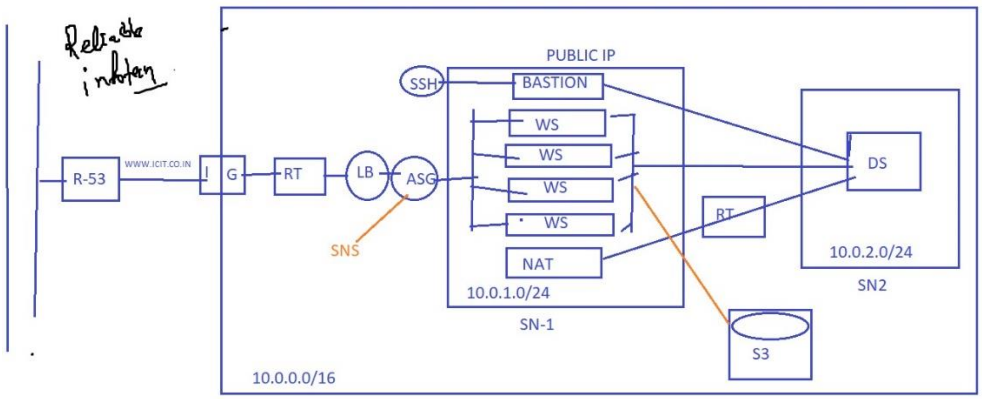
AWS Project using VPC

This is a simple AWS project for beignner. This Project consist of Vitual Private Cloud(VPC), Elastic Compute Cloud(EC2), Route 53, ASG, Loadbalancer.

Using this all services you will deploy a website on your public network simultaneously you will connect private and public servers.

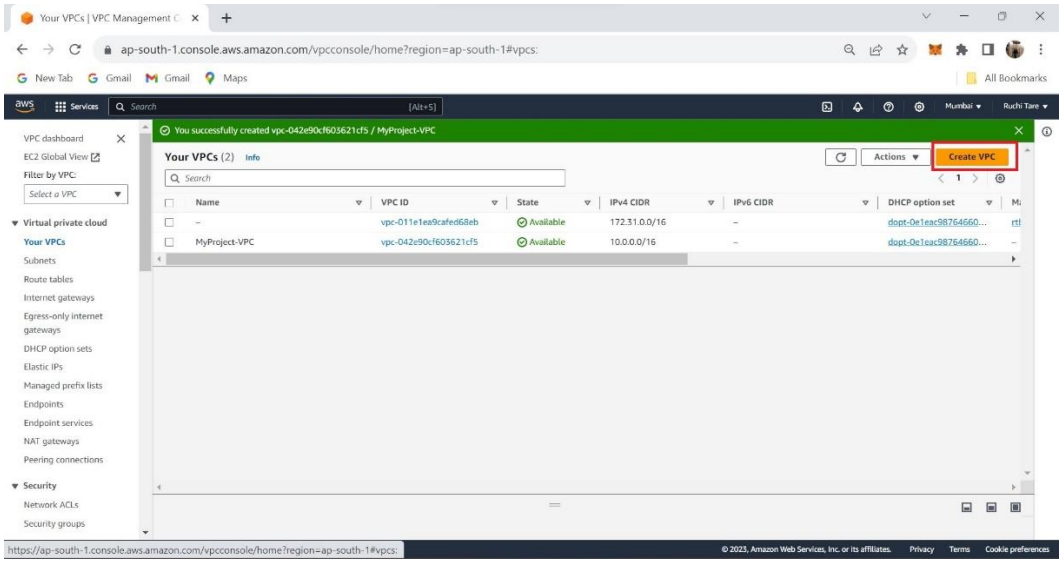


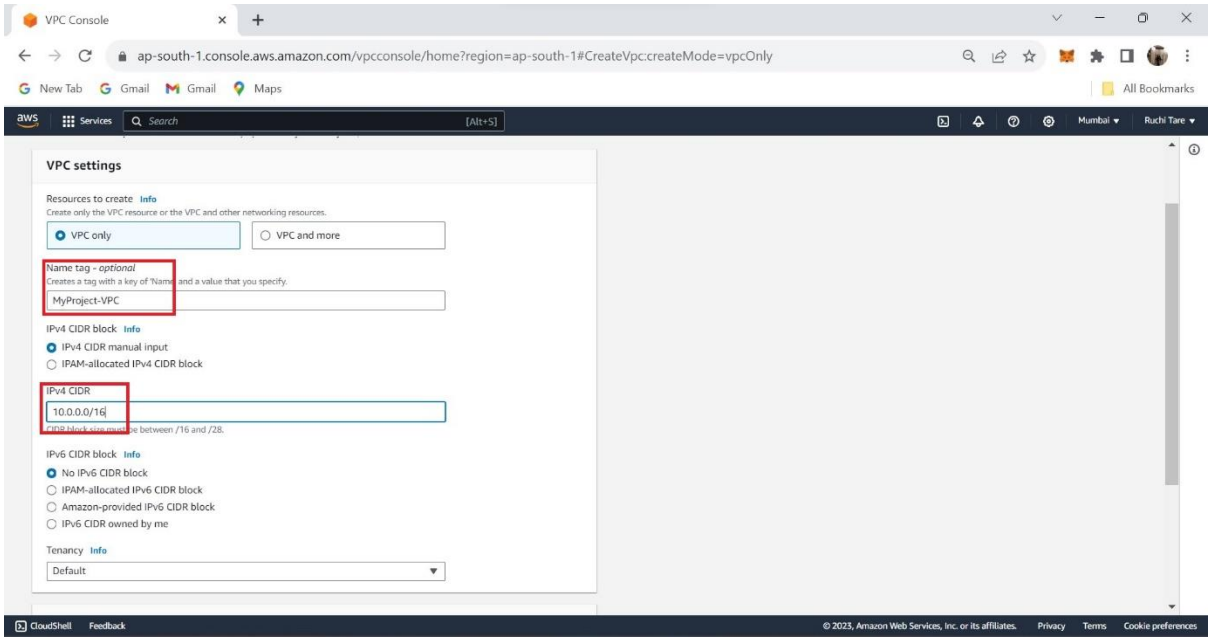
Step 1 : Connect to VPC

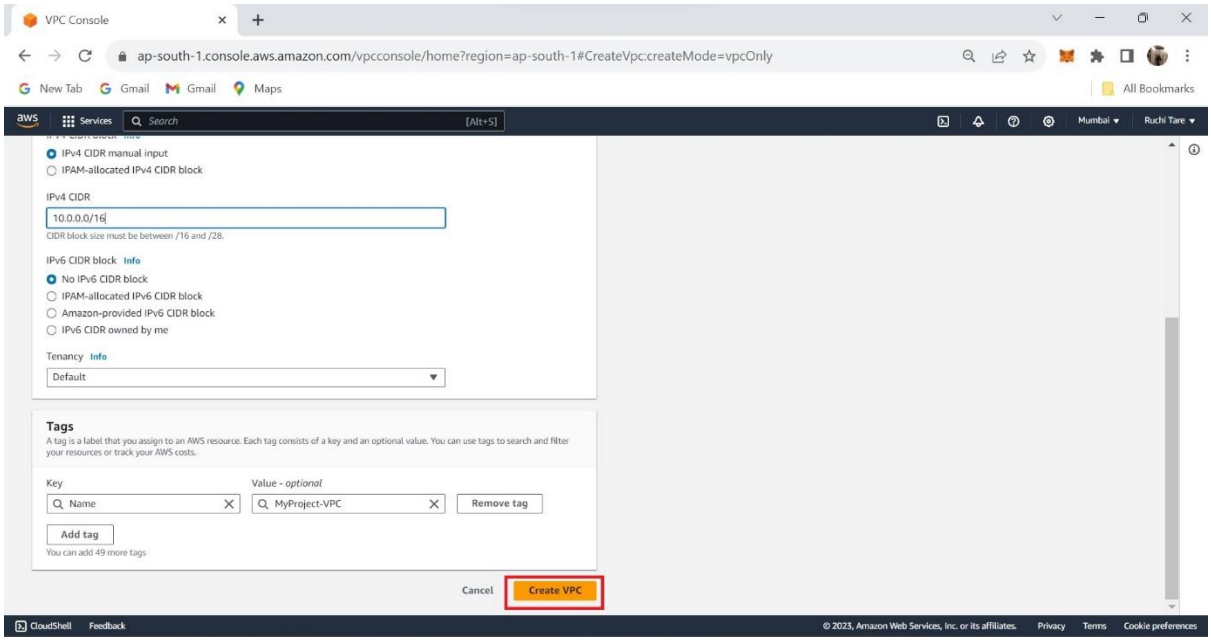
Virtual Private Cloud(VPC) : A virtual private cloud (VPC) is a secure, isolated private cloud hosted within a public cloud. VPC customers can run code, store data, host websites, and do anything else they could do in an ordinary private cloud, but the private cloud is hosted remotely by a public cloud provider.

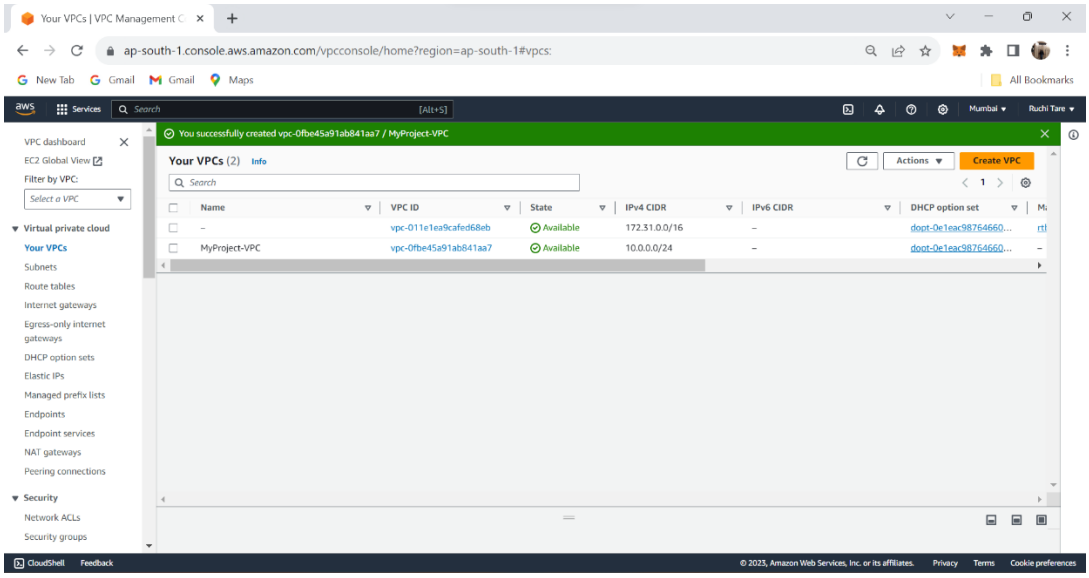
1. Login to Aws Console , after that search for VPC.

2. Create a VPC with CIDR 10.0.0.0/16.



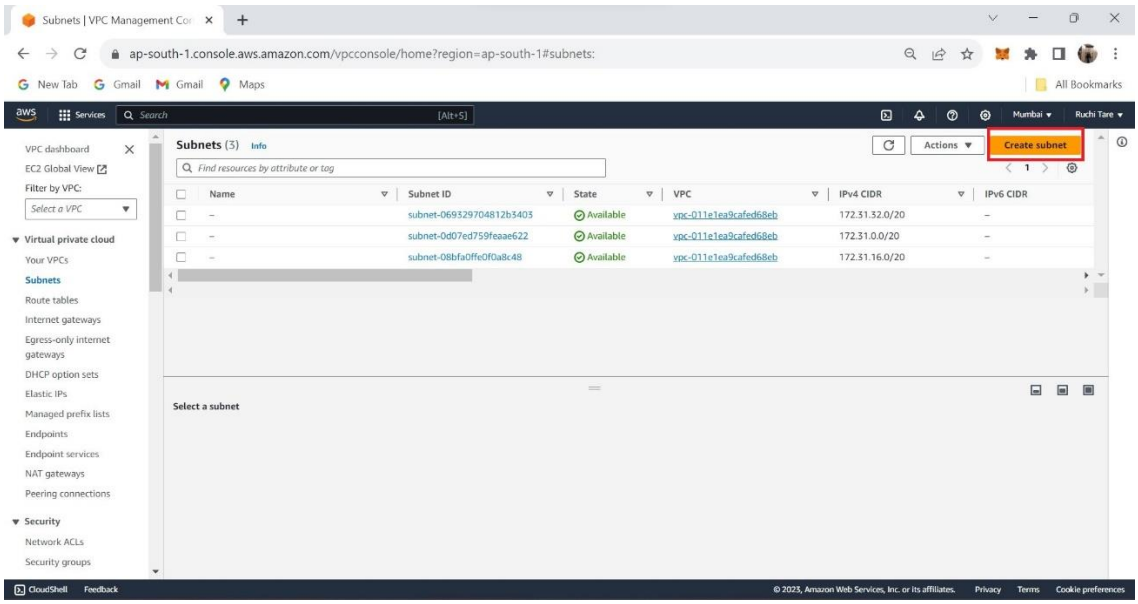

VPC Console
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateVpc:createMode=vpcOnly
New Tab
Gmail
Gmail
Maps
All Bookmarks
Services
Search
[Alt+S]
Mumbai
Ruchi Tare
VPC settings
Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
VPC only
VPC and more
Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
MyProject-VPC
IPv4 CIDR block Info
IPv4 CIDR manual input
IPAM-allocated IPv4 CIDR block
IPv4 CIDR
10.0.0.0/16
CIDR block size must be between /16 and /28.
IPv6 CIDR block Info
No IPv6 CIDR block
IPAM-allocated IPv6 CIDR block
Amazon-provided IPv6 CIDR block
IPv6 CIDR owned by me
Tenancy Info
Default
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


VPC Console
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateVpc:createMode=vpcOnly
New Tab
Gmail
Gmail
Maps
All Bookmarks
Services
Search
[Alt+S]
Mumbai
Ruchi Tare
IPv4 CIDR manual input
IPAM-allocated IPv4 CIDR block
IPv4 CIDR
10.0.0.0/16
CIDR block size must be between /16 and /28.
IPv6 CIDR block Info
No IPv6 CIDR block
IPAM-allocated IPv6 CIDR block
Amazon-provided IPv6 CIDR block
IPv6 CIDR owned by me
Tenancy Info
Default
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
MyProject-VPC
Remove tag
Add tag
You can add 49 more tags
Cancel
Create VPC
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

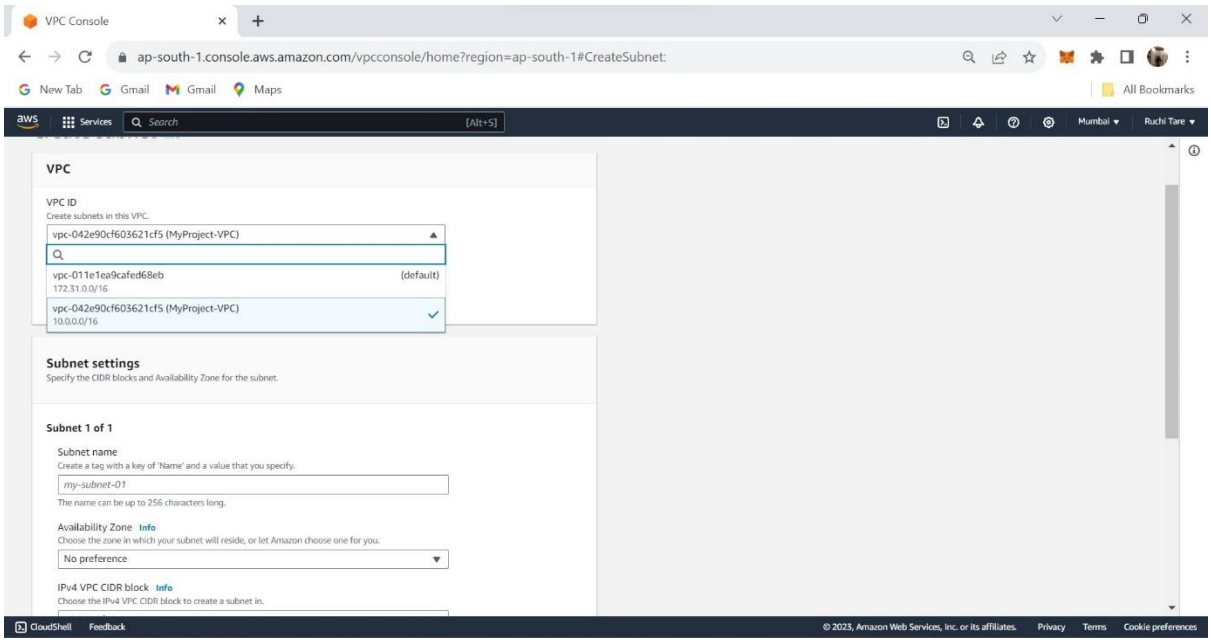


3. After creating vpc next step is to create 2 Subnet public and private subnet
4. public subnet CIDR 10.0.1.0/24
5. private subnet CIDR 10.0.2.0/24

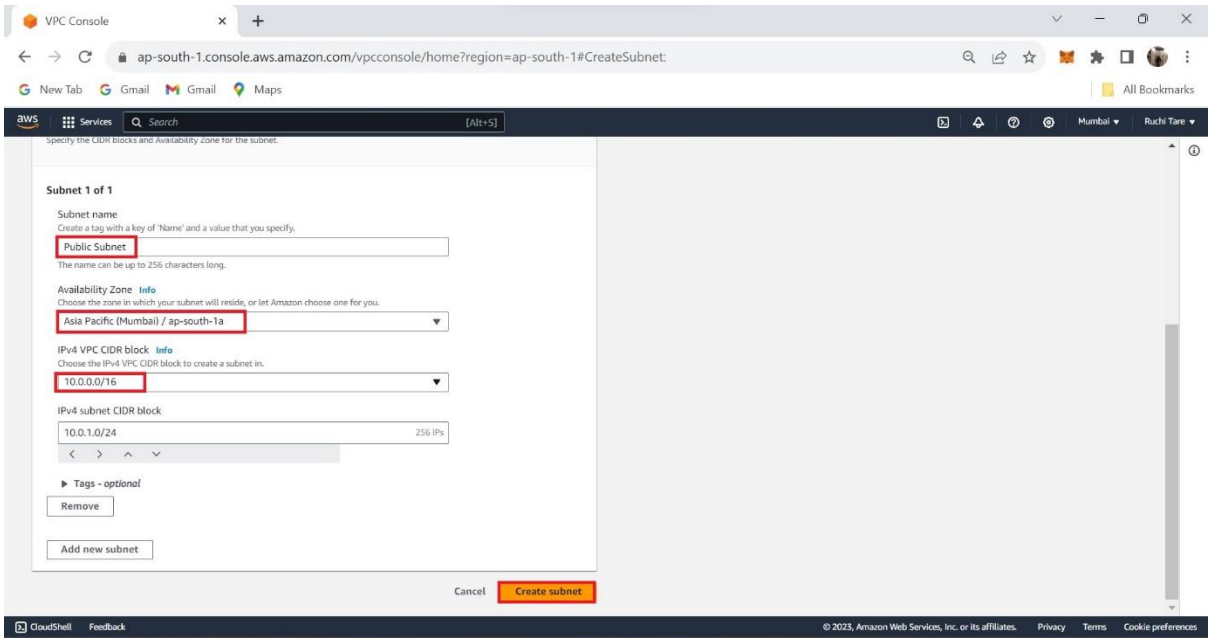
First click on create a subnet.



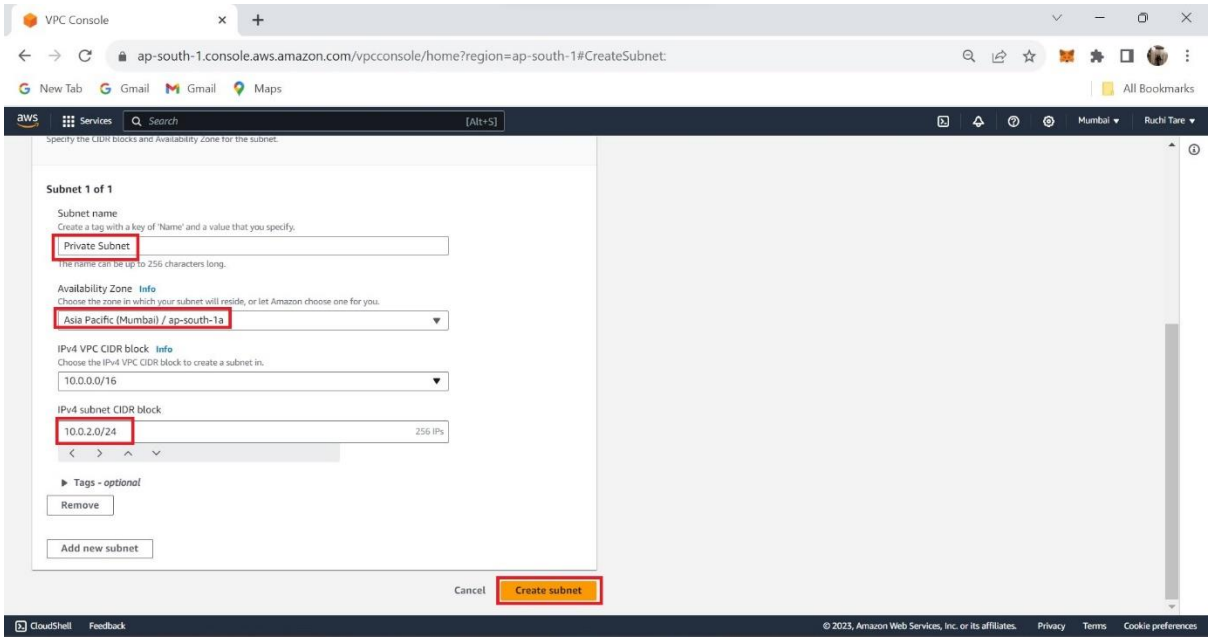
Select the VPC that you have created.

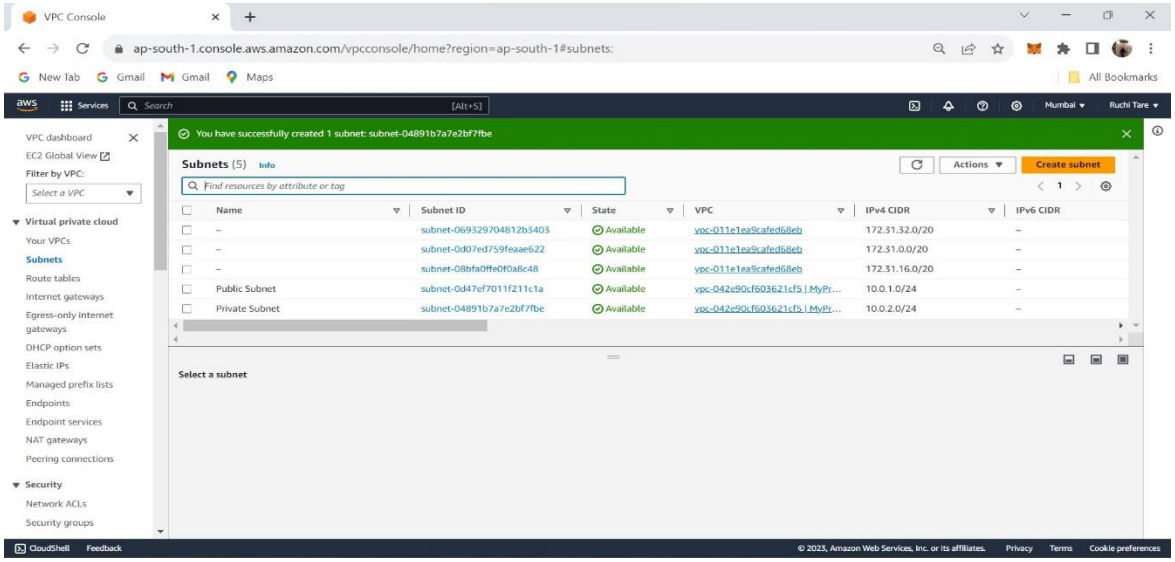


Enter Public Subnet name and CIDR and Availability Zone



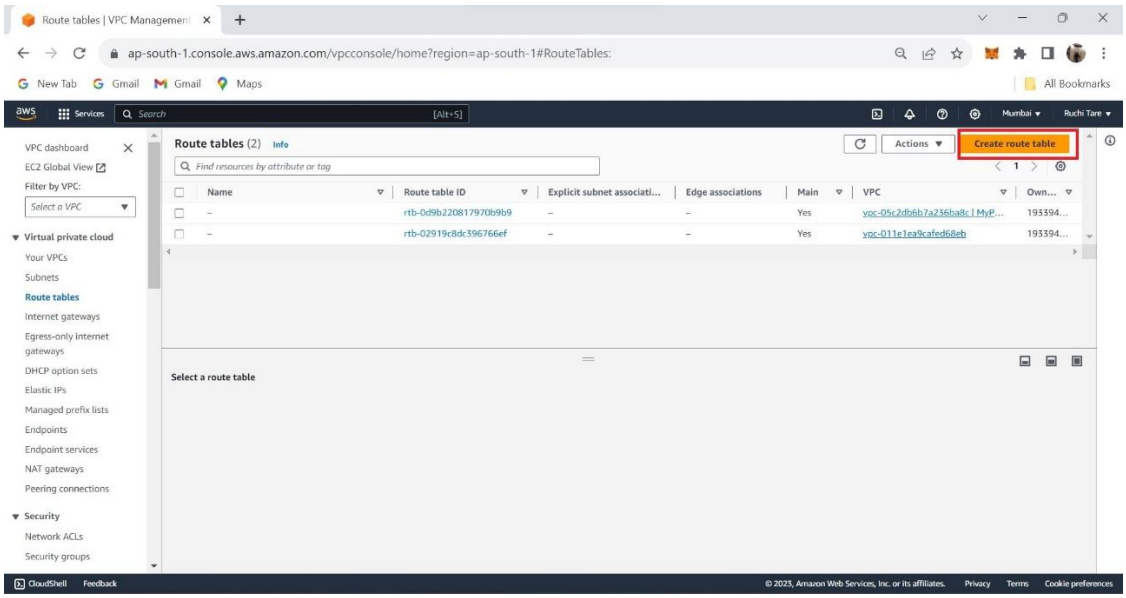
Do the same for Private Subnet.



