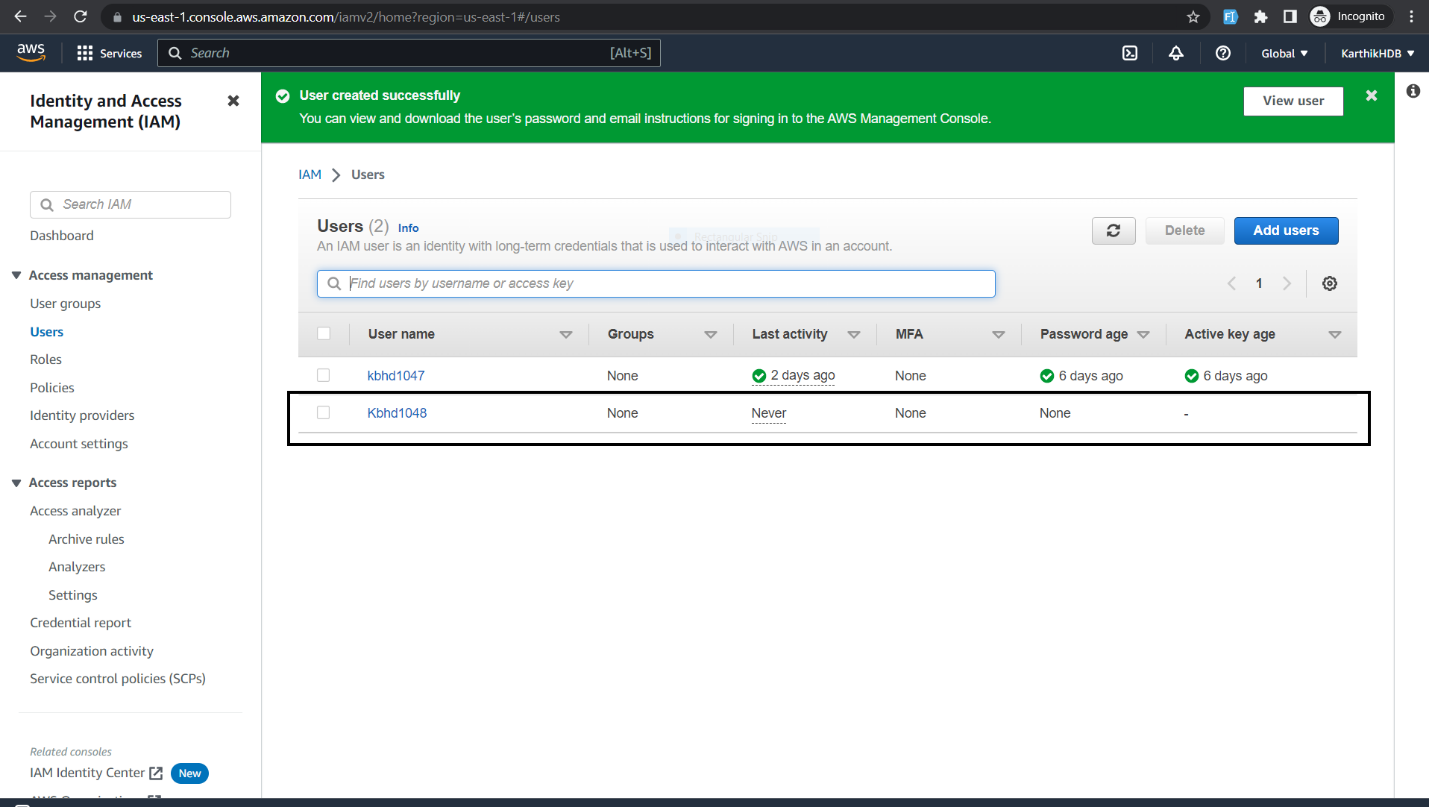
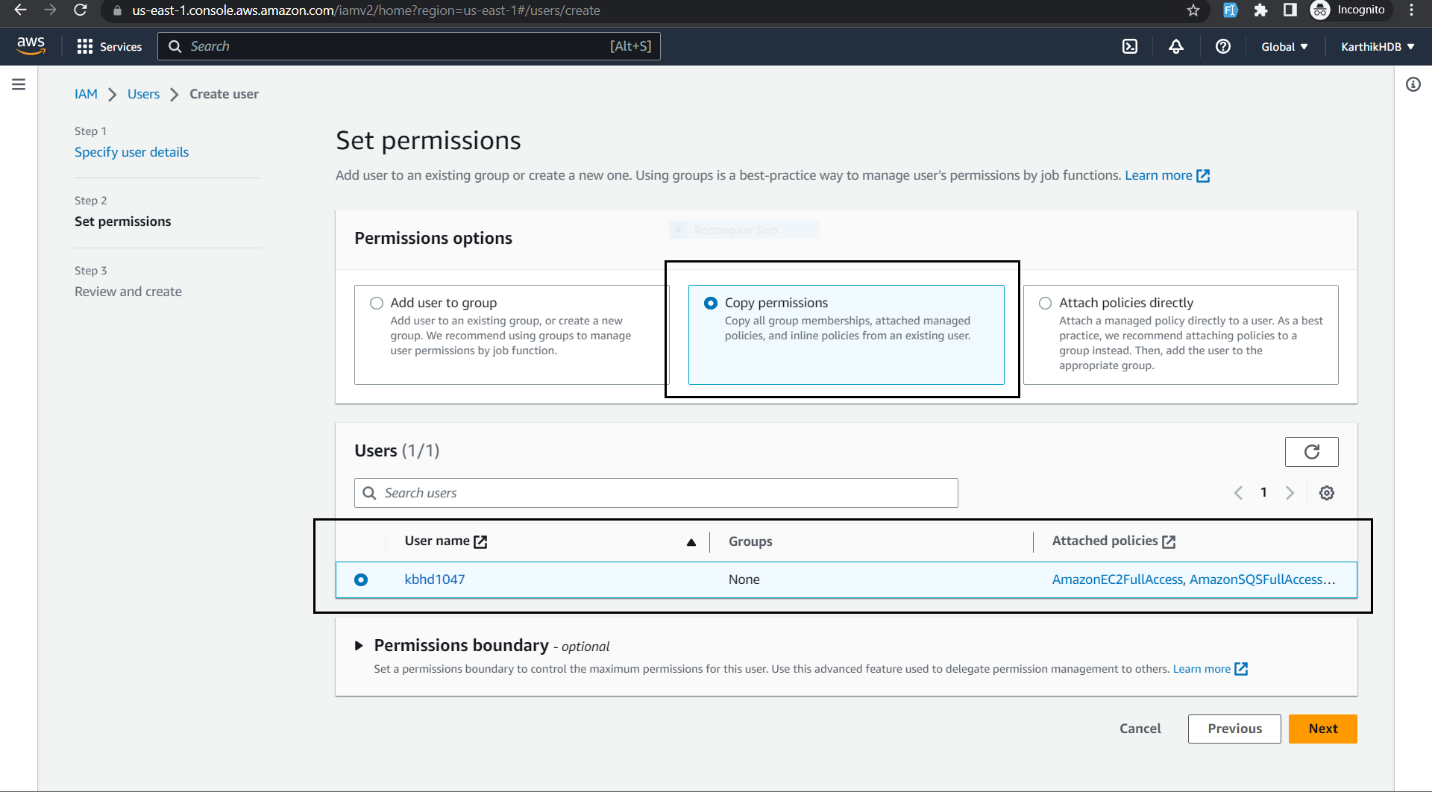
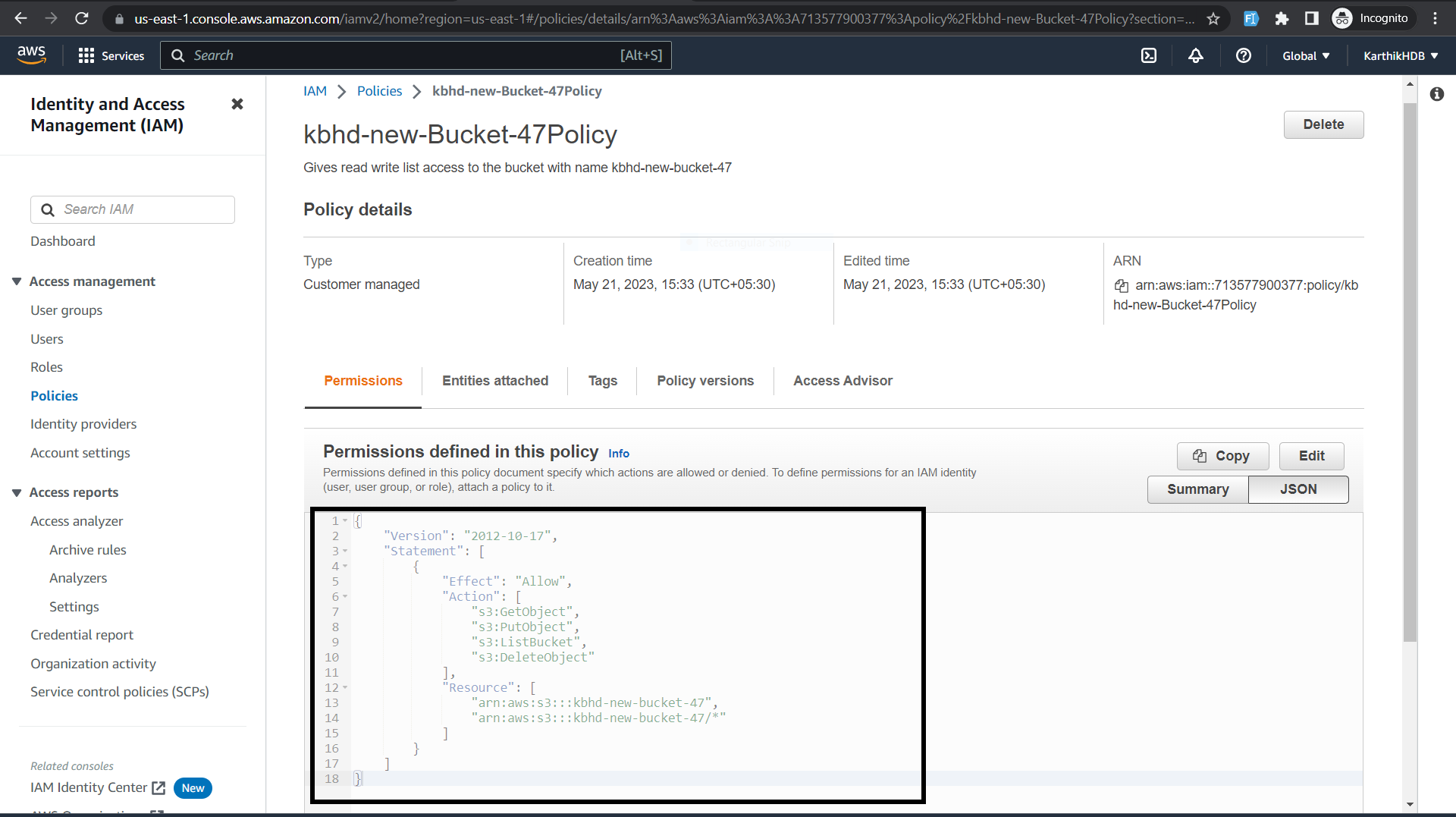
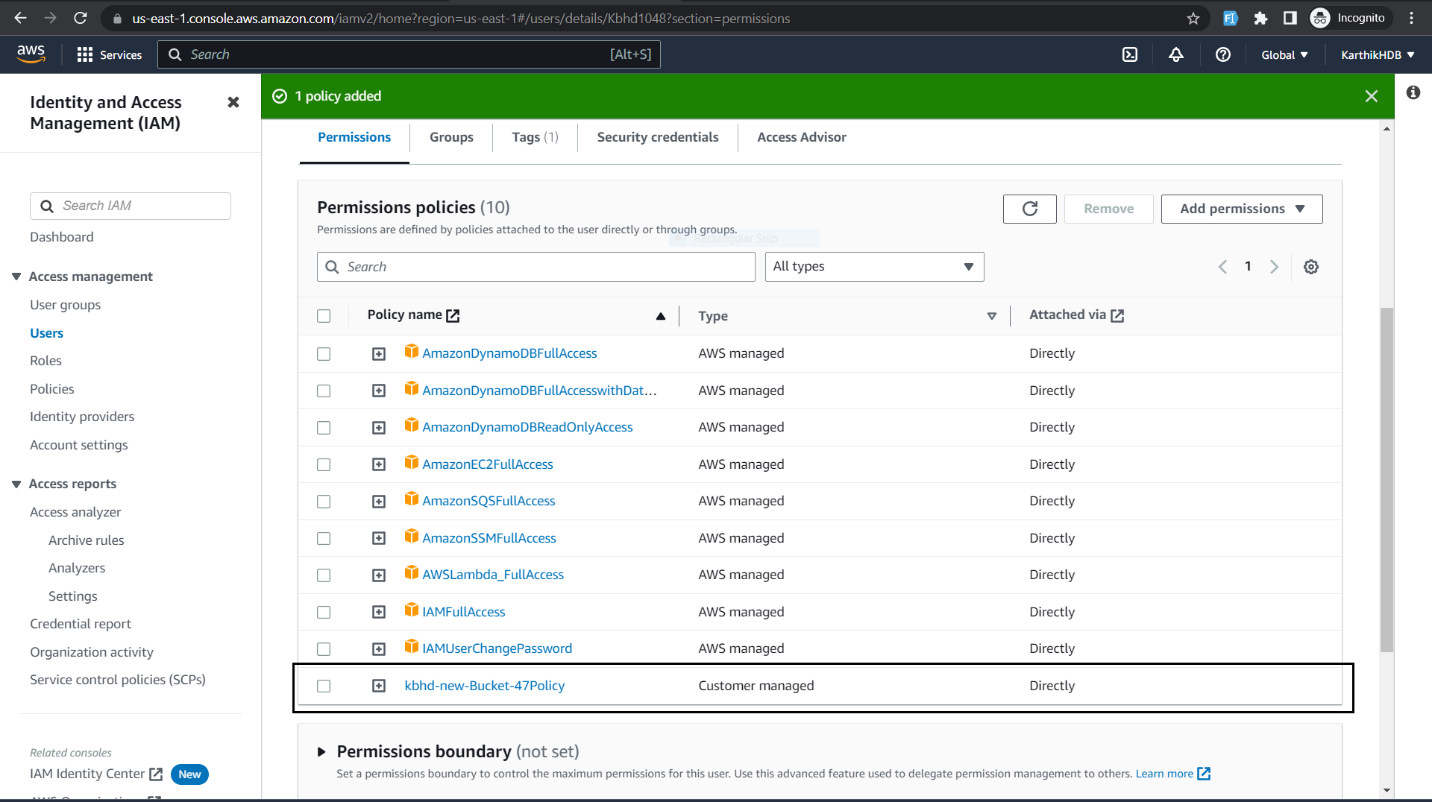
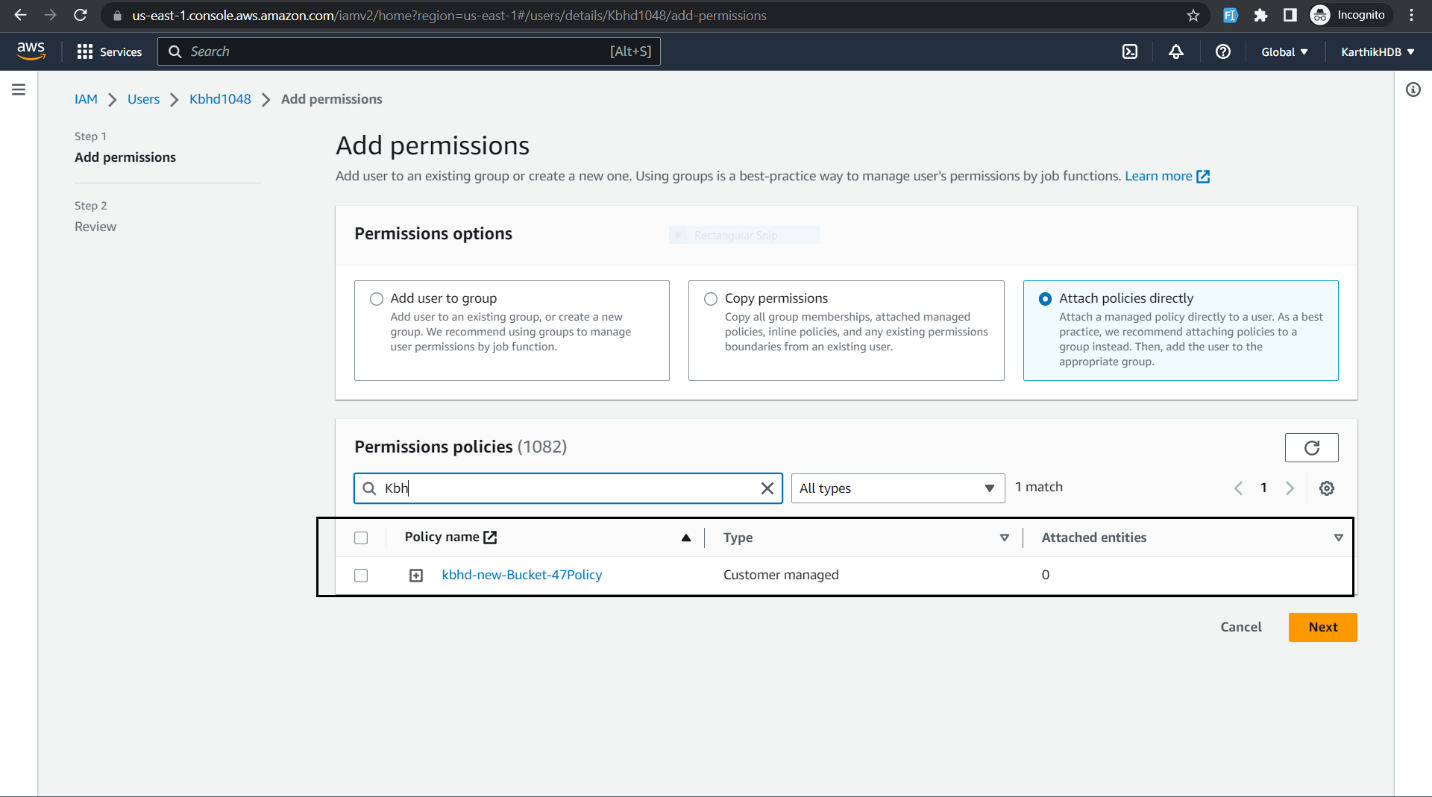
1. Create a new IAM user with programmatic access only and generate an access key and secret access key.

