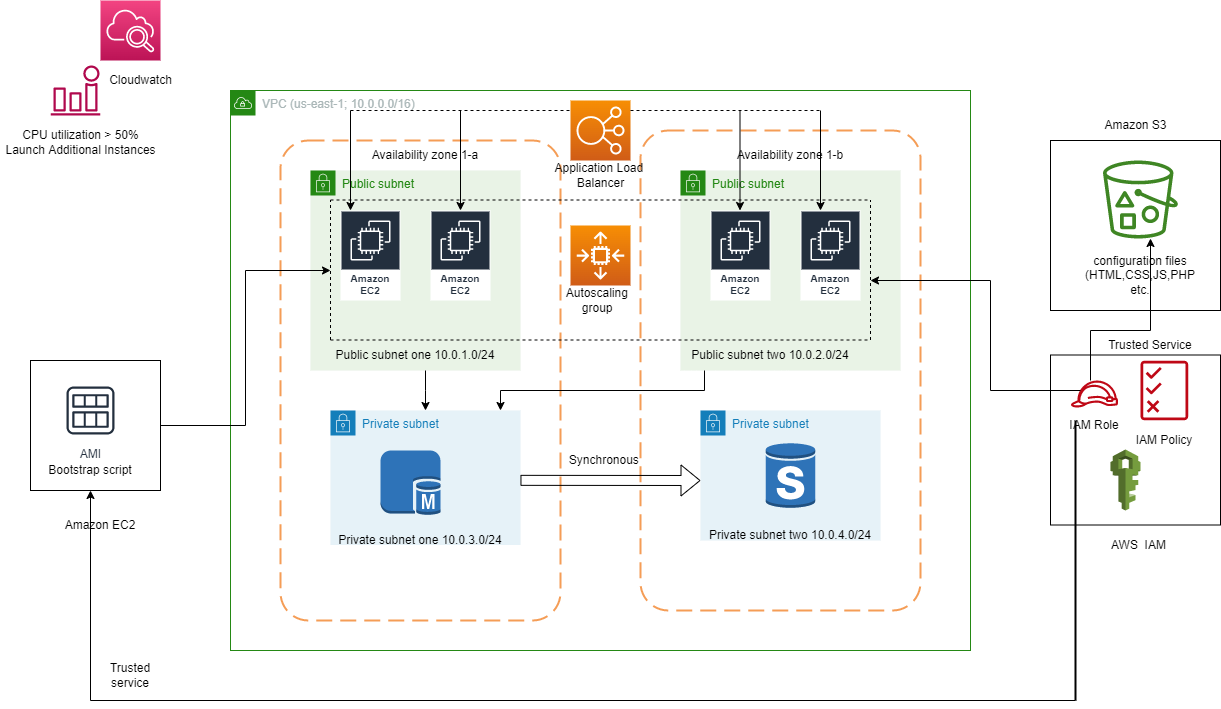
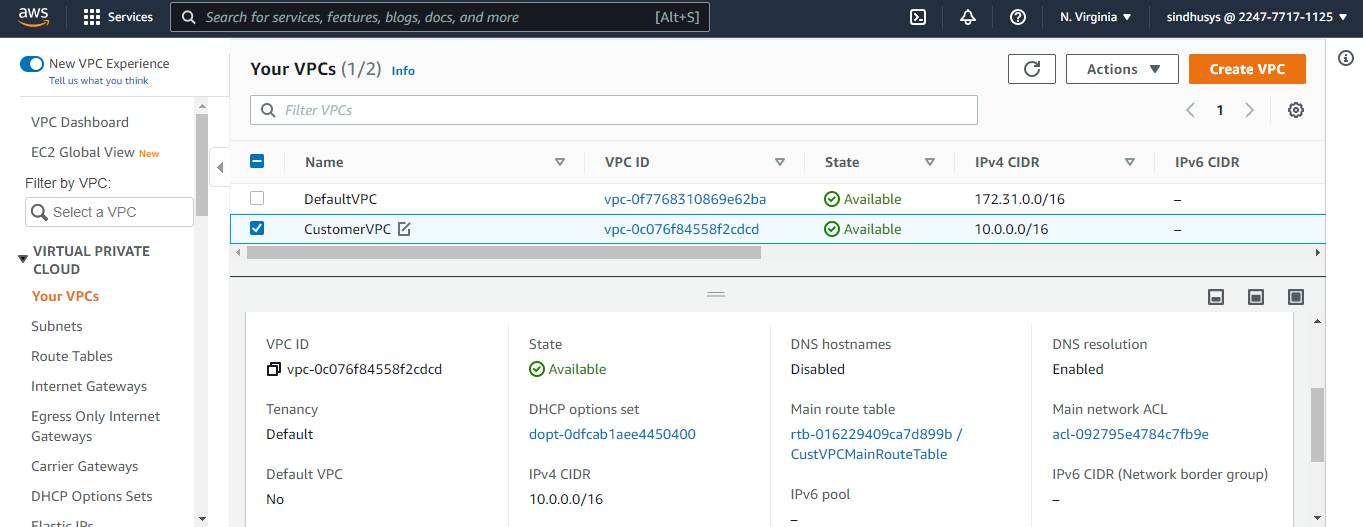
Working Diagram:

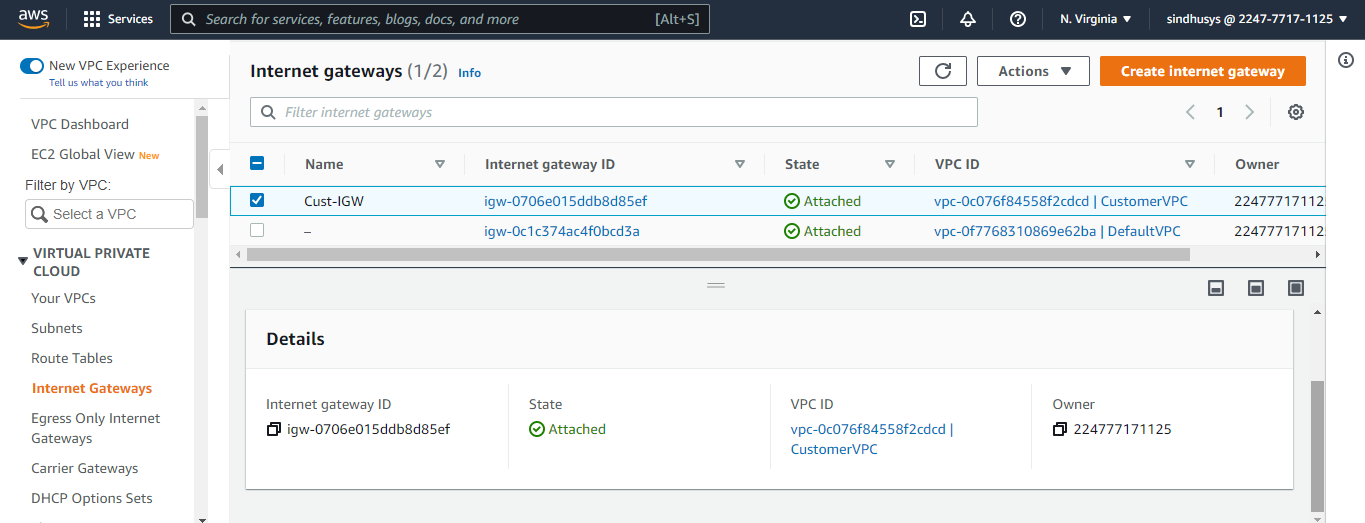


Step 1:

