Karan(2301410015)

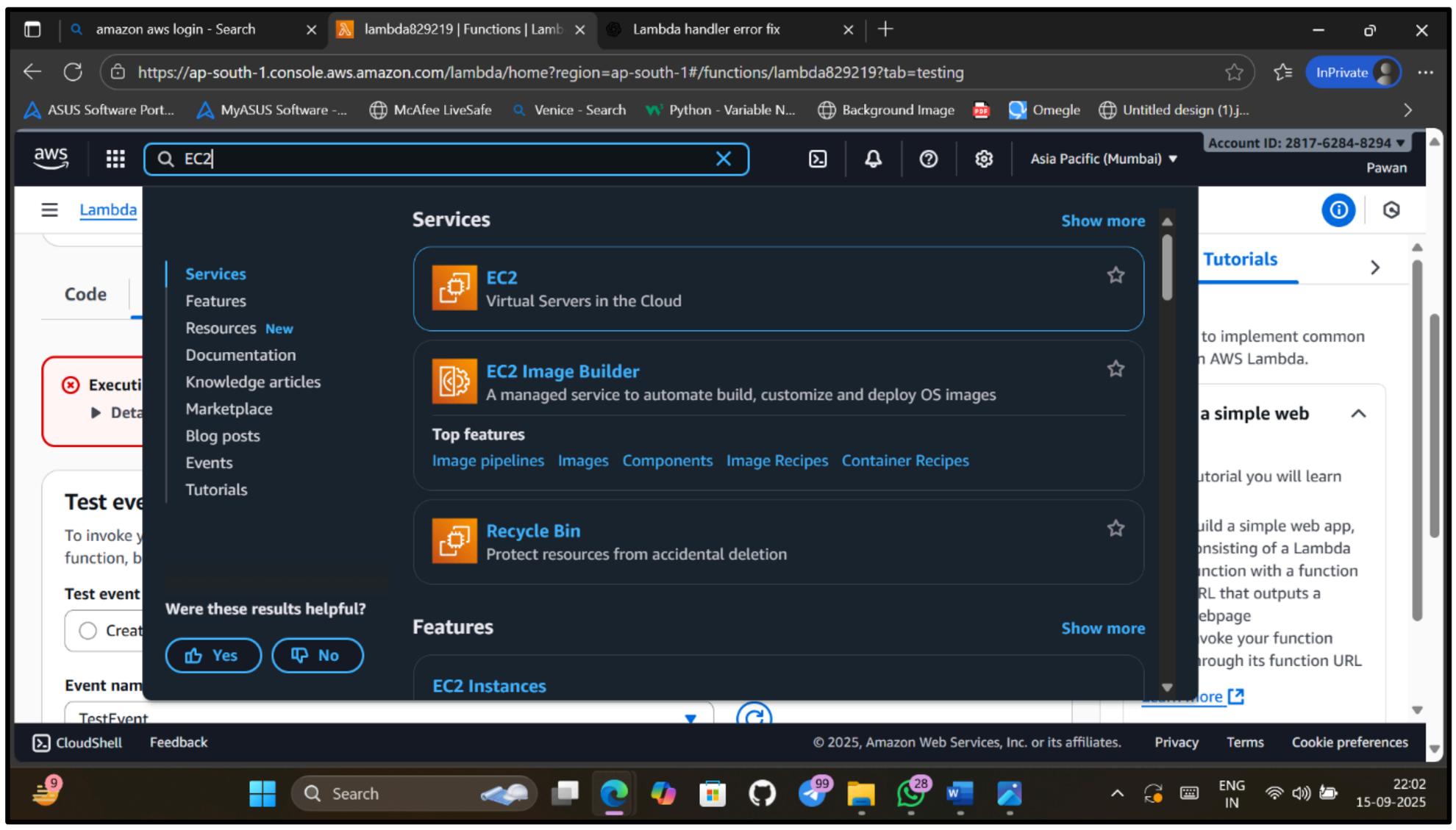
B.Tech CSE (Cyber security)

AWS CLOUD LAB ASSIGNMENT

1. Create a EC2 instance in Amazon AWS

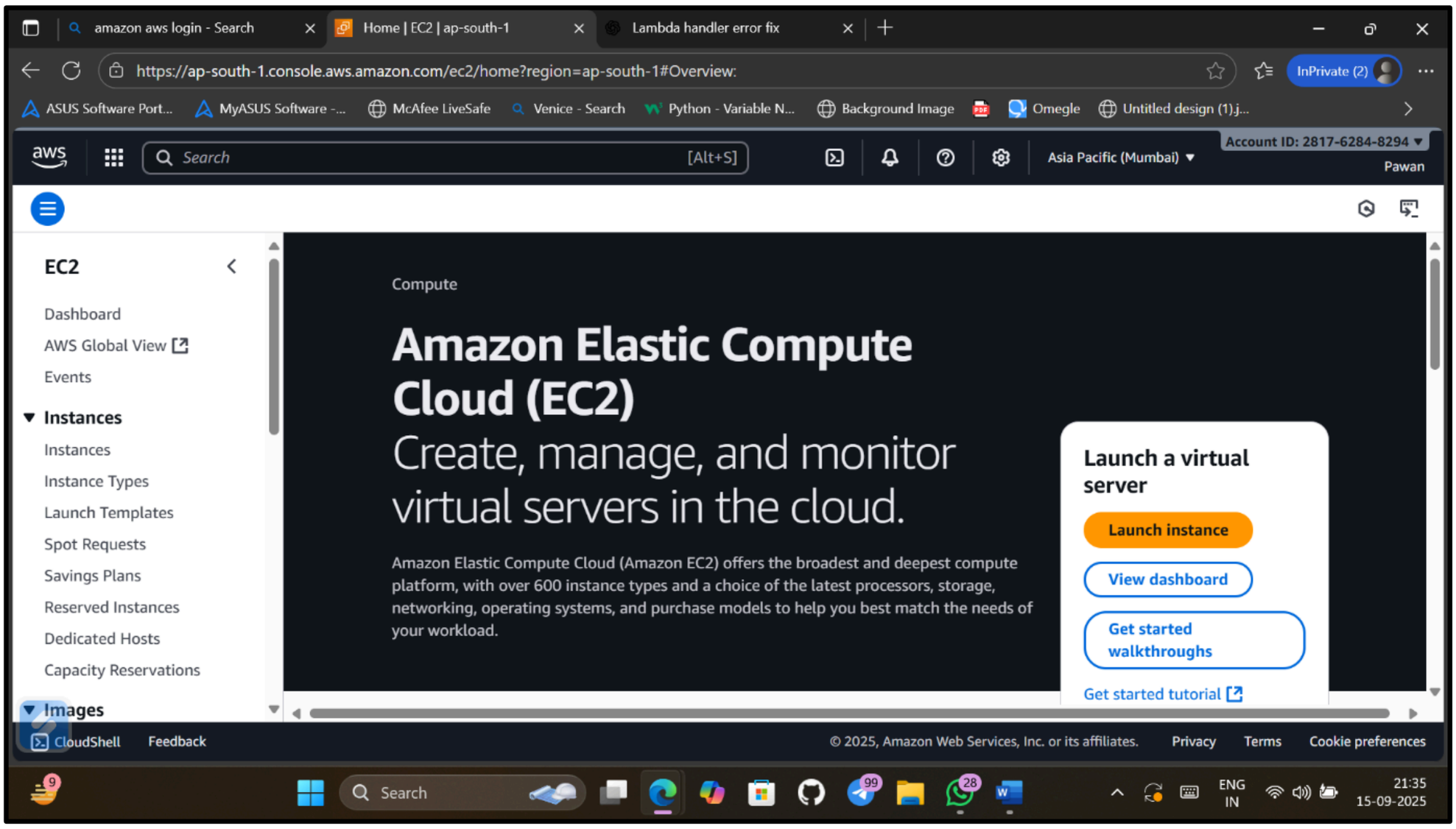
Step -1 Navigate to the EC2 Dashboard

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.



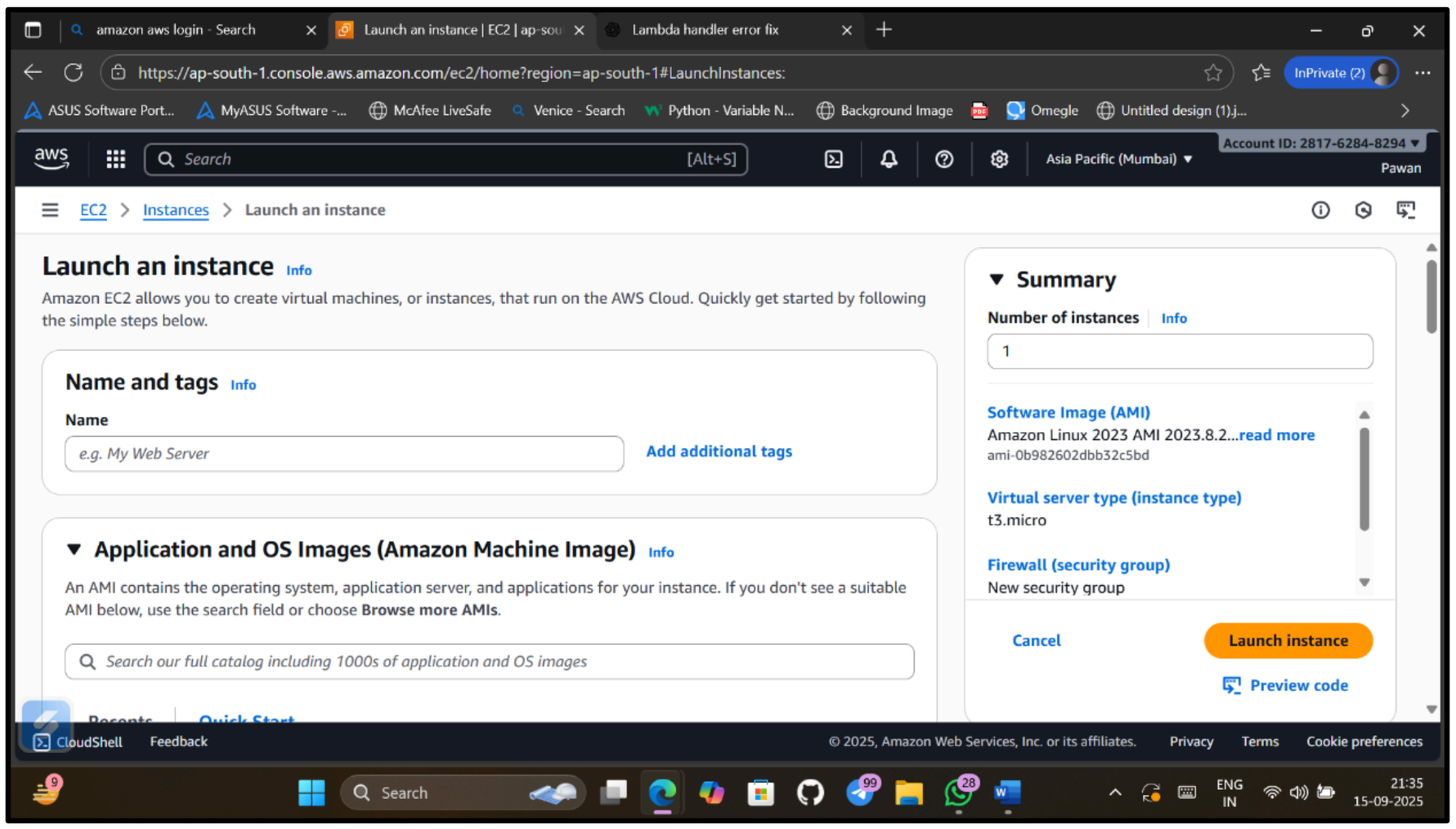
Step -2 Launch an Instance

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

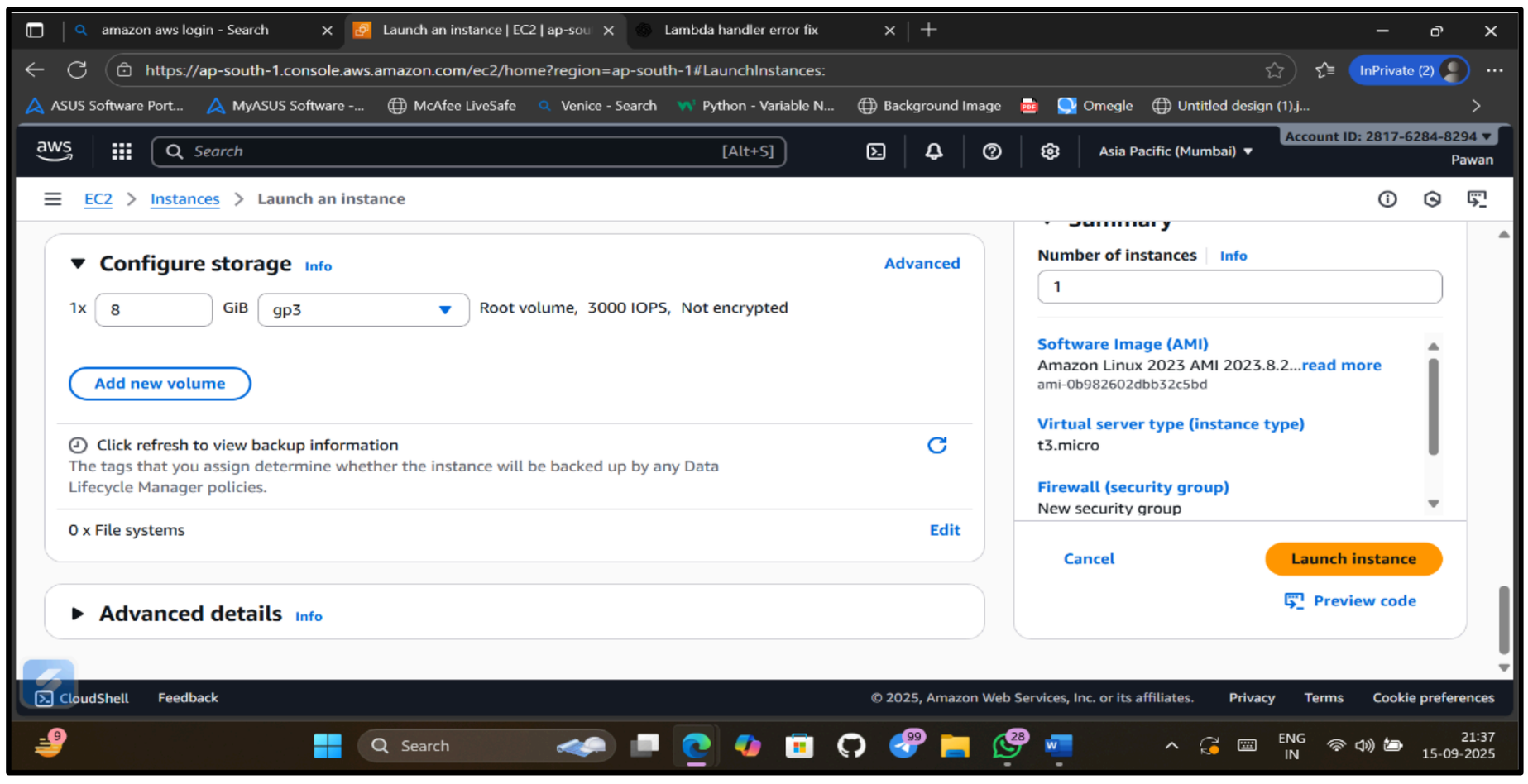
An instance type determines the CPU, memory, storage, and networking capacity of your instance. For most basic use cases, the t2.micro or t3.micro instance types are a great choice as they are free tier eligible.

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,

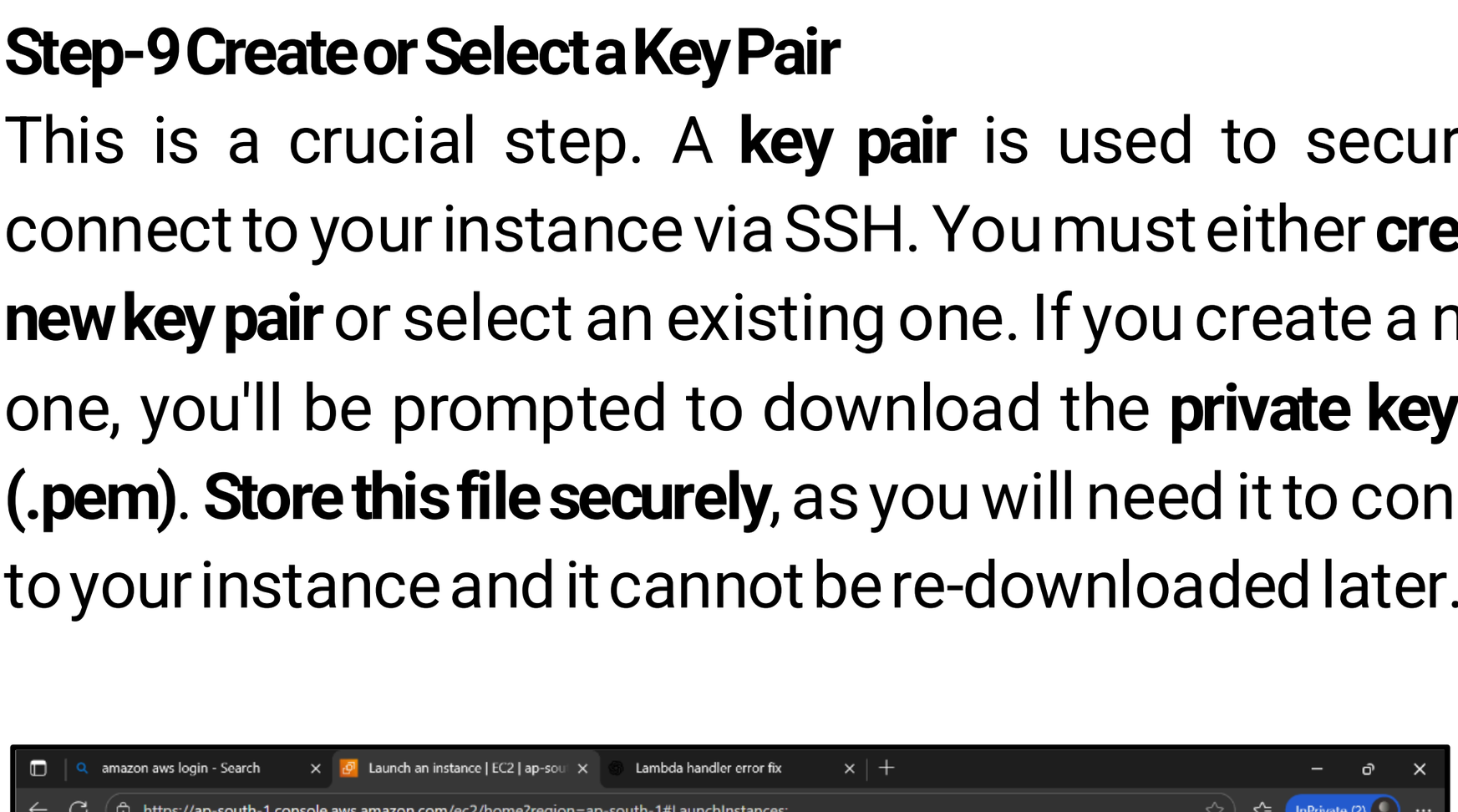
controlling inbound and outbound traffic. You can create a new security group or use an existing one. For a basic web server, you'll need to allow inbound traffic on port 80 (HTTP) and port 22 (SSH) to connect to the instance.