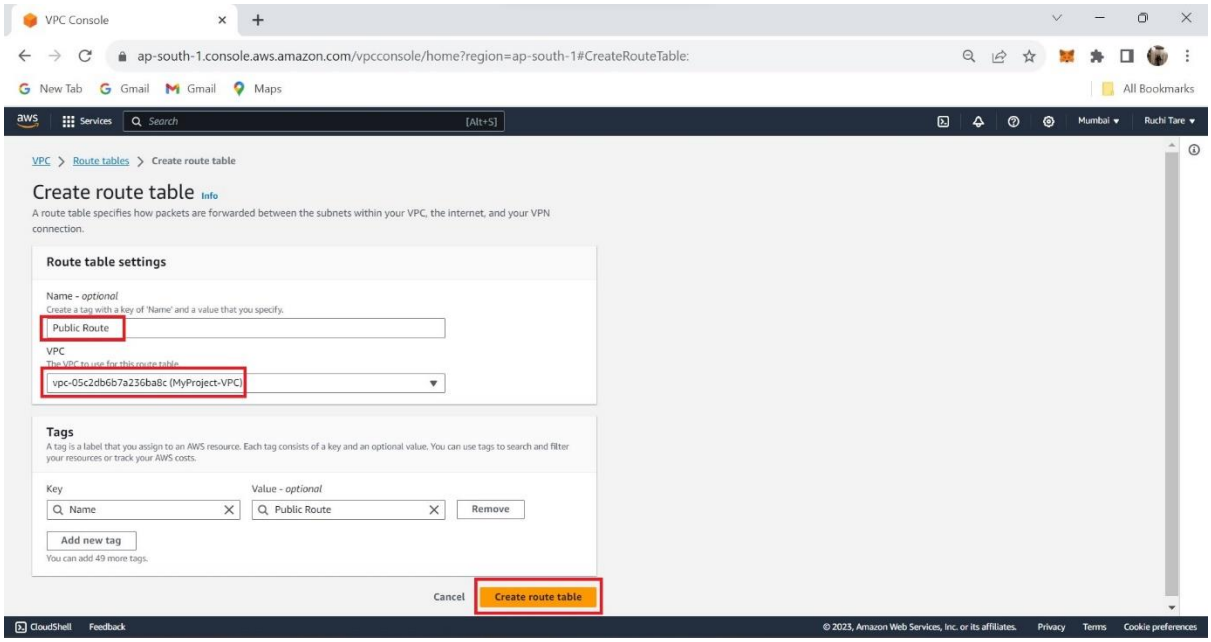


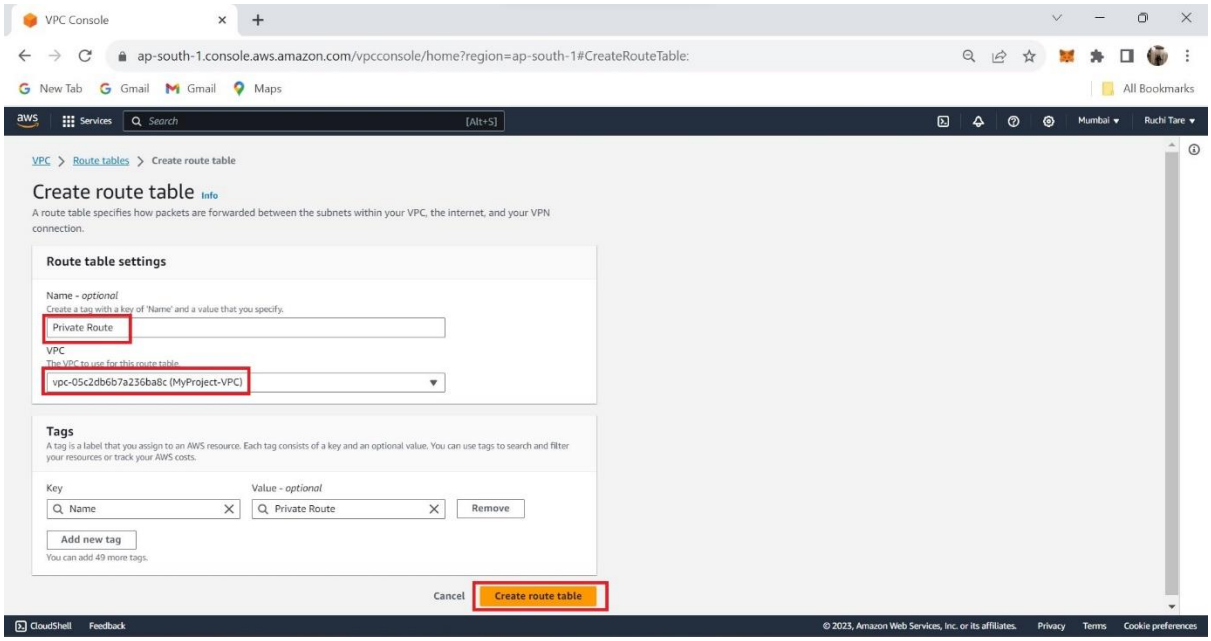
4. Create 2 Route table of which one is public and private

First click on create Route Table

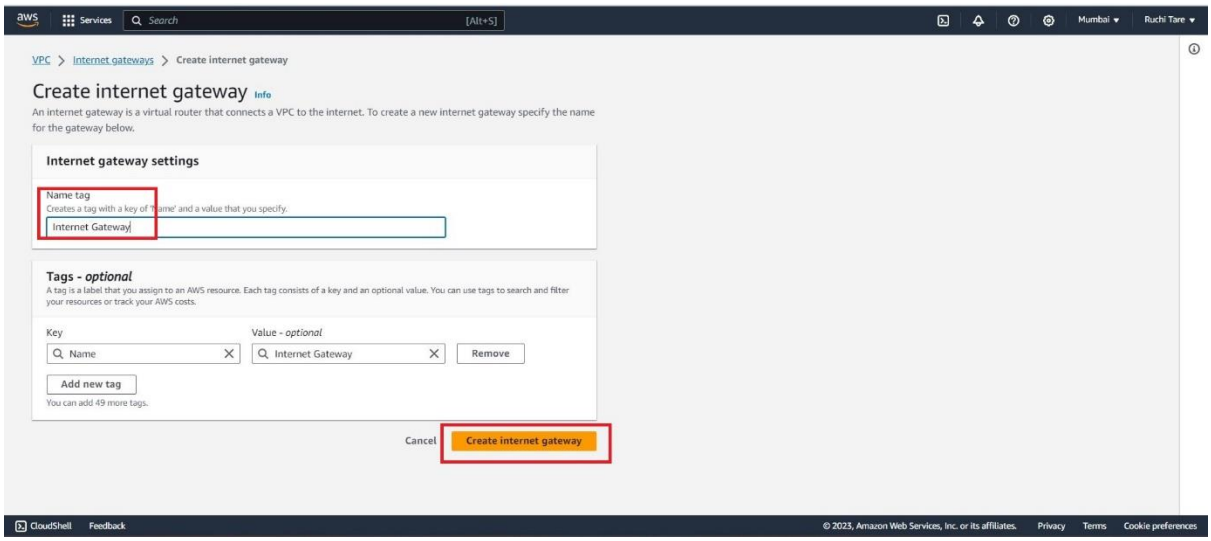


Create a public route table , add the created vpc and the name for route table do the same for private route table

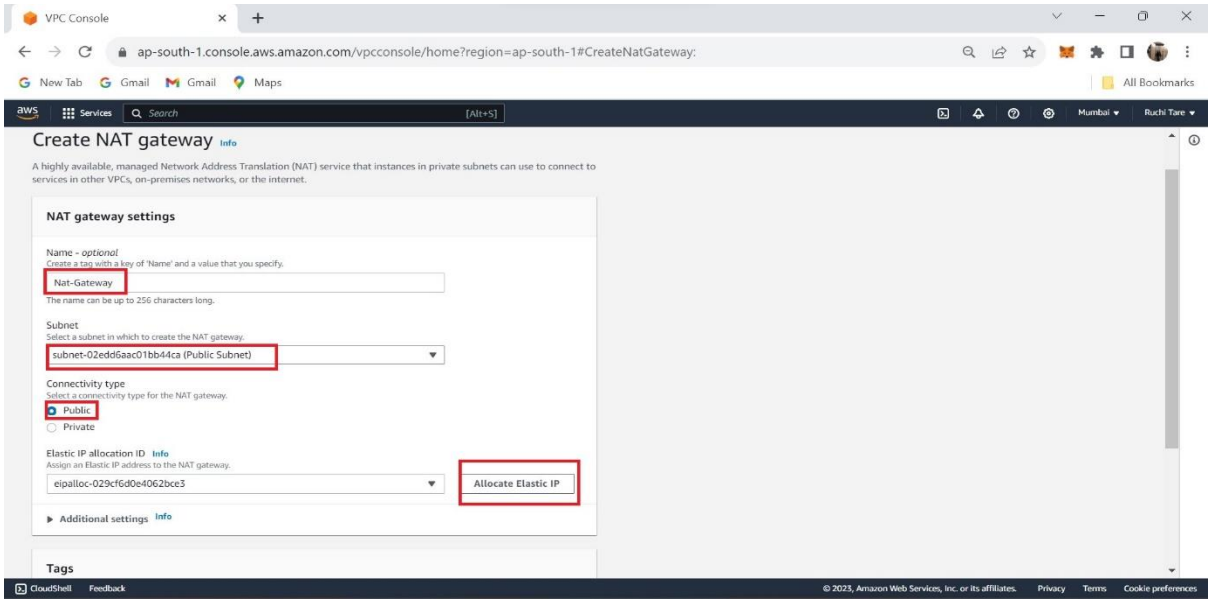




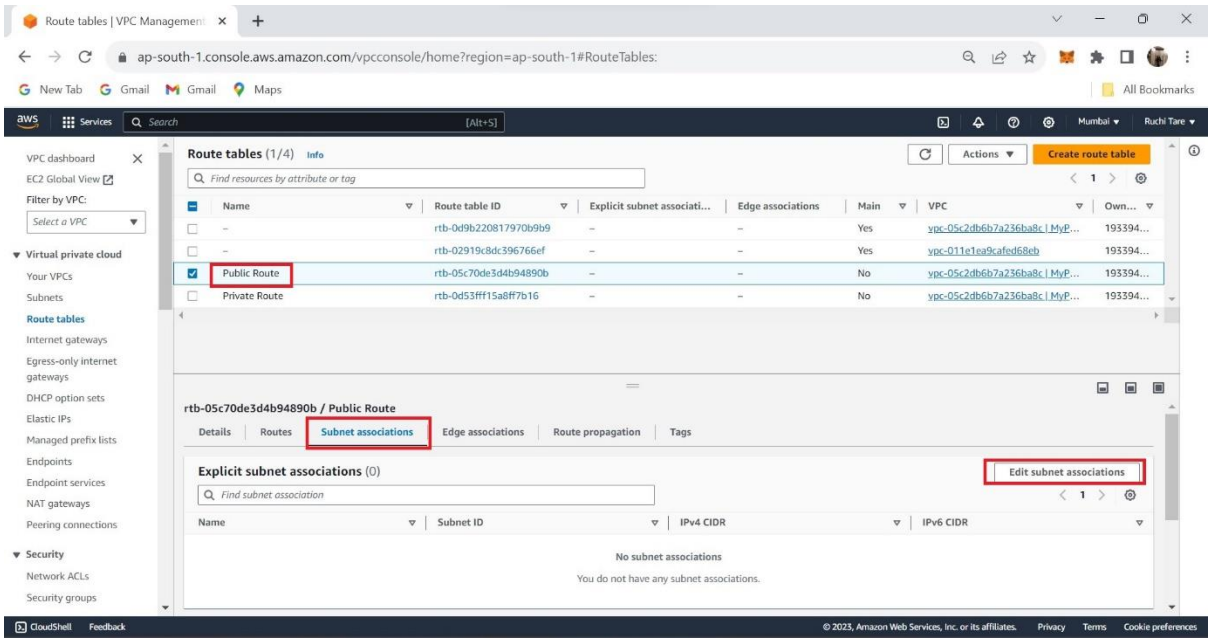
5. Create a Internet Gateway for connecting Internet to Subnets and also attach that with vpc

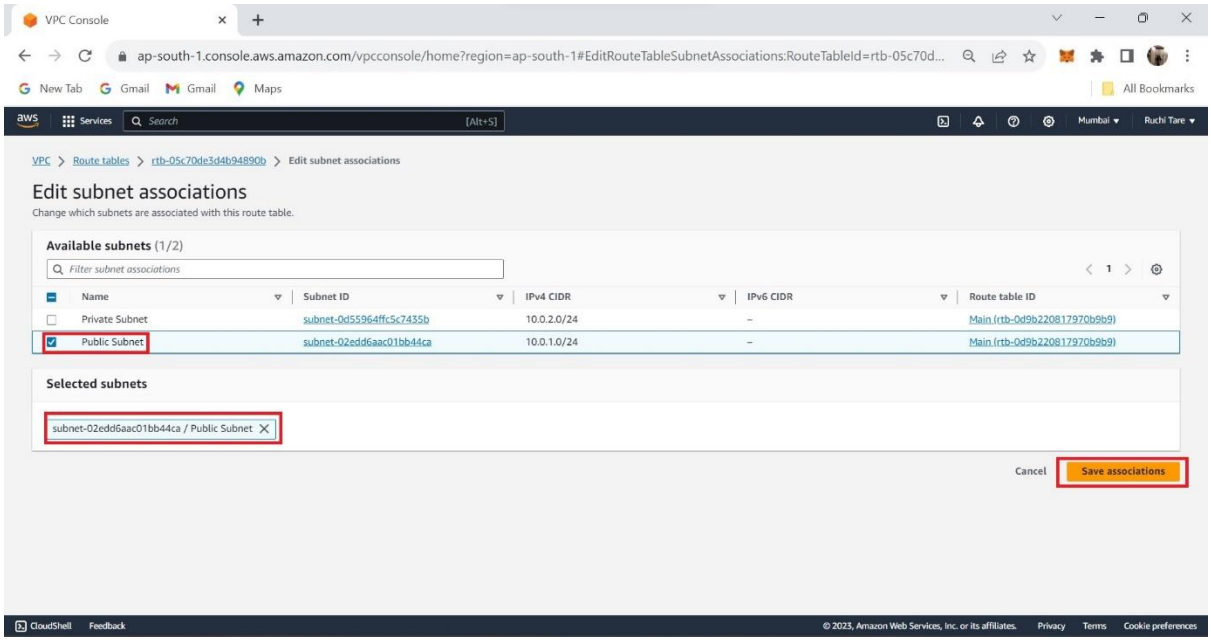


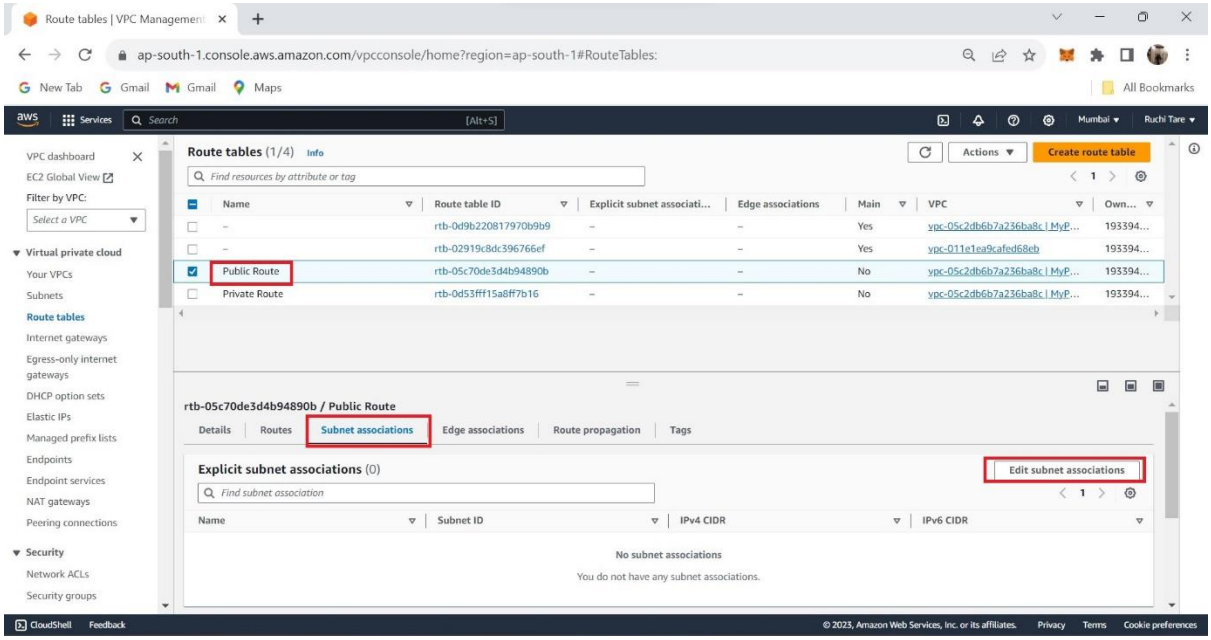
6. Create a NAT gateway for connecting private subnet through internet, we will place Nat gateway in the public subnet also we will attach elastic IP to it.



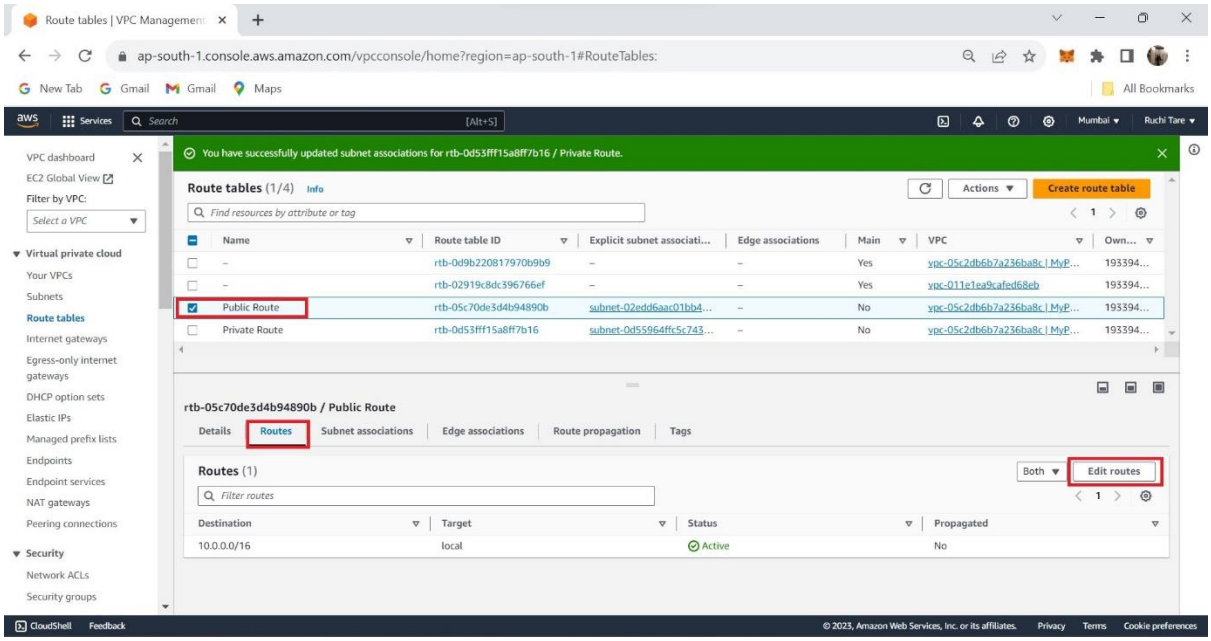
7. Next step is to Associate the subnets to the Route Table , Public route to public subnet and private route to the private subnet.



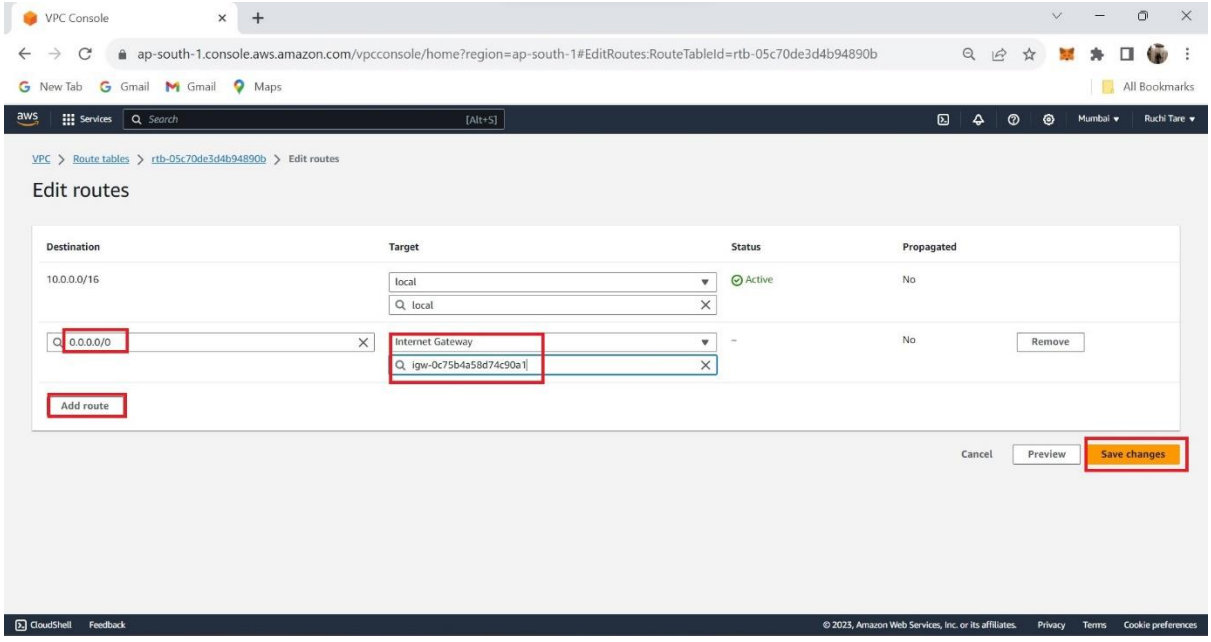

VPC Console
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#EditRouteTableSubnetAssociations:RouteTableId=rtb-05c70d...
New Tab
Gmail
Gmail
Maps
All Bookmarks
Services
Search
[Alt+S]
Mumbai
Ruchi Tare
VPC > Route tables > rtb-05c70de3d4b94890b > Edit subnet associations
Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (1/2)
Filter subnet associations
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
Private Subnet
subnet-0d55964ffc5c7435b
10.0.2.0/24
–
Main (rtb-0d9b220817970b9b9)
Public Subnet
subnet-02edd6aac01bb44ca
10.0.1.0/24
–
Main (rtb-0d9b220817970b9b9)
Selected subnets
subnet-02edd6aac01bb44ca / Public Subnet
Cancel
Save associations
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Route tables | VPC Management
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTables:
New Tab
Gmail
Gmail
Maps
All Bookmarks
Services
Search
[Alt+S]
Mumbai
Ruchi Tare
VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
Route tables (1/4) Info
Find resources by attribute or tag
Actions
Create route table
Name
Route table ID
Explicit subnet associati...
Edge associations
Main
VPC
Own...
–
rtb-0d9b220817970b9b9
–
–
Yes
vpc-05c2db6b7a236ba8c | MyP...
193394...
–
rtb-02919c8dc396766ef
–
–
Yes
vpc-011e1ea9cafed68eb
193394...
Public Route
rtb-05c70de3d4b94890b
–
–
No
vpc-05c2db6b7a236ba8c | MyP...
193394...
Private Route
rtb-0d53fff15a8ff7b16
–
–
No
vpc-05c2db6b7a236ba8c | MyP...
193394...
rtb-05c70de3d4b94890b / Public Route
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (0)
Find subnet association
Edit subnet associations
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
No subnet associations
You do not have any subnet associations.
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

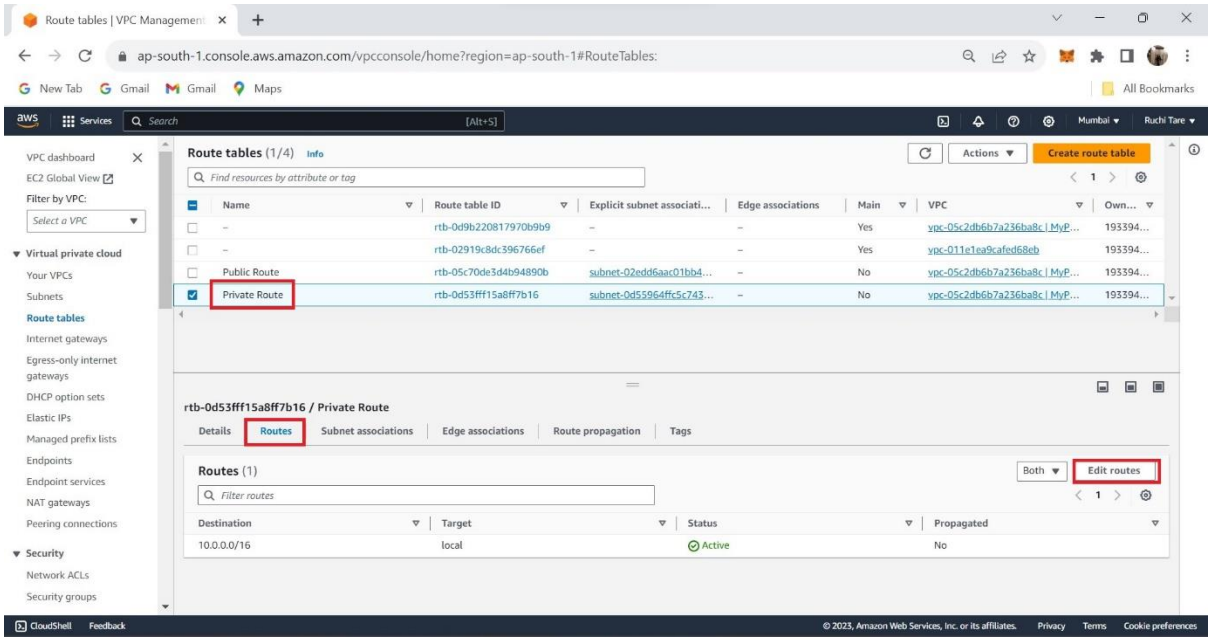
7. Route the Internet Gateway with public route for providing internet connectivity.

