

Tổng hợp bài học AWS Practitioner Cloud

Sonthkl95

08/07/2025

Mục lục

1	What is Cloud Computing?	3
1.1	What is a server composed of?	3
1.2	IT Terminology	3
1.3	Problems with traditional IT approach	3
1.4	What is Cloud Computing?	4
1.5	You've been using some Cloud services	4
1.6	The Deployment Models of the Cloud	5
1.7	The five characteristics of Cloud Computing	5
1.8	Six Advantages of Cloud Computing	6
1.9	Problems solved by the Cloud	6
1.10	Types of Cloud Computing	7
1.11	Example of Cloud Computing Types	8
1.12	Pricing of the Cloud - Quick Overview	8
1.13	AWS Cloud History	8
1.14	AWS Cloud Use Cases	9
1.15	AWS Regions	9
1.16	How to choose AWS Region?	9
1.17	AWS Availability Zones	10
1.18	Shared Responsibility Model Diagram	10
1.19	AWS Acceptable Use Policy	11
2	IAM - Identity and Access Management	12
2.1	Users & Groups	12
2.2	Permissions	12
2.3	IAM Policies inheritance	13
2.4	IAM Policies structure	13
2.5	IAM Password Policy	14
2.6	Multi Factor Authentication - MFA	14
2.7	MFA devices options in AWS	15
2.8	How can users access AWS?	15
2.9	What's the AWS CLI?	16
2.10	What's the AWS SDK?	16
2.11	IAM Roles for Services	16
2.12	IAM Security Tools	17
2.13	IAM Guidelines & Best Practices	17
2.14	Shared Responsibility Model for IAM	18
2.15	IAM - Summary	18
3	EC2 Section	20
3.1	Amazon EC2	20
3.2	EC2 sizing & configuration options	20

1 What is Cloud Computing?

Điện toán đám mây là gì

1.1 What is a server composed of?

Máy chủ gồm những thành phần nào

- Compute (tính toán): CPU
- Memory (bộ nhớ): RAM
- Storage (kho lưu trữ): Data
- Database (Cơ sở dữ liệu): Store data in a structured way (Lưu trữ dữ liệu một cách có cấu trúc)
- Network (mạng lưới): Routers (bộ định tuyến), switch (bộ chuyển mạch), DNS server (Máy chủ DNS)

1.2 IT Terminology

Thuật ngữ IT

- Network (mạng lưới): bao gồm các loại dây cáp (cables), các bộ định tuyến (routers) và các máy chủ được kết nối với nhau.
- Router (bộ định tuyến): Một mạng lưới các thiết bị dùng chuyển tiếp các gói dữ liệu giữa các mạng lưới máy tính. Nó biết nơi cần gửi các gói dữ liệu của bạn trên internet.
- Switch (bộ chuyển đổi): Nhận gói dữ liệu và gửi nó đến chính xác máy chủ/ người dùng trên network của bạn

1.3 Problems with traditional IT approach

Các vấn đề với cách tiếp cận CNTT truyền thống

- Pay for the rent the data center (Trả tiền thuê cho trung tâm dữ liệu)
- Pay for power supply, cooling, maintenance (Trả tiền cho nguồn điện, hệ thống làm mát và bảo trì, bảo dưỡng)
- Adding and replacing hardware takes time (Việc thêm và thay thế thiết bị phần cứng tốn thời gian)
- Scaling is limited (Việc mở rộng bị giới hạn)
- Hire 24/7 team to monitor the infrastructure (Thuê đội ngũ trực 24/7 để giám sát hạ tầng)
- How to deal with disasters? (earthquake, power shutdown, fire, ...) (Làm sao để ứng phó với các sự cố ? (động đất, mất điện, cháy, ...))

1.4 What is Cloud Computing?

Điện toán đám mây là gì?

- Cloud computing is the on-demand delivery of compute power, database storage, applications, and other IT resources (Điện toán đám mây là hình thức cung cấp theo yêu cầu sức mạng tính toán, lưu trữ cơ sở dữ liệu, ứng, và các tài nguyên công nghệ thông tin khác)
- Through a cloud services platform with pay-as-you-go pricing (Thông qua một nền tảng dịch vụ đám mây với mô hình tính phí theo mức sử dụng)
- You can provision exactly the right type and size of computing resources you need (Bạn có thể triển khai một cách chính xác đúng với kiểu và kích thước tính toán tài nguyên mà bạn cần)
- You can access as many resources as you need, almost instantly (Bạn có thể truy cập nhiều tài nguyên mà bạn cần, gần như ngay lập tức)
- Simple way to access servers, storage, databases and a set of application services (Một cách đơn giản để truy cập các máy chủ, kho lưu trữ, các cơ sở dữ liệu và một tập hợp dịch vụ ứng dụng)
- Amazon Web Service owns and maintains the network-connected hardware required for these application services, while you provision and use what you need via a web application (Amazon Web Service sở hữu và duy trì thiết bị phần cứng kết nối mạng lưới cần thiết cho các dịch vụ ứng dụng này trong khi bạn triển khai và sử dụng thông qua một ứng dụng web)

