AWS Lab 28

VPC Endpoint

Overview of the lab

In this lab you will learn how EC2 instance(s) in private subnet uses the IAM role & VPC Endpoint to access S3 bucket

IAM Role

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

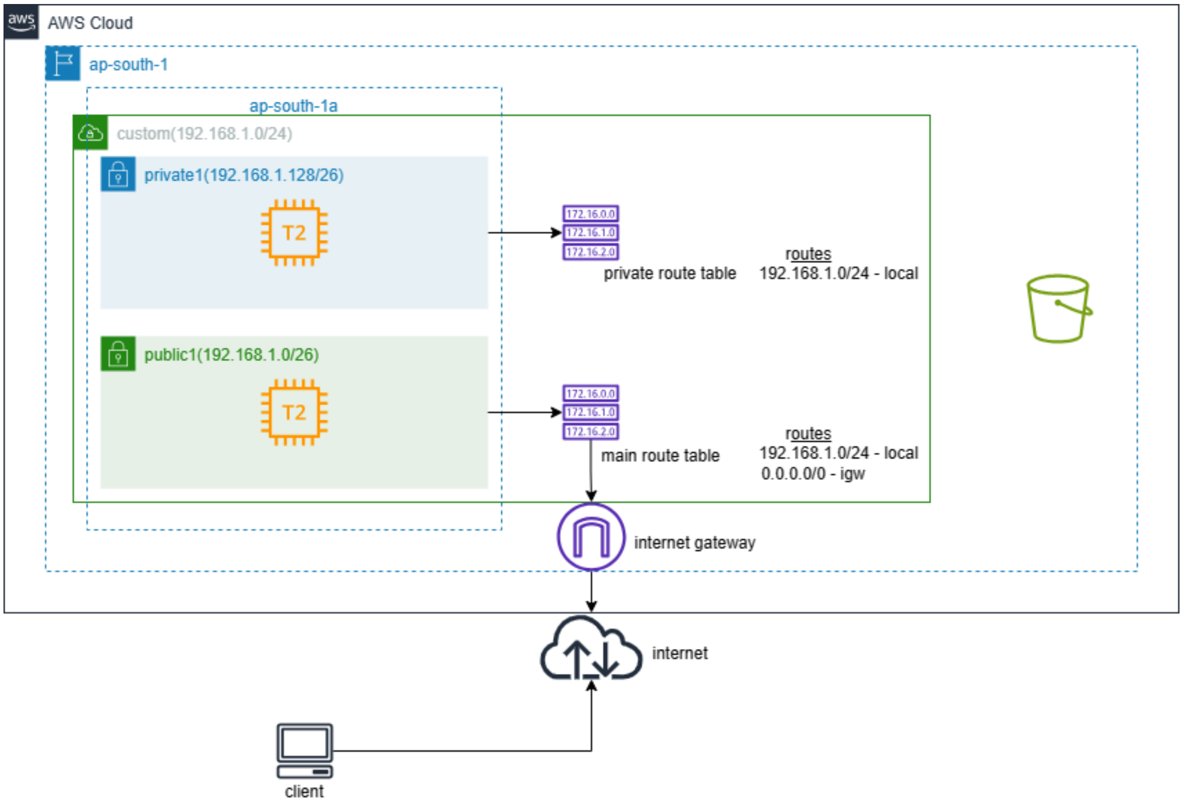
AWS CLI in Amazon Linux

It comes pre installed with amazon linux

VPC Endpoint

It is a private link, resources within VPC uses this link to connect public services (eg: s3, dynamodb) internally

Initial Architecture



Step by Step Lab

Launch instance in public subnet with public IP

1. In EC2 management console, click on launch instance
   a. Name and tag – linux-public
   b. Application and OS Images – Amazon Linux
   c. Instance type - t2.micro
   d. Key pair – select the existing keypair
   e. Edit Network settings
      a. VPC - custom-vpc

   b. Subnet – custom-vpc-public1
   c. Auto-assign public IP - Enable
   d. Firewall – Select existing security group
   e. Common security groups - custom-vpc-sg

f. Click on Advanced details - IAM instance profile - Select ec2-accessing-s3 (created in previous lab)
g. Click on launch instance

Launch instance in private subnet without public IP

2. Again click on launch instance
   a. Name and tag – linux-private
   b. Application and OS Images – Amazon Linux
   c. Instance type - t2.micro
   d. Key pair – select the existing keypair
   e. Edit Network settings
      i. VPC - custom-vpc
      ii. Subnet – custom-vpc-private1
      iii. Auto-assign public IP - Disable
      iv. Firewall – Select existing security group
      v. Common security groups - custom-vpc-demo-sg
   f. Click on Advanced details - IAM instance profile - Select ec2-accessing-s3 (created in previous lab)
   g. Click on launch instance

