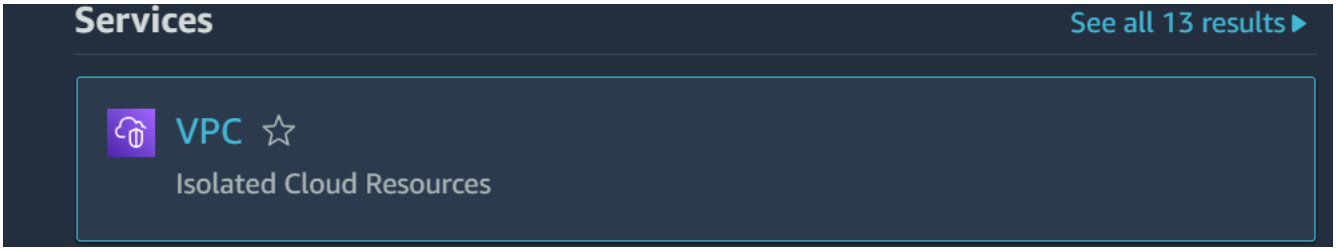
ASSIGNMENT-14

Cloud Computing Practical Assignment No: 14

Implementation of VPC using AWS.

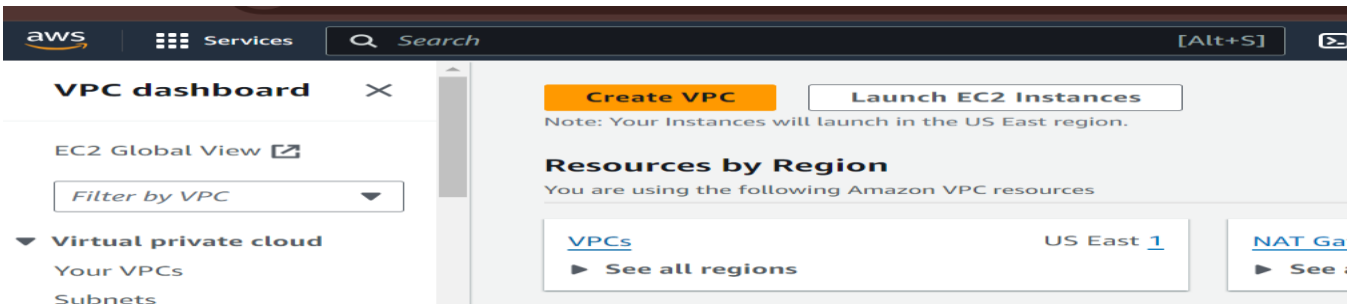
Task 1: Create Your VPC

1. Go to the VPC console (search for "VPC" in the search bar).

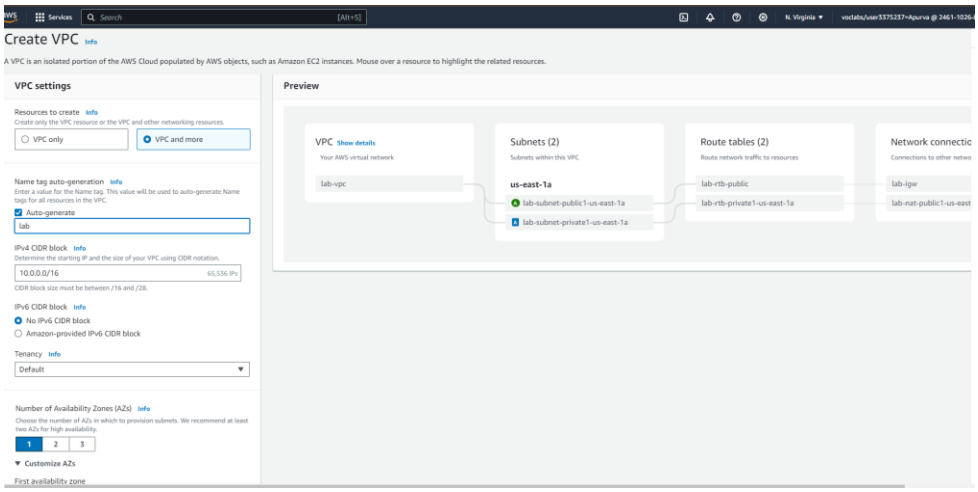


2. Verify the region is N. Virginia (us-east-1).

3. Choose "Create VPC".

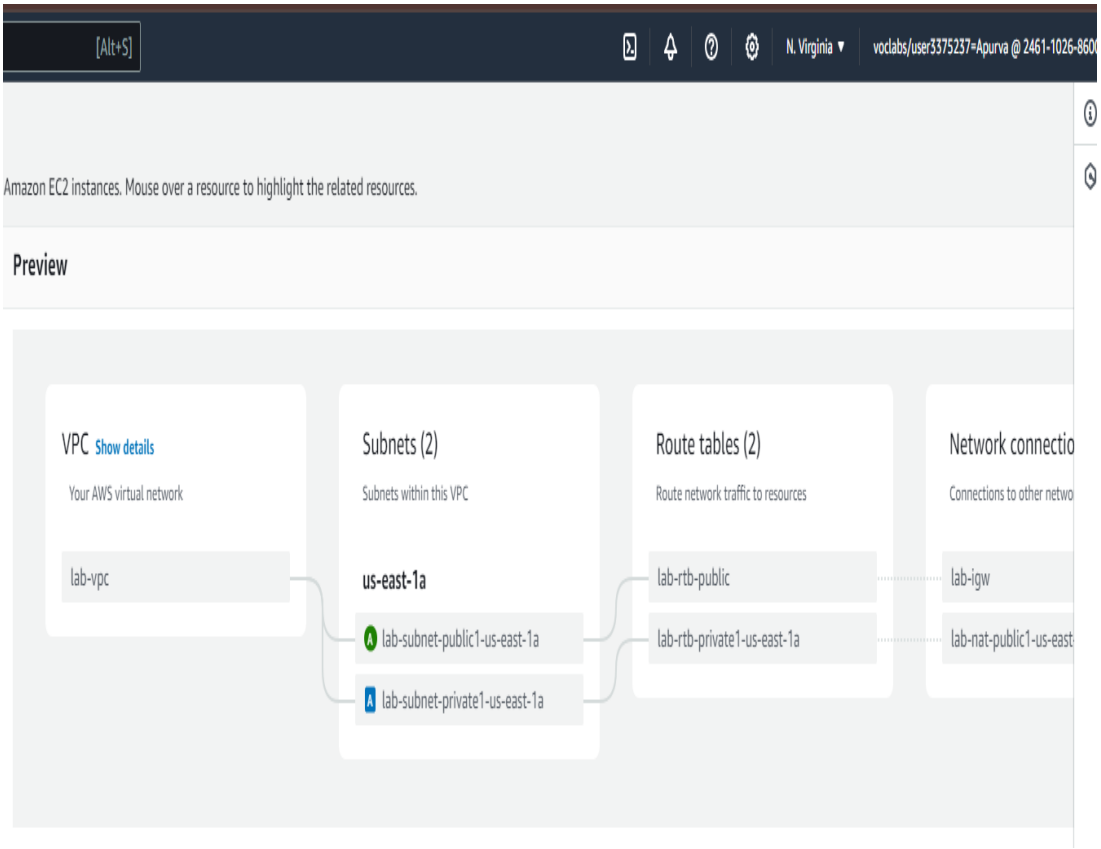


4. Under VPC settings:
   - Keep "Auto-generate" selected for Name tag, but change the value to "lab".
   - Keep IPv4 CIDR block set to 10.0.0.0/16.
   - Choose 1 for Number of Availability Zones.

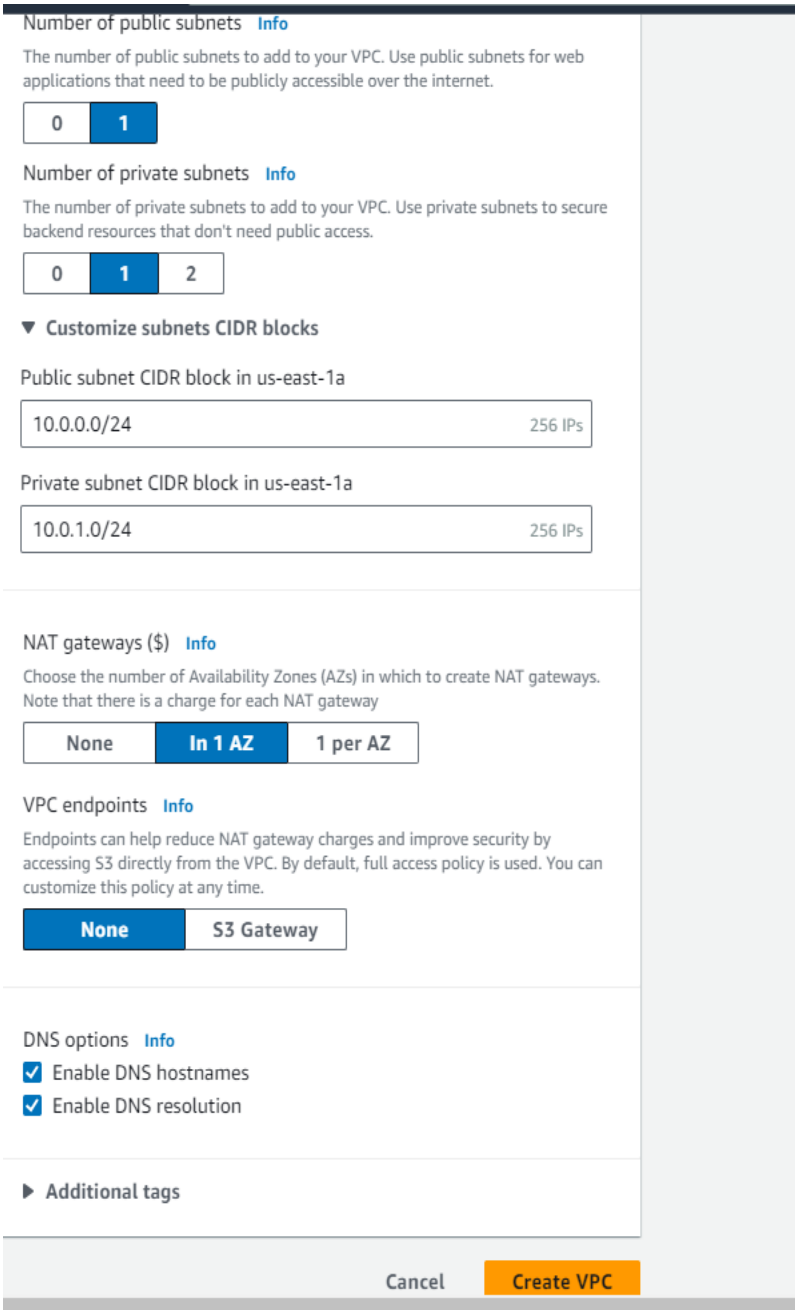


   - Keep settings for Number of public subnets (1) and Number of private subnets (1).
   - Expand "Customize subnets CIDR blocks" and change:

        - Public subnet CIDR block to 10.0.0.0/24
        - Private subnet CIDR block to 10.0.1.0/24
    - Set NAT gateways to "In 1 AZ".
    - Keep VPC endpoints set to "None".
5. Review the settings in the Preview panel.



