

aws

# **Khóa học cơ bản tổng thể hệ thống điện toán đám mây Amazon Web Services (AWS Certified Cloud Practitioner)**



## Giới thiệu về khóa học

- ❑ Khóa học này cung cấp các kiến thức kỹ năng cần thiết căn bản cho người đã có một chút kinh nghiệm, và chưa có kinh nghiệm về điện toán đám mây AWS.
- ❑ Bằng việc tham gia khóa học, bạn sẽ hiểu được:  
Các dịch vụ lõi của AWS, bao gồm ảo hóa, hệ thống hạ tầng mạng, cơ sở dữ liệu, và lưu trữ .
- ❑ Các phương pháp thực tiễn về bảo mật và tuân thủ trong điện toán đám mây AWS.
- ❑ Các trường hợp như làm thế nào để xây dựng sản phẩm và ứng dụng trong thực tế. Cũng như chi phí, lợi ích, và tính kinh tế làm việc trong môi trường điện toán đám mây AWS.



- **Giảng viên: Lưu Hồ Phương**, IT Cloud and Network System Infrastructure Consultant
- Trên 18 năm kinh nghiệm làm việc tại các vị trí như : Lập trình viên, kỹ sư mạng, kỹ sư quản trị hệ thống, trưởng phòng IT, và giám đốc kỹ thuật cho các công ty IT của Việt Nam, Singapore, Nhật Bản.
- Kinh nghiệm tham gia tư vấn thiết kế, triển khai, quản trị nhiều dự án. Xây dựng hệ thống ứng dụng, mạng, bảo mật, và điện toán đám mây trong và ngoài nước. Đã từng tham gia giảng dạy tại các trung tâm và học viện CNTT.
- Có chứng chỉ quốc tế: MCSE Cloud Platform and Infrastructure, MCSE Server Infrastructure, LPIC-2 (Linux Professional Institute), AWS Certified Solutions Architect, AWS Certified SysOps Administrator, Linux Academy Red Hat Certified Engineer

# Tìm hiểu về điện toán đám mây AWS



# Bạn nghĩ gì? Bạn đã từng nghe đến điện toán đám mây?

Điện toán đám mây thực sự là gì. Dữ liệu của bạn được lưu ở đâu?

Dữ liệu của tôi  
nằm trong đám  
mây



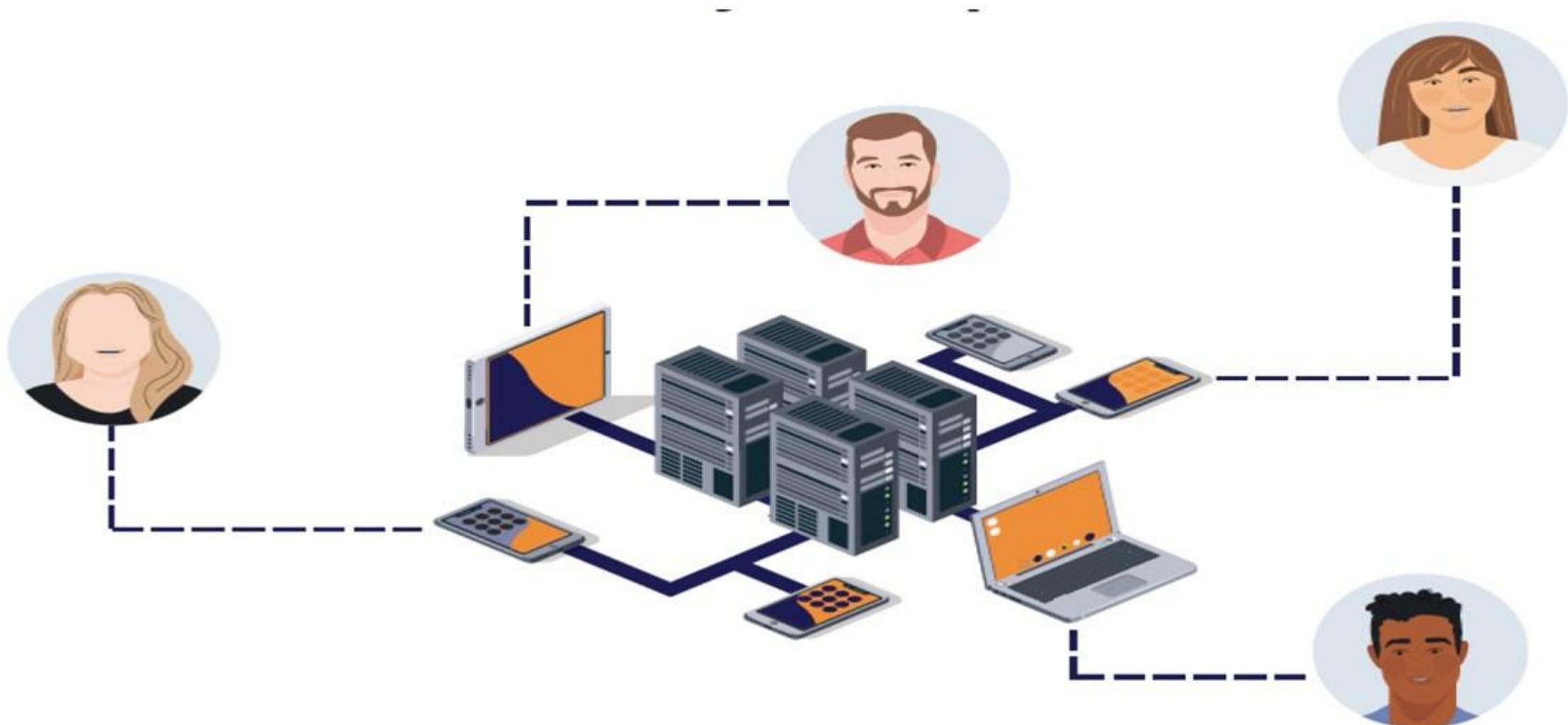
Bạn nên di chuyển  
đến đám mây



Bạn nên làm việc  
trong đám mây



**Điện toán đám mây có thể hiểu là có những trung tâm dữ liệu, cung cấp dịch vụ tài nguyên CNTT cho người dùng qua Internet**



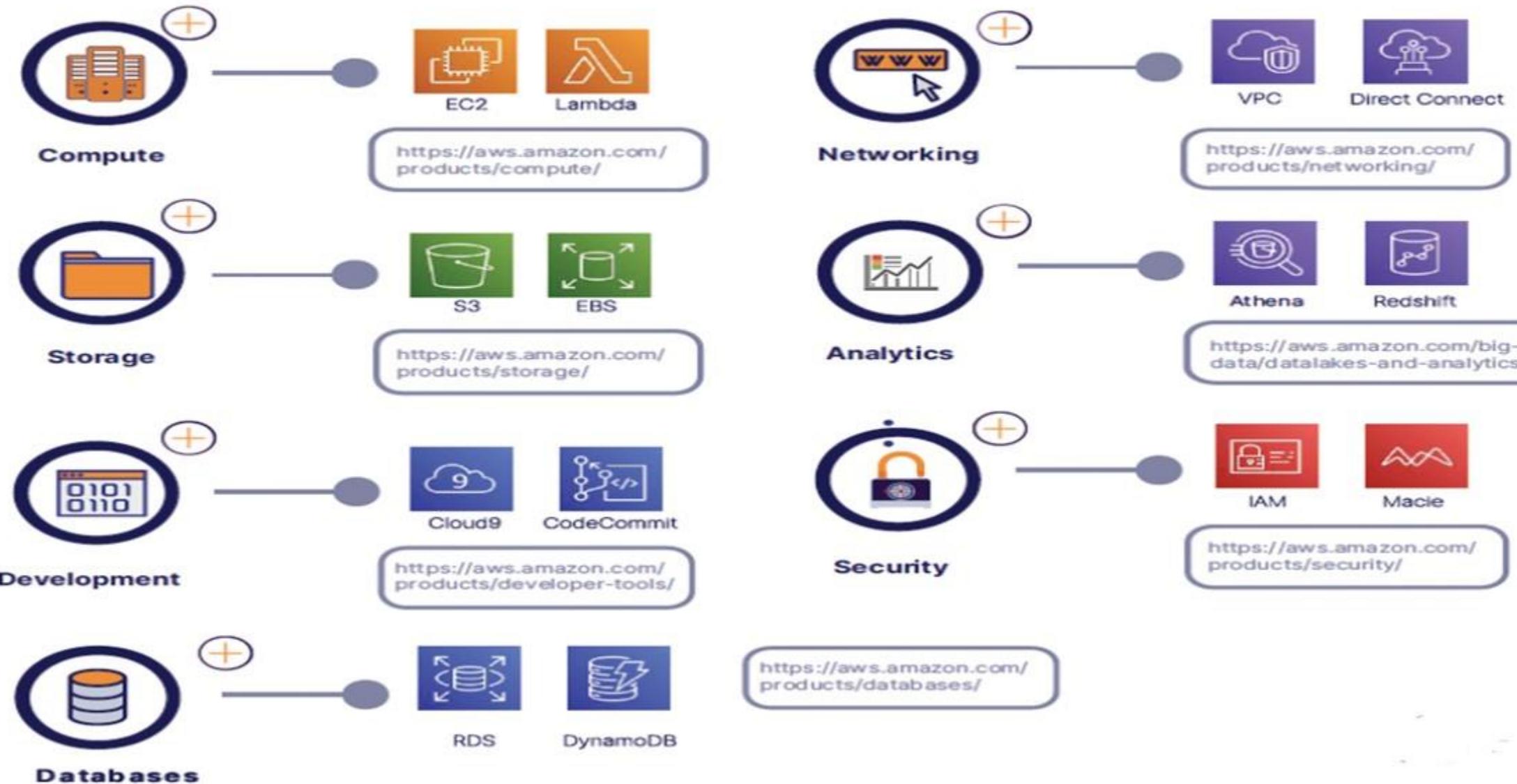
## Data Centers

Nhà cung cấp dịch vụ điện toán đám mây có những trung tâm dữ liệu, là nơi cung cấp hàng nghìn máy chủ (Servers), luôn sẵn sàng cho người dùng sử dụng qua Internet.



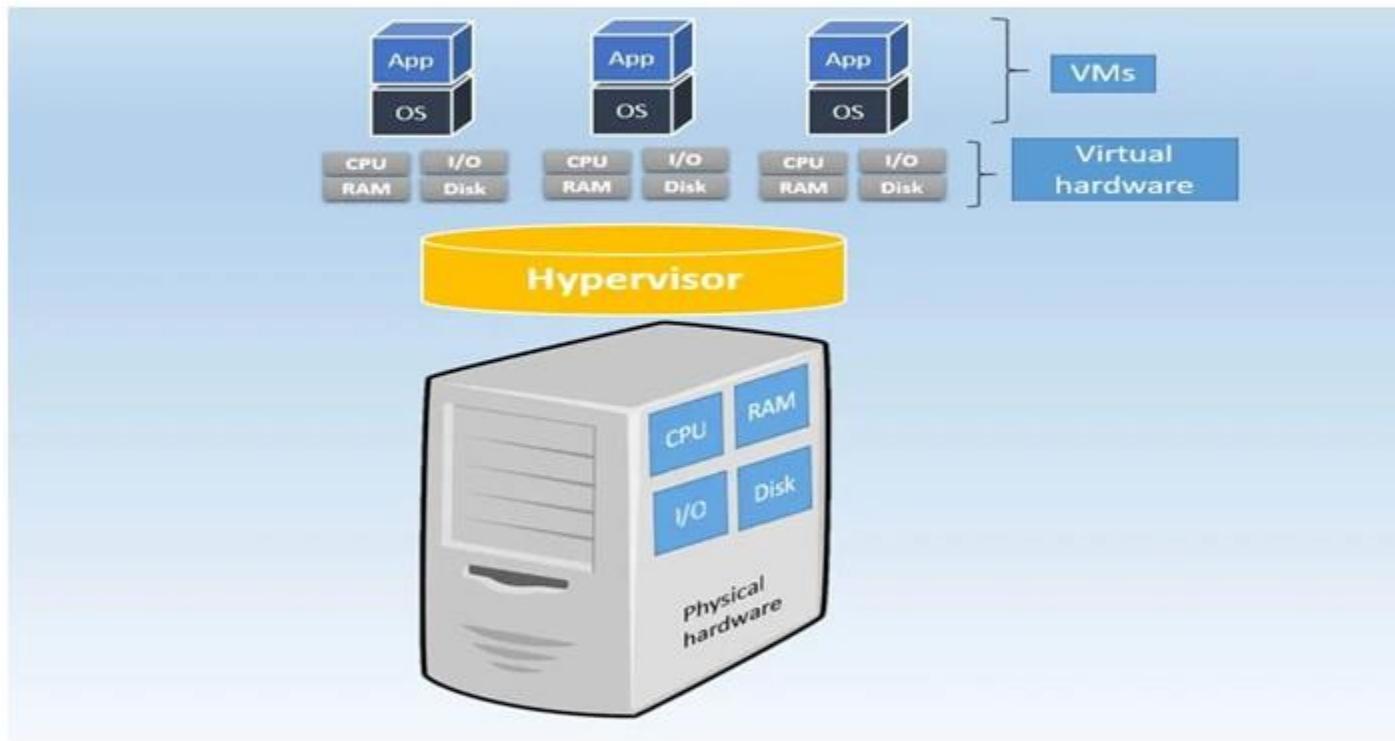


# Điện toán đám mây cung cấp nhiều dịch vụ CNTT qua internet. Mô tả chi tiết ở dưới về các dịch vụ AWS cung cấp



# Dịch vụ ảo hóa

Dịch vụ ảo hóa là dịch vụ chia các tài nguyên phần cứng trong một máy chủ vật lý, thành nhiều đơn vị nhỏ hơn cho nhiều máy chủ ảo



**Trong sử dụng tài nguyên AWS, bạn chỉ phải trả tiền cho dịch vụ khi bạn sử dụng nó:**

- 1) On demand: Không cam kết trả phí cho dịch vụ dài hạn từ 1-3 năm (No long-term commitments or upfront payments)
- 2) Pay as You Go: Bạn chỉ phải trả phí cho phí cho máy chủ ảo(dịch vụ) tính theo phút, giờ. Dùng bao nhiêu trả bấy nhiêu

# **Khám phá các lợi thế của điện toán đám mây**



# Có 6 lợi thế khi sử dụng điện toán đám mây (Cloud Computing)

- 1) Làm việc trên ứng dụng mọi lúc, mọi nơi khi có Internet(Go global in minutes): Bạn có thể triển khai các ứng dụng trên Internet nhanh chỉ bằng một click chuột.
- 2) Bạn không phải tốn chi phí để mua sắm, và bảo trì máy chủ. Do đó giúp bạn tập trung vào công việc, thay vì quan tâm đến bảo trì hệ thống mạng, máy chủ.
- 3) Lợi ích kinh tế từ quy mô lớn của đám mây: Giảm giá số lượng lớn được chuyển cho bạn, cung cấp mức trả thấp hơn khi bạn tiếp tục sử dụng dịch vụ
- 4) Tăng tốc độ và linh hoạt: Các nhà cung cấp dịch vụ điện toán đám mây cho phép bạn cài tiến và phân phối ứng dụng của bạn đến người dùng nhanh và mạnh mẽ hơn
- 5) Không phải quan tâm đến dung lượng phần cứng, như phải mua sắm thêm máy chủ, ổ cứng, ram, phân cứng cho hệ thống mạng
- 6) Tiết kiệm chi phí và thời gian: Bạn chỉ trả tiền cho những dịch vụ mà bạn sử dụng, thay vì đầu tư trả trước cho những gì không sử dụng đến

**Khi một công ty nghĩ đến việc sử dụng điện toán  
đám mây, cho các dịch vụ CNTT**



# Bạn có biết có nhiều lợi ích của điện toán đám mây?

- 1) Tính sẵn sàng(High Availability): Những hệ thống có tính sẵn sàng cao được thiết kế để hoạt động cung cấp các tài nguyên ra ngoài Internet mà không xảy ra lỗi dịch vụ. Nó tránh được lỗi gián đoạn dịch vụ bằng cách sử dụng hệ thống dự phòng, và quản trị lỗi.
- 2) Với elasticity khả năng co dãn linh hoạt. Dịch vụ cloud cho phép người dùng chủ động nâng cấp hoặc giảm lượng tài nguyên cần sử dụng.
- 3) Tính Linh hoạt(Agility): Cloud tăng tốc nhanh sự cải tiến các ứng dụng CNTT. Giúp bạn đưa sản phẩm của bạn đến với thị trường nhanh hơn
- 4) Tính bền vững(Durability): Tính bền vững là tất cả về dữ liệu được bảo vệ trong thời gian dài. Có nghĩa là dữ liệu của bạn sẽ được lưu trữ trong hệ thống cloud mà không bị lỗi hay hư hại

# Tổng quan về điện toán đám mây và các mô hình triển khai

## Tổng quan chung bài học



**Các mô hình điện toán đám mây  
( Cloud Computing Models)**

**Các mô hình triển khai  
điện toán đám mây  
( Cloud Deployment Models)**

**Tổng kết**

# Các mô hình điện toán đám mây ( Cloud Computing Models)

## 1) Mô hình dịch vụ Điện toán đám mây-Infrastructure as a service (IaaS):

- ✓ Cung cấp, cho thuê các khối hạ tầng mạng, máy chủ, và lưu trữ dữ liệu
- ✓ Cung cấp dịch vụ Webhosting cho người thuê chạy các trang web trả tiền theo tháng

## 2) Mô hình phần mềm dạng dịch vụ - Software as a Service (SaaS)

- ✓ Sử dụng các ứng dụng phần mềm trên nền tảng Web, cung cấp cho người dùng thuê
- ✓ SaaS là những ứng dụng email cá nhân mà chúng ta đang sử dụng

## 3) Mô hình Nền tảng như một dịch vụ - Platform as a Service (PaaS)

- ✓ Cung cấp các nền tảng (phần cứng, phần mềm, kết nối mạng...) cho phép người dùng tự phát triển và triển khai các ứng dụng riêng của mình trên đó qua mạng Internet. Do đó người sử dụng không phải lo lắng đến hạ tầng mạng và máy chủ.
- ✓ Các trang web ứng dụng bán hàng được xây dựng trên nền tảng PaaS

# Có 3 mô hình triển khai điện toán đám mây phổ biến nhất

1

## Private Cloud



INTERNAL DATABASES



LOCAL NETWORK

- 1) Phục vụ cho một công ty hay một tổ chức
- 2) Được vận hành trong trung tâm dữ liệu nội bộ(internal data center)
- 3) Không có các lợi thế như các nhà cung cấp dịch vụ điện toán đám mây

# Có 3 mô hình triển khai điện toán đám mây phổ biến nhất



- 1) Được cung cấp bởi AWS
- 2) Bạn không phải chịu trách nhiệm hay quan tâm đến phần cứng
- 3) Cung cấp tất cả các lợi thế của dịch vụ điện toán đám mây

Có 3 mô hình triển khai điện toán  
đám mây phổ biến nhất

### 3

### Hybrid Cloud

A hybrid cloud is a combination  
of public and private clouds.



- 1) Ví dụ kiến trúc cho một giải pháp Hybrid Cloud
- 2) Dữ liệu cực kỳ nhạy cảm và bảo mật được lưu tại mạng nội bộ
- 3) Ứng dụng Web được chạy trên nền tảng hạ tầng AWS
- 4) AWS cung cấp những công cụ do đó hai bên có thể nói chuyện với nhau

# Tổng kết

Có 3 mô hình (Models)

Triển khai (Deployment)

1

Mô hình dịch vụ  
Điện toán đám mây  
Infrastructure as a  
service (IaaS):

2

Mô hình phần mềm  
dạng dịch vụ  
Software as a Service  
(SaaS)

3

Mô hình Nền tảng như  
một dịch vụ -  
Platform as a  
Service(PaaS)

1) Private Cloud

2) Public Cloud

3) Hybrid Cloud

# Tìm hiểu về cơ sở hạ tầng toàn cầu AWS

## Tổng quan chung bài học



Vùng miền, quốc gia  
(regions)

Khu vực trung tâm dữ liệu  
(availability zone)

Các địa điểm đặt/thuê  
trung tâm dữ liệu  
(Edge Locations)

Tổng kết

# Vùng miền, Quốc gia (Regions)

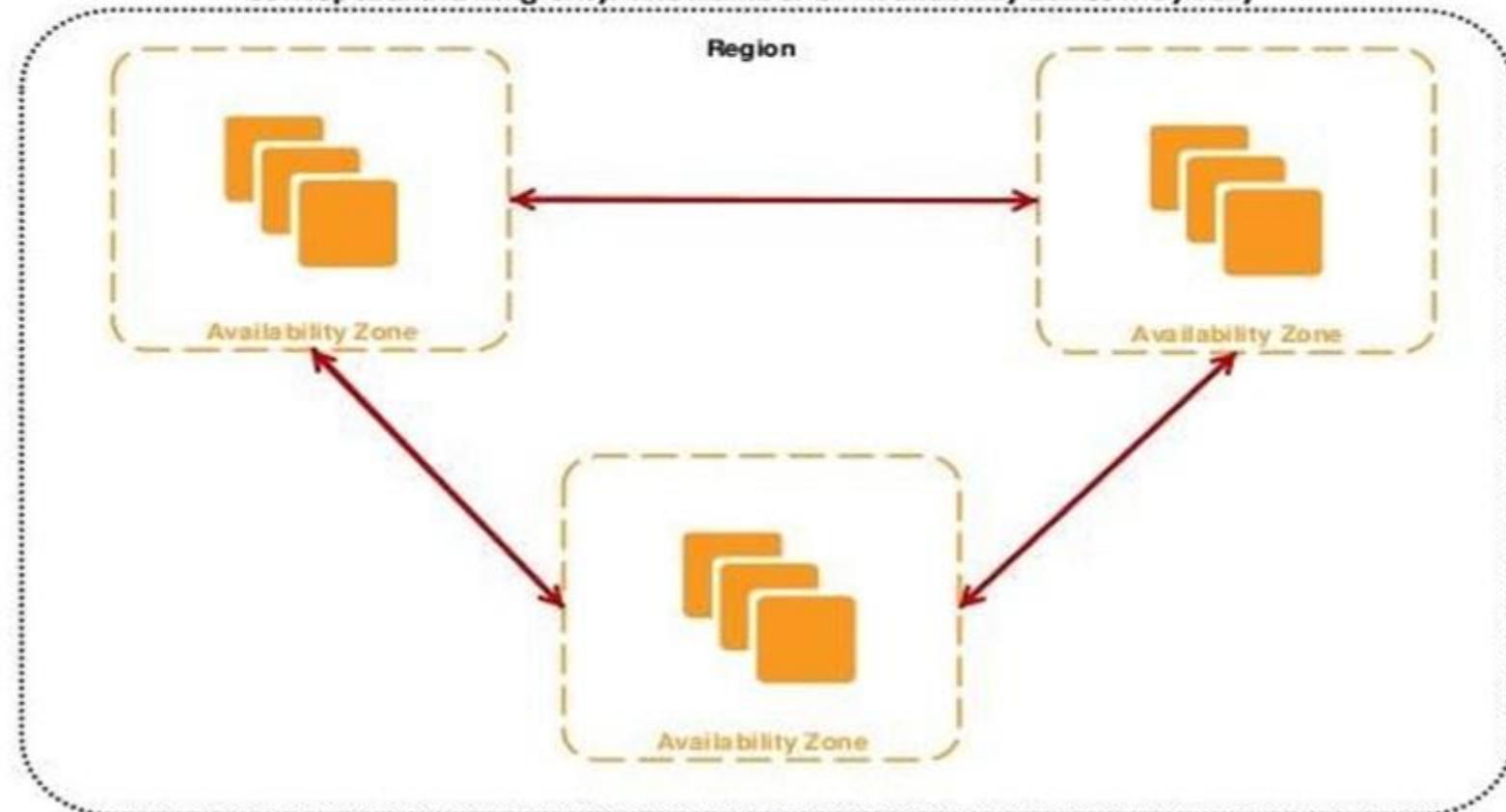
- Một vùng miền là một khu vực các quốc gia, nơi mà AWS xây dựng hạ tầng mạng vật lý, các Data Centers của họ ở đó.
- Mỗi region là độc lập với các region khác về mặt cơ sở hạ tầng như khu vực, hệ thống điện, hệ thống cung cấp nước...
- AWS hiện có 27 regions tại khắp các Quốc Gia, lãnh thổ trên toàn cầu.



Trong mỗi region chứa các khu vực khả dụng (availability zone - AZ).

## AWS Regions and Availability Zones

Conceptual drawing only. The number of Availability Zones may vary

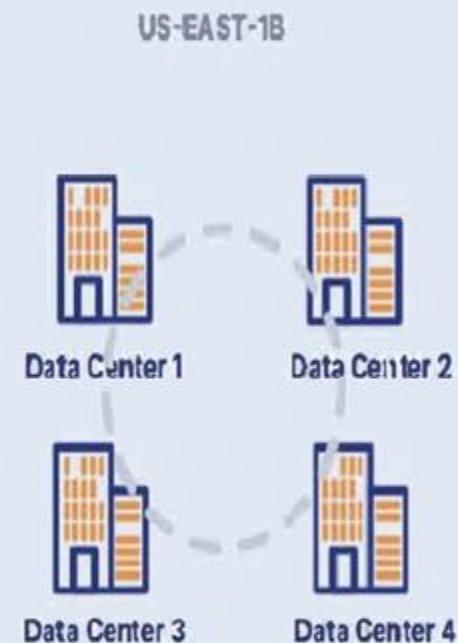


# Khu vực trung tâm dữ liệu (Availability Zone)

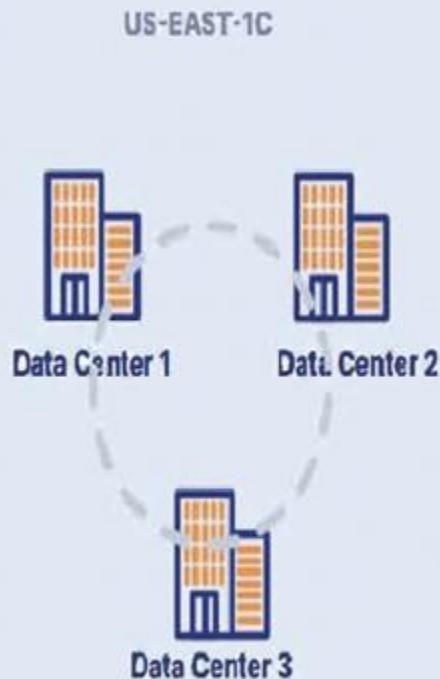
- ❖ Khu vực trung tâm dữ liệu - Availability Zone(AZ) bao gồm một hay nhiều khu vực vùng địa lý, với các trung tâm dữ liệu(Data Centers) tách biệt.
- ❖ Mỗi Data Center có nguồn điện, mạng và kết nối dự phòng và riêng biệt, để giảm khả năng hai khu vực bị lỗi đồng thời. Mỗi Availability Zone sẽ được hỗ trợ bởi nhiều data center vật lý, Có những availability zone lớn được hỗ trợ bởi nhiều data center.



## Availability Zone B



## Availability Zone C



### Các đặc điểm của Azs

- Hệ thống hạ tầng mạng riêng biệt
- Kết nối mạng tốc độ cao
- Được thiết kế với khả năng chịu lỗi
- Có tính sẵn sàng cao

## Các địa điểm đặt/thuê trung tâm dữ liệu (Edge Locations)

Là các vị trí trung gian, lưu trữ và nhận yêu cầu (request) từ người dùng, giúp tăng tốc trong việc xử lý thông tin cho hệ thống AWS.



# Tổng kết

## 1) Vùng miền, quốc gia (regions)

Region là một khu vực địa lý trên thế giới, nó bao gồm các Azs (các trung tâm dữ liệu Data Centers)

- ✓ Một region là một tập hợp các Azs
- ✓ Bạn nên cài đặt các tài nguyên trong các AWS Regions gần nhất với Quốc Gia của bạn
- ✓ Hầu hết các tài nguyên được ràng buộc với một Region cụ thể

## 2) Khu vực trung tâm dữ liệu(availability zone)

Một AZ là một tập hợp của một hoặc nhiều trung tâm dữ liệu (Data Centers)

- ✓ Một AZ có nhiều máy chủ (Servers) mà bạn sẽ thuê để sử dụng, dùng để triển khai các ứng dụng của bạn
- ✓ Một AZ được gán với một Region độc lập

## 3) Các địa điểm đặt/thuê trung tâm dữ liệu (Edge Locations)

- ✓ Một Edge Location được sử dụng để làm bộ nhớ đệm (cache) chứa nội dung dữ liệu, cho tăng tốc độ phân phối trong truy cập thông tin
- ✓ Được sử dụng cho các ứng dụng Content Delivery network(CDN), và Amazon CloudFront
- ✓ Giảm tốc độ xử lý trong kết nối mạng internet (Reduced latency )
- ✓ Một Edge Location là giống như một trung tâm dữ liệu (Data Center) mini, Nhưng nó không chạy như trung tâm dữ liệu

# Tìm hiểu bên trong tài khoản Amazon Web Services

## Tổng quan chung bài học



# AWS Management Console

**AWS management Console cho phép bạn truy cập tài khoản AWS của bạn và quản lý các ứng dụng đang chạy trong tài khoản của bạn từ trình duyệt Web( Web browser)**

**1** Người mới



Nếu bạn mới tham gia  
Vào cloud, và muốn thử  
Nghiệm với 1 số dịch vụ trong ánh, và làm các nghề khác  
cloud. AWS management  
console là nơi để bạn bắt đầu

**2** Người không biết  
kỹ thuật

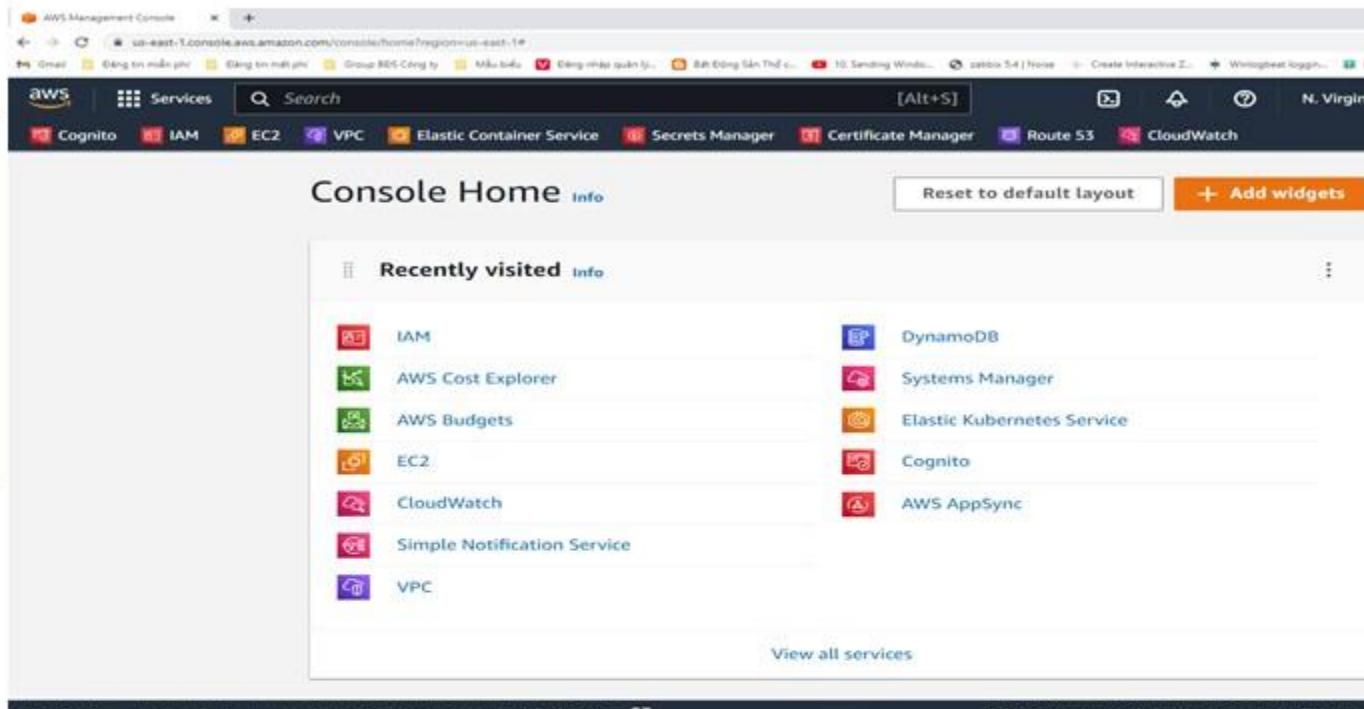


Nếu bạn là nhân viên: phân  
tích kinh doanh, quản trị dự  
nghiệp với 1 số dịch vụ trong ánh, và làm các nghề khác  
cloud. AWS management

**3** Nhân viên kỹ thuật



Nếu bạn làm nhân viên kỹ  
thuật như:  
Kỹ sư phần mềm, lập trình  
web, kỹ sư thiết kế giải pháp,  
và là kỹ sư kỹ thuật khác.



**AWS management Console cho phép  
người dùng dễ dàng tìm kiếm các dịch  
vụ (services)**

## Root User

Bạn có biết root user được tự động tạo ra trong lần đầu bạn đăng ký tài khoản trong AWS?

## Root User

Được bảo vệ sử dụng phương thức xác thực đa lớp multi-factor authentication (MFA)



# AWS Command Line Interface (CLI)

**AWS Command Line Interface (CLI) là giao diện dòng lệnh, nó cho phép bạn truy cập tài khoản AWS của bạn qua một thiết bị đầu cuối hoặc một cửa sổ lệnh.**

## 1 Giao diện dòng lệnh



CLI cho phép bạn quản lý Các dịch vụ AWS từ thiết bị đầu cuối trong Laptop của bạn

## 2 Code ứng dụng



Các dịch vụ AWS có thể được truy cập từ code ứng dụng sử dụng công cụ phát triển phần mềm SDKs và gọi từ code lập trình.

## 3 Công cụ phát triển phần mềm (SDKs)



SDKs cho phép bạn truy cập Các dịch vụ AWS từ các ngôn ngữ lập trình phổ biến như Java, Python, C#, và một số ngôn ngữ khác.

```
Command Prompt - aws configure
Microsoft Windows [Version 10.0.18363.1198]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\colby>aws configure
AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [None]: us-east-1
Default output format [None]: json
```

**Thỉnh thoảng các tính năng mới được AWS thêm vào qua AWS CLI trước khi có trong AWS management console**

# Tổng kết

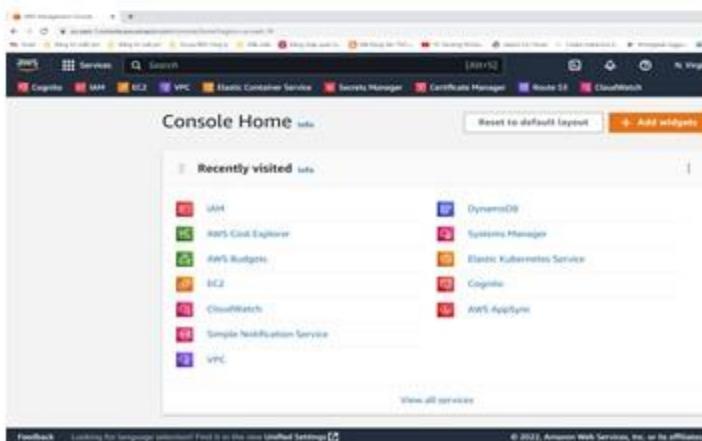
## Root Users

Root user được tự động tạo ra trong lần đầu bạn đăng ký tài khoản trong AWS.



