

EC2 Instance:

Instance Launching

The screenshot shows the AWS EC2 Instances Launch wizard. At the top, there's a green success banner stating "Successfully initiated launch of instance i-0a406efef1fccaaecd". Below it, a "Next Steps" section contains four cards: "Create billing and free tier usage alerts", "Connect to your instance", "Connect an RDS database", and "Create EBS snapshot policy". Each card has a "Learn more" link and a "Create" button.

The screenshot shows the AWS EC2 Instances list. It displays one instance: "Shraeyaa's server" (i-0a406efef1fccaaecd), which is "Running". The instance is located in "eu-north-1b" and has a public IP of "ec2-16-171-255-242.eu-north-1.compute.amazonaws.com". The "Launch instances" button is highlighted in orange at the top right of the list table.

The screenshot shows the AWS EC2 Instance details page for "i-0a406efef1fccaaecd (Shraeyaa's server)". The "Details" tab is selected. Key information shown includes:

Attribute	Value
Instance ID	i-0a406efef1fccaaecd (Shraeyaa's server)
Public IPv4 address	16.171.255.242 Open address
Private IPv4 addresses	172.31.33.214
Instance state	Running
Public IPv4 DNS	ec2-16-171-255-242.eu-north-1.compute.amazonaws.com Open address

```
AWS | Services | Search [Alt+5]
System load: 0.23      Temperature: -273.1 C
Usage of /: 10.5% of 14.46GB  Processes: 114
Memory usage: 24%      Users logged in: 0
Swap usage: 0%          IPv4 address for ens5: 172.31.33.214

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

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

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

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

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

ubuntu@ip-172-31-33-214:~$
```

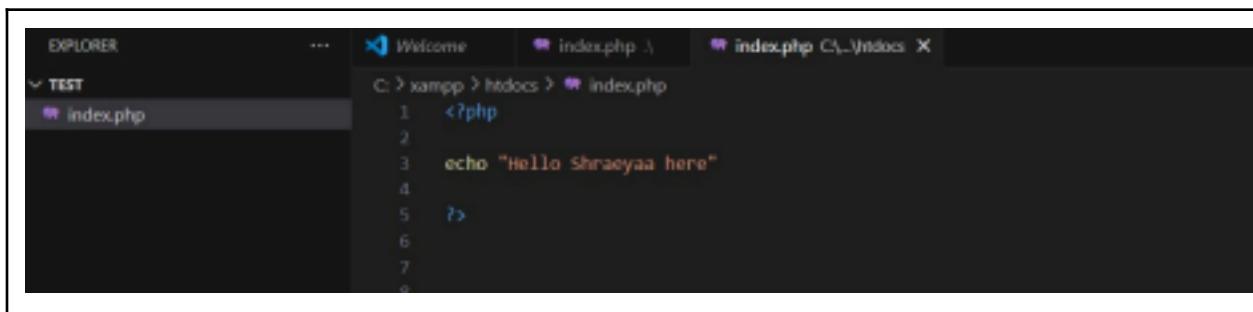
i-0a406efe1fccaaecd (Shraeyaa's server)
PublicIPs: 16.171.255.242 PrivateIPs: 172.31.33.214

A) To develop a website and host it on local machine on a VM

The screenshot shows a code editor interface with an 'EXPLORER' sidebar on the left containing files: 'index.php', 'file.html', 'index.php (1).index', 'file.html (1)', and 'shraeyaa.png'. The 'file.html' file is selected and its content is displayed in the main editor area:

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Document</title>
    <style>
        img{
            height: 250px;
            width: 250px;
        }
    </style>
</head>
<body>
    <h1>Name:Shraeyaa Bhagade</h1>
    <h2>Div(B1SA)</h2>
    <h2>Roll no.: 15</h2>
    
</body>
</html>
```

On the right side of the editor, there is a preview window showing a basic web page with the title 'Document'. It contains the text 'Name:Shraeyaa Bhagade' and 'Div(B1SA)' in bold. Below that, it says 'Roll no.: 15'. There is also a placeholder image where the 'shraeyaa.png' file should be displayed.



B)Setup Devops infrastructure on CloudWork and setup IDE on Cloud9

Create environment Info

Details

Name

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

Description - optional

Limit 200 characters.

Environment type Info

Determines what the Cloud9 IDE will run on.

New EC2 instance

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

Existing compute

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

New EC2 instance

Instance type Info

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

t2.micro (1 GiB RAM + 1 vCPU)

Free-tier eligible. Ideal for educational users and exploration.

t3.small (2 GiB RAM + 2 vCPU)

Recommended for small web projects.

m5.large (8 GiB RAM + 2 vCPU)

Recommended for production and most general-purpose development.

Additional instance types

Explore additional instances to fit your need.

Platform Info

This will be installed on your EC2 instance. We recommend Amazon Linux 2023.



Timeout

How long Cloud9 can be inactive (no user input) before auto-hibernating. This helps prevent unnecessary charges.



Network settings [Info](#)

Connection
How your environment is accessed.

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

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

VPC settings [Info](#)

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

The following IAM resources will be created in your account

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

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

Environments (1)					
	Delete	View details	Open in Cloud9	Create environment	
My environments					
Name	Cloud9 IDE	Environment type	Connection	Permissions	Owner ARN
webapp	Open	EC2 instance	AWS Systems Manager (SSM)	Owner	arn:aws:iam::011528263675:root

webapp - /home/ec2-user

README.md

vesindex.html

```

1  <!DOCTYPE html>
2  <html>
3      <head>
4          <title>Welcome to VESIT</title>
5      </head>
6      <body>
7          <h1>Hello everyone</h1>
8      </body>
9  </html>
```

ADV DEVOPS EXP2

AIM:

To Build Your Application using AWS Code Build and Deploy on S3 / SEBS using AWS CodePipeline, deploy Sample Application on EC2 instance using AWS Code Deploy.

Create role

Select trusted entity

Trusted entity type

- AWS service
- AWS account
- Web identity
- SAML 2.0 federation
- Custom trust policy

Use case

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

Service or use case

EC2

Add permissions

Permissions policies (1/946)

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

Policy name	Type	Description
<input checked="" type="checkbox"/> AmazonEC2RoleforAWSCodeDeploy	AWS managed	Provides EC2 access to S3 bucket to do...
<input type="checkbox"/> AmazonEC2RoleforAWSCodeDeployLi...	AWS managed	Provides EC2 limited access to S3 buck...
<input type="checkbox"/> AWSCodeDeployDeployerAccess	AWS managed	Provides access to register and deploy ...
<input type="checkbox"/> AWSCodeDeployFullAccess	AWS managed	Provides full access to CodeDeploy res...
<input type="checkbox"/> AWSCodeDeployReadOnlyAccess	AWS managed	Provides read only access to CodeDepl...
<input type="checkbox"/> AWSCodeDeployRole	AWS managed	Provides CodeDeploy service access to ...
<input type="checkbox"/> AWSCodeDeployRoleForCloudFormation	AWS managed	Provides CodeDeploy service access to ...
<input type="checkbox"/> AWSCodeDeployRoleForECS	AWS managed	Provides CodeDeploy service wide acce...
<input type="checkbox"/> AWSCodeDeployRoleForECSLimited	AWS managed	Provides CodeDeploy service limited a...

Role Details

The screenshot shows the 'Name, review, and create' step of the 'Create role' wizard. In the 'Role details' section, the 'Role name' is set to 'EC2CodeDeploy'. The 'Description' field contains the text 'Allows EC2 instances to call AWS services on your behalf.' In the 'Step 1: Select trusted entities' section, the 'Trust policy' is displayed with the following JSON code:

```
1+ [  
2+     "Version": "2012-10-17",  
3+     "Statement": [  
4+         {  
5+             "Effect": "Allow",  
6+             "Principal": "*"  
7+         }  
8+     ]  
9+ ]
```

At the bottom right of the main area is an 'Edit' button.

Role Created

The screenshot shows the 'Roles' page with a green banner at the top stating 'Role EC2CodeDeploy created.' The 'Roles (3) Info' section lists three roles: 'AWSServiceRoleForSupport', 'AWSServiceRoleForTrustedAdvisor', and 'EC2CodeDeploy'. The 'EC2CodeDeploy' role is highlighted. Below this, the 'Roles Anywhere' section provides options for accessing AWS services from non-AWS workloads, using X.509 certificates, or managing temporary credentials.

Create Role 2

The screenshot shows the 'Name, review, and create' step of the 'Create role' wizard. In the 'Role details' section, the 'Role name' is set to 'CodeDeployRole'. The 'Description' field contains the text 'Allows CodeDeploy to call AWS services such as Auto Scaling on your behalf.' In the 'Step 1: Select trusted entities' section, the 'Trust policy' is displayed with the following JSON code:

```
1+ [  
2+     "Version": "2012-10-17",  
3+     "Statement": [  
4+         {  
5+             "Effect": "Allow",  
6+             "Principal": "CodeDeploy.amazonaws.com"  
7+         }  
8+     ]  
9+ ]
```

At the bottom right of the main area is an 'Edit' button.

Screenshot of the AWS IAM 'Select trusted entity' step. The page shows the 'Trusted entity type' section with four options: AWS service (selected), AWS account, SAML 2.0 federation, and Custom trust policy. Below this is the 'Use case' section, which is currently empty. A dropdown menu for 'Service or use case' shows 'CodeDeploy' selected.

Launch instance after creating role

Network settings

- Network: vpc-0f45b9105239befd2
- Subnet: No preference (Default subnet in any availability zone)
- Auto-assign public IP: Enabled
- Additional charges apply when outside of free tier allowance
- Firewall (security groups): Select existing security group (selected)
- Common security groups: default sg-087439adff63cf516c (selected)

Advanced details

- Domain join directory: Select (Create new directory)
- IAM instance profile: EC2CodeDeploy (Create new IAM profile)
- Hostname type: IP name
- DNS Hostname: Enable IP name IPv4 (A record) DNS requests (checked)
- Enable resource-based IPv4 (A record) DNS requests (checked)

Quick Start

Amazon Machine Image (AMI)

Amazon Linux	macOS	Ubuntu	Wind

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

Description

Amazon Linux 2023 AMI
Free tier eligible
ami-090abff6ae1141d7d (64-bit (x86), uefi-preferred) / ami-0a44bcb8b18f238d (64-b...
Virtualization: hvm ENA enabled: true Root device type: ebs

Architecture: 64-bit (x86)
Boot mode: uefi-preferred
AMI ID: ami-090abff6ae1141d7d
Verified provider

aws Services Search [Alt+S]

EC2 > Instances > Launch an instance

Success Successfully initiated launch of instance (i-06c90a085fa0de0fb)

Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

1 2 3 4 5 6

Create billing and free tier usage alerts
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more

Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy

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

Developer Tools > CodeDeploy > Applications > Create application

Create application

Application configuration

Application name
Enter an application name
 100 character limit

Compute platform
Choose a compute platform

Tags

Cancel

Enter a deployment group name
 100 character limit

Service role

Enter a service role
Enter a service role with CodeDeploy permissions that grants AWS CodeDeploy access to your target instances.
 X

Deployment type

Choose how to deploy your application

In-place
Updates the instances in the deployment group with the latest application revisions. During a deployment, each instance will be briefly taken offline for its update

Blue/green
Replaces the instances in the deployment group with new instances and deploys the latest application revision to them. After instances in the replacement environment are registered with a load balancer, instances from the original environment are deregistered and can be terminated.

AWS Services Search [Alt+S] Stockholm eeshachavan

Developer Tools CodeDeploy

- Source • CodeCommit
- Artifacts • CodeArtifact
- Build • CodeBuild
- Deploy • CodeDeploy
 - Getting started
 - Deployments
 - Applications
 - Application**
 - Settings
 - Deployment configurations
 - On-premises instances
 - Pipeline • CodePipeline
 - Settings
- Go to resource
- Feedback

Application created
In order to create a new deployment, you must first create a deployment group.

Developer Tools > CodeDeploy > Applications > AAR-CICD

AAR-CICD

Notify Delete application

Application details

Name	AAR-CICD	Compute platform	EC2/On-premises
------	----------	------------------	-----------------

Deployments Deployment groups Revisions

Deployment groups

Name	Status	Last attempted deploy...	Last successful deploy...	Trigger count
No deployment groups				

Create deployment group

AWS Services Search [Alt+S] Stockholm eeshachavan

Developer Tools CodeDeploy

- Source • CodeCommit
- Artifacts • CodeArtifact
- Build • CodeBuild
- Deploy • CodeDeploy
 - Getting started
 - Deployments
 - Applications
 - Application**
 - Settings
 - Deployment configurations
 - On-premises instances
 - Pipeline • CodePipeline
 - Settings
- Go to resource
- Feedback

Success Deployment group created

Developer Tools > CodeDeploy > Applications > AAR-CICD > AAR-CICD-DP

AAR-CICD-DP

Edit Delete Create deployment

Deployment group details

Deployment group name	Application name	Compute platform
AAR-CICD-DP	AAR-CICD	EC2/On-premises
Deployment type	Service role ARN	Deployment configuration
In-place	arn:aws:iam::010928190992:role/CodeDeployRole	CodeDeployDefault.AllAtOnce
Rollback enabled	Agent update scheduler	
False	Learn to schedule update in AWS Systems Manager	

Environment configuration: Amazon EC2 instances

Key	Value
Name	-

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

▼ Advanced details [Info](#)

Domain join directory | [Info](#)

Select

 [Create new directory](#)

IAM instance profile | [Info](#)

EC2CodeDeploy

arn:aws:iam::022499027707:instance-profile/EC2CodeDeploy

 [Create new IAM profile](#)

Hostname type | [Info](#)

IP name

DNS Hostname | [Info](#)

Enable IP name IPv4 (A record) DNS requests

Enable resource-based IPv4 (A record) DNS requests

▼ Network settings [Info](#)

[Edit](#)

Network [Info](#)

vpc-0f45b9105239befd2

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of **free tier allowance**

Firewall (security groups) [Info](#)

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

Create security group

Select existing security group

Common security groups [Info](#)

Select security groups ▾

[Compare](#)

 [security group rules](#)

default sg-087439adf63cf516c 
VPC: vpc-0f45b9105239befd2

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Create pipeline step by step

Screenshot of the AWS CodePipeline 'Review' step (Step 5 of 5) showing pipeline settings.

Step 1: Choose pipeline settings

Pipeline settings		
Pipeline name	AAR-CICD-PIPELINE	
Pipeline type	V2	
Execution mode	QUEUED	
Artifact location	A new Amazon S3 bucket will be created as the default artifact store for your pipeline	
Service role name	AWSCodePipelineServiceRole-ap-southeast-2-AAR-CICD-PIPELINE	

Variables

Name	Default value	Description
		© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Screenshot of the 'Add source stage' step (Step 2 of 5) showing the 'Source' provider selected as GitHub (Version 2).

New GitHub version 2 (app-based) action

To add a GitHub version 2 action in CodePipeline, you create a connection, access your repository. Use the options below to choose an existing connection or create a new one.

Create a connection

Create GitHub App connection

Connection name: AAR-CICD-GIT

Tags - optional

Connect to GitHub

Screenshot of the 'Create connection' step showing the GitHub connection settings.

GitHub connection settings

Connection name: AAR-CICD-GIT

App installation - optional

Install GitHub App to connect as a bot. Alternatively, leave it blank to connect as a GitHub user, which can be used in AWS CodeBuild projects.

Q 53892311 or Install a new app

Tags - optional

Connect

Screenshot of the AWS CloudFormation console showing the creation of a pipeline. The pipeline is currently at Step 5: Review.

Step 3: Add build stage

Step 4: Add deploy stage

Step 5: Review

Deploy

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

AWS CodeDeploy

Region: Europe (Stockholm)

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

No more than 100 characters

Application name: Choose an application that you have already created in the AWS CodeDeploy console. Or create an application in the AWS CodeDeploy console and then return to this task.

AAR-CICD

Deployment group: Choose a deployment group that you have already created in the AWS CodeDeploy console. Or create a deployment group in the AWS CodeDeploy console and then return to this task.

AAR-CICD-DR

Configure automatic rollback on stage failure

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

Step 1: Choose pipeline settings

Pipeline settings

Pipeline name

AAR-CICD-PIPELINE

Pipeline type

V2

Execution mode

QUEUED

Artifact location

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

Service role name

AWSCodePipelineServiceRole-eu-north-1-AAR-CICD-PIPELINE

Step 2: Add source stage

Source action provider

```
Source action provider
GitHub (Version 2)
OutputArtifactFormat
CODE_ZIP
DetectChanges
false
ConnectionArn
arn:aws:codeconnections:eu-north-1:022499027707:connection/11f0aa91-d0a7-4358-9471-ba18c8472ba9
FullRepositoryId
shrayasic/aws_cicd_pipeline_codedeploy
Default branch
main
```

Trigger configuration

You can add additional pipeline triggers after the pipeline is created.

Trigger type

Step 3: Add build stage

Build action provider

Build stage

No build

Step 4: Add deploy stage

Deploy action provider

Deploy action provider

AWS CodeDeploy

ApplicationName

AAR-CICD

DeploymentGroupName

AAR-CICD-DP

Configure automatic rollback on stage failure

Disabled

Cancel

Previous

Create pipeline

Pipeline Created

[EC2](#) > [Security Groups](#) > [sg-087439adf63cf516c - default](#) > Edit inbound rules

Edit inbound rules info

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

Inbound rules <small>Info</small>						
Security group rule ID	Type <small>Info</small>	Protocol <small>Info</small>	Port range	Source <small>Info</small>	Description - optional <small>Info</small>	
<small>Info</small>						
sgr-03c8e532e3aebfcca	All traffic	All	All	Custom	<input type="text" value="sg-087439adf63cf516c"/> <small>X</small>	<small>Delete</small>
-	HTTP	TCP	80	Anyw...	<input type="text" value="0.0.0.0"/> <small>X</small>	<small>Delete</small>
-	SSH	TCP	22	Anyw...	<input type="text" value="0.0.0.0"/> <small>X</small>	<small>Delete</small>

[Add rule](#)



Congratulations! The pipeline AAR-CICD-PIPELINE has been created.

[Create a notification rule for this pipeline](#)

[Developer Tools](#) > [CodePipeline](#) > [Pipelines](#) > AAR-CICD-PIPELINE

AAR-CICD-PIPELINE

Pipeline type: V2 Execution mode: QUEUED

[Notify](#) ▼ [Edit](#) [Stop execution](#) [Clone pipeline](#) [Release change](#)

⊕ **Source** In progress

Pipeline execution ID: [06a28e89-6fc9-48b7-abec-3d0ad3fa1bb8](#)

Source

⊕ In progress - Just now

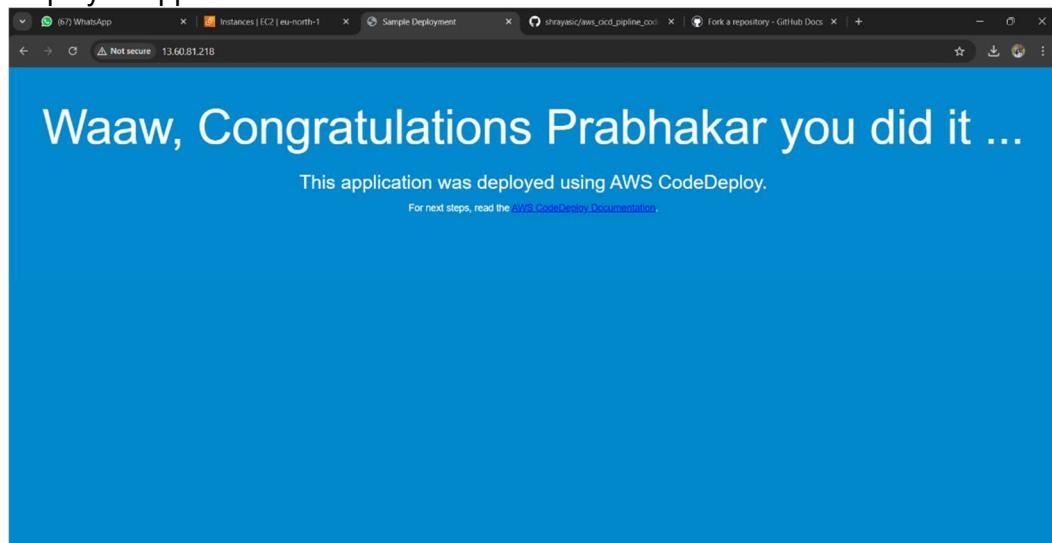
[View details](#)

[Disable transition](#)

⊕ **Deploy** ⓘ Didn't Run

[Start rollback](#)

Deployed application



EXPERIMENT 3

SHRAEYAA DHAIGUDE

D15A15

Experiment 3.

Aim: To understand the kubernetes Cluster Architecture, install and spin up a Kubernetes cluster on Linux Machine / Cloud Platforms.

Theory:

Container-based microservices architectures have transformed how software is developed and deployed by simplifying scaling and deployment. However, they also introduce complexity due to the new infrastructure ecosystem they create. Companies are now managing thousands of container instances daily, a challenge addressed by Kubernetes.

Kubernetes automates the deployment, scaling and management of containerized applications. It abstracts the underlying infrastructure, allowing developers to focus on the app while Kubernetes handles the load.

- Managing resource consumption to prevent overuse
- Balancing application load across hosts
- Automatically restarting apps if they consume too many resources
- Shifting applications between hosts
- Seamlessly adding new hosts
- Enabling easy rollbacks

Steps:

1. Create 2 EC2 Ubuntu Instances on AWS.

(Name 1 as Master, the 2 as worker-node)

The screenshot shows the AWS EC2 'Launch an instance' success page. At the top, a green bar indicates 'Success' with the message 'Successfully initiated launch of instances (i-0dbd49314505a02fb, i-0c46e36963b0f9487)'. Below this, there's a 'Launch log' link. The main area is titled 'Next Steps' with a sub-instruction 'Q. What would you like to do next with these instances, for example "create alarm" or "create backup"?' followed by a navigation bar with links 1 through 6. Four cards are displayed below: 'Create billing and free tier usage alerts' (with a 'Create billing alerts' button), 'Connect to your instance' (with a 'Learn more' link), 'Connect an RDS database' (with 'Connect an RDS database', 'Create a new RDS database', and 'Learn more' buttons), and 'Create EBS snapshot policy' (with a 'Create EBS snapshot policy' button).

2. Edit the Security Group Inbound Rules to allow SSH

The screenshot shows the 'Edit inbound rules' page. It includes a header note about inbound rules controlling incoming traffic. The main interface has tabs for 'Inbound rules' and 'Info'. Under 'Inbound rules', there's a table with columns: Security group rule ID, Type, Protocol, Port range, Source, and Description - optional. A single row is shown with 'All traffic' selected for Type, All for Protocol, All for Port range, Anywh... for Source, and an empty Description field. Buttons for 'Add rule', 'Delete', and a search bar are present. A warning message at the bottom left says '⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.' At the bottom right are 'Cancel', 'Preview changes', and a highlighted 'Save rules' button.

3. Connect Instances

The screenshot shows the 'Connect to instance' page. It starts with a note 'Connect to your instance i-0dbd49314505a02fb (Master) using any of these options'. Below are tabs for 'EC2 Instance Connect', 'Session Manager', 'SSH client', and 'EC2 serial console'. A warning box states '⚠ All ports are open to all IPv4 addresses in your security group' and provides details about the inbound rule. The 'EC2 Instance Connect' tab is active, showing the instance ID 'i-0dbd49314505a02fb (Master)'. Under 'Connection Type', two options are listed: 'Connect using EC2 Instance Connect' (selected) and 'Connect using EC2 Instance Connect Endpoint'. Below these are fields for 'Public IPv4 address' (13.60.199.55) and 'Username' (left empty). A note at the bottom says 'Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username.'

4. From now on, until mentioned, perform these steps on all 3 machines.

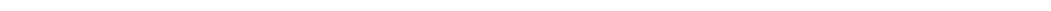
Install Docker

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

Then, configure cgroup in a daemon.json file.