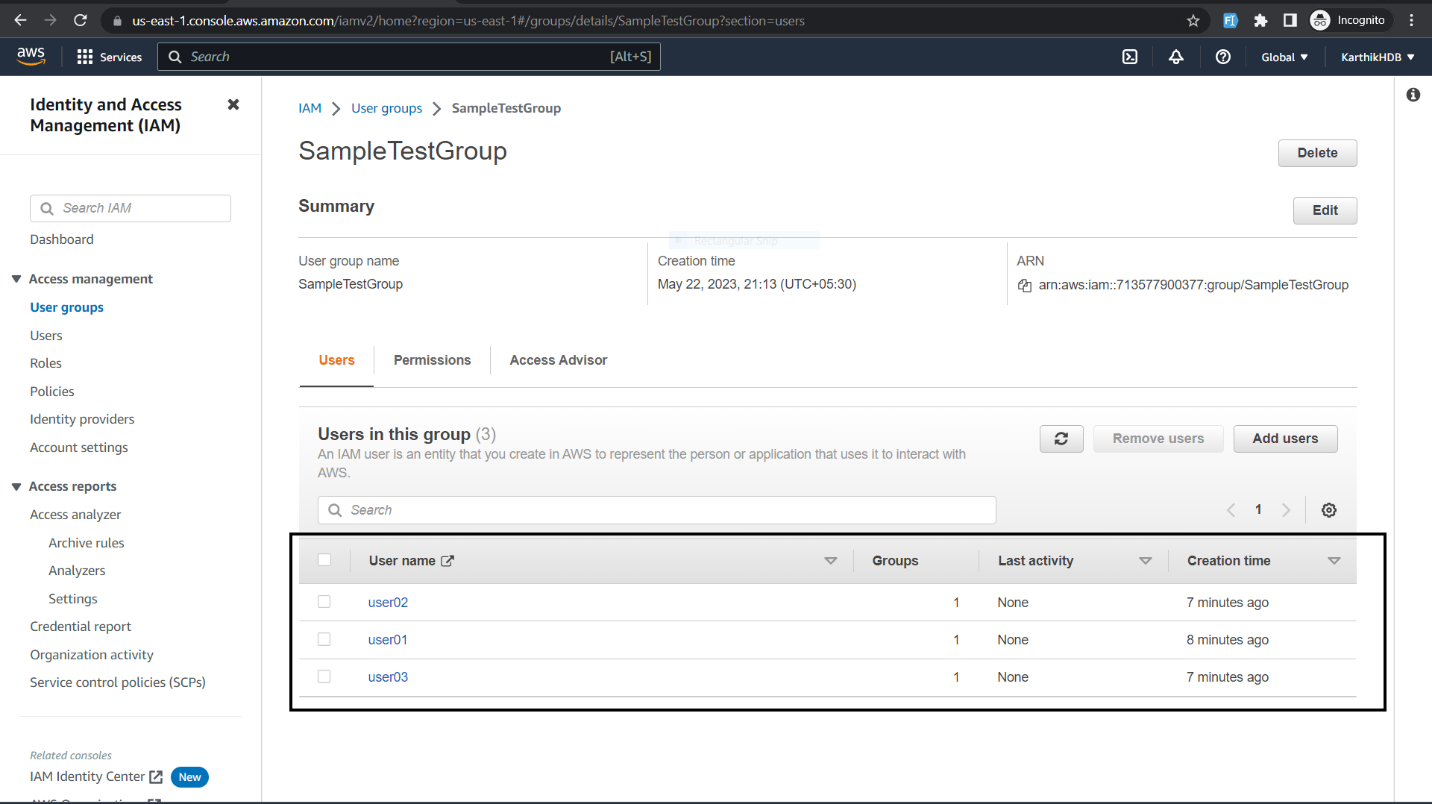
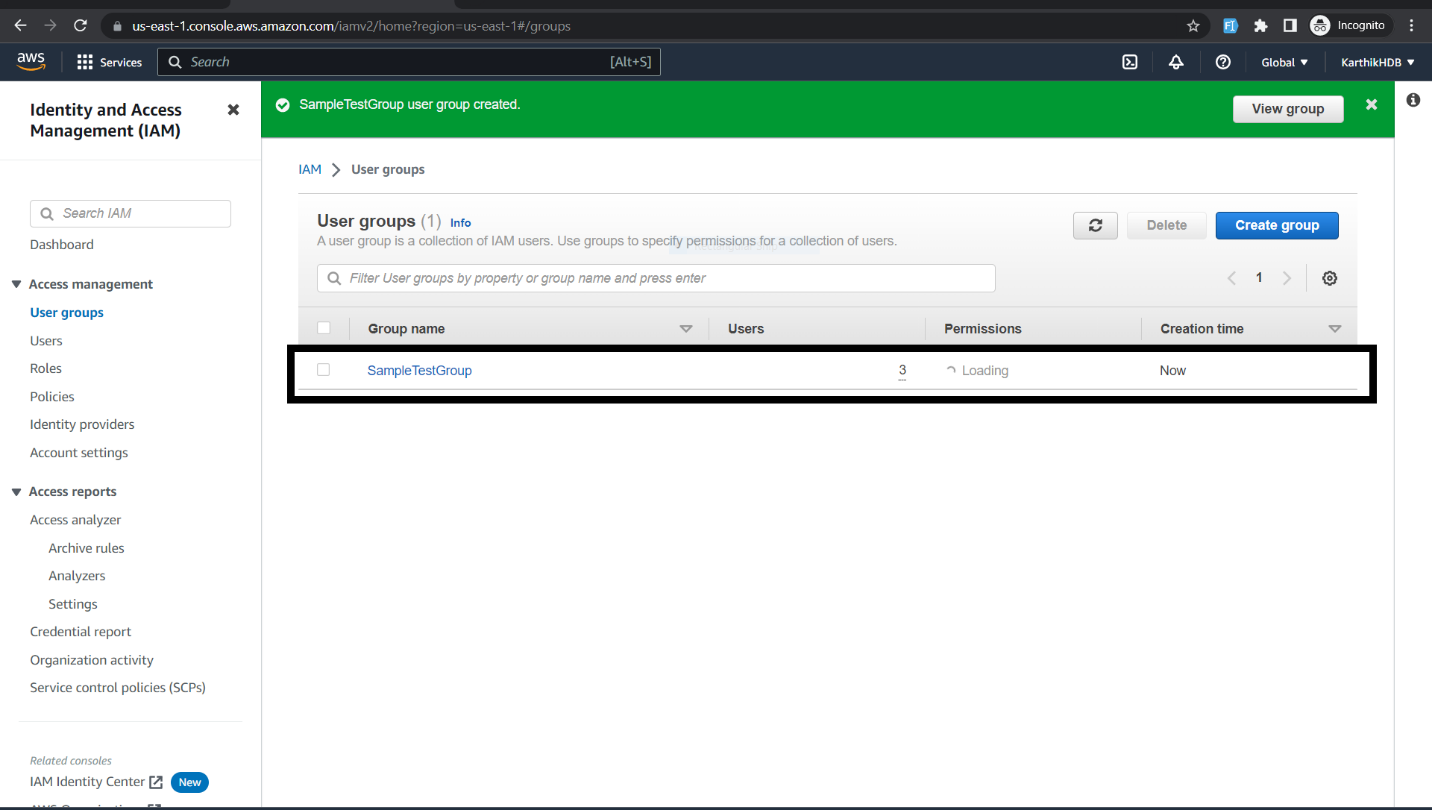
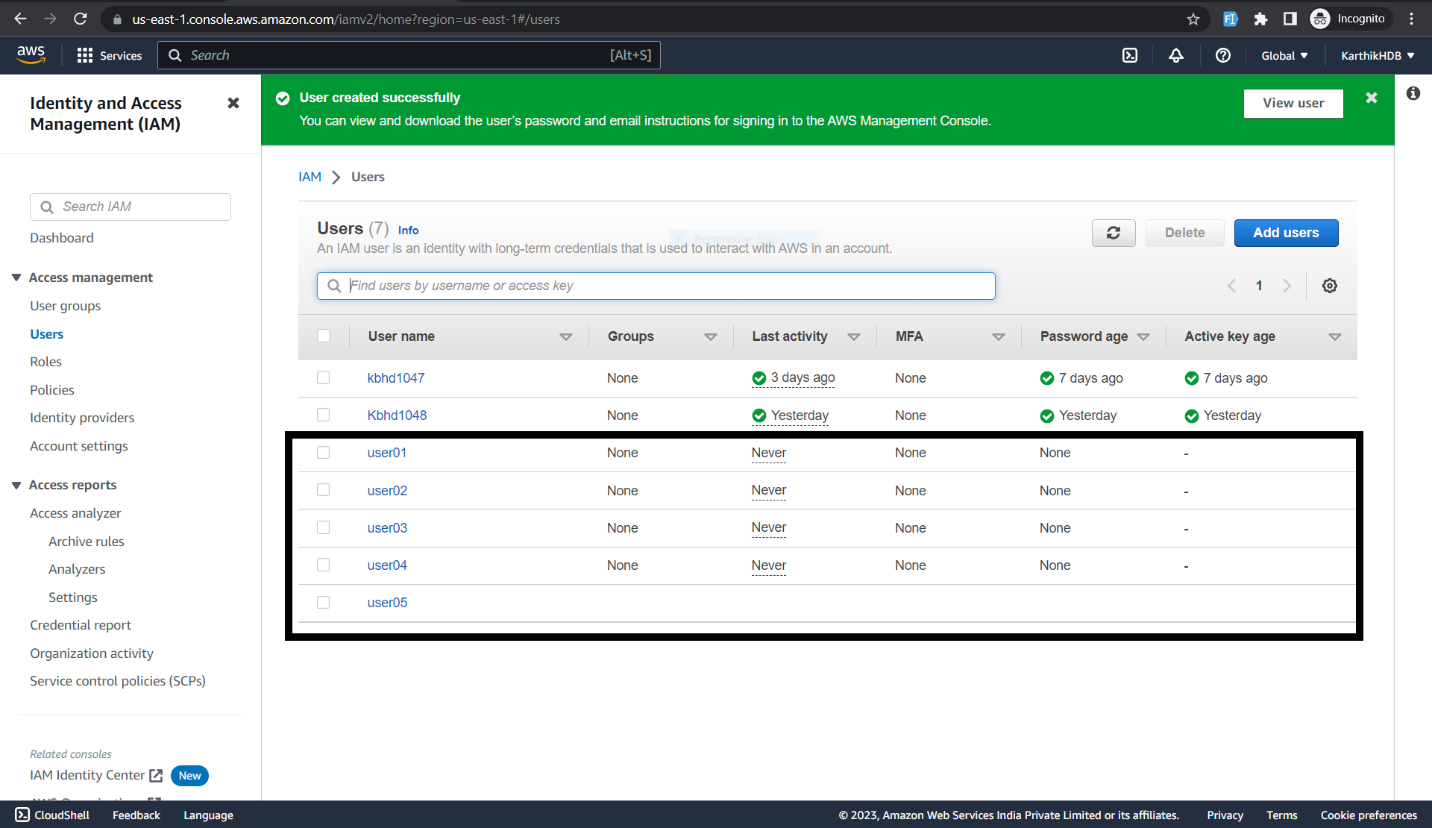
A screenshot of a computer

