* **Introduction to Identity & Access Management**
* **Components of IAM**
* **Creating and Managing Users & Groups**
* **Creating and Managing IAM Policies**
* **Roles and its use cases**
* **Multi-Factor Authentication – [MFA]**
* **Security Features in IAM**
* **Best Practices of IAM**

**Components of IAM:-**

**->groups**

**->users**

**->roles**

**->polices**

**->identity management**

**IAM --Identity and Access Management (user management)**

aws--resource-->user

Root -->IAM--> secure -->resource

**IAM is a global service**

**it is free**

service-->resources (object) (component)

**IAM is a aws service and its resource or object or component are user which we create.**

user--> secured access to use aws resource

Group-->collection of user

(dir --> rwx) --> policy --> attached-->username

Policy-->Rapping of permission

Role

**In IAM we can create 5000 user**

**At a time we can create 10 user**

**300 groups**

**Policy are 1000 and we can give 10 policy to a single user.**

**features:-**

============

1. Share access to your aws account

2. Granular permission

3. MFA (multi factor authentication service) with help of otp

4. Free to use

5. Centralized control of your AWS account

6. Permission based on organizational groups

7. Networking controls

8. Provide temporary access for user/device and services where necessary

9. Integrates with many different aws services.

10. Eventually consistent.

**Password Access type in AWS:**

=========================

**Programmatic**==> cli ,s/w development kit

i)Access key id

ii) Secrete access key

python 2.5

libries

aws cli

aws configure

**Console =**=>username ,password

h/w --> API ?

user --> Akshya-->programmatic + console

user--> permission

#add user to group

#copying permission from exiting user

#attach existing policies directly

aws manage policy ==>policy--> user permission(read access, full access)

Customer manage policy==>there will be no icon->the policy which we create

**POLICIES:-**

It use to allocate permission to user.

user==>dir1 (if we want to give user read write permission on a particular directory)

**Policies type:-**

**1)aws manage policy-->**limited policy we get->full access, read only, we will get to attach to a user->user-->attaches

**2)Custom manage policy-->** customize policy--> user can apply

There is one service s3 service--> bucket-->it store data in object form

company-->aws acc created-->100 user or employee will access

two team :-i)developer ii)operation

\*go to s3 create one bucket and give bucket name (myaws-bc1)

\*name should be worldwide unique

\*cheek it by other user is he accessing that bucket ( it will access) and he will acces other bucket too because we have attached aws manage policy to him.

\*but i want that a particular user only access my created bucket(myaws-bc1) not other bucket so i have to attach him custom policy.

\*go to iam click on policy and click on create policy

\*I have to create that policy in which a particular user can access my created particular bucket which he can read and list only

manoj --> policyname (s3(service name +myaws33(backute name) + read list(action))

click on create policy(visual editior or by JSON)

chosse service name -->s3

choose actions --> read, list

click on resources

choose bucket

add ARN and add bucket name to it

next tags

add tags (key -purpose value - read list operation) next review

review policy:- name(Bucketreadlist) ,description

click on create policy

go to other user (manoj) cheek if he can use that buket and we can see he can use or read all buckets.

now go to root account and and click on your created user (manoj)

now search s3 service cheek your created bucket (myaws -bc1)

now i want that my user(manoj) only access my created bucket not others

for this purpose i created one policy in which i already selected service na resource name.

now i have to attach that policy to that particular user (manoj)

remove all existing (detach) policy from user (manoj) and attach created policy to it.

click on filter policy and then coustum manage policy and choose your created policy(BucketReadlist).

now try to access from other user (manoj)

cheek his acess colomn

we use or read our created bucket which is attached in our policy.

we cant read other bucket.

choose created bucket in s3 service/resources --> myaws -33

manoj --> policy name (s3 +myaws33(bucket name) + read list)

service name -->s3

actions --> read, list

resources --> myaws -33

**ARN:-Amazon Resource Name**

manoj-> myaws-33(ARN)

arn:aws:s3(service name):(region):account no:myaws-33(resource name)

**ARN dived into 6 fields**

1. arn

2. partition --> aws , aws-cn(for china) ,aws-gov-us

3. service name --> iam,s3,ec2

4. region name --> iam global ,s3(it will be empty if it is global service)

5. account no -->

6. service resource type/ name -->

**Roles:-**

=======

==>with the help of role we can do communication between two aws resources.

aws service

Another aws account

\*give a particular user (user-1) ec2fullaccess permission

go to that user create an ec2 instance

launch instance

we need key select new pair of key

tick on i knowledge

key pair name and download it

select on particular machine

copy public ip address

go to mobaxtrem

go to session ->ssh-> in remote host enter public ip address and enter ec2 -user

add private key

sudo -i

aws -version

aws s3 ls(unable to locate credentials. you can configure creditiantals by running "aws config")

now click on roles create role

1.aws service 2.another aws account 3. web identity(fb id ,google id,amazon id) 3.SAML 2.0 federation

choose aws service->Ec2(have to create role for ec2 to access s3 service)

next permission->s3fullacess->purpose s3 service

role name(s3FAP)-> create role

now attach role-> go to machine on cansole->select that machine->

->go to action ->security->modify IAM role->chose IAM role->select your role(s3FAP)->save

refresh

go to xtreamobile

type comand aws s3 ls it will work.

=====================================================================================

**\*identiy provider**

xyz company --> on primises --> user id-->ldap service

\*account setting

change passwd policy

my security creditainls->MFA-multi factor authetication(additional security it provide)->like otp->

mfa device:-h/w aggents and s/w

active mfa->virtual mfa device->continue->