1.5 You've been using some Cloud services

Bạn đang sử dụng vài dịch vụ đám mây

- Gmail
 - E-mail cloud service (Dịch vụ đám mây E-mail)
 - Pay for only your emails stored (no infrastructure, etc.) (Bạn chỉ phải trả tiền cho số email của bạn được lưu trữ (không phải trả chi phí cho hạ tầng hệ thống hay các chi phí khác))
- Dropbox
 - Cloud Storage Service (Dịch vụ lưu trữ đám mây)
 - Originally built on AWS (Ban đầu được xây dựng trên AWS)
- Netflix
 - Build on AWS (Xây dựng AWS)
 - Video on demand (Video theo yêu cầu)

1.6 The Deployment Models of the Cloud

Các mô hình triển khai của đám mây

- Private Cloud (Điện toán đám mây riêng)
 - Cloud services used by a single organization, not exposed to the public (Dịch vụ đám mây được sử dụng bởi một tổ chức duy nhất, không để lộ ra ngoài)
 - Complete control (Hoàn toàn kiểm soát)
 - Security for sensitive applications (Bảo mật cho các ứng dụng nhạy cảm)
 - Meet specific business needs (Đáp ứng nhu cầu kinh doanh cụ thể)
- Public Cloud (Điện toán đám mây công cộng)
 - Cloud resources owned and operated by a third-party cloud service (Tài nguyên đám mây được sở hữu và vận hành bởi một nhà cung cấp dịch vụ đám mây bên thứ ba)
 - Six advantages of Cloud Computing (Sáu lợi ích của điện toán đám mây)
- Hybrid Cloud (Điện toán đám mây lai)
 - Keep some servers on premises and extend capabilities to the Cloud (Giữ lại một số máy chủ tại văn phòng và mở rộng một số tính năng lên đám mây)
 - Control over sensitive assets in your private infrastructure (Kiểm soát các tài nguyên nhạy cảm trong hệ thống hạ tầng riêng của bạn)
 - Flexibility and cost-effectiveness of the public cloud (Tính linh hoạt và hiệu quả chi phí của điện toán đám mây công cộng)

1.7 The five characteristics of Cloud Computing

Năm tính năng của điện toán đám mây

- On-demand self-service (Dịch vụ tự phục vụ theo yêu cầu)
 - Users can provision resources and use them without human interaction from the service provider (Người dùng có thể tự cấp phát tài nguyên và sử dụng chúng mà không cần sự tương tác của con người từ phía nhà cung cấp)
- Broad network access (Khả năng truy cập trên phạm vi rộng)
 - Resources available over the network, and can be accessed by diverse client platforms (Các tài nguyên có sẵn thông qua mạng, và có thể được kết nối bởi các nền tảng người dùng đa dạng)
- Multi-tenancy and resources pooling (Kiến trúc nhiều người dùng và Gộp tài nguyên)
 - Multiple customers can share same infrastructure and applications with security and privacy (Nhiều khách hàng có thể chia sẻ chung hạ tầng và ứng dụng mà vẫn đảm bảo bảo mật và quyền riêng tư)
 - Multiple customers are serviced from the same physical resources (Nhiều khách hàng được phục vụ từ cùng một hệ thống tài nguyên vật lý)

- Rapid elasticity and scalability (Khả năng mở rộng nhanh chóng và khả năng điều chỉnh tài nguyên)
 - Automatically and quickly acquire and dispose resources when need (Tự động và nhanh chóng cấp phát và giải phóng tài nguyên khi cần thiết.)
 - Quickly and easily scale based on demand (Nhanh chóng và dễ dàng mở rộng tài theo yêu cầu)
- Measured service (Dịch vụ được đo lường)
 - Usage is measured, users pay correctly for what they have used (Việc sử dụng được đo lường và ghi nhận, người dùng trả đúng với những gì họ đã sử dụng)