```
cd /etc/docker  
cat <<EOF | sudo tee /etc/docker/daemon.json  
{  
    "exec-opts": ["native.cgroupdriver=systemd"],  
    "log-driver": "json-file",  
    "log-opt": {  
        "max-size": "100m"  
    },  
    "storage-driver": "overlay2"  
}  
EOF  
sudo systemctl enable docker  
sudo systemctl daemon-reload  
sudo systemctl restart  
docker
```

```
ubuntu@ip-172-31-36-117:~$ sudo hostnamectl set-hostname master-node  
ubuntu@ip-172-31-36-117:~$ exit  
logout
```



```
ubuntu@worker1:~$ sudo apt-get update  
Hit:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble InRelease  
Hit:2 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates InR  
Hit:3 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-backports I  
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 k
```



```
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 ubun  
Suggested packages:  
  ifupdown aufs-tools cgroupfs-mount | cgroup-lite debootstrap dock  
The following NEW packages will be installed:  
  bridge-utils containerd dns-root-data dnsmasq-base docker.io pigz  
0 upgraded, 8 newly installed, 0 to remove and 133 not upgraded.  
Need to get 76.8 MB of archives.  
After this operation, 289 MB of additional disk space will be used.  
Do you want to continue? [Y/n] Y
```

```
aws | Services | Search

ubuntu@master-node:~$ sudo systemctl enable docker
ubuntu@master-node:~$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
    Loaded: loaded (/usr/lib/systemd/system/docker.service;
              Active: active (running) since Sun 2024-09-15 18:07:29
TriggeredBy: ● docker.socket
    Docs: https://docs.docker.com
   Main PID: 3174 (dockerd)
      Tasks: 9
     Memory: 72.3M (peak: 74.3M)
        CPU: 364ms
      CGroup: /system.slice/docker.service
              └─3174 /usr/bin/dockerd -H fd:// --containerd=/run/ct
Sep 15 18:07:29 master-node systemd[1]: Starting docker.servi
Sep 15 18:07:29 master-node dockerd[3174]: time="2024-09-15T
Sep 15 18:07:29 master-node systemd[1]: Started docker.servi
lines 1-21/21 (END)
```

```
ubuntu@master-node:~$ sudo apt-get install ca-certificates curl
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.
The following additional packages will be installed:
  libcurl3t64-gnutls libcurl4t64
The following packages will be upgraded:
  curl libcurl3t64-gnutls libcurl4t64
3 upgraded, 0 newly installed, 0 to remove and 130 not upgraded.
Need to get 900 kB of archives.
After this operation, 3072 B of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@master-node:~$ sudo install -m 0755 -d /etc/apt/keyrings
ubuntu@master-node:~$ sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /etc/apt/keyrings/docker.asc
ubuntu@master-node:~$ echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] https://download.docker.com/linux/ubuntu \
> $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
> sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
ubuntu@master-node:~$ sudo apt-get update
Hit:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:4 https://download.docker.com/linux/ubuntu noble InRelease [48.8 kB]
Hit:5 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:6 https://download.docker.com/linux/ubuntu noble/stable amd64 Packages [13.8 kB]
Fetched 62.6 kB in 1s (107 kB/s)
Reading package lists... Done
ubuntu@master-node:~$
```

```
ubuntu@master-node:~$ sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  bridge-utils dns-root-data dnsmasq-base ubuntu-fan
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  docker-ce-rootless-extras libltdl7 libslirp0 slirp4netns
```

Install Kubernetes on all 3 machines

```
curl -s https://packages.cloud.google.com/apt/doc/apt-key.gpg |  
sudo apt-key add -  
cat << EOF | sudo tee /etc/apt/sources.list.d/kubernetes.list  
deb https://apt.kubernetes.io/ kubernetes-xenial main EOF  
sudo apt-get update  
sudo apt-get install -y kubelet kubeadm kubectl  
ubuntu@master-node:~$ curl -fsSL https://pkgs.k8s.io/core:/stable:/v1.31/deb/Release.key | sudo gpg --dearmor -o /etc/apt  
ubuntu@master-node:~$ echo 'deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable  
es.list.d/kubernetes.list  
deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:/v1.31/deb/ /  
ubuntu@master-node:~$ sudo apt-get update  
Hit:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble InRelease  
Hit:2 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease  
Hit:3 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease  
Hit:4 https://download.docker.com/linux/ubuntu noble InRelease  
Hit:5 https://security.ubuntu.com/ubuntu noble-security InRelease  
Get:6 https://prod-cdn.packages.k8s.io/repositories/isv/:kubernetes/:core:/stable:/v1.31/deb InRelease [1186 B]  
Get:7 https://prod-cdn.packages.k8s.io/repositories/isv/:kubernetes/:core:/stable:/v1.31/deb Packages [4865 B]  
Fetched 6051 B in 1s (8955 B/s)  
Reading package lists... Done  
ubuntu@master-node:~$ sudo apt-get install -y kubelet kubeadm kubectl  
Reading package lists... Done
```



```
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
ubuntu@master-node:~$ sudo apt-mark hold kubelet kubeadm kubectl  
kubelet set on hold.  
kubeadm set on hold.  
kubectl set on hold.  
ubuntu@master-node:~$ kubeadm version  
kubeadm version: &version.Info{Major:"1", Minor:"31", GitVersion:"v1.31.1"  
"2024-09-11T21:26:49Z", GoVersion:"go1.22.6", Compiler:"gc", Platform:"lin  
ubuntu@master-node:~$ █
```

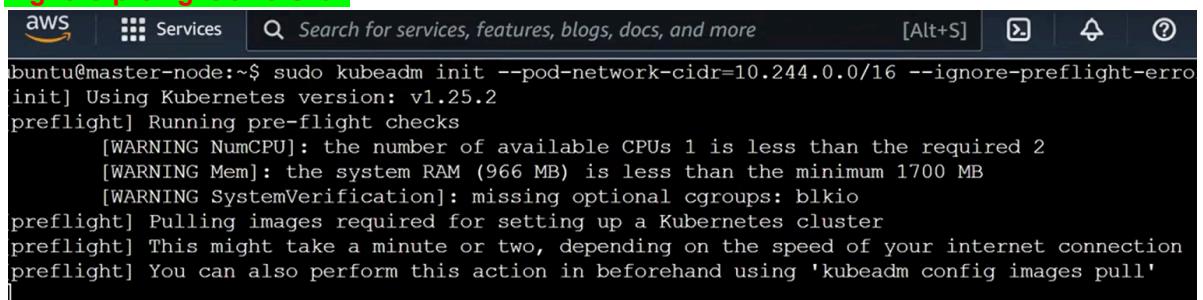
After installing Kubernetes, we need to configure internet options to allow bridging.

```
sudo swapoff -a  
echo "net.bridge.bridge-nf-call-iptables=1" | sudo tee -a /etc/sysctl.conf  
sudo sysctl -p
```

5. Perform this **ONLY** on the Master machine

Initialize the Kubecluster

```
sudo kubeadm init --pod-network-cidr=10.244.0.0/16  
--ignore-preflight-errors=all
```



```
buntu@master-node:~$ sudo kubeadm init --pod-network-cidr=10.244.0.0/16 --ignore-preflight-error  
init] Using Kubernetes version: v1.25.2  
preflight] Running pre-flight checks  
[WARNING NumCPU]: the number of available CPUs 1 is less than the required 2  
[WARNING Mem]: the system RAM (966 MB) is less than the minimum 1700 MB  
[WARNING SystemVerification]: missing optional cgroups: blkio  
preflight] Pulling images required for setting up a Kubernetes cluster  
preflight] This might take a minute or two, depending on the speed of your internet connection  
preflight] You can also perform this action in beforehand using 'kubeadm config images pull'  
█
```

Copy the join command and keep it in a notepad, we'll need it later.

Copy the mkdir and chown commands from the top and execute them

```

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

kubeadm join 172.31.37.90:6443 --token vklnbn.5al6lbt30wv4e539 \
--discovery-token-ca-cert-hash sha256:f140f2ea454a23d5fcf8ed5534de0da7a6
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) $HOME/.kube/config
ubuntu@master-node:~$ █

```

Then, add a common networking plugin called flannel file as mentioned in the code.

```

kubectl apply -f
https://raw.githubusercontent.com/coreos/flannel/master/Documentation/kube-flannel.yml

```

```

ubuntu@worker1:~$ sudo kubeadm join 172.31.37.90:6443 --token vklnbn.5al6lbt30wv4e539 --discovery-token-ca-cert-hash sha256:f140f2ea454a23d5fcf8ed5534de0da7a6330118fc9eb92a972b6ac3699a6b5c --ignore-preflight-errors=all
[preflight] Running pre-flight checks
[WARNING SystemVerification]: missing optional cgroups: blkio
[preflight] Reading configuration from the cluster...
[preflight] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
[kubelet-start] Writing kubelet configuration to file "/var/lib/kubelet/config.yaml"
[kubelet-start] Writing kubelet environment file with flags to file "/var/lib/kubelet/kubeadm-flags.env"
[kubelet-start] Starting the kubelet
[kubelet-start] Waiting for the kubelet to perform the TLS Bootstrap...
█

```

Check the created pod using this command

Now, keep a watch on all nodes using the following command

```
watch kubectl get nodes
```

6. Perform this **ONLY** on the worker machines

```

sudo kubeadm join <ip> --token <token> \
--discovery-token-ca-cert-hash <hash>

```

Now, notice the changes on the master terminal

NAME	STATUS	ROLES	AGE	VERSION
master-node	Ready	control-plane	24m	v1.25.2
worker1	Ready	<none>	100s	v1.25.2

That's it, we now have a Kubernetes cluster running across 3 AWS EC2 Instances. This cluster can be used to further deploy applications and their loads being distributed across these machines.

Conclusion:

Steps:

1. Create 2 EC2 Ubuntu Instances on AWS.

(Name 1 as Master, the 2 as worker-node)

The screenshot shows the AWS EC2 Instances "Launch an instance" success page. At the top, a green banner displays the message: "Success Successfully initiated launch of instances (i-0dbd49314505a02fb, i-0c4e36963b0f9487)". Below the banner, there is a "Launch log" link. The main area is titled "Next Steps" and contains a search bar with the placeholder "Q. What would you like to do next with these instances, for example "create alarm" or "create backup"" and a navigation menu with links 1 through 6. Four cards are displayed below:

- Create billing and free tier usage alerts**: To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds. Includes a "Create billing alerts" button.
- Connect to your instance**: Once your instance is running, log into it from your local computer. Includes a "Learn more" link.
- Connect an RDS database**: Configure the connection between an EC2 instance and a database to allow traffic flow between them. Includes a "Connect an RDS database" button, a "Create a new RDS database" link, and a "Learn more" link.
- Create EBS snapshot policy**: Create a policy that automates the creation, retention, and deletion of EBS snapshots. Includes a "Create EBS snapshot policy" button.

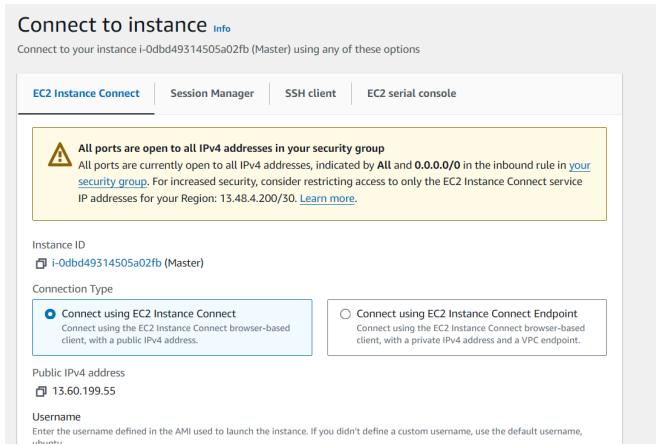
2. Edit the Security Group Inbound Rules to allow SSH

The screenshot shows the AWS Security Groups "Edit inbound rules" page. The title is "Edit inbound rules" with an "Info" link. A note below says: "Inbound rules control the incoming traffic that's allowed to reach the instance." The main table has columns: "Security group rule ID", "Type", "Protocol", "Port range", "Source", and "Description - optional". A single row is shown with the following values:

- Security group rule ID: -
- Type: All traffic
- Protocol: All
- Port range: All
- Source: Anywh...
- Description: 0.0.0.0/0

A warning message at the bottom left states: "⚠️ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only." Buttons at the bottom right include "Cancel", "Preview changes", and "Save rules".

3. Connect Instances



4. From now on, until mentioned, perform these steps on all 3 machines.

Install Docker

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

Then, configure cgroup in a daemon.json file.

cd /etc/docker
cat <<EOF | sudo tee /etc/docker/daemon.json
{
  "exec-opts": ["native.cgroupdriver=systemd"],
  "log-driver": "json-file",
  "log-opt": {
    "max-size": "100m"
  },
  "storage-driver": "overlay2"
}
EOF
sudo systemctl enable docker
sudo systemctl daemon-reload
sudo systemctl restart docker
```

```
ubuntu@ip-172-31-36-117:~$ sudo hostnamectl set-hostname master-node
ubuntu@ip-172-31-36-117:~$ exit
logout
```

```
aws | Services | Q Search
ubuntu@worker1:~$ sudo apt-get update
Hit:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates InR
Get:3 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-backports I
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 k
aws | Services | Q Search
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 ubun
Suggested packages:
  ifupdown aufs-tools cgroupfs-mount | cgroup-lite debootstrap dock
The following NEW packages will be installed:
  bridge-utils containerd dns-root-data dnsmasq-base docker.io pigz
0 upgraded, 8 newly installed, 0 to remove and 133 not upgraded.
Need to get 76.8 MB of archives.
After this operation, 289 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

```
aws | Services | Q Search
ubuntu@master-node:~$ sudo systemctl enable docker
ubuntu@master-node:~$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service;
             Active: active (running) since Sun 2024-09-15 18:07:29 UTC
     TriggeredBy: ● docker.socket
                  Docs: https://docs.docker.com
            Main PID: 3174 (dockerd)
              Tasks: 9
             Memory: 72.3M (peak: 74.3M)
                CPU: 364ms
              CGroup: /system.slice/docker.service
                        └─3174 /usr/bin/dockerd -H fd:// --containerd=/run/ct
Sep 15 18:07:29 master-node systemd[1]: Starting docker.serv
Sep 15 18:07:29 master-node dockerd[3174]: time="2024-09-15T
Sep 15 18:07:29 master-node systemd[1]: Started docker.servi
lines 1-21/21 (END)
```

```

ubuntu@master-node:~$ sudo apt-get install ca-certificates curl
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.
The following additional packages will be installed:
  libcurl3t64-gnutls libcurl4t64
The following packages will be upgraded:
  curl libcurl3t64-gnutls libcurl4t64
3 upgraded, 0 newly installed, 0 to remove and 130 not upgraded.
Need to get 900 kB of archives.
After this operation, 3072 B of additional disk space will be used.
Do you want to continue? [Y/n] Y

```

```

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@master-node:~$ sudo install -m 0755 -d /etc/apt/keyrings
ubuntu@master-node:~$ sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc
ubuntu@master-node:~$ echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] https://download.docker.com/linux/ubuntu \
> $ . /etc/os-release && echo \"$VERSION_CODENAME\" stable" | \
> sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
ubuntu@master-node:~$ sudo apt-get update
Hit:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:4 https://download.docker.com/linux/ubuntu noble InRelease [48.8 kB]
Hit:5 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:6 https://download.docker.com/linux/ubuntu noble/stable amd64 Packages [13.8 kB]
Fetched 62.6 kB in 1s (107 kB/s)
Reading package lists... Done
ubuntu@master-node:~$ 

```

```

ubuntu@master-node:~$ sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  bridge-utils dns-root-data dnsmasq-base ubuntu-fan
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  docker-ce-rootless-extras libltdl7 libslirp0 slirp4netns

```

Install Kubernetes on all 3 machines

```

curl -s
https://packages.cloud.google.com/apt/doc/apt-key.gpg |
sudo apt-key add -
cat << EOF | sudo tee
/etc/apt/sources.list.d/kubernetes.list deb
https://apt.kubernetes.io/ kubernetes-xenial main EOF
sudo apt-get update
sudo apt-get install -y kubelet kubeadm kubectl

```

```

ubuntu@master-node:~$ curl -fsSL https://pkgs.k8s.io/core:/stable:v1.31/deb/Release.key | sudo gpg --dearmor -o /etc/apt
ubuntu@master-node:~$ echo 'deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable
es.list.d/kubernetes.list
deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:v1.31/deb /
ubuntu@master-node:~$ sudo apt-get update
Hit:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 https://download.docker.com/linux/ubuntu noble InRelease
Hit:5 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:6 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:v1.31/deb InRelease [1186 B]
Get:7 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:v1.31/deb Packages [4865 B]
Fetched 6051 B in 1s (8955 B/s)
Reading package lists... Done
ubuntu@master-node:~$ sudo apt-get install -y kubelet kubeadm kubectl
Reading package lists... Done

```

```

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@master-node:~$ sudo apt-mark hold kubelet kubeadm kubectl
kubelet set on hold.
kubeadm set on hold.
kubectl set on hold.
ubuntu@master-node:~$ kubeadm version
kubeadm version: &version.Info{Major:"1", Minor:"31", GitVersion:"v1.31.1"
"2024-09-11T21:26:49Z", GoVersion:"go1.22.6", Compiler:"gc", Platform:"lin
ubuntu@master-node:~$ 

```

After installing Kubernetes, we need to configure internet options to allow bridging.

```

sudo swapoff -a
echo "net.bridge.bridge-nf-call-iptables=1" | sudo tee -a
/etc/sysctl.conf sudo sysctl -p

```

5. Perform this **ONLY on the Master machine**

Initialize the Kubecluster

```

sudo kubeadm init --pod-network-cidr=10.244.0.0/16
--ignore-preflight-errors=all

```

```

ubuntu@master-node:~$ sudo kubeadm init --pod-network-cidr=10.244.0.0/16 --ignore-preflight-erro
init] Using Kubernetes version: v1.25.2
preflight] Running pre-flight checks
    [WARNING NumCPU]: the number of available CPUs 1 is less than the required 2
    [WARNING Mem]: the system RAM (966 MB) is less than the minimum 1700 MB
    [WARNING SystemVerification]: missing optional cgroups: blkio
preflight] Pulling images required for setting up a Kubernetes cluster
preflight] This might take a minute or two, depending on the speed of your internet connection
preflight] You can also perform this action in beforehand using 'kubeadm config images pull'

```

Copy the join command and keep it in a notepad, we'll need it later.

Copy the mkdir and chown commands from the top and execute them

```

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

kubeadm join 172.31.37.90:6443 --token vk1nbn.5a16lbt30wv4e539 \
    --discovery-token-ca-cert-hash sha256:f140f2ea454a23d5fcf8ed5534de0da7a6
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) $HOME/.kube/config
ubuntu@master-node:~$ 

```

Then, add a common networking plugin called flannel file as mentioned in the code.

