What is IAM?

* AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, you can centrally manage permissions that control which AWS resources users can access. (Với IAM, bạn có thể quản lý tập trung các quyền kiểm soát những tài nguyên AWS mà người dùng có thể truy cập). You use IAM to control who is authenticaed and authorized (has permissions) top use resources.
* When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create account. We strongly recommend that you don’t user the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the AWS Account Management Reference Guide.

IAM features

IAM gives you the following features:

* Shared access to your AWS account:

+ You can grant other people permission to administer and use resources in your AWS account without having to share your password or access key.

* Granular permissions (quyền chi tiết)  
  + You can grant different permissions to different people for different resources. For example, you might allow some users complete access to Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3) and other AWS services. For other users, you can allow read-only access to just some S3 buckets, or permission to administer just some EC2 instances, or to access your billing information but nothing else.
* Secure access to AWS resources for applications that run on Amazon EC2

+ You can use IAM features to securely provide credentials for applications that run on EC2 instances. These credentials provide permission for your application to access other AWS resources. Example include S3 and DynamoDB tables.

* Multi-factor authentication (MFA)

+ You can add two-factor authentication to your account and to individual (cá nhân) users for extra (thêm, tăng) security. With MFA you or your users must provide not only a password or access key to work with your account, but also a code from a specially configured device. If you already use a FIDO security key with other services, and it has an AWS supported configuration, you can use WebAuthn for MFA security.

* Identity federation (liên kết danh tính)

+ You can allow users who already have passwords elsewhere—for example, in your corporate network or with an internet identity provider—to get temporary access to your AWS account.

* Identity information for assurance (Thông tin nhận dạng để đảm bảo)  
  + Nếu bạn sử dụng AWS CloudTrail, bạn sẽ nhận được bản ghi nhật ký thông tin bao gồm thông tin về những người đã yêu cầu tài nguyên trong tài khoản của bạn. Thông tin đó dựa trên danh tính IAM.
* Integrated with many AWS services.  
  + For a list of AWS services that work with IAM, see AWS services that work with IAM.
* PCD DSS Compliance
* Eventually Consistent (cuối cùng nhất quán)

+ IAM, like many other AWS services, is eventually consistent. IAM achieves high availability by replicating data across multiple servers within Amazon’s data center

+ IAM đạt được tính sẵn sằng cao bằng cách sao chép dữ liệu trên nhiều máy chủ trong các trung tâm dữ liệu của Amazon trên khắp thế giới. Nếu yêu cầu thay đôi một số dữ liệu thành công, thay đổi sẽ được cam kết và lưu trữ an toàn. Tuy nhiên, thay đổi phải được sao chép trên IAM, quá trình này có thể mất một chút thời gian. Những thay đổi đó bao gồm việc tạo hoặc cập nhật người dùng, nhóm, vai trò hoặc chính sách. Thay vào đó, hãy thực hiện các thay đổi IAM trong quy trình khởi tạo hoặc thiết lập riêng biệt mà bạn chạy ít thường xuyên hơn. Ngoài ra, hãy đảm bảo xác minh rằng các thay đổi đã được phổ biến trước khi quy trình sản xuất phụ thuộc vào chúng. Để biết thêm thông tin, hãy xem những thay đổi mà tôi thực hiện không phải lúc nào cũng hiển thị nay lập tức.

* Free to use

+ AWS Identity and Access Management (IAM) và AWS Security Token Service (AWS STS) là các tính năng của tài khoản AWS được cung cấp miễn phí. Bạn chỉ bị tính phí khi truy cập các dịch vụ AWS khác bằng cách sử dụng người dùng IAM hoặc thông tin đăng nhập bảo mật tạm thời.

Accessing IAM

You can work with AWS Identity and Access Management in any of the following ways.

AWS Management Console  
AWS Command Line Tools  
AWS SDKs  
IAM Query API