1.8 Six Advantages of Cloud Computing

Sáu lợi ích của điện toán đám mây

- Trade capital expense (CAPEX) for operational expense (OPEX) (Chuyển đổi chi phí đầu tư dài hạn sang chi phí vận hành)
 - Pay On-Demand: Don't own hardware (Trả tiền theo yêu cầu: Không sở hữu phần cứng)
 - Reduce Total Cost of Ownership (TCO) & Operational Expense (OPEX) (Giảm tổng chi phí sở hữu và chi phí vận hành)
- Benefit from massive economies of scale (Hưởng lợi từ tiết kiệm quy mô lớn)
 - Prices are reduced as AWS is more efficient due to large scale (Giá thành được giảm xuống nhờ AWS hoạt động hiệu quả nhờ quy mô lớn)
- Stop guessing capacity (Dừng đoán dung lượng)
 - Scale based on actual measured usage (Mở rộng quy mô dựa trên mức sử dụng thực tế đã được đo lường)
- Increase speed and agility (Tăng tốc độ và sự linh hoạt)
- Stop spending money running and maintaining data centers (Nhưng chi tiền để vận hành và bảo trì các trung tâm dữ liệu)
- Go global in minutes (Mở rộng ra toàn cầu trong vài phút): Leverage the AWS global infrastructure (Tận dụng hạ tầng toàn cầu của AWS)

1.9 Problems solved by the Cloud

Các vấn đề được giải quyết bởi Cloud

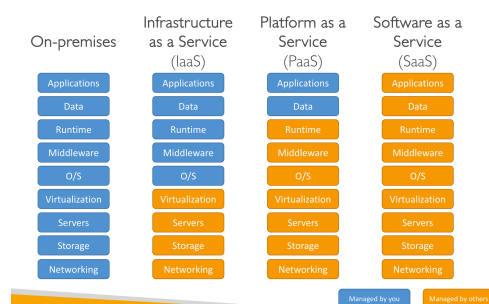
- Flexibility (Tính linh hoạt): Change resource types when needed (Thay đổi loại tài nguyên khi cần thiết)
- Cost-Effectiveness (Hiệu quả về chi phí): Chỉ trả tiền cho những gì bạn sử dụng

- Scalability (Khả năng mở rộng): Accommodate large loads by stronger or adding additional nodes (Đáp ứng tải lớn hơn bằng cách nâng cấp phần cứng hoặc thêm các nút bổ sung.)
- Elasticity (Khả năng điều chỉnh tài nguyên): Ability to scale out and scale in when needed (Khả năng mở rộng hoặc thu hẹp tài nguyên linh hoạt khi cần thiết)
- High-availability and fault-tolerance (Tính sẵn sàng và khả năng chịu lỗi cao): build across data centers (Xây dựng trên nhiều trung tâm dữ liệu)
- Agility (Tính linh hoạt): Rapidly develop, test and launch software applications (Phát triển, kiểm thử và khởi động ứng dụng phần mềm một cách nhanh chóng)

1.10 Types of Cloud Computing

Các loại dịch vụ điện toán đám mây

- Infrastructure as a Service (IaaS) (Cơ sở hạ tầng như một dịch vụ)
 - Provide building blocks for Cloud IT (Cung cấp các thành phần cơ bản cho hệ thống CNTT đám mây)
 - Provides networking, computers, data storage space (Cung cấp kết nối mạng, máy tính và không gian lưu trữ dữ liệu)
 - Highest level of flexibility (Sự linh hoạt ở cấp độ cao nhất)
 - Easy parallel with traditional on-premises IT (Dễ dàng tích hợp song song với hệ thống CNTT truyền thống tại chỗ)
- Platform as a Service (PaaS) (Nền tảng như một dịch vụ)
 - Removes the need for your organization to manage the underlying infrastructure (Loại bỏ nhu cầu quản lý hạ tầng cơ sở của tổ chức bạn)
 - Focus on the deployment and management of your applications (Tập trung cho việc triển khai và quản lý ứng dụng của bạn)
- Software as a Service (SaaS) (Ứng dụng như một dịch vụ)
 - Completed product that is run and managed by the service provider (Sản phẩm hoàn chỉnh được vận hành và quản lý bởi nhà cung cấp dịch vụ)



Hình 1: paas-saas-iaas

1.11 Example of Cloud Computing Types

Ví dụ các loại điện toán đám mây

- Infrastructure as a Service
 - Amazon EC2 (on AWS)
 - GCP, Azure, Rackspace, Digital Ocean, Linode
- Platform as a Service
 - Elastic Beanstalk (on AWS)
 - Heroku, Google App Engine (GCP), Windows Azure (Microsoft)
- Software as a Service
 - Many AWS services (ex: Rekognition for Machine Learning)
 - Google Apps (Gmail), Dropbox, Zoom

