1. What is the need of IAM?

Identity and access management, or IAM, is the security discipline that makes it possible for the right entities (people or things) to use the right resources (applications or data) when they need to, without interference, using the devices they want to use.

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

You an check out the details and various types of policies which is well explained on AWS website on policies and permissions column.

1. Please define a scenario in which you would like to create your on own IAM policy?

To create a new policy we can checkout the website AWS policy generator where we can create our new policy according to our convenience. Atlast after creating the policy, we can generate the policy and activate it using JSON .

1. Why do we prefer not using root account?

The primary reasons are thus: Every hacker / virus knows that there is a root account. If they are blindly attacking a system, it's a known entry point, and very likely to be a target. This is why your root account should have logins disabled.

1. How to revoke policy for an IAM user?

Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/ . In the navigation pane, choose Roles, and then choose the name (not the check box) of the role whose permissions you want to revoke. On the Summary page for the selected role, choose the Revoke sessions tab.

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

An IAM user group is a collection of IAM users. You can use user groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users. For example, you could have a user group called Admins and give that user group the types of permissions that administrators typically need. Any user in that user group automatically has the permissions that are assigned to the user group. If a new user joins your organization and should have administrator privileges, you can assign the appropriate permissions by adding the user to that user group. Similarly, if a person changes jobs in your organization, instead of editing that user's permissions, you can remove him or her from the old user groups and add him or her to the appropriate new user groups. A user group cannot be identified as a Principal in a resource-based policy. A user group is a way to attach policies to multiple users at one time. When you attach an identity-based policy to a user group, all of the users in the user group receive the permissions from the user group.