Q.1.Implement IAM policies to enforce multi-factor authentication (MFA) for IAM users attempting to perform sensitive actions, such as terminating EC2 instances or deleting S3 buckets.

🡺

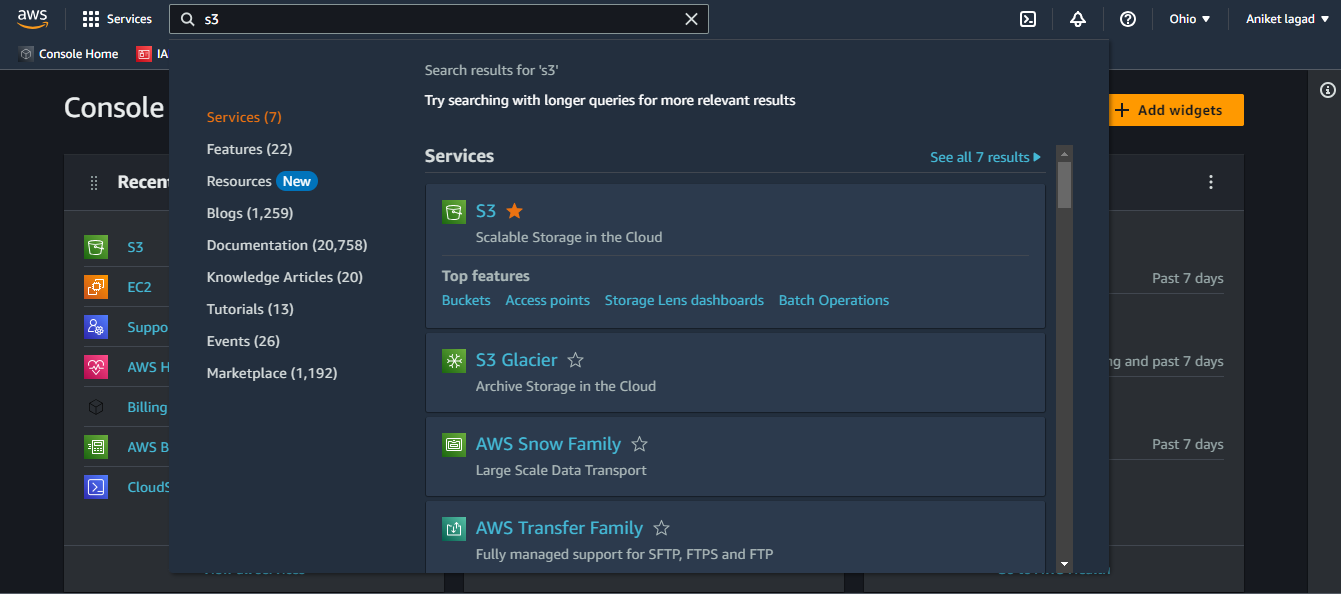
Q.2.Set up a lifecycle policy for an S3 bucket to automatically transition objects to less expensive storage classes, such as moving infrequently accessed data to Glacier for long-term archiving.

🡺

Step 1:-

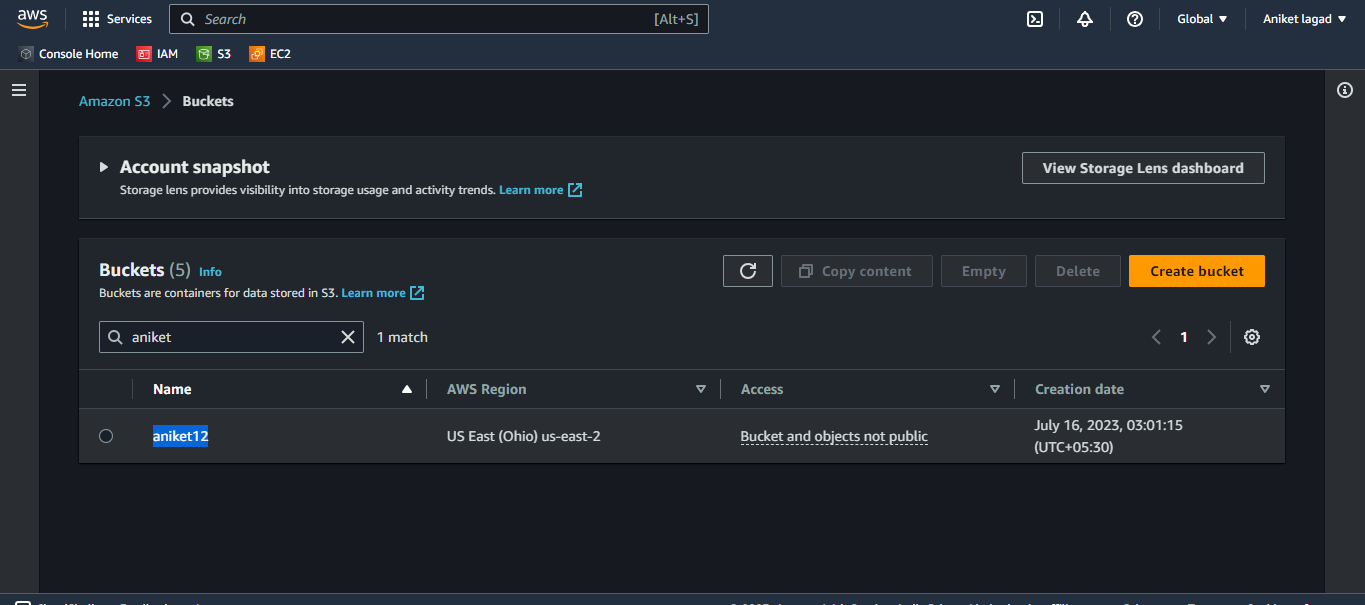
Login to aws account and open s3 service.





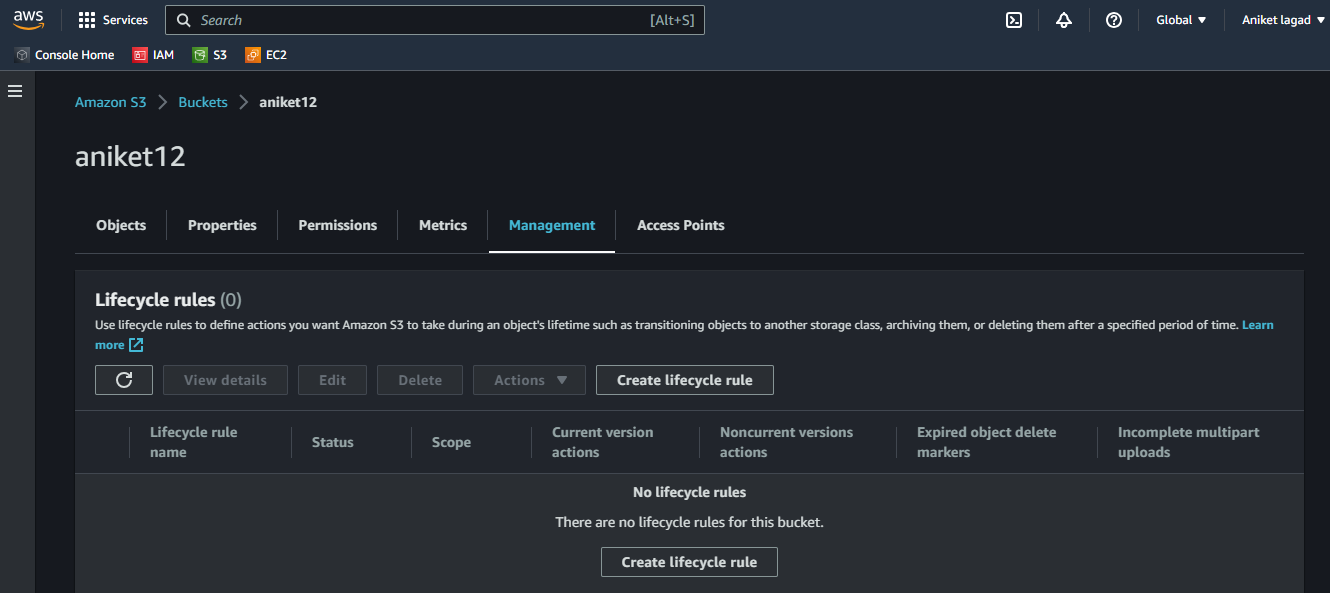
Step 2:-

Now go to that bucket which u have to set up a lifecycle policy.



Step 3:-

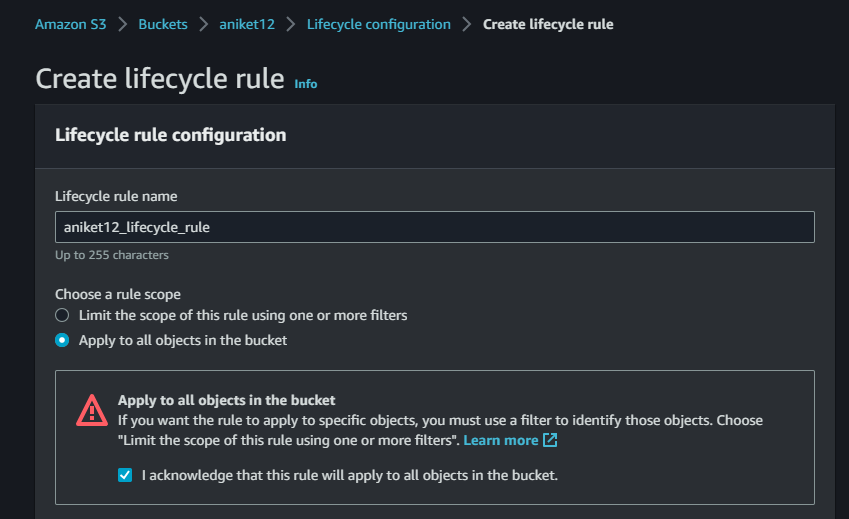
After that you will see the option management click on that and next you will see the create lifecycle role click on it.

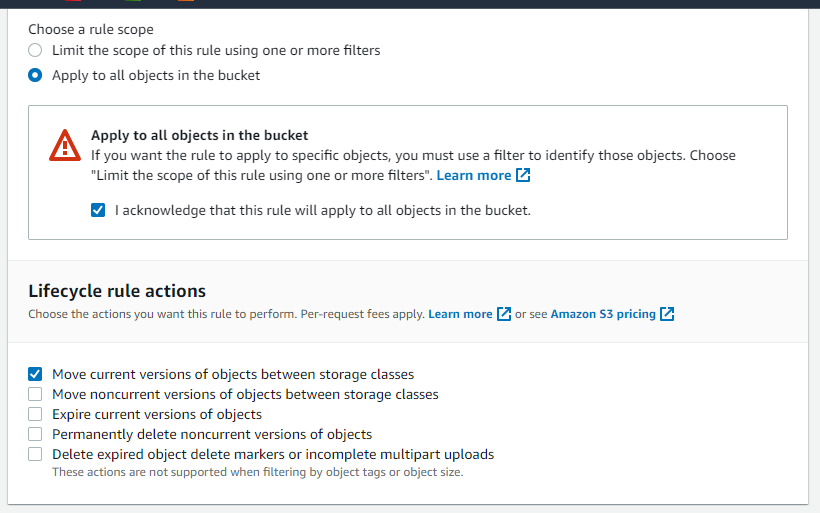


Step 4:-

Oky now you have to gave a lifecycle role name and next prefix it means whenever you want to search a lifecycle role then you can filter by its prefix.Also you can apply to all object of bucket.

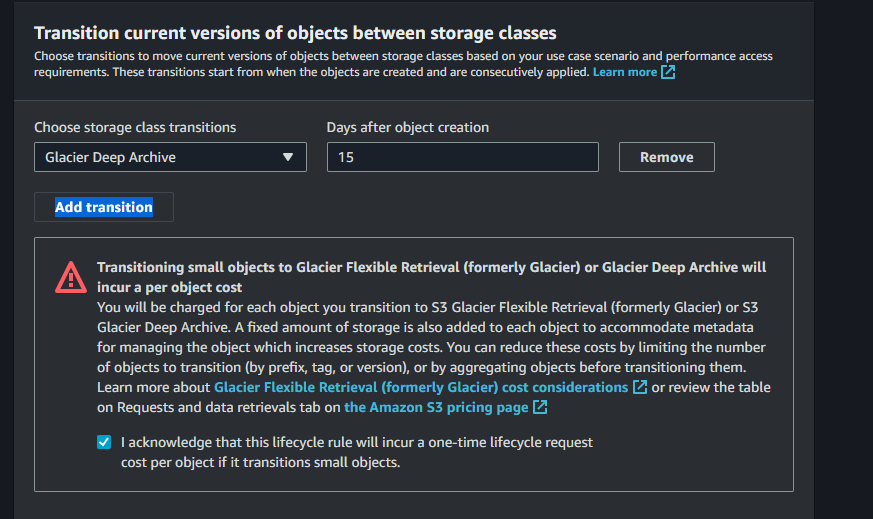
See following how to get that option.



