22110377_Huỳnh Minh Mẫn

Module 6: Virtual Storage

Các Thuật ngữ:

- Amazon Elastic Block Store (Amazon EBS): Lưu trữ dành riêng cho các phiên bản Amazon Elastic Compute Cloud (Amazon EC2).

- Amazon Elastic Compute Cloud (Amazon EC2): Dịch vụ web cung cấp khả năng tính toán có thể thay đổi kích thước một cách an toàn trên đám mây.

- Hard disk drive (HDD): Lưu trữ chậm hơn, sử dụng đĩa quay để lưu trữ dữ liệu.

- Input/Output Operations Per Second (IOPS): Thước đo hiệu suất thường dùng để đánh giá các thiết bị lưu trữ máy tính như ổ cứng HDD và ổ cứng thể rắn SSD.

- Solid state drive (SSD): Lưu trữ rất nhanh, sử dụng bộ nhớ flash thay vì đĩa quay.

Phần nội dung:

- Amazon EBS là kho lưu trữ cho các phiên bản EC2 với những lợi ích chính:

    + Tính khả dụng của dữ liệu

    + Tính bền vững của dữ liệu

    + Mã hóa dữ liệu

    + Ảnh chụp nhanh (Snapshots)

- Amazon EBS được triển khai dưới dạng một loạt các khối cố định có thể đọc và ghi bởi hệ điều hành. Các khối này tương tự như hệ thống tệp NTFS hoặc FAT chạy trên PC hoặc Mac, nghĩa là chúng có thể được truy cập nhanh chóng. Có hai loại khối EBS chính, và mỗi loại lớn có hai loại con. Mỗi loại có lợi ích và hạn chế riêng

- Amazon S3 được triển khai dưới dạng các đối tượng cần được ứng dụng sử dụng đối tượng đó đọc và ghi. Các đối tượng chứa siêu dữ liệu - dữ liệu về thuộc tính của đối tượng giúp hệ thống phân loại và xác định đối tượng. Ví dụ về đối tượng bao gồm hình ảnh, video, và nhạc. Các đối tượng không thể xử lý dần dần mà phải được đọc và ghi toàn bộ, điều này có thể ảnh hưởng đến hiệu suất và tính nhất quán.

- Một số điểm khác biệt chính giữa Amazon S3 và Amazon EBS:

    + Amazon EBS chỉ có thể sử dụng khi được gắn vào một phiên bản EC2. Trong khi đó, Amazon S3 có thể được truy cập độc lập bằng giao thức HTTP.

    + Amazon EBS không thể lưu trữ nhiều dữ liệu như Amazon S3.

    + Amazon EBS chỉ có thể gắn vào một phiên bản EC2, trong khi dữ liệu trong một bucket S3 có thể được truy cập bởi nhiều phiên bản EC2.

+ Amazon S3 có độ trễ cao hơn so với Amazon EBS khi ghi dữ liệu.

+ Các khối EBS được mã hóa toàn bộ, trong khi các đối tượng Amazon S3 được mã hóa riêng lẻ bằng mã hóa phía máy chủ (SSE).

- Amazon EBS bao gồm ba loại khối, trong khi Amazon S3 có nhiều loại hơn, bao gồm:

+ S3 Standard

+ S3 Standard-Infrequent Access (S3 Standard-IA)

+ S3 One Zone-Infrequent Access (S3 One Zone-IA)

+ S3 Intelligent-Tiering

+ S3 Glacier

+ S3 Glacier Deep Archive

Phần câu hỏi:

Questions

1. In your opinion, how has cloud computing impacted the way that society interacts with technology? Is it a positive or negative impact overall? Why?

Điện toán đám mây đã thay đổi cách mọi người sử dụng công nghệ, giúp dễ dàng truy cập vào tài nguyên trực tuyến từ bất kỳ đâu mà không cần đầu tư vào hạ tầng phần cứng. Điều này làm tăng tính tiện lợi và khả năng cộng tác, đặc biệt trong học tập và công việc từ xa. Mặc dù có những lo ngại về bảo mật, em cho rằng tác động tổng thể là tích cực vì nó giúp công nghệ trở nên dễ tiếp cận hơn và hiệu quả hơn.

