K.R. MANGALAM UNIVERSITY
THE COMPLETE WORLD OF EDUCATION

11/28/2025

Cloud Security Fundamentals

Practical File ENCS-353

B. Tech CSE (Spec. Cyber Security)

Sankarshan 2301410027
K.R. MANGALAM UNIVERSITY

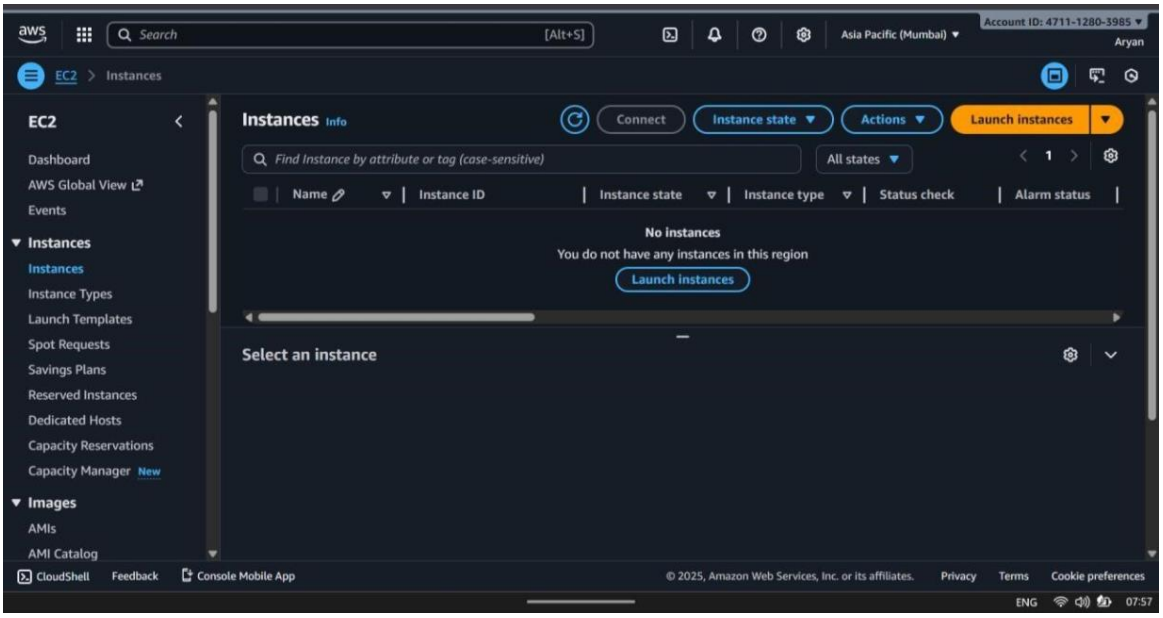
Index

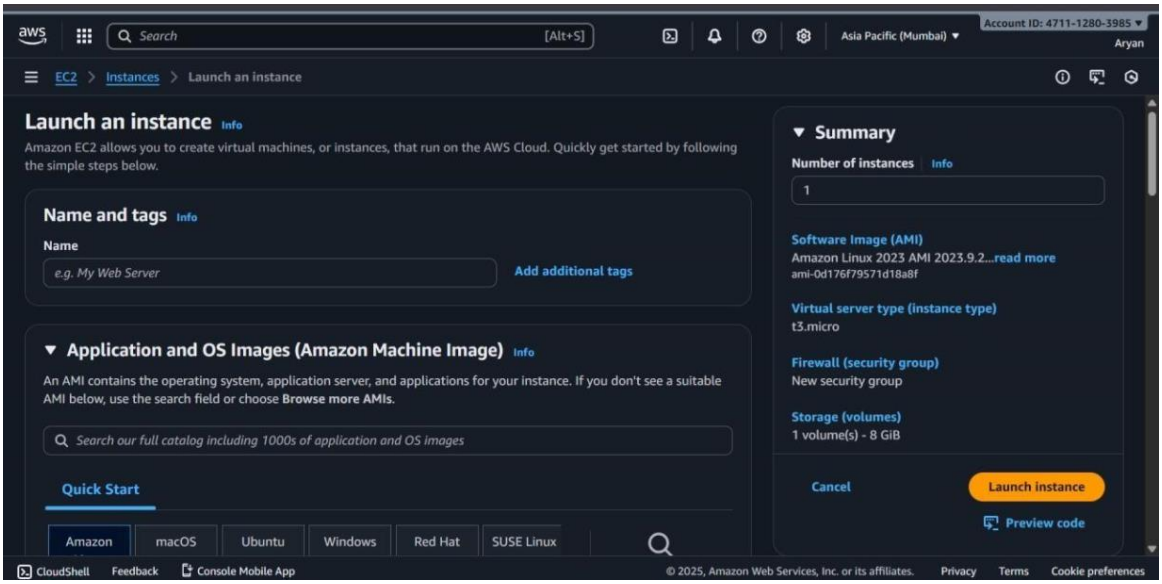
PRACTICAL-1

OBJECTIVE - TO CREATE EC2 INSTANCE

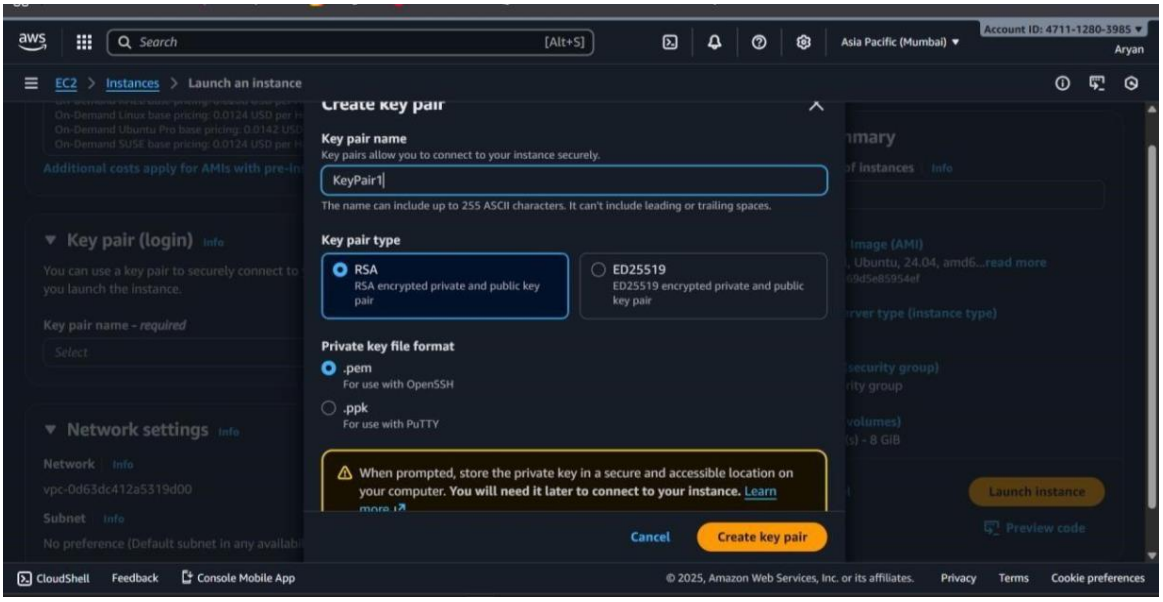
Steps to Create an EC2 Instance

1. **Login to AWS** ○ Go to AWS Management Console.
    - ○ Sign in with your credentials.
2. **Navigate to EC2** ○ In the search bar, type **EC2** and select it.
3. **Launch Instance** ○ Click **Instances → Launch Instance**.
    - ○ Give your instance a **name**.



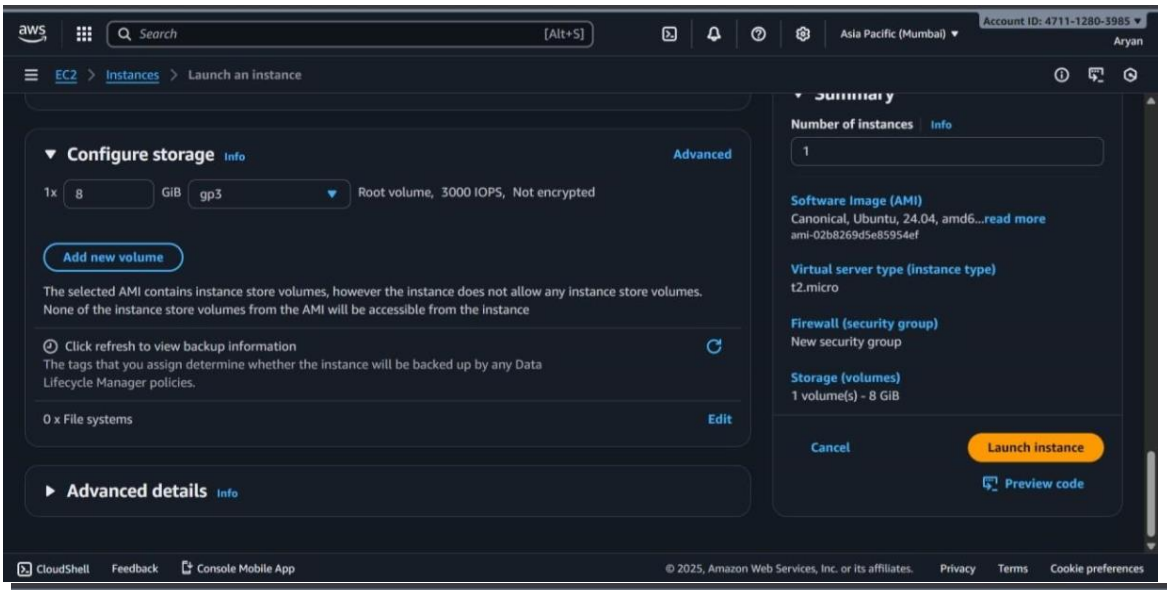


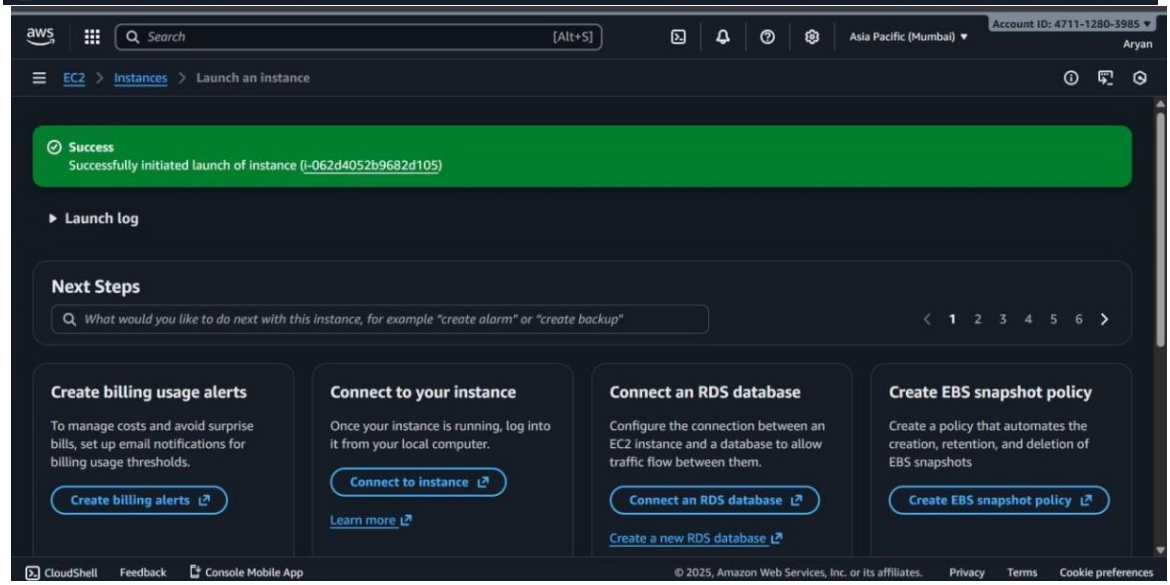
4. **Choose Amazon Machine Image (AMI)** ○ Select an OS image (e.g., Amazon Linux 2, Ubuntu, Windows). ○ For beginners, choose **Amazon Linux 2 (Free tier eligible)**.
    - I chose **Ubuntu**.
5. **Choose Instance Type** ○ Select **t2.micro** (free tier eligible).
6. **Configure Key Pair** ○ Create a new key pair (RSA) and download the **.pem file**.

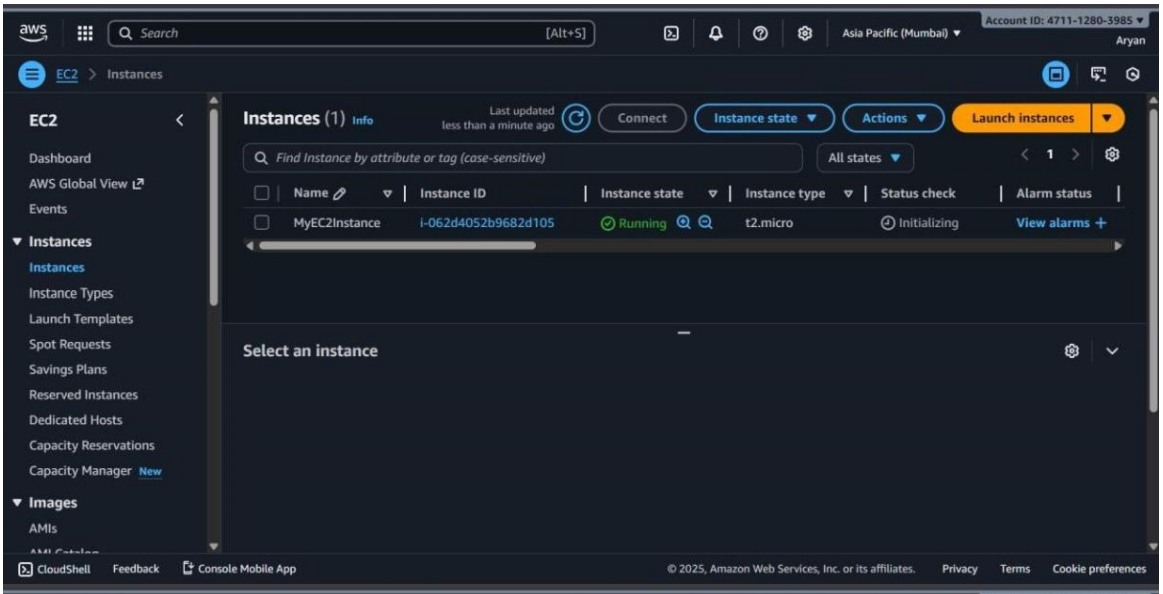


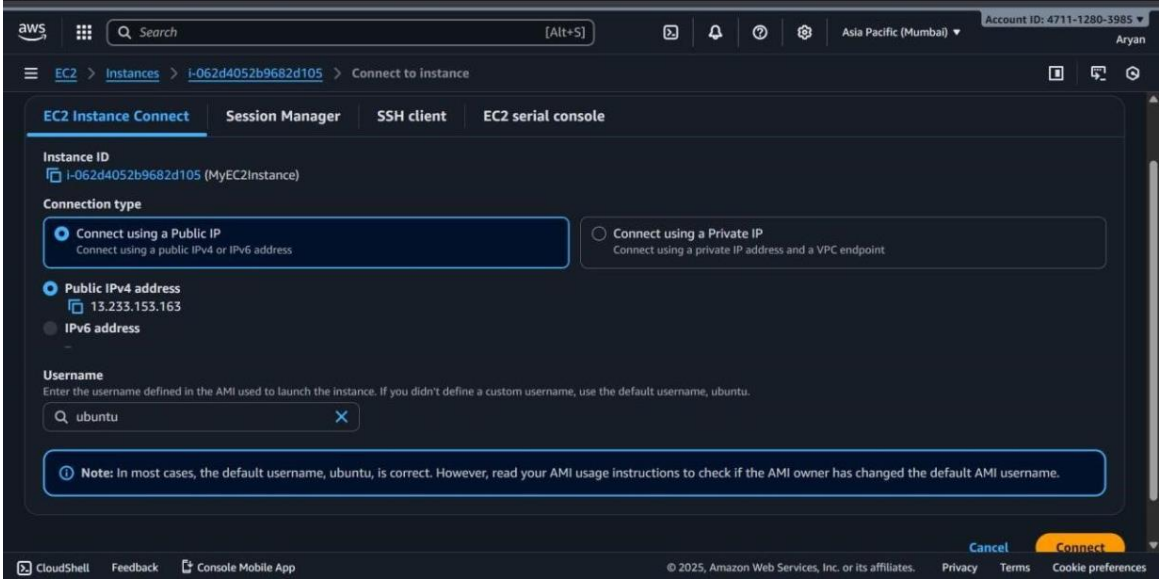
This will be used later to connect to your instance.

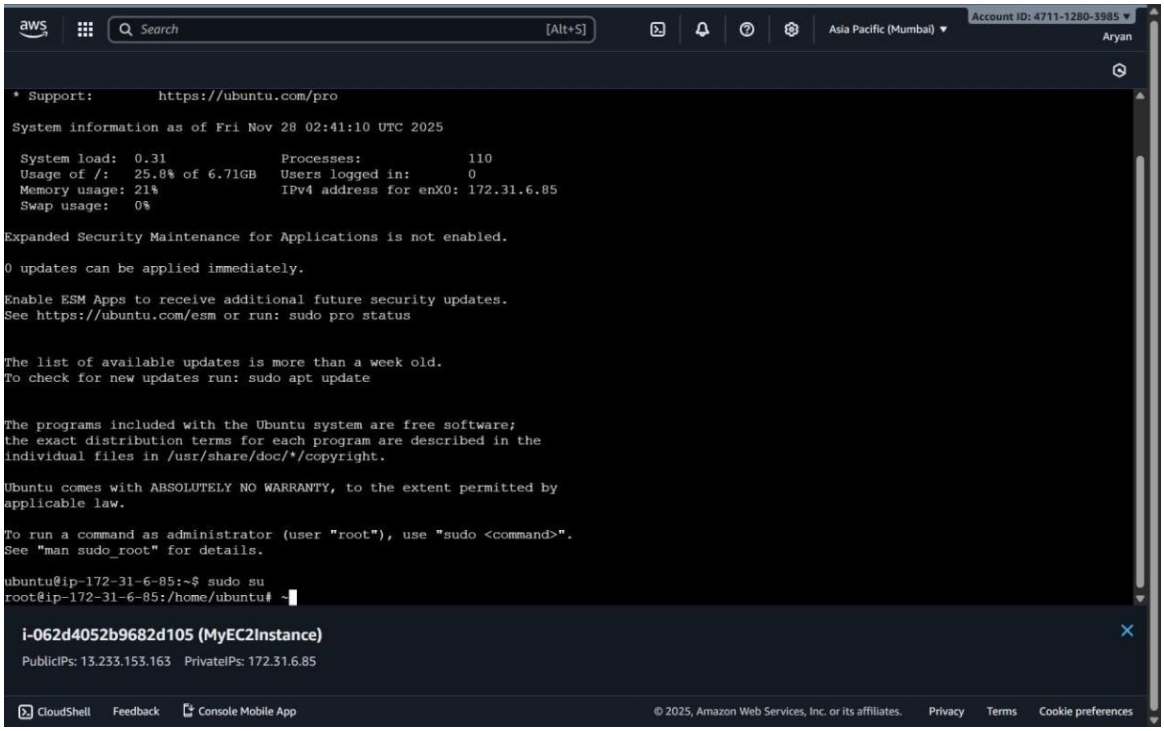
7. **Configure Network & Security** ○ Leave default **VPC and subnet** (unless you want custom networking).
    - ○ Under **Security group**, allow:
        - **SSH (port 22)** for Linux
        - **RDP (port 3389)** for Windows
        - **HTTP/HTTPS** if you're hosting a website.
8. **Configure Storage** ○ Default 8 GB is fine (increase if needed).
9. **Launch Instance** ○ Click **Launch Instance**.
    - ○ AWS will start your instance.






Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
EC2 > Instances
EC2
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
AMIs
Instances (1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
MyEC2Instance
i-062d4052b9682d105
Running
t2.micro
Initializing
View alarms
Select an instance
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

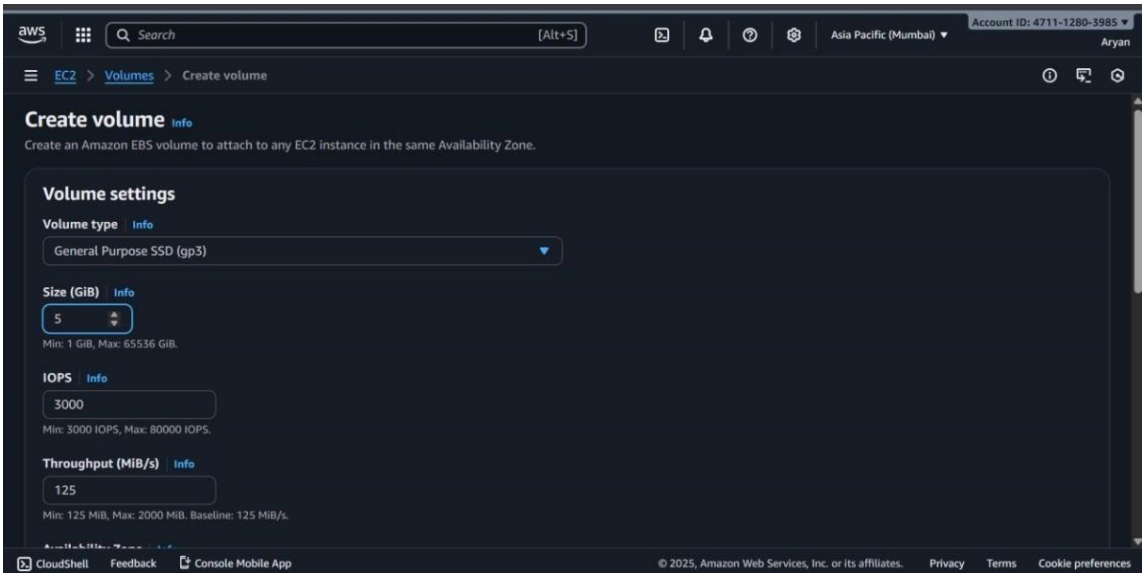

Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
EC2 > Instances > i-062d4052b9682d105 > Connect to instance
EC2 Instance Connect
Session Manager
SSH client
EC2 serial console
Instance ID
i-062d4052b9682d105 (MyEC2Instance)
Connection type
Connect using a Public IP
Connect using a public IPv4 or IPv6 address
Connect using a Private IP
Connect using a private IP address and a VPC endpoint
Public IPv4 address
13.233.153.163
IPv6 address
Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ubuntu.
ubuntu
Note: In most cases, the default username, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.
Cancel
Connect
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
* Support: https://ubuntu.com/pro
System information as of Fri Nov 28 02:41:10 UTC 2025
System load: 0.31
Usage of /: 25.8% of 6.71GB
Memory usage: 21%
Swap usage: 0%
Processes: 110
Users logged in: 0
IPv4 address for enX0: 172.31.6.85
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-172-31-6-85:~$ sudo su
root@ip-172-31-6-85:/home/ubuntu# ~
i-062d4052b9682d105 (MyEC2Instance)
PublicIPs: 13.233.153.163 PrivateIPs: 172.31.6.85
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