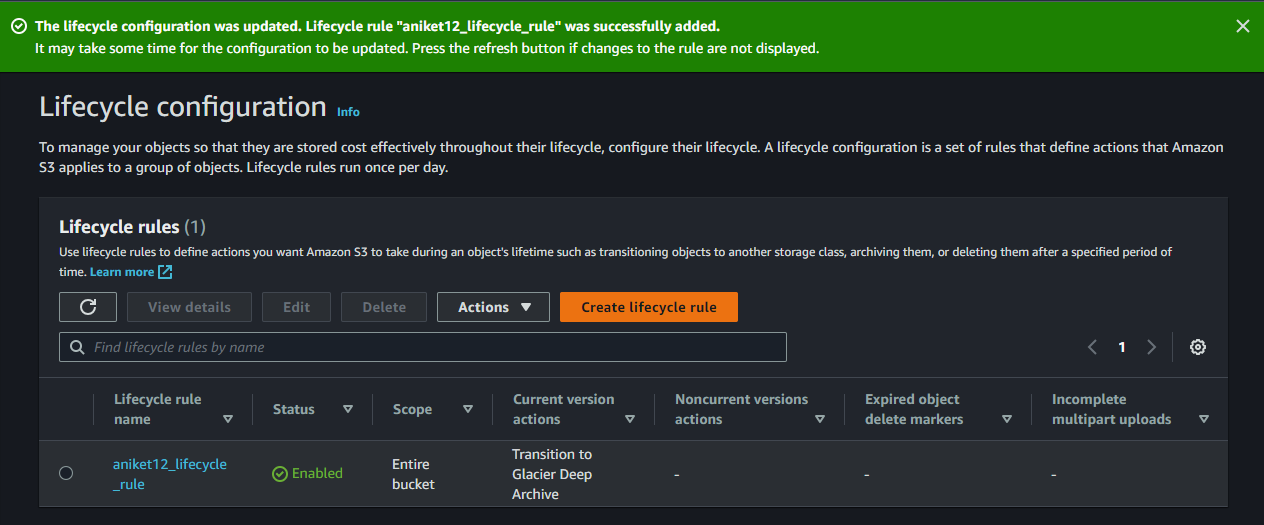


Step 5:-

Next you will see the lifecycle rule actions option that option is for perform the rule it has fee apply to per-request.



Step 6:-

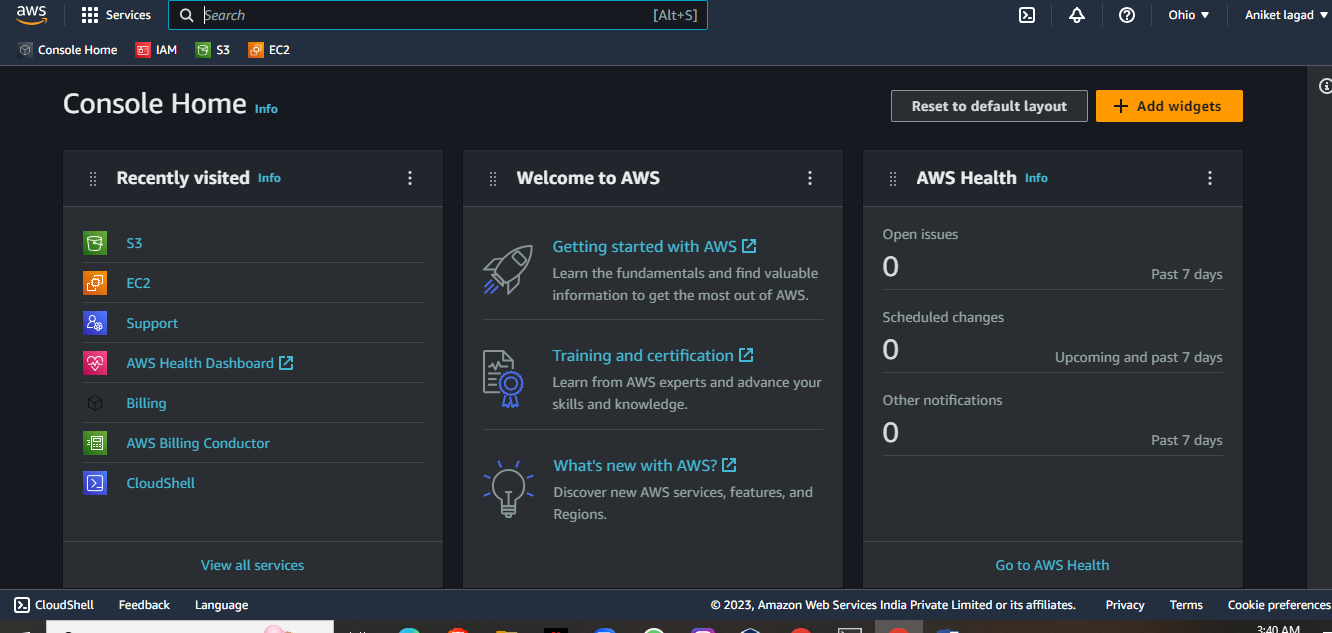
After that see the lifecycle review and the click on create role.And adter that you see the lifecycle role. 

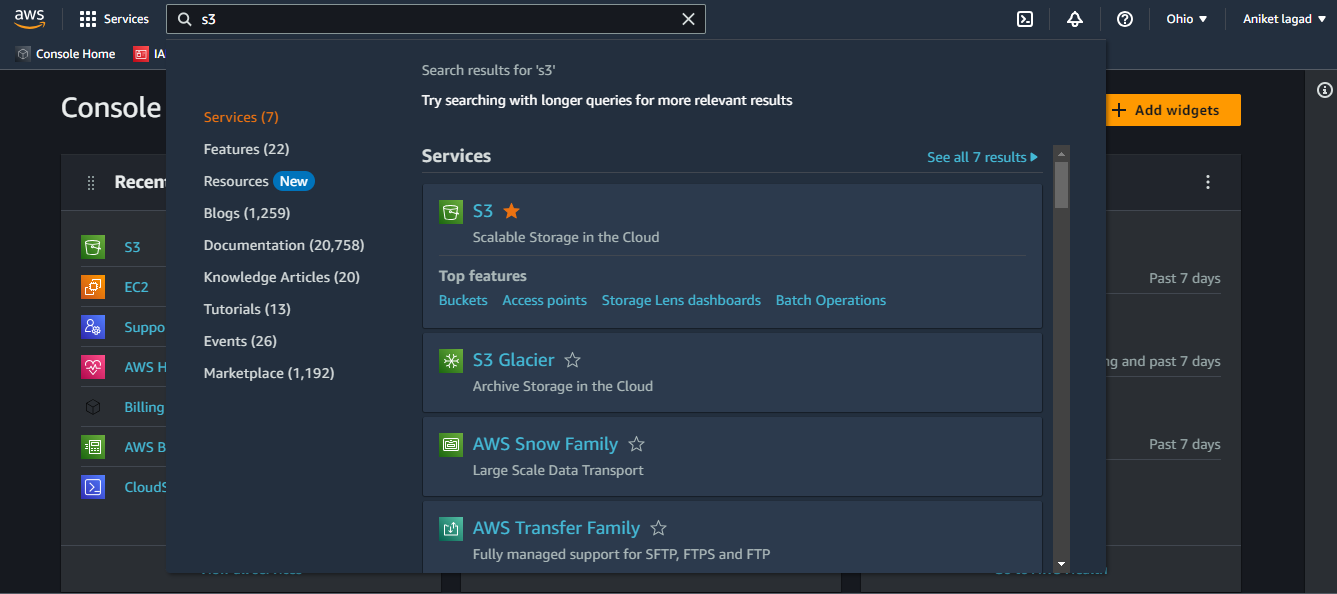
Q.3.Configure cross-region replication for an S3 bucket to replicate the bucket contents to a different region for data redundancy and disaster recovery purposes.

==>

Step 1:-

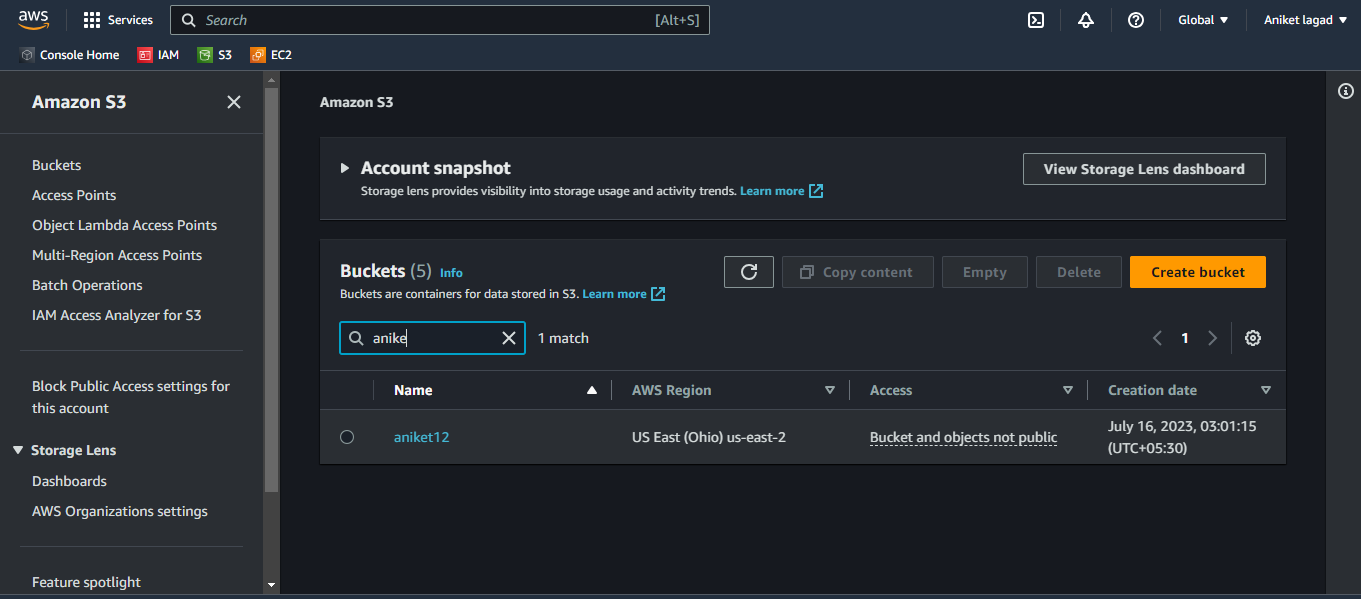
Login to aws account.And after that search s3 service and open it.





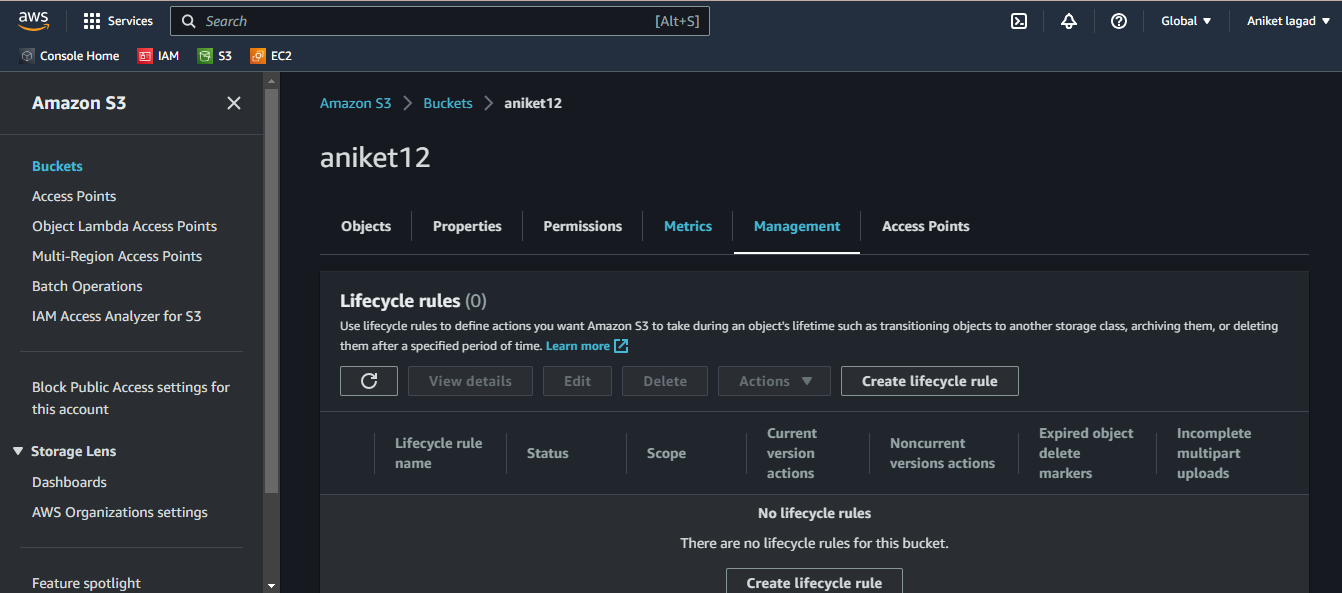
Step 2:-

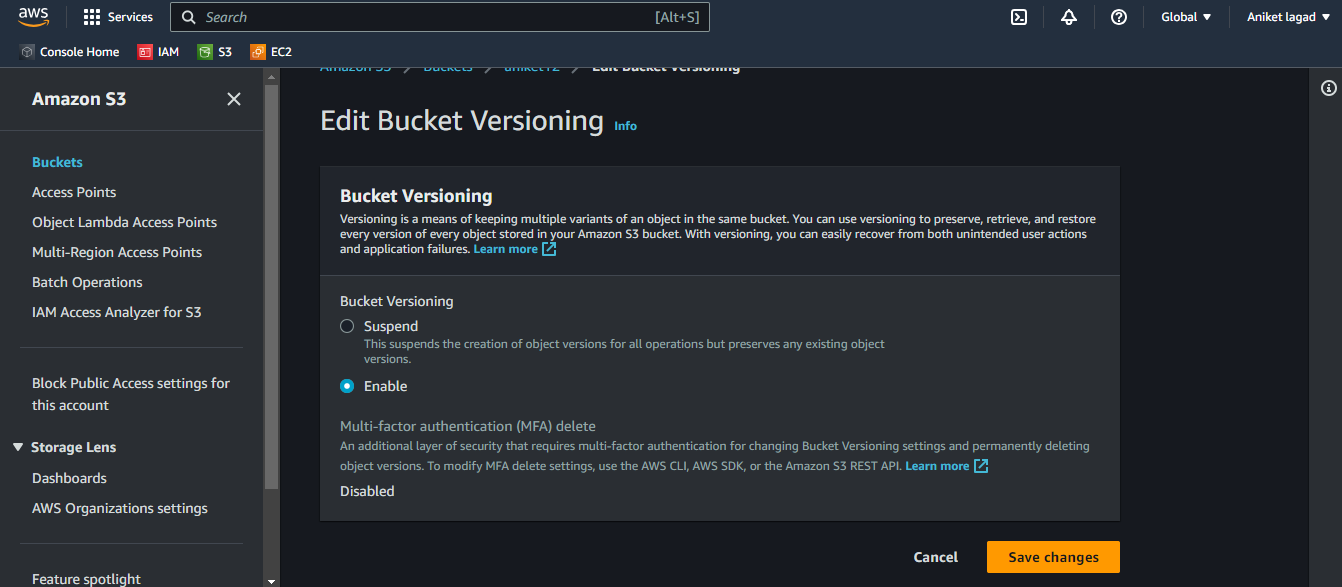
After that select a bucket that you want replicate data.