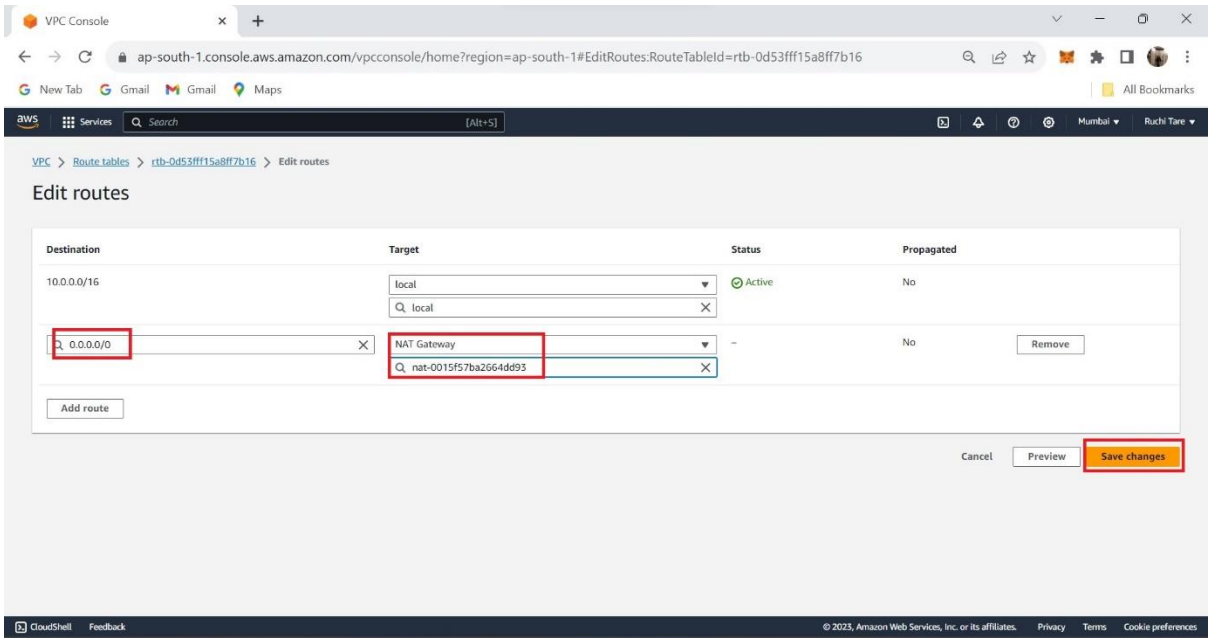


Click on public subnet → route → Edit route → Add Route → select 0.0.0.0/0 →Internet gateway → save changes.



DO the same process with the Private Subnet but instead of Internet gateway you will have to add NAT Gateway , you will provide internet to the private subnet through NAT Gateway.

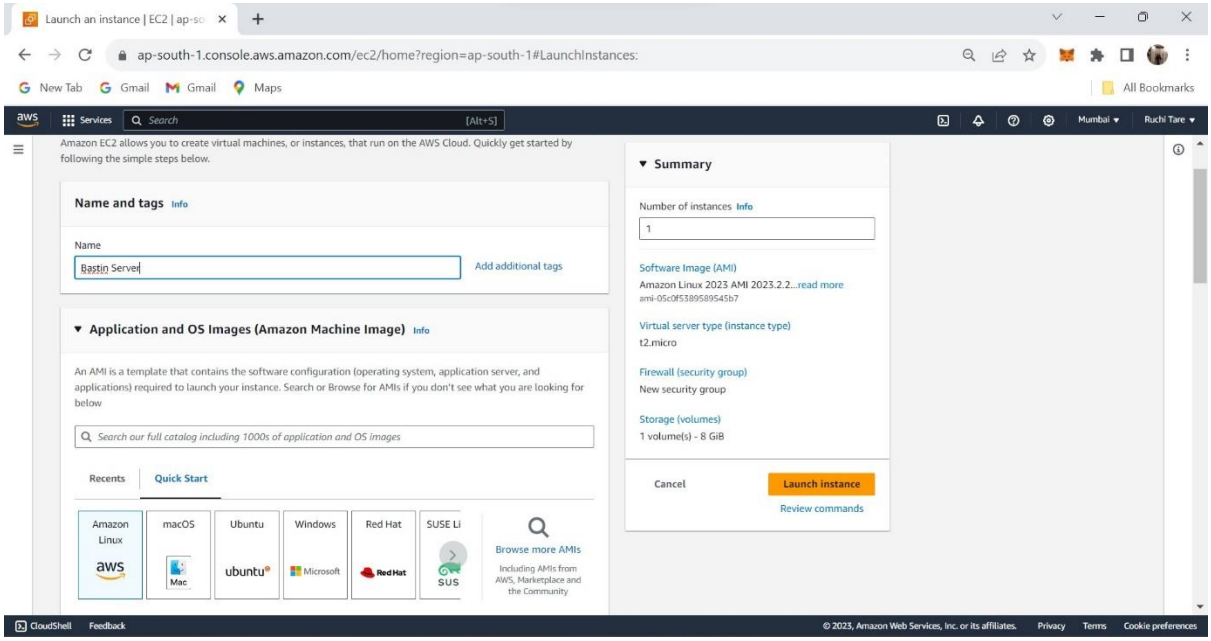




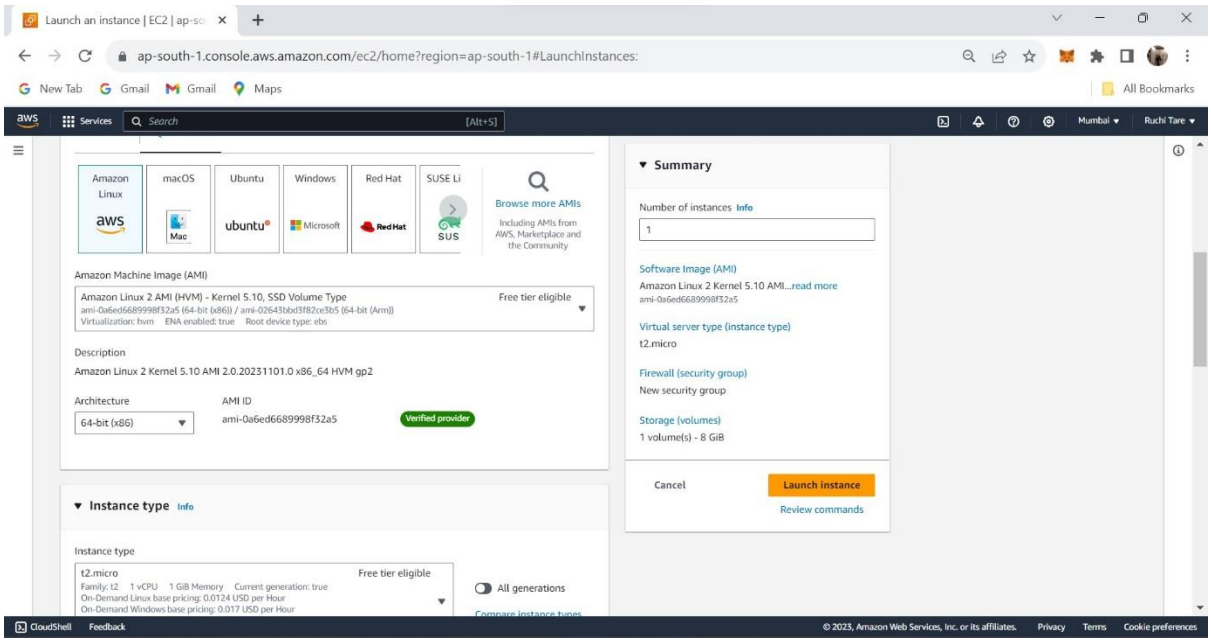
Step 2: Now create EC2 environment:

1. Go to EC2 and create two instance
2. 1st instance is Bastin Server which is a Public server and this server is running on the Linux server for that for authentication we required Key , so download a .ppk file.

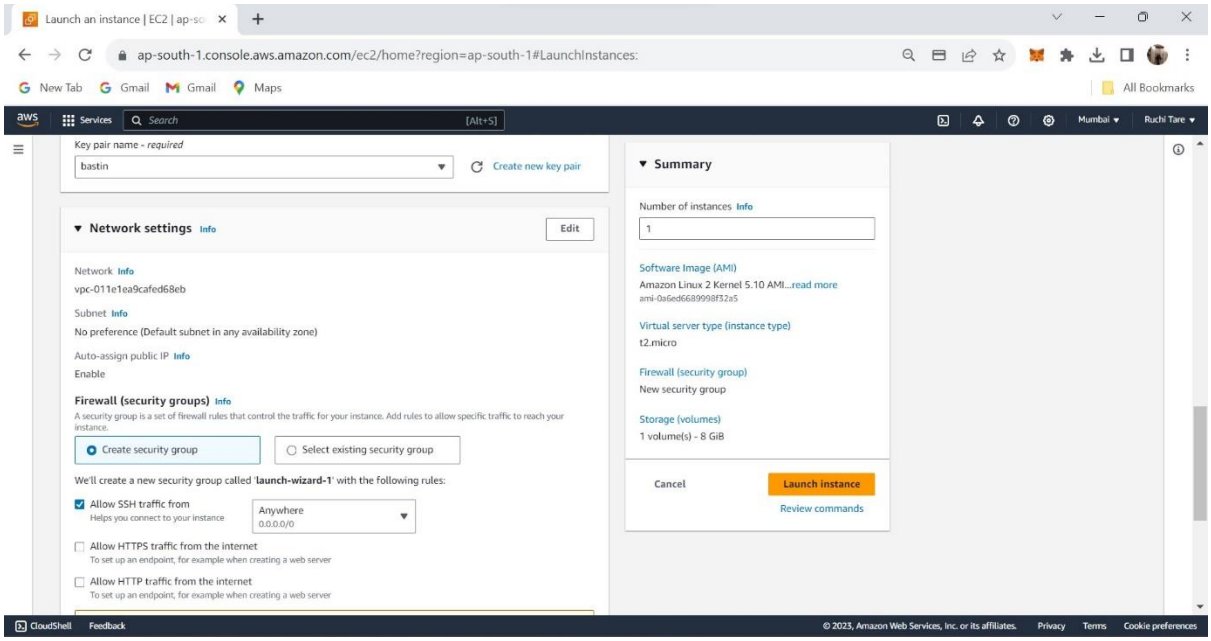
Write the name of the server you and select the operating system as linux.



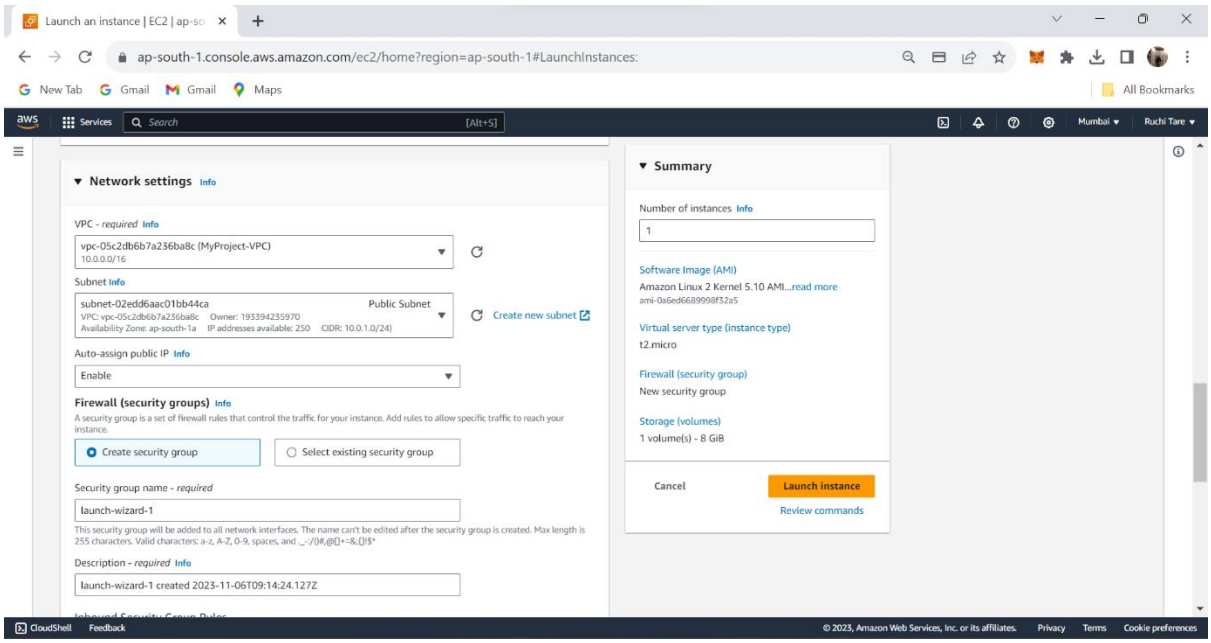
Select the Amazon Linux 2 AMI as your operating system. Select t2micro instance type.



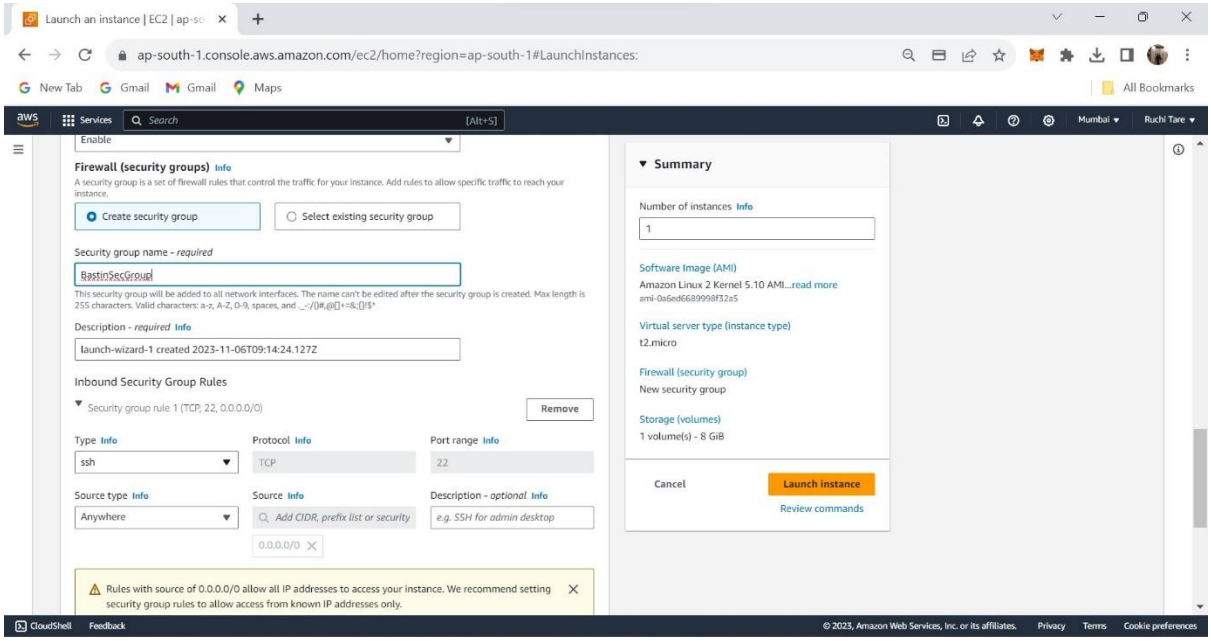
Select the key pair you have created and under network setting select the created VPC with the public subnet, enable the IP addresess.

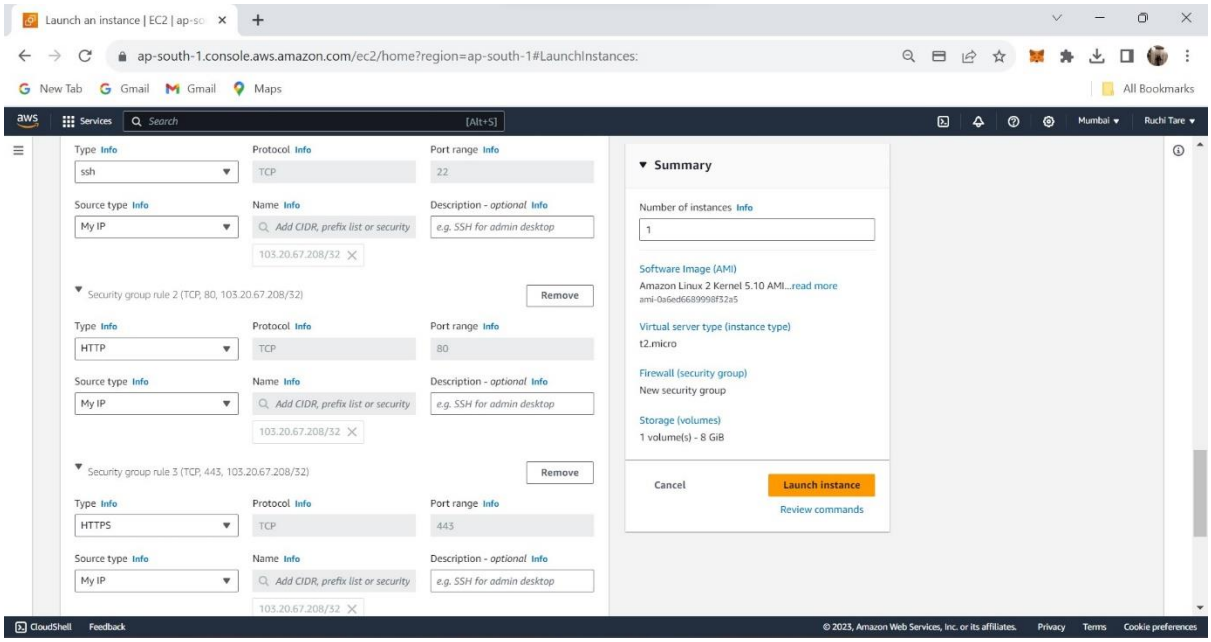


Create a new security group , give name to that group,



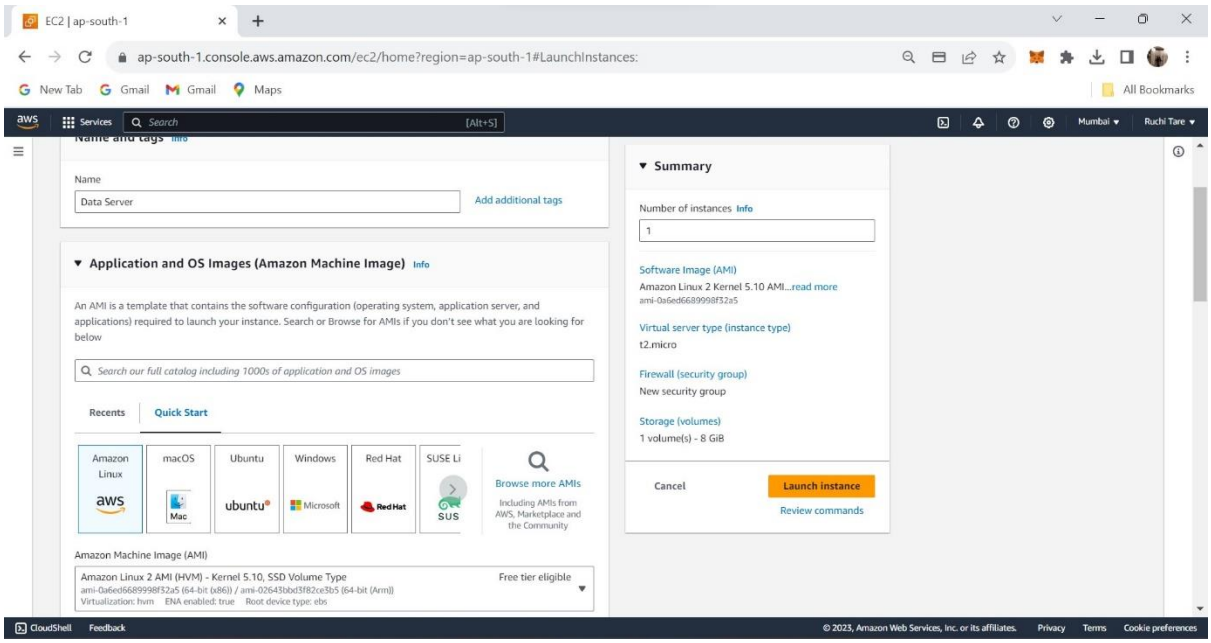
Add the security rule of SSH with MyIP followed by MySql, HTTP and HTTPS with the security type as MyIP.

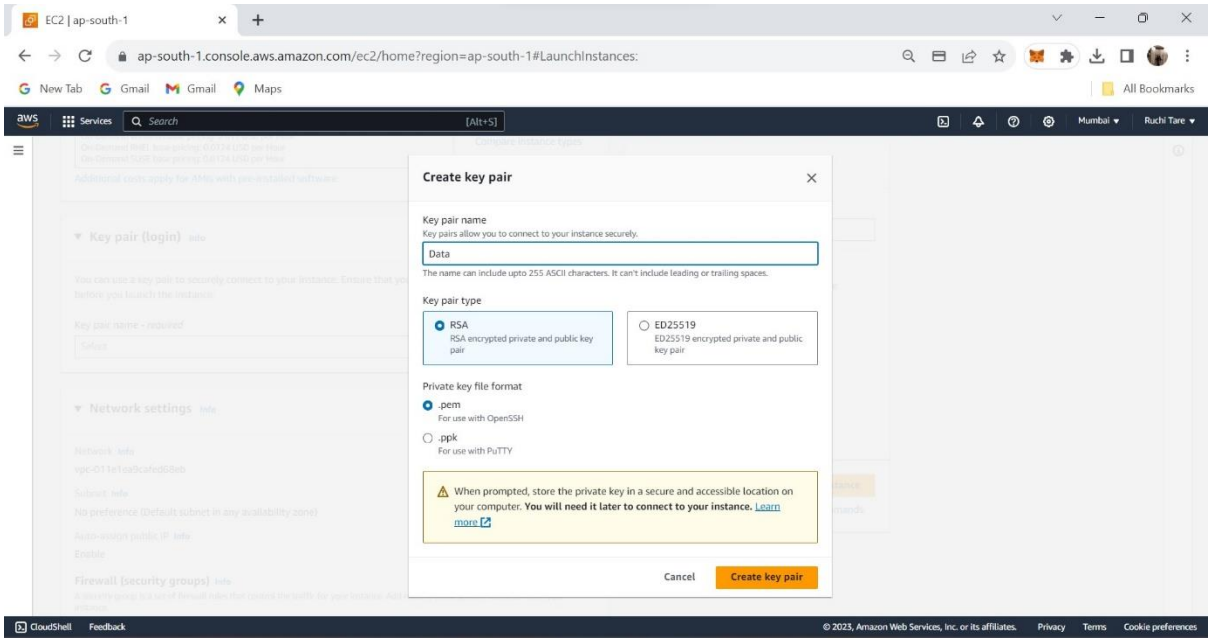


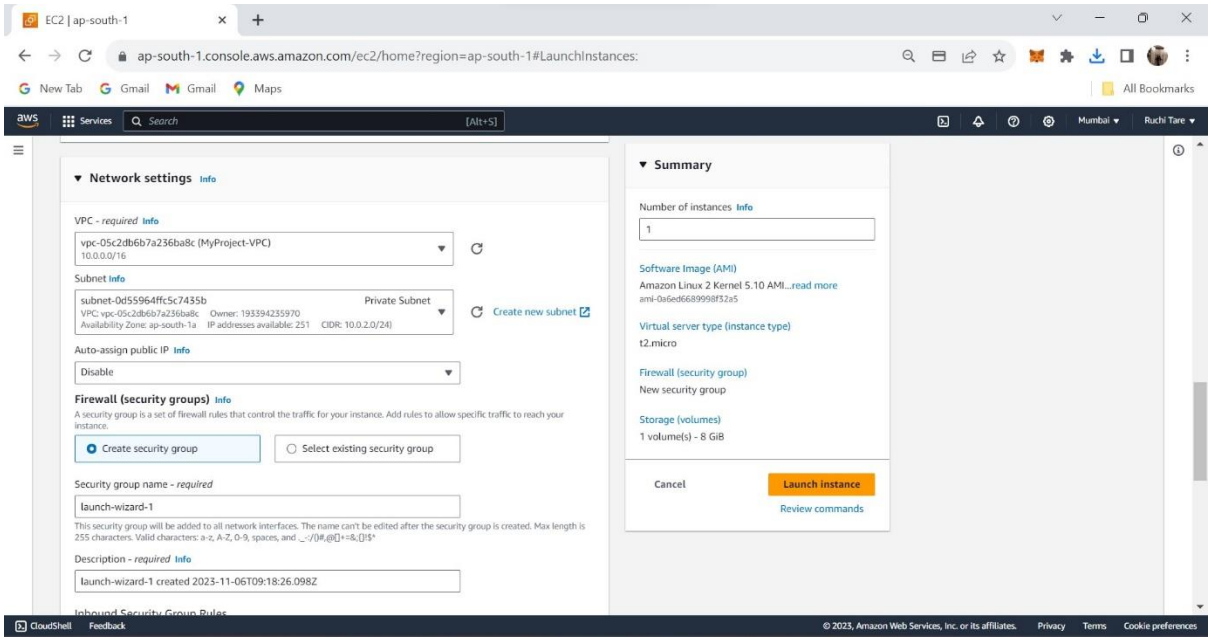


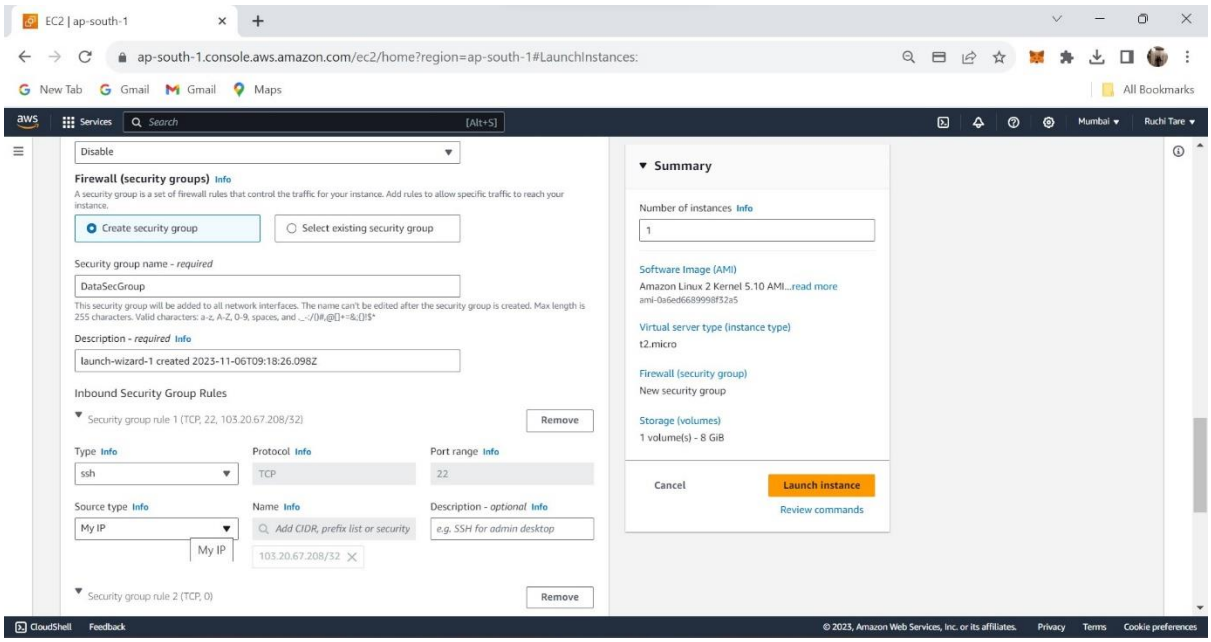
After the above steps are done recheck it and the click on the Launch the Instance button.