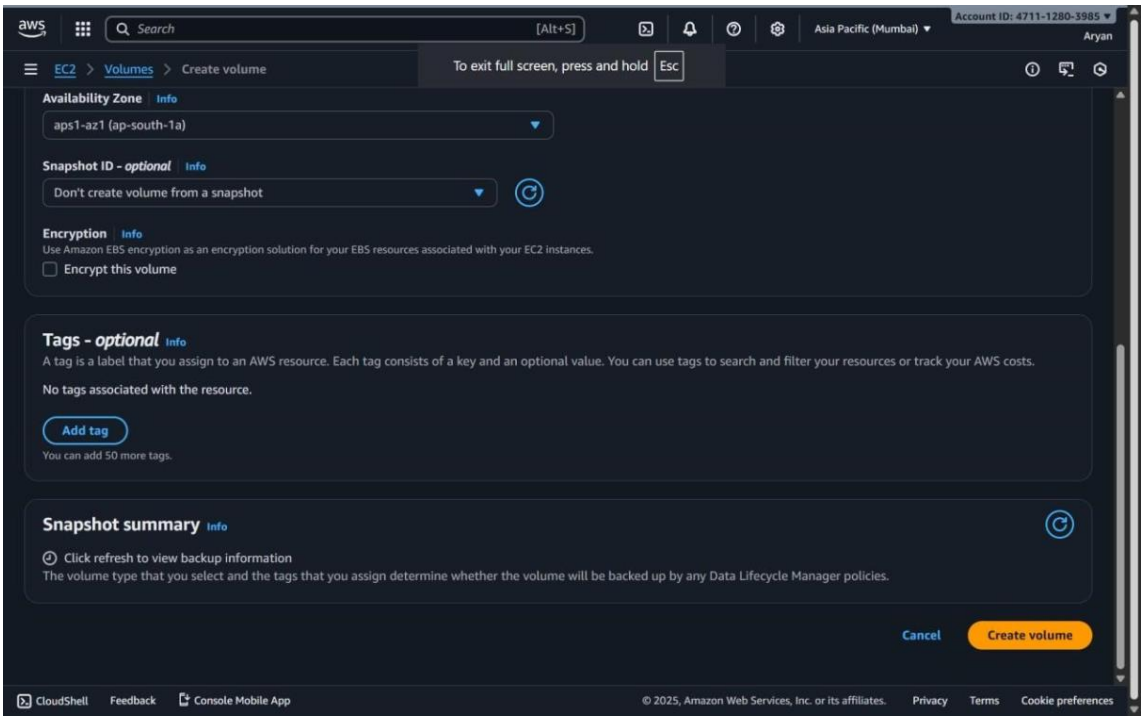
Practical:- 2

Objective:- Create Amazon Elastic Block Store (EBS) volumes in AWS

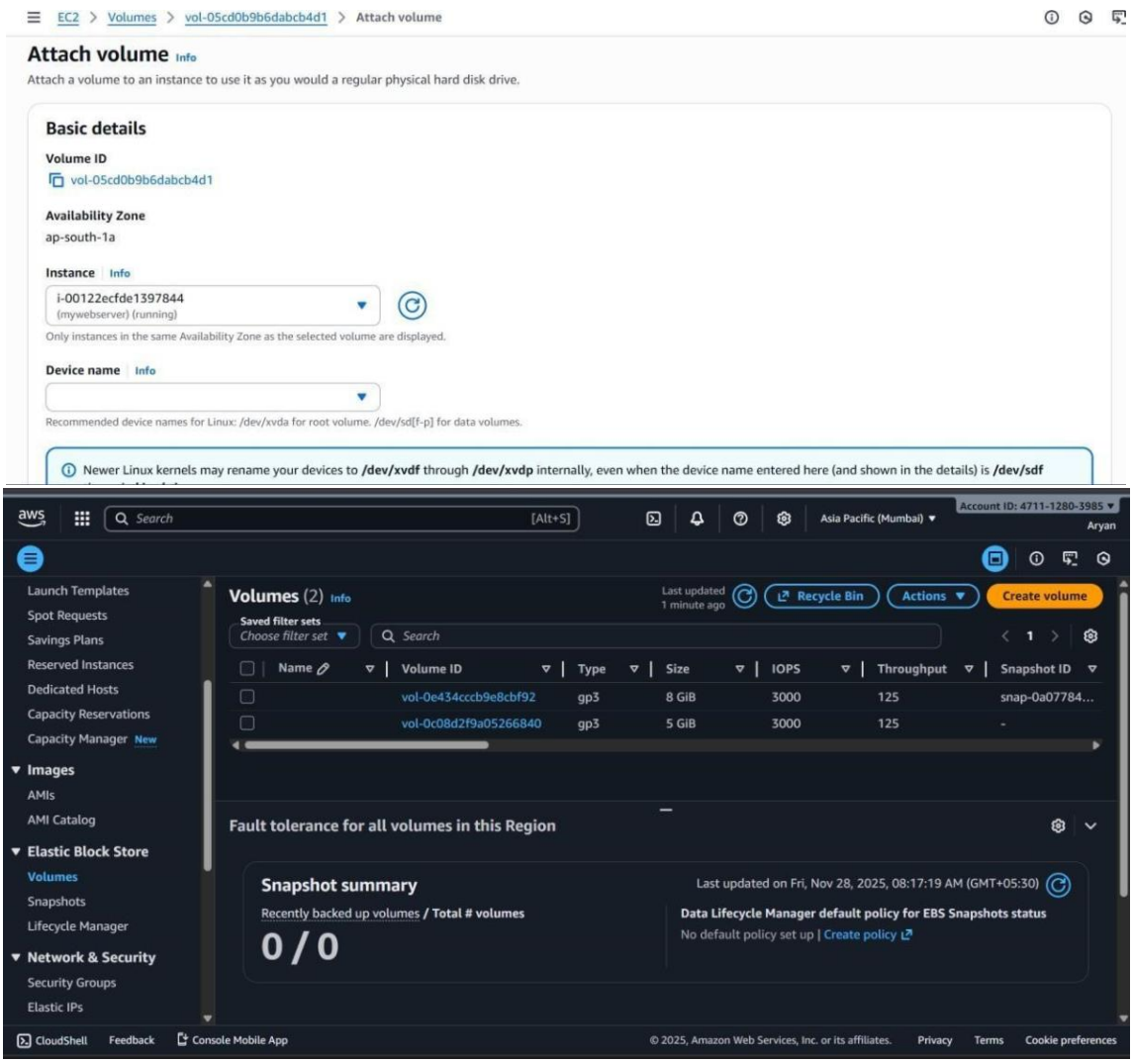
Step1:- Search EC2 and scroll to volumes.



Step 2:- Click on create volume and choose the settings as per the requirements. (here we have chosen gp3 -> size=5 and rest are default.



Step 3:- Keep the availability zone as the required zone in other activities too.



Newly created volume is marked by the red colour.

PRACTICAL -3

OBJECTIVE- CREATE AN S3 BUCKET IN AWS

1. Log in to AWS Management Console

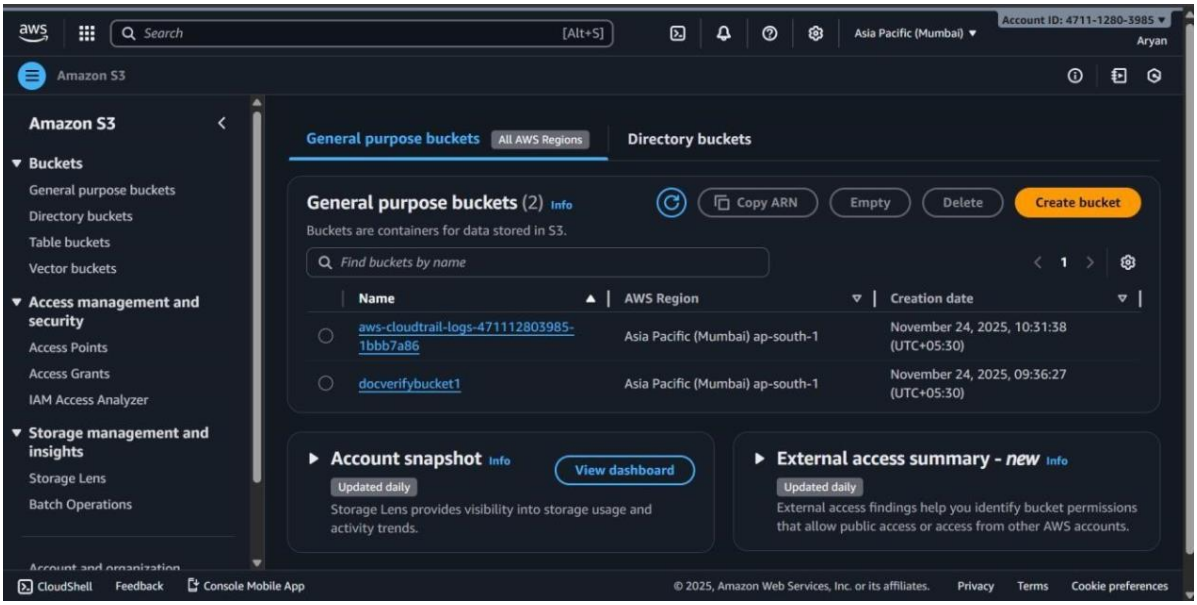
- Go to AWS Console.
- Sign in with your AWS account credentials.

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.

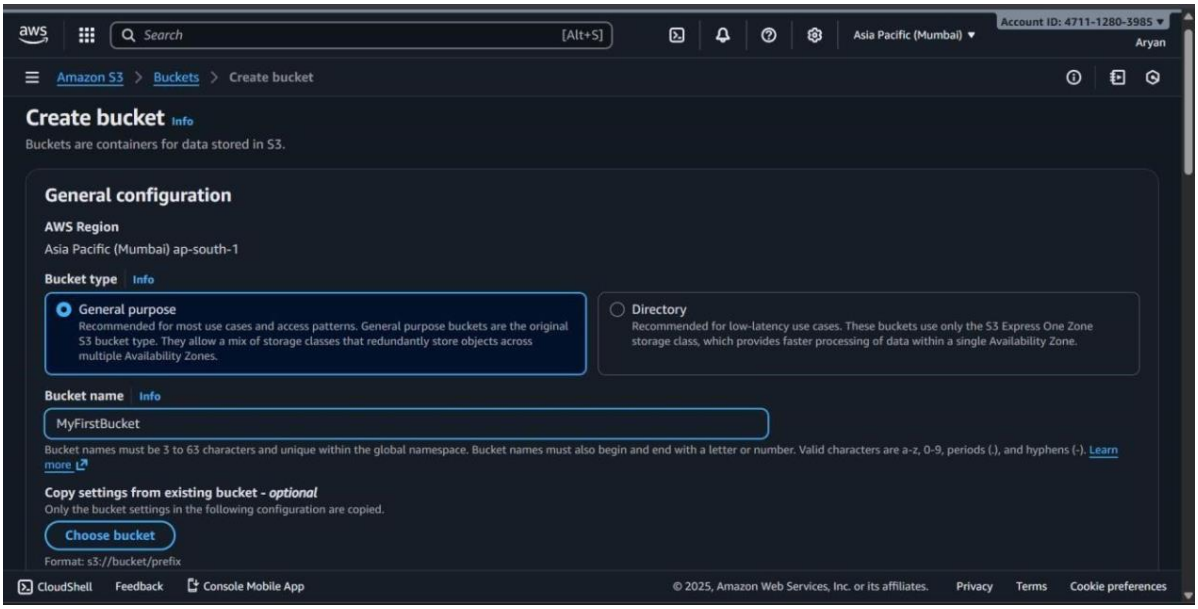


4. Configure Bucket Settings

- **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

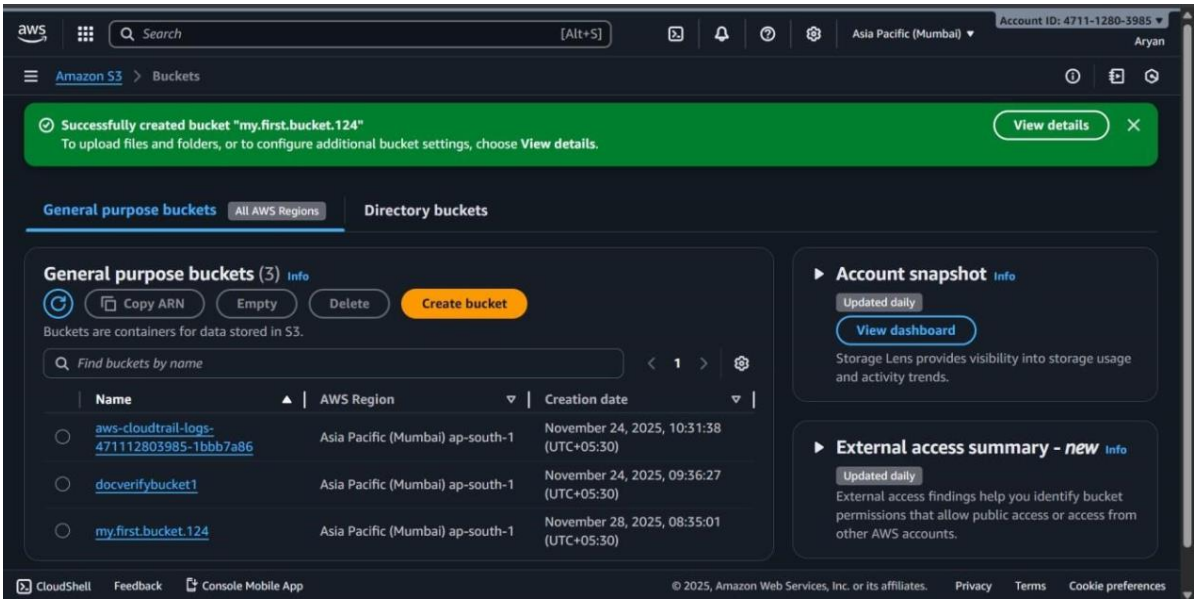
- **Object Ownership**:
  - Choose **ACLs disabled (recommended)** for most use cases.
- **Block Public Access**:
  - By default, all public access is blocked (recommended for private buckets).
  - If you need a public bucket (for hosting static websites), uncheck the option and acknowledge the warning.

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.

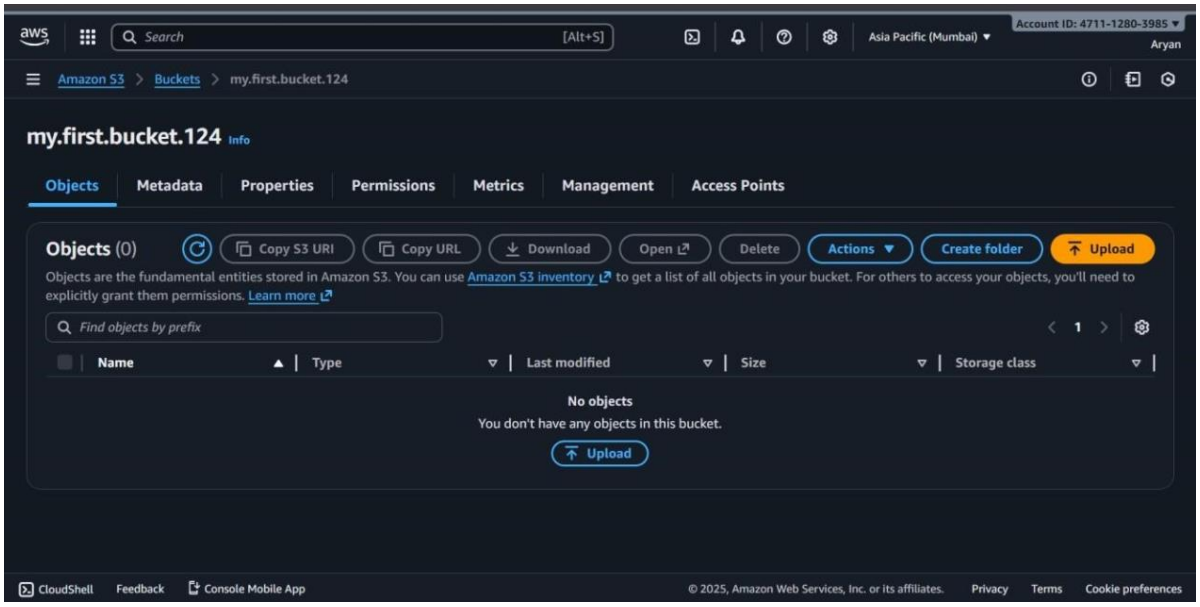
7. Review and Create

- 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**.



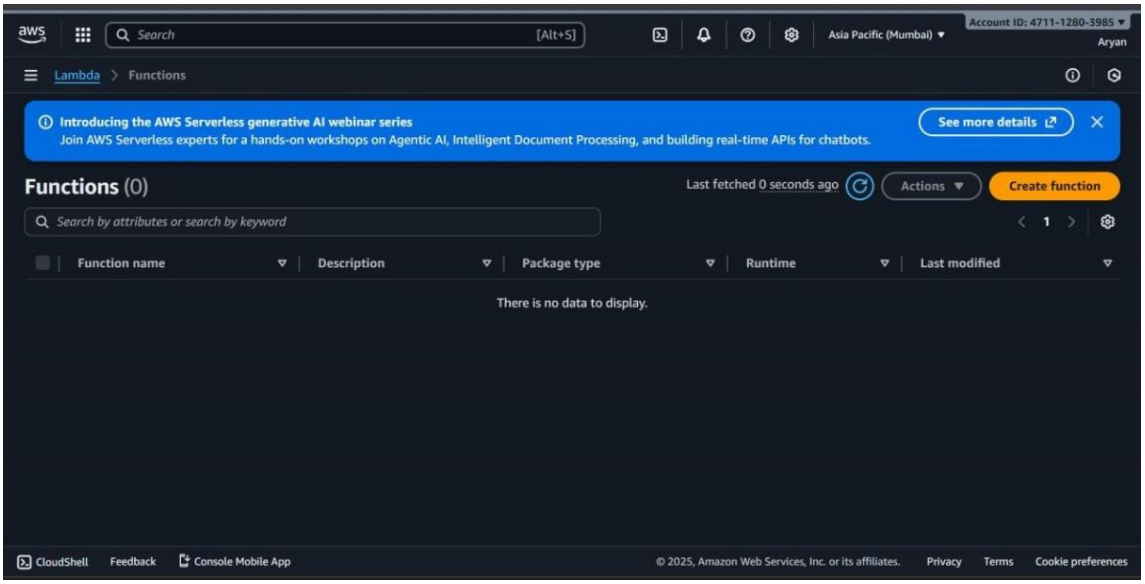
PRACTICAL-4

OBJECTIVE – 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**.

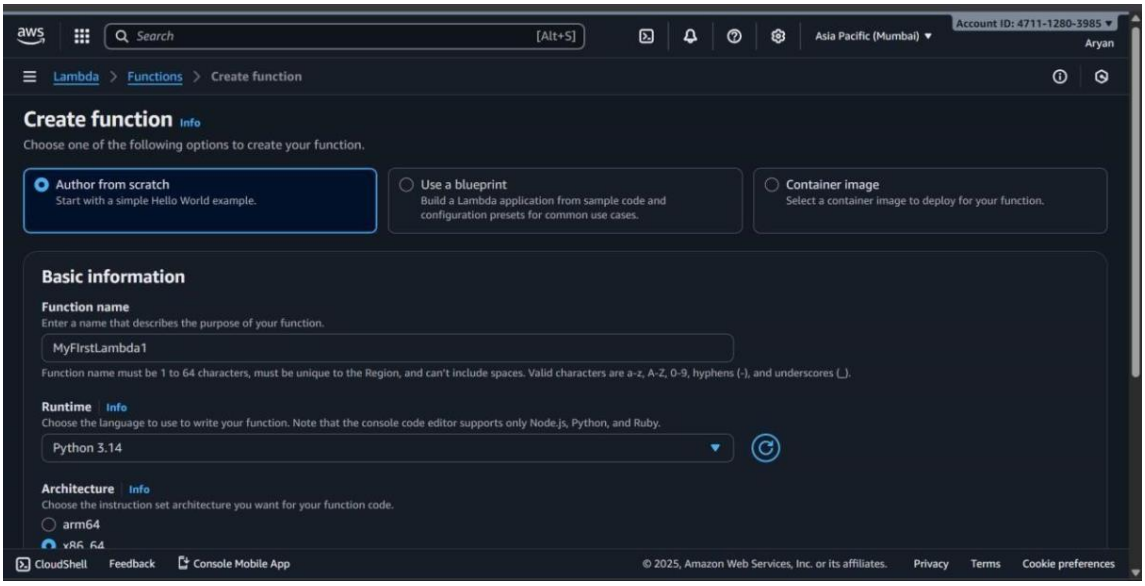


4. **Choose a Creation Method** You'll see 3 options:
   1. **Author from scratch** → (most common, start fresh).
   2. **Use a blueprint** → predefined templates.

3. **Container image** → deploy code as Docker container. Select **Author from scratch**.

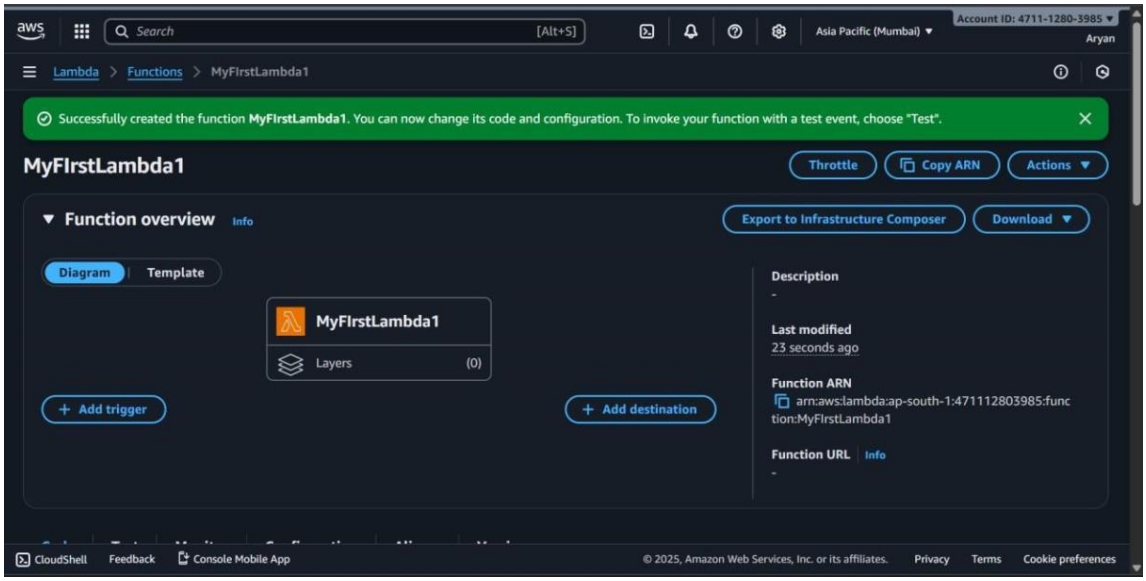
5. Configure Basic Settings

- **Function name**: Enter a unique name (e.g., MyFirstLambda).
- **Runtime**: Choose a runtime (Node.js, Python, Java, Go, etc. → example: **Python 3.9**).
- **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.

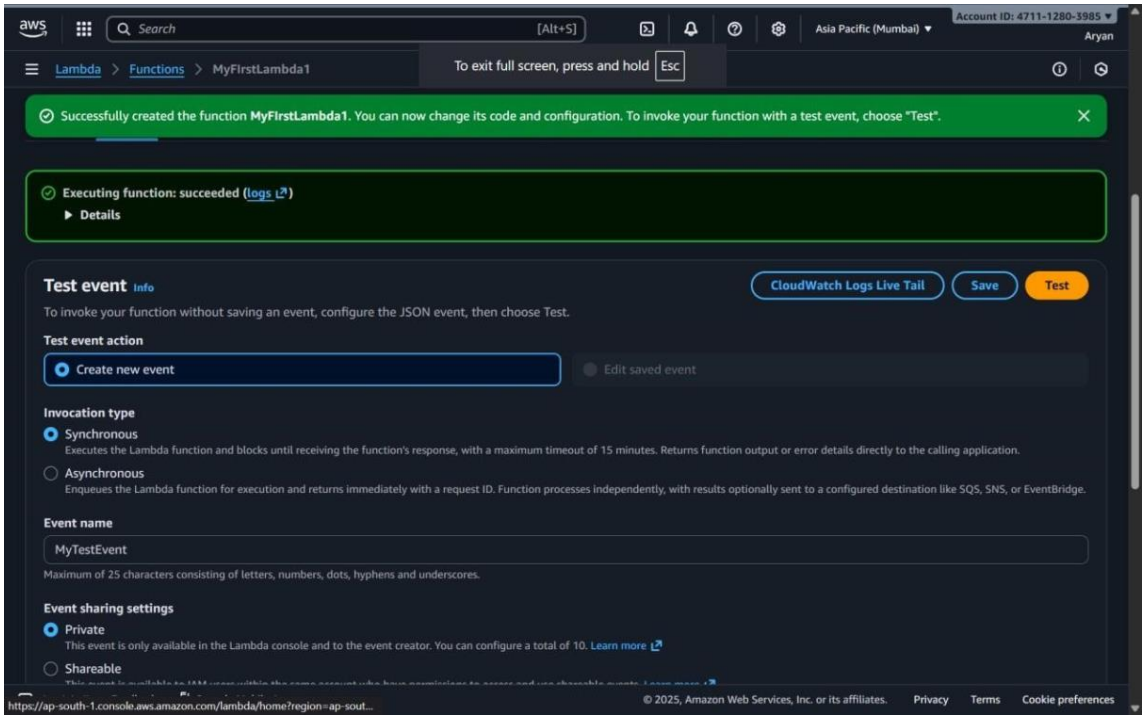


7. Add Your Code

- 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 Python: def lambda_handler(event, context):

```
    return {
        'statusCode': 200,
        'body': 'Hello from Lambda!'
    }
```



8. Configure Test Event

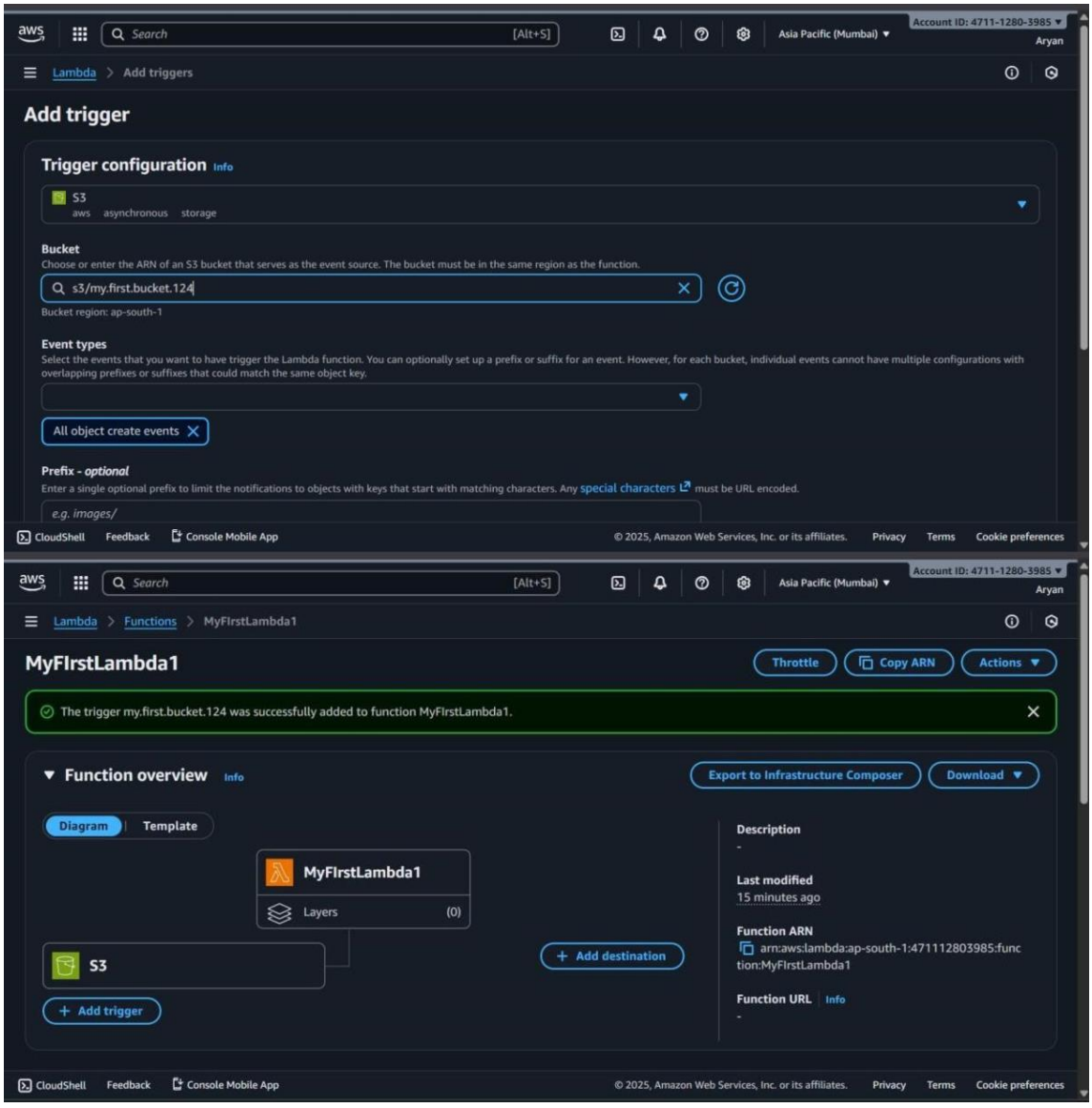
- Click **Test** → **Configure test event**.
- Give it a name (e.g., TestEvent).
- Keep the default event JSON or modify as needed.
- Save.

9. Run the Function

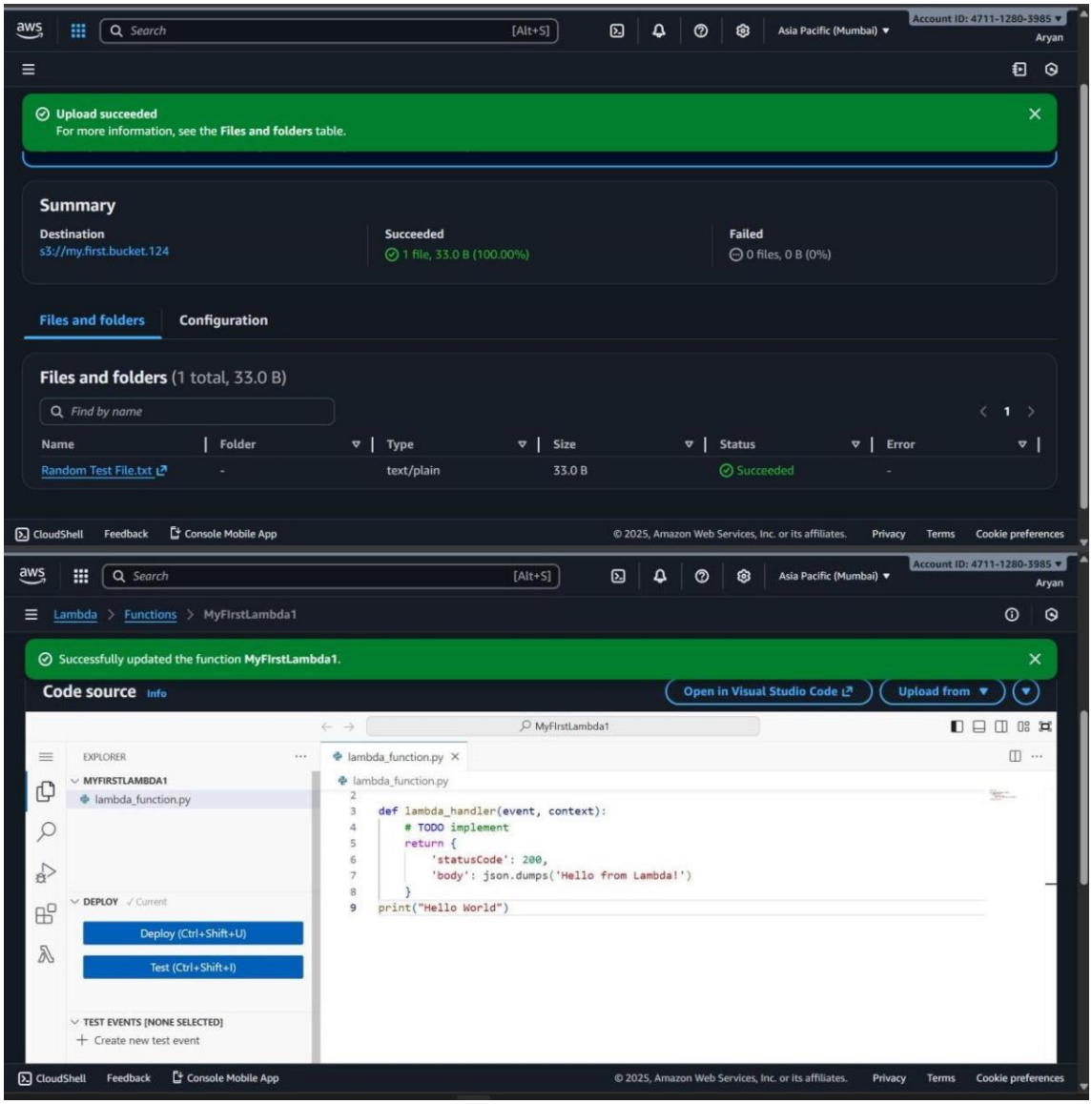
- Click **Test** again.
- Check the execution results (output, logs, and status).

10. (Optional) Add a Trigger

- You can connect Lambda to services like:
    - API Gateway (for REST APIs) ○ S3 (trigger on file uploads) ○ DynamoDB (trigger on database changes) ○ EventBridge (scheduled events)


Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
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/my.first.bucket.124
Bucket region: ap-south-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 events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.
All object create events
Prefix - optional
Enter a single optional prefix to limit the notifications to objects with keys that start with matching characters. Any special characters must be URL encoded.
e.g. images/
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
Lambda > Functions > MyFirstLambda1
MyFirstLambda1
Throttle
Copy ARN
Actions
The trigger my.first.bucket.124 was successfully added to function MyFirstLambda1.
Function overview Info
Export to Infrastructure Composer
Download
Diagram
Template
MyFirstLambda1
Layers (0)
S3
Add destination
Add trigger
Description
-
Last modified
15 minutes ago
Function ARN
arn:aws:lambda:ap-south-1:471112803985:function:MyFirstLambda1
Function URL Info
-
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
Upload succeeded
For more information, see the Files and folders table.
Summary
Destination
s3://my.first.bucket.124
Succeeded
1 file, 33.0 B (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 total, 33.0 B)
Find by name
Name
Folder
Type
Size
Status
Error
Random Test File.txt
-
text/plain
33.0 B
Succeeded
-
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

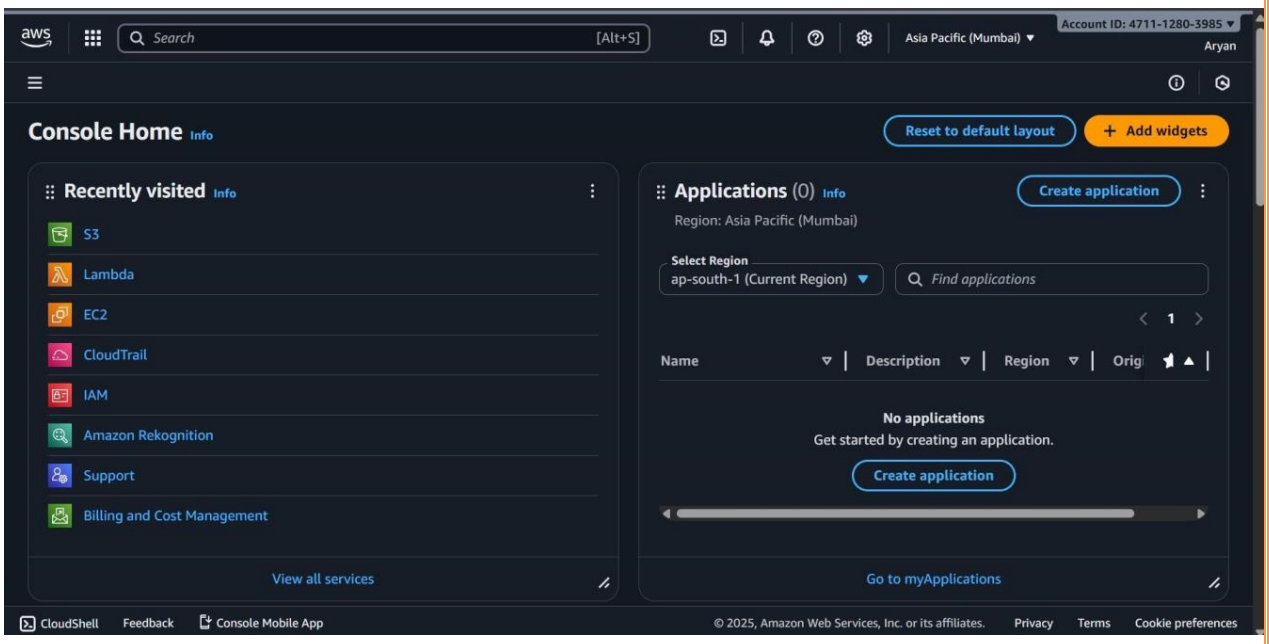
Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
Lambda > Functions > MyFirstLambda1
Successfully updated the function MyFirstLambda1.
Code source Info
Open in Visual Studio Code
Upload from
MyFirstLambda1
EXPLORER
MYFIRSTLAMBDA1
lambda_function.py
DEPLOY
Current
Deploy (Ctrl+Shift+U)
Test (Ctrl+Shift+I)
TEST EVENTS [NONE SELECTED]
Create new test event
lambda_function.py
def lambda_handler(event, context):
# TODO implement
return {
'statusCode': 200,
'body': json.dumps('Hello from Lambda!')
}
print("Hello World")
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Practical:-5

Objective:- Creating **an** IAM (Identity and Access Management) user in AWS is to provide secure and controlled access to AWS resources for individuals or applications without using the root account.

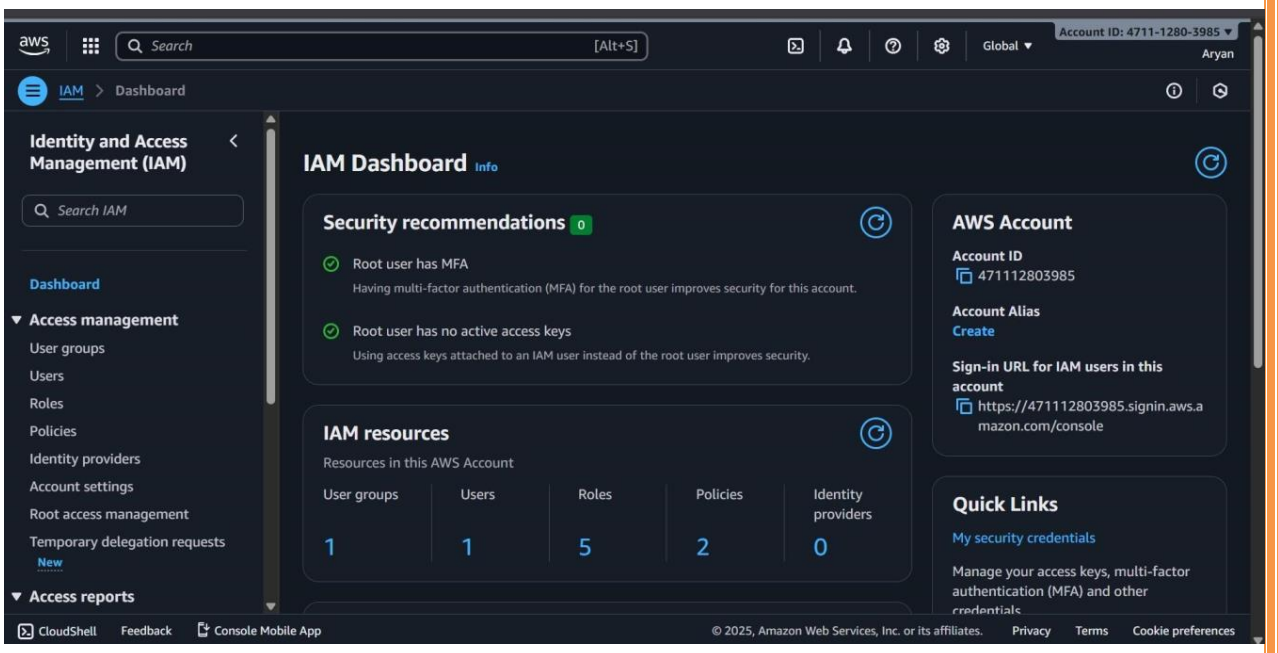
Step 1: Sign in to AWS Console

Log in to your **AWS Management Console** using your **root account** or an **IAM user** who has **Administrator privileges**.



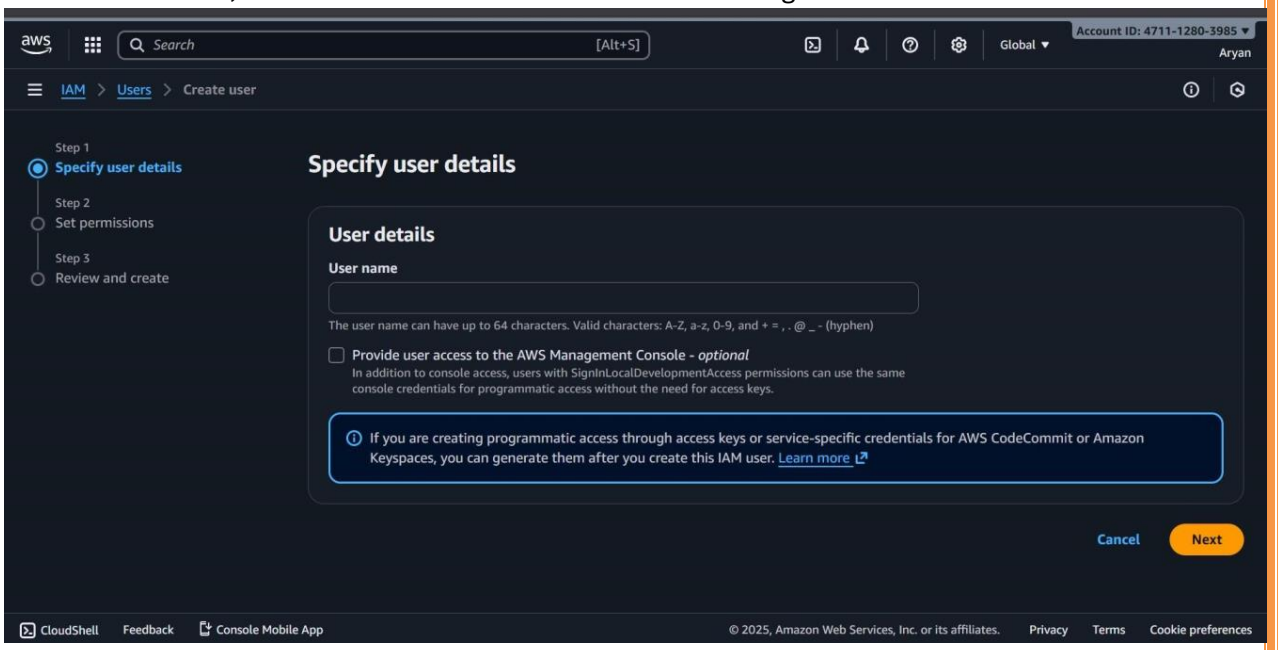
Step 2: Open IAM Service

In the search bar at the top, type **IAM**. Select **IAM (Identity and Access Management)**.



Step 3: Go to Users Section

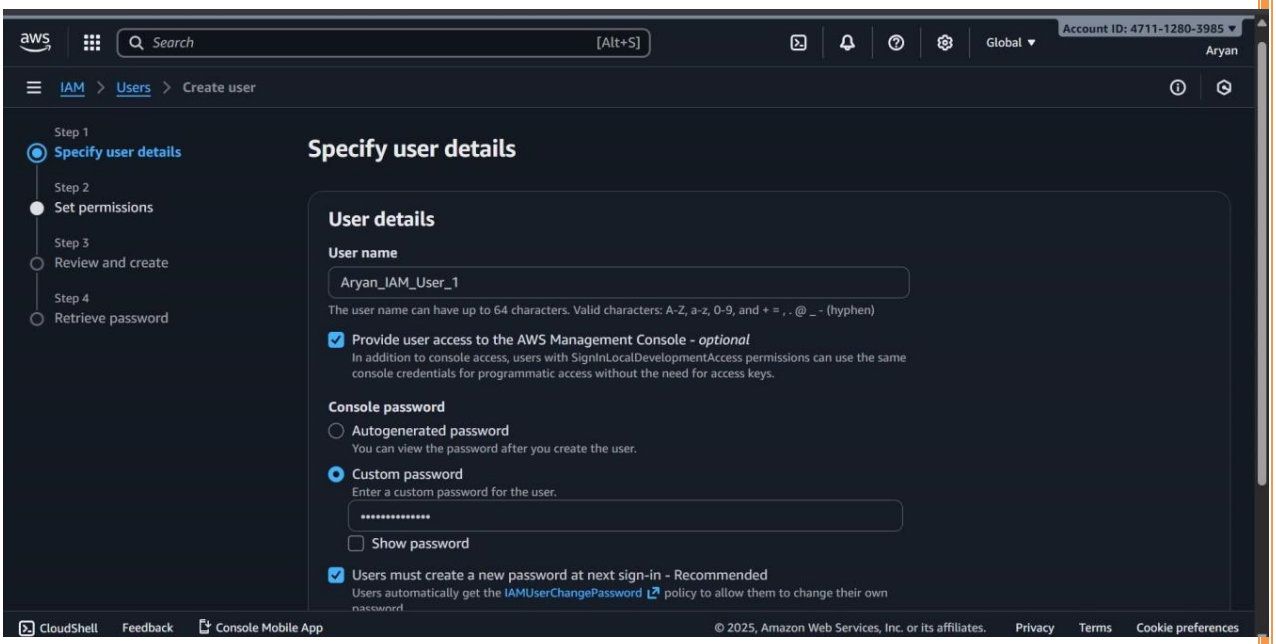
In the left sidebar, click on **Users**. You will see a list of all existing users. Click **"Create user"**



to add a new one.