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

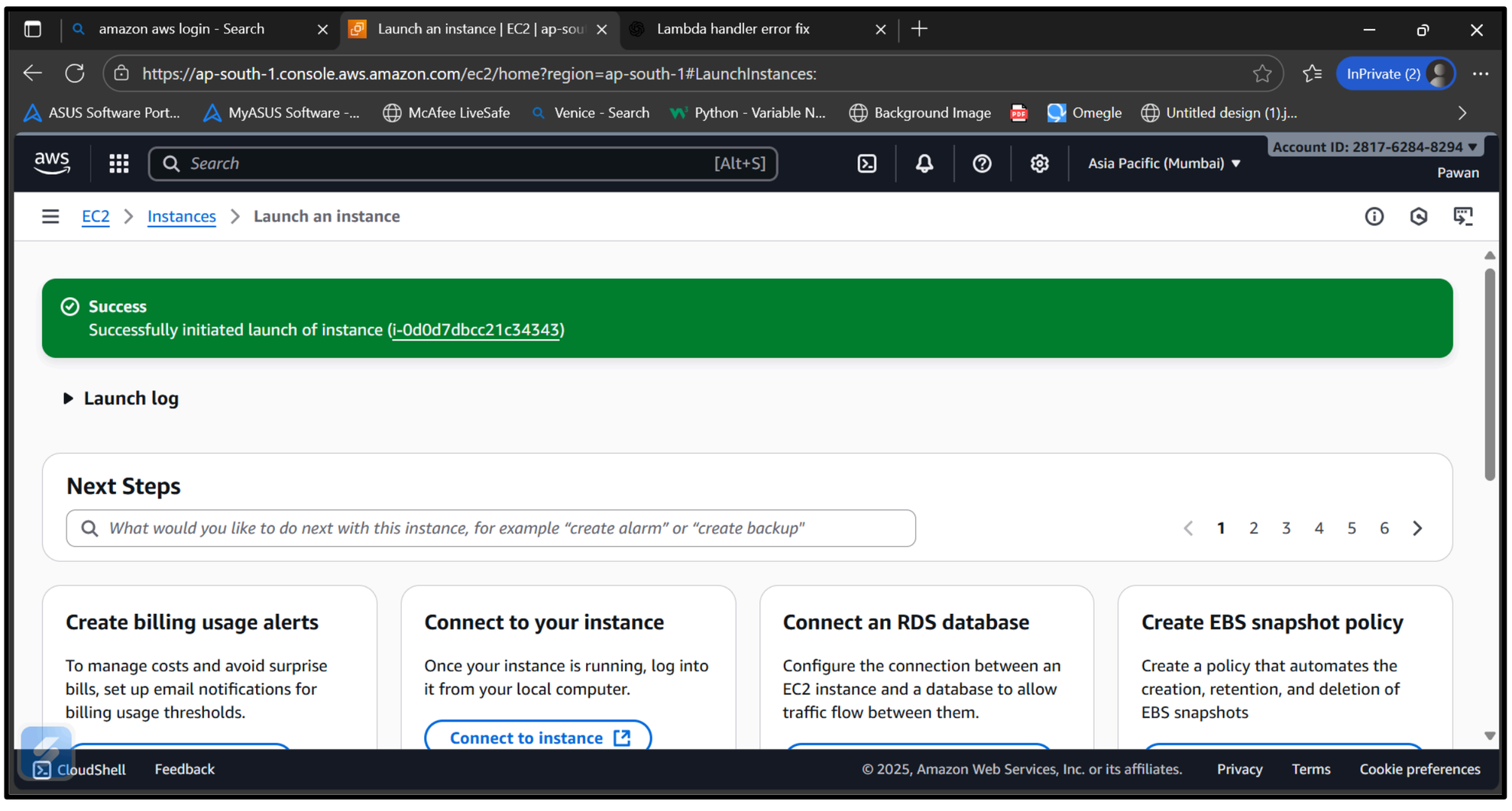
This is a crucial step. A **key pair** is used to securely connect to your instance via SSH. You must either **create a new key pair** or select an existing one. If you create a new one, you'll be prompted to download the **private key file (.pem)**. **Store this file securely**, as you will need it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

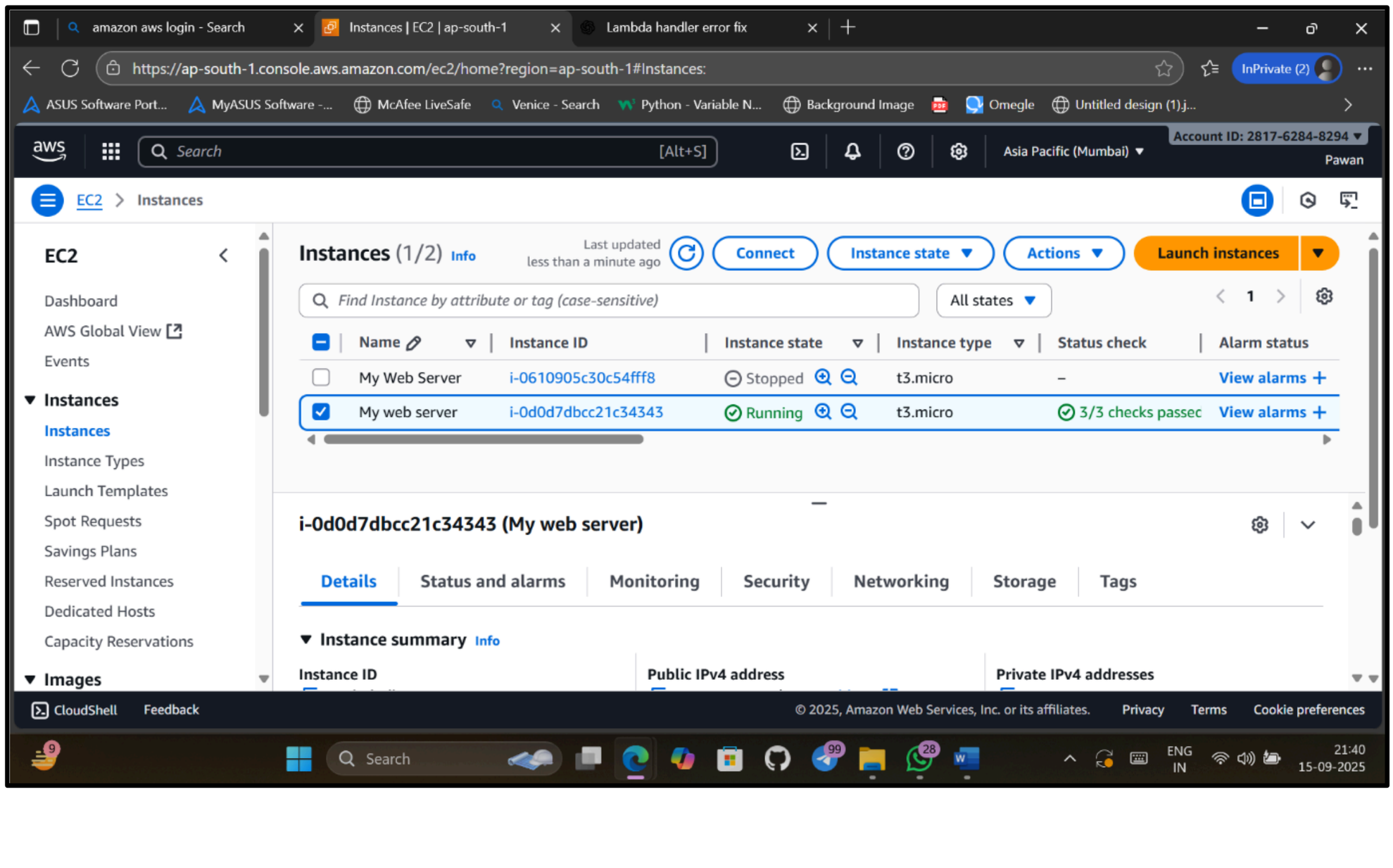


Step-10 Launch the Instance

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.





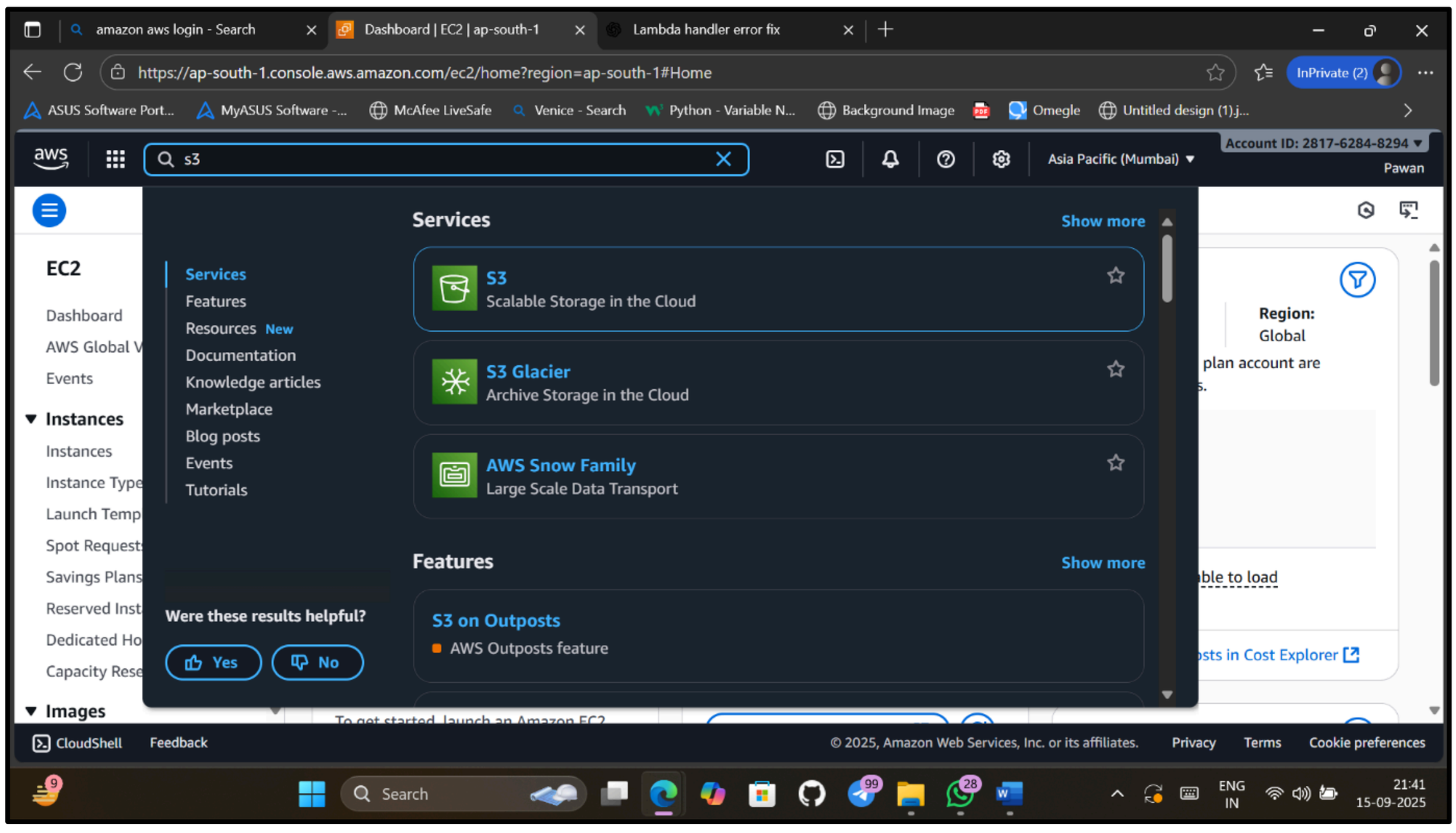
2. Create an S3 Bucket in AWS

1. Log in to AWS Management Console

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

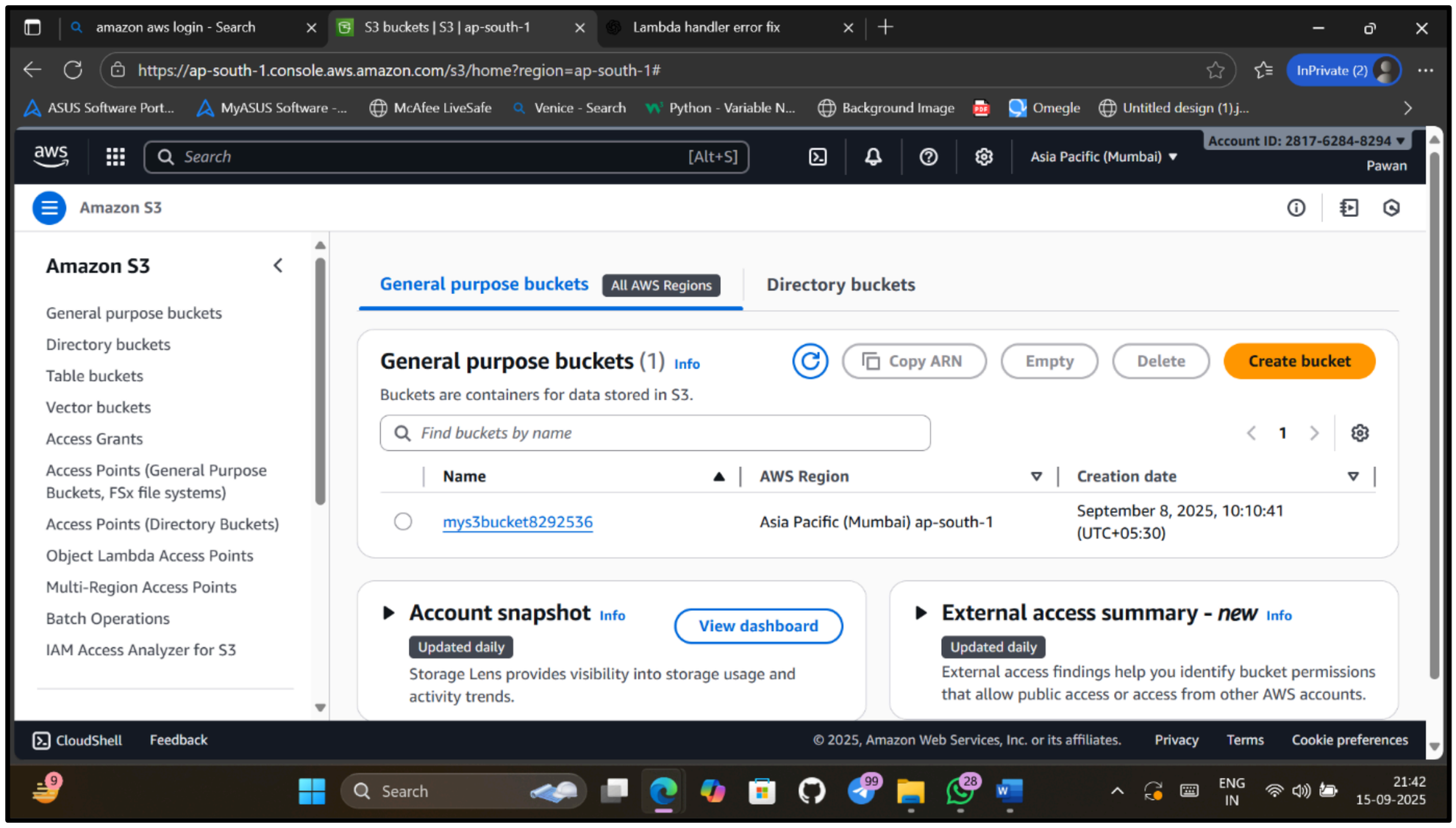
2. Navigate to S3

- 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.

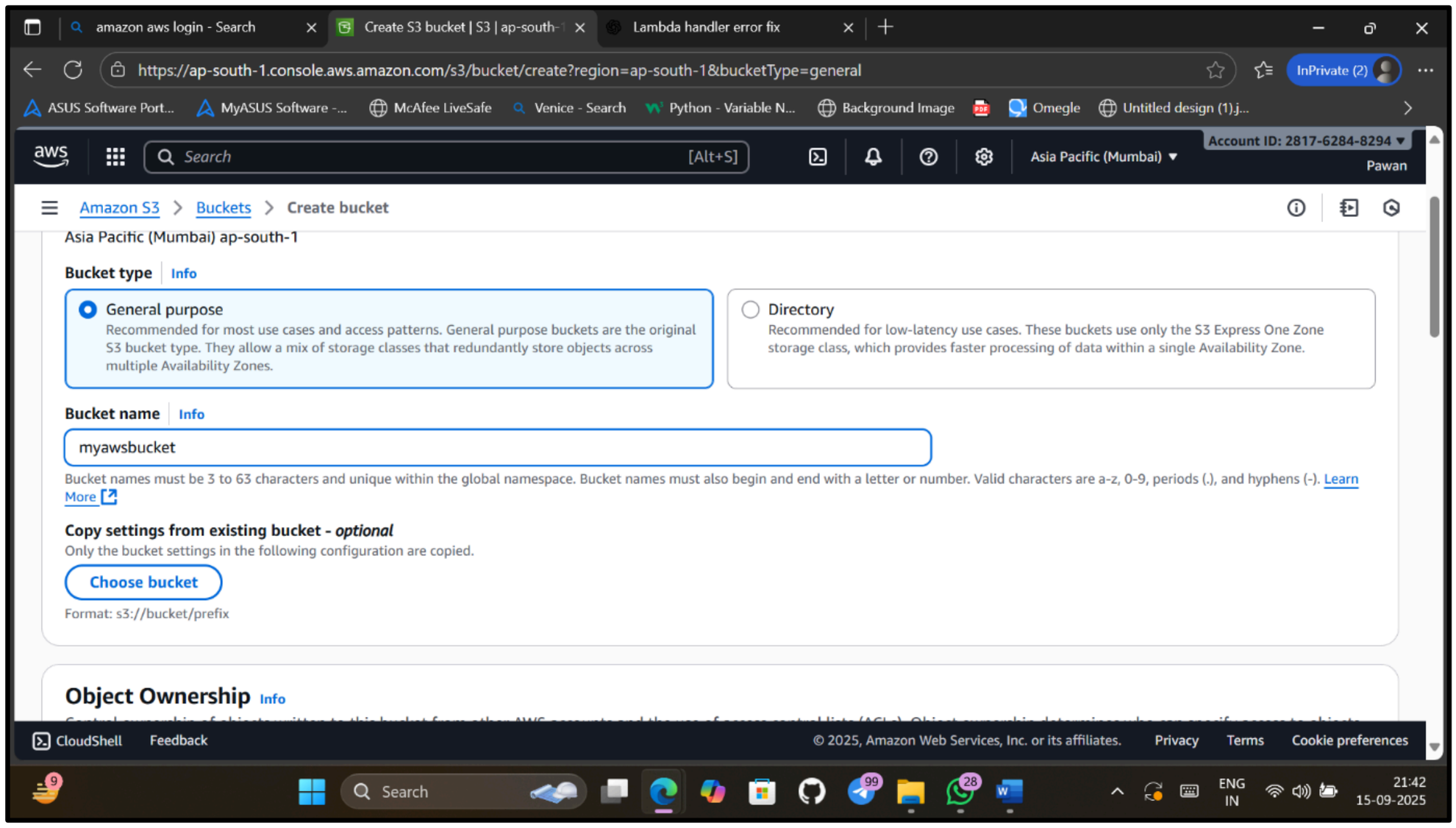


4. Configure Bucket Settings

- **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.

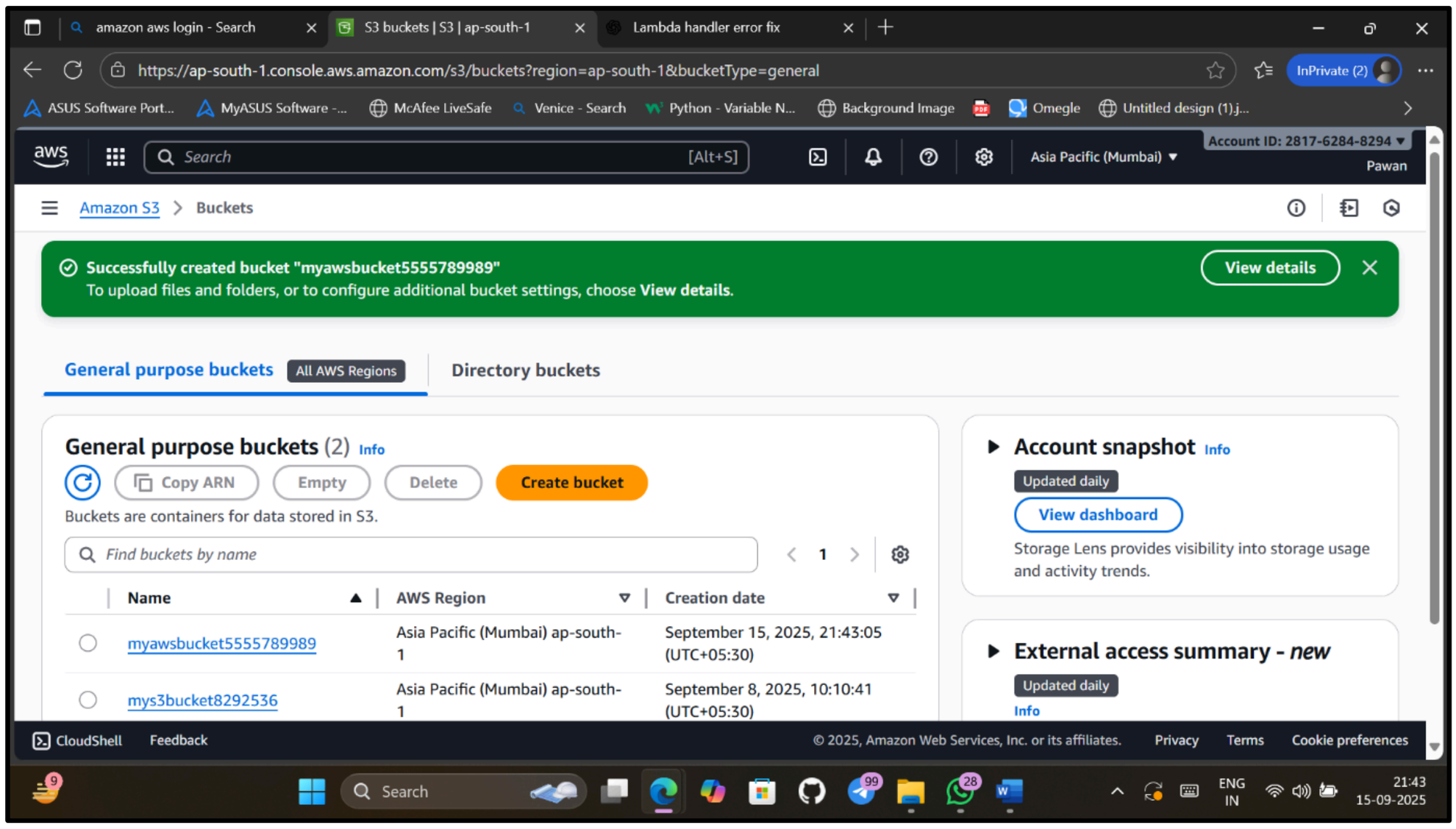
6. Configure Bucket Settings (Optional)

- **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.