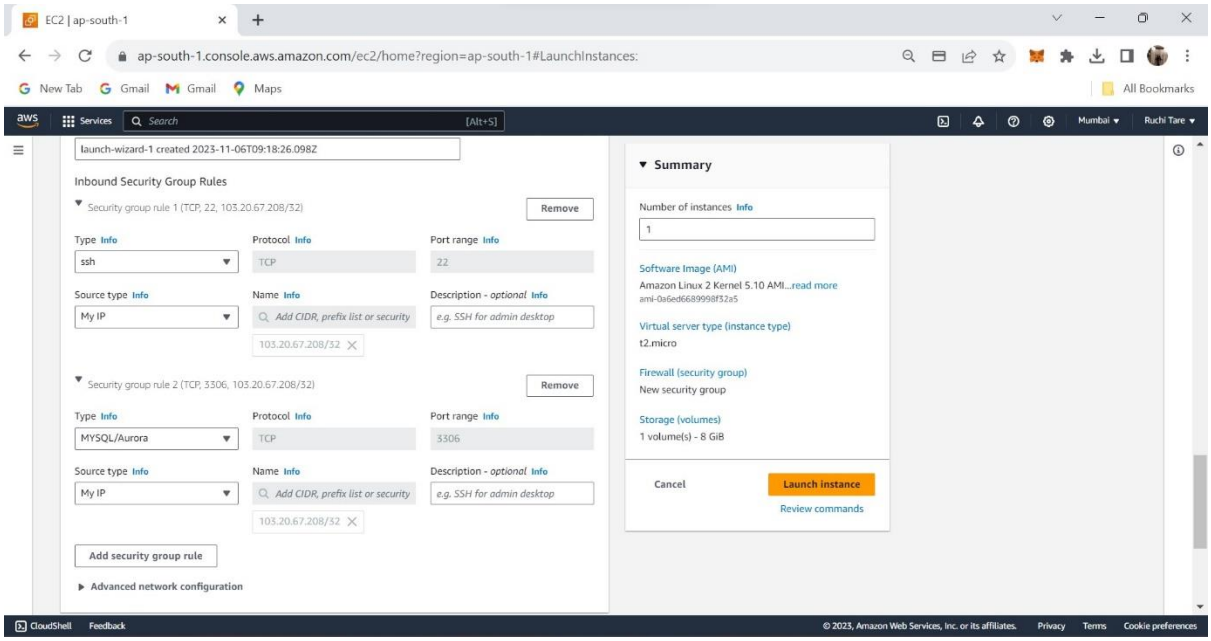
3. 2nd instance is Data instance with the Data.pem key followed by its name and new Security group with security rule as SSH and MySql and Http and Https.



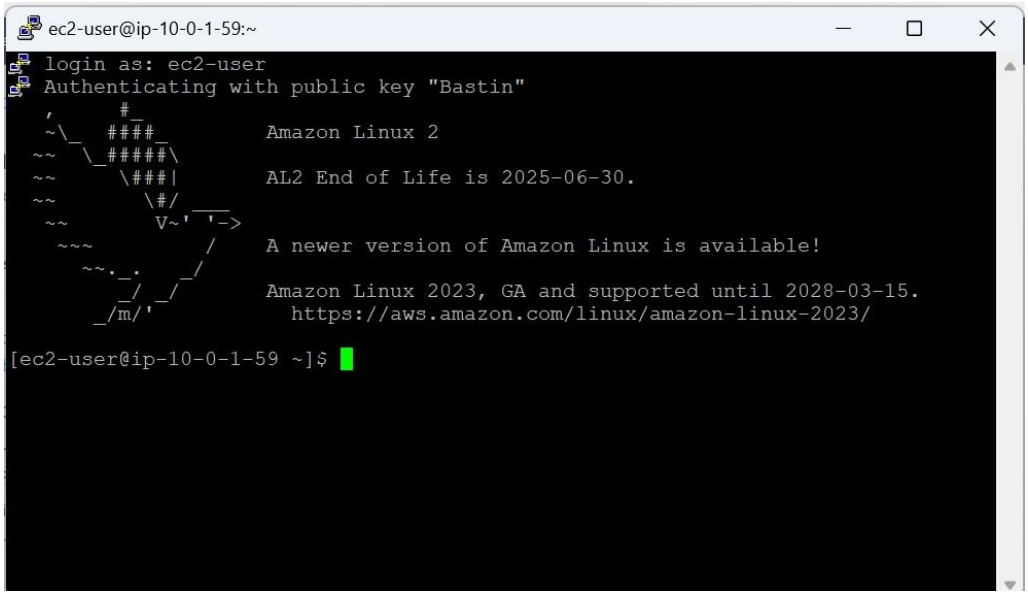



EC2 | ap-south-1
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
New Tab
Gmail
Gmail
Maps
All Bookmarks
Services
Search
[Alt+S]
Mumbai
Ruchi Tare
Network settings Info
VPC - required Info
vpc-05c2db6b7a236ba8c (MyProject-VPC)
10.0.0.0/16
Subnet Info
subnet-0d55964ffc5c7435b
Private Subnet
VPC: vpc-05c2db6b7a236ba8c Owner: 193394235970
Availability Zone: ap-south-1a IP addresses available: 251 CIDR: 10.0.2.0/24)
Create new subnet
Auto-assign public IP Info
Disable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Security group name - required
launch-wizard-1
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#,@[]+=&;{}!$*
Description - required Info
launch-wizard-1 created 2023-11-06T09:18:26.098Z
Inbound Security Group Rules
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0a6ed6689998f32a5
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


EC2 | ap-south-1
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
New Tab
Gmail
Gmail
Maps
All Bookmarks
Services
Search
[Alt+S]
Mumbai
Ruchi Tare
Disable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Security group name - required
DataSecGroup
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#,@[]+=&;{}!$*
Description - required Info
launch-wizard-1 created 2023-11-06T09:18:26.098Z
Inbound Security Group Rules
Security group rule 1 (TCP, 22, 103.20.67.208/32)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
My IP
Name Info
Add CIDR, prefix list or security
Description - optional Info
e.g. SSH for admin desktop
My IP
103.20.67.208/32
Security group rule 2 (TCP, 0)
Remove
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0a6ed6689998f32a5
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



4. Connect the Bastin Server.
5. To connect bastin server you will have to first download putty app https://www.putty.org/
6. Open the putty server paste your bastin Public IP in the addresses of your putty then go to SSH→Auth→Credential then browser your .ppk key of your bastin server and select that key your bastin terminal will get open

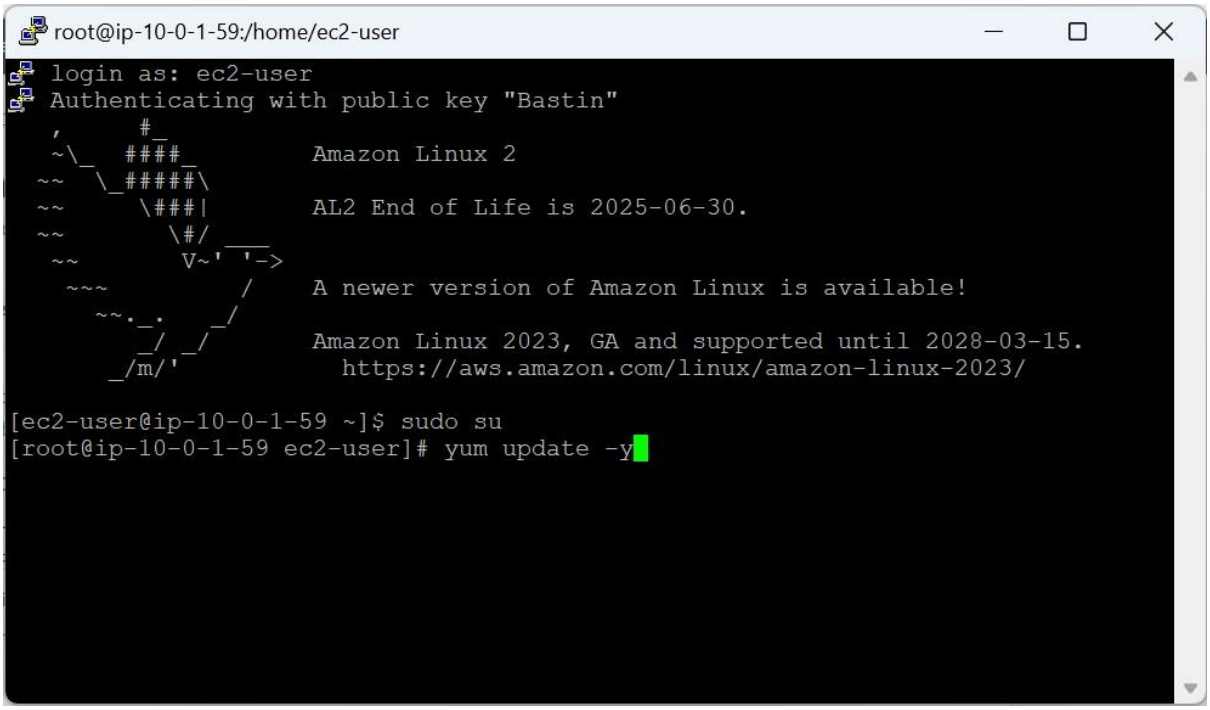


Login to Bastin server through the command **ec2-user**.

Then write the command

Sudo su

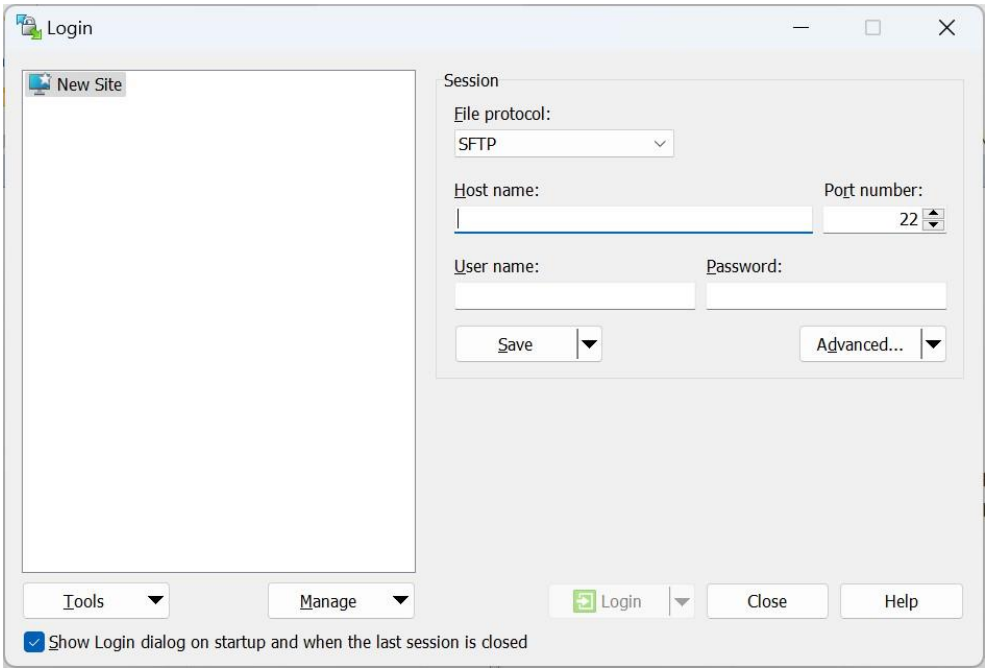
Yum update -y in your bastin terminal

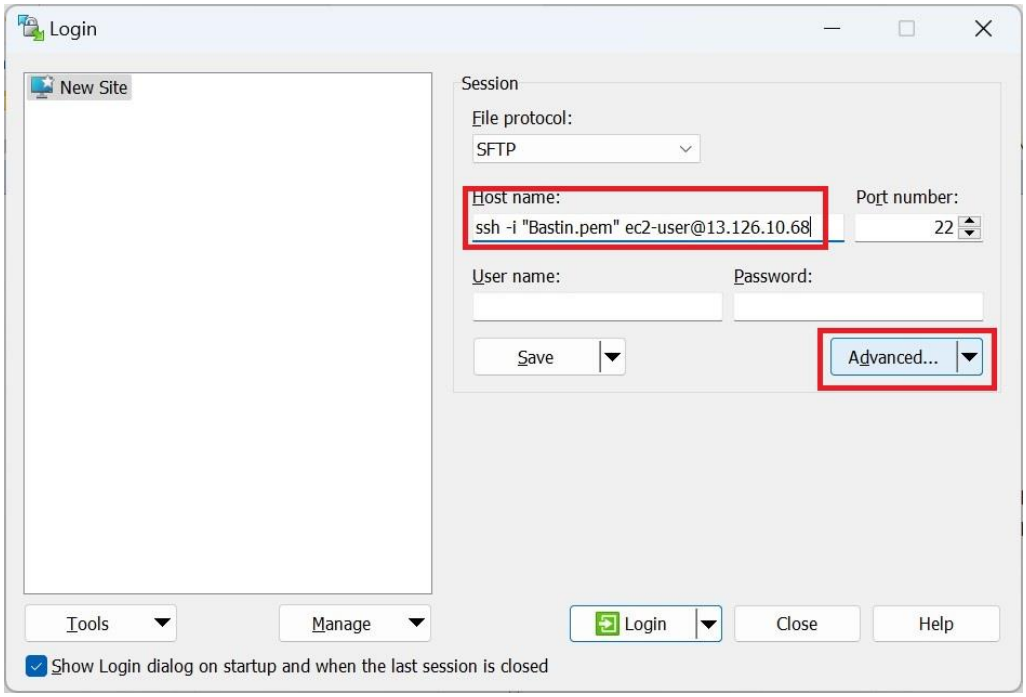


7. Download the Winscp in your computer [https://winscp.net/eng/download.php.](https://winscp.net/eng/download.php)

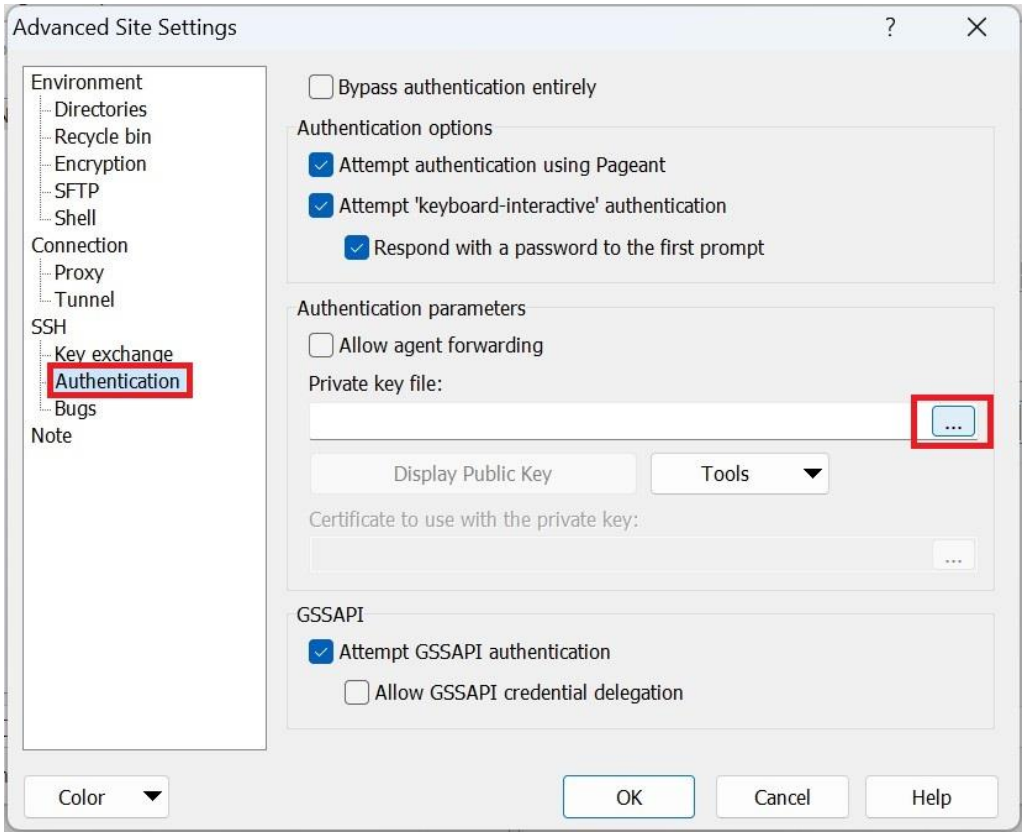
Once the Winscp is downloaded and installed properly login into it with bastin hostname.

To copy the hostname go to bastin instance→select the bastin instance→connect→ssh→example url.

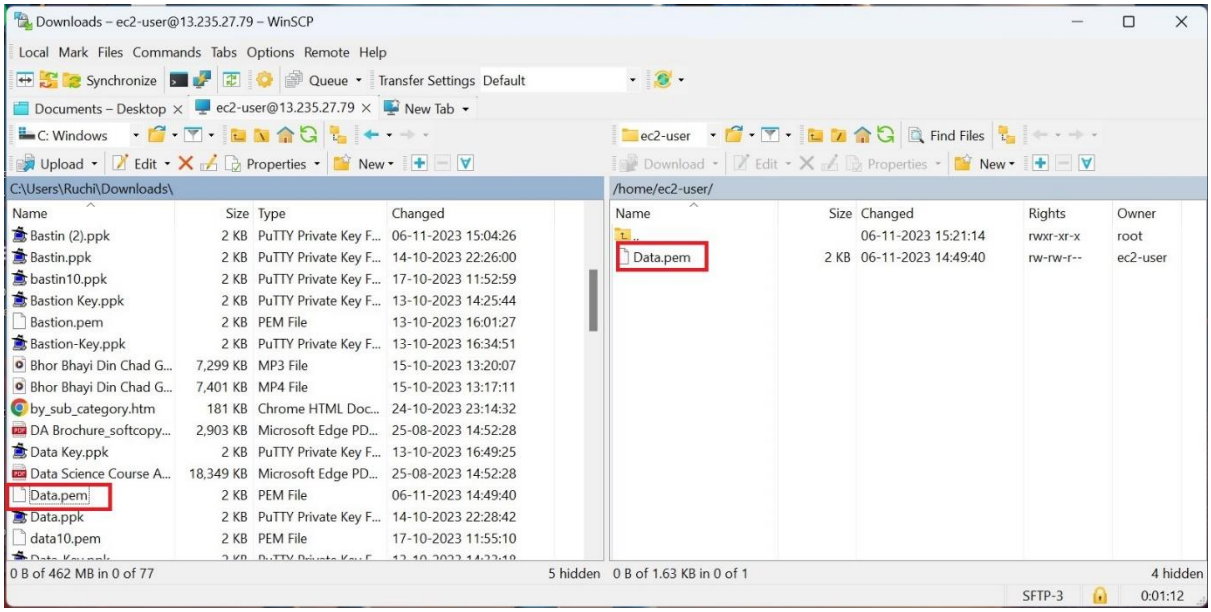




After copying the hostname then paste the url and then click on advance.

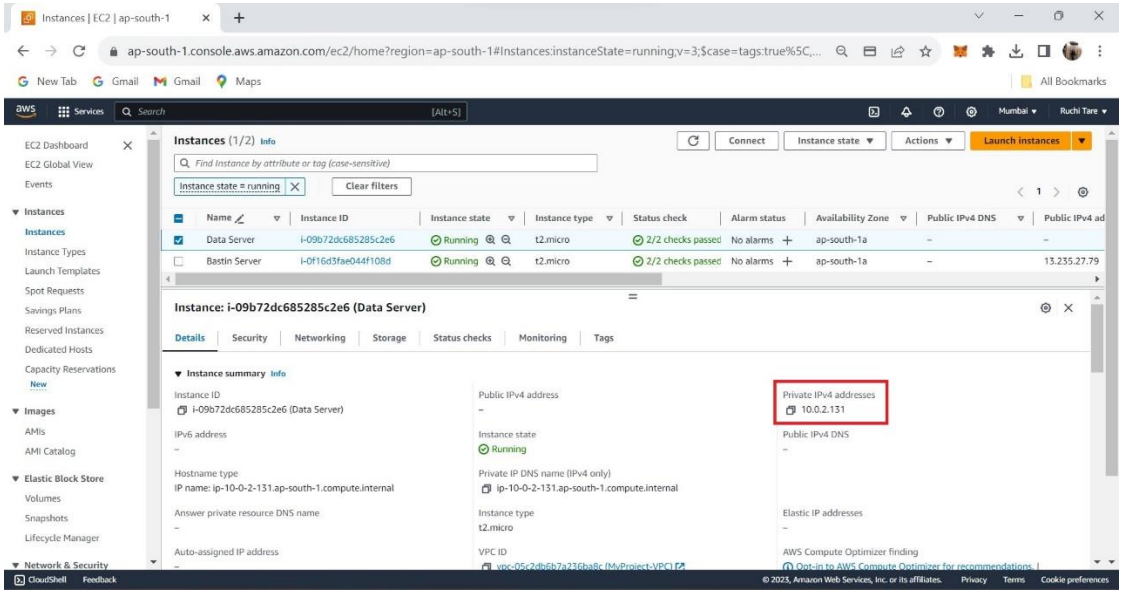


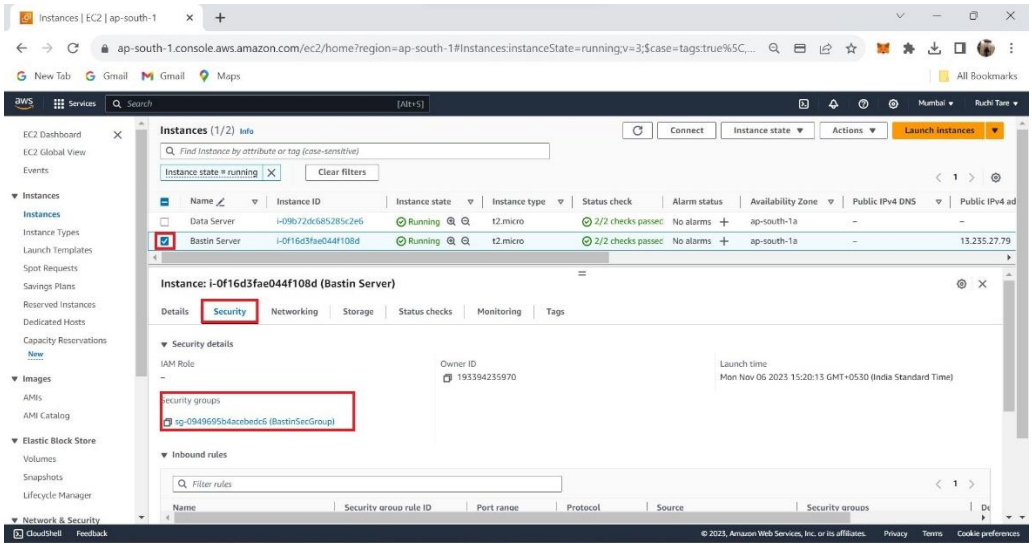
Click on Authentication on SSH and the browser for your bastin .ppk key select that key and click on ok.

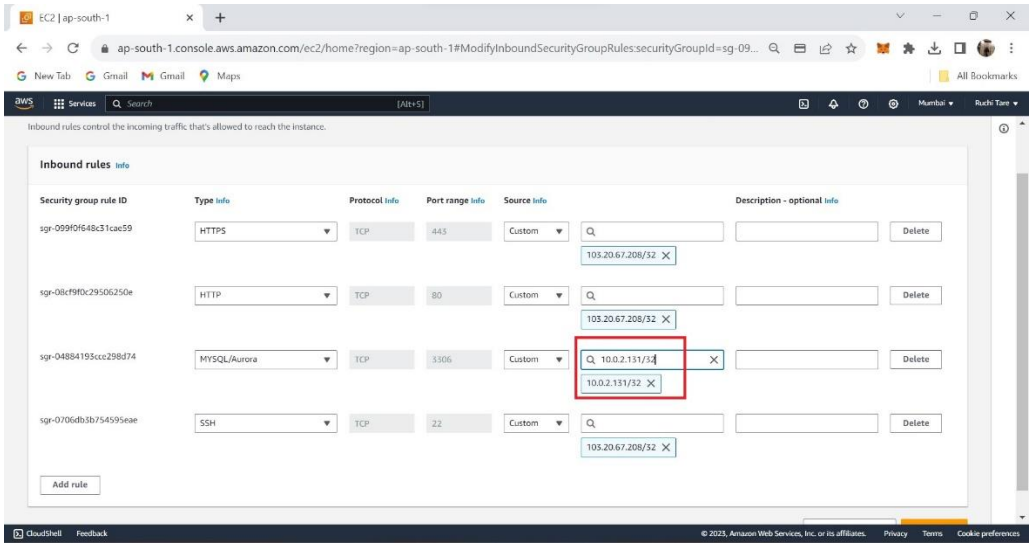


After that on the left side check for your data.pem key and drag and paste it on the right side of your winscp.

