1. **IAM là gì**

AWS identity and access management (IAM) cho phép bạn quản lý truy cập vào các dịch vụ và tài nguyên AWS một cách bảo mật mà không cần chia sẻ thông tin user, password. Đây là Global Service

Identity = Authentication

Access = Authorization



1. **IAM features**

**Share access permission**

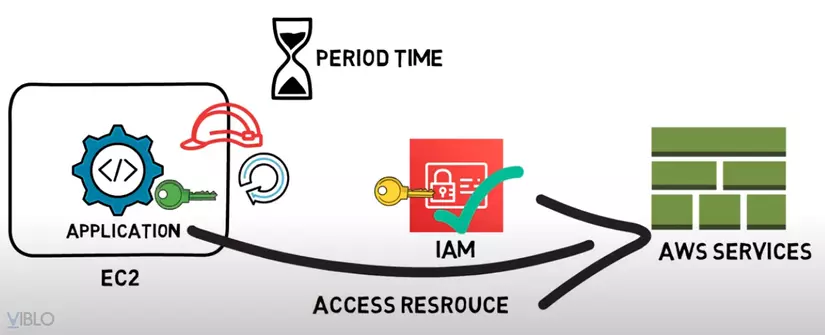
IAM cho phép admin có thể chia sẻ và gán quyền cho các users là thành viên của projects hoặc nhiều thành viên liên quan sử dụng aws.

**Granular permission**

IAM cho phép gán quyền cụ thể và chi tiết đối với từng user, từng service và từng action cụ thể.

**Using role to access AWS resource**

IAM cho phép các ứng dụng chạy trên dịch vụ EC2, có quyền truy cập vào các tài nguyên khác của AWS, nhờ việc cung cấp các Credentials một cách bảo mật, bằng cách sử dụng IAM role.



Multi-Factor Authenticator (MFA)

IAM cho phép thêm các lớp bảo mật, bảo mật 2 lớp. Việc này nhằm nâng cao mức độ bảo mật của tài khoản, tránh rủi ro không đáng có khi bị lộ thông tin.



Identity Federation

IAM cho phép các users sử dụng các tài nguyên AWS thông qua việc xác thực từ các Identity Provider như Google, Facebook …

Identity Information for assurance

IAM cho phép cung cấp thông tin các thực thể đã thao tác, hành động, truy cập trên tài nguyên AWS cho các dịch vụ lưu trữ như CloudTrail nhằm mục đích kiểm tra, truy vết.

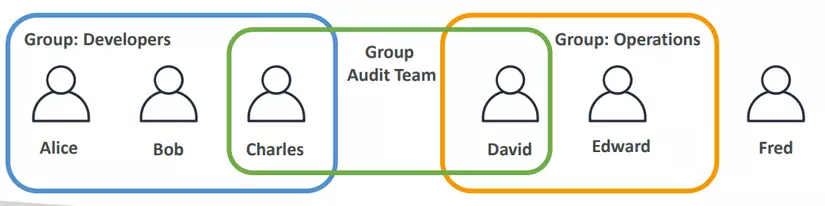
1. Thuật ngữ liên quan đến IAM
2. User & Group

Root account được tạo ra mặc định, không nên được sử dụng hay chia sẻ.

User là thành viên trong 1 project, và có thể được thêm vào group để dễ dàng quản lý và cấp quyền.

Group chỉ gồm users, không bao gồm groups.

Users không nhất thiết phải thuộc về 1 group, 1 user có thể thuộc 1 hoặc nhiều group khác nhau.



1. Permission

Users hoặc Groups hoặc role sẽ được gán permissions trong Policy

Policy là một văn bản được viết dưới dạng JSON, định nghĩa quyền hạn cho các user, group, role.

1. User truy cập vào AWS bằng cách nào

User có thể thông qua 3 cách:

1. AWS Management Console (Authen với password + MFA)
2. AWS Command Line Interface (Authen với access\_keys)
3. AWS Software Developer Kit (Authen với access\_keys)
4. IAM Roles

Role phổ biến:

1. EC2 instance roles
2. Lambda Funtions Roles
3. Roles for CloudFormation
4. IAM Security Tools

IAM Credentials Report (account – level)

Là loại báo cáo liệt kê tất cả các loại người dùng và trạng thái của các thông tin đăng nhập (credential) của họ.

IAM Access Advisor (user – level)

Là một cố vấn truy cập, có nhiệm vụ show ra các dịch vụ được cấp cho user và thời điểm các dịch vụ đó được truy cập lần cuối (last – accessed)

Những thông tin này là căn cứ để bạn có chính sách thay đổi policy phù hợp.

1. Trách nhiệm của từng vai trò khi sử dụng IAM

Đối tượng: Infrastructure (Global Network Security)

Nhiệm vụ:

Cấu hình và phân tích lỗ hổng

Tuân thủ các quy chuẩn

Đối tượng: Admin

Nhiệm vụ:

Theo dõi các users, groups, roles, policies

Bật MFA cho tất cả các users

Sử dụng IAM tools để đáp ứng các quyền thích hợp

Phân tích các kiểu truy cập (access patterns) và review permissions

1. Nguyên tắc khi sử dụng IAM

Không được sử dụng root account trừ khi dùng thư viện setup account đó

1 Người dùng vật lý = 1 AWS user

Gán user và groups và gán permissions và groups

Tạo 1 chính sách mật khẩu mạnh

Bắt buộc sử dụng MFA

Tạo và sử dụng Roles khi cấp các quyền cho các dịch vụ AWS

Sử dụng Access Keys khi truy cập IAM (CLI/SDK)

Kiểm tra permissions cho account thông qua IAM Credential Report

Không được phép share IAM users & Access Keys

1. Tổng kết

User map với người dùng vật lý, có password khi dùng AWS Console

Groups chỉ chứa users

Policies là văn bản JSON định nghĩa permissions cho users hoặc groups hoặc roles

Roles dùng cho EC2 instances hoặc AWS services

Security thiết lập Password policy + MFA

Access Keys dùng cho truy cập AWS bằng CLI/SDK

Audit công cụ kiểm tra như IAM Credential Reports & IAM Access Advisor

https://viblo.asia/p/gioi-thieu-ve-dich-vu-iam-cua-aws-LzD5dandKjY