# **Trần Thị Ngọc Trang - 21133109**

# **Module 1: Global Infrastructure**

## **Module purpose**

Mục đích của module này là để đánh giá lại các khái niệm cơ bản về điện toán đám mây. Nó sẽ bao gồm các lợi ích của việc tính toán trong đám mây và những lý do tại sao các công ty đã bắt đầu chuyển từ việc tính toán trên nền tảng cơ sở đến điện toán đám mây. Nó cũng sẽ đề cập đến các dịch vụ chính được cung cấp bởi các nhà cung cấp điện toán đám mây.

## **Module description**

Trong module này, bạn sẽ ghi chú về các lợi ích của điện toán đám mây và các dịch vụ được cung cấp bởi các nhà cung cấp điện toán đám mây. Chúng tôi sẽ thảo luận về một số tác động của điện toán đám mây.

## **I.** **Technology terminology**

**1.** **Cloud computing**

Cloud computing là việc cung cấp các nguồn lực tính toán, cơ sở dữ liệu, lưu trữ, ứng dụng và các tài nguyên CNTT khác theo yêu cầu sử dụng internet với cơ chế thanh toán theo từng lần sử dụng.

**2.** **Amazon Web Services (AWS)**

Amazon Web Services (AWS) là một nền tảng cung cấp một loạt các dịch vụ đám mây.

**3.** **Cloud storage**

Cloud storage là việc lưu trữ dữ liệu bằng cách sử dụng một nhà cung cấp dịch vụ đám mây (CSP) thay vì sử dụng máy chủ vật lý.

**4. Server**

Một máy tính được thiết kế để xử lý các yêu cầu và cung cấp dữ liệu cho một máy tính khác qua Internet hoặc mạng nội bộ. Trong môi trường đám mây, máy chủ được lưu trữ bởi một nhà cung cấp bên ngoài, có thể truy cập qua internet.

## **II.** **Background and misconceptions**

**1.** **What is cloud computing?**

Bất kỳ khi nào bạn đang làm việc hoặc lưu trữ thông tin trực tuyến (ví dụ: gửi email hoặc xem video trực tuyến)—khác với việc trên máy tính cục bộ của bạn hoặc trên một máy chủ trên mạng nội bộ của bạn—bạn đang sử dụng điện toán đám mây.

2. **Why do businesses use cloud computing?**

Các lợi ích kinh doanh của điện toán đám mây bao gồm:

· Thanh toán ít hơn để bắt đầu kinh doanh của bạn.

· Thanh toán nhiều hơn khi doanh nghiệp của bạn phát triển.

· Dịch vụ rẻ hơn vì chi phí được phân tán qua nhiều người dùng.

· Năng lực tính toán và lưu trữ của bạn mở rộng để phù hợp với những gì bạn cần, vì vậy bạn chỉ trả tiền cho những gì bạn sử dụng.

· Nhanh chóng và dễ dàng để thêm tài nguyên mới khi bạn cần chúng.

· Các nhà cung cấp đám mây duy trì, bảo mật và vận hành máy tính và cơ sở cho các dịch vụ đám mây.

· Dễ dàng để phát hành ứng dụng của bạn hoặc quảng cáo bất cứ nơi nào trên thế giới vì mọi thứ đều trực tuyến.

3. **What types of cloud services are there?** Loại Dịch vụ Đám mây Có gì

| **Loại Dịch Vụ**  **Đám Mây** | **Chức Năng** | **Ví dụ** |
| --- | --- | --- |
| Infrastructure as a Service (IaaS) | Cung cấp sức mạnh tính toán, mạng lưới, và lưu trữ qua internet | Amazon Elastic Compute Cloud (Amazon EC2), Rackspace, Google Compute Engine |
| Platform as a Service (PaaS) | Cung cấp các công cụ qua internet để tạo ra các chương trình và ứng dụng | AWS Elastic Beanstalk, Microsoft Azure, Google App Engine |
| Software as a Service (SaaS) | Cung cấp các ứng dụng và chương trình được truy cập và cung cấp qua internet | Dropbox, Slack, Spotify, YouTube, Microsoft Office 365, Gmail |

4. **How did AWS get started?**

· Xuất phát từ năm 2002 khi Amazon bắt đầu dịch vụ web Amazon.com.

· Cung cấp các công cụ cho nhà phát triển làm việc trên danh mục sản phẩm của Amazon.

· Vào năm 2003, Amazon nhận ra rằng các dịch vụ cơ sở hạ tầng của mình có thể mang lại lợi thế so với các đối thủ.

· Cung cấp sức mạnh phần cứng, lưu trữ và cơ sở dữ liệu cùng với các công cụ phần mềm để kiểm soát chúng.

· Vào năm 2004, Amazon công bố công khai rằng họ đang làm việc trên một dịch vụ đám mây.

· Vào năm 2006, Amazon ra mắt AWS với chỉ một số dịch vụ hiện vẫn còn tồn tại ngày nay.

· Bởi năm 2009, AWS đã thêm vào nhiều dịch vụ khác.