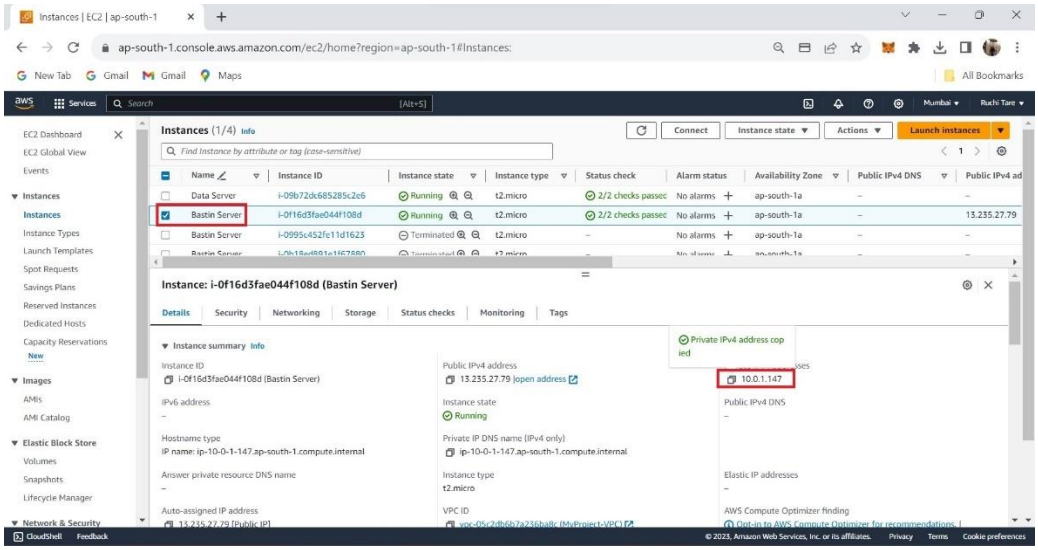
8. Come back to your console and in EC2 service select the Data instance copy the private key of DATA and paste it in the security group of BASTIN Security group MYSQL.

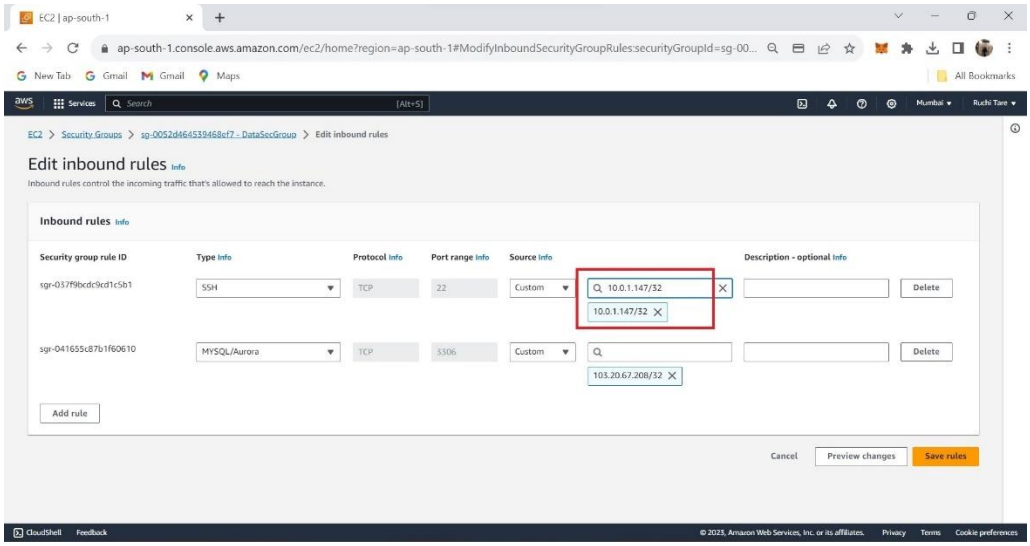




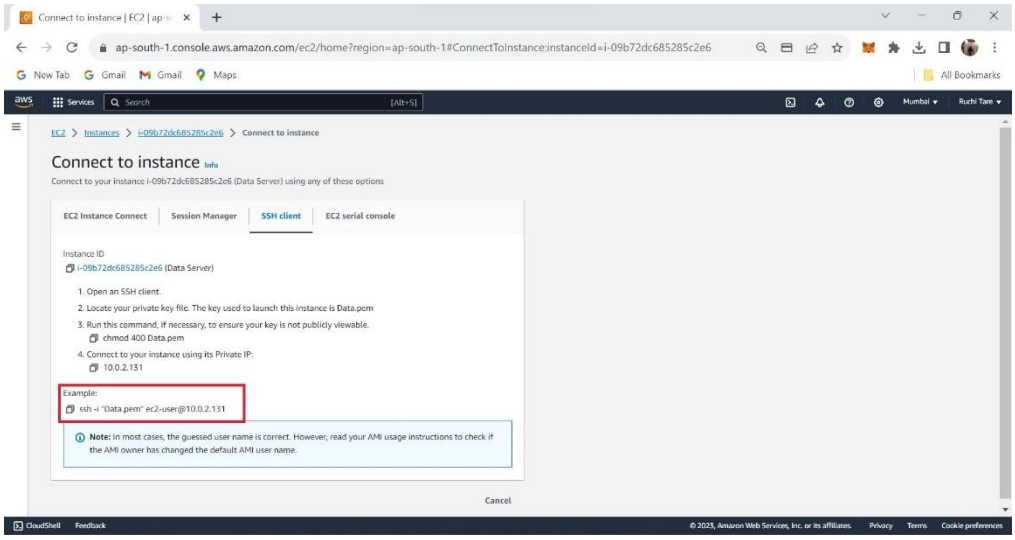


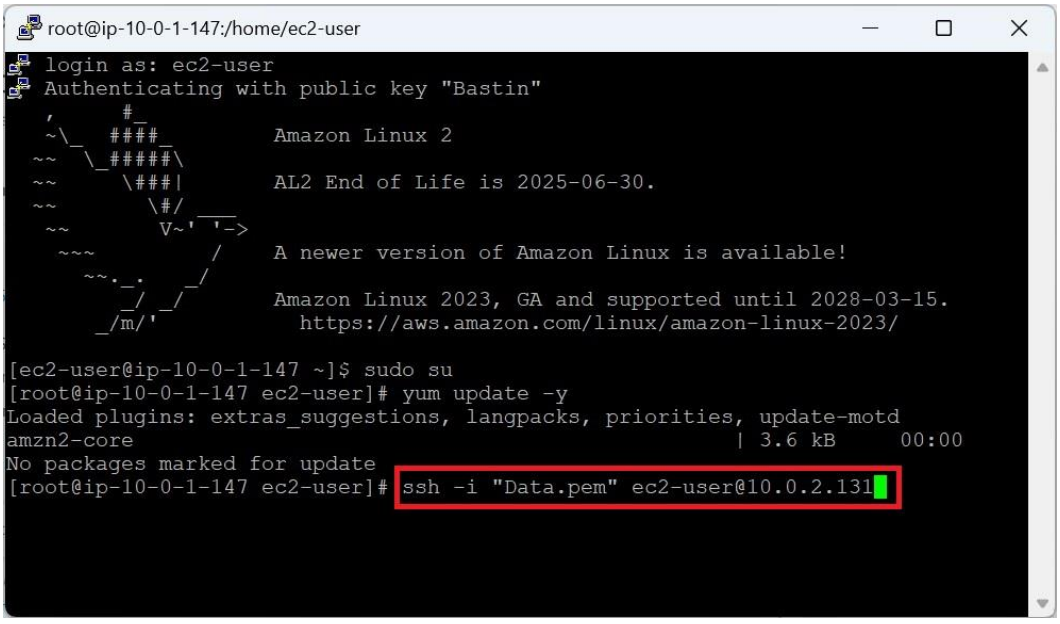
9. Copy the bastin private key and paste it to Data Security Group SSH.





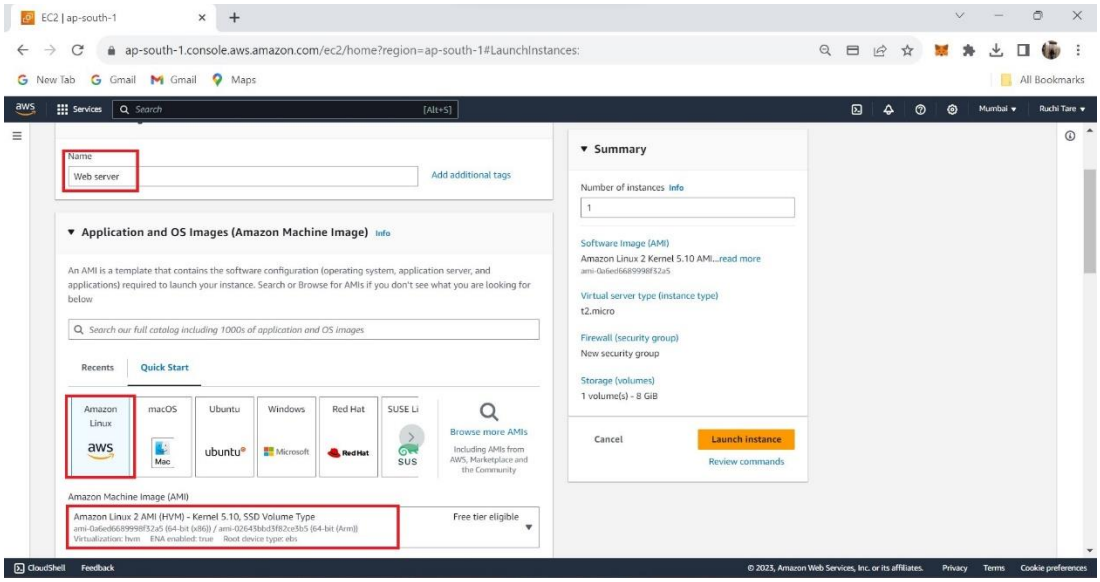
10. Select the Data instance→connect and copy the entire example url and paste it in Bastin CMD.

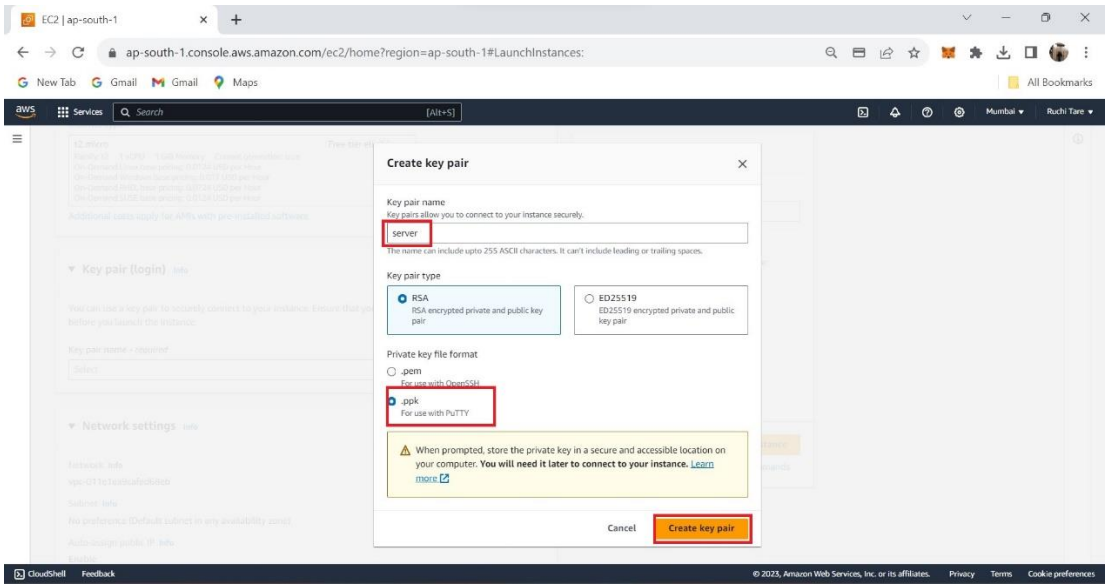


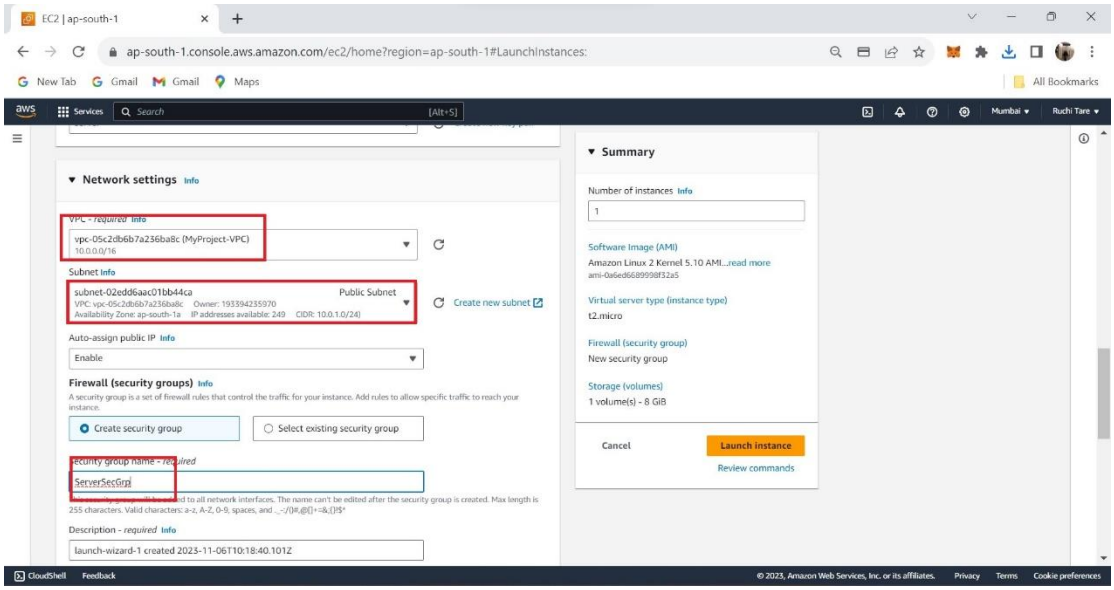


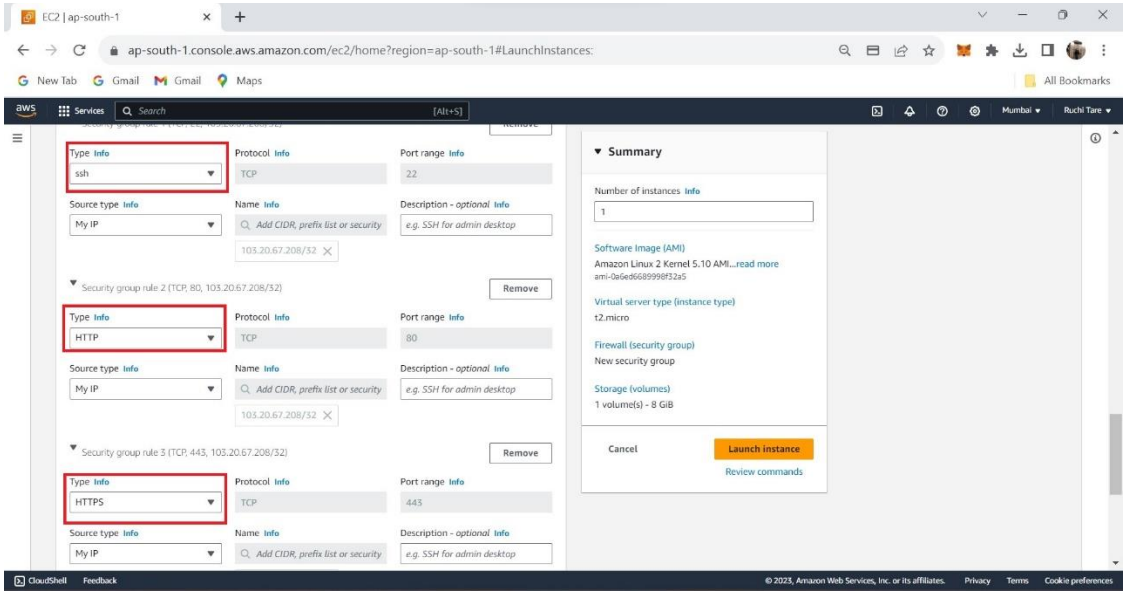
Step 3:

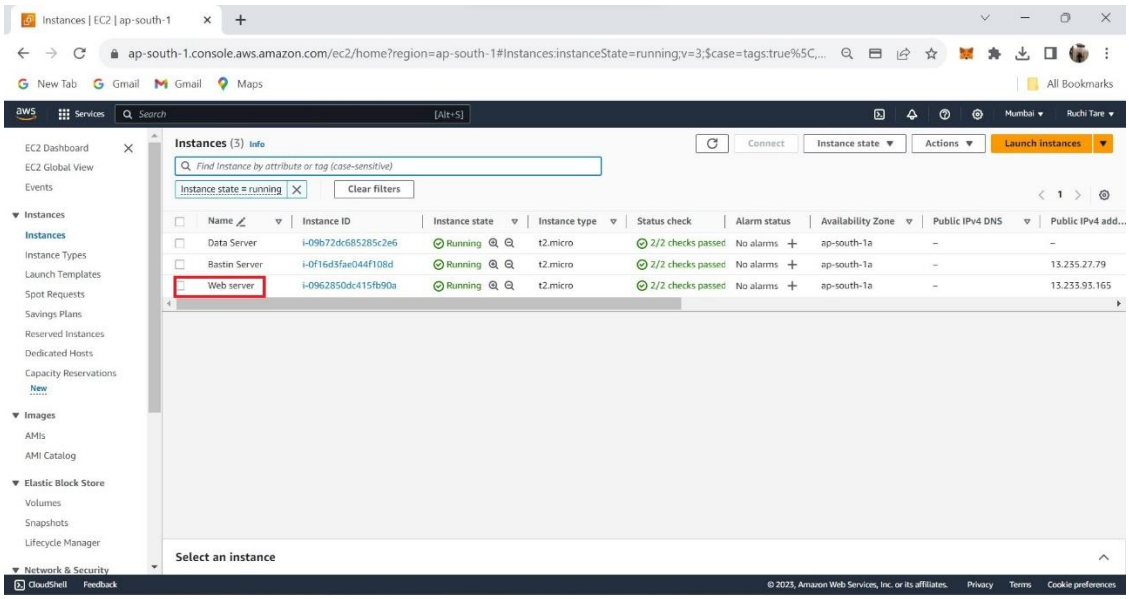
1. Launch a Web Server name “Instance” with the Linux OS along with key pair and Security group of HTTP&HTTPS.



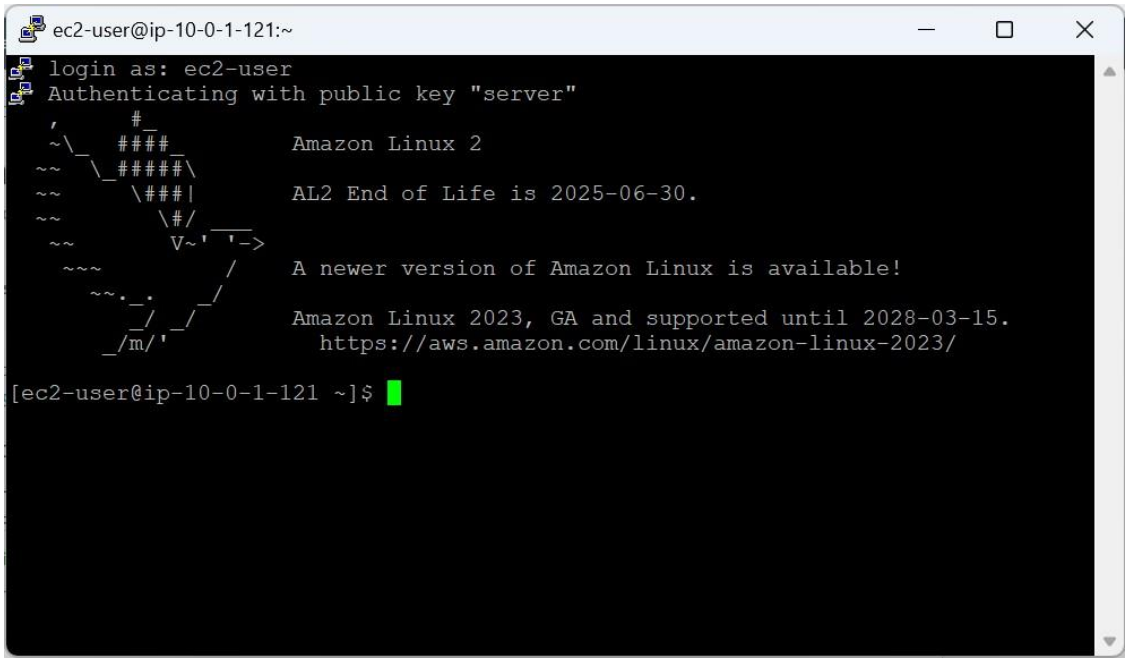


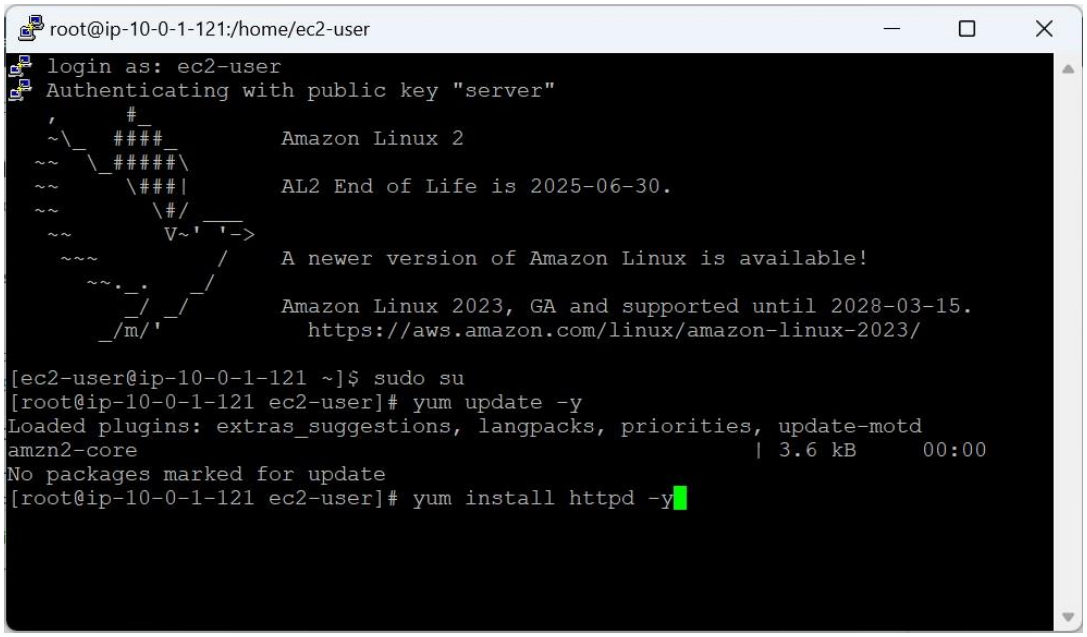

EC2 | ap-south-1
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Network settings Info
VPC - required Info
vpc-05c2db6b7a236ba8c (MyProject-VPC)
10.0.0.0/16
Subnet Info
subnet-02edd6aac01bb44ca
Public Subnet
Create new subnet
Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Security group name - required
ServerSecGrp
Description - required Info
launch-wizard-1 created 2023-11-06T10:18:40.101Z
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

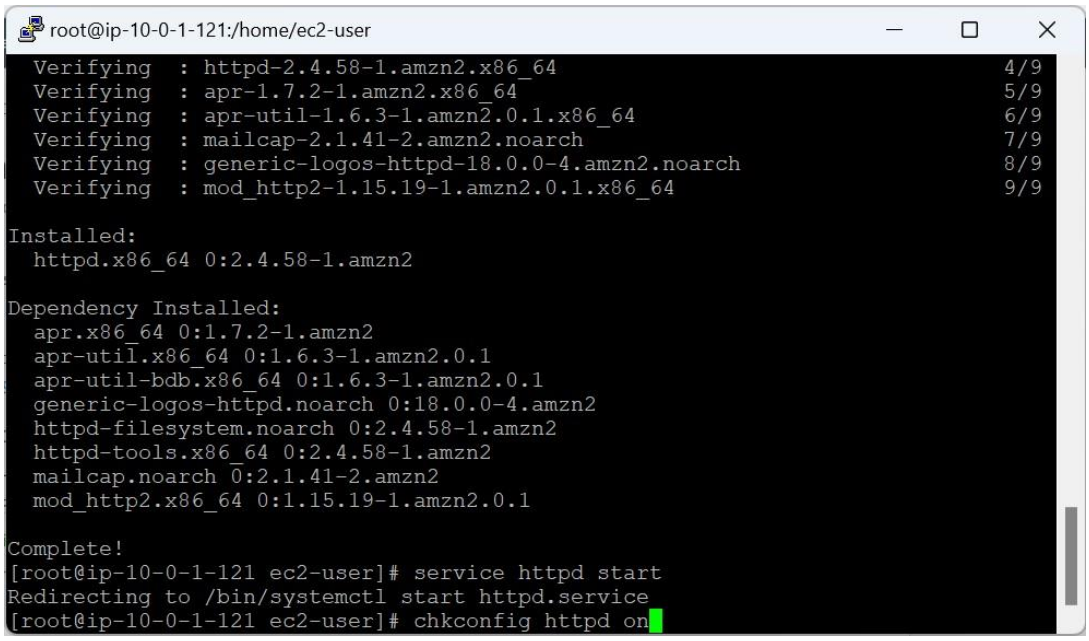

EC2 | ap-south-1
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
My IP
Name Info
Add CIDR, prefix list or security
Description - optional Info
e.g. SSH for admin desktop
103.20.67.208/32
Security group rule 2 (TCP, 80, 103.20.67.208/32)
Remove
Type Info
HTTP
Protocol Info
TCP
Port range Info
80
Source type Info
My IP
Name Info
Add CIDR, prefix list or security
Description - optional Info
e.g. SSH for admin desktop
103.20.67.208/32
Security group rule 3 (TCP, 443, 103.20.67.208/32)
Remove
Type Info
HTTPS
Protocol Info
TCP
Port range Info
443
Source type Info
My IP
Name Info
Add CIDR, prefix list or security
Description - optional Info
e.g. SSH for admin desktop
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

