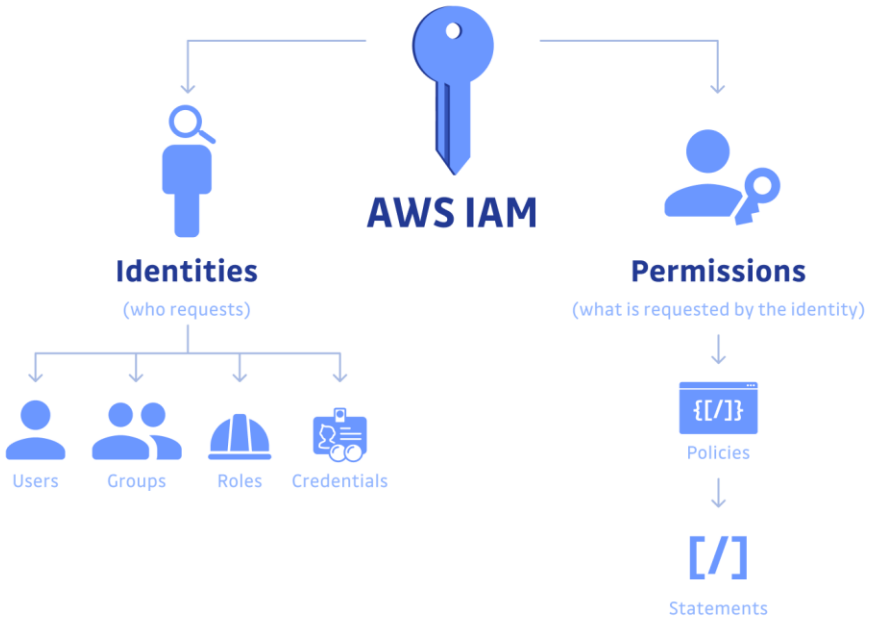
AWS Identity And Access Management (IAM)

AWS IAM is the heart of AWS security because it empowers you to control access by creating users and groups, assigning specific permissions and policies to specific users, Managing Root Access Keys, setting up MFA Multi-Factor authentication, for additional security, and so much more. And the cherry on top, **IAM is free to use**!

AWS Identity And Access Management

- IAM is preventative security control.
- It can create and manage AWS users and groups and use permissions to allow and deny access to AWS resources
- IAM deals with 4 terms such as users, groups, Roles, and Policies.
- It controls both centralized and fine grained-API resources plus a management console.
- You can specify permissions to control which operations a user or role can perform on AWS resources
- IAM service provides access to the AWS Management Console, AWS API, and AWS Command-Line Interface (CLI)

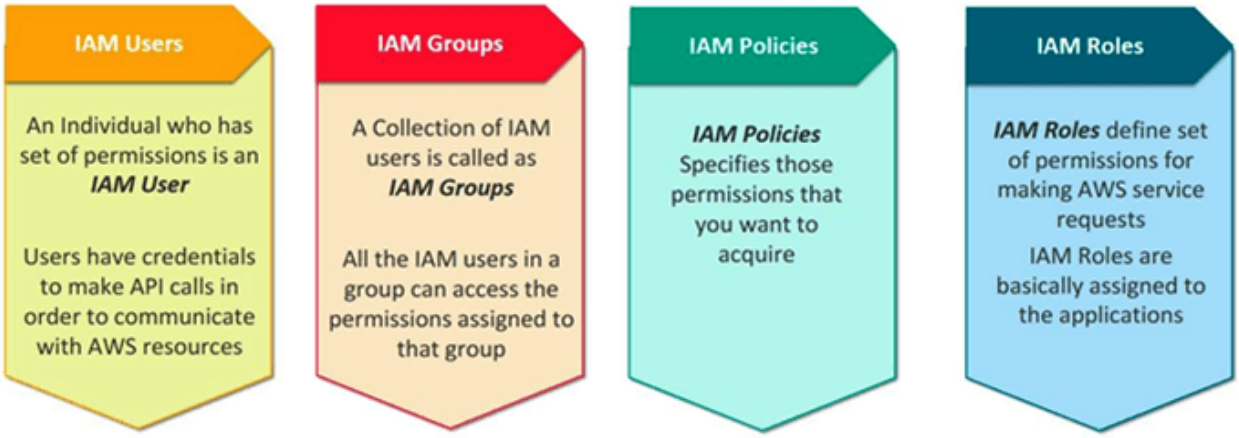


AWS IAM—Key Features

We should consider IAM as the initial move towards making sure about all your AWS administrations and assets.

