Exercise

**Steps that I have implemented:**

1. Created 3 IAM users in AWS

user\_venkat

user\_rama

user\_raju

1. Created login profiles for the IAM users that I have created (For logging in to AWS console)

By using Terraform, passwords will be auto generated and I have displayed them in the output.tf file

1. Created 3 IAM groups

S3-Support

EC2-Admin

EC2-Support

1. Mapped the users to the respective groups using iam group membership

user\_venkat 🡪 S3-Support

user\_rama 🡪 EC2-Support

user\_raju 🡪 EC2-Admin

1. Attached the default policies to the groups as required

S3-Support 🡪 arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess (S3 read only access)

EC2-Support 🡪 arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess (EC2 read only access)

EC2-Admin 🡪 arn:aws:iam::aws:policy/AmazonEC2FullAccess (EC2 Full access)

1. Created an EC2 Instance

With only below values

ami 🡪 ami-04a81a99f5ec58529 (Ubuntu)

instance\_type 🡪 t2.micro

1. Created a S3 Bucket

**Date:** 08/10/2024

**Observation from this exercise:**

1. All users can be able to login to AWS console
2. Users from S3-Support group (user\_venkat 🡪 S3-Support) can only be able to view the S3 bucket list and cannot able to view/create the EC2 instances.
3. Users from EC2-Support group (user\_rama 🡪 EC2-Support) can only be able to view the EC2 instances list and cannot be able to perform any action on EC2 instances and cannot be able to view the S3 buckets.
4. Users from EC2-Admin group (user\_raju 🡪 EC2-Admin) can only be able to view the EC2 instances list and able to perform any action on EC2 instances and cannot be able to view the S3 buckets.