**AWS – VPC**

Create a new VPC:

* Click on "Create VPC" and specify a name for your VPC.
* Choose an appropriate IPv4 CIDR block for your VPC, such as "10.0.0.0/16".
* Click on "Create" to create the VPC.

Create the subnets:

* Click on "Subnets" in the VPC dashboard.
* Create two public subnets and two private subnets within the VPC.
* Specify the subnet details including the name, VPC, availability zone, and an appropriate IPv4 CIDR block for each subnet.
* Ensure that the public subnets have their "Auto-assign public IPv4 address" option enabled.

Create an internet gateway:

* Click on "Internet Gateways" in the VPC dashboard.
* Click on "Create internet gateway" and give it a name.
* Attach the internet gateway to your VPC.

Configure routing:

* Click on "Route Tables" in the VPC dashboard.
* Select the default route table associated with your VPC.
* Edit the route table and add a route for "0.0.0.0/0" to the internet gateway created in the previous step.
* Associate the public subnets with this route table.

Launch a bastion server (jump box):

* Launch an EC2 instance in one of the public subnets.
* Assign a public IP address to the instance.
* Ensure that the security group associated with the bastion server allows SSH (port 22) access from your IP address.

Launch EC2 instances in the private subnets:

* Launch your desired EC2 instances in the private subnets.
* Ensure that the security groups associated with these instances allow inbound access from the bastion server's security group on the required ports.

Connect to the EC2 instances in the private subnets:

* SSH into the bastion server using its public IP address and appropriate credentials.
* From the bastion server, you can then SSH into the private EC2 instances using their private IP addresses.

Create a NAT gateway:

* Go to the AWS Management Console and navigate to the VPC service.
* Click on "NAT Gateways" in the VPC dashboard.
* Click on "Create NAT Gateway" and select the public subnet associated with one of your availability zones.
* Choose an existing Elastic IP or allocate a new one to associate with the NAT gateway.
* Click on "Create NAT Gateway" to create it.

Configure routing:

* Go to the VPC dashboard and click on "Route Tables".
* Select the route table associated with your private subnets.
* Edit the route table and add a new route for destination "0.0.0.0/0" pointing to the NAT gateway created in the previous step.
* Save the route table configuration.

Update the network access control lists (ACLs):

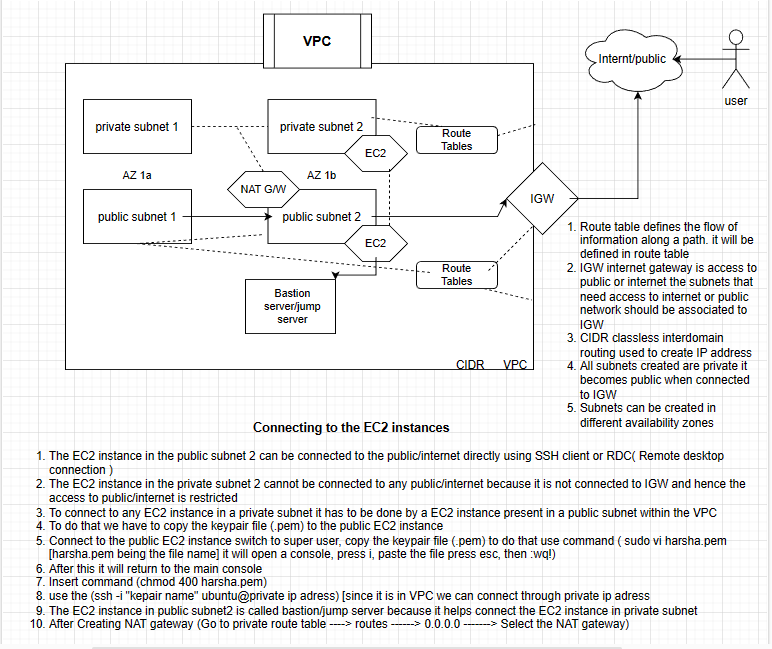
* Go to the VPC dashboard and click on "Network ACLs".
* Select the network ACL associated with your private subnets.
* Ensure that both inbound and outbound rules allow necessary traffic for your applications.
* By default, outbound traffic is allowed from private subnets, so there might not be any changes needed here.

Launch EC2 instances in the private subnets:

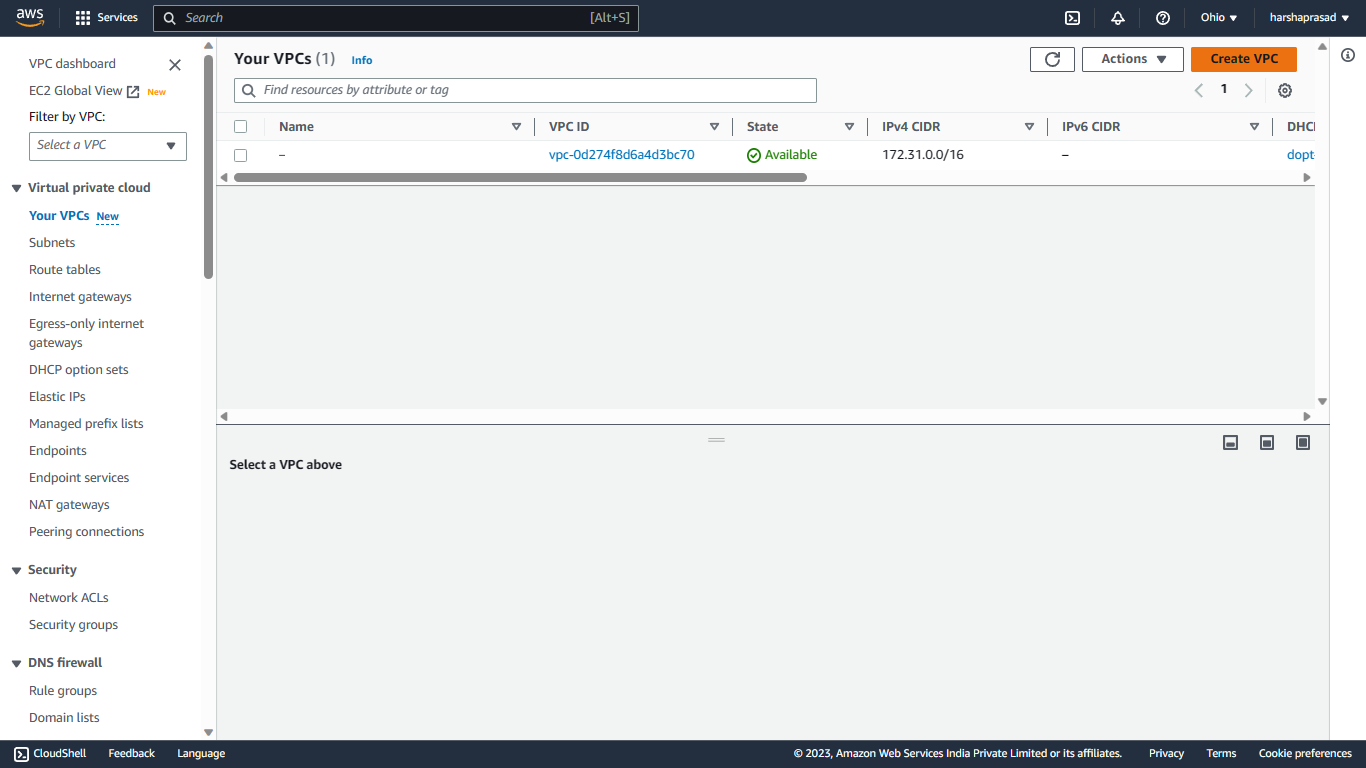
* Launch your desired EC2 instances in the private subnets.
* Ensure that the security groups associated with these instances allow outbound traffic on the required ports.

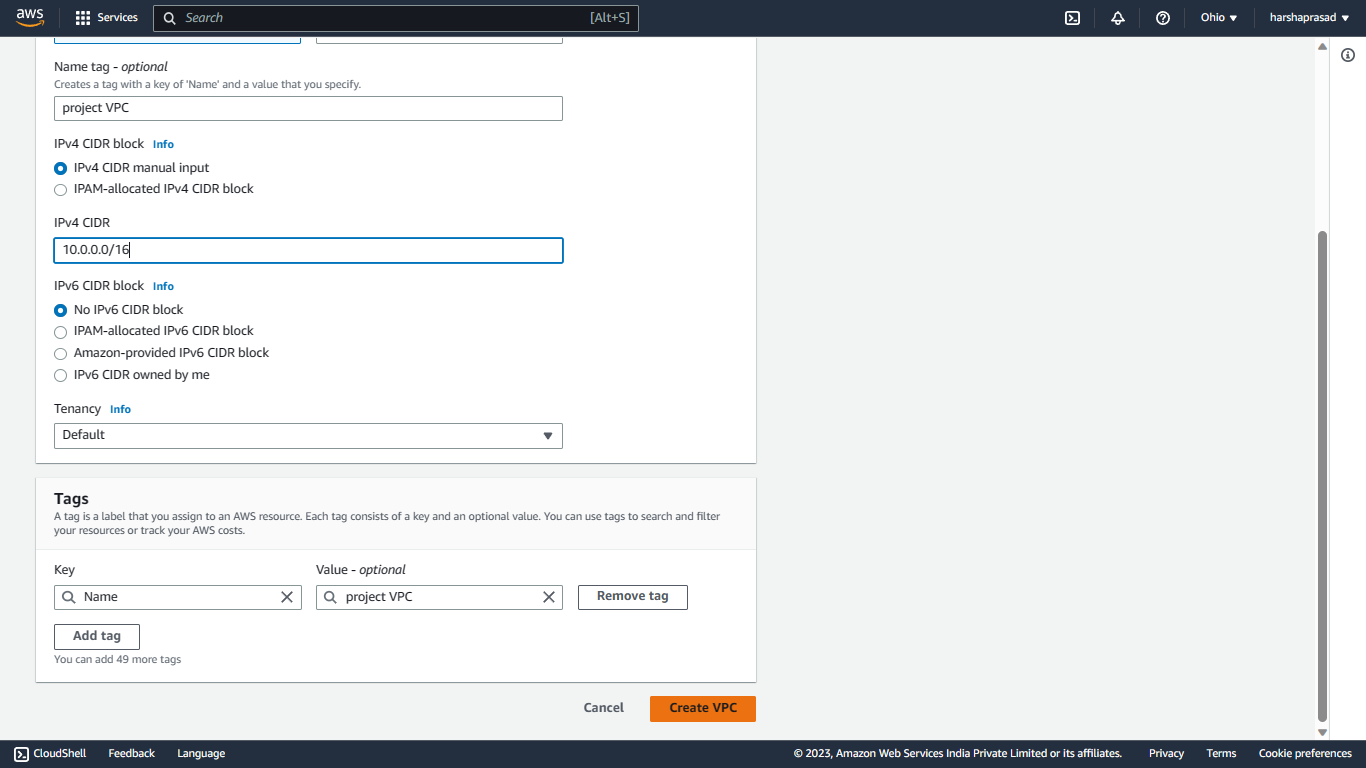
Verify internet connectivity:

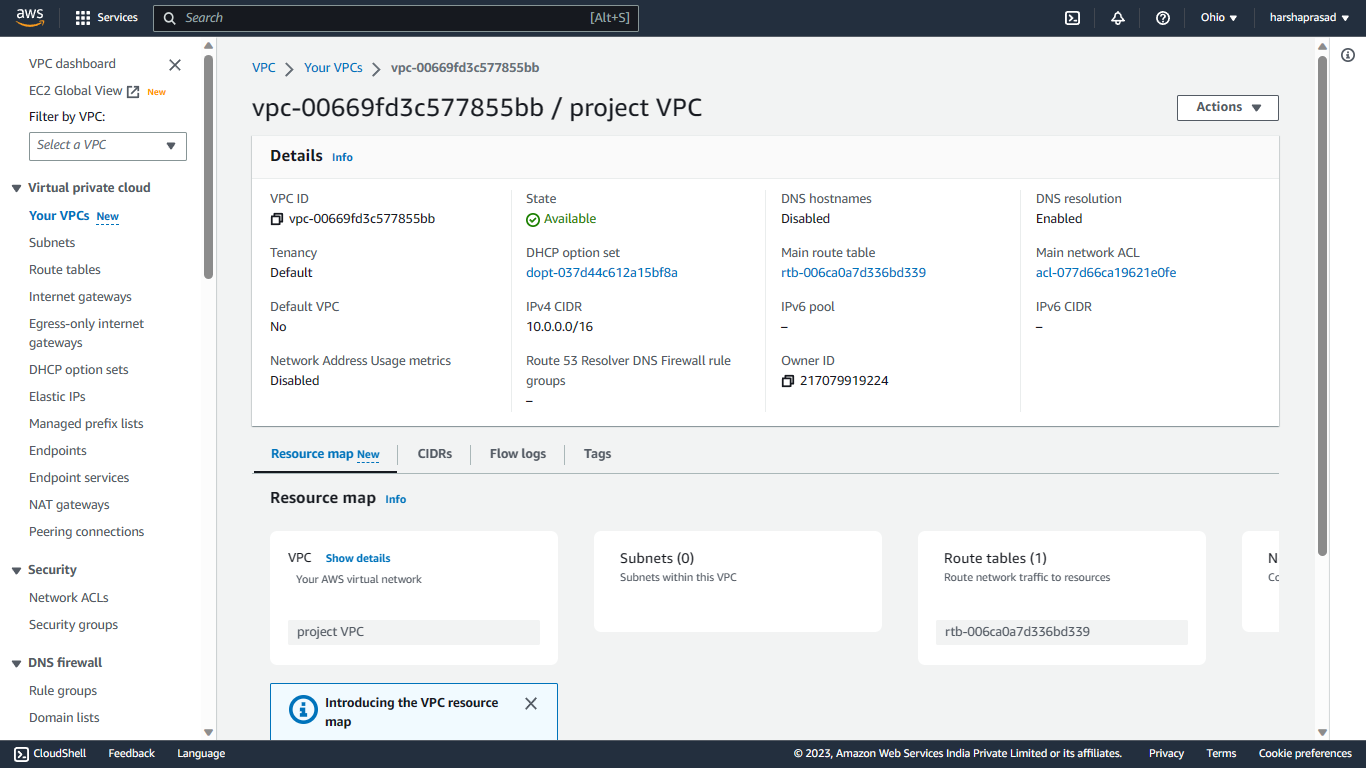
* Connect to one of the EC2 instances in the private subnet using SSH or any other desired protocol.
* Try to access the internet by pinging a public IP or updating the machine.
* If everything is configured correctly, the private EC2 instance should be able to access the internet through the NAT gateway.



