E-HEALTH

Designing and Implementing a Secure AWS Cloud Solution

APRIL 22, 2021

SURENDRA DURA
2020436@student.cct.ie

Table of Contents

Introduction:

E-Health is a SME medical company in Ireland who like to develop a website in the AWS, and they hired me for the AWS architect to make a secure and high availability AWS application. So, I would go on make the AWS architect on the based of the customer requirements.

TASK 1: Technical Solution on the base of customer requirements:

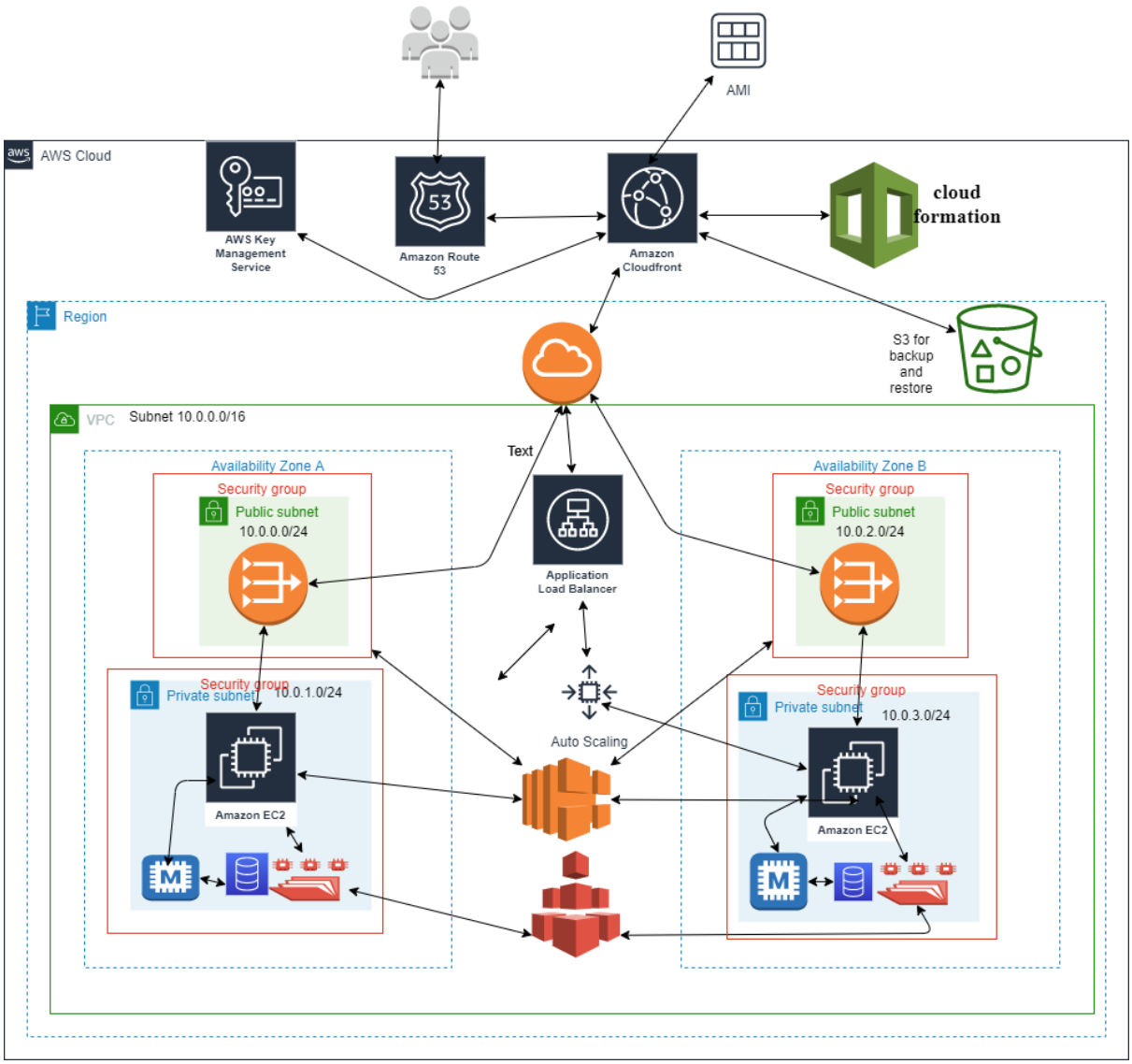
The technical solution of the AWS architect on the based of customer requirement are as follows:

1. At first, I will choose the region(Global Infrastructure Regions & AZs, 2021) which is “eu-west-1” because it is the region available in Ireland where my physical data has been saved. On the other hand, for the North America I will choose the “us-west-2” region because it is near the North America. The two regions help me that the customer feel better experience while using the website in the two different location and if one region fail than another region will work, and my system will not fail so that my website is still working.
2. Then, I will make Virtual Private Cloud(VPC)(Amazon Virtual Private Cloud (VPC), 2021) inside each region which help me to customize my VPC network so that I will make private and public subnet inside the VPC. In the public subnet, I will make web tier with the access of internet so that the customer can use my website and in the private subnet I will put my database with no internet access so that my database will be secure from the hackers. VPC also help me to develop a security groups and network access control so that my Amazon EC2 instances will be run smoothly and securely.
3. Then, I will make two Availability Zones(AZ)(Global Infrastructure Regions & AZs, 2021) so that I will get my website is highly available, fault tolerance and scalable in the data centre. If the one AZ will not work because of the natural disaster than another AZ will work so that my customer can use the website. Both the AZ will have same thing inside it like public subnet, private subnet, EC2 instance, Database and soon.
4. Inside the public subnet, I will have NAT gateway(NAT gateways - Amazon Virtual Private Cloud, 2021) so that I will get the internet access to the private subnet using the route table.
5. Inside the private subnet, I will make Amazon EC2 instance(What is Amazon EC2? - Amazon Elastic Compute Cloud, 2021, p. 2) on the Amazon Linux 2 AMI because they want their system in Linux base machines. By using EC2 instance, I can scale my virtual computer on their capacity, security group, networking. It also helps me to flexible to chance my storage and networking anytime. EC2 comes with Amazon Elastic Block Store(Amazon Elastic Block Store (EBS) - Amazon Web Services, 2021) which help me to resize my EC2 instance anytime.
6. Inside the private subnet, I will use Amazon RDS(Amazon RDS | Cloud Relational Database | Amazon Web Services, 2021) so that I will store my relational database inside the AWS.
7. The Two EC2 instance available in the two AZ will be connect with the Amazon EC2 Auto Scaling(Amazon EC2 Auto Scaling, 2021) so that my application will be automatically scaling on the base of the requirements. For example, if the more user come on my site than it will automatically scale the EC2 and give more power so that customer experience the same result in any condition.

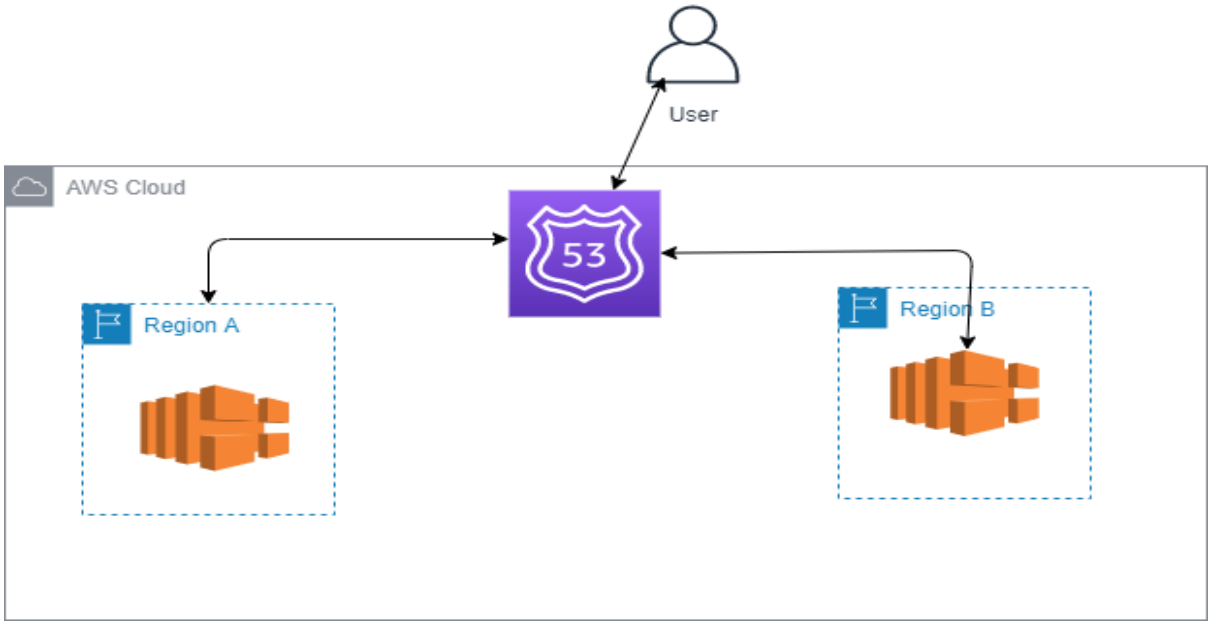
8. Inside the private subnet, I will use Amazon EFS(What is Amazon Elastic File System? - Amazon Elastic File System, 2021) so that it gives me flexibility while adding and removing files because in my requirement, the customer have the option to add or remove the file. EFS help me to maintaining the file storage automatically.
9. Inside the private subnet, I will use Amazon ElastiCache for Memcahed(Amazon ElastiCache for Memcached, 2021) so that the customer can easily access the database from my website.
10. Outside the public and private subnet, I will make security group so it will control the inbound and outbound traffic to AWS resources. For example, web tier can be access from any user, but the application and database tier can only be access from the admin which secure my website.
11. I will connect two AZ with the Application Load Balancer(What is an Application Load Balancer? - Elastic Load Balancing, 2021) so it will automatically control the incoming traffic across the two AZ. So that traffic coming from the HTTP and HTTPs will access my website.
12. I will use the Internet Gateway to flow the internet inside the VPC and two AZ.
13. I will use Amazon Route 53(Amazon Route 53 - Amazon Web Services, 2021) show that it will translates my Ip address to the domain names.
14. I will use Amazon Cloud Watch(Amazon CloudWatch - Application and Infrastructure Monitoring, 2021) for the monitoring of my application so that I will can easily detect the problem in my system.
15. I will use AWS Cloud Formation(AWS CloudFormation - Infrastructure as Code & AWS Resource Provisioning, 2021) so that it will help me to model, create and manage the AWS resources in my application. It will also help me to control the version in the deployment.
16. For the development, I will make another EC2 instance AMI so that If I can use another EC2 instance AMI for my development and then I will move my development to the original EC2 instance for the production.
17. For the disaster recovery, they want to use backup and restore pattern recovery because it is the cheapest pattern in AWS. For this process, I will going to use the AWS Storage Gateway(AWS Storage Gateway | Amazon Web Services, 2021) which help me to back up my data. By using the Amazon S3.
18. I will used AWS Key Management Service (KMS)(Key Management Service - Amazon Web Services (AWS), 2021) to create and manage my crypto graphic keys so that I will have control in my AWS services and the application.