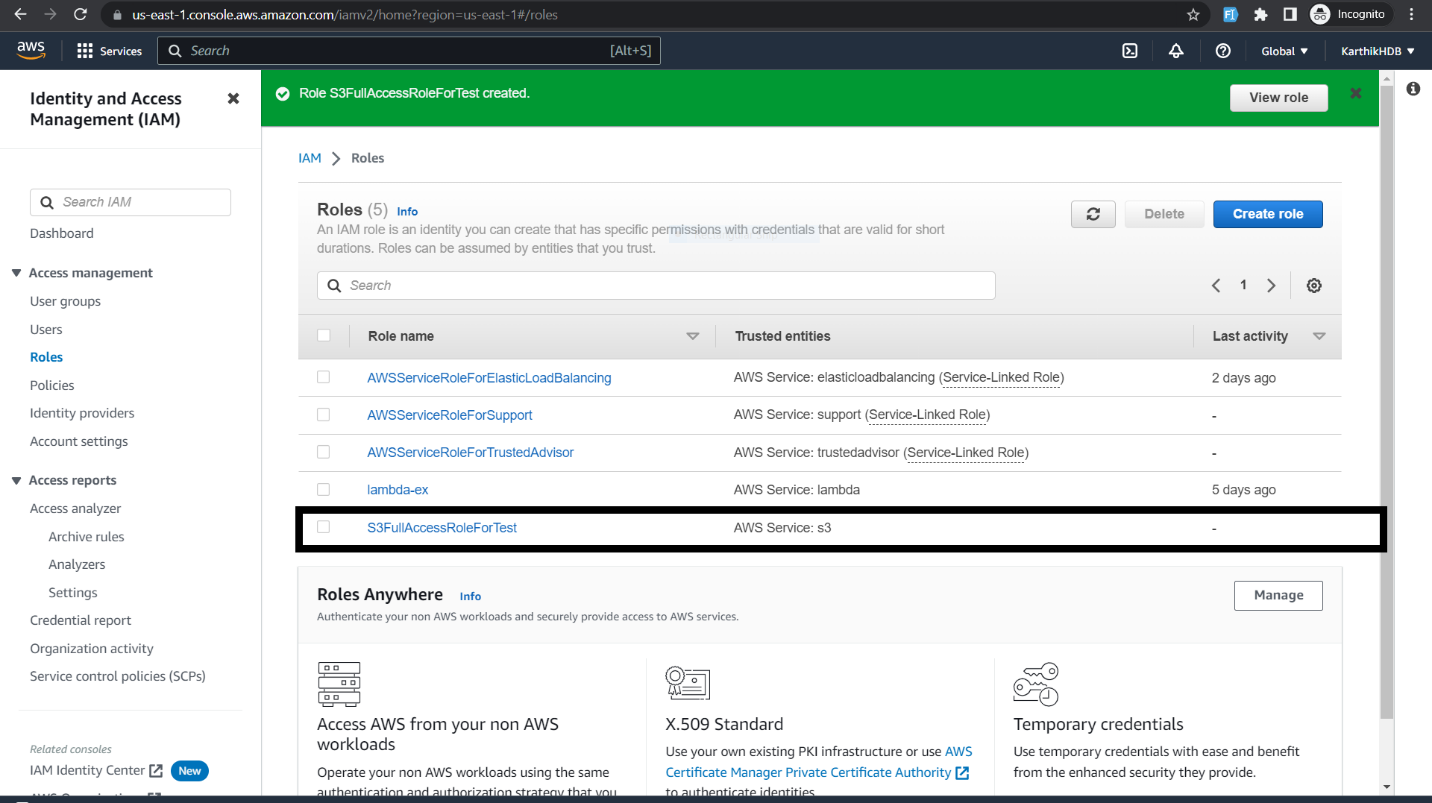
Description automatically generated with medium confidence

