K.R. MANGALAM UNIVERSITY

THE COMPLETE WORLD OF EDUCATION

11/28/2025

Fundamentals Of Cloud Computing & its Security lab

Practical File ENCS-353

B. Tech CSE Cyber Security

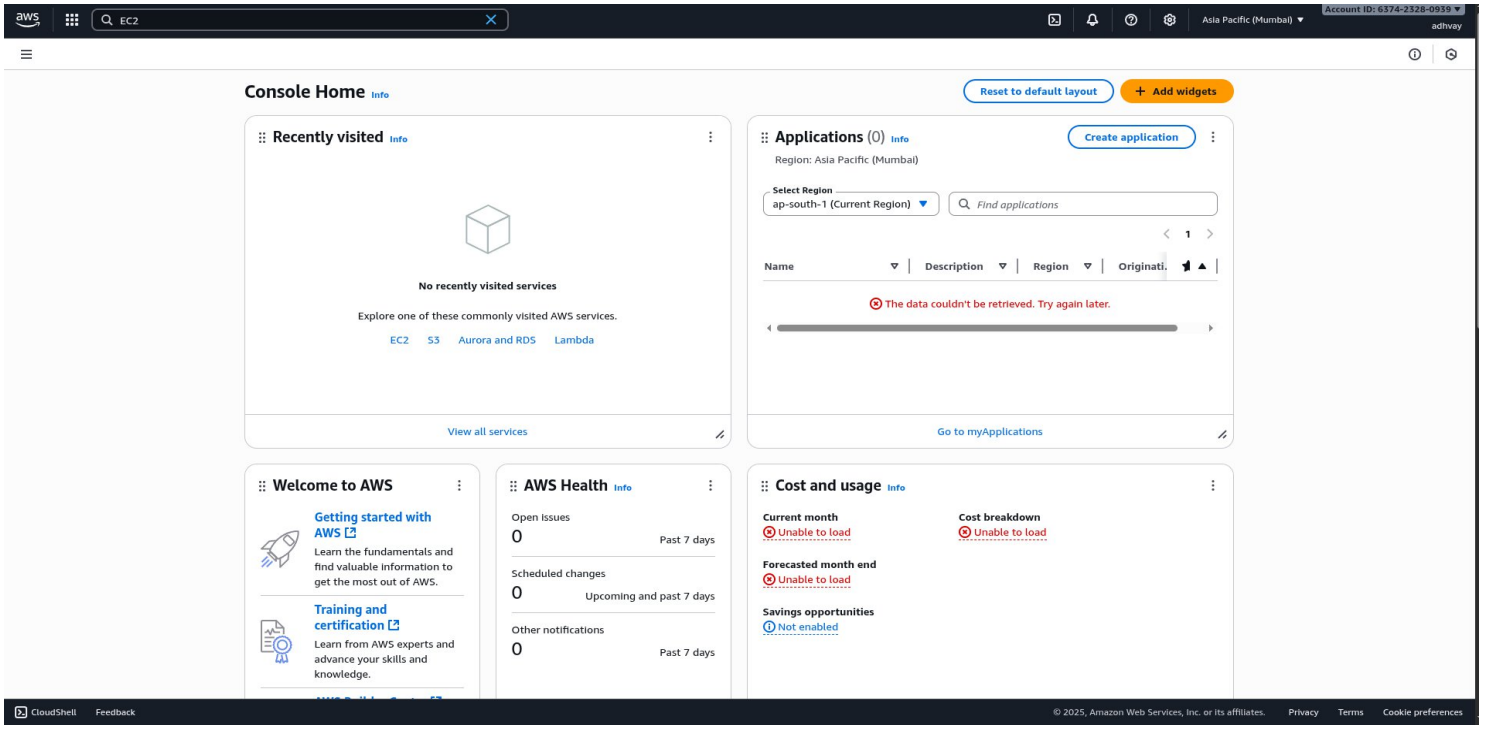
Adhvay Banerjee 2301410002

K.R. MANGALAM UNIVERSITY

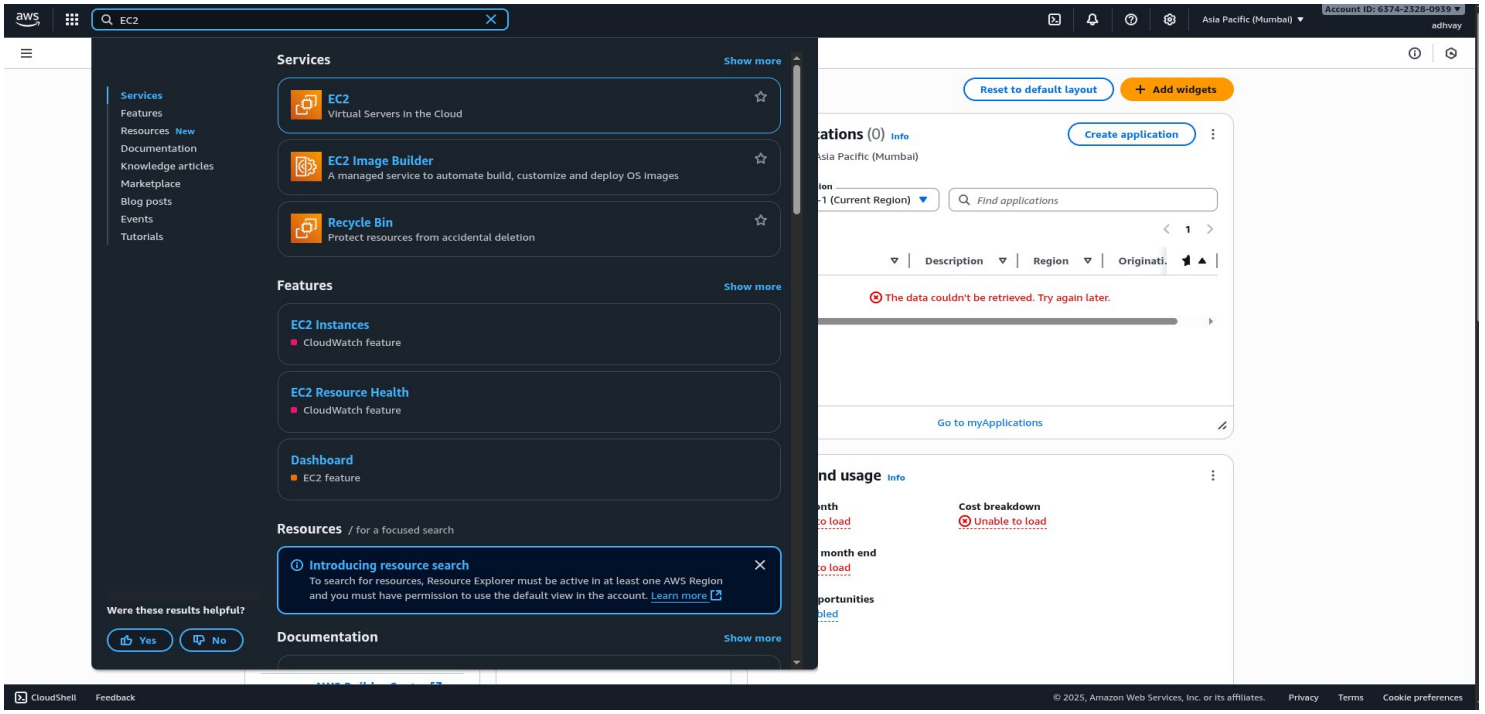
Index

Practical 1: To launch an EC2 instance in AWS

Step -1 Navigate to the EC2 Dashboard



Once signed in, use the search bar at the top to find and select EC2. This will take you to the EC2 dashboard, where you can manage your virtual servers.

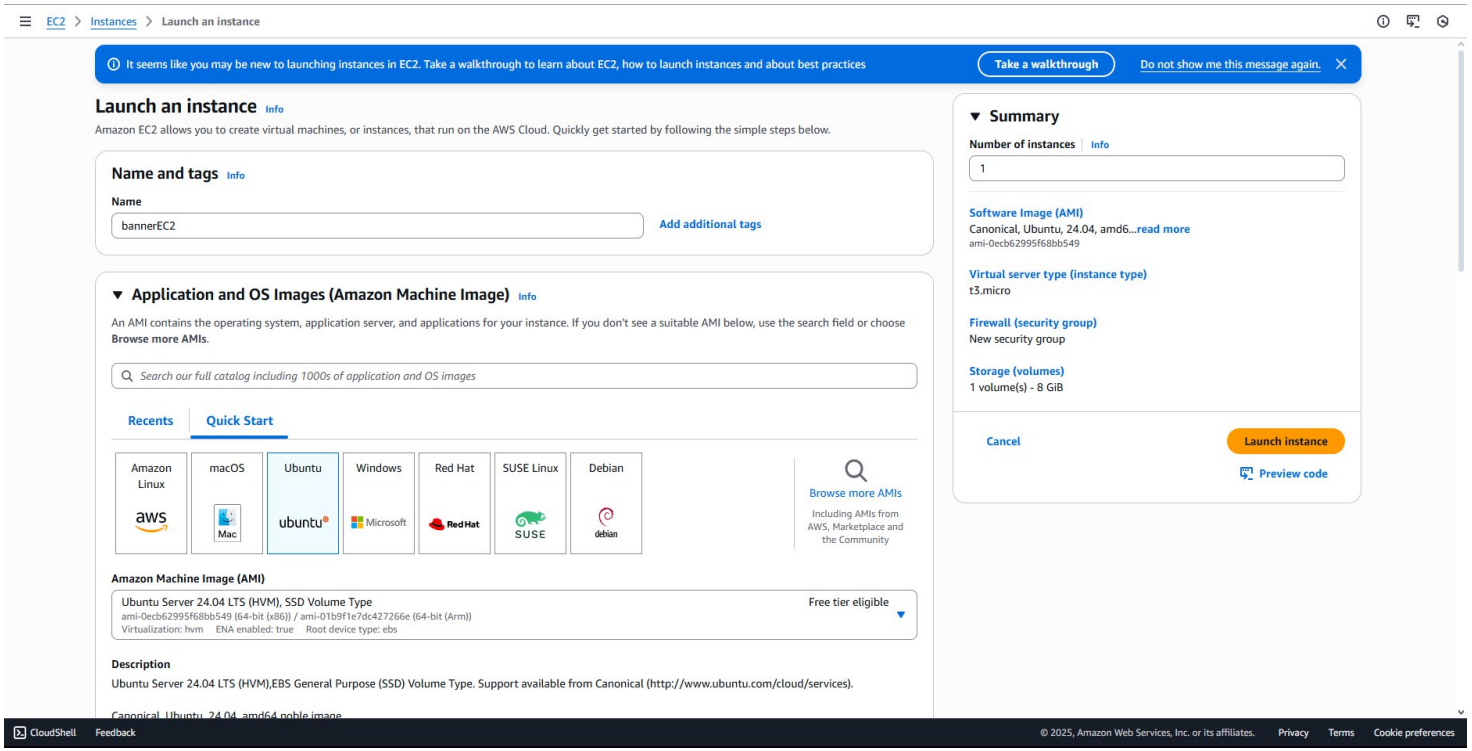


Step -2 Launch an Instance

On the EC2 dashboard, click the **"Launch instance"** button. This will start the wizard for creating a new EC2 instance.

Step -3 Choose an Amazon Machine Image (AMI)

Select an AMI, which is a template for your instance's operating system and software. For a basic setup, I choose a free tier eligible AMI like Amazon Linux 2023 AMI or Ubuntu Server 22.04 LTS.



Step -4 Choose an Instance Type

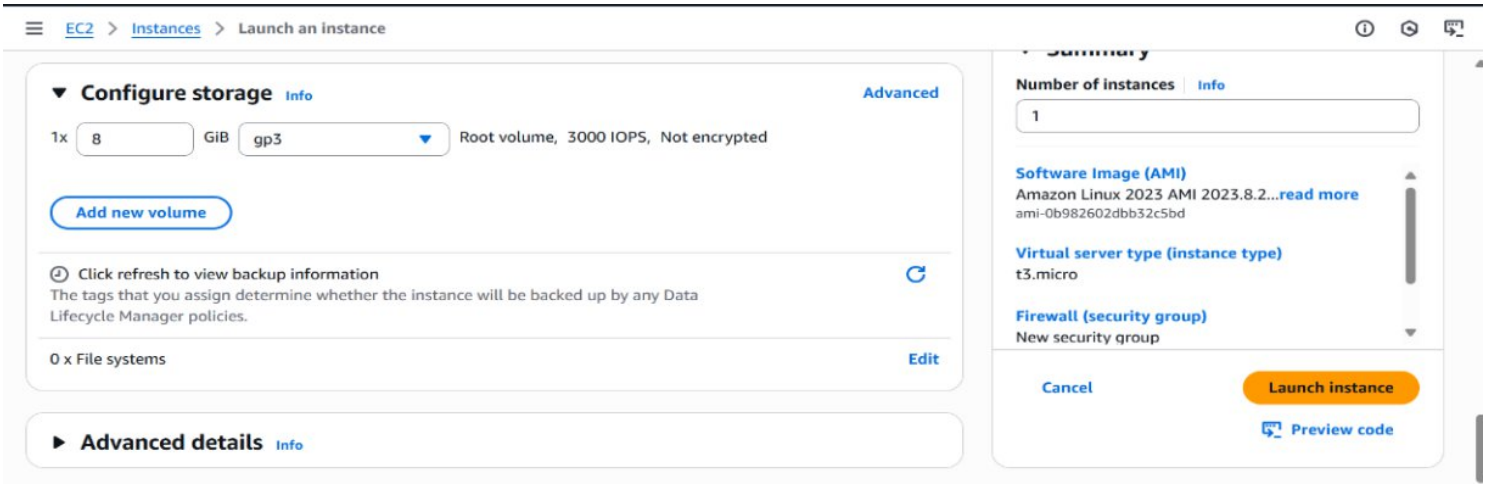
An instance type determines the CPU, memory, storage, and networking capacity of your instance. For most basic use cases, the t2.micro or t3.micro instance types are a great choice as they are free tier eligible.

Step-5 Configure Instance Details

On this page, you can configure network settings, assign an IAM role, and more. For a simple setup, you can often leave most of the settings at their defaults.

Step-6 Add Storage

Here you can specify the size and type of the root volume (the main disk) for your instance. The default is usually sufficient, but you can increase it if you need more space. Free tier includes up to 30 GB of EBS General Purpose SSD (gp2) or Magnetic storage.



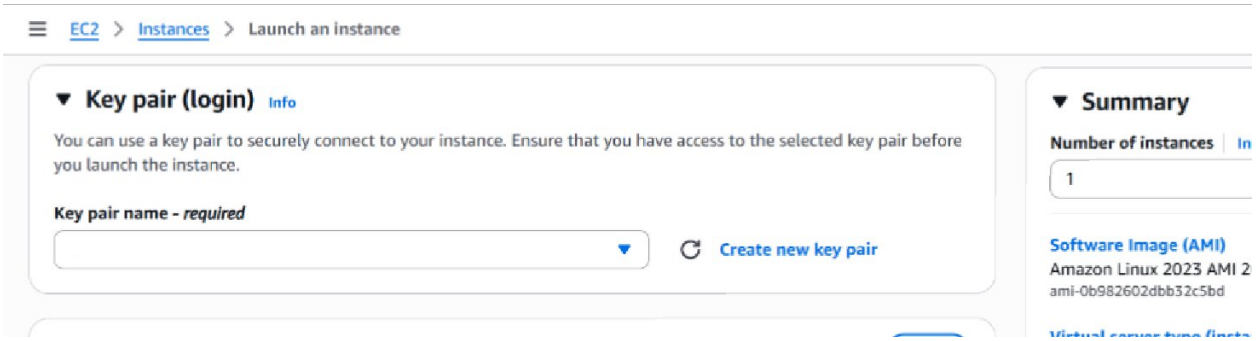
Step-7 Configure Security Group

A security group acts as a virtual firewall for your instance, controlling inbound and outbound traffic. You can create a new security group or use an existing one. For a basic web server, you'll need to allow inbound traffic on port 80 (HTTP) and port 22 (SSH) to connect to the instance.

Step-8 Review and Launch

Review all the settings you've chosen. If everything looks correct, click the "Launch" button

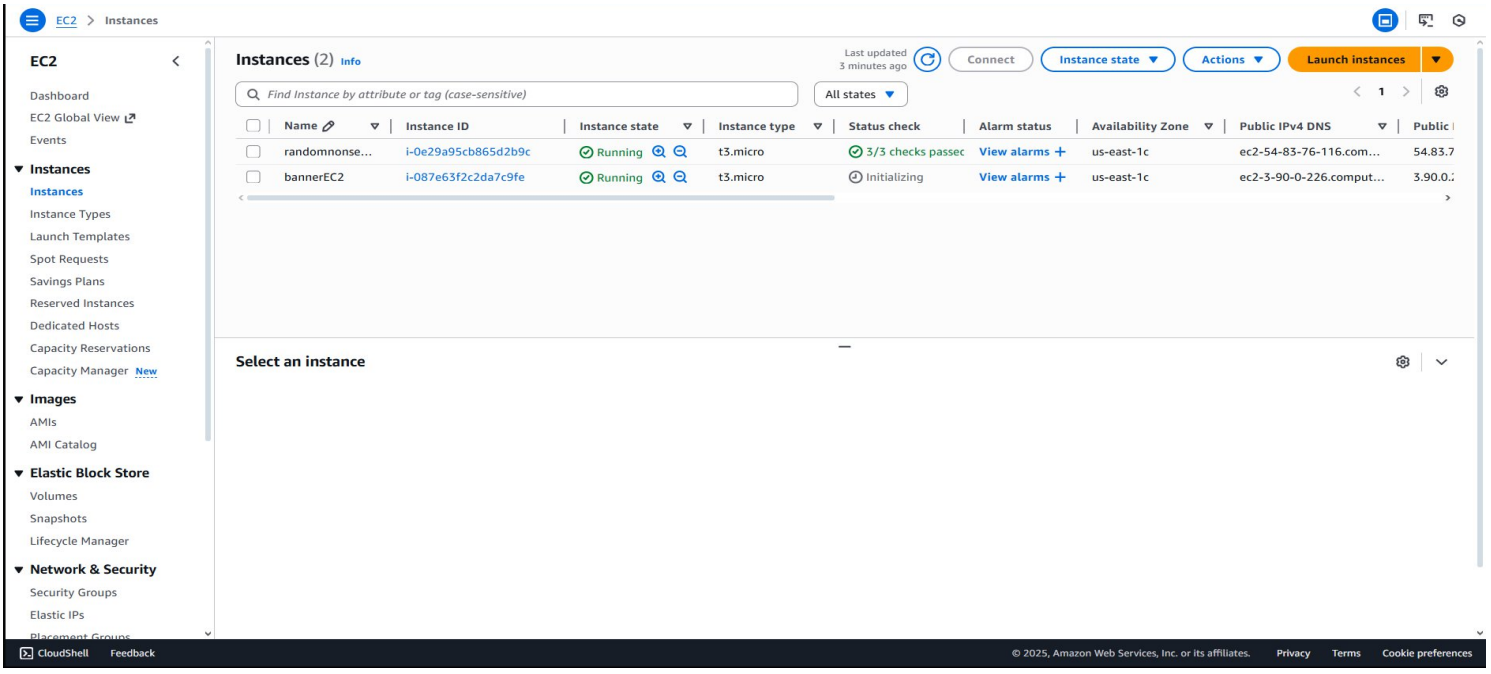
Step-9 Create or Select a Key Pair

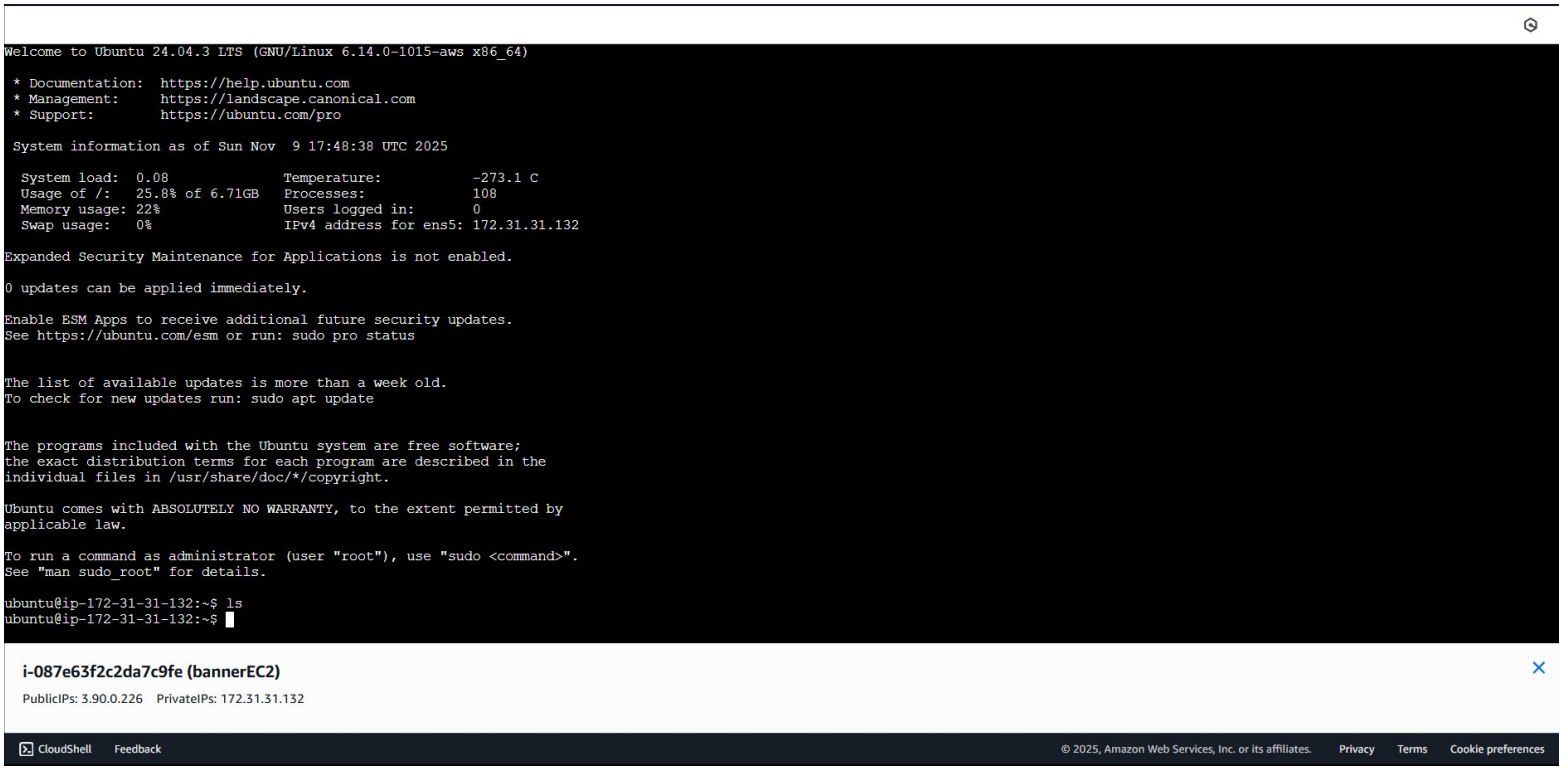


This is a crucial step. A **key pair** is used to securely connect to your instance via SSH. You must either **create a new key pair** or select an existing one. If you create a new one, you'll be prompted to download the **private key file (.pem)**. **Store this file securely**, as you will need it to connect to your instance and it cannot be re-downloaded later.

