Akshat Chheda
A007

In AWS, Identity and Access Management (IAM) is a service that enables secure management of users and permissions for accessing AWS resources. IAM lets you create users and groups with specified permissions, helping control who can access what within your AWS environment.

IAM (Identity and Access Management)

IAM is AWS's service for managing access to resources securely. It allows you to define who (users and groups) has permission to perform specific actions on AWS resources. By assigning permissions based on roles, IAM helps enforce security best practices, like the principle of least privilege , where users only have the minimum access needed.

Role of IAM

User and Group Management: IAM allows you to create individual users and organize them into groups for easier permission management.

Access Control: You can set permissions for users and groups to restrict access to specific AWS services or resources.

Roles and Temporary Access: IAM roles allow entities (like users, applications, or services) to assume specific permissions temporarily, reducing the risk of long-term access exposure.

Multi-Factor Authentication (MFA): IAM supports MFA, adding an extra layer of security by requiring a second form of verification.

Policy Management: IAM uses policies (written in JSON format) to define precise access controls, ensuring that each user, group, or role has specific access rights based on organizational needs.

IAM enables secure, flexible, and scalable access management for AWS resources, ensuring only authorized users and applications can perform specific actions

: