Deploy a secure, highly available, and scalable website.

High-availability

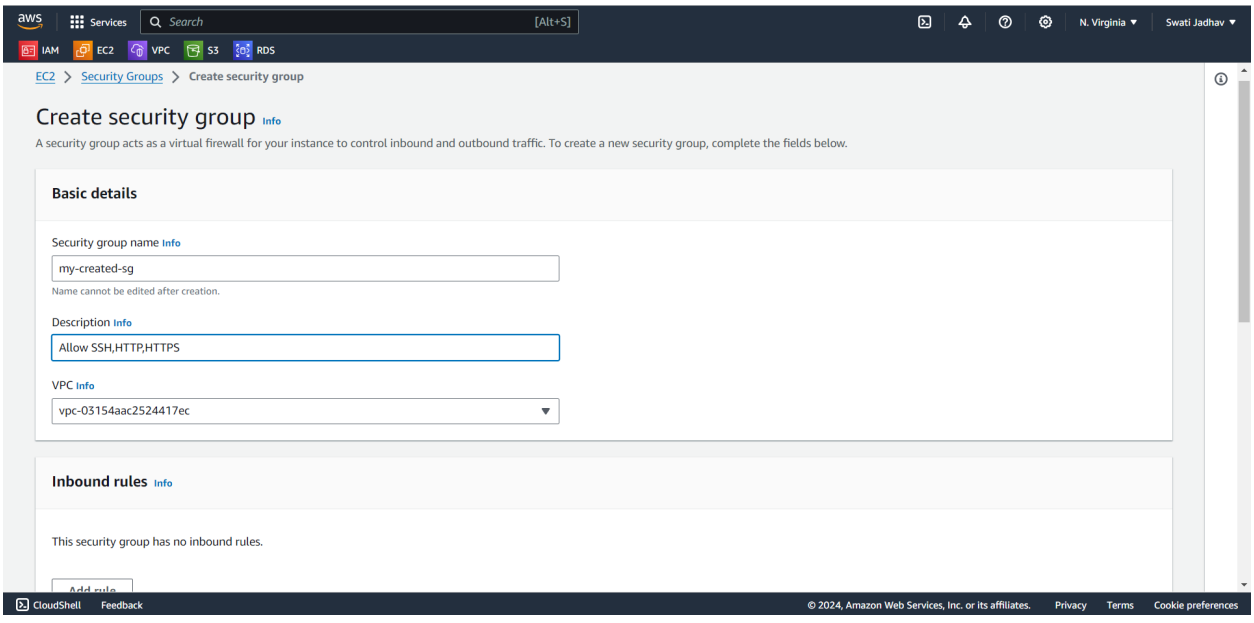
High-availability infrastructure is configured to deliver quality performance and handle different loads and failures with minimal or zero downtime.

Scalable

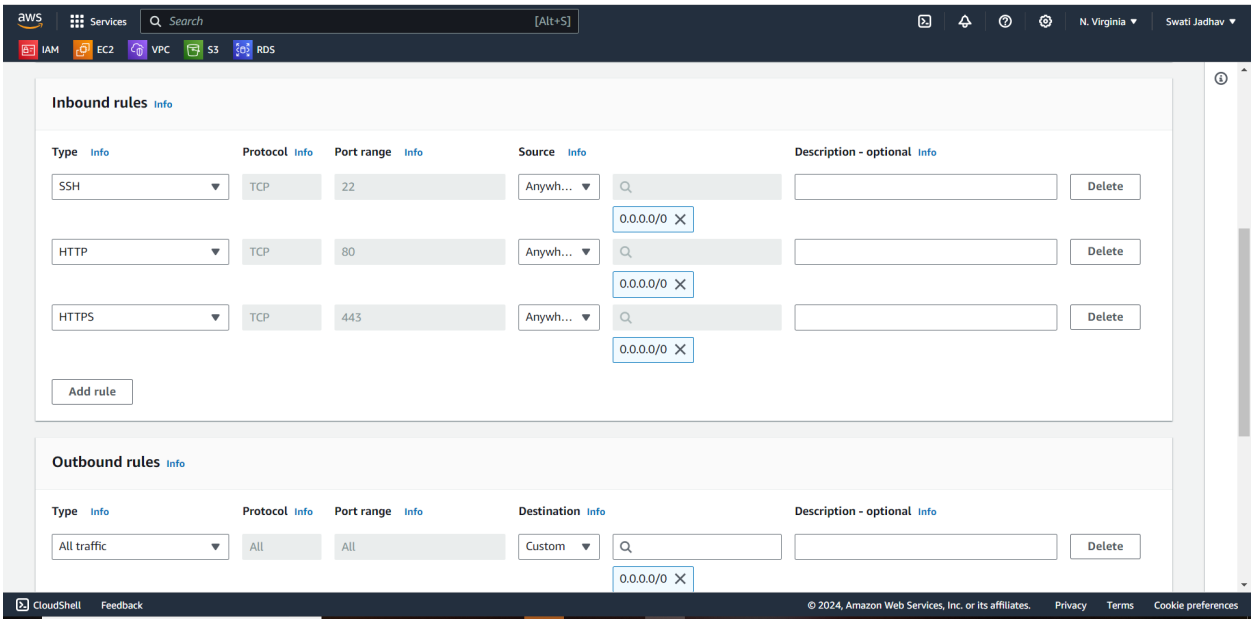
The ability to increase or decrease IT resources as needed to meet changing demand.

Step 1: Create a Security Group.

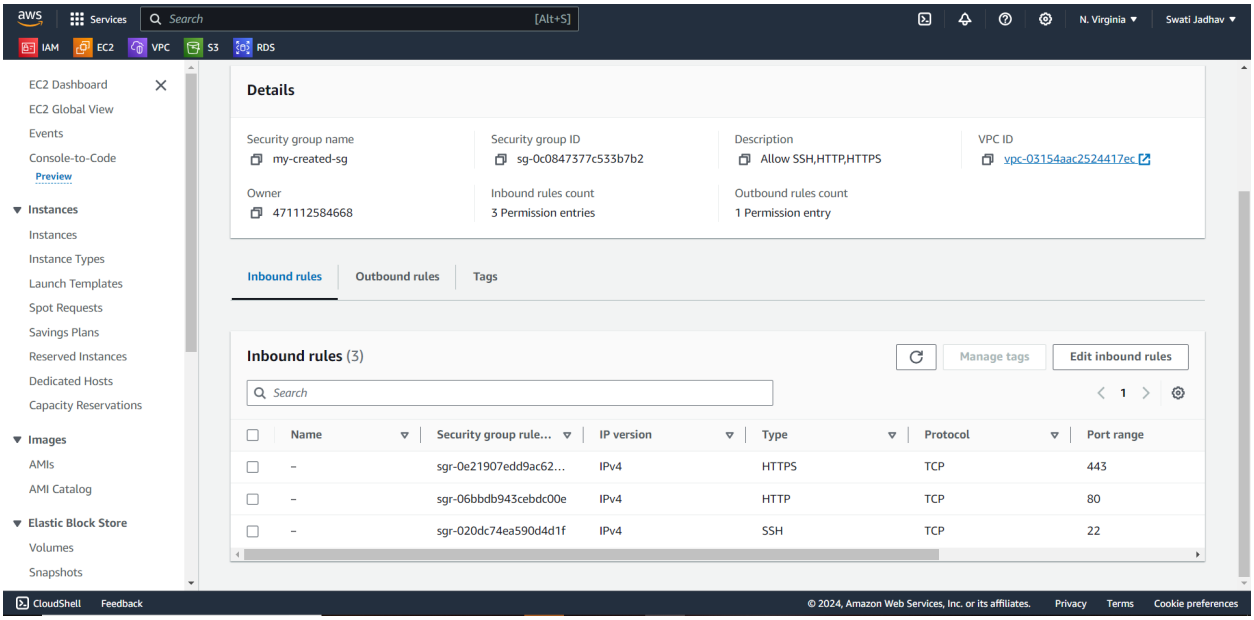
- Login into the AWS Console using the login credentials.
- Create a security group.
- Give an appropriate name, and description to that security group. Also, select the VPC.



- Add SSH, HTTP, and HTTPS in the inbound rules.

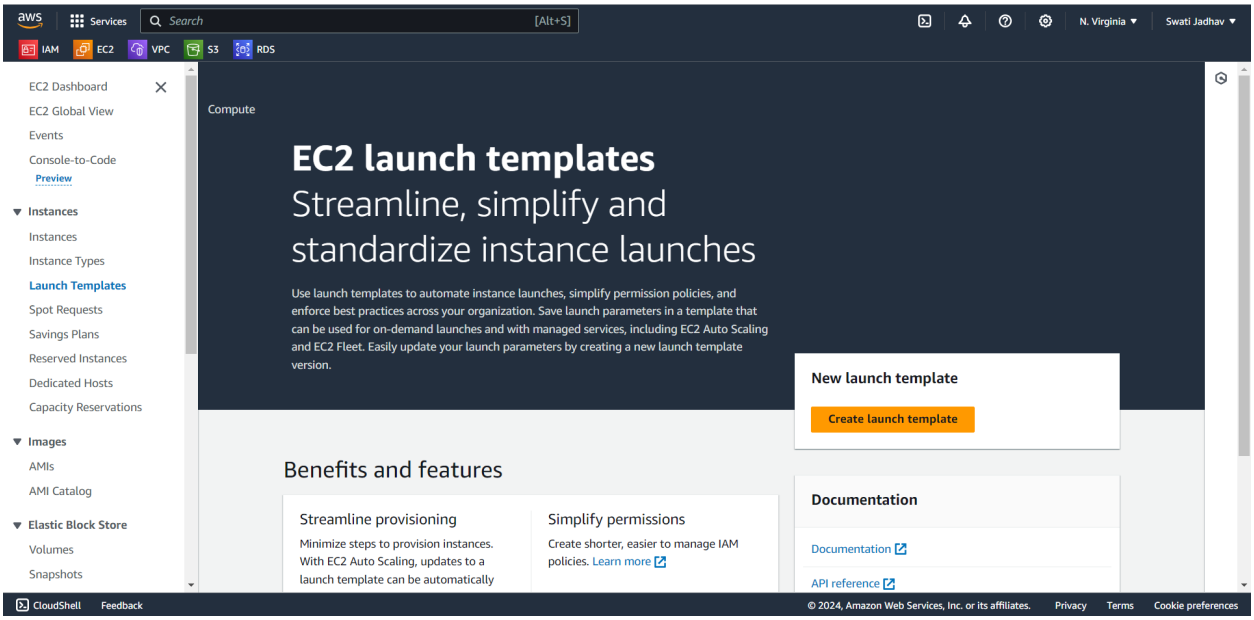


- The security group is created successfully.

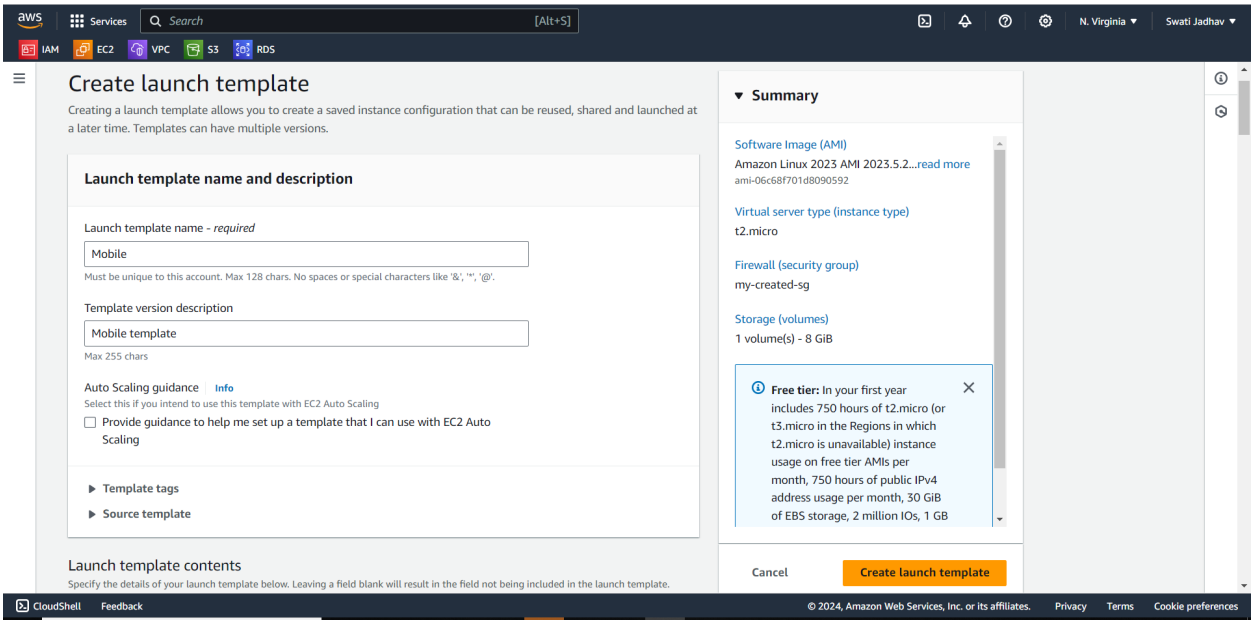


Step 2: Launch Templates

- Launch three EC2 Templates.

