22110377_Huỳnh Minh Mẫn

Module 1: AWS Security Models

Các Thuật ngữ:

- Dịch vụ đám mây (Cloud services): Hệ thống công nghệ lưu trữ, xử lý và cho phép truy cập thông tin chia sẻ trong đám mây.

- Mô hình trách nhiệm chia sẻ (Shared responsibility model): Dịch vụ đám mây cung cấp công cụ và phương pháp bảo mật đám mây, nhưng người dùng cũng phải thực hiện bảo mật dựa trên các dịch vụ được cung cấp.

- Cơ sở hạ tầng như một dịch vụ (Infrastructure as a service - IaaS): Mô hình sử dụng các máy ảo và máy chủ để khách hàng có thể lưu trữ nhiều ứng dụng khác nhau và cung cấp các dịch vụ IT.

- Phần mềm như một dịch vụ (Software as a service - SaaS): Cung cấp các ứng dụng thông qua internet và do bên thứ ba quản lý.

- Nền tảng như một dịch vụ (Platform as a service - PaaS): Cung cấp một nền tảng ảo để khách hàng tạo phần mềm tùy chỉnh.

- Quản lý danh tính và quyền truy cập (Identity and access management - IAM): Áp dụng các kiểm soát đối với người dùng cần truy cập vào tài nguyên tính toán.

- Nguyên tắc đặc quyền tối thiểu (Principle of least privilege): Nguyên tắc này tập trung vào việc chỉ cấp các quyền tối thiểu cần thiết cho người dùng để thêm, sửa đổi hoặc xóa thông tin.

- Tấn công từ chối dịch vụ (Denial of service - DoS): Kẻ tấn công có thể thực hiện cuộc tấn công DoS đối với dịch vụ đám mây để làm cho nó không thể truy cập được, gây gián đoạn dịch vụ. Có nhiều cách để kẻ tấn công làm gián đoạn dịch vụ trong môi trường đám mây ảo hóa: sử dụng hết CPU, RAM, dung lượng đĩa hoặc băng thông mạng.

- Tấn công 'Watering hole': Một lỗ hổng bảo mật mà kẻ tấn công nhắm đến việc xâm nhập vào một nhóm người dùng cụ thể bằng cách nhiễm độc các trang web mà nhóm này thường truy cập. Mục tiêu là lây nhiễm máy tính của người dùng mục tiêu và truy cập vào mạng tại nơi làm việc của họ.

- Xác thực đa yếu tố (Multi-factor authentication - MFA): Hệ thống bảo mật yêu cầu nhiều hơn một phương pháp xác thực từ các loại thông tin xác thực độc

lập để xác minh danh tính của người dùng khi đăng nhập hoặc thực hiện giao dịch khác.

Phần nội dung:

Các mục tiêu bảo mật bao gồm tính bảo mật (confidentiality), toàn vẹn (integrity), khả dụng (availability), tính xác thực (authenticity), trách nhiệm giải trình (accountability), trách nhiệm pháp lý (liability) và quyền riêng tư (privacy) là cơ sở cho bảo mật CNTT nói chung. Những mục tiêu này cũng được áp dụng cho các hệ thống đám mây. Tuy nhiên, chúng không thể áp dụng một cách đơn giản cho các hệ thống đám mây theo tỷ lệ một-một vì các dịch vụ và kiến trúc ứng dụng khác nhau có các yêu cầu khác nhau.

Các thực tiễn tốt nhất về bảo mật AWS bắt đầu từ mô hình trách nhiệm chia sẻ của AWS, quy định những kiểm soát bảo mật nào thuộc trách nhiệm của AWS và kiểm soát nào thuộc trách nhiệm của khách hàng.

Theo bản chất của tên gọi "mô hình trách nhiệm chia sẻ của AWS", điều này rõ ràng rằng việc thực hiện bảo mật trên AWS Cloud không phải là trách nhiệm duy nhất của một bên nào, mà được chia sẻ giữa AWS và khách hàng.

Đám mây đang phát triển nhanh chóng và các dịch vụ mới đang xuất hiện hàng ngày.

Phần câu hỏi:

1. You own a small standalone coffee shop.

a. You have identified several resources that you would need to protect for your business.

Next, you need to prioritize your security needs. Evaluate the risk associated with each resource. Describe the impact a security breach would have on your business. Rate the likelihood of the resource being compromised, and then explain your rationale for your ratings.

