FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING Department of Computer Engineering

Course, Subject & Experiment Details

|  |  |
| --- | --- |
| Practical No: |  |
| Title: | To study and Implement Infrastructure as a Service using AWS/Microsoft Azure |
| Name of the Student: | Warren Fernandes |
| Roll No: | 8940 |
| Date of Performance: | 28/03/2022 |
| Date of Submission: | 28/03/2022 |

Evaluation:

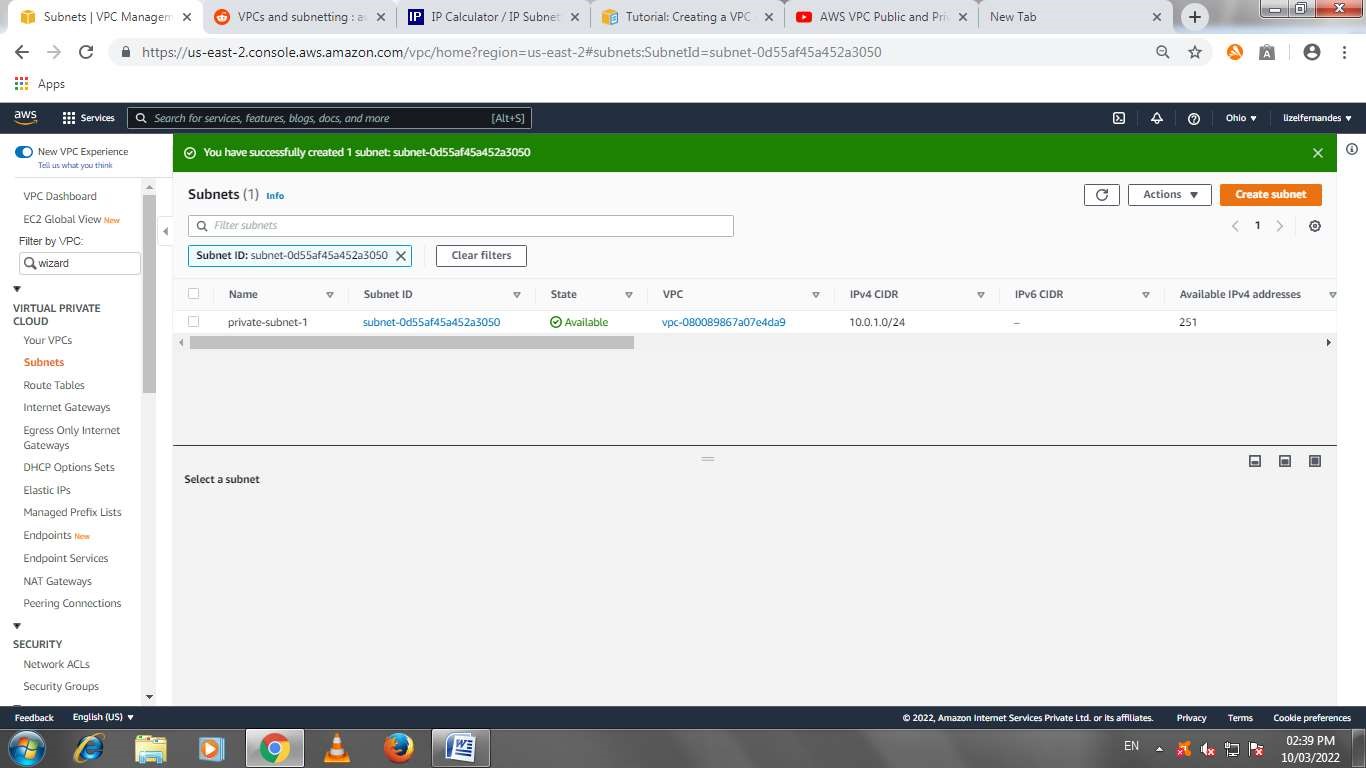
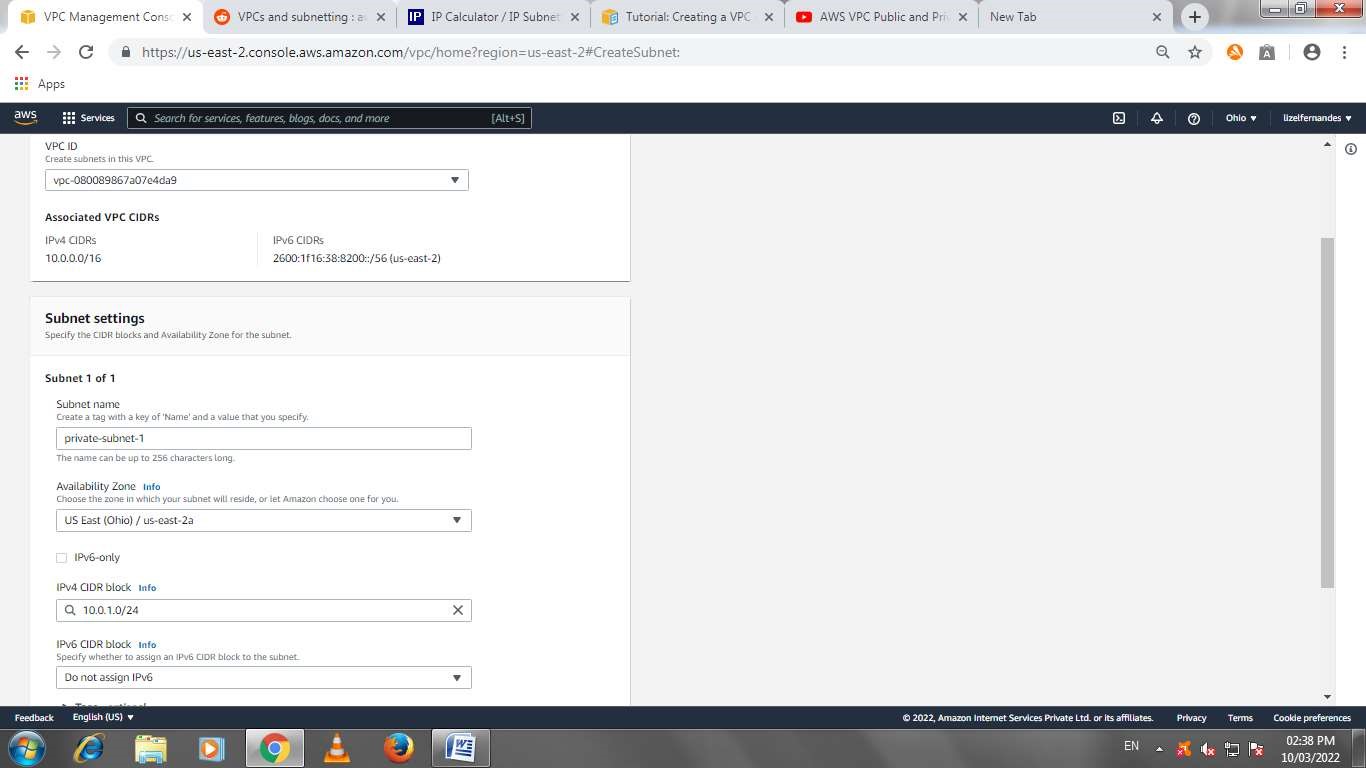
|  |  |  |
| --- | --- | --- |
| Sr. No. | Rubric | Grade |
| 1 | On time submission/completion (2) |  |
| 2 | Preparedness (2) |  |
| 3 | Skill (4) |  |
| 4 | Output (2) |  |