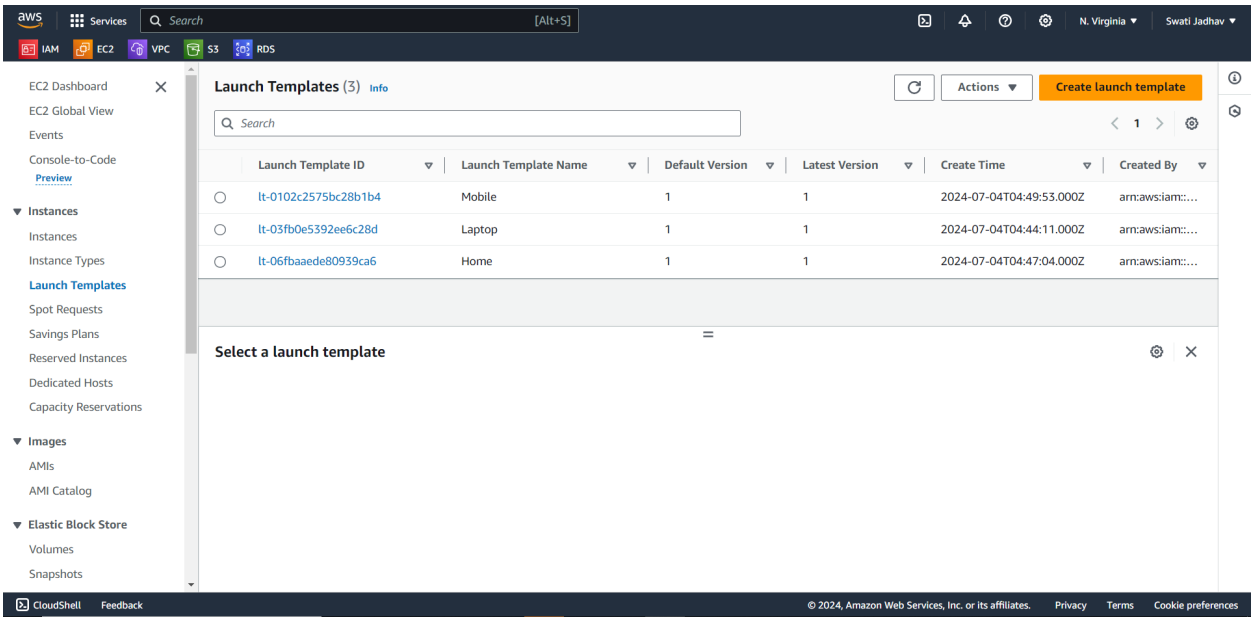


- Create a launch template, and give a name to that template.



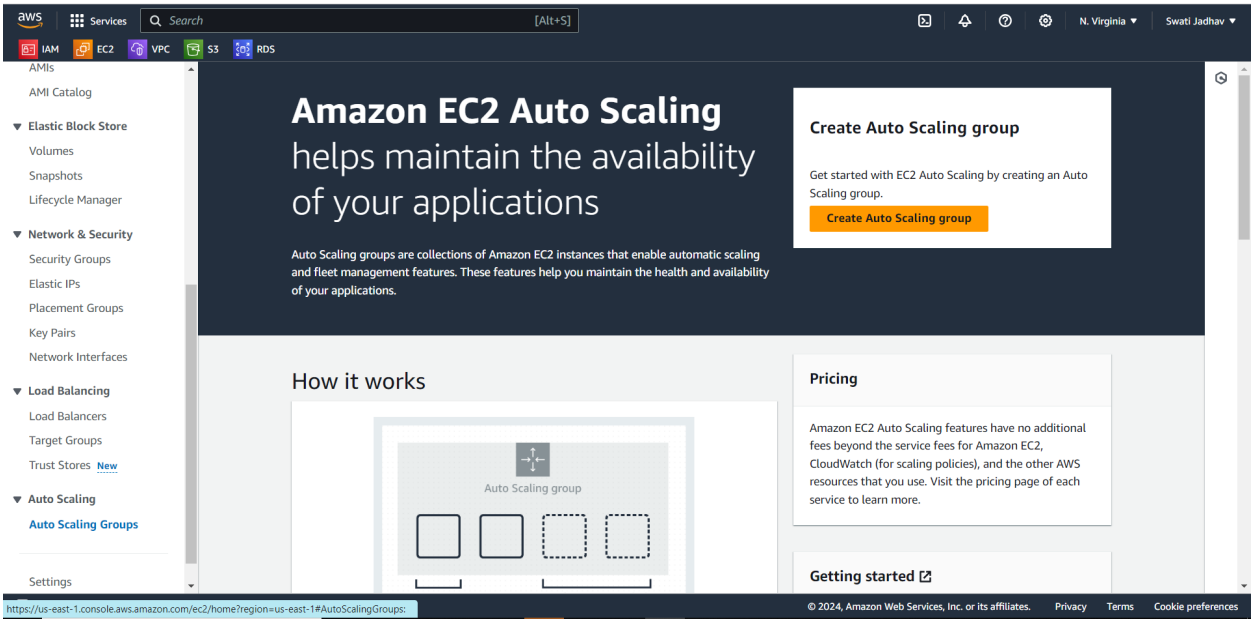
- Likewise, Create three templates

- Mobile, Laptop, and Home these are the three different templates for different web pages.

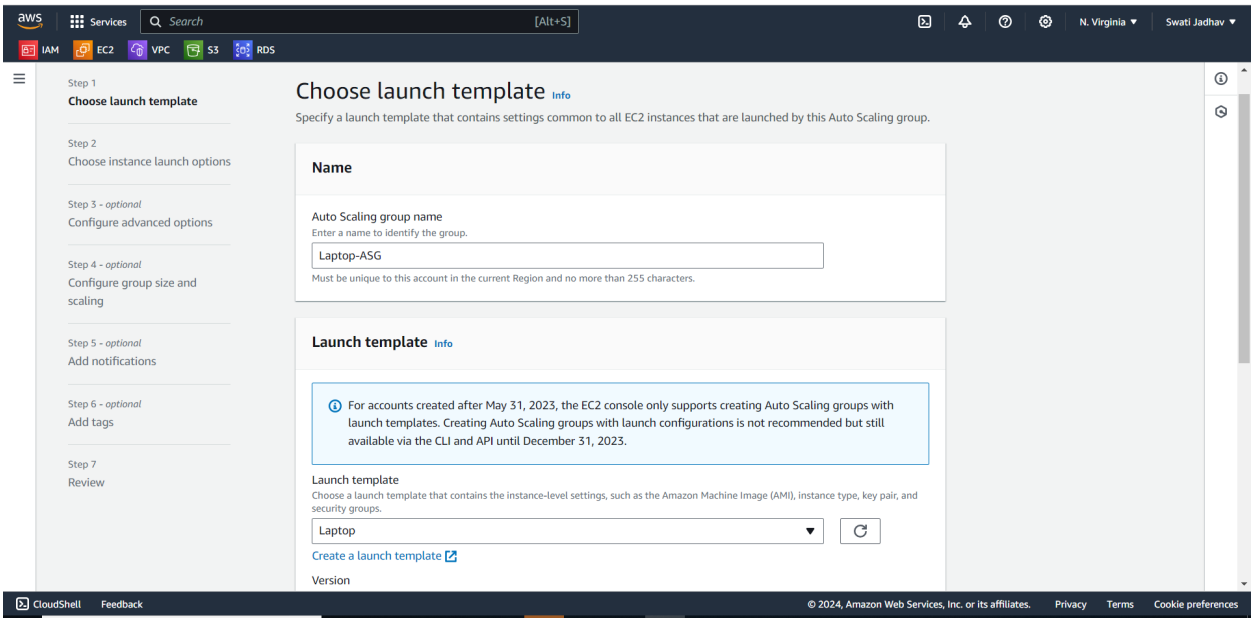


Step 3: Create three Auto Scaling Group

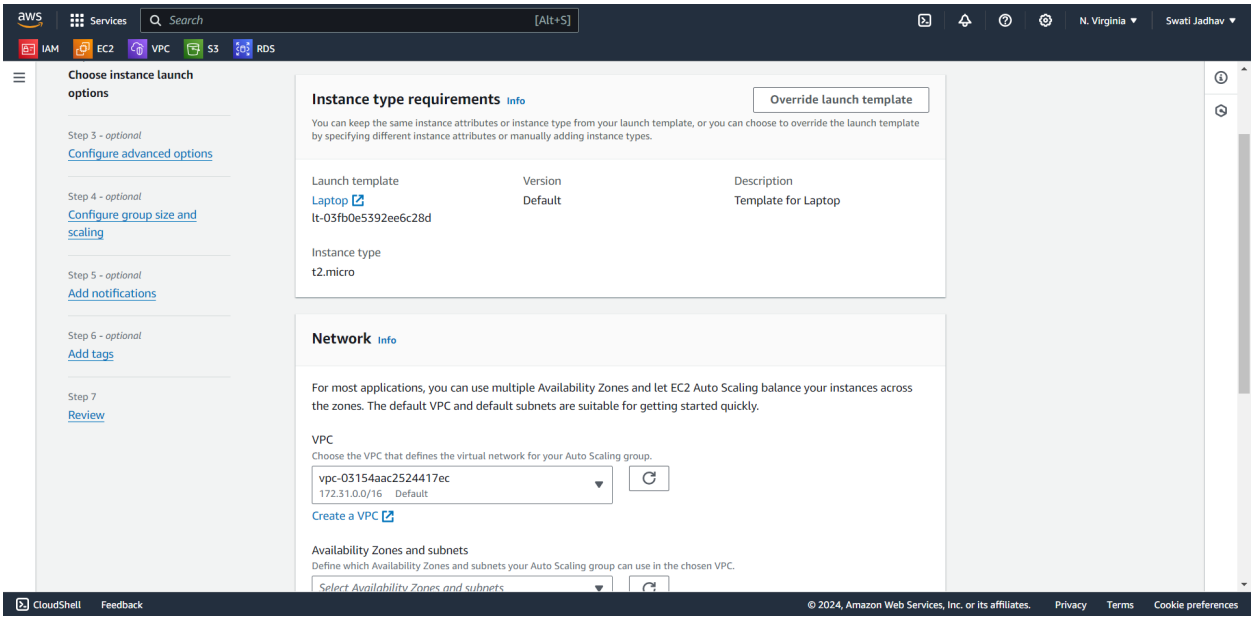
- Search auto-scaling in the search box.



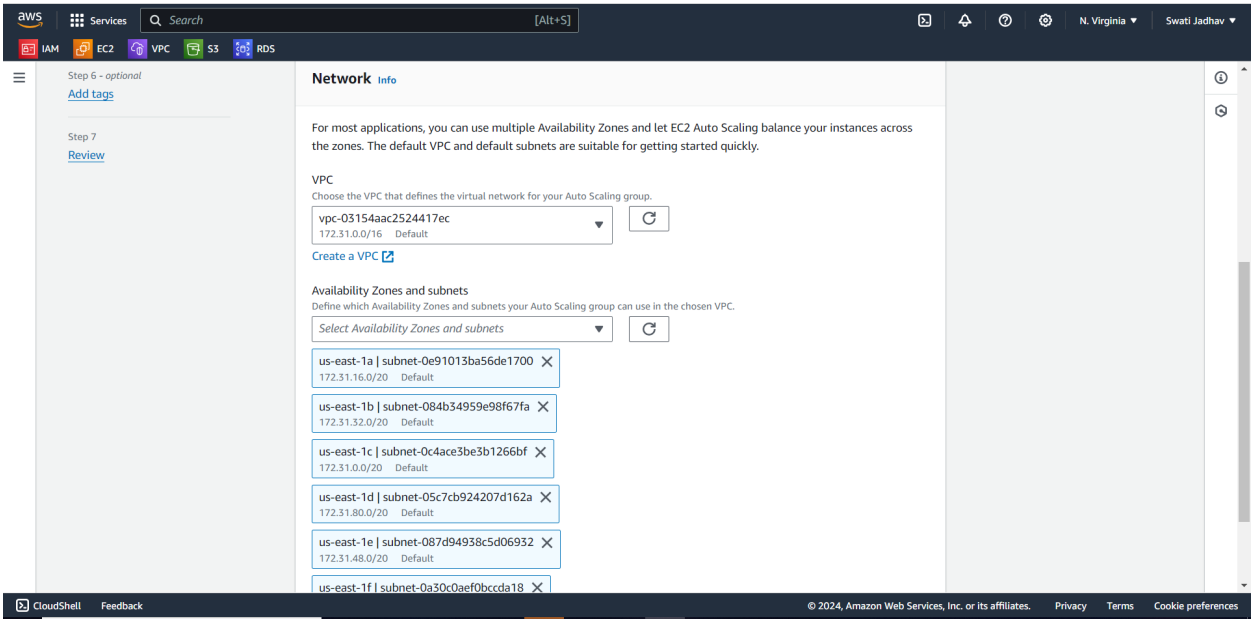
- Give a name to the auto-scaling group and choose the launch template.



