1.Identity and Access Management (IAM) is a service offered by Amazon to control the users, create groups and allow or deny access to specific resources within the AWS environment.

2. Policies are like permission for services offered to the user. If anyone wants to access any service they need to have permission to use that particular service. In the same way in AWS we will attach resources permissions to the either USERS, ROLE or GROUPS to access any service.

3.let’s consider there is team of dev and testers so dev needs a set of service and testers need a separate set of services to access. Here we can create a group and attach policies which are needed to that group so by this way they can access services.

4.It is not recommended to use root account because it can give full access to all the AWS services .If data is stolen then there may be a chance of misusing the data.

5.In users there will be two ways to attach policy one is by using Groups another is by attaching inline policy so to remove any policy we can select user->permissions and there we can revoke policy.

6.Yes a User can be a part of policies via groups let's suppose there are two groups red and blue then a user can be a part of both groups so that they can be having multiple policies. In case of root it can access all the resources without any limitations