### AWS Management Console

Cho phép người dùng truy cập dịch vụ AWS qua giao diện web



### AWS CLI

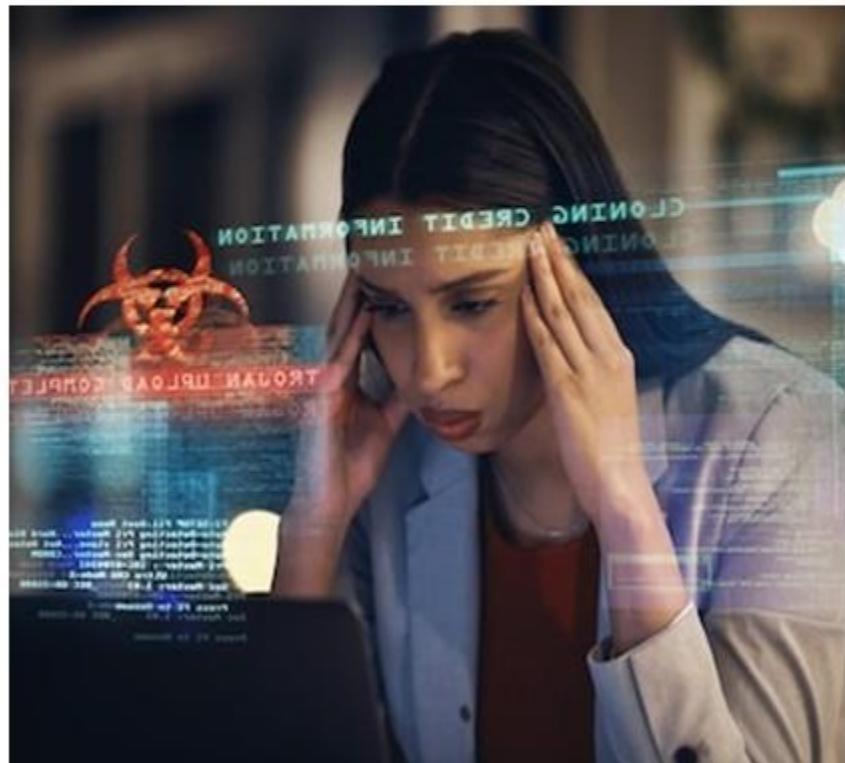
AWS Command Line Interface (CLI) là giao diện dòng lệnh, nó cho phép bạn truy cập tài khoản AWS của bạn qua một thiết bị đầu cuối hoặc một cửa sổ lệnh.

```
Command Prompt - aws configure
Microsoft Windows [Version 10.0.18363.1198]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\colby>aws configure
AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [None]: us-east-1
Default output format [None]: json
```

## PHẦN 2: Các công nghệ điện toán đám mây AWS

# Giới thiệu tổng quan



## Các dịch vụ (Services) AWS

Chúng ta sẽ học nhiều dịch vụ trong phần 2 này

Bạn có thể cảm thấy giống như  
đang đi vào khu rừng vậy. Nó  
làm bạn khó thở và bối rối.  
Nhưng không sao tôi sẽ giúp  
bạn!!!

## Compute



### EC2

EC2 allows you to rent and manage virtual servers in the cloud.



### Lambda

Lambda is a serverless compute service that lets you run code without managing servers.



### Fargate

Fargate is a serverless compute engine for containers.



### Lightsail

Lightsail allows you to quickly launch all the resources you need for small projects.



### Outposts

Outposts allows you to run cloud services in your internal data center.



### Batch

Batch allows you to process large workloads in smaller chunks (or batches).

## Storage



### S3

S3 is an object storage service for the cloud that is highly available.



### EBS

EBS is a storage device (called a volume) that can be attached to (or removed from) your instance.



### EFS

EFS is a serverless network file system for sharing files.



### Storage Gateway

Storage Gateway is a hybrid storage service.

## Content Delivery



### CloudFront

CloudFront is a CDN that delivers data and applications globally with low latency.



### Global Accelerator

Global Accelerator sends your users through the AWS global network when accessing your content, speeding up delivery.



### S3 Transfer Acceleration

S3 Transfer Acceleration improves content uploads and downloads to and from S3 buckets.

## Networking



### Route 53

Route 53 is a DNS service that routes users to applications.



### Virtual Private Cloud (VPC)

VPC is a foundational service that allows you to create a secure private network in the AWS Cloud where you launch your resources.



### Direct Connect

Direct Connect is a dedicated physical network connection from your on-premises data center to AWS.



### Virtual Private Network (VPN)

Site-to-Site VPN creates a secure connection between your internal networks and your AWS VPCs.

## Databases



### Relational Database Service (RDS)

RDS is a service that makes it easy to launch and manage relational databases.



### Aurora

Aurora is a relational database compatible with MySQL and PostgreSQL that was created by AWS.



### DynamoDB

DynamoDB is a fully managed NoSQL key-value and document database.



### DocumentDB

DocumentDB is a fully managed document database that supports MongoDB.



### ElastiCache

ElastiCache is a fully managed in-memory datastore compatible with Redis or Memcached.



### Neptune

Neptune is a fully managed graph database that supports highly connected datasets.

## Migration and Transfer



### Database Migration Service (DMS)

DMS helps you migrate databases to or within AWS.



### Server Migration Service (SMS)

SMS allows you to migrate on-premises servers to AWS.



### Snow Family

The Snow Family allows you to transfer large amounts of on-premises data to AWS using a physical device.



### DataSync

DataSync allows for online data transfer from on-premises to AWS storage services like S3 or EFS.

## Analytics



### Redshift

Redshift is a scalable data warehouse solution.



### Athena

Athena is a query service for Amazon S3.



### Glue

Glue prepares your data for analytics.



### Kinesis

Kinesis allows you to analyze data and video streams in real time.



### Elastic MapReduce (EMR)

EMR helps you process large amounts of data.



### Data Pipeline

Data Pipeline helps you move data between compute and storage services running either on AWS or on-premises.

## Machine Learning



### Rekognition

Rekognition allows you to automate your image and video analysis.



### Comprehend

Comprehend is a natural-language processing (NLP) service that finds relationships in text.



### Polly

Polly turns text into speech.



### SageMaker

SageMaker helps you build, train, and deploy machine learning models quickly.



### Translate

Translate provides language translation.



### Lex

Lex helps you build conversational interfaces like chatbots.

## Developer Tools



### Cloud9

Cloud9 allows you to write code within an integrated development environment (IDE) from within your web browser.



### CodeCommit

CodeCommit is a source control system for private Git repositories.



### CodeBuild

CodeBuild allows you to build and test your application source code.



### CodeDeploy

CodeDeploy manages the deployment of code to compute services in the cloud or on-premises.



### CodePipeline

CodePipeline automates the software release process.



### X-Ray

X-Ray helps you debug production applications.

## Deployment and Infrastructure Management



### CloudFormation

CloudFormation allows you to provision AWS resources using Infrastructure as Code (IaC).



### Elastic Beanstalk

Elastic Beanstalk allows you to deploy your web applications and web services to AWS.



### OpsWorks

OpsWorks allows you to use Chef or Puppet to automate the configuration of your servers and deploy code.

## Messaging and Integration



### Simple Queue Service (SQS)

SQS is a message queuing service that allows you to build loosely coupled systems.



### Simple Notification Service (SNS)

SNS allows you to send emails and text messages from your applications.



### Simple Email Service (SES)

SES is an email service that allows you to send richly formatted HTML emails from your applications.

## Auditing, Monitoring, and Logging



### CloudWatch

CloudWatch is a collection of services that help you monitor and observe your cloud resources.



### CloudTrail

CloudTrail tracks user activity and API calls within your account.

# Khám phá và tìm hiểu dịch vụ máy chủ ảo EC2

## Tổng quan chung bài học

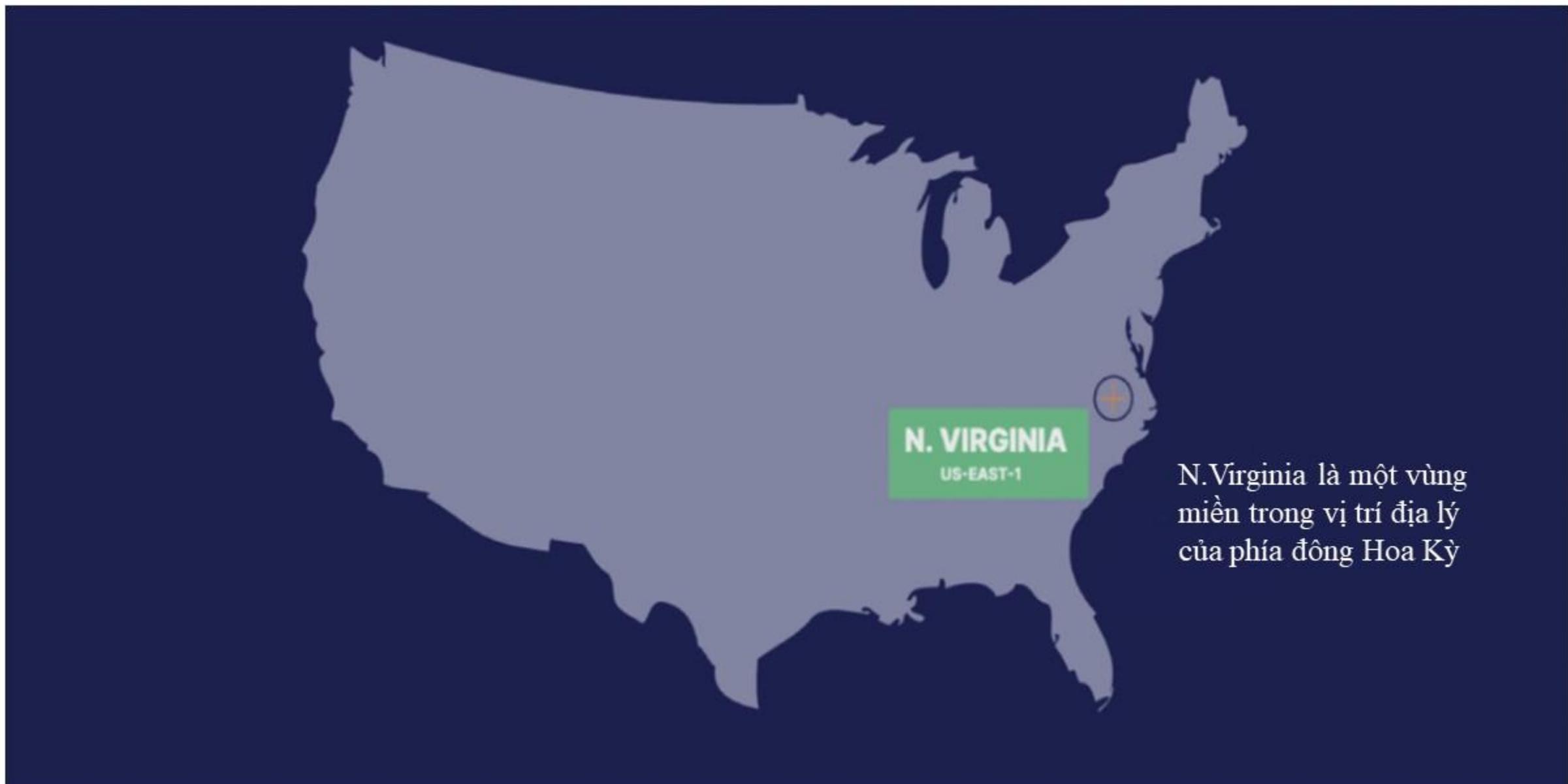


Máy chủ ảo Elastic Computer Cloud (EC2)

Dịch vụ EC2 cho phép bạn thuê và quản lý các máy chủ ảo trong cloud



# Tổng quan chung về Amazon EC2



N.Virginia là một vùng  
miền trong vị trí địa lý  
của phía đông Hoa Kỳ

1

## Vùng miền Region

Một vùng miền có  
nhiều AZs

2

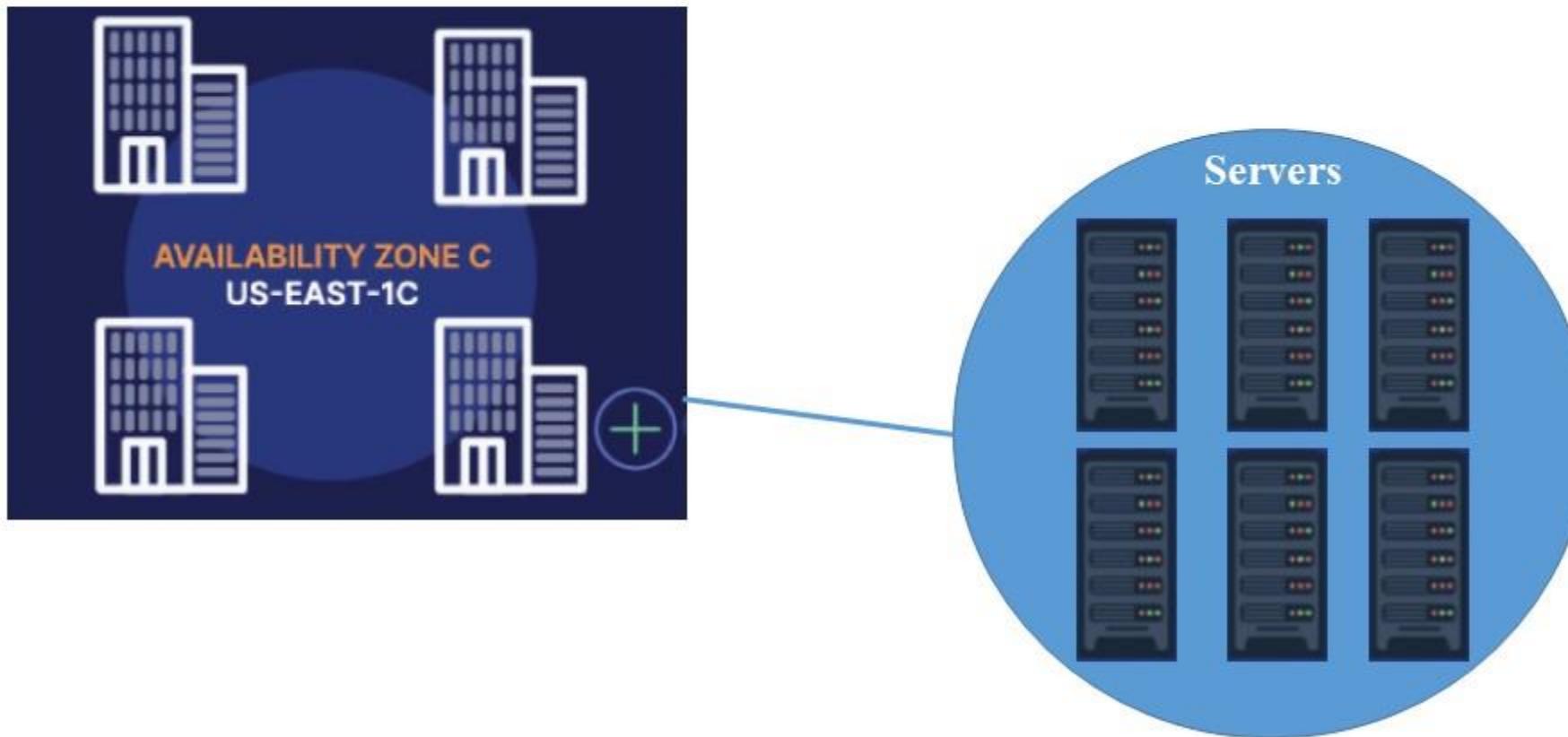
## Khu vực trung tâm dữ liệu Availability Zone (AZ)

Một khu vực trung tâm dữ liệu(AZ)  
có nhiều trung tâm dữ liệu

3

## Trung tâm dữ liệu Data Center

Một trung tâm dữ liệu có  
nhiều máy chủ Servers



- ❑ Máy chủ (Servers) là máy chủ vật lý chạy trong Data Center
- ❑ EC2 instances là các máy chủ chạy trong những máy chủ vật lý này.

# Một cái nhìn gần hơn về EC2

EC2 là một dịch vụ căn bản được sử dụng trong việc quản lý các máy chủ ảo hóa

**1**

Bạn có thể cài đặt một máy chủ ảo hóa EC2 chỉ bằng cái click chuột

**2**

Bạn có thể sử dụng một mẫu cấu hình có sẵn, gọi là một Amazon Machine Learning (AMI) để cài đặt, và tạo một máy chủ EC2

**3**

Bạn có thể triển khai cài đặt các ứng dụng, ngay trong khi khởi tạo, cài đặt EC2

**4**

Bạn có thể nhận 750 giờ /tháng miễn phí sử dụng EC2, trong tài khoản AWS Free tier plan.  
Được tạo tại trang web:  
<https://aws.amazon.com/vi/free/>

# EC2 trong ứng dụng thực tế

1

**Triển khai cài đặt một máy chủ cơ sở dữ liệu(database)**

- ✓ Cài đặt một máy chủ EC2 cho phép bạn toàn quyền kiểm soát cơ sở dữ liệu database server

2

**Triển khai cài đặt một máy chủ chạy ứng dụng Web**

- ✓ Có thể cài đặt một máy chủ chạy ứng dụng Web với tính sẵn sàng chịu lỗi cao, trong nhiều khu vực trung tâm dữ liệu (Azs)

# Các phương pháp truy cập vào một EC2 Instance

## Có một vài cách để truy cập vào EC2 Instances



### AWS Management Console

Bạn có thể truy cập, cấu hình và quản trị các máy chủ (instances), sử dụng giao diện Web browser



### Secure Shell (SSH)

SSH cho phép bạn thiết đặt một kết nối bảo mật (secure connection) với máy chủ (instance), từ máy tính & Laptop của bạn



### EC2 Instance Connect (EIC)

EIC cho phép bạn sử dụng các chính sách IAM (IAM policies) để kiểm soát SSH, truy cập đến các máy chủ của bạn (instances), mà không cần yêu cầu phải có SSH keys



### AWS Systems Manager

System Manager cho phép bạn truy cập và quản lý Các máy chủ EC2 instances, bằng cách sử dụng Giao diện web browser hoặc công cụ giao diện dòng lệnh AWS CLI

Cách phổ biến để truy cập đến máy chủ ảo EC2 chạy hệ điều hành Linux, là sử dụng Secure Shell (SSH).



# Các lựa chọn giá, chi phí cho EC2 (EC2 Pricing Options)

Có một vài lựa chọn chi phí, giá để lựa chọn cho EC2 instances

Sử dụng bao nhiêu trả tiền bấy nhiêu (ON- Demand)

- ✓ Mức giá được tính tiền sử dụng máy chủ ảo (Instances) theo phút, giờ sử dụng, dựa trên kiểu Instance. Người dùng không cần phải có hợp đồng với Amazon

**Trường hợp sử dụng On-Demand khi:**

- 1) Bạn quan tâm đến chi phí thấp, mà không cần để ý đến các hình thức trả giá dịch vụ theo hình thức upfront Payment và long-term commitment
- 2) Các ứng dụng của bạn có khối lượng công việc ngắn hạn, hoặc không thể đoán trước, và máy chủ ảo được chạy xuyên suốt và không bị gián đoạn
- 3) Các ứng dụng trong máy ảo đang trong giai đoạn chạy thử nghiệm và phát triển
- 4) Máy chủ thường chạy theo thời vụ và dưới 1 năm

# Spot Instances

- Spot instances để cho bạn có được lợi thế sử dụng lượng những máy chủ ảo EC2 dư thừa, không sử dụng đến. Để sử dụng Spot instance, bạn phải yêu cầu (request) đến AWS, để họ xem có máy chủ ảo đang dư thừa hay không, sau đó cho phép bạn sử dụng.



EC2 Dashboard

Events

Tags

Reports

Limits

**INSTANCES**

- Instances
- Launch Templates
- Spot Requests**
- Reserved Instances
- Dedicated Hosts
- Scheduled Instances

**IMAGES**

- AMIs
- Bundle Tasks

Request Spot Instances

Spot Advisor

Actions ▾

Pricing History

Request type: all ▾ State: all ▾ Search by keyword

Request Id	Request type	Instance type	State	Capacity
------------	--------------	---------------	-------	----------

You currently have no Spot requests in the system.

If you are new to EC2 Spot instances, visit the [Getting Started guide](#).

Click the Request Spot Instances button to launch a request.

Request Spot Instances

Select a Spot request above to see more details

A screenshot of the AWS EC2 Spot Requests page. The left sidebar shows navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES (with Instances, Launch Templates, and Spot Requests highlighted), IMAGES (with AMIs and Bundle Tasks), and a large red circle around Spot Requests. The main content area has tabs for Request Spot Instances, Spot Advisor, Actions, and Pricing History (which is circled in red). Below these are filters for Request type and State, and a search bar. A table header for Request Id, Request type, Instance type, State, and Capacity is shown, followed by a message stating "You currently have no Spot requests in the system." A "Request Spot Instances" button is at the bottom.

## Các trường hợp sử dụng Spot Instances:

- 1) Bạn không quan tâm về quãng thời gian khi nào thì bắt đầu có spot instance để chạy, và khi nào thì bị dừng máy chủ ảo
- 2) Máy chủ của bạn có thể bị gián đoạn trong một khoảng thời gian
- 3) Khi bạn chỉ có ngân sách cho việc chi tiêu cho thuê máy chủ với giá tính toán chi phí rất thấp
- 4) Bạn có thể tiết kiệm đến 90% chi phí
- 5) Bạn chỉ phải chi trả khi Instance spot đang trong trạng thái hoạt động

# Reserved Instances

- Reserved instance cho phép bạn cam kết sử dụng một kiểu instance type cụ thể, trong một vùng lãnh thổ (region) cụ thể (region), thời gian sử dụng từ 1 đến 3 năm

## Trường hợp sử dụng Reserved instance:

- 1) Máy chủ của bạn cần phải có tình trạng sử dụng ổn định, và bạn có thể cam kết sử dụng từ 1 đến 3 năm
- 2) Bạn có thể trả tiền trước (upfront) để nhận được giảm giá
- 3) Ứng dụng của bạn yêu cầu cần phải có một dung lượng, cấu hình dự trữ nhất định
- 4) bạn có thể tiết kiệm đến 75% chi phí
- 5) Bạn đòi hỏi phải ký hợp đồng với Amazon
- 6) Bạn có thể đặt trước dung lượng cấu hình của Instance trong một Availability Zone cụ thể
- 7) bạn có thể trả tiền theo hình thức: Trả tiền hết một lần (All Upfront), hoặc trả tiền một phần(Partial Upfront), hoặc chưa trả hết tiền ngay (No Upfront). Hình thức trả tiền hết một lần (All Upfront) sẽ được giảm giá cao nhất

# Dedicated Hosts

Dedicated Hosts cho phép bạn trả tiền cho một máy chủ vật lý, máy chủ này sẽ được dành để chạy toàn bộ các máy chủ ảo của bạn. Hoặc môi trường ứng dụng không hỗ trợ máy ảo và đòi hỏi phải có máy chủ vật lý

## **Trường hợp sử dụng Dedicated Hosts:**

- 1) Bạn muốn đưa máy chủ của bạn bao gồm các bản quyền phần mềm, như bản quyền sử dụng Windows, hay Oracle lên AWS
- 2) Bạn cần có những yêu cầu đòi hỏi phải có sự tuân thủ quy định của công ty về mô hình thuê máy chủ
- 3) Bạn có thể tiết kiệm đến 70% chi phí
- 4) Bạn có thể dịch chuyển toàn bộ hệ thống hiện có của bạn như cấu hình phần cứng, bản quyền phần mềm lên Dedicated Hosts
- 5) Không có multi-tenancy, có nghĩa là máy chủ không được chia sẻ với các khách hàng khác
- 6) Một Dedicated Host là một máy chủ vật lý, và một Dedicated instance chạy trên máy chủ vật lý này

# Kế hoạch tiết kiệm (Savings Plan)

- Kế hoạch tiết kiệm cho phép bạn cam kết sử dụng máy chủ từ 1 đến 3 năm (được đo lường theo giờ)
- **Trường hợp sử dụng Savings Plan như sau:**
  - 1) Bạn muốn trả phí thấp cho dịch vụ thuê nhiều máy chủ
  - 2) Bạn muốn sự mềm dẻo để thay đổi các dịch vụ máy chủ, kiểu cấu hình của máy chủ(Instance types), hệ điều hành, hoặc lãnh thổ quốc gia (regions)
  - 3) Bạn có thể tiết kiệm đến 72% chi phí
  - 4) Bạn sẽ không phải làm cam kết phải thuê Dedicated Host, mà chỉ là tính toán sử dụng dịch vụ sao cho hợp lý
  - 5) Tiết kiệm chi phí có thể được chia sẻ giữa nhiều dịch vụ compute như EC2, Fargate, và Lambda

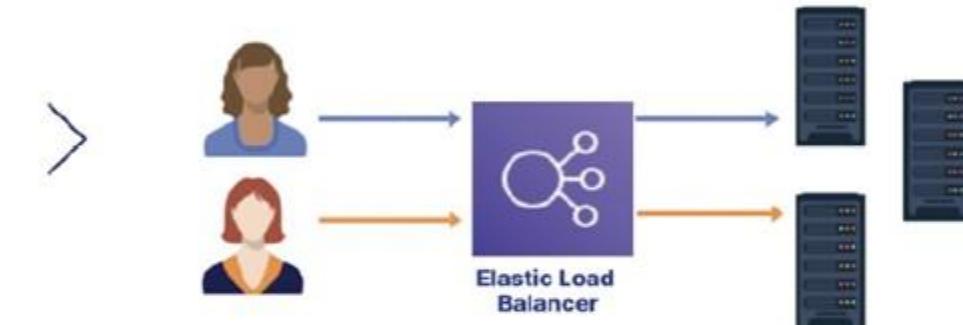
# Các tính năng trong sử dụng EC2

EC2 có tính năng cân bằng tải (load balancing) và tự động điều chỉnh quy mô (Auto Scaling)

1

Tính năng cân bằng tải(Elastic Load Balancing):

Tự động phân phối các luồng truy cập (incoming application traffic) của người dùng từ bên ngoài , đến các ứng dụng chạy trên các máy ảo. Cho các máy ảo EC2 Instances



CLASSIC LOAD BALANCERS | APPLICATION LOAD BALancers | GATEWAY LOAD BALANCERS | NETWORK LOAD BALANCERS

2

Tính năng tự động điều chỉnh quy mô (Auto Scaling):

Tính năng này sẽ tự động thêm vào, hoặc thay thế EC2 Instances giữa các vùng Azs. Dựa trên sự cần thiết và sự thay đổi theo nhu cầu về quy mô sử dụng.

Lưu ý: Chúng ta không được lầm lẫn giữa horizontal scaling với Vertical scaling (Scaling Up). **Horizontal Scaling** (scaling out) được dùng để nâng cấp thêm cấu hình như CPU, RAM, cho một EC2 instance đang chạy trong hệ thống



HORIZONTAL SCALING, HOẶC LÀ SCALING OUT

Tự động giảm sự ảnh hưởng của các lỗi hệ thống, và Tăng cường sự ổn định, tính sẵn sàng của ứng dụng chạy trên máy chủ EC2

# TỔNG KẾT

EC2 Instance

Sự kết nối  
(Connectivity)

Các lựa chọn chi phí  
(Pricing Options)

Các tính năng  
(Features)

## EC2 Instance:

EC2 cho phép bạn thuê và quản trị các máy chủ ảo trong đám mây. AWS virtual servers được gọi là Instances

### Sự kết nối(Connectivity)

Có nhiều cách để truy cập vào máy chủ EC2 instance.

- |                           |                       |
|---------------------------|-----------------------|
| 1) AWS Management Console | 2) Secure Shell(SSH)  |
| 3) EC2 Instance Connect   | 4) AWS System Manager |

### Các lựa chọn chi phí (Pricing Options)

- 1) On-demand
- 2) Spot
- 3) Reserved Instances
- 4) Dedicated Hosts
- 5) Saving Plans

### Các tính năng trong sử dụng EC2 (Features)

**1) Tự động phân phối các luồng truy cập**  
(incoming application traffic) của người dùng từ bên ngoài , đến các ứng dụng chạy trên các máy ảo. Cho các máy ảo EC2 Instances

### 2) Tính năng tự động điều chỉnh quy mô (Auto Scaling):

Tính năng này sẽ tự động thêm vào hoặc thay thế EC2 Instances giữa các vùng Azs. Dựa trên sự cần thiết và sự thay đổi theo nhu cầu về quy mô sử dụng.

# Thực hành khởi tạo máy chủ ảo EC2



## Một ví dụ Demo tạo một máy chủ ảo EC2

Trong video này, bạn sẽ được xem về AWS Platform, và một vài cách để vào dịch vụ compute, để tạo EC2 Instance.

# Tìm hiểu dịch vụ Lambda

Tổng quan chung bài học



# AWS Lambda

- Lambda là dịch vụ compute service. Là môi trường, nền tảng thực thi ứng dụng và dịch vụ mà không cần phải quan tâm đến máy chủ.  
Bạn chạy code mà không cần phải quan tâm đến máy chủ Servers.
- 1) Bạn viết code cho ứng dụng, được gọi là functions. Sử dụng các ngôn ngữ phổ biến
  - 2) Lambda tự động điều chỉnh quy mô (Scales Automatically)
  - 3) Serverless có nghĩa là, bạn không phải lo lắng về việc quản lý máy chủ servers như là đối với máy chủ EC2

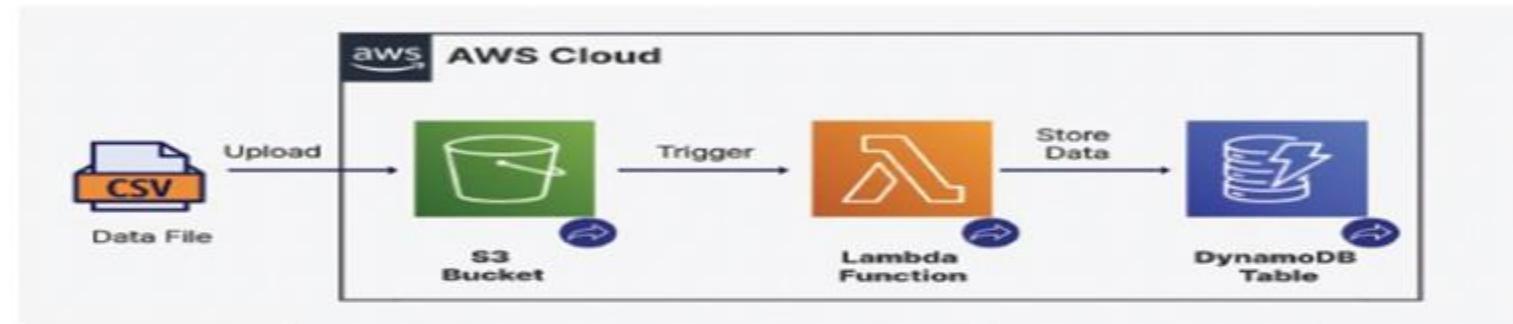


# Tổng quan về Lambda

- Lambda cho phép các kỹ sư phát triển phần mềm tập trung vào logic của cốt lõi kinh doanh của ứng dụng, mà họ sẽ phát triển thay vì lo lắng về vấn đề quản trị nhiều máy chủ (servers)

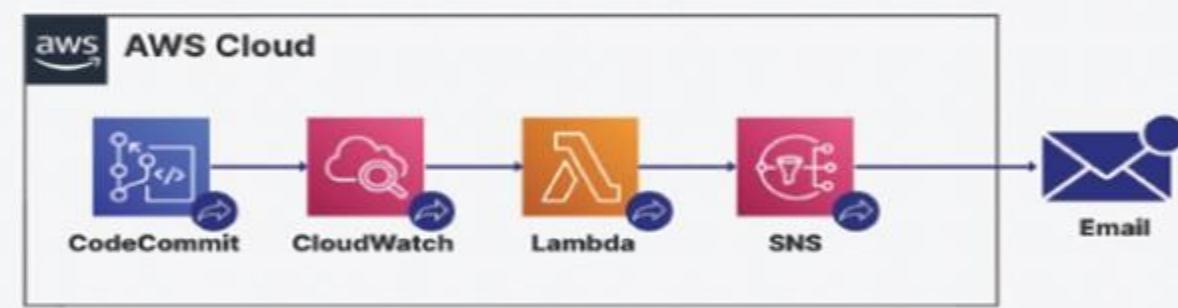
1

Xử lý file theo thời gian thực



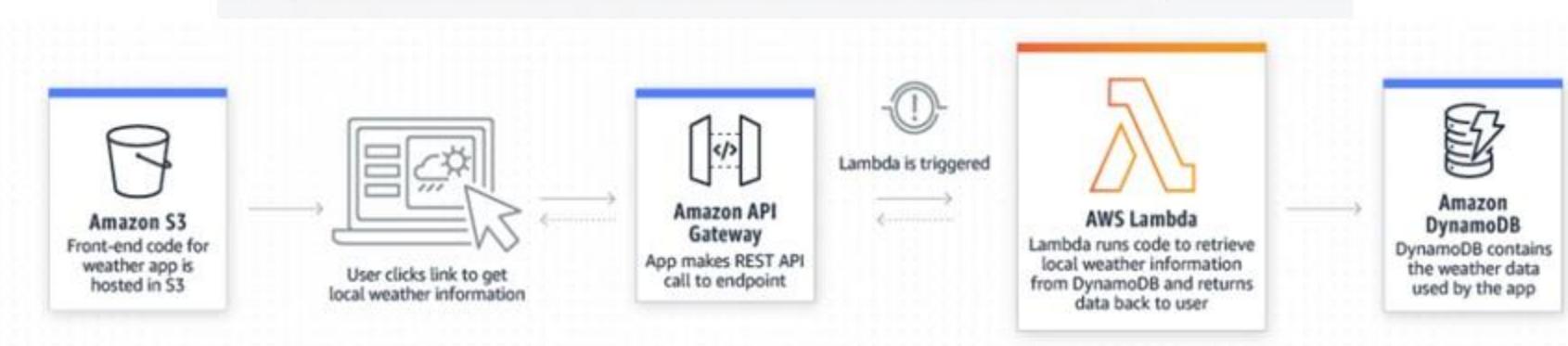
2

Gửi email thông báo



3

Ứng dụng Web



# Các tính năng (Features)

1

Hỗ trợ các ngôn ngữ lập trình phổ biến  
Như: Java, Go, PowerShell, Node.js, C#,  
Python, và Ruby

2

Bạn có thể viết code sử dụng môi trường  
Phát triển & ngôn ngữ lập trình mà bạn thích.  
Qua console trong Lambda

3

Lambda có thể thực thi code  
trong phản hồi đến các sự kiện

4

Lambda function có 15 phút timeout

# Mô hình chi phí (Pricing Model)

- Bạn được tính phí dựa trên cái quãng thời gian chạy, và số lượng yêu cầu truy cập ứng dụng (number of requests)

## 1) Thời gian tính toán(Compute time)

Chỉ trả tiền cho thời gian sử dụng, không tính phí nếu code ứng dụng không chạy

2) Đếm Request(Request count): Một request được đếm mỗi lần trong thời gian nó bắt đầu thực thi, kể cả test thử code ứng dụng.

