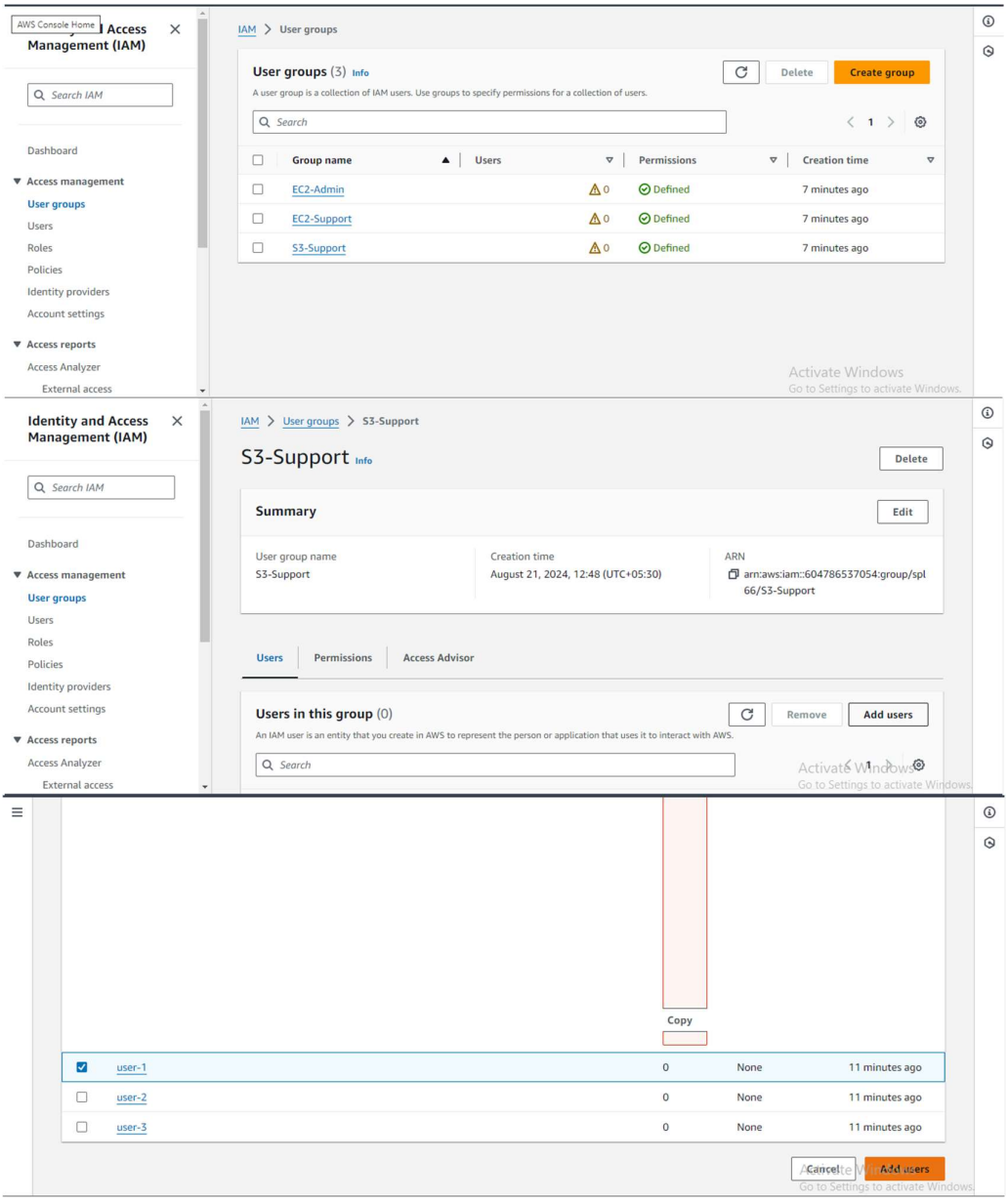
Practical-6

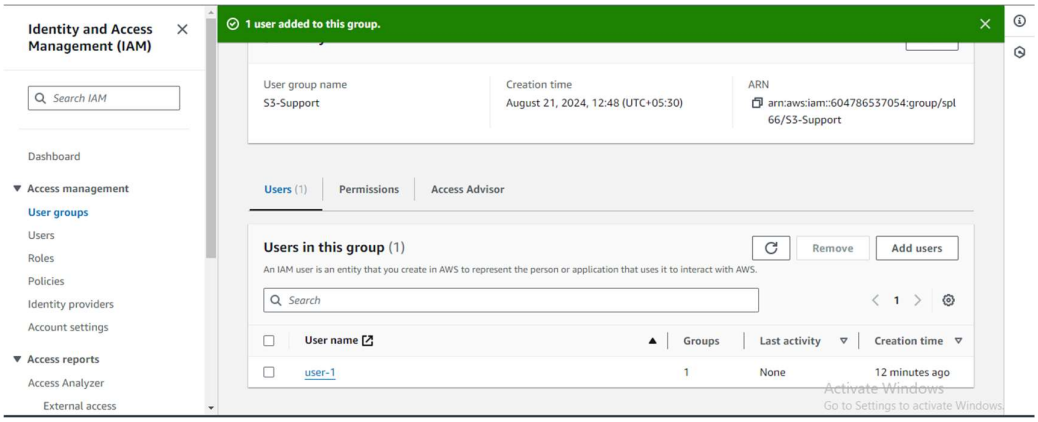
Aim: Introduction to AWS Identity and Access Management (IAM).

(Here we already have 3 Users Created and 3 Groups Created i.e user-1, user-2, user-3 and EC2-Admin, EC2-Support and S3-Support)

Step 1: Adding User 1 in S3 support Group.

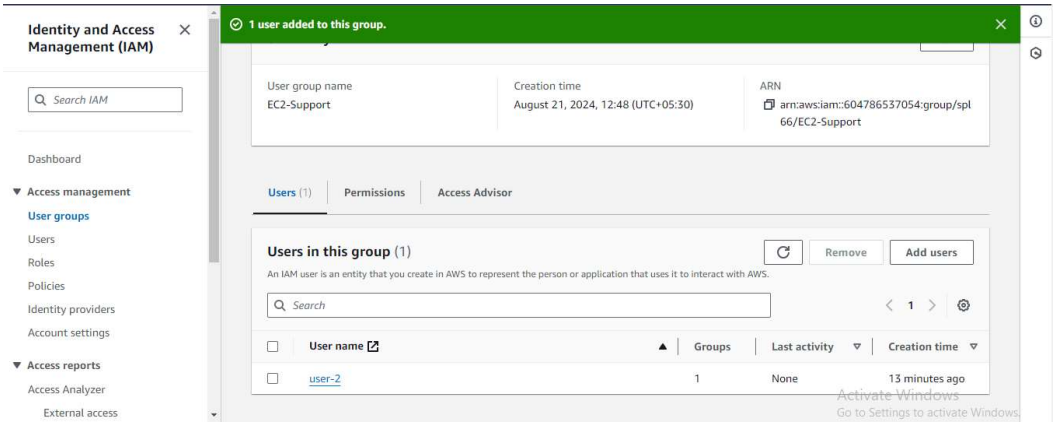
In the left navigation pane, choose User groups. Choose the S3-Support group link. Choose the Users tab. In the Users tab, choose Add users.



