

# AWS

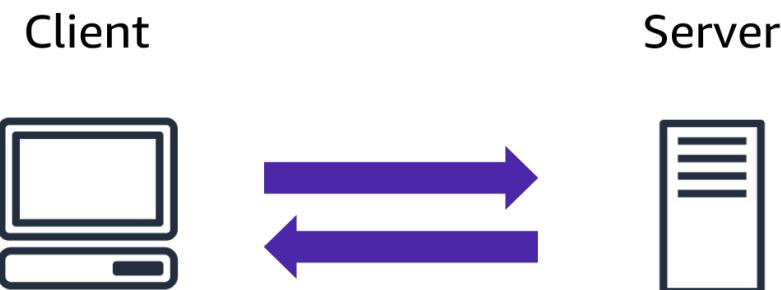
## Điện toán đám mây là gì?

Trước khi chúng ta tìm hiểu sâu hơn về các phần và bộ phận của AWS,hãy thu nhỏ và lẫymột định nghĩa hoạt động tốt về đám mây.Điện toán đám mây là việc cung cấp theo yêu cầucủa tài nguyên CNTT trênInternet với mức giá trả theo mức sử dụng.Hãy phá vỡ điều này.Phân phối theo yêu cầu cho biết AWScó các nguồn lực bạn cần khi bạn cần chúng.Bạn không cần cho chúng tôi biết trướcrằng bạn sẽ cần chúng.Đột nhiên bạn thấy mình cần 300 máy chủ ảo.Vâng, chỉ cần một vài cú nhấp chuột và khởi chạy chúng.Hoặc bạn cần dung lượng lưu trữ 2.000 terabyte;bạn không cần phải báo trước cho chúng tôi,chỉ cần bắt đầu sử dụng bộ nhớ bạn cần khi bạn cần.Không cần chúng nữa,nhanh chóng bạn có thể quay lạihọ và ngừng thanh toán ngay lập tức.Sự linh hoạt đó không phải làcó thể thực hiện được khi bạn đang quản lý trung tâm dữ liệu của riêng mình.Ý tưởng về nguồn lực CNTTthực sự là một phần quan trọng trong triết lý của AWS.Chúng tôi thường được hỏi tại sao AWS có nhiều sản phẩm đến vậy.Câu trả lời thực sự đơn giản.Vì doanh nghiệp cần họ.Nếu có các yếu tố CNTTphổ biến ở nhiều doanh nghiệpthì đây không phải là điểm khác biệt.Lấy cơ sở dữ liệu MySQL làm ví dụ.Nếu doanh nghiệp của bạn chạy cơ sở dữ liệu MySQL,khả năng cài đặt của bạn có tốt khôngcông cụ MySQL tạo raBạn là một công ty tốt hơn đối thủ cạnh tranh của bạn? Vâng, có lẽ không phải vậy.Bạn có giữ bản sao lưu theo cáchkhiến bạn vượt trội hơn những người chơi khác trong ngành của bạn?Một lần nữa, nghi ngờ.Dữ liệu bên trong cơ sở dữ liệu của bạn,bây giờ điều đó cực kỳ khác biệt.Cách bạn xây dựng bảng và quản lý cấu trúchoàn toàn tách biệt bạn khỏi cuộc thi.Nhưng động cơ chỉ là động cơ.Tại AWS, chúng tôi gọi đó là không phân biệt,gánh nặng của CNTT.Những công việc chung,thường lặp đi lặp lại và cuối cùng là tốn thời gian.Đây là những nhiệm vụ AWS muốn trợ giúp bạnđể bạn có thể tập trung vào điều khiến bạn trở nên độc đáo.Qua Internet có vẻ đơn giản,nhưng nó ngụ ý rằng bạn có thể truy cập các tài nguyên đó bằng cách sử dụngmột bảng điều khiển trang web an toàn hoặc theo chương trình.Không cần thêm hợp đồng hoặc cuộc gọi bán hàng.Với mức giá trả theo mức sử dụng, chúng tôiinhấn mạnh lại những gì chúng tôi đã chỉ ra ở quán cà phê này.Bạn không bố trí nhân viên một cửa hàng 24/24ngày ở mức độ tương tự như bạn làm trong

giờ cao điểm.Trên thực tế, có một số giờ bạn thậm chí có thể không bố trí nhân viên cho họ.Tại sao phải trả tiền cho môi trường dành cho nhà phát triển, ví dụ:vào cuối tuần nếu nhà phát triển của bạn không làm việc vào cuối tuần?

## Mô hình Client-Server là gì?

Bạn vừa tìm hiểu thêm về AWS và cách hầu hết tất cả điện toán hiện đại đều sử dụng mô hình máy khách-máy chủ cơ bản. Hãy tóm tắt lại mô hình client-server là gì.



Trong điện toán, **máy khách** có thể là trình duyệt web hoặc ứng dụng máy tính để bàn mà một người tương tác để gửi yêu cầu đến máy chủ máy tính. Máy **chủ** có thể là các dịch vụ như Amazon Elastic Computing Cloud (Amazon EC2), một loại máy chủ ảo. Ví dụ: giả sử khách hàng đưa ra yêu cầu về một bài báo, tỷ số trong trò chơi trực tuyến hoặc một video hài hước. Máy chủ đánh giá chi tiết của yêu cầu này và thực hiện nó bằng cách trả lại thông tin cho khách hàng.

## Mô hình triển khai cho điện toán đám mây

Khi lựa chọn chiến lược đám mây, công ty phải xem xét các yếu tố như các thành phần ứng dụng đám mây bắt buộc, các công cụ quản lý tài nguyên ưu tiên và mọi yêu cầu về cơ sở hạ tầng CNTT kế thừa.

Ba mô hình triển khai điện toán đám mây là dựa trên đám mây, tại chỗ và kết hợp.

### Triển khai dựa trên đám mây

- Chạy tất cả các phần của ứng dụng trên đám mây.
- Di chuyển các ứng dụng hiện có sang đám mây.
- Thiết kế và xây dựng các ứng dụng mới trên đám mây.

Trong mô hình **triển khai dựa trên đám mây**, bạn có thể di chuyển các ứng dụng hiện có sang đám mây hoặc bạn có thể thiết kế và xây dựng các ứng dụng mới trên đám mây. Bạn có thể xây dựng các ứng dụng đó trên cơ sở hạ tầng cấp thấp yêu cầu

nhân viên CNTT của bạn quản lý chúng. Ngoài ra, bạn có thể xây dựng chúng bằng cách sử dụng các dịch vụ cấp cao hơn để giảm bớt các yêu cầu về quản lý, kiến trúc và mở rộng quy mô của cơ sở hạ tầng cốt lõi.

Ví dụ: một công ty có thể tạo một ứng dụng bao gồm máy chủ ảo, cơ sở dữ liệu và các thành phần mạng hoàn toàn dựa trên đám mây.

### **Triển khai tại chỗ**

- Triển khai tài nguyên bằng cách sử dụng các công cụ ảo hóa và quản lý tài nguyên.
- Tăng cường sử dụng tài nguyên bằng cách sử dụng công nghệ ảo hóa và quản lý ứng dụng.

**Triển khai tại chỗ** còn được gọi là *triển khai đám mây riêng*. Trong mô hình này, tài nguyên được triển khai tại cơ sở bằng cách sử dụng các công cụ quản lý tài nguyên và ảo hóa. Ví dụ: bạn có thể có các ứng dụng chạy trên công nghệ được lưu giữ hoàn toàn trong trung tâm dữ liệu tại chỗ của bạn. Mặc dù mô hình này rất giống với cơ sở hạ tầng CNTT truyền thống nhưng việc kết hợp các công nghệ ảo hóa và quản lý ứng dụng giúp tăng cường sử dụng tài nguyên.

### **Triển khai kết hợp**

- Kết nối các tài nguyên dựa trên đám mây với cơ sở hạ tầng tại chỗ.
- Tích hợp các tài nguyên dựa trên đám mây với các ứng dụng CNTT cũ.

Trong **triển khai kết hợp**, tài nguyên dựa trên đám mây được kết nối với cơ sở hạ tầng tại chỗ. Bạn có thể muốn sử dụng phương pháp này trong một số trường hợp. Ví dụ: bạn có các ứng dụng cũ được bảo trì tốt hơn tại cơ sở hoặc các quy định của chính phủ yêu cầu doanh nghiệp của bạn lưu giữ một số hồ sơ nhất định tại cơ sở.

Ví dụ: giả sử một công ty muốn sử dụng các dịch vụ đám mây có thể tự động hóa việc xử lý và phân tích dữ liệu hàng loạt. Tuy nhiên, công ty có một số ứng dụng cũ phù hợp hơn tại cơ sở và sẽ không được di chuyển sang đám mây. Với việc triển khai kết hợp, công ty sẽ có thể duy trì các ứng dụng cũ tại chỗ trong khi vẫn hưởng lợi từ các dịch vụ phân tích và dữ liệu chạy trên đám mây.

## **Lợi ích của điện toán đám mây**

Hãy xem xét lý do tại sao một công ty có thể chọn áp dụng một phương pháp điện toán đám mây cụ thể khi giải quyết các nhu cầu kinh doanh.

### **Chuyển đổi chi phí trả trước thành chi phí biến đổi**

Chi phí trả trước đề cập đến trung tâm dữ liệu, máy chủ vật lý và các tài nguyên khác mà bạn cần đầu tư trước khi sử dụng chúng. Chi phí biến đổi có nghĩa là bạn chỉ trả tiền cho các tài nguyên máy tính mà bạn sử dụng thay vì đầu tư mạnh vào trung tâm dữ liệu và máy chủ trước khi bạn biết mình sẽ sử dụng chúng như thế nào.

Bằng cách áp dụng phương pháp điện toán đám mây mang lại lợi ích về chi phí thay đổi, các công ty có thể triển khai các giải pháp đổi mới đồng thời tiết kiệm chi phí.

### **Ngừng chi tiền để vận hành và bảo trì trung tâm dữ liệu**

Việc tính toán trong trung tâm dữ liệu thường đòi hỏi bạn phải tốn nhiều tiền và thời gian hơn để quản lý cơ sở hạ tầng và máy chủ. Lợi ích của điện toán đám mây là khả năng tập trung ít hơn vào các nhiệm vụ này và tập trung nhiều hơn vào ứng dụng và khách hàng của bạn.

### **Ngừng đoán khả năng**

Với điện toán đám mây, bạn không cần phải dự đoán mình sẽ cần bao nhiêu năng lực cơ sở hạ tầng trước khi triển khai một ứng dụng. Ví dụ: bạn có thể khởi chạy các phiên bản Amazon EC2 khi cần và chỉ trả tiền cho thời gian điện toán bạn sử dụng. Thay vì trả tiền cho những tài nguyên không được sử dụng hoặc phải đổi mặt với dung lượng hạn chế, bạn chỉ có thể truy cập vào dung lượng mà bạn cần. Bạn cũng có thể mở rộng quy mô hoặc mở rộng quy mô để đáp ứng nhu cầu.

### **Hưởng lợi từ quy mô kinh tế lớn**

Bằng cách sử dụng điện toán đám mây, bạn có thể đạt được chi phí biến đổi thấp hơn mức bạn có thể tự mình nhận được. Vì mức sử dụng của hàng trăm nghìn khách hàng có thể tổng hợp trên đám mây nên các nhà cung cấp, chẳng hạn như AWS, có thể đạt được hiệu quả kinh tế nhờ quy mô cao hơn. Tính kinh tế của quy mô chuyển thành mức giá trả theo mức sử dụng thấp hơn.

### **Tăng tốc độ và sự nhanh nhẹn**

Tính linh hoạt của điện toán đám mây giúp bạn phát triển và triển khai ứng dụng dễ dàng hơn.

Tính linh hoạt này giúp bạn có nhiều thời gian hơn để thử nghiệm và đổi mới. Khi tính toán trong trung tâm dữ liệu, có thể mất vài tuần để có được tài nguyên mới mà bạn cần. Để so sánh, điện toán đám mây cho phép bạn truy cập các tài nguyên mới trong vòng vài phút.

### **Vươn ra toàn cầu trong vài phút**

Dấu ấn toàn cầu của Đám mây AWS cho phép bạn triển khai ứng dụng cho khách hàng trên toàn thế giới một cách nhanh chóng, đồng thời mang đến cho họ độ trễ thấp. Điều này có nghĩa là ngay cả khi bạn ở một nơi khác trên thế giới với khách hàng của mình, khách hàng vẫn có thể truy cập ứng dụng của bạn với độ trễ tối thiểu.

Ở phần sau của khóa học này, bạn sẽ khám phá cơ sở hạ tầng toàn cầu của AWS một cách chi tiết hơn. Bạn sẽ xem xét một số dịch vụ mà bạn có thể sử dụng để cung cấp nội dung cho khách hàng trên toàn thế giới.

## Đám mây điện toán đám mây của Amazon (Amazon EC2)

Nếu bạn còn nhớ quán cà phê của chúng tôi, nhân viên là phép ẩn dụ chomô hình máy chủ khách, trong đó khách hàng gửi yêu cầu đến máy chủ. Máy chủ thực hiện một số công việc và sau đó gửi phản hồi. Ví dụ đó dành cho quán cà phê, nhưng ý tưởng tương tự cũng áp dụng cho các doanh nghiệp khác. Doanh nghiệp của bạn, cho dù đó là lĩnh vực chăm sóc sức khỏe, sản xuất, bảo hiểm, hoặc cung cấp nội dung video tới hàng triệu người dùng trên toàn thế giới. Cũng đang sử dụng mô hình này để cung cấp sản phẩm, Tài nguyên hoặc dữ liệu cho người dùng cuối của bạn. Và bạn sẽ cần máy chủ để hỗ trợ doanh nghiệp và ứng dụng của mình. Bạn cần khả năng tính toán thô để lưu trữ các ứng dụng của mình và cung cấp sức mạnh tính toán mà doanh nghiệp của bạn cần.

Khi bạn làm việc với AWS, các máy chủ đó là ảo và máy chủ bạn sử dụng để có quyền truy cập vào máy chủ ảo được gọi là EC2. Sử dụng EC2 để tính toán có tính linh hoạt cao, tiết kiệm chi phí và nhanh chóng khi bạn so sánh nó với việc chạy các máy chủ của riêng bạn tại cơ sở trong trung tâm dữ liệu mà bạn sở hữu. Thời gian và tiền bạc cần thiết để thiết lập và vận hành các nguồn lực tại chỗ khá cao khi bạn sở hữu đội máy chủ vật lý của riêng mình. Trước tiên, bạn phải thực hiện nhiều nghiên cứu để xem bạn muốn sử dụng loại máy chủ nào mua, và bạn sẽ cần bao nhiêu. Sau đó, bạn mua trả trước phần cứng đó. [ÂM THANH] Bạn sẽ đợi nhiều tuần hoặc nhiều tháng để một nhà cung cấp để cung cấp các máy chủ đó cho bạn. Sau đó, bạn đưa chúng đến trung tâm dữ liệu mà bạn sở hữu hoặc thuê để lắp đặt chúng trên giá và xếp chúng lại và nối dây tất cả lại. Sau đó, bạn đảm bảo rằng chúng được an toàn và được cấp nguồn, đồng thời sau đó chúng đã sẵn sàng để được sử dụng. Chỉ khi đó bạn mới có thể bắt đầu lưu trữ ứng dụng của mình trên các máy chủ này. Điều tệ nhất là, khi bạn mua những máy chủ này, bạn bị mắc kẹt với chúng, cho dù bạn có sử dụng chúng hay không. Với EC2, việc bắt đầu dễ dàng hơn nhiều. AWS đã giải quyết phần khó khăn cho bạn rồi. AWS đã xây dựng và bảo mật các trung tâm dữ liệu. AWS đã mua các máy chủ, sắp xếp và xếp chồng chúng lên nhau,

đồng thời chúng đã trực tuyến, sẵn sàng để sử dụng.AWS liên tục vận hành một lượng công suất tính toán khổng lồ.Và bạn có thể sử dụng bất kỳ phần nào trong khả năng đó khi bạn cần.

Tất cả những gì bạn phải làm là yêu cầu các phiên bản EC2 mà bạn muốn,và chúng sẽ khởi chạy và khởi động, sẵn sàng để sử dụng trong vòng vài phút.Sau khi hoàn tất, bạn có thể dễ dàng dừng hoặc chấm dứt các phiên bản EC2.Bạn không bị khóa hoặc mắc kẹt với các máy chủ mà bạn không cần hoặc không muốnn.[Việc](#) sử dụng phiên bản EC2 của bạn có thể thay đổi rất nhiều theo thời gian và bạn chỉ trả tiền cho những gì bạn sử dụng.Vì với EC2, bạn chỉ phải trả tiền cho các phiên bản đang chạy, không phải các phiên bản bị dừng hoặc chấm dứt(EC2 chạy trên các máy chủ vật lý do AWS quản lý bằng cách sử dụng công nghệ ảo hóa.Khi bạn tạo một phiên bản EC2,bạn không nhất thiết phải lấy toàn bộ máy chủ cho riêng mình.Thay vào đó, bạn đang chia sẻ máy chủ với nhiều phiên bản khác,còn được gọi là máy ảo.Và một hypervisor chạy trên máy chủ sẽ chịu trách nhiệmchia sẻ tài nguyên vật lý cơ bản giữa các máy ảo.

Ý tưởng chia sẻ phần cứng cơ bản này được gọi là multitenancy.Hypervisor chịu trách nhiệm điều phối tính đa dạng này và nó được quản lý bởi AWS.Hypervisor chịu trách nhiệm cách ly các máy ảo khỏi nhau kinh khác khi họ chia sẻ tài nguyên từ máy chủ.

Điều này có nghĩa là các phiên bản EC2 được bảo mật ngay cả khi chúng có thể đang chia sẻ tài nguyên.Một phiên bản EC2 không biết về bất kỳ phiên bản EC2 nào khác trên máy chủ đó.Họ được an toàn và tách biệt với nhau.May mắn thay, đây không phải là thứ bạn cần phải thiết lập.Nhưng điều quan trọng là phải biết ý tưởng về việc thuê nhiều nơi và có sự hiểu biết ở mức độ cao về cách thức hoạt động của nó.

EC2 mang đến cho bạn sự linh hoạt và khả năng kiểm soát tuyệt vời.Bạn không chỉ có thể khởi động các máy chủ mới hoặc đưa chúng ngoại tuyến theo ý muốn mà còn bạn cũng có sự linh hoạt và quyền kiểm soát cấu hình của những phiên bản đó.

Khi bạn cung cấp phiên bản EC2,bạn có thể chọn hệ điều hành dựa trên Windows hoặc Linux.Bạn có thể cung cấp hàng nghìn phiên bản EC2 trên nhu cầu với sự kết hợp của hệ điều hành và cấu hình để hỗ trợ các ứng dụng khác nhau cho doanh nghiệp của bạn.[Ngoài](#) hệ điều hành, bạn còn định cấu hình phần mềm nào bạn muốn chạy trên phiên bản đó.Cho dù đó là ứng dụng kinh doanh nội bộ của riêng bạn, ứng dụng web đơn giản hay các ứng dụng web, cơ sở dữ liệu phức tạp hoặc phần mềm của bên thứ ba.[Giống](#) như các gói phần mềm doanh nghiệp,bạn có toàn quyền kiểm soát những gì xảy ra trong trường hợp đó.