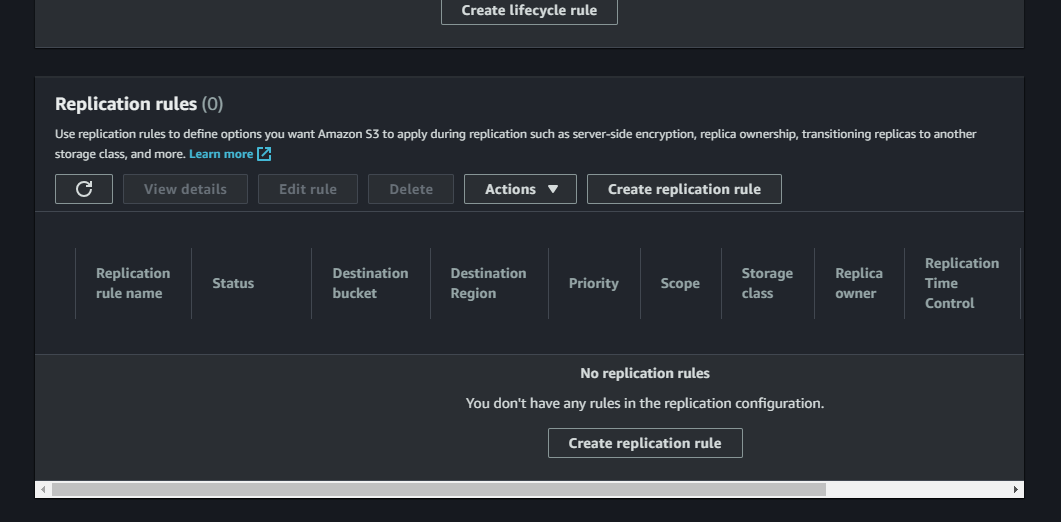


Step 3:-

Now click on management option and go downword and you see replication rule optin clickc on that option to replicate data for you want first to do enable bucket versioning.

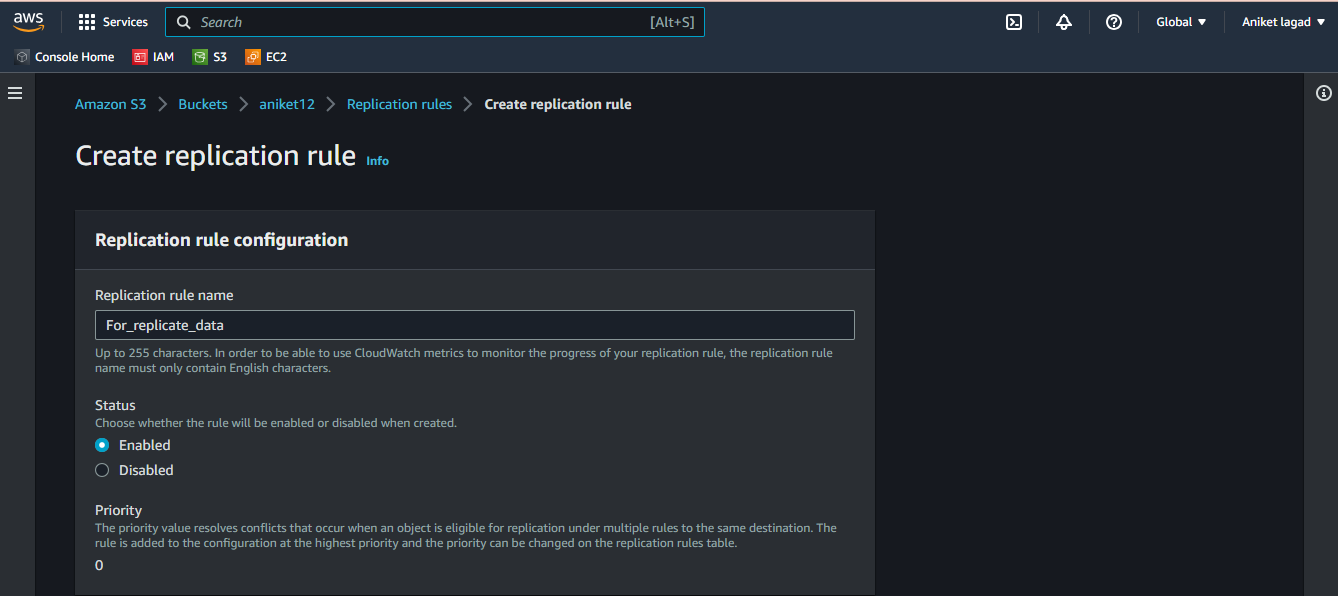






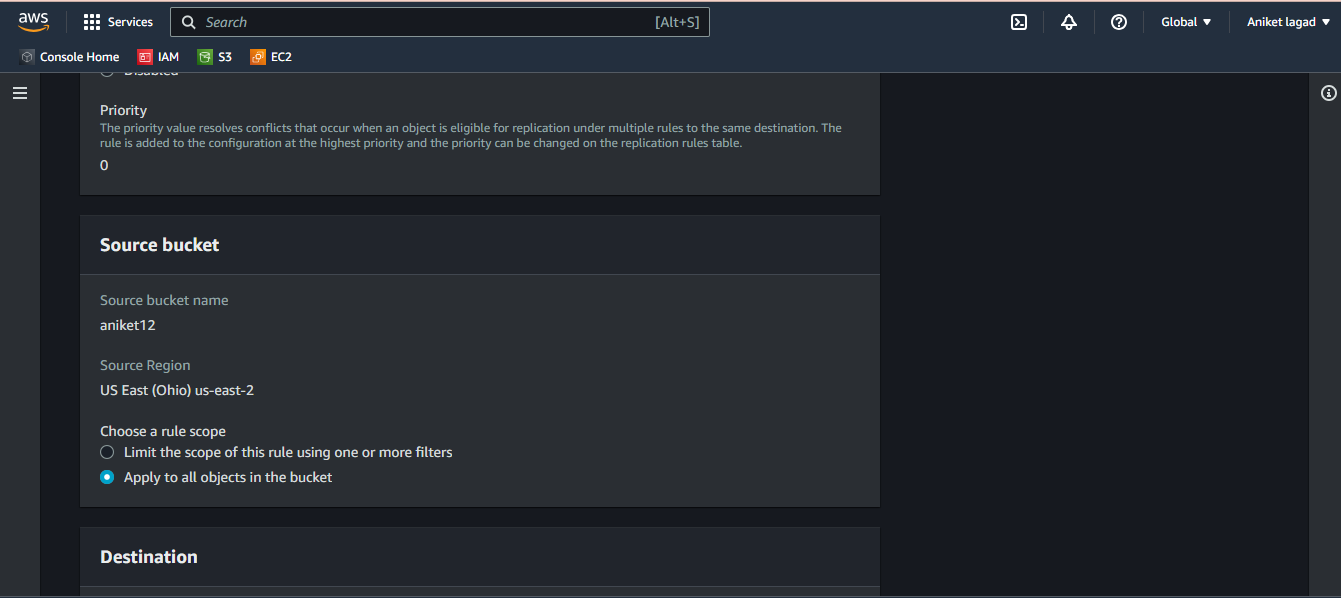
Step 4:-

Next gave a name a replication.and status select on status enabled.

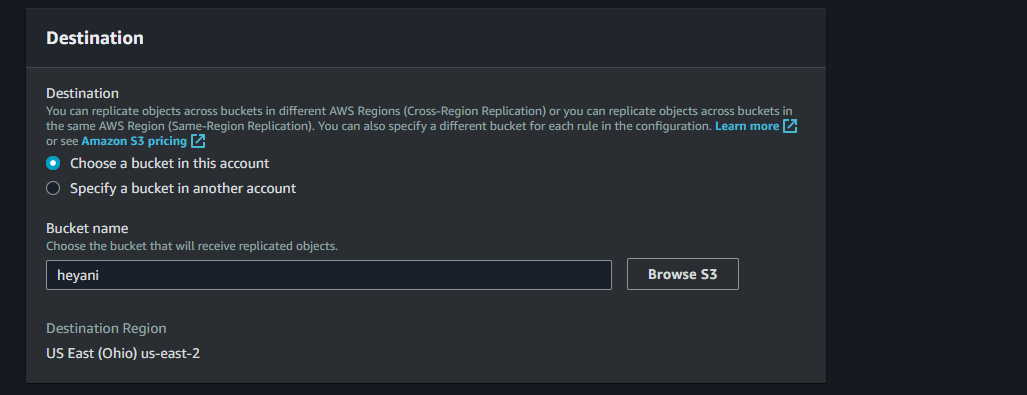


Step 5:-

Now you will see source of bucket and in it choose a rule scope option click on apply to all objects in the bucket.

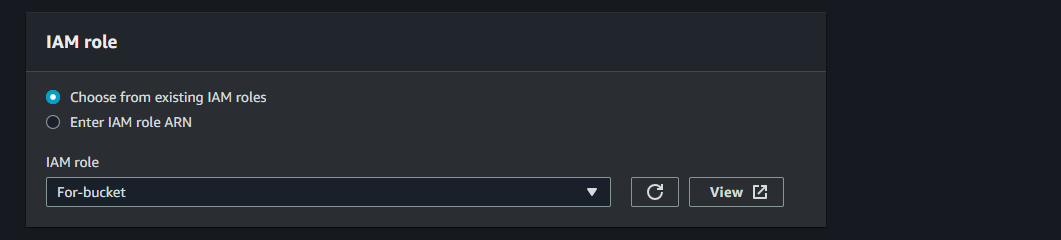


Step 6:-

After that you want select a destination to you want to replicate your bucket.there where 2 options for make a replicate bucket your bucket only and to others account bucket choose where to replicate data. Select it by click on browse s3 you see all region buckets click select on that.

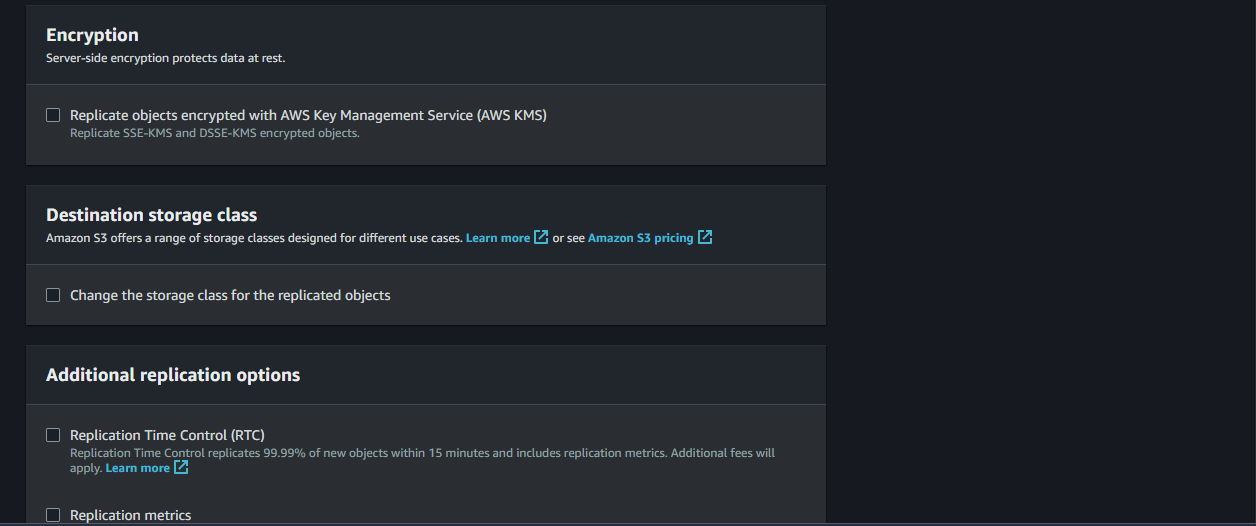
Step 7:-

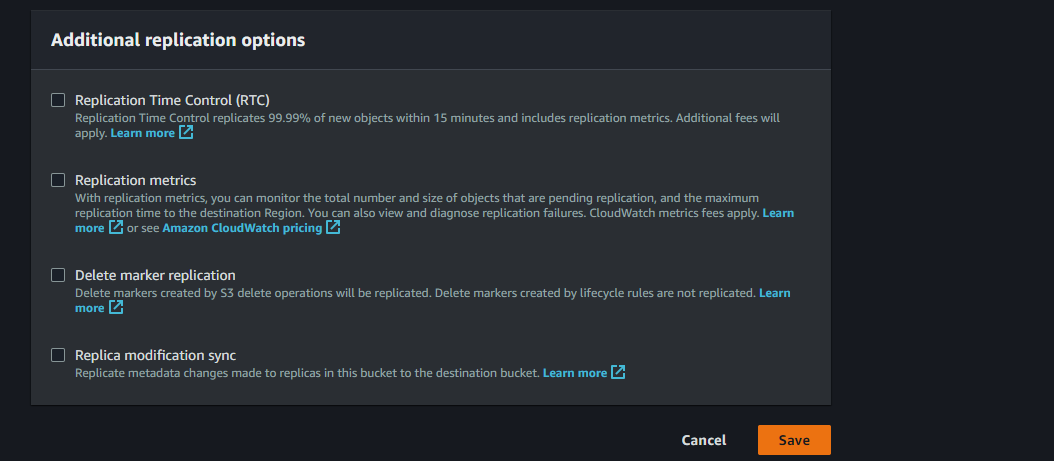
Now choose iam role.



