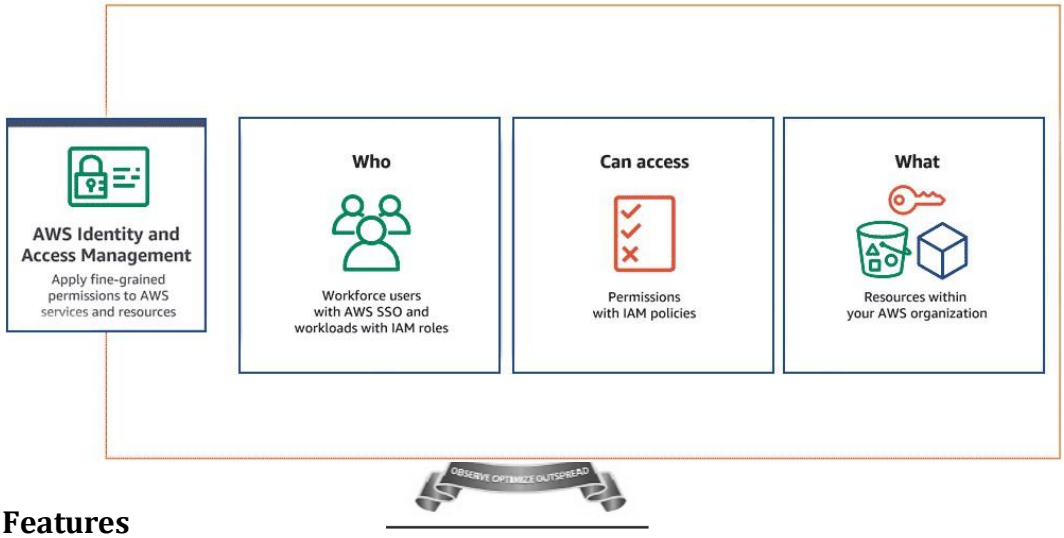
5.5. IDENTITY AND ACCESS MANAGEMENT

Identity and Access Management (IAM) is a combination of policies and technologies that allows organizations to identify users and provide the right form of access as and when required. There has been a burst in the market with new applications, and the requirement for an organization to use these applications has increased drastically. The services and resources you want to access can be specified in IAM. IAM doesn't provide any replica or backup. IAM can be used for many purposes such as, if one want's to control access of individual and group access for your AWS resources. With IAM policies, managing permissions to your workforce and systems to ensure least-privilege permissions becomes easier. The AWS IAM is a global service.



IAM Features

Shared Access to your Account: A team working on a project can easily share resources with the help of the shared access feature.

1. Free of cost: IAM feature of the AWS account is free to use & charges are added only when you access other Amazon web services using IAM users.

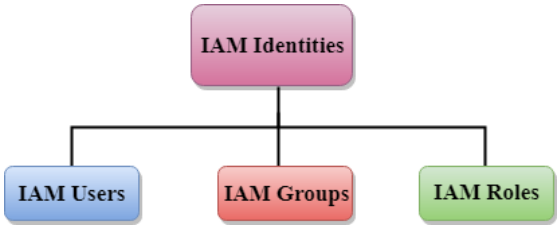
2. Have Centralized control over your AWS account: Any new creation of users, groups, or any form of cancellation that takes place in the AWS account is controlled by you, and you have control over what & how data can be accessed by the user.

3. Grant permission to the user: As the root account holds administrative rights, the user will be granted permission to access certain services by IAM.

4. Multifactor Authentication: Additional layer of security is implemented on your account by a third party, a six-digit number that you have to put along with your password when you log into your accounts.

IAM Identities

IAM identities are created to provide authentication for people and processes in your AWS account. IAM identities are categorized as given below:



IAM User

An IAM User is an entity created in AWS that provides a way to interact with AWS resources. The main purpose of IAM Users is that they can sign in to the AWS Management Console and can make requests to the AWS services. The newly created IAM users have no password and no access key. If a user wants to use the AWS resources using the AWS Management Console, you need to create the user password. If a user wants to interact using the AWS programmatically (using the CLI (Command Line Interface)), you need to create the access key for that user. The credentials created for IAM User are what exactly uniquely identify themselves to AWS.

IAM Groups

An IAM Group is a collection of users. Group specifies the permission for a collection of users, and it also makes it possible to manage the permissions easily for those users. You created a group known as Admin and assigned the permissions to the group that administrators typically need. Any user joins the admin group; then the user will have all the permissions that are assigned to the group. If a new user joins the organization, then he should have administrator privileges, and you can assign the appropriate permissions by adding him to the group. If a person changes his job profile, instead of editing his permissions, you can remove him from a group and add him to the group.

Characteristics of IAM Group

- A group is a collection of users, and a user can also belong to multiple groups.
- Groups cannot be nested, i.e., a group cannot contain another group.
- No default group that automatically includes all the users in AWS account. If you want a group like this, create a group and then add the users in a group.
- There is a limit to the number of groups that you can have and also have a limit to the number of groups that a user can belong to.

IAM Roles

A role is a set of permissions that grant access to actions and resources in AWS. These permissions are attached to the role, not to an IAM User or a group. An IAM User can use a role in the same AWS account or a different account. An IAM User is similar to an IAM User; role is also an AWS identity with permission policies that determine what the identity can and cannot do in AWS. A role is not uniquely associated with a single person; it can be used by anyone who needs it. A role does not have long term security credential, i.e., password or security key. Instead, if the user uses a role, temporarily security credentials are created and provided to the user. You can use the roles to delegate access to users, applications or services that generally do not have access to your AWS resources**.**

AWS Account Root User

When you first create an AWS account, you create an account as a root user identity which is used to sign in to AWS. You can sign to the AWS Management Console by entering your email address and password. The combination of email address and password is known as root user credentials. When you sign in to AWS account as a root user, you have unrestricted access to all the resources in AWS account. The Root user can also access the billing information as well as can change the password also.