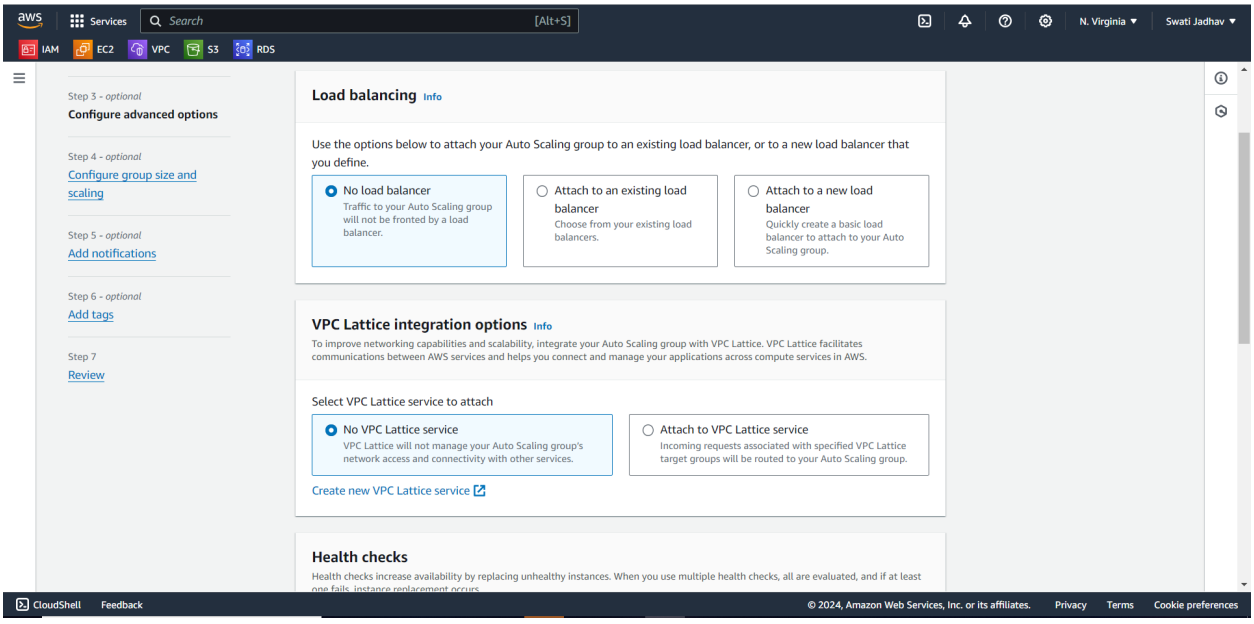
- Check the Instance type requirements.



- Select the Availability zones

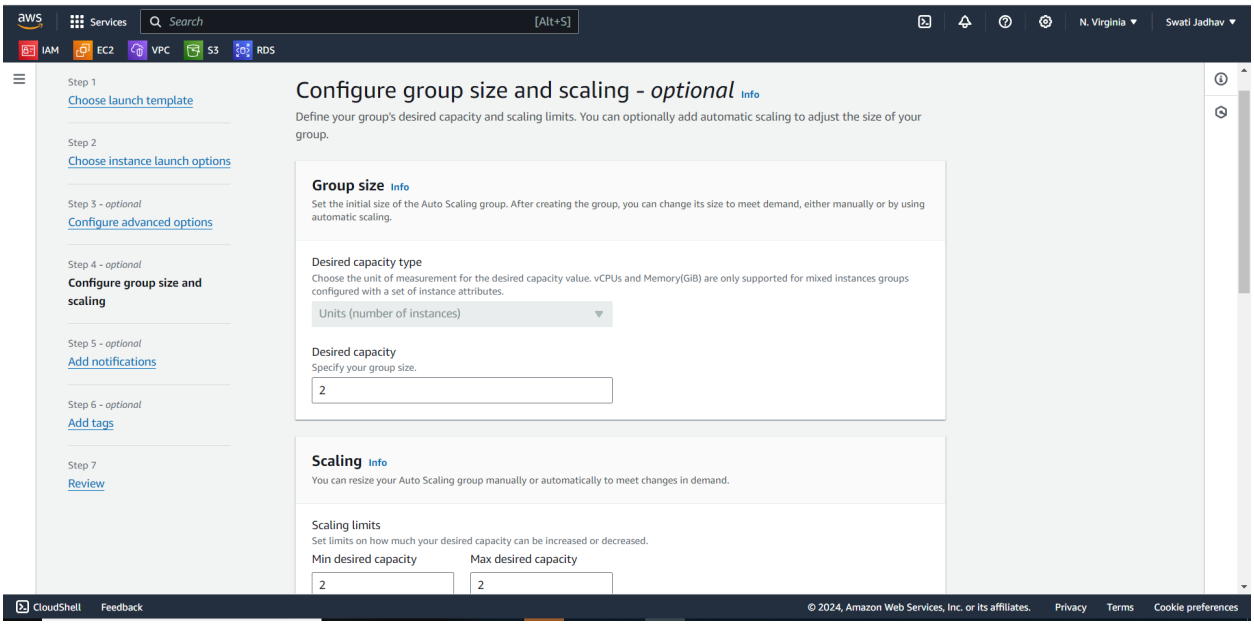


- Select No load balancer, as we haven't yet created a load balancer

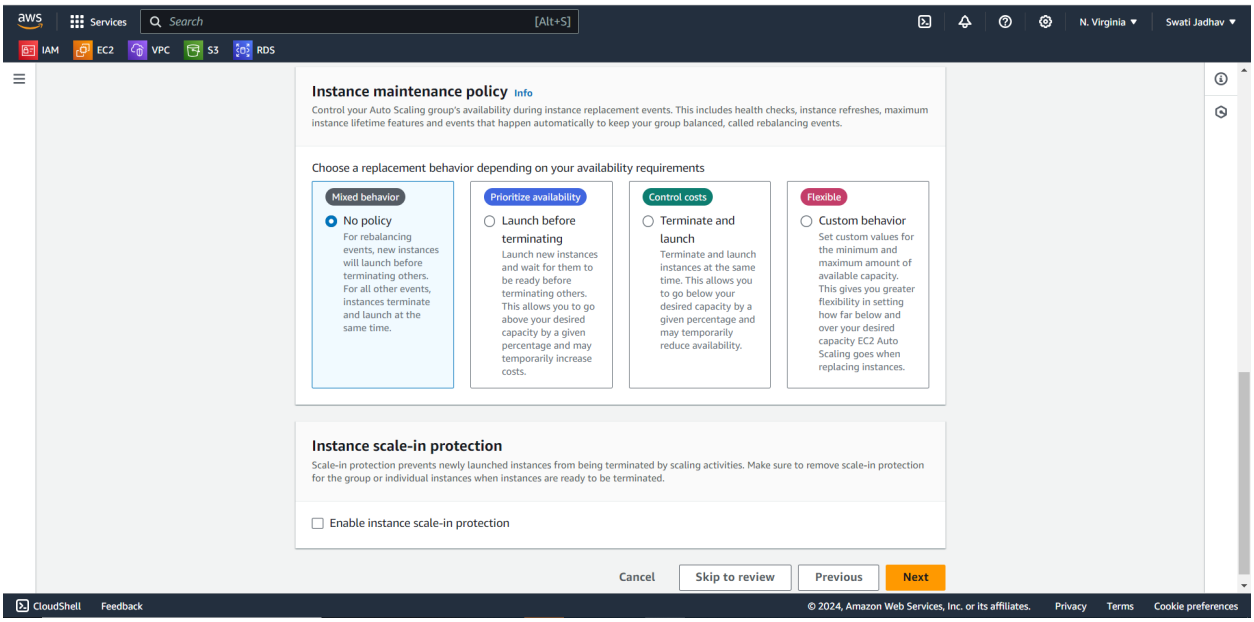


- Configure group size and scaling

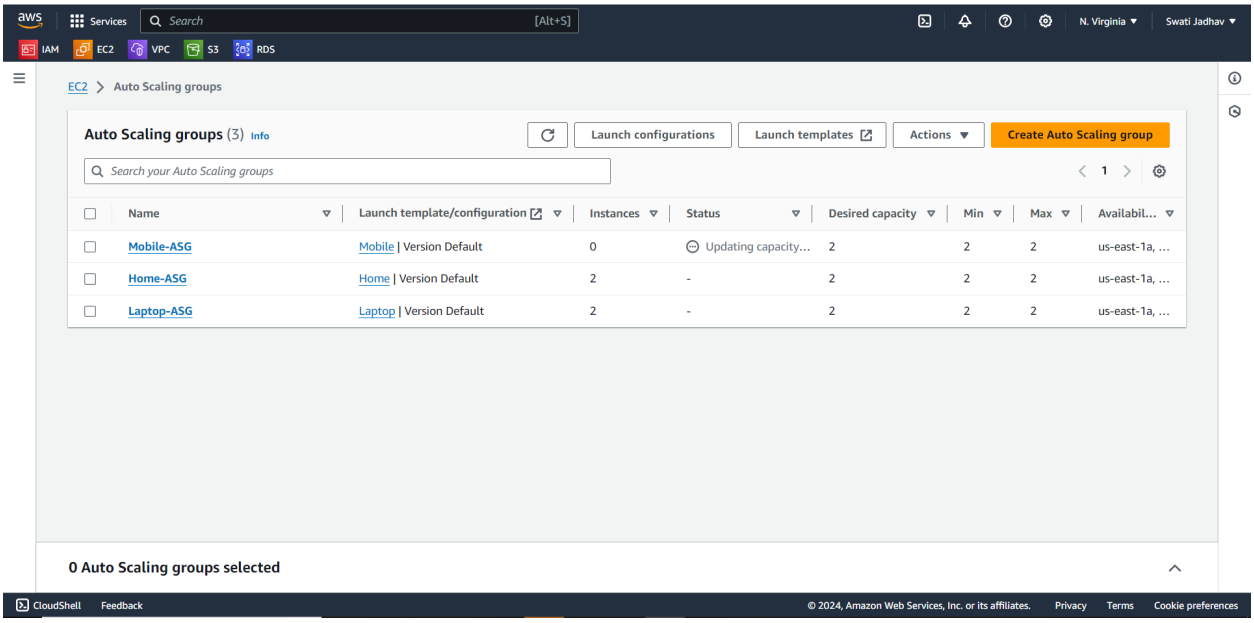
- Give the desired capacity(min.desired and max.desired)



- Choose instance maintenance policy.

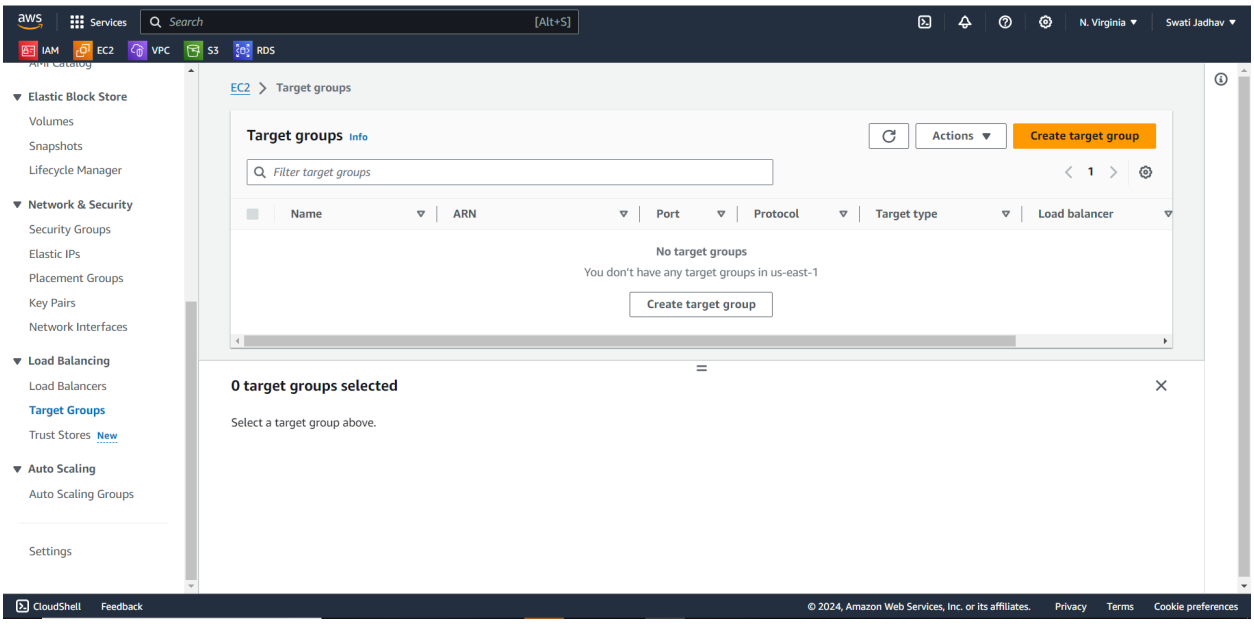


- Create the same configuration of the auto-scaling group for home and mobile templates

