what is IAM?

- IAM stands for identity access management.
- AWS identity and access management is a web service that helps you securely control access to AWS resources.
- with IAM you can manage permissions that control which AWS resources users can access.
- you use IAM to control who is authenticated and authorized to use resources.
- IAM provides the infrastructure necessary to control authentication and authorization for your AWS accounts.

why should i use IAM?

- AWS identity and access management is a powerful tool for securely managing access to your AWS resources.
- one of the primary benefits of using IAM is the ability to grant shared access to your AWS account.
- IAM allows you to assign granular permissions, enabling you to assign permissions, enabling you to control exactly what actions different users can perform on specific resources.
- IAM also provides several other security features.

what are the features of IAM?

- shared access to your AWS account.
- Granular permissions.
- secure access to AWS resource for applications that run on Amazon EC2.
- multifactor authentication.
- identity federation.
- identity information for assurance
- PCI DSS[payment card industry data security standard] compilance.
- integrated with many AW services.
- free to use.

How to access IAM?

- Open the AWS Management Console at https://console.aws.amazon.com/.
- The main sign-in page appears. Choose IAM user, enter the account ID (12 digits) or alias, and select Next.

Note:

You might not have to enter your account ID or alias if you've previously signed in as the IAM user with your current browser or if you are using your account sign-in URL.

- Enter your IAM user name and password and choose Sign in.
- If MFA is enabled for your IAM user, you then authenticate using it. For more information, see Using multi-factor authentication (MFA) in AWS.
- After authentication the AWS Management Console opens to the Console Home page.

How IAM works?

- https://docs.aws.amazon.com/images/IAM/latest/UserGuide/images/intro-diagram%20_policies_800.png
- the above link is the example of IAM workflow.

components of a request:

when principal tries to use the AWS management console, the AWS API or the CLI that principal sends a request to AWS. the request includes the following information.

Actions or operations:

- the actions or operations that the principal wants to perform.
- such as an action in the AW management console, or an operation in the AWS CLI or AWS API.

Resources:

- the AWS resource object upon which the principal requests to perform an action or operation.

principal:

- the person or application that use an entity to send the request.
- information about the principal includes the permissions policies.

Environment data:

- information about the ip address user agent, SSL enabled status, and the timestamp.

Resource data:

- Data related to the resource requested, such as a DynamoDB table name or a tag on an Amazon EC2 instance.