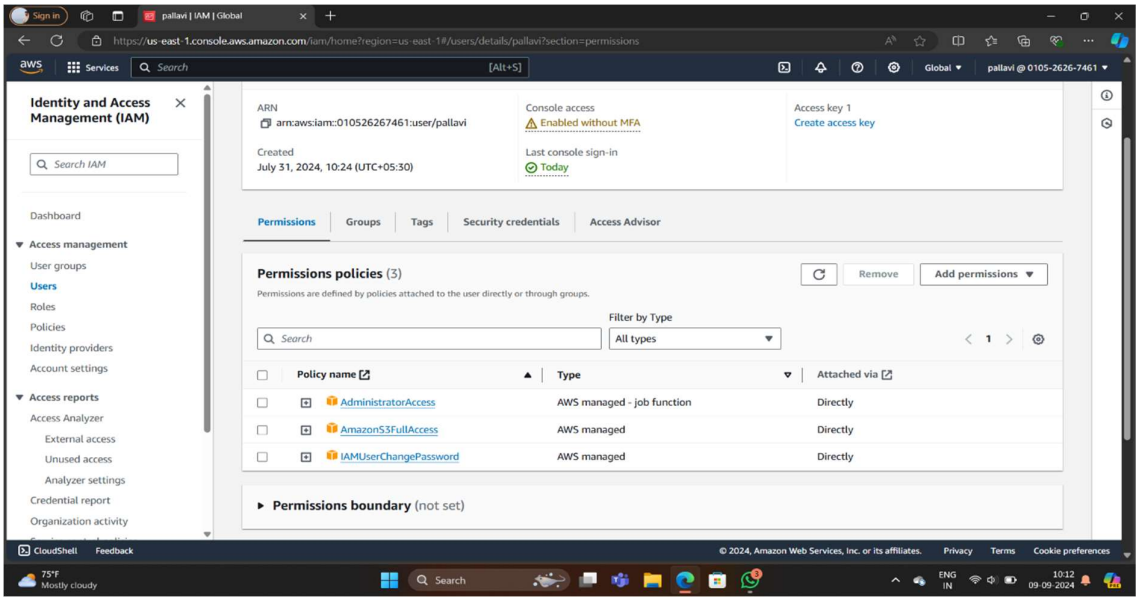
ACCESS S3 OBJECTS FROM EC2 INSTANCE

➢ Create an IAM instance profile that grants access to Amazon S3

Complete the following steps:

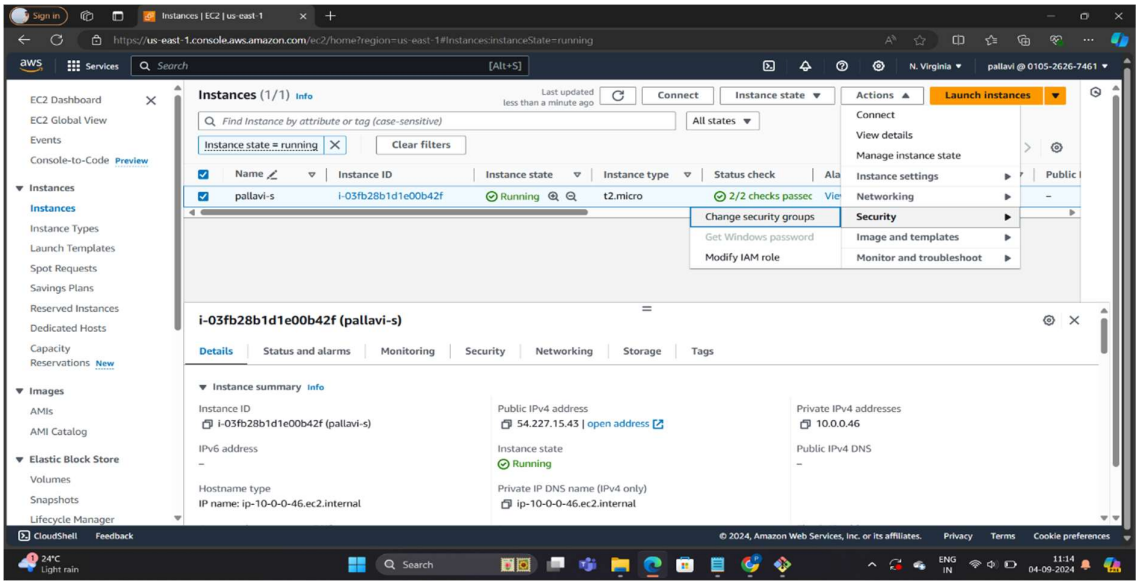
- Open the **AWS Identity and Access Management (IAM) console.**
- In the navigation pane, under **Access management**, choose **Roles.**
- Choose Create role.
- Under Trusted entity type, choose **AWS service**, and then choose **EC2**.
- Choose Next.
- Create a custom policy that provides the minimum required permissions to **access your S3 bucket.**
  Note: It's a security best practice to create a policy with the minimum required permissions. However, to allow EC2 access to all your S3 buckets, use the **AmazonS3ReadOnlyAccess** or **AmazonS3FullAccess** managed IAM policy.
- Choose Next.
- Enter a role name, and then choose Create role.