```

kubectl apply -f
https://raw.githubusercontent.com/coreos/flannel/master/Dокументation/kube-flannel.yml

```

```

aws | Services | Search for services, features, blogs, docs, and more [Alt+S] | 
ubuntu@worker1:~$ sudo kubeadm join 172.31.37.90:6443 --token vk1nbn.5a16lbt30wv4e539 --discovery-token-ca-ce
a23d5fcf8ed5534de0da7a6330118fc9eb92a972b6ac3699a6b5c --ignore-preflight-errors=all
[preflight] Running pre-flight checks
[WARNING SystemVerification]: missing optional cgroups: blkio
[preflight] Reading configuration from the cluster...
[preflight] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
[kubelet-start] Writing kubelet configuration to file "/var/lib/kubelet/config.yaml"
[kubelet-start] Writing kubelet environment file with flags to file "/var/lib/kubelet/kubeadm-flags.env"
[kubelet-start] Starting the kubelet
[kubelet-start] Waiting for the kubelet to perform the TLS Bootstrap...

```

Check the created pod using this command

Now, keep a watch on all nodes using the following command

```
watch kubectl get nodes
```

6. Perform this **ONLY** on the worker machines

```
sudo kubeadm join <ip> --token <token> \
    --discovery-token-ca-cert-hash <hash>
```

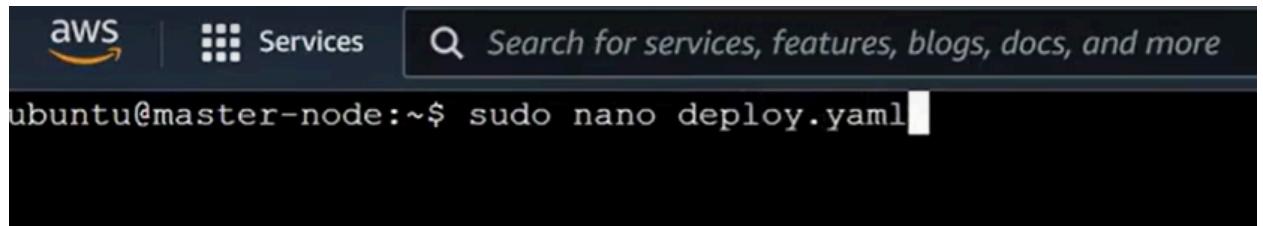
Now, notice the changes on the master terminal

NAME	STATUS	ROLES	AGE	VERSION
master-node	Ready	control-plane	24m	v1.25.2
worker1	Ready	<none>	100s	v1.25.2

That's it, we now have a Kubernetes cluster running across 3 AWS EC2 Instances. This cluster can be used to further deploy applications and their loads being distributed across these machines.

7. Now that the cluster is up and running, we can deploy our nginx server on this cluster. Apply this deployment file using this command to create a deployment

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

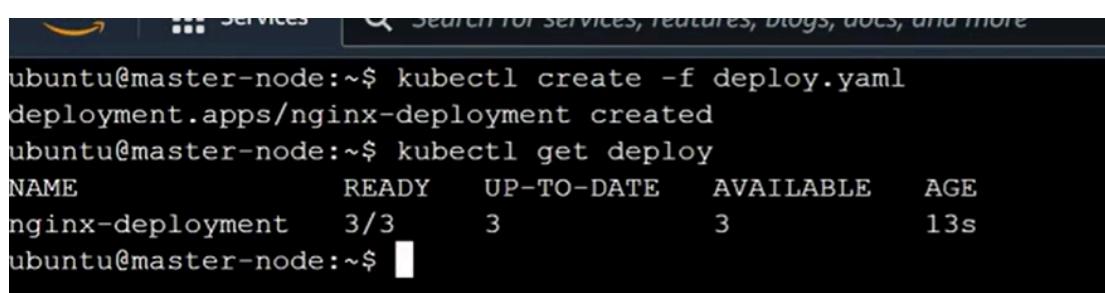


A screenshot of a terminal window showing the "GNU nano 6.2" editor. The file content is a YAML configuration for a deployment:

```
- name: nginx  
  image: nginx:1.14.2  
  ports:  
    - containerPort: 80
```

The terminal also shows the standard nano editor key bindings at the bottom:

^G Help ^O Write Out ^W Where Is ^K Cut ^T Exec
^X Exit ^R Read File ^\ Replace ^U Paste ^J Just



Use ‘kubectl get pods’ to verify if the deployment was properly created and the pod is working correctly.

Next up, create a name alias for this pod.

```
POD_NAME=$(kubectl get pods -l app=nginx -o jsonpath=".items[0].metadata.name")
```

8. Lastly, port forward the deployment to your localhost so that you can

```
view it. kubectl port-forward $POD_NAME 8080:80
```

```
ubuntu@master-node:~$ kubectl expose deployment.apps/nginx-deployment --type="LoadBalancer"
service/nginx-deployment exposed
ubuntu@master-node:~$ kubectl get svc
NAME           TYPE      CLUSTER-IP   EXTERNAL-IP   PORT(S)        AGE
kubernetes     ClusterIP  10.96.0.1    <none>        443/TCP       50m
nginx-deployment LoadBalancer 10.111.72.92  <pending>    80:31642/TCP  13s
ubuntu@master-node:~$ █
```

9. Verify your deployment

Open up a new terminal and ssh to your EC2 instance.

Then, use this curl command to check if the Nginx server is running.

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

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

If the response is 200 OK and you can see the Nginx server name, your deployment was successful.

We have successfully deployed our Nginx server on our EC2 instance.

Conclusion:

ADVDEVOPS EXP 5

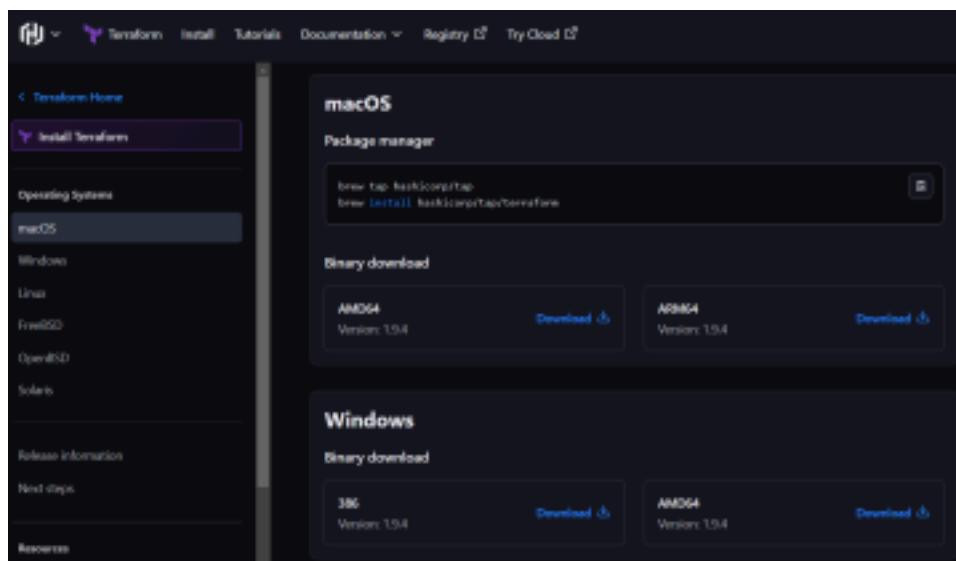
A) Installation and Configuration of Terraform in Windows

Step 1: Download terraform

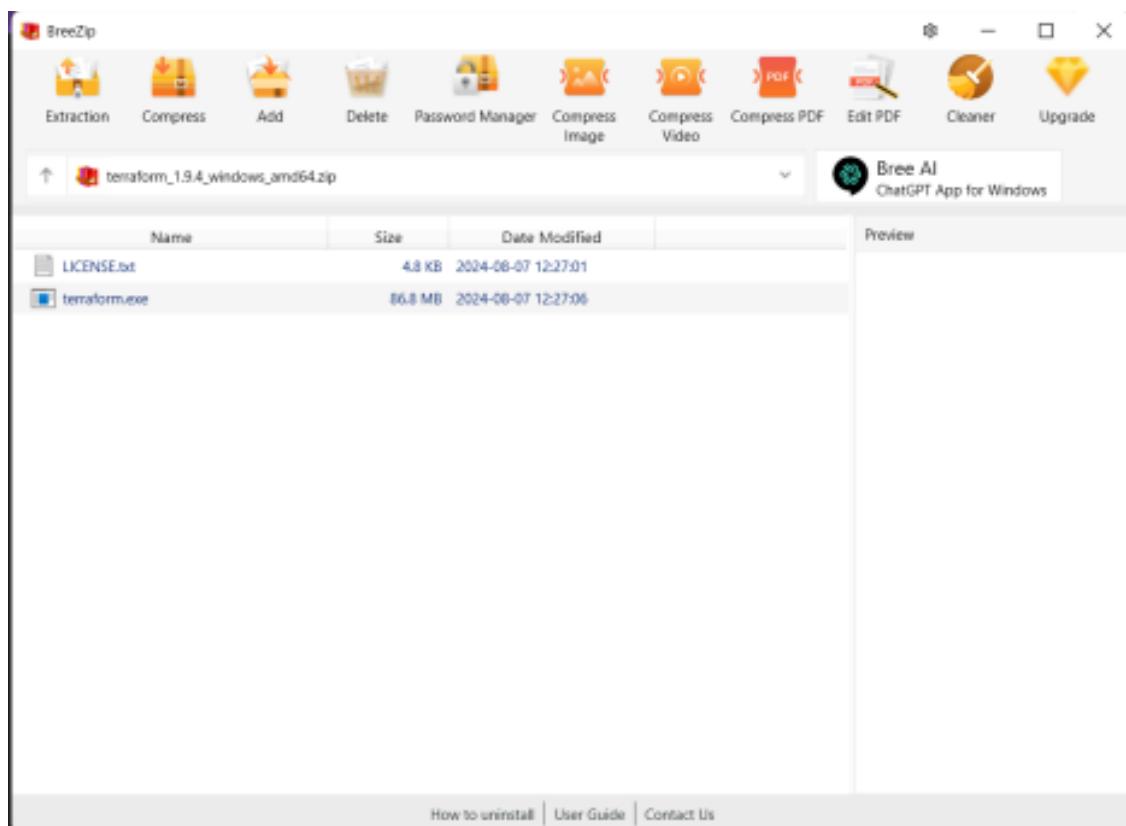
To install Terraform, First Download the Terraform Cli Utility for windows from terraforms official website

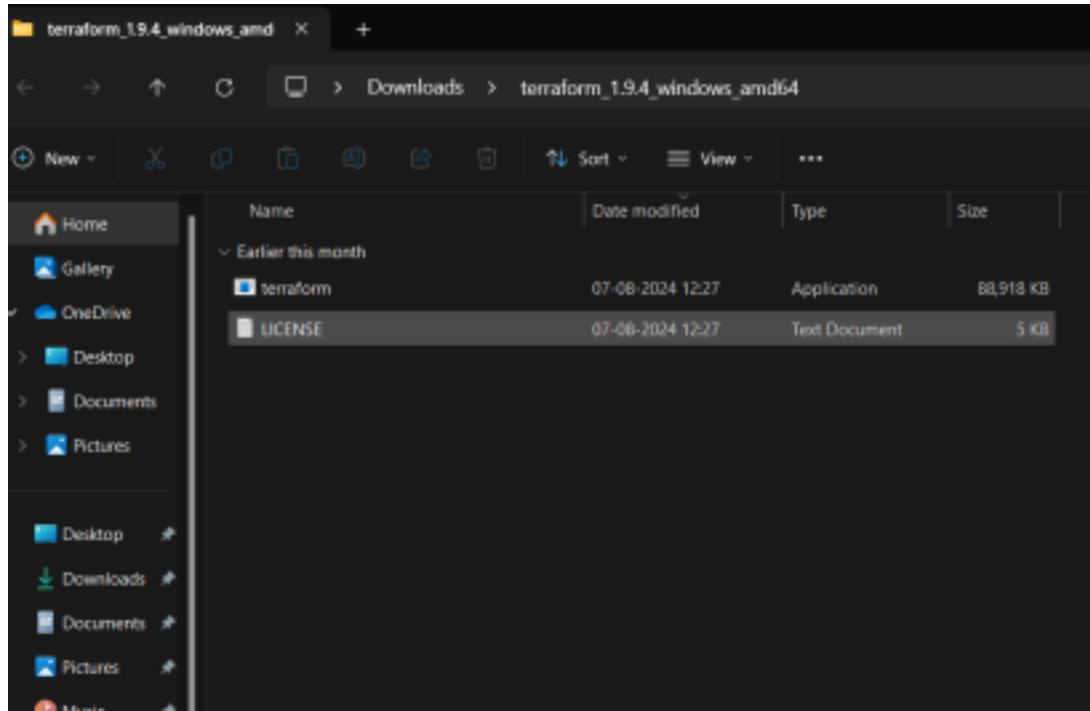
website:<https://www.terraform.io/downloads.html>

Select the Operating System Windows followed by either 32bit or 64 bit based on your OS type.

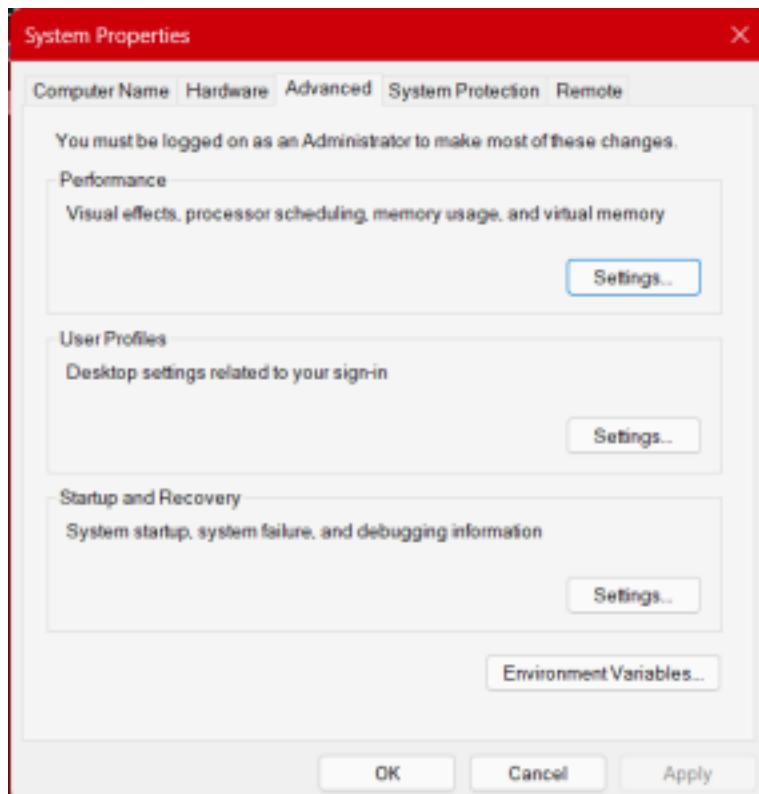


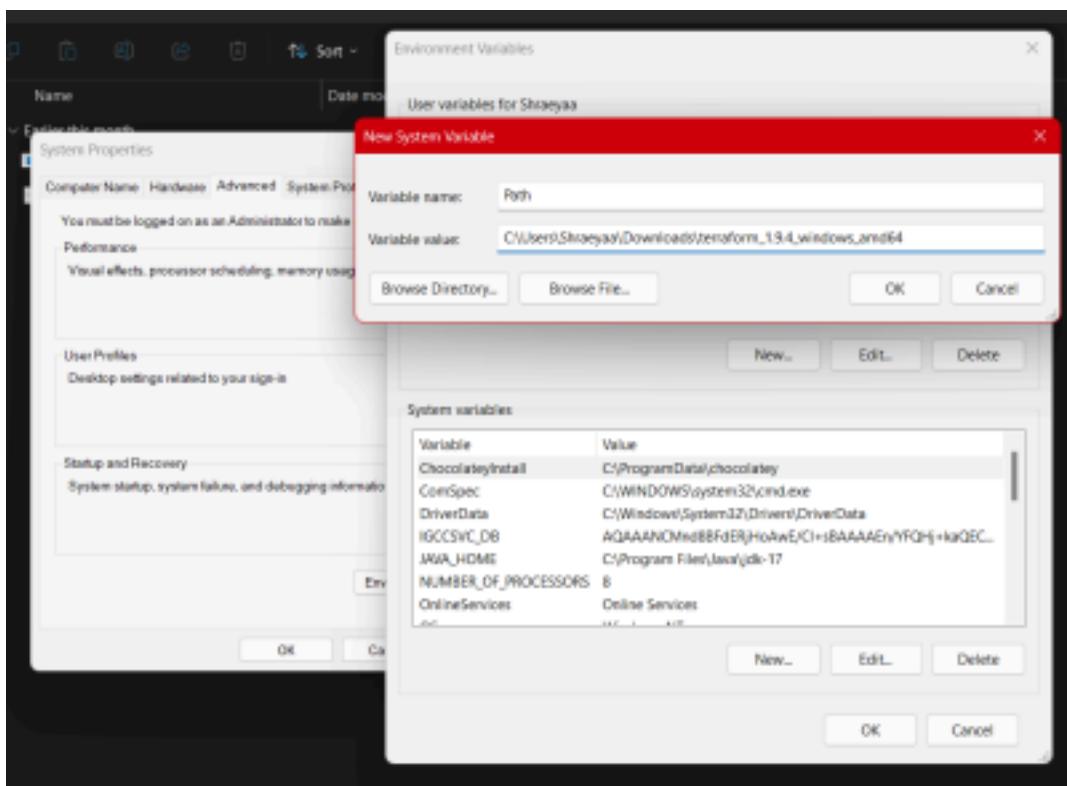
Step 2: Extract the downloaded setup file Terraform.exe in C:\Terraform directory





Step 3: Set the System path for Terraform in Environment Variables





System variables

Variable	Value
IGCCSVC_DB	AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAEn/YFQHj+kaQEC...
JAVA_HOME	C:\Program Files\Java\jdk-17
NUMBER_OF_PROCESSORS	8
OnlineServices	Online Services
OS	Windows_NT
Path	C:\Users\Shraeyaa\Downloads\terraform_1.9.4_windows_amd...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.PY;.PYW

New...

Edit...

Delete

OK

Cancel

Step 4:: Open Terraform in PowerShell and check its functionality

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

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

PS C:\Users\Shraeyaa> terraform
Usage: terraform [global options] <subcommand> [args]

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

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

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

Global options (use these before the subcommand, if any):
```

ADVANCE DEVOPS EXP 6

Docker Installation:

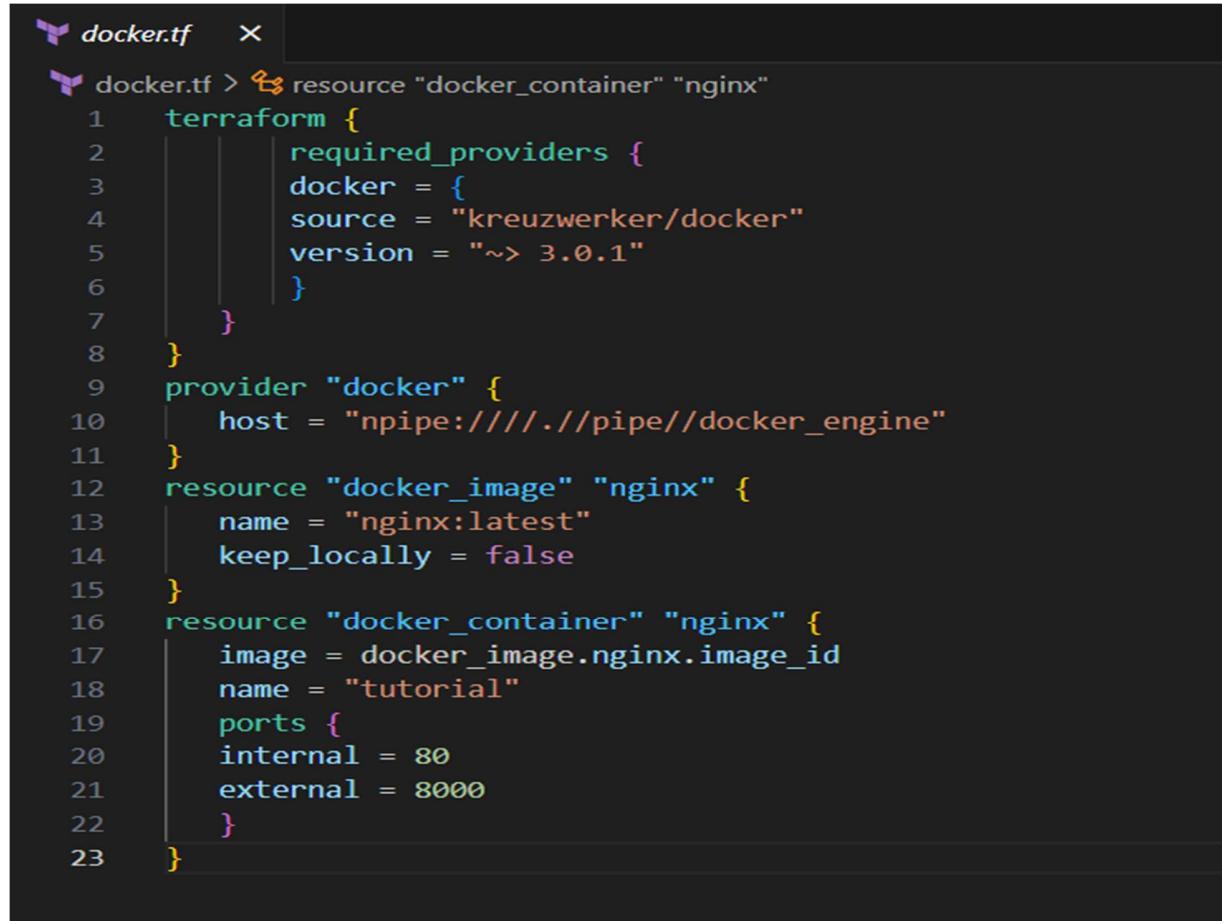
```
PS C:\Users\Shraeyaa> docker --version
Docker version 27.1.1, build 6312585
PS C:\Users\Shraeyaa>
```

Before using terraform commands:

```
C:\Terraform scripts\Docker>docker images
REPOSITORY      TAG      IMAGE ID      CREATED      SIZE
react-img       latest   5f0b23d1bdea  2 weeks ago   320MB
<none>          <none>  3bd8656788a8  2 weeks ago   320MB
```

```
C:\Terraform scripts\Docker>docker container list
CONTAINER ID      IMAGE      COMMAND      CREATED      STATUS      PORTS      NAMES
C:\Terraform scripts\Docker>
```