Step 8:-

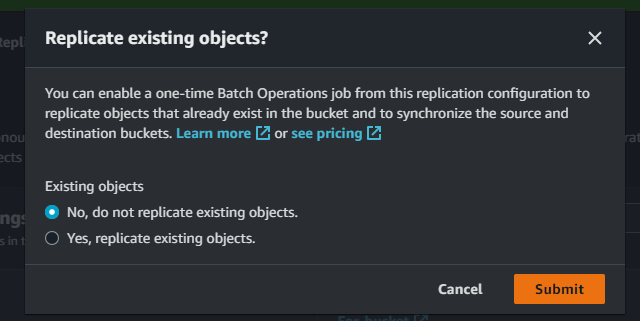
Next you will see extra options are there if you want to select then click on it otherwise leave it and as it is and next click on save.

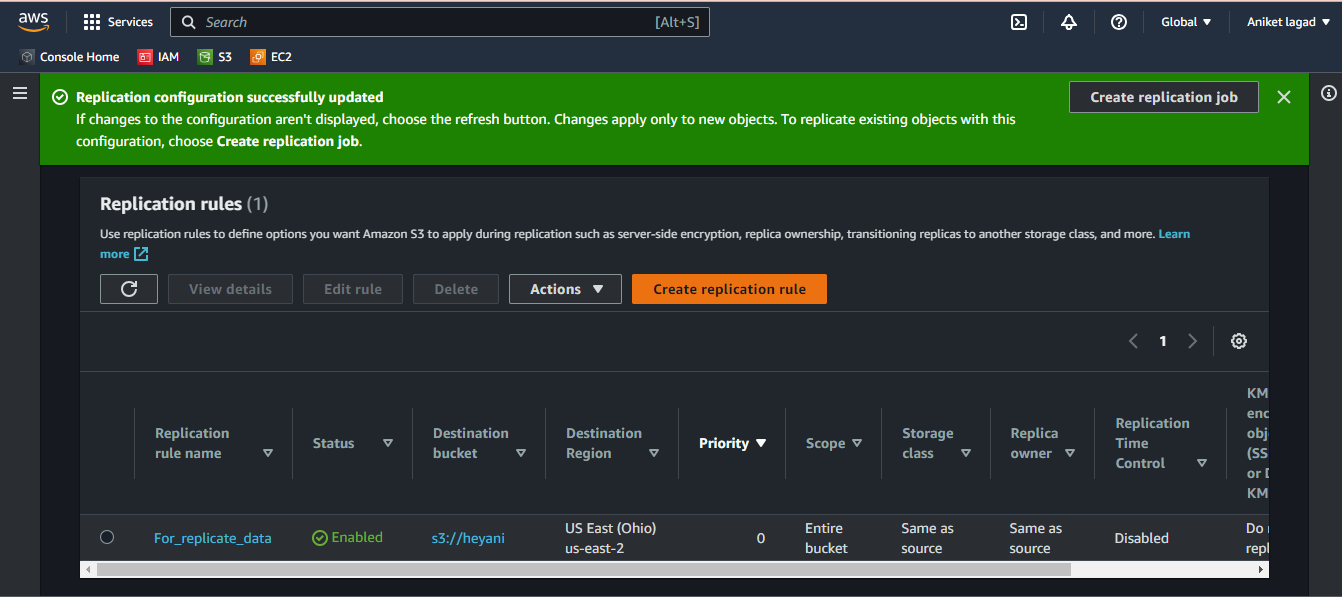




Step 9:-

Last step is next you will see the option to exiting objects if you want to replicate exiting objects then click on it otherwise click on submite and youe data replicate rule is ready.

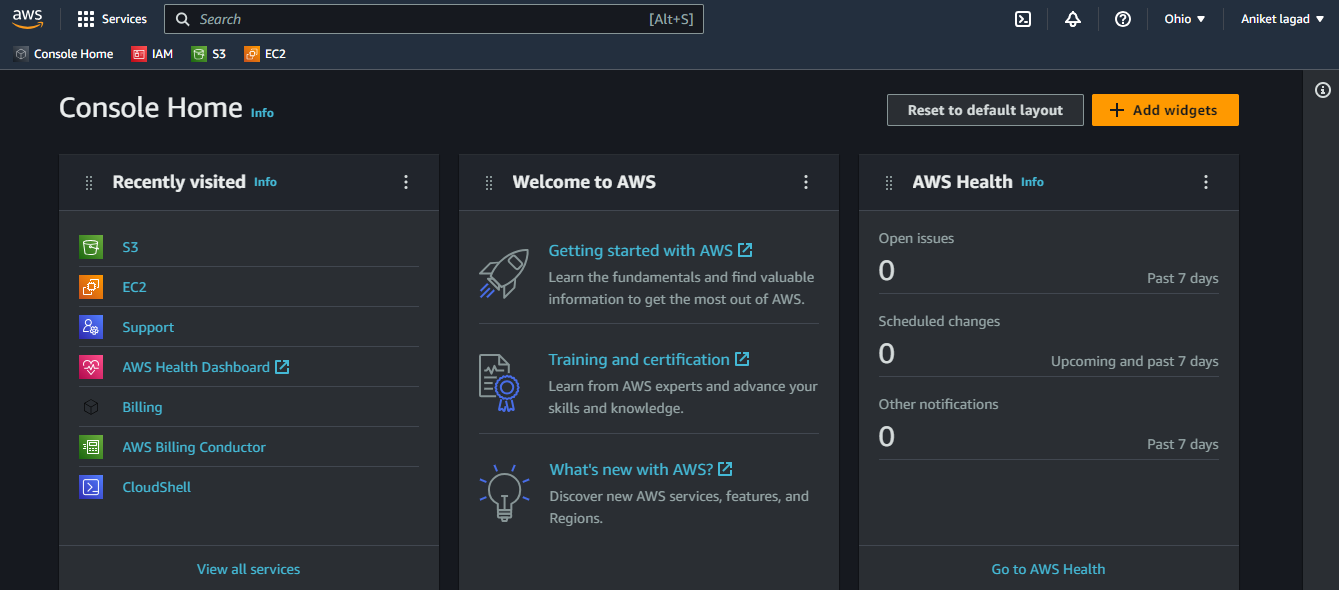


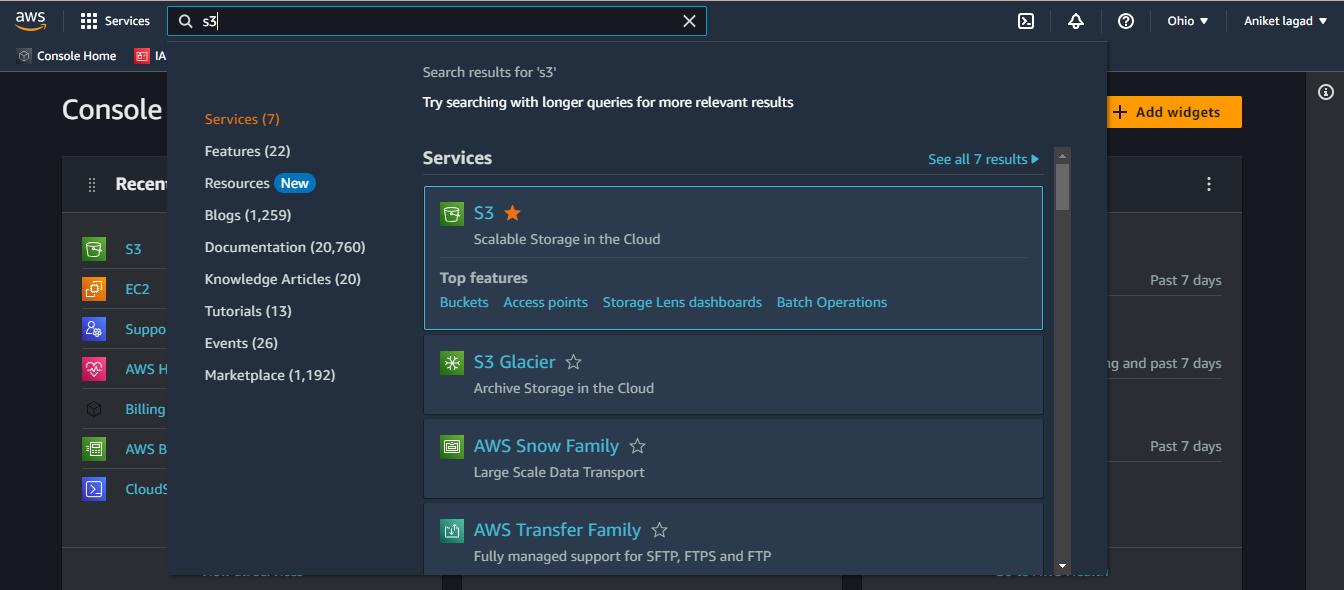


Q.4.Generate pre-signed URLs for specific objects in an S3 bucket, allowing time-limited access to those objects for authorized users.

==>

Step 1:-

First of all login to aws account and then go to s3 service.



Step 2:-

After that click on bucket that you want allowing time limit for sharing by URL.



Step 3:-

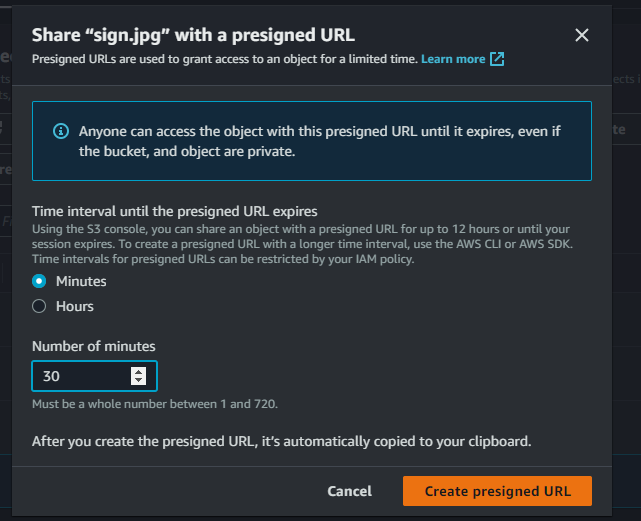
Now select a subject to apply a rule of time limit sharing.

And then click on actions option.There will be a sub-option share with a presigned URL cllikck on it.



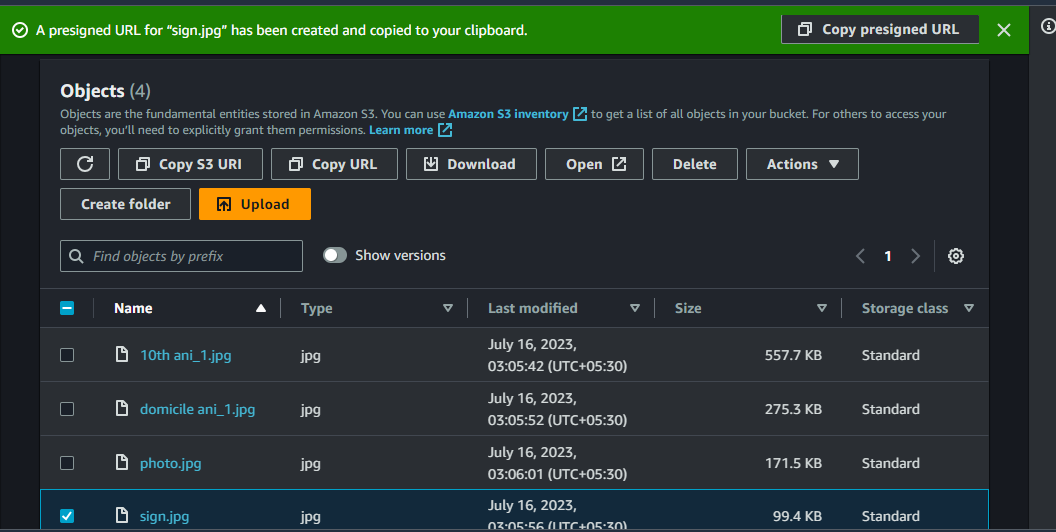
Step 4:-

And next you will see the time interval until the presigned URL exoires and in that minute and hours fileds.Select what you want to select and click on create presigned URl.



Step 5:-

Now copy that presigned URl and send to user who want share.