TASK 2(a): Architecture Diagram:

The architect diagram of the AWS Region is showing below:



So, I will have two region which have same diagram and then I will connect to region with each other. The reason will relate to the Amazon Route 53 so that the IP address can be change into DNS. And it also helps me to choose the region for the customer. For example, Ireland customer use Ireland region and USA customer choose USA region. The region also helps me to copy my backups across Region.



TASK 2(b): Security Design Principal:

The Security design principal in the AWS(Cloud Security, Identity, and Compliance Products – Amazon Web Services (AWS), 2021) are categories in to 5 ways which are a follow:

1. Data Protection
2. Identity and access management
3. Network and application protection
4. Threat detection and continuous monitoring
5. Compliance and data privacy

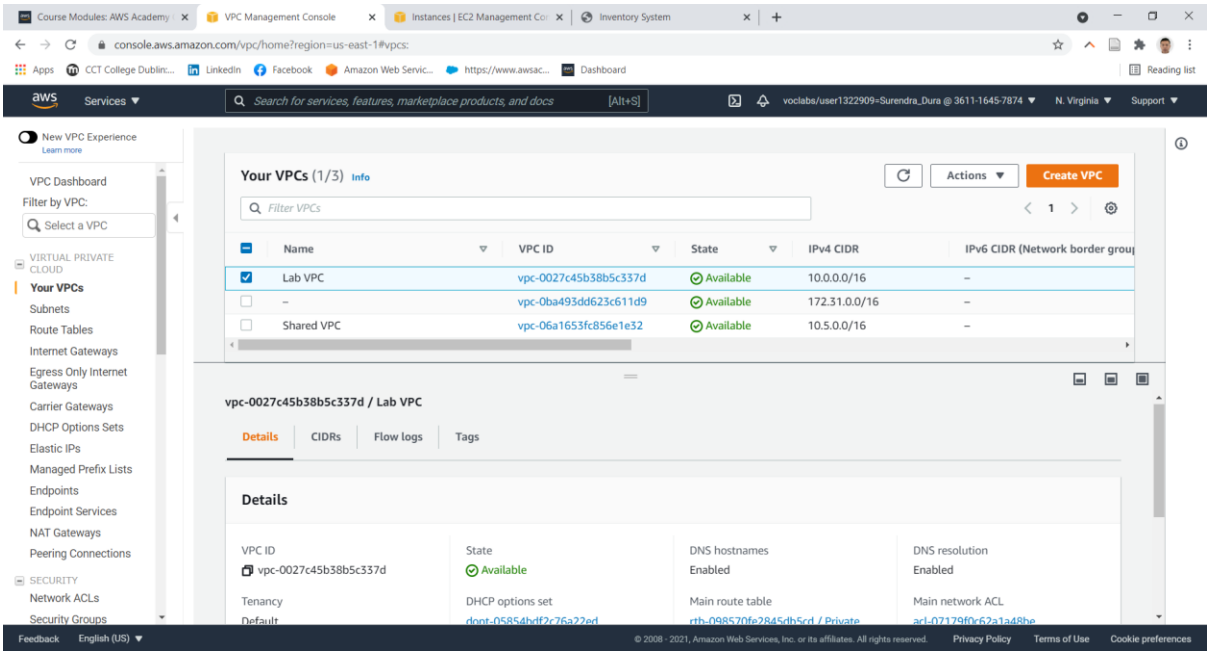
Under this category there are various services inside the AWS. The service I am going to talk about is Amazon Cognito which is under the Identity and access management principal. Amazon Cognito(Amazon Cognito - Simple and Secure User Sign Up & Sign In | Amazon Web Services (AWS), 2021) is the service which help me to add the user registration and login control in the AWS. By using this service, I can easily make registration and login page, and this is the main part of the E-health website also because we must record the database of each patient and doctors. By the authorization process we can track them.

TASK 3: THREE Services:

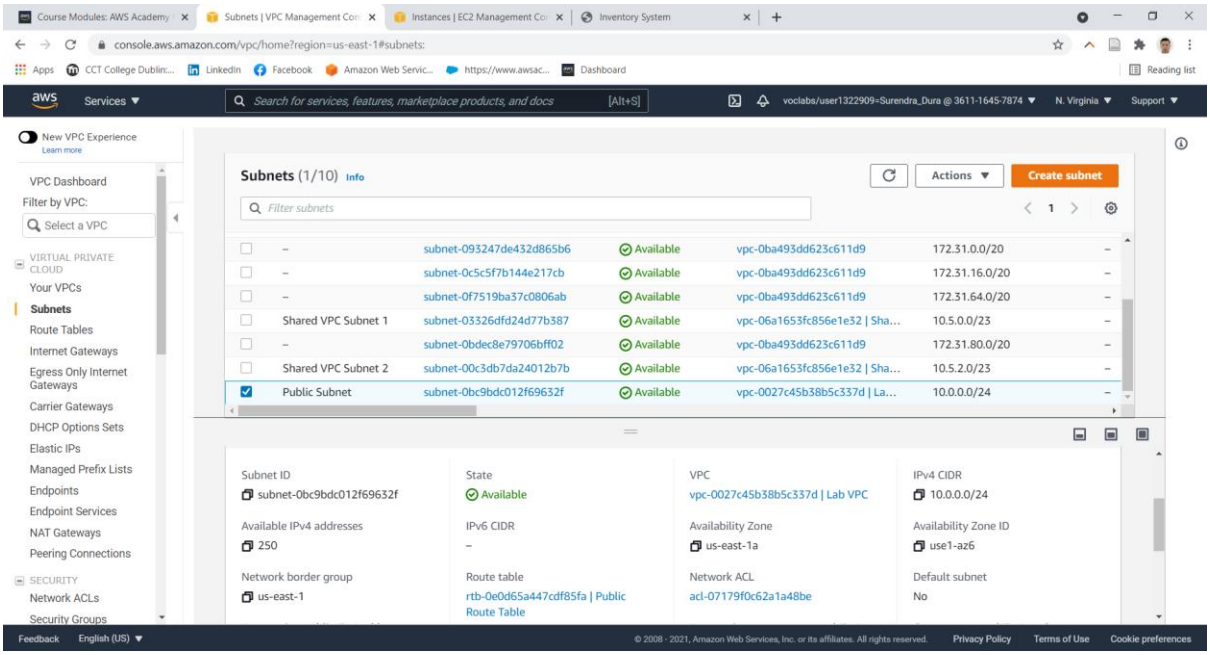
The three services which are going to help me to meet the solution for the E-Health are as follows:

1. ## Creating a Virtual Private Cloud and run the EC2 instance:

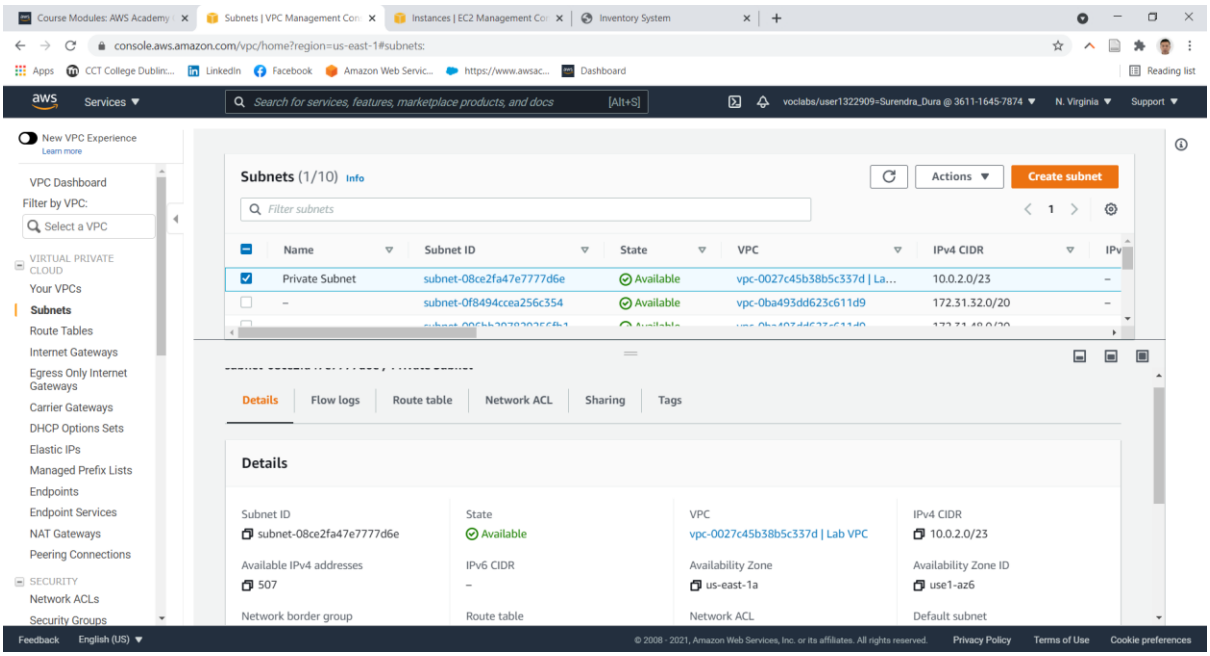
   At first, I went to the amazon web service and I selected the VPC. Then, I made the VPC with the name tag Lab VPC and IPv4 CIDR block 10.0.0.0/16. Then, I enable the DNS hostnames so that EC2 instance inside the VPC will automatically connected with the DNS host.



