NAME: BANDE PRIYATHAM NAGA AASHISH

Assignment Interview question

Note:-Please prepare the answer of these questions in brief :- (in your own words)

1. **What is the need of IAM?**

Ans:

Identity and Access Management (IAM) is a security practice that involves managing access to resources in a system. It helps to ensure that only authorized users have access to resources, and that they have only the permissions they need to perform their assigned tasks.

There are several reasons why IAM is important:

Security: IAM helps to protect sensitive resources and prevent unauthorized access, which can reduce the risk of data breaches and other security incidents.

Compliance: Many industries and organizations have regulations that require proper access controls to be in place. IAM can help organizations meet these requirements and avoid fines and other penalties.

Productivity: By providing users with only the permissions they need to do their jobs, IAM can help to improve productivity by eliminating the need for users to request access to resources they don't need.

Cost Savings: Properly implemented IAM can help organizations reduce the cost of managing user access to resources by automating processes and reducing the need for manual intervention.

Overall, IAM is an important practice that helps organizations to secure their resources, meet compliance requirements, improve productivity, and reduce costs.

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

Ans:

An IAM policy is a set of rules that defines what actions a user or group of users can take on specific resources.

For example, a policy might allow a user to read and write files in a specific folder, but not delete them. Another policy might allow a group of users to create and delete Amazon S3 objects, but not modify them.

Policies can be created at the user or group level, or they can be applied to resources directly. They can be created using simple statements that define the allowed actions, resources, and conditions under which those actions can be performed.

As a non-technical person, it may be helpful to think of IAM policies as a set of rules that dictate who can do what with specific resources in your organization. By creating and applying these policies, you can ensure that only authorized users have access to the resources they need to do their jobs, and that they can only perform the actions that are necessary for their roles.

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

Ans:

Here is a scenario in which you might create your own IAM policy:

Imagine that you are the administrator of an AWS account, and you have just created a new S3 bucket that will be used to store sensitive financial data. You want to ensure that only a specific group of users in your organization have access to this data, and that they can only read and write files, but not delete them.

To accomplish this, you could create an IAM policy that allows the group of users in question to perform the necessary actions on the S3 bucket. The policy might look something like this:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject", "s3:PutObject"],
      "Resource": "arn:aws:s3:::my-sensitive-data-bucket/*",
      "Condition": {
        "StringNotLike": {
          "s3:x-amz-delete-marker": "true"
        }
      }
    }
  ]
}
```

This policy allows the specified group of users to perform the GetObject and PutObject actions on objects in the my-sensitive-data-bucket, but it denies the DeleteObject action. The Condition block further limits the allowed actions by denying requests that include a delete marker, which effectively prevents the users from deleting objects.

By creating this policy and attaching it to the group of users, you can ensure that only the authorized users have access to the sensitive data in the S3 bucket, and that they can only perform the necessary actions on the data.

4. Why do we prefer not using root account?

Ans: The root account is the primary account in an AWS account and has full administrative privileges. It has the ability to perform any action and access any resource in the account, and is not subject to any IAM policies or service quotas.

While the root account is powerful and convenient, it is generally not recommended to use it for everyday tasks. This is because:

Security: The root account has unlimited access to all resources and can make changes to the account that could compromise security. If the root account's credentials are compromised, an attacker could potentially gain full control of the account.

Auditability: The root account's actions are not logged by AWS CloudTrail, which makes it more difficult to track and audit changes made to the account.

Best Practices: AWS recommends using IAM to manage access to resources and enforce least privilege. By using IAM, you can create separate users and groups with specific permissions, which makes it easier to manage access to resources and track changes made by different users.

Overall, it is generally best practice to use the root account only to create the initial users and groups in the account, and then use those users and groups to perform everyday tasks. This helps to improve security, auditability, and compliance in your AWS account.

5. **How to revoke policy for an IAM user?**

   Ans:

   To revoke a policy for an IAM user, you can follow these steps:

   Sign in to the AWS Management Console and open the IAM dashboard.

   In the left-hand navigation menu, click on the "Users" link.

   On the Users page, find the user whose policy you want to revoke, and click on their name to open their details page.

   On the user's details page, click on the "Permissions" tab.

   Under the "Permissions" tab, you will see a list of all the policies that are attached to the user. To revoke a policy, click on the checkbox next to the policy, and then click on the "Detach Policy" button.

   In the confirmation dialog that appears, click on the "Detach" button to confirm the action.

This will revoke the selected policy from the user, and they will no longer have the permissions granted by that policy. You can repeat this process to revoke additional policies from the user, if necessary.

It's important to note that revoking a policy from a user does not delete the policy itself, it just removes the association between the policy and the user. The policy will continue to exist and can be re-attached to other users or resources as needed.

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

Ans:

Yes, a single IAM user can be a part of multiple policies via groups and the root account. This can be done in the following ways:

Group membership: An IAM user can be a member of one or more IAM groups, and each group can have its own set of policies attached to it. When a user is a member of a group, they inherit the permissions granted by the group's policies.

Direct policy attachments: In addition to group membership, an IAM user can also have policies attached directly to their user account. These policies are in addition to any policies they inherit from group membership, and they take precedence over group policies.

Root account permissions: Finally, an IAM user can also have permissions granted by the root account. The root account has full administrative privileges and can grant any permissions to any users or resources in the account.

Overall, an IAM user can have multiple policies applied to their account through group membership, direct policy attachments, and root account permissions. These policies are combined and evaluated together to determine the user's effective permissions.