Code:



```
docker.tf  X
docker.tf >  resource "docker_container" "nginx"
1   terraform {
2     required_providers {
3       docker = {
4         source = "kreuzwerker/docker"
5         version = "~> 3.0.1"
6       }
7     }
8   }
9   provider "docker" {
10    host = "npipe://./pipe/docker_engine"
11  }
12  resource "docker_image" "nginx" {
13    name = "nginx:latest"
14    keep_locally = false
15  }
16  resource "docker_container" "nginx" {
17    image = docker_image.nginx.image_id
18    name = "tutorial"
19    ports {
20      internal = 80
21      external = 8000
22    }
23 }
```

Terraform Commands:

- PS C:\Terraform scripts\ Docker> **terraform init**
Initializing the backend...
Initializing provider plugins...
 - Finding kreuzwerker/docker versions matching "~> 3.0.1"...
 - Installing kreuzwerker/docker v3.0.2...
 - Installed kreuzwerker/docker v3.0.2 (self-signed, key ID BD080C4571C6104C)
Partner and community providers are signed by their developers.
If you'd like to know more about provider signing, you can read about it here:
<https://www.terraform.io/docs/cli/plugins/signing.html>Terraform has created a lock file **.terraform.lock.hcl** to record the provider selections it made above. Include this file in your version control repository so that Terraform can guarantee to make the same selections by default when you run "terraform init" in the future.
- Terraform has been successfully initialized!**

- PS C:\Terraform scripts\ Docker> **terraform** plan

```
Terraform used the selected providers to generate the following execution plan. Resources: + create
```

Terraform will perform the following actions:

```
# docker_container.nginx will be created
+ resource "docker_container" "nginx" {
    + attach = false
    + bridge = (known after apply)
    + command = (known after apply)
    + container_logs = (known after apply)
    + container_read_refresh_timeout_milliseconds = 15000
    + entrypoint = (known after apply)
    + env = (known after apply)
    + exit_code = (known after apply)
    + hostname = (known after apply)
    + id = (known after apply)
```

- PS C:\Terraform scripts\ Docker> **terraform** apply

```
Terraform used the selected providers to generate the following execution plan. Resources: + create
```

Terraform will perform the following actions:

```
# docker_container.nginx will be created
+ resource "docker_container" "nginx" {
    + attach = false
    + bridge = (known after apply)
    + command = (known after apply)
    + container_logs = (known after apply)
    + container_read_refresh_timeout_milliseconds = 15000
```

Enter a value: yes

```
docker_image.nginx: Creating...
docker_image.nginx: Still creating... [10s elapsed]
docker_image.nginx: Still creating... [20s elapsed]
docker_image.nginx: Still creating... [30s elapsed]
docker_image.nginx: Creation complete after 38s [id=sha256:5ef79149e0ec84a7a9f9284c3f91aa3c20608f8391f5445eabe92ef07dbda0]
docker_container.nginx: Creating...
docker_container.nginx: Creation complete after 1s [id=19c3b26e694e3b26a5daa18288d68c790f0168d547f94171a49e3491bd173ae9]
```

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

- PS C:\Terraform scripts\ Docker>

After using Terraform commands:

```
C:\Terraform scripts\ Docker> docker images
REPOSITORY      TAG      IMAGE ID      CREATED      SIZE
nginx           latest   5ef79149e0ec  12 days ago  188MB
react-img       latest   5f0b23d1bdea  2 weeks ago  320MB
<none>          <none>   3bd8656788a8  2 weeks ago  320MB
```

```
C:\Terraform scripts\docker> docker container list
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS               NAMES
19c3b26e694e        5ef79149e0ec   "/docker-entrypoint..."   2 minutes ago    Up About a minute   0.0.0.0:8000->80/tcp   tutorial

C:\Terraform scripts\docker>
```

To Delete the Containers created:

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

Prerequisites:

1) Docker

Run docker -v command.

Use this command to check if docker is installed and running on your system.

```
C:\Users\Shraeyaa>docker -v  
Docker version 27.1.1, build 6312585
```

2) Install SonarQube image Command: docker pull sonarqube

This command helps you to install an image of SonarQube that can be used on the local system without actually installing the SonarQube installer.

```
C:\Users\Shraeyaa>docker pull sonarqube  
Using default tag: latest  
What's next:  
View a summary of image vulnerabilities and recommendations → docker scout quickview sonarqube  
error during connect: Post "http://%2F%2F.pipe%2FdockerDesktopLinuxEngine/v1.46/images/create?fromImage=sonarqube&tag=latest": open //./pipe/dockerDeskt  
pLinuxEngine: The system cannot find the file specified.  
C:\Users\Shraeyaa>
```

3) Keep jenkins installed on your system.

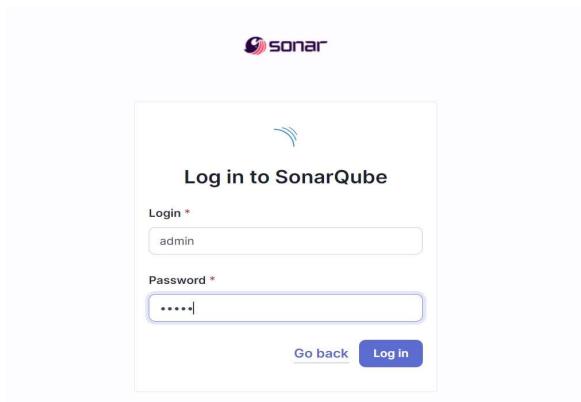
Experiment Steps:

1. Run SonarQube in a Docker container using this command docker run -d --name sonarqube -e

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

```
C:\Users\Shraeyaa>docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest  
4be9b2af1602f07d33c1e6f4fbcc35a8f70386b231a43669a03e4e134b355058  
C:\Users\Shraeyaa>
```

2. Once the container is up and running, you can check the status of SonarQube at localhost port 9000.
3. Login to SonarQube using username admin and password admin.



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

To view your password or add a note about it, click the key icon

How do you want to create your project?

Do you want to benefit from all of SonarQube's features (like repository import and Pull Request decoration)? Create your project from your favorite DevOps platform.

First, you need to set up a DevOps platform configuration.

Import from Azure DevOps Import from Bitbucket Cloud Import from Bitbucket Server

Import from GitHub Import from GitLab

Create a local project

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

Click on Create a Local Project.

1 of 2

Create a local project

Project display name *

project

Project key *

project

Main branch name *

main

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

Cancel

Next

Set up the project as required and click on create.

2 of 2

Set up project for Clean as You Code

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

Choose the baseline for new code for this project

Use the global setting

Previous version

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

Recommended for projects following regular versions or releases.

Define a specific setting for this project

Previous version

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

Recommended for projects following regular versions or releases.

Number of days

Any code that has changed in the last x days is considered new code. If no action code.

Recommended for projects following continuous delivery.

5. Open Jenkins on whichever port it is installed. (<http://localhost:<port number>>).

6. Go to Manage Jenkins → Plugins → Available Plugins

Search for Sonarqube Scanner for Jenkins and install it.

The screenshot shows the Jenkins 'Available Plugins' page. A search bar at the top contains the text 'sonarqub'. Below the search bar, there are two buttons: 'Install' (highlighted in blue) and a refresh icon. The main table lists available plugins. The 'SonarQube Scanner' plugin is selected for installation, indicated by a checked checkbox in its row. Other visible plugins include 'Sonar Gerrit' and 'SonarQube Generic Coverage'. The table includes columns for 'Install' (checkbox), 'Name' (sorted by name), and 'Released' (date). The 'SonarQube Scanner' plugin was released 7 months and 15 days ago.

Install	Name ↓	Released
<input checked="" type="checkbox"/>	SonarQube Scanner 2.17.2 External Site/Tool Integrations Build Reports This plugin allows an easy integration of SonarQube, the open source platform for Continuous Inspection of code quality.	7 mo 15 days ago
<input type="checkbox"/>	Sonar Gerrit 388.v9b_f1cb_e42306 External Site/Tool Integrations This plugin allows to submit issues from SonarQube to Gerrit as comments directly.	3 mo 29 days ago
<input type="checkbox"/>	SonarQube Generic Coverage 1.0 TODO	5 yr 2 mo ago

- Under Jenkins 'Configure System', look for SonarQube Servers and enter the details.
I have named the server 'sonarqube' and added the server url for jenkins.
Enter the Server Authentication token if needed.

SonarQube installations

List of SonarQube installations

Name
project

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

Server authentication token
SonarQube authentication token. Mandatory when anonymous access is disabled.
- none -
+ Add ▾

Advanced ▾

- Search for SonarQube Scanner under Global Tool Configuration. Choose the latest configuration and choose Install automatically.

Add SonarQube Scanner

≡ SonarQube Scanner

Name
project

Install automatically ?

≡ Install from Maven Central

Version
SonarQube Scanner 6.2.1.4610

Add Installer ▾

Add SonarQube Scanner

- After configuration, create a New Item → choose a freestyle project and name your project. Here, I have given the 'sonarqube', then click on OK.

New Item

Enter an item name

project

Select an item type



Freestyle project

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



Maven project

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



Pipeline

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



Multi-configuration project

Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.

10. Choose the github repository https://github.com/shazforiot/MSBuild_firstproject. It is a sample hello-world project with no vulnerabilities and issues, just to test the integration.
Fork this repository.

The screenshot shows the GitHub repository page for 'MSBuild_firstproject' (Public). The repository was forked from 'shazforiot/MSBuild_firstproject'. The master branch is up-to-date with the upstream master branch. The repository contains 1 branch and 0 tags. The commit history shows updates from 'shazforiot' 4 years ago. The README file is present. The repository has 0 stars, 0 forks, and 0 releases. There are no packages published.

Code Pull requests Actions Projects Wiki Security Insights Settings

MSBuild_firstproject (Public)
forked from shazforiot/MSBuild_firstproject

master 1 Branch 0 Tags Go to file Add file Code

This branch is up to date with shazforiot/MSBuild_firstproject:master . Contribute Sync fork

shazforiot updated f2bc042 · 4 years ago 4 Commits

.vs/Firstproject Deleted 4 years ago

HelloWorldCore updated 4 years ago

HelloWorldTests updated 4 years ago

HelloWorldCore.sln updated 4 years ago

README

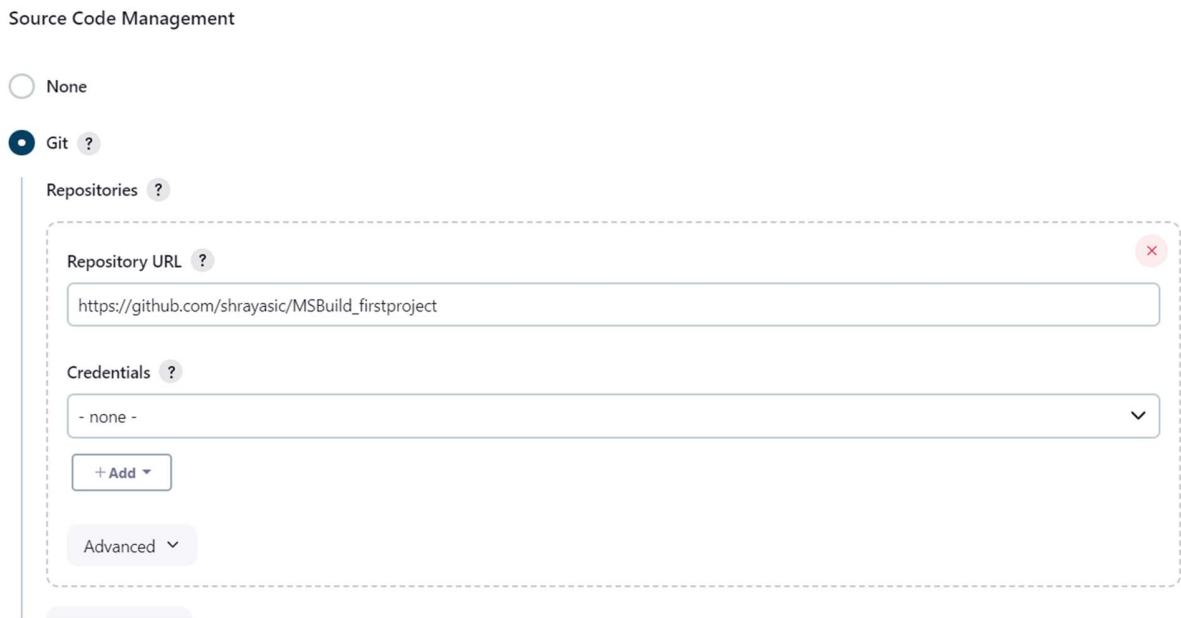
No description, website, or topics provided.

Activity 0 stars 0 watching 0 forks

Releases No releases published Create a new release

Packages No packages published Publish your first package

11. Enable git and add the repository you forked.



12. Under Build Steps, select Execute Sonarqube Scanner, enter these Analysis properties. Mention the SonarQube Project Key, Login, Password, Source path and Host URL.



13. Then click on save. Go to http://localhost:9000/<user_name>/permissions and allow Execute Permissions to the Admin user.

The screenshot shows the SonarQube Administration interface under the Security tab. It lists four groups: 'sonar-administrators', 'sonar-users', 'Anyone DEPRECATED', and 'Administrator admin'. The 'Administrator admin' group is selected. The 'Administrator' column has a checked checkbox. The 'Execute Analysis' column has an unchecked checkbox. The 'Create' column has a checked checkbox. The 'Projects' column has a checked checkbox. A search bar at the top right says 'Search for users or groups...'.

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

4 of 4 shown

14. Go back to jenkins. Go to the job you had just built and click on Build Now.

The screenshot shows a Jenkins project configuration page for 'project'. It includes a sidebar with options like Status, Changes, Workspace, Build Now, Configure, Delete Project, SonarQube, and Rename. Below the sidebar is a 'Permalinks' section with a SonarQube icon and the text 'SonarQube'. At the bottom is a 'Build History' section with a sun icon, a dropdown menu set to 'trend', a 'Filter...' input field, a build number '#1' with a checkmark, a date 'Oct 2, 2024, 1:30 AM', and links for 'Atom feed for all' and 'Atom feed for failures'.

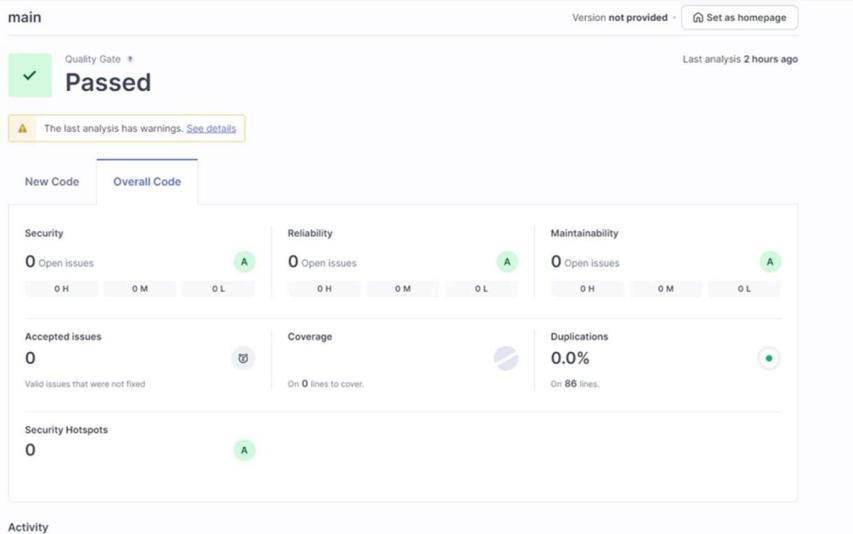
15. Check the console Output.

```
Dashboard > project > #1 > Console Output

01:33:31.504 INFO Sensor Analysis Warnings Import [csharp]
01:33:31.506 INFO Sensor Analysis Warnings Import [csharp] (done) | time~2ms
01:33:31.506 INFO Sensor CM File Caching Sensor [csharp]
01:33:31.507 WARN Incremental PR analysis: Could not determine common base path, cache will not be computed. Consider setting 'sonar.projectBaseDir' property.
01:33:31.507 INFO Sensor CM File Caching Sensor [csharp] (done) | time=1ms
01:33:31.508 INFO Sensor CM File Caching Sensor [csharp]
01:33:31.509 INFO Sensor Code Coverage Sensor (done) | time~20ms
01:33:31.511 INFO SCM Publisher SCM provider for this project is: git
01:33:31.516 INFO SCM Publisher 4 source files to be analyzed
01:33:32.201 INFO SCM Publisher A/A source files have been analyzed (done) | time~760ms
01:33:32.207 INFO CPD Executor Calculating CPD for 0 files
01:33:32.208 INFO CPD Executor CPD calculation finished (done) | time~0ms
01:33:32.521 INFO SCM revision ID: "7fb0d2e0bdcf2a27c7c8080acecd6fec7b7b0df"
01:33:32.812 INFO Analysis report generated in 217ms, dir size=201.0 kB
01:33:32.912 INFO Analysis report uploaded in 98ms, zip size=22.3 kB
01:33:32.913 INFO Analysis report uploaded in 98ms
01:33:32.914 INFO ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=project
01:33:33.608 INFO Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
01:33:33.609 INFO More about the report processing at http://localhost:9000/api/cr/task?id=790d66d-1d66-9937-c70520af12a
01:33:33.627 INFO Analysis total time: 56.745 s
01:33:33.629 INFO SonarScanner Engine completed successfully
01:33:33.760 INFO EXECUTION SUCCESS
01:33:33.833 INFO Total time: 1:35.284s
Finished: SUCCESS
```

REST API Jenkins 2.46.2

16. Once the build is complete, go back to SonarQube and check the project linked.



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

Prerequisites:

1) Docker

Run docker -v command.

Use this command to check if docker is installed and running on your system.

```
C:\Users\Shraeyaa>docker -v
Docker version 27.1.1, build 6312585
```

2) Install SonarQube image Command: docker pull sonarqube

This command helps you to install an image of SonarQube that can be used on the local system without actually installing the SonarQube installer.

```
C:\Users\Shraeyaa>docker pull sonarqube
Using default tag: latest
What's next:
  View a summary of image vulnerabilities and recommendations → docker scout quickview sonarqube
error during connect: Post "http://%2F%2FdockerDesktopLinuxEngine/v1.46/images/create?fromImage=sonarqube&tag=latest": open //./pipe/dockerDesktopLinuxEngine: The system cannot find the file specified.
C:\Users\Shraeyaa>
```

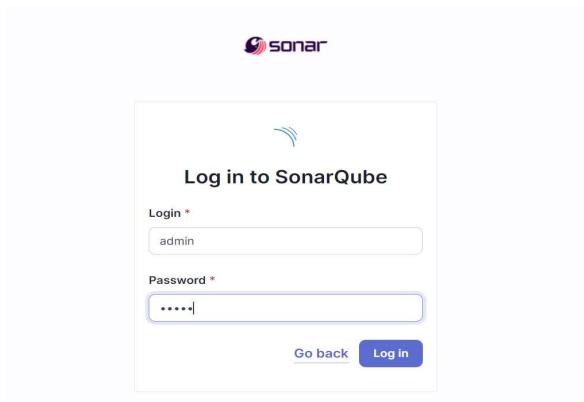
3) Keep jenkins installed on your system.

Experiment Steps:

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

```
C:\Users\Shraeyaa>docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
4be9b2af1602f07d33c1e6f4fbcc35a8f70386b231a43669a03e4e134b355058
C:\Users\Shraeyaa>
```

2. Once the container is up and running, you can check the status of SonarQube at localhost port 9000.
3. Login to SonarQube using username admin and password admin.



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

To view your password or add a note about it, click the key icon

How do you want to create your project?

Do you want to benefit from all of SonarQube's features (like repository import and Pull Request decoration)? Create your project from your favorite DevOps platform.

First, you need to set up a DevOps platform configuration.

Import from Azure DevOps Import from Bitbucket Cloud Import from Bitbucket Server

Import from GitHub Import from GitLab

Create a local project

Are you just testing or have an advanced use-case? Create a local project.

Create a local project

Click on **Create a Local Project.**

1 of 2

Create a local project

Project display name *

 ✓

Project key *

 ✓

Main branch name *

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

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

Set up the project as required and click on create.

2 of 2

Set up project for Clean as You Code

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

Choose the baseline for new code for this project

Use the global setting

[Previous version](#)

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

Recommended for projects following regular versions or releases.

Define a specific setting for this project

Previous version

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

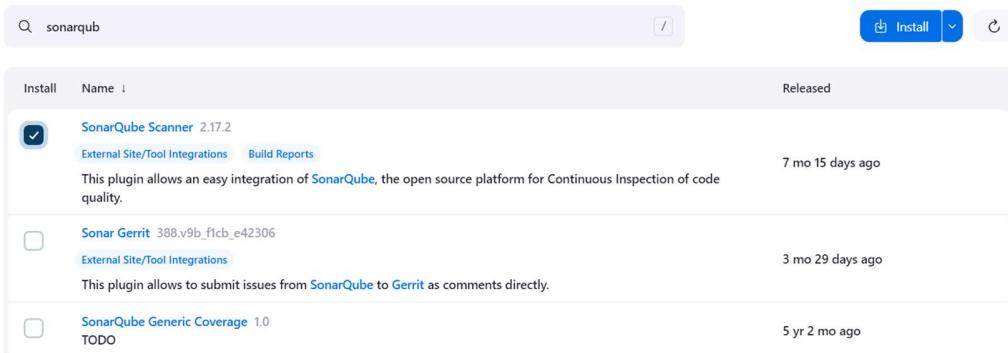
Recommended for projects following regular versions or releases.

Number of days

Any code that has changed in the last x days is considered new code. If no action code.

