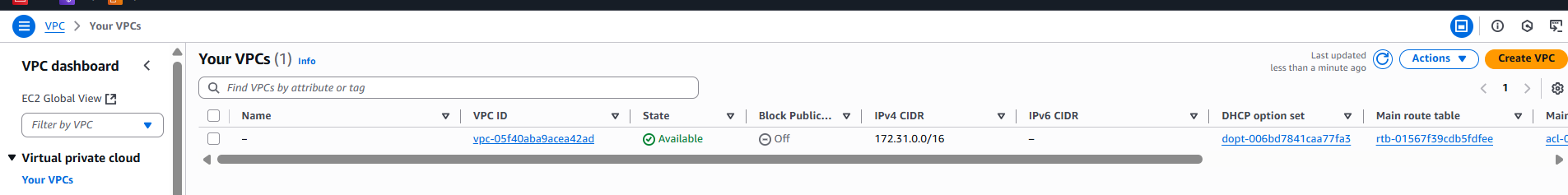
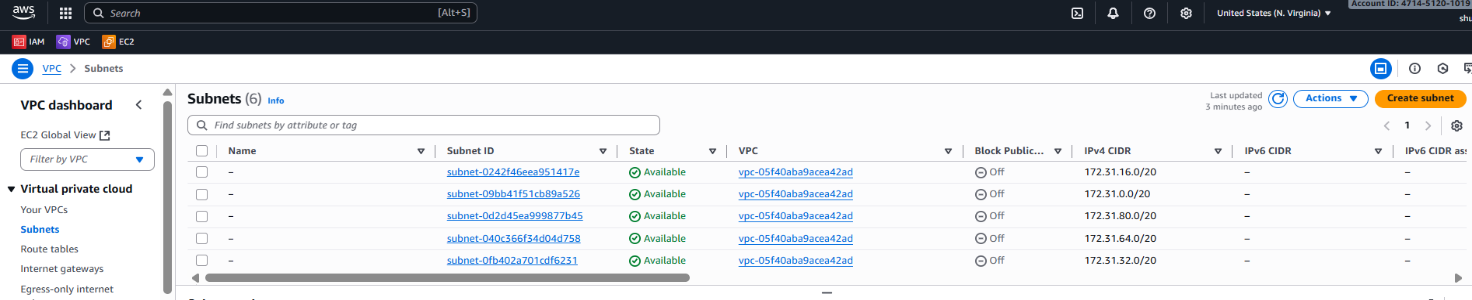
1. Create VPC with 2 private and 2 public subnets.
   1. Create vpc

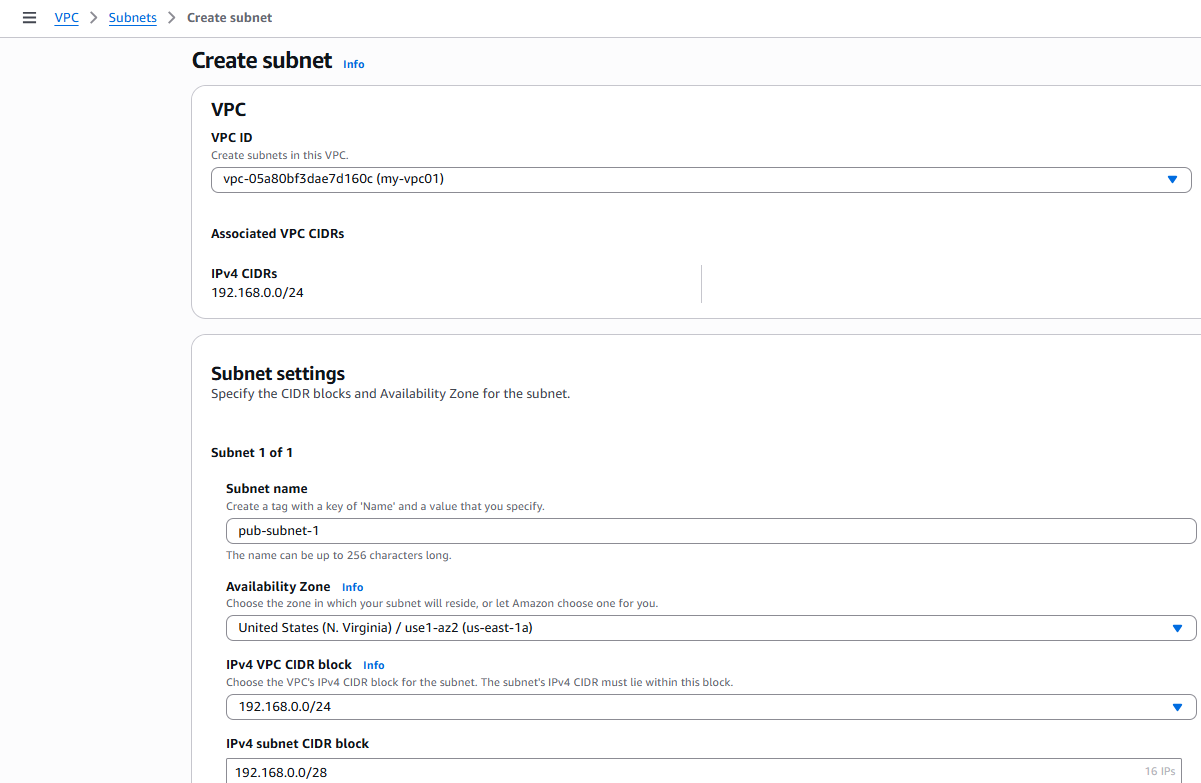


* 1. Give name for vpc and cidr range:

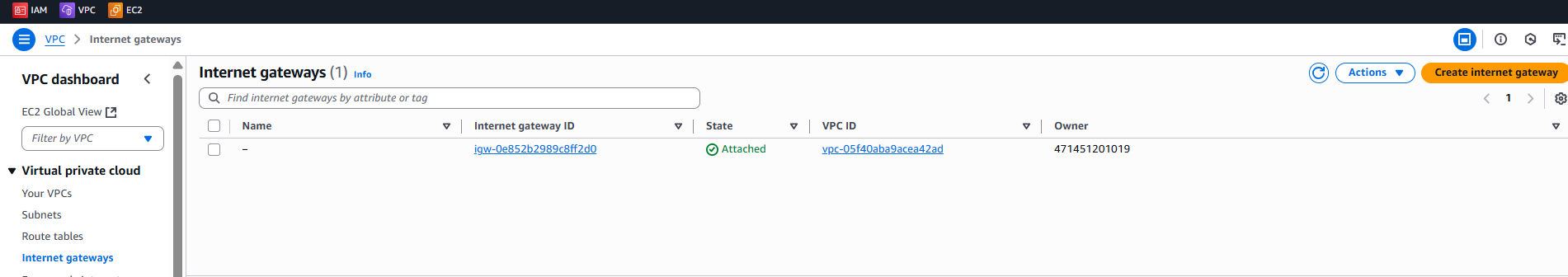


Create subnet:

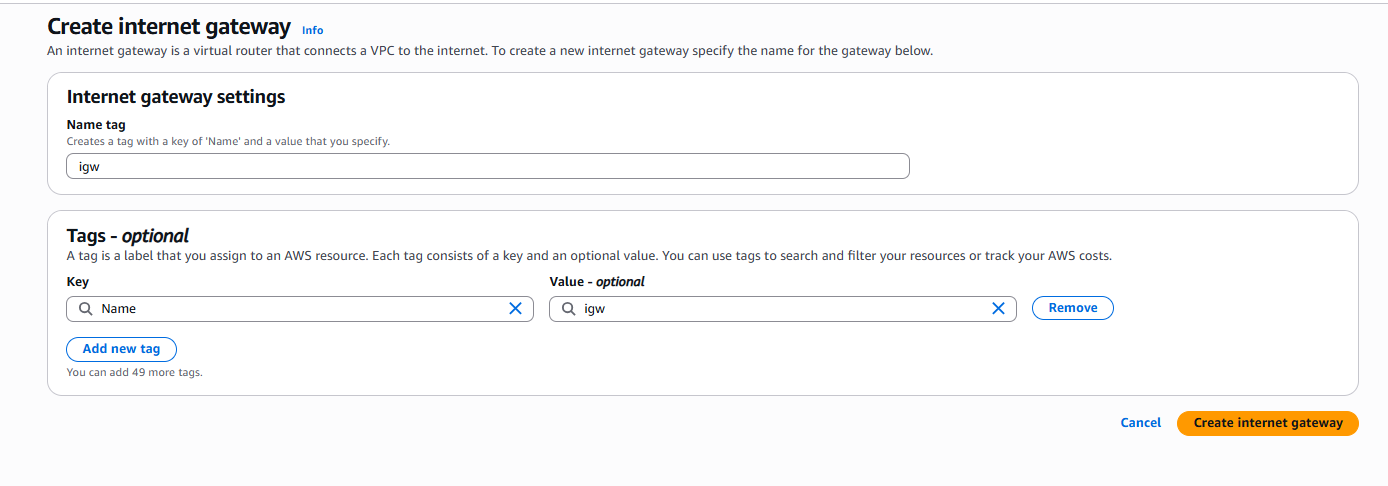
Give the name and cidr range 192.168.0.0/28:



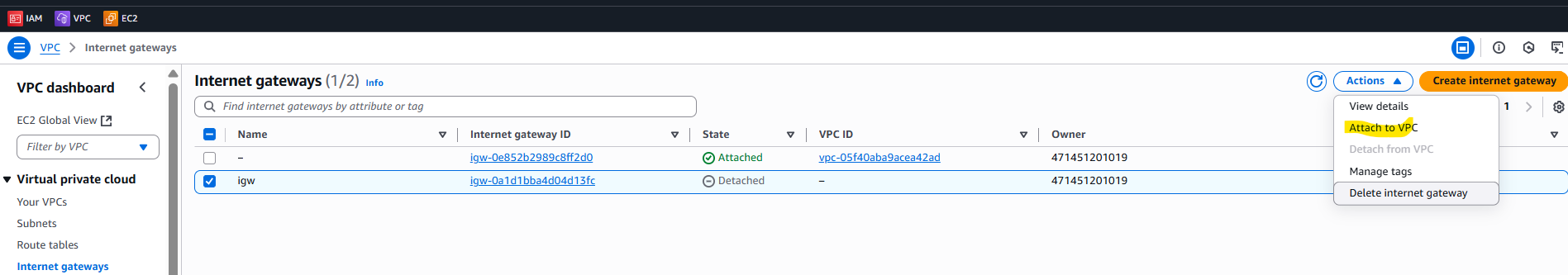
* 1. Create Internet Gateway:



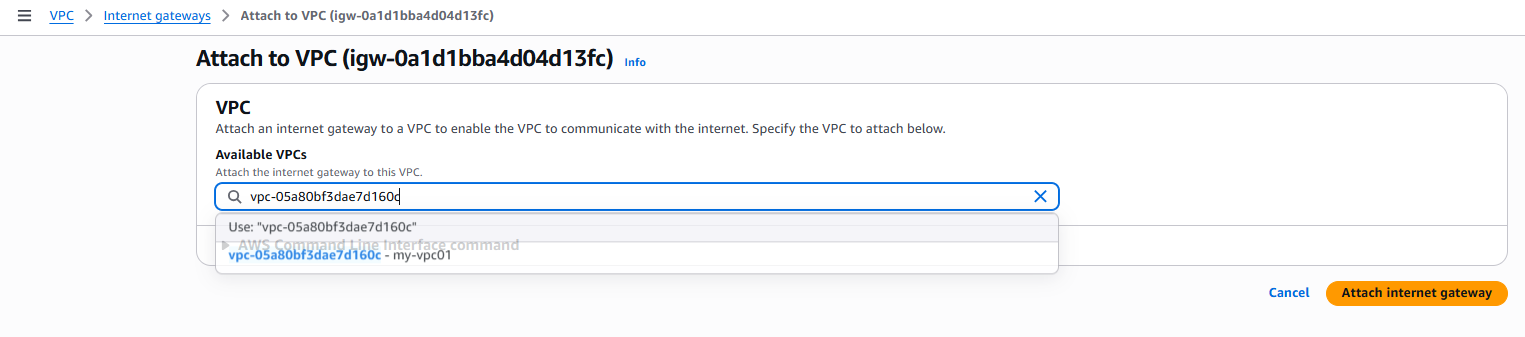
* 1. Give name and click on Create Internet Gateway:



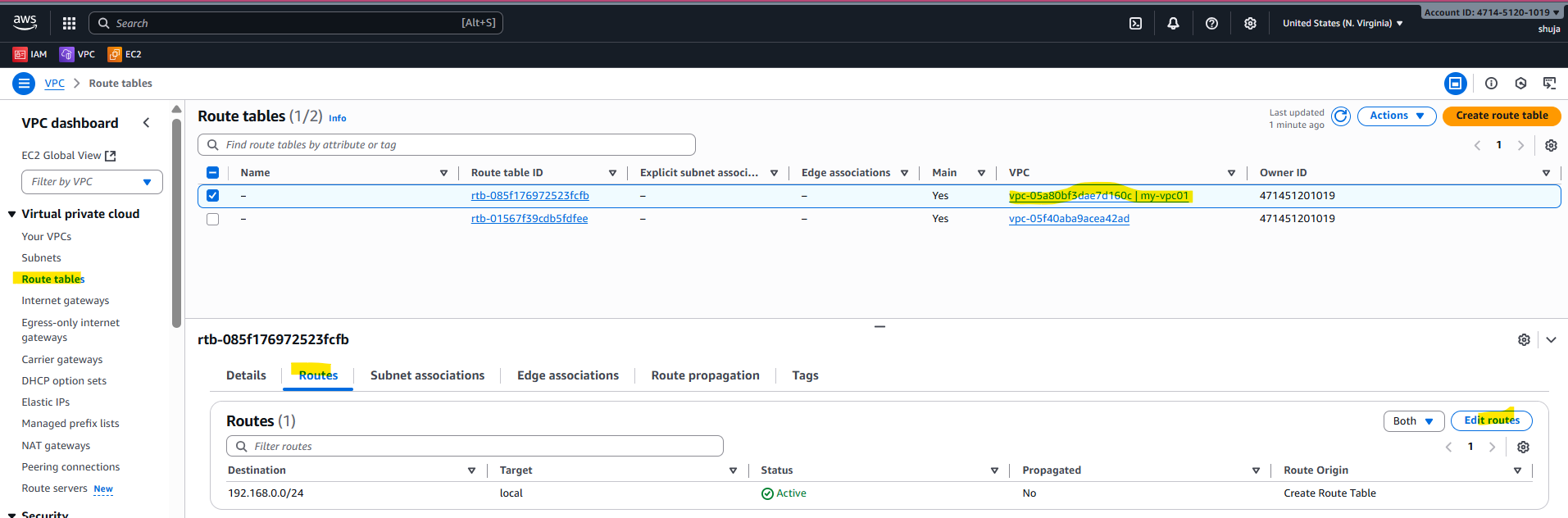
* 1. Attach igw to vpc:



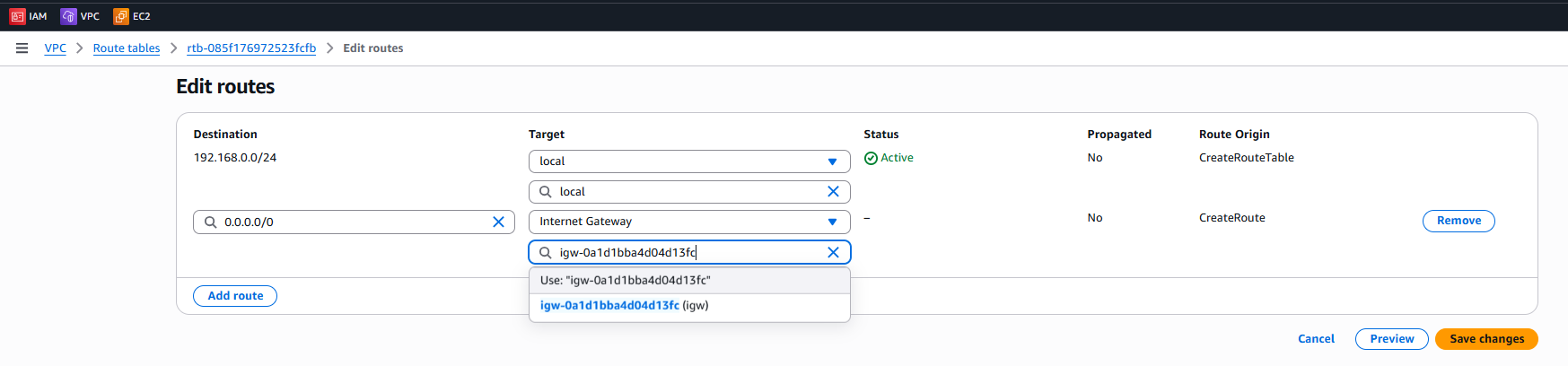
* 1. Select your vpc and click on Attach internet gateway:



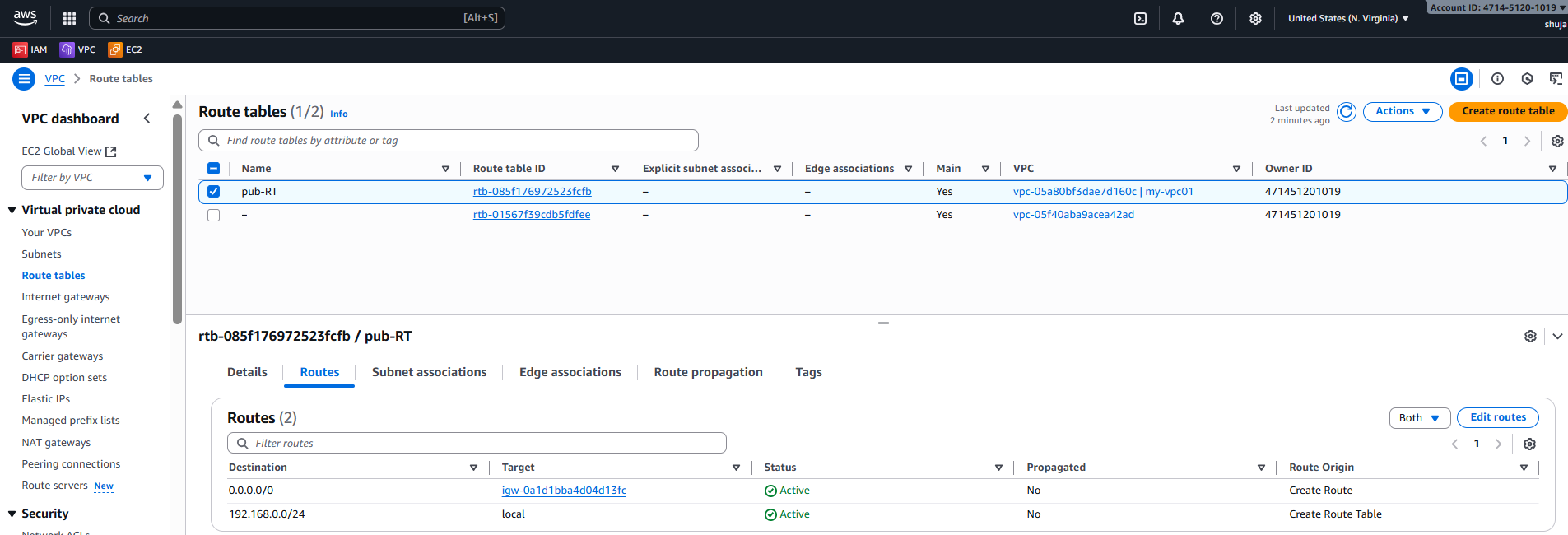
* 1. Selecting the existing created Route Table, making it as Public Route Table:



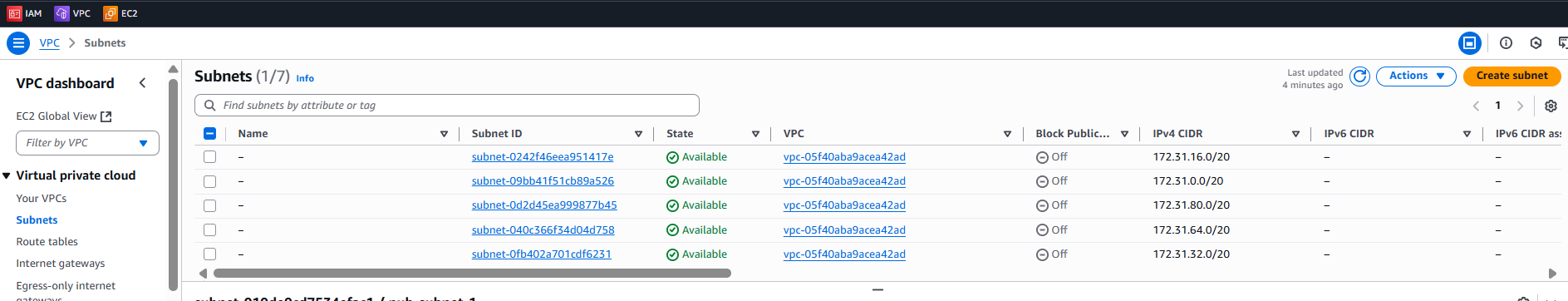
* 1. Adding internet gateway in the Route:



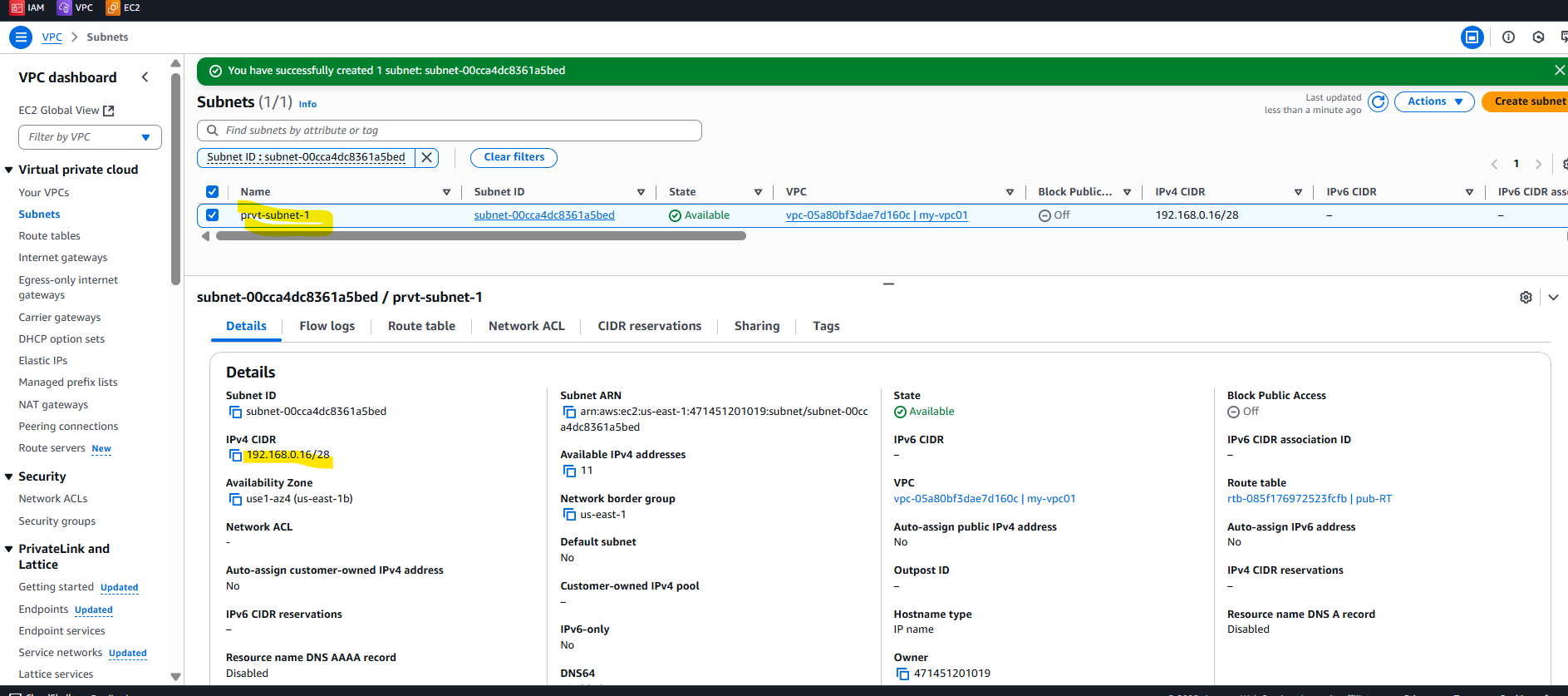
* 1. We can see public RT has route to internet gateway:



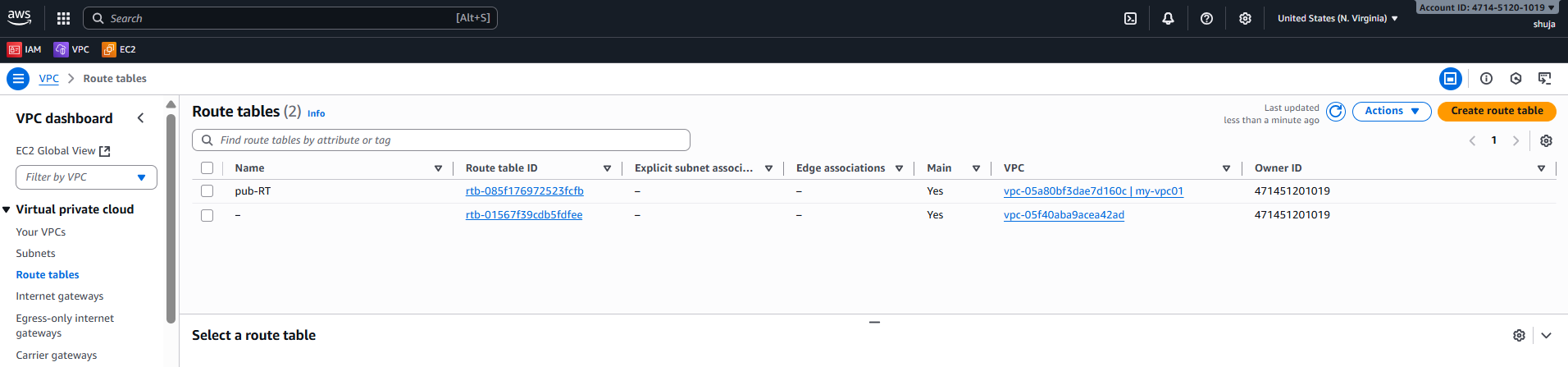
* 1. Create the Subnet:



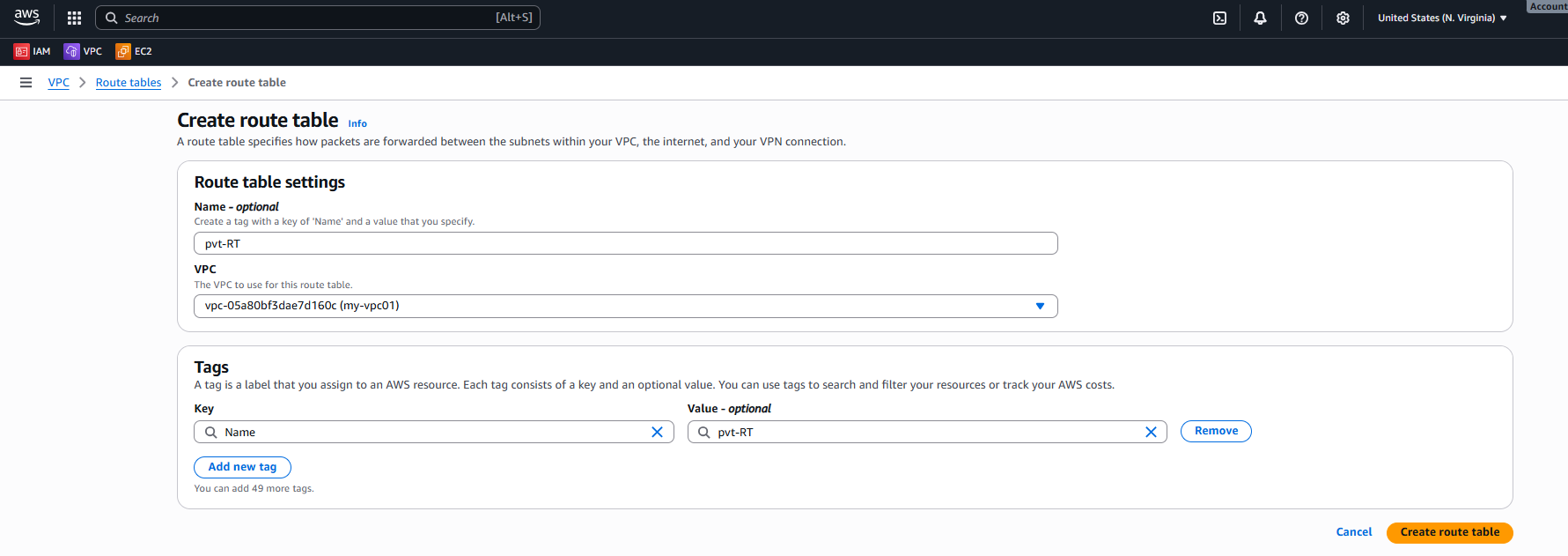
* 1. Select your vpc and give the cidr range 192.168.0.16/28:



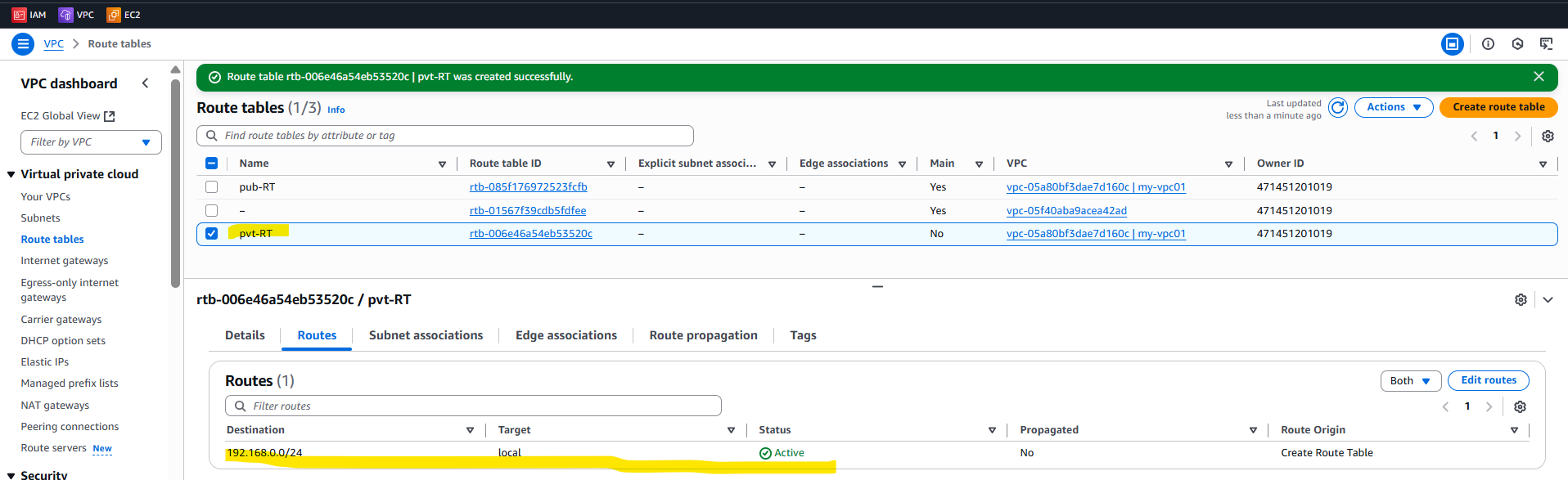
Xii) Crete Route Table (for private subnet):



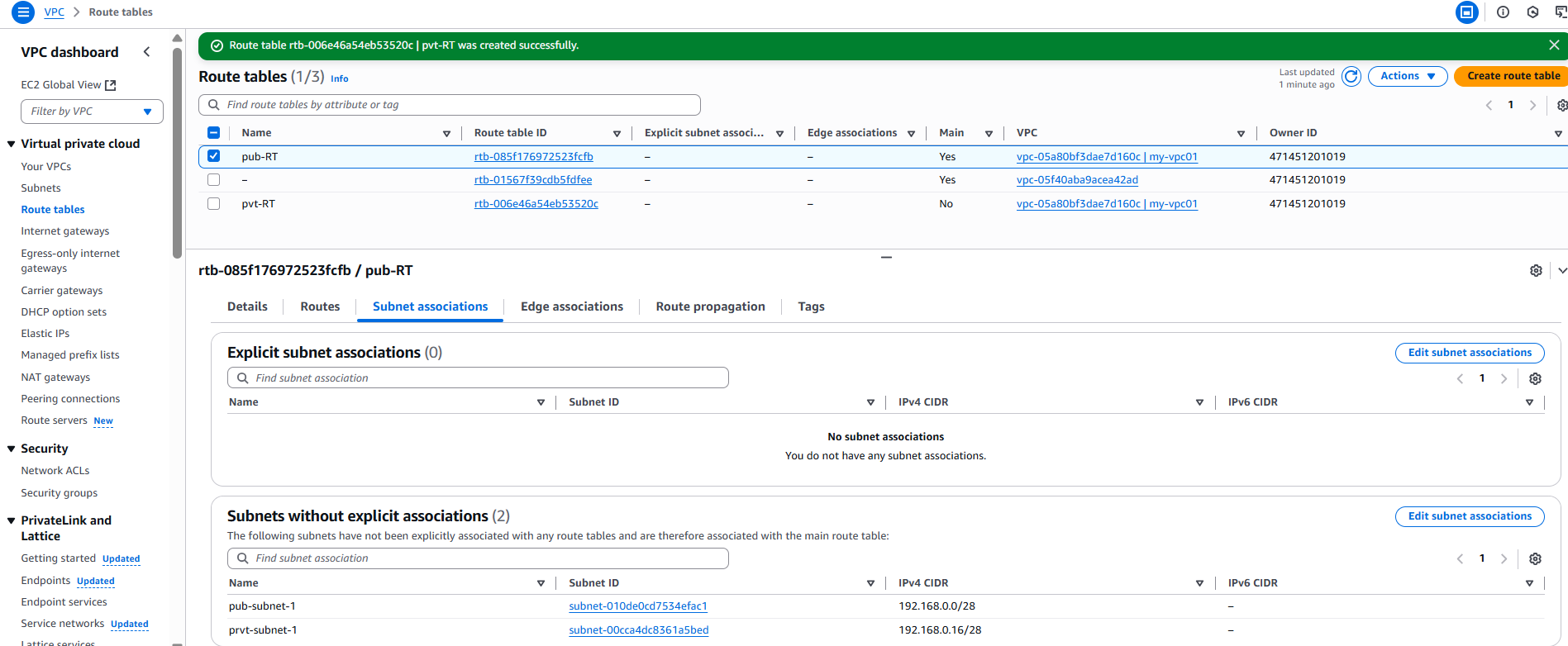
* 1. Give the name and Select your vpc :



* 1. Route Table contains only local route:



Subnet association: Public RT associate with public Public subnet



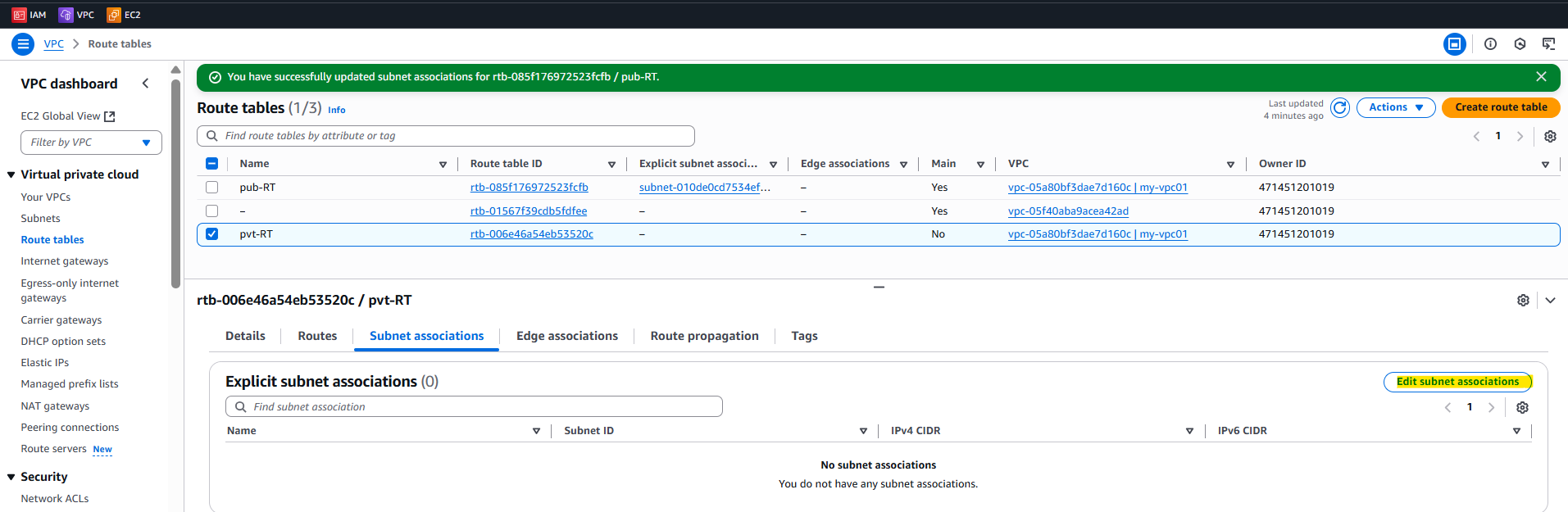
Save



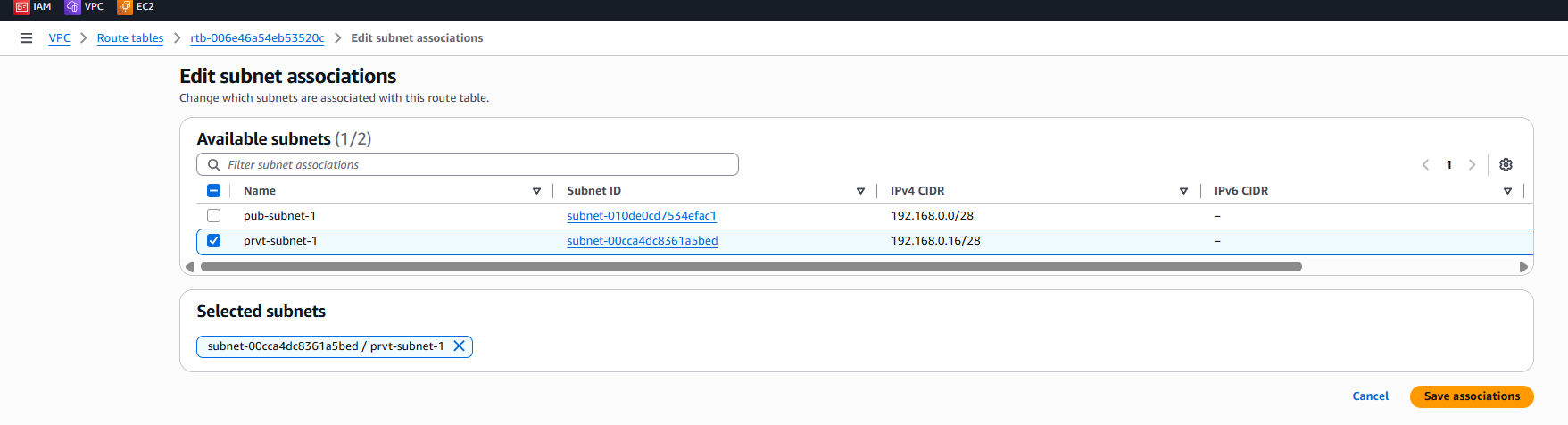
Then we can see public subnet associated with public RT:



Associate private RT with private subnet:



Save

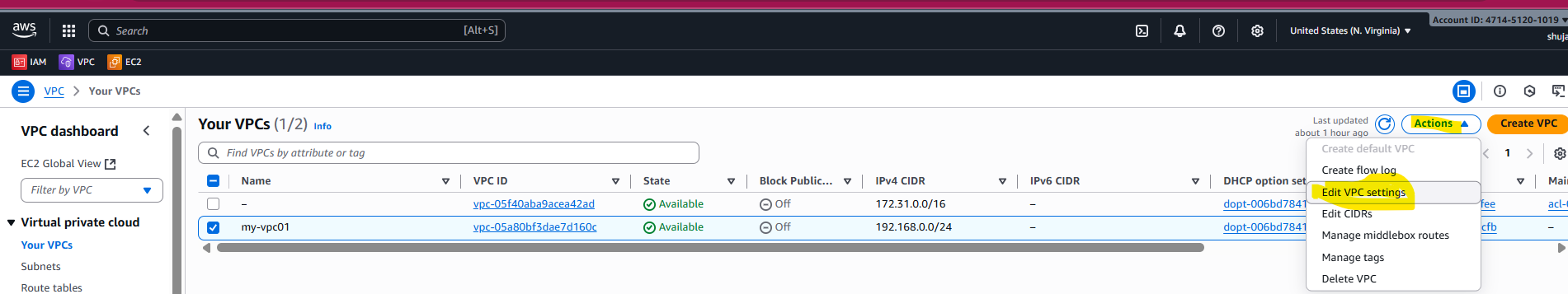


Similarly create another subnet i.e., public subnet 2 and private subnet 2.