1. Create VPC: CustomerVPC with a new CIDR block 10.0.0.0/16:

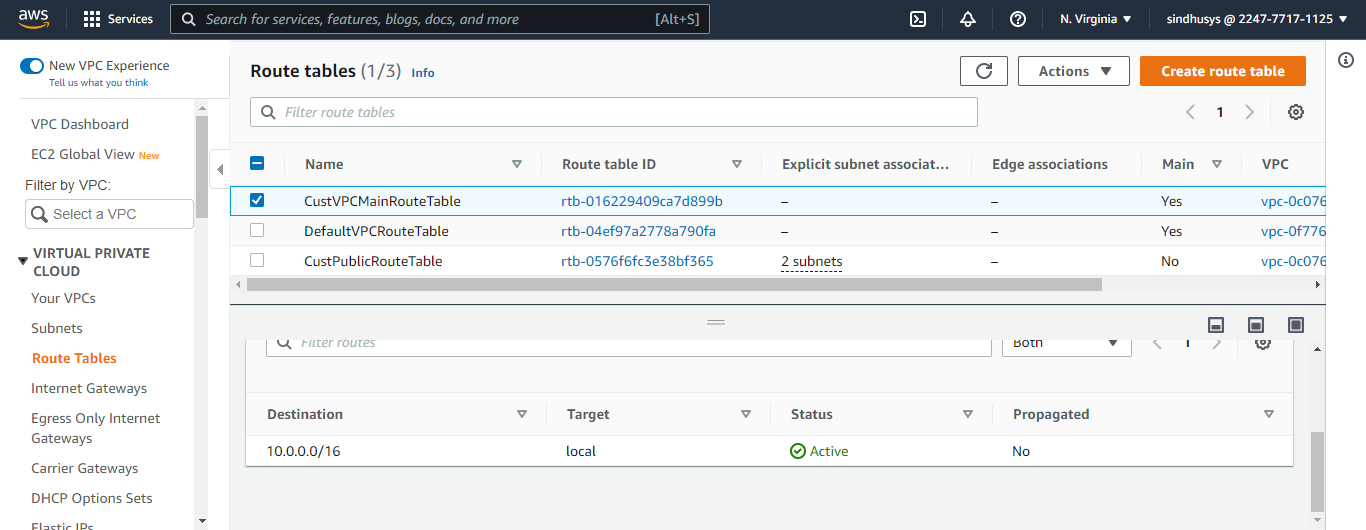


1. Create Internet Gateway (IGW) and attach the CustomerVPC to it:

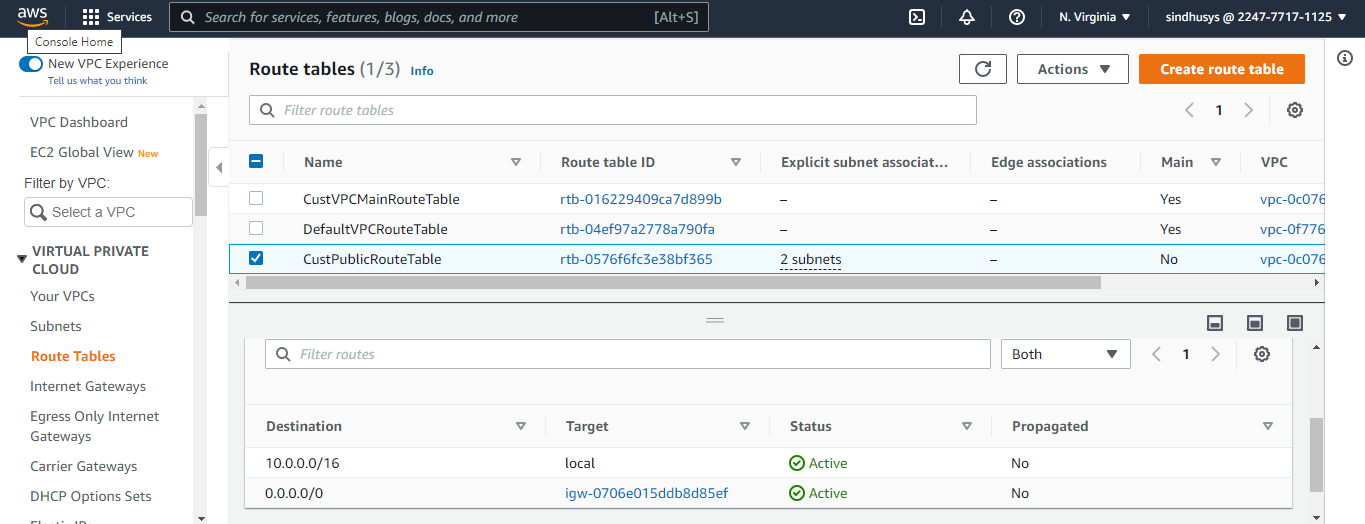


1. Create Public RouteTable and add public route (0.0.0.0/0) attached with IGW to it:

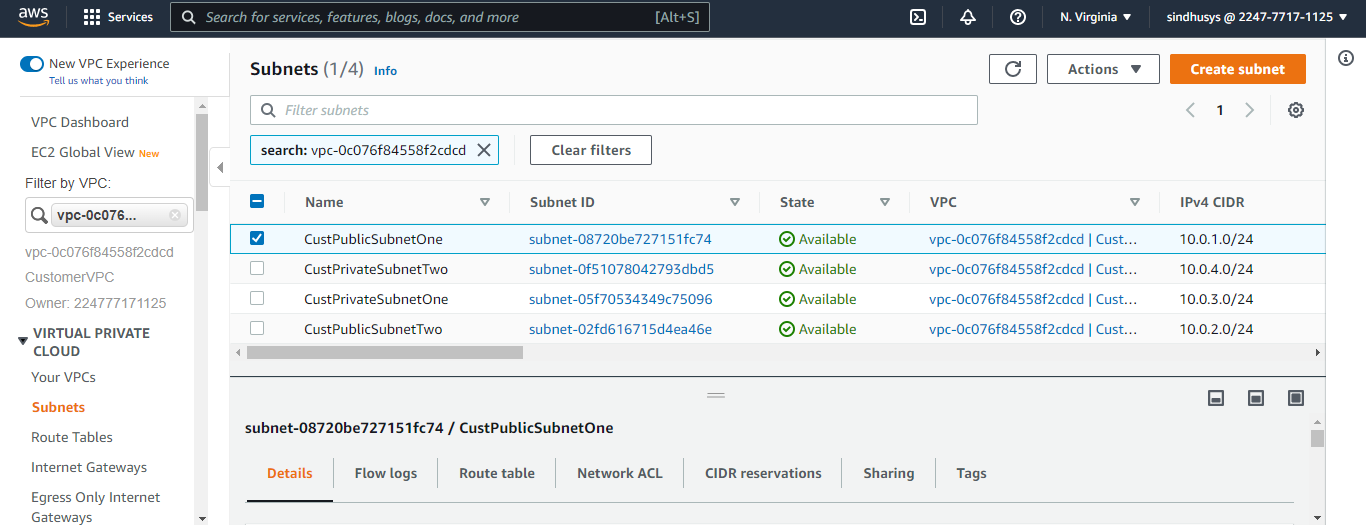
MainRouteTable is created by default:



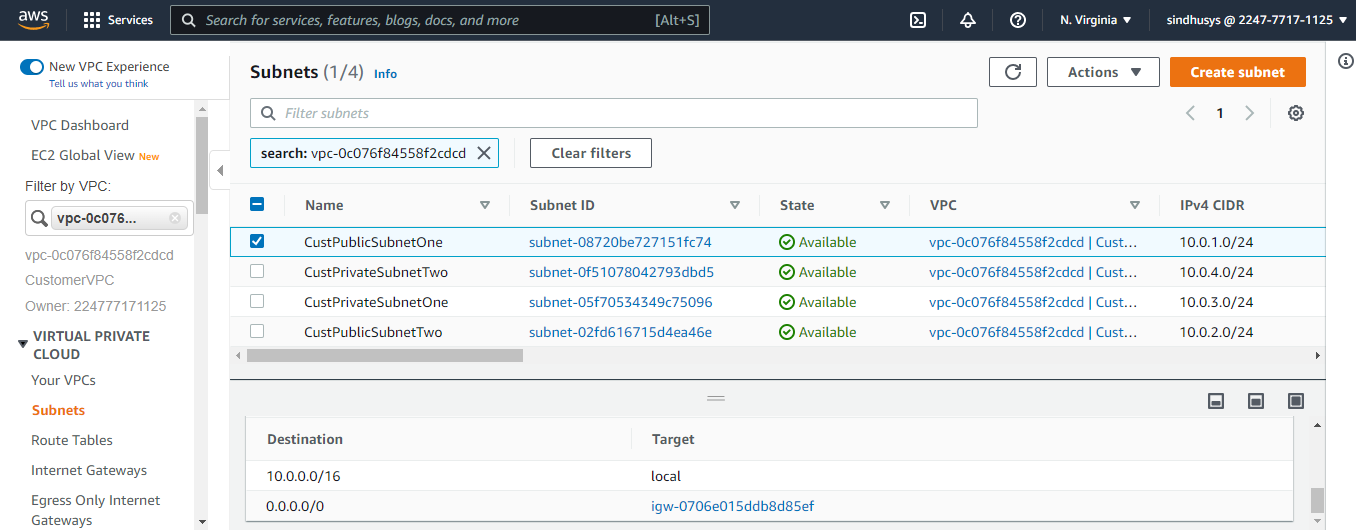
PublicRouteTable:

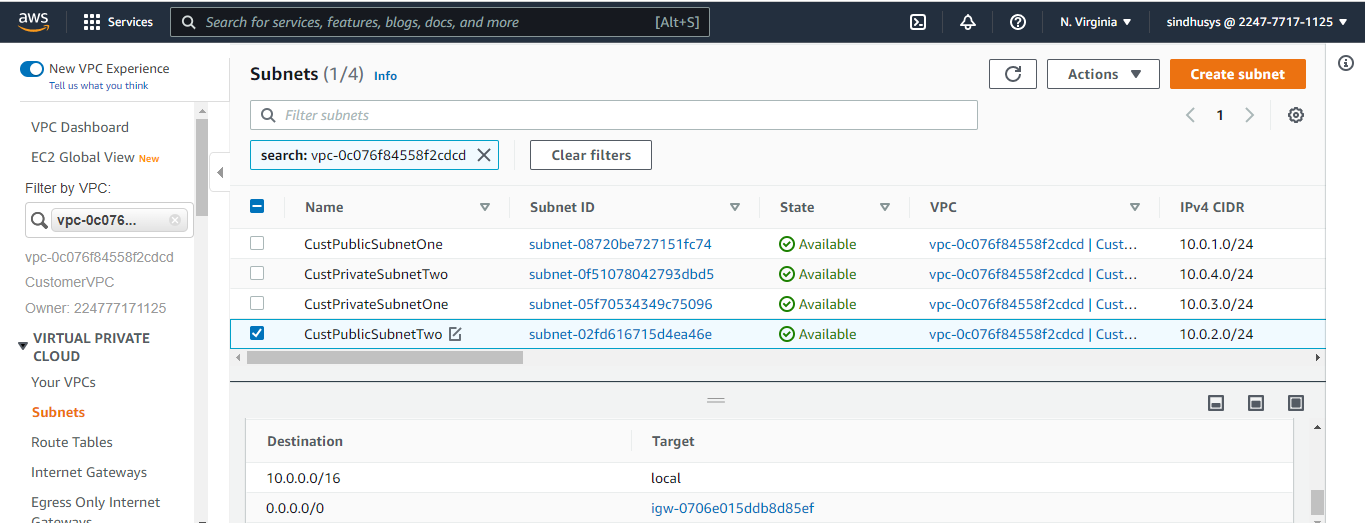


1. Create Public subnets and Private Subnets in different availability zone. The subnets are by default attached to MainRouteTable. Add PublicRouteTable to the public subnets.