Recommended for projects following continuous delivery.

5. Open Jenkins on whichever port it is installed. (<http://localhost:<port number>>).
6. Go to Manage Jenkins → Plugins → Available Plugins
Search for Sonarqube Scanner for Jenkins and install it.



7. Under Jenkins 'Configure System', look for SonarQube Servers and enter the details. I have named the server 'sonarqube' and added the server url for jenkins. Enter the Server Authentication token if needed.

Dashboard > Manage Jenkins > System >

Name
raeqube

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

Server authentication token
SonarQube authentication token. Mandatory when anonymous access is disabled.
- none -
+ Add +

Advanced

Add SonarQube

8. Search for SonarQube Scanner under Global Tool Configuration. Choose the latest configuration and choose Install automatically.

SonarQube Scanner

Name
raeqube

Install automatically

Install from Maven Central

Version
SonarQube Scanner 6.2.1.4610

Add Installer

Add SonarQube Scanner

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

New Item

Enter an item name
raeqube

Select an item type

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

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

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

10.Under Pipeline script, enter the following:

The screenshot shows a pipeline configuration interface. At the top, it says "Pipeline" and "Definition". Below that is a "Pipeline script" section containing the following Groovy code:

```
1 > node {  
2 > stage('Cloning the GitHub Repo') {  
3 > git 'https://github.com/shazforiot/GOL.git'  
4 > }  
5 > stage('SonarQube analysis') {  
6 > withSonarQubeEnv('raeqube'){  
7 > bat ""  
8 > "C:\\\\Users\\\\Shraeaya\\\\Downloads\\\\sonar-scanner-cli-6.2.0.4584-windows-x64\\\\sonar-scanner-6.2.0.4584-windows-x64\\\\bin\\\\sonar-scanner.bat" ^  
9 > -D sonar.login=squ_f39eb556eb18a136706b797d46ea1271f4a03d2d ^  
10 > -D sonar.projectKey=raeqube ^  
11 > -D sonar.exclusions=vendor/**,resources/**,java ^  
12 > -D sonar.host.url=http://localhost:9000/  
13 > ""  
14 > }  
15 > }  
16 > }
```

There is a "try sample Pipeline..." button next to the code editor. Below the code editor is a checkbox labeled "Use Groovy Sandbox". At the bottom are "Save" and "Apply" buttons.

11. Go to the job you had just built and click on Build Now.

The screenshot shows a Jenkins job summary page for "raeqube #1". The top navigation bar includes "Dashboard", "raeqube", and "#1". The main content area has a "Status" tab selected, showing "Build #1 (Oct 2, 2024, 2:14:15 AM)" with a green checkmark icon. Other tabs include "Changes", "Console Output", "Edit Build Information", "Delete build '#1'", "Timings", "Git Build Data", "Pipeline Overview", "Pipeline Console", and "Replay".

On the right side, there is a summary of the build's duration and a "git" section showing revision information:

- Started by anonymous user
- This run spent:
 - 98 ms waiting;
 - 18 min build duration;
 - 18 min total from scheduled to completion.
- Revision: ba799ba7e1b576f04a4612322b0412c5e6e1e5e4
- Repository: <https://github.com/shazforiot/GOL.git>
- refs/remotes/origin/master

12.Once it is built, check the console output.

Dashboard > raeguide > #1

Console Output

Scanning 4750 KB. Full Log

```

02:18:40.253 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/report/writer/ReportSummary.html For block at line 17. keep only the first 100 references.
02:18:40.353 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/report/writer/ReportSummary.html For block at line 303. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 32. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 115. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 640. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 653. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 651. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 17. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 122. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 123. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 655. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 655. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 155. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 153. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 92. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 92. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 87. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 86. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 86. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 65. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 64. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 40. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 41. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 17. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 18. keep only the first 100 references.
02:18:40.453 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/math/StatCalculator.html For block at line 74. keep only the first 100 references.
02:18:40.523 WARN Too many duplication references on file gameoflife-web/tools/jmeter/control/gui/package-tree.html For block at line 20. keep only the first 100 references.
02:18:40.523 WARN Too many duplication references on file gameoflife-web/tools/jmeter/control/gui/package-tree.html For block at line 16. keep only the first 100 references.

```

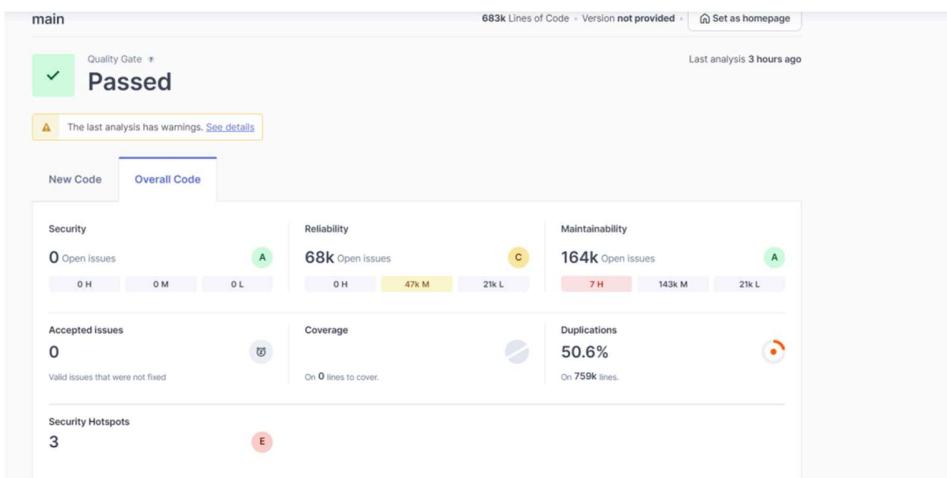
the first 100 references.

```

02:18:51.352 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/ldap/ctl/ldapExtTestSamplerGui.html For block at line 520. Keep only the first 100 references.
02:18:51.352 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/ldap/ctl/ldapExtTestSamplerGui.html For block at line 519. Keep only the first 100 references.
02:18:51.352 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/ldap/ctl/ldapExtTestSamplerGui.html For block at line 155. Keep only the first 100 references.
02:18:51.352 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/ldap/ctl/ldapExtTestSamplerGui.html For block at line 155. Keep only the first 100 references.
02:18:51.352 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/ldap/ctl/ldapExtTestSamplerGui.html For block at line 155. Keep only the first 100 references.
02:18:51.352 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/ldap/ctl/ldapExtTestSamplerGui.html For block at line 768. Keep only the first 100 references.
02:18:51.352 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/ldap/ctl/ldapExtTestSamplerGui.html For block at line 714. Keep only the first 100 references.
02:18:51.352 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/ldap/ctl/ldapExtTestSamplerGui.html For block at line 688. Keep only the first 100 references.
02:18:51.355 INFO CRD Factorizer CRD calculation finished (done) | time=20773ms
02:18:51.355 INFO SOT revision ID "be799be7e137f04a44232208412c5e5e1e4"
02:18:51.409 INFO Analysis report generated in 584ms, dir size=127.2 kB
02:18:51.409 INFO Analysis report compressed in 2433ms, zip size=29.1 MB
02:18:06.151 INFO Analysis report uploaded in 91ms
02:18:05.134 INFO ANALYSIS SUCCESSFUL, you can find the results at http://localhost:9000/dashboard
02:18:06.134 INFO Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
02:18:06.134 INFO More about the report processing at http://localhost:9000/api/cx/task?tid=f559c449-f557-479f-87b0-2d63da4dc028
02:18:23.529 INFO Analysis total time: 17:47:332 s
02:18:24.321 INFO SonarScanner Engine completed successfully
02:18:24.321 INFO EXECUTION SUCCESS
02:18:24.321 INFO EXECUTION SUCCESS
[Pipeline] End of Pipeline
Finished: SUCCESS

```

13. Once the build is complete, go back to SonarQube and check the project linked.



Installation of Nagios

Prerequisites: AWS Free Tier

Steps:

1. Create an Amazon Linux EC2 Instance in AWS and name it - nagios-host

The screenshot shows the AWS CloudWatch Instances console. At the top, there's a search bar and a 'Find Instance by attribute or tag (case-sensitive)' input field. Below the search bar are buttons for 'Connect', 'Instance state ▾', 'Actions ▾', and a yellow 'Launch instances' button. A navigation bar at the bottom includes icons for back, forward, and refresh, along with a 'Launch instances' button.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IP
nagios-host	i-08dda25e9ecd71ba0	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b	ec2-35-174-12-134.co...	35.174.1...

2. Under Security Group, make sure HTTP, HTTPS, SSH, ICMP are open from everywhere.

The screenshot shows the AWS CloudWatch Security Groups console. At the top, there's a search bar and a 'Search' input field. Below the search bar are buttons for 'Manage tags' and 'Edit inbound rules'. A navigation bar at the bottom includes icons for back, forward, and refresh, along with a 'Edit inbound rules' button.

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
-	sgr-0b6217a1e4c6e6d...	IPv4	SSH	TCP	22	0.0.0.0/0
-	sgr-03235f110ad0bec4b	IPv6	HTTP	TCP	80	::/0
-	sgr-0818365fb43557e...	IPv6	All ICMP - IPv6	IPv6 ICMP	All	::/0
-	sgr-0fcfb1563456427a1b	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0
-	sgr-08e10c75da45b02dc	IPv4	HTTPS	TCP	443	0.0.0.0/0
-	sgr-096d1020b78983...	IPv4	All traffic	All	All	0.0.0.0/0
-	sgr-0d67fb89f96740155	IPv4	Custom TCP	TCP	5666	0.0.0.0/0

You have to edit the inbound rules of the specified Security Group for this.

3. SSH into Your EC2 instance or simply use EC2 Instance Connect from the browser.

The screenshot shows a terminal window with the following session:

```
ec2-user@ip-172-31-33-152:~$ ssh -i "Nagios-Key (1).pem" ec2-user@ec2-35-174-12-134.compute-1.amazonaws.com
Shraeyaa@LAPTOP-9IB41CE$ cd /c/Users/Shraeyaa/Downloads
Shraeyaa@LAPTOP-9IB41CE$ chmod 400 "Nagios-Key (1).pem"
Shraeyaa@LAPTOP-9IB41CE$ ssh -i "Nagios-Key (1).pem" ec2-user@ec2-35-174-12-134.compute-1.amazonaws.com
The authenticity of host 'ec2-35-174-12-134.compute-1.amazonaws.com (35.174.12.134)' can't be established.
ED25519 key fingerprint is SHA256:sePj45z2oVn8j2Boe5Meyel9wuf9YpPfwZt3qoiJz7E.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-35-174-12-134.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-172-31-33-152 ~]$
```

- Update the package indices and install the following packages using yum

```
sudo yum update
sudo yum install httpd php
sudo yum install gcc glibc glibc-common
sudo yum install gd gd-devel
```

Package	Architecture	Version	Repository	Size
gd	x86_64	2.3.3-5.amzn2023.0.3	amazonlinux	139 k
gd-devel	x86_64	2.3.3-5.amzn2023.0.3	amazonlinux	38 k
Installing dependencies:				
brotli	x86_64	1.0.9-4.amzn2023.0.2	amazonlinux	314 k
brotli-devel	x86_64	1.0.9-4.amzn2023.0.2	amazonlinux	31 k
hzip2-devel	x86_64	1.0.8-6.amzn2023.0.2	amazonlinux	214 k
cairo	x86_64	1.17.6-2.amzn2023.0.1	amazonlinux	684 k
cmake-filesystem	x86_64	3.22.2-1.amzn2023.0.4	amazonlinux	16 k
fontconfig	x86_64	2.13.94-2.amzn2023.0.2	amazonlinux	273 k
fontconfig-devel	x86_64	2.13.94-2.amzn2023.0.2	amazonlinux	128 k

- Create a new Nagios User with its password. You'll have to enter the password twice for confirmation.

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

```
libXpm-devel-3.5.15-2.amzn2023.0.3.x86_64
libxt-1.2.0-4.amzn2023.0.2.x86_64
libffi-devel-3.4.4-1.amzn2023.0.1.x86_64
libicu-devel-67.1-7.amzn2023.0.3.x86_64
libjpeg-turbo-devel-2.1.4-2.amzn2023.0.5.x86_64
libpng-2:1.6.37-10.amzn2023.0.6.x86_64
libselinux-devel-3.4-5.amzn2023.0.2.x86_64
libtiff-4.4.0-4.amzn2023.0.18.x86_64
libwebp-1.2.4-1.amzn2023.0.6.x86_64
libxcb-1.13.1-7.amzn2023.0.2.x86_64
libxml2-devel-2.10.4-1.amzn2023.0.6.x86_64
pcre2-utf16-10.40-1.amzn2023.0.3.x86_64
pixman-0.40.0-3.amzn2023.0.3.x86_64
xml-common-0.6.3-56.amzn2023.0.2.noarch
xz-devel-5.2.5-9.amzn2023.0.2.x86_64

Complete!
[ec2-user@ip-172-31-33-152 ~]$ sudo adduser -m nagios
[ec2-user@ip-172-31-33-152 ~]$ sudo passwd nagios
Changing password for user nagios.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[ec2-user@ip-172-31-33-152 ~]$ |
```

- Create a new user group

```
sudo groupadd nagcmd
```

7. Use these commands so that you don't have to use sudo for Apache and Nagios

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

```
passwd: all authentication tokens updated successfully.  
[ec2-user@ip-172-31-33-152 ~]$ sudo groupadd nagcmd  
[ec2-user@ip-172-31-33-152 ~]$ sudo usermod -a -G nagcmd nagios  
[ec2-user@ip-172-31-33-152 ~]$ sudo usermod -a -G nagcmd apache  
[ec2-user@ip-172-31-33-152 ~]$ mkdir ~/downloads  
[ec2-user@ip-172-31-33-152 ~]$ cd ~/downloads  
[ec2-user@ip-172-31-33-152 downloads]$ wget https://sourceforge.net/projects/nagios/files/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz/download?use_mirror=excellmedia  
--2024-10-12 20:11:57-- https://sourceforge.net/projects/nagios/files/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz/download?use_mirror=excellmedia  
Resolving sourceforge.net (sourceforge.net)... 172.64.150.145, 104.18.37.111, 2606:4700:4400::6812:256f, ...  
Connecting to sourceforge.net (sourceforge.net)|172.64.150.145|:443... connected.  
HTTP request sent, awaiting response... 302 Found  
Location: https://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz?ts=gAAAAABnCtgNAc21XA-ySFq5jucny2FxowPcfML23xyawGs2h1oghpAeGTRG8qGaJX9ufJKbzJkXVS-1GVawVl_1Ix4cLx0%3D%3D&use_mirror=excellmedia&r= [following]  
--2024-10-12 20:11:57-- https://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz?ts=gAAA
```

8. Create a new directory for Nagios downloads

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

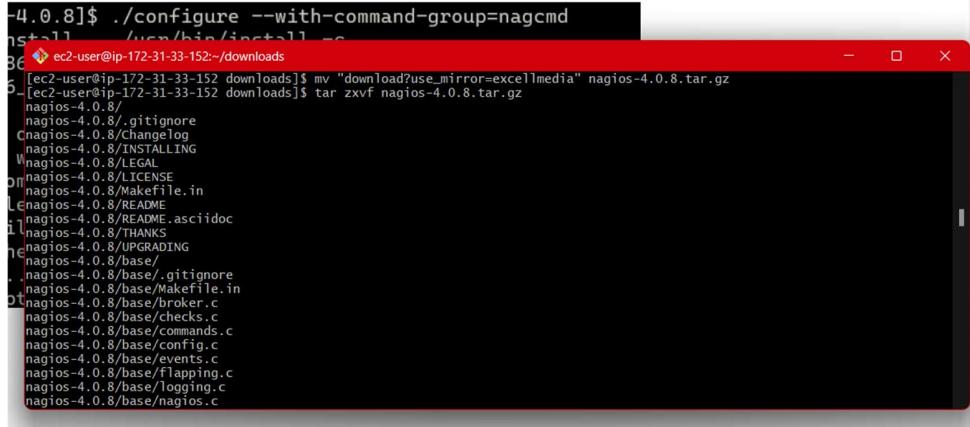
9. Use wget to download the source zip files.

```
wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz  
wget http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz
```

```
*****  
ec2-user@ip-172-31-33-152:~/downloads  
xz-devel-5.2.5-9.amzn2023.0.2.x86_64 zlib-devel-1.2.11-33.amzn2023.0.5.x86_64  
Complete!  
[ec2-user@ip-172-31-33-152 ~]$ sudo adduser -m nagios  
[ec2-user@ip-172-31-33-152 ~]$ sudo passwd nagios  
Changing password for user nagios.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[ec2-user@ip-172-31-33-152 ~]$ sudo groupadd nagcmd  
[ec2-user@ip-172-31-33-152 ~]$ sudo usermod -a -G nagcmd nagios  
[ec2-user@ip-172-31-33-152 ~]$ sudo usermod -a -G nagcmd apache  
[ec2-user@ip-172-31-33-152 ~]$ mkdir ~/downloads  
[ec2-user@ip-172-31-33-152 ~]$ cd ~/downloads  
[ec2-user@ip-172-31-33-152 downloads]$ wget https://sourceforge.net/projects/nagios/files/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz/download?use_mirror=excellmedia  
--2024-10-12 20:11:57-- https://sourceforge.net/projects/nagios/files/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz/download?use_mirror=excellmedia  
Resolving sourceforge.net (sourceforge.net)... 172.64.150.145, 104.18.37.111, 2606:4700:4400::6812:256f, ...  
Connecting to sourceforge.net (sourceforge.net)|172.64.150.145|:443... connected.  
HTTP request sent, awaiting response... 302 Found  
Location: https://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz?ts=gAAAAABnCtgNAc21XA-ySFq5jucny2FxowPcfML23xyawGs2h1oghpAeGTRG8qGaJX9ufJKbzJkXVS-1GVawVl_1Ix4cLx0%3D%3D&use_mirror=excellmedia&r= [following]  
--2024-10-12 20:11:57-- https://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz?ts=gAAA
```

10. Use tar to unzip and change to that directory.

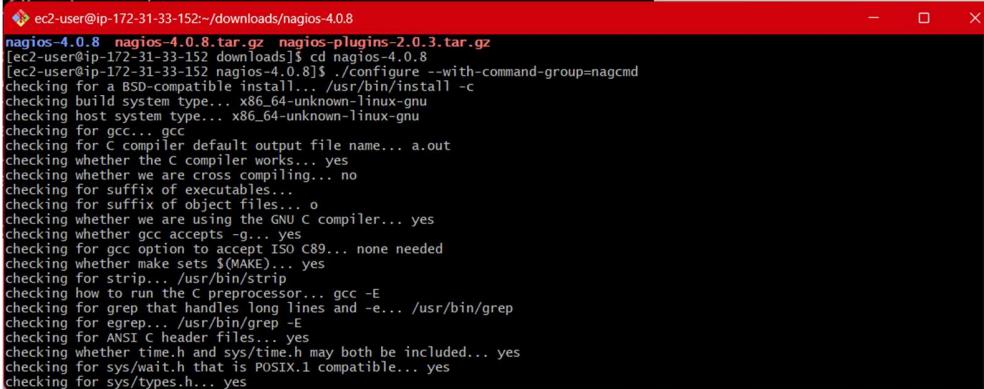
```
tar zxvf nagios-4.0.8.tar.gz
```



```
[4.0.8]$ ./configure --with-command-group=nagcmd
[nagios-4.0.8] [ec2-user@ip-172-31-33-152 ~]$ mv "download?use_mirror=excellmedia" nagios-4.0.8.tar.gz
[nagios-4.0.8] [ec2-user@ip-172-31-33-152 ~]$ tar zxvf nagios-4.0.8.tar.gz
[nagios-4.0.8]/.gitignore
[nagios-4.0.8]/CHANGELOG
[nagios-4.0.8]/INSTALLING
[nagios-4.0.8]/LEGAL
[nagios-4.0.8]/LICENSE
[nagios-4.0.8]/Makefile.in
[nagios-4.0.8]/README
[nagios-4.0.8]/README.asciidoc
[nagios-4.0.8]/THANKS
[nagios-4.0.8]/UPGRADING
[nagios-4.0.8]/base
[nagios-4.0.8]/base/.gitignore
[nagios-4.0.8]/base/Makefile.in
[nagios-4.0.8]/base/broker.c
[nagios-4.0.8]/base/checks.c
[nagios-4.0.8]/base/commands.c
[nagios-4.0.8]/base/config.c
[nagios-4.0.8]/base/events.c
[nagios-4.0.8]/base/flapping.c
[nagios-4.0.8]/base/logging.c
[nagios-4.0.8]/base/nagios.c
```

11. Run the configuration script with the same group name you previously created.

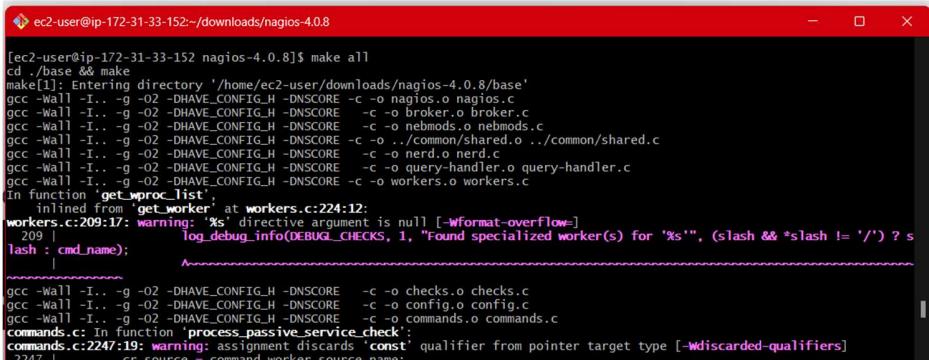
```
./configure --with-command-group=nagcmd
```



```
[4.0.8] [ec2-user@ip-172-31-33-152 ~]$ ./configure --with-command-group=nagcmd
[nagios-4.0.8] [ec2-user@ip-172-31-33-152 ~]$ cd nagios-4.0.8
[nagios-4.0.8] [ec2-user@ip-172-31-33-152 nagios-4.0.8]$ ./configure --with-command-group=nagcmd
checking for a BSD-compatible install... /usr/bin/install -c
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether make sets ${MAKE}... yes
checking for strip... /usr/bin/strip
checking how to run the C preprocessor... gcc -E
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for ANSI C header files... yes
checking whether time.h and sys/time.h may both be included... yes
checking for sys/wait.h that is POSIX.1 compatible... yes
checking for sys/types.h... yes
```