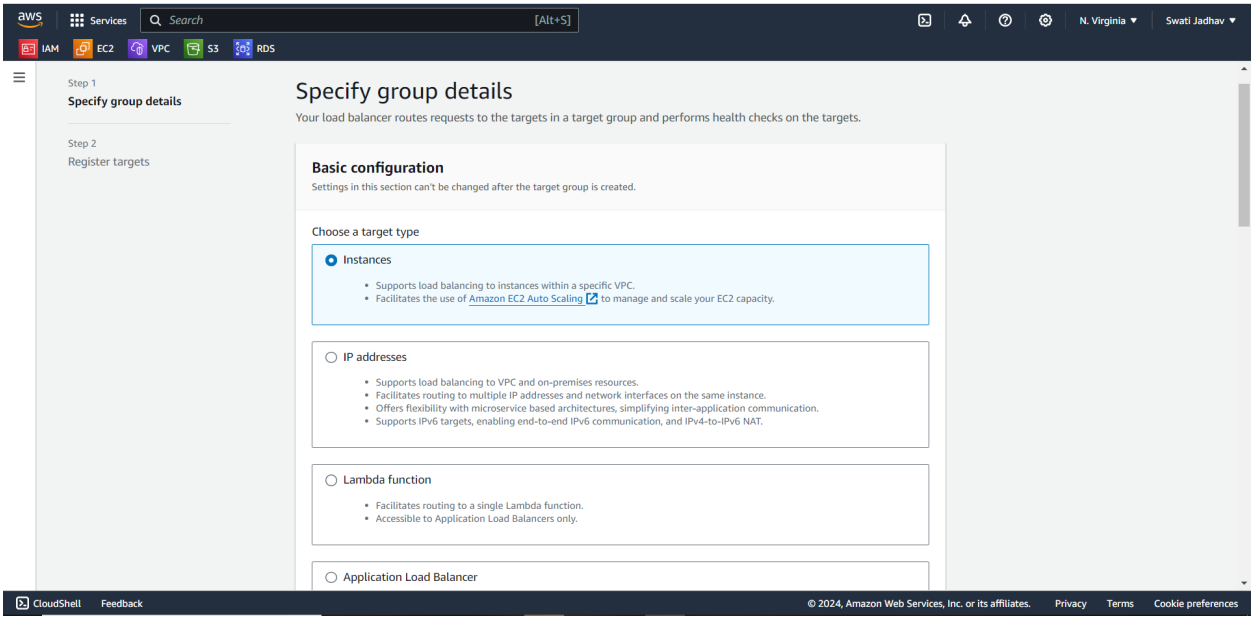


Step 4: Create target group

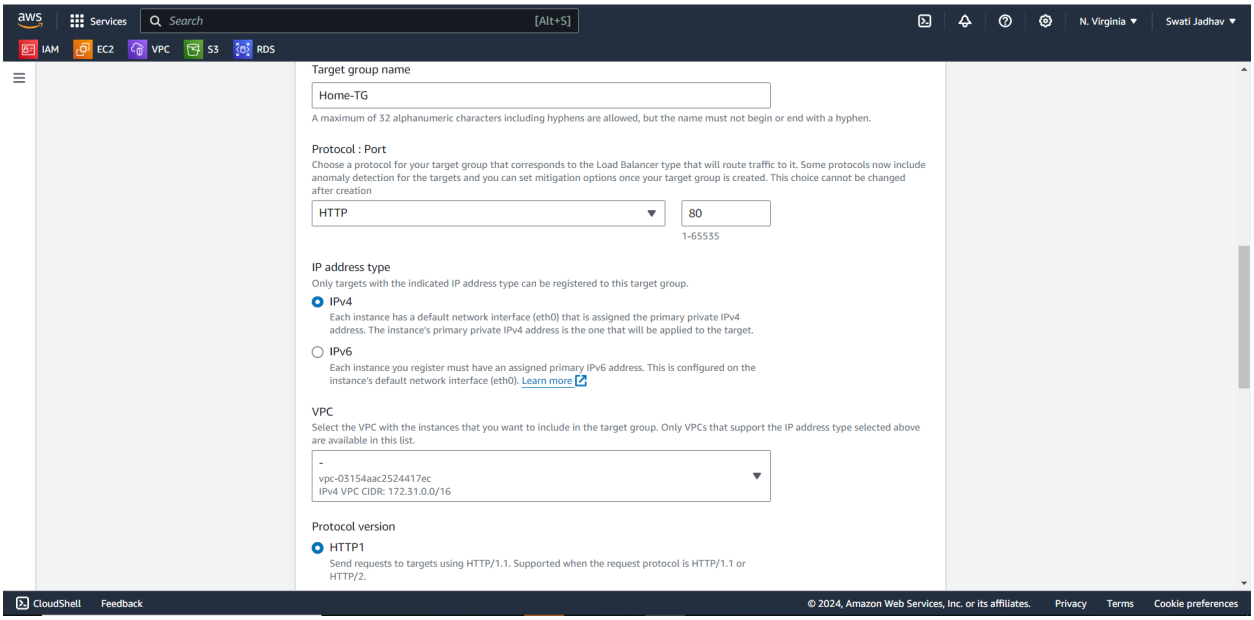
- Create three different target group.



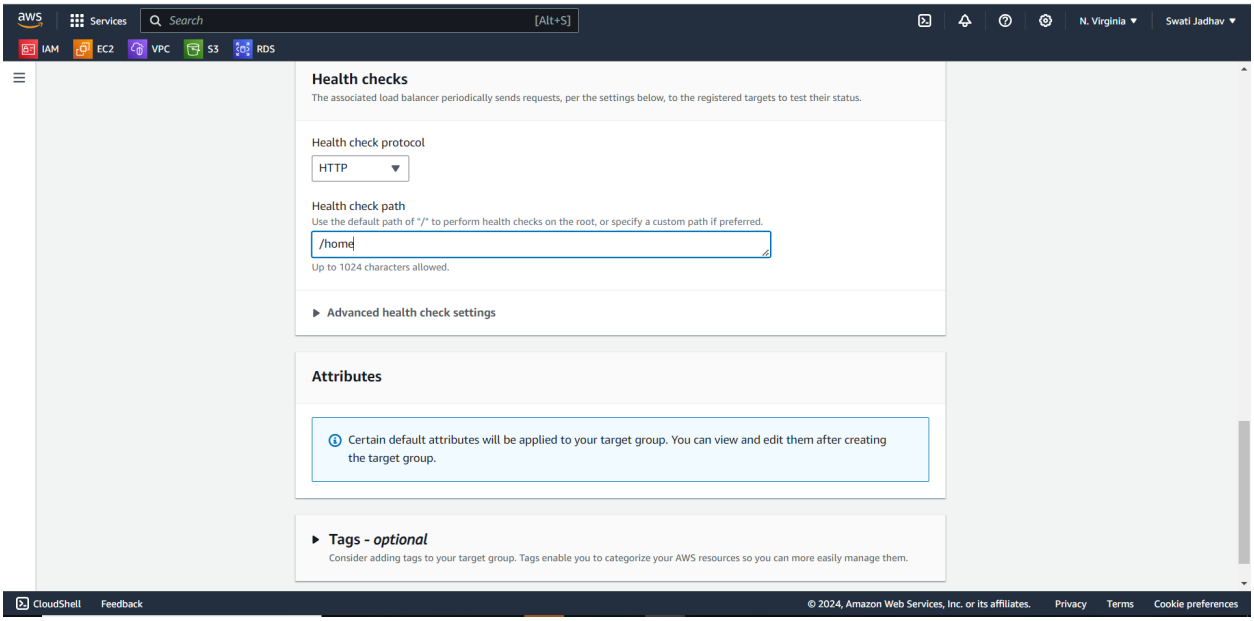
- Specific group details, Choose the target type.



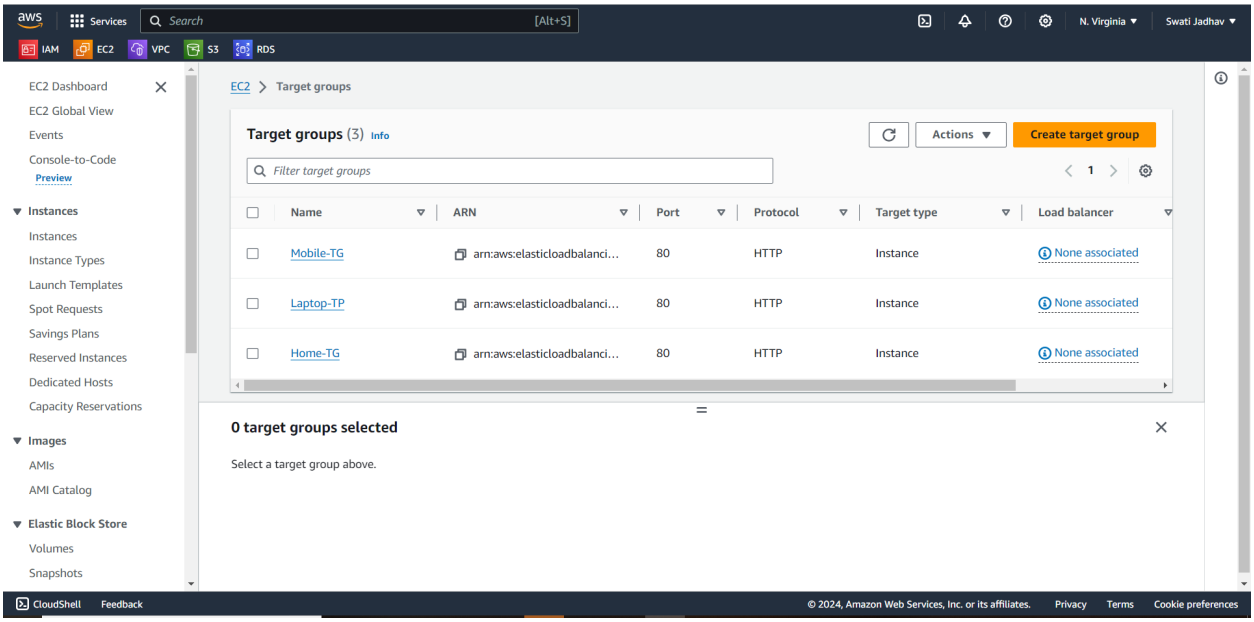
- Give a name for the target group.



- Give the health check path

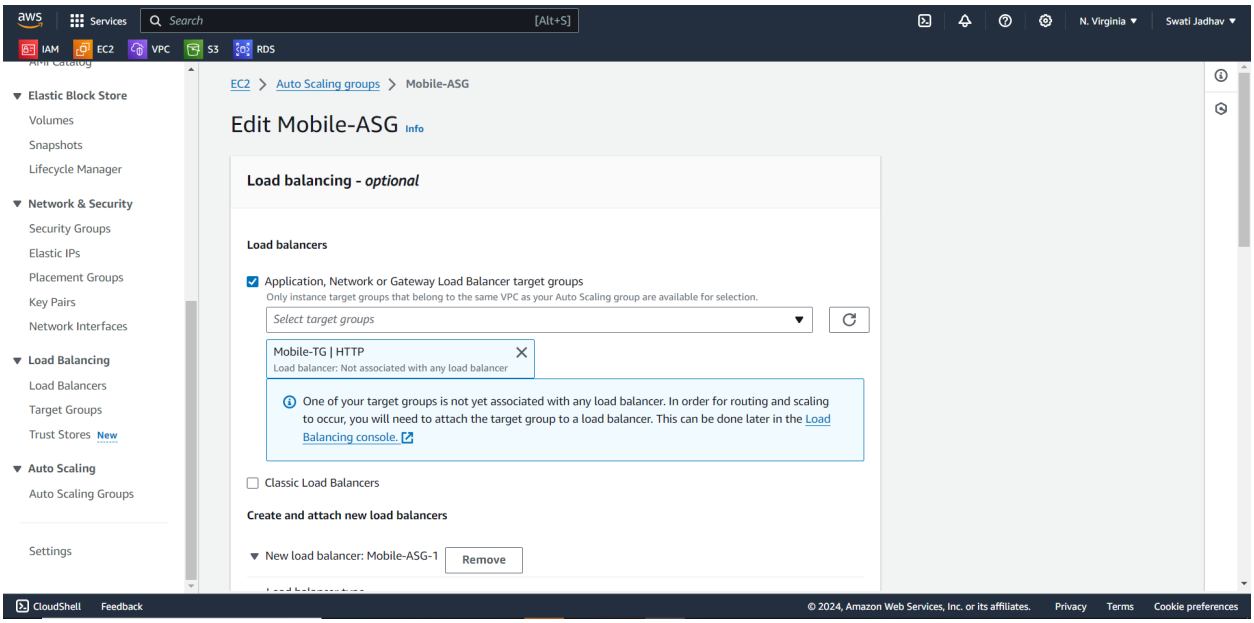


- And create all three target groups.