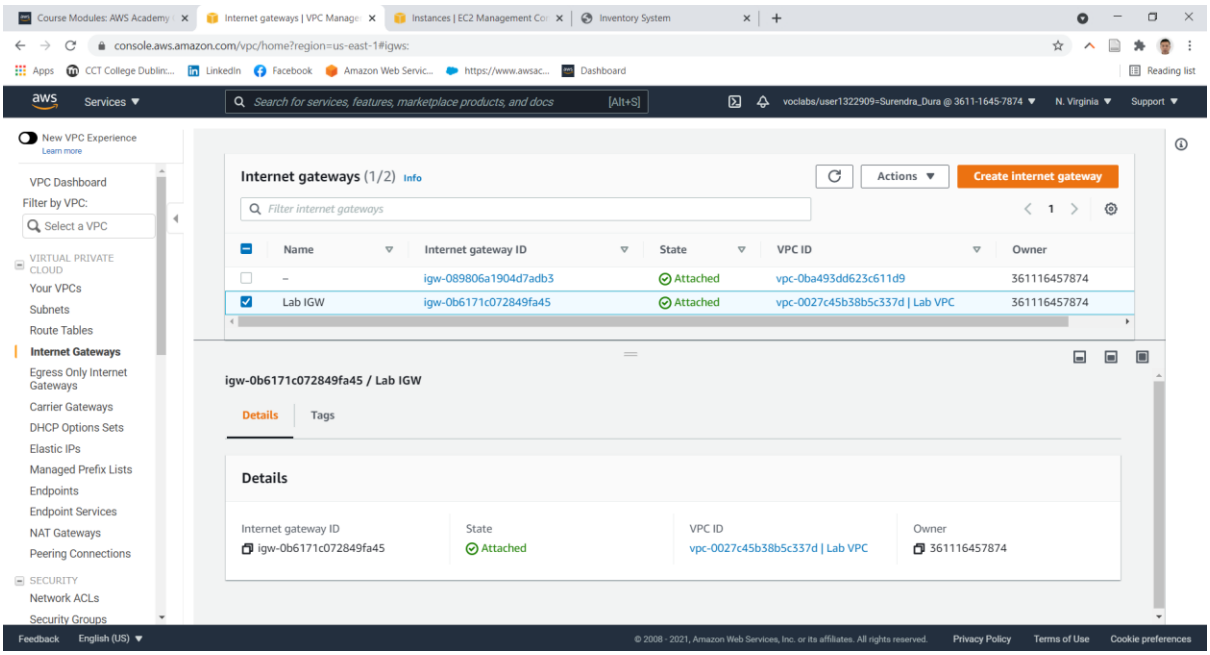
Then, I made a public subnet inside the Lab VPC with the IPv4 CIDR block 10.0.0.0/24 and I enable the auto assign IPv4.



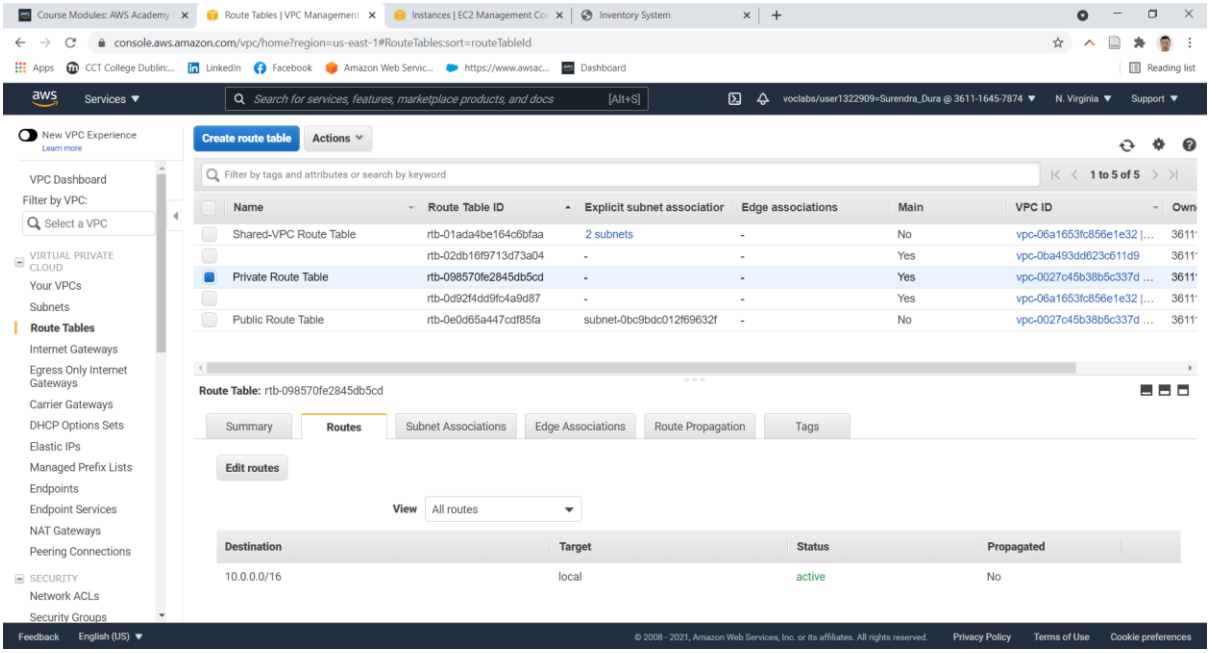
Then, I made the private subnet inside the same Lab VPC with the IPv4 CIDR block 10.0.2.0/23. I put 2 instead of 0 because I must put more resources in the private subnet like EC2, database and soon.



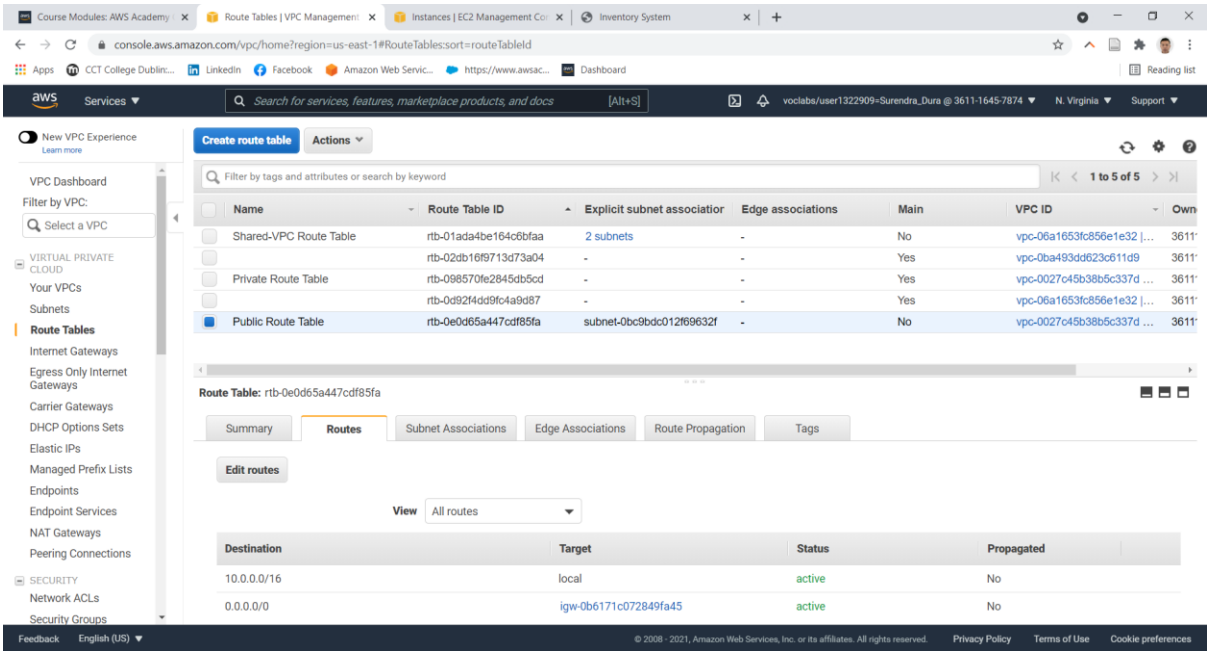
Then, I made the internet getaway with the name Lab IGW and attached with Lab VPC. It helps me to communicated to the VPC and the internet.



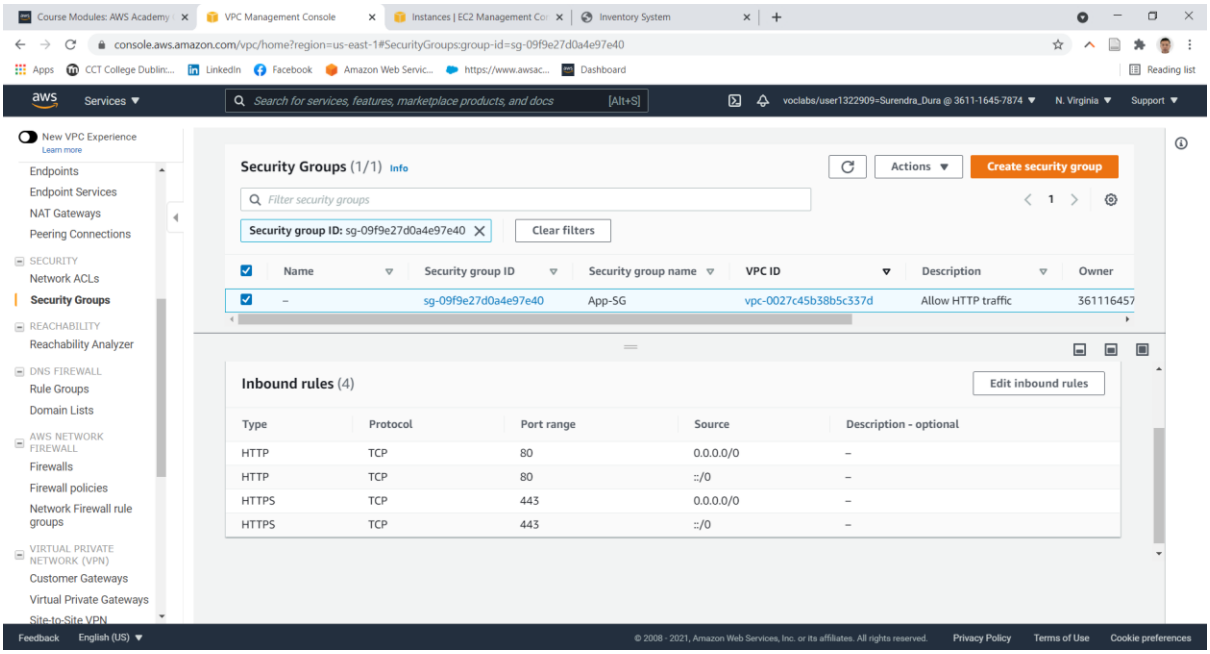
Then, I went to the route table and I give the lab VPC id to the Private Route Table which has traffic 10.0.0.0/16.