2. In an election, it is important to make sure that the vote count is accurate. Do you know how votes are actually counted? In some areas, election officials manually read each ballot and add up the number of votes in each race. Other areas have computerized voting systems that transmit vote totals to the central counting facility. Computerized voting is faster than counting ballots by hand, but some people argue that it is risky because it opens elections up to the possibility of hacking. Do you think that it is a good idea to use cloud services to protect and count votes? Why or why not?

Em nghĩ rằng sử dụng dịch vụ đám mây để đếm phiếu bầu có thể hiệu quả, vì tốc độ và tính chính xác được cải thiện. Tuy nhiên, việc này cần đảm bảo các biện pháp bảo mật cao cấp để tránh rủi ro bị tin tặc tấn công. Nếu có sự giám sát chặt chẽ và hệ thống bảo mật tốt thì em thấy đây là một giải pháp khả thi, nhưng cần cẩn trọng để đảm bảo tính minh bạch và công bằng trong bầu cử.

3. As a student, how do you think cloud computing services could improve your school? Think about the ways that you turn in work, take exams, attend classes and events, or any other factor related to your school.

Điện toán đám mây có thể giúp trường học em rất nhiều, đặc biệt trong việc nộp bài, lưu trữ tài liệu, và làm bài kiểm tra trực tuyến. Sinh viên có thể dễ dàng truy cập tài liệu học tập mọi lúc mọi nơi, và các giáo viên cũng có thể quản lý bài tập, điểm số nhanh chóng hơn. Ngoài ra, các lớp học trực tuyến hoặc hội thảo qua đám mây sẽ giúp tăng sự linh hoạt trong việc học, nhất là trong bối cảnh hiện nay.

Module 7: Security I

Các Thuật ngữ:

- AWS Identity and Access Management (IAM): Liên quan đến việc áp dụng các kiểm soát cho người dùng cần truy cập vào tài nguyên điện toán.

- Role: Một danh tính IAM mà bạn có thể tạo trong tài khoản của mình với các quyền cụ thể.

- User: Một thực thể mà bạn tạo trong Amazon Web Services (AWS) để đại diện cho người hoặc ứng dụng sử dụng nó để tương tác với AWS. Một người dùng trong AWS bao gồm một tên và thông tin xác thực.

- Security group: Nhóm bảo mật hoạt động như một tường lửa ảo cho phiên bản của bạn để kiểm soát lưu lượng truy cập vào và ra.

- Policy: Một đối tượng trong AWS mà khi liên kết với một danh tính hoặc tài nguyên, xác định quyền của nó. AWS đánh giá các chính sách này khi một thực thể chính (người dùng hoặc vai trò) thực hiện yêu cầu.

- Amazon Inspector: Giúp khách hàng xác định các lỗ hổng bảo mật và sự sai lệch khỏi các thực tiễn bảo mật tốt nhất trong ứng dụng, trước khi triển khai và trong khi chúng đang chạy trong môi trường sản xuất.

- Group: Một nhóm IAM là một tập hợp các người dùng IAM. Nhóm cho phép bạn xác định quyền cho nhiều người dùng, giúp quản lý quyền cho những người dùng đó dễ dàng hơn.

- Root user: Khi bạn lần đầu tạo tài khoản AWS, bạn bắt đầu với một danh tính đăng nhập duy nhất có quyền truy cập hoàn toàn vào tất cả các dịch vụ và tài nguyên AWS trong tài khoản.

- Credential: Thông tin xác thực bảo mật AWS xác minh bạn là ai và liệu bạn có quyền truy cập vào các tài nguyên mà bạn đang yêu cầu hay không.

- Enable multi-factor authentication (MFA): Cách tiếp cận xác thực này yêu cầu hai hoặc nhiều thông tin độc lập để được xác thực.

- JavaScript Object Notation (JSON): Một cú pháp để lưu trữ và trao đổi dữ liệu.

- Multi-factor authentication (MFA): Một hệ thống bảo mật yêu cầu hơn một phương pháp xác thực từ các loại thông tin xác thực độc lập để xác minh danh tính người dùng cho một lần đăng nhập hoặc giao dịch khác.