IAM Policies

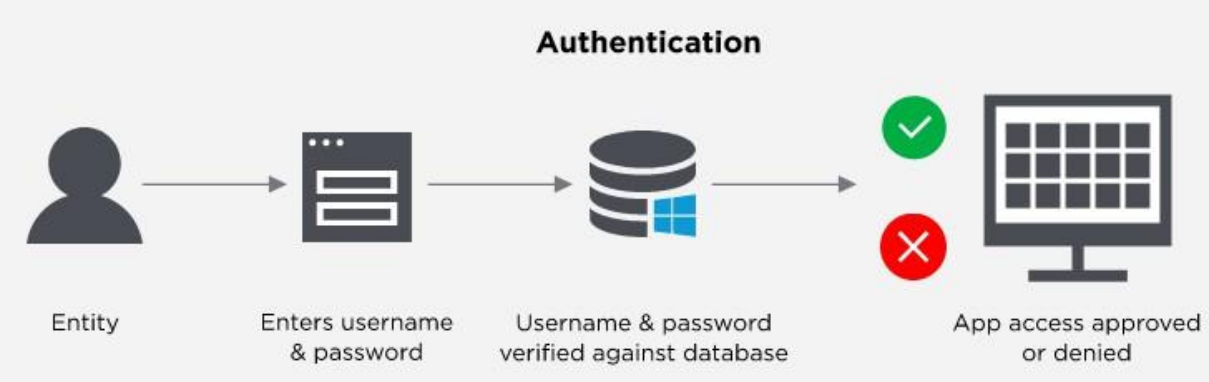
IAM Policies can manage access for AWS by attaching them to the IAM Identities or resources IAM policies defines permissions of AWS identities and AWS resources when a user or any resource makes a request to AWS will validate these policies and confirms whether the request to be allowed or to be denied. AWS policies are stored in the form of Jason format the number of policies to be attached to particular IAM identities depends upon Number of permissions required for one IAM identity. IAM identity can have multiple policies attached to them.

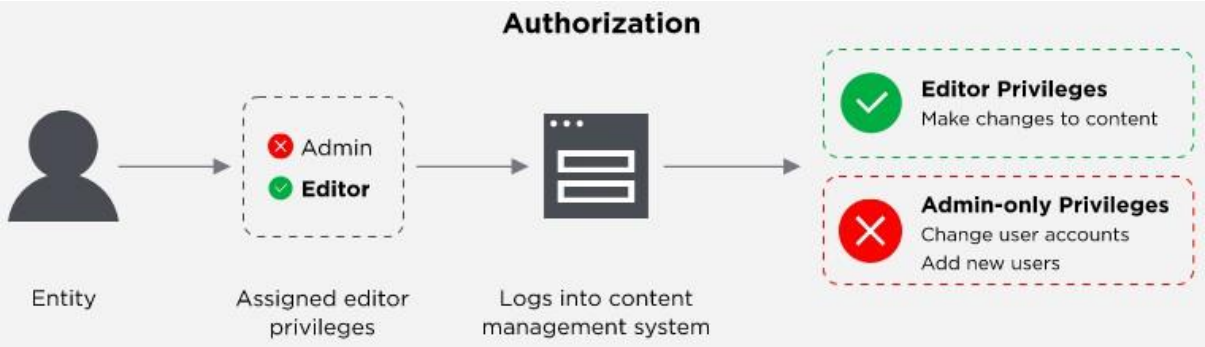
How Does IAM Work?

Identity management solutions generally perform two tasks:

1. IAM confirms that the user, software, or hardware is who they say they are by authenticating their credentials against a database. IAM cloud identity tools are more secure and flexible than traditional username and password solutions.
2. Identity access management systems grant only the appropriate level of access. Instead of a username and password allowing access to an entire

Software suite, IAM allows for narrow slice so faces to be portioned out, i.e. editor, viewer, and commenter in a content management system.





Difference between Identity Management and Access Management?

Identity management confirms that you are you and stores information about you. An identity management database holds information about your identity - for example, your job title and your direct reports - and authenticates that you are, indeed, the person described in the database.

Access management uses the information about your identity to determine which software suites you're allowed access to and what you're allowed to do when you access them. For example, access management will ensure that every manager with direct reports has access to an app for timesheet approval, but not so much access that they can approve their own timesheets.

IAM Technologies

An IAM system is expected to be able to integrate with many different systems. Because of this, there are certain standards or technologies that all IAM systems are expected to support: Security Access Markup Language, OpenID Connect, and System for Cross-domain Identity Management.

Security Access Markup Language (SAML)

SAML is an open standard used to exchange authentication and authorization information between an identity provider system such as an IAM and a service or application. This is the most commonly used method for an IAM to provide a user with the ability to log in to an application that has been integrated with the IAM platform.

OpenID Connect (OIDC)

OIDC is a newer open standard that also enables users to log in to their application from an identity provider. It is very similar to SAML, but is built on the OAuth 2.0 standards and uses JSON to transmit the data instead of XML which is what SAML uses.

System for Cross-domain Identity Management (SCIM)

SCIM is standard used to automatically exchange identity information between two systems. Though both SAML and OIDC can pass identity information to an application during the authentication process, SCIM is used to keep the user information up to date whenever new users are assigned to the service or application, user data is updated, or users are deleted. SCIM is a key component of user provisioning in the IAM space.