1. What is the need of IAM?

IAM in AWS is used to define a set of permission for a user.  
For example a tester doesn’t needs the access for billings In AWS for the resources, so to restrict that user from accessing, we can give the permissions which is only required for him.

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

Consider an example where there is a shop owner and 3 employees each employee has their own role the shop owner collects cash and has the key to his shop. Out of other 3 employee one is working as a janitor, other as watchman and another one as salesman. Now a janitor doesn’t have the access to the items which sales person shows to the customer. The salesperson will not have the access to shop key as it is managed by the owner. Similarly, in IAM root has the full access and other IAM role have their own set of policies defined.

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

I would like to create when there are multiple teams in an organization exists. For example, developer team is one group in that IAM users with group policies and individual policies. Similarly testing team, operation team, finance team etc.

1. Why do we prefer not using root account?

Because it has all access to every resource in the AWS and by mistake if we delete a resource which is valuable to the company it would incur a huge loss, and root account cannot be shared to everyone in an organization which posts security threat to company. So its advised to not use root account.

1. How to revoke policy for an IAM user?

Login to root user and then under IAM select the user whose access needs to be restricted and then select the IAM policies which are not required and remove it.

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

Yes a single user can be part of multiple group then he would be part of policies defined for those multiple group and also his own individual policies.