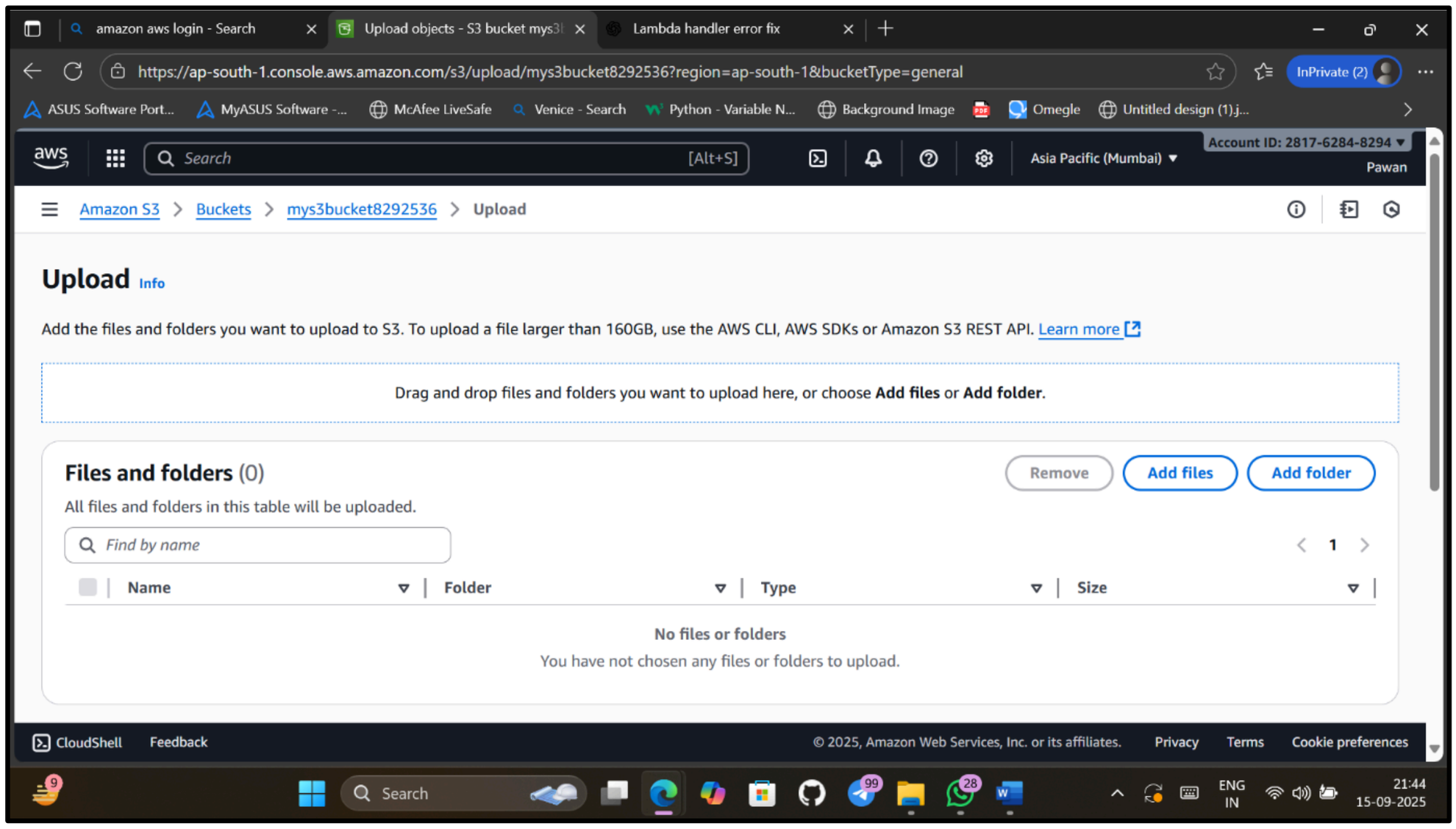
7. Review and Create

- 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**.


amazon aws login - Search
Upload objects - S3 bucket mys3
Lambda handler error fix
https://ap-south-1.console.aws.amazon.com/s3/upload/mys3bucket8292536?region=ap-south-1&bucketType=general
InPrivate (2)
ASUS Software Port...
MyASUS Software -...
McAfee LiveSafe
Venice - Search
Python - Variable N...
Background Image
Omegle
Untitled design (1).j...
aws
Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 2817-6284-8294
Pawan
Amazon S3 > Buckets > mys3bucket8292536 > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (0)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
1
Name
Folder
Type
Size
No files or folders
You have not chosen any files or folders to upload.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
21:44
15-09-2025

amazon aws login - Search
mys3bucket8292536 - S3 bucket
Lambda handler error fix
https://ap-south-1.console.aws.amazon.com/s3/buckets/mys3bucket8292536?region=ap-south-1&bucketType=general&tab=objects
InPrivate (2)
ASUS Software Port...
MyASUS Software -...
McAfee LiveSafe
Venice - Search
Python - Variable N...
Background Image
Omegle
Untitled design (1).j...
aws
Search
[Alt+S]
Asia Pacific (Mumbai)
Account ID: 2817-6284-8294
Pawan
Amazon S3 > Buckets > mys3bucket8292536
mys3bucket8292536 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (1)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Find objects by prefix
Show versions
1
Name
Type
Last modified
Size
Storage class
Resume (1).pdf
pdf
September 8, 2025, 10:11:23 (UTC+05:30)
46.8 KB
Standard
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
21:44
15-09-2025

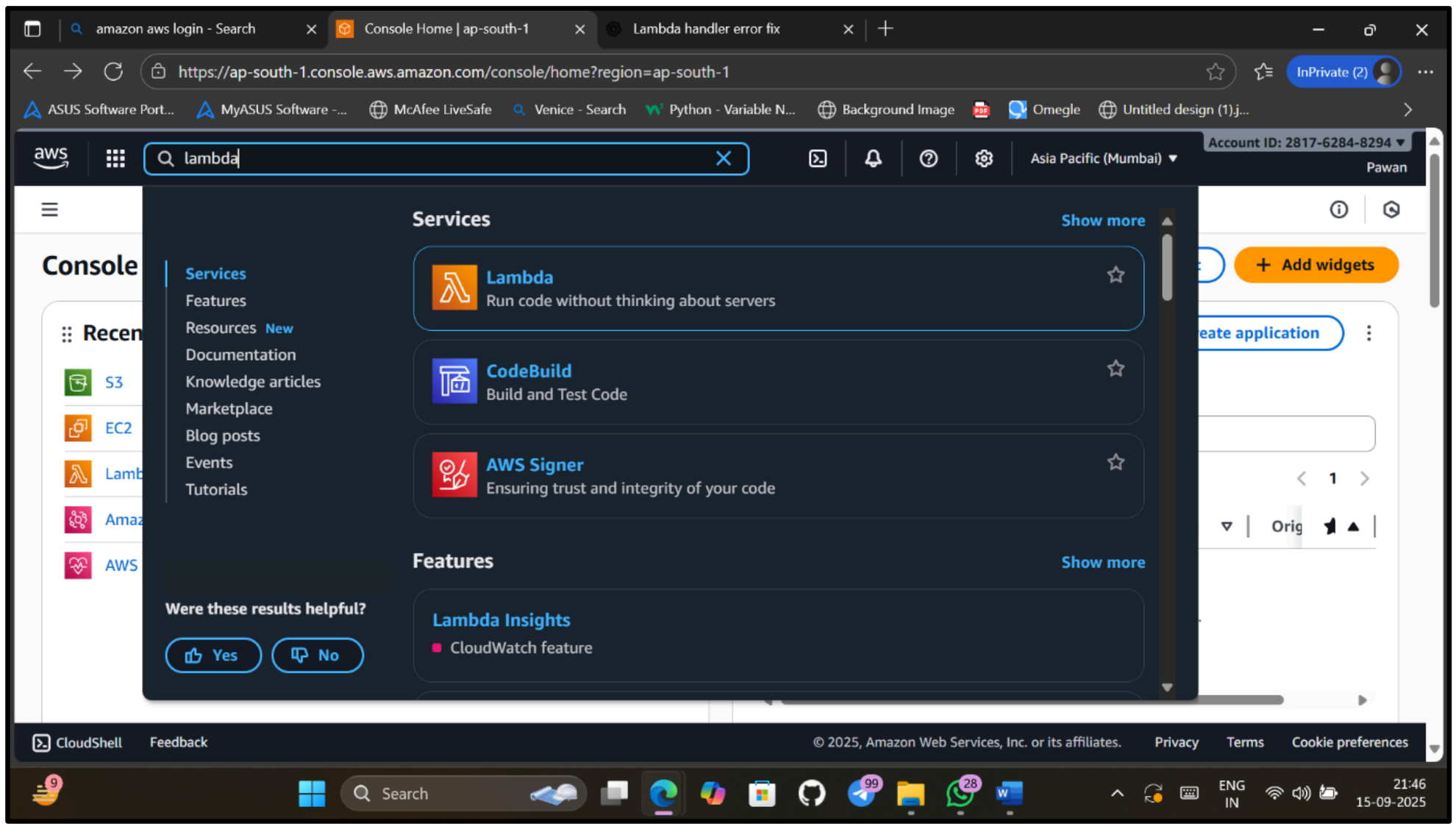
3. Steps to Create an AWS Lambda Function

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

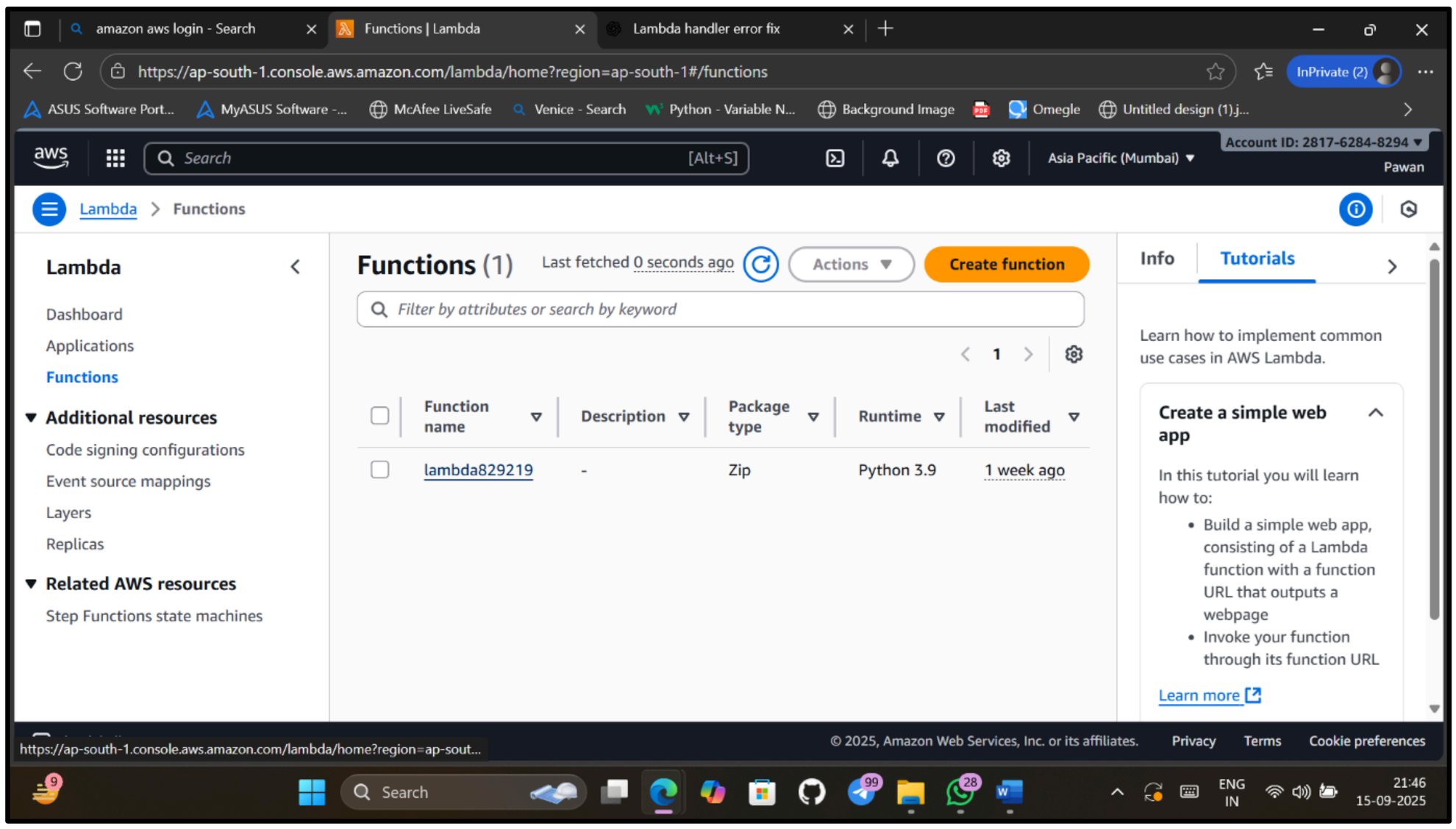
- Click **Create function**.

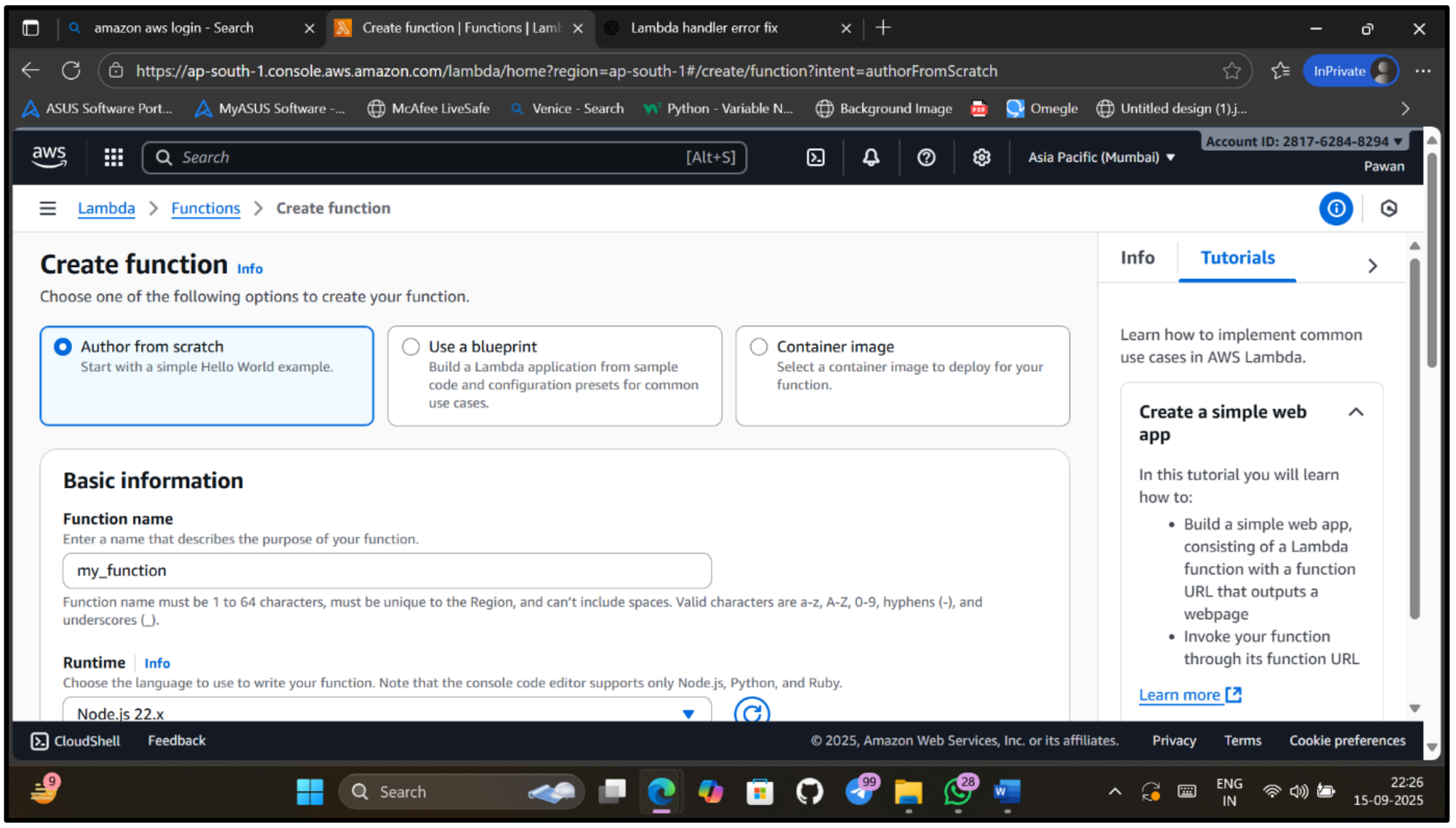
4. Choose a Creation Method

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.

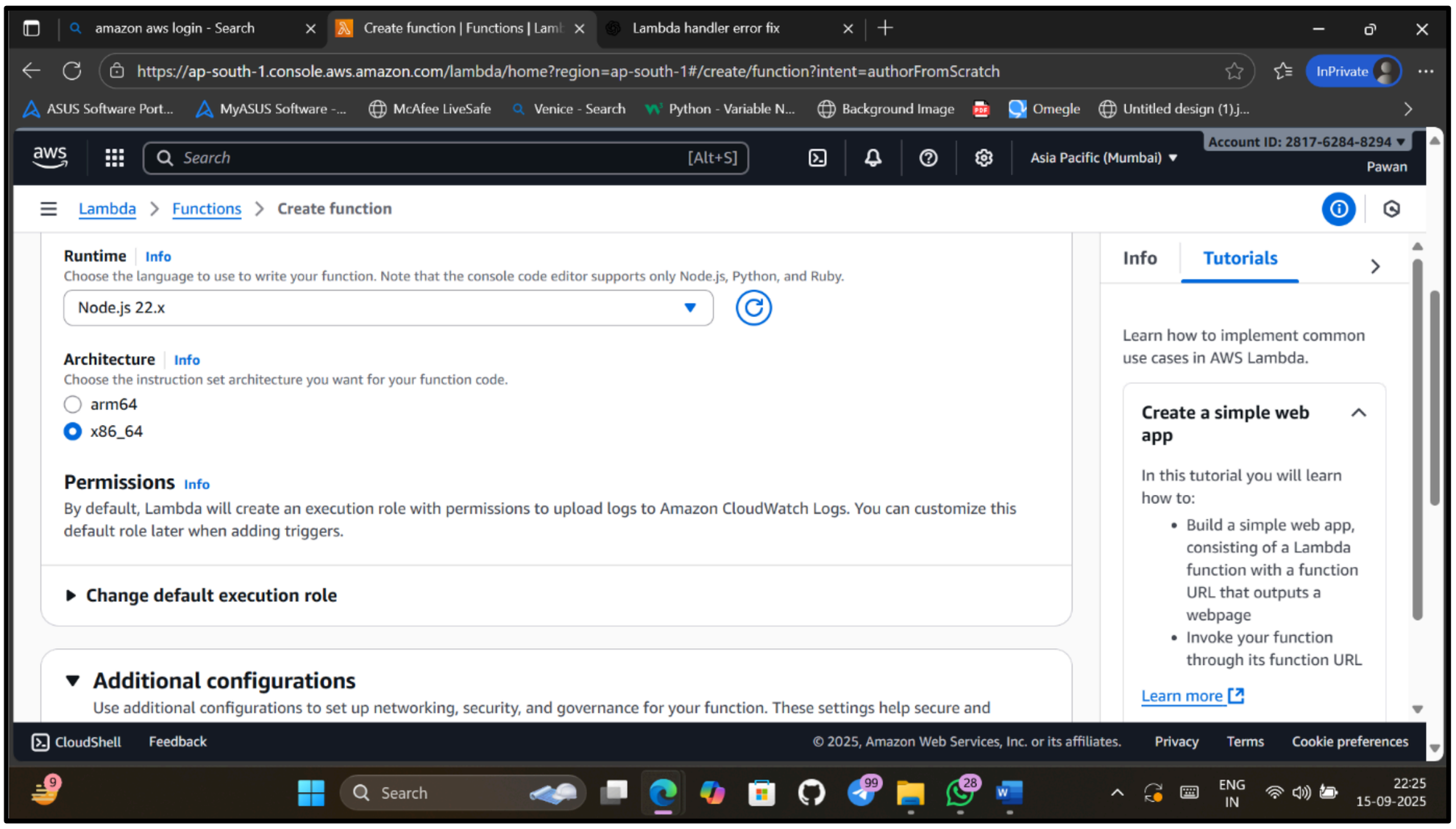
👉Select **Author from scratch**.



