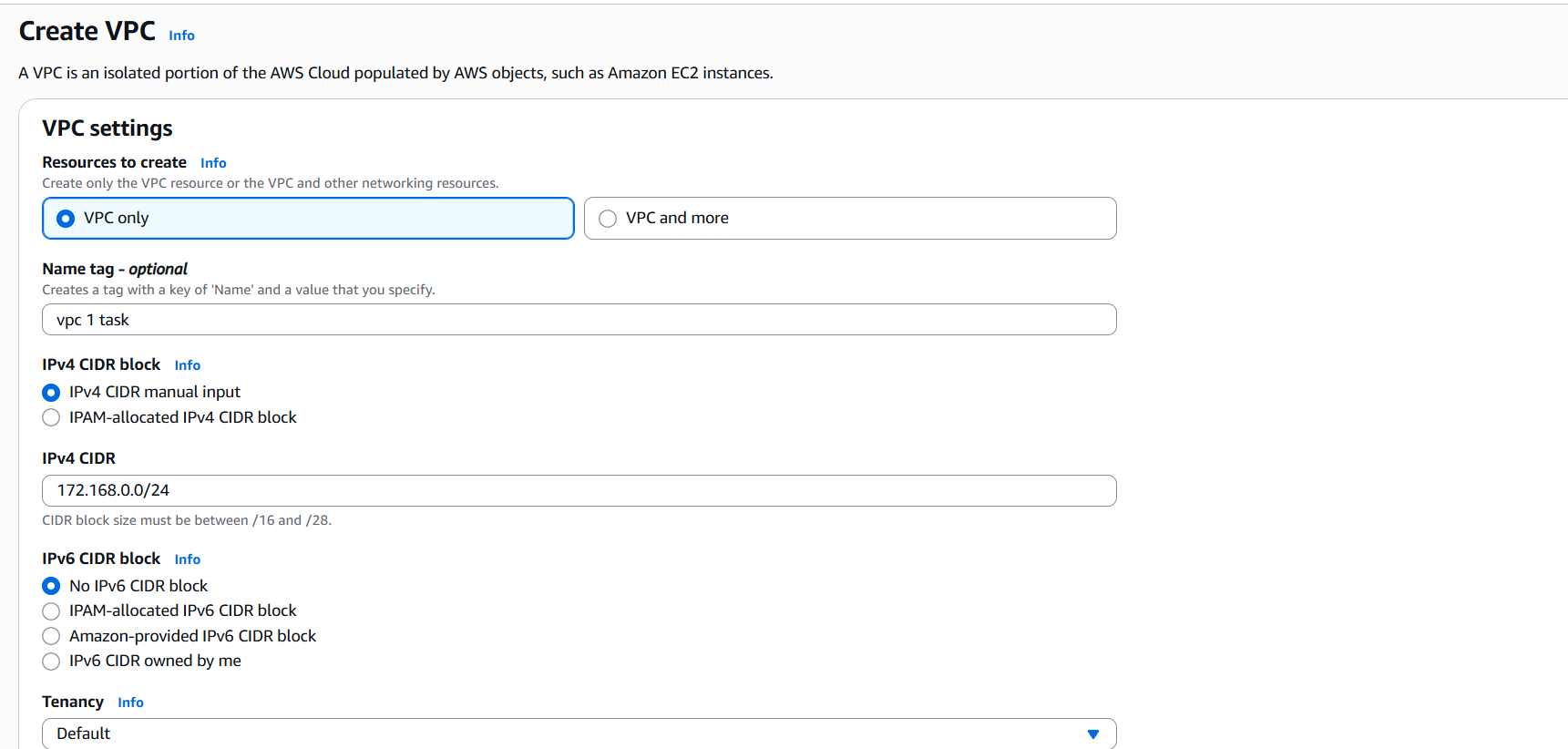
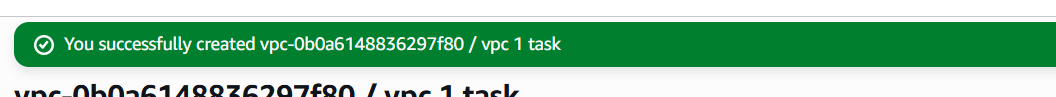
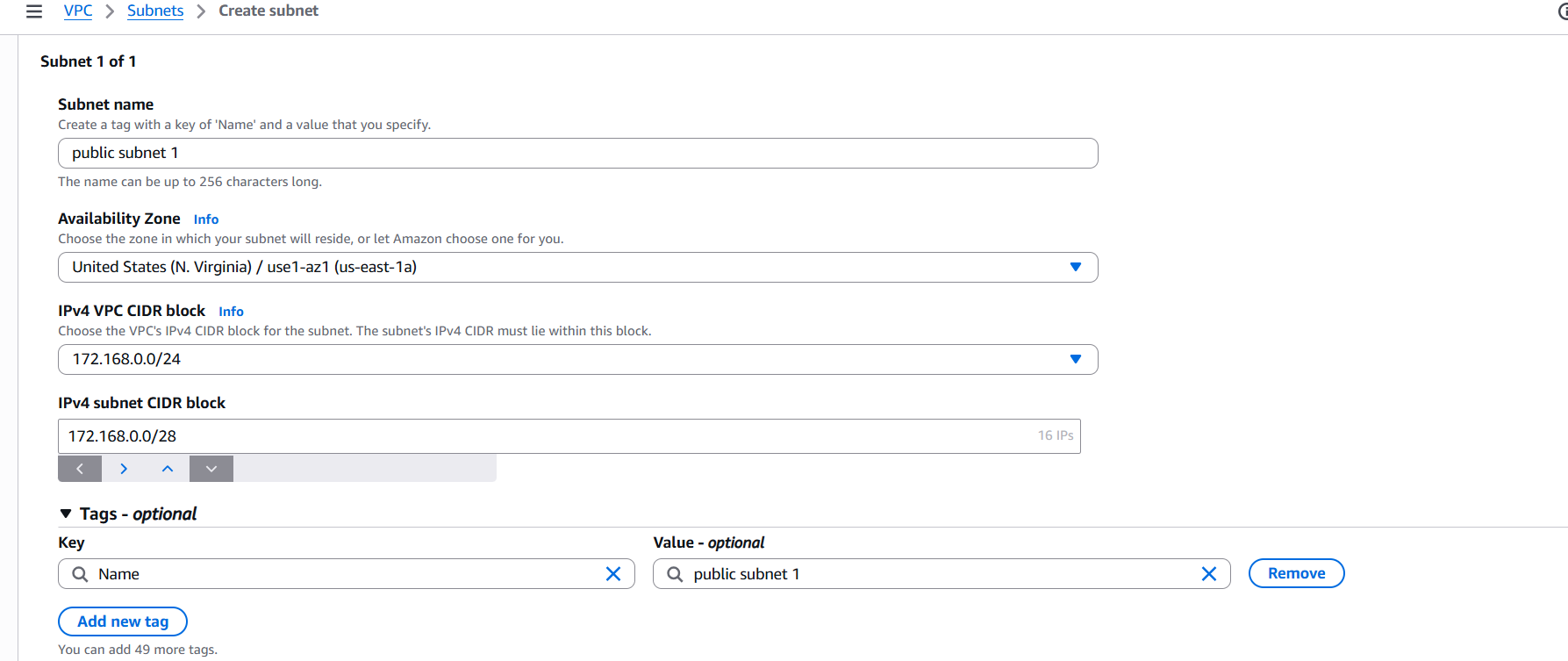
**Task on VPC -01**

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





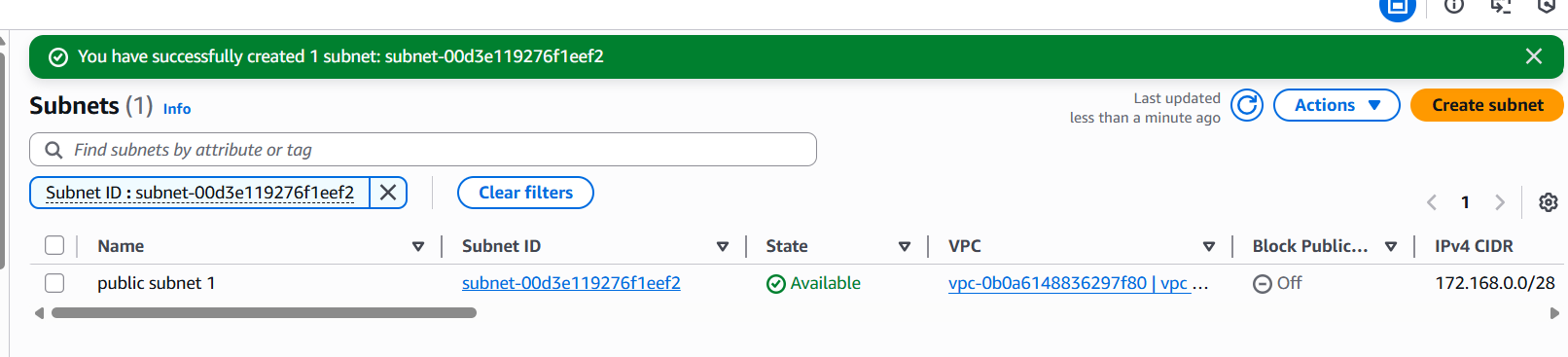
then create subnet



create subnet public 1 and named vpc as puiblic subnet 1 and selected availability zone 1a

subnet starts from 0 so here I took 172.168.0.0/28

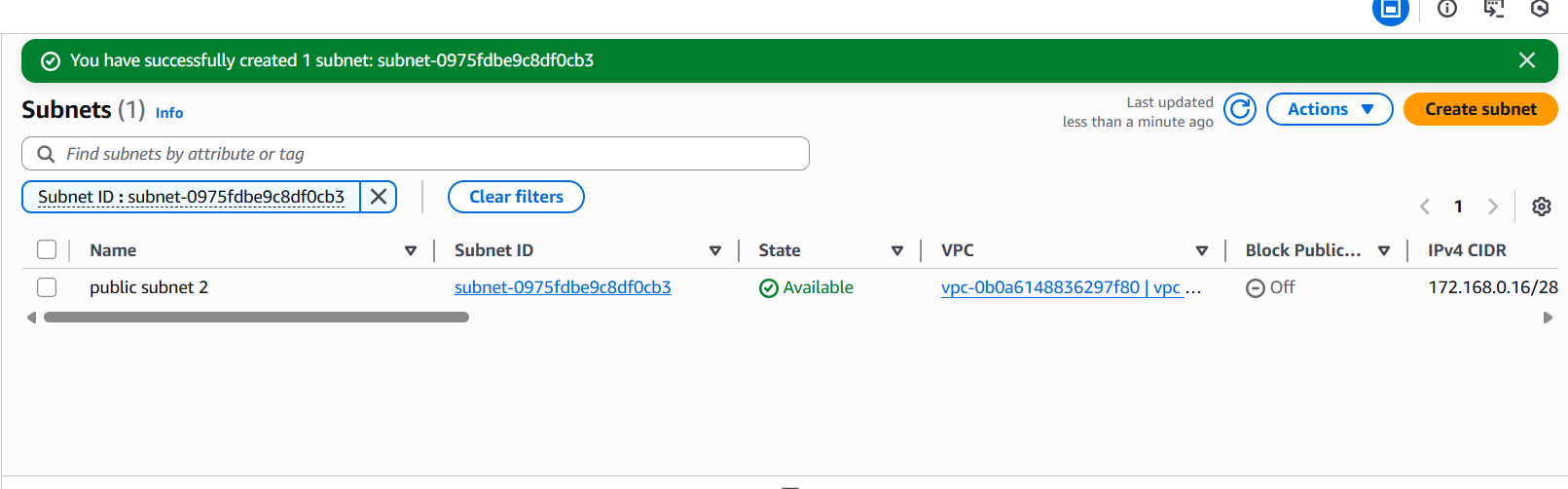
now 16 ip’s has been utilized



created public subnet 2 and named vpc as piblic subnet 1 and selected availability zone 1b

now here already 16 has been utilized now we need to start from 17

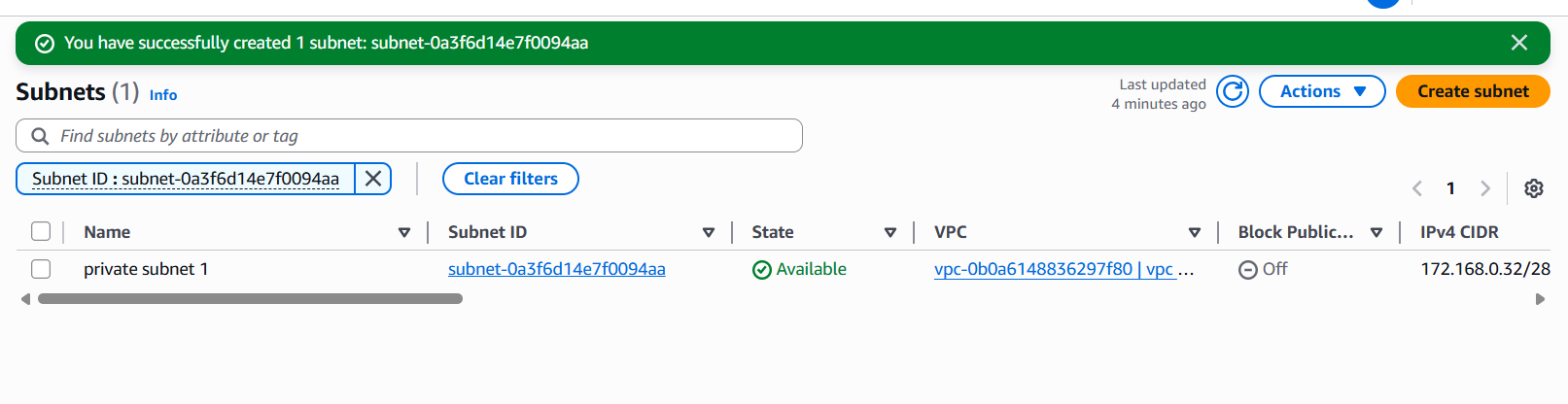
here I entered 172.168.0.17/28



created private subnet 1 and named vpc as private subnet 1 and selected availability zone 1a

now here 32 has been utilized now we need to start from 33

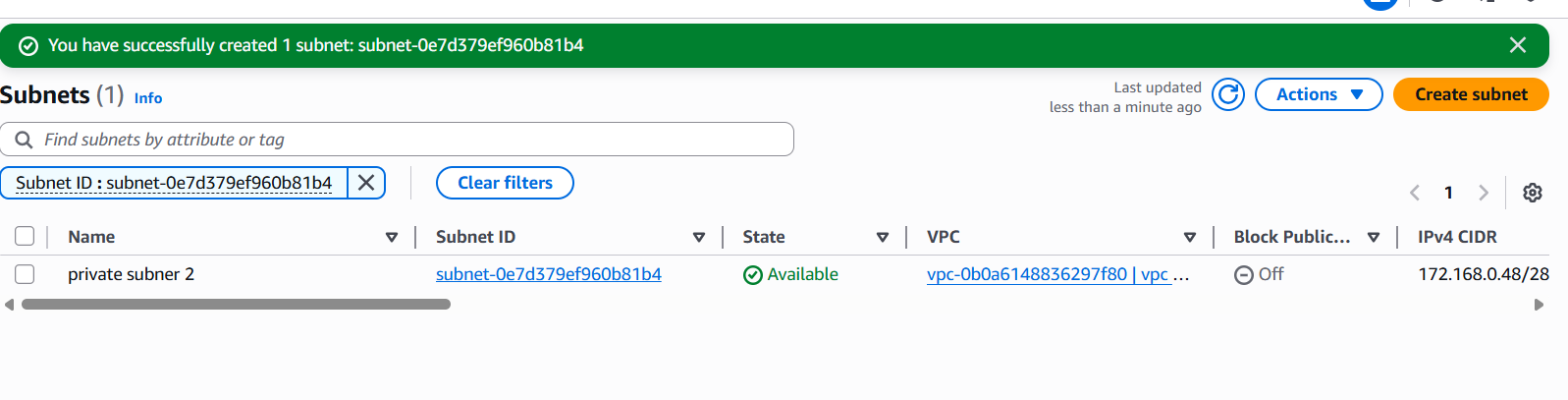
here I entered 172.168.0.33/28



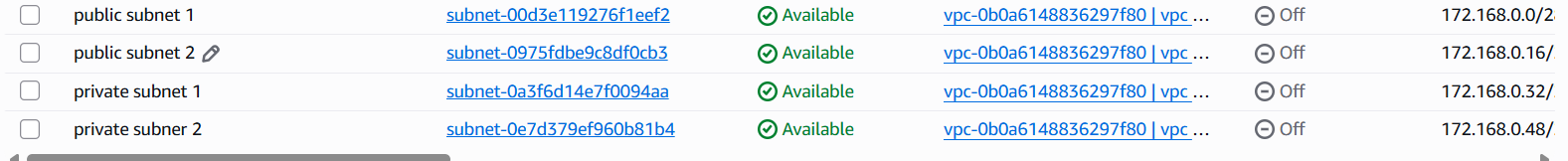
crated private subnet 2

here 48 has been utilized now we need to start from 49

here I entered 172.168.0.49/28 and named vpc as private subnet 2 and selected availability zone 1b



