PROJECT-9:

Configuring IAM identities, MFA, and Access keys:

* IAM stands for Identity and Access Management, and it is a service provided by Amazon Web Services (AWS) that helps you manage access to your AWS resources.
* IAM allows you to control who can access your AWS resources (authentication) and what actions they can perform (authorization).
* With IAM, you can create and manage AWS users, groups, and roles.
* Each user is given a unique set of security credentials, such as a username and password or access keys, which are used to authenticate their identity when accessing AWS services.
* IAM enables you to create and manage individual IAM users within your AWS account.
* IAM allows you to organize your users into groups, making it easier to manage permissions and access for multiple users who have similar responsibilities.
* IAM supports MFA, which adds an extra layer of security by requiring users to provide an additional authentication factor, such as a one-time password generated by a hardware device or a virtual MFA app.
* IAM enables the creation and management of access keys (access key ID and secret access key) for programmatic access to AWS services using APIs or command-line interfaces.

STEPS:

1.Create 3 users user1, user2 and user3.A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

2. Create 3 user groups RDS-admin, S3-support, EC2-Support.A screenshot of a computer

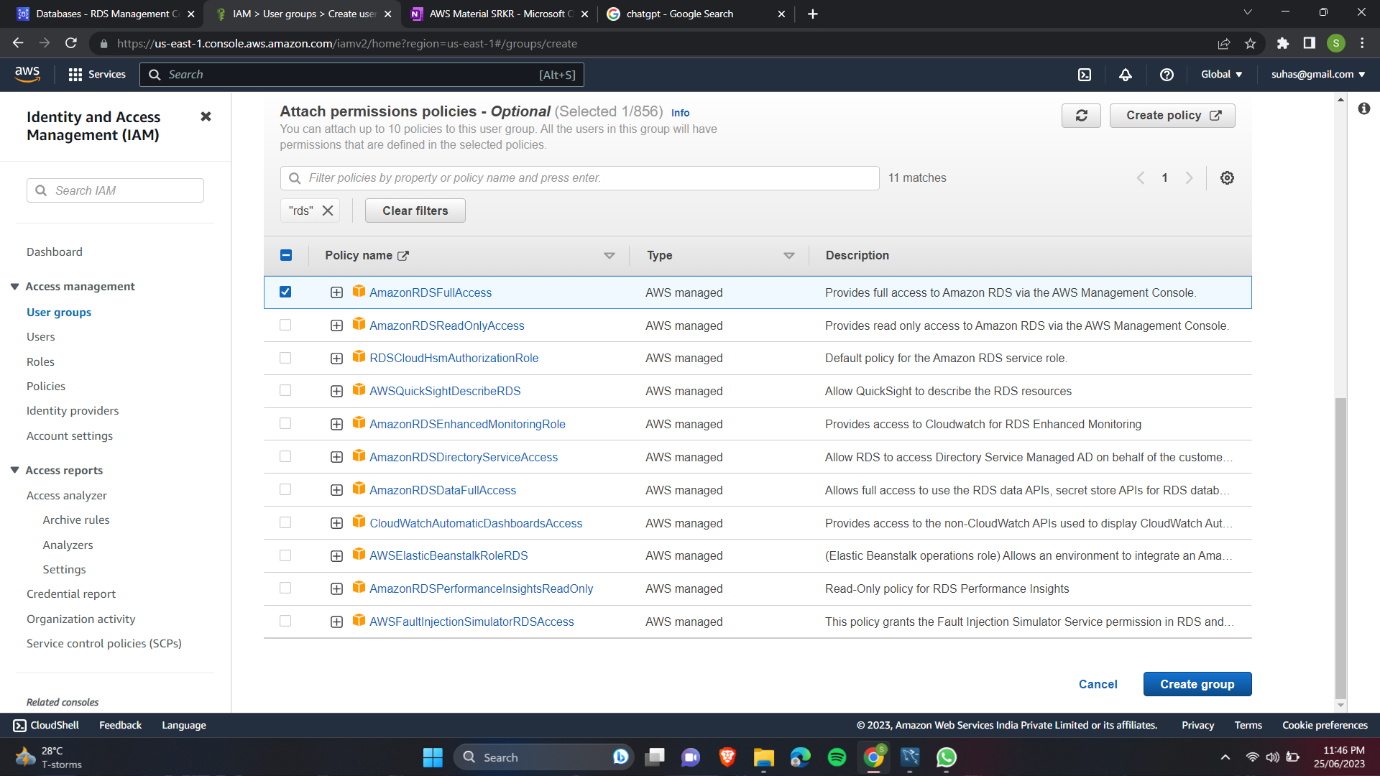
Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

