AWS Identity and Access Management (IAM)

Overview

Purpose: Manage access to AWS resources and services.

Users and Access

Root User:

Access: Full access to all AWS resources and services.

Responsibilities: Create and manage IAM users, groups, and roles.

Best Practice: Use only for account setup; use IAM users for daily tasks.

IAM Users:

Access: Limited to permissions defined by IAM policies.

Login: Can access the AWS Management Console based on assigned permissions.

IAM Roles:

Access: Temporary access to AWS resources for users or services.

Use: Ideal for cross-account access and delegating permissions.

IAM Groups:

Access: Collect multiple IAM users to manage permissions collectively.

Function: Assign permissions to groups rather than individual users.

Policies

Definition: JSON documents that define permissions for AWS resources.

Creating Policies:

Custom Policies: Write your own policies or use AWS templates.

Attach: Apply policies to users, groups, or roles to grant permissions.

Types:

Managed Policies:

AWS Managed: Predefined by AWS.

Customer Managed: Created by you.

Inline Policies: Directly attached to specific users, groups, or roles.

Scalability and Management

Scalability: IAM adapts to your needs, managing many users and permissions easily.

Best Practices:

Least Privilege: Give only the permissions needed.

Use Roles: Prefer roles for temporary access.

Regular Reviews: Check and update permissions regularly.