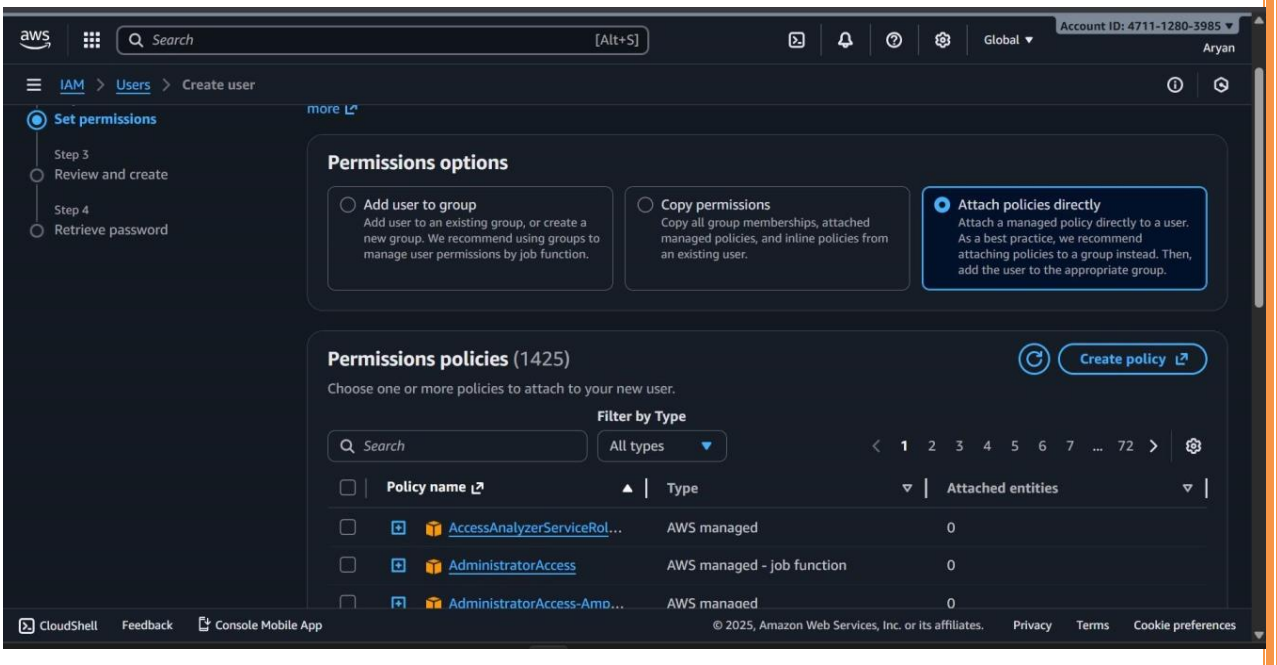
Step 4: Enter User Details

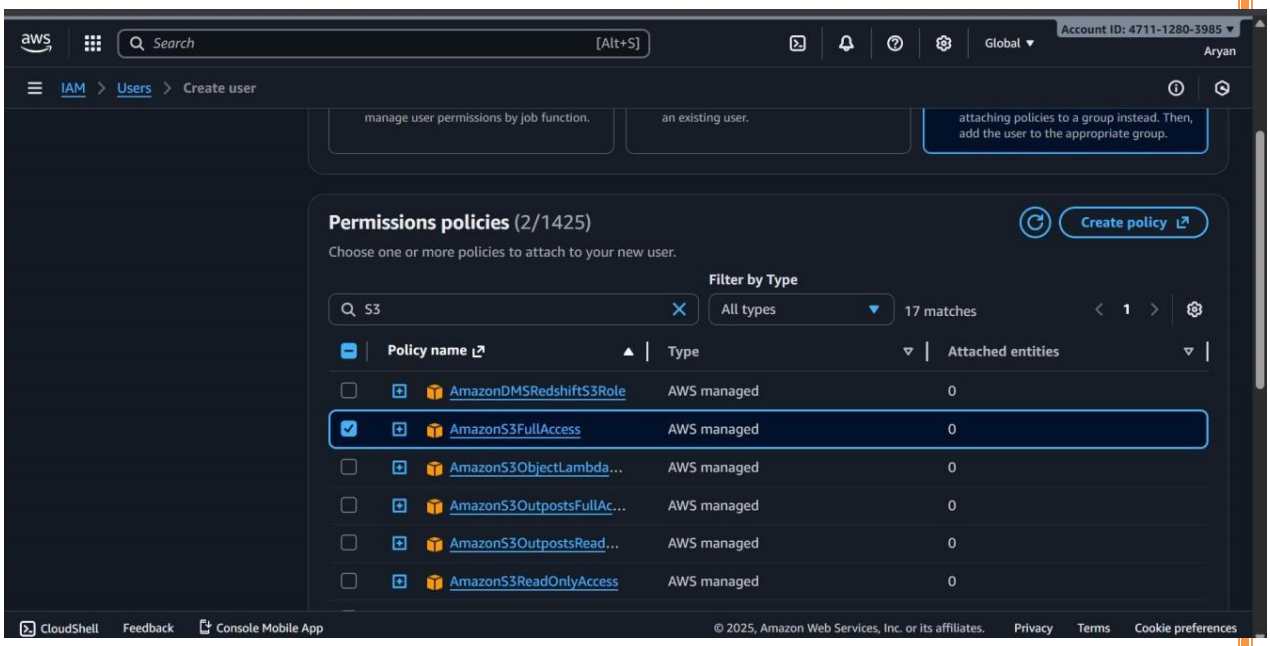
Enter a **User name** . Choose the type of access: **Password access** → if the user needs to log in to the AWS Console. Click **Next.**



Step 5: Set Permissions

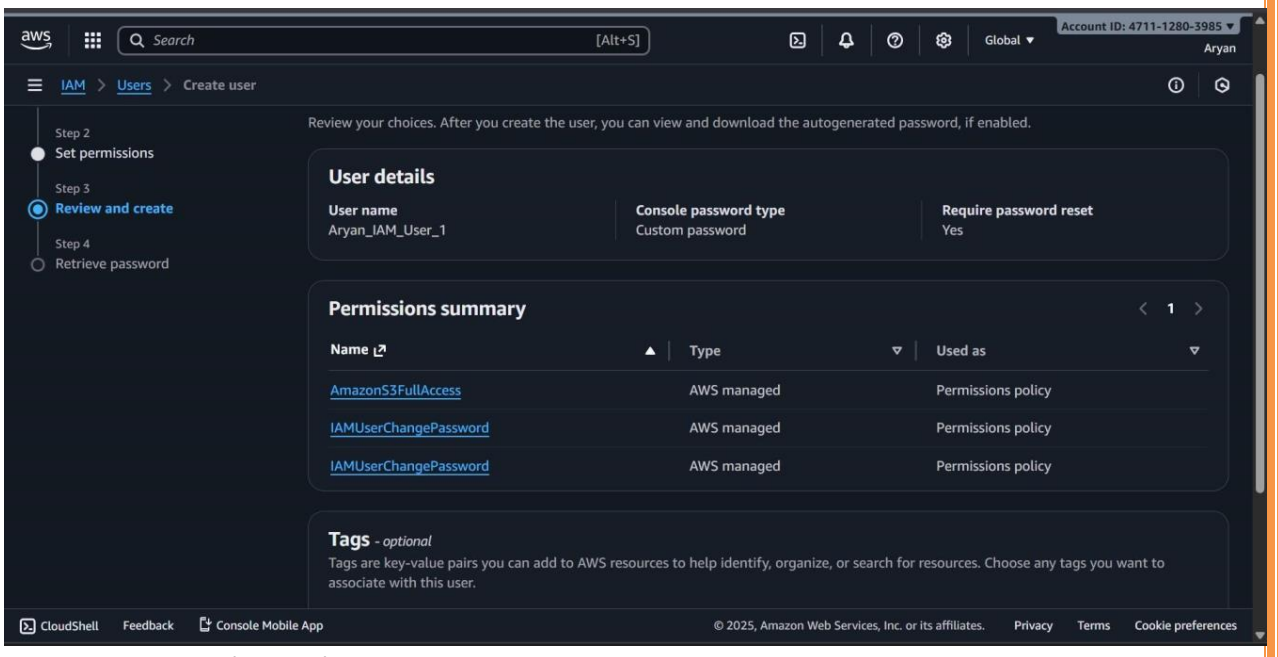
Choose **Attach policies directly** → assign permissions manually (e.g., AmazonS3FullAccess, AdministratorAccess, etc.). Then click **Next.**





Step 6: Review and Create

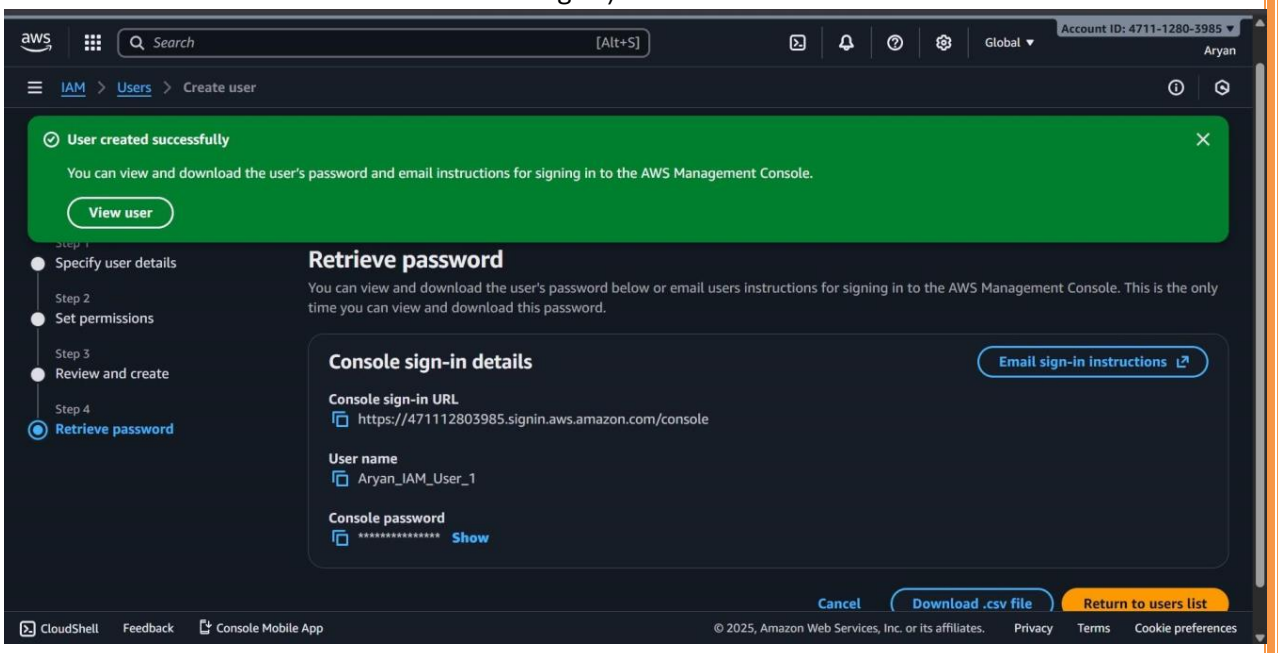
Review all details carefully. Click **Create user**.



Step 7: Save Login Details

- Once the user is created, AWS will show:

- **User ARN (Amazon Resource Name)** ○ **Console login link**
- **Password or Access key/Secret key** (Download the .csvfile — it won't be shown again).

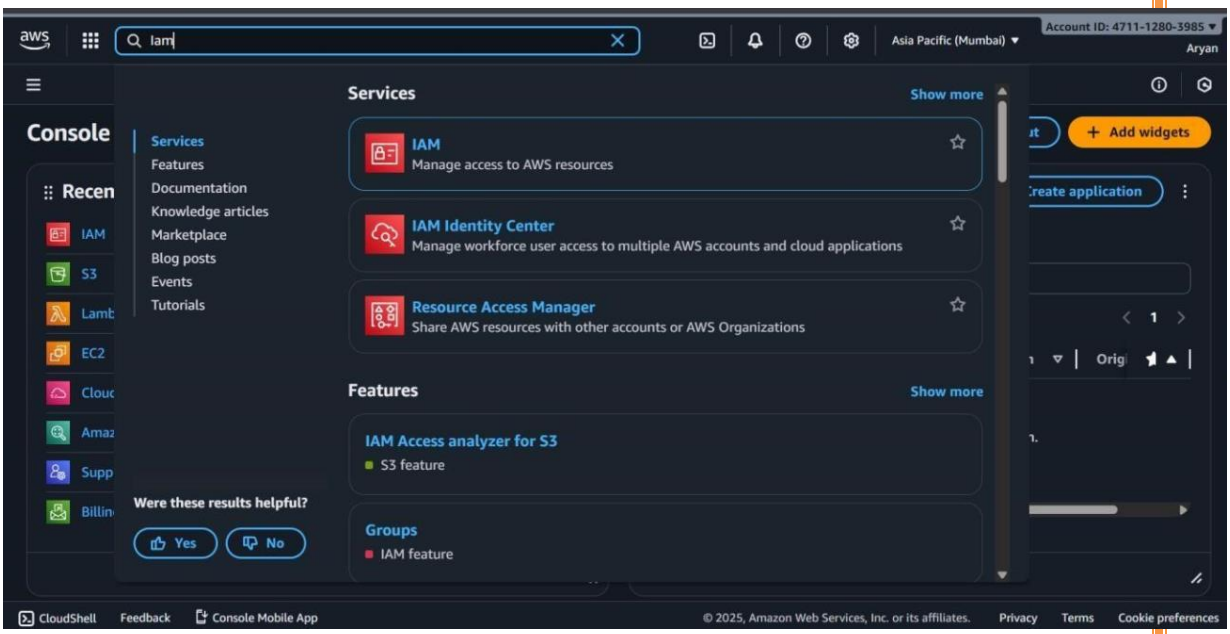


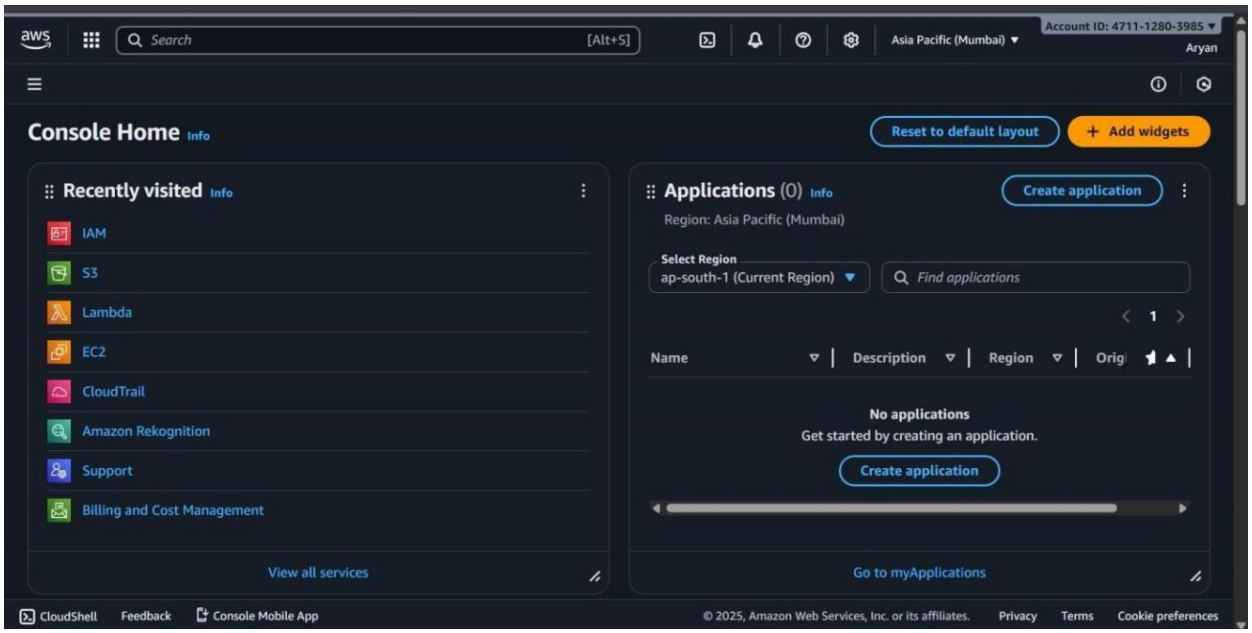
Practical :-6

Objective:- To secure an AWS IAM user account by enabling Multi-Factor Authentication (MFA), adding an extra verification step to prevent unauthorized access.

Step 1:- Sign in to AWS Management Console

- Log in using your **root account** or **IAM admin user**.
- Open the console.



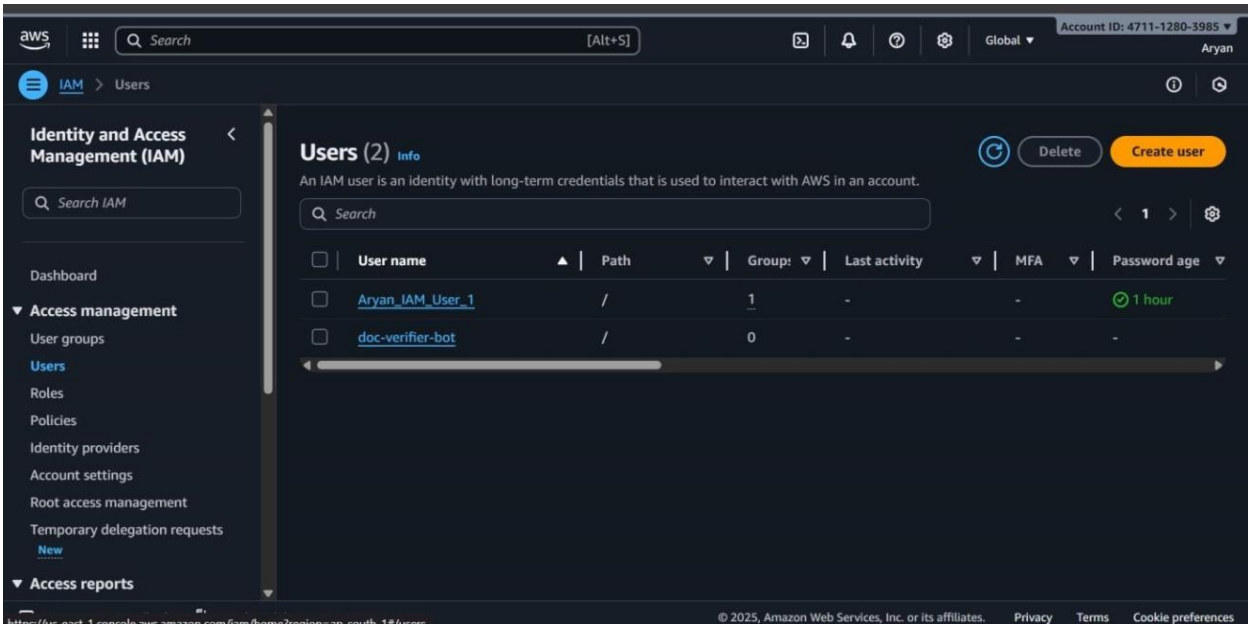


Step 2:- Go to IAM Service

- In the search bar, type **IAM**.

- Click IAM (Identity and Access Management).

Step 3:-Open “Users”

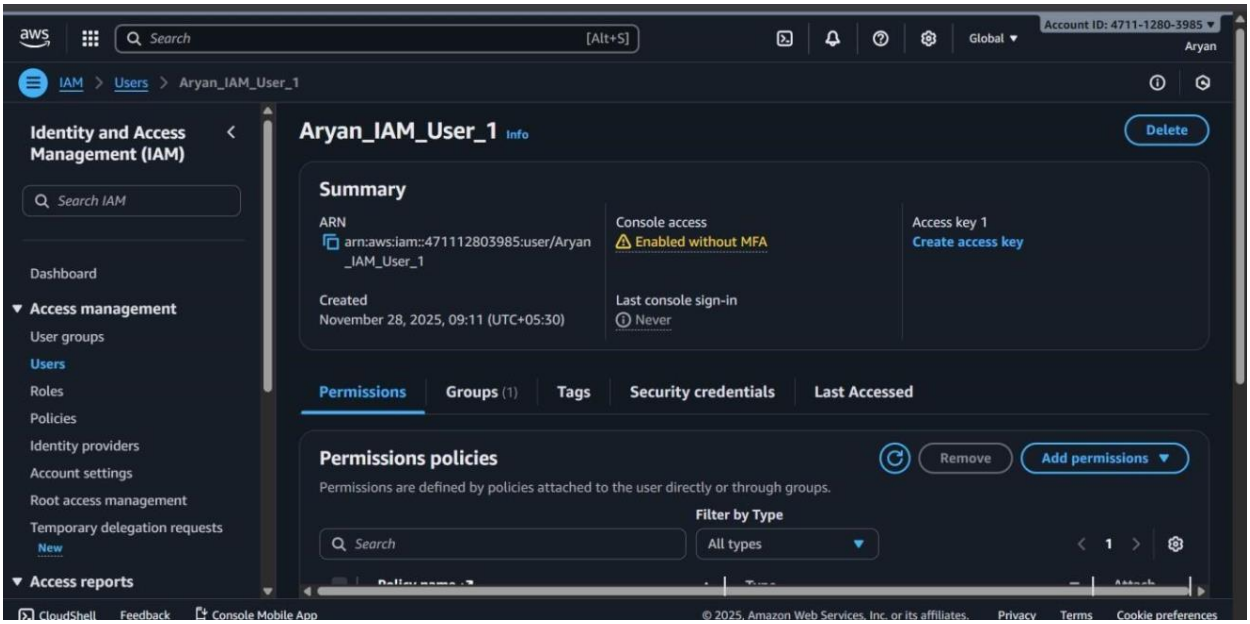


- In the left navigation panel, select **Users**.

Click the **username** for which you want to enable MFA.

Step 4:-Go to the “Security Credentials” Tab

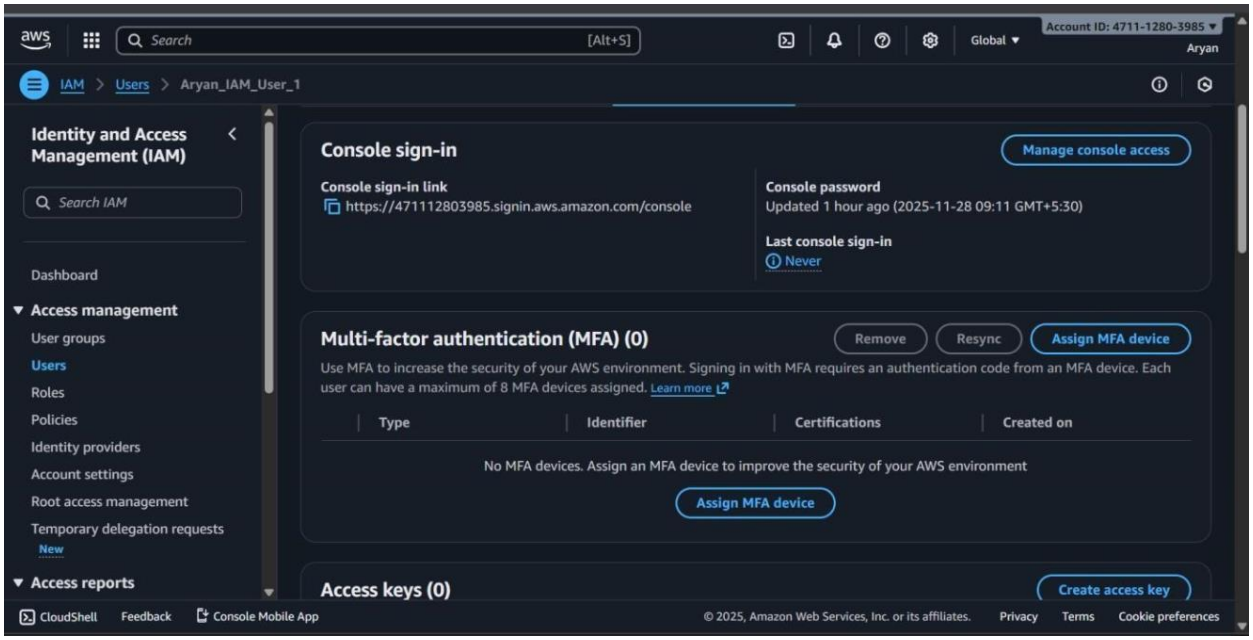
- After opening the user’s profile, click on **Security credentials**.
- Scroll down to the section **Multi-Factor Authentication (MFA)**.

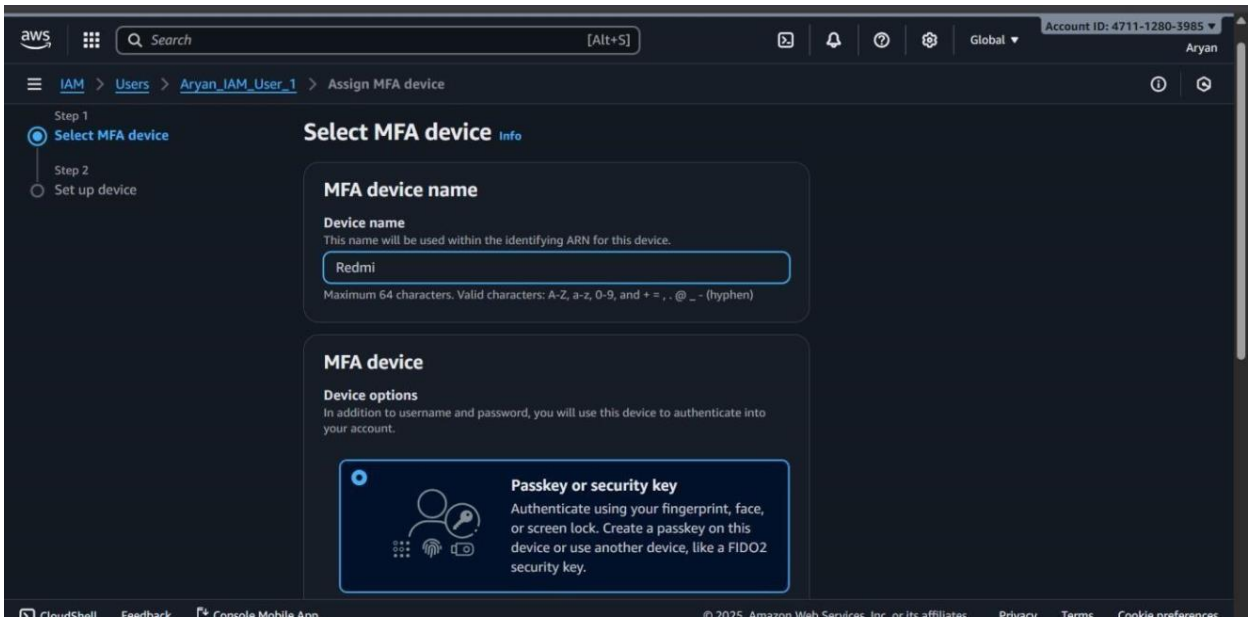


Step 5:-Click “Assign MFA Device”

- 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**.





