AWS IAM Integration Steps

Subtitle

Neeharica Madanu

Studio-Ghibli

1 April 2024

# AWS IAM

AWS Identity and Access Management (IAM), also known as Amazon Web Services Identity and Access Management, is an effective solution for securely managing access to AWS resources. It offers a comprehensive range of features, including the ability to manage users and groups, define permissions, and enforce multi-factor authentication for added security. IAM also enables the creation and management of roles to delegate permissions, as well as supports identity federation for streamlined single sign-on access. As such, IAM is a critical component for safeguarding the security of your AWS environment.

# IAM Integration Steps

The process of creating AWS IAM user roles involves comprehending the procedures for IAM role creation and determining the necessary permissions for administrators, testers, and developers in the project.

To create IAM roles, we can use either the AWS Management Console or the AWS Command Line Interface (CLI).

To create an admin role, we must define and create an IAM role with full access to AWS services required for administrative tasks.

To create roles for testers and developers, we must define and create IAM roles with permissions tailored to their specific job functions, adhering to the principle of least privilege.

In addition, we will need to attach the appropriate IAM policies to each role to grant the necessary permissions.

Finally, after creating the IAM roles, it is crucial to test them to ensure that users assuming these roles have the expected permissions and access.