6. Click "Create VPC".

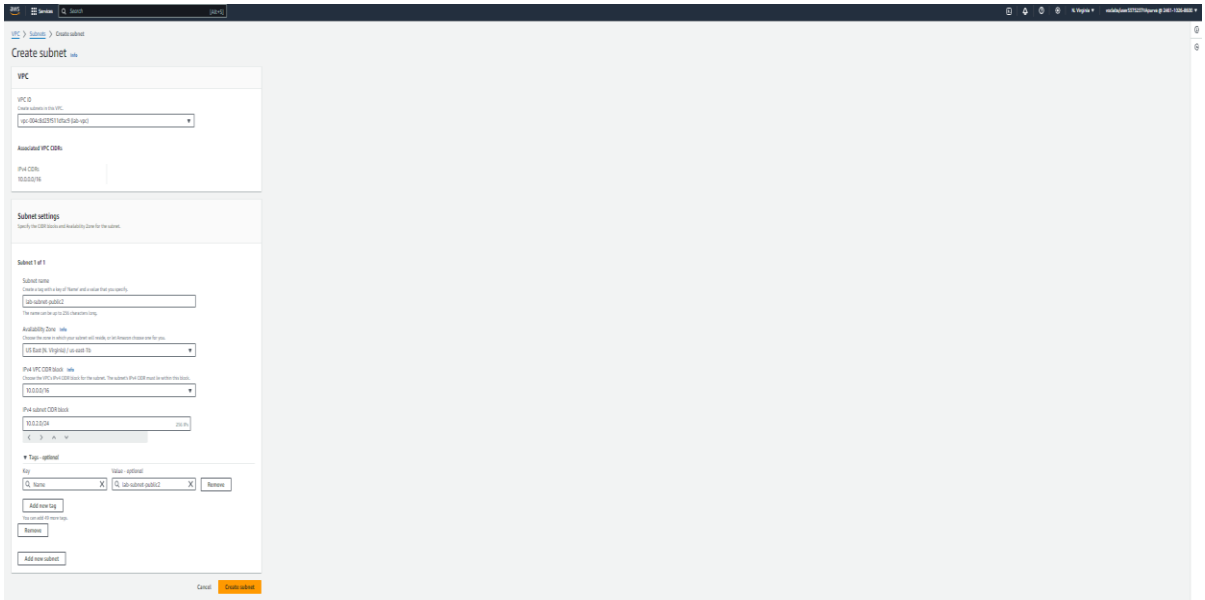


7. Wait for the VPC resources to be created (including the NAT Gateway).

8. Once complete, choose "View VPC".

Task 2: Create Additional Subnets

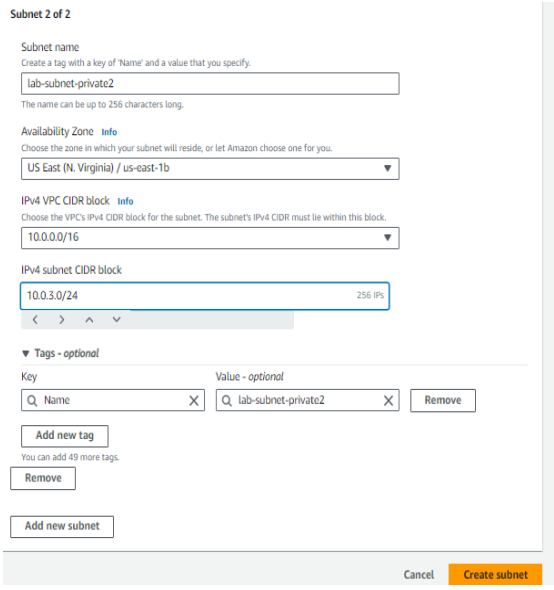
1. Go to the Subnets section in the VPC console.
2. Create a second public subnet with:
   - VPC ID: lab-vpc
   - Subnet name: lab-subnet-public2
   - Availability Zone: Select the second zone (e.g., us-east-1b)
   - IPv4 CIDR block: 10.0.2.0/24



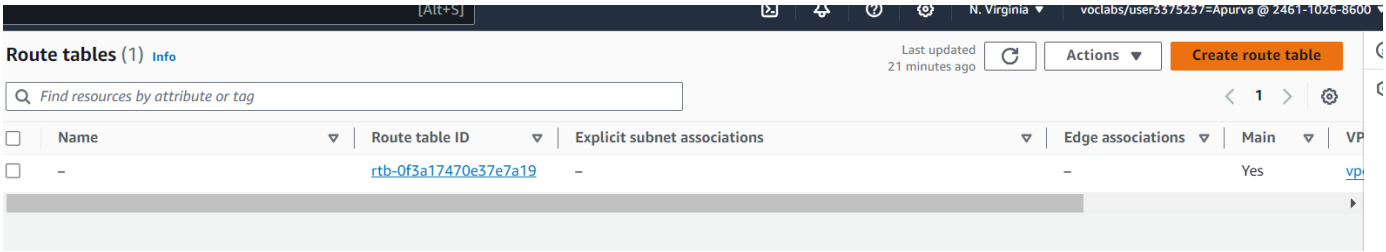
3. Create a second private subnet with:
   - VPC ID: lab-vpc

- Subnet name: lab-subnet-private2
- Availability Zone: Select the second zone (e.g., us-east-1b)
- IPv4 CIDR block: 10.0.3.0/24

4. Configure the new private subnet to route internet traffic to the NAT Gateway (explained in the full instructions).



Go to the Route tables section in the VPC console.