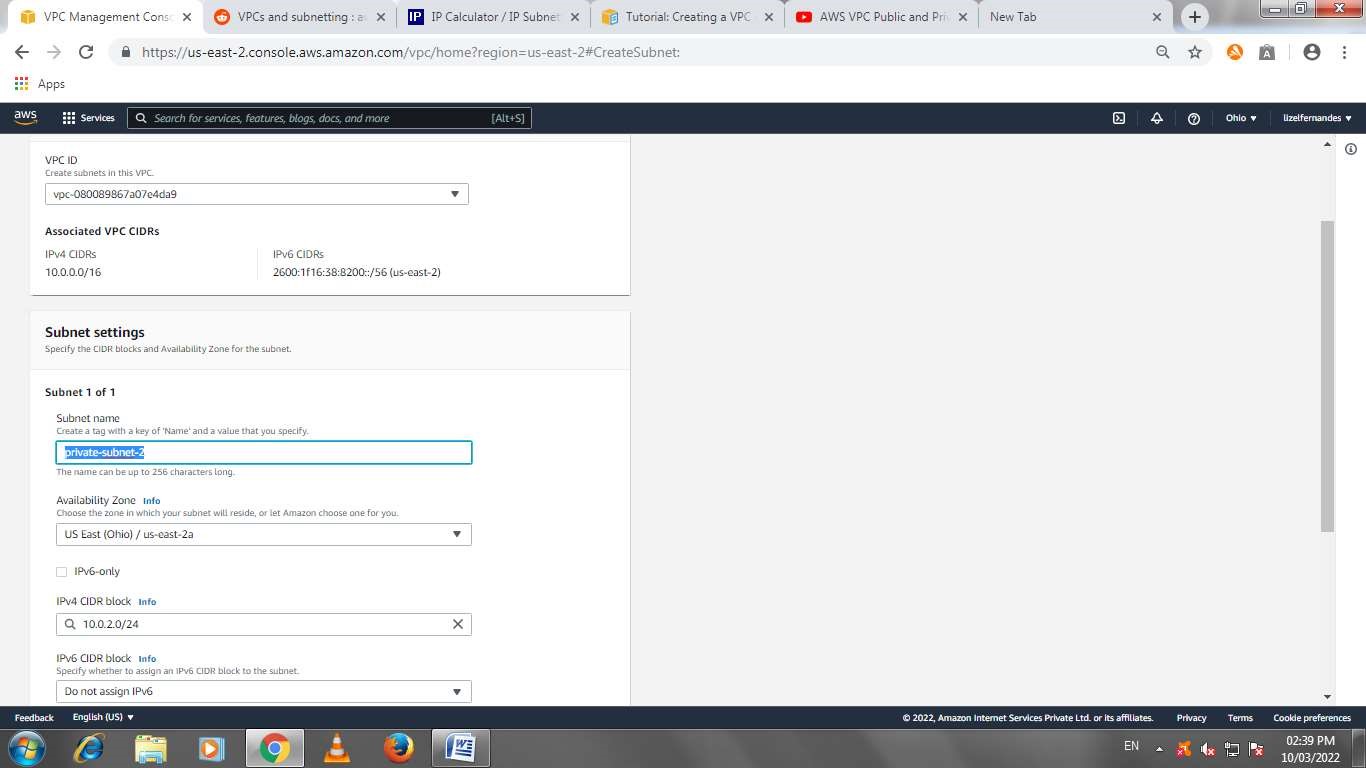
Signature of the Teacher

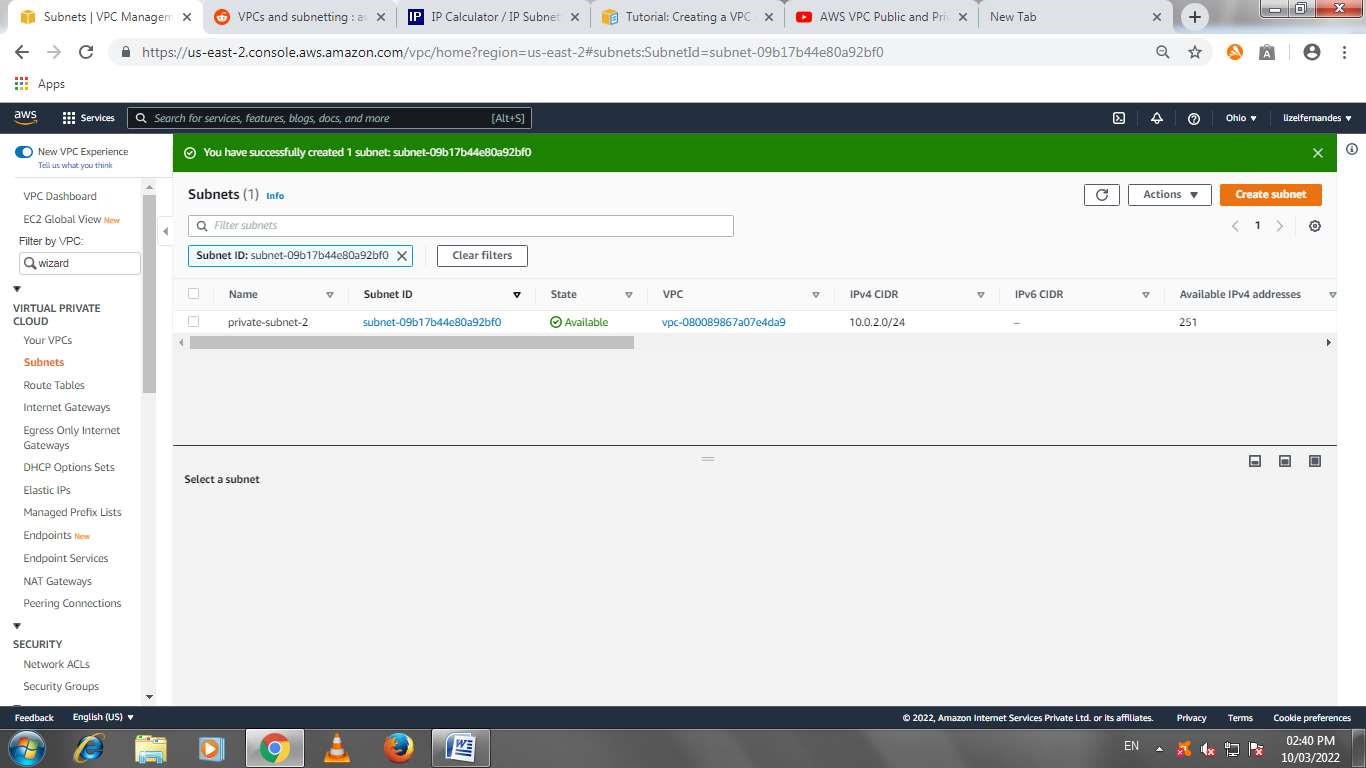
AWS VPC Configuration

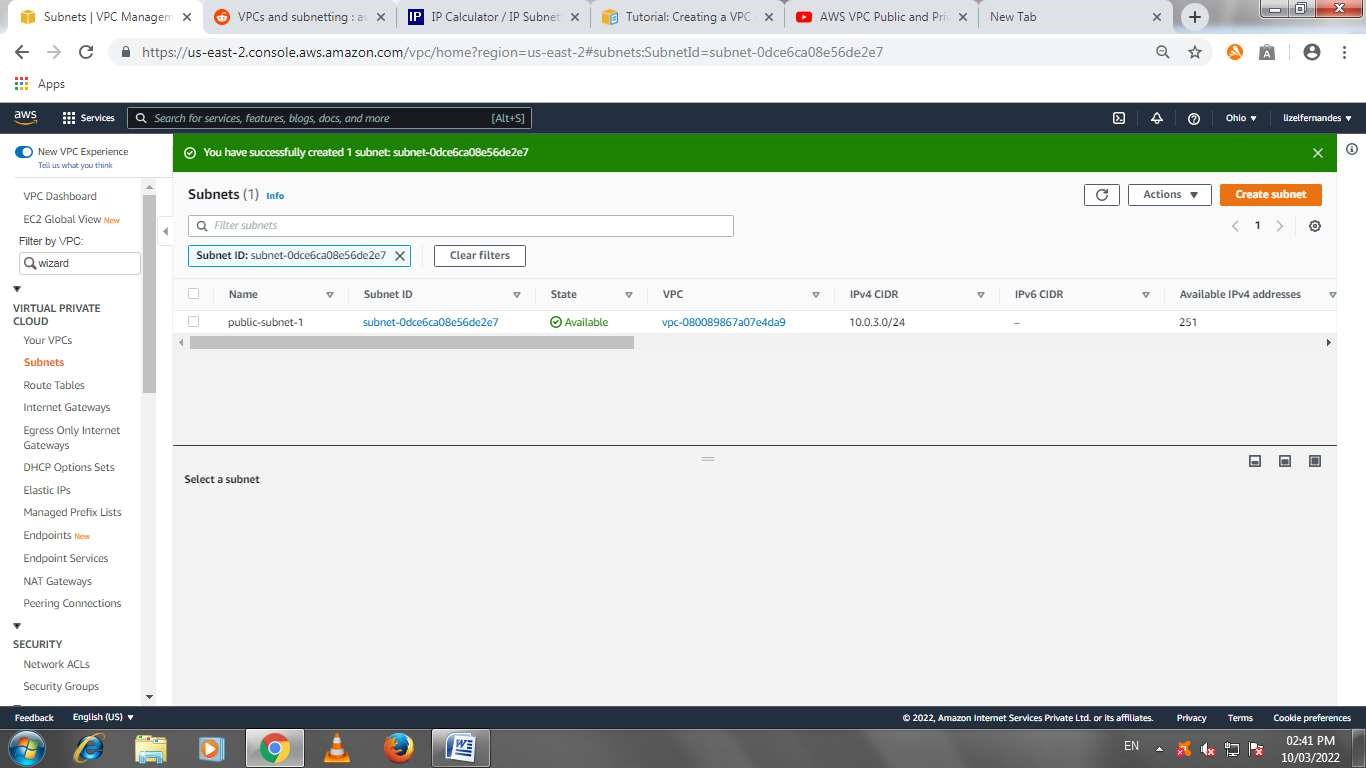
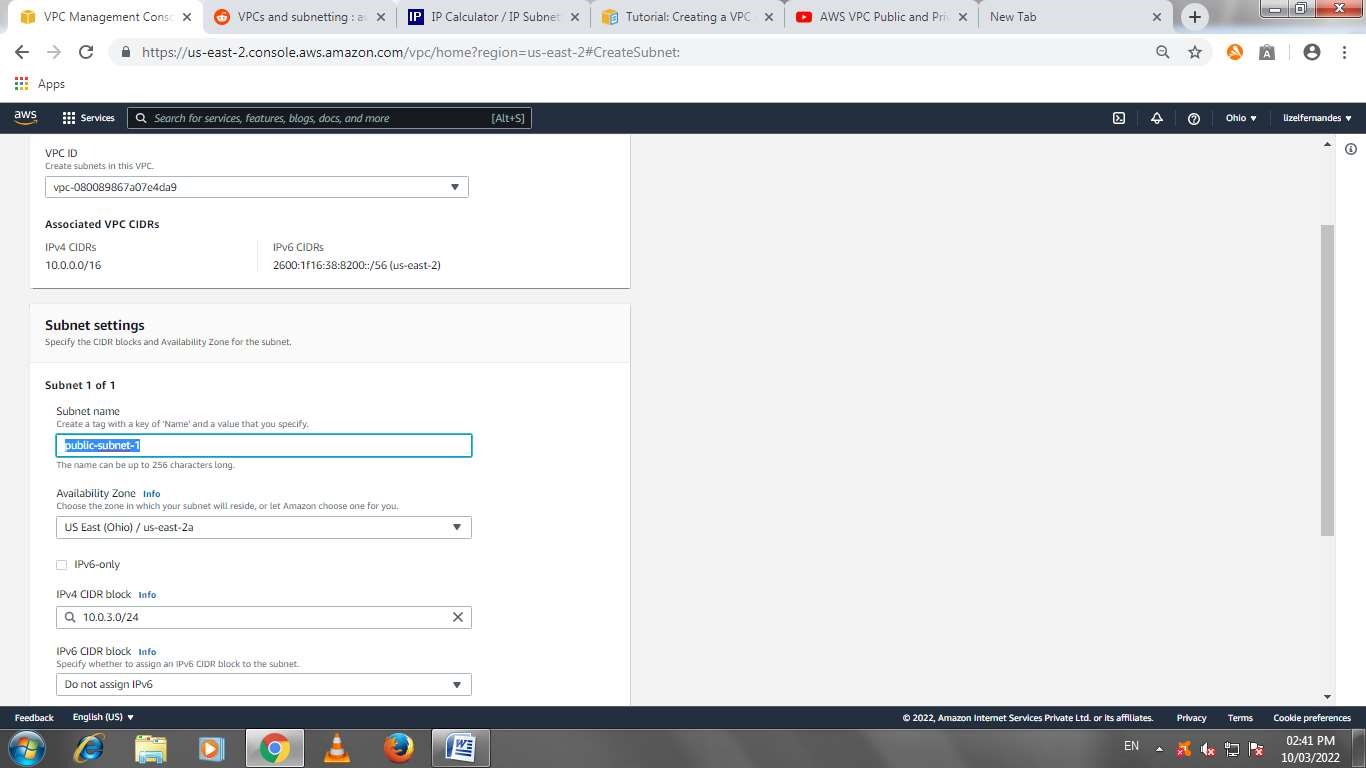
Steps to create a VPC

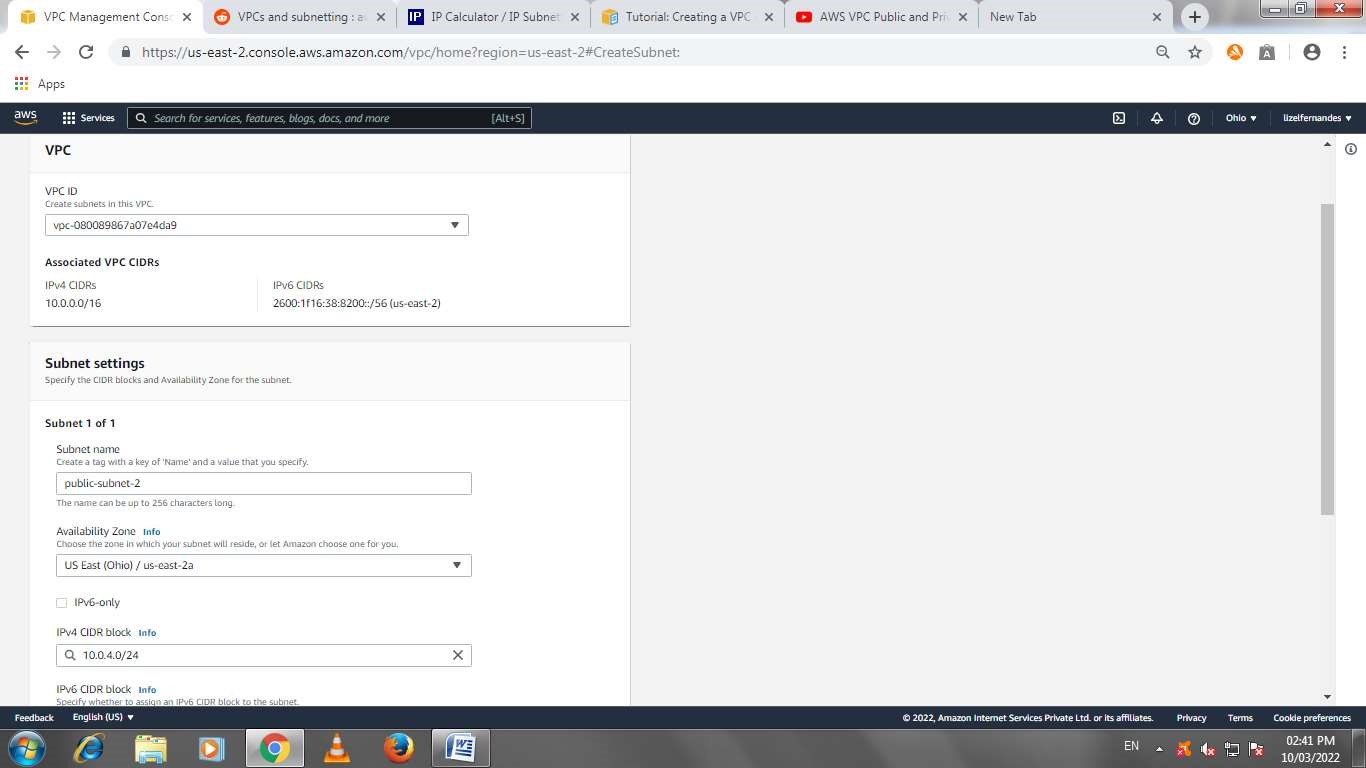
* Create VPC and public and private subnets
* Create Internet Gateway and attach to VPC
* Create public and private routing tables
* Set public routing table for IG
* Add subnet association (public subnet) in public routing table
* Create NAT Gateway in public subnet
* Set private routing table for NAT
* Add subnet association (private subnet) in private routing table  Create EC2 instances for public and private subnets

