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

2) Enable DNS Hostname in VPC

3) Enable Auto Assign Public ip in 2 public subnets

4) Add 2 private subnets in private route table

5) Add 2 public subnets in public route table

6) Public route table will have the routes to internet and local

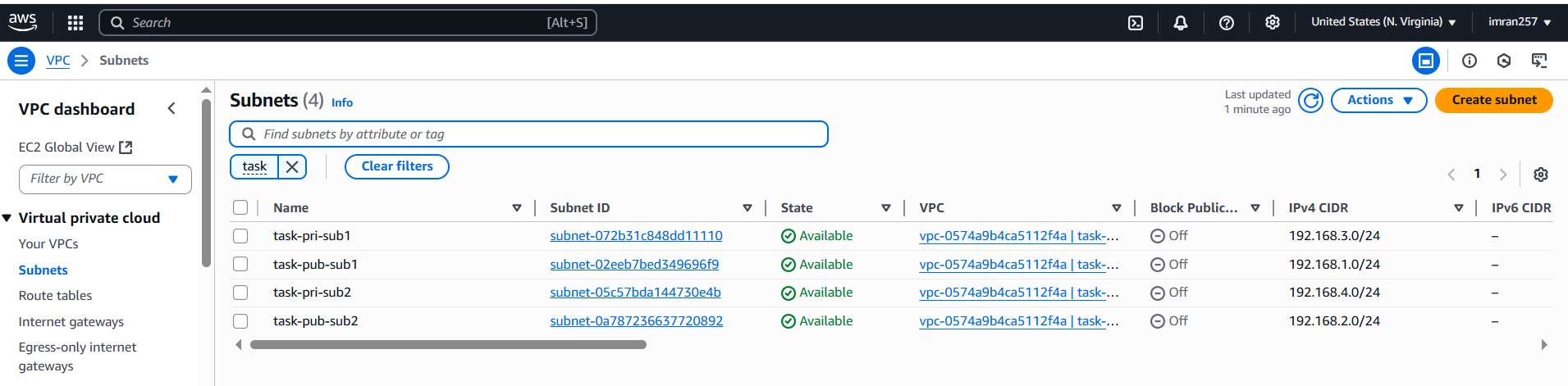
7) Create Ec2 in public subnet with t2micro and install php

8) Configure Nat gateway in public subnet and connect to private Instance

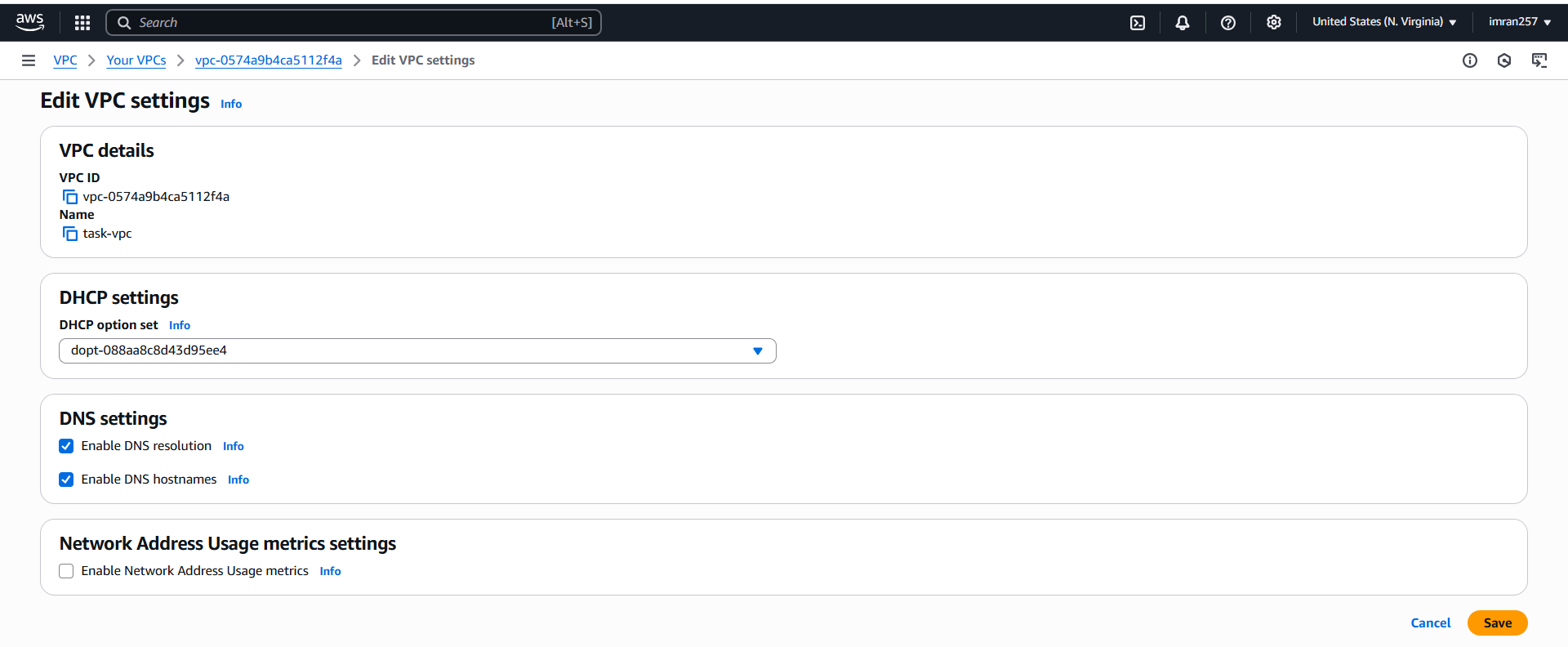
9) Install Apache Tomcat in private ec2 and deploy a sample app.

10) Configure VPC flow logs and store the logs in s3 and CloudWatch.

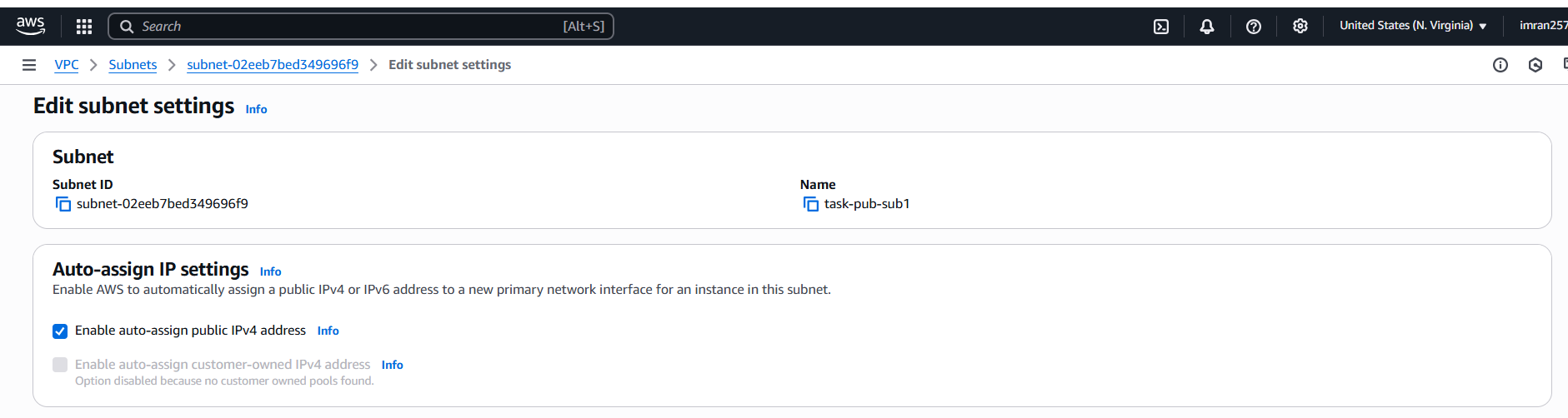
**1) Create VPC with 2 private and 2 public subnets.**

