IAM Assignment

1. What is IAM?
2. IAM refers to a framework or policy and technologies for ensuring that the proper people in an organization have the appropriate access to technology resources.
3. Why is IAM important?
4. With an increase in security threats and user privacy preferences turning more difficult to handle. IAM has started to play a crucial role for organizations, irrespective of the industry and size.
5. Default limitation for IAM?
6. IAM user limit is 5000 per AWS account. You can add up to 10 users at one time.
7. You are also limited to 300 groups per AWS account.
8. You are limited to 1000 IAM roles under AWS account.
9. IAM user can be a member of 10 groups (max).
10. Which capabilities provide AWS IAM?

Ans) AWS IAM provides

1. Access control to AWS resource
2. Multi factor authentication
3. Federated access
4. Analytics
5. Shared access
6. Free of cost
7. Grant permission to the user
8. What is federated access?

Ans) In federated access IAM provides the capability to grant access for AWS resources to existing employees of a company using the existing identity system.

1. What are different identities provided by IAM?

Ans) AWS providers three different identities users, user groups and roles to manage access to AWS resources.

1. What is AWS account root user?

Ans) The root user is the user id and password used to first create the aws account. Root user has complete access to all the aws services and resources in the account. After creating the aws account it is recommended to create a separate admin user to manage admin and everyday tasks instead of using the root user.

1. What are the best practices to manage access to aws resources?

Ans) The following are the some of the best practices to manage access to AWS

* Do not use root account
* Use groups
* Enable multi factor authentication
* Grant least privileges

1. What are AWS policies?

Ans) policies are objects in AWS that are associated with an entity. Policies are stored in AWS as JSON objects. AWS supports six types of policies

* Identity based policies
* Resources based
* Permissions boundaries
* Organizations SCPs
* ACLs
* Session policies

1. What is an IAM role?

Ans) IAM role is an entity that defines a set of permissions for making AWS services request they are not associated by a specific user.

We cannot assign the IAM role to users or groups.

1. How to remove an AWS customer IAM policy?

Ans) we cannot rename an IAM policy but we can copy, create or delete an IAM policy.

1. Are root users and IAM users are the same?

Ans) No, root user is also called master user. The IAM user is a subset of the root user.

1. In the IAM service, can we monitor the IAM user activity?

Ans) yes, you can monitor the activities of IAM users, if any violation you can remove access for the user.

1. How to control authorization in AWS IAM?

Ans) You can control authorization by creating policies.

1. What is the other name of IAM user?

Ans) IAM is also known as IAM entity.