IAM [IDENTITY & ACCESS MANAGEMENT]

* IAM is used to create multiple users and groups in one aws account and giving them permissions to use aws resources.
* The main reason for IAM is creating new users & groups and giving only certain permissions to only some aws resources within only one account.
* You can set passwords, policies, add users to groups.
* By default, users can't access to your account until you assign them policies to access.
* We create users, assign password to the users. Create groups, add users to groups and assign policies to the groups and users.
* We can assign policies to the users, when we add user to group, the user will get his own policies and the group policies.
* After you create an IAM user, an ARN will come, iam user has to login with that ARN and with the password we have created.

CREATE AN IAM USER AND GROUP

* To create an IAM user. Go to IAM console

**Click users.**

**Click Add user.**

**Type a user name.**

**Select Access type (programming or console or both).**

**Give a password (auto-generated or custom).**

**Select policies to user & add to grp.**

**Click Create and user is created.**

* To create groups,

**Click groups (left pane).**

**Click add group.**

**Type a name to group.**

**Add policies to group.**

**Click Create.**

**Click on Group.**

**Click add user.**

**Select users to add to group.**

* To add policies to an IAM user,

**Go to users.**

**Select user.**

**Click ADD permissions.**

**Select policies you want.**

**Click, Save.**

* By default, except root no one has access to billing even if IAM user has admin access. To access billing you have to create a new policy and add it to IAM user.
* To create billing policy,

**Go to IAM.**

**Select policies.**

**Click Create policy.**

**Select policy generator.**

**Effect = allow.**

**AWS Service = Billing.**

**Select Actions (view, write).**

**Type a name to policy and click create.**

* You can set a password policy like min length, upper letters, special characters and allow IAM users to change their own passwords and password expiration etc.

**To create a password policy.**

**Go to IAM.**

**Click account settings.**

**In password policy section.**

**Select the options you want to set for policy and click Apply.**

MFA [MULTI FACTOR AUTHENTICATION]

* MFA adds extra security by sending a code to the registered device. You need to enter that code when users access aws website or resources
* There are three types of devices which are supported by aws. They are
* **Virtual mfa device** - A virtual device is software running in your mobile or any device.
* **Hardware mfa device** - A hardware device is a device which supported by aws.
* **Sms-based device** - An SMS-Based device is nothing, but a SMS comes to your mobile.
* To enable a virtual device

**Go to IAM, click users.**

**Select user to assign MFA.**

* In security credentials tab.

**Click Assign MFA device.**

**Select type of device = virtual.**

**It gives a configuration key and QR code.**

**Open the software type the key or scan QR code.**

**After scanning or entering key.**

**the virtual device generates OTP’S. Type code 1 and code 2.**

**Choose Activate MFA.**

* To Enable hardware device,

**Go to IAM.**

**Click user to assign MFA.**

* In security credentials tab.

**Click assign MFA.**

**Select type of device = hardware.**

**Type the serial number of your hardware device (back on your device). Type authentication code 1 and wait 30sec type code 2.**

**Choose Activate MFA.**

* To Enable SMS-based device,

**Go to IAM.**

**Click user to assign MFA.**

* In security credentials tab.

**Click assign MFA.**

**Choose sms-based.**

**Type mobile number.**

**It will send a sms to your registered number.**

**Click Activate MFA.**