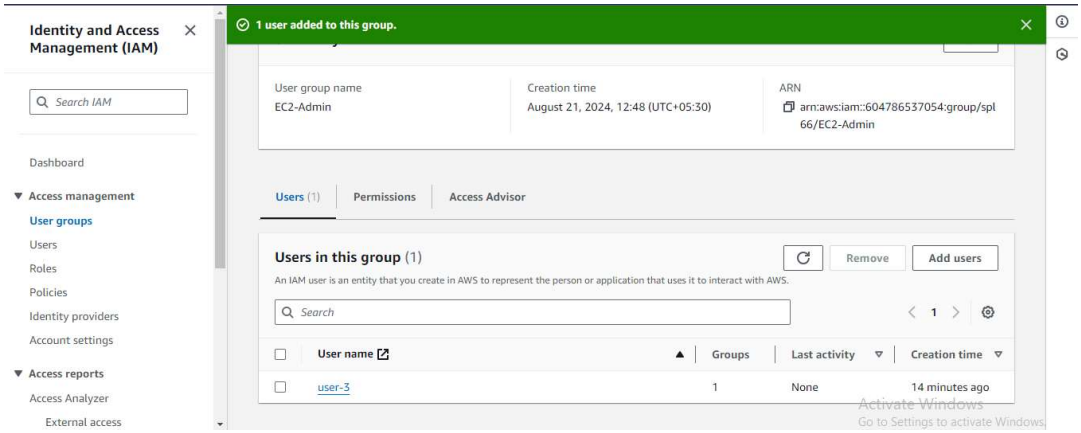


Step 2: Adding User 2 in the EC2 Support.

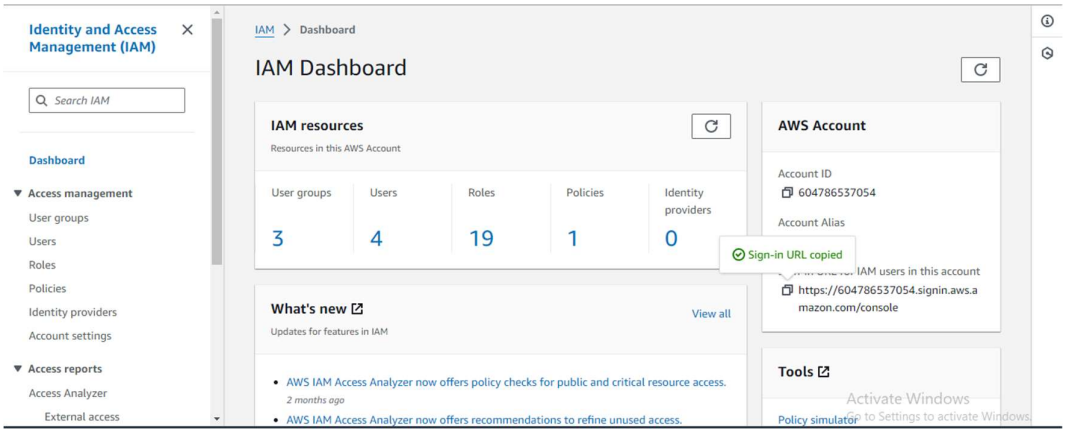
Using similar steps to the ones above, add user-2 to the EC2-Support group



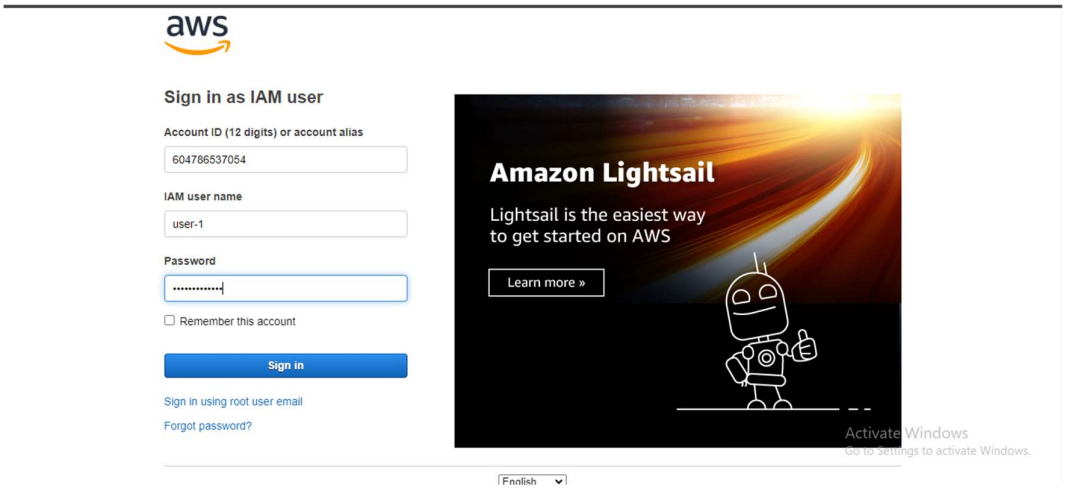
Step 3: Similarly Add User 3 in EC2-Admin.

