**1. Tổng quan về Cloud Computing**

Cloud Computing, là thuật ngữ mô tả việc cung cấp phân phối các tài nguyên máy tính (như máy chủ, lưu trữ, cơ sở dữ liệu, mạng, phần mềm) qua internet, giúp người dùng truy cập và sử dụng theo nhu cầu mà không cần quản lý hạ tầng vật lý.

**2. Các mô hình dịch vụ trong Cloud Computing**

* **Infrastructure as a Service (IaaS):** Cung cấp tài nguyên cơ sở hạ tầng như máy chủ, lưu trữ và mạng dưới dạng dịch vụ. Người dùng có quyền kiểm soát hệ điều hành và ứng dụng, nhưng không quản lý hạ tầng vật lý. Amazon EC2
* **Platform as a Service (PaaS):** Cung cấp nền tảng mà nhà phát triển cần để xây dựng, chạy và quản lý ứng dụng, từ máy chủ và hệ điều hành đến tất cả các mạng, lưu trữ, phần mềm trung gian, công cụ, v.v. Google App Engine
* **Software as a Service (SaaS):** Cung cấp ứng dụng phần mềm qua Internet, giúp người dùng truy cập các ứng dụng mà không cần cài đặt hoặc quản lý chúng. Microsoft 365

**3. Các mô hình triển khai Cloud Computing**

* **Public Cloud:** Dịch vụ đám mây được cung cấp qua Internet công cộng và chia sẻ giữa nhiều tổ chức.
* **Private Cloud:** Dịch vụ đám mây được sử dụng độc quyền bởi một tổ chức, cung cấp mức độ kiểm soát và bảo mật cao hơn.
* **Hybrid Cloud:** Kết hợp giữa public và private cloud, cho phép dữ liệu và ứng dụng được chia sẻ giữa chúng.

**4. Giới thiệu về AWS**

Amazon Web Services (AWS) là một nền tảng dịch vụ đám mây toàn diện và được chấp nhận rộng rãi, cung cấp hơn 200 dịch vụ đầy đủ tính năng từ các trung tâm dữ liệu trên toàn cầu.

[aws.amazon.com](https://aws.amazon.com/vi/what-is-cloud-computing/?utm_source=chatgpt.com)

**6. Cơ sở hạ tầng toàn cầu của AWS**

**AWS**

- region: chỉ các khu vực địa lý tiêng biệt thường là quy mô quốc gia hoặc vùng lãnh thổ rộng lớn

Trong Mỗi region chứa các availability zones được kết nối với nhau với độ trễ thấp và chúng thường nằm ở vị trí đủ xa về vị trí địa lý để đảm bảo sự cố xảy ra ở ez này không ảnh hưởng đến các ez khác

Bên trong az thì là các data center

Edge location là data center được dùng để lưu trữ giữ liệu như cache nhằm giảm độ trể trong việc truyển tải dự liệu tới người dùng

Edge location được phân bổ tại các thành phố lớn gần người dùng

Ví dụ ta có người dùng việt nam truy cập youtube để xem 1 video mà youtube đặt data center ở mỹ . khi video được gửi về người dùng và sau đó sẽ được cache lại edge location ở gần việt nam

Tiếp theo người dùng mới truy cập youtube xem video này thay vì nhận dự liệu ở mỹ thì nhận dự liệu từ cache edge location điều này sẽ làm giảm độ trễ cho video này

7. dịch vụ indentity and access management (IAM)

Iam là dịch vụ để xác thức và cấp quyền các tài nguyên của aws như ec2 ,s3

Iam cho các admin gán quyền user sử dùng tài nguyên aws mà không cần phải share user và pass của minh

User là người dùng tương tác với aws

Group nhóm các user thường nhóm lại có các vại trò giống nhau để dễ dàng quản lý

Policy là 1 văn bản viết dưới dạng json

Khi policicy được gắn vào user, group, role nó sẽ định nghĩa quyền hạn permission của thực thể này

Khi các thực thể này yêu cầu truy cập đến 1 tài nguyên của aws thì policy sẽ đánh giá xem yêu cầu chấp nhận hay ko