Để bảo vệ an ninh cho quán cà phê nhỏ của tôi, cần xác định và ưu tiên các nhu cầu bảo mật. Mỗi nguồn tài nguyên đều có những rủi ro bảo mật khác nhau. Cần đánh giá tác động của sự cố bảo mật đối với từng nguồn tài nguyên và xác định khả năng nguồn tài nguyên đó bị xâm phạm. Sau đó, giải thích lý do cho mỗi mức độ đánh giá.

b. Use the following table as a guide:

Resource	If it were breached, what would be the impact on your business?	Likelihood the resource will be compromised (high, medium, low)	Rationale
Website	Nếu website của tôi bị xâm phạm, quán cà phê có thể mất doanh thu do khách hàng không thể đặt hàng online hoặc truy cập thông tin, gây ảnh hưởng đến uy tín của doanh nghiệp.	Trung bình	Website thường xuyên đối mặt với các mối đe dọa trực tuyến, nhưng nếu tôi bảo mật tốt thì khả năng bị xâm phạm có thể được giảm thiểu.
Customer credit card data	Nếu dữ liệu thẻ tín dụng bị xâm phạm, tôi có thể phải chịu trách nhiệm về các vi phạm an ninh nghiêm trọng, dẫn đến mất lòng tin từ khách hàng và có thể gặp phải các hậu quả pháp lý.	Cao	Dữ liệu thẻ tín dụng là thông tin nhạy cảm, và nếu không được mã hóa hoặc bảo vệ kỹ lưỡng, sẽ dễ bị tấn công bởi hacker nhằm mục đích trục lợi tài chính.
Employee information	Nếu thông tin nhân viên bị xâm phạm, tôi có thể mất lòng tin từ nhân viên và đối mặt với các vấn đề pháp lý, ảnh hưởng xấu đến danh tiếng của doanh nghiệp.	Thấp	Thông tin nhân viên thường được lưu trữ trong nội bộ và ít bị nhắm đến hơn, nhưng tôi vẫn cần bảo vệ nó để tránh các mối đe dọa về bảo mật nội bộ.

2. The PoLP is centered on the concept that the least number of permissions is to be applied to a user to search (READ), add (WRITE), delete (DELETE), modify (WRITE and/or DELETE), or edit permissions for all other users and take ownership for any and all data (FULL). The PoLP can be applied to every level of a system. It applies to end users, systems, processes, networks, databases, applications, and every other facet of an IT environment.

For example, with the PoLP, an employee whose job is to enter data into a database only needs the ability to add (WRITE) records to that specific database. If malware infects that employee's computer or if the employee clicks a link in a phishing email, the malicious attack is limited to making database entries. If that employee has root (FULL) access privileges, however, the infection can spread system-wide.

In your coffee shop, you have hired a new barista to help with the morning shift. They will be accepting customers' orders, filling the orders, and taking payment for the orders.

a. Use the PoLP to determine what systems this new employee would need access to. What privileges would they need for each system? Would you give them open access to your systems? Why or why not?

Trong quán cà phê của tôi, khi áp dụng nguyên tắc PoLP (nguyên tắc đặc quyền tối thiểu), nhân viên mới này chỉ cần truy cập vào các hệ thống cần thiết cho công việc của họ. Họ sẽ cần quyền truy cập vào hệ thống đặt hàng và thanh toán. Cụ thể:

- Hệ thống đặt hàng: Họ chỉ cần quyền WRITE để nhập các đơn hàng của khách hàng vào hệ thống.

- Hệ thống thanh toán: Họ cần quyền WRITE để xử lý các giao dịch thanh toán.

Tôi sẽ không cho họ quyền truy cập mở rộng vào các hệ thống khác như quản lý dữ liệu khách hàng, kho hàng, hay quản lý hệ thống vì điều này không cần thiết cho vai trò của họ. Nếu cho họ quyền truy cập quá mức, rủi ro bảo mật sẽ tăng lên, ví dụ như việc truy cập nhầm hoặc vi phạm dữ liệu. Vì vậy, việc hạn chế quyền truy cập là rất quan trọng để đảm bảo an toàn thông tin cho doanh nghiệp của tôi.

b. Your coffee shop has added a new frequent buyer program. What additional systems (if any) would this new employee need access to? What privileges would they need for each system? Is it sensible from an information security standpoint to provide them with each of these privileges?

Với chương trình khách hàng thân thiết mới được thêm vào, nhân viên này có thể cần truy cập vào hệ thống quản lý khách hàng để ghi nhận và theo dõi số lần mua hàng của khách. Tuy nhiên, theo nguyên tắc PoLP, tôi chỉ cấp cho họ quyền READ và WRITE trên hệ thống khách hàng thân thiết, đủ để họ ghi nhận và cập nhật thông tin mua hàng.