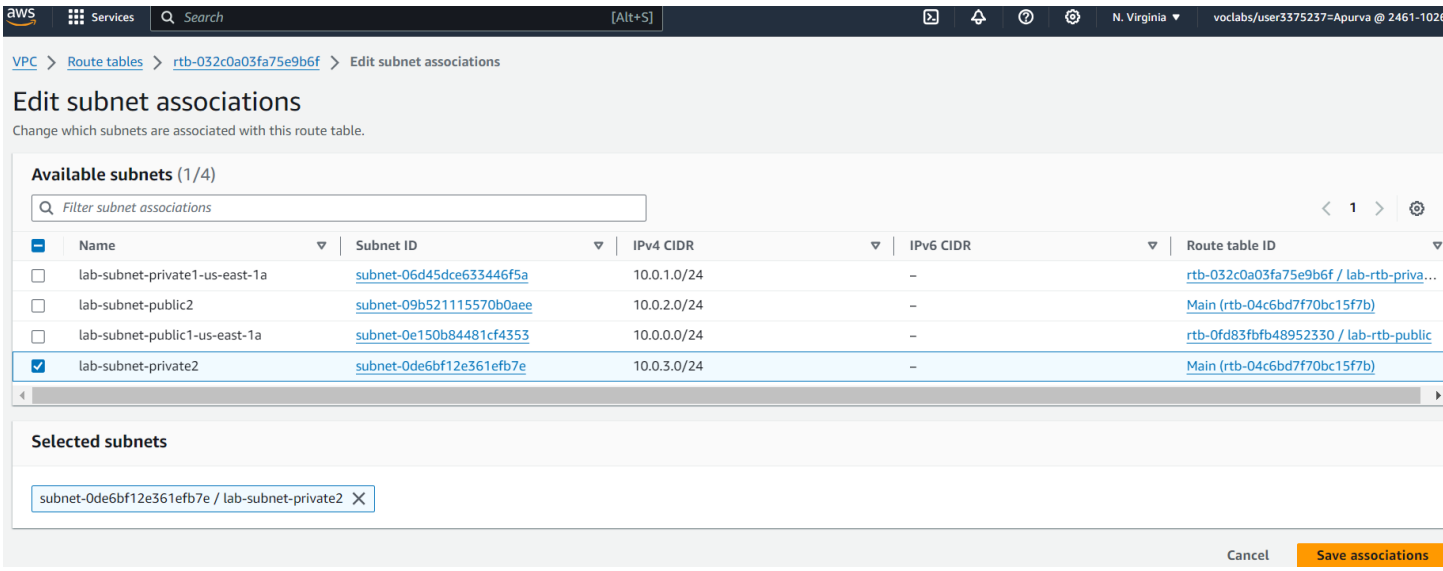
Select the lab-rtb-private1-us-east-1a route table.

In the Routes tab, verify that the destination 0.0.0.0/0 is set to Target nat-xxxxxxxx. This means that traffic destined for the internet will be sent to the NAT Gateway.

Go to the Subnet associations tab.

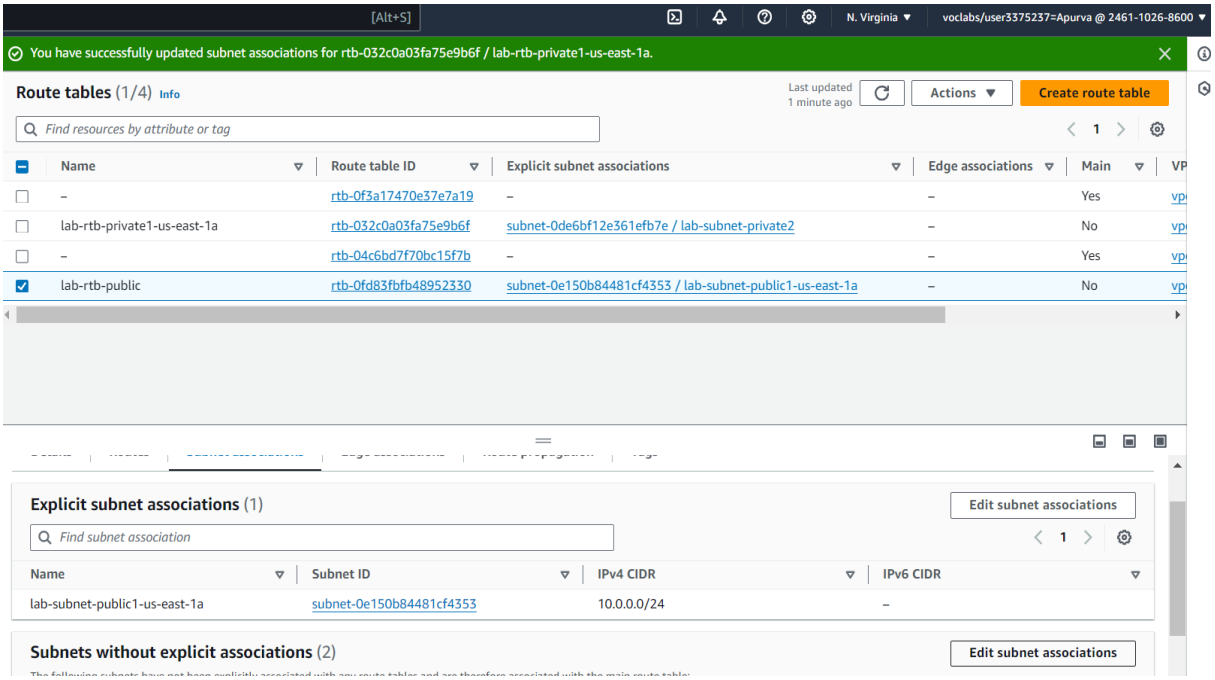
In the Explicit subnet associations panel, choose Edit subnet associations.

Select lab-subnet-private2 in addition to lab-subnet-private1-us-east-1a.



Click Save associations.

Select the lab-rtb-public route table (and deselect any other subnets).