Creating a VPC

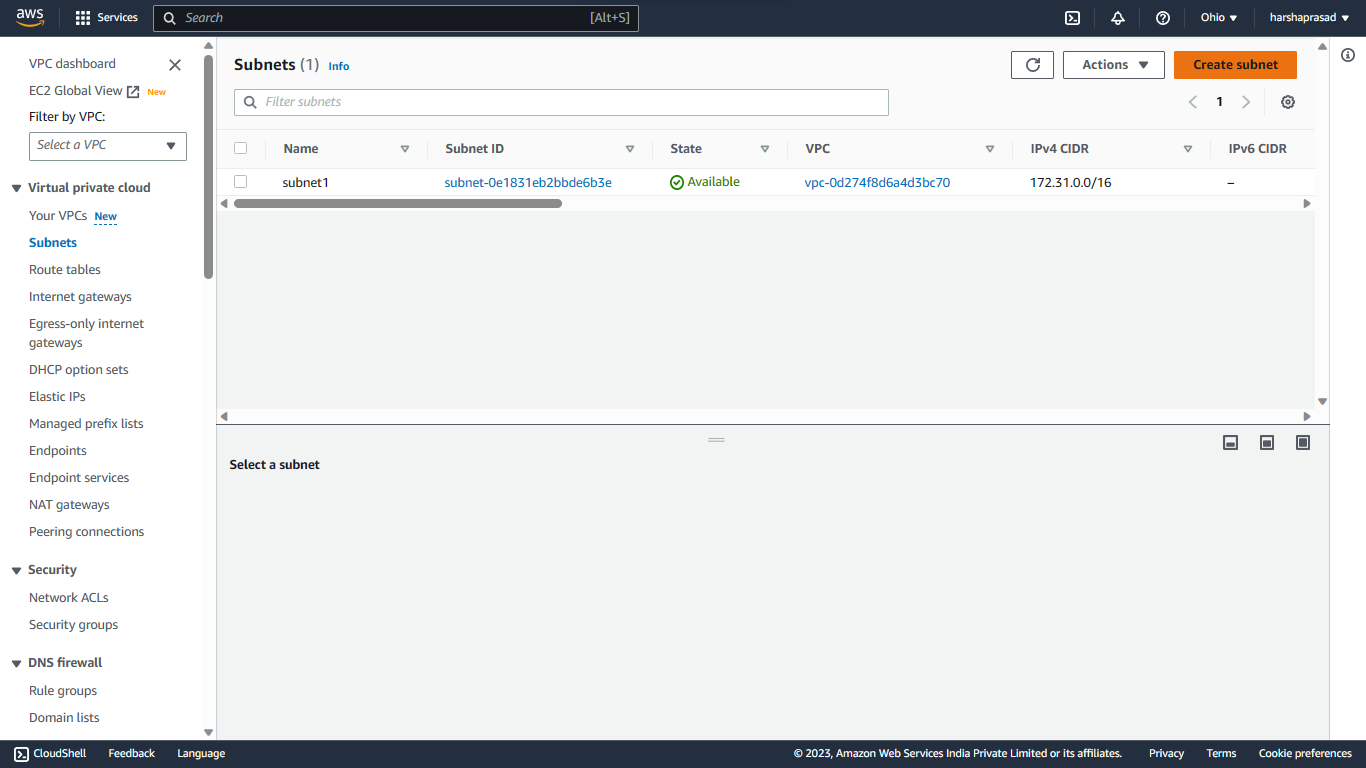
****

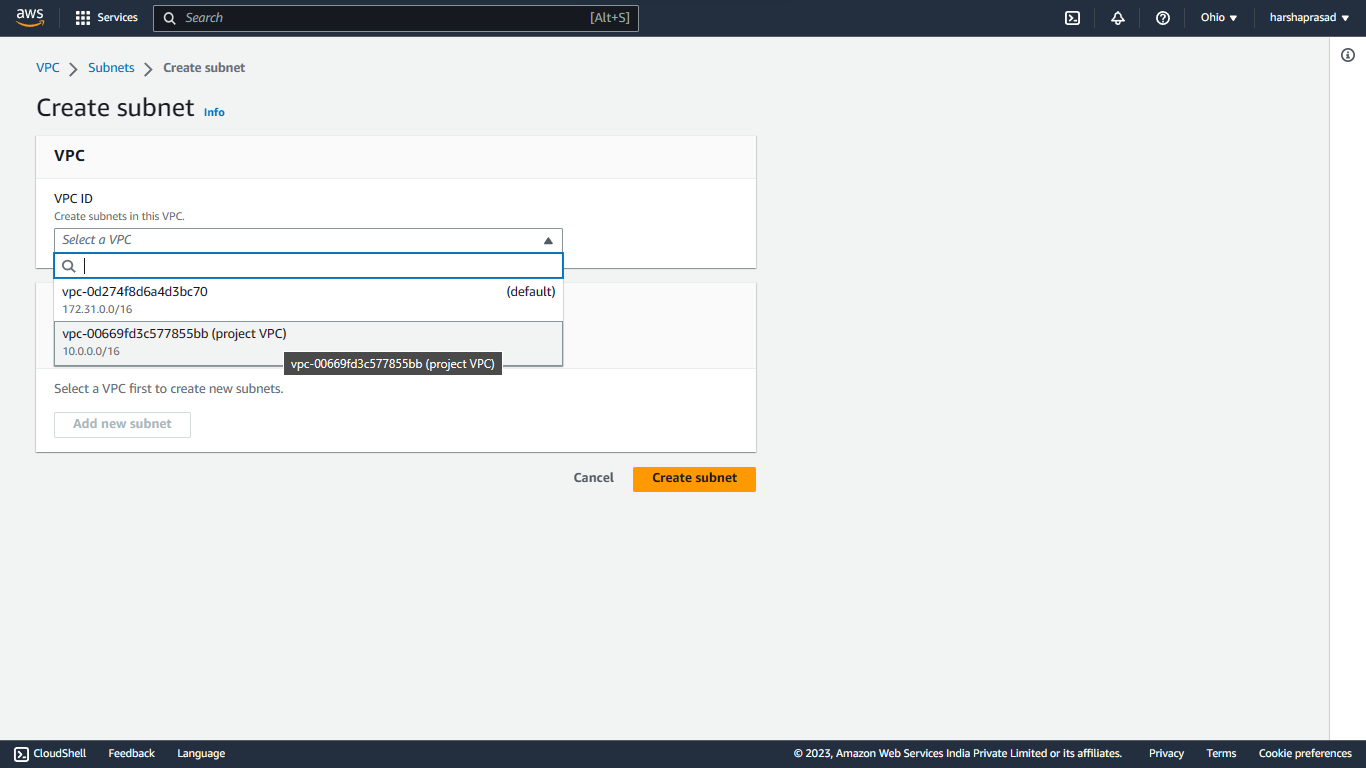




A screenshot of a computer

Description automatically generated

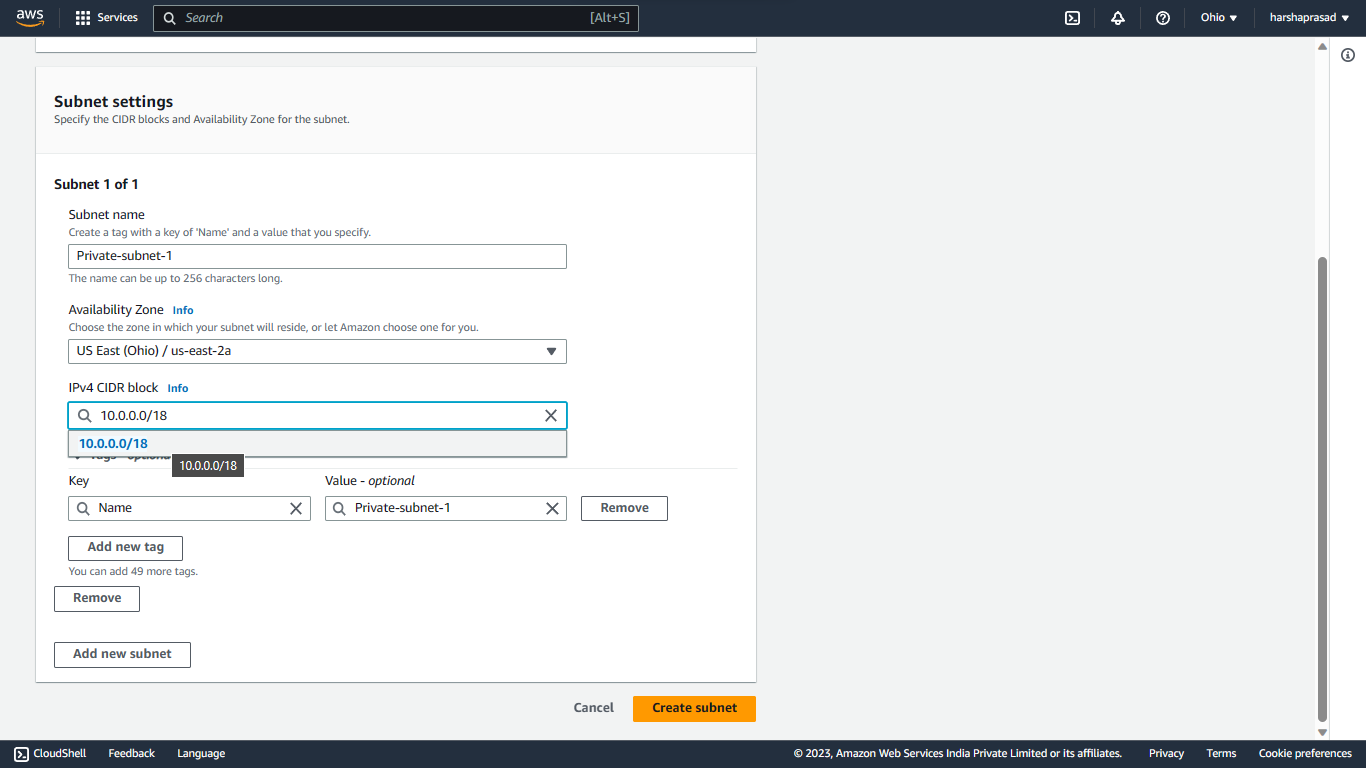
Creating SUBNETS

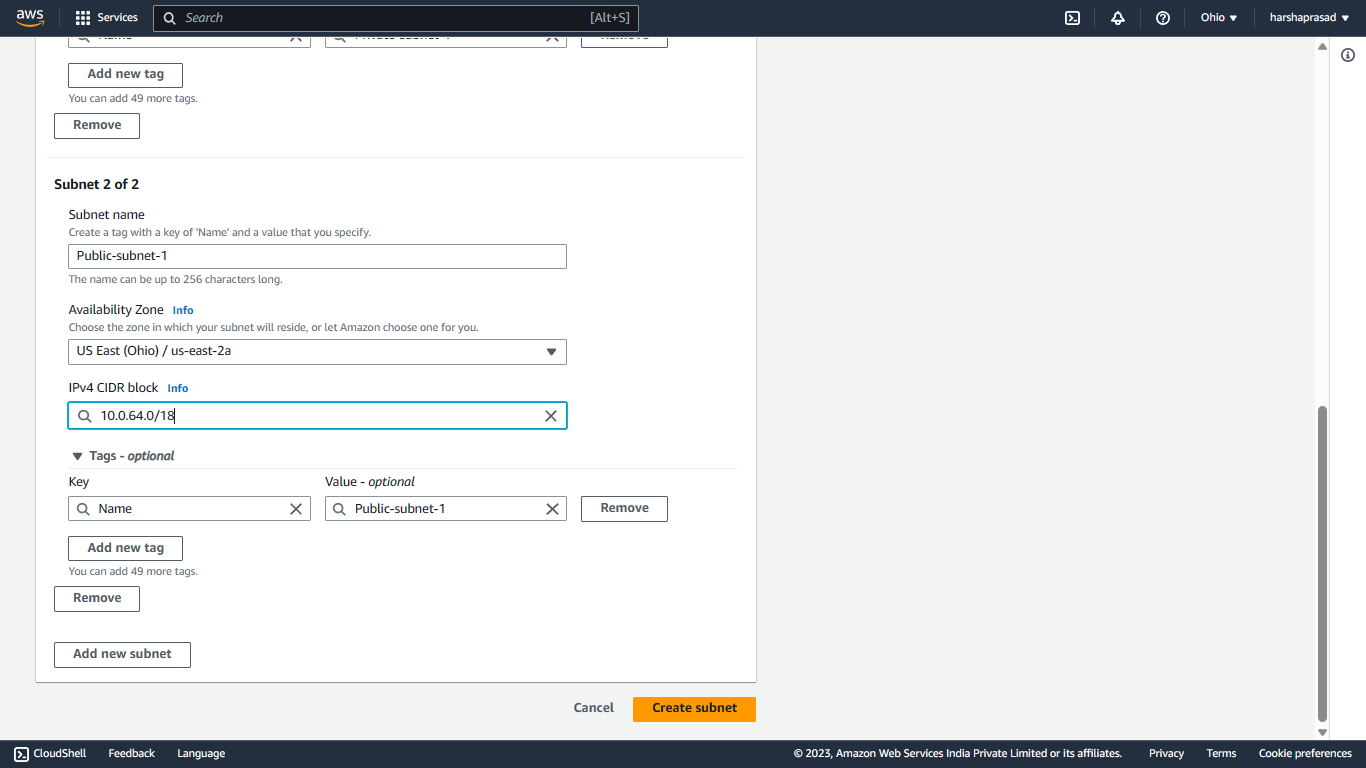
****

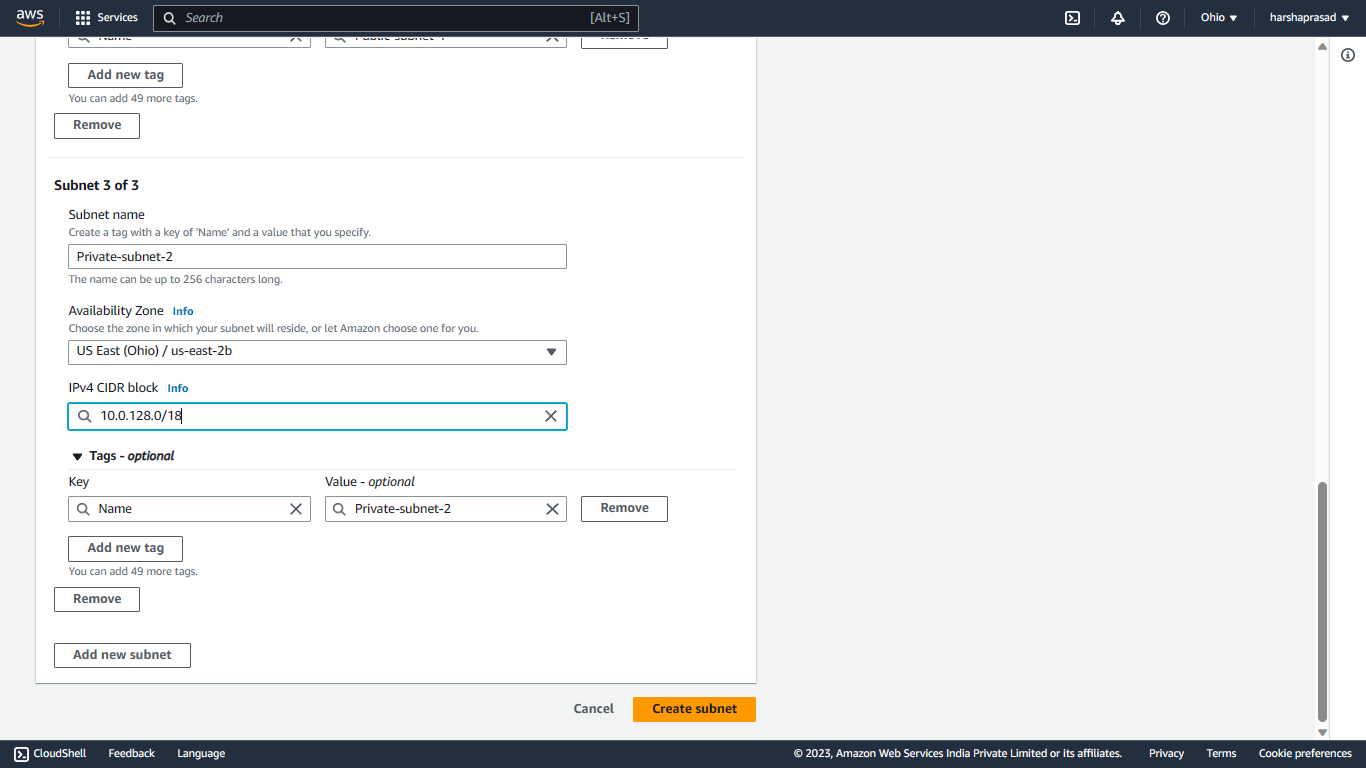
Creating a 2 Private and 2 Public subnets in 2 Different availability zones