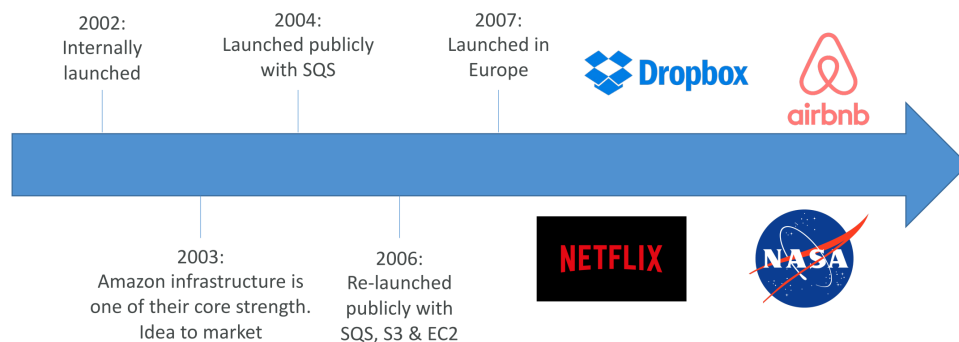
1.12 Pricing of the Cloud - Quick Overview

Cách tính phí của Đám mây - Tổng quan nhanh

- AWS has 3 pricing fundamentals, following the pay-as-you-go pricing model (AWS có 3 nguyên tắc định giá cơ bản, dựa trên mô hình trả tiền theo mức sử dụng)
- Compute (Tính toán): Pay for compute time (Trả cho thời gian tính toán)
- Storage (Lưu trữ): Pay for data stored in the Cloud (Trả tiền cho lưu trữ dữ liệu trên đám mây)
- Data transfer OUT of the Cloud: Data transfer IN is free (Truy xuất dữ liệu từ đám mây sẽ bị tính phí: việc tải dữ liệu lên là miễn phí.)
- Solves the expensive issue of traditional IT (Giải quyết bài toán chi phí cao của hạ tầng IT truyền thống)

1.13 AWS Cloud History

Lịch sử đám mây AWS



Hình 2: history-aws-cloud

1.14 AWS Cloud Use Cases

Các trường hợp sử dụng đám mây AWS

- AWS enables you to build sophisticated, scalable applications (AWS cho phép bạn xây dựng các ứng dụng phức tạp và có khả năng mở rộng)
- Applicable to a diverse set of industries (Có thể áp dụng cho nhiều ngành công nghiệp khác nhau)
- Use cases include
 - Enterprise IT, Backup & Storage, Big data analytics
 - Web hosting, Mobile & Social Apps
 - Gaming

1.15 AWS Regions

- AWS has Regions all around the world (AWS có các Regions trên khắp thế giới.)
- Names can be us-east-1, eu-west-3, ...(Có thể là us-east-1, eu-west-3)
- A region is a cluster of data centers (Một region là một cụm trung tâm dữ liệu.)
- Most AWS services are region-scoped (Hầu hết các dịch vụ AWS có phạm vi theo vùng (region).)

1.16 How to choose AWS Region

Cách chọn một AWS Region?

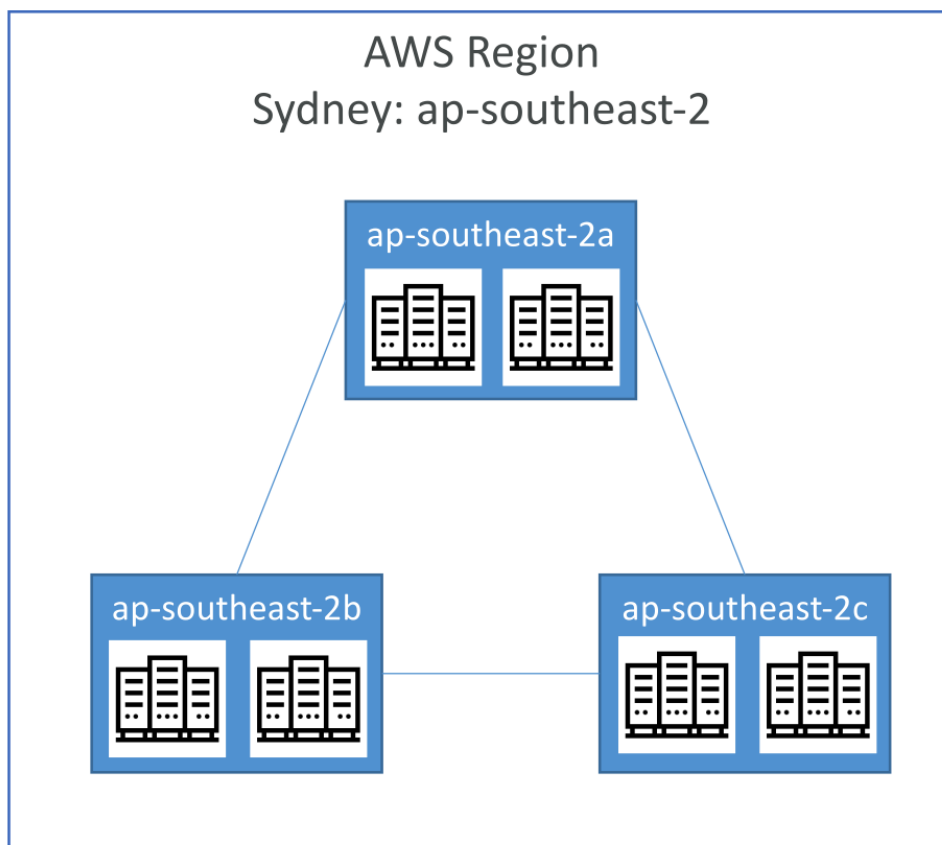
if you need launch a new application, where should you do it?