Các phiên bản EC2 cũng có thể thay đổi kích thước.Bạn có thể bắt đầu với một ví dụ nhỏ,nhận ra ứng dụng bạn đang chạy đang bắt đầu sử dụng tối đa máy chủ đó.Và sau đó bạn có thể cung cấp cho phiên bản đó nhiều bộ nhớ hơn và nhiều CPU hơn.Đó là

những gì chúng tôi gọi là chia tỷ lệ theo chiều dọc một phiên bản.Về bản chất, bạn có thể làm cho các phiên bản lớn hơn hoặc nhỏ hơn bất cứ khi nào bạn cần.Bạn cũng kiểm soát khía cạnh kết nối mạng của EC2.Vậy loại yêu cầu nào gửi đến máy chủ của bạn và liệu chúng có thể truy cập công khai hay riêng tư hay không là do bạn quyết định.[Chúng](#) ta sẽ đề cập chi tiết hơn về vấn đề này sau trong khóa học.Máy ảo không phải là điều gì mới mẻ mà là sự dễ dàng cung cấp phiên bản EC2 cho phép các lập trình viên và doanh nghiệp đổi mới nhanh hơn.[AWS](#) vừa làm cho việc này trở nên dễ dàng hơn rất nhiều và tiết kiệm chi phí hơn cho bạn có được máy chủ thông qua mô hình Dịch vụ điện toán này.

## Đám mây điện toán đám mây của Amazon (Amazon EC2)

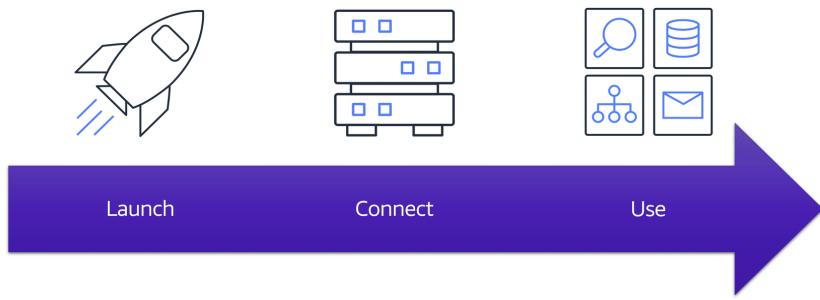
Đám mây điện toán đám mây của Amazon (Amazon EC2) cung cấp khả năng tính toán an toàn, có thể thay đổi kích thước trên đám mây dưới dạng phiên bản Amazon EC2. Hãy tưởng tượng bạn chịu trách nhiệm về kiến trúc tài nguyên của công ty mình và cần hỗ trợ các trang web mới. Với các tài nguyên tại chỗ truyền thống, bạn phải làm như sau:

- Chi tiền trả trước để mua phần cứng.
- Đợi máy chủ được giao cho bạn.
- Cài đặt máy chủ trong trung tâm dữ liệu vật lý của bạn.
- Thực hiện tất cả các cấu hình cần thiết.

Để so sánh, với phiên bản Amazon EC2, bạn có thể sử dụng máy chủ ảo để chạy các ứng dụng trên Đám mây AWS.

- Bạn có thể cung cấp và khởi chạy phiên bản Amazon EC2 trong vòng vài phút.
- Bạn có thể ngừng sử dụng nó khi đã chạy xong khối lượng công việc.
- Bạn chỉ phải trả tiền cho thời gian điện toán bạn sử dụng khi phiên bản đang chạy chứ không phải khi phiên bản đó bị dừng hoặc chấm dứt.
- Bạn có thể tiết kiệm chi phí bằng cách chỉ trả tiền cho dung lượng máy chủ mà bạn cần hoặc muốn.

## Cách hoạt động của Amazon EC2



## Phóng

Đầu tiên, bạn khởi chạy một phiên bản. Bắt đầu bằng cách chọn mẫu có cấu hình cơ bản cho phiên bản của bạn. Các cấu hình này bao gồm hệ điều hành, máy chủ ứng dụng hoặc ứng dụng. Bạn cũng chọn loại phiên bản, đây là cấu hình phần cứng cụ thể cho phiên bản của bạn.

Khi chuẩn bị khởi chạy một phiên bản, bạn chỉ định các cài đặt bảo mật để kiểm soát lưu lượng mạng có thể vào và ra khỏi phiên bản của bạn. Ở phần sau của khóa học này, chúng ta sẽ khám phá các tính năng bảo mật của Amazon EC2 một cách chi tiết hơn.

## Kết nối

Tiếp theo, kết nối với phiên bản. Bạn có thể kết nối với phiên bản theo nhiều cách. Các chương trình và ứng dụng của bạn có nhiều phương thức khác nhau để kết nối trực tiếp với phiên bản và trao đổi dữ liệu. Người dùng cũng có thể kết nối với phiên bản bằng cách đăng nhập và truy cập vào màn hình máy tính.

## Sử dụng

Sau khi bạn đã kết nối với phiên bản, bạn có thể bắt đầu sử dụng nó. Bạn có thể chạy các lệnh để cài đặt phần mềm, thêm bộ nhớ, sao chép và sắp xếp tệp, v.v.

# Các loại phiên bản Amazon EC2

Bây giờ chúng ta đã tìm hiểu về Phiên bản EC2 và vai trò quan trọng của chúng trong AWS,hãy nói về các loại Phiên bản EC2 khác nhau hiện có.

Nghĩ lại ví dụ tương tự về quán cà phê của chúng ta, bạn sẽ nhớ rằng Phiên bản EC2 giống như nhân viên của chúng tôi và họ phục vụ các yêu cầu của khách hàng.Nếu chúng ta muốn có một quán cà phê có thể phục vụ được nhiều khách hàng, thì có lẽ chúng ta sẽ cần nhiều nhân viên, phải không?Và tất cả họ không thể chỉ là nhân viên thu ngân.[Chúng](#) ta cũng cần người pha chế đồ uống, người chế biến thức ăn,và có thể ai đó

sẽ thực hiện tác phẩm nghệ thuật pha cà phê tuyệt vời mà khách hàng của chúng tôi vô cùng yêu thích.[Giống](#) như bất kỳ hoạt động kinh doanh nào, có rất nhiều nhiệm vụ cần phải được thực hiện và họ thường yêu cầu các bộ kỹ năng khác nhau.Nếu chúng ta muốn doanh nghiệp của mình hoạt động hiệu quả nhất có thể, điều quan trọng là phải đảm bảo rằng kỹ năng của nhân viên phù hợp với vai trò của họ.Cũng giống như quán cà phê của chúng tôi có nhiều loại nhân viên khác nhau,AWS có nhiều loại Phiên bản EC2 khác nhau mà bạn có thể tạo ra và triển khai vào môi trường AWS.Mỗi loại phiên bản được nhóm lại theo một họ phiên bản và được tối ưu hóa cho một số loại nhiệm vụ nhất định.

Các loại phiên bản cung cấp nhiều cách kết hợp CPU, bộ nhớ, dung lượng lưu trữ và kết nối mạng, đồng thời cho phép bạn linh hoạt lựa chọn sự kết hợp tài nguyên thích hợp cho các ứng dụng của bạn.

Các dòng phiên bản khác nhau trong EC2 đều có mục đích chung, được tối ưu hóa về mặt điện toán, tối ưu hóa bộ nhớ, tăng tốc tính toán và tối ưu hóa lưu trữ.

Các phiên bản có mục đích chung cung cấp sự cân bằng tốt giữa tính toán, bộ nhớ và tài nguyên mạng và có thể được sử dụng cho nhiều khối lượng công việc đa dạng như dịch vụ web hoặc mã. Phiên bản điện toán được tối ưu hóa lý tưởng cho các tác vụ điện toán chuyên sâu như chơi game, dịch vụ, điện toán hiệu năng cao hoặc HPC và thậm chí cả mô hình khoa học.Tương tự, các phiên bản được tối ưu hóa bộ nhớ sẽ phù hợp cho các tác vụ đòi hỏi nhiều bộ nhớ.Tính toán tăng tốc, rất tốt cho việc tính toán số liệu phẩy động, xử lý đồ họa hoặc khớp mẫu dữ liệu, khi họ sử dụng bộ tăng tốc phần cứng.Và cuối cùng, việc tối ưu hóa dung lượng lưu trữ rất tốt, bạn có đoán được không? Khối lượng công việc đòi hỏi hiệu suất cao cho dữ liệu được lưu trữ cục bộ.

Bây giờ nếu chúng ta ánh xạ lại quán cà phê của mình, nhân viên thu ngân sẽ trở thành ký ức.Phiên bản EC2 được tối ưu hóa, nhân viên pha chế trở thành phiên bản được tối ưu hóa về mặt điện toán và nhân viên nghệ thuật pha cà phê của chúng tôi là loại phiên bản điện toán tăng tốc.Và bạn đã có nó, các loại Phiên bản EC2.

#### READING:

[Các loại phiên bản Amazon EC2](#) được tối ưu hóa cho các nhiệm vụ khác nhau. Khi chọn loại phiên bản, hãy xem xét nhu cầu cụ thể của khối lượng công việc và ứng dụng của bạn. Điều này có thể bao gồm các yêu cầu về khả năng tính toán, bộ nhớ hoặc lưu trữ.

#### **Các trường hợp có mục đích chung**

**Các phiên bản có mục đích chung** cung cấp sự cân bằng giữa tài nguyên điện toán, bộ nhớ và mạng. Bạn có thể sử dụng chúng cho nhiều khối lượng công việc khác nhau,

chẳng hạn như:

- máy chủ ứng dụng
- máy chủ chơi game
- máy chủ phụ trợ cho các ứng dụng doanh nghiệp
- cơ sở dữ liệu vừa và nhỏ

Giả sử bạn có một ứng dụng trong đó tài nguyên cần cho tính toán, bộ nhớ và kết nối mạng gần như tương đương. Bạn có thể cân nhắc việc chạy nó trên một phiên bản có mục đích chung vì ứng dụng không yêu cầu tối ưu hóa trong bất kỳ vùng tài nguyên nào.

## Tính toán các phiên bản được tối ưu hóa

**Phiên bản điện toán được tối ưu hóa** là lựa chọn lý tưởng cho các ứng dụng thiên về điện toán được hưởng lợi từ bộ xử lý hiệu năng cao. Giống như các phiên bản có mục đích chung, bạn có thể sử dụng các phiên bản điện toán được tối ưu hóa cho các khối lượng công việc như máy chủ web, ứng dụng và trò chơi.

Tuy nhiên, điểm khác biệt là các ứng dụng được tối ưu hóa điện toán lý tưởng cho các máy chủ web hiệu suất cao, máy chủ ứng dụng chuyên sâu về điện toán và máy chủ chơi game chuyên dụng. Bạn cũng có thể sử dụng các phiên bản điện toán được tối ưu hóa cho khối lượng công việc xử lý hàng loạt yêu cầu xử lý nhiều giao dịch trong một nhóm.

## Phiên bản được tối ưu hóa bộ nhớ

**Phiên bản được tối ưu hóa bộ nhớ** được thiết kế để mang lại hiệu năng nhanh cho khối lượng công việc xử lý tập dữ liệu lớn trong bộ nhớ. Trong điện toán, bộ nhớ là vùng lưu trữ tạm thời. Nó chứa tất cả dữ liệu và hướng dẫn mà bộ xử lý trung tâm (CPU) cần để có thể hoàn thành các hành động. Trước khi một chương trình hoặc ứng dụng máy tính có thể chạy, nó sẽ được tải từ bộ lưu trữ vào bộ nhớ. Quá trình tải trước này cho phép CPU truy cập trực tiếp vào chương trình máy tính.

Giả sử bạn có khối lượng công việc yêu cầu tải trước lượng lớn dữ liệu trước khi chạy ứng dụng. Kịch bản này có thể là cơ sở dữ liệu hiệu suất cao hoặc khối lượng công việc liên quan đến việc thực hiện xử lý thời gian thực một lượng lớn dữ liệu phi cấu trúc.

Trong các loại trường hợp sử dụng này, hãy cân nhắc sử dụng phiên bản được tối ưu hóa bộ nhớ. Phiên bản được tối ưu hóa bộ nhớ cho phép bạn chạy khối lượng công việc có nhu cầu bộ nhớ cao và nhận được hiệu năng tuyệt vời.

## Phiên bản điện toán tăng tốc

**Phiên bản điện toán tăng tốc** sử dụng bộ tăng tốc phần cứng hoặc bộ đồng xử lý để thực hiện một số chức năng hiệu quả hơn mức có thể trong phần mềm chạy trên CPU. Ví dụ về các chức năng này bao gồm tính toán số dấu phẩy động, xử lý đồ họa và khớp mẫu dữ liệu.

Trong điện toán, bộ tăng tốc phần cứng là một thành phần có thể đẩy nhanh quá trình xử lý dữ liệu. Phiên bản điện toán tăng tốc rất lý tưởng cho các khối lượng công việc như ứng dụng đồ họa, phát trực tuyến trò chơi và truyền phát ứng dụng.

### **Phiên bản được tối ưu hóa bộ nhớ**

**Phiên bản được tối ưu hóa về lưu trữ** được thiết kế cho khối lượng công việc yêu cầu quyền truy cập đọc và ghi tuần tự cao vào các tập dữ liệu lớn trên bộ nhớ cục bộ. Ví dụ về khối lượng công việc phù hợp với các phiên bản được tối ưu hóa về lưu trữ bao gồm hệ thống tệp phân tán, ứng dụng lưu trữ dữ liệu và hệ thống xử lý giao dịch trực tuyến (OLTP) tần số cao.

Trong điện toán, thuật ngữ hoạt động đầu vào/đầu ra mỗi giây (IOPS) là thước đo đo hiệu suất của thiết bị lưu trữ. Nó cho biết một thiết bị có thể thực hiện bao nhiêu thao tác đầu vào hoặc đầu ra khác nhau trong một giây. Các phiên bản được tối ưu hóa về lưu trữ được thiết kế để cung cấp hàng chục nghìn IOPS ngẫu nhiên, có độ trễ thấp cho các ứng dụng.

Bạn có thể coi các thao tác nhập dữ liệu là dữ liệu được đưa vào hệ thống, chẳng hạn như các bản ghi được nhập vào cơ sở dữ liệu. Hoạt động đầu ra là dữ liệu được tạo bởi máy chủ. Một ví dụ về đầu ra có thể là phân tích được thực hiện trên các bản ghi trong cơ sở dữ liệu. Nếu bạn có một ứng dụng có yêu cầu IOPS cao, phiên bản được tối ưu hóa về bộ nhớ có thể mang lại hiệu năng tốt hơn so với các loại phiên bản khác không được tối ưu hóa cho loại trường hợp sử dụng này.

## **Giá Amazon EC2**

Chúng ta đã nói về hai loại phiên bản EC. Nhưng có lẽ tất cả các bạn đang thắc mắc việc này sẽ khiến tôi tốn bao nhiêu tiền?

Đừng lo lắng vì EC hai chúng tôi có sẵn nhiều tùy chọn thanh toán. Cái đầu tiên và cái mà hầu hết mọi người quen thuộc đều được gọi theo yêu cầu. Điều đó có nghĩa là bạn chỉ trả tiền cho khoảng thời gian mà phiên bản của bạn chạy. Tốc độ này có thể là mỗi giờ hoặc mỗi giây, tùy thuộc vào loại phiên bản và hệ điều hành bạn chọn để chạy. Ngoài ra, không cần cam kết dài hạn hoặc thanh toán trả trước. [c. Kiểu](#) định giá này thường áp dụng khi bạn bắt đầu và muốn khởi động máy chủ để kiểm tra khối lượng công việc và

thử nghiệm.Bạn không cần bất kỳ hợp đồng trước hoặc liên lạc với AWS để sử dụng giá theo yêu cầu.Bạn cũng có thể sử dụng chúng để có được đường cơ sở chomức sử dụng trung bình của bạn sẽ đưa chúng tôi đến kế hoạch tiết kiệm tùy chọn giá tiếp theo.Gói tiết kiệm đưa ra mức giá thấp khi sử dụng EC2 để đổi lấy cam kết về lượng sử dụng nhất quán.Được đo bằng đô la mỗi giờ trong thời hạn một hoặc ba năm.[m.Do](#) đó, mô hình định giá linh hoạt này có thể giúp tiết kiệm tốitới 72% mức sử dụng điện toán AWS của bạn.Điều này có thể giảm giá sử dụng EC 2 của bạn bất kể trường hợp nào,dòng, quy mô xu hướng hệ điều hành hoặc khu vực AWS.Điều này cũng áp dụng cho việc sử dụng AWS fargate và AWS lambda.Có các tùy chọn điện toán serverless mà chúng tôi sẽ đề cập sau trong khóa học này.

Một lựa chọn khác là các phiên bản dành riêng.[Chúng](#) phù hợp với khối lượng công việc ở trạng thái ổn định hoặc khối lượng công việc có mức sử dụng có thể dự đoán được.Và cung cấp cho bạn mức giảm giá lên tới 75% so với giá theo yêu cầu.Bạn đủ điều kiện được giảm giá khi bạn cam kết thời hạn một hoặc ba năm và có thể thanh toán cho họ bằng ba tùy chọn thanh toán.Tất cả đều trả trước, trong đó bạn thanh toán đầy đủ cho chúng khi bạn cam kết một phần trả trước bạn sẽ trả một phần khi bạn cam kết và không trả trước khi bạn không trả bất cứ điều gì ngay từ đầu?

Tùy chọn tiếp theo là các phiên bản giao ngay và chúng cho phép bạn yêu cầu các phiên bản dự phòng.Dung lượng điện toán Amazon EC2, lên tới 90% giá theo yêu cầu.Điều hấp dẫn ở đây là AWS có thể lấy lại phiên bản đó bất kỳ lúc nào họ cần.Đưa ra cảnh báo hai phút cho bạn để hoàn thành công việc và lưu trạng thái.Bạn luôn có thể tiếp tục sau nếu cần.Vì vậy, khi chọn các trường hợp tại chỗ, đảm bảo khối lượng công việc của bạn có thể chịu đựng được việc bị gián đoạn.Một ví dụ điển hình trong số đó là khối lượng công việc hàng loạt.

Và cuối cùng, Chúng tôi có máy chủ chuyên dụng.Máy chủ vật lý nào dành riêng cho bạn sử dụng cho EC2.Đây thường là để đáp ứng các yêu cầu tuân thủ nhất định,và không ai khác sẽ chia sẻ quyền thuê máy chủ đó.

## READING

Với Amazon EC2, bạn chỉ phải trả phí cho thời gian tính toán mà bạn sử dụng. Amazon EC2 cung cấp nhiều tùy chọn giá khác nhau cho các trường hợp sử dụng khác nhau. Ví dụ: nếu trường hợp sử dụng của bạn có thể chịu được tình trạng gián đoạn, bạn có thể

lưu bằng Phiên bản dùng ngay. Bạn cũng có thể tiết kiệm bằng cách cam kết sớm và khóa ở mức sử dụng tối thiểu với Phiên bản dự trữ.

## On-Demand

**Phiên bản Theo yêu cầu** lý tưởng cho khối lượng công việc ngắn hạn, không thường xuyên và không thể bị gián đoạn. Không áp dụng chi phí trả trước hoặc hợp đồng tối thiểu. Các phiên bản chạy liên tục cho đến khi bạn dừng chúng và bạn chỉ phải trả tiền cho thời gian điện toán mà bạn sử dụng. Các trường hợp sử dụng mẫu cho Phiên bản theo yêu cầu bao gồm việc phát triển và thử nghiệm các ứng dụng cũng như chạy các ứng dụng có kiểu sử dụng không thể đoán trước. Phiên bản theo yêu cầu không được khuyến nghị cho khối lượng công việc kéo dài một năm hoặc lâu hơn vì những khối lượng công việc này có thể tiết kiệm chi phí nhiều hơn khi sử dụng Phiên bản dự trữ.