3.Assign RDS policy to group1,S3 policy to group2 and EC2 to group3.

A screenshot of a computer screen

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

4.Add User1 under Group RDS-admin.

A screenshot of a computer

Description automatically generated

5. Add User2 under Group S3-Support.

A screenshot of a computer

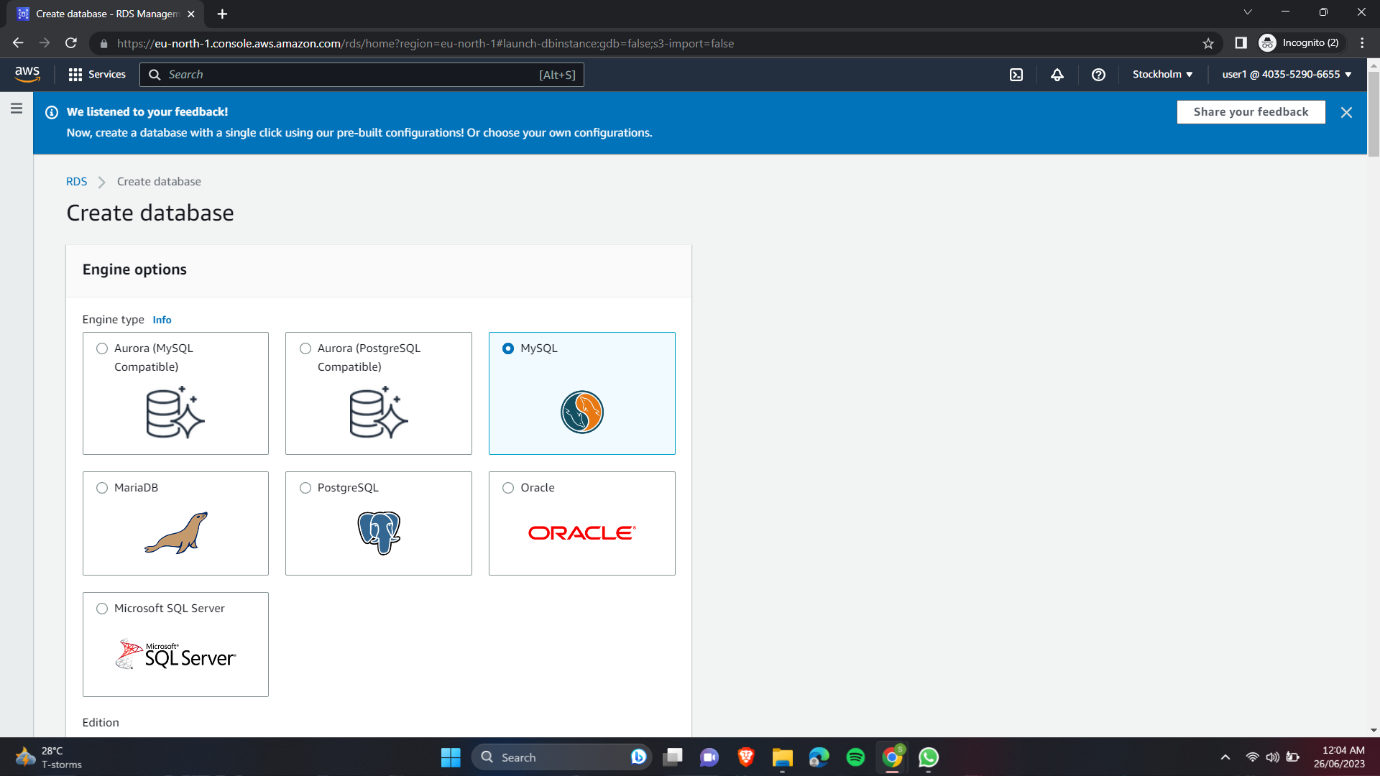
Description automatically generated

6. Add User3 under Group EC2-support.

A screenshot of a computer

