# AWS Identity and Access Management(IAM)

- Securely manage identities and access to AWS services and resources

- IAM makes it easy to provide multiple users secure access to AWS resources.

-

Benefits of AWS Identity and Access Management

1. Set permission guardrails and fine-grained access

2. Manage workload and workforce identities across your AWS accounts

3. Use temporary security credentials and permission sets to access your AWS resources

4. Analyze access and validate IAM policies as you move toward least privilege

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.
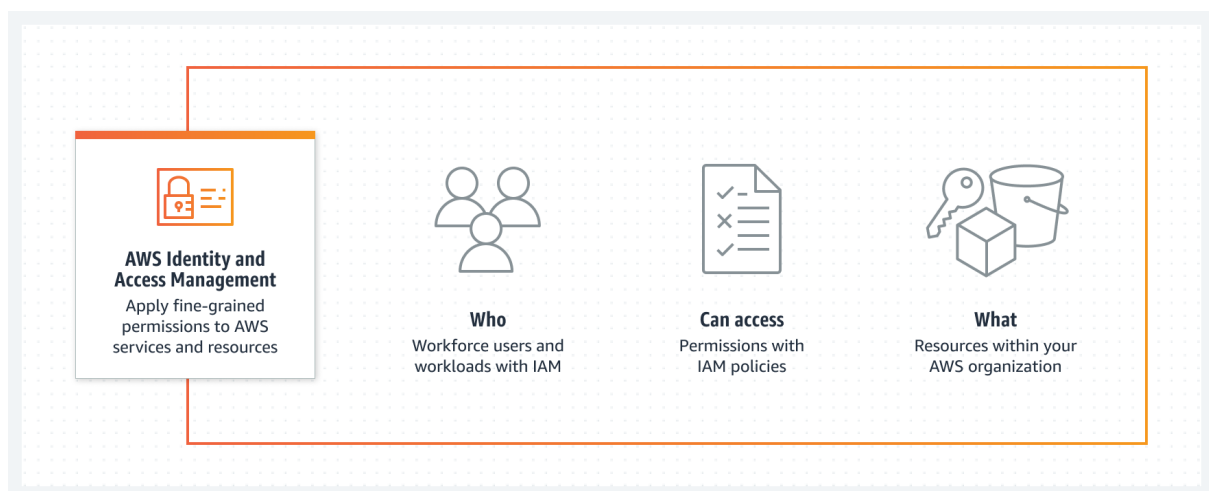
Use cases

- Apply fine-grained permissions and scale with attribute-based access control

- Manage per-account access or scale access across AWS accounts and applications

- Establish organization-wide and preventative guardrails on AWS

- Set, verify, and right-size permissions toward least privilege