Phần nội dung:

- Bảo mật là điều thiết yếu khi sử dụng tài nguyên đám mây để xử lý và lưu trữ dữ liệu. Do cơ sở dữ liệu, trang web và ứng dụng trên đám mây có thể xử lý thông tin nhạy cảm như hồ sơ ngân hàng và y tế, các tài nguyên đám mây này cần phải có kiểm soát chặt chẽ về việc ai có thể truy cập và quyền lợi của họ trong quá trình truy cập.

- IAM liên quan đến việc áp dụng các kiểm soát cho người dùng cần truy cập vào tài nguyên tính toán. Để duy trì một môi trường đám mây an toàn, việc duy trì các thực tiễn tốt nhất cho IAM là rất quan trọng.

- Khi nghĩ về IAM trong AWS, có các vai trò, danh tính và nhóm, tất cả đều được quản lý bởi các chính sách.

- Ở cấp cao nhất là người dùng root. Đây là danh tính đã tạo tài khoản AWS. Người dùng root có quyền truy cập vào mọi khía cạnh của AWS và đóng vai trò như một quản trị viên toàn cầu. Thông tin xác thực của người dùng root không bao giờ nên được chia sẻ, và thậm chí không khuyến nghị cho người tạo tài khoản thực hiện các tác vụ hàng ngày dưới dạng người dùng root. Thay vào đó, tài khoản người dùng root nên được sử dụng để tạo một tài khoản quản trị viên. Chỉ một vài nhiệm vụ cần được thực hiện dưới dạng người dùng root, chẳng hạn như thay đổi kế hoạch hỗ trợ AWS hoặc đóng tài khoản.

- Một người dùng IAM là một thực thể được tạo trong AWS. Nó đại diện cho người sử dụng dịch vụ AWS và cho phép người đó đăng nhập vào AWS. Một người dùng sẽ được chỉ định một tên và mật khẩu để truy cập vào bảng điều khiển AWS. Khi tạo một người dùng, việc chỉ định họ vào một nhóm có chính sách quyền phù hợp được coi là thực tiễn tốt nhất.

- Một nhóm là một tập hợp các người dùng IAM. Bạn có thể sử dụng nhóm để chỉ định quyền cho một tập hợp người dùng, điều này có thể giúp quản lý các quyền đó dễ dàng hơn.

- Các vai trò IAM tương tự như người dùng ở chỗ chúng là danh tính với các chính sách quyền xác định những gì danh tính đó có thể và không thể làm trong AWS. Tuy nhiên, một vai trò không có thông tin xác thực (mật khẩu hoặc khóa truy cập) liên quan đến nó. Thay vì được liên kết độc quyền với một người, một vai trò được thiết kế để có thể được giả định bởi bất kỳ ai cần nó. Một người dùng IAM có thể giả định một vai trò để tạm thời nhận các quyền khác cho một nhiệm vụ cụ thể. Các vai trò rất hữu ích trong các trường hợp mà một ứng dụng di động đang truy cập dữ liệu AWS.

- Trước đó, một chính sách đã được đề cập liên quan đến các quyền mà một nhóm có thể được gán. Một chính sách, khi được đính kèm với một người dùng, vai trò hoặc nhóm, xác định quyền của họ. Các chính sách được lưu trữ trong AWS dưới dạng tài liệu JSON. Thực tiễn tốt nhất là gán chính sách cho các nhóm và sau đó gán mỗi người dùng và vai trò vào một nhóm khi được tạo.

Phần câu hỏi:

1. What three things do you own that are most valuable to you? How do you secure each one? How can you secure something in multiple ways? How do you determine how secure something needs to be?

Ba thứ quý giá nhất đối với em là máy tính cá nhân, điện thoại và tài khoản ngân hàng. Em bảo vệ máy tính và điện thoại bằng cách sử dụng mật khẩu mạnh và xác thực hai yếu tố. Đối với tài khoản ngân hàng, em thường xuyên kiểm tra các giao dịch và sử dụng các biện pháp bảo mật mà ngân hàng cung cấp. Để bảo vệ một thứ bằng nhiều cách, có thể sử dụng kết hợp mật khẩu, xác thực hai yếu tố và giám sát liên tục. Mức độ bảo mật cần thiết phụ thuộc vào giá trị và tính nhạy cảm của thông tin hoặc tài sản đó.