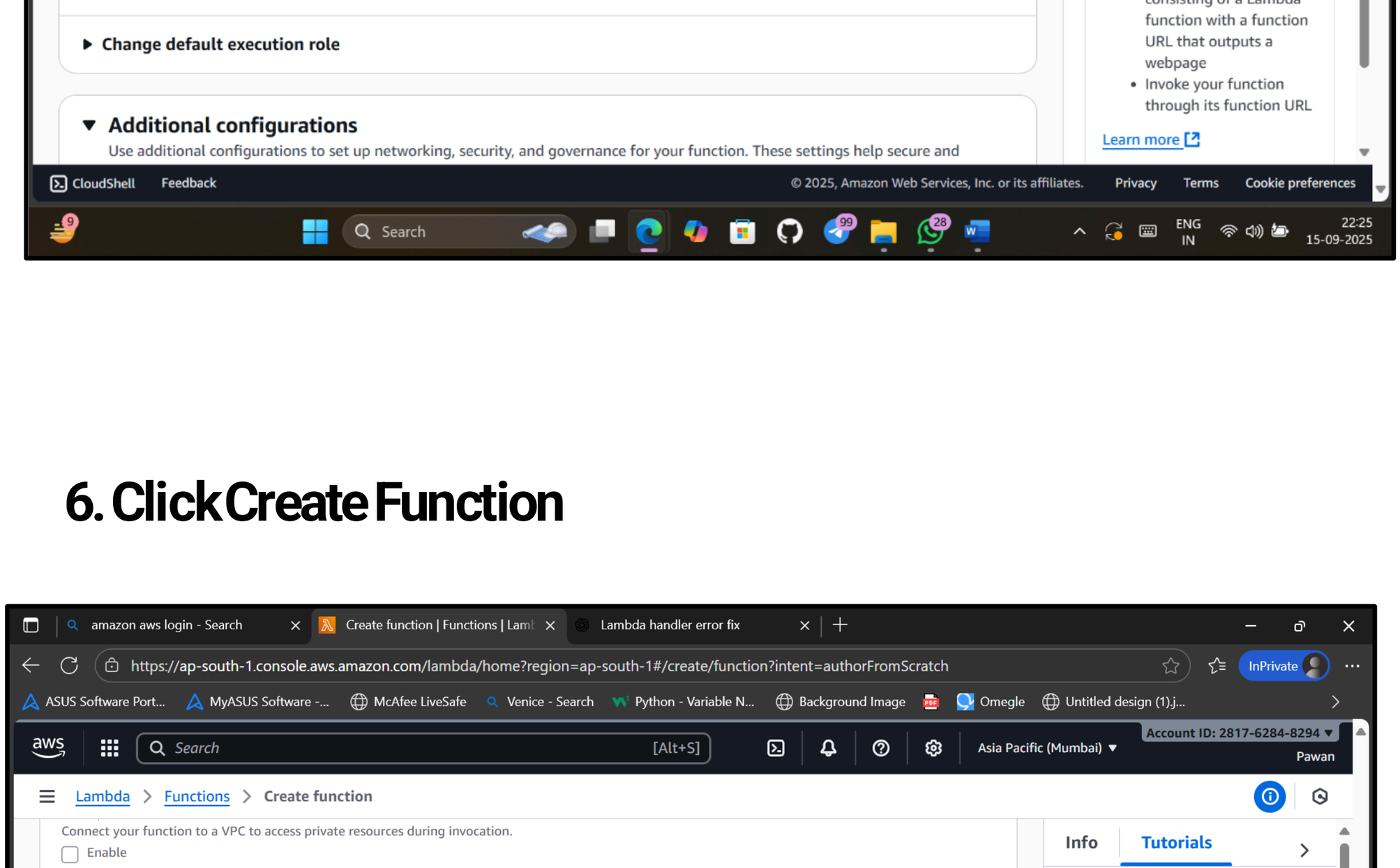


5. Configure Basic Settings

- **Function name**: Enter a unique name (e.g., 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



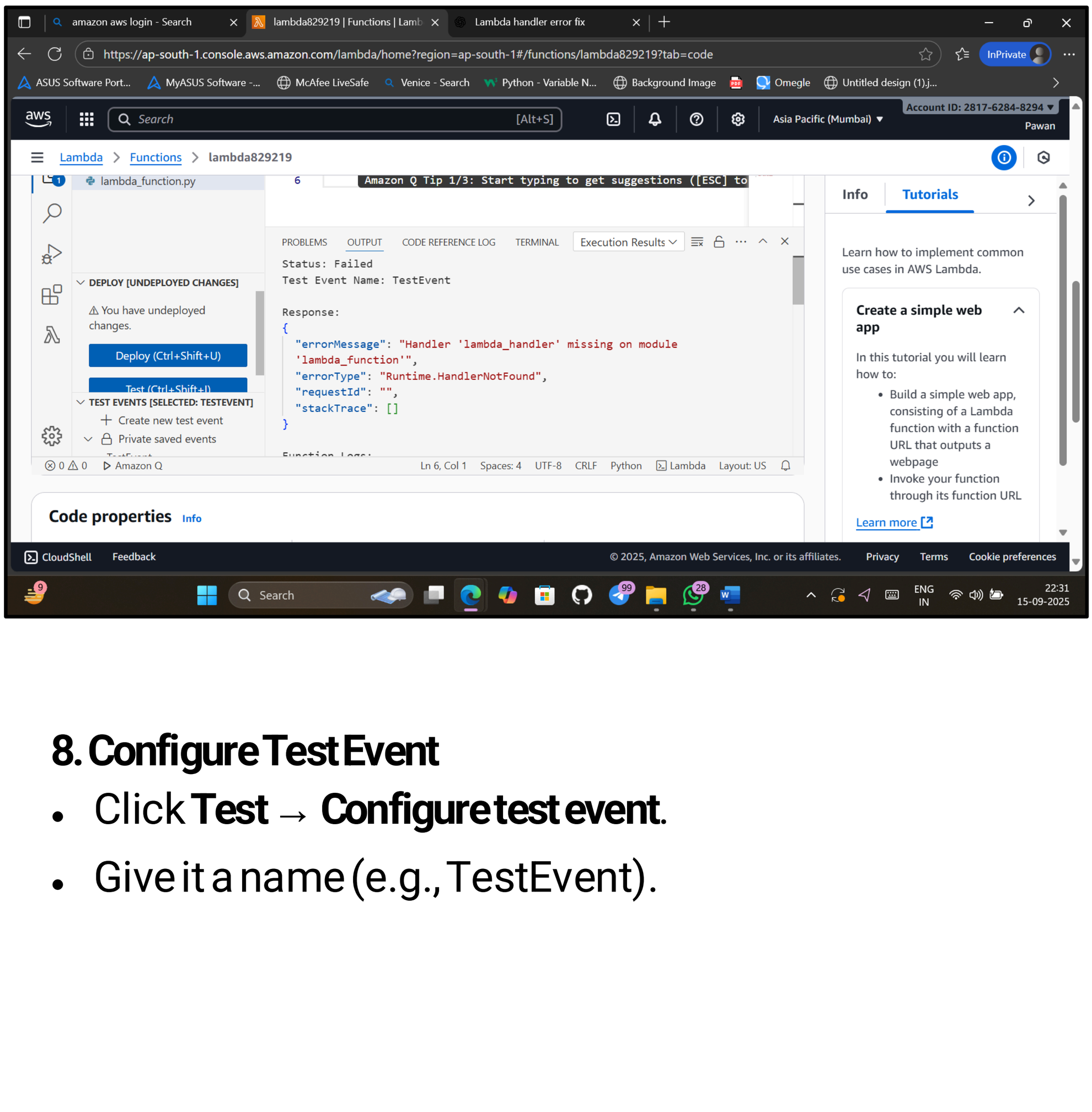
Wait a few seconds while AWS provisions the function.

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

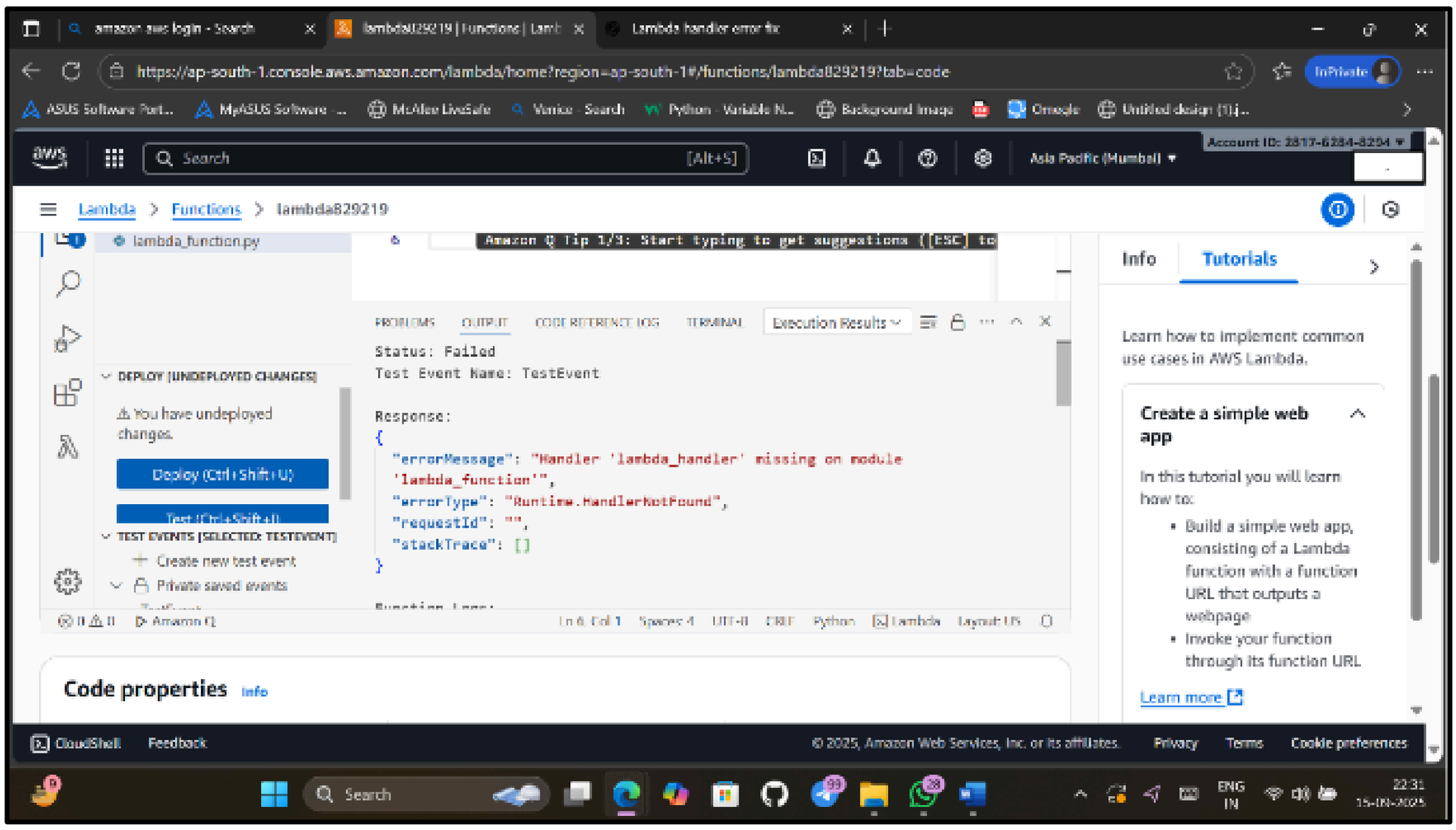
- Click **Test** → **Configure test event**.
- Give it a name (e.g., TestEvent).

- 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

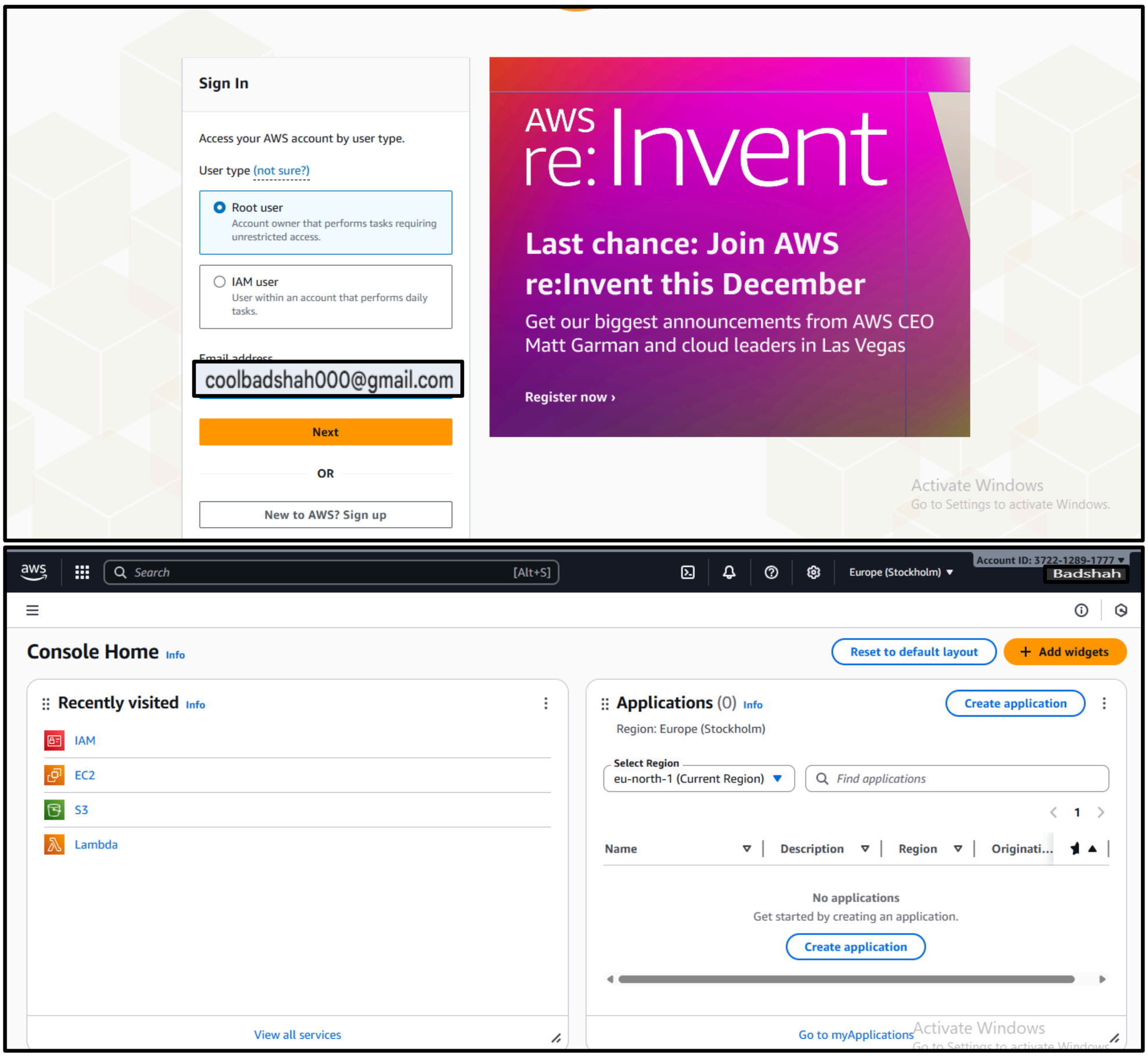


Experiment:-4

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.**

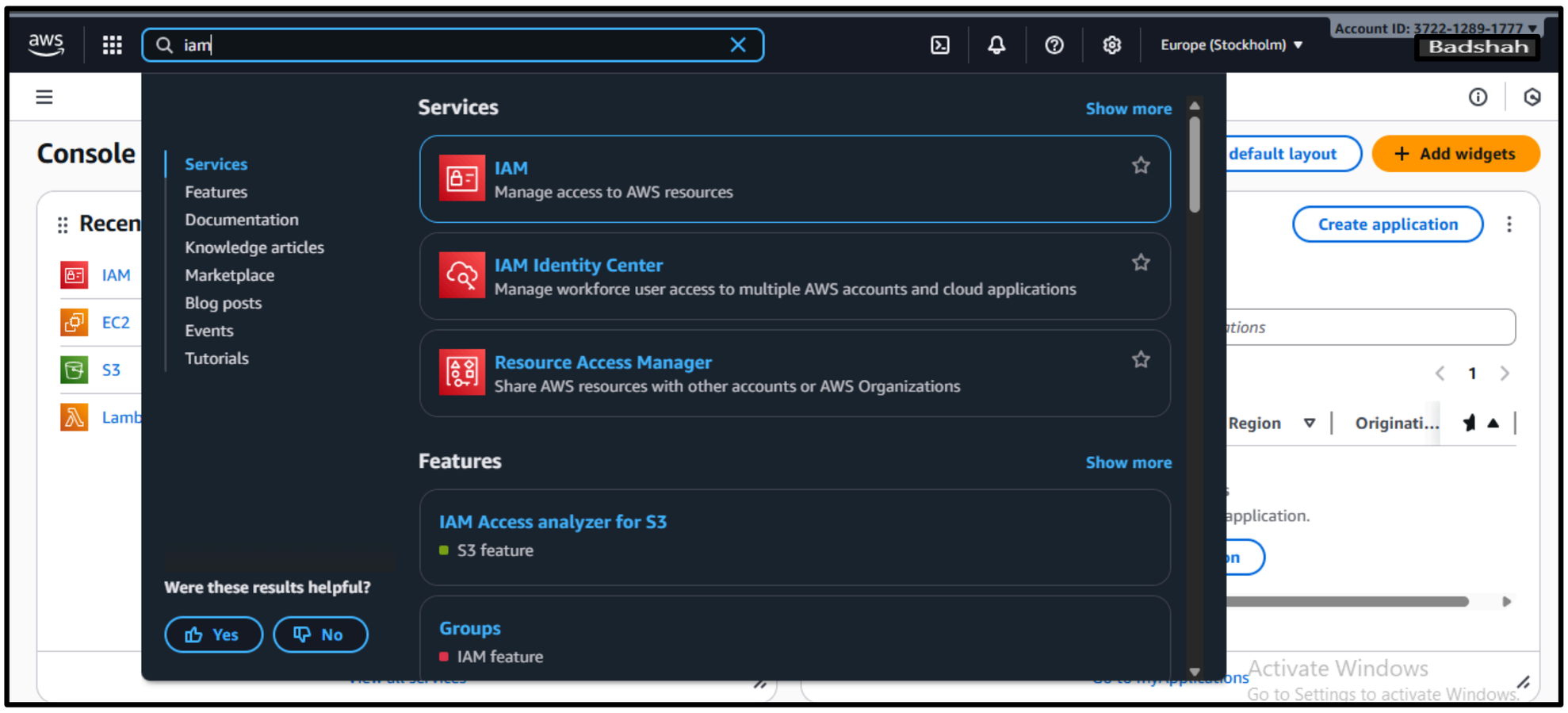
Step 1: Sign in to AWS Console

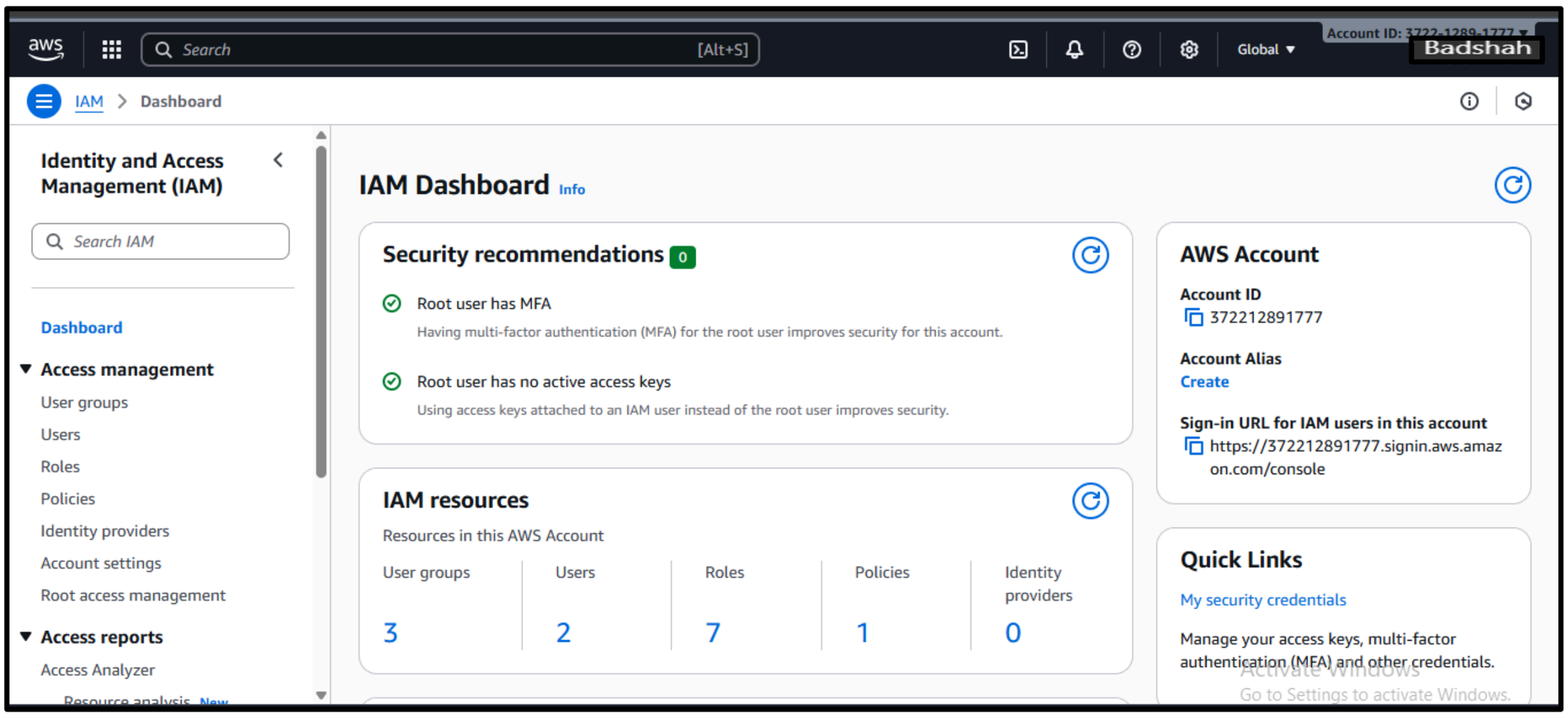
Log in to your **AWS Management Console** using your **root account** or an **IAM user** who has **Administrator privileges**.