to vow the list of subnets u have created click on subnets



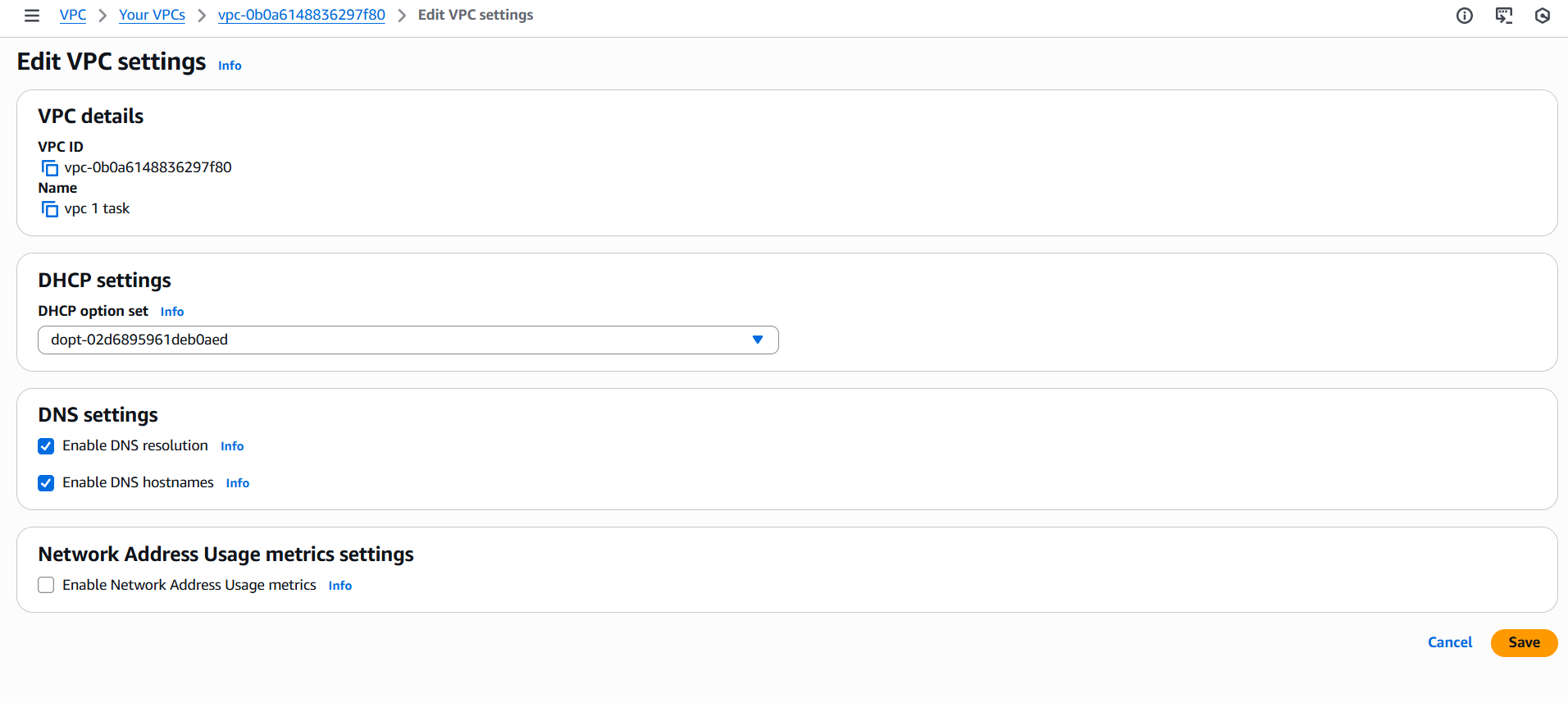
1. Enable DNS Hostname in VPC.

first click on your VPCs

then go to actions-edit vpc settings



after opening vpc settings click on enable DNS hostname and save it



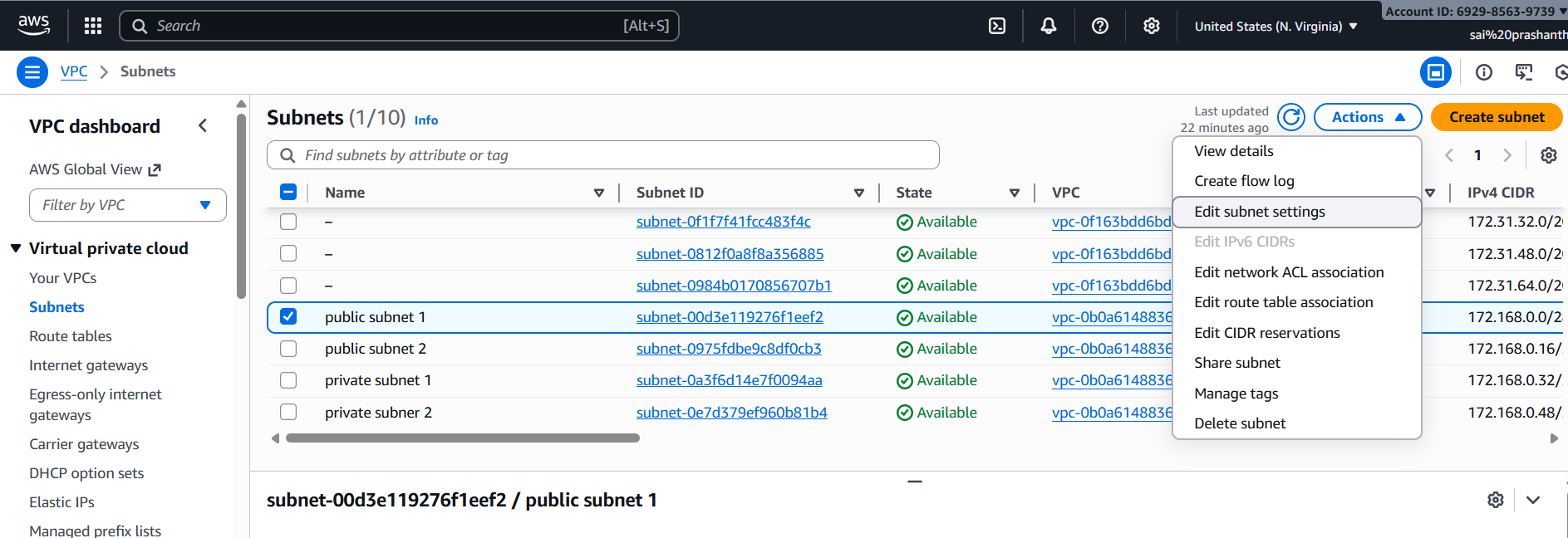
now the DNS hostname has been created

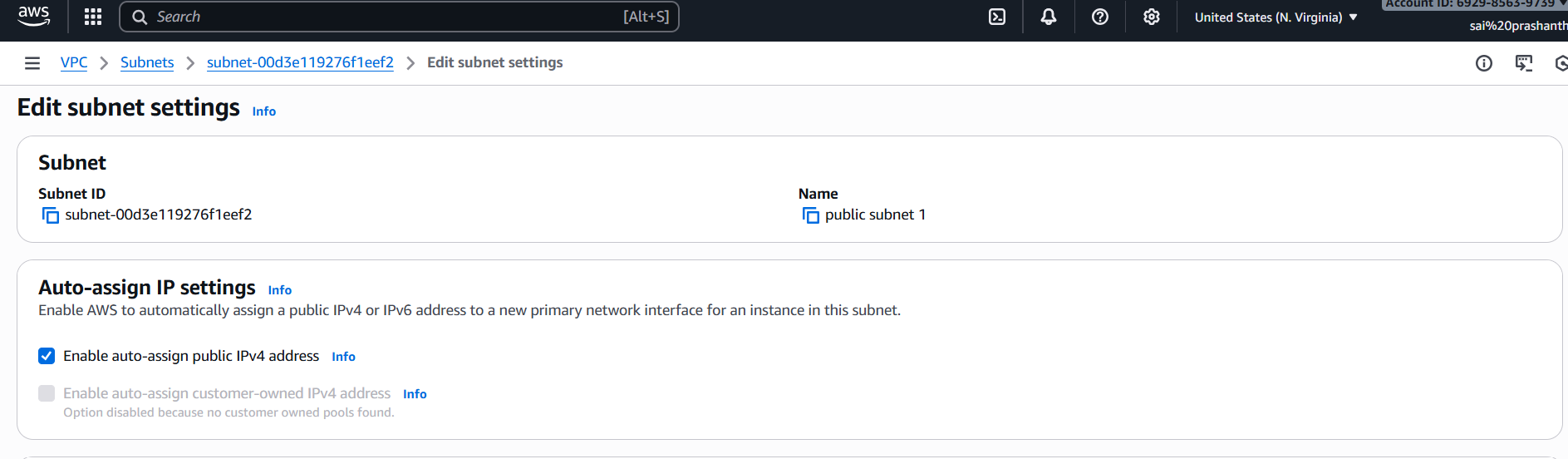
1. Enable Auto Assign Public IP in 2 public subnets.

first click on subnets

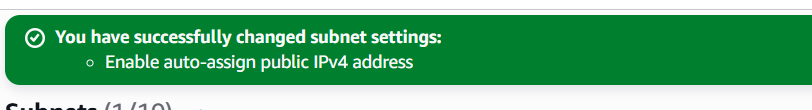
click on public subnet 1

then go to actions-edit subnet settings-then click on enable auto-assign public IPv4 settings





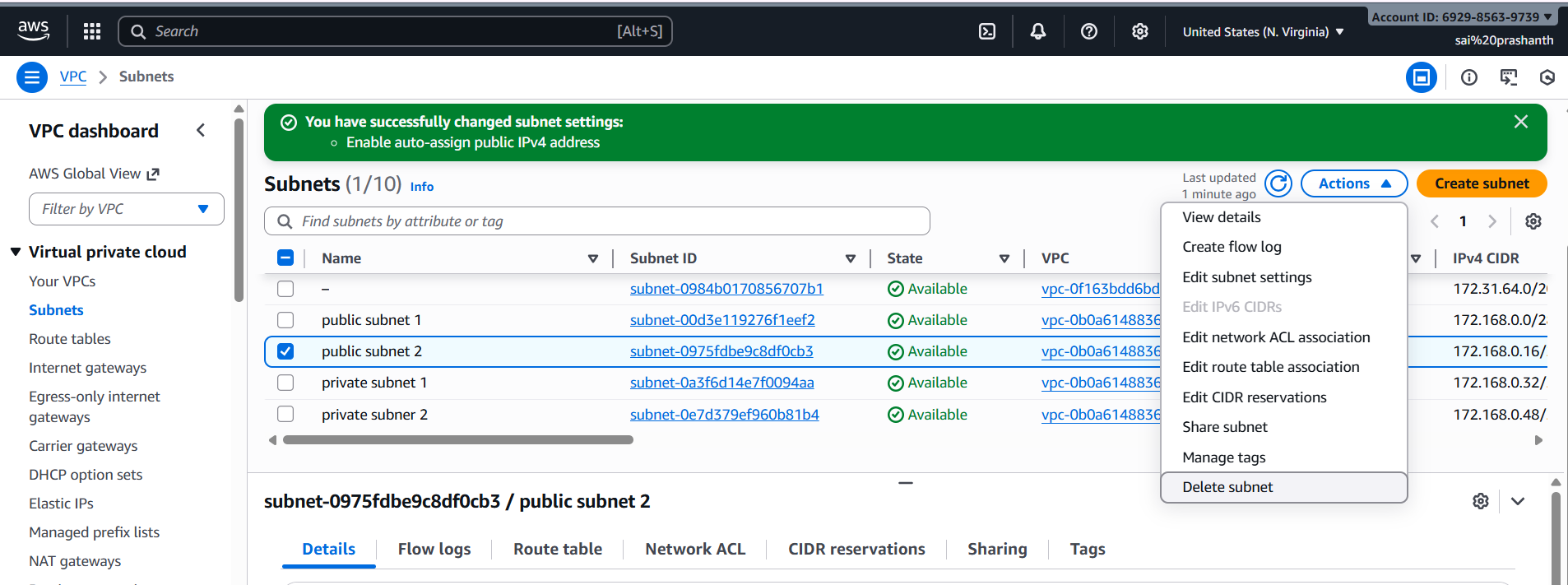
click on save



repeat same for public subnet 2

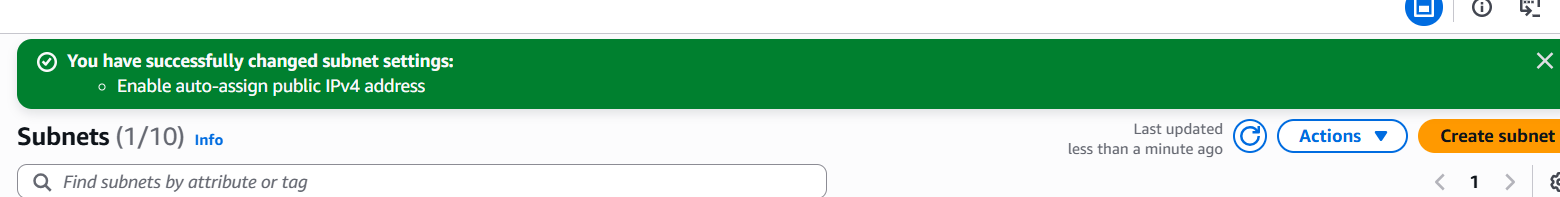
click on public subnet 2

then go to actions-edit subnet settings-then click on enable auto-assign public IPv4 settings





