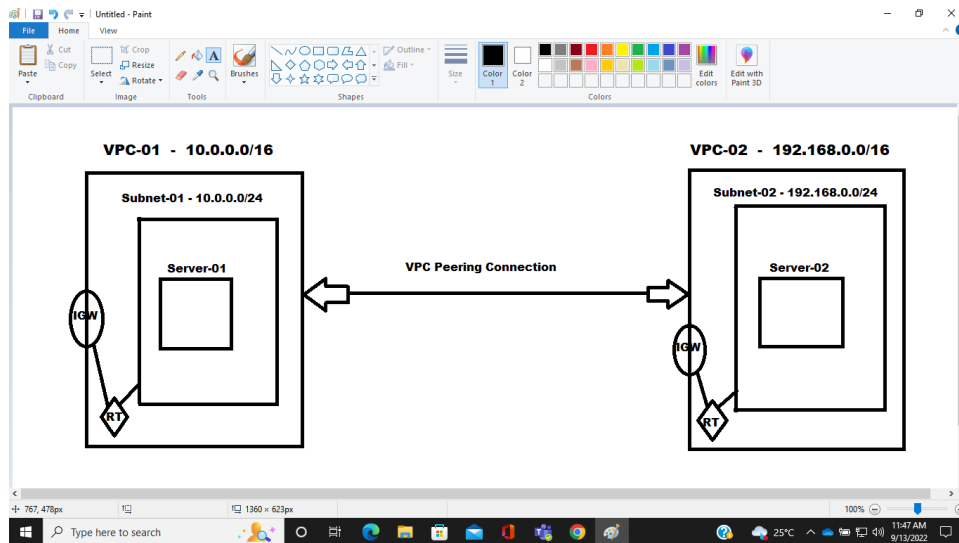


# VPC Peering

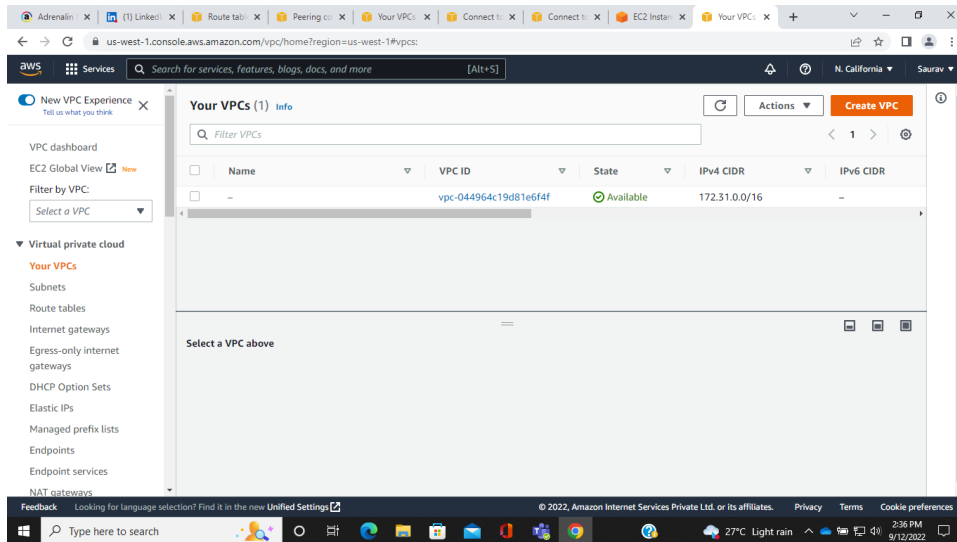
Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.



**Steps to create the VPC Connection:**

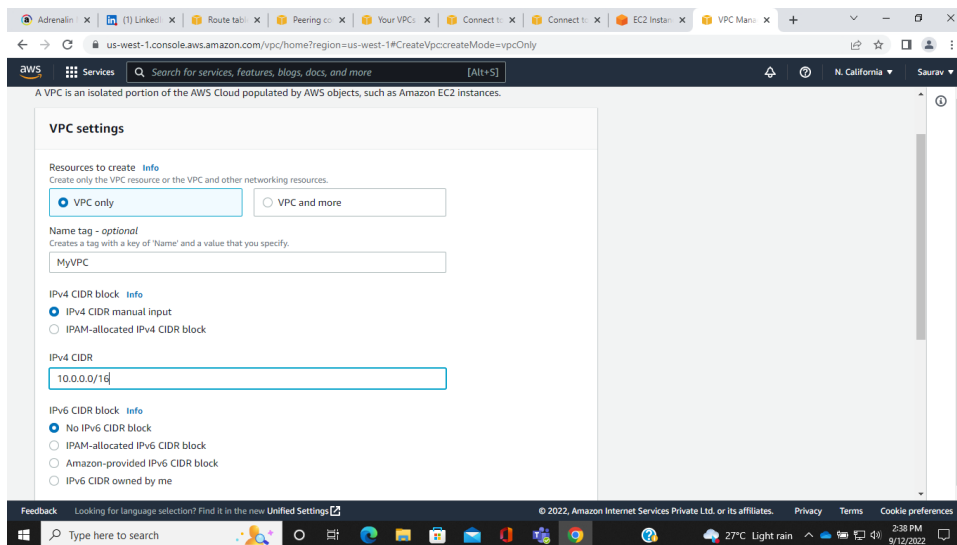
**Create two VPC i.e., VPC-01: 10.0.0.0/16 and 192.168.0.0/16**