Việc cấp quyền hạn chế này là hợp lý từ góc độ bảo mật thông tin vì nó giúp ngăn chặn việc truy cập không cần thiết hoặc nhầm lẫn. Họ không cần có quyền DELETE hay FULL để chỉnh sửa thông tin quan trọng, vì điều đó sẽ làm tăng rủi ro bảo mật cho hệ thống.

3. A DoS attack is a deliberate attempt to make your website or application unavailable to users, such as by flooding it with network traffic. To achieve this, attackers use a variety of techniques that consume large amounts of network bandwidth or tie up other system resources, disrupting access for legitimate users. In its simplest form, a lone attacker uses a single source to run a DoS attack against a target.

But in a distributed denial of service (DDoS) attack, an attacker uses multiple sources—which might be distributed groups of malware-infected computers, routers, Internet of Things (IoT) devices, and other endpoints—to orchestrate an attack against a target. A network of compromised hosts participates in the attack, generating a flood of packets or requests to overwhelm the target.

The most common DDoS attacks are infrastructure layer attacks. An attacker generates large volumes of traffic that can inundate the capacity of a network or tie up resources on systems like a server, firewall, intrusion protection system (IPS), or load balancer. Although these attacks can be easy to identify, to effectively mitigate them, you must have a network or systems that scale up capacity more rapidly than the inbound traffic flood. This extra capacity is to filter out or absorb the attack traffic, enabling your system and application to respond to your legitimate customer traffic.

a. How would the owner of a coffee shop best protect their assets from a DDoS?

Để bảo vệ quán cà phê của tôi khỏi tấn công DDoS, tôi sẽ sử dụng CDN để phân tán lưu lượng và WAF để lọc các yêu cầu độc hại. Đồng thời, tôi chọn nhà cung cấp dịch vụ có khả năng mở rộng linh hoạt, giám sát lưu lượng mạng thường xuyên để phát hiện các bất thường, và đăng ký dịch vụ chống DDoS từ các nhà cung cấp lớn như AWS hoặc Cloudflare để ngăn chặn tấn công hiệu quả. Các biện pháp này giúp duy trì hoạt động ổn định và bảo vệ tài sản của tôi.

Module 2: Shared Security

Các Thuật ngữ:

- Amazon Inspector: Dịch vụ đánh giá bảo mật tự động giúp kiểm tra khả năng truy cập mạng của các phiên bản Amazon Elastic Compute Cloud (Amazon EC2) và tình trạng bảo mật của các ứng dụng chạy trên các phiên bản đó.

- AWS Trusted Advisor: Dịch vụ đánh giá bảo mật áp dụng cho toàn bộ tài khoản Amazon Web Services (AWS). Nó cung cấp lời khuyên về các thực tiễn tốt nhất liên quan đến bảo mật, tối ưu hóa chi phí, hiệu suất, khả năng chịu lỗi, và giới hạn dịch vụ.

- Amazon Simple Storage Service (Amazon S3): Dịch vụ do AWS cung cấp để lưu trữ dữ liệu của người dùng trên đám mây.

- Xác thực đa yếu tố (Multi-factor authentication - MFA): Hệ thống bảo mật yêu cầu nhiều hơn một phương pháp xác thực từ các loại thông tin xác thực độc lập để xác minh danh tính của người dùng khi đăng nhập hoặc thực hiện giao dịch khác.

- AWS Identity and Access Management (IAM): Kiểm soát quyền truy cập cho người dùng cần tiếp cận các tài nguyên tính toán.

- Amazon Elastic Block Store (Amazon EBS): Lưu trữ dành riêng cho các phiên bản EC2. Có thể coi nó như ổ đĩa lưu trữ cho phiên bản EC2 của bạn.

- Amazon Relational Database Service (Amazon RDS): Dịch vụ cho phép các nhà phát triển tạo và quản lý cơ sở dữ liệu quan hệ trên đám mây. Cơ sở dữ liệu quan hệ là tập hợp dữ liệu với các mối quan hệ 1-1. Ví dụ, cơ sở dữ liệu giao dịch trong một cửa hàng sẽ khớp từng khách hàng với các lần mua hàng của họ. Amazon RDS cho phép các nhà phát triển theo dõi lượng dữ liệu lớn và tìm kiếm thông tin một cách hiệu quả. RDS được trang bị ngôn ngữ truy vấn có cấu trúc (SQL) giúp người dùng tương tác dễ dàng với RDS.

Phần nội dung:

Các dịch vụ đa dạng do AWS cung cấp có thể được kết hợp theo nhiều cách khác nhau để đạt được các mục tiêu của một ứng dụng. Amazon Inspector và Trusted Advisor là những công cụ để đo lường mức độ hiệu quả của cách tiếp cận nhất định trong việc đạt được các mục tiêu về chi phí, hiệu suất, hiệu quả, và bảo mật. Module này khám phá Amazon Inspector và Trusted Advisor, đồng thời cung cấp một khung so sánh giữa hai dịch vụ quan trọng của AWS này.