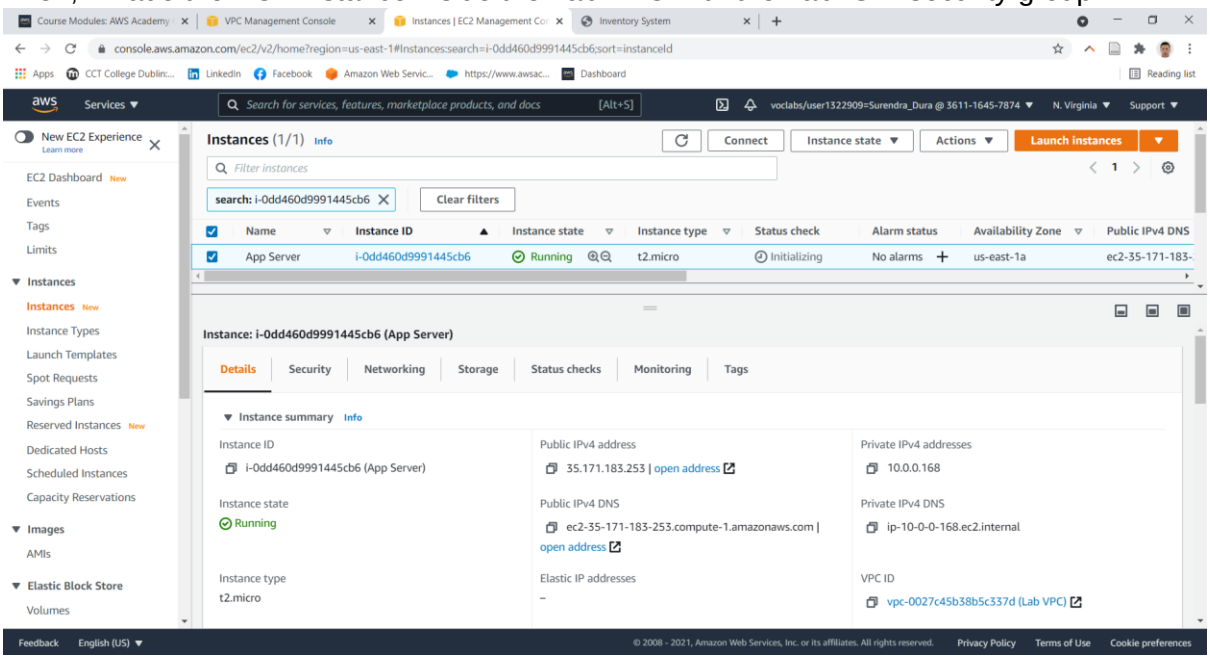
Then, I made the public route table for the lap VPC with the inbound route 0.0.0.0/0 and chose the public subnet.



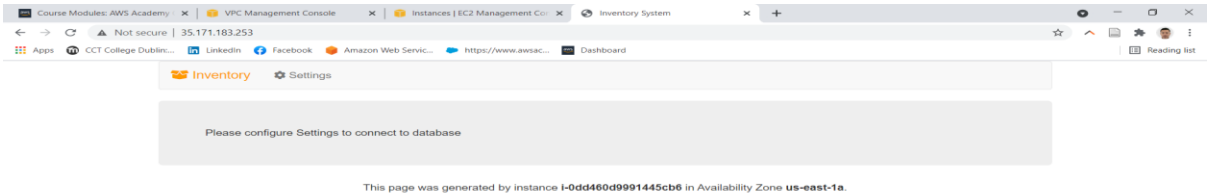
Then, I made a security group and add the inbound rule for the HTTP and HTTPs so that the traffic coming from the 0.0.0.0/0 will executed.



Then, I made the EC2 instance inside the Lab VPC with the Lab IGW security group.



With the help of the public IPv4 address of EC2 instance, I got the website running on it.

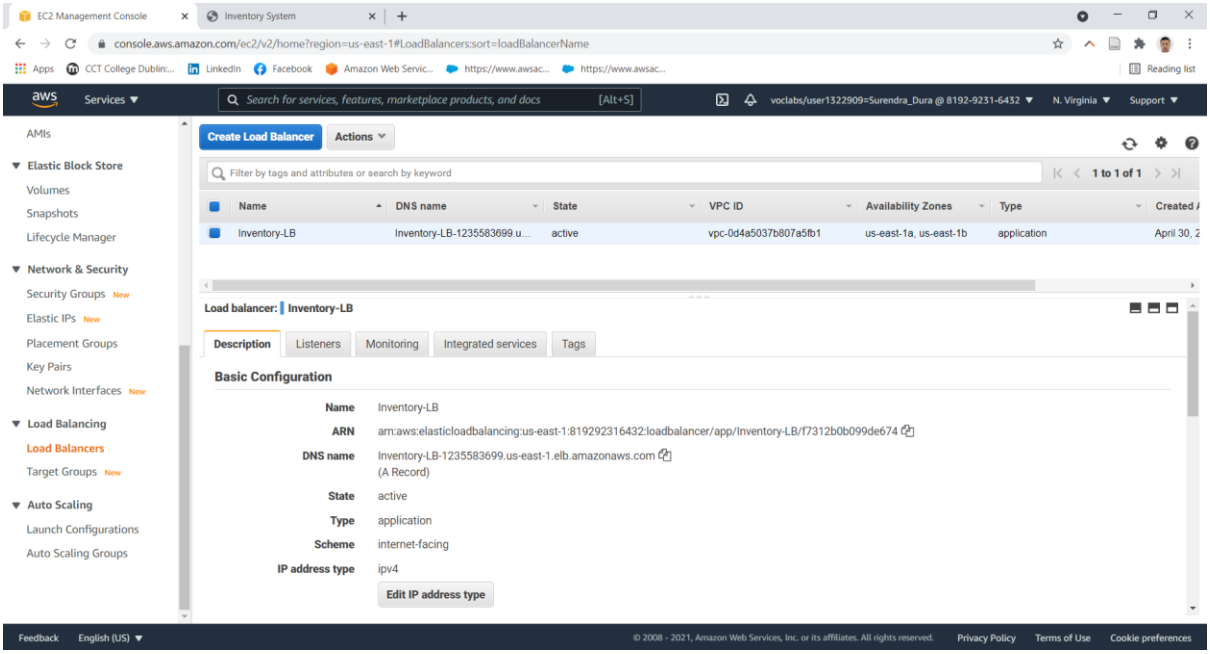


This process helps me to develop the VPC of the E-Health and how to secure the VPC with the internet. It also helps me to make a public and private subnet inside the VPC. Then, it helps me to make internet gateway and security group. Then, I help me to make an Amazon EC2 inside the VPC. This all are the requirement of the E-Health.

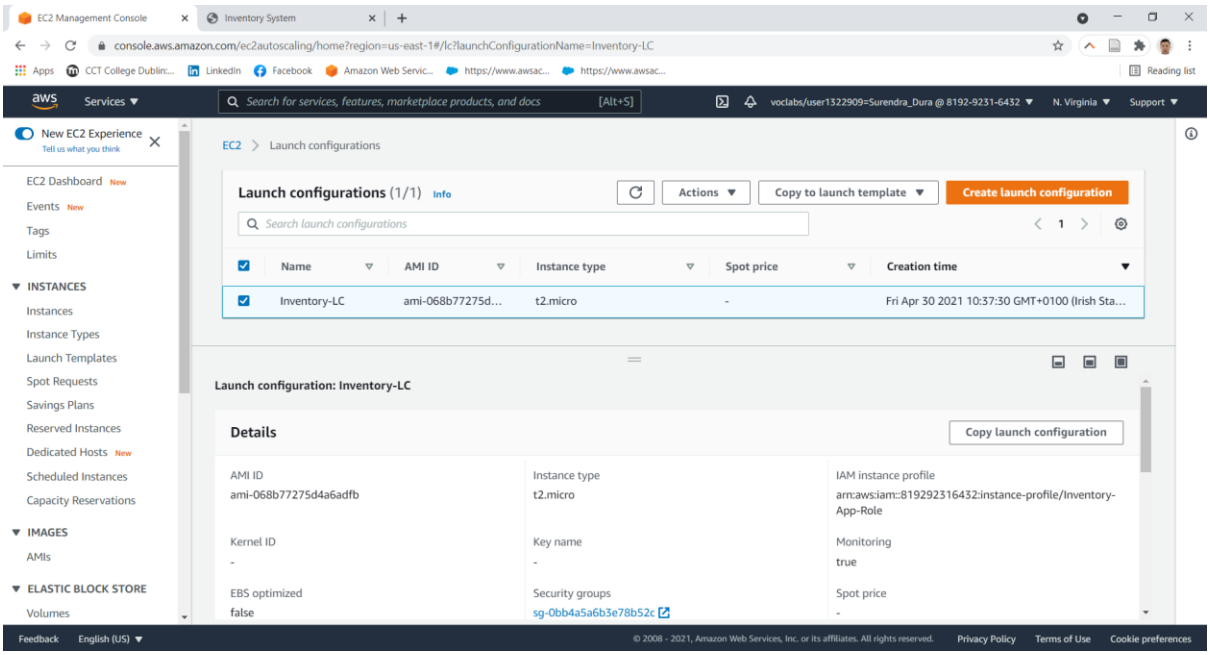
2. Creating a Highly Available Environment:

The E-Health application should be highly available in the Amazon Web Services so that in any failure the application will still be running in the environment.

