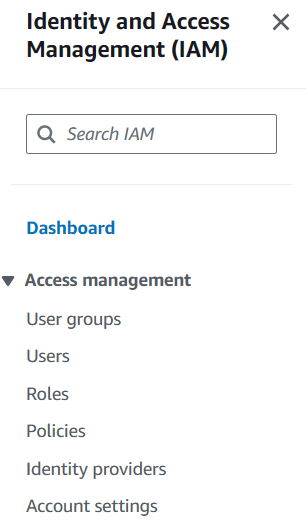
AWS IAM



* AWS IAM is a life time free service among AWS 200+ services
* We need IAM service, to provide authentication and authorization
* **IAM – IDENTITY(**Authentication) **ACCESS(**Authorization**) MANAGEMENT**

**Authentication:**

* If user wants to use AWS Services, he needs to login using credentials like user name and password this is called authentication.
* AWS also provide the second layer protection for security purpose which is called MFA (Multi Factor Authentication)



1**.credentials**



**2. MFA**



**I – Identity – Authentication will be provided (Eg: MFA) -only to login**

**A – Access – To use any of those 200+ services we need access (authorization)**

**M – Management**

After login, if we want to use any services, we need authorization.

Username and password – root credentials/ root user (in AWS)

>root user is used only to create the account. So, AWS will say the best practice is to create IAM User and use all the services.

**IDENTITY:**

**IAM USER**

Identity has 2 sub features

**IAM ROLE**

**IAM USER:**

* IAM Users will just login they don’t have any permissions

Eg: Organization has 20 people we will create 20 IAM Users

* After creating, there are so many ways to login like console, cli, http Api’s and program. So, for that when creatin IAM user we have 2 options console or cli/sdk. If one needed to login through programming, one requires access keys, secret keys
* So, as we said earlier user has permission only to login, if they need permissions we need to authorize.
* Every user many not require all the permissions, for example we have DB User, Storage user and so on… so we give permission to DB User only for DB & Storage user only storage. These permissions are called IAM Policies
* Username, password, secret keys, access keys are provided only to IAM Users

**IAM ROLES:**

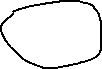
* IAM Roles will be used only for authentication
* In general, we use IAM Roles for temporary credentials

EG: I want to download files from s3 by connecting from EC2 server

Can create IAM USER



I have 2 options



Can create IAM ROLE



In the above example, we can simple create IAM Role and attach it to EC2 Server. So, when we create the role, AWS will itself create temporary credentials. When we call EC2 server, temporary credentials will be provided, that temporary credentials will be automatically expired after an hour.



* IAM Roles just have access and secret keys, they don’t have console access
* For console access, we need to attach policies to IAM Roles

**ACCESS:**

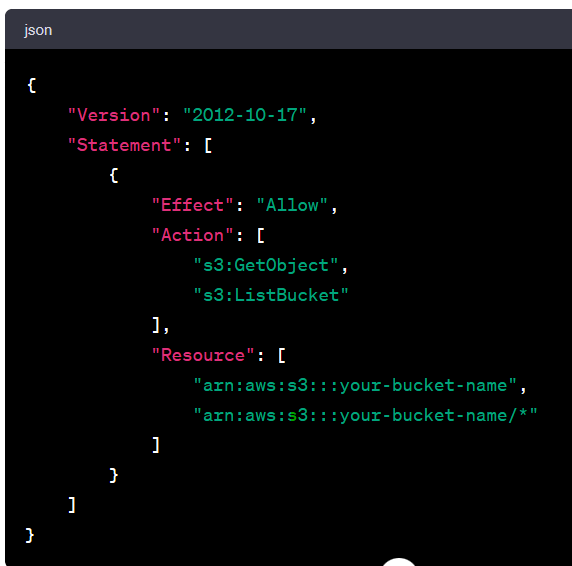
**IAM POLICIES:**

* AWS provides 2 types of policies
* AWS Managed – standard policies created by AWS

EG: Administrative full access

* Customer Managed- In order to provide operation based fine grain control access
* To use any service in AWS, AWS provides two types of access
* Full permission – read, delete, add
* Read only Access
* In AWS, every policy will be in Json format

Example:



**IAM GROUPS:**

Example: we have 4 teams:

* DB team – 20 DB groups
* Storage team – 20 storage groups each group has 20 users
* Admin team – 20 admin groups
* Compute team – 20 compute groups

For all the users we need to create IAM policies and if its for 100 users creating policies for each member will be difficult, so we create groups, apply policies to that groups and add users into that individual groups, so that policies will be applicable to each user.

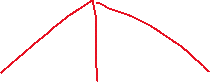
1. How to Create IAM USER?

* First login to the AWS Console
* Then go to IAM service
* Then go to users
* Click on create user -> provide the username and it can be done in 2 ways:
* Console -mostly used
* Cli/sdk
* After checking AWS console -> want to create IAM User -> auto generate password -> user change password for next login -> set permissions

Attach policies

Copy permissions

Add users to group



* We will restrict the users by attaching policies, and policies will be of two types 1. **Custom managed** & 2. **AWS managed**
* click on next and check on create user. User will be created and a .csv file will be generated we will download that credentials and login using those credentials and as we chose the option of user changing password-it will ask to reset password after entering the credentials.