Trusted Advisor là một công cụ trực tuyến quét cơ sở hạ tầng AWS của khách hàng, so sánh với các thực tiễn tốt nhất của AWS trong năm hạng mục và cung cấp hướng dẫn theo thời gian thực để giúp khách hàng cấp phát tài nguyên trong khi tuân thủ các thực tiễn tốt nhất của AWS. Nó làm nổi bật các vấn đề tiềm năng trong cách khách hàng sử dụng AWS.

Amazon Inspector kiểm tra khả năng truy cập mạng của các phiên bản EC2 của khách hàng và tình trạng bảo mật của các ứng dụng chạy trên những phiên bản đó. Amazon Inspector tạo ra danh sách chi tiết các phát hiện về bảo mật, được ưu tiên theo mức độ nghiêm trọng. Những phát hiện này có thể được xem trực tiếp hoặc là một phần của các báo cáo đánh giá chi tiết có sẵn qua bảng điều khiển Amazon Inspector hoặc giao diện lập trình ứng dụng (API). Tự động hóa là một nguyên tắc trung tâm của các phương pháp bảo mật hiện đại; khách hàng AWS có thể tự động hóa các bài kiểm tra bảo mật với Amazon Inspector.

Sự khác biệt chính giữa hai dịch vụ này:

- Trusted Advisor áp dụng cho tài khoản AWS và quản trị AWS.

- Amazon Inspector áp dụng cho nội dung của các phiên bản EC2 khác nhau.

Phần câu hỏi:

1. Make a list of functions that a nutritional advisor might perform. Which of these advisory functions can be automated? Do you foresee any security concerns with automating any of these functions?

Danh sách chức năng của cố vấn dinh dưỡng: Phân tích khẩu phần ăn, tư vấn chế độ dinh dưỡng, theo dõi tiến trình sức khỏe.

Chức năng có thể tự động hóa: Theo dõi tiến trình và đưa ra kế hoạch dinh dưỡng cơ bản.

Lo ngại bảo mật: Rủi ro lộ thông tin cá nhân nếu không bảo mật tốt.

2. What functions do fitness trackers provide? How might a fitness tracker assist a nutritional advisor to meet a customer’s health and fitness needs?

Chức năng của thiết bị theo dõi thể chất: Đo nhịp tim, số bước, lượng calo tiêu thụ.

Cách hỗ trợ cố vấn dinh dưỡng: Cung cấp dữ liệu về hoạt động thể chất để tư vấn dinh dưỡng chính xác hơn.

3. Make a list of functions that a cloud security advisor might perform. Which of these advisory functions can be automated? Do you foresee any security concerns with automating any of these functions?

Danh sách chức năng của cố vấn bảo mật đám mây: Đánh giá bảo mật, phát hiện lỗ hổng, đề xuất biện pháp bảo mật.

Chức năng có thể tự động hóa: Quét lỗ hổng và cảnh báo bảo mật.

Lo ngại bảo mật: Hệ thống tự động có thể bị tấn công hoặc tạo ra lỗi nếu không giám sát tốt.

4. What functions would you anticipate a security tracker such as Amazon Inspector to provide? How might a security tracker assist a security advisor such as Trusted Advisor to meet the organization's security needs?

Chức năng của Amazon Inspector: Quét lỗ hổng bảo mật, cung cấp báo cáo chi tiết.

Cách hỗ trợ Trusted Advisor: Cung cấp thông tin về lỗ hổng để Trusted Advisor đưa ra giải pháp bảo mật tổng thể.

Module 3: Cloud Services and Instance States

Các Thuật ngữ:

- Amazon Elastic Compute Cloud (Amazon EC2): Dịch vụ web cung cấp khả năng tính toán bảo mật và có thể thay đổi kích thước trên đám mây. Hãy nghĩ về nó như việc thuê một máy tính trong đám mây.

- EC2 instance: Một máy chủ ảo trong Amazon Elastic Compute Cloud (Amazon EC2) để chạy các ứng dụng trên hạ tầng Amazon Web Services (AWS).

- Amazon Elastic Block Store (Amazon EBS): Lưu trữ dành riêng cho các phiên bản Amazon Elastic Compute Cloud (Amazon EC2). Hãy nghĩ về nó như ổ đĩa lưu trữ cho phiên bản EC2 của bạn.

- Instance store volumes: Lưu trữ tạm thời, không được duy trì sau khi phiên bản bị dừng, kết thúc, hoặc gặp lỗi phần cứng.