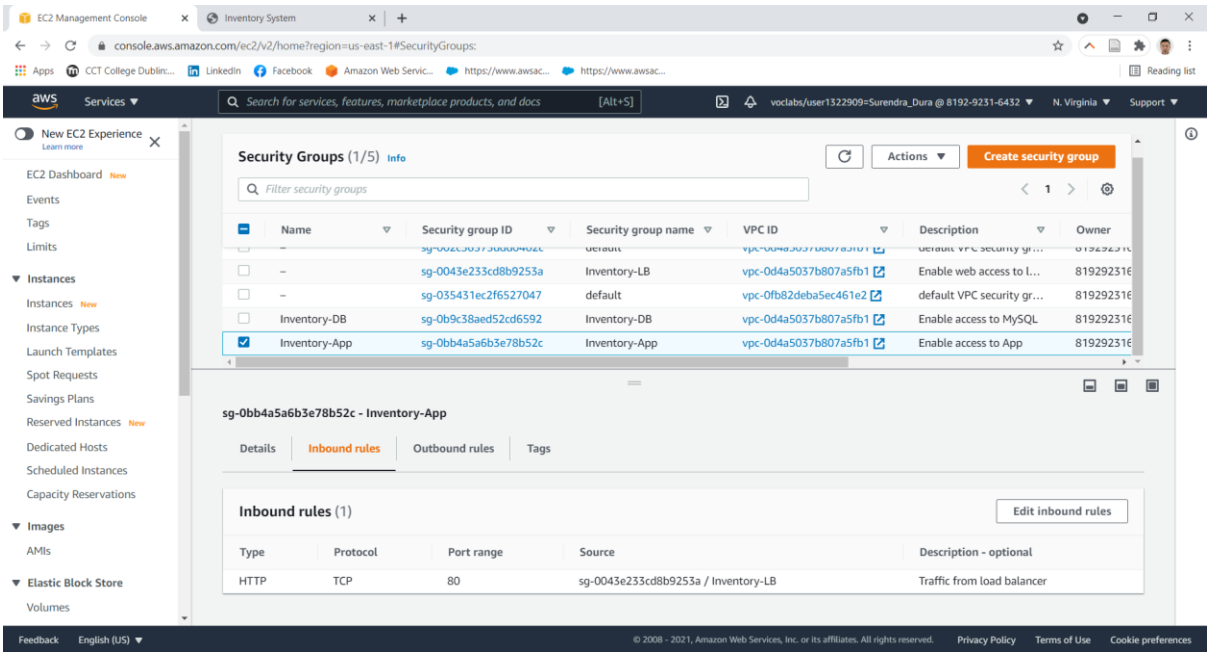
At first, I made VPC from the above process which I show you in the part 1. Then, I made an Application load balancer so that application will run in the multiple AZ and it also check the health of the application. The below picture shows the application load balancer.



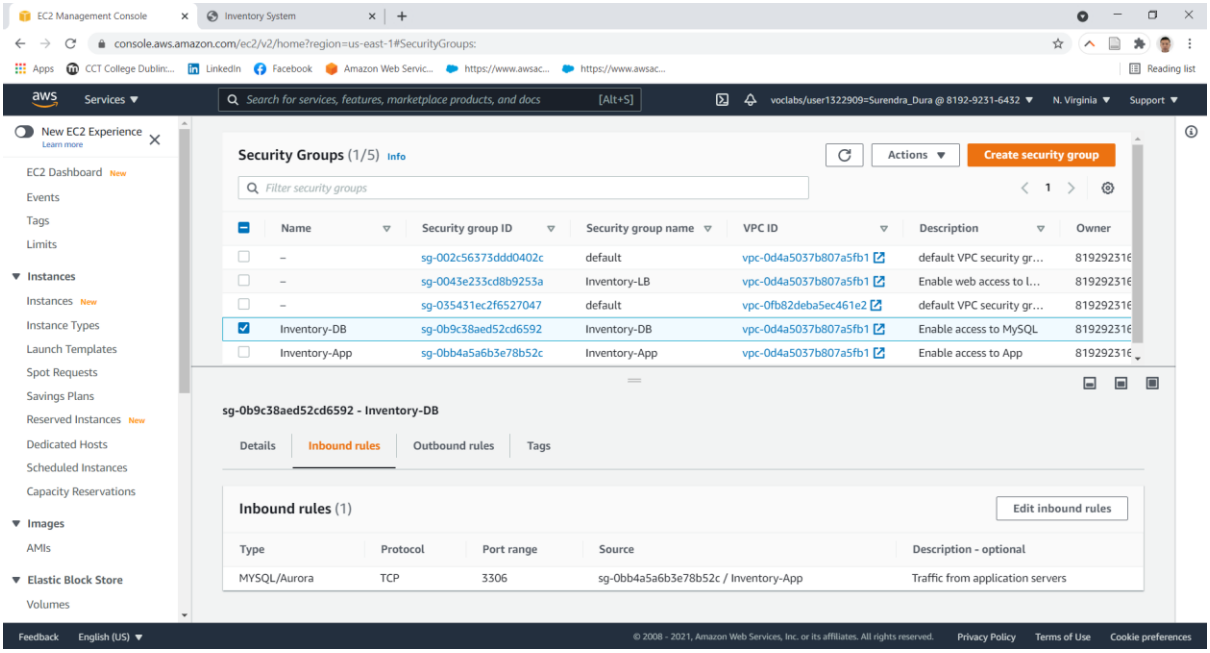
Then, I made an Amazon EC2 Auto Scaling group so that my EC2 instance can launch or terminate automatically. For that, First I made an image of the EC2 instance running in my server. Then, I made the Auto Scaling group which was show in the below picture.



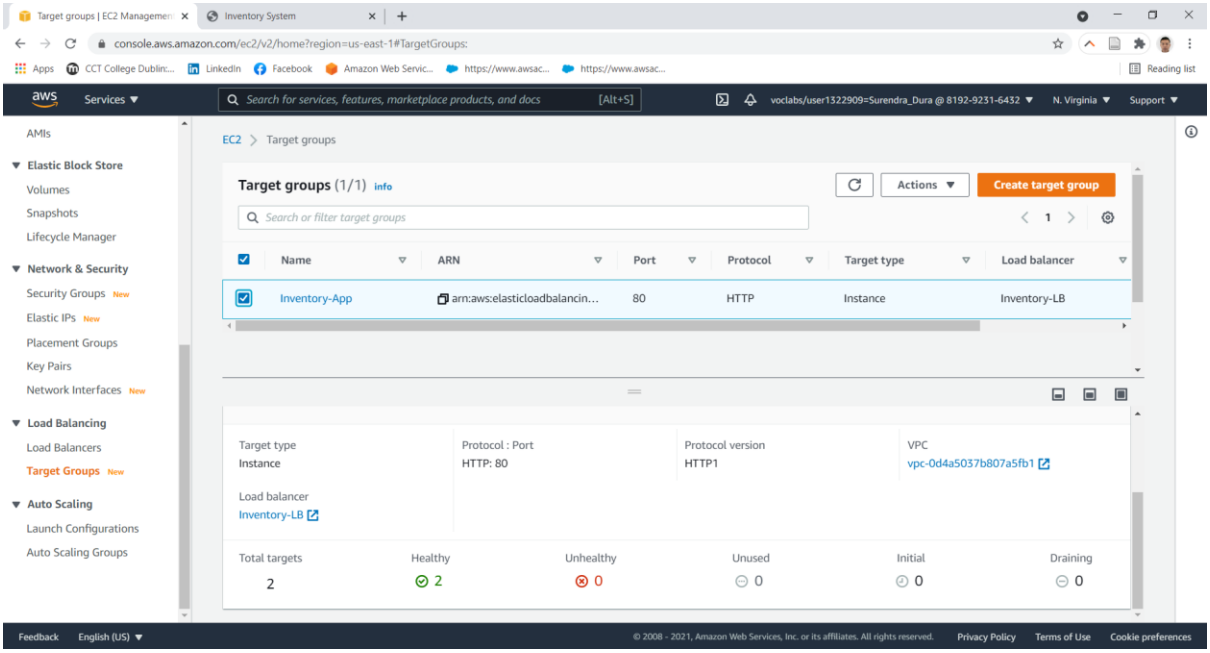
Now, I must make a security group for the three tier which are application Load balancer, application server and the Amazon RDS. So, First, I made a security group for the Application server so that the all the HTTP request coming from the application load balancer will performed automatically.



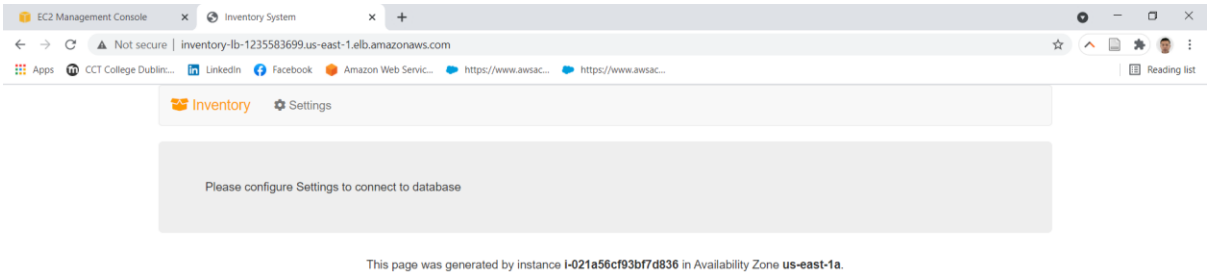
Then, I made the database security system so that only the traffic come from application server will performed.



Then, I check the application status so that the application health will be performed well.