Step 6:-Select “Authenticator App” and Continue

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

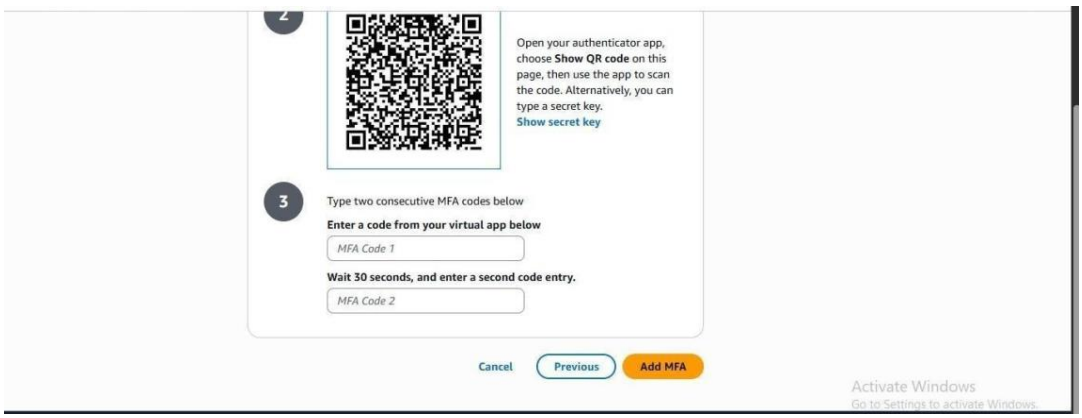
Step 7:-Open your Authenticator App

You can use any app:

- Google Authenticator
- Authy
- Microsoft Authenticator
- LastPass Authenticator

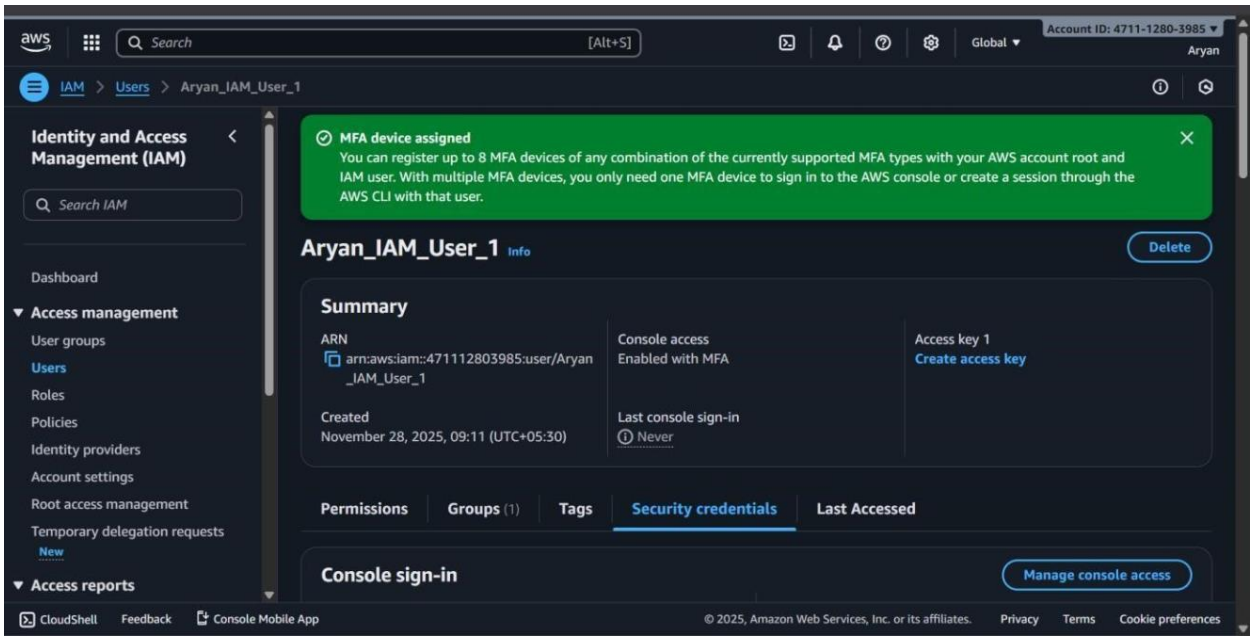
Click **Add Account** → **Scan QR Code**.

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



Step 8:-MFA Successfully Enabled

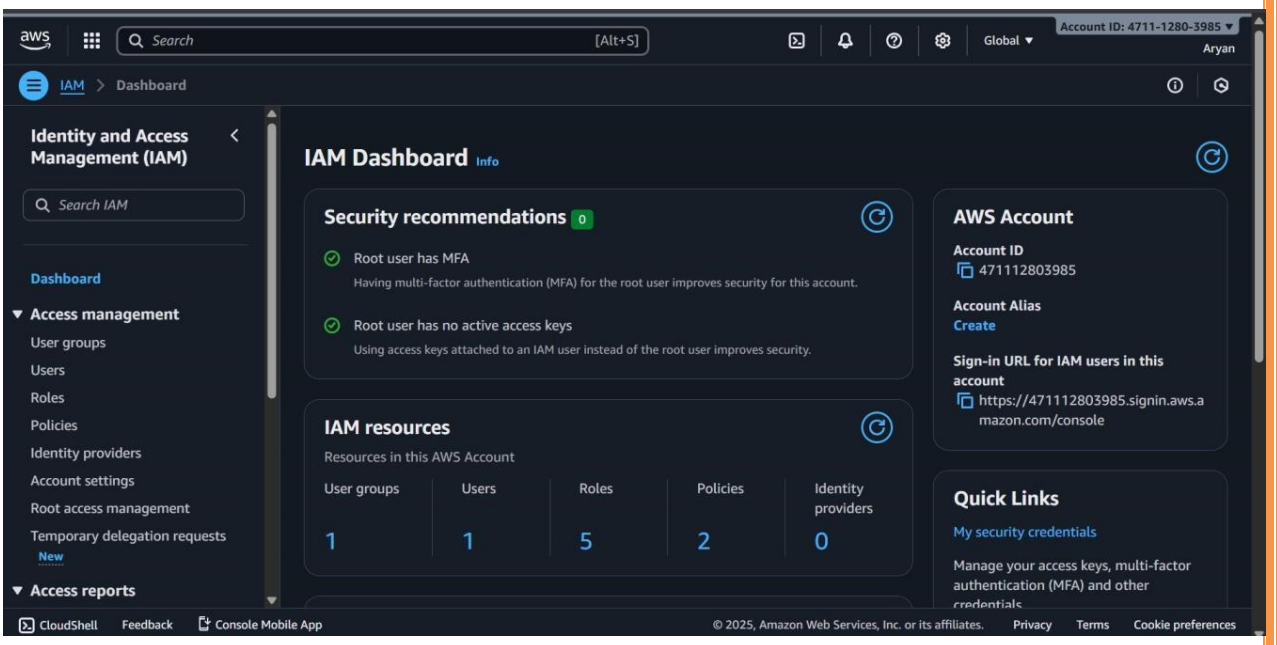
“MFA device assigned successfully”



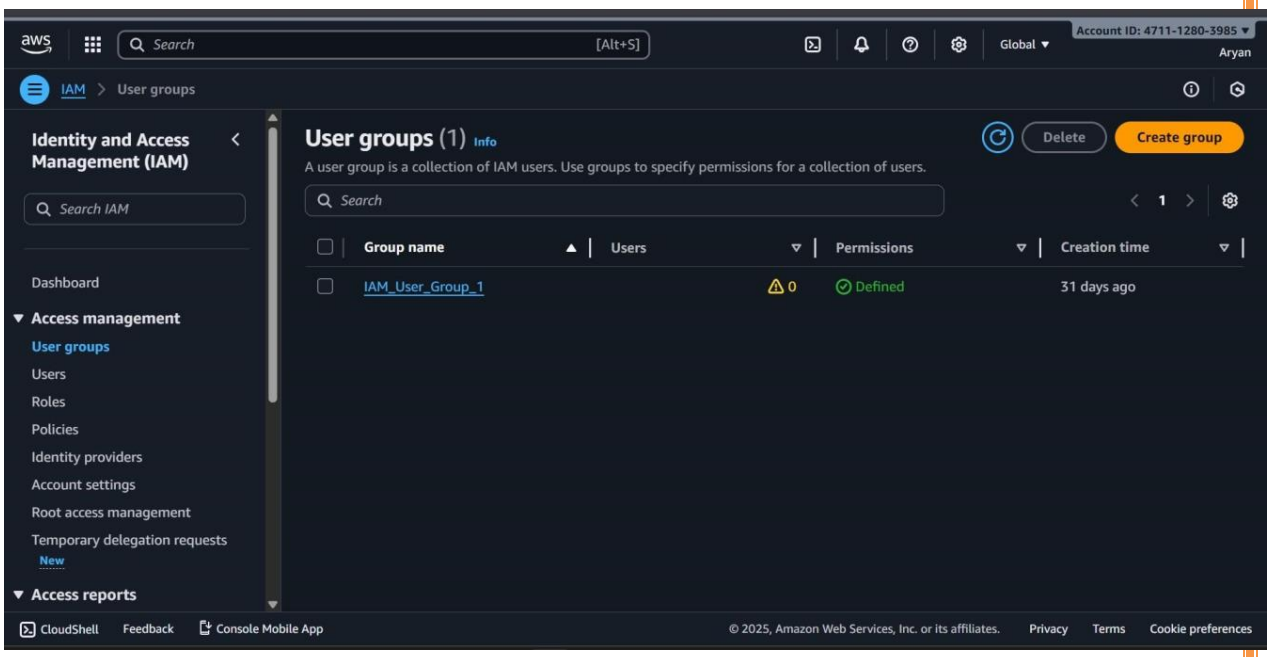
Practical:-7

Objective: To create a user group in AWS IAM in order to manage permissions collectively for multiple users having similar roles or responsibilities.

Step1:- Open the IAM Service:
In the search bar at the top of the console, type **IAM**, then select **Identity and Access Management** from the results.

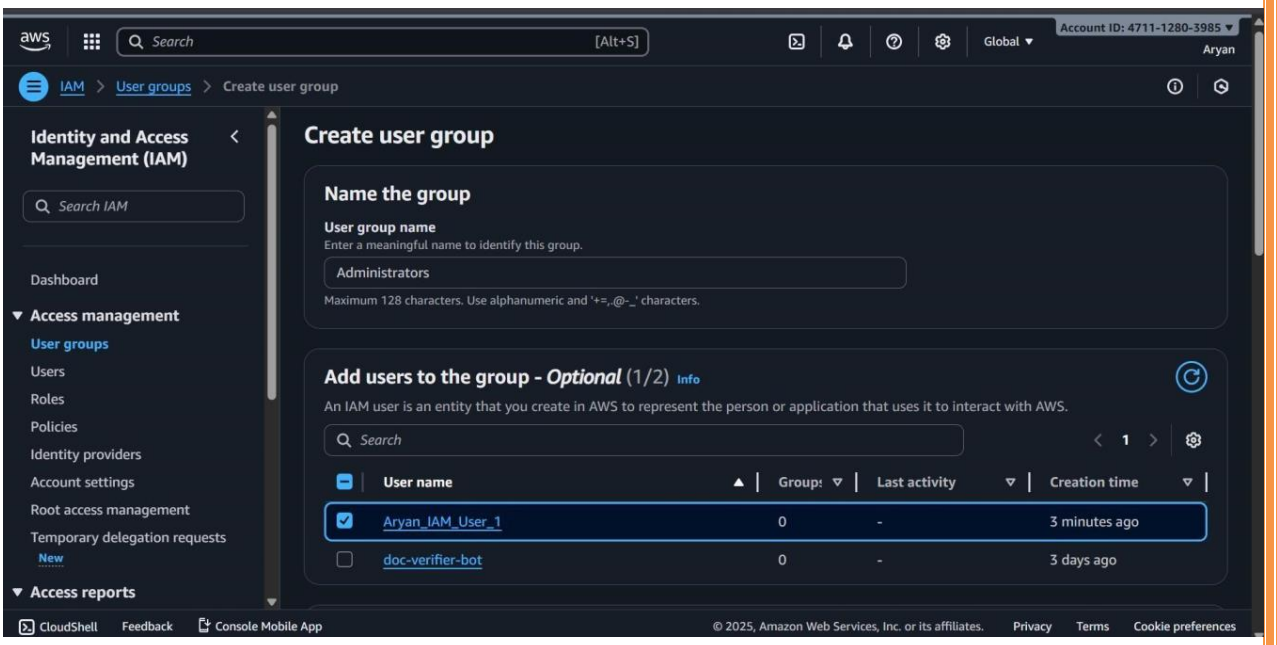


Step 2:- Go to User Groups Section:
In the left-hand sidebar, click on **User groups**.



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:

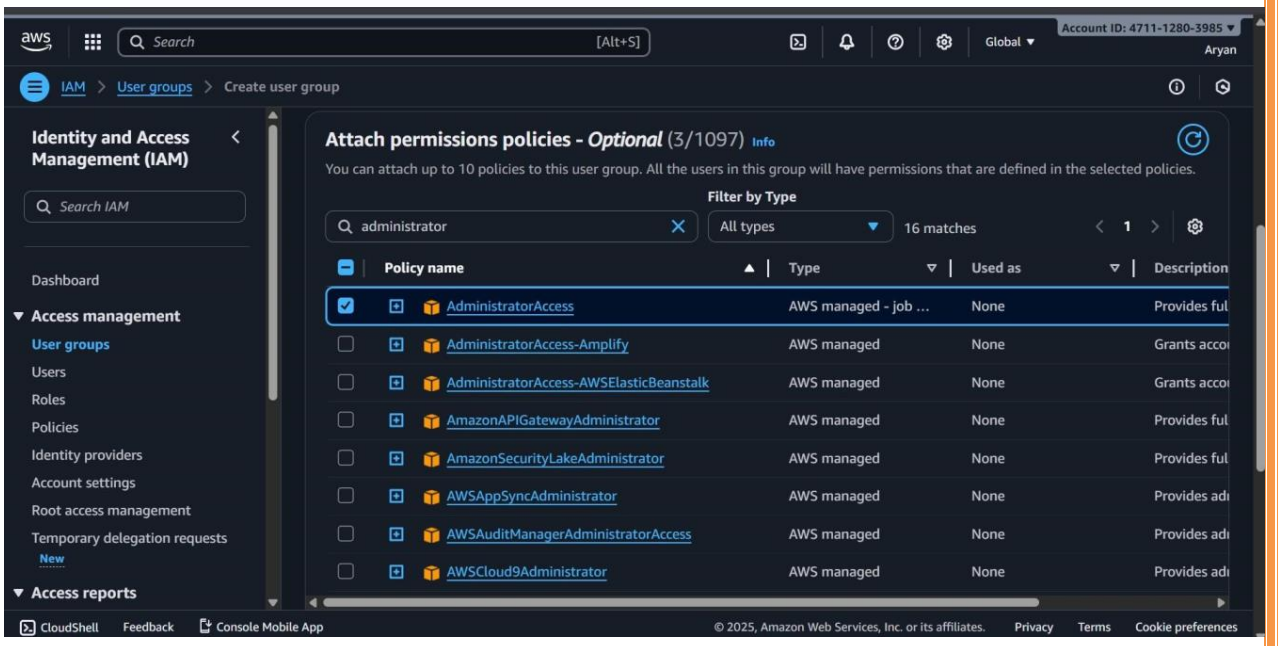
Type a **unique name** for your group (for example, *Developers*, *Admins*, or *ReadOnlyUsers*). For Example, here Administrators.

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**.

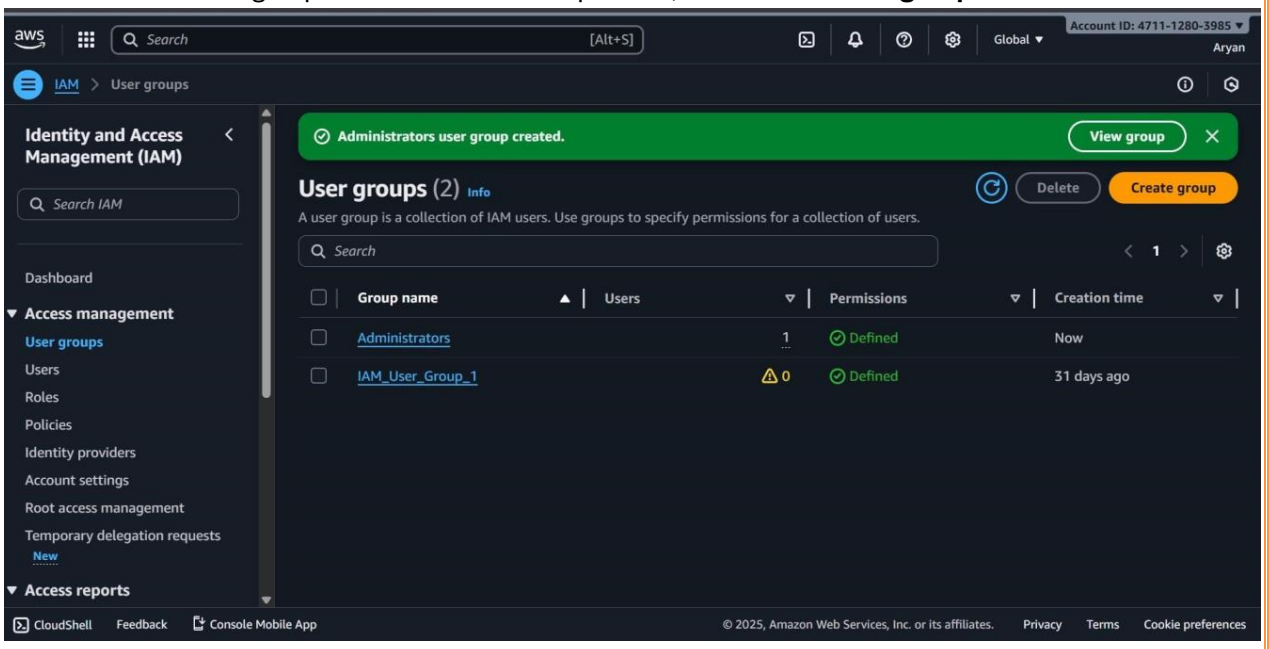


Step 6:- Add Users to the Group (Optional):

You can select existing IAM users to include in this group now, or you can add users later after creating the group.

Step 7:- Review and Create Group:

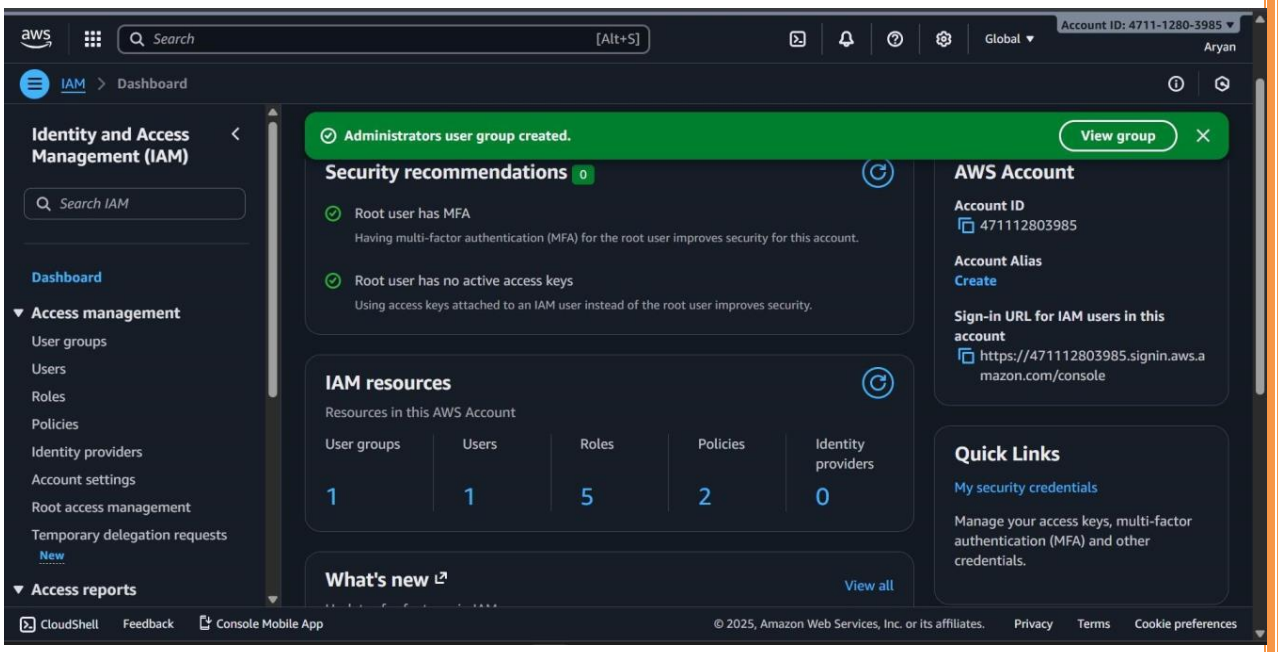
Review the group details and attached policies, then click **Create group**.



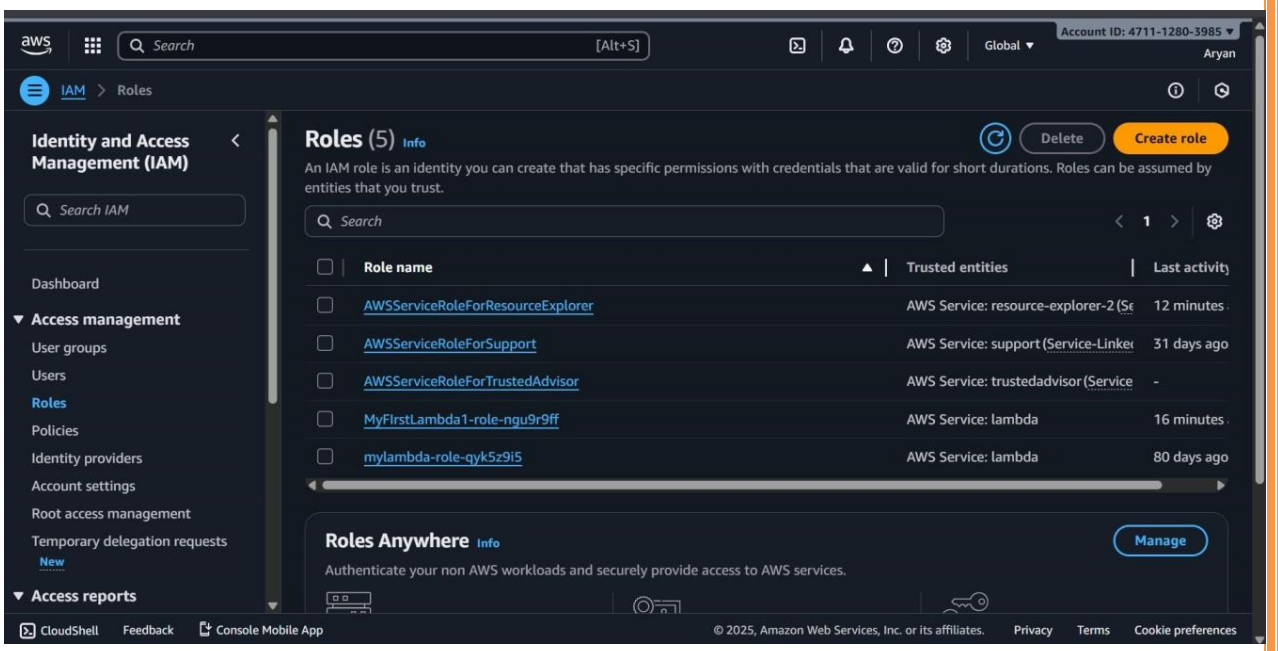
Practical:-8

Objective:-To create a security role in AWS IAM that allows AWS services or users to securely access specific AWS resources with defined permissions, ensuring controlled and temporary access without sharing long-term credentials.

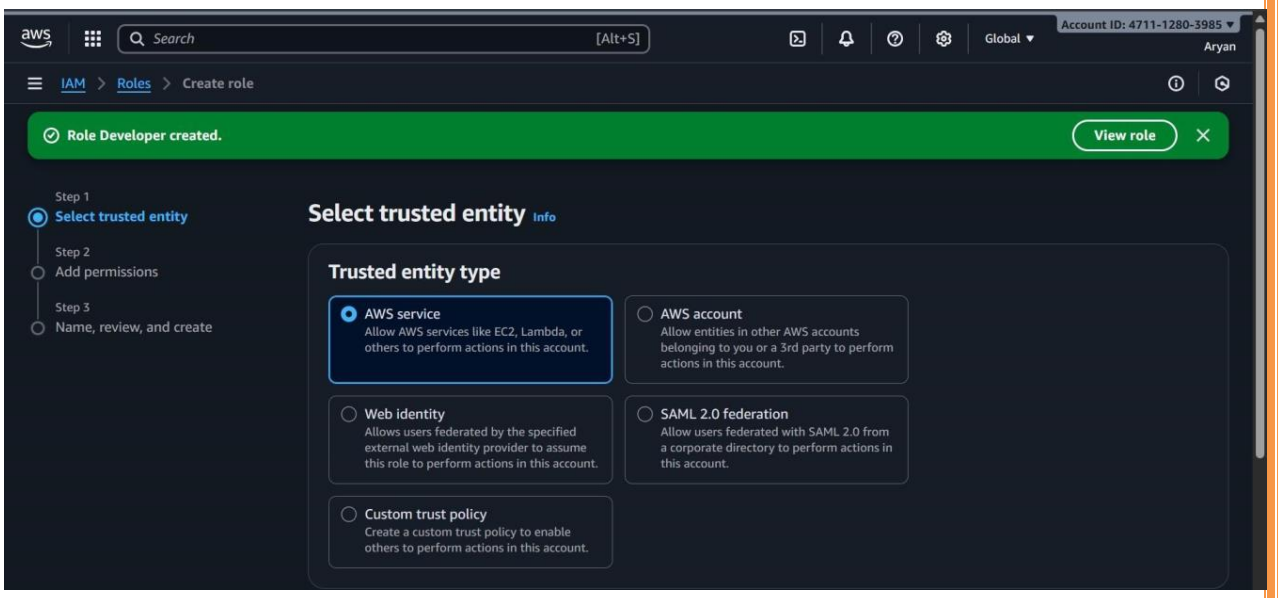
Step 1:- Open the IAM Service:
In the search bar at the top of the console, type **IAM**, then select **Identity and Access Management** from the results.