**Click on the Create VPC Button**

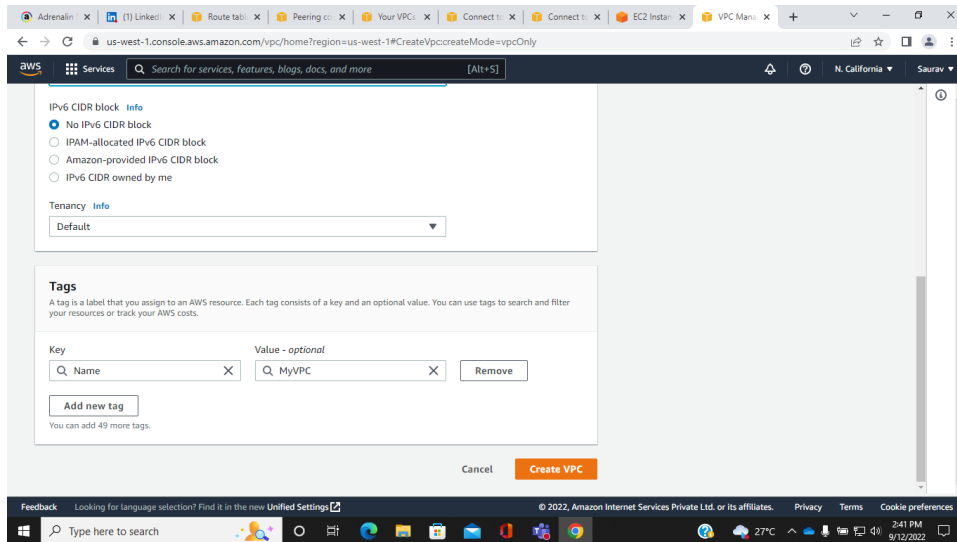


**Give the Name of the VPC**

**Put the CIDR Range: 10.0.0.0/16**



**Click on the Create VPC Button**

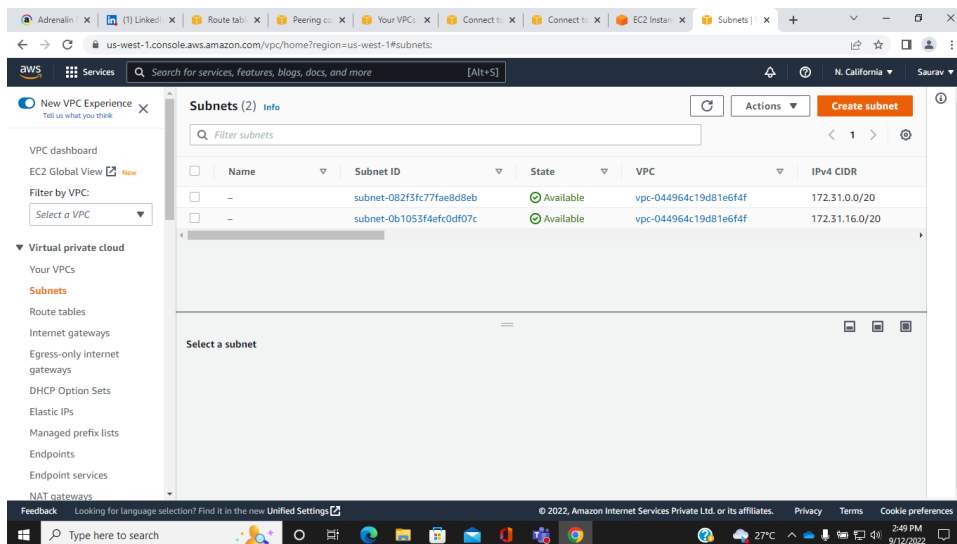


Create another VPC with CIDR: 192.168.0.0/16

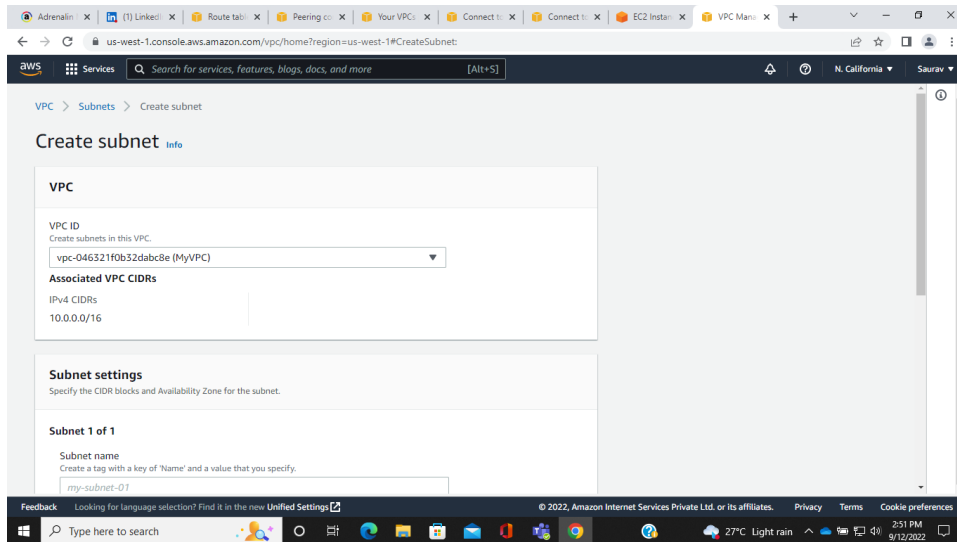
Now, create 2 subnets: One for VPC-01 and another for VPC-02