· AWS đã phát triển các đối tác với một số công ty lớn. AWS đã phát triển và thêm vào các dịch vụ và công cụ mới từ đó

## **III. Questions**

**1. Imagine if one of your social media accounts was hacked and all your data was made public or held for ransom. How would this make you feel? Do you think the trade-off is worth the risk to have all the cloud services at your fingertips?**

Nếu tài khoản mạng xã hội của tôi bị hack và dữ liệu của tôi bị tiết lộ hoặc bị giữ làm con tin, tôi sẽ cảm thấy rất bị xâm phạm và lo lắng. Việc này có thể gây ra hậu quả lớn, bao gồm mạo danh, mất danh tiếng và tổn thương tinh thần. Dù dịch vụ đám mây mang lại sự thuận tiện và tiện lợi, việc đánh đổi về mặt bảo mật và riêng tư có thể khiến cho người dùng phải đối mặt với những rủi ro đáng kể.

**2. What kind of information do you have stored online? What are the risks of that information being compromised or shared without your consent? What kinds of laws or regulations do you think are necessary to keep your information safe?**

Thông tin tôi lưu trữ trực tuyến bao gồm tài liệu cá nhân, ảnh và hồ sơ tài chính. Rủi ro liên quan đến việc thông tin này bị tiết lộ bao gồm mạo danh, gian lận tài chính và tổn thương danh tiếng. Các luật và quy định đóng vai trò quan trọng trong việc bảo vệ quyền riêng tư và bảo mật dữ liệu cá nhân của cá nhân.

**3. What are some ways that the internet has made your life easier? What are some ways that the internet has made your life more difficult? What is one thing you wish you could do online, but the technology doesn’t exist yet?**

Internet đã làm cho cuộc sống của tôi dễ dàng hơn bằng cách cung cấp truy cập vào thông tin, công cụ giao tiếp, mua sắm trực tuyến và cơ hội làm việc hoặc học tập từ xa. Tuy nhiên, nó cũng mang lại thách thức như quá tải thông tin, mối đe dọa về an ninh mạng.

Một điều tôi ước mong có thể làm trực tuyến, nhưng công nghệ chưa tồn tại, đó là trải nghiệm thực tế ảo hoặc thực tế tăng cường một cách hoàn toàn sâu sắc và liền mạch cho các hoạt động hàng ngày như giao tiếp xã hội, khám phá những nơi xa xôi hoặc tham gia các sự kiện.

# **Module 6: Virtual Storage**

**Module purpose**

Mục đích của mô-đun này là cung cấp tổng quan về Amazon Elastic Block Store (Amazon EBS), so sánh giữa Amazon EBS và Amazon Simple Storage Service (Amazon S3), và hướng dẫn cách lựa chọn loại lưu trữ phù hợp nhất cho một tình huống cụ thể.

**Module description**

Mô-đun bao gồm việc thảo luận về các lợi ích và tính năng của Amazon EBS, phân tích các trường hợp thực tế liên quan đến Amazon EBS, và hướng dẫn cách tạo và gắn các khối lưu trữ EBS vào máy ảo Amazon Elastic Compute Cloud (Amazon EC2).

1. **Technology terminology**
2. **Amazon Elastic Block Store (Amazon EBS)** là dịch vụ lưu trữ dành riêng cho các máy ảo Amazon Elastic Compute Cloud (Amazon EC2). Nó có thể được xem như ổ lưu trữ cho máy ảo EC2 của bạn.
3. A**mazon Elastic Compute Cloud (Amazon EC2)** là một dịch vụ web cung cấp khả năng tính toán có thể điều chỉnh và bảo mật trong đám mây. Nó có thể được coi như việc thuê một máy tính trong đám mây.
4. **Ổ đĩa cứng (HDD)** là một loại lưu trữ chậm sử dụng đĩa quay để lưu trữ dữ liệu.
5. **Input/Output Operations Per Second (IOPS)** là một đơn vị đo hiệu suất phổ biến được sử dụng để đánh giá các thiết bị lưu trữ máy tính như ổ đĩa cứng (HDD) và ổ đĩa rắn (SSD).
6. **Ổ đĩa rắn (SSD)** là một loại lưu trữ rất nhanh sử dụng bộ nhớ flash thay vì đĩa quay.
7. **Background and misconceptions**

Amazon Elastic Block Store (Amazon EBS) cung cấp lưu trữ cho các phiên bản EC2 với những lợi ích chính:

* Sẵn có dữ liệu
* Dữ liệu liên tục
* Mã hóa dữ liệu
* Bản snapshot

Lưu trữ Amazon EBS được triển khai dưới dạng một loạt các khối có độ dài cố định có thể được đọc và ghi bởi hệ điều hành. Khối rất giống như hệ thống tệp NTFS hoặc FAT chạy trên PC hoặc Mac của bạn, không có gì lưu trữ về những khối này đại diện cho gì hoặc thuộc tính của chúng. Điều này có nghĩa là chúng có thể được truy cập nhanh chóng.

Lưu trữ Amazon S3 được triển khai dưới dạng một đối tượng phải được đọc và ghi bởi ứng dụng sử dụng đối tượng đó. Đối tượng chứa siêu dữ liệu - dữ liệu về các thuộc tính của đối tượng giúp hệ thống đánh giá và xác định đối tượng. Ví dụ về các đối tượng là hình ảnh, video và âm nhạc. Các đối tượng không thể được xử lý theo cách từng phần. Chúng phải được đọc và ghi toàn bộ. Điều này có thể ảnh hưởng đến hiệu suất và tính nhất quán.