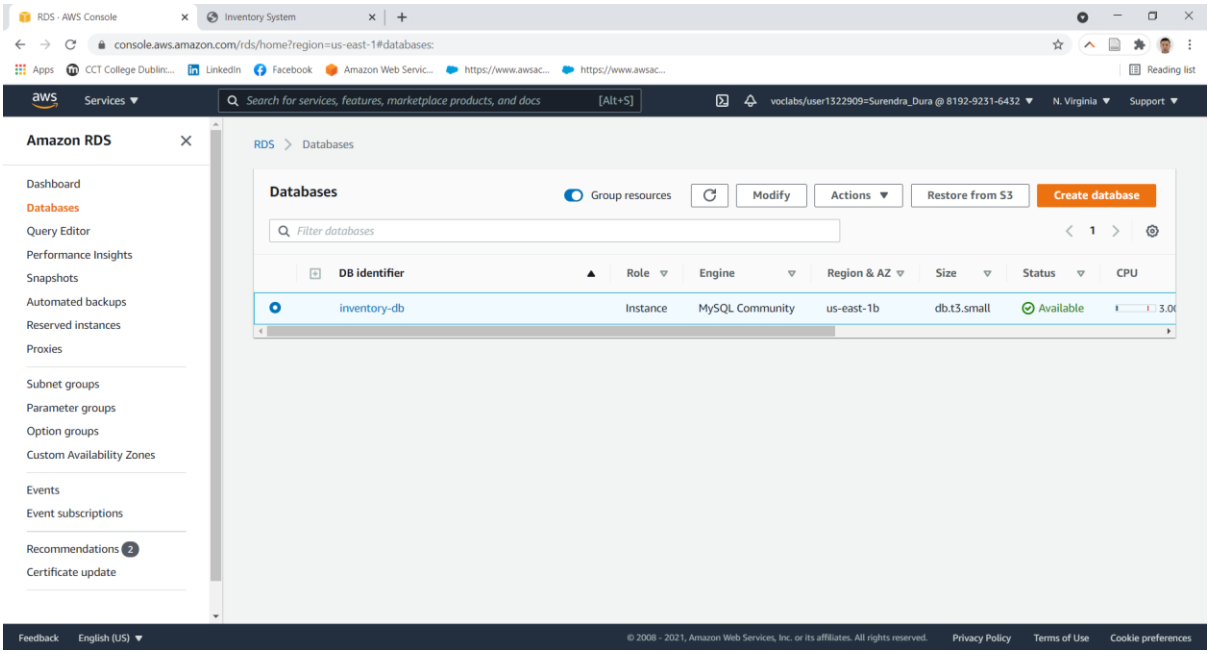


With the help of the DNS name inside the load balancer I can see that my application switch in the AZ.

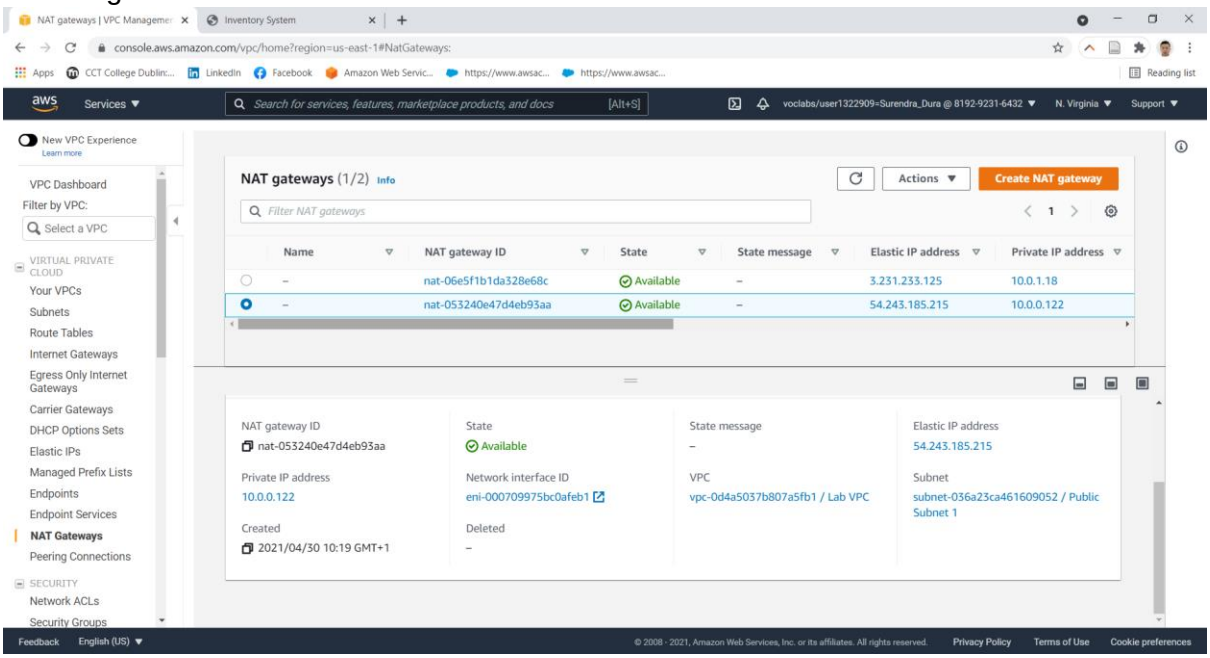


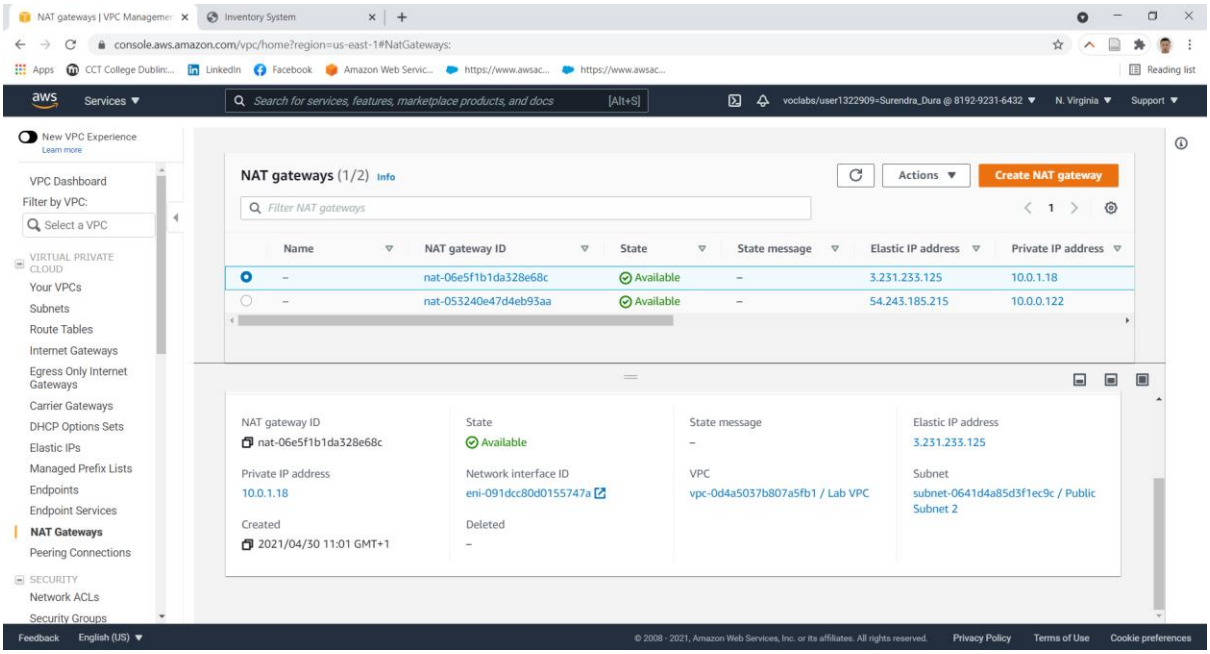
Then, I terminate my one of the EC2 instance, but the application is still running.

Then, I made my database high availability so that if the database crash in one AZ than Another AZ will performed.



Then, I made the NAT gateway high available so that if the NAT gateway present in one AZ does not work than the NAT gateway present in another AZ will perform so that we get internet all the time inside our AZ.



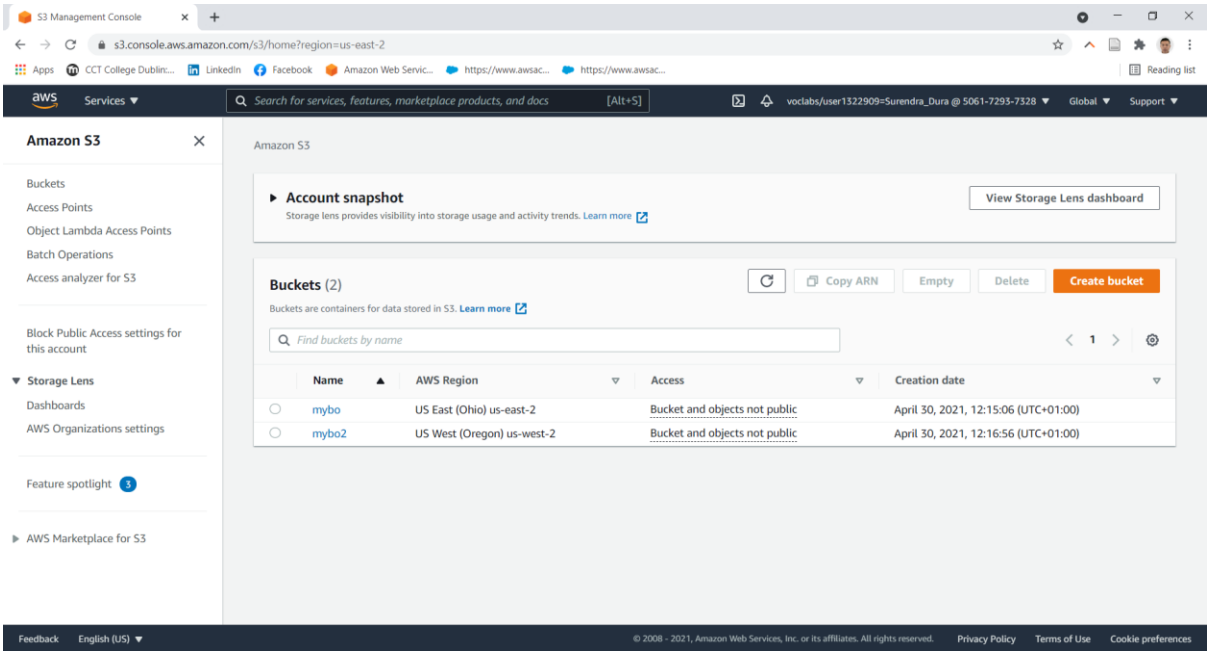


This service helps the E-Health application to be highly available and secure the system. And it also helps to develop the Application load balancer, Amazon EC2 Auto Scaling, and how to distribute the Nat gateway and database inside the two AZ.