Steps to create Subnet-01

Click on Create Subnet



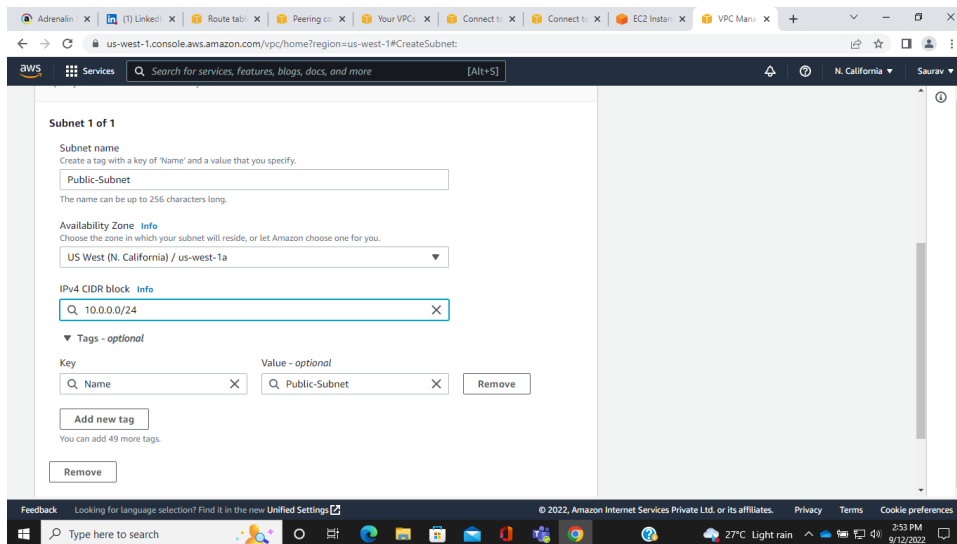
Select the VPC



**Give the Name of the Subnet**

**Select the Availability Zone**

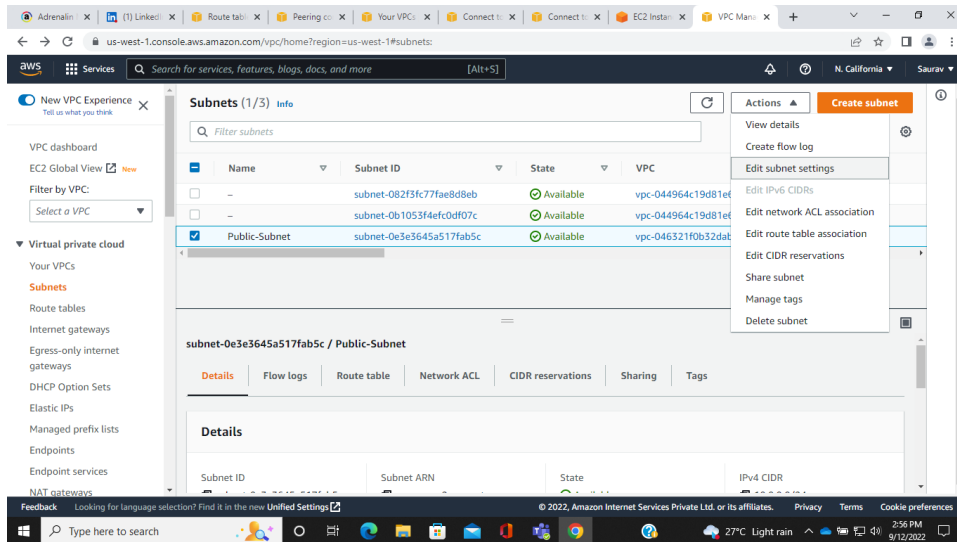
**Put the CIDR Range: 10.0.0.0/24**



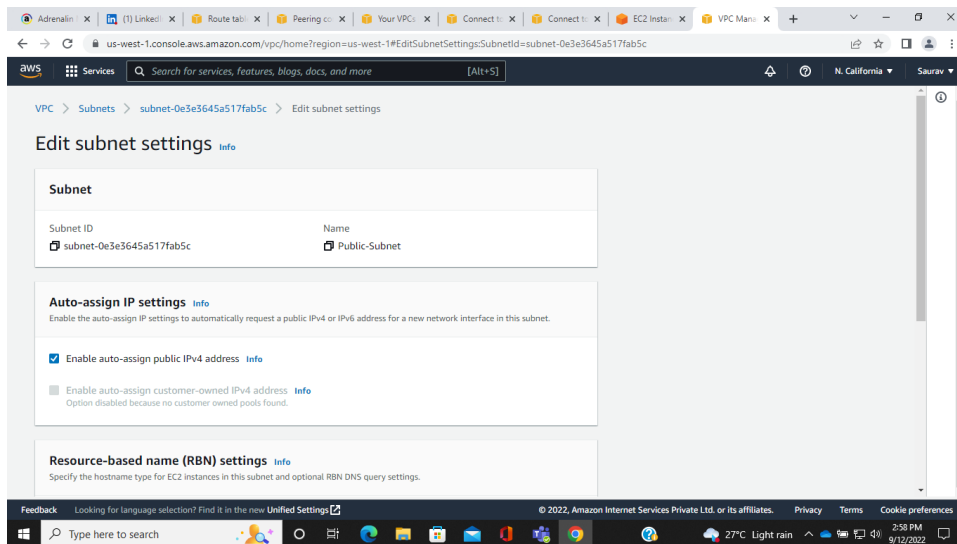
**Steps to make the Subnet Public**

**Select the Subnet and click on the Action Button**

**Now Select the Edit subnet settings**

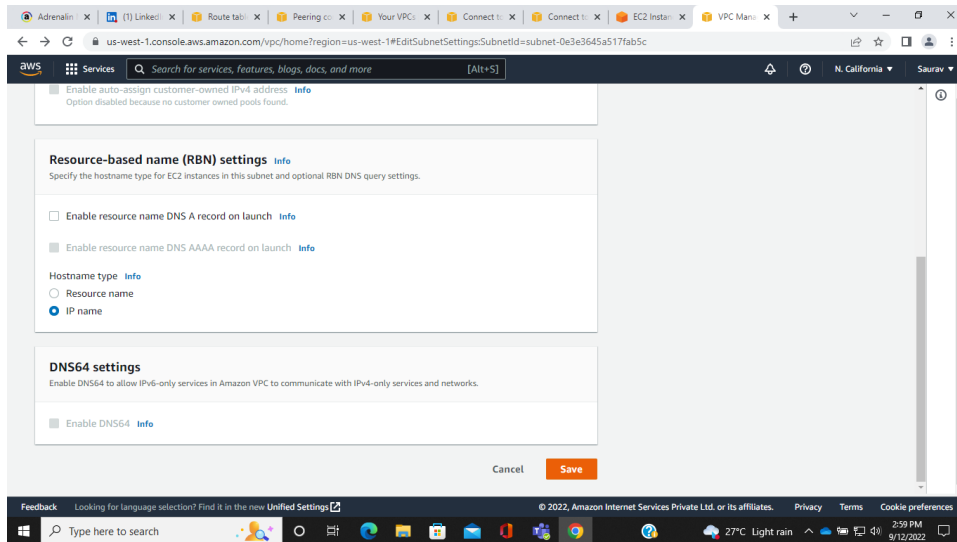


## Select the Auto-assign IP settings



Click on Save Button

The Subnet has become Public now

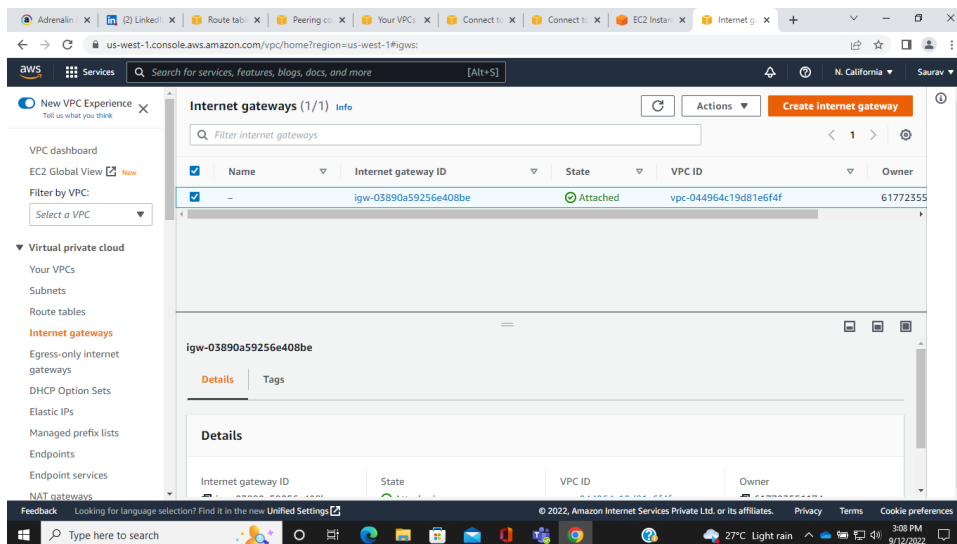


**Create another Subnet-02 with CIDR: 192.168.0.0/24**

**Repeat the same above steps**

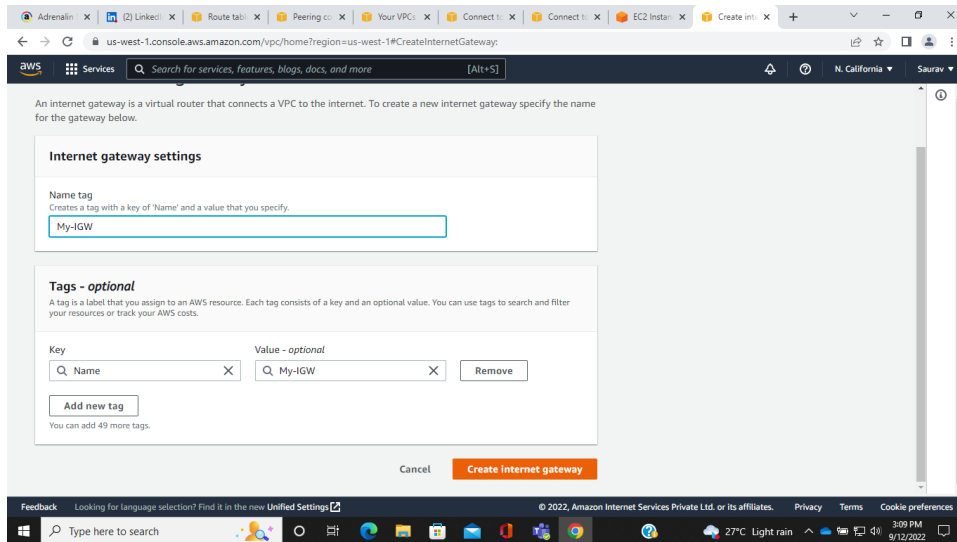
**Now, attach the Internet Gateway to VPC-01**

**Click on the Create Internet Gateway Button**



**Give the name of the Internet Gateway**

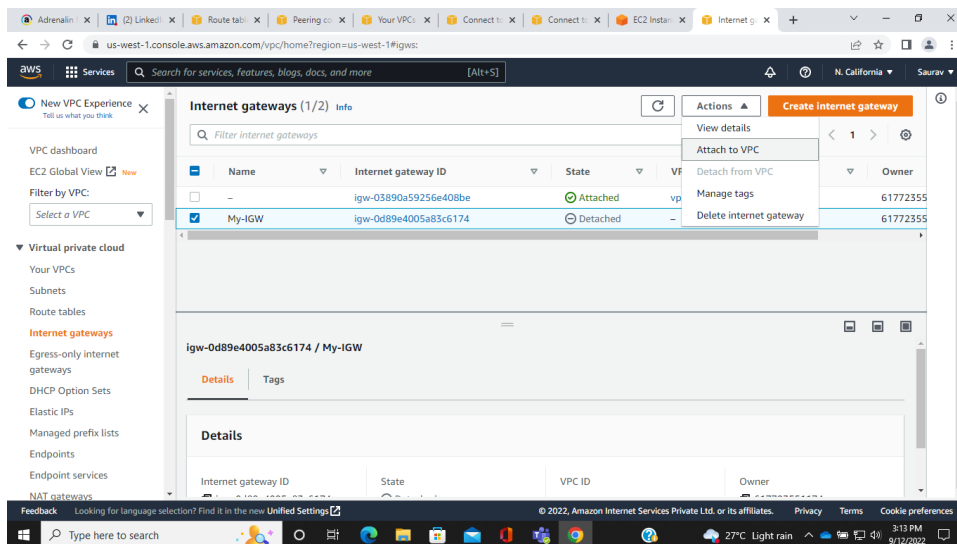
**Click on the Create Internet Gateway Button**