Có nhiều sự khác biệt khác giữa lưu trữ Amazon S3 và Amazon EBS, bao gồm sự khác biệt về chi phí, thông lượng và hiệu suất. Những sự khác biệt này được thảo luận trên trang web Lưu trữ Đám mây trên AWS. Người dùng hoặc nhà thiết kế ứng dụng phải quyết định liệu lưu trữ Amazon S3 hoặc Amazon EBS phù hợp hơn cho một ứng dụng cụ thể.

Có hai loại chính của các khối EBS, và mỗi loại chính có hai loại phụ. Mỗi loại có những ưu và nhược điểm riêng, vì vậy quan trọng là chọn loại phù hợp nhất với công việc bạn đang sử dụng nó cho.

Thông tin chi tiết về các loại khối EBS có thể được tìm thấy trên trang web AWS, Loại khối Amazon EBS.

Một số khác biệt chính khác giữa lưu trữ dữ liệu Amazon S3 và Amazon EBS:

1. Amazon EBS chỉ có thể sử dụng khi được gắn vào một phiên bản EC2. Ngược lại, Amazon S3 có thể được truy cập một cách độc lập bằng cách sử dụng giao thức HTTP.
2. Amazon EBS không thể chứa nhiều dữ liệu như Amazon S3.
3. Amazon EBS chỉ có thể được gắn vào một phiên bản EC2, trong khi dữ liệu trong một bucket S3 có thể được truy cập bởi nhiều phiên bản EC2.
4. Amazon S3 trải qua nhiều trễ hơn so với Amazon EBS khi ghi dữ liệu.
5. Các khối EBS được mã hóa toàn bộ, trong khi các đối tượng Amazon S3 được mã hóa một cách riêng lẻ bằng mã hóa phía máy chủ (SSE).
6. Amazon EBS bao gồm ba loại khối, trong khi Amazon S3 bao gồm nhiều loại hơn:

* 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

1. **Focus questions**
2. **In your opinion, how has cloud computing impacted the way that society interacts with technology? Is it a positive or negative impact overall? Why?Theo bạn, điện toán đám mây đã tác động như thế nào đến cách xã hội tương tác với công nghệ? Đó là một tác động tích cực hay tiêu cực tổng thể? Tại sao?**  
   - Điện toán đám mây (cloud computing) đã có một tác động rất lớn đối với cách xã hội tương tác với công nghệ, và tác động này có thể được coi là tích cực trong nhiều khía cạnh, nhưng cũng có một số thách thức tiêu cực.

- Giải thích:

• Tác động tích cực:

* Tiện lợi và linh hoạt
* Tiết kiệm chi phí
* Tích hợp dễ dàng
* Khả năng mở rộng

• Tác động tiêu cực:

* Bảo mật và quyền riêng tư
* Phụ thuộc vào nhà cung cấp
* Quản lý dữ và kiểm soát dữ liệu phức tạp hơn

1. **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?**

- Việc sử dụng dịch vụ đám mây để bảo vệ và kiểm phiếu có thể là một ý tưởng tiềm năng, nhưng nó cũng đi kèm với một số thách thức và cần phải được xem xét cẩn thận. Dưới đây là một số điểm để xem xét:

- Ưu điểm:

• Tăng tính minh bạch

• Tiện lợi và tốc độ

• Khả năng kiểm tra và xác thực hiệu quả

- Nhược điểm và thách thức:

• Rủi ro bảo mật và xâm nhập

• Tính riêng tư của cử tri không được đảm bảo

1. **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. Là một sinh viên, bạn nghĩ dịch vụ điện toán đám mây có thể cải thiện trường học của bạn như thế nào? Hãy suy nghĩ về cách bạn làm việc, tham gia các kỳ thi, tham dự các lớp học và sự kiện hoặc bất kỳ yếu tố nào khác liên quan đến trường học của bạn.**

-Dịch vụ điện toán đám mây giúp cải thiện trường học qua các hoạt động:

* Học trực tuyến
* Việc lưu trữ và chia sẻ tài liệu giữa sinh viên và giảng viên
* Hợp tác trực tuyến thông qua các công cụ như Google docs, Microsoft Teams
* Hệ thống quản lý học tập (LMS)

# **Module 7: Security I**

**Module purpose**

Trong mô-đun này, bạn sẽ được tổng quan về bảo mật đám mây liên quan đến Quản lý danh tính và Truy cập của AWS (IAM). Điều này bao gồm thông tin về các thực hành tốt nhất, vai trò, người dùng, chính sách và nhóm bảo mật.

**Module description**

Các hoạt động trong mô-đun này sẽ yêu cầu bạn ghi chú về thông tin được trình bày và thu thập. Bạn cũng sẽ tham gia vào một cuộc thảo luận hoặc diễn tả vai trong các tác động xã hội của bảo mật đám mây. Bạn sẽ xác định quy trình để giải quyết lỗ hổng trong một máy chủ web."