12. Compile the source code.

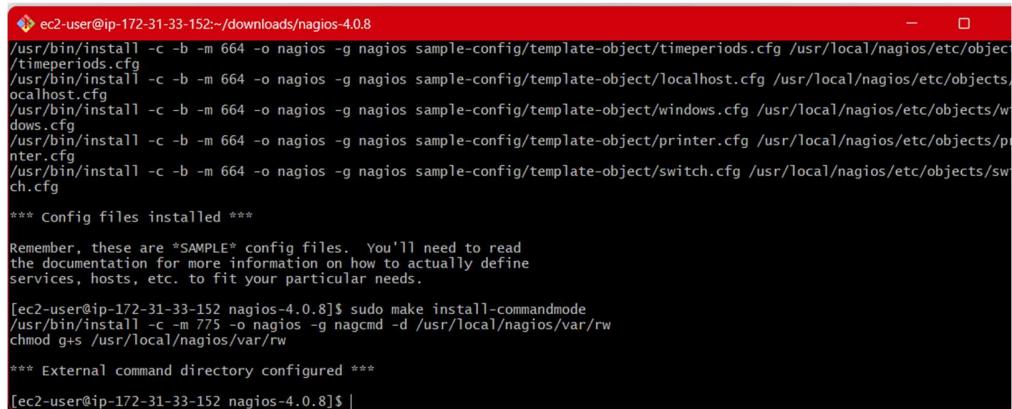
```
make all
```



```
[4.0.8] [ec2-user@ip-172-31-33-152 nagios-4.0.8]$ make all
[nagios-4.0.8] [ec2-user@ip-172-31-33-152 nagios-4.0.8]$ cd /base && make
make[1]: Entering directory '/home/ec2-user/downloads/nagios-4.0.8/base'
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nagios.o nagios.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o broker.o broker.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nebmods.o nebmods.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o ..//common/shared.o ..//common/shared.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nerd.o nerd.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o query-handler.o query-handler.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o workers.o workers.c
In function 'get_worker_list':
  inlined from 'get_worker' at workers.c:224:12:
workers.c:209: warning: 'xs' directive argument is null [-Wformat-overflow=]
  209 |           log_debug_info(DEBUG_CHECKS, 1, "found specialized worker(s) for '%s'", (slash && *slash != '/') ? s
|   |
|   lash : cmd_name);
|   |
|   ~~~~~
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o checks.o checks.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o config.o config.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o commands.o commands.c
commands.c: In function 'process_passive_service_check':
commands.c:2247: warning: assignment discards 'const' qualifier from pointer target type [-Wdiscarded-qualifiers]
  2247 |         er source = command.worker.source.name.
```

13. Install binaries, init script and sample config files. Lastly, set permissions on the external command directory.

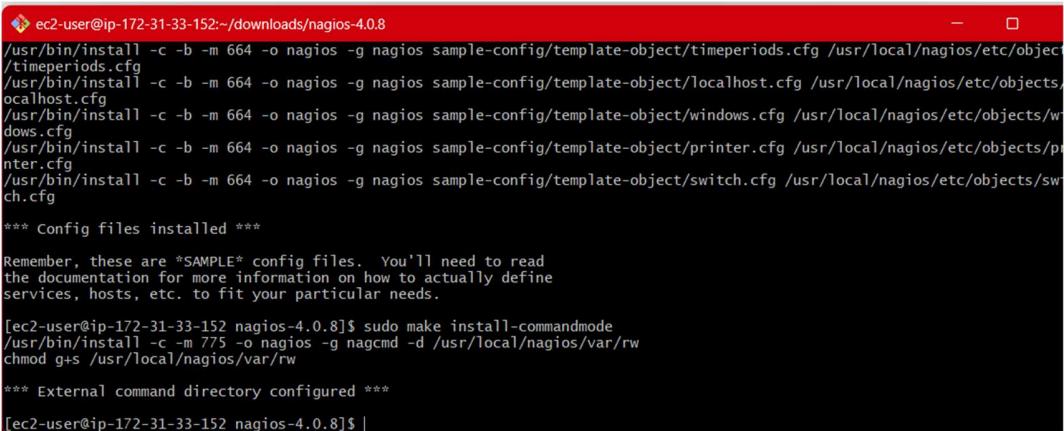
```
sudo make install sudo make  
install-init sudo make  
install-config sudo make  
install-commandmode
```



```
[ec2-user@ip-172-31-33-152:~/downloads/nagios-4.0.8]  
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/timeperiods.cfg /usr/local/nagios/etc/objects/timeperiods.cfg  
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/localhost.cfg /usr/local/nagios/etc/objects/localhost.cfg  
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/windows.cfg /usr/local/nagios/etc/objects/windows.cfg  
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/printer.cfg /usr/local/nagios/etc/objects/printer.cfg  
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/switch.cfg /usr/local/nagios/etc/objects/switch.cfg  
  
*** Config files installed ***  
  
Remember, these are *SAMPLE* config files. You'll need to read  
the documentation for more information on how to actually define  
services, hosts, etc. to fit your particular needs.  
  
[ec2-user@ip-172-31-33-152 nagios-4.0.8]$ sudo make install-commandmode  
/usr/bin/install -c -m 775 -o nagios -g nagcmd -d /usr/local/nagios/var/rw  
chmod g+s /usr/local/nagios/var/rw  
  
*** External command directory configured ***  
[ec2-user@ip-172-31-33-152 nagios-4.0.8]$ |
```

14. Edit the config file and change the email address. sudo nano

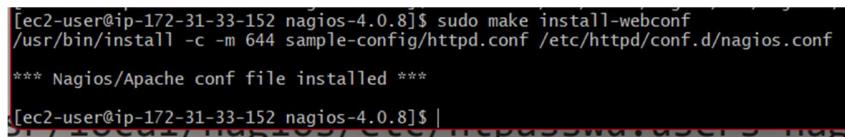
```
/usr/local/nagios/etc/objects/contacts.cfg
```



```
[ec2-user@ip-172-31-33-152:~/downloads/nagios-4.0.8]  
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/timeperiods.cfg /usr/local/nagios/etc/objects/timeperiods.cfg  
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/localhost.cfg /usr/local/nagios/etc/objects/localhost.cfg  
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/windows.cfg /usr/local/nagios/etc/objects/windows.cfg  
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/printer.cfg /usr/local/nagios/etc/objects/printer.cfg  
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/switch.cfg /usr/local/nagios/etc/objects/switch.cfg  
  
*** Config files installed ***  
  
Remember, these are *SAMPLE* config files. You'll need to read  
the documentation for more information on how to actually define  
services, hosts, etc. to fit your particular needs.  
  
[ec2-user@ip-172-31-33-152 nagios-4.0.8]$ sudo make install-commandmode  
/usr/bin/install -c -m 775 -o nagios -g nagcmd -d /usr/local/nagios/var/rw  
chmod g+s /usr/local/nagios/var/rw  
  
*** External command directory configured ***  
[ec2-user@ip-172-31-33-152 nagios-4.0.8]$ |
```

15. Configure the web interface.

```
sudo make install-webconf
```



```
[ec2-user@ip-172-31-33-152 nagios-4.0.8]$ sudo make install-webconf  
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/httpd/conf.d/nagios.conf  
  
*** Nagios/Apache conf file installed ***  
  
[ec2-user@ip-172-31-33-152 nagios-4.0.8]$ |
```

16. Create a nagiosadmin account for nagios login along with password. You'll have to specify the password twice.

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

```
[ec2-user@ip-172-31-33-152 nagios-4.0.8]$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
[ec2-user@ip-172-31-33-152 nagios-4.0.8]$
```

17. Restart Apache

```
sudo service httpd restart
```

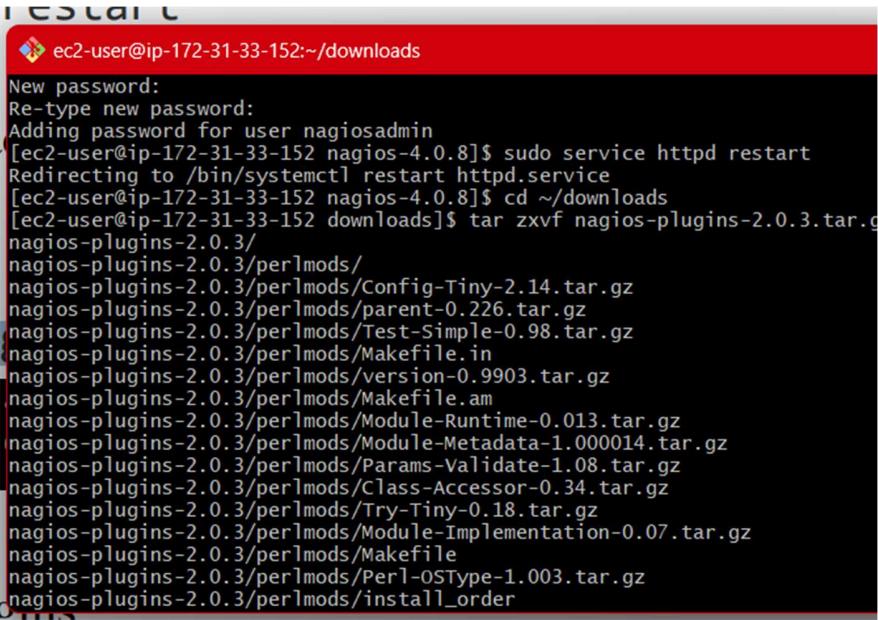
18. Go back to the downloads folder and unzip the plugins zip file.

```
cd ~/downloads
tar zxvf nagios-plugins-2.0.3.tar.gz
```

```
ec2-user@ip-172-31-33-152:~/downloads
New password:
Re-type new password:
Adding password for user nagiosadmin
[ec2-user@ip-172-31-33-152 nagios-4.0.8]$ sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[ec2-user@ip-172-31-33-152 nagios-4.0.8]$ cd ~/downloads
[ec2-user@ip-172-31-33-152 downloads]$ tar zxvf nagios-plugins-2.0.3.tar.gz
nagios-plugins-2.0.3/
nagios-plugins-2.0.3/perlmods/
nagios-plugins-2.0.3/perlmods/Config-Tiny-2.14.tar.gz
nagios-plugins-2.0.3/perlmods/parent-0.226.tar.gz
nagios-plugins-2.0.3/perlmods/Test-Simple-0.98.tar.gz
nagios-plugins-2.0.3/perlmods/Makefile.in
nagios-plugins-2.0.3/perlmods/version-0.9903.tar.gz
nagios-plugins-2.0.3/perlmods/Makefile.am
nagios-plugins-2.0.3/perlmods/Module-Runtime-0.013.tar.gz
nagios-plugins-2.0.3/perlmods/Module-Metadata-1.000014.tar.gz
nagios-plugins-2.0.3/perlmods/Params-Validate-1.08.tar.gz
nagios-plugins-2.0.3/perlmods/Class-Accessor-0.34.tar.gz
nagios-plugins-2.0.3/perlmods/Try-Tiny-0.18.tar.gz
nagios-plugins-2.0.3/perlmods/Module-Implementation-0.07.tar.gz
nagios-plugins-2.0.3/perlmods/Makefile
nagios-plugins-2.0.3/perlmods/Perl-OStype-1.003.tar.gz
nagios-plugins-2.0.3/perlmods/install_order
```

19. Compile and install plugins

```
cd nagios-plugins-2.0.3
./configure --with-nagios-user=nagios --with-nagios-group=nagios
make sudo make install
```



```
ec2-user@ip-172-31-33-152:~/downloads
New password:
Re-type new password:
Adding password for user nagiosadmin
[ec2-user@ip-172-31-33-152 nagios-4.0.8]$ sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[ec2-user@ip-172-31-33-152 nagios-4.0.8]$ cd ~/downloads
[ec2-user@ip-172-31-33-152 downloads]$ tar zxvf nagios-plugins-2.0.3.tar.gz
nagios-plugins-2.0.3/
nagios-plugins-2.0.3/perlmods/
nagios-plugins-2.0.3/perlmods/Config-Tiny-2.14.tar.gz
nagios-plugins-2.0.3/perlmods/parent-0.226.tar.gz
nagios-plugins-2.0.3/perlmods/Test-Simple-0.98.tar.gz
nagios-plugins-2.0.3/perlmods/Makefile.in
nagios-plugins-2.0.3/perlmods/version-0.9903.tar.gz
nagios-plugins-2.0.3/perlmods/Makefile.am
nagios-plugins-2.0.3/perlmods/Module-Runtime-0.013.tar.gz
nagios-plugins-2.0.3/perlmods/Module-Metadata-1.000014.tar.gz
nagios-plugins-2.0.3/perlmods/Params-Validate-1.08.tar.gz
nagios-plugins-2.0.3/perlmods/Class-Accessor-0.34.tar.gz
nagios-plugins-2.0.3/perlmods/Try-Tiny-0.18.tar.gz
nagios-plugins-2.0.3/perlmods/Module-Implementation-0.07.tar.gz
nagios-plugins-2.0.3/perlmods/Makefile
nagios-plugins-2.0.3/perlmods/Perl-OSType-1.003.tar.gz
nagios-plugins-2.0.3/perlmods/install_order
```

20. Start Nagios

Add Nagios to the list of system services

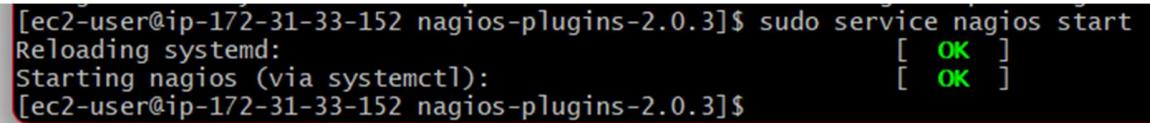
```
sudo chkconfig --add nagios
sudo
chkconfig nagios on
```

Verify the sample configuration files

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

If there are no errors, you can go ahead and start Nagios.

```
sudo service nagios start
```



```
[ec2-user@ip-172-31-33-152 nagios-plugins-2.0.3]$ sudo service nagios start
Reloading systemd: [ OK ]
Starting nagios (via systemctl): [ OK ]
[ec2-user@ip-172-31-33-152 nagios-plugins-2.0.3]$
```

21. Check the status of Nagios

```
sudo systemctl status nagios
```

```

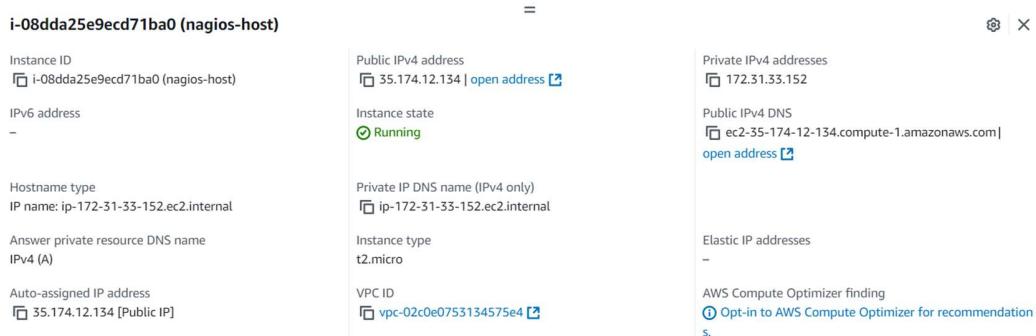
ec2-user@ip-172-31-33-152:~/downloads/nagios-plugins-2.0.3
Docs: man:systemd-sysv-generator(8)
Process: 68138 ExecStart=/etc/rc.d/init.d/nagios start (code=exited, status=0/SUCCESS)
Tasks: 6 (limit: 1112)
Memory: 3.0M
CPU: 28ms
Group: /system.slice/nagios.service
-- 
[68160 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
-68162 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
-68163 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
-68164 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
-68165 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.gh
-68166 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Oct 12 20:52:37 ip-172-31-33-152.ec2.internal nagios[68160]: nerd: Channel hostchecks registered successfully
Oct 12 20:52:37 ip-172-31-33-152.ec2.internal nagios[68160]: nerd: Channel servicechecks registered successfully
Oct 12 20:52:37 ip-172-31-33-152.ec2.internal nagios[68160]: nerd: Channel opatchchecks registered successfully
Oct 12 20:52:37 ip-172-31-33-152.ec2.internal nagios[68160]: nerd: Fully initialized and ready to rock!
Oct 12 20:52:37 ip-172-31-33-152.ec2.internal nagios[68160]: wproc: Executed command registered managed @wproc with query handler
Oct 12 20:52:37 ip-172-31-33-152.ec2.internal nagios[68160]: wproc: Registry request: name=Core worker 68165;pid=68165
Oct 12 20:52:37 ip-172-31-33-152.ec2.internal nagios[68160]: wproc: Registry request: name=Core worker 68164;pid=68164
Oct 12 20:52:37 ip-172-31-33-152.ec2.internal nagios[68160]: wproc: Registry request: name=Core worker 68162;pid=68162
Oct 12 20:52:37 ip-172-31-33-152.ec2.internal nagios[68160]: Successfully launched command file worker with pid 68166

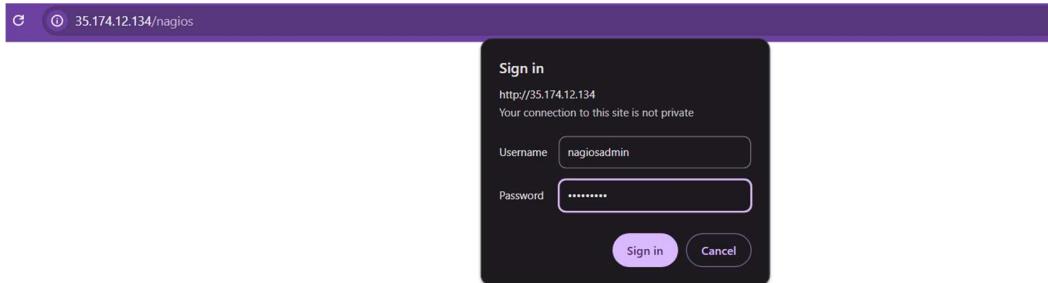
```

Lines 4-26/26 (END)

22. Go back to EC2 Console and copy the Public IP address of this instance



23. Open up your browser and look for http://<your_public_ip_address>/nagios



Enter username as nagiosadmin and password which you set in Step 16.

24. After entering the correct credentials, you will see this page.

The screenshot shows the Nagios Core web interface. At the top right, the Nagios logo is displayed with the text "Nagios® Core™" and a green checkmark indicating "Daemon running with PID 68654". Below the logo, the text "Nagios® Core™ Version 4.4.6" is shown, along with the date "April 28, 2020" and a link "Check for updates". A blue banner at the top right states "A new version of Nagios Core is available! Visit nagios.org to download Nagios 4.5.5." On the left side, there is a vertical navigation menu with sections: General (Home, Documentation), Current Status (Tactical Overview, Map (Legacy), Hosts, Services, Host Groups, Service Groups), Problems (Services, Hosts (Unhandled), Network Outages), Reports (Availability, Trends (Legacy), Alerts, History, Summary, Histogram (Legacy)), Notifications, Event Log, and System (Comments, Downtime, Process Info, Performance Info, Scheduling Queue, Configuration). The main content area is divided into several boxes: "Get Started" (bullet points: Start monitoring your infrastructure, Change the look and feel of Nagios, Extend Nagios with hundreds of addons, Get support, Get training, Get certified), "Quick Links" (bullet points: 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" (empty), and "Don't Miss..." (empty). At the bottom of the page, a small copyright notice reads "Copyright © 2010-2020 Nagios Core Development Team and Community Contributors. Copyright © 1999-2009 Ethan Galstad. See the THANKS file for more information".

This means that Nagios was correctly installed and configured with its plugins so far.

ADVANCE DEVOPS EXP-10

SHRAEYAA DHAIGUDE

D15A/15

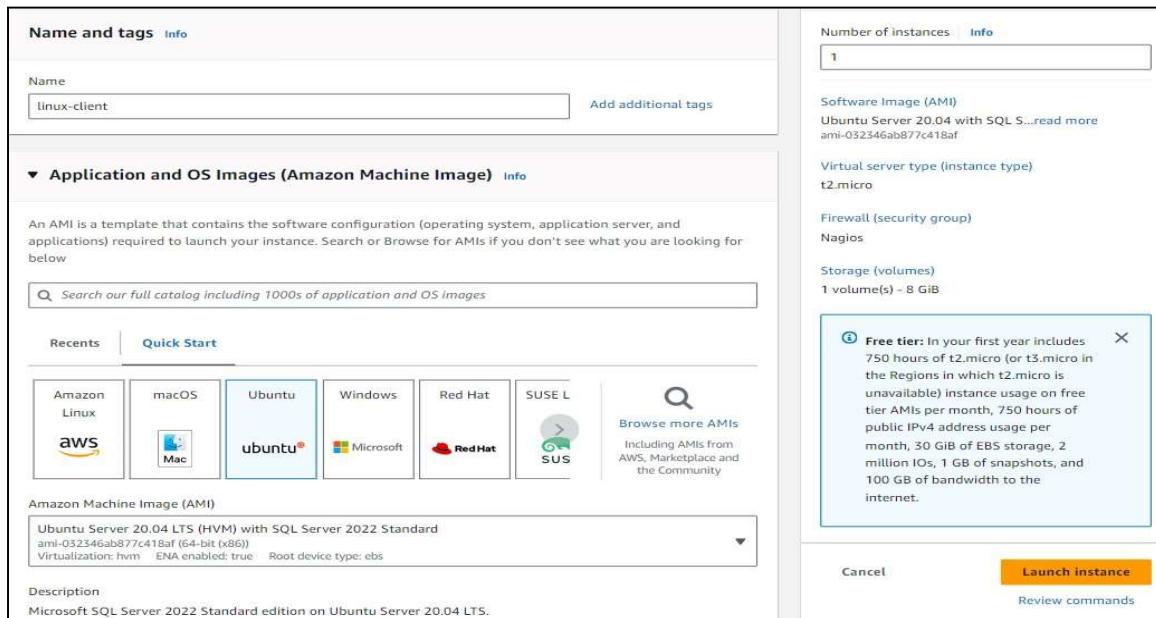
Aim: To perform Port, Service monitoring, Windows/Linux server monitoring using Nagios.