Step-10 Launch the Instance

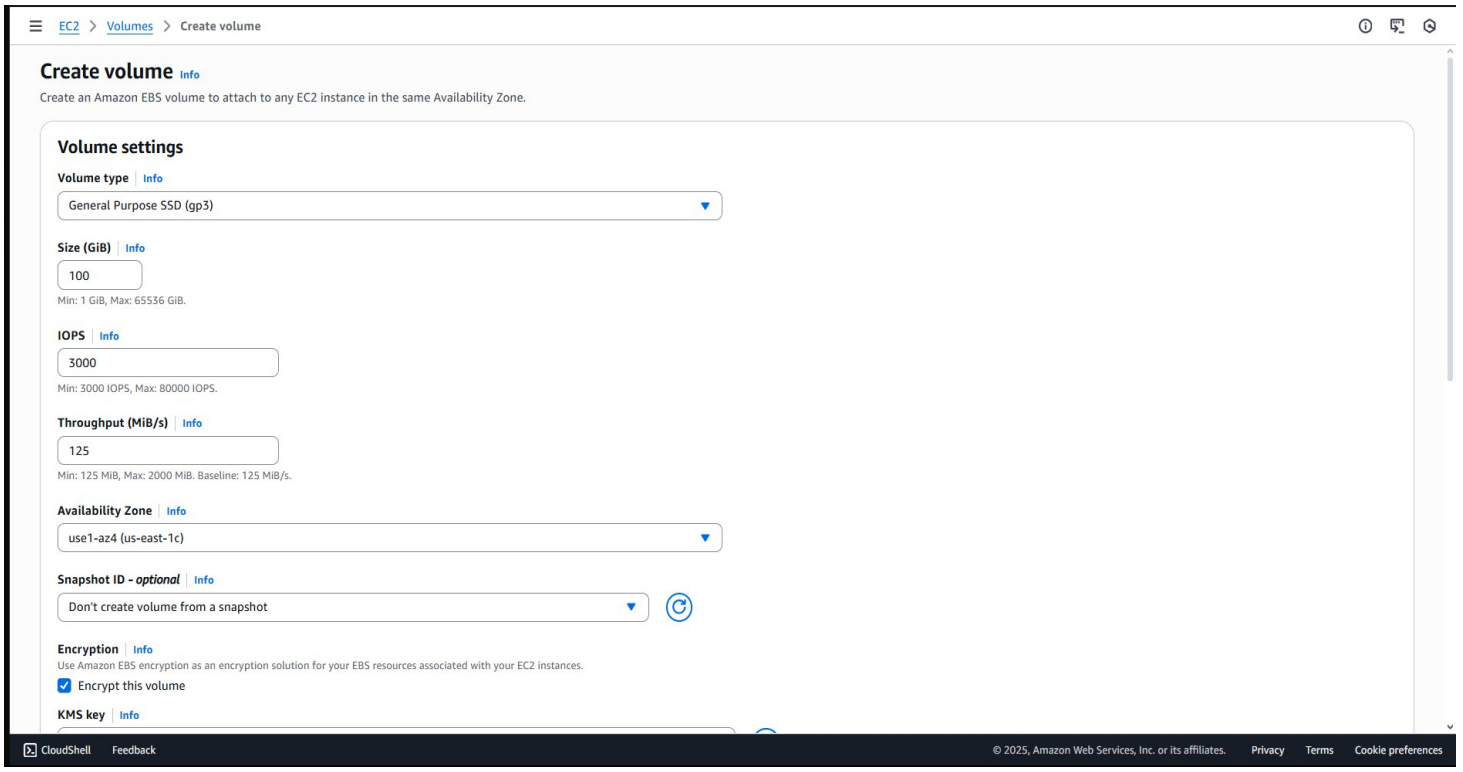
After selecting or creating the key pair, click **"Launch instance"**. AWS will now provision your new EC2 instance. You can monitor its status on the EC2 dashboard, where it will show up as **"Pending"** and then transition to **"Running"** when it's ready.




Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1015-aws x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Sun Nov 9 17:48:38 UTC 2025
System load: 0.08
Usage of /: 25.8% of 6.71GB
Memory usage: 22%
Swap usage: 0%
Temperature: -273.1 C
Processes: 108
Users logged in: 0
IPv4 address for ens5: 172.31.31.132
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ip-172-31-31-132:~$ ls
ubuntu@ip-172-31-31-132:~$
i-087e63f2c2da7c9fe (bannerEC2)
PublicIPs: 3.90.0.226 PrivateIPs: 172.31.31.132
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

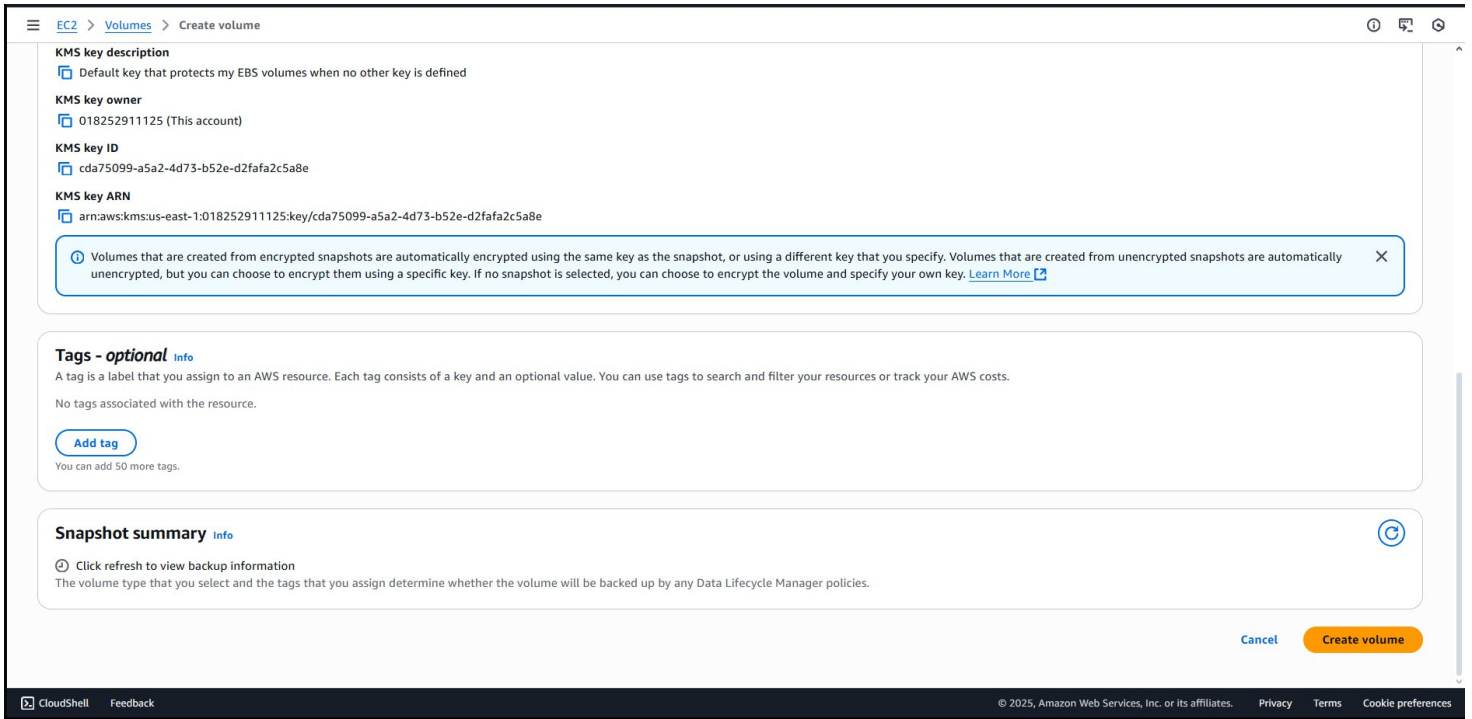
Practical 2 . Create Volume

Step-1: Search EC2 & scroll to volumes



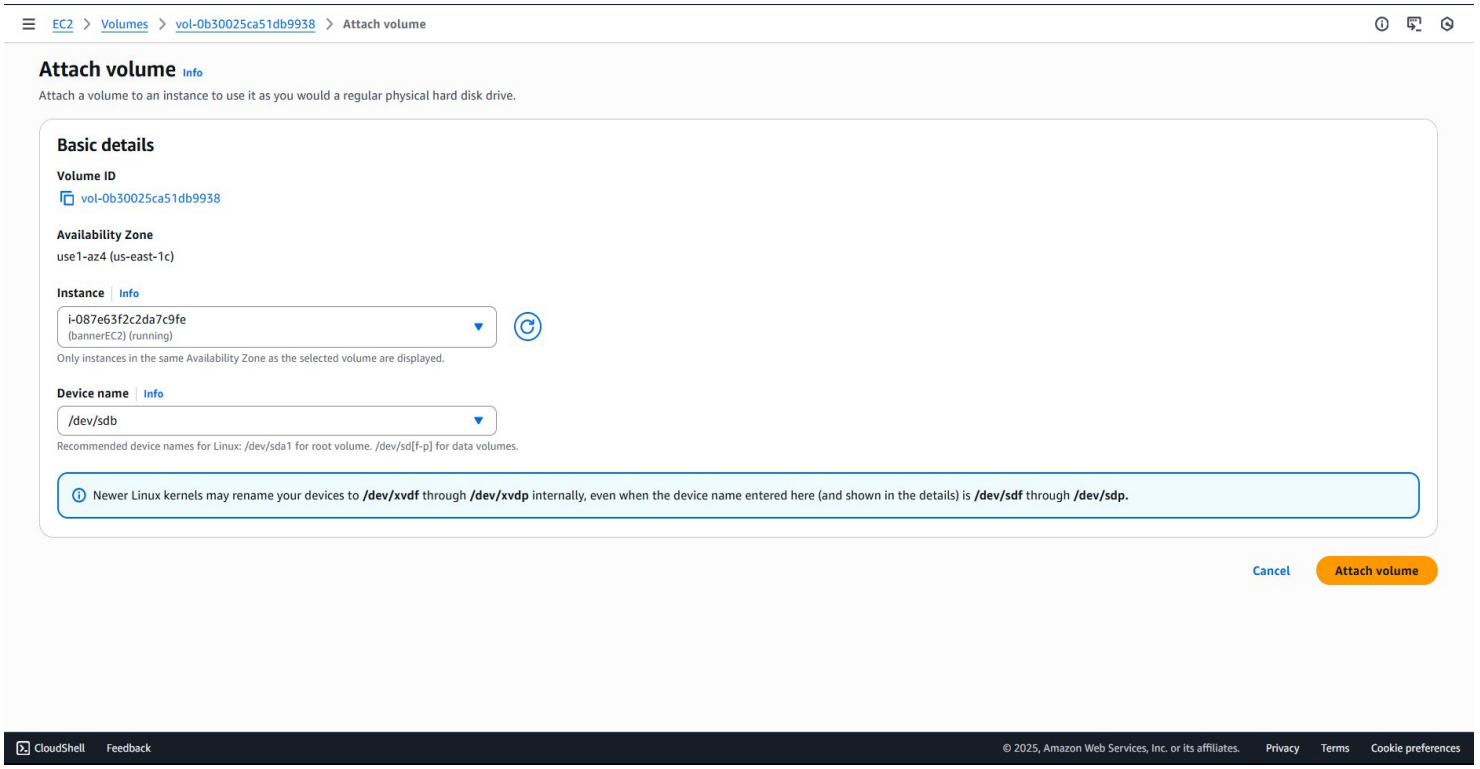
Click on create volume and choose the settings as per the requirements. (here we have chosen gp3 -> size=5 and rest are default.

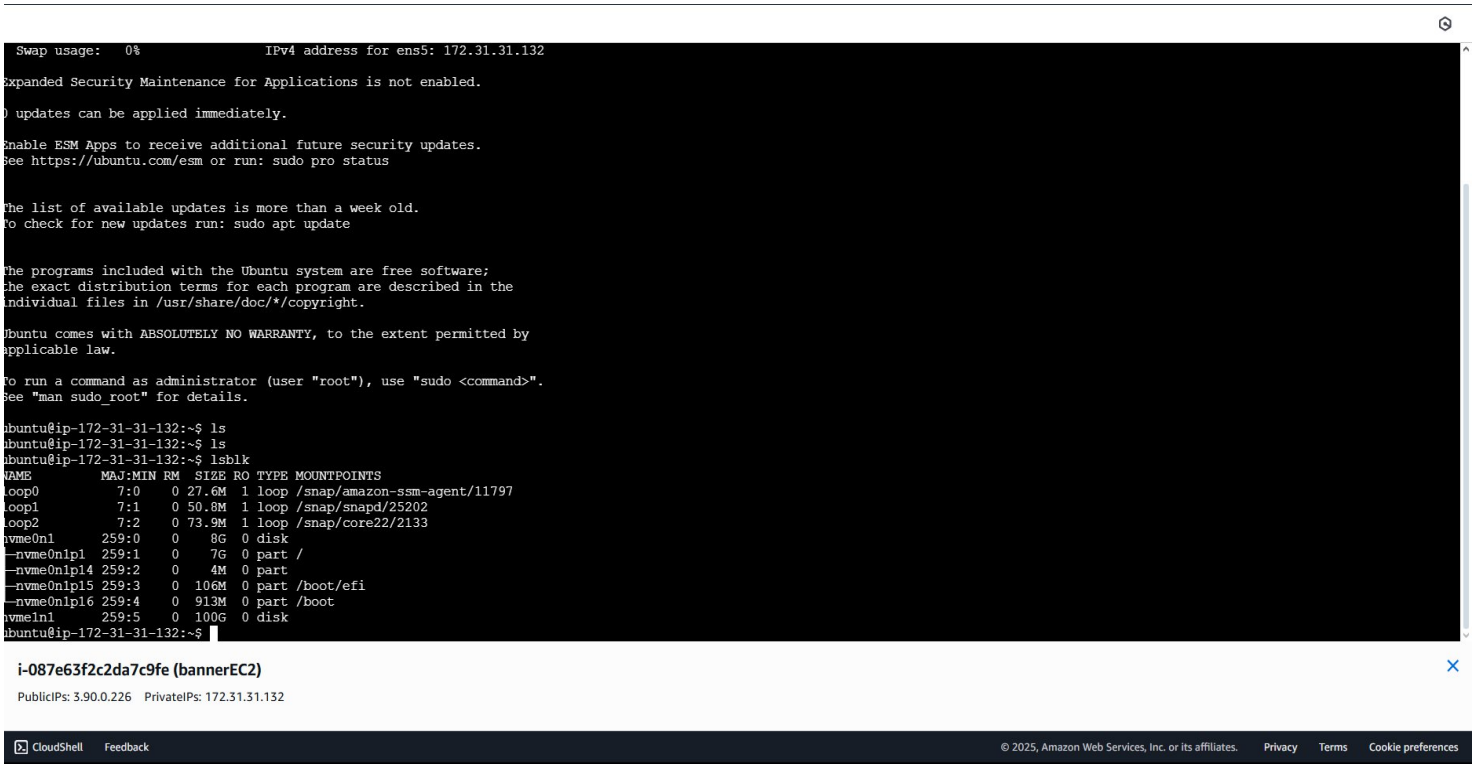
Step 2:- Keep the availability zone as the required zone in other activities



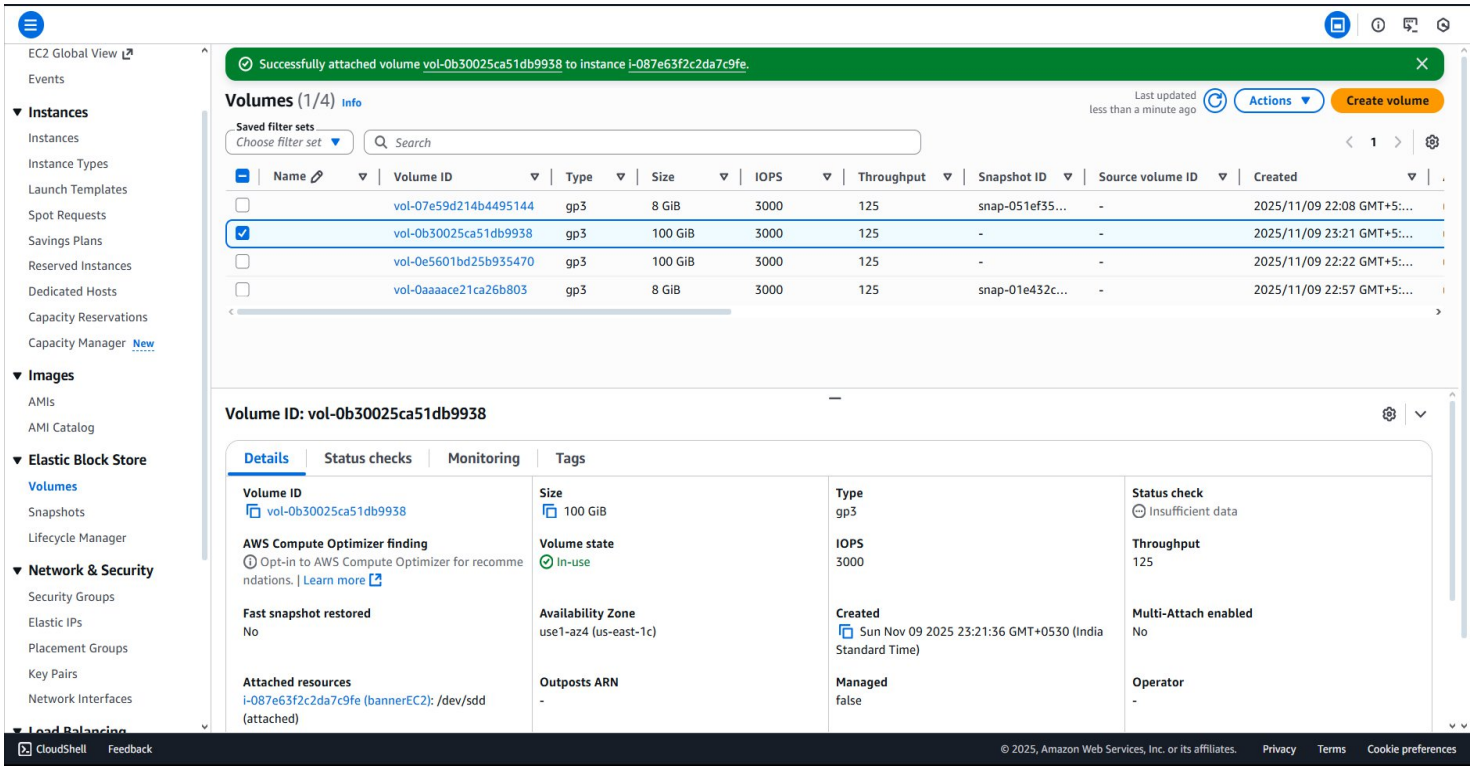
to
o.

Step 3: Attach the volume





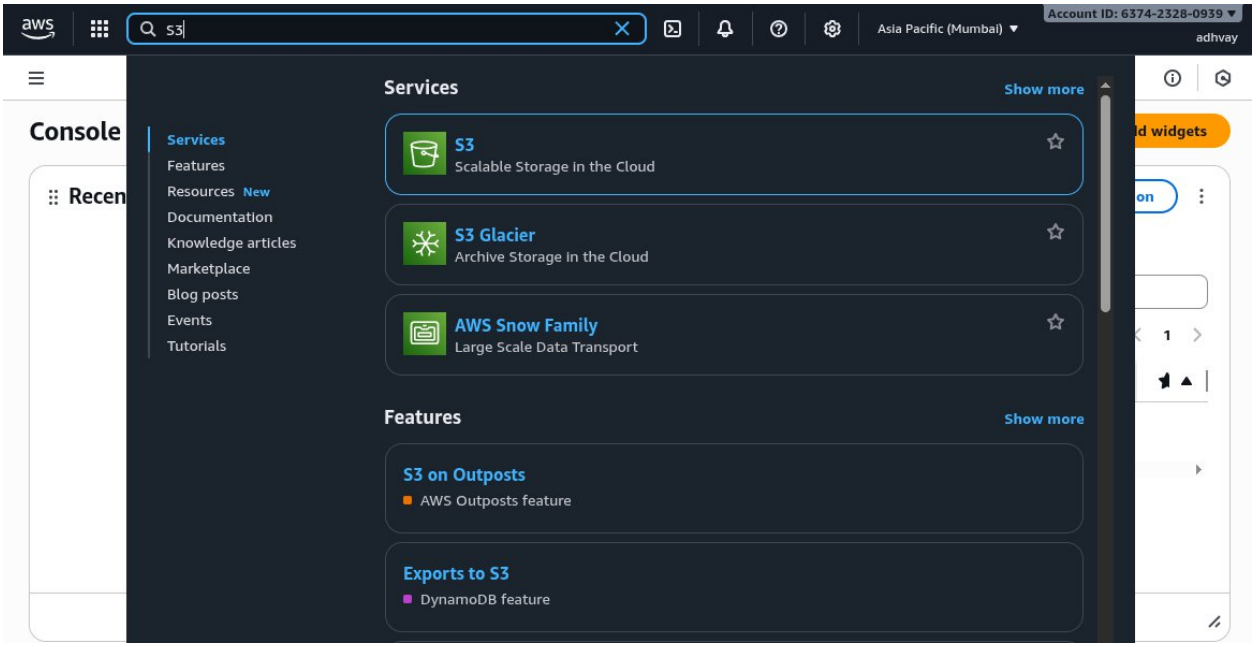
Finally the volume is attached


EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Load Balancing
Successfully attached volume vol-0b30025ca51db9938 to instance i-087e63f2c2da7c9fe.
Volumes (1/4) Info
Last updated less than a minute ago
Actions
Create volume
Saved filter sets
Choose filter set
Search
Name
Volume ID
Type
Size
IOPS
Throughput
Snapshot ID
Source volume ID
Created
vol-07e59d214b4495144 gp3 8 GiB 3000 125 snap-051ef35... - 2025/11/09 22:08 GMT+5:...
vol-0b30025ca51db9938 gp3 100 GiB 3000 125 - - 2025/11/09 23:21 GMT+5:...
vol-0e5601bd25b935470 gp3 100 GiB 3000 125 - - 2025/11/09 22:22 GMT+5:...
vol-0aaaace21ca26b803 gp3 8 GiB 3000 125 snap-01e432c... - 2025/11/09 22:57 GMT+5:...
Volume ID: vol-0b30025ca51db9938
Details
Status checks
Monitoring
Tags
Volume ID
vol-0b30025ca51db9938
Size
100 GiB
Type
gp3
Status check
Insufficient data
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more
Volume state
In-use
IOPS
3000
Throughput
125
Fast snapshot restored
No
Availability Zone
use1-az4 (us-east-1c)
Created
Sun Nov 09 2025 23:21:36 GMT+0530 (India Standard Time)
Multi-Attach enabled
No
Attached resources
i-087e63f2c2da7c9fe (bannerEC2): /dev/sdd (attached)
Outposts ARN
-
Managed
false
Operator
-
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Practical 3 - CREATE AN S3 BUCKET IN AWS

2. Navigate to S3

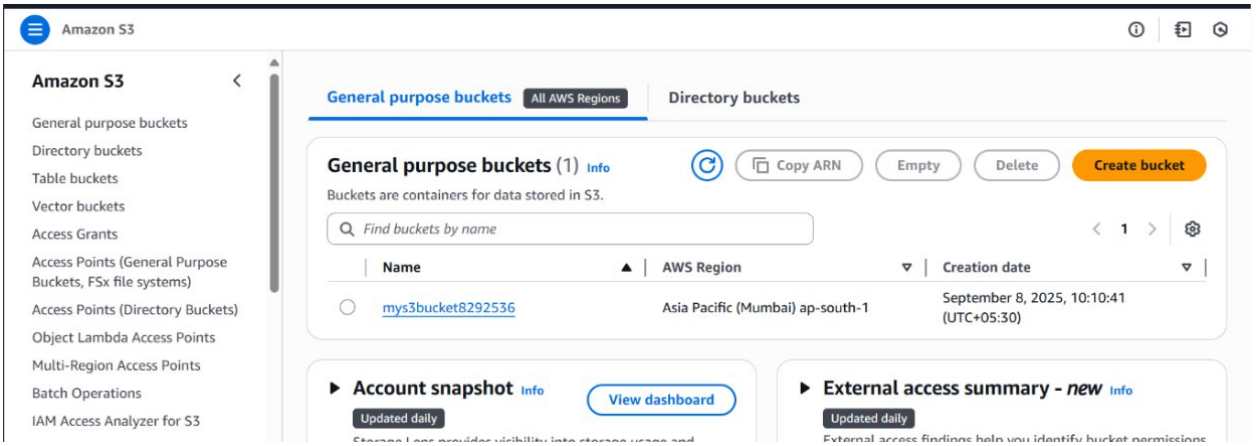
- In the search bar at the top, type **S3**.
- Click on **S3 (Scalable Storage in the Cloud)**.



---

3. Create a New Bucket

- Click on **“Create bucket”** button.