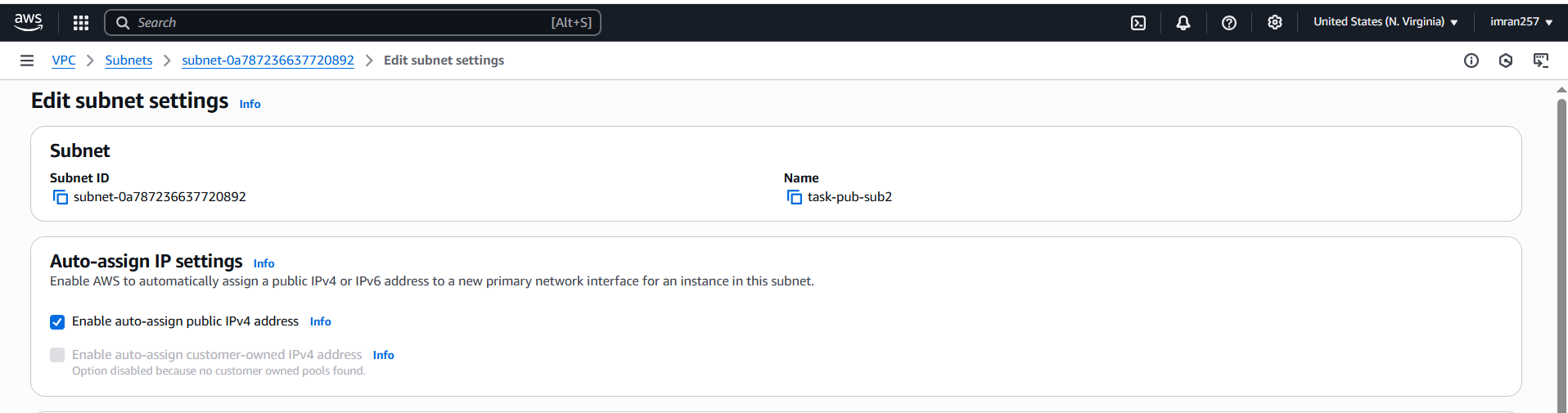
****

**2) Enable DNS Hostname in VPC**

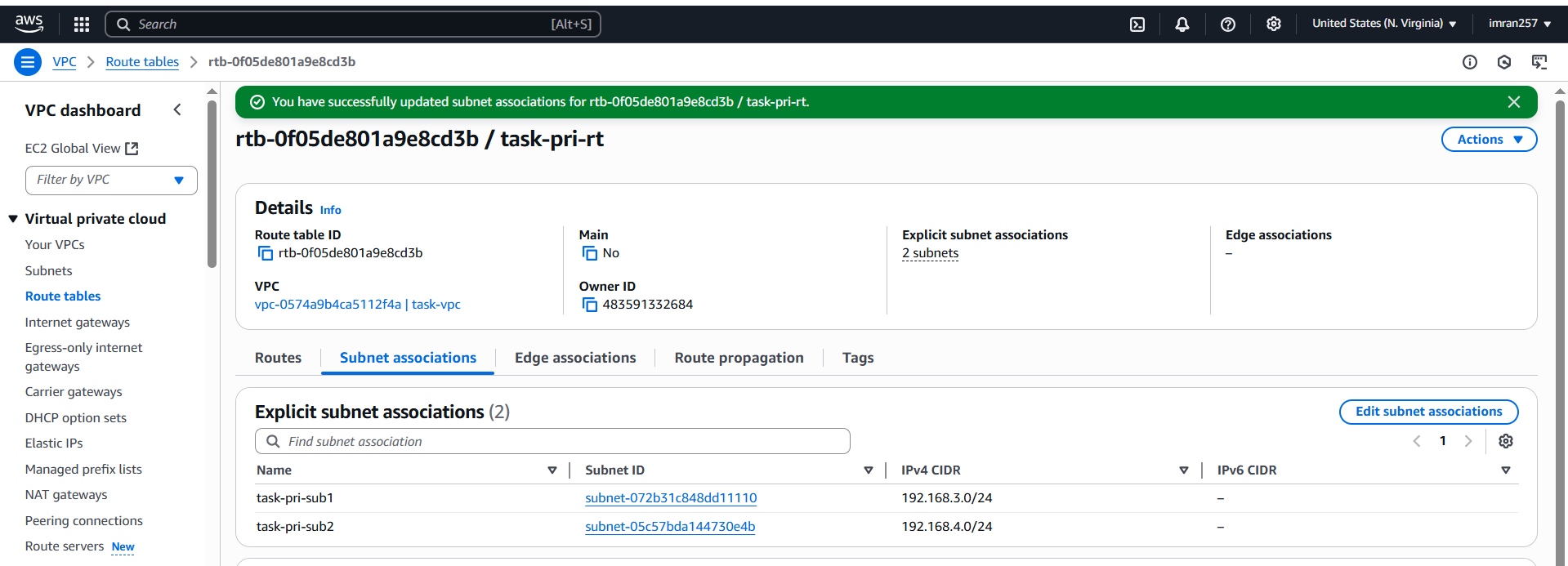
****

**3) Enable Auto Assign Public ip in 2 public subnets**

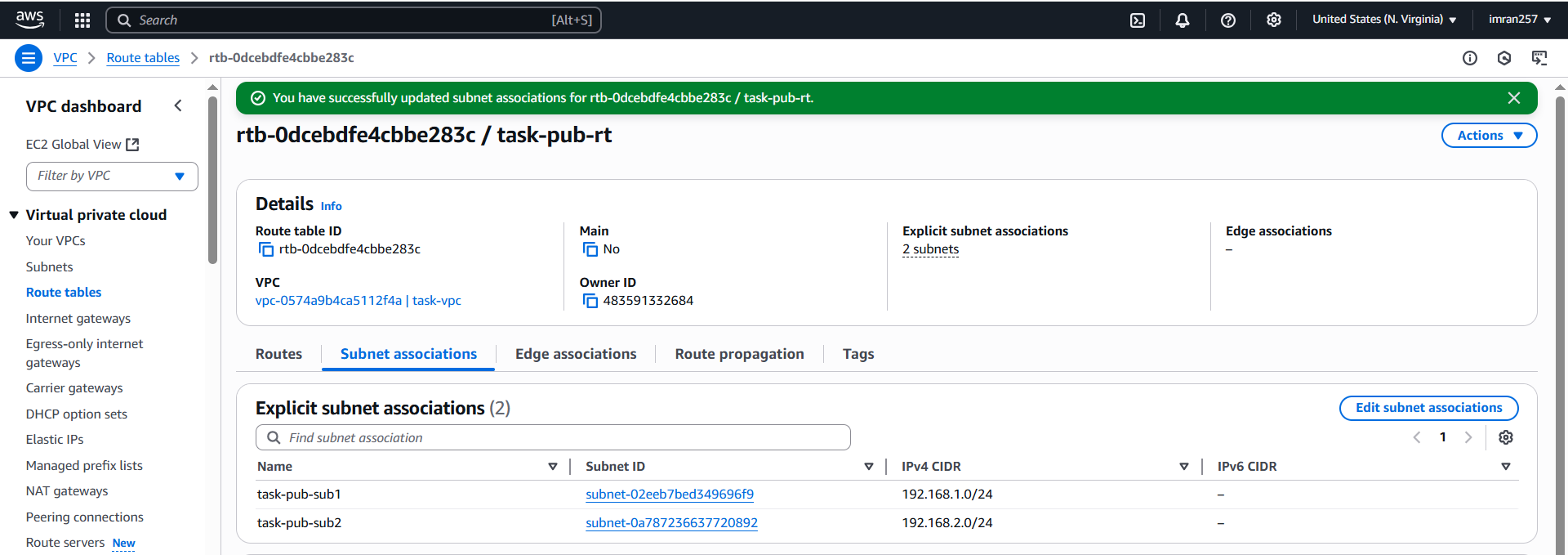