## Amazon EC2 Savings Plans

AWS cung cấp Savings Plans cho một số dịch vụ điện toán, bao gồm cả Amazon EC2. **Gói tiết kiệm Amazon EC2** cho phép bạn giảm chi phí điện toán bằng cách cam kết mức sử dụng điện toán nhất quán trong thời hạn 1 năm hoặc 3 năm. Cam kết có thời hạn này giúp tiết kiệm tới 72% so với chi phí Theo yêu cầu.

Mọi mức sử dụng vượt quá cam kết đều được tính theo mức giá của Savings Plan đã chiết khấu (ví dụ: 10 USD một giờ). Mọi mức sử dụng vượt quá cam kết sẽ bị tính phí theo mức giá Theo yêu cầu thông thường.

Ở phần sau của khóa học này, bạn sẽ xem xét AWS Cost Explorer, một công cụ cho phép bạn trực quan hóa, hiểu và quản lý chi phí cũng như mức sử dụng AWS của mình theo thời gian. Nếu bạn đang cân nhắc các lựa chọn cho Savings Plans, AWS Cost Explorer có thể phân tích mức sử dụng Amazon EC2 của bạn trong 7, 30 hoặc 60 ngày qua. AWS Cost Explorer cũng cung cấp các đề xuất tùy chỉnh cho Kế hoạch tiết kiệm. Những đề xuất này ước tính số tiền bạn có thể tiết kiệm được trên chi phí Amazon EC2 hàng tháng của mình, dựa trên mức sử dụng Amazon EC2 trước đó và số tiền cam kết hàng giờ trong Kế hoạch tiết kiệm 1 năm hoặc 3 năm.

## Reserved Instances

**Phiên bản dự trữ** là khoản chiết khấu thanh toán được áp dụng cho việc sử dụng Phiên bản theo yêu cầu trong tài khoản của bạn. Bạn có thể mua Phiên bản dự trữ tiêu chuẩn và Phiên bản dự trữ có thể chuyển đổi với thời hạn 1 năm hoặc 3 năm và Phiên bản dự trữ theo lịch trình với thời hạn 1 năm. Bạn nhận ra mức tiết kiệm chi phí lớn hơn với tùy chọn 3 năm.

Khi kết thúc thời hạn của Phiên bản dự trữ, bạn có thể tiếp tục sử dụng phiên bản Amazon EC2 mà không bị gián đoạn. Tuy nhiên, bạn sẽ bị tính phí theo mức giá Theo yêu cầu cho đến khi bạn thực hiện một trong những thao tác sau:

- Chấm dứt phiên bản.
- Mua Phiên bản dự trữ mới phù hợp với các thuộc tính của phiên bản (loại phiên bản, Khu vực, đối tượng thuê và nền tảng).

## **Spot Instances**

**Phiên bản Spot** lý tưởng cho khối lượng công việc có thời gian bắt đầu và kết thúc linh hoạt hoặc có thể chịu được sự gián đoạn. Phiên bản Spot sử dụng công suất điện toán Amazon EC2 chưa sử dụng và giúp bạn tiết kiệm chi phí với mức giảm tới 90% so với giá Theo yêu cầu. Giả sử bạn có một công việc xử lý nền có thể bắt đầu và dừng khi cần thiết (chẳng hạn như công việc xử lý dữ liệu cho một cuộc khảo sát khách hàng). Bạn muốn bắt đầu và dừng công việc xử lý mà không ảnh hưởng đến hoạt động chung của doanh nghiệp mình. Nếu bạn thực hiện yêu cầu Spot và dung lượng Amazon EC2 có sẵn, Phiên bản Spot của bạn sẽ khởi chạy. Tuy nhiên, nếu bạn thực hiện yêu cầu Spot và dung lượng Amazon EC2 không khả dụng thì yêu cầu đó sẽ không thành công cho đến khi có dung lượng. Dung lượng không khả dụng có thể trì hoãn việc khởi chạy công việc xử lý nền của bạn. Sau khi bạn khởi chạy Phiên bản Spot, nếu dung lượng không còn hoặc nhu cầu về Phiên bản Spot tăng lên, phiên bản của bạn có thể bị gián đoạn. Điều này có thể không gây ra bất kỳ vấn đề nào cho công việc xử lý nền của bạn. Tuy nhiên, trong ví dụ trước về phát triển và thử nghiệm ứng dụng, rất có thể bạn sẽ muốn tránh những gián đoạn không mong muốn. Do đó, hãy chọn loại phiên bản EC2 khác lý tưởng cho các tác vụ đó.

## **Dedicated Hosts**

**Máy chủ chuyên dụng** là máy chủ vật lý có dung lượng phiên bản Amazon EC2 hoàn toàn dành riêng cho mục đích sử dụng của bạn.

Bạn có thể sử dụng giấy phép phần mềm trên mỗi ổ cắm, mỗi lõi hoặc mỗi VM hiện có của mình để giúp duy trì việc tuân thủ giấy phép. Bạn có thể mua Máy chủ chuyên dụng theo yêu cầu và Đặt trước máy chủ chuyên dụng. Trong số tất cả các tùy chọn Amazon EC2 được đề cập, Máy chủ chuyên dụng là đắt nhất.

# **Mở rộng quy mô Amazon EC2 (Phần 1)**

## **Scalability**

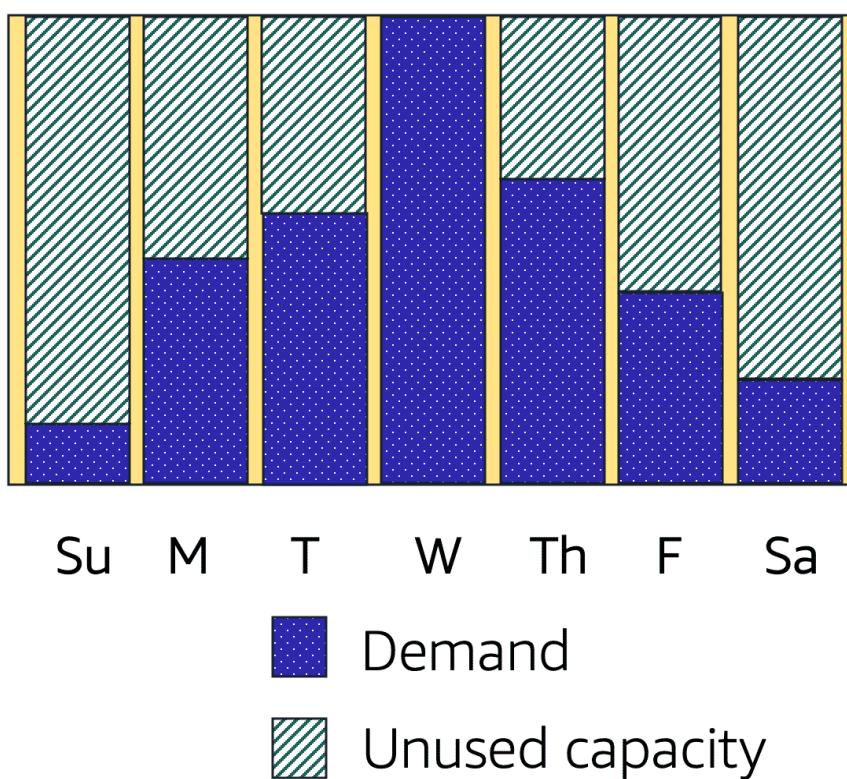
**Khả năng mở rộng** bao gồm việc bắt đầu chỉ với những tài nguyên bạn cần và thiết kế kiến trúc của mình để tự động đáp ứng nhu cầu thay đổi bằng cách mở rộng hoặc thu nhỏ. Do đó, bạn chỉ trả tiền cho những tài nguyên bạn sử dụng. Bạn không phải lo lắng về việc thiếu khả năng tính toán để đáp ứng nhu cầu của khách hàng.

Nếu muốn quá trình thay đổi quy mô diễn ra tự động, bạn sẽ sử dụng dịch vụ AWS nào?

Dịch vụ AWS cung cấp chức năng này cho phiên bản Amazon EC2 là **Amazon EC2 Auto Scaling**.

### Amazon EC2 Auto Scaling

Nếu bạn đã cố gắng truy cập một trang web không tải và thường xuyên bị hết thời gian chờ, trang web đó có thể đã nhận được nhiều yêu cầu hơn mức nó có thể xử lý. Tình huống này tương tự như việc xếp hàng dài chờ đợi ở quán cà phê, khi chỉ có một nhân viên pha chế có mặt để nhận đơn đặt hàng từ khách hàng.



Amazon EC2 Auto Scaling cho phép bạn tự động thêm hoặc xóa phiên bản Amazon EC2 để đáp ứng nhu cầu thay đổi của ứng dụng. Bằng cách tự động mở rộng quy mô phiên bản của bạn khi cần, bạn có thể duy trì cảm giác sẵn sàng hơn về ứng dụng.

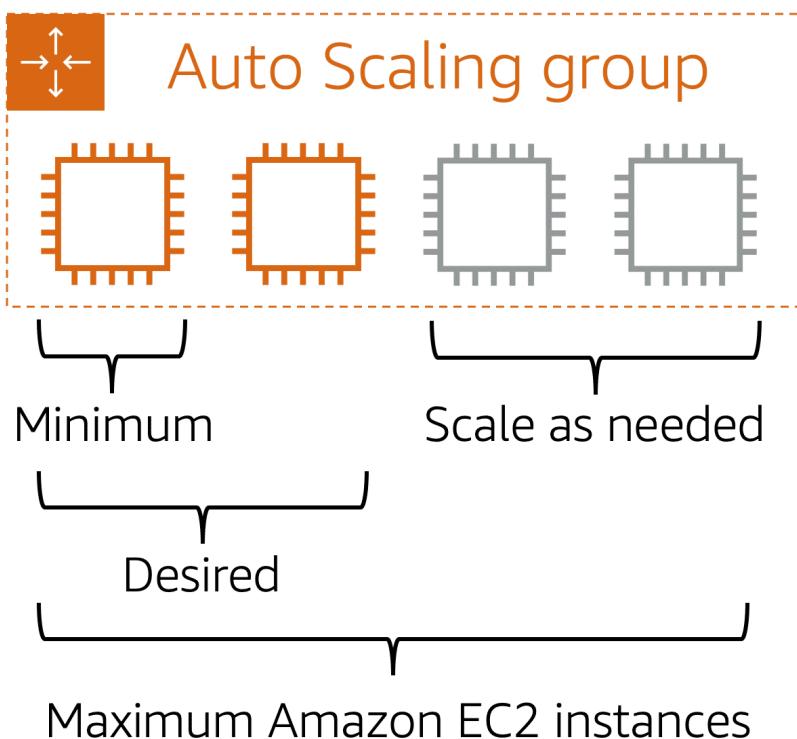
Trong Amazon EC2 Auto Scaling, bạn có thể sử dụng hai phương pháp: chia tỷ lệ động và chia tỷ lệ dự đoán.

- *Quy mô động* đáp ứng nhu cầu thay đổi.
- *Quy mô dự đoán* tự động lên lịch đúng số lượng phiên bản Amazon EC2 dựa trên nhu cầu dự đoán.

## Mở rộng quy mô Amazon EC2 (Phần 2)

Trong đám mây, sức mạnh tính toán là tài nguyên được lập trình, do đó bạn có thể áp dụng cách tiếp cận linh hoạt hơn đối với vấn đề mở rộng quy mô. Bằng cách thêm Amazon EC2 Auto Scaling vào ứng dụng, bạn có thể thêm phiên bản mới vào ứng dụng khi cần thiết và chấm dứt chúng khi không còn cần thiết nữa.

Giả sử bạn đang chuẩn bị khởi chạy một ứng dụng trên phiên bản Amazon EC2. Khi định cấu hình kích thước của nhóm Auto Scaling, bạn có thể đặt số lượng phiên bản Amazon EC2 tối thiểu tại một. Điều này có nghĩa là luôn phải có ít nhất một phiên bản Amazon EC2 đang chạy.



Khi tạo nhóm Auto Scaling, bạn có thể đặt số lượng phiên bản Amazon EC2 tối thiểu. Dung **minimum capacity (lượng tối thiểu)** là số phiên bản Amazon EC2 khởi chạy ngay sau khi bạn tạo nhóm Auto Scaling. Trong ví dụ này, nhóm Auto Scaling có dung lượng tối thiểu là một phiên bản Amazon EC2.

Tiếp theo, bạn có thể đặt **desired capacity(công suất mong muốn)** ở hai phiên bản Amazon EC2 ngay cả khi ứng dụng của bạn cần tối thiểu một phiên bản Amazon EC2 để chạy.

**Lưu ý :** Nếu bạn không chỉ định số lượng phiên bản Amazon EC2 mong muốn trong nhóm Auto Scaling thì dung lượng mong muốn sẽ mặc định là dung lượng tối thiểu của bạn.

Cấu hình thứ ba mà bạn có thể thiết lập trong nhóm Auto Scaling là **maximum capacity(dung lượng tối đa)** . Ví dụ: bạn có thể định cấu hình nhóm Auto Scaling để mở rộng quy mô nhằm đáp ứng nhu cầu ngày càng tăng, nhưng chỉ với tối đa bốn phiên bản Amazon EC2.

Vì Amazon EC2 Auto Scaling sử dụng phiên bản Amazon EC2 nên bạn chỉ phải trả phí cho phiên bản bạn sử dụng khi bạn sử dụng chúng. Bây giờ bạn có một kiến trúc tiết kiệm chi phí, mang lại trải nghiệm tốt nhất cho khách hàng đồng thời giảm chi phí.

## Elastic Load Balancer

Chúng tôi đã giải quyết vấn đề mở rộng quy mô với khả năng tự động thay đổi quy mô của Amazon EC2.Nhưng bây giờ chúng ta đang gặp chút vấn đề về giao thông phải không?Chúng ta hãy nhìn vào tình hình.Khi khách hàng bước vào quán cà phê,ngay bây giờ họ cóba lựa chọn để nhân viên thu ngân nói chuyện,để đặt hàng, và thật kỳ lạ,hầu hết họ đang xếp hàng thành một hàng,gây ra sự phân bổ khách hàng không đồng đều trên mỗi tuyến.Mặc dù chúng tôi có nhân viên thu ngân khác chờ nhận lệnh,đứng xung quanh không làm gì cả.Khách hàng đến và không chắc chắn chính xác nơi để định tuyến đơn đặt hàng của họ,sẽ giúp ích rất nhiều nếu chúng ta thêm một máy chủ vào tình huống này.Một người chủ nhà đứng ở cửa và khi khách hàng bước vào quán cà phê, họ bảo họ nên đi dòng nào tiến hành đặt hàng của họ.Chủ nhà để mắt đến nhân viên thu ngân gọi món và đếm số người xếp hàng,mỗi nhân viên thu ngân đang phục vụ.Sau đó nó sẽ hướng khách hàng mới đến quầy thu ngân có đường ngắn nhất là ít bị sa lầy nhất.Do đó cho phép các dòng được đồng đều trên nhân viên thu ngân và hỗ trợ khách hàng được phục vụ một cách hiệu quả nhất có thể.Ý tưởng tương tự cũng áp dụng cho môi trường AWS của bạn.Khi bạn có nhiều phiên bản EC2 tất cả đều chạy các chương trình giống nhau đều phục vụ cùng một mục đích,và một yêu cầu xuất hiện,làm thế nào để yêu cầu đó biết nên chuyển đến phiên bản EC2 nào?Làm thế nào bạn có thể đảm bảo có phân bổ đồng đều khối lượng công việc trên các phiên bản EC2.Không chỉ một

cái được sao lưu trong khinhững người khác thì nhàn rỗi, ngồi bên cạnh.Bạn cần một cách để định tuyến các yêu cầu đến trờng hợp để xử lý yêu cầu đó.Những gì bạn cần để giải quyết vấn đề này được gọi là cân bằng tải.Cân bằng tải là một ứng dụng tiếp nhận các yêu cầu và định tuyến chúng đến các trờng hợp cần xử lý.Hiện nay có rất nhiều bộ cân bằng tải sẵn có hoạt động tốt trên AWS.Nếu bạn có một hương vị yêu thích nó đã thực hiện chính xác những gì bạn muốn, thì hãy yên tâm tiếp tục sử dụng nó.Trong trờng hợp đó, nó sẽ tùy thuộc vào nhóm vận hành của bạn sẽ cài đặt, quản lý, cập nhật, mở rộng quy mô, xử lý chuyển đổi dự phòng và tính khả dụng.Điều đó có thể thực hiện được, rất có thể là những gì bạn thực sự làm được nhu cầu chỉ là phân phối hợp lý giao thông ở hiệu suất cao, chi phí hiệu quả, có tính sẵn sàng cao, hệ thống có khả năng mở rộng tự động bạn chỉ có thể thiết lập và quên đi.Giới thiệu cân bằng tải đàn hồi.Cân bằng tải đàn hồi, hoặc ELB, là một trong những dịch vụ được quản lý lớn đầu tiên chúng ta sẽ nói về trong khóa học này.Nó được thiết kế để giải quyết việc cân bằng tải nặng nề không phân biệt được

## READING

**Cân bằng tải đàn hồi** là dịch vụ AWS tự động phân phối lưu lượng ứng dụng đến trên nhiều tài nguyên, chẳng hạn như phiên bản Amazon EC2.

Bộ cân bằng tải hoạt động như một điểm liên lạc duy nhất cho tất cả lưu lượng truy cập web đến nhóm Tự động chia tỷ lệ của bạn. Điều này có nghĩa là khi bạn thêm hoặc xóa phiên bản Amazon EC2 theo lượng lưu lượng truy cập đến, những yêu cầu này sẽ định tuyến đến bộ cân bằng tải trước tiên. Sau đó, các yêu cầu sẽ trải rộng trên nhiều tài nguyên sẽ xử lý chúng. Ví dụ: nếu bạn có nhiều phiên bản Amazon EC2, Cân bằng tải đàn hồi sẽ phân phối khối lượng công việc trên nhiều phiên bản để không một phiên bản nào phải gánh phần lớn khối lượng công việc đó.

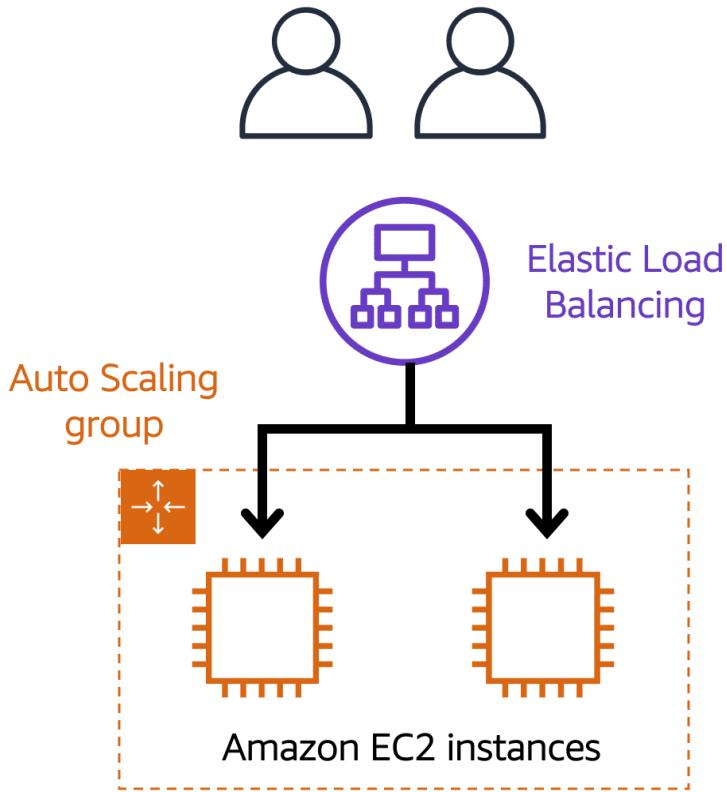
Mặc dù Elastic Load Balancing và Amazon EC2 Auto Scaling là các dịch vụ riêng biệt nhưng chúng phối hợp với nhau để giúp đảm bảo rằng các ứng dụng chạy trong Amazon EC2 có thể mang lại hiệu năng và độ khả dụng cao.

