IAM (Identity and Access Management) is a fundamental service in AWS that allows you to manage access to resources securely. Here's a breakdown of your questions:

Q1: IAM User vs. IAM Roles

IAM User:

- An IAM user represents a person or service that interacts with AWS. Each user has unique security credentials and permissions.

- Typically used for long-term access to AWS resources, especially for individuals or entities requiring persistent access.

IAM Role:

- An IAM role is similar to a user, but it is not associated with a specific person or service. Instead, it is assumed by anyone or anything that needs it for a specific task.

- Roles are temporary and can be assumed by AWS services, IAM users, or even external identities (e.g., users authenticated through a corporate directory).

- Roles are often used for granting access across AWS accounts or services and for providing temporary permissions to applications running on EC2 instances or Lambda functions.

Typical Uses:

- **IAM User:** Human users or services that require ongoing access to AWS resources. For example, developers, administrators, or automated scripts.

- **IAM Role:** Temporary access to resources for a specific task or use case. For example, granting permissions to an application running on EC2 to access an S3 bucket or allowing an AWS Lambda function to write to a DynamoDB table.

Q2: IAM Policy vs. Service Control Policy

IAM Policy:

- An IAM policy is a document that defines permissions, allowing or denying actions on AWS resources.

- These policies are attached to IAM identities (users, groups, or roles) and define what actions they can perform and on which resources.

- IAM policies are used for controlling access within a single AWS account.

Service Control Policy (SCP):

- An SCP is a type of policy in AWS Organizations that specifies the maximum permissions for member accounts in an organization.

- SCPs are applied at the organization level and affect all AWS accounts within the organization.

- SCPs are used for controlling permissions across multiple AWS accounts within an organization, enforcing centralized security policies, and ensuring compliance.

Difference:

- The main difference lies in their scope of application and purpose. IAM policies control access within individual AWS accounts, while SCPs control access across multiple accounts within an organization in AWS Organizations.

Typical Uses:

- **IAM Policy:** Controlling access to specific AWS resources within a single account.

- **Service Control Policy:** Enforcing security and compliance requirements across multiple AWS accounts within an organization.