Thadomal Shahani Engineering College

Bandra (W.), Mumbai - 400 050.

CERTIFICATE

Certify that Mr./~~Miss~~ AYUSH SANJAY SHARMA

of I.T Department, Semester V with

Roll No. 117 has completed a course of the necessary

experiments in the subject ADVANCE DEVOPS LAB under my

supervision in the **Thadomal Shahani Engineering College**

Laboratory in the year 2025 - 2026

Monday
09/10/25

Teacher In- Charge

Head of the Department

Date 09/10/25

Principal

THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

CONTENTS

Assignment-1

Aim- To study Advanced DevOps,its tools,features,benefits and principles.

Theory-

What is advanced DevOps-

Advanced DevOps represents a significant step up from the foundational principles of DevOps. While traditional DevOps focuses on automating the software delivery pipeline and fostering collaboration between development and operations teams, advanced DevOps emphasizes a more comprehensive and holistic approach to software delivery, integrating a broader range of practices and technologies throughout the entire software delivery lifecycle.

Tools Used in Advanced DevOps

There are many tools used in Advanced DevOps, grouped by their functions:

CI/CD Tools (Continuous Integration and Continuous Delivery/Deployment):

Tools like Jenkins,AWS, GitLab CI, GitHub Actions, Argo CD, Tekton, and Spinnaker automate the build, test, and deployment processes. They help push code into production more frequently and reliably.

Infrastructure as Code (IaC):

Tools like Terraform, Pulumi, AWS CloudFormation, Ansible, Chef, and Puppet allow infrastructure to be managed with code. This means servers, networks, databases, and other resources can be created and destroyed automatically using configuration files.

Containerization and Orchestration:

Docker is used to package applications into containers. Kubernetes orchestrates and manages those containers at scale. Helm is used to package Kubernetes applications, while Istio and Linkerd provide service mesh capabilities like traffic routing and security between microservices.

Monitoring and Observability:

Monitoring tools like Prometheus, Grafana, Datadog, New Relic, and the ELK Stack (Elasticsearch, Logstash, Kibana) provide real-time insight into system health, application performance, and logs.

Security and Compliance (DevSecOps):

Tools such as Snyk, Aqua Security, Trivy, and HashiCorp Vault help integrate security into the DevOps pipeline. Open Policy Agent (OPA) is used to enforce policies like access control or configuration standards automatically.

Collaboration and Project Management:

Platforms like Slack, Jira, Confluence, Microsoft Teams, and Trello are used to manage communication, track issues, and document development processes across teams.

Key Features of Advanced DevOps

Advanced DevOps includes many features that go beyond the basics:

GitOps is a way to manage infrastructure and application deployment using Git as the single source of truth. This makes rollbacks, audits, and collaboration easier.

Progressive Delivery includes strategies like blue-green deployments, canary releases, and feature flags to minimize risk during software rollouts.

Self-Healing Systems automatically detect and recover from failures using health checks, auto-scaling, and rollback mechanisms.

Immutable Infrastructure means replacing infrastructure entirely with a new version rather than modifying the existing one. This reduces errors and makes systems more predictable.

Policy as Code allows compliance and security policies to be defined and enforced using code, ensuring consistency and reducing human error.

Chaos Engineering involves deliberately injecting failures into the system to test its resilience and improve system robustness. Tools like Chaos Monkey help simulate these failures.

AI and Machine Learning in DevOps help with predictive incident detection, smart alerts, anomaly detection, and optimizing CI/CD workflows.

Benefits of Advanced DevOps-

Faster Software Delivery: Advanced DevOps automates many manual processes like building, testing, and deploying code. This speeds up the release cycle, enabling teams to deliver new features and bug fixes much faster than traditional methods.

Higher Quality and Reliability: Automated testing and continuous monitoring catch bugs and issues early. With practices like canary releases and blue-green deployments, updates can be rolled out safely with minimal risk of downtime or errors.

Improved Collaboration: Advanced DevOps breaks down silos between development, operations, and security teams. Everyone works together using shared tools and processes, which improves communication, reduces misunderstandings, and speeds up problem-solving.

Scalability: Using infrastructure as code and container orchestration, organizations can easily scale their applications and infrastructure up or down based on demand. This flexibility helps handle traffic spikes smoothly without overprovisioning resources.

Better Security (DevSecOps): Security becomes an integral part of the development pipeline. Automated security scanning, policy enforcement, and secrets management reduce vulnerabilities and compliance risks.

Cost Efficiency: By automating routine tasks and optimizing infrastructure usage, Advanced DevOps reduces manual effort and lowers infrastructure costs. Cloud resource management tools help avoid waste and optimize spending.

Conclusion- Advanced DevOps transforms traditional software delivery by combining automation, collaboration, and security to enable faster, more reliable releases. It leverages modern tools and practices like CI/CD, infrastructure as code, and observability to improve scalability and resilience. Ultimately, Advanced DevOps empowers organizations to innovate rapidly while maintaining high quality and strong security.

LO Mapping-LO1

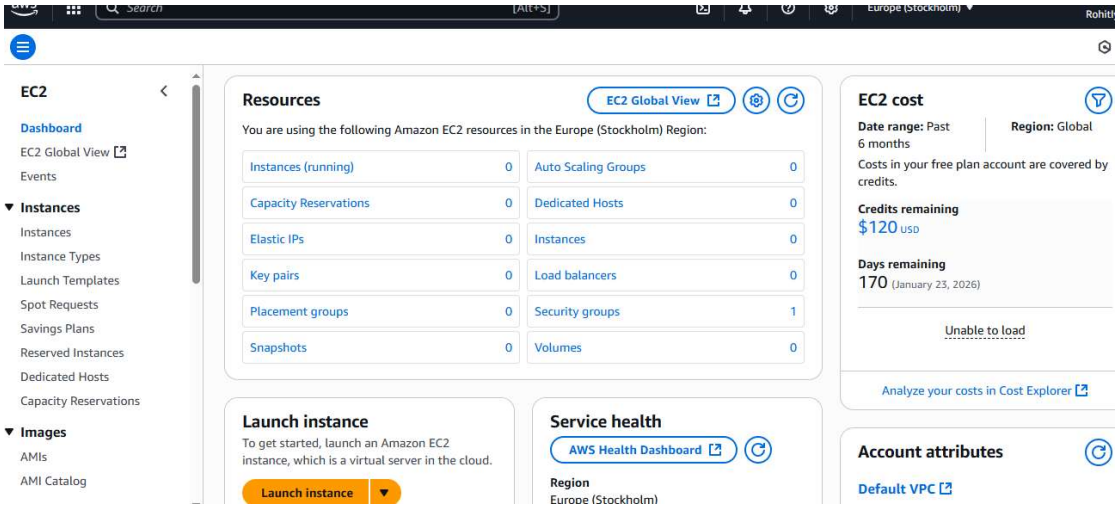
Assignment 2: To launch EC2 instance

Aim: To study and perform the setup of AWS EC2 service and launch an EC2 instance

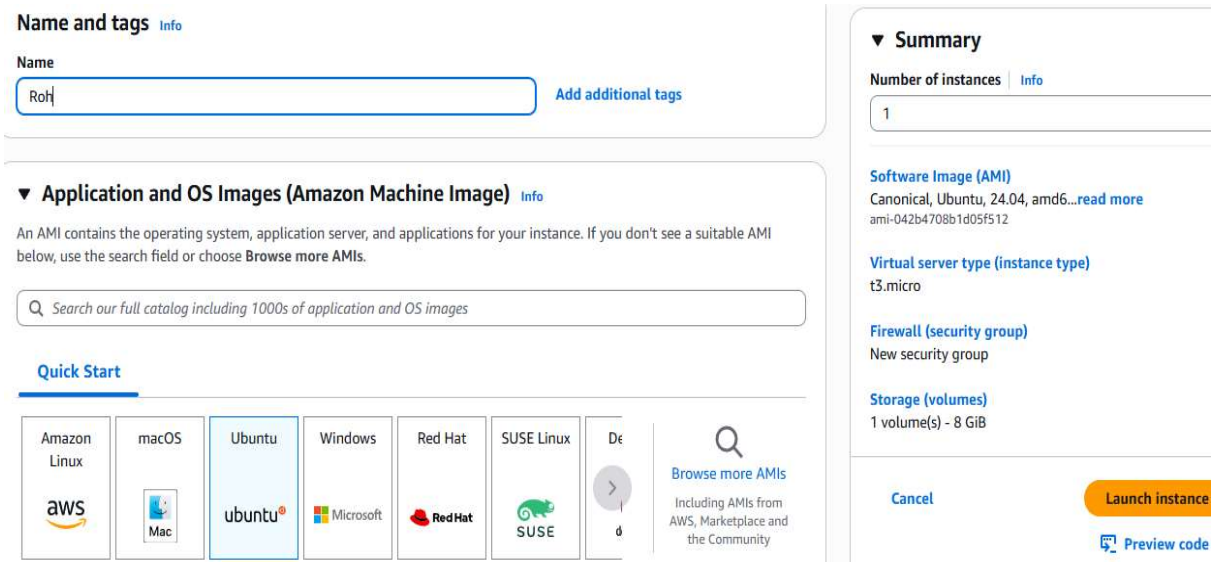
Theory: An EC2 instance in AWS is a virtualized compute resource running on Amazon's Elastic Compute Cloud, provisioned using Xen or Nitro hypervisors. It provides configurable vCPUs, RAM, storage through EBS or instance store, and network capacity within a chosen Availability Zone. Instances are launched from Amazon Machine Images and can run Linux or Windows environments. They integrate with AWS services like VPC, IAM, and Auto Scaling for secure and scalable deployments.

Steps:

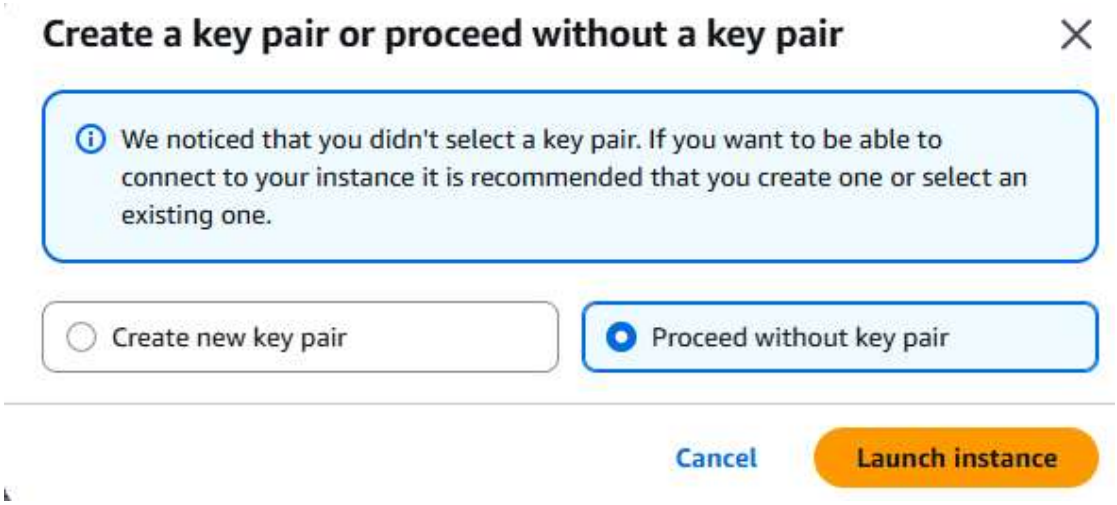
1)Sign in the AWS, Go on dashboard and select EC2, click on instances(running)



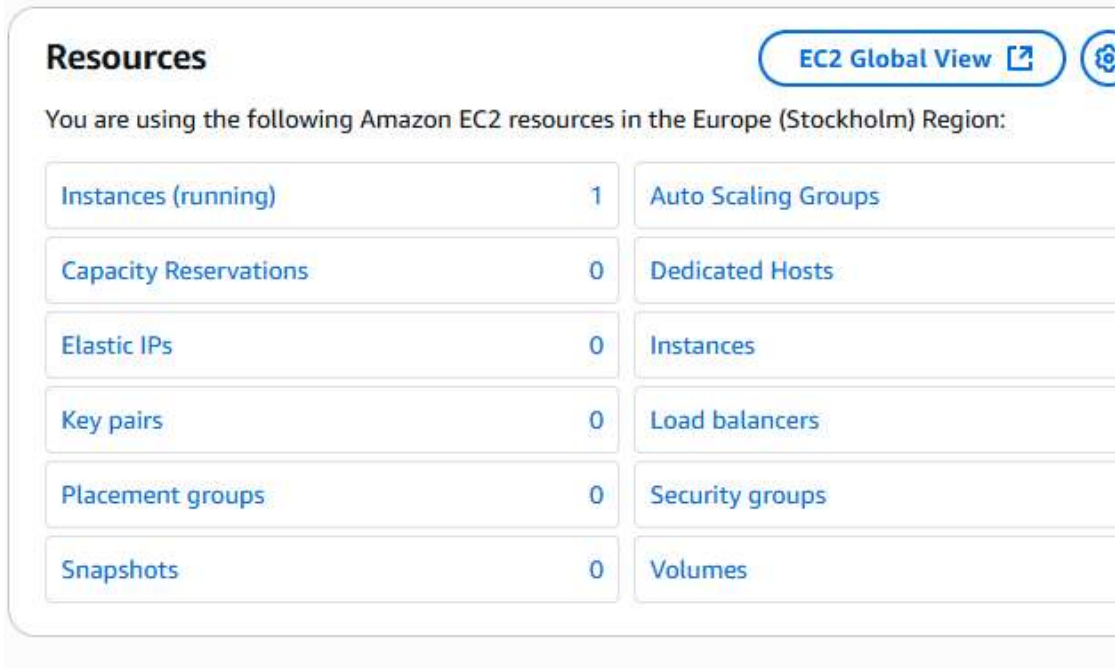
2) Select your desired Operating system and assign a name to your instance, then click on launch instance.

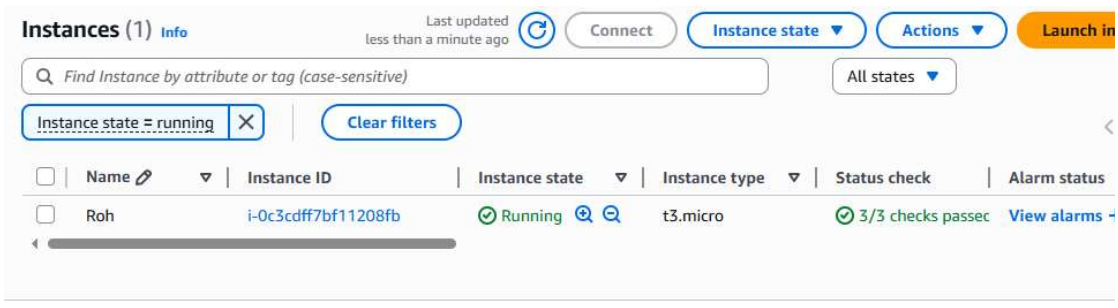


3) Proceed without key pair

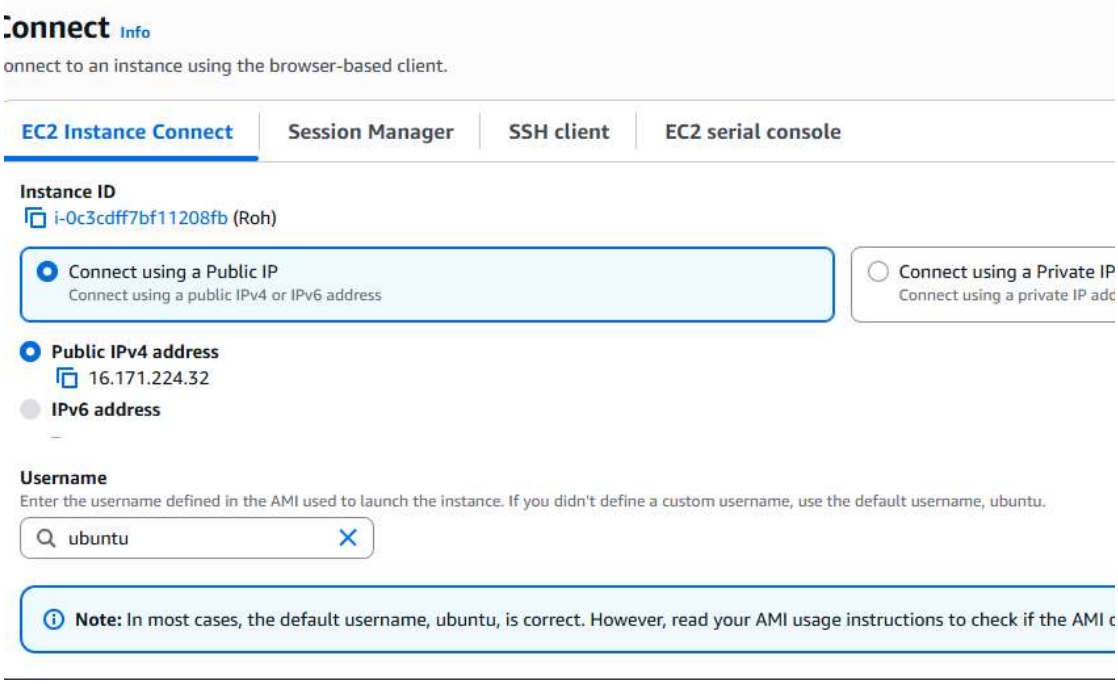


4) Click on the instance running and select connect option

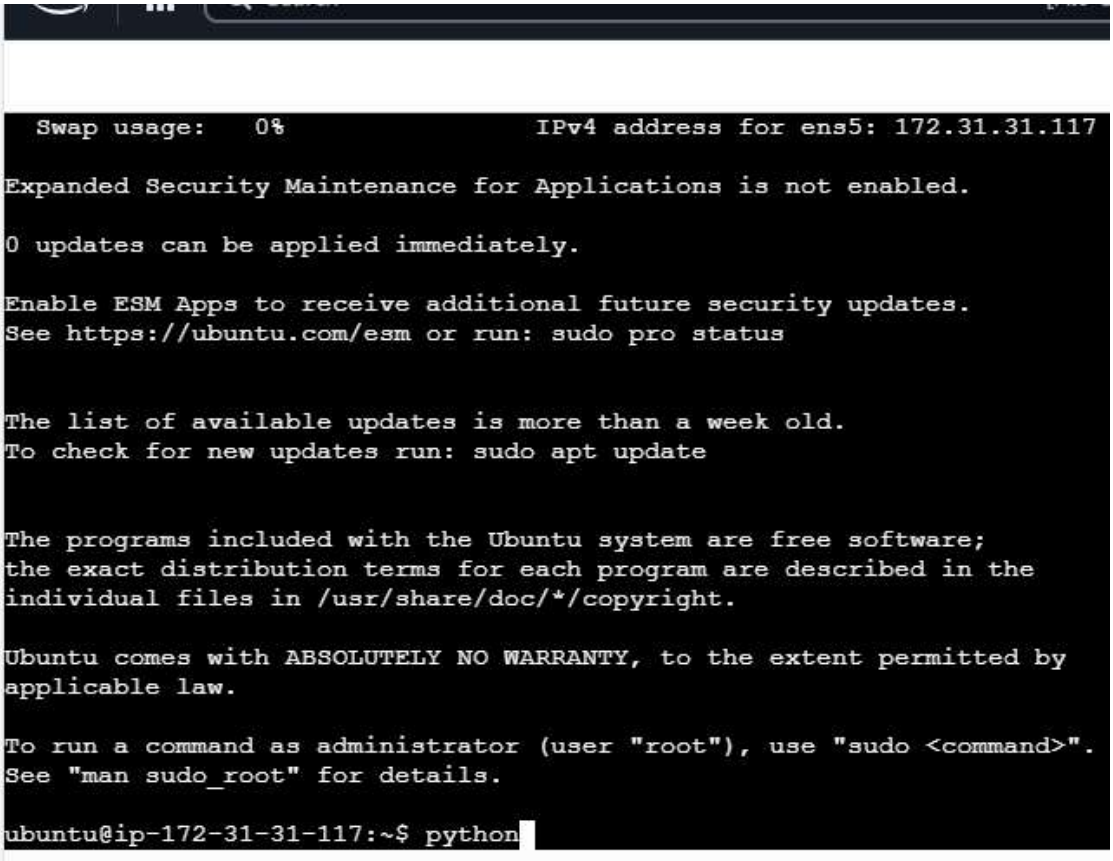




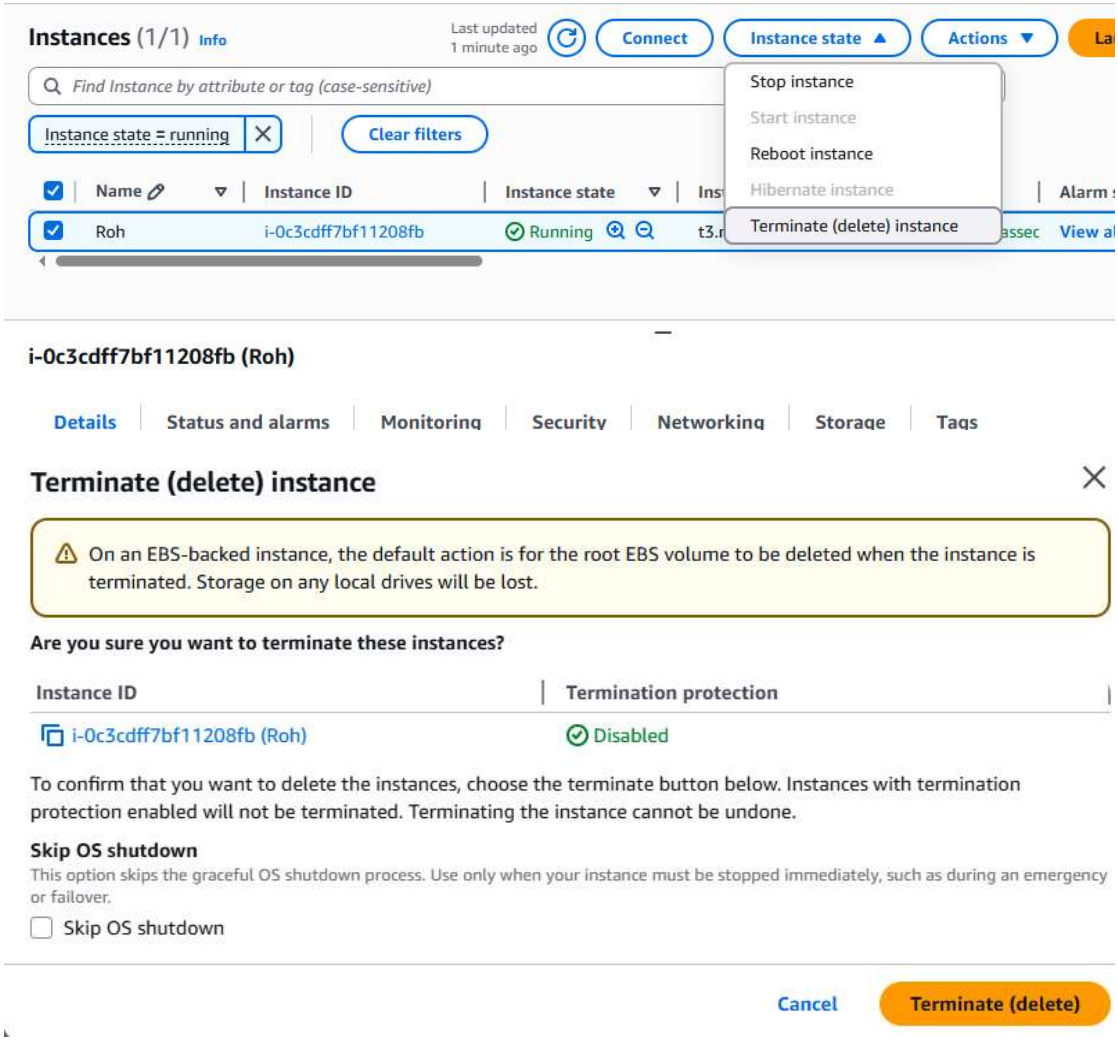
5) Select the following and assign a username



6) EC2 instance launched



7) Terminate the instance once done



Conclusion: In conclusion, launching an EC2 instance provides a flexible and scalable way to deploy applications in the cloud. With customizable configurations and integration with other AWS services, it enables efficient resource management and reliable performance for a wide range of workloads.

LO Mapping: LO1

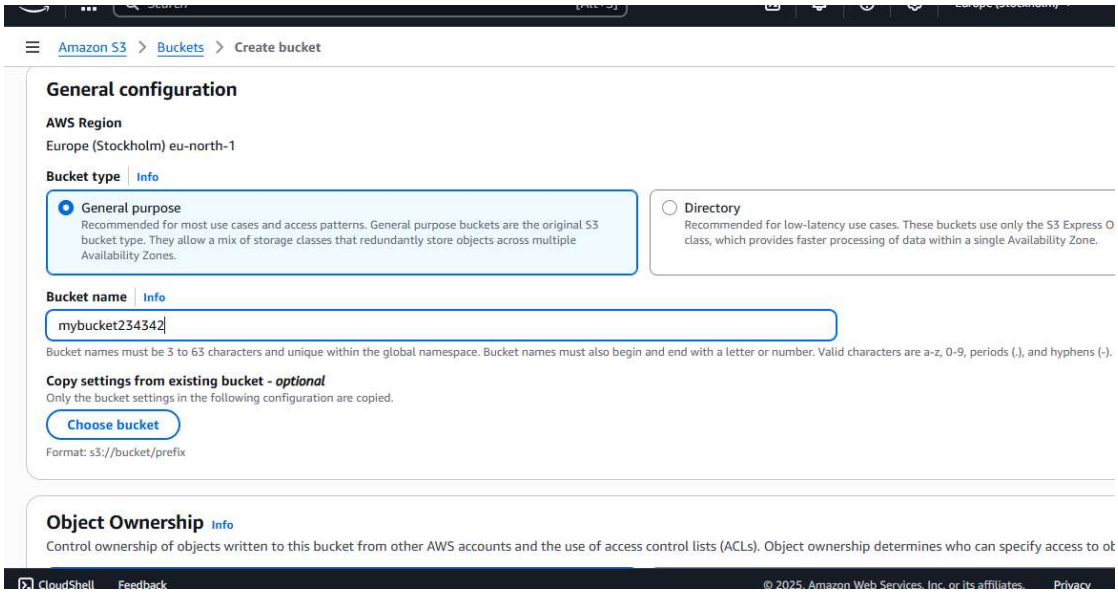
Assignment 3: S3 Bucket

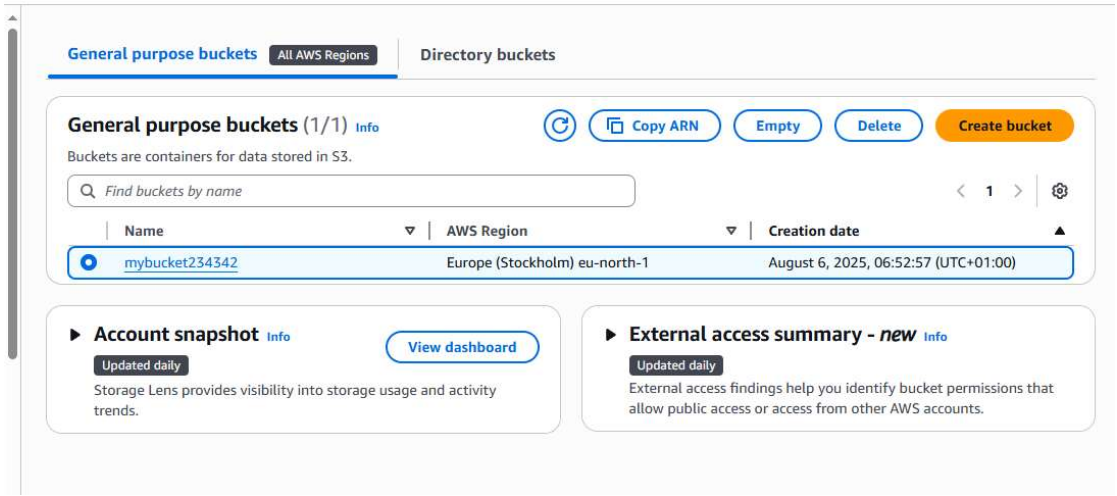
Aim: To study AWS S3 service and create a bucket for hosing static web application.

Theory: An S3 bucket in AWS is a storage container used to store and organize objects such as files, images, or backups in Amazon Simple Storage Service. It offers virtually unlimited storage capacity with high durability and availability. Data in S3 can be accessed over the internet and managed with permissions for security. It also supports features like versioning, lifecycle rules, and integration with other AWS services for data processing and distribution.

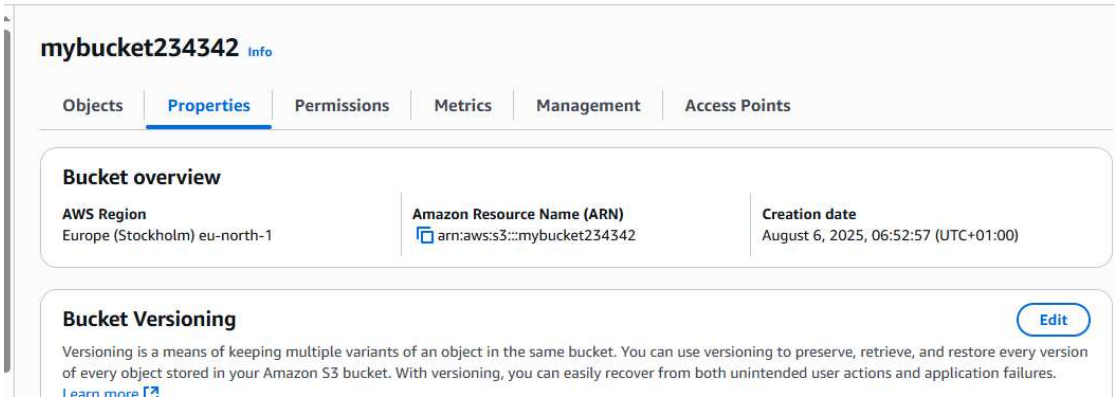
Steps:

1)Select S3 buckets in the dashboard and select on create bucket. Add a unique bucket name and proceed to create bucket

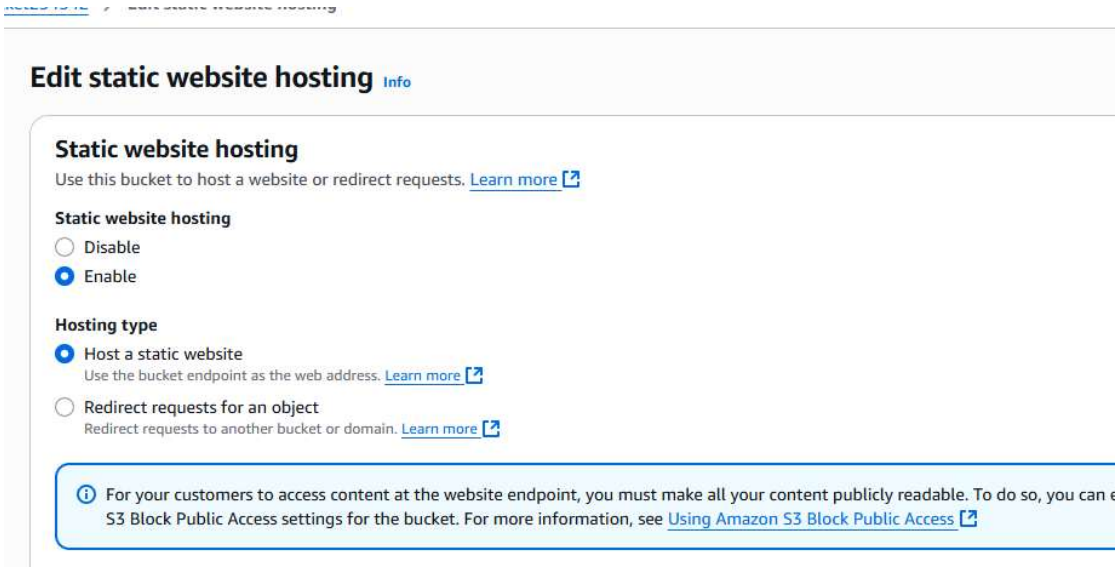




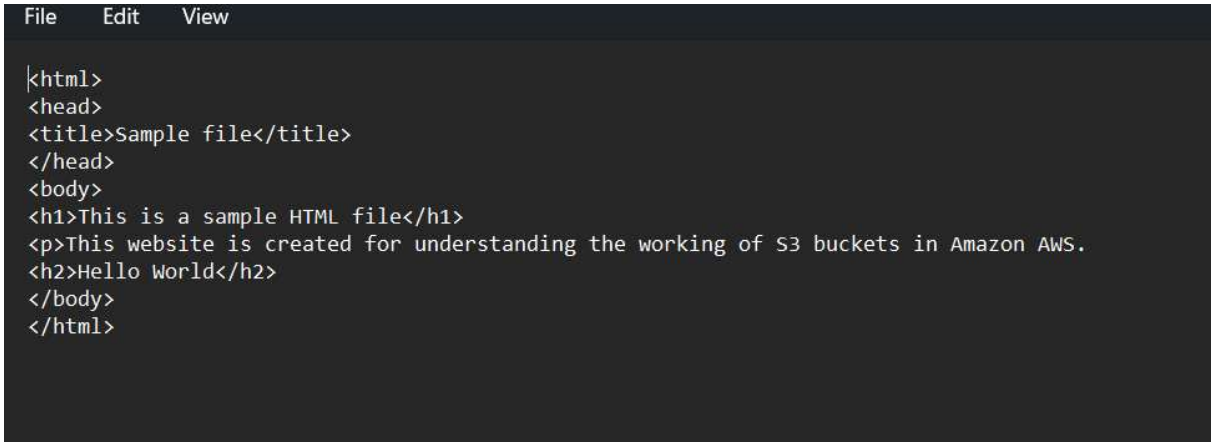
2)Go to properties

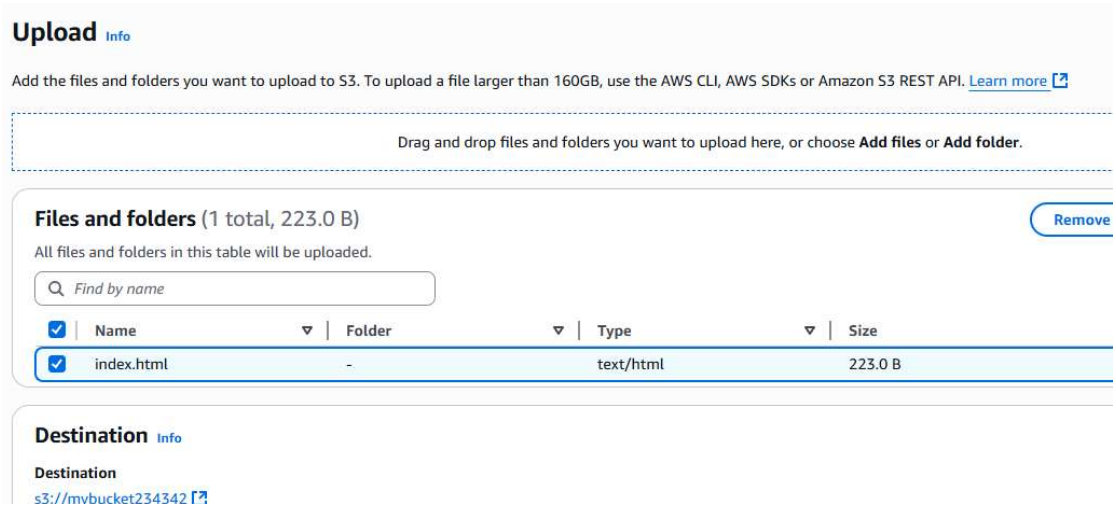


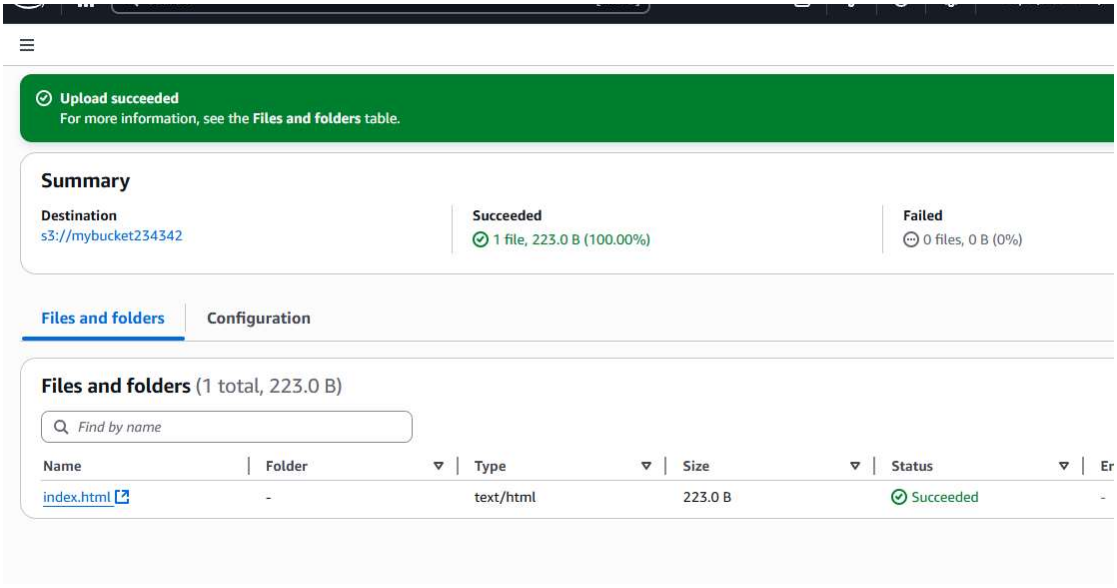
4)Enable static hosting

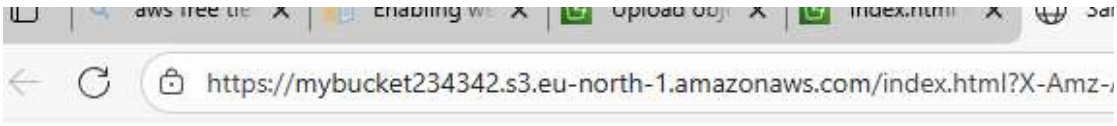


5)Create a HTML file and upload it









This is a sample HTML file

This website is created for understanding the working of S3 buckets in Amazon AWS.

Hello World

Conclusion: In conclusion, creating an S3 bucket to host a static website offers a simple, cost-effective, and highly available solution for delivering content over the internet. With minimal setup, it eliminates the need for managing servers while ensuring scalability and seamless integration with other AWS services. This makes it an ideal choice for hosting lightweight, static web applications or personal projects.

LO Mapping: LO1

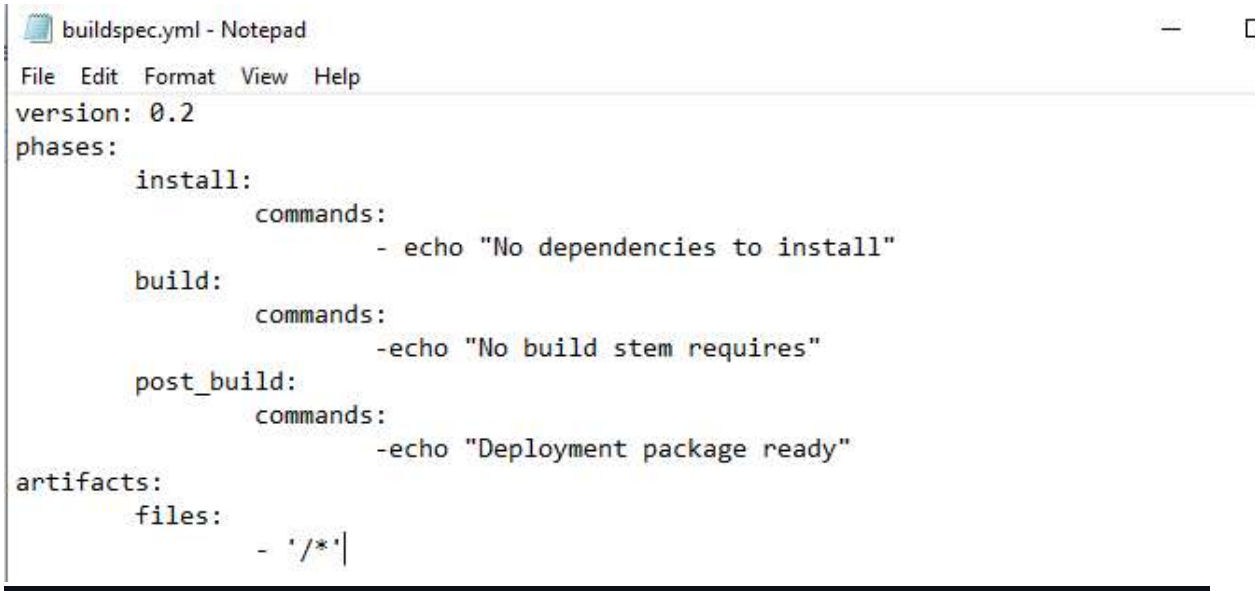
Assignment-4:CodePipeline

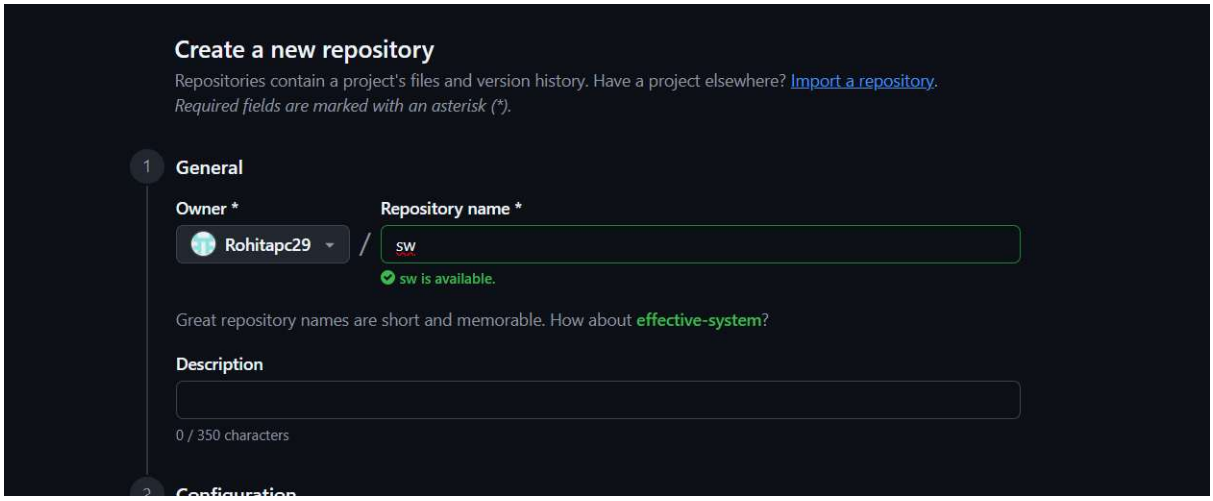
Aim: To study AWS CodePipeline and deploy web application using CodePipeline.