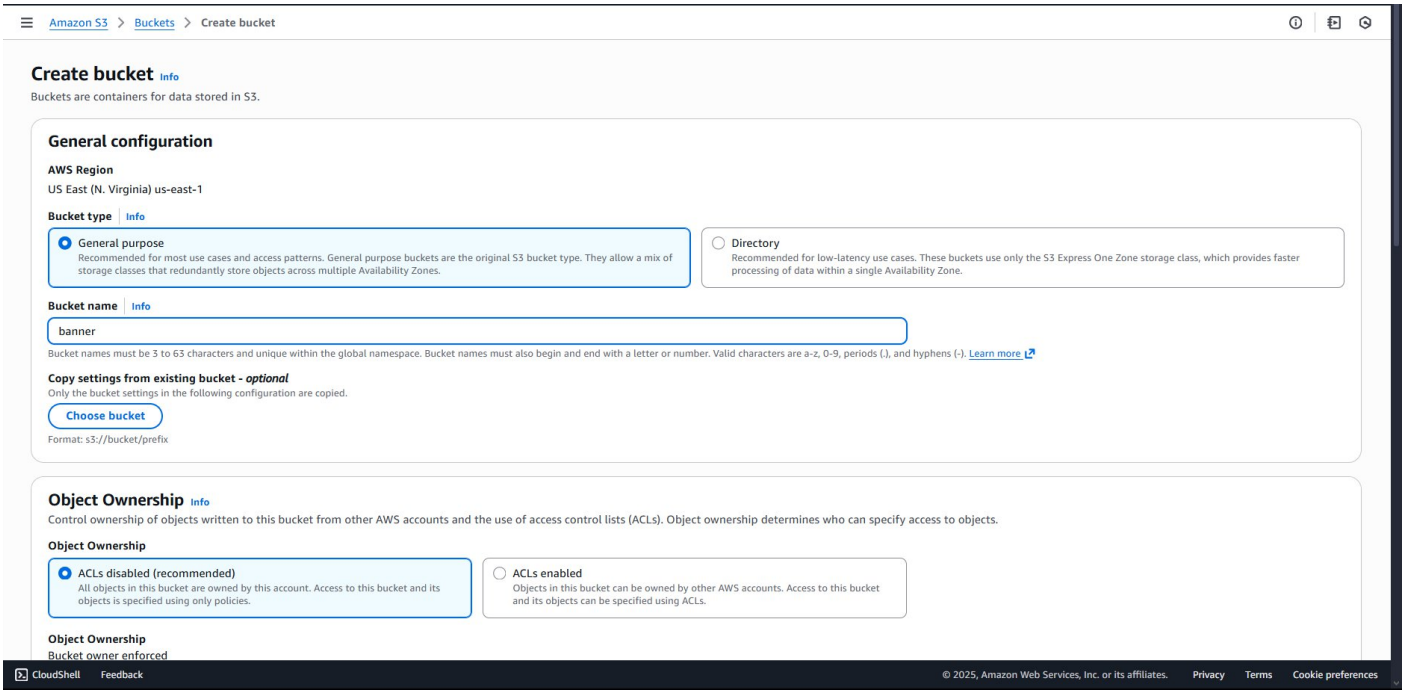


4. Configure Bucket Settings

- **Bucket name**: Enter a unique name (e.g., my-first-s3-bucket-2025).

⚠ Bucket names must be globally unique across AWS.

- **AWS Region**: Select a region (choose one closest to your users for better performance).



---

5. Set Bucket Options

- **Object Ownership**:
- Choose **ACLs disabled (recommended)** for most use cases.
- **Block Public Access**:
- By default, all public access is blocked (recommended for private buckets).
- If you need a public bucket (for hosting static websites), uncheck the option and acknowledge the warning.

---

6. Configure Bucket Settings (Optional)

- **Versioning**: Enable if you want to keep multiple versions of an object.
- **Encryption**: Enable default encryption if required.
- **Tags**: Add key-value tags if you want to manage cost tracking or organization.

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.

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.

Encryption type Info

Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

- (•) Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ( ) Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Amazon S3 > Buckets > Create bucket

- ( ) 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.

Encryption type Info

Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

- (•) Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ( ) Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- ( ) Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

- ( ) Disable
- (•) Enable

▶ **Advanced settings**

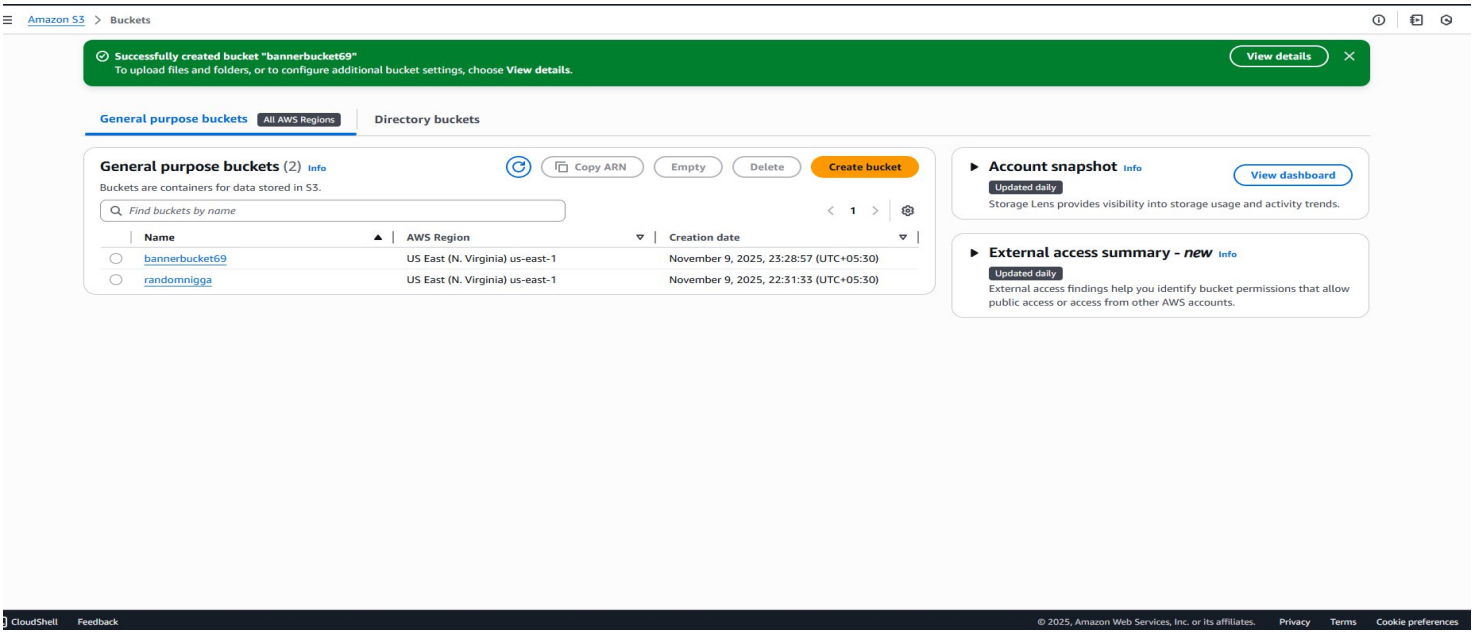
ⓘ After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel Create bucket

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

7. Review and Create

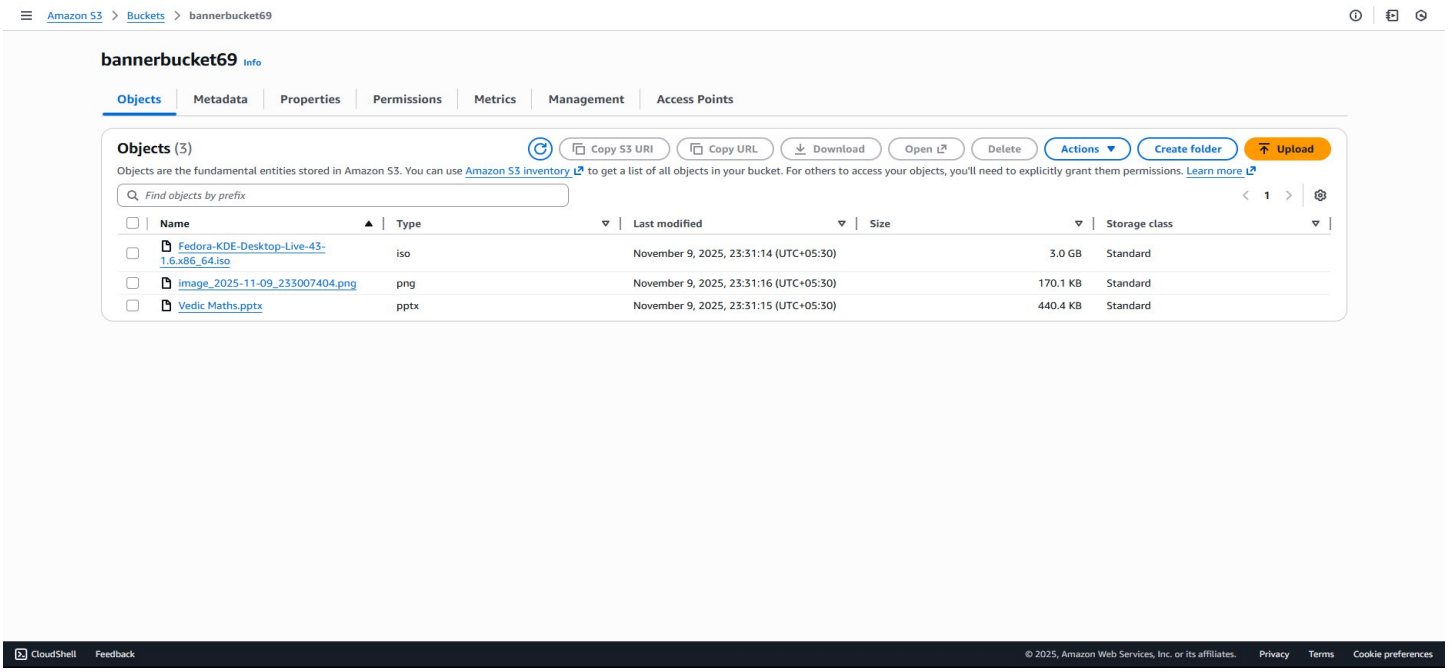
- Review your settings.
- Click **Create bucket**.

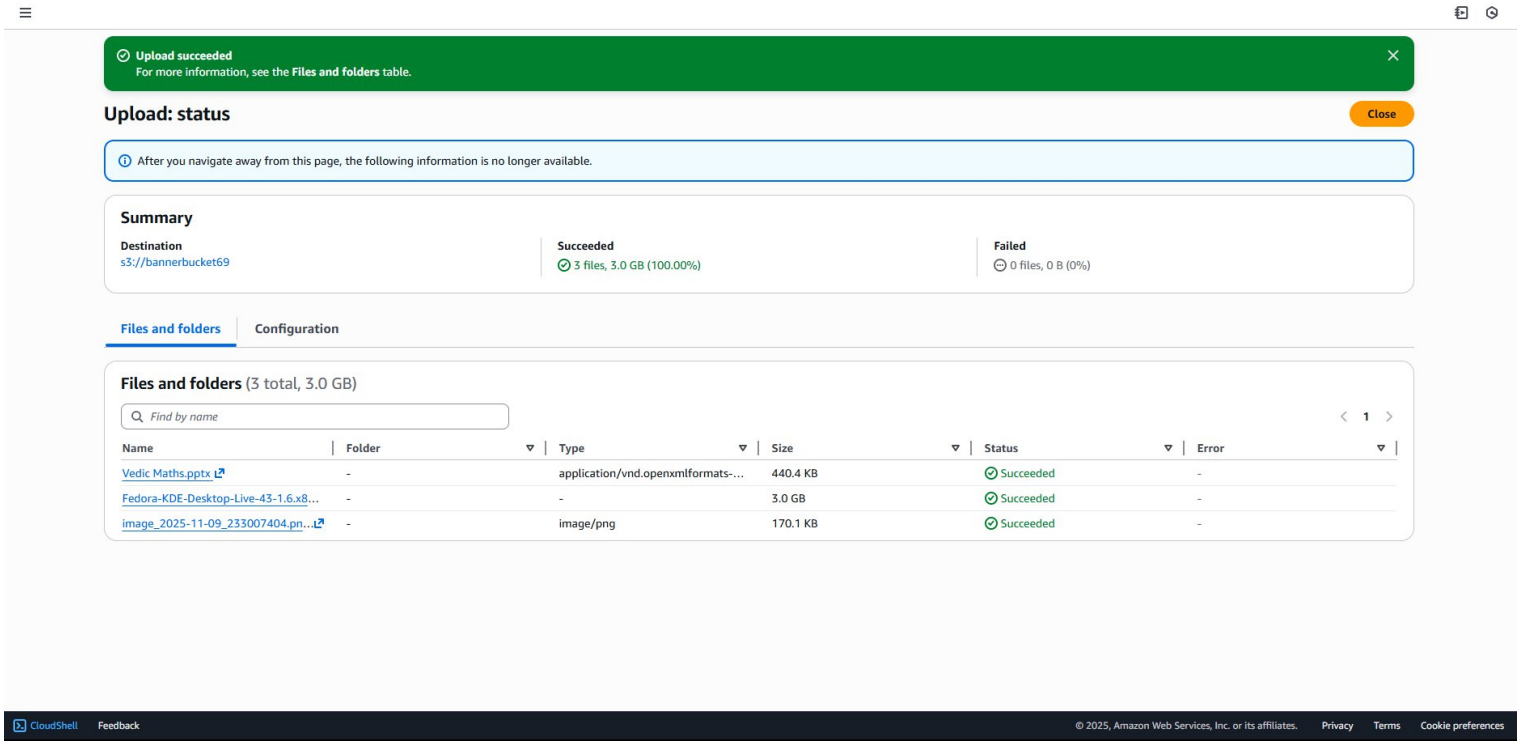


---

8. Upload Objects (Optional)

- After creation, open the bucket.
- Click **Upload → Add files**.
- Select your file(s), then click **Upload**.





Practical 4 . Steps to Create an AWS Lambda Function

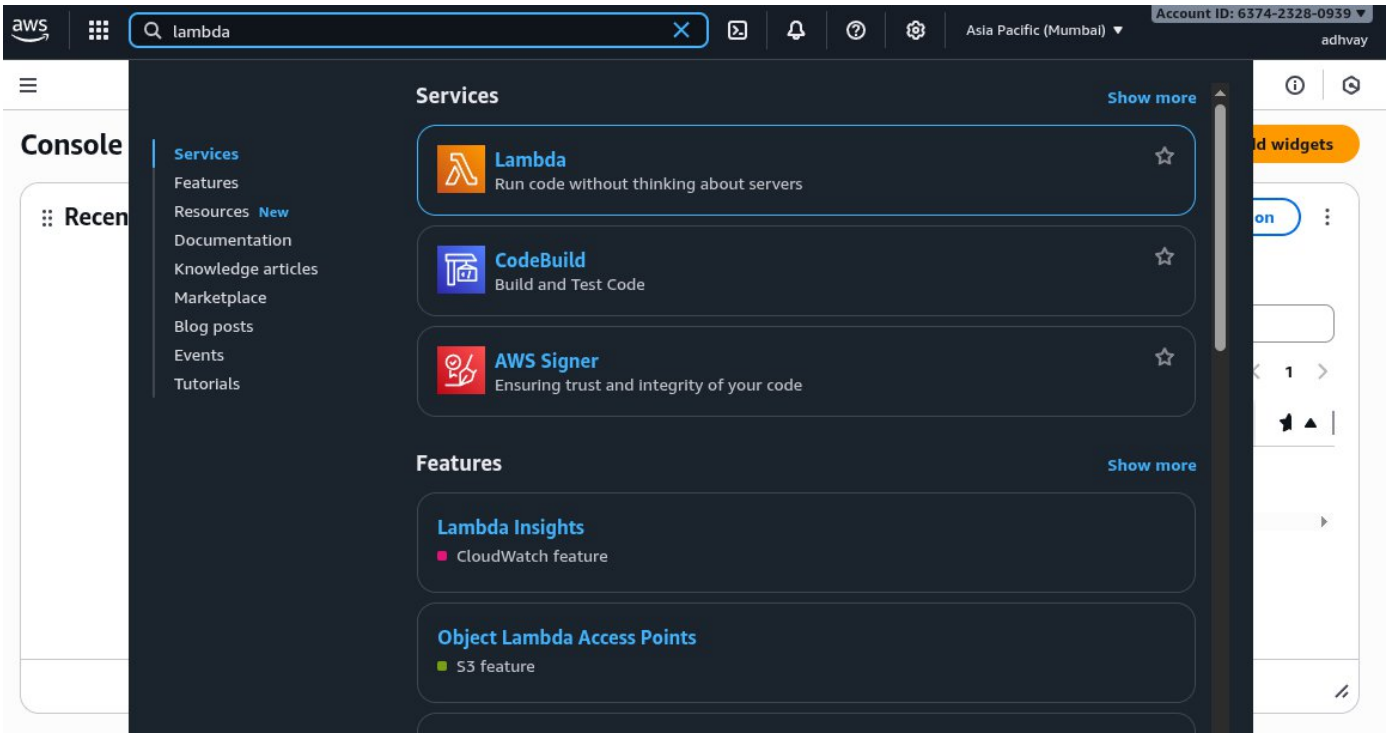
1. Log in to AWS Management Console

- Go to AWS Console.
- Sign in with your credentials.

---

2. Navigate to AWS Lambda

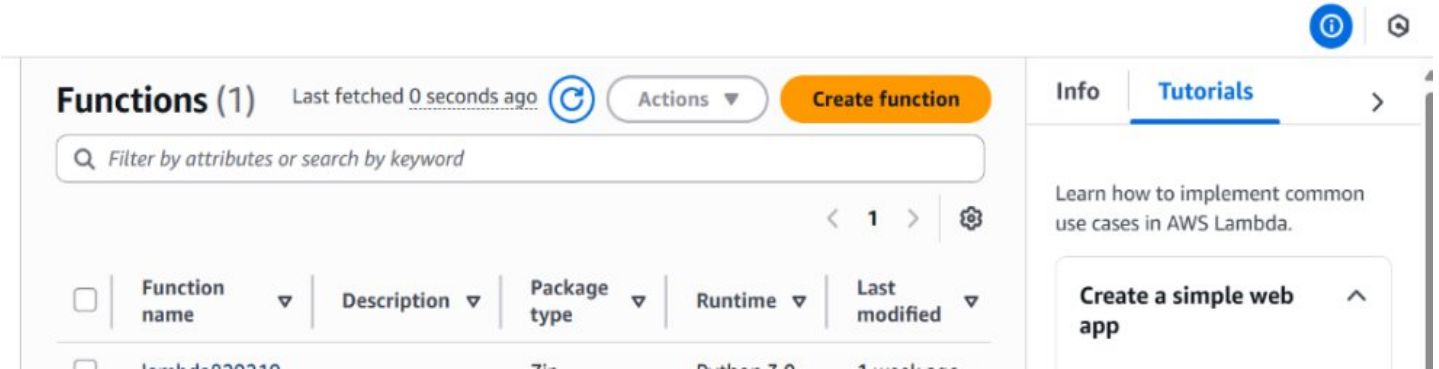
- In the search bar, type **Lambda**.
- Click on **Lambda** service.



---

3. Create a New Lambda Function

- Click **Create function**.

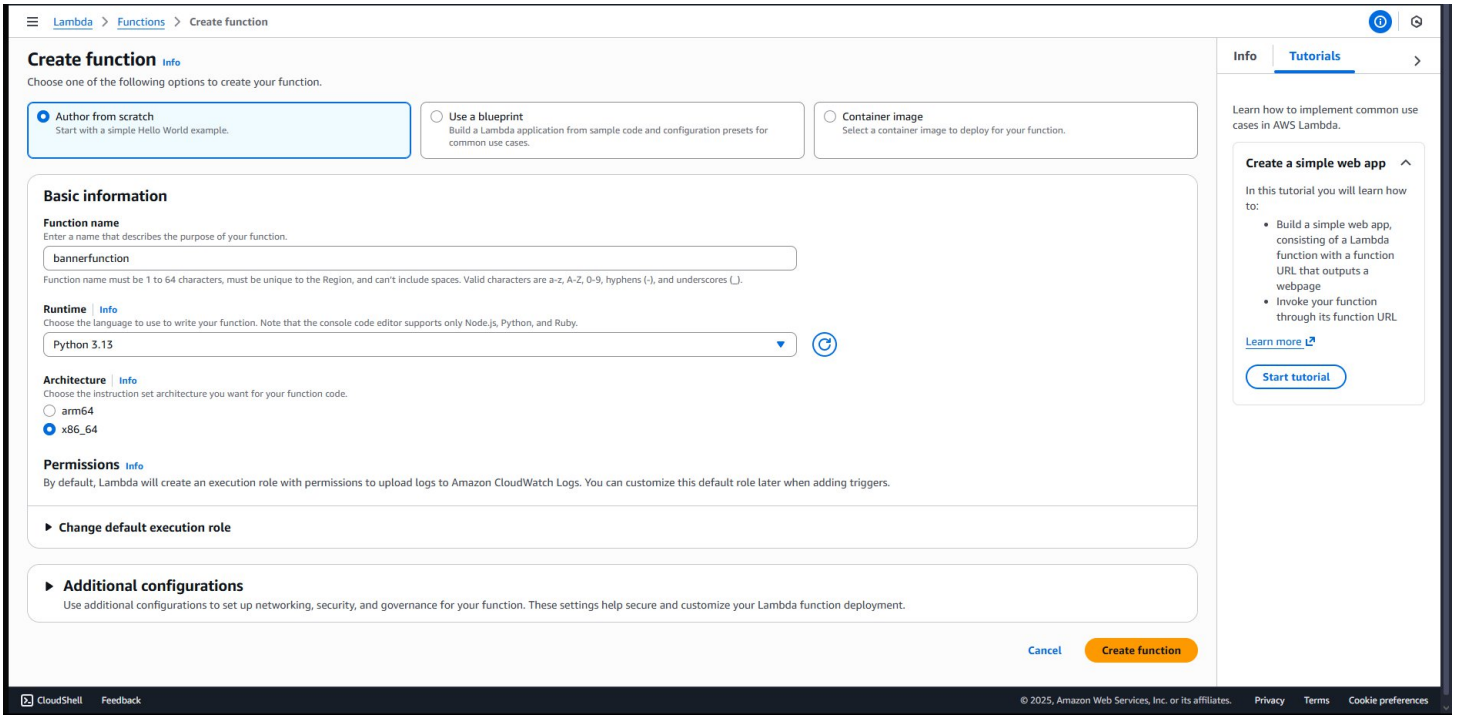


4. Choose a Creation Method

You'll see 3 options:

1. **Author from scratch** → (most common, start fresh).
2. **Use a blueprint** → predefined templates.
3. **Container image** → deploy code as Docker container.

☞ Select **Author from scratch**.



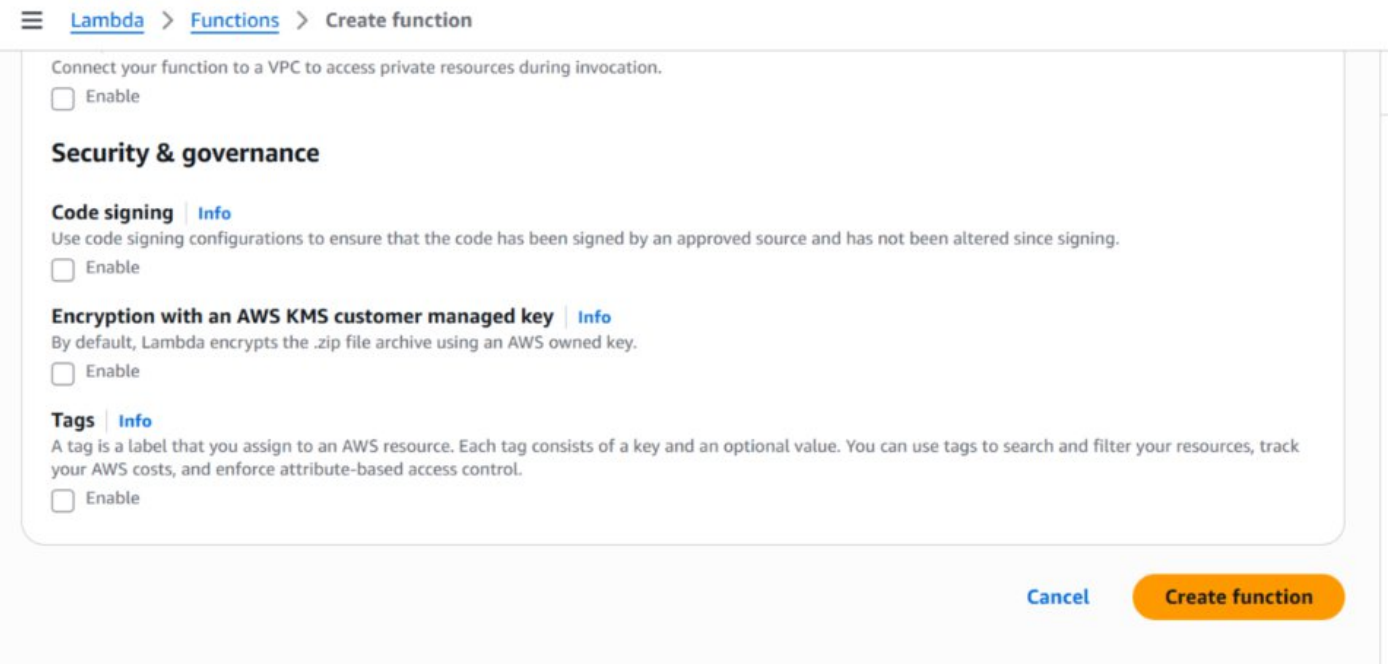
5. Configure Basic Settings

- **Function name**: Enter a unique name (e.g., SampleLambda).
- **Runtime**: Choose a runtime (Python, Go, etc. → example: **Python 3.12**).
- **Permissions (Execution Role)**:

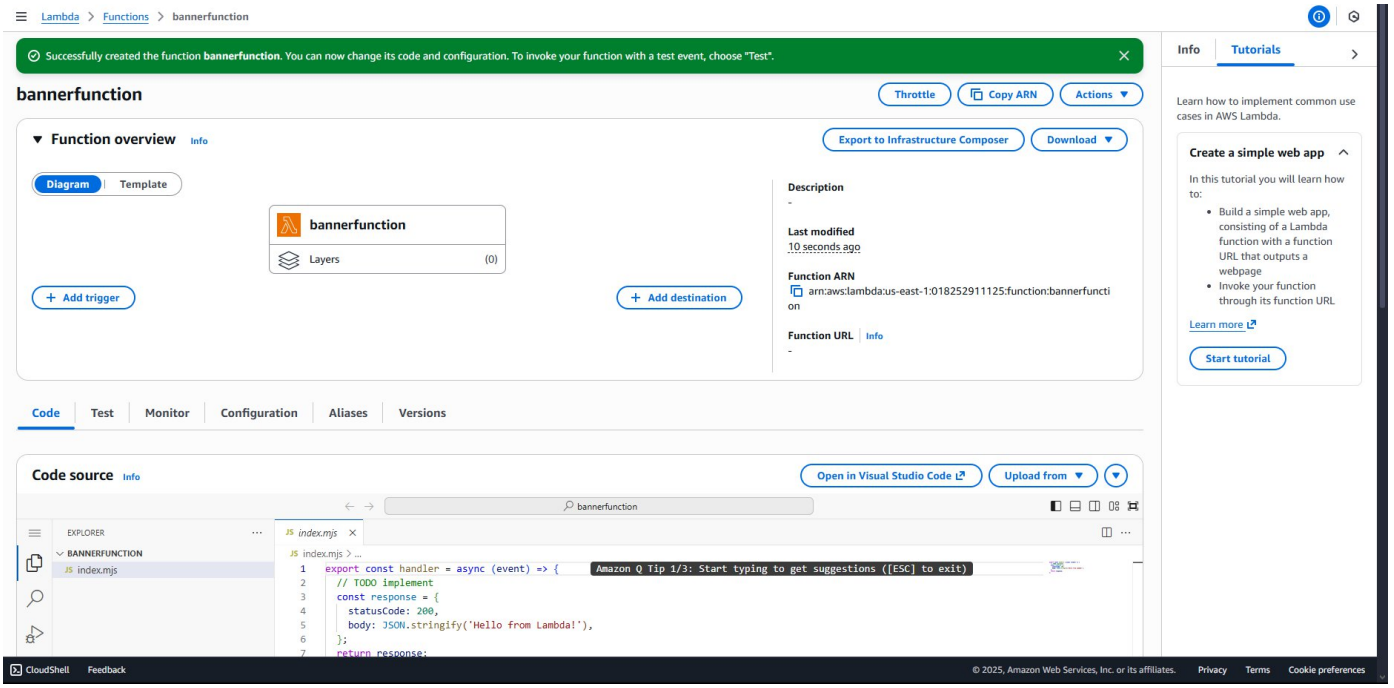
- **Create a new role with basic Lambda permissions** (recommended if you're new).
- Or choose an existing IAM role if you already have one.

