Identity and Access Management

When it comes to accessing your account (the root account) and then working inside of it, you need the Identity and Access Management (IAM) services of AWS. IAM allows you to grant access to other individuals for team management of the services. IAM permits extremely granular permissions. For example, you might grant someone read access to only a single bucket of objects in S3. Other features of IAM include the following:

Access from service to service in AWS

For example, you can have an application running on an EC2 instances access an S3 bucket. We often use roles for such access.

Multi-factor authentication (MFA)

Permitting access through a password and a code from an approved device, thus strengthening security greatly.

Identity federation

Users who have already authenticated with another service can gain temporary access to resources and services in your account.

Identity information for assurance

CloudTrail can trace and log all SPI activity against every service and resource in your account.

PCI DSS compliance

IAM supports the processing, storage, and transmission of credit card data by a merchant or service provider, and it has been validated as being compliant with the Payment Card Industry (PCI) Data Security Standard (DSS).

Integration

In order to be successful, IAM integrates with every major service of AWS.

Eventually consistent

Amazon replicates important data around the world with their Global Infrastructure, to help ensure high availability (HA). As a result, data in some locations might lag others. Therefore, with IAM, consider implementing your changes for IAM first, then verify full replication before working with dependent service deployments.

Always free

While some services of AWS can be used for one year free (using the Free Tier account), IAM services remain free for the life of your account.

Accessibility options

You can access the components of IAM in a variety of ways, including the AWS Management Console, AWS command-line tools, AWS SDKs, and the IAM HTTPS API.

Main Identities Used In IAM

- AWS account root user: This is the account you
- established when you signed up for AWS. note that
- the user name for this account is the email address
- used for signup.
- Users: These are the entities you create in AWS to
- represent the people or services that use the IAM user to interact with AWS. When you create an IAM user, you grant it permissions by making it a member of a group that has appropriate permission policies attached (recommended) or by directly attaching policies to the user. You can also clone the permissions of an existing IAM user, which automatically makes the new user a member of the same groups and attaches all the same policies.
- Groups: A collection of IAM users. You can use groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users.
- Roles: These are similar to user accounts, but they do not have any credentials (password or access keys) associated with them.