- Amazon Machine Image (AMI): Một loại thiết bị ảo đặc biệt được sử dụng để tạo máy ảo (VM) trong Amazon Elastic Compute Cloud (Amazon EC2). Nó là đơn vị cơ bản để triển khai các dịch vụ sử dụng Amazon EC2.

- Địa chỉ IPv4 (IPv4 address): Một số 32-bit nhận dạng duy nhất một giao diện mạng trên một máy. Địa chỉ IPv4 thường được viết dưới dạng số thập phân và được định dạng thành bốn trường 8-bit, phân cách bằng dấu chấm.

- Địa chỉ IPv6 (IPv6 address): Một chuỗi ký tự 128-bit nhận dạng thiết bị trong hệ thống địa chỉ của IPv6. Địa chỉ IPv6 thường được sử dụng bởi các chuyên gia như kỹ sư mạng, công ty công nghệ, trung tâm dữ liệu và nhà mạng di động.

- Địa chỉ IP linh hoạt (Elastic IP address): Một địa chỉ IPv4 tĩnh được thiết kế cho tính toán đám mây động và được liên kết với tài khoản Amazon Web Services (AWS) của bạn. Địa chỉ Elastic IP vẫn giữ nguyên ngay cả khi xảy ra các sự kiện thường làm thay đổi địa chỉ như dừng hoặc khởi động lại phiên bản.

Phần nội dung:

Một trong những lợi ích chính của công nghệ đám mây là khả năng trả phí chỉ cho những gì cần và trả theo mức độ sử dụng. Để làm được điều này, chi phí cho các máy ảo (VMs) trong AWS được chia thành các trạng thái mà các phiên bản (instances) trải qua trong suốt vòng đời của chúng.

Khi khởi chạy một phiên bản ban đầu, nó sẽ vào trạng thái đang chờ xử lý (pending). Điều này có nghĩa là AWS đang chuẩn bị phiên bản, và chưa thể truy cập vào nó. Sau khi phiên bản sẵn sàng, nó sẽ chuyển sang trạng thái đang chạy (running). Có thể kết nối với phiên bản đang chạy và sử dụng nó giống như đang sử dụng một máy tính trước mặt mình.

Ngay khi phiên bản chuyển sang trạng thái đang chạy sẽ bị tính phí theo từng giây, với tối thiểu 1 phút, ngay cả khi phiên bản vẫn không hoạt động và không kết nối với nó.

Khi không còn cần phiên bản nữa, có thể dừng hoặc kết thúc (terminate) nó. Ngay khi trạng thái của phiên bản thay đổi thành đang tắt (shutting down) hoặc đã kết thúc (terminated), sẽ ngừng bị tính phí cho phiên bản đó. Có thể dừng hoặc đặt phiên bản ở chế độ ngủ đông (hibernate) và khởi động lại sau. Tuy nhiên, một số dữ liệu tạm thời có thể bị mất khi bạn thực hiện điều này.

Characteristic	Reboot	Stop/Start (Amazon EBS Backed Instances Only)	Hibernate (Amazon EBS Backed Instances Only)	Terminate

Máy chủ (Host computer)	Phiên bản vẫn ở trên cùng một máy chủ.	Trong hầu hết các trường hợp, chúng tôi di chuyển phiên bản sang một máy chủ mới. Phiên bản có thể ở lại trên cùng một máy chủ nếu không có vấn đề gì với máy chủ.	Trong hầu hết các trường hợp, chúng tôi di chuyển phiên bản sang một máy chủ mới. Phiên bản có thể ở lại trên cùng một máy chủ nếu không có vấn đề gì với máy chủ.	Không có.
Địa chỉ IPv4 riêng và công cộng	Các địa chỉ này không thay đổi.	Phiên bản giữ địa chỉ IPv4 riêng. Phiên bản sẽ nhận được địa chỉ IPv4 công cộng mới, trừ khi nó có địa chỉ Elastic IP, địa chỉ này không thay đổi trong quá trình dừng hoặc bắt đầu.	Phiên bản giữ địa chỉ IPv4 riêng. Phiên bản sẽ nhận được địa chỉ IPv4 công cộng mới, trừ khi nó có địa chỉ Elastic IP, địa chỉ này không thay đổi trong quá trình dừng hoặc bắt đầu.	Không có.
Địa chỉ Elastic IP (IPv4)	Địa chỉ Elastic IP vẫn được liên kết với phiên bản.	Địa chỉ Elastic IP vẫn được liên kết với phiên bản.	Địa chỉ Elastic IP vẫn được liên kết với phiên bản.	Địa chỉ Elastic IP không còn được liên kết với phiên bản.
Địa chỉ IPv6	Địa chỉ không thay đổi.	Phiên bản giữ địa chỉ IPv6.	Phiên bản giữ địa chỉ IPv6.	Không có.
Dung lượng bộ lưu trữ	Dữ liệu được bảo toàn.	Dữ liệu bị xóa.	Dữ liệu bị xóa.	Dữ liệu bị xóa.