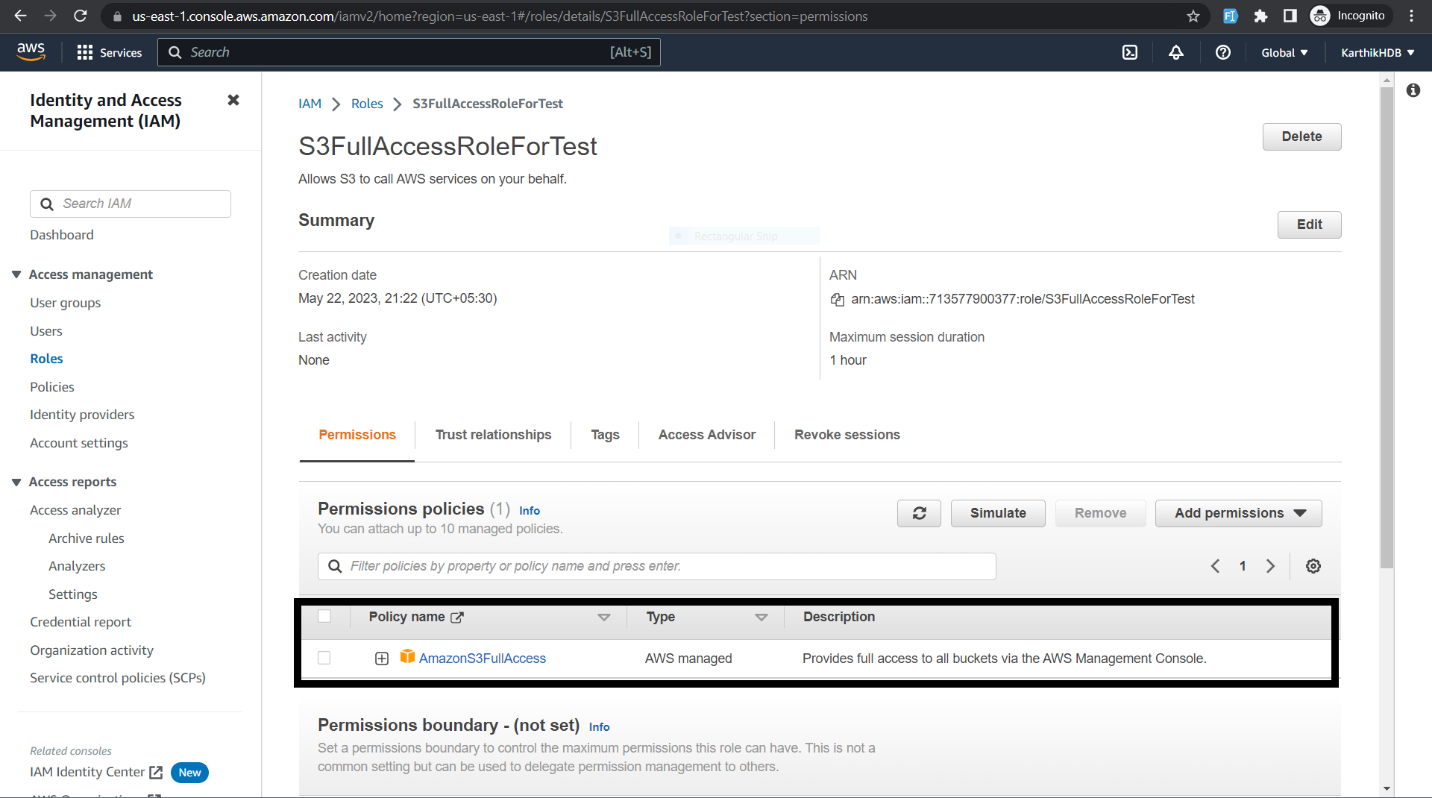
1. Create an IAM policy that allows the user to read and write to an S3 bucket and attach it to the user. 