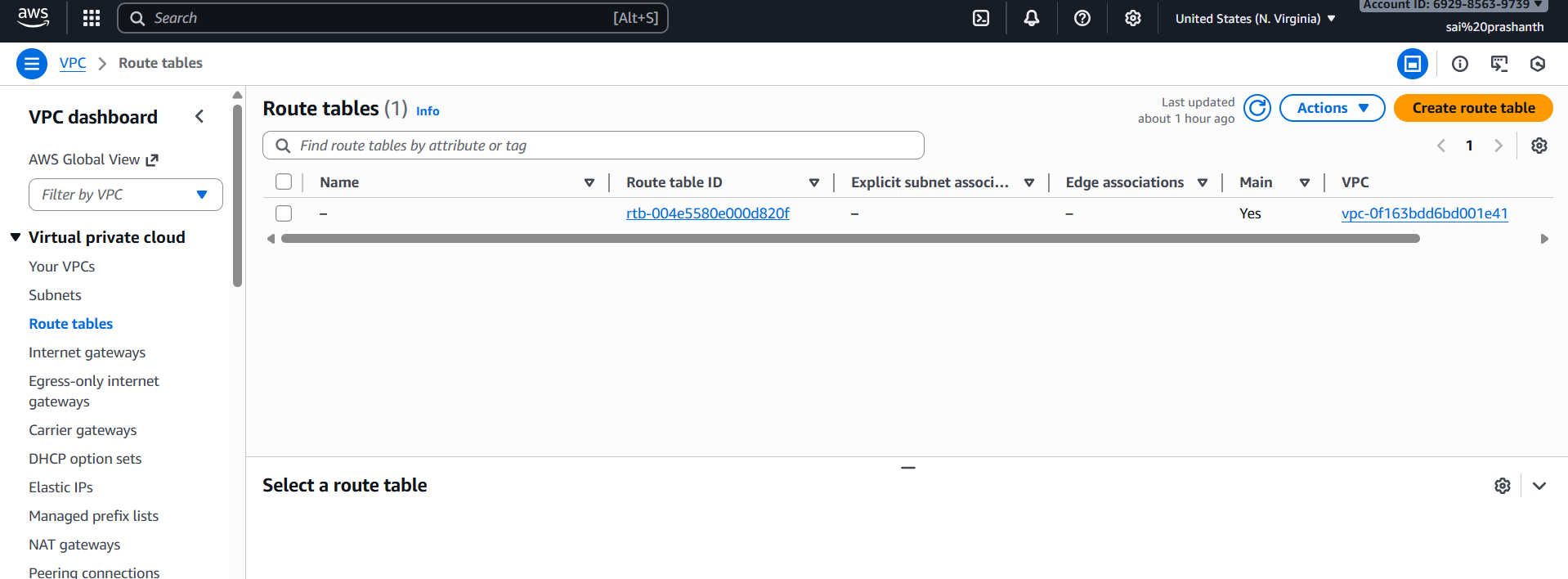
then click on save

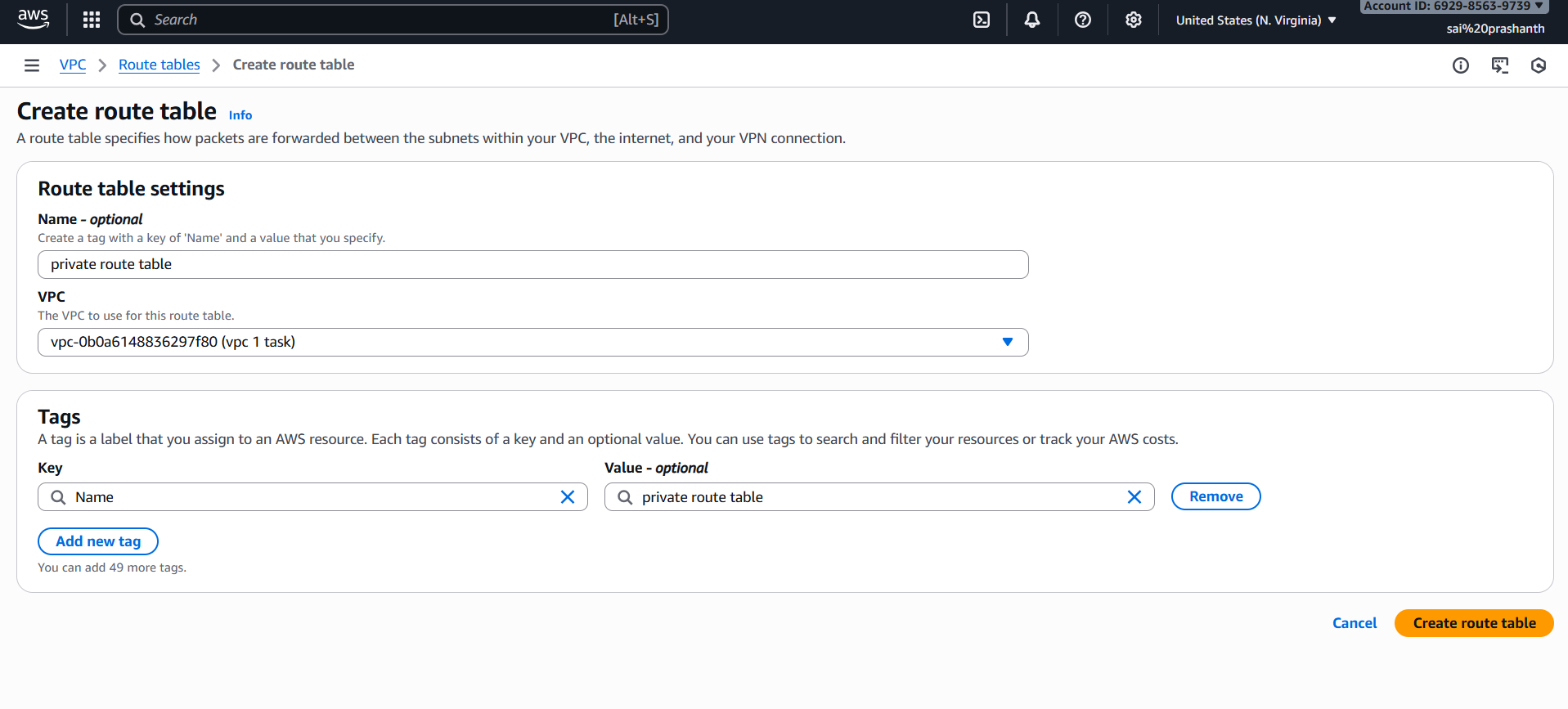


1. Add 2 private subnets in private route table.

furst go to route tables and click on create route table

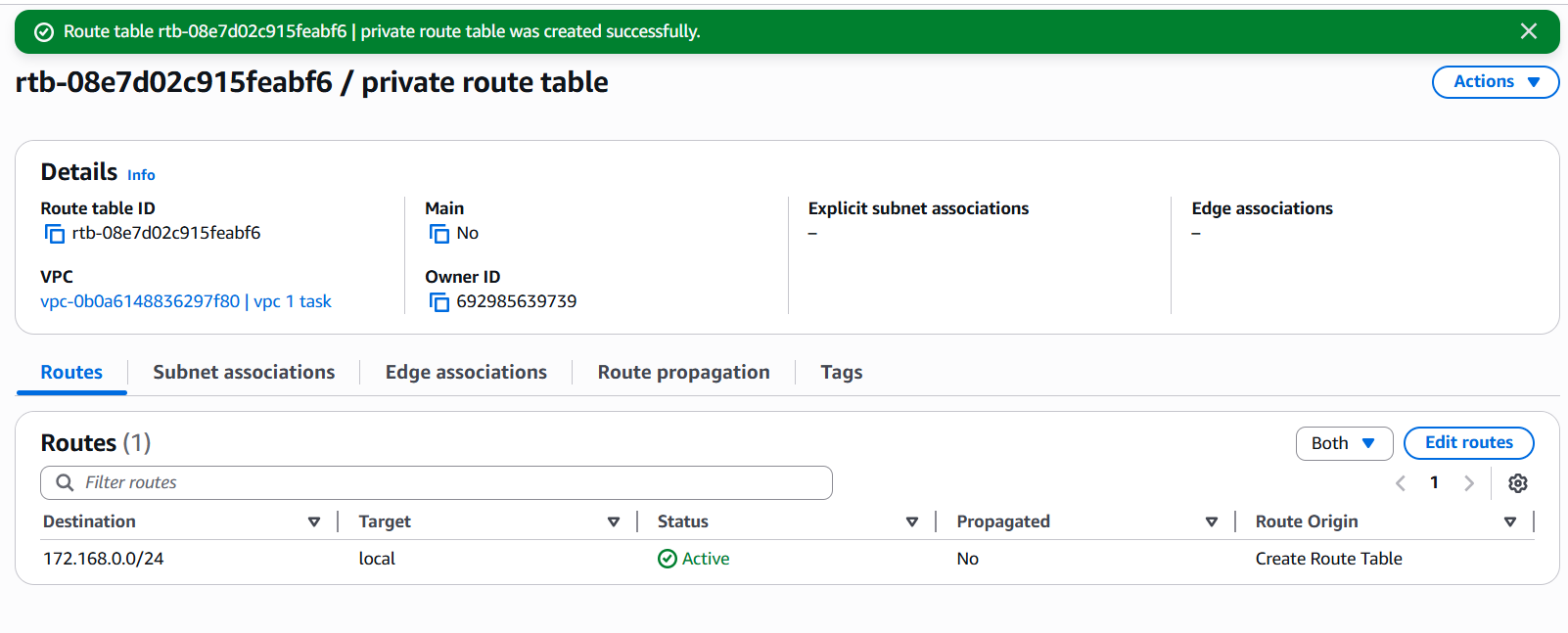
after clicking it enter route table as private route table