phiên bản				
Dung lượng ổ đĩa gốc	Dung lượng được bảo toàn.	Dung lượng được bảo toàn.	Dung lượng được bảo toàn.	Dung lượng bị xóa theo mặc định.
Bộ nhớ truy cập ngẫu nhiên (RAM)	RAM bị xóa.	RAM bị xóa.	RAM được lưu vào tệp trên ổ đĩa gốc.	RAM bị xóa.
Thanh toán (Billing)	Giờ tính phí của phiên bản không thay đổi.	Bạn ngừng bị tính phí cho một phiên bản ngay khi trạng thái của nó chuyển sang dừng. Mỗi khi phiên bản chuyển từ dừng sang chạy, chúng tôi bắt đầu một kỳ tính phí mới, tính tối thiểu 1 phút mỗi lần bạn khởi động lại phiên bản.	Bạn bị tính phí khi phiên bản ở trạng thái dừng nhưng ngừng tính phí khi phiên bản ở trạng thái dừng hẳn. Mỗi khi phiên bản chuyển từ dừng sang chạy, chúng tôi bắt đầu một kỳ tính phí mới, tính tối thiểu 1 phút mỗi lần bạn khởi động lại phiên bản.	Bạn ngừng bị tính phí cho một phiên bản ngay khi trạng thái của nó chuyển sang kết thúc.

Phần câu hỏi:

1. When it comes to cell phone plans, understanding your data usage can help you save money. Understanding usage and state of your EC2 instances can help you better provision your resources to control costs.

   a. What is considered data usage on your cell phone?

Sử dụng dữ liệu trên điện thoại di động được coi là tất cả các hoạt động truy cập internet hoặc truyền tải dữ liệu qua mạng di động, bao gồm việc xem

video, tải tệp, duyệt web, sử dụng ứng dụng cần kết nối mạng, gửi và nhận email, hoặc sử dụng các dịch vụ phát trực tuyến.

b. What are some common ways data is used on smartphones? How is this similar to using EC2 instances for computing power?

Một số cách sử dụng dữ liệu phổ biến trên smartphone bao gồm: xem video, lướt web, chơi game trực tuyến, phát nhạc, và sử dụng mạng xã hội. Điều này tương tự như việc sử dụng phiên bản EC2 cho sức mạnh tính toán, khi người dùng chạy các ứng dụng, xử lý dữ liệu, hoặc lưu trữ nội dung trên đám mây. Cả hai đều liên quan đến việc sử dụng tài nguyên mạng và điện toán một cách liên tục và tính phí dựa trên mức độ sử dụng.

2. Why might you use an On-Demand Instance when you can predict your instance needs far in advance or for ongoing, fluctuating computing power?

a. What attributes are used to determine the price of family cell phone plans? When would it be desirable to pay a set amount for instances rather than a variable amount based on usage?

Các yếu tố được sử dụng để xác định giá của gói cước điện thoại gia đình bao gồm: số lượng người sử dụng trong gói, dung lượng dữ liệu được chia sẻ, tốc độ truy cập mạng, và các tính năng bổ sung như tin nhắn, cuộc gọi không giới hạn. Tương tự, trong trường hợp của EC2, việc trả một mức giá cố định (ví dụ như Reserved Instances) thay vì biến đổi theo mức sử dụng có thể hữu ích khi bạn biết rõ nhu cầu tài nguyên trong dài hạn và muốn tối ưu chi phí, đặc biệt khi cần sức mạnh tính toán liên tục và ổn định.

Module 4: Dynamic Web Servers I

Các Thuật ngữ:

- Trang web tĩnh (Static website): Một trang web không thay đổi dựa trên tương tác của người dùng; thường được xây dựng bằng HyperText Markup Language (HTML) và Cascading Style Sheets (CSS).

- Trang web động (Dynamic website): Một trang web thay đổi dựa trên tương tác của người dùng; thường được xây dựng bằng Python, JavaScript, PHP, hoặc ASP kết hợp với HTML.

