**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 (has 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 root Account.

Owner of the account, can create user accounts.

We can give limited privileges to the user accounts.

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) Assign permissions to groups and users.

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

As all of our created AWS account.

That means, we have started using IAM Service.

By default, we are all administrators.

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

Let’s login to AWS

Services ---> Security, Identity and Compliance --> IAM

Observe, under security status

We have five options.

IAM is all about working with those 5 options.

1) Delete you root access keys

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

It is tick.

This means out root access keys are deleted.

We can Work with AWS using GUI and CLI

Till now we are accessing AWS using GUI

To login to AWS using GUI, we need email address and password

To login to AWS using CLI, we need access keys.

As root access keys are deleted, we cannot login using CLI

2) Activate MFA on your root account (Multi factor authentication)

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

Select activate MFA on your root account ---> Manage MFA ---> Continue to security credentials

--> Multifactor authentication ---> Activate MFA ---> Virtual MFA device --> Continue --> Show QR code.

Now, scan QR code by using "Google Authenticator Mobile APP"

We will get MFA codes, Enter MFA codes

3) Create Individual users

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

Let’s create two groups

1st Group name - Ec2Group

2nd Group name - S3Group

For 1st group, lets provide Ec2 full access.

For 2nd group, lets provide S3 full access.

Let’s create two users

Raj and Hari

We will Assign Raj to Ec2Group

Assign Hari to S3Group.

Now, for both the users, will attach a policy "Glacier full access"

So, Now Hari will have two permissions (S3 full access and Glacier full access)

If Hari is removed from the group, He will have only Glacier full access)

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

Let’s practically implement it.

Creating users

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

Select Create individual IAM users -->Manage users ---> Add user -->

username - raj (Add another user)

- hari

Access type - programmatic access (CLI)

AWS Management console access (GUI)

Select both the check boxes

Select autogenerate password

Require reset password - uncheck (We do not want users to change the password)

next: permissions ---> Create group.

Group name - Ec2-Group

Under Filter policies -- search for - ec2 (Select AmazonEC2FullAccess)

Create group.

Next: Tags ---> Next: Review ---> Create users.

Close

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

Observation:

Both the users are assigned to EC2Group

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

Let’s create 2nd group

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

In dashboard --> groups ----> create new group --> Group name: S3-Group

Next Step --> Policy type - search for - S3 (Select AmazonS3FullAccess)

Next Step --> Create Group.

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

Goto Ec2 group --> Remove hari from group.

Now, select groups (Dashboard) --> S3-group --> Add users to group --> Select hari --> Add Users

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

Now, Assign Glacier full access directly to the users

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

Users---> Select hari ---> Add permissions --> Attach existing policies directly

search for "glacier" (Select AmazonGlacierFullAccess) ---> Next: Review --> Add permissions

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

Go back to dashboard

Apply an IAM password policy

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

Manage password policy ---> set password policy

min length - 8

select all check boxes

Save changes

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

Now go to dashboard, We have discussed, all the five options.

Let’s test:

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

Users ---> raj ---> Security credentials ---> create access key

console password: Manage

Set password: Autogenerated password

Apply

Show password (Copy it)

Take note to account ID from My Account

++++

How Raj can login

Open new browser (Private window)

Login to AWS

Enter Account ID --> Next -->

IAM User name - raj

Password - provide the password

Sign in

Services ---> EC2

test, can he launch instances?

Try

Service ---> S3

Error Access Denied!!!

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

If a user needs to regenerate password

Console password: Manage

Autogenerated password --- Apply

Show password (Provide new password to user)

We get the new password

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

Users ---> Hari

We can see two permissions (Glacier full - Attached directly

S3 full -- Attached from group)

Remove the user from the group.

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

Users -- Delete Users

Groups -- Delete Groups

Apply an IAM password policy ---> Manage password policy --> Delete password policy

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