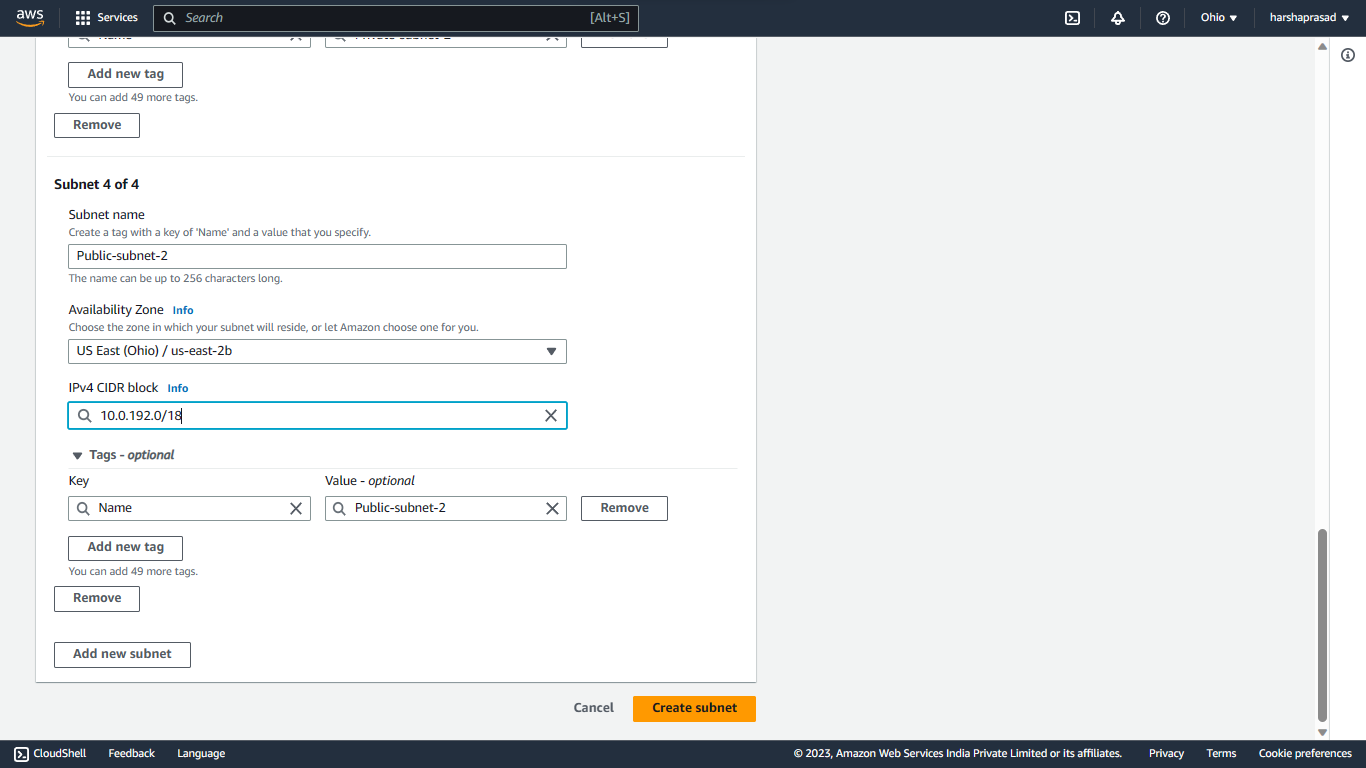
**A screenshot of a computer

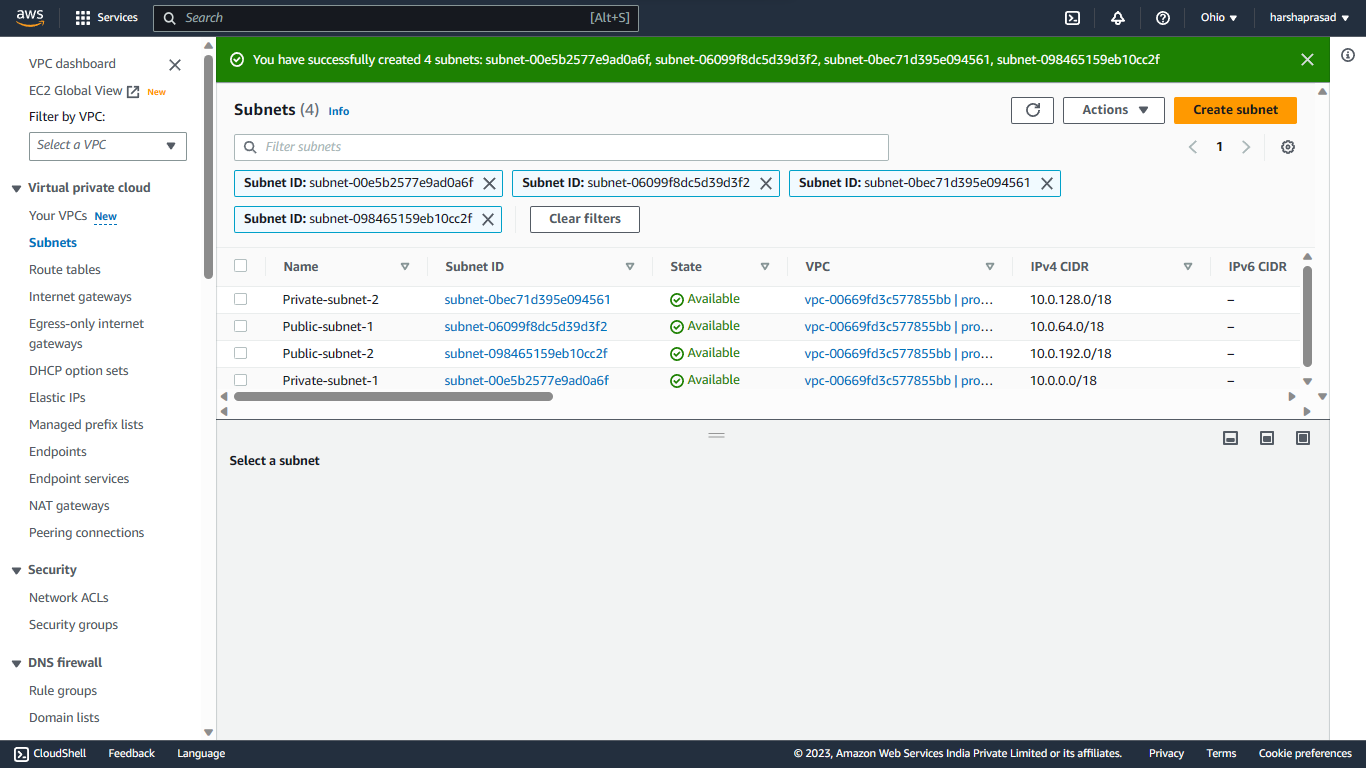
Description automatically generated**

****

****

****

****

****

**Creating Route Tables**

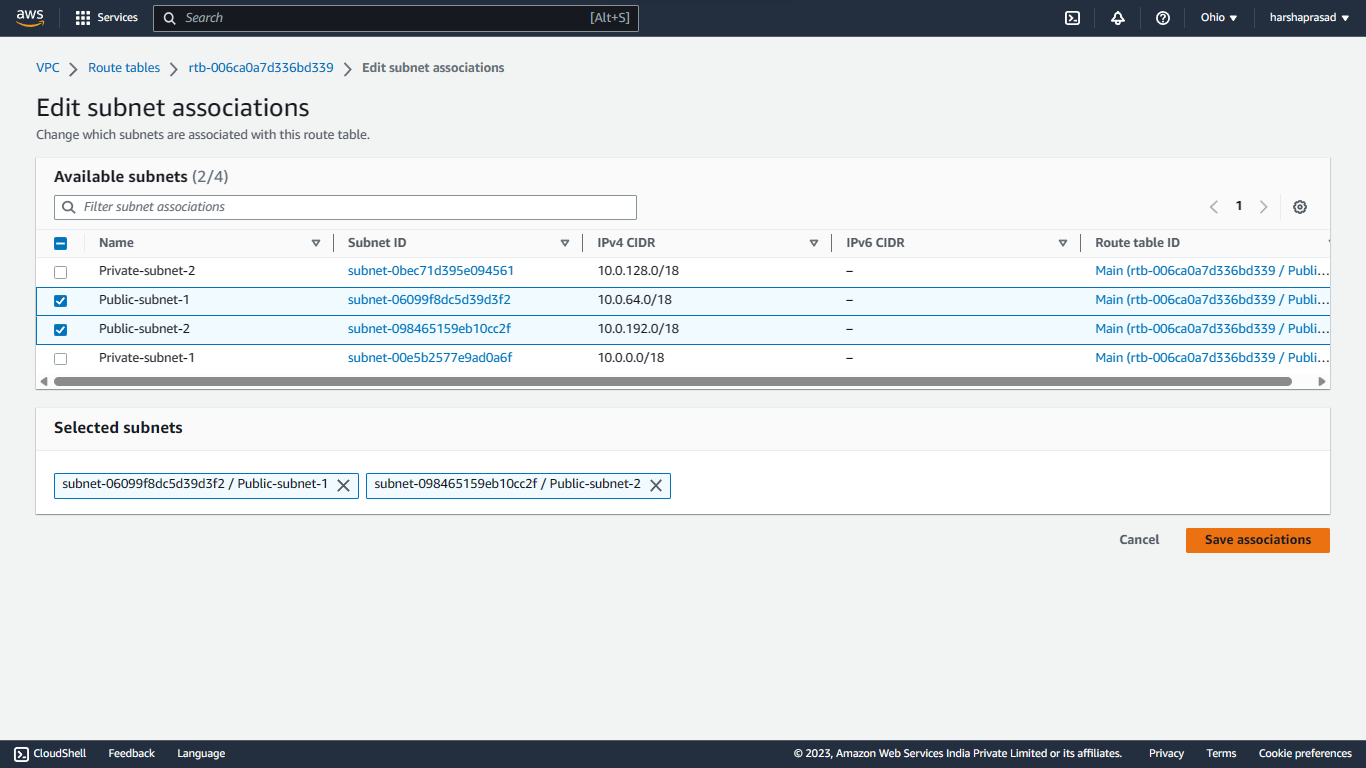
* A default Route table will be created during VPC creation, which will be converted to Public Route table.