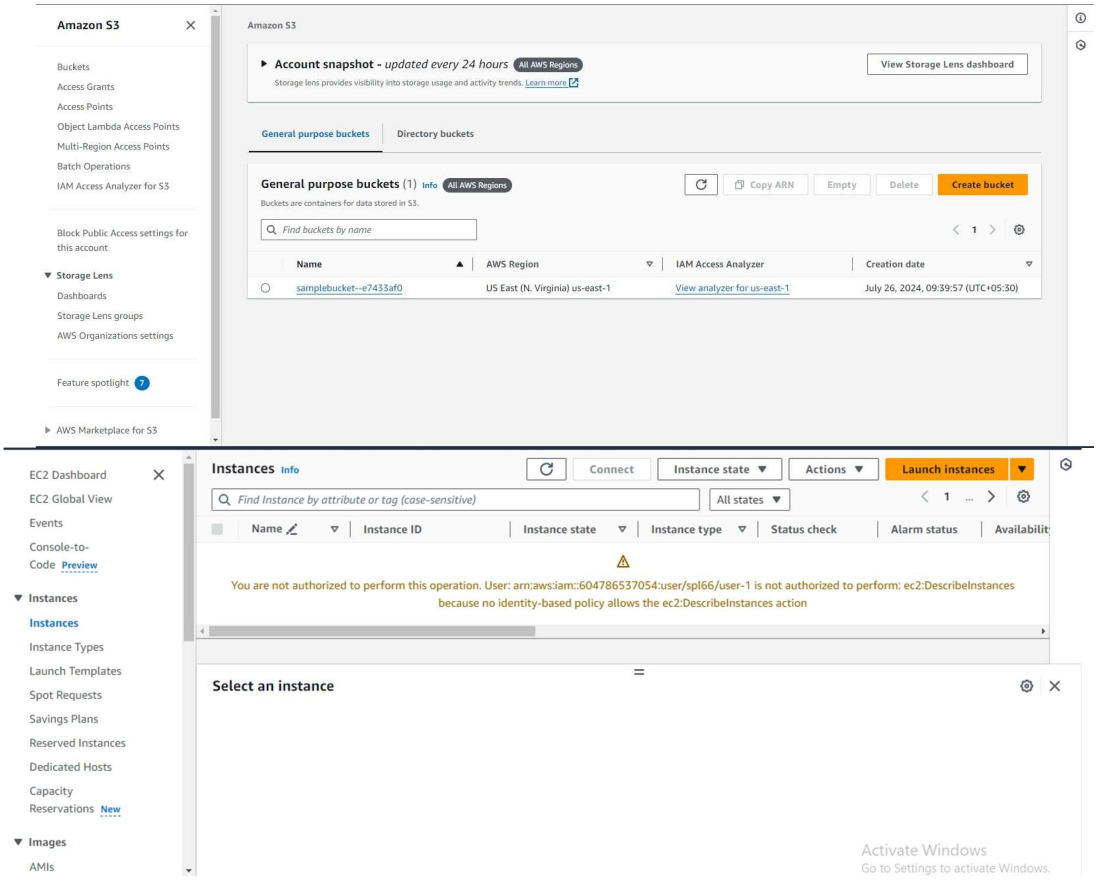


Step 4: Go to Dashboard and Copy the User Sign in Link and paste in Private window.

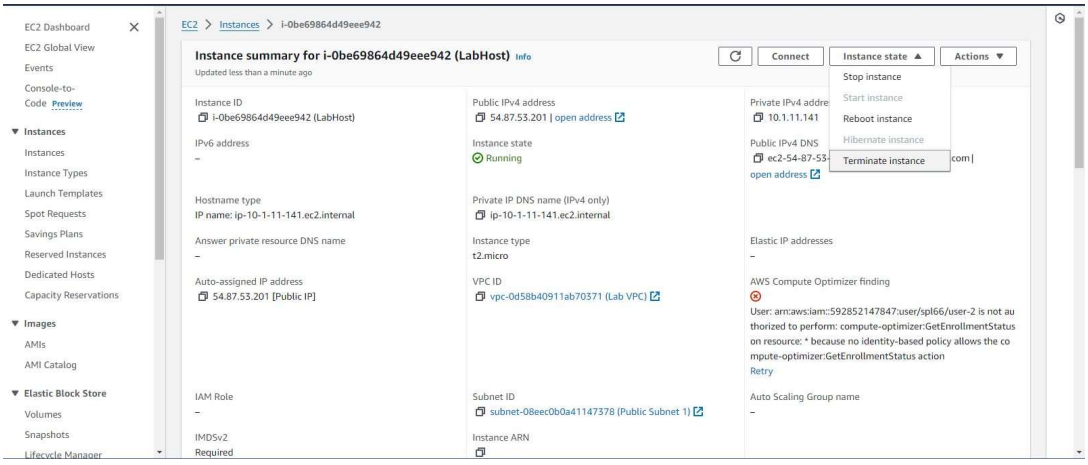


Step 5: Now Enter User-1 Id and Password in the console opened in private window, to check the permissions of User-1 first check for s3 bucket it will show up then try to create an EC2 Instance, will see an error message because user-1 don't have permission to create instance as he is part of S3-Support group.