1. **Technology terminology**
2. **AWS Identity and Access Management (IAM):**Quản lý danh tính và Truy cập của AWS (IAM) là quá trình áp dụng các điều khiển đối với người dùng cần truy cập vào các tài nguyên máy tính.
3. **Role**:Vai trò là một danh tính IAM bạn có thể tạo trong tài khoản của mình có các quyền cụ thể.
4. **User**:Người dùng là một thực thể mà bạn tạo ra trong Amazon Web Services (AWS) để đại diện cho người hoặc ứng dụng sử dụng nó để tương tác với AWS.
5. **Security group**:Một nhóm bảo mật hoạt động như một tường lửa ảo cho máy chủ của bạn để kiểm soát lưu lượng vào và ra.
6. **Policy:C**hính sách là một đối tượng trong AWS, khi được liên kết với một danh tính hoặc tài nguyên, xác định các quyền của nó.
7. **Amazon Inspecto**r:Amazon Inspector giúp khách hàng xác định các lỗ hổng bảo mật và sai lệch từ các thực tiễn tốt nhất về bảo mật trong các ứng dụng, trước khi chúng được triển khai và trong khi chúng đang chạy trong một môi trường sản xuất.
8. **Grou**p:Nhóm IAM là một tập hợp các người dùng IAM.
9. **Root user:**Người dùng gốc là khi bạn tạo một tài khoản AWS, bạn bắt đầu với một định danh đăng nhập duy nhất có quyền truy cập đầy đủ vào tất cả các dịch vụ và tài nguyên AWS trong tài khoản.
10. **Credential:**Chứng chỉ bảo mật AWS xác minh bạn là ai và liệu bạn có quyền truy cập vào các tài nguyên bạn đang yêu cầu hay không.
11. **Enable multi-factor authentication (MFA**):Bật xác thực đa yếu tố (MFA) yêu cầu hai hoặc nhiều thông tin độc lập để xác minh.
12. **JavaScript Object Notation (JSON)**:JSON là cú pháp để lưu trữ và trao đổi dữ liệu.
13. **Multi-factor authentication (MFA):**MFA là hệ thống bảo mật yêu cầu nhiều hơn một phương pháp xác minh từ các loại thông tin độc lập nhau để xác minh danh tính người dùng cho một đăng nhập hoặc giao dịch khác.

**II. Background and misconceptions**

Bảo mật là yếu tố quan trọng khi sử dụng tài nguyên đám mây để xử lý và lưu trữ dữ liệu nhạy cảm như hồ sơ ngân hàng và y tế. Quản lý quyền truy cập thông qua IAM là cần thiết khi một tài khoản AWS của một công ty có thể được quản lý bởi nhiều người từ các bộ phận khác nhau, có trách nhiệm và vị trí khác nhau. Để duy trì một môi trường đám mây an toàn, việc tuân thủ các thực tiễn tốt nhất trong IAM là không thể thiếu. Để biết thêm chi tiết, xem Hướng dẫn người dùng Quản lý Danh tính và Truy cập của AWS.

**AWS identities**

IAM trong AWS bao gồm vai trò, danh tính và nhóm, đều được quản lý bằng chính sách. Người dùng gốc là người tạo tài khoản AWS, có quyền truy cập toàn bộ và hoạt động như quản trị viên toàn cầu. Thông tin đăng nhập của người dùng gốc không nên được tiết lộ và không nên sử dụng hàng ngày, thay vào đó, nên tạo một tài khoản quản trị viên. Chỉ một số nhiệm vụ nhất định cần thực hiện dưới dạng người dùng gốc, như thay đổi kế hoạch hỗ trợ AWS hoặc đóng tài khoản.

**Người dùng IAM** là thực thể trong AWS, đại diện cho người dùng và cho phép họ đăng nhập vào AWS. Khi tạo người dùng, cần gán họ vào nhóm với chính sách quyền phù hợp.

**Nhóm l**à một tập hợp các người dùng IAM được sử dụng để chỉ định quyền cho một nhóm người dùng cụ thể. Ví dụ, bạn có thể tạo một nhóm quản trị viên và gán quyền quản trị viên cho nhóm đó. Bất kỳ người dùng nào trong nhóm sẽ tự động có các quyền tương ứng. Khi có người dùng mới hoặc người dùng thay đổi công việc, bạn có thể dễ dàng quản lý quyền bằng cách thêm hoặc xóa họ khỏi các nhóm thích hợp.

**Vai trò IAM** giống như người dùng vì cả hai đều có chính sách quyền xác định hoạt động trong AWS. Tuy nhiên, vai trò không có thông tin đăng nhập và được thiết kế để có thể được sử dụng bởi bất kỳ ai cần nó. Người dùng IAM có thể giả định một vai trò để nhận quyền tạm thời cho một nhiệm vụ cụ thể, phù hợp trong các ứng dụng di động truy cập dữ liệu AWS mà không cần thông tin đăng nhập vĩnh viễn.