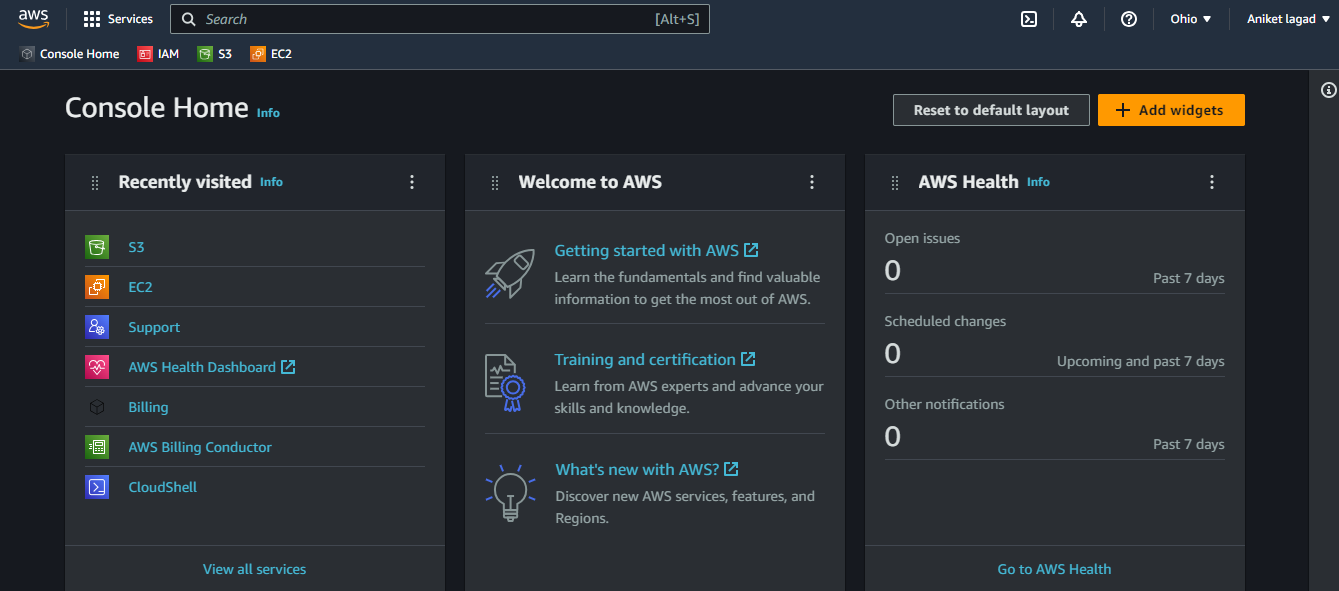


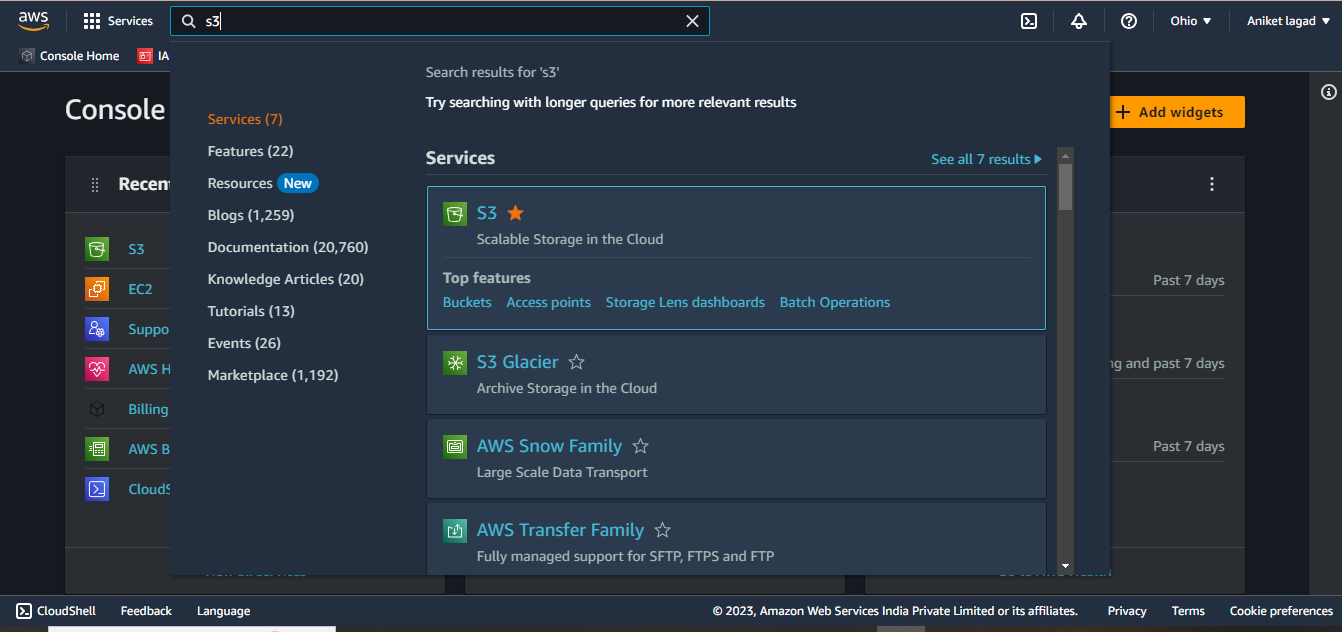
Q.5.create a policy for s3 to prevent deletion of object even for root

🡺

Step 1:-

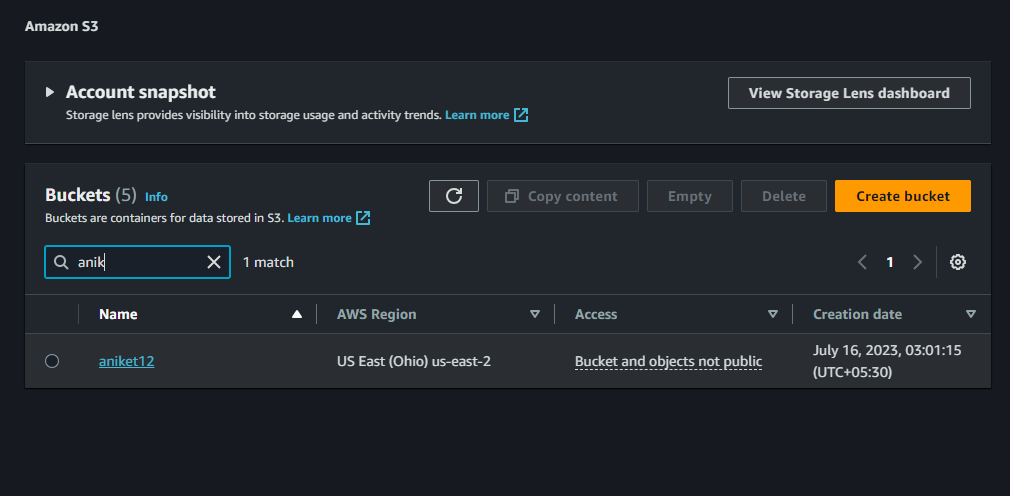
Login to aws account and open s3 service.





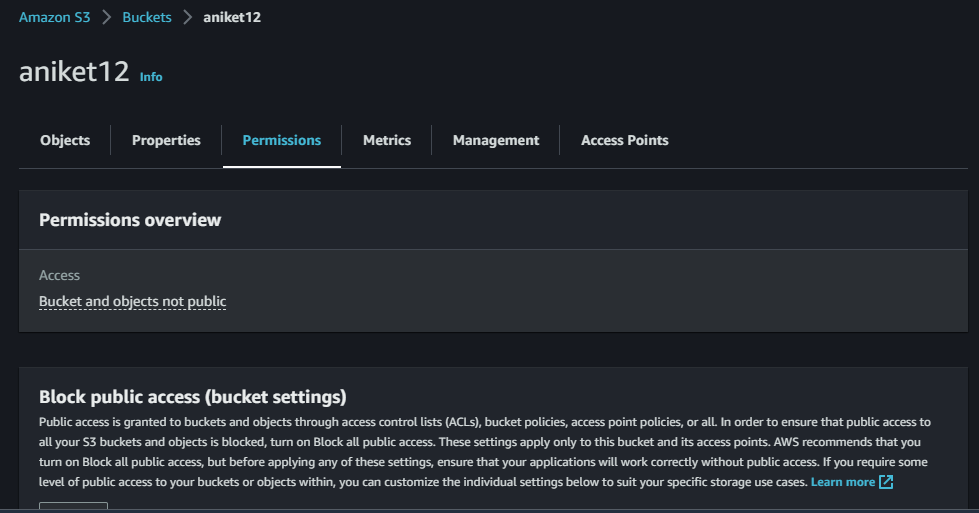
Step 2:-

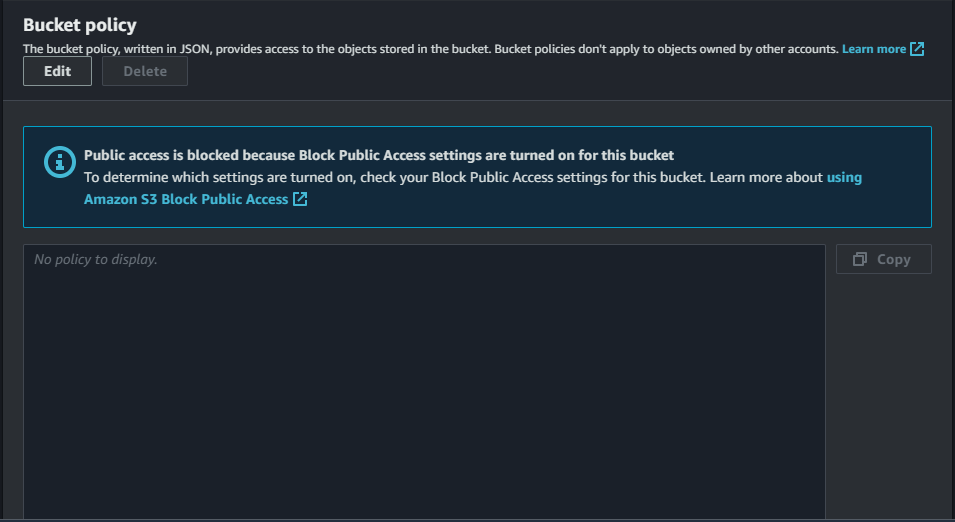
Now click on bucket and enter in it.



Step 3:-

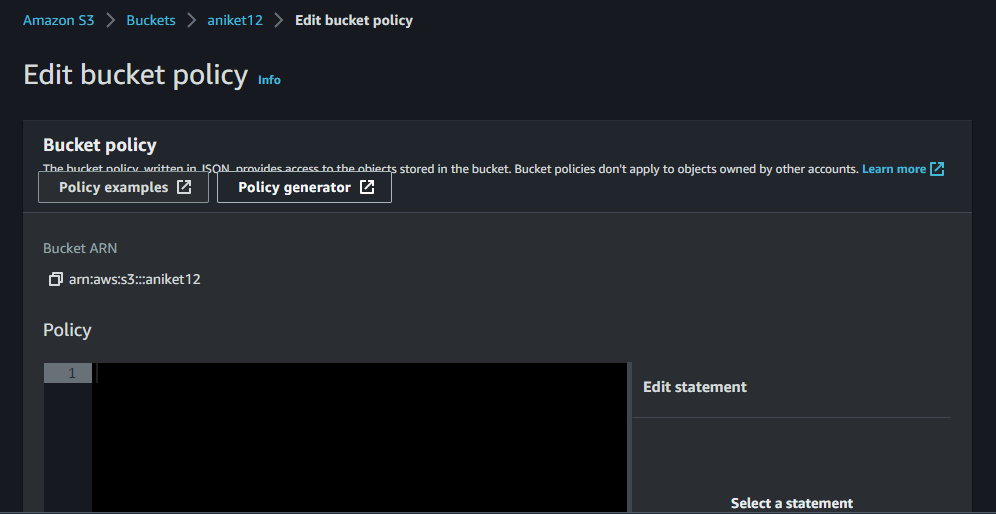
After that you see permissions option and click on that and scroll down you see bucket policy option in that you have to click on edit.





Step 4:-

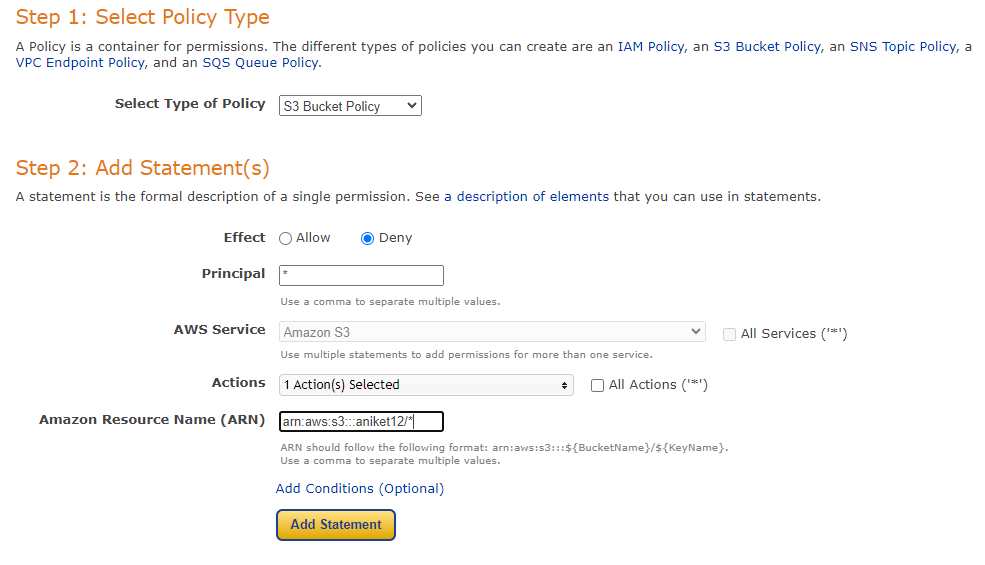
Now you have to click on policy generator and generate policy of deny policy of delete object.