2. What are some examples of places that have different levels of access based on who you are? What are some things that people can use to prove that they have access to places? Why are certain places restricted based on a person's access level?

Một số địa điểm như ngân hàng, văn phòng chính phủ hay khu vực an ninh có mức độ truy cập khác nhau. Mọi người có thể sử dụng thẻ ID, mã PIN hoặc thông tin xác thực sinh trắc học như vân tay để chứng minh quyền truy cập. Một số địa điểm bị hạn chế để bảo vệ thông tin nhạy cảm và đảm bảo an ninh cho mọi người, vì những người không có quyền truy cập có thể gây ra rủi ro.

3. Have you or someone you know ever had something stolen or broken into? How did it feel? Did it change how safe you felt you or your things were? How so? Did it change how you managed your security? How so?

Em có một người anh từng bị mất chiếc xe máy. Cảm giác của anh ấy rất tệ và hoang mang, khiến anh ấy cảm thấy không còn an toàn khi để xe ngoài đường. Sau đó, anh ấy đã sử dụng các biện pháp bảo mật như khóa chống trộm và luôn tìm nơi gửi xe an toàn hơn. Điều này không chỉ thay đổi cảm giác an toàn của anh ấy mà còn khiến em và những người xung quanh cũng chú ý hơn đến việc bảo mật tài sản của mình, từ việc sử dụng các thiết bị an ninh đến việc lựa chọn nơi để xe cẩn thận hơn.

Module 8: Security II

Các Thuật ngữ:

- AWS Shield: Một dịch vụ bảo vệ khỏi tấn công từ chối dịch vụ phân tán (DDoS) được quản lý, bảo vệ các ứng dụng chạy trên Amazon Web Services (AWS).

- AWS WAF: Dịch vụ cho phép bạn kiểm soát lưu lượng truy cập vào hoặc chặn đến ứng dụng web của bạn bằng cách xác định các quy tắc bảo mật web có thể tùy chỉnh.

- Distributed denial of service (DDoS): Một nỗ lực tấn công xấu để làm cho hệ thống mục tiêu, chẳng hạn như trang web hoặc ứng dụng, không thể truy cập được đối với người dùng hợp pháp. Để đạt được điều này, kẻ tấn công sử dụng nhiều kỹ thuật tiêu thụ tài nguyên mạng hoặc các tài nguyên khác, làm gián đoạn quyền truy cập của người dùng hợp pháp.

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

- AWS Artifact: Nguồn tài nguyên tập trung cho thông tin liên quan đến tuân thủ. Nó cung cấp quyền truy cập theo yêu cầu vào các báo cáo bảo mật và tuân thủ của AWS cũng như các thỏa thuận trực tuyến được chọn.

Phần nội dung:

- Bốn lĩnh vực bảo mật cần được quan tâm trong điện toán đám mây:

+ Dữ liệu: Bảo vệ thông tin được lưu trữ và xử lý trong đám mây.

+ Quyền truy cập: Kiểm soát ai có quyền truy cập vào các tài nguyên và dữ liệu trong đám mây.

+ Cơ sở hạ tầng: Bảo vệ các máy móc và phần cứng chạy, lưu trữ và xử lý dữ liệu trong đám mây.

+ Đánh giá bảo mật: Kiểm tra cơ sở hạ tầng, quyền truy cập và dữ liệu để đảm bảo chúng an toàn.

- AWS Shield và AWS WAF là các dịch vụ nhằm ngăn chặn các cuộc tấn công vào cơ sở hạ tầng, chủ yếu là mạng lưới được sử dụng để truy cập các tài nguyên đám mây.

- Amazon Inspector hỗ trợ đánh giá bảo mật bằng cách kiểm tra mức độ bảo vệ của các tài nguyên đám mây như các instance EC2. Nó cũng kiểm tra xem các tài nguyên này có tuân thủ theo các nguyên tắc bảo mật tốt nhất hay không.

