Shaheer Ur Rehman
231451798
— — — — — — — —

Link to Video Demo

To create an AWS (Amazon Web Services) account and set up users, roles, and access for an imaginary application, we can follow these steps:

Create an AWS Account:

Go to the AWS website (https://aws.amazon.com/) and click on the "Create an AWS Account" button.

Following instructions and providing the necessary information to create your AWS account.

Set up Users and Roles:

Once I have created my AWS account, I log in to the AWS Management Console (https://console.aws.amazon.com/).

I Open the IAM (Identity and Access Management) service from the console.

Create IAM users: I navigate to "Users" in the IAM console and click on "Add User" to create individual users who will have access to my AWS resources.

Create IAM roles: Roles are used to grant permissions to AWS services. I create roles based on the services I want to access. For example, I plan to use Amazon S3, so I can create a role with S3 access permissions.

Grant Access to Services:

Depending on the specific services I want to access, I need to configure the appropriate permissions for the users or roles I created.

For example, let's say that I want to access Amazon S3, I need to grant S3 permissions to the users or roles. Similarly, for other services like Amazon EC2 or AWS Lambda, I will need to configure the necessary permissions accordingly.

I can assign permissions by creating and attaching IAM policies to users or roles. IAM policies define the actions and resources that are allowed or denied.

Test Access and Services:

Once I have set up users, roles, and permissions, I can test access to your desired services.

Use the AWS Management Console or AWS CLI (Command Line Interface) to interact with the services and verify that I can perform the intended actions.