**III. Focus questions**

**1. Ba thứ bạn sở hữu có giá trị nhất đối với bạn là gì? Làm thế nào để bạn bảo mật từng cái? Làm thế nào bạn có thể bảo mật một cái gì đó bằng nhiều cách? Làm thế nào để bạn xác định mức độ an toàn của một cái gì đó?**

- Ba thứ sở hữu có giá trị nhất của tôi có thể bao gồm:

* Sức khỏe
* Thông tin cá nhân
* Thời gian

- Cách bảo mật từng cái của tôi:

* Sức khỏe: ăn uống điều độ, ngủ sớm, tập thể dục nếu có thể.
* Thông tin cá nhân: Sử dụng mật khẩu mạnh, nhiều phương thức xác thực đăng nhập, không chia sẻ quá nhiều thông tin cá nhân lên mạng xã hội.
* Thời gian: dành thời gian cho những việc quan trọng và có ý nghĩa trong cuộc sống.

- Để xác định mức độ an toàn của một cái gì đó, tôi có thể thực hiện các biện pháp như kiểm tra các hệ thống bảo mật (ví dụ: kiểm tra mã nguồn phần mềm), đánh giá rủi ro, thực hiện kiểm tra bảo mật định kỳ, và tuân thủ các quy tắc và tiêu chuẩn bảo mật quy định. Cần hiểu rằng mức độ an toàn có thể thay đổi theo thời gian và yêu cầu sự liên tục để duy trì.

**2. Một số ví dụ về những địa điểm có cấp độ truy cập khác nhau tùy theo bạn là ai? Một số thứ mà mọi người có thể sử dụng để chứng minh rằng họ có quyền tiếp cận các địa điểm là gì? Tại sao một số địa điểm nhất định bị hạn chế dựa trên cấp độ truy cập của một người?**

- Ví dụ về những địa điểm có cấp độ truy cập khác nhau tùy theo bạn là ai:

* Email và Hộp Thư Điện Tử: Email cá nhân yêu cầu mật khẩu để truy cập, và chỉ người dùng có mật khẩu mới có quyền đọc và gửi email từ tài khoản đó.
* Trang web doanh nghiệp: Các trang web của các doanh nghiệp thường có các khu vực có giới hạn truy cập dành riêng cho nhân viên, khách hàng, hoặc đối tác. Điều này đảm bảo rằng chỉ những người có quyền được truy cập thông tin nhạy cảm hoặc tài liệu nội bộ.

- Thứ mà mọi người có thể sử dụng để chứng minh rằng họ có quyền tiếp cận các địa điểm bao gồm:

* ·Tài khoản và mật khẩu
* Token xác minh

- Một số địa điểm bị hạn chế truy cập dựa trên cấp độ truy cập của một người vì các lý do sau đây:

* ·Bảo mật thông tin cá nhân
* · Bảo vệ nội dung bản quyền
* · Bảo mật kinh doanh

3. **Bạn hoặc ai đó bạn biết đã từng bị đánh cắp hoặc đột nhập thứ gì đó chưa? Nó cảm thấy thế nào? Nó có thay đổi mức độ an toàn của bạn hoặc đồ đạc của bạn không? Làm sao vậy? Nó có thay đổi cách bạn quản lý bảo mật của mình không? Làm sao vậy?**

Tôi và những người tôi quen biết chưa từng bị đánh cắp hoặc đột nhập thứ gì đó.

# **Module 8: Security II**

**1. Module purpose**

- Tiếp tục phát triển hiểu biết của bạn về bảo mật đám mây.

**2. Module description**

- Bạn sẽ được đưa ra các tình huống liên quan đến AWS Cloud. Bạn sẽ đánh giá xem các quy tắc bảo mật tốt có được áp dụng không và đề xuất các biện pháp để khắc phục bất kỳ khe hở bảo mật nào.

**I. Technology terminology**

**1. AWS Shield:**

- AWS Shield là một dịch vụ được quản lý giúp bảo vệ chống lại các cuộc tấn công từ chối dịch vụ phân tán (DDoS), giữ an toàn cho các ứng dụng chạy trên AWS.

- AWS Shield cung cấp khả năng phát hiện luôn sẵn sàng và các biện pháp giảm nhẹ tự động để giảm thiểu thời gian ngừng hoạt động và độ trễ của ứng dụng.

- Một ví dụ về AWS Shield là khi bạn sử dụng Amazon CloudFront, Amazon Route 53 hoặc Elastic Load Balancing, bạn sẽ được hưởng lợi từ AWS Shield Standard, một phiên bản miễn phí của AWS Shield.

**2. AWS WAF:**

**-**  AWS WAF là một tường lửa ứng dụng web giúp bảo vệ các ứng dụng và API trước những hình thức khai thác và bot tiêu hao tài nguyên, làm sai lệch chỉ số hoặc gây ra tình trạng ngừng hoạt động.

- AWS WAF cho phép bạn định nghĩa các quy tắc bảo mật tùy chỉnh để cho phép hoặc chặn lưu lượng truy cập web theo các tiêu chí như địa chỉ IP, chuỗi truy vấn, tiêu đề HTTP, kích thước yêu cầu, chuỗi ký tự độc hại, loại nội dung và nhiều hơn nữa.

