Reference:

FAQs

Category:

Security, Identity, and Compliance

AWS Identity and Access Management (IAM)

What?

- AWS Identity and Access Management (IAM) provides fine-grained access control across all of AWS Services. With IAM, you can specify who can access which services and resources, and under which conditions.
- With IAM policies, you manage permissions to your workforce and systems to ensure least-privilege permissions.

Why?

- You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.
- You can grant other people permission to administer and use resources in your AWS account without having to share your password or access key.

When?

- You want to grant different fine-grained permissions to different people for different resources.
- You want to add two-factor authentication to your account and to individual users for extra security.
- You need to use existing corporate identities to grant secure access to AWS resources using identity federation.

Where?

- IAM is a global service.
- You use IAM to control access to tasks that are performed using the AWS Management Console, the AWS Command Line Tools, or service API operations using the AWS SDKs.

Who?

- You manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources.
- You can create multiple IAM users under your AWS account or enable temporary access through identity federation.

Complete book:

Click Here

How?

- With IAM, you define who can access what by specifying fine-grained permissions. IAM then enforces those permissions for every request. Access is denied by default and access is granted only when permissions specify an “Allow”.
- You can delegate access to users or AWS services to operate within your AWS account.

Created by:

Ashish Prajapati

How much?

- There is no charge to use IAM.