****

****

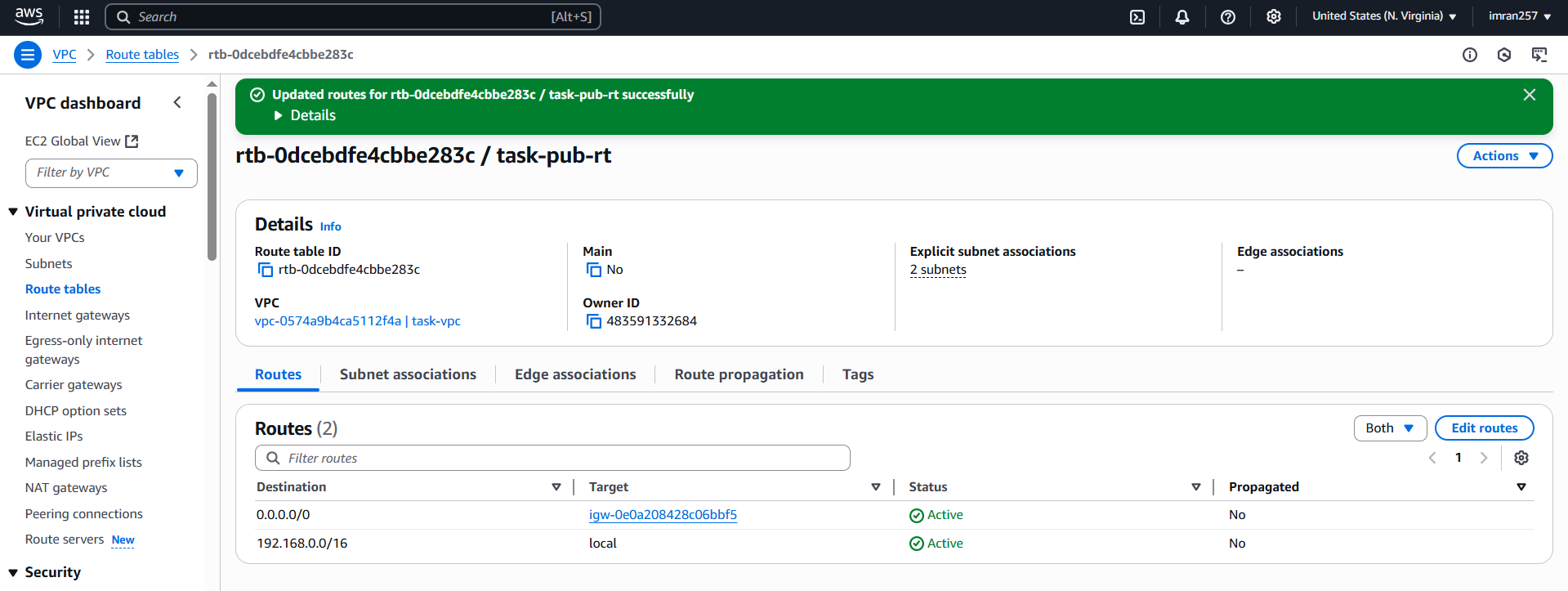
**4) Add 2 private subnets in private route table**

****

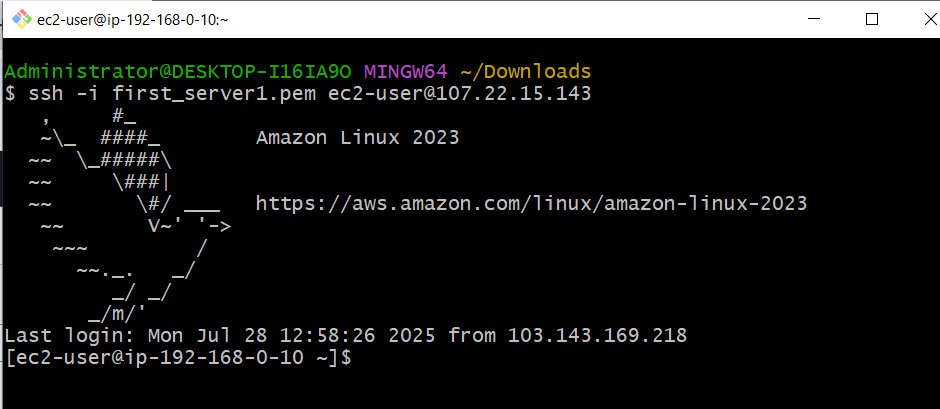
**5) Add 2 public subnets in public route table**