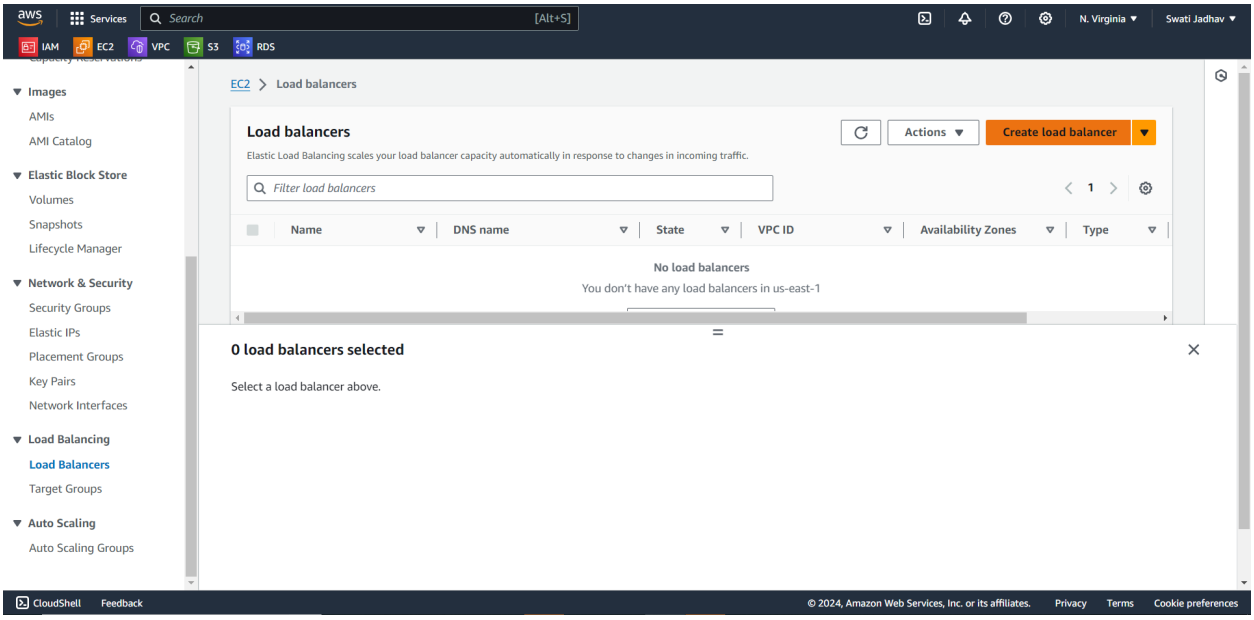
Step 5:Attach target group to the Auto-scaling group

- Go to the auto-scaling group and on a particular group.
- Scroll down and in the load balancer click on edit.
- Select the Application Load balancer
- Now, select the target group that you want to attach the auto-scaling group.
- Likewise, attach all three target groups to the auto-scaling group.

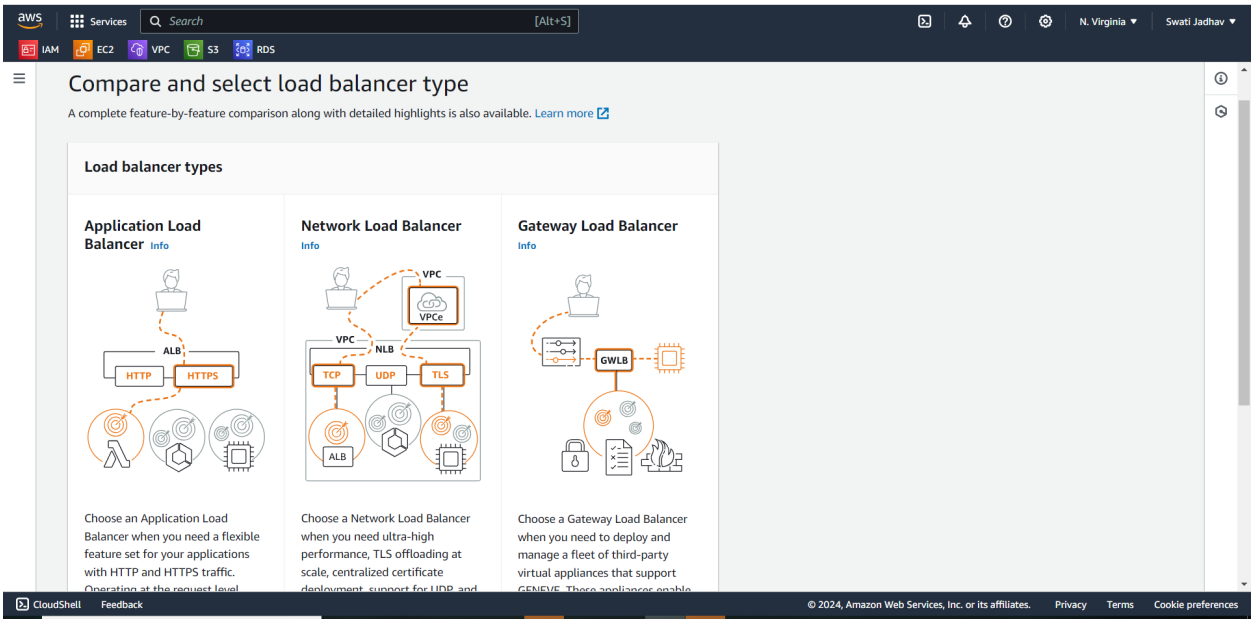


Step 6 :Create a Load Balancer

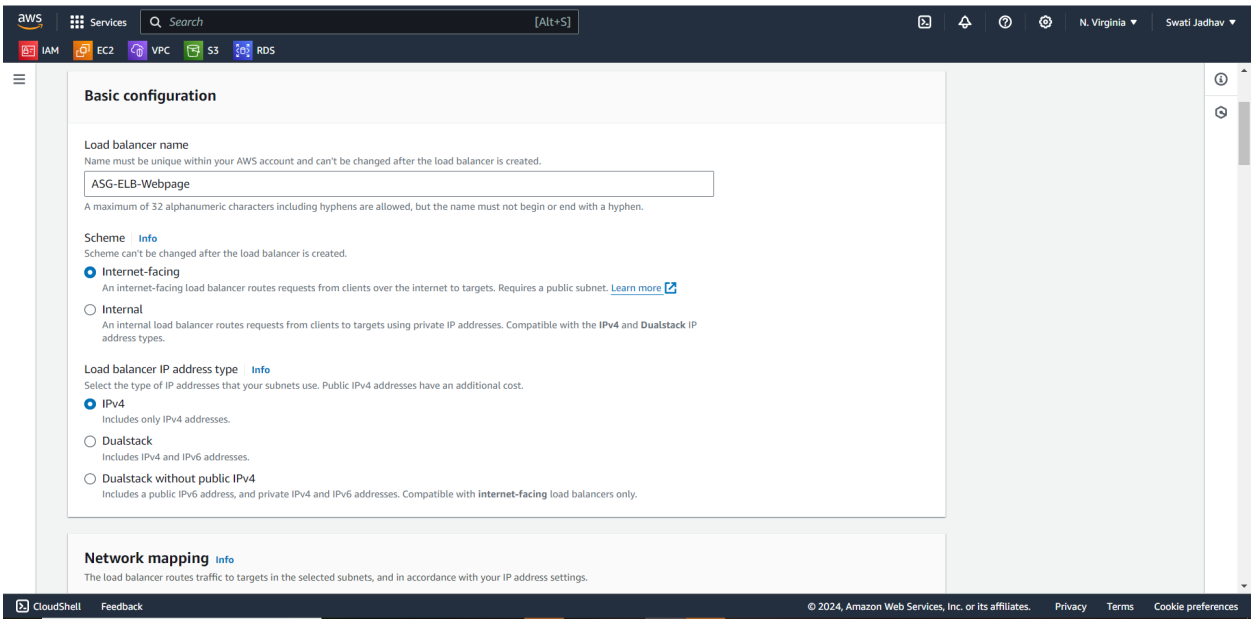
- Select the load balancer from sidebar.



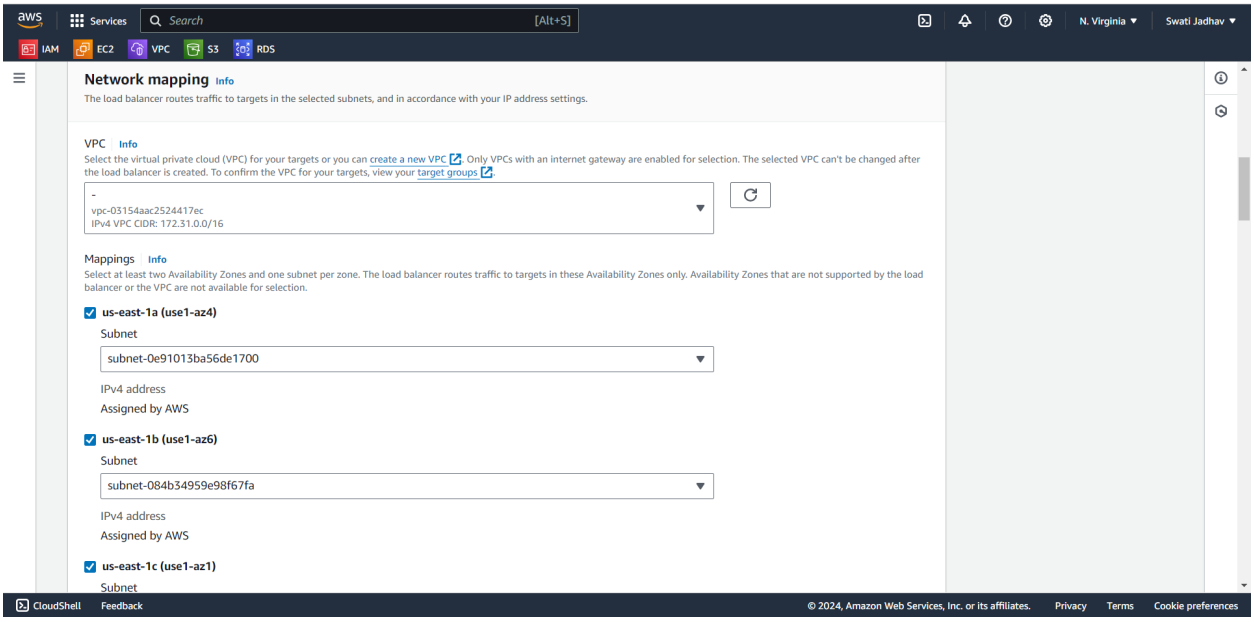
- Choose a load Balancer type(Application Load Balancer)



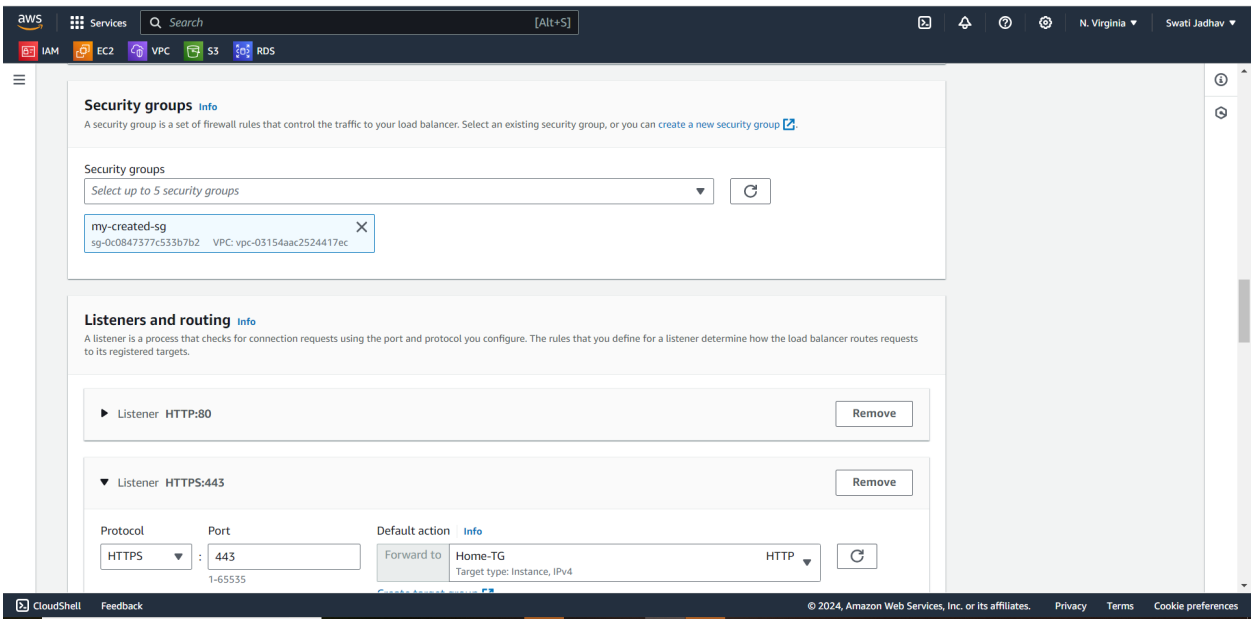
- In, Basic Configuration, give a name to the load balancer.