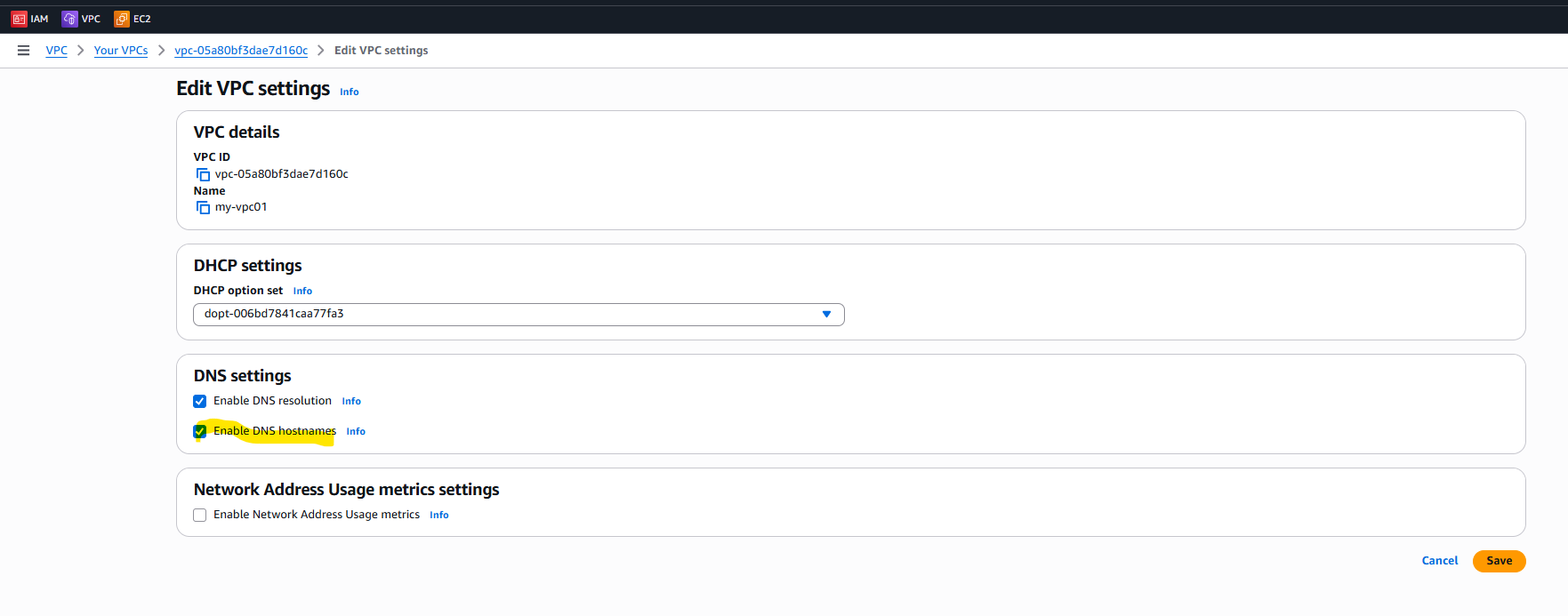
-----------------------------

1. Enable DNS Hostname in VPC.

Goto vpc and select your vpc ->Actions->Edit vpc settings:

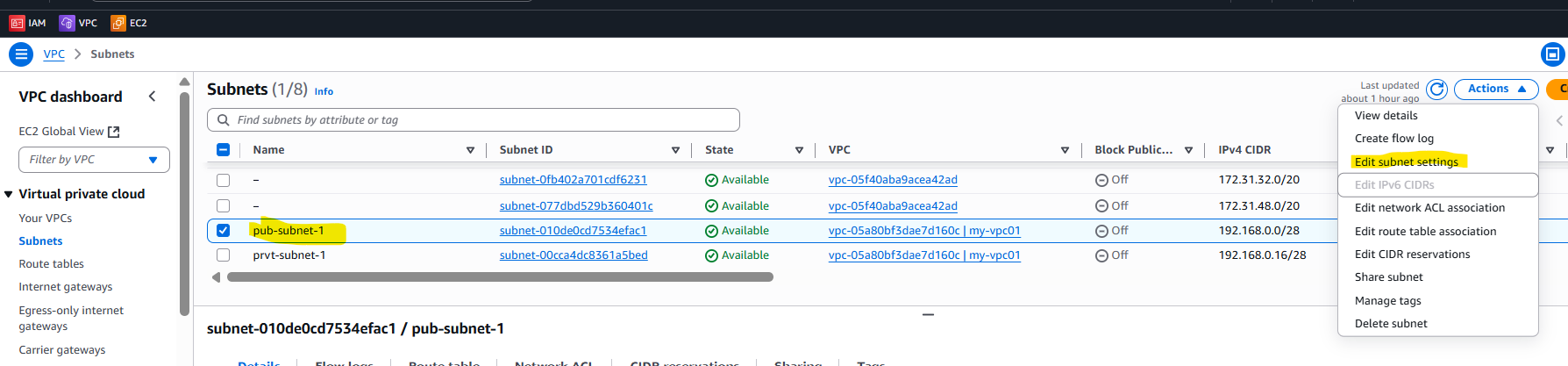


Enable DNS hostname checkbox:

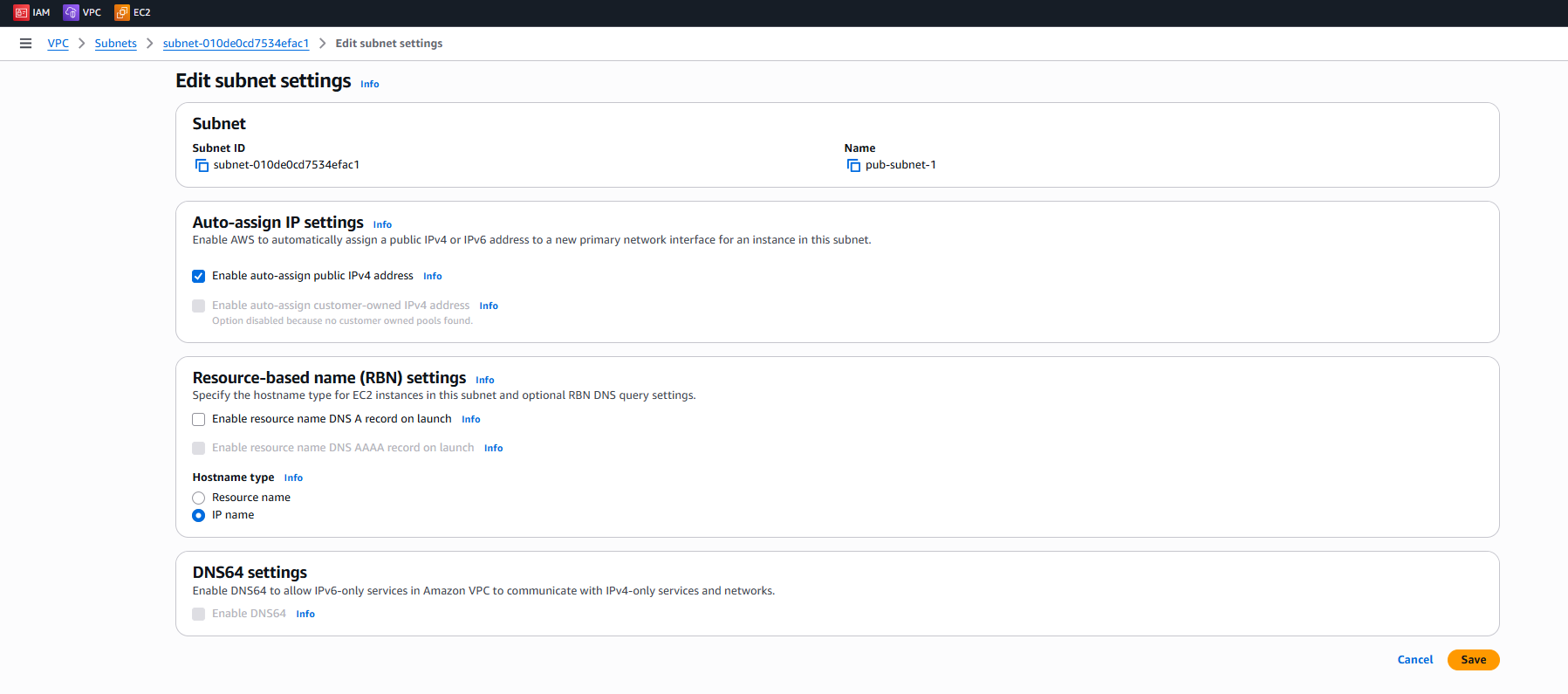


1. Enable Auto Assign Public IP in 2 public subnets.

Select your vpc and edit subnet settings;



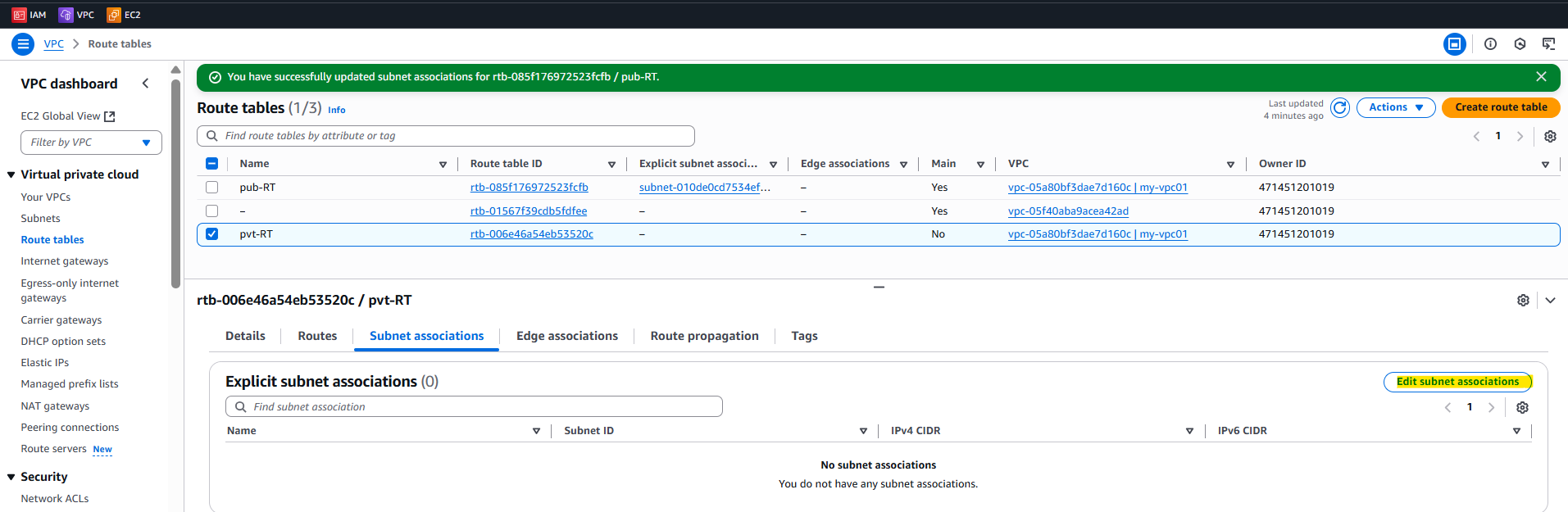
Auto assign public IP4 checkbox check:

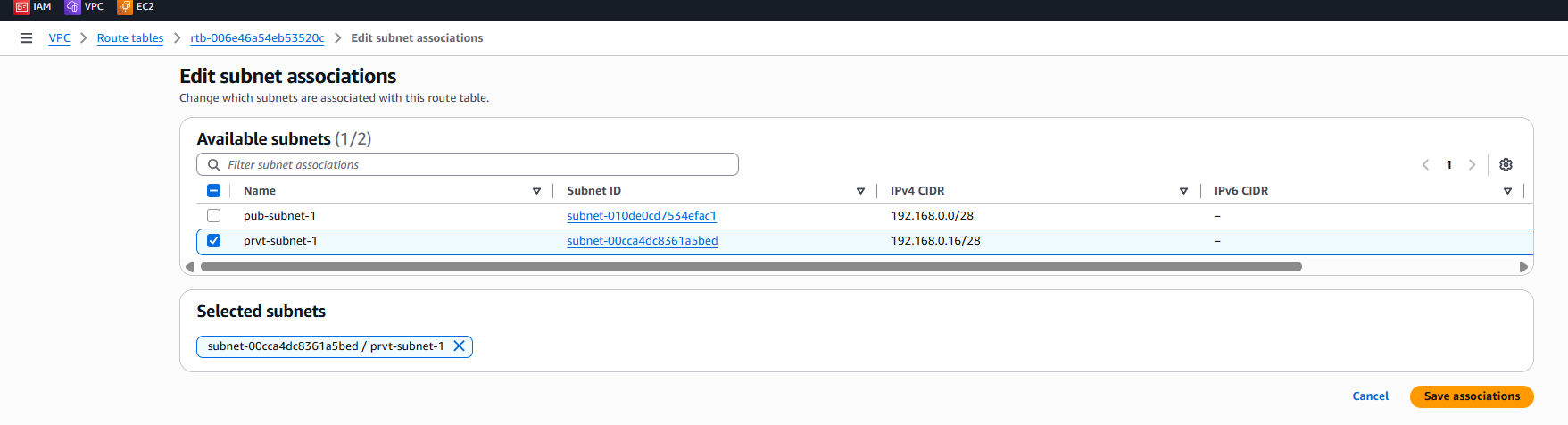


-------------

1. Add 2 private subnets in private route table.

Associate private RT with private subnet:

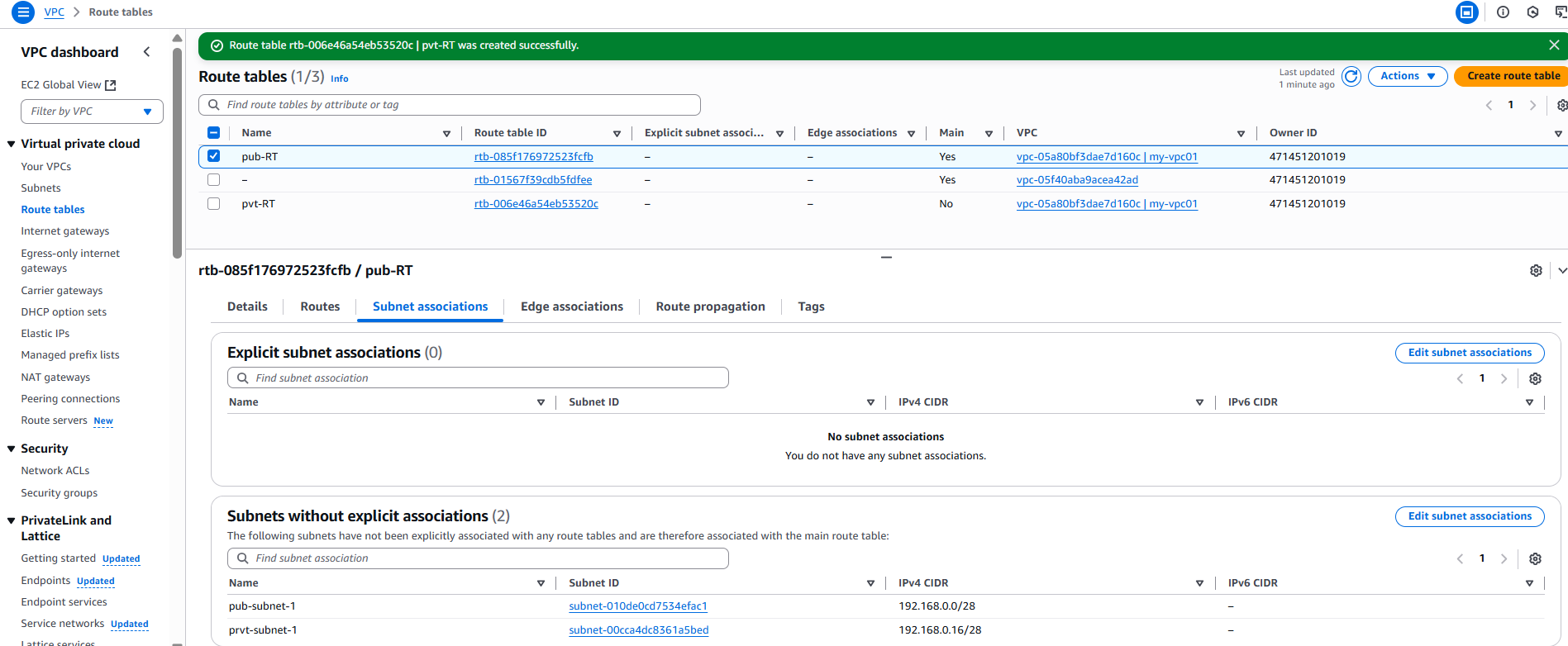




Save

1. Add 2 public subnets in public route table.

Subnet association: Public RT associate with public Public subnet



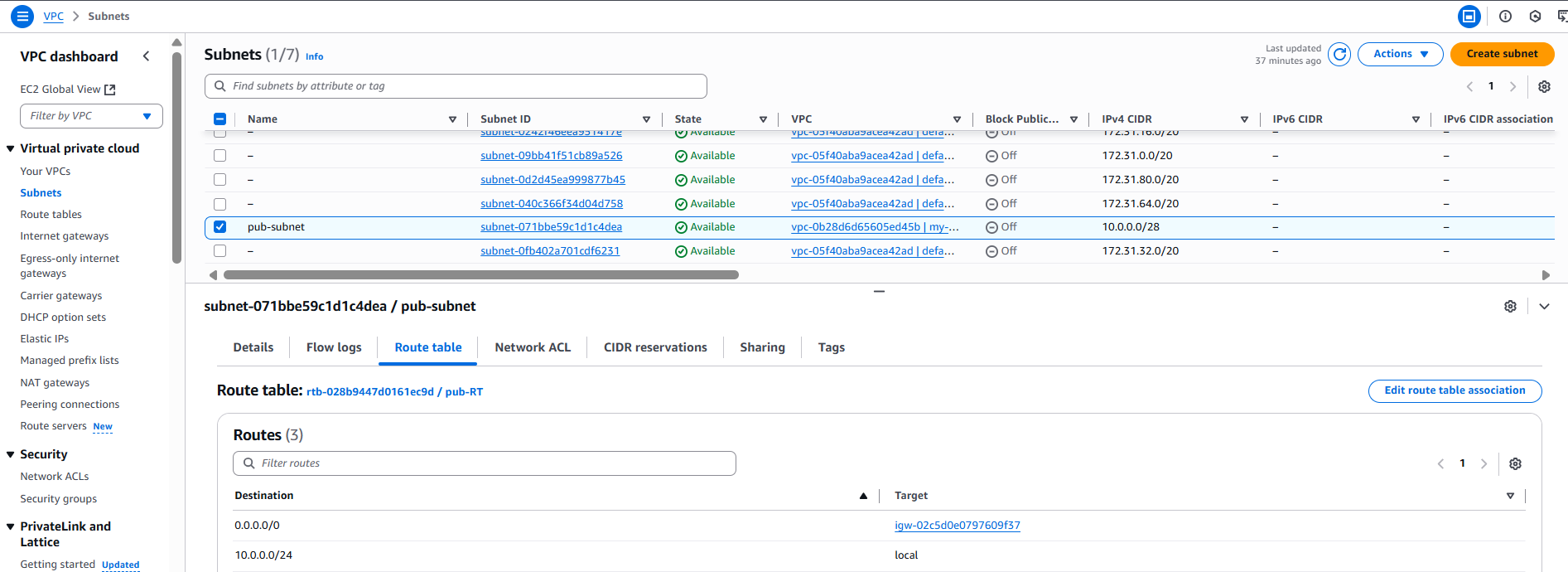
Save



Then we can see public subnet associated with public RT:

1. Public route table will have the routes to internet and local.

Add the Internet Gateway to the public Route Table, it will have default local:



1. Create EC2 in public subnet with t2.micro and install PHP.

Create vpc by giving name and cidr range.

Create Internet Gateway and assign to your vpc.

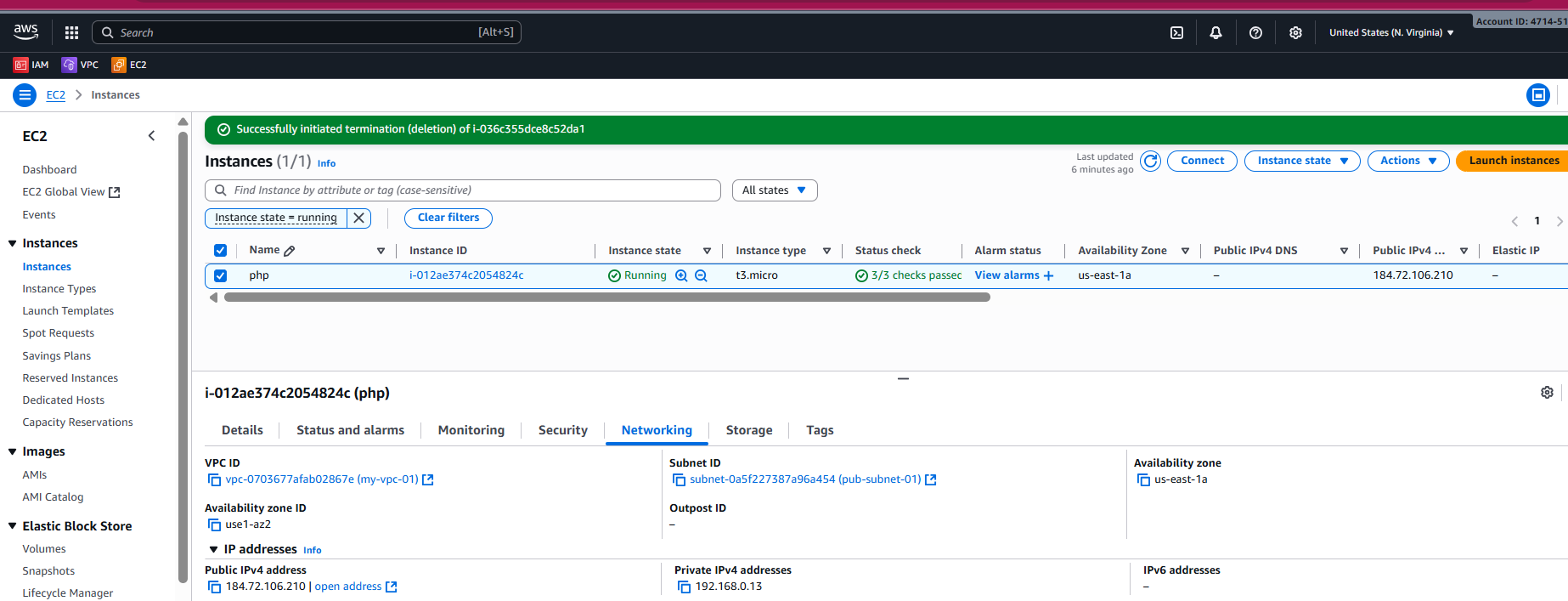
Create Subnet and give name and your vpc and select the vpc cidr and give subnet cidr.

Create Route Table.

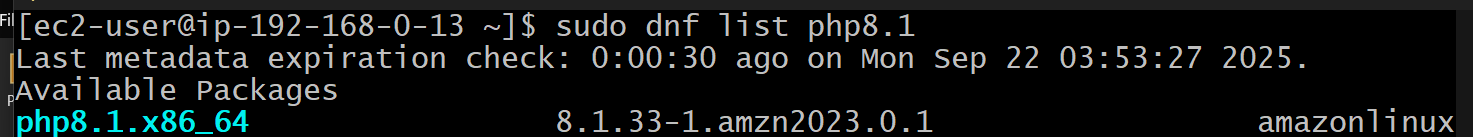
Add Route to Internet Gateway in Route Table.

Add Route Table to Subnet i.e., do subnet association.

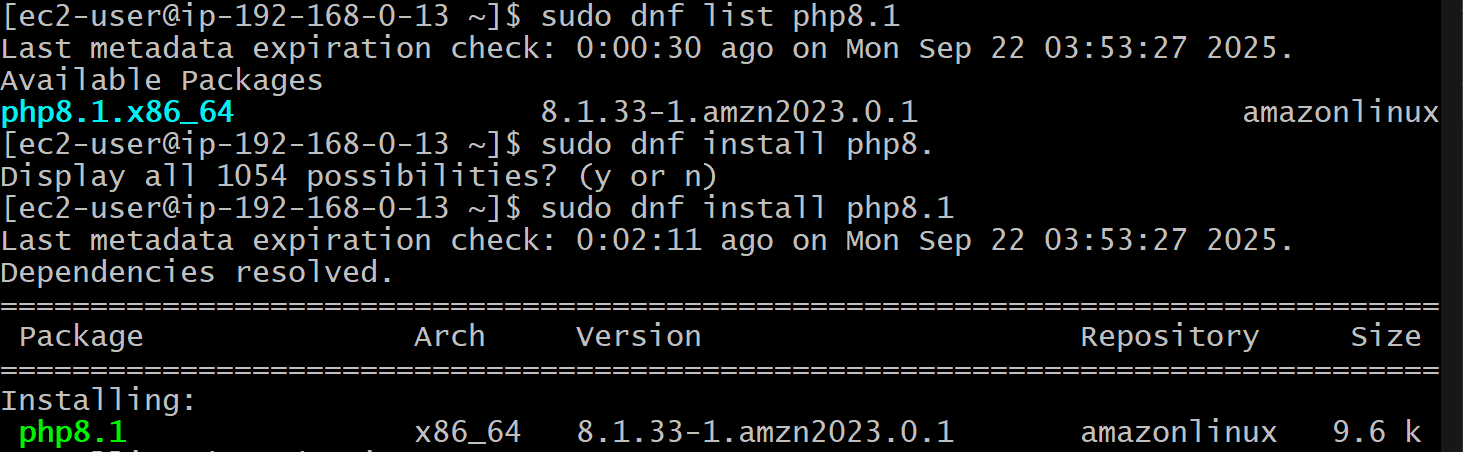
Create Ec2 in public subnet with t3.micro:



Check whether the package of php8.1 is there:



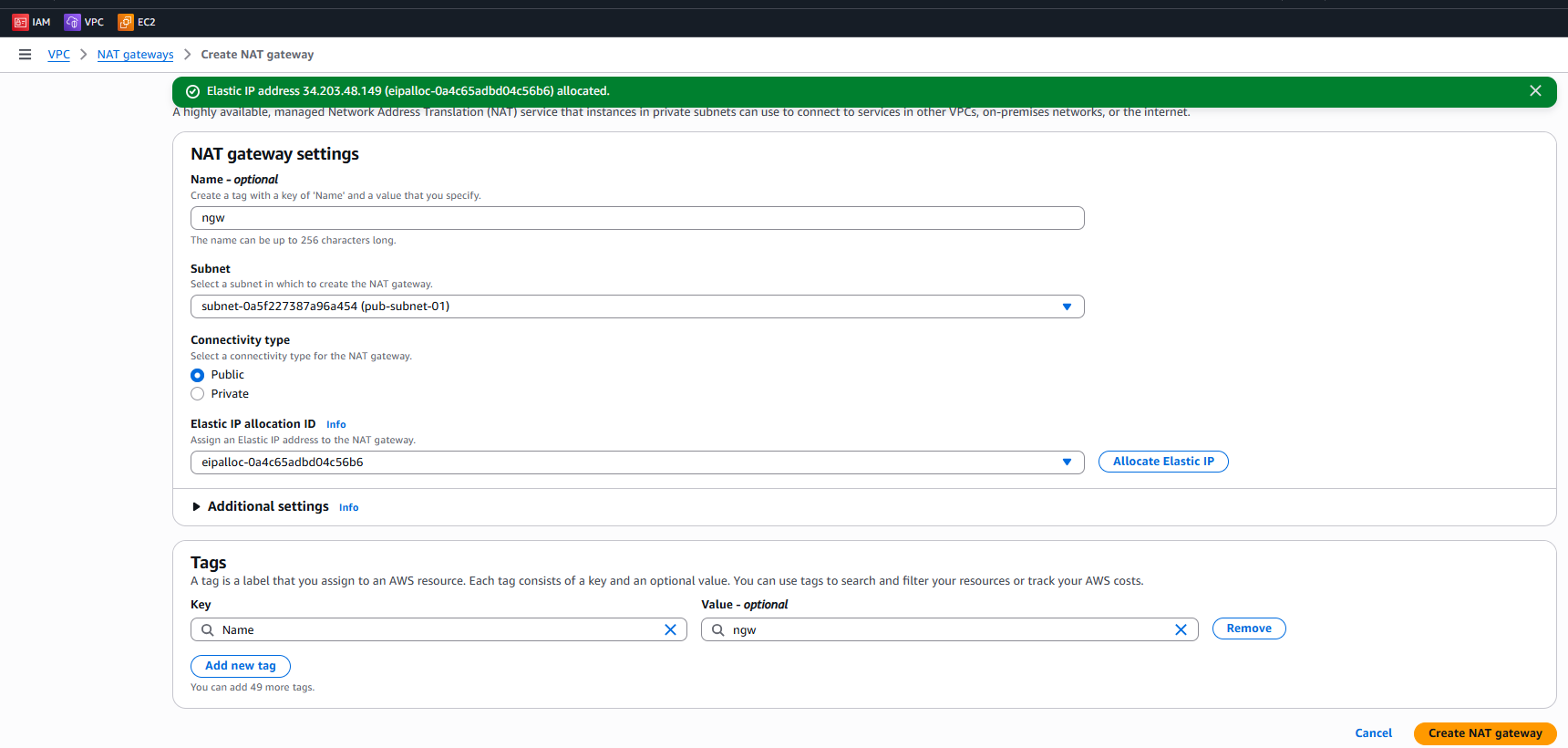
Install php8.1:



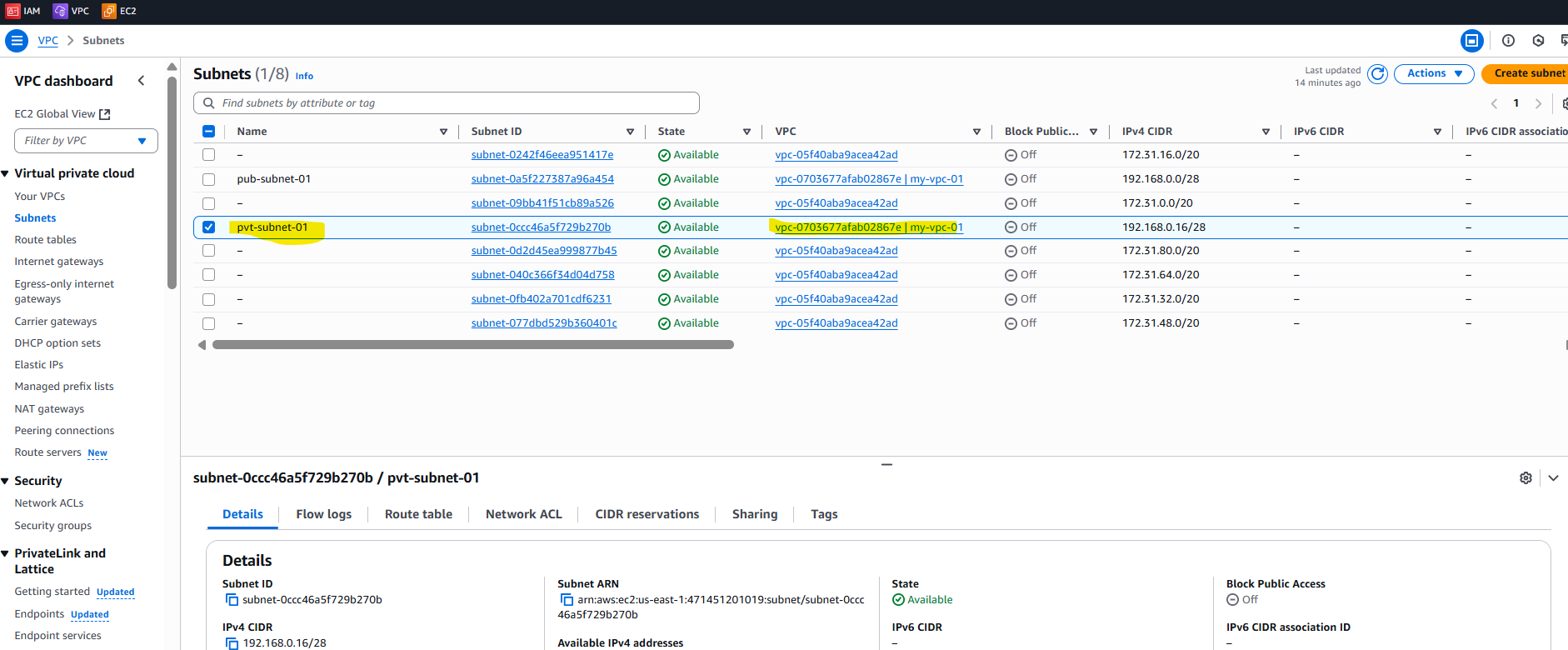
---------------

1. Configure NAT gateway in public subnet and connect to private instance.

Create NAT Gateway and assign elastic ip and select public subnet:



Create a private Subnet:



Create route table and add the route to NAT gateway.

Create ec2 instance in private subnet with only private ip.

Create ec2 instance in public subnet with public ip

Login to public subnet ec2.

Copy the pem key to public subnet ec2.

Change the permission of the pem key.

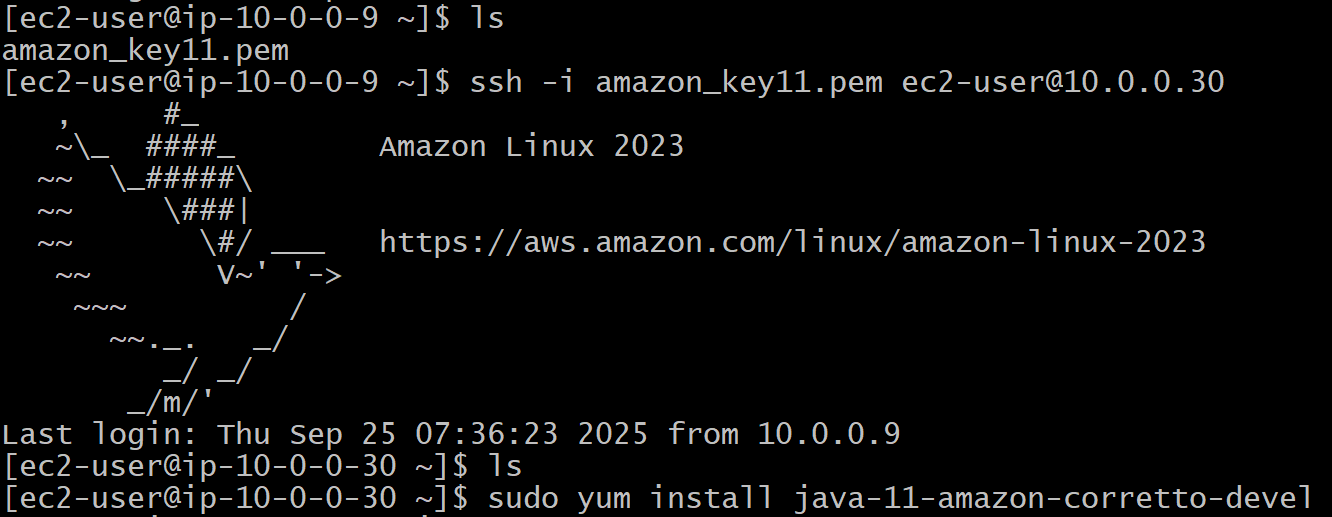
And login with private key of private subnet ec2:



-----------------

1. Install Apache Tomcat in private EC2 and deploy a sample app.

Create a Bastion Server and log in to the private ec2 instance and install java and apache Tomcat :



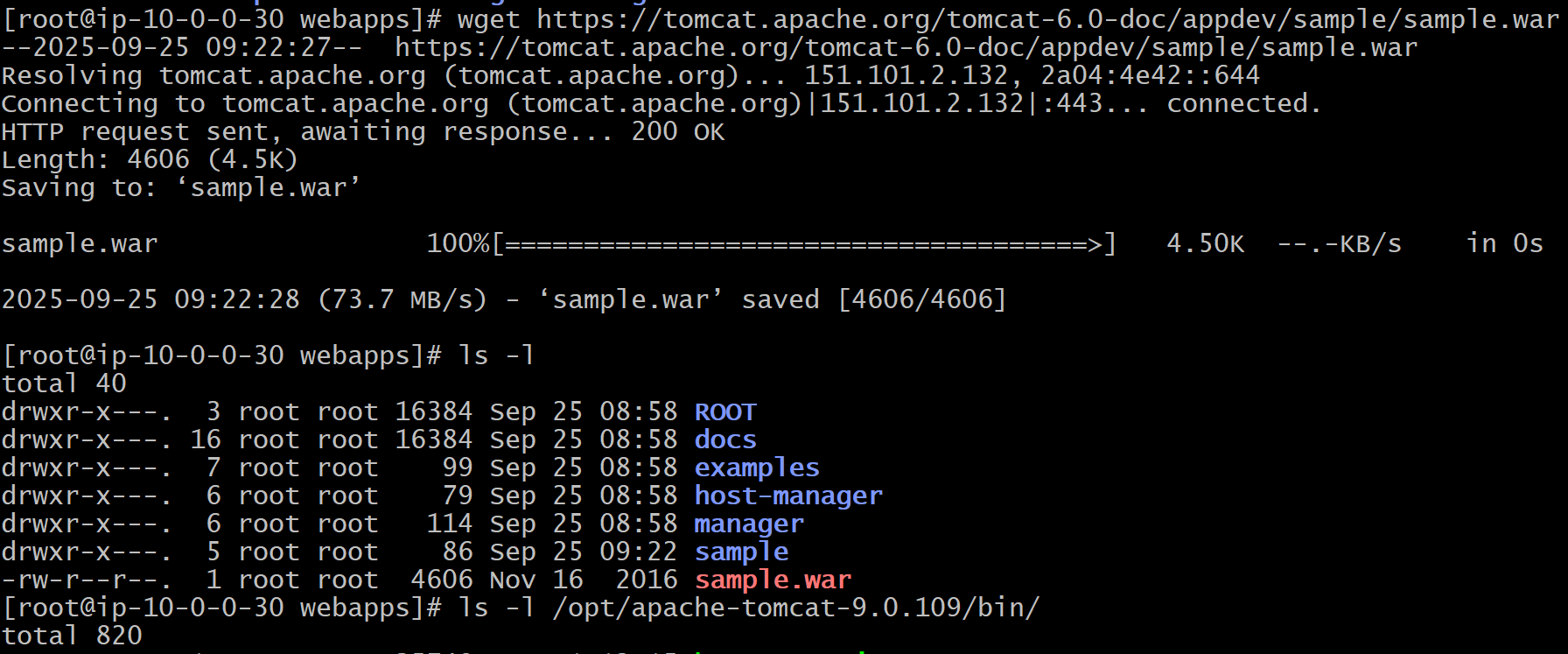
In the /opt directory install tomcat:



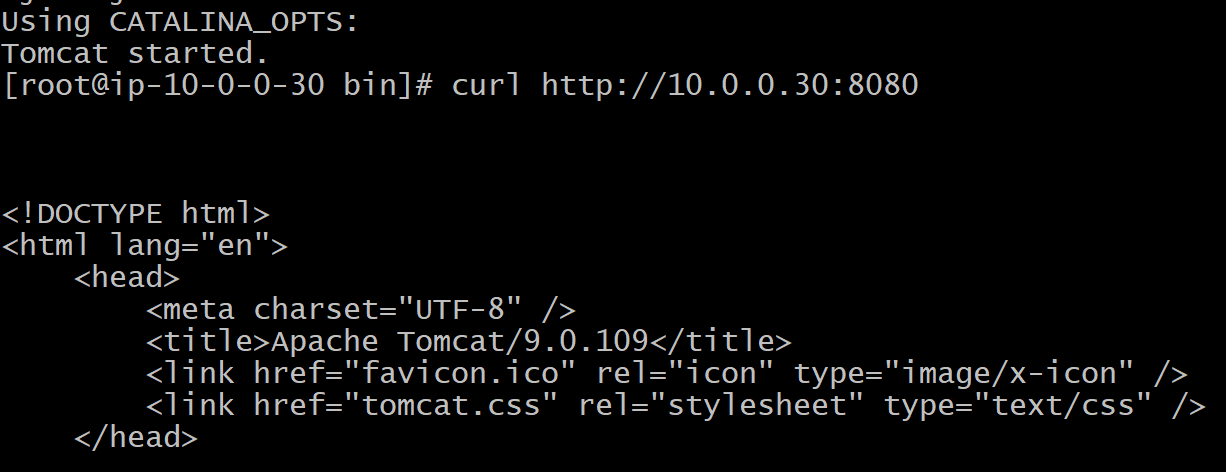
Change the permission of bin directory:



Goto directory /opt/apache\_tomat9/webapps and download the sample war :



curl http://localhost:8080

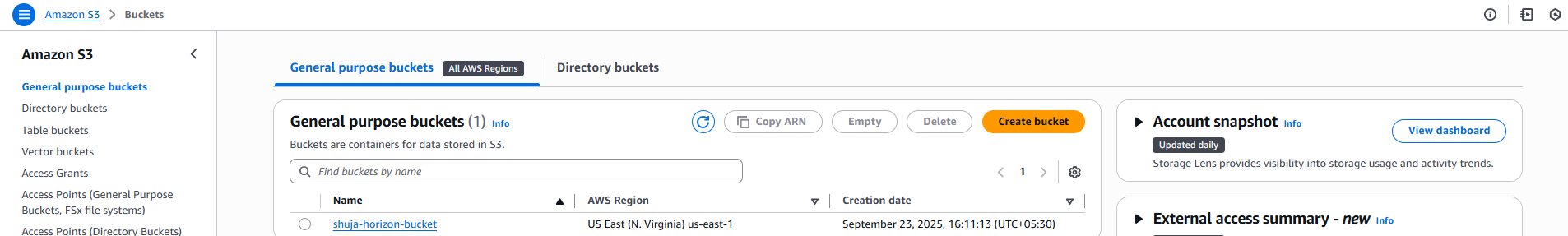


----------------done---------

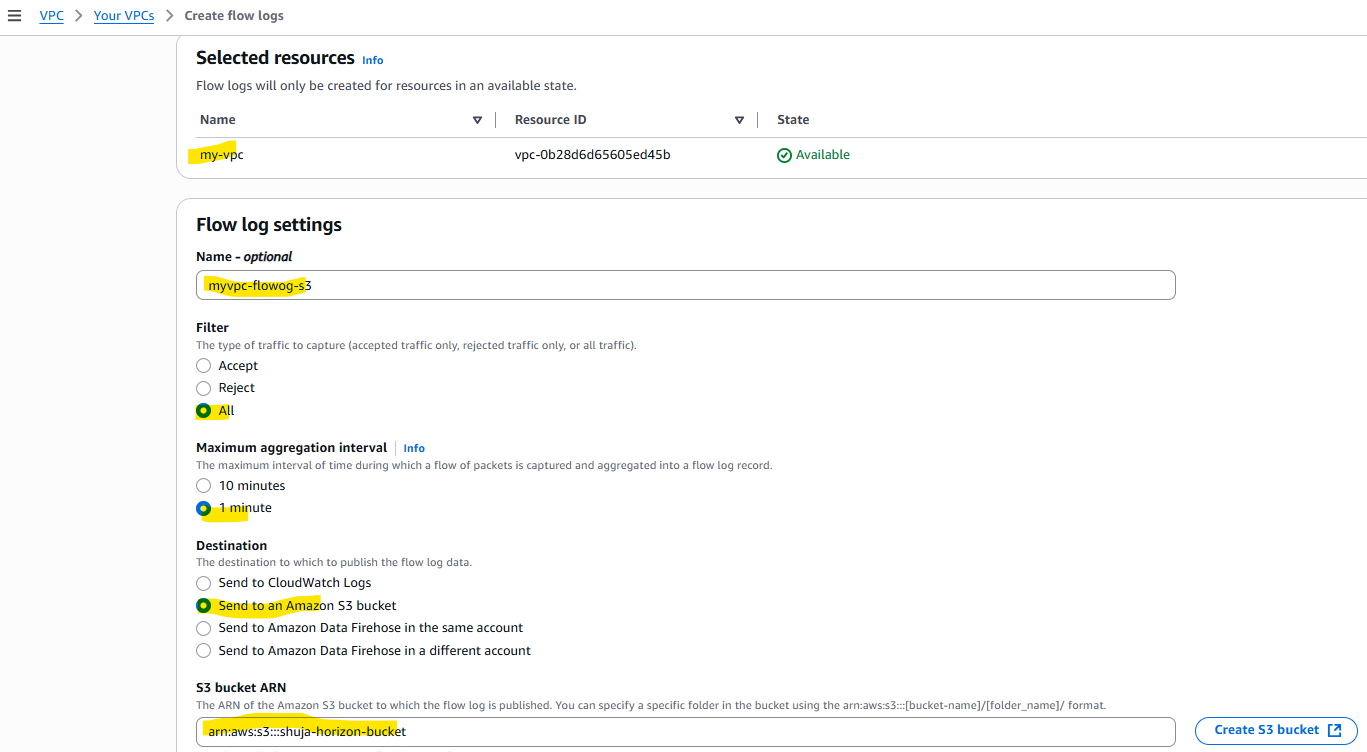
1. Configure VPC flow logs and store the logs in S3 and CloudWatch.