- **Compliance** with data governance and legal requirements: data never leaves a region without your explicit permission (Tuân thủ các yêu cầu về quản trị dữ liệu và pháp lý: dữ liệu không bao giờ rời khỏi khu vực mà không có sự cho phép rõ ràng từ bạn)
- **Proximity** to Customer: reduced latency (Gần với khách hàng: giảm độ trễ hệ thống)
- **Available services** within a Region: new services and new features aren't available in every Region (Các dịch vụ có sẵn trong khu vực: Các dịch vụ mới và tính năng không có sẵn ở mọi khu vực)
- **Pricing**: pricing varies region to region and is transparent in the service pricing page (Giá cả: Giá cả thay đổi từ khu vực này sang khu vực khác và được công khai trên trang giá dịch vụ)

1.17 AWS Availability Zones

AZ

- Each region has many availability zones (usually 3, min is 3, max is 6). (Example:)
 - ap-southeast-2a
 - ap-southeast-2b
 - ap-southeast-2c
- Each availability zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity (Mỗi AZ là một hoặc nhiều trung tâm dữ liệu riêng biệt với năng lượng dự phòng, mạng lưới và kết nối dự phòng)
- They're separate from each other, so that they're isolated from disasters (Chúng tách rời nhau, nên chúng bị cô lập khỏi thảm họa)
- They're connected with high bandwidth, ultra-low latency networking (AZ được kết nối với băng thông cao, độ trễ mạng siêu thấp)