Step-1. Confirm Nagios is Running on the Server. sudo systemctl status nagios Proceed if you see that Nagios is active and running.

```
[ec2-user@ip-172-31-90-152 nagios-plugins-2.3.3]$ cd
[ec2-user@ip-172-31-90-152 ~]$ sudo systemctl restart nagios
[ec2-user@ip-172-31-90-152 ~]$ sudo systemctl status nagios
● nagios.service - Nagios Core 4.5.5
   Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
   Active: active (running) since Mon 2024-09-30 19:41:36 UTC; 7s ago
     Docs: https://www.nagios.org/documentation
 Process: 80238 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
 Process: 80239 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
 Main PID: 80240 (nagios)
   Tasks: 6 (limit: 1112)
  Memory: 4.0M
    CPU: 15ms
   CGroup: /system.slice/nagios.service
           ├─80240 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
           ├─80241 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─80242 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─80243 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─80244 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           └─80245 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: qh: Socket '/usr/local/nagios/var/rw/nagios.qh' successfully initialized
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: qh: core query handler registered
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: qh: echo service query handler registered
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: qh: help for the query handler registered
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Successfully registered manager @wproc with query handler
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80244;pid=80244
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80243;pid=80243
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80242;pid=80242
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80241;pid=80241
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: Successfully launched command file worker with pid 80245
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: qh: core query handler registered
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: qh: echo service query handler registered
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: qh: help for the query handler registered
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Successfully registered manager @wproc with query handler
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80244;pid=80244
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80243;pid=80243
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80242;pid=80242
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: wproc: Registry request: name=Core Worker 80241;pid=80241
Sep 30 19:41:36 ip-172-31-90-152.ec2.internal nagios[80240]: Successfully launched command file worker with pid 80245
```

Step-2. Create an Ubuntu 20.04 Server EC2 Instance



Step-3: Verify Nagios Process on the Server

```
[ec2-user@ip-172-31-80-215 nagios-plugins-2.3.3]$ ps -ef | grep nagios
nagios  68654      1  0 20:29 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios  68655  68654  0 20:29 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios  68656  68654  0 20:29 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios  68657  68654  0 20:29 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios  68658  68654  0 20:29 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios  68659  68654  0 20:29 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
ec2-user  69588  26447  0 20:44 pts/0    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-80-215 nagios-plugins-2.3.3]$
```

Step-4: Become Root User and Create Directories sudo su , mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts and to copy the same config file- cp /usr/local/nagios/etc/objects/localhost.cfg, /usr/local/nagios/etc/objects/monitorhosts/linuxserver.cfg

```
[ec2-user@ip-172-31-80-215 nagios-plugins-2.3.3]$ sudo su
[root@ip-172-31-80-215 nagios-plugins-2.3.3]# mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
[root@ip-172-31-80-215 nagios-plugins-2.3.3]# cp /usr/local/nagios/etc/objects/localhost.cfg
cp: missing destination file operand after '/usr/local/nagios/etc/objects/localhost.cfg'
Try 'cp --help' for more information.
[root@ip-172-31-80-215 nagios-plugins-2.3.3]# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxserver.cfg
[root@ip-172-31-80-215 nagios-plugins-2.3.3]#
```

i-0ae1aae975bae3b7a (nagios-host)

Step-5: Edit the Configuration File

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

- Change hostname to linuxserver everywhere in the file • Change address to the public IP address of your linux-client.
- Change host_group name under hostgroup to linux_server

```
#####
# HOST DEFINITION
#
#####

# Define a host for the local machine

define host {
    use             linux-server           ; Name of host template to use
                                ; This host definition will inherit all variables that are defined
                                ; in (or inherited by) the linux-server host template definition.

    host_name       linuxserver
    alias          linuxserver
    address        35.174.139.220
}

#####
# HOST GROUP DEFINITION
#
#####

# Define an optional hostgroup for Linux machines

define hostgroup {
    hostgroup_name   linux-servers1      ; The name of the hostgroup
    alias            Linux Servers        ; Long name of the group
    members          localhost           ; Comma separated list of hosts that belong to this group
}

[ Read 157 lines ]
^G Help      ^C Write Out      ^W Where Is      ^K Cut      ^E Execute      ^C Location      M-U Undo      M-A Set Mark      M-1 To
^X Exit      ^R Read File      ^V Replace      ^U Paste      ^J Justify      ^Y Go To Line     M-B Redo      M-6 Copy      ^D Where
```

Step-6: Update Nagios Configuration sudo

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

Add the command - cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/

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

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

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

Step-7: Verify Configuration Files sudo /usr/local/nagios/bin/nagios -v

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

```
[ec2-user@ip-172-31-80-215 ~]$ sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Nagios Core 4.4.6
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2020-04-28
License: GPL

Website: https://www.nagios.org
Reading configuration data...
  Read main config file okay...
Warning: Duplicate definition found for service 'HTTP' on host 'localhost' (config file '/usr/local/nagios/etc/objects/localhost.cfg')
Warning: Duplicate definition found for service 'SSH' on host 'localhost' (config file '/usr/local/nagios/etc/objects/localhost.cfg')
Warning: Duplicate definition found for service 'Swap Usage' on host 'localhost' (config file '/usr/local/nagios/etc/objects/localhost.cfg')
Warning: Duplicate definition found for service 'Current Load' on host 'localhost' (config file '/usr/local/nagios/etc/objects/localhost.cfg')
Warning: Duplicate definition found for service 'Total Processes' on host 'localhost' (config file '/usr/local/nagios/etc/objects/localhost.cfg')
Warning: Duplicate definition found for service 'Current Users' on host 'localhost' (config file '/usr/local/nagios/etc/objects/localhost.cfg')
Warning: Duplicate definition found for service 'Root Partition' on host 'localhost' (config file '/usr/local/nagios/etc/objects/localhost.cfg')
Warning: Duplicate definition found for service 'PING' on host 'localhost' (config file '/usr/local/nagios/etc/objects/localhost.cfg')
  Read object config files okay...

Running pre-flight check on configuration data...

Checking objects...
  Checked 8 services.
  Checked 2 hosts.
  Checked 2 host groups.
  Checked 0 service groups.
  Checked 1 contacts.
  Checked 1 contact groups.
  Checked 24 commands.
  Checked 5 time periods.
  Checked 0 host escalations.
  Checked 0 service escalations.
Checking for circular paths...
  Checked 2 hosts
  Checked 0 service dependencies
  Checked 0 host dependencies
  Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors: 0
```

Step-8: Restart Nagios Service
sudo
systemctl restart nagios

Step-9: SSH into the Client Machine

Use SSH or EC2 Instance Connect to access the linux-client.

Step-10: Update Package Index and Install Required Packages

sudo apt update -y

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

```
ubuntu@ip-172-31-86-24:~$ sudo apt update -y
sudo apt install gcc -y
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://us-east-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://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [380 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [83.1 kB]
Get:10 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4560 B]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [274 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [535 kB]
Get:18 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [116 kB]
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [130 kB]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [8652 B]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [379 kB]
```

Step-11: Edit NRPE Configuration File

Commands -

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

Add your Nagios host IP address under allowed_hosts:

```
allowed_hosts=<Nagios_Host_IP>

# Note: The daemon only does rudimentary checking of the client's IP
# address. I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd

allowed_hosts=127.0.0.1,35.174.139.220

# COMMAND ARGUMENT PROCESSING
# This option determines whether or not the NRPE daemon will allow clients
# to specify arguments to commands that are executed. This option only works
# if the daemon was configured with the --enable-command-args configure script
# option.
#
# *** ENABLING THIS OPTION IS A SECURITY RISK! ***
# Read the SECURITY file for information on some of the security implications
# of enabling this variable.
#
# Values: 0=do not allow arguments, 1=allow command arguments

dont_blame_nrpe=0
```

Step-12: Restart NRPE Server

Commands -

```
sudo systemctl restart nagios-nrpe-server
```

Step-13:Check Nagios Dashboard

Open your browser and navigate to http://<Nagios_Host_IP>/nagios.
Log in with nagiosadmin and the password you set earlier.
You should see the new host linuxserver added.
Click on Hosts to see the host details.
Click on Services to see all services and ports being monitored

Nagios® Core™
✓ Daemon running with PID 71172

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

A new version of Nagios Core is available!
[Visit nagios.org to download Nagios 4.5.5.](http://nagios.org)

<p>Get Started</p> <ul style="list-style-type: none"> • Start monitoring your infrastructure • Change the look and feel of Nagios • Extend Nagios with hundreds of addons • Get support • Get training • Get certified 	<p>Quick Links</p> <ul style="list-style-type: none"> • Nagios Library (tutorials and docs) • Nagios Labs (development blog) • Nagios Exchange (plugins and addons) • Nagios Support (tech support) • Nagios.com (company) • Nagios.org (project) 	
<p>Latest News</p> <p>Don't Miss...</p>		

Copyright © 2010-2020 Nagios Core Development Team and Community Contributors. Copyright © 1999-2009 Ethan Galstad. See the THANKS file for more information on contributors.

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:](#)

Current Network Status

Last Updated: Mon Sep 30 21:16:41 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.4.6 - www.nagios.org
Logged in as nagiosadmin

[View Service Status Detail For All Host Groups](#)

[View Status Overview For All Host Groups](#)

[View Status Summary For All Host Groups](#)

[View Status Grid For All Host Groups](#)

Host Status Totals

Up	Down	Unreachable	Pending
2	0	0	0

All Problems	All Types
0	2

Service Status Totals

Ok	Warning	Unknown	Critical
6	1	0	1

All Problems	All Types
2	8

Host Status Details For All Host Groups

Host	Status	Last Check	Duration	Status Information
linuxserver	UP	09-30-2024 21:14:52	0d 0h 11m 49s	PING OK - Packet loss = 0%, RTA = 0.98 ms
localhost	UP	09-30-2024 21:14:01	0d 0h 47m 2s	PING OK - Packet loss = 0%, RTA = 0.04 ms

Results 1 - 2 of 2 Matching Hosts

Current Network Status

Last Updated: Mon Sep 30 21:21:11 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.4.6 - www.nagios.org
Logged in as nagiosadmin

[View History for all Hosts](#)

[View Notifications For All Hosts](#)

[View Host Status Detail For All Hosts](#)

Host Status Totals

Up	Down	Unreachable	Pending
2	0	0	0

All Problems	All Types
0	2

Service Status Totals

Ok	Warning	Unknown	Critical
6	1	0	1

All Problems	All Types
2	8

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	09-30-2024 21:20:16	0d 0h 50m 55s	1/4	OK - load average: 0.00, 0.00, 0.00
localhost	Current Users	OK	09-30-2024 21:20:54	0d 0h 50m 17s	1/4	USERS OK - 1 users currently logged in
HTTP		WARNING	09-30-2024 21:19:31	0d 0h 46m 40s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 319 bytes in 0.001 second response time
localhost	PING	OK	09-30-2024 21:17:09	0d 0h 49m 2s	1/4	PING OK - Packet loss = 0%, RTA = 0.04 ms
localhost	Root Partition	OK	09-30-2024 21:17:46	0d 0h 48m 25s	1/4	DISK OK - free space: / 6080 MB (74.91% inode=98%)
SSH		CRITICAL	09-30-2024 21:18:24	0d 0h 47m 47s	1/4	SSH OK - OpenSSH_8.7 (protocol 2.0)
localhost	Swap Usage	CRITICAL	09-30-2024 21:17:01	0d 0h 44m 10s	4/4	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.
localhost	Total Processes	OK	09-30-2024 21:19:39	0d 0h 46m 32s	1/4	PROCS OK: 36 processes with STATE = RSDT

Results 1 - 8 of 8 Matching Services

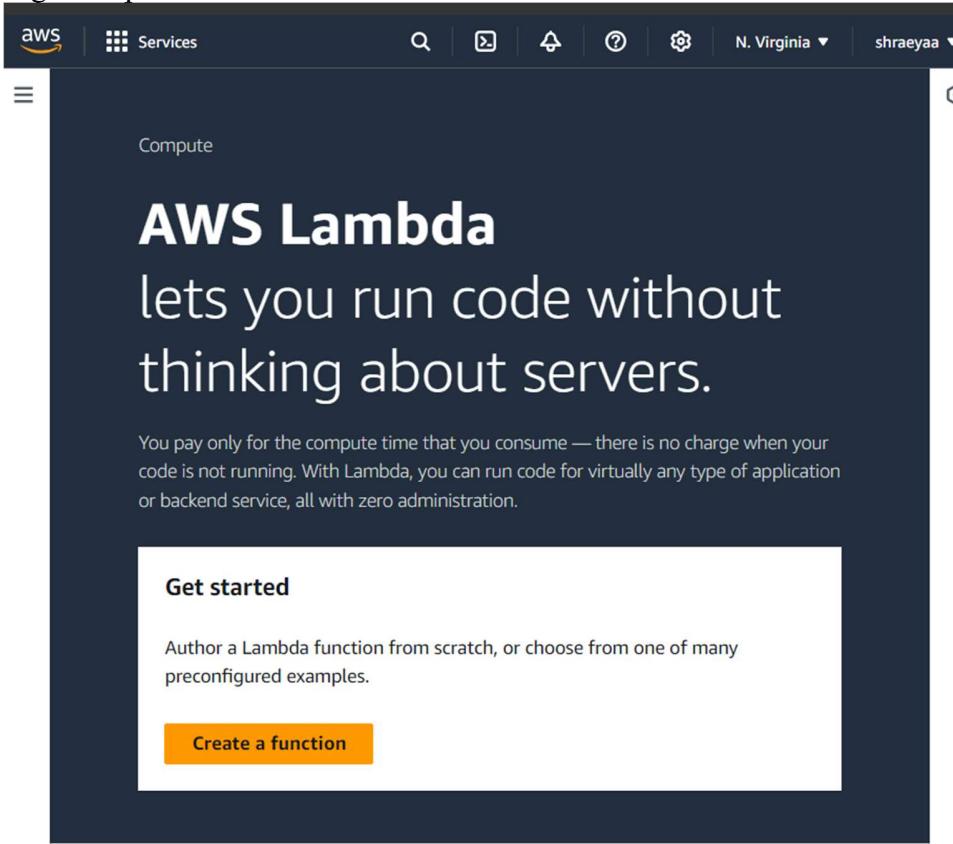
Advance Devops-11

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

Steps to create an AWS Lambda function

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

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



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

Then, choose a runtime env for your function, under the dropdown, you can see all the options AWS supports, Python, Nodejs, .NET and Java being the most popular ones.

After that, choose to create a new role with basic Lambda permissions if you don't have an existing one.

aws Services N. Virginia shraeyaa

Create function Info

Choose one of the following options to create your function.

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

Basic information

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

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

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

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

Permissions Info

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

Change default execution role

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

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

Lambda will create an execution role named lambdashraeyaa-role-l4l1w09a, with permission to upload logs to Amazon CloudWatch Logs.

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

Lambda > Functions > lambdashraeyaa

lambdashraeyaa

Throttle Actions ▾

▼ Function overview Info

Description
-

Last modified
44 seconds ago

Function ARN
Function URL Info
-

☰ ⌚ Successfully updated the function lambdashraeyaa. X

Info"/>

↻ ↺ ↻ ⚙️

Environment Var × (+) +

Environment

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

Basic settings [Info](#)

Description - *optional*

Memory [Info](#)
Your function is allocated CPU proportional to the memory configured.

128 MB

Set memory to between 128 MB and 10240 MB

Ephemeral storage [Info](#)
You can configure up to 10 GB of ephemeral storage (/tmp) for your function. [View pricing](#)

512 MB

Set ephemeral storage (/tmp) to between 512 MB and 10240 MB.

SnapStart [Info](#)
Reduce startup time by having Lambda cache a snapshot of your function after the function has initialized. To evaluate whether your function code is resilient to snapshot operations, review the [SnapStart compatibility considerations](#).

None

Supported runtimes: Java 11, Java 17, Java 21.

Timeout

0 min 3 sec

Execution role

Successfully updated the function lambdashraeyaa. X

[Code](#) [Test](#) [Monitor](#) [Configuration](#) [Aliases](#) [Versions](#)

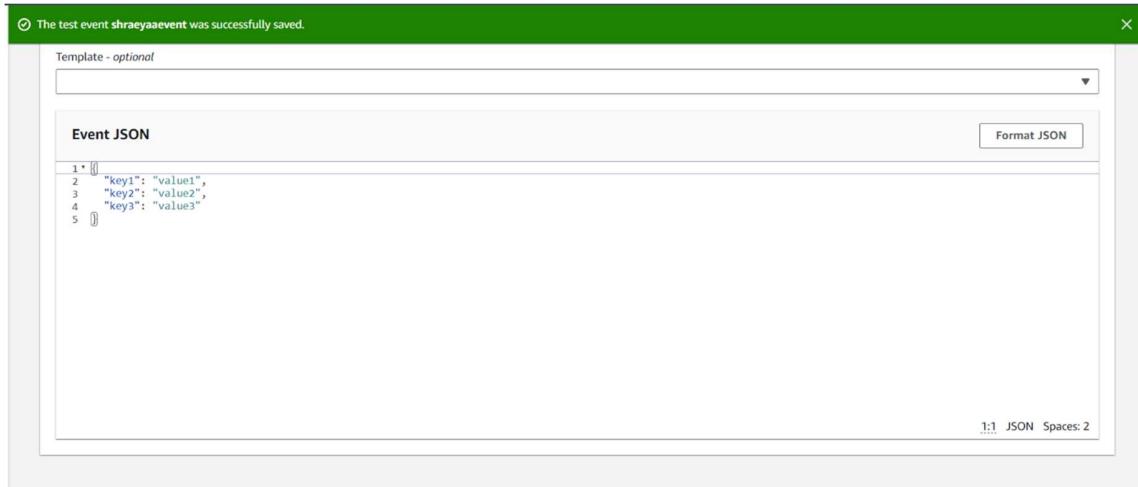
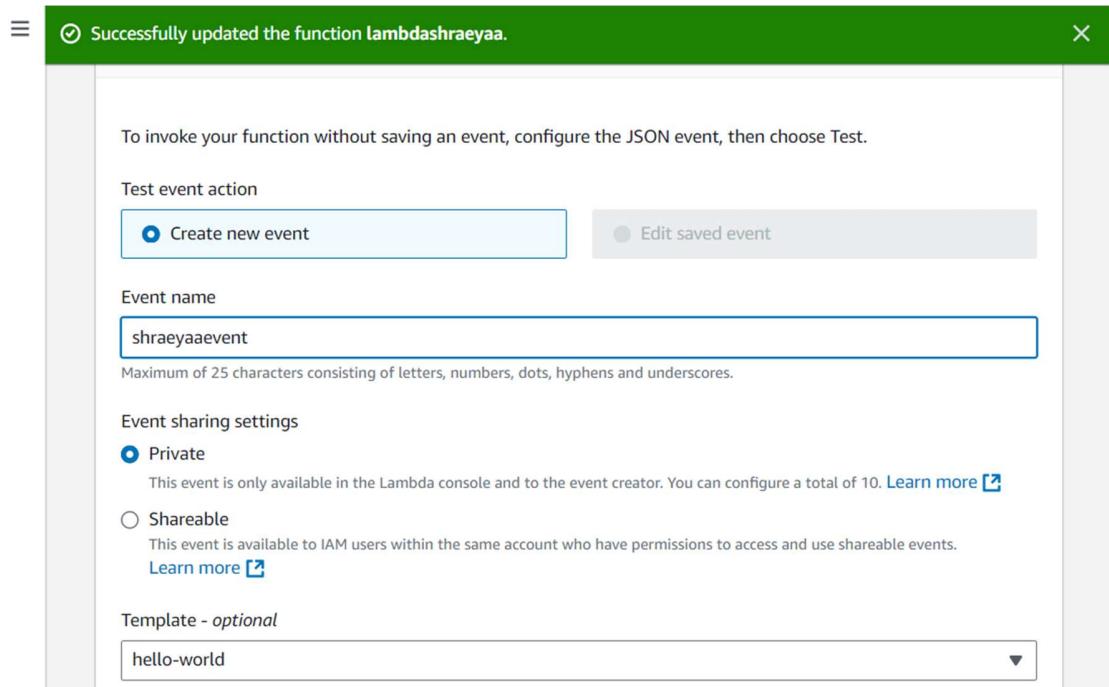
Code source [Info](#) [Upload from](#)

File Edit Find View Go Tools Window [Test](#) Deploy Environment Var

Go to Anything (Ctrl-P)

Environment lambdashraeyaa / lambda_function.py

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



Click on the *Create* button.

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

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

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

Ephemeral storage [Info](#)

You can configure up to 10 GB of ephemeral storage (/tmp) for your function. [View pricing](#)

512

 MB
Set ephemeral storage (/tmp) to between 512 MB and 10240 MB.

