Project – 02

Identify-Based policies, S3 bucket shared among 2 IAM users one has full access and another read-only (edit policies)

AIM

There is a bucket named (IAM bucket) that needs to be shared among 2 users, i.e., Lucas and Anitha. User Anitha should not have access to the confidential folder**.**

Required Services IAM & S3

Procedure

- Go to IAM Service and click on Create Policy. Select the service, i.e., S3 and expand the List and select the Get Data Access Denied Policy and create the policy by giving any name.
- Now click on the Users and create two users. One is LUCAS and another one is ANITHA. While attaching policy, select the policy which we created earlier i.e., Get Data Access Denied Policy and S3 Read Only Policy to ANITHA and attach S3 Full Access Policy to LUCAS.
- Now login with Anitha user, we can't get the data which is presented in the object, because this user don't have any permission to read or write.

Verifying through AWS CLI :-

- First, we need to create access and secret access keys to the users Anitha and Lucas. Then download the access keys PDF into the laptop.
- Launch Instance and connect through Putty and install AWS CLI.
  # sudo su –
  # apt-get update
  # apt-get install awscli -y
  # aws –version
  # aws s3 ls
- Enable to route credentials. You can configure credentials by running the command "aws configure"
  # aws configure
- Now it will ask Access keys details
  AWS Access ID : <copy & paste ID>
  AWS secret Access key : <copy & paste IP>
  Default region name : us-east-1
  Default output format [Name] :- Enter
  # aws s3 ls
- Now it shows the list of buckets.
  # aws s3 ls_s3://<bucket name>(use URL of s3 bucket)
- So, it lists objects in the specific bucket.