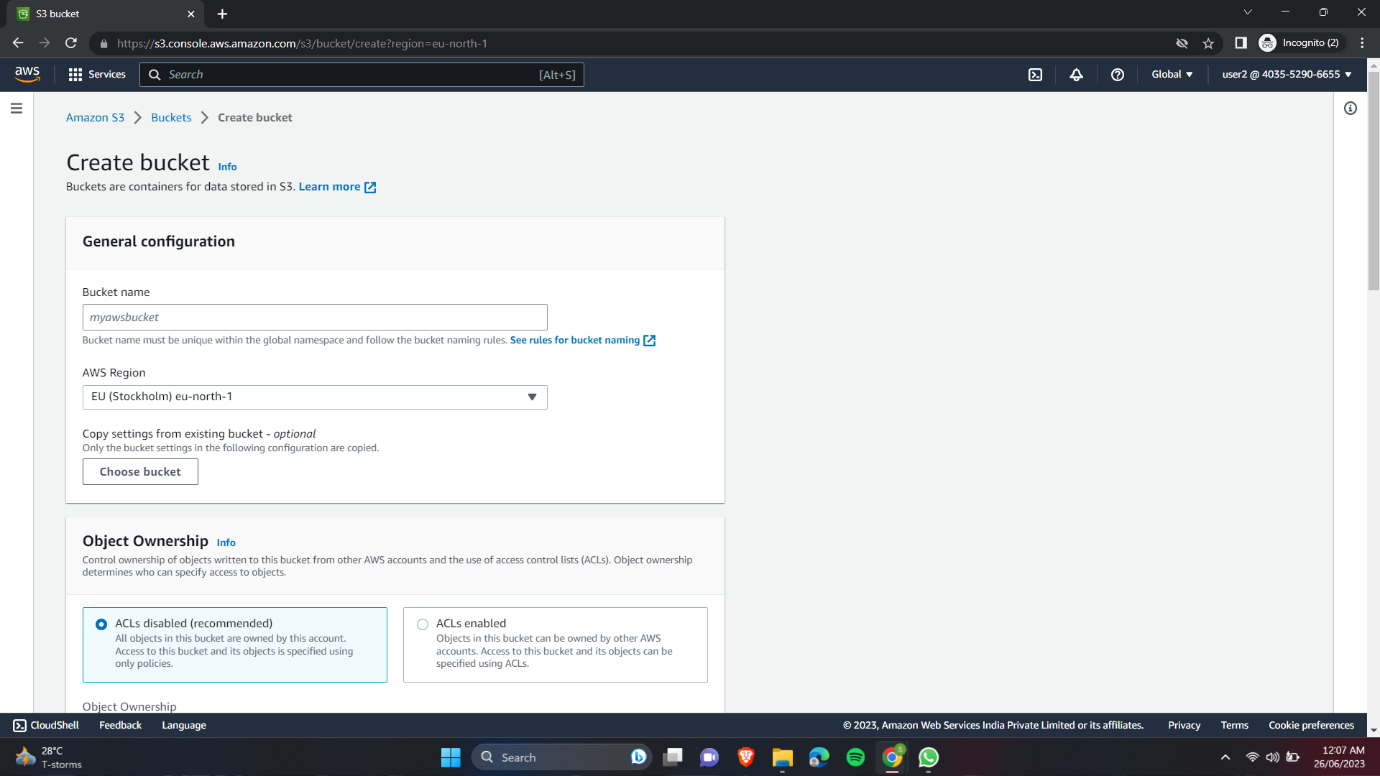
Description automatically generated

7. Login as User 1 and check if User 1 can launch an RDS database.

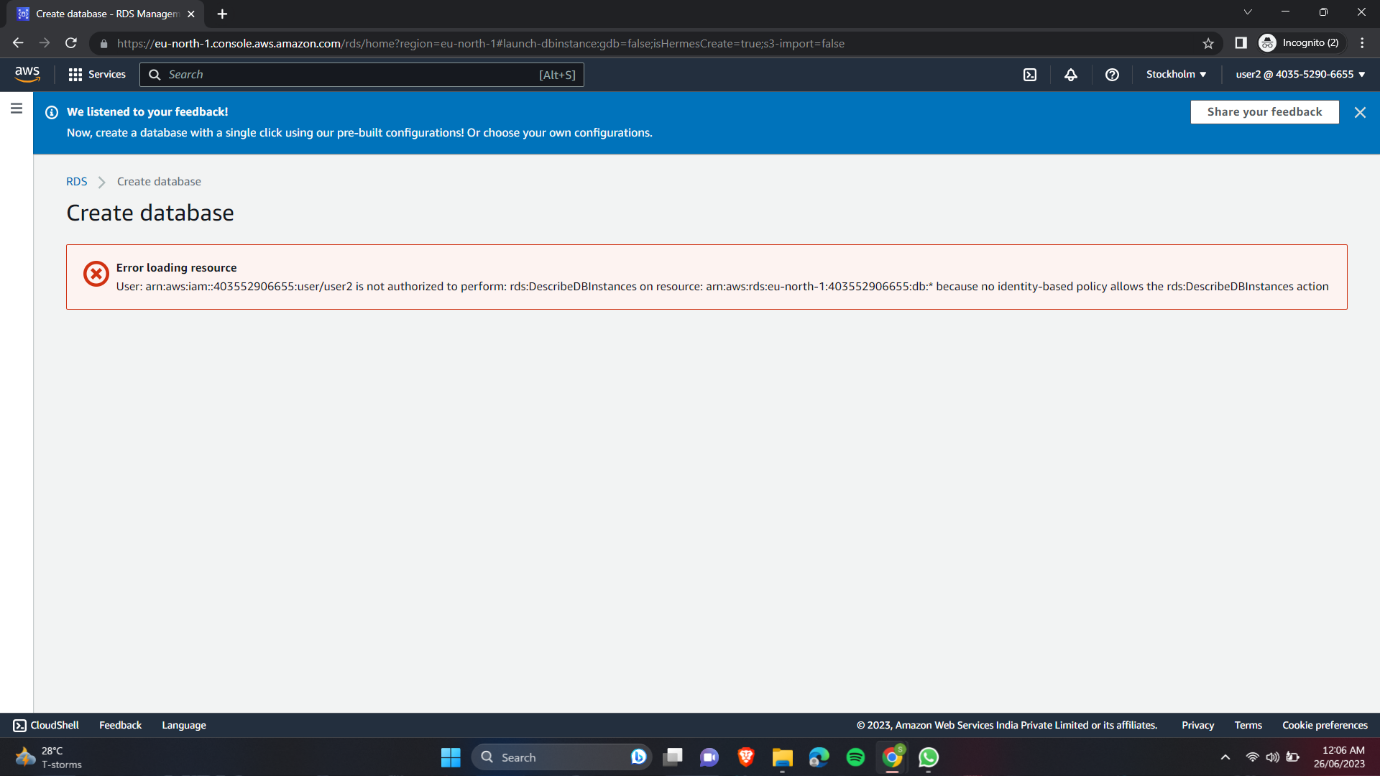


* we can create a database because it is having only RDS access.