Creating VPC flow logs and storing in S3:

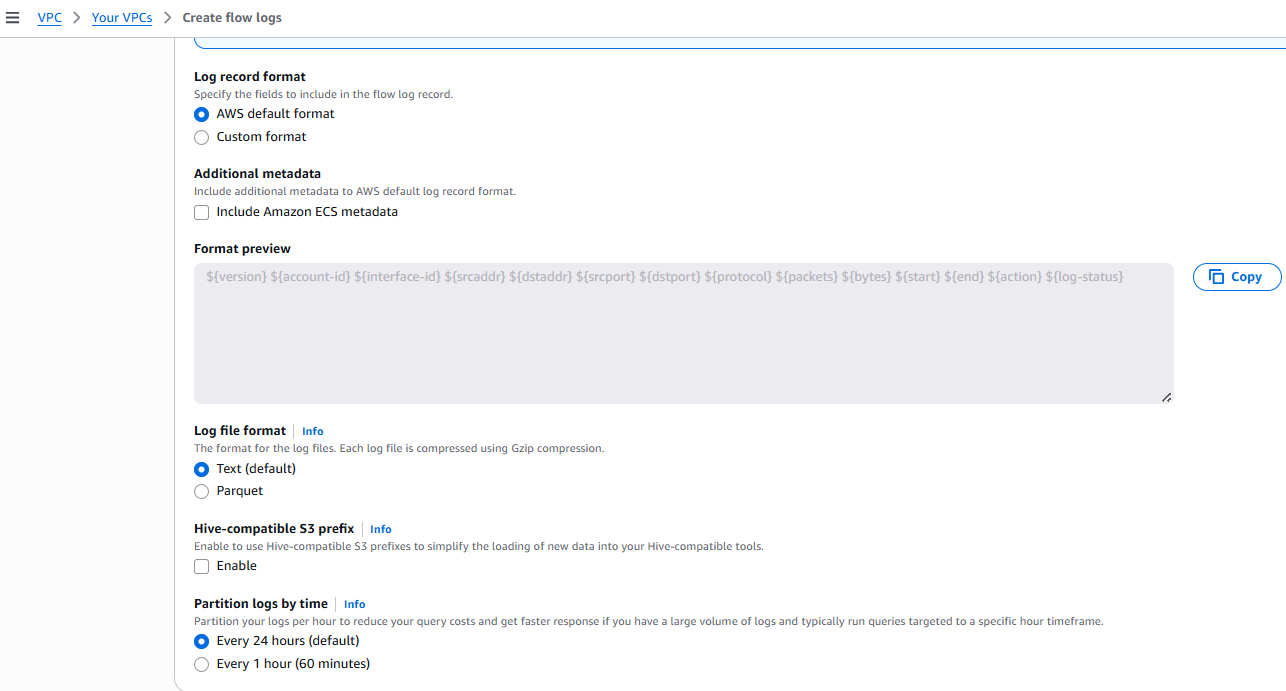
Create S3 bucket:



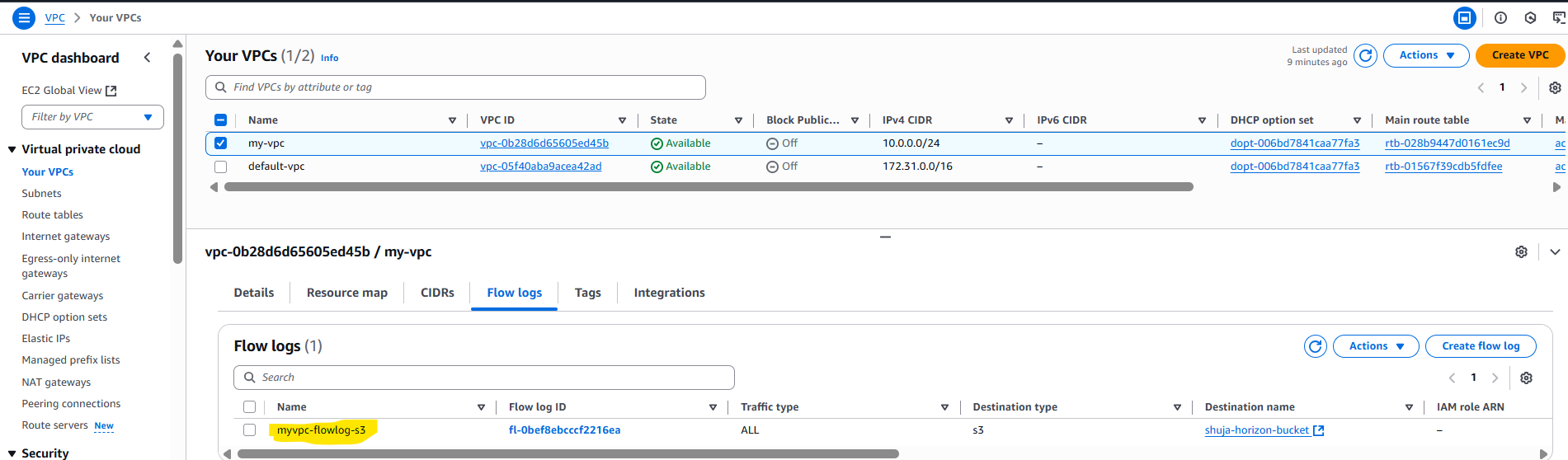
Select VPC for which you want to create vpc flow logs and click on Create flow logs and give the arn of s3 and the Filter while creating vpc flow log:



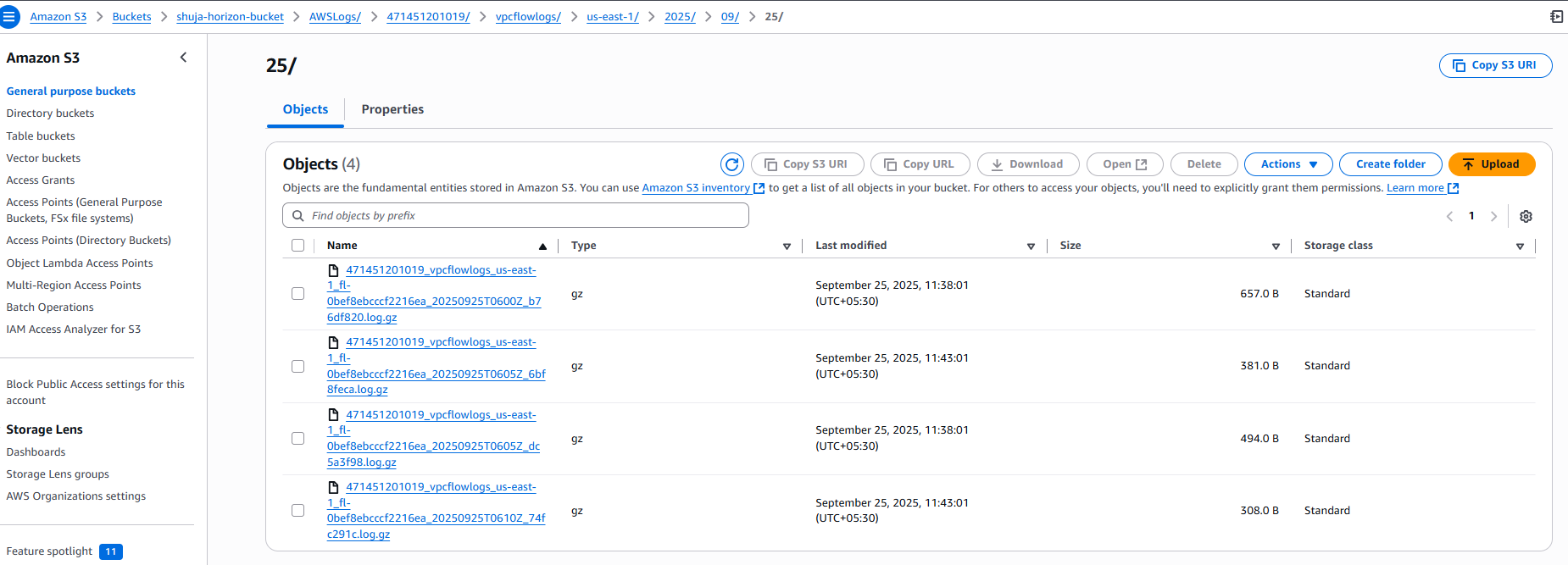
The log format I selected is default format:



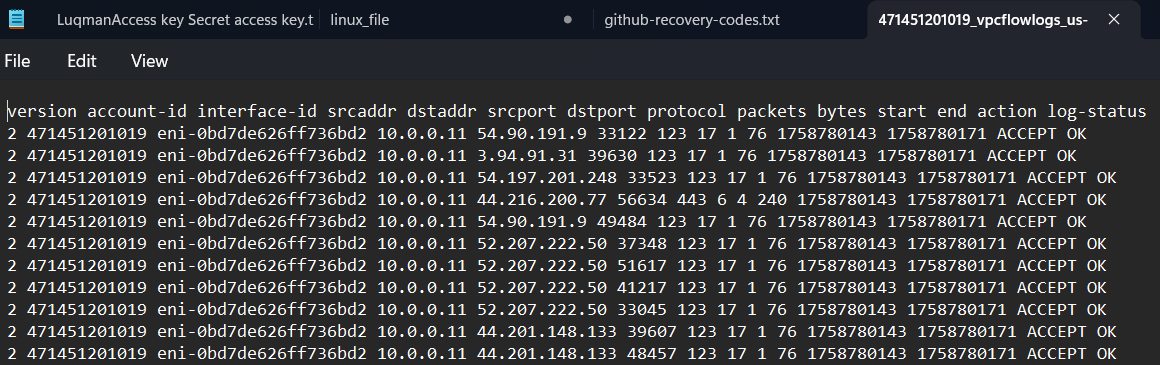
And vpc flow log will get created:



if you perform any action like create ec2 or terminate or any other action then logs will get generated in the s3 bucket:



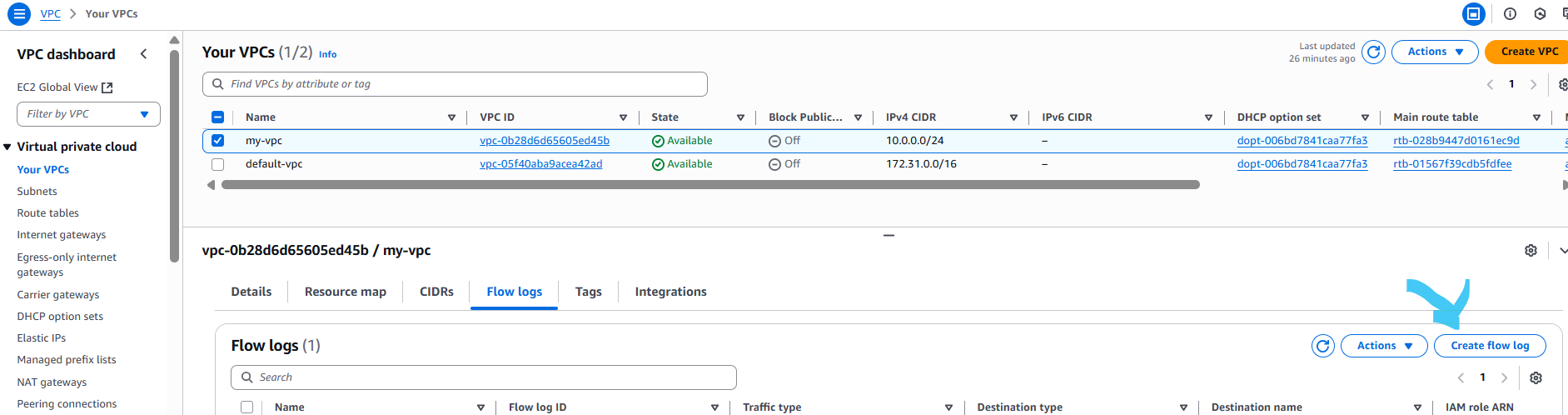
We can download those and see the logs:



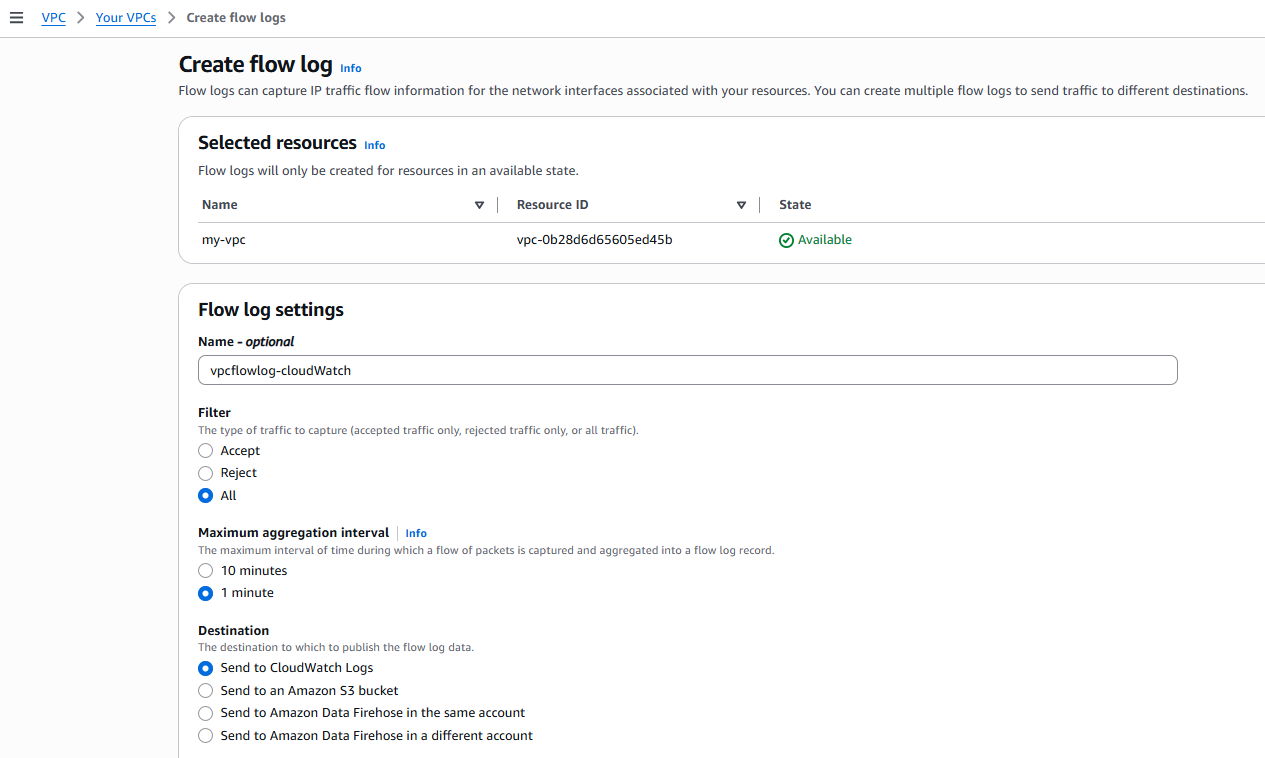
--------------done---------

**Configure VPC flow logs and store the logs in CloudWatch.**

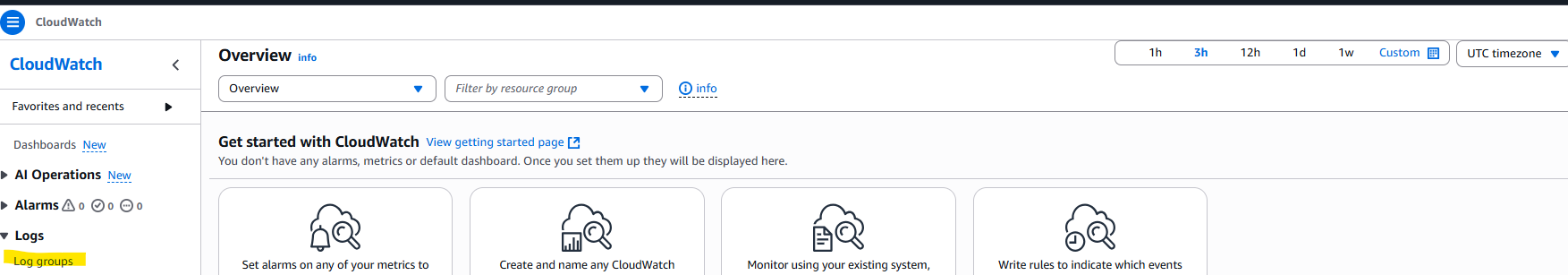
**Select your required vpc for which you want to create flow logs and click on create flow log:**

****

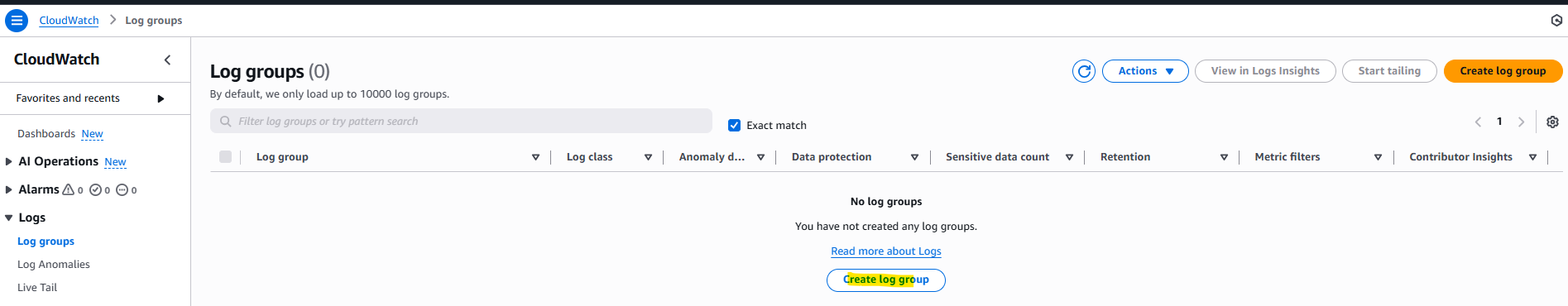
**Give the name , filter, maxm aggregation interval and Destination:**

****

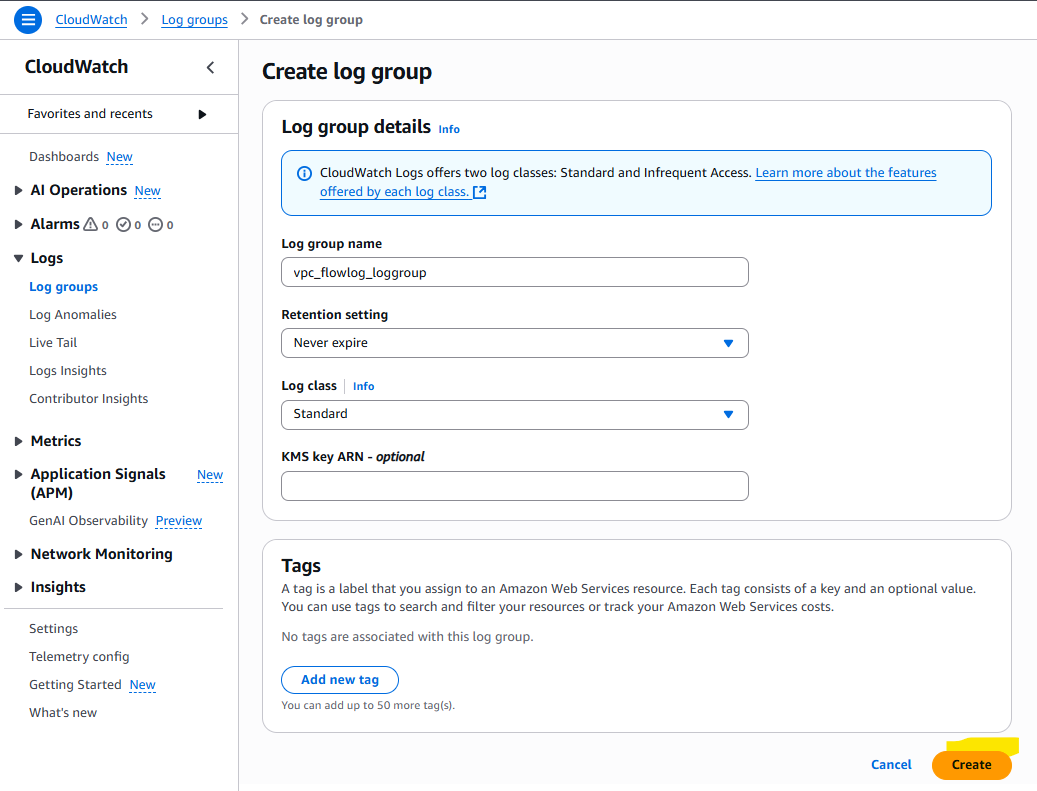
**As we are storing in the cloudwatch log group so first we have to create the Log group in CloudWatch, goto CloudWatch and select log group:**

****

**Create log group:**

****

**Provide the details and create log group:**

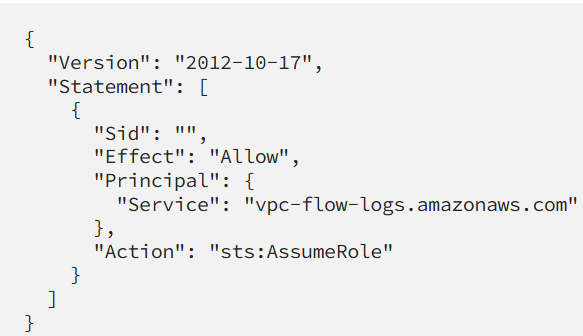
****

**Then create the IAM role with policy for vpc flow log to store logs in cloudWatch:**

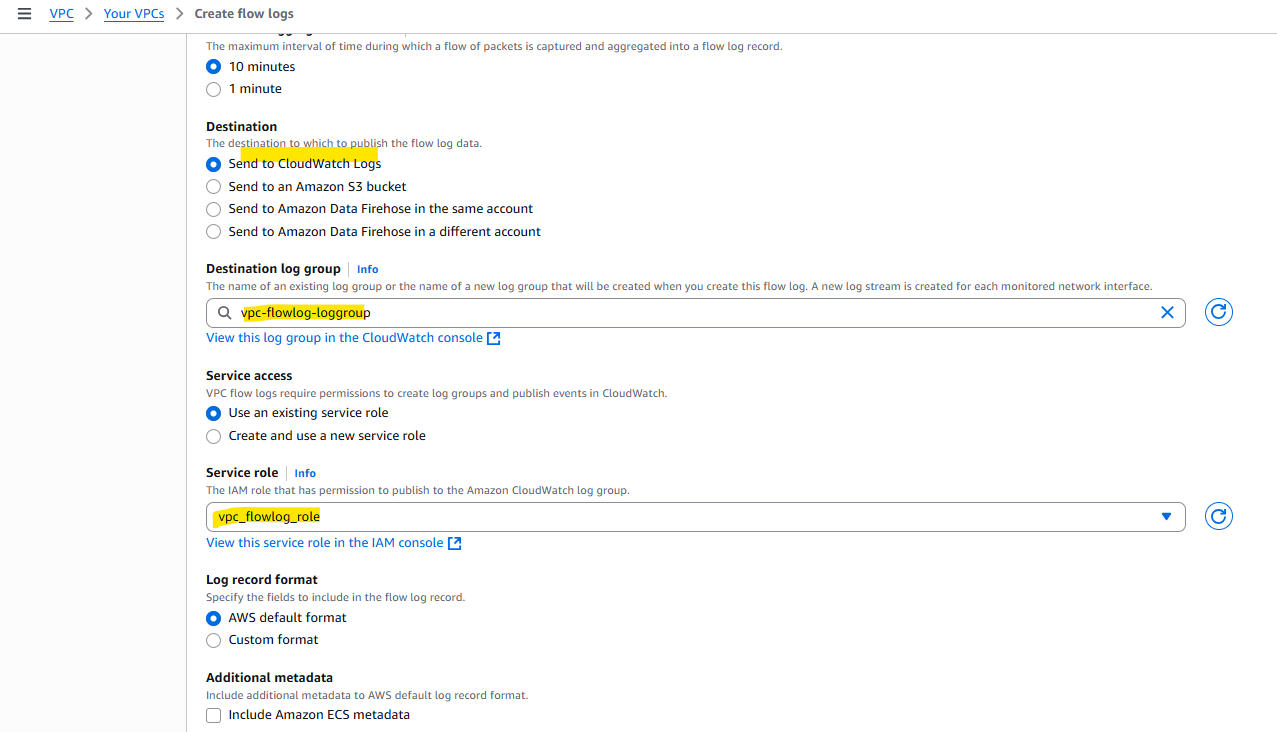
**IAM Policy:**

****

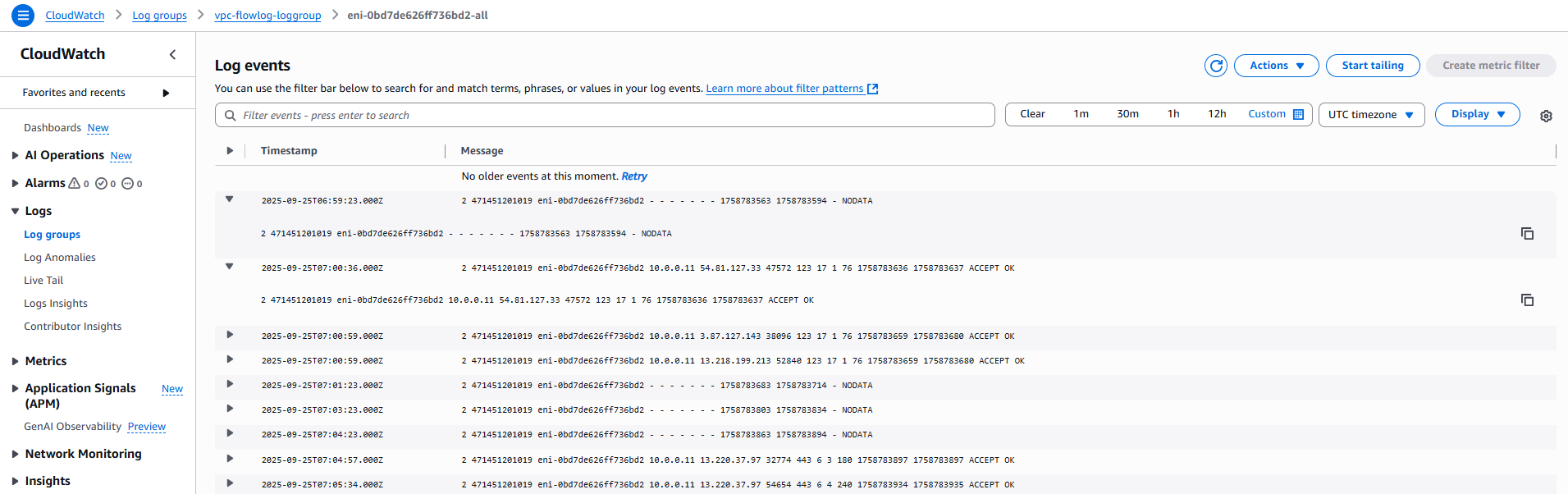
**And create the role with Trust policy:**

****

**And assign the above created policy to this role and select this role while creating vpc flow log:**

****

**And the logs will get saved in the cloudWatch log group:**

****

**-----------------done-----------**