## 3) Luôn miễn phí (Always free)

Cho phép 1 triệu free requests mỗi tháng (The free usage tier)

# Tổng kết

1) Lambda là một dịch vụ serverless compute service, nó cho phép bạn chạy code mà không cần quản trị máy chủ servers.

**2) Tính năng (Features):** Hỗ trợ môi trường code lập trình phát triển qua console.

**3) Chi phí (Pricing):**

Thời gian tính toán (Compute time)

Số lượng yêu cầu truy cập (Request count)

Luôn miễn phí (Always free)

# Thực hành tạo một chương trình Lambda với AWS Management Console



## Một ví dụ Demo tạo một chương trình Lambda

Trong video này, bạn sẽ tạo một chương trình Lambda sử dụng ngôn ngữ Python trong AWS console. Sau đó bạn sẽ kiểm tra logs của chương trình sau khi chạy xong trong dịch vụ Cloud Watch.



**Lambda**



**Cloud Watch**

# Các bước để tạo chương trình Lambda trong AWS console

- 1) Đăng nhập vào AWS Management Console của bạn.
- 2) Chuyển hướng vào dịch vụ Lambda
- 3) Click vào nút **Create Function**
- 4) Chọn mục tùy chọn “**Author from scratch**”
- 5) Trong mục: “**Function name:**”, nhập tên chương trình của bạn
- 6) Trong mục: “**Runtime:**”, lựa chọn phiên bản mới nhất của Python (Latest version of Python)
- 7) Mở rộng mục “**Change default execution role**” bằng cách click vào mũi tên , sau đó chọn: “ **Create a new role with basic Lambda permissions**”
- 8) Click vào nút: “**Create function**”
- 9) Sau khi cái Function được tạo, bạn di chuyển tới mục Code Tab
- 10) Bên dưới mục **Code Source**, lựa chọn lambda\_function.py
- 11) Thay đổi toàn bộ cái code ví dụ bằng code như dưới đây:

```
import json

def lambda_handler(event, context):
    message = 'Hello {} {}! Ban rat tuyet voi!'.format(event['Ho'], event['Ten'])

    #Ghi log den CloudWatch logs
    print(message)

    return {
        'message' : message
    }
```

- 12) Click vào nút **Deploy**.
- 13) Tạo 1 test event và thực thi Lambda: Lựa chọn nút “Test”, vào Select Test > Configure test event.
- 14) Cho mục Event name, nhập: mytest.
- 15) Trong mục Event JSON box, thay đổi cái sample code như sau: { "Ho": "Nhập họ ban o day", "Ten": "Nhập họ ban o day" }. Cập nhật code sử dụng họ tên của bạn.
- 16) Click vào Format JSON, Click vào Save, Click vào Test. Sau đó kết quả của chương trình chạy sẽ hiện ra
- 17) Xem logs trong CloudWatch bằng cách click vào “**View logs in CloudWatch**.”. Dưới mục log streams, bạn click vào cái nút “**most recent log stream**”. Và xem log của chương trình Lambda.

# Tìm hiểu các loại dịch vụ bổ sung có trong AWS

Tổng quan chung bài học



# AWS Fargate

Fargate là một Serverless compute engine cho việc chạy containers

- ✓ Fargate cho phép bạn quản lý, chạy các containers, như là Docker.
- ✓ Tự động tăng giảm quy mô (Scales automatically).



- ✓ Serverless có nghĩa là bạn, không cần quan tâm về cung cấp môi trường hệ điều hành, chạy ứng dụng, và cài đặt cấu hình các dịch vụ máy chủ. Hay mở rộng & nâng cấp cấu hình các máy chủ.

# Amazon Lightsail

Lightsail cho phép bạn nhanh chóng khởi tạo các tài nguyên bạn cần, cho các dự án nhỏ

- ✓ Triển khai các ứng dụng đã  
Được cấu hình, cài đặt  
sẵn nhanh, như là WordPress  
Websites, chỉ bằng click chuột
- ✓ Sử dụng giao diện quản trị đơn  
giản, dễ dàng. Cho người không  
có kinh nghiệm về điện toán đám mây



- ✓ Cung cấp máy chủ ảo, SSD căn bản, truyền và lưu trữ dữ liệu, chương trình quản trị DNS, và 1 IP internet tĩnh(public static IP)
- ✓ Chi phí thấp theo tháng, căn bản 3,50\$/1 máy chủ, 512 Mb Ram, CPU 1 nhân (Core), 20GB SSD, 1 TB băng thông

# AWS Outposts

Outposts cho phép bạn chạy các dịch vụ cloud trong trung tâm dữ liệu của bạn

- ✓ Hỗ trợ các dịch vụ cần phải có độ trễ (latency) mạng thấp, hoặc cần phải xử lý dữ liệu trong mạng nội bộ.
- ✓ AWS cung cấp và cài đặt các máy chủ ngay trong hệ thống trung tâm dữ liệu của bạn



- ✓ Sử dụng cho sự trải nghiệm hồn hợp(hybrid Experience) giữa mạng nội bộ và điện toán đám mây (cloud).
- ✓ Có thể truy cập đến các dịch vụ điện toán đám mây và các APIs của AWS, để phát triển các ứng dụng tại chỗ.

## AWS Batch

Batch cho phép bạn xử lý các tải trọng công việc lớn trong các thành phần nhỏ hơn



- ✓ Chạy hàng trăm, và hàng ngàn Batch để xử lý các công việc (jobs)

- ✓ Có thể biến đổi năng động cung cấp các instances dựa trên khối lượng volume

## Tổng kết

- 1) **Fargate:** Là một dịch vụ serverless compute engine cho container
- 2) **Lightsail :** Cho phép bạn nhanh chóng khởi tạo các tài nguyên bạn cần, cho các dự án nhỏ
- 3) **Outposts:** cho phép bạn chạy các dịch vụ cloud trong trung tâm dữ liệu của bạn
- 4) **Batch:** Cho phép bạn xử lý các tải trọng công việc lớn trong các thành phần nhỏ hơn

# Giới thiệu dịch vụ lưu trữ dữ liệu đơn giản S3

Tổng quan chung bài học



# Tổng quan về S3

Ngày nay, các công ty cần phải thu thập, lưu trữ, và phân tích các dữ liệu, mà họ đã tích lũy được qua năm tháng ở quy mô lớn. Các dịch vụ lưu trữ dữ liệu trong đám mây chính là nơi để các công ty lưu trữ dữ liệu.



# Khả năng truy cập dữ liệu (Data Accessibility)

Tính bền vững(Durability) và Tính sẵn sàng (Availability) là 2 yếu tố khác nhau của sự truy cập dữ liệu.

**1**

Tính bền vững



Tính bền vững rất quan trọng, do đó các dữ liệu phải không bao giờ bị mất, hoặc bị hư hỏng & bị đánh cắp

Amazon S3 Standard được thiết kế cho tính bền vững lên đến 99.99999999%

**2**

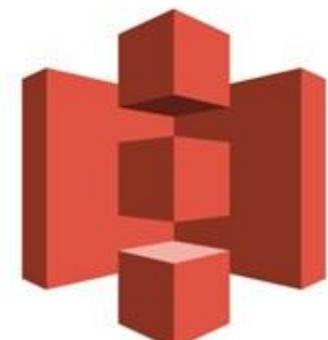
Tính sẵn sàng



Tính sẵn sàng rất quan trọng do đó bạn có thể truy cập dữ liệu của bạn nhanh, khi bạn cần đến nó

Amazon S3 Standard được thiết kế cho tính sẵn sàng lên đến 99.99%

# Các loại lưu trữ S3 (S3 Storage Classes)



Amazon S3

### 1) S3 Standard

- ✓ Mục đích nói chung là sử dụng để lưu trữ dữ liệu
- ✓ Dữ liệu được lưu trên nhiều vùng trung tâm dữ liệu để đảm bảo sự sẵn sàng.
- ✓ Có độ trễ thấp (low latency) và thông lượng cao (throughput).

**Tư vấn dùng cho trường hợp:** Thường xuyên truy cập dữ liệu

### 2) S3 Intelligent-Tiering

- ✓ Tự động giảm chi phí lưu trữ bằng cách chuyển dữ liệu của bạn sang bậc truy cập tiết kiệm chi phí nhất, dựa trên tần xuất truy cập mà không ảnh hưởng đến hiệu năng, chi phí truy xuất và vận hành.
- ✓ Tự động tiết kiệm chi phí
- ✓ Không tính phí truy xuất dữ liệu
- ✓ Dữ liệu được lưu trên nhiều vùng trung tâm dữ liệu để đảm bảo sự sẵn sàng.

**Tư vấn dùng cho trường hợp:** Dữ liệu không xác định, hoặc thay đổi cách thức truy cập

### 3) S3 Standard-Infrequent Access(IA)

- ✓ Dữ liệu ít truy cập thường xuyên, nhưng đòi hỏi tốc độ truy cập nhanh
- ✓ Dữ liệu được lưu trên nhiều vùng trung tâm dữ liệu để đảm bảo sự sẵn sàng.
- ✓ Chi phí sử dụng rẻ hơn S3 Standard

**Tư vấn dùng cho trường hợp:** Lưu trữ dữ liệu lâu dài, ít truy cập thường xuyên, truy cập dữ liệu tốc độ cao mức Millisecond khi cần

### 4) S3 One Zone-Infrequent Access(IA)

- ✓ Giống như S3 Standard-Infrequent Access(IA), nhưng data chỉ được lưu trong một vùng trung tâm dữ liệu
- ✓ Chi phí sử dụng rẻ hơn 20% S3 Standard-Infrequent (IA)
- ✓ Dữ liệu được lưu trong lớp lưu trữ dữ liệu có thể bị mất

**Tư vấn dùng cho trường hợp:** Có khả năng tạo lại dữ liệu, không cần truy cập thường xuyên với tốc độ truy cập dữ liệu theo milli giây, không quan trọng cần phải lưu dữ liệu với tính sẵn sàng và tính bền vững

### S3 Glacier

- ✓ Lưu trữ dữ liệu dài hạn và lưu trữ với giá thấp
- ✓ Khi truy xuất dữ liệu có dung lượng lớn thường phải mất một thời gian dài mới có thể truy xuất (trong 5-12 giờ)
- ✓ Có 3 khoảng thời gian cho lựa chọn truy xuất dữ liệu: 1-5 phút, 3-5 giờ, hoặc 5 đến 12 giờ
- ✓ Dữ liệu được lưu trên nhiều vùng trung tâm dữ liệu để đảm bảo sự sẵn sàng.

**Tư vấn dùng cho trường hợp:** Sao lưu (Backup) dữ liệu trong một thời gian dài. Dùng cho trường hợp lưu trữ dữ liệu giá rẻ

### S3 Glacier Deep Archive

- ✓ Giống với S3 Glacier, nhưng mất thời gian truy cập lấy dữ liệu lâu hơn
- ✓ Có 2 khoảng thời gian cho lựa chọn truy xuất dữ liệu: 12 giờ hoặc 48 giờ
- ✓ Rẻ nhất trong các lựa chọn lưu trữ S3
- ✓ Dữ liệu được lưu trên nhiều vùng trung tâm dữ liệu để đảm bảo sự sẵn sàng.

**Tư vấn dùng cho trường hợp:** Sao lưu (Backup) dữ liệu trong một thời gian dài hoặc hai năm một lần. Dùng cho lưu trữ có các yêu cầu tuân thủ nghiêm ngặt.

### S3 Outposts

- ✓ Cung cấp dịch vụ lưu trữ dữ liệu ngay tại chỗ
- ✓ S3 trên Outposts cung cấp một lớp lưu trữ S3 duy nhất
- ✓ Dữ liệu được lưu trữ trên nhiều thiết bị lưu trữ và các máy chủ

**Tư vấn dùng trong trường hợp:** Dữ liệu của bạn phải được lưu trữ trong mạng nội bộ, Đòi hỏi tốc độ truy xuất dữ liệu và ứng dụng rất cao.

# Sử dụng S3 trong thực tế

- 1**  Websites tĩnh (Static websites)  
Triển khai các websites tĩnh, và sử dụng CloudFront cho phân phối nội dung
- 2**  Lưu trữ sao lưu(backup) dữ liệu sử dụng S3 Glacier  
Lưu trữ sao lưu dữ liệu
- 3**  Các hệ thống phân tích dữ liệu (Analytics systems)  
Lưu trữ dữ liệu trong S3 sử dụng với các dịch vụ phân tích dữ liệu như Redshift và Athena
- 4**  Các ứng dụng Smart phone (Mobile Applications)  
Các ứng dụng của người dùng chạy trên Smart Phone sử dụng để tải dữ liệu (upload) lên S3 bucket

# Tổng kết

S3 là một đối tượng dịch vụ với một vài các lớp lưu trữ dữ liệu :

- 1) S3 Standard
- 2) S3 Intelligent-Tiering
- 3) S3 Standard-Infrequent Access(IA)
- 4) S3 One Zone-Infrequent Access(IA)
- 5) S3 Glacier
- 6) S3 Glacier Deep Archive
- 7) S3 Outposts

# Thực hành tạo lưu trữ dữ liệu S3 Bucket

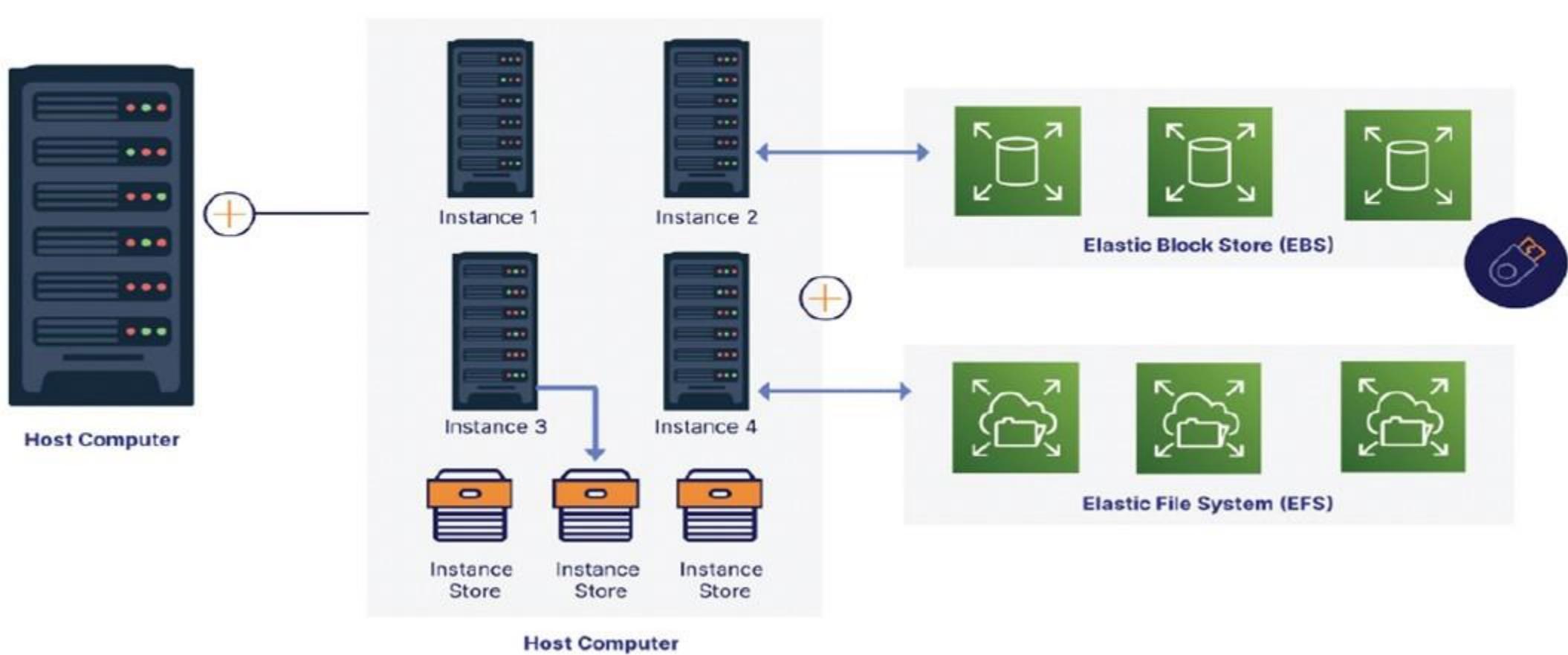


# Tìm hiểu thêm các loại dịch vụ lưu trữ dữ liệu trong AWS



# Một bức tranh toàn cảnh về EC2 Storage

- EC2 hỗ trợ một số sự lựa chọn lưu trữ cho các máy chủ ảo(Instances) của bạn



# Amazon Elastic Block Store (EBS)

EBS là một thiết bị lưu trữ (được gọi là một Volume), nó có thể được gắn( hoặc loại bỏ) vào trong máy chủ ảo EC2 instance của bạn.

Dữ liệu vẫn tồn tại, ngay cả khi máy chủ ảo EC2 không chạy

Được gắn liền với một khu vực trung tâm dữ liệu (Availability Zone)



Có thể chỉ được gắn vào một máy ảo instance trong một Khu vực trung tâm dữ liệu giống nhau

## Sử dụng trong trường hợp:

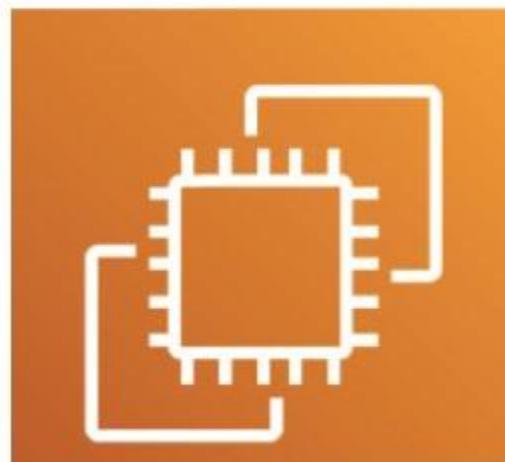
- ✓ Cần phải có tốc độ truy xuất dữ liệu nhanh
- ✓ Cài đặt và chạy một máy chủ cơ sở dữ liệu (database instance)
- ✓ Lưu trữ dữ liệu trong một thời gian dài

# EC2 Instance Store

- Một instance store là vùng lưu trữ cục bộ nằm trong các ổ cứng vật lý. Các ổ cứng này được gắn với một máy chủ vật lý chứa các máy ảo EC2 instances và không thể gỡ bỏ.

Là bộ lưu trữ trong các ổ cứng  
Vật lý, được gắn vào một máy chủ ảo  
EC2 Instance

Là ổ lưu trữ dữ liệu tốc độ cao  
(Higher I/O Speeds)



Khi máy chủ ảo bị dừng (stopped) dữ liệu sẽ bị mất

## Sử dụng trong các trường hợp:

- ✓ Cần lưu trữ dữ liệu tạm thời
- ✓ Dữ liệu của bạn đã được sao lưu,  
sao chép trong các bộ lưu trữ, hoặc  
trong các máy chủ ảo EC2 Instance

# Amazon Elastic File System(EFS)

- EFS là một serverless network file system, dành cho dịch vụ chia sẻ files trong đám mây AWS

Chỉ hỗ trợ cho các máy  
chủ chạy HĐH Linux

Chi phí sử dụng đắt hơn EBS



Có thể truy cập giữa các vùng trung tâm dữ liệu  
Khác nhau, trong một Region giống nhau.

## Sử dụng trong các trường hợp:

- ✓ Là những thư mục chính cho các ứng dụng kinh doanh quan trọng.
- ✓ Sử dụng cho lưu trữ các tệp dữ liệu lớn, để(**Lift & shift**) chuyển dịch những ứng dụng lớn đang chạy của doanh nghiệp lên đám mây, giúp giảm chi phí cơ sở hạ tầng cố định.

# Storage Gateway

- Storage Gateway là một dịch vụ lưu trữ lai đám mây ( Storage Service)

Kết nối tại chỗ và dữ liệu đám mây

Hỗ trợ mô hình lưu trữ dữ liệu lai  
(Hybrid model)



## Sử dụng cho các trường hợp:

- ✓ Di chuyển sao lưu(backup) dữ liệu lên đám mây
- ✓ Giảm các chi phí cho thiết bị lưu trữ lai đám mây
- ✓ Có thể truy cập dữ liệu nhanh, độ trễ thấp(Low latency)

# Tổng kết

- Có 2 loại lưu trữ dữ liệu là : EC2 Storage và Storage Gateway
- EC2 Storage hỗ trợ một vài sự lựa chọn cho các máy chủ ảo EC2 instances:
  - 1) Elastic Block Store(EBS)
  - 2) Instance Store
  - 3) Elastic File System (EFS)

# Tìm hiểu dịch vụ phân phối nội dung-Content Delivery Services

## Tổng quan chung bài học



# Bức tranh tổng quan về dịch vụ phân phối nội dung

- Dịch vụ phân phối nội dung-content delivery network(CDN) là gì?



Một dịch vụ phân phối nội dung (CDN) là một cơ chế dùng để phân phối nhanh và hiệu quả đưa dịch vụ nội dung đến với người dùng, dựa trên vị trí vật lý gần nhất

- Độ trễ (Latency) trong dịch vụ phân phối nội dung(CDN) là gì?



Độ trễ (Latency) hiểu theo nghĩa đơn giản là thời gian phản hồi yêu cầu đến người dùng, từ dịch vụ phân phối nội dung.

Độ trễ thấp là tốt!

# Amazon CloudFront

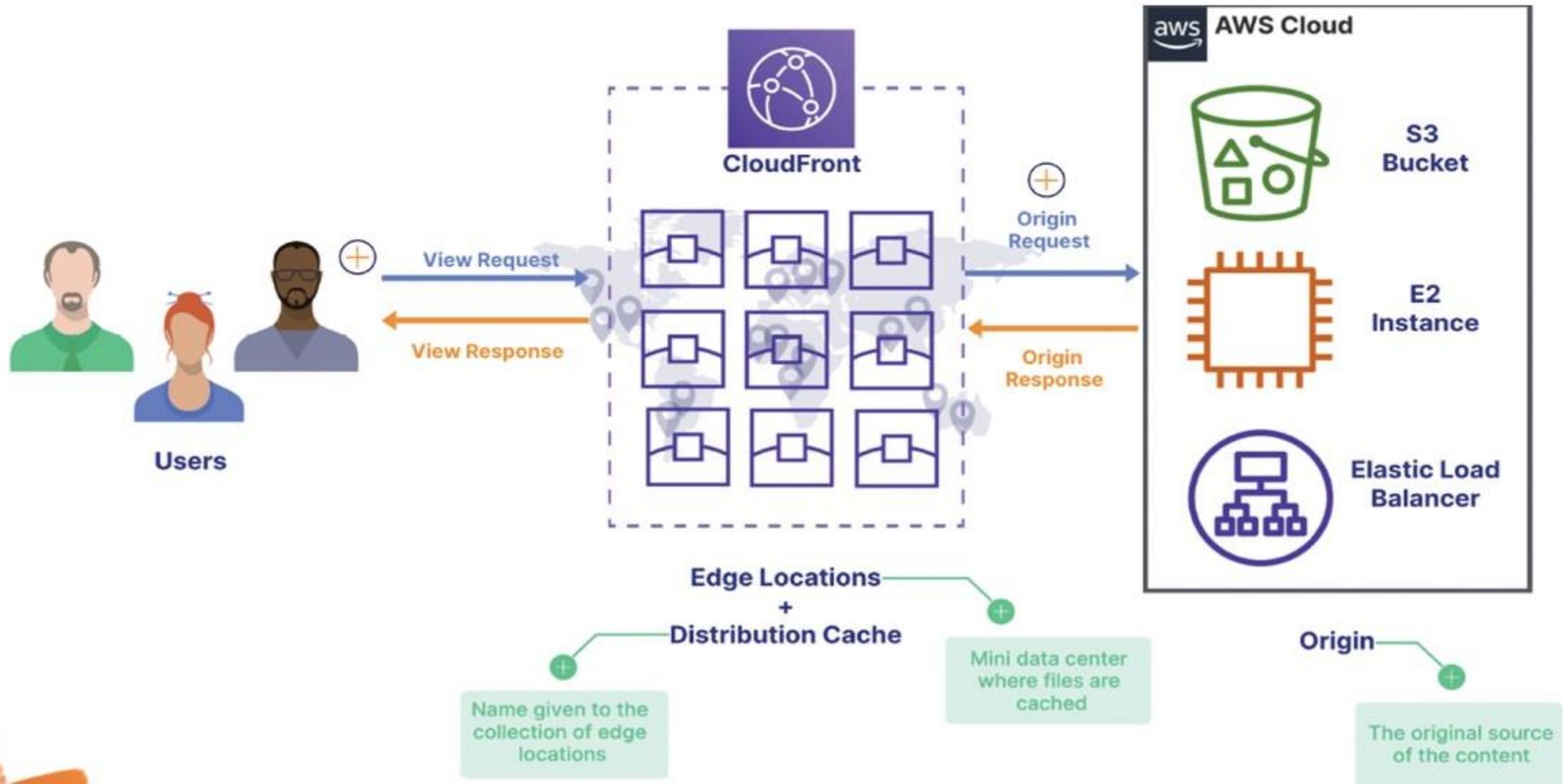
- CloudFront là một dịch vụ phân phối nội dung(CDN), nó phân phối dữ liệu và các ứng dụng ra toàn cầu với độ trễ thấp (low latency)
- ✓ Cung cấp nội dung toàn cầu, hoặc giới hạn nó dựa trên vị trí địa lý
- ✓ Tăng tốc độ phân phối nội dung  
Trang web tĩnh và web động



- ✓ Sử dụng các mạng lưới phân phối dữ liệu (**Edge Locations**), để làm bộ đệm(cache) cho nội dung dữ liệu.



Bạn có biết nếu nội dung đã được lưu trong một bộ phân phối dữ liệu (Edge location), CloudFront phân phối nó ngay lập tức? nếu không, CloudFront lấy files nội dung từ nguyên bản tại máy chủ cung cấp dịch vụ.



# CloudFront trong ứng dụng thực tế



CloudFront thường được sử dụng cùng với S3 cho việc triển khai phân phối nội dung ra toàn cầu

**S3 Websites tĩnh (Static websites)**



CloudFront có thể ngăn chặn tốt các tấn công máy chủ web, giống như tấn công DDoS

**Ngăn chặn tấn công (Prevent attacks)**



Giới hạn (Geo-restriction) người dùng truy cập nội dung theo khu vực địa lý trong các quốc gia được chỉ định

**IP address blocking**

# Amazon Global Accelerator

- Global Accelerator là một dịch vụ giúp cải thiện hiệu suất lưu lượng , tăng tốc độ truy cập của người dùng thông qua mạng lưới toàn cầu của Amazon (AWS global network)

✓ Cải thiện độ trễ(latency) và tính sẵn sàng của ứng dụng một vùng



✓ Gửi các lưu lượng truy cập(traffic) xuyên suốt qua cơ sở hạ tầng mạng lưới toàn cầu Của Amazon (AWS global network Infrastructure)

✓ Tăng hiệu suất lưu lượng truy cập của người dùng lên đến 60%

✓ Tự động định tuyến lại lưu lượng truy cập của người dùng đến điểm cuối ổn định có kết nối gần nhất, để giảm thiểu sự cố trên điểm cuối

# Amazon S3 Transfer Acceleration

- S3 Transfer Acceleration cải thiện tăng tốc độ nội dung, trong việc tải files lên (uploads) và tải files xuống (downloads) từ S3 Buckets

✓ Truyền tập tin một cách nhanh chóng  
từ các khoảng cách xa



✓ S3 Transfer Acceleration tận dụng hạ tầng  
mạng lưới phân phối toàn cầu(Edge locations)  
của Amazon CloudFront,  
để giúp tăng tốc độ downloads & uploads file trên Amazon S3

✓ Khách hàng khắp nơi trên thế giới có thể  
tải files (uploads) đến một trung tâm bucket,  
trên Amazon S3

# Tổng kết

- **CloudFront** là một dịch vụ phân phối nội dung(CDN), nó phân phối dữ liệu và các ứng dụng ra toàn cầu với độ trễ thấp (low latency)
- **Global Accelerator** là một dịch vụ giúp cải thiện hiệu suất lưu lượng , tăng tốc độ truy cập của người dùng thông qua mạng lưới toàn cầu của Amazon (AWS global network)
- **S3 Transfer Acceleration** cải thiện tăng tốc độ nội dung , trong việc tải files lên (uploads) và tải files xuống (downloads) từ S3 Buckets

## Tìm hiểu kiến trúc dịch vụ mạng VPC và các thành phần hệ thống

- **Một bức tranh tổng quan về hệ thống mạng ảo (Virtual Networking)**
  - ✓ Hệ thống mạng ảo (Virtual Networking) kết nối các máy tính với nhau và cho phép chia sẻ dữ liệu, các ứng dụng trong mạng nội bộ và toàn cầu, trong một môi trường mạng an toàn sử dụng các bộ định tuyến ảo(virtual routers), tường lửa (firewalls), và các dịch vụ quản trị hệ thống(nework management services).

# Chúng ta có một cái nhìn gần hơn về hệ thống mạng ảo

- **Amazon Virtual Private Cloud(VPC)**

VPC là một dịch vụ nền tảng, nó cho phép bạn tạo mạng riêng bảo mật ( secure private network) trong AWS cloud, nơi bạn cài đặt & tạo các tài nguyên hệ thống.

Private virtual network



Cô lập và bảo mật các tài nguyên

Cài đặt các tài nguyên,  
như là EC2 instances bên trong  
VPC



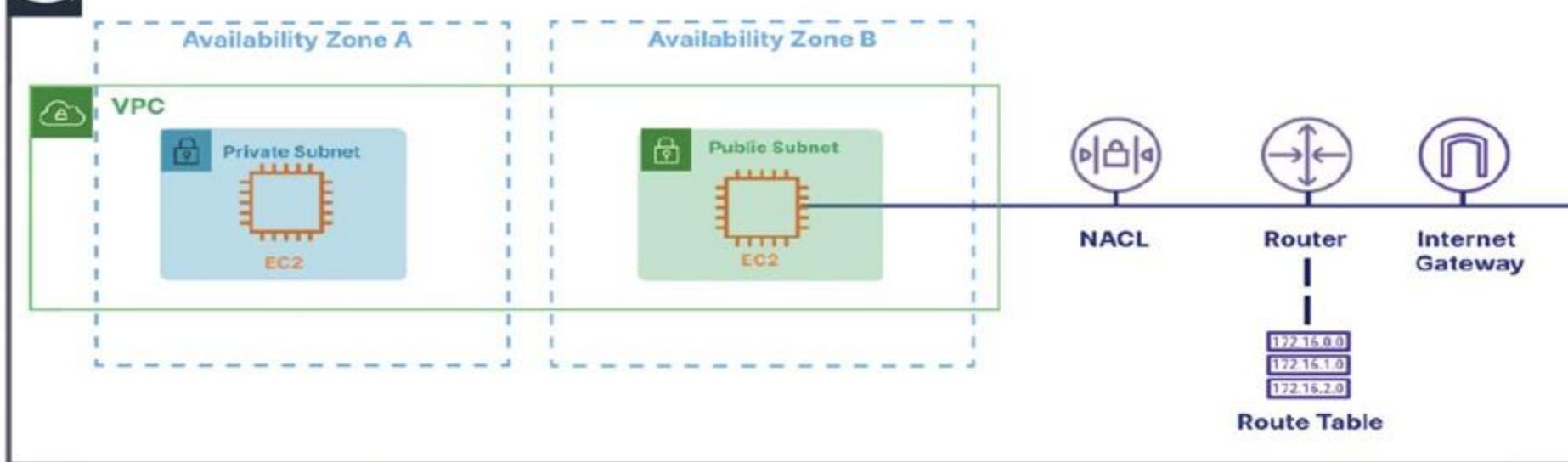
Internet  
Gateway



Peering  
Connection

Một VPC kéo dài đến các khu vực trung tâm dữ liệu  
(Availability Zones) trong một Region





### Router and Route Table

Được định nghĩa nơi mà các luồng lưu lượng mạng(network traffic) được định tuyến

### Network ACL

Access control lists(ACLs) đảm bảo các luồng truy cập mạng thích hợp, được cho phép đi vào bên trong mạng con(subnet)

### Mạng con (Subnet)

Bên trong một VPC cho phép bạn chia một hệ thống mạng ảo ra nhiều mạng con(subnet), và đây là nơi để bạn tạo các tài nguyên như EC2 Instances



### VPC

Một VPC là một mạng riêng ảo trong AWS cloud



### AZ

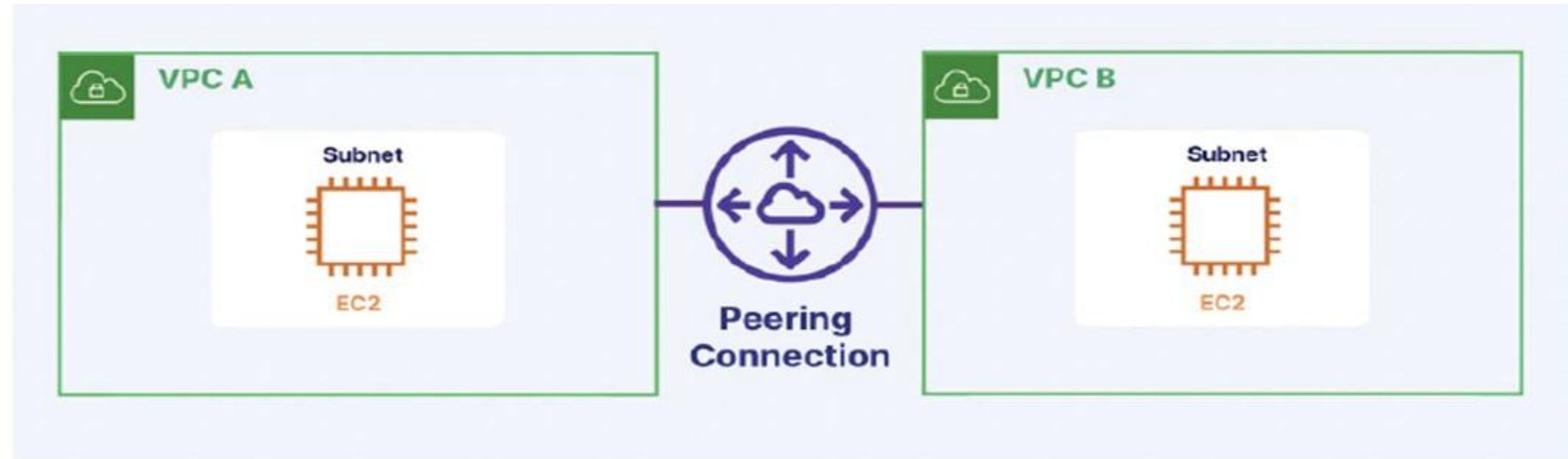
Các khu vực trung tâm dữ liệu Availability Zones(Azs) Bao gồm một hoặc nhiều hơn các trung tâm dữ liệu (data centers), mỗi một trung tâm dữ liệu có các hệ thống: Máy phát điện dự phòng, hệ thống mạng, các hệ thống kết nối, được đặt trong các cơ sở Riêng biệt

### Internet Gateway

Một internet Gateway cho phép các tài nguyên bên trong VPC được ra ngoài Internet, và ngược lại

# VPC peering cho phép bạn kết nối 2 VPCs với nhau

Peering hỗ trợ trong việc truyền dữ liệu một cách an toàn.