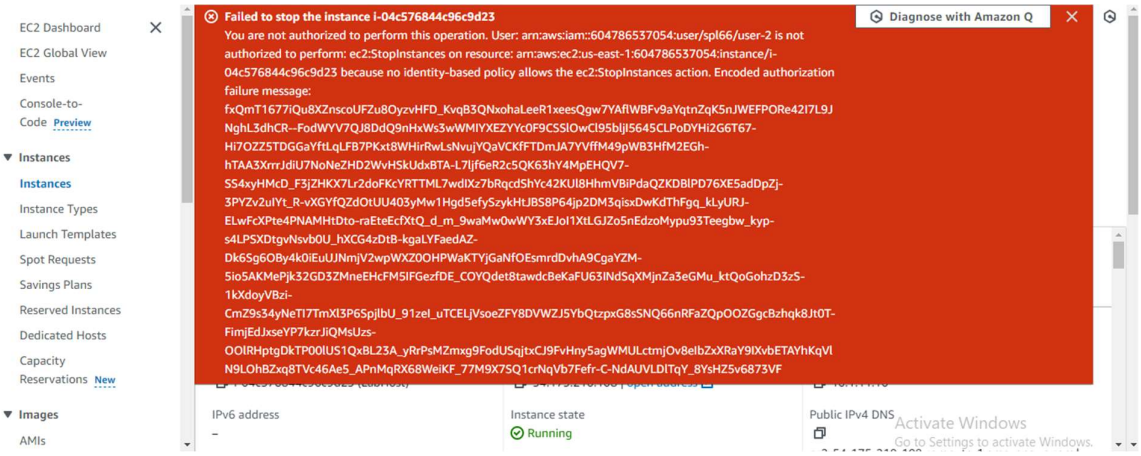




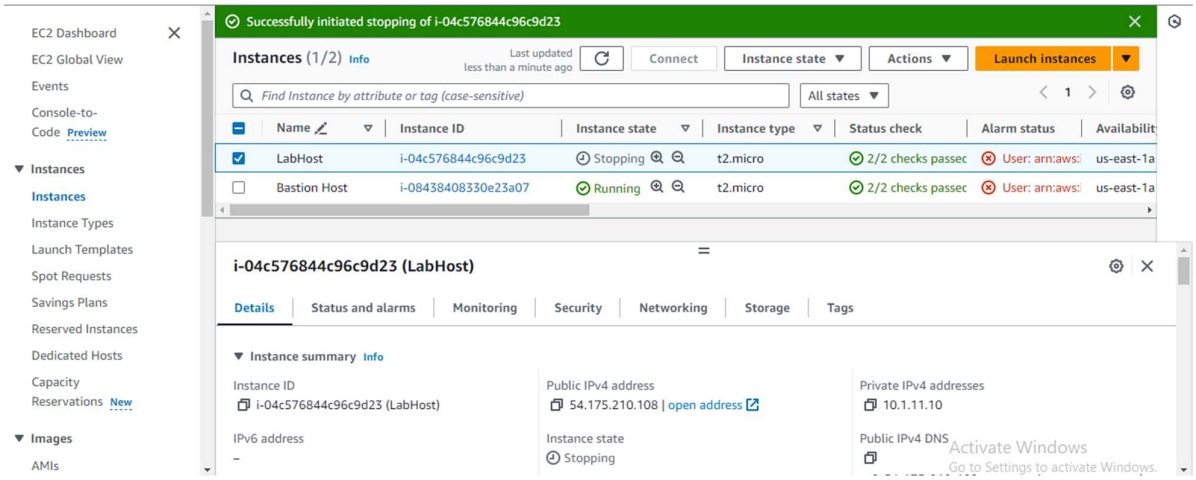
Step 6: Similarly Enter the user-2 Id a password in the console opened in private window and check for EC2 support permission which refers to only reading the EC2.



Step 7: Check the permission of User 2, Try to stop the instance Lab-Host, you will get an error message as the user is part of EC2-Support that only has Read Only permission.



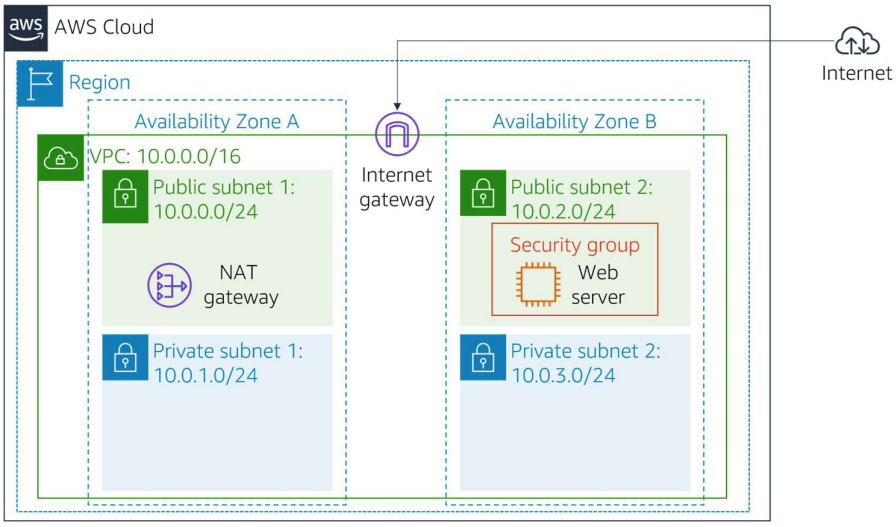
Step 8: Now enter user-3 Id and password and check the permissions for User 3 Try to stop the instance and it will be stopped because he part of EC2-Admin group and has admin privileges.



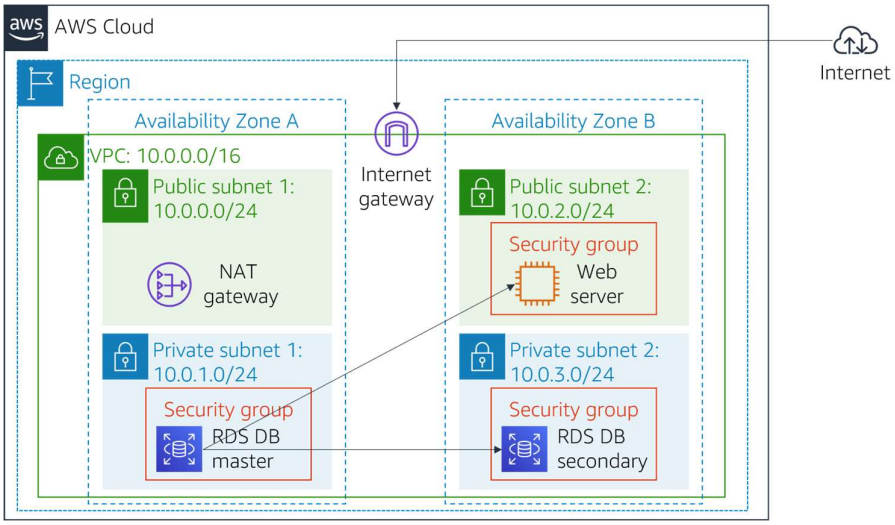
Practical-5

Aim: Build Your DB Server and Interact with Your DB Using an App.

Already Configured VPC:



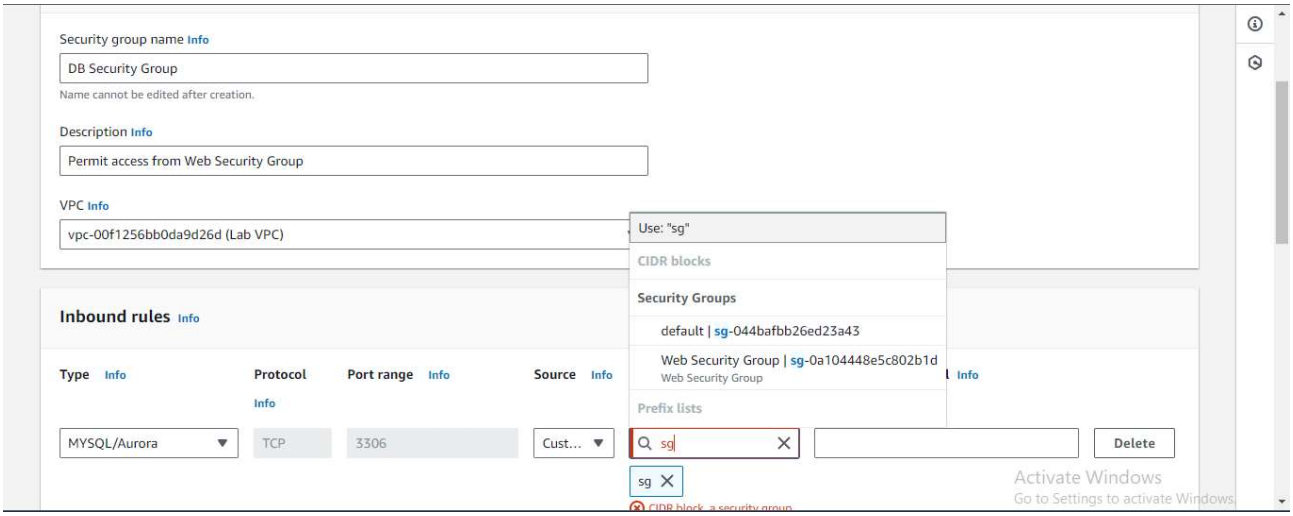
Additional Configuration We're going to Perform:



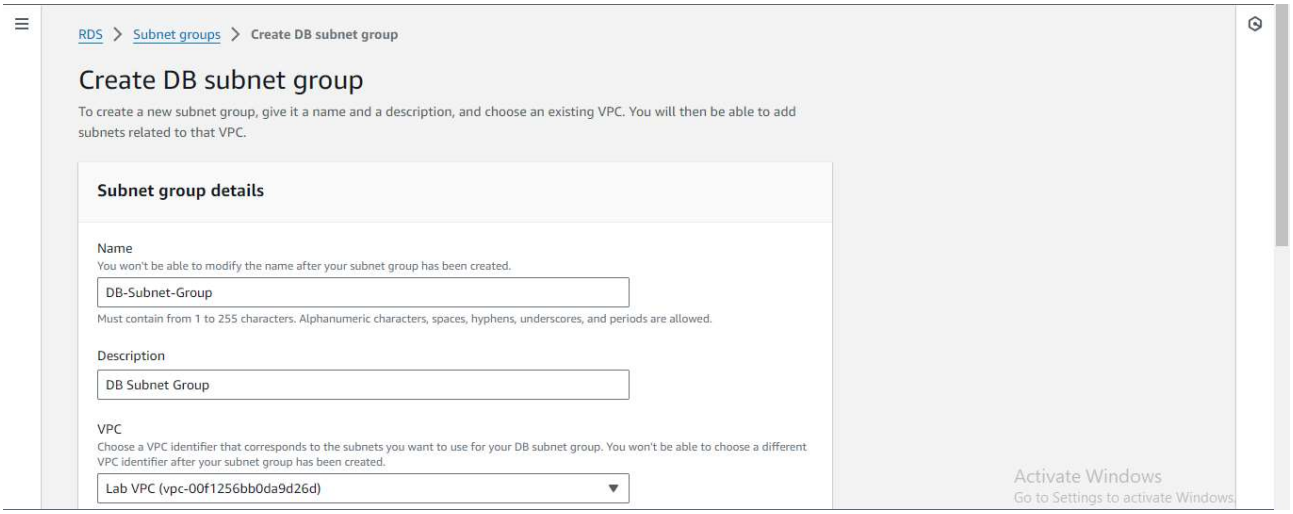
Step 1: Create security group for the RDS DB instance, go to VPC and security groups then choose create security group and provide below given specifications, and create it.

-Select the create VPC (here Lab VPC).

-Add an inbound rule which configures database security group to permit inbound traffic on port 3306 from any EC2 instance that is associated with the web security group. Here, as we are using MySQL DB engine, we will select relevant type and source as Web Security Group.

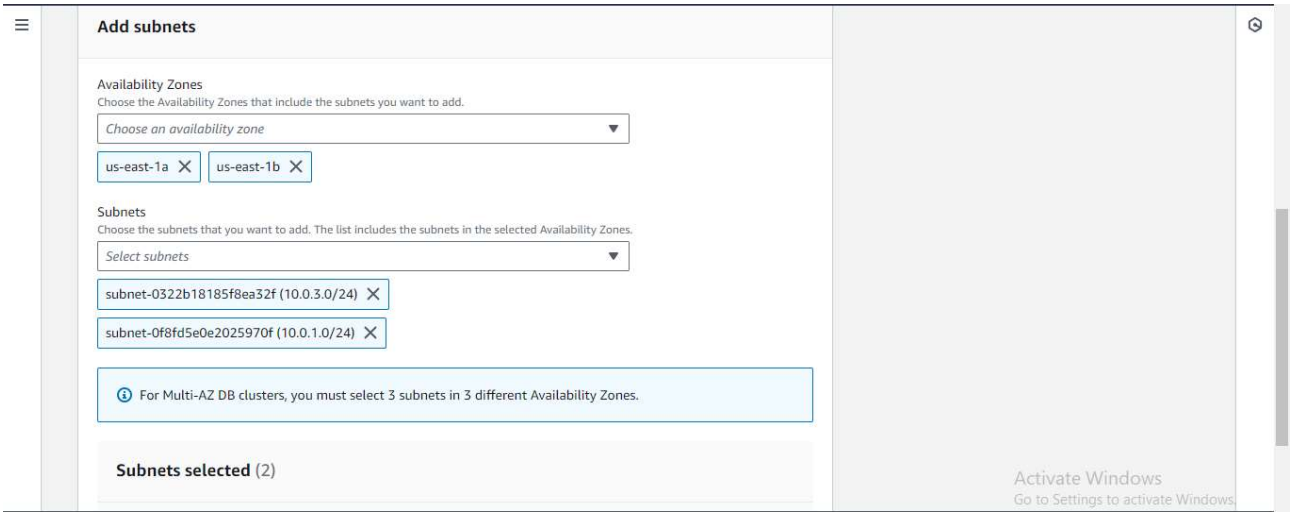


Step 2: Create a DB subnet group, go to RDS from services then choose subnet groups from left navigation pane, click on create DB subnet group and provide specifications as shown in screenshot below.

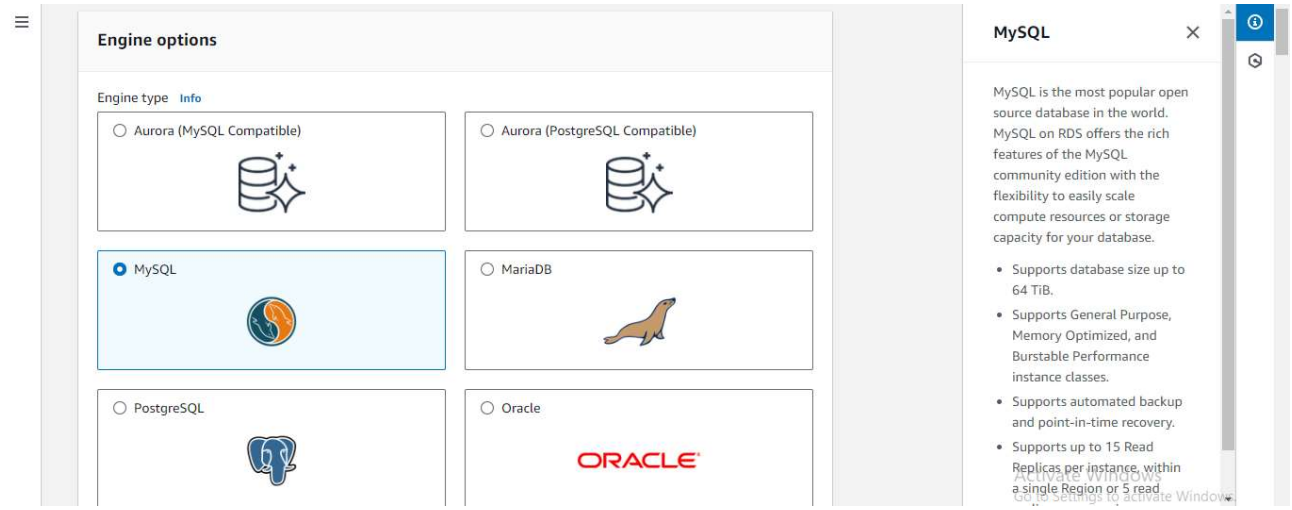


-We create DB subnet group in order to create multi availability zone deployment, amazon RDS provides facility of replication in different availability zone for availability and durability of service.

