An IAM policy is a way to allow or deny users to perform certain actions in an AWS account. When a user or a role is created, by default they only have permission to login. They cannot view, modify, or create any new resources. IAM policies are used to grant additional permissions. IAM policies can be defined at very granular levels, so it's important that you understand how to use them safely.

Kion helps you apply IAM policies across your organization and acts as a central repository for all of your IAM policies. Create a policy once and apply it to all the necessary cloud access roles. When you need to make a change, just update the policy in a single place and Kion will modify that policy in all of your accounts via cloud access roles.

Different types of policies in AWS often overlap. AWS IAM policies, AWS SCPs, and permissions boundaries all control an entity's (i.e. a user, user group, or role) permissions. To learn more about this, see the What is a Permissions Boundary? article.