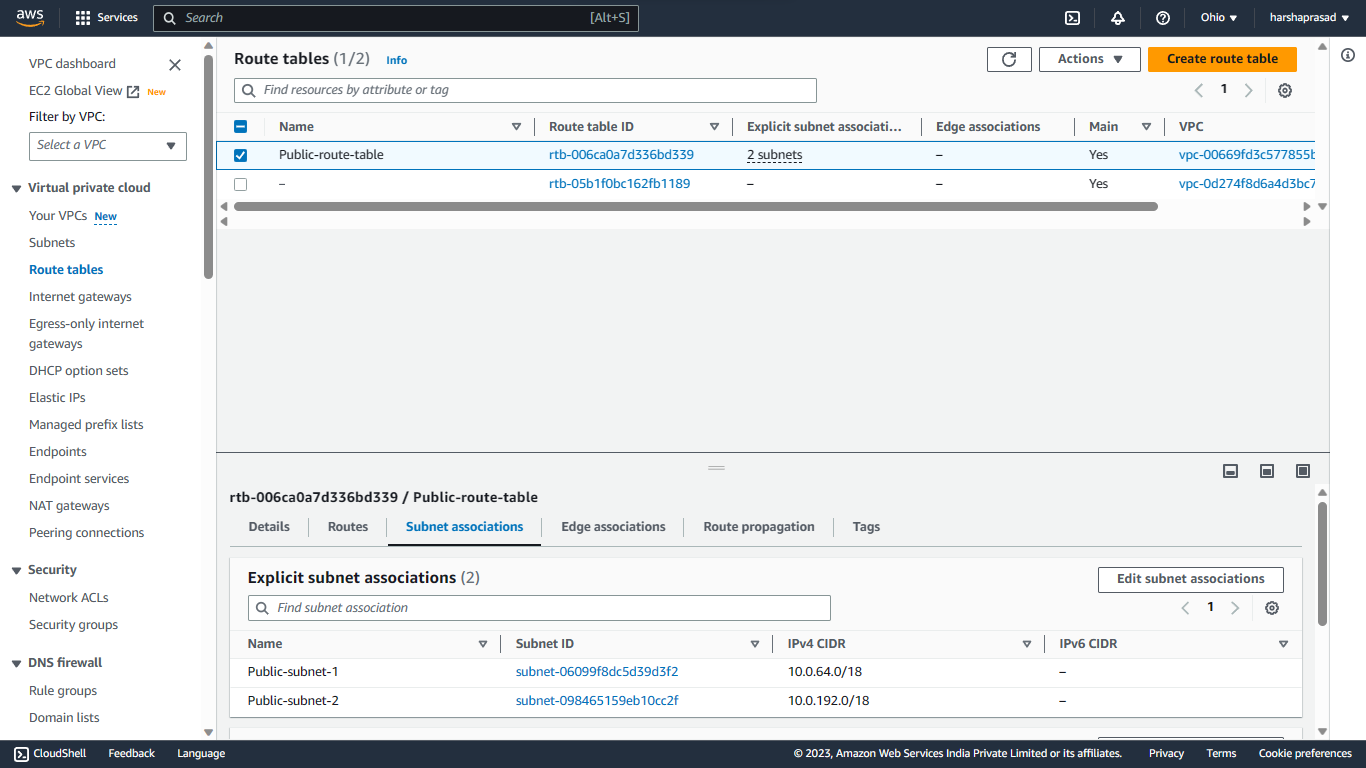


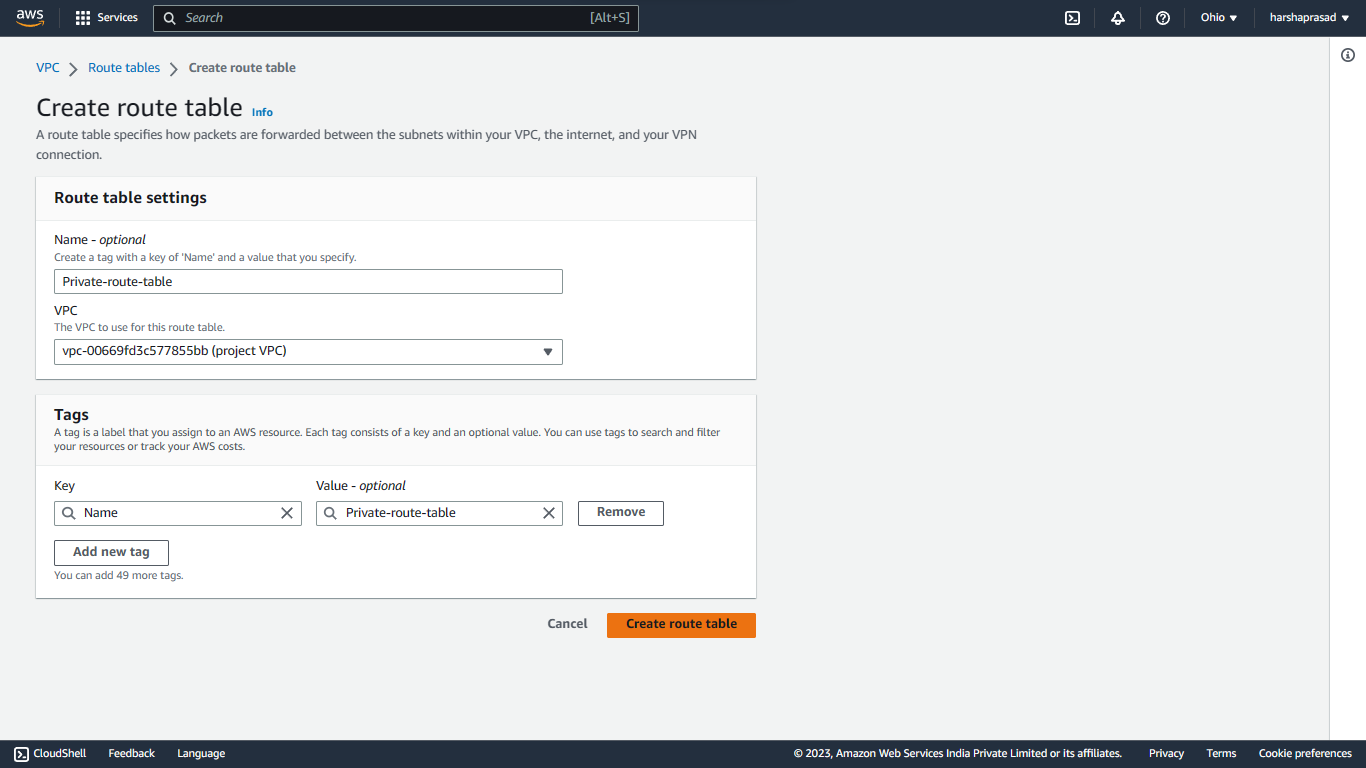
Associate Public subnets to Public route table

A screenshot of a computer

Description automatically generated

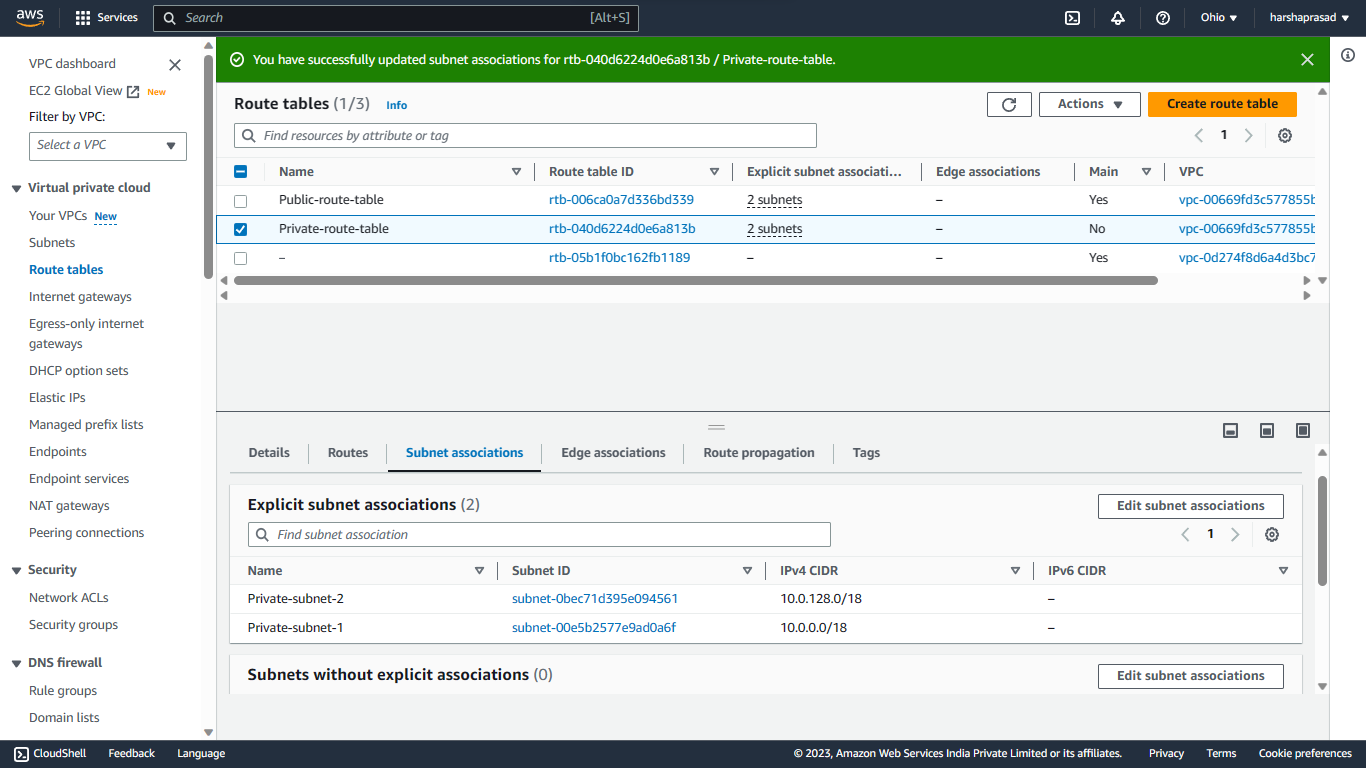




Creating a Private Route table

A screenshot of a computer

Description automatically generated

Subnet association to Private Route Table

We can see the association of subnet below

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedCreating Internet Gateway and attaching it to the VPC and Public route table

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedAssociate Project-IGW to Public route table

A screenshot of a computer

Description automatically generated

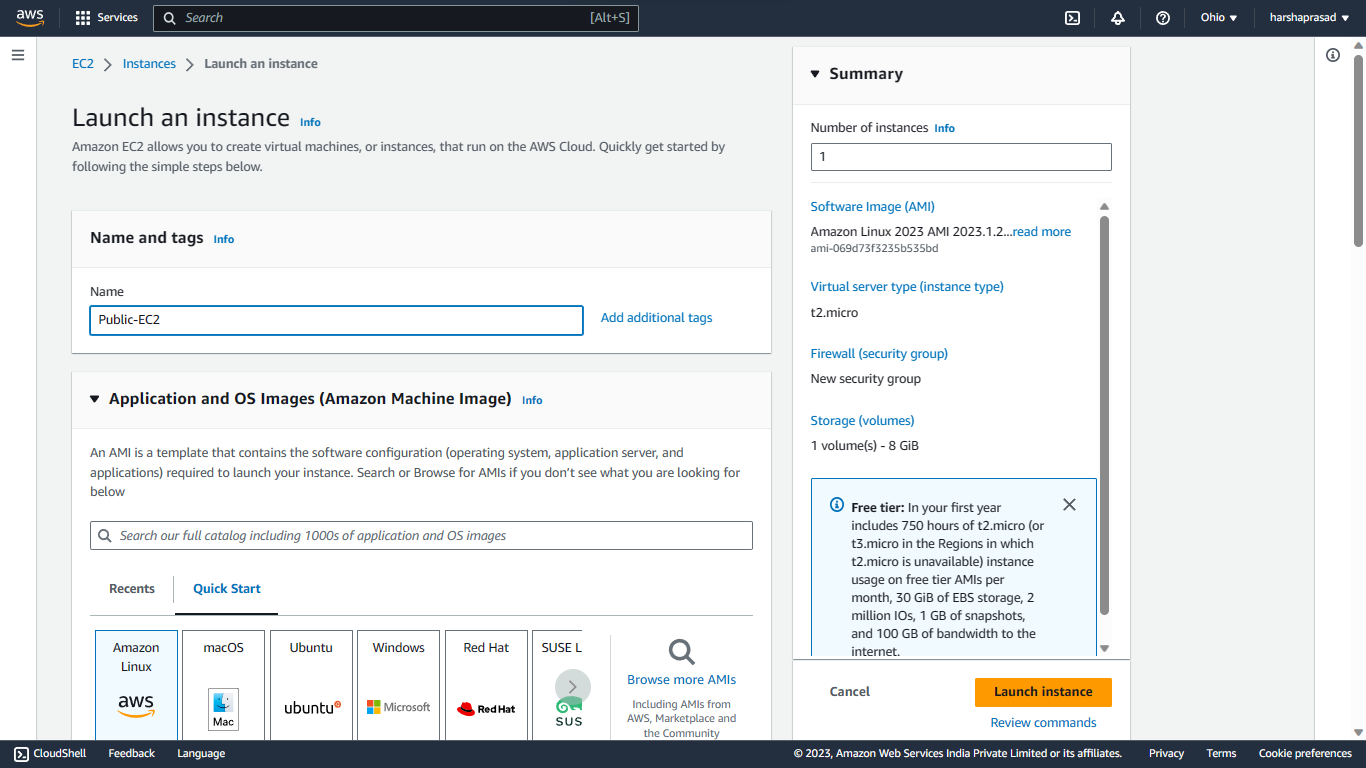
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedBelow is the final connection.