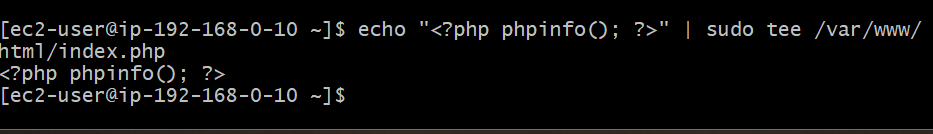
****

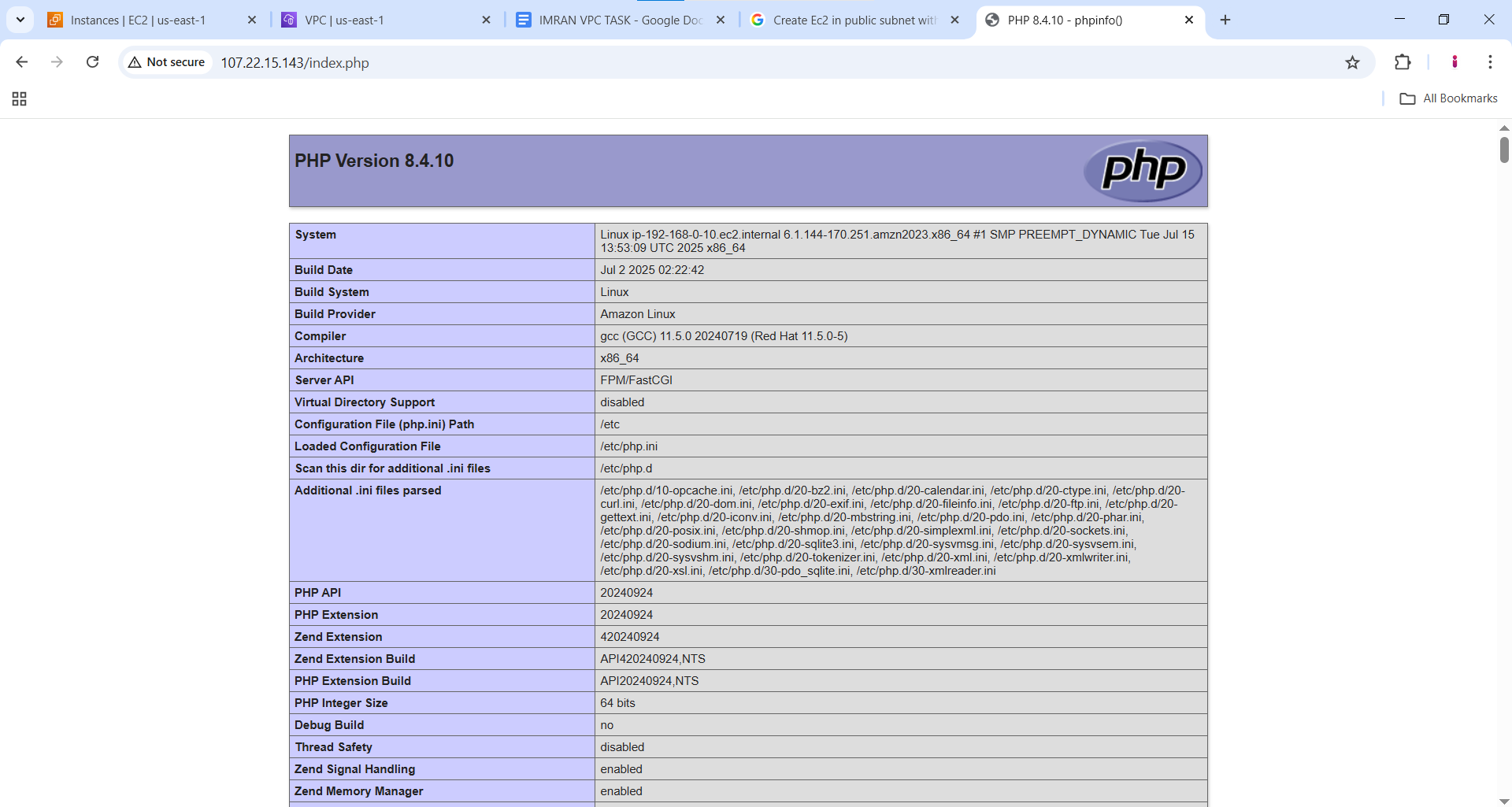
**6) Public route table will have the routes to internet and local**

****

**7) Create Ec2 in public subnet with t2micro and install php**

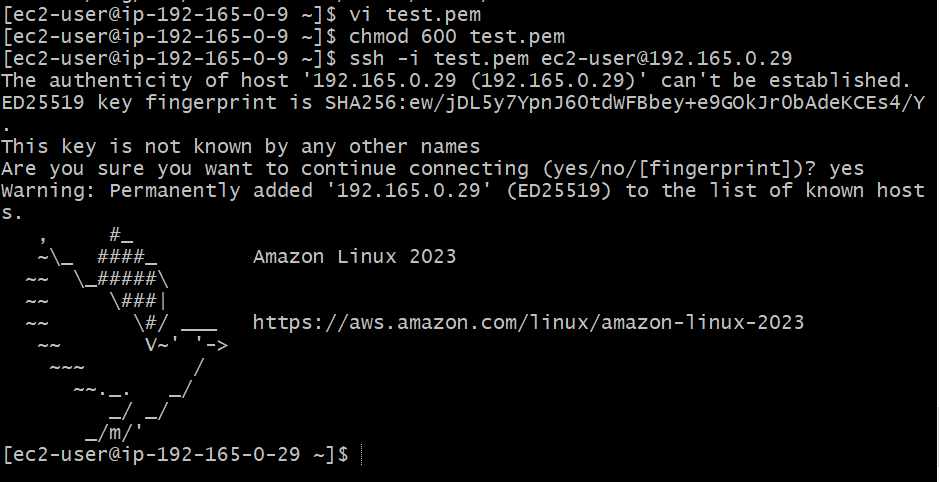
****

****

****

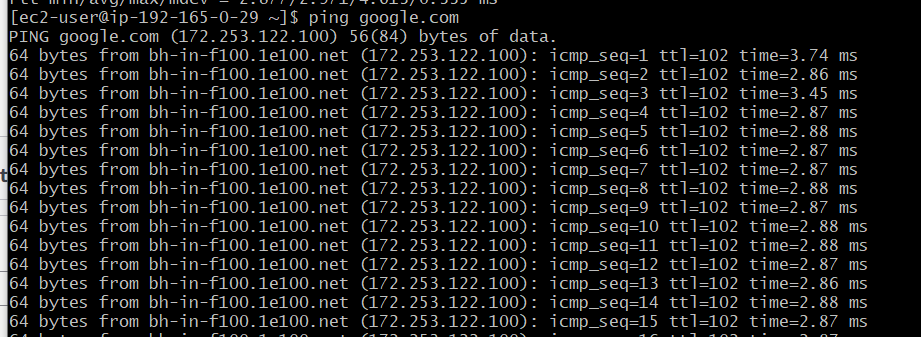
**8) Configure Nat gateway in public subnet and connect to private Instance**

**Step1: From pri instance copied the pem key and create test.pem in pub instance and doing ssh from pub instance using the pri instance private ip.**