### Ví dụ: Cân bằng tải đàn hồi

#### Low-demand period

Đây là ví dụ về cách hoạt động của Cân bằng tải đàn hồi. Giả sử có một số khách hàng đã đến quán cà phê và sẵn sàng gọi món.

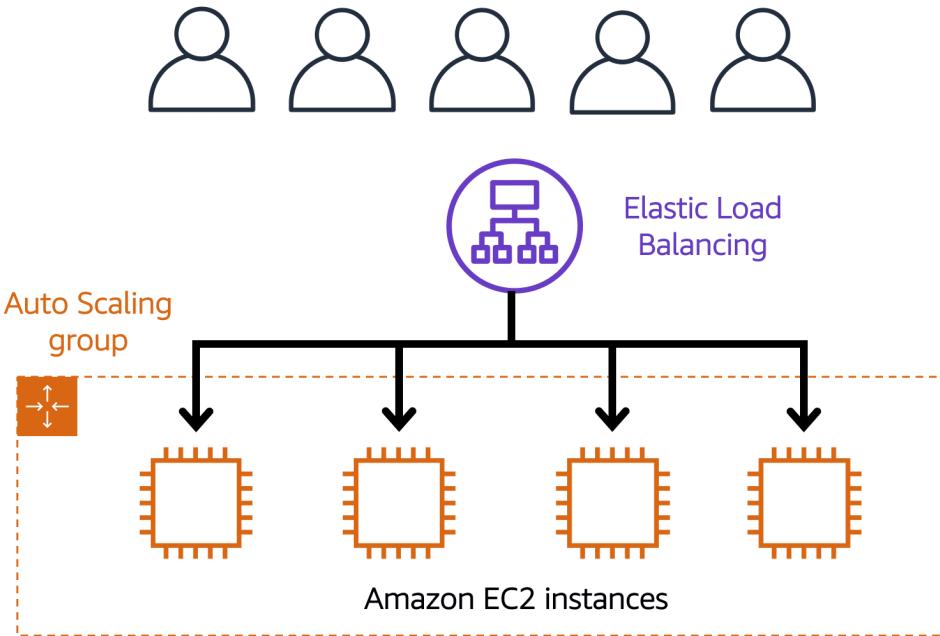
Nếu chỉ mở một số sổ đăng ký thì phù hợp với nhu cầu của khách hàng có nhu cầu sử dụng dịch vụ. Quán cà phê ít có khả năng có quầy đăng ký mở mà không có khách hàng. Trong ví dụ này, bạn có thể coi các thanh ghi là phiên bản Amazon EC2.



### High-demand period

Trong ngày, khi số lượng khách hàng tăng lên, quán cà phê sẽ mở thêm quầy đăng ký để phục vụ họ. Trong sơ đồ, nhóm Auto Scaling thể hiện điều này.

Ngoài ra, nhân viên quán cà phê sẽ hướng dẫn khách hàng đến sổ đăng ký phù hợp nhất để số lượng yêu cầu có thể phân bổ đều trên các sổ đăng ký đang mở. Bạn có thể coi nhân viên quán cà phê này như một người cân bằng tải.



## Messaging and Queueing

Đặc điểm nổi bật của kiến trúc liên kết chặt chẽ là nếu một thành phần đơn lẻ bị lỗi hoặc thay đổi, nó sẽ gây ra sự cố cho các thành phần khác hoặc thậm chí toàn bộ hệ thống. Phát video bắt đầu từ và theo dõi bản ghi. Ví dụ: nếu chúng ta có ứng dụng A và nó đang gửi tin nhắn trực tiếp đến ứng dụng B. Nếu ứng dụng B gặp lỗi và không thể chấp nhận những tin nhắn đó, ứng dụng A cũng sẽ bắt đầu gặp lỗi. Đây là một kiến trúc liên kết chặt chẽ. Một kiến trúc đáng tin cậy hơn được kết hợp lỏng lẻo. Đây là kiến trúc mà nếu một thành phần bị lỗi, nó sẽ bị cô lập và do đó sẽ không gây ra lỗi liên tục trên toàn bộ hệ thống. Nếu chúng tôi mã hóa ứng dụng để sử dụng kiến trúc được liên kết lỏng lẻo hơn, thì nó có thể trông như sau, giống như nhân viên thu ngân và nhân viên pha chế của chúng tôi, chúng tôi đã giới thiệu một vùng đệm giữa hai người.

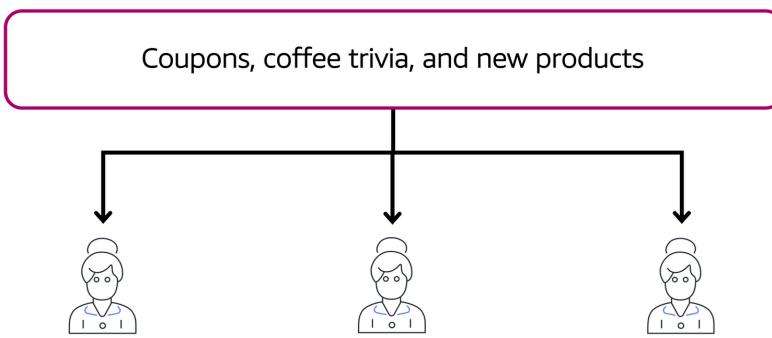
Trong trường hợp này, chúng tôi đã giới thiệu một hàng đợi tin nhắn, các tin nhắn sẽ được ứng dụng A đưa vào hàng đợi và chúng được ứng dụng B xử lý. Nếu ứng dụng B bị lỗi, ứng dụng A sẽ không gặp bất kỳ sự gián đoạn nào. Tin nhắn đang được gửi vẫn có thể được gửi đến hàng đợi và sẽ ở đó cho đến khi chúng được xử lý cuối cùng. Điều này được kết nối lỏng lẻo. Đây là điều chúng tôi cố gắng đạt được với kiến trúc trên AWS. Và điều này đưa tôi đến với hai dịch vụ AWS có thể hỗ trợ về mặt này.

# Amazon Simple Notification Service (Amazon SNS)

**Dịch vụ thông báo đơn giản của Amazon (Amazon SNS)** là dịch vụ publish(xuất bản)/subscribe(đăng ký). Bằng cách sử dụng các chủ đề của Amazon SNS,publisher sẽ xuất bản tin nhắn tới subscribers. Điều này tương tự như quán cà phê; nhân viên thu ngân cung cấp đơn đặt hàng cà phê cho nhân viên pha chế đồ uống.

Trong Amazon SNS, người đăng ký có thể là máy chủ web, địa chỉ email, chức năng AWS Lambda hoặc một số tùy chọn khác.

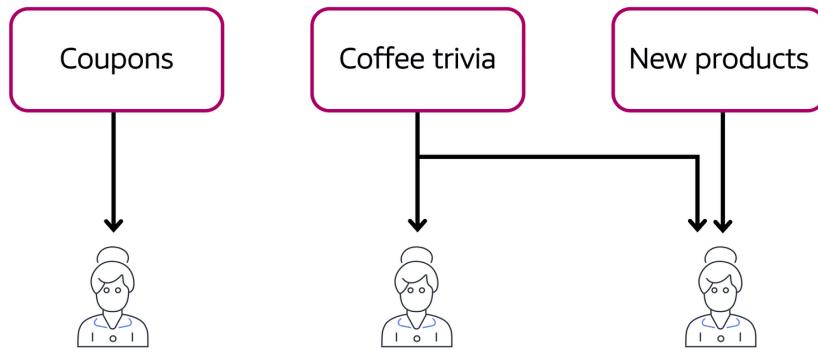
## Xuất bản cập nhật từ một chủ đề duy nhất



Giả sử quán cà phê có một bản tin duy nhất bao gồm các thông tin cập nhật từ tất cả các lĩnh vực kinh doanh của mình. Nó bao gồm các chủ đề như phiếu giảm giá, câu đố về cà phê và các sản phẩm mới. Tất cả các chủ đề này được nhóm lại vì đây là một bản tin duy nhất. Tất cả khách hàng đăng ký nhận bản tin đều nhận được thông tin cập nhật về phiếu giảm giá, câu đố về cà phê và các sản phẩm mới.

Sau một thời gian, một số khách hàng bày tỏ rằng họ muốn nhận các bản tin riêng biệt chỉ về những chủ đề cụ thể mà họ quan tâm. Các chủ quán cà phê quyết định thử phương pháp này.

## Xuất bản cập nhật từ nhiều chủ đề



Giờ đây, thay vì có một bản tin duy nhất cho tất cả các chủ đề, quán cà phê đã chia nó thành ba bản tin riêng biệt. Mỗi bản tin được dành cho một chủ đề cụ thể: phiếu giảm giá, câu đố về cà phê và các sản phẩm mới.

Người đăng ký giờ đây sẽ chỉ nhận được thông tin cập nhật ngay lập tức về những chủ đề cụ thể mà họ đã đăng ký.

Người đăng ký có thể đăng ký một chủ đề hoặc nhiều chủ đề. Ví dụ: khách hàng đầu tiên chỉ đăng ký chủ đề phiếu giảm giá và người đăng ký thứ hai chỉ đăng ký chủ đề đồ vui về cà phê. Khách hàng thứ ba đăng ký cả chủ đề về cà phê và sản phẩm mới.

## Amazon Simple Queue Service (Amazon SQS)

**Amazon Simple Queue Service (Amazon SQS)** là dịch vụ xếp hàng tin nhắn.

Khi sử dụng Amazon SQS, bạn có thể gửi, lưu trữ và nhận tin nhắn giữa các thành phần phần mềm mà không làm mất tin nhắn hoặc yêu cầu phải có sẵn các dịch vụ khác.

Trong Amazon SQS, một ứng dụng sẽ gửi tin nhắn vào hàng đợi. Người dùng hoặc dịch vụ lấy một tin nhắn từ hàng đợi, xử lý nó và sau đó xóa nó khỏi hàng đợi.

### Ví dụ: Thực hiện đơn hàng

Giả sử quán cà phê có quy trình gọi món, trong đó nhân viên thu ngân nhận đơn hàng và nhân viên pha chế thực hiện đơn hàng. Hãy coi nhân viên thu ngân và nhân viên pha chế là hai thành phần riêng biệt của một ứng dụng.

Đầu tiên, nhân viên thu ngân nhận đơn đặt hàng và viết nó ra một tờ giấy. Tiếp theo, nhân viên thu ngân giao giấy cho nhân viên pha chế. Cuối cùng, nhân viên pha chế pha chế đồ uống và đưa cho khách hàng.

Khi có đơn hàng tiếp theo, quá trình này lặp lại. Quá trình này diễn ra suôn sẻ miễn là cả nhân viên thu ngân và nhân viên pha chế đều phối hợp với nhau.

Điều gì có thể xảy ra nếu nhân viên thu ngân nhận đơn đặt hàng và đi giao cho nhân viên pha chế, nhưng nhân viên pha chế đang nghỉ giải lao hoặc đang bận với một đơn hàng khác? Nhân viên thu ngân sẽ phải đợi cho đến khi nhân viên pha chế sẵn sàng chấp nhận đơn hàng. Điều này sẽ gây ra sự chậm trễ trong quá trình đặt hàng và buộc khách hàng phải chờ lâu hơn để nhận được đơn hàng.

Khi quán cà phê trở nên phổ biến hơn và dòng người xếp hàng di chuyển chậm hơn, các chủ quán nhận thấy rằng quy trình đặt hàng hiện tại rất tốn thời gian và không hiệu quả. Họ quyết định thử một cách tiếp cận khác sử dụng hàng đợi.

### **Ví dụ: Đơn đặt hàng trong hàng đợi**

Hãy nhớ lại rằng nhân viên thu ngân và nhân viên pha chế là hai thành phần riêng biệt của một ứng dụng.

Dịch vụ xếp hàng tin nhắn như Amazon SQS cho phép gửi tin nhắn giữa các thành phần ứng dụng được tách rời.

Trong ví dụ này, bước đầu tiên của quy trình vẫn giống như trước: khách hàng đặt hàng với nhân viên thu ngân.

Nhân viên thu ngân xếp đơn hàng vào hàng đợi. Bạn có thể coi đây như một bảng đặt hàng đóng vai trò là vùng đệm giữa nhân viên thu ngân và nhân viên pha chế. Ngay cả khi nhân viên pha chế ra ngoài trong giờ giải lao hoặc bận rộn với một đơn hàng khác, nhân viên thu ngân vẫn có thể tiếp tục đặt các đơn hàng mới vào hàng đợi.

Tiếp theo, nhân viên pha chế kiểm tra hàng đợi và lấy đơn hàng.

Barista chuẩn bị đồ uống và đưa cho khách hàng.

Sau đó, nhân viên pha chế sẽ xóa đơn hàng đã hoàn thành khỏi hàng đợi.

Trong khi nhân viên pha chế đang chuẩn bị đồ uống, nhân viên thu ngân có thể tiếp tục nhận đơn đặt hàng mới và thêm chúng vào hàng đợi.

## **Additional Compute Services**

EC2 yêu cầu bạn thiết lập và quản lý nhóm phiên bản của bạn theo thời gian. Khi bạn đang sử dụng EC2, bạn có trách nhiệm và phiên bản của bạn khi gói phần mềm mới xuất hiện, thiết lập quy mô của các Trường hợp đó, cũng như đảm bảo rằng bạn đã kiến trúc các giải pháp của bạn sẽ được lưu trữ theo cách có tính khả dụng cao. Đây vẫn chưa phải là cách quản lý nhiều như bạn mong muốn có nếu bạn lưu trữ những thứ này tại chỗ. Nhưng các quy trình quản lý vẫn sẽ cần phải được thực hiện. Có thể bạn đang thắc

mắc,AWS cung cấp những dịch vụ nào khác cho điện toán, thuận tiện hơn từ góc độ quản lý? Đây là lúc thuật ngữ serverless xuất hiện.AWS cung cấp nhiều tùy chọn điện toán serverless.Serverless có nghĩa là bạn thực sự không thể xem hoặc truy cập cơ sở hạ tầng cơ bản,hoặc Phiên bản đang lưu trữ ứng dụng của bạn.Thay vào đó, mọi hoạt động quản lý của môi trường cơ bản từ việc cung cấp,quản điểm mở rộng quy mô,tính sẵn sàng cao và bảo trì,được chăm sóc cho bạn.Tất cả những gì bạn cần làm là tập trung vào ứng dụng của mình,và phần còn lại được chăm sóc. AWS Lambda là một tùy chọn điện toán serverless.Lambda là một dịch vụ cho phép bạn tải lên mã của bạn thành cái được gọi là hàm Lambda.Định cấu hình trình kích hoạt và từ đó,dịch vụ chờ kích hoạt.Khi kích hoạt được phát hiện,mã được tự động chạy trong môi trường được quản lý.Một môi trường mà bạn không cần phải lo lắng quá nhiều,bởi vì nó có khả năng mở rộng tự động,tính sẵn sàng cao,và tất cả việc duy trì môi trường chính nó được thực hiện bởi AWS.Nếu bạn có một hoặc 1.000 trình kích hoạt đến,Lambda sẽ mở rộng chức năng của bạn để đáp ứng nhu cầu.Lambda được thiết kế để chạy mã dưới 15 phút.Điều này không dành cho các quá trình chạy dài như học sâu.Nó phù hợp hơn để xử lý nhanh,giống như các yêu cầu xử lý back-end trên web,hoặc dịch vụ xử lý báo cáo chi phí phụ trợ,mỗi lần gọi sẽ diễn ra ở đâu chưa đầy 15 phút là xong.Nếu bạn chưa hoàn toàn sẵn sàng cho serverless,hoặc bạn cần quyền truy cập vào môi trường cơ bản,nhưng vẫn muốn tính hiệu quả và tính di động,bạn nên xem xét các dịch vụ container AWS,như [Amazon Elastic Container Service](#)**(Dịch vụ container đàn hồi của Amazon)**,còn được gọi là **ECS**,hoặc **Dịch vụ Kubernetes** đàn hồi của Amazon,còn được gọi là **EKS**.Cả hai dịch vụ này đều là công cụ điều phối vùng chứa.Nhưng trước khi tôi đi quá xa ở đây,một container,trong trường hợp này,là một vùng chứa Docker.Docker là một nền tảng được sử dụng rộng rãi,sử dụng ảo hóa cấp hệ điều hành để phân phối phần mềm trong các thùng chứa.Bây giờ,vùng chứa là một gói dành cho mã của bạn,nơi bạn đóng gói ứng dụng của mình,đó cũng là sự phụ thuộc như bất kỳ cấu hình nào nó cần để chạy.Các vùng chứa này chạy trên Phiên bản EC2,và chạy tách biệt với nhau.Tương tự như cách hoạt động của máy ảo.Nhưng trong trường hợp này,máy chủ là Phiên bản EC2.Khi bạn sử dụng bộ chứa Docker trên AWS,bạn cần các quy trình để bắt đầu, dừng, khởi động lại,và giám sát các container chạy ngang quanh không chỉ một Phiên bản EC2,nhưng một số trong số chúng cùng nhau,được gọi là một cụm.Quá trình thực hiện các công việc này được gọi là điều phối container.Hóa ra, thật khó để tự mình làm được.Công cụ điều phối đã được tạo để giúp bạn quản lý vùng chứa của mình.ECS được thiết kế để giúp bạn chạy các ứng dụng được chứa trong container của bạn trên quy mô lớn,không gặp rắc rối trong việc quản lý phần mềm điều phối vùng chứa của riêng bạn.EKS cũng làm điều tương tự,nhưng sử dụng các công cụ khác nhau và có các tính

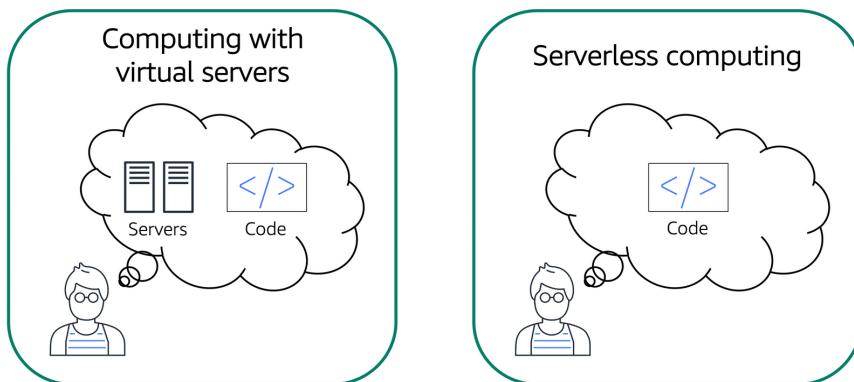
năng khác nhau.Cả Amazon ECS và Amazon EKS đều có thể chạy trên EC2.Nhưng nếu bạn thậm chí không muốn nghĩ về việc sử dụng EC2 để lưu trữ vùng chứa của bạn,bởi vì bạn không cần truy cập vào hệ điều hành cơ bản,hoặc bạn không muốn quản lý các Phiên bản EC2 đó,bạn có thể sử dụng nền tảng điện toán có tên **AWS Fargate**.Fargate là nền tảng điện toán serverless dành cho ECS hoặc EKS.Trình độ hơi cao đấy và nó có thể gây nhầm lẫn.