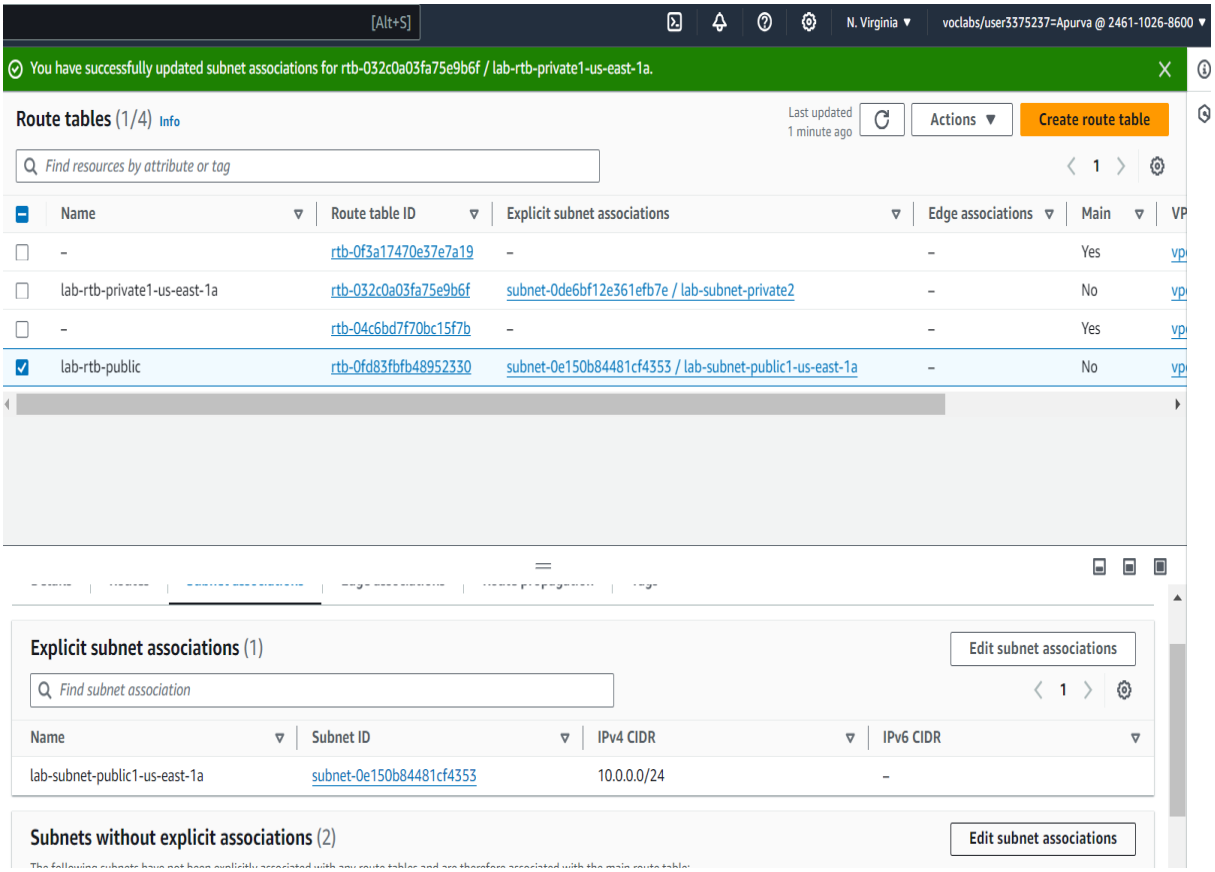
In the Routes tab, verify that the destination 0.0.0.0/0 is set to Target igw-xxxxxxxx, which is an Internet Gateway.

Go to the Subnet associations tab.

In the Explicit subnet associations area, choose Edit subnet associations.

Select lab-subnet-public2 in addition to lab-subnet-public1-us-east-1a.

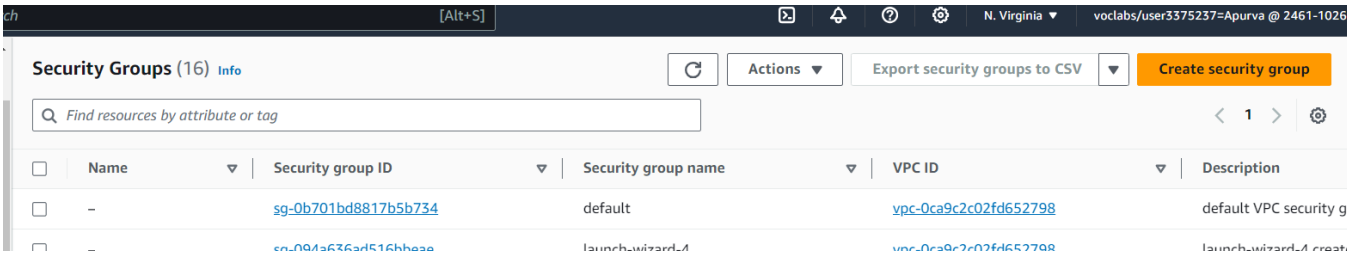
Click Save associations.



