1. What is the need of IAM?

Identity and Access management (IAM) is used as authorization tool on AWS. We can create different users with specific permissions so as to prevent unauthorized access or misuse of resources in AWS which could generate unwanted bills.

1. If I am a non tech person, how will you define policies in IAM?

Think of IAM as a country and policies as its constitution. In order to live in a country we need to follow its constitution, rules & regulations. Similarly, we have to follow policies in IAM to use tools & resources in AWS.

1. Please define a scenario in which you would like to create your own IAM policy.
2. Why do we prefer not using root account?

Root account has all the permissions by default, and using it could be risky as one wrong step and we may end up losing everything. It is always recommended to use user account because even if we lose our user account, we can always create a new user and start again.

5. How to revoke policy for an IAM user?

To revoke policy for an IAM user, steps are given below:-

* Login as IAM user whose policy you want to revoke.
* Go to IAM console
* Select users option in left side of the page
* Click on permissions tab
* Search for the policy you want to revoke
* Click the cross (x) button against the policy you want to revoke.
* A popup will appear, select “detach”.

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

Yes. One can create different groups in IAM as per the requirement of the task.

And can always add a particular user into multiple groups.