Nếu bạn đang cố gắng lưu trữ các ứng dụng truyền thống,và muốn có toàn quyền truy cập vào hệ điều hành cơ bản,như Linux hay Windows,bạn sẽ muốn sử dụng EC2.Nếu bạn đang muốn lưu trữ các chức năng chạy ngắn,các ứng dụng hướng dịch vụ hoặc hướng sự kiện,và bạn không muốn quản lý môi trường cơ bản chút nào,hãy xem xét AWS Lambda không có máy chủ.Nếu bạn đang muốn chạy Khối lượng công việc dựa trên bộ chứa Docker trên AWS,trước tiên bạn cần chọn công cụ điều phối của mình.Bạn muốn sử dụng Amazon ECS hay Amazon EKS?Sau khi bạn chọn công cụ của mình,sau đó bạn cần chọn nền tảng của mình.Bạn có muốn chạy container của mình trên Phiên bản EC2 mà bạn quản lý,hoặc trong môi trường không có máy chủ như AWS Fargate,được quản lý cho bạn?

## Serverless Computing

Trước đó trong mô-đun này, bạn đã tìm hiểu về Amazon EC2, một dịch vụ cho phép bạn chạy các máy chủ ảo trên đám mây. Nếu bạn có ứng dụng muốn chạy trên Amazon EC2, bạn phải làm như sau:

1. Các instances cung cấp (máy chủ ảo).
2. Tải lên mã của bạn.
3. Tiếp tục quản lý các phiên bản trong khi ứng dụng của bạn đang chạy.



Thuật ngữ serverless “không có máy chủ” có nghĩa là mã của bạn chạy trên máy chủ nhưng bạn không cần cung cấp hoặc quản lý các máy chủ này. Với điện toán không có

máy chủ, bạn có thể tập trung nhiều hơn vào việc đổi mới các sản phẩm và tính năng mới thay vì bảo trì máy chủ.

Một lợi ích khác của điện toán serverless là tính linh hoạt trong việc tự động mở rộng quy mô ứng dụng serverless. Điện toán phi máy chủ có thể điều chỉnh công suất của ứng dụng bằng cách sửa đổi đơn vị tiêu thụ, chẳng hạn như thông lượng và bộ nhớ. Dịch vụ AWS dành cho điện toán không có máy chủ là **AWS Lambda**.

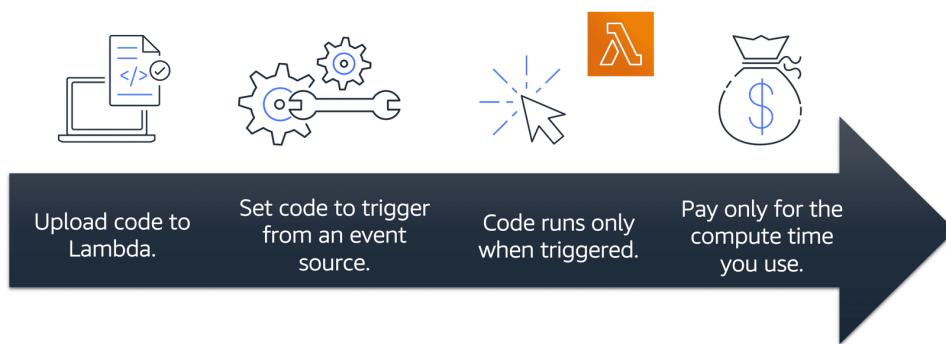
## AWS Lambda

**AWS Lambda** là dịch vụ cho phép bạn chạy mã mà không cần cung cấp quản lý máy chủ.

Khi sử dụng AWS Lambda, bạn chỉ phải trả phí cho thời gian tính toán mà bạn sử dụng. Phí chỉ áp dụng khi mã của bạn đang chạy. Bạn cũng có thể chạy mã cho hầu hết mọi loại ứng dụng hoặc dịch vụ phụ trợ mà không cần quản trị.

Ví dụ: một hàm Lambda đơn giản có thể liên quan đến việc tự động thay đổi kích thước hình ảnh đã tải lên đám mây AWS. Trong trường hợp này, chức năng sẽ kích hoạt khi tải hình ảnh mới lên.

## Cách thức hoạt động của AWS Lambda



1. Bạn tải mã của mình lên Lambda.
2. Bạn đặt mã của mình để kích hoạt từ nguồn sự kiện, chẳng hạn như dịch vụ AWS, ứng dụng di động hoặc điểm cuối HTTP.
3. Lambda chỉ chạy mã của bạn khi được kích hoạt.
4. Bạn chỉ trả tiền cho thời gian tính toán mà bạn sử dụng. Trong ví dụ trước về thay đổi kích thước hình ảnh, bạn sẽ chỉ trả tiền cho thời gian tính toán mà bạn sử dụng khi tải hình ảnh mới lên. Việc tải hình ảnh lên sẽ kích hoạt Lambda chạy mã cho chức năng thay đổi kích thước hình ảnh.

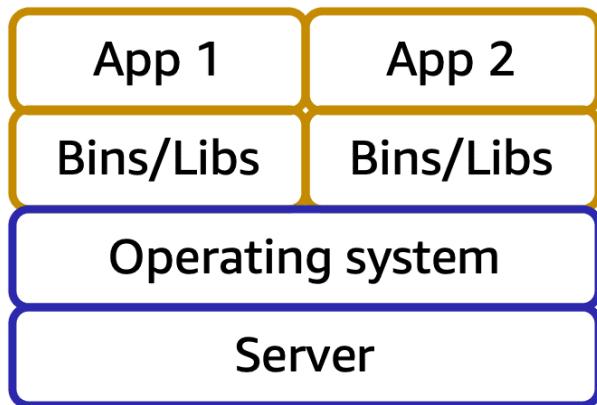
## Containers

Trong AWS, bạn cũng có thể xây dựng và chạy các ứng dụng **được đóng gói trong bộ chứa**.

**Bộ chứa** cung cấp cho bạn một cách tiêu chuẩn để đóng gói mã và các phần phụ thuộc của ứng dụng vào một đối tượng duy nhất. Bạn cũng có thể sử dụng vùng chứa cho các quy trình và quy trình làm việc trong đó có các yêu cầu thiết yếu về bảo mật, độ tin cậy và khả năng mở rộng.

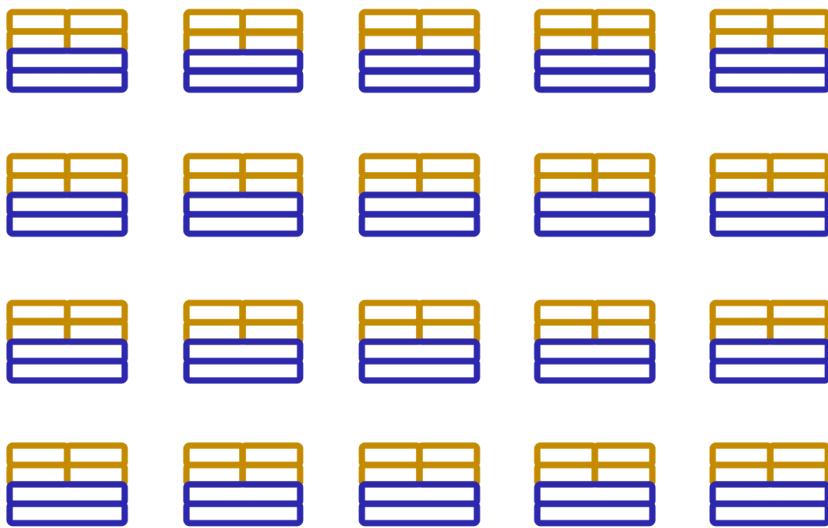
Ví dụ:

### Một máy chủ có nhiều container



Giả sử rằng nhà phát triển ứng dụng của công ty có môi trường trên máy tính của họ khác với môi trường trên máy tính được nhân viên vận hành CNTT sử dụng. Nhà phát triển muốn đảm bảo rằng môi trường của ứng dụng vẫn nhất quán bất kể việc triển khai, vì vậy họ sử dụng phương pháp tiếp cận được chứa trong vùng chứa. Điều này giúp giảm thời gian gỡ lỗi ứng dụng và chẩn đoán sự khác biệt trong môi trường máy tính.

### Hàng chục máy chủ với hàng trăm container



Khi chạy các ứng dụng được đóng gói, điều quan trọng là phải xem xét khả năng mở rộng. Giả sử thay vì một máy chủ có nhiều vùng chứa, bạn phải quản lý hàng chục máy chủ với hàng trăm vùng chứa. Ngoài ra, bạn phải quản lý hàng trăm máy chủ với hàng nghìn container. Ở quy mô lớn, hãy tưởng tượng bạn sẽ mất bao nhiêu thời gian để theo dõi việc sử dụng bộ nhớ, bảo mật, ghi nhật ký, v.v.

### **Amazon Elastic Container Service (Amazon ECS)**

**Dịch vụ container đàn hồi của Amazon (Amazon ECS) là một hệ thống quản lý bộ chứa hiệu suất cao, có khả năng mở rộng cao, cho phép bạn chạy và mở rộng quy mô các ứng dụng được chứa trong bộ chứa trên AWS.** Amazon ECS hỗ trợ bộ chứa Docker. [Docker](#) là một nền tảng phần mềm cho phép bạn xây dựng, thử nghiệm và triển khai các ứng dụng một cách nhanh chóng. AWS hỗ trợ sử dụng Docker Community Edition nguồn mở và Docker Enterprise Edition dựa trên đăng ký. Với Amazon ECS, bạn có thể sử dụng lệnh gọi API để khởi chạy và dừng các ứng dụng hỗ trợ Docker.

## **Regions**

Để hiểu cơ sở hạ tầng toàn cầu AWS, tôi muốn bắt đầu từ nhu cầu kinh doanh cơ bản của bạn. Bạn có một ứng dụng phải chạy để tìm nội dung bạn cần lưu trữ hoặc dữ liệu

bạn cần phân tích. Về cơ bản, bạn có những thứ cần phải sống và hoạt động ở đâu đó. Trong lịch sử, các doanh nghiệp phải chạy ứng dụng trong trung tâm dữ liệu của riêng họ vì họ không có lựa chọn nào khác. Khi AWS có sẵn, các công ty như của bạn giờ đây có thể chạy ứng dụng của họ ở các trung tâm dữ liệu khác mà họ không thực sự sở hữu. Nhưng cuộc trò chuyện còn nhiều hơn thế. Bởi vì tôi muốn bạn hiểu một vấn đề cơ bản với bất kỳ trung tâm dữ liệu nào, bất kể ai xây dựng nó hay ai sở hữu nó. Các sự kiện có thể xảy ra khiến bạn mất kết nối với tòa nhà đó. Nếu bạn điều hành trung tâm dữ liệu của riêng mình, bạn phải tìm ra cách trả lời câu hỏi bạn sẽ làm gì khi thảm họa xảy ra với tòa nhà của bạn. Bạn có thể vận hành một trung tâm dữ liệu thứ hai, nhưng chỉ giá bất động sản thôi cũng có thể cản trở bạn, chưa nói đến tất cả các chi phí trùng lặp về phần cứng, nhân viên, điện, sưởi ấm và làm mát, an ninh. Hầu hết các doanh nghiệp chỉ đơn giản là lưu trữ các bản sao lưu ở đâu đó, rồi hy vọng thảm họa sẽ không bao giờ xảy ra và hy vọng đó không phải là một kế hoạch kinh doanh tốt. AWS trả lời câu hỏi điều gì sẽ xảy ra khi thảm họa xảy ra bằng cách xây dựng trung tâm dữ liệu của chúng tôi theo các nhóm lớn mà chúng tôi gọi là khu vực và đây là cách nó được thiết kế. Trên toàn cầu, AWS xây dựng các khu vực gần nhất với nhu cầu lưu lượng kinh doanh. Các địa điểm như Paris, Tokyo, San Paulo, Dublin, Ohio. Trong mỗi khu vực, chúng tôi có nhiều trung tâm dữ liệu có tất cả bộ lưu trữ điện toán và các dịch vụ khác mà bạn cần để chạy ứng dụng của mình. Mỗi vùng có thể được kết nối với nhau thông qua mạng cáp quang tốc độ cao do AWS kiểm soát. Một hoạt động toàn cầu thực sự từ góc này sang góc khác nếu bạn cần. Trước khi chúng ta đi vào kiến trúc về cách xây dựng từng khu vực, điều quan trọng cần biết là bạn, người ra quyết định kinh doanh, có quyền chọn khu vực mà bạn muốn loại bỏ. Và mỗi vùng đều bị cô lập với mọi vùng khác. Theo nghĩa là hoàn toàn không có dữ liệu nào đi vào hoặc ra khỏi môi trường của bạn trong khu vực đó mà không có sự cấp phép rõ ràng của bạn để di chuyển dữ liệu đó. Đây là một cuộc trò chuyện bảo mật quan trọng cần có. Ví dụ: bạn có thể có các yêu cầu tuân thủ của chính phủ rằng thông tin tài chính của bạn ở Frankfurt không thể rời khỏi Đức. Chà, đây hoàn toàn là cách AWS vận hành vượt trội mà mọi dữ liệu được lưu trữ ở khu vực Frankfurt sẽ không bao giờ rời khỏi khu vực Frankfurt. Hoặc dữ liệu ở khu vực Luân Đôn không bao giờ rời khỏi Luân Đôn hoặc Sydney không bao giờ rời khỏi Sydney, trừ khi bạn yêu cầu xuất dữ liệu một cách rõ ràng với thông tin xác thực và quyền phù hợp. Chủ quyền dữ liệu khu vực là một phần trong thiết kế quan trọng của các khu vực AWS với dữ liệu phải tuân theo luật pháp và quy chế địa phương của quốc gia nơi khu vực đó sinh sống. Vì vậy, với sự hiểu biết rằng dữ liệu mà ứng dụng của bạn tồn tại và chạy trong một khu vực, một trong những quyết định đầu tiên bạn phải đưa ra là bạn chọn khu vực nào? Có bốn yếu tố kinh doanh ảnh hưởng đến việc lựa chọn khu vực, số một là

sự tuân thủ. Trước bất kỳ yếu tố nào khác, trước tiên bạn phải xem xét các yêu cầu tuân thủ của mình. Bạn có yêu cầu không? Dữ liệu của bạn phải nằm trong ranh giới của Vương quốc Anh. Vậy thì bạn nên chọn khu vực London, chấm hết. Ý tôi là, không có lựa chọn nào còn lại quan trọng cả. Hoặc, giả sử bạn phải chạy trong biên giới Trung Quốc, thì bạn nên chọn một trong các khu vực Trung Quốc của chúng tôi. Tuy nhiên, hầu hết các doanh nghiệp không bị chi phối bởi những quy định nghiêm ngặt như vậy. Vì vậy, nếu bạn không có biện pháp kiểm soát tuân thủ hoặc quản lý quy định khu vực của mình thì bạn có thể xem xét các yếu tố khác. Số 2, sự gần gũi. Mức độ gần gũi của bạn với cơ sở khách hàng là yếu tố chính vì tốc độ ánh sáng vẫn là quy luật của vũ trụ. Nếu hầu hết khách hàng của bạn sống ở Singapore, hãy cân nhắc việc rời khỏi khu vực Singapore. Bạn chắc chắn có thể chạy ra khỏi Virginia. Nhưng thời gian để gửi thông tin hoặc độ trễ giữa Mỹ và Singapore luôn là một yếu tố. Nay giờ chúng ta có thể đang phát triển điện toán lượng tử nhưng mạng lượng tử vẫn còn một chặng đường dài. Thời gian ánh sáng cần để đi vòng quanh thế giới luôn là vấn đề cần cân nhắc. Định vị gần cơ sở khách hàng của bạn, thường là cuộc gọi phù hợp. Thứ ba, tính khả dụng. Đôi khi khu vực gần nhất có thể không có tất cả các tính năng AWS mà bạn mong muốn. Đây là một trong những điều thú vị về AWS. Chúng tôi không ngừng đổi mới thay mặt cho khách hàng của mình. Mỗi năm AWS phát hành hàng nghìn tính năng và sản phẩm mới nhằm đáp ứng yêu cầu và nhu cầu của khách hàng. Nhưng đôi khi những dịch vụ hoàn toàn mới đó cần rất nhiều phần cứng vật lý mới mà AWS phải xây dựng để dịch vụ có thể hoạt động. Và đôi khi điều đó có nghĩa là chúng tôi phải xây dựng dịch vụ cho từng khu vực một. Vì vậy, giả sử nhà phát triển của bạn muốn chơi với Amazon, nền tảng điện toán lượng tử mới của chúng tôi. Chà, vậy thì chúng phải chạy ở những khu vực đã cài đặt phần cứng rồi, liệu chúng ta có thể mong đợi nó sẽ có ở mọi khu vực không? Vâng, đó là một kỳ vọng tốt. Nhưng nếu bạn muốn sử dụng nó ngay hôm nay thì đó có thể là yếu tố quyết định của bạn. Số bốn, giá cả. Ngay cả khi phần cứng ở khu vực này tương đương với khu vực tiếp theo, thì một số địa điểm vẫn có chi phí hoạt động đắt hơn. Ví dụ: Brazil. Hiện nay, cơ cấu thuế của Brazil khiến chi phí của AWS để vận hành các dịch vụ tương tự ở đó cao hơn đáng kể so với nhiều quốc gia khác. Chẳng hạn, khối lượng công việc tương tự ở San Paulo có thể đắt hơn 50% khi chạy ở Oregon ở Hoa Kỳ. Giá có thể được xác định bởi nhiều yếu tố. Vì vậy, AWS có mức giá chi tiết rất minh bạch mà chúng ta sẽ tiếp tục thảo luận trong lớp này, nhưng hãy lưu ý rằng mỗi khu vực có một bảng giá khác nhau. Vì vậy, nếu ngân sách là mối quan tâm hàng đầu của bạn, ngay cả khi khách hàng của bạn sống ở Brazil, bạn vẫn có thể muốn hoạt động trở lại ở một quốc gia khác nếu giá cả là động lực chính của bạn.

# Selecting a Region

Khi xác định Khu vực phù hợp cho dịch vụ, dữ liệu và ứng dụng của bạn, hãy xem xét bốn yếu tố kinh doanh sau.

## **Compliance with data governance and legal requirements (Tuân thủ các yêu cầu pháp lý và quản trị dữ liệu)**

Tùy thuộc vào công ty và vị trí của bạn, bạn có thể cần chạy dữ liệu của mình ở các khu vực cụ thể. Ví dụ: nếu công ty của bạn yêu cầu tất cả dữ liệu của công ty nằm trong ranh giới của Vương quốc Anh, bạn sẽ chọn Khu vực Luân Đôn.

Không phải tất cả các công ty đều có quy định về dữ liệu theo vị trí cụ thể, vì vậy bạn có thể cần tập trung hơn vào ba yếu tố còn lại.

## **Proximity to your customers (Sự gần gũi với khách hàng của bạn)**

Việc chọn Khu vực gần với khách hàng của bạn sẽ giúp bạn đưa nội dung đến với họ nhanh hơn. Ví dụ: công ty của bạn có trụ sở tại Washington, DC và nhiều khách hàng của bạn sống ở Singapore. Bạn có thể cân nhắc việc vận hành cơ sở hạ tầng của mình ở Khu vực Bắc Virginia để gần trụ sở công ty và chạy các ứng dụng của bạn từ Khu vực Singapore.

