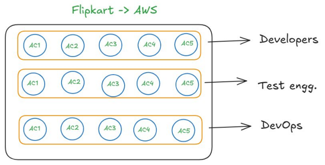
IAM

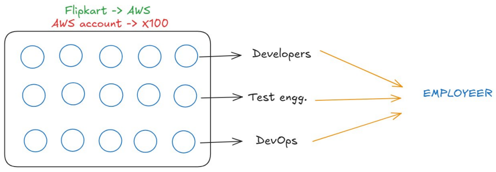
Identity & Access Management

Identity -> unique identifier



-> Each individual should have an account to login into AWS.
-> If each individual has it's own account:

- Difficult for the organization to manage the cost.
- There is no restriction to any services.
- Difficult to collaborate.

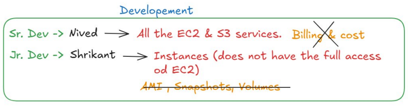


-> A single AWS account & providing access on this particular account.
-> This can be made possible with the help of a service called as 'IAM'.

-> With the help of IAM, we are creating multiple individuals & we called them as 'Identities'.
-> Providing those identities - permissions to access the services, based on their identities.

Features of IAM:

1. It is used to provide the access for an individual/an identity, for a specific service OR a part of the service.

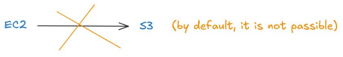

Developement

Sr. Dev -> Nived -> All the EC2 & S3 services. Billing & cost

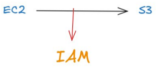
Jr. Dev -> Shrikant -> Instances (does not have the full access od EC2)

~~AMI , Snapshots, Volumes~~

2. It is used to provide access for one service to access another service.



(by default, it is not passible)



Components of IAM:

1. Users: Represents a person/application that accesses AWS services.

2. User Groups: Collection of AWS users.

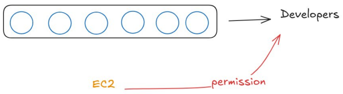
3. Roles: Temporary identity with specific permission given to a service.

4. Policies: A document of well-defined permissions

5. Identity Providers (IdPs): lets external AWS users log in into a particular AWS account.

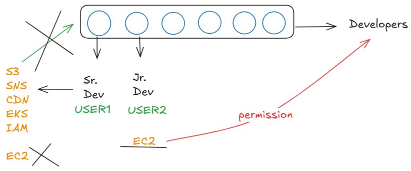
User Groups

-> used to divide the permissions based upon the identities.
-> helps organizer the users & manage the permissions collectively.
-> becomes easier to the manage the individuals.



-> The permission that is given to a group, that reflects upon all the identities.

-> Permissions can be given to a particular group & also certain permissions can be provided to a particular identity.



>> Explicitly denied policies/permissions overrules any other policy/permissions.

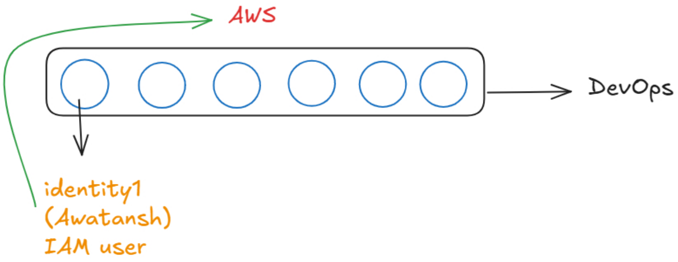
Steps to create User Groups:

1. Go to IAM Dashboard.
2. Left side panel -> 'User Groups', click on it.
3. Click on 'Create Group'.
4. Give a name to the group & scroll down to 'Attach permission policies'.
5. Search to the policy (AmazonEC2FullAcceess) & select it.
6. Click on 'Create User Group'.

what permissions
for accessing any
services.

User

-> Users are the individual identities who are going to access a specific account/services for which they have the permission.
-> They are the 'created users'
-> Created users in AWS are called as 'IAM users'.



Steps to create an User:

1. Go to IAM Dashboard.
2. Left side panel -> 'Users', click on it.
3. Click on 'Create Users'.
4. Give a username & select 'Provide user access to the AWS Management Console'.
5. In 'User type', select 'I want to create an IAM user'.
6. in 'Console Password', click on 'Password' & provide a password for the user.
7. Deselect 'Users must create a new password at next sign-in' & click on 'Next'.

-> Set permission for the user

- Add users to the group: permissions that is given to the group, that will reflect upon the identity/user.
- Copy permissions: particular permissions which are given to an already existing user, will be attached to the newly created user.
- Attach policies directly: directy giving the permission to a particular user.

8. In 'Permissions options', select 'Add users to the group'.
9. Find the group, select it & click on 'Next' & click on 'Create User'.
10. Download the .csv file and copy the console sign-in link.
11. Go Incognito and paste the user to sign-in.
12. Provide the username & password for sign-in.

Permissions/policies can be of 2 types:

i. Attach Policy: Policies which are pre-defined by AWS.
ii. Create inline Policy: Custom policies (we can define our own permissions & policies).