## Steps to attach the Internet Gateway to VPC-01

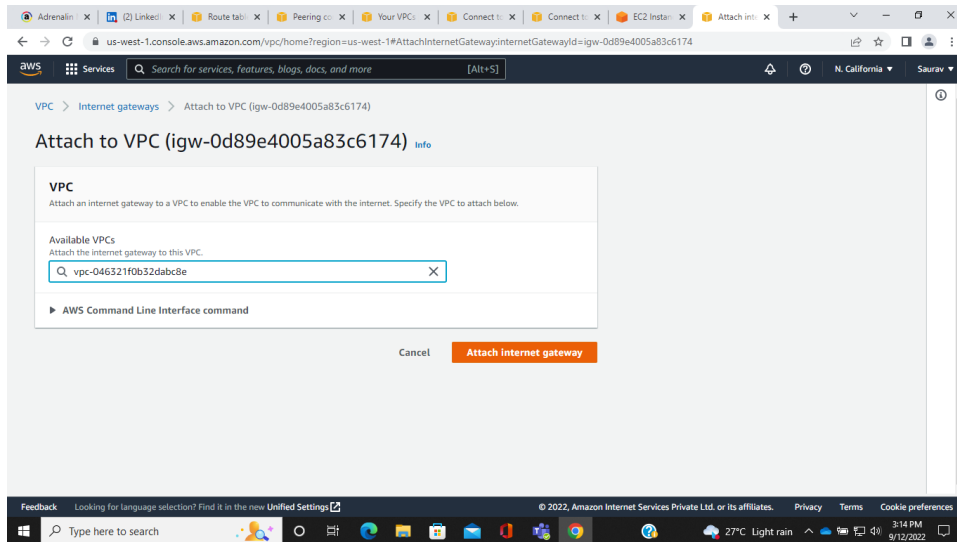
### Select the Internet Gateway

### Click on the Action Button and select Attach to VPC Button



### Select the VPC you want to attach to the Internet Gateway

### Click on the Attach Internet Gateway Button



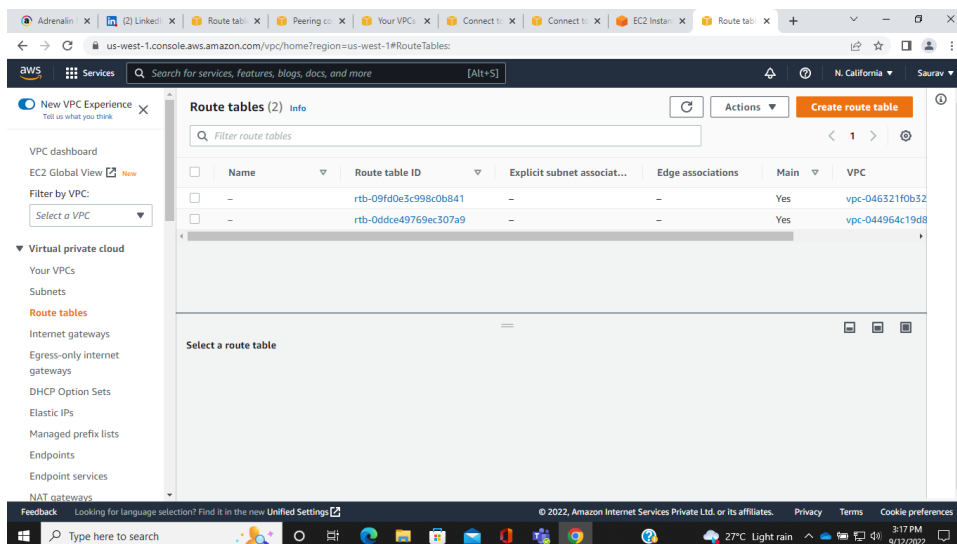
**Now, create another Internet Gateway to attach the VPC-02**

**Repeat the same above steps to attach the VPC-02**

**Now, create two Route Table**

**One for VPC-01 and another for VPC-02**

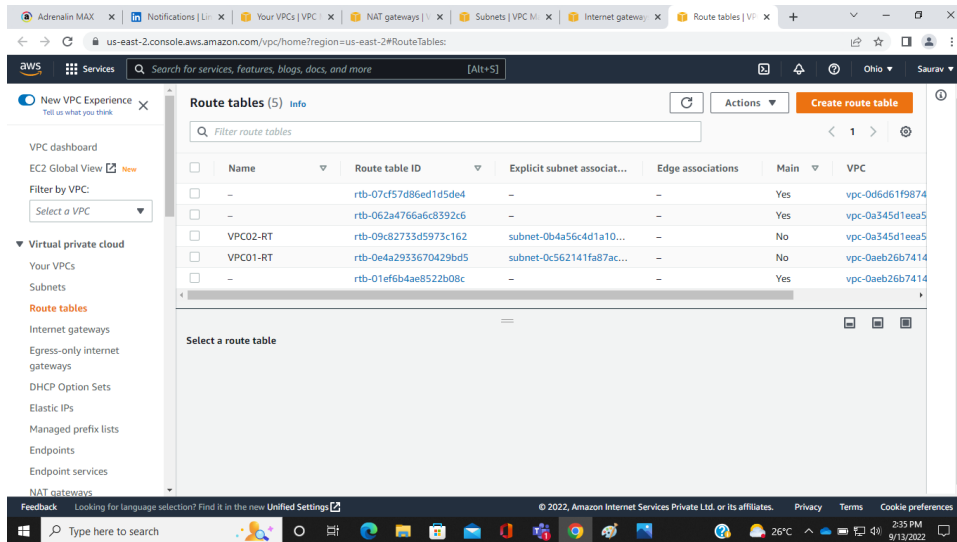
**Select the create Route Table Button**



**Give the name of the Route Table**

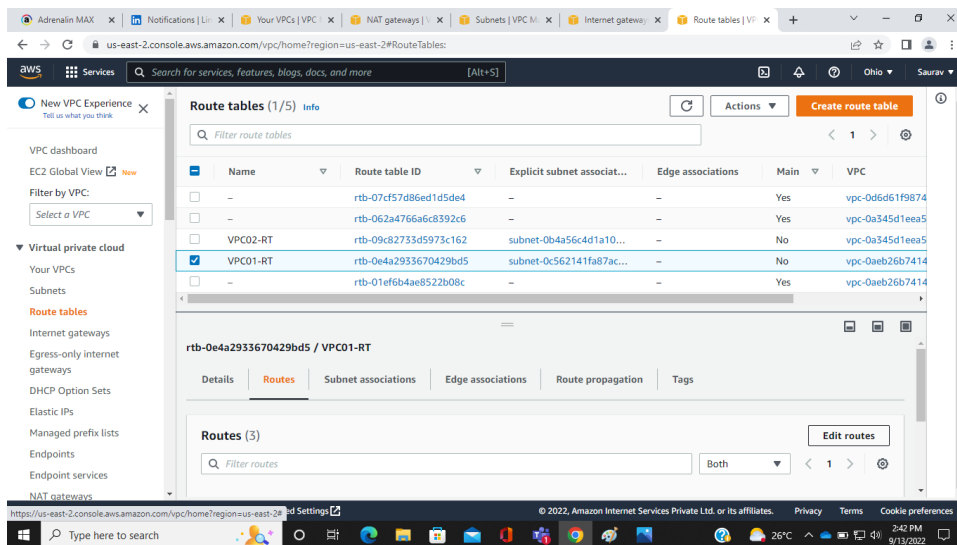
**Select the VPC and click on the Create Route Table Button**