Các bạn sẽ xem một demo, làm thế nào để tạo một VPC

# Thực hành khởi tạo, cài đặt một máy chủ ảo EC2 Instance trong một Virtual Private Cloud(VPC)

- Trong tình huống của bài thực hành này. Giám đốc công ty Labogini đang tìm kiếm cách để cài đặt một Website giúp quảng cáo hệ thống cửa hàng bán lẻ phụ kiện điện thoại thông minh của anh ấy trên Amazon cloud.

Chúng ta sẽ giúp bằng cách cài đặt máy chủ cung cấp dịch vụ website cho anh ấy .

Xuyên suốt bài thực hành này chúng ta sẽ khám phá và tìm hiểu các nền tảng dịch vụ mạng ảo căn bản của AWS. Chúng ta sẽ tạo một Virtual private cloud(VPC), mạng con subnet giữa các khu vực trung tâm dữ liệu Azs, routers và một internet gateway. Những dịch vụ này là cái nền tảng của kiến trúc hệ thống mạng bên trong AWS và bao gồm các khái niệm như: Cơ sở hạ tầng mạng (Network infrastructure), thiết kế(design), định tuyến(routing), và bảo mật(security).

- Các bước làm trong bài thực hành:**

- 1) Tạo một VPC
- 2) Tạo một mạng con Public Subnet
- 3) Tạo Routers và cấu hình Internet Gateway
- 4) Tạo & cài đặt cấu hình máy chủ ảo EC2 trong Subnet
- 5) Truy cập vào kiểm tra xem chủ ảo EC2, hoạt động cung cấp dịch vụ có như mục tiêu hay không?

## I) Tạo VPC

- 1) Vào mục VPC > Your VPCs.
- 2) Click Create VPC, và nhập vào các giá trị sau:

Select: VPC Only

Name tag: my-vpc

IPv4 CIDR block: 10.0.0.0/16

- 3) Để IPv6 CIDR block và Tenancy fields giá trị mặc định default values.

- 4) Click Create VPC.

## II) Tạo Public Subnet

- 1) Click Subnets trong menu phía bên trái.
- 2) Click Create subnet, và nhập vào các giá trị sau:

VPC ID: my-vpc

Subnet name: my-public-subnet

Availability Zone: us-east-1a

IPv4 CIDR block: 10.0.0.0/24

- 3) Click Create subnet.

## III) Tạo Routes và cấu hình Internet Gateway

- 1) Với my-public-subnet selected, click Actions > Edit subnet settings.
- 2) Check the box to Enable auto-assign public IPv4 address.
- 3) Click Save.
- 4) Click Internet Gateways trong menu phía bên trái.
- 5) Click Create internet gateway.
- 6) Set Name tag as "my-internet-gateway".
- 7) Click Create internet gateway.

8) Trong màn hình tiếp theo, click Actions > Attach to VPC.

9) In the Available VPCs dropdown, chọn my-vpc.

10) Click Attach internet gateway.

11) Click Route Tables in the left-hand menu.

12) Click Create route table, và nhập vào các giá trị sau:

Name: publicRT

VPC: my-vpc

13) Click Create route table.

14) On the next screen, click Edit routes.

15) Click Add route, and set the following values:

Destination: 0.0.0.0/0

Target: Internet Gateway, my-internet-gateway

16) Click Save changes.

17) Click the Subnet associations tab.

18) Click Edit subnet associations.

19) Select the box for my-public-subnet.

20) Click Save associations.

#### **IV) Tạo EC2 Instance trong Subnet**

1) Vào EC2 > Instances.

2) Click Launch instances.

3) On the AMI page, select the Amazon Linux 2 AMI.

4) CHọn t2.micro .

5) Click Review and Launch > Launch.

6) Trong key pair dialog, chọn Create a new key pair.

7) đặt tên Key pair là "my-keypair".

8) Click Download Key Pair.

9) Click Launch Instances.

10) Click View Instances, và chờ một vài phút để nó hiện lên server đã trong tình trạng Running state.

#### **IV) Truy cập vào (Access ) EC2 Instance**

1) Khi nó đã trong Running state, chọn cái nút gần nó.

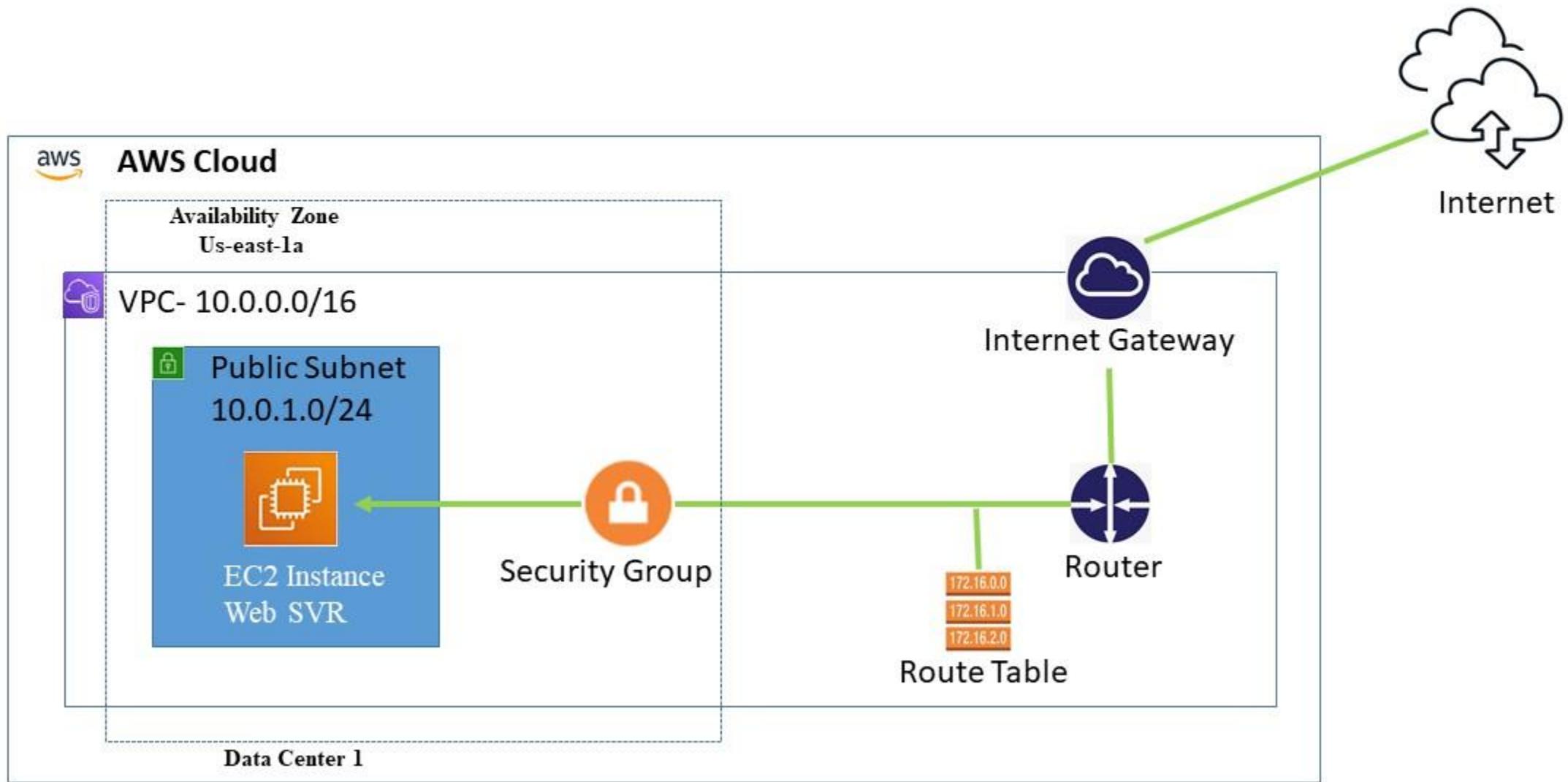
2) Click Connect trên đầu.

3) Trong EC2 Instance Connect section, click Connect.

Nó sẽ mở ra một cái tab trình duyệt browser hiển thị a command line interface.

Như vậy bạn bạn đã hoàn thành xong bài thực hành!!!

# Sơ đồ hệ thống EC2 Instance trong Virtual Private Cloud (VPC)



# Tìm hiểu về các dịch vụ mạng AWS bổ sung: Route 53, Direct Connect, Site-to-Site VPN

## Tổng quan chung bài học



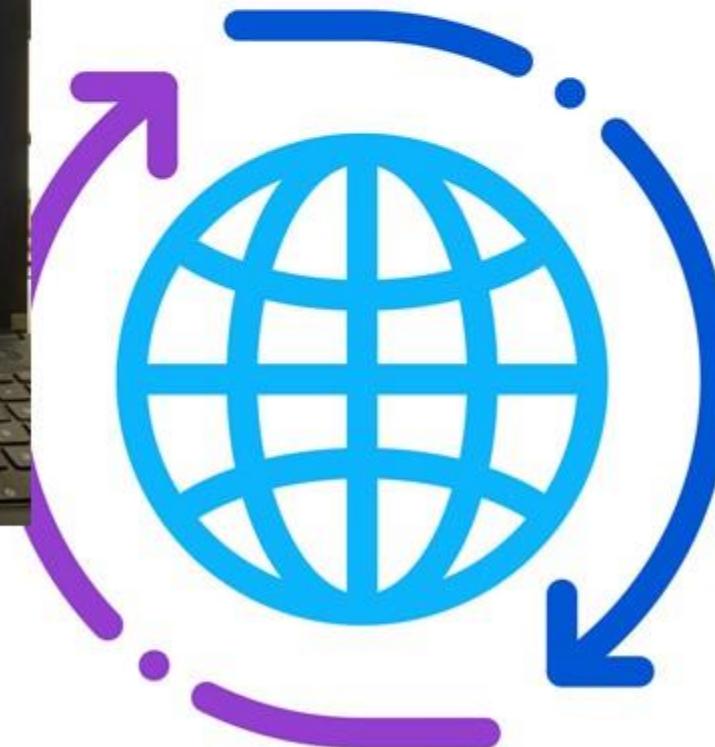
# DNS là gì

- DNS là Domain Name System, được hiểu là hệ thống phân giải tên miền. Nó là một hệ thống chuyển đổi các tên miền website, chuyển từ dạng www.tenmien.com sang dạng địa chỉ IP tương ứng với tên miền và ngược lại.

**www.unica.vn**



**202.92.4.5**



# Amazon Route 53

- Route 53 là một dịch vụ DNS, nó định tuyến người dùng truy cập từ máy tính đến các websites, ứng dụng của các máy chủ trên Internet.

- ✓ Đăng ký tên domain
- ✓ Thực hiện các kiểm tra tình trạng hoạt động “Sức khỏe”(health checks) của các tài nguyên hệ thống trong AWS cloud



172.16.0.0
172.16.1.0
172.16.2.0

Bảng định tuyến  
(route Table)



Hosted  
Zone

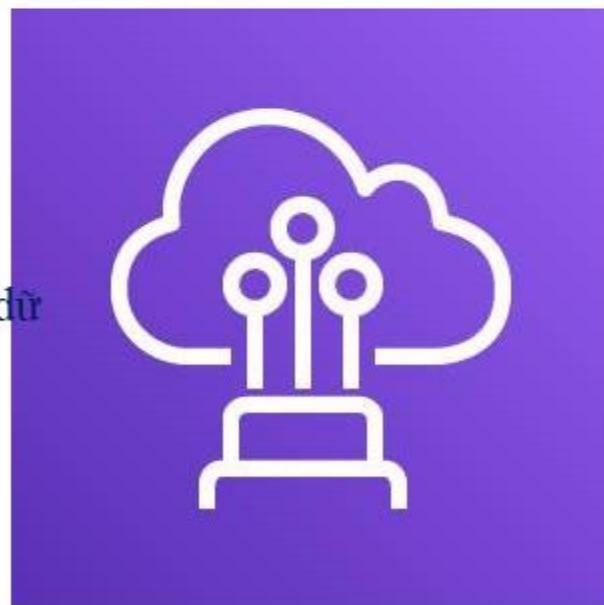
- ✓ Hỗ trợ kiến trúc hệ thống mạng lai đám mây (hybrid cloud)

# AWS Direct Connect

- Direct Connect là một kết nối mạng riêng vật lý, trực tiếp từ hệ thống mạng của một doanh nghiệp đến trung tâm dữ liệu Data Center của AWS cloud

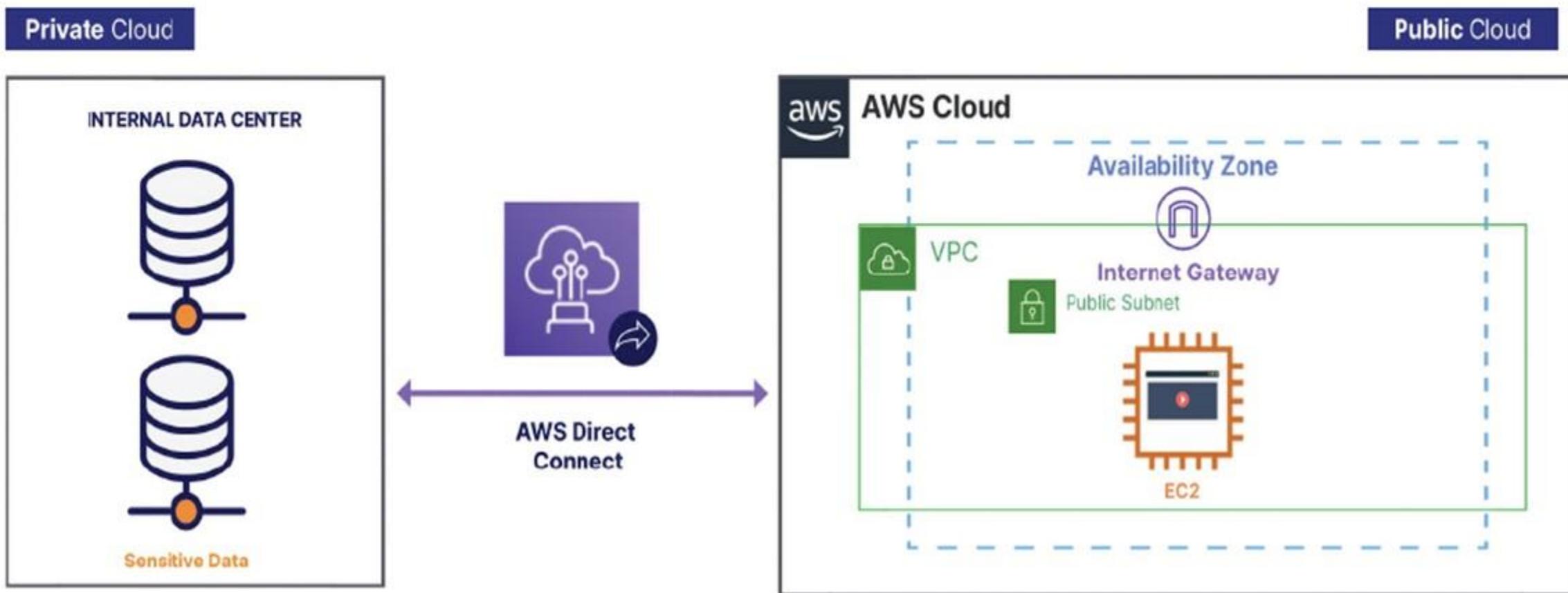
✓ Kết nối mạng vật lý trực tiếp

✓ Kết nối ngay tại chỗ giữa trung tâm dữ liệu Data Center của doanh nghiệp và AWS cloud



- ✓ Hệ thống mạng truy cập dữ liệu giữa mạng nội bộ và AWS Cloud nhanh, như là làm việc trong mạng nội bộ LAN
- ✓ Hỗ trợ một môi trường lai giữa mạng nội bộ và đám mây (hybrid environment)

# Một sơ đồ Hybrid cloud, là một sự phối hợp giữa public và private clouds

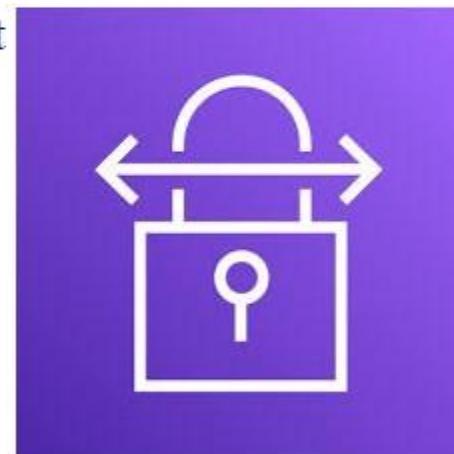


# AWS VPN

- Site to Site VPN tạo một sự kết nối bảo mật và ổn định giữa mạng nội bộ của bạn và hệ thống AWS cloud của bạn.

✓ Tương tự như kết nối Direct Connect , tuy nhiên dữ liệu đi qua internet

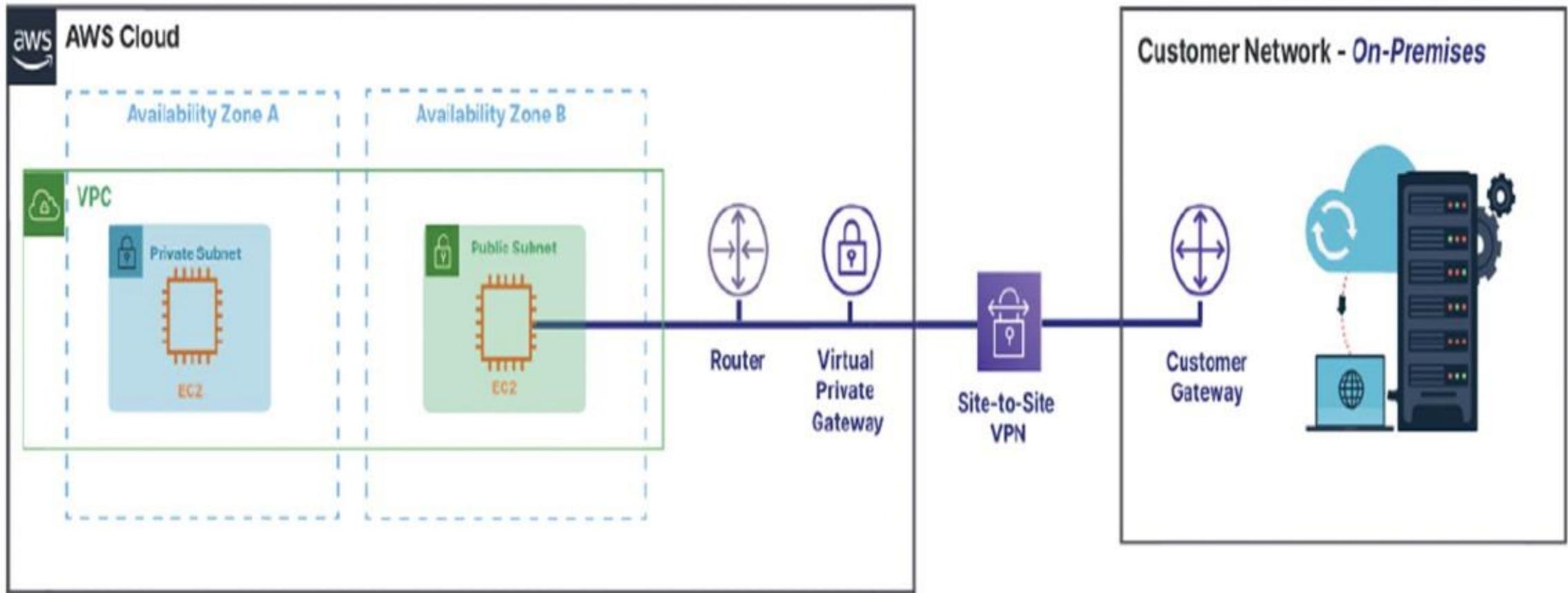
✓ Dữ liệu được mã hóa

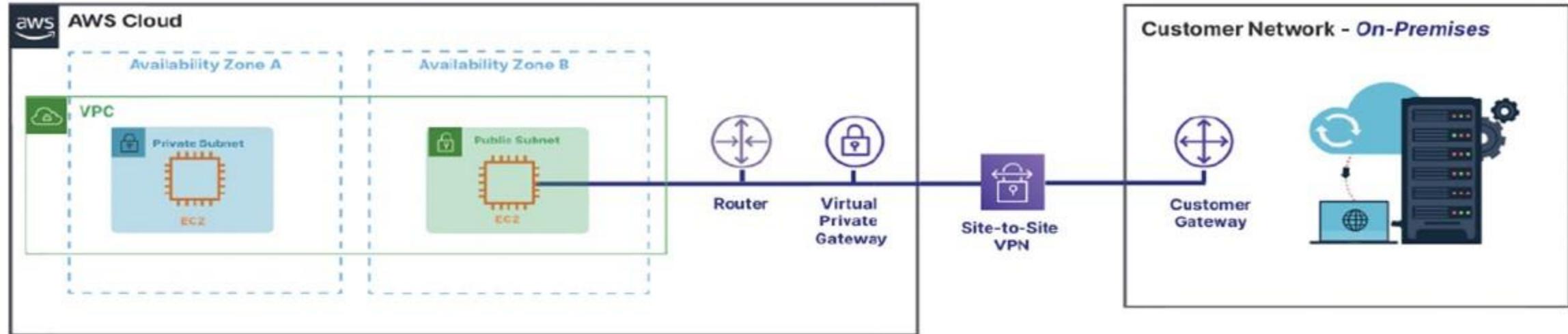


✓ Kết nối ngay tại chỗ giữa trung tâm dữ liệu Data Center của doanh nghiệp và AWS cloud

✓ Hỗ trợ một môi trường lai giữa mạng nội bộ và đám mây (hybrid environment)

# Một Site to Site VPN giúp cho việc chuyển dịch ứng dụng lên đám mây dễ dàng hơn





### **Virtual Private Gateway**

Là router ảo cho kết nối VPN nằm tại AWS



### **Router**

Được định nghĩa nơi mà các luồng lưu lượng mạng(network traffic) được định tuyến



### **Customer Gateway**

Là router cho kết nối VPN phía khách hàng



### **Mạng con (Subnet)**

Bên trong một VPC cho phép bạn chia một hệ thống mạng ảo ra nhiều mạng con(subnet). và đây là nơi để bạn tạo các tài nguyên như EC2 Instances



### **VPC**

Một VPC là một mạng riêng ảo trong AWS cloud

### **AZ**

Các khu vực trung tâm dữ liệu Availability Zones(Azs)  
Bao gồm một hoặc nhiều hơn các trung tâm dữ liệu  
(data centers), mỗi một trung tâm dữ liệu có  
các hệ thống: Máy phát điện dự phòng, hệ thống  
mạng, các hệ thống kết nối, được đặt trong các cơ sở  
 Riêng biệt

### **Site to Site VPN**

một sự kết nối bảo mật và ổn định giữa mạng nội bộ  
của bạn và hệ thống AWS cloud của bạn

# Tổng kết

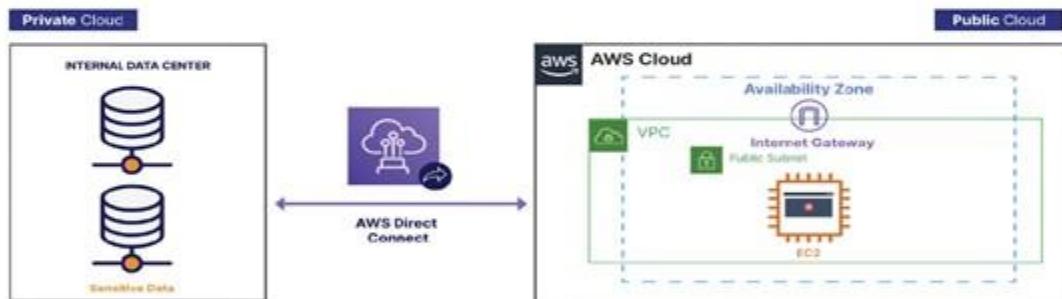
- Route 53:

[www.unica.vn](http://www.unica.vn)

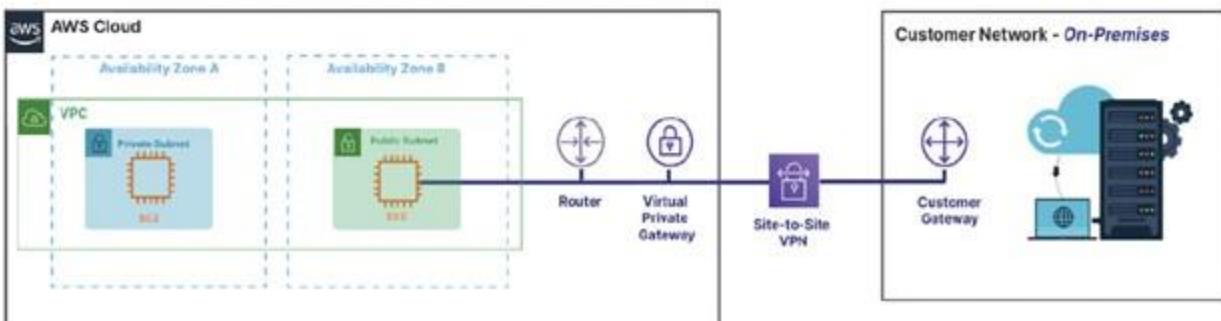


Route 53 là một dịch vụ DNS tự động hóa, phân giải tên miền cho người dùng đến với các ứng dụng trên Internet

- Direct Connect:** Là một kết nối mạng riêng vật lý, trực tiếp từ hệ thống mạng của một doanh nghiệp đến trung tâm dữ liệu Data Center của AWS cloud



- Site to Site VPN:** Tạo một sự kết nối bảo mật và ổn định giữa mạng nội bộ của bạn và hệ thống AWS cloud của bạn.



# Sử dụng các ứng dụng cơ sở dữ liệu Databases



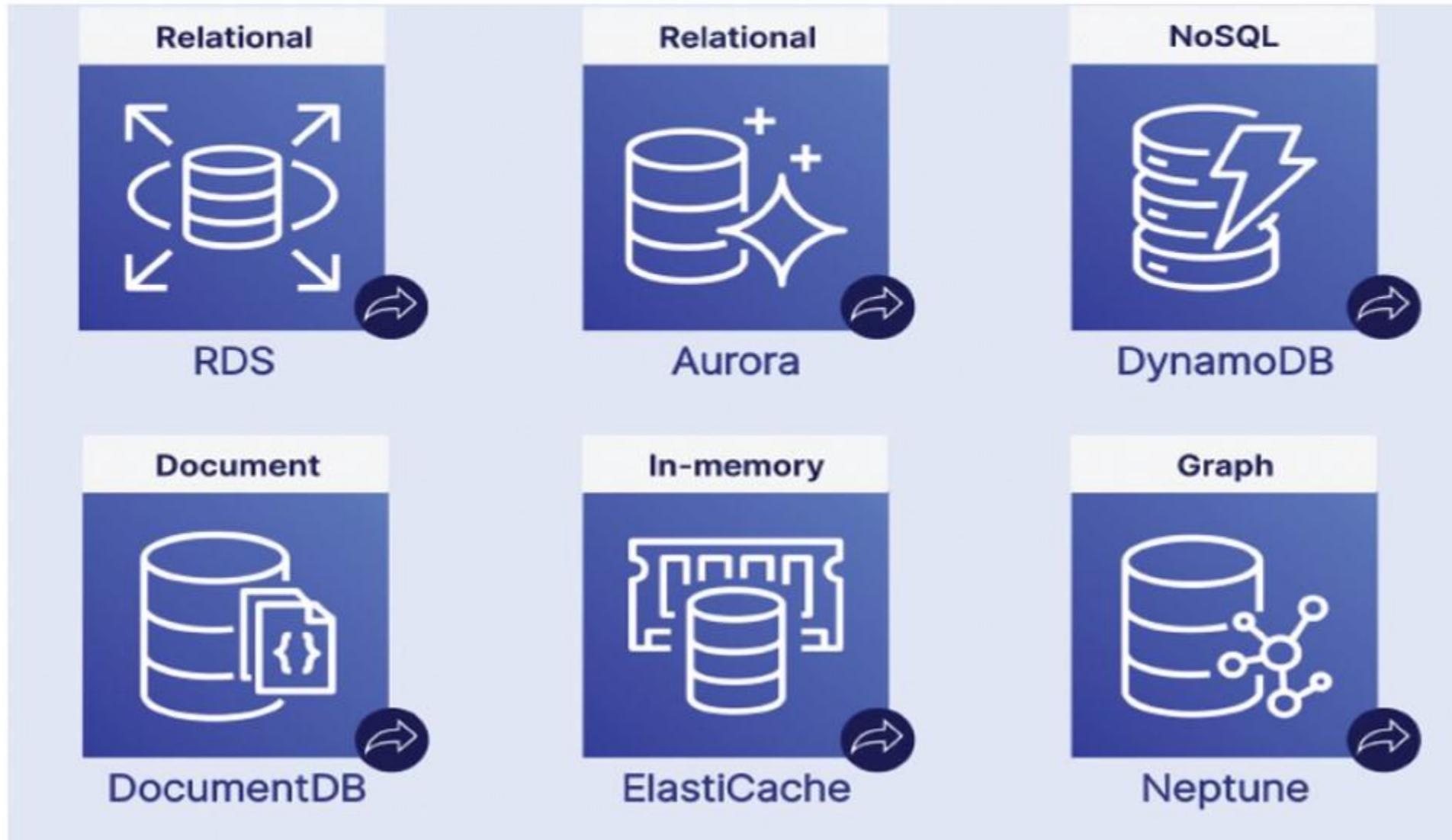
# Một bức tranh tổng quan về cơ sở dữ liệu Databases



**Database**

- ✓ Cơ sở dữ liệu cho phép chúng ta tập hợp, lưu trữ, truy vấn, sắp xếp, thống kê, và xử lý số liệu.
- ✓ Một cơ sở dữ liệu là một tập hợp có tổ chức của nhiều dạng dữ liệu khác nhau
- ✓ Cơ sở dữ liệu được sử dụng cho nhiều loại ứng dụng: Web, mobile, Services VV..
- ✓ Cơ sở dữ liệu là cần thiết để duy trì dữ liệu xuyên suốt quá trình chạy ứng dụng
- ✓ Chúng ta có thể truy cập dữ liệu được lưu trong một CSDL bằng cách sử dụng câu lệnh để truy vấn dữ liệu
- ✓ Các cơ sở dữ liệu thường được kiểm soát bởi một hệ thống quản lý cơ sở dữ liệu

Trong hệ sinh thái của AWS, có nhiều kiểu khác nhau của các cơ sở dữ liệu, và nó hỗ trợ các trường hợp sử dụng khác nhau



# Amazon Relational Database Service (RDS)

- RDS là một dịch vụ, nó cho phép dễ dàng trong việc tạo, cài đặt & quản lý các hệ CSDL quan hệ

✓ Hỗ trợ các hệ CSDL phổ biến



✓ Nó cung cấp tính sẵn sàng cao (high availability) và tính chịu lỗi (fault tolerance) sử dụng tùy chọn trong triển khai Multi-AZ

✓ AWS quản lý CSDL trong việc tự động cài đặt các bản vá lỗi, tự động backup, bảo trì hệ điều hành, VV..

✓ Có thể tạo nhiều CSDL đọc giống nhau (read replicas) giữa các Regions để cung cấp Khả năng gia tăng hiệu xuất và tính bền vững



# Amazon Aurora

- Aurora là một cơ sở dữ liệu quan hệ, nó tương thích với MySQL và PostgreSQL, và được phát triển bởi Amazon

✓ Hỗ trợ MySQL và PostgreSQL  
Database engines



✓ Nhanh hơn 5 lần so với  
MySQL và hơn 3 lần so với PostgreSQL

✓ Tự động tăng quy mô, cung cấp  
tính bền vững và tính sẵn sàng cao

✓ Quản lý bởi Amazon RDS



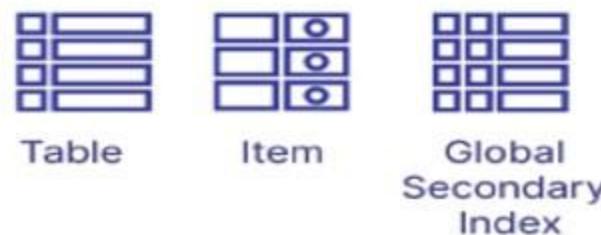
# Amazon DynamoDB

- **DynamoDB** là một cơ sở dữ liệu NoSQL khóa-giá trị được quản lý hoàn toàn, phi máy chủ và được thiết kế để chạy các ứng dụng hiệu suất cao trên mọi quy mô.

✓ NoSQL khóa-giá trị(key-value) CSDL



✓ Được quản lý hoàn toàn và phi máy chủ (serverless)



✓ Không sử dụng quan hệ CSDL (Non-relational)

✓ Tự động mở rộng quy mô xử lý dữ liệu, khi gặp phải tải trọng công việc lớn, đòi hỏi CSDL phải có hiệu xuất cao

# Amazon DocumentDB

DocumentDB là dịch vụ cơ sở dữ liệu có thể mở rộng, có độ bền cao và được quản lý đầy đủ để vận hành những khối lượng công việc, giống với MongoDB

- ✓ Là cơ sở dữ liệu tài liệu (Document database)



- ✓ Tương thích với MongoDB

- ✓ Được quản lý hoàn toàn và phi máy chủ (serverless)

- ✓ Không sử dụng quan hệ CSDL (Non-relational)

# Amazon ElastiCache

**ElastiCache** là một dịch vụ được quản lý hoàn toàn lưu trữ dữ liệu tạm thời trên RAM, ElastiCache tương thích với Redis và Memcached.

- ✓ Lưu trữ dữ liệu trong RAM



- ✓ Tương thích với Redis và Memcached.

- ✓ Dữ liệu có thể bị mất

- ✓ Có tốc độ truy xuất dữ liệu rất cao(High Performance) và độ trễ cực thấp( low Latency)



ElastiCache for  
Memcached



ElastiCache for  
Redis

# Amazon Neptune

**Neptune** là một dịch vụ được quản lý hoàn toàn lưu trữ dữ liệu đồ thị(Graph database), nó hỗ trợ kết nối bộ dữ liệu cao

- ✓ lưu trữ dữ liệu đồ thị(Graph database)
- ✓ Nó hỗ trợ bộ kết nối cao giống như mạng xã hội (social media networks)



- ✓ Được quản lý hoàn toàn và phi máy chủ (serverless)
- ✓ Có tốc độ truy xuất dữ liệu nhanh và đáng tin cậy

# Sử dụng databases trong thực tế

- Mặc dù các cơ sở dữ liệu trong AWS hỗ trợ nhiều trường hợp. Tuy nhiên có một số lựa chọn tốt sau cho mỗi trường hợp.