---

6. Click Create Function



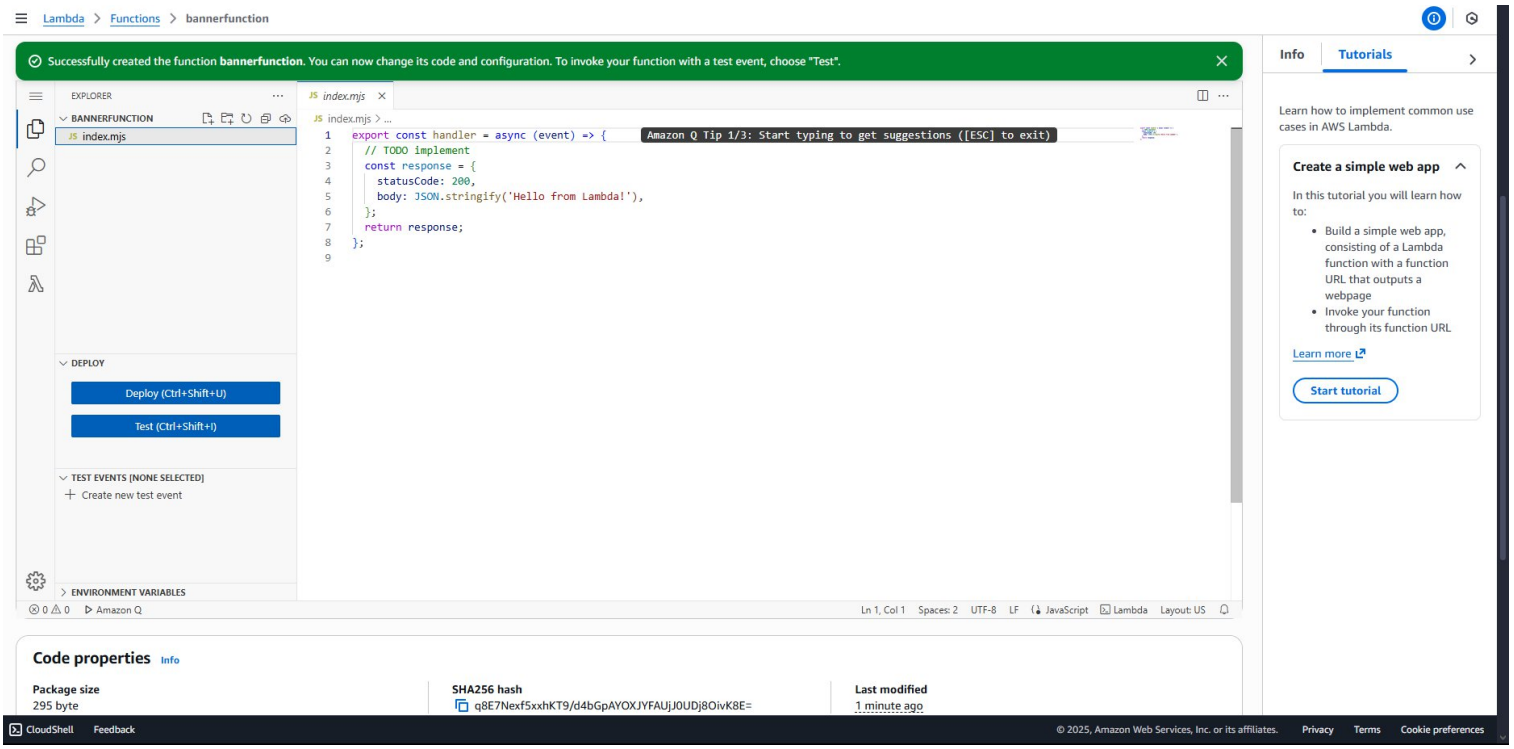
Wait a few seconds while AWS provisions the function.

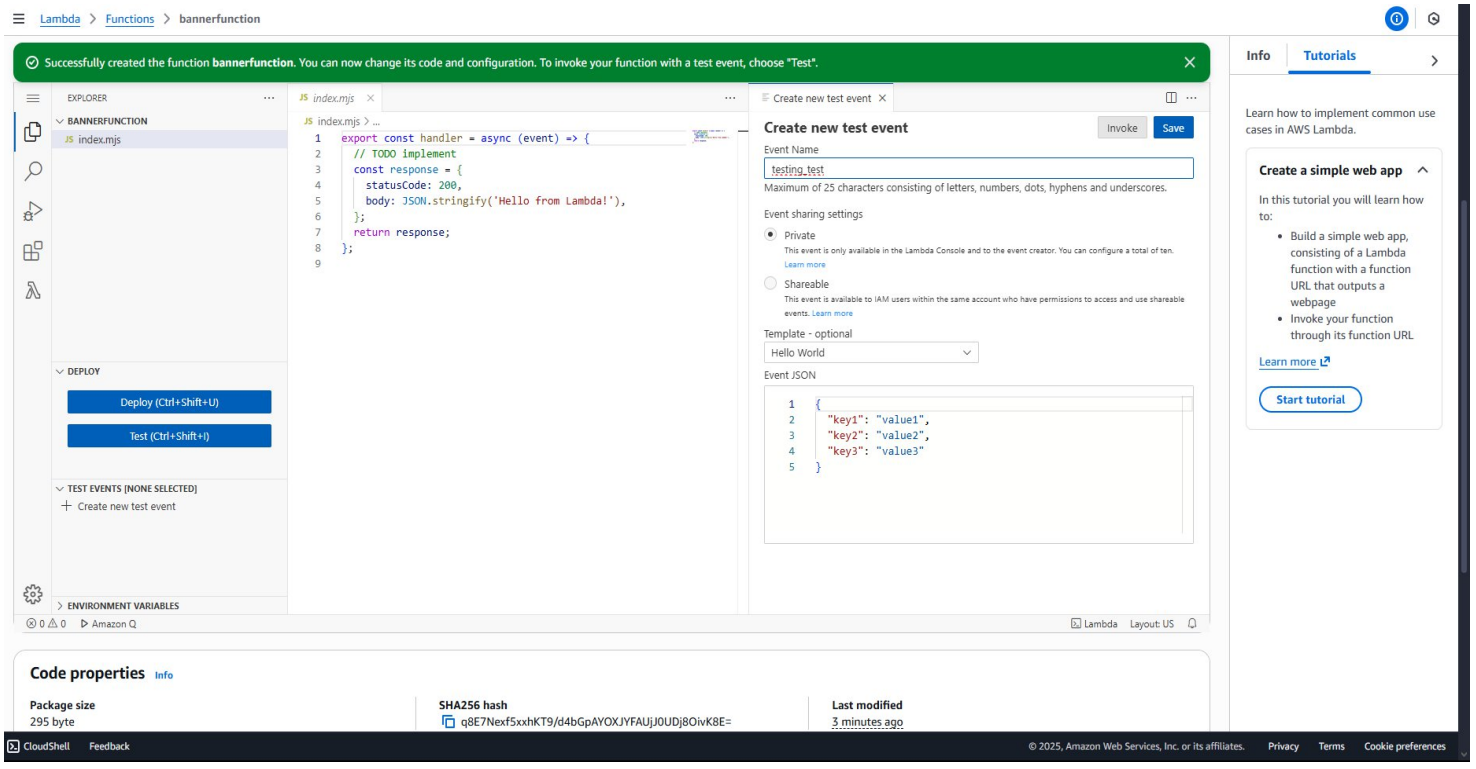


7. Add Your Code

- In the **Function code** section, you can:
- Write inline code in the editor.
- Or upload a .zip file.
- Or use **Amazon S3** (if your code is stored there).

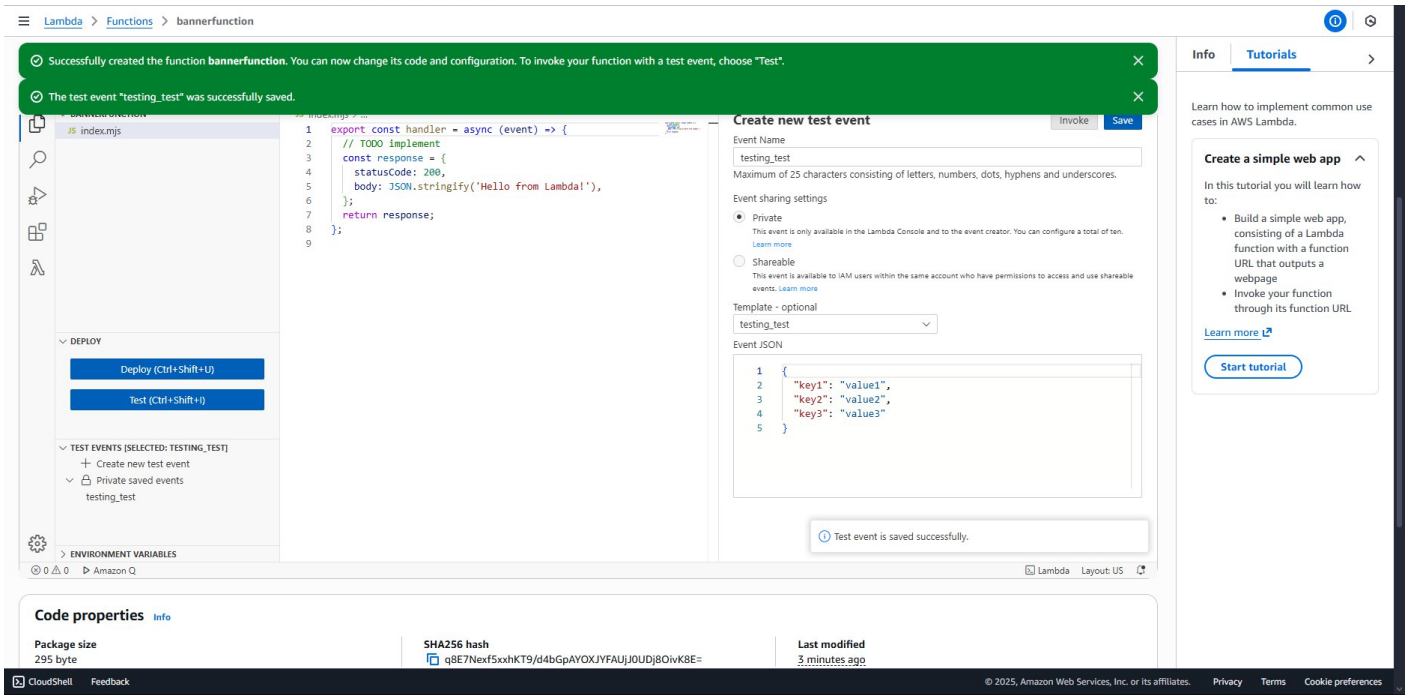
Example default code in Js:





8. Configure Test Event

- Click **Test** → **Configure test event**.



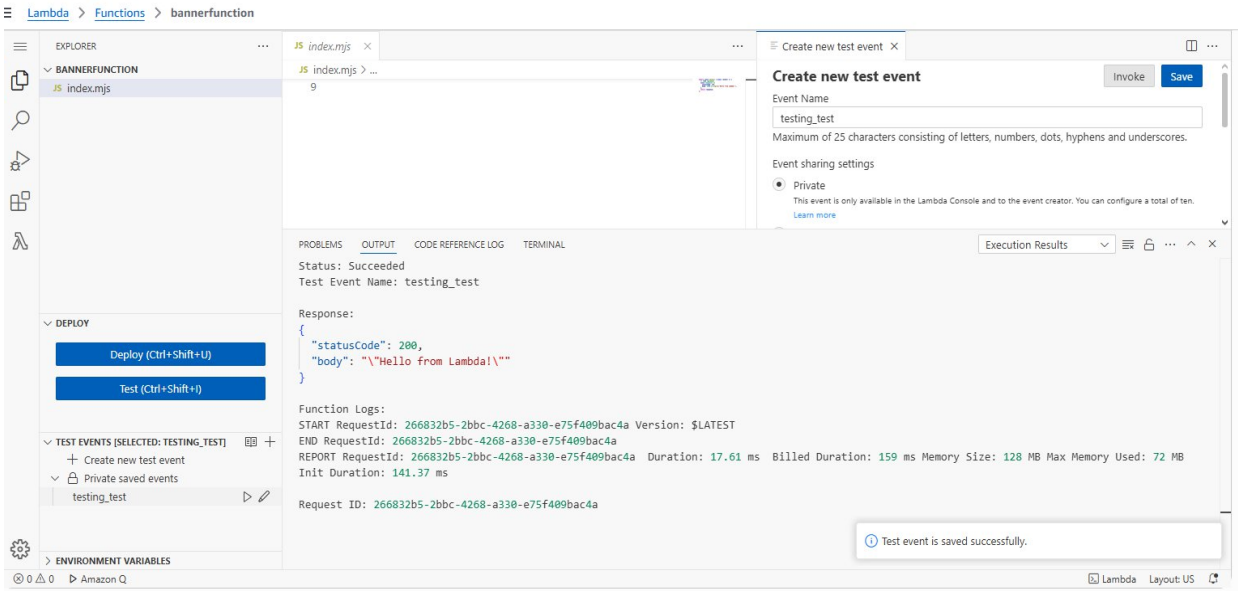
- Give it a name (e.g., TestEvent).
- Keep the default event JSON or modify as needed.

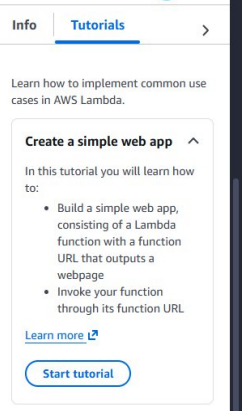
- Save.

9. Run the Function

- Click **Test** again.

Check the execution results (output, logs, and status





Code properties Info

Package size
295 byte

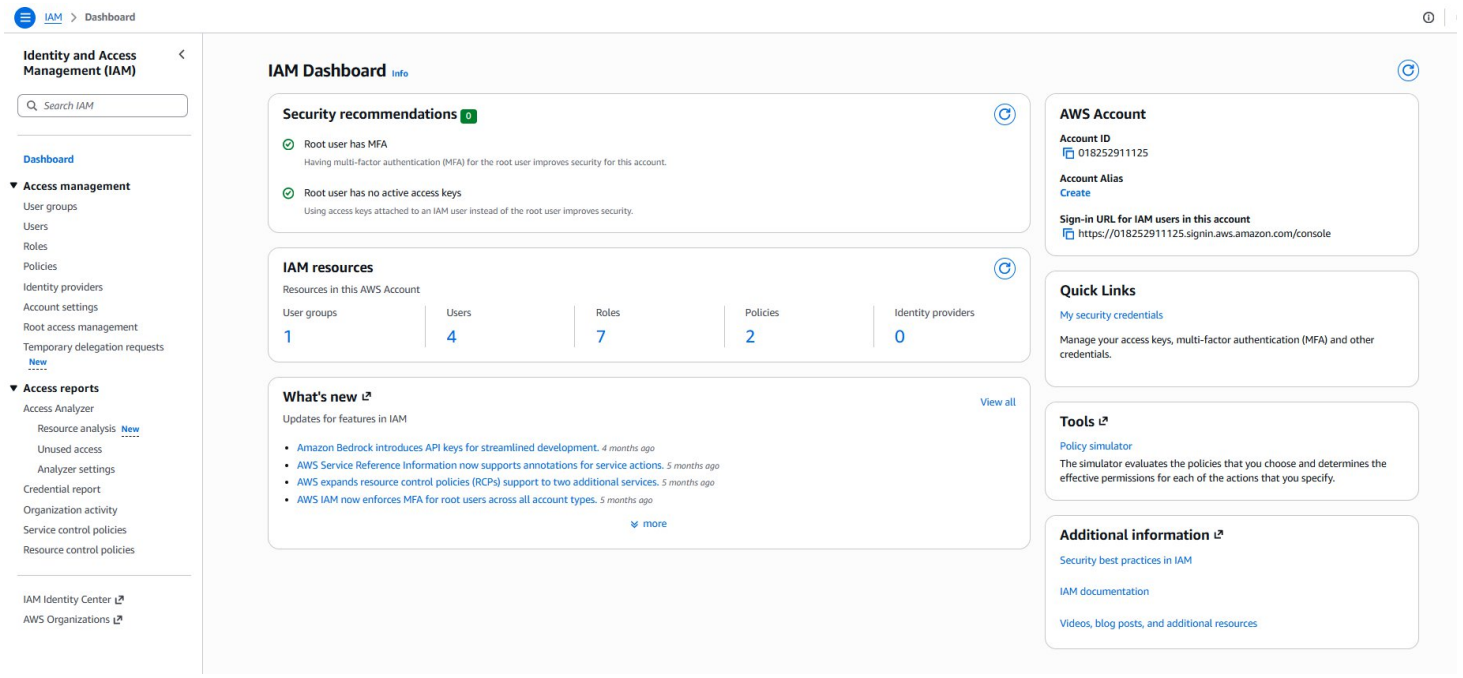
SHA256 hash
q8E7Nexf5xxhKT9/d4bGpAYOXJYFAUjJ0UDj8OivK8E=

Last modified
4 minutes ago

▶ **Encryption with AWS KMS customer managed KMS key** Info

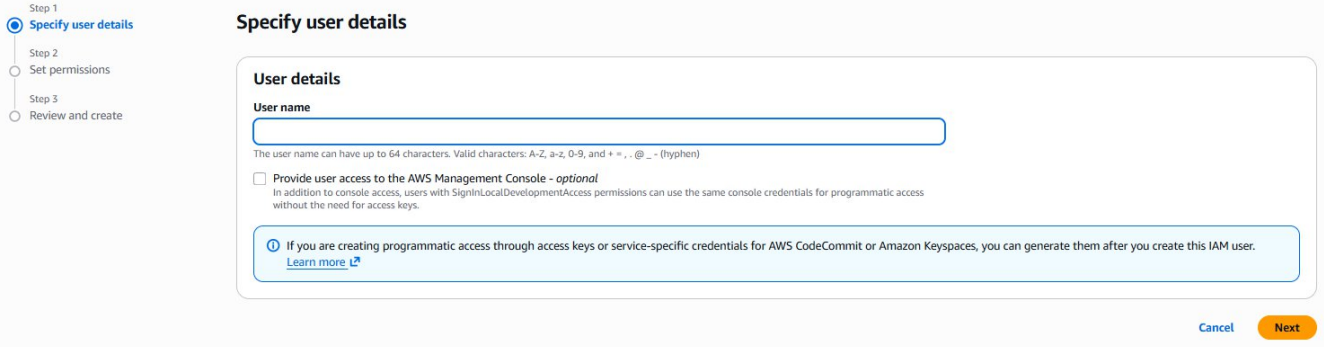
Practical 5: Creating an IAM (Identity and Access Management) user in AWS

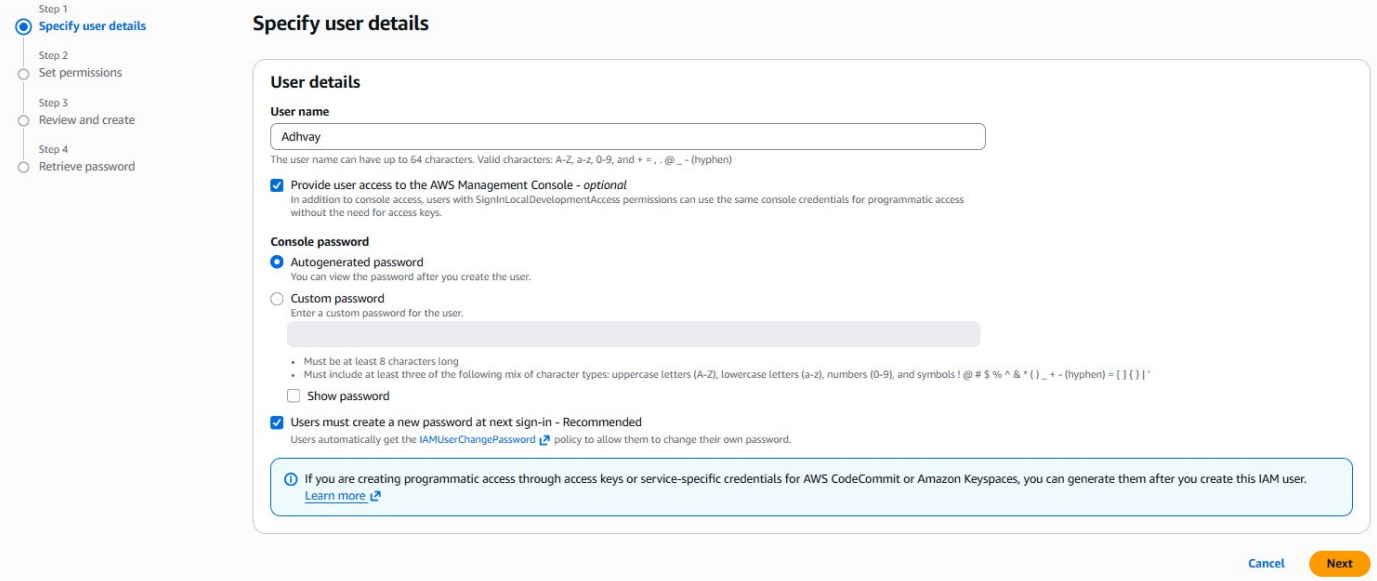
1. Open the IAM dashboard



2. Go to Users Section

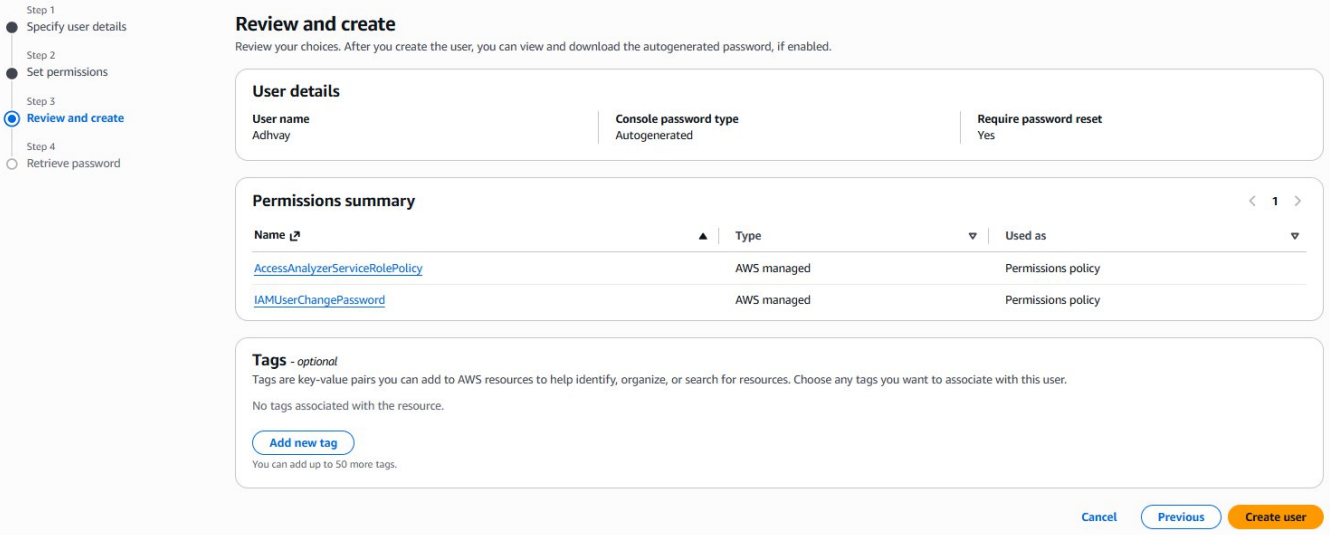
In the left sidebar, click on Users. You will see a list of all existing users. Click “Create user”