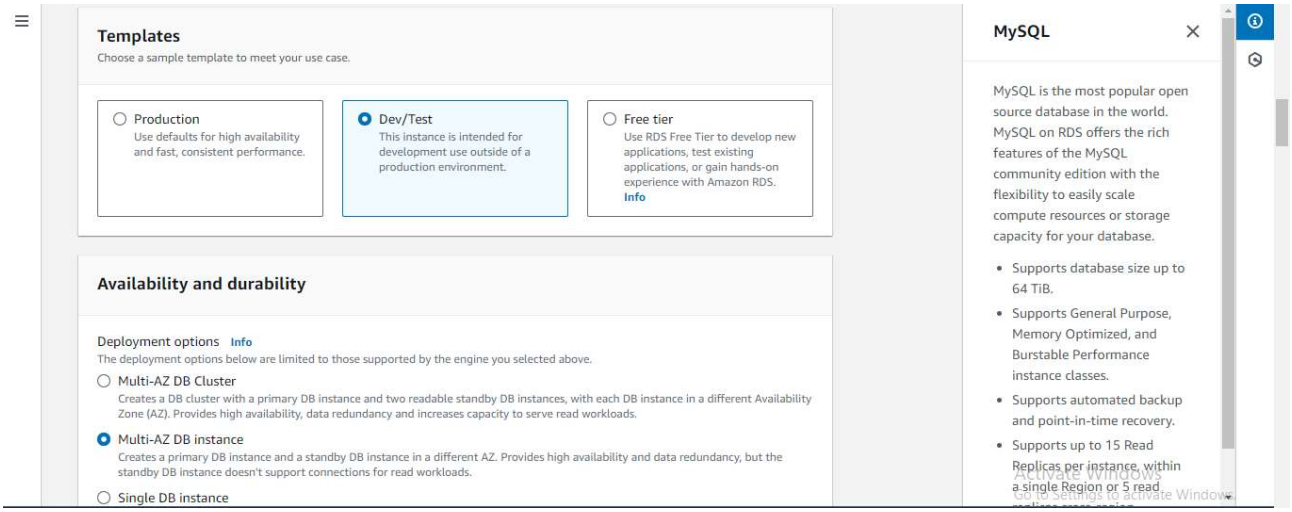
-Select AZs and Subnets in which you want to create RDS instances or to have database service as per below screenshot and click on create.



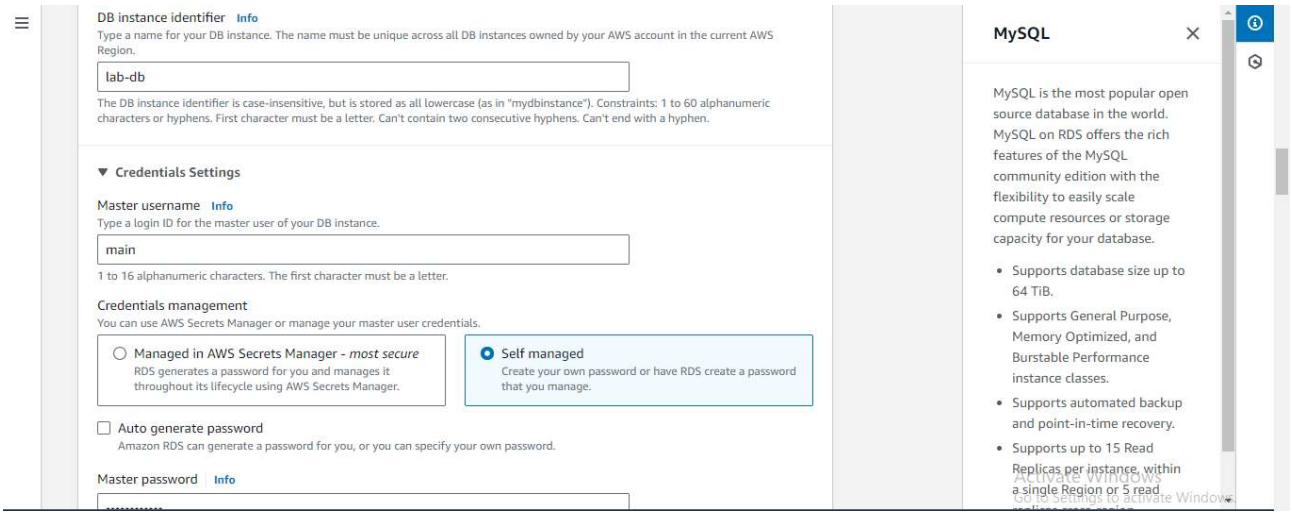
Step 3: Create an amazon RDS DB instance, select MySQL from Engine Options.



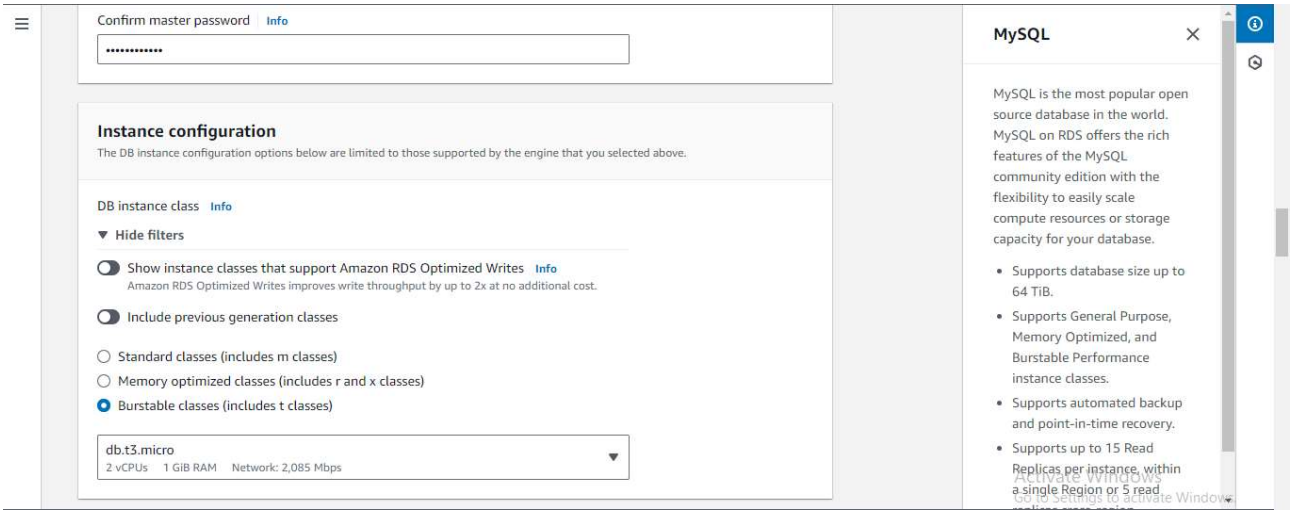
-Select template as Dev/Test refers to development and testing.