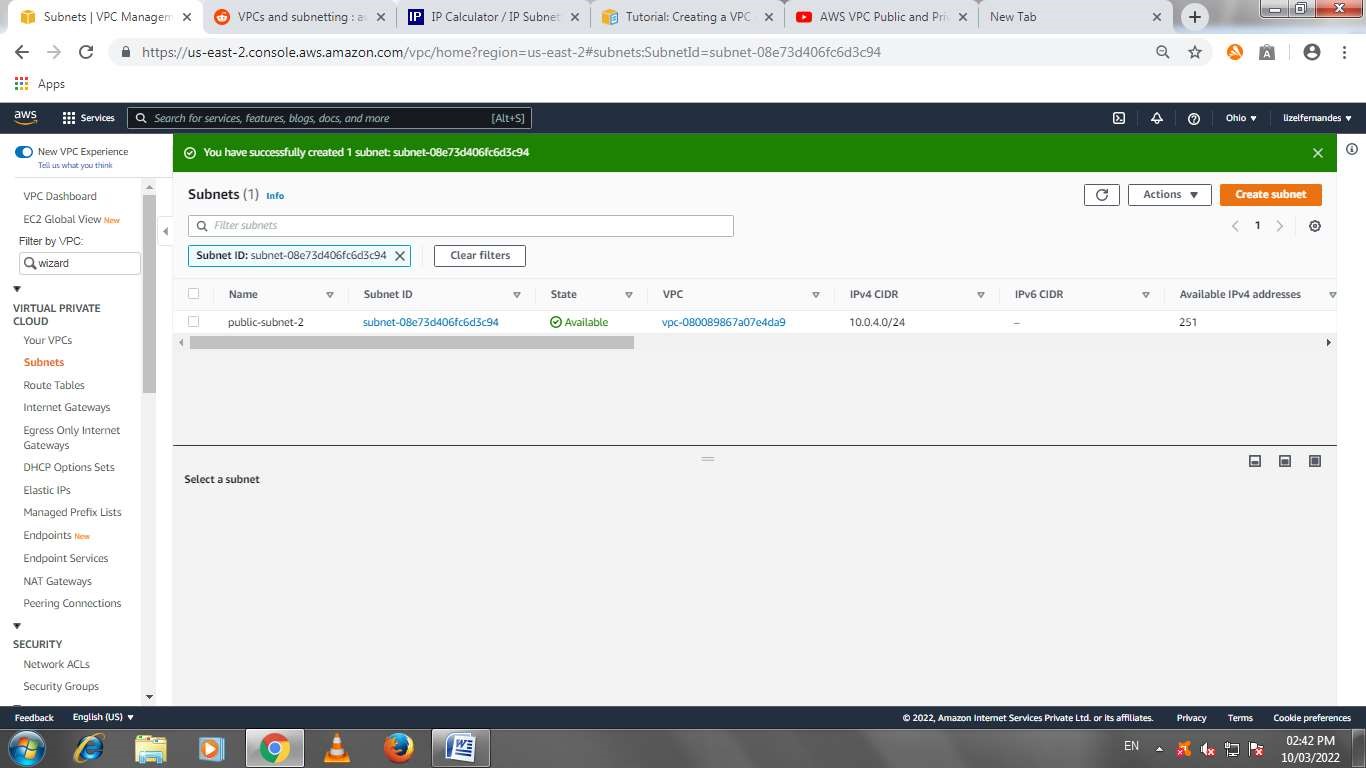


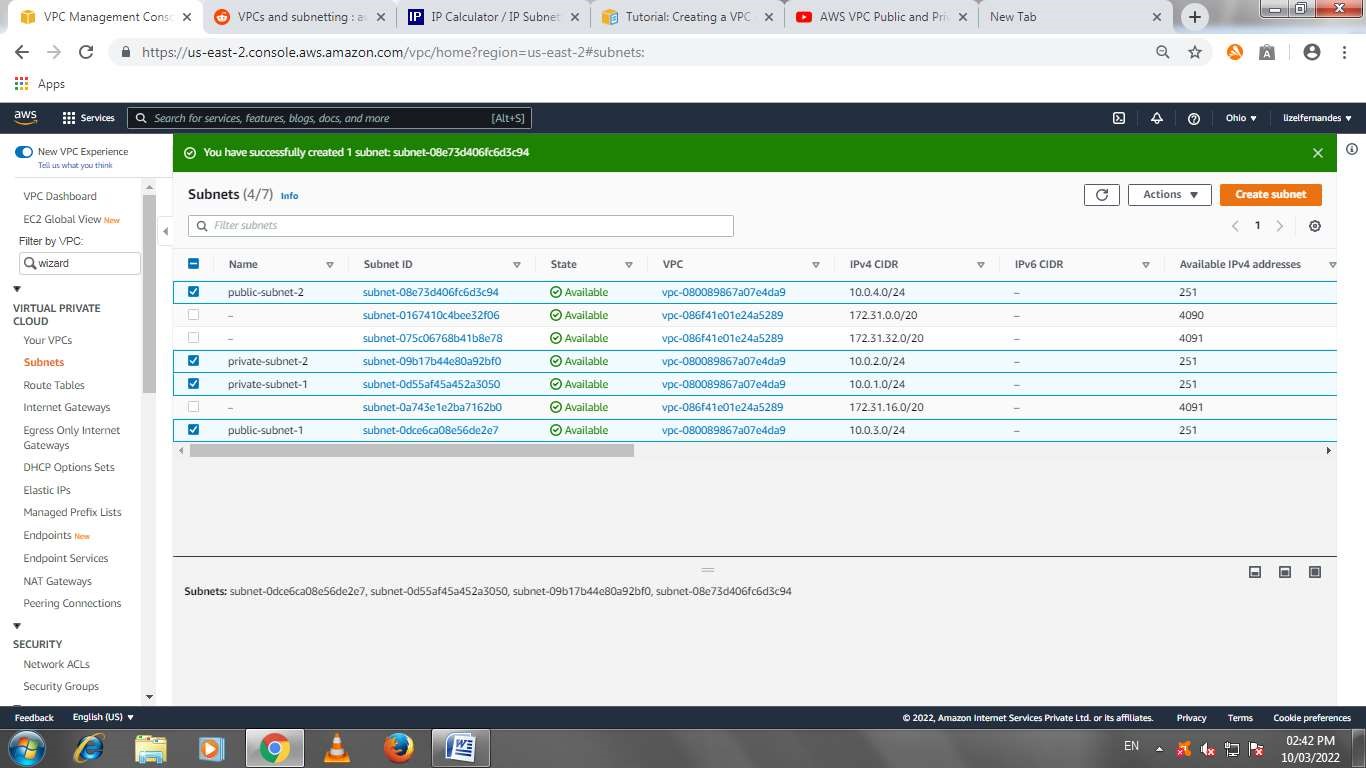








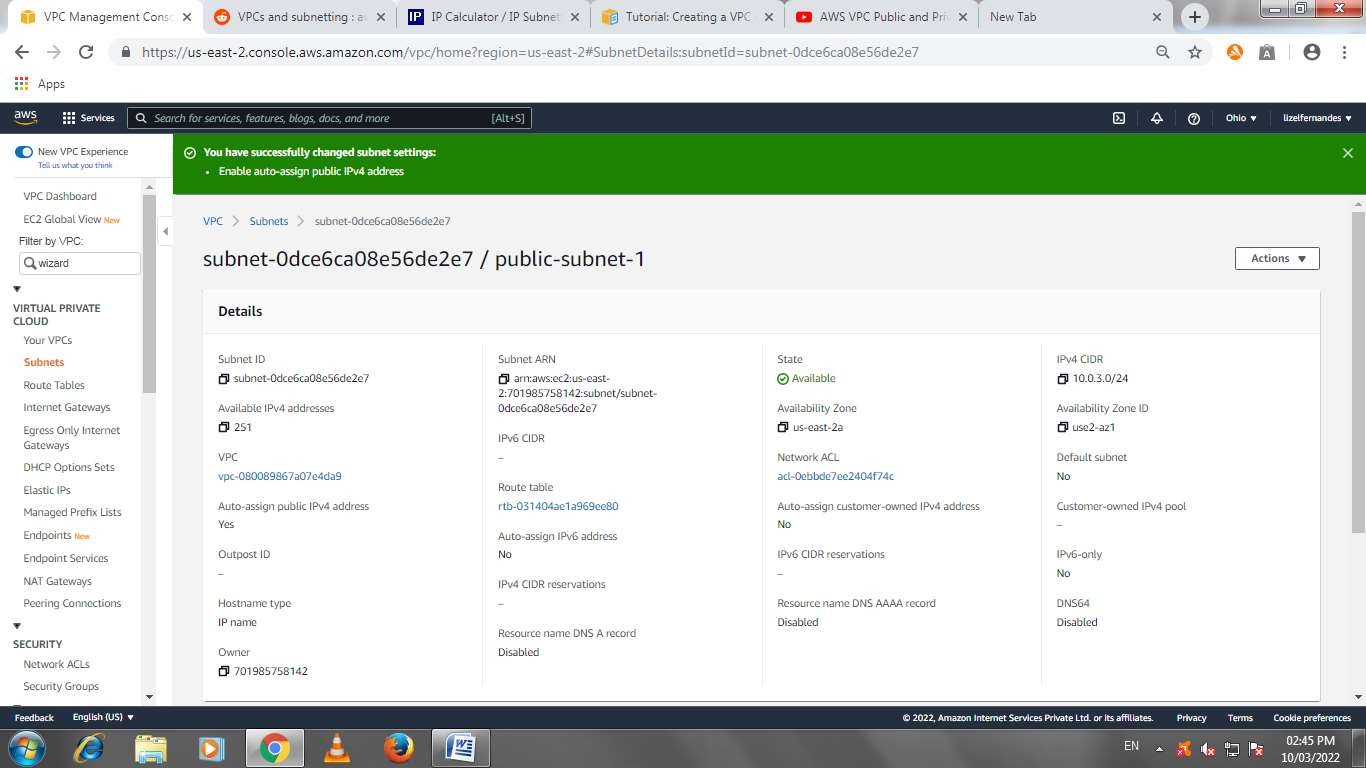




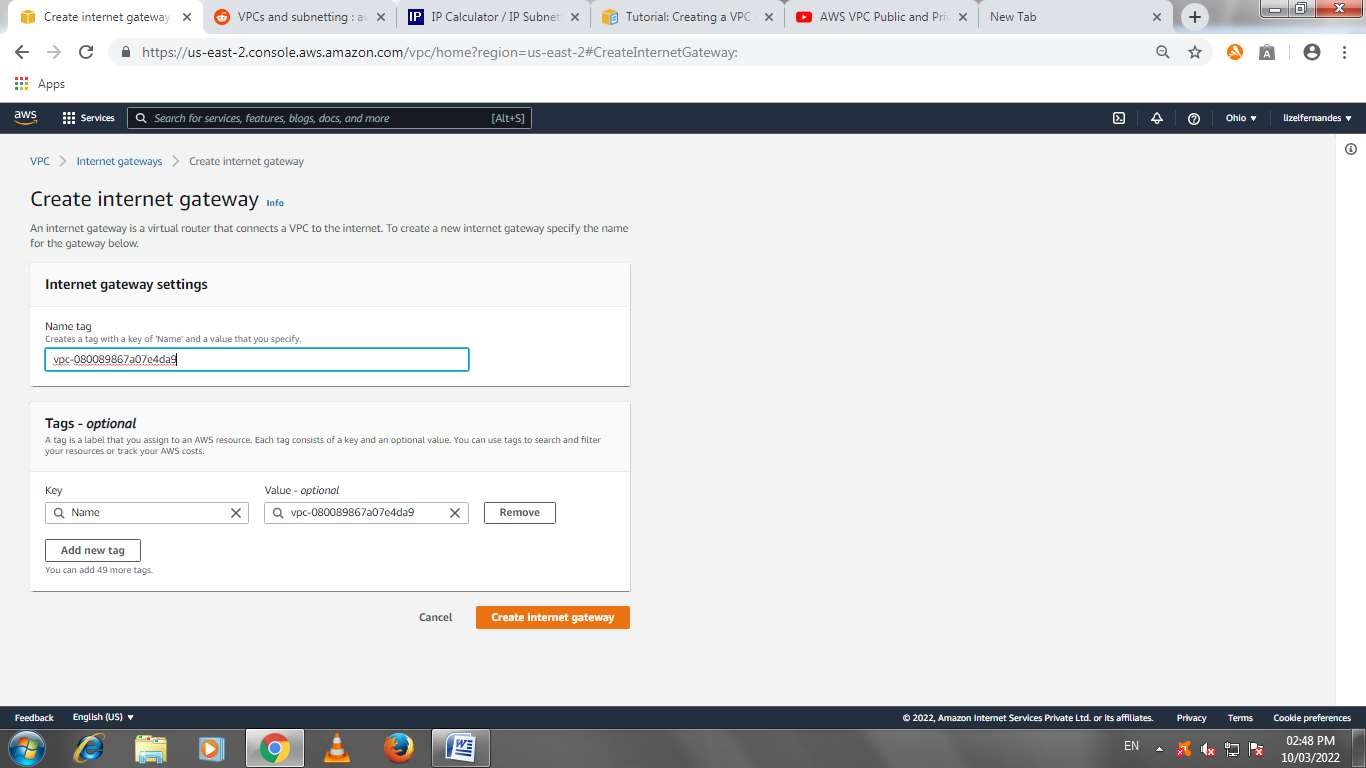
Auto assign enable for public subnet 2

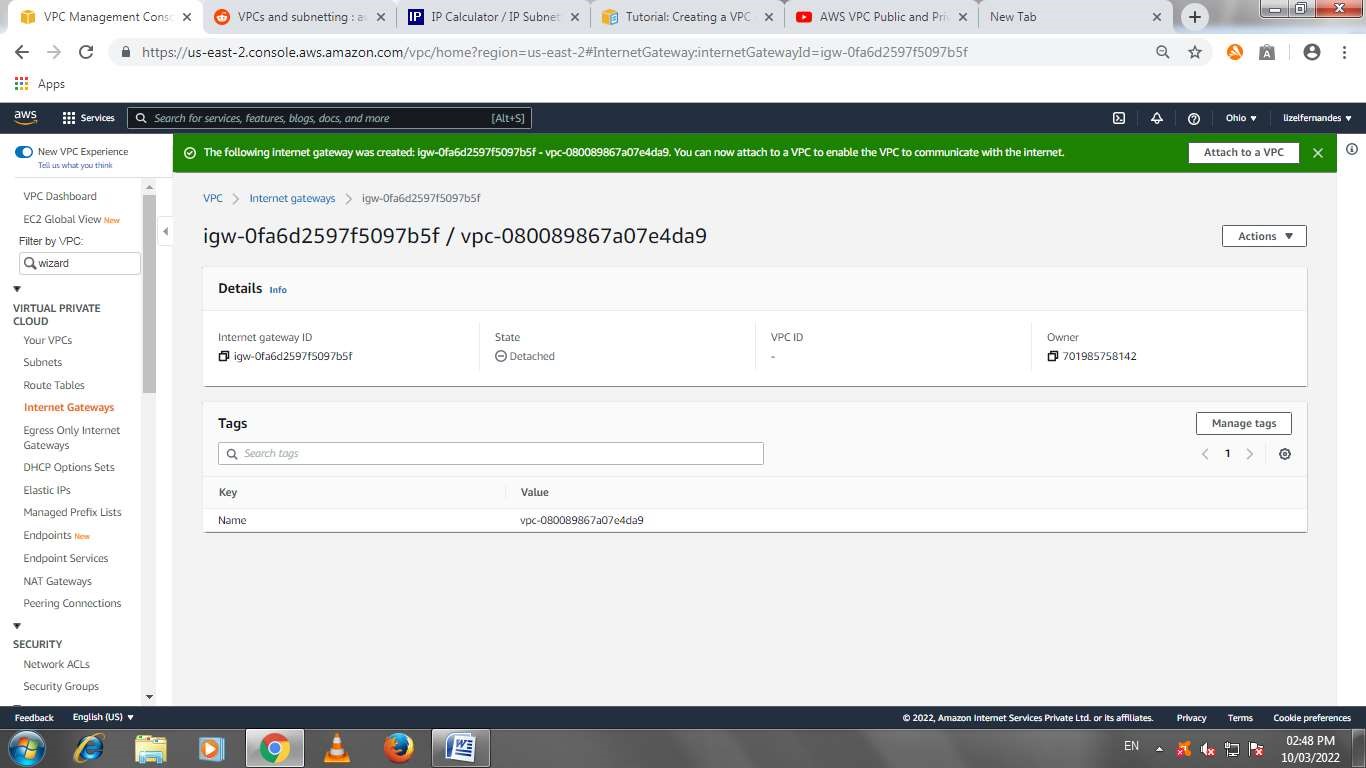


Auto assign enable for public subnet 1