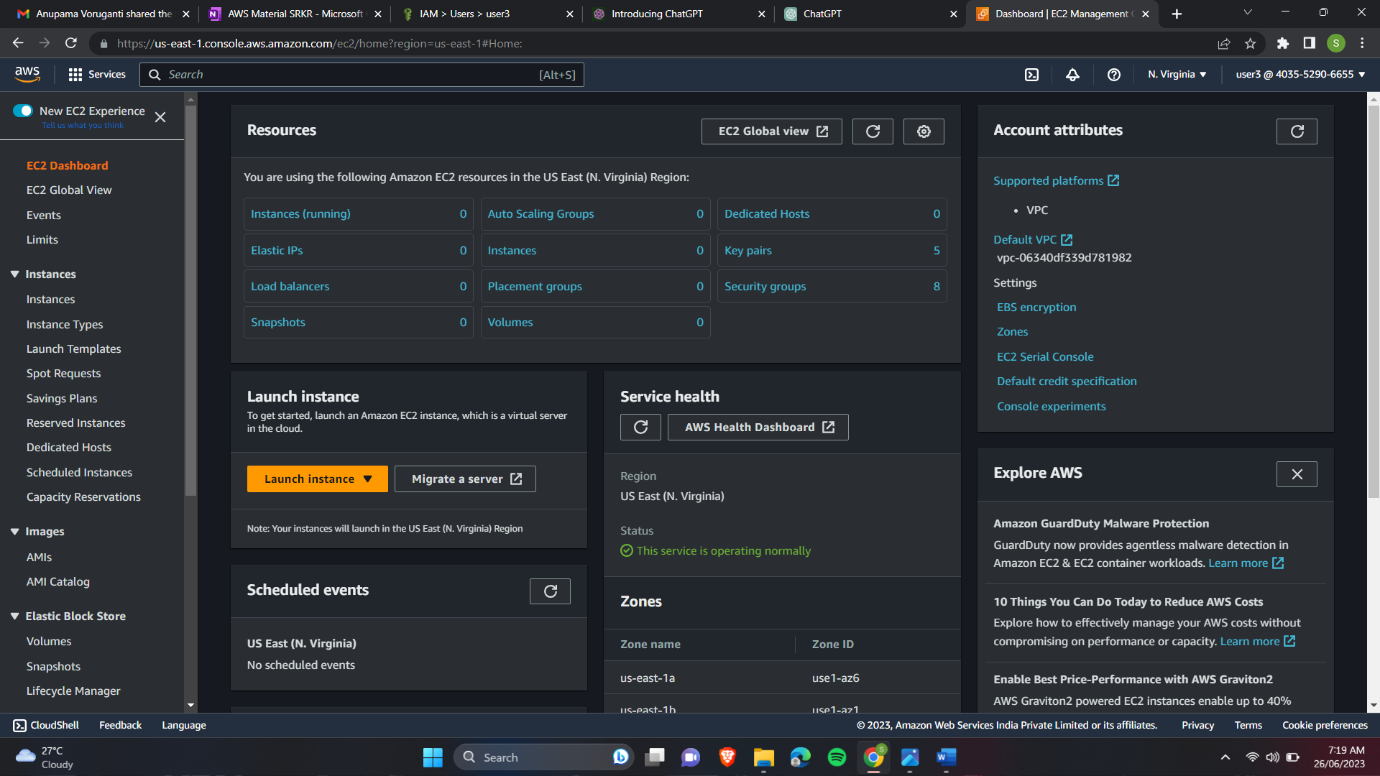
8. Login as User2 and check if User2 can create an S3 bucket.



* we can create a S3 bucket and unable to create a database because it is having only S3 access.



9. Login as User3 and check if User3 can launch an EC2 instance.



10.Go to Multi-Factor-Authentication and click on assign MFA device.

A screenshot of a computer

Description automatically generated

11.Provide device name and chose authenticator app option.

A screenshot of a computer

Description automatically generated

12.Scan the QR-Code in your authenticator app.