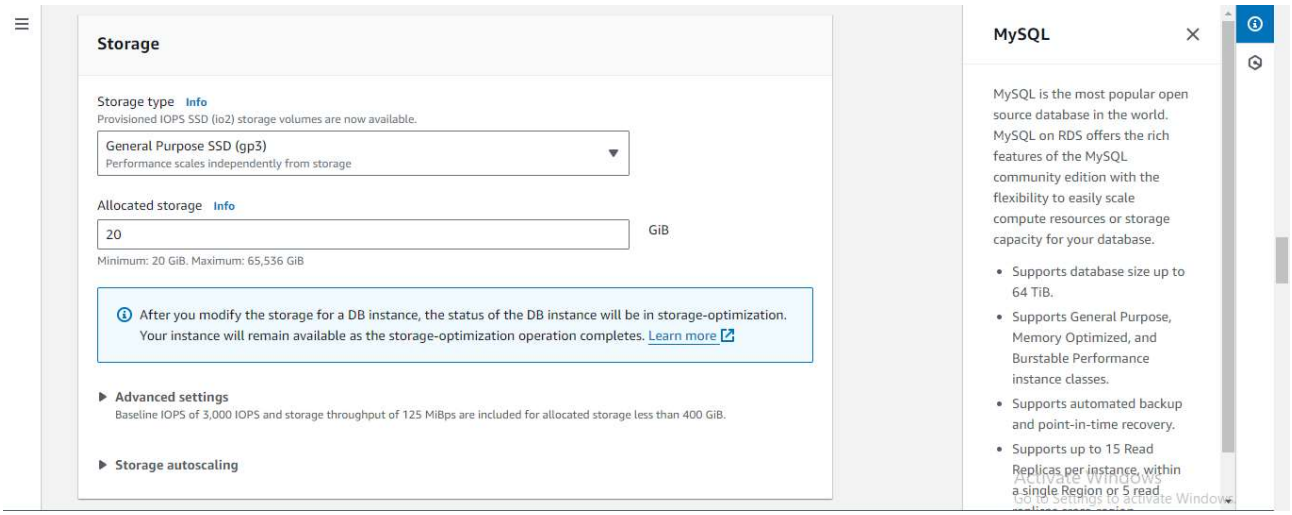
-Provide credentials details as given below in screenshot.



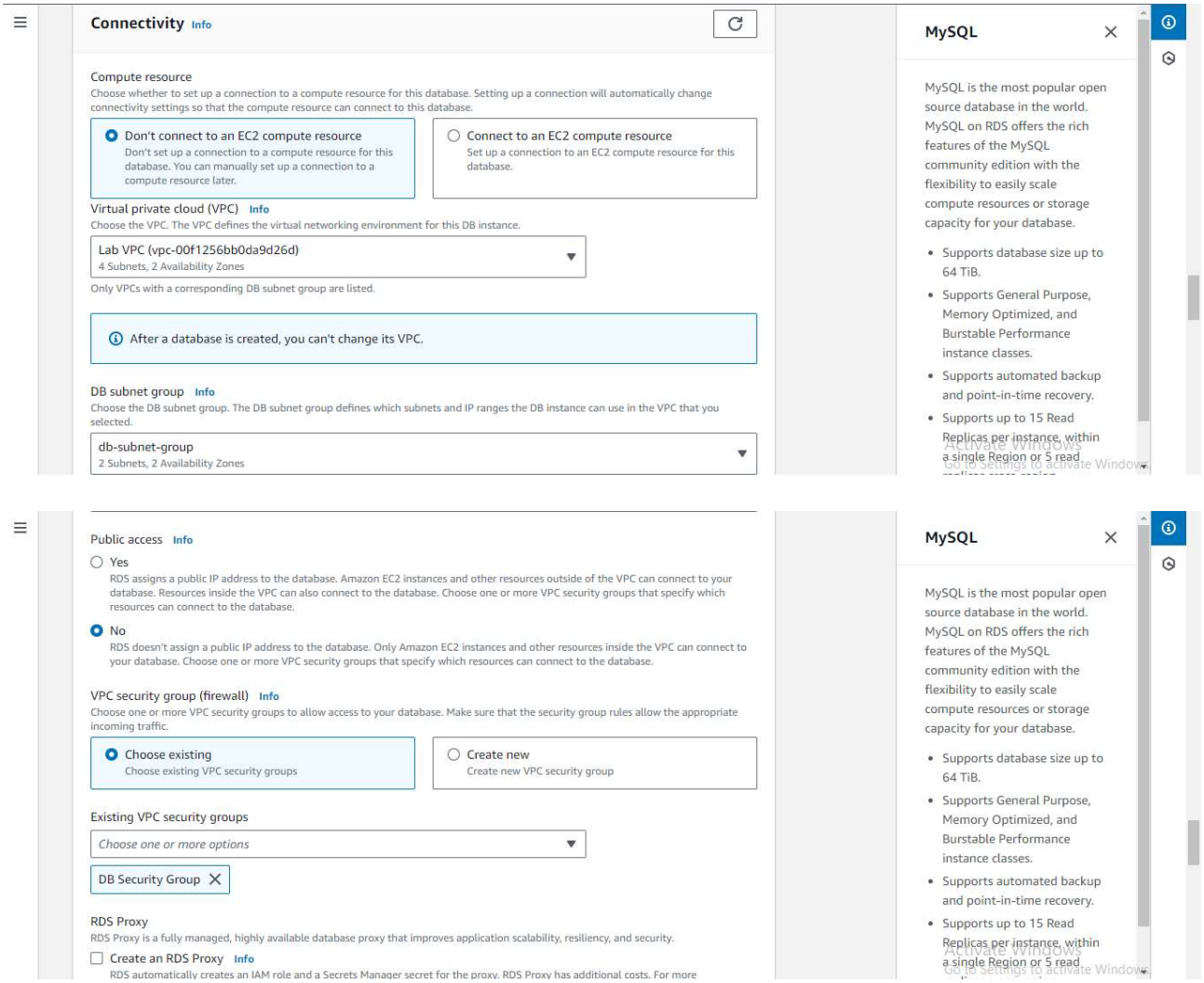
-In instance configuration select burstable classes and db.t3.micro for free tier access.