- Một loại tấn công mạng phổ biến là DDoS (tấn công từ chối dịch vụ phân tán). Cuộc tấn công DDoS xảy ra khi kẻ tấn công sử dụng các chương trình để gửi hàng ngàn hoặc hàng triệu yêu cầu đến một ứng dụng, trang web hoặc dịch vụ cùng lúc. Lưu lượng tăng đột biến này có thể làm cạn kiệt tài nguyên, khiến trang web hoặc ứng dụng không thể truy cập được với người dùng hợp pháp.

- AWS Shield hoạt động cùng với Elastic Load Balancing (ELB), Amazon CloudFront, và Amazon Route 53 để bảo vệ trước các cuộc tấn công DDoS. Có hai cấp độ dịch vụ:

+ AWS Shield Standard: Có sẵn cho tất cả người dùng AWS mà không tốn thêm chi phí. Nó bảo vệ người dùng khỏi các cuộc tấn công DDoS phổ biến nhất. Lớp bảo

vệ này tự động được áp dụng cho các tài nguyên ELB, phân phối CloudFront và tài nguyên Route 53.

+ AWS Shield Advanced: Cung cấp thêm khả năng giảm thiểu các cuộc tấn công DDoS có quy mô lớn, khả năng phát hiện thông minh và giảm thiểu các cuộc tấn công ở cấp độ ứng dụng và mạng. Người dùng có quyền truy cập 24/7 vào DDoS Response Team (DRT) để giảm thiểu tùy chỉnh trong quá trình bị tấn công.

- AWS WAF là một công cụ phòng thủ khác được cung cấp bởi AWS. Nó giúp bảo vệ ứng dụng web khỏi các lỗ hổng có thể ảnh hưởng đến tính khả dụng hoặc bảo mật, hoặc tiêu tốn tài nguyên. AWS WAF có thể theo dõi lưu lượng web đến ứng dụng và quyết định nên cho phép lưu lượng nào dựa trên yêu cầu cụ thể.

- Amazon Inspector không trực tiếp bảo vệ các dịch vụ AWS. Thay vào đó, nó giám sát các dịch vụ và cung cấp các cập nhật về lỗ hổng bảo mật hoặc những nơi mà chưa tuân thủ các thực hành tốt nhất.

- Amazon Inspector hoạt động bằng cách chạy các đánh giá trên các instance EC2. Các đánh giá này kiểm tra một loạt các thực hành tốt nhất được xác định trước. Sau khi thực hiện đánh giá, Amazon Inspector tạo ra một danh sách chi tiết về các phát hiện bảo mật, được sắp xếp theo mức độ nghiêm trọng. Những phát hiện này có thể được xem trực tiếp hoặc thông qua các báo cáo đánh giá chi tiết có sẵn trên Amazon Inspector Console hoặc API.

Đánh giá bảo mật của Amazon Inspector giúp kiểm tra khả năng truy cập ngoài ý muốn vào các instance EC2 của bạn và kiểm tra các lỗ hổng trên các instance đó. Đánh giá này được cung cấp dưới dạng các gói quy tắc được định sẵn, liên kết với các thực hành bảo mật tốt nhất và định nghĩa lỗ hổng phổ biến. Ví dụ về các quy tắc được tích hợp bao gồm:

+ Kiểm tra quyền truy cập vào các instance EC2 từ internet.

+ Kích hoạt đăng nhập root từ xa hoặc phiên bản phần mềm dễ bị tổn thương được cài đặt.

AWS Artifact là một nguồn tài nguyên tập trung cho thông tin liên quan đến tuân thủ bảo mật. Các tổ chức khác nhau yêu cầu các nhà cung cấp dịch vụ đám mây (CSPs) phải đáp ứng nhiều chứng nhận và quy tắc để lưu trữ dữ liệu hoặc xử lý các yêu cầu. AWS Artifact liệt kê và cung cấp chi tiết về các tiêu chuẩn tuân thủ mà AWS đáp ứng.

