Om Shete
THADOMAL SHAHANI TSEC ENGINEERING COLLEGE
TE C32
2103163

Experiment No: 7

Aim: To study and implement Identity and access management (IAM) practices on AWS

Theory:

1. Explain the concept and need of access management

⇒ Access management (AM) is process of identifying and controlling and managing authorized or specified user access to a system, application or only IT instances.

- It is a board concept that encompases all policies, methodologies and tools to maintain access privilage.
- AM is primarily an information security, IT and data governance process used in gamming acceisses to valid users of prohibiting involved users.
- Typically AM is used in conjuction with identity access management IAM.
- Identify management creates, provision and controls the different users, roles and groups and policies whereas AM ensures that these roles and policies are allowed
- An AM based application states the different user roles and their policies.

• Explain IAM and its components

⇒ IAM is an identity and access management is the security discipline that enables the right individuals to access the right resources at the right reasons.

- These resources could be tools required to complete a job, access a database with mission critical data, on services and application hosted in cloud, etc.

- Components

It can be categorized into four components:-

1) Authentication
2) Authorisation
3) User Management
4) Central User Repository

• Compare the following in AWS

⇒

1) Root User and AWS IAM user

⇒ Root user is the first cloud service identity created by default when you create your cloud service provider account.

- It is important to note all cloud services providers have some form of root elements.
- AWS IAM users can be created by a root user or another IAM user who has entitlements on create additional IAM user.

- Can authenticate on start a remote session using their credentials on alias.
- Can corresponds to human, application process on another machine based identity.

2) Roles and Policies

⇒

Roles	Policies
i) Intended for guaranting temporary access for entities like application of service.	i) Defines permission and can be attached to user groups or roles.
ii) AWS resources on services.	ii) Attached to the IAM users, groups.
iii) Temporary access.	iii) Permanent permission.
iv) Defines who can assume the role.	iv) Trust relationship is not applicable as they do not involve.
v) Provides a way to grant precise permissions to a specific entity.	v) Defines a set of permissions that can be attached to multiple entities.

- Explain Inline and custom policies in AWS

⇒ An online policy is a policy created for a single IAM identity.

- Inline policies maintain a strict one to one relationship between a policy and identity either you can create a policy and embed it in an identity.
- An AWS managed policy is a standalone policy that is created and administration by AWS.
- Standalone policy that the policy has its own ARN that includes the policy name.
- You can create standalone policy in your own AWS account that you can attach to principal entities.

- Explain Multifactor Authentication in AWS

⇒ It is an AWS entity identity and Access Management best practice that requires a second authentication factor in addition.

(A) 15/3/2024