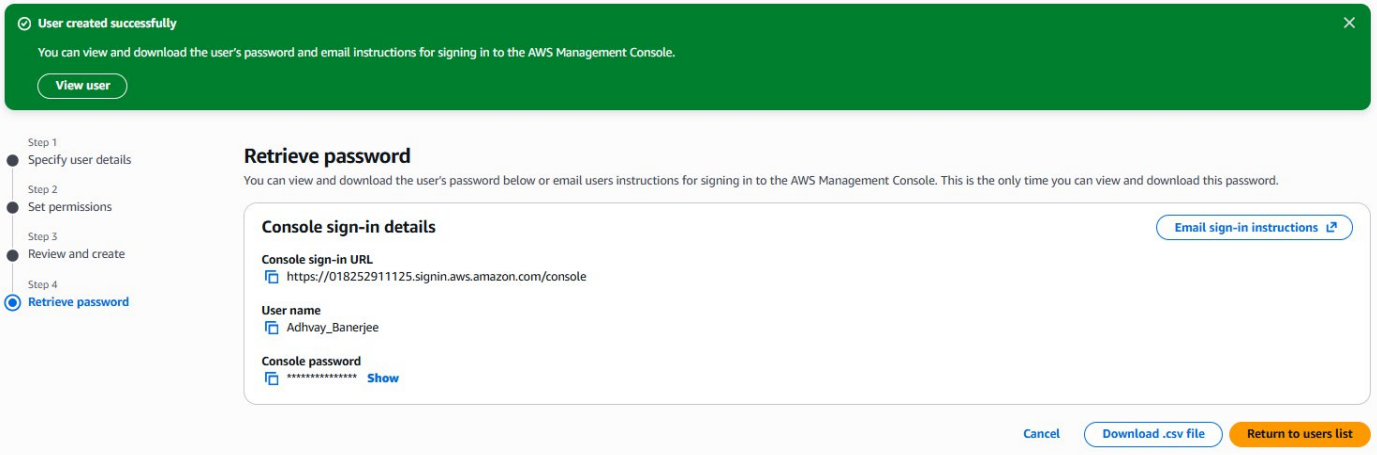


3. Set Permissions

Choose Attach policies directly → assign permissions manually (e.g., AmazonS3FullAccess, AdministratorAccess, etc.)



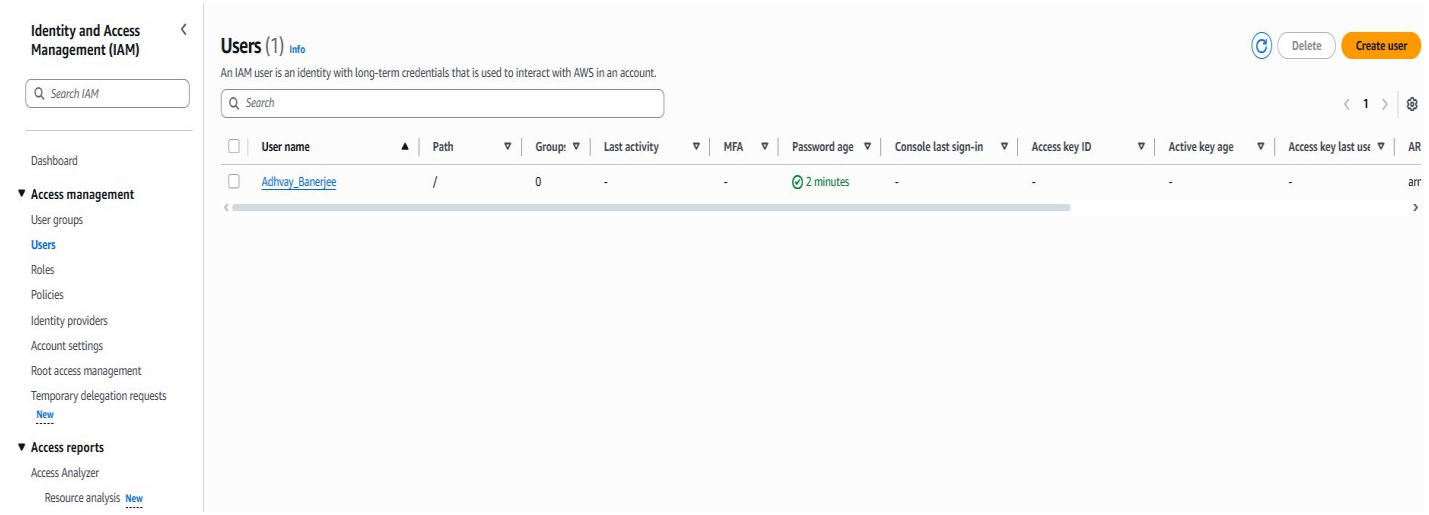
Finally click “Create User”

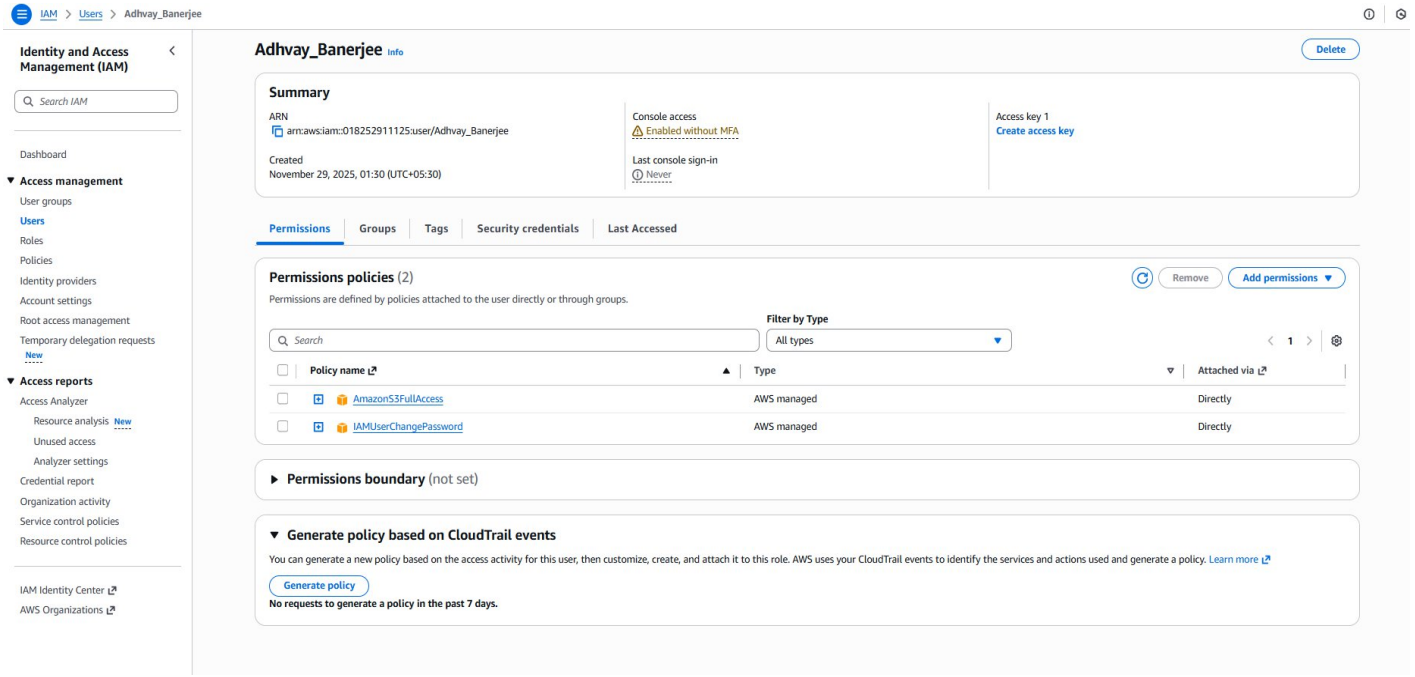


Practical :-6

Objective:- To secure an AWS IAM user account by enabling Multi-Factor Authentication (MFA)

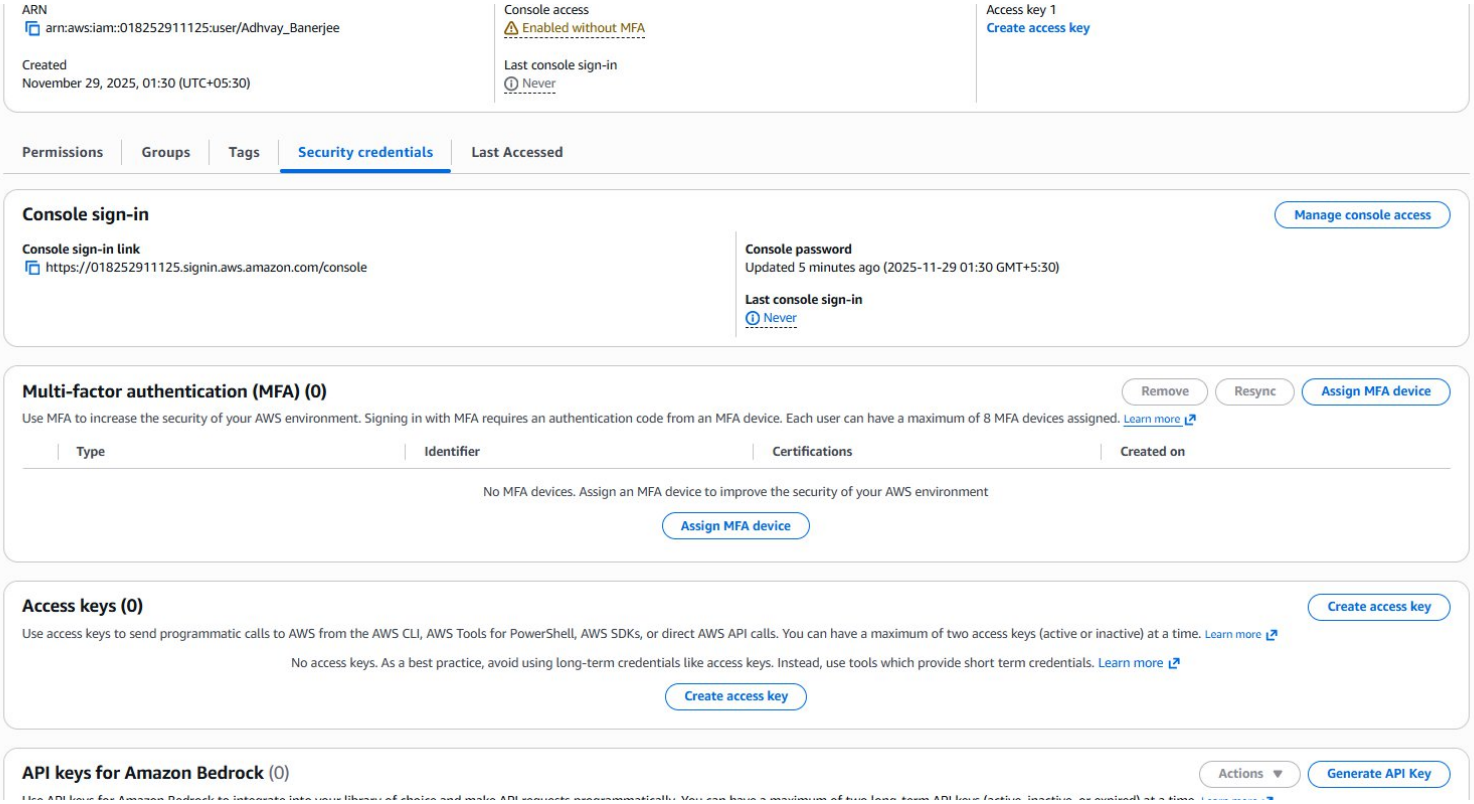
Step 1 :-Open “Users”





Step 2. In the left navigation panel, select Users.
Click the username for which you want to enable MFA.

- Go to the “Security Credentials” Tab
- After opening the user’s profile, click on Security credentials.
- Scroll down to the section Multi-Factor Authentication (MFA).

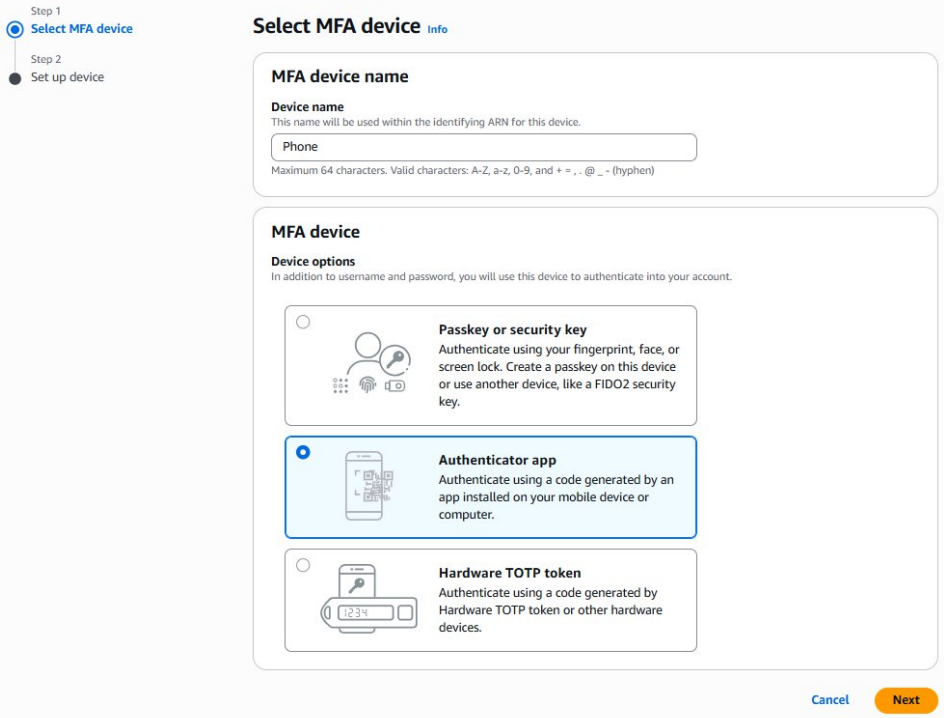


Step 3: Click “Assign MFA Device”

- A popup will open with 3 options:

1. FIDO2 Security Key
2. Authenticator App (Google Authenticator / Authy / Microsoft Authenticator)
3. Hardware TOTP Device

For most labs, choose Authenticator App for simplicity.



Step 4:-Select “Authenticator App” and Continue

- Click Continue.
- AWS will show a QR code for MFA enrollment.

Step 5:-Open your Authenticator App

You can use any app:

- Google Authenticator
- Authy
- Microsoft Authenticator
- LastPass Authenticator

Click Add Account → Scan QR Code.

The app will generate a 6-digit one-time password (OTP) that refreshes every 30 seconds.

Step 1
Select MFA device

Step 2
Set up device

Set up device Info

Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1. Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

   See a list of compatible applications

2. Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. **Show secret key**

3. Type two consecutive MFA codes below

Enter a code from your virtual app below

MFA Code 1

Wait 30 seconds, and enter a second code entry.

MFA Code 2

Cancel | Previous | Add MFA

IAM > Users > Adhvay_Banerjee

Identity and Access Management (IAM)

Search IAM

- Dashboard
- **Access management**
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
  - Root access management
  - Temporary delegation requests New
- **Access reports**
  - Access Analyzer
    - Resource analysis New
    - Unused access
    - Analyzer settings
  - Credential report
  - Organization activity
  - Service control policies
  - Resource control policies
- IAM Identity Center
- AWS Organizations

MFA device assigned
You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

Adhvay_Banerjee Info

Delete

Summary

ARN
arn:aws:iam::018252911125:user/Adhvay_Banerjee

Created
November 29, 2025, 01:30 (UTC+05:30)

Console access
Enabled with MFA

Last console sign-in
Never

Access key 1
Create access key

Permissions | Groups | Tags | Security credentials | Last Accessed

Console sign-in

Manage console access

Console sign-in link
https://018252911125.signin.aws.amazon.com/console

Console password
Updated 8 minutes ago (2025-11-29 01:30 GMT+5:30)

Last console sign-in
Never

Multi-factor authentication (MFA) (1)

Remove | Resync | Assign MFA device

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

Type	Identifier	Certifications	Created on
Virtual	arn:aws:iam::018252911125:mfa/Phone	Not Applicable	Sat Nov 29 2025

Access keys (0)

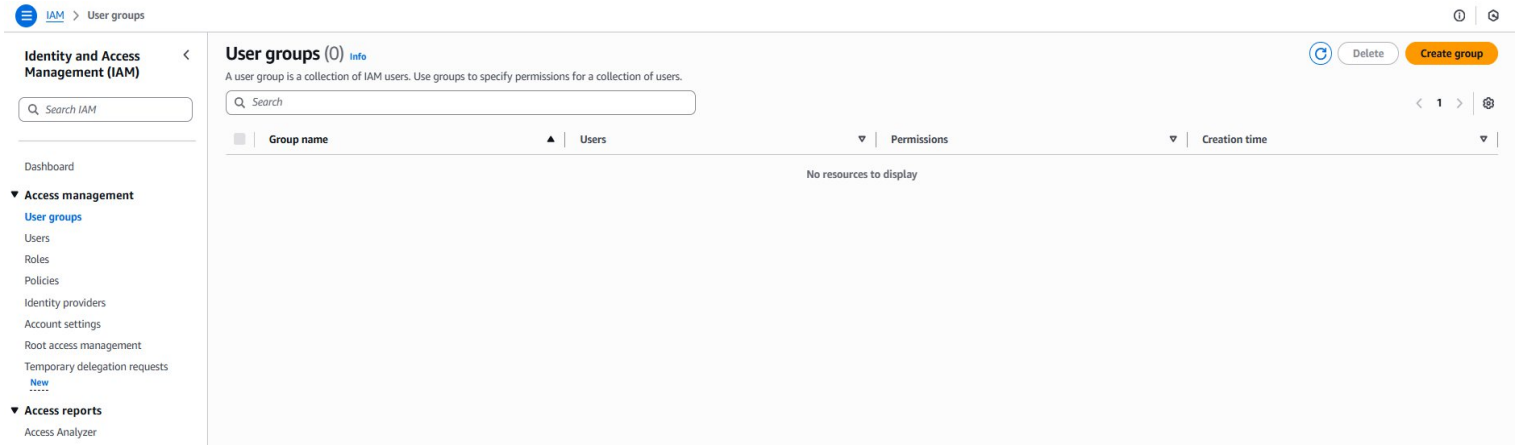
Create access key

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

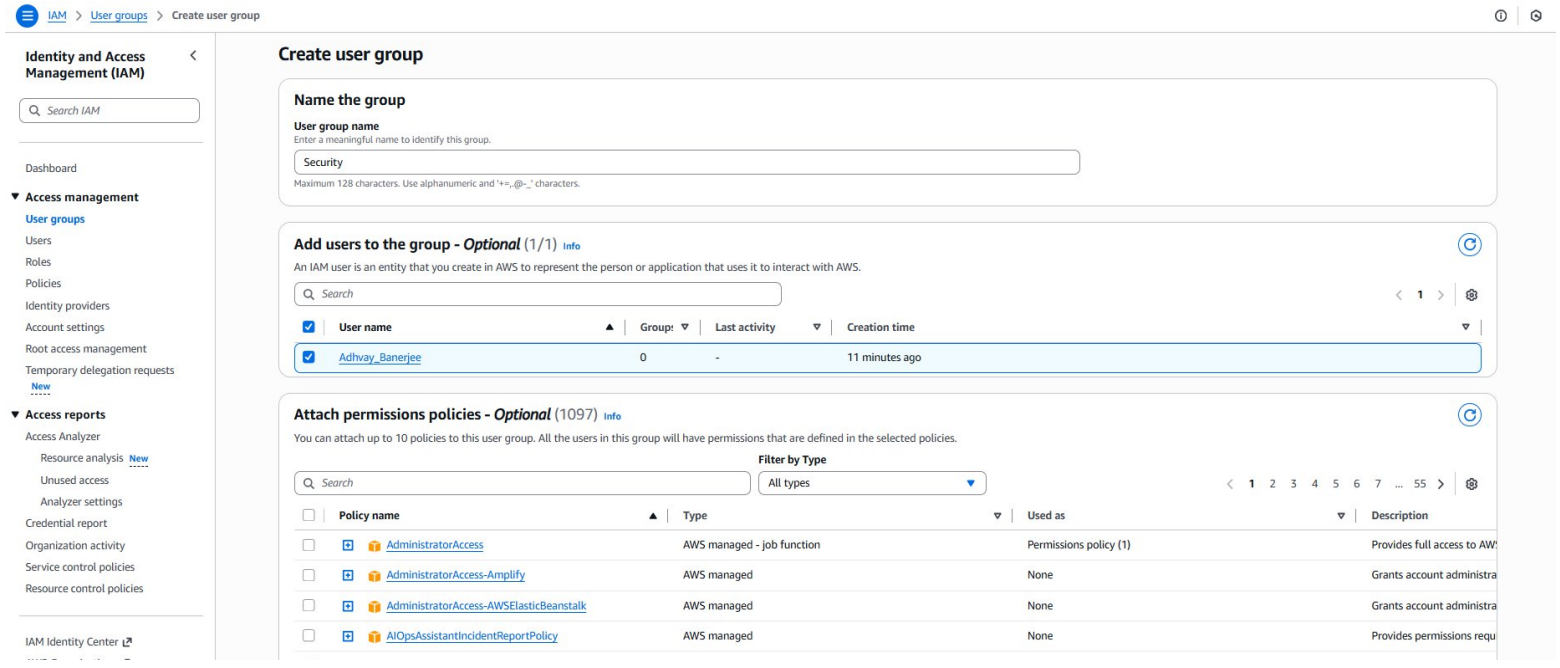
No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more

Practical:-7
Objective: To create a user group in AWS IAM

Step 1:- Go to User Groups Section:
In the left-hand sidebar, click on User groups.



