Module-1 : IAM (Identity and Access Management)

Key Features of IAM

- 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 for users / devices and services where necessary
- Allows you to setup your own password rotation policy
- Integrates with many different AWS services
- Supports PCI DSS Compliance

Key terminology for IAM

1. **Users**
    i. End users such as people, employees of an organization etc.
2. **Groups**
    i. A collection of users. Each user in the group will inherit the permissions of the group.
3. **Policies**
    i. Policies are made up of documents, called Policy Documents. These documents are in format called JSON (Java Script Object Notation) and they give permission as to what a User/Group/Role is able to do.
4. **Roles**
    i. You creates roles and then assign them to AWS resources.

Create IAM user in practical

Steps

1 Open AWS console - login to your aws account

2 Be sure about your region - select always US East (North Virginia)
-why to select mainly this region ?
-Because all of any New Services or Products are available or Launch for that region firstly

3 Open Services tab in console - Select IAM
In IAM user board there is link of IAM user and also you can customize which is publicly accessible URL for user from anywhere he can login.

Steps

1 Delete your root access keys

2 Activate multifactor authentication using MFA on your root account

Activate any MFA

- what is virtual MFA? = A virtual MFA device uses a software application to generate an authentication code with which a user is granted access only after successfully providing evidence to an authentication device. Ex-Microsoft authenticator - take snapshot or photo of your QR code safe somewhere so you can access or activate again your account if you use lost your phone or else.

- what is u2f security key?= Universal 2nd Factor (U2F) is an open standard that strengthens and simplifies two-factor authentication (2FA) using specialized Universal Serial Bus (USB) or near-field communication (NFC) devices based on similar security technology found in smart cards.

- what is other hardware MFA devices? = A hardware MFA device generates a six-digit numeric code based upon a time-synchronized one-time password algorithm.

Note - while creating user region is automatically set up to global, you can't create same user in different region.

Steps for creating IAM users

4 Select create individual IAM users
-select manage users - add user - name - XYZ -
-Select AWS access type - select - programmatic access (for EC2 instance) and AWS management console access both

-Console password - select autogenerated password
- tick on checkbox of must create new password new sign in
-Set Permissions - Add user to group - create group
-group name - developers
- add policies - example - administration access (GOD Mode)
- create group
- click next to add user to group
-next review
-click add user

After

User details
- access key ID - it is for user
- secret access key - it is for programmatic access(EC2) and it is only for one time show so you can just download and save very safe.

5 Apply an IAM password policy
- click manage password policy
- click on checkbox you want that In policy
- click apply

***Note - Open CSV file to see your passwords**

What is IAM Roles ?
= Use of One AWS service to other AWS service

Create Roles
Steps

1 Add AWS service - Select EC2
2 Click Next Permissions - attached permission policies - s3 full access (orange icon means Amazon managed policies)
3 Click on - Create Role
i. Role name - ABC_admin_access
ii. Click - create role

What we have learn so far ?

- **IAM is universal. It does not apply to regions at this time.**
- **The "root account" is simply the account created when first setup your AWS account. It has complete Admin access .**
- **New users have no Permissions when first created**
- **New users are assigned Access key ID & Secret access keys when first created**
- **These are not same as password. You cannot use the access key ID & Secret Access key to login in to the console. You can use this to access AWS via the APIs and Command Line.**
- **You can get to view these only once. If you loose them, you have to regenerate them. So, save them (CSV file) in a secure location.**
- **Always setup MFA authentication on your root account.**
- **You can create and customize your own password policies.**