Phần câu hỏi:

1. What might motivate someone to initiate a cyberattack against a company? What might attackers have to gain? Include an example of a company or a type of business and a kind of cyberattack it might be a victim of.

Điều có thể thúc đẩy một cuộc tấn công mạng thường xuất phát từ các động cơ như tài chính, cạnh tranh, chính trị, hoặc thậm chí là mục đích phá hoại. Ví dụ, một

công ty công nghệ lớn như Amazon có thể là mục tiêu của một cuộc tấn công DDoS nhằm làm gián đoạn dịch vụ, khiến trang web hoặc ứng dụng của họ không thể truy cập được, làm tổn hại đến uy tín và doanh thu. Các kẻ tấn công có thể nhằm mục đích gây thiệt hại tài chính, giành lợi thế cạnh tranh, hoặc buộc công ty phải chi tiền để giảm thiểu các cuộc tấn công.

2. Do you think there should be different security standards for the cloud based on the type of data that is being stored or processed? Why do you think that? Give an example. How do you think security differs between data stored in the cloud and data stored on premises?

Có, các tiêu chuẩn bảo mật nên thay đổi tùy thuộc vào loại dữ liệu. Dữ liệu nhạy cảm như hồ sơ y tế hoặc thông tin ngân hàng yêu cầu các tiêu chuẩn bảo mật nghiêm ngặt hơn so với dữ liệu thông thường. Ví dụ, một tổ chức chăm sóc sức khỏe có thể cần tuân thủ các quy định như HIPAA để bảo vệ thông tin bệnh nhân.

Bảo mật dữ liệu trên đám mây có thể phức tạp hơn dữ liệu tại chỗ vì đám mây được quản lý bởi các bên thứ ba và yêu cầu các biện pháp kiểm soát truy cập mạnh mẽ. Trong khi đó, dữ liệu tại chỗ thường có các biện pháp bảo mật vật lý bổ sung và quyền kiểm soát trực tiếp hơn đối với cơ sở hạ tầng.

3. What character traits do you think a successful cloud security administrator would need? Why? Would this be a role that you would be interested in?

Một quản trị viên bảo mật cloud thành công có lẽ cần sự tỉ mỉ, cẩn trọng, và khả năng làm việc dưới áp lực. Họ cũng cần luôn cập nhật kiến thức vì các mối đe dọa bảo mật không ngừng thay đổi.

Module 9: Monitoring the Cloud

Các Thuật ngữ:

- Amazon CloudWatch: Dịch vụ giám sát cho phép theo dõi các tài nguyên AWS và ứng dụng mà bạn chạy trên AWS.

- AWS CloudTrail: Dịch vụ giúp theo dõi và ghi lại mọi hành động thực hiện trên tài khoản AWS của bạn nhằm mục đích bảo mật.

- AWS Config: Dịch vụ cho phép bạn đánh giá, kiểm tra và đánh giá các cấu hình của tài nguyên AWS.

- Amazon Simple Notification Service (Amazon SNS): Công cụ của AWS cho phép gửi tin nhắn văn bản, email và thông điệp đến các dịch vụ đám mây khác, đồng thời gửi thông báo từ đám mây đến khách hàng dưới nhiều hình thức.

Phần nội dung:

- AWS cung cấp các công cụ mạnh mẽ để giám sát tất cả các dịch vụ đám mây. Những công cụ này làm việc cùng nhau để cung cấp một bộ dịch vụ giúp người dùng đám mây nắm bắt được thông tin cần thiết.

- CloudWatch là một dịch vụ giám sát các tài nguyên AWS và các ứng dụng mà bạn chạy trên AWS.

- CloudTrail và CloudWatch đều là các dịch vụ giám sát đám mây, nhưng chúng thực hiện các chức năng khác nhau:

+ CloudTrail theo dõi và ghi lại mọi hành động mà người dùng thực hiện trong tài khoản AWS. Điều này có nghĩa là CloudTrail sẽ ghi lại mỗi khi có người tải dữ liệu lên, chạy mã, tạo một phiên bản Amazon EC2, hoặc thực hiện bất kỳ hành động nào khác.