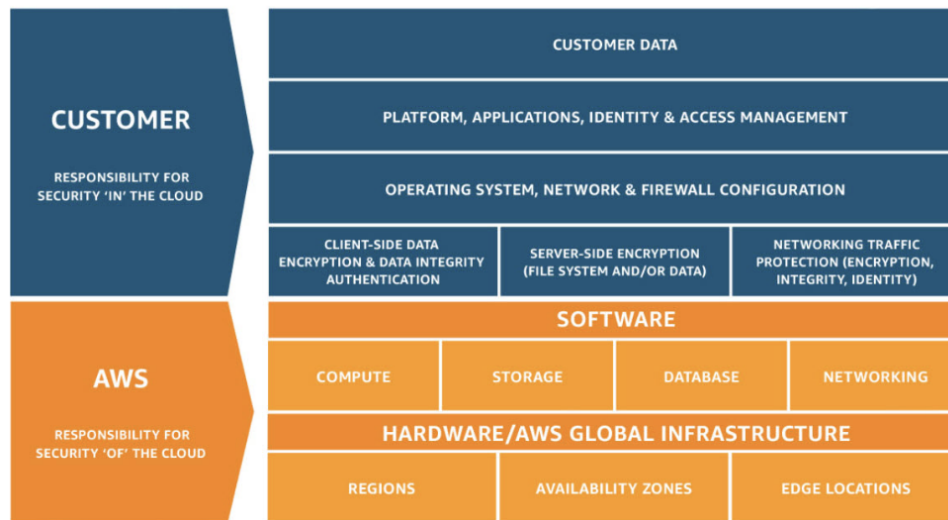
Hình 3: Mô hình AZ

1.18 Shared Responsibility Model Diagram

Sơ đồ mô hình chia sẻ trách nhiệm

- CUSTOMER = RESPONSIBILITY FOR THE SECURITY IN CLOUD

- AWS = RESPONSIBILITY FOR THE SECURITY FOR CLOUD



Hình 4: shared-responsibility

1.19 AWS Acceptable Use Policy

Chính sách sử dụng được chấp nhận của AWS

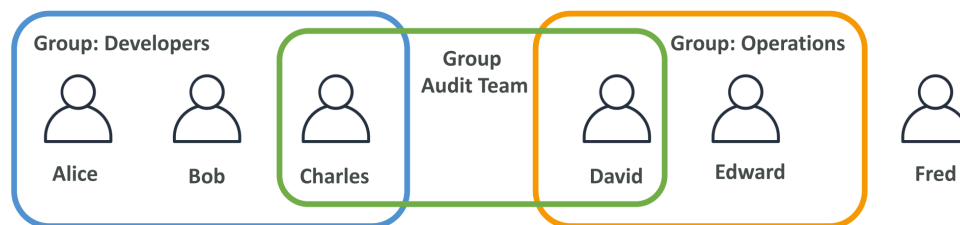
- No Illegal, Harmful, or Offensive Use or Content (Bạn không được sử dụng dịch vụ AWS để tạo, truyền, hoặc lưu trữ bất kỳ thứ gì bất hợp pháp, gây hại hoặc mang tính xúc phạm.)
- No Security Violations (Không được vi phạm các bảo mật)
- No Network Abuse (Không lạm dụng mạng)
- No E-mail or Other Message Abuse (Không lạm dụng email hoặc các hình thức nhắn tin khác)

2 IAM - Identity and Access Management

IAM - Định danh và quản lý quyền hạn

2.1 Users & Groups

- IAM = Identity and Access Management, Global service
- **Root account** created by default, shouldn't be used or shared
- **Users** are people within your organization, and can be grouped
- **Group** only contain users, not other groups
- Users don't have to belong to a group, and user can belong to multiple groups (Người dùng không bắt buộc phải thuộc vào một nhóm nào, và một người dùng có thể thuộc về nhiều nhóm.)



Hình 5: iam-group

2.2 Permissions

Các quyền hạn

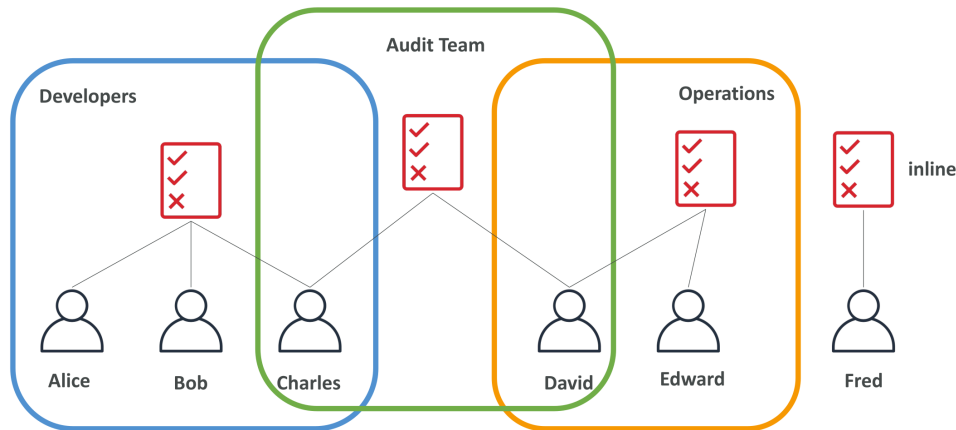
- **Users or Group** can be assigned JSON documents called policies (Các người dùng và nhóm có thể được gán tài liệu JSON được gọi là policies)
- These policies define the permission of the users (Các policies định nghĩa quyền hạn của các người dùng)
- In AWS you apply the **least privilege principle**: don't give more permissions than a user needs (Trong AWS, bạn áp dụng nguyên tắc đặc quyền tối thiểu: không cấp nhiều quyền hơn mức người dùng thực sự cần.)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "allow",
      "Action": "elasticloadbalancing:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "allow",
      "Action": [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

Hình 6: iam-policies

2.3 IAM Policies inheritance

Kế thừa IAM Policies



Hình 7: iam-policies-inheritance

2.4 IAM Policies structure

Cấu trúc IAM Policies

- Consists of
 - Version: policy language version, always include "2012-10-17"
 - ID: an identifier for the policy (optional)
 - Statement: one or more individual statements (required) (Một hoặc nhiều câu lệnh riêng lẻ)
- Statement consists of
 - Sid: an identifier for that statement (optional)
 - Effect: whether the statement allows or denies access (Allow, Deny)
 - Principal: account/ user/ role to which this policy applied to
 - Action: list of actions this policy allows or denies
 - Resource: list of resources to which the actions applied to
 - Condition: conditions for when this policy is in effect (optional)

```
{
  "Version": "2012-10-17",
  "Id": "Policy-Permissions",
  "Statement": [
    {
      "Sid": "1",
      "Effect": "Allow",
      "Principal": {
        "AWS": ["arn:aws:iam::123456789012:root"]
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": ["arn:aws:s3:::mybucket/*"]
    }
  ]
}
```