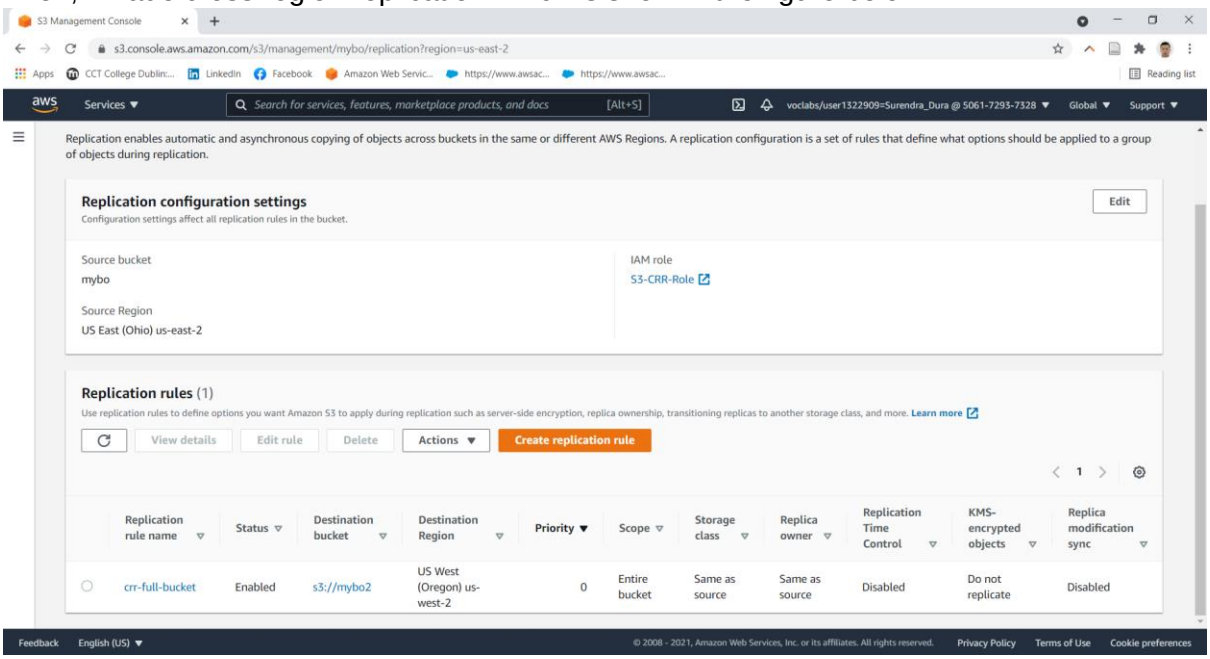
3. Hybrid Storage and AWS Storage Gateway File Gateway:

Hybrid storage and AWS Storage Gateway File Gateway help us to replicate the data into different region with the help of Amazon S3 so that our data will be recovery when the system fail in one region automatically.

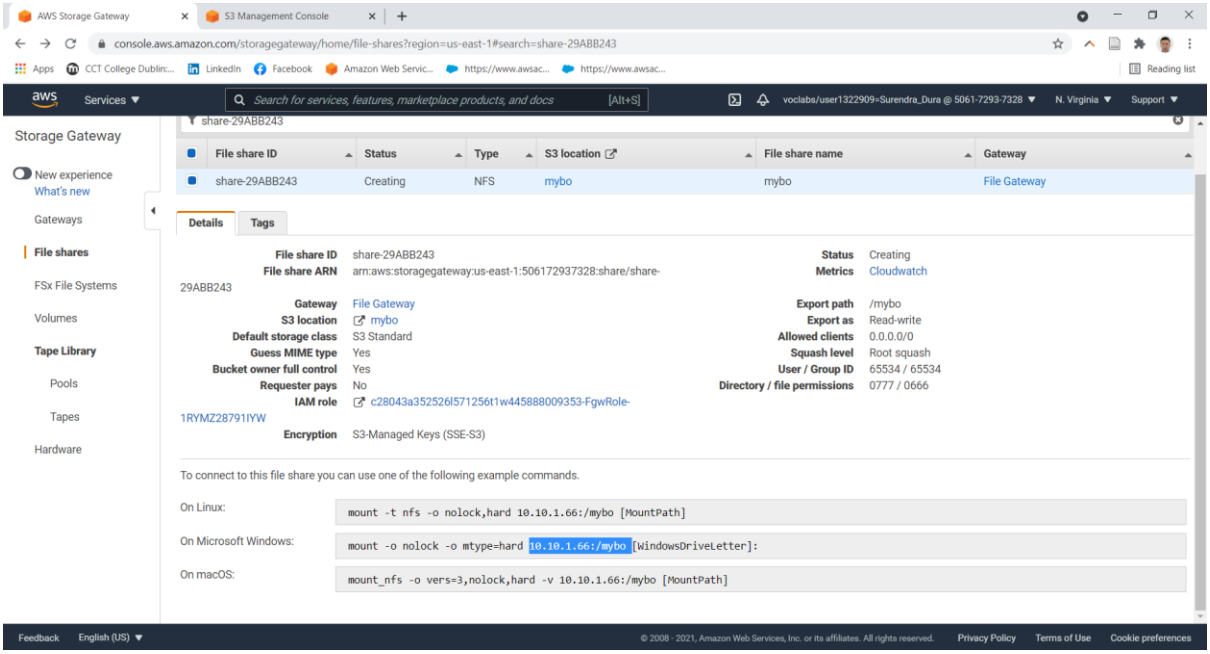
At first, I made the two S3 bucket in two different AWS regions.



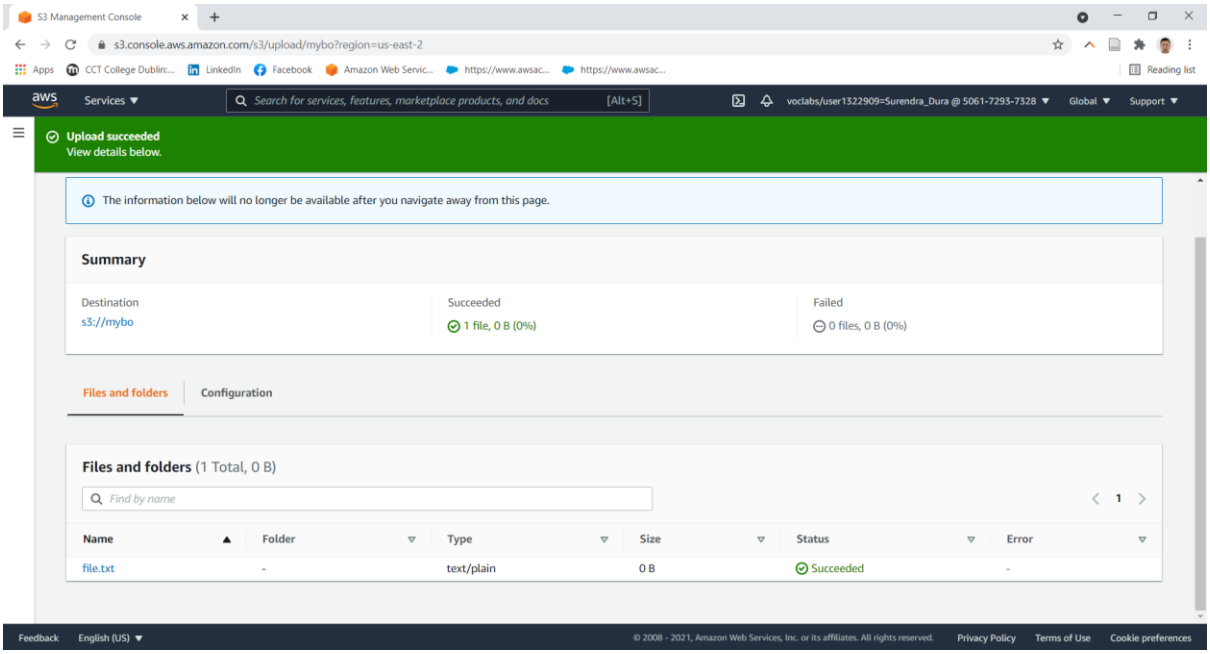
Then, I made cross region replication which is show in the figure below.

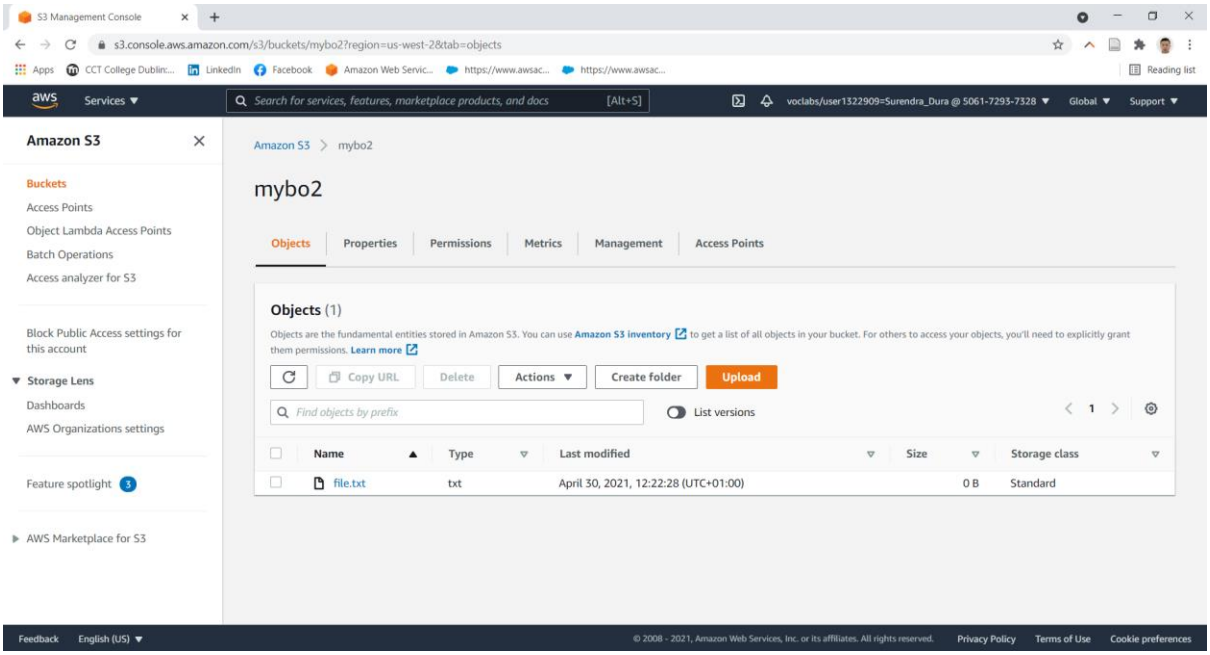


Then, I made the storage gateway in the different region.

