IAM Roles:
==========
1) By using roles we can give access of one account
resources to other account.
2) Roles can be assigned to EC2 instances,If EC2 instances
want to access to other aws services ,it requires
Access Key and Secreate Accesskey details.If we configure
these details in ec2 instance,we are compramissing our account
security, To avoid these type of things we will assign
roles to ec2 instance.

Creating EC2 Instances (Instance Profiles) Roles:
==========
Ex: Ubuntu Ec2 instance want to access s3 bucket,
Both are
in same account.
Prereq:
========
1) Launch Ubnuntu EC2 instance
2) Install AWS CLI

Note :No need to configure Access key.

Role Creation:
==========
1) Goto Iam Dash Board
2) Click on "Roles"
3) Click on "Create Role"
4) Select "EC2" Service Role
5) Click On "Next"
6) Add an existing policies(in this case s3full permissions)
7) Give any name to the role
8) Click on "Create Role"
'
Attaching role to Ec2 Instance
==========
1) Goto Ec2 Dash Board
2) Select the Instance
3) Goto "Action" --> "Instance Settings"-->
Attach/Replace Iam Role
4) Select an IAm role which we have created
5) Click On "Apply"
6) Login into EC2 instance and aws cli commands to
access s3 buckets.
ex : aws s3 ls

Creating Another Account Access roles:
==========
ex : Allow Account2 to Access Account1 Ec2/s3 resources.

Account1:

=========
1) Create an Another Account Role
2) Attach require policies to the Role

Account2:
=========
3) CReate a policy to consume Another Account Role
4) Attach Step3 policy to IAM user.

Nav Related to Account1:
========================
1) Goto IAM Dash Board
2) Click on "Roles"
3) Click on "Create Role"
4) Select "Another AWS Account"
5) Give Account number of Another Account (Account2)
6) Click On "Next"
6) Add an existing policies(in this case s3 & ec2 full permissions)
7) Give any name to the role
8) Click on "Create Role"

Nav Related to Account2:
========================
1) Goto Iam DashBoard
2) Click "Policies"
3) Click on "Create Policy"
4) Click ON JSON tab
5) Copy Paste below things

```
  {
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": "sts:AssumeRole",
         "Resource": "arn:aws:iam::521937342151:role/testrole_oct30"
      }
   ]
}
```

Note : Change the account number and role name ARN format
    as per your requirement.

6) Click on "Review"
7) Give any name to the Policy
8) Click on "Create Policy"
9) Assign this policy any IAM user.
10) Login into IAM user
   a)Swith to Another to Role
  i) Click (^) IAm user from aws service Dash board
  ii) Click Switch Role
  iii) Give Account number of Account1
  iv) Give Role name of the Acccount1

v) Switch Role.

Note : To Access Another AWS account Resources we will "STS"(Secure Token Service)