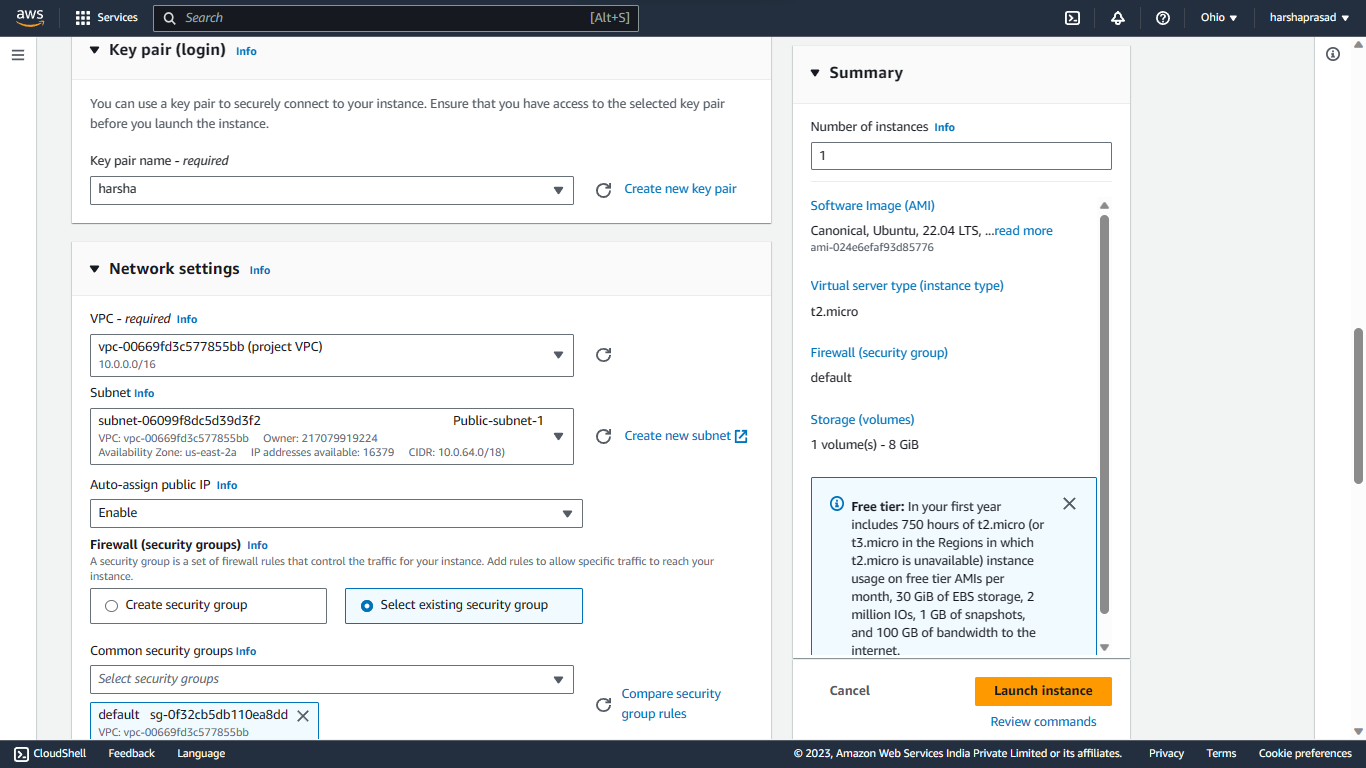
Creating Bastion server / Jump server



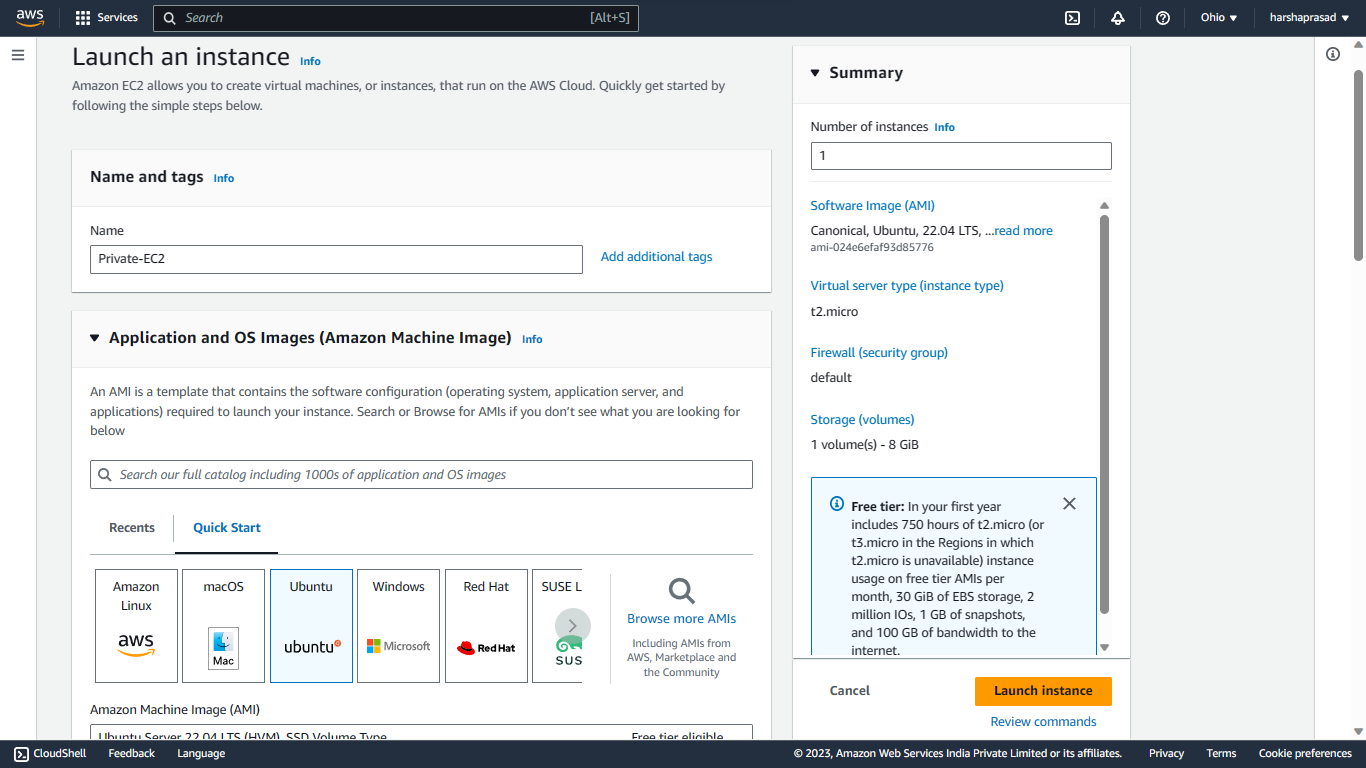
A screenshot of a computer

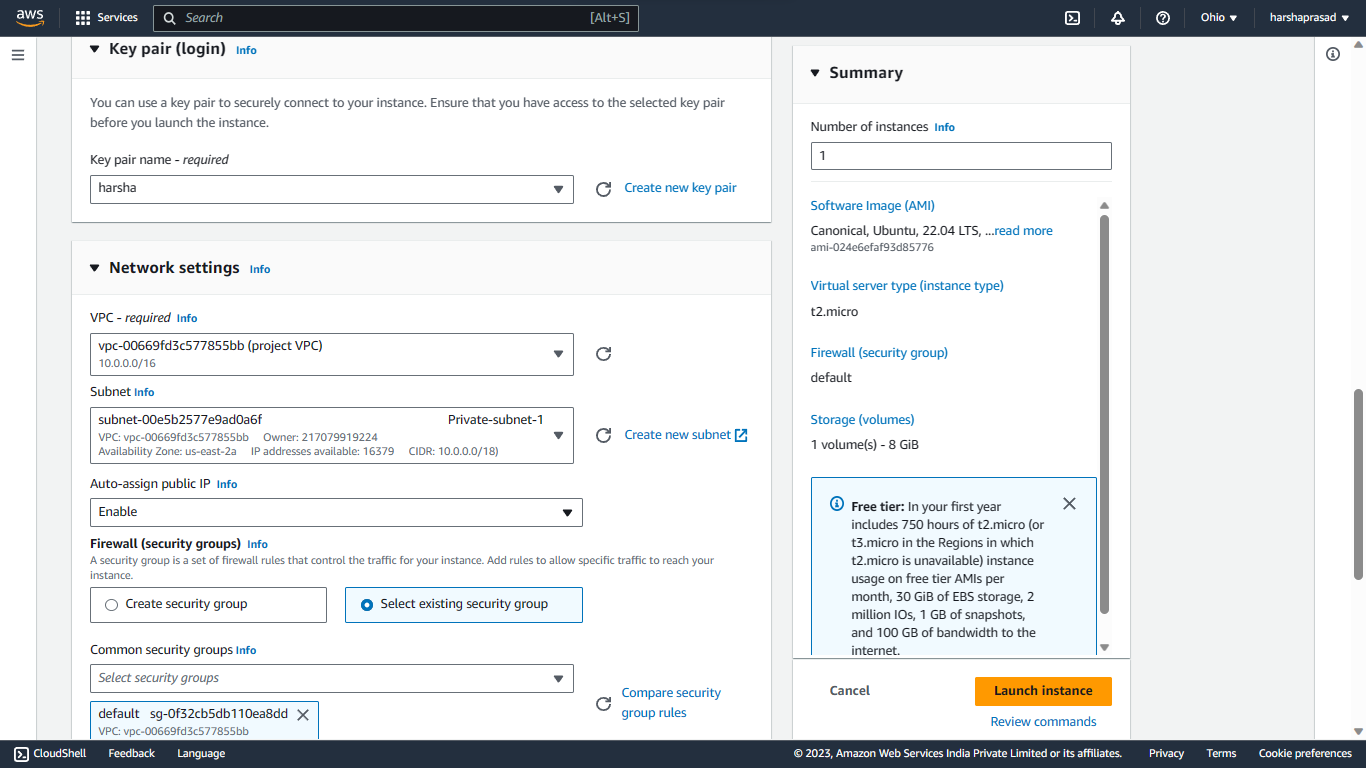
Description automatically generated

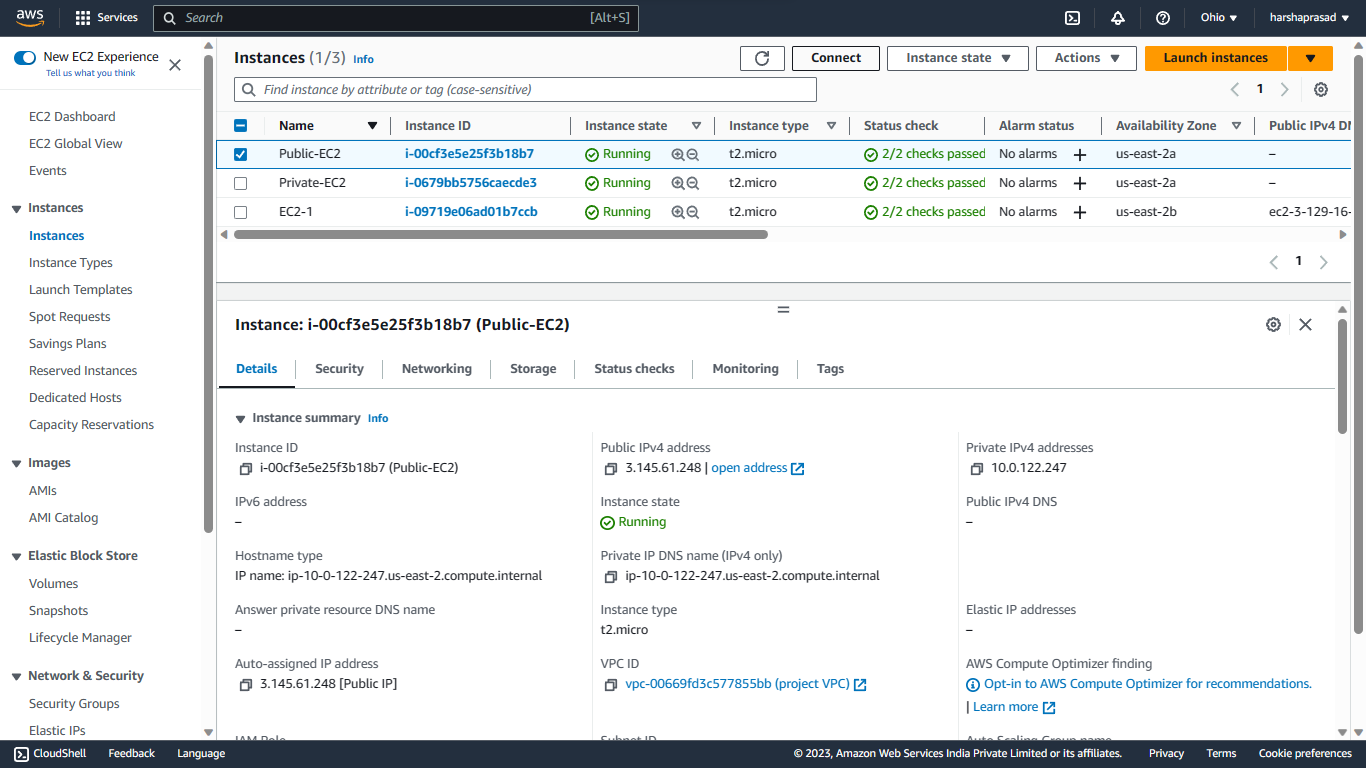
* Select the Keypair
* Select the Subnet you want the EC2 in
* Auto-assign public Ip 🡪 Enable.
* Select the security Group.
* Launch Instance



