1. **Why is IAM important?**

With a rise in security threats and user privacy preferences turning harder to handle, IAM has begun to play an important role for organizations, regardless of the business and size. The IAM is vital at a time when passwords are hacked within seconds, data breaches become common, and intruders infiltrate government and organizational organizations.

2. **Define identity directory service?**
   Most IAM projects involve working with active directories and other types of repositories that comply with the Light Directory Access Protocol (LDAP). Therefore, LDAP skills are needed throughout the project for repository consolidation, QA testing, data conversion, and other tasks.

3. **What is the method for giving a user access to an Active Directory server? And how to disable a person in the Active Directory?**

To give a user access, first, browse the server in the current directory and find the affected access groups in the server properties. Then add the user to the preferred group that provides access to the particular service. On the other hand, to disable someone, search for the user in the organizational unit (OR) and right-click, choose Disable Account.

4. **What IAM solutions and tools do you choose to work with?**

   As a result, IAM may be a unique product or a combination of hardware, cloud services, software and processes that provide administrators with visibility and regulation of the organization's data. So, if you have already used IAM tools and solutions, state them in detail.

5. How have you experienced identity directory services such as Active Directory?

Most IAM projects involve working with Active Directory or other kinds of LDAP-compliant repositories. According to a blog published by Avatier, LDAP skills are required throughout an IAM project for data conversions, QA tests, repository consolidation, and other tasks. “Being able to put in writing scripts that push and pull information between databases and also the target LDAP directory provides a good deal of power that may be leveraged to accelerate project work,” the Avatier weblog states.

6. **What is the IAM service within AWS Cloud?**

IAM stands for Identity Access Management. This is an AWS Cloud service that allows you to create user accounts and groups and securely manage their access to AWS services and resources. IAM is a global service and there are no extra charges.

7. **Explain the various types of user accounts within AWS Cloud?**

   Root User is the owner account (administrator) and is created when an AWS account is created. It has complete default access to all services and resources within the AWS account. This user may not be explicitly refused access to AWS resources or services with IAM policies. In order to limit permissions to this user account, this should be done using the AWS organization's Service Control Policy (SCP). Specific tasks such as shutting down an AWS account may only be performed by the primary user of the AWS account.

   IAM User is a standard user account with no authorization for any AWS service or resource. This account is set up by a root user or IAM administrator. IAM policies are used to set permission for this user account. All the users, that need to login into AWS Management Console, put together services, or access resources programmatically, will have their individual IAM user account with a completely different set of policies associated with them. Certain tasks such as shutting down an AWS account cannot be performed by that user account.

8. **What is the identity-based policy within AWS IAM?**

The identity-based policy is the most commonly used JSON permissions policy document. It is used to control the actions of identity (individual user, user group or role) that may perform on an AWS asset under certain circumstances.

9.What kinds of identity-based policies are available on AWS IAM?

There are two types of identity-based policies that are managed and/or integrated: Managed Policy: This is simply a policy that you may apply to an individual IAM user, a user group, or a role in the AWS account.

Inline Policy: These policies focus on a specific identity, e.g. user, group or role. These policies are deleted as the related ID is deleted. These policies have a strict, individual relationship with the associated identity and cannot be associated with a different identity.

10.Are the root and IAM users similar?

No, the root user is also known as the master user. The IAM user is a subset to the root user.