Step 3:- Click on “Create group”:
On the User Groups page, click the “Create group” button to start creating a new group



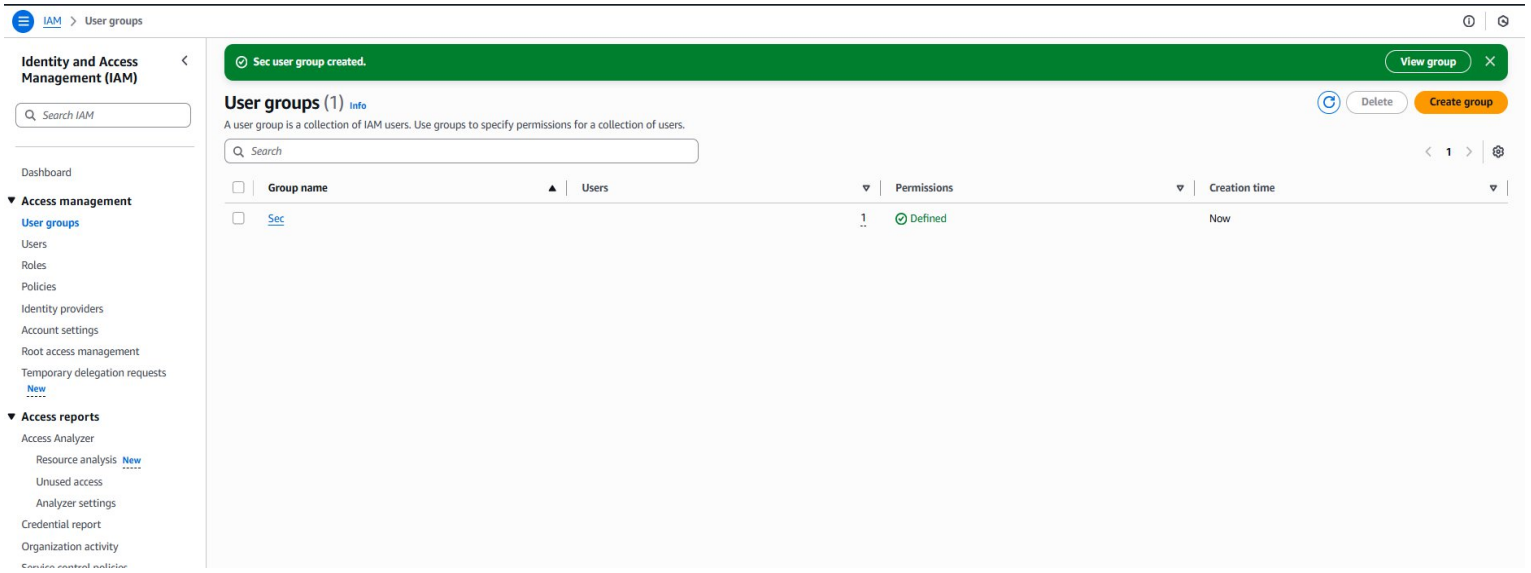
Step 4:- Enter Group Name:

Type a unique name for your group (for example, Developers, Admins, or ReadOnlyUsers).
For Example, here Administrators.

Step 5:- Attach Permissions Policies (Optional):
You can choose policies to attach to this group, such as:

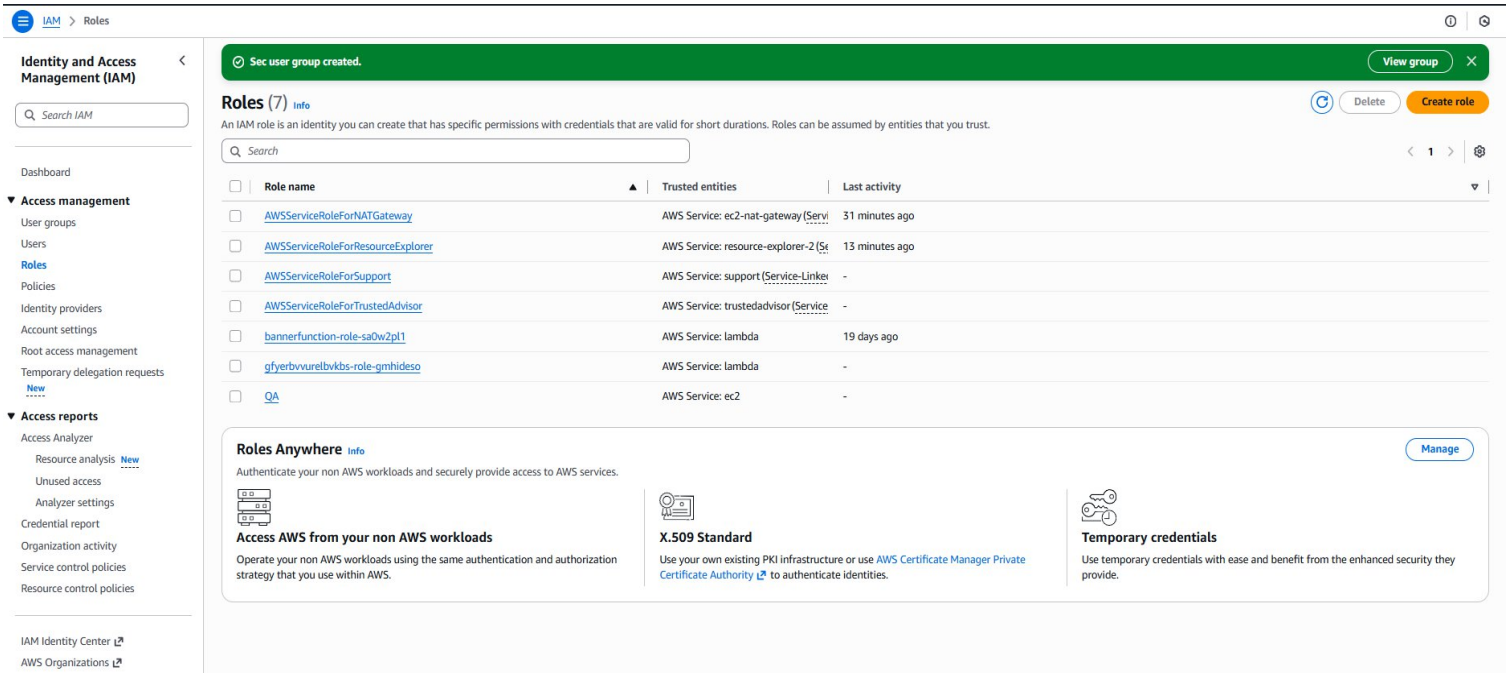
- AmazonS3FullAccess
- AmazonEC2ReadOnlyAccess
- AdministratorAccess

If you want to add permissions later, you can skip this step and click Next.



Practical:-8
Objective:-To create a security role in AWS IAM

Step 1:- Go to Roles Section:
In the left-hand navigation pane, click on Roles.

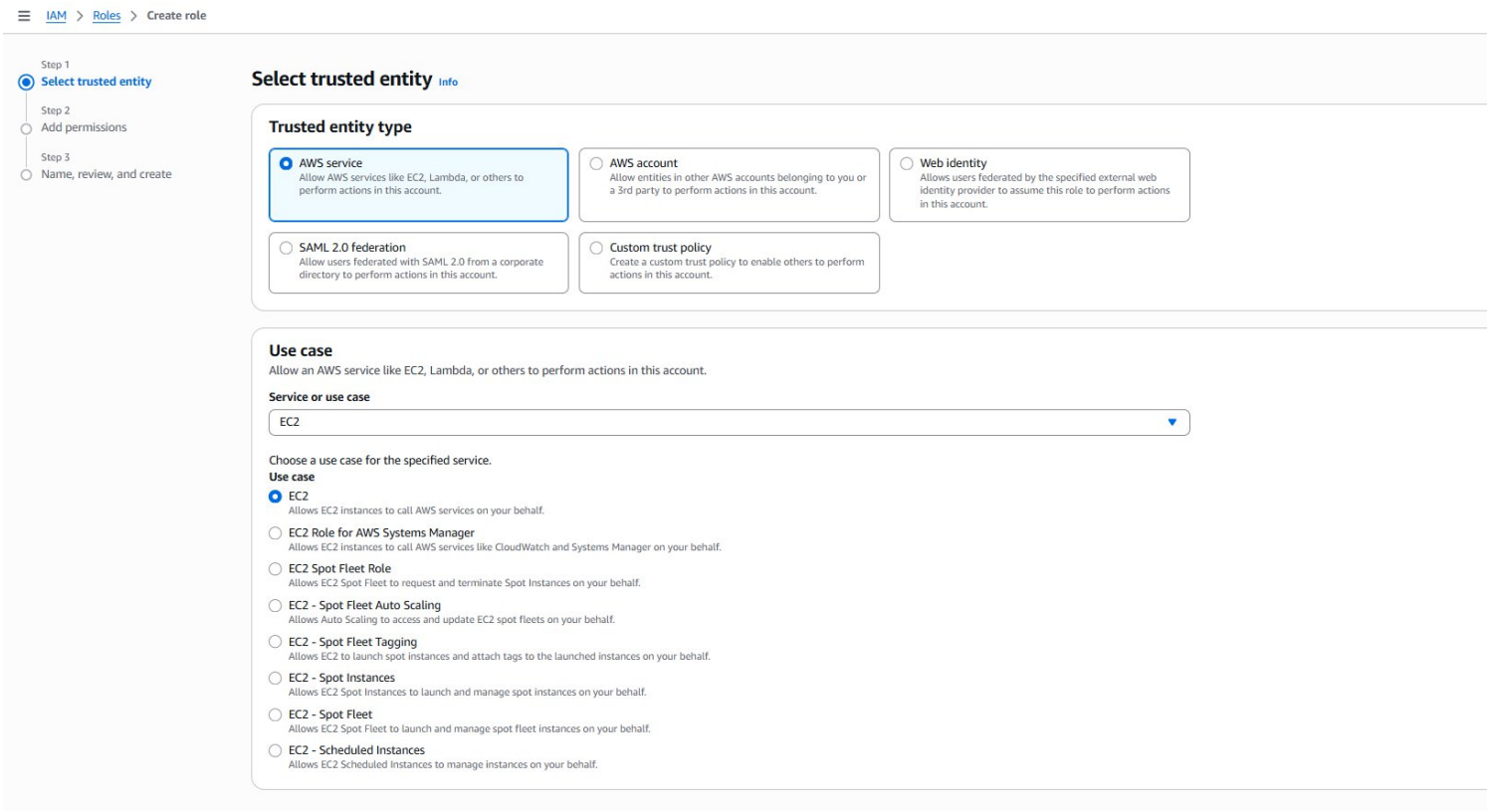


Step 2:- Click on “Create role”:
On the Roles page, click the “Create role” button to start the process.

Step 3:- Select Trusted Entity Type:
Choose who will use the role, such as:

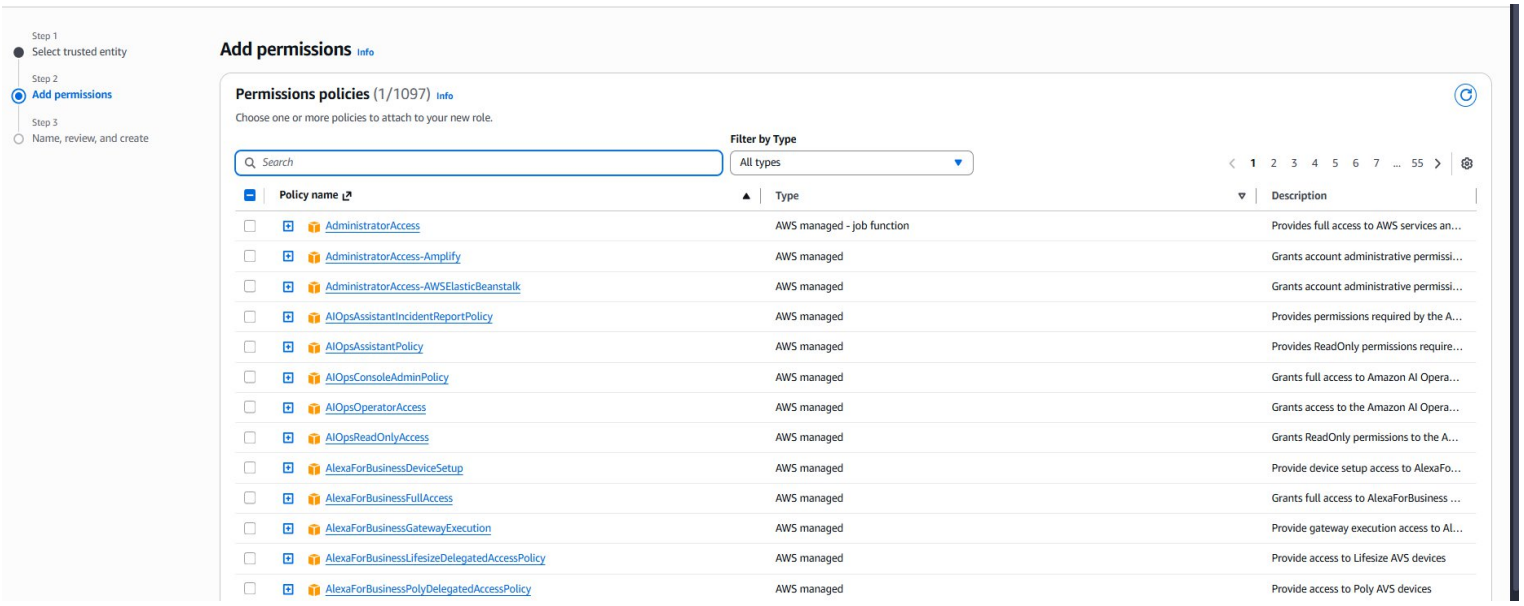
- AWS Service (e.g., EC2, Lambda)
- Another AWS Account
- Web Identity or SAML 2.0 Federation

Click Next after selecting the appropriate option.



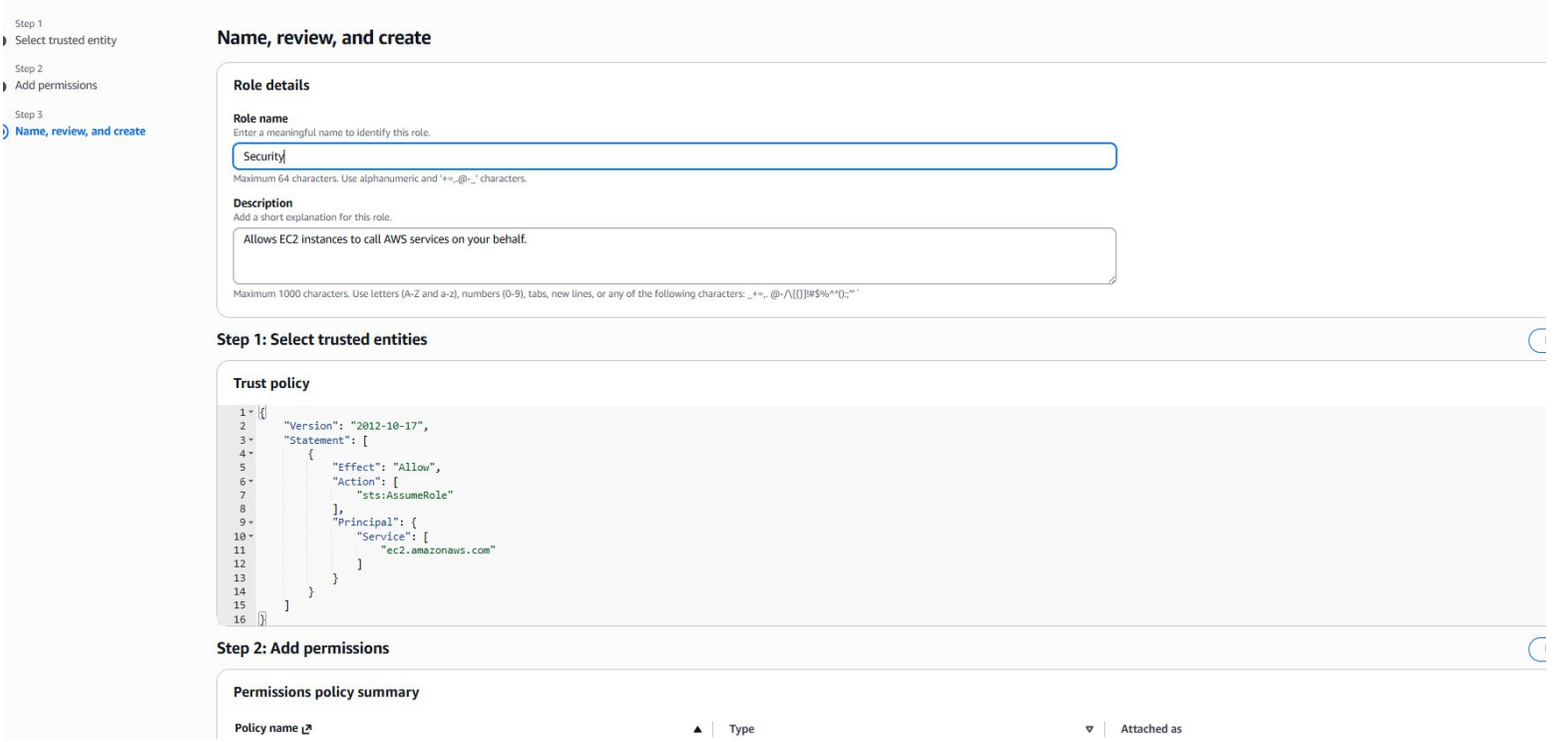
Step 4:-Attach Permissions Policies:

Select the permissions policies that define what actions the role can perform (for example, AmazonS3FullAccess or AmazonEC2FullAccess)



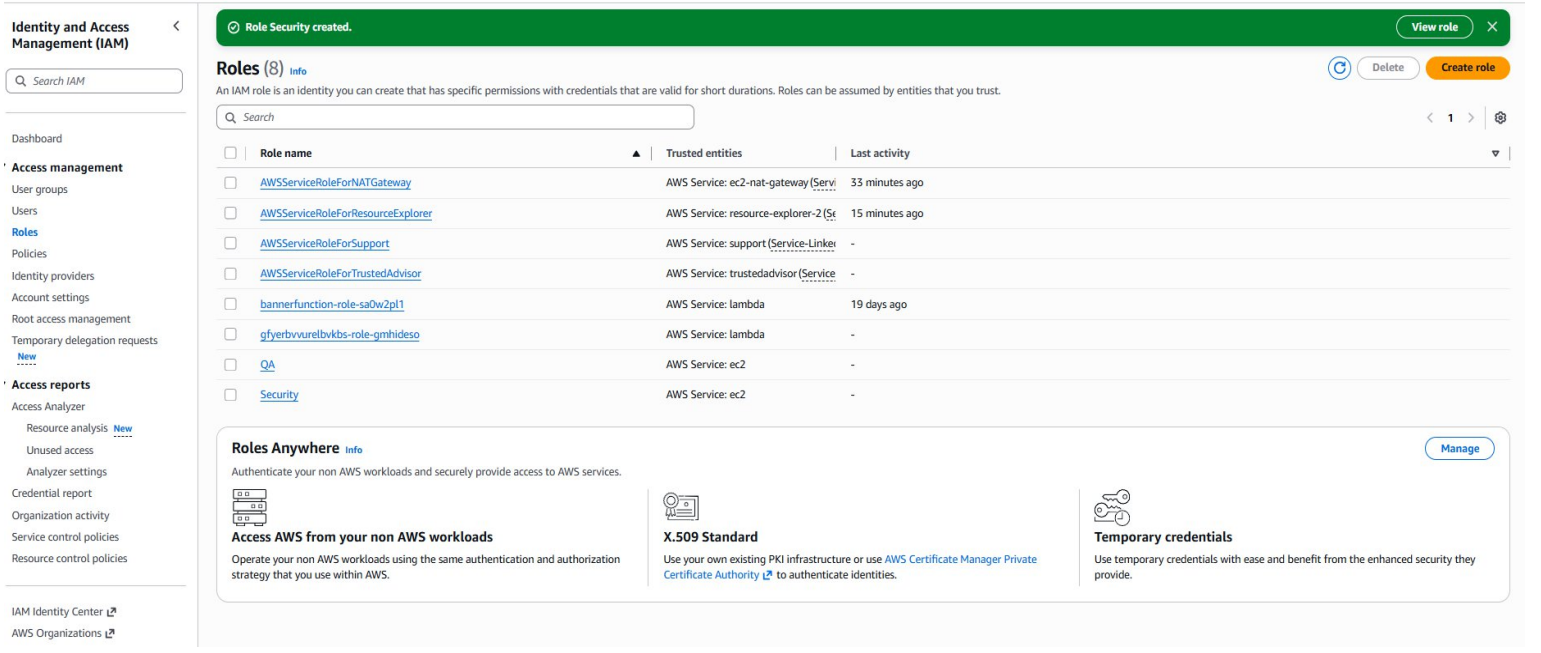
Step 5:- Name and Review the Role:

Enter a role name (for example, EC2SecurityRole or LambdaAccessRole) and review all selected settings.



Step 6:- Create the Role:

Click Create role to finish.

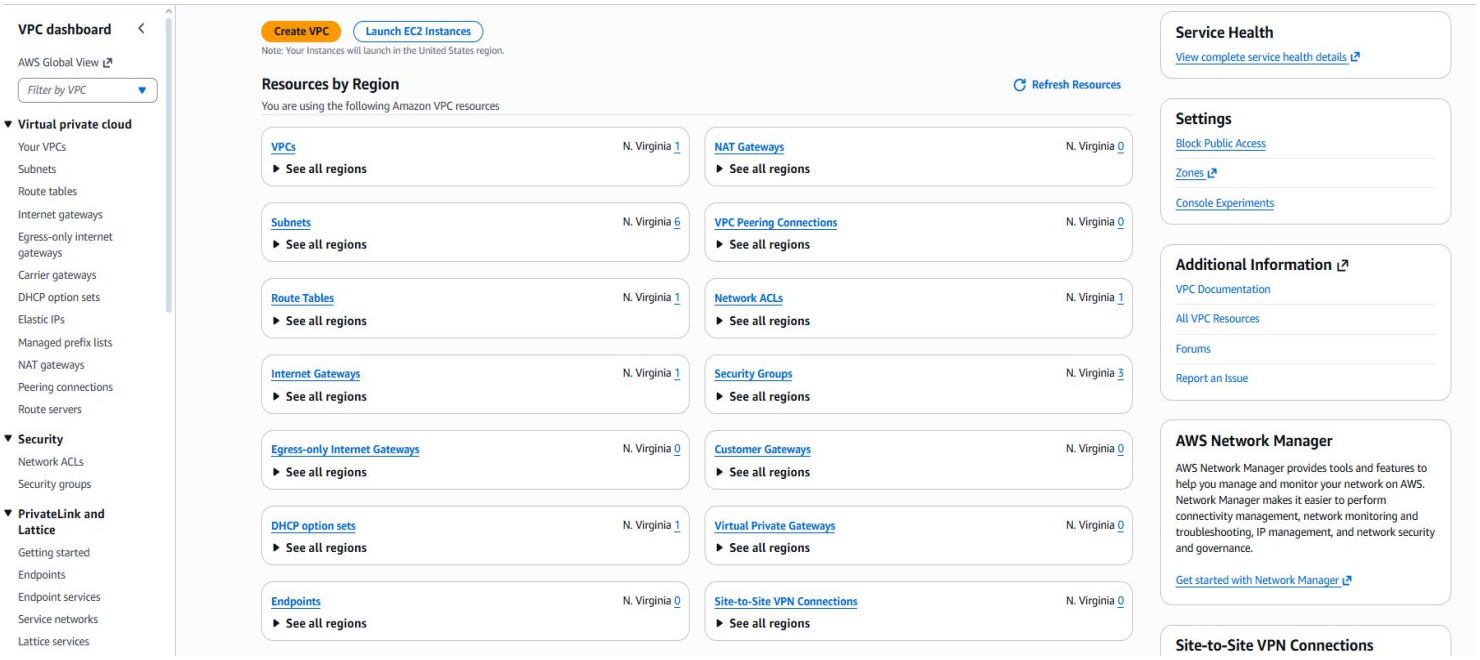


Practical :- 9

Objective:- To understand how to design and create a Virtual Private Cloud (VPC) in AWS.

Step 1. Open VPC Dashboard

- Sign in to AWS Console.
- Search VPC in the services search bar.
- Click VPC Dashboard.



Step 2. Start Creating a VPC

- On the left menu, select Your VPCs.
- Click Create VPC.