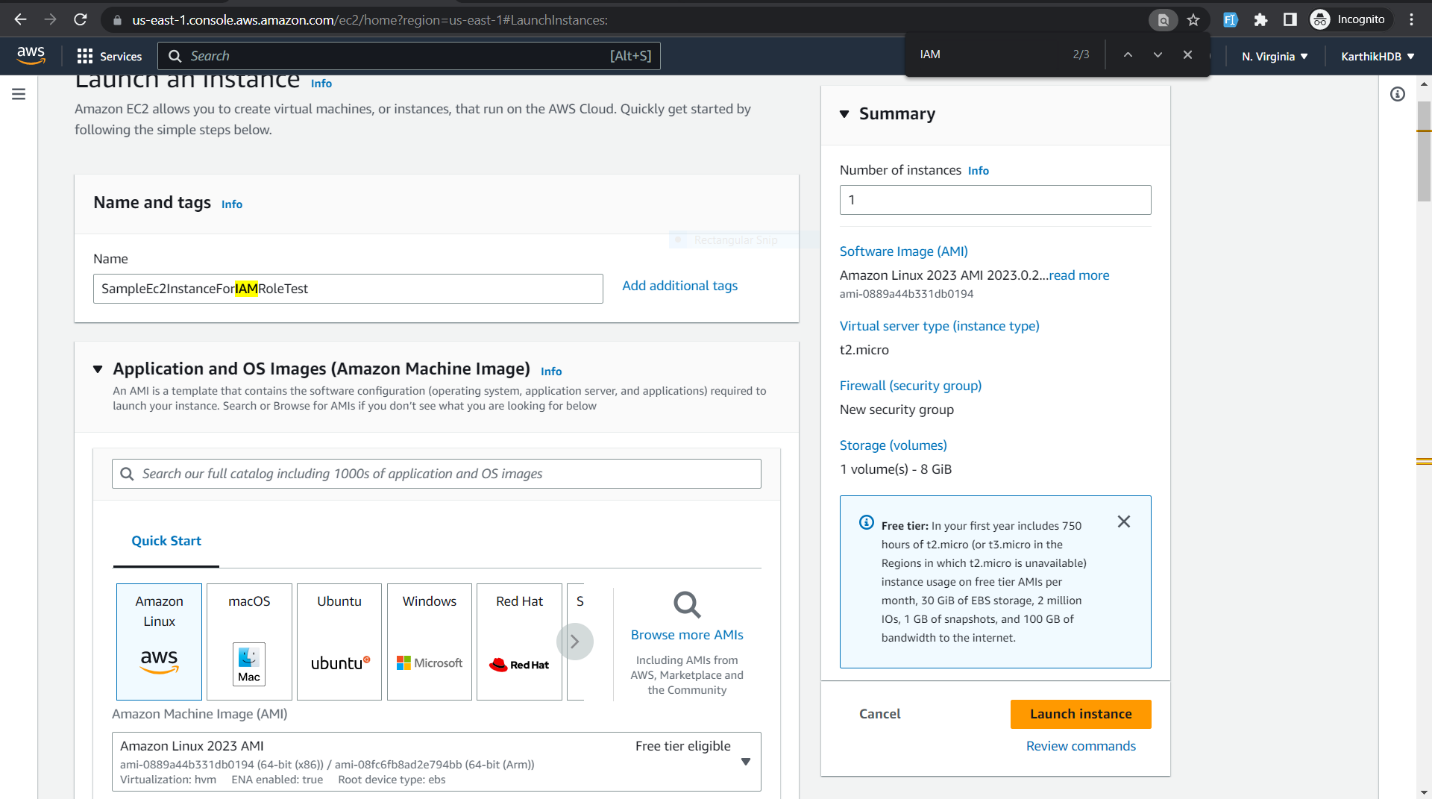


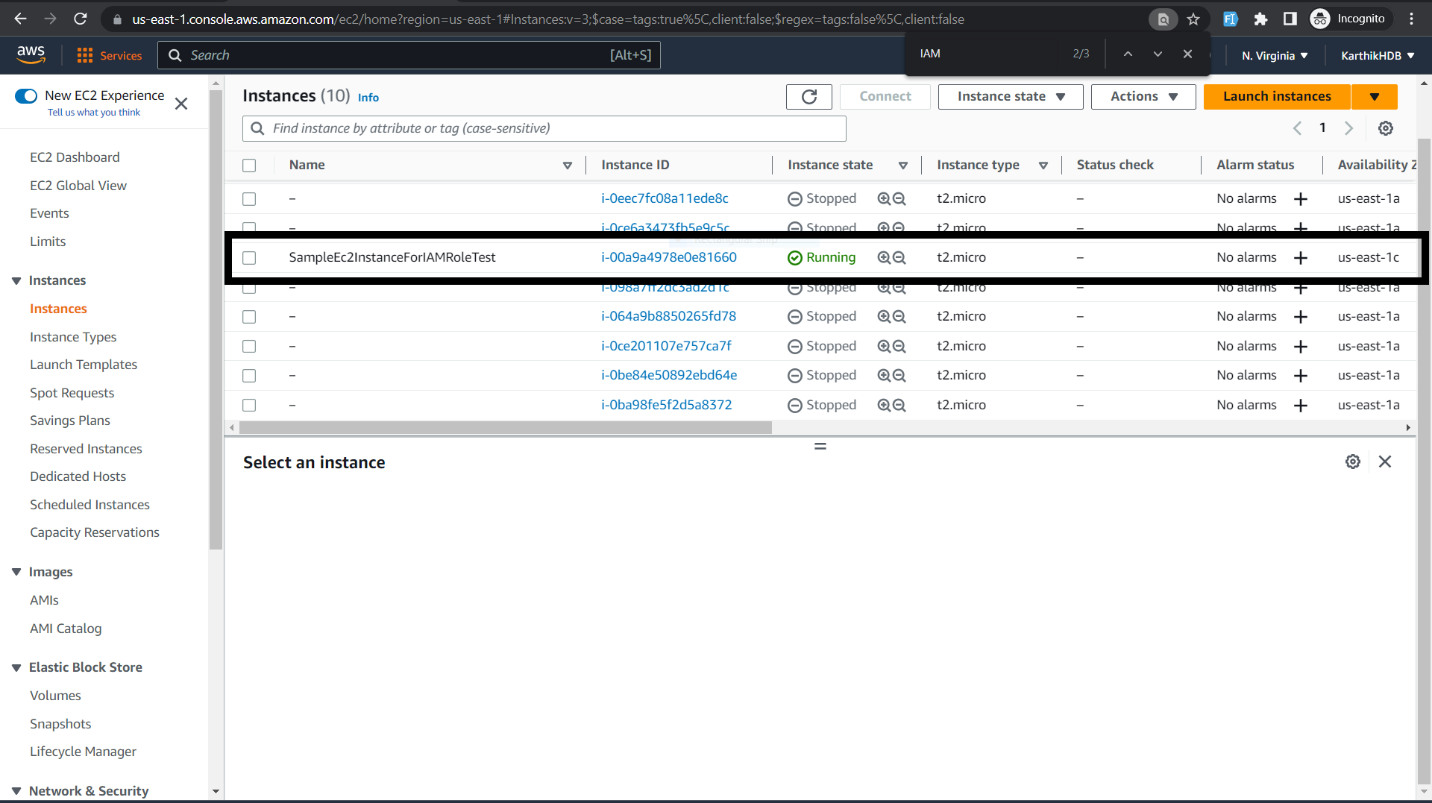
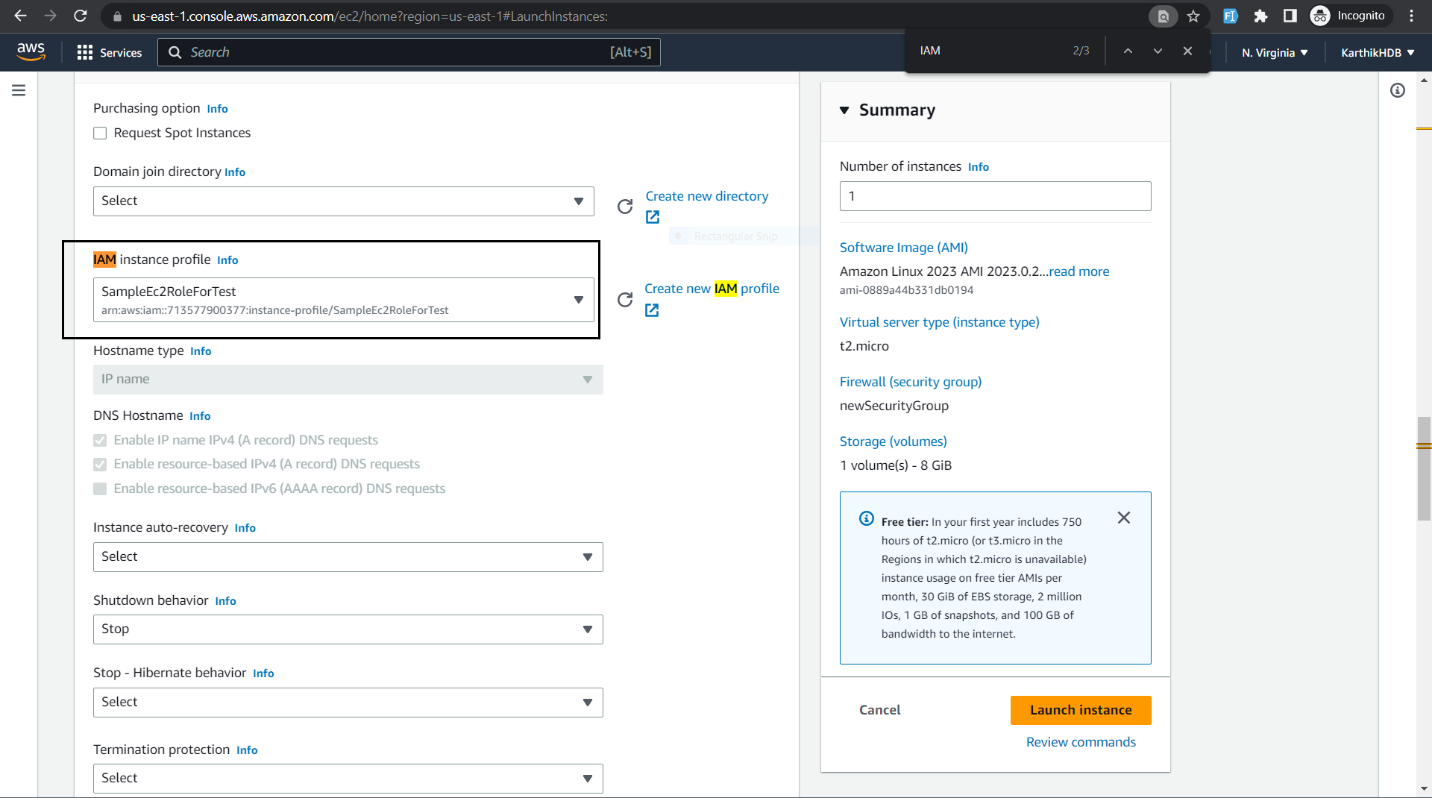
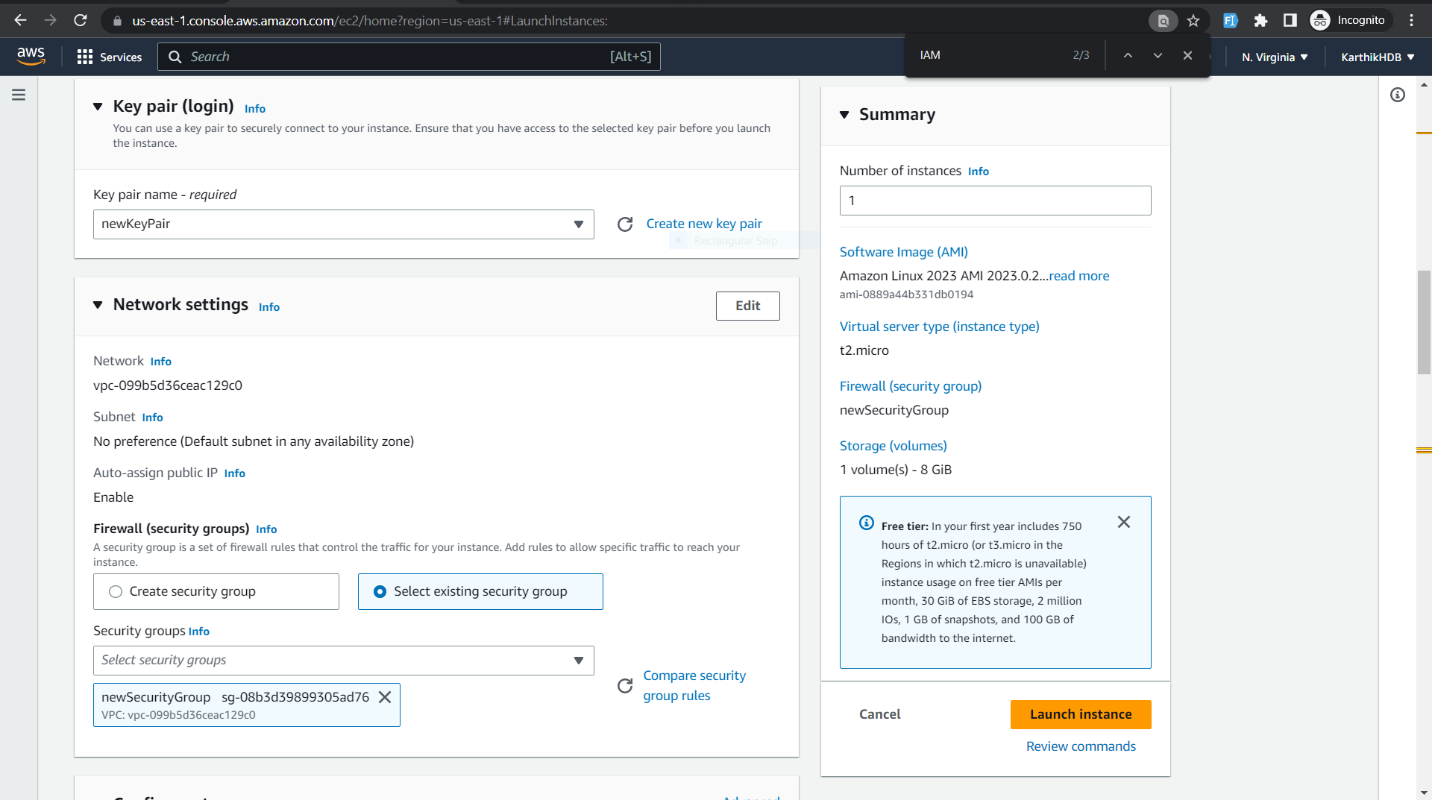
3.Create an IAM group and add the user to it.



4.Create an IAM role and assign it a policy that allows it to access an S3 bucket.