Step 2: Open IAM Service

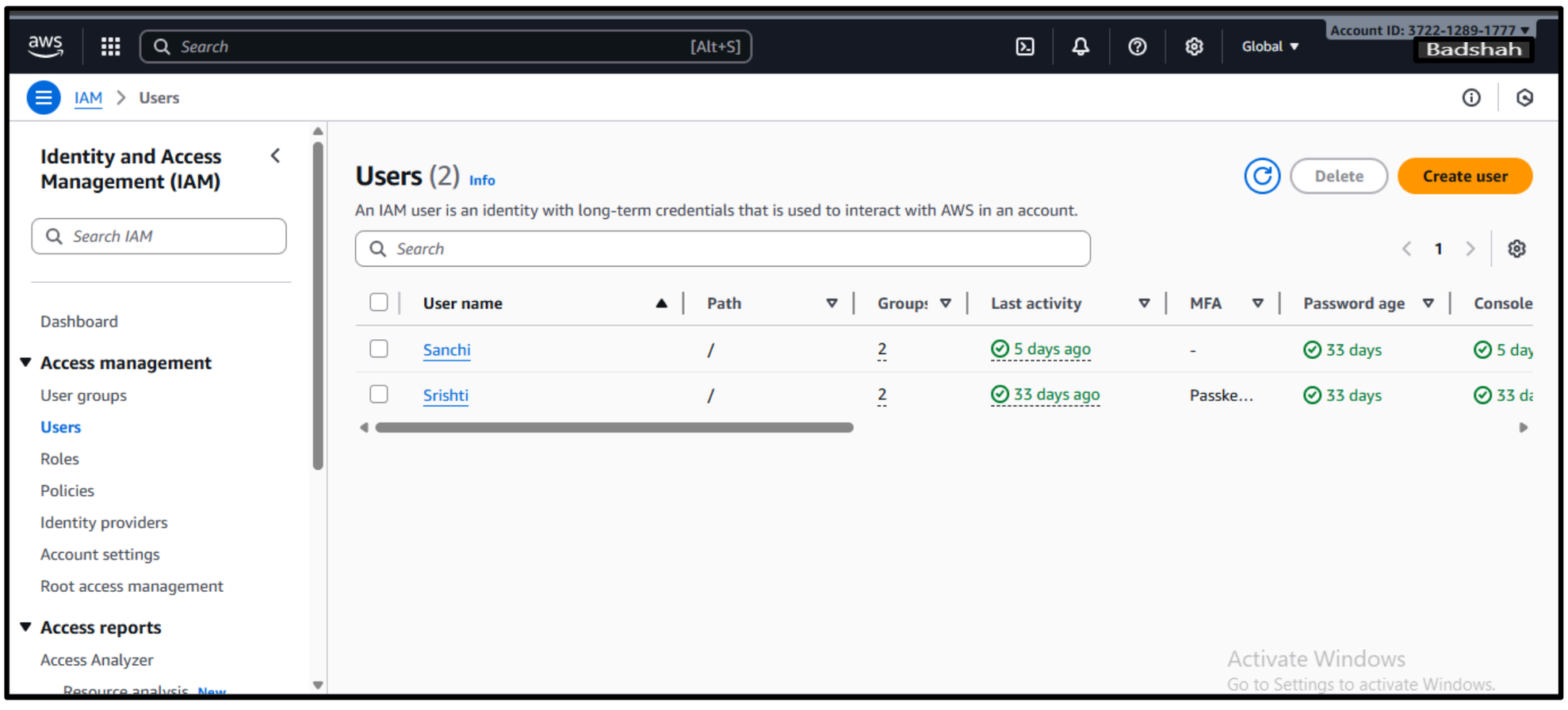
In the search bar at the top, type **IAM**. Select **IAM (Identity and Access Management)**.





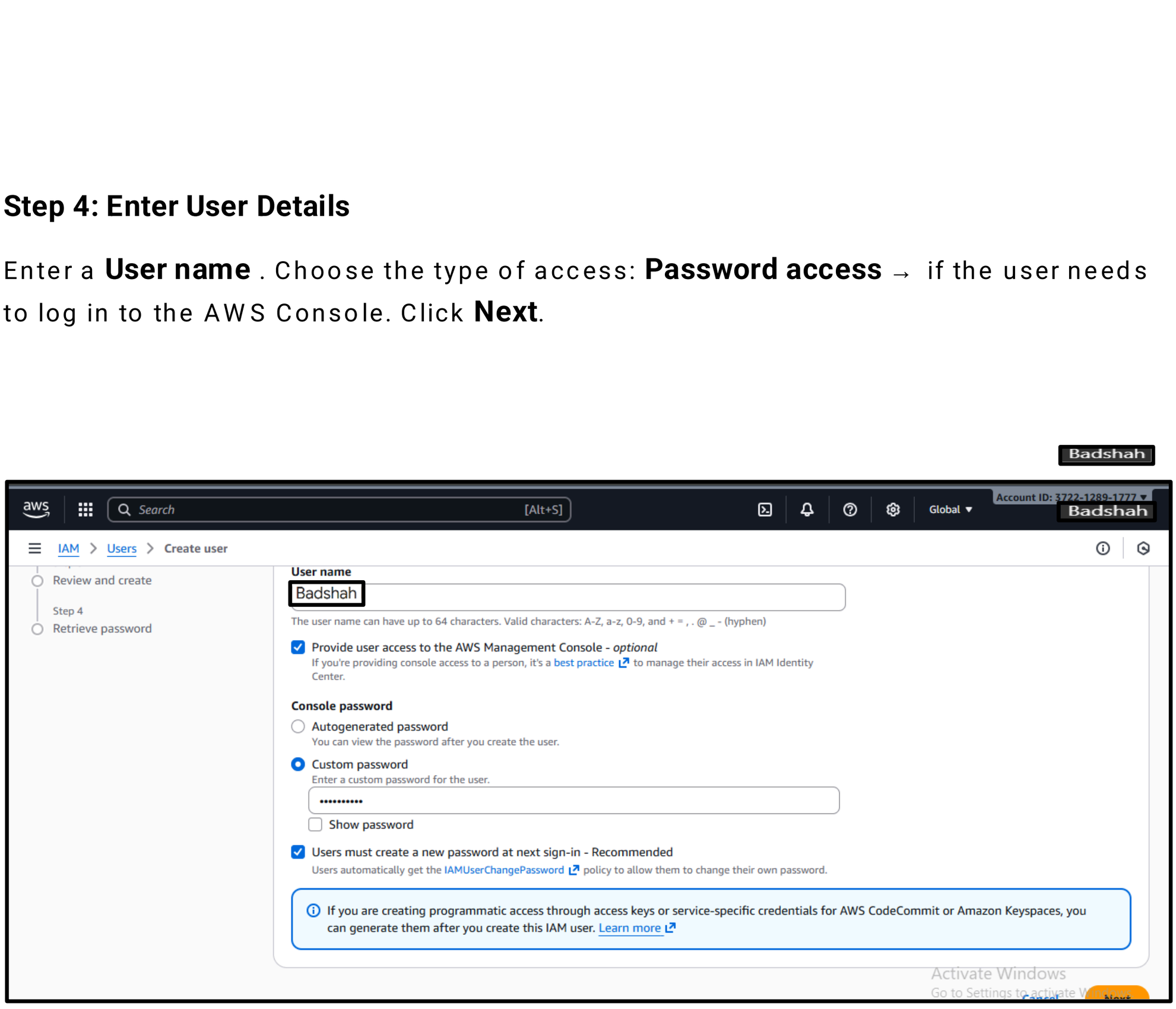
Step 3: Go to Users Section

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

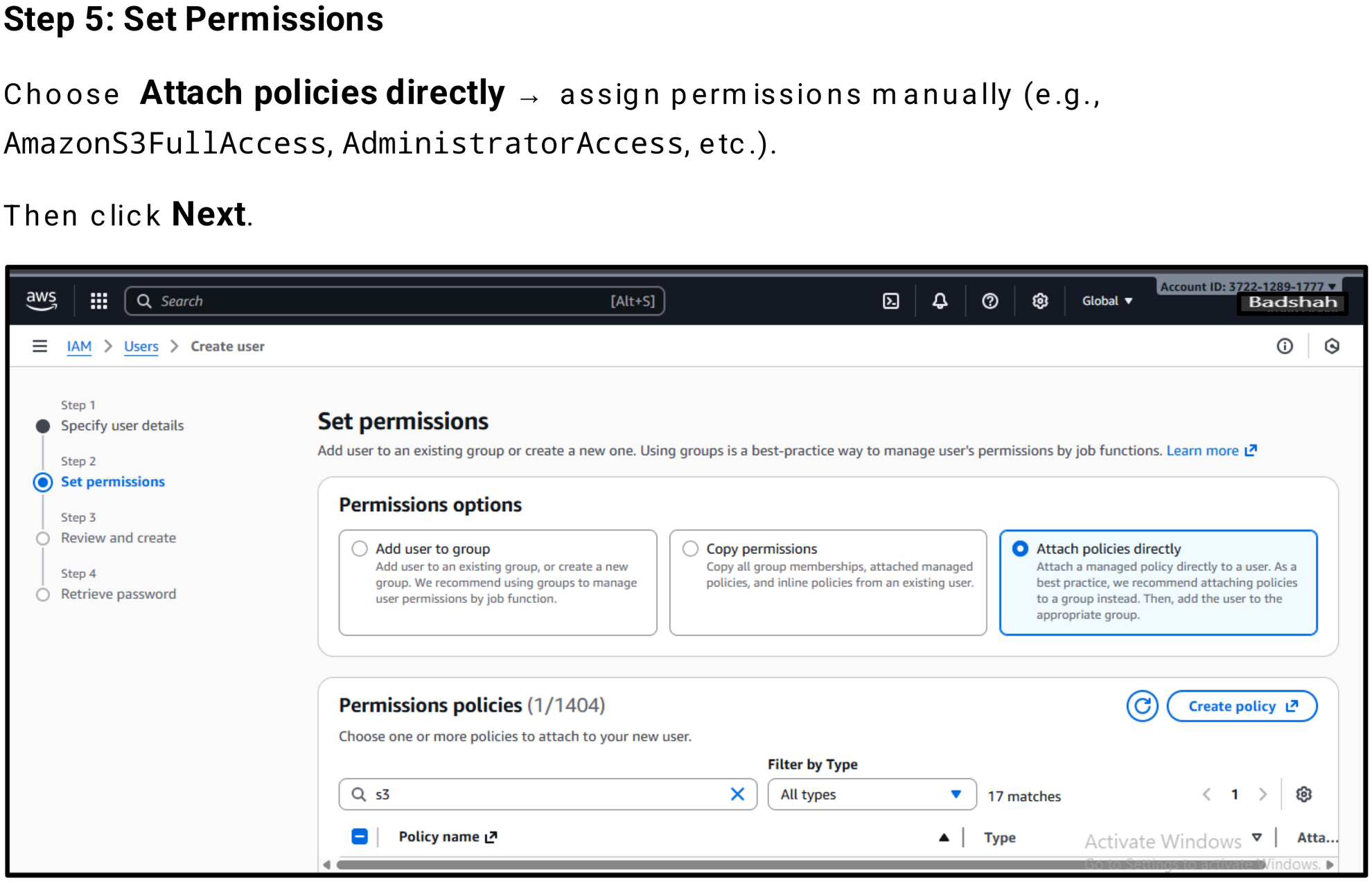
Enter a **User name** . Choose the type of access: **Password access** → if the user needs to log in to the AWS Console. Click **Next**.

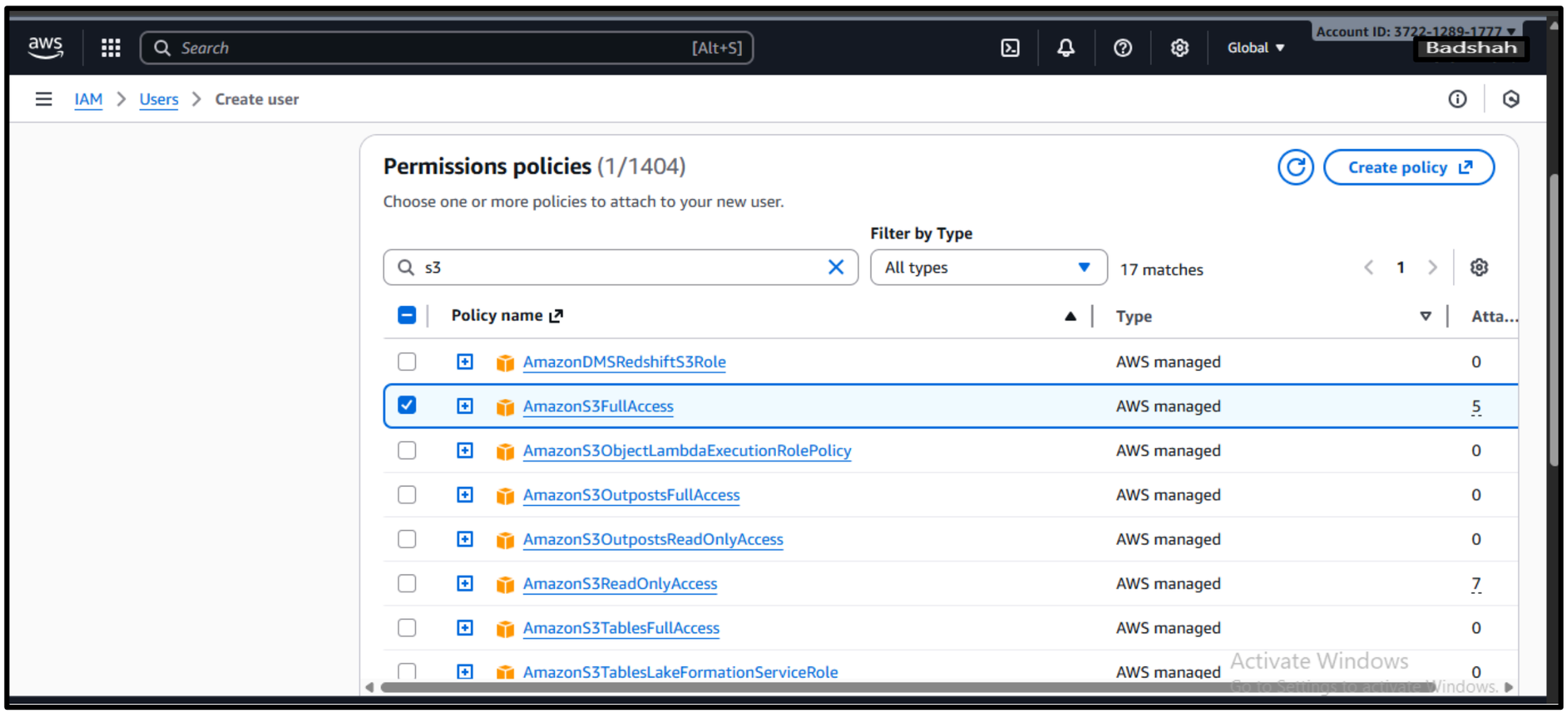


Step 5: Set Permissions

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

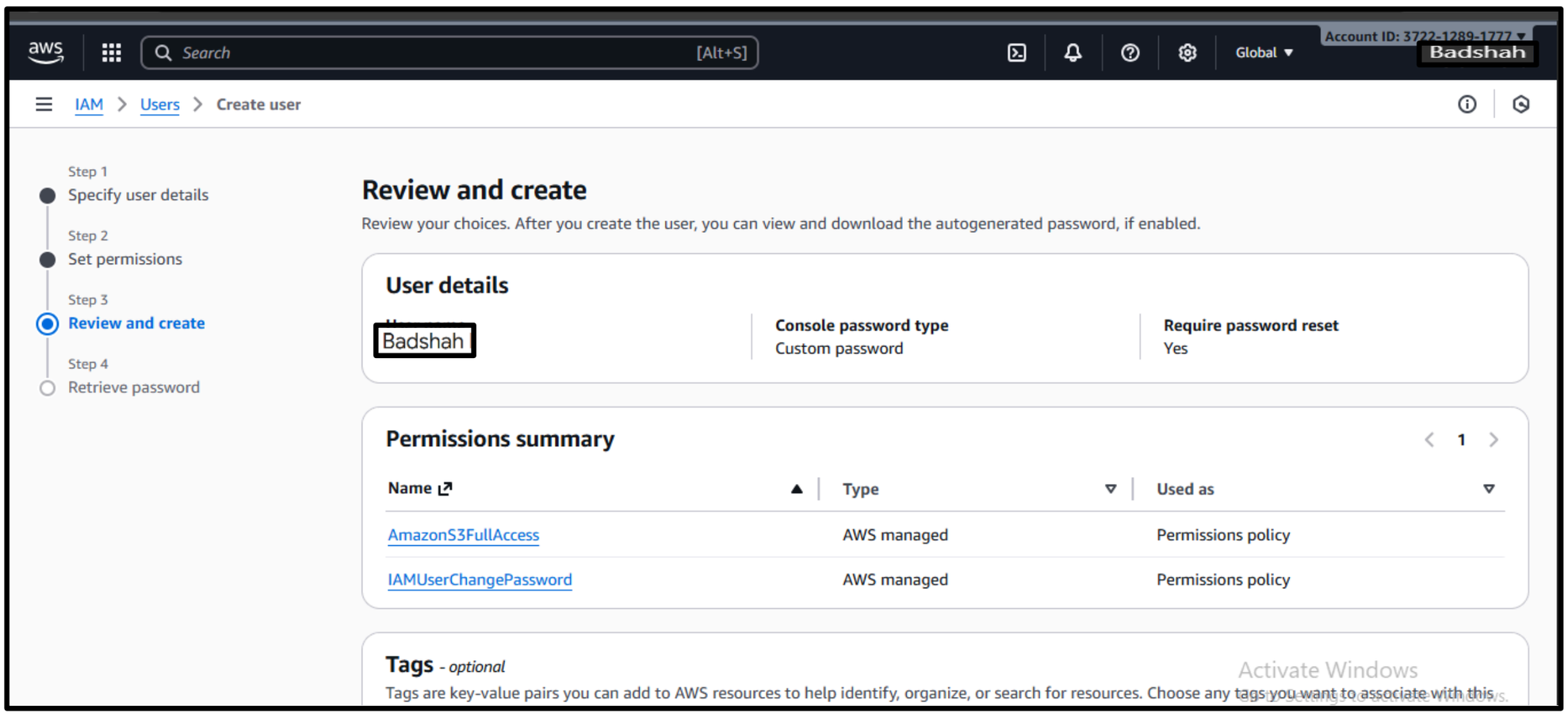
Then click **Next**.

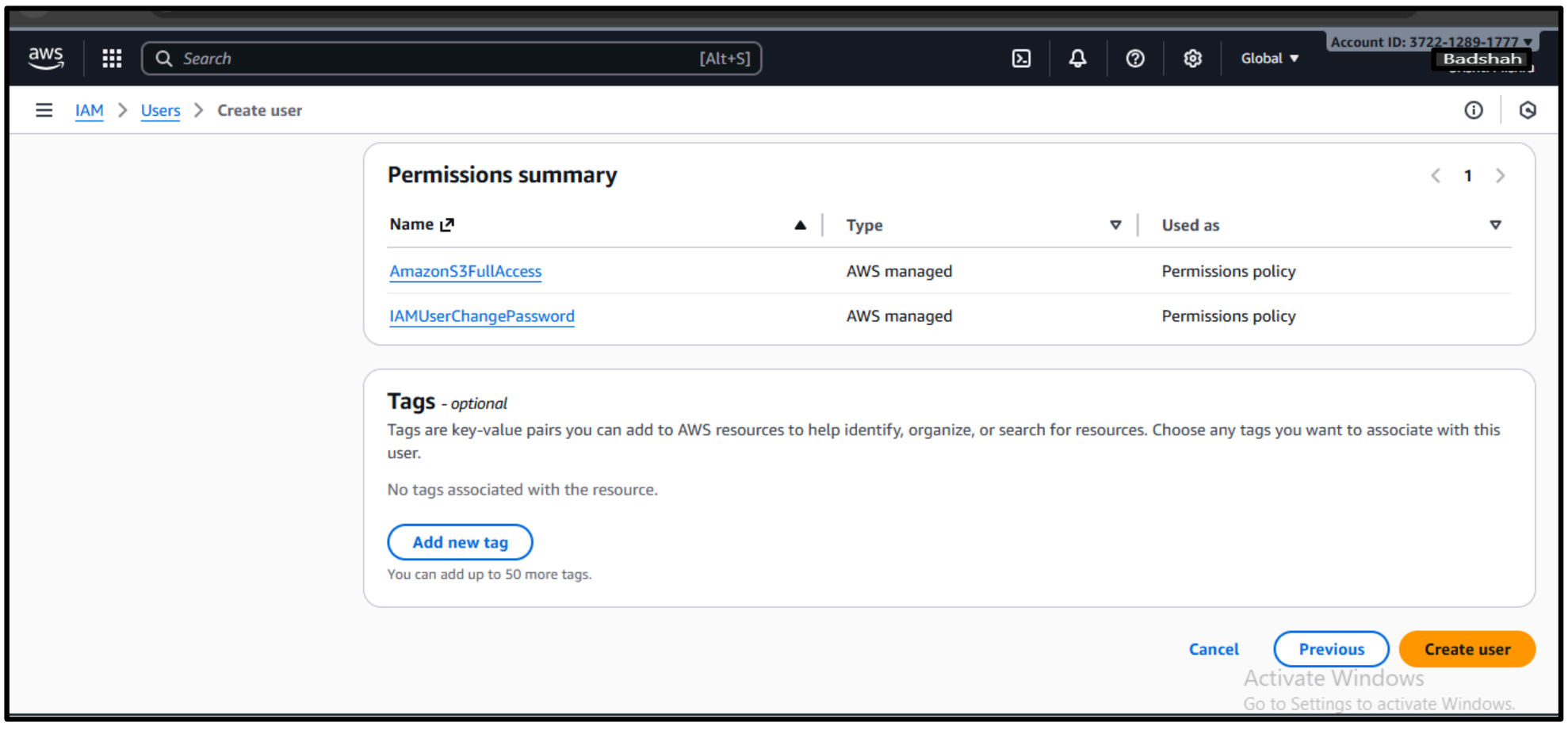




Step 6: Review and Create

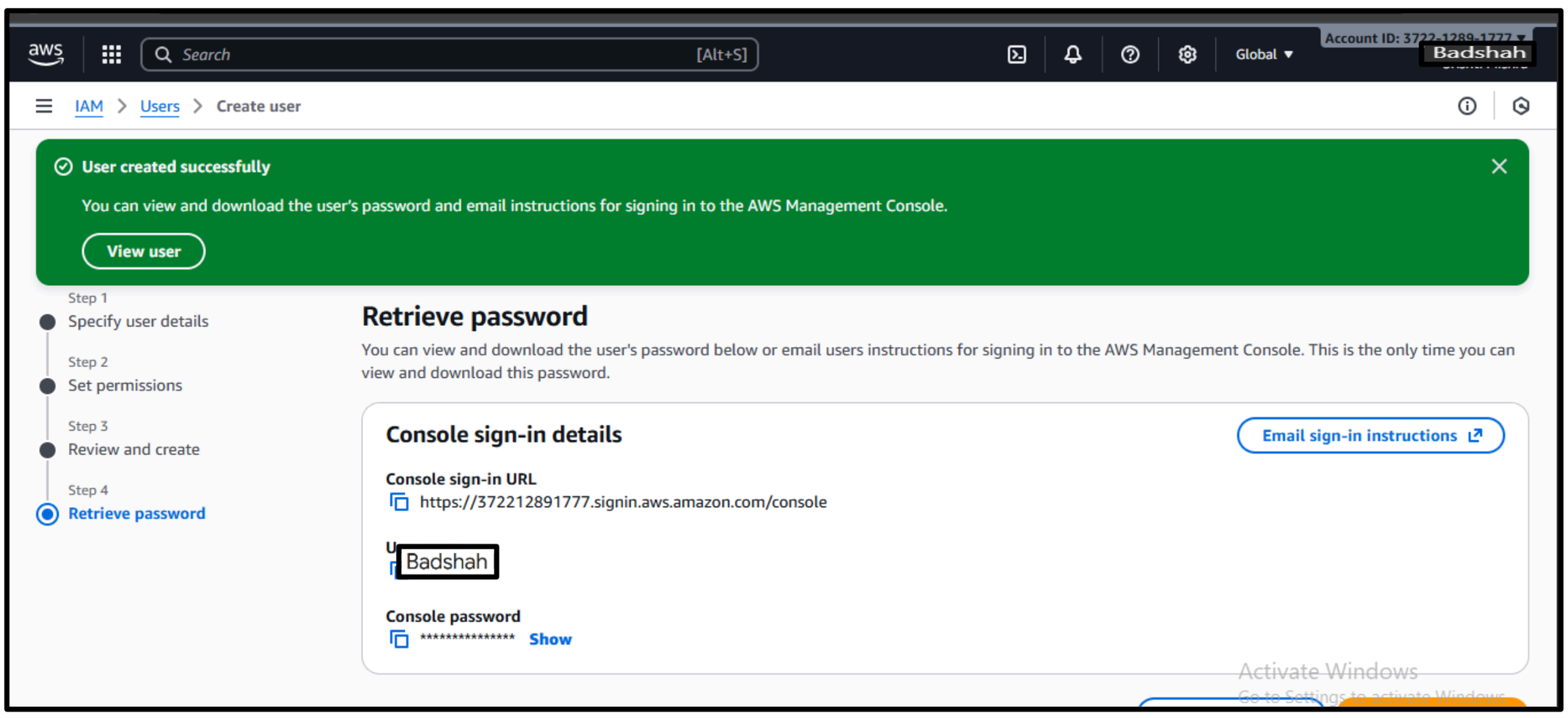
Review all details carefully. Click **Create user**.