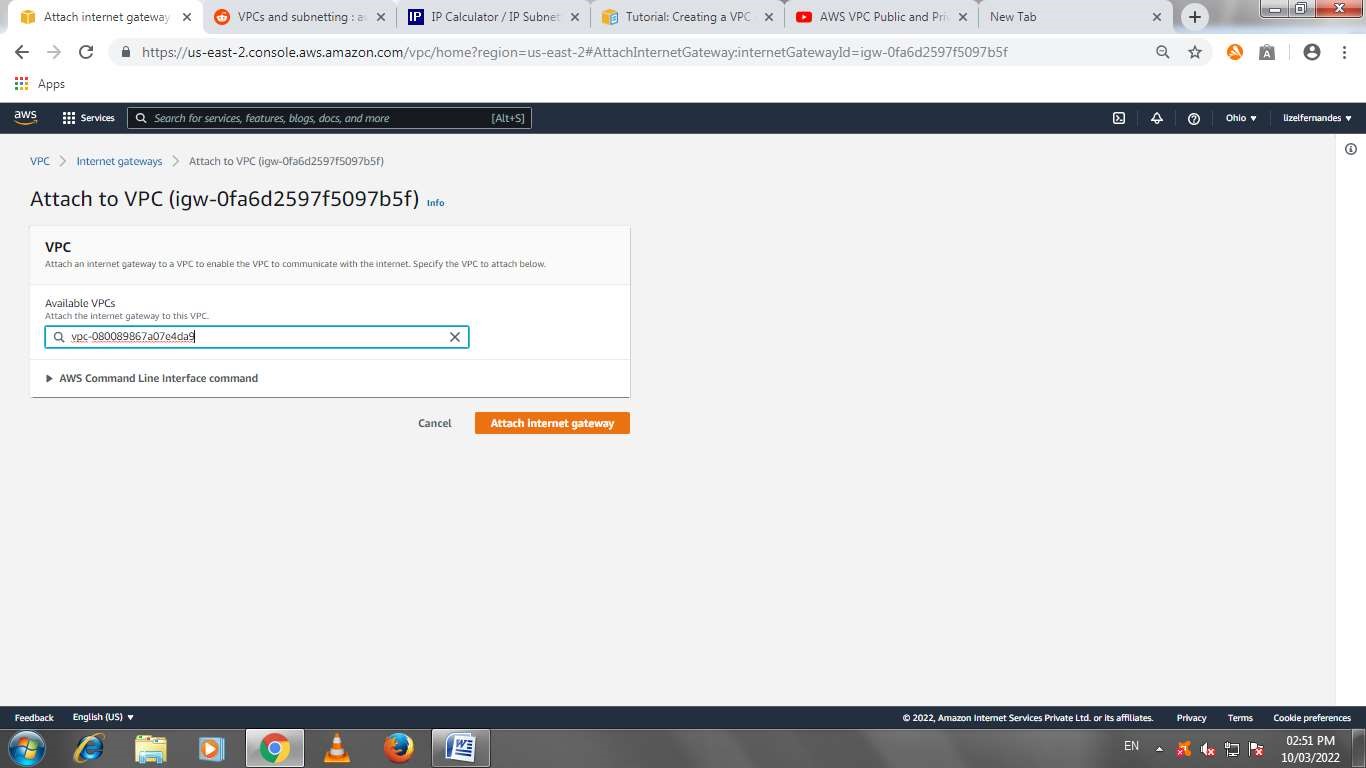


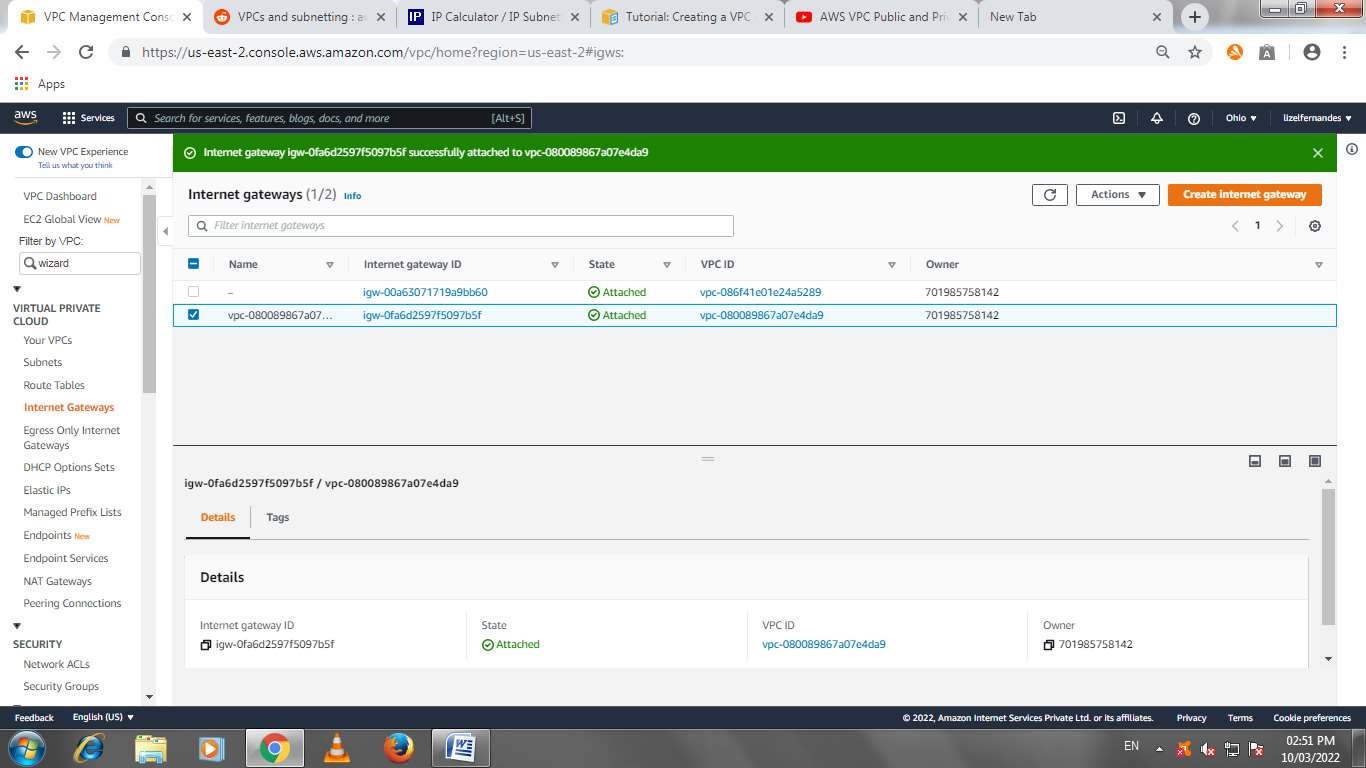
Internet gateway



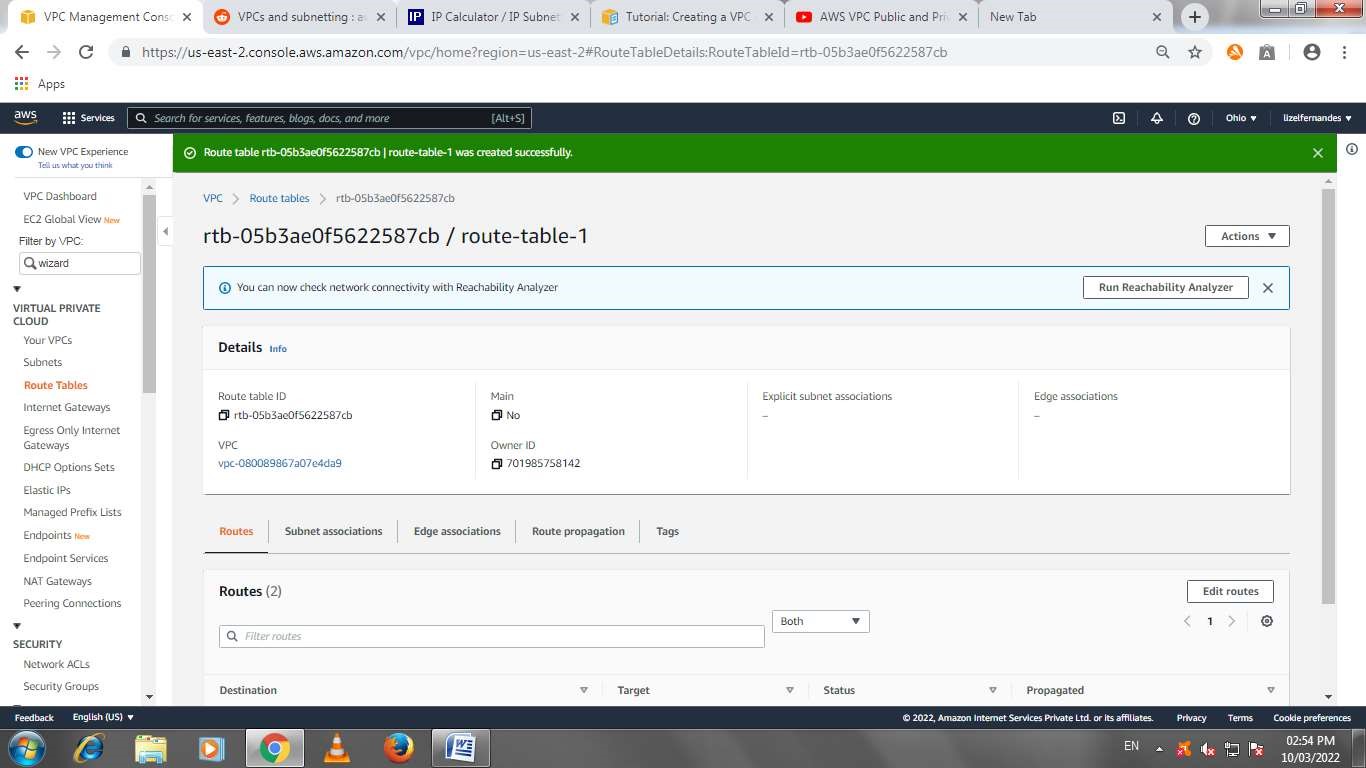


Internet gateway attached to vpc

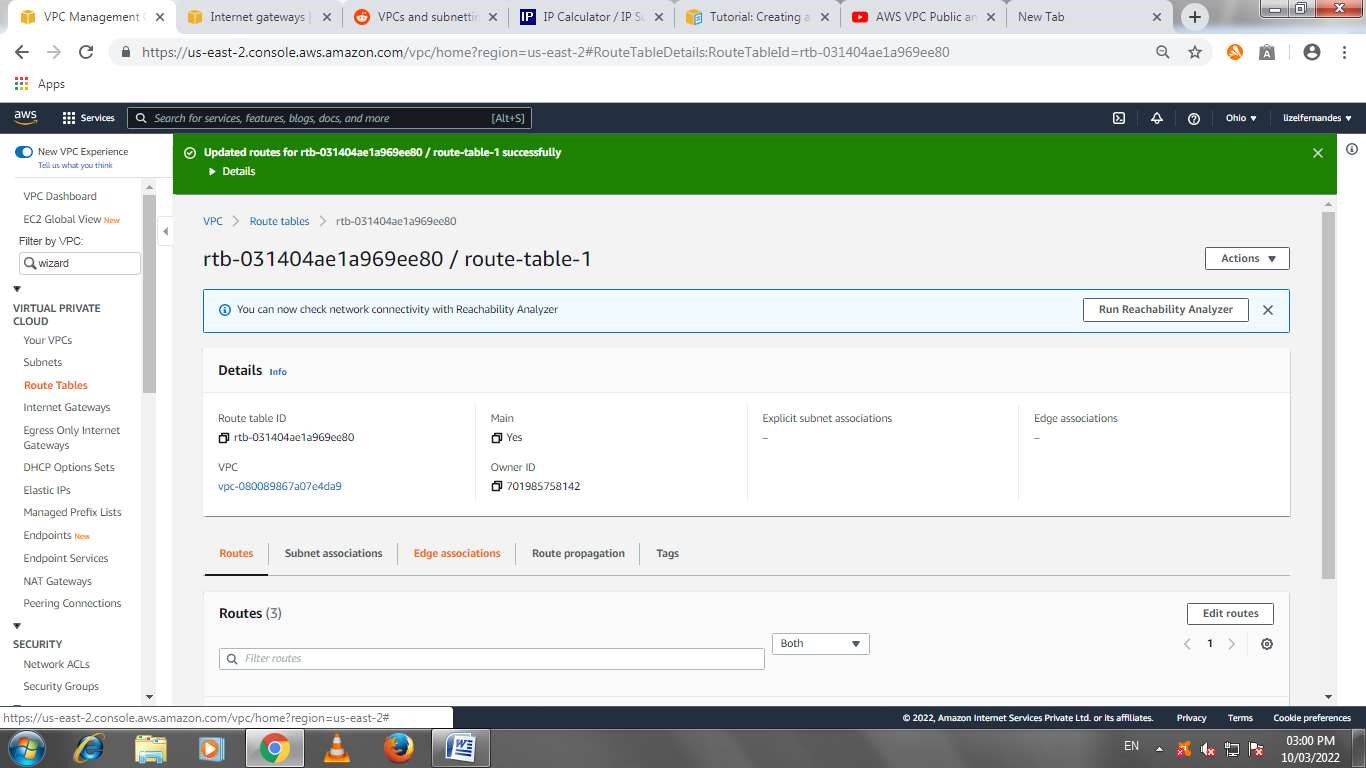
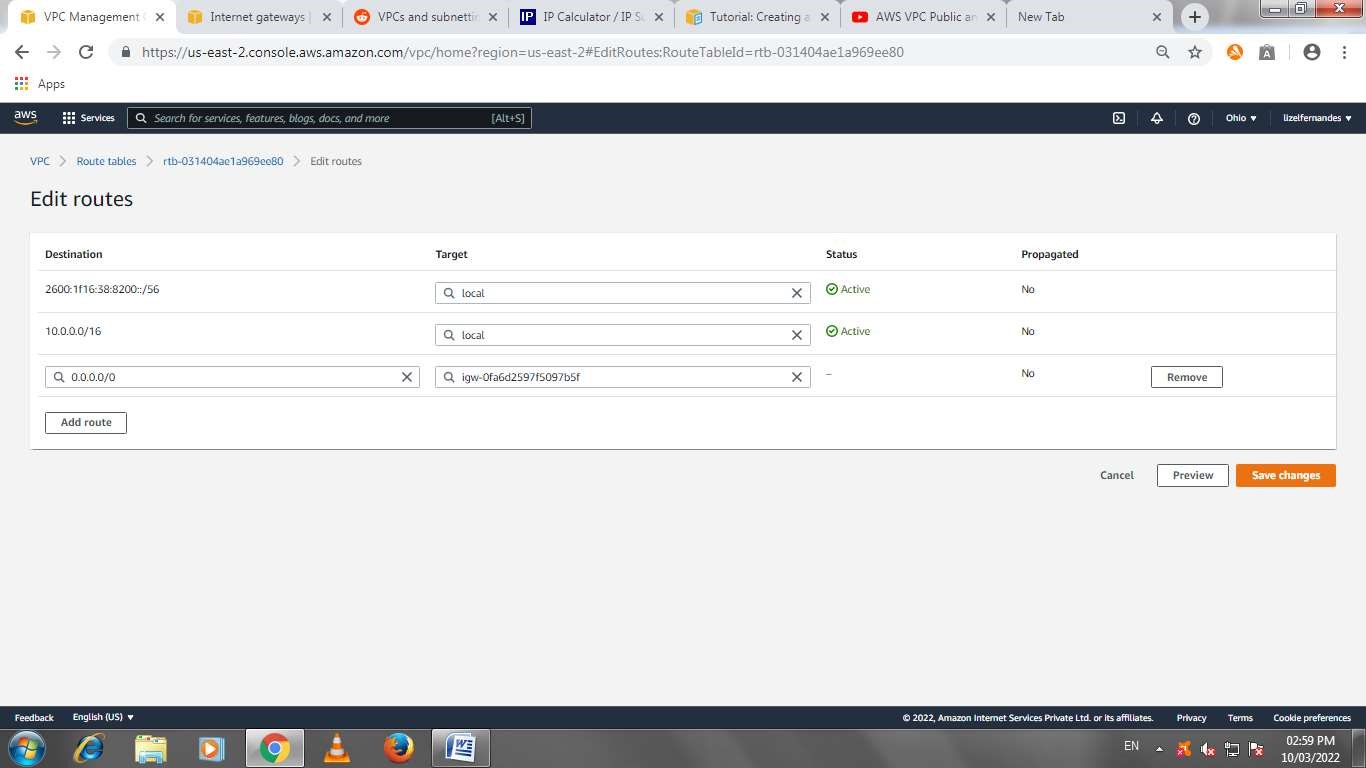