Login to instance in public subnet via SSH using public IP address

```
ssh -i "ssh-private-key.pem" ec2-user@<public_ip>
```

Login to instance in private subnet via SSH using private IP address from public subnet instance

#create the private key within public subnet instance

```
vi ssh-private-key.pem
```

<copy the content of private key from local computer>

```
Esc
:wq
```

#change the permission for the key

```
chmod 600 ssh-private-key.pem
```

#login to private subnet instance

```
ssh -i "ssh-private-key.pem" ec2-user@<private_ip>
```

#create a test file

```
echo hello > hello.txt
```

#use aws cli command to copy file to s3

```
aws s3 cp hello.txt s3://bucket-name --region ap-south-1
```

(This will timeout & fail since private subnet instance does not have route to reach internet & s3 is a public service)

VPC Endpoint for creating a private link from VPC to s3

3. In VPC - Click on Endpoints
    a. Click on Create endpoint
    b. Name tag - demo-vpc-endpoint
    c. Service Category - AWS services

    d. Services - search s3 and select Gateway type
    e. Select the VPC (custom-vpc)
    f. Route tables - select custom-vpc-private-rt
4. Click on Create endpoint

(Route to reach s3 will be added to private route table)

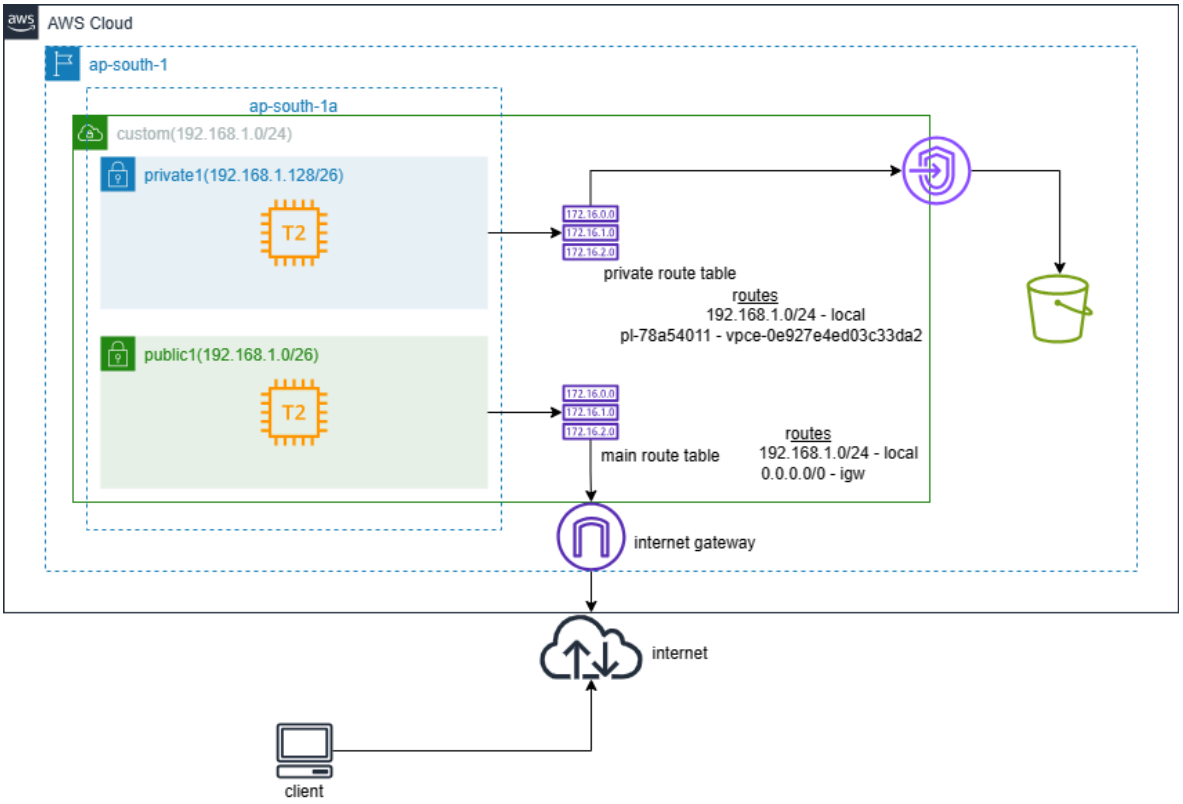
5. again from the private subnet instance

#use aws cli command to copy file to s3

```
aws s3 cp hello.txt s3://bucket-name --region ap-south-1
```

(This will work)

Final Architecture



Clean Up Step

1. In EC2 - Select the instances and terminate it
2. In VPC - Select the endpoint and delete it