Step 1: Create an S3 Bucket and Upload a File

1. **Create an S3 Bucket:**
    - Open the **AWS Management Console**.
    - Go to **S3** → Click **Create Bucket**.
    - Enter a **unique bucket name** (e.g., mys3demobucket2020).
    - Choose a **region** and keep other settings default.
    - Click **Create bucket**.
2. **Upload a File to the S3 Bucket:**
    - Open the **S3 bucket** you just created.
    - Click **Upload** → **Add files**.
    - Select a file (e.g., aws.txt).
    - Click **Upload** to store the file in S3.

Step 2: Create an IAM Role for S3 Read-Only Access

1. **Open the IAM Console:**
    - Go to the **AWS Management Console** → Open the **IAM** service.
2. **Create a New IAM Role:**
    - Click **Roles** → **Create Role**.
    - Select **AWS Service** as the trusted entity.
    - Choose **EC2** as the use case.
    - Click **Next**.
3. **Attach the S3 Read-Only Policy:**
    - In the **Permissions** section, search for AmazonS3ReadOnlyAccess.
    - Select it and click **Next**.
4. **Name the Role:**
    - Enter the role name as **EC2S3ReadOnlyRole**.
    - Click **Create role**.
5. **Attach the IAM Role to the EC2 Instance:**
    - Open the **EC2 console** → Select your **EC2 instance**.
    - Click **Actions** → **Security** → **Modify IAM Role**.
    - Choose **EC2S3ReadOnlyRole** from the dropdown and click **Update IAM Role**.

Step 3: Verify IAM Role by Accessing S3 from EC2

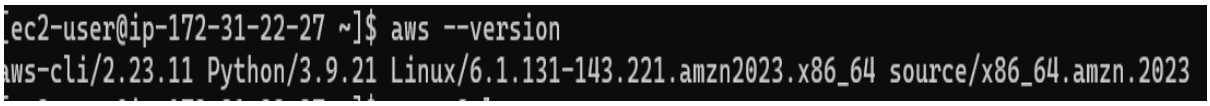
1. **Connect to the EC2 Instance:**
    - Open **Command Prompt (Windows)** or **Terminal (Mac/Linux)**.
    - Use SSH to connect to the EC2 instance:

RUN **: ssh -i "C:\Users\Harshitha Basavaraju\Downloads\myec2instance.pem" ec2-user@<EC2-Public-IP>**

Type yes when prompted to confirm the connection.

Check if AWS CLI is Installed:

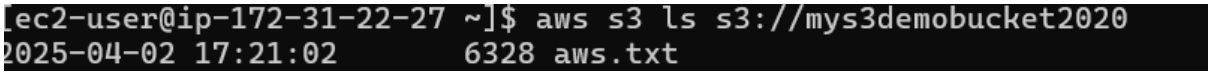
- Run the following command to verify AWS CLI installation: **aws –version**
- If installed, you should see an output like:



List S3 Buckets:

- Run the command: **aws s3 ls**
- Run the command to download a file from the S3 bucket:

  aws s3 cp s3://mys3demobucket2020/aws.txt .
- Read from S3 **: aws s3 cp s3://mys3demobucket2020/aws.txt .**



- Delete from S3**: aws s3 rm s3://mys3demobucket2020/aws.txt**
  Since the IAM role EC2S3ReadOnlyRole only grants read access, the delete command should return an "Access Denied" error. This confirms that the role is correctly configured with read-only permissions**.**