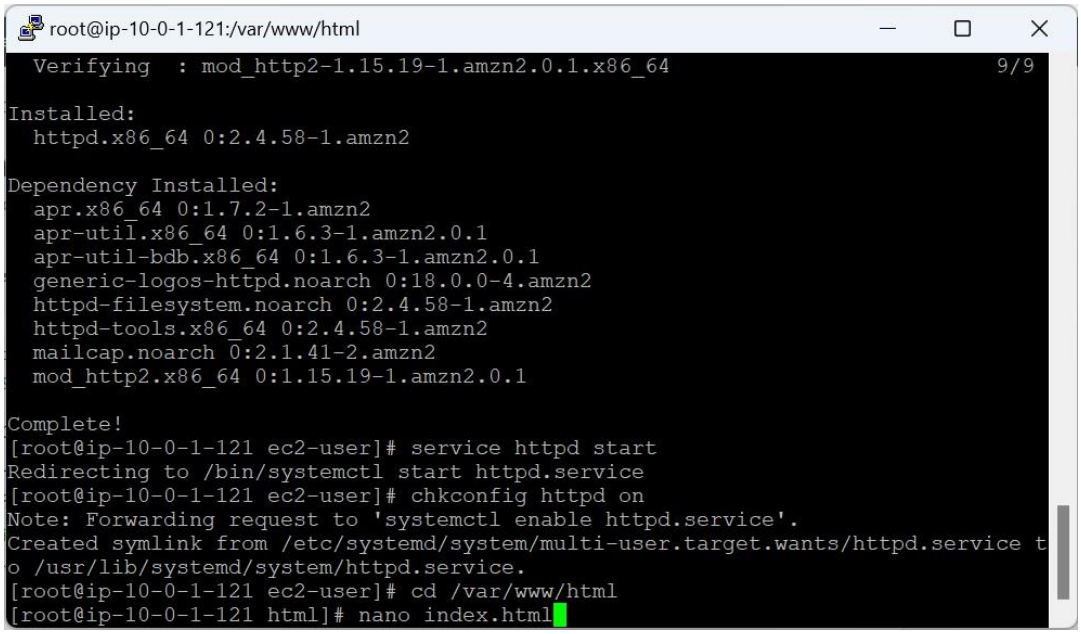

Instances | EC2 | ap-south-1
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:instanceState=running;v=3;$case=tags:true%5C,...
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Instances (3) Info
Find Instance by attribute or tag (case-sensitive)
Instance state = running
Clear filters
Connect
Instance state
Actions
Launch instances
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 add...
Data Server
i-09b72dc685285c2e6
Running
t2.micro
2/2 checks passed
No alarms
ap-south-1a
Bastin Server
i-0f16d3fae044f108d
Running
t2.micro
2/2 checks passed
No alarms
ap-south-1a
13.235.27.79
Web server
i-0962850dc415fb90a
Running
t2.micro
2/2 checks passed
No alarms
ap-south-1a
13.233.93.165
Select an instance
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

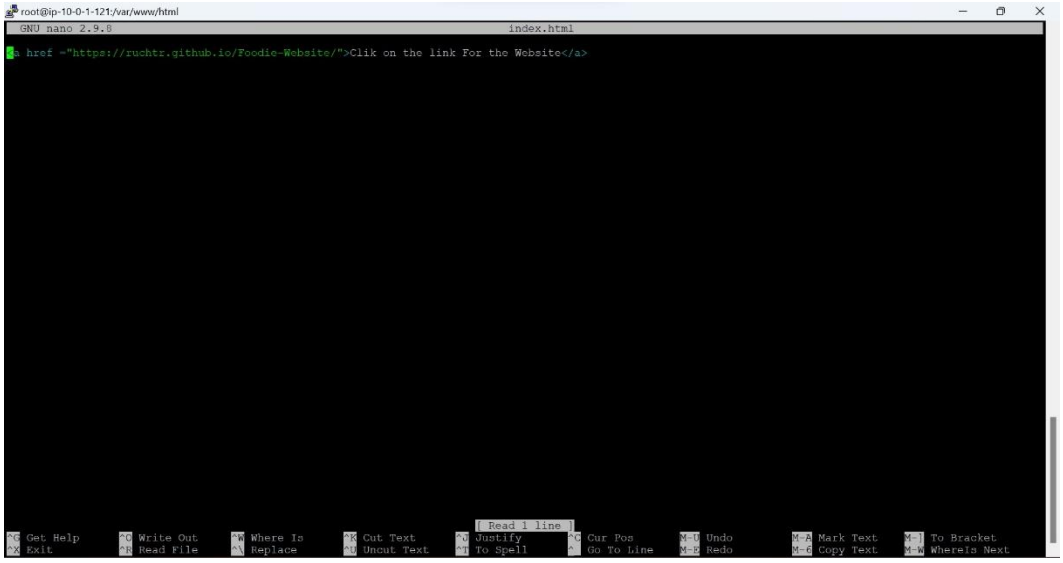
2. After launched connect it and write the below command.
   ec2-user
   sudo su
   yum update -y
   yum install httpd -y
   service httpd start
   chkconfig httpd on
   cd /var/www/html
   nano index.html
   Website name
   Ctrl x
   Y
   Ctrl c+enter.



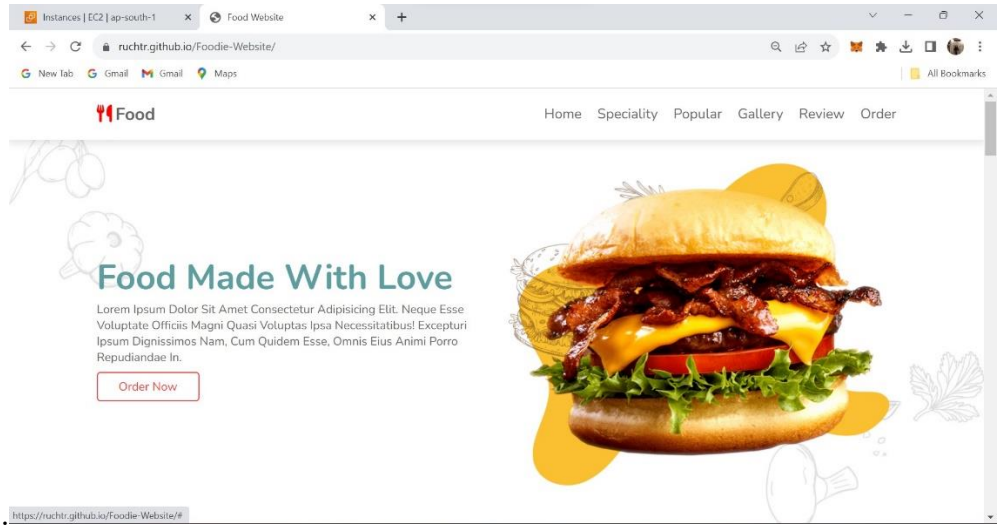

root@ip-10-0-1-121:/home/ec2-user
login as: ec2-user
Authenticating with public key "server"
Amazon Linux 2
AL2 End of Life is 2025-06-30.
A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/
[ec2-user@ip-10-0-1-121 ~]$ sudo su
[root@ip-10-0-1-121 ec2-user]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core | 3.6 kB 00:00
No packages marked for update
[root@ip-10-0-1-121 ec2-user]# yum install httpd -y


root@ip-10-0-1-121:/home/ec2-user
Verifying : httpd-2.4.58-1.amzn2.x86_64 4/9
Verifying : apr-1.7.2-1.amzn2.x86_64 5/9
Verifying : apr-util-1.6.3-1.amzn2.0.1.x86_64 6/9
Verifying : mailcap-2.1.41-2.amzn2.noarch 7/9
Verifying : generic-logos-httpd-18.0.0-4.amzn2.noarch 8/9
Verifying : mod_http2-1.15.19-1.amzn2.0.1.x86_64 9/9
Installed:
httpd.x86_64 0:2.4.58-1.amzn2
Dependency Installed:
apr.x86_64 0:1.7.2-1.amzn2
apr-util.x86_64 0:1.6.3-1.amzn2.0.1
apr-util-bdb.x86_64 0:1.6.3-1.amzn2.0.1
generic-logos-httpd.noarch 0:18.0.0-4.amzn2
httpd-filesystem.noarch 0:2.4.58-1.amzn2
httpd-tools.x86_64 0:2.4.58-1.amzn2
mailcap.noarch 0:2.1.41-2.amzn2
mod_http2.x86_64 0:1.15.19-1.amzn2.0.1
Complete!
[root@ip-10-0-1-121 ec2-user]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-10-0-1-121 ec2-user]# chkconfig httpd on

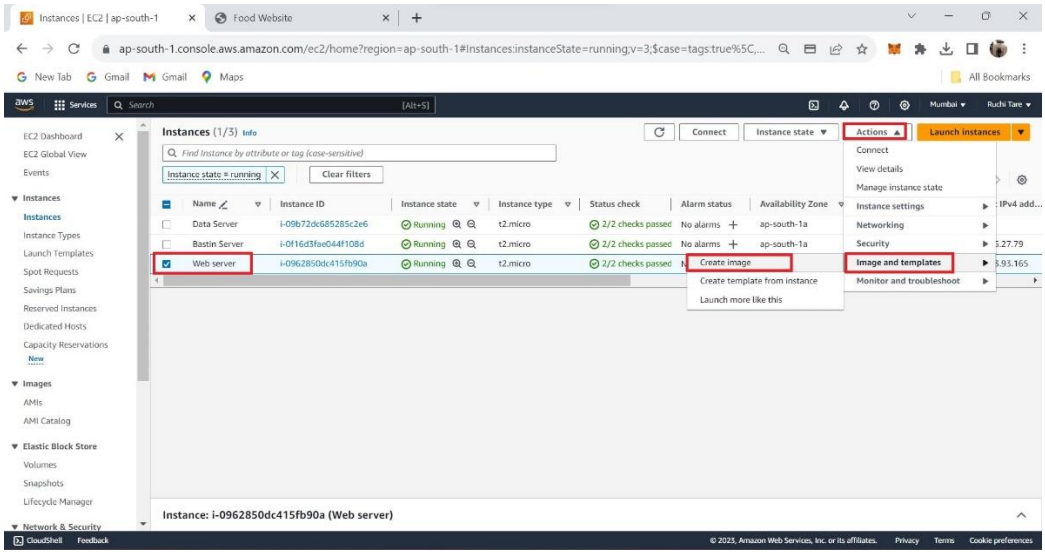


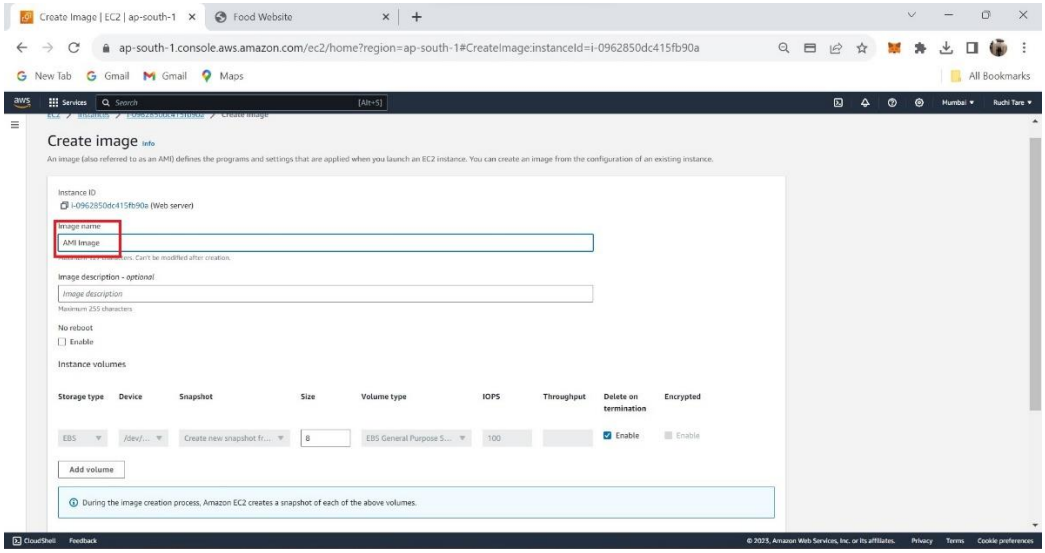


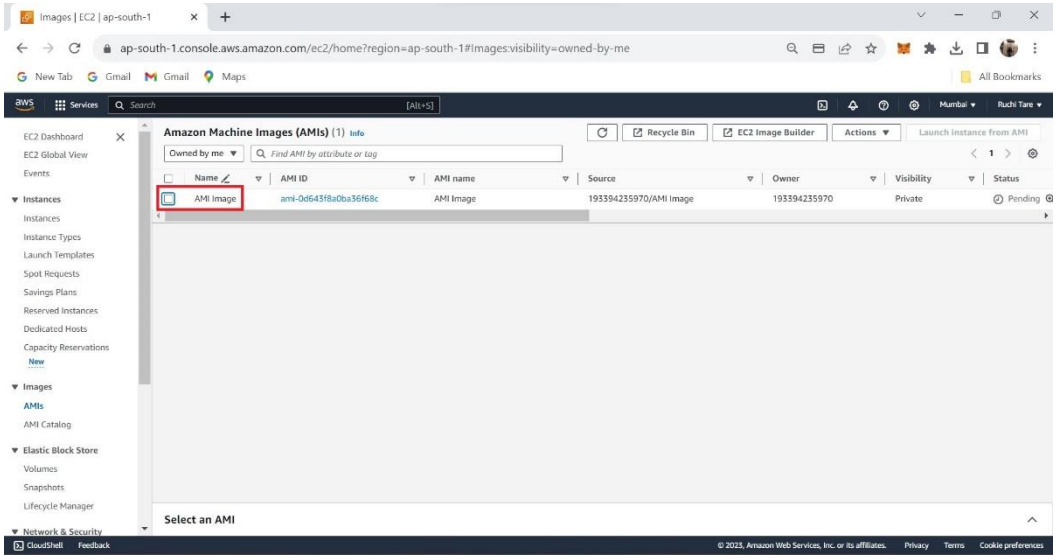
3. Come to aws console and copy the web server instance URL and paste it on the new tab

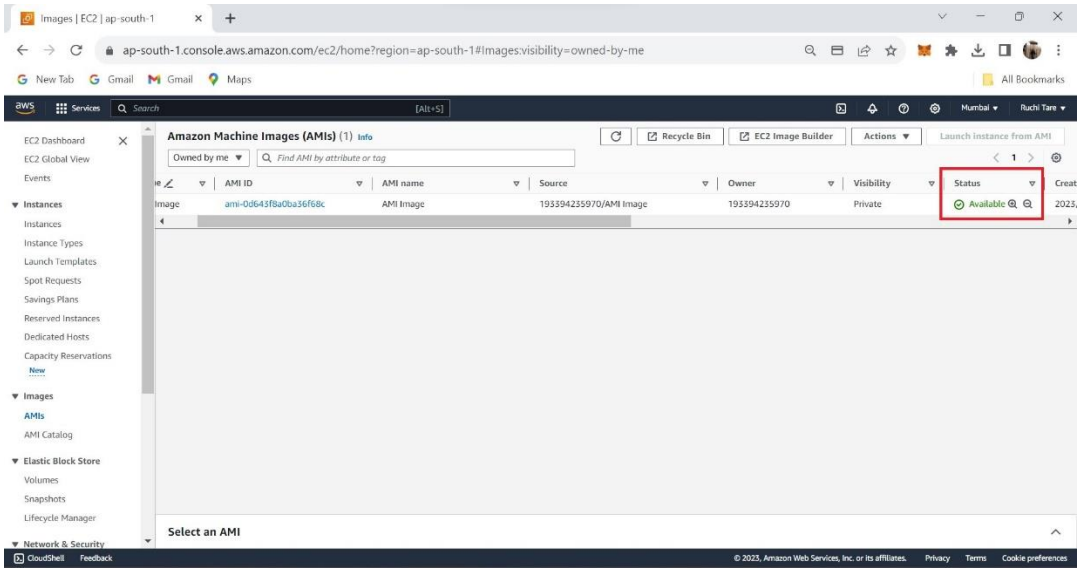


4. Afte that create a AMI of the web server with same key pair and security group.









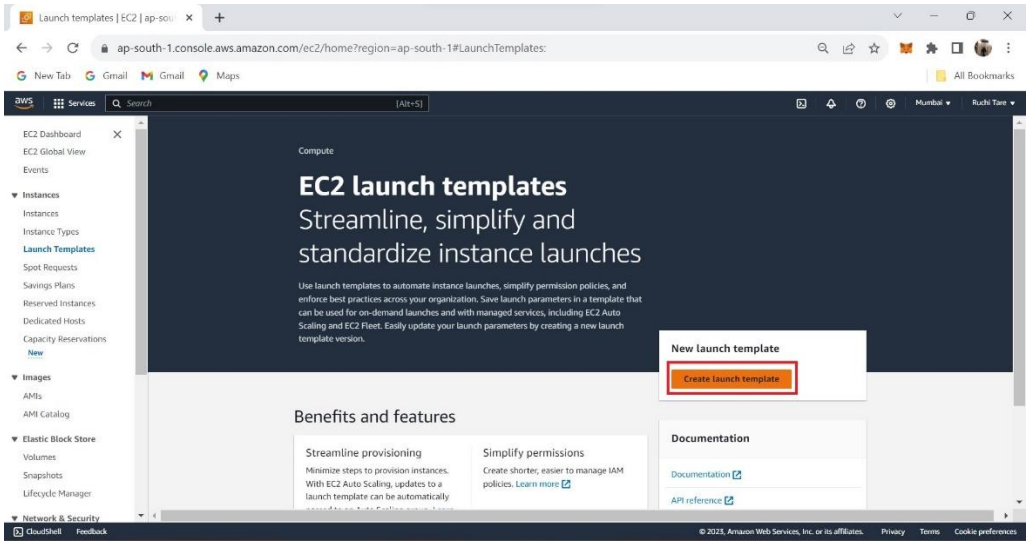
Note: AMI takes time to get available.

Once it is available the next step is to launch a template.

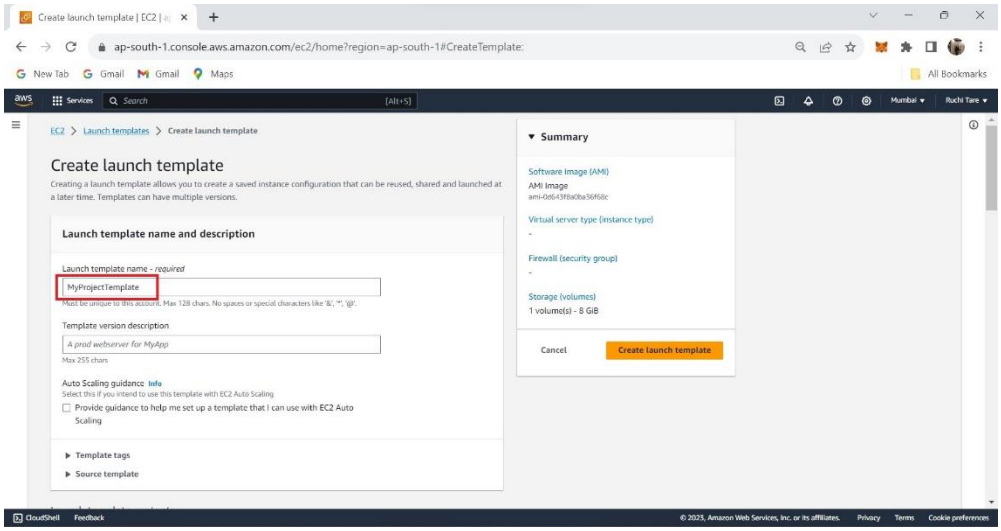
A template is like a pre-made set of instructions or a blueprint that tells a computer system, like AWS, how to create and configure resources. It's a handy way to automate the process of setting up things like servers or services with specific settings, saving time and ensuring consistency in the deployment of resources

Step 4:

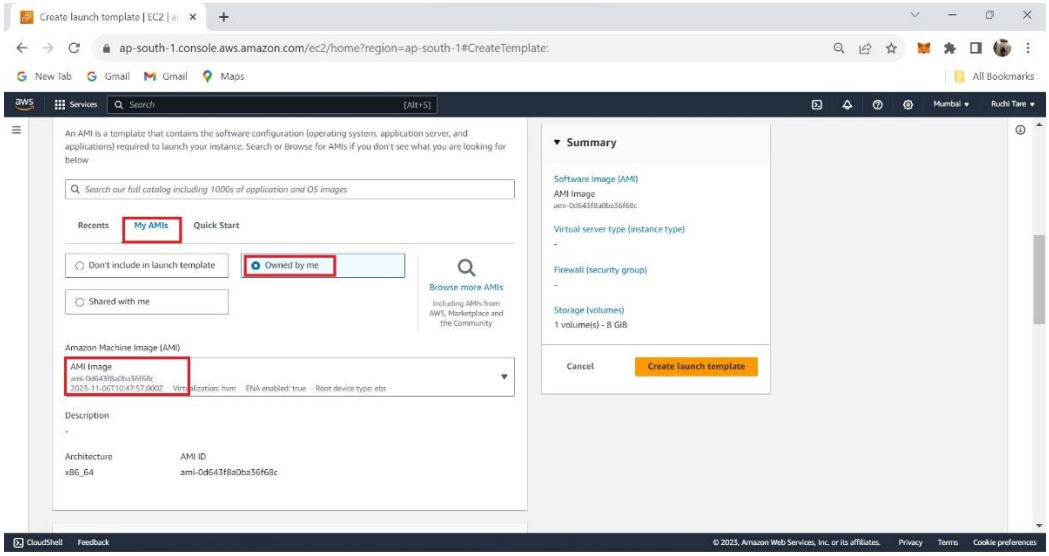
1. Go to the launch template in EC2 click in create launch template.



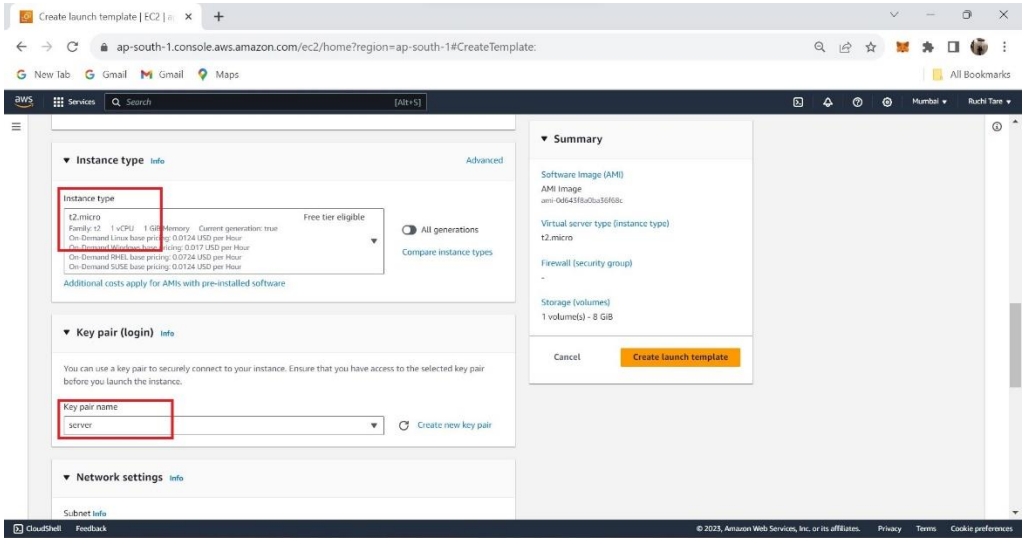
2. Give name to your template.

