What is a Role?

- A role is a set of permissions that grant access to actions and resources in AWS. These permissions are attached to the role, not to an IAM User or a group.
- An IAM User can use a role in the same AWS account or a different account.
- An IAM User is similar to an IAM User; role is also an AWS identity with permission policies that determine what the identity can and cannot do in AWS.
- A role is not uniquely associated with a single person; it can be used by anyone who needs it.
- A role does not have long term security credential, i.e., password or security key. Instead, if the user uses a role, temporarily security credentials are created and provided to the user.
- You can use the roles to delegate access to users, applications or services that generally do not have access to your AWS resources.

Situations in which "IAM Roles" can be used:

- Sometimes you want to grant the users to access the AWS resources in your AWS account.
- Sometimes you want to grant the users to access the AWS resources in another AWS account.
- It also allows the mobile app to access the AWS resources, but not want to store the keys in the app.
- It can be used to grant access to the AWS resources which have identities outside of AWS.
- It can also be used to grant access to the AWS resources to the third party so that they can perform an audit on AWS resources.

Following are the important terms associated with the "IAM Roles":

- **Delegation:** Delegation is a process of granting the permissions to the user to allow the access to the AWS resources that you control. Delegation sets up the trust between a trusted account (an account that owns the resource) and a trusting account (an account that contains the users that need to access the resources). **The trusting and trusted account can be of three types:**

- Same account
- Two different accounts under the same organization control
- Two different accounts owned by different organizations.

To delegate permission to access the resources, an IAM role is to be created in the trusting account that has the two policies attached.

Permission Policy: It grants the user with a role the needed permissions to carry out the intended tasks.

Trust Policy: It specifies which trusted account members can use the role.

- **Federation:** Federation is a process of creating the trust relationship between the external service provider and AWS. For example, Facebook allows the user to login to different websites by using their facebook accounts.
- **Trust policy:** A document was written in JSON format to define who is allowed to use the role. This document is written based on the rules of the IAM Policy Language.
- **Permissions policy:** A document written in JSON format to define the actions and resources that the role can use. This document is based on the rules of the IAM Policy Language.
- **Permissions boundary:** It is an advanced feature of AWS in which you can limit the maximum permissions that the role can have. The permission boundaries can be applied to IAM User or IAM role but cannot be applied to the service-linked role.
- **Principal:** A principal can be AWS root account user, an IAM User, or a role. The permissions that can be granted in one of the two ways:
  - Attach a permission policy to a role.
  - The services that support resource-based policies, you can identify the principal in the principal element of policy attached to the resource.
- **Cross-account access: Roles vs Resource-Based Policies:** It allows you to grant access to the resources in one account to the trusted principal in another account is known as cross-account access. Some services allow you to attach the policy directly, known as

Resource-Based policy. The services that support Resource-Based Policy are Amazon S3 buckets, Amazon SNS, Amazon SQS Queues.