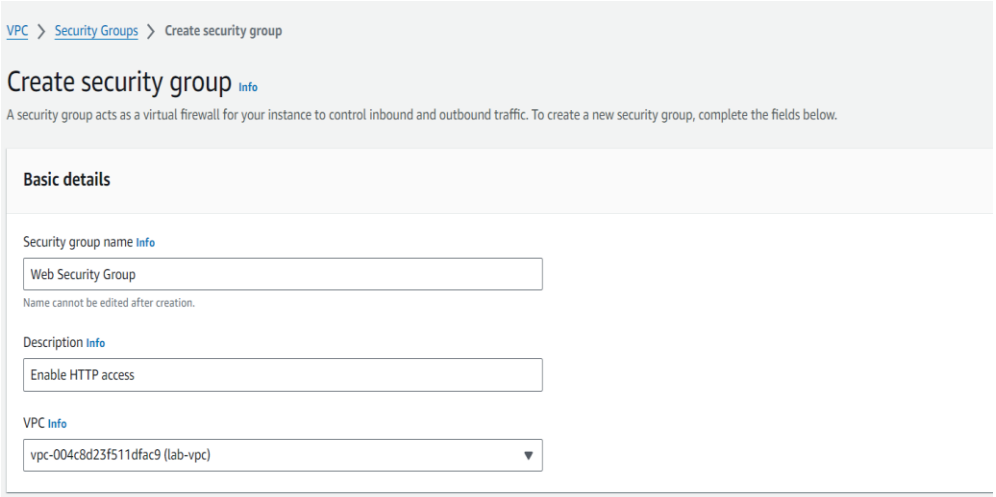
These steps will configure the route tables for the newly created subnets, ensuring that private subnet traffic is routed through the NAT Gateway and public subnet traffic is routed directly to the Internet Gateway.

Task 3: Create a VPC Security Group

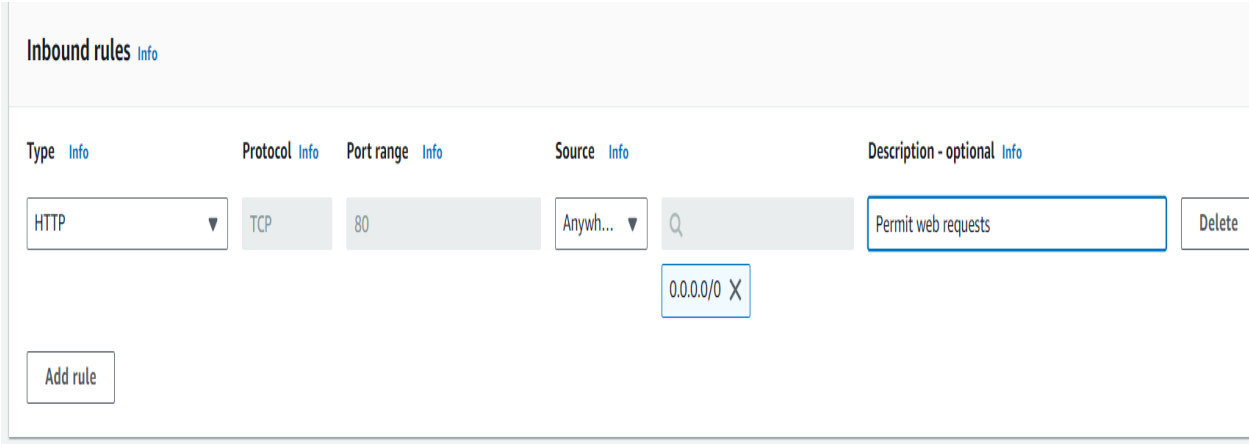
1. Go to the Security groups section in the VPC console.



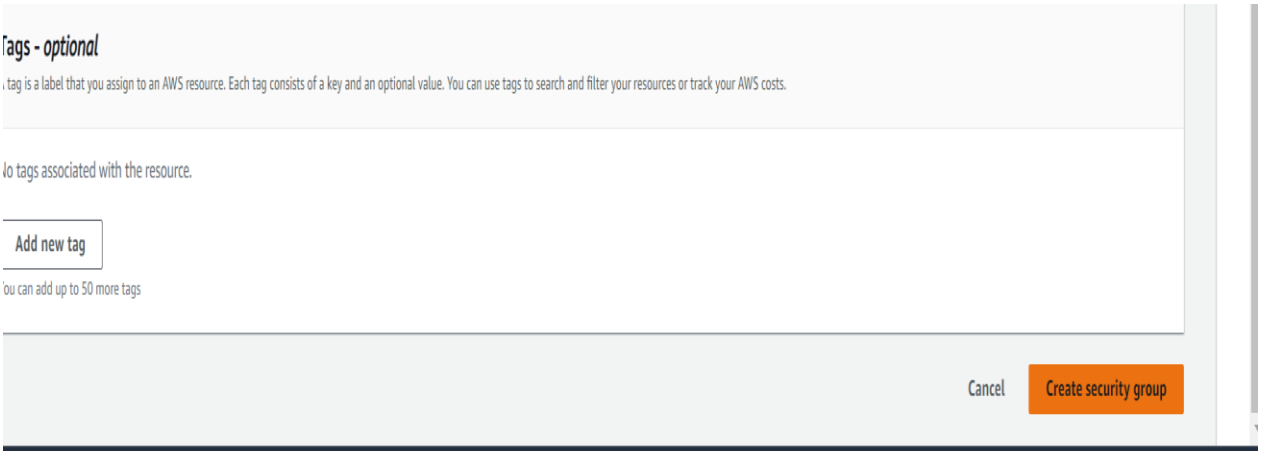
2. Create a security group with:
   - Security group name: Web Security Group
   - Description: Enable HTTP access
   - VPC: Choose lab-vpc