Theory: AWS CodePipeline is a fully managed CI/CD service that automates software release workflows. It connects source control, build tools, test suites, and deployment targets into a unified pipeline. Each stage in the pipeline triggers actions based on code changes or events. This enables faster, more reliable deployments while promoting DevOps best practices.

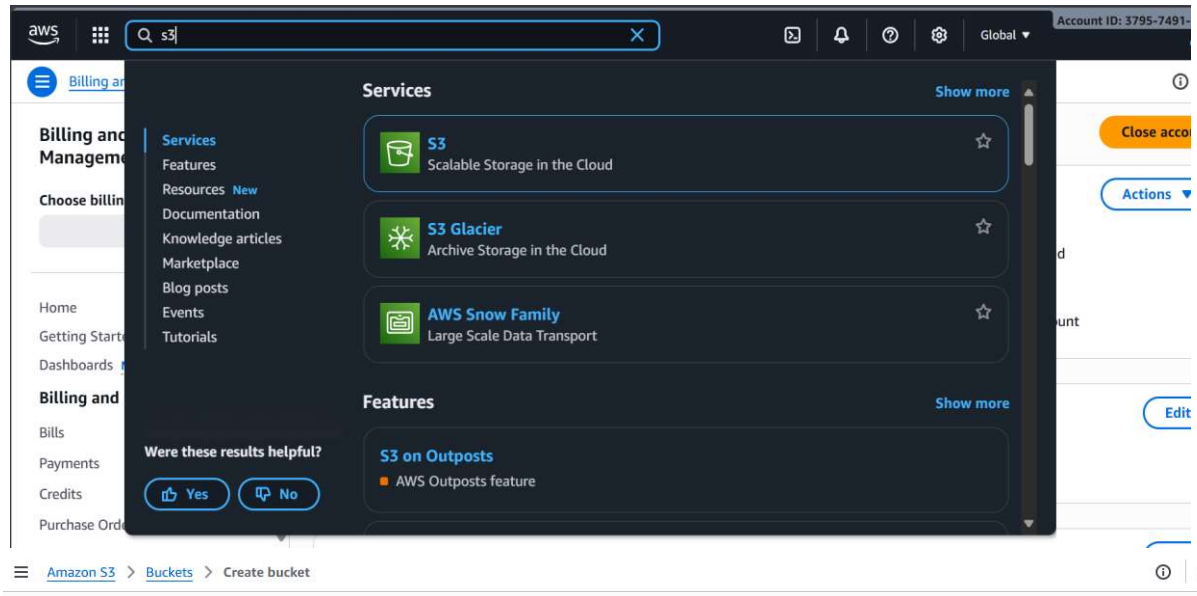
Steps:

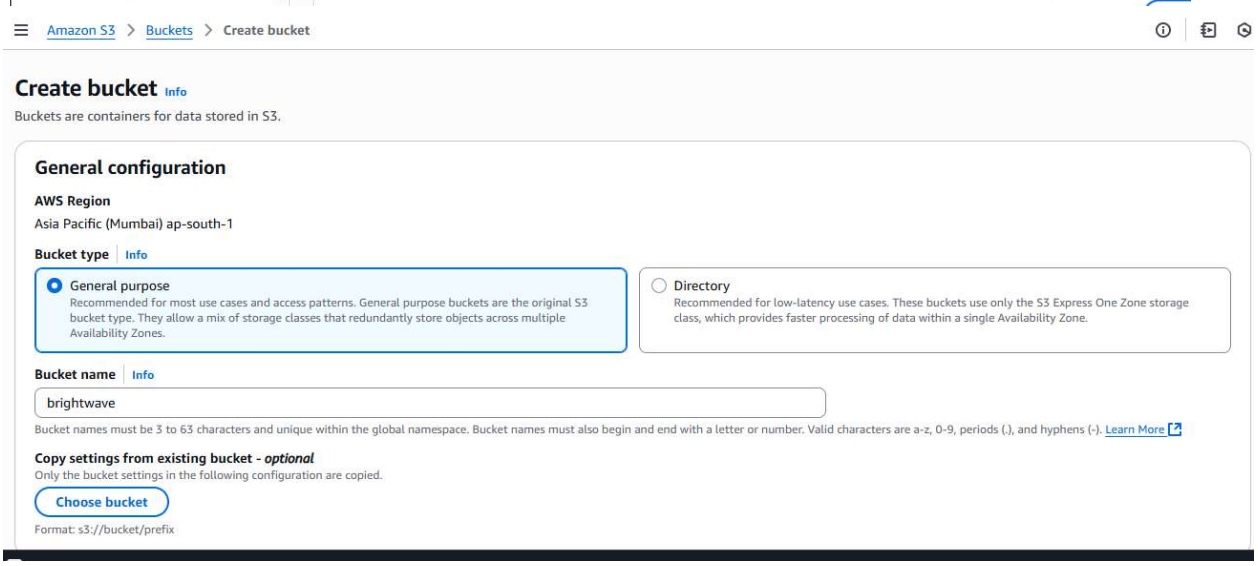
1)Create a YML file and





2)Create an S3 bucket





Block Public Access settings for this bucket

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

- [ ] **Block *all* public access**
  Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
  - [ ] **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
    S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
  - [ ] **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
    S3 will ignore all ACLs that grant public access to buckets and objects.
  - [ ] **Block public access to buckets and objects granted through *new* public bucket or access point policies**
    S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
  - [ ] **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
    S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

- [x] I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning

- ( ) Disable
- (•) Enable

Tags - *optional* (0)

You can use bucket tags to track storage costs and organize buckets. Learn more

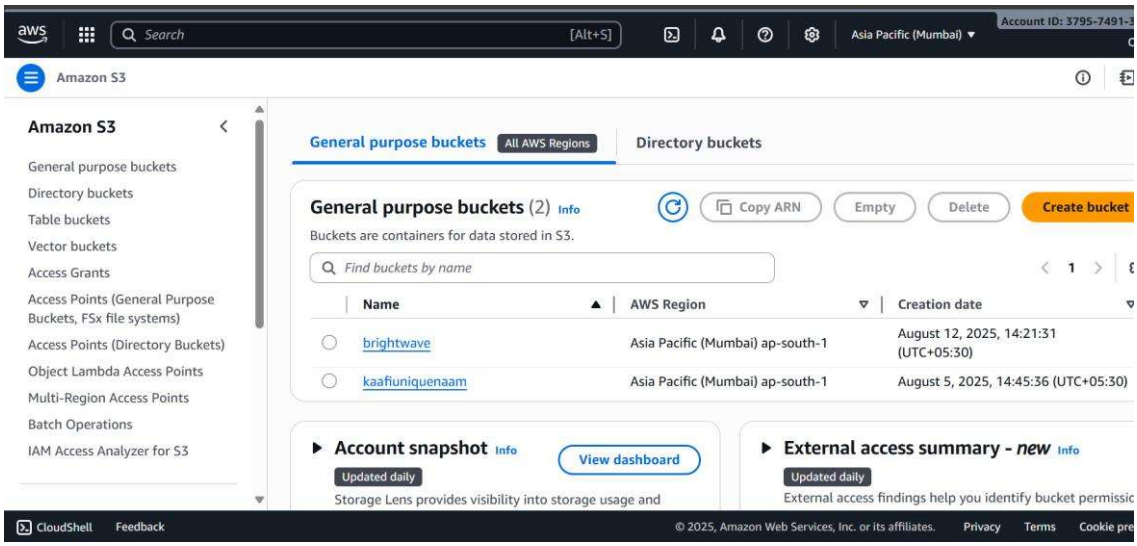
No tags associated with this bucket.

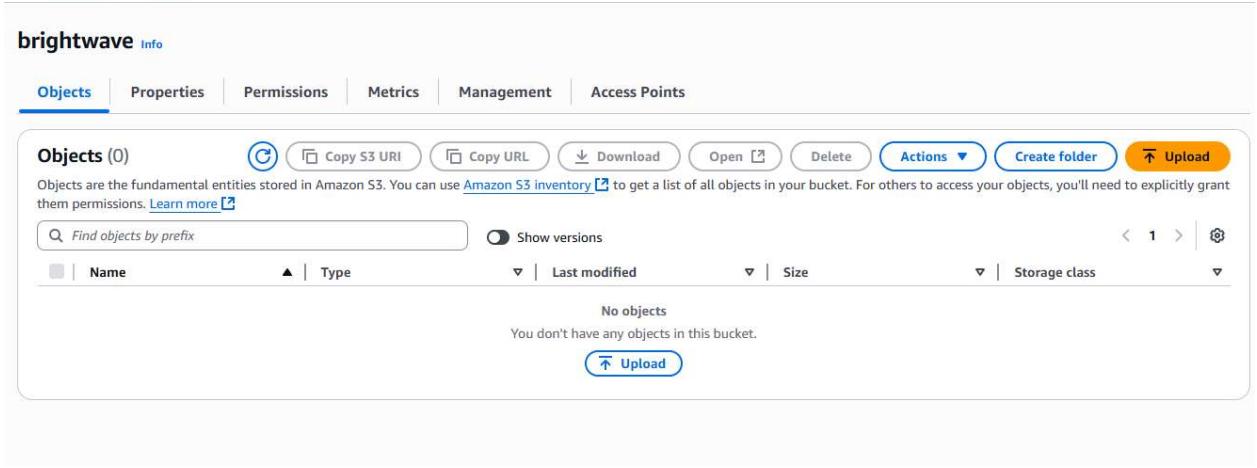
Add new tag

You can add up to 50 tags.

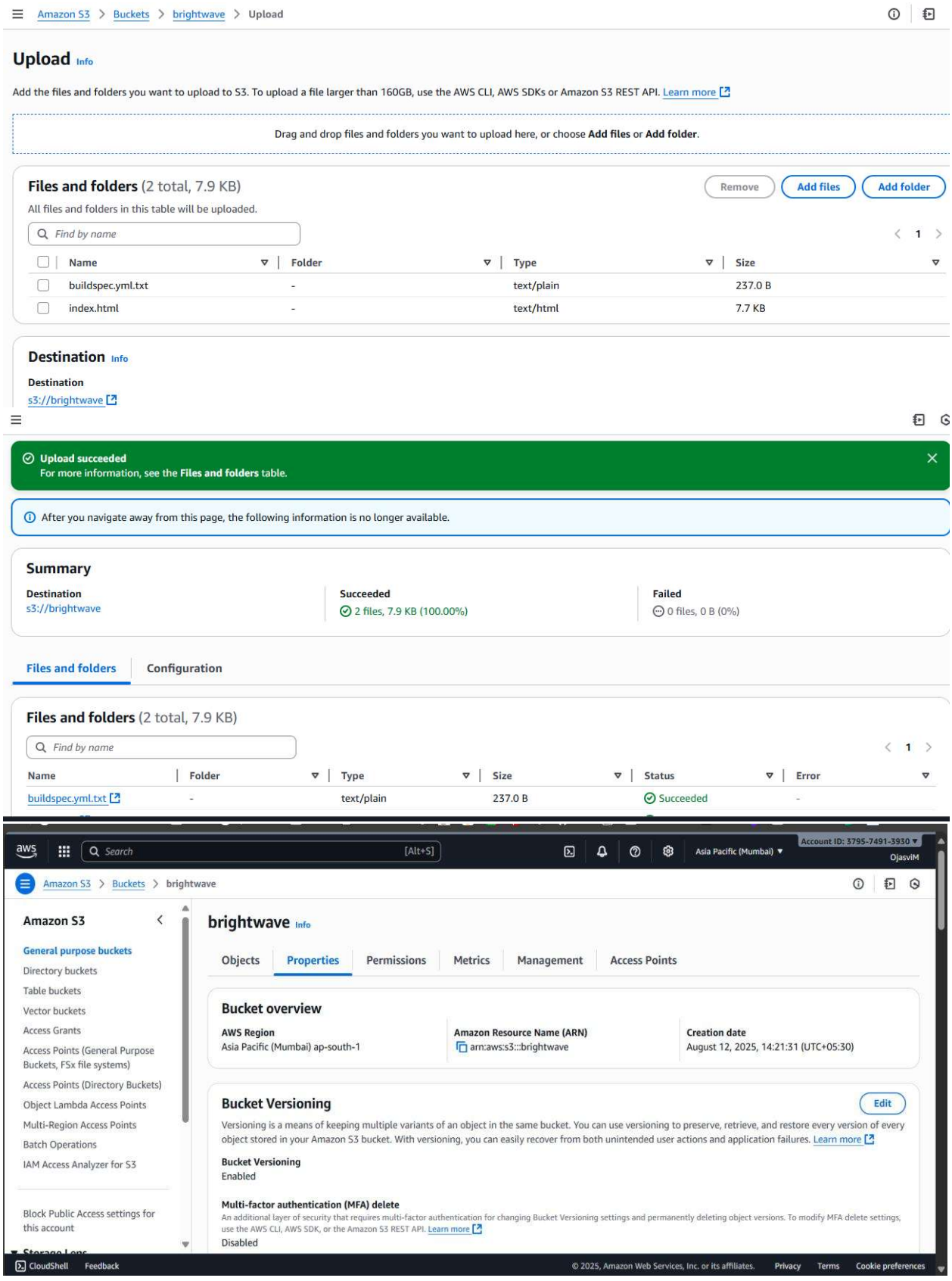
Default encryption Info

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

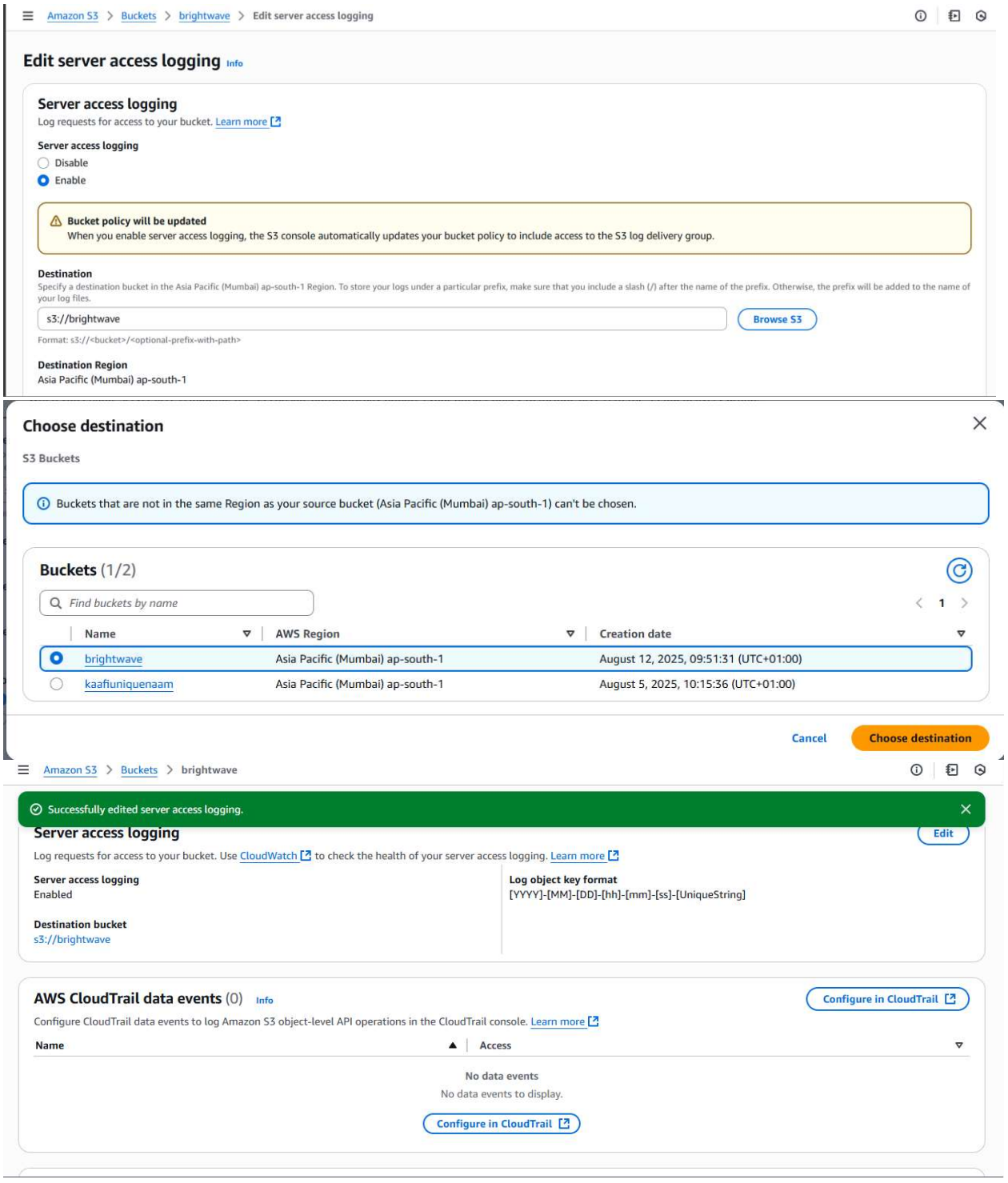




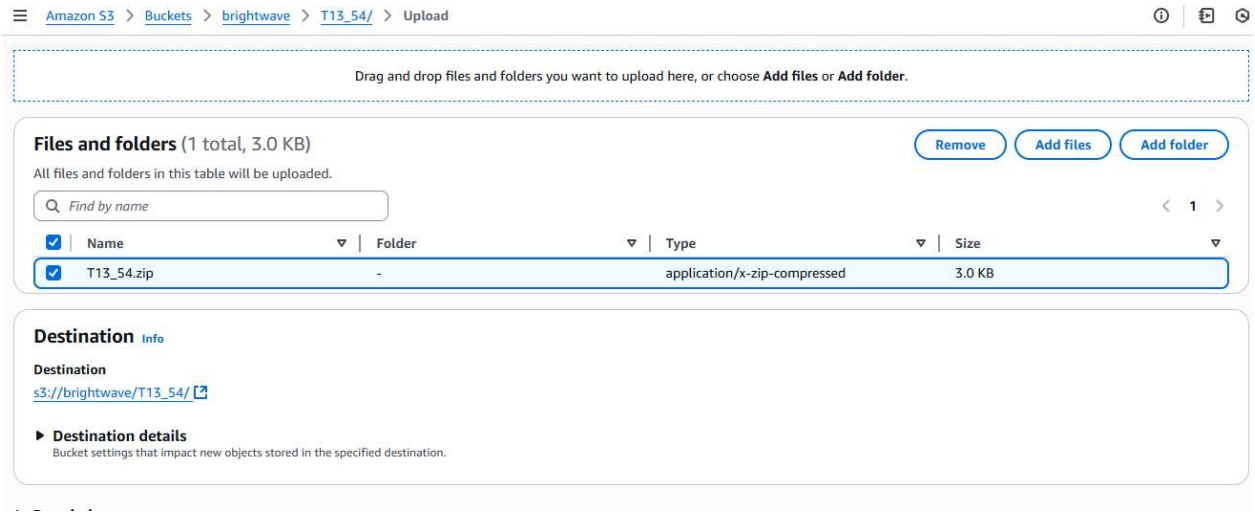
3)Upload the yml and html files to the bucket

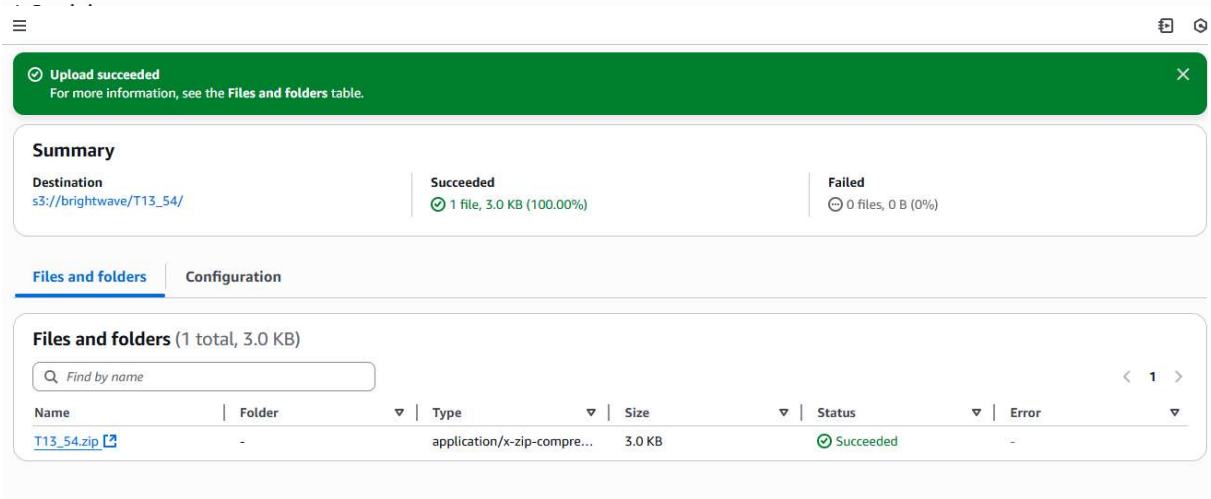


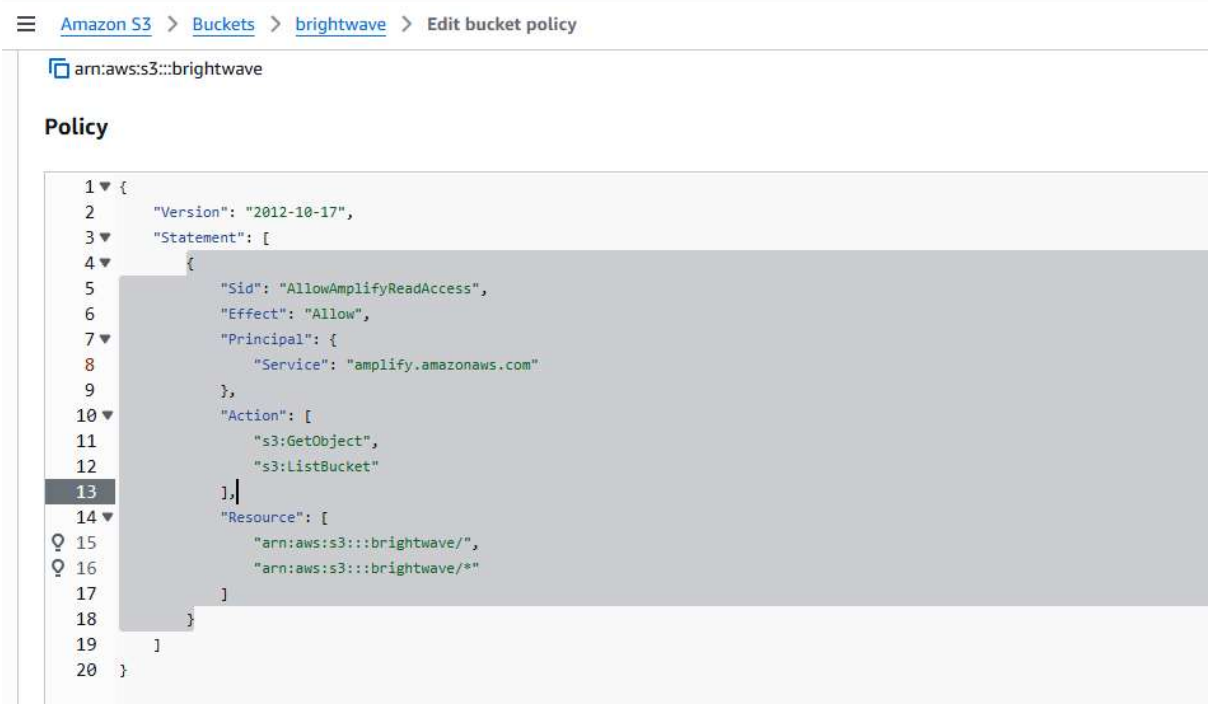
4)Edit server access logging and choose destination appropriately

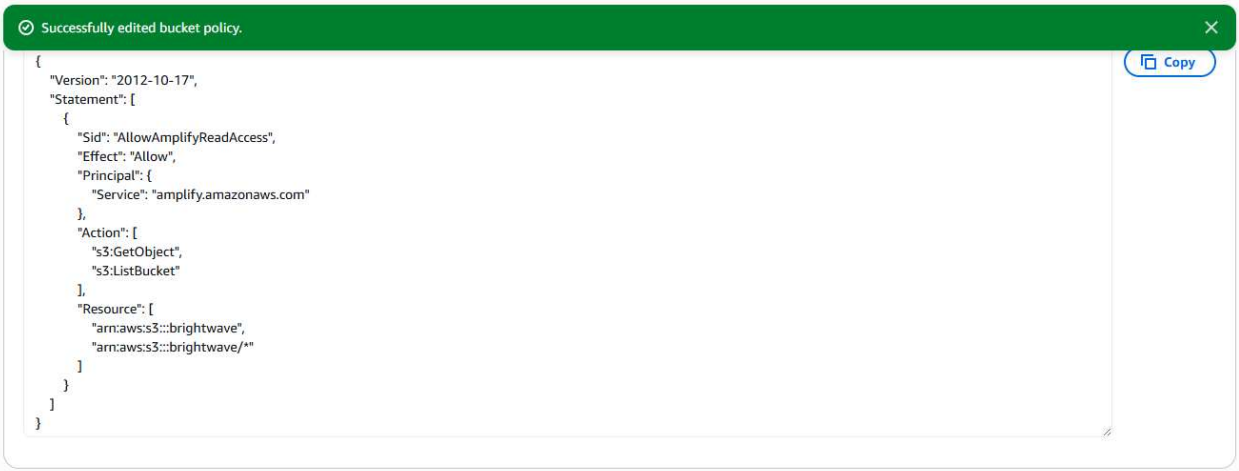

Amazon S3 > Buckets > brightwave > Edit server access logging
Edit server access logging Info
Server access logging
Log requests for access to your bucket. Learn more
Server access logging
Disable
Enable
Bucket policy will be updated
When you enable server access logging, the S3 console automatically updates your bucket policy to include access to the S3 log delivery group.
Destination
Specify a destination bucket in the Asia Pacific (Mumbai) ap-south-1 Region. To store your logs under a particular prefix, make sure that you include a slash (/) after the name of the prefix. Otherwise, the prefix will be added to the name of your log files.
s3://brightwave
Browse S3
Format: s3://<bucket>/<optional-prefix-with-path>
Destination Region
Asia Pacific (Mumbai) ap-south-1
Choose destination
S3 Buckets
Buckets that are not in the same Region as your source bucket (Asia Pacific (Mumbai) ap-south-1) can't be chosen.
Buckets (1/2)
Find buckets by name
1
Name
AWS Region
Creation date
brightwave
Asia Pacific (Mumbai) ap-south-1
August 12, 2025, 09:51:31 (UTC+01:00)
kaafiuniquenaam
Asia Pacific (Mumbai) ap-south-1
August 5, 2025, 10:15:36 (UTC+01:00)
Cancel
Choose destination
Amazon S3 > Buckets > brightwave
Successfully edited server access logging.
Server access logging
Edit
Log requests for access to your bucket. Use CloudWatch to check the health of your server access logging. Learn more
Server access logging
Enabled
Destination bucket
s3://brightwave
Log object key format
[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
AWS CloudTrail data events (0) Info
Configure in CloudTrail
Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. Learn more
Name
Access
No data events
No data events to display.
Configure in CloudTrail

5)Upload the folder and edit bucket policy

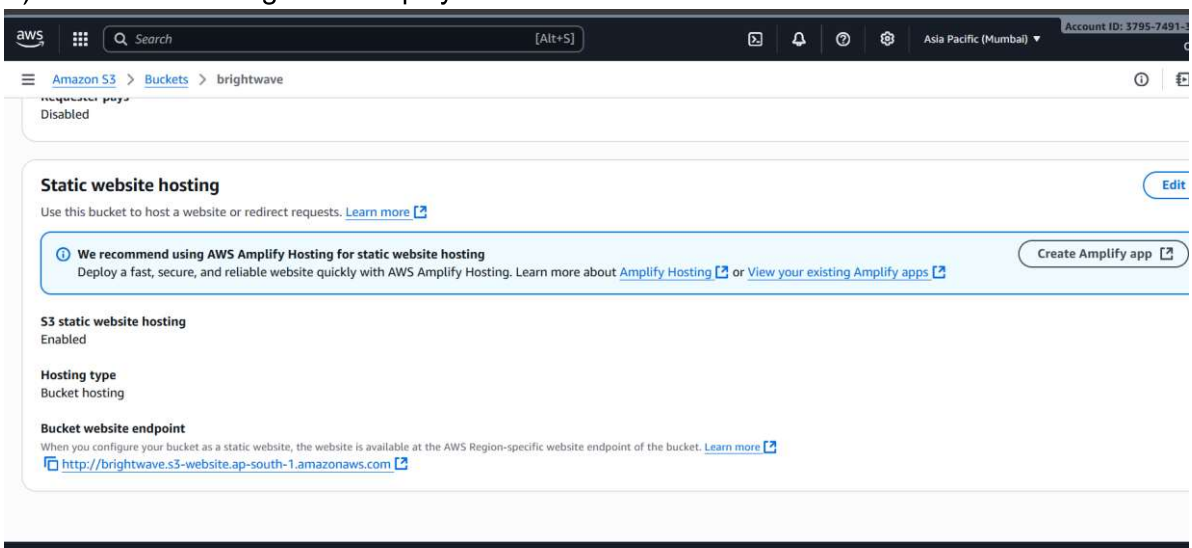


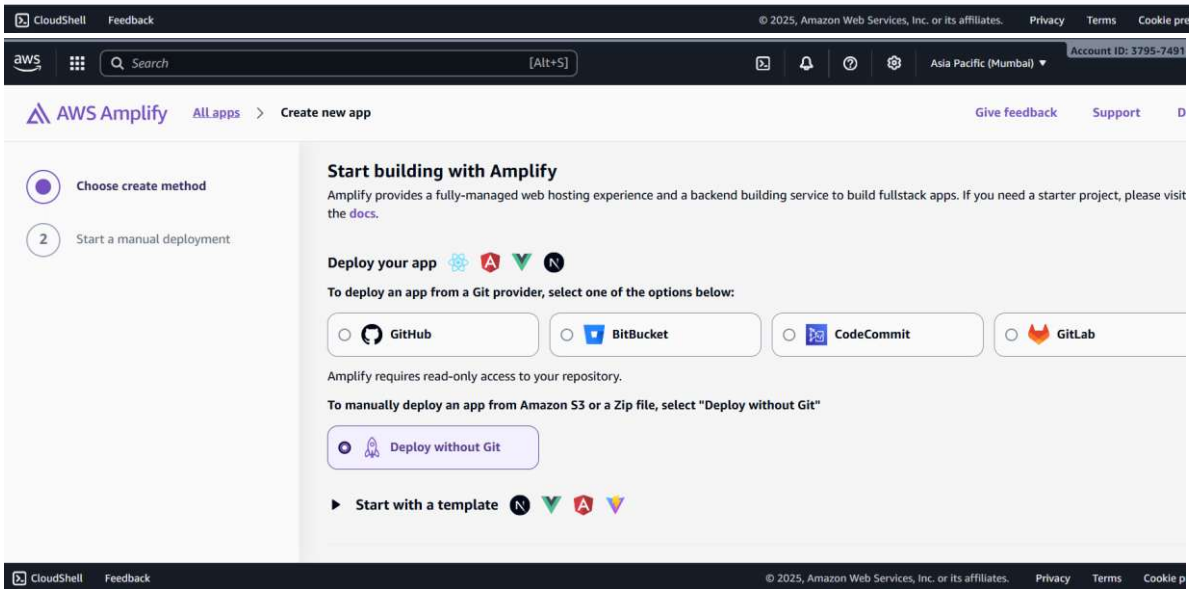


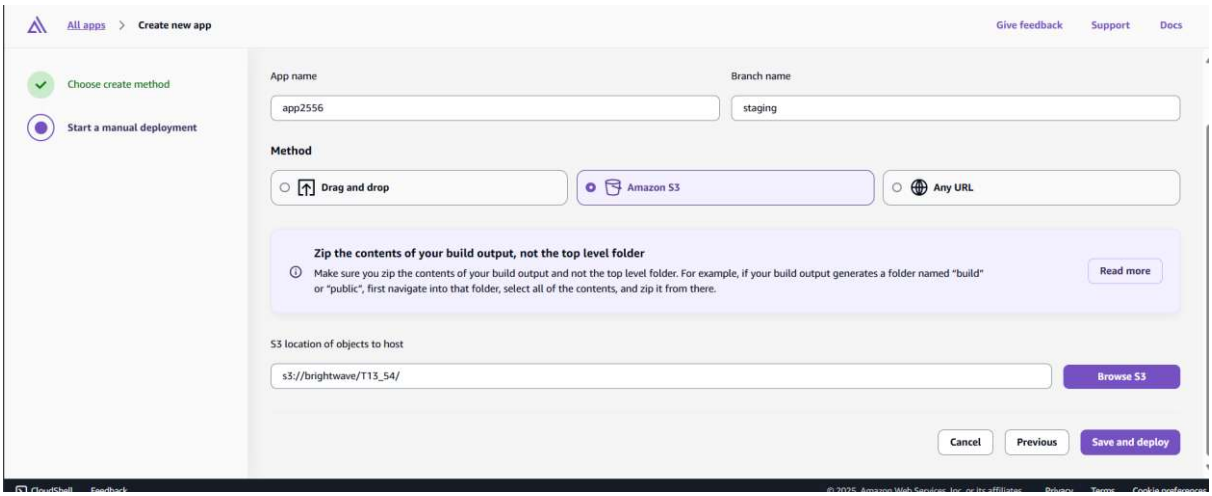


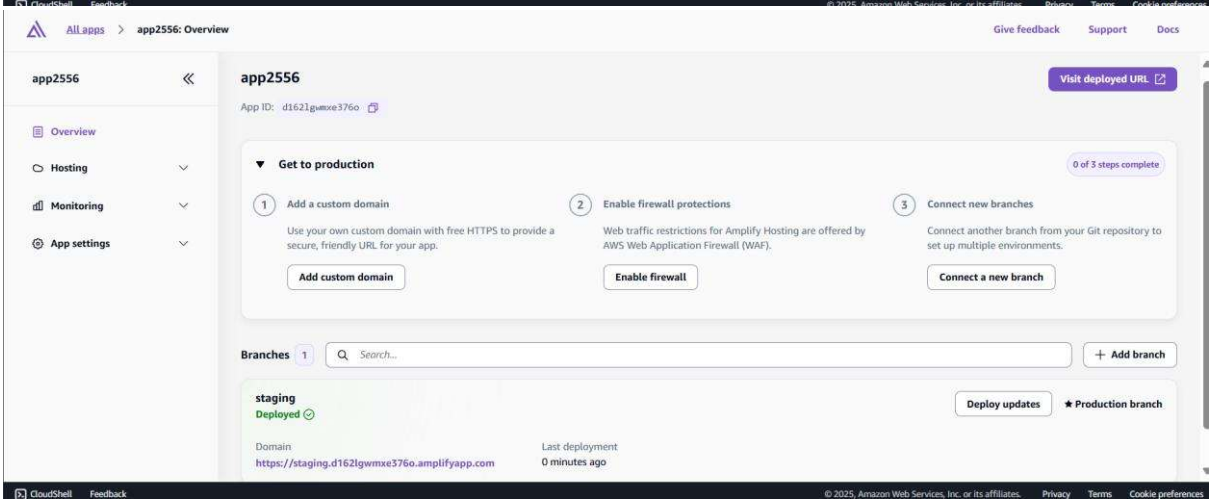


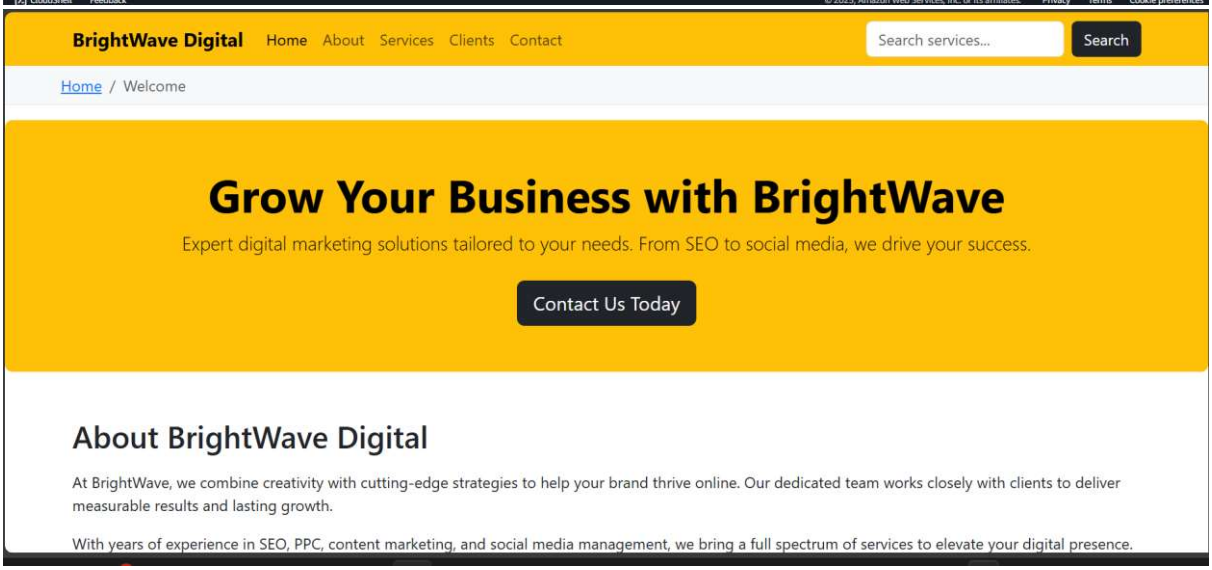
6)Host website using AWS amplify



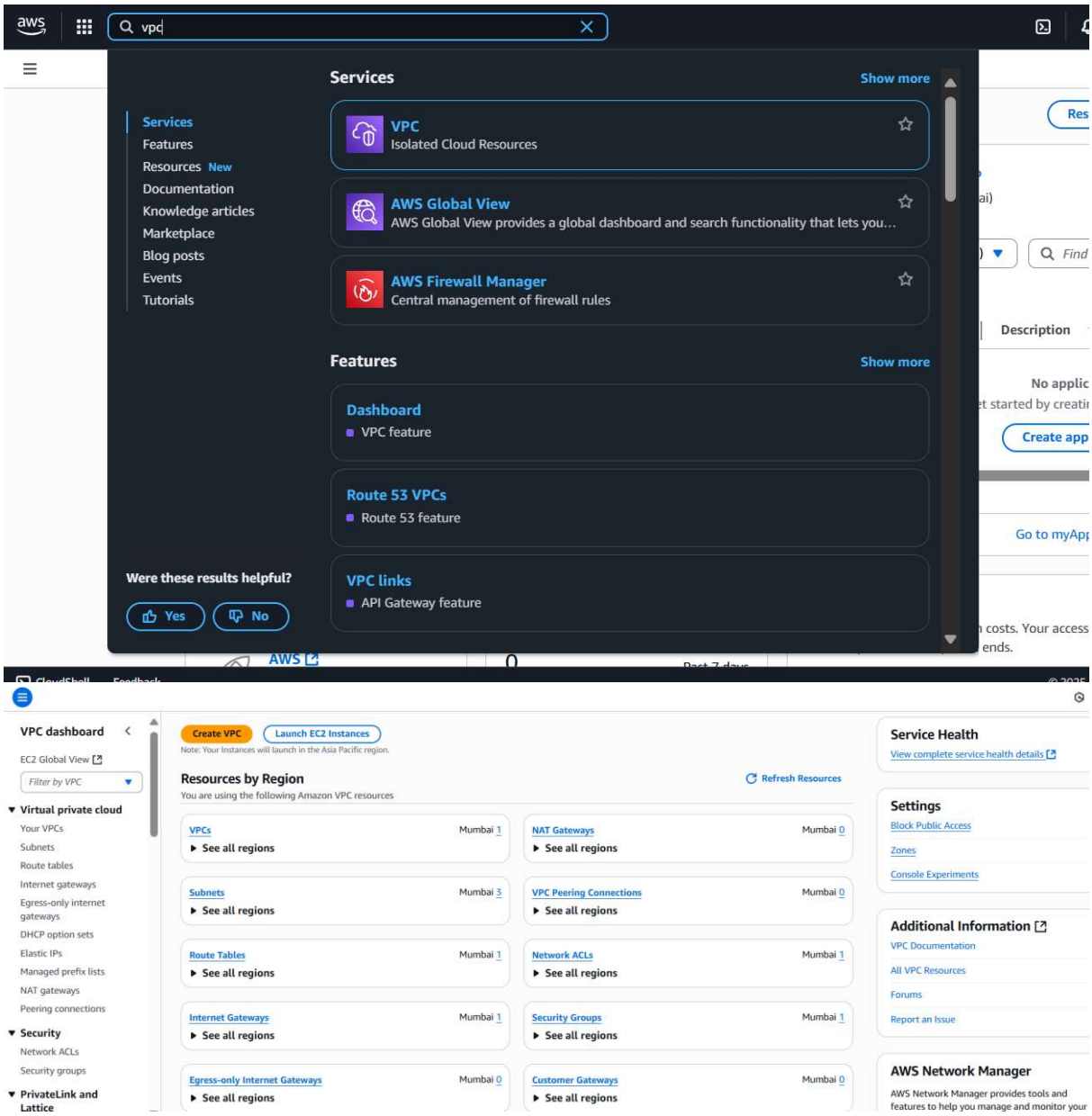


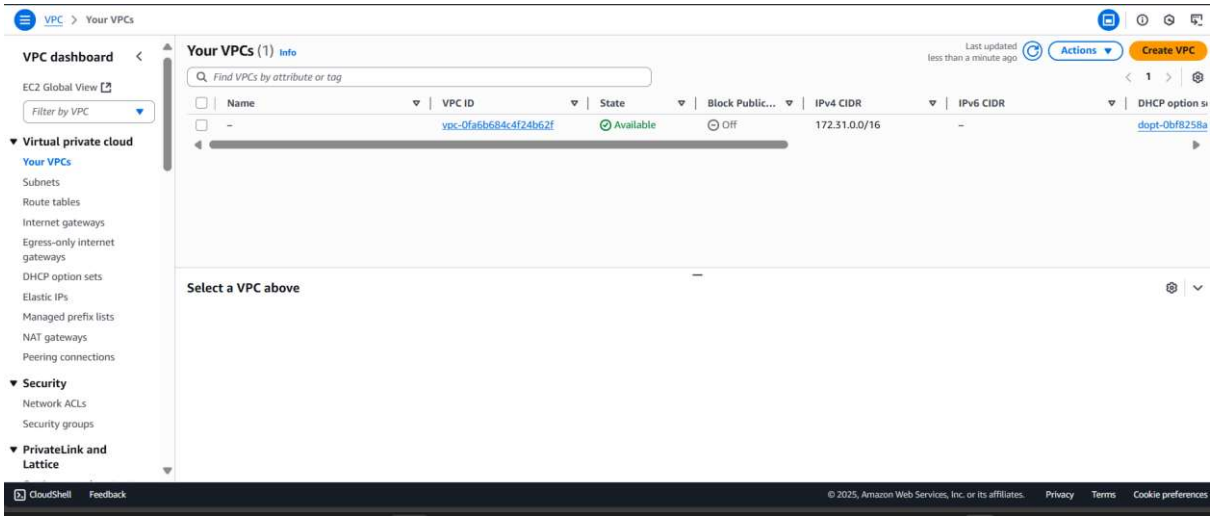

All apps > Create new app
Give feedback
Support
Docs
Choose create method
Start a manual deployment
App name
app2556
Branch name
staging
Method
Drag and drop
Amazon S3
Any URL
Zip the contents of your build output, not the top level folder
Make sure you zip the contents of your build output and not the top level folder. For example, if your build output generates a folder named "build" or "public", first navigate into that folder, select all of the contents, and zip it from there.
Read more
S3 location of objects to host
s3://brightwave/T13_54/
Browse S3
Cancel
Previous
Save and deploy