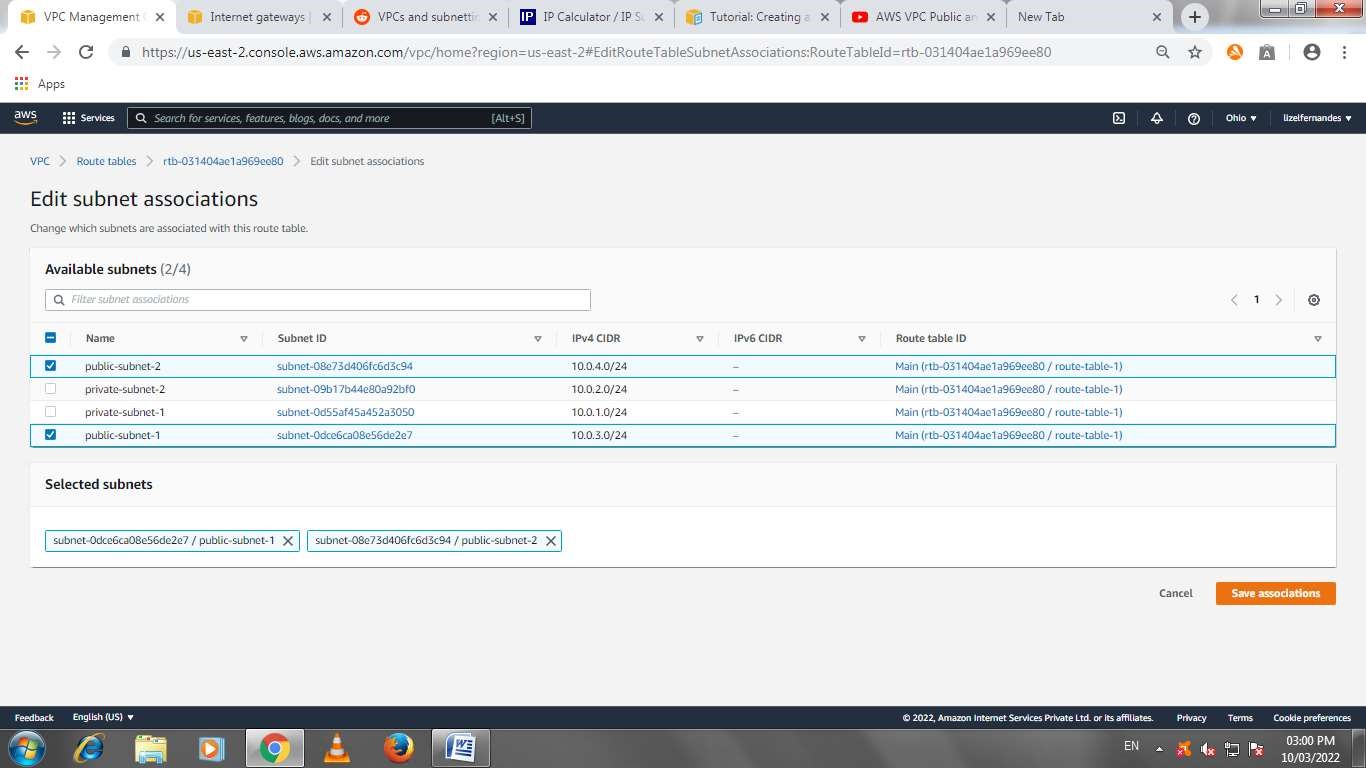
Route table creation



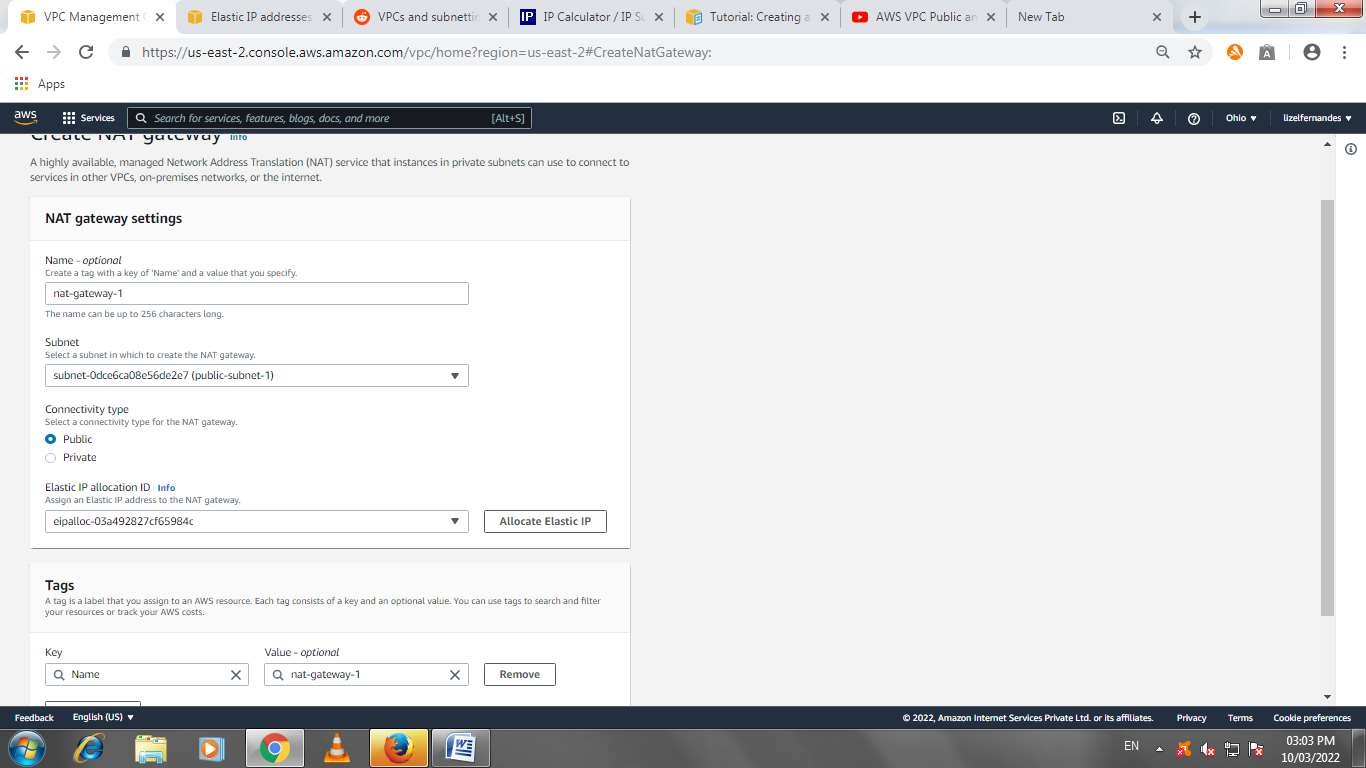
Adding internet gateway

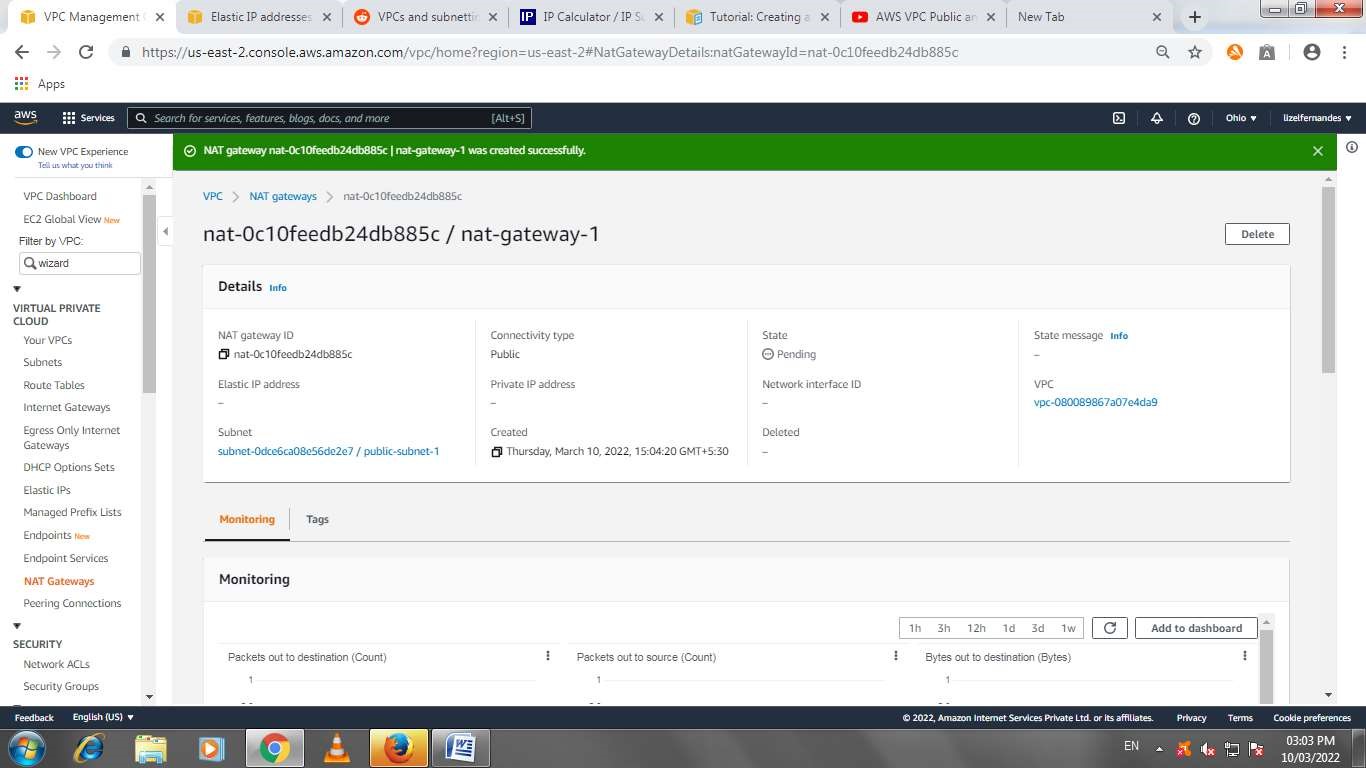


Adding public subnets to the route table

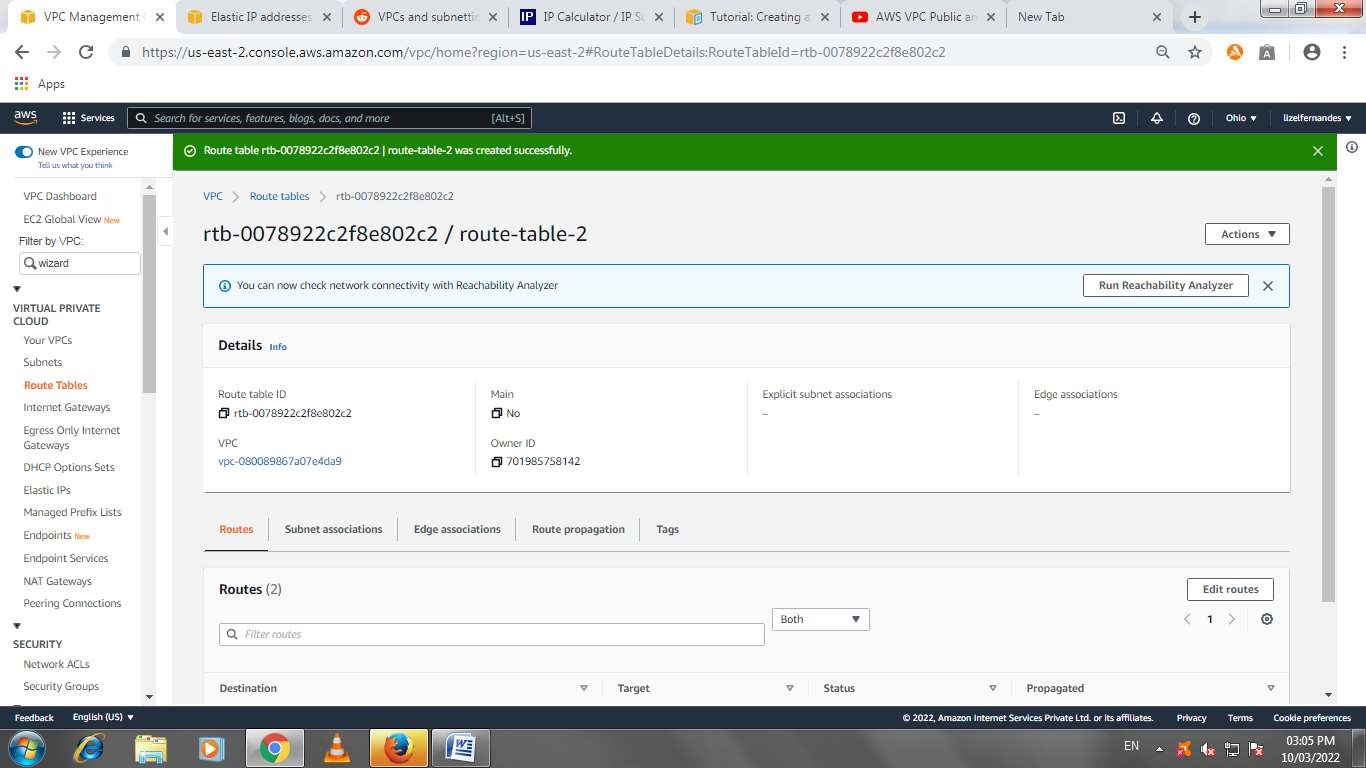


Nat gateway creation

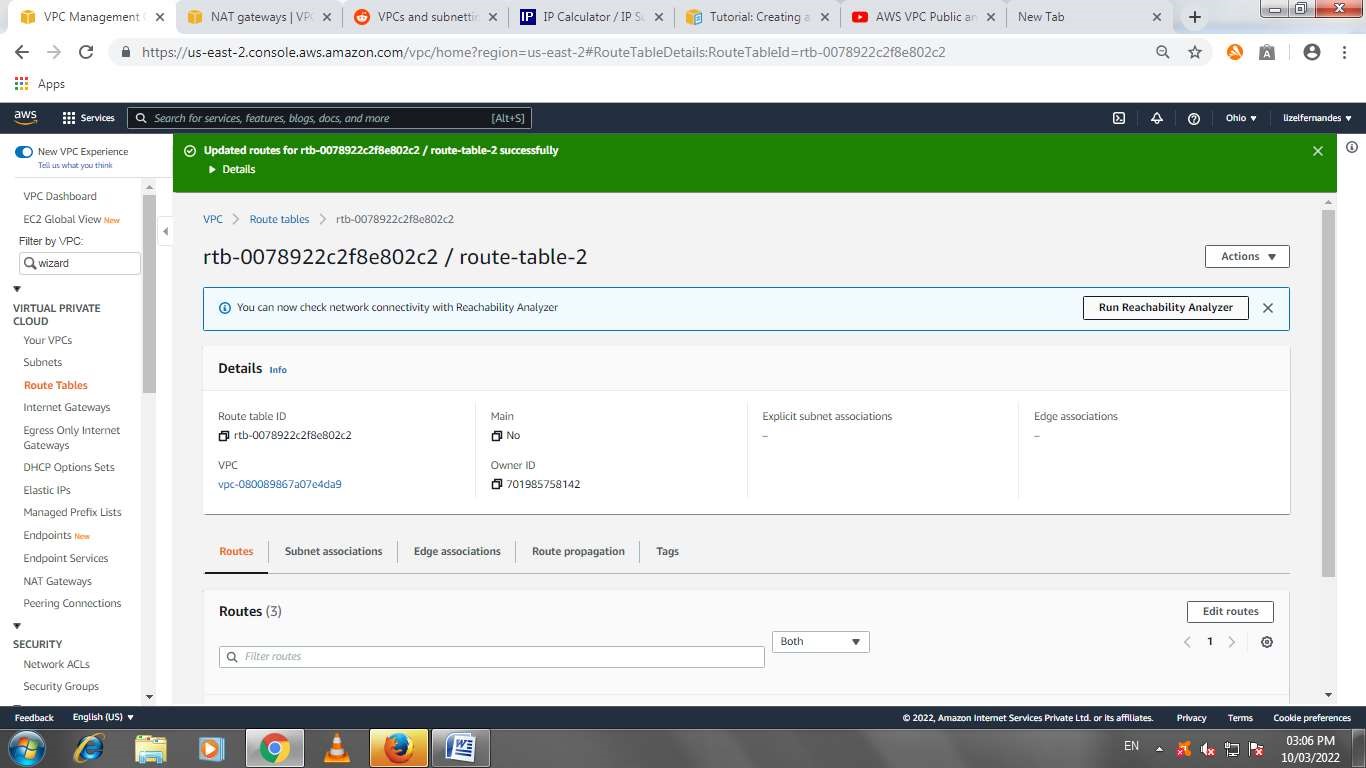