Step 5:-

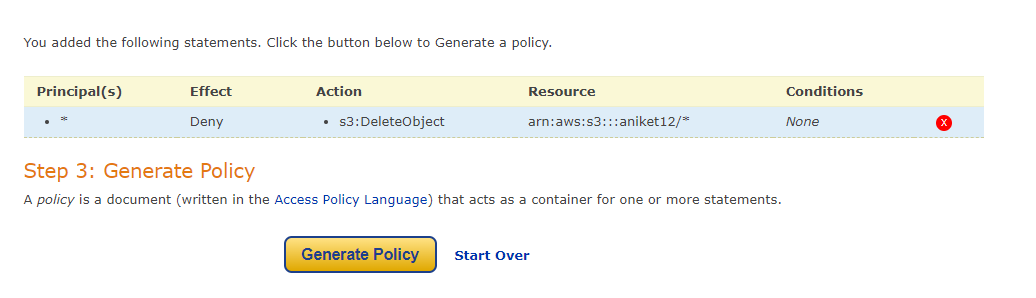
After you have go to aws policy generator.

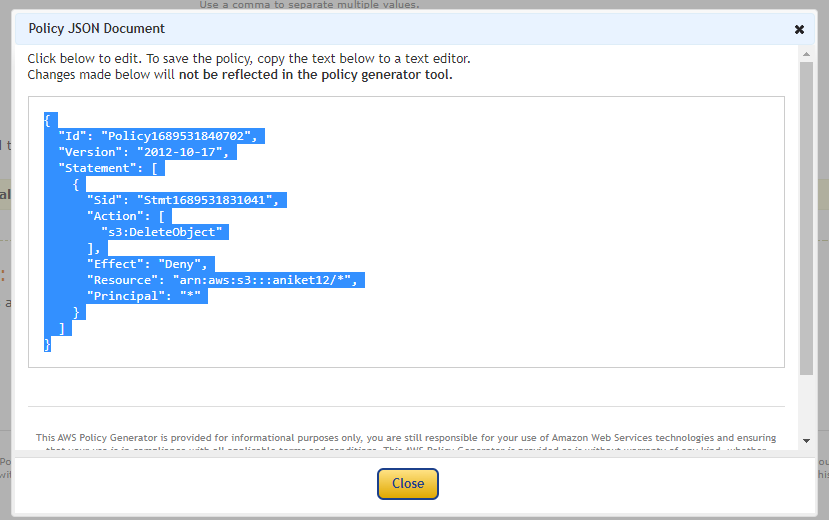
In select policy select s3 bucket policy. And in effect select deny and in principle colum put \*. After that auto select aws service amazon s3. And in actions select delete object policy and after that in ARN column put bucket ARN and end of ARN put /\*. And click on add statement.



Step 6:-

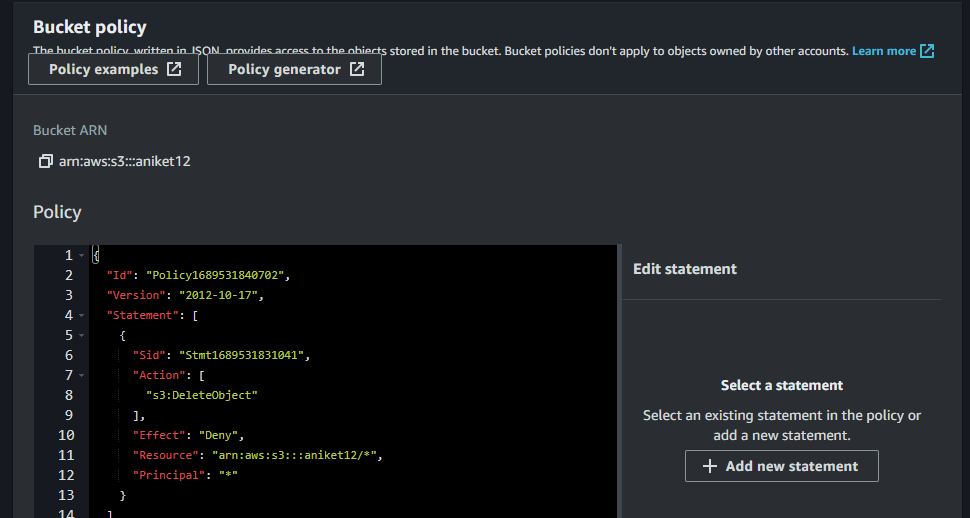
Now you have to click on generate policy and after copy that policy and go to bucket policy.

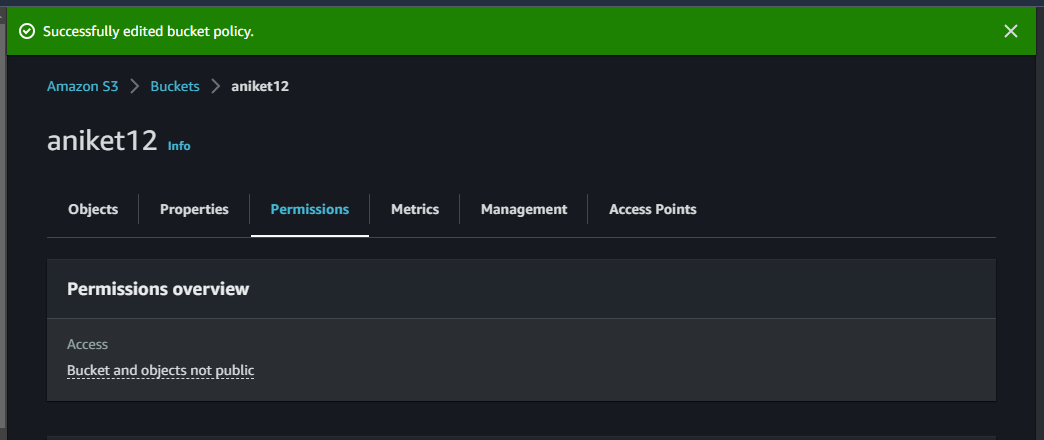




Step 7:-

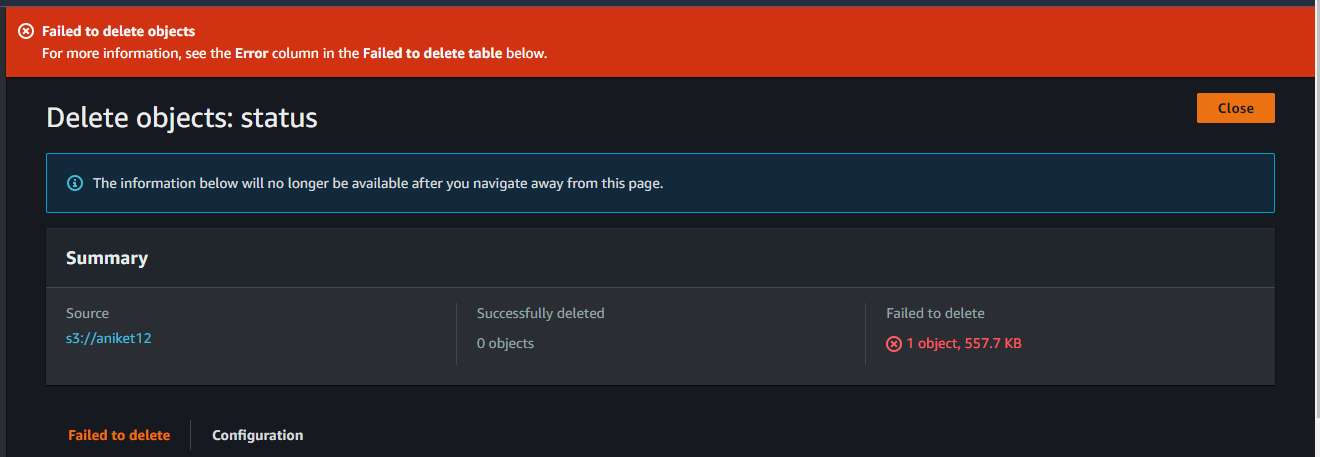
Now click on add statement and paste that policy in it and save changes.





Step 8:-

Now see root account also can not delete that buckets objects so it has applied deny permission.

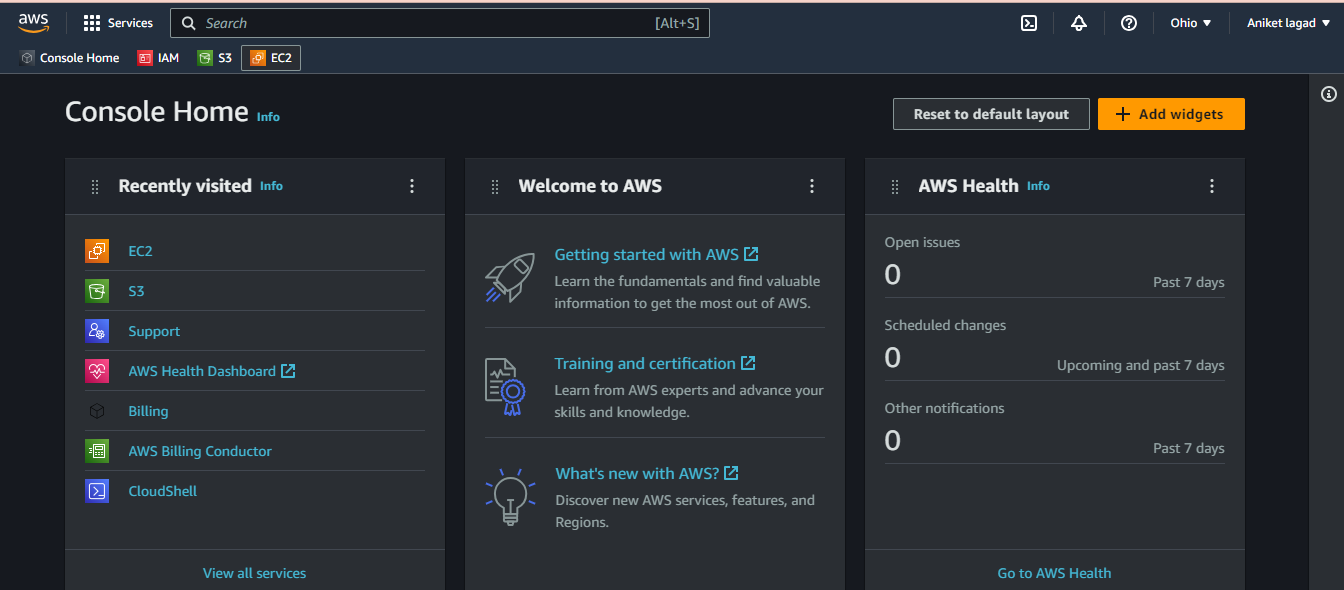


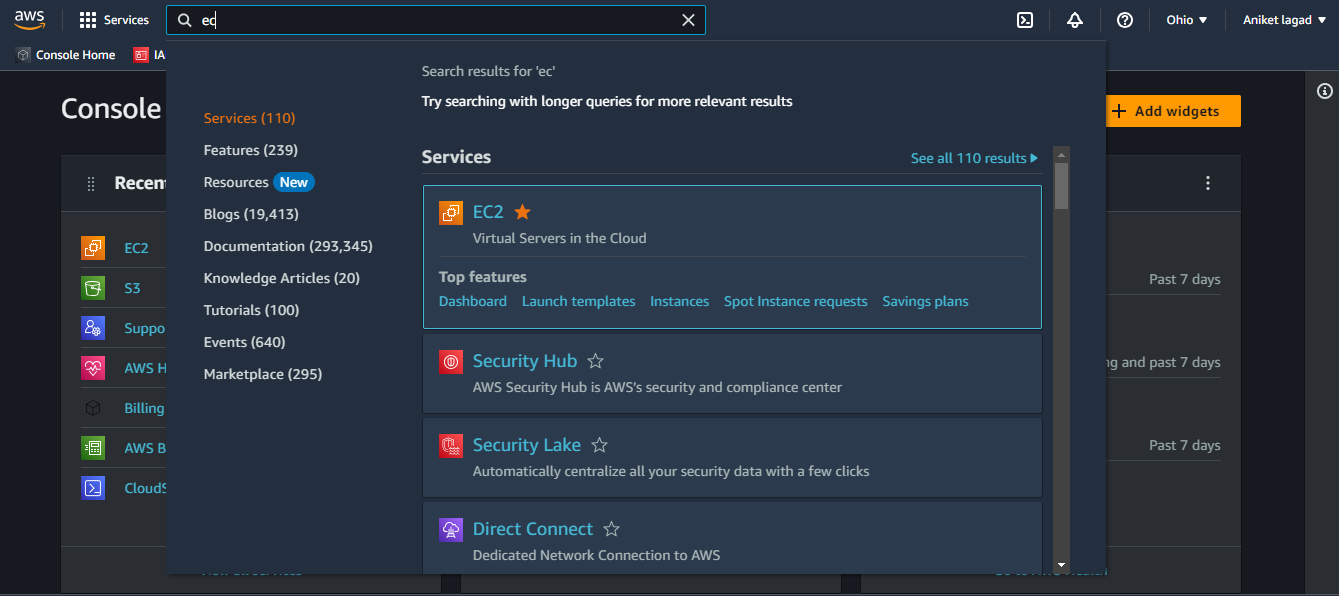
Q.6.Create a custom Amazon Machine Image (AMI) from an existing EC2 instance, which can be used to launch identical instances in the future.share the AMI with other account.