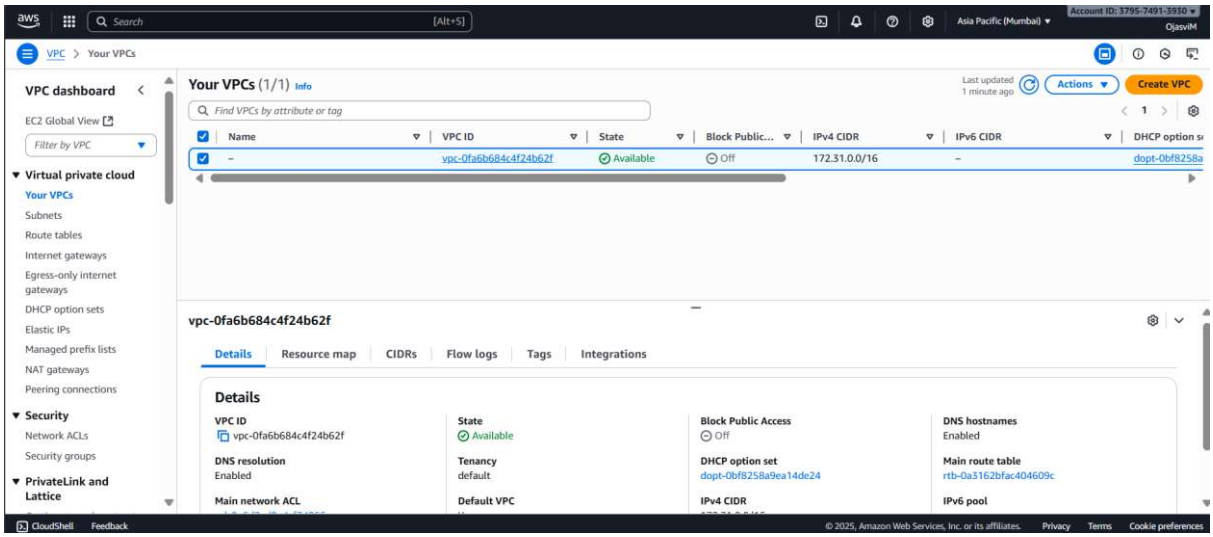

All apps > app2556: Overview
Give feedback
Support
Docs
app2556
Overview
Hosting
Monitoring
App settings
app2556
Visit deployed URL
Get to production
0 of 3 steps complete
Add a custom domain
Use your own custom domain with free HTTPS to provide a secure, friendly URL for your app.
Add custom domain
Enable firewall protections
Web traffic restrictions for Amplify Hosting are offered by AWS Web Application Firewall (WAF).
Enable firewall
Connect new branches
Connect another branch from your Git repository to set up multiple environments.
Connect a new branch
Branches
Search...
Add branch
staging
Deployed
Deploy updates
Production branch
Domain
https://staging.d162lgwmxe376o.amplifyapp.com
Last deployment
0 minutes ago
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


BrightWave Digital
Home
About
Services
Clients
Contact
Search services...
Search
Home / Welcome
Grow Your Business with BrightWave
Expert digital marketing solutions tailored to your needs. From SEO to social media, we drive your success.
Contact Us Today
About BrightWave Digital
At BrightWave, we combine creativity with cutting-edge strategies to help your brand thrive online. Our dedicated team works closely with clients to deliver measurable results and lasting growth.
With years of experience in SEO, PPC, content marketing, and social media management, we bring a full spectrum of services to elevate your digital presence.

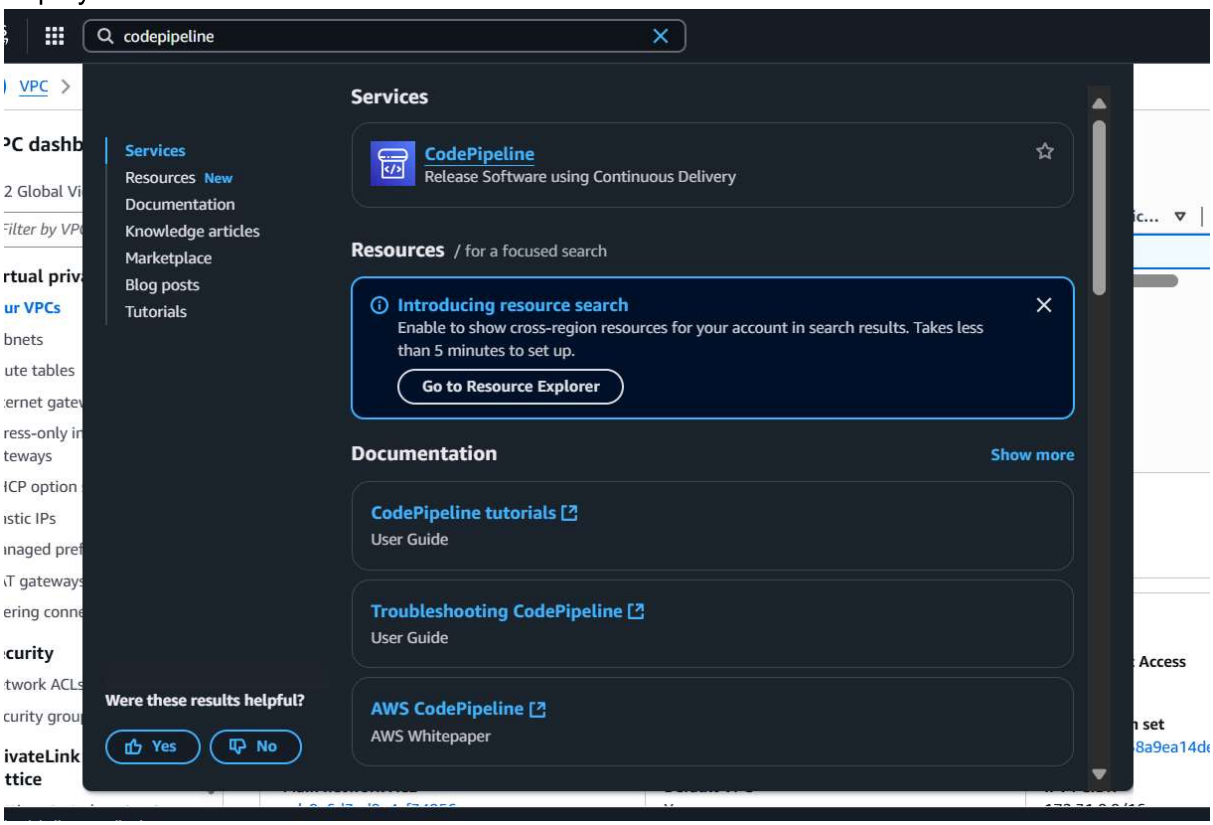
7)Go to VPC and select a VPC

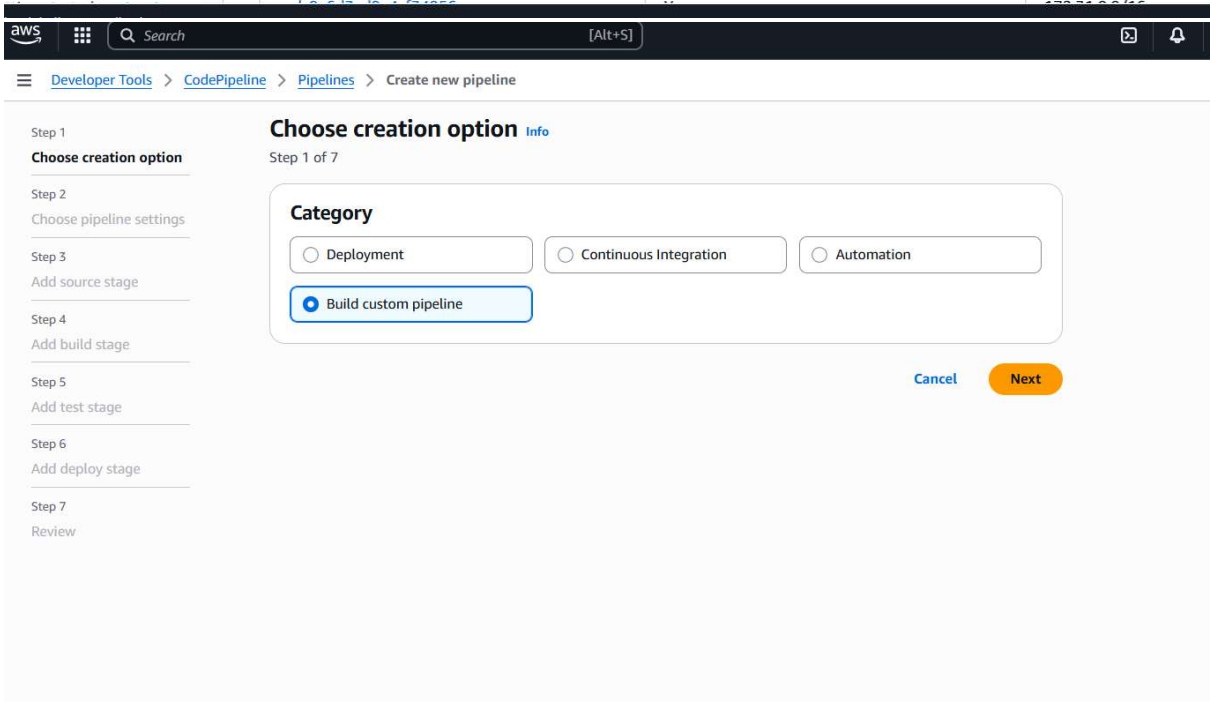


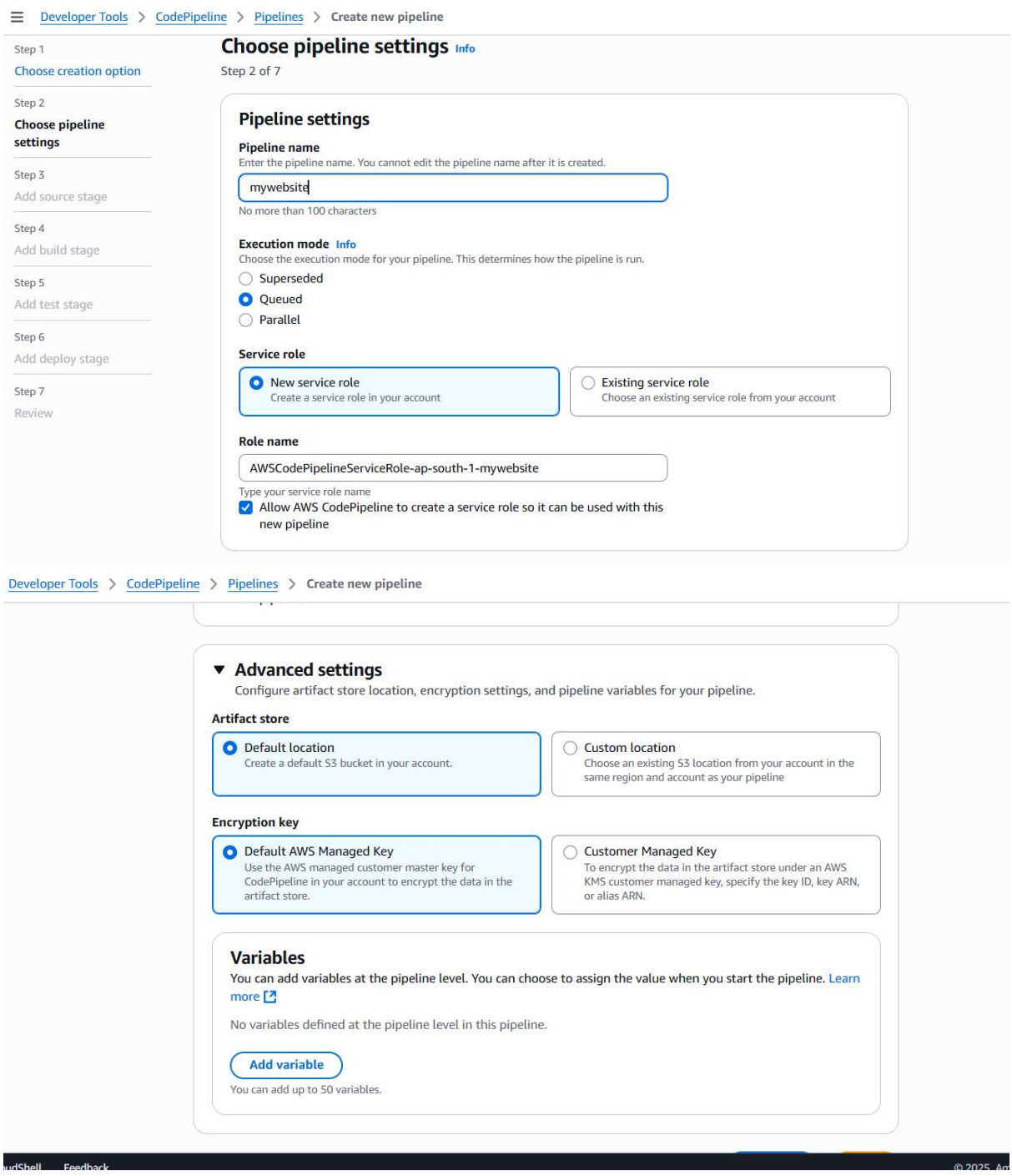

VPC > Your VPCs
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Security
Network ACLs
Security groups
PrivateLink and Lattice
Your VPCs (1) Info
Find VPCs by attribute or tag
Last updated less than a minute ago
Actions
Create VPC
Name
VPC ID
State
Block Public...
IPv4 CIDR
IPv6 CIDR
DHCP option s
vpc-0fa6b684c4f24b62f
Available
Off
172.31.0.0/16
dopt-0bf8258a
Select a VPC above
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

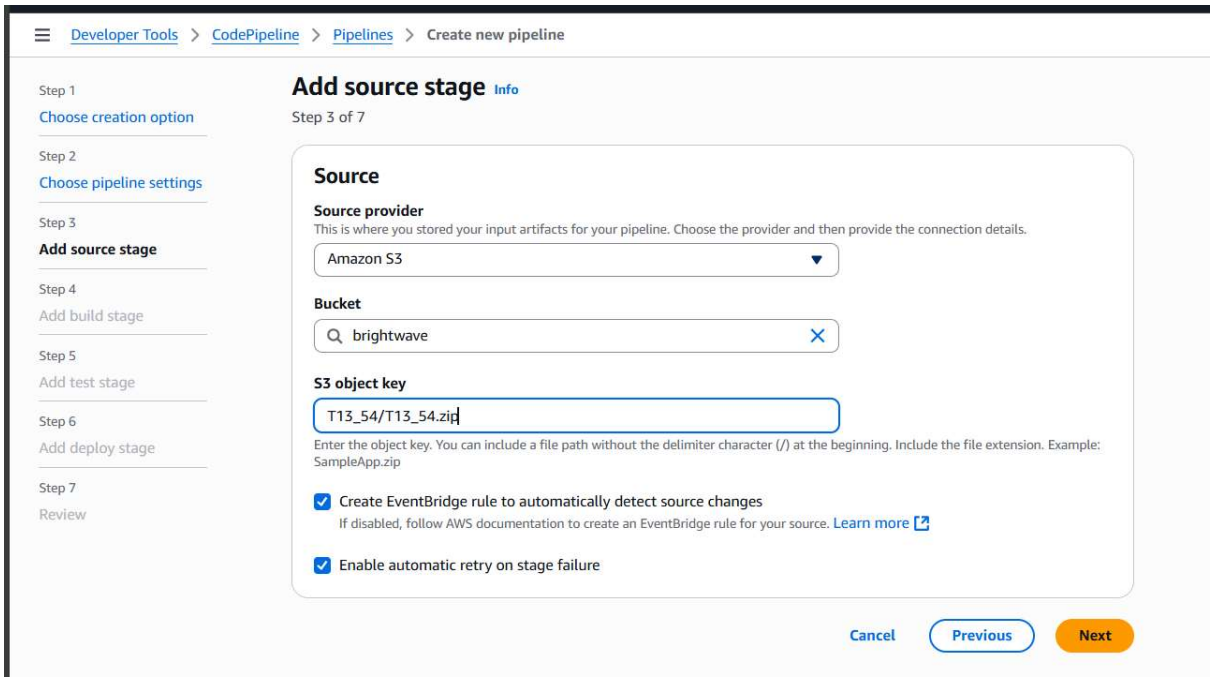

Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 3795-7491-3930
OjasvIM
VPC > Your VPCs
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Security
Network ACLs
Security groups
PrivateLink and Lattice
Your VPCs (1/1) Info
Find VPCs by attribute or tag
Last updated 1 minute ago
Actions
Create VPC
Name
VPC ID
State
Block Public...
IPv4 CIDR
IPv6 CIDR
DHCP option s
vpc-0fa6b684c4f24b62f
Available
Off
172.31.0.0/16
dopt-0bf8258a
vpc-0fa6b684c4f24b62f
Details
Resource map
CIDRs
Flow logs
Tags
Integrations
Details
VPC ID
vpc-0fa6b684c4f24b62f
State
Available
Block Public Access
Off
DNS hostnames
Enabled
DNS resolution
Enabled
Tenancy
default
DHCP option set
dopt-0bf8258a9ea14de24
Main route table
rtb-0a3162bfac404609c
Main network ACL
Default VPC
IPv4 CIDR
IPv6 pool
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

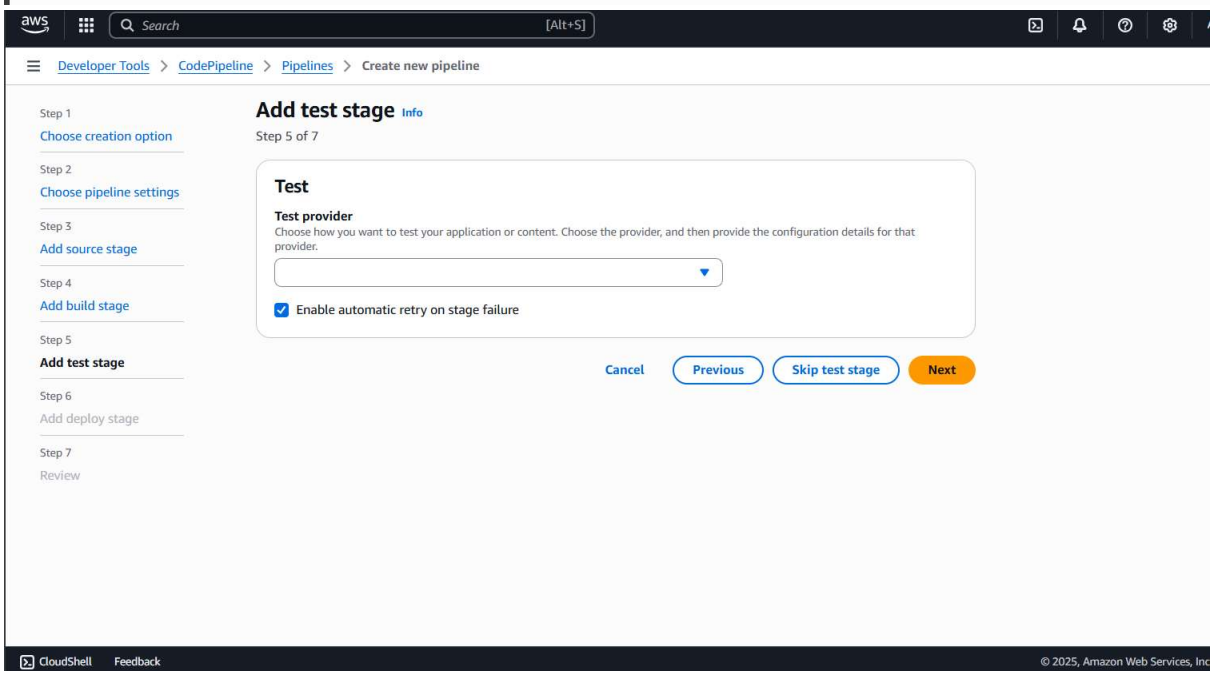
8)Go to AWS code pipeline and build a custom pipeline,choose the same S3 object and deploy

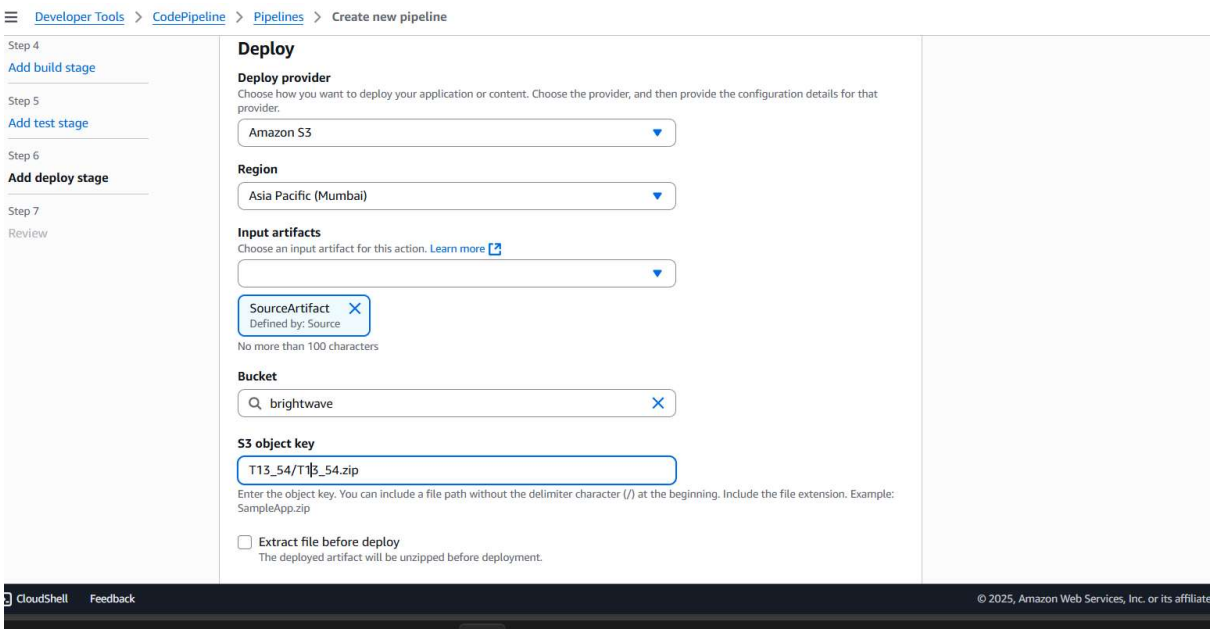


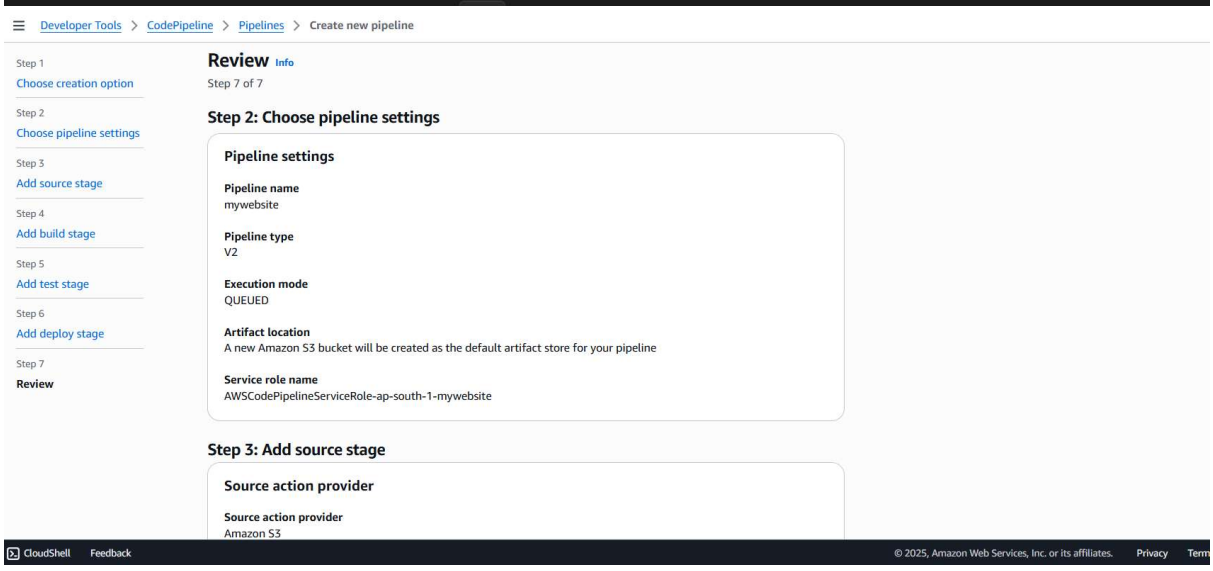


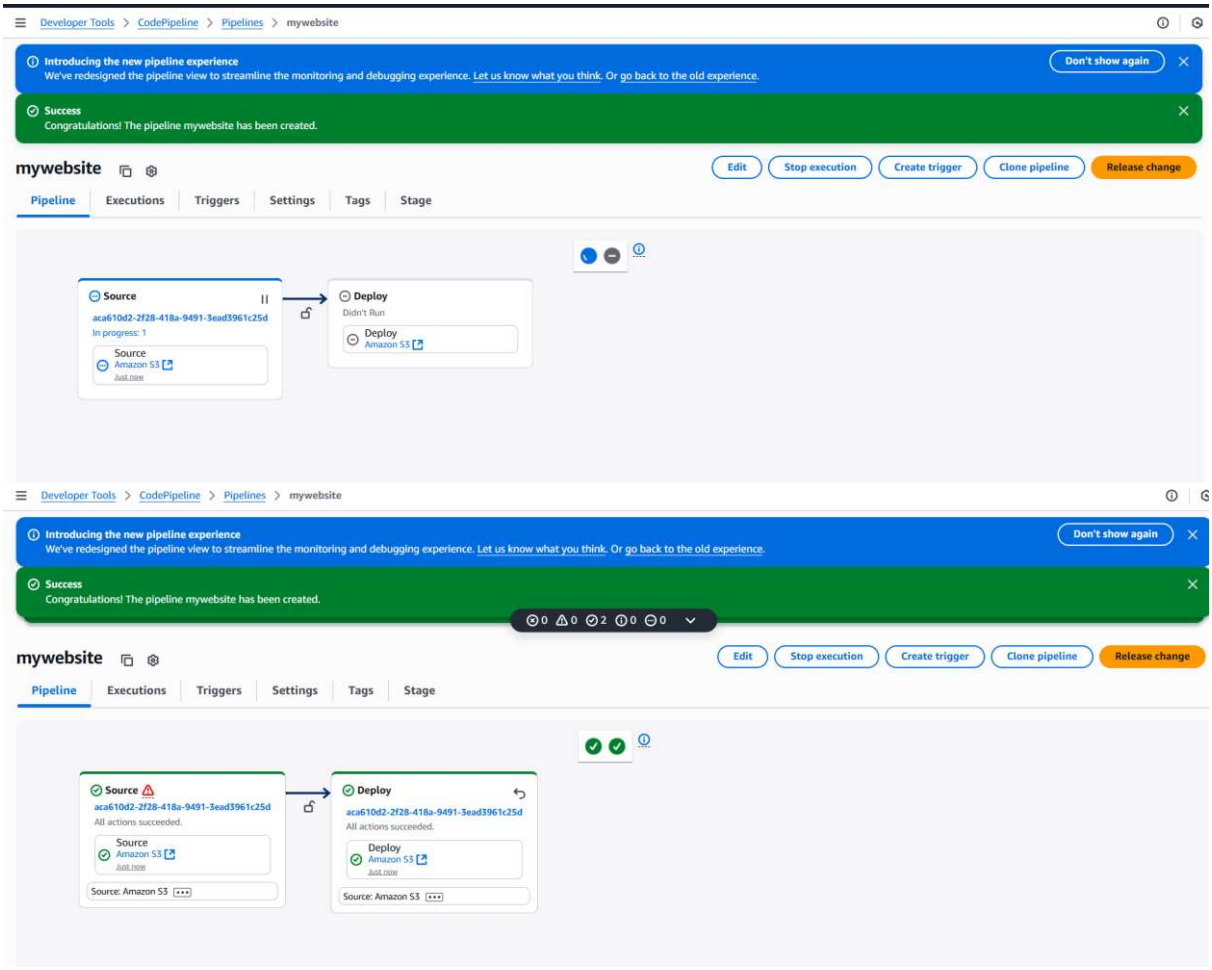

Developer Tools > CodePipeline > Pipelines > Create new pipeline
Step 1
Choose creation option
Step 2
Choose pipeline settings
Step 3
Add source stage
Step 4
Add build stage
Step 5
Add test stage
Step 6
Add deploy stage
Step 7
Review
Choose pipeline settings Info
Step 2 of 7
Pipeline settings
Pipeline name
Enter the pipeline name. You cannot edit the pipeline name after it is created.
mywebsite
No more than 100 characters
Execution mode Info
Choose the execution mode for your pipeline. This determines how the pipeline is run.
Superseded
Queued
Parallel
Service role
New service role
Create a service role in your account
Existing service role
Choose an existing service role from your account
Role name
AWSCodePipelineServiceRole-ap-south-1-mywebsite
Type your service role name
Allow AWS CodePipeline to create a service role so it can be used with this new pipeline
Developer Tools > CodePipeline > Pipelines > Create new pipeline
Advanced settings
Configure artifact store location, encryption settings, and pipeline variables for your pipeline.
Artifact store
Default location
Create a default S3 bucket in your account.
Custom location
Choose an existing S3 location from your account in the same region and account as your pipeline
Encryption key
Default AWS Managed Key
Use the AWS managed customer master key for CodePipeline in your account to encrypt the data in the artifact store.
Customer Managed Key
To encrypt the data in the artifact store under an AWS KMS customer managed key, specify the key ID, key ARN, or alias ARN.
Variables
You can add variables at the pipeline level. You can choose to assign the value when you start the pipeline. Learn more
No variables defined at the pipeline level in this pipeline.
Add variable
You can add up to 50 variables.
udShell
Feedback


Developer Tools > CodePipeline > Pipelines > Create new pipeline
Step 1
Choose creation option
Step 2
Choose pipeline settings
Step 3
Add source stage
Step 4
Add build stage
Step 5
Add test stage
Step 6
Add deploy stage
Step 7
Review
Add source stage Info
Step 3 of 7
Source
Source provider
This is where you stored your input artifacts for your pipeline. Choose the provider and then provide the connection details.
Amazon S3
Bucket
brightwave
S3 object key
T13_54/T13_54.zip
Enter the object key. You can include a file path without the delimiter character (/) at the beginning. Include the file extension. Example: SampleApp.zip
Create EventBridge rule to automatically detect source changes
If disabled, follow AWS documentation to create an EventBridge rule for your source. Learn more
Enable automatic retry on stage failure
Cancel
Previous
Next


aws
Search
[Alt+S]
Developer Tools > CodePipeline > Pipelines > Create new pipeline
Step 1
Choose creation option
Step 2
Choose pipeline settings
Step 3
Add source stage
Step 4
Add build stage
Step 5
Add test stage
Step 6
Add deploy stage
Step 7
Review
Add test stage Info
Step 5 of 7
Test
Test provider
Choose how you want to test your application or content. Choose the provider, and then provide the configuration details for that provider.
Enable automatic retry on stage failure
Cancel
Previous
Skip test stage
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc


Developer Tools > CodePipeline > Pipelines > Create new pipeline
Step 4
Add build stage
Step 5
Add test stage
Step 6
Add deploy stage
Step 7
Review
Deploy
Deploy provider
Choose how you want to deploy your application or content. Choose the provider, and then provide the configuration details for that provider.
Amazon S3
Region
Asia Pacific (Mumbai)
Input artifacts
Choose an input artifact for this action. Learn more
SourceArtifact
Defined by: Source
No more than 100 characters
Bucket
brightwave
S3 object key
T13_54/T13_54.zip
Enter the object key. You can include a file path without the delimiter character (/) at the beginning. Include the file extension. Example: SampleApp.zip
Extract file before deploy
The deployed artifact will be unzipped before deployment.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliate


Developer Tools > CodePipeline > Pipelines > Create new pipeline
Step 1
Choose creation option
Step 2
Choose pipeline settings
Step 3
Add source stage
Step 4
Add build stage
Step 5
Add test stage
Step 6
Add deploy stage
Step 7
Review
Review Info
Step 7 of 7
Step 2: Choose pipeline settings
Pipeline settings
Pipeline name
mywebsite
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-south-1-mywebsite
Step 3: Add source stage
Source action provider
Source action provider
Amazon S3
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy



Conclusion: Thus, we learn that deploying a web application using AWS CodePipeline ensures a fully automated, reliable, and repeatable release process.
It minimizes manual intervention, reduces deployment errors, and accelerates delivery cycles. By integrating source, build, and deploy stages, CodePipeline streamlines CI/CD for modern cloud-native applications.

LO Mapping: LO1

ASSIGNMENT-5

Aim: To understand Kubernetes Cluster Architecture

Theory:

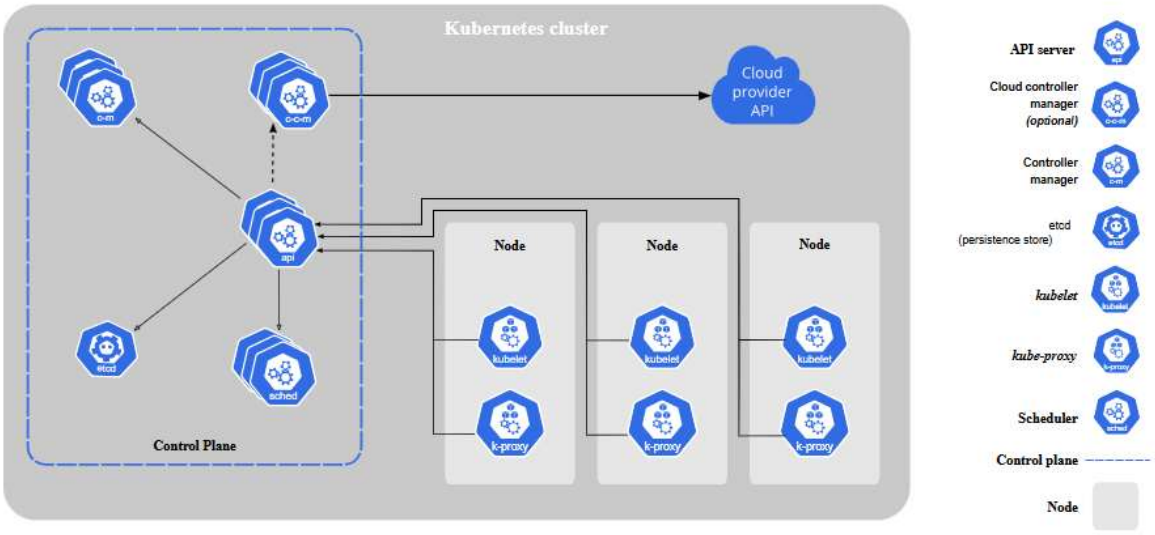
What is Kubernetes?

Kubernetes is an open-source container orchestration system for automating deployment, scaling, and management of containerized applications. It abstracts infrastructure and provides a unified API to manage workloads across clusters of machines

Containers are a good way to bundle and run your applications. In a production environment, you need to manage the containers that run the applications and ensure that there is no downtime. For example, if a container goes down, another container needs to start. Wouldn't it be easier if this behaviour was handled by a system?

That's how Kubernetes helps. Kubernetes provides you with a framework to run distributed systems resiliently. It takes care of scaling and failover for your application, provides deployment patterns, and more. For example: Kubernetes can easily manage a canary deployment for your system.

Kubernetes Cluster components overview



A Kubernetes cluster consists of a control plane and one or more worker nodes. Here's a brief overview of the main components:

Control Plane Components

-Manage the overall state of the cluster:

- kube-apiserver- The core component server that exposes the Kubernetes HTTP API. etcd Consistent and highly-available key value store for all API server data.
- kube-scheduler Looks for Pods not yet bound to a node, and assigns each Pod to a suitable node.
- kube-controller-manager Runs controllers to implement Kubernetes API behavior.
- cloud-controller-manager (optional) Integrates with underlying cloud provider(s).

