AWS Security – IAM

IAM provides the infrastructure necessary to control authentication and authorization for your account. It includes following elements.

IAM Resources

The user, group, role, policy, and identity provider objects that are stored in IAM. As with other AWS services, you can add, edit, and remove resources from IAM.

IAM Identities

The IAM resource objects that are used to identify and group. You can attach a policy to an IAM identity. These include users, groups, and roles.

IAM Entities

The IAM resource objects that AWS uses for authentication. These include IAM users and roles.

Principals

A person or application that uses the AWS account root user, an IAM user, or an IAM role to sign in and make requests to AWS. Principals include federated users and assumed roles.

Actions or operations

IAM supports approximately 40 actions for a user resource, including the following actions:

* CreateUser
* DeleteUser
* GetUser
* UpdateUser

To allow a principal to perform an operation, you must include the necessary actions in a policy that applies to the principal or the affected resource.

## **How Does IAM Work?**

The IAM workflow includes the following six elements:

1. A principal is an entity that can perform actions on an AWS resource. A user, a role or an application can be a principal.
2. Authentication is the process of confirming the identity of the principal trying to access an AWS product. The principal must provide its credentials or required keys for authentication.
3. Request: A principal sends a request to AWS specifying the action and which resource should perform it.
4. Authorization: By default, all resources are denied. IAM authorizes a request only if all parts of the request are allowed by a matching policy. After authenticating and authorizing the request, AWS approves the action.
5. Actions are used to view, create, edit or delete a resource.
6. Resources: A set of actions can be performed on a resource related to your AWS account.

Let us explore the components of IAM in the next section of the AWS IAM tutorial.

AWS IAM Resources

1. User
   1. Can be user/application.
2. Group
   1. Collection of users.
   2. All users in the group will inherit permission of the group
3. Role
   1. Roles created are assigned to AWS resources.
4. Policy
   1. Defines Permissions
   2. JSON formatted document
   3. Can be assigned to User/Group/Role