- Một ví dụ về AWS WAF là khi bạn sử dụng Amazon CloudFront để phân phối nội dung web của mình, bạn có thể sử dụng AWS WAF để kiểm soát lưu lượng truy cập vào các ứng dụng web của mình**.**

**3. Distributed denial of service (DdoS):**

- Tấn công từ chối dịch vụ phân tán (DDoS) là một loại tấn công máy tính nhằm làm cho một hệ thống, như một website hoặc ứng dụng, không khả dụng đối với người dùng cuối. Để làm được điều này, kẻ tấn công sử dụng nhiều kỹ thuật khác nhau để tiêu thụ tài nguyên mạng hoặc tài nguyên khác, ngắt quãng việc truy cập của người dùng hợp pháp.

- Một ví dụ về tấn công DDoS là khi một nhóm hacker sử dụng hàng nghìn máy tính bị lây nhiễm virus để gửi các yêu cầu giả mạo đến một website, khiến cho website không thể xử lý được các yêu cầu hợp lệ từ người dùng thực.

**4. Amazon Inspector:**

**-** Amazon Inspector là một 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 (Amazon EC2) của bạn và trạng thái bảo mật của các ứng dụng chạy trên các phiên bản đó. Amazon Inspector cho phép bạn định cấu hình các máy quét lỗ hổng để xác định và gắn cờ các lỗ hổng trong môi trường máy chủ của bạn dựa trên các bộ nguyên tắc do AWS cung cấp.

- Một ví dụ về Amazon Inspector là khi bạn sử dụng Terraform để triển khai các tài nguyên AWS, bạn có thể sử dụng Amazon Inspector để kiểm tra bảo mật của các phiên bản EC2 của bạn.

**5. AWS Artifact:**

**-**  AWS Artifact là một tài nguyên trung tâm, tổng hợp cho thông tin liên quan đến việc tuân thủ quan trọng đối với bạn. Nó cung cấp quyền truy cập theo nhu cầu vào các báo cáo tuân thủ và bảo mật từ AWS cũng như Nhà cung cấp phần mềm độc lập (ISV) bán sản phẩm trên AWS.

- Bạn có thể tải xuống các tài liệu như các chứng chỉ ISO của AWS, các báo cáo Thẻ thanh toán (PCI), và các báo cáo Kiểm soát tổ chức dịch vụ (SOC).

- Một ví dụ về AWS Artifact là khi bạn muốn xem báo cáo SOC của AWS, bạn có thể đăng nhập vào AWS Artifact và yêu cầu báo cáo đó.

**II. Background and Misconceptions:**

**1. Bốn lĩnh vực bảo mật cần xem xét cho đám mây tích hợp:**

* Dữ liệu: Bảo vệ thông tin được lưu trữ và xử lý trong đám mây.
* Quyền hạn: Quản lý người dùng được phép truy cập tài nguyên và dữ liệu trong đám mây.
* Cơ sở hạ tầng: Bảo vệ máy chủ và phần cứng chạy, lưu trữ và xử lý dữ liệu trong đám mây.
* Đánh giá: Kiểm tra cơ sở hạ tầng, quyền hạn và dữ liệu để đảm bảo tính bảo mật.

**2. Các dịch vụ AWS đáp ứng hai khía cạnh chính:**

* **Bảo vệ cơ sở hạ tầng:**
* AWS Shield: Bảo vệ trước các cuộc tấn công DDoS, hoạt động kết hợp với Elastic Load Balancing, Amazon CloudFront và Amazon Route 53. Có hai cấp độ: AWS Shield Standard (miễn phí) và AWS Shield Advanced (phụ thuộc vào giá).
* AWS WAF: Bảo vệ ứng dụng web khỏi các cuộc tấn công có thể ảnh hưởng đến tính sẵn có hoặc bảo mật và tiêu thụ tài nguyên. AWS WAF có thể kiểm tra lưu lượng web và quyết định lưu lượng nào được phép dựa trên các quy tắc được tạo bởi người dùng.
* **Đánh giá cơ sở hạ tầng:**
* Amazon Inspector: Kiểm tra cách bảo vệ các tài nguyên đám mây được thực hiện, đặc biệt là EC2 instances. Nó cung cấp thông tin về các lỗ hổng và không tuân thủ các hướng dẫn tốt nhất.
* AWS Artifact: Trung tâm thông tin về tuân thủ liên quan đến bảo mật. Liệt kê và cung cấp thông tin về các tiêu chuẩn tuân thủ khác nhau mà AWS đáp ứng để chứa dữ liệu hoặc xử lý yêu cầu từ các tổ chức khác nhau.

**III. Focus questions**

**1. Điều gì có thể thúc đẩy ai đó bắt đầu một cuộc tấn công mạng chống lại một công ty? Những kẻ tấn công có thể đạt được gì? Bao gồm ví dụ về một công ty hoặc một loại hình kinh doanh và một loại tấn công mạng mà công ty đó có thể là nạn nhân.**

- Có nhiều yếu tố có thể thúc đẩy ai đó bắt đầu một cuộc tấn công mạng chống lại một công ty.