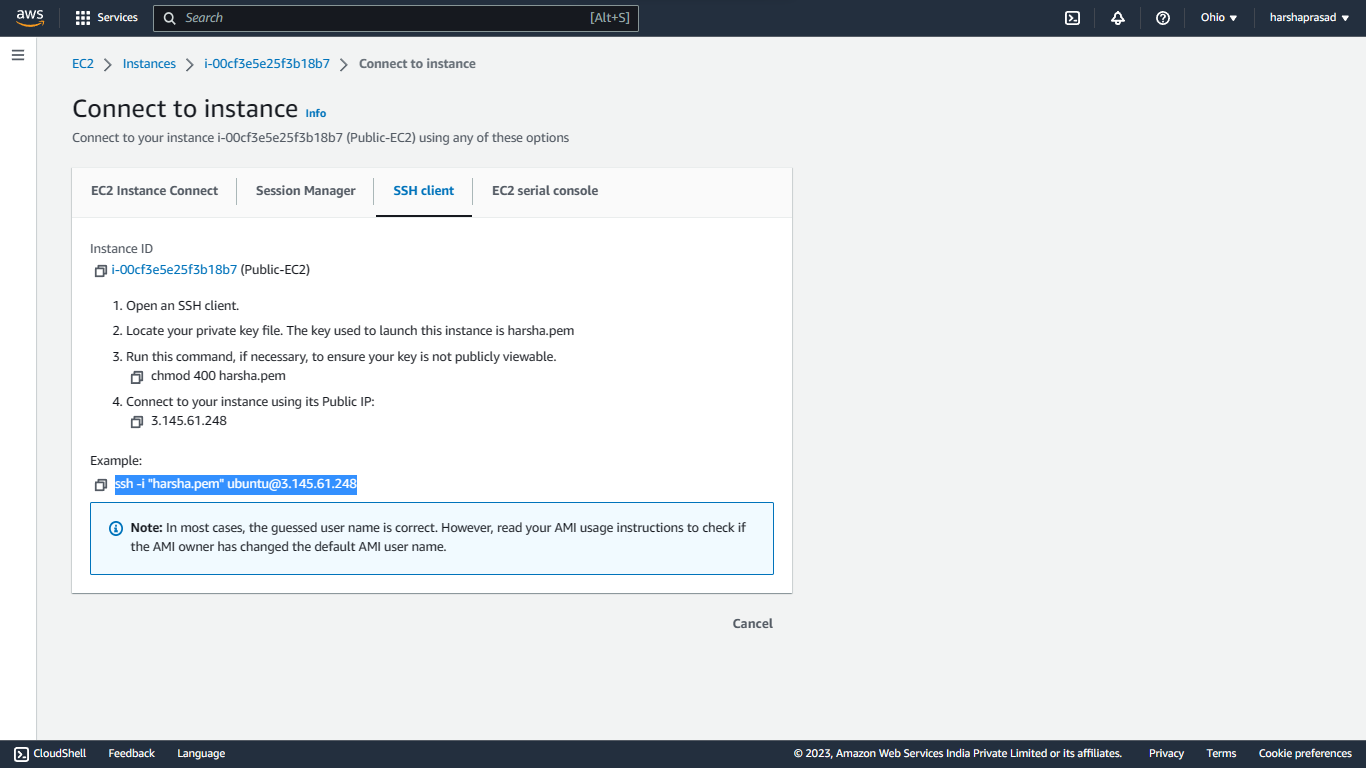
Above the steps to Create EC2 in Public subnet, same followed in Private subnet By selecting any private subnet

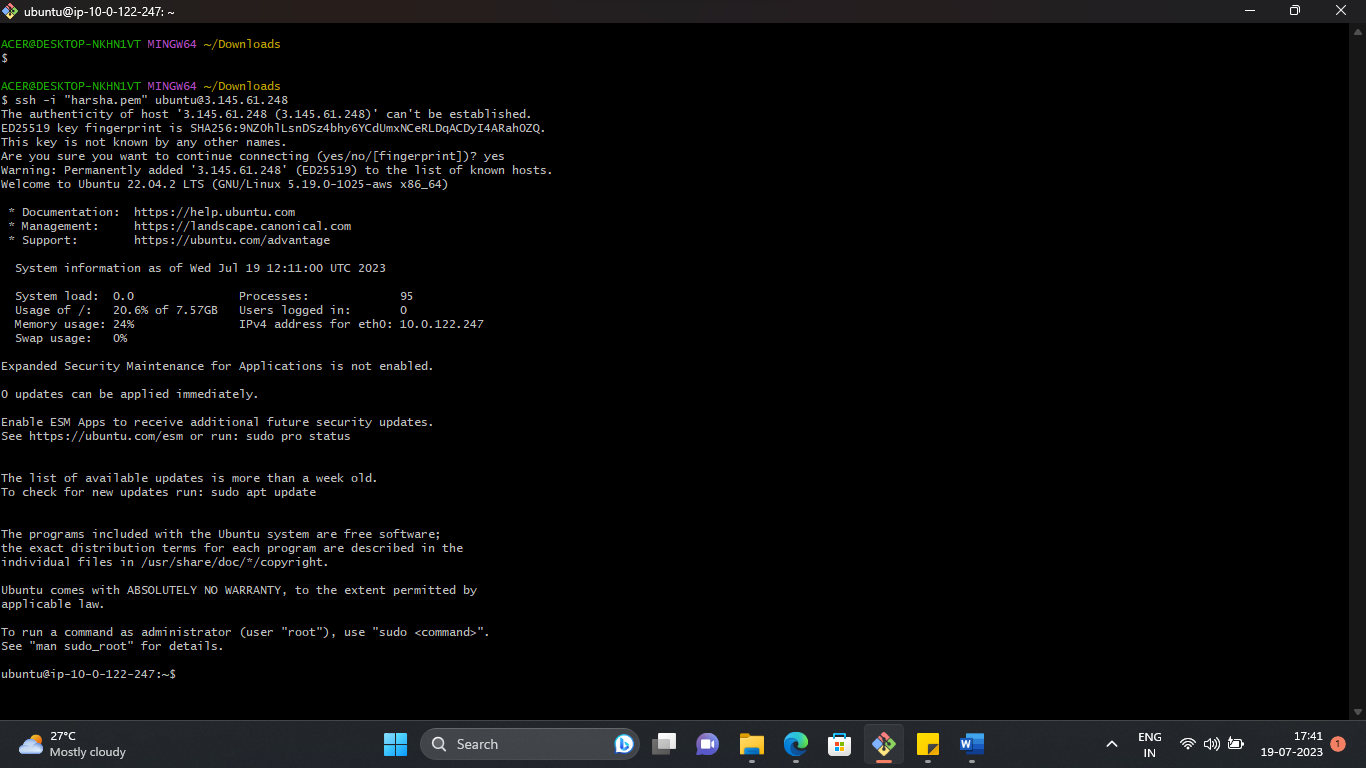




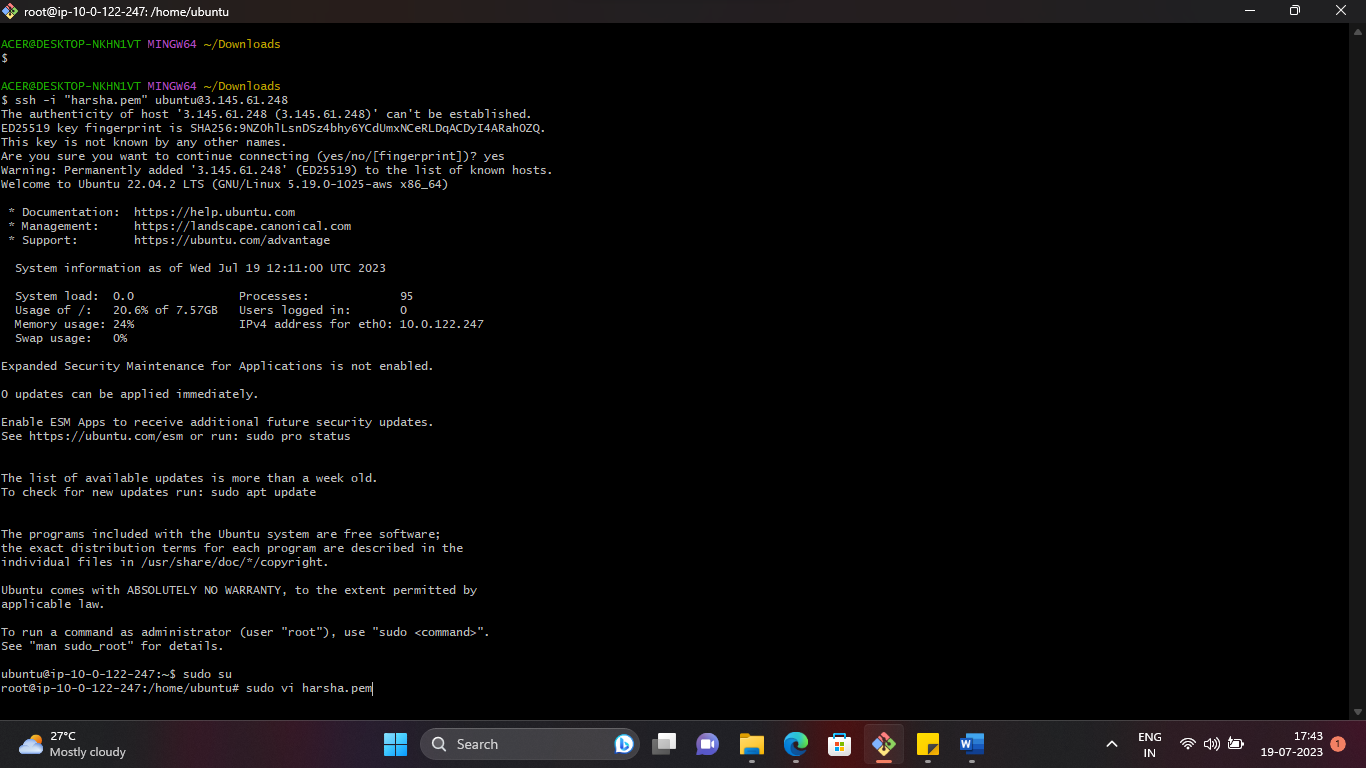


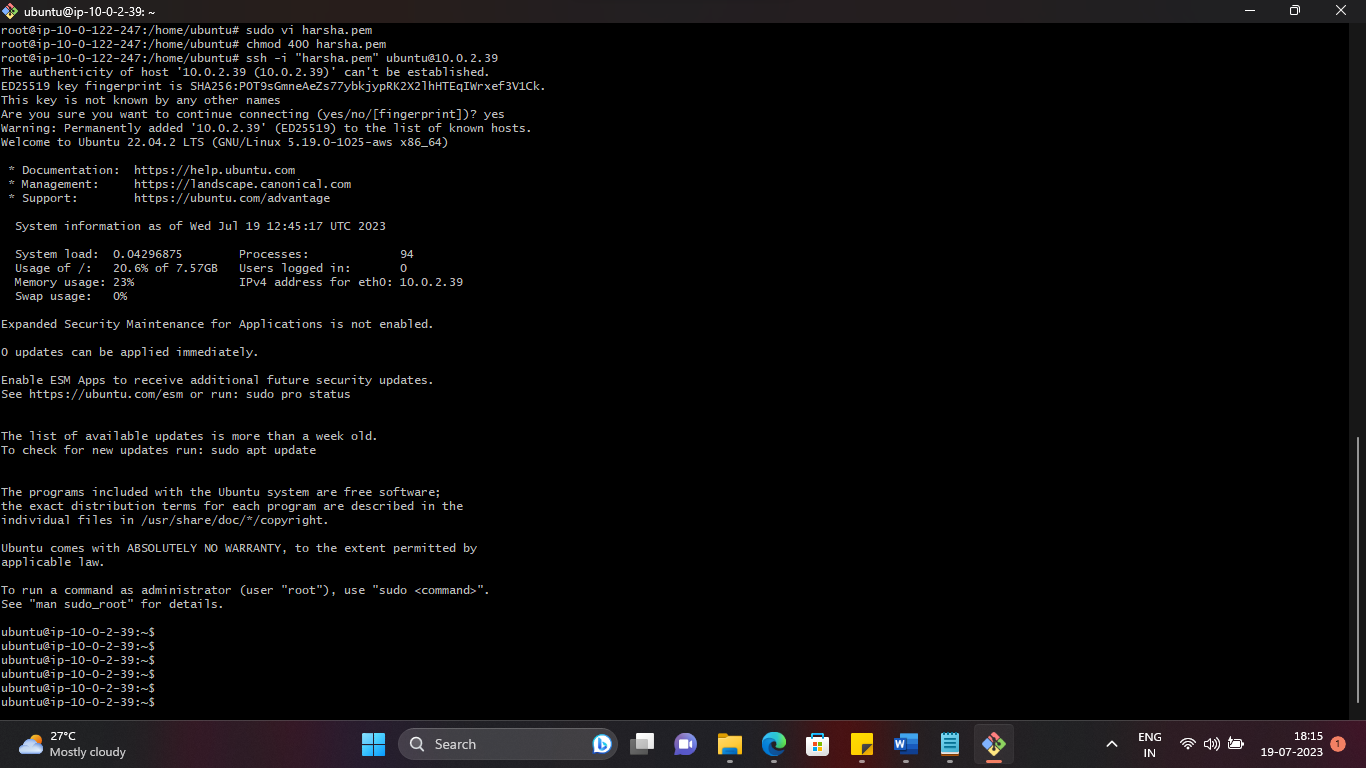
Connect the Public EC2 instance using SSH client.