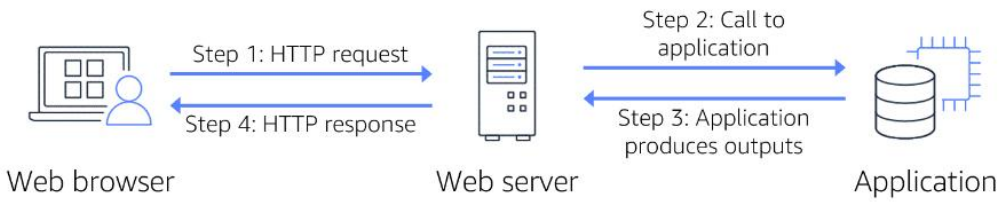
Phần nội dung:

Trang web tĩnh được cung cấp cho người dùng đúng như cách nó được lưu trữ, trái ngược với trang web động, được tạo ra bởi một ứng dụng web. Trang web tĩnh phù hợp nhất với các trang có ít tác giả và nội dung thay đổi không

thường xuyên. Các trường hợp sử dụng phổ biến của trang web tĩnh là các trang cá nhân và trang marketing đơn giản. Trang web tĩnh cung cấp các tệp HTML, JavaScript, hình ảnh, video và các tệp khác cho khách truy cập trang web của bạn, và không chứa mã ứng dụng.

Static Website

Trang web động khác biệt bởi việc sử dụng các ứng dụng web để tạo ra các trang riêng lẻ trên trang web. Có hai loại chính của trang web động: loại được xây dựng trên phần mềm quản lý nội dung (CMS) và loại được xây dựng từ đầu. Hệ thống CMS chứa các tệp, hình ảnh và video được sử dụng để xây dựng giao diện hiển thị bởi trình duyệt trên máy khách. Việc xây dựng này được thực hiện trên máy chủ và gửi đến dưới dạng các tệp HTML cho máy khách. Tất cả quá trình này được thực hiện để đáp ứng yêu cầu nhận từ máy khách. Các trang web dựa trên CMS như WordPress, Joomla và Drupal cung cấp cho người chỉnh sửa trang web các tính năng để dễ dàng xây dựng và cập nhật trang web.



Dynamic Website

Trang web động được xây dựng từ đầu mang lại tính tương tác cao hơn (ví dụ: đặt vé máy bay, xem phim trực tuyến) và dựa vào logic ứng dụng, chẳng hạn như các tập lệnh Python, PHP, hoặc Ruby trên máy chủ, để hiển thị trang web.

Phần câu hỏi:

1. Have you ever seen a website run by a sole author or with infrequent updates? What was the website? Did the lack of current content or updates

make you feel a certain way? This is known as a static website. Why do you think people choose this type of website?

Tôi đã từng thấy một trang web do một tác giả duy nhất quản lý hoặc có ít cập nhật, ví dụ như các blog cá nhân hoặc trang giới thiệu công việc cá nhân. Thiếu cập nhật hoặc nội dung mới thường khiến tôi cảm thấy trang web không được quan tâm hoặc kém chuyên nghiệp. Những người chọn loại trang web tĩnh này thường vì chi phí thấp, dễ duy trì, và không cần thay đổi thường xuyên.

2. Have you ever used a website to consume a lot of content, such as a video-streaming service? What was it? This is an example of a dynamic website. How is this website different than other websites you have used?

Tôi đã sử dụng các trang web để tiêu thụ nhiều nội dung, chẳng hạn như dịch vụ xem phim trực tuyến Netflix. Đây là một ví dụ về trang web động. Khác với các trang tĩnh, Netflix tương tác nhiều hơn với người dùng, cho phép chọn phim, phát trực tuyến và điều chỉnh theo sở thích cá nhân. Sự khác biệt rõ rệt là tính tương tác và khả năng thay đổi nội dung theo nhu cầu người dùng.

3. What is the most informative website you use? Which is the least informative website you use? Which website that you use has the most features? How do these features help you?

Trang web cung cấp nhiều thông tin nhất mà tôi sử dụng có lẽ là Wikipedia, vì nó chứa rất nhiều bài viết đa dạng và chi tiết. Trang ít thông tin nhất mà tôi dùng có thể là một trang web bán hàng nhỏ lẻ chỉ liệt kê sản phẩm mà không cung cấp nhiều thông tin chi tiết. Trang web có nhiều tính năng nhất mà tôi sử dụng là Google, với các công cụ tìm kiếm, bản đồ, dịch vụ email, và nhiều hơn nữa. Những tính năng này giúp tôi tìm kiếm thông tin nhanh chóng, liên lạc, và định vị một cách tiện lợi.

Module 5: Dynamic Web Servers II

Các Thuật ngữ:

- Amazon CloudFront: Dịch vụ mạng phân phối nội dung (CDN) cung cấp nội dung như video, dữ liệu, ứng dụng, và nhiều hơn nữa một cách an toàn.

- Mạng phân phối nội dung (Content delivery network - CDN): Một mạng lưới các dịch vụ phân phối nội dung web và các trang web dựa trên vị trí địa lý của người dùng một cách an toàn.