🡺

Step 1:-

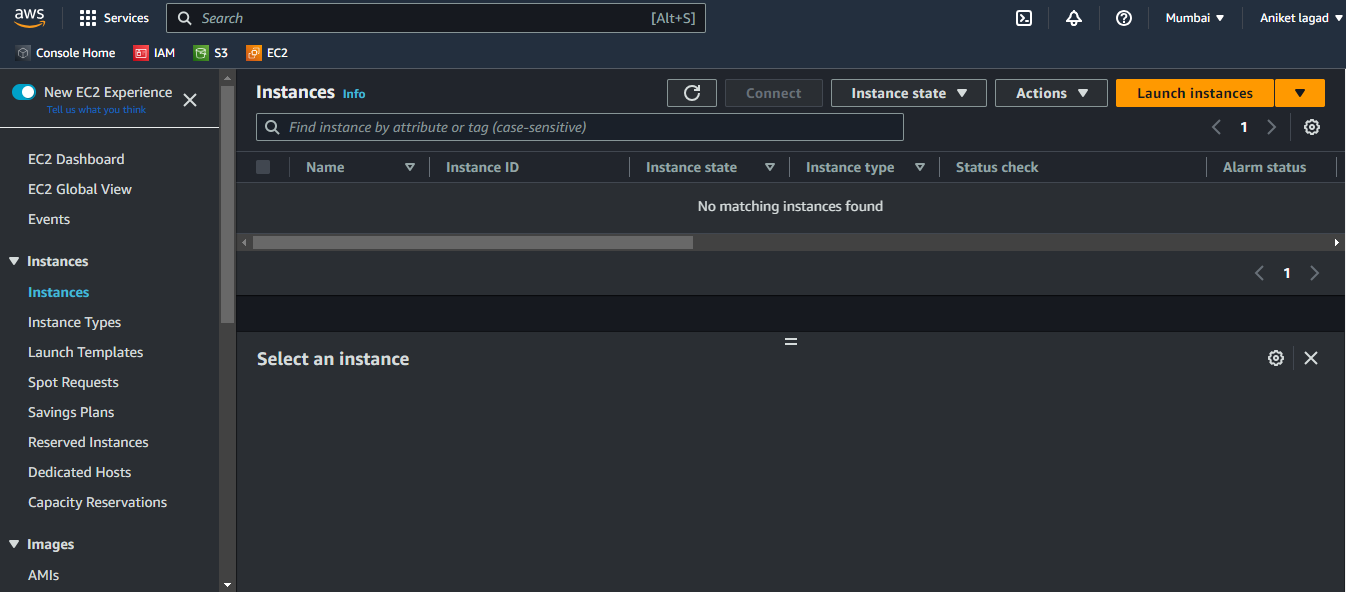
Login aws account and go to ec2 service.





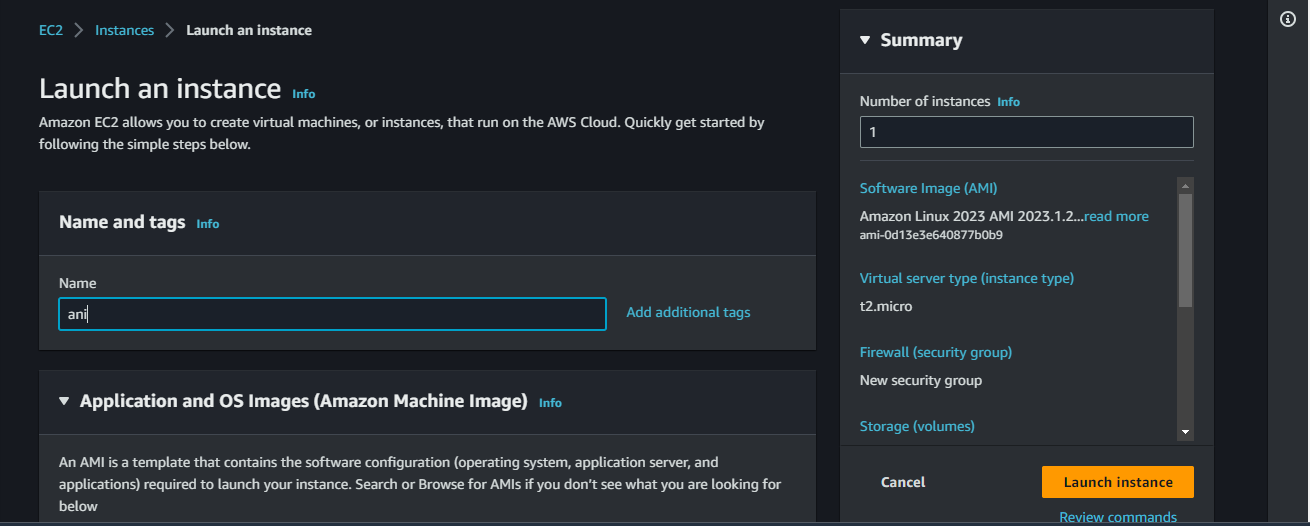
Step 2:-

Create a instance by following steps.First click on create instance.



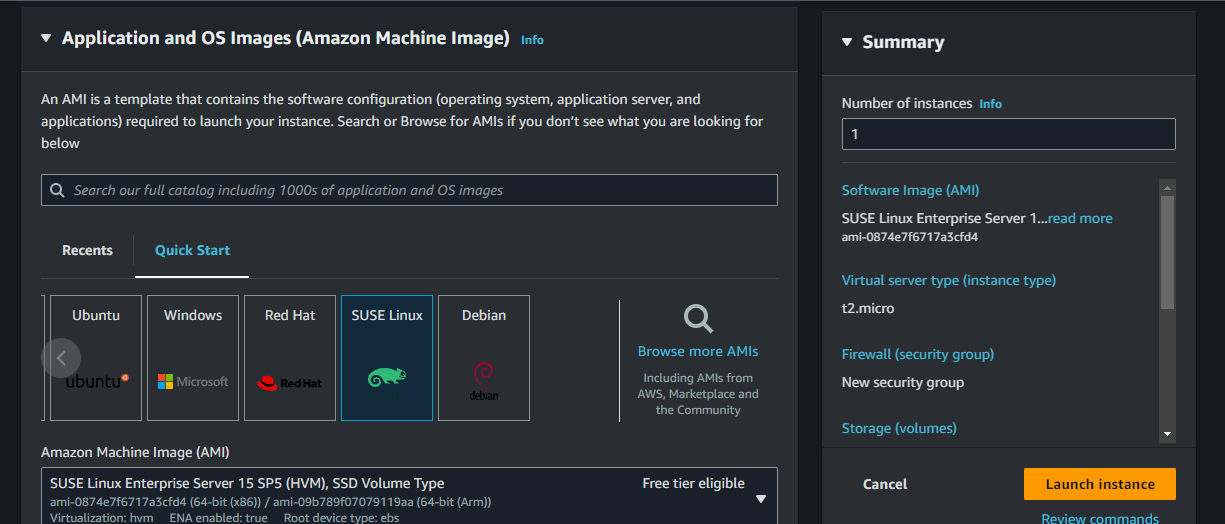
Step 2:-

Gave a instance name.



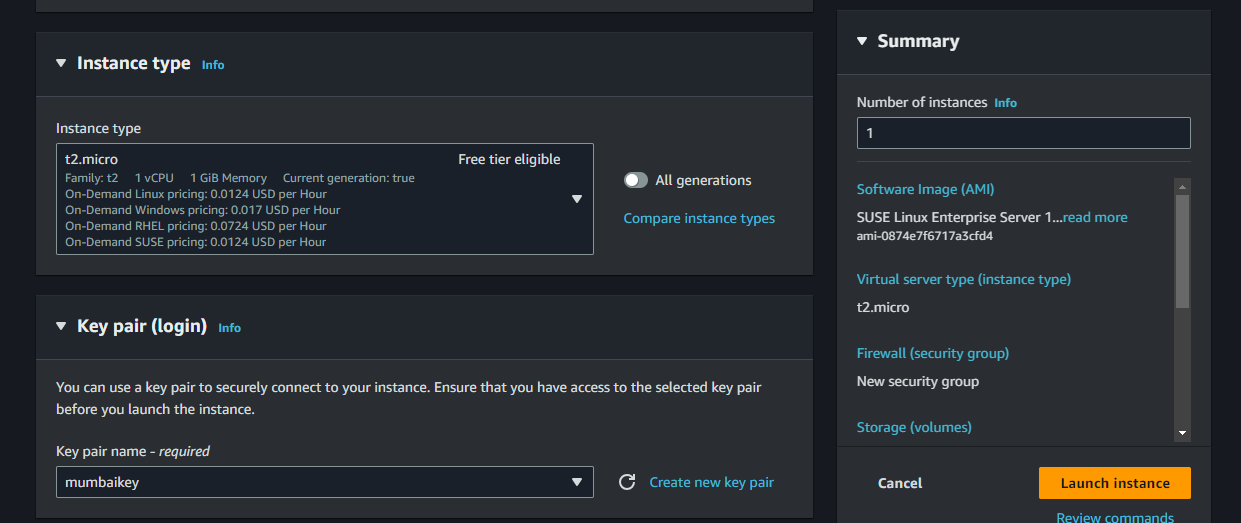
Step 3:-

Next select a image to launch a instance.

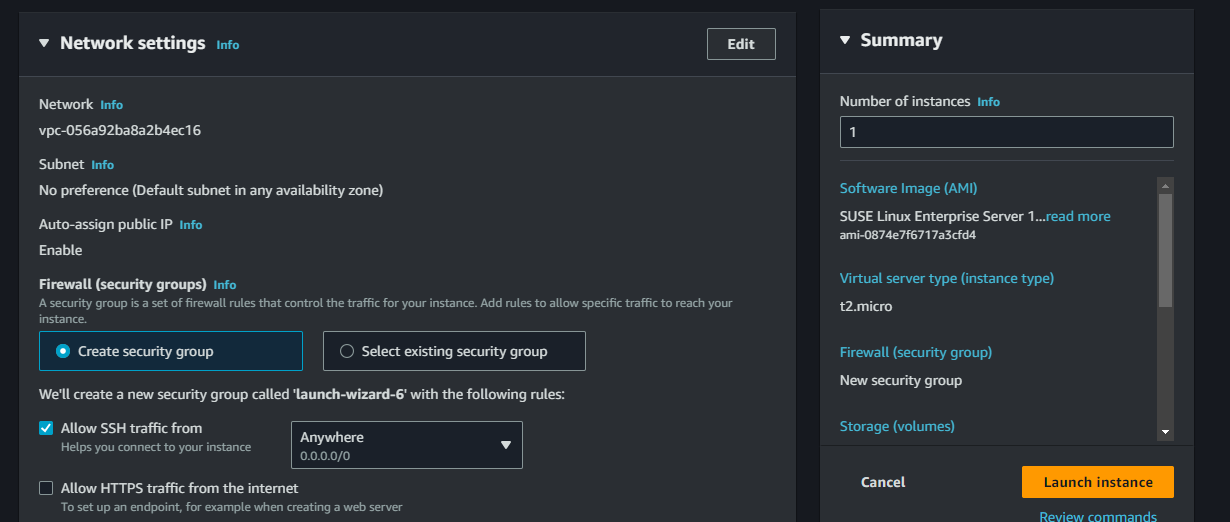


Step 4:-

Next you will see instance type by default it select if you want to change you can also change. And next add already created region key or create new pair.



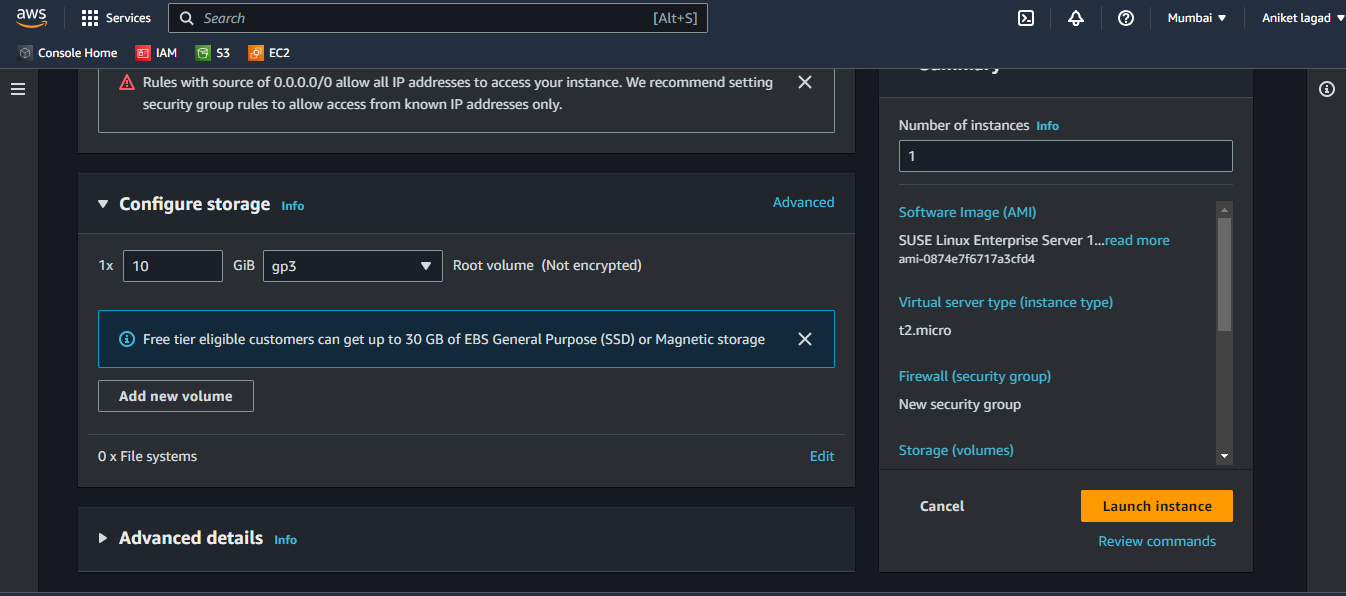
Step 5:-

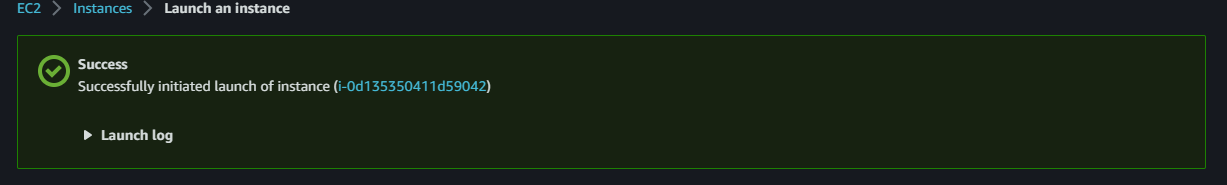
Now you want add firewall/sercurity groups of services.