You will get two options:

1. VPC Only → Create VPC manually
2. VPC and more → Automatically create VPC with subnets, IGW, route tables, etc.

Choose VPC Only for full control

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

- (•) VPC only
- ( ) VPC and more

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

MYvpc

IPv4 CIDR block Info

- (•) IPv4 CIDR manual input
- ( ) IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

- (•) No IPv6 CIDR block
- ( ) IPAM-allocated IPv6 CIDR block
- ( ) Amazon-provided IPv6 CIDR block
- ( ) IPv6 CIDR owned by me

Tenancy Info

Default

VPC encryption control ($) - *new* Info
Monitor mode provides visibility into encryption status without blocking traffic. Enforce mode prevents unencrypted traffic. Additional charges apply

- (•) None
- ( ) Monitor mode — See which resources in your VPC are unencrypted but allow the creation of unencrypted resources.
- ( ) Enforce mode — Requires all resources, except exclusions, in your VPC to be encryption-capable and blocks creation of unencrypted resources.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	MYvpc	Remove tag

You successfully created vpc-0c3a476b1a18805a7 / MYvpc

vpc-0c3a476b1a18805a7 / MYvpc

Actions

Details Info

VPC ID vpc-0c3a476b1a18805a7	**State** Available	**Block Public Access** Off	**DNS hostnames** Disabled
DNS resolution Enabled	**Tenancy** default	**DHCP option set** dopt-0844d923f3579dd97	**Main route table** rtb-0d08dd78c975602e2
Main network ACL acl-036e6dd8f5333de01	**Default VPC** No	**IPv4 CIDR** 10.0.0.0/16	**IPv6 pool** –
IPv6 CIDR (Network border group) –	**Network Address Usage metrics** Disabled	**Route 53 Resolver DNS Firewall rule groups** –	**Owner ID** 018252911125
Encryption control ID –	**Encryption control mode** –		

Resource map | CIDRs | Flow logs | Tags | Integrations

Resource map Info

Show all details

VPC
Your AWS virtual network
MYvpc

Subnets (0)
Subnets within this VPC

Route tables (1)
Route network traffic to resources
rtb-0d08dd78c975602e2

Network Connections (0)
Connections to other networks

VPC dashboard
AWS Global View
Filter by VPC

- Virtual private cloud
  - Your VPCs
  - Subnets
  - Route tables
  - Internet gateways
  - Egress-only internet gateways
  - Carrier gateways
  - DHCP option sets
  - Elastic IPs
  - Managed prefix lists
  - NAT gateways
  - Peering connections
  - Route servers
- Security
  - Network ACLs
  - Security groups
- PrivateLink and Lattice

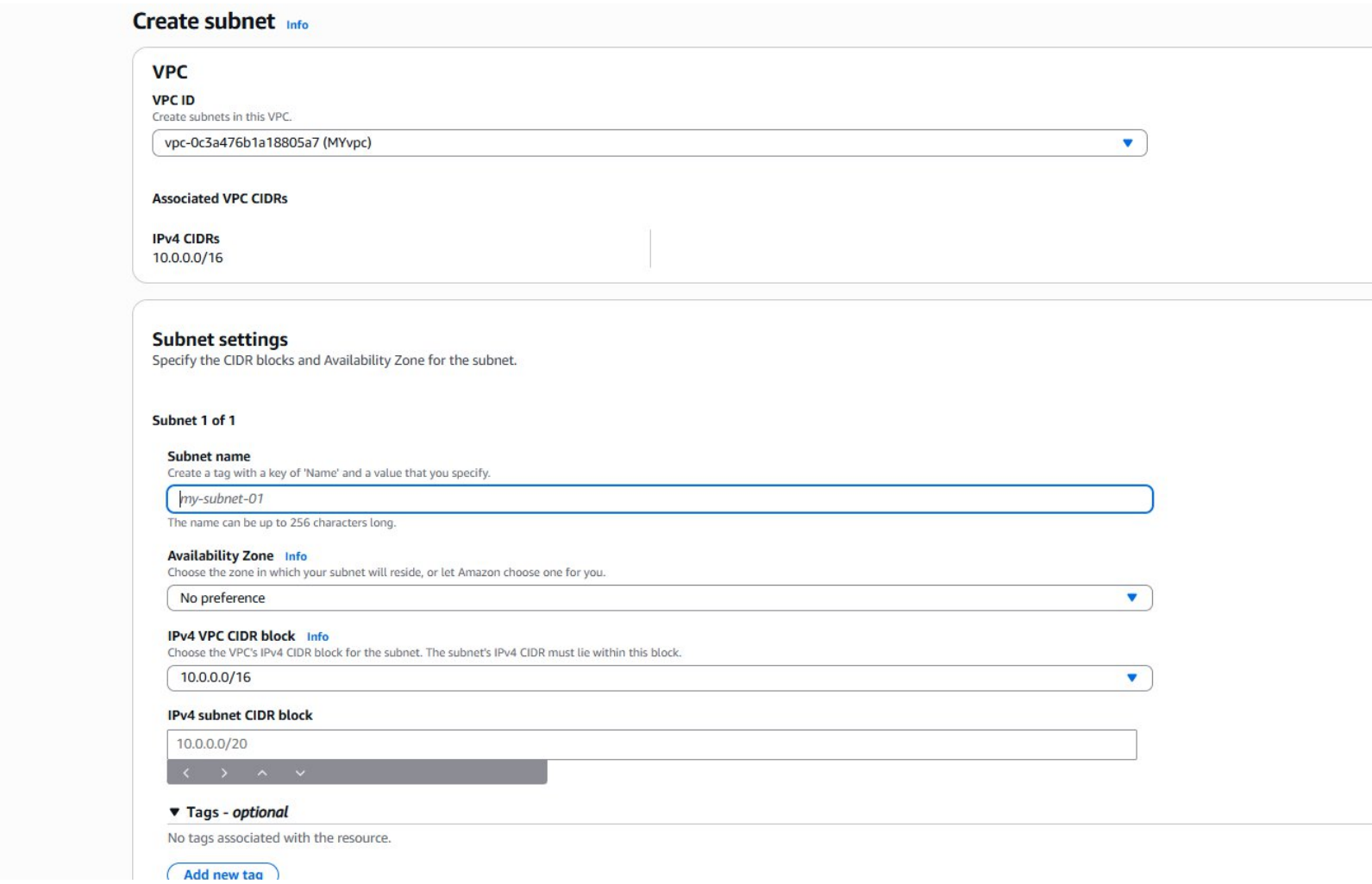
Subnets (6) Info

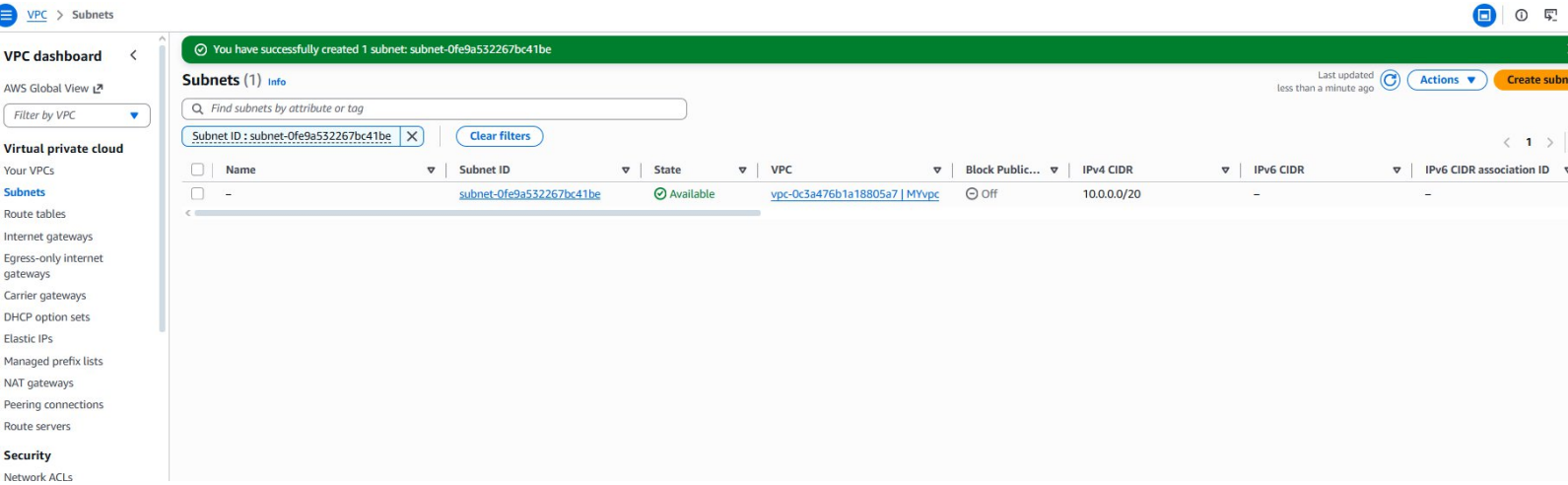
Last updated 4 minutes ago | Actions | Create subnet

Find subnets by attribute or tag

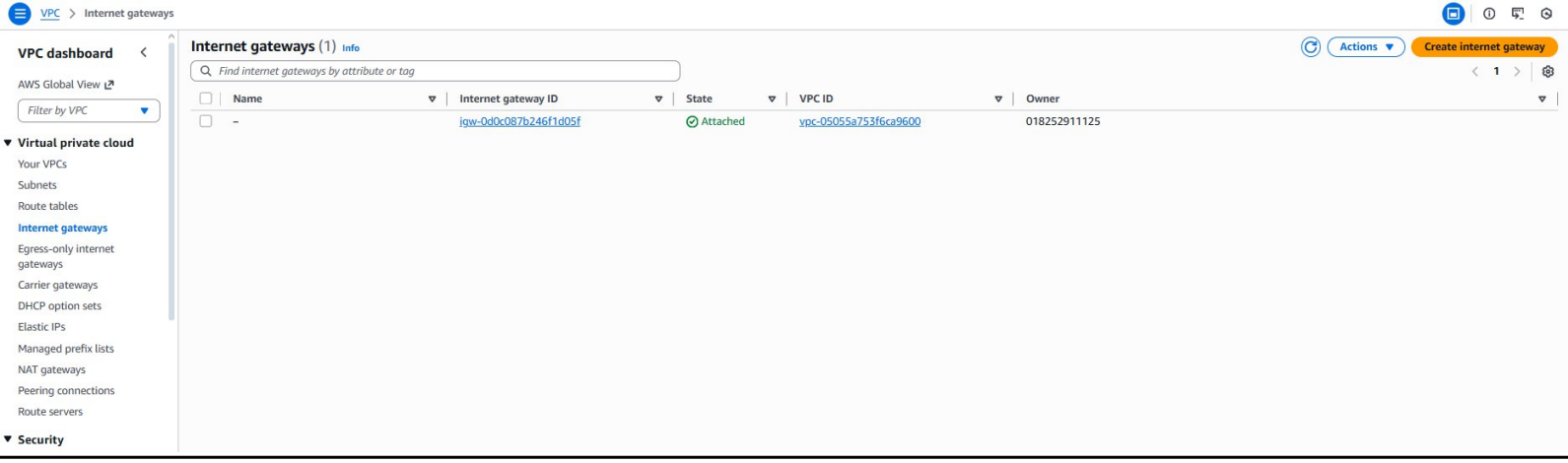
Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID
–	subnet-07b82a2bcf038f96d	Available	vpc-05055a753f6ca9600	Off	172.31.32.0/20	–	–
–	subnet-0c4564cfbc6f77de0	Available	vpc-05055a753f6ca9600	Off	172.31.0.0/20	–	–
–	subnet-0dca66f936b21f36f	Available	vpc-05055a753f6ca9600	Off	172.31.80.0/20	–	–
–	subnet-0cab952223f097fa6	Available	vpc-05055a753f6ca9600	Off	172.31.16.0/20	–	–
–	subnet-0f6049bff35706840	Available	vpc-05055a753f6ca9600	Off	172.31.48.0/20	–	–
–	subnet-04310741ab7640e80	Available	vpc-05055a753f6ca9600	Off	172.31.64.0/20	–	–

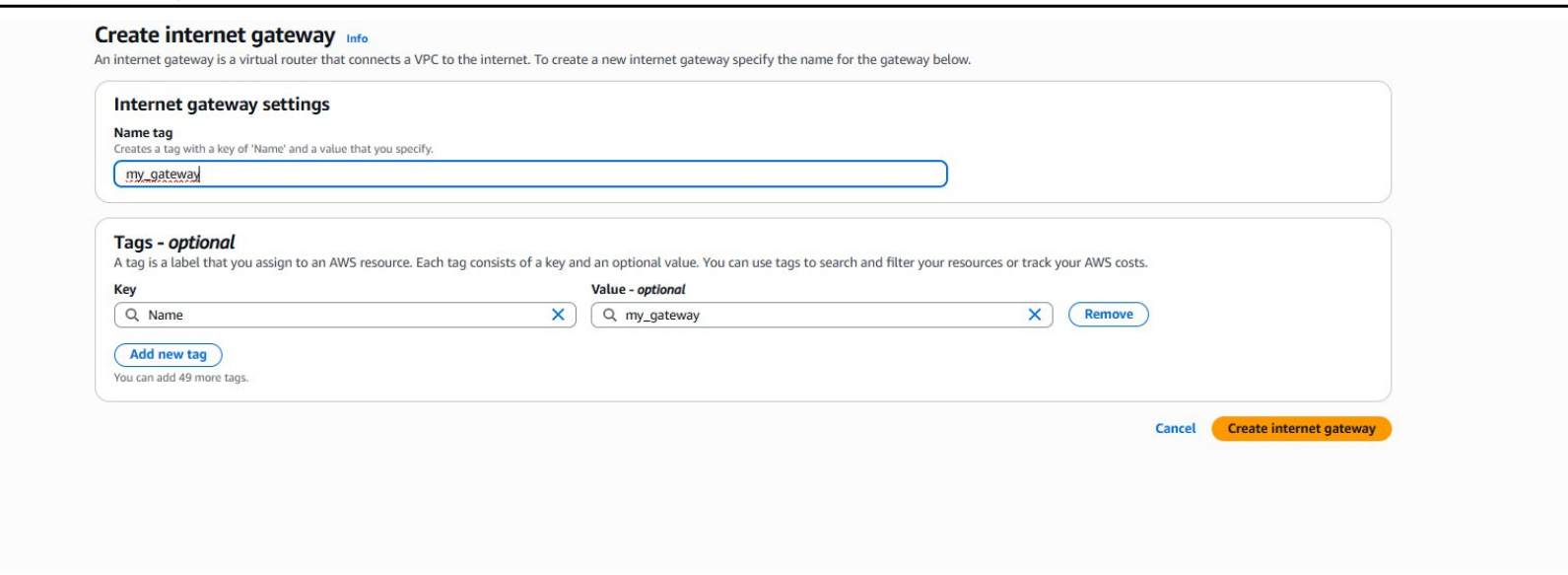
Step 3: Create Subnet

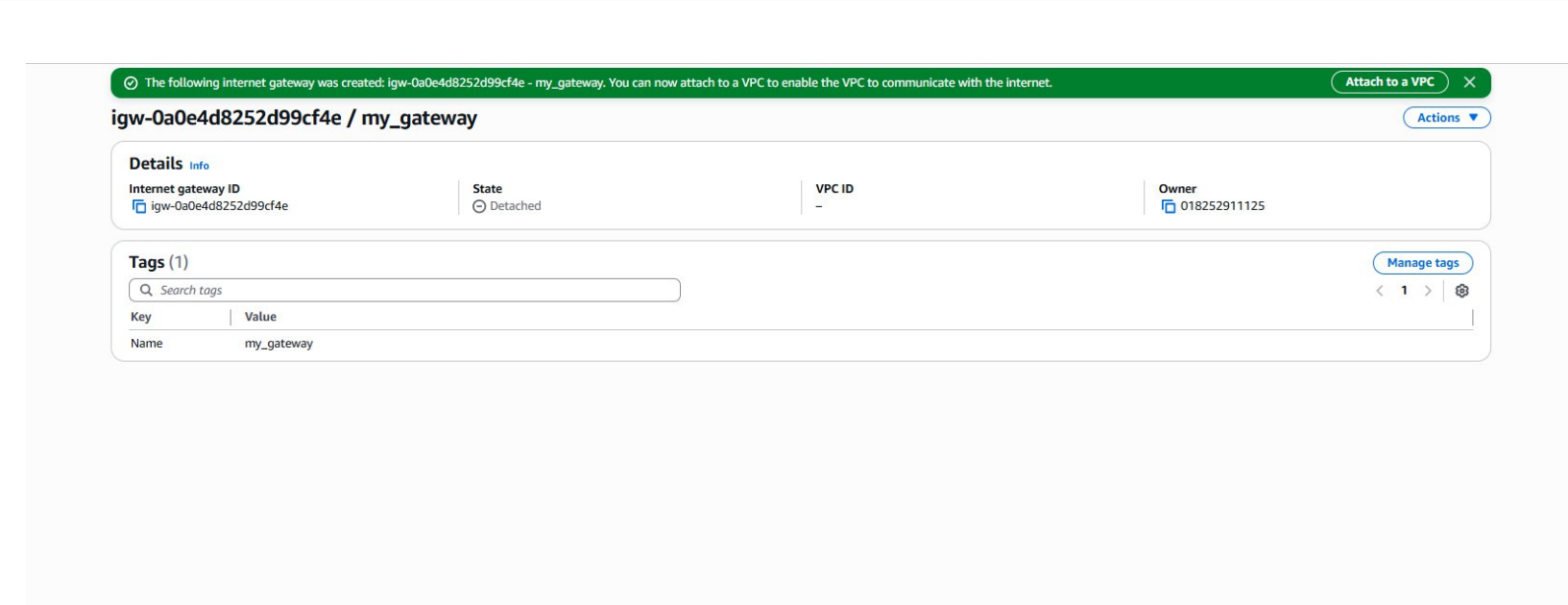


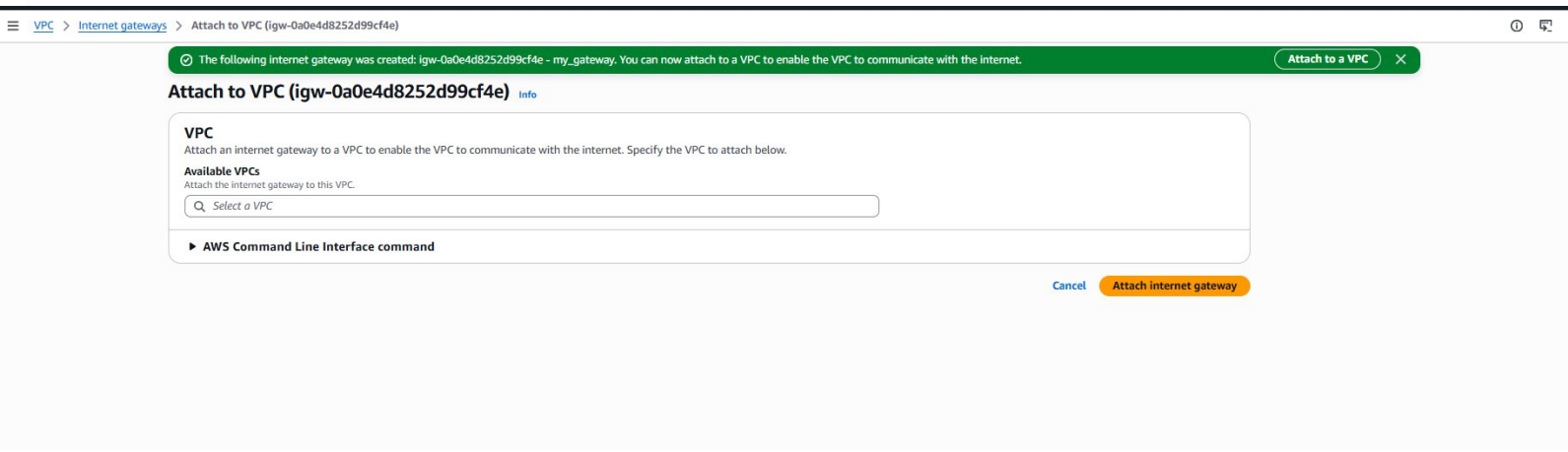


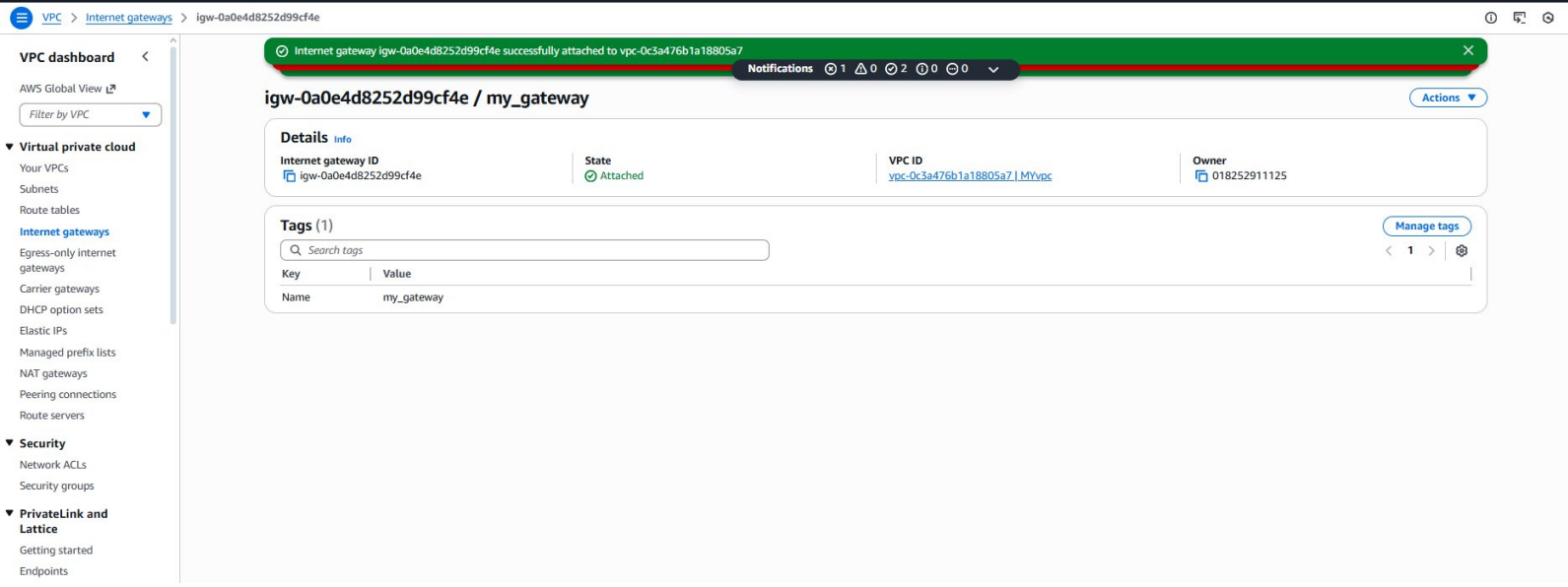
Step 4: Create Internet Gateways

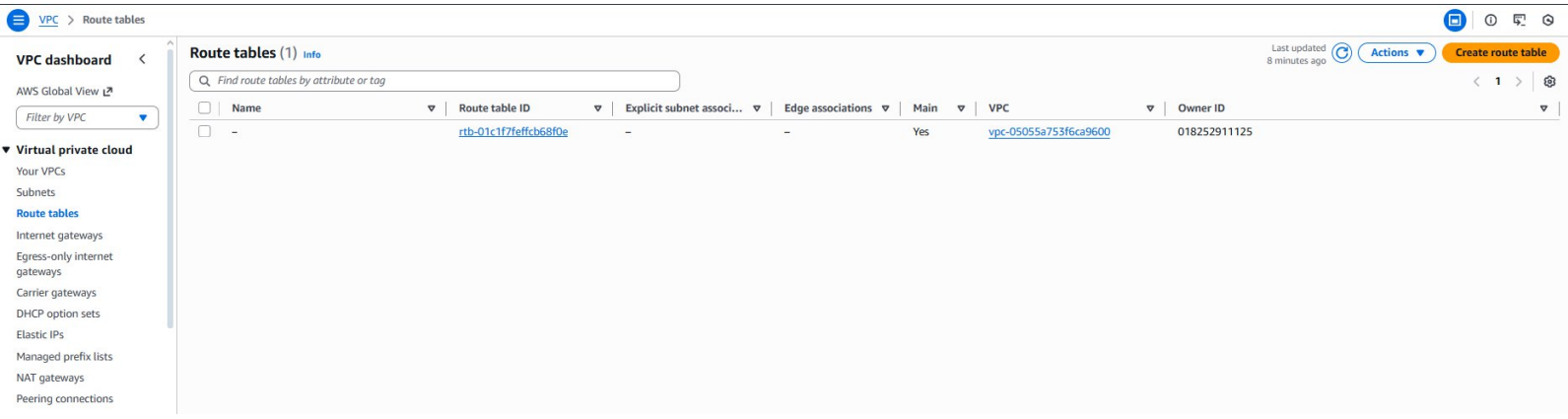

VPC > Internet gateways
VPC dashboard
AWS Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers
Security
Internet gateways (1) Info
Find internet gateways by attribute or tag
Actions
Create internet gateway
Name
Internet gateway ID
State
VPC ID
Owner
– igw-0d0c087b246f1d05f Attached vpc-05055a753f6ca9600 018252911125


Create internet gateway Info
An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.
Internet gateway settings
Name tag
Creates a tag with a key of 'Name' and a value that you specify.
my_gateway
Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Name
Value - optional
my_gateway
Remove
Add new tag
You can add 49 more tags.
Cancel
Create internet gateway