**Select the VPC01-RT Route Table**

**Click on the Route Option and Select Edit Routes**



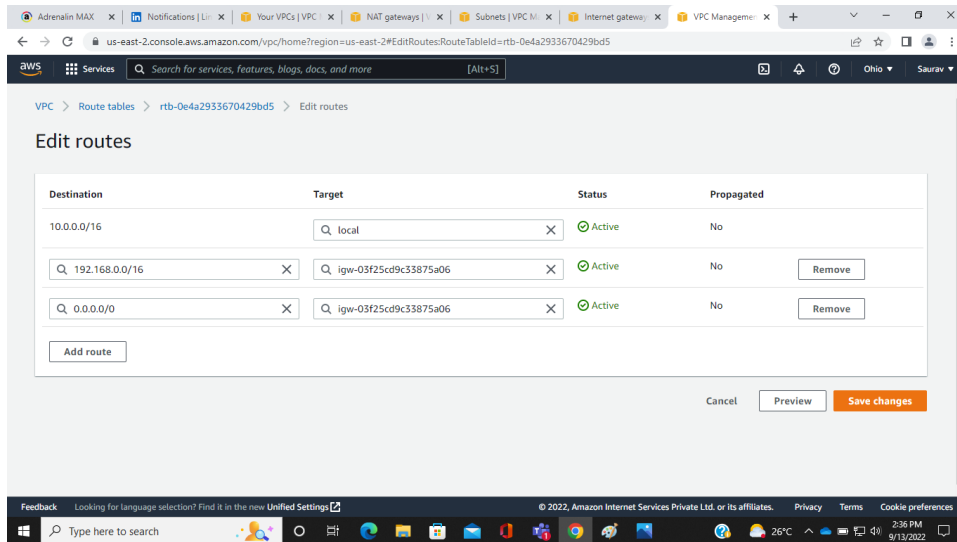
**Click on Add Route**

**Enter Destination and target: 0.0.0.0/0 and Internet Gateway**

**Add another route to the another VPC**

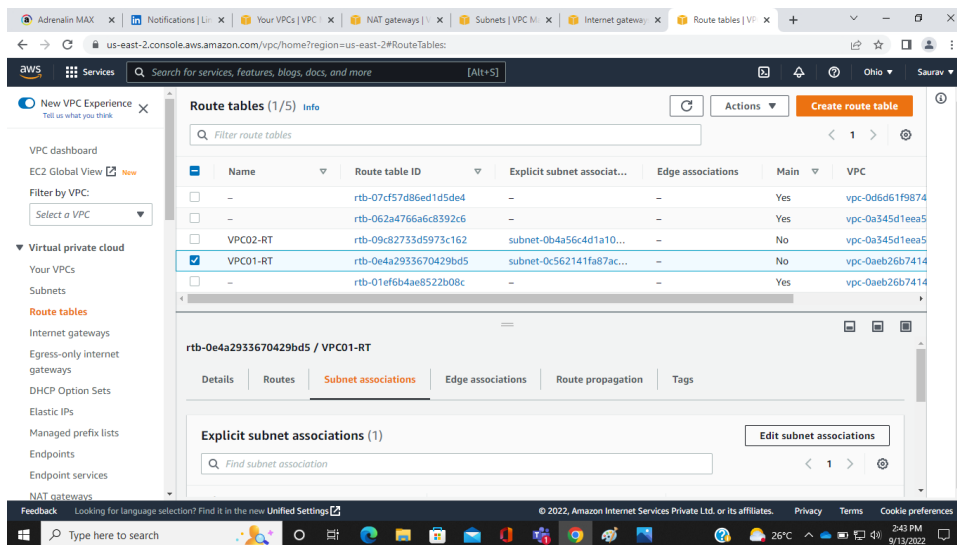
**Enter Destination and target: 192.168.0.0/16 and Internet Gateway**

**Click on Save changes**

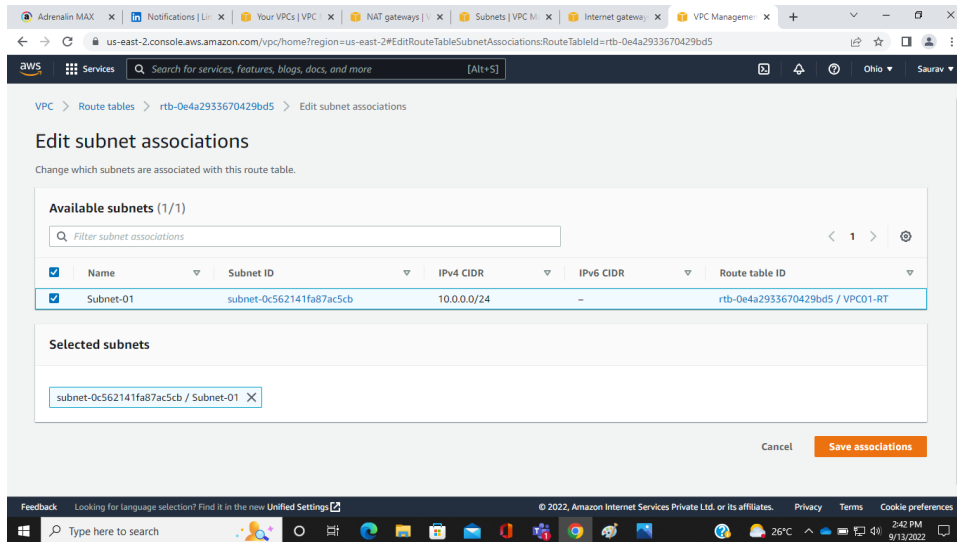


**Select the VPC01-RT Route Table**

**Click on the Subnet Association Option and Select Edit Subnet Association**



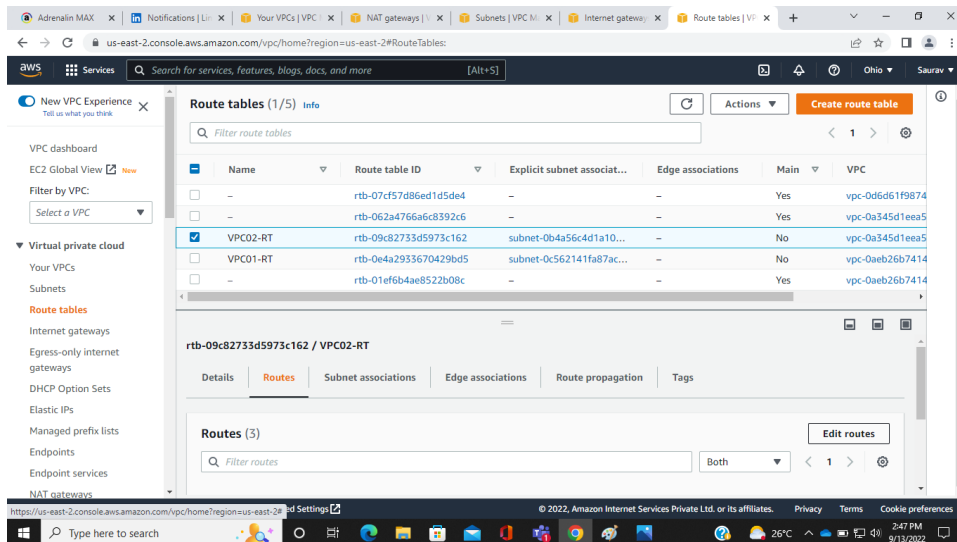
**Select Subnet-01 and Click on the Save Association Button**