Node Components

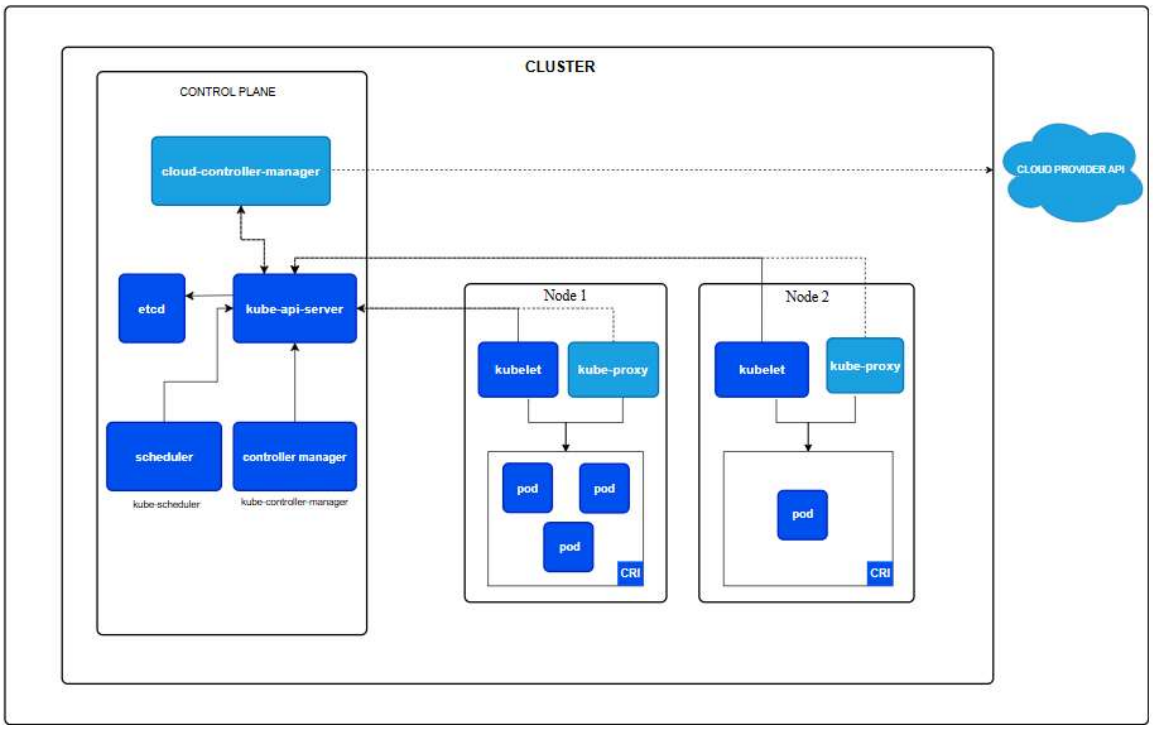
-Run on every node, maintaining running pods and providing the Kubernetes runtime environment:

- kubelet- Ensures that Pods are running, including their containers.
- kube-proxy (optional) Maintains network rules on nodes to implement Services.
- Container runtime Software- responsible for running containers.

Kubernetes Cluster Architecture

A Kubernetes cluster consists of a control plane plus a set of worker machines, called nodes, that run containerized applications. Every cluster needs at least one worker node in order to run Pods.

The worker node(s) host the Pods that are the components of the application workload. The control plane manages the worker nodes and the Pods in the cluster. In production environments, the control plane usually runs across multiple computers and a cluster usually runs multiple nodes, providing fault-tolerance and high availability.



In the diagram, each node runs kube-proxy component. You need a network proxy component on each node to ensure that the Service API and associated behaviours are available on your cluster network. However, some network plugins provide their own, third party implementation of proxying. When you use that kind of network plugin, the node does not need to run kube-proxy. The components described are same as above

Cluster Characteristics

- Control plane components can run on any machine but are typically isolated from user workloads.
- Production clusters often run control plane components across multiple machines for high availability.
- Worker nodes host Pods and must be registered with the control plane.

Advantages of Kubernetes

1. Automated Scaling & Self-Healing
   Kubernetes can automatically scale applications based on resource usage and restart failed containers without manual intervention.
2. Declarative Configuration & Version Control
   Infrastructure and application state are defined using YAML/JSON manifests, enabling reproducible deployments and easy rollback.
3. Cloud-Agnostic & Extensible
   Kubernetes runs on-premises or across public clouds (AWS, Azure, GCP) and supports plugins for networking (CNI), storage (CSI), and runtime (CRI).

Disadvantages of Kubernetes

1. Steep Learning Curve
   The architecture, terminology, and configuration syntax require significant time and expertise to master.
2. Complex Setup & Maintenance
   Initial cluster setup, upgrades, and monitoring demand deep operational knowledge and often third-party tooling.
3. Resource Overhead
   Running Kubernetes itself consumes CPU, memory, and storage — which can be inefficient for small-scale applications.

Conclusion- Thus we understand that Kubernetes is a robust, cloud-agnostic orchestration platform designed to manage containerized applications at scale. Its architecture is modular and resilient, built around a control plane that governs cluster state and worker nodes that execute workloads. Through components like kube-apiserver, etcd, kube-scheduler, and kubelet, it ensures declarative configuration, automated scaling, fault tolerance, and seamless networking

LO Mapping- LO2

Asssignment-6

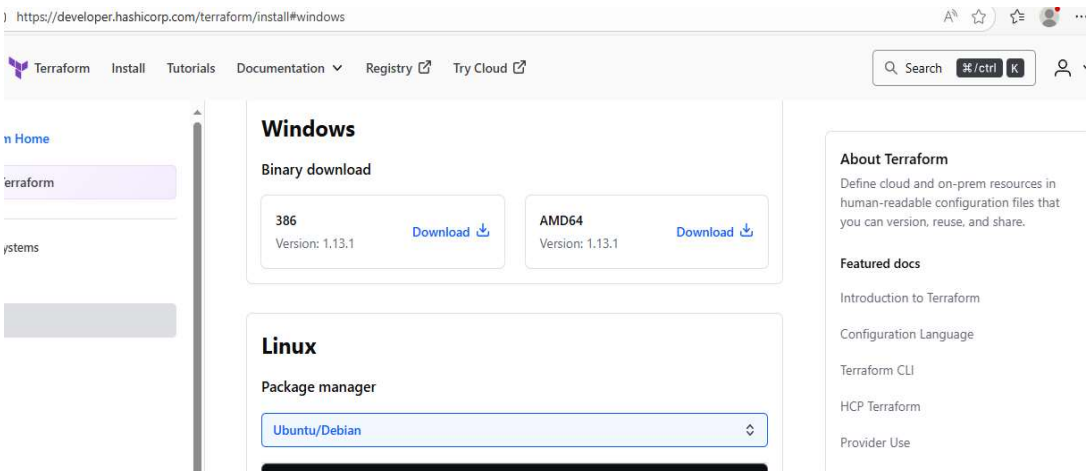
Aim: To understand terraform lifecycle and to build , change , and destroy AWS infrastructure using Terraform.

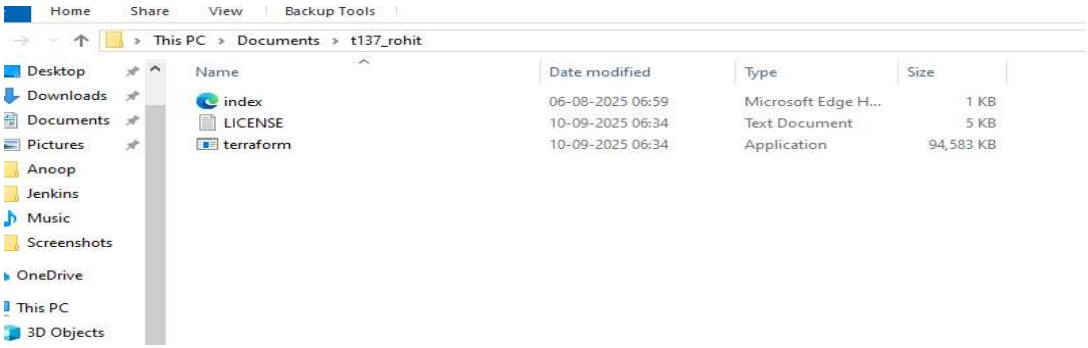
Theory:

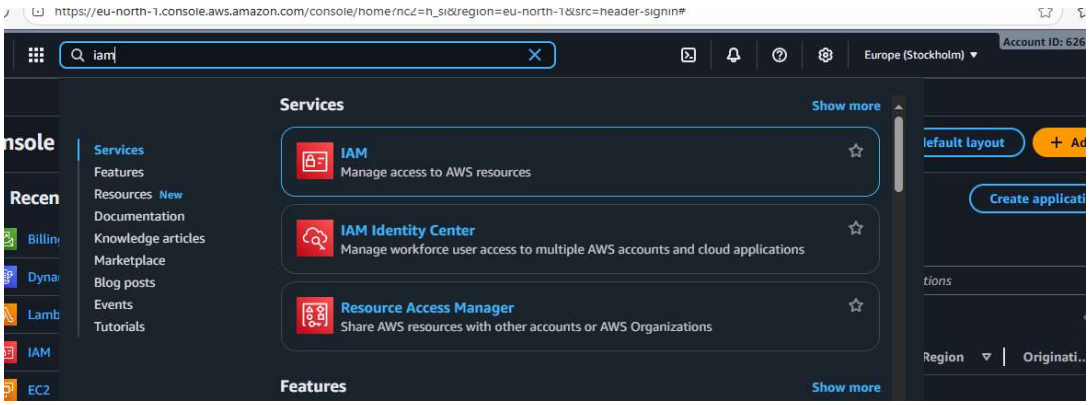
Terraform is an open-source Infrastructure as Code (IaC) tool developed by HashiCorp that enables users to define, provision, and manage cloud infrastructure using declarative configuration files. It supports multiple cloud providers like AWS, Azure, Google Cloud, and others, allowing for consistent infrastructure deployment across environments. Terraform uses a high-level configuration language called HCL (HashiCorp Configuration Language) to describe the desired infrastructure state, which it then translates into API calls to create and manage resources. Its execution plan feature previews changes before applying them, ensuring safe and predictable updates.

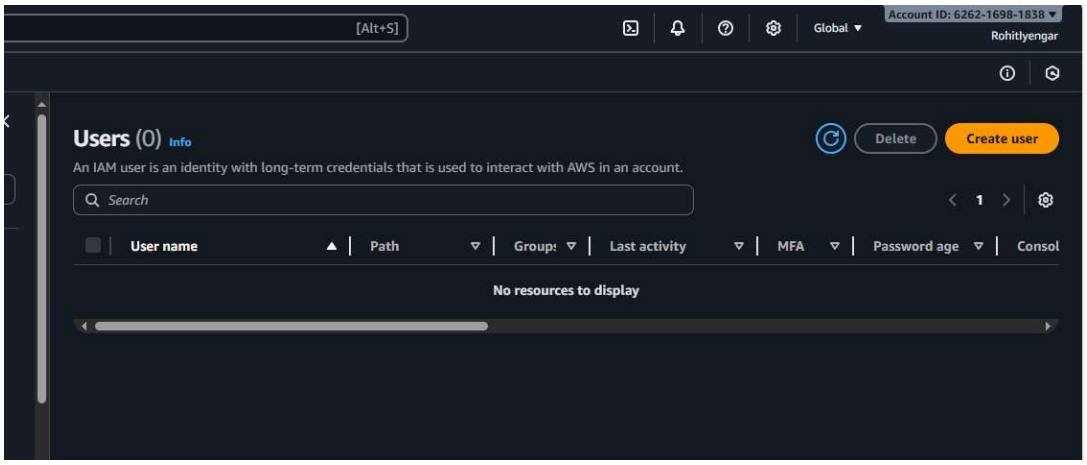
One of Terraform's key strengths is its ability to manage dependencies and maintain state. The state file records the current infrastructure configuration, enabling Terraform to detect changes and apply only the necessary updates. It also supports modules, which promote reusability and modular design, making complex infrastructure easier to manage. Terraform's provider ecosystem allows integration with a wide range of services, and its workflow—init, plan, apply—ensures a structured approach to infrastructure changes. Overall, Terraform simplifies infrastructure management, enhances scalability, and supports DevOps practices by automating provisioning and reducing manual errors.

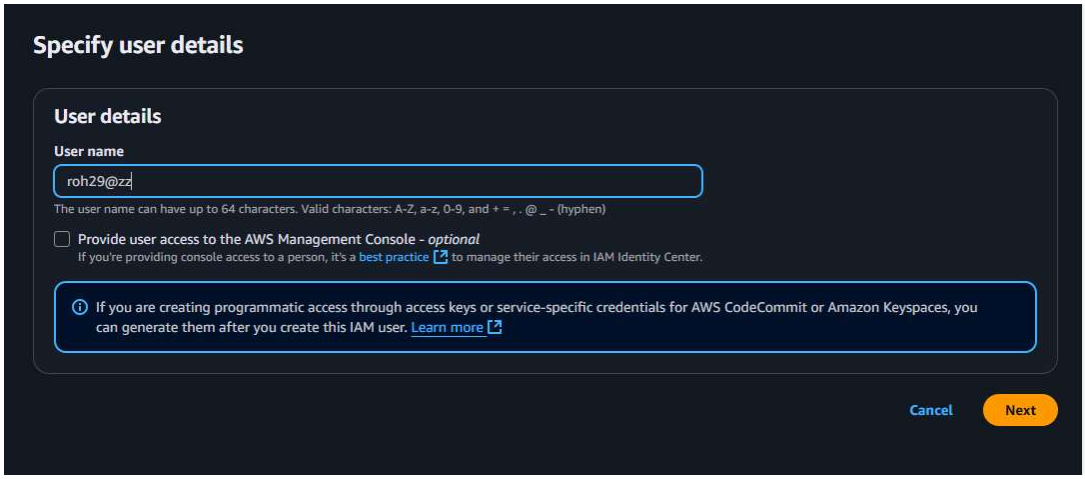
Steps:

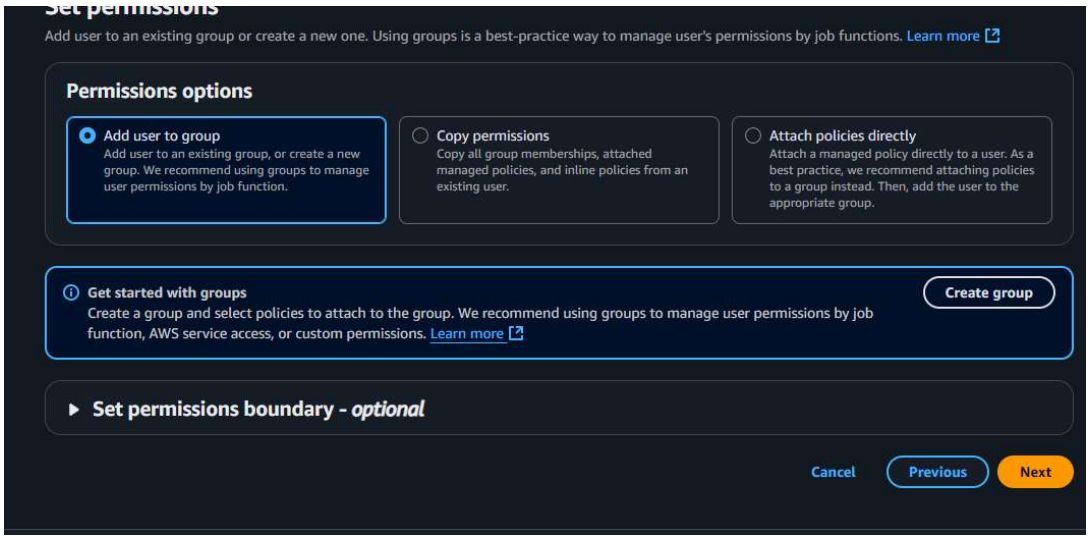


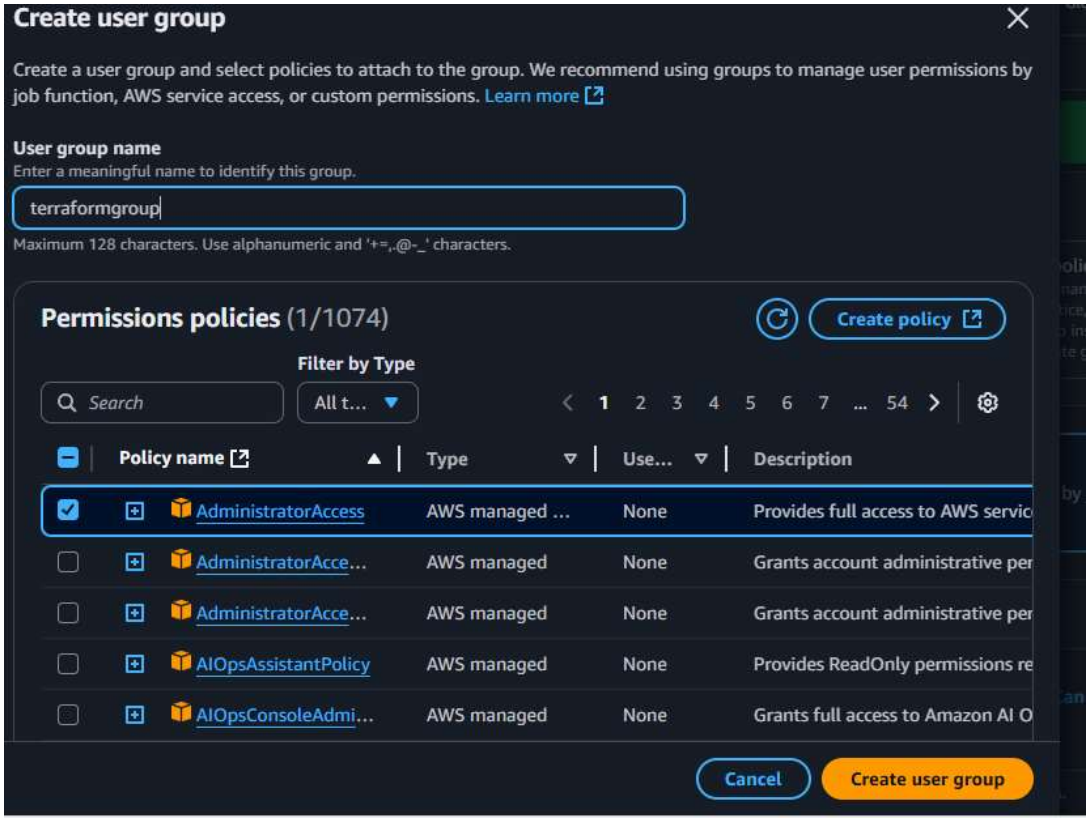

Home
Share
View
Backup Tools
This PC
Documents
t137_rohit
Desktop
Downloads
Documents
Pictures
Anoop
Jenkins
Music
Screenshots
OneDrive
This PC
3D Objects
Name
Date modified
Type
Size
index
06-08-2025 06:59
Microsoft Edge H...
1 KB
LICENSE
10-09-2025 06:34
Text Document
5 KB
terraform
10-09-2025 06:34
Application
94,583 KB

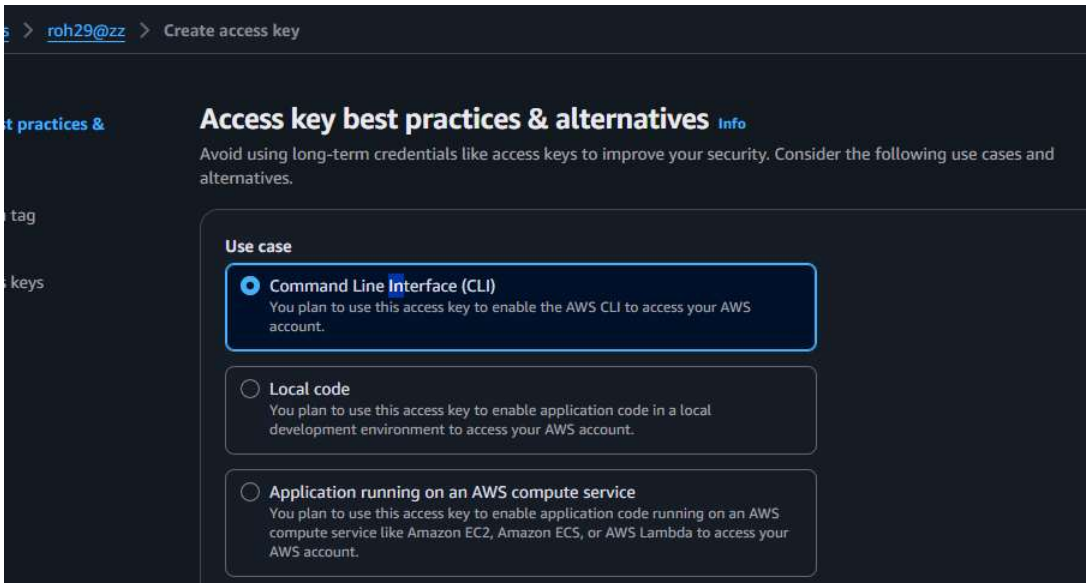

iam
Europe (Stockholm)
Services
Show more
Services
Features
Resources New
Documentation
Knowledge articles
Marketplace
Blog posts
Events
Tutorials
IAM
Manage access to AWS resources
IAM Identity Center
Manage workforce user access to multiple AWS accounts and cloud applications
Resource Access Manager
Share AWS resources with other accounts or AWS Organizations
Features
Show more

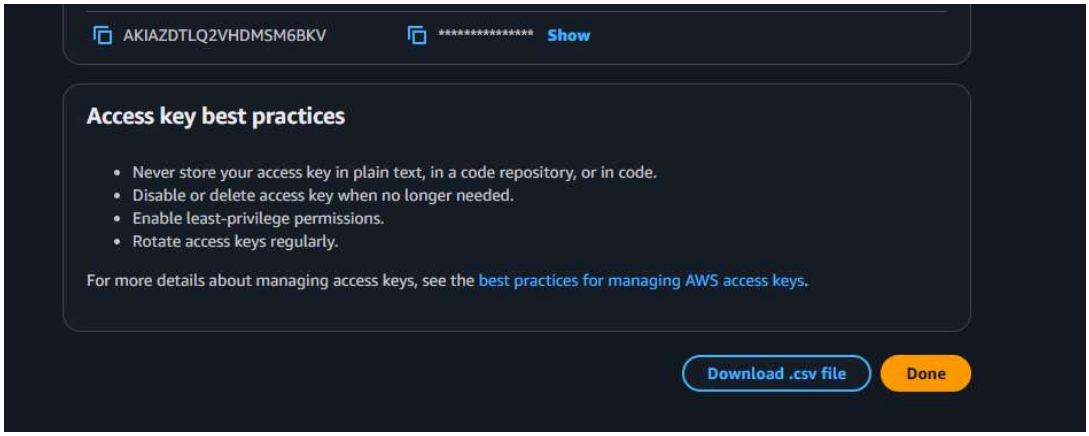

[Alt+S]
Global
Rohitlyengar
Users (0) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Last activity
MFA
Password age
No resources to display

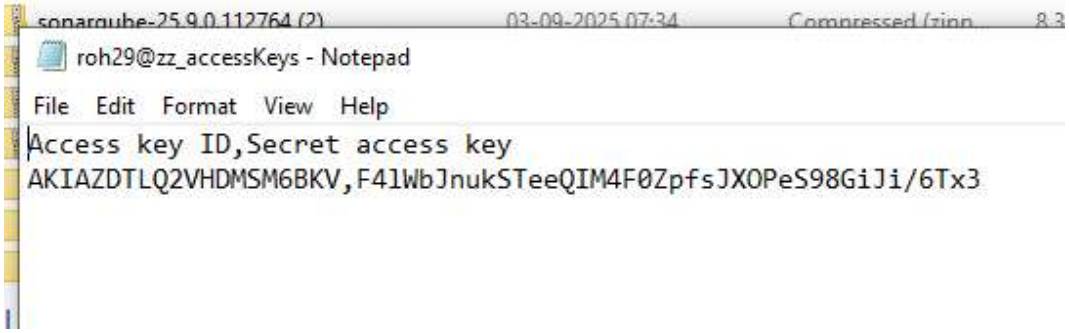

Specify user details
User details
User name
roh29@zz
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more
Cancel
Next

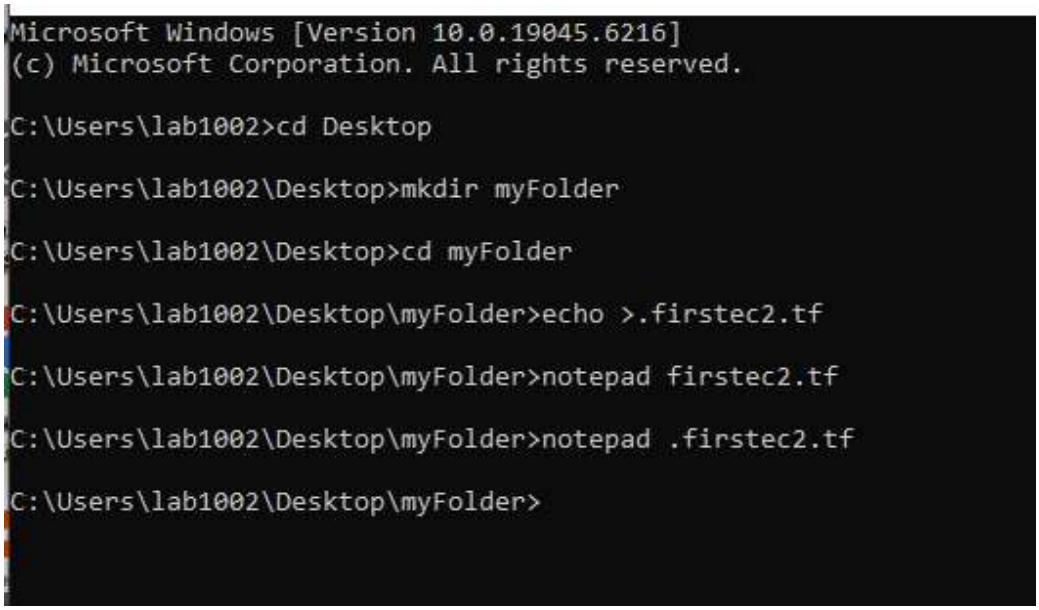

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more
Create group
Set permissions boundary - optional
Cancel
Previous
Next

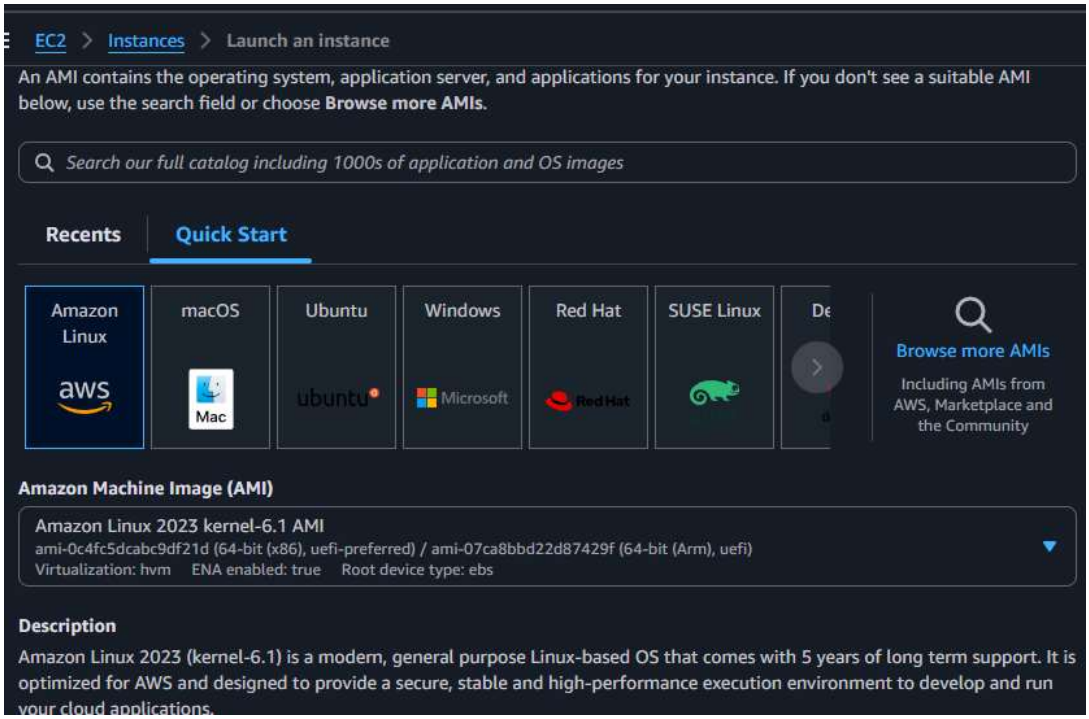

Create user group
Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more
User group name
Enter a meaningful name to identify this group.
terraformgroup
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions policies (1/1074)
Create policy
Filter by Type
Search
All t...
1 2 3 4 5 6 7 ... 54
Policy name
Type
Use...
Description
AdministratorAccess
AWS managed ...
None
Provides full access to AWS servic
AdministratorAcce...
AWS managed
None
Grants account administrative per
AdministratorAcce...
AWS managed
None
Grants account administrative per
AIOpsAssistantPolicy
AWS managed
None
Provides ReadOnly permissions re
AIOpsConsoleAdmi...
AWS managed
None
Grants full access to Amazon AI O
Cancel
Create user group

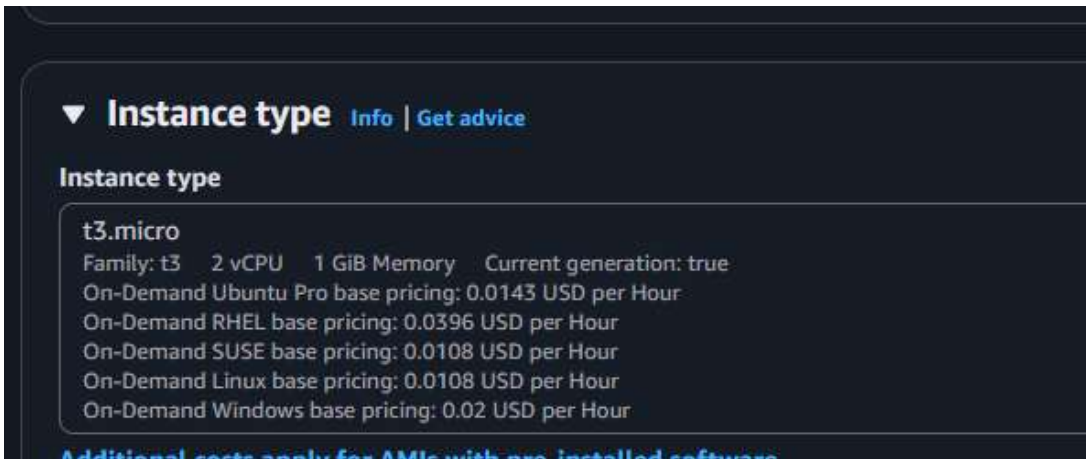

roh29@zz
Create access key
Access key best practices & alternatives
Info
Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.
Use case
Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.
Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.
Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

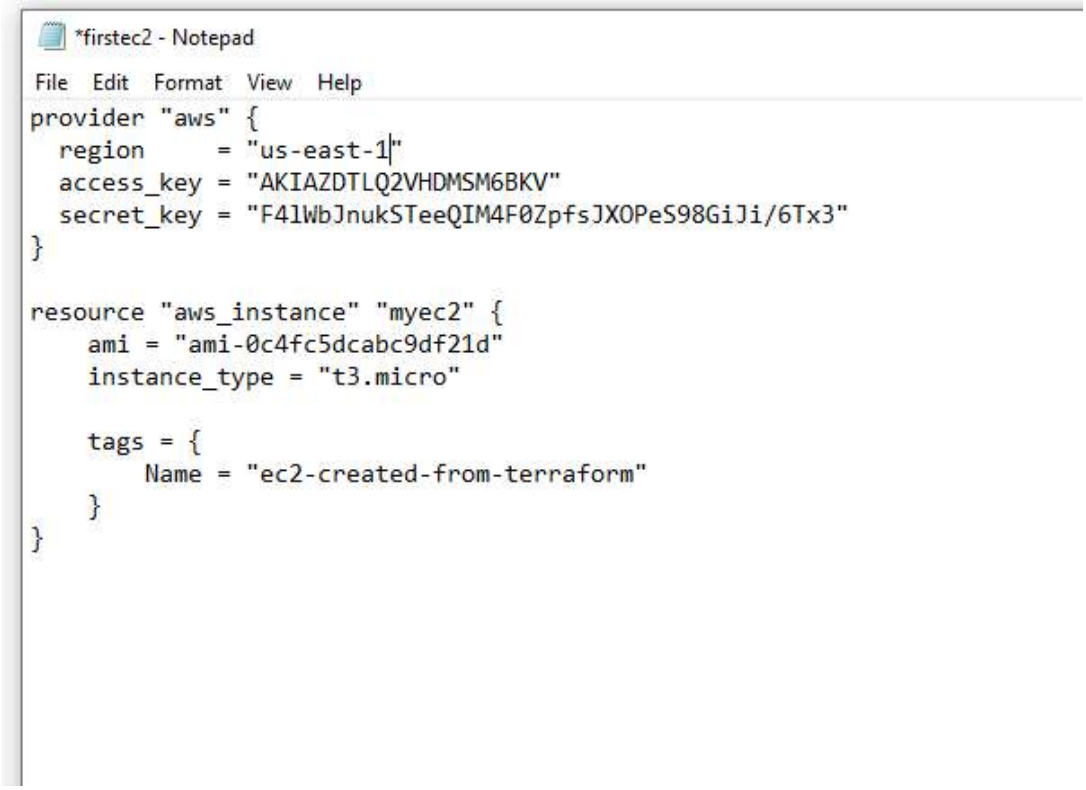

AKIAZDTLQ2VHDMSM6BKV
********** Show
Access key best practices
Never store your access key in plain text, in a code repository, or in code.
Disable or delete access key when no longer needed.
Enable least-privilege permissions.
Rotate access keys regularly.
For more details about managing access keys, see the best practices for managing AWS access keys.
Download .csv file
Done

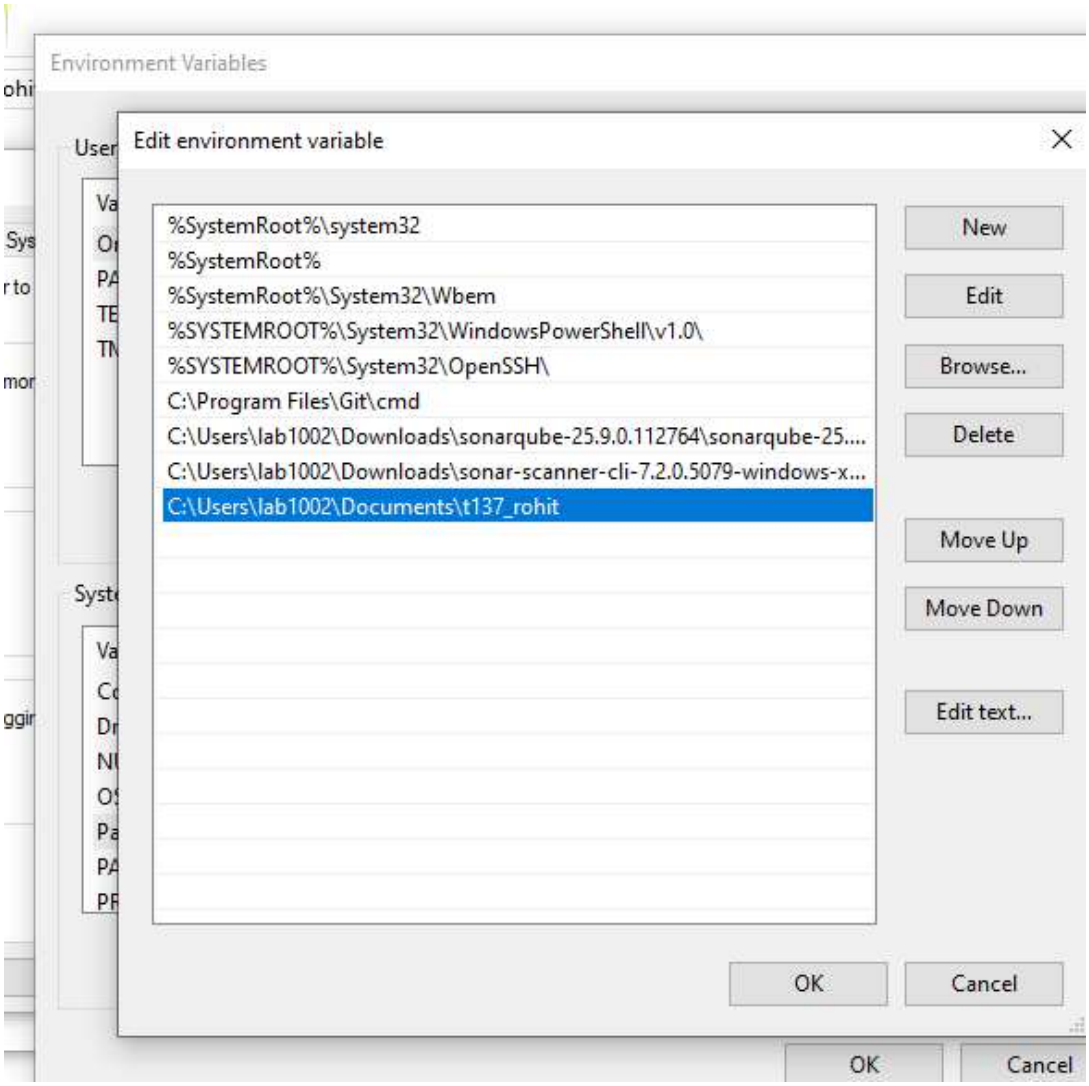

sonarqube-25.9.0.112764 (2) 03-09-2025 07:34 Compressed (zipp... 8,3
roh29@zz_accessKeys - Notepad
File Edit Format View Help
Access key ID,Secret access key
AKIAZDTLQ2VHDMSM6BKV,F41WbJnukSTeeQIM4F0ZpfsJXOPeS98GiJi/6Tx3

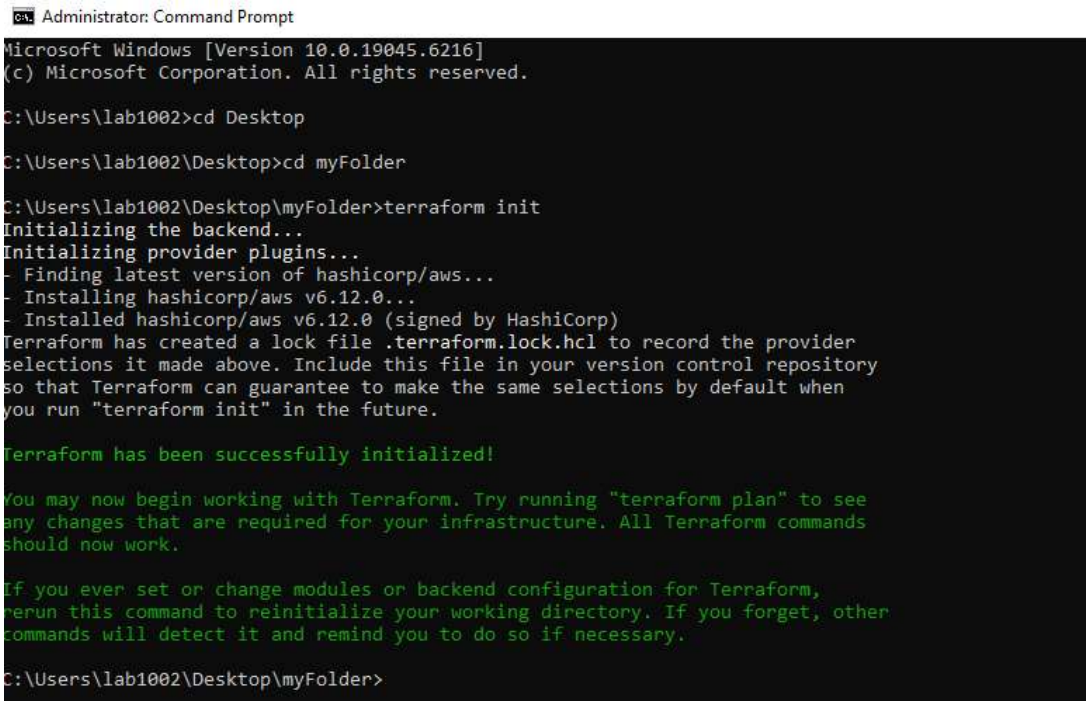

Microsoft Windows [Version 10.0.19045.6216]
(c) Microsoft Corporation. All rights reserved.
C:\Users\lab1002>cd Desktop
C:\Users\lab1002\Desktop>mkdir myFolder
C:\Users\lab1002\Desktop>cd myFolder
C:\Users\lab1002\Desktop\myFolder>echo >.firstec2.tf
C:\Users\lab1002\Desktop\myFolder>notepad firstec2.tf
C:\Users\lab1002\Desktop\myFolder>notepad .firstec2.tf
C:\Users\lab1002\Desktop\myFolder>

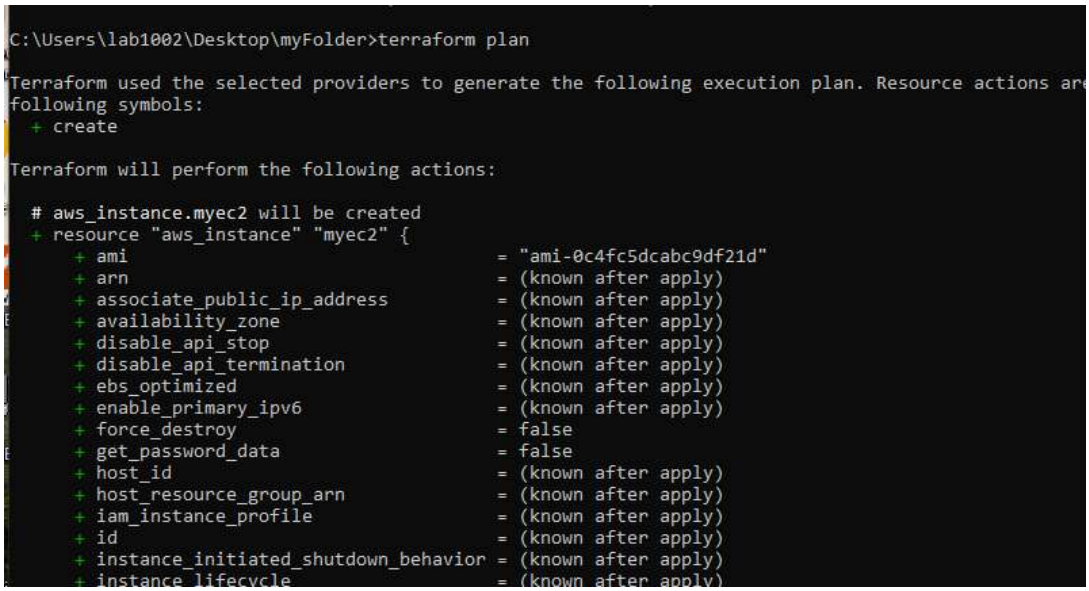

EC2 > Instances > Launch an instance
An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Amazon Linux 2023 kernel-6.1 AMI
ami-0c4fc5dcabc9df21d (64-bit (x86), uefi-preferred) / ami-07ca8bbd22d87429f (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs
Description
Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.


Instance type Info | Get advice
Instance type
t3.micro
Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand Ubuntu Pro base pricing: 0.0143 USD per Hour
On-Demand RHEL base pricing: 0.0396 USD per Hour
On-Demand SUSE base pricing: 0.0108 USD per Hour
On-Demand Linux base pricing: 0.0108 USD per Hour
On-Demand Windows base pricing: 0.02 USD per Hour


*firstec2 - Notepad
File Edit Format View Help
provider "aws" {
region = "us-east-1"
access_key = "AKIAZDTLQ2VHDMSM6BKV"
secret_key = "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"
}
resource "aws_instance" "myec2" {
ami = "ami-0c4fc5dcabc9df21d"
instance_type = "t3.micro"
tags = {
Name = "ec2-created-from-terraform"
}
}


Environment Variables
Edit environment variable
%SystemRoot%\system32
%SystemRoot%
%SystemRoot%\System32\Wbem
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\
%SYSTEMROOT%\System32\OpenSSH\
C:\Program Files\Git\cmd
C:\Users\lab1002\Downloads\sonarqube-25.9.0.112764\sonarqube-25....
C:\Users\lab1002\Downloads\sonar-scanner-cli-7.2.0.5079-windows-x...
C:\Users\lab1002\Documents\t137_rohit
New
Edit
Browse...
Delete
Move Up
Move Down
Edit text...
OK
Cancel
OK
Cancel





Conclusion- Thus terraform simplifies the process of building, changing, and destroying AWS infrastructure using Infrastructure as Code. By following its lifecycle -init, plan, apply, and destroy—you can manage resources efficiently, automate deployments, and maintain consistency across environments.

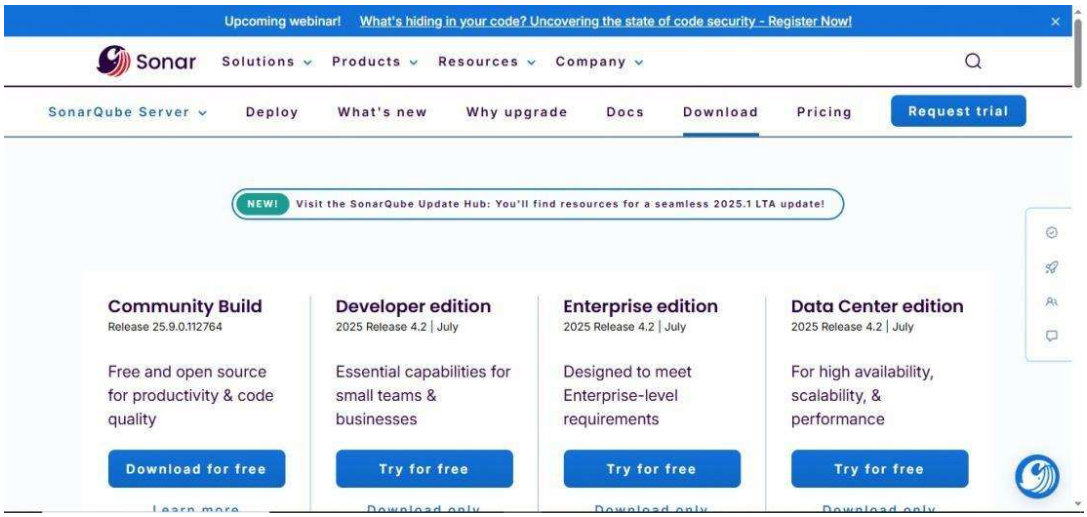
LO Mapping: LO3

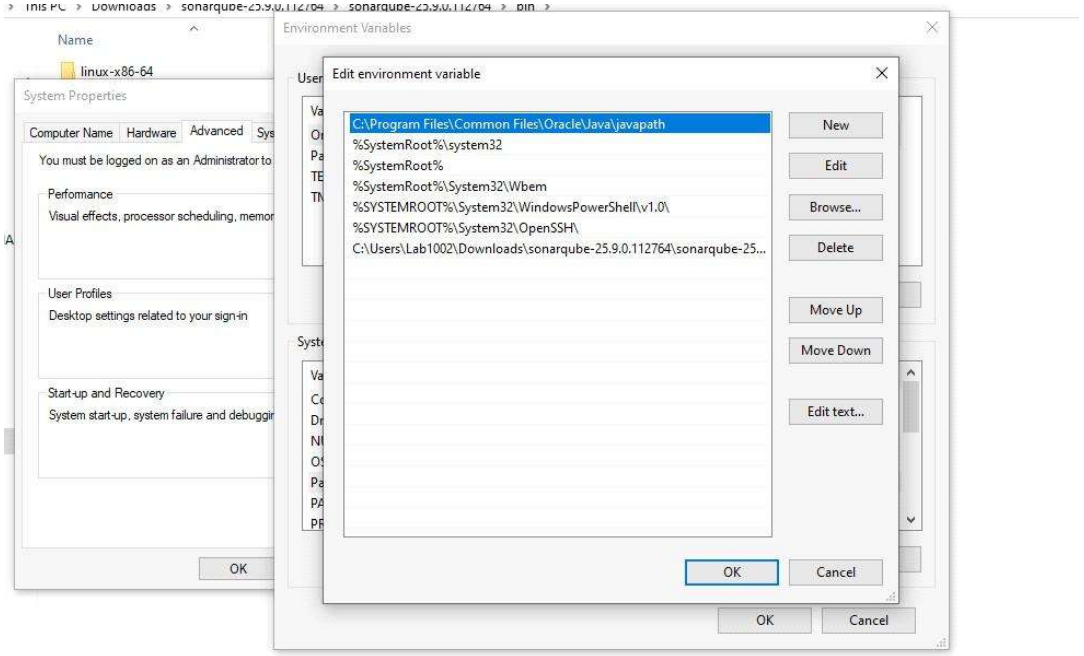
Assignment-7

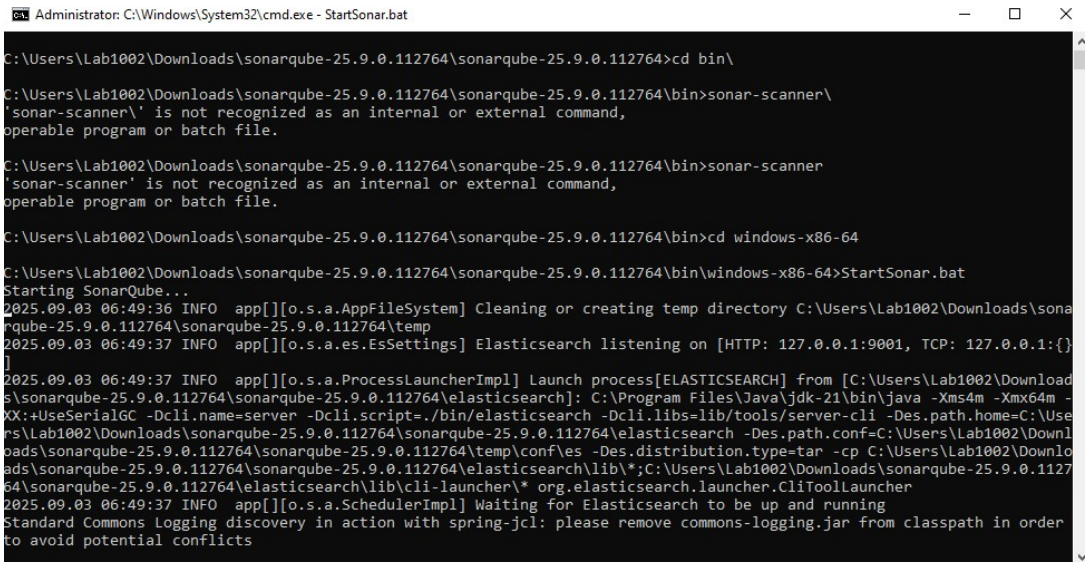
Aim: To perform static analysis on python programs using SonarQube SAST process

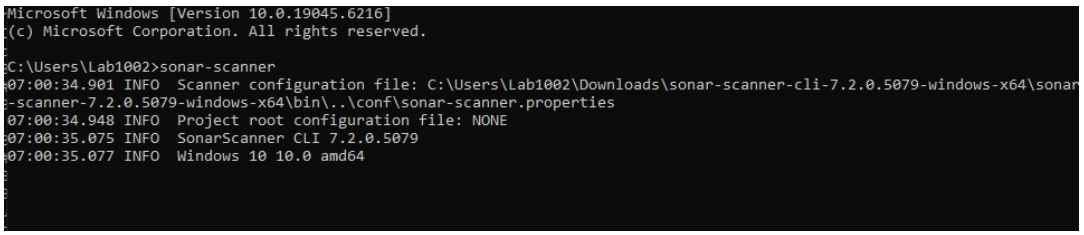
Theory: SonarQube is a static application security testing (SAST) tool that analyzes source code without executing it, helping developers identify vulnerabilities early in the development cycle. It scans for issues like SQL injection, cross-site scripting (XSS), insecure API usage, and hardcoded secrets by applying rule-based checks across multiple languages. Integrated into CI/CD pipelines, SonarQube enforces security and quality gates automatically, ensuring that only safe and maintainable code gets deployed. Its dashboard provides detailed insights and remediation guidance, while IDE plugins allow developers to fix issues directly during coding. By combining static analysis with continuous integration, SonarQube strengthens code security and reduces technical debt.

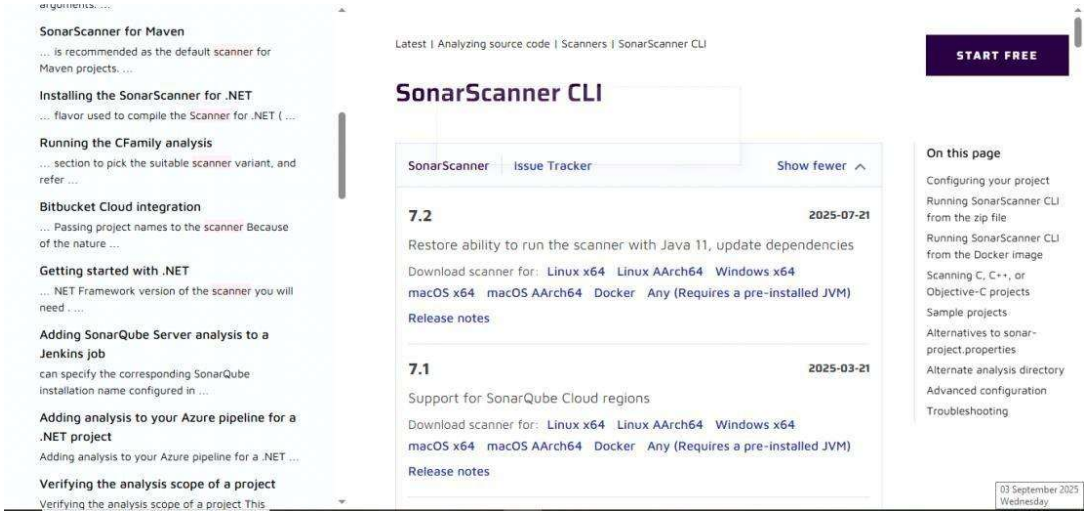
Steps:




Name
linux-x86-64
System Properties
Computer Name
Hardware
Advanced
You must be logged on as an Administrator to
Performance
Visual effects, processor scheduling, memor
User Profiles
Desktop settings related to your sign-in
Start-up and Recovery
System start-up, system failure and debuggir
OK
Environment Variables
Edit environment variable
C:\Program Files\Common Files\Oracle\Java\javapath
%SystemRoot%\system32
%SystemRoot%
%SystemRoot%\System32\Wbem
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\
%SYSTEMROOT%\System32\OpenSSH\
C:\Users\Lab1002\Downloads\sonarqube-25.9.0.112764\sonarqube-25...
New
Edit
Browse...
Delete
Move Up
Move Down
Edit text...
OK
Cancel
OK
Cancel


Administrator: C:\Windows\System32\cmd.exe - StartSonar.bat
C:\Users\Lab1002\Downloads\sonarqube-25.9.0.112764\sonarqube-25.9.0.112764>cd bin\
C:\Users\Lab1002\Downloads\sonarqube-25.9.0.112764\sonarqube-25.9.0.112764\bin>sonar-scanner\
'sonar-scanner\' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Lab1002\Downloads\sonarqube-25.9.0.112764\sonarqube-25.9.0.112764\bin>sonar-scanner
'sonar-scanner' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Lab1002\Downloads\sonarqube-25.9.0.112764\sonarqube-25.9.0.112764\bin>cd windows-x86-64
C:\Users\Lab1002\Downloads\sonarqube-25.9.0.112764\sonarqube-25.9.0.112764\bin\windows-x86-64>StartSonar.bat
Starting SonarQube...
2025.09.03 06:49:36 INFO app[][o.s.a.AppFileSystem] Cleaning or creating temp directory C:\Users\Lab1002\Downloads\sona
rqube-25.9.0.112764\sonarqube-25.9.0.112764\temp
2025.09.03 06:49:37 INFO app[][o.s.a.es.EsSettings] Elasticsearch listening on [HTTP: 127.0.0.1:9001, TCP: 127.0.0.1:{}
]
2025.09.03 06:49:37 INFO app[][o.s.a.ProcessLauncherImpl] Launch process[ELASTICSEARCH] from [C:\Users\Lab1002\Download
s\sonarqube-25.9.0.112764\sonarqube-25.9.0.112764\elasticsearch]: C:\Program Files\Java\jdk-21\bin\java -Xms4m -Xmx64m -
XX:+UseSerialGC -Dcli.name=server -Dcli.script=./bin/elasticsearch -Dcli.libs=lib/tools/server-cli -Des.path.home=C:\Use
rs\Lab1002\Downloads\sonarqube-25.9.0.112764\sonarqube-25.9.0.112764\elasticsearch -Des.path.conf=C:\Users\Lab1002\Downl
oads\sonarqube-25.9.0.112764\sonarqube-25.9.0.112764\temp\conf\es -Des.distribution.type=tar -cp C:\Users\Lab1002\Downlo
ads\sonarqube-25.9.0.112764\sonarqube-25.9.0.112764\elasticsearch\lib*;C:\Users\Lab1002\Downloads\sonarqube-25.9.0.1127
64\sonarqube-25.9.0.112764\elasticsearch\lib\cli-launcher* org.elasticsearch.launcher.CliToolLauncher
2025.09.03 06:49:37 INFO app[][o.s.a.SchedulerImpl] Waiting for Elasticsearch to be up and running
Standard Commons Logging discovery in action with spring-jcl: please remove commons-logging.jar from classpath in order
to avoid potential conflicts


Microsoft Windows [Version 10.0.19045.6216]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Lab1002>sonar-scanner
07:00:34.901 INFO Scanner configuration file: C:\Users\Lab1002\Downloads\sonar-scanner-cli-7.2.0.5079-windows-x64\sonar
-scanner-7.2.0.5079-windows-x64\bin\..\conf\sonar-scanner.properties
07:00:34.948 INFO Project root configuration file: NONE
07:00:35.075 INFO SonarScanner CLI 7.2.0.5079
07:00:35.077 INFO Windows 10 10.0 amd64

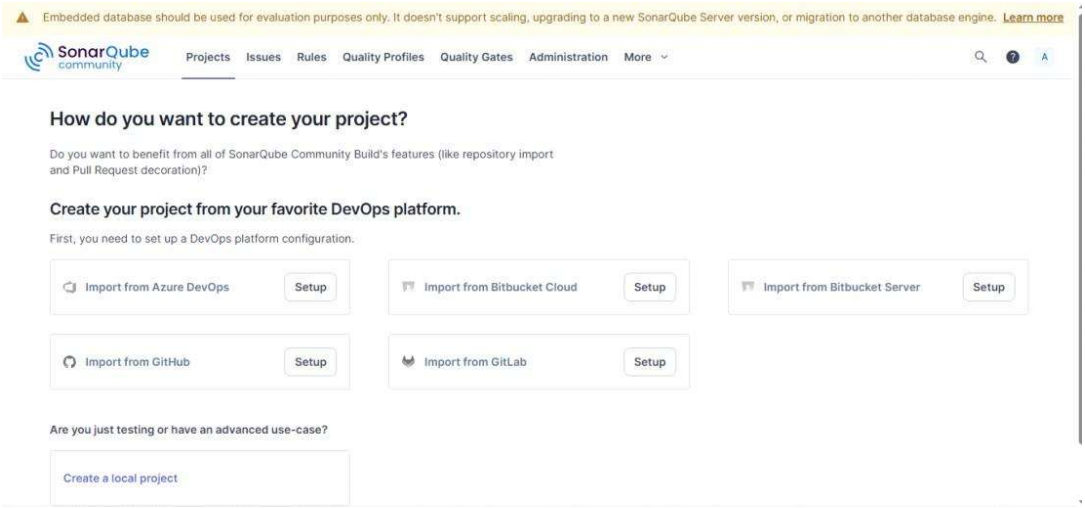

SonarScanner for Maven
... is recommended as the default scanner for Maven projects. ...
Installing the SonarScanner for .NET
... flavor used to compile the Scanner for .NET (...
Running the CFamily analysis
... section to pick the suitable scanner variant, and refer ...
Bitbucket Cloud integration
... Passing project names to the scanner Because of the nature ...
Getting started with .NET
... NET Framework version of the scanner you will need . ...
Adding SonarQube Server analysis to a Jenkins job
can specify the corresponding SonarQube installation name configured in ...
Adding analysis to your Azure pipeline for a .NET project
Adding analysis to your Azure pipeline for a .NET ...
Verifying the analysis scope of a project
Verifying the analysis scope of a project This
Latest | Analyzing source code | Scanners | SonarScanner CLI
START FREE
SonarScanner CLI
SonarScanner
Issue Tracker
Show fewer
7.2
2025-07-21
Restore ability to run the scanner with Java 11, update dependencies
Download scanner for: Linux x64 Linux AArch64 Windows x64
macOS x64 macOS AArch64 Docker Any (Requires a pre-installed JVM)
Release notes
7.1
2025-03-21
Support for SonarQube Cloud regions
Download scanner for: Linux x64 Linux AArch64 Windows x64
macOS x64 macOS AArch64 Docker Any (Requires a pre-installed JVM)
Release notes
On this page
Configuring your project
Running SonarScanner CLI from the zip file
Running SonarScanner CLI from the Docker image
Scanning C, C++, or Objective-C projects
Sample projects
Alternatives to sonar-project.properties
Alternate analysis directory
Advanced configuration
Troubleshooting
03 September 2025
Wednesday

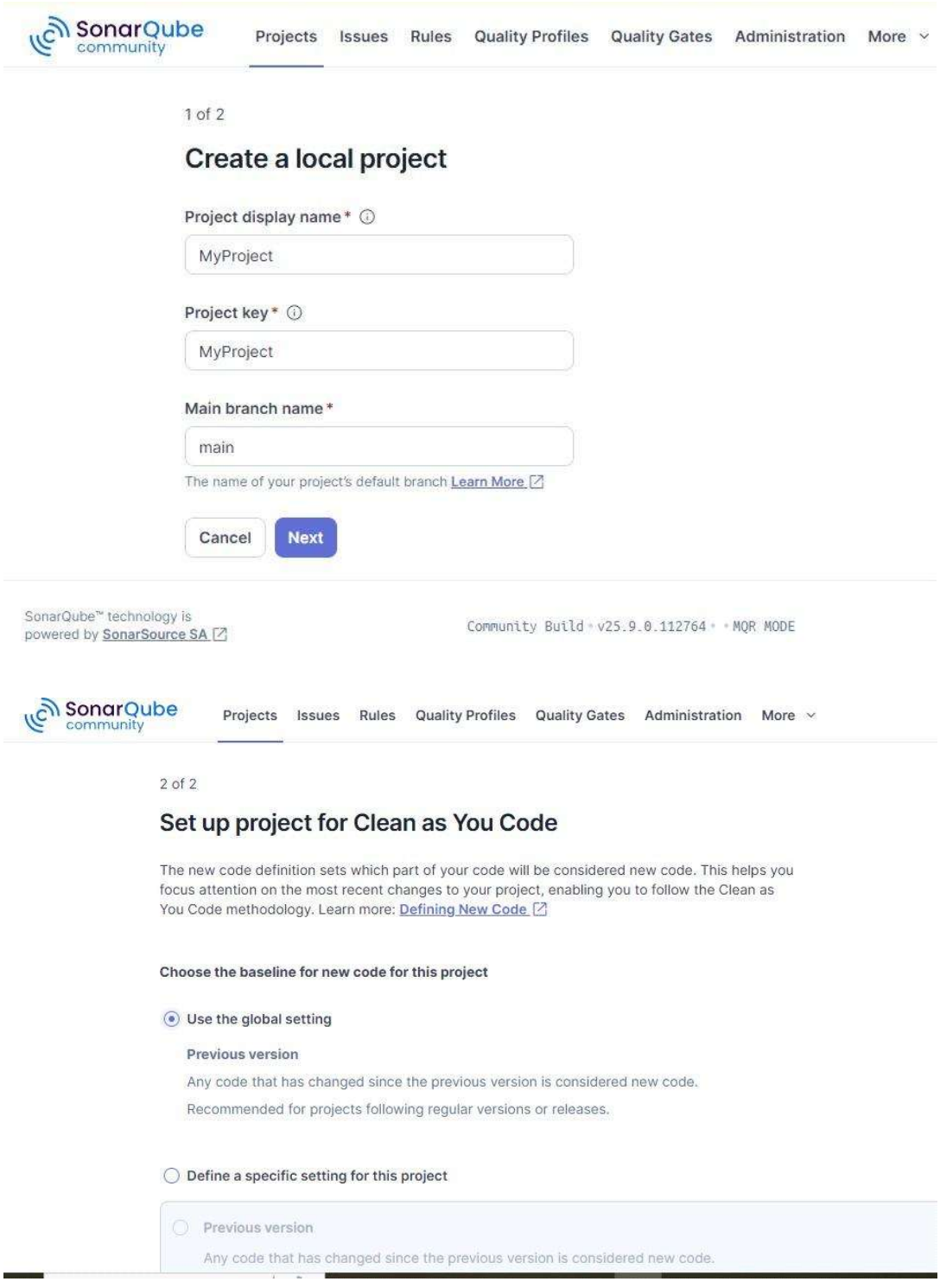

Sonar
Log in to SonarQube
Login *
Password *
Go back
Log in

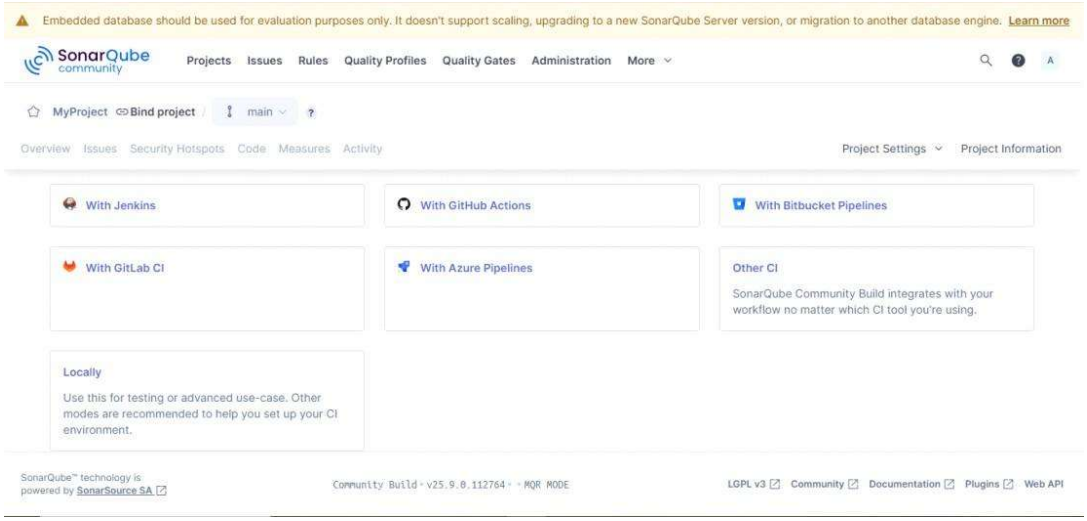

Sonar
Log in to SonarQube
Login *
admin
Password *
Go back
Log in

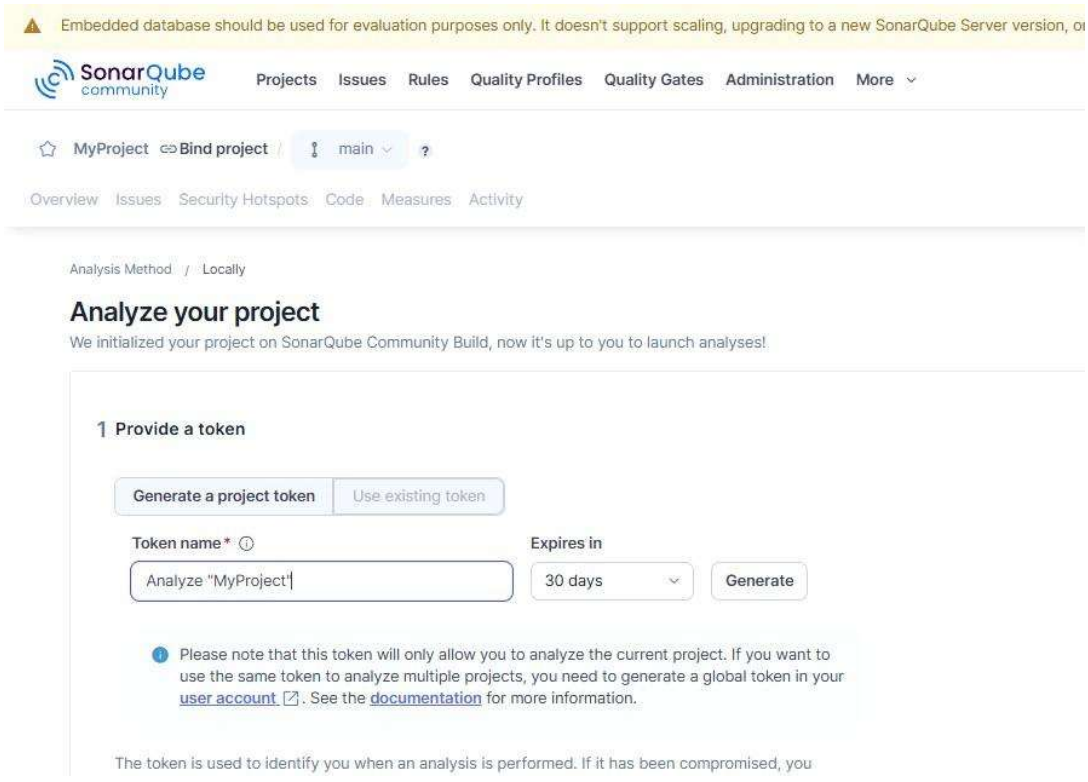

Embedded database should be used for evaluation purposes only. It doesn't support scaling, upgrading to a new SonarQube Server version, or migration to another database engine. Learn more
The way in which security, reliability, and maintainability counts and ratings are calculated has changed. Learn more in SonarQube documentation
SonarQube community
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
A

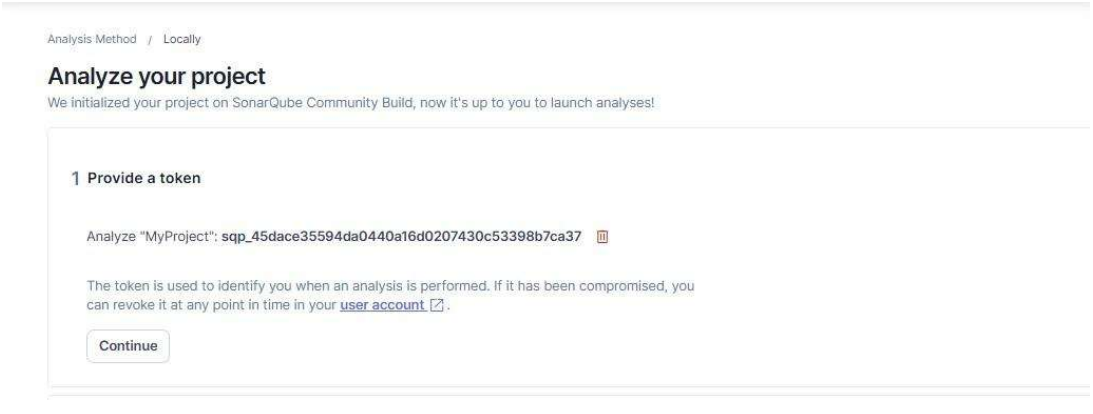

SonarQube™ technology is powered by SonarSource SA
Community Build · v25.9.0.112764 · · MQR MODE
LGPL v3
Community
Documentation
Plugins
Web API

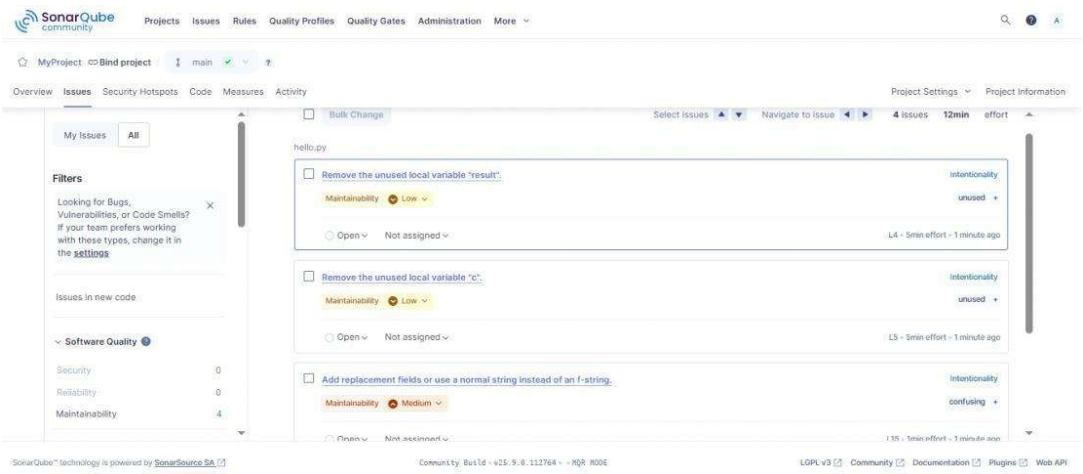

Embedded database should be used for evaluation purposes only. It doesn't support scaling, upgrading to a new SonarQube Server version, or migration to another database engine. Learn more
SonarQube community
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
A
How do you want to create your project?
Do you want to benefit from all of SonarQube Community Build'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
Setup
Import from Bitbucket Cloud
Setup
Import from Bitbucket Server
Setup
Import from GitHub
Setup
Import from GitLab
Setup
Are you just testing or have an advanced use-case?
Create a local project


SonarQube community
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
1 of 2
Create a local project
Project display name *
MyProject
Project key *
MyProject
Main branch name *
main
The name of your project's default branch Learn More
Cancel
Next
SonarQube™ technology is powered by SonarSource SA
Community Build • v25.9.0.112764 • MQR MODE
SonarQube community
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
2 of 2
Set up project for Clean as You Code
The new code definition sets which part of your code will be considered new code. This helps you focus attention on the most recent changes to your project, enabling you to follow the Clean as You Code methodology. Learn more: Defining New Code
Choose the baseline for new code for this project
Use the global setting
Previous version
Any code that has changed since the previous version is considered new code.
Recommended for projects following regular versions or releases.
Define a specific setting for this project
Previous version
Any code that has changed since the previous version is considered new code.


Embedded database should be used for evaluation purposes only. It doesn't support scaling, upgrading to a new SonarQube Server version, or migration to another database engine. Learn more
SonarQube community
Projects Issues Rules Quality Profiles Quality Gates Administration More
MyProject Bind project main
Overview Issues Security Hotspots Code Measures Activity
Project Settings Project Information
With Jenkins
With GitHub Actions
With Bitbucket Pipelines
With GitLab CI
With Azure Pipelines
Other CI
SonarQube Community Build integrates with your workflow no matter which CI tool you're using.
Locally
Use this for testing or advanced use-case. Other modes are recommended to help you set up your CI environment.
SonarQube™ technology is powered by SonarSource SA
Community Build · v25.9.0.112764 · MQR MODE
LGPL v3 Community Documentation Plugins Web API


Embedded database should be used for evaluation purposes only. It doesn't support scaling, upgrading to a new SonarQube Server version, o
SonarQube community
Projects Issues Rules Quality Profiles Quality Gates Administration More
MyProject Bind project main
Overview Issues Security Hotspots Code Measures Activity
Analysis Method / Locally
Analyze your project
We initialized your project on SonarQube Community Build, now it's up to you to launch analyses!
1 Provide a token
Generate a project token
Use existing token
Token name *
Analyze "MyProject"
Expires in
30 days
Generate
Please note that this token will only allow you to analyze the current project. If you want to use the same token to analyze multiple projects, you need to generate a global token in your user account. See the documentation for more information.
The token is used to identify you when an analysis is performed. If it has been compromised, you

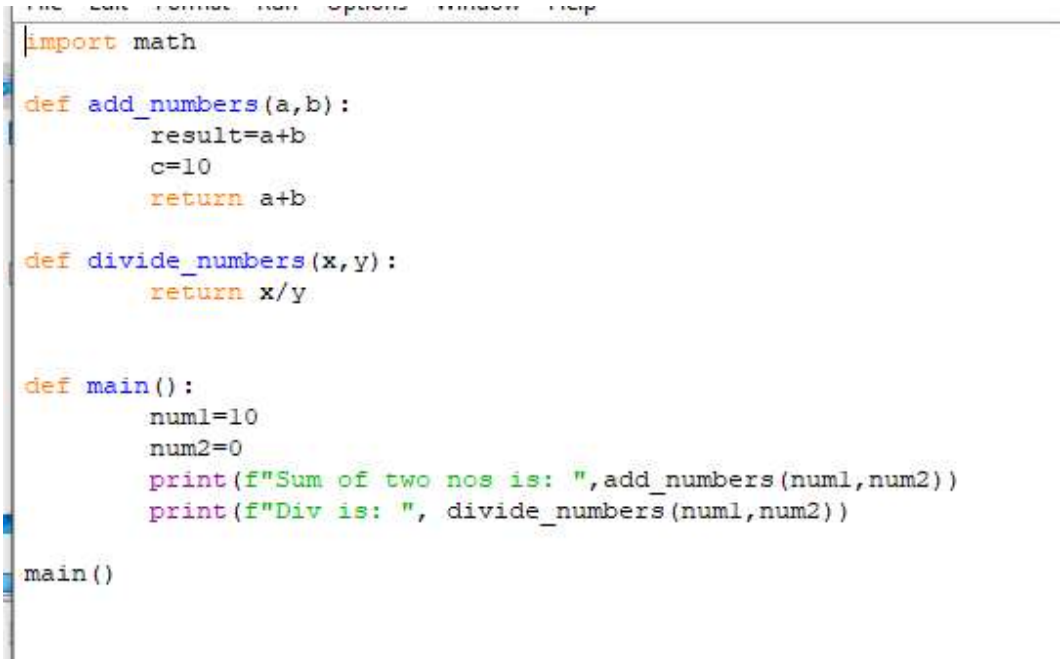





```
  * Any directory in the file path is named: "doc", "docs", "test" or "tests"
  * Any directory in the file path has a name ending in "test" or "tests"

INFO: Start fetching files for the text and secrets analysis
INFO: Using JGit to retrieve untracked files
WARNING: Retrieving only language associated files, make sure to run the analysis inside a git repository to make
 inclusions specified via "sonar.text.inclusions"
INFO: Starting the text and secrets analysis
INFO: 1 source file to be analyzed for the text and secrets analysis
INFO: 1/1 source file has been analyzed for the text and secrets analysis
INFO: Sensor TextAndSecretsSensor [text] (done) | time=4559ms
INFO: ------------- Run sensors on project
INFO: Sensor Zero Coverage Sensor
INFO: Sensor Zero Coverage Sensor (done) | time=24ms
INFO: ------------- Gather SCA dependencies on project
INFO: Dependency analysis skipped
INFO: SCM Publisher No SCM system was detected. You can use the 'sonar.scm.provider' property to explicitly specif
INFO: CPD Executor Calculating CPD for 1 file
INFO: CPD Executor CPD calculation finished (done) | time=19ms
INFO: Analysis report generated in 383ms, dir size=250.5 kB
INFO: Analysis report compressed in 42ms, zip size=29.0 kB
INFO: Analysis report uploaded in 790ms
INFO: ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=MyProject
INFO: Note that you will be able to access the updated dashboard once the server has processed the submitted analy
port
INFO: More about the report processing at http://localhost:9000/api/ce/task?id=540adf3f-4ab9-4d14-aa38-8fb43cdcab2
INFO: Analysis total time: 13.962 s
INFO: SonarScanner Engine completed successfully

C:\Users\Lab1002\Desktop\CICD>
```



```
import math

def add_numbers(a,b):
        result=a+b
        c=10
        return a+b

def divide_numbers(x,y):
        return x/y


def main():
        num1=10
        num2=0
        print(f"Sum of two nos is: ",add_numbers(num1,num2))
        print(f"Div is: ", divide_numbers(num1,num2))

main()
```

Conclusion: Thus, we ensure that Python code undergoes early and thorough security checks using SonarQube's SAST process, minimizing vulnerabilities before runtime. We strengthen code integrity by enforcing consistent standards across the development lifecycle. Ultimately, we achieve safer, more maintainable Python applications with reduced risk and technical debt.

LO Mapping: LO4

ASSIGNMENT 8

AIM: To understand Continuous Monitoring using Nagios.

THEORY:
Nagios Core is a powerful open-source monitoring tool used to monitor systems, networks, and infrastructure. It provides real-time alerting and visualization for servers, services, switches, applications, and more.

