AWS IAM (Identity and Access Management) Documentation

Overview

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources.

IAM Architecture Diagram

Refer to the AWS IAM architecture diagram at:
https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

Key Components

Component	Description
IAM Users	Individuals with long-term credentials to access AWS services.
IAM Groups	Collections of users with identical permissions.
IAM Roles	Entities that define a set of permissions for making AWS service requests.
IAM Policies	JSON documents defining permissions (Allow/Deny) for users, groups, and roles.
Root User	The account created when you first set up your AWS environment with full access.
MFA	Multi-Factor Authentication adds an extra layer of security.

How to Configure IAM

Step 1: Access IAM Console

Go to AWS Console → Search "IAM" → Open IAM Dashboard

Step 2: Create a User

IAM Dashboard → Users → Add users
Enter username
Choose Access type (programmatic or console)
Set permissions

Step 3: Create Groups (Optional)

IAM Dashboard → User groups → Create group
Add users to the group
Attach policies

Step 4: Assign Policies

Attach existing policies or create custom JSON policy to define what actions the user/group/role can perform

Step 5: Enable MFA

Go to IAM → Users → Select User → Security Credentials → Manage MFA
Use virtual or hardware MFA device

Step 6: Use Roles for EC2 or Lambda

Assign IAM roles to AWS services (e.g., EC2, Lambda) so they can access other AWS services securely

Sample Use Case

A user named `DevUser` is added to a group `Developers` that has AmazonS3FullAccess policy. This allows the user to upload, read, and delete objects in S3 buckets.

Best Practices

- Do not use the root account for daily tasks.
- Enforce MFA for all users.
- Grant least privilege access.
- Rotate credentials regularly.
- Use roles instead of embedding credentials in applications.

References

• https://docs.aws.amazon.com/IAM/

• https://aws.amazon.com/iam/faqs/