1) Confirmation: AWS IAM allows you to make and oversee characters, for example, clients, gatherings, and jobs, which means you can issue and empower verification for assets, individuals, administrations, and applications inside your AWS account.
2) Approval: Access to the executives or approval in IAM is made of two essential segments: Policies and Permissions.
3) Fine-grained consents: Consider this—you need to give the business group in your association admittance to charging data, yet in addition need to permit the engineering group full admittance to the EC2 administration, and the promoting group admittance to choose S3 pails. Utilizing IAM, you can design and tune these consents according to the necessities of your clients.
4) Common admittance to AWS accounts: Most associations have more than one AWS account, and now and again need to designate access between them. IAM lets you do this without sharing your accreditations and all the more as of late, AWS delivered ControlTower to additionally streamline multi-account designs.
5) AWS Organizations: For fine-grained control of various AWS accounts, you can utilize AWS Organizations to portion accounts into gatherings and allot consent limits.
6) Personality Federation: On many occasions, your association should combine access from other character suppliers, for example, Okta, G Suite, or Active Directory. IAM empowers you to do this with an element called Identity Federation.

IAM Components



IAM Users:
- IAM users can be an individual, systems, or applications requiring access to AWS services
- A user account consists of a unique name and security credentials such as a password, access key, and/or multi-factor authentication (MFA)
- IAM users only need passwords when they access the AWS Management Console

AM Groups:
- IAM Groups are a way to assign permissions to logical and functional units of your organization
- IAM groups are a tool to help with operational efficiency, Bulk permissions management (scalable), and easy to change permissions as individuals change teams (portable)
- A group can contain many users, and a user can belong to multiple groups.
- Groups can't be nested; they can contain only users, not other groups.

IAM Policies:
- IAM policies are JSON-based statements that define access control and permissions.

- IAM policies can be “inline” or “managed” and can be attached to a user or a group
- Inline policies – policies that you create and manage, and that are embedded directly into a single user, group, or role.
- Managed policies – standalone policies that you can manage separately from the IAM users, groups, or roles to which they are attached.

Elements of IAM Policies

Version	Specifies the current version of the policy language
Statement	Contain an array of elements
Effect	Whether the statement will result in an allow or an explicit deny
Action	Describes the specific action or actions that will be allowed or denied
Resource	Specifies the object or objects that the statement covers
Principal	Principal element specifies the identity

IAM Roles:

- An IAM role is like a user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS.
- You can authorize roles to be assumed by humans, Amazon EC2 instances, custom code, or other AWS services for specific access to services.
- Roles do not have standard long-term credentials such as a password or access keys associated with it, instead, when you assume a role, it provides you with temporary security credentials for your role session.

AWS IAM Access Analyzer

If you have two or more AWS accounts, do yourself a favor and start using the IAM access analyzer for your organizational security. The access analyzer gives you all the AWS resources which are exposed outside of your AWS organization.

- IAM Access Analyzer continuously monitors resource policies for changes, eliminating the need to rely on intermittent manual checks in order to catch issues as policies are added or updated.
- It helps you to create an extensive report for all your AWS assets that could be accessed publically by utilizing Access Analyzer,
- Access Analyzer is a piece of Amazon’s Provable Security endeavors to accomplish the most significant levels of security utilizing mechanized thinking innovation and scientific rationale.

How it works

1 Create an analyzer

You can set the scope for the analyzer to an organization or an AWS account. This is your zone of trust. The analyzer scans all of the supported resources within your zone of trust.

2 Review active findings

When Access Analyzer finds a policy that allows access to a resource from outside of your zone of trust, it generates an active finding. Findings include details about the access so that you can take action.

3 Take action

If the access is intended, you can archive the finding so that you can focus on reviewing active findings. If the access is not intended, you can resolve the finding by modifying the policy to remove access to the resource.

IAM Access Analyzer is in accordance with the general ethos of AWS IAM administration, which means it includes no extra expense and is incorporated as a feature of the IAM support.