Hình 8: iam-policies-structure

2.5 IAM Password Policy

IAM chính sách mật khẩu

- Strong passwords = higher security for your account
- In AWS, you can setup a password policy:
 - Set a minimum password length
 - Require specific character types:
 - * including uppercase letters
 - * lowercase letters
 - * numbers
 - * non-alphanumeric characters (Các ký tự không phải chữ cái và số)
 - Allow all IAM users to change their own passwords
 - Require users to change their password after some time (password expiration)
 - Prevent password re-user

2.6 Multi Factor Authentication - MFA

Nhiều tác nhân Xác thực

- Users have access to your account and can possibly change configurations or delete resources in your AWS account
- You want to protect your Root Accounts and IAM users
- MFA = password you know + security device you own
- Main benefit of MFA: if a password is stolen or hacked, the account is not compromised (Nếu mật khẩu bị đánh cắp hoặc bị hack, tài khoản của bạn không bị xâm nhập)



Hình 9: iam-password-mfa

2.7 MFA devices options in AWS

Tùy chọn thiết bị MFA trong AWS



Hình 10: iam-mfa-option-devices

2.8 How can users access AWS?

Người dùng truy cập AWS bằng cách nào?

- To access AWS, you have three options:
 - AWS Management Console (protected by password + MFA)
 - AWS Command Line Interface (CLI): protected by access keys
 - AWS Software Developer Kit (SDK) - for code: protected by access keys
- Access Key are generated through the AWS Console (Access Key được tạo thông qua bảng điều khiển của AWS)
- Users manage their own access keys
- Access Keys are secret, just like a password. Don't share them
- Access Key ID = username
- Secret Access Key = password

2.9 What's the AWS CLI?

AWS CLI là gì?

- A tool that enables you to interact with AWS services using commands in your command-line shell (Một công cụ cho phép bạn tương tác với các dịch vụ aws bằng cách sử dụng các dòng lệnh trong command-line shell của bạn)
- Direct access to the public APIs of AWS services (Truy cập trực tiếp đến các API công khai của các dịch vụ AWS)
- You can develop scripts to manage your resources
- It's open-source: <https://github.com/aws/aws-cli>
- Alternative to using AWS Management Console (Phương án thay thế cho việc sử dụng AWS Management Console)

2.10 What's the AWS SDK?

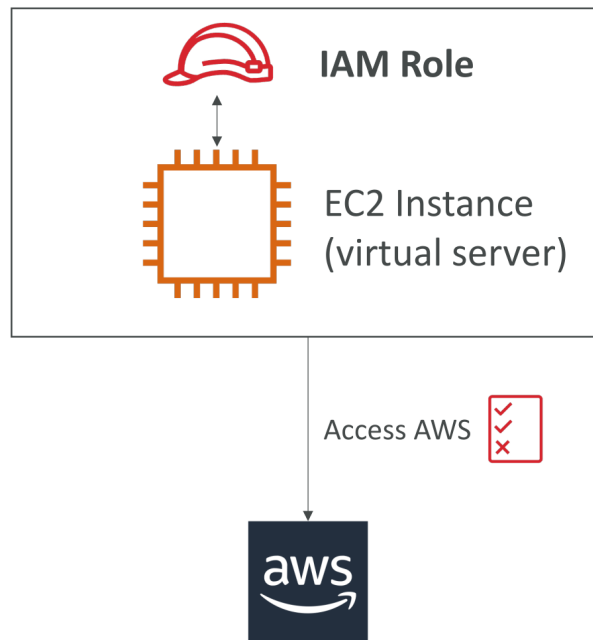
SDK CLI là gì?

- AWS Software Development Kit (AWS SDK)
- Language-specific APIs (set of libraries) (Các API dành riêng cho từng ngôn ngữ lập trình (tập hợp các thư viện))
- Enables you to access and manage AWS services programmatically (Cho phép truy cập và quản lý các dịch vụ AWS bằng lập trình)
- Embedded within your application (Được nhúng bên trong ứng dụng của bạn)
- Supports
 - SDKs (JavaScript, Python, PHP, .NET, Ruby, Java, Go, Node.js, C++)
 - Mobile SDKs (Android, iOS, ...)
 - IoT Device SDKs (Embedded C, Arduino, ...)
- Example: AWS CLI is built on AWS SDK for Python

2.11 IAM Roles for Services

IAM Roles cho các dịch vụ

- Some AWS service will need to perform actions on your behalf (Một vài dịch vụ AWS cần thực hiện các hoạt động thay mặt bạn)
- To do so, we will assign permissions to AWS services with IAM Roles (Để làm được điều đó, chúng ta sẽ gán quyền cho các dịch vụ AWS thông qua IAM Roles.)
- Common roles (các vai trò phổ biến):
 - EC2 Instance Roles
 - Lambda Function Roles
 - Roles for CloudFormation



