Q5 : Create an IAM group named Developers with permission to only manage EC2 instances.

1. Creating the IAM Group "Developers"

1. Log in to the AWS Management Console.
2. Navigate to the IAM (Identity and Access Management) Console.
3. Click on Groups in the left panel.
4. Click Create New Group and enter the group name as Developers.
5. Click Next Step and proceed to attach a policy.
6. Search for AmazonEC2FullAccess and select it.
7. Click Next Step and then Create Group.

2. Creating the IAM User "Developer-Demo" and Adding to Group

1. In the IAM Console, click **Users** from the left panel.
2. Click **Add User** and enter **Developer-Demo** as the username.
3. Click **Add User to Group** and select **Developers**.
4. Click **Next** and then **Create User**.

3. Creating an EC2 Instance

1. Go to the **EC2 Console**.
2. Click **Launch Instance**.
3. Choose an appropriate **Amazon Machine Image (AMI)**.
4. Select an **Instance Type** (e.g., t2.micro).
5. Configure settings and add storage as needed.
6. Select or create a **Key Pair** for SSH access.
7. Click **Launch Instance** and wait for it to start.

4. Switching to Root Account and Creating an Access Key for Developer-Demo

1. Log in as the **Root User** or an **Admin IAM User**.
2. Go to **IAM Console** → Click **Users**.
3. Select **Developer-Demo**.
4. Click **Security Credentials** → Scroll to **Access Keys**.
5. Click **Create Access Key** and download the credentials.

5. Configuring AWS CLI for Developer-Demo User

1. Open **Command Prompt (Windows) or Terminal (Mac/Linux)**.
2. Run the following command: **aws configure**
3. Enter the **Access Key ID** and **Secret Access Key** from the previous step.
4. Set the **default region** (e.g., us-east-1).
5. Press **Enter** for the output format (defaults to JSON).

```
C:\Users\Harshitha Basavaraju>aws configure
AWS Access Key ID [****************JG2P]: AKIA52J2NMSVFV5SNPRJ
AWS Secret Access Key [****************FI93]: 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
Default region name [us-west-2]: us-west-2
Default output format [json]: json
```

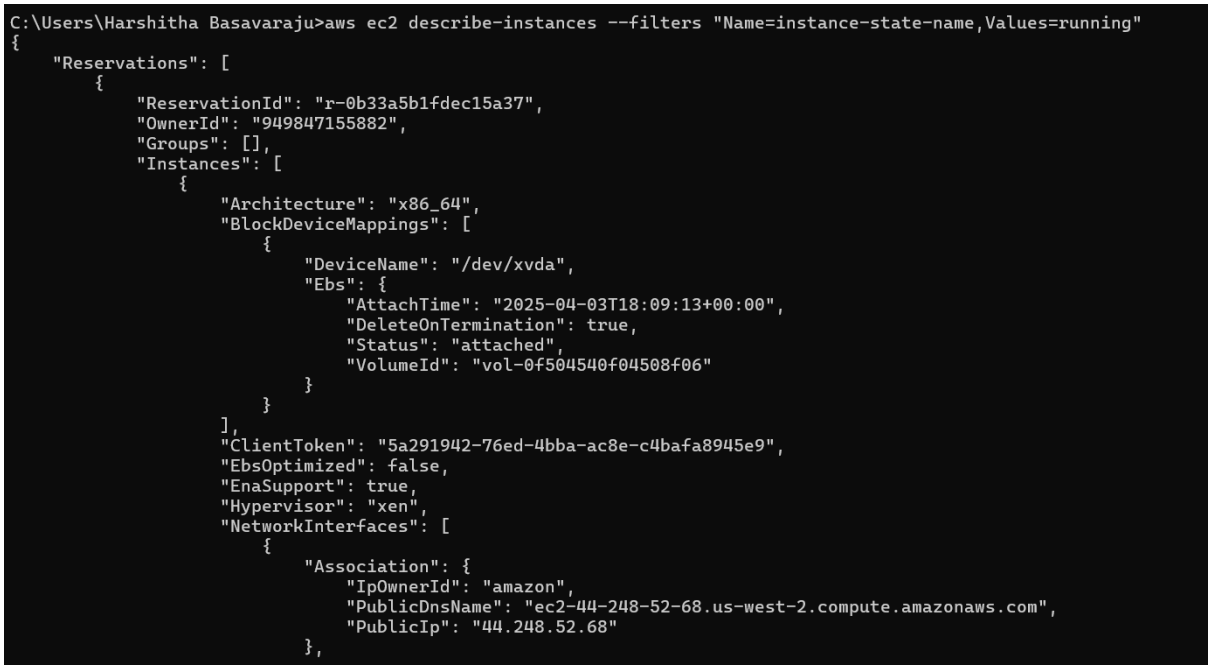
6. Verifying EC2 Instance Access

Check Running Instances

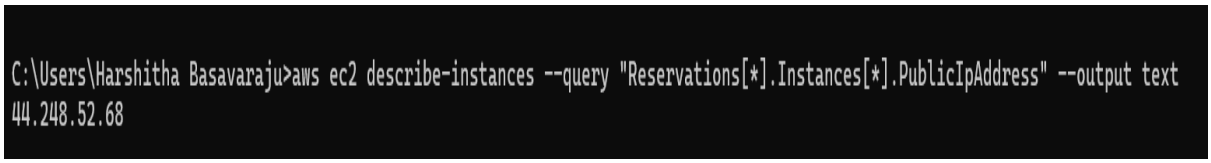
Run the following command to list running EC2 instances:

RUN : **aws ec2 describe-instances --filters "Name=instance-state-name,Values=running"**

Retrieve the Public IP Address of the Instance

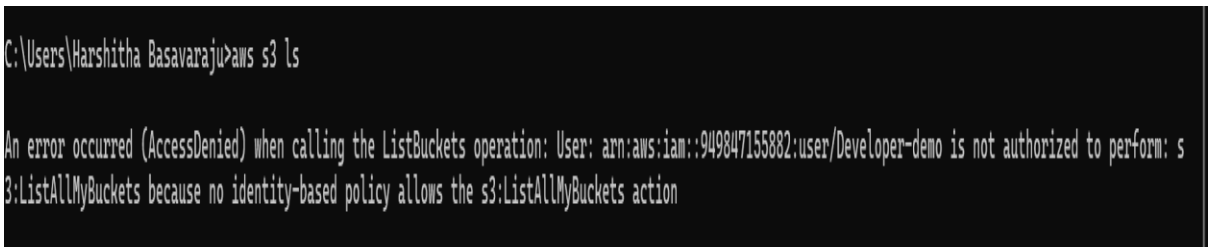


RUN : **aws ec2 describe-instances --query "Reservations[*].Instances[*].PublicIpAddress" --output text**



7. Verifying Access Restrictions (S3 Access Denied)

To ensure the user **only has EC2 access**, attempt to list S3 buckets: **aws s3 ls**



This confirms that **Developer-Demo** cannot access S3, maintaining the intended restrictions.