## **Available services within a Region (Các dịch vụ có sẵn trong một Khu vực)**

Đôi khi, Khu vực gần nhất có thể không có tất cả các tính năng mà bạn muốn cung cấp cho khách hàng. AWS thường xuyên đổi mới bằng cách tạo ra các dịch vụ mới và mở rộng các tính năng trong các dịch vụ hiện có. Tuy nhiên, việc cung cấp các dịch vụ mới trên toàn thế giới đôi khi đòi hỏi AWS phải xây dựng phần cứng vật lý cho từng Khu vực tại một thời điểm.

Giả sử bạn đang xem xét việc chạy các ứng dụng sử dụng Amazon Braket (nền tảng điện toán lượng tử AWS). Theo khóa học này, Amazon Braket chưa có sẵn ở mọi Khu vực AWS trên toàn thế giới, vì vậy các nhà phát triển của bạn sẽ phải chạy nó ở một trong những Khu vực đã cung cấp dịch vụ này.

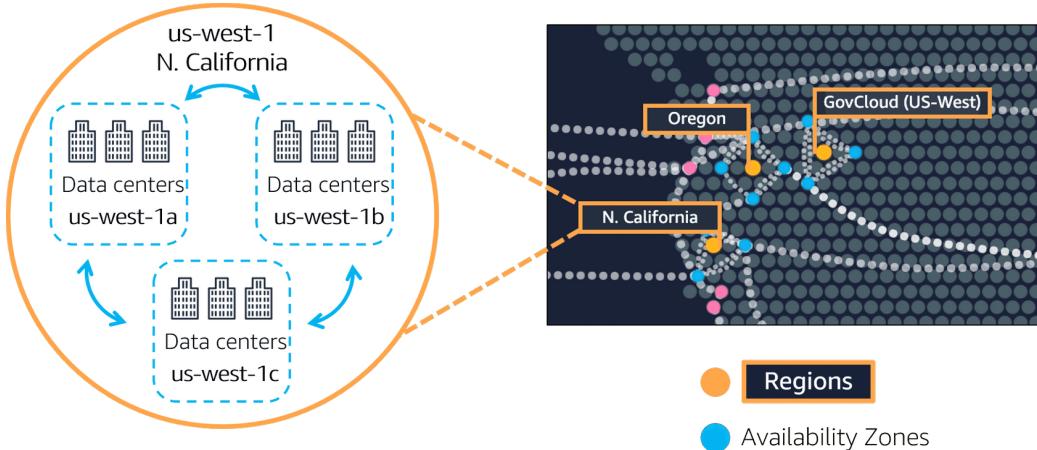
## **Pricing (Định giá)**

Giả sử bạn đang xem xét việc chạy các ứng dụng ở cả Hoa Kỳ và Brazil. Theo cách thiết lập cơ cấu thuế của Brazil, chi phí để vận hành cùng một khối lượng công việc ở Vùng São Paulo có thể cao hơn 50% so với Vùng Oregon. Bạn sẽ tìm hiểu chi tiết hơn rằng một số yếu tố quyết định giá cả, nhưng hiện tại hãy biết rằng chi phí dịch vụ có thể khác nhau tùy theo Khu vực.

# Availability Zones

Nếu một khu vực là nơi tải tất cả các phần và bộ phận của ứng dụng của bạn, một số bạn có thể nghĩ rằng chúng tôi chưa bao giờ thực sự giải quyết được vấn đề mà chúng tôi đã trình bày trong video trước. Hãy để tôi trình bày lại vấn đề. Bạn không muốn chạy ứng dụng của mình trong một tòa nhà vì một tòa nhà có thể bị lỗi vì bất kỳ lý do không thể tránh khỏi nào. Có thể bạn đang nghĩ, nếu doanh nghiệp của tôi cần chống chọi với thảm họa thì tôi không thể chỉ hoạt động ở một địa điểm. Vâng, bạn hoàn toàn đúng. AWS đồng ý với tuyên bố đó và đó là lý do tại sao các khu vực của chúng tôi không phải là một địa điểm. Để bắt đầu, AWS có các trung tâm dữ liệu, rất nhiều trung tâm dữ liệu trên khắp thế giới và mỗi khu vực được tạo thành từ nhiều trung tâm dữ liệu. AWS gọi một trung tâm dữ liệu duy nhất hoặc một nhóm trung tâm dữ liệu và vùng sẵn sàng hoặc AZ. Mỗi vùng sẵn sàng là một hoặc nhiều trung tâm dữ liệu riêng biệt có nguồn điện, mạng và kết nối dự phòng. Khi bạn khởi chạy một phiên bản Amazon EC2, nó sẽ khởi chạy một máy ảo trên phần cứng vật lý được cài đặt trong vùng khả dụng. Điều này có nghĩa là mỗi khu vực AWS bao gồm nhiều vùng sẵn sàng, biệt lập và tách biệt về mặt vật lý trong một khu vực địa lý. Nhưng chúng tôi không xây dựng các vùng sẵn sàng ngay cạnh nhau vì chẳng hạn, nếu xảy ra sự cố quy mô lớn như thiên tai, bạn có thể mất kết nối với mọi thứ trong vùng sẵn sàng đó. Câu hỏi, điều gì xảy ra trong trường hợp thảm họa, mới quan trọng. Nếu bạn đã quen với việc lập kế hoạch khắc phục thảm họa, bạn thậm chí có thể biết chúng ta sẽ đi đâu với việc này. Nếu bạn chỉ chạy một phiên bản EC2, nó chỉ chạy trong một tòa nhà hoặc một vùng sẵn sàng và xảy ra thảm họa quy mô lớn, liệu ứng dụng của bạn còn có thể chạy và phục vụ doanh nghiệp của bạn không? Giải pháp hiển nhiên cho vấn đề này là chạy nhiều phiên bản EC2, giống như chúng tôi đã trình bày trong ví dụ mở rộng quy mô trước đó. Nhưng điều quan trọng nhất là đừng chạy chúng trong cùng một tòa nhà, thậm chí đừng chạy chúng trên cùng một con phố. Đẩy chúng ra xa nhất có thể trước khi tốc độ ánh sáng yêu cầu bạn dừng lại nếu bạn vẫn muốn liên lạc có độ trễ thấp. Hóa ra tốc độ ánh sáng sẽ cho phép chúng ta di chuyển các vùng sẵn sàng này cách xa nhau hàng chục dặm mà vẫn giữ được độ trễ một chữ số tính bằng mili giây giữa các vùng sẵn sàng này. Bây giờ, nếu thảm họa xảy ra, ứng dụng của bạn vẫn tiếp tục hoạt động tốt vì thảm họa này chỉ ảnh hưởng đến một số công suất của bạn chứ không phải tất cả và như chúng ta đã thấy trong phần trước, bạn có thể nhanh chóng tăng thêm công suất trong các vùng khả dụng còn lại, do đó cho phép doanh nghiệp của bạn để tiếp tục hoạt động mà không bị gián đoạn. Theo phương pháp tốt nhất với AWS, chúng tôi luôn khuyên bạn

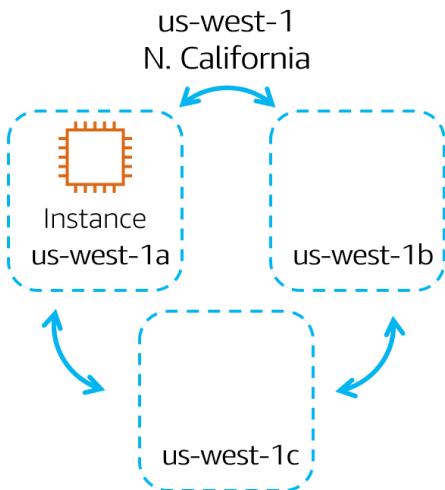
nên chạy qua ít nhất hai vùng sẵn sàng trong một khu vực. Điều này có nghĩa là triển khai dư thừa Cơ sở hạ tầng của bạn ở hai AZ khác nhau. Nhưng có nhiều khu vực hơn là chỉ những nơi chạy EC2. Nhiều dịch vụ AWS chạy ở cấp khu vực, nghĩa là chúng chạy đồng bộ trên nhiều AZ mà không cần bạn phải nỗ lực thêm. Lấy ELB mà chúng ta đã nói trước đây. Đây thực sự là một công trình mang tính khu vực. Nó chạy trên tất cả các vùng sẵn sàng, giao tiếp với các phiên bản EC2 đang chạy trong một vùng sẵn sàng cụ thể. Theo định nghĩa, các dịch vụ khu vực đã sẵn có ở mức độ cao mà bạn không phải tốn thêm chi phí nỗ lực nào. Vì vậy, khi bạn lập kế hoạch cho tính sẵn sàng cao, bất kỳ dịch vụ nào được liệt kê là dịch vụ trong phạm vi khu vực, bạn đã chọn hộp đó.



Vùng **sẵn sàng** là một trung tâm dữ liệu hoặc một nhóm trung tâm dữ liệu trong một Khu vực. Các Vùng sẵn sàng nằm cách nhau hàng chục dặm. Khoảng cách này đủ gần để có độ trễ thấp (khoảng thời gian từ khi nội dung được yêu cầu đến khi nhận được) giữa các Vùng sẵn sàng. Tuy nhiên, nếu thảm họa xảy ra ở một phần của Khu vực, chúng sẽ đủ xa để giảm khả năng nhiều Vùng sẵn sàng bị ảnh hưởng.

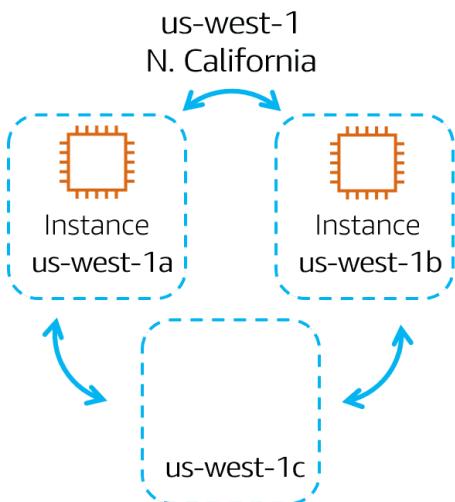
## Chạy phiên bản Amazon EC2 trong nhiều Vùng sẵn sàng

### **Phiên bản Amazon EC2 trong một Vùng sẵn sàng duy nhất**



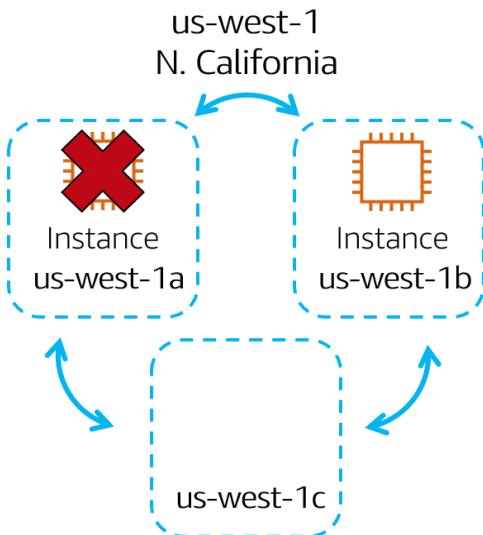
Giả sử bạn đang chạy một ứng dụng trên một phiên bản Amazon EC2 duy nhất ở Khu vực Bắc California. Phiên bản đang chạy trong Vùng sẵn sàng us-west-1a. Nếu us-west-1a không thành công, bạn sẽ mất phiên bản của mình.

### **Phiên bản Amazon EC2 trong nhiều Vùng sẵn sàng**



Cách tốt nhất là chạy ứng dụng trên ít nhất hai Vùng sẵn sàng trong một Khu vực. Trong ví dụ này, bạn có thể chọn chạy phiên bản Amazon EC2 thứ hai trong us-west-1b.

### **Lỗi vùng sẵn sàng**



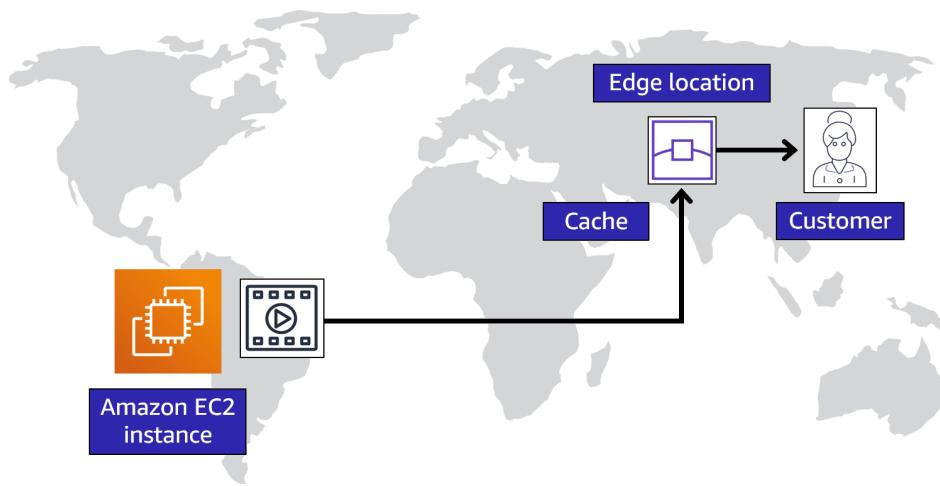
Nếu us-west-1a không thành công, ứng dụng của bạn vẫn chạy trong us-west-1b.

## Edge Locations

Một trong những điều tuyệt vời về cơ sở hạ tầng toàn cầu AWS là cách nó được thiết kế để giúp bạn phục vụ khách hàng tốt hơn. Hãy nhớ rằng, khi chọn một khu vực, một trong những tiêu chí quan trọng đã ở gần khách hàng của bạn. Nhưng nếu bạn có khách hàng khắp nơi trên thế giới hoặc ở các thành phố không gần một trong các khu vực của chúng tôi? Vâng, hãy nghĩ về quán cà phê của chúng tôi. Nếu bạn có cơ sở khách hàng tốt ở một thành phố mới, bạn có thể xây dựng một cửa hàng vệ tinh để phục vụ những khách hàng đó. Bạn không cần phải xây dựng toàn bộ trụ sở mới. Từ góc độ CNTT, nếu bạn có khách hàng ở Mumbai cần quyền truy cập vào dữ liệu của bạn, nhưng dữ liệu được lưu trữ bên ngoài khu vực Tokyo, thay vì có tất cả khách hàng ở Mumbai gửi yêu cầu đến tận Tokyo để truy cập dữ liệu, chỉ cần đặt một bản sao cục bộ hoặc lưu trữ một bản sao ở Mumbai. Lưu bản sao dữ liệu vào bộ nhớ đệm đến gần hơn với khách hàng trên toàn thế giới sử dụng khái niệm: content delivery networks (mạng phân phối nội dung) hoặc CDN. CDN thường được sử dụng. Tại AWS, chúng tôi gọi CDN của mình là **Amazon CloudFront**. Amazon CloudFront là một dịch vụ giúp cung cấp dữ liệu, video, ứng dụng và API cho khách hàng trên toàn thế giới với độ trễ thấp và tốc độ truyền cao. Amazon CloudFront sử dụng những gì được gọi là các vị trí Edge xung quanh thế giới giúp tăng tốc giao tiếp với người dùng bất kể họ ở đâu. Các vị trí biên tách biệt với các vùng, để bạn có thể đẩy nội dung từ bên trong một vùng vào một tập hợp các vị trí Edge trên toàn thế giới để tăng tốc truyền thông và cung cấp nội dung. Các vị trí AWS Edge cũng không chỉ chạy trên CloudFront. Họ điều hành dịch vụ tên miền hoặc DNS, được gọi là Tuyến đường Amazon 53, giúp hướng dẫn khách hàng đến các vị trí web chính xác với độ trễ

thấp đáng tin cậy.Nhưng nếu doanh nghiệp của bạn muốn sử dụng Dịch vụ AWS bên trong tòa nhà của chính họ?Vâng, chắc chắn, AWS có thể làm điều đó cho bạn.Giới thiệu **AWS Outposts**, nơi AWS về cơ bản sẽ cài đặt một khu vực nhỏ hoạt động đầy đủ ngay bên trong trung tâm dữ liệu của riêng bạn.Nó được sở hữu và vận hành bởi AWS,sử dụng 100% chức năng của AWS,nhưng bị cô lập trong tòa nhà của riêng bạn.Đó không phải là giải pháp mà hầu hết khách hàng cần.Nhưng nếu bạn gặp vấn đề cụ thể có thể chỉ được giải quyết bằng cách ở trong tòa nhà của chính bạn,nhưng chúng tôi hiểu rằng AWS Outposts có thể giúp ích.

**An edge location** là trang web mà Amazon CloudFront sử dụng để lưu trữ các bản sao nội dung được lưu trong bộ nhớ đệm của bạn gần hơn với khách hàng để phân phối nhanh hơn.



**Nguồn gốc** Giả sử dữ liệu của công ty bạn được lưu trữ ở Brazil và bạn có khách hàng sống ở Trung Quốc. Để cung cấp nội dung cho những khách hàng này, bạn không cần phải di chuyển tất cả nội dung sang một trong các Khu vực của Trung Quốc.

### Edge Location

Thay vì yêu cầu khách hàng của bạn lấy dữ liệu từ Brazil, bạn có thể lưu một bản sao vào bộ nhớ đệm cục bộ tại một vị trí biên gần với khách hàng của bạn ở Trung Quốc.

### Khách hàng

Khi khách hàng ở Trung Quốc yêu cầu một trong các tệp của bạn, Amazon CloudFront sẽ truy xuất tệp từ bộ đệm ở vị trí biên và gửi tệp cho khách hàng. Tệp được gửi đến khách hàng nhanh hơn vì tệp đến từ vị trí rìa gần Trung Quốc thay vì nguồn ban đầu ở Brazil.

# How to Provision AWS Resources (Part 1)

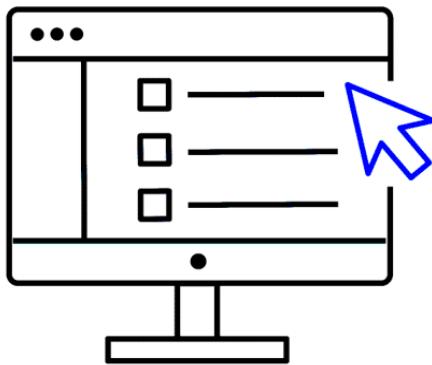
Chúng ta đã nói về một số tài nguyên AWS khác nhau như cũng như cơ sở hạ tầng toàn cầu của AWS. Có thể bạn đang thắc mắc, làm thế nào để tối ưu hóa sự tương tác với các dịch vụ này? Câu trả lời là API. Trong AWS, mọi thứ đều là lệnh gọi API. API là một giao diện lập trình ứng dụng. Điều đó có nghĩa là có những cách định sẵn cho bạn để tương tác với các dịch vụ AWS. Bạn có thể gọi hoặc gọi các API này để cung cấp, cấu hình và quản lý tài nguyên AWS của bạn. Ví dụ: bạn có thể khởi chạy phiên bản EC2, hoặc bạn có thể tạo hàm AWS Lambda. Mỗi cái đó sẽ là các yêu cầu khác nhau và các lệnh gọi API khác nhau tới AWS. Bạn có thể sử dụng **AWS Management Console** (Bảng điều khiển quản lý AWS), **AWS Command Line Interface** (Giao diện dòng lệnh AWS), **AWS Software Development Kits** (Bộ công cụ phát triển phần mềm AWS), hoặc nhiều công cụ khác như AWS CloudFormation để tạo yêu cầu gửi đến API AWS để tạo và quản lý tài nguyên AWS.