Hình 11: iam-roles

2.12 IAM Security Tools

Các công cụ bảo mật IAM

- IAM Credentials Report (account-level)
 - A report that lists all your account's users and the status of their various credentials (Báo cáo liệt kê tất cả người dùng trong tài khoản của bạn và trạng thái của các loại thông tin xác thực mà họ đang sử dụng)
- IAM Access Advisor (user-level)
 - Access Advisor shows the service permissions granted to a user and when those services were last accessed (Access Advisor cho thấy các quyền truy cập dịch vụ đã được cấp cho một người dùng và thời điểm các dịch vụ đó được truy cập lần cuối)
 - You can use this information to revise your policies (Bạn có thể sử dụng các thông tin này để sửa đổi các policy của bạn)

2.13 IAM Guidelines & Best Practices

IAM Hướng dẫn và cách làm tối ưu nhất

- Don't use the root account except for AWS account setup (Chỉ sử dụng tài khoản root cho các bước thiết lập ban đầu của tài khoản AWS.)
- One physical user = One AWS user (Mỗi người dùng thực tế nên có một tài khoản người dùng AWS riêng biệt)
- Assign users to groups and assign permissions to groups
- Create a strong password policy

- Use and enforce the use of Multi Factor Authentication (MFA)
- Create and use Roles for giving permissions to AWS services
- Use Access Keys for Programmatic Access (CLI/SDK)
- Audit permissions of your account using IAM Credentials Report & IAM Access Advisor (Kiểm tra quyền truy cập của tài khoản của bạn bằng cách sử dụng IAM Credentials Report và IAM Access Advisor)
- Never share IAM users & Access Keys

2.14 Shared Responsibility Model for IAM

Mô hình chia sẻ trách nhiệm của IAM

- AWS
 - Infrastructure (global network security)
 - Configuration and vulnerability analysis (Cấu hình và phân tích lỗ hổng bảo mật)
 - Compliance validation (Xác thực tuân thủ)
- You
 - Users, Groups, Roles, Policies management and monitoring (quản lý và giám sát)
 - Enable MFA on all accounts
 - Rotate all your keys often (Thường xuyên thay đổi các key của bạn)
 - Use IAM tools to apply appropriate permissions (Sử dụng các công cụ IAM để áp dụng quyền hạn thích hợp)
 - Analyze access patterns & review permission (Phân tích các mẫu truy cập và xem lại các quyền truy cập)

2.15 IAM - Summary

- Users: mapped to a physical user, has a password for AWS Console (gắn liền với người dùng thật, có mật khẩu để đăng nhập AWS Console)
- Groups: contains users only
- Policies: JSON document that outlines permissions for users or groups (là tài liệu JSON mô tả các quyền truy cập dành cho người dùng hoặc nhóm.)
- Roles: for EC2 instances or AWS services
- Security: MFA + Password Policy
- AWS CLI: manage your AWS services using the command-line
- AWS SDK: manage your AWS services using a programming language

- Access Keys: access AWS using the CLI or SDK
- Audit: IAM Credential Reports & IAM Access Advisor

3 EC2 Section

3.1 Amazon EC2

- EC2 is one of the most popular of AWS's offering (EC2 là một trong những sản phẩm nổi tiếng nhất được cung cấp bởi AWS)
- EC2 = Elastic Compute Cloud = Infrastructure as a Service
- It mainly consists in the capability of:(Nó chủ yếu nằm ở khả năng của:)
 - Renting virtual machines (EC2)
 - Sorting data on virtual drives (Sắp xếp dữ liệu trên ổ đĩa ảo)(EBS)
 - Distributing load across machines(chia tải công việc ra giữa nhiều máy khác nhau) (ELB)
 - Scaling the services using an auto-scaling group (Mở rộng dịch vụ bằng cách sử dụng nhóm tự động mở rộng) (ASG)
- Knowing EC2 is fundamental to understand how the Cloud works

3.2 EC2 sizing & configuration options

- Operating System (OS): Linux, Windows or Mac OS
- How much compute power & cores
- How much random-access memory
- How much storage space:
 - Network-attached
 - hardware (EC2 Instance Store)
- Network card: speed of the card, public IP address
- Firewall rules:security group
- Bootstrap script(configure at first launch): EC2 User Data

3.3 EC2 User Data

- It is possible to bootstrap our instances using an EC2 User Data script
- bootstrapping means launching commands when a machine start
- That script is only run once at the instance first start
- EC2 user data is used to automate boot tasks such as:
 - Installing updates
 - Installing software
 - Downloading common files from the internet
 - Any thing you can think of
- The EC2 User Data Script runs with the root user

3.4 EC2 Instance Types - Overview

- You can use different types of EC2 instances that are optimised for different use cases
- AWS has following naming convention:

m5.2xlarge