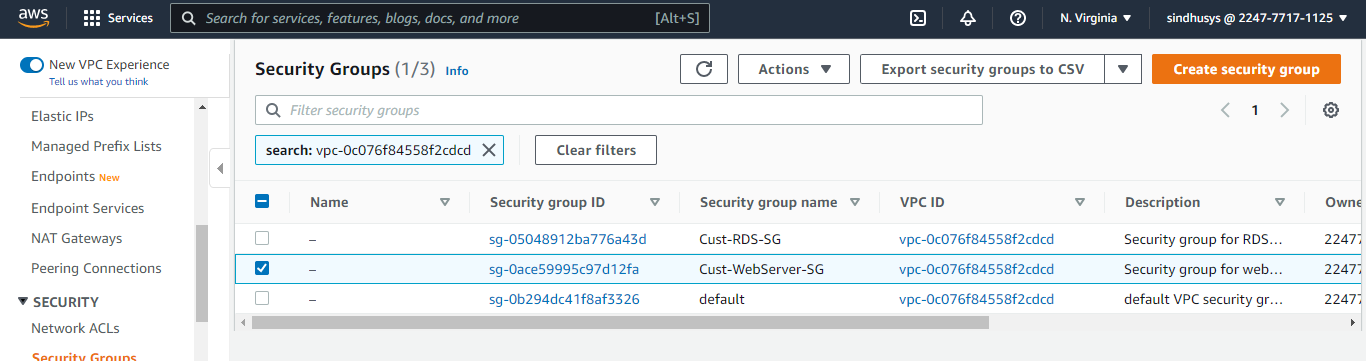


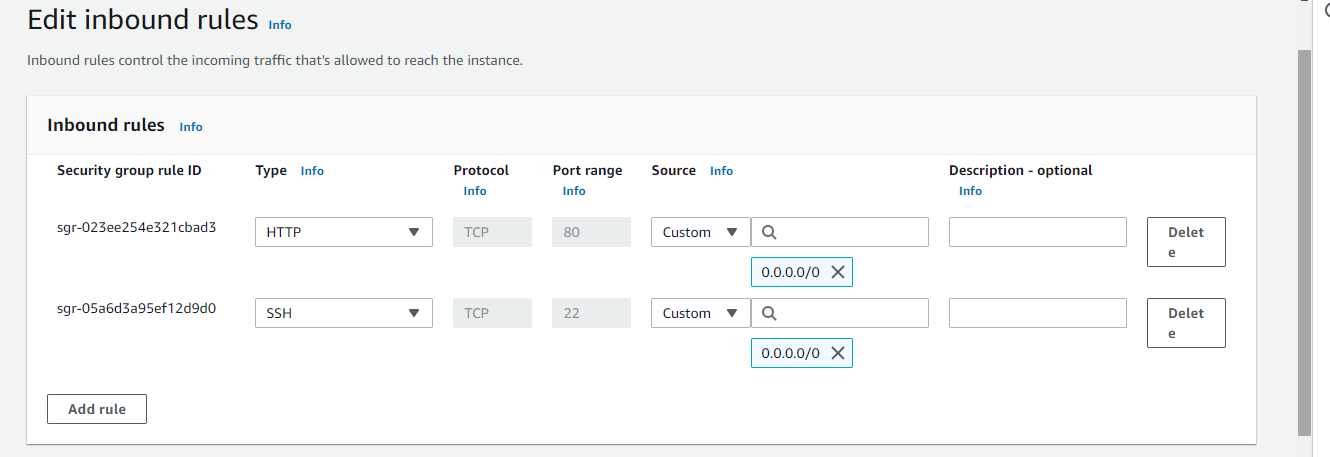
Associate public RT to public subnets:

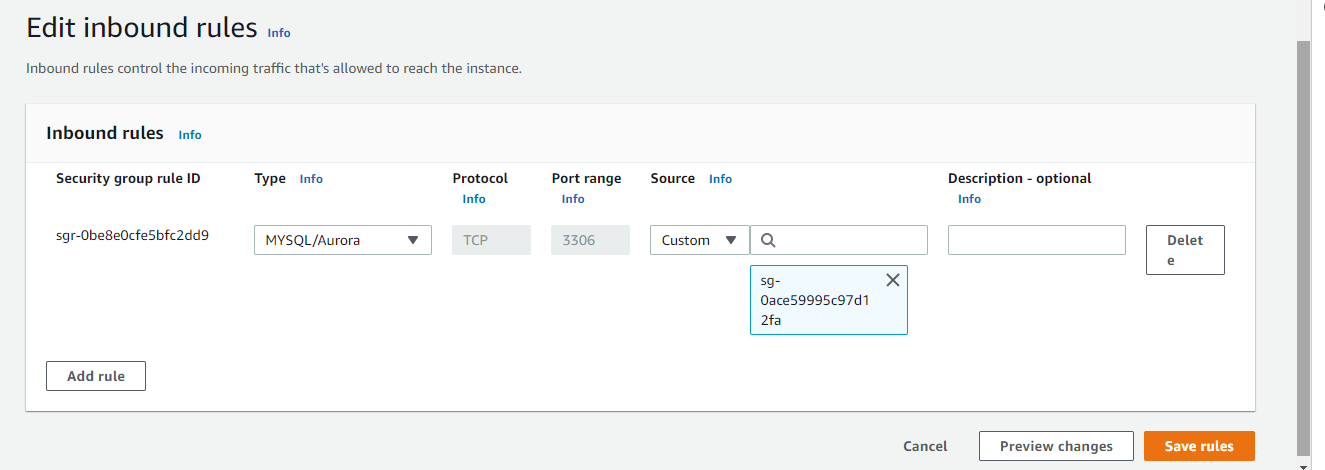




1. Create security group, one for the web server in public subnets and the other for RDS Database in private subnets:

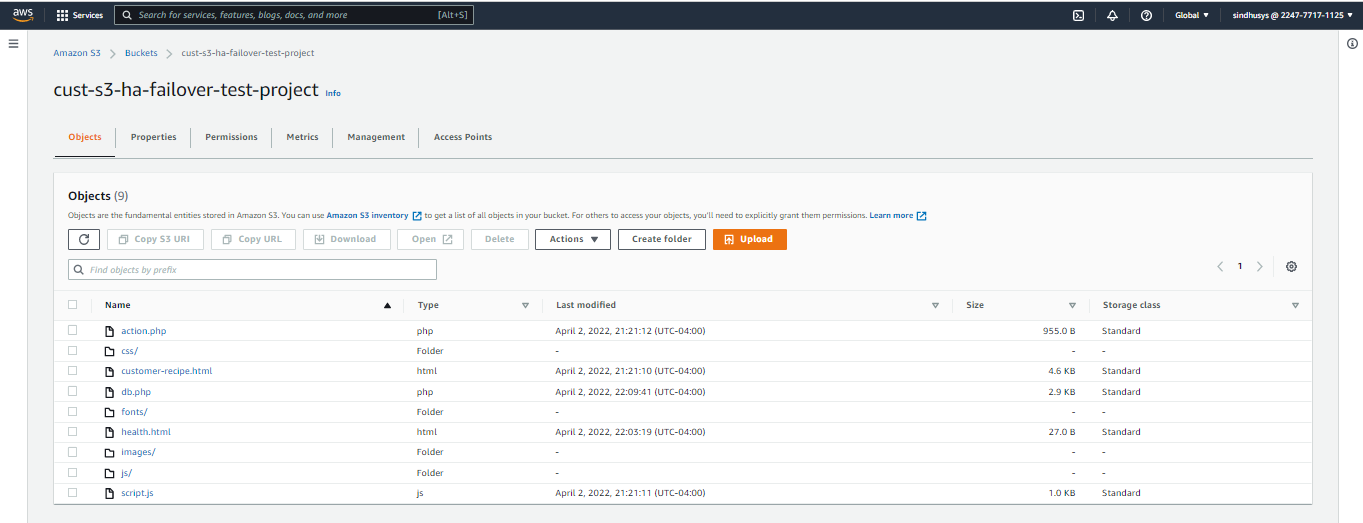






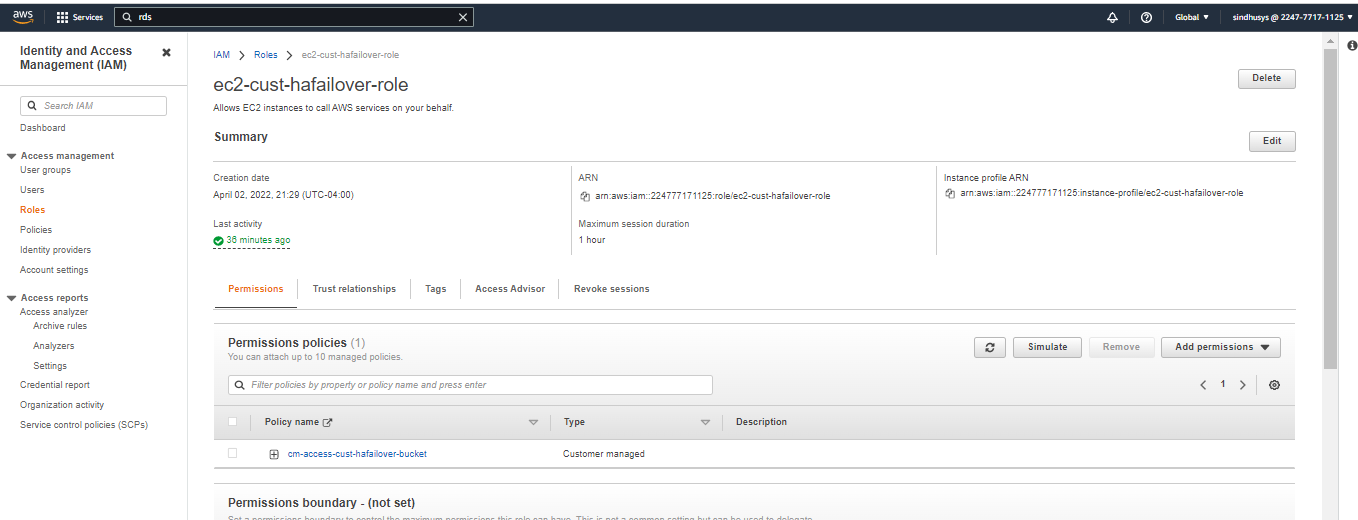
Step2:

1. Create s3 bucket i.e. cust-s3-ha-failover-project and upload the configuration files :



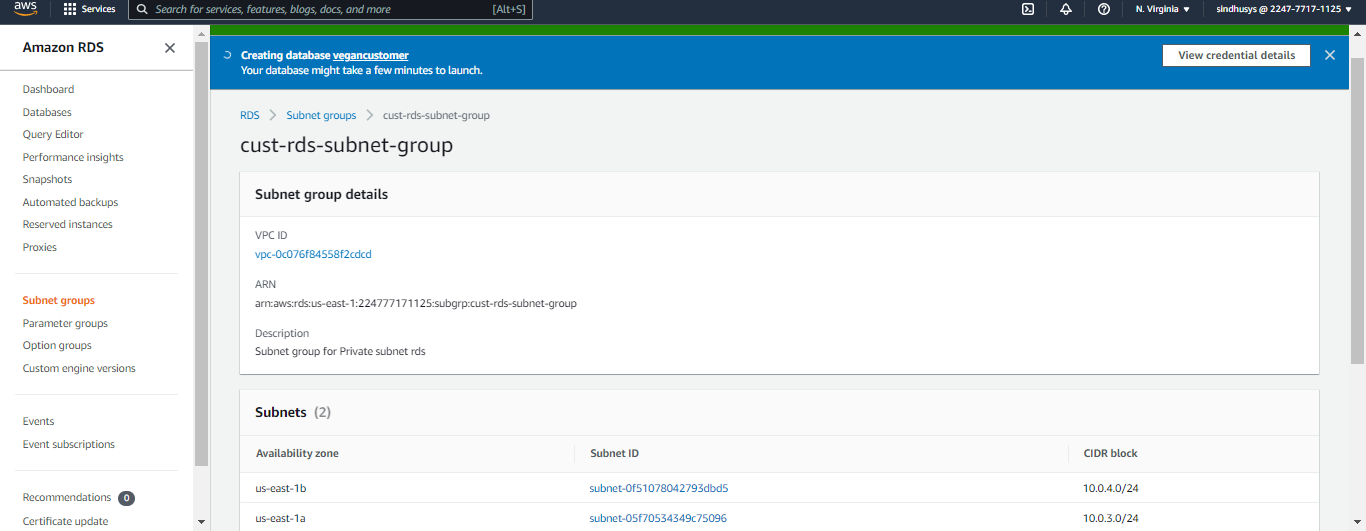
Step 3:

1. Create IAM Policy and attach it to the role I.e.) ec2-cust-hafailover-role:

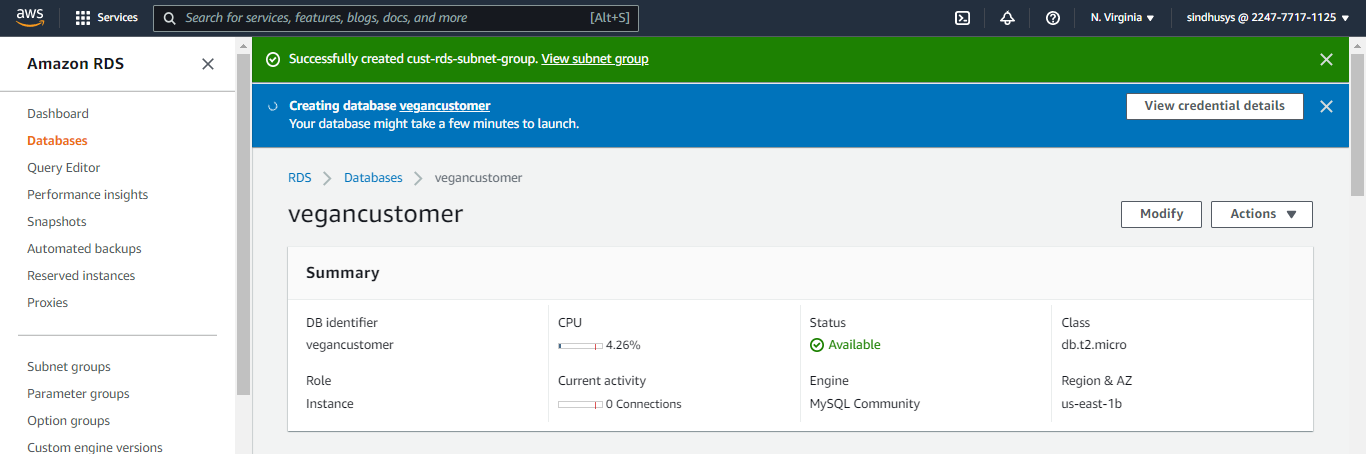


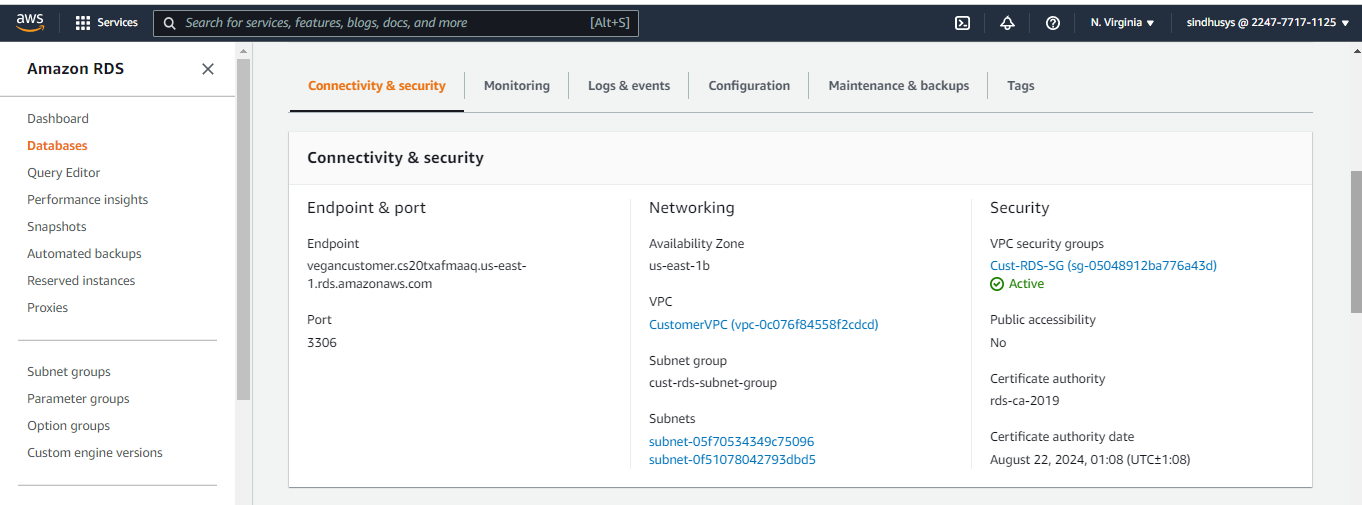
Step 4:

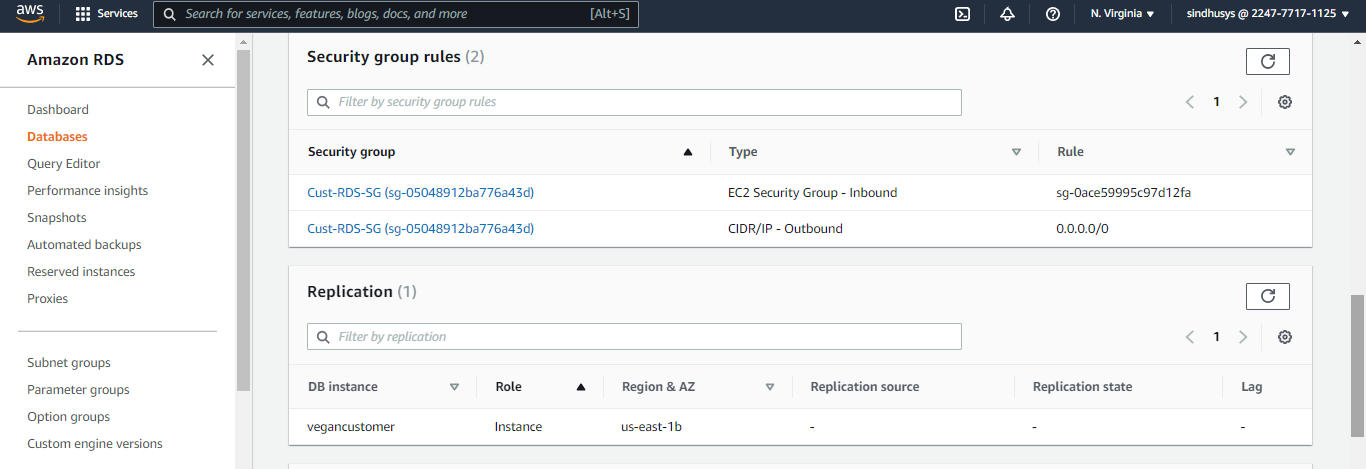
1. Create subnet group with two private subnets, MYSQL RDS DB in DEV/TEST environment with multiAZ capability, instance type t2.micro, storage SSD 20gb, Backup Retention- 1 day and disable enhanced monitoring. Note down the dB endpoint, dB name, username, password for future use.
2. Create Subnet group:



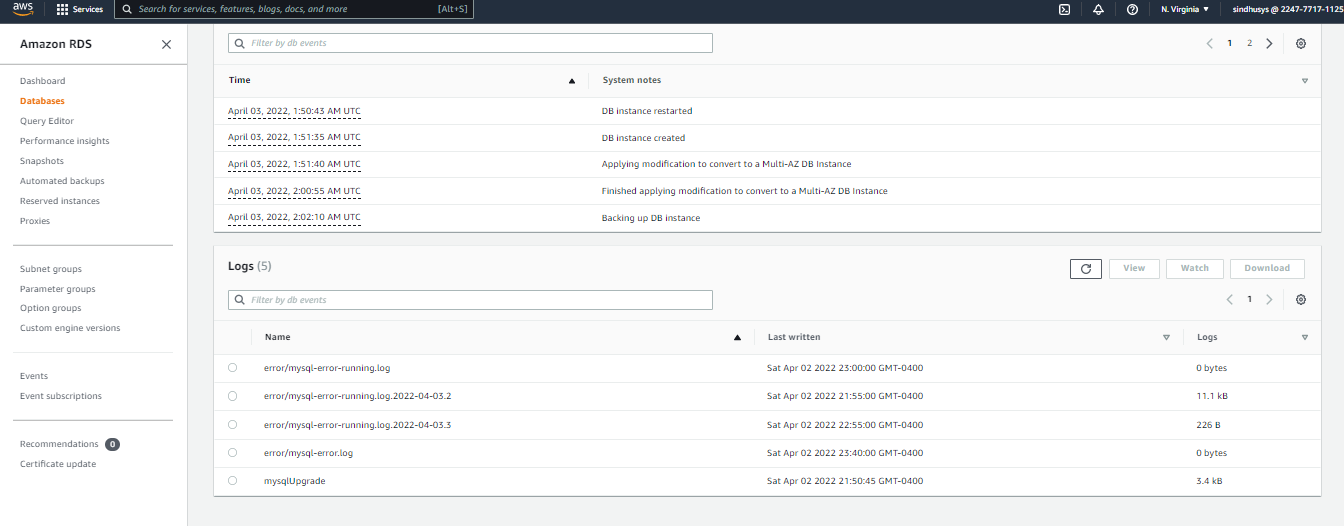
1. Create dB:

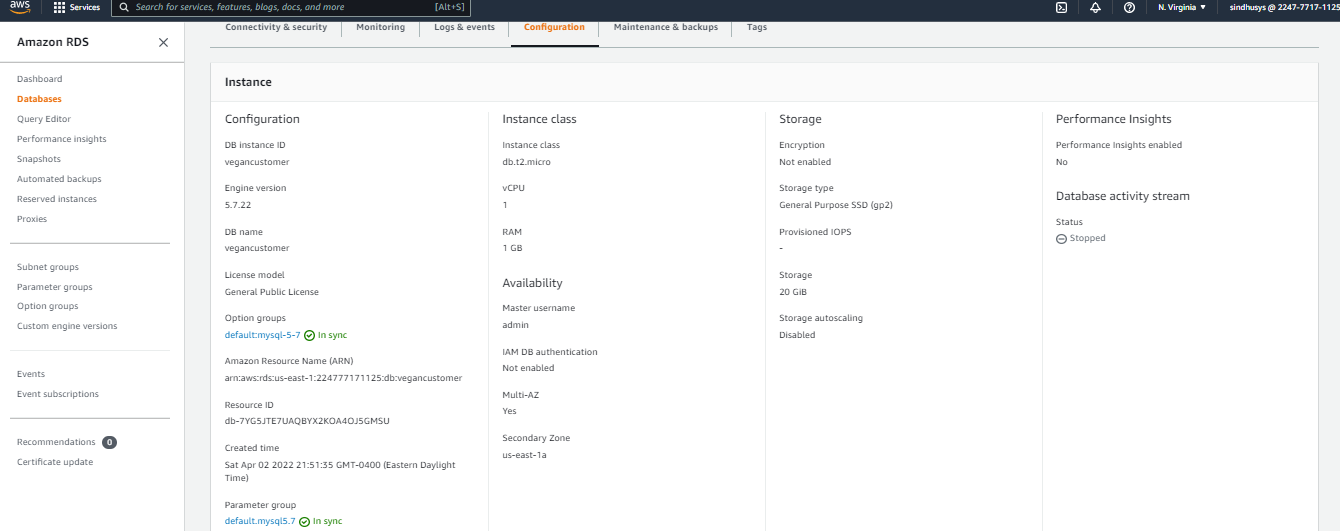






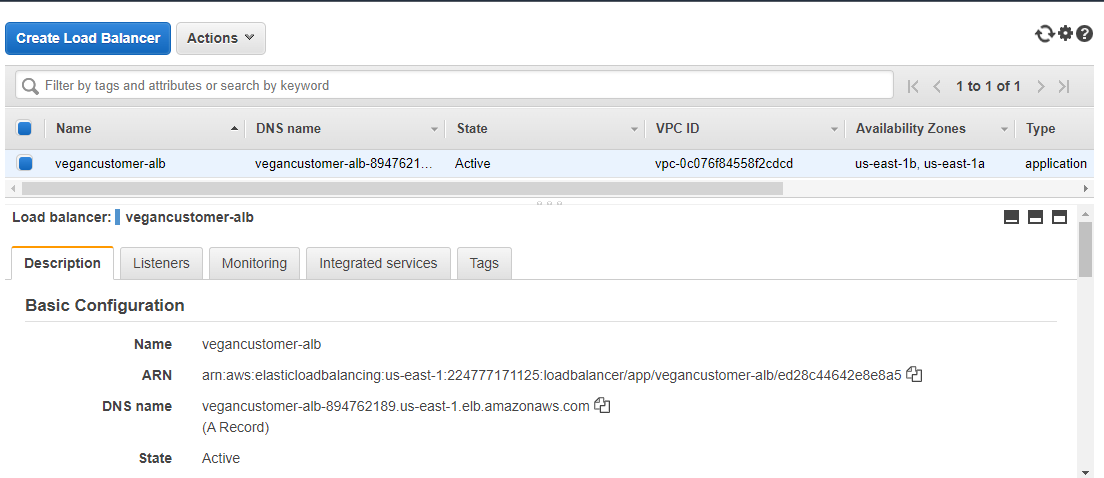
Once dB created, check the Log&events and configuration:



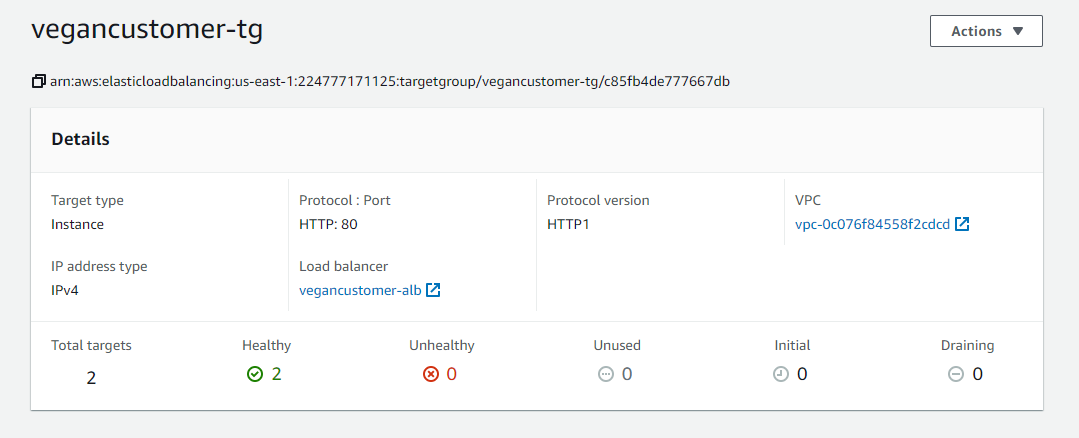


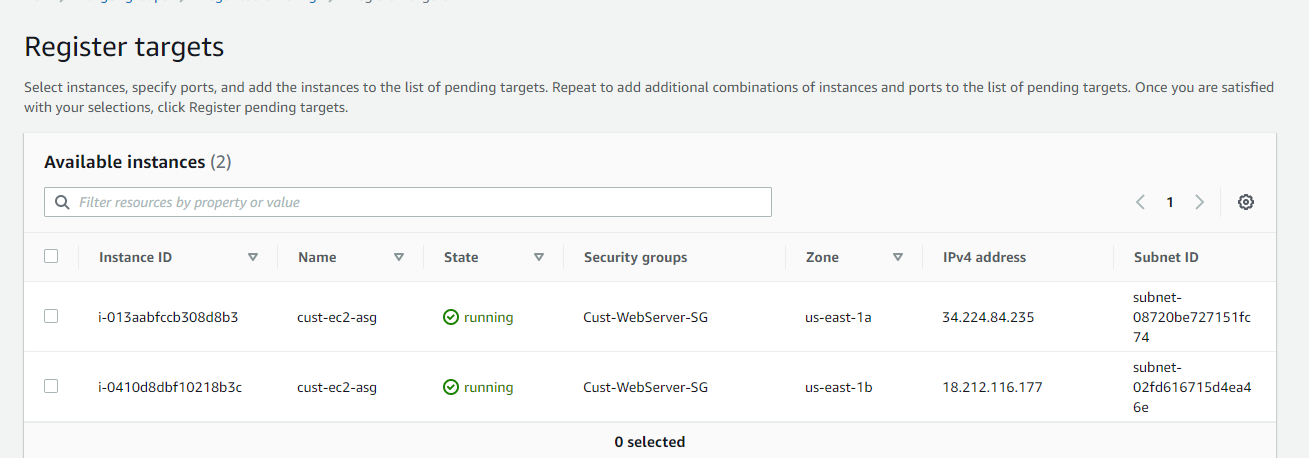
Step 5:

1. Create target group and ALB and configure health checks /health.html:



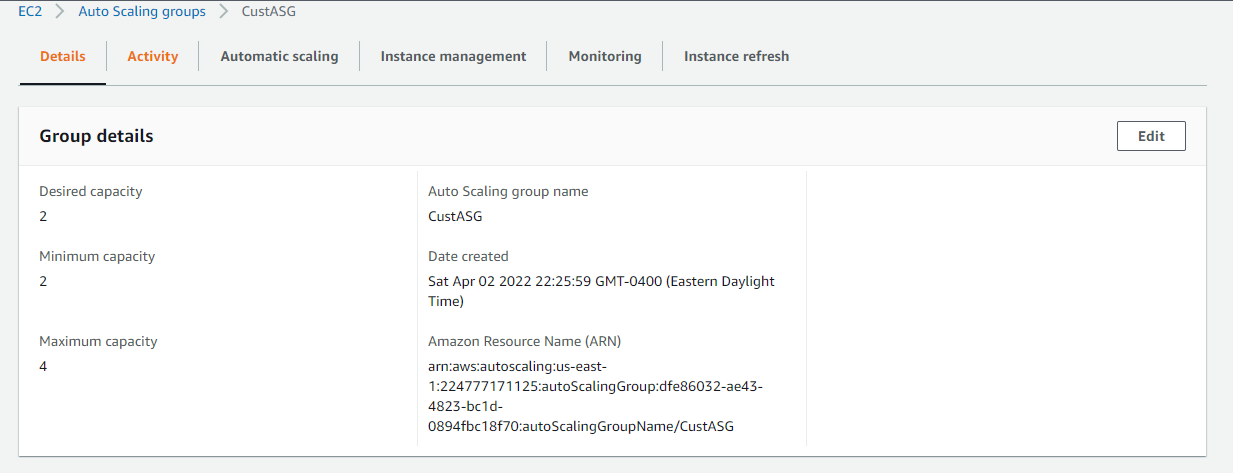
Target group:



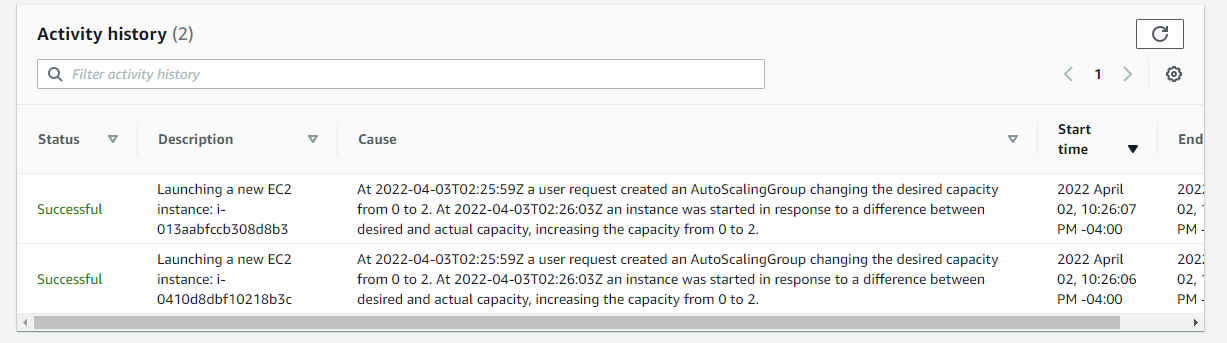


Step 6:

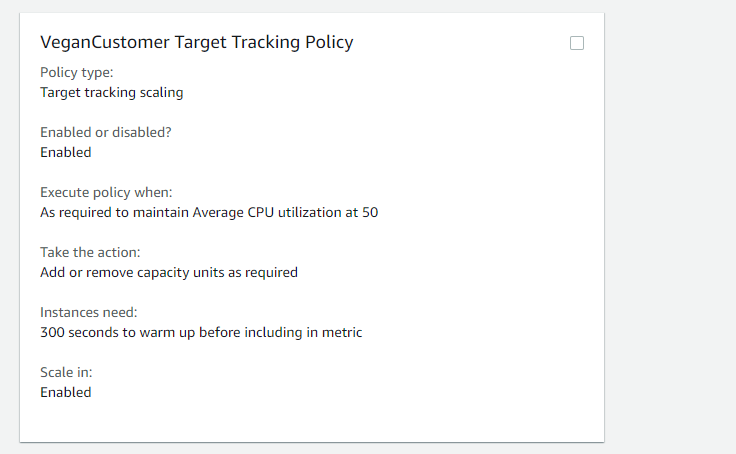
1. Create Launch configuration with AMI-Linux 2, s3 bucket IAM role, user data, security group, create keypair and ASG with desired capacity-2, minimum capacity -2, maximum capacity –4 and scaling policy as target scaling policy with Average CPU Utilization as 50%.



Activity History:

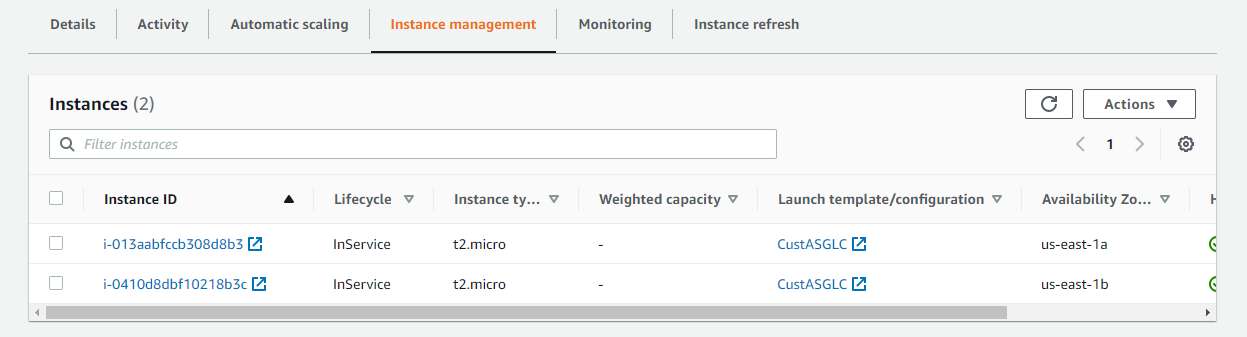


Scaling Policy:

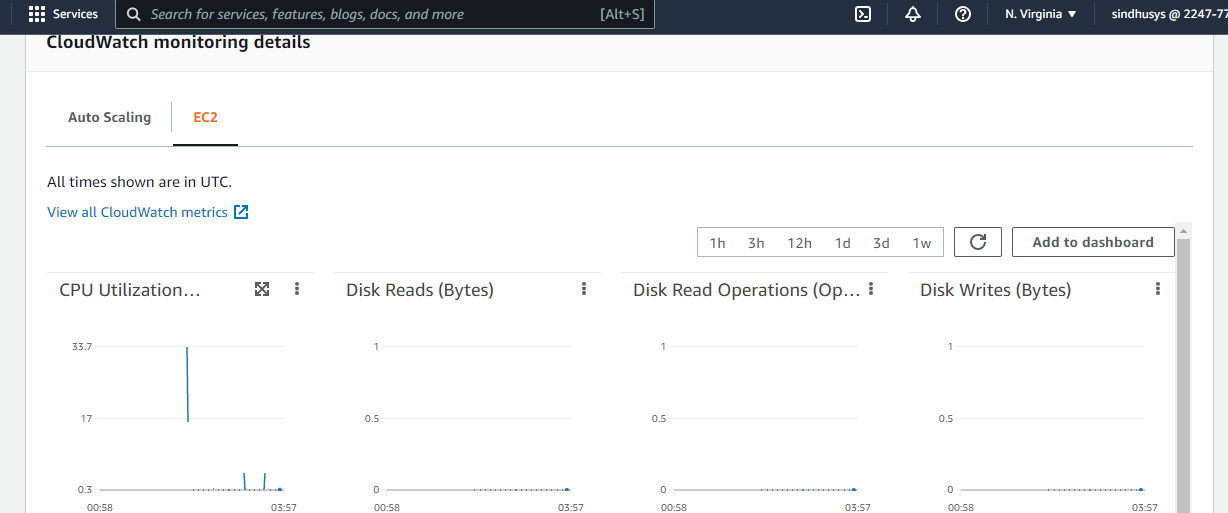


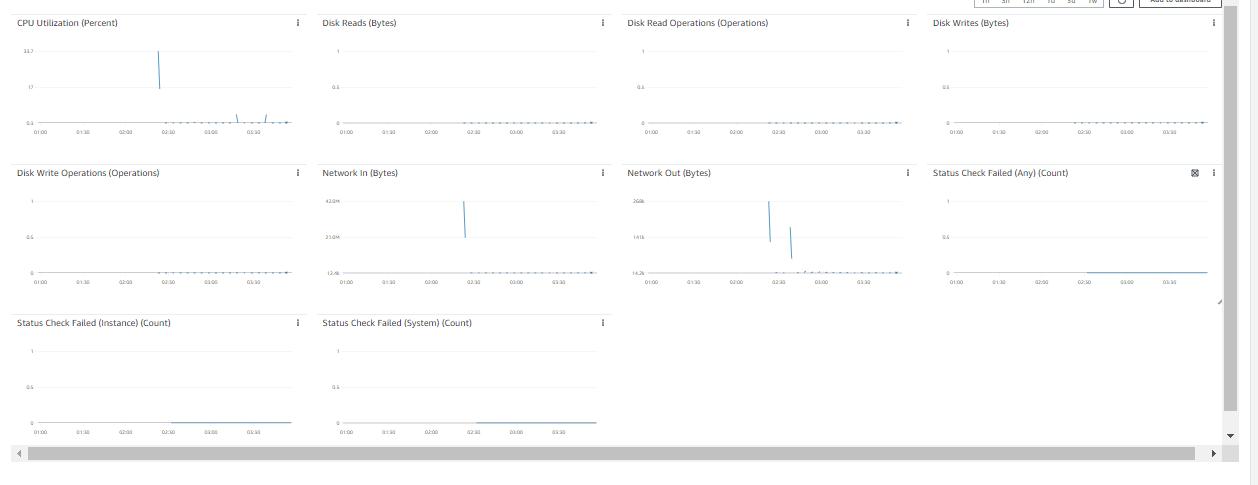
Once ASG created, Instances get launched and check it under Instance Management.