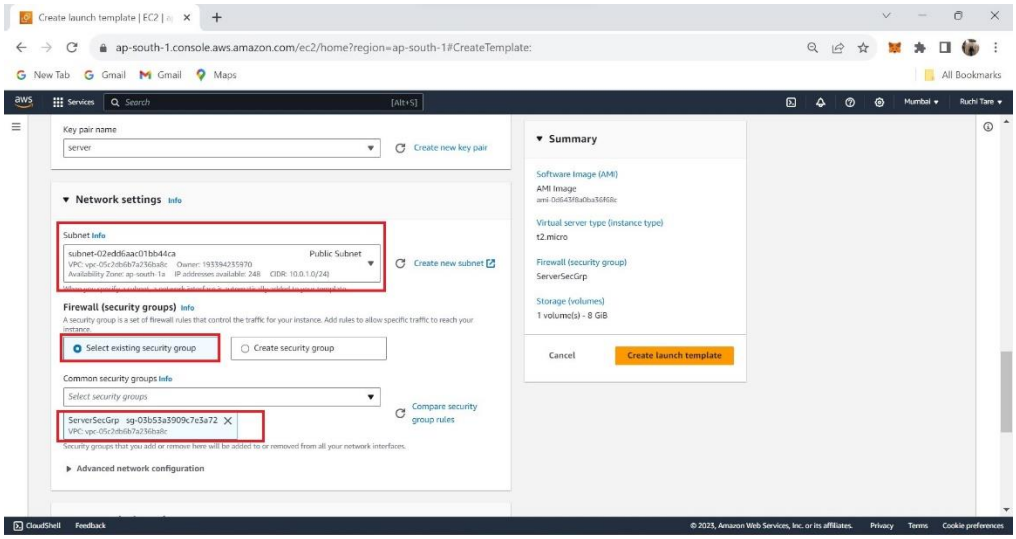


3. Click on My Ami ad your created ami will be visisble.

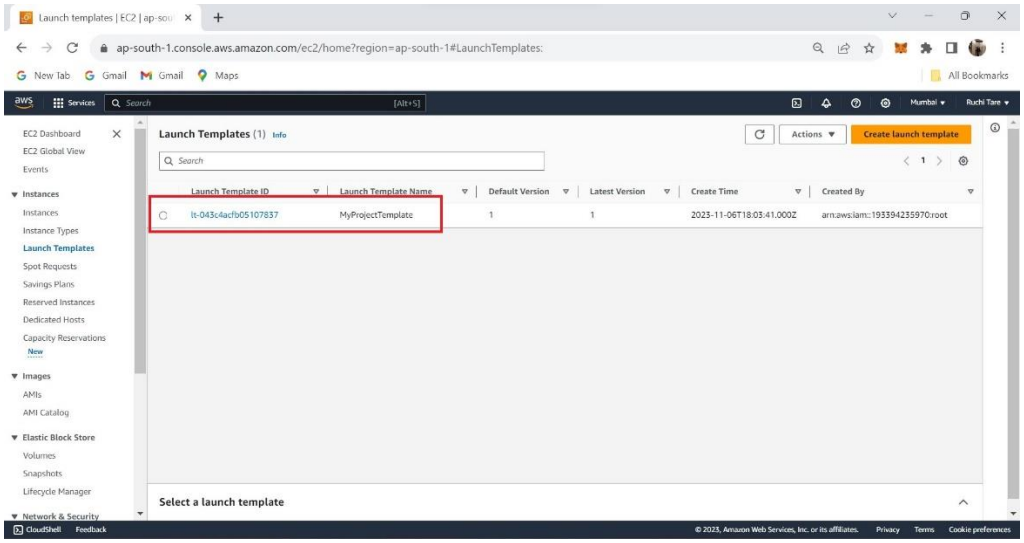


4. Select the same key pair , subnet should be public and security group should be same.





Click on the launch button.

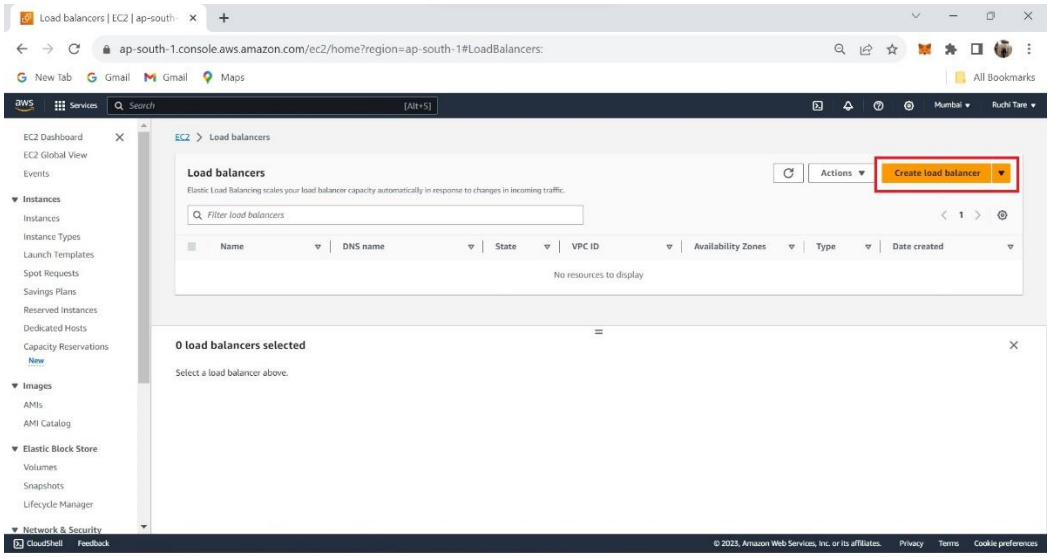


Your template is created.

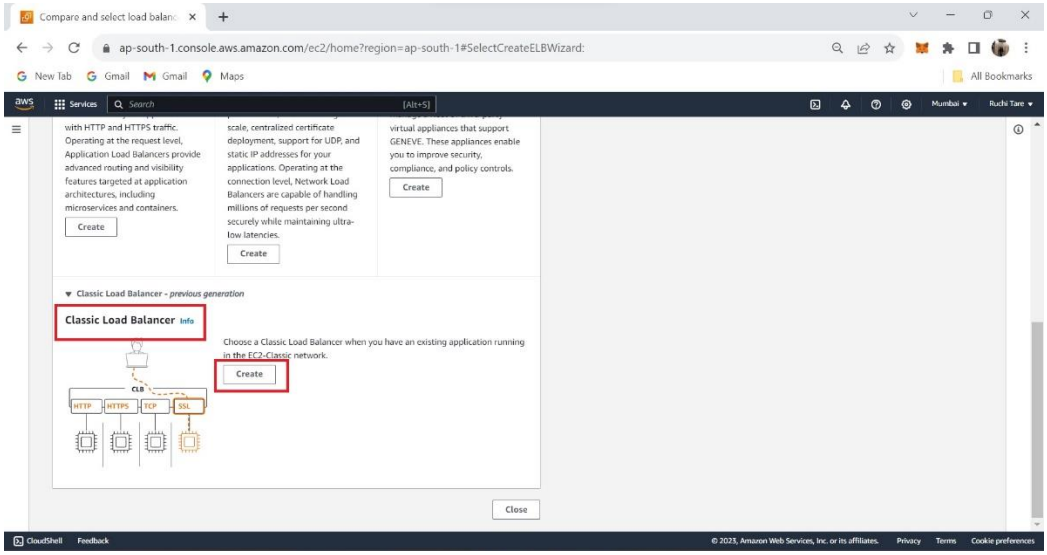
Step 5:

Once the template is launched, next step is to launch a classic load balancer.

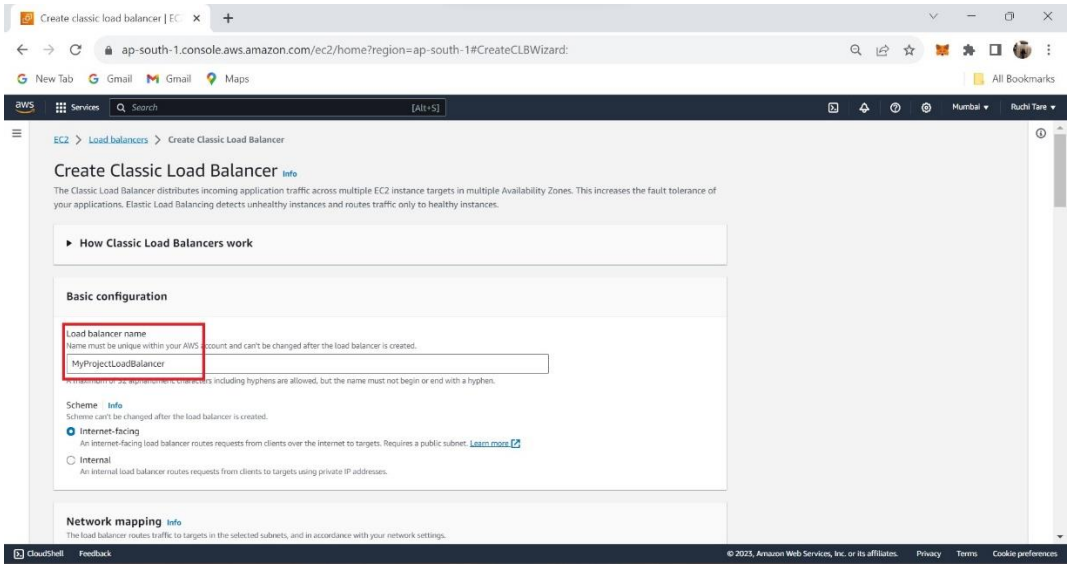
1. Select the load balancer from EC2 service and click on create load balancer.



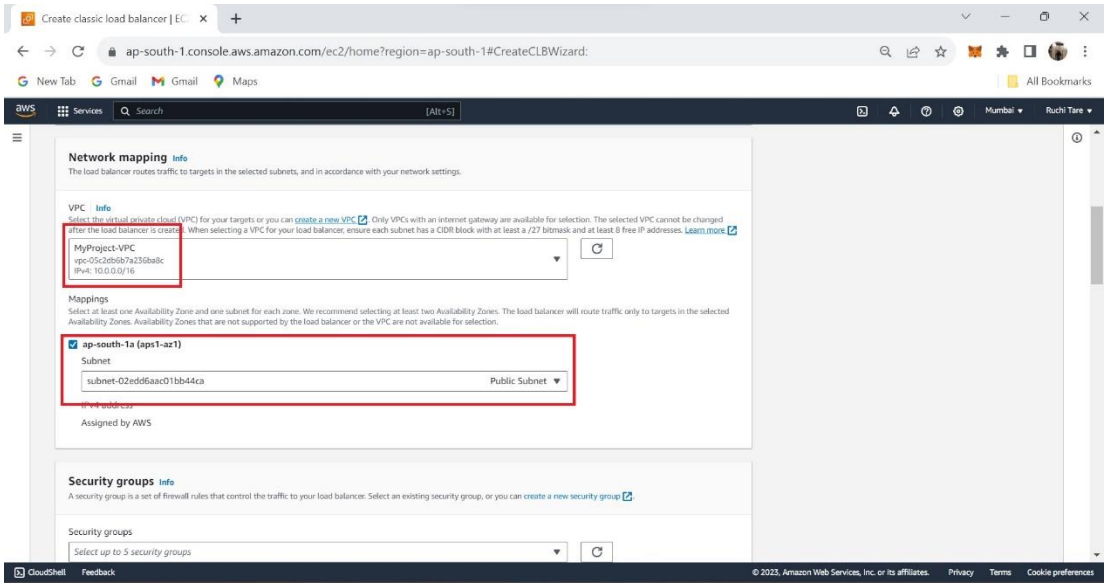
2. Scroll Down and click on previous generation → classic load balancer→create.



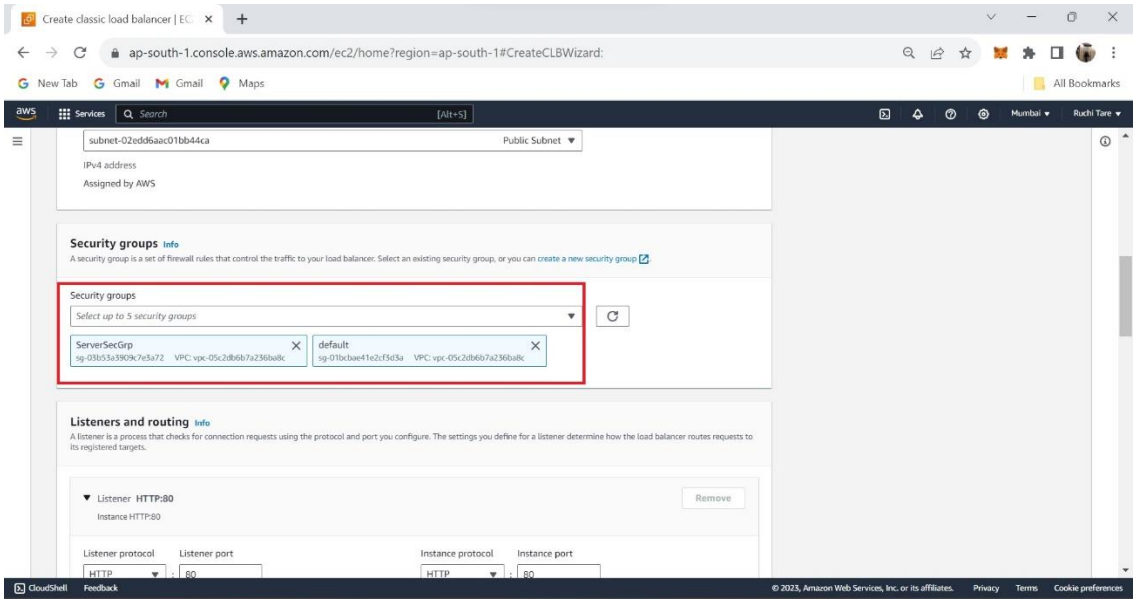
3. Give the name for the load balancer and select internet – facing.



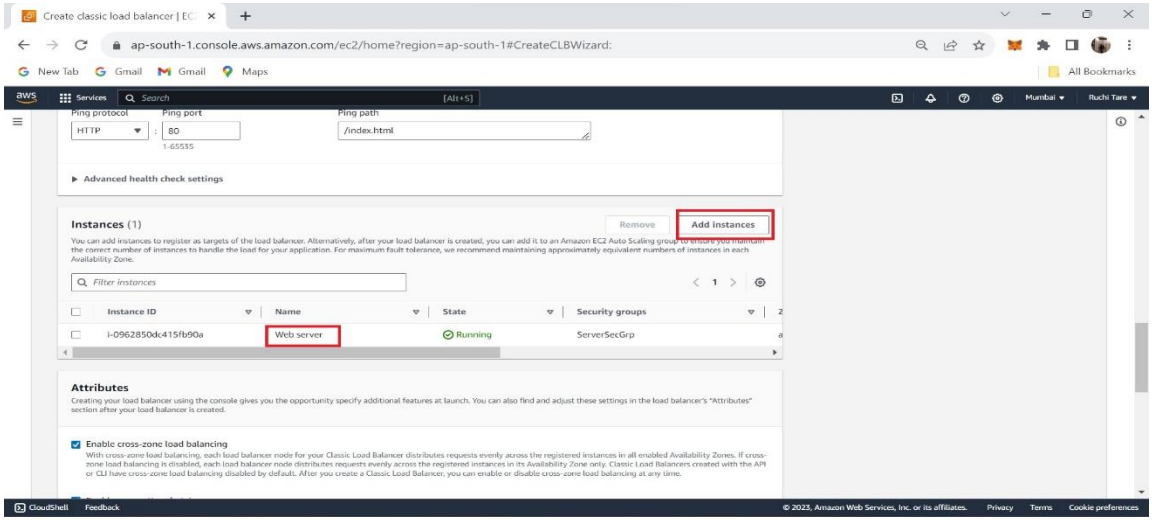
4. Select the created VPC and select public subnet.



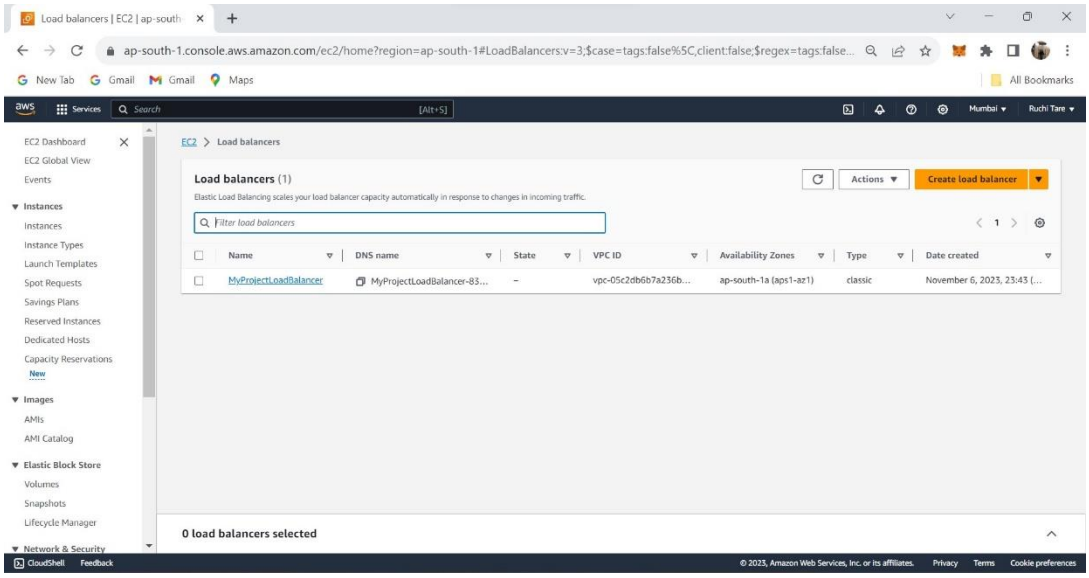
5. Select the same security group which you have created for Web server insatance.



6. Select the Web server instance as you are going to create the load balancer of web server which will balance the load of your server → then click on create load balancer.



7. The Load Balancer is created.

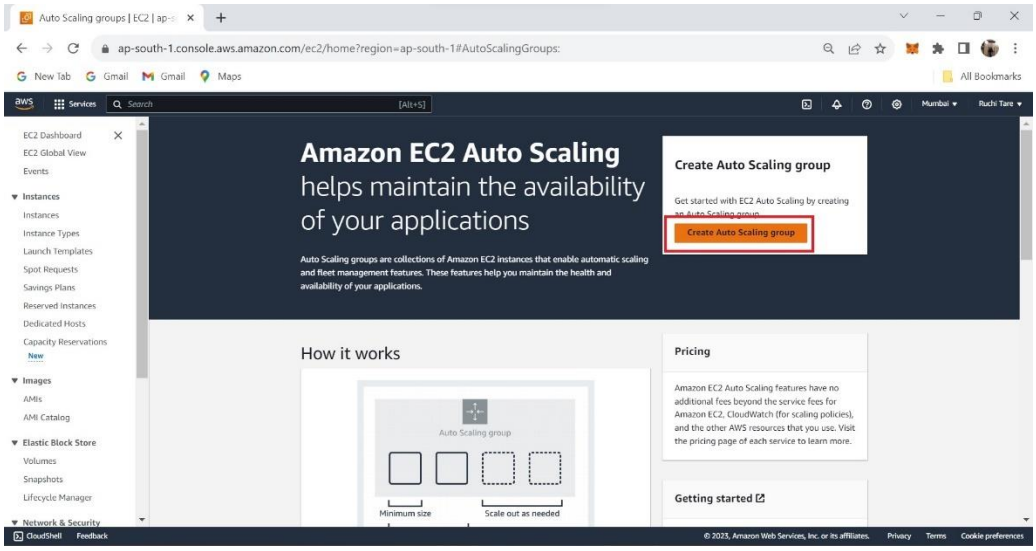


Step 6:

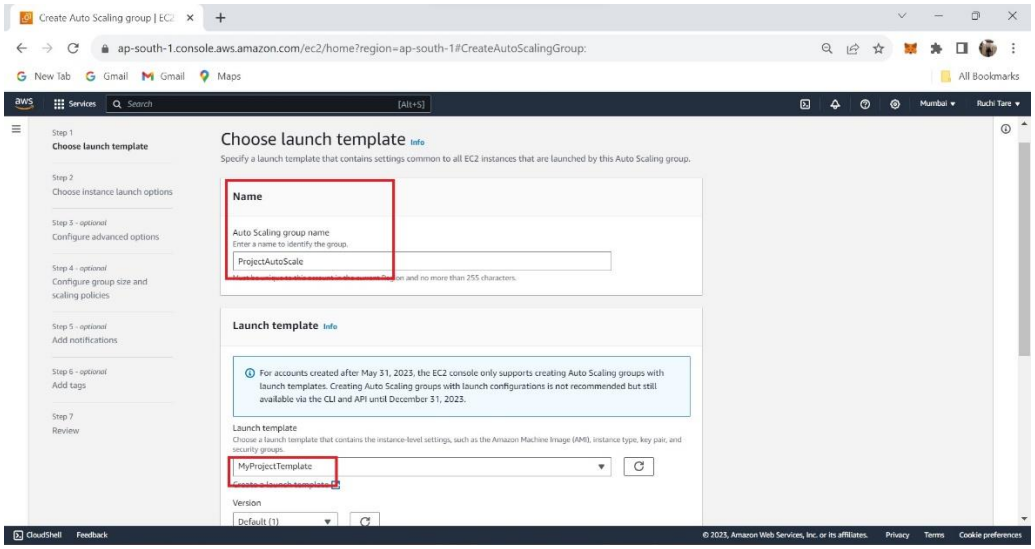
Now that your load balancer is created the next step of yours is to create a Auto Scaling Group.

Auto Scaling Group is used here to Scale the instance in and out when the instance extend its load.

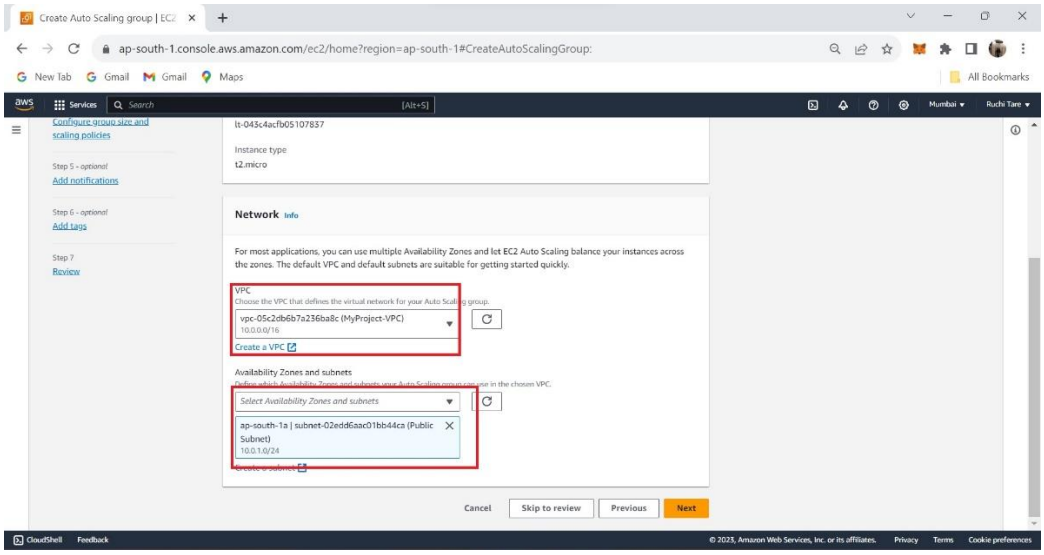
1. Select the Auto Scaling Group in the EC2 service and then click on create Auto Scaling Group.



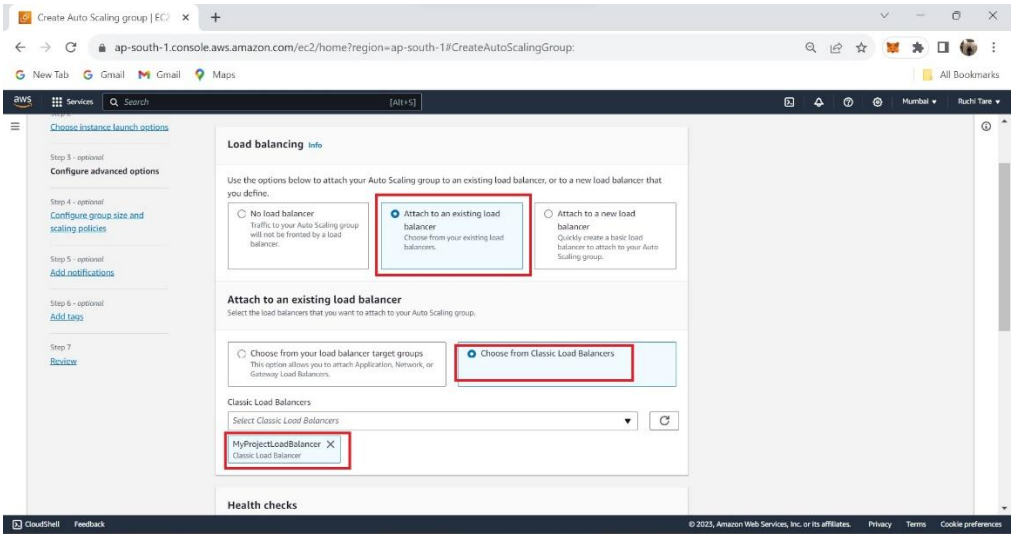
2. Give your Auto Scaling Group a name and select your created template.



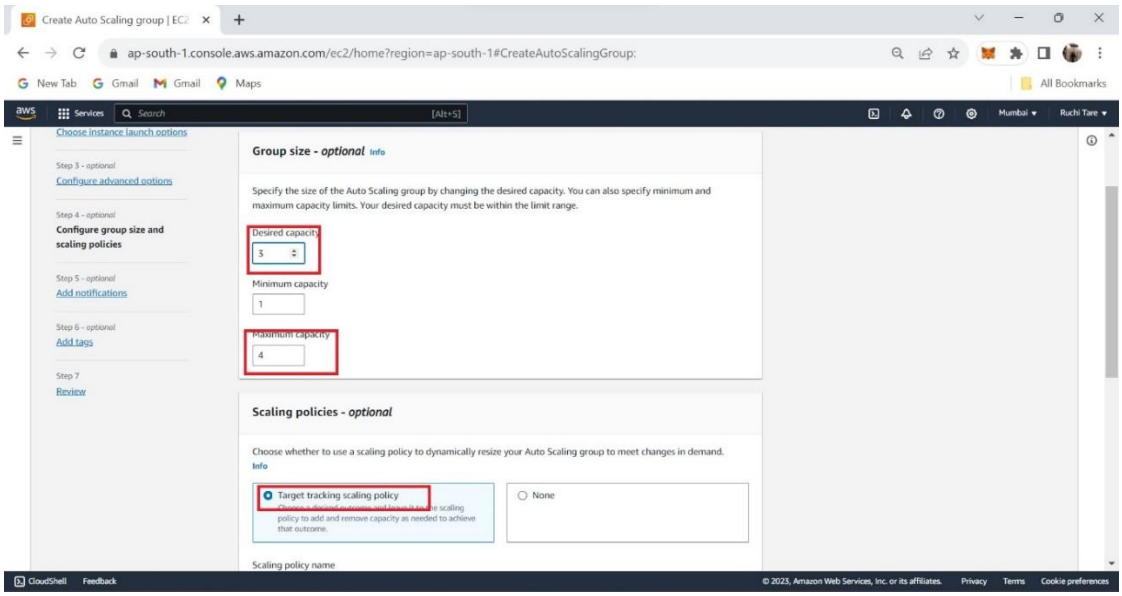
3. Select the VPC that you have created and public subnet.



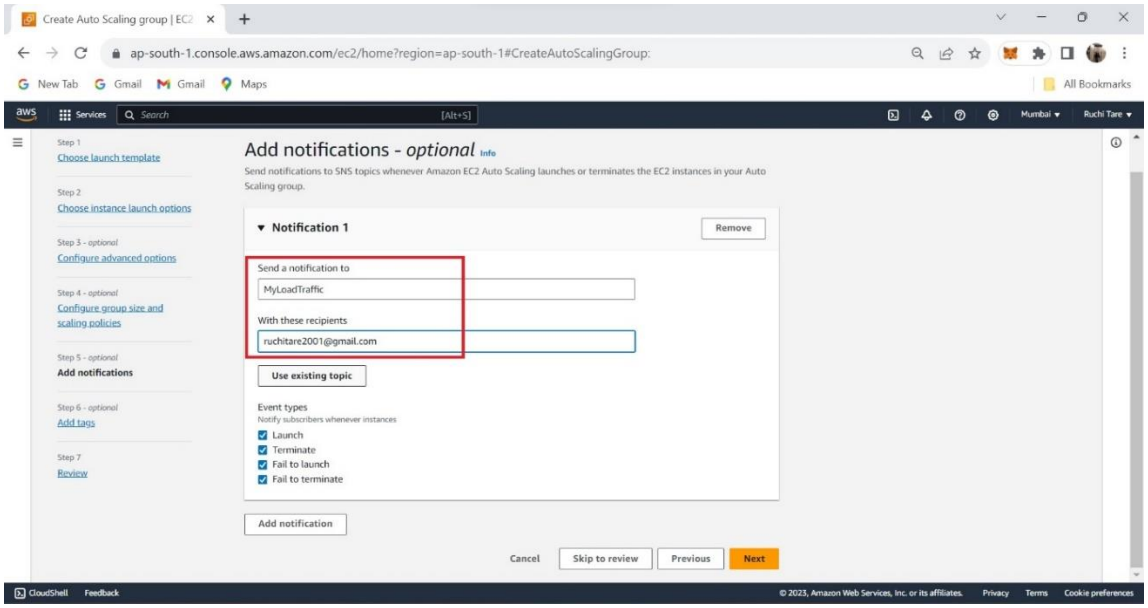
4. Click on next button and next step is to attach load balancing→ Attach exciting load balancer →choose from classic load balancer→Select the load balancerthat you have created.

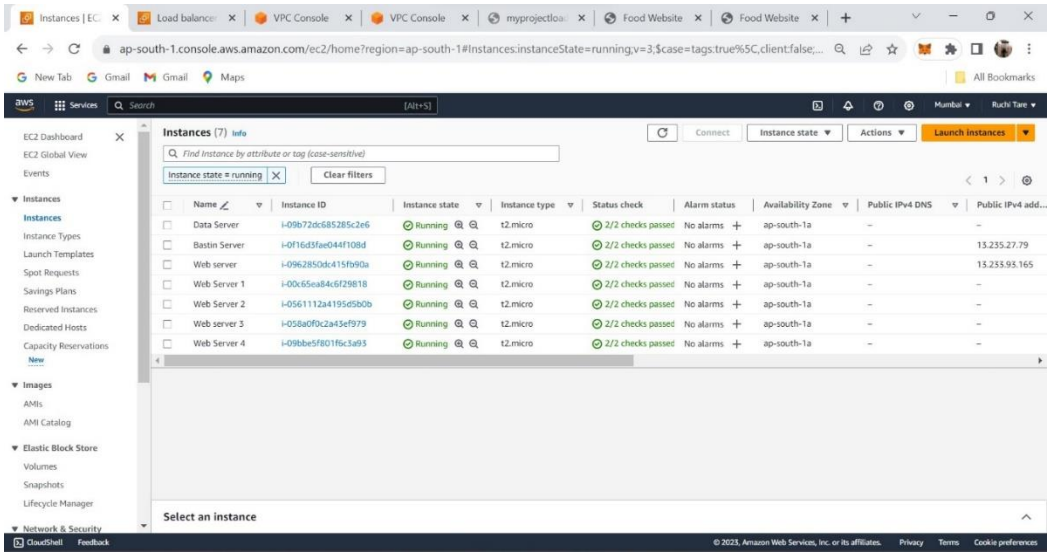


5. Click next → choose the desired capacity of instance you want to create first→then choose the maximum instance you want.



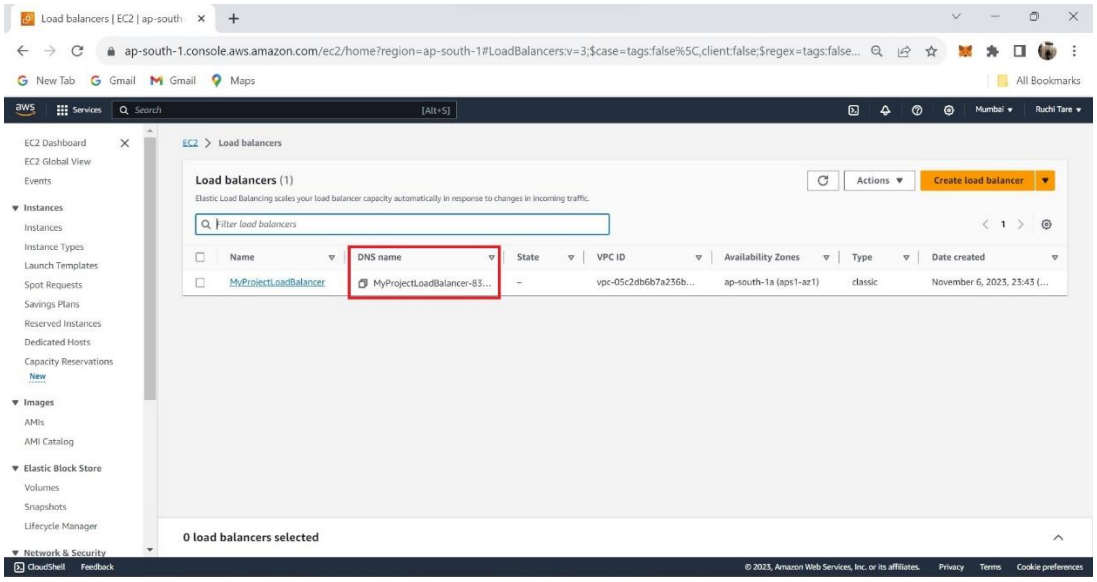
6. Auto Scaling Group will send you the message whenever the a load on one instance exceed and another instance is created so for that we will create an SNS group.
Click on next→Give name title to your message→enter the recipients to whom you want to send message →click on next→ Review your Auto Scaling Group and then click on create.

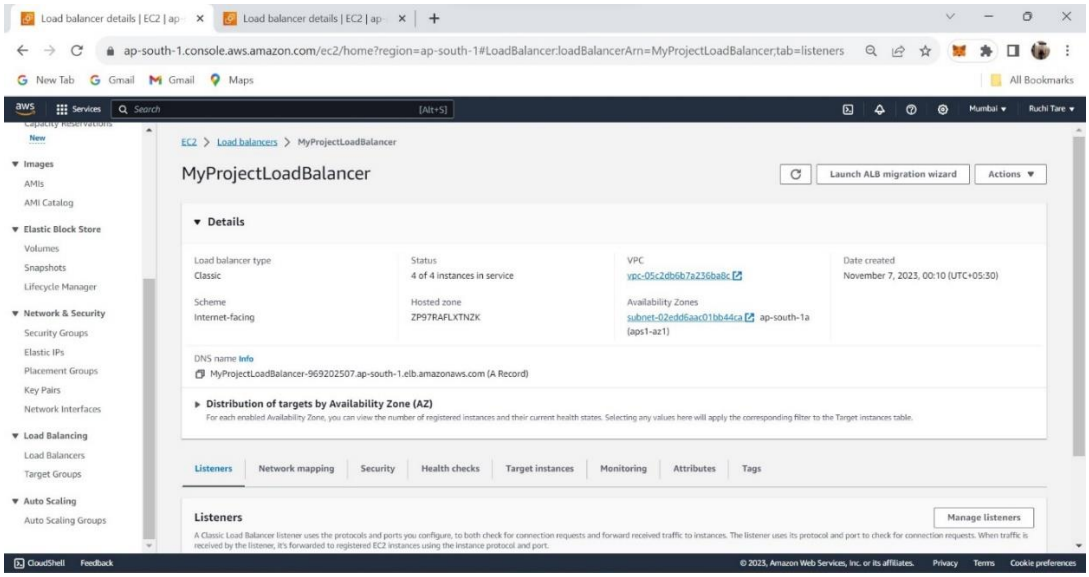




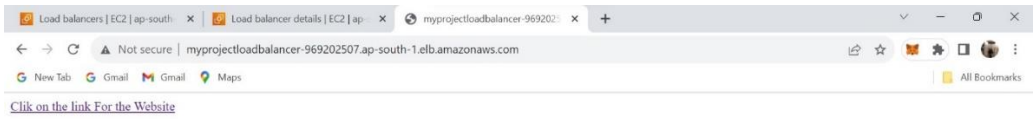
The above 4 instances is created by the Auto Scaling Group. Where the load is extended beyond 50% of the CPU limit.

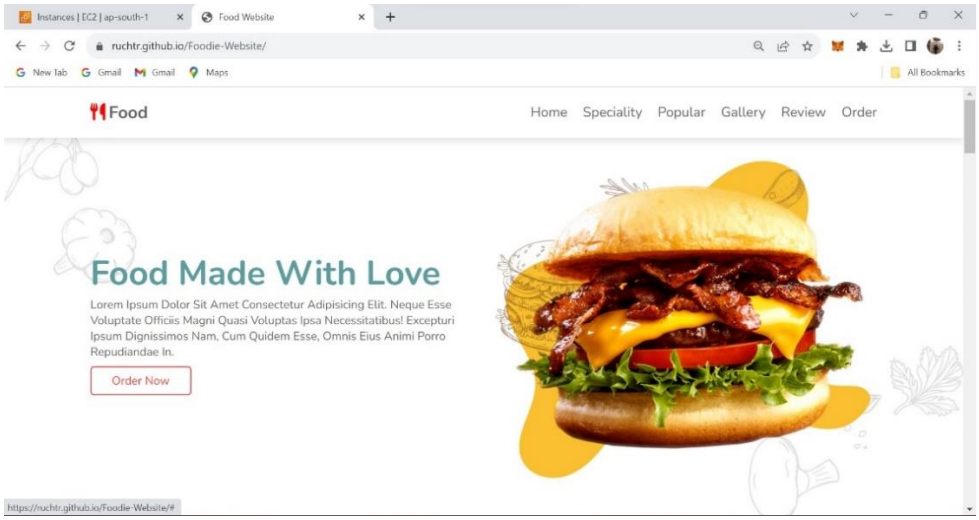
Go to the load Balancer and then check whether the status is showing 4 of 4 instances in service which means your load balancer is working properly and it is dividing the load between the instances.





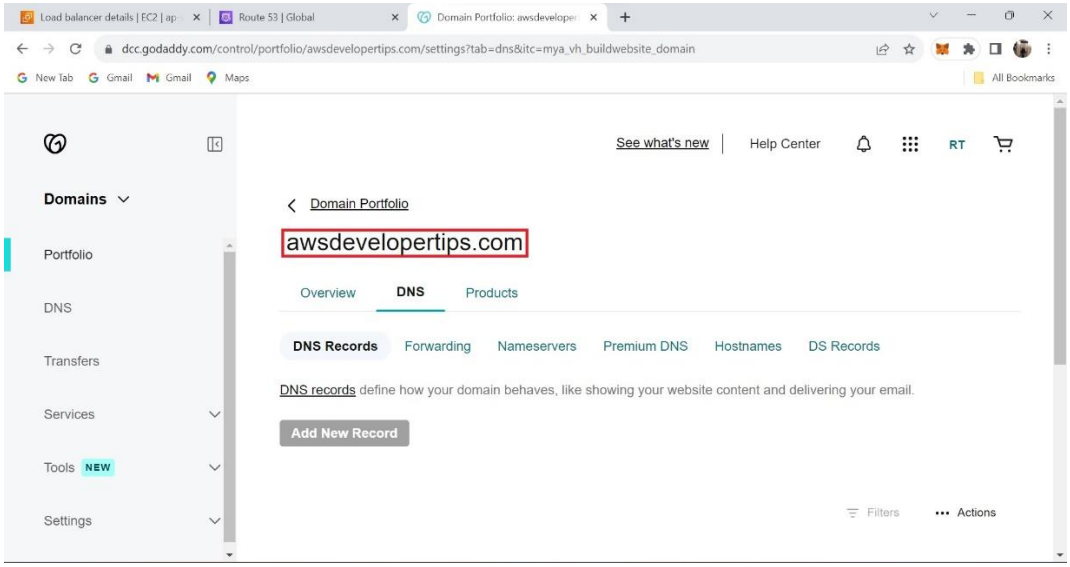
Click again on the DNS of the load balancer then check whether you website is working properly.



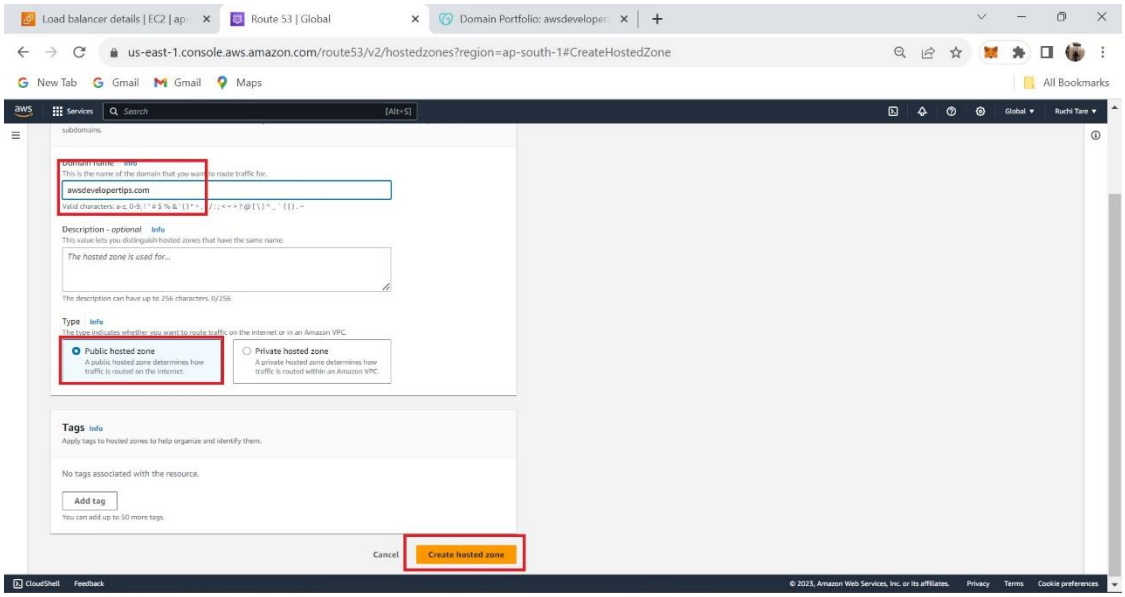


Step 7: Now we have to host our website on the server for that we are going to use Route 53.

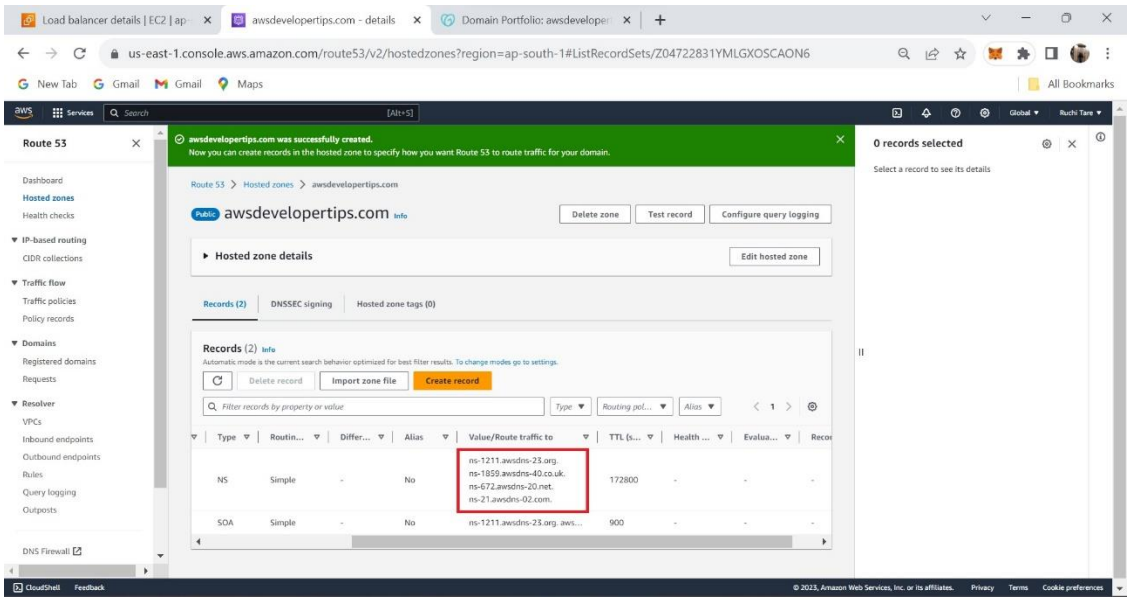
1. Before creating a hosted zone for your website you will have to create a domain name.
2. You can create a domain name in aws itself or else you can buy it from Godaddy.com
3. Click on the link below and complete the registration details and also buy the domain that you want.



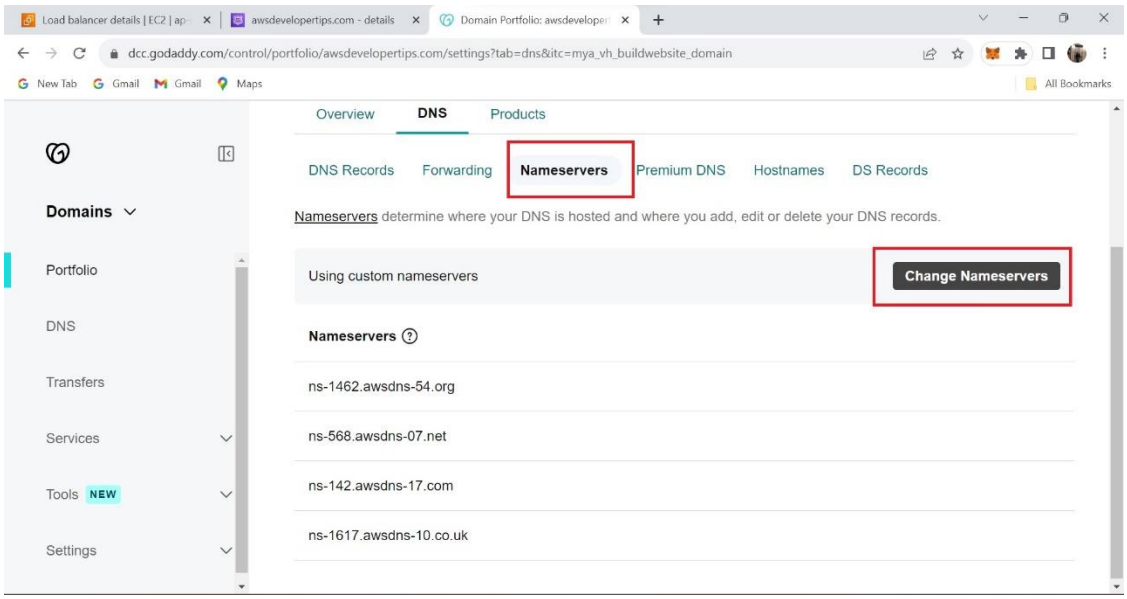
4. Once you have buyed the domain name go to Route 53 and click on Hosted click→create hosted zone→add the domain name to your hosted zone and also select public hosted zone→click on create hosted zone.



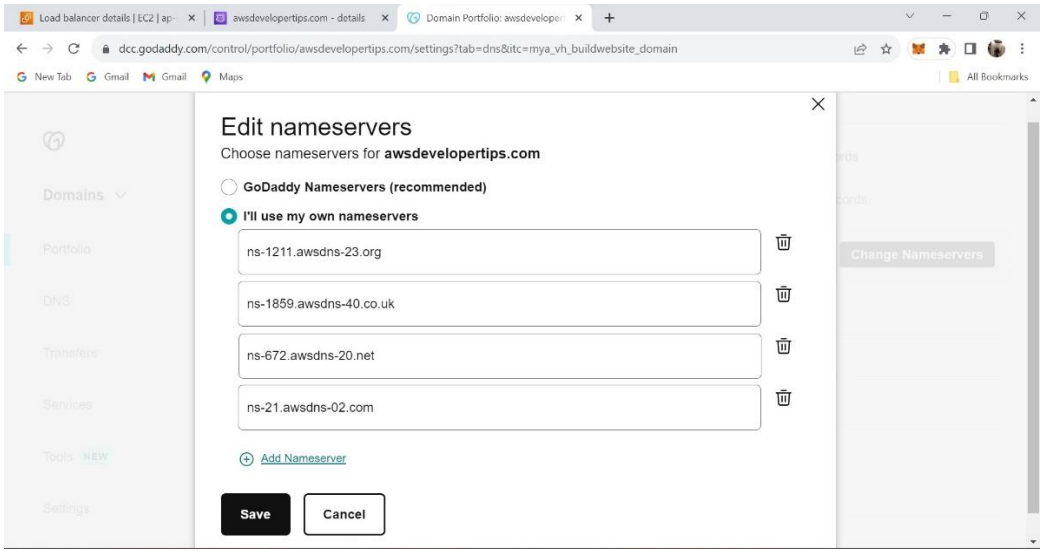
5. Now click on the created hosted zone and copy the name server URL and paste it on the name server of your godaddy account.



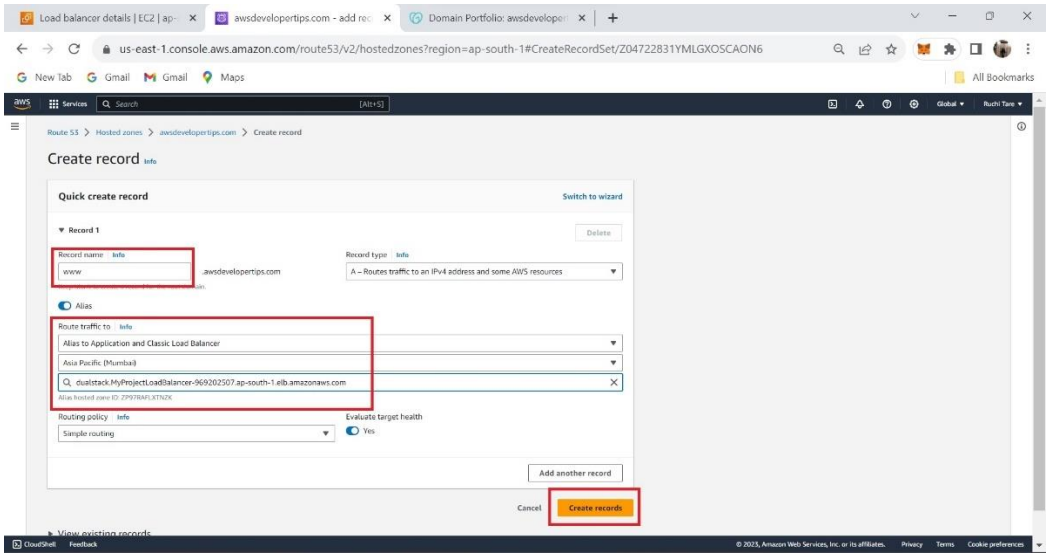
6. Go to your godaddy account click on nameservers → change nameserver.



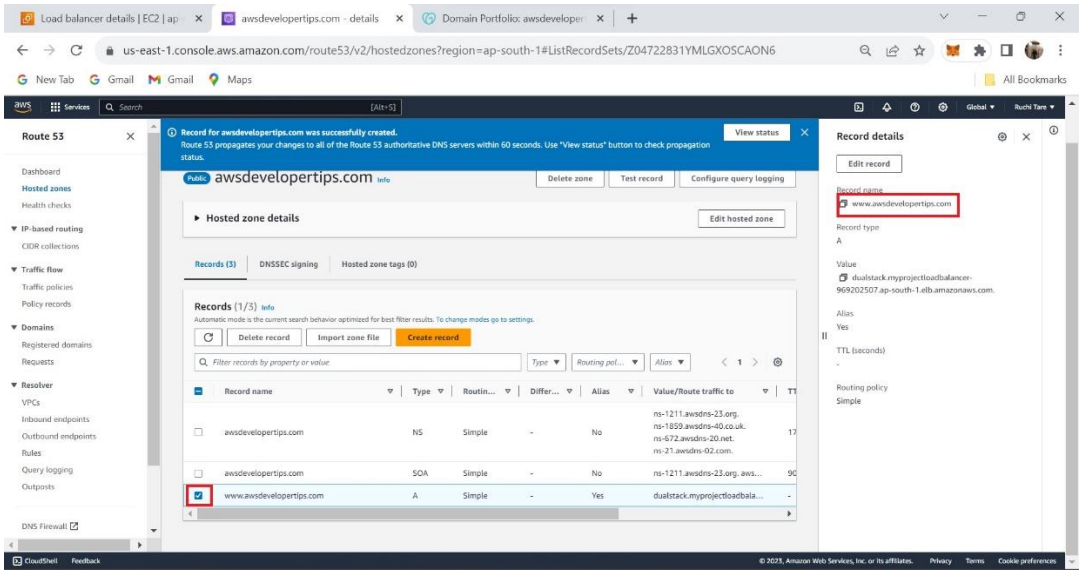
7. Paste all the name server that you have copied from your hosted zone.



8. Create a record with subdomain www and load balancer endpoint and then click on create record.



9. Once the record is created click again on the hosted zone and click on the URL which is given by aws and paste it on new tab to see your website.



As you can see the website is visible through the URL.