A screenshot of a computer

Description automatically generated

13.Provide with two MFA codes which you will see in your authenticator app.

A screenshot of a computer

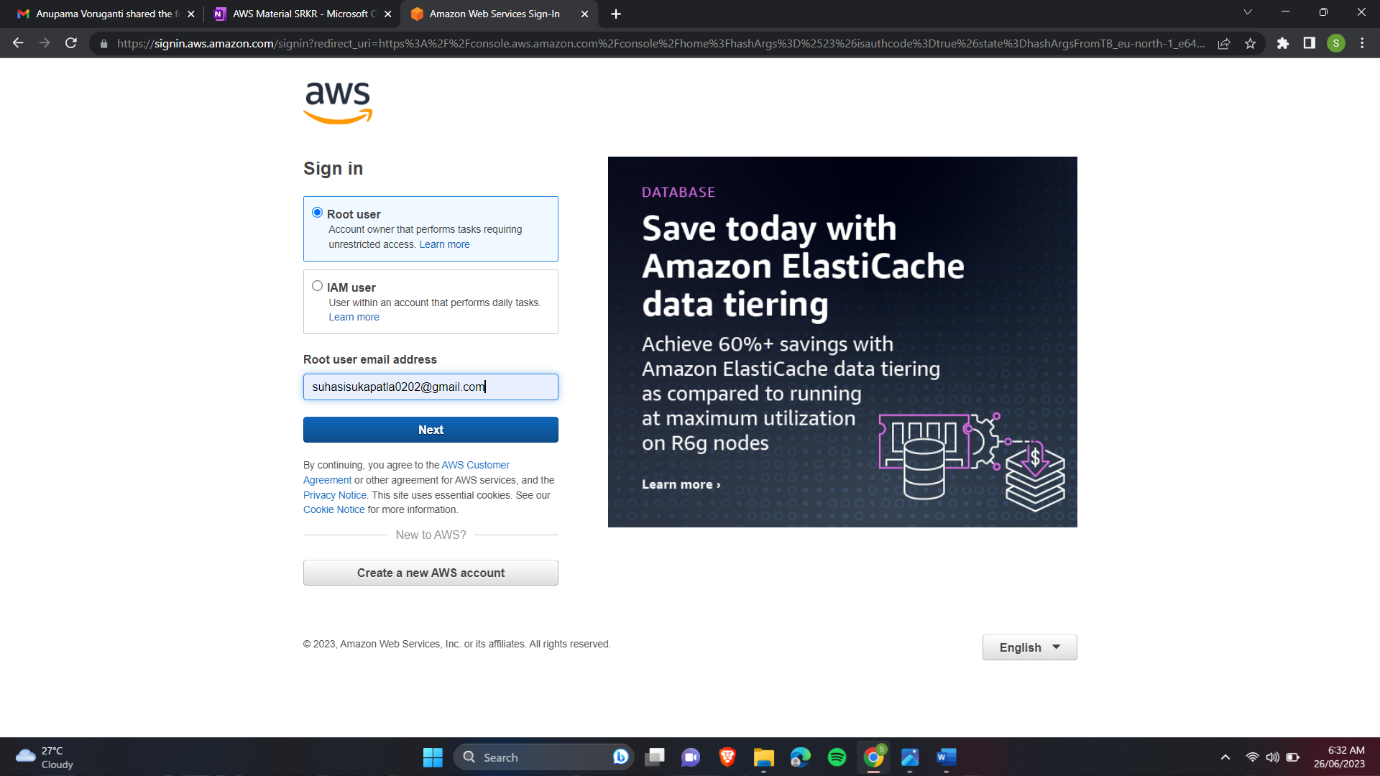
Description automatically generated

14.Now sign out and try to login again.

A screenshot of a computer

Description automatically generated

15.After providing your credentials it will ask MFA code which will be in your authenticator app.



A screenshot of a computer

Description automatically generated

16.You will be successfully signed in.

A screenshot of a computer

Description automatically generated