- Vị trí biên (Edge location): Nơi nội dung web được lưu trữ tạm thời (được lưu vào bộ nhớ đệm - cached).

- Nguồn gốc (Origin): Vị trí nơi tất cả các đối tượng liên quan đến trang web được lưu trữ vĩnh viễn.

- Phân phối (Distribution): Tập hợp các vị trí biên.

- Thời gian sống (Time to live - TTL): Thời gian tối thiểu và tối đa để lưu trữ nội dung trong bộ nhớ đệm tại vị trí biên.

Phần nội dung:

CloudFront là một dịch vụ mạng phân phối nội dung (CDN) nhanh, cung cấp dữ liệu, video, ứng dụng và giao diện lập trình ứng dụng (API) cho khách hàng trên toàn cầu với độ trễ thấp và tốc độ truyền cao, tất cả đều trong một môi trường thân thiện với nhà phát triển. CloudFront được tích hợp với Amazon Web Services (AWS) — các địa điểm vật lý được kết nối trực tiếp với cơ sở hạ tầng toàn cầu của AWS và các dịch vụ khác của AWS. CloudFront hoạt động liền mạch với các dịch vụ bao gồm AWS Shield để giảm thiểu tấn công từ chối dịch vụ phân tán (DDoS), Amazon Simple Storage Service (Amazon S3), Elastic Load Balancing (ELB) hoặc Amazon Elastic Compute Cloud (Amazon EC2) làm nguồn gốc cho các ứng dụng, và Lambda@Edge để chạy mã tùy chỉnh gần hơn với người dùng và tùy chỉnh trải nghiệm của họ.

Mạng CDN của CloudFront được mở rộng quy mô lớn và phân phối toàn cầu. Mạng CloudFront có 200 điểm hiện diện (PoPs), và sử dụng mạng xương sống AWS có độ bền cao để mang lại hiệu suất và khả năng sẵn sàng tốt nhất cho người dùng cuối.

CloudFront là một CDN bảo mật cao cung cấp bảo vệ ở cấp độ mạng và ứng dụng. Có thể sử dụng các tính năng có thể cấu hình như AWS Certificate Manager (ACM) để tạo và quản lý chứng chỉ SSL tùy chỉnh.

Các tính năng của CloudFront có thể được tùy chỉnh theo yêu cầu cụ thể của ứng dụng. Các chức năng Lambda@Edge, được kích hoạt bởi các sự kiện của CloudFront, mở rộng mã tùy chỉnh đến các vị trí AWS trên toàn thế giới, vì vậy người dùng có thể di chuyển logic ứng dụng phức tạp đến gần người dùng cuối hơn để cải thiện khả năng phản hồi.

CloudFront được tích hợp với các dịch vụ AWS như Amazon S3, Amazon EC2, ELB, Amazon Route 53, và AWS Elemental Media Services.

Phần câu hỏi:

1. Have you ever experienced a persistently slow website? Describe the website, its content, and your experiences.

Tôi đã từng gặp phải một trang web chạy rất chậm, đó là một trang thương mại điện tử nhỏ với nhiều hình ảnh sản phẩm và video giới thiệu. Mỗi khi tôi cố gắng tải trang hoặc xem hình ảnh chi tiết của sản phẩm, trang mất rất nhiều thời gian để phản hồi, khiến trải nghiệm của tôi rất khó chịu. Việc trang web quá tải nội dung và không được tối ưu hóa làm giảm hiệu suất truy cập đáng kể.

2. CloudFront allows websites to cache content around the world using edge locations. How could a service like CloudFront improve performance for a website that is persistently slow?

CloudFront có thể cải thiện hiệu suất của một trang web chậm bằng cách lưu trữ (cache) nội dung tại các vị trí biên (edge locations) trên toàn thế giới. Điều này giúp nội dung được truy xuất từ vị trí gần nhất với người dùng, giảm độ trễ và thời gian tải trang. Nhờ đó, các trang web nặng về hình ảnh và video sẽ tải nhanh hơn, cải thiện trải nghiệm người dùng.

3. How would using CloudFront to cache content around the world using edge locations help provide steady, expedient access to a website around the world?

Sử dụng CloudFront để lưu trữ nội dung tại các vị trí biên trên toàn thế giới giúp cung cấp quyền truy cập ổn định và nhanh chóng cho người dùng ở khắp mọi nơi. Bằng cách đưa nội dung gần hơn với vị trí của người dùng, CloudFront giảm thiểu khoảng cách truyền tải dữ liệu, giúp trang web phản hồi nhanh và duy trì tốc độ truy cập ổn định, ngay cả khi người dùng truy cập từ các khu vực địa lý khác nhau.