 Always assign a role to the EC2 Instance to ensure secure access to AWS resources from EC2 Instances. An IAM role is similar to a user; it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, an IAM role does not have standard long-term credentials (password or access keys) associated with it. Instead, if a user assumes a role, temporary security credentials are created dynamically and provided to the user. You can use roles to delegate access to users, applications, or services that normally don't have access to your AWS resources.