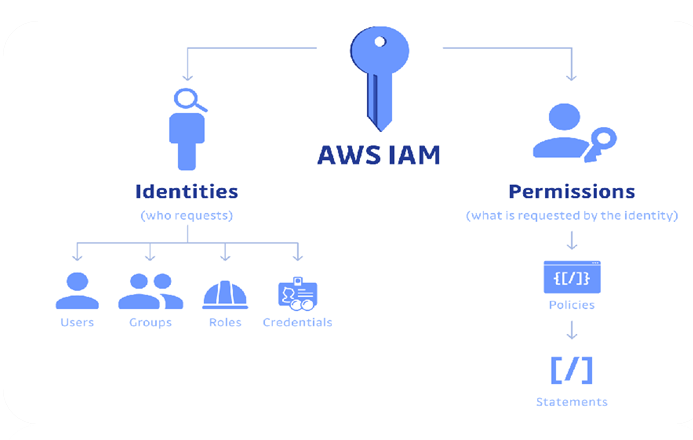
AWS IDENTITY AND ACCESS MANAGEMENT

AWS Identity and Access Management (IAM) :

It is a service that helps you securely control access to your AWS resources. It allows you to manage authentication (verifying who you are) and authorization (determining what you are allowed to do) for users and applications.



Identity :

An AWS identity is an entity that can be authenticated to access AWS resources and is used to determine what actions are allowed or denied.

Root user :

When an AWS account is first created, it has a single sign-in identity known as the root user. It has complete and unrestricted access to all services and resources within the account.

IAM user :

An IAM user is a permanent identity created within an AWS account to represent a person or application.

IAM Roles :

An IAM role is a secure identity that can be assumed by an entity that needs to interact with your AWS resources. Unlike an IAM user, a role does not have standard long-term credentials like passwords or permanent access keys.

* A role's permission is determined by the policies attached to it. It is designed to be temporary and provides access only for the duration of a session. When an entity assumes a role, it receives temporary security credentials.

Creditentials :

In AWS, IAM credentials are the authentication materials used to prove the identity of a principal (a person or application) to gain access to resources.

IAM Policies :

An IAM policy is the core document that explicitly defines what actions are allowed or denied on specific AWS resources.

* Policies are written in JSON and contain statements that define permissions.
* A policy statement includes elements like Effect (allow or deny), Action (e.g., s3:GetObject), and Resource (e.g., a specific S3 bucket).
* Policies can be attached to users, groups, or roles, controlling what those identities can do in AWS.

There are several types of IAM policies:

* AWS Managed Policies: Pre-built policies that are created and maintained by AWS for common services and use cases (e.g., AmazonS3ReadOnlyAccess).
* Customer Managed Policies: Standalone policies that you create and manage yourself, offering granular control and reusability across multiple identities.
* Inline Policies: Policies that are embedded directly into a single IAM user, group, or role. They are not reusable and are deleted when the identity is deleted.
* Resource-Based Policies: Policies that are attached directly to a resource (e.g., an S3 bucket or Lambda function) to specify who has access to it.

IAM and Identity Center :

* In AWS, IAM and Identity Center are both used for managing identities and access, but they serve different purposes and operate at different scopes.
* Whereas Identity Center is for managing workforce access across multiple AWS accounts and applications.

Amazon Cognito :

Amazon Cognito is a Customer Identity and Access Management (CIAM) service that allows developers to add user sign-up, sign-in, and access control to web and mobile applications.