Identity Access management (IAM)

01 March 2025 19:59

What is IAM in AWS?

AWS **Identity and Access Management (IAM)** is a service that helps you securely control access to AWS resources. It allows you to manage **users, groups, roles, and policies** to define who can access what resources in AWS.

Key Features of IAM

1. **User Management** – Create and manage AWS users with specific permissions.
2. **Group Management** – Organize multiple users and apply policies to them collectively.
3. **Roles** – Assign temporary access permissions to AWS services or users.
4. **Policies** – Define rules for access control using JSON-based documents.
5. **Multi-Factor Authentication (MFA)** – Adds an extra layer of security to user authentication.
6. **Fine-Grained Permissions** – Restrict access to AWS services with detailed policies.

Types of IAM Policies

1. **AWS Managed Policies** – Predefined policies by AWS (e.g., AdministratorAccess, ReadOnlyAccess).
2. **Customer Managed Policies** – Custom policies created by users for specific needs.
3. **Inline Policies** – Directly attached to a user, group, or role.

3. What are IAM users, groups, roles, and policies?

- **IAM User** – A person or application that interacts with AWS.
- **IAM Group** – A collection of users with the same permissions.
- **IAM Role** – A temporary identity for AWS services, cross-account access, or applications.
- **IAM Policy** – A JSON document defining permissions for users, groups, or roles.

4. How does IAM help in securing AWS resources?

- Controls access using **least privilege principles**.
- Implements **MFA** for extra security.
- Uses **policies** to grant/deny access.
- Provides **temporary credentials** for applications.
- Monitors access through **AWS CloudTrail** lo

5. What is the difference between an IAM user and an IAM role?

IAM User

- **Definition**: An IAM user is an entity that represents a person or application that interacts with AWS resources.

IAM Role

- **Definition**: An IAM role is an identity that can be assumed by users, applications, or services to grant temporary

6. Can IAM policies be applied to groups?

Yes, IAM policies can be applied to **groups**, and all users in that group inherit the permissions. This helps in managing permissions more efficiently

7. What is the default permission for a new IAM user in AWS?

By default, a new IAM user **has no permissions**. The user must be assigned **policies** or added to **groups** to gain access.

8. What is an IAM policy

IAM policies are **JSON documents** that define permissions for AWS users, groups, or roles.

9. What is the difference between AWS Managed Policies and Customer Managed Policies?

AWS Managed Policy Predefined by AWS, used for common tasks (e.g., AdministratorAccess).
Customer Managed Policy Created by users to customize permissions.

10. What is an Inline Policy, and how is it different from a Managed Policy?

- **Inline Policies** are attached directly to a single IAM entity (user, group, or role).
- **Managed Policies** are reusable and can be attached to multiple IAM entities.