Now, the same steps we follow for another Route Table i.e., VPC02-RT

Select the VPC02-RT Route Table

Click on the Route Option and Select Edit Routes



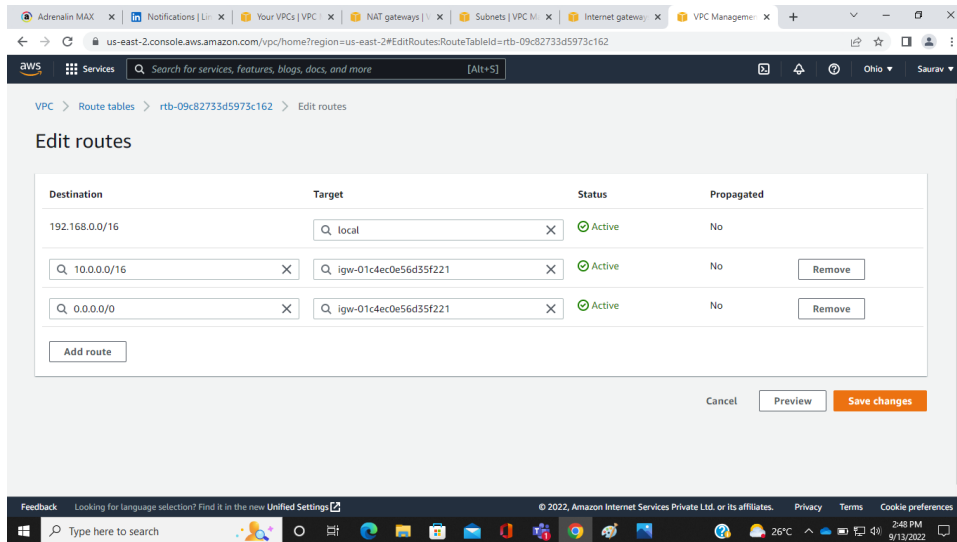
Click on Add Route

Enter Destination and target: 0.0.0.0/0 and Internet Gateway

Add another route to the another VPC

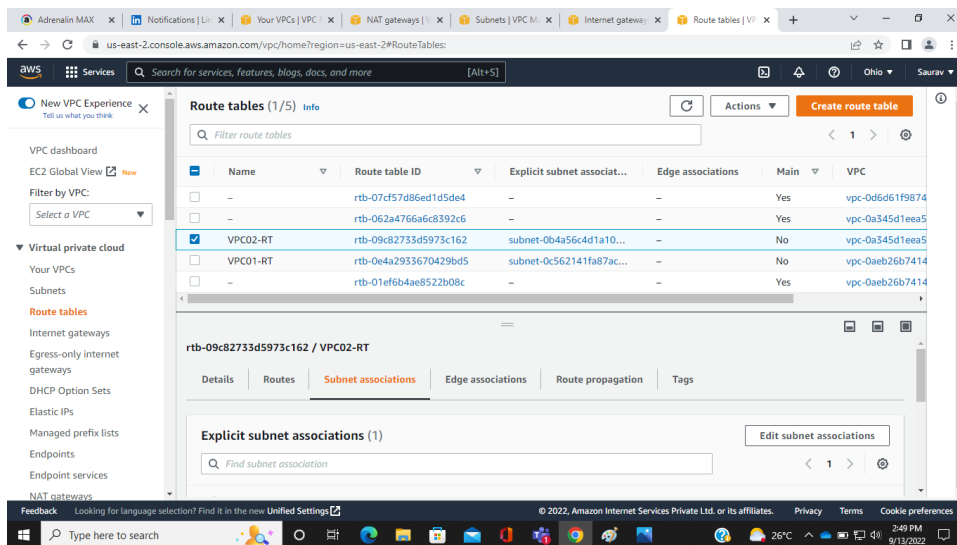
Enter Destination and target: 10.0.0.0/16 and Internet Gateway

Click on Save changes

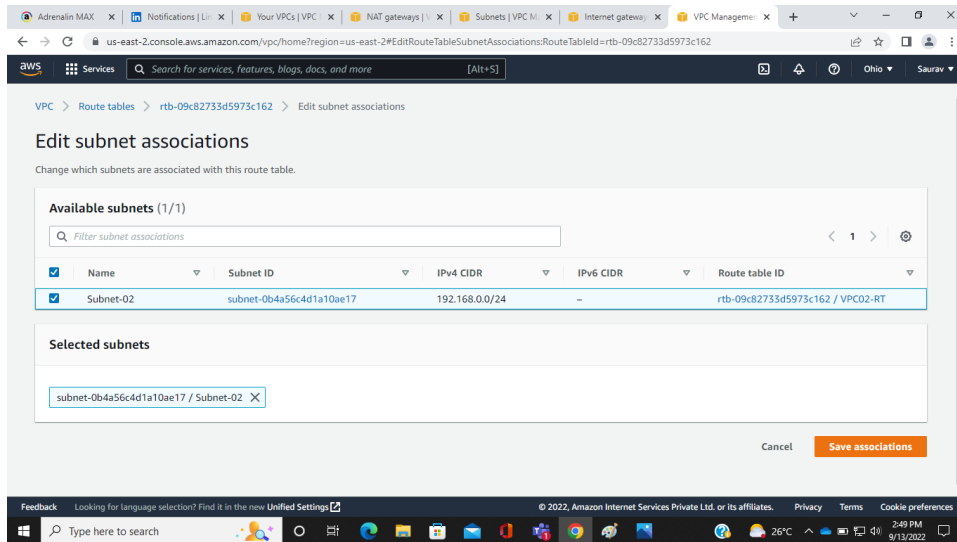


**Select the VPC01-RT Route Table**

**Click on the Subnet Association Option and Select Edit Subnet Association**



**Select Subnet-01 and Click on the Save Association Button**

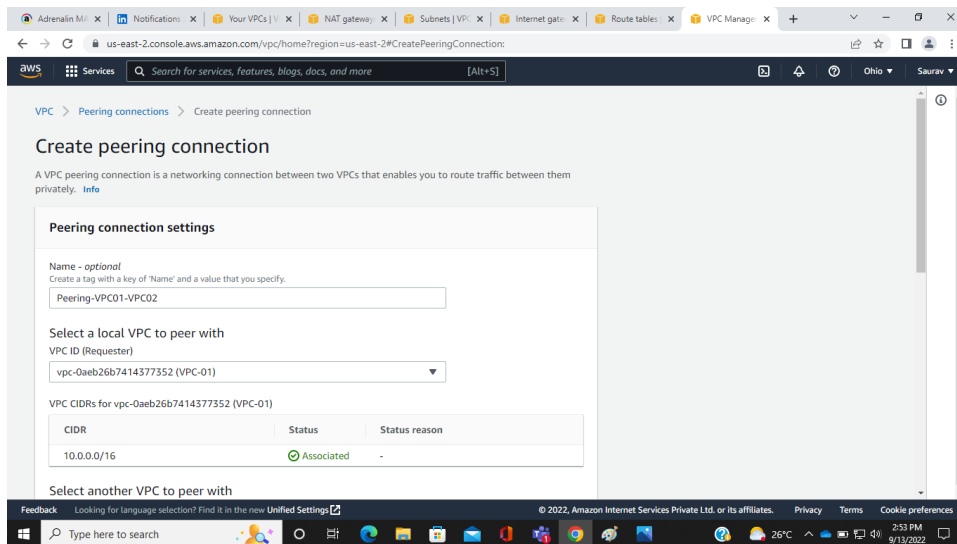


Now, create the peering connection.

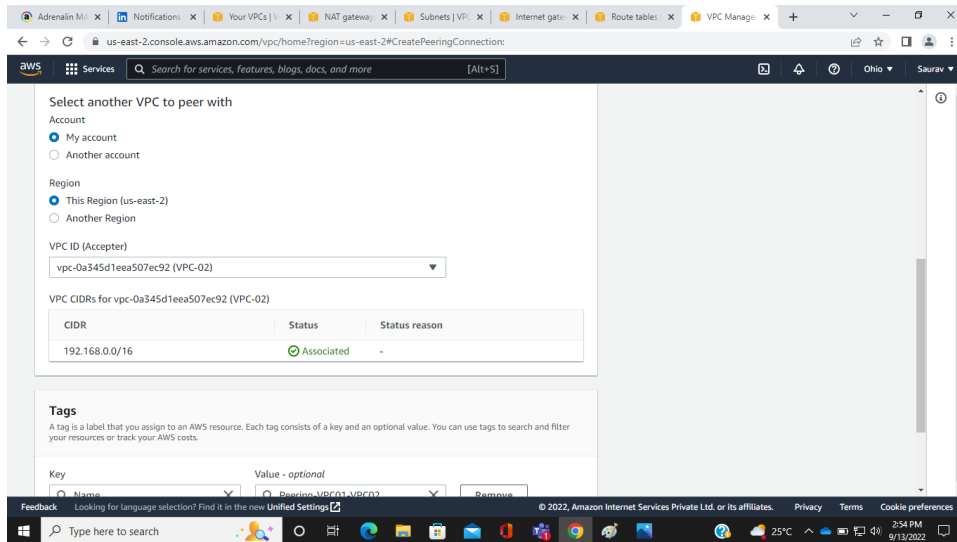
Click on the create peering connection button

Now, give the name of the peering connection

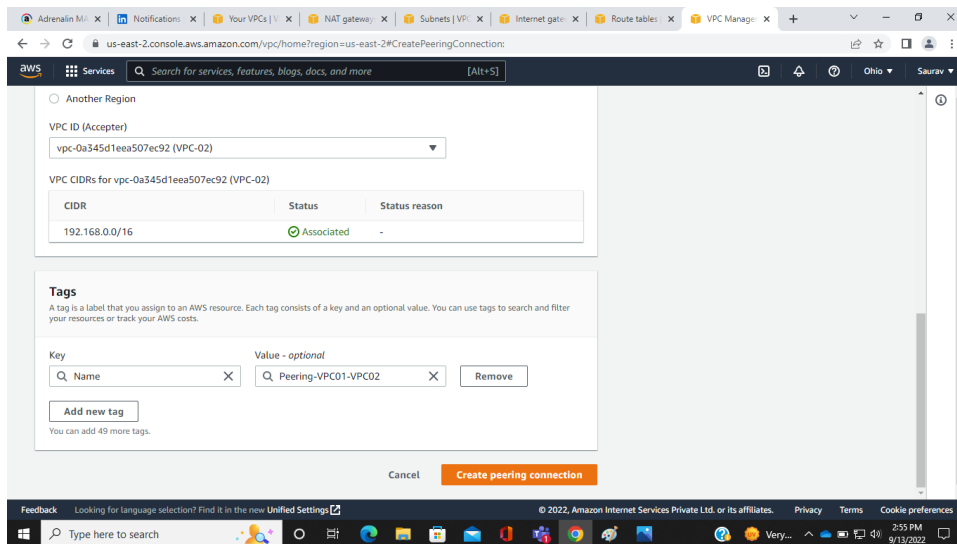
Select the VPC Requester i.e., VPC-01



Select the VPC Acceptor i.e., VPC-02

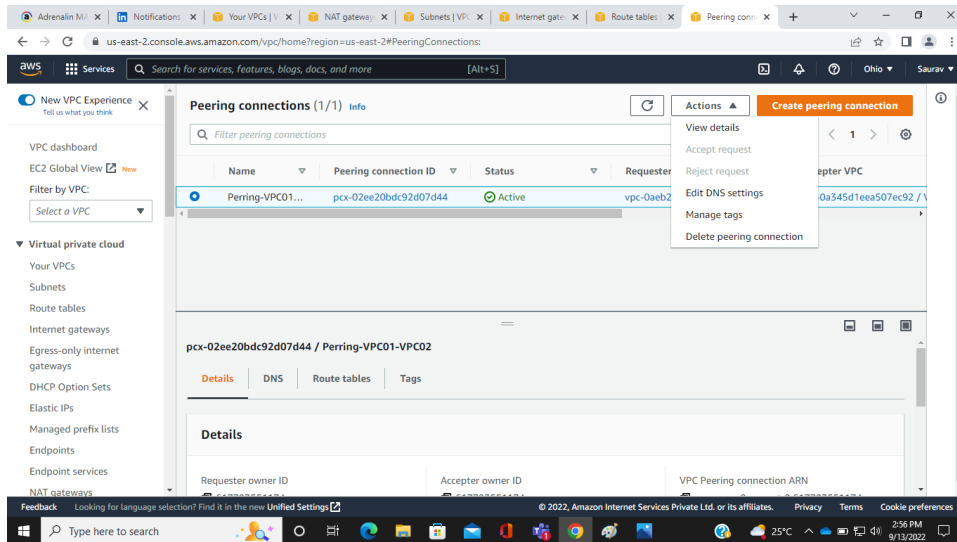


**Click on the create peering connection button**



**Select the peering connection**

**Go to Action Button and Click on Accept request option**



**The Peering Connection has been successfully created.**

**Now create two instances**

**One for VPC-01 and another for VPC-02**

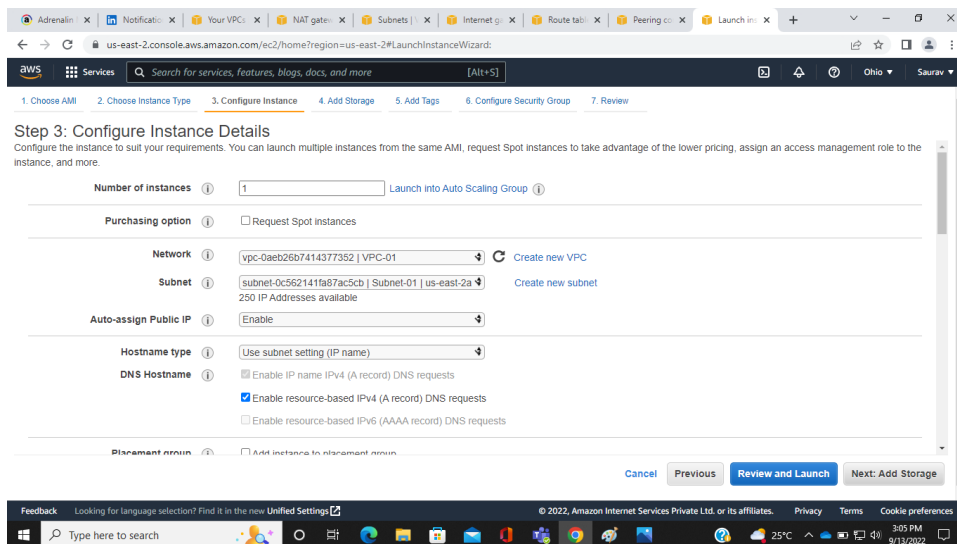
**Click on the Launch Instance Button**

**Choose AMI -> Linux**

**Choose Instance Type -> t2.micro**

**Choose Configure Instance Details -> Select Custom VPC i.e., VPC-01 from Network Option**

**Select Subnet-01 from Subnet option**



## Add Storage -> Default

## Add Tags -> Server-01

## Configure Security Group -> Open SSH Port and All Traffic

**Step 6: Configure Security Group**

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group  
☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Anywhere (0.0.0.0/0, :::/0)	e.g. SSH for Admin Desktop
All traffic	All	0 - 65535	Anywhere (0.0.0.0/0, :::/0)	e.g. SSH for Admin Desktop

[Add Rule](#)

**Warning**

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Previous](#) [Review and Launch](#)

## Click on Review and Launch

## Create a new key pair and Download the Key Pair

## Now, click on Launch Instance

**Step 7: Review Instance Launch**

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

**Improve your instances' security. Your security group, launch-wizard-1, is open to the world.**

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

▼ AMI Details [Edit AMI](#)

**Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type - ami-0568773882d492fc8**

Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is n...