Key Features:

- Server & network monitoring
- Email/SMS alerts for failures
- Web interface for visualization
- Extensible with plugins and custom checks

Prerequisites

- A Linux machine (Ubuntu/Debian-based system)
- Root or `sudo` privileges
- Apache web server
- Basic networking knowledge

STEPS:

1. Update System & Install Dependencies

```
sudo apt update
sudo apt install -y apache2 php libapache2-mod-php build-essential \
  libgd-dev unzip curl wget libssl-dev daemon make gcc
```

2. Create Nagios User and Group

```
sudo useradd nagios
sudo groupadd nagcmd
sudo usermod -aG nagcmd nagios
sudo usermod -aG nagcmd www-data
```

3. Download and Compile Nagios Core

```
cd /tmp
wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.5.1.tar.gz
tar -xzf nagios-4.5.1.tar.gz
cd nagios-4.5.1
./configure --with-command-group=nagcmd
make all
sudo make install
```

sudo make install-commandmode
sudo make install-init
sudo make install-config
sudo make install-webconf

. Set Up Web Interface Authentication
Create a login user for the web interface (e.g. `admin`):
sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users admin
Note: Choose a strong password and remember it.

5. nstall Nagios Plugins

cd /tmp
wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz
tar -xzf nagios-plugins-2.3.3.tar.gz
cd nagios-plugins-2.3.3
./configure --with-nagios-user=nagios --with-nagios-group=nagios
make
sudo make install

6. Enable Required Apache Modules

sudo a2enmod rewrite cgi
sudo systemctl restart apache2
7. Start Nagios Service

bash
sudo systemctl enable nagios
sudo systemctl start nagios

Accessing the Nagios Web Interface

Steps:

1. Get your server IP:

ip a | grep inet

Example output: `192.168.4.104`

2. Open a browser and visit:

http://192.168.4.104/nagios

3. Login with:

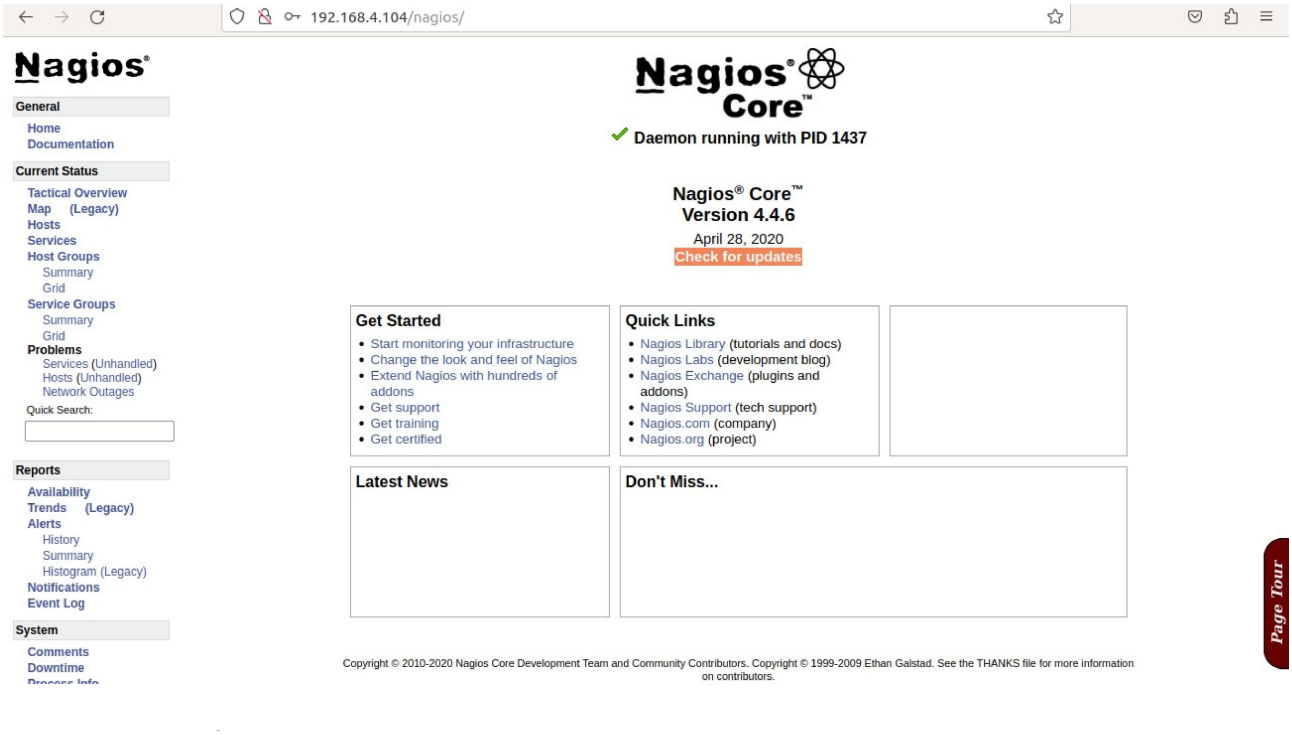
Username: `admin`

Password: (the one you set earlier)

```
lab1002@lab1002-HP-280-G3-MT:~$ sudo apt update
Hit:1 https://download.docker.com/linux/ubuntu bionic InRelease
Hit:2 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu bionic InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:5 http://in.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
47 packages can be upgraded. Run 'apt list --upgradable' to see them.
lab1002@lab1002-HP-280-G3-MT:~$ sudo apt install -y autoconf gcc make unzip apac
he2 php libapache2-mod-php \
>   libgd-dev libmcrypt-dev libssl-dev daemon wget bc gawk dc build-essential \
>   snmp libnet-snmp-perl gettext
Reading package lists... Done
Building dependency tree
Reading state information... Done
bc is already the newest version (1.07.1-2).
bc set to manually installed.
build-essential is already the newest version (12.4ubuntu1).
```

```
lab1002@lab1002-HP-280-G3-MT:~$ sudo usermod -a -G nagcmd nagios
lab1002@lab1002-HP-280-G3-MT:~$ sudo usermod -a -G nagcmd www-data
lab1002@lab1002-HP-280-G3-MT:~$ ip a | grep inet
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 192.168.4.104/24 brd 192.168.4.255 scope global dynamic noprefixroute e
np4s0
    inet6 fe80::59a0:c15b:f605:a620/64 scope link noprefixroute
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
lab1002@lab1002-HP-280-G3-MT:~$ ls /etc/apache2/sites-enabled/nagios.conf
/etc/apache2/sites-enabled/nagios.conf
lab1002@lab1002-HP-280-G3-MT:~$ sudo systemctl reload apache2
lab1002@lab1002-HP-280-G3-MT:~$ ls /usr/local/nagios/share
angularjs              includes            media
bootstrap-3.3.7        index.php           robots.txt
config.inc.php         infobox.html        side.php
contexthelp            js                  spin
d3                     jsonquery.html      ssi
docs                   locale              stylesheets
graph-header.html      main.php            trends-form.html
histogram-form.html    map-directive.html  trends-graph.html
histogram-graph.html   map-form.html       trends-host-yaxis.html
```

```
lab1002@lab1002-HP-280-G3-MT:~$ cat /usr/local/nagios/etc/htpasswd.users
admin:$apr1$2XweygvH$ReiuYPl/sfqlhcYq9xuMn/
lab1002@lab1002-HP-280-G3-MT:~$ sudo a2enmod rewrite cgi
Module rewrite already enabled
Module cgi already enabled
lab1002@lab1002-HP-280-G3-MT:~$ sudo systemctl restart apache2
lab1002@lab1002-HP-280-G3-MT:~$ sudo htpasswd /usr/local/nagios/etc/htpasswd.use
rs admin
New password:
Re-type new password:
Updating password for user admin
lab1002@lab1002-HP-280-G3-MT:~$ sudo systemctl restart apache2
lab1002@lab1002-HP-280-G3-MT:~$
```



CONCLUSION: This experiment successfully demonstrates the use of Nagios for continuous monitoring of IT infrastructure. It provides a clear understanding of how N tracks the health and performance of servers, services, and network devices, generates time alerts, and displays system status through a web interface. Continuous monitorin Nagios enables proactive detection of issues, reduces downtime, and ensures reliable a efficient management of critical systems and services.

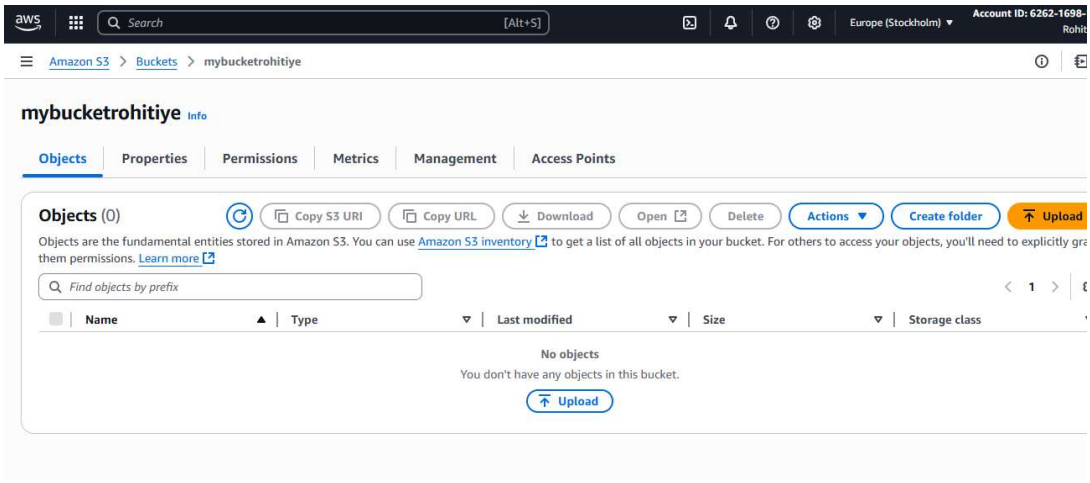
LO MAPPING: LO5

Assignment 9:S3 lambda

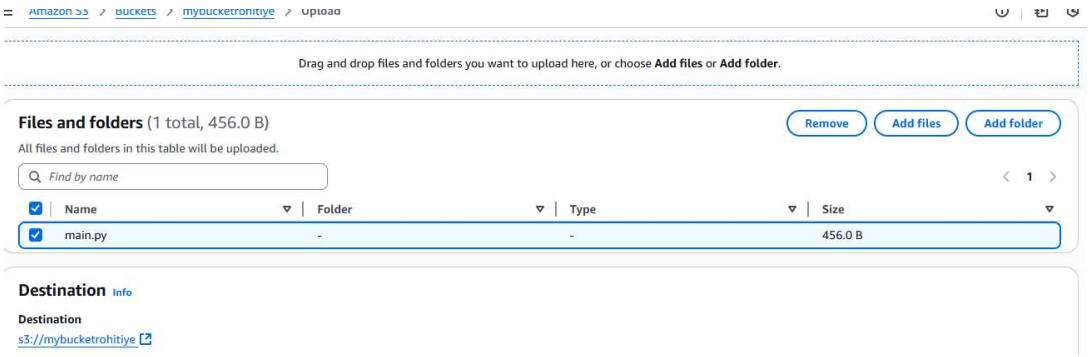
Aim: To understand lambda functions and create a lambda function using python to log message once file is added to S3 bucket

Theory- In AWS, a Lambda function is a serverless compute service that runs code in response to events without managing servers. When integrated with Amazon S3, it can automatically trigger actions—like processing files or updating databases—whenever objects are uploaded, modified, or deleted in a bucket. This enables real-time automation and streamlines workflows across cloud applications.

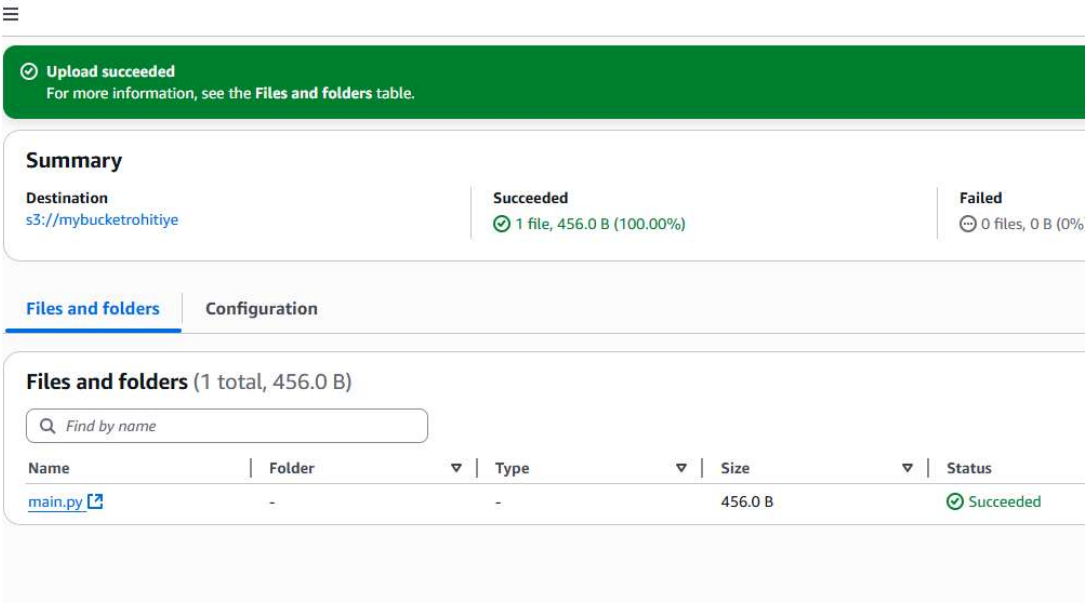
1)



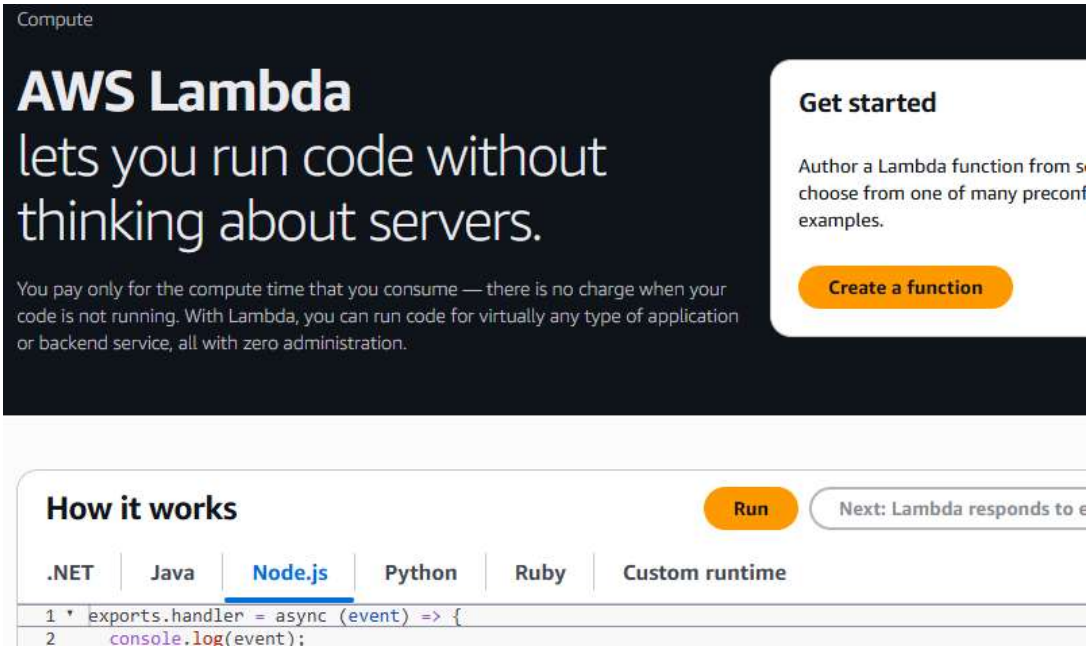
2)



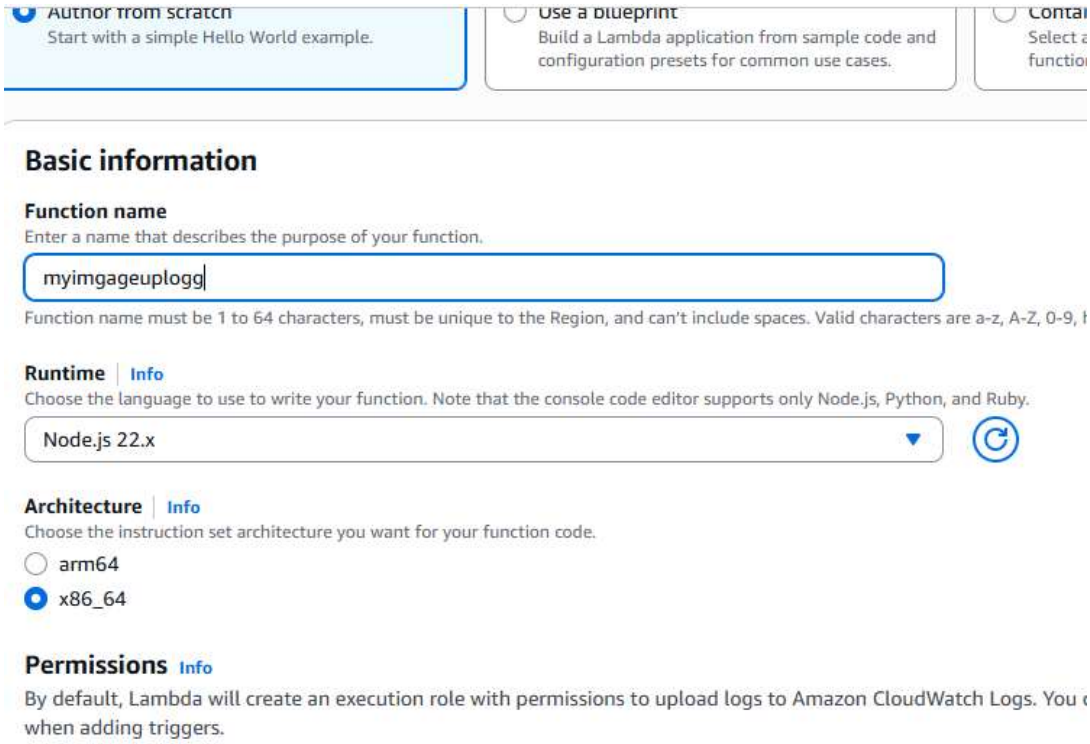
3)


Upload succeeded
For more information, see the Files and folders table.
Summary
Destination
s3://mybucketrohitiye
Succeeded
1 file, 456.0 B (100.00%)
Failed
0 files, 0 B (0%
Files and folders
Configuration
Files and folders (1 total, 456.0 B)
Find by name
Name
Folder
Type
Size
Status
main.py
-
-
456.0 B
Succeeded

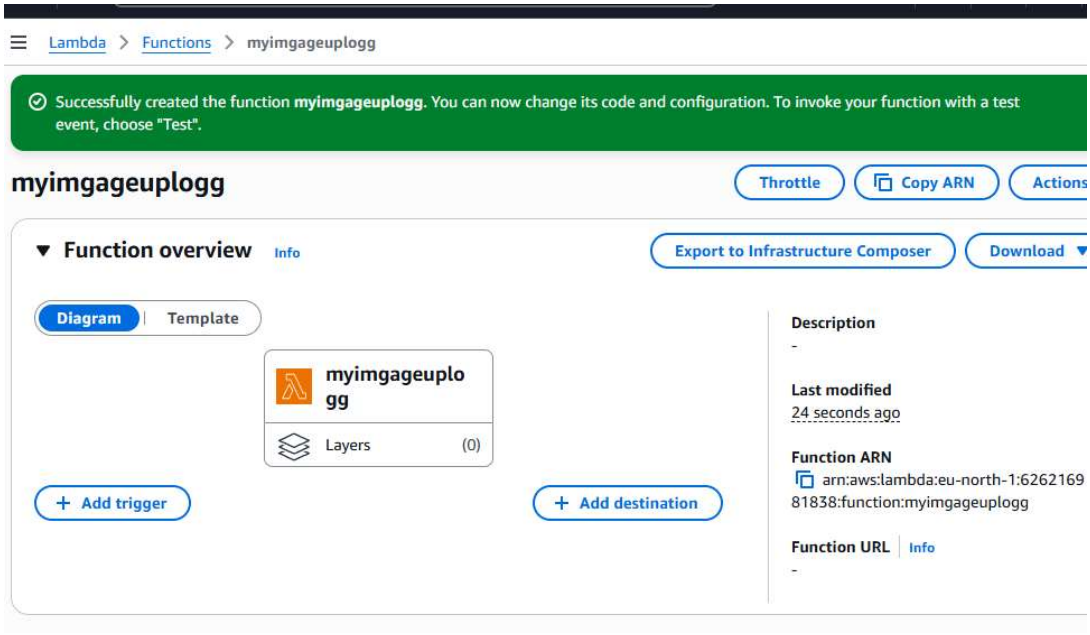
4)


Compute
AWS Lambda
lets you run code without thinking about servers.
You pay only for the compute time that you consume — there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or backend service, all with zero administration.
Get started
Author a Lambda function from s
choose from one of many preconf
examples.
Create a function
How it works
Run
Next: Lambda responds to e
.NET
Java
Node.js
Python
Ruby
Custom runtime
1 ▾ exports.handler = async (event) => {
2 console.log(event);

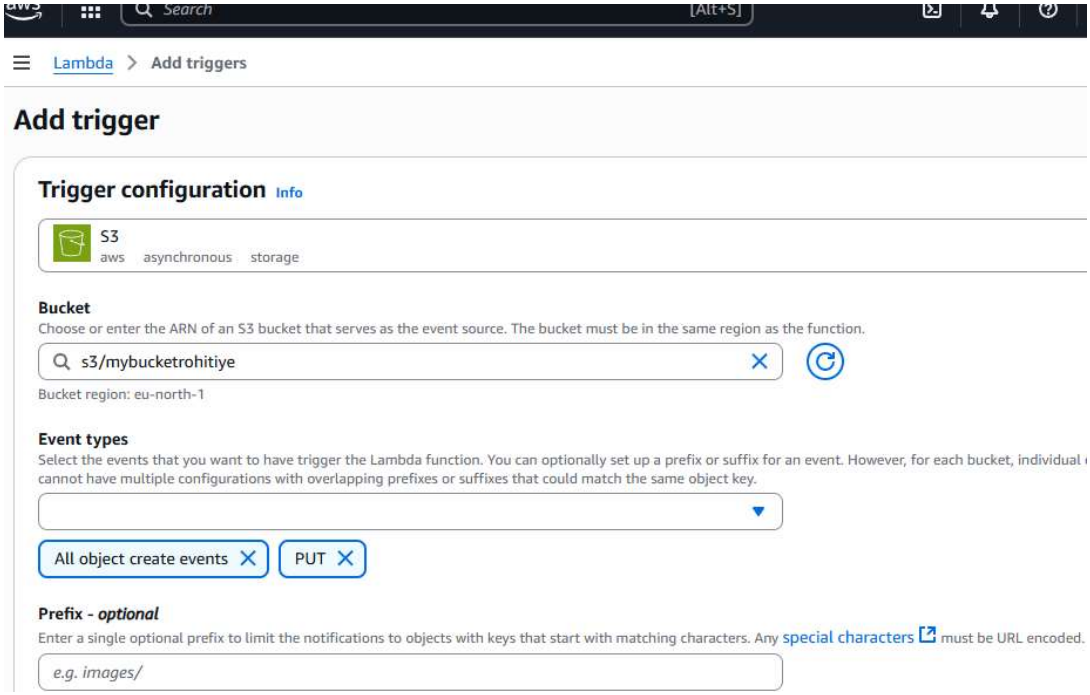
5)


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.
Basic information
Function name
Enter a name that describes the purpose of your function.
myimgageuplogg
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,
Runtime Info
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.
Node.js 22.x
Architecture Info
Choose the instruction set architecture you want for your function code.
arm64
x86_64
Permissions Info
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You
when adding triggers.

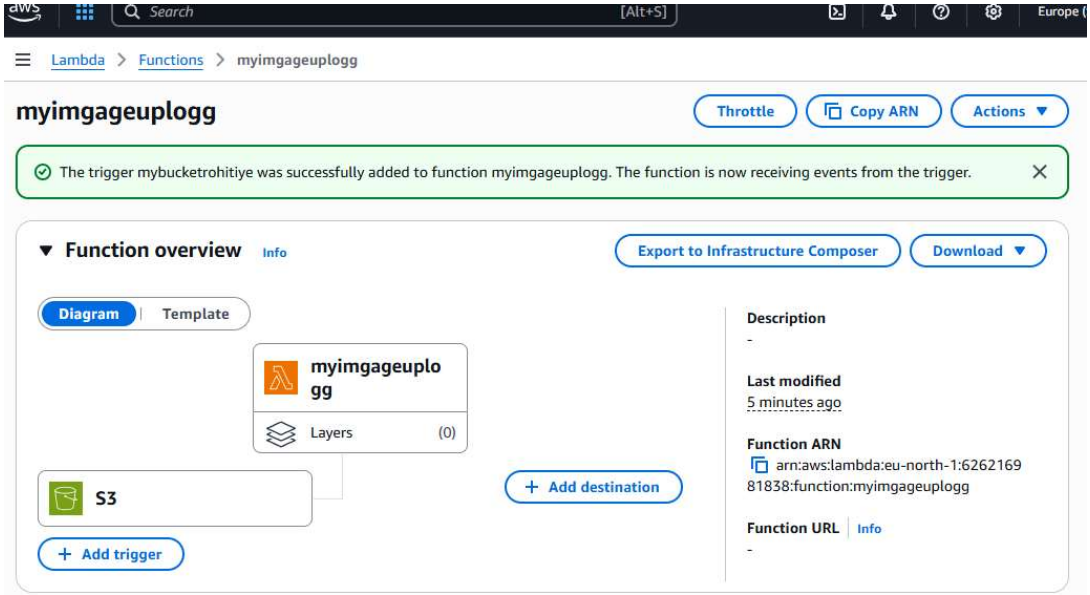
6)


Lambda > Functions > myimgageuplogg
Successfully created the function myimgageuplogg. You can now change its code and configuration. To invoke your function with a test event, choose "Test".
myimgageuplogg
Throttle
Copy ARN
Actions
Function overview Info
Export to Infrastructure Composer
Download
Diagram
Template
myimgageuplo gg
Layers (0)
Add trigger
Add destination
Description
-
Last modified
24 seconds ago
Function ARN
arn:aws:lambda:eu-north-1:6262169 81838:function:myimgageuplogg
Function URL Info
-

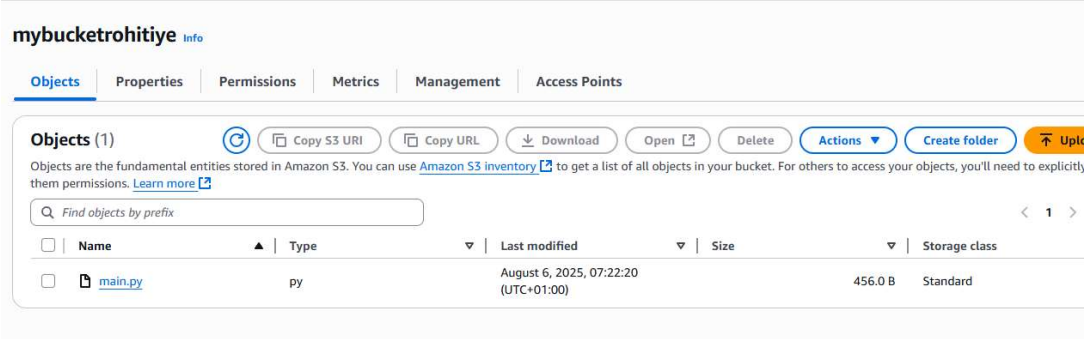
7)

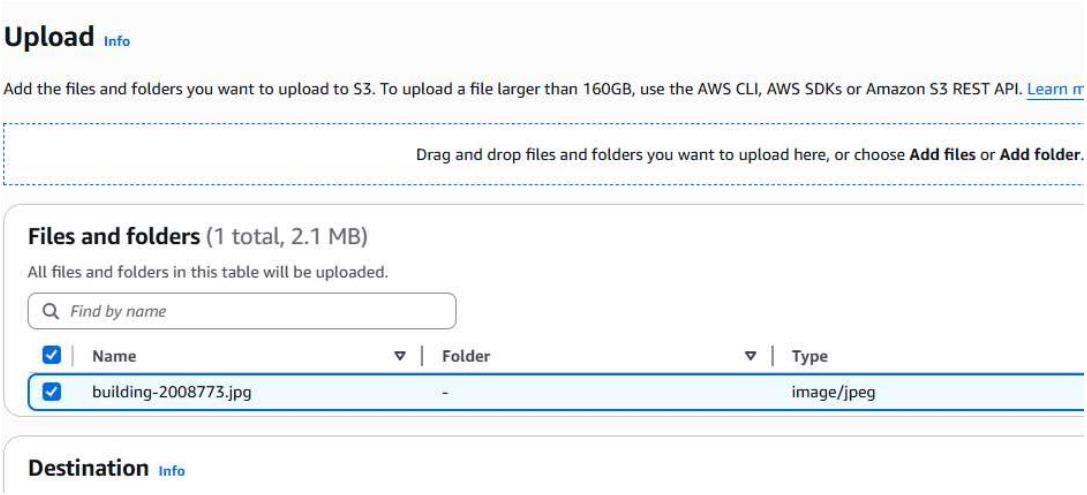

Search
[Alt+S]
Lambda > Add triggers
Add trigger
Trigger configuration Info
S3
aws asynchronous storage
Bucket
Choose or enter the ARN of an S3 bucket that serves as the event source. The bucket must be in the same region as the function.
s3/mybucketrohitiye
Bucket region: eu-north-1
Event types
Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual
cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.
All object create events
PUT
Prefix - optional
Enter a single optional prefix to limit the notifications to objects with keys that start with matching characters. Any special characters must be URL encoded.
e.g. images/

8)

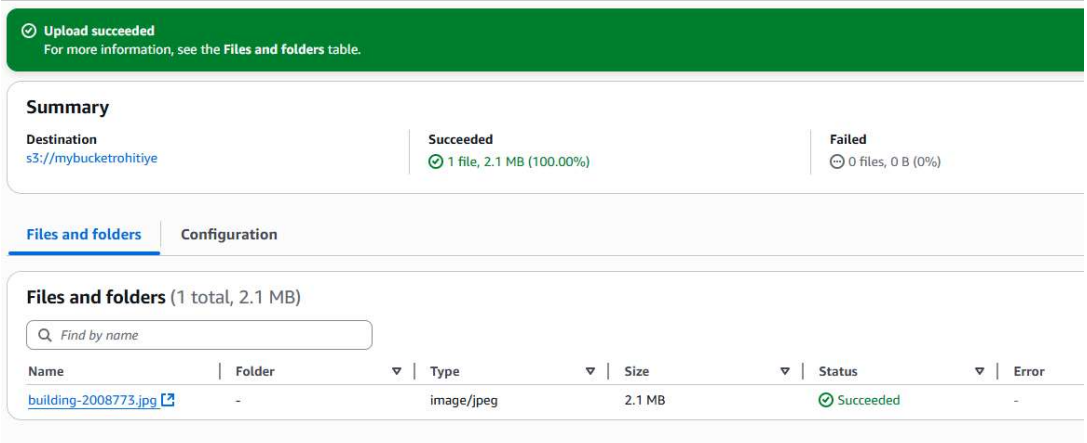

Search
[Alt+S]
Europe
Lambda > Functions > myimgageuplogg
myimgageuplogg
Throttle
Copy ARN
Actions
The trigger mybucketrohitiye was successfully added to function myimgageuplogg. The function is now receiving events from the trigger.
Function overview Info
Export to Infrastructure Composer
Download
Diagram
Template
myimgageuplogg
Layers (0)
S3
Add destination
Add trigger
Description
-
Last modified
5 minutes ago
Function ARN
arn:aws:lambda:eu-north-1:626216981838:function:myimgageuplogg
Function URL Info
-

9)

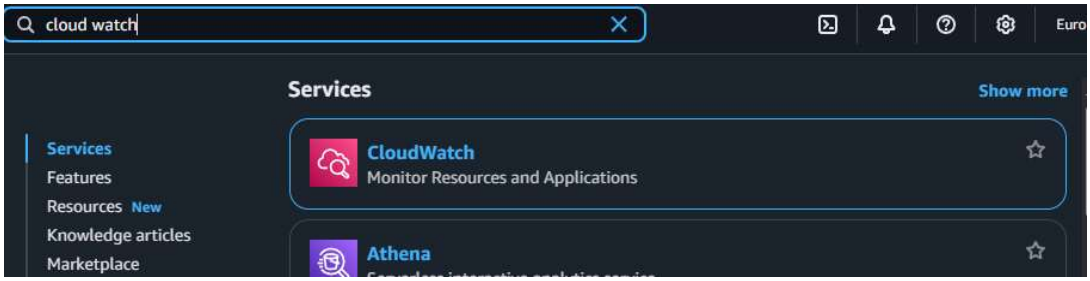

mybucketrohitiye Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (1)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly them permissions. Learn more
Find objects by prefix
Name
Type
Last modified
Size
Storage class
main.py
py
August 6, 2025, 07:22:20 (UTC+01:00)
456.0 B
Standard


Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. Learn m
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (1 total, 2.1 MB)
All files and folders in this table will be uploaded.
Find by name
Name
Folder
Type
building-2008773.jpg
-
image/jpeg
Destination Info

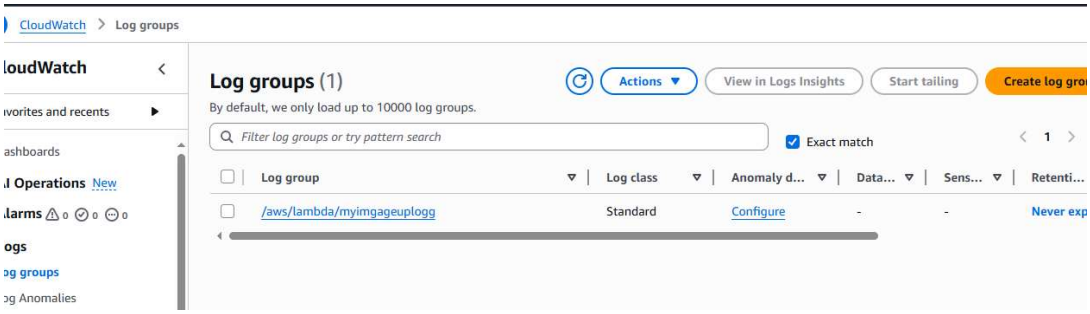
10)


Upload succeeded
For more information, see the Files and folders table.
Summary
Destination
s3://mybucketrohitiye
Succeeded
1 file, 2.1 MB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 total, 2.1 MB)
Find by name
Name
Folder
Type
Size
Status
Error
building-2008773.jpg
-
image/jpeg
2.1 MB
Succeeded
-

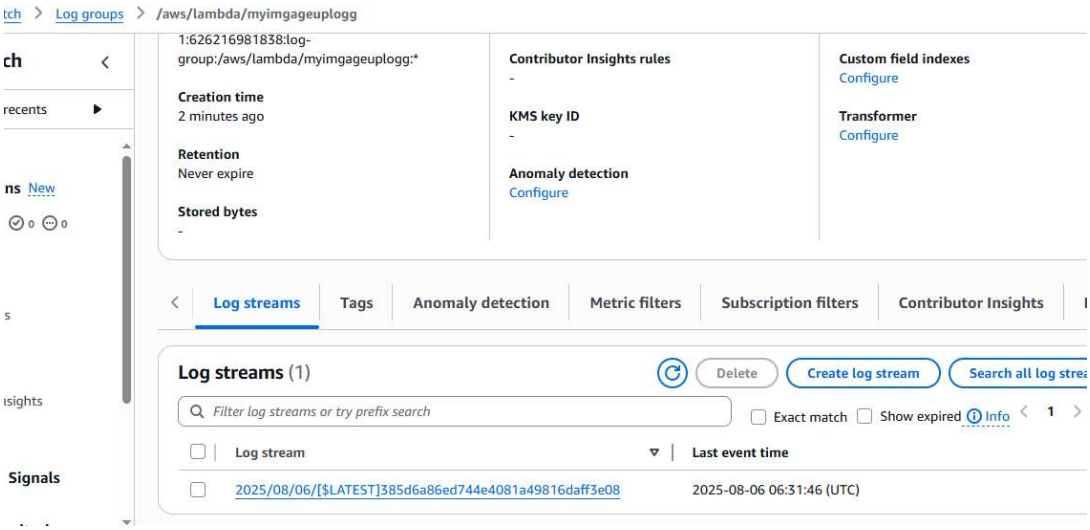
11)



12)



13)



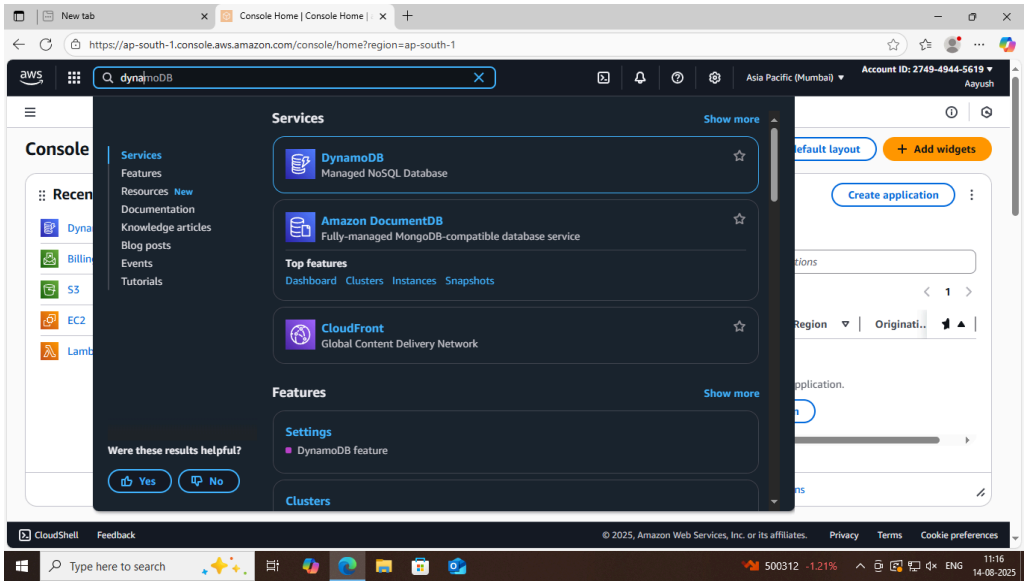
Conclusion- In conclusion, integrating AWS Lambda with Amazon S3 using Python offers a powerful, serverless solution for automating file-based workflows. By triggering Lambda functions on S3 events—such as object uploads or deletions—developers can process data in real time without provisioning or managing infrastructure. This approach enhances scalability, reduces operational overhead, and enables seamless integration with other AWS services, making it ideal for building efficient, event-driven cloud applications.