Đầu tiên, hãy nói về Bảng điều khiển quản lý AWS. Bảng điều khiển quản lý AWS dựa trên trình duyệt. Thông qua bảng điều khiển, bạn có thể quản lý tài nguyên AWS của mình một cách trực quan và theo cách dễ tiêu hóa. Nó cũng hữu ích cho việc xây dựng môi trường thử nghiệm hoặc xem hóa đơn AWS, xem, theo dõi và làm việc với các nguồn lực phi kỹ thuật khác. Tuy nhiên, một khi bạn đã thiết lập và chạy trong môi trường kiểu sản xuất, bạn không muốn dựa vào điểm và nhấp chuột phong cách mà bảng điều khiển mang lại cho bạn tạo và quản lý tài nguyên AWS của bạn. Ví dụ: để tạo một phiên bản Amazon EC2, bạn cần nhấp qua nhiều màn hình khác nhau, thiết lập tất cả các cấu hình bạn muốn, và sau đó bạn khởi chạy phiên bản của mình. Nếu sau này bạn muốn khởi chạy một phiên bản EC2 khác, bạn sẽ cần quay lại bảng điều khiển và nhấp qua màn hình của họ một lần nữa để thiết lập và chạy nó. Bằng cách yêu cầu con người thực hiện việc cung cấp thủ công này, bạn đang tự mở ra những lỗi tiềm ẩn. Rất dễ quên chọn hộp kiểm hoặc viết sai chính tả điều gì đó khi bạn đang làm mọi thứ một cách thủ công. Câu trả lời cho vấn đề này là sử dụng các công cụ cho phép bạn viết kịch bản hoặc lập trình các lệnh gọi API. Một công cụ bạn có thể sử dụng là Giao diện dòng lệnh AWS hoặc CLI. CLI cho phép bạn thực hiện lệnh gọi API sử dụng thiết bị đầu cuối trên máy của bạn. Điều này khác với kiểu điều hướng trực quan của Bảng điều khiển quản lý. Viết lệnh bằng CLI giúp hành động có thể viết được và có thể lặp lại. Vì vậy, bạn có thể viết và chạy các lệnh của bạn để khởi chạy phiên bản EC2, và nếu bạn muốn khởi chạy một cái khác, bạn chỉ có thể chạy lại lệnh viết sẵn. Điều này làm cho nó ít bị ảnh hưởng bởi lỗi của con người. Bạn có thể để các tập lệnh này chạy tự động, như theo lịch trình hoặc

được kích hoạt bởi một quy trình khác.Tự động hóa là rất quan trọng để có triển khai đám mây thành công và có thể dự đoán được theo thời gian.Một cách khác để tương tác với AWS là thông qua Bộ công cụ phát triển phần mềm AWS hoặc SDK.SDK cho phép bạn tương tác với Tài nguyên AWS thông qua nhiều ngôn ngữ lập trình khác nhau. Điều này làm cho nó dễ dàng cho các nhà phát triển tạo ra các chương trình sử dụng AWS mà không sử dụng API cấp thấp,cũng như tránh việc tạo tài nguyên thủ công mà chúng ta vừa nói đến.

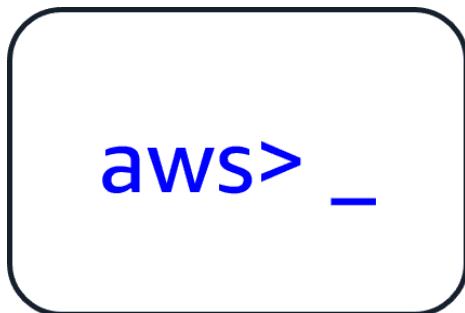
## Ways to Interact with AWS Services

### AWS Management Console



Bảng điều khiển quản lý AWS là giao diện dựa trên web để truy cập và quản lý các dịch vụ AWS. Bạn có thể nhanh chóng truy cập các dịch vụ được sử dụng gần đây và tìm kiếm các dịch vụ khác theo tên, từ khóa hoặc từ viết tắt. Bảng điều khiển bao gồm các trình hướng dẫn và quy trình làm việc tự động có thể đơn giản hóa quá trình hoàn thành nhiệm vụ. Bạn cũng có thể sử dụng ứng dụng di động AWS Console để thực hiện các tác vụ như giám sát tài nguyên, xem cảnh báo và truy cập thông tin thanh toán. Nhiều danh tính có thể duy trì trạng thái đăng nhập vào ứng dụng di động AWS Console cùng một lúc.

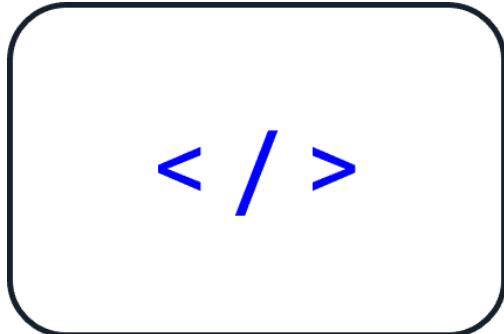
### AWS Command Line Interface



Để tiết kiệm thời gian khi thực hiện yêu cầu API, bạn có thể sử dụng **Giao diện dòng lệnh AWS (AWS CLI)**. AWS CLI cho phép bạn kiểm soát nhiều dịch vụ AWS trực tiếp từ dòng lệnh trong một công cụ. AWS CLI có sẵn cho người dùng trên Windows, macOS và Linux.

Bằng cách sử dụng AWS CLI, bạn có thể tự động hóa các hành động mà dịch vụ và ứng dụng của bạn thực hiện thông qua tập lệnh. Ví dụ: bạn có thể sử dụng lệnh để khởi chạy phiên bản Amazon EC2, kết nối phiên bản Amazon EC2 với một nhóm Auto Scaling cụ thể, v.v.

### Software development kits (SDK)



Một tùy chọn khác để truy cập và quản lý dịch vụ AWS là **bộ công cụ phát triển phần mềm (SDK)**. SDK giúp bạn sử dụng dịch vụ AWS dễ dàng hơn thông qua API được thiết kế cho ngôn ngữ lập trình hoặc nền tảng của bạn. SDK cho phép bạn sử dụng dịch vụ AWS với các ứng dụng hiện có của mình hoặc tạo các ứng dụng hoàn toàn mới sẽ chạy trên AWS.

Để giúp bạn bắt đầu sử dụng SDK, AWS cung cấp tài liệu và mã mẫu cho từng ngôn ngữ lập trình được hỗ trợ. Các ngôn ngữ lập trình được hỗ trợ bao gồm C++, Java, .NET, v.v.

## How to Provision AWS Resources (Part 2)

**AWS Elastic Beanstalk** là dịch vụ giúp bạn cung cấp Môi trường dựa trên Amazon EC2. Thay vì nhập vào bảng điều khiển hoặc viết nhiều lệnh để xây dựng mạng của bạn, phiên bản EC2, bộ cân bằng tải linh hoạt và thay đổi quy mô, thay vào đó bạn có thể cung cấp mã ứng dụng của bạn và cấu hình mong muốn để dịch vụ AWS Elastic Beanstalk, sau đó sẽ lấy thông tin đó và xây dựng môi trường cho bạn. AWS Elastic Beanstalk cũng làm được điều đó dễ dàng lưu cấu hình môi trường để có thể triển khai lại chúng một cách dễ dàng. AWS Elastic Beanstalk mang đến cho bạn thuận tiện khi không phải cung cấp và quản lý tất cả các phần này một cách riêng biệt trong khi vẫn cung cấp cho bạn khả năng hiển thị và kiểm soát các tài nguyên cơ bản. Bạn có thể tập

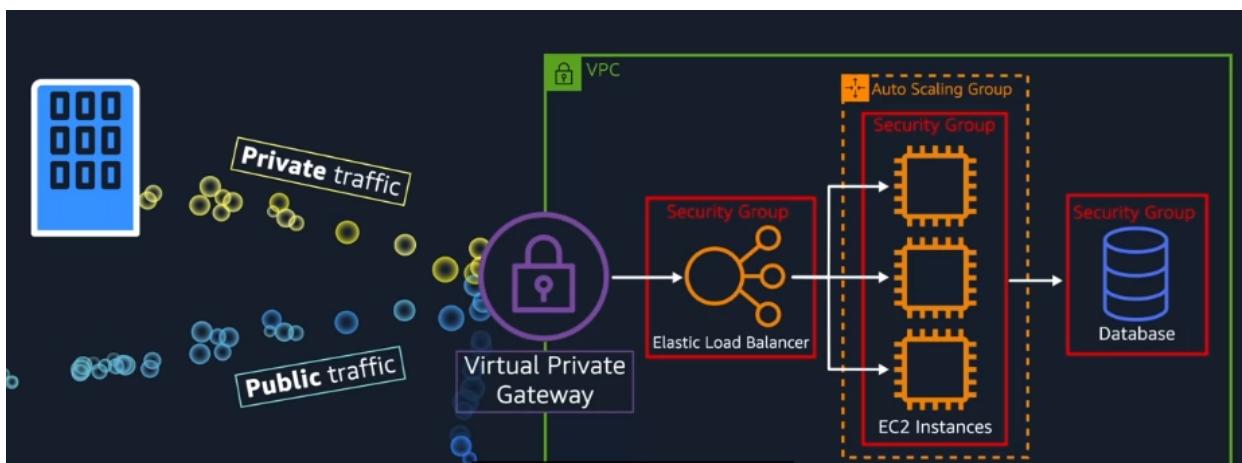
trung vào công việc kinh doanh của mình ứng dụng chứ không phải cơ sở hạ tầng. Một dịch vụ khác bạn có thể sử dụng để giúp tạo các hoạt động triển khai tự động và có thể lặp lại là AWS CloudFormation. **AWS CloudFormation** là một cơ sở hạ tầng là công cụ mã, cho phép bạn xác định nhiều loại tài nguyên AWS theo cách khai báo bằng cách sử dụng các tài liệu dựa trên văn bản JSON hoặc YAML, được gọi là Mẫu CloudFormation. Một định dạng khai báo như thế này cho phép bạn xác định những gì bạn muốn xây dựng mà không cần chỉ định chi tiết chính xác làm thế nào để xây dựng nó.

CloudFormation cho phép bạn xác định những gì bạn muốn và công cụ CloudFormation sẽ lo lắng về các chi tiết khi gọi API để xây dựng mọi thứ. Nó cũng không chỉ giới hạn đến các giải pháp dựa trên EC2. CloudFormation hỗ trợ nhiều các tài nguyên AWS khác nhau từ bộ lưu trữ, cơ sở dữ liệu, phân tích, học máy, v.v. Khi bạn đã xác định được tài nguyên của mình trong mẫu CloudFormation, CloudFormation sẽ phân tích mẫu và bắt đầu cung cấp tất cả các tài nguyên bạn đã xác định song song. CloudFormation quản lý tất cả các cuộc gọi vào API AWS phía sau dành cho bạn. Bạn có thể chạy cùng một đội hình đám mây mẫu và nhiều tài khoản hoặc nhiều vùng và nó sẽ tạo môi trường giống hệt nhau trên chúng. Có ít chỗ cho lỗi của con người hơn đó là một quá trình hoàn toàn tự động.

## Connectivity to AWS

**VPC** hoặc Virtual Private Cloud (Đám mây riêng ảo), về cơ bản là mạng riêng của bạn trong AWS. VPC cho phép bạn xác định một dải IP riêng cho tài nguyên AWS của bạn, và bạn đặt những thứ như phiên bản ec2 và ELB bên trong VPC của bạn. Bây giờ, bạn không chỉ đi néo tài nguyên của bạn vào VPC và tiếp tục. Bạn đặt chúng vào các mạng con khác nhau. **Subnets** (Mạng con) là các khối địa chỉ IP trong VPC của bạn cho phép bạn nhóm các tài nguyên lại với nhau, kiểm soát xem tài nguyên có công khai hoặc có sẵn riêng tư. Điều chúng tôi chưa nói với bạn, thực sự có những cách bạn có thể kiểm soát lưu lượng truy cập nào vào VPC của bạn. Ý tôi là, đối với một số VPC, bạn có thể có tài nguyên truy cập Internet mà công chúng có thể tiếp cận, như một trang web công cộng chẳng hạn. Tuy nhiên, trong các kịch bản khác, bạn có thể có những tài nguyên mà bạn chỉ muốn có thể truy cập nếu ai đó đăng nhập vào mạng riêng của bạn. Đây có thể là các dịch vụ nội bộ như ứng dụng nhân sự, hoặc cơ sở dữ liệu phụ trợ. Đầu tiên, hãy nói về các nguồn lực dành cho công chúng. Để cho phép lưu lượng truy cập từ Internet công cộng để chảy vào và ra khỏi VPC của bạn, bạn phải đính kèm cái được gọi là cổng Internet, hoặc IGW vào VPC của bạn. Một cổng Internet giống như một cánh cửa mở ra cho công chúng. Hãy nghĩ về một quán cà phê. Không có cửa trước, khách hàng không

thể vào được, và gọi cà phê của họ. Vì vậy, chúng tôi lắp đặt một cửa trước, và sau đó mọi người có thể ra vào cánh cửa đó khi đến và đi từ cửa hàng của chúng tôi. Cửa trước trong ví dụ này giống như một cổng [Internet.Không](#) có nó, không ai có thể đặt được các tài nguyên được đặt bên trong VPC của bạn. Tiếp theo, hãy nói về VPC với tất cả các tài nguyên riêng tư nội bộ. Chúng tôi không muốn bất cứ ai từ bất cứ nơi nào để có thể tiếp cận những tài nguyên này, vì vậy chúng tôi không muốn có một cổng Internet được gắn vào VPC của mình. Thay vào đó, chúng tôi muốn có một cổng riêng chỉ cho phép mọi người vào nếu họ đến từ một mạng được phê duyệt, không phải Internet công cộng. Ô cửa riêng này được gọi là cổng riêng ảo, và nó cho phép bạn tạo kết nối VPN giữa một mạng riêng, như trung tâm dữ liệu tại chỗ của bạn, hoặc mạng nội bộ công ty tới VPC của bạn.



Hãy liên hệ điều này với quán cà phê, điều này sẽ giống như có một tuyến xe buýt riêng đi từ tòa nhà của tôi đến quán cà phê. Nếu tôi muốn đi uống cà phê, Đầu tiên tôi phải đăng nhập vào tòa nhà xác thực danh tính của tôi, và sau đó tôi có thể đi tuyến xe buýt bí mật tới quán cà phê nội bộ đó chỉ những người trong tòa nhà của tôi mới có thể sử dụng. Nếu bạn muốn thành lập kết nối VPN được mã hóa tới địa chỉ riêng tư của bạn, tài nguyên AWS nội bộ, bạn sẽ cần đính kèm một cổng riêng ảo vào VPC của bạn. Bây giờ, vấn đề với tuyến xe buýt siêu bí mật của chúng tôi là nó vẫn sử dụng con đường rộng mở. Nó dễ bị tắc giao thông và sự chậm lại do phần còn lại gây rắc rối đang tiến hành công việc kinh doanh của họ. Điều tương tự cũng đúng với các kết nối [VPN](#). [Chúng](#) là riêng tư và được mã hóa, nhưng họ vẫn sử dụng kết nối Internet thông thường có băng thông đang được chia sẻ bởi nhiều người sử dụng Internet. Vì vậy những gì tôi đã làm để khiến mọi thứ trở nên đáng tin cậy hơn, và ít bị ảnh hưởng bởi sự chậm lại, tôi đã làm một việc hoàn toàn riêng biệt: cánh cửa ma thuật dẫn thẳng từ studio thành quán cà phê. Không ai khác đang lái xe trên đường có thể làm tôi chậm lại, bởi vì đây là lối vào trực tiếp của tôi. [Không](#) ai khác có thể sử dụng nó. Cái gì? Bạn không có một cánh cửa

ma thuật bí mật dẫn vào quan cà phê yêu thích của bạn? Tiếp tục nào.Vấn đề là bạn vẫn muốn có kết nối riêng tư,nhưng bạn muốn nó được dành riêng và không chia sẻ với ai khác.Bạn muốn độ trễ thấp nhất có thể với mức độ bảo mật cao nhất có thể.Với AWS, bạn có thể đạt được điều đó sử dụng cái được gọi là AWS Direct Connect.

**AWS Direct Connect** (Kết nối trực tiếp) cho phép bạn thiết lập một hoàn toàn riêng tư,kết nối cáp quang chuyên dụng từ trung tâm dữ liệu của bạn đến AWS.Bạn làm việc với đối tác Direct Connect ở khu vực của bạn để thiết lập kết nối này.Bởi vì giống như cánh cửa kỳ diệu của tôi,AWS Direct Connect cung cấp đường truyền vật lý kết nối mạng của bạn với AWS VPC.Điều này có thể giúp bạn gặp nhau cầu thủ và quy định cao,cũng như tránh mọi vấn đề về băng thông tiềm ẩn.Điều quan trọng cần lưu ý là một VPC có thể có nhiều loại công nghệ đính kèm cho nhiều loại tài nguyên,tất cả đều cư trú trong cùng một VPC,chỉ trong các mạng con khác nhau

## Connectivity to AWS

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

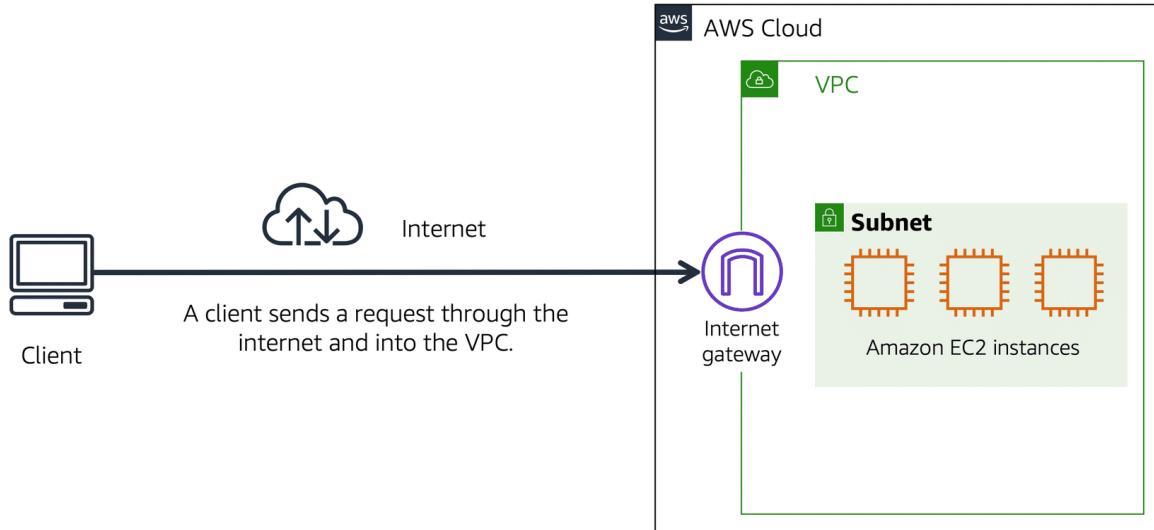
Hãy tưởng tượng hàng triệu khách hàng sử dụng dịch vụ AWS. Ngoài ra, hãy tưởng tượng hàng triệu tài nguyên mà những khách hàng này đã tạo ra, chẳng hạn như phiên bản Amazon EC2. Nếu không có ranh giới xung quanh tất cả các tài nguyên này, lưu lượng mạng sẽ có thể di chuyển giữa chúng mà không bị hạn chế.