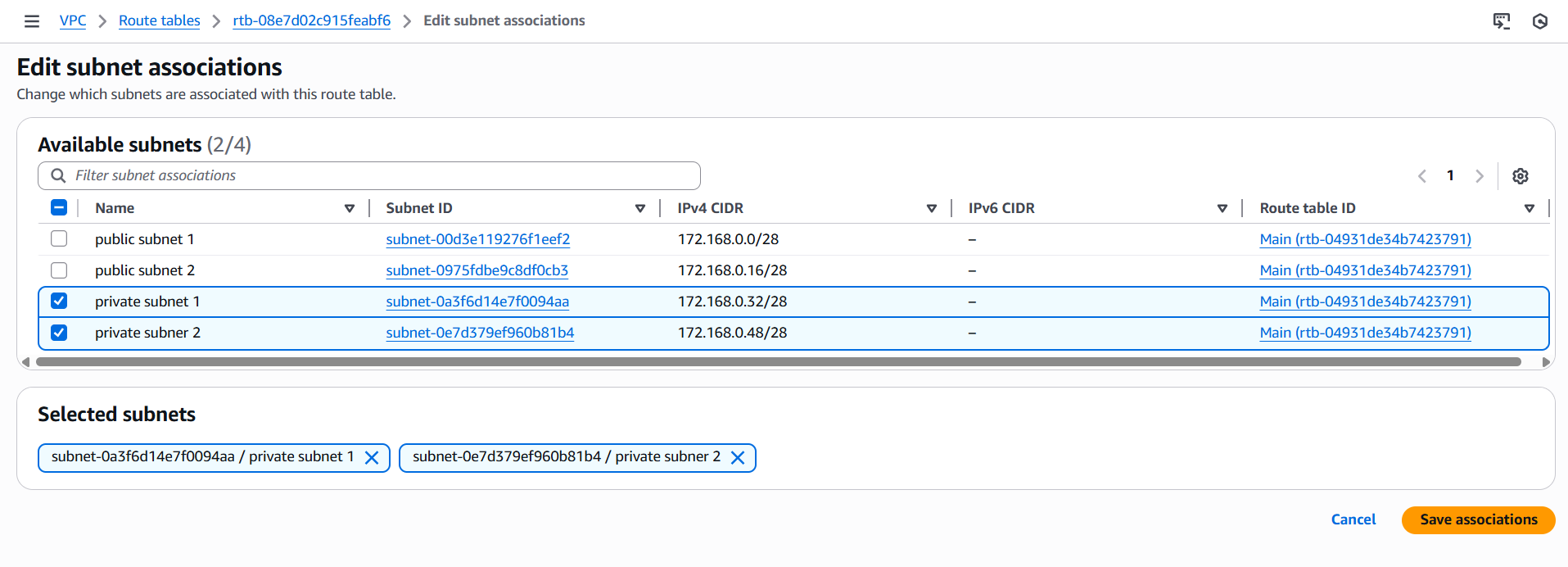
click on create route table

route table has been created successfully



now go to actions-edit subnet associations-add both private subnets 1 and 2

click on save associations



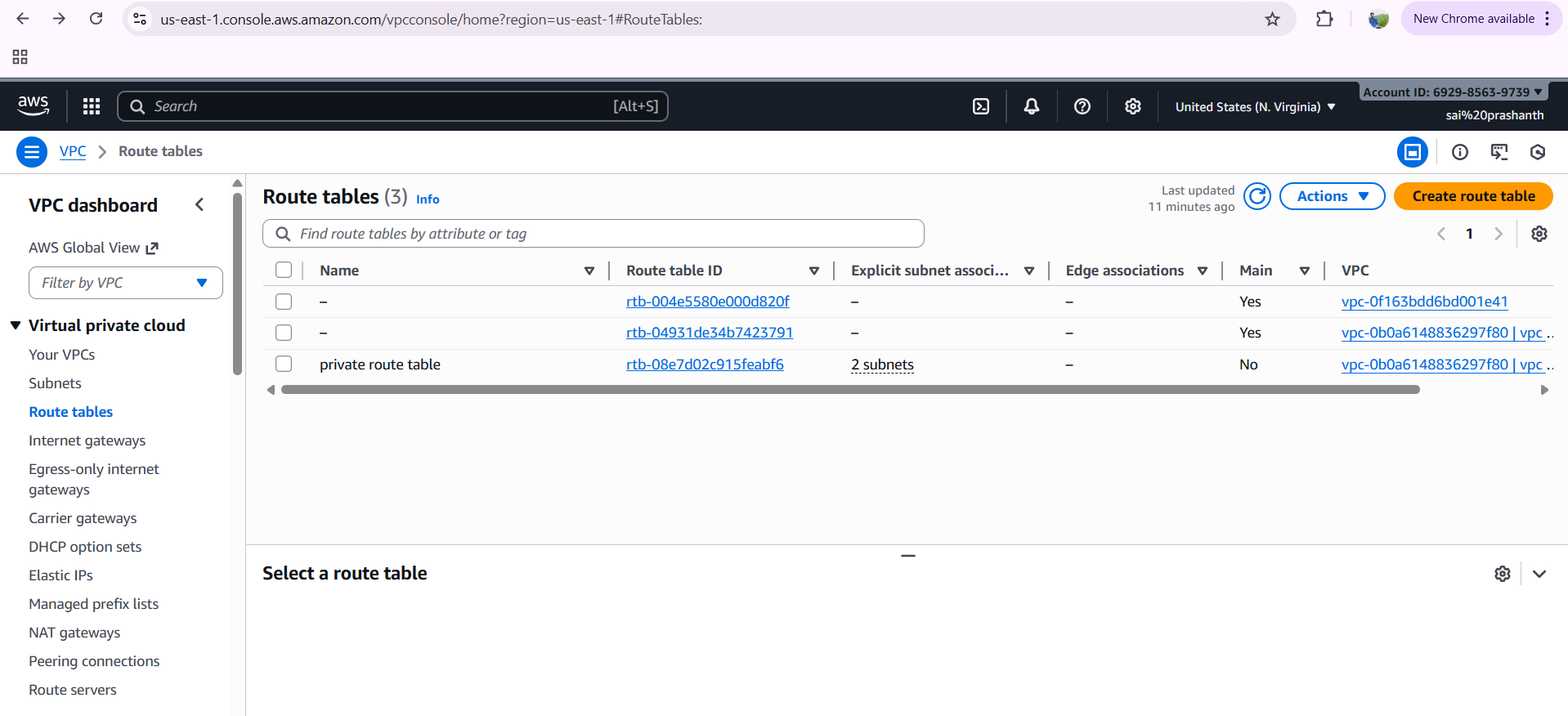
after saving it

you can see 2 private subnets has been saved in private route table

1. Add 2 public subnets in public route table.

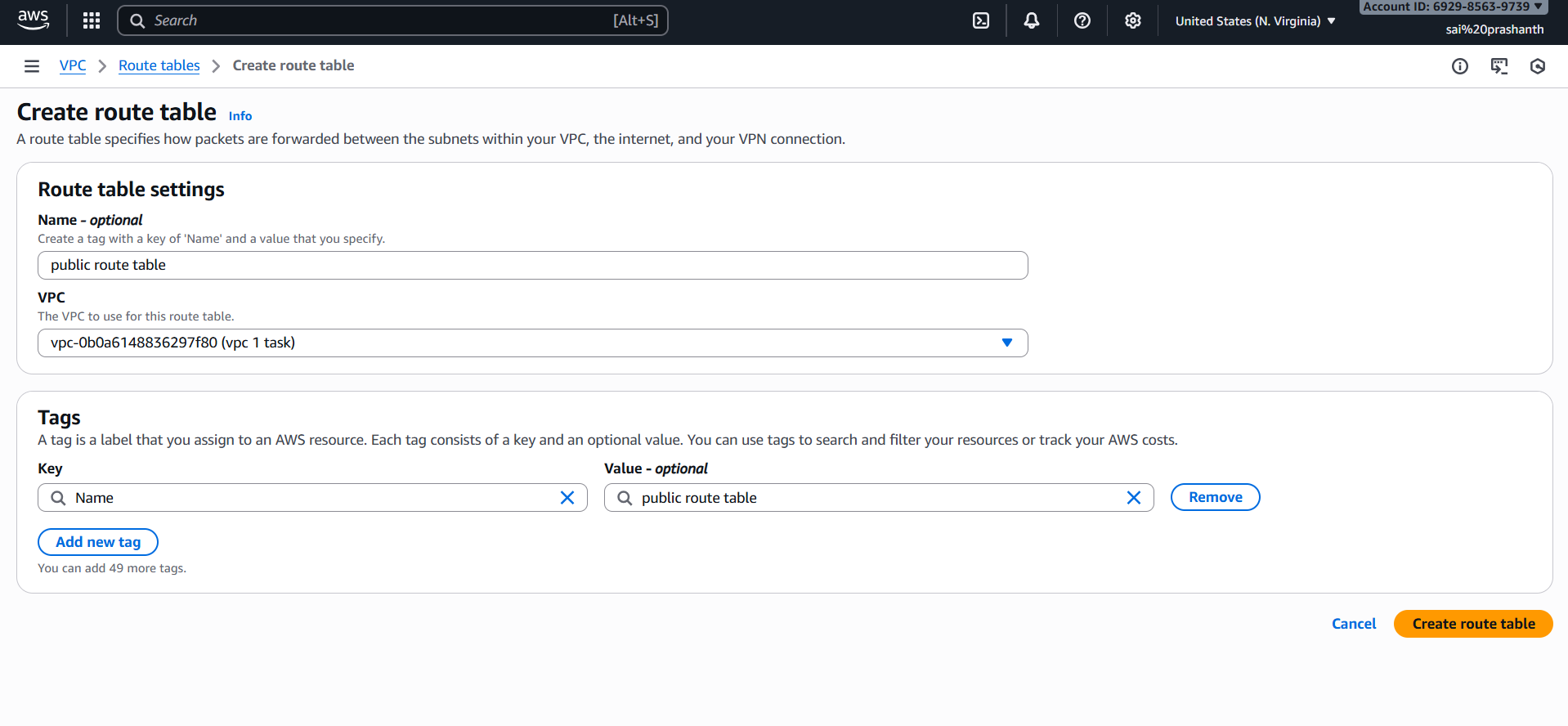
first go to route tables

click on route table

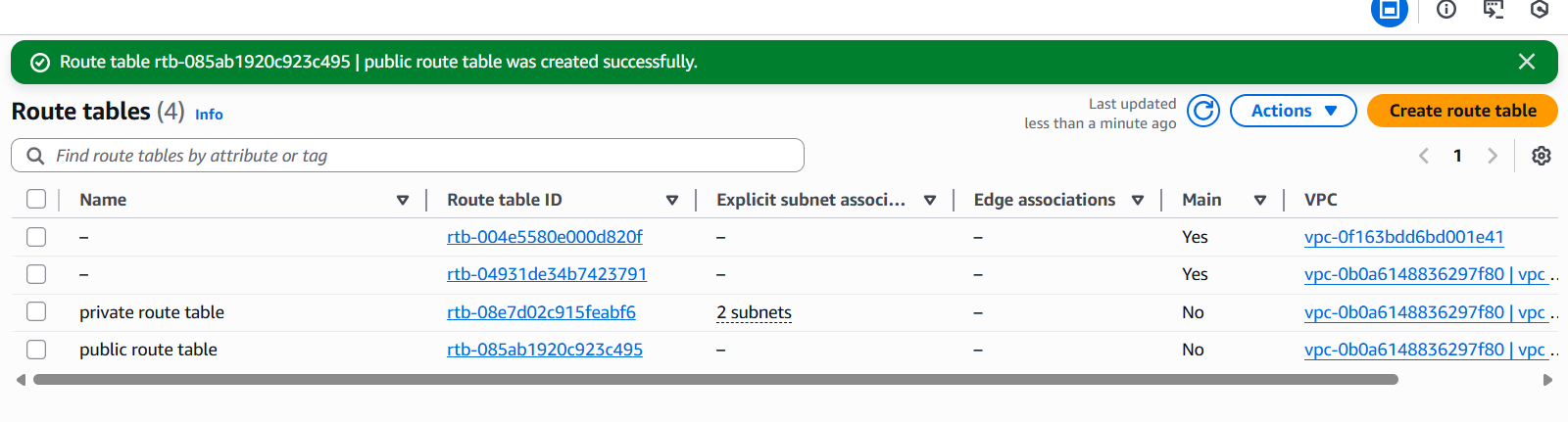


after clicking it enter route name as public route table

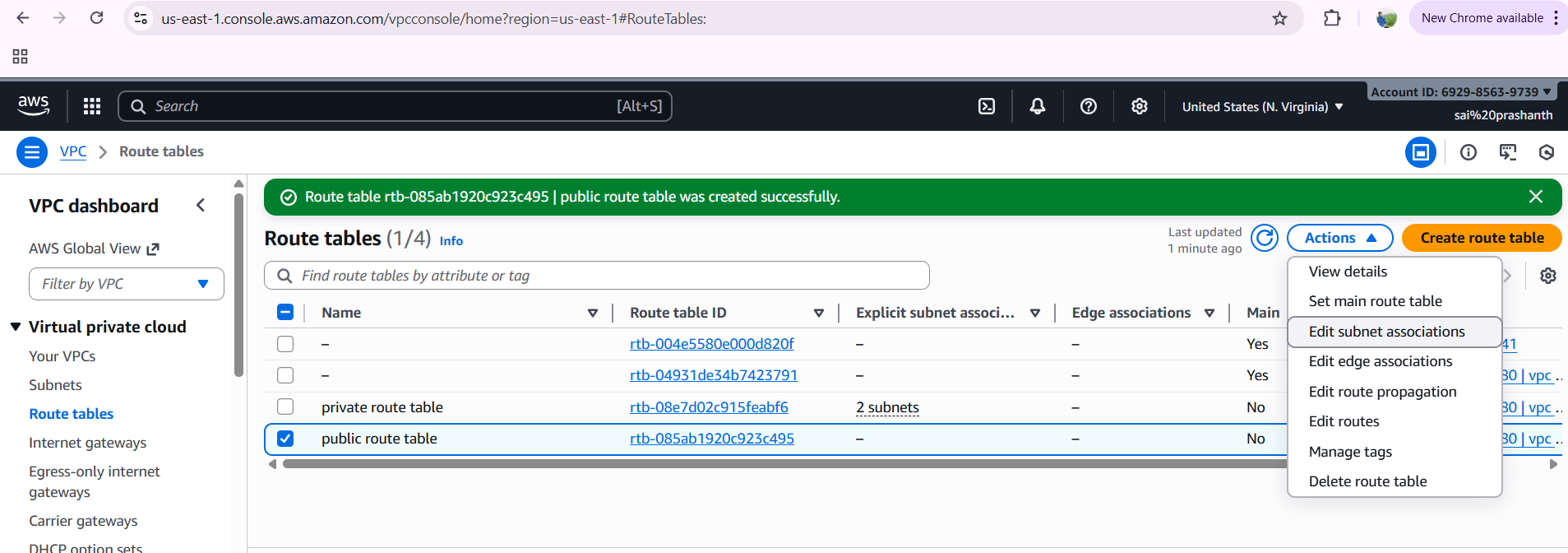
and click on create route table



public route table has been created

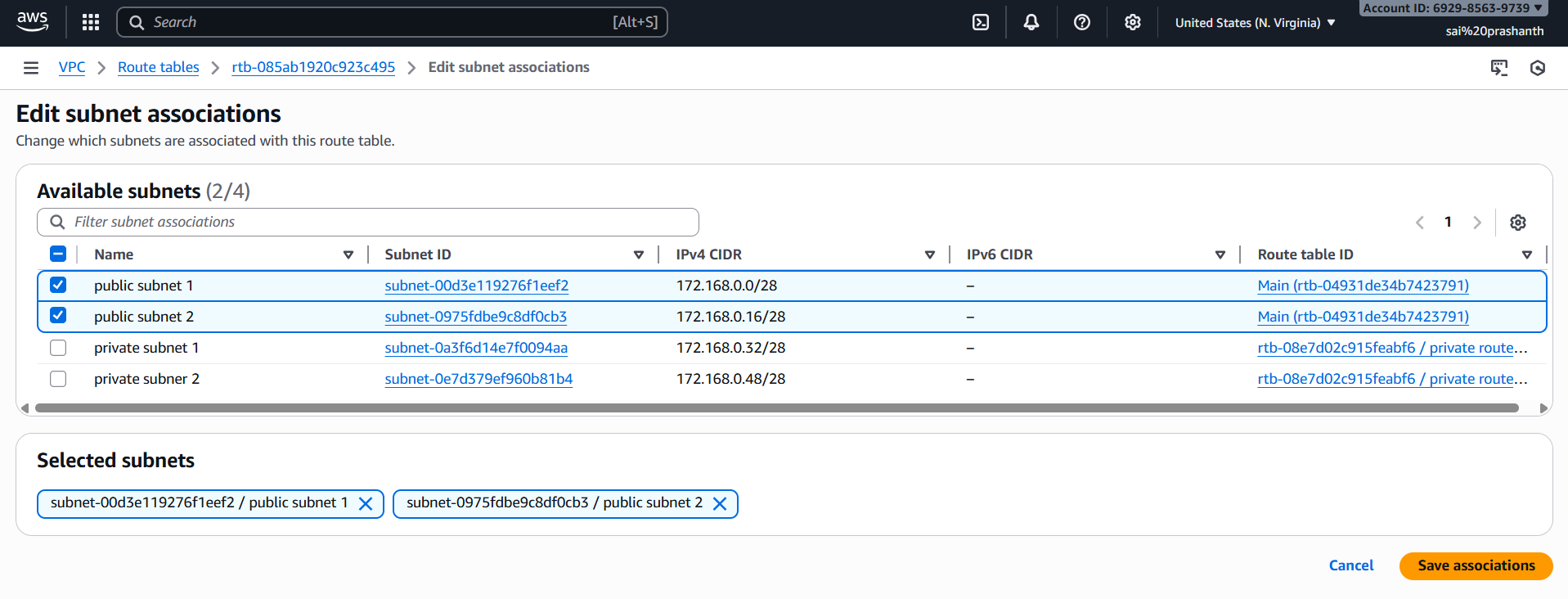


now select public route table column and go to actions-edit subnet associations

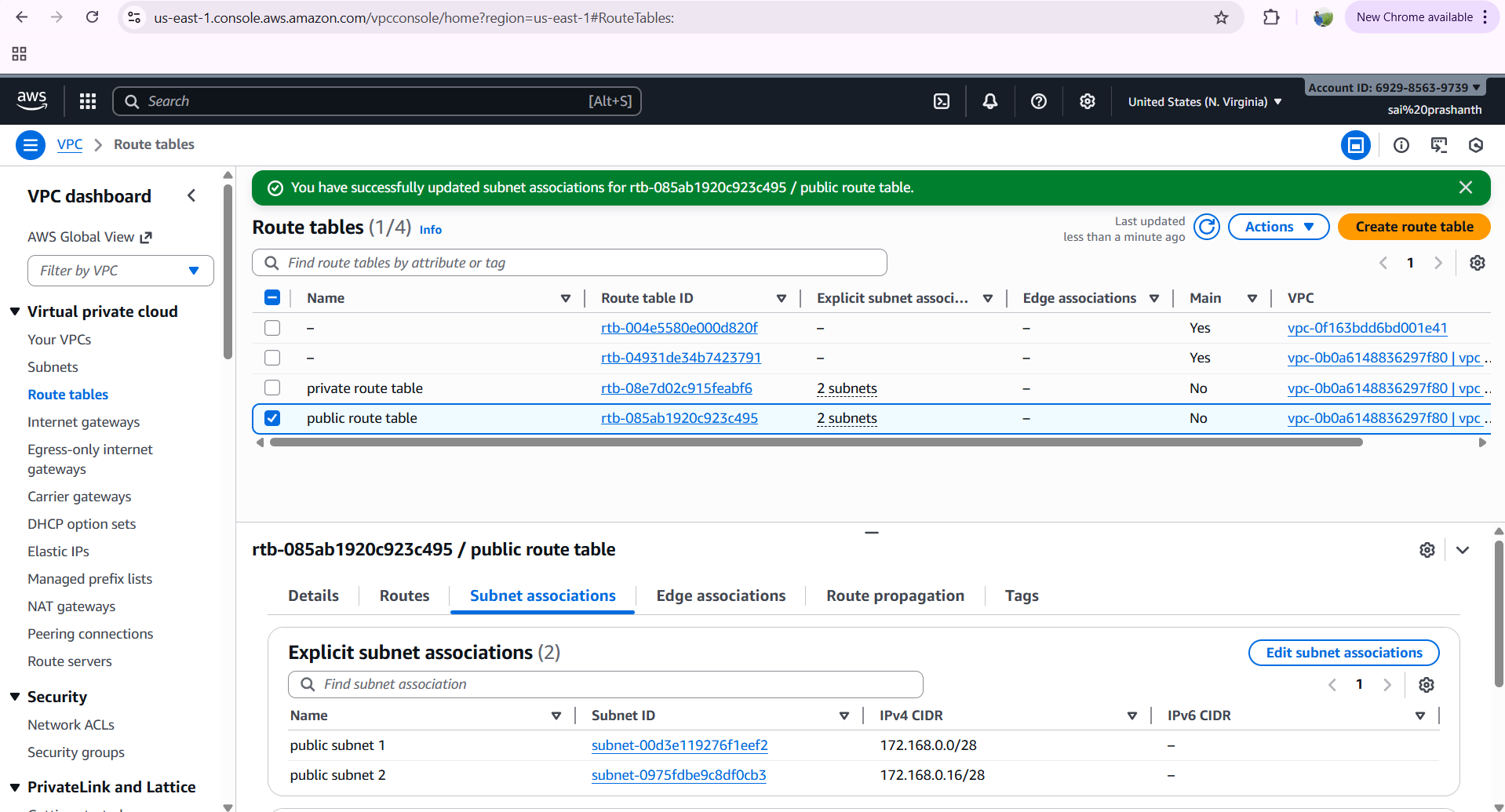


select both public subnets 2

and click on save associations



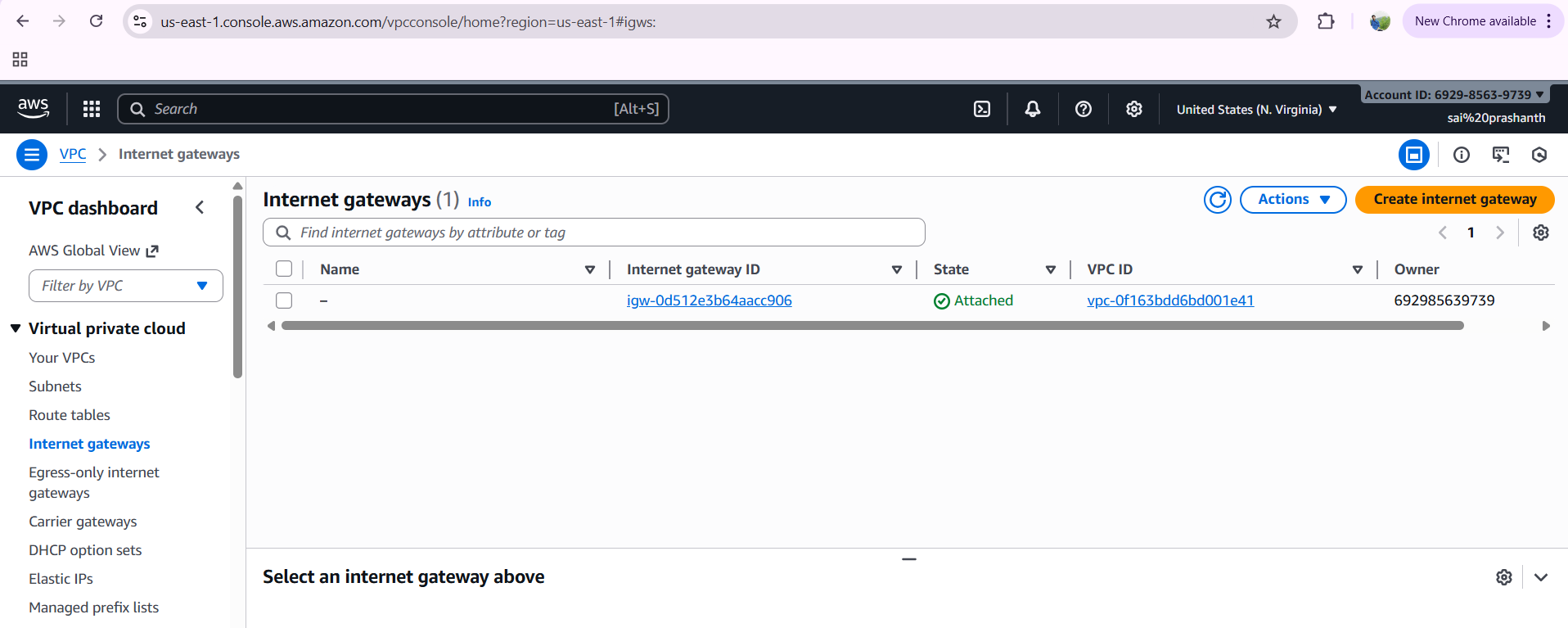
finally, the public subnets 2 has been saved in public route table