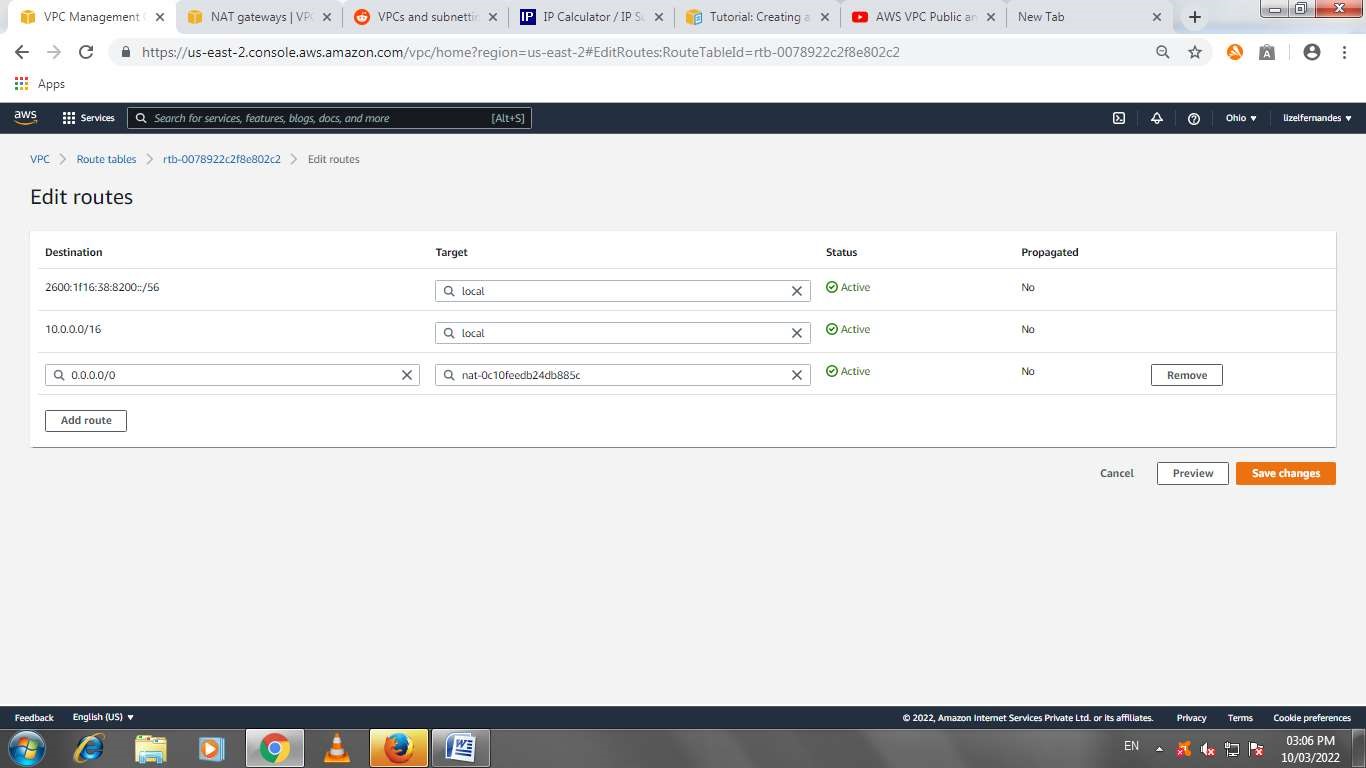




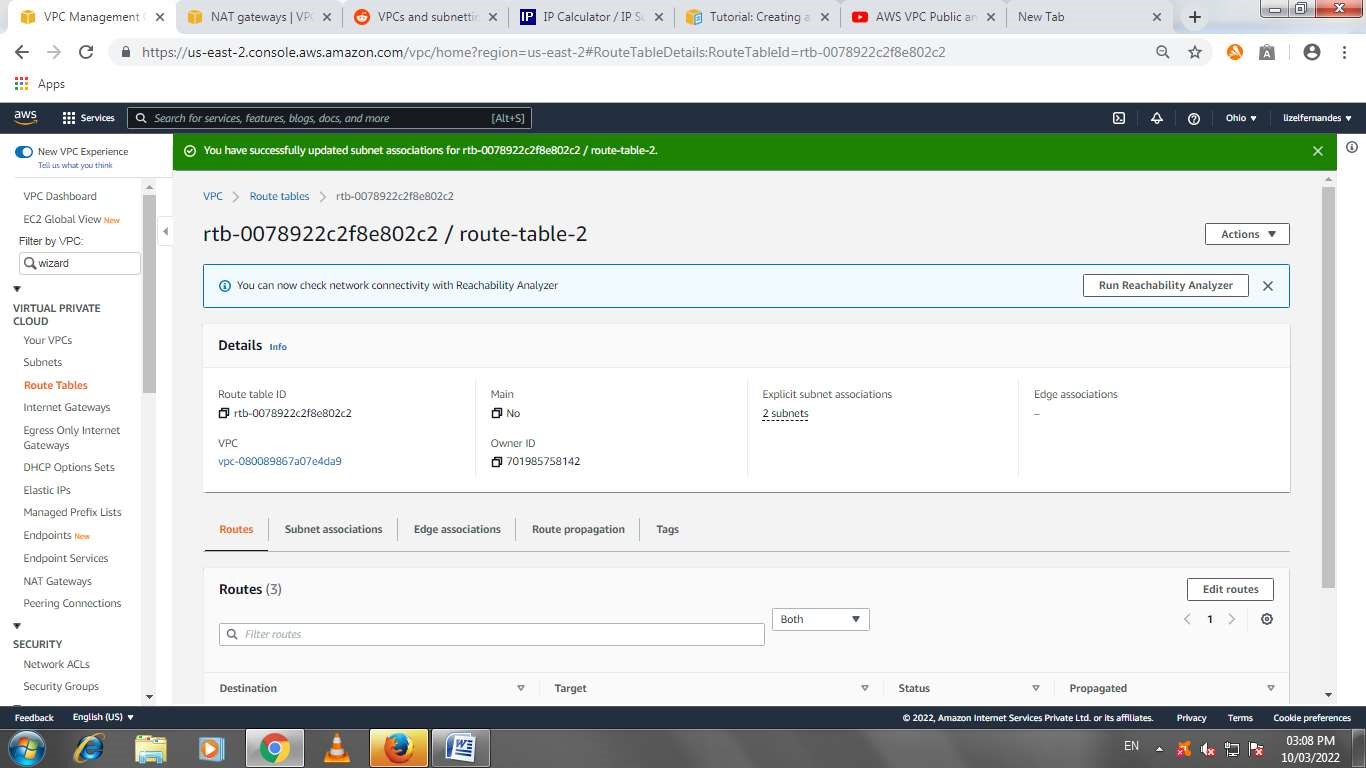
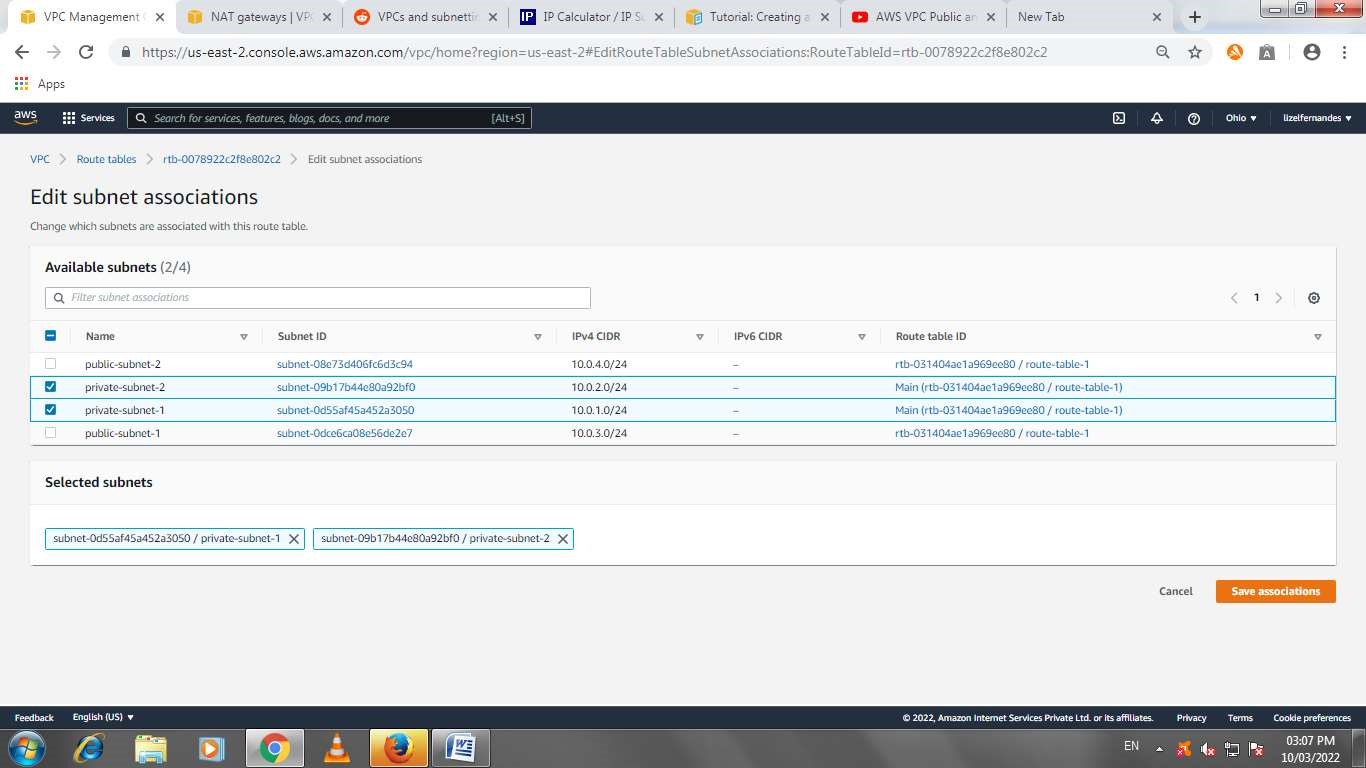
Route table 2 creation



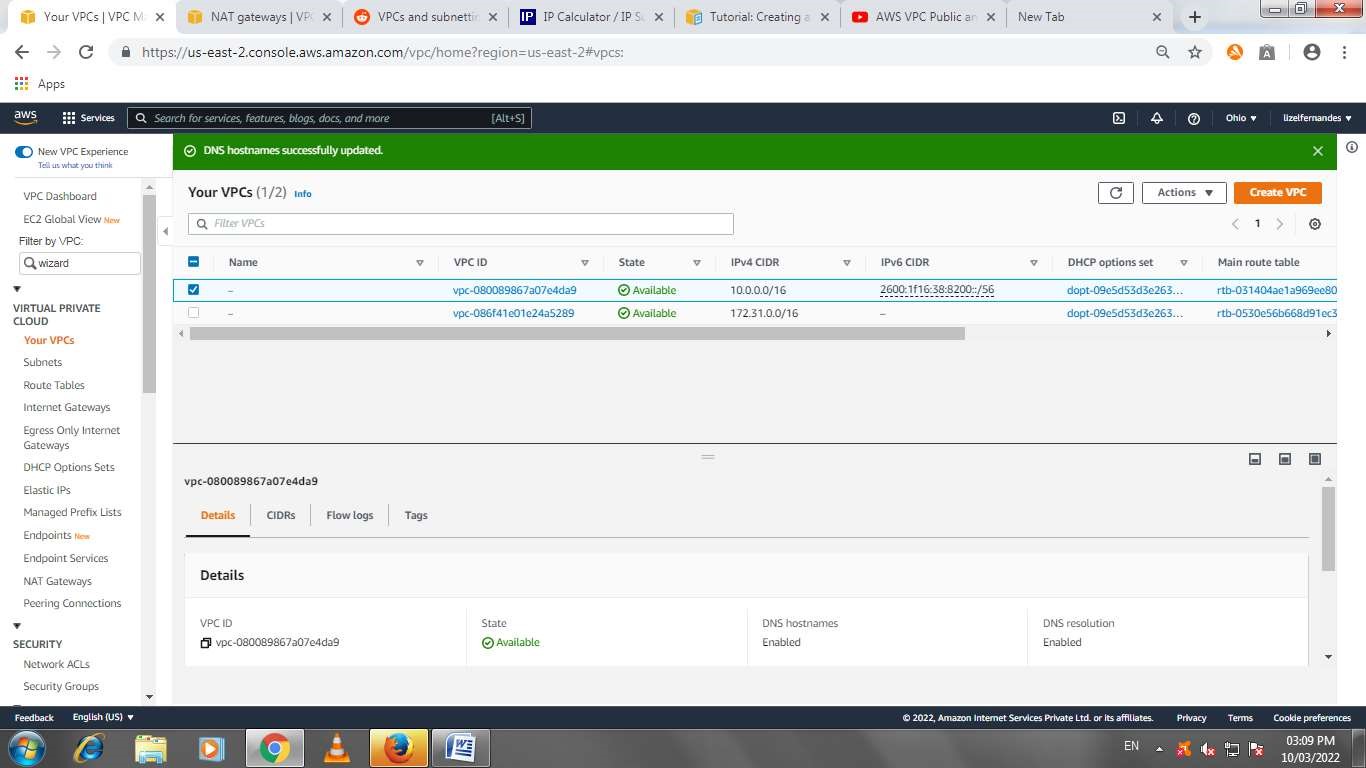
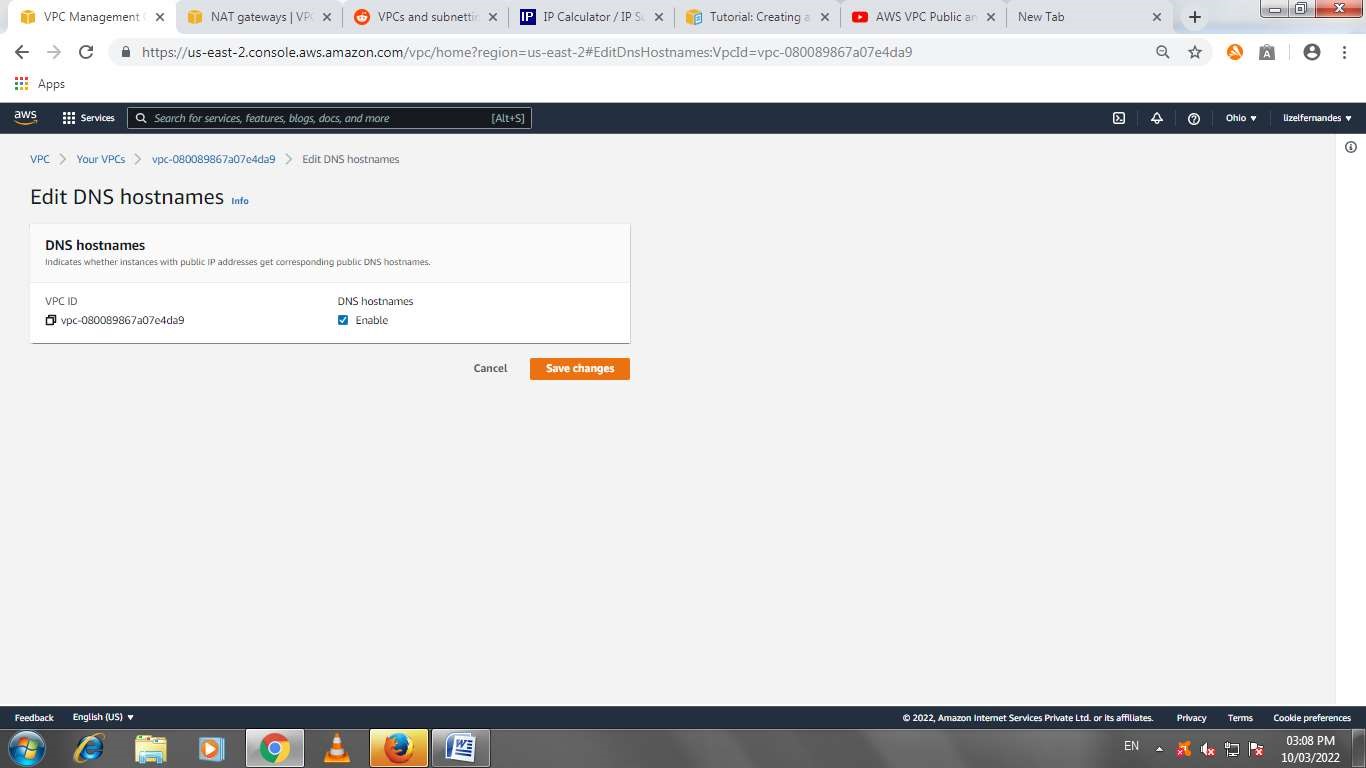
Adding nat gateway for the private subenests