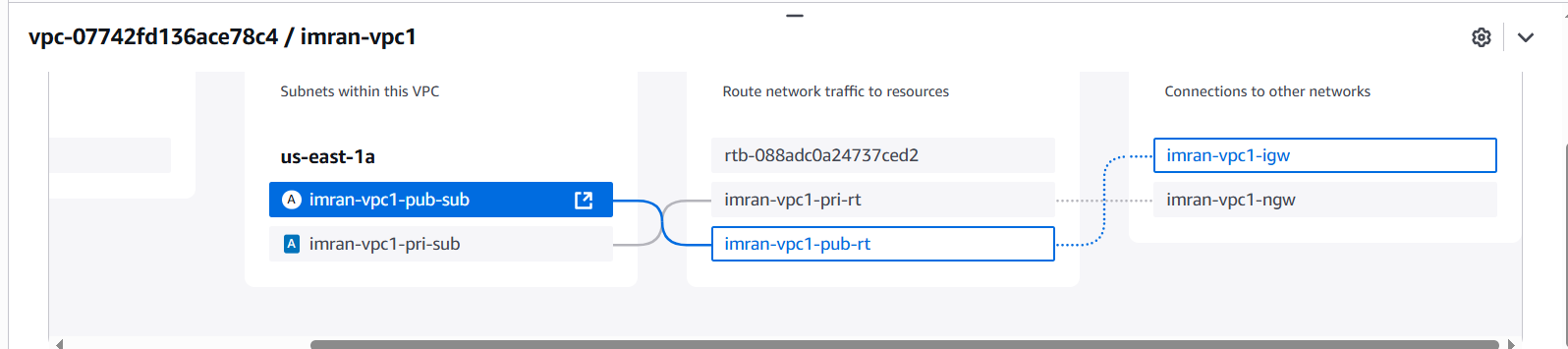
****

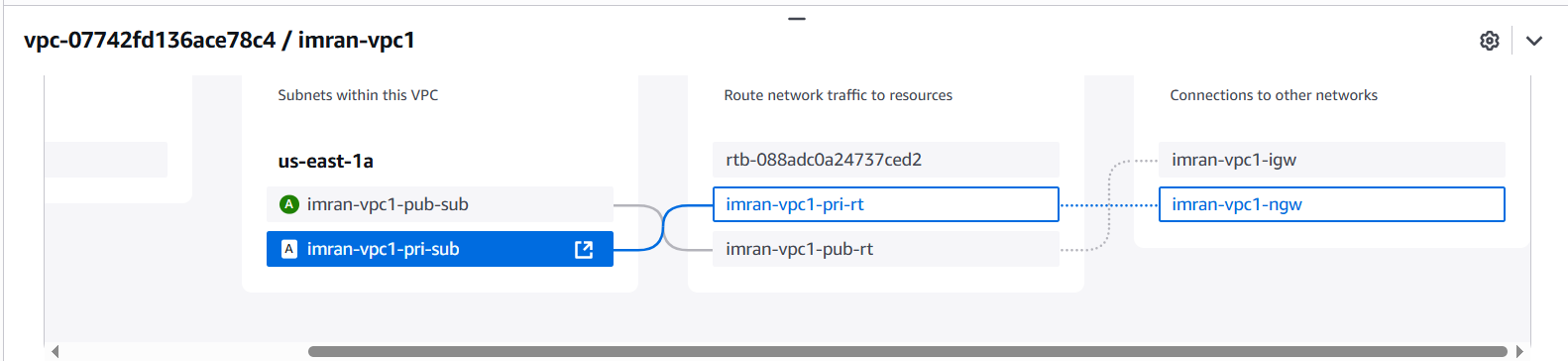
**Step2: create natgateway and allocate elastic ip its , then go to your vpc and go to prive route table and add route in target select nat gateway.**