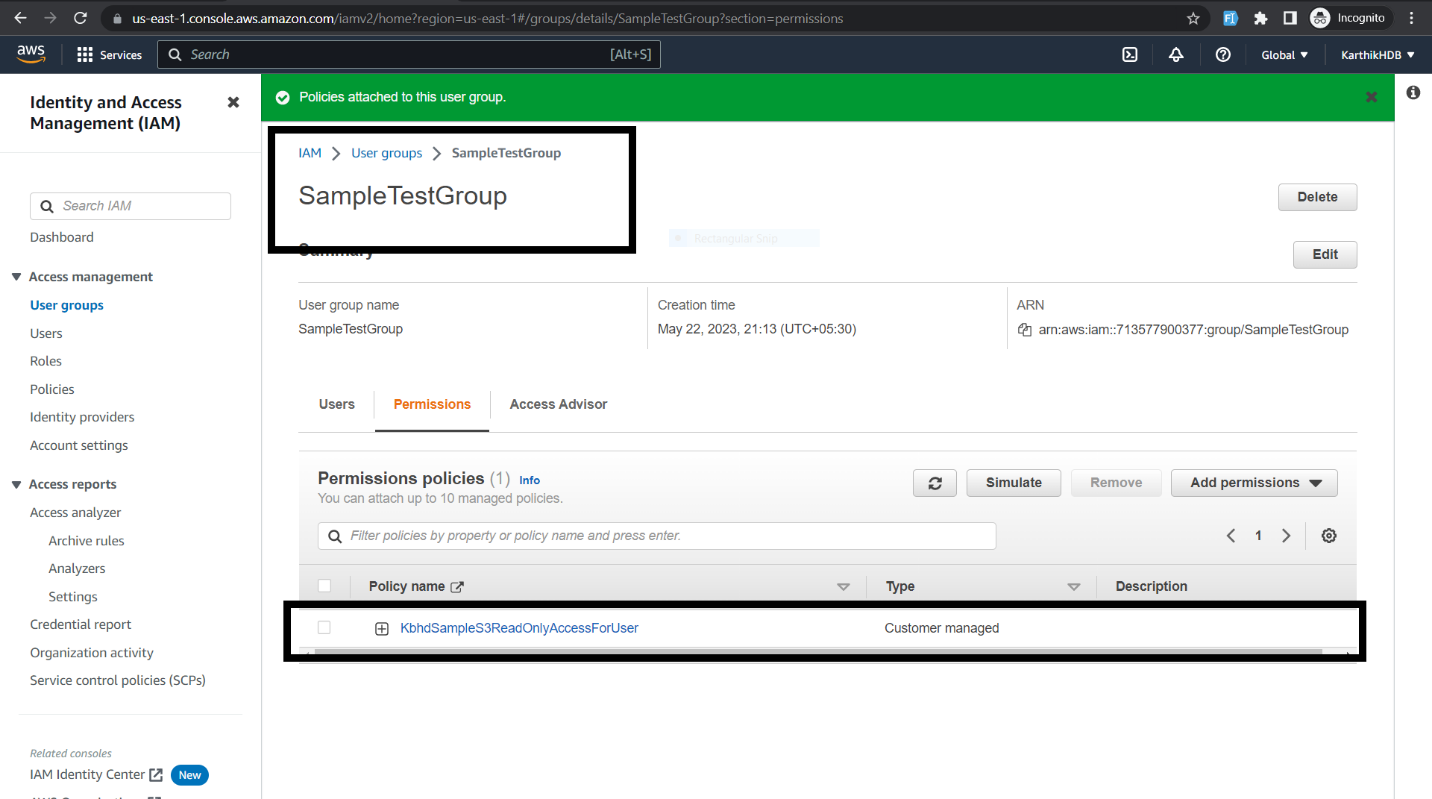
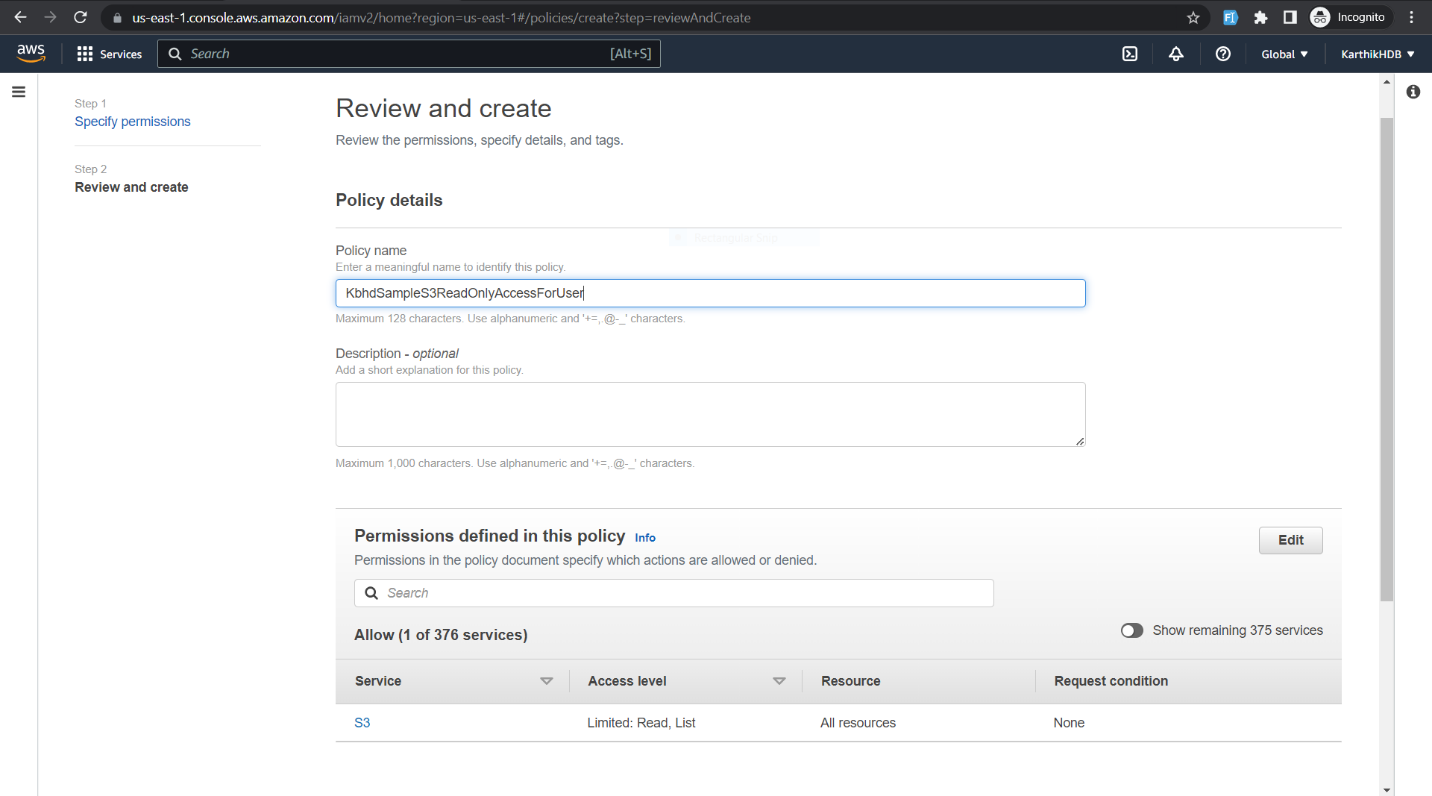