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 .csv file — it won't be shown again).

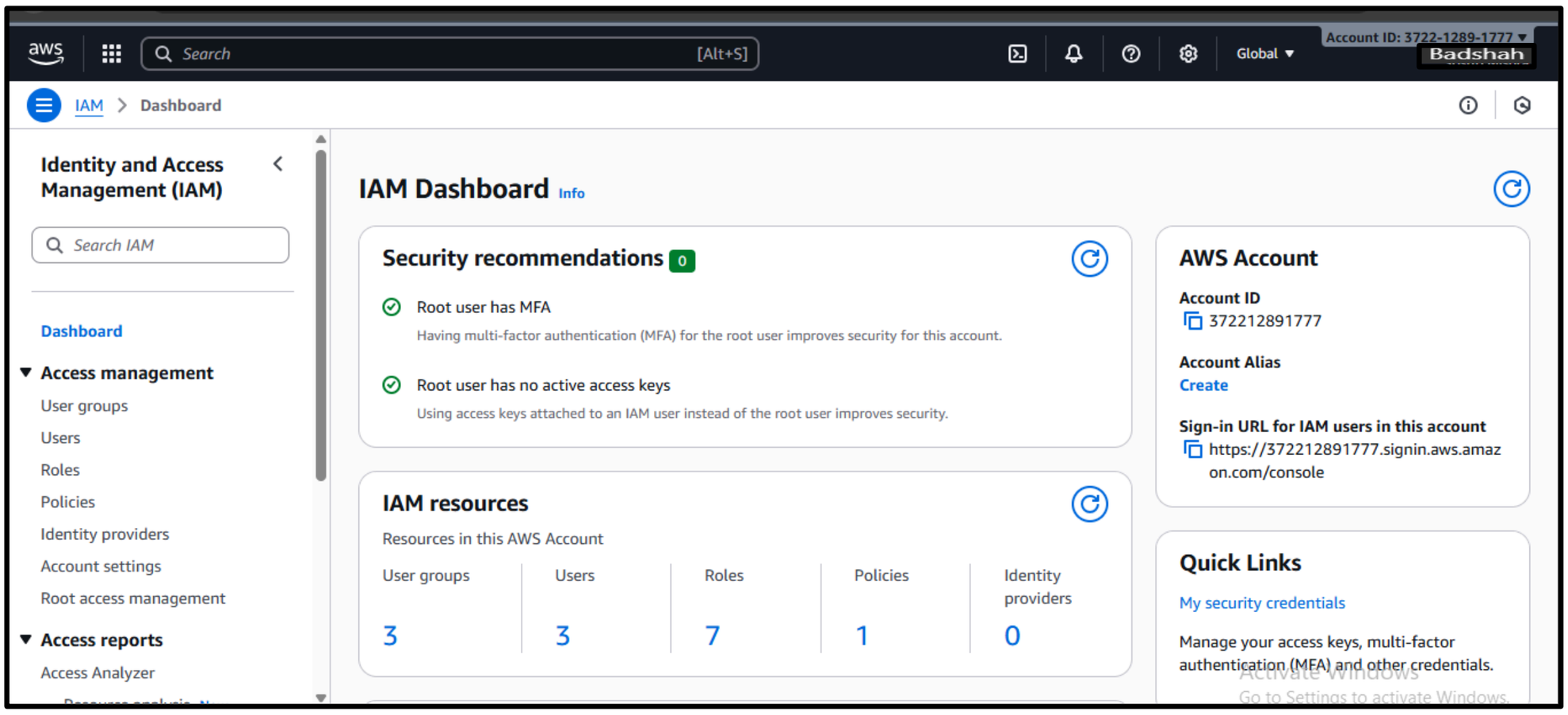


EXPERIMENT:-5

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

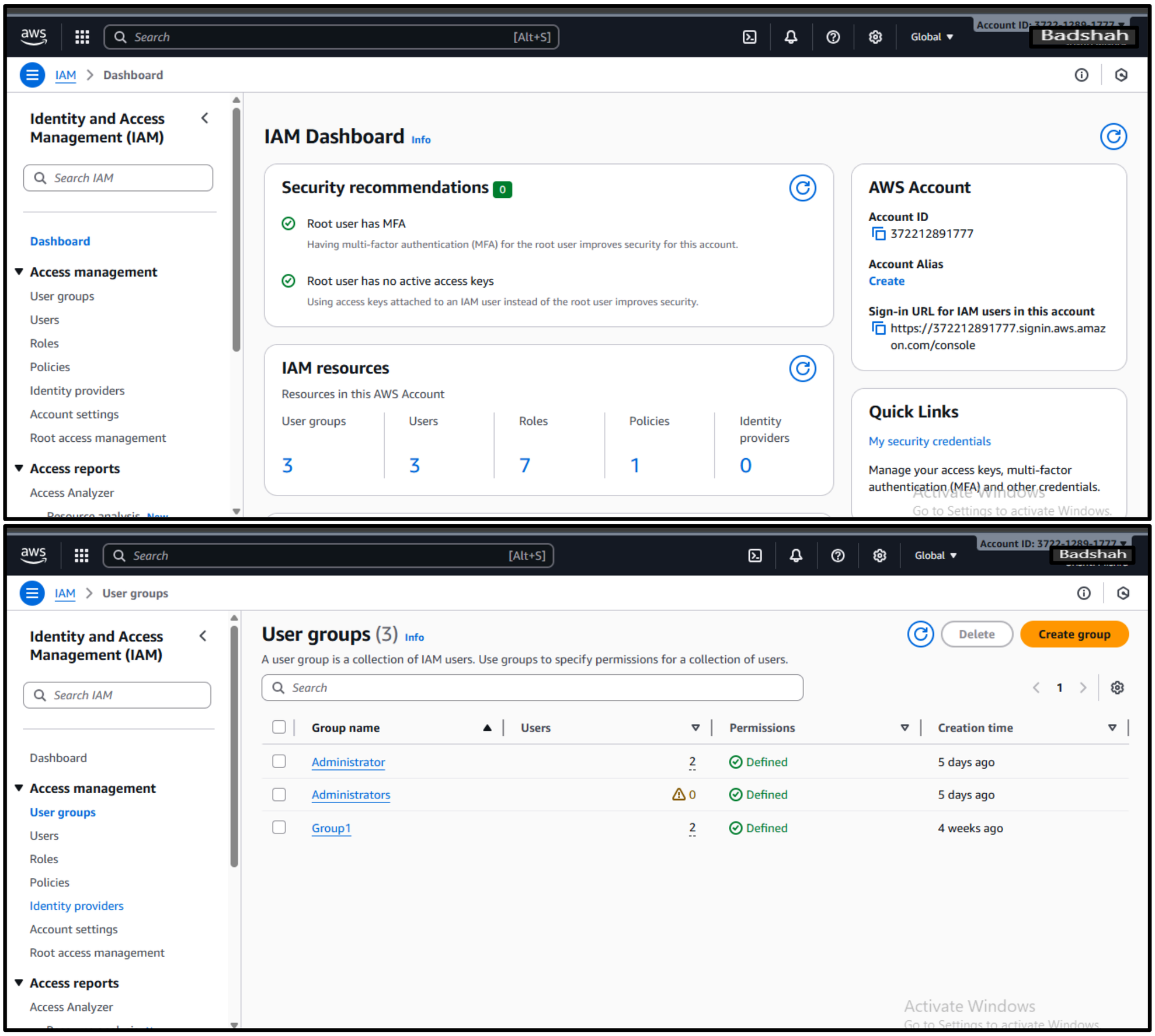
Step1:- Open the IAM Service:

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



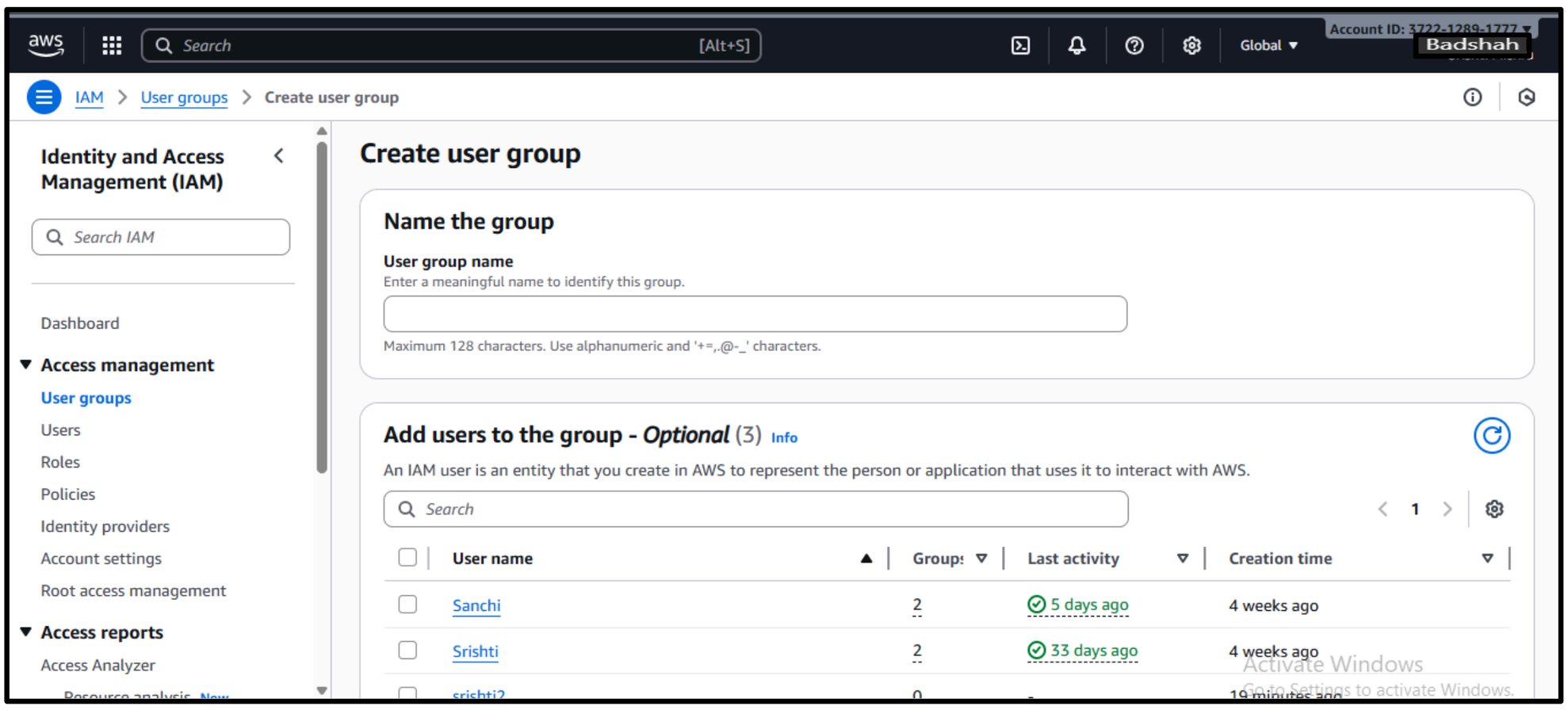
Step2:- Go to User Groups Section:

In the left-hand sidebar, click on **User groups**.



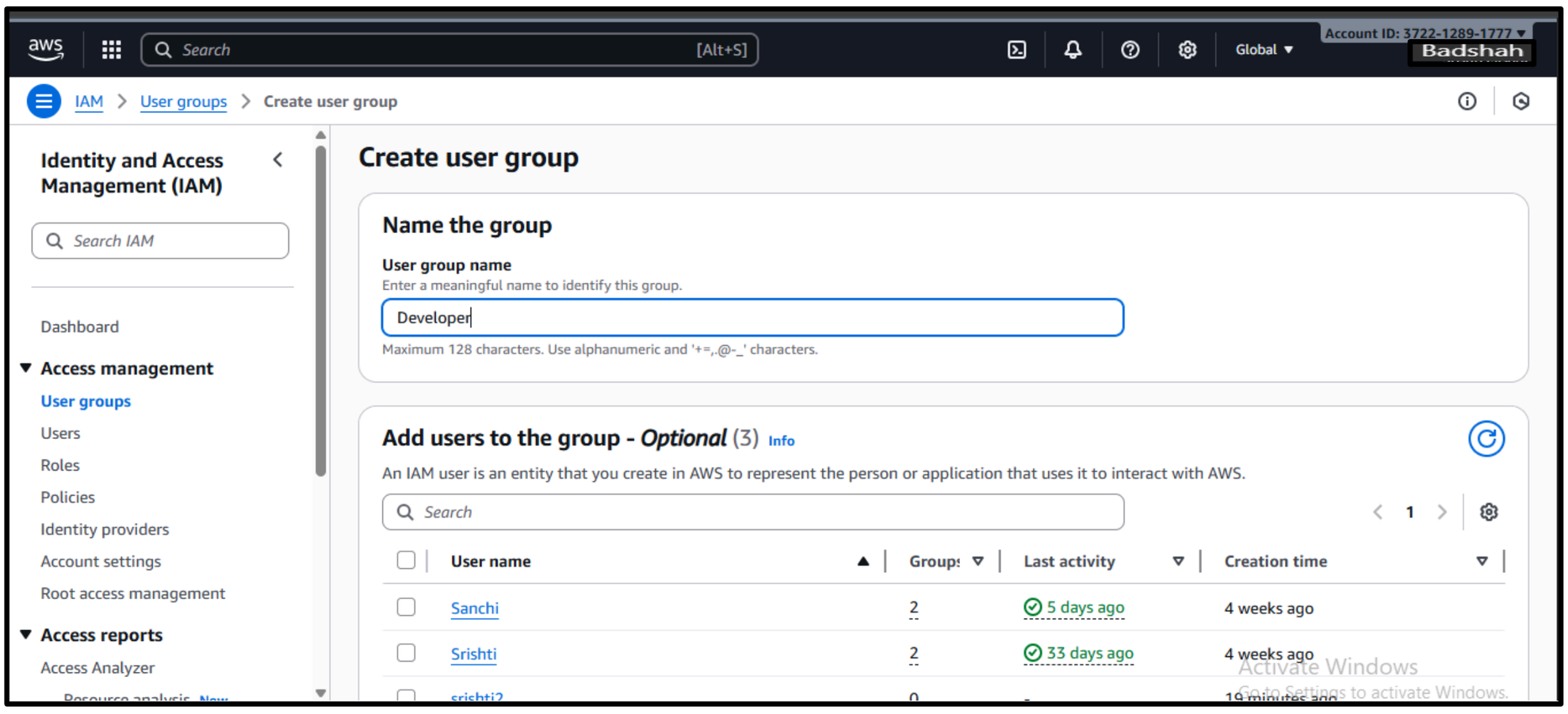
Step3:- Click on " Create group" :

On the User Groups page, click the " **Create group**" button to start creating a new group.



Step4:- Enter Group Name:

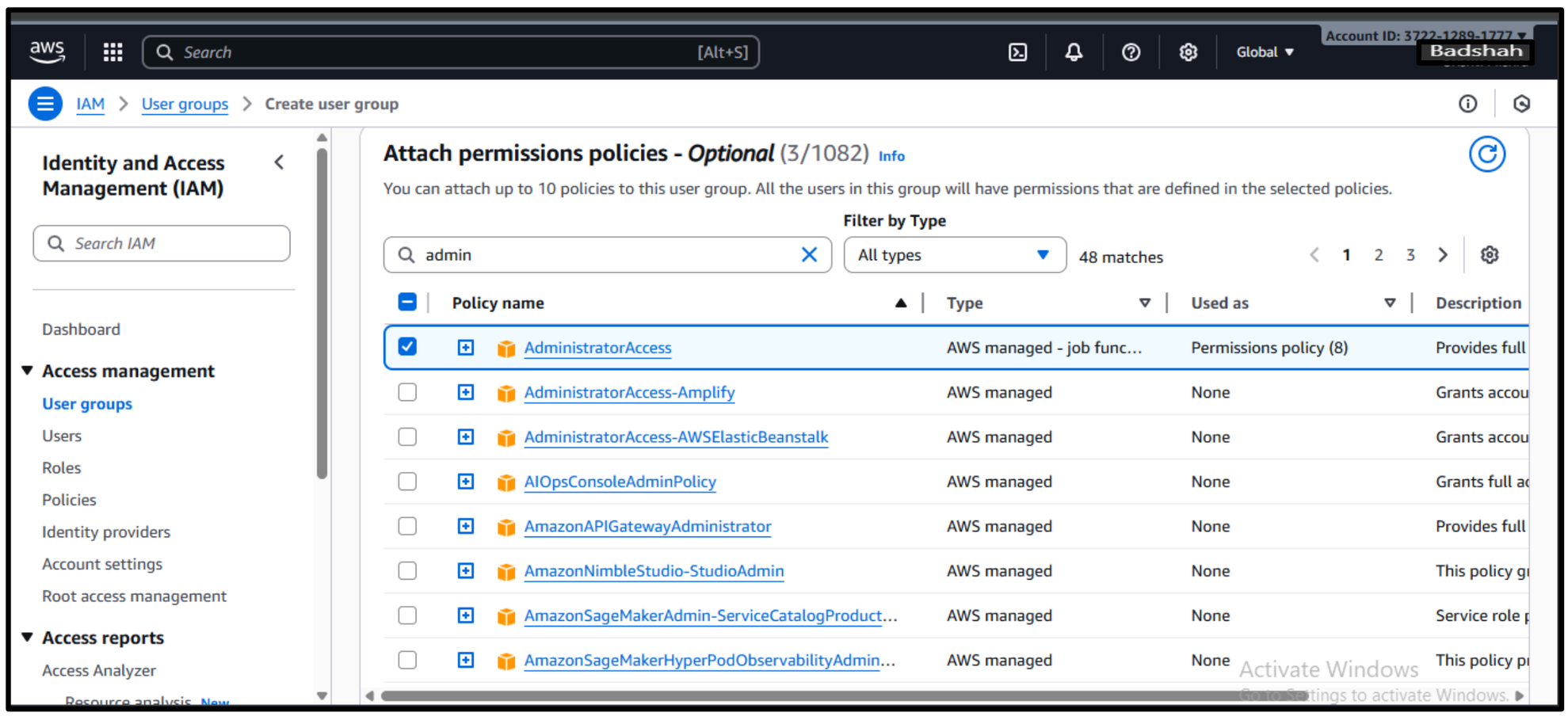
Type a **unique name** for your group (for example, *Developers*, *Admins*, or *ReadOnlyUsers*).