**Step3: now check internet access for pri instance from pub instance.**

****

**9) Install Apache Tomcat in private ec2 and deploy a sample app.**

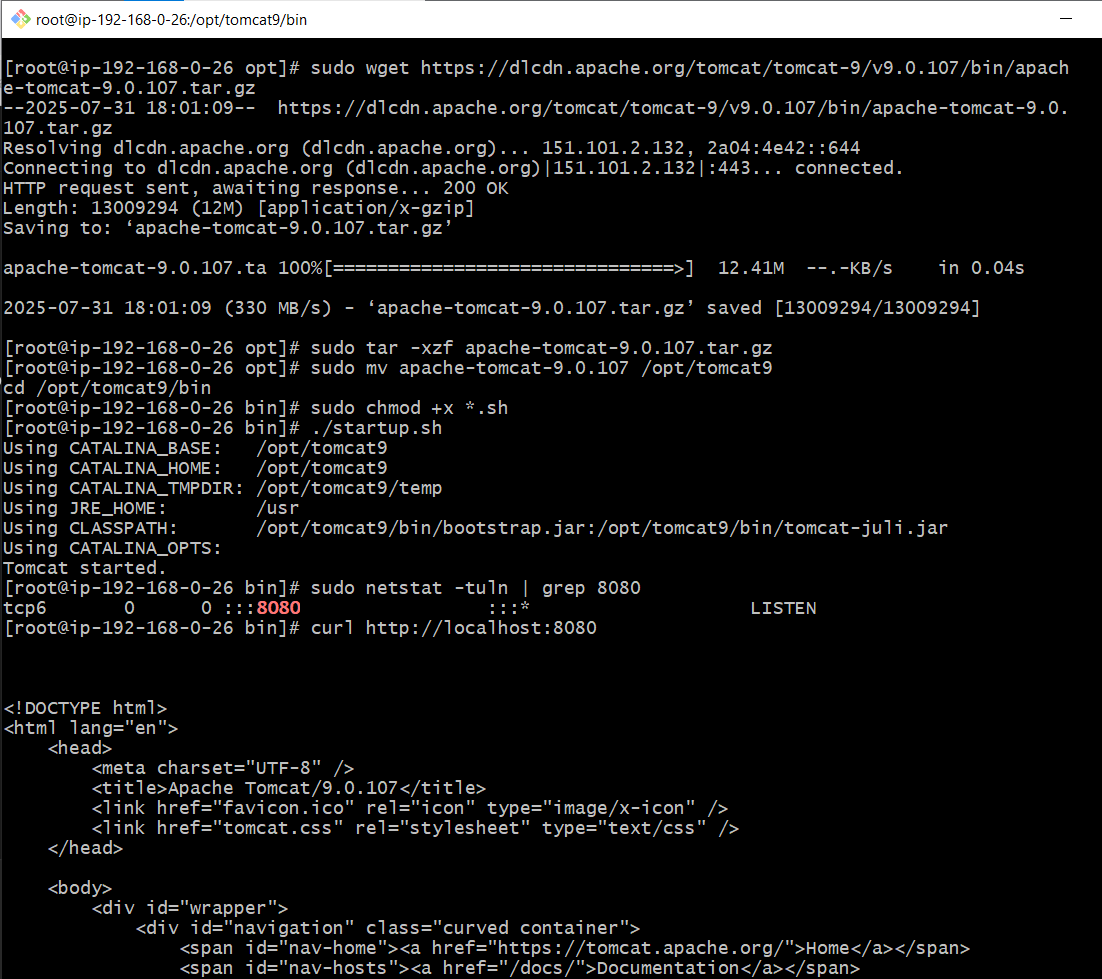
****

****

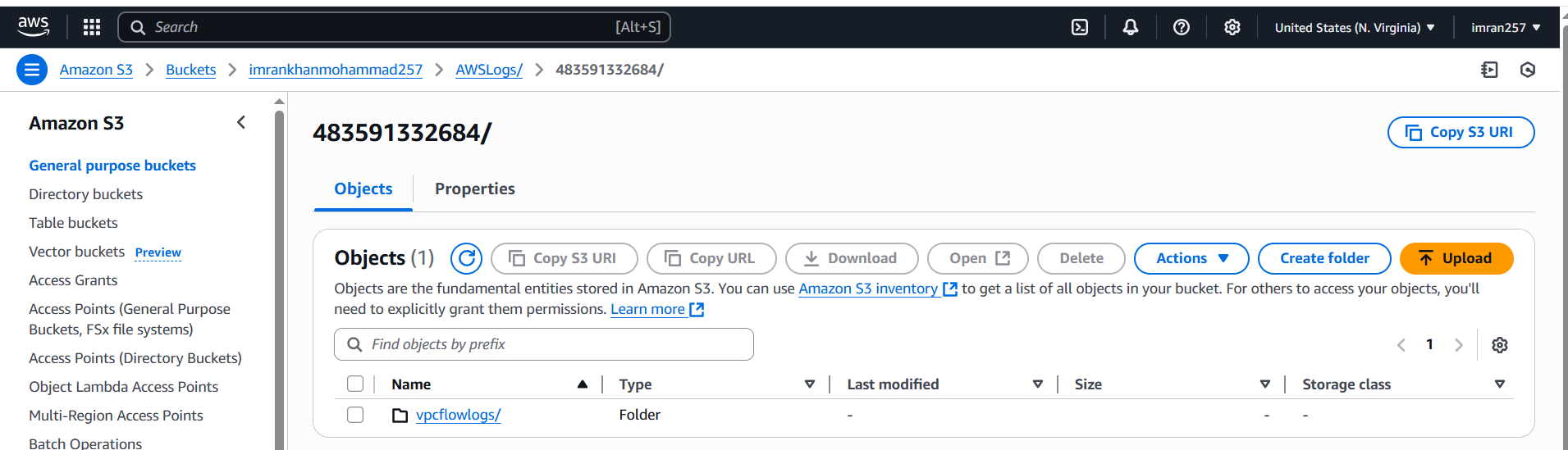
1. **After above setup i created 1 public instance with public subnet (enable public ip) and created 1 private instance with private subnet (disable public ip)with same VPC to both instance.**
2. **I copied the (cat first\_server1.pem from my local machine)**
3. **I created pub instance as jump or bastion server, i ssh to my public ec2 and came to root and create test.pem and paste the pem key.**
4. **Give permission chmod 600 test.pem**
5. **Now ssh -i test.pem ec2-user@(private ip of private ec2)and go to root.**
6. **Check internet access ping** [**google.com**](http://google.com)
7. ****
8. **Cd /opt**
9. **Sudo wget** [**https://dlcdn.apache.org/tomcat/tomcat-9/v9.0.107/bin/apache-tomcat-9.0.107.tar.gz**](https://dlcdn.apache.org/tomcat/tomcat-9/v9.0.107/bin/apache-tomcat-9.0.107.tar.gz)

**sudo tar -xzf** [**apache-tomcat-9.0.107.tar.gz**](http://apache-tomcat-9.0.107.tar.gz)

1. **sudo mv apache-tomcat-9.0.107 /opt/tomcat9**
2. **cd /opt/tomcat9/bin**
3. **sudo chmod +x \*.sh**
4. **./**[**startup.sh**](http://startup.sh) **-> can see output tomcat started**
5. **sudo netstat -tuln | grep 8080**
6. **curl http://localhost:8080**