- Select the availability zones in the Network.

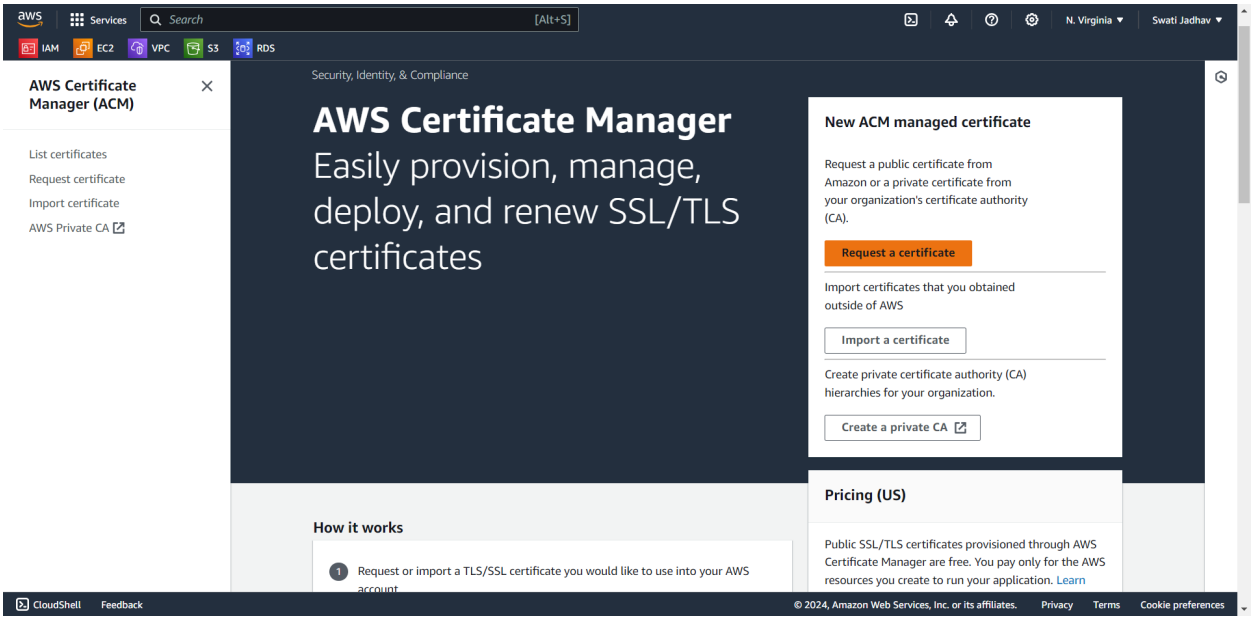


- Attach the Security group.
- Add the Listeners port as 443 for HTTPS.

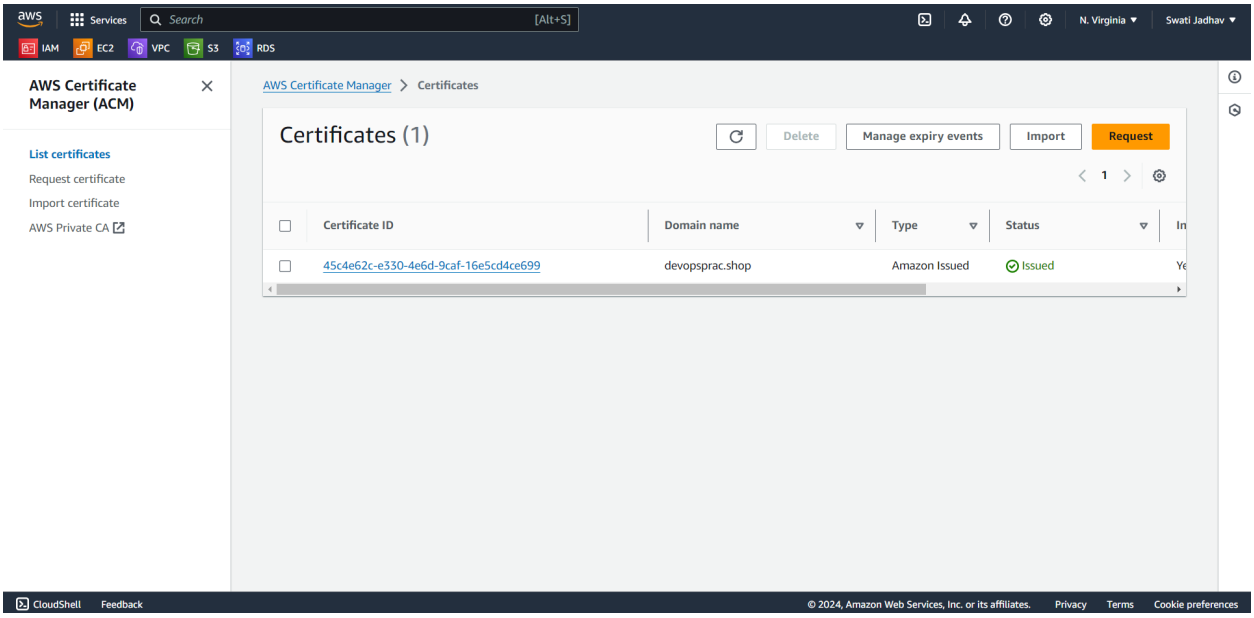


Step 7: Create an AWS Certificate Manager

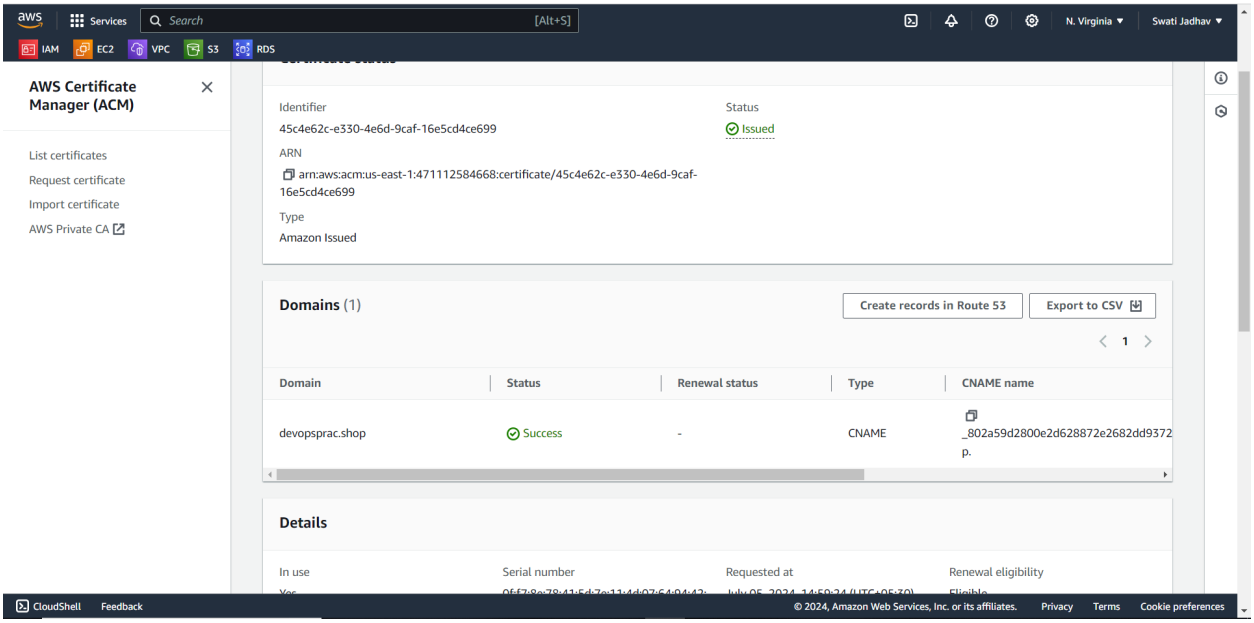
- Search AWS Certificate Manager in the search bar in the console.



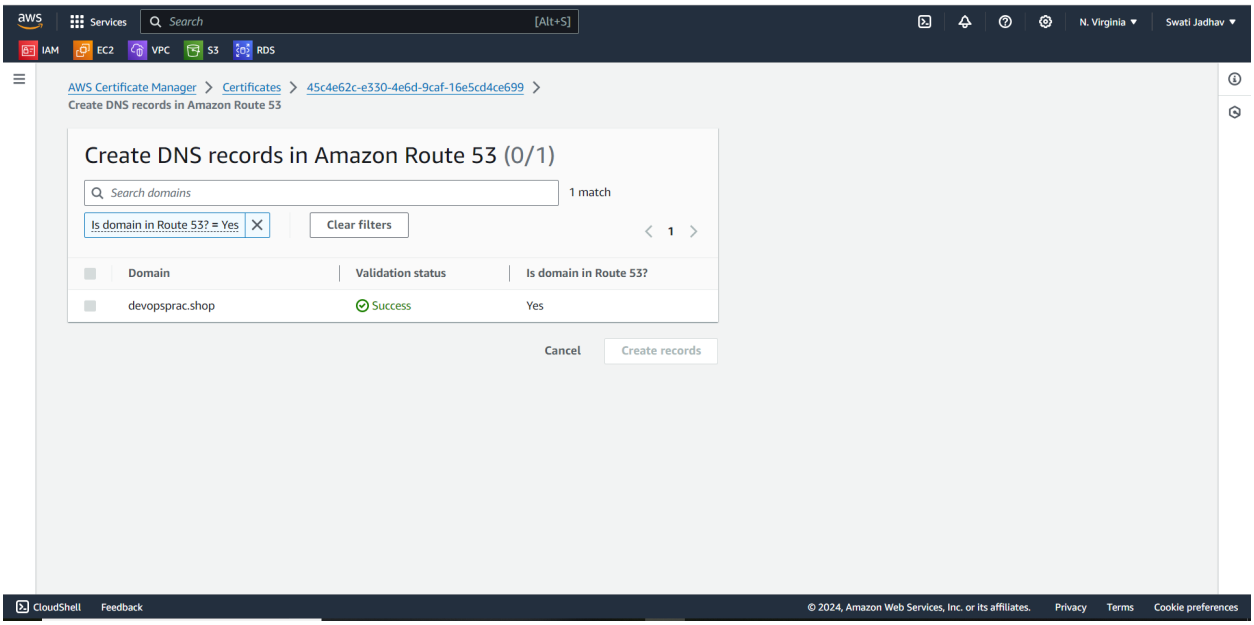
- Give your DNS Name, and request the certificate.



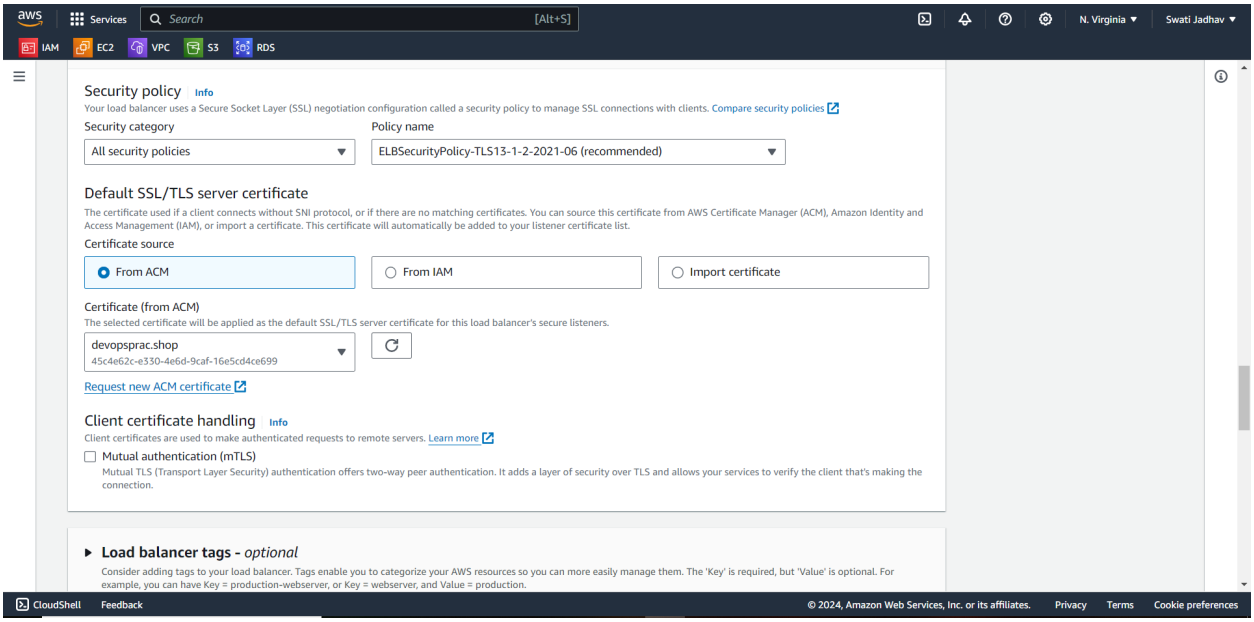
- Once the certificate is issued then, click on the Certificate ID.
- Create a record in route53.