5. Launch an EC2 instance and assign the IAM role to it.

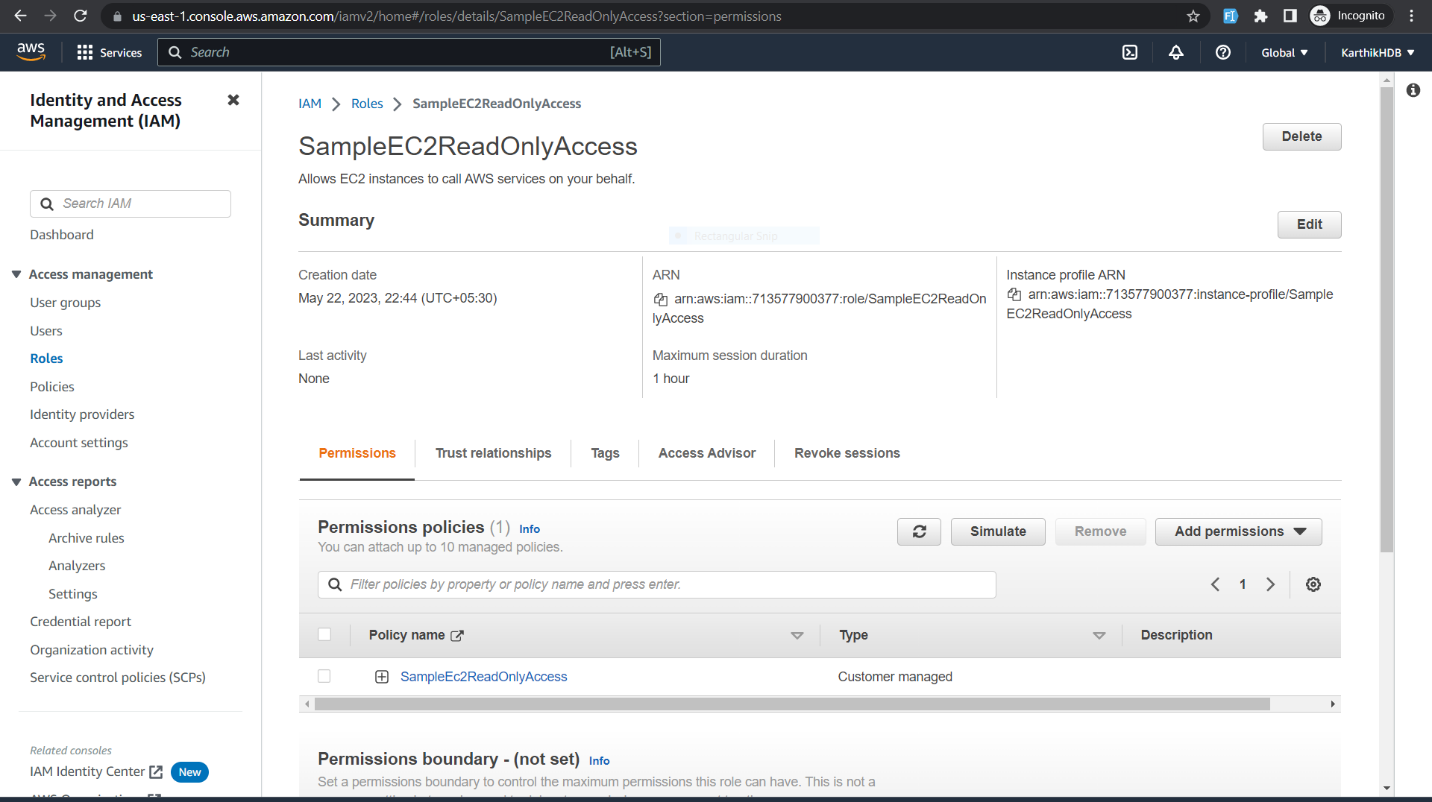
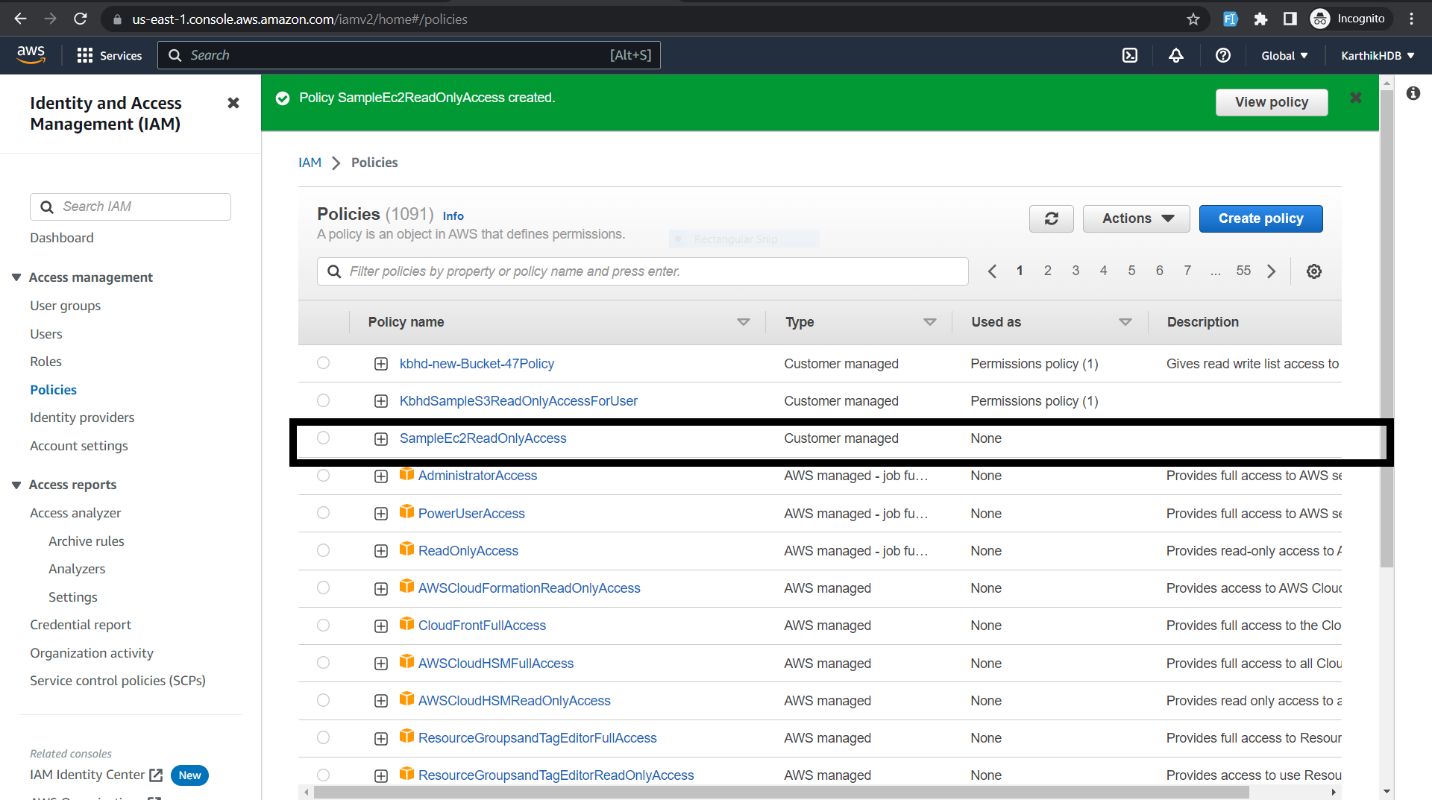
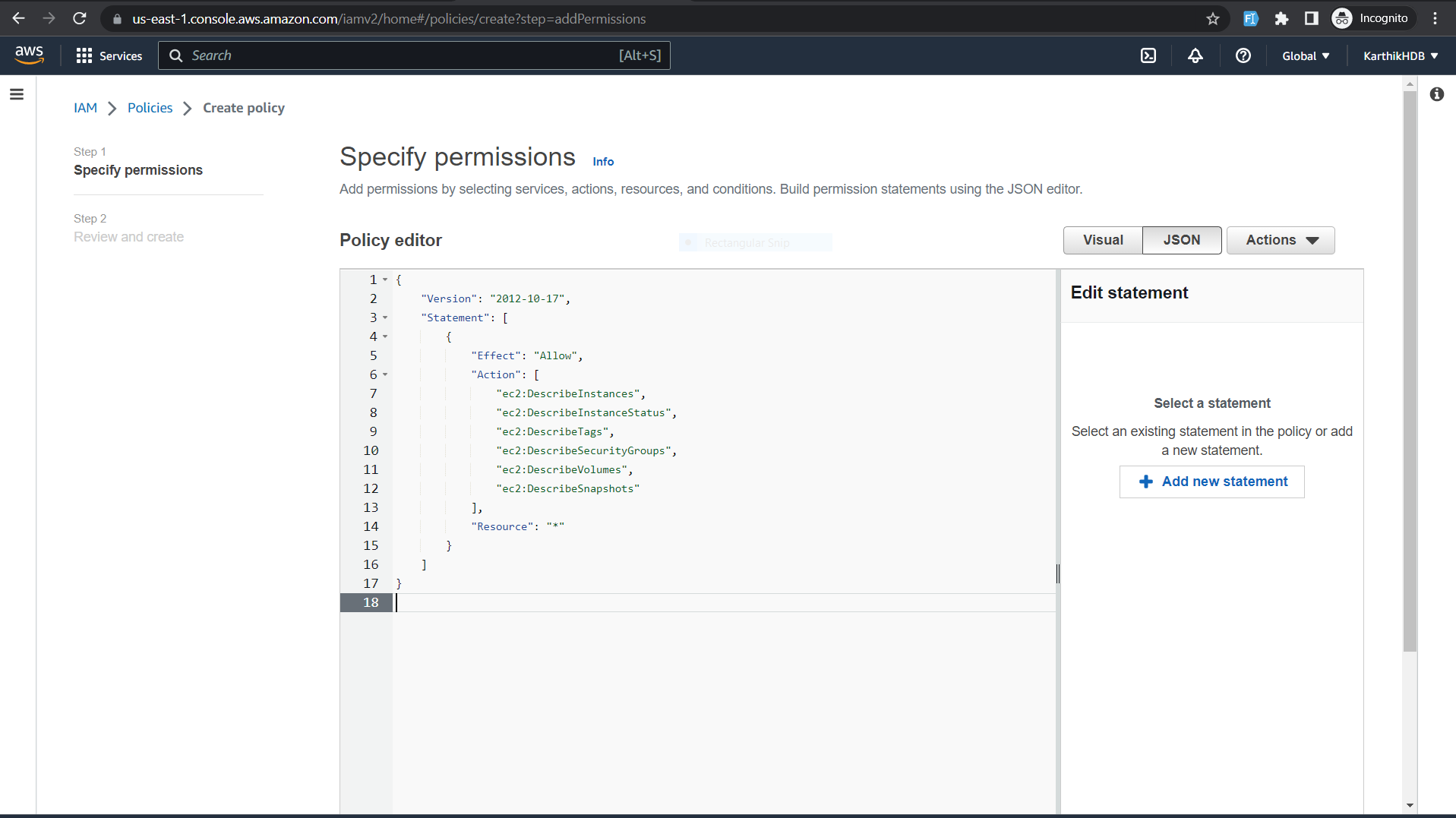


6.Create an IAM policy that allows read-only access to an S3 bucket and attach it to a group.A screenshot of a computer