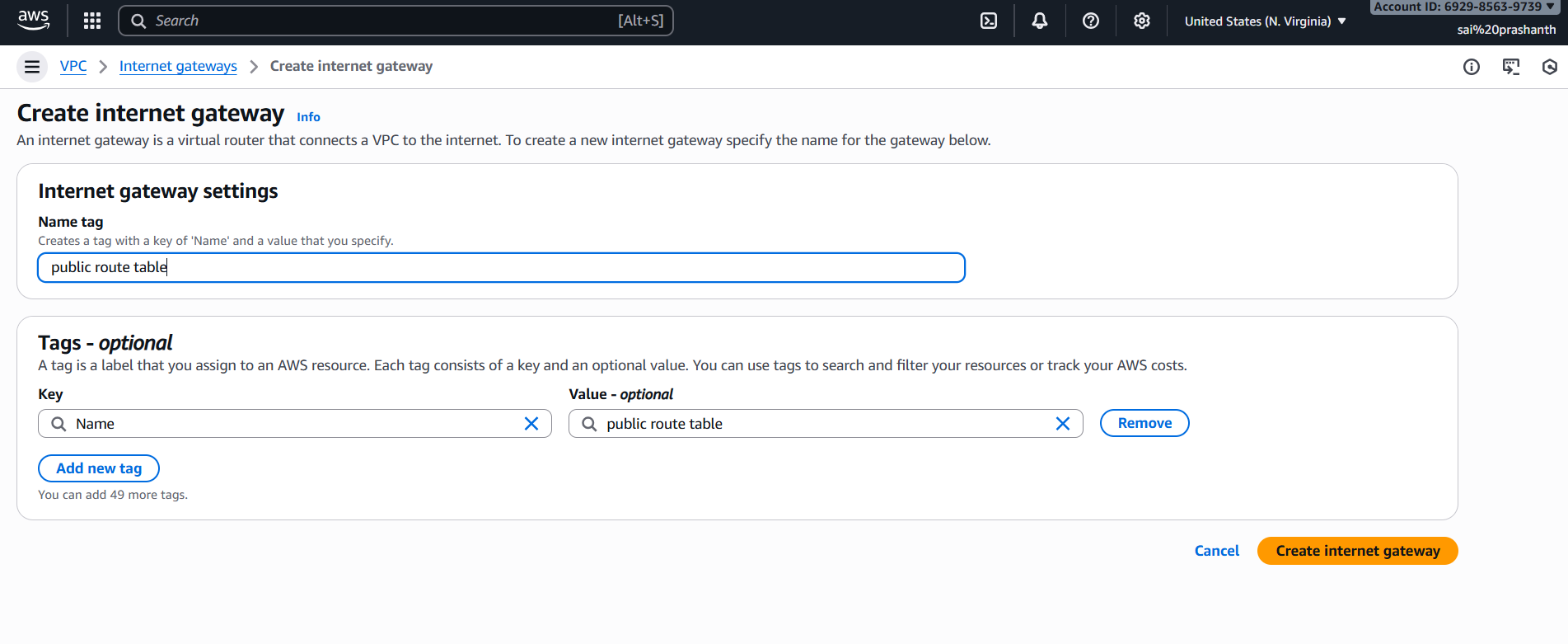
1. Public route table will have the routes to internet and local.

first to access the internet and local to public route

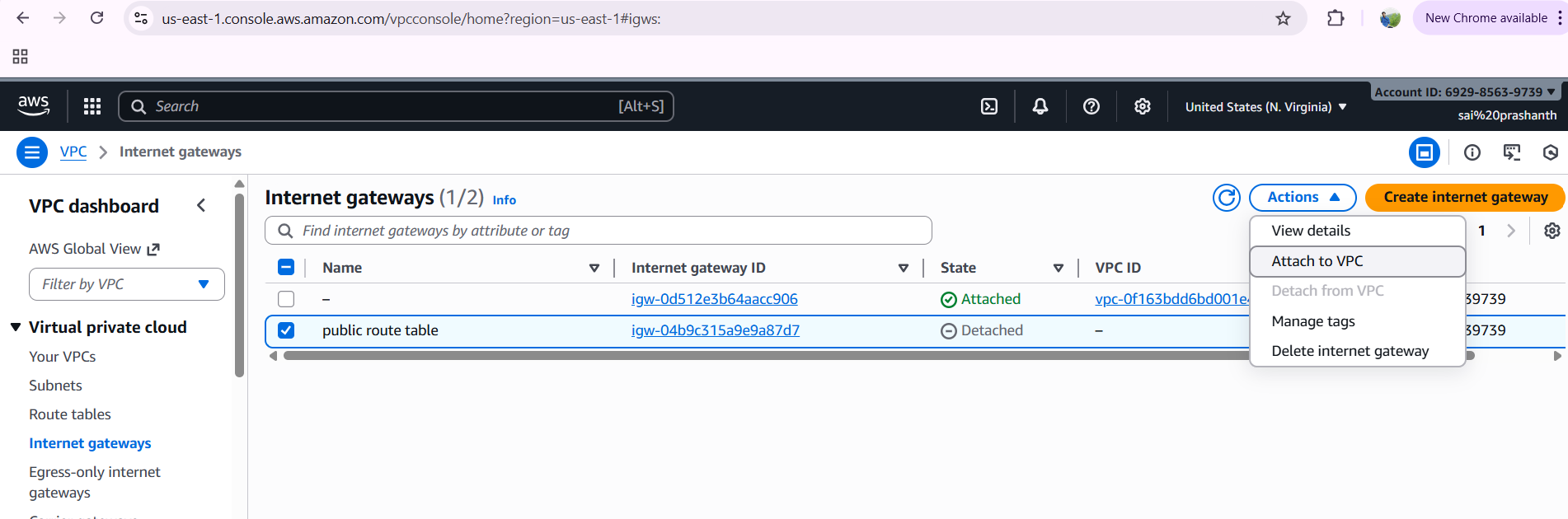
go to internet gateways and click on create internet gateway



after clicking it add the gateway as public route table and click on create



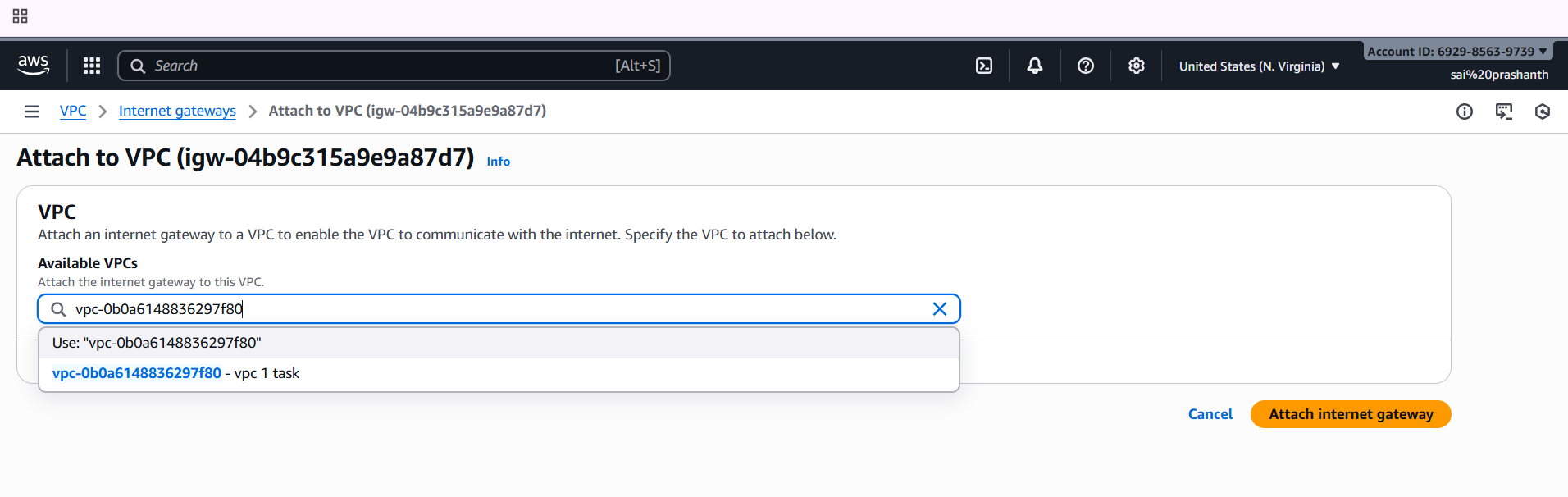
once it has been created click on actions—attach to vpc