3. Add an inbound rule:
   - Type: HTTP
   - Source: Anywhere-IPv4
   - Description: Permit web requests

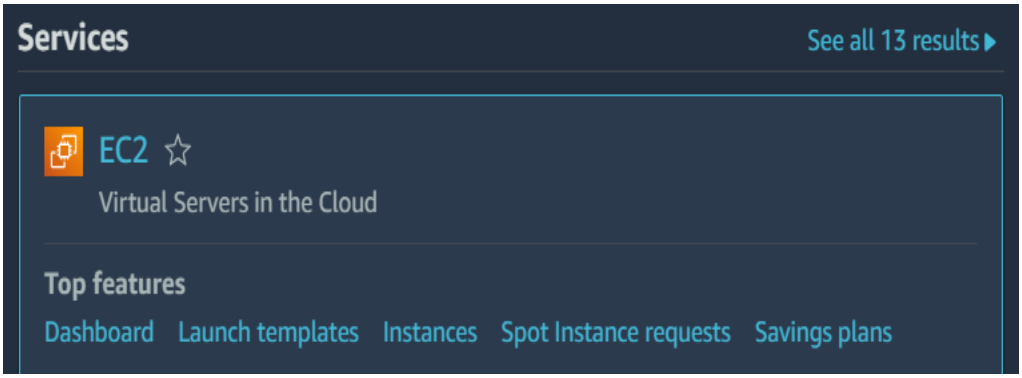


4. Save the security group.

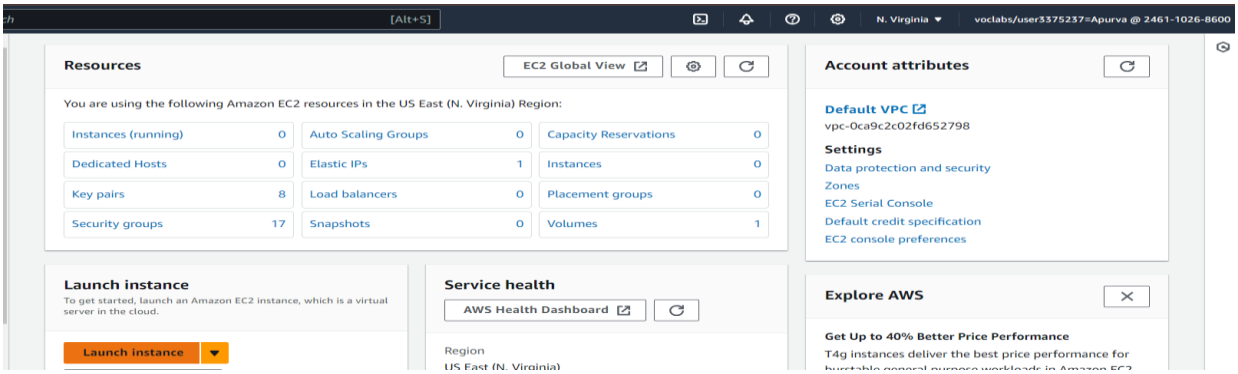


Task 4: Launch a Web Server Instance

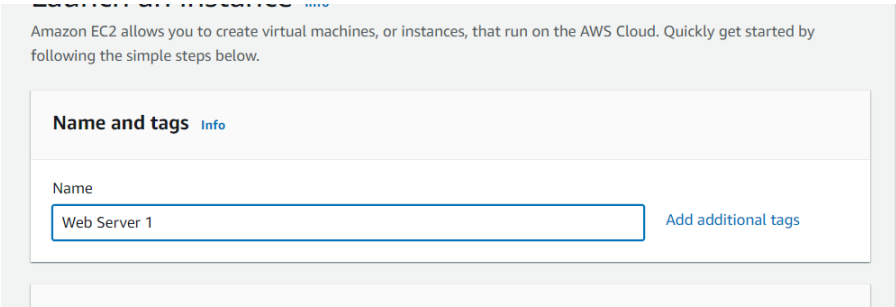
1. Go to the EC2 console (search for "EC2" in the search bar).



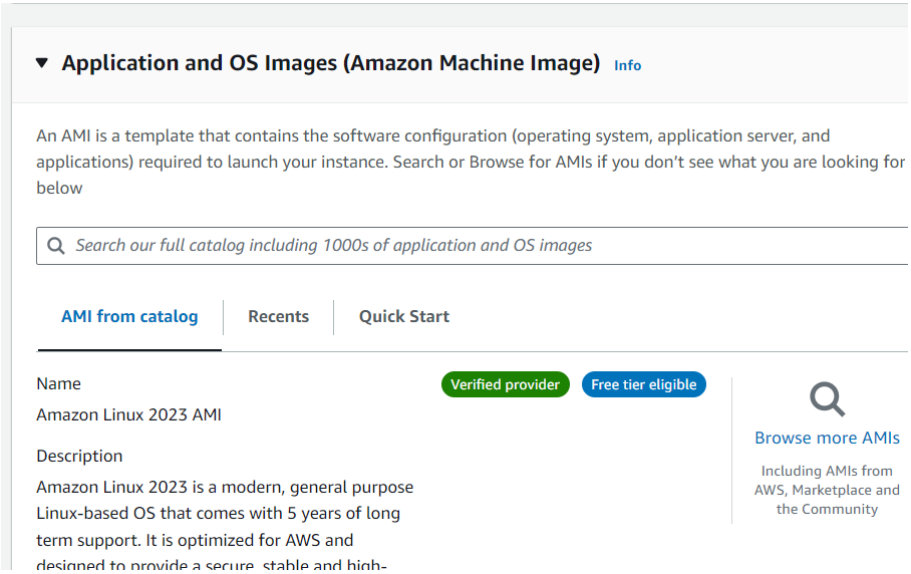
2. Launch a new instance.