Description automatically generated

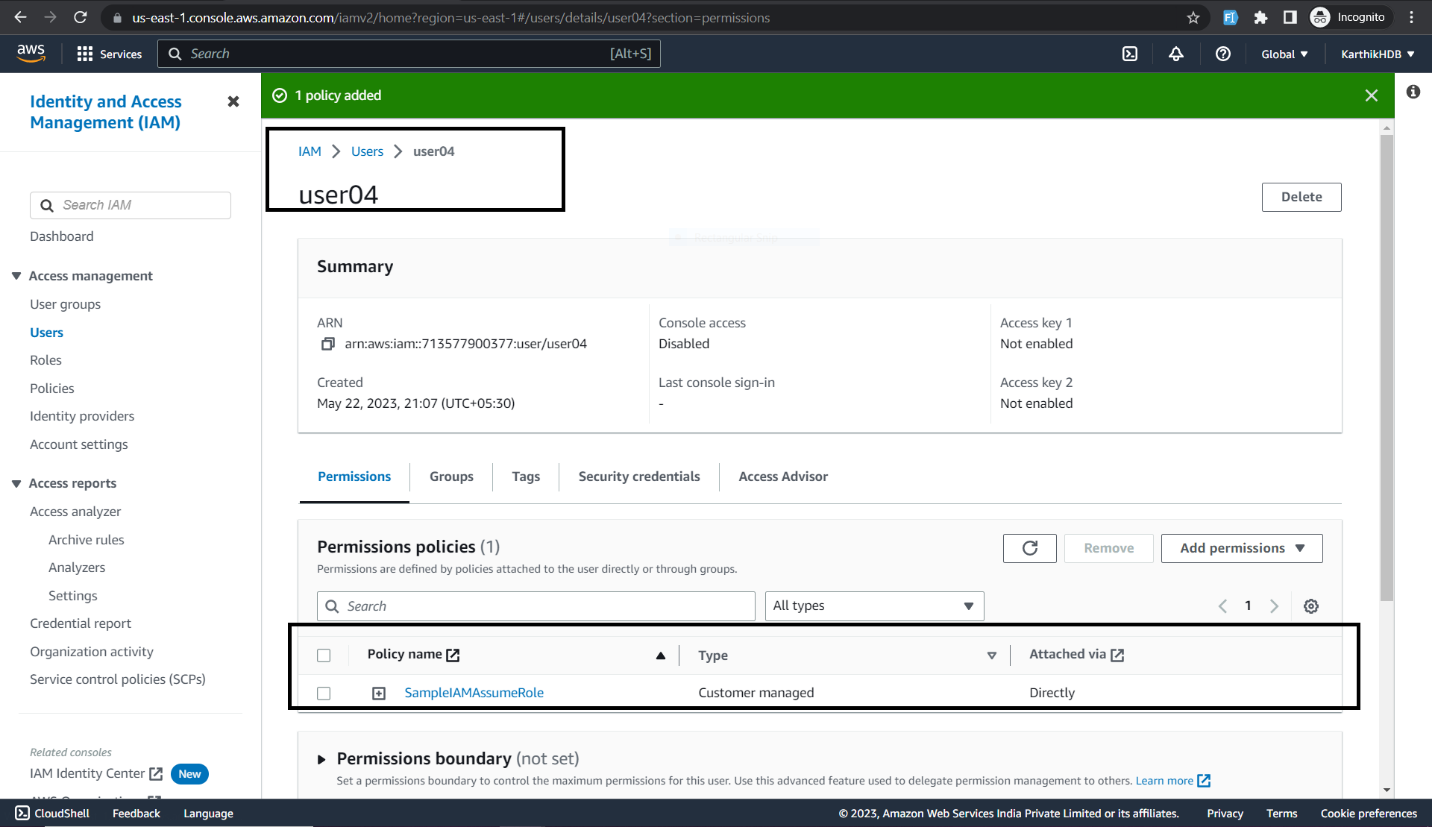
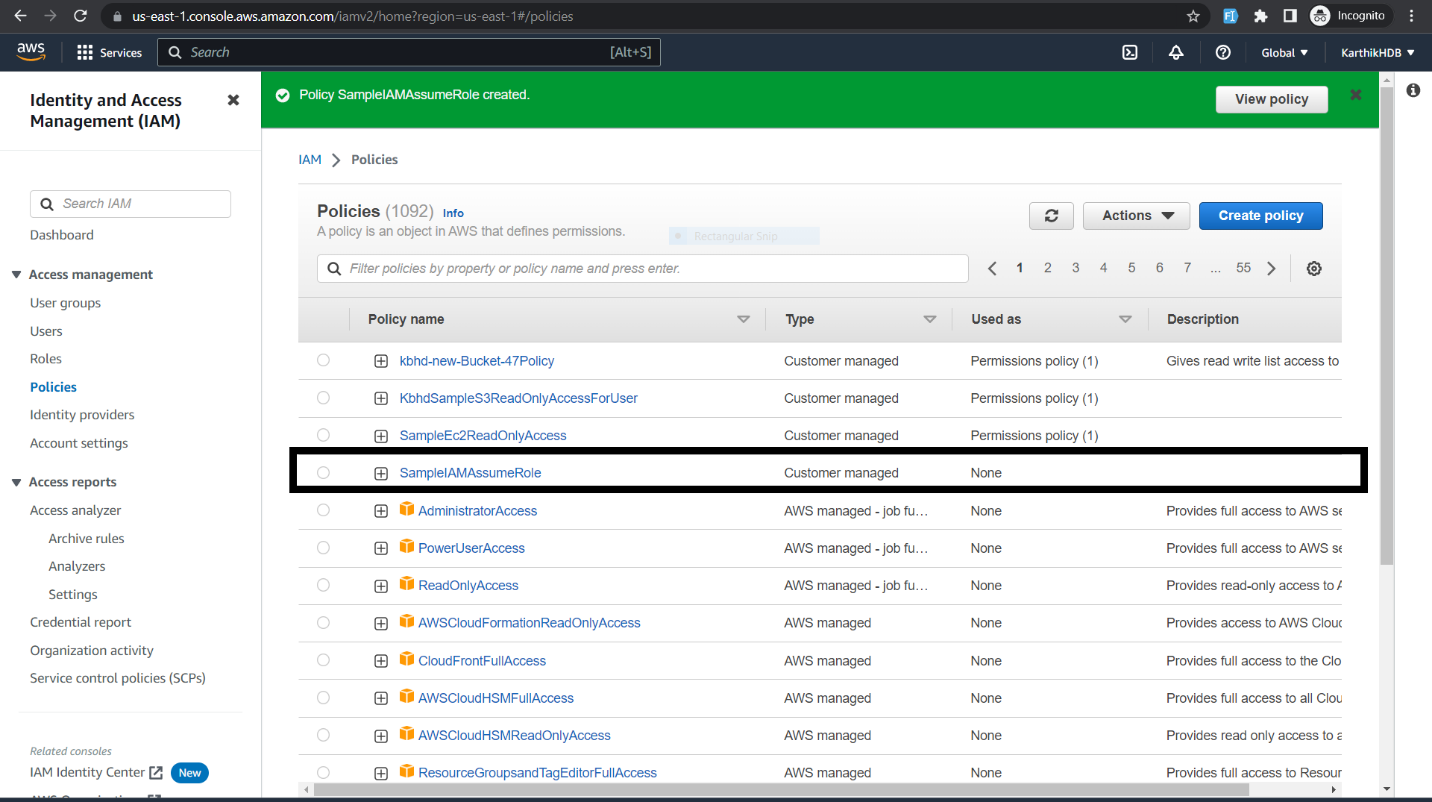
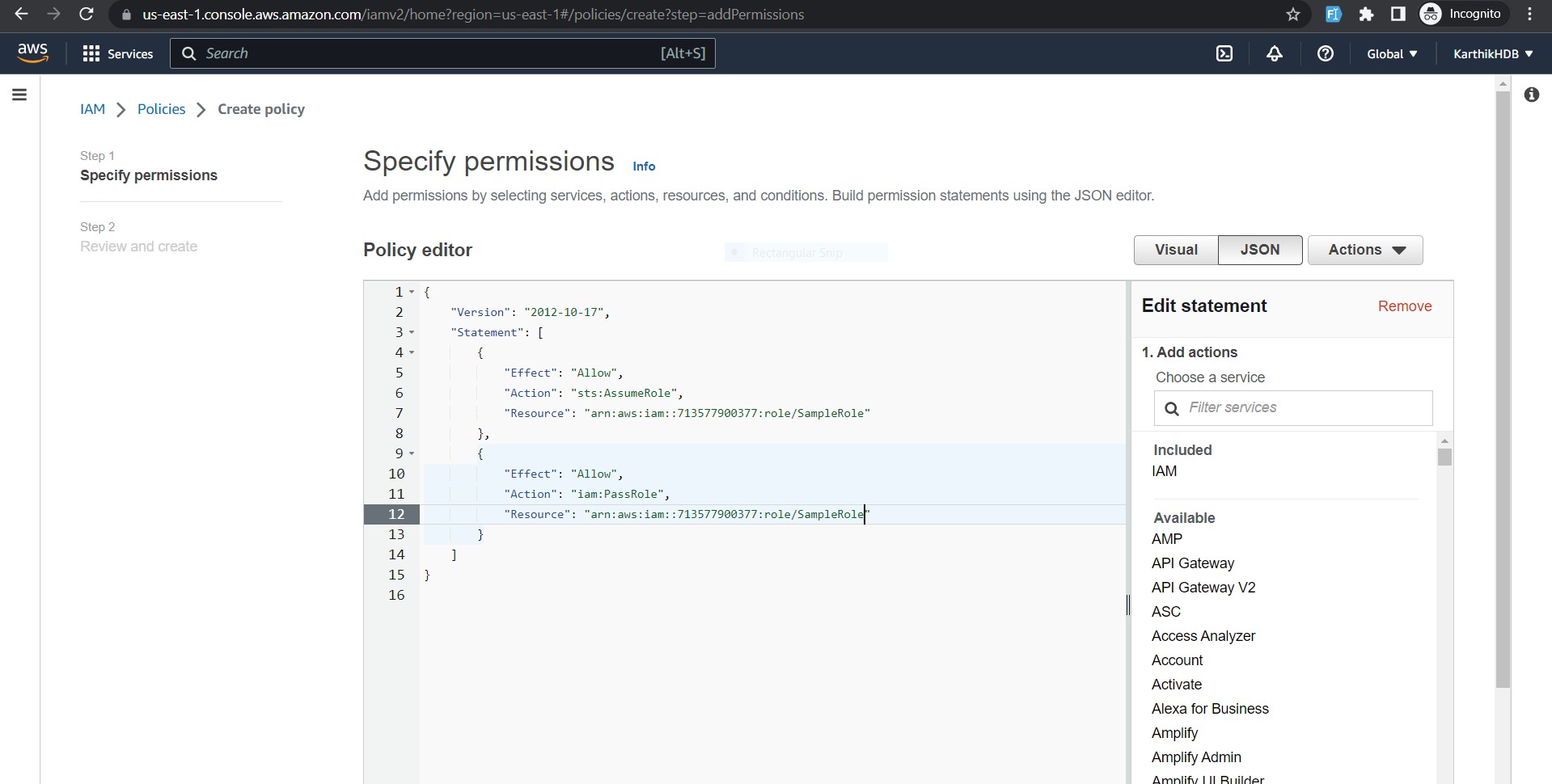


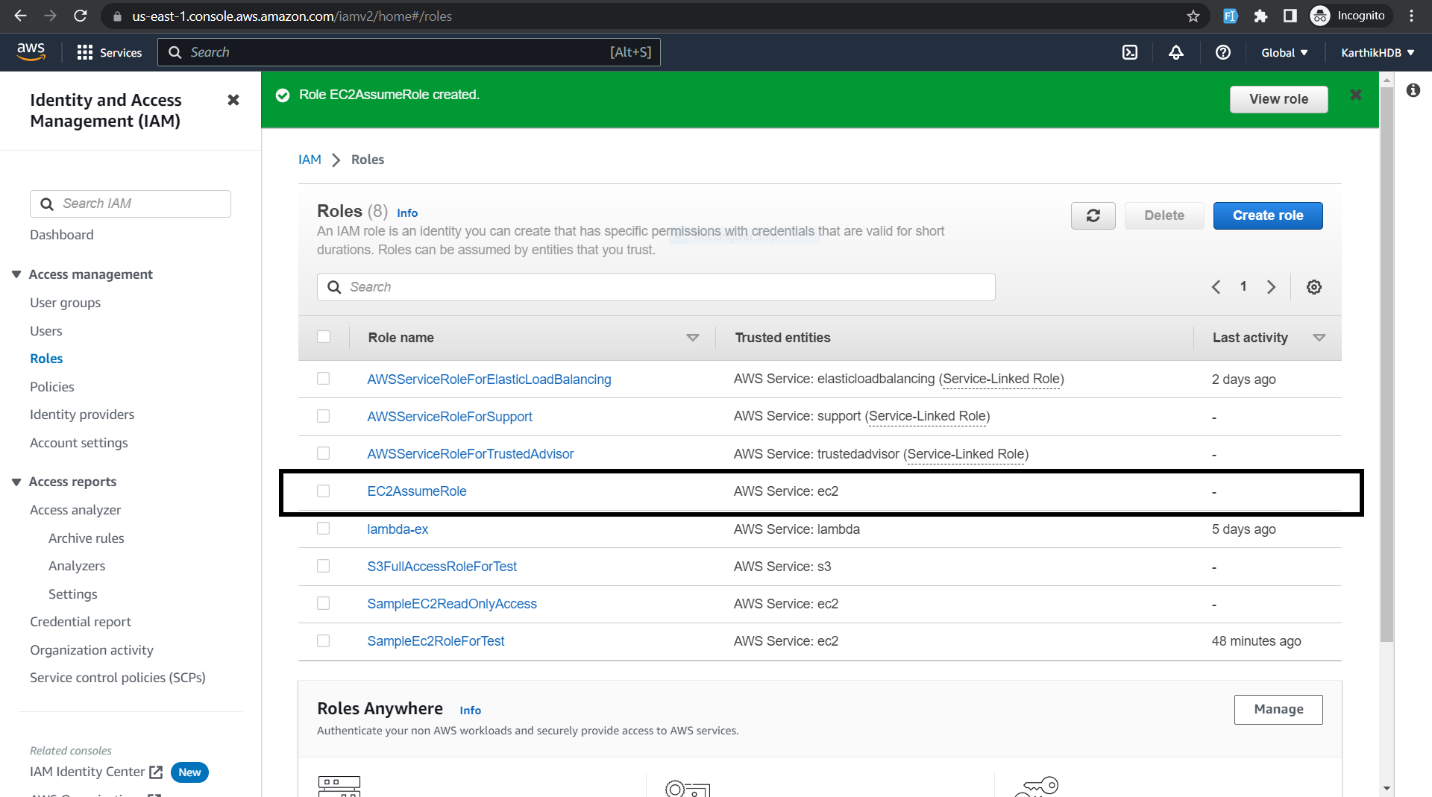
7.Create an IAM policy that allows read-only access to an EC2 instance and attach it to a role.



8.Create an IAM policy that allows an IAM user to assume a role and assign it to the user.

9.Create an IAM policy that allows an EC2 instance to assume a role and assign it to the instance.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

10. Create an IAM policy that denies access to an S3 bucket and attach it to a user, group, or role.