select your vpc id

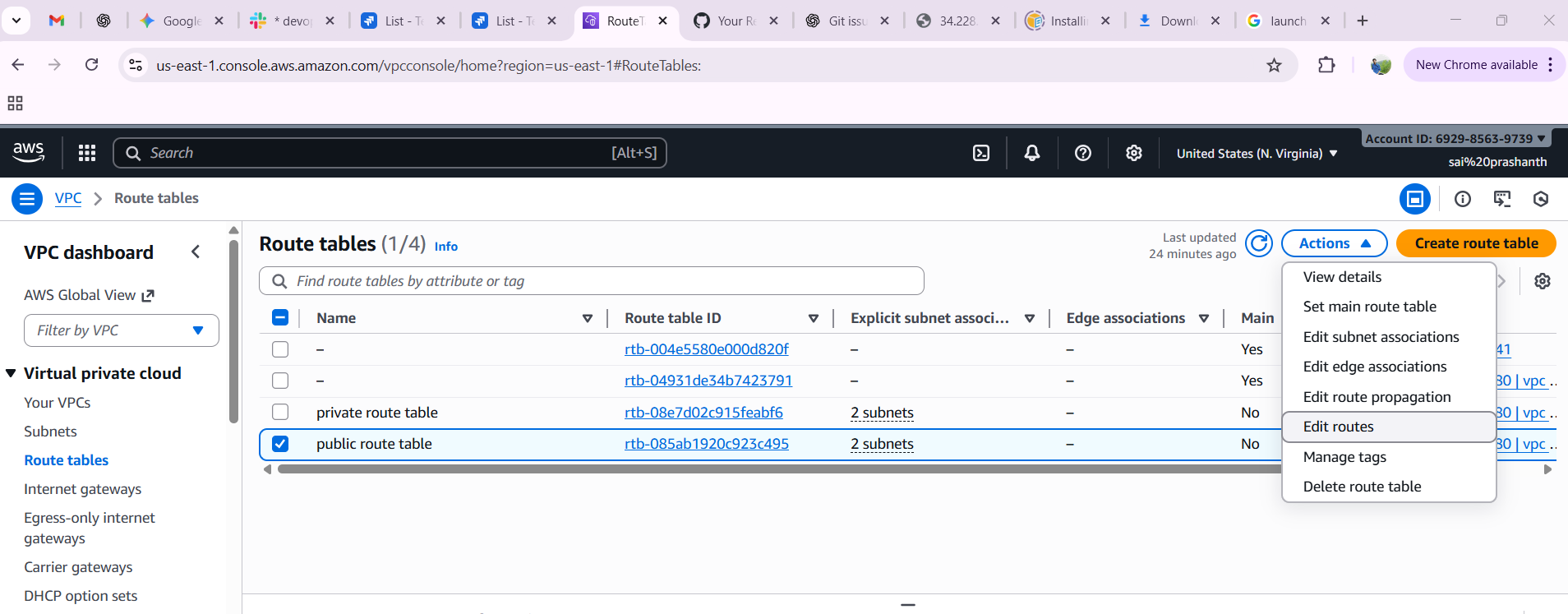
and click on attach internet gateway

once it has been attached, we provide the access to internet for public route

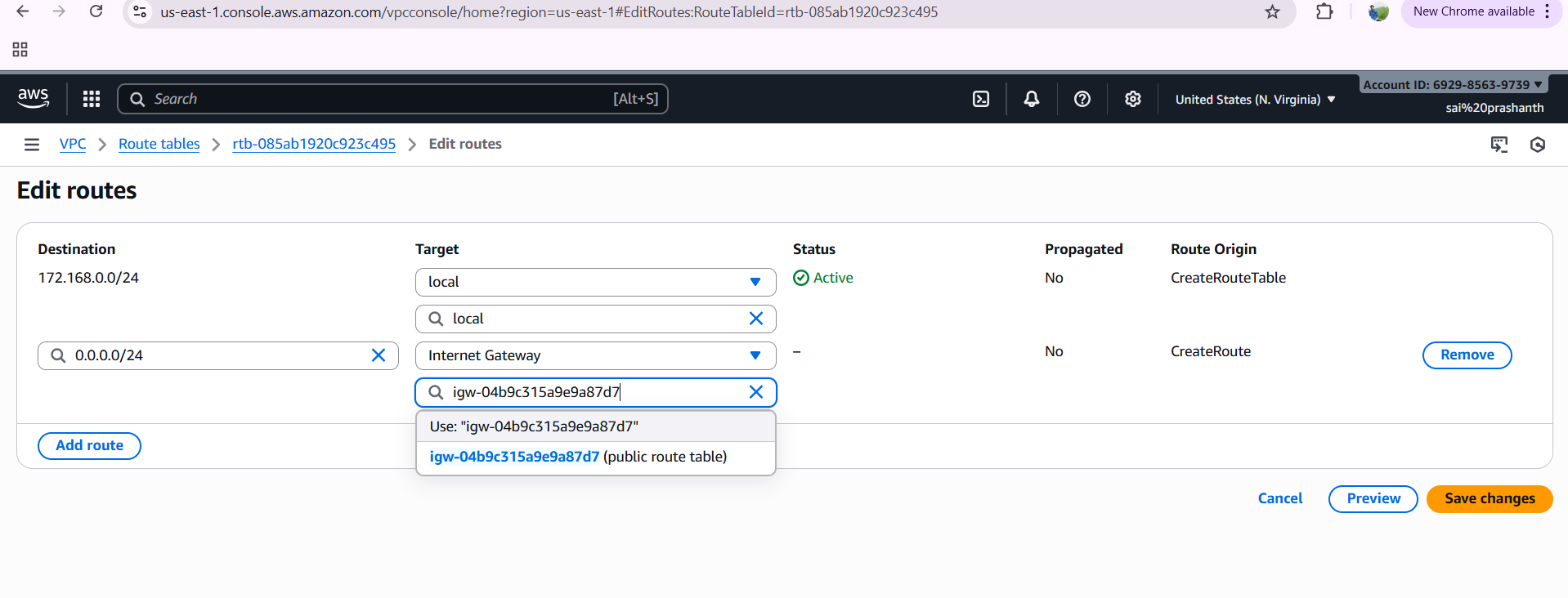


now again click on route table

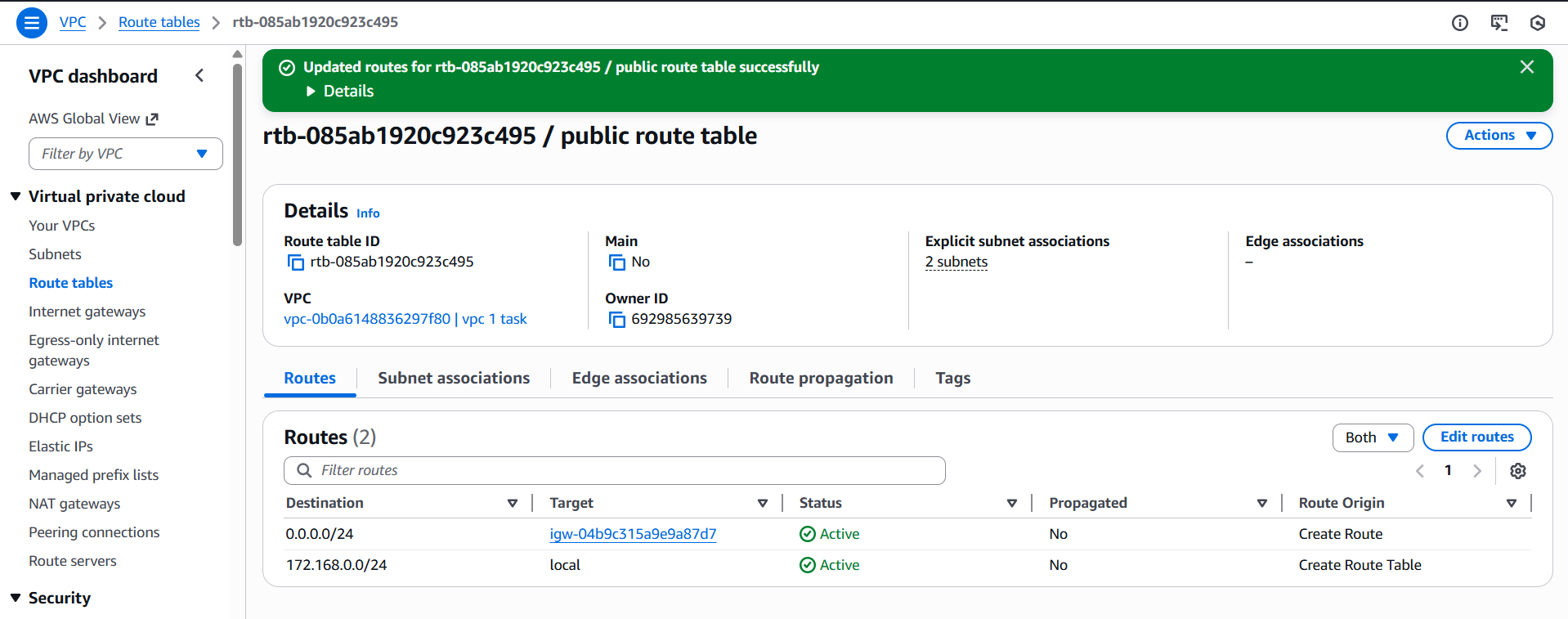
select public route table option—click on actions—select edit routes to give inbound and outbound access



now add the internet gateway with ig id as local has been defaultly added and click on save changes



finally the local and internet has been added to public route table



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

first create instance and in network settings add the vpc id and select public subnet 1 then add default security group and create instance.

now connect in git bash through your ssh

switch to root user and install php

yum update -y

now to install php

yum install php -y

connect php httpd and try to install along with httpd

yum install httpd php -y

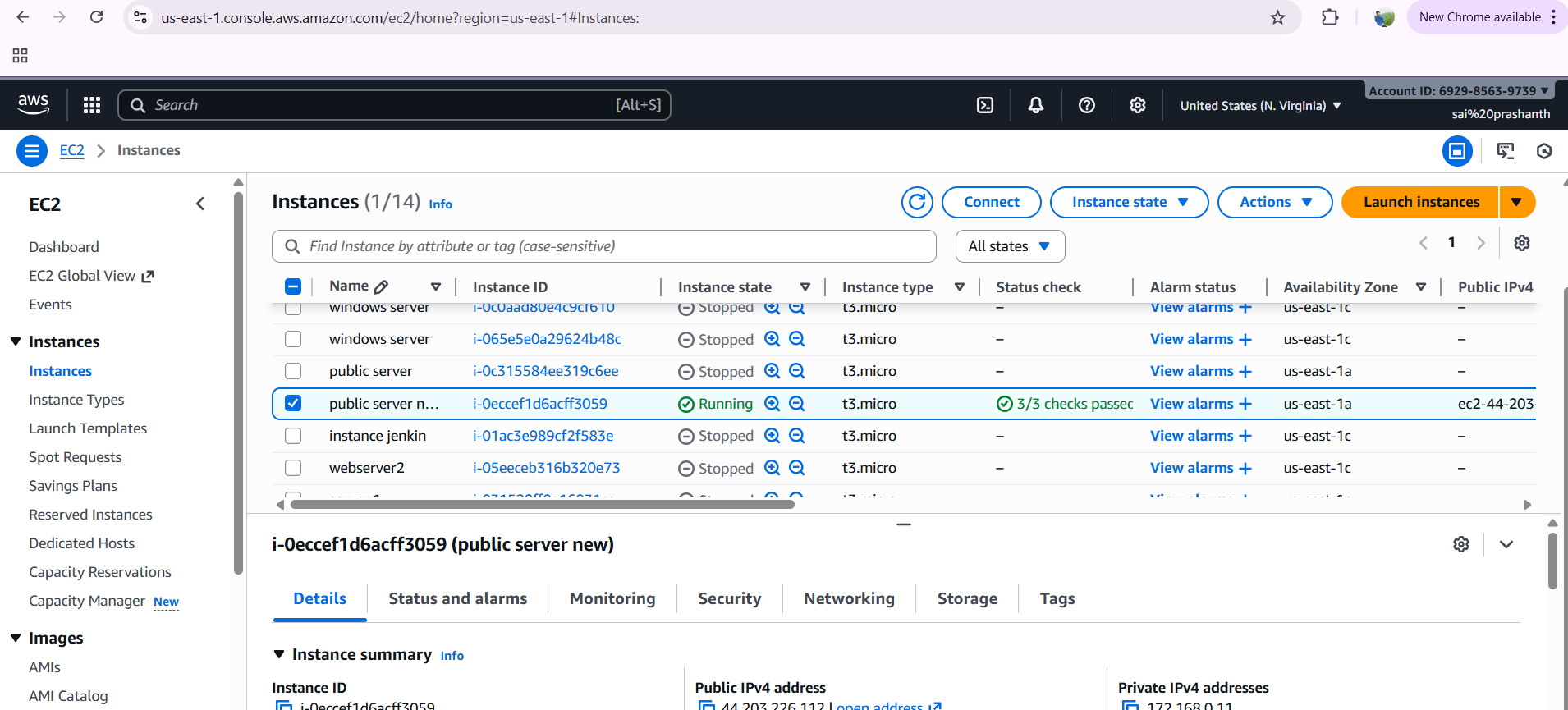
now systemctl start, status and enable httpd

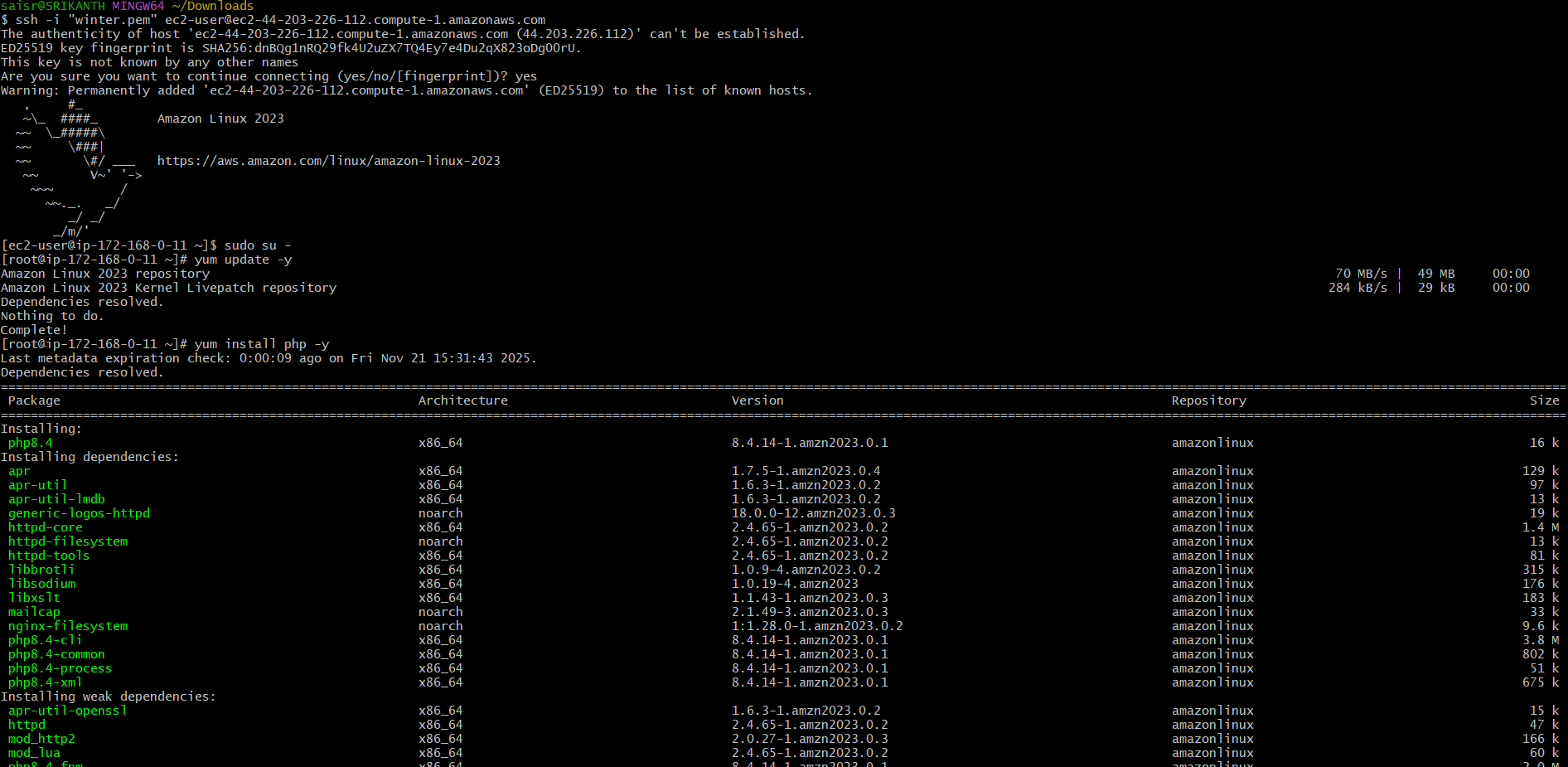
to verify the installation

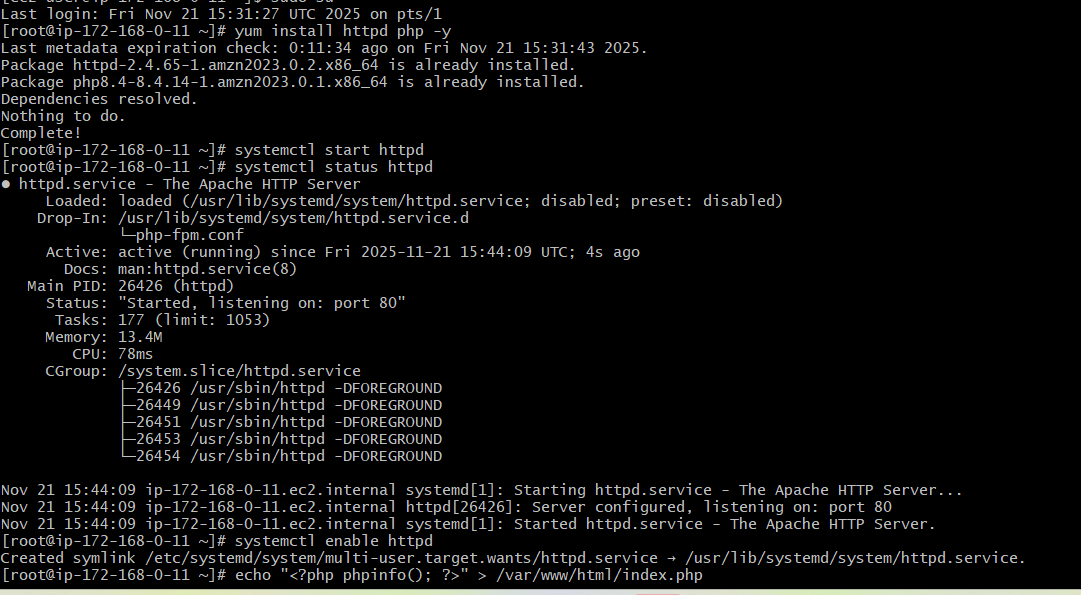
use the command

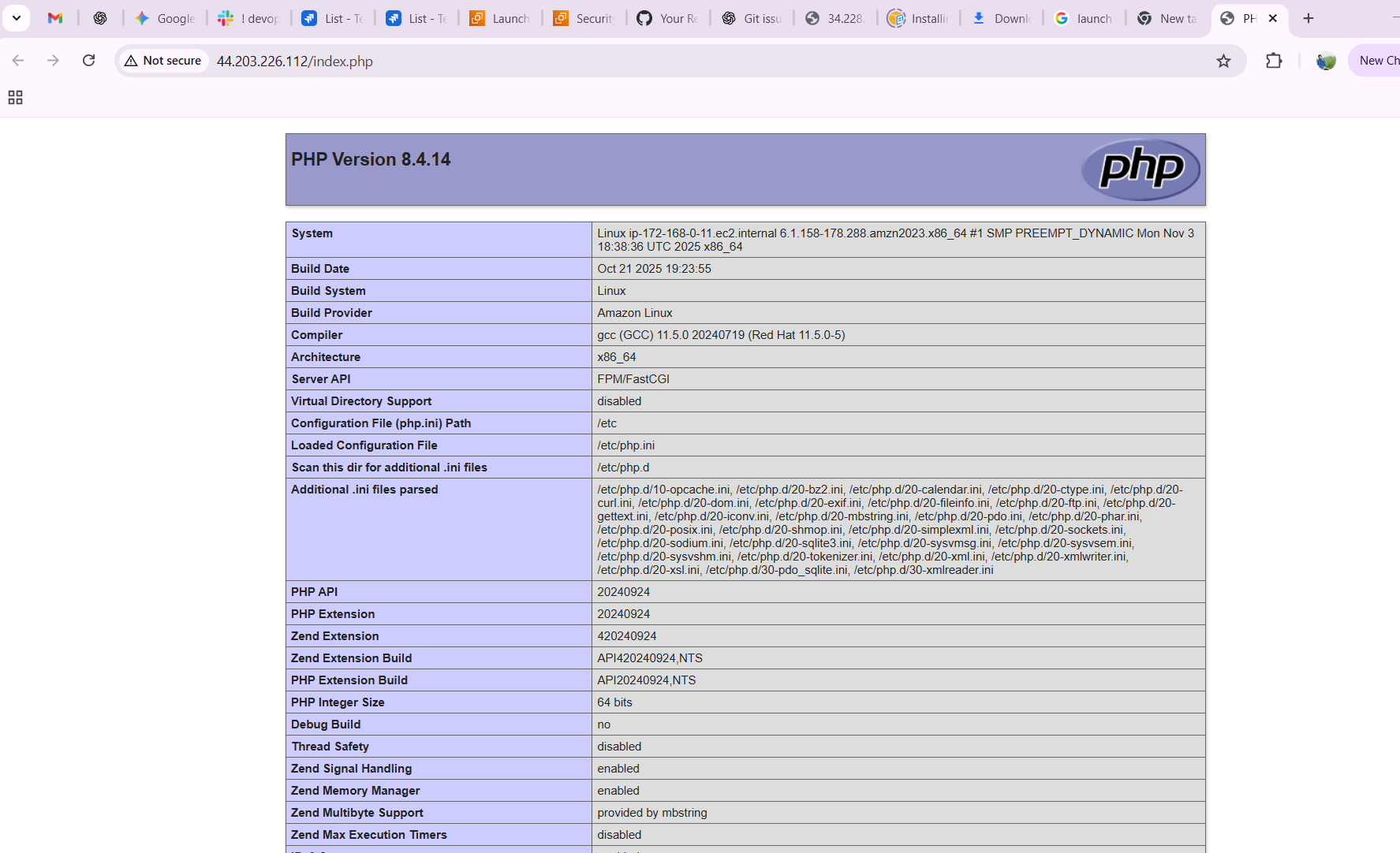
echo "<?php phpinfo(); ?>" > /var/www/html/index.php