Step5:- Attach Permissions Policies (Optional):

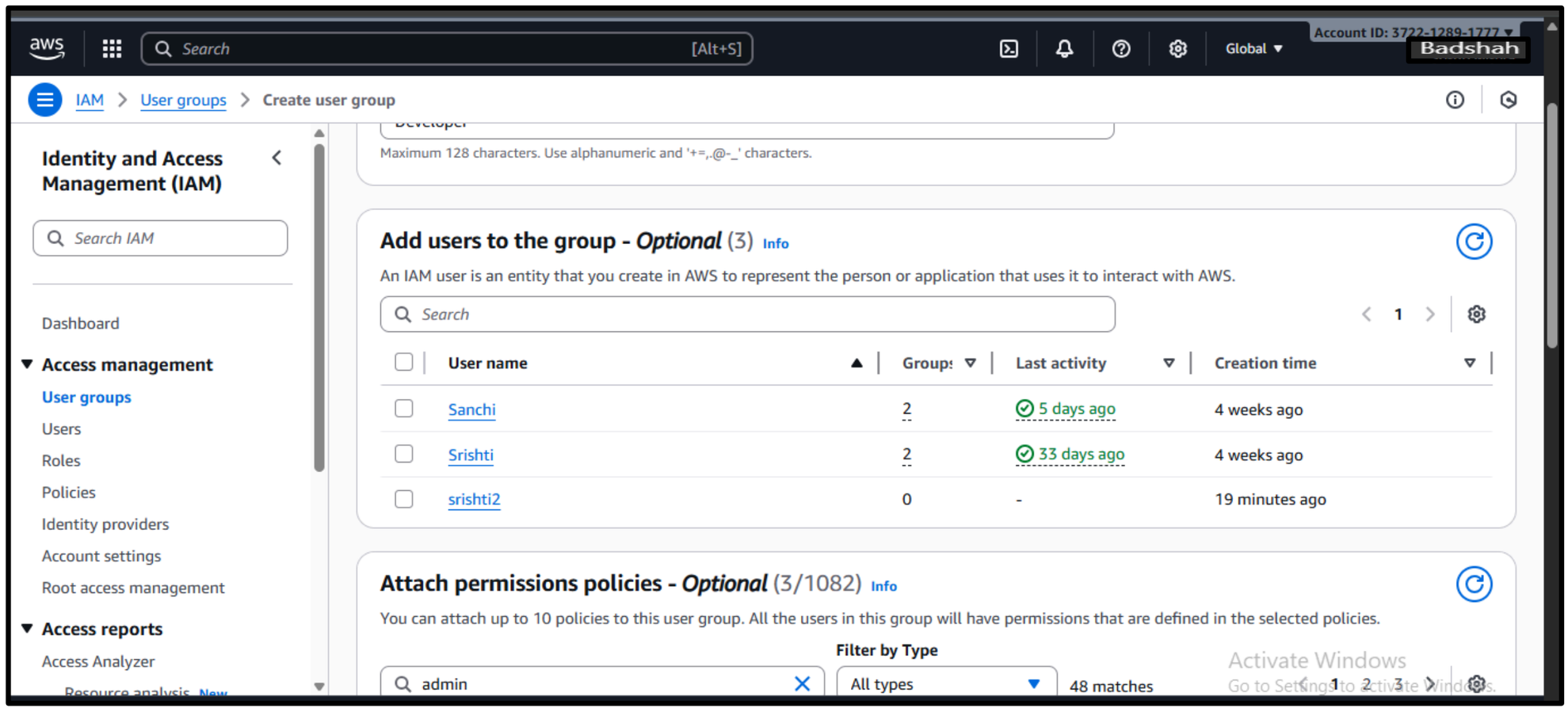
You can choose policies to attach to this group, such as:

- `AmazonS3FullAccess`
- `AmazonEC2ReadOnlyAccess`
- `AdministratorAccess`
  If you want to add permissions later, you can **skip this step** and click **Next**.



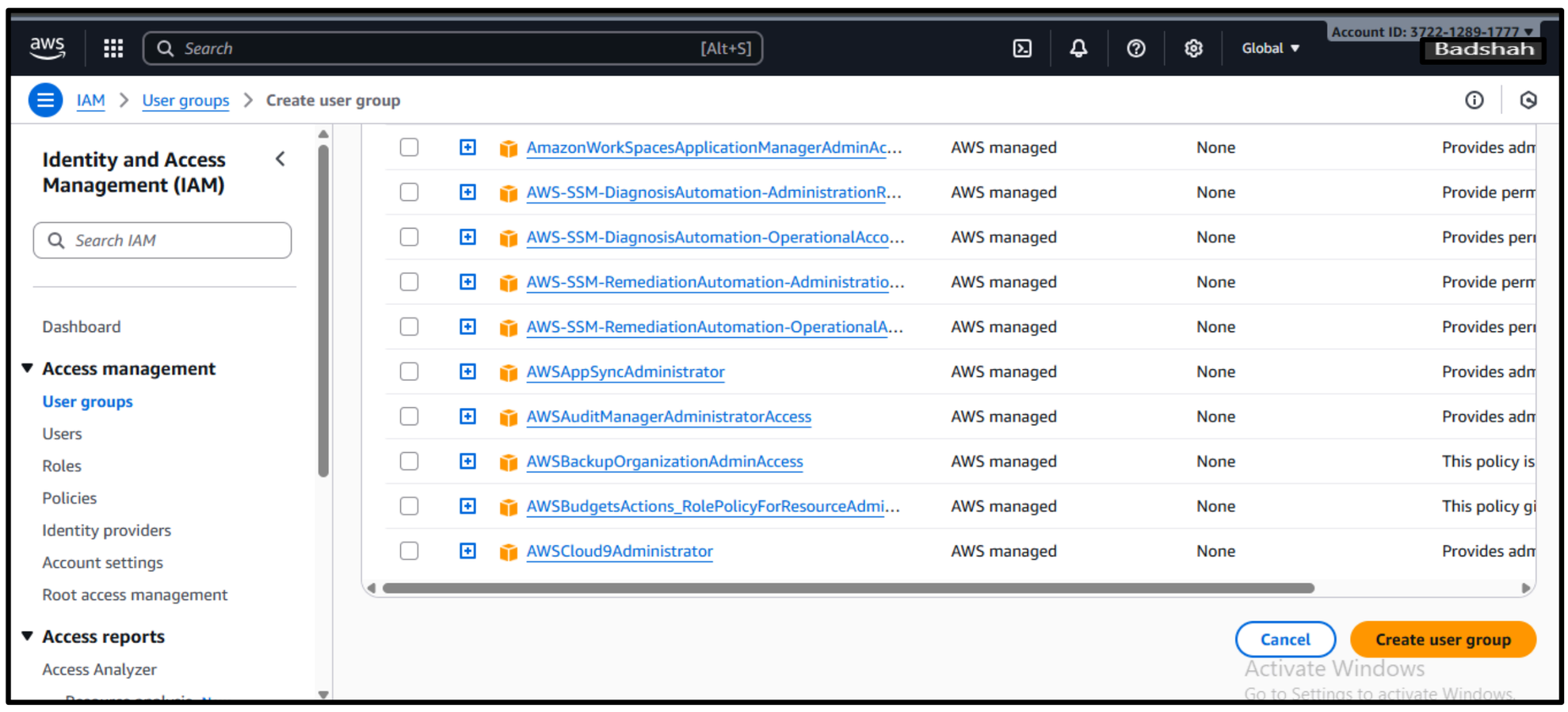
Step6:- Add Users to the Group (Optional):

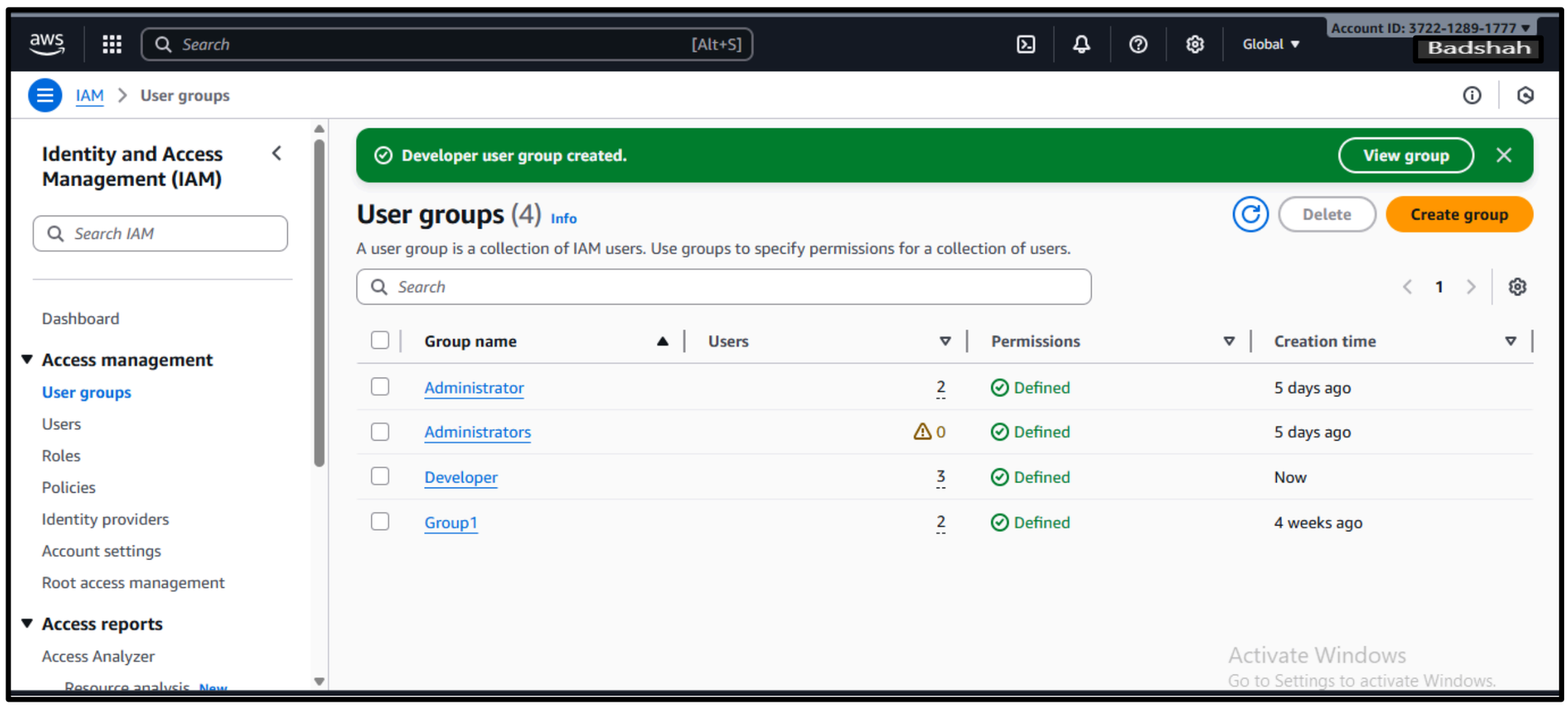
You can select existing IAM users to include in this group now, or you can add users later after creating the group.



Step 7:- **Review and Create Group:**

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

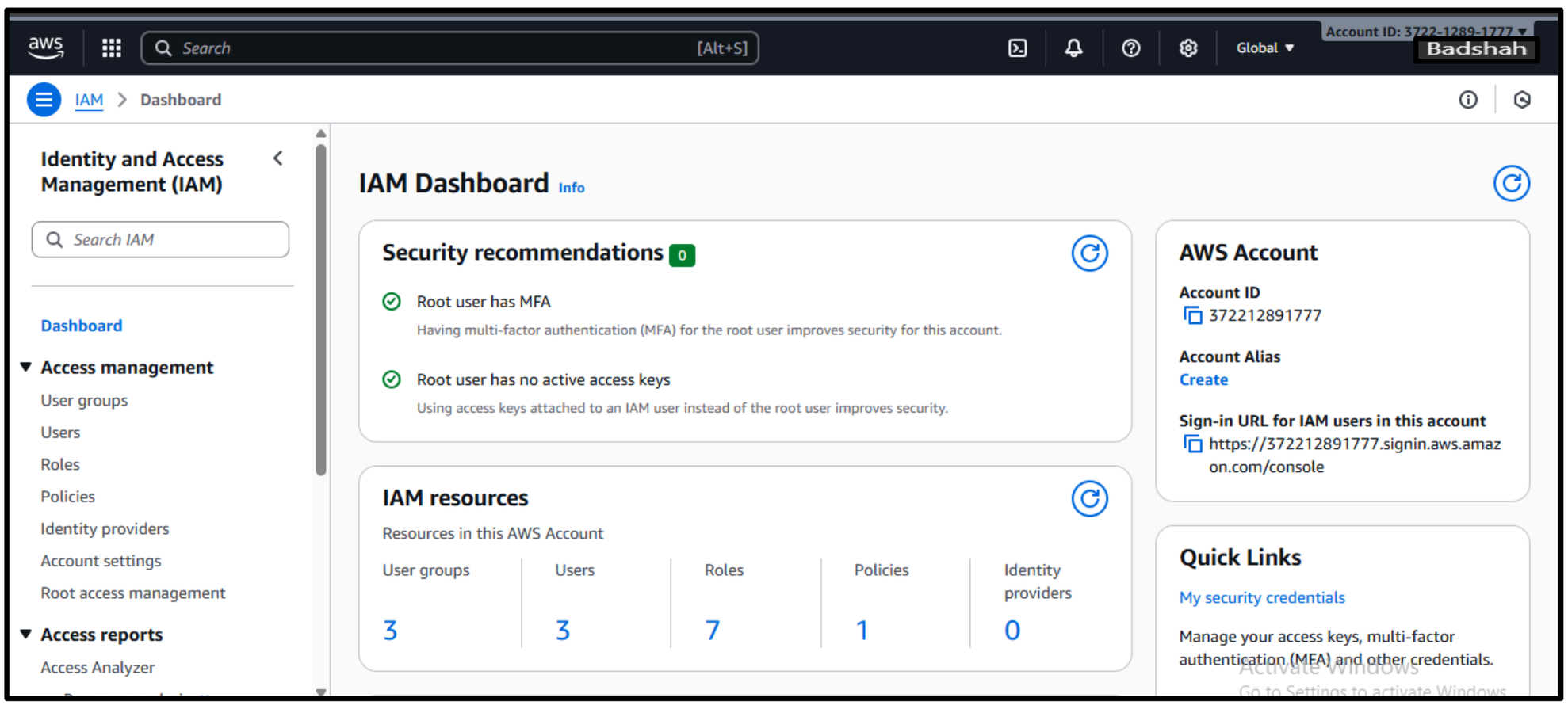




EXPERIMENT:-6

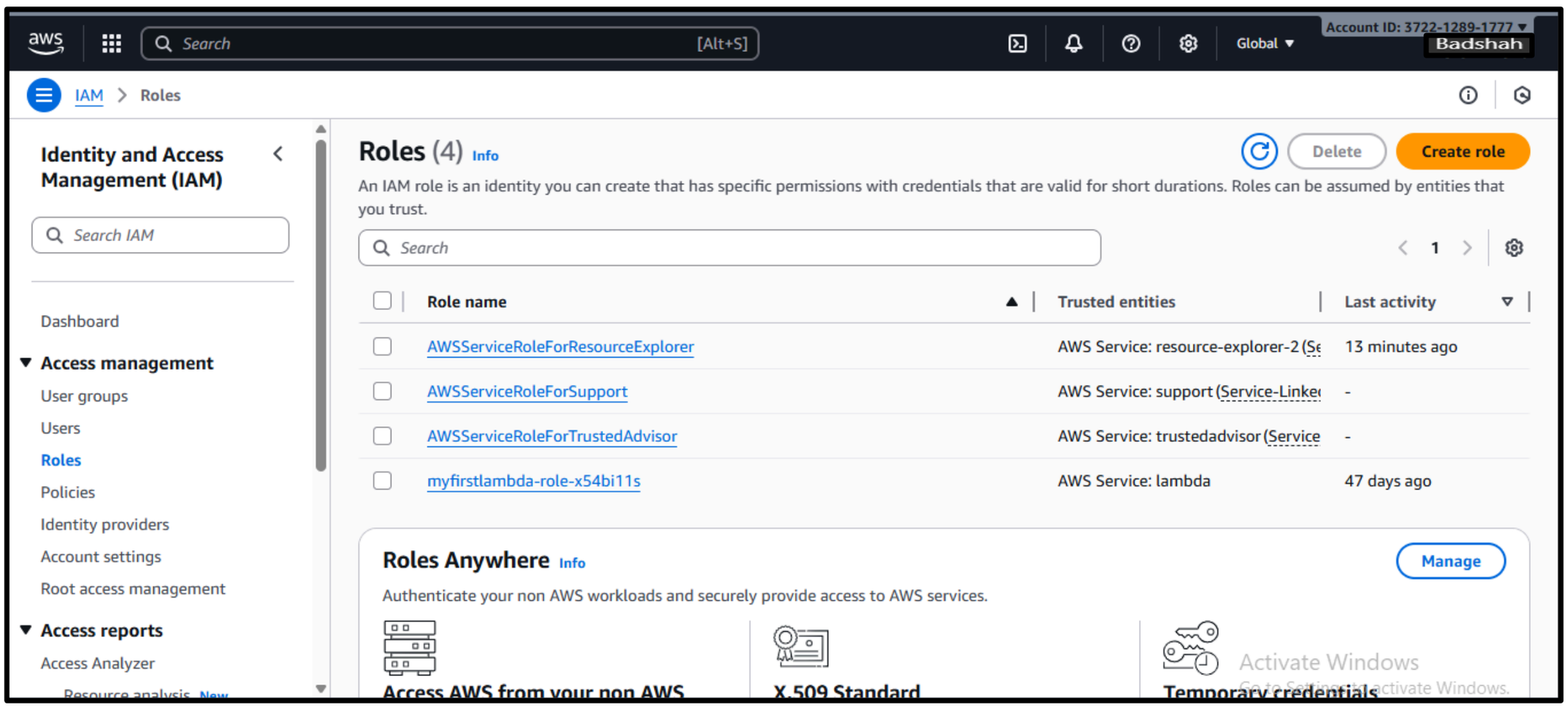
Objective:-To create a security role in AWS IAM that allows AWS services or users to securely access specific AWS resources with defined permissions, ensuring controlled and temporary access without sharing long-term credentials.

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.



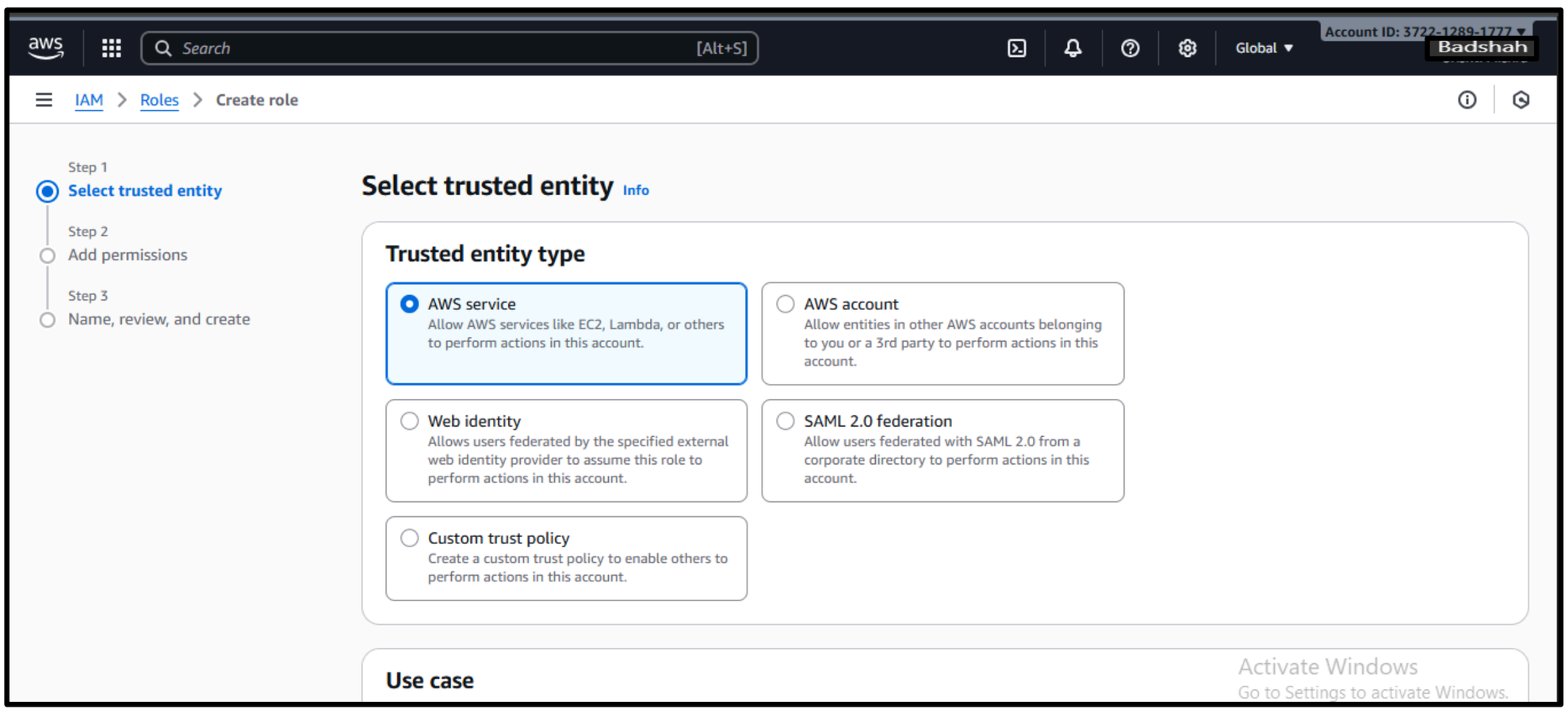
Step2:- **Go to Roles Section:**

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.

