Chapter 3 : IAM (Identity Access Management)

Rahul Daware

May 9, 2018

IAM allows you to manage users and their level of access to the AWS console

What does IAM gives you?

- Centralized control of your AWS account
- Shared access to your AWS account
- Granular permissions
- Identity Federation (including Active Directory, Facebook, LinkedIn etc)
- Multifactor Authentication
- Provide temporary access to users/devices when necessary
- Allows you to setup your own password rotation policy
- Integrates with many AWS services
- Supports PCI DSS Compliance

Critical Terms

- Users - End Users (think people)
- Group - A collection of users under once set of permissions
- Roles - You create roles and assign them to AWS resources
- Policies - A document that defines one or more permissions

Summary

IAM consists of the following:

- Users
- Groups (A way to group our users and apply policies to them collectively)
- Roles
- Policy Documents (Made of JSON)
- IAM is universal. It does not apply to regions at this time
- Root account is simply the account created when first setup your AWS account. It has complete Admin access.
- New users are assigned **Access Key ID and Secret Access Keys** when first created

- These are not the same as password, and you cannot use the access key ID and secret access key to login to the console. You can use this to access AWS via the APIs and command line however
- Always setup multifactor authentication on your root account
- You can create and customise your own password rotation policies