VPC (ENDPOINT)

# Region is most imp for this task

Agar app bina internet pe jaye AWS ke resources ko use karna chahate hai to ye possible hai vpc endpoint se.

Isse pehale NAT Gateway se possible tha , NAT gateway se data ( 10 gb) ko share karneka bill jyada ata tha, upper se NAT ka bill bharna padta tha.5

VPC Endpoint free hai or data transefer ka bill hai vo kafi kam ata hai.

VPC Endpoint se privately data ko access karna or share karna possible hai.

A vpc endpoint enables you to privately connect your vpc to supported AWS services . Instance in your vpc do not require public IP addresses to communicate with resources in the service.

Vpc Endpoint is a virtual device , it is not available in hardware it is available in Virtually cloud device , it is not physically show but you can access it.

 Endpoint are virtual device

Steps

**Go to the VPC**

Select **Your VPCs**

Select **vpc** only

Name:- **end-point**

Put ip **192.168.0.0/20** this is used subnetting concept

Tenancy – **Default**  --- if you are change then you pay money

**Create VPC**

Go to **subnet**

Now you see the default subnet

Create **new subnet first**

Select vpc Id :- **public-sub**

Put Subnet name:- **my-sub**

Availability zone :select **any one 1a**

Ipv4 CIDR block :- put **192.168.1.0/24**

**Create subnet**

Create **new subnet second**

Select vpc Id :- **private-sub**

Put Subnet name:- **my-sub**

Availability zone :select **any one 1c**

Ipv4 CIDR block :- put **192.168.2.0/24**

**Create subnet**

Go to **internet getways**

**Create internet getway**

**Name:- endpoint-IG**

**Create gate way**

Go to the **internet getway**

Select **endpoint-IG**

Select **action**

**Attach vpc**

**Create route table first**

Name:- **public-RT**

Vpc :-**endpoint**

**Create route table**

**Select public-RT**

**Edit route :- 0.0.0.0/0 select :-internet getway save**

**Edit subnet association :- select :- public save**

**Create route table Second**

Name:- **Private-RT**

Vpc :-**endpoint**

**Create route table**

**Select public-RT**

**Edit subnet association :- select :- Private save**

Go to the **instance**

Go to **EC2**

* **Launch instance** **first**

Name:- **public-instance**

**Ami**

**T2 micro**

Key name:- **newkey**

**Network setting:- select vpc :-endpoint select sub:- public sub Auto-assign public ip:- Enable**

Create security group

Name:- endpoint security

Ssh – anywhere

**Launch**

* **Launch instance** **second**

Name:- **private-instance**

**Ami**

**T2 micro**

Key name:- **newkey**

**Network setting:- select vpc :-endpoint select sub:- private sub Auto-assign public ip:- Disable**

Selelct existing group

Endpoint security

Ssh – anywhere

**Launch**

**Select public instance & connect**

**Go to the gitbash**

**Cd download**

**Scp -I newkey.pem newkey.pem ec2-user@pub-ip:/home/ec2-user ---** ye hame by scp command se public sub me key bhejna hai

Then go to the **public-instance terminal**

**Ls** – now you see the key is on terminal

**Sudo chmod 700 newkey.pem**  first permission set on this key

Then

**Ssh -I newkey.pem ec2-user@private-ip**

Now you see the private instance login on this console

But we want to access s3 bucket without internet then 1st we create a end point first

Go to the **vpc**

Select **endpoint**

**Name:- my-end-point**

**Serach s3**

Select **:- service-name com.amazonaws.us-east-2.s3**

Select :- **gateway**

Select :- **vpc**

Select :- **private route**

**Create endpoint**

Go to **terminal**

**aws s3 ls** now you see the aws configure

**aws configure**

**put Access id :-**  you want access key go to the security credential

**put Secrate id :-**

**next**

**next**

then

aws s3 ls **--region=us-east-1** --- now you see the **buckets on your terminal**

us-east-1 this is north vergina region if you want to check region the go to the

vpc endpoint and check detail

if agr **ls** nhi ho raha hai to

create **iam role**

go to the **iam**

select **role**

**create role**

select :-**ec2**

serach s3 :- **s3 full access**

name:-**s3-endpoint**

**create role**

go the **instance**

select **private instance :-** **action**:- **security**:- **modified iam role**:- select role when we create (endpoint)

go the **terminal private instance**

**aws s3 ls –region=us-east-1** **now you see the bucket list on your account without internet by using end point**