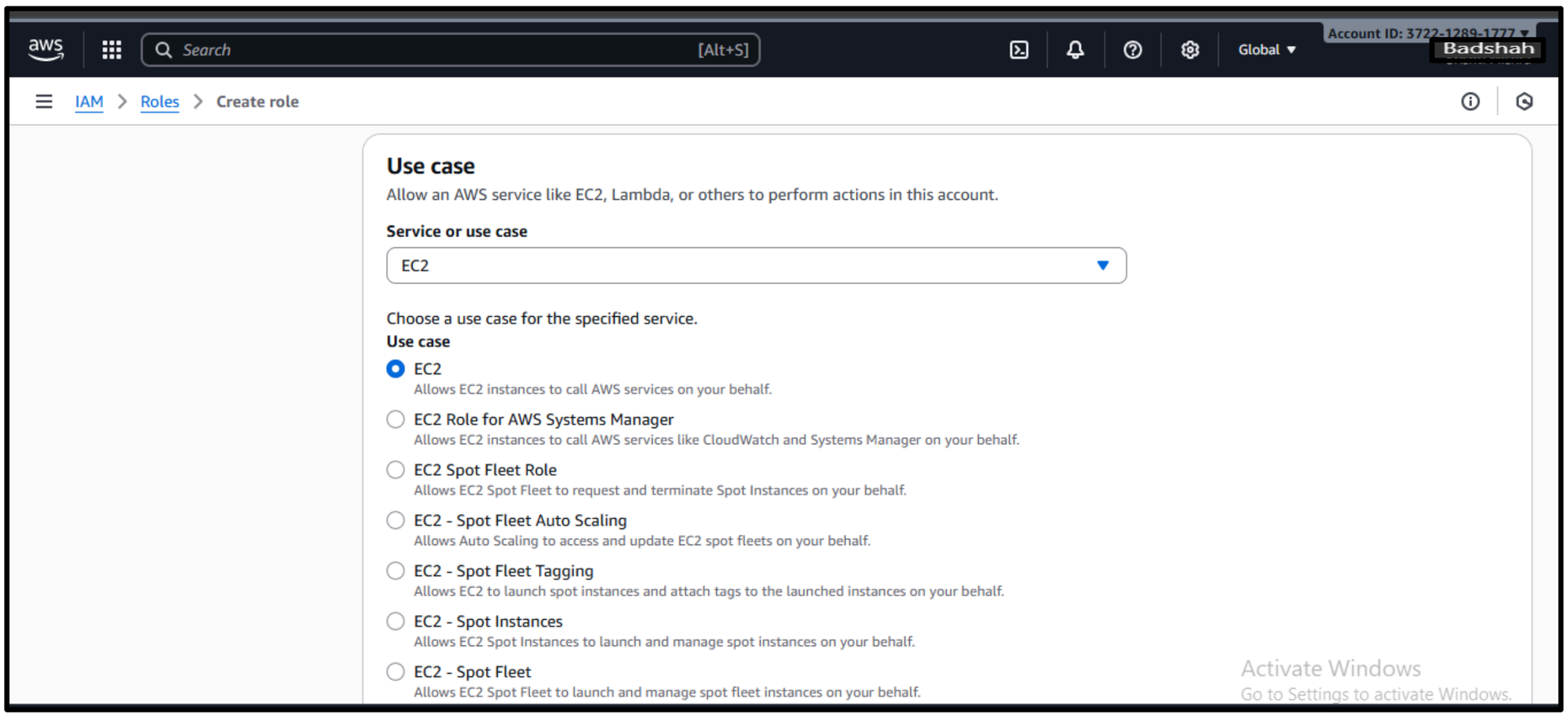


Step4:- Select Trusted Entity Type:

Choose who will use the role, such as:

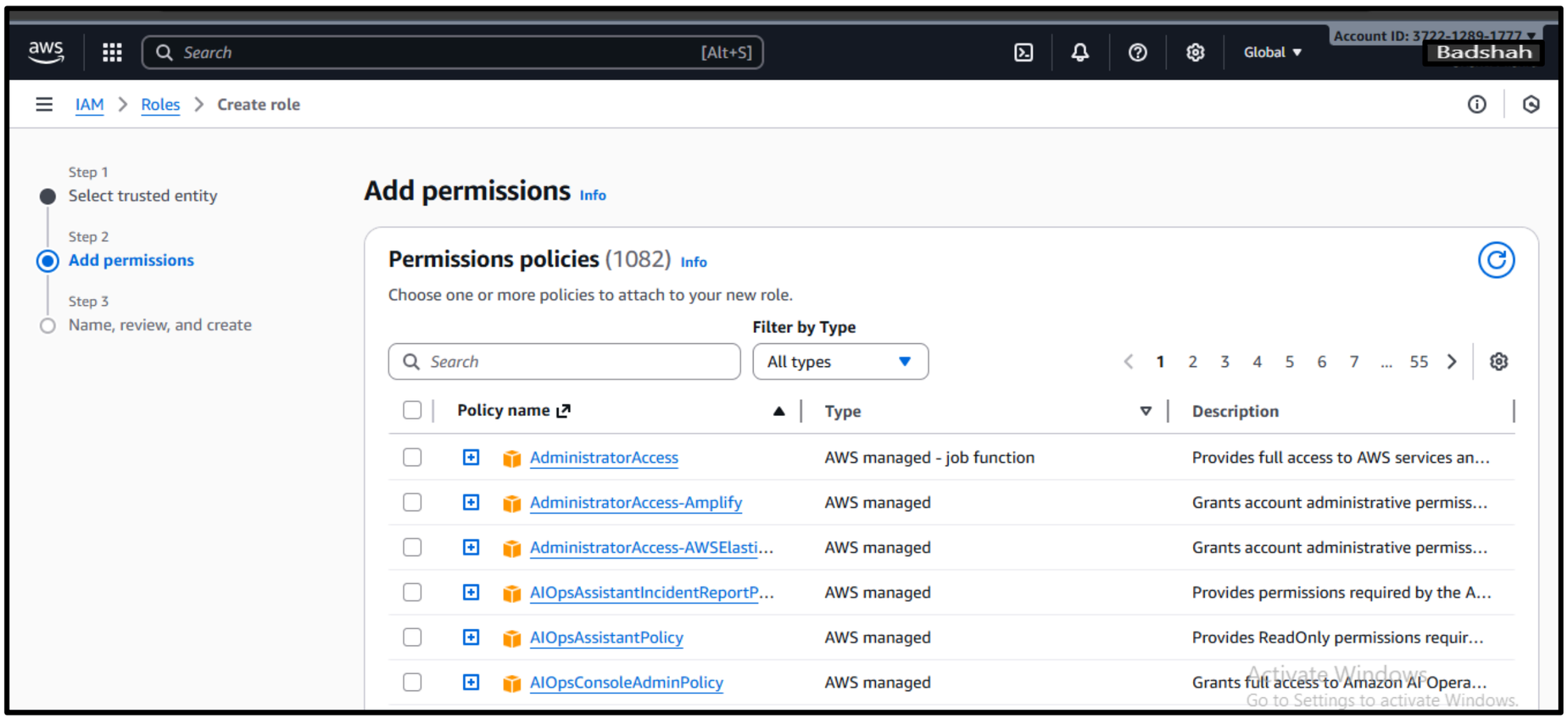
- **AWS Service** (e.g., EC2, Lambda)
- **Another AWS Account**
- **Web Identity** or **SAML 2.0 Federation**

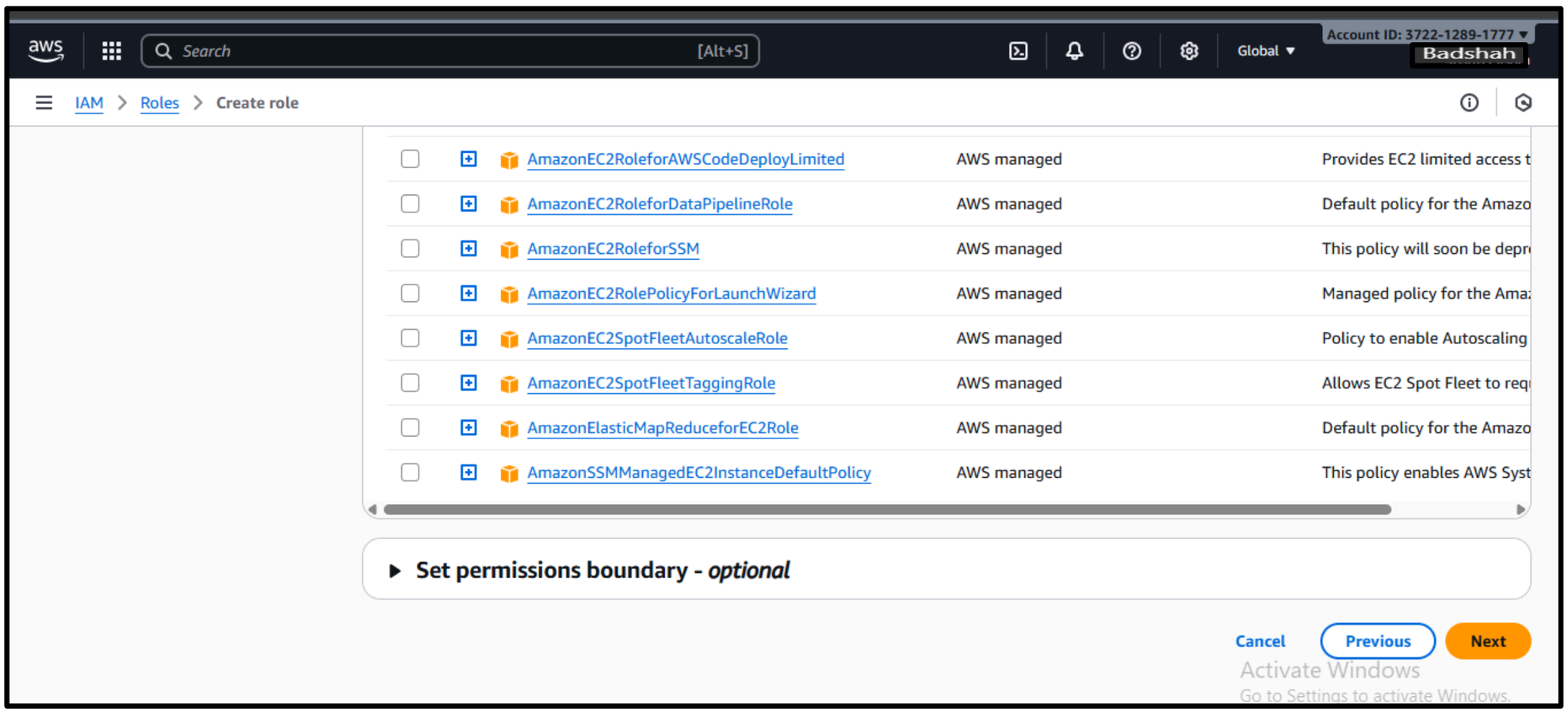
Click **Next** after selecting the appropriate option.



Step:-5Attach Permissions Policies:

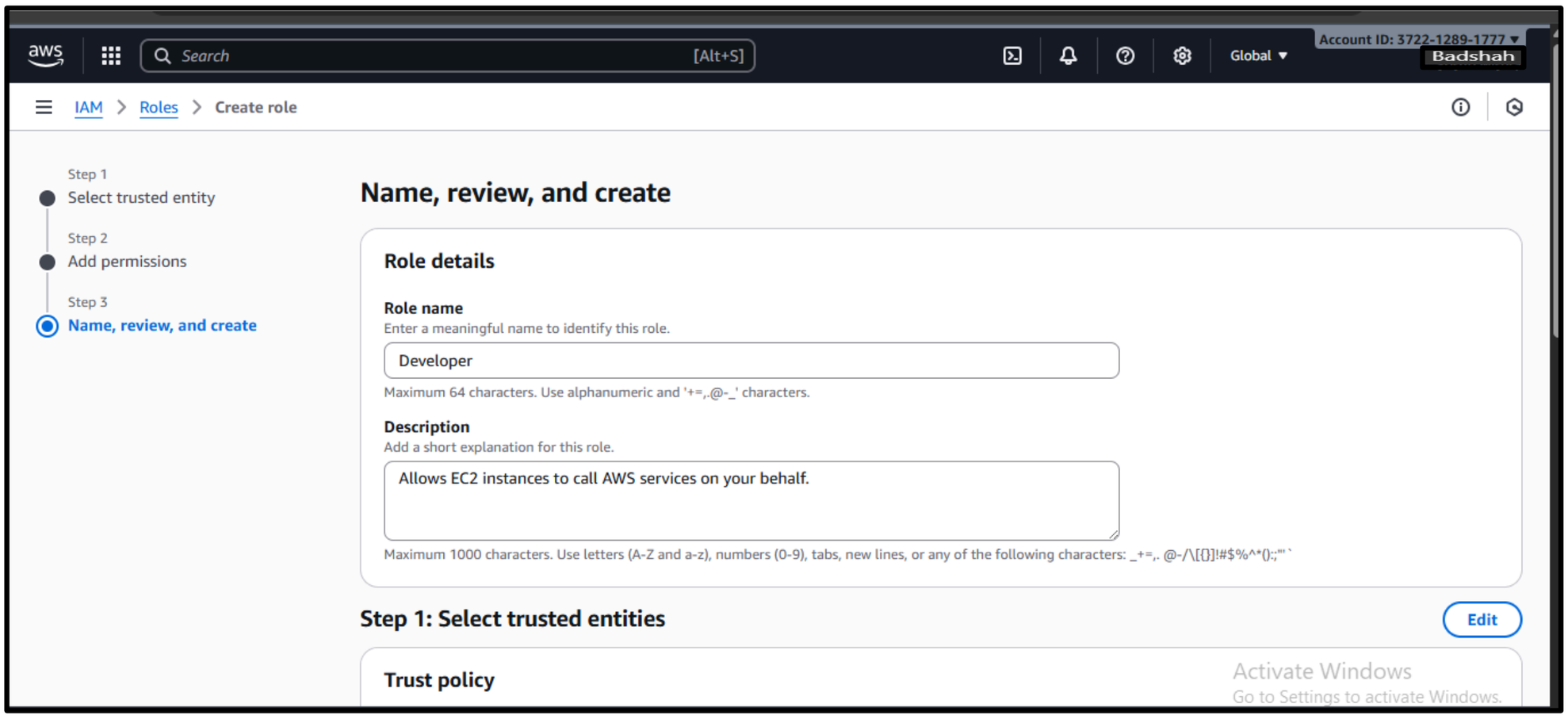
Select the **permissions policies** that define what actions the role can perform (for example, AmazonS3FullAccess or AmazonEC2FullAccess).

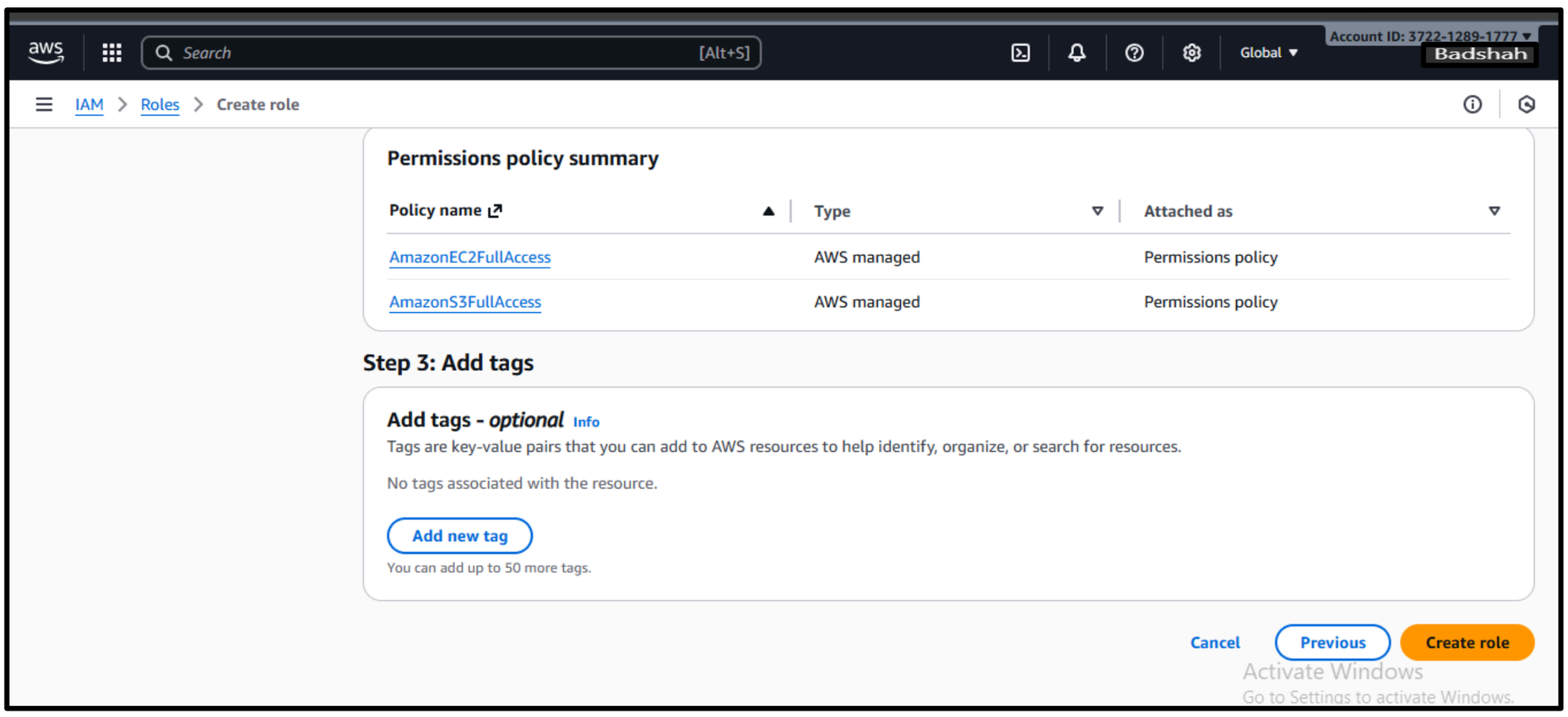




Step 6:- **Name and Review the Role:**

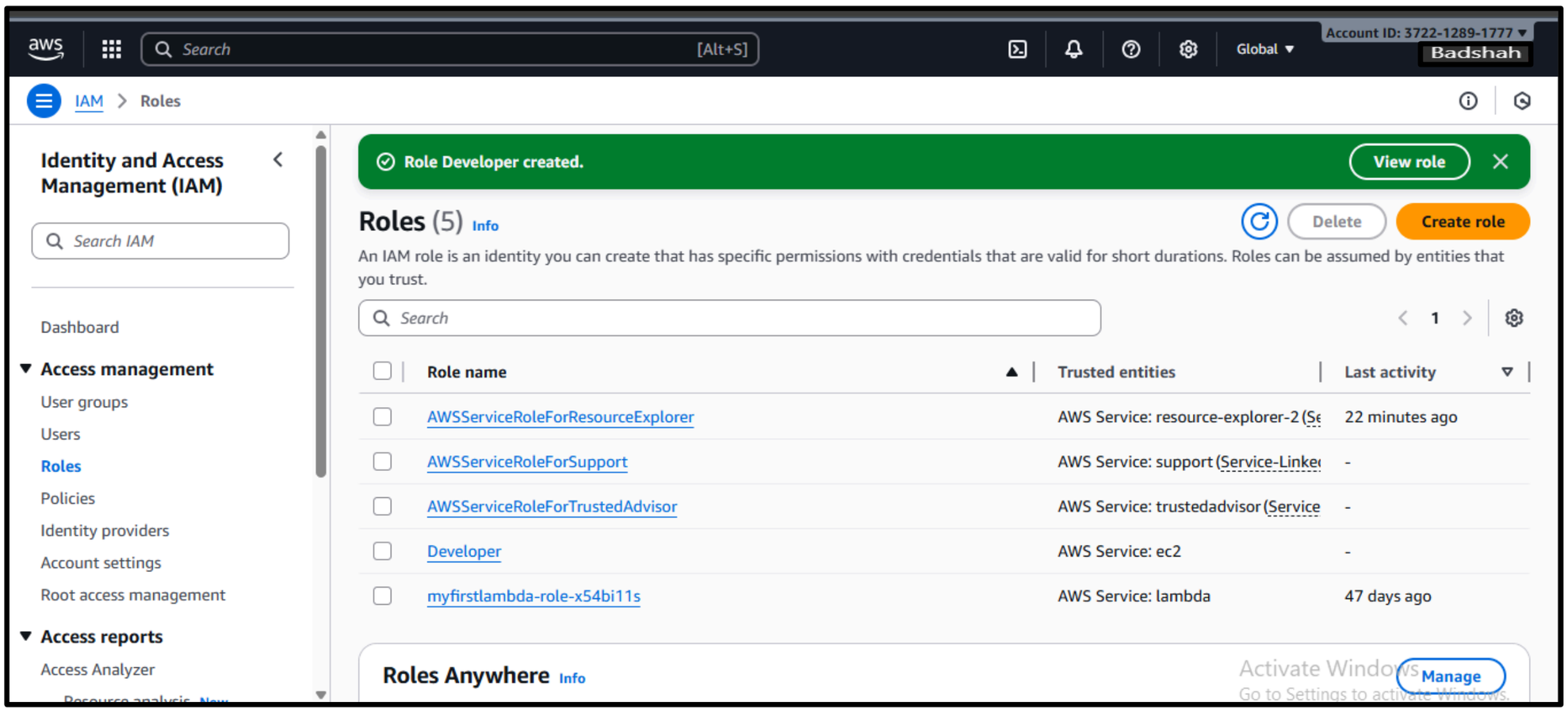
Enter a **role name** (for example, *EC2SecurityRole* or *LambdaAccessRole*) and review all selected settings.





Step 7:- **Create the Role:**

Click **Create role** to finish.


aws
Search
[Alt+S]
Global
Account ID: 3722-1289-1777
Badshah
IAM > Roles
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Access reports
Access Analyzer
Role Developer created.
View role
Roles (5) Info
Delete
Create role
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Search
1
Role name
Trusted entities
Last activity
AWSServiceRoleForResourceExplorer
AWS Service: resource-explorer-2 (Se
22 minutes ago
AWSServiceRoleForSupport
AWS Service: support (Service-Linke
-
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (Service
-
Developer
AWS Service: ec2
-
myfirstlambda-role-x54bi11s
AWS Service: lambda
47 days ago
Roles Anywhere Info
Manage
Activate Windows
Go to Settings to activate Windows.