**IAM: USERS AND GROUPS**

IAM = Identity and Access Management. It is a global service, IAM is used to create users and assign them to group(s). Groups can only contain users. A user can belong to two or more groups, also a user can stand alone (belong to no group).

Groups helps us to assign various permission and services to certain users. Grouping is a good way of limiting what a user can or can’t do.

Permissions can also be referred to as policies

**IAM: PASSWORD POLICY**

IAM allows us to implement certain set of policies for password creation. This includes:

* Strong password = better security for your/our account.
* AWS allows a user to set password policies:
  + Set minimum length
  + Set allowed characters
* Allows users to change their own passwords.
* Allows users to change their passwords after a period of time.
* Prevent password re-use
* Multi Factor Authentication – MFA

MFA allows a user to protect their account. This is a combination of your password and your logged in device. This ensures that if your password is compromised, the hacker will not have access to your account unless they have access to your device. There are certain applications that offer the MFA service on AWS.

They are:

- Google Authenticator

- Authy device

- Others…

The only downside in using MFA is; losing your device. You will not be able to log in to your AWS account.

**Accessing AWS as a user**

A user can accessed its AWS account through certain means. They include:

- AWS Management console.

- AWS Command Line interface

- AWS Software Development Kit

Any permissions given to a group/user through the console, will reflect in CLI.

AWS have a terminal/CLI just in case a user does not want to use the one on its local machine.

**IAM ROLES.**

Roles are used to grant permission to entities that a user trusts. They act as ‘middlewares’.

**IAM Guidelines and Best Practices**.

- Remember not to use the root user except you want to create other users with it.

- Do not expose your access keys.

- Create a strong security this include the password policies and the MFA.

- Before using a service, make sure a Role have been created for it.

- Make sure users are always in group.

- The term policies refers to users/groups while roles refer to services.