now to verify in the browser use publicid/index.php



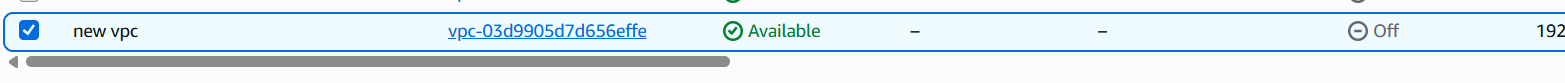




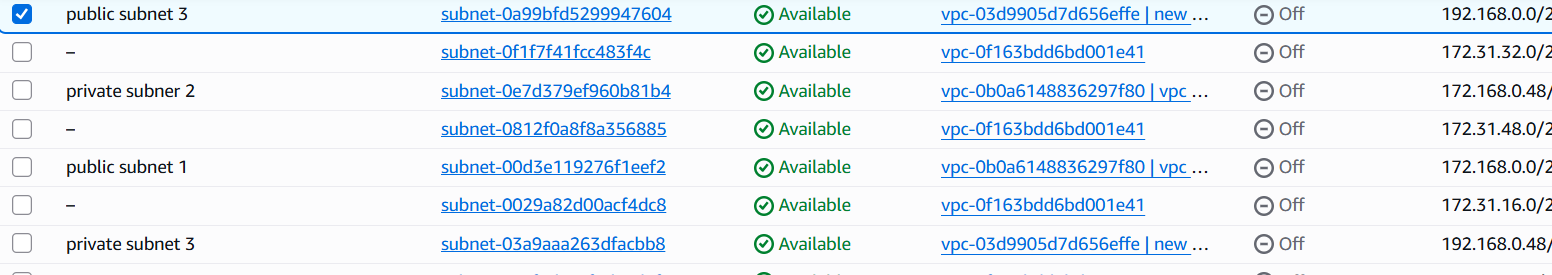


1. Configure NAT gateway in public subnet and connect to private instance.

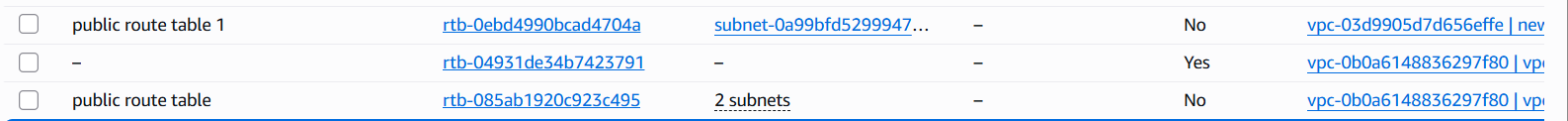
first to create vpc



creating of public subnet and private subnet



crate router tables 2



create internet gateway and attach vpc to it

attach the internet gateway in public subnet route table

create Nat gateway and select public connectivity and attach public subnet to it



generate elastic ip while creating gateway

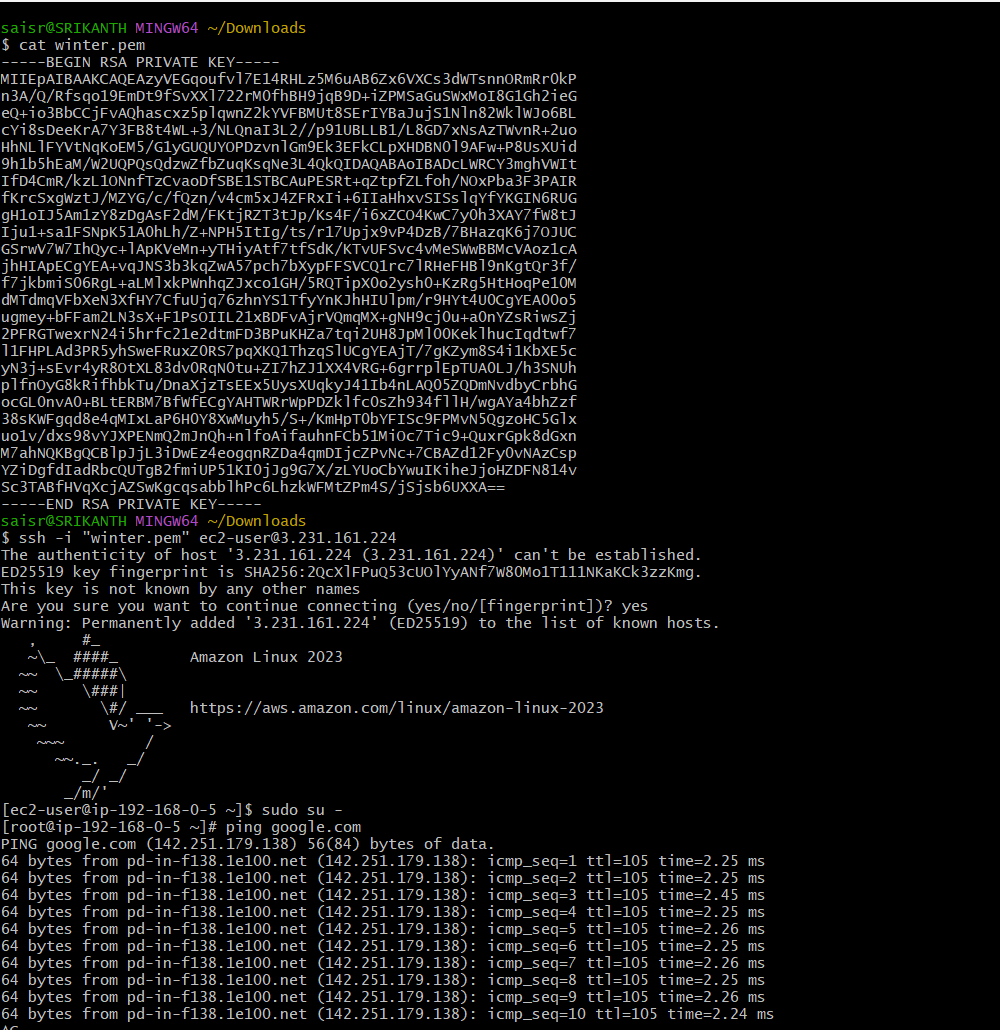
apply internet gateway for public route table

apply Nat gateway for private route table

launch 2 instances for private and public

connect to instance using ssh and enable security group settings

verify the internet connection using ping google.com



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

first do yum install java

cd opt/

wget and download the link and psate it

ls

tar xvf and paste the link

ls

cd apache….

ls

bin webapps conf lib

cd bin/

ls

./startup.sh

tomcat started

cd ..