SnapStart [Info](#)

Reduce startup time by having Lambda cache a snapshot of your function after the function has initialized. To evaluate whether your function code is resilient to snapshot operations, review the [SnapStart compatibility considerations](#).

None

Supported runtimes: Java 11, Java 17, Java 21.

Timeout

0

 min

1

 sec

Execution role

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

Use an existing role
 Create a new role from AWS policy templates

Existing role

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

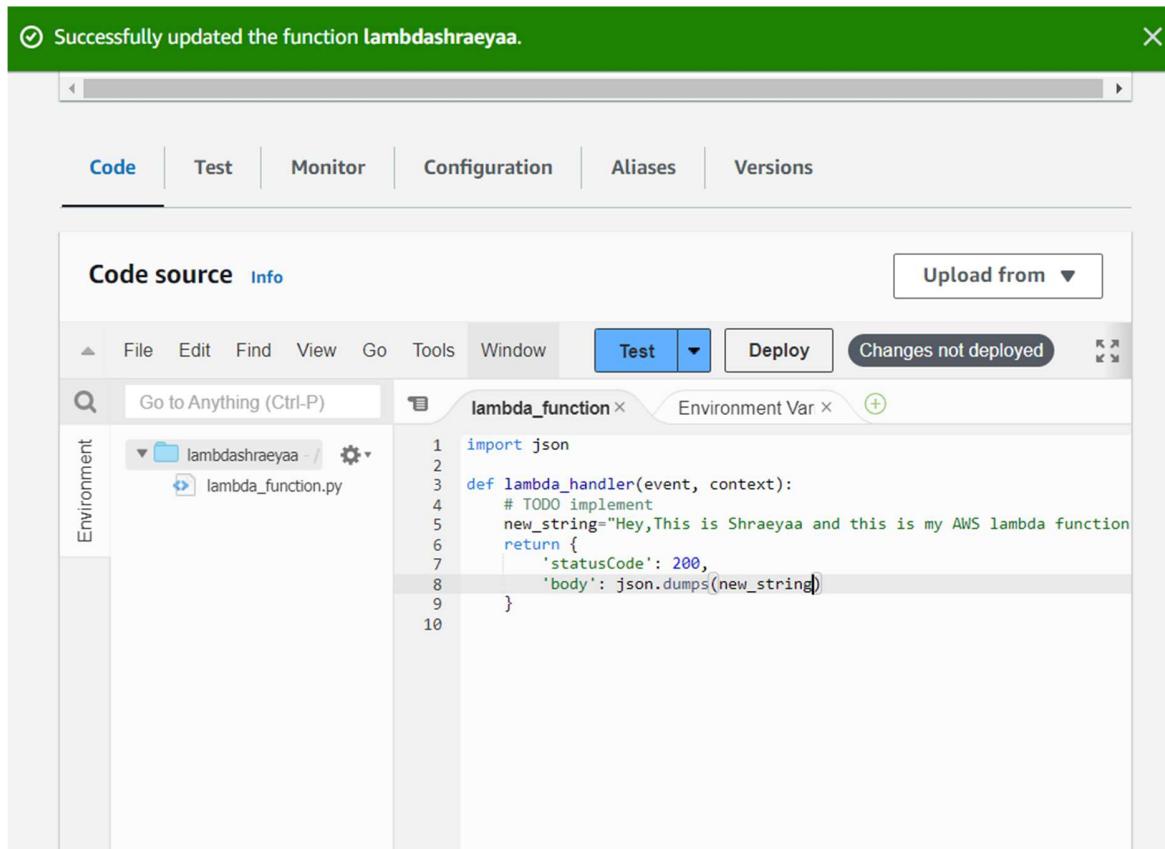
service-role/lambdashraeyaa-role-l4l1w09a

[View the lambdashraeyaa-role-l4l1w09a role](#)

[on the IAM console.](#)

[Cancel](#) [Save](#)

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



The screenshot shows the AWS Lambda function editor interface. At the top, there's a green success message: "Successfully updated the function lambdashraeyaa." Below the message, the navigation bar includes tabs for Code, Test, Monitor, Configuration, Aliases, and Versions. The Code tab is selected. In the main area, the "Code source" tab is active, showing the Python code for the lambda function:

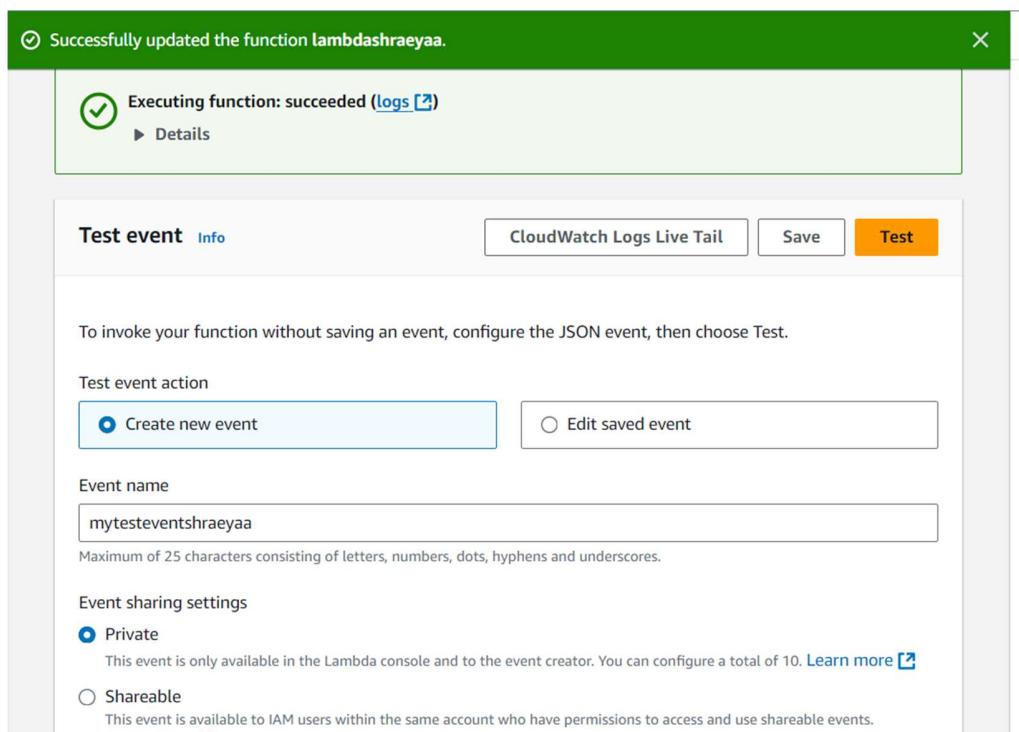
```

import json

def lambda_handler(event, context):
    # TODO implement
    new_string="Hey,This is Shraeyaa and this is my AWS lambda function"
    return {
        'statusCode': 200,
        'body': json.dumps(new_string)
    }

```

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



The screenshot shows the AWS Lambda function test configuration page. At the top, there's a green success message: "Successfully updated the function lambdashraeyaa." Below the message, a notification says "Executing function: succeeded (logs [?])". The main area is titled "Test event" and includes a "Test" button. It has sections for "Test event action" (with "Create new event" selected), "Event name" (set to "mytesteventshraeyaa"), and "Event sharing settings" (with "Private" selected). A note states: "This event is only available in the Lambda console and to the event creator. You can configure a total of 10." Below this, there's a section for "Shareable" events with a note: "This event is available to IAM users within the same account who have permissions to access and use shareable events."

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

The screenshot shows the AWS Lambda Test interface. At the top, a green checkmark icon indicates "Executing function: succeeded". Below it, a "Details" section shows the last 4 KB of the execution log, which contains the following JSON response:

```
{  
  "statusCode": 200,  
  "body": "\"Hey, This is Shraeyaa and this is my AWS lambda function\""  
}
```

Below the log, there is a "Summary" table with the following data:

Code SHA-256	Execution time
hfjfj/XFj8MQZGbFS6Jnrb8wkwPugSbSHesMiDX wWVc=	51 seconds ago
Request ID	Function version
f49f6e23-8323-4c24-b4a7-ad3125f7a44e	\$LATEST
Init duration	Duration
81.22 ms	2.89 ms
Billed duration	Resources configured
3 ms	128 MB

At the bottom, the "Test" tab is selected in the navigation bar. The "Execution result" panel shows the status "Succeeded" and the response body again. The "Function Logs" panel displays the log entries:

```
START RequestId: 3bc969c4-1868-41c7-ac84-d3c177bb1678 Version: $LATEST  
END RequestId: 3bc969c4-1868-41c7-ac84-d3c177bb1678  
REPORT RequestId: 3bc969c4-1868-41c7-ac84-d3c177bb1678 Duration: 1.24 ms Bi:  
Request ID  
3bc969c4-1868-41c7-ac84-d3c177bb1678
```

Conclusion:

AWS Lambda is a serverless computing service that allows you to run code without managing servers, making it highly scalable, cost-effective, and easy to use. It automatically manages the compute resources, executes your code in response to specific events such as API calls, file uploads, or database updates, and scales based on the demand. The workflow of AWS Lambda involves defining a function with specific logic, configuring triggers that will invoke the function, and setting permissions to control access. Lambda supports multiple programming languages, including Python, Java, and Node.js, enabling developers to choose the best fit for their applications. Creating your first Lambda function is straightforward: you write the code, define triggers, and deploy, allowing you to quickly build and run applications without the overhead of managing infrastructure. This simplicity and flexibility make AWS Lambda an excellent tool for building modern, event-driven applications.

Advance Devops-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

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
US East (N. Virginia) us-east-1

Bucket type | [Info](#)

General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name | [Info](#)

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#) ↗

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.
[Choose bucket](#)

Format: s3://bucket/prefix

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

[View details](#) X

[General purpose buckets](#) [Directory buckets](#)

General purpose buckets (3) [Info](#) All AWS Regions

[Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Buckets are containers for data stored in S3.

< 1 > ⚙

Name	AWS Region	IAM Access Analyzer	Creation date
codepipeline-eu-north-1-117394251014	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	August 24, 2024, 15:43:08 (UTC+05:30)
elasticbeanstalk-eu-north-1-022499027707	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	August 24, 2024, 14:36:38 (UTC+05:30)
shraeyaalambdabucket	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 20, 2024, 15:04:51 (UTC+05:30)

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

Lambda > Functions > shraeyaaimageloader

shraeyaaimageloader

Throttle Copy ARN Actions ▾

▼ Function overview [Info](#)

[Export to Application Composer](#) [Download ▾](#)

Diagram [Template](#)

 shraeyaa
imagine
loader

 Layers (0)

+ Add trigger + Add destination

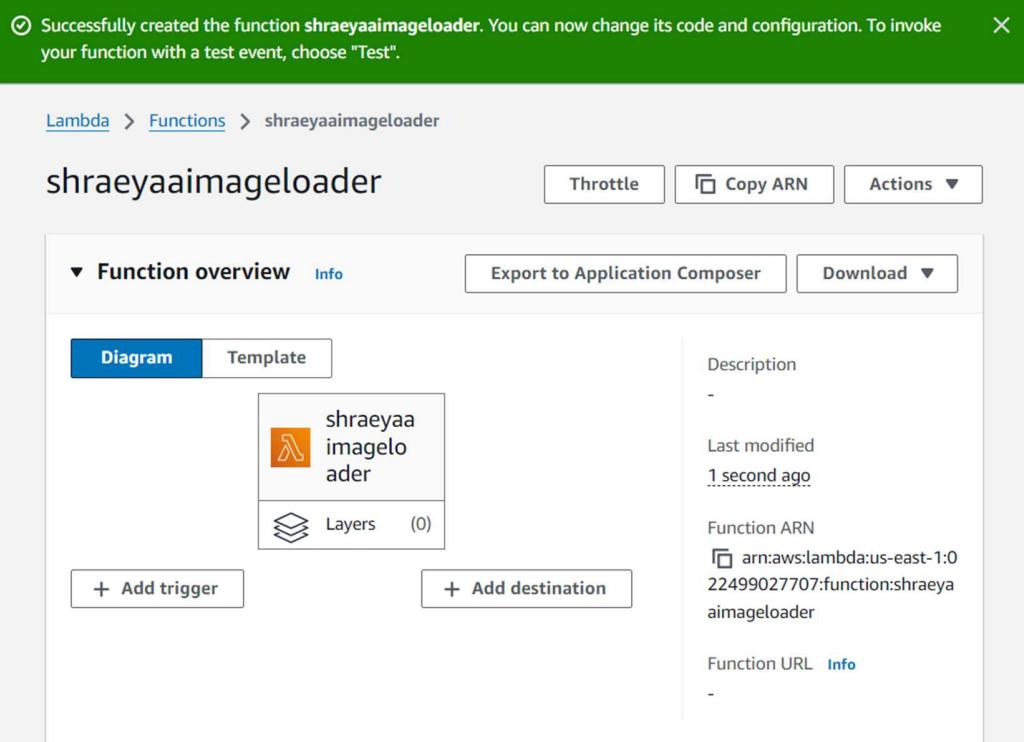
Description -

Last modified 1 second ago

Function ARN [arn:aws:lambda:us-east-1:22499027707:function:shraeyaaimageloader](#)

Function URL [Info](#)

-



✓ Successfully updated the function shraeyaaimageloader.

Code source [Info](#)

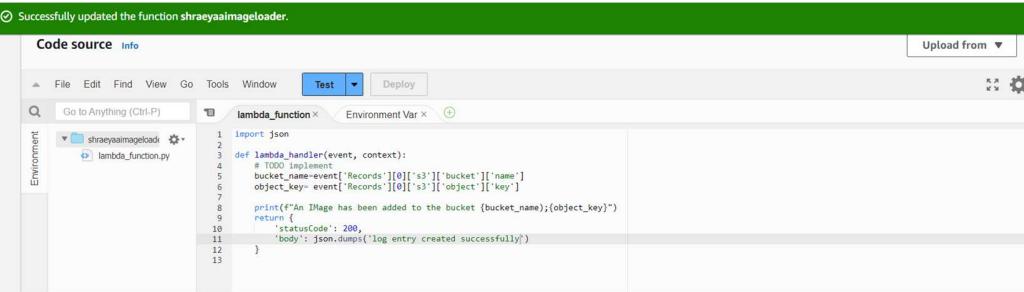
File Edit Find Go Tools Window Test Deploy

Upload from ▾

Environment

lambda_function Environment Var

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



Lambda > Add triggers

Add trigger

Trigger configuration [Info](#)

S3 aws asynchronous storage

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

s3/shraeyaalambdabucket

Use: "s3/shraeyaalambdabucket"

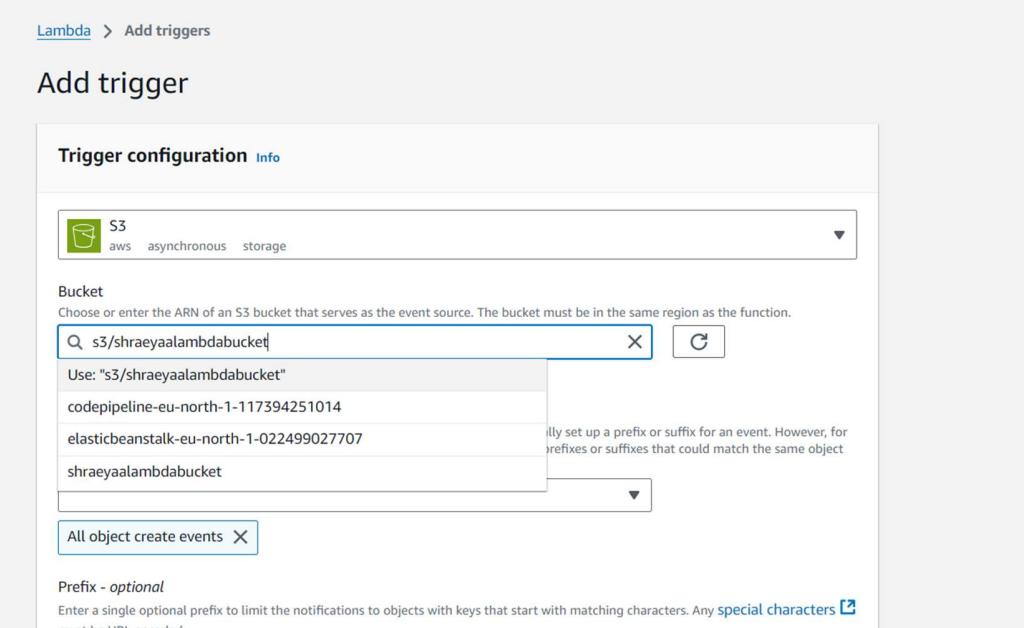
codepipeline-eu-north-1-117394251014

elasticbeanstalk-eu-north-1-022499027707

shraeyaalambdabucket

All object create events

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



shraeyaaimageloader

Throttle Copy ARN Actions ▾

The trigger shraeyaaalambdabucket was successfully added to function shraeyaaimageloader. The function is now receiving events from the trigger. X

Function overview Info Export to Application Composer Download ▾

Diagram Template

shraeyaa imageloader

Layers (0)

S3 + Add destination + Add trigger

Description -

Last modified 6 minutes ago

Function ARN arn:aws:lambda:us-east-1:22499027707:function:shraeyaaimageloader

Function URL Info -

Code Test Monitor Configuration Aliases Versions

General configuration Triggers (1) Info

Fix errors Edit Delete Add trigger

Find triggers < 1 >

Trigger S3: shraeyaaalambdabucket arn:aws:s3:::shraeyaaalambdabucket

Details

- General configuration
- Triggers
- Permissions
- Destinations
- Function URL
- Environment variables
- Tags
- VPC
- RDS databases
- Monitoring and

The screenshot shows the AWS Lambda Resource-based policy statements interface. At the top, there's a search bar and navigation links for 'machines' and 'N. Virginia'. The main area displays a table titled 'Resource-based policy statements (1) [Info](#)'. The table has columns: Statement, Principal, Conditions, and Action. A single row is shown: 'lambda-5...' with principal 's3.amazonaws.com', condition 'StringEquals', and action 'lambda:In...'. Below the table is a section titled 'Auditing and compliance'.

Statement	Principal	Conditions	Action
lambda-5...	s3.amazonaws.com	StringEquals	lambda:In...

The screenshot shows the AWS S3 Bucket details page for 'shraeyaalambdabucket'. The left sidebar includes links for Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings, Storage Lens, Dashboards, Storage Lens groups, AWS Organizations settings, and Feature spotlight (7). The main content area shows the bucket name 'shraeyaalambdabucket' with an 'Info' link. It features tabs for Objects, Properties, Permissions, Metrics, and Metrics. The 'Objects' tab is selected, showing a table with 0 objects. The table has columns: Name, Type, Last modified, and Size. Buttons for Copy S3 URI, Copy URL, Download, Open, Delete, Actions, Create folder, and Upload are available. A search bar for 'Find objects by prefix' and a pagination area are also present.

Name	Type	Last modified	Size
(empty)			

Upload Info

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

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

Files and folders (1 Total, 31.9 KB)

All files and folders in this table will be uploaded.

[Remove](#)

[Add files](#)

[Add folder](#)

[Find by name](#)

< 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	download (15).jpg	-	image/jpeg	31.9 KB

Destination Info

Destination

[s3://shraeyaalambdabucket](#)

Upload succeeded

View details below.

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

Summary

Destination
[s3://shraeyaalambdabucket](#)

Succeeded

1 file, 31.9 KB (100.00%)

Failed

0 files, 0 B (0%)

[Files and folders](#)

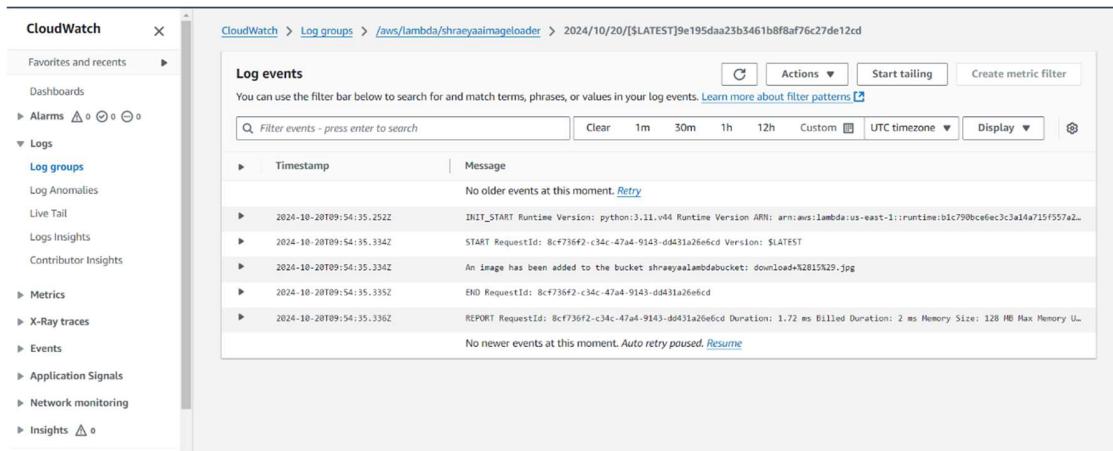
[Configuration](#)

Files and folders (1 Total, 31.9 KB)

[Find by name](#)

< 1 >

Name	Folder	Type	Size	Status	Error
download (...)	-	image/jpeg	31.9 KB	<input checked="" type="checkbox"/> Succeeded	-



Conclusion:

Integrating AWS Lambda with S3 allows for real-time, automated processing of events such as file uploads. In this example, a Lambda function is configured to log a message whenever an image is added to a specific S3 bucket. This setup demonstrates the power and flexibility of serverless computing by automating tasks without requiring manual intervention or server management. By leveraging AWS Lambda, developers can efficiently handle event-driven workflows, reduce operational overhead, and quickly deploy scalable solutions that respond to specific actions within cloud environments.