**IAM ( Identity And Access management)**

IAM

------------------

It’s related to administration.

AWS identity and access management ( IAM ) is a service that helps you securely control access to Aws resources . you use IAM to control who is authorized(permissions) to use resources .

When you first create an Aws account ,it has complete access to all Aws services . this identity is called the AWS account root user .

++++++++++++++++++++++++++++++++++++++++++++++++

Every company will have only one AWS Account .

Owner of the account,can create user account .

We can give limited privileges to user account .

Ex :

User A ----- > should have Ec2 full Access

User B ------ > should have s3 full Access

User C ----- > should have EC2 read only access

Using IAM ,we can

1. Create users.
2. Create groups.
3. Assing permissions to the users and groups.

++++++++++++++++++++++++++++++++++++

As All of our created aws account .

That mean ,we started using IAM service.

By default ,we are all adminisitrators.

+++++++++++++++++++++++++++++

Lets login to aws account.

Service ------ >security,identity and compliance --🡪 IAM

++++++++++++++++++++++++++++++++++++++++++++++++++++++

**Lets create a user**.

Then go to users ----- > Add user --- > user name --- > RAVI --- >

Access type ---we select both

Programmatic Access

AWS management console Access

Custom paswd ----Ravi123@

NOTE : - We are not select the reset passwd (remove the tick mark)

------- > Next:permissions

We select Attach existing policies

Then we need [AmazonEC2FullAccess](https://console.aws.amazon.com/iam/home?region=ap-southeast-1#/policies/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEC2FullAccess)

NEXT---- > next --- > create user

Then again create a new user called LATHA

Then go to users ----- > Add user --- > user name --- > LATHA --- >

Access type ---we select both

Programmatic Access

AWS management console Access

Custom paswd ----Latha123@

NOTE : - We are not select the reset passwd (remove the tick mark)

------- > Next:permissions

We select Attach existing policies

Then we need [AmazonS3FullAccess](https://console.aws.amazon.com/iam/home?region=ap-southeast-1#/policies/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonS3FullAccess)

NEXT---- > next --- > create user

Account id :

RAVI

ravi123@

LATHA

Latha123@

Then signout the Amazon account & sign in again

long with -----IAM USER

Account id : 432970265736

IAM USER NAME : RAVI

PASSWORD : Ravi123@

He can have a EC2 full access only

The create a EC2 instance

But he cannot create a s3 bucket because he didn’t have any other permissions.

Then signout the Amazon account & sign in again

long with -----IAM USER

Account id : 432970265736

IAM USER NAME: LATHA

PASSWORD : Latha123@

He can have a s3 full access only

The create a s3 bucket

But he cannot create a EC2 instanse because he didn’t have any other permissions.

Let’s try

Existing user can have two permissons (add one more policies)

Then select the user (ravi or latha ) any one of them -- > Add permissions --- > Attach existing policies directly

AMAZON s3 full access -- > add permissions ---- >

**GROUP CONCEPT**

Lets create a group

Then groups --- > group name ---EC2Group ---- > Attach policies --- > AmazonEC2FullAccess --- > Next --- > create group -- >

Note : this is group is doesn’t have any users.

Then go to users ----- > Add user --- > user name --- > user1 --- >

Access type ---we select both

Programmatic Access

AWS management console Access

Custom paswd : user123@

NOTE : - We are not select the reset passwd (remove tick mark)

Next --- > permissions -- > Add users to group ---- >

Select the ----- > EC2GROUP --- > NEXT --- > creat user

Then go to groups—select the Ec2 group --- > select the user1 --- > adduser

And as well as we remove the user also.

AWS services connected in to ways

GUI ( graphical user interphase )

CLI ( command line interphase)

**IAM ROLES CONCEPT**

USE of role : when one service is communicate with other service at that time we are using IAM roles.

EX : EC2 ----------------------------------- -----S3

Communicate with

Then create a one EC2 instance --- Allowed --- > all traffic ---- > create

Connted with git bash.(top)

**Note : --- Now create one role**

Then go to IAM Dash board --- > roles --- > create role --- >

Select type of trusted entity ----- . inthis --🡪 we select -🡪

-🡪 AWS SERVICE EC2 LAMBDA AND OTHERS ----- >**Common use cases ----select ---------- -- EC2-----**---- > next permissions -- >

**Note : Attach policies to the role**

Attach permission policies -- >

---- > [AmazonS3FullAccess](https://console.aws.amazon.com/iam/home?region=ap-southeast-1#/policies/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonS3FullAccess) --- > next -- > role name --- Myrole1

Role description 🡪 ALLOW EC2 instances to call service on your behalf

---- > create role --->

**Note : This role having s3 full access**

**3 ) Attach role to EC2 machine**

**Then go EC2 dash board ---- > select the particular machine --- > actions**

**--- >security ----- > modify IAM role --- > then select the myrole1 --- >save**

**Then create s3 bucket**

**aws s3 ls**

**it will be appear in git bash**

**then create one user**

aws iam create-user --user-name test1

note : we don’t have permissions to crate it .

then go --- >IAM --- > select the myrole 1 -- > Attach policies --- > [IAMFullAccess](https://console.aws.amazon.com/iam/home?region=ap-southeast-1#/policies/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FIAMFullAccess) --- >attach policies

NOW go to git bash

aws iam create-user --user-name test2

it will work out

then delete the role