cd webapps/

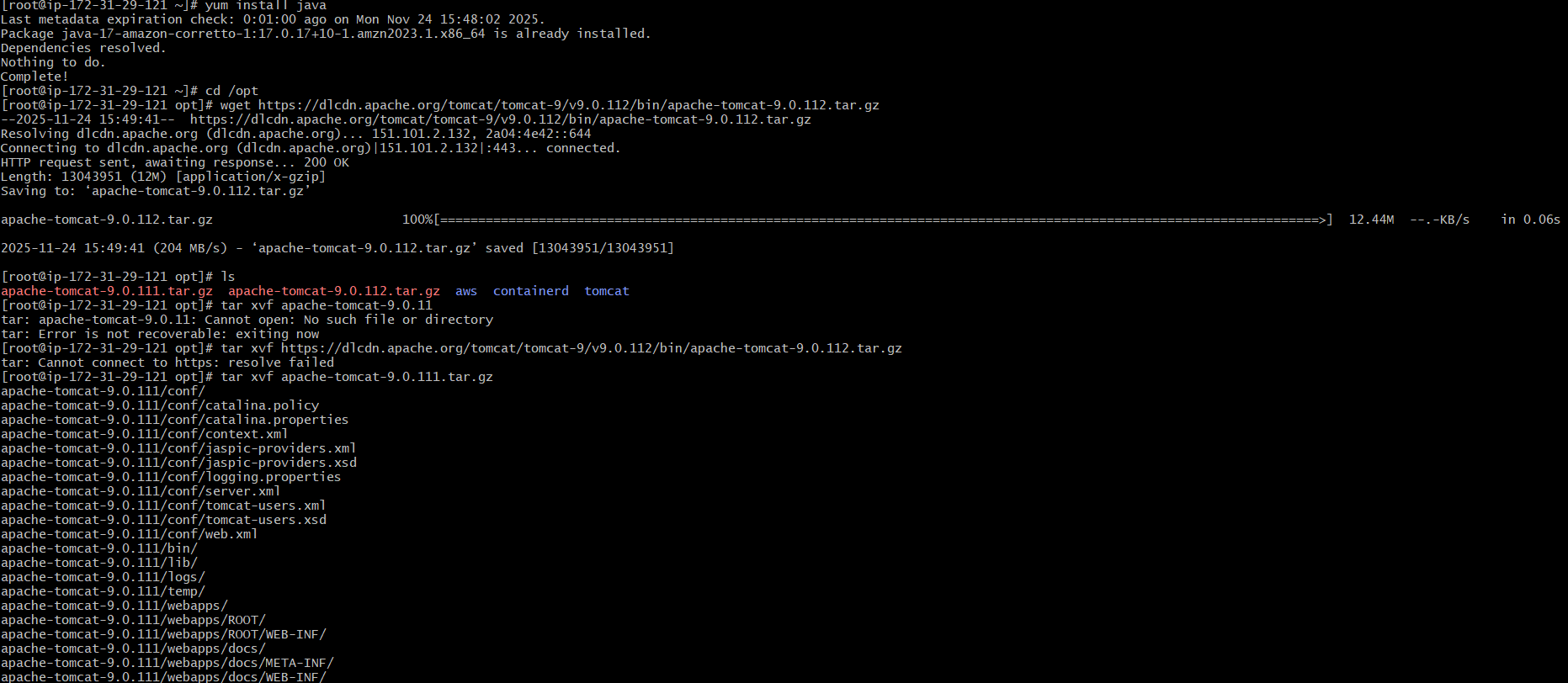
wget and paste the link from browser

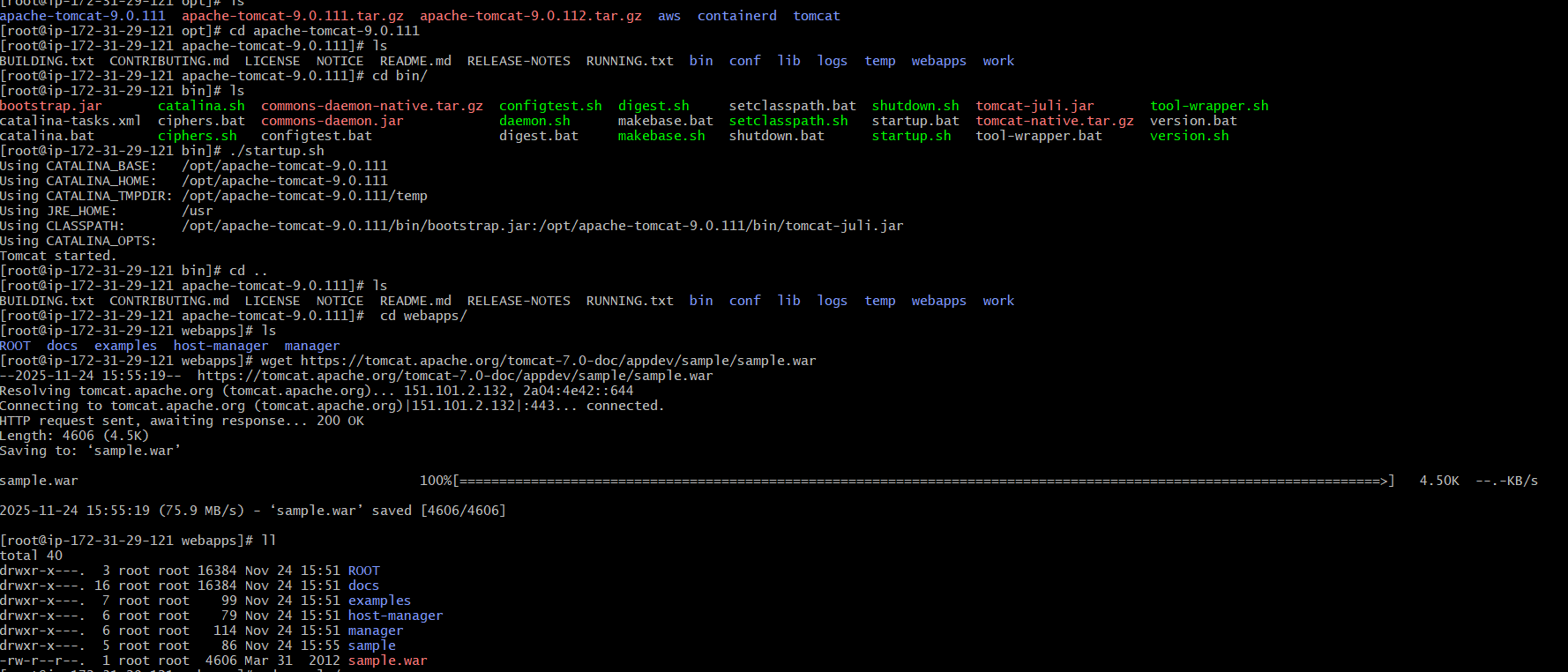
ll

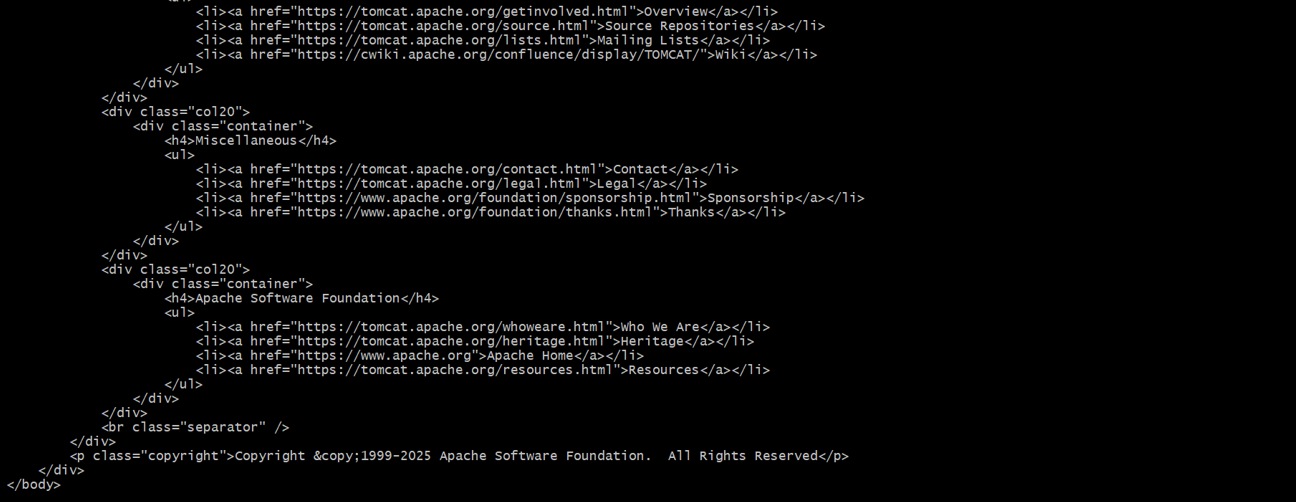
cd sample/

vi index.html

curl <http://privateid:8080>







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

first go to vpc console

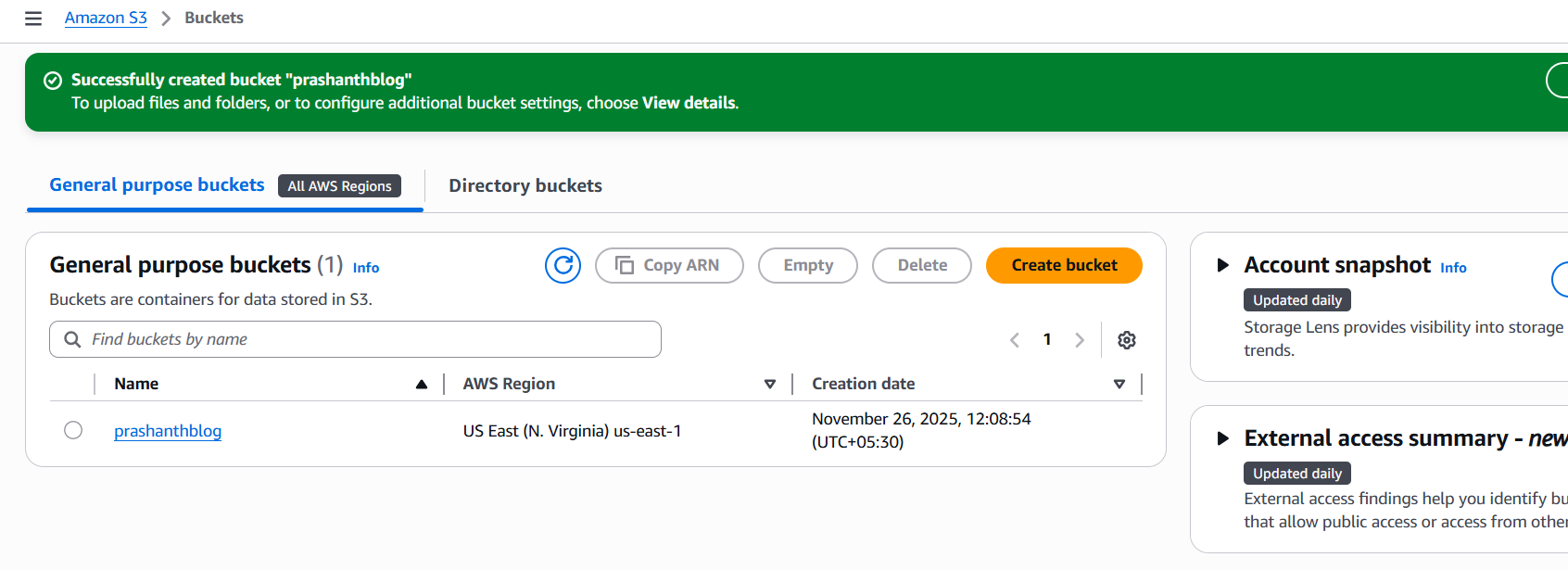
before creating flowlog create bucket in s3

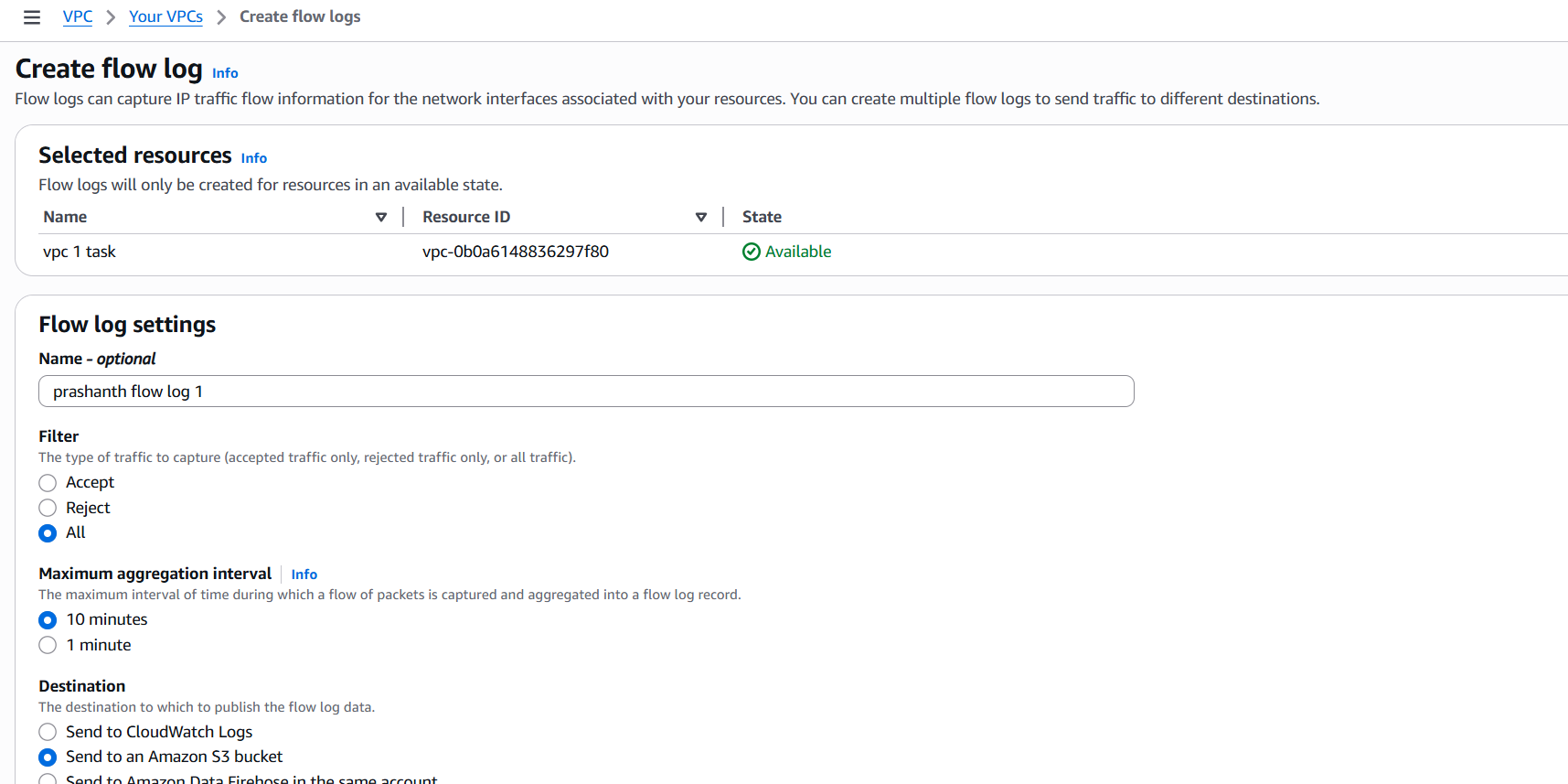
once you create bucket name it will provide you ARN id

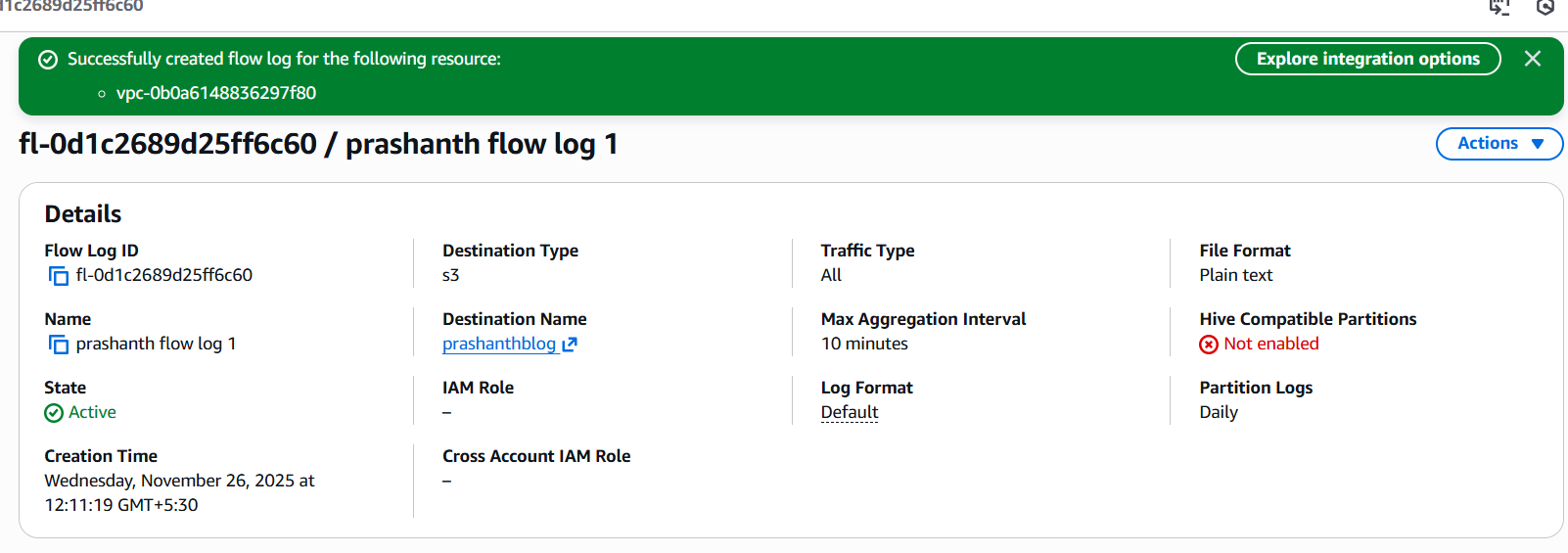
copy the arn and now create flowlog from your vpc and paste it in arn column

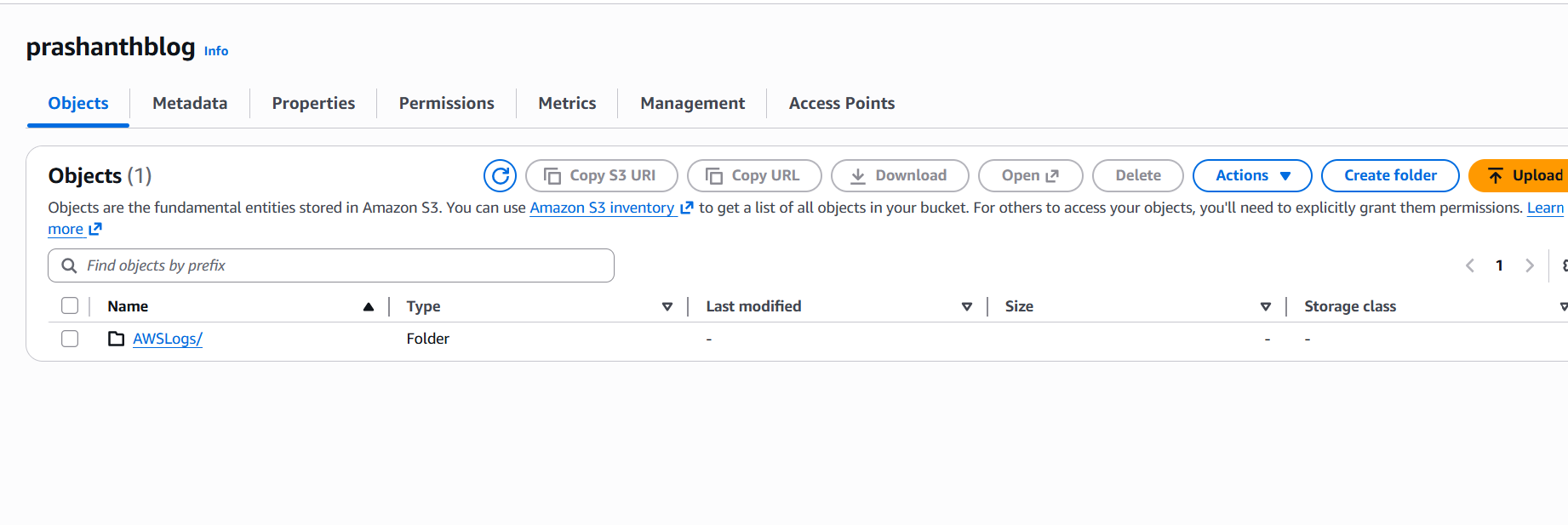
now click on create flowlog

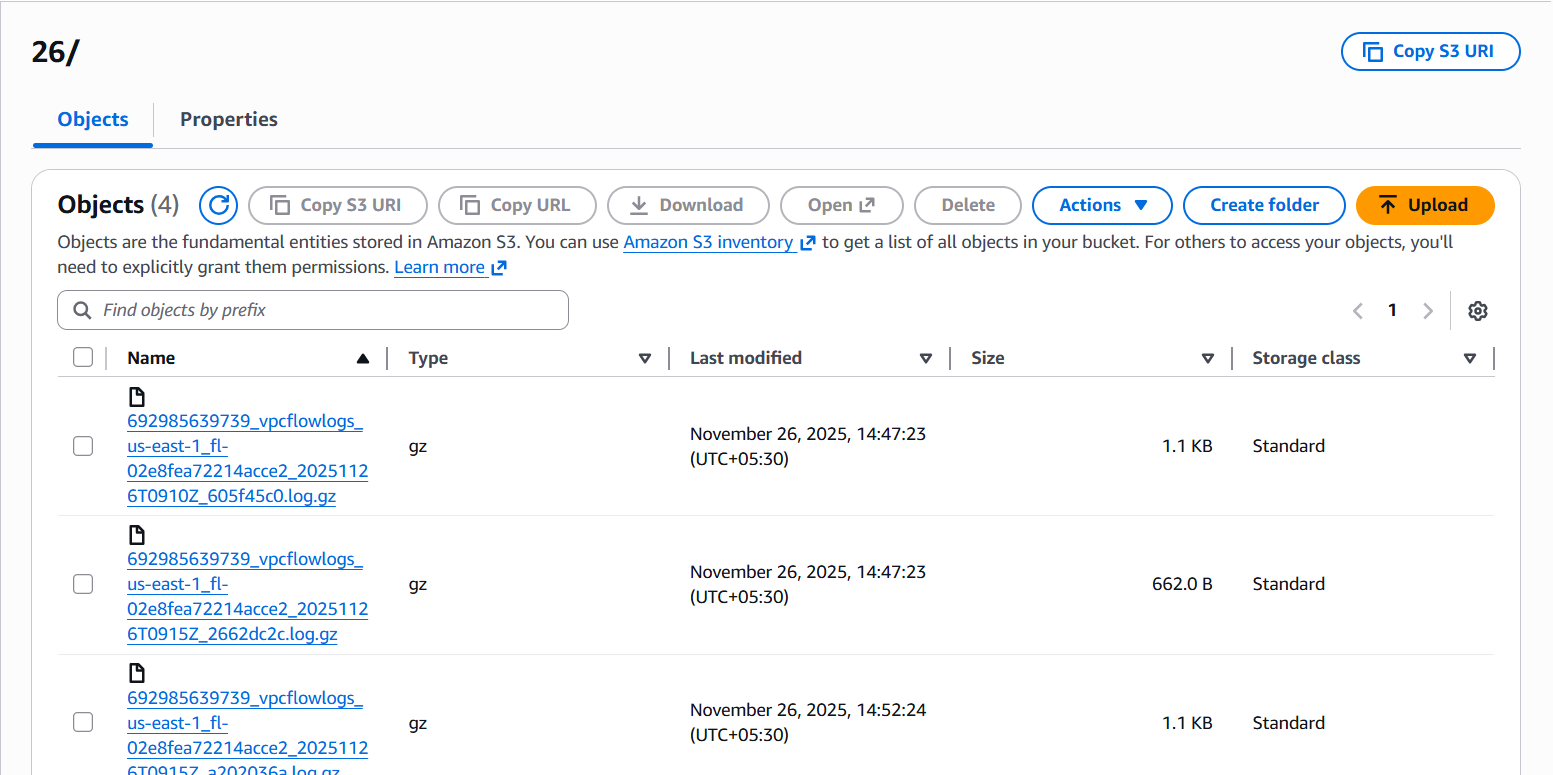
once the flowlog has been created to view the logs go to the buckets and you can see the list











cloudwatch

first we need to create the rule and policies for publishing flowlogs to cloudwatch

use the link <https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-iam-role.html>

got IAM-policies- create the policy

paste the content to specify the permission

permission has been created

now click on roles-enter one role name and paste the trust policy content and next

now come to vpc and create flowlog-select the service role and create

to view go to cloudwatch-loggroups

you cans ee the list of logs

