IAM Role

Role is a set of permissions given to internally communicate between two AWS services.

To create role, first create a VPC with two subnets

*IPv4 VPC CIDR block 10.0.0.0/24*

*IPv4 subnet1 CIDR block:10.0.0.0/25 (publicsubnet - eu-west-2a)*

*IPv4 subnet2 CIDR block: 10.0.0.128/25(privatesubnet - eu-west-2b)*

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

 I have created all new VPC, Subnets, IG, RT, PRT, NAT for this project.

VPC

A screenshot of a computer

Description automatically generated

2 Subnets, 1 public and 1 private

A screenshot of a computer

Description automatically generated

Internet Gateway and attached to VPC

A screenshot of a computer

Description automatically generated

Created RT for public and also **private** (not necessary, to connect NAT gateway)

A screenshot of a computer

Description automatically generated

NAT step is not necessary for this LAB, but I have created, out of interest!!! To check private server gets internet or not, it does!

A screenshot of a computer

Description automatically generated

Now, let’s connect the public server and see, if we can connect s3 via public server or not!!!

Public server is connected but unable to list another AWS service say s3

A screenshot of a computer

Description automatically generated

We can communicate server or work on s3 externally using CLI method by using aws configure with its access key and secret key

But, to communicate AWS services internally, for example, a server and s3, we need a IAM ROLE

Steps to connect s3 externally or from Locally we need the following …

1. Install AWS CLI
2. Configure keys (root or user)
3. Connect services

IAM ROLE:

Steps to connect s3 internally between two services, say from ec2 to s3, we need the following …

1. Create IAM Role
2. Attach permission S3 and SNS
3. Attach role to required ec2 instance

Let’s create a role to connect ec2 and s3

IAM -> Role -> Create Role - select use case: EC2 from the list > next

Add permission -> search s3 full access > next

Give role name > rolepublicserver -> **Create role**

We have now created a role for ec2 to connect s3 buckets

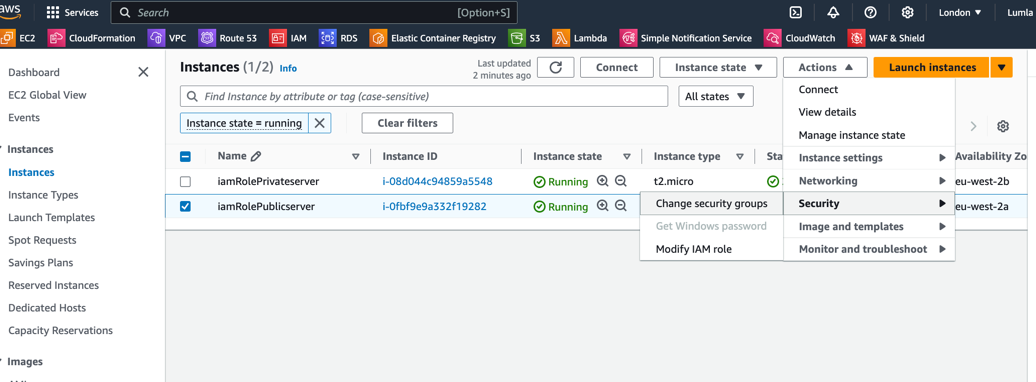
A screenshot of a computer

Description automatically generated

Now, go to public server and try and connect it, it will show s3 buckets ☺

But, before that, for the role to work, we need to do one more step, which is adding security by attaching the role to ec2

Go to EC2 > select iamRolePublicServer > action > security ->Modify IAM Role



Select the role from the dropdown, that we just created for ec2 to connect s3 which is **rolepublicserver > update IAM role**

A screenshot of a computer

Description automatically generated

**Note: IAM role** is for connecting AWS services **internally** and that's the ideal way too, but if you are connecting AWS services from **external**, then, go for **CLI method.**

 See, now we can see all the s3 buckets via ec2 connection

A computer screen shot of a black screen

Description automatically generated

Note: At the moment, Aws provides **two most commonly used services** for connecting other AWS services like s3, which is by EC2 and Lambda

Also note: Login services can only access other services like EC2, but not s3, because s3 is not a Login service

A screenshot of a computer

Description automatically generated

Now, let's create a private server and connect it…

Before connecting, check your security group setting

A screenshot of a computer

Description automatically generated

All good to go…

Now take your ssh client details to connect the private server in public server

A screenshot of a computer

Description automatically generated

ssh -i "LondonKP.pem" ec2-user@10.0.0.228

vi LondonKP.pem

chmod 400 LondonKP.pem

Now, we have connected using private server

A screenshot of a computer screen

Description automatically generated

Now, how to access other services from private server? Ex: s3

S3 is outside of the VPC, how to connect private server?