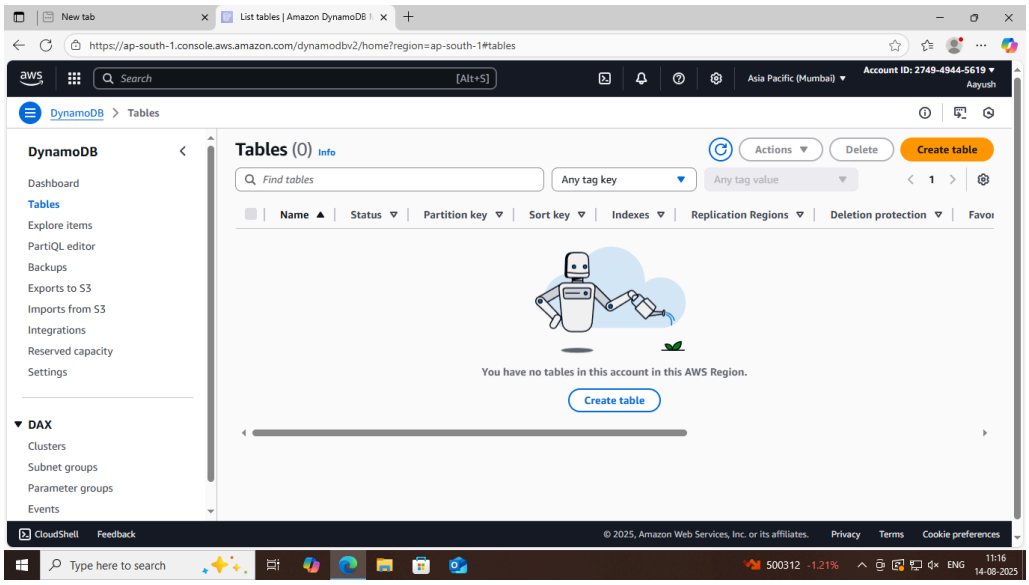
LO Mapping: LO6

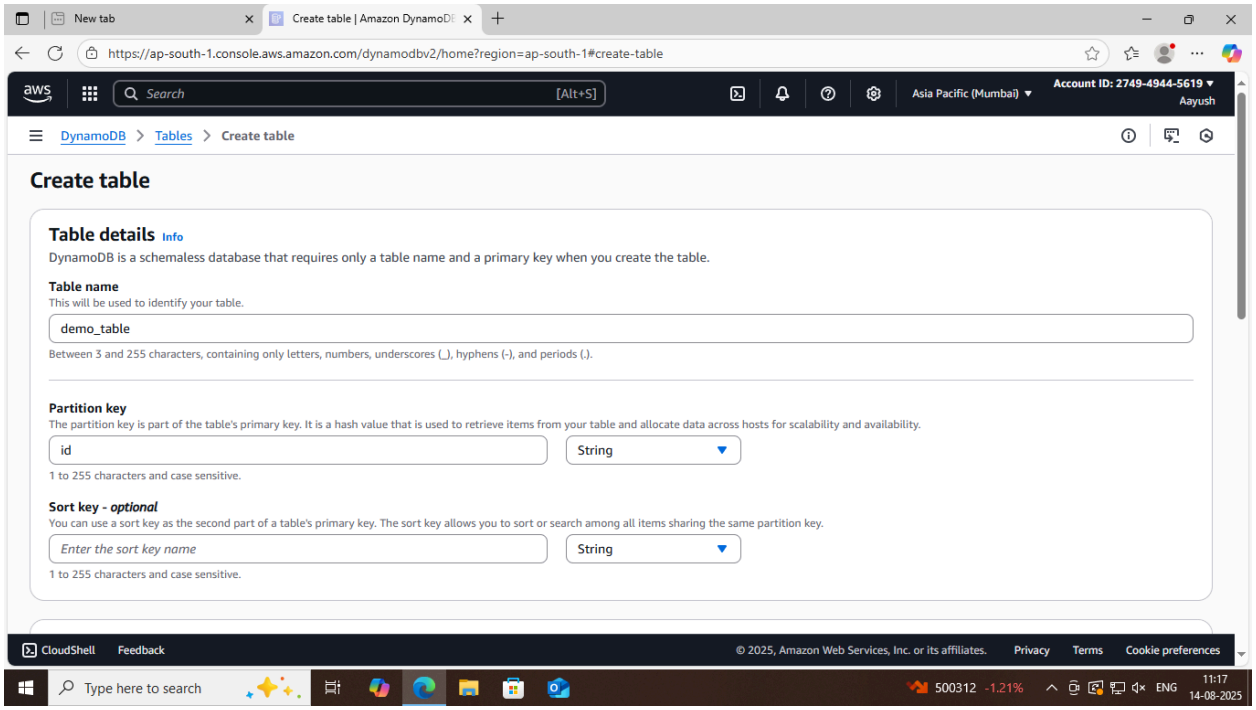
Assignment-10

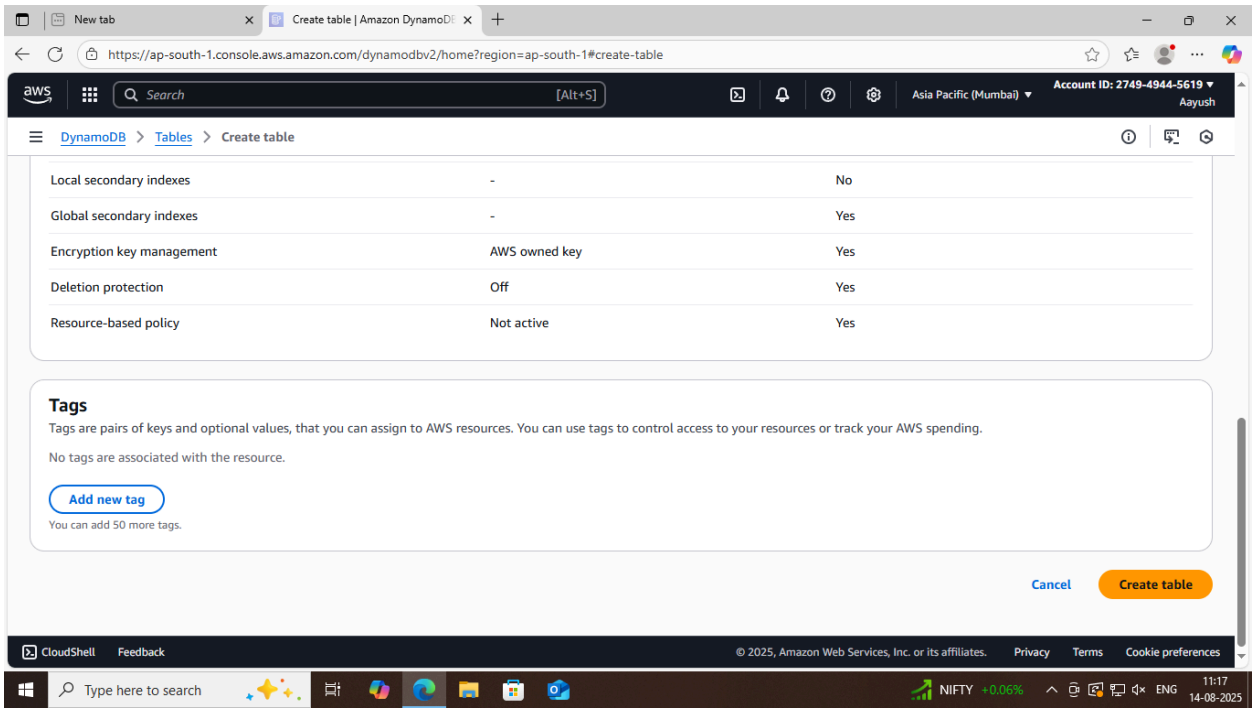
Aim: To create a lambda function using python for adding data to dynamo DB database.

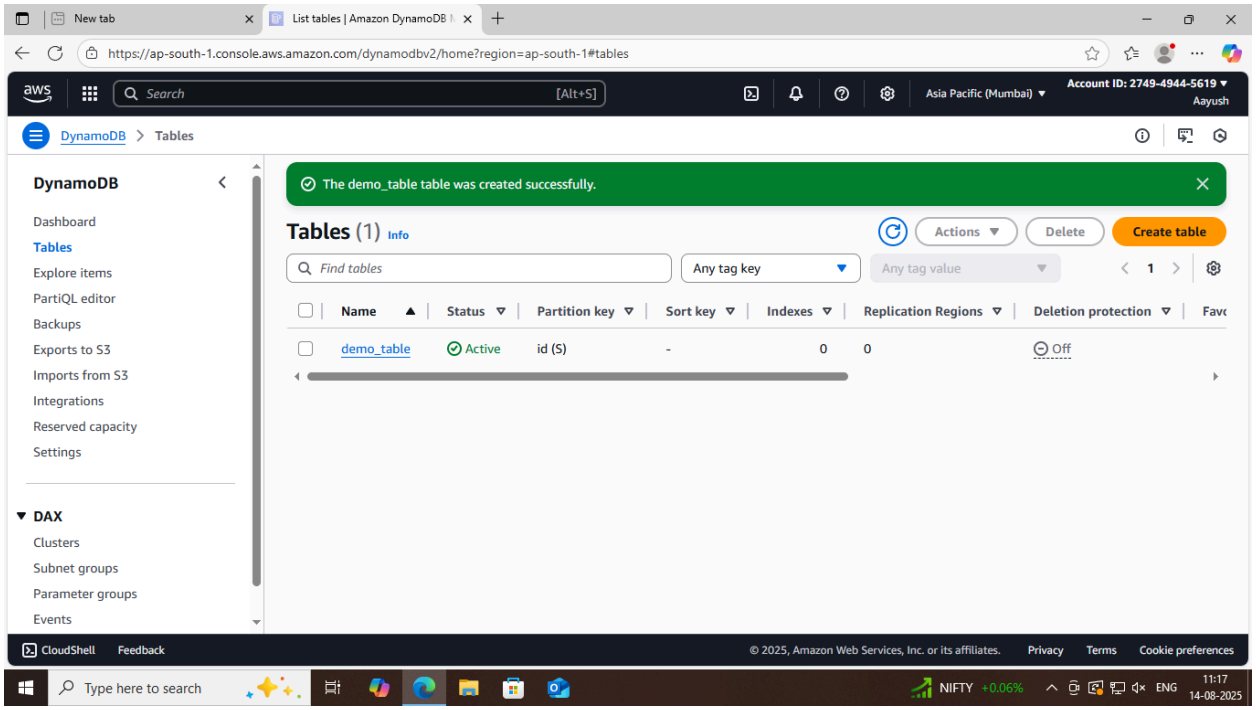
Theory: A Python lambda function for adding data to a DynamoDB table typically serves as a lightweight, serverless backend component triggered by events such as API calls or changes in other AWS services. Using the AWS SDK for Python (boto3), the lambda function initializes a DynamoDB client or resource, constructs an item with the required attributes, and performs a ”put_item” operation to insert the data into the specified DynamoDB table. This approach enables scalable, on-demand data insertion without managing servers, making it ideal for event-driven applications and real-time data processing in cloud environments.

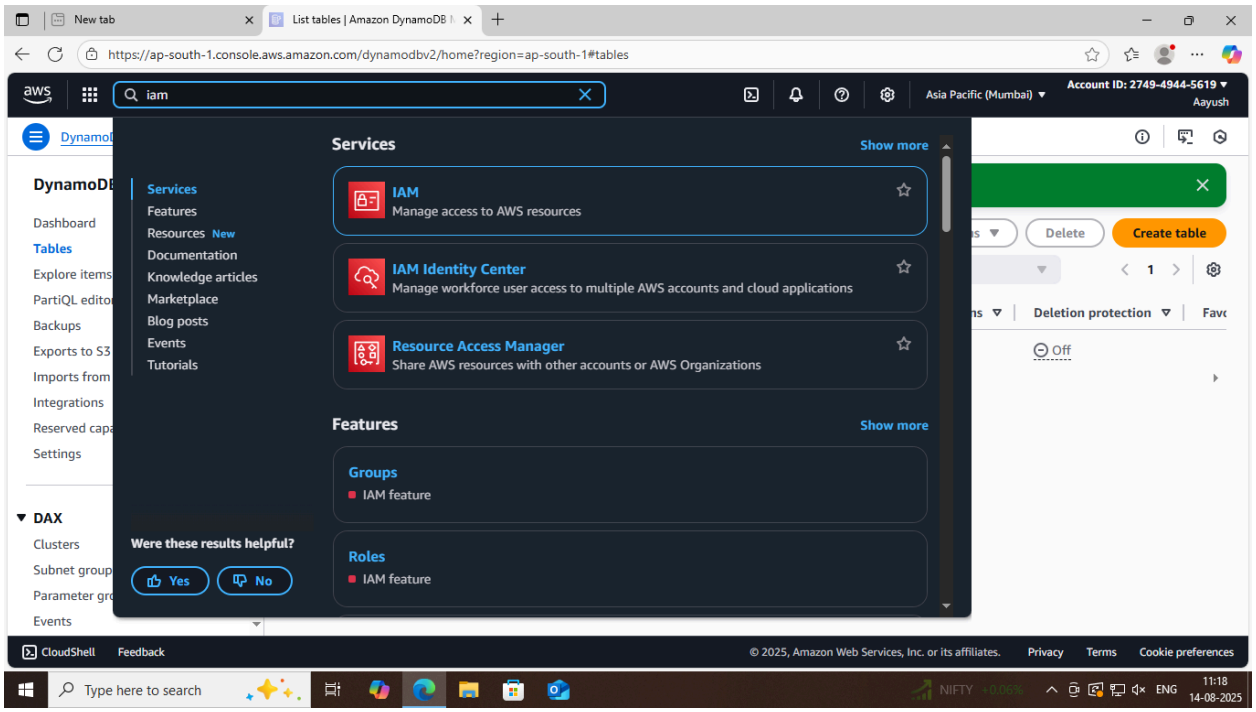


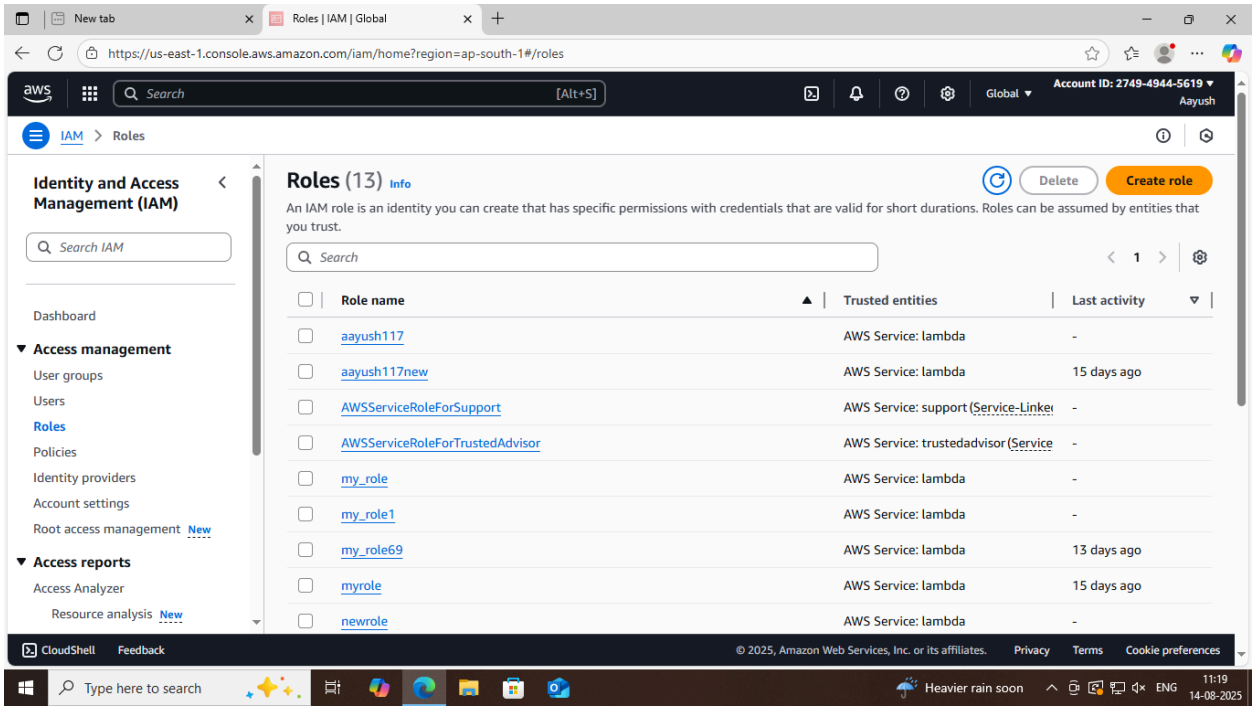


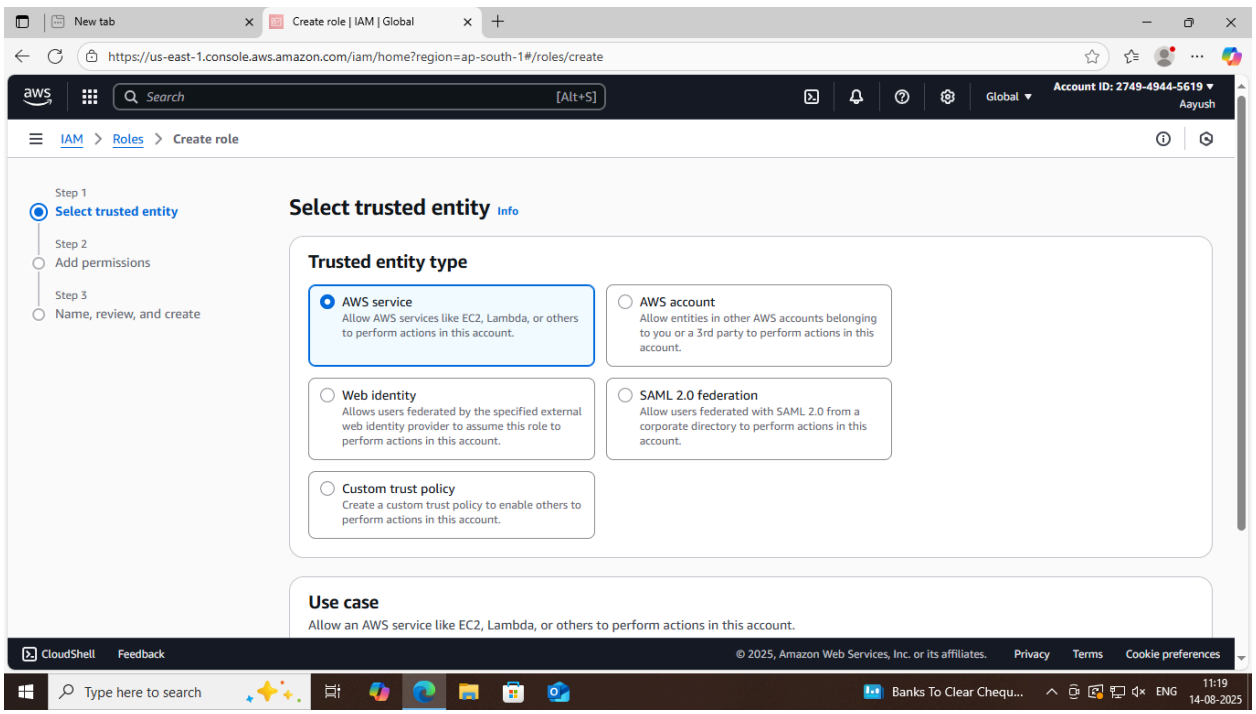

New tab
Create table | Amazon DynamoDB
https://ap-south-1.console.aws.amazon.com/dynamodbv2/home?region=ap-south-1#create-table
Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 2749-4944-5619
Aayush
DynamoDB > Tables > Create table
Create table
Table details Info
DynamoDB is a schemaless database that requires only a table name and a primary key when you create the table.
Table name
This will be used to identify your table.
demo_table
Between 3 and 255 characters, containing only letters, numbers, underscores (_), hyphens (-), and periods (.).
Partition key
The partition key is part of the table's primary key. It is a hash value that is used to retrieve items from your table and allocate data across hosts for scalability and availability.
id
String
1 to 255 characters and case sensitive.
Sort key - optional
You can use a sort key as the second part of a table's primary key. The sort key allows you to sort or search among all items sharing the same partition key.
Enter the sort key name
String
1 to 255 characters and case sensitive.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
500312 -1.21%
ENG
11:17
14-08-2025

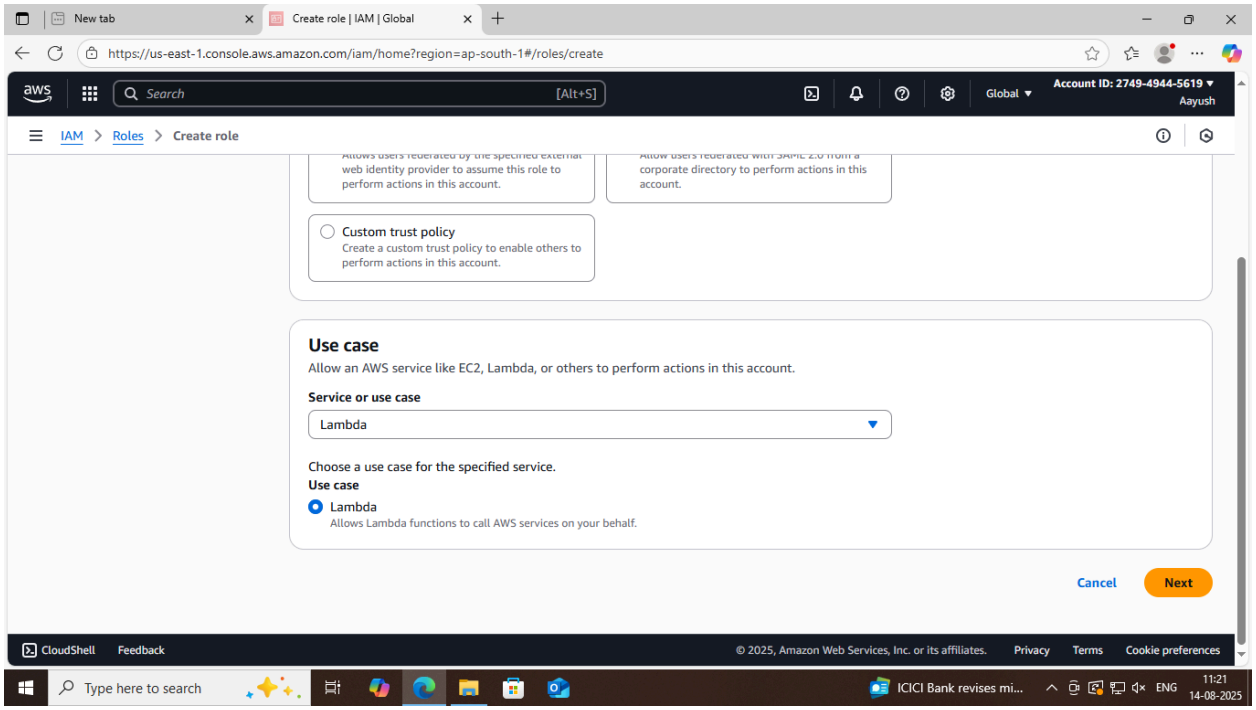

New tab
Create table | Amazon DynamoDB
https://ap-south-1.console.aws.amazon.com/dynamodbv2/home?region=ap-south-1#create-table
Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 2749-4944-5619
Aayush
DynamoDB > Tables > Create table
Local secondary indexes - No
Global secondary indexes - Yes
Encryption key management AWS owned key Yes
Deletion protection Off Yes
Resource-based policy Not active Yes
Tags
Tags are pairs of keys and optional values, that you can assign to AWS resources. You can use tags to control access to your resources or track your AWS spending.
No tags are associated with the resource.
Add new tag
You can add 50 more tags.
Cancel
Create table
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
NIFTY +0.06%
ENG
11:17
14-08-2025

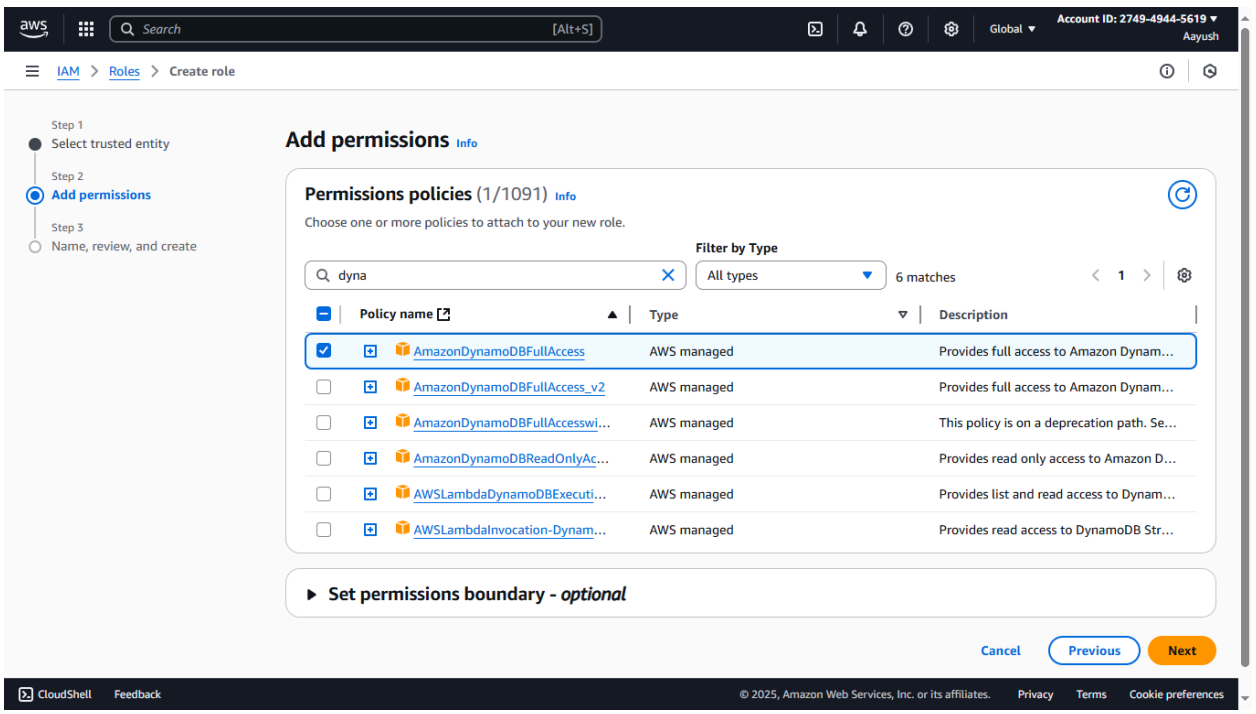

New tab
List tables | Amazon DynamoDB
https://ap-south-1.console.aws.amazon.com/dynamodbv2/home?region=ap-south-1#tables
Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 2749-4944-5619
Aayush
DynamoDB > Tables
DynamoDB
Dashboard
Tables
Explore items
PartiQL editor
Backups
Exports to S3
Imports from S3
Integrations
Reserved capacity
Settings
DAX
Clusters
Subnet groups
Parameter groups
Events
The demo_table table was created successfully.
Tables (1) Info
Actions
Delete
Create table
Find tables
Any tag key
Any tag value
Name
Status
Partition key
Sort key
Indexes
Replication Regions
Deletion protection
demo_table
Active
id (S)
-
0
0
Off
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
NIFTY +0.06%
ENG
11:17
14-08-2025

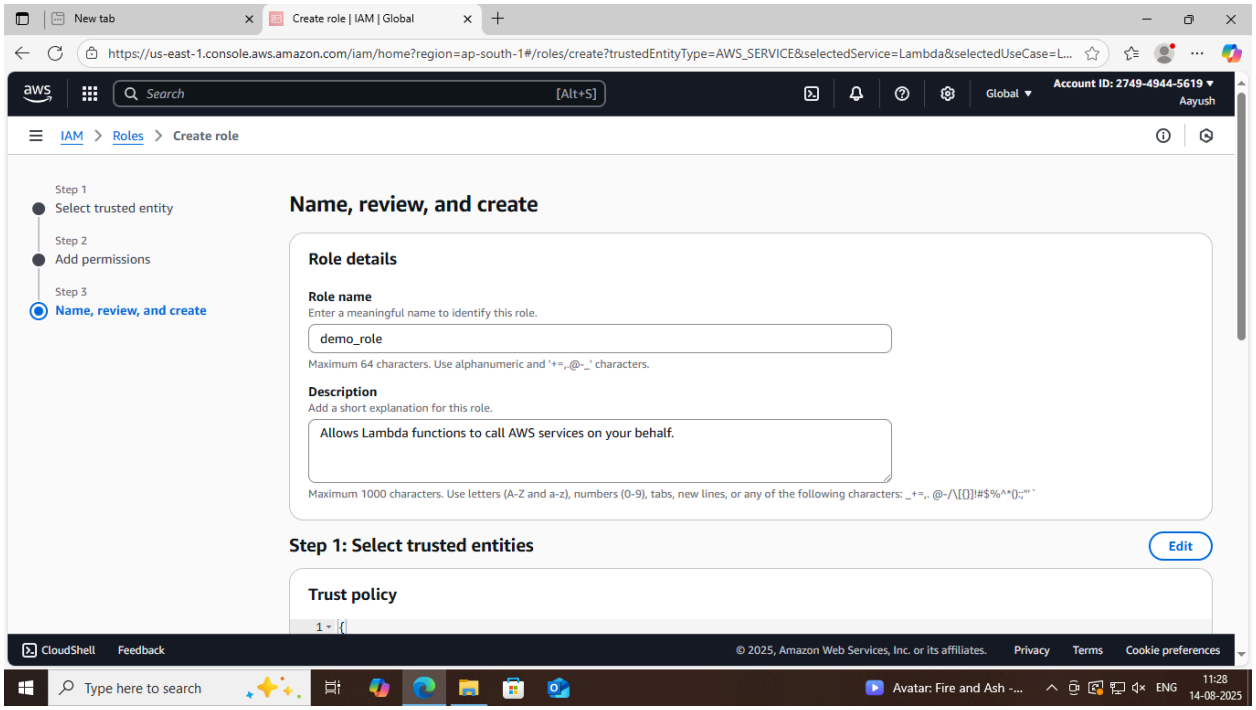

New tab
List tables | Amazon DynamoDB
https://ap-south-1.console.aws.amazon.com/dynamodbv2/home?region=ap-south-1#tables
iam
Asia Pacific (Mumbai)
Account ID: 2749-4944-5619
Aayush
Services
Features
Resources New
Documentation
Knowledge articles
Marketplace
Blog posts
Events
Tutorials
Services
Show more
IAM
Manage access to AWS resources
IAM Identity Center
Manage workforce user access to multiple AWS accounts and cloud applications
Resource Access Manager
Share AWS resources with other accounts or AWS Organizations
Features
Show more
Groups
IAM feature
Roles
IAM feature
Were these results helpful?
Yes
No
Create table
Deletion protection
Off
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
11:18
14-08-2025

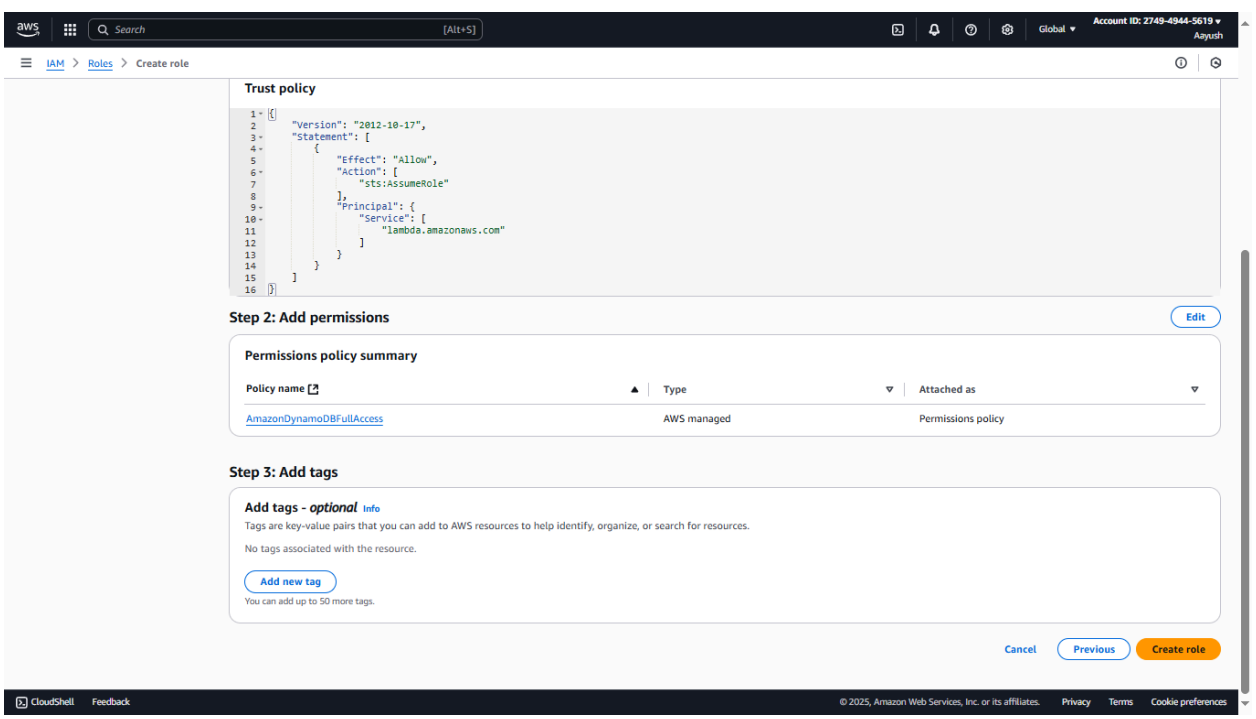

New tab
Roles | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles
Search [Alt+S]
Global
Account ID: 2749-4944-5619
Aayush
IAM > Roles
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Resource analysis New
Roles (13) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Delete
Create role
Search
Role name
Trusted entities
Last activity
aayush117 AWS Service: lambda -
aayush117new AWS Service: lambda 15 days ago
AWSServiceRoleForSupport AWS Service: support (Service-Linke -
AWSServiceRoleForTrustedAdvisor AWS Service: trustedadvisor (Service -
my_role AWS Service: lambda -
my_role1 AWS Service: lambda -
my_role69 AWS Service: lambda 13 days ago
myrole AWS Service: lambda 15 days ago
newrole AWS Service: lambda -
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
Heavier rain soon
ENG
11:19
14-08-2025

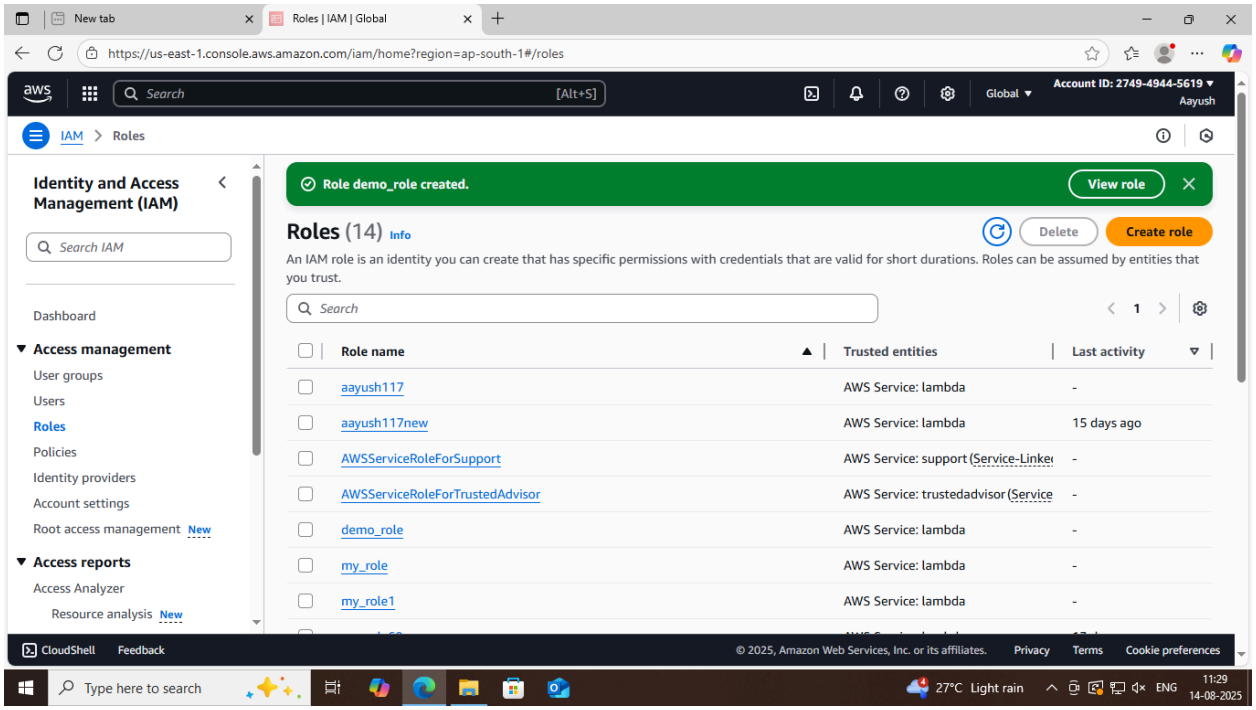

New tab
Create role | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create
Search [Alt+S]
Global
Account ID: 2749-4944-5619
Aayush
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Select trusted entity Info
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
Banks To Clear Chequ...
ENG
11:19
14-08-2025

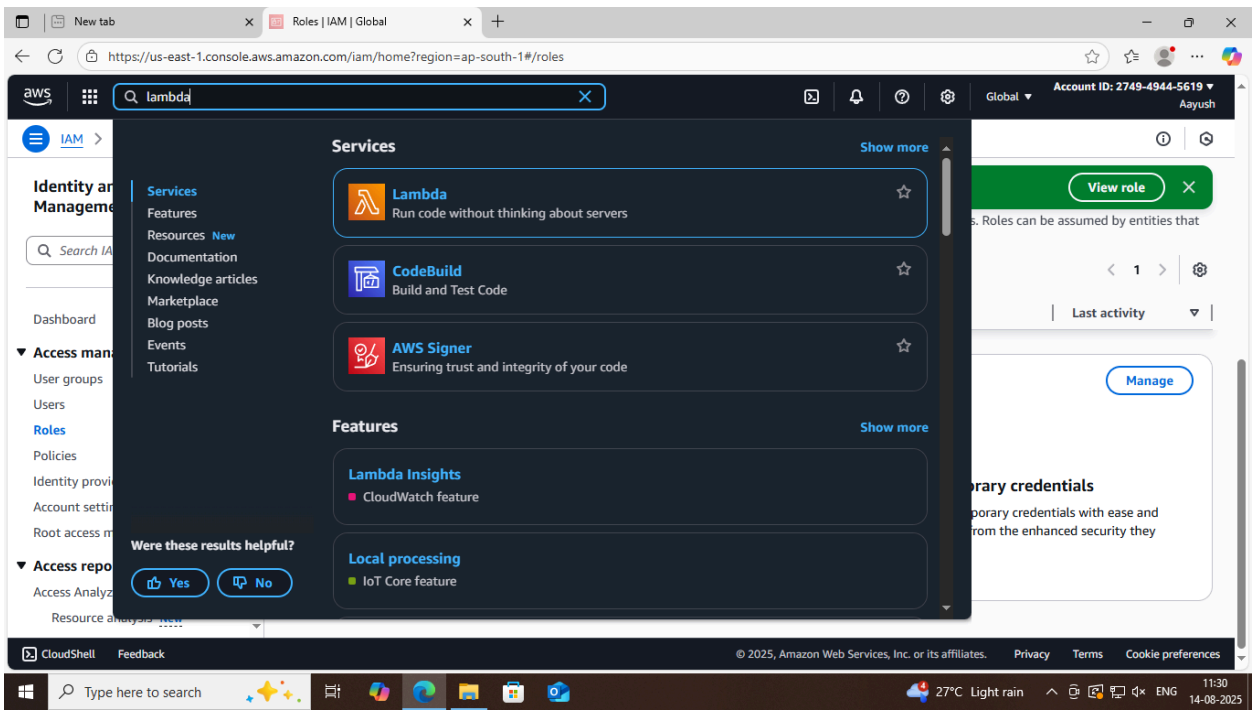

New tab
Create role | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create
Search [Alt+S]
Global
Account ID: 2749-4944-5619
Aayush
IAM > Roles > Create role
web identity provider to assume this role to perform actions in this account.
corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
Service or use case
Lambda
Choose a use case for the specified service.
Use case
Lambda
Allows Lambda functions to call AWS services on your behalf.
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ICICI Bank revises mi...
ENG
11:21
14-08-2025

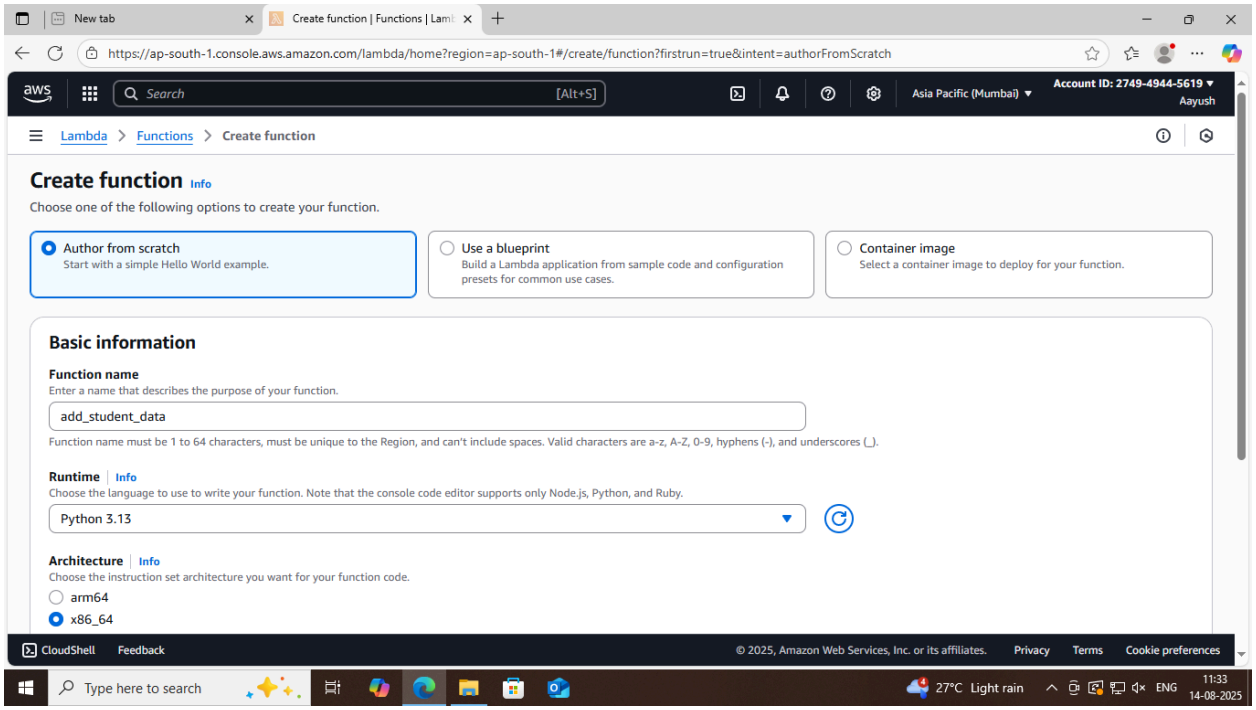

Search [Alt+S]
Global
Account ID: 2749-4944-5619
Aayush
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Add permissions Info
Permissions policies (1/1091) Info
Choose one or more policies to attach to your new role.
Filter by Type
dyna
All types
6 matches
1
Policy name
Type
Description
AmazonDynamoDBFullAccess
AWS managed
Provides full access to Amazon Dynam...
AmazonDynamoDBFullAccess_v2
AWS managed
Provides full access to Amazon Dynam...
AmazonDynamoDBFullAccesswi...
AWS managed
This policy is on a deprecation path. Se...
AmazonDynamoDBReadOnlyAc...
AWS managed
Provides read only access to Amazon D...
AWSLambdaDynamoDBExecuti...
AWS managed
Provides list and read access to Dynam...
AWSLambdaInvocation-Dynam...
AWS managed
Provides read access to DynamoDB Str...
Set permissions boundary - optional
Cancel
Previous
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