- Dưới đây là một số yếu tố và mục tiêu mà kẻ tấn công có thể đạt được:

* Lợi ích tài chính
* Cạnh tranh kinh doanh
* Phân quyền chính trị hoặc xã hội
* Kiếm điểm danh tiếng

- Một ví dụ cụ thể có thể là một công ty thương mại điện tử bị tấn công bằng phương thức tấn công "SQL Injection". Trong trường hợp này, kẻ tấn công có thể tìm cách thâm nhập vào hệ thống của công ty để truy cập cơ sở dữ liệu khách hàng và đánh cắp thông tin cá nhân, thẻ tín dụng hoặc thông tin thanh toán. Mục tiêu của kẻ tấn công có thể là lợi nhuận thông qua việc bán thông tin này trên thị trường đen hoặc làm hỏng danh tiếng của công ty để giành lợi thế cạnh tranh.

**2. Bạn có nghĩ nên có các tiêu chuẩn bảo mật khác nhau cho đám mây dựa trên loại dữ liệu đang được lưu trữ hoặc xử lý không? Tại sao bạn nghĩ rằng? Cho một ví dụ. Bạn nghĩ bảo mật khác nhau như thế nào giữa dữ liệu được lưu trữ trên đám mây và dữ liệu được lưu trữ tại cơ sở?**

* Có, tôi nghĩ rằng nên có các tiêu chuẩn bảo mật khác nhau cho đám mây dựa trên loại dữ liệu đang được lưu trữ hoặc xử lý.
* Lý do cho điều này là vì mức độ quan trọng và độ nhạy cảm của dữ liệu có thể thay đổi tùy thuộc vào loại dữ liệu và ngữ cảnh sử dụng.
* Ví dụ minh họa và sự khác biệt trong tiêu chuẩn bảo mật giữa dữ liệu được lưu trữ trên đám mây và dữ liệu được lưu trữ tại cơ sở: Dữ liệu cá nhân, như thông tin về khách hàng hoặc dữ liệu y tế, thường được coi là độc quyền và đầy đủ quyền riêng tư. Đối với dữ liệu cá nhân lưu trữ trên đám mây, cần tuân thủ các tiêu chuẩn bảo mật nghiêm ngặt như GDPR (General Data Protection Regulation) hoặc HIPAA (Health Insurance Portability and Accountability Act) tùy thuộc vào lĩnh vực. Điều này bao gồm mã hóa mạnh, kiểm tra và giám sát liên tục, và quản lý quyền truy cập nghiêm ngặt
* Sự khác biệt trong tiêu chuẩn bảo mật giữa dữ liệu lưu trữ trên đám mây và dữ liệu lưu trữ tại cơ sở chủ yếu nằm ở mức độ quản lý rủi ro và biện pháp bảo mật được triển khai. Dữ liệu quan trọng và nhạy cảm thường đòi hỏi các biện pháp bảo mật cao hơn và mức độ kiểm tra nghiêm ngặt hơn. Tuy nhiên, cả hai trường hợp đều cần đảm bảo an toàn và tuân thủ các tiêu chuẩn bảo mật phù hợp.

**3. Bạn nghĩ một quản trị viên bảo mật đám mây thành công cần có những đặc điểm tính cách nào? Tại sao? Đây có phải là vai trò mà bạn quan tâm không?**

- Những đặc điểm tính cách cần có:

* Kiến thức chuyên môn sâu
* Tư duy phân tích
* Kiên nhẫn
* Tỉ mỉ
* Hợp tác, sáng tạo
* Chịu học học

- Đây không phải là vai trò mà tôi quan tâm.

# 

# **Module 9: Monitoring the Cloud.**

**Mục đích của module:**

- Tìm hiểu về các công cụ mà Amazon Web Services (AWS) cung cấp để giám sát các dịch vụ đám mây:

* AWS Config
* AWS CloudTrail
* Amazon CloudWatch.

**Mô tả module:**

- AWS hỗ trợ giám sát, ghi nhật ký và báo cáo về việc sử dụng dịch vụ của mình bằng cách cung cấp các công cụ để thực hiện việc đó.

## **Các khái niệm:**

**1.** **Amazon CloudWatch:**

- Amazon CloudWatch là một hệ thống giám sát được tích hợp sẵn và được lập trình trước, được sử dụng với tất cả các dịch vụ đám mây của Amazon và được thiết kế đặc biệt để đáp ứng yêu cầu báo cáo hiệu suất của các kiến trúc sư hệ thống và quản trị viên.

- *Một số ví dụ:*

* *Giám sát hiệu năng ứng dụng: Hiển thị dữ liệu hiệu năng, tạo cảnh báo và so sánh các dữ liệu để hiểu và giải quyết nguyên nhân gốc rễ của các vấn đề hiệu năng trong tài nguyên AWS của bạn.*
* *Kiểm thử ảnh hưởng lên trang web: Xem ảnh chụp màn hình, bản ghi và yêu cầu trang web tại bất kỳ thời điểm nào để biết chính xác thời điểm và khoảng thời gian trang web của bạn bị ảnh hưởng.*

**2.** **AWS CloudTrail:**

- AWS CloudTrail là một dịch vụ cho phép thực hiện việc quản lý, kiểm tra vận hành và đánh giá rủi ro cho tài khoản AWS của bạn.