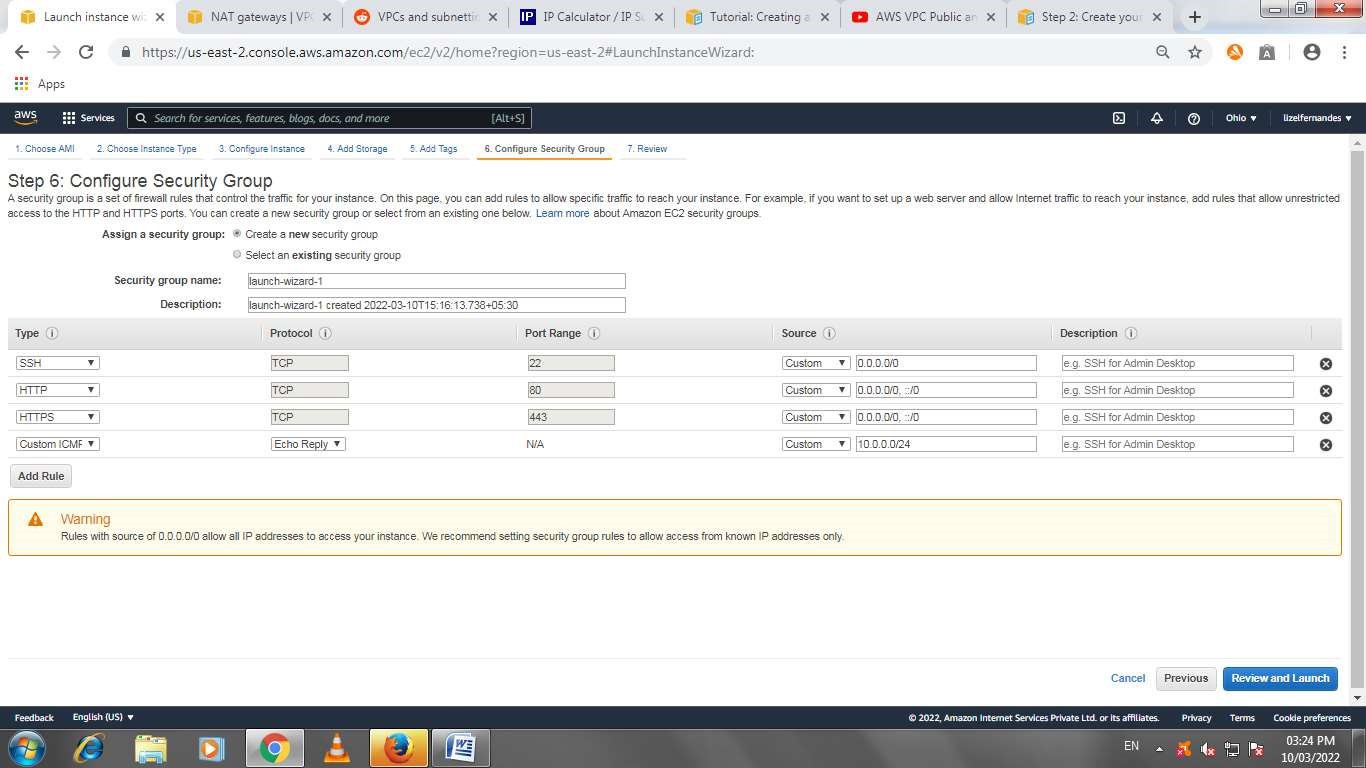
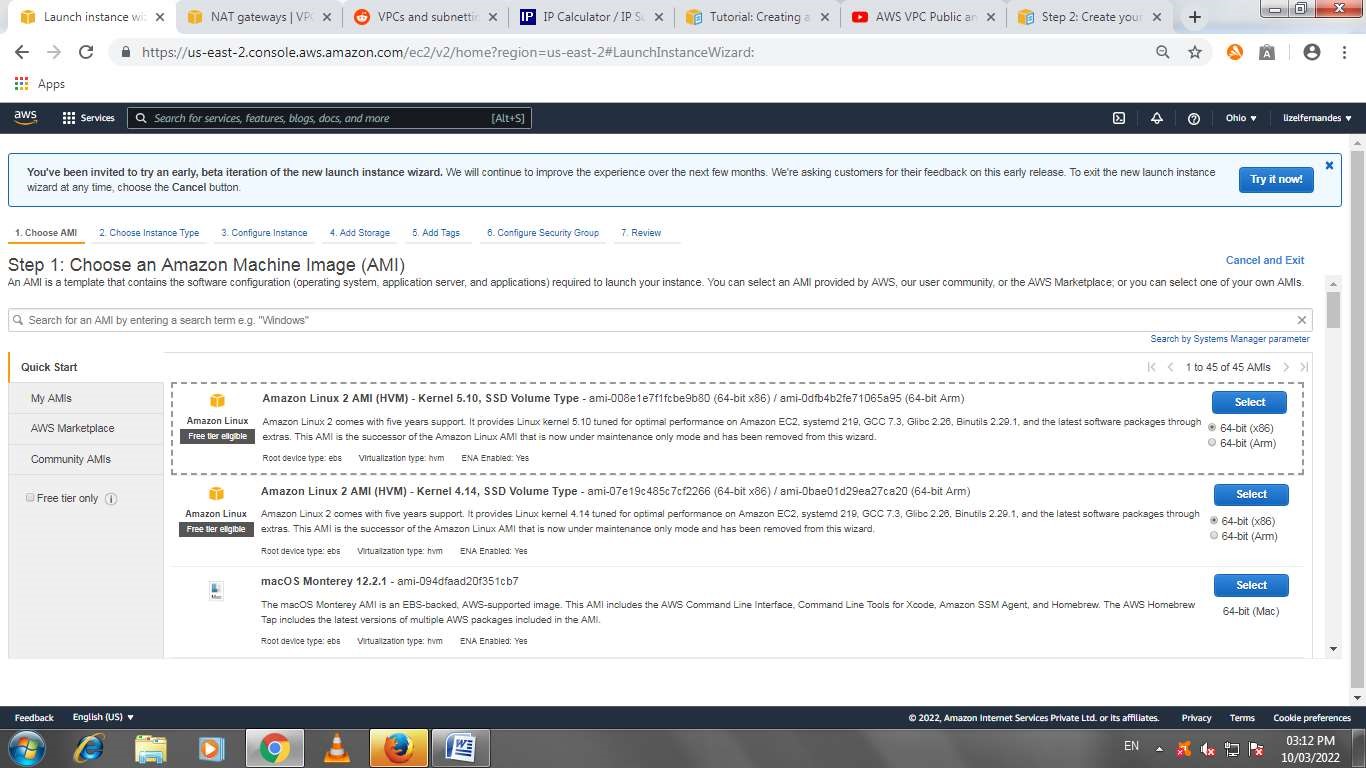
Adding association for the private subnets (route table for private subnets)



Enable dns for the vpc



Create ec2 instance and connections for new instances

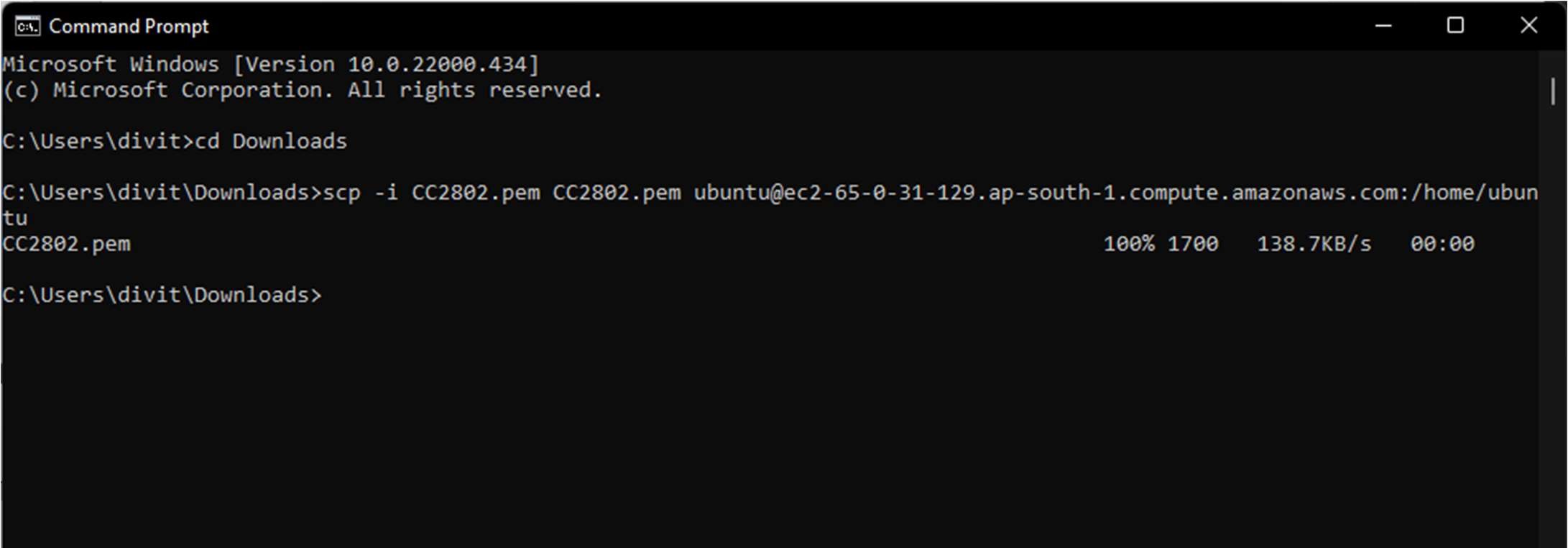


To enable internet on private instance we must do the following:

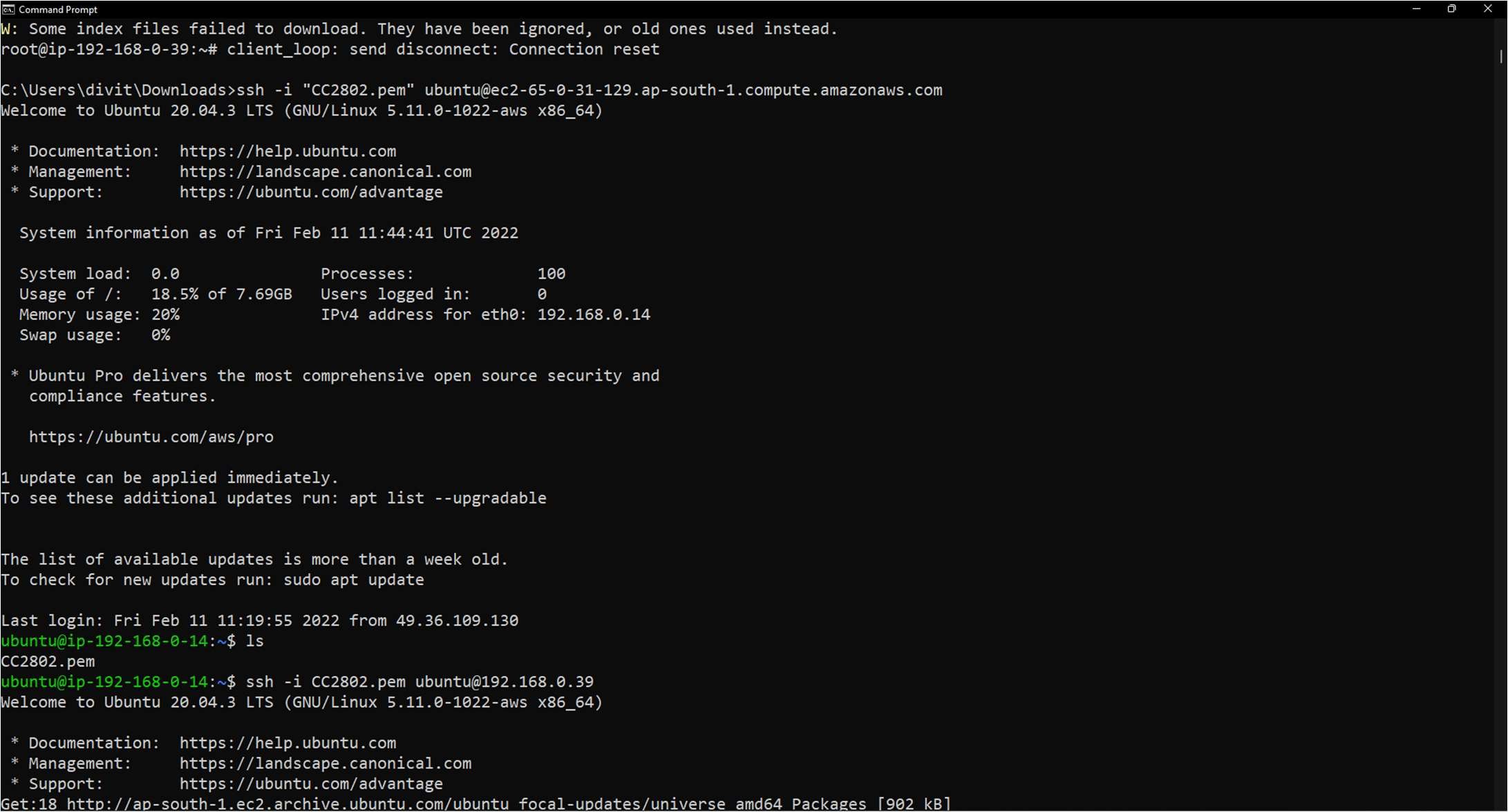
* Go to the folder where the keypair is stored for the instance
* Copy the file from your machine to the public instance scp -i keyname.pem keyname.pem ubuntu@public ipv4 dns:/home/ubuntu