****

**10) Configure VPC flow logs and store the logs in s3 and CloudWatch.**

****

1. **Created IAM role and with choosing “custom trust policy”**

**With below trust policy pasted in the user data.**

**{**

**"Version": "2012-10-17",**

**"Statement": [**

**{**

**"Effect": "Allow",**

**"Principal": {**

**"Service": "vpc-flow-logs.amazonaws.com"**

**},**

**"Action": "sts:AssumeRole"**

**}**

**]**

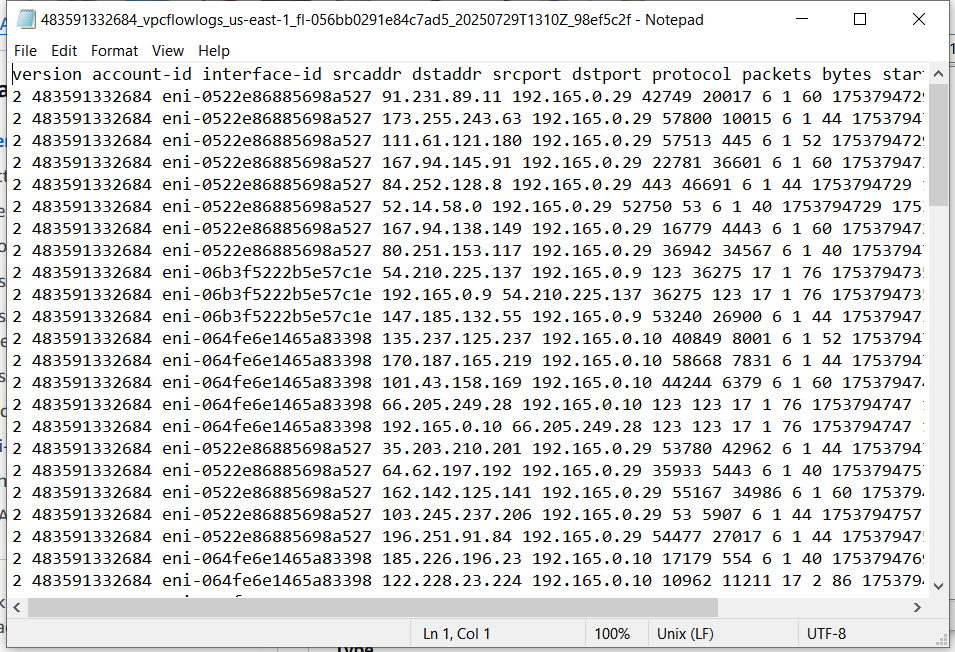
**}**

**Taken permissions**

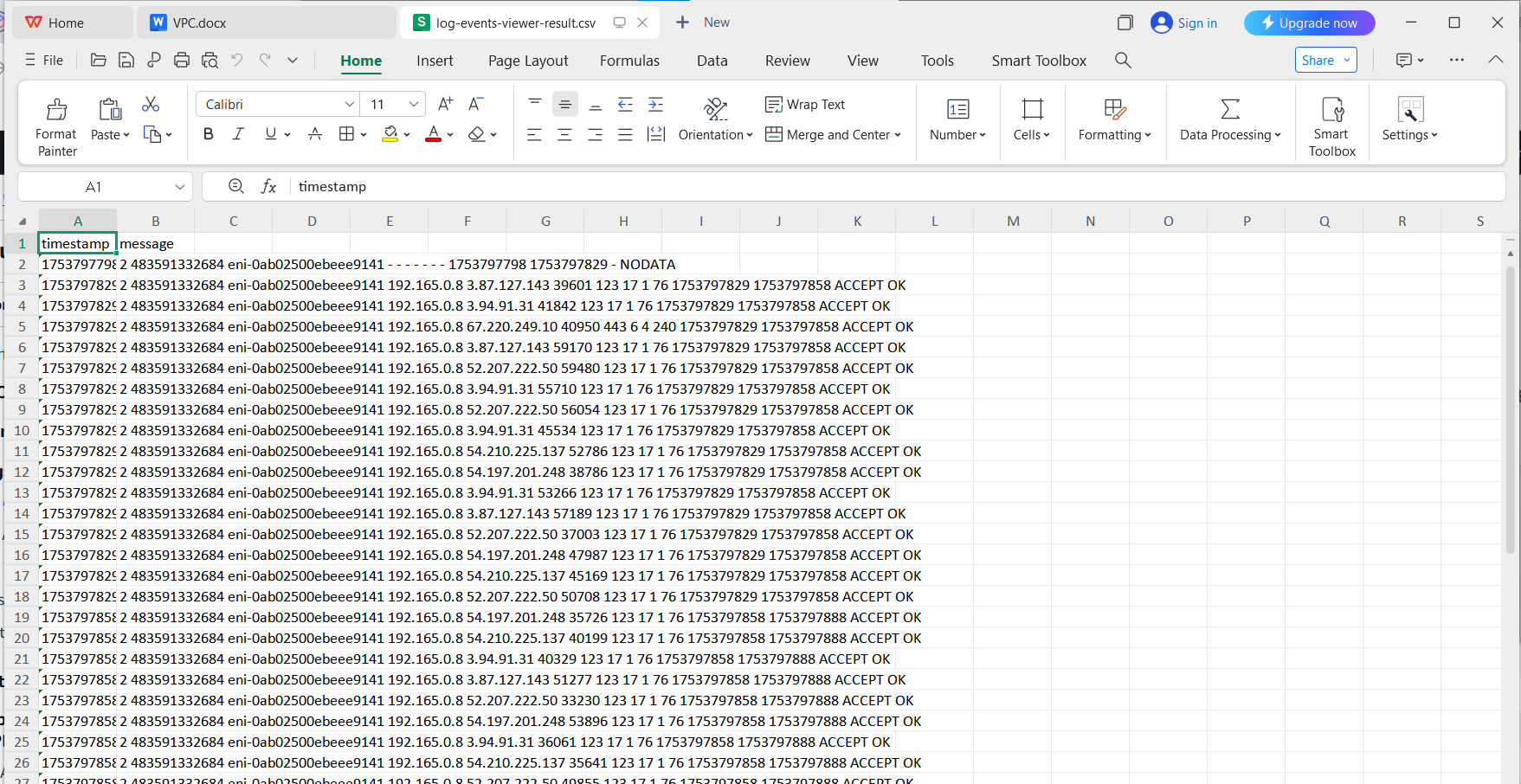
**AmazonS3FullAccess ,CloudWatchLogsFullAccess**

**Then created role.**

**Vpc flow logs stored in S3 and downloaded in my laptop.**

****

**Cloud watch logs downloaded in my laptop.**

****