+ CloudWatch theo dõi những gì các dịch vụ khác nhau đang làm và các tài nguyên chúng đang sử dụng. CloudTrail ghi lại các hoạt động, trong khi CloudWatch giám sát các hoạt động đó. CloudWatch giúp bạn đảm bảo rằng các dịch vụ đám mây của bạn hoạt động trơn tru. Công cụ này cũng giúp bạn sử dụng tài nguyên một cách hợp lý, tránh việc sử dụng quá nhiều hoặc quá ít, điều này rất quan trọng để kiểm soát ngân sách.

- AWS Config là một dịch vụ cho phép bạn đánh giá, kiểm tra và đánh giá cấu hình của các tài nguyên AWS của mình. AWS Config liên tục theo dõi và ghi lại cấu hình của các tài nguyên AWS và cho phép bạn tự động đánh giá những cấu hình này so với cấu hình mong muốn.

- Về khả năng truy cập: Khi có sự thay đổi cấu hình trong tài nguyên AWS của bạn.

+ AWS Config ghi lại và chuẩn hóa các thay đổi thành định dạng nhất quán. AWS Config tự động đánh giá các cấu hình đã ghi lại so với các cấu hình mà bạn chỉ định.

+ Bạn có thể truy cập lịch sử thay đổi và kết quả tuân thủ bằng cách sử dụng giao diện điều khiển hoặc API. CloudWatch Events hoặc SNS sẽ cảnh báo bạn khi có sự thay đổi xảy ra. Lịch sử thay đổi và tệp snapshot có thể được lưu vào S3 bucket để phân tích.

- Amazon SNS là cách mà AWS giao tiếp trong nội bộ đám mây và với thế giới bên ngoài. Khi một sự kiện được kích hoạt hoặc một chương trình cảnh báo AWS gửi thông báo, Amazon SNS sẽ gửi tin nhắn đến người dùng hoặc các dịch vụ khác của AWS.

Phần câu hỏi:

1. What tools do you use to stay organized and keep track of your life, work, and schedule? Why are these tools important? What kinds of tools would be helpful to monitor or keep track of your resources in the cloud?

Em thường dùng các ứng dụng như Google Calendar để sắp xếp công việc và theo dõi lịch trình. Những công cụ này giúp em không quên các sự kiện quan trọng và duy trì sự tự giác trong cuộc sống hàng ngày. Tương tự trong cloud, các công cụ như Amazon CloudWatch và AWS Config rất quan trọng để giám sát và kiểm tra tình trạng của các tài nguyên. Chúng giúp kiểm soát việc sử dụng tài nguyên, theo dõi các thay đổi và ngăn chặn các sự cố.

2. Have you ever missed or been late to an event you had scheduled, or forgotten an assignment? What happened? How might you have prevented the error? Do you think a similar error might happen when using cloud services with AWS? How might this be prevented?

Đã có lần em quên mất nộp một bài tập quan trọng vì không ghi chú lại. Điều này khiến em gặp rắc rối và phải nộp bài trễ. Nếu em theo dõi lịch tốt hơn, chắc chắn đã có thể tránh được sai lầm này. Trong cloud, việc quên cấu hình hoặc không kiểm soát tài nguyên cũng có thể gây ra những sự cố tương tự. Để tránh điều này, AWS cung cấp công cụ như CloudWatch và SNS để tự động gửi thông báo và cảnh báo khi có sự cố hoặc thay đổi bất thường.

3. A cell phone company uses AWS to let users download mobile apps that let them print remotely from their devices. What data points do you think this company needs to keep track of in their cloud services? Why?

Công ty này cần theo dõi các thông tin như số lượng yêu cầu in ấn, trạng thái của các máy in, và lượng dữ liệu được truyền tải qua cloud. Việc này rất quan trọng để đảm bảo rằng dịch vụ hoạt động ổn định và không bị gián đoạn. Họ cũng cần theo dõi tài nguyên hệ thống như CPU, bộ nhớ và băng thông thông qua CloudWatch để đảm bảo rằng không xảy ra quá tải, đồng thời duy trì hiệu suất dịch vụ tốt nhất cho người dùng.