**1**

Chuyển dịch (Migrate) một CSDL Oracle lên Cloud



RDS

**2**

Chuyển dịch (Migrate) một CSDL PostgreSQL lên Cloud



RDS



Aurora

**3**

Giảm tải trong việc có quá nhiều người dùng thường xuyên truy cập CSDL



ElastiCache

**4**

Xử lý một lượng lớn hồ sơ người dùng (User profiles) và các tương tác trong mạng xã hội



Neptune

**5**

CSDL NoSQL đủ nhanh để xử lý hàng triệu Yêu cầu từ người dùng trong mỗi giây



DynamoDB

**6**

Hoạt động giống với MongoDB, nhưng Hỗ trợ tài trọng xử lý dữ liệu nhanh bằng cách mở rộng quy mô



DocumentDB

# Tổng kết

1) RDS là một dịch vụ, nó giúp dễ dàng tạo & cài đặt các CSDL quan hệ



2) Aurora là một cơ sở dữ liệu quan hệ, nó tương thích với MySQL và PostgreSQL, và được phát triển bởi Amazon



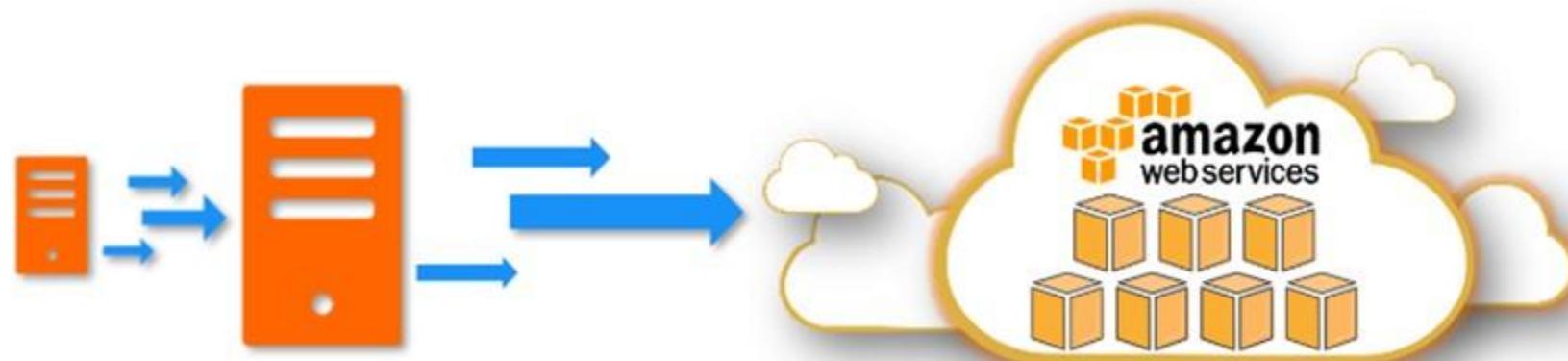
3) **DynamoDB** là một cơ sở dữ liệu NoSQL khóa-giá trị được quản lý hoàn toàn, phi máy chủ và được thiết kế để chạy các ứng dụng hiệu suất cao trên mọi quy mô.

4) **Neptune** là một dịch vụ được quản lý hoàn toàn lưu trữ dữ liệu đồ thị(Graph database), nó hỗ trợ kết nối bộ dữ liệu cao.

5) **ElastiCache** là một dịch vụ được quản lý hoàn toàn lưu trữ dữ liệu tạm thời trên RAM, ElastiCache tương thích với Redis và Memcached.

# Tìm hiểu dịch vụ di chuyển ứng dụng lên đám mây (Cloud migration Services)

Tổng quan chung bài học



- Một bức tranh tổng quan về di chuyển lên đám mây

- ✓ Ngày nay có nhiều công ty đang di chuyển lên đám mây, và họ cần giảm chi phí, tốc độ cao, và các cách bảo mật an toàn dữ liệu để chuyển dịch dữ liệu tại chỗ trong hệ thống mạng của họ lên AWS Cloud



# Database Migration Service(DMS)

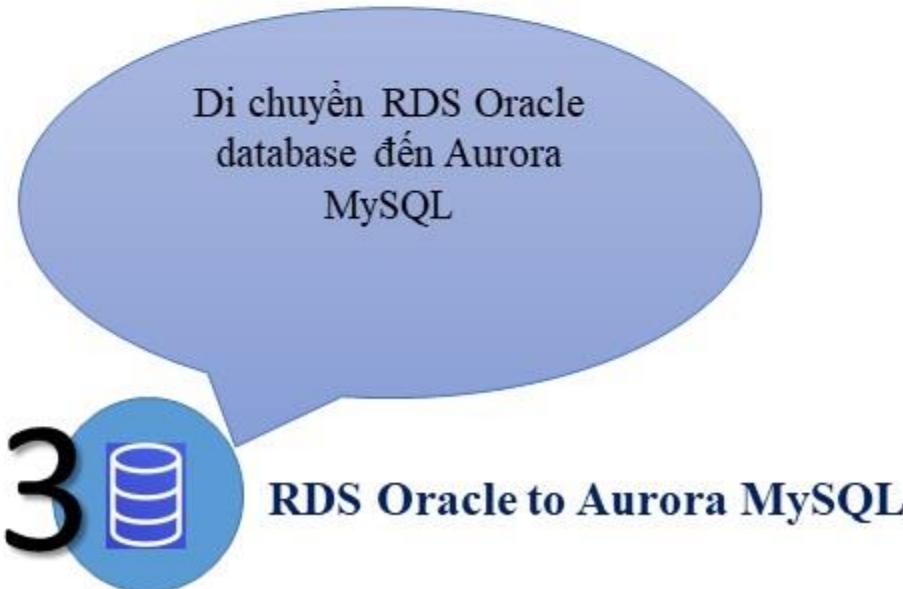
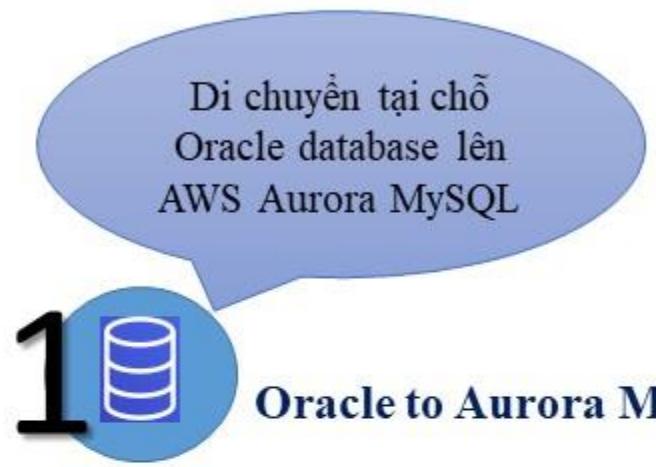
DMS giúp bạn di chuyển các cơ sở dữ liệu(databases) lên AWS

- ✓ Di chuyển các cơ sở dữ liệu tại chỗ lên AWS
- ✓ Dữ liệu liên tục được sao chép đồng bộ



- ✓ Hỗ trợ di chuyển các loại cơ sở dữ liệu đồng nhất và không đồng nhất
- ✓ Hầu như không có thời gian chết (no downtime)

# DMS trong thực tế sử dụng



# Server Migration Service(SMS)

SMS cho phép bạn di chuyển các máy chủ tại chỗ lên AWS

- ✓ Di chuyển các máy chủ tại chỗ lên AWS



- ✓ Server được lưu như là một Amazon Machine Image (AMI)

- ✓ Trong ứng dụng thực tế, Cloud9 đã được cấu hình sẵn môi trường phát triển phần mềm với bộ công cụ & phần mềm để phát triển các ứng dụng(SDKs) và các thư viện cần thiết (libraries).

Bạn có thể dễ dàng viết code cho Lambda function trực tiếp trong web browser của bạn

- ✓ Sử dụng AMI để tạo các máy chủ như Là EC2 instances

# AWS Snow Family



Snowcone



Snowcone and Snowball



Snowmobile

# Snow Family

Snow Family cho phép bạn chuyển một số lượng lớn dữ liệu tại chỗ lên AWS cloud sử dụng các thiết bị vật lý

- ✓ Dung lượng dữ liệu nhỏ nhất của thiết bị vận chuyển dữ liệu
- ✓ Bộ lưu trữ 8 terabytes



**Snowcone**

- ✓ Offline Vận chuyển bằng phương tiện vận tải
- ✓ Online sử dụng DataSync



- ✓ Giải pháp vận chuyển với dung lượng dữ liệu lên đến Petabyte
- ✓ Truyền dữ liệu bên trong và bên ngoài



**Snowball và Snowball Edge**

- ✓ Chi phí rẻ hơn truyền dữ liệu qua Internet
- ✓ Snowball Edge hỗ trợ EC2 và Lambda



- ✓ Vận chuyển dung lượng dữ liệu lên đến nhiều petabyte hoặc exabyte
- ✓ Dữ liệu được tải lên S3



**Snowmobile**

- ✓ Vận chuyển được bảo vệ  
bảo mật nghiêm ngặt



# DATA Sync

DataSync cho phép truyền dữ liệu online tại chỗ lên các dịch vụ lưu trữ AWS S3 hoặc EFS

- ✓ Di chuyển dữ liệu tại chỗ lên AWS



- ✓ Copy dữ liệu qua kết nối Direct Connect với AWS cloud hoặc qua internet

- ✓ Copy dữ liệu với nhau giữa các dịch vụ lưu trữ của AWS

- ✓ Nhận bản dữ liệu(Replicate) giữa các Region hoặc giữa các Account

# Tổng kết

1) DMS giúp bạn di chuyển các cơ sở dữ liệu(databases) lên AWS



2) DataSync cho phép truyền dữ liệu online tại chỗ lên các dịch vụ lưu trữ như AWS S3 hoặc EFS

3) SMS cho phép bạn di chuyển các máy chủ tại chỗ lên AWS



4) Snow Family cho phép bạn chuyển một số lượng lớn dữ liệu tại chỗ lên AWS cloud sử dụng các thiết bị vật lý



# Các công cụ dùng trong phát triển phần mềm - Developer Tools



## • Tại sao developer tools là quan trọng

- ✓ Các kỹ sư phát triển phần mềm sử dụng các công cụ để tăng tốc độ phát triển, phát hành, và quản lý vòng đời sản phẩm phần mềm



A screenshot of a developer's terminal or code editor showing a large amount of jQuery UI sortable code. The code is written in JavaScript and uses color-coded syntax highlighting. It includes several functions and methods related to the sortable widget, such as `selecting`, `startselected`, `selectable`, `extend`, `ui.selectable`, `version`, `ui.sortable`, `mouse`, `widgetEventPrefix`, `parent`, `axis`, `connectWith`, `containment`, `connectTo`, `axis`, `placeholder`, `revert`, `scroll`, `scrolls`, `cancel`, `options`, `containerCache`, `element.addClass`, `axis`, `refresh`, `floating`, `length`, `axis`, `getOffset`, `test`, `item.css`, `display`, `offset`, `disabled`, `removeData`, `sortable`, `unbind`, `disabled`, `return`, `this`, `_setOption`, `function`, `d`, `c`, `addClass`, `removeClass`, `mouseCapture`, `apply`, `this.arguments`, `type`, `static`, `return false`, `e=a(this)`, `andSelf`, `each`, `has`, `eq`, `length`, `return true`.

# CLOUD9

Cloud9 **cho phép bạn viết code bên trong một môi trường phát triển phần mềm tích hợp (IDE) từ bên trong** giao diện web của bạn

- ✓ Integrated development environment (IDE)
- ✓ Viết code và gỡ lỗi(debug) code



- ✓ Hỗ trợ các ngôn ngữ phổ biến

**Ứng dụng Cloud9 trong thực tế:** Cloud9 đã được cấu hình sẵn môi trường phát triển phần mềm, với bộ công cụ và phần mềm(SDKs), các thư viện(libraries) phục vụ cho việc phát triển ứng dụng . Bạn có Thể dễ dàng viết code cho Lambda function trực tiếp ngay trong web browser.

# CodeCommit

- CodeCommit là một dịch vụ kiểm soát nguồn, với quy mô vô cùng linh hoạt và bảo mật để lưu trữ các kho Git repositories riêng. Được quản lý bởi AWS

✓ Tạo các repositories để lưu code



✓ Commit, branch, và merge code

✓ Hỗ trợ sự hợp tác cùng phát triển phần mềm với các lập trình viên khác

**Ứng dụng Code commit trong thực tế:** CodeCommit có thể được sử dụng để quản lý source code và các phiên bản khác nhau của các file ứng dụng. Code Commit hoạt động tương tự như GitHub.

# CodeBuild

CodeBuild cho phép bạn xây dựng và kiểm thử (test) ứng dụng source code của bạn.

- ✓ Biên dịch(compilers) source code và chạy tests
- ✓ Cho phép liên tục tích hợp và phân phối các ứng dụng



Code Build

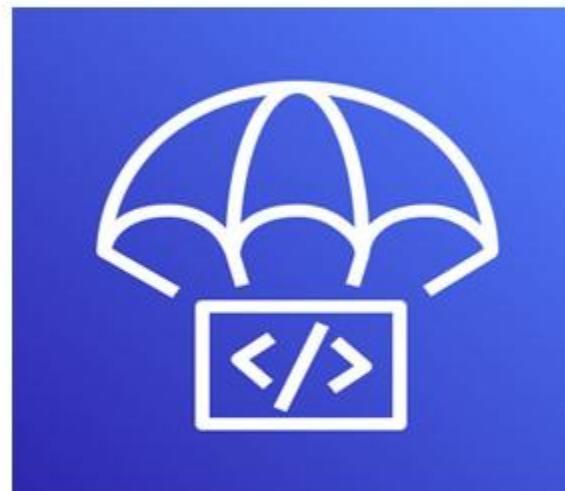
- ✓ Quản lý cấu hình dự án và luôn sẵn sàng để triển khai

**Ứng dụng Code build trong thực tế- chạy tests trước khi triển khai một phiên bản mới của một ứng dụng, và phát hành đến môi trường chạy thật(production):**

Codebuild cho phép bạn chạy nhiều luồng test ứng dụng song song khi cần thiết, cho phép triển khai những thay đổi của ứng dụng lên môi trường chạy thật nhanh hơn.

# CodeDeploy

- CodeDeploy quản lý triển khai code đến dịch vụ compute services trong cloud hoặc cho các servers ngay tại chỗ.



- ✓ Triển khai code cho EC2, Fagate, Lambda, và ngay tại chỗ.

- ✓ Duy trì uptime ứng dụng

Code build

**Ứng dụng CodeDeploy trong thực tế- duy trì ứng dụng uptime, trong khi triển khai một phiên bản mới của một ứng dụng, và phát hành đến môi trường chạy thật (production):**

CodeDeploy loại bỏ thời gian downtime của ứng dụng của bạn trong khi đang triển khai một phiên bản của ứng dụng mới. Có thể dễ dàng dừng và hoàn nguyên quá trình triển khai phần mềm về thời điểm trước đó (chưa xảy ra lỗi ) nếu xảy ra lỗi.

# CodePipeline

- CodePipeline tự động hóa quá trình phát triển phần mềm.
- ✓ Nhanh chóng phân phối các tính năng và các bản cập nhật mới
- ✓ Tích hợp với CodeBuild để chạy builds và unit tests
- ✓ Tích hợp với CodeCommit để lấy source code
- ✓ Tích hợp với CodeDeploy để triển khai những thay đổi của ứng dụng của bạn



Code Pipeline

**Ứng dụng CodePipeline trong thực tế- Thêm sự tự động hóa để xây dựng, kiểm thử(test) và triển khai ứng dụng:**  
DEV-TEST- PROD-> Khi kết hợp với các công cụ phát triển phần mềm khác, CodePipeline giúp các nhóm phát triển thực hiện các công cụ DevOps, tự động kiểm thử (testing) và triển khai code đến với môi trường chạy thật của ứng dụng.

# X-RAY

X-Ray giúp bạn gỡ lỗi(debug) các ứng dụng đang chạy trong môi trường thật (production applications).

- ✓ Phân tích và gỡ lỗi(debug) các ứng dụng đang chạy trong môi trường thật (production applications).
- ✓ Tạo biểu đồ các thành phần của ứng dụng, giúp bạn xem các mối quan hệ giữa dịch vụ và tài nguyên trong ứng dụng của bạn theo thời gian thực



- ✓ Hiển thị các yêu cầu điểm cuối đến điểm cuối của ứng dụng

**Ứng dụng X-Ray trong thực tế:** X-Ray có thể giúp bạn tạo biểu đồ theo dõi các yêu cầu được thực hiện tới RDS database từ bên trong ứng dụng của bạn. Bạn có thể theo dõi thông tin về các truy vấn SQL được tạo ra và nhiều vấn đề khác.

# Tổng kết

- 1) Cloud9 cho phép bạn viết code bên trong một môi trường phát triển phần mềm tích hợp (IDE) từ bên trong giao diện web của bạn
- 2) CodeCommit là một dịch vụ kiểm soát nguồn, với quy mô vô cùng linh hoạt và bảo mật để lưu trữ các kho Git repositories riêng.
- 3) CodeBuild cho phép bạn xây dựng và kiểm thử (test) ứng dụng source code của bạn.
- 4) CodeDeploy quản lý triển khai code đến dịch vụ compute services trong cloud hoặc cho các servers ngay tại chỗ.
- 5) CodePipeline tự động hóa quá trình phát triển phần mềm.
- 6) X-Ray giúp bạn gỡ lỗi(debug) các ứng dụng đang chạy trong môi trường thật (production applications).

# Tìm hiểu dịch vụ triển khai, quản lý, và tự động hóa cơ sở hạ tầng hệ thống AWS

## Tổng quan chung bài học



- **Lợi ích của dịch vụ triển khai và quản lý cơ sở hạ tầng IT**

- ✓ Các dịch vụ này giúp bạn nhanh chóng thiết lập các ứng dụng mới, tự động hóa trong việc quản trị cơ sở hạ tầng, và cung cấp khả năng hiển thị theo thời gian thực về tình trạng hệ thống



# Bạn có biết về Infrastructure as Code (IaC)?

- IaC cho phép bạn viết một kịch bản (script) để tạo các tài nguyên trong AWS. Lợi ích của nó là giúp bạn tạo các tài nguyên trong một cách là có thể tái sử dụng lại và giúp tiết kiệm thời gian, công sức.

```
“MyBucket”: {  
    “Type” : “AWS::S3::Bucket”  
}
```

**JSON Script**

```
MyBucket :  
  Type : AWS::S3::Bucket
```

**YAML Script**



**MyBucket**

Không cần phải sử dụng trình quản trị S3 trong trình duyệt Web AWS console (S3 Management Console) để tạo một buckket

# CloudFormation

CloudFormation cho phép bạn tạo các tài nguyên AWS sử dụng Infrastructure as Code (IaC)

- ✓ Cung cấp một quá trình lặp lại trong việc tạo các tài nguyên
- ✓ Làm việc với hầu hết các dịch vụ của AWS (AWS services)



- ✓ Tạo các mẫu code chương trình (templates) cho các tài nguyên AWS mà bạn muốn tạo

CloudFormation



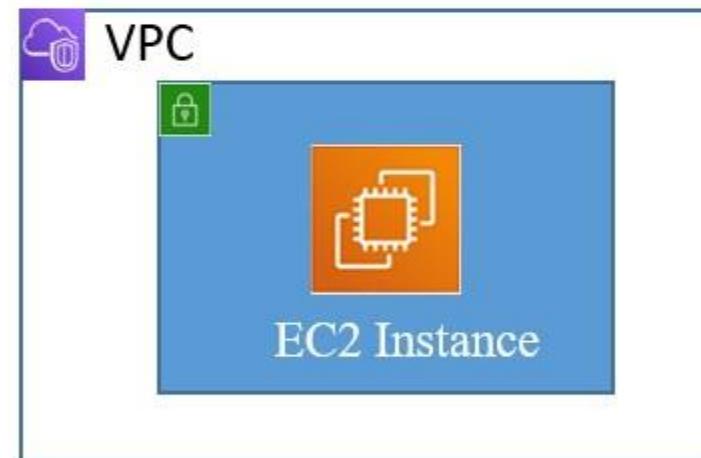
Template      Stack

# Sử dụng CloudFormation trong thực tế

Bạn có thể sử dụng CloudFormation để tự động hóa tạo một máy chủ EC2 instance trong tài khoản (Account )AWS của bạn



CloudFormation Template



Stack được tạo dựa trên mẫu code chương trình(template)

# Elastic Beanstalk

**Elastic Beanstalk cho phép bạn triển khai các ứng dụng web của bạn và các dịch vụ web trong AWS Cloud nhanh chóng.**

- ✓ Sử dụng một tổ hợp các dịch vụ để tạo các tài nguyên trong AWS
- ✓ Tự động xử lý việc triển khai các ứng dụng



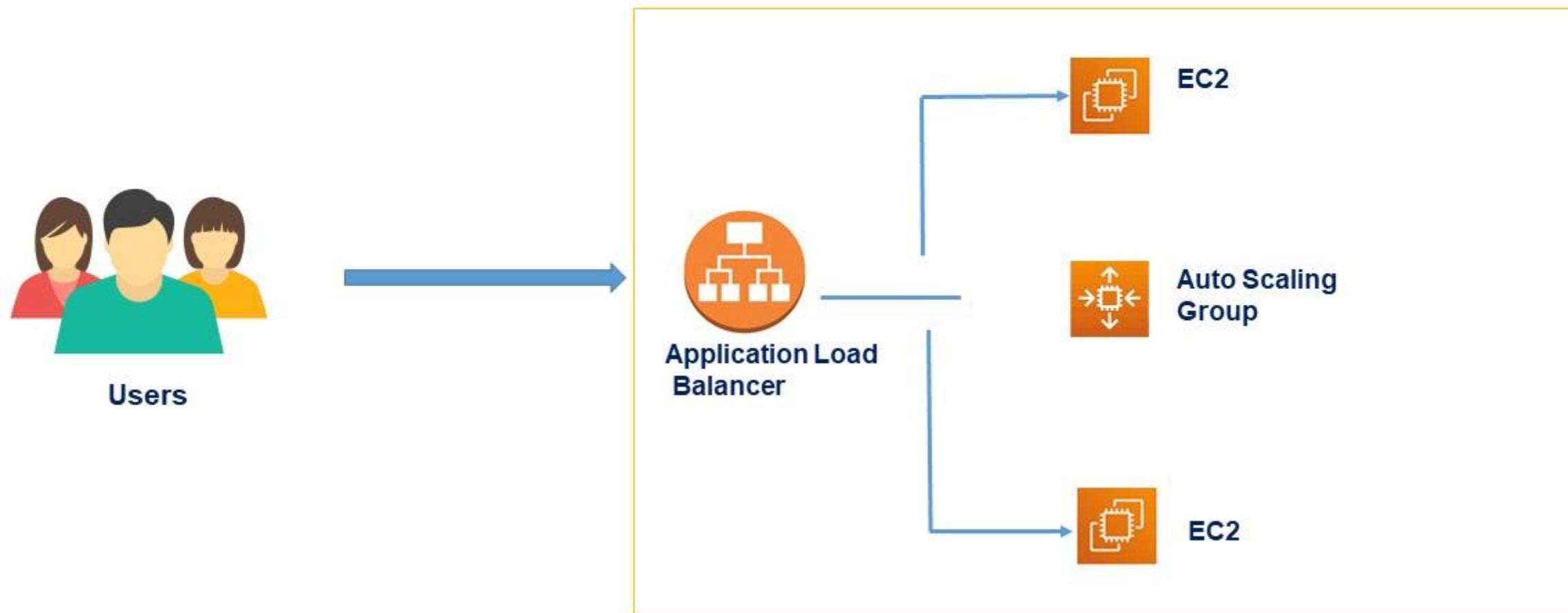
- ✓ Tự động giám sát trạng thái sức khỏe của ứng dụng qua màn hình health dashboard

**Elastic Beanstalk**

# Sử dụng Elastic Beanstalk trong thực tế

- Nhanh chóng triển khai một dịch vụ ứng dụng Java-Based web trong AWS cloud:

Sau khi bạn tải(upload) java code của bạn, sử dụng Elastic Beanstalk để triển khai ứng dụng bao gồm các thành phần dịch vụ mà aws cung cấp như: Ec2, Load blancing, Auto Scaling, và Tự động giám sát trạng thái sức khỏe của ứng dụng qua màn hình health dashboard.



# OpsWorks

**OpsWork cho phép bạn sử dụng các công cụ Chef và Puppet để tự động hóa các cấu hình các cho máy chủ(servers) của bạn và triển khai code**

- ✓ Triển khai code và quản trị các ứng dụng



- ✓ Quản trị các máy chủ tại chỗ, hoặc EC2 instances trong AWS Cloud

- ✓ Làm việc với công cụ Chef và puppet để tự động hóa các cấu hình hệ thống máy chủ

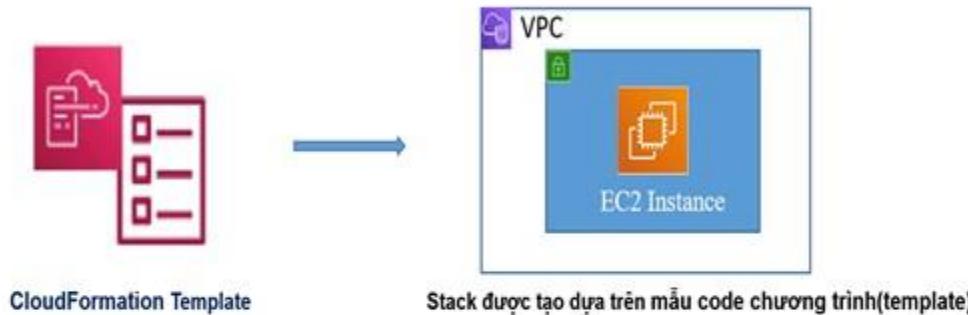


## Ứng dụng OpsWorks trong thực tế:

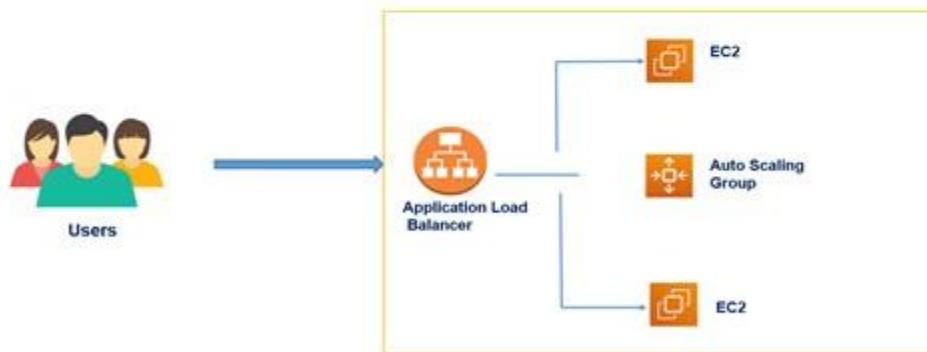
- 1) Tự động hóa các cấu hình phần mềm ứng dụng và quản trị cơ sở hạ tầng máy chủ cho ứng dụng của bạn
- 2) Cho phép bạn tạo/viết các kịch bản(Scripts) để tự động hóa việc cài đặt cấu hình các ứng dụng chạy trong máy chủ của bạn

# Tổng kết

1) CloudFormation cho phép bạn tạo các tài nguyên AWS sử dụng Infrastructure as Code (IaC)



2) Elastic Beanstalk cho phép bạn triển khai các ứng dụng web của bạn và các dịch vụ web trong AWS Cloud nhanh chóng.



3) OpsWork cho phép bạn sử dụng các công cụ Chef và Puppet để tự động hóa các cấu hình các cho máy chủ(servers) của bạn và triển khai code



# Thực hành tạo một Cơ sở dữ liệu DynamoDB Table sử dụng Cloudformation

- Trong tình huống của bài thực hành này, Giám đốc công ty Labogini đang tìm kiếm cách để xây dựng một ứng dụng web giúp quản lý kho cung ứng bán lẻ của anh ấy, và anh ấy muốn tìm kiếm sự giúp đỡ trong việc cài đặt, cấu hình hạ tầng CSDL, CSDL này sẽ lưu trữ các dữ liệu của ứng dụng.

Bạn sẽ giúp anh ấy bằng cách sử dụng Cloudformation để viết code cho việc tạo CSDL DynamoDB, giúp lưu trữ dữ liệu kho cung ứng bán lẻ cho ứng dụng của anh ấy. Qua bài thực hành này bạn sẽ hiểu được cách tạo cơ sở hạ tầng AWS Cloud sử dụng code.

- Các bước làm trong bài thực hành:**

- Tạo một file cloudFormation Template
- Tạo CloudFormation Stack
- Xác nhận đã có thể tạo được DynamoDB

# Tạo một DynamoDB table sử dụng cloudFormation

AWS Cloud



AWSTemplateFormatVersion: 2010-09-09

Description: CloudFormation Template To Create Labogini's Inventory DynamoDB Table

Resources:

InventoryTable:

Type: AWS::DynamoDB::Table

Properties:

TableName: Inventory

AttributeDefinitions:

-  
AttributeName: !Ref HashKeyElementName

AttributeType: !Ref HashKeyElementType

KeySchema:

-  
AttributeName: !Ref HashKeyElementName

KeyType: HASH

ProvisionedThroughput:

ReadCapacityUnits: 5

WriteCapacityUnits: 5

Parameters:

HashKeyElementName:

Type: String

Default: InventoryId

Description: Hash Key Name

HashKeyElementType:

Type: String

Default: S

Description: Hash Key Type

Outputs:

Inventory:

Description: Labogini's Inventory Table

Value: !Ref InventoryTable

## **Giải pháp**

Log in vào AWS Management Console sử dụng tài khoản của bạn.

Tạo file : acg-dynamodb-template.yaml.

Tạo CloudFormation Stack

Từ trên cùng của AWS console tại search bar, tìm kiếm dịch vụ CloudFormation.

Click Create stack > với new resources (standard).

Lựa chọn Template is ready.

Lựa chọn Upload a template file.

Click Choose file.

Lựa chọn acg-dynamodb-template.yaml file từ máy tính của bạn.

Click Open.

Click Next.

Cho Stack name, đặt tên là: MyStack.

Click Next.

Trong trang Configure stack options để tất cả là mặc định, và click Next.

Trong trang review MyStack, click Create stack.

Click the refresh icon phía bên phải của Events list để kiểm tra tình trạng của stack đang chạy.

Note: Nó sẽ mất một vài phút để tạo tài nguyên trong AWS Cloud.

Xác nhận DynamoDB Table đã được tạo

Một khi stack đã được tạo, sử dụng search bar trên cùng của AWS console để tìm kiếm dịch vụ DynamoDB.

Trong DynamoDB phía bên trái menu, click Tables.

Click vào Inventory table. Và nó sẵn sàng để nhập dữ liệu và sử dụng.