Root Device Type: ebs Virtualization type: hvm

▼ Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

[Cancel](#) [Previous](#) [Launch](#)



Create another instance

Click on the Launch Instance Button

Choose AMI -> Linux

Choose Instance Type -> t2.micro

Choose Configure Instance Details -> Select Custom VPC i.e., VPC-02 from Network Option

Select Subnet-02 from Subnet option

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances  Launch into Auto Scaling Group

Purchasing option ☐ Request Spot instances

Network  Create new VPC

Subnet  Create new subnet

Auto-assign Public IP

Hostname type

DNS Hostname ☒ Enable IP name IPv4 (A record) DNS requests  
☒ Enable resource-based IPv4 (A record) DNS requests  
☐ Enable resource-based IPv6 (AAAA record) DNS requests

Placement group ☐ Add instance to placement group

Cancel Previous Review and Launch Next: Add Storage

Add Storage -> Default

Add Tags -> Server-02

Configure Security Group -> Open SSH Port and All Traffic

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more about Amazon EC2 security groups.](#)

Assign a security group: ☒ Create a new security group  
☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Anywhere	e.g. SSH for Admin Desktop
All traffic	All	0 - 65535	Anywhere	e.g. SSH for Admin Desktop

Add Rule

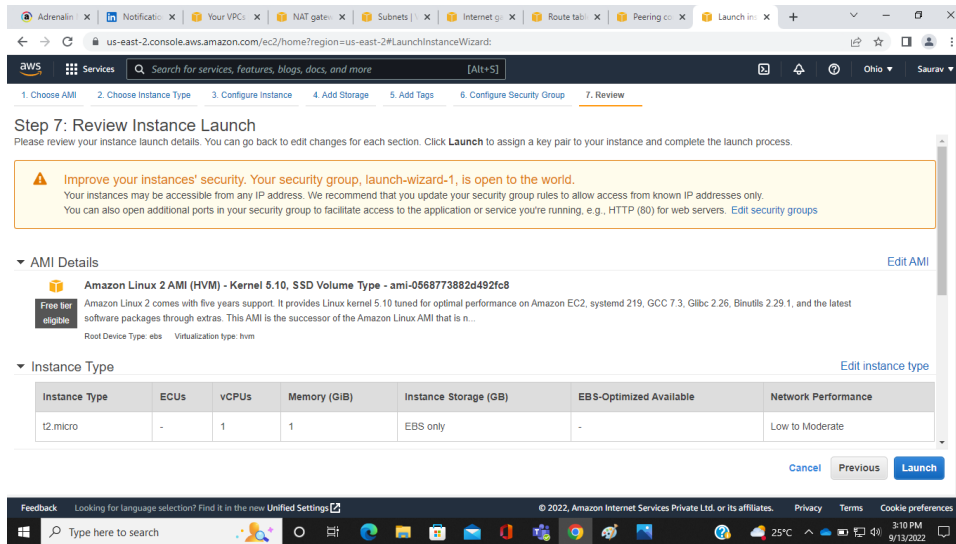
**Warning**  
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Previous Review and Launch

Click on Review and Launch

Create a new key pair and Download the Key Pair

Now, click on Launch Instance

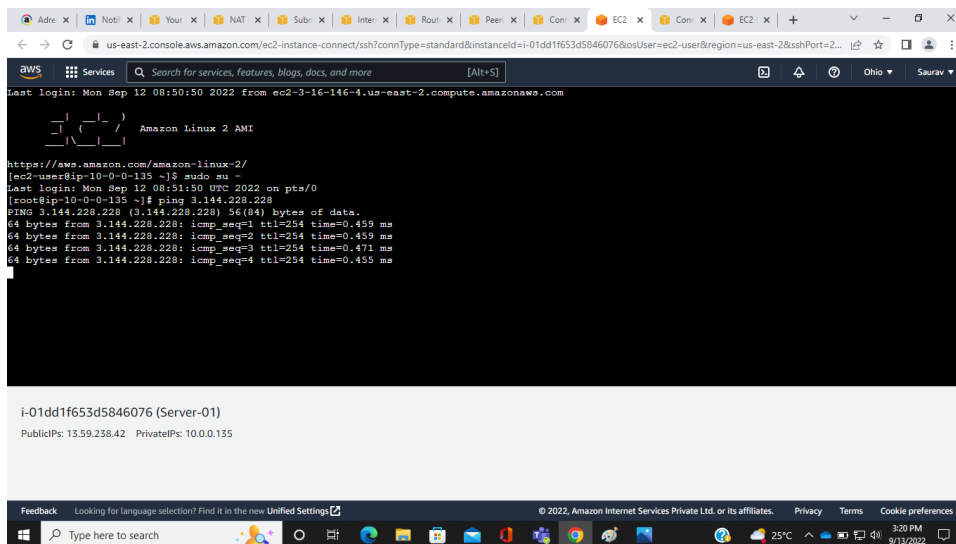


The instances have been successfully created.

Now, we ping one server to another server.

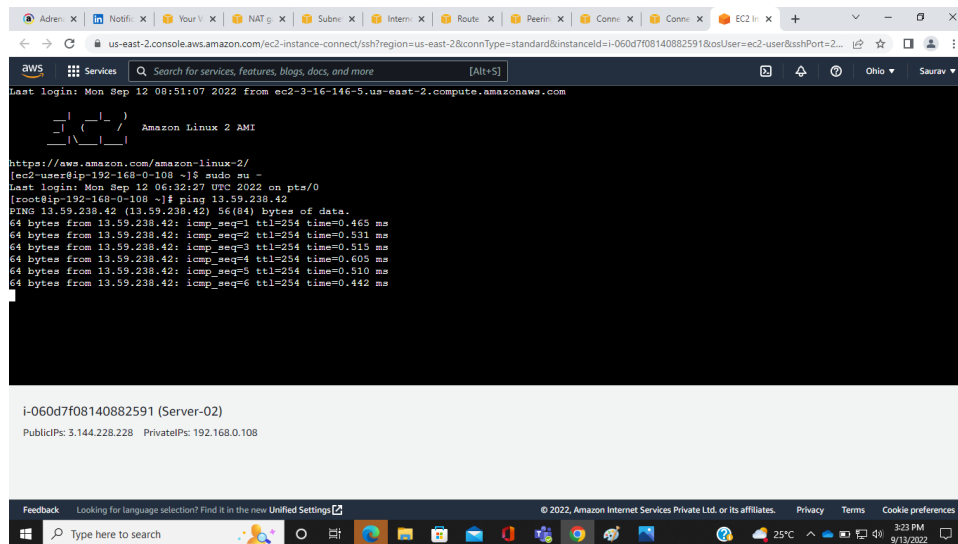
Connect the Server-01

Run this command: ping “Public IP of another Server-02”



Now, connect the Server-02

Run this command: ping “Public IP of another Server-01”



The screenshot shows a terminal window within the AWS Management Console. The terminal is connected to an Amazon Linux 2 instance (i-060d7f08140882591) in the us-east-2 region. The user has logged in as 'ec2-user' and executed the command 'ping 13.59.238.42'. The output shows six successful ping requests, each receiving 64 bytes of data from the target IP address with varying response times between 0.465 ms and 0.510 ms. Below the terminal output, the instance details for 'i-060d7f08140882591 (Server-02)' are displayed, showing its PublicIPs as 3.144.228.228 and PrivateIPs as 192.168.0.108. The bottom of the image shows the Windows taskbar with various application icons and the system clock indicating 3:23 PM on 9/13/2022.

```
aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Last login: Mon Sep 12 08:51:07 2022 from ec2-3-16-146-5.us-east-2.compute.amazonaws.com

 _ _ _ _ _
|_| ( _ _ )
|_| \_/_/   Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-192-168-0-108 ~]$ sudo su -
Last login: Mon Sep 12 06:32:27 UTC 2022 on pts/0
[root@ip-192-168-0-108 ~]# ping 13.59.238.42
PING 13.59.238.42 (13.59.238.42) 56(84) bytes of data:
64 bytes from 13.59.238.42: icmp_seq=1 ttl=254 time=0.465 ms
64 bytes from 13.59.238.42: icmp_seq=2 ttl=254 time=0.501 ms
64 bytes from 13.59.238.42: icmp_seq=3 ttl=254 time=0.515 ms
64 bytes from 13.59.238.42: icmp_seq=4 ttl=254 time=0.605 ms
64 bytes from 13.59.238.42: icmp_seq=5 ttl=254 time=0.510 ms
64 bytes from 13.59.238.42: icmp_seq=6 ttl=254 time=0.442 ms
^C
```

i-060d7f08140882591 (Server-02)  
PublicIPs: 3.144.228.228 PrivateIPs: 192.168.0.108

Feedback Looking for language selection? Find it in the new Unified Settings © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences  
Type here to search 25°C 3:23 PM 9/13/2022

Both Server has been successfully pinged with another.