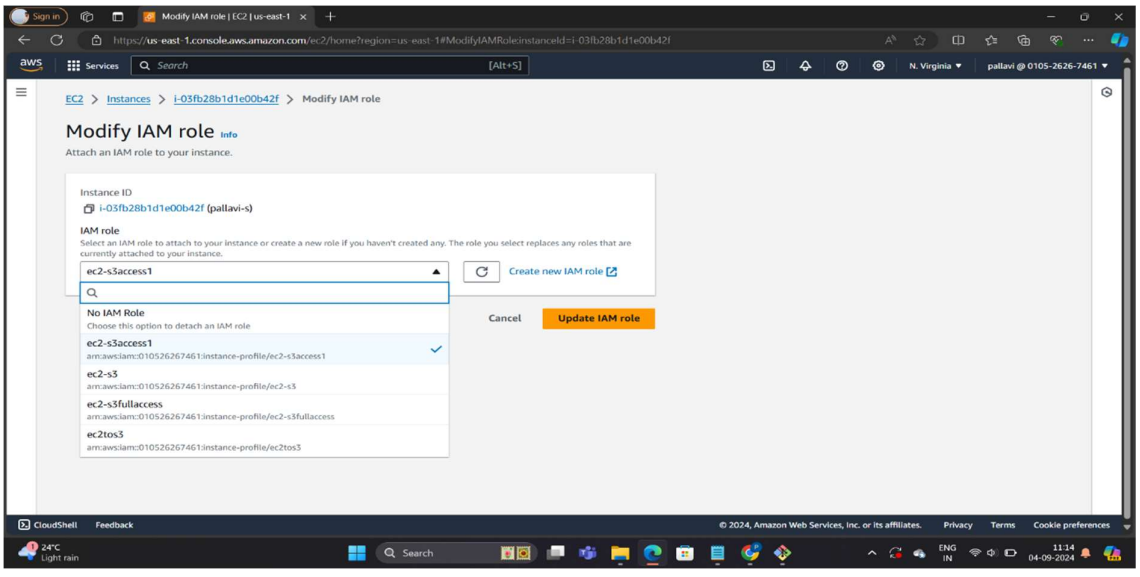


➢ Attach the IAM instance profile to the EC2 instance

Complete the following steps:

- Open the Amazon EC2 console.
- In the navigation pane, choose Instances.
- Select the instance that you want to attach the IAM role to.
- Choose the Actions tab, and then choose Security.
- Choose Modify IAM role.
- Select the IAM role, and then choose Save. The IAM role is assigned to your EC2 instance





➢ Verify access to S3 buckets

Complete the following steps:

Note: If you receive errors when you run AWS Command Line Interface (AWS CLI) commands, then see Troubleshoot AWS CLI errors. Also, make sure that you're using the most recent AWS CLI version.

- Install the AWS CLI on your EC2 instance.
- Run the following command to verify access to your S3 buckets:

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET
```