Step 2:- Go to Roles Section:
In the left-hand navigation pane, click on **Roles**.



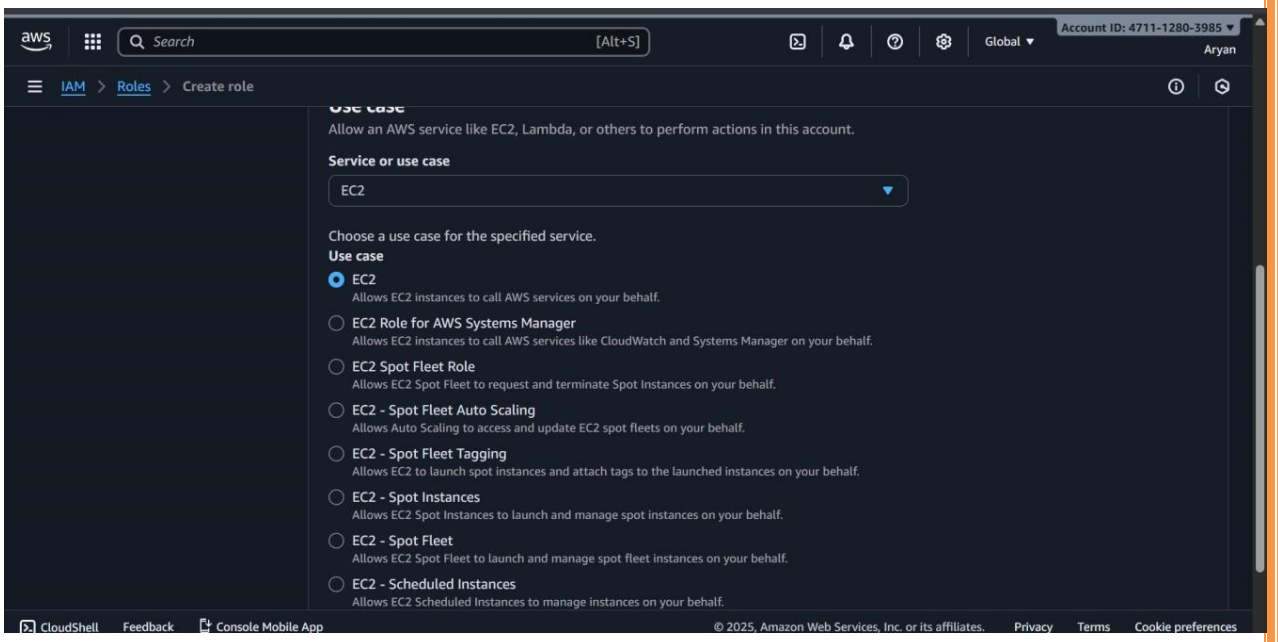
Step 3:- Click on "Create role":
On the Roles page, click the **"Create role"** button to start the process.



Step 4:- Select Trusted Entity Type:
Choose who will use the role, such as:

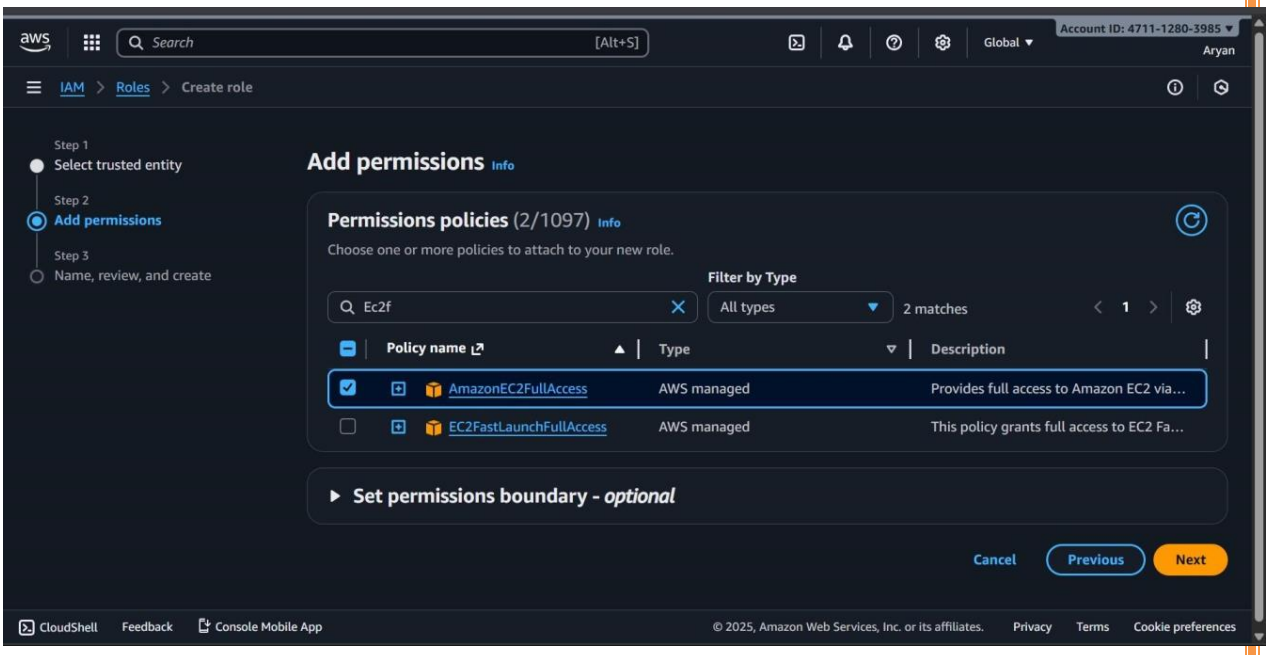
- **AWS Service** (e.g., EC2, Lambda)
- **Another AWS Account**
- **Web Identity** or **SAML 2.0 Federation**

Click **Next** after selecting the appropriate option.

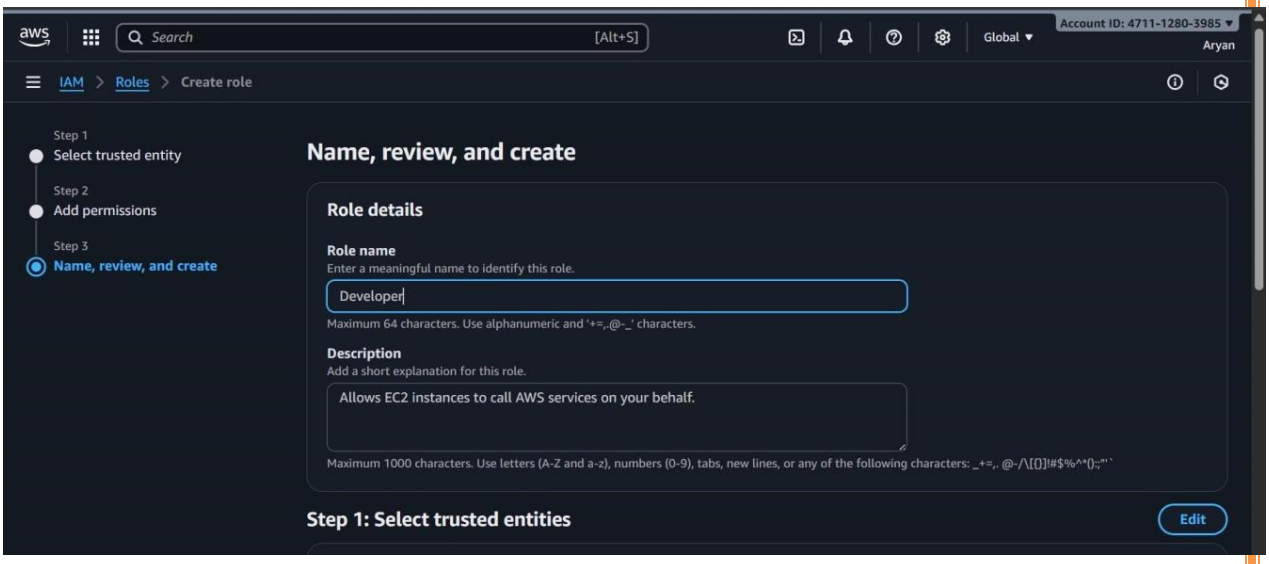


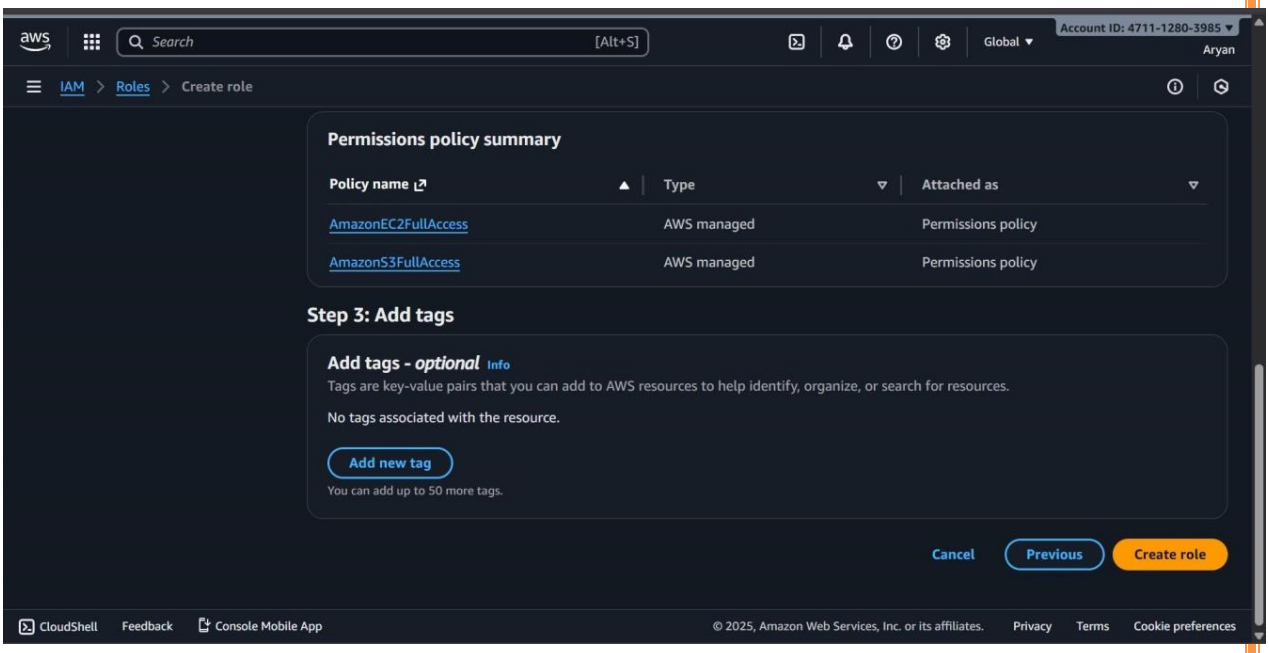
Step 5:-Attach Permissions Policies:

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



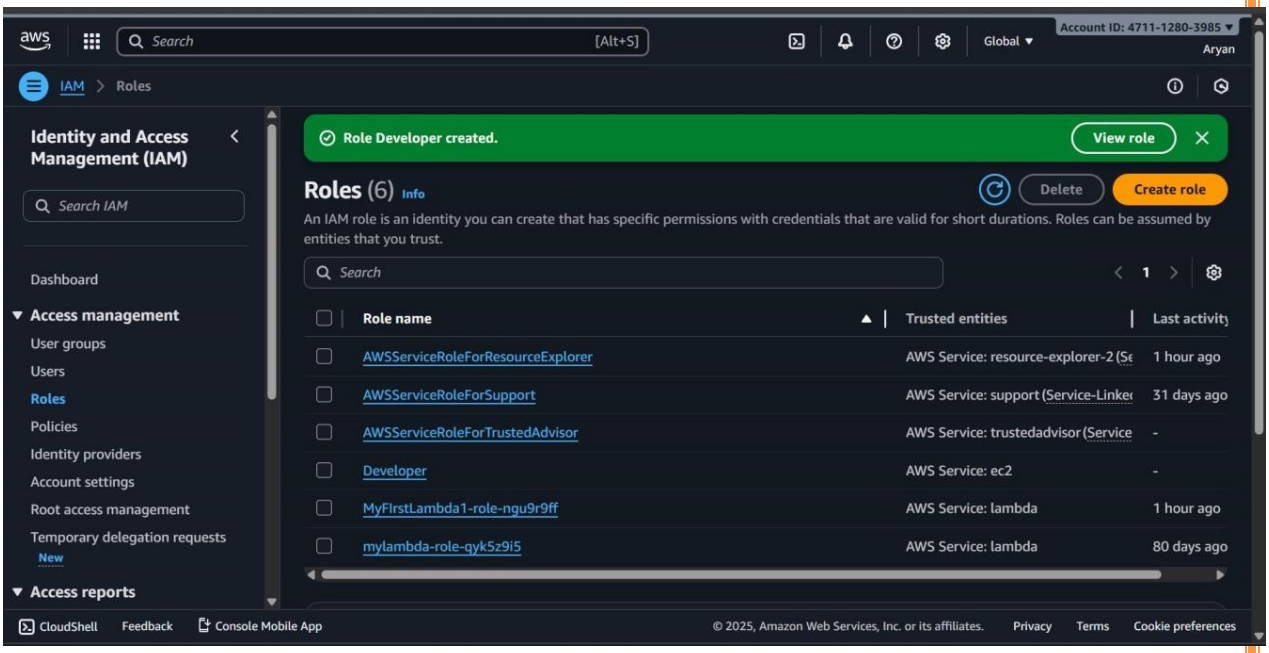
Step 6:- Name and Review the Role:
Enter a **role name** (for example, *EC2SecurityRole* or *LambdaAccessRole*) and review all selected settings.





Step7:- **Create the Role:**

Click **Create role** to finish.

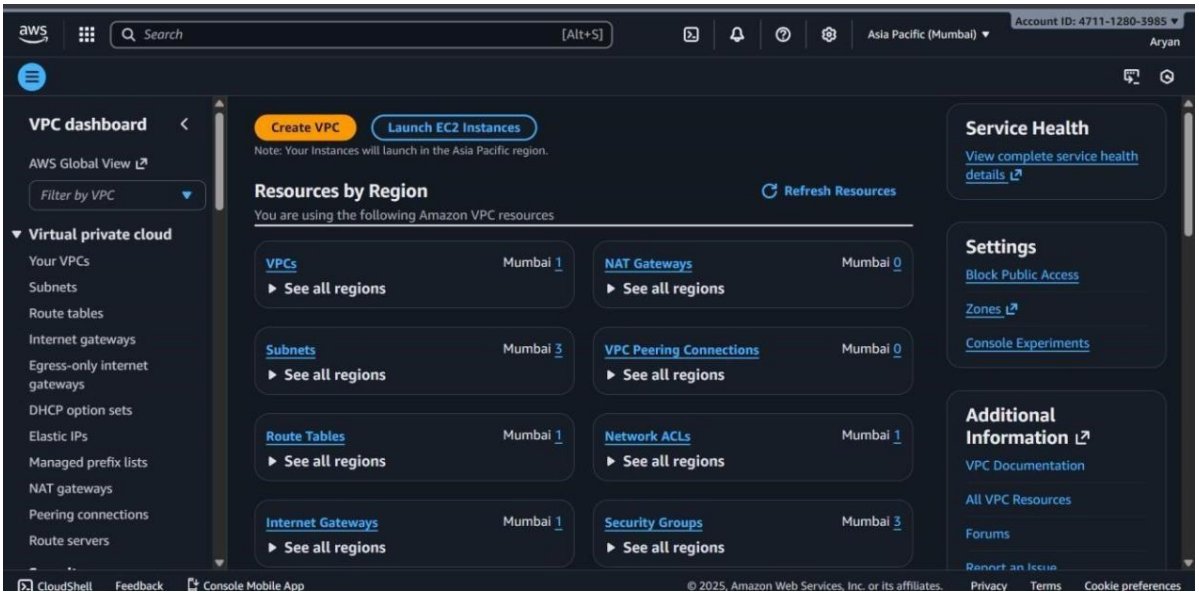


Practical :- 9

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

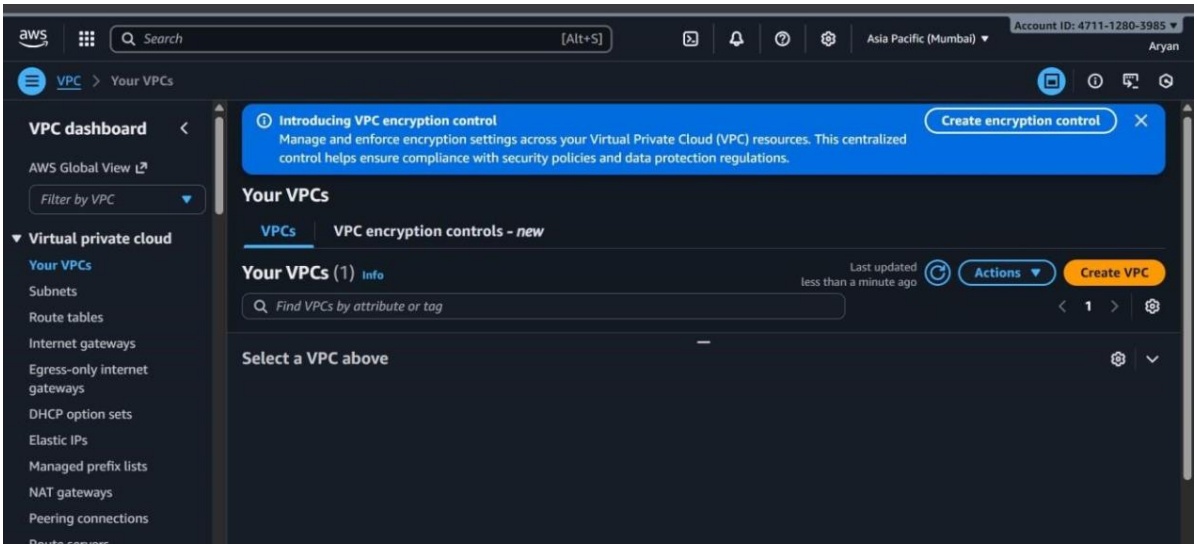
Step1. Open VPC Dashboard

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



Step2. Start Creating a VPC

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



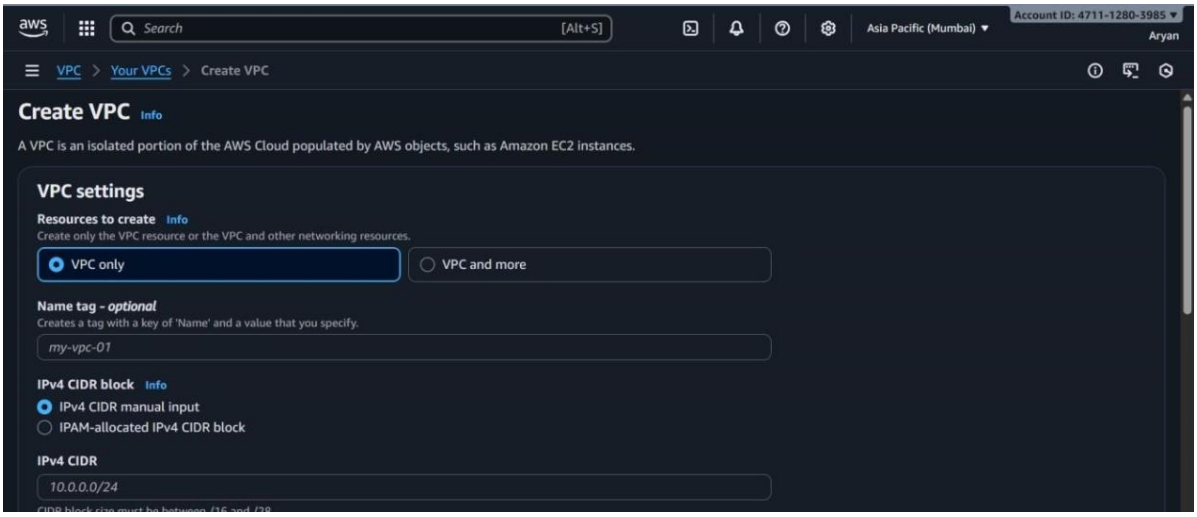
Step3. Select VPC Creation Method

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.



Step 4. Configure VPC Settings

Fill the form:

(a) Name tag • Example: MyVPC

(b) IPv4 CIDR Block

- Example: 10.0.0.0/16

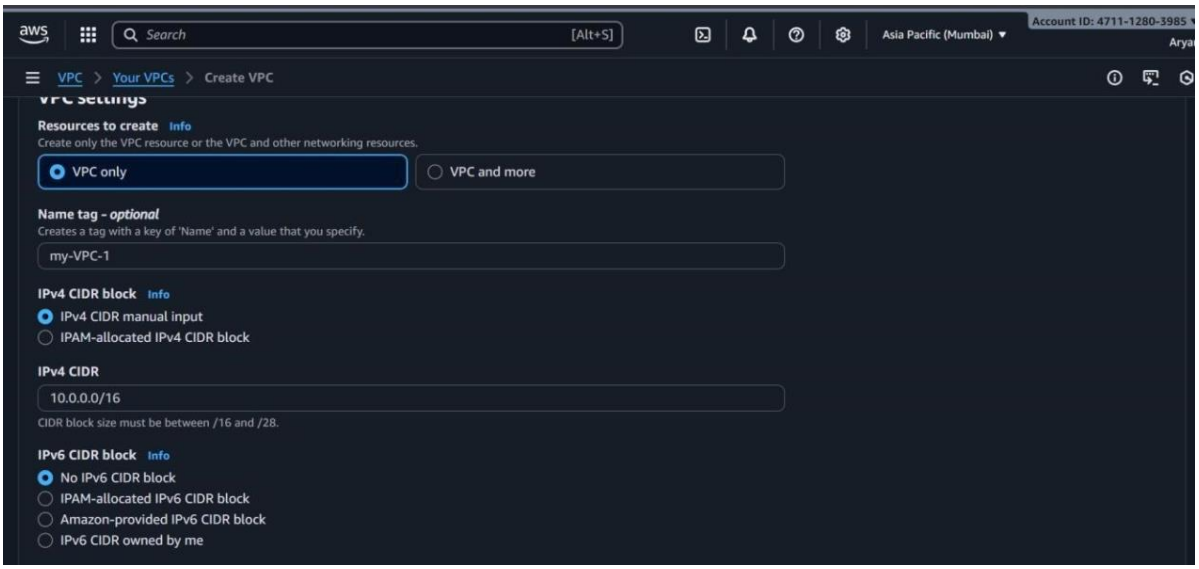
(c) IPv6 CIDR Block

- Choose **No IPv6 CIDR block** (optional)

(d) Tenancy

- Default (recommended)

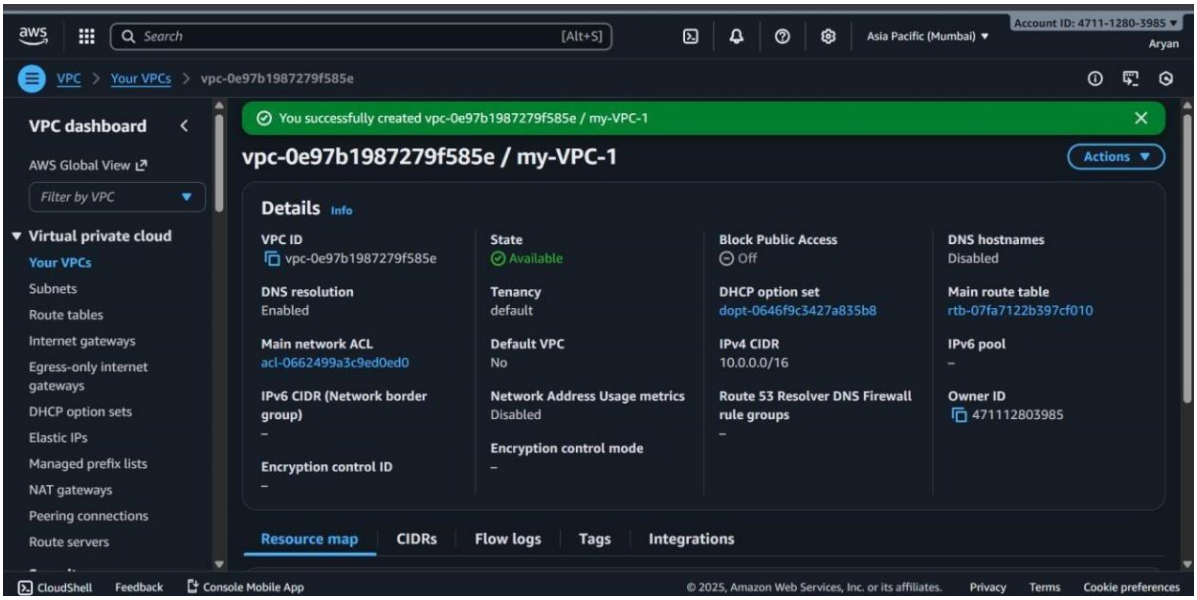
Click **Create VPC**.