A diagram of a cloud computing diagram

Description automatically generated

We have already connected public server and accessed S3 buckets internally!

A diagram of an application

Description automatically generated

To connect, private server to s3 with NAT is possible but without NAT, there is a way, that is called VPC endpoints

 My current IP for public and private servers

iamRolePublicServer has ip -> 10.0.0.85 for this address 3.8.124.145

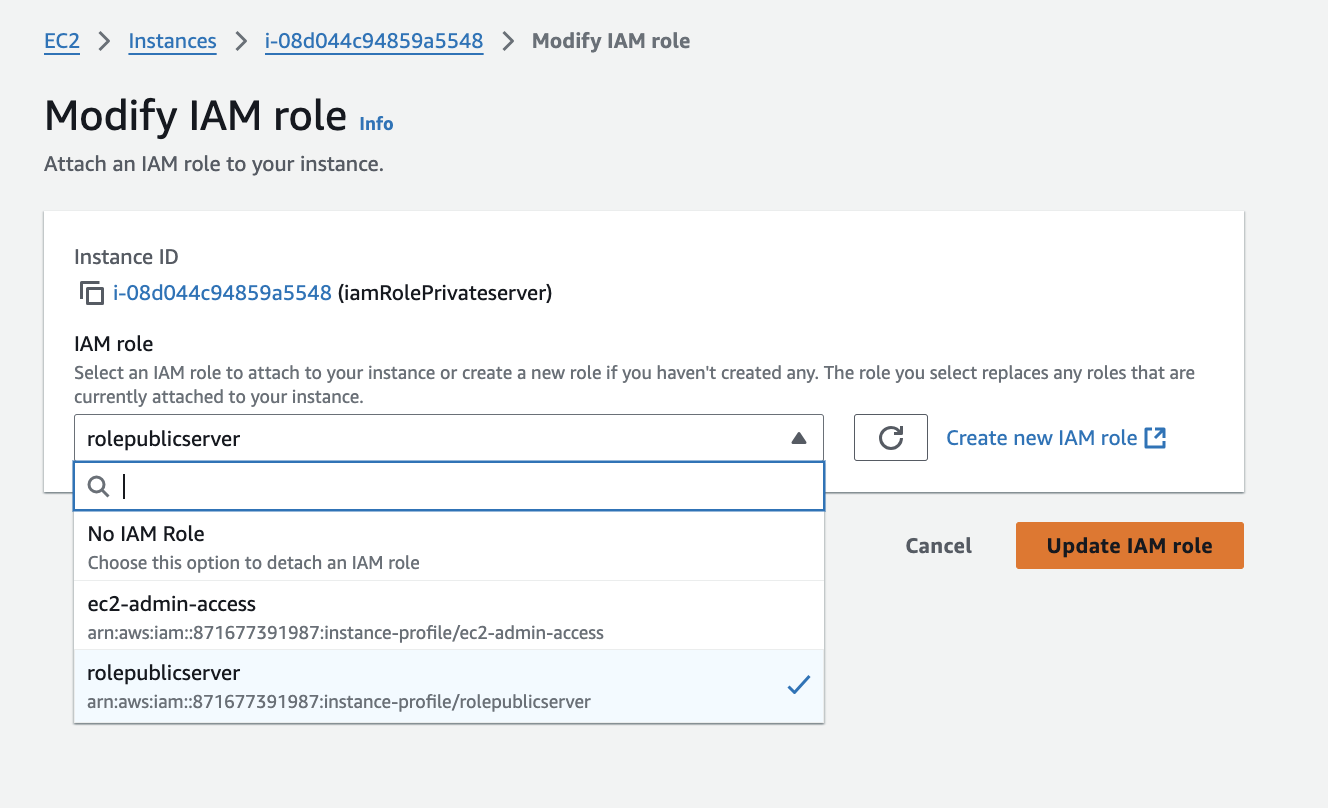
iamRolePrivateServer has ip -> 10.0.0.228

A computer screen shot of a black screen

Description automatically generated

Now, let’s give the role for iamRolePrivateServer, and see if we can access s3 or not??

Go to EC2 > select iamRolePrivateServer > action > security ->Modify IAM Role and update IAM role



A diagram of a connection

Description automatically generated

Unable to connect, even after giving role to private server, so to internally communicating from private server we need VPC endpoints, role just not enough!

VPC endpoints is used for connecting different AWS services without internet, and connection is also secure

Go to VPC > Endpoints > create endpoints

**Give name** tag- **Roleprivateendpoint**

**Services** - search s3 and choose **s3 gateway**

Network settings - Vpc - choose your VPC - **rolevpc**

**RouteRt -** choose your private RT **(imaRolePRT)**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Now go to your RT to check, whether this VPC endpoints is updated or not

Check in your **iamRolePRT, it is updated and also active!**

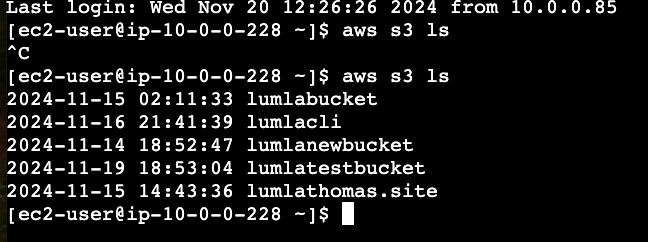
A screenshot of a computer

Description automatically generated

I am currently in my private server

A black screen with white text

Description automatically generated



A screenshot of a computer

Description automatically generated

iamRolePublicServer has ip -> 10.0.0.85

iamRolePrivateServer has ip -> 10.0.0.228

Now, even my private server is also showing s3 buckets :)

A screen shot of a computer

Description automatically generated

Now, let’s create an empty file called file1

A screenshot of a computer

Description automatically generated

If you give read only access to your role and attach to your private server, it will throw error like this …

A computer screen with white text

Description automatically generated

We need write permission to makebucket or createbucket in s3

use this command to make any s3 bucket

aws s3 mb s3://lumlarolebucket

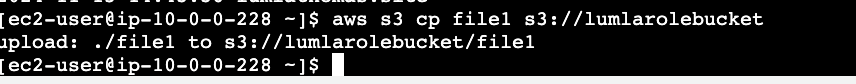
I have given all permission for the ec2 privateserver, hence I can create new bucket using private server

A screenshot of a computer

Description automatically generated

Now, l**et’s copy a file to the newly created bucket** using this below command..

aws s3 cp file1 s3://lumlarolebucket



Now, let's confirm the file1 is copied to the lumlarolebucket or not, by going to the s3 dashboard and bucket, yes, it is copied successfully!

A screenshot of a computer

Description automatically generated

We can also copy file1 to any particular folder too…

aws s3 cp file1 s3://lumlarolebucket/testrole/

A black and white text

Description automatically generated

A screenshot of a computer

Description automatically generated

Now, let’s stop the instances running using this command prompt/terminal for public server

aws ec2 stop-instances --instance-ids i-0fbf9e9a332f19282

Couldn’t stop the server, throws this error

A black and white screen

Description automatically generated

Maybe, I am in private server. Let’s see …

Let's take the private instance id and then try to stop the server

aws ec2 stop-instances --instance-ids i-08d044c94859a5548

Throws the same error for both instance ids

A screen shot of a computer screen

Description automatically generated

 Let’s try and use this command to stop a server

sudo init 0

- undefined 
sudo init O 
init 1 
init 2 
init 3 
init 5 
init 6 
init 4 
shutdown 
single user mode no GUI 
multi user- no nw no GUI 
multi user - NW Access No GUI 
multi user - NW access GUI 
RESTART THE SERVER! 

A screenshot of a computer program

Description automatically generated

Now, let’s check in the EC2 dashboard, if it is stopped or not!

Yes, it is stopped, but now only my public server is running…

A screenshot of a computer

Description automatically generated

I have given s**udo init 0** again

Now, both the servers have been stopped.

A screenshot of a computer

Description automatically generated

 Lab done! ☺