4. Identity and Access Management (IAM)

IAM is a service that helps to gain control over user identifications based on the Accessing of services privileged to an authorized user in an environment or system.

IAM service is used to deal with Authorized as well as non-Authorized users which can or cannot use privileged IT resources or Services.

The main function of the IAM is to prevent access of the It services or resources to Unauthorized users.

The 4 main components of Identify and Access Management (IAM) are:

1. Authentication.
2. Authorization.
3. User Management.
4. Credentials management.

This can be remembered as AAUM.

Authentication:

- It checks whether the user is authenticated or not.

- Checks whether the user has a valid username password or essential credential modes or not.

- The most used Authentication is the username and password combination.

- These credential modes also include Digital Signature, iris Scanner, fingerprint lock, and digital certificates.

Authorization:

- It is the Access control protocol.

- It checks whether the authenticated user has access to the particular service or IT resource which is being used.

User Management:

- Creating new users.

- Create a record.

- Adding user to the required access group.

- maintaining password policies.

- Maintaining privileges.

Credential management:

- Establishes identities and access controls.

- Checks the credentials entered by the user to access the resources.

Pt2:

Root account:

- The account which is created by the user using a credit card or debit card is called the root account.

- The root account has access to all the resources you need (All AWS resources are paid).

- In the root accounts, numerous AWS branch accounts can be created.

- Branch account does not have access to all the services, it is guided by the root user.

- Each branch account can have its own sets of Services according to the need.

- For example, if an employee is given the EC2 instance to work on, only EC2 service can be accessed via branch user.

- They do not have the authority to use the services which are not assigned.

- Only the Root user (the one who created this account) is allowed to append,

according to the needs.

- The root user can also delete the account if he wants to.

- Do not use the root account for administrative purpose, instead create one branch account which has more access than the other branch accounts.

- Either way, the root user will have more control and would have more superiority over the branch nodes.

Limitation to AWS IAM service:

1. IAM user limit is 5000 branch users per AWS Account. You can add up to 10 users at a time:

- The limit of branch users we can create is 5000.

- These are the users which will work on the AWS branch account under the Root user.

- There are other possible users assigned which are meant for read-only access. They are not considered among the 5000 branch users.

- you cannot dynamically assign a required numbers of branch users above 10.

- Only up to 10 of Branch Users can be assigned by the root user.

1. You are limited to 300 groups per AWS account:

- Each root user can create up to 300 groups. For example, HR group, Admin group, Banking group, networking group, etc.

- The number of Branch users can be allocated according to the requirement of the group; but cannot exceed more than the maximum number of Branch roots i.e. 5000.

1. You are limited to 1000 IAM roles per AWS account:

- In a Group, up to 1000 IAM roles can be assigned to the branch users.

- There are some default roles that are provided by the IAM, but some roles can be manually assigned to the branch user.

- For example: some roles may include software developer, database administrator, software tester, network administrator, etc. up to 100 roles.

1. Default limits to the managed policies attached to an IAM role and IAM user is 10:

- Policies are the rules associated to a particular role or a particular user.

- These rules are assigned to the user based via IAM based on the decision of the root User.

1. IAM user can be a member of 10 groups:

- One user under IAM can be simultaneously present in N number of groups if required, which can be assigned by default by the Root user.

1. We can assign 2 access keys max to the IAM User:

- Generally, 1 access key is assigned to the IAM user.

- But 2 can also be set if allowed by the Root User.

Situation:

- A company has a large amount of data which shouldn’t be accessed by the

Employees.

- If a Company named XYZ needs some employees for Cloud, and one of the

user wants to access database, he cannot since the particular service is not

activated by the root user to the employee.

- IAM can block the branch accounts as well since we no longer need that service.

- The IAM is the God of all other accounts.

- It can manage all the branch accounts based on their usage.

Features offered by IAM are:

1. Shared Access to your AWS account:

- We can share the AWS account to numerous users at a time.

- By that, we don’t have to give the credentials, but just grant a permission to the requesting account to access the features.

- These accounts do not necessarily mean accessing the features.

- For security purposes, the granting access can be also be for READ ONLY purpose.

2. Granular Permission:

- Granular means according to need and purpose oriented.

- Granular Permissions are the permissions which are based on the level of the user who is accessing the account.

- You can grant different permission to different users for different resources by the implementation of IAM.

- The various levels of permission are:

1. Read Only.

2. Read and Write.

3. Admin.

- For example: The read only permission can be given to the employee of the company, whereas, the admin permission can be given to the higher authority of the company.

- For some S3 resources can be accessible but form some Read Only is granted.

1. Secure access to AWS resources for Applications that run on Amazon EC2:

- Accessing the applications that run on the Virtual Environment by the service EC2 can also be done via IAM.

- The level of security will be provided to the EC2 instance as well as the applications that that are present in the EC2 if the access is granted.

- Various Accessing Protocols such as Read only, Read and Write, Admin, can be given via IAM to the EC2 instance.

- For example, in some cases the IAM can secure the EC2 instance only.

- And it can also protect the data in the DynamoDB and S3 service if the permission is not granted.

1. Multifactor Authentication:

- Analogy: When we have to sync the info of our personal account into another device, we have a special feature of authorization to sync the data from one to another.

- For Example: We use OTP process for syncing the Google accounts, where YES or NO selection in the main device can also be used.

- Example 2: For syncing the whatsapp account on desktop, we use the QR scanner from the main device and QR pattern on the Desktop.

- It is the 2nd step of authentication after username and password combination.

- It can be the OTP or a QR scannable code which will retrieve our data into the other device.

- Similarly, in the IAM, a code is required for the final authentication process.

- This code is sent to the root account, in which the account receives a code which should be added to the further Authentication purpose.

- This code is available for a limited amount of time, and then refreshes once the time expires.

- By default, MFA (multi-factor authentication) is not enabled. You can enable and manage MFA devices for the AWS account root user by going to the Security Credentials page or the IAM dashboard in the AWS Management Console.

1. Identify Federation:

- Example: We use Sign-in using Google or Sign-in via Facebook when registering on a website for the first time.

- Analogy: When we are using a website or an application where we have to register for a site individually, there is an option where we can directly fill the detail via giving specific permissions from the third-party authenticator.

This third-party application can be trusted by various websites and applications.

- Similarly, there is an option for the AWS account authentication where we can fill the data by a trusted source.

- You can allow the users to authenticate via other resources in which the authentication is already done.

They authenticate us as a recognized user.

1. Identity information for Assurance:

- Example: When we open THIS PC on the desktop, we can see the recent activities, like the files and docs which are accessed by the user.

- We can check the activities performed on the AWS user account with the use of IAM.

- It grants the info of the accessors that have been using the account.

- This displays the Data in form of Logs where which user has requested access to which resource, is displayed and saved for later purposes.

1. PCI-DSS Compliance:

- Example: When we add a card in Amazon Account, that card is saved and can be used later for future transactions. Next time when the card is being used, this process only needs CVV and OTP from mobile to prepay for the delivery.

- IAM supports the processing, storage and transmission of Credit Card that is used by the merchant or the user.

- This process is validated by the Payment Card Industries (PCI) and Data Security Standard (DSS).

1. Eventually Consistent:

- Is consistent in changing the data fast that needs to be changed when the load is low and is not critically needed for some functions.

- IAM includes high availability by replicating data and forwarding it to the various regional zones.

- It is Consistent in changing, replicating and saving the data.

1. Free of cost:

- Is provided free of cost to the users who have an access to the AWS services.

- If any user creates a service inside the IAM, the created service is charged but not the IAM.