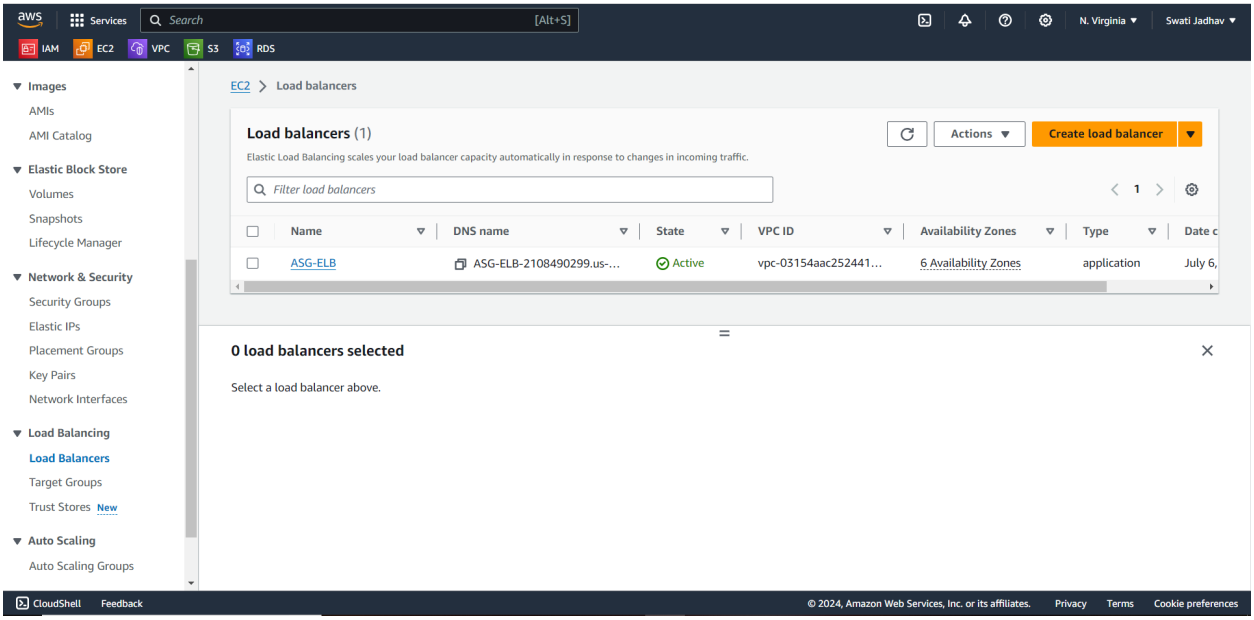
- Select the Is domain in Route53, select the domain name, and Click on Create Record.



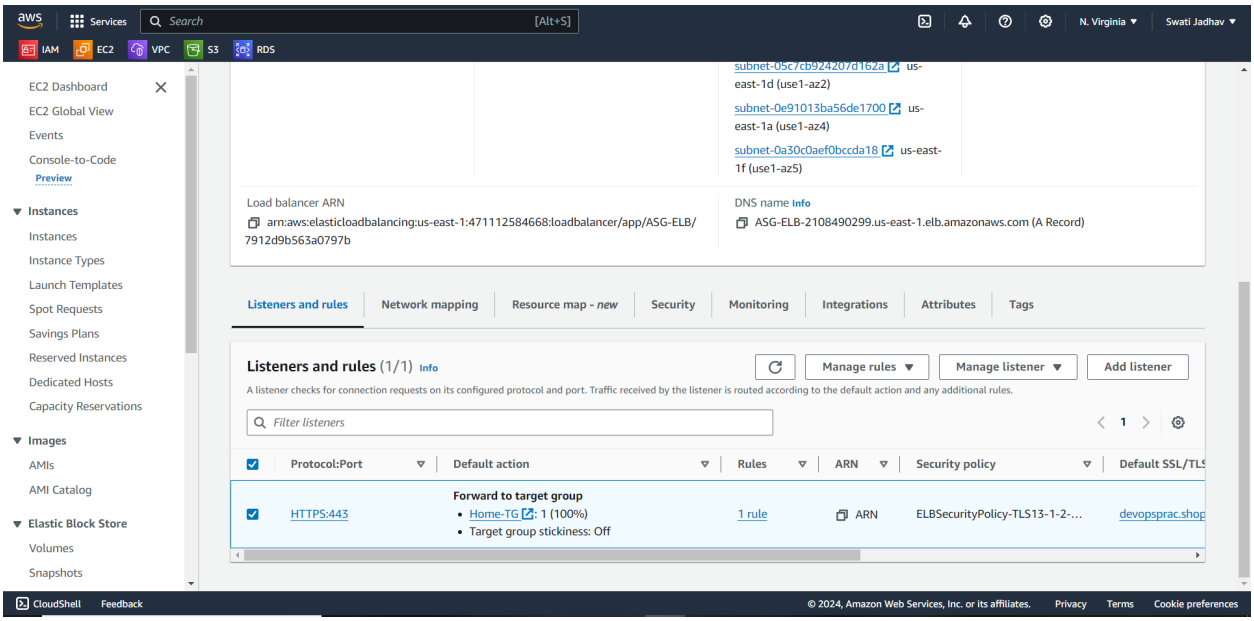
- In the Security policy, you need to give a certificate for HTTPS. Select your certificate.



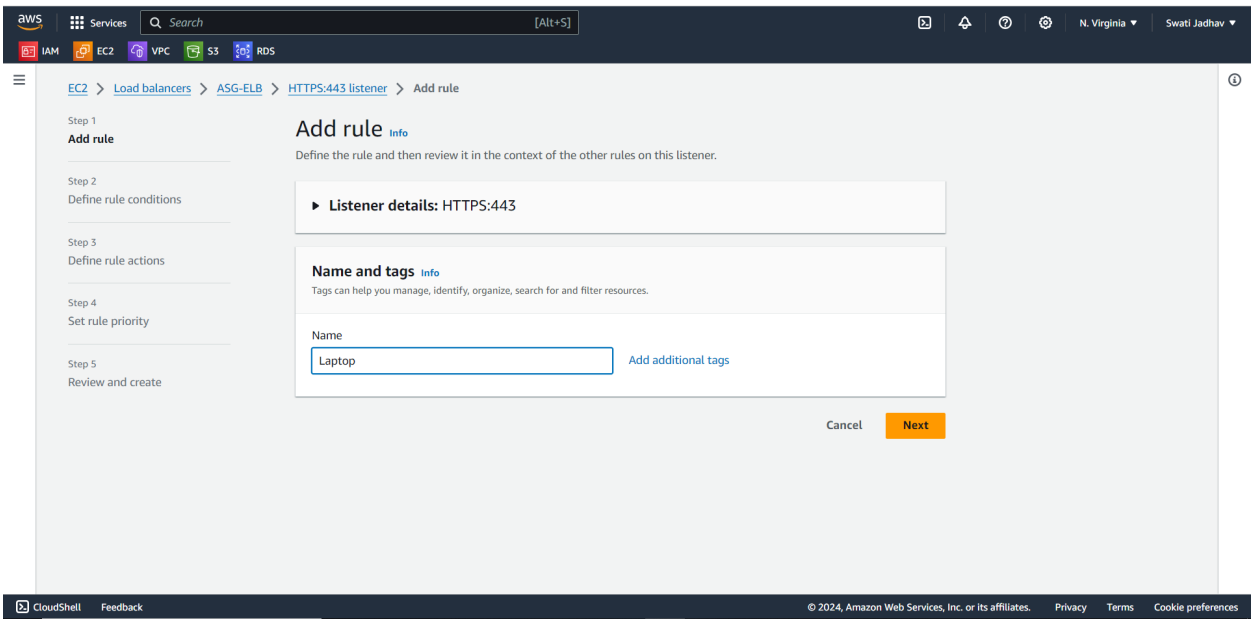
- The load balancer is successfully created.



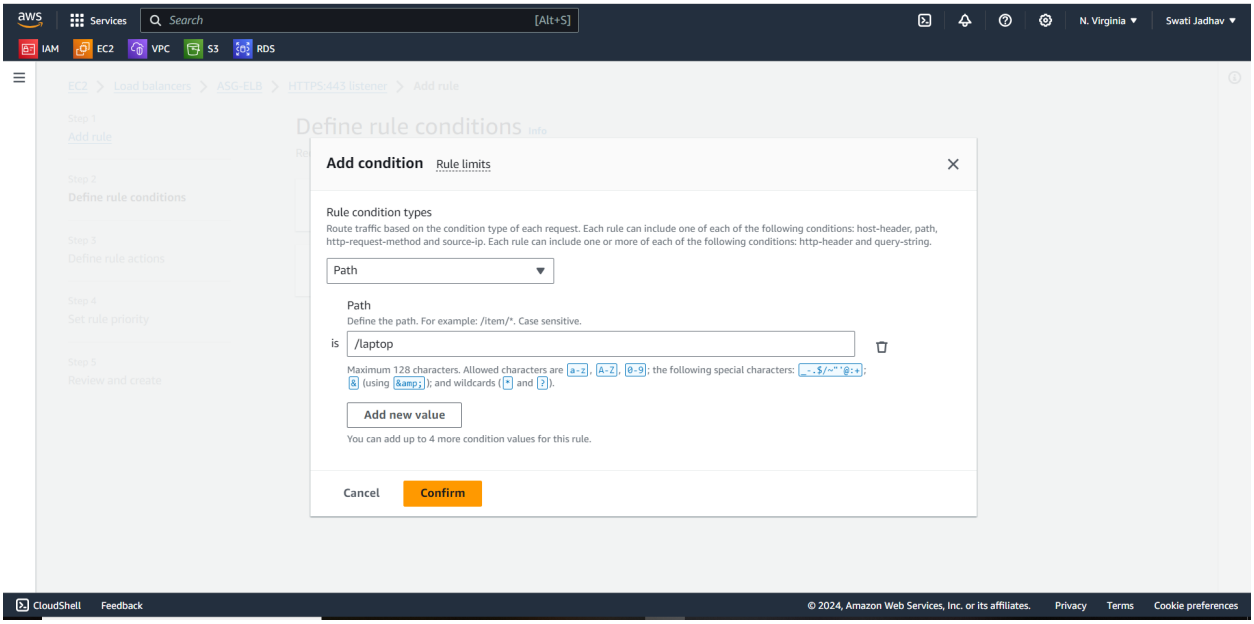
- Click on the ALB name and scroll to manage the rules.
- Check the Check box next to the port.