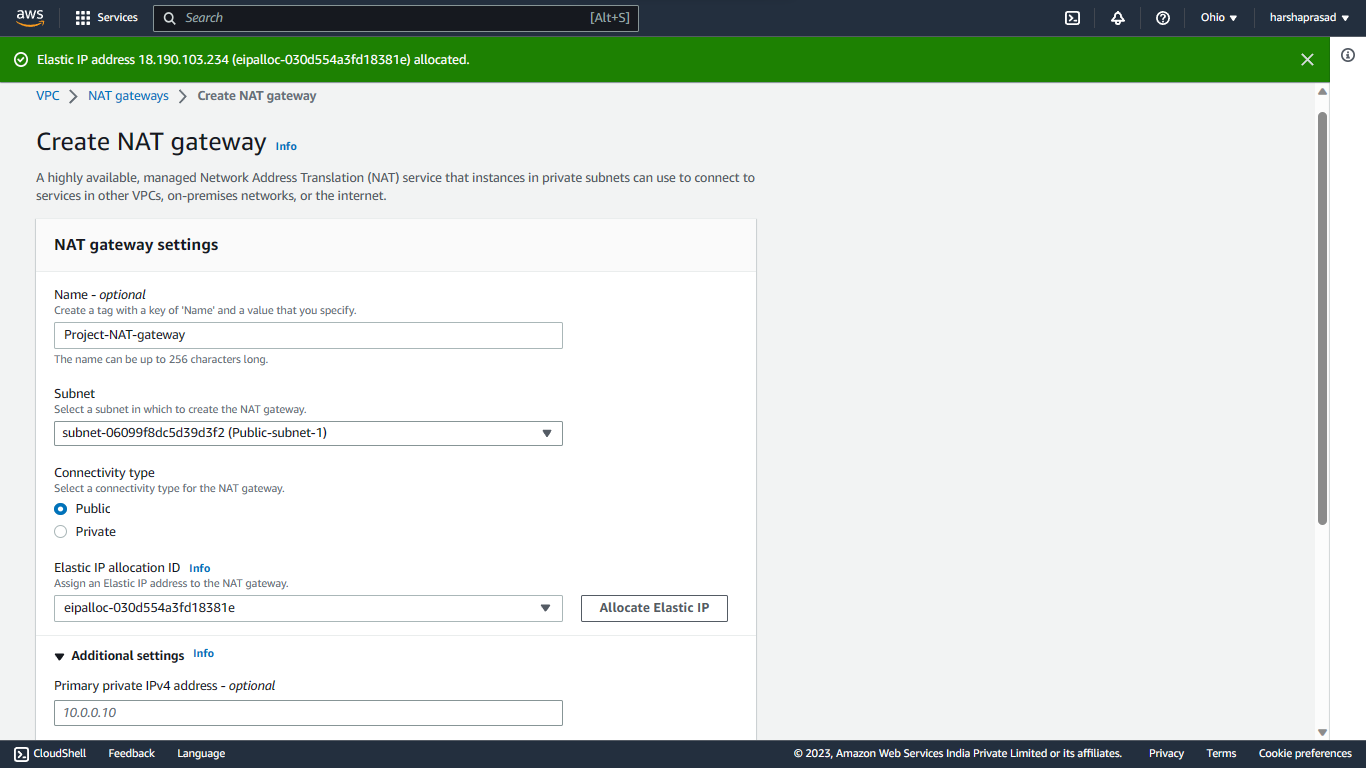


Copy paste the Keypair File to access the private EC2 instance from public EC2 instance



Below we can see that the Private EC2 is connected from Public EC2

Next to create NAT gateway which gives access to the private EC2 instance to public



In private Route table give access for NAT gateway to internet/public

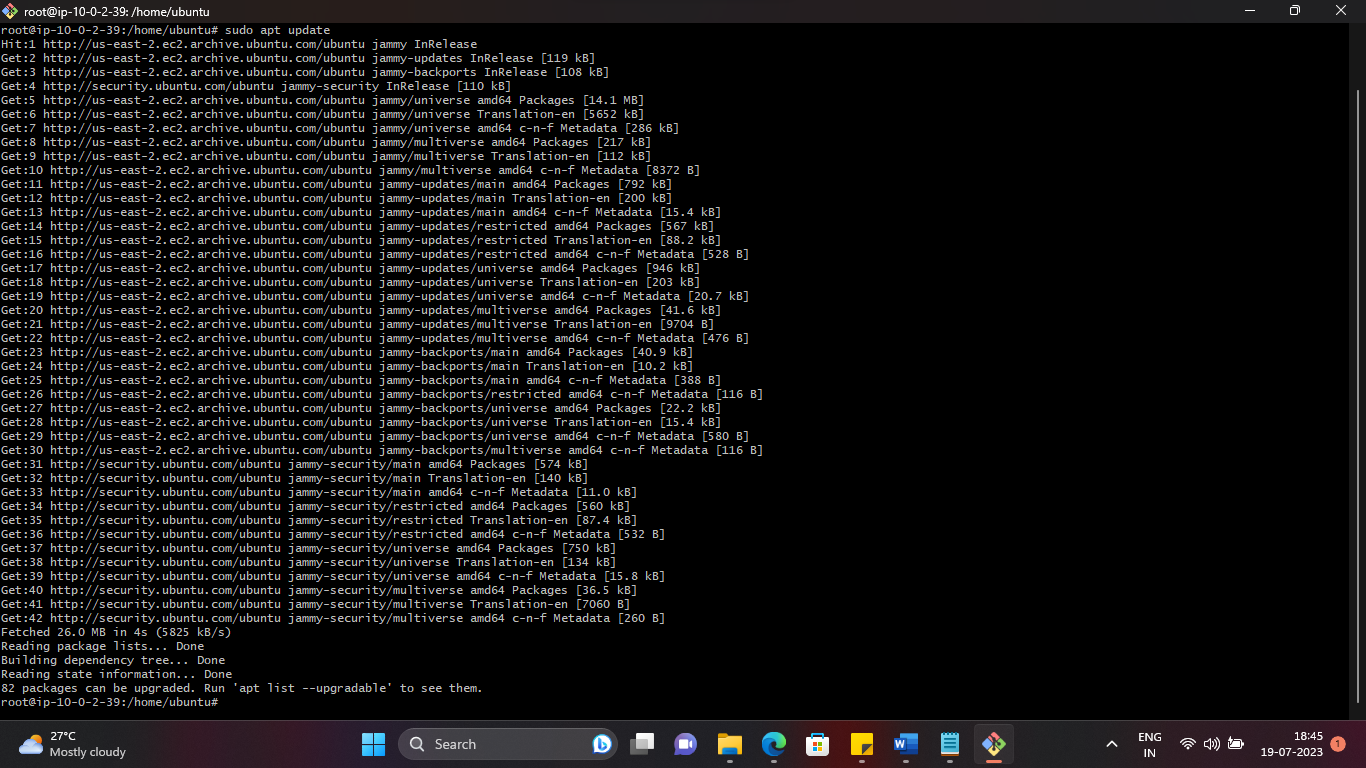
A screenshot of a computer

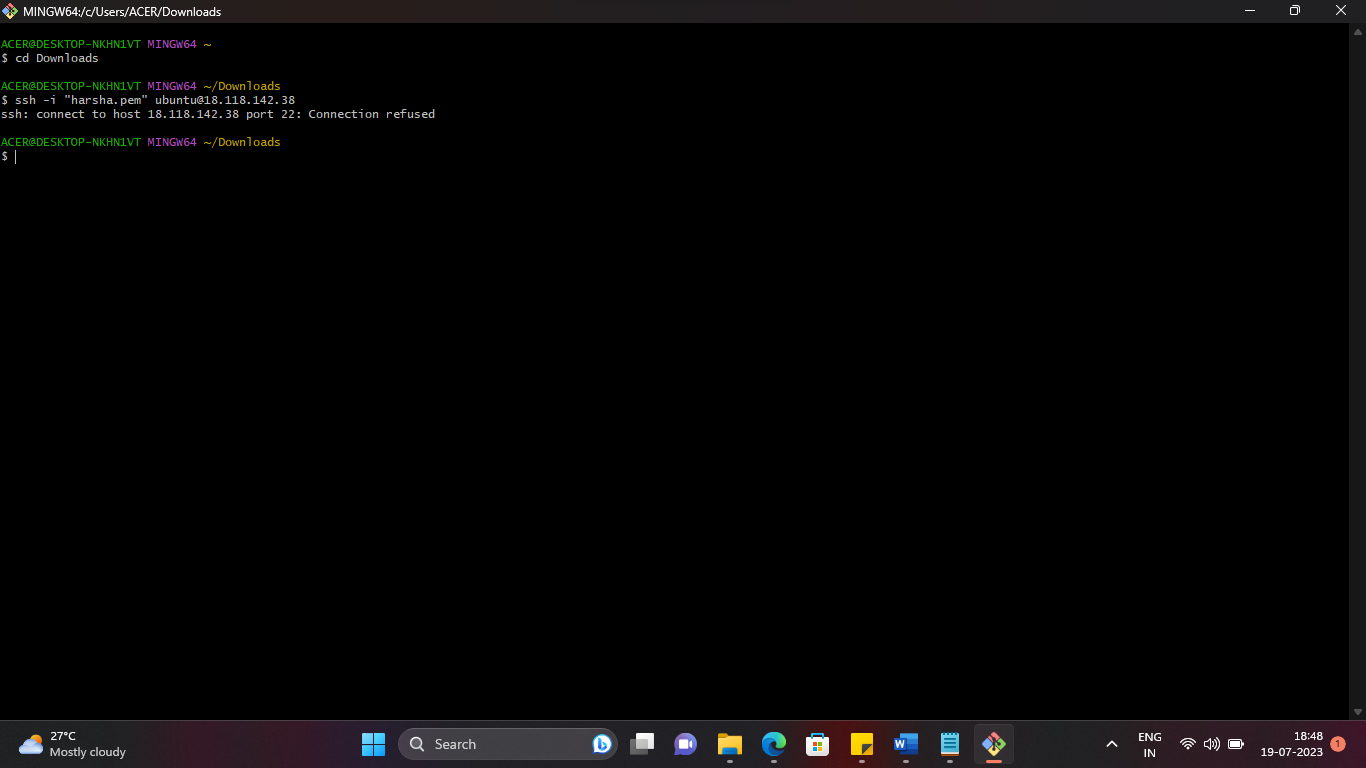
Description automatically generated

A screenshot of a computer

Description automatically generated

The Private EC2 instance will be able to access the internet After the Nat gateway is Attached to Private Route table but not the other way back.



The EC2 in the private subnet is being updated by connecting to the internet But cannot be connected from public network. Only through a bastion server