# Dịch vụ hàng đợi và lưu trữ thông điệp Simple Queue Service(SQS)

Tổng quan chung bài học

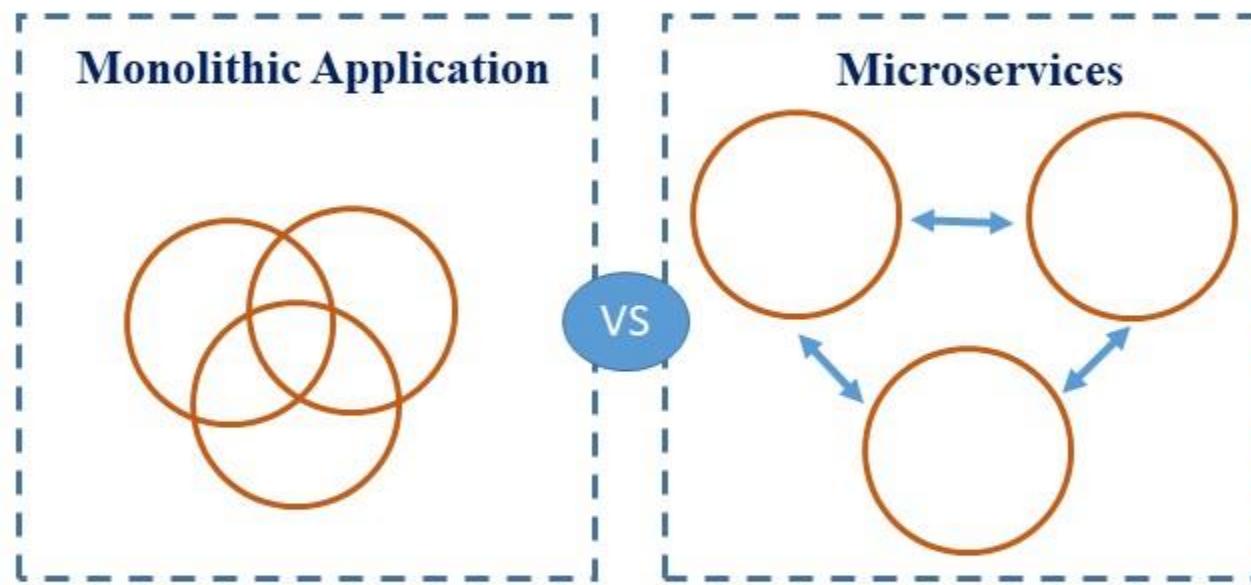
1  
**Simple Queue  
Service(SQS)**

2  
**Tổng kết**



# Bạn đã bao giờ nghe về loose coupling

Coupling định nghĩa là sự phụ thuộc lẫn nhau hoặc sự kết nối giữa các thành phần của một hệ thống.  
Loose coupling giúp giảm nguy cơ rủi ro xảy ra các lỗi giữa các thành phần



- ✓ **Tightly coupling:** Các thành phần có sự phụ thuộc cao lẫn nhau
- ✓ **Loosely coupling:** Các thành phần được kết nối với nhau, nhưng không phụ thuộc vào nhau

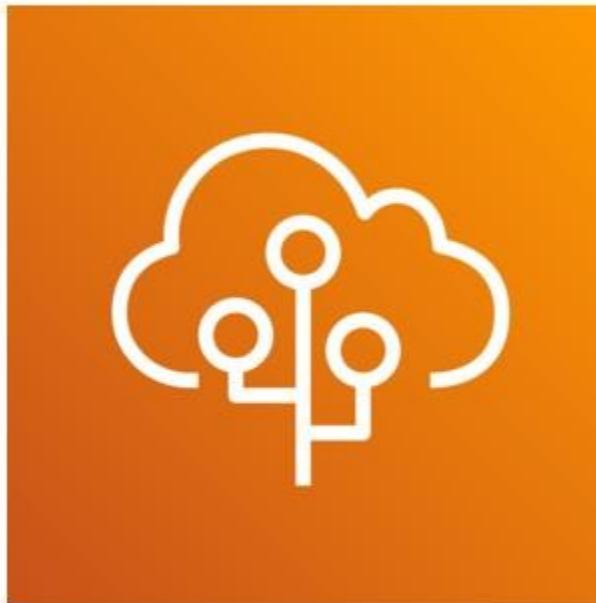
**Queues được sử dụng là thành phần trung gian giúp kết nối các ứng dụng dịch vụ với nhau, trong hệ thống loosely coupled systems**



# Simple Queue Service(SQS)

SQS là một dịch vụ hàng đợi và lưu trữ thông điệp, nó cho phép bạn xây dựng hệ thống loosely coupled systems

- ✓ Cho phép sự kết nối, giao tiếp giữa các thành phần sử dụng các thông điệp(messages)
- ✓ Các thành phần ứng dụng (hoặc các nhà sản xuất) có thể thêm các thông điệp (messages) vào trong hàng đợi



- ✓ Các thông điệp (messages) được xử lý theo cách không đồng bộ

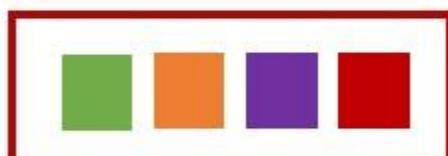
# Sử dụng SQS trong thực tế

Xây dựng một ứng dụng chuyển tiền, hoạt động tốt dưới áp lực phải xử lý một lượng tải trọng lớn, từ các yêu cầu của người dùng

SQS giúp bạn phát triển một ứng dụng, nó gọi là loose coupling cho phép các thành phần ứng dụng gửi, lưu trữ, và nhận các thông điệp(messages). Sự sử dụng của một thông điệp hàng đợi, giúp cải thiện hiệu xuất và khả năng mở rộng của hệ thống



Tạo yêu cầu  
chuyển tiền



Yêu cầu được thêm vào hàng đợi



Amazon SQS

Sẽ có thể có các yêu cầu của người dùng  
khác phía trước hoặc đằng sau bạn



Các yêu cầu được xử lý theo thứ tự  
vào trước- ra trước (First-in-first-out(FIFO))



Sau một khoảng  
thời gian, bạn của bạn  
nhận được tiền mà bạn  
đã chuyển khoản

# Tổng kết

## Simple Queue Service(SQS)

SQS là một dịch vụ hàng đợi và lưu trữ thông điệp, nó cho phép bạn xây dựng hệ thống loosely coupled systems



# Dịch vụ gửi thông điệp(Messaging) SNS và SES

Tổng quan chung bài học

1  
Simple Notification Service(SNS)

2  
Simple Email Service (SES)

3  
Tổng kết



**Đôi khi, người dùng các ứng dụng của bạn cần được thông báo khi một số sự kiện nhất định xảy ra**



# Simple Notification Service(SNS)

SNS cho phép bạn gửi emails và các tin nhắn điện thoại từ các ứng dụng của bạn

- ✓ Gửi emails và các tin nhắn điện thoại
- ✓ Publish thông điệp (messages) đến một chủ đề (topic)



SNS



- ✓ Người đăng ký(subscribers) nhận thông điệp thông báo (messages)

# Sử dụng SNS trong thực tế

Gửi một Email, khi tình trạng sử dụng CPU (CPU utilization) của một máy chủ EC2 instance lên đến 80%

SNS làm việc với CloudWatch khi mà một báo động đạt đến một ngưỡng nhất định, nó sẽ gửi một email thông báo đến người quản trị hệ thống administrator



CloudWatch  
Alarm



Email

# CloudTrail

**Cloudtrail theo dõi các hoạt động của người dùng và API calls trong tài khoản AWS của bạn**

- ✓ Thu thập logs và lưu giữ các hoạt động của các tài khoản người dùng
- ✓ Theo dõi các hoạt động của tài khoản người dùng thông qua console, SDKs, và CLI

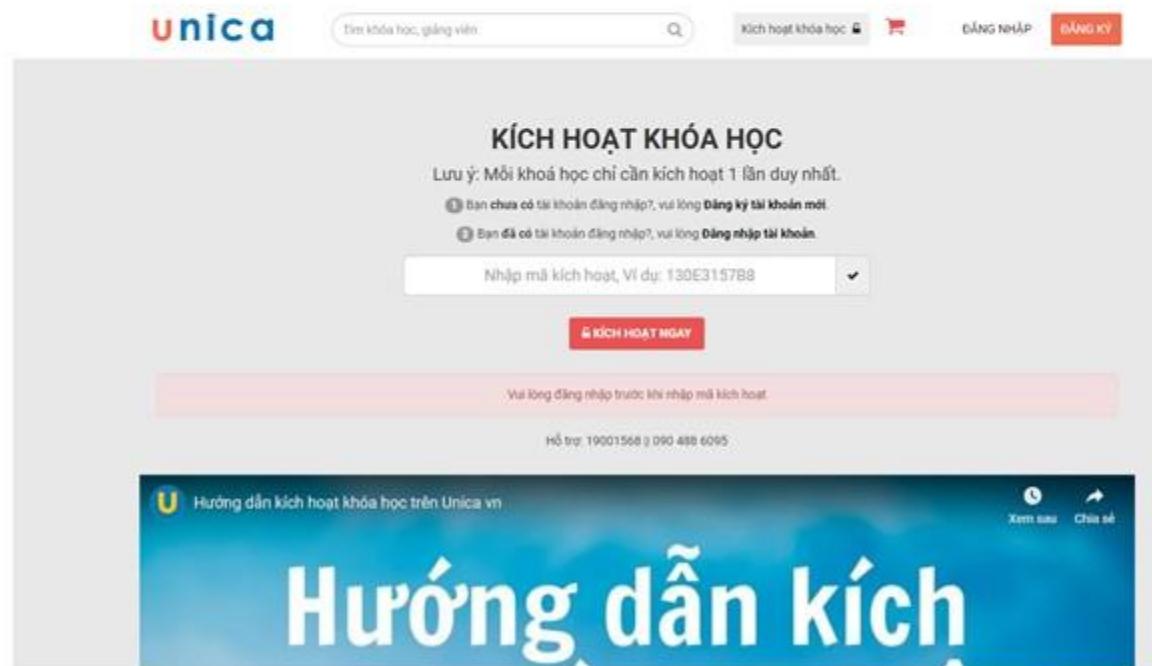


- ✓ Nhận diện tài khoản nào đã thực hiện các việc thay đổi
- ✓ Phát hiện ra các hoạt động bất thường trong tài khoản của bạn

# Sử dụng SES trong thực tế

Gửi một Email Marketing  
và theo dõi tỉ lệ mở hoặc  
click vào email

SES cho phép bạn gửi hàng loạt HTML Emails được định dạng phong phú, và có được những thông tin chi tiết có giá trị về hiệu quả của chiến dịch của bạn.



# Tổng kết

## Simple Notification Service(SNS)

SNS cho phép bạn gửi emails và các tin nhắn điện thoại từ các ứng dụng của bạn



## Simple Email Service(SES)

SES là một dịch vụ email, nó cho phép bạn gửi HTML Emails được định dạng phong phú từ ứng dụng của bạn

The screenshot shows the Unica website's activation page. At the top, there is a navigation bar with the Unica logo, a search bar, and links for 'Kích hoạt khóa học' (Activate course), 'ĐĂNG NHẬP' (Log in), and 'ĐĂNG KÝ' (Sign up). The main content area has a heading 'KÍCH HOẠT KHÓA HỌC'. It includes a note: 'Lưu ý: Mỗi khóa học chỉ cần kích hoạt 1 lần duy nhất.' Below this are two status messages:

- Bạn chưa có tài khoản đăng nhập?, vui lòng [Đăng ký tài khoản mới](#).
- Bạn đã có tài khoản đăng nhập?, vui lòng [Đăng nhập tài khoản](#).

A text input field is provided for entering the activation code, with the placeholder 'Nhập mã kích hoạt, Ví dụ: 130E3157B8'. A red button labeled 'KÍCH HOẠT NGAY' (Activate now) is below the input field. A pink banner at the bottom says 'Vui lòng đăng nhập trước khi nhập mã kích hoạt.' (Please log in before entering the activation code.). At the bottom of the page, there is footer information: 'Hỗ trợ: 19001568 || 090 488 6093', a 'Xem sau' (View later) link, and a 'Chia sẻ' (Share) link. A large blue banner at the bottom reads 'Hướng dẫn kích' (Activation guide).

# Tìm hiểu dịch vụ kiểm tra thông tin(auditing), giám sát(monitoring), và ghi lại hoạt động(Logging)

## Tổng quan chung bài học



- **Một bức tranh tổng quan về các dịch vụ:** Kiểm định an toàn (Auditing), theo dõi (Monitoring), và ghi lại nhật ký hoạt động (Logging) của hệ thống IT.

➤ Tại sao bạn cần phải có các hệ thống auditing, Monitoring, Logging?

✓ Bởi vì các dịch vụ này rất quan trọng, nó cho bạn có một cái nhìn bên trong các hệ thống, dịch vụ có đang hoạt động ổn định không? Và giúp bạn chủ động tìm kiếm các giải pháp để xử lý các lỗi hệ thống.



# Câu hỏi

- Bạn có thể trả lời nhiều câu hỏi sử dụng auditing, monitoring và logging services trong AWS cloud

**1** Người dùng nào?, ai đã đăng nhập làm các thay đổi qua AWS Management Console?

**2** Tình trạng hoạt động của CPU, Ram của EC2 instance hiện tại đang có tải trọng là bao nhiêu % sử dụng?

**3** Cái gì là nguyên nhân gốc rễ gây lên lỗi của một ứng dụng này

**4** Cái đường dẫn thực thi câu lệnh nào đã tạo ra lỗi này?

# CloudWatch

CloudWatch là một bộ sưu tập các ứng dụng, nó giúp bạn giám sát và theo dõi các tài nguyên trong AWS cloud

- ✓ Thu thập các số liệu(metrics), logs, và các sự kiện(events)



- ✓ Phát hiện sự bất thường trong môi trường hệ thống của bạn

- ✓ Thiết đặt các báo động

- ✓ Hiển thị nhật ký(logs)

CloudWatch

# Các thành phần của CloudWatch

Thiết đặt các  
cảnh báo

1 CloudWatch Alarms

Giám sát logs  
ứng dụng

2 CloudWatch Logs

Hiện thị biến đổi thu thập thông tin từ  
các số liệu, về tình trạng hoạt động  
cũng như hiệu suất của cơ sở hạ tầng  
AWS cloud, theo thời gian thực,  
trong bảng thông tin CloudWatch

3 CloudWatch Metrics

Kích hoạt một sự  
kiện dựa trên một  
điều kiện

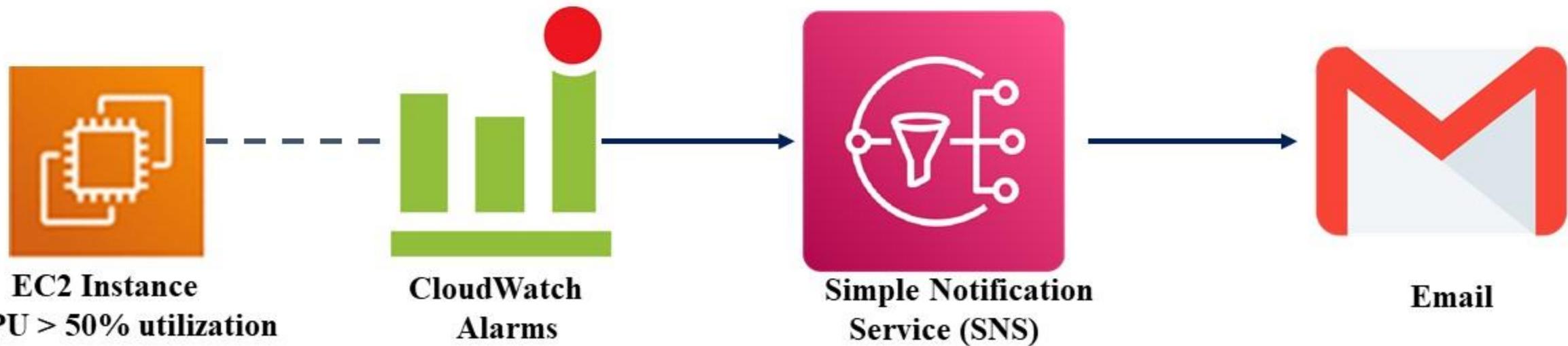
4 CloudWatch Events

# Sử dụng CloudWatch trong thực tế

## A) Trường hợp 1

Cung cấp sự theo dõi các hoạt động của EC2 Instances theo thời gian thực

CloudWatch Alarms có thể thông báo đến bạn nếu một EC2 Instance bị dừng hoạt động (Stopped state) hoặc tình trạng hoạt động của máy chủ ảo đang bị quá tải



# Sử dụng CloudWatch trong thực tế

## B) Trường hợp 2

Bạn sẽ nhận một email thông báo, bất cứ khi nào mà tài khoản root của bạn có sự hoạt động

CloudWatch event rule thông báo gửi email đến bạn bất cứ khi nào tài khoản root user API được phát hiện ra là đang có sự hoạt động trong tài khoản

Root user sign in

Email  
abcd@company.com

Password  
.....

Sign In

[Sign in to a different account](#)

[Forgot your password?](#)

Root User  
Login Event



CloudWatch  
Alarms



Simple Notification  
Service (SNS)



Email

## Chúng ta làm một Demo

- Trong demo này, bạn sẽ xem AWS Platform nhìn như thế nào, bạn cũng sẽ học được cách, làm thế nào để bạn làm việc với hệ thống AWS cloud của bạn. Demo này hướng dẫn cách tạo một cảnh báo thanh toán (billing alarm) sử dụng dịch vụ CloudWatch.

# CloudTrail

**Cloudtrail theo dõi các hoạt động của người dùng và API calls trong tài khoản AWS của bạn**

- ✓ Thu thập logs và lưu giữ các hoạt động của các tài khoản người dùng
- ✓ Theo dõi các hoạt động của tài khoản người dùng thông qua console, SDKs, và CLI



- ✓ Nhận diện tài khoản nào đã thực hiện các việc thay đổi
- ✓ Phát hiện ra các hoạt động bất thường trong tài khoản của bạn

# Sử dụng CloudTrail trong thực tế

Theo dõi một thời gian,  
một sự kiện cụ thể đã  
xảy ra trong tài khoản  
của bạn

Bạn có thể theo dõi thời gian một sự kiện cụ thể đã xảy ra trong tài khoản của bạn. Vì vậy, điều này cho phép bạn xử lý sự cố dựa trên sự kiện trong 90 ngày qua bằng cách sử dụng nhật ký lịch sử sự kiện của CloudTrail(CloudTrail event history log). Và bạn có thể thu hẹp thời gian cụ thể một sự kiện đã xảy ra trên cơ sở trong mỗi khu vực (Region).

# Các đối tượng bạn có thể sử dụng CloudTrail để theo dõi



Người dùng (Username)



Time



IP address



Access key



Region



Error code

# Tổng kết

## CloudWatch

CloudWatch là một bộ sưu tập các ứng dụng, nó giúp bạn giám sát và theo dõi các tài nguyên trong AWS cloud

CloudWatch Alarms

CloudWatch Logs

CloudWatch Metrics

CloudWatch Events

## Cloudtrail

Cloudtrail theo dõi các hoạt động của người dùng và API calls trong tài khoản AWS của bạn



# Giới thiệu tổng quan về bảo mật và tuân thủ(Security and Compliance)

## 1) Mô hình chia sẻ trách nhiệm trong bảo mật AWS Cloud (Shared Responsibility Model)



Trách nhiệm của AWS



Trách nhiệm của bạn

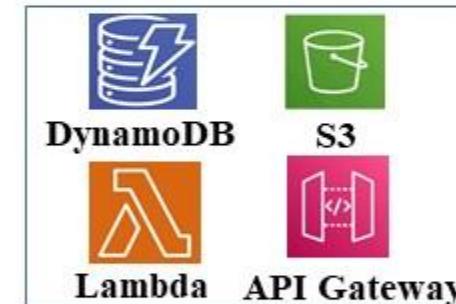
## 2) Tìm hiểu về Identity and Access Management (IAM) cho phép bạn kiểm soát quyền hạn truy cập các dịch vụ và tài nguyên AWS của bạn.



Users



Policy



## 3) Tìm hiểu về các dịch vụ bảo mật



AWS WAF



Amazon Macie

# Tìm hiểu mô hình chia sẻ trách nhiệm trong bảo mật AWS Cloud (Shared Responsibility Model)

## Tổng quan chung bài học

1  
**Mô hình chia sẻ  
trách nhiệm**

2  
**Tổng kết**



# Mô hình chia sẻ trách nhiệm (Shared Responsibility Model)

Trong môi trường public cloud, có một trách nhiệm chia sẻ bảo mật giữa bạn và AWS



Trách nhiệm của AWS



Bảo mật hệ thống Cloud



Trách nhiệm của bạn



Bảo mật trong Cloud

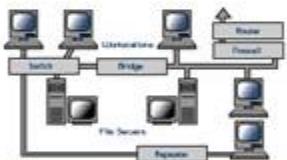
# Bảo mật hệ thống Cloud



1

Cơ sở hạ tầng toàn cầu AWS  
(AWS Global Infrastructure)

AWS chịu trách nhiệm cho cơ sở hạ tầng toàn cầu: Region, các địa điểm đặt/thuê trung tâm dữ liệu (Edge Locations)



3

Hệ thống hạ tầng mạng  
(Networking Components)

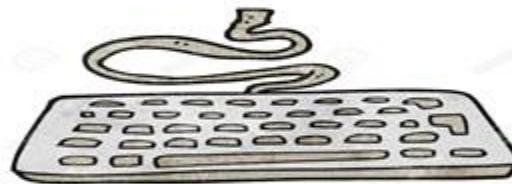
AWS chịu trách nhiệm bảo trì hệ thống mạng, máy chủ, các thành phần: máy phát điện, hệ thống bộ lưu điện UPS, hệ thống điều hòa(CRAC), hệ thống PCCC, VVV..



2

Bảo vệ trung tâm dữ liệu  
(Building Security)

AWS kiểm soát, bảo vệ các trung tâm dữ liệu, là nơi mà lưu trữ các dữ liệu của bạn



4

Phần mềm  
(Software)

AWS chịu trách nhiệm cho quản trị toàn bộ Các dịch vụ như RDS, S3, ECS, Lambda, và lỗi(patching) của các máy chủ vật lý(host operating systems), và các điểm truy cập dữ liệu(data access endpoints)

# Bảo mật trong Cloud

1

Dữ liệu ứng dụng  
(Application Data)

**Bạn chịu trách nhiệm cho việc quản trị các dữ liệu ứng dụng, bao gồm các tùy chọn mã hóa**

3

Bản vá lỗi (Patching)

**Bạn chịu trách nhiệm quản trị hệ điều hành(OS) trong các máy chủ EC2 instances, như cập nhật các bản vá lỗi để đảm bảo sự bảo mật kịp thời**

5

Luồng truy cập mạng  
(Network Traffic)

**Bạn chịu trách nhiệm cho bảo mật, quản trị các luồng truy cập vào ra trong hệ thống mạng ảo VPC, bao gồm cấu hình security group, tường lửa Firewall**

2

Cấu hình bảo mật  
(security Configuration)

4

Quản lý định danh và truy cập  
(Identity and access Management)

**Bạn chịu trách nhiệm cho việc bảo mật ứng dụng, quản lý định danh và truy cập các tài nguyên trong tài khoản AWS của bạn**

6

Cài đặt phần mềm  
(installed Software)

**Bạn chịu trách nhiệm cho các code ứng dụng (application code), cài đặt phần mềm..vv, bạn nên thường xuyên tìm, quyết (scan) các yếu điểm dễ bị tổn thương trong code của bạn**

# Ai chịu trách nhiệm cho cái gì?



Cấu hình tường lửa(Firewall)



Bảo mật phần cứng và trung tâm dữ liệu



Đảm bảo mã hóa ổ lưu trữ EBS volumes



Các phiên bản ngôn ngữ Lập trình của Lambda



Sao lưu(backup) CSDL trong RDS



Cập nhật các bản firmware cho các máy chủ vật lý chứa các máy chủ ảo EC2 instances



Quản trị hệ thống cơ sở hạ tầng mạng vật lý



Cập nhật các bản vá lỗi cho hệ điều hành chạy trong EC2



Hủy bỏ các thiết bị phần cứng, khi các thiết bị này đã hết hạn sử dụng

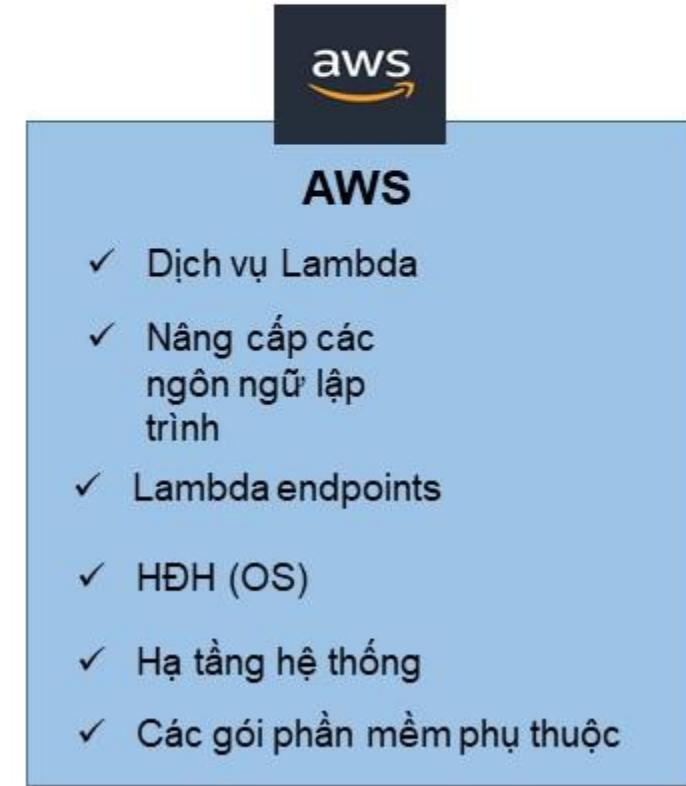
# Mô hình chia sẻ trách nhiệm EC2

Có một cái nhìn gần hơn về mô hình chia sẻ trách nhiệm với máy chủ EC2 instance



# Mô hình chia sẻ trách nhiệm Lambda

Có một cái nhìn gần hơn về mô hình chia sẻ trách nhiệm với dịch vụ Lambda



# Các trách nhiệm bảo mật nào được chia sẻ

## Quản lý các bản vá lỗi



**AWS**

Cài đặt các bản vá lỗi  
cho cơ sở hạ tầng



**Bạn**

Cài đặt các bản vá lỗi  
HĐH (OS) và ứng dụng

## Quản lý cấu hình



**AWS**

Cấu hình các thiết bị hạ tầng mạng



**Bạn**

Cấu hình CSDL và ứng dụng

## Nhận thức và đào tạo



**AWS**

Nhân viên AWS



**Bạn**

Nhân viên của bạn

# Làm thế nào để báo cáo trọng trường hợp phát hiện có sự xâm phạm các tài nguyên AWS

- Liên hệ AWS Trust & Safety team sử dụng Report Amazon AWS abuse form hoặc liên lạc gửi mail đến địa chỉ abuse@amazonaws.com



# Tổng kết

## Mô hình chia sẻ trách nhiệm

Trong public cloud, có mô hình chia sẻ trách nhiệm bảo mật giữa bạn và AWS



Trách nhiệm của AWS



Bảo mật hệ thống Cloud



Trách nhiệm của bạn



Bảo mật trong Cloud

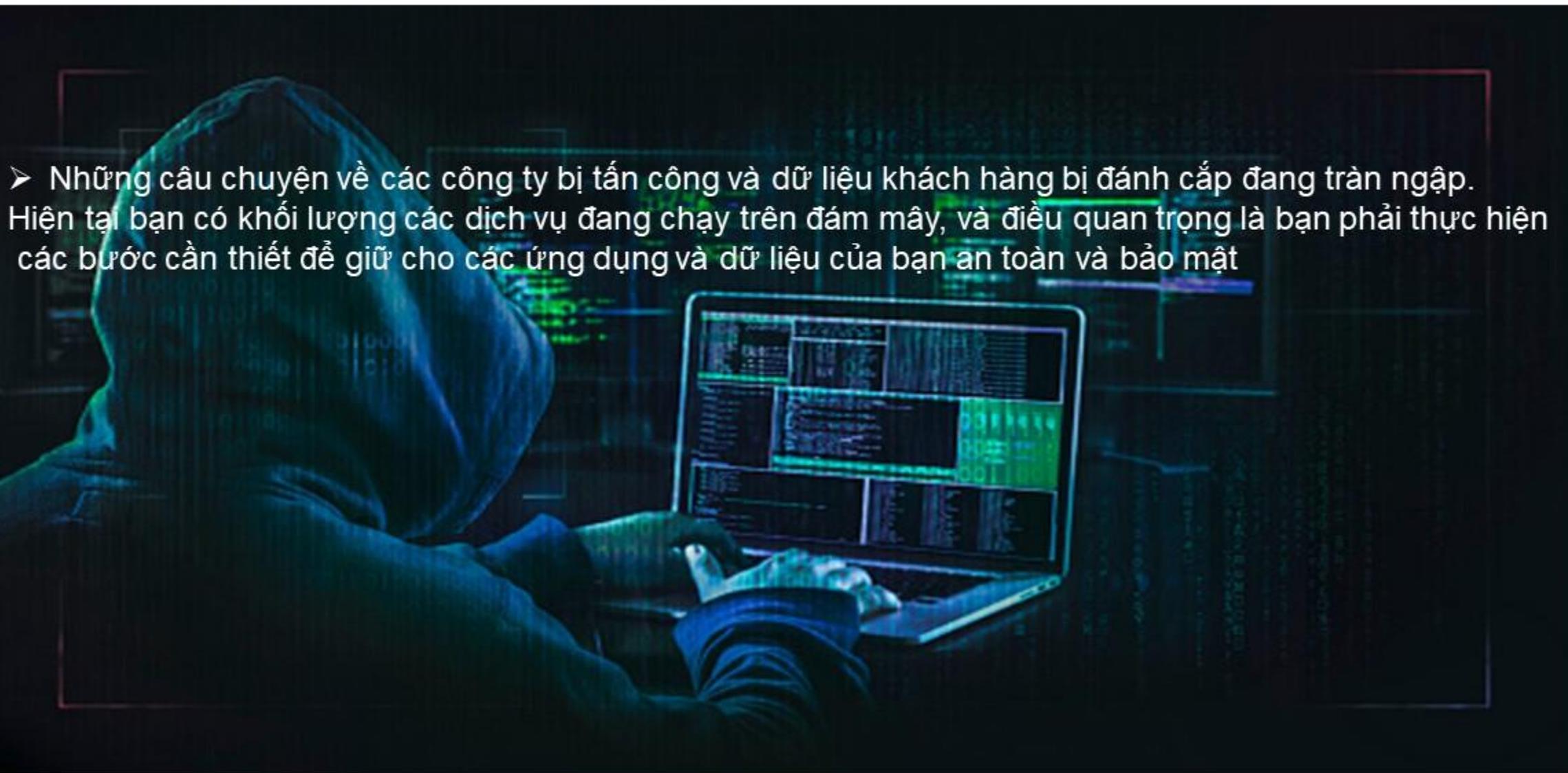
# Tìm hiểu IAM USERS

Tổng quan chung bài học



## Một bức tranh tổng quan

Tại sao bạn nên kiểm soát truy cập các dịch vụ & tài nguyên AWS của bạn.



- Những câu chuyện về các công ty bị tấn công và dữ liệu khách hàng bị đánh cắp đang tràn ngập. Hiện tại bạn có khối lượng các dịch vụ đang chạy trên đám mây, và điều quan trọng là bạn phải thực hiện các bước cần thiết để giữ cho các ứng dụng và dữ liệu của bạn an toàn và bảo mật

# Quản lý nhận dạng và truy cập Identity and Access Management(IAM)

IAM cho phép bạn kiểm soát truy cập vào các dịch vụ, tài nguyên AWS

- ✓ Giúp bạn bảo mật các tài nguyên đám mây
- ✓ Bạn định nghĩa người dùng ai truy cập cái gì



- ✓ Bạn định nghĩa người dùng có thể làm gì
- ✓ Một dịch vụ miễn phí

# Identities vs. Access



Nhận dạng(Identities)

Ai có thể truy cập các tài nguyên của bạn



- Root user
- Individual users
- Groups
- Roles

VS



Truy cập(Access)

Các tài nguyên nào họ có thể truy cập



- Chính sách (Policies)
- AWS managed policies
- Customer managed policies
- Permissions boundaries

# Xác thực (Authentication) ai “Who” vs được quyền (Authorization) cái gì (“What”)

Cái gì là xác thực  
(Authentication)

**Xác thực** là nơi bạn phải khai báo sự nhận dạng của bạn(username) và cung cấp mật khẩu>Password) cho sự đăng nhập vào 1 hệ thống.



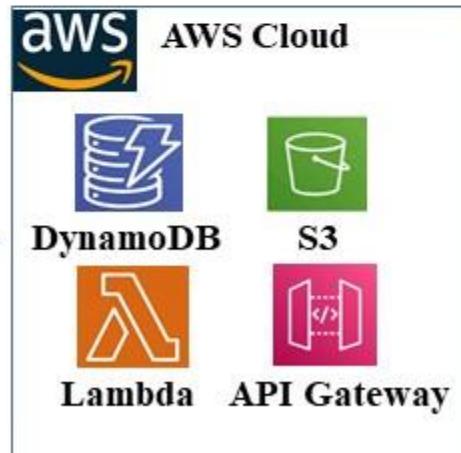
Ai (Who)

Cái gì là  
**Được quyền**  
(Authorization)

**Được quyền** định nghĩa các dịch vụ nào và tài nguyên nào được quyền truy cập vào.

**POLICY**

```
{  
  "Version": "...",  
  "Statement": [  
    {  
      "Action": "...",  
      "Effect": "Allow",  
      "Resource": "*"  
    }  
  ]  
}
```



Cái gì (What)

## Người dùng (Users)

Bạn có thể tạo Users trong IAM để đại diện cho người dùng và ứng dụng cần phải truy cập các tài nguyên AWS.



**Root user được tạo ra trong lần đầu tiên bạn tạo tài khoản trong AWS của bạn**  
**Những việc gì chỉ root user mới có thể làm được?**

- ✓ Đóng tài khoản AWS của bạn
- ✓ Thay đổi địa chỉ mail của tài khoản AWS của bạn
- ✓ Sửa đổi kế hoạch hỗ trợ của bạn



**Người dùng độc lập(individual users) được tạo trong IAM và được sử dụng cho các công việc hàng ngày.**  
**Những việc gì người dùng có thể làm được?**

- ✓ Thực hiện quản lý các công việc
- ✓ Truy cập các code ứng dụng
- ✓ Tạo, cấu hình EC2 instances
- ✓ Cấu hình CSDL trong RDS

**Lưu ý:** Những hoạt động sử dụng tài nguyên AWS người dùng độc lập(individual users) diễn ra trong tài khoản AWS của bạn được tính phí cho tài khoản của bạn



**Bạn có biết các ứng dụng có thể là người dùng (users)?**

- ✓ Bạn tạo một người dùng(user) trong IAM, vì vậy bạn có thể tạo một access keys cho một ứng dụng đang chạy tại chỗ và nó cần truy cập vào tài nguyên cloud của bạn

**Nguyên tắc phân quyền cho người dùng(Users), đó là cấp quyền truy cập tài nguyên & dịch vụ tối thiểu, cần thiết để họ có thể hoàn thành công việc**



Lập trình viên

AWS Cloud

DynamoDB      Organizations      Cost Explorer      Lambda      S3      API Gateway

**Lập trình viên chịu trách nhiệm cho phát triển phần mềm**



Quản lý dự án

AWS Cloud

DynamoDB      Organizations      Cost Explorer      Lambda      S3      API Gateway

**Quản lý dự án chịu trách nhiệm quản lý ngân sách, chi phí**

# Các phương pháp tốt nhất trong sử dụng IAM

1

## Kích hoạt sử dụng MFA cho người dùng quản lý có quyền hạn cao

Bạn nên kích hoạt sử dụng xác thực truy cập nhiều lớp (MFA) cho root user và các user quản lý

2

## Thực hiện đặt mật khẩu mạnh(password)

Bạn nên yêu cầu IAM users thường xuyên thay đổi mật khẩu và không sử dụng lại mật khẩu cũ.

3

## Tạo các users riêng thay vì sử dụng root

Bạn không nên sử dụng root user cho công việc hàng ngày

4

## Sử dụng roles cho Amazon EC2 instances

Bạn nên sử dụng role cho các ứng dụng chạy trong EC2 thay vì sử dụng access keys để cấu hình cấp quyền cho EC2 trong một thời gian dài

# Nhóm (Groups)

Một nhóm (Groups) là tập hợp của các IAM users, nó giúp bạn áp dụng các kiểm soát truy cập đến tất cả các thành viên.



Administrators

Quản trị hệ thống thực hiện các công việc quản trị như tạo các người dùng mới



Lập trình viên  
(Developers)

Lập trình viên sử dụng dịch vụ Compute và CSDL để phát triển phần mềm



Phân tích  
(Analysts)

Phân tích ngân sách và các báo cáo sử dụng dịch vụ.



**Lưu ý:** Không được lẫn lộn nhóm bảo mật cho EC2 với IAM groups. Bảo mật EC2 sử dụng tường lửa(firewall) như là AWS Security groups. Trong khi IAM Groups là tập hợp các users.

## Chú ý quan trọng

Sử dụng groups users để nhóm người dùng thực hiện các công việc giống nhau.

Quyền hạn truy cập tài nguyên, được áp dụng cho tất cả các thành viên trong nhóm

Sử dụng Policies và roles để cấp quyền truy cập cho groups

# Groups trong trong thực tế

Áp dụng kiểm soát truy cập giống nhau đến một số lượng lớn người dùng

Sử dụng nhóm (Groups) tiết kiệm thời gian bằng cách cho phép bạn áp dụng các kiểm soát truy cập giống nhau đến nhiều hơn một người dùng trong 1 lần thực hiện. Khi một người dùng không cần phải truy cập tài nguyên, bạn loại người dùng ra khỏi nhóm

# Tổng kết

## IAM

IAM cho phép bạn kiểm soát truy cập vào các dịch vụ, tài nguyên AWS



### Users

Bạn có thể tạo Users trong IAM để đại diện cho người dùng và ứng dụng cần phải truy cập các tài nguyên AWS.



### Groups

Một nhóm (Groups) là tập hợp của các IAM users, nó giúp bạn áp dụng các kiểm soát truy cập đến tất cả các thành viên.



# Tìm hiểu IAM Permissions

Tổng quan chung bài học



## Roles

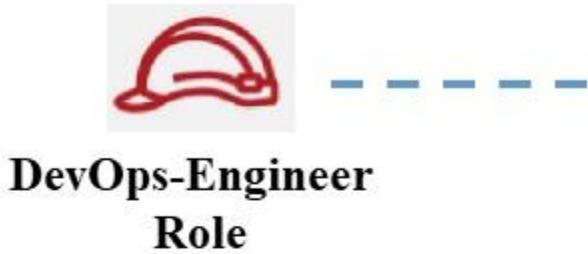
- Roles được định nghĩa là các quyền truy cập (access permissions), và là các giấy phép tạm thời có các quyền truy cập được đảm nhận bởi IAM user hoặc dịch vụ (service).



**DevOps-Engineer  
Role**



**Lambda-Execution  
Role**



Tạo code branch trong **CodeCommit**



Liệt kê pipelines trong **CodePipeline**



Liệt kê các files và thư mục của **S3 bucket**



Truy vấn dữ liệu trong **DynamoDB**



### Các mục cần ghi nhớ

- ✓ Bạn đảm nhận một role để thực hiện một công việc trong một phiên duy nhất
- ✓ Đảm nhận bởi người dùng(user) hoặc dịch vụ, mà cần đến role
- ✓ Truy cập được chỉ định sử dụng policies
- ✓ Bạn cấp quyền cho người dùng trong 1 tài khoản AWS, cho các tài nguyên trong tài khoản AWS khác

# Roles trong thực tế

Gắn một role cho một EC2 instance để cho phép máy chủ này truy cập vào S3

Bạn có thể gắn một role cho một EC2 instance, để nó cung cấp những đặc quyền (e.g., Tải file từ EC2 lên S3) cho các ứng dụng chạy trong EC2. Roles giúp bạn tránh phải chia sẻ và sử dụng access keys để cấu hình cấp quyền cho EC2 trong một thời gian dài, và bảo vệ các EC2 instances từ các truy cập trái phép.



Put (upload) objects  
Permission

# Policies

Bạn quản lý các phân quyền sử dụng tài nguyên và dịch vụ cho IAM users, groups và roles bằng cách tạo một policy Document trong định dạng JSON và gắn nó vào các đối tượng này



User



RDS



Developer Group



Cloud9



Role

AWSCloud9 Administrator Managed Policy



S3



# Roles trong thực tế

Bạn có thể giới hạn các users cụ thể truy cập đến Amazon S3 Bucket

Bạn có thể thêm một bucket policy trực tiếp đến một Amazon S3 bucket để cấp các quyền truy cập của IAM users cho bucket và các đối tượng trong bucket này

# Các phương pháp tốt nhất trong sử dụng IAM

1

## Kích hoạt sử dụng MFA cho người dùng quản lý có quyền hạn cao

Bạn nên kích hoạt sử dụng xác thực truy cập nhiều lớp (MFA) cho root user và các user quản lý

2

## Thực hiện đặt mật khẩu mạnh(password)

Bạn nên yêu cầu IAM users thường xuyên thay đổi mật khẩu và không sử dụng lại mật khẩu cũ.

3

## Tạo các users riêng thay vì sử dụng root

Bạn không nên sử dụng root user cho công việc hàng ngày

4

## Sử dụng roles cho Amazon EC2 instances

Bạn nên sử dụng role cho các ứng dụng chạy trong EC2 thay vì sử dụng access keys để cấu hình cấp quyền cho EC2 trong một thời gian dài

## Chúng ta làm một Demo

- Trong demo này hướng dẫn cách tạo group, user, và tìm hiểu nghĩa của role, policy.

# IAM Credential Report

IAM credential report liệt kê tất cả các người dùng(users) trong tài khoản AWS của bạn về các thông tin đăng nhập khác nhau của họ

- ✓ **Liệt kê users và tình trạng của passwords, access keys, và MFA devices**



- ✓ **Sử dụng cho việc kiểm định, và tuân thủ các quy định bảo mật, an toàn**

# Tổng kết

## Roles

- Roles được định nghĩa là các quyền truy cập (access permissions), và là các giấy phép tạm thời có các quyền truy cập được đảm nhận bởi IAM user hoặc dịch vụ (service).



## Policies

Bạn quản lý các phân quyền sử dụng tài nguyên và dịch vụ cho IAM users, groups và roles bằng cách tạo một policy Document trong định dạng JSON và gắn nó vào các đối tượng này

POLICY
<pre>{   "Version": "2012-10-17",   "Statement": [     {       "Effect": "Allow",       "Action": "s3:*",       "Resource": "*"     }   ] }</pre>
<b>JSON</b>

## Credential Report

IAM credential report liệt kê tất cả các người dùng(users) trong tài khoản AWS của bạn về các thông tin đăng nhập khác nhau của họ



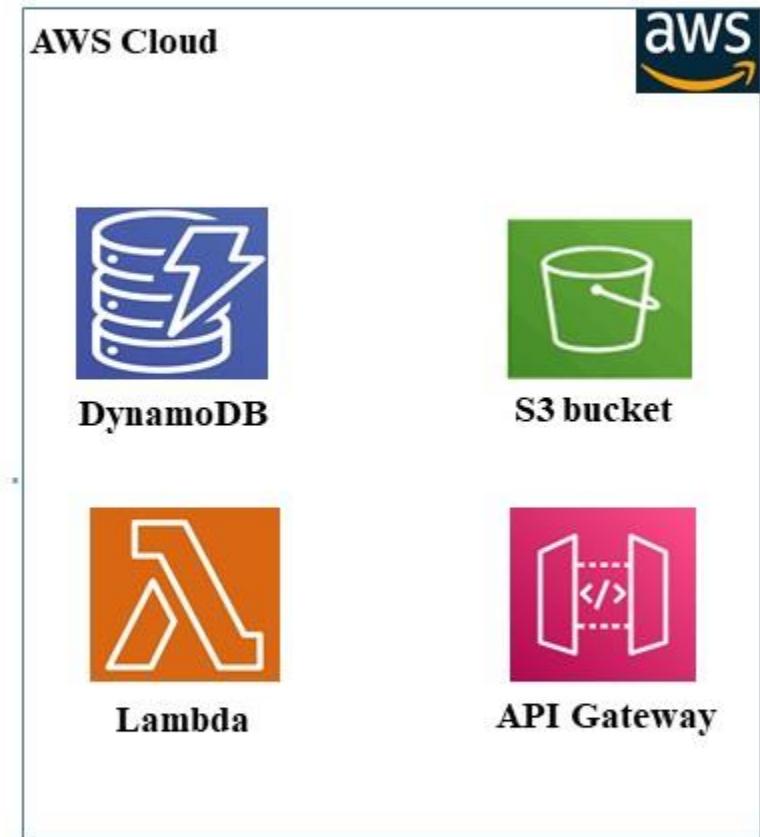
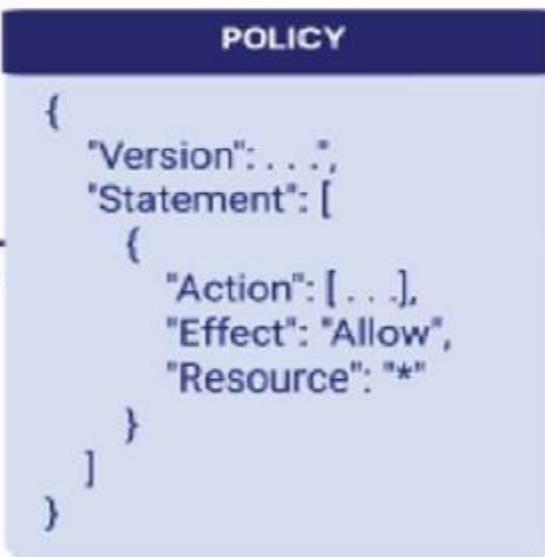
## Bài thực hành tạo Users và quản lý phân quyền (Permissions) sử dụng Groups và Policies trong IAM

- Trong một tình huống, giám đốc công ty Palocato tuyển bạn vào vị trí là một kỹ sư bảo mật cho hệ thống web app của anh ấy, hệ thống này cho phép các khách hàng đặt hàng online. Anh ấy mới tuyển thêm 4 kỹ sư phần mềm, anh ấy cần bạn giúp phân quyền cho các kỹ sư truy cập để phát triển web app trong dịch vụ AWS Lambda, và đảm bảo tính bảo mật là không được phép truy cập các dịch vụ khác trong tài khoản AWS. Bạn sẽ sử dụng AWS Identity và Access Management(IAM). Bạn sẽ nhóm users vào 1 nhóm và cấp quyền truy cập cho nhóm của 4 kỹ sư phần mềm sử dụng policies.

# Tạo Users và quản lý phân quyền (Permissions) sử dụng Groups và Policies trong IAM



Nhóm kỹ sư phần mềm  
Developer Group



Log in vào AWS Management Console sử dụng tài khoản AWS của bạn.

1. Chuyển hướng tới **IAM > Users**
2. Click **Policies** trong menu phía bên trái.
3. Click **Create policy**.
4. Click **Import managed policy** phía bên phải của trang .
5. Tìm kiếm và chọn **AWSLambda\_FullAccess**.
6. Click **Import**.
7. Kế tiếp **EC2**, click **Remove**.
8. Click **Next: Tags**.
9. Click **Next: Review**.
10. Đặt tên policy là *my\_dev\_access*.
11. Click **Create policy**.

#### Tạo một Group được kiểm soát qua một Customer Managed Policy

1. Click **User groups** in menu phía bên trái.
2. Click **Create group**, và nhập các giá trị sau:
  - **User group name:** nhập *developers*.
  - **Attach permissions policies:** chọn *my\_dev\_access*.
3. Click **Create group**.

#### Cho các Users vào nhóm (Group)

1. Click the **developers** group.
2. Bên dưới **Users** tab, click **Add users**.
3. Lựa chọn 4 developer users.
4. Click **Add users**.

# Tìm hiểu dịch vụ bảo mật ứng dụng ( Application Security Services)

Tổng quan chung bài học



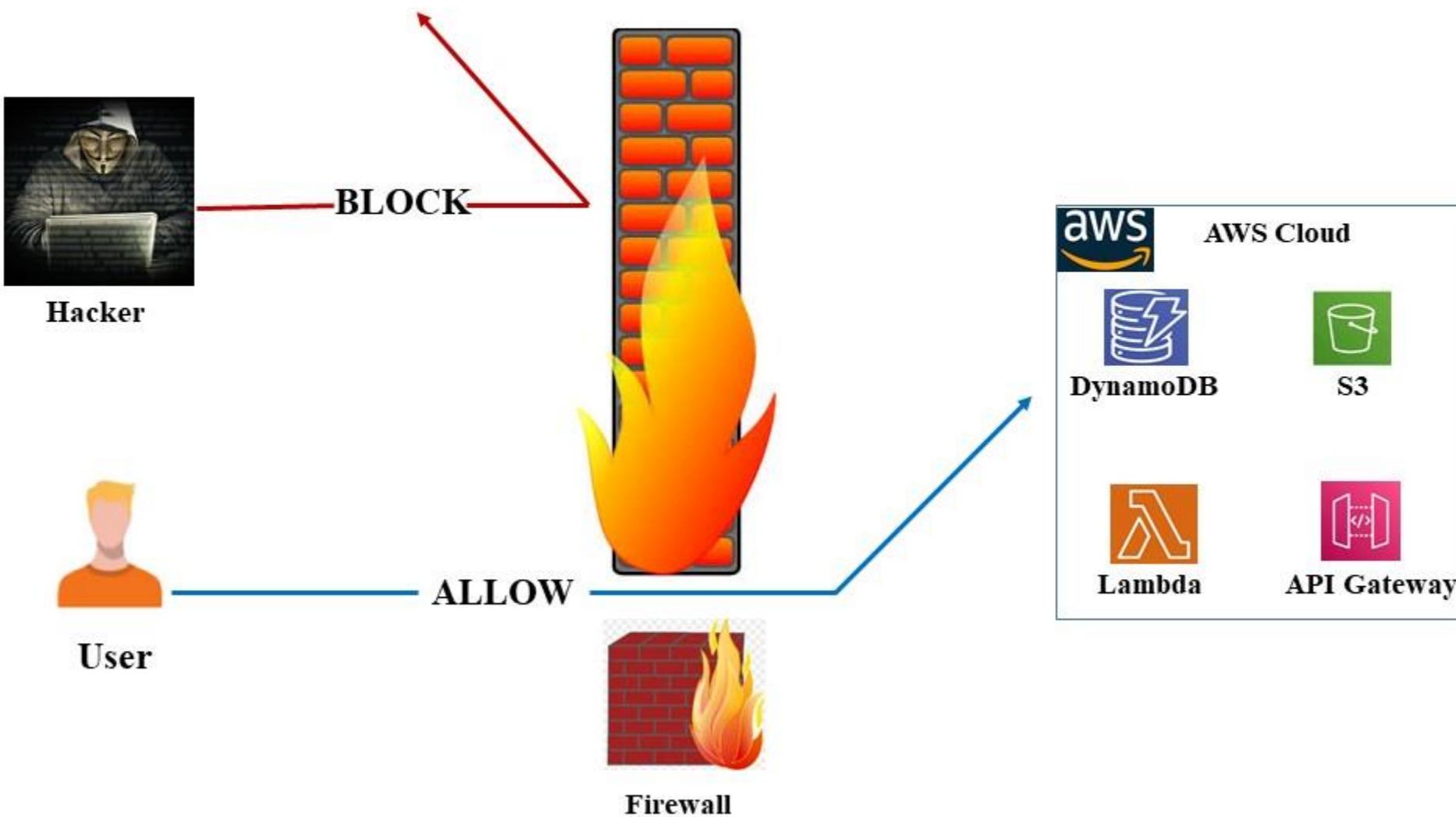
## Một bức tranh tổng quan

Tại sao bạn nên kiểm soát sự truy cập các dịch vụ và tài nguyên sử dụng các công cụ bảo mật.

- AWS có cung cấp sẵn sàng một vài công cụ bảo mật để giúp bạn theo dõi và bảo mật các tài nguyên của bạn.



# Tường lửa (Firewall) là gì?



# Web Application Firewall(WAF)

WAF giúp bạn bảo vệ các ứng dụng web chống lại các tấn công phổ biến từ ngoài internet

- ✓ Giúp bạn bảo mật các ứng dụng trong đám mây, chống lại các kiểu tấn công phổ biến
- ✓ Bảo vệ chống lại các tấn công SQL injection



**WAF**

- ✓ Bảo vệ chống lại các cuộc tấn công chèn các đoạn mã độc (cross-site scripting).

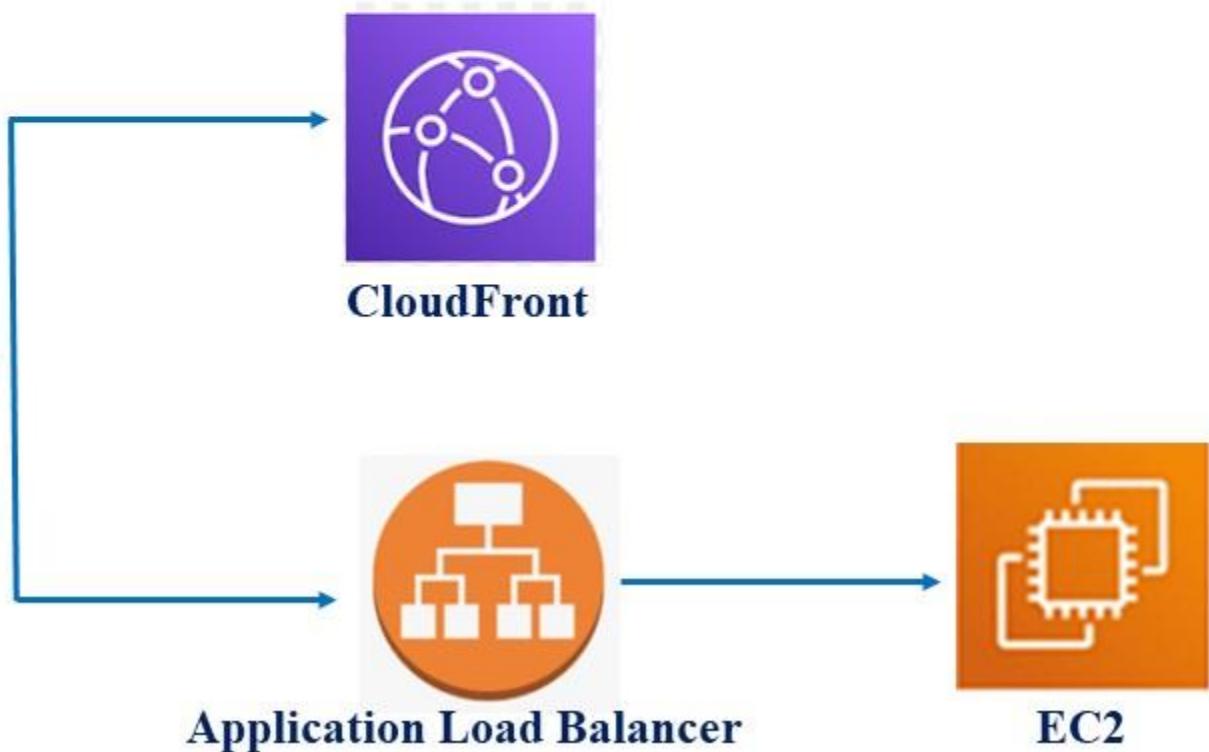
# WAF trong thực tế

- ✓ Bảo vệ ứng dụng web của bạn chống lại cuộc tấn công chèn các đoạn mã độc. (cross-site scripting)



WAF

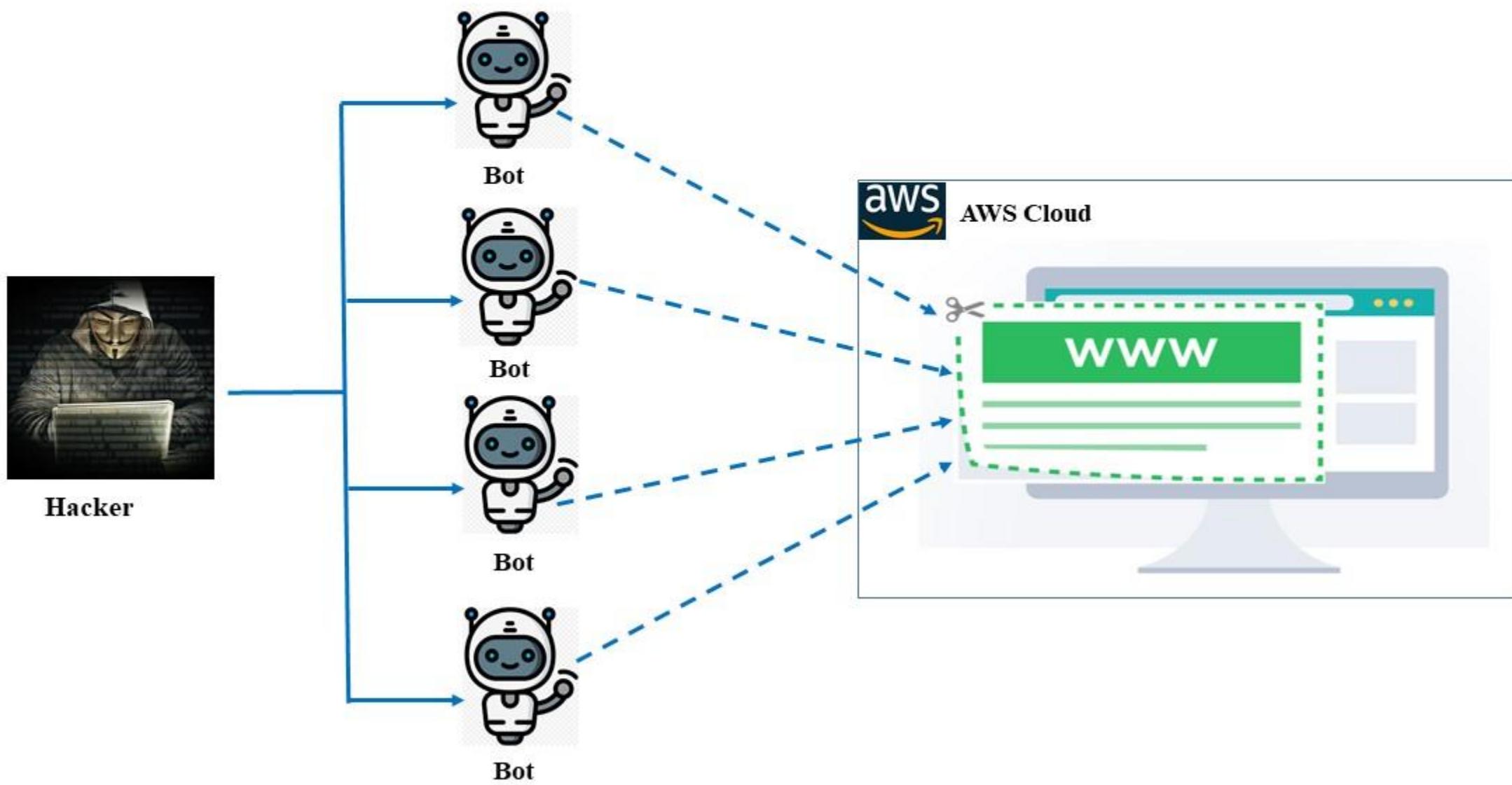
Bạn có thể triển khai cài đặt một ứng dụng web trong EC2 instance và sử dụng tường lửa WAF để bảo vệ ứng dụng web từ các cuộc tấn công chèn các đoạn mã độc(cross-site scripting).Bạn cũng có thể triển khai WAF cho CloudFront như là một phần của giải pháp phân phối nội dung (CDN) của bạn để ngăn chặn (block) các luồng truy cập(traffic) vào ra.



## Distributed Denial of Service(DDos) Tấn công từ chối dịch vụ.



# Bạn đã bao giờ nghe về tấn công từ chối dịch vụ DDoS?



# Shield

Shield là một dịch vụ quản lý bảo mật và bảo vệ máy chủ ứng dụng web chống lại các cuộc tấn công từ chối dịch vụ(DDoS)

- ✓ Luôn dò tìm các mối đe dọa , để loại bỏ các nguy cơ từ các cuộc tấn công (Always-on detection)
- ✓ Shield Standard là miễn phí



Shield



- ✓ Cung cấp miễn phí bảo vệ chống lại các cuộc tấn công phổ biến và các cuộc tấn công thường xuyên



- ✓ Cung cấp tăng cường các sự bảo vệ, và có sự hỗ trợ miễn phí 24/7 từ các chuyên gia AWS

- ✓ Shield Advanced là một dịch vụ tính phí

Một vài dịch vụ sau được **Shield Advanced** bảo vệ chống lại các cuộc tấn công từ chối dịch vụ(**DDoS**)



**CloudFront**



**Route 53**



**Elastic Load  
Balancing**



**AWS Global  
Accelerator**

# Shield trong trong thực tế

Nhận các thông báo  
theo thời gian thực của  
các vụ nghi ngờ có thể  
là tấn công từ chối dịch  
vụ (DDoS)

Shield Advanced sẽ gửi đến bạn các thông báo theo thời gian thực của các vụ nghi ngờ có thể là tấn công từ chối dịch vụ từ CloudWatch metrics.Thêm nữa, với Shield Advanced, bạn được hỗ trợ 24/7 bởi chuyên gian từ AWS.

# Macie

**Macie** giúp tìm kiếm và bảo vệ các thông tin nhạy cảm

- ✓ Sử dụng máy học (machine learning)
- ✓ Đánh giá môi trường S3



- ✓ Dò tìm ra các thông tin nhạy cảm cá nhân

# Macie trong thực tế

Dò tìm các thông tin  
của hộ chiếu của cá  
nhân, được lưu trong  
S3

Macie có thể được sử dụng để tìm kiếm thông tin nhạy cảm như: Thông tin hộ chiếu, thông tin, thông tin an sinh xã hội, và thông tin thẻ tín dụng của cá nhân trong lưu trữ S3

# Tổng kết

## WAF

WAF giúp bạn bảo vệ các ứng dụng web chống lại các tấn công phổ biến từ ngoài internet



## Shield

Shiled là một dịch vụ quản lý bảo mật và bảo vệ máy chủ ứng dụng web chống lại các cuộc tấn công từ chối dịch vụ(DDoS)



## Macie

Macie giúp tìm kiếm và bảo vệ các thông tin nhạy cảm



## Chương IV.

Giới thiệu tổng quan về giá dịch vụ, thanh toán và quản trị, hỗ trợ & giải đáp  
(Pricing, Billing, and Governance, support plans).

### 1) Giá dịch vụ và thanh toán

#### Pricing



##### Application Discovery Service

Application Discovery Service helps you plan migration projects to the AWS Cloud.

#### Billing



##### Budgets

Budgets allows you to set custom budgets that alert you when your costs or usage exceed your budgeted amount.

### 2) Tìm hiểu về dịch vụ quản trị, hỗ trợ và giải đáp

#### Management and Governance



##### Organizations

Organizations allows you to centrally manage multiple AWS accounts under one umbrella.



##### Professional Services

Professional Services helps enterprise customers move to a cloud-based operating model.

# Tìm hiểu giá dịch vụ (AWS Pricing)

Tổng quan chung bài học



# Giá (Pricing)

Có 3 chi phí căn bản trong sử dụng các dịch vụ AWS



# Các hình thức sử dụng miễn phí

Có 3 hình thức sử dụng miễn phí, mà AWS đưa ra cho khách hàng, tùy thuộc vào kiểu dịch vụ mà bạn chọn

1

12 tháng miễn phí



12 tháng sử dụng dịch vụ AWS cloud miễn phí, tính từ ngày bắt đầu tạo tài khoản AWS

2

Luôn miễn phí



Những ưu đãi này không bao giờ hết hạn, và có sẵn cho tất cả khách hàng AWS.

3

Dùng thử (trials)



Những ưu đãi này là những bản dùng thử miễn phí, ngắn hạn, bắt đầu từ ngày bạn kích hoạt một dịch vụ cụ thể.

# EC2 Pricing

Có 5 cách để trả chi phí cho sử dụng dịch vụ EC2 instances.



## On-demand



Bạn trả theo giờ, hoặc giây  
sử dụng, bạn sử dụng bao  
nhiêu bạn trả bấy nhiêu, và  
không phải trả tiền trước

## Saving Plan



Cam kết sử dụng dịch vụ,  
được đo lường tính toán  
theo giờ trong vòng 1 hoặc  
3 năm

## Reserved instances



Cam kết sử dụng dịch vụ,  
được kế hoạch trước trong  
vòng 1 hoặc 3 năm. Bất kể  
có sử dụng hay không

## Spot instances



Instances chỉ được cung  
cấp nếu AWS vẫn còn tài  
nguyên

## Dedicated Hosts



Thuê và trả tiền toàn bộ 1  
máy chủ vật lý

# Lambda Pricing

Chỉ tính phí khi bạn sử dụng Lambda



Số lượng truy cập  
(requests) dịch vụ



Bao gồm cả test ứng dụng  
từ console

Thời gian thực thi code



Từ khi bắt đầu chạy code chương  
trình ứng dụng, cho tới khi dừng  
chương trình

1.000.0000



1 triệu requests được miễn phí  
mỗi tháng.

# S3 Pricing

Bạn trả cho số lượng dữ liệu mà bạn đang lưu trữ.



**Storage classes**  
↓  
Trả tiền theo các kiểu lớp lưu trữ (Storage classes) khác nhau

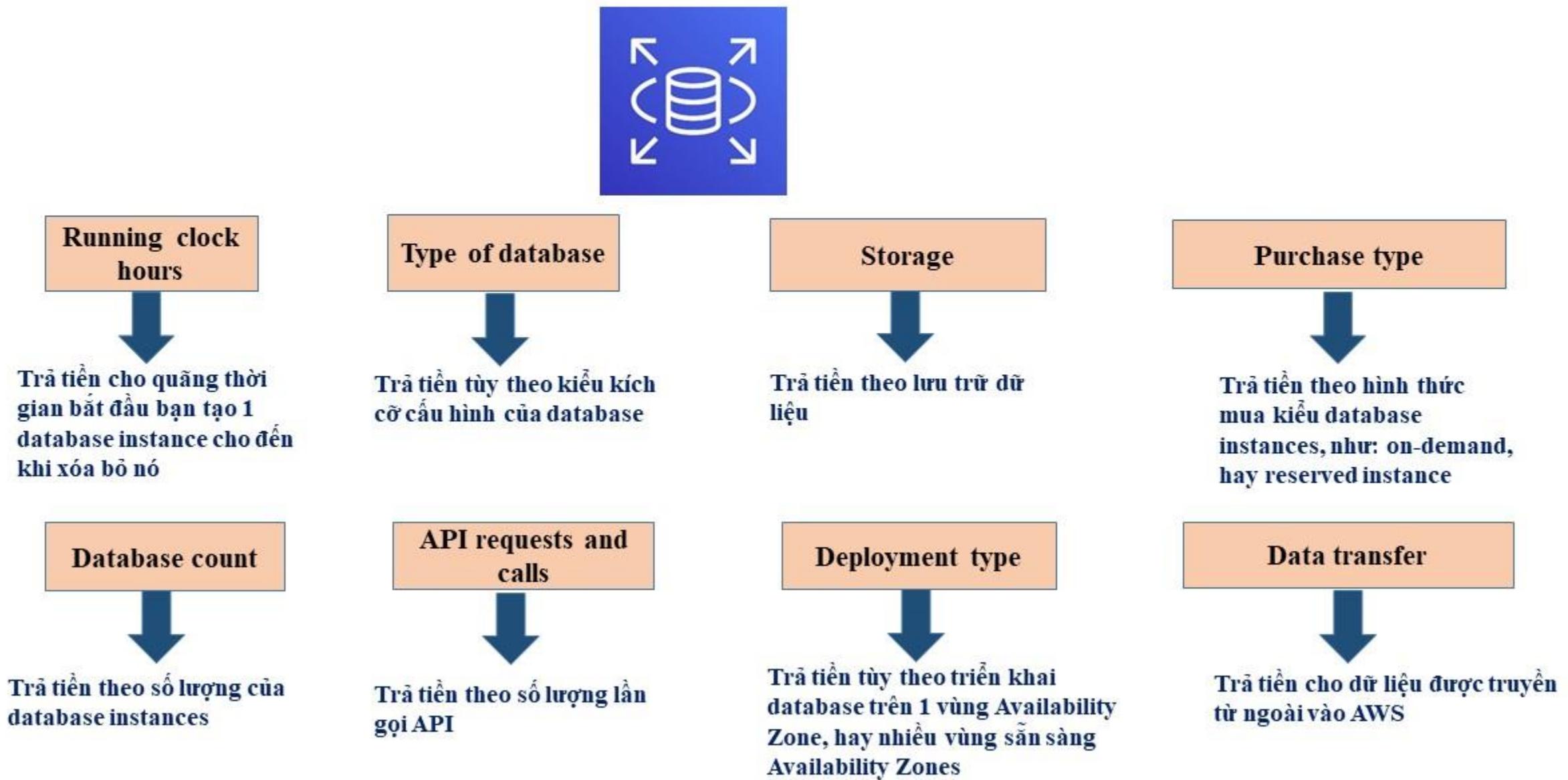
**Storage**  
↓  
Trả tiền theo số lượng bucket và dung lượng dữ liệu lưu trữ trong S3

**Data transfer**  
↓  
Trả tiền cho dữ liệu được truyền ra bên ngoài S3 region

**Request and data retrieval**  
↓  
Trả tiền theo số lượng các yêu cầu truy vấn dữ liệu từ ứng dụng hoặc người dùng

# RDS Pricing

## Tính phí theo mỗi hình thức trả tiền của RDS



# Bạn đã bao giờ nghe về Total Cost of Ownership(TCO)?

TCO là một ước tính tài chính giúp bạn hiểu về chi phí trực tiếp và chi phí gián tiếp, trong sử dụng các dịch vụ của AWS

- ✓ Cần bao nhiêu chi phí để dịch chuyển hệ thống lên AWS Cloud?
- ✓ Làm thế nào để tôi giảm tổng số chi phí phải trả trong sử dụng AWS?

# Application Discovery Services

**Application Discovery Services giúp bạn lên kế hoạch dịch chuyển các dự án lên đám mây**

- ✓ Lên phương án dịch chuyển dự án lên đám mây
- ✓ Thường được sử dụng để ước tính TCO



- ✓ Làm việc với các dịch vụ khác để dịch chuyển servers lên đám mây

## Một số cách sử dụng AWS để giảm chi phí TCO của bạn

**1** Giảm tối thiểu chi tiêu vốn



AWS giúp bạn giảm tối thiểu chi tiêu vốn lớn, việc này làm giảm tổng thể TCO

**2** Sử dụng Reserved Instances



AWS cung cấp Reserved Instances Giúp bạn tiết kiệm chi phí, và làm giảm TCO của bạn

**3** Chọn kích cỡ tài nguyên đúng



AWS giúp bạn làm phù hợp việc cung cấp tài nguyên theo nhu cầu sử dụng của bạn. Làm giảm TCO của bạn

## Chúng ta làm một Demo

- Chúng ta xem demo về cách tính TCO, bằng cách sử dụng công cụ Pricing Calculator của AWS. Đây là 1 công cụ miễn phí giúp bạn ước tính TCO tổng thể của bạn.

Truy cập vào trang: <https://calculator.aws/>

# AWS Price List API

Price List API cho phép bạn truy vấn giá các dịch vụ AWS



- ✓ Truy vấn sử dụng JSON hoặc HTML

- ✓ Nhận thông báo giá mới, khi giá dịch vụ có sự thay đổi

## AWS Cost Management



AWS Cost Management > Home

Current month costs

\$49.53



↓ 0%  
Over budget month

Forecasted month end costs

\$100.86



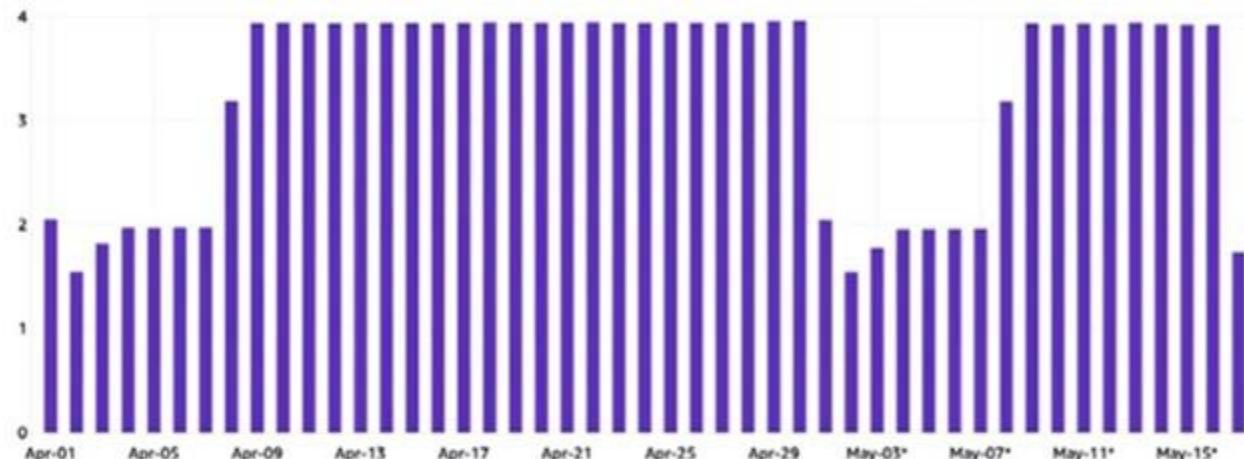
↓ 2%  
Over last month

May trends ⓘ

Once you have more usage across AWS, we will provide helpful cost and usage insights.

Daily unblended costs (\$)

Explore costs



Recently accessed reports [View all reports](#)

You have not accessed any reports recently from this device. To view all of your reports, visit the [report library](#).

Preferences

Billing Console

Documentation

# Tìm hiểu dịch vụ thanh toán (Billing Services)

## Tổng quan chung bài học

1

Ngân sách  
(Budgets)

2

Chi phí và báo  
 cáo sử dụng

3

Tìm hiểu chi phí dịch vụ

4

Tổng kết



## Một bức tranh tổng quan

- Làm thế nào để có dịch vụ lập hóa đơn và ngân sách phù hợp cho một bức tranh toàn cảnh
  - Có một số công cụ sẵn trong AWS để giúp bạn liên tục theo dõi chi phí dịch vụ

# Budgets

**Budgets cho phép bạn đặt các tùy chọn của ngân sách chi tiêu, giúp cảnh báo bạn, khi chi phí hoặc phí sử dụng dịch vụ vượt quá ngân sách của bạn.**

- ✓ Cải thiện việc lên kế hoạch và kiểm soát chi phí
- ✓ Chi phí, sử dụng dịch vụ, và đặt trước ngân sách



**Budgets**

- ✓ Cảnh báo chi phí

# Budget Types



**Cost Budgets**



Lên kế hoạch bao nhiêu tiền bạn  
muốn chi tiêu cho 1 dịch vụ



**Usage Budgets**



Lên kế hoạch bao nhiêu tiền bạn  
muốn sử dụng cho một hoặc nhiều  
hơn một dịch vụ



**Reservation Budgets**



Đặt RIs, hoặc kế hoạch tiết  
kiệm trong sử dụng dịch vụ  
, hoặc các mục tiêu

# Budgets trong thực tế

Theo dõi việc sử dụng EC2 free Tier, do đó bạn sẽ không bị tính phí cho chi phí không mong muốn

Bạn có thể theo dõi việc sử dụng EC2 Free Tier để đảm bảo bạn không bị vượt quá sự cho phép miễn phí sử dụng và phải trả các chi phí phát sinh không mong muốn. Bạn có thể thiết đặt một cảnh báo thông báo cho bạn khi mà chi phí sử dụng dịch vụ trong tài khoản của bạn gần bằng một số tiền cụ thể.

## Chúng ta làm một Demo

- Chúng ta xem demo về cách thiết lập thông báo thanh toán và ngân sách, tạo ngân sách chi phí bằng dịch vụ AWS Budget

# Chi phí và báo cáo sử dụng (Cost and Usage Report)

**Chi phí và báo cáo sử dụng bao gồm hầu hết toàn bộ các tập hợp dữ liệu chi phí và sử dụng**

- ✓ Có thể tải(download) chi tiết báo cáo về Laptop



- ✓ Liệt kê mức sử dụng của từng loại dịch vụ

- ✓ Tổng hợp dữ liệu sử dụng theo hàng ngày, hàng giờ, hoặc hàng tháng

**Cost and Usage  
Report**

# Chi phí và báo cáo sử dụng trong thực tế

Xem dữ liệu chi phí  
chi tiết nhất về sử  
dụng dữ liệu

Chi phí và báo cáo sử dụng cho phép bạn khả năng để xem chi tiết sâu nhất về dữ liệu chi phí sử dụng dữ liệu của bạn. Khi thiết đặt dịch vụ này, bạn có thể tải báo cáo sử dụng của Amazon S3 console.

# Cost Explorer

**Cost Explorer cho phép bạn xem và dự báo chi phí sử dụng dịch vụ trong một quãng thời gian**

- ✓ Xem chi phí qua thời gian
- ✓ Xem chi phí 12 tháng qua



- ✓ Dự báo chi phí 3 tháng tiếp theo

**Cost Explorer**

# Cost Explorer trong thực tế

Phân tích sử dụng  
EC2 qua thời gian  
trong quá khứ 7, 30,  
60 ngày

Nếu bạn đang xem xét các sự lựa chọn cho các kế hoạch tiết kiệm chi phí , AWS Cost Explorer có thể giúp phân tích sử dụng EC2 qua thời gian trong quá khứ 7, 30, 60 ngày.

## AWS Cost Management



AWS Cost Management > Home

Current month costs

\$49.53



↓ 0%  
Over budget month

Forecasted month end costs

\$100.86



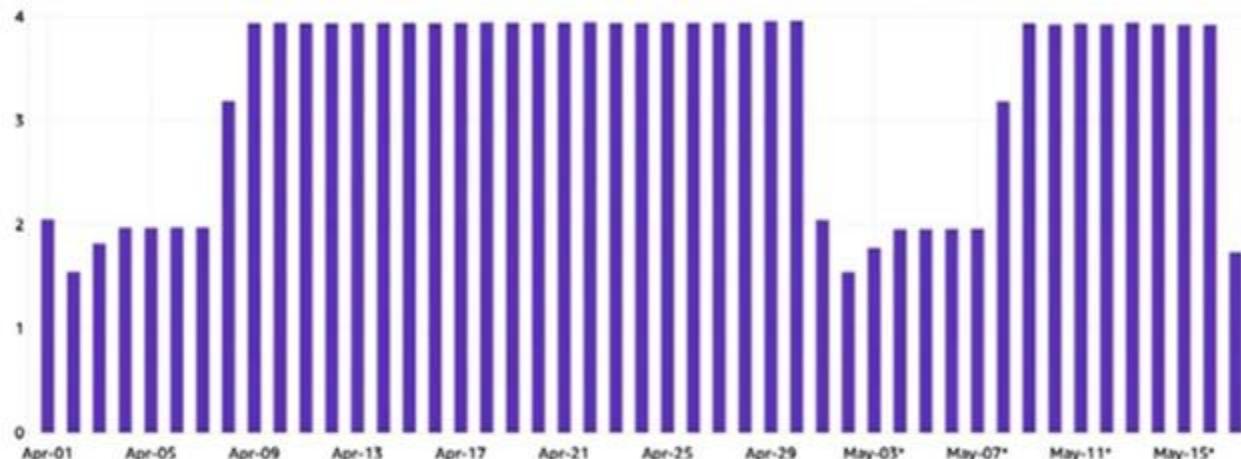
↓ 2%  
Over last month

May trends ⓘ

Once you have more usage across AWS, we will provide helpful cost and usage insights.

Daily unblended costs (\$)

Explore costs



Recently accessed reports [View all reports](#)

You have not accessed any reports recently from this device. To view all of your reports, visit the [report library](#).

Preferences

Billing Console

Documentation

Save as...

Recent reports ▾

New report

Home

Cost Explorer

Reports

Budgets

Cost Anomaly Detection

Rightsizing recommendations

## ▼ Savings Plans

Overview

Inventory

Recommendations

Purchase Savings Plans

Utilization report

Coverage report

Cart 0

## ▼ Reservations

Overview

Recommendations

Utilization report

Coverage report

Preferences

Billing Console ▾

Documentation ▾

Last 6 Months

Monthly

0

In Bar

Group by:

Service

Linked Account

Region

Instance Type

Usage Type

Resource

Cost Category

Tag

API Operation

More

▲ FILTERS

CLEAR ALL

Service

Include all ▾

Linked Account

Include all ▾

Region

Include all ▾

Instance Type

Include all ▾

Usage Type

Include all ▾

Usage Type Group

Include all ▾

Resource

Include all ▾

Cost Category

Include all

Tag

Include all

More filters ▾

▲ ADVANCED OPTIONS

0

Show costs as

Unblended costs ▾

Include costs related to

 Show only untagged resources Show only uncategorized resources Show forecasted values

Download CSV

Service	Nov	Dec	Jan	Feb	Mar
Total cost (\$)	0.03	12.01	6.57	0.00	0.00
Registrar (\$)		24.00			
CloudWatch (\$)	0.00	0.00	5.00	0.00	0.00
S3 (\$)	0.09	0.15	0.24	0.12	0.11
Secrets Manager (\$)	0.00	0.00	0.80	0.00	0.00
Route 53 (\$)		0.00	0.50	0.00	0.00

# Tổng kết

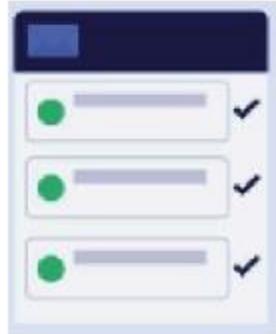
## Budgets

Budgets cho phép bạn đặt các tùy chọn của ngân sách chi tiêu, giúp cảnh báo bạn, khi chi phí hoặc phí sử dụng dịch vụ vượt quá ngân sách của bạn.



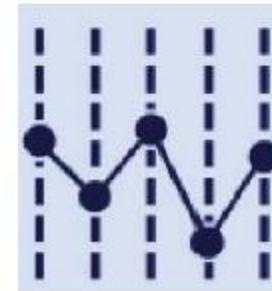
## Cost and Usage Report

Chi phí và báo cáo sử dụng bao gồm hầu hết toàn bộ các tập hợp dữ liệu chi phí và sử dụng



## Cost Explorer

Cost Explorer cho phép bạn xem và dự báo chi phí sử dụng dịch vụ trong một khoảng thời gian



# Tìm hiểu dịch vụ quản trị (Governance Services)



## Một bức tranh tổng quan

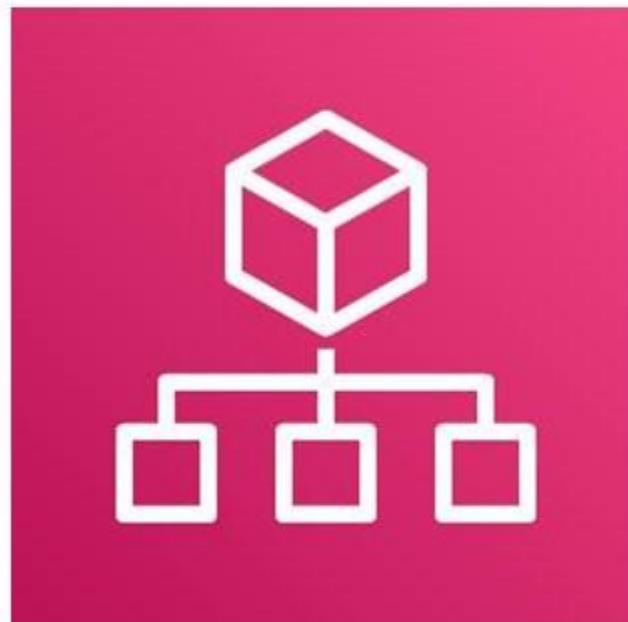
- Dịch vụ Governance và management giúp bạn duy trì sự kiểm soát về chi phí, tuân thủ và bảo mật trong các tài khoản AWS của bạn.



# Organizations

**Organizations cho phép bạn trung tâm hóa việc quản lý nhiều tài khoản AWS dưới một cái ô.**

- ✓ Nhóm nhiều tài khoản (accounts)



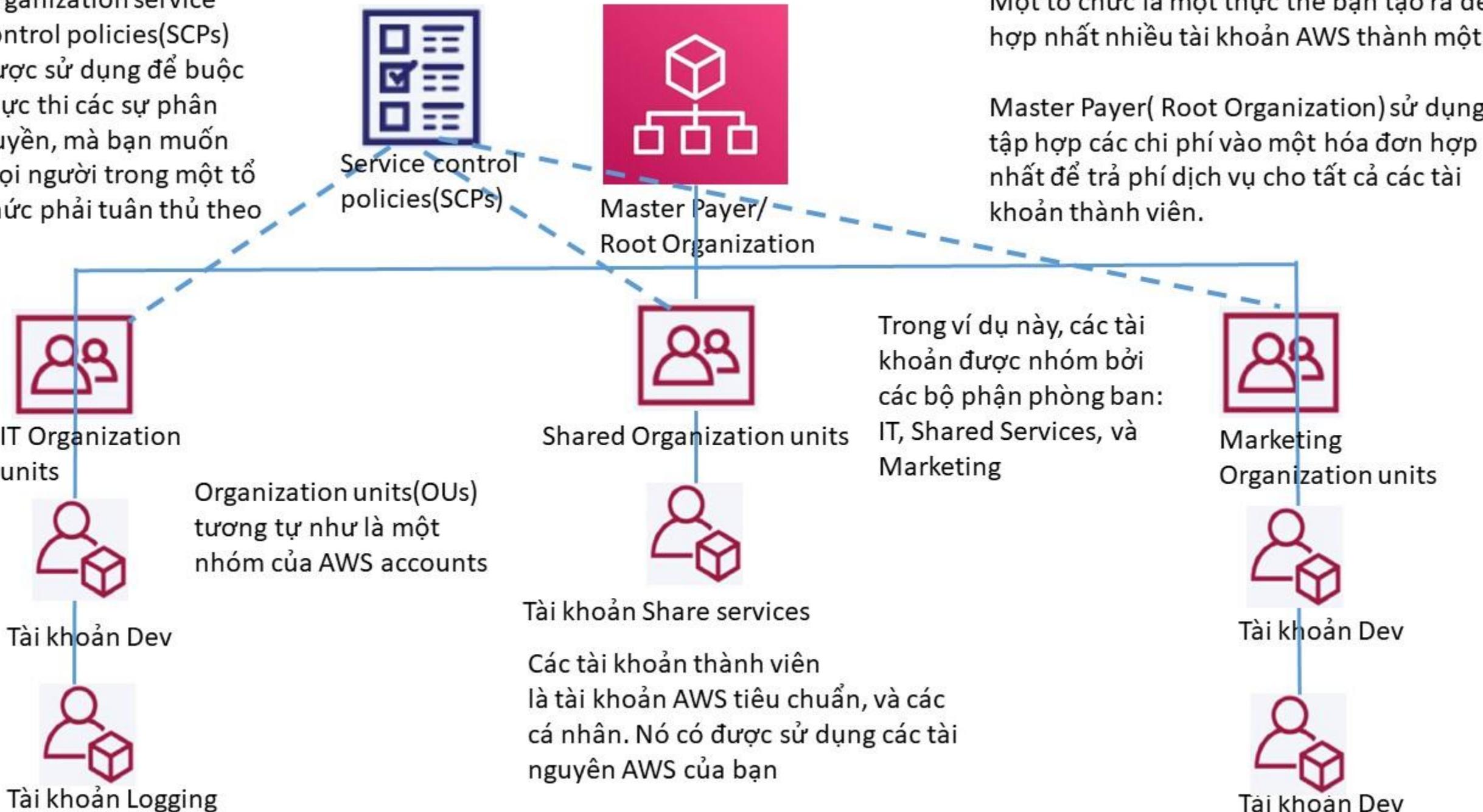
**Organizations**

- ✓ Đơn giản hóa trả tiền phí dịch vụ cho tất cả các tài khoản

- ✓ Tự động hóa tạo tài khoản (account)

- ✓ Phân phối tài nguyên, và áp dụng các chính sách cho các accounts

Organization service control policies(SCPs) được sử dụng để buộc thực thi các sự phân quyền, mà bạn muốn mọi người trong một tổ chức phải tuân thủ theo



# Organizations mang lại những lợi ích gì?

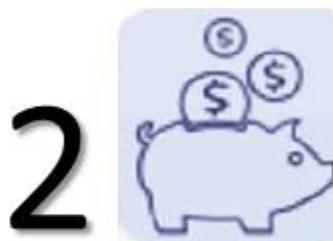
Organization đưa ra nhiều lợi ích cho tổ chức, doanh nghiệp.



Tập trung hóa thanh toán



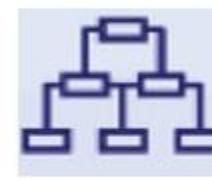
Lên kế hoạch bao nhiêu tiền bạn  
muốn chi tiêu cho 1 dịch vụ



Tiết kiệm chi phí



Lên kế hoạch bao nhiêu tiền bạn  
muốn sử dụng cho một hoặc nhiều  
hơn một dịch vụ



Quản lý các tài khoản theo  
mô hình tập trung



Bạn có thể nhanh chóng và tự  
động hóa tạo các tài khoản  
hoặc mời các tài khoản đang  
hiện hữu

# Organizations trong thực tế

**Giảm các chi phí sử dụng dịch vụ bằng cách chia sẻ các tài nguyên giữa các tài khoản**

**Organizations** cho phép bạn tiết kiệm tiền sử dụng Reserved Instance(RI) chia sẻ(sharing) . RI sharing cho phép tất cả các tài khoản trong một Organization nhận được lợi ích về chi phí của Ris đã được mua bởi một vài tài khoản khác. Bạn có thể sử dụng master payer(or root) organization để tắt RI sharing.

# Control Tower

**Control Tower cho phép bạn đảm bảo các tài khoản của bạn tuân thủ các chính sách của công ty.**

- ✓ Giúp tạo các tài khoản mới sử dụng một multi-account strategy
- ✓ Làm việc trực tiếp với AWS Organizations



- ✓ Bắt buộc tuân thủ trong thực thi việc sử dụng tốt nhất các dịch vụ trên các tài khoản
- ✓ Cung cấp một màn hình điều khiển (dashboard) để quản lý các tài khoản

# Control Tower trong thực tế

**Không cho phép quyền ghi public vào tất cả S3 giữa các tài khoản của bạn**

**Control Tower cho phép bạn quản lý môi trường nhiều tài khoản của bạn bằng cách cho phép kiểm tra bảo mật nhiều tài khoản, hoặc ngăn chặn hoặc phát hiện các vấn đề bảo mật thông qua các hành lang bảo vệ bắt buộc hoặc tùy chọn.**

# System Manager

**System Manager cung cấp cho bạn khả năng hiển thị và kiểm soát các tài nguyên AWS của bạn.**

- ✓ Tự động hóa các công việc vận hành tài nguyên hệ thống
- ✓ Nhóm các tài nguyên và thực hiện công việc



**System Manager**

- ✓ Cập nhật các bản vá lỗi, chạy các câu lệnh đồng loạt cho các máy chủ EC2 hoặc quản trị RDS instances

# System Manager trong thực tế

Tự động hóa việc triển khai cập nhật các bản vá lỗi cho hệ điều hành và các ứng dụng trong một nhóm có nhiều các máy chủ EC2

System Manager cho phép bạn tự động hóa cập nhật cài đặt các bản vá lỗi cho hệ điều hành và nhiều ứng dụng phần mềm chạy trong máy chủ EC2 instances tuân theo một lịch trình.

## Trusted Advisor

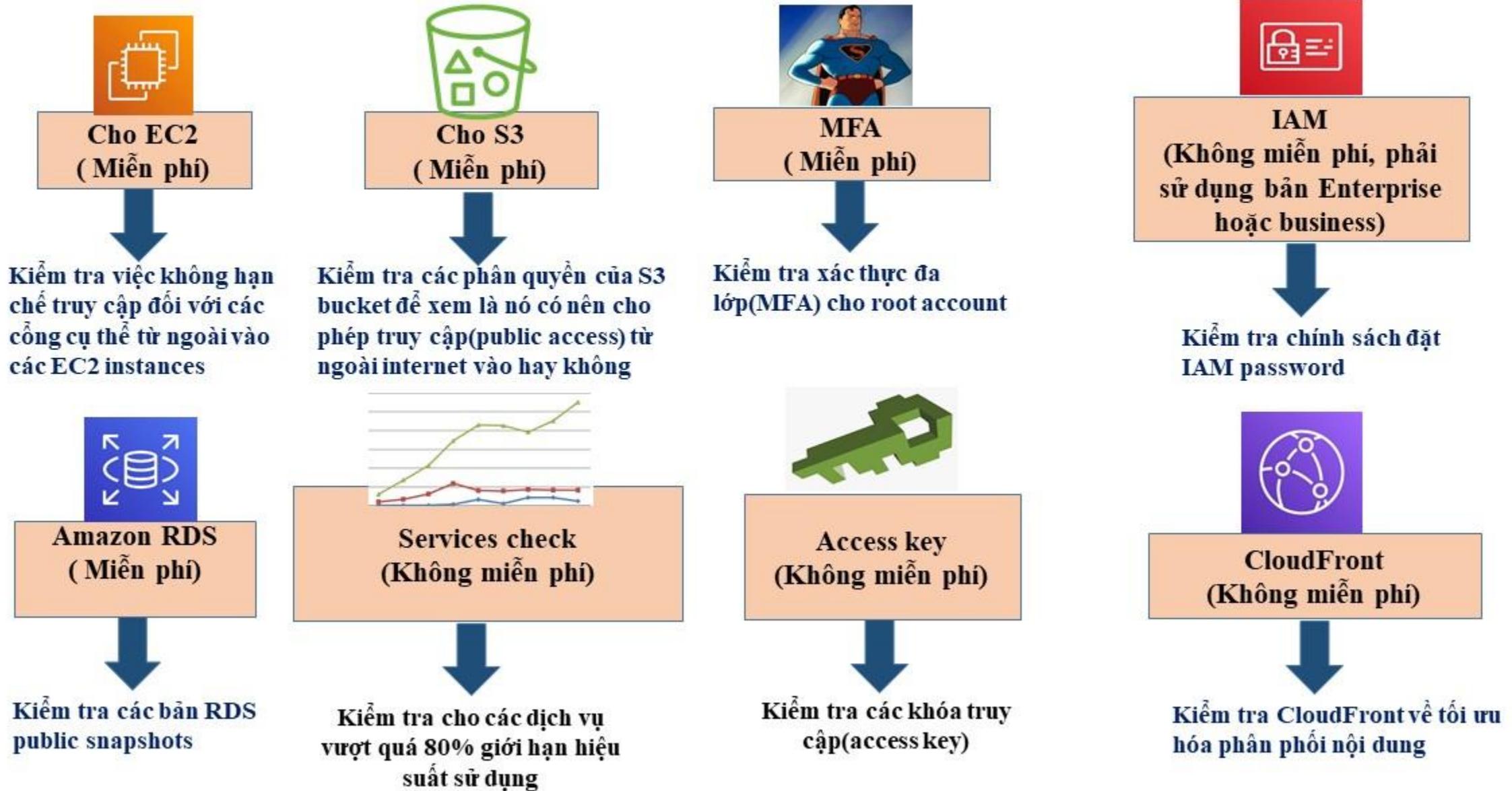
**Trusted Advisor cung cấp hướng dẫn theo thời gian thực để giúp bạn cung cấp các tài nguyên AWS của hạn đến với người dùng theo cách hiệu quả nhất.**

- ✓ Kiểm tra tài khoản của bạn và đưa ra các khuyến nghị
- ✓ Giúp bạn xem các giới hạn dịch vụ



- ✓ Giúp bạn hiểu các phương pháp tốt nhất

# Một vài khuyến nghị phổ biến của Trusted Advisor



# Trusted Advisor trong thực tế



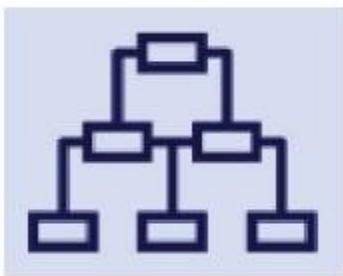
Kiểm tra giới hạn dung lượng đọc(read) và ghi(write) cho DynamoDB

Trusted Advisor giúp bạn giảm thiểu toàn bộ chi phí bằng cách theo dõi các giới hạn dịch vụ

# Tổng kết

## Organizations

Organizations cho phép bạn trung tâm hóa việc quản lý nhiều tài khoản AWS dưới một cái ô.



## System Manager

System Manager cung cấp cho bạn khả năng hiển thị và kiểm soát các tài nguyên AWS của bạn.



## Control Tower

Control Tower cho phép bạn đảm bảo các tài khoản của bạn tuân thủ các chính sách của công ty.



## Trusted Advisor

Trusted Advisor cung cấp hướng dẫn theo thời gian thực để giúp bạn cung cấp các tài nguyên AWS của hạn đến với người dùng theo cách hiệu quả nhất.



# Sử dụng quản trị dịch vụ (Management Services)

1

Managed  
Services

2

Professional  
Services

3

AWS Partner  
Network (APN)

4

Marketplace

5

Tổng kết



## Một bức tranh tổng quan

Có một vài dịch vụ giúp bạn dịch chuyển và xây dựng hệ thống IT của bạn nhanh hơn trong đám mây

- Có một nhóm chuyên gia luôn sẵn sàng giúp bạn quản trị và vận hành hệ thống môi trường đám mây của bạn



# Managed Services

**Managed Services giúp bạn vận hành hiệu quả hơn hệ thống cơ sở hạ tầng AWS của bạn.**

- ✓ Tăng thêm nhân viên nội bộ của bạn
- ✓ Cung cấp khả năng quản lý liên tục cơ sở hạ tầng của bạn



**Managed Services**

- ✓ Giảm rủi ro trong vận hành hệ thống

- ✓ Tuân thủ (Compliance), quản lý cập nhật cài đặt các bản vá lỗi hệ điều hành, phần mềm ứng dụng (Patch Management).
- ✓ Giám sát, theo dõi hệ thống( Monitoring), quản lý các sự kiện (Event Management), quản lý truy cập hệ thống(Access Management).
- ✓ Quản lý bảo mật(Security Management), quản lý sự thay đổi(Change Management).
- ✓ Quản trị hệ thống hạ tầng mạng (Network Management), quản trị sự hoạt động liên tục của hệ thống (Continuity Management).
- ✓ Quản lý sự cố(Incident Management), quản lý nhật ký hệ thống(Logging).
- ✓ Báo cáo (Reporting), Tối ưu hóa chi phí sử dụng dịch vụ (Cost Optimization).

# Managed Services trong thực tế

Phát triển dịch vụ theo  
dõi sức khỏe cho ứng  
dụng, sử dụng dịch vụ  
CloudWatch

Managed services có thể làm tăng hiệu quả vận hành hệ thống của bạn bằng cách giúp bạn phát triển dịch vụ theo dõi sức khỏe cho ứng dụng sử dụng CloudWatch.

# Professional Services

**Professional Services giúp khách hàng doanh nghiệp chuyển lên một nền tảng mô hình vận hành hệ thống trong đám mây**

- ✓ Đề xuất các giải pháp



- ✓ Thiết kế các giải pháp

- ✓ Thực hiện các giải pháp

Professional  
Services

# Professional Services trong thực tế

Có được sự giúp đỡ  
đánh giá một ứng dụng  
cho việc dịch chuyển lên  
đám mây

Bạn có thể nhanh chóng chuyển dịch ứng dụng của bạn tại chỗ lên đám mây sử dụng dịch vụ Professional Services

## AWS Partner Network(APN)

**APN là một cộng đồng toàn cầu gồm các đối tác được phê duyệt cung cấp các giải pháp phần mềm và dịch vụ tư vấn cho AWS**

- ✓ Đưa ra các đối tác công nghệ, họ cung cấp các giải pháp phần mềm
- ✓ Cung cấp các đối tác tư vấn, họ đưa ra các dịch vụ chuyên nghiệp



APN

- ✓ Tìm kiếm nhà cung cấp được phê duyệt bởi AWS, với trình độ chuyên môn cao

# APN trong thực tế

Bạn cần giúp đỡ thiết kế  
và xây dựng một ứng  
dụng mới

Nếu như nhóm của bạn thiếu các kỹ năng để xây dựng và triển khai các ứng dụng cloud, dịch vụ APN có thể giúp bạn xử lý những việc này một cách nhanh chóng.



Standard  
Consulting  
Partner



Advanced  
Technology  
Partner

# Marketplace

- Marketplace là một danh sách số của giải pháp đã được xây dựng, bạn có thể mua bản quyền. Bạn cũng có thể bán các giải pháp của bạn đến khách hàng thông qua Marketplace.

✓ Bạn có thể mua phần mềm của bên thứ 3



✓ Bán các giải pháp cho khách hàng của AWS

✓ Bạn có thể tìm kiếm danh sách của các phần mềm, và cài đặt nó với 1 click chuột.

# Marketplace trong thực tế

Thử ứng dụng trước khi  
cam kết mua cho sử  
dụng lâu dài

Một số sản phẩm phần mềm được liệt kê trên Marketplace cung cấp bản dùng thử miễn phí, bản dùng thử miễn phí cho phép bạn dùng thử phần mềm trước khi mua.

# Tổng kết

## Managed Services

Manager Services giúp bạn vận hành hiệu quả hơn hệ thống cơ sở hạ tầng AWS của bạn.



APN

APN là một cộng đồng toàn cầu gồm các đối tác được phê duyệt cung cấp các giải pháp phần mềm và dịch vụ tư vấn cho AWS.



Standard  
Consulting  
Partner



Advanced  
Technology  
Partner

## Professional Services

Professional Services giúp khách hàng doanh nghiệp chuyển lên một nền tảng mô hình vận hành hệ thống trong đám mây.

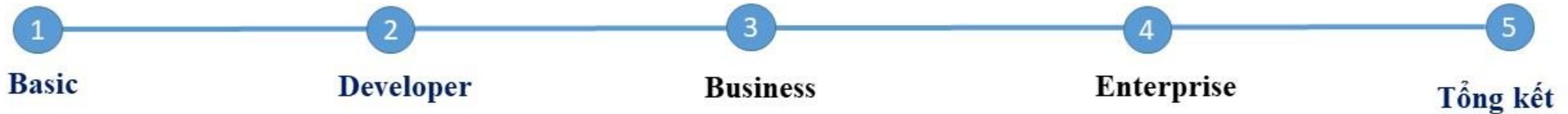


Marketplace

Marketplace là một danh sách số của giải pháp đã được xây dựng, bạn có thể mua bản quyền. Bạn cũng có thể bán các giải pháp của bạn đến khách hàng thông qua Marketplace.



# Tìm hiểu về dịch vụ hỗ trợ & giải đáp (Support Plans)



# Support Plans

Có 4 loại support plans

**1**

## Basic

Hỗ trợ căn bản(Basic Support) được bao gồm miễn phí cho tất cả các tài khoản AWS.

**3**

## Business

Business Support bắt đầu là 100\$/tháng, và nó được khuyên dùng cho môi trường chạy thật.

**2**

## Developer

Developer support là loại hỗ trợ phải trả phí bắt đầu là 29\$/tháng, và nó hỗ trợ kiểm thử (testing) và phát triển dịch vụ trong hệ thống AWS.

**4**

## Enterprise

Enterprise Support bắt đầu là 15.000\$/tháng, và nó được khuyên dùng cho môi trường kinh doanh chuyên nghiệp.

# Các kiểu trường hợp support

Có 3 kiểu trường hợp support bạn có thể mở với AWS Support



**Tài khoản (Account) và  
hóa đơn thanh toán(billing)**



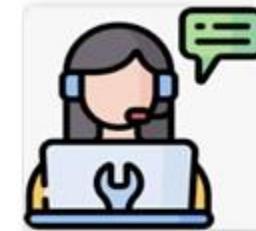
Những thắc mắc liên quan đến tài khoản AWS và hóa đơn thanh toán(billing) có thể được mở bởi tất cả các khách hàng.



**Tăng giới hạn dịch vụ**



Tăng giới hạn dịch vụ hoặc quota có thể được mở bởi tất cả các khách hàng.



**Hỗ trợ kỹ thuật  
(Technical support)**



Các trường hợp cần có hỗ trợ kỹ thuật có thể chỉ được mở bởi khách hàng có sử dụng các gói Developer, Business hoặc Enterprise



AWS Support không cho phép hỗ trợ các trường hợp hỗ trợ cho code phát triển phần mềm, sửa lỗi phần mềm của khách hàng, và các công việc liên quan đến việc quản trị hệ thống

# Basic Support Plan

Hỗ trợ căn bản(Basic Support) được bao gồm miễn phí cho tất cả các tài khoản AWS



Tài khoản (Account) và  
hóa đơn thanh toán(billing)



Tăng giới hạn dịch vụ



Customer Service



24/7 chỉ được liên lạc  
qua email

# Developer Support Plan

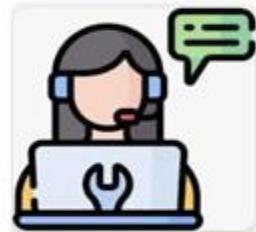
Developer support là loại hỗ trợ phải trả phí bắt đầu là 29\$/tháng, và nó hỗ trợ kiểm thử (testing) và phát triển dịch vụ trong hệ thống AWS.



Tài khoản (Account) và  
hóa đơn thanh toán(billing)



Tăng giới hạn dịch vụ



Hỗ trợ kỹ thuật  
(Technical support)



Được liên lạc  
với nhân viên kỹ thuật



Không giới hạn các  
trường hợp hỗ trợ



Cloud Support Associate



Thời gian làm việc  
văn phòng, chỉ được  
liên lạc qua email



Thời gian phản hồi

<24 h hướng dẫn chung  
<12 h hệ thống bị lỗi

# Business Support Plan

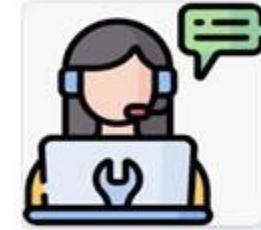
Business Support bắt đầu là 100\$/tháng, và nó được khuyên dùng cho môi trường chạy thật.



Tài khoản (Account) và  
hóa đơn thanh toán(billing)



Tăng giới hạn dịch vụ



Hỗ trợ kỹ thuật  
(Technical support)



Không giới hạn liên lạc  
với nhân viên kỹ thuật



Không giới hạn các  
trường hợp hỗ trợ



Được sử dụng full dịch vụ  
Trusted Advisor checks



24/7 được trao đổi qua email,  
điện thoại, hoặc chat



Thời gian phản hồi

<24 h hướng dẫn chung

<12 h hệ thống bị lỗi

<4 h hệ thống chạy trong môi trường  
dùng (Production system) thật bị lỗi

<1 h nếu hệ thống chạy trong môi trường dùng  
(Production system) thật bị down

# Enterprise Support Plan

Enterprise Support bắt đầu là 15.000\$/tháng, và nó được khuyên dùng cho môi trường kinh doanh chuyên nghiệp.



Tài khoản (Account) và hóa đơn thanh toán(billing)



Tăng giới hạn dịch vụ



Hỗ trợ kỹ thuật  
(Technical support)



Không giới hạn liên lạc với nhân viên kỹ thuật



Không giới hạn các trường hợp hỗ trợ



Được sử dụng full dịch vụ  
Trusted Advisor checks



Technical Account Manager (TAM)



Hỗ trợ từ tổng đài dịch vụ



Infrastructure Event Management

Cloud Support Engineers



24/7 được trao đổi qua email, điện thoại, hoặc chat



Thời gian phản hồi

<24 h hướng dẫn chung

<12 h hệ thống bị lỗi

<4 h hệ thống chạy trong môi trường dùng (Production system) thật bị lỗi

<1 h nếu hệ thống chạy trong môi trường dùng (Production system) thật bị down

<15 phút nếu hệ thống kinh doanh quan trọng bị down

# Tổng kết

## Basic

Hỗ trợ căn bản(Basic Support) được bao gồm miễn phí cho tất cả các tài khoản AWS.



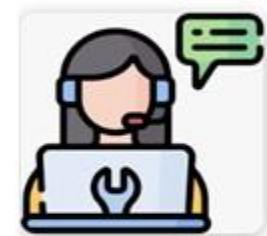
## Business Support Plan

Business Support bắt đầu là 100\$/tháng, và nó được khuyên dùng cho môi trường chạy thật.



## Developer Support Plan

Developer support là loại hỗ trợ phải trả phí bắt đầu là 29\$/tháng, và nó hỗ trợ kiểm thử (testing) và phát triển dịch vụ trong hệ thống AWS.



## Enterprise Support Plan

Enterprise Support bắt đầu là 15.000\$/tháng, và nó được khuyên dùng cho môi trường kinh doanh chuyên nghiệp.