Role khác với user là có thể sử dụng bởi bất kì ai được phép

7. EC2

Elastic compute cloud

Ec nó sẽ cung cấp các máy tính để thực hiện hiện tính toán. Các máy máy tính này là máy tính ảo từ các hạ tầng của aws được cung cấp dịch qua internet

1 máy ảo chạy trên aws gọi là instance

**3. Các loại Instance EC2**

AWS cung cấp nhiều loại instance phục vụ các nhu cầu khác nhau:

| **Loại** | **Mô tả** | **Ví dụ** |
| --- | --- | --- |
| **General Purpose** | Cân bằng giữa CPU, RAM và I/O | t2.micro, m5.large |
| **Compute Optimized** | Tối ưu hiệu năng xử lý CPU | c5.large, c6g.xlarge |
| **Memory Optimized** | Dành cho ứng dụng cần nhiều RAM | r5.large, x1e.xlarge |
| **Storage Optimized** | Dành cho ứng dụng I/O cao | i3.large, d2.xlarge |
| **GPU Instances** | Dùng cho AI, Machine Learning, Đồ họa | g4dn.xlarge, p4d.24xlarge |

**6. Chi phí sử dụng EC2 💰**

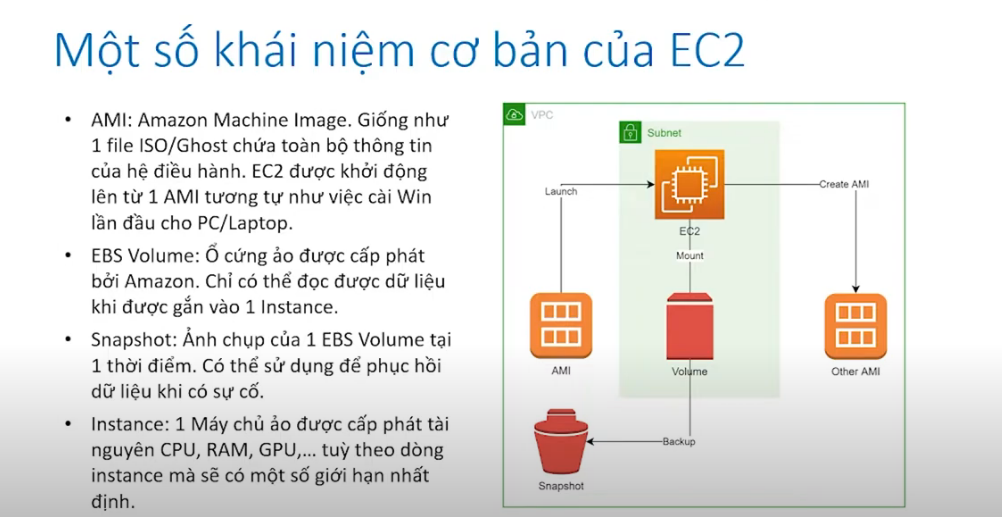
Bạn chỉ trả tiền cho tài nguyên sử dụng, bao gồm:

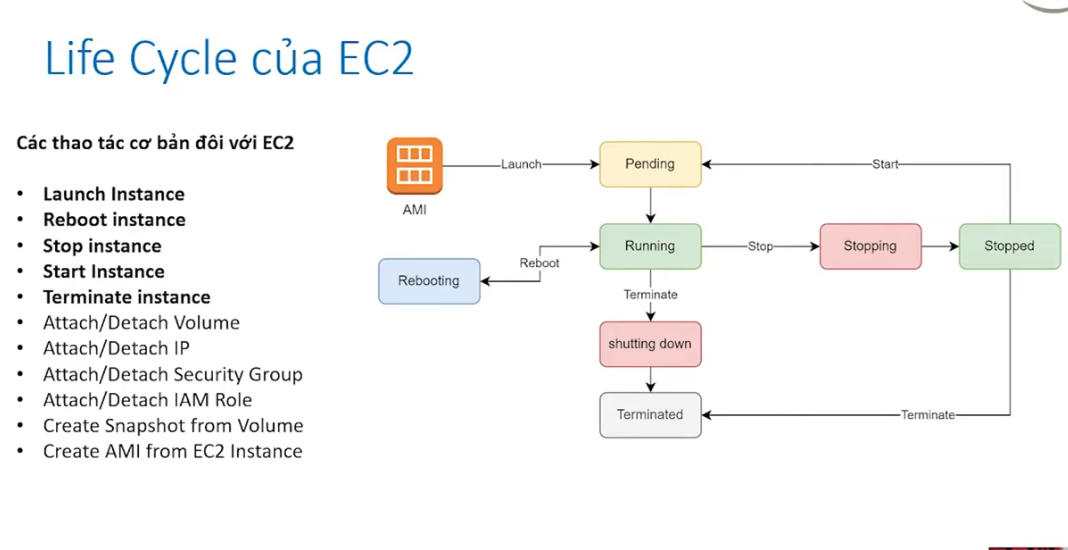
* **On-Demand Pricing** – Trả theo giờ/giây (linh hoạt, giá cao hơn).
* **Spot Pricing** – Giá rẻ hơn nhưng có thể bị AWS thu hồi nếu tài nguyên thiếu hụt.

**Reserved Pricing – Trả trước theo năm, giảm đến 75%.**

**Auto Scaling là gì?**

* Auto Scaling là quy trình tự động add mới hoặc remove EC2 instance dựa trên yêu cầu traffic của application hoặc của hệ thống.
* **ELB (Elastic Load Balancer) là gì? 🚀**
* **ELB (Elastic Load Balancer)** là một dịch vụ của AWS giúp **phân phối lưu lượng mạng (traffic)** giữa nhiều EC2 instances hoặc container để **cân bằng tải**, giúp hệ thống hoạt động ổn định và có khả năng mở rộng tốt hơn.
* **Mô hình cơ bản của Auto Scaling**





Tạo mới instance từ ami sau đó vô trạng thái pending và sau khi hoàn tất quá trình khởi động sẽ vào trạng thái running. bạn có thể thực hiện các hành động khác trên phiên bản. Chẳng hạn như khởi động lại (**reboot**), chấm dứt (**terminate**), dừng (**stop**) và dừng chế độ ngủ đông (**stop-hibernate**).

**Tổng quan về AWS ECS (Elastic Container Service)**

**1. AWS ECS là gì?**

**Amazon ECS (Elastic Container Service)** là dịch vụ quản lý container của AWS, giúp bạn chạy, dừng và quản lý **Docker container** trên cụm **EC2 instances** hoặc **AWS Fargate** mà không cần tự quản lý cơ sở hạ tầng.

**2. Kiến trúc ECS**

AWS ECS bao gồm các thành phần chính sau:

**1️⃣ Cluster**

* Là tập hợp các tài nguyên tính toán để chạy container (**EC2 instances hoặc Fargate**).

**2️⃣ Task Definition**

* Là cấu hình mô tả container, gồm:  
  ✅ Image Docker  
  ✅ CPU & RAM  
  ✅ Network (bridge, host, awsvpc)  
  ✅ Logging (CloudWatch Logs)  
  ✅ Các biến môi trường

**3️⃣ Task**

* Là một instance của **Task Definition** đang chạy trên ECS.

**4️⃣ Service**

* Đảm bảo **Task** chạy liên tục (có thể mở rộng hoặc tự phục hồi khi bị lỗi).

S3 Permissions xác định ai có thể **đọc, ghi, xóa** dữ liệu trong một **S3 bucket hoặc object**.  
Có 3 cách để cấp quyền trong S3:  
✅ **Bucket Policy** (Quy tắc cấp quyền cho cả bucket)  
✅ **IAM Policy** (Cấp quyền theo user hoặc role)  
✅ **ACL (Access Control List)** (Cấp quyền từng object)

**🔹 2. Bucket Policy là gì?**

**Bucket Policy** là một tập hợp các quy tắc kiểm soát quyền truy cập vào **toàn bộ bucket hoặc một phần bucket**.  
Bucket Policy sử dụng **JSON format** và có thể:  
✅ **Cho phép hoặc từ chối (Allow/Deny) quyền truy cập** vào bucket.  
✅ **Áp dụng cho user IAM, role, AWS account khác hoặc public**.  
✅ **Hạn chế quyền truy cập theo IP hoặc dịch vụ cụ thể**.

**🔹 1. Amazon EBS (Elastic Block Store) là gì?**

**Amazon EBS** là **bộ nhớ khối (block storage)** được gắn vào một **EC2 instance** để lưu trữ dữ liệu như ổ cứng HDD/SSD trong máy vật lý.

📌 **Đặc điểm chính của EBS:**  
✅ **Gắn trực tiếp vào EC2** (chỉ một EC2 sử dụng một volume tại một thời điểm).  
✅ **Tương tự ổ đĩa trên máy tính** (HDD hoặc SSD).  
✅ **Dữ liệu vẫn còn nếu EC2 bị tắt** (trừ khi chọn xóa khi terminate).

**Amazon EFS(elastic file system)** là **bộ nhớ tệp (file storage)** cho phép **nhiều EC2 cùng truy cập dữ liệu cùng lúc**.

📌 **Đặc điểm chính của EFS:**  
✅ **Hỗ trợ truy cập từ nhiều EC2 instances cùng lúc**.  
✅ **Tự động mở rộng dung lượng khi có thêm file**.

**1. Amazon VPC (Virtual Private Cloud)**

Amazon VPC là một dịch vụ cho phép bạn khởi chạy các tài nguyên AWS trong một mạng ảo được định nghĩa riêng. Các thành phần chính của VPC bao gồm:

### **1.1 Subnets (Mạng con)**

Subnet là một phần nhỏ của VPC, giúp phân chia mạng thành các khu vực khác nhau để tăng cường bảo mật và tối ưu hóa luồng dữ liệu.

* **Public Subnet (Mạng con công khai)**:
  + Có kết nối trực tiếp đến internet thông qua **Internet Gateway (IGW)**.
  + Thường chứa các tài nguyên có thể truy cập từ internet như **Web Server, Load Balancer**.
* **Private Subnet (Mạng con riêng tư)**:
  + Không thể kết nối trực tiếp với internet.
  + Thường chứa các tài nguyên nội bộ như **Database, Application Server**.
  + Có thể truy cập internet thông qua **NAT Gateway** để cập nhật hoặc gửi dữ liệu ra ngoài mà không bị truy cập từ internet.

### **1.2 Route Tables (Bảng định tuyến)**

Bảng định tuyến trong VPC xác định cách lưu lượng mạng được chuyển hướng đến các subnet và ra ngoài.

* **Mỗi subnet có một Route Table** xác định đường đi của gói tin.
* Route Table chứa các **Route (tuyến đường)** gồm:
  + **Destination (đích đến)**: CIDR block của mạng đích (ví dụ: 0.0.0.0/0 cho internet).
  + **Target (mục tiêu)**: Cổng hoặc thiết bị mạng chuyển tiếp gói tin (Internet Gateway, NAT Gateway, VPC Peering...).
* **Gateways**:
  + **Internet Gateway (IGW)**: Cung cấp truy cập internet cho subnet công khai.
  + **NAT Gateway**: Cho phép các instance trong subnet riêng gửi yêu cầu ra internet nhưng chặn lưu lượng vào.
  + **VPC Peering**: Kết nối hai VPC với nhau.

**2. Security Groups và Network ACLs**

**1.1 Security Groups là gì?**

* **Security Group (SG)** hoạt động như một **tường lửa ảo** cho các **instance** (máy ảo EC2).
* **SG được gắn vào từng instance**, giúp kiểm soát các kết nối vào và ra.
* **Chỉ có thể thiết lập ALLOW (cho phép), không thể BLOCK (chặn)**.

💡 **Ví dụ thực tế**:  
Bạn có một web server chạy trên EC2. Để cho phép người dùng truy cập, bạn cần mở cổng **80 (HTTP)** hoặc **443 (HTTPS)** trong Security Group.

