What is IAM?

* AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources.
* You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

Access types:

Programmatic access: access AWS cli

Aws management console access: access AWS console dashboard.

COMPONENTS:

USER:

* any person who wants to access your AWS account has to be added as user.

GROUPS:

* The users created, can also be divided among groups, and then the rules and policies that apply on the group, apply on the user level as well.

ROLES:

* Roles are similar to users but roles applied to applications.

POLICIES:

* To assign permissions to user, group, role or resource you create a policy, which is a document that explicitly lists permissions.

Policies and accounts

* If you manage a single account in AWS, then you define the permissions within that account using policies.
* If you manage permissions across multiple accounts, it is more difficult to manage permissions for your users. You can use IAM roles, resource-based policies, or access control lists (ACLs) for cross-account permissions.

Identity-based and resource-based policies

* To provide your users with permissions to access the AWS resources in their own account, you need only identity-based policies.
* Resource-based policies are popular for granting [cross-account access](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_permissions-required.html#UserPermissionsAcrossAccounts).
* Identity-based policies are permissions policies that you attach to an IAM identity, such as an IAM user, group, or role.
* Resource-based policies are permissions policies that you attach to a resource such as an Amazon S3 bucket or an IAM role trust policy.

Managed policies

* standalone identity-based policies that you can attach to multiple users, groups, and roles in your AWS account.
* You can use two types of managed policies:

AWS managed policies

* Managed policies that are created and managed by AWS. If you are new to using policies, we recommend that you start by using AWS managed policies.

Customer managed policies

* Managed policies that you create and manage in your AWS account.

Inline policies

* Policies that you create and manage and that are embedded directly into a single user, group, or role.
* In most cases, we don't recommend using inline policies.

Multifactor authentication:

* Provides additional security layer