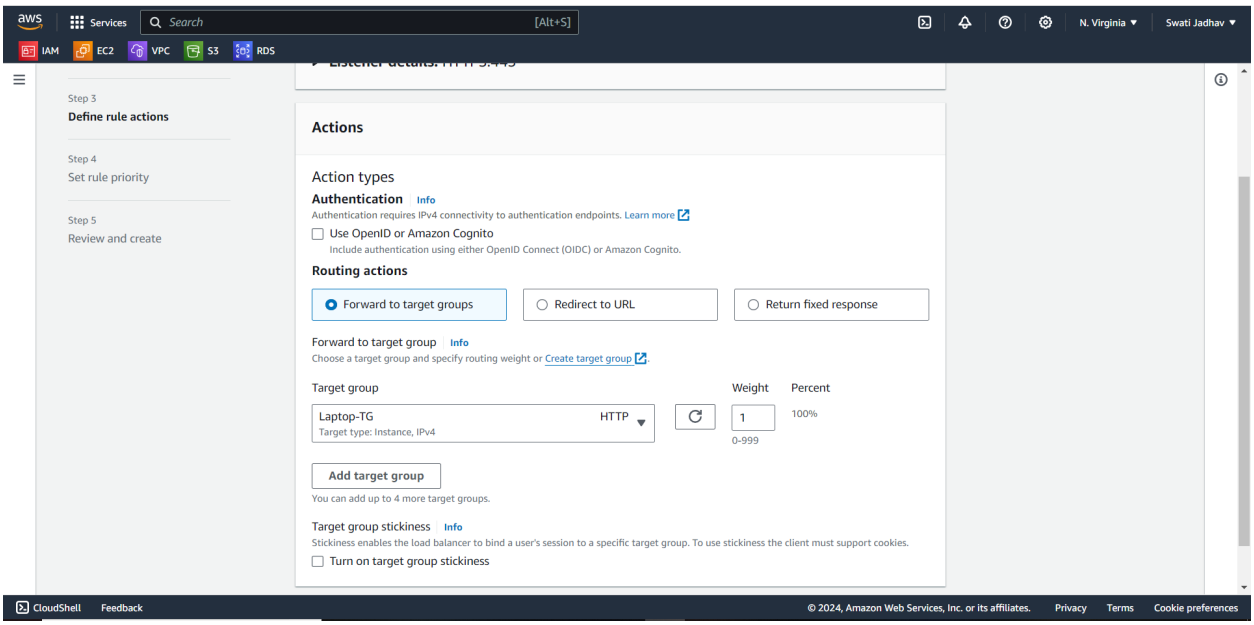
- Add rule for Laptop then click next.



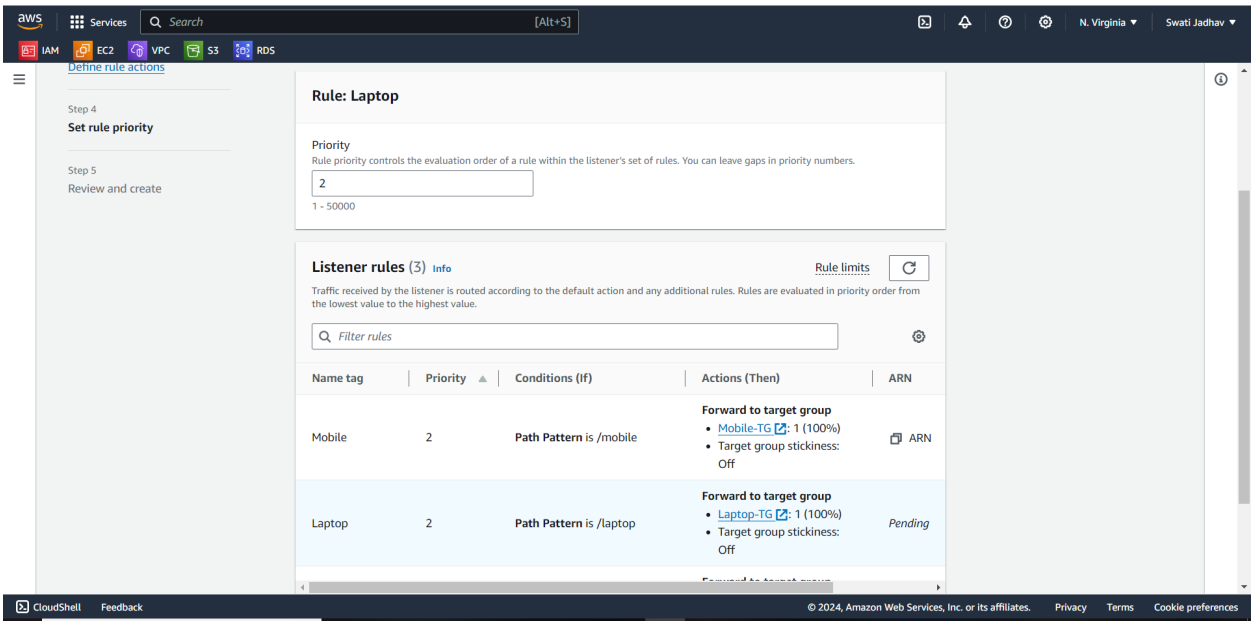
- In the add condition, Select the path in the dropdown, and give the path that you want, and click on Confirm.



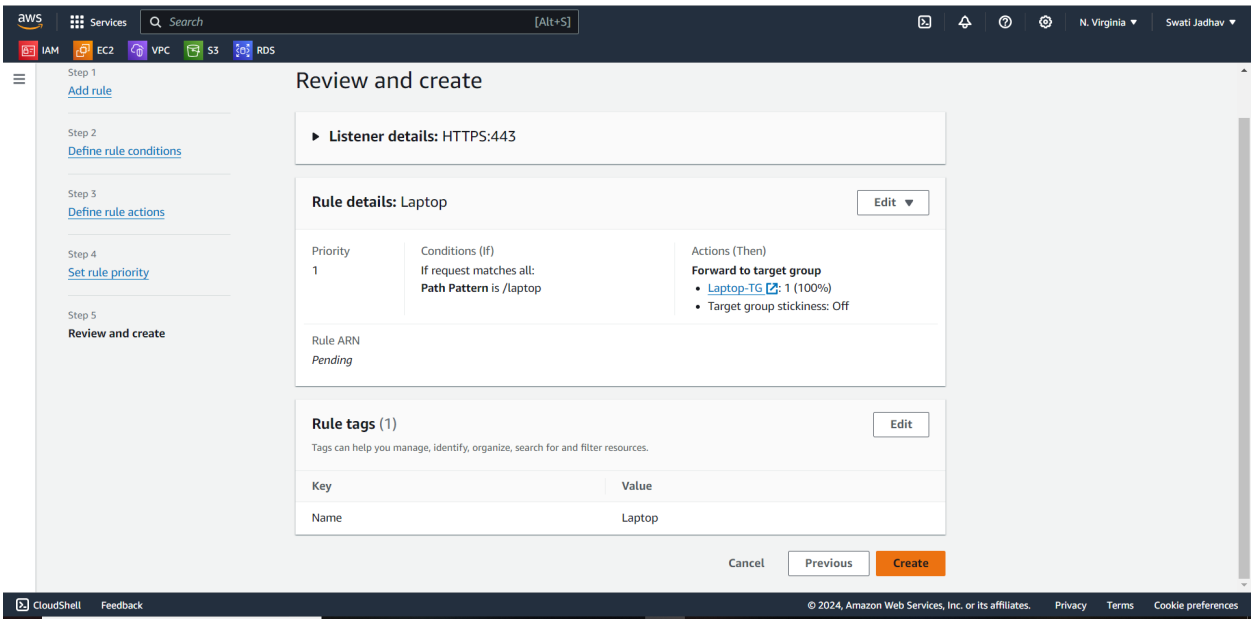
- Now in action give the target group.



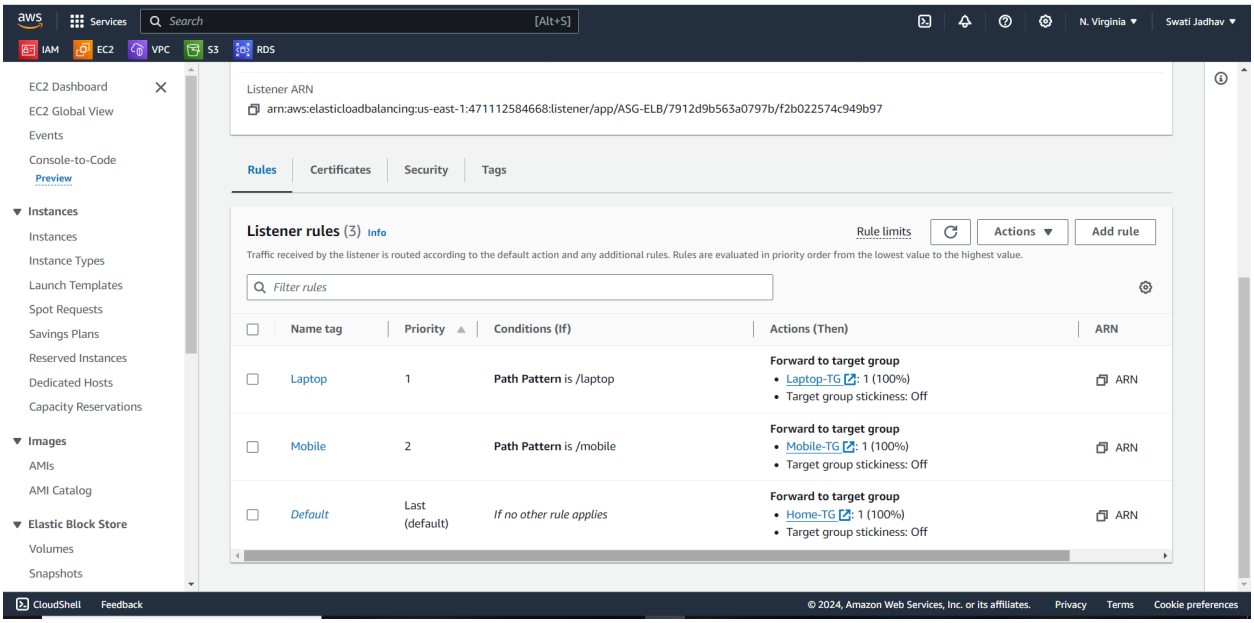
- Set the priority for the rule.



- Review and create the rule.

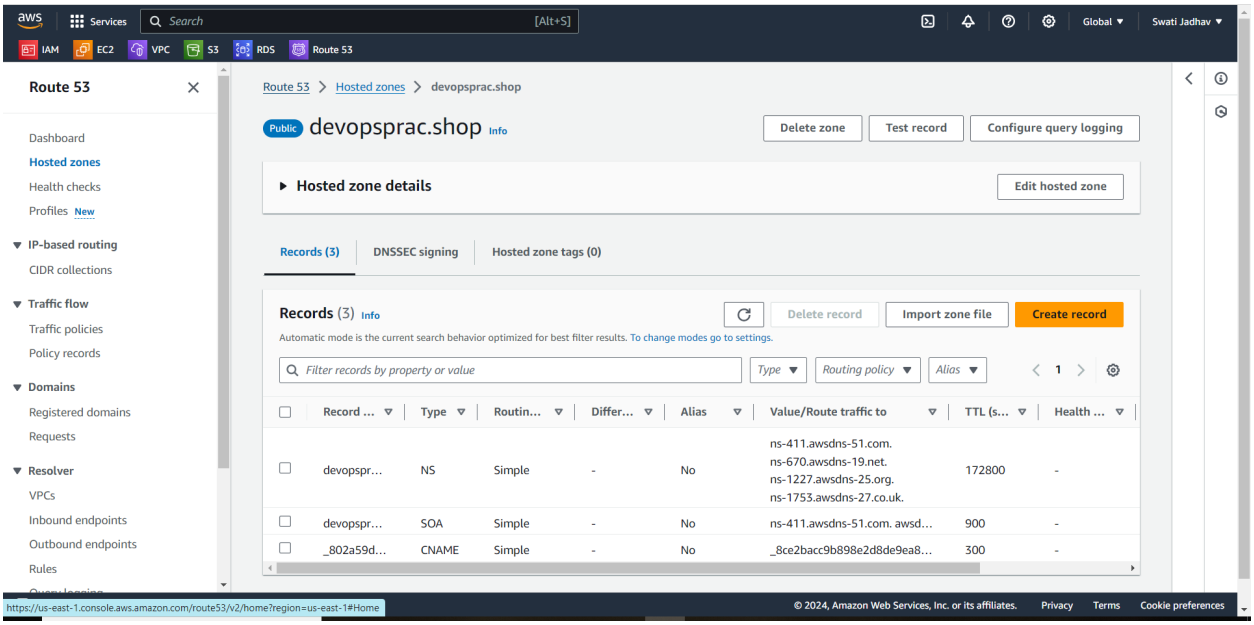


- Likewise, Create rule for mobile also.



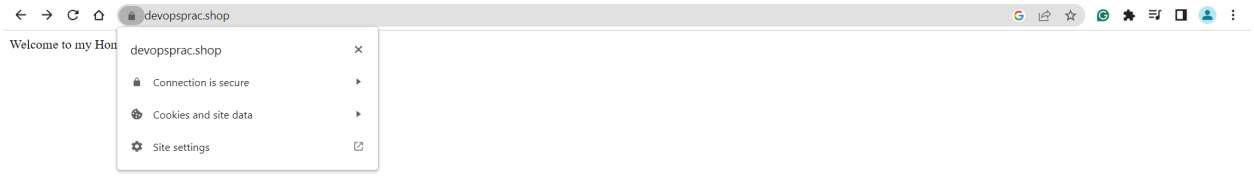
- In Route 53, Create one hosted zone.
- Click on the hosted zone, you will get the value that you will have to add in the Hostinger(From where you have purchased the DNS)

- The record will be created



When you hit the DNS the website is successfully displayed.

- The connection for the Website is secure.



Summary

You have successfully set up a scalable and load-balanced infrastructure that secures your connection with HTTPS and SSL. This will ensure that your application can handle increased traffic and provide a secure connection for users.