrl+Shift+U)' and 'Test (Ctrl+Shift+I)'. The right side of the interface includes a 'Tutorials' section with a link to 'Create a simple web app'.

Step 8:

Now, save the Lambda function. Open S3 from Amazon services and open the bucket we created earlier namely lambdawiths3.



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



Upload the image in it as shown below –

Click **Add files** to add files. You can also drag and drop the files. Now, click **Upload** button.

The screenshot shows the AWS S3 console interface. In the top navigation bar, the path is Amazon S3 > Buckets > lamdawiths3bh > Upload. The main area is titled "Upload" with an "Info" link. It contains a large dashed blue box for dragging and dropping files. Below this is a table titled "Files and folders (1 total, 147.7 KB)". The table has columns for Name, Folder, Type, and Size. One item, "1.png", is listed with a size of 147.7 KB and type image/png. There are "Remove", "Add files", and "Add folder" buttons at the top right of the table. Under "Destination" (Info), the destination is set to "s3://lamdawiths3bh". The "Destination details" section notes bucket settings for new objects. The "Permissions" section grants public access. At the bottom, there are links for CloudShell, Feedback, and copyright information.

Thus, we have uploaded one image in our S3 bucket.

The screenshot shows the AWS S3 console after the upload. A green banner at the top says "Upload succeeded. For more information, see the Files and folders table." Below this is a summary table with sections for "Succeeded" (1 file, 147.7 KB) and "Failed" (0 files, 0 B). The "Files and folders" tab is selected, showing a table with columns: Name, Folder, Type, Size, Status, and Error. The single file "1.png" is listed with a status of "Succeeded". The bottom of the page includes CloudShell, Feedback, and copyright information.



Step 9

To see the trigger details, go to AWS service and select CloudWatch. Open the logs for the Lambda AWS Lambda function gets triggered when file is uploaded in S3 bucket and the details are logged in Cloudwatch as shown below –

The screenshot shows the AWS CloudWatch Log Groups interface. The left sidebar is collapsed. The main area displays a log group named '/aws/lambda/lambdawiths3bucket'. The 'Log streams' tab is selected. It shows one log stream entry:

Log stream	Last event time
2025/07/31/[LATEST]81a81bb5537a247ea8f76d9404ae812e9	2025-07-31 06:09:09 (UTC)

The screenshot shows the AWS CloudWatch Log Events interface. The left sidebar is collapsed. The main area displays log events for the same log group. The 'Display' dropdown is set to 'Timestamp'. The log events table shows the following entries:

Timestamp	Message
2025-07-31T06:14:22.013Z	INIT_START Runtime Version: nodejs:18.v76 Runtime Version ARN: arn:aws:lambda:ap-south-1::runtime:db8a276f9276d75e613561...
2025-07-31T06:14:22.156Z	START RequestId: 5cf01e98-158d-4640-9e40-6267c654dc9 Version: \$LATEST
2025-07-31T06:14:22.157Z	2025-07-31T06:14:22.157Z 5cf01e98-158d-4640-9e40-6267c654dc9 INFO Incoming Event: {}
2025-07-31T06:14:22.159Z	2025-07-31T06:14:22.159Z 5cf01e98-158d-4640-9e40-6267c654dc9 INFO No records found in the event.
2025-07-31T06:14:22.200Z	END RequestId: 5cf01e98-158d-4640-9e40-6267c654dc9
2025-07-31T06:14:22.200Z	REPORT RequestId: 5cf01e98-158d-4640-9e40-6267c654dc9 Duration: 42.31 ms Billed Duration: 43 ms Memory Size: 128 MB Max...
2025-07-31T06:15:07.367Z	START RequestId: f732eab6-b2e2-4c93-be18-eab4ad917541 Version: \$LATEST
2025-07-31T06:15:07.368Z	2025-07-31T06:15:07.368Z f732eab6-b2e2-4c93-be18-eab4ad917541 INFO Incoming Event: { Records: [{ eventVersion: '2.1', e...
2025-07-31T06:15:07.376Z	2025-07-31T06:15:07.376Z f732eab6-b2e2-4c93-be18-eab4ad917541 INFO An Image has been added - lambdawiths3bh -> 2.png
2025-07-31T06:15:07.458Z	END RequestId: f732eab6-b2e2-4c93-be18-eab4ad917541
2025-07-31T06:15:07.458Z	REPORT RequestId: f732eab6-b2e2-4c93-be18-eab4ad917541 Duration: 89.94 ms Billed Duration: 90 ms Memory Size: 128 MB Max...



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



An image has been Added -> 2.png you can see in cloudwatch logs.

Conclusion: Write your own findings.