AWS Lab 27

IAM Role

Overview of the lab

In this lab you will learn how EC2 instance in public subnet uses the IAM role to access S3 bucket

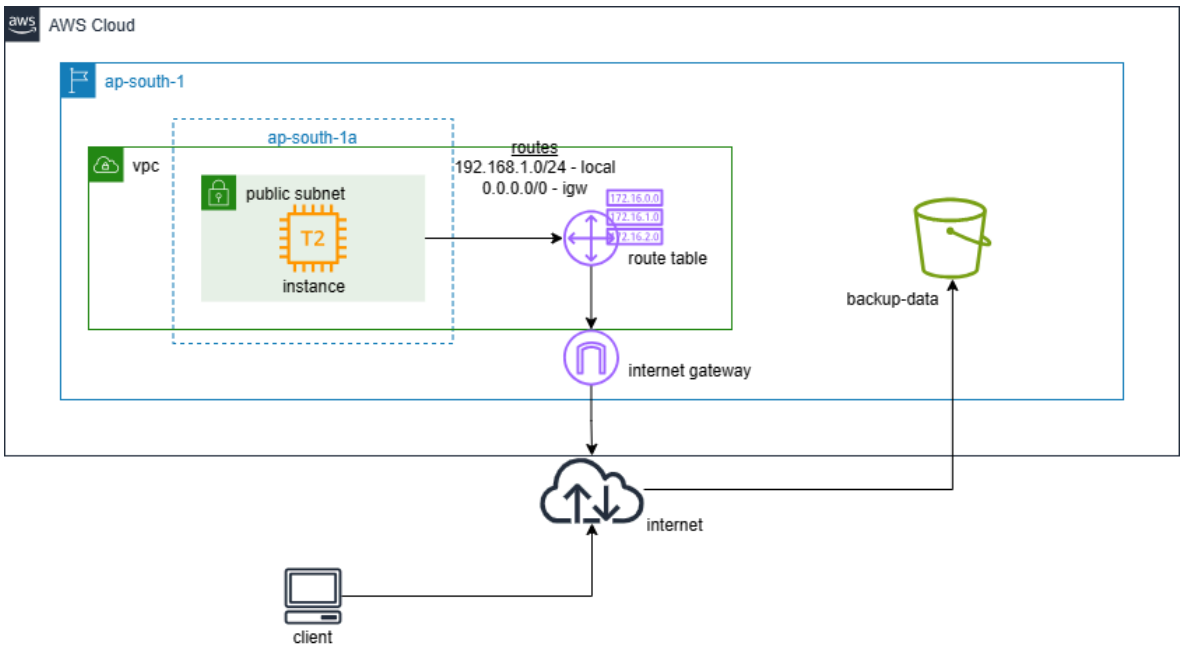
IAM Role

It is a short term credential with the permission to access services

AWS CLI in Amazon Linux

It comes pre installed with amazon linux

Initial Architecture



Step by Step Lab

Launch instance

1. In EC2 management console, launch instance
   1.1. Name and tag – linux-server
   1.2. Application and OS Images – Amazon Linux
   1.3. Instance type - t2.micro
   1.4. Key pair – select the existing keypair
   1.5. Edit Network settings
      a. Subnet – subnet in ap-south-1a (even no preference is fine)
      b. Firewall – select existing security group
2. Number of instances - 1 (Leave all other settings as default and launch instance)

Create S3 Bucket

3. In S3 Management Console
   3.1. Bucket name - backup-data (replace bucket name)
   3.2. AWS Region - Asia Pacific (Mumbai) ap-south-1
4. Click on Create bucket

Try Uploading data from EC2 to S3

5. Login to instance via EC2 instance connect and execute the following commands

```
#create a file
echo hello > sample.txt
#upload the file to s3 bucket (this will fail)
aws s3 cp sample.txt s3://backup-data    (replace bucket name)
```

Create IAM Role

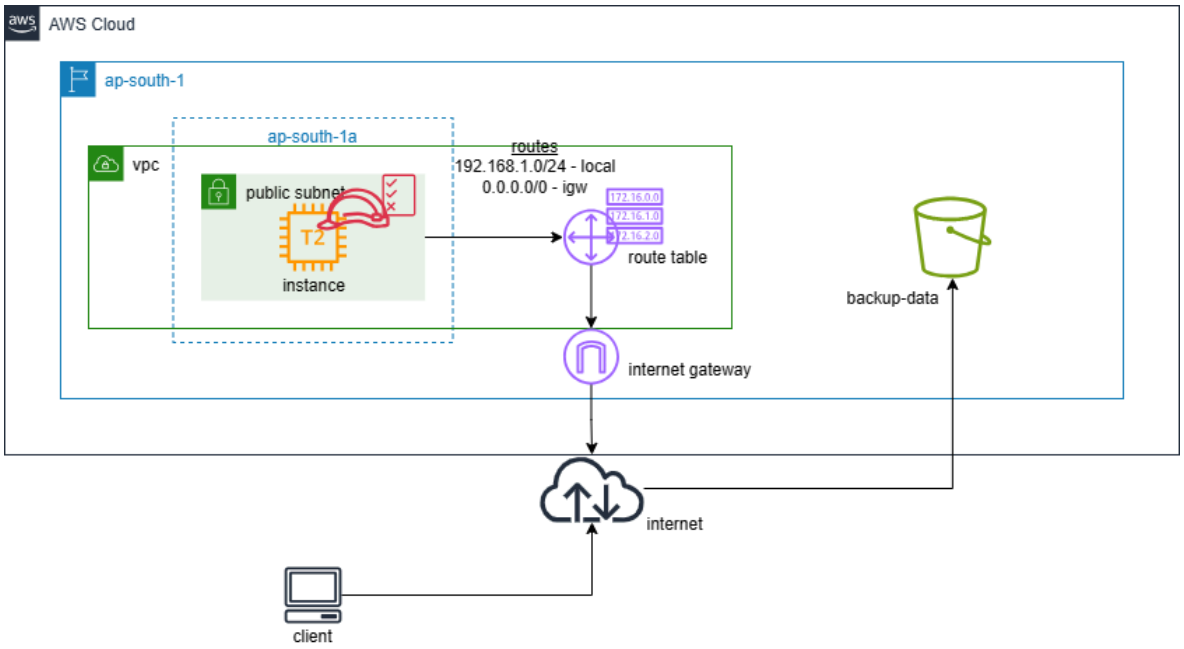
6. In IAM - click on Roles
7. Click on Create role
   7.1. Trusted entity type - AWS service
   7.2. Use case - Service or use case - EC2 - click on Next
   7.3. Permissions policies - Select - AmazonS3FullAccess - click on Next
   7.4. Role name - ec2-accessing-s3
8. Click on Create role

Map IAM Role to EC2 Instance

9. In EC2 - select the linux-server instance, In Actions Click on Security and Modify IAM role
10. IAM role - choose IAM role (ec2-accessing-s3)

11. Click on Update IAM role

Final Architecture



Upload data from EC2 to S3

12. Login to the linux instance via EC2 Instance Connect
13. Try uploading the same file using aws cli command (this time it will work)

    #upload the file to s3 bucket

    aws s3 cp sample.txt s3://backup-data (replace bucket name)

Clean Up Step

1. Select the instance and terminate it