(e.g., scp -i CC2802.pem CC2802.pem ubuntu@ec2-65-0-31-129.ap-south1.compute.amazonaws.com:/home/ubuntu)

(Note: if you created instance using linux put ec2-user instead of ubuntu everywhere)



* Now connect your public EC2 instance through SSH or putty



* You can check if the .pem file is copied by ‘ls’ command  Set the permissions for the file:

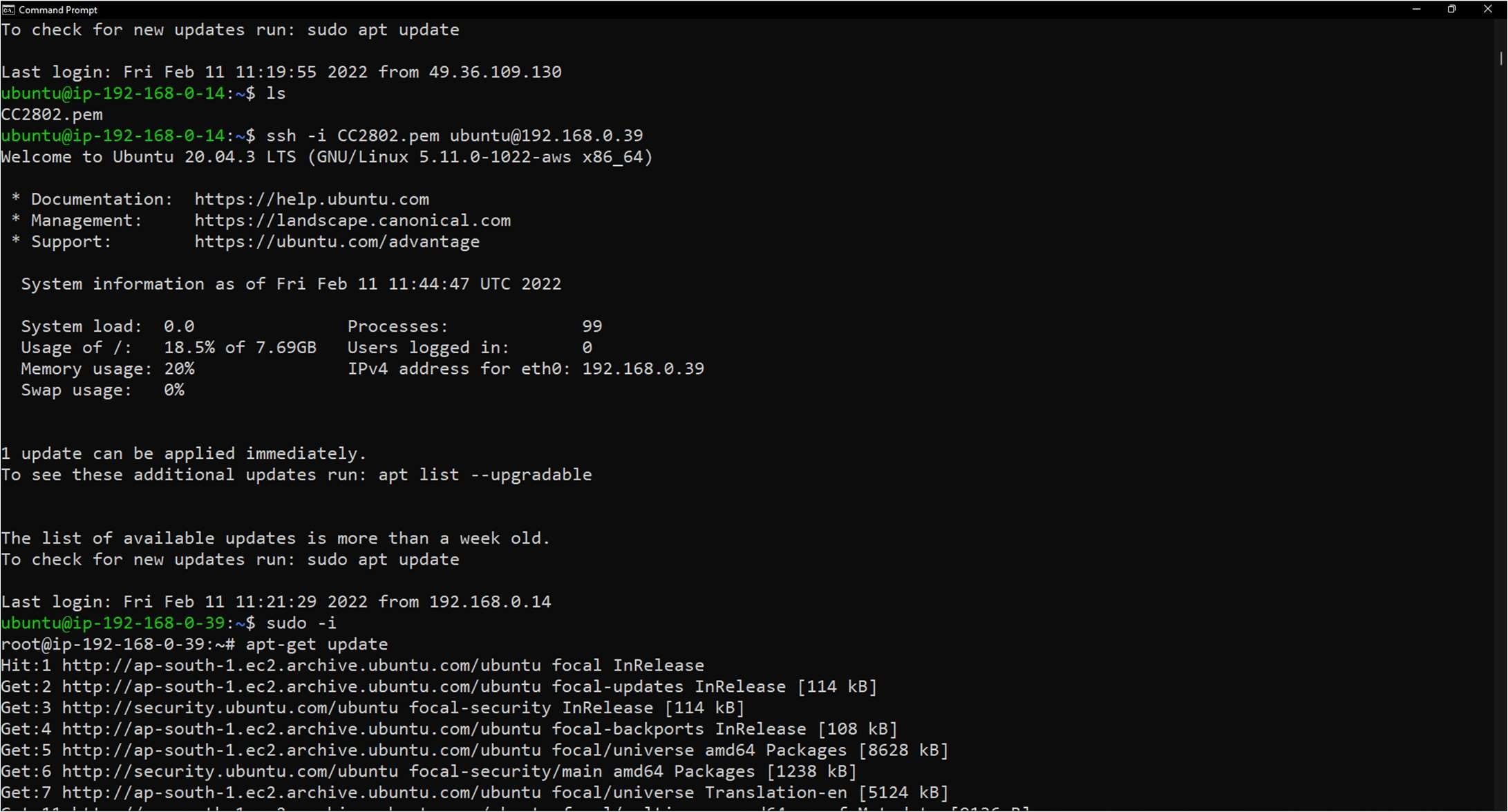
chmod 400 keyname.pem

* To connect private instance, enter the command:

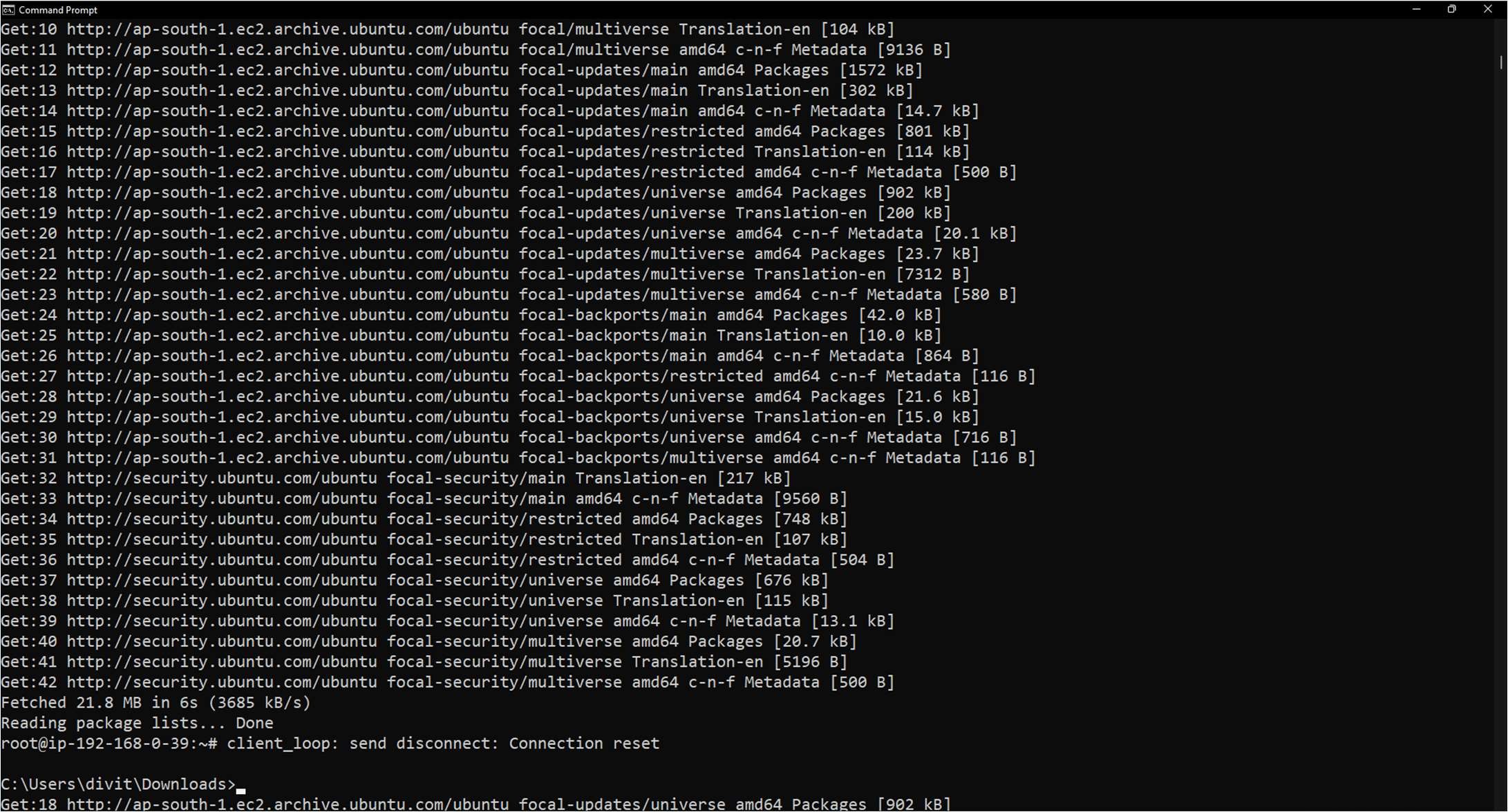
ssh -i keyname.pem ubuntu@private ip address (private instance)

(Note: you can see that the ip address is changed from public to private after this)

* To check if connection is correct: sudo -i -> apt-get update



* This will show that the connections are correct and now you can install any dependencies you want from the private instance



Experiment 7: Amazon Web Services VPC Post Lab Questions

Q1. What are the components of Amazon VPC?

In AWS the VPC cosists of the following components:-

Subnet: A segment of a VPC’s where you can place groups to isolated resources.

Internet Gateway: VPC side of a connection to utilize public Internet.

NAT Gateway: A highly available, managed Network Address Translation (NAT) service for your resources in a private subnet to access the Internet.

Virtual private gateway: The Amazon VPC side of a VPN connection for secure transactions.

Peering Connection: To route traffic via private IP addresses between two peered VPCs.

VPC Endpoints: Enables private connectivity for your service in AWS without using an Internet Gateway, VPN, Network Address Translation (NAT) devices, or firewall proxies.

Egress-only Internet Gateway: A stateful gateway that provides egress only access for IPv6 traffic from the VPC to the Internet.

Q2. How do I get started with Amazon VPC?

To get started using Amazon VPC, you can launch an EC2 instance into your default VPC and default public subnets. Your default VPC is suitable for getting started quickly with Amazon VPC. To learn more about default VPCs and the default public subnets that come with the, see Default VPCs.

Step 1: View information about your default VPC

Step 2: Launch an instance into your VPC

Step 3: Connect to an E2 instance in your public subnet

Step 4: Clean up

Q3. What are the different types of VPC endpoints available on Amazon VPC?

VPC endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components.

* Interface endpoints

An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet. It serves as an entry point for traffic destined to a service that is owned by AWS

or owned by an AWS customer or partner. For a list of AWS services that integrate with AWS PrivateLink, see AWS services that integrate with AWS PrivateLink.

* Gateway Load Balancer endpoints

A Gateway Load Balancer endpoint is an elastic network interface with a private IP address from the IP address range of your subnet. It serves as an entry point to intercept traffic and route it to a network or security service that you've configured using a Gateway Load Balancer. You specify a Gateway Load Balancer endpoint as a target for a route in a route table. Gateway Load Balancer endpoints are supported only for endpoint services that are configured using a Gateway Load Balancer.

 Gateway endpoints

A gateway endpoint is a gateway that is a target for a route in your route table used for traffic destined to either Amazon S3 or DynamoDB.

There is no charge for using gateway endpoints.

Q4. What are the connectivity options for Amazon VPC?

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| Option | Use Case | Advantages | Limitations |
|  |  |  |  |
| AWS  Managed VPN | AWS managed IPsec VPN connection over the internet to individual VPC | Reuse existing VPN equipment and processes  Reuse existing internet connections AWS managed high  availability VPN service Supports static routes or dynamic Border Gateway Protocol (BGP) peering and routing policies | Network latency, variability, and  availability are dependent on internet conditions  Customer managed endpoint is responsible for implementing redundancy and failover  (if required)  Customer device must support single-hop BGP (when leveraging BGP for dynamic routing) |
| AWS Transit  Gateway +  VPN | AWS managed IPsec VPN connection over the internet to regional router for multiple VPCs | Same as the previous option  AWS managed high  availability and scalability regional network hub for up to 5,000 attachments | Same as the previous option |
| AWS Direct Connect | Dedicated network connection over private lines | More predictable network performance Reduced bandwidth costs  Supports BGP peering and routing policies | May require additional telecom and hosting provider relationships or new network circuits to be provisioned |
| AWS Direct  Connect +  AWS Transit  Gateway | Dedicated network connection over private lines to regional router for multiple VPCs | Same as the previous option  AWS managed high  availability and scalability regional network hub for up to 5,000 attachments | Same as previous option |
|  |  |  |  |
| Option | Use Case | Advantages | Limitations |
|  |  |  |  |
| AWS Direct  Connect +  VPN | IPsec VPN connection over private lines | More predictable network performance Reduced bandwidth costs  Supports BGP peering and routing policies on AWS Direct Connect Reuse existing VPN equipment and processes  AWS managed high  availability VPN service Supports static routes or dynamic Border Gateway Protocol (BGP) peering and routing policies on VPN connection | May require additional telecom and hosting provider relationships or new network circuits to be provisioned  Customer managed endpoint is responsible for implementing redundancy and failover  (if required)  Customer device must support single-hop BGP (when leveraging BGP for dynamic routing) |
| AWS Direct  Connect +  AWS Transit  Gateway +  VPN | IPSec VPN connection over private lines to regional router for multiple VPCs | Same as previous option  AWS managed high  availability and scalability regional network hub for up to 5,000 attachments | Same as previous option |
| AWS VPN CloudHub | Connect remote branch offices in a hub-and-spoke model for primary or backup connectivity | Reuse existing internet connections and AWS VPN connections  AWS managed high  availability VPN service Supports BGP for exchanging routes and routing priorities | Network latency, variability, and availability are dependent on the internet  User managed branch office endpoints are responsible for implementing  redundancy and failover  (if required) |
| Software Siteto-Site VPN | Software appliancebased VPN connection over the internet | Supports a wider array of VPN vendors, products, and protocols Fully customermanaged solution | Customer is responsible  for implementing HA  (high availability) solutions for all VPN endpoints (if required) |