- *Dưới đây là một số ví dụ về việc sử dụng AWS CloudTrail:*

* *Giám sát hiệu năng ứng dụng: Hiển thị dữ liệu hiệu năng, tạo cảnh báo và so sánh các dữ liệu để hiểu và giải quyết nguyên nhân gốc rễ của các vấn đề hiệu năng trong tài nguyên AWS của bạn.*
* *Phân tích nguyên nhân gốc rễ: Phân tích chỉ số, bản ghi, dữ liệu thống kê bản ghi và yêu cầu của người dùng để giảm thiểu thời gian giải quyết trung bình.*

**3.** **AWS Config:**

- AWS Config là một công cụ cấu hình giúp bạn ước đoán, kiểm tra cũng như đánh giá cấu hình và mối quan hệ của các tài nguyên.

- *Dưới đây là một số ví dụ về việc sử dụng AWS Config:*

* · *Tối ưu hóa tài nguyên: Tự động hóa hoạt động hoạch định nguồn lực và giảm thiểu chi phí bằng cách thiết lập triển khai hành động khi đạt ngưỡng dựa trên thông số hoặc mô hình máy học của bạn.*
* *Kiểm thử ảnh hưởng lên trang web: Xem ảnh chụp màn hình, bản ghi và yêu cầu trang web tại bất kỳ thời điểm nào để biết chính xác thời điểm và khoảng thời gian trang web của bạn bị ảnh hưởng*.

4. **Amazon Simple Notification Service (Amazon SNS)**

- Amazon Simple Notification Service (Amazon SNS) là một dịch vụ quản lý thông báo được tích hợp sẵn trong AWS. Nó cho phép gửi và nhận thông báo giữa các ứng dụng, hệ thống phân tán và các dịch vụ khác nhau.

- *Dưới đây là một số ví dụ về việc sử dụng Amazon SNS:*

* *Giám sát hiệu năng ứng dụng: Hiển thị dữ liệu hiệu năng, tạo cảnh báo và so sánh các dữ liệu để hiểu và giải quyết nguyên nhân gốc rễ của các vấn đề hiệu năng trong tài nguyên AWS của bạn.*
* *Phân tích nguyên nhân gốc rễ: Phân tích chỉ số, bản ghi, dữ liệu thống kê bản ghi và yêu cầu của người dùng để giảm thiểu thời gian giải quyết trung bình.*

## **Tóm tắt phần Background and Misconceptions:**

**Quản lý Đám Mây AWS: Một Bộ Công Cụ Quan Trọng:**

- AWS cung cấp nhiều dịch vụ liên kết giúp doanh nghiệp quản lý đám mây phức tạp.

- CloudWatch theo dõi tài nguyên và ứng dụng chạy trên AWS

- CloudTrail ghi lại các hoạt động người dùng trong tài khoản AWS.

- AWS Config đánh giá và kiểm tra cấu hình tài nguyên AWS, giúp tự động hóa việc kiểm tra cấu hình.

## Câu hỏi trong phần questions:

**1.** **Bạn sử dụng công cụ nào để luôn ngăn nắp và theo dõi cuộc sống, công việc và lịch trình của mình? Tại sao những công cụ này lại quan trọng? Những loại công cụ nào sẽ hữu ích để giám sát hoặc theo dõi tài nguyên của bạn trên đám mây?**

- Công cụ mà tôi sử dụng: Notion, Google Calendar

- Các công cụ này giúp tôi luôn ngăn nắp và theo dõi một cách chủ động, hiệu quả công việc và cuộc sống của tôi.

- Những loại công cụ hữu ích để giám sát hoặc theo dõi tài nguyên trên đám mây: Amazon CloudWatch, Amazon CloudTrail, AWS Config,…

**2.** **Bạn đã bao giờ bỏ lỡ hoặc đến muộn một sự kiện mà bạn đã lên lịch hoặc quên bài tập chưa? Chuyện gì đã xảy ra thế? Bạn có thể ngăn chặn lỗi bằng cách nào? Bạn có nghĩ lỗi tương tự có thể xảy ra khi sử dụng dịch vụ đám mây với AWS không? Làm thế nào điều này có thể được ngăn chặn?**

- Tôi có lỡ hẹn và đôi khi đến muộn.

- Chuyện xảy ra: tôi quên.

- Tôi có thể ngăn chặn lỗi bằng cách: thêm những việc cần làm vào reminder.

- Tôi nghĩ là có.

- Để ngăn chặn thì chúng ta nên sử dụng các công cụ để giám sát và theo dõi tài nguyên đám mây.

**3.** **Một công ty điện thoại di động sử dụng AWS để cho phép người dùng tải xuống ứng dụng di động cho phép họ in từ xa từ thiết bị của mình. Bạn nghĩ công ty này cần theo dõi những điểm dữ liệu nào trong dịch vụ đám mây của họ? Tại sao?**

- Tài nguyên EC2 và S3.

- Amazon RDS (Relational Database Service)

- CloudWatch Logs và CloudTrail.

- CloudFront và ELB (Elastic Load Balancer).

- Bảo mật và IAM (Identity and Access Management).

Việc theo dõi các điểm dữ liệu này giúp công ty đảm bảo tính khả dụng, hiệu suất, bảo mật và tính nhất quán của dịch vụ in từ xa trên đám mây của họ. Điều này giúp phát hiện và khắc phục sự cố nhanh chóng và đảm bảo rằng người dùng có trải nghiệm tốt khi sử dụng ứng dụng di động của họ.