1. **What is the need of IAM?**
    a. IAM which is identity access management service which is provided by AWS to manage the resources in the AWS cloud.
    b. It can be used to give and limit the access of users in the AWS cloud.
    c. IAM helps the organization to keep them secure provides greater control of user access to your system
    d. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources
    e. With AWS Identity and Access Management (IAM), you can specify who or what can access services and resources in AWS.
    f. Without IAM it is difficult to manage the AWS resources access.

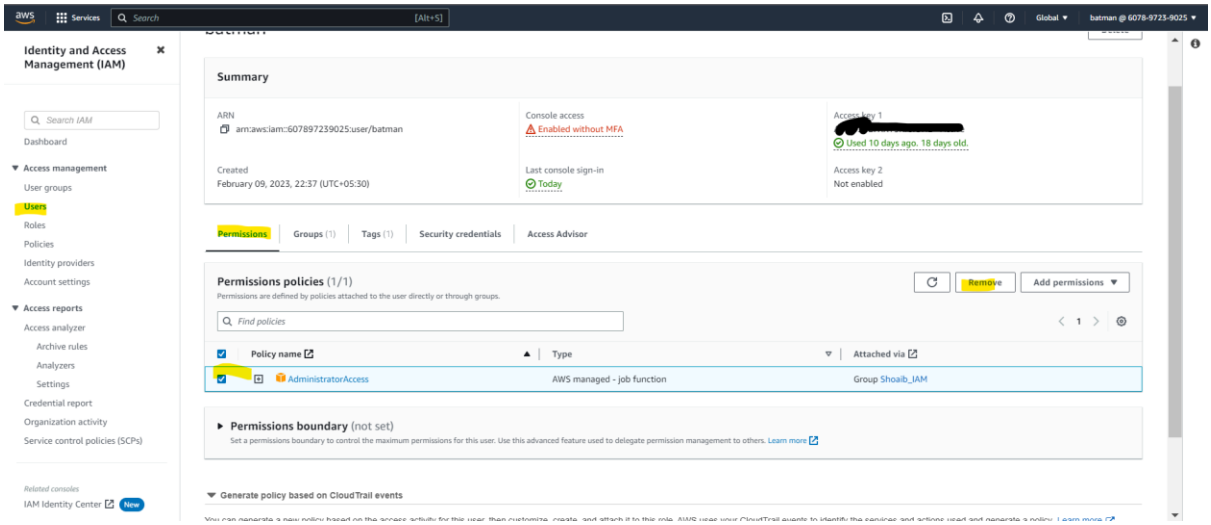
2. **If I am a non tech person, how will you define policies in IAM?**
    a. Policies are use to define what kind of action or access a user can have for a particular role they have.
    b. Policies are use to define whether the request is allowed or not.
    c. Just to explain you in simple terms if you are a manager so you have assigned a policy where you can access the employees details but as an employees you cant access other employees details because you have not given the set of access which is required.
    d. In AWS if we define a policy that a user can read the number of EC2 instance in particular region then that user can only read the EC2 instance details but it cannot create it.

3. **Please define a scenario in which you would like to create your own IAM policy?**
    a. Allows starting or stopping Amazon EC2 instances when the resource and principal tags match
    b. Allows enabling and disabling AWS Regions.

4. **Why do we prefer not using root account?**
    a. Because they allow full access to all your resources for all AWS services.

b. Using the AWS root account means that there is potential for its compromise
c. If someone get access to the root user then they can destroy and manage all the AWS resources so it is not a good practices to use root user for everyday task instead use IAM for that.

5. How to revoke policy for an IAM user?



a. Login to AWS console. Go to IAM
b. Click on user
c. Select the permission then select the policy
d. Then select the action. Like to remove the policy please sleect REMOVE

6. Can a single IAM user be a part of multiple policy via group and root? How?

a. Yes, we can add a single user into the multiple policy via group
b. A user group can contain many users, and a user can belong to multiple user groups
c. User groups can't be nested; they can contain only users, not other user groups
d. Create two group A and B then create a user X then add the user in both the group which have different policies set.