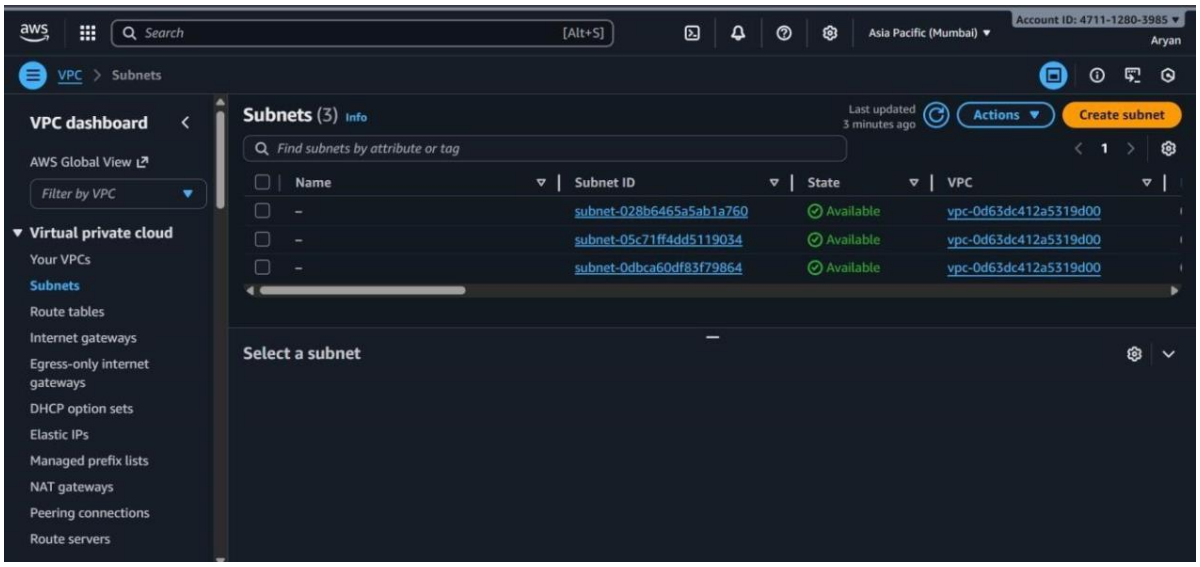


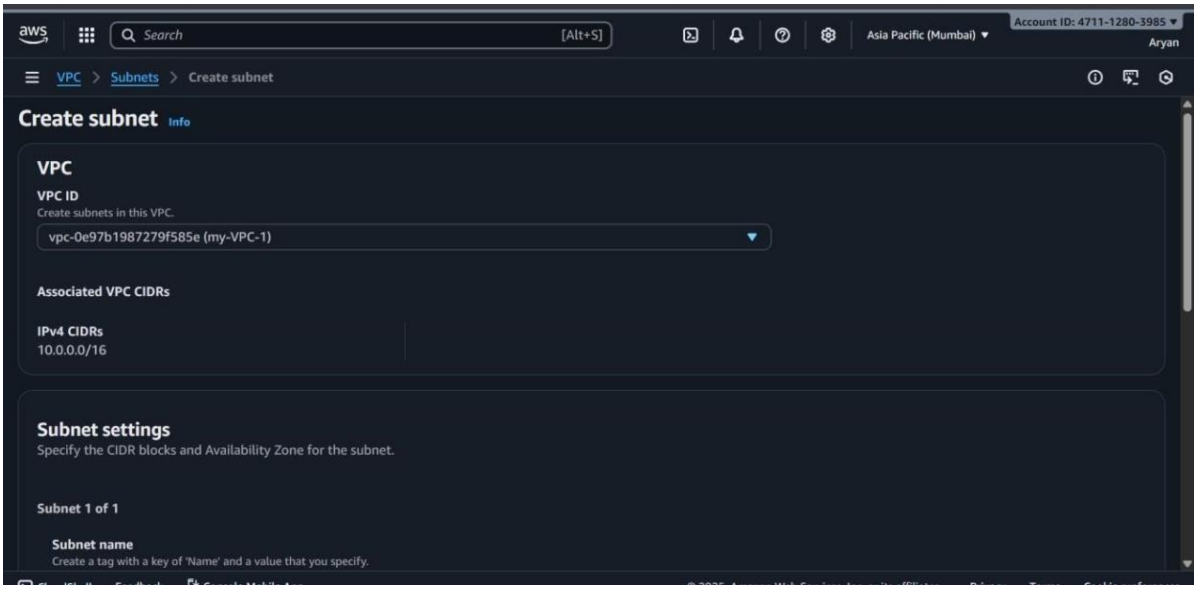
Step 5. Create Subnets

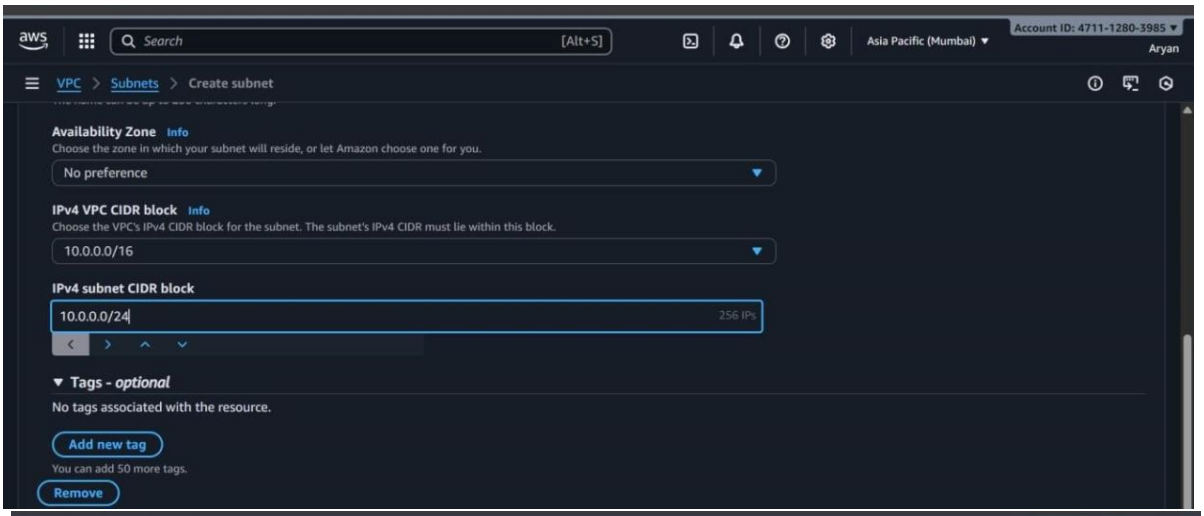
- On the left side, click **Subnets** → **Create subnet**.
- Select your **VPC**.
- Add at least **two subnets**: o Public → 10.0.1.0/24 o Private → 10.0.2.0/24
- Choose different **Availability Zones**.

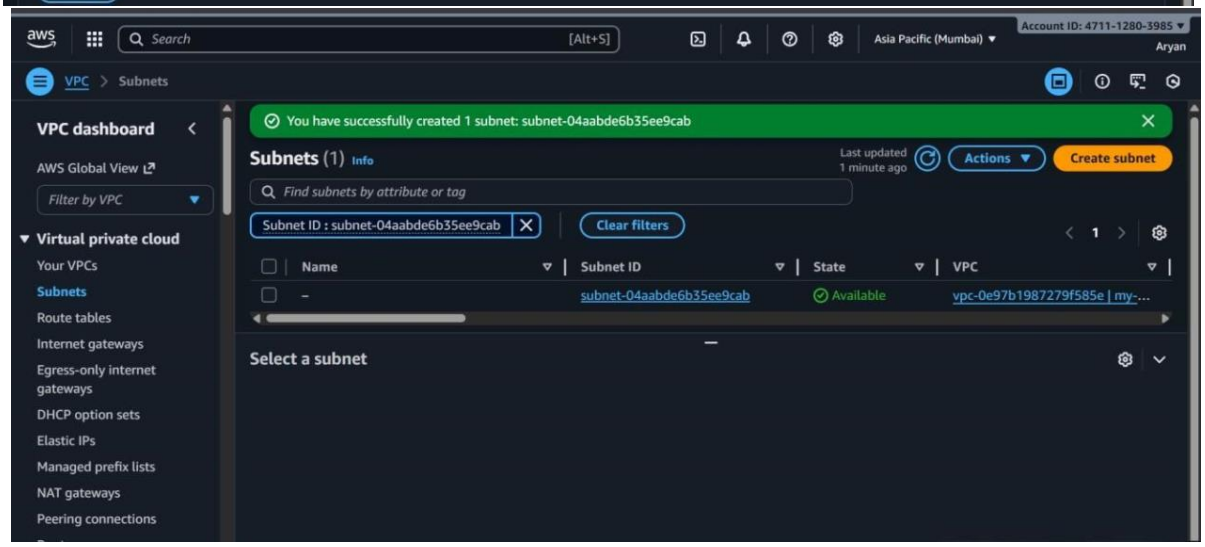
Click **Create Subnet**.




Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
VPC > Subnets
VPC dashboard
AWS 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
Route servers
Subnets (3) Info
Last updated 3 minutes ago
Actions
Create subnet
Find subnets by attribute or tag
Name
Subnet ID
State
VPC
subnet-028b6465a5ab1a760
Available
vpc-0d63dc412a5319d00
subnet-05c71ff4dd5119034
Available
vpc-0d63dc412a5319d00
subnet-0dbca60df83f79864
Available
vpc-0d63dc412a5319d00
Select a subnet

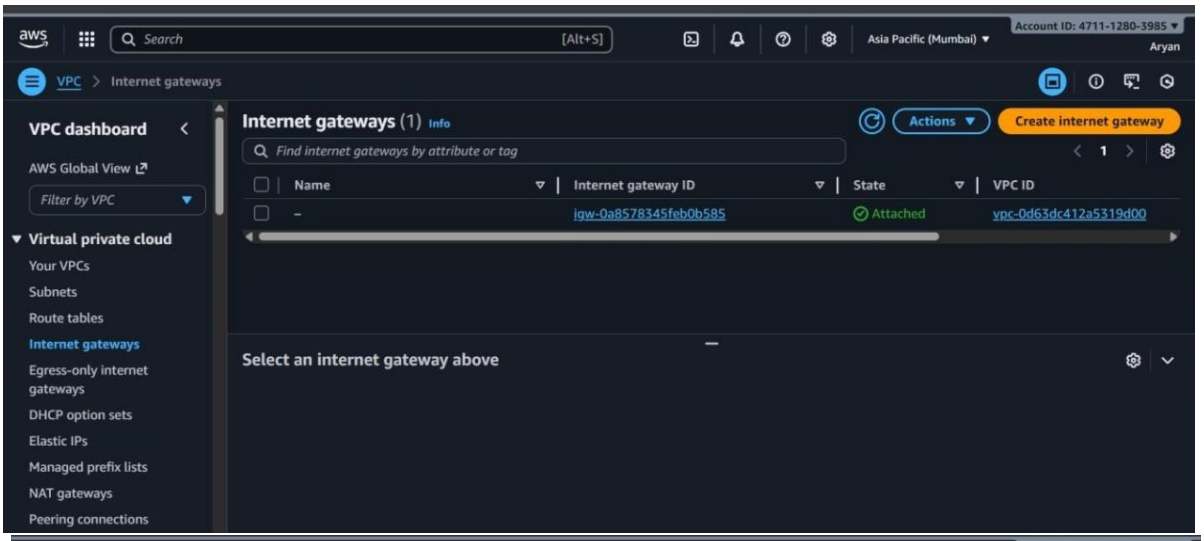

Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
VPC > Subnets > Create subnet
Create subnet Info
VPC
VPC ID
Create subnets in this VPC.
vpc-0e97b1987279f585e (my-VPC-1)
Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16
Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.

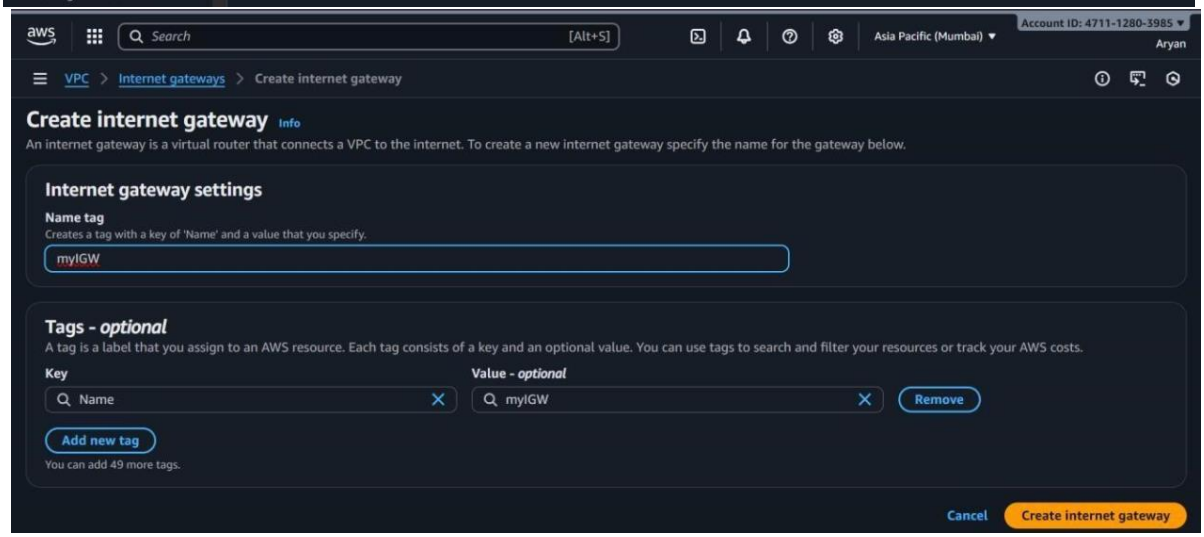


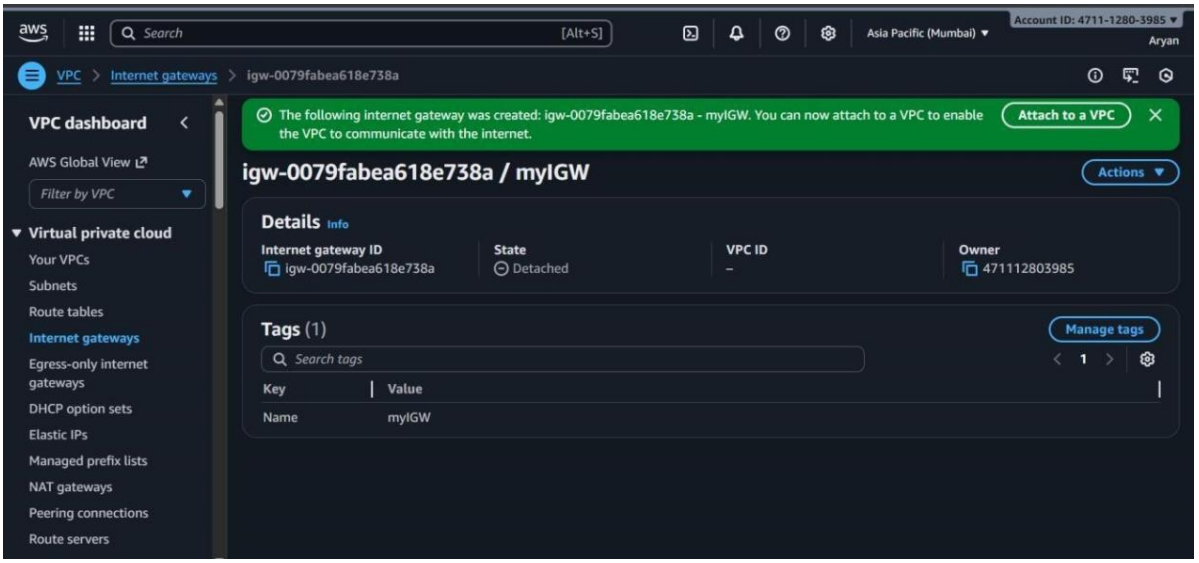


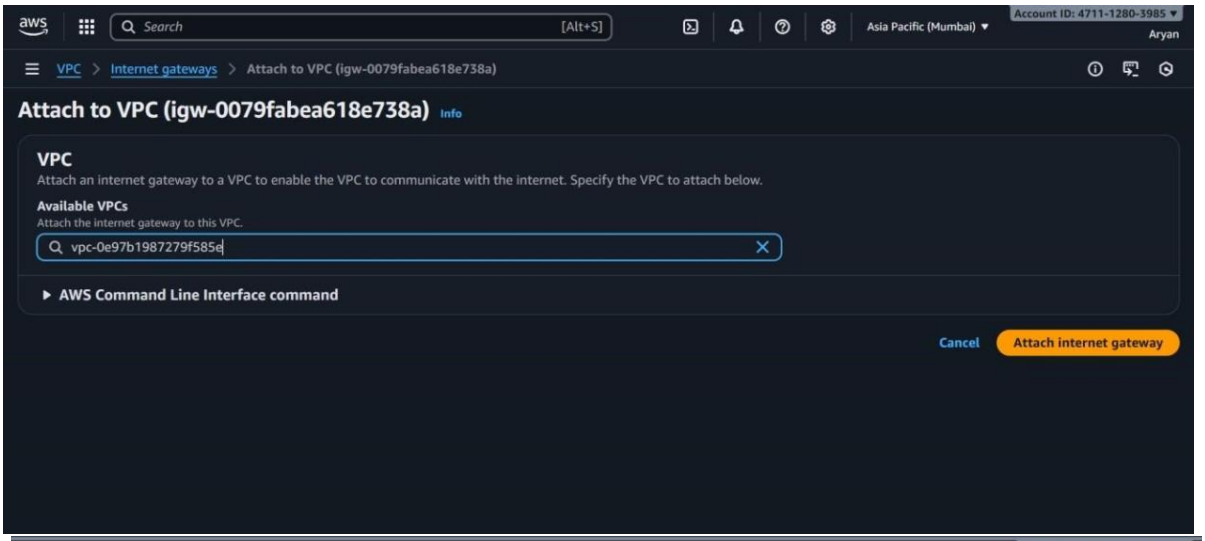
Step 6. Create an Internet Gateway (IGW)

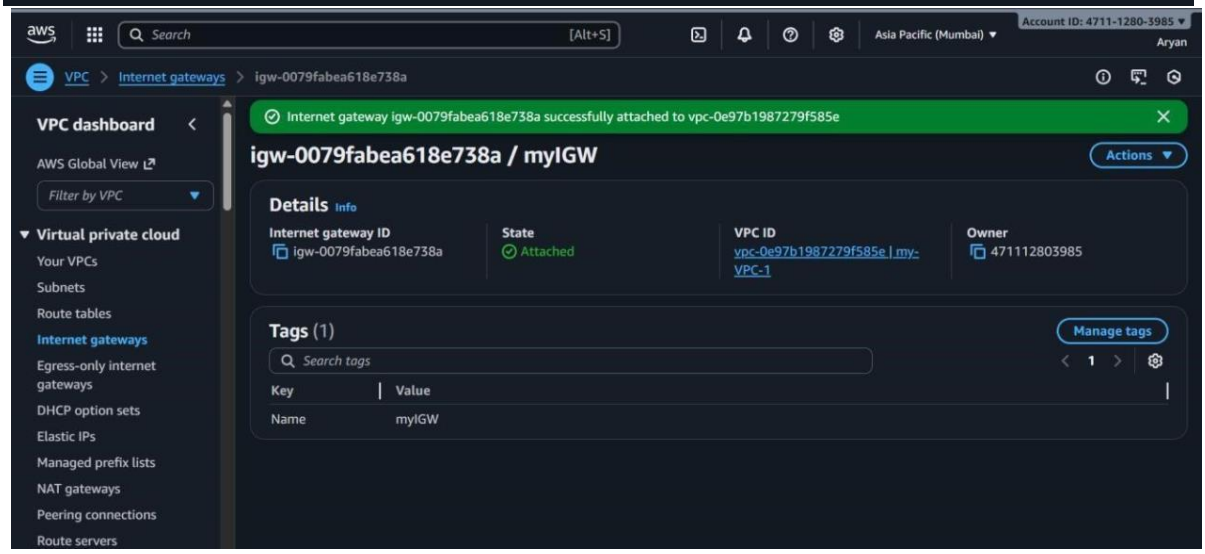
- Click **Internet Gateways** → **Create IGW**.
- Name it e.g., MyIGW.
- After creation, select it → click **Attach to VPC** → choose your **VPC**.


Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
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
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Internet gateways (1) Info
Actions
Create internet gateway
Find internet gateways by attribute or tag
Name
Internet gateway ID
State
VPC ID
igw-0a8578345feb0b585
Attached
vpc-0d63dc412a5319d00
Select an internet gateway above


Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
VPC > Internet gateways > Create internet gateway
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.
myIGW
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
Value - optional
Name
myIGW
Remove
Add new tag
You can add 49 more tags.
Cancel
Create internet gateway


Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
VPC > Internet gateways > igw-0079fabea618e738a
VPC dashboard
AWS 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
Route servers
The following internet gateway was created: igw-0079fabea618e738a - myIGW. You can now attach to a VPC to enable the VPC to communicate with the internet.
Attach to a VPC
igw-0079fabea618e738a / myIGW
Actions
Details Info
Internet gateway ID
igw-0079fabea618e738a
State
Detached
VPC ID
–
Owner
471112803985
Tags (1)
Manage tags
Search tags
Key
Value
Name
myIGW





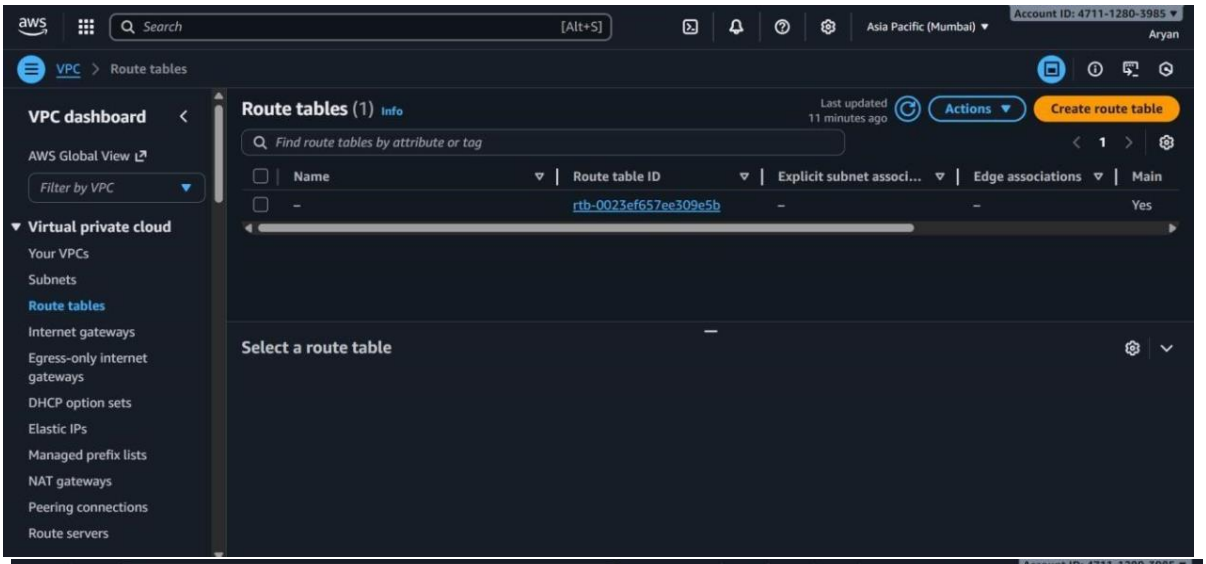
Step 7. Configure Route Tables

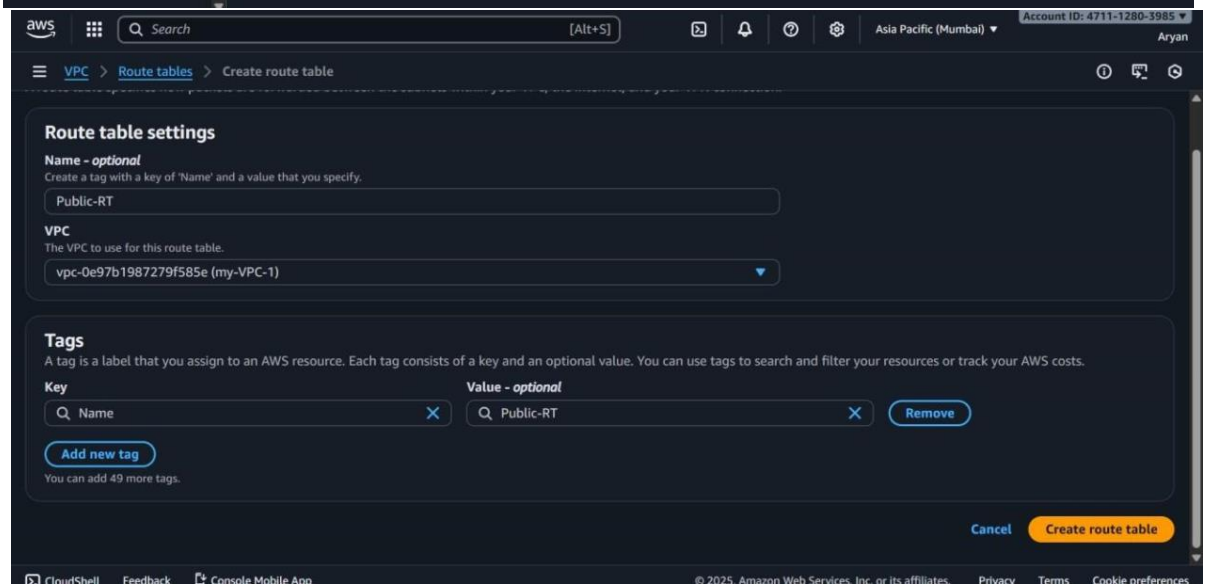
Public Route Table

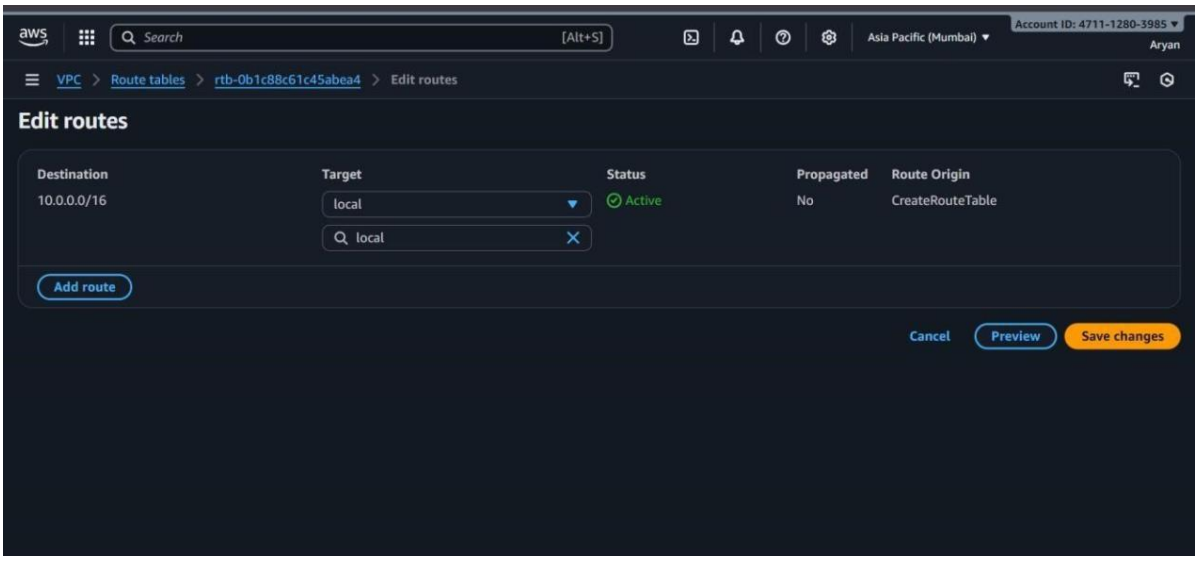
- Go to **Route Tables** → Create route table.
- Name: PublicRT.
- Select your VPC and create.
- Go to **Routes** → Edit → Add route:
  - Destination: 0.0.0.0/0
  - Target: **Internet Gateway**
- Go to **Subnet Associations** → Associate with **public subnet**.

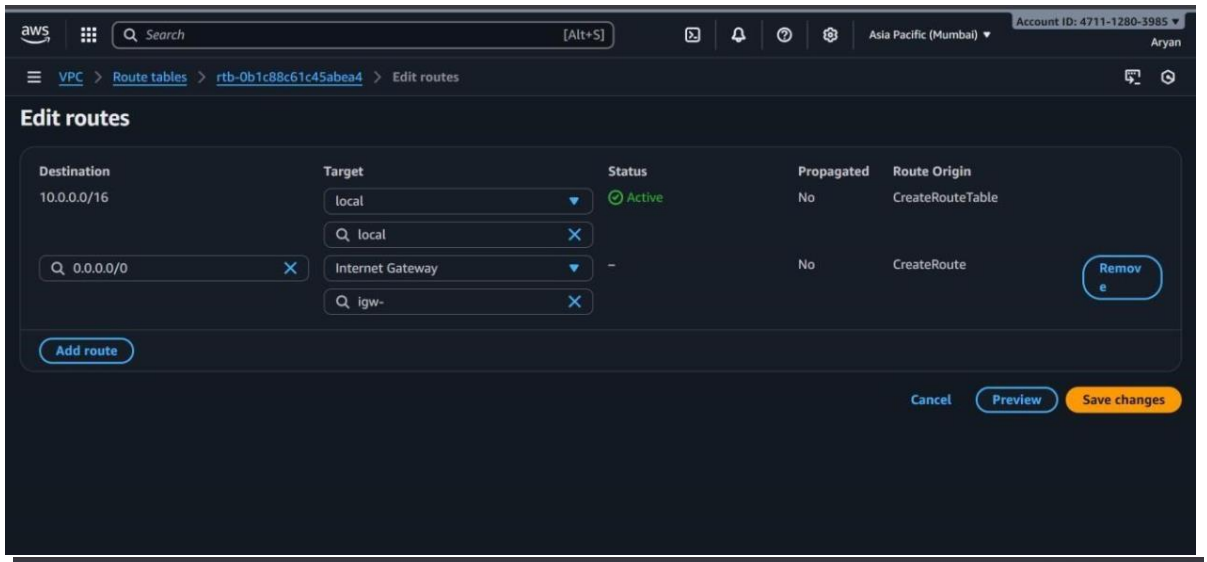
Private Route Table

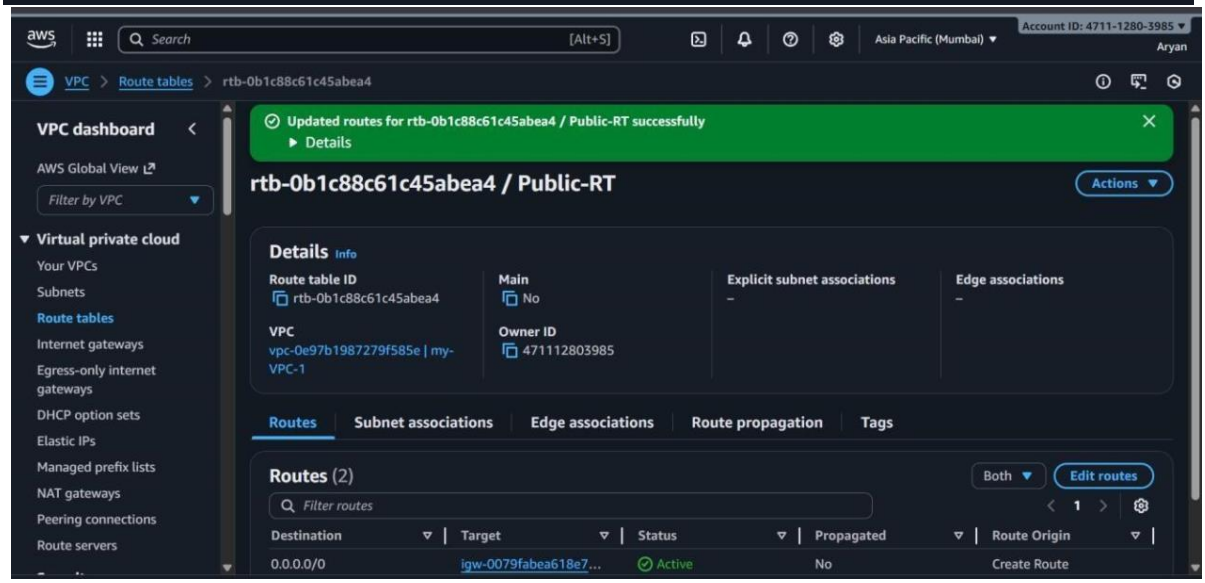
- Create another route table named PrivateRT.
- Associate it with **private subnet** (no internet route).

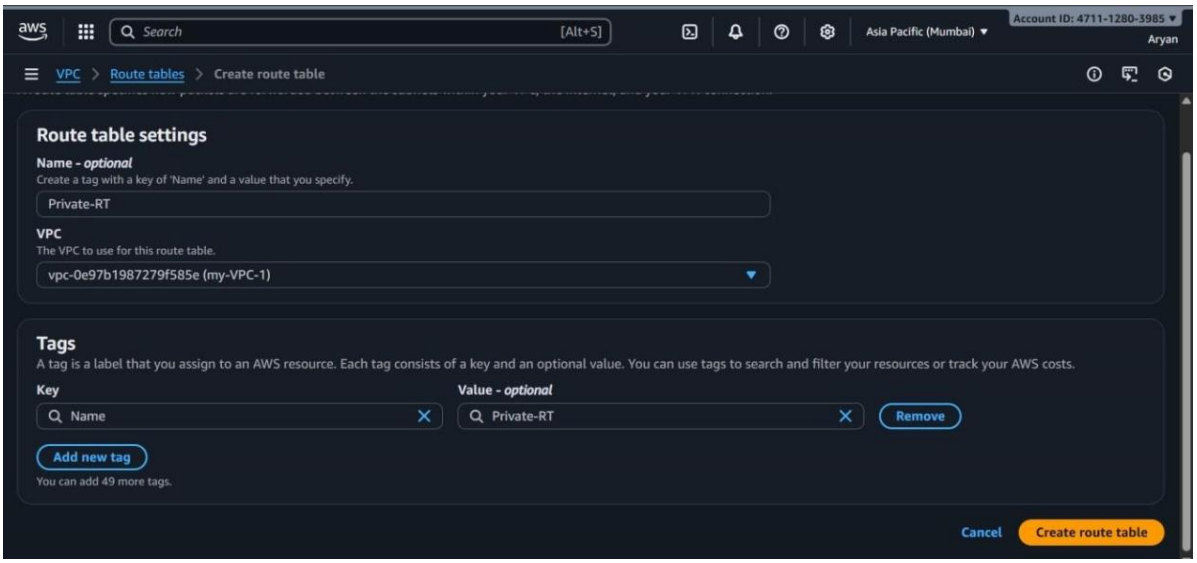

Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
VPC > Route tables
VPC dashboard
AWS Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers
Route tables (1) Info
Last updated 11 minutes ago
Actions
Create route table
Find route tables by attribute or tag
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
rtb-0023ef657ee309e5b
Yes
Select a route table

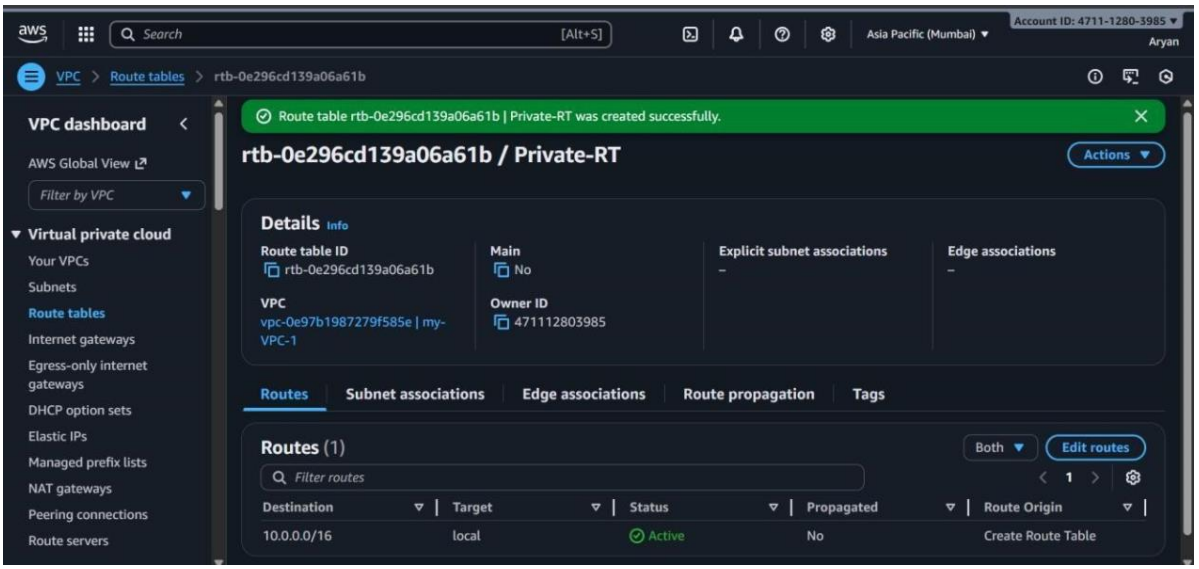

Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
VPC > Route tables > Create route table
Route table settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
Public-RT
VPC
The VPC to use for this route table.
vpc-0e97b1987279f585e (my-VPC-1)
Tags
A 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
Public-RT
Remove
Add new tag
You can add 49 more tags.
Cancel
Create route table
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
VPC > Route tables > rtb-0b1c88c61c45abea4 > 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


Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
VPC > Route tables > rtb-0b1c88c61c45abea4 > 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-
Add route
Cancel
Preview
Save changes

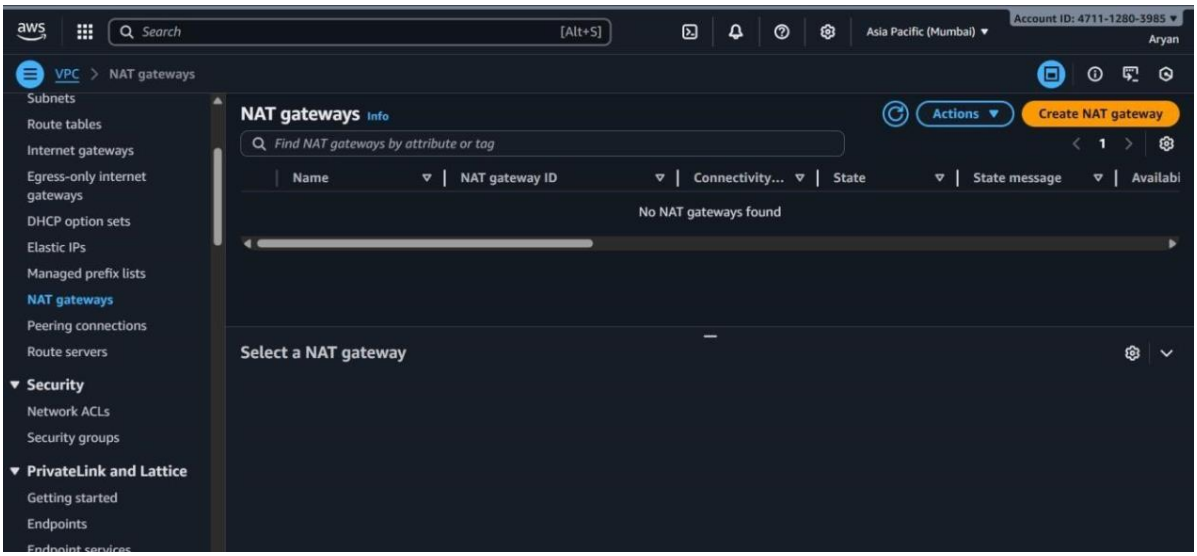

Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
VPC > Route tables > rtb-0b1c88c61c45abea4
VPC dashboard
AWS Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers
Updated routes for rtb-0b1c88c61c45abea4 / Public-RT successfully
Details
rtb-0b1c88c61c45abea4 / Public-RT
Actions
Details Info
Route table ID
rtb-0b1c88c61c45abea4
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-0e97b1987279f585e | my-VPC-1
Owner ID
471112803985
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
1
Destination
Target
Status
Propagated
Route Origin
0.0.0.0/0
igw-0079fabea618e7...
Active
No
Create Route

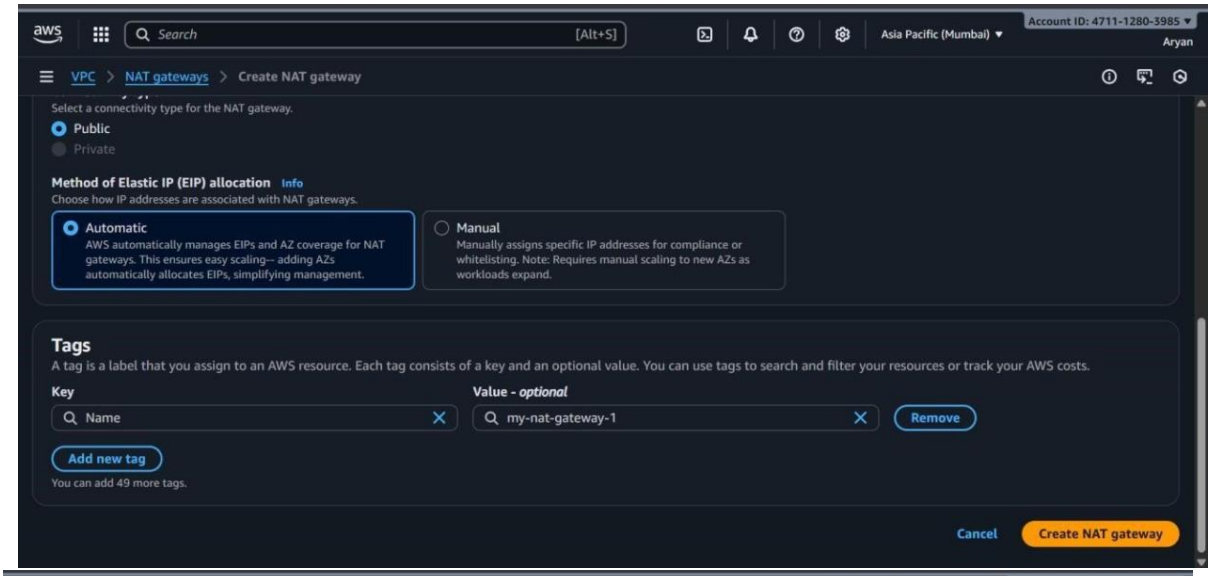


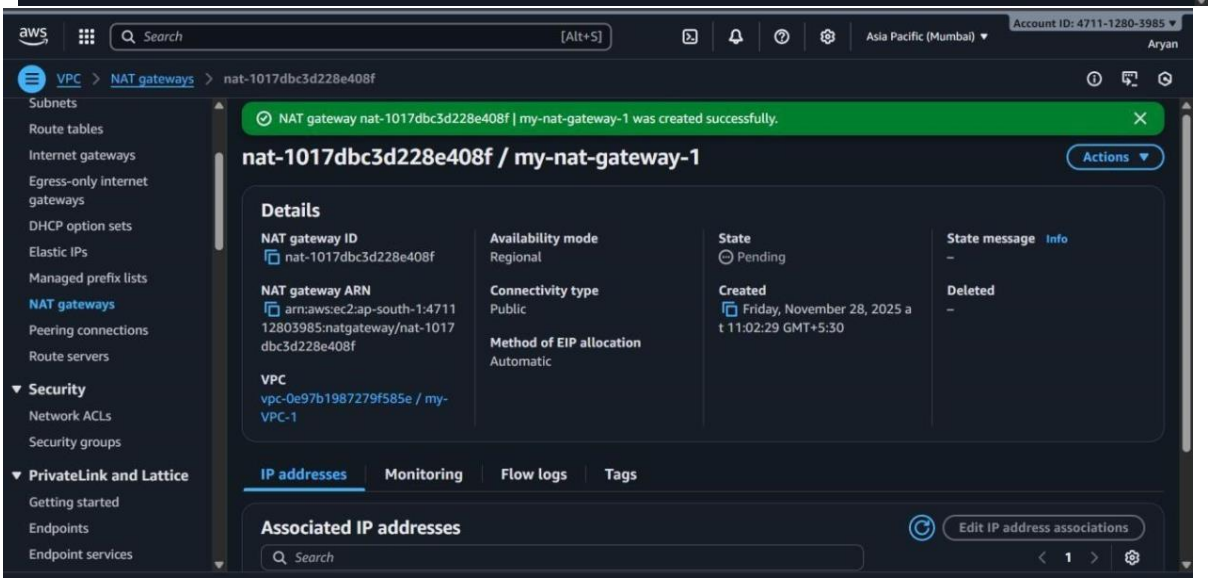


Step 8. Create a NAT Gateway (Optional for private subnet internet)

- Go to **NAT Gateways** → Create NAT Gateway.
- Select:
  - Subnet: **Public subnet**
  - Allocate Elastic IP
- Update **PrivateRT → Routes** to:
  - Destination: 0.0.0.0/0
  - Target: **NAT Gateway**


Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
VPC > NAT gateways
Subnets
Route tables
Internet gateways
Egress-only internet 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
NAT gateways Info
Actions
Create NAT gateway
Find NAT gateways by attribute or tag
Name
NAT gateway ID
Connectivity...
State
State message
Availabi
No NAT gateways found
Select a NAT gateway


Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
VPC > NAT gateways > Create NAT gateway
Select a connectivity type for the NAT gateway.
Public
Private
Method of Elastic IP (EIP) allocation Info
Choose how IP addresses are associated with NAT gateways.
Automatic
AWS automatically manages EIPs and AZ coverage for NAT gateways. This ensures easy scaling-- adding AZs automatically allocates EIPs, simplifying management.
Manual
Manually assigns specific IP addresses for compliance or whitelisting. Note: Requires manual scaling to new AZs as workloads expand.
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
my-nat-gateway-1
Remove
Add new tag
You can add 49 more tags.
Cancel
Create NAT gateway


Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 4711-1280-3985
Aryan
VPC > NAT gateways > nat-1017dbc3d228e408f
Subnets
Route tables
Internet gateways
Egress-only internet 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
NAT gateway nat-1017dbc3d228e408f | my-nat-gateway-1 was created successfully.
nat-1017dbc3d228e408f / my-nat-gateway-1
Actions
Details
NAT gateway ID
nat-1017dbc3d228e408f
NAT gateway ARN
arn:aws:ec2:ap-south-1:471112803985:natgateway/nat-1017dbc3d228e408f
VPC
vpc-0e97b1987279f585e / my-VPC-1
Availability mode
Regional
Connectivity type
Public
Method of EIP allocation
Automatic
State
Pending
Created
Friday, November 28, 2025 at 11:02:29 GMT+5:30
State message Info
-
Deleted
-
IP addresses
Monitoring
Flow logs
Tags
Associated IP addresses
Edit IP address associations
Search