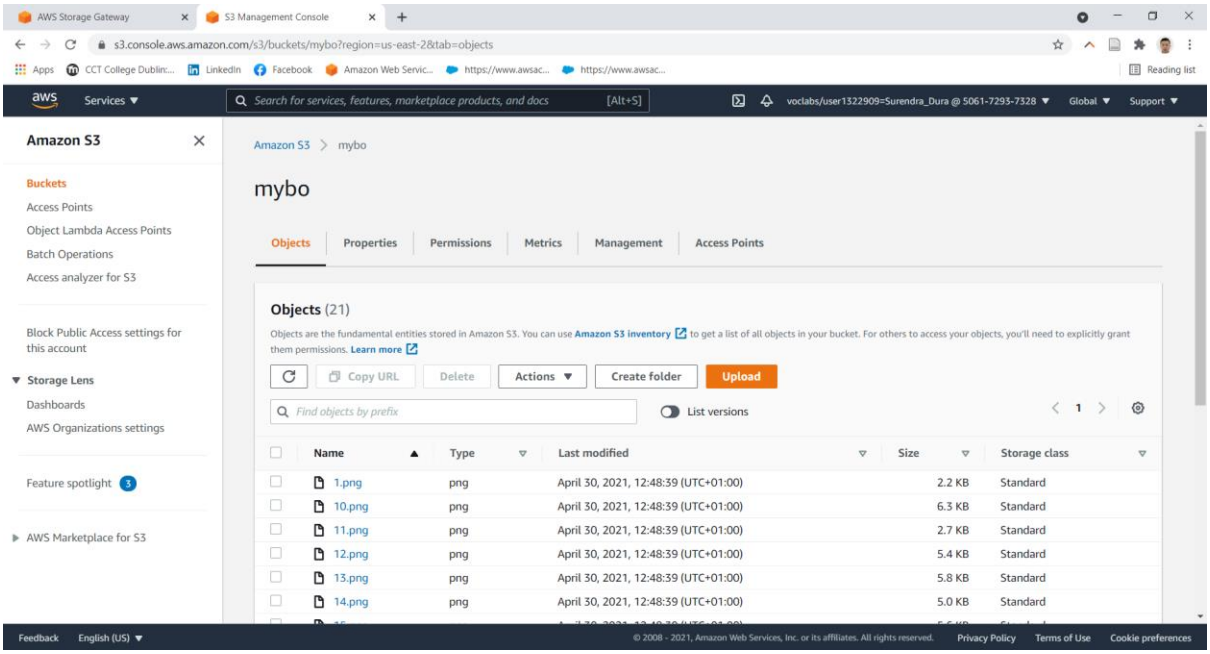


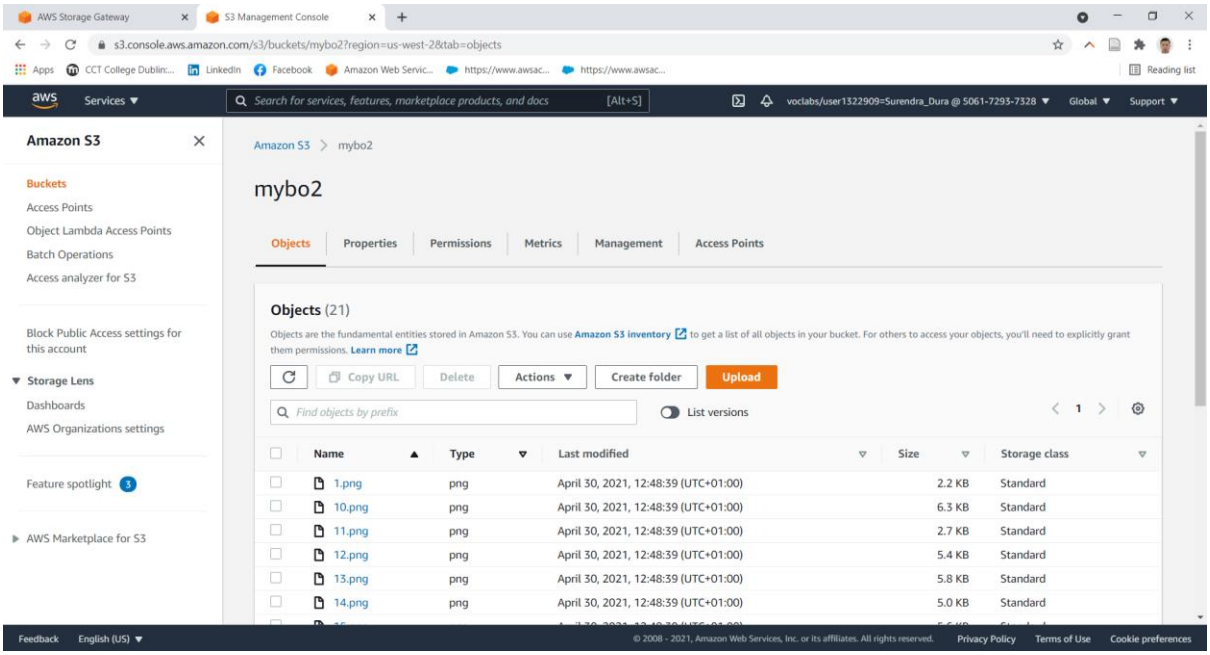
Then, I upload the document in one region, and it automatically replicated into another region.





Then, with the help of the EC2 Linux instance I mounted the file share and migrate to the data centres. And I can see the files in my both S3 bucket.





This process helps us to replicate our data in the region so that we can recovery our data if one of the regions did not work. This is the very important part for the E-health application.

All the service which I show above are done by the help of AWS Academy(*AWS Academy Cloud Architecting [2687]*, 2021).

TASK 4: AWS Key Management Service (AWS KMS):

AWS Key management service(Matt Kohrs, 2014) is very useful for the E-Health application because the application should have sensitive information of the patient so that the file should be encrypted, so that the information will not be leaked. AWS KMS help us to create a master key and then we can manage to define the user in the KMS who can access the key to do the encryption and decryption the file. The enable and disable help us to active and deactivate the key. So, we have all the power in the KMS to create, delete or store the keys.

The customer managed keys play the important role in the E-Health because customers are uploading document and images on the website, so which are the highly sensitive information. That is why the information should be encrypted and send to the related doctor which they like to send, and the related doctor can decrypt the document and access the document. So, it is very useful for the E-Health to secure the databases. So, AWS KMS give an extra security layer to the E-health application. On the other hand, doctor also send sensitive document to the patient so that document should be encrypted and give permission to related patient. So, it helps to secure the document from both sides.

References:

Amazon CloudWatch - Application and Infrastructure Monitoring (2021) *Amazon Web Services, Inc.* Available at: https://aws.amazon.com/cloudwatch/ (Accessed: 29 April 2021).

Amazon Cognito - Simple and Secure User Sign Up & Sign In | Amazon Web Services (AWS) (2021) *Amazon Web Services, Inc.* Available at: https://aws.amazon.com/cognito/ (Accessed: 29 April 2021).

Amazon EC2 Auto Scaling (2021). Available at: https://aws.amazon.com/ec2/autoscaling/ (Accessed: 29 April 2021).

Amazon Elastic Block Store (EBS) - Amazon Web Services (2021) *Amazon Web Services, Inc.* Available at: https://aws.amazon.com/ebs/ (Accessed: 29 April 2021).

Amazon ElastiCache for Memcached (2021) *Amazon Web Services, Inc.* Available at: https://aws.amazon.com/elasticache/memcached/ (Accessed: 29 April 2021).

Amazon RDS | Cloud Relational Database | Amazon Web Services (2021) *Amazon Web Services, Inc.* Available at: https://aws.amazon.com/rds/ (Accessed: 29 April 2021).

Amazon Route 53 - Amazon Web Services (2021). Available at: https://aws.amazon.com/route53/ (Accessed: 29 April 2021).

Amazon Virtual Private Cloud (VPC) (2021) *Amazon Web Services, Inc.* Available at: https://aws.amazon.com/vpc/ (Accessed: 29 April 2021).

AWS Academy Cloud Architecting [2687] (2021). Available at: https://awsacademy.instructure.com/courses/2687 (Accessed: 30 April 2021).

AWS CloudFormation - Infrastructure as Code & AWS Resource Provisioning (2021) *Amazon Web Services, Inc.* Available at: https://aws.amazon.com/cloudformation/ (Accessed: 29 April 2021).

AWS Storage Gateway | Amazon Web Services (2021) *Amazon Web Services, Inc.* Available at: https://aws.amazon.com/storagegateway/ (Accessed: 29 April 2021).

Cloud Security, Identity, and Compliance Products – Amazon Web Services (AWS) (2021) *Amazon Web Services, Inc.* Available at: https://aws.amazon.com/products/developer-tools/ (Accessed: 29 April 2021).

Global Infrastructure Regions & AZs (2021) *Amazon Web Services, Inc.* Available at: https://aws.amazon.com/about-aws/global-infrastructure/regions_az/ (Accessed: 29 April 2021).

Key Management Service - Amazon Web Services (AWS) (2021) *Amazon Web Services, Inc.* Available at: https://aws.amazon.com/kms/ (Accessed: 29 April 2021).

Matt Kohrs (2014) *Getting Started with AWS Key Management Service*. Available at: https://www.youtube.com/watch?v=-5MPXHvKDnc (Accessed: 29 April 2021).

NAT gateways - Amazon Virtual Private Cloud (2021). Available at: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html (Accessed: 29 April 2021).

What is Amazon EC2? - Amazon Elastic Compute Cloud (2021). Available at: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html (Accessed: 29 April 2021).

What is Amazon Elastic File System? - Amazon Elastic File System (2021). Available at: https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html (Accessed: 29 April 2021).

What is an Application Load Balancer? - Elastic Load Balancing (2021). Available at: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html (Accessed: 29 April 2021).