Step 6:-

Oky now you see the configure storage option in it you to gave storage to instace.

And after that launch a instancee.

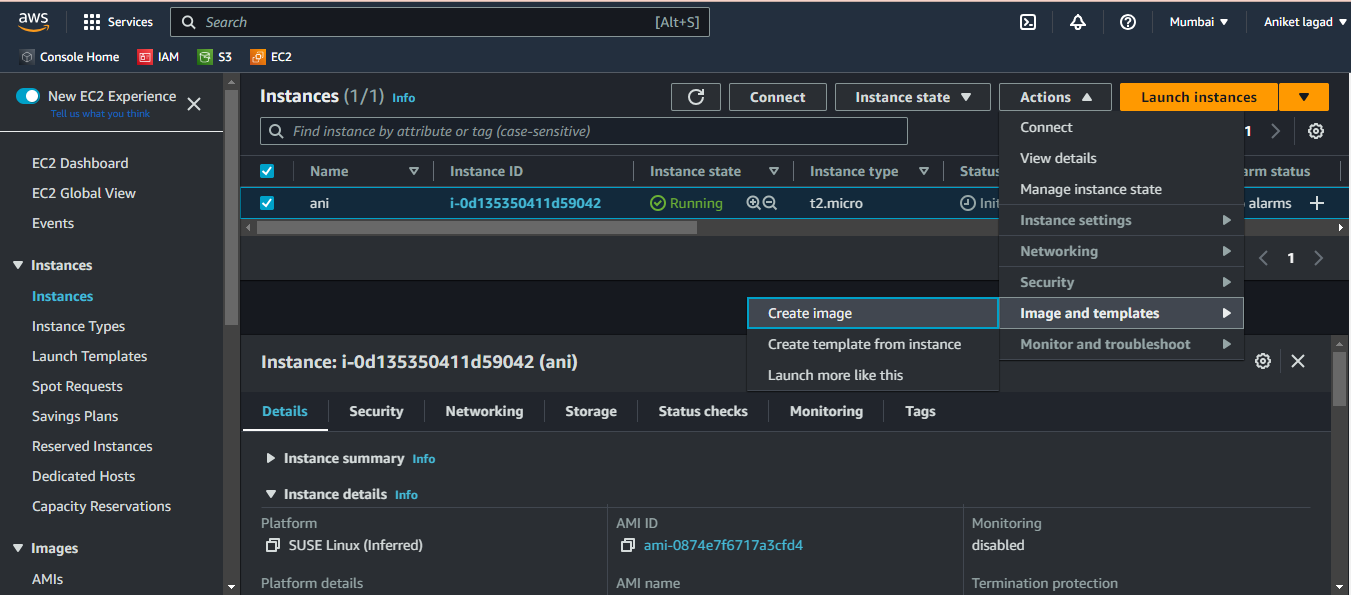




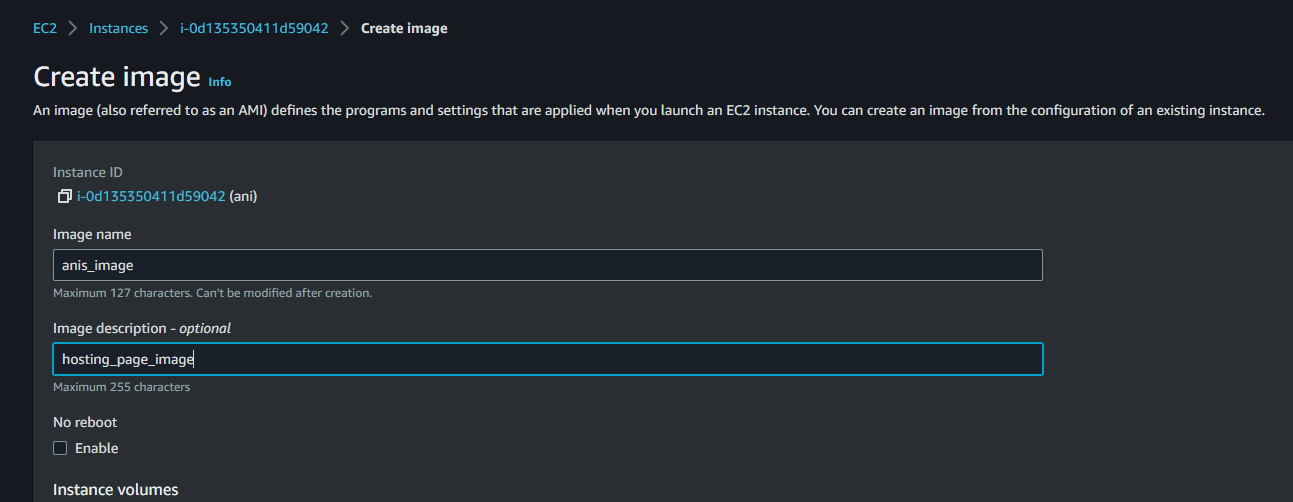
Step 7:-

Now go to instance section where all instanc are see.

And select your instance and click on actions after that you will see the sub-option image and templates click on it and after that create image.

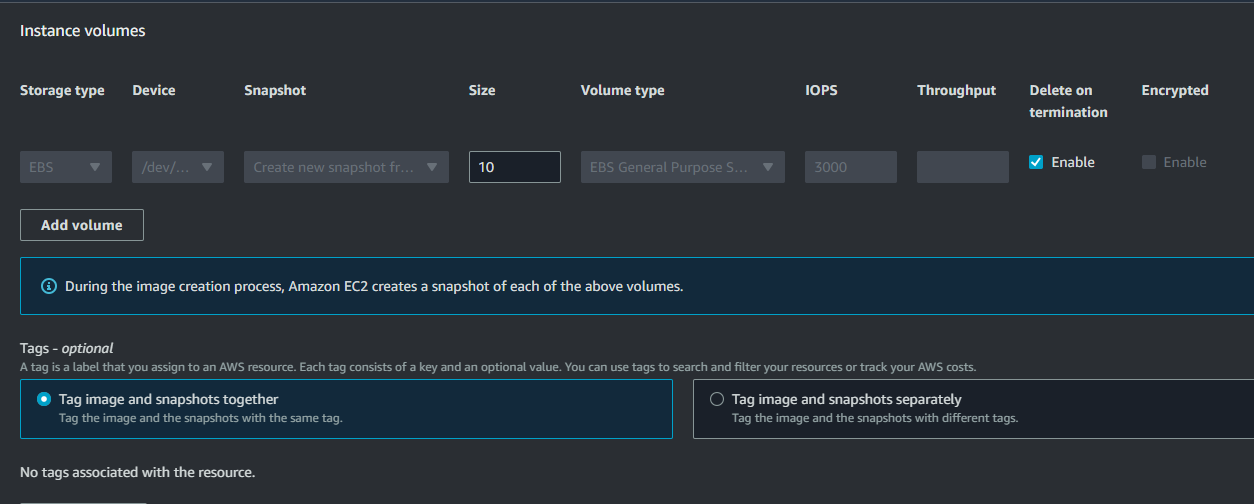


Step 8:-

now you will see the create image section. Gave a image name and image description. 

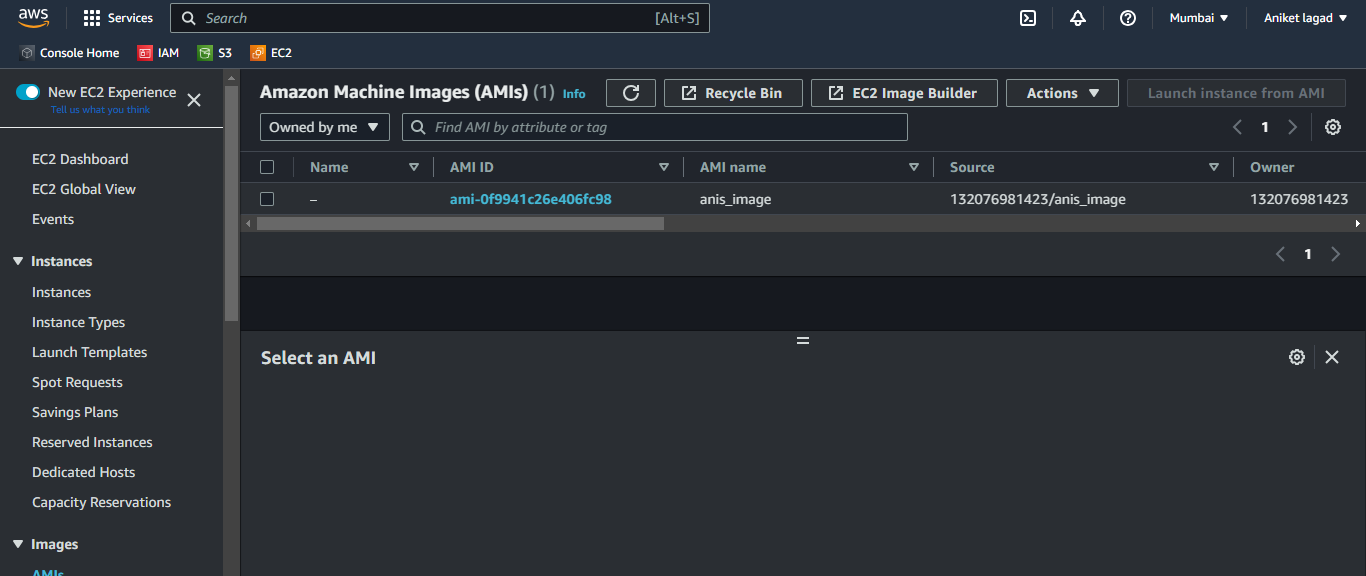
Step 9:-

After that gave instance volume or leave it to by default volume.

And select image and snapshot you want together or separately. And click on create image and your image was created.

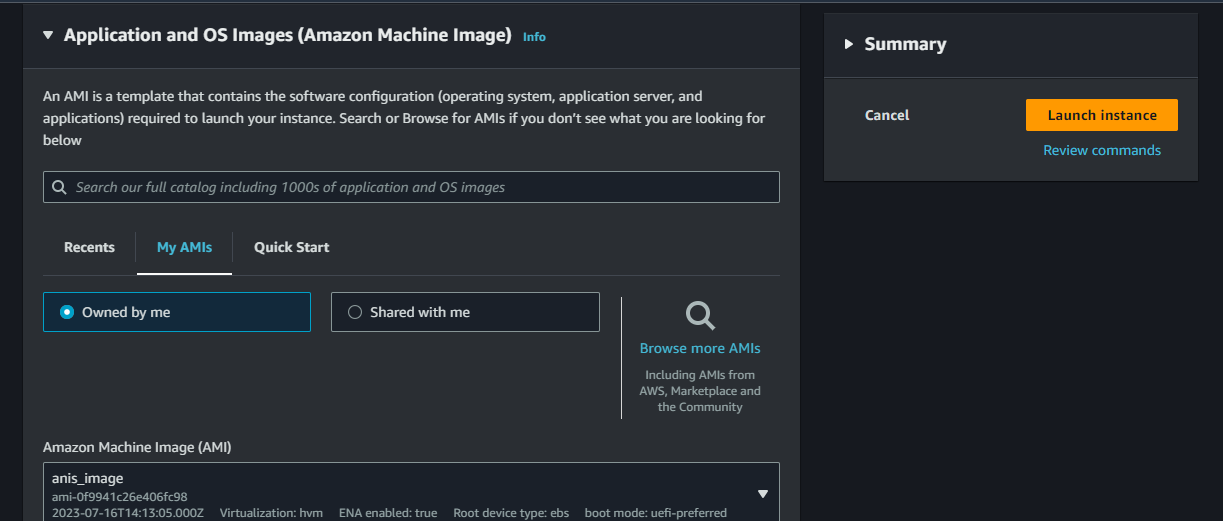
Step 10:-

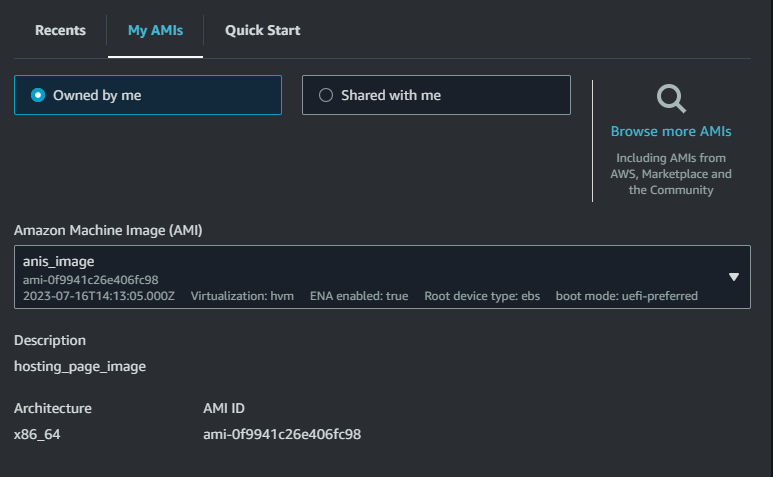
Your image are see in AMIs section.



Step 11:-

Now whenever you want to get that image back to attach instance you create instance and attach to instance. See following images to how to attach image to instance. And you will be back your instance with all services.





\*\*\* End \*\*\*