IAM

Name: Kantha Sishanth S

Reg No: 212222100020

Aim

To implement Identity and Access Management (IAM) in AWS to securely control access to resources by creating and managing IAM users, groups, roles, and policies for team collaboration.

Algorithm

1. Sign in to the AWS Management Console.
2. Navigate to the IAM service.
3. Create IAM groups with defined policies (e.g., Admin, Developer).
4. Create IAM users and assign them to appropriate groups.
5. Create IAM roles if cross-account or service-based access is needed.
6. Attach permissions using managed or custom policies.
7. Enable MFA (Multi-Factor Authentication) for users.
8. Monitor access using IAM Access Analyzer and CloudTrail.

Procedure

1. Access IAM

- Go to **AWS Console → Services → IAM**

2. Create IAM Groups

- Click **Groups → Create New Group**
- Name the group (e.g., `Admins`, `Developers`)

- Attach predefined or custom policies (e.g., `AmazonEC2FullAccess`, `ReadOnlyAccess`)

3. Create IAM Users

- Click **Users** → **Add Users**
- Provide usernames
- Choose access type:
  - **Programmatic access**
  - **AWS Management Console access**
- Assign users to the appropriate IAM group

4. Create IAM Roles (Optional)

- Go to **Roles** → **Create Role**
- Select a use case:
  - AWS service
  - Another AWS account
- Attach policies as required

5. Apply Policies

- Use AWS Managed Policies or create custom policies using JSON
- Attach them to:
  - Users
  - Groups
  - Roles

6. Enable Multi-Factor Authentication (MFA)

- Go to the IAM user → **Security credentials**
- Click **Manage MFA**
- Choose **Virtual MFA device** (e.g., Google Authenticator)

7. Monitor IAM Usage

- Use **IAM Access Analyzer** to review access
- Use **AWS CloudTrail** to audit actions and access logs

Sample Output

Entity Type	Name	Permissions Attached	MFA Enabled	Assigned Group
Group	Admins	`AdministratorAccess`	-	-
Group	Developers	`AmazonEC2FullAccess`	-	-
User	alice_dev	Inherits from Developers	Yes	Developers
User	bob_admin	Inherits from Admins	Yes	Admins
Role	EC2-S3-Access	`AmazonS3ReadOnlyAccess`	N/A	-

Outcome

- IAM users `alice_dev` and `bob_admin` were created and assigned to the appropriate groups.
- Groups `Admins` and `Developers` were configured with managed policies.
- MFA was enabled for all users.
- An IAM role `EC2-S3-Access` was created for EC2 instances to access S3 in a read-only mode.

Result

Successfully implemented identity and access management using **Amazon IAM**, enabling secure, role-based access control and ensuring team collaboration with best security practices.