Dịch vụ mạng mà bạn có thể sử dụng để thiết lập ranh giới xung quanh tài nguyên AWS của mình là [\*\*Đám mây riêng ảo của Amazon \(Amazon VPC\)\*\*](#).

Amazon VPC cho phép bạn cung cấp một phần riêng biệt của Đám mây AWS. Trong phần biệt lập này, bạn có thể khởi chạy các tài nguyên trong mạng ảo mà bạn xác định. Trong đám mây riêng ảo (VPC), bạn có thể sắp xếp tài nguyên của mình thành các mạng con. Mạng **con** là một phần của VPC có thể chứa các tài nguyên như phiên bản Amazon EC2.

### **Internet gateway**

Để cho phép lưu lượng truy cập công cộng từ internet truy cập vào VPC của bạn, bạn gắn một **cổng internet** vào VPC.



Cổng internet là kết nối giữa VPC và internet. Bạn có thể coi cổng internet giống như một cánh cửa mà khách hàng sử dụng để vào quán cà phê. Nếu không có cổng internet, không ai có thể truy cập tài nguyên trong VPC của bạn.

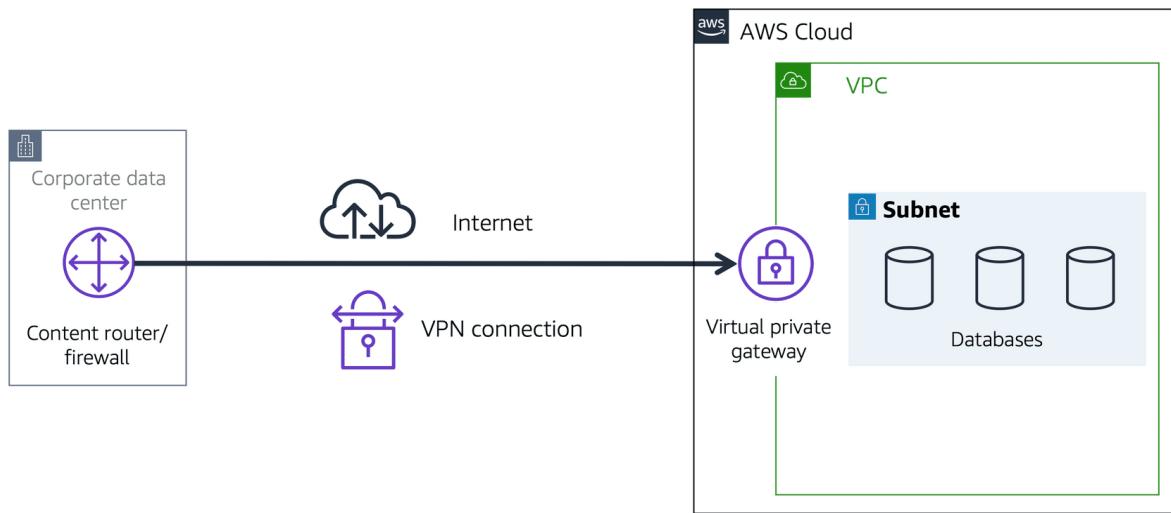
**Điều gì sẽ xảy ra nếu bạn có một VPC chỉ bao gồm các tài nguyên riêng tư?**

### **Virtual private gateway**

Đây là ví dụ về cách hoạt động của cổng riêng ảo. Bạn có thể coi Internet như con đường giữa nhà bạn và quán cà phê. Giả sử bạn đang đi trên con đường này có một vệ sĩ bảo vệ bạn. Bạn vẫn đang sử dụng con đường giống như những khách hàng khác, nhưng có thêm một lớp bảo vệ.

Vệ sĩ giống như một kết nối mạng riêng ảo (VPN) mã hóa (hoặc bảo vệ) lưu lượng truy cập internet của bạn khỏi tất cả các yêu cầu khác xung quanh nó.

Cổng riêng ảo là thành phần cho phép lưu lượng truy cập internet được bảo vệ đi vào VPC. Mặc dù kết nối của bạn với quán cà phê được bảo vệ thêm nhưng vẫn có thể xảy ra ùn tắc giao thông do bạn đang sử dụng cùng một con đường với những khách hàng khác.



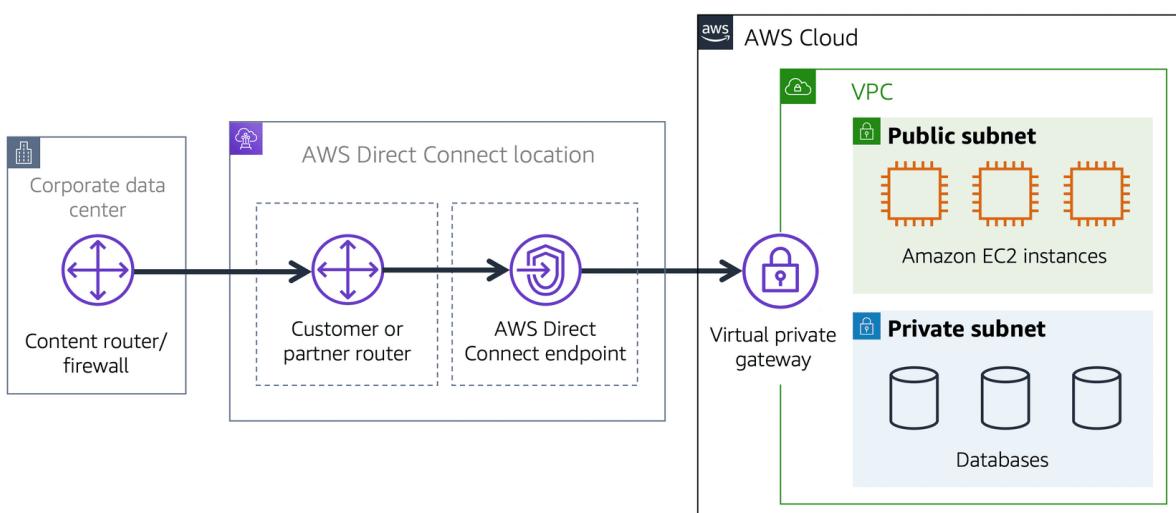
Cổng riêng ảo cho phép bạn thiết lập kết nối mạng riêng ảo (VPN) giữa VPC của bạn và mạng riêng, chẳng hạn như trung tâm dữ liệu tại chỗ hoặc mạng nội bộ của công ty. Cổng riêng ảo chỉ cho phép lưu lượng truy cập vào VPC nếu nó đến từ một mạng được phê duyệt.

## Kết nối trực tiếp AWS

**Kết nối trực tiếp AWS** là dịch vụ cho phép bạn thiết lập kết nối riêng tư chuyên dụng giữa trung tâm dữ liệu của bạn và VPC.

Giả sử có một tòa nhà chung cư có hành lang nối thẳng tòa nhà với quán cà phê. Chỉ những cư dân của tòa nhà chung cư mới có thể đi qua hành lang này.

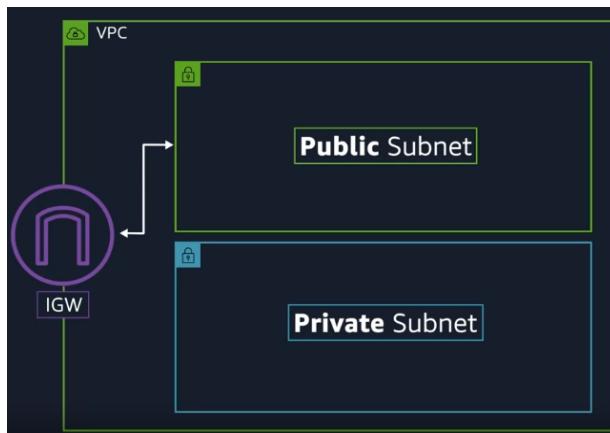
Hành lang riêng này cung cấp cùng loại kết nối chuyên dụng như AWS Direct Connect. Cư dân có thể vào quán cà phê mà không cần sử dụng đường công cộng chung với các khách hàng khác.



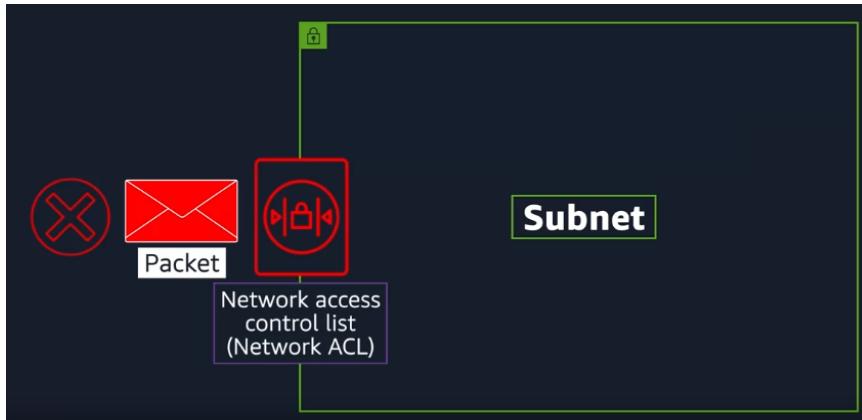
Kết nối riêng mà AWS Direct Connect cung cấp giúp bạn giảm chi phí mạng và tăng lượng băng thông có thể truyền qua mạng của bạn.

## Subnets and Network Access Control Lists

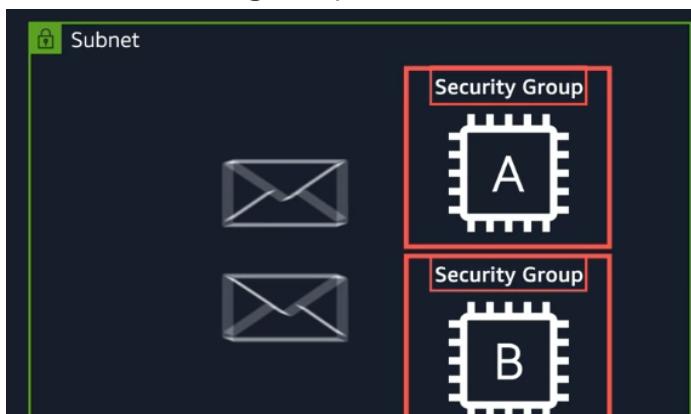
Chào mừng đến với VPC của bạn. Bạn có thể coi nó như một pháo đài kiên cố, nơi không có gì có thể ra vào mà không có sự cho phép rõ ràng. Bạn có một cổng trên VPC chỉ cho phép lưu lượng truy cập vào hoặc ra khỏi VPC. AWS có nhiều công cụ bao gồm mọi lớp bảo mật, bảo mật ứng dụng tăng cường mạng, nhận dạng người dùng, xác thực và ủy quyền. Từ chối dịch vụ phân tán hoặc ngăn chặn DDoS, tính toàn vẹn dữ liệu, mã hóa, v.v.



Hiện tại, lý do kỹ thuật duy nhất để sử dụng Mạng con trong VPC là để kiểm soát quyền truy cập vào Cổng. Mạng con công cộng có quyền truy cập vào Cổng Internet, Mạng con riêng tư thì không. Nhưng mạng con cũng có thể kiểm soát quyền truy cập. Các gói là các tin nhắn từ internet và mọi gói vượt qua ranh giới mạng con sẽ được kiểm tra dựa trên thứ gọi là danh sách kiểm soát truy cập mạng hoặc **Network ACL**. Việc kiểm tra này nhằm xem liệu gói có quyền rời khỏi hoặc vào mạng con hay không, dựa trên việc gói được gửi từ ai và cách nó cố gắng liên lạc.



Bạn có thể coi Network ACL là nhân viên kiểm soát hộ chiếu. Nếu bạn nằm trong danh sách được phê duyệt thì bạn sẽ vượt qua, nếu bạn không có tên trong danh sách hoặc nếu bạn rõ ràng nằm trong danh sách không được nhập thì bạn sẽ bị chặn. Mạng ACL kiểm tra lưu lượng truy cập vào và ra khỏi mạng con, giống như kiểm soát hộ chiếu. Danh sách này được kiểm tra trên đường bạn vào một quốc gia và trên đường ra. Và chỉ vì bạn được phép vào không nhất thiết có nghĩa là họ sẽ cho bạn ra ngoài. Lưu lượng truy cập đã được phê duyệt có thể được gửi trên đường đi và lưu lượng truy cập có khả năng gây hại cố gắng giành quyền kiểm soát hệ thống thông qua các yêu cầu quản trị. Họ bị chặn trước khi chạm vào mục tiêu. Bạn không thể hack những gì bạn không thể chạm vào. Bây giờ, điều này nghe có vẻ an toàn tuyệt vời. Nhưng nó không giải đáp được tất cả các vấn đề về điều khiển mạng. Bởi vì ACL mạng chỉ được đánh giá một gói nếu nó vượt qua ranh giới mạng con, vào hoặc ra. Nó không đánh giá liệu một gói có thể tiếp cận một Phiên bản EC2 cụ thể hay không. Đôi khi bạn sẽ có nhiều Phiên bản EC2 trong cùng một mạng con. Nhưng họ có thể có những quy định khác nhau về việc ai có thể gửi tin nhắn, những tin nhắn đó được phép gửi đến cổng nào. Vì vậy, bạn cũng cần bảo mật mạng ở cấp độ cá thể.



Để giải quyết các câu hỏi về quyền truy cập ở cấp phiên bản, chúng tôi giới thiệu **Security Group** (Nhóm bảo mật). Mỗi Phiên bản EC2 khi được khởi chạy đều tự động

có Nhóm bảo mật. Theo mặc định, Nhóm bảo mật hoàn toàn không cho phép bất kỳ lưu lượng truy cập nào vào phiên bản. Tất cả các cổng đều bị chặn, tất cả các địa chỉ IP gửi gói đều bị chặn. Điều đó rất an toàn nhưng có lẽ không hữu ích lắm, nếu bạn muốn một phiên bản thực sự chấp nhận lưu lượng truy cập từ bên ngoài, chẳng hạn như tin nhắn từ bạn bè và phiên bản hoặc tin nhắn từ internet. Vì vậy, rõ ràng là bạn có thể sửa đổi Nhóm bảo mật để chấp nhận một loại lưu lượng truy cập cụ thể. Trong trường hợp là một trang web, bạn muốn lưu lượng truy cập dựa trên web hoặc HTTPS được chấp nhận. Nhưng không phải các loại lưu lượng truy cập khác như hệ điều hành hoặc yêu cầu quản trị. Nếu Narcos là cơ quan kiểm soát hộ chiếu thì nhóm bảo mật giống như người gác cửa tại tòa nhà của bạn, tòa nhà đó là Phiên bản EC2 trong trường hợp này. Người gác cửa sẽ kiểm tra danh sách để đảm bảo rằng ai đó được phép vào tòa nhà, nhưng sẽ không thèm kiểm tra danh sách trên đường ra. Với Nhóm bảo mật, bạn cho phép lưu lượng truy cập cụ thể vào và theo mặc định, tất cả lưu lượng truy cập đều được phép ra.

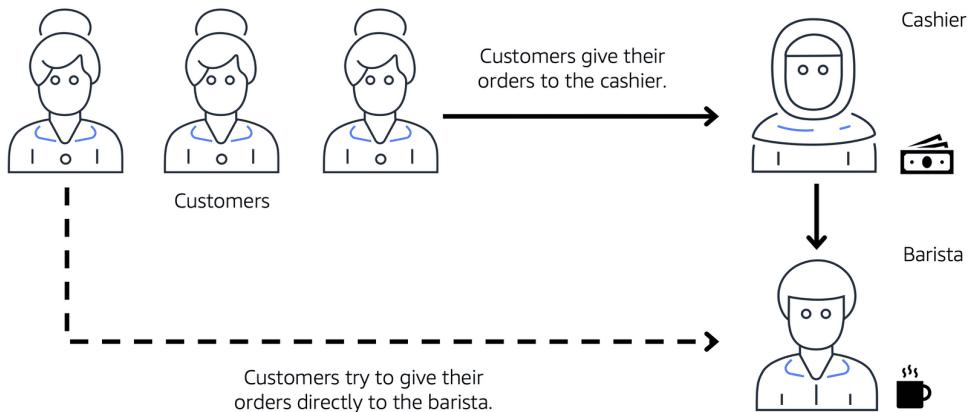
Bảo mật mạng tốt sẽ tận dụng được cả Network ACL và Nhóm bảo mật vì tính bảo mật và độ sâu là rất quan trọng đối với các kiến trúc hiện đại.

## Subnets and Network Access Control Lists

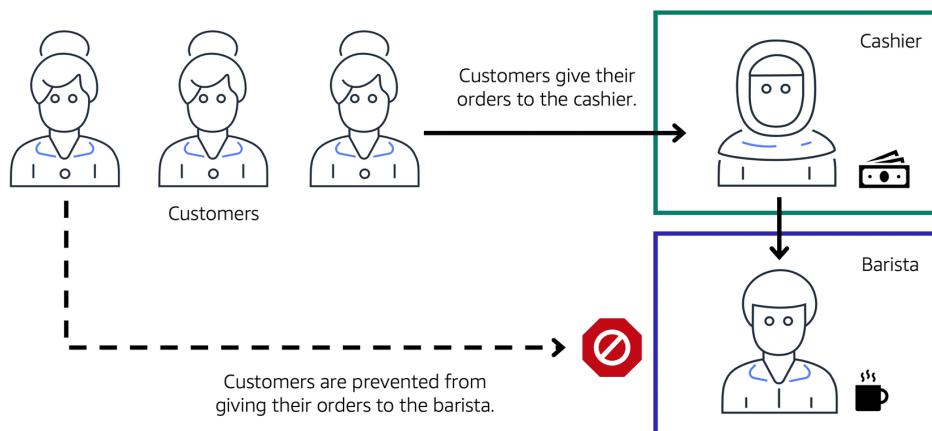
Để tìm hiểu thêm về vai trò của mạng con trong VPC, hãy xem lại ví dụ sau từ quán cà phê.

Đầu tiên, khách hàng đưa đơn hàng của mình cho nhân viên thu ngân. Nhân viên thu ngân sau đó chuyển đơn đặt hàng cho nhân viên pha chế. Quá trình này cho phép dây chuyền tiếp tục hoạt động trơn tru khi có nhiều khách hàng đến.

Giả sử rằng một số khách hàng cố gắng bỏ qua quầy thu ngân và trực tiếp đưa đơn hàng của họ cho nhân viên pha chế. Điều này làm gián đoạn luồng giao thông và dẫn đến việc khách hàng tiếp cận một phần của quán cà phê mà họ bị hạn chế.



Để khắc phục điều này, các chủ quán cà phê chia khu vực quầy tính tiền bằng cách đặt nhân viên thu ngân và nhân viên pha chế ở những khu vực làm việc riêng biệt. Khu vực làm việc của nhân viên thu ngân hướng ra phía công cộng và được thiết kế để tiếp khách hàng. Khu vực của barista là khu vực riêng tư. Nhân viên pha chế vẫn có thể nhận order từ nhân viên thu ngân nhưng không thể nhận trực tiếp từ khách hàng.



Điều này tương tự như cách bạn có thể sử dụng các dịch vụ mạng AWS để tách biệt tài nguyên và xác định chính xác luồng lưu lượng mạng.