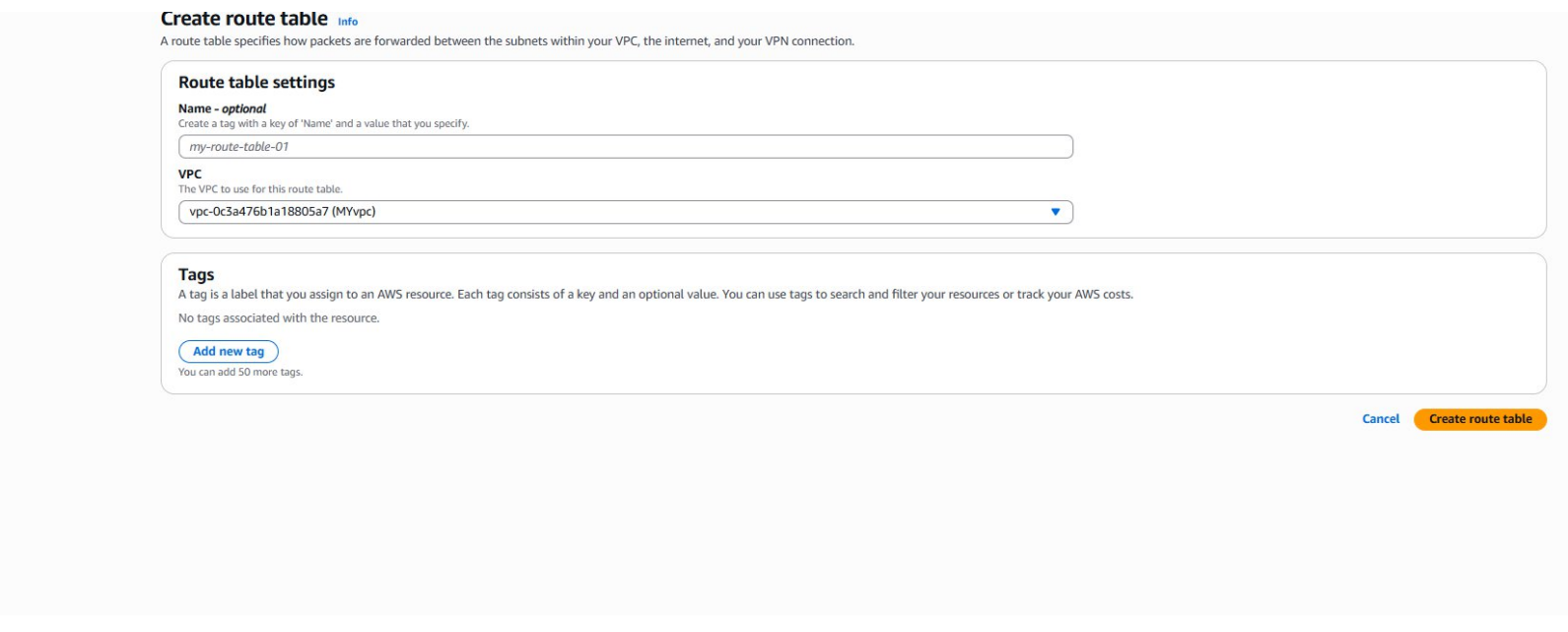

The following internet gateway was created: igw-0a0e4d8252d99cf4e - my_gateway. You can now attach to a VPC to enable the VPC to communicate with the internet.
Attach to a VPC
igw-0a0e4d8252d99cf4e / my_gateway
Actions
Details Info
Internet gateway ID
igw-0a0e4d8252d99cf4e
State
Detached
VPC ID
–
Owner
018252911125
Tags (1)
Manage tags
Search tags
Key
Value
Name
my_gateway

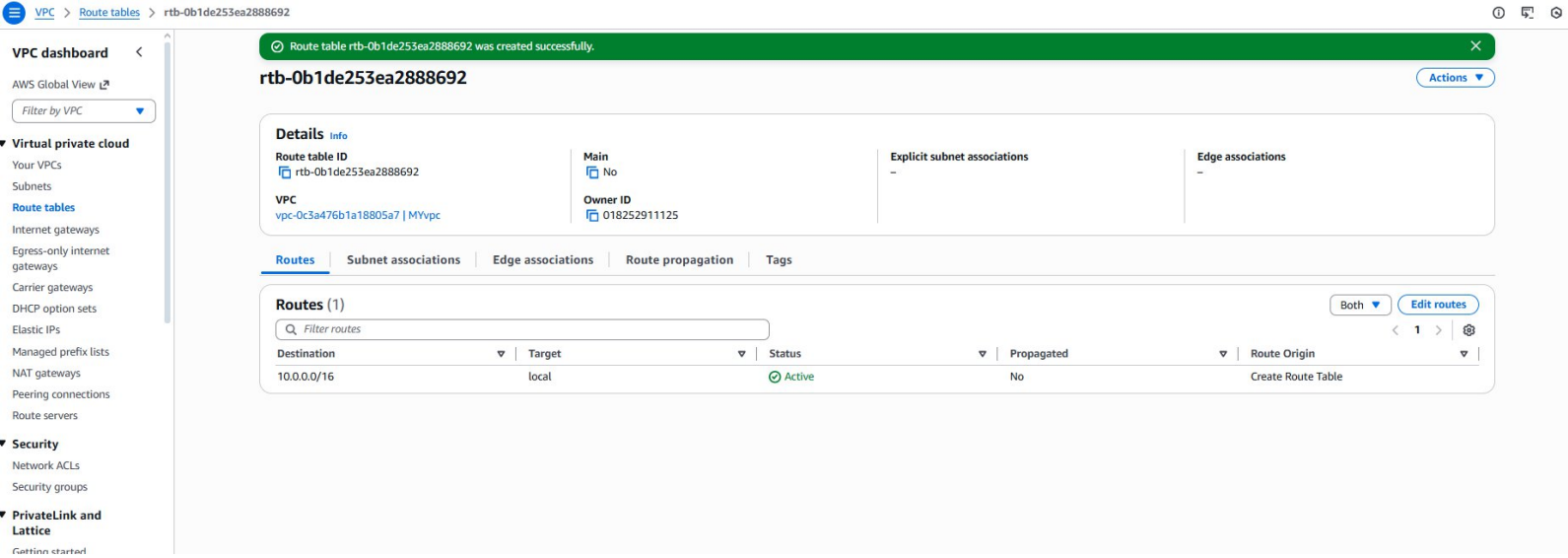

VPC > Internet gateways > Attach to VPC (igw-0a0e4d8252d99cf4e)
The following internet gateway was created: igw-0a0e4d8252d99cf4e - my_gateway. You can now attach to a VPC to enable the VPC to communicate with the internet.
Attach to a VPC
Attach to VPC (igw-0a0e4d8252d99cf4e) Info
VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.
Available VPCs
Attach the internet gateway to this VPC.
Select a VPC
AWS Command Line Interface command
Cancel
Attach internet gateway

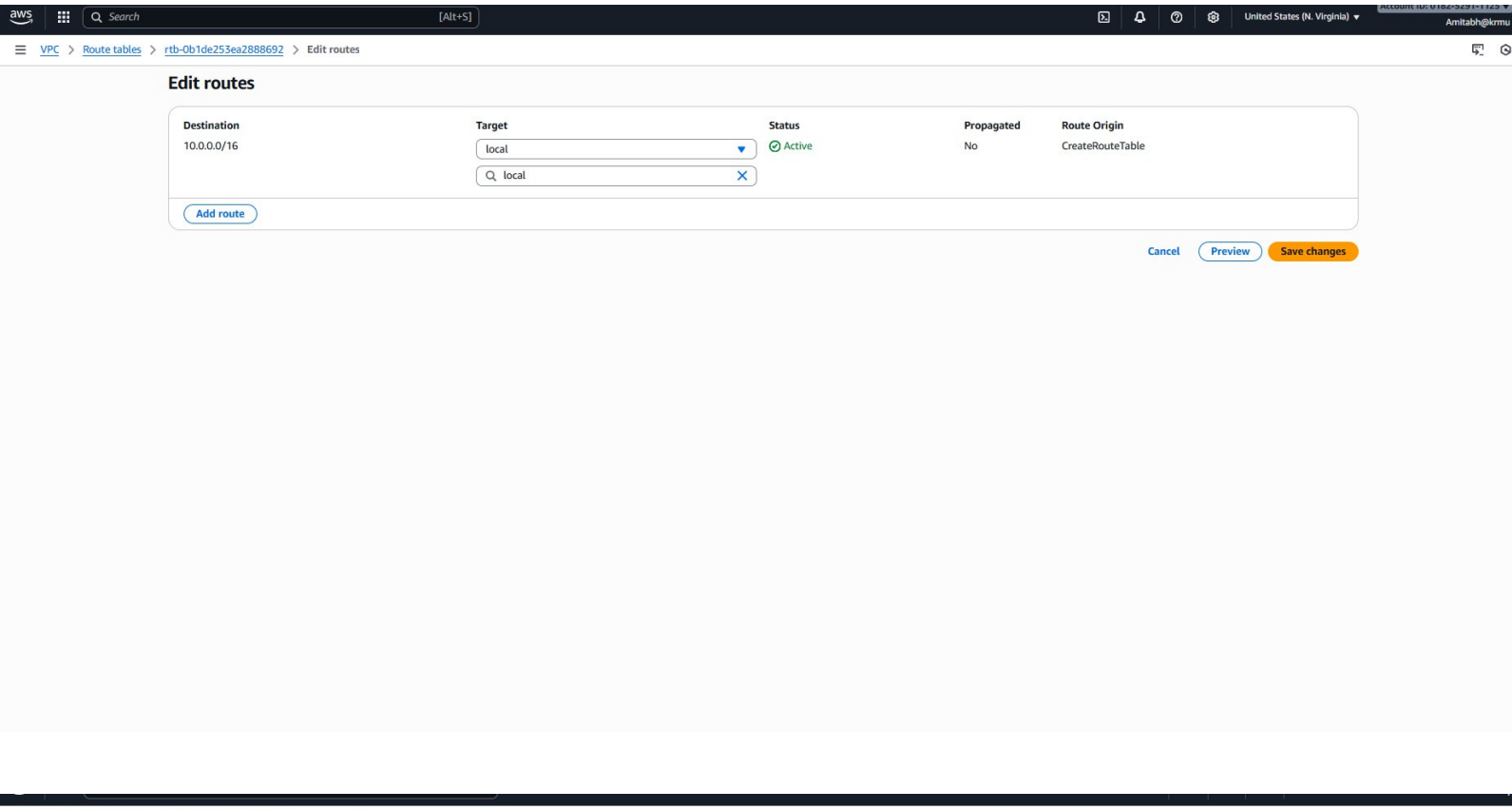


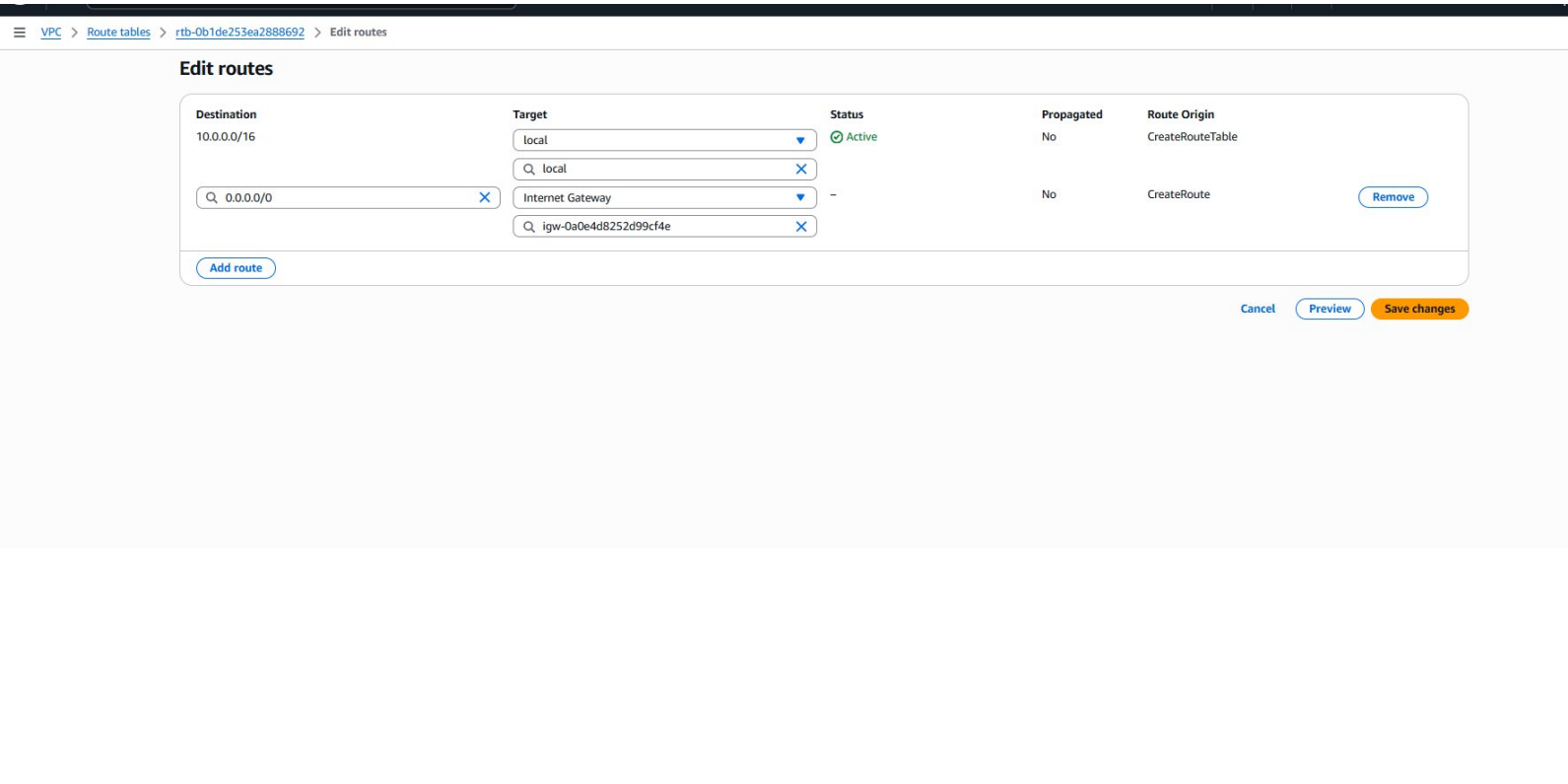


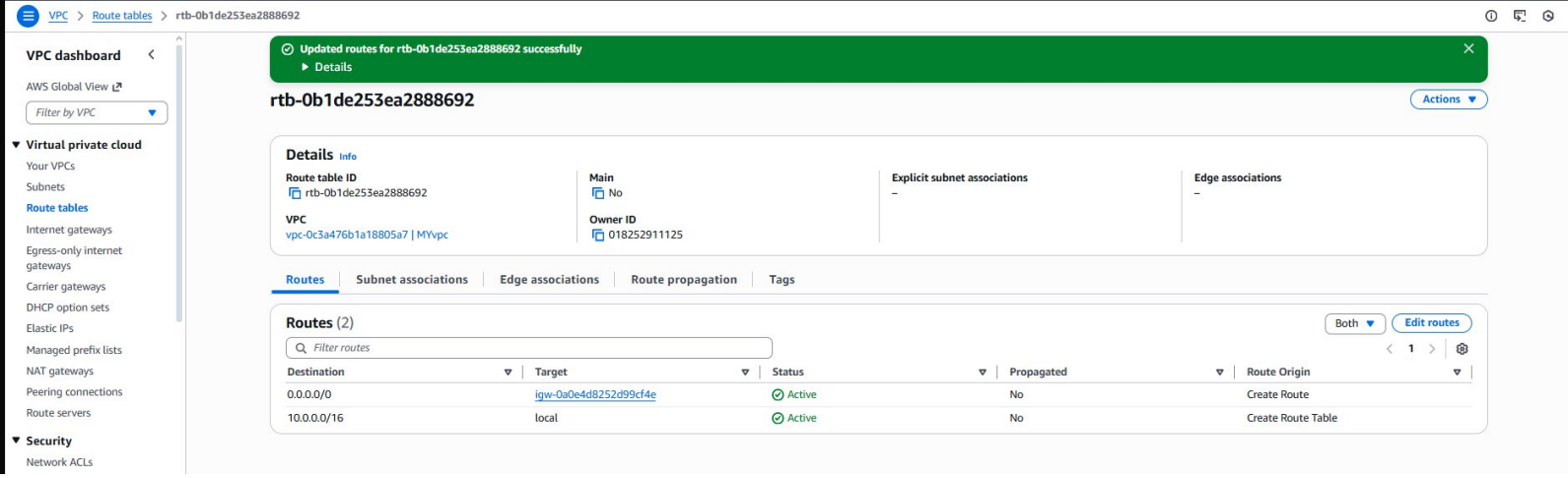
Step 5: Create Route Table



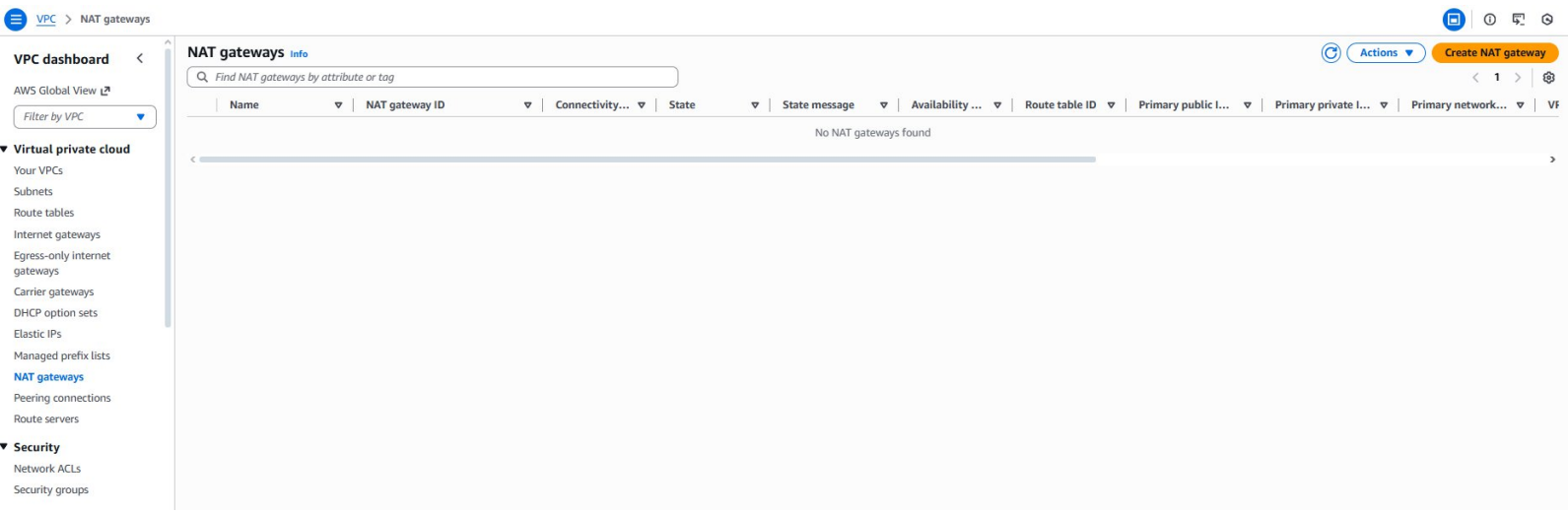

VPC > Route tables > rtb-0b1de253ea2888692
VPC dashboard
AWS Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers
Security
Network ACLs
Security groups
PrivateLink and Lattice
Getting started
Route table rtb-0b1de253ea2888692 was created successfully.
rtb-0b1de253ea2888692
Actions
Details Info
Route table ID
rtb-0b1de253ea2888692
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-0c3a476b1a18805a7 | MYvpc
Owner ID
018252911125
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (1)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
Route Origin
10.0.0.0/16
local
Active
No
Create Route Table

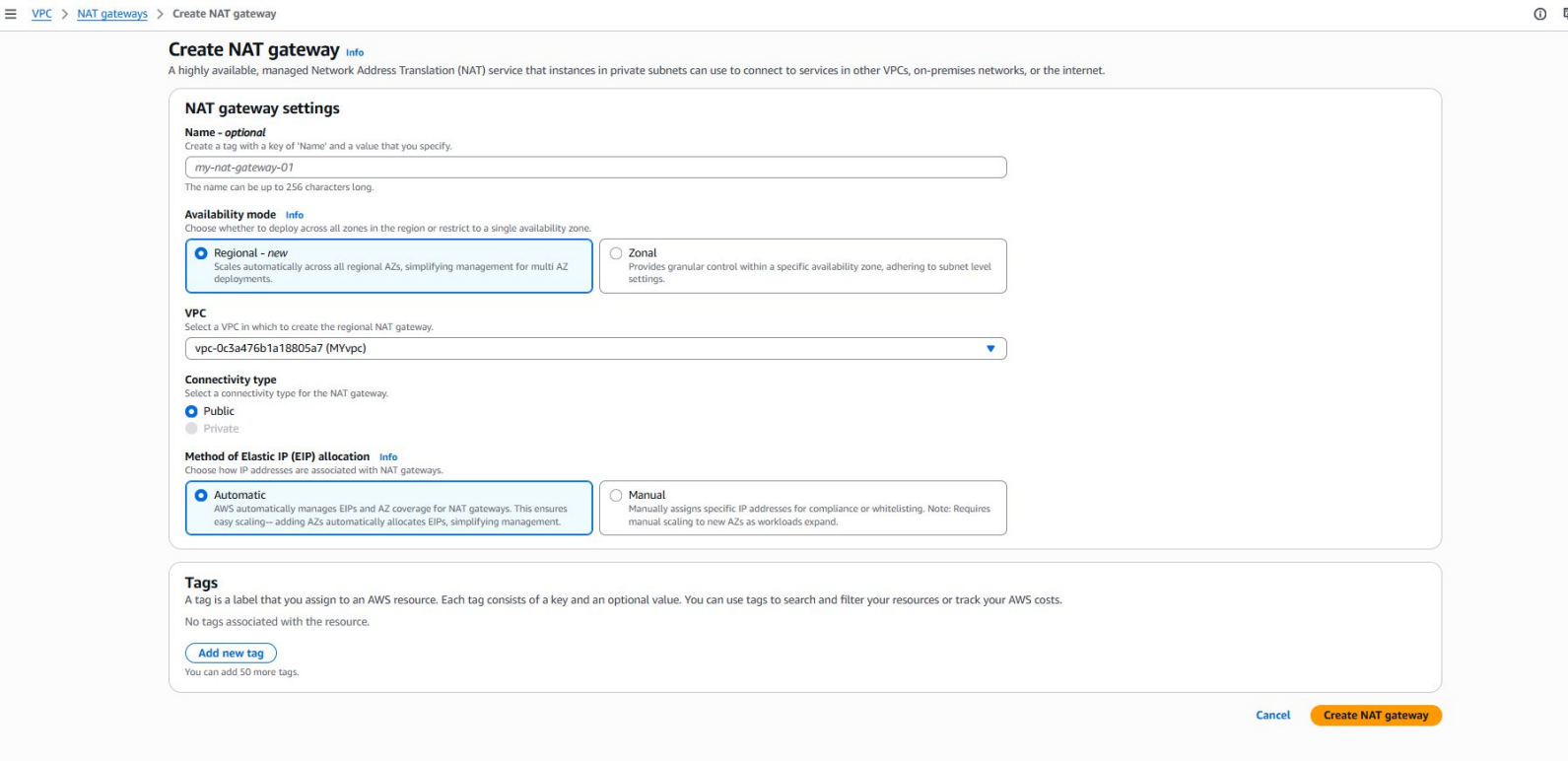

Search
[Alt+S]
United States (N. Virginia)
Amitabh@krmu
VPC > Route tables > rtb-0b1de253ea2888692 > Edit routes
Edit routes
Destination
Target
Status
Propagated
Route Origin
10.0.0.0/16
local
Active
No
CreateRouteTable
local
Add route
Cancel
Preview
Save changes


VPC > Route tables > rtb-0b1de253ea2888692 > Edit routes
Edit routes
Destination
Target
Status
Propagated
Route Origin
10.0.0.0/16
local
Active
No
CreateRouteTable
local
0.0.0.0/0
Internet Gateway
–
No
CreateRoute
Remove
igw-0a0e4d8252d99cf4e
Add route
Cancel
Preview
Save changes



Step 6: Create NAT Gateway





VPC dashboard
AWS Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers
Security
Network ACLs
Security groups
PrivateLink and Lattice
Getting started
Endpoints
Endpoint services
Service networks

NAT gateway nat-16a1555850760ed57 was created successfully.

nat-16a1555850760ed57

Actions

Details

NAT gateway ID
nat-16a1555850760ed57

NAT gateway ARN
arn:aws:ec2:us-east-1:018252911125:natgateway/nat-16a1555850760ed57

VPC
vpc-0c3a476b1a18805a7 / MYvpc

Availability mode
Regional

Connectivity type
Public

Method of EIP allocation
Automatic

State
Pending

Created
Saturday, November 29, 2025 at 01:09:40 GMT+5:30

State message Info
–

Deleted
–

IP addresses | Monitoring | Flow logs | Tags

Associated IP addresses

Edit IP address associations

Search

1

IP address	Status	Availability Zone	Allocation ID	Association ID

No associated IP adresses found. If this NAT gateway was recently created with the automatic allocation method, your IP addresses are still be being allocated. Click the refresh button to view them