-In storage set general purpose storage type and allocate 20 GB of storage.



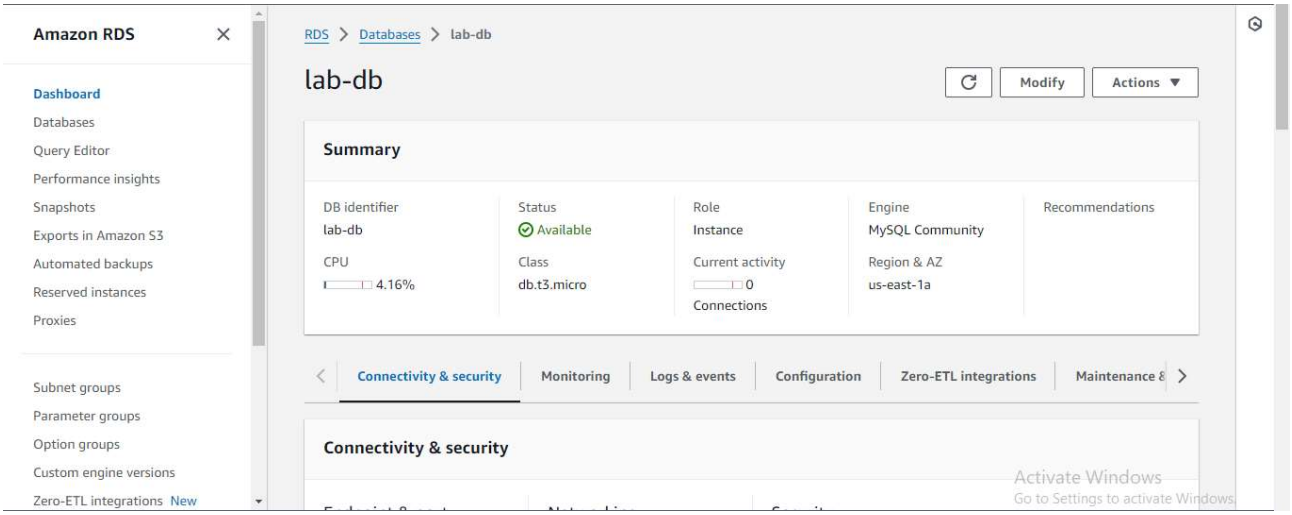
-In connectivity, select Lab VPC and db-subnet-group created above and give no to public access with configuration of db security group.

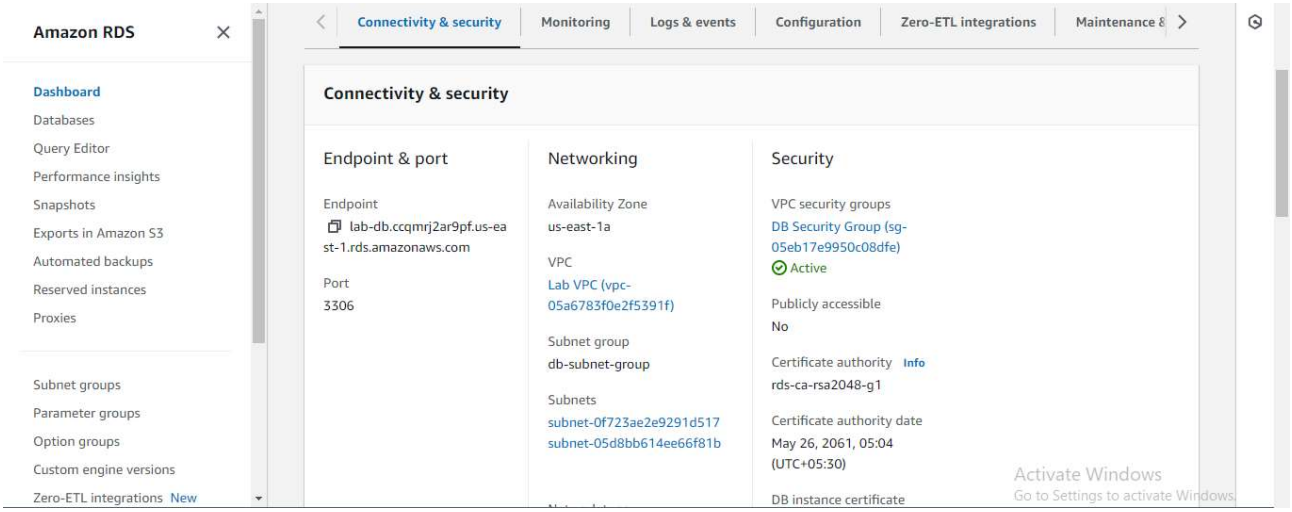


-Also uncheck all the options like Enable advanced monitoring, Enable storage backup and Enable encryption to faster instance creation.

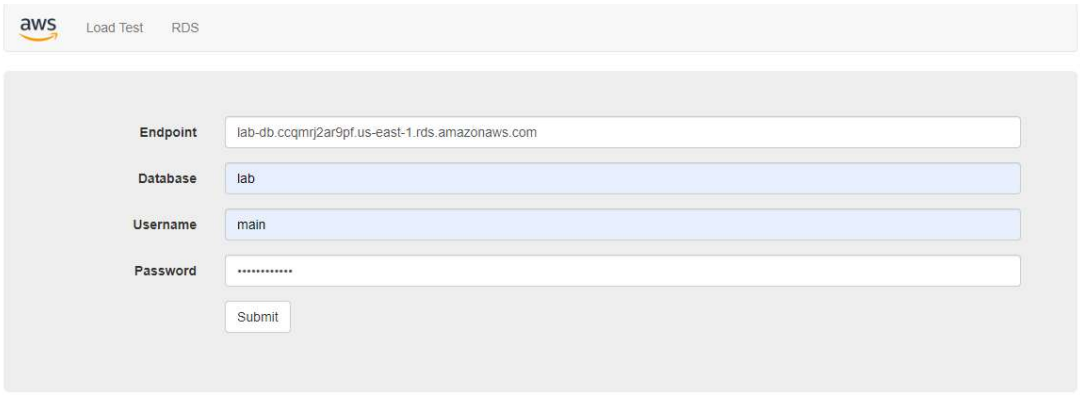
-As well as provide initial database name as lab.

-As soon as status of DB instance gets available goto connectivity and security and copy the endpoint for further use





Step 4: Interact with your database, copy the ip address of web server and paste it to the browser's new tab and click on RDS link and then it will ask for an endpoint and other credentials so provide it and then click on submit, you will find a page which prompts regarding command execution for database access.



-Address book will be displayed and we can add, edit or remove contact from database via web server.