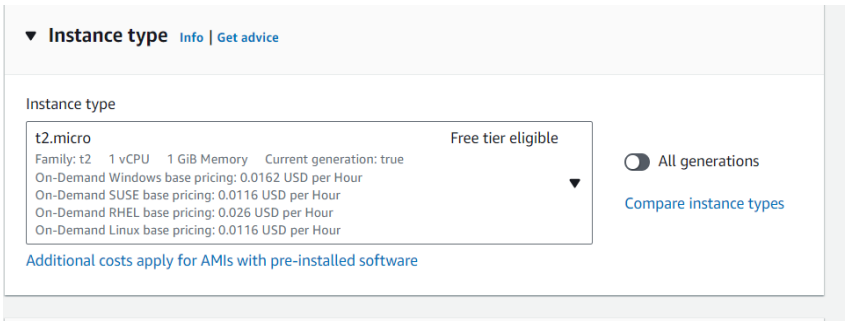
3. Name the instance: Web Server 1



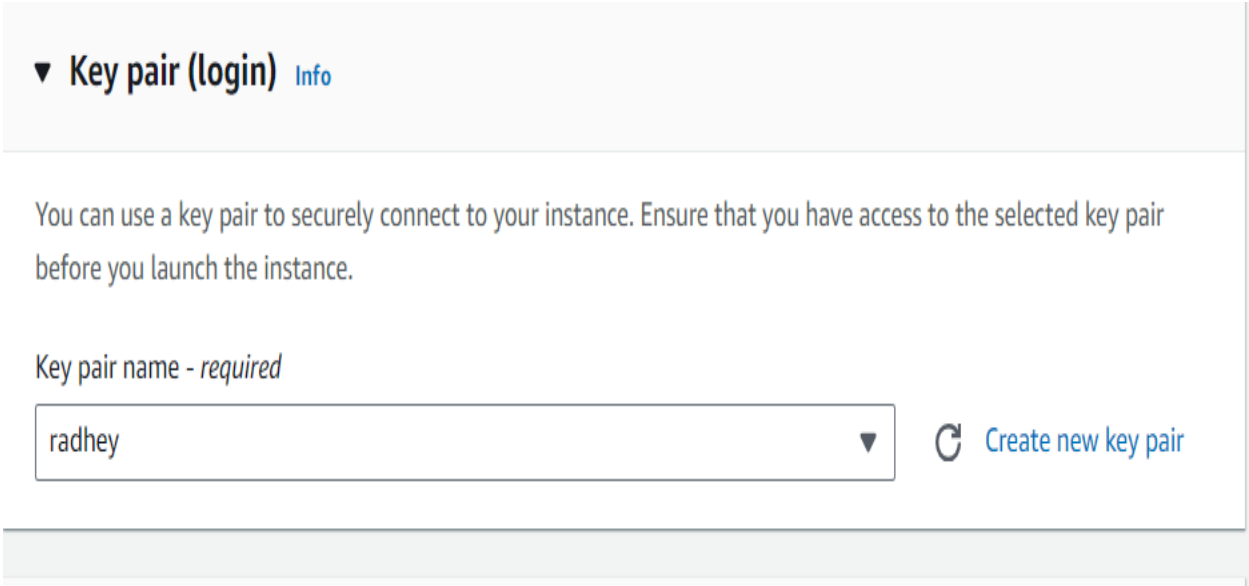
4. Choose the Amazon Linux 2023 AMI.



5. Choose the t2.micro instance type.

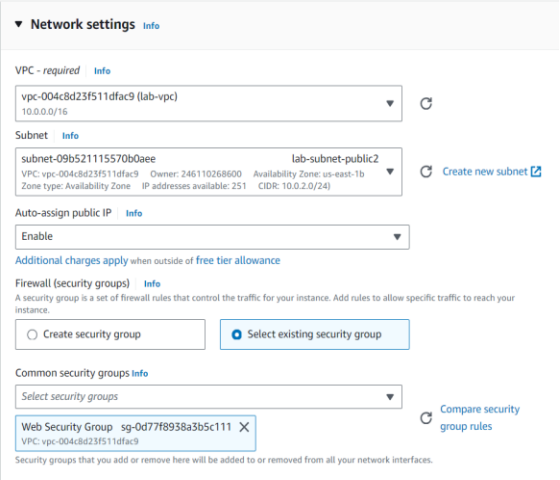


6. Select your key pair (e.g., radhey).



7. Configure network settings:
   - Network: lab-vpc
   - Subnet: lab-subnet-public2 (public subnet)
   - Auto-assign public IP: Enable

- Security group: Web Security Group (previously created)



8. Keep the default storage settings.

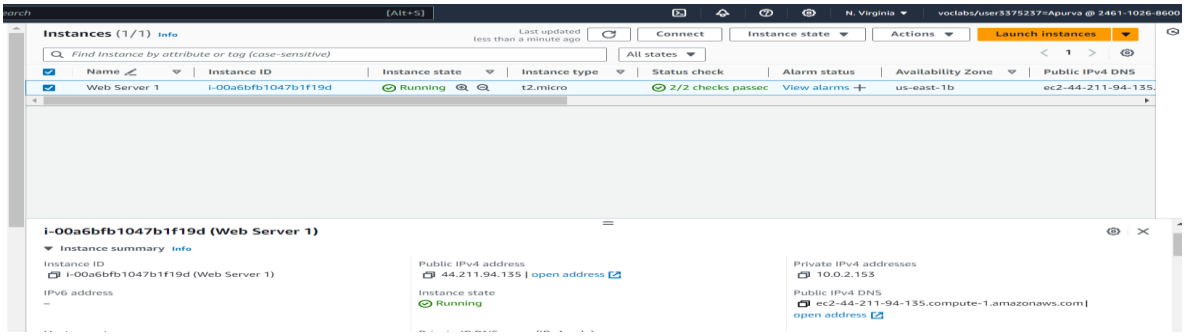
9. In the User data box, paste the script provided in the instructions. This script installs a web server and configure it.

```
#!/bin/bash
# Install Apache Web Server and PHP
dnf install -y httpd wget php mariadb105-server
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-
ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

10. Launch the instance.

11. Wait for the instance to launch (may take a few minutes).

12. Once launched, find the Public IPv4 DNS value in the instance details.



13. Open a web browser and paste the Public IPv4 DNS value. You should see a web page with the AWS logo and instance metadata.