Instance management:



Cloudwatch monitoring:





Step 7:

The application can be accessed from the ALB DNS Name:

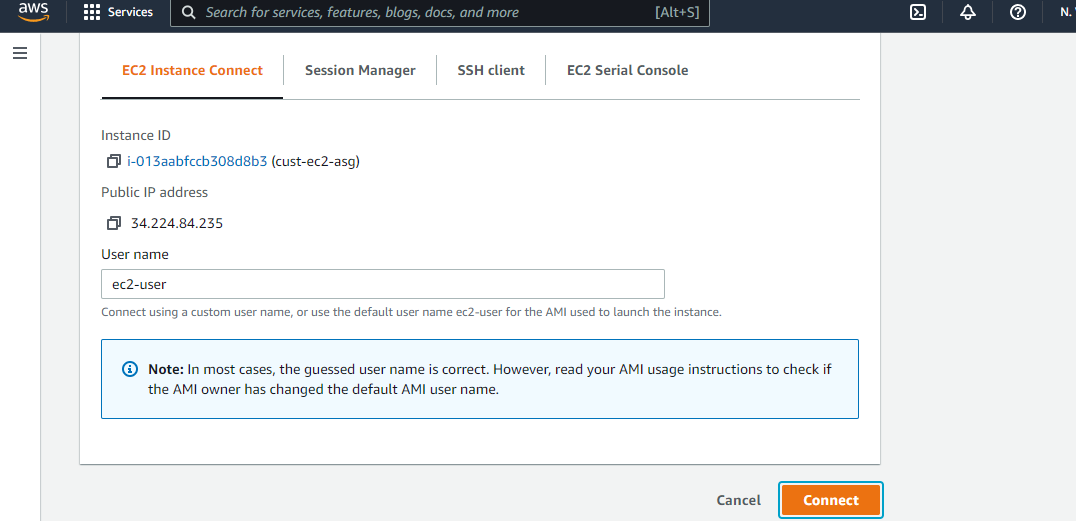
<http://vegancustomer-alb-894762189.us-east-1.elb.amazonaws.com/customer-recipe.html>



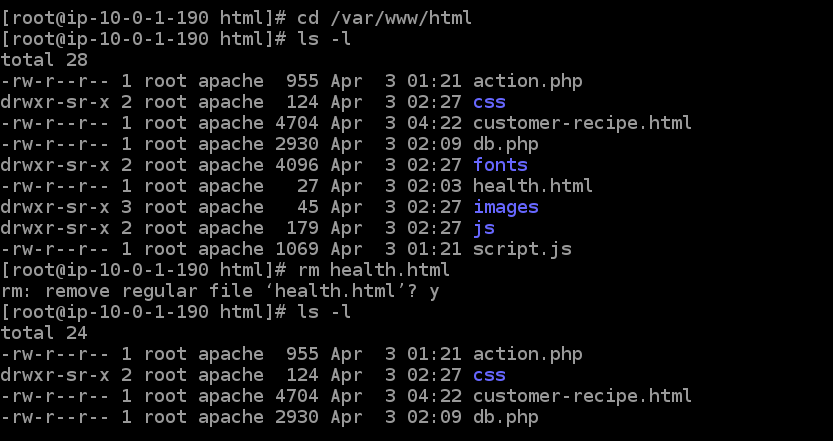
Step 8:

High Availability Test:

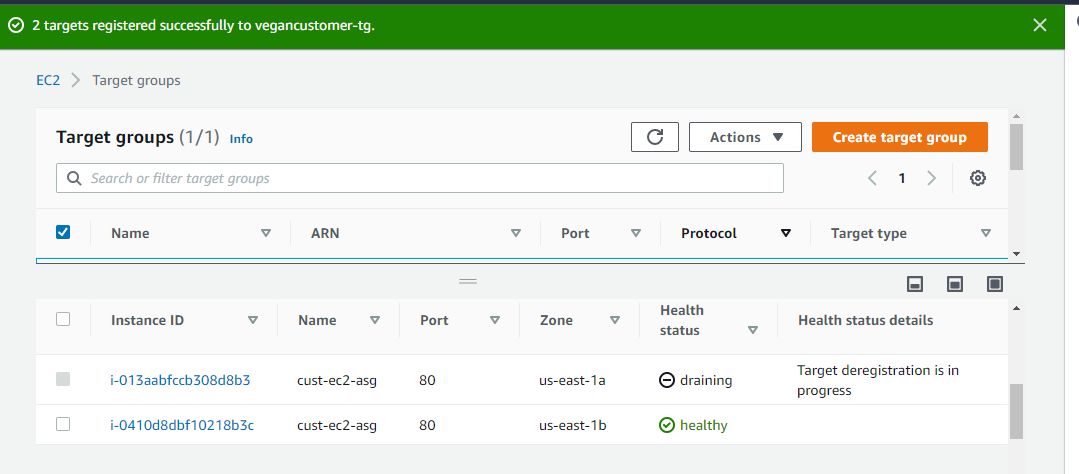
1. SSH into one of your instances and remove the health.html file from the s3 bucket. This ensures the application to run even if the instances health check is failed which tests the High Availability of the application.



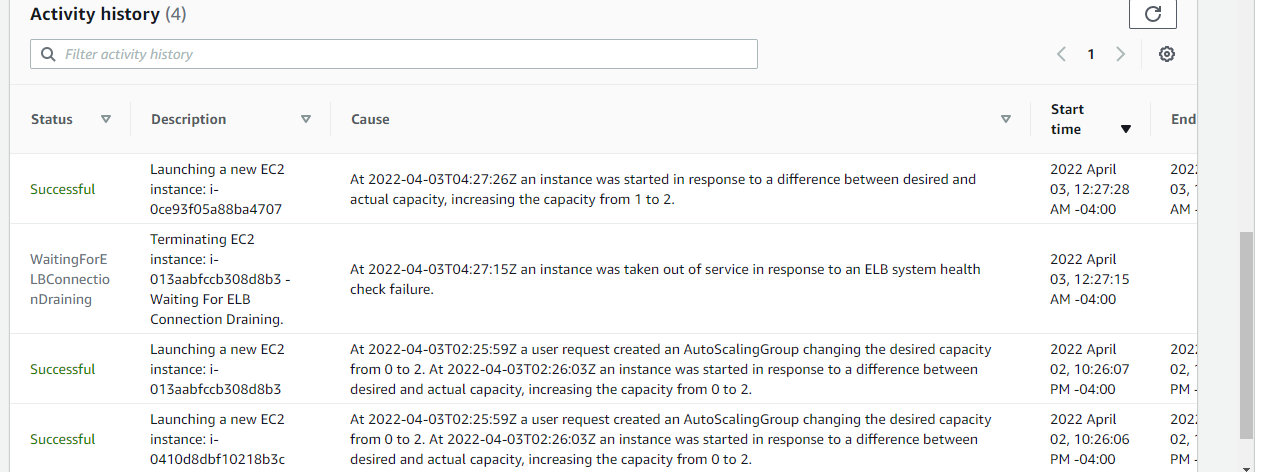
1. Commands for removing the health.html file from configuration files folder:

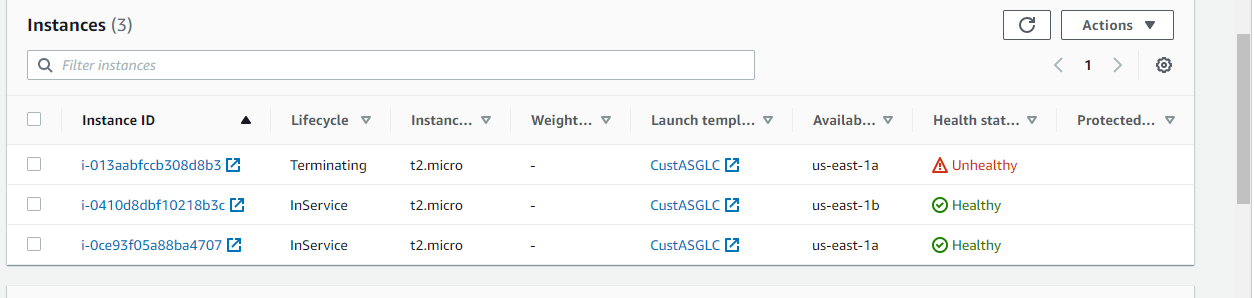


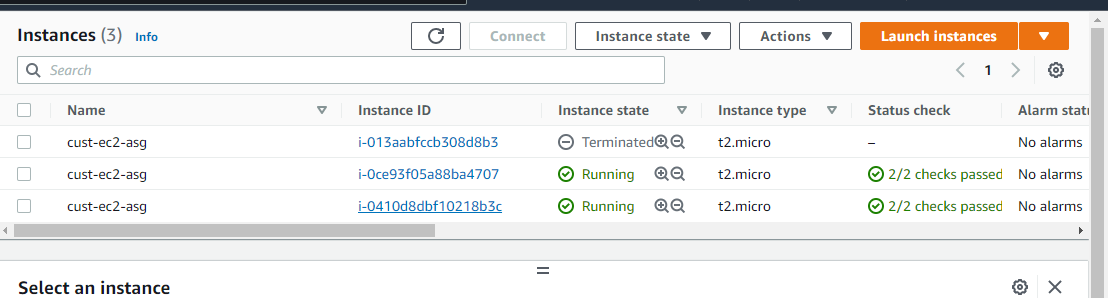
1. Target group de-registers the failed instance from the ALB.

