Experiment No. 8

Aim: To study and implement Identity and Access Management (IAM) practices on AWS/Azure cloud

Objective: Understand the working of Identity and Access Management IAM in cloud computing and to demonstrate the case study based on Identity and Access Management (IAM) on AWS/Azure cloud platform

Theory:

- Identity Management is a set of business processes, and a supporting infrastructure, for the creation, maintenance and use of digital identities.
- IAM is an essential function for protecting the privacy of information, enhancing user experience, enabling accountability, and controlling access to an organization's assets.
- IAM is the collection of processes and technology used to manage digital identities and the resource access provided through them.
- Components of access management
    - Establishing unique identities and associated authentication credentials.
    - Authoritative source is maintained as a central repository for storage.
    - Providing capability to identities to request entitlements
    - Assigning roles or entitlements to identities.
    - Managing off boarding and other business work processes by workflows
    - Providing capability to approve, revoke, review or certify entitlements or roles assigned to users.

Steps:

----- Configuring IAM Dashboard -----

1. Go to IAM dashboard
2. Click on create option under Account Alias and give a valid name; save changes
3. (Download Google Authenticator from PlayStore in your Mobile Phone)

----- Configuring IAM Dashboard -----

1. Click on "users" in the left column
2. Click on Add users button
3. Set a custom valid psw (Imc: Qwertyuiop123) and check the Require psw rest box which will make you create a next psw in the next sign in
4. Click on Next: Tags
5. Add a tag if you want to just to keep track of your activities; then click on Next: Review

6. Click on Create User Button
7. Open the URL in Incognito Mode (Imc: https://nimitjjw.signin.aws.amazon.com/console)
Open the URL in Incognito Mode (Imc: https://nimitjjw.signin.aws.amazon.com/console)

----- Logging in as the new User & Checking their permissions -----

1. Enter the new user's name and psw saved earlier
2. Enter a new valid psw
3. After logging in, you will notice that you don't have permission to do anything yet

----- Adding MFA for the user via Root User -----

1. Type "AWS CLI" in a new window of any browser and go to it's the main page of AWS regarding the same Click on 64-bit hyperlink in the RHS column under the Windows section and download, install the AWS CL
2. Type "cmd" in the windows search bar and run it as an administrator
3. Type aws configure, it will ask for a few inputs; AWS Access Key ID and Key are the ones which we saved earlier Default region name is whichever region AWS you are using; in case of Mumbai, its: apsouth-1 The output format is json in our case
4. The next two steps are OPTIONAL:
   aws –version
   aws s3 ls

0. Go in the security credentials tab under Users of IAM Dashboard
0. Click on the "Manage" Hyperlink
0. Use the Google Authenticator app downloaded earlier to scan the QR Code
0. Enter two of the codes which are shown in the Google Authenticator App over a span of 30 secs each; click on Assign MFA Button

----- Logging in as the new user after MFA -----

1. Again try logging in via the new user created earlier; this time it will ask for MFA after you click on Sign In
2. Use the code being shown in the Google Authenticator
3. Now, after opening the root user window again After going in the Users section of IAM Dashboard, we can see that MFA has been activated for the new user

----- Adding 3 More Users and Giving them permissions ----

1. Now, Adding 3 More Users
2. Not giving them an Access key and not checking the Psw Reset Checkbox; Click on the Next: Permissions
3. We will create a group later We can see the previous user listed under the copy "permission from existing user" section (just for observation purpose) Click on the third section: Attach existing policies directly
4. Type in ec2fullaccess in the search box and click the check box for it; click on Next: Tags
5. Input the Key and Value for the Tag to keep track of your activities; Click on Next: Review

6. Click on Create Users Button

----- Logging in as one of the 3 new Users and Checking their permissions ----

1. Try logging in as one of the 3 new users just created
2. Try launching an EC2 instance via the new user
3. Hence, an instance has been created
4. Delete the bucket when done with your work

----- Creating a new Group and Giving it permissions ----

1. Select the members to be present in the group (max 4 per group)
2. Giving this group ec2fullaccess and s3fullaccess

----- Logging in as a member of the Group & Checking their permissions –

1. Now, login as one of the users from the group and try creating a S3 bucket
2. S3 bucket successfully created
3. Delete the bucket when done with your work

----- Creating a new Role -----

1. Go in the root user window and click on "create role" button in the "Roles" section of IAM Dashboard
2. Let it be the default options (you can choose any use case you like) Click in Next button
3. Give the permission suitable to the use case chosen
4. Give suitable Role name and description; rest would remain as default
5. Add a tag if you want to; click on Create Role button
6. The role has been successfully created
7. Just to check the overall users, groups and roles, you can check out the IAM Dashboard

Output/Observation:

Conclusion: Comment on implementation of IAM .