AWS Identity and Access Management

Securely manage identities and access to AWS services and resources

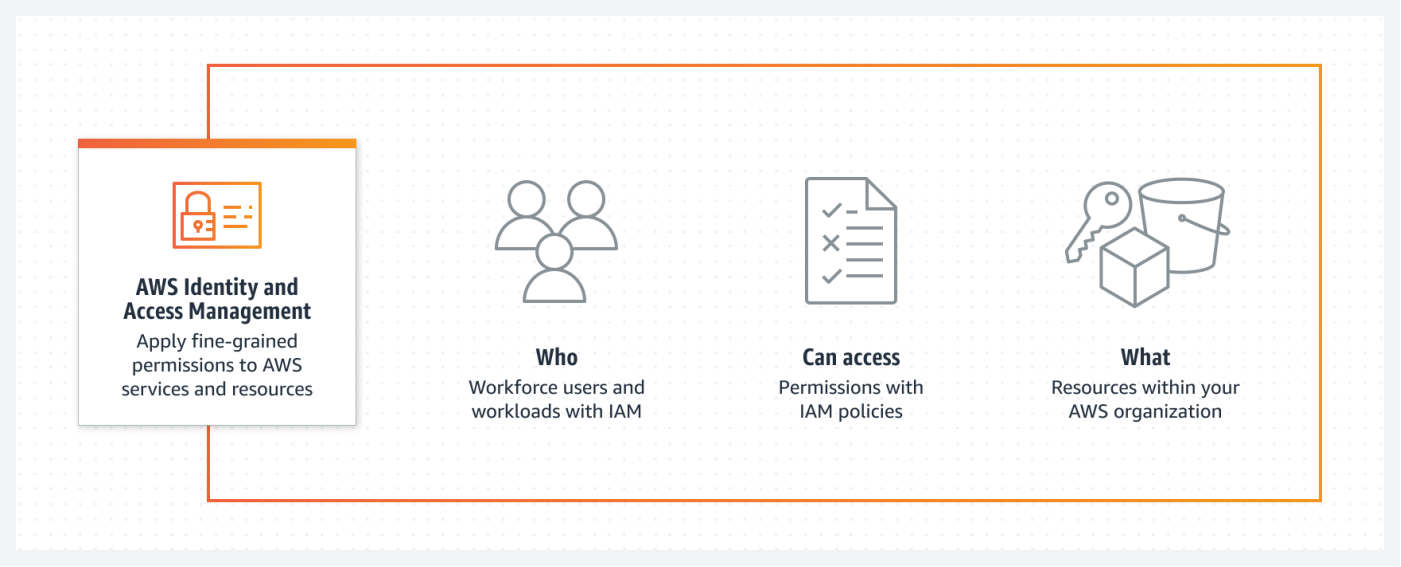
AWS Identity and Access Management (IAM) helps you manage access to your AWS resources. With IAM, you create identities, such as users, groups, and roles, and attach policies to those identities to specify which resources they can access.

Concepts

- **Users:** People, services, or applications that can access your AWS resources.
- **User groups:** Collections of IAM users. Instead of managing permissions individually, you can assign permissions to a group with multiple users. All users in the group will share the same permissions.
- **Roles:** Provide temporary access to AWS services, applications, or users.
- **Policies:** JSON documents that define permissions for users, groups, and roles.

How It Works

With AWS Identity and Access Management (IAM), you can specify who or what can access services and resources in AWS, centrally manage fine-grained permissions, and analyze access to refine permissions across AWS.



Use Cases

Manage user access
Provide unique credentials to each user, ensuring accountability and precise access control.

Enable federation with external identity providers
Allow users to access AWS resources usig their existing corporate credentials.

Enforce security policies
Require MFA, enforce password complexity rules, or restrict access based on IP address ranges.

Implement role-based access
Define permissions for specific job functions, such as developers, database administrators, and more.