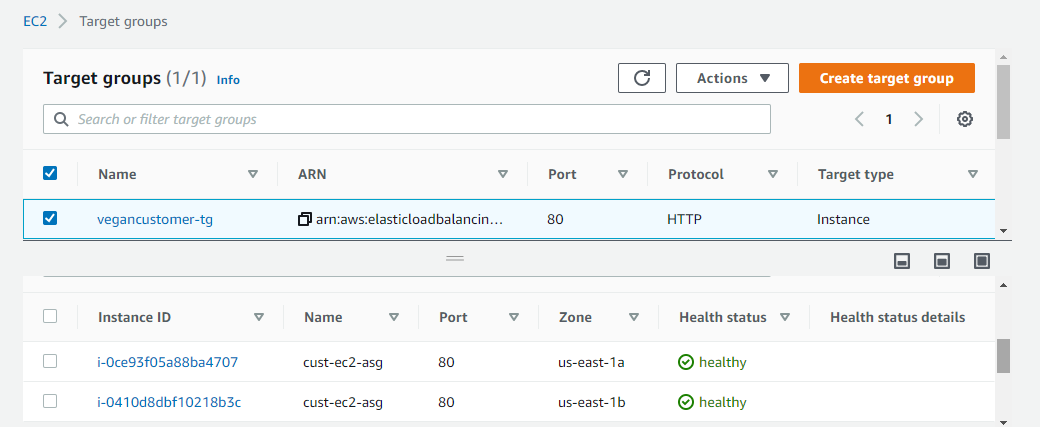


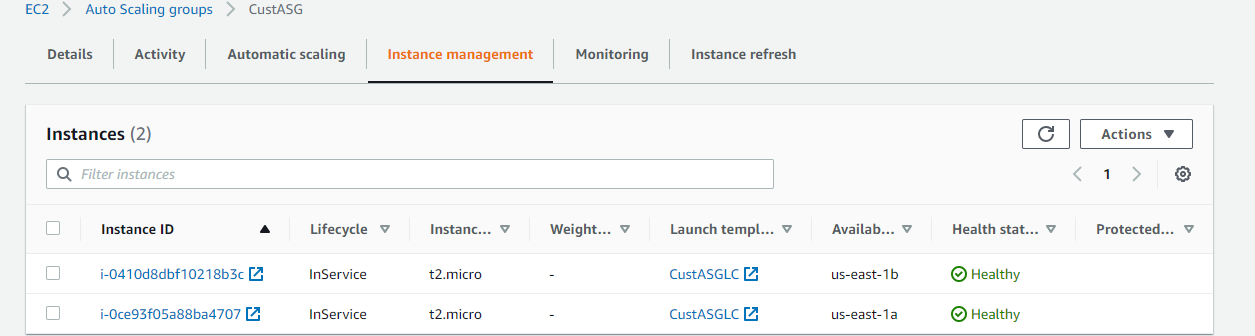
1. ASG terminates the failed instances and launches the new instance.







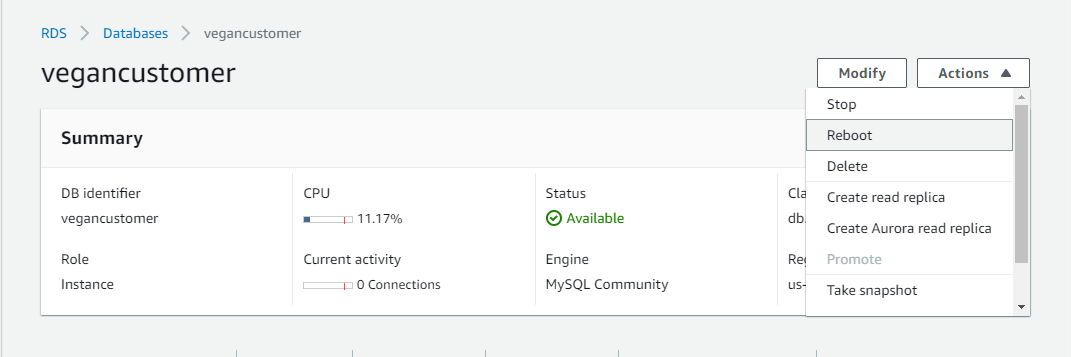




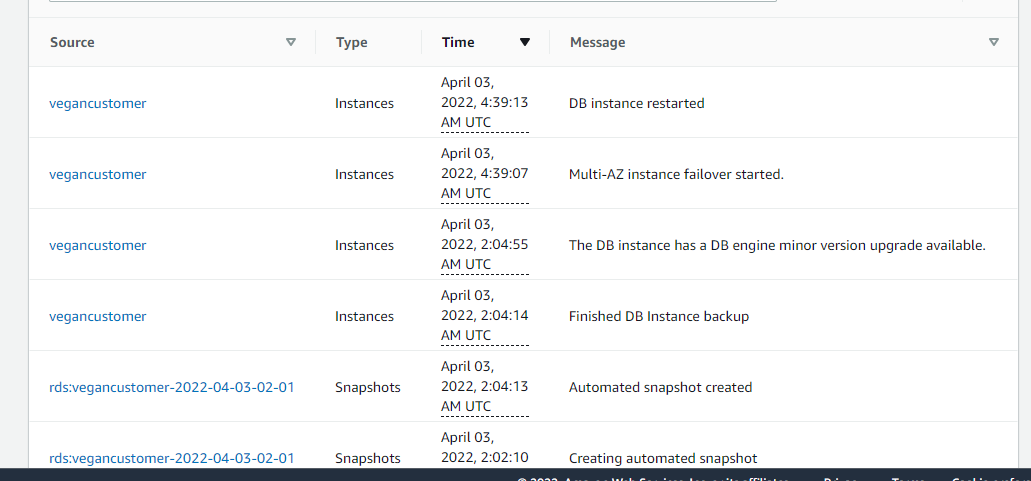
Step 9:

Failover Test:

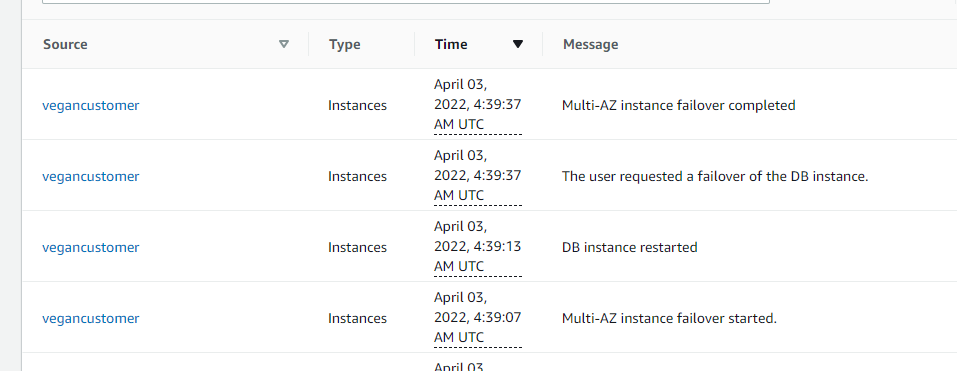
1. For failover test, reboot the RDS instance.



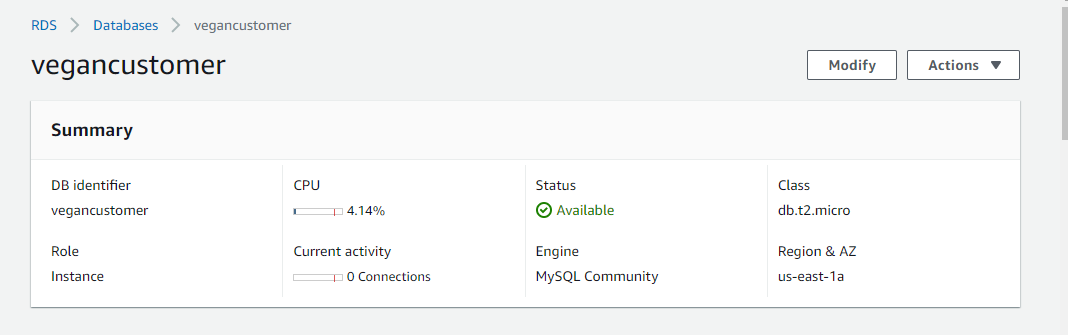
1. Failover started and the dB instance restarted.

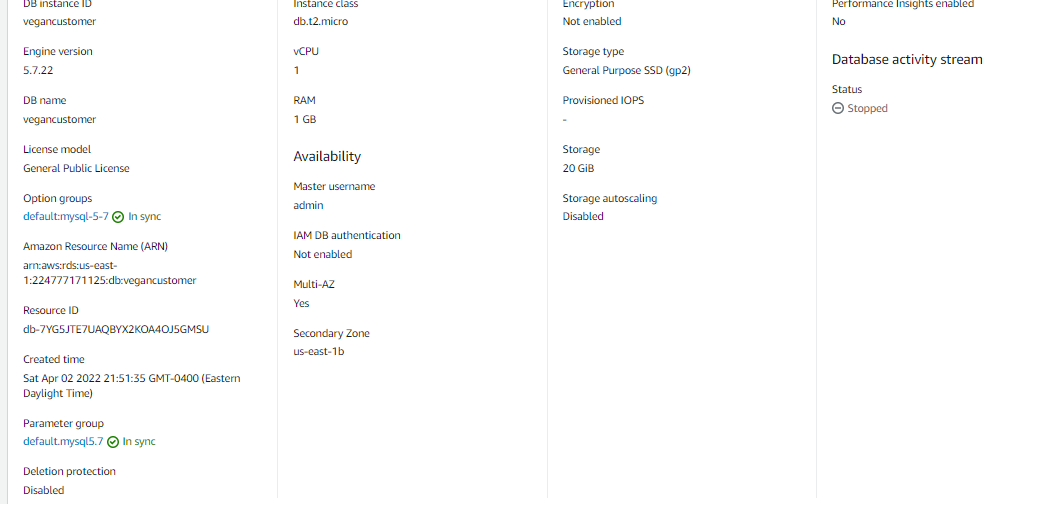


1. dB instance failover completed.



1. Check the dB Region & AZ failover succeeded through Primary and secondary zone in the RDS Instance Summary Page.





Cloudwatch :