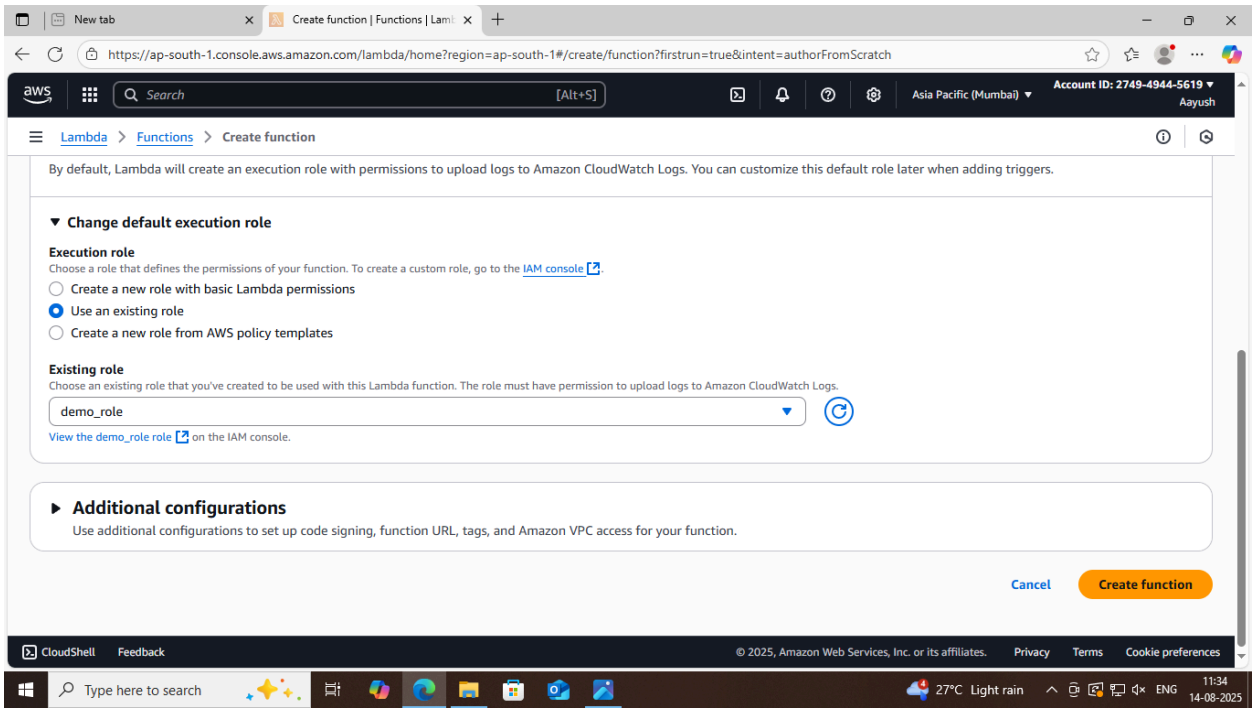

New tab
Create role | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?trustedEntityType=AWS_SERVICE&selectedService=Lambda&selectedUseCase=L...
Search [Alt+S]
Global
Account ID: 2749-4944-5619
Aayush
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
demo_role
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Allows Lambda functions to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{}]!#$%^*();:"' `
Step 1: Select trusted entities
Edit
Trust policy
1 {
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
Avatar: Fire and Ash -...
ENG
11:28
14-08-2025

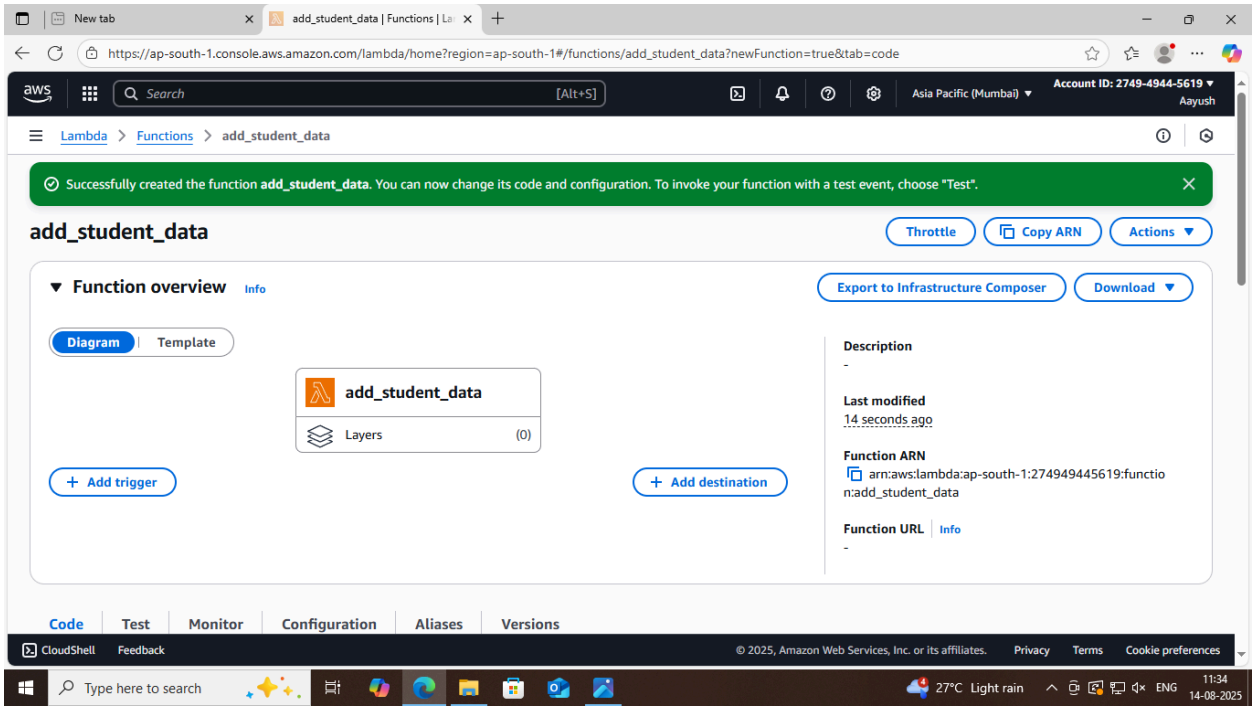

Search [Alt+S]
Global
Account ID: 2749-4944-5619
Aayush
IAM > Roles > Create role
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"sts:AssumeRole"
],
"Principal": {
"Service": [
"lambda.amazonaws.com"
]
}
}
]
}
Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
AmazonDynamoDBFullAccess
AWS managed
Permissions policy
Step 3: Add tags
Add tags - optional Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create role
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

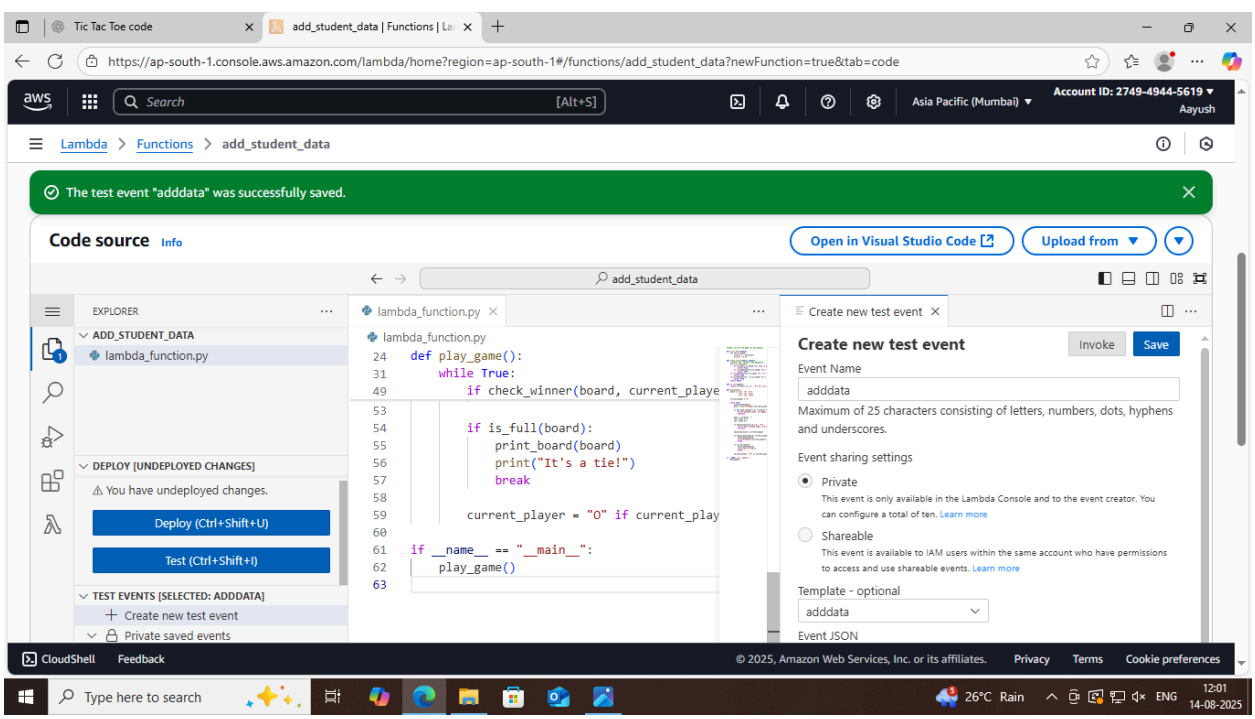

New tab
Roles | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles
Search [Alt+S]
Global
Account ID: 2749-4944-5619
Aayush
IAM > Roles
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Resource analysis New
Role demo_role created.
View role
Roles (14) Info
Delete
Create role
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Search
Role name
Trusted entities
Last activity
aayush117 AWS Service: lambda -
aayush117new AWS Service: lambda 15 days ago
AWSServiceRoleForSupport AWS Service: support (Service-Linke -
AWSServiceRoleForTrustedAdvisor AWS Service: trustedadvisor (Service -
demo_role AWS Service: lambda -
my_role AWS Service: lambda -
my_role1 AWS Service: lambda -
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
27°C Light rain
ENG
11:29
14-08-2025

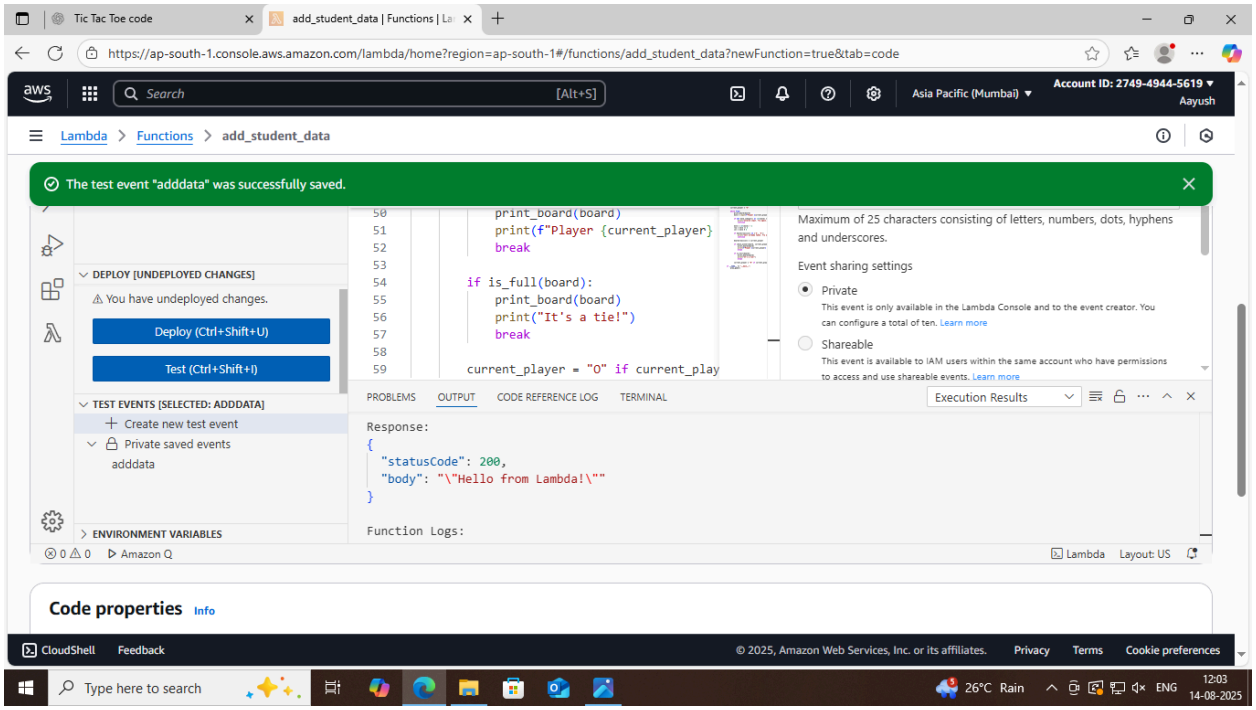

New tab
Roles | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles
lambda
Global
Account ID: 2749-4944-5619
Aayush
Services
Features
Resources New
Documentation
Knowledge articles
Marketplace
Blog posts
Events
Tutorials
Services
Show more
Lambda
Run code without thinking about servers
CodeBuild
Build and Test Code
AWS Signer
Ensuring trust and integrity of your code
Features
Show more
Lambda Insights
CloudWatch feature
Local processing
IoT Core feature
Were these results helpful?
Yes
No
View role
Manage
Last activity
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
27°C Light rain
ENG
11:30
14-08-2025

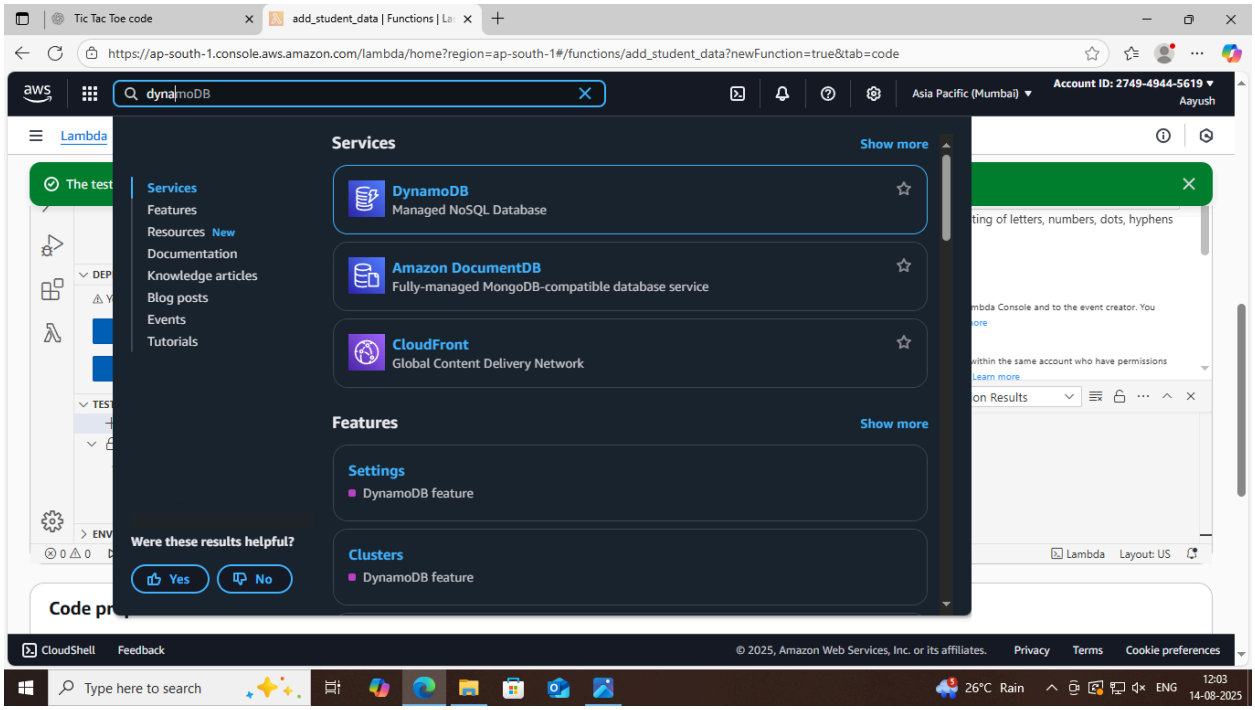

New tab
Create function | Functions | Lam
https://ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/create/function?firstrun=true&intent=authorFromScratch
Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 2749-4944-5619
Aayush
Lambda > Functions > Create function
Create function Info
Choose one of the following options to create your function.
Author from scratch
Start with a simple Hello World example.
Use a blueprint
Build a Lambda application from sample code and configuration presets for common use cases.
Container image
Select a container image to deploy for your function.
Basic information
Function name
Enter a name that describes the purpose of your function.
add_student_data
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.
Python 3.13
Architecture Info
Choose the instruction set architecture you want for your function code.
arm64
x86_64
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
27°C Light rain
ENG
11:33
14-08-2025

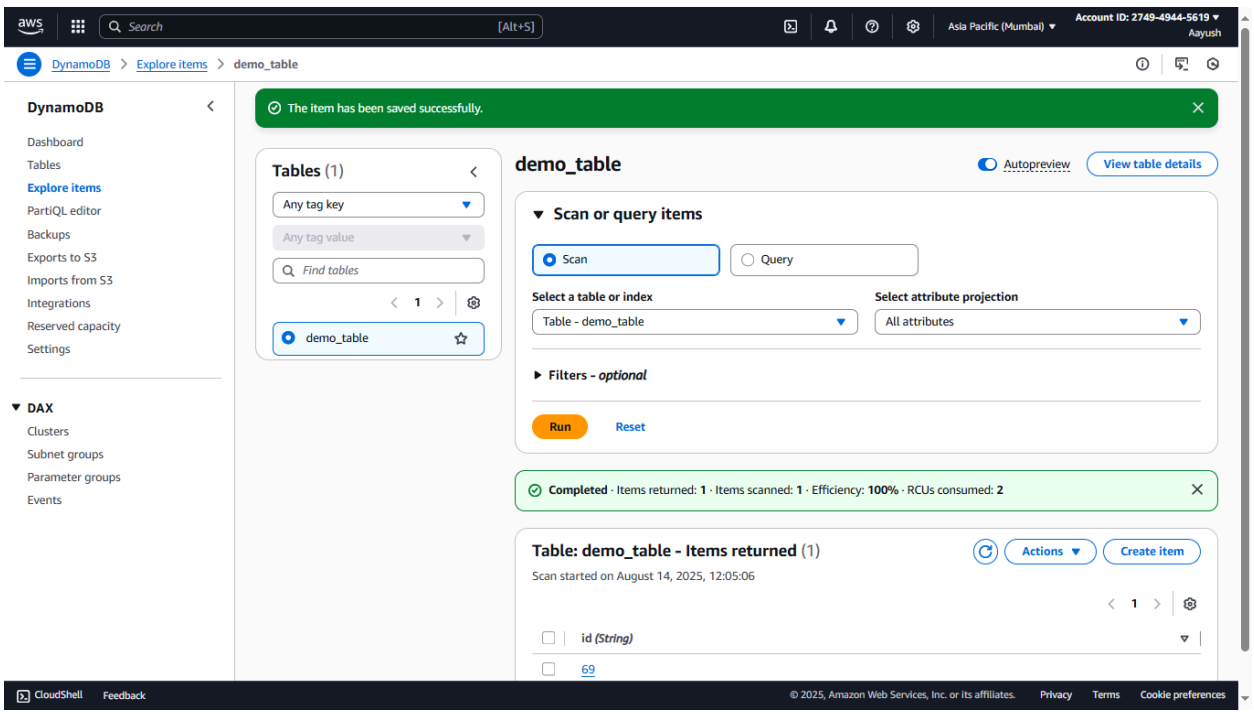

New tab
Create function | Functions | Lam
https://ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/create/function?firstrun=true&intent=authorFromScratch
Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 2749-4944-5619
Aayush
Lambda > Functions > Create function
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.
Change default execution role
Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console.
Create a new role with basic Lambda permissions
Use an existing role
Create a new role from AWS policy templates
Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.
demo_role
View the demo_role role on the IAM console.
Additional configurations
Use additional configurations to set up code signing, function URL, tags, and Amazon VPC access for your function.
Cancel
Create function
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
27°C Light rain
ENG
11:34
14-08-2025


New tab
add_student_data | Functions | La
https://ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/functions/add_student_data?newFunction=true&tab=code
Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 2749-4944-5619
Aayush
Lambda > Functions > add_student_data
Successfully created the function add_student_data. You can now change its code and configuration. To invoke your function with a test event, choose "Test".
add_student_data
Throttle
Copy ARN
Actions
Function overview Info
Export to Infrastructure Composer
Download
Diagram
Template
add_student_data
Layers (0)
+ Add trigger
+ Add destination
Description
-
Last modified
14 seconds ago
Function ARN
arn:aws:lambda:ap-south-1:274949445619:function:add_student_data
Function URL Info
-
Code
Test
Monitor
Configuration
Aliases
Versions
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
27°C Light rain
ENG
11:34
14-08-2025


Tic Tac Toe code
add_student_data | Functions | La
https://ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/functions/add_student_data?newFunction=true&tab=code
Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 2749-4944-5619
Aayush
Lambda > Functions > add_student_data
The test event "adddata" was successfully saved.
Code source Info
Open in Visual Studio Code
Upload from
EXPLORER
ADD_STUDENT_DATA
lambda_function.py
DEPLOY [UNDEPLOYED CHANGES]
You have undeployed changes.
Deploy (Ctrl+Shift+U)
Test (Ctrl+Shift+I)
TEST EVENTS [SELECTED: ADDDATA]
Create new test event
Private saved events
lambda_function.py
def play_game():
while True:
if check_winner(board, current_player
if is_full(board):
print_board(board)
print("It's a tie!")
break
current_player = "O" if current_play
if __name__ == "__main__":
play_game()
Create new test event
Invoke
Save
Event Name
adddata
Maximum of 25 characters consisting of letters, numbers, dots, hyphens and underscores.
Event sharing settings
Private
This event is only available in the Lambda Console and to the event creator. You can configure a total of ten. Learn more
Shareable
This event is available to IAM users within the same account who have permissions to access and use shareable events. Learn more
Template - optional
adddata
Event JSON
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Rain
ENG
12:01
14-08-2025


Tic Tac Toe code
add_student_data | Functions | La
https://ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/functions/add_student_data?newFunction=true&tab=code
Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 2749-4944-5619
Aayush
Lambda
Functions
add_student_data
The test event "adddata" was successfully saved.
DEPLOY [UNDEPLOYED CHANGES]
You have undeployed changes.
Deploy (Ctrl+Shift+U)
Test (Ctrl+Shift+I)
TEST EVENTS [SELECTED: ADDDATA]
Create new test event
Private saved events
adddata
ENVIRONMENT VARIABLES
print_board(board)
print(f"Player {current_player}
break
if is_full(board):
print_board(board)
print("It's a tie!")
break
current_player = "O" if current_play
Maximum of 25 characters consisting of letters, numbers, dots, hyphens and underscores.
Event sharing settings
Private
This event is only available in the Lambda Console and to the event creator. You can configure a total of ten. Learn more
Shareable
This event is available to IAM users within the same account who have permissions to access and use shareable events. Learn more
PROBLEMS
OUTPUT
CODE REFERENCE LOG
TERMINAL
Execution Results
Response:
{
"statusCode": 200,
"body": "\"Hello from Lambda!\""
}
Function Logs:
Amazon Q
Lambda
Layout: US
Code properties
Info
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Rain
ENG
12:03
14-08-2025


Tic Tac Toe code
add_student_data | Functions | La
https://ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/functions/add_student_data?newFunction=true&tab=code
dynamoDB
Asia Pacific (Mumbai)
Account ID: 2749-4944-5619
Aayush
Lambda
Services
Show more
Services
Features
Resources New
Documentation
Knowledge articles
Blog posts
Events
Tutorials
DynamoDB
Managed NoSQL Database
Amazon DocumentDB
Fully-managed MongoDB-compatible database service
CloudFront
Global Content Delivery Network
Features
Show more
Settings
DynamoDB feature
Clusters
DynamoDB feature
Were these results helpful?
Yes
No
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Rain
ENG
12:03
14-08-2025


Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 2749-4944-5619
Aayush
DynamoDB
Explore items
demo_table
DynamoDB
Dashboard
Tables
Explore items
PartiQL editor
Backups
Exports to S3
Imports from S3
Integrations
Reserved capacity
Settings
DAX
Clusters
Subnet groups
Parameter groups
Events
The item has been saved successfully.
Tables (1)
Any tag key
Any tag value
Find tables
demo_table
demo_table
Autopreview
View table details
Scan or query items
Scan
Query
Select a table or index
Table - demo_table
Select attribute projection
All attributes
Filters - optional
Run
Reset
Completed · Items returned: 1 · Items scanned: 1 · Efficiency: 100% · RCUs consumed: 2
Table: demo_table - Items returned (1)
Scan started on August 14, 2025, 12:05:06
Actions
Create item
id (String)
69
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Conclusion- In conclusion, using a Python lambda function to add data to DynamoDB provides a simple, efficient, and scalable way to manage database operations within a serverless architecture. It leverages AWS's managed services to minimize infrastructure overhead while ensuring seamless integration and real-time data handling, making it an ideal solution for modern cloud-based applications.

LO Mapping- LO6

Written assignment-1

Q1) What are the key features and advantages of AWS Cloud 9 ? LO1

AWS Cloud9 – Key Features and Advantages

1. Cloud-Based IDE

AWS Cloud9 is a browser-accessible development environment that eliminates the need for local setup. It includes a code editor, terminal, and debugger—all integrated into one interface. Developers can start coding instantly without installing tools or configuring environments.

2. Real-Time Collaboration

Multiple users can work on the same codebase simultaneously. Cloud9 supports shared environments where teammates can see each other's cursors, chat live, and co-edit files. This is especially useful for remote teams, pair programming, and mentoring.

3. Built-In Terminal with AWS CLI

The IDE includes a Linux-based terminal with pre-installed AWS CLI. Developers can run shell commands, manage AWS services, and deploy applications directly from the IDE—without switching to another tool or terminal.

4. Preconfigured Development Environments

Cloud9 supports multiple programming languages like JavaScript, Python, PHP, Ruby, Go, and C++. It comes with essential tools like Git, Docker, and Node.js pre-installed. This reduces setup time and ensures consistency across teams.

5. Deep Integration with AWS Services

Cloud9 is tightly integrated with AWS. Developers can create and manage EC2 instances, Lambda functions, S3 buckets, and DynamoDB tables directly from the IDE. It's ideal for building serverless applications and cloud-native solutions.

6. Secure Access via IAM

Access to Cloud9 environments is controlled using AWS Identity and Access Management (IAM). This ensures secure, role-based access without exposing credentials. Developers can work safely within defined permission boundaries.

7. Environment Portability and Management

Cloud9 environments can be EC2-backed or connected via SSH to existing servers. Developers can clone, pause, or terminate environments as needed. This flexibility supports both cloud-based and hybrid workflows.

Advantages of AWS Cloud9

- **No local setup**: Code from any device with a browser.
- **Scalable**: Use AWS compute resources for heavy workloads.
- **Secure**: IAM-based access control and no credential leakage.
- **Collaborative**: Real-time editing and communication.
- **Integrated**: AWS CLI, Git, and language runtimes built-in.
- **Efficient**: Reduces context switching and setup overhead.

Q2) What is the difference between Cloud 9 and Lambda ? LO1,LO6

The difference between cloud9 and Lambda is given:

Feature	**AWS Cloud9**	**AWS Lambda**
Type	Cloud-based Integrated Development Environment (IDE)	Serverless compute service
Purpose	Write, edit, and debug code in the cloud	Run code in response to events without managing servers
Usage	Development and collaboration	Execution of backend logic, automation, APIs, etc.
Environment	Full Linux-based dev environment with terminal access	Stateless function container managed by AWS
Language Support	Multiple: JavaScript, Python, PHP, Go, etc.	Multiple: Node.js, Python, Java, Go, .NET, Ruby
Execution Model	Manual execution via terminal or editor	Event-driven execution (e.g., API call, file upload)
Persistence	Persistent workspace and file system	Ephemeral—no persistent storage between executions
Scalability	Not auto-scaled; depends on EC2 instance	Automatically scales with incoming requests

Feature	AWS Cloud9	AWS Lambda
Pricing	Based on EC2 usage and storage	Pay-per-use (requests and compute time)
Ideal For	Coding, debugging, team collaboration	Microservices, automation, backend APIs

Q3) What are the three components of AWS Lambda ? LO1,LO6

AWS Lambda is characterized by being serverless, provisioningless, and function-based. Its main use is located in the computing layer of an application which does not have a server, in addition to its main purpose is to create applications based on events and that have the possibility of being activated by various AWS events.

If the situation of having multiple concurrent events arises, AWS lambda will trigger multiple copies of the function, making Lambda a Function of Service (FaaS) type.

In AWS Lambda, the Function is the core component where the actual code resides. This code is written to perform a specific task, such as processing an image, handling an API request, or responding to a database update. The function is stateless and designed to execute quickly and efficiently. Developers write this code in supported languages like Python, Node.js, Java, or Go, and it is uploaded to AWS either directly or via deployment tools. The function is the executable logic that AWS invokes when triggered by an event.

The Configuration component defines how the function should behave during execution. It includes settings such as memory allocation, timeout duration, environment variables, IAM roles for permissions, and concurrency limits. These parameters allow developers to fine-tune performance, security, and resource usage. For example, increasing memory can improve execution speed, while setting a timeout ensures that long-running functions are terminated appropriately. Configuration also determines how the function integrates with other AWS services and manages its runtime environment.

The Event Source is the trigger mechanism that initiates the function's execution. It can be any AWS service capable of generating events, such as S3 (file uploads), DynamoDB (table updates), API Gateway (HTTP requests), or CloudWatch (scheduled tasks). Third-party services or custom applications can also act as event sources via AWS SDKs or messaging systems. While event sources are optional, they are essential for building reactive, event-driven architectures. When configured, AWS automatically invokes the function whenever the specified event occurs, enabling seamless automation and integration across cloud services.

Q4) Discuss the difference between Kubernetes and other container orchestration tools like Docker Swarm? LO1,LO2

Architecture & Complexity

- Kubernetes has a more complex architecture with components like etcd, kube-apiserver, kube-scheduler, and kube-controller-manager. It offers fine-grained control over deployments, networking, and storage.
- Docker Swarm is simpler and tightly integrated with Docker. It uses a manager-worker model and is easier to set up for small-scale applications.

Scalability & Performance

- Kubernetes is designed for large-scale, production-grade workloads. It supports auto-scaling, rolling updates, and self-healing mechanisms.
- Docker Swarm is suitable for smaller clusters and simpler use cases. It lacks advanced scaling and recovery features found in Kubernetes.

Load Balancing & Networking

- Kubernetes uses a robust networking model with built-in service discovery, DNS-based load balancing, and support for ingress controllers.
- Docker Swarm provides basic internal load balancing and service discovery but lacks advanced ingress and traffic routing capabilities.

Configuration & Management

- Kubernetes uses YAML manifests for declarative configuration, offering extensive customization and automation.
- Docker Swarm uses Docker Compose files with limited orchestration features and less flexibility in defining complex deployments.

Security & Role Management

- Kubernetes supports Role-Based Access Control (RBAC), secrets management, and network policies.
- Docker Swarm has basic security features like mutual TLS between nodes but lacks granular access control.

Ecosystem & Community

- Kubernetes has a vast ecosystem with tools like Helm, Istio, Prometheus, and ArgoCD. It's backed by the Cloud Native Computing Foundation (CNCF) and widely adopted across industries.

- Docker Swarm has a smaller community and fewer integrations. Docker Inc. has shifted focus toward Kubernetes support.

Written Assignment-2

Q1) What are the key Terraform commands, explain ? LO1,LO3

The key terraform commands are as shown :

- **terraform init**

This command initializes a Terraform working directory. It sets up the backend configuration, downloads required provider plugins, and prepares the environment for further Terraform operations. You should run terraform init once when starting a new project or after modifying the provider configuration in your .tf files.

- **terraform plan**

This command shows you what Terraform will do before it actually makes any changes. It compares your current infrastructure state with the desired state defined in your configuration files and outputs a detailed execution plan. This helps you verify and review changes before applying them, making it a safe step in any deployment workflow.

- **terraform apply**

This command executes the actions proposed in the plan and creates or updates infrastructure accordingly. It prompts for confirmation before proceeding unless you use the -auto-approve flag. After running terraform apply, your infrastructure will match the configuration defined in your .tf files.

- **terraform destroy**

This command removes all infrastructure managed by your Terraform configuration. It's used when you want to tear down your environment completely. Like apply, it shows a plan and asks for confirmation before executing unless you use -auto-approve.

- **terraform validate**

This command checks whether your Terraform configuration files are syntactically valid. It does not access remote services or check the correctness of resource arguments, but it ensures that your .tf files are properly structured and free of syntax errors.

- **terraform fmt**

This command formats your Terraform configuration files to follow the standard style conventions. It helps maintain clean, readable code and is especially useful when working in teams or reviewing code in version control.

- **terraform state**

This command lets you inspect and manage the Terraform state file, which tracks the current state of your infrastructure. You can use subcommands like terraform state list to view resources or terraform state rm to remove specific items from state tracking.

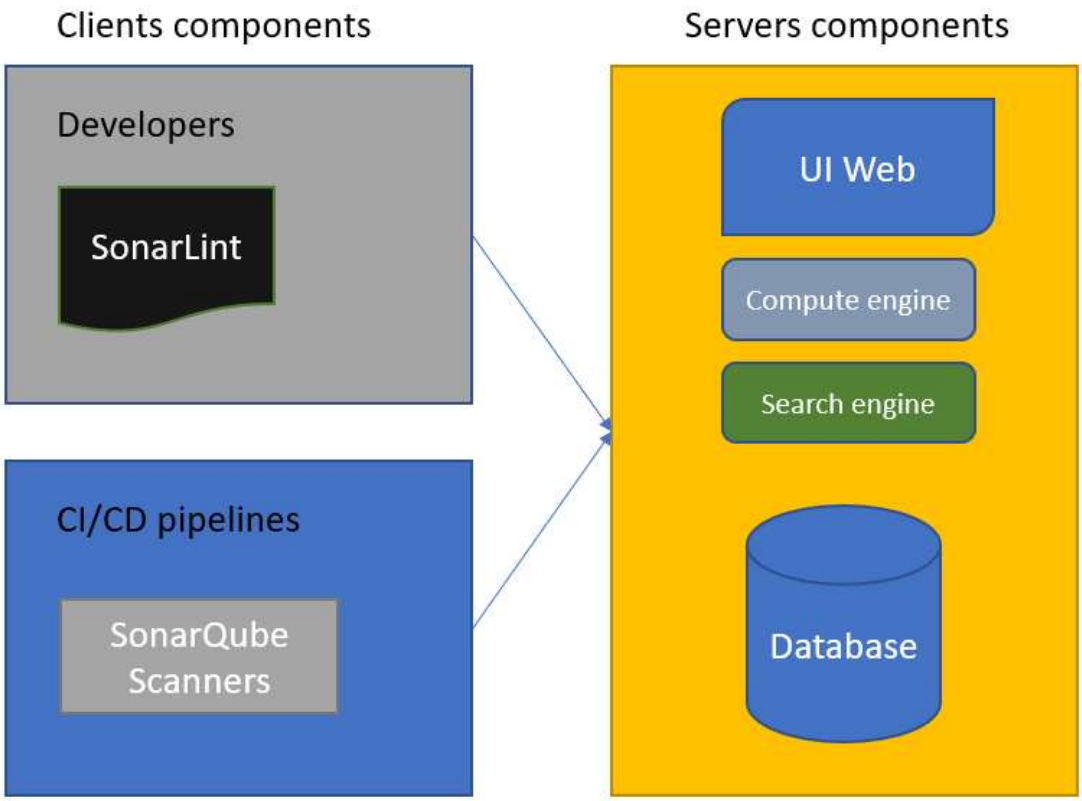
- **terraform output**

This command displays the output values defined in your configuration after running terraform apply. These outputs can include IP addresses, resource IDs, or any other values you've marked as outputs in your .tf files. It's useful for retrieving dynamic values that other tools or scripts might need.

Q2) Explain the key components of Sonarqube's architecture? LO1,LO4

SonarQube is a client-server tool, which means that its architecture is composed of artifacts on the server side and also on the client side.

A simplified SonarQube architecture is shown in the following diagram:



Client components are primarily involved in the development and automated testing/deployment processes:

1. **Developers:** This area focuses on individual developer workstations or environments.
    - **SonarLint:** This is an IDE (Integrated Development Environment) extension used by developers to provide real-time feedback on code quality and security issues while they write code. It acts as a local, "shift-left" tool for static analysis.
2. **CI/CD pipelines:** This represents the continuous integration and continuous delivery/deployment automation infrastructure.
    - **SonarQube Scanners:** These are tools integrated into the CI/CD pipeline (e.g., Jenkins, GitHub Actions, GitLab CI) that perform static analysis on the entire codebase as part of the build process. They typically send their findings to a central SonarQube Server component for detailed reporting and quality gating.

Server components represent the core application or platform that processes requests and manages data:

- The entire server-side application is contained within the large yellow box.
- **UI Web:** This is the user interface, likely a web application, that users interact with.
- **Compute engine:** This component handles the business logic, processing, and computational tasks of the application.
- **Search engine:** This component is dedicated to indexing data and executing fast, complex search queries, often used by the UI Web or Compute engine.
- **Database:** This is the persistent storage layer for the application's data.

The client components (specifically the code/artifacts produced by Developers and analyzed by CI/CD pipelines) interact with and feed into the server environment, resulting in a process where developed and validated code is deployed to run the server component

Q3) What are the 3 full deployment modes that can be used for AWS? LO1,LO3

The three full deployment modes commonly used in AWS environments, each suited to different stages of development and operational needs are:

- **Development Mode**

Development mode is used for building and testing applications in a non-production environment. Resources are typically provisioned with minimal cost and scale, allowing developers to iterate quickly. This mode often includes mock data, debugging tools, and relaxed security settings to facilitate experimentation and rapid prototyping.

- **Staging Mode**

Staging mode replicates the production environment as closely as possible but is isolated from live users. It is used for final testing, performance validation, and quality assurance before deployment. This mode helps identify issues that may not surface during development and ensures that the application behaves as expected under realistic conditions.

- **Production Mode**

Production mode is the live environment where real users interact with the application. Resources are provisioned for high availability, scalability, and security. Monitoring, logging, and backup systems are typically enabled, and infrastructure is optimized for performance and reliability. This mode represents the final and most critical stage of deployment.

Q4) What are the benefits of NAGIOS in AdvDevOps ? LO1,LO5

They key benefits of using of using Nagios are:

- **Real-time Monitoring**: Nagios provides continuous monitoring of servers, applications, services, and network devices, helping teams detect issues before they impact users.
- **Alerting and Notifications**: It sends alerts via email, SMS, or custom scripts when thresholds are breached or failures occur, enabling rapid incident response.
- **Scalability**: Nagios can monitor thousands of hosts and services using plugins and distributed architectures, making it suitable for large-scale DevOps environments.
- **Extensibility via Plugins**: With a rich ecosystem of community and custom plugins, Nagios can be tailored to monitor virtually any system metric or application.
- **Performance Graphing**: Integration with tools like PNP4Nagios or Grafana allows visualization of performance data over time, aiding in capacity planning and optimization.
- **Infrastructure Visibility**: Nagios offers a centralized dashboard that gives DevOps teams a clear view of system health, dependencies, and service status.
- **Automation Integration**: It can trigger automated remediation scripts or workflows when specific conditions are met, aligning with DevOps principles of self-healing systems.
- **Audit and Reporting**: Nagios logs all events and alerts, supporting compliance, post-mortem analysis, and continuous improvement.
- **Multi-platform Support**: It supports monitoring across Linux, Windows, Unix, and cloud platforms, making it versatile for hybrid infrastructure setups.
- **Community and Enterprise Editions**: Nagios Core is open-source and widely adopted, while Nagios XI offers enterprise-grade features for advanced DevOps teams.