**2.1 Network ACLs là gì?**

* **NACLs hoạt động ở cấp độ subnet, giúp kiểm soát lưu lượng vào và ra cho tất cả các instance trong subnet đó.**
* **NACLs giống như một firewall subnet, giúp tăng cường bảo mật hơn so với Security Group.**
* **Có thể cho phép (ALLOW) hoặc chặn (DENY) các kết nối.**

**💡 Ví dụ thực tế:  
Bạn có một private subnet chứa database và muốn chặn tất cả các truy cập từ internet. Bạn có thể cấu hình NACLs để từ chối (DENY) tất cả lưu lượng từ 0.0.0.0/0.**

**3. ELB (Elastic Load Balancing)**

**Elastic Load Balancing (ELB) là dịch vụ của AWS giúp cân bằng tải giữa nhiều EC2 instances, containers (ECS), hoặc IP addresses, đảm bảo ứng dụng của bạn chịu tải tốt hơn và luôn sẵn sàng.**

AWS cung cấp **3 loại Load Balancer chính**:

* **Application Load Balancer (ALB)** – Hoạt động ở **Lớp 7 (HTTP/HTTPS), phù hợp với ứng dụng web.**
* **Network Load Balancer (NLB)** – Hoạt động ở **Lớp 4 (TCP/UDP/TLS), thích hợp cho các ứng dụng yêu cầu hiệu suất cao.**
* **Classic Load Balancer (CLB)** – Hỗ trợ cả Lớp 4 & 7
* 🔹 **Lớp 4 và Lớp 7 là gì?**
* **Lớp 4 (Transport Layer – TCP/UDP)**: Chỉ quan tâm đến địa chỉ IP và cổng, không xem xét nội dung gói tin.
* **Lớp 7 (Application Layer – HTTP/HTTPS)**: Xử lý dữ liệu dựa trên nội dung HTTP (Headers, Cookies, Path, Query, Host).

Open Systems Interconnection

| * **Lớp** | **Tên** | **Chức năng chính** | **Ví dụ** |
| --- | --- | --- | --- |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lớp 7** | **Application (Ứng dụng)** | Giao tiếp trực tiếp với người dùng, cung cấp dịch vụ mạng như web, email, FTP. | HTTP, HTTPS, SMTP, FTP, DNS |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lớp 6** | **Presentation (Trình bày)** | Chuyển đổi định dạng dữ liệu (mã hóa, nén, giải mã). | SSL/TLS, JPEG, PNG, ASCII, MP3 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lớp 5** | **Session (Phiên kết nối)** | Quản lý kết nối giữa hai hệ thống, duy trì phiên giao tiếp. | NetBIOS, RPC, PPTP |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lớp 4** | **Transport (Vận chuyển)** | Kiểm soát truyền dữ liệu, đảm bảo tin cậy hoặc tốc độ cao. | TCP, UDP |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lớp 3** | **Network (Mạng)** | Định tuyến gói tin giữa các mạng khác nhau. | IP, ICMP, ARP, OSPF, BGP |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lớp 2** | **Data Link (Liên kết dữ liệu)** | Điều khiển truy cập mạng, phát hiện lỗi, đóng gói dữ liệu thành frame. | Ethernet, MAC Address, PPP, VLAN |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lớp 1** | **Physical (Vật lý)** | Truyền dữ liệu dưới dạng tín hiệu điện, quang hoặc sóng. | Cáp mạng, Wi-Fi, Bluetooth, sóng vô tuyến |

**4. Amazon CloudFront (CDN)**

mazon **CloudFront** là dịch vụ **mạng phân phối nội dung (Content Delivery Network - CDN)** của AWS, giúp **tăng tốc phân phối nội dung** như:  
✅ **Website tĩnh & động** (HTML, CSS, JS, API)  
✅ **Video, hình ảnh, file lớn**  
✅ **Ứng dụng web & API**  
✅ **Live streaming & video on demand**

CloudFront giúp **giảm độ trễ (latency), cải thiện tốc độ tải trang và tiết kiệm chi phí băng thông**, bằng cách lưu trữ dữ liệu tại các máy chủ biên (**Edge Locations**) gần với người dùng nhất.

**5. Amazon Route 53**

Route 53 là một dịch vụ DNS có khả năng:

* **Định tuyến lưu lượng** đến các dịch vụ AWS hoặc server khác.
* **Cung cấp DNS failover** để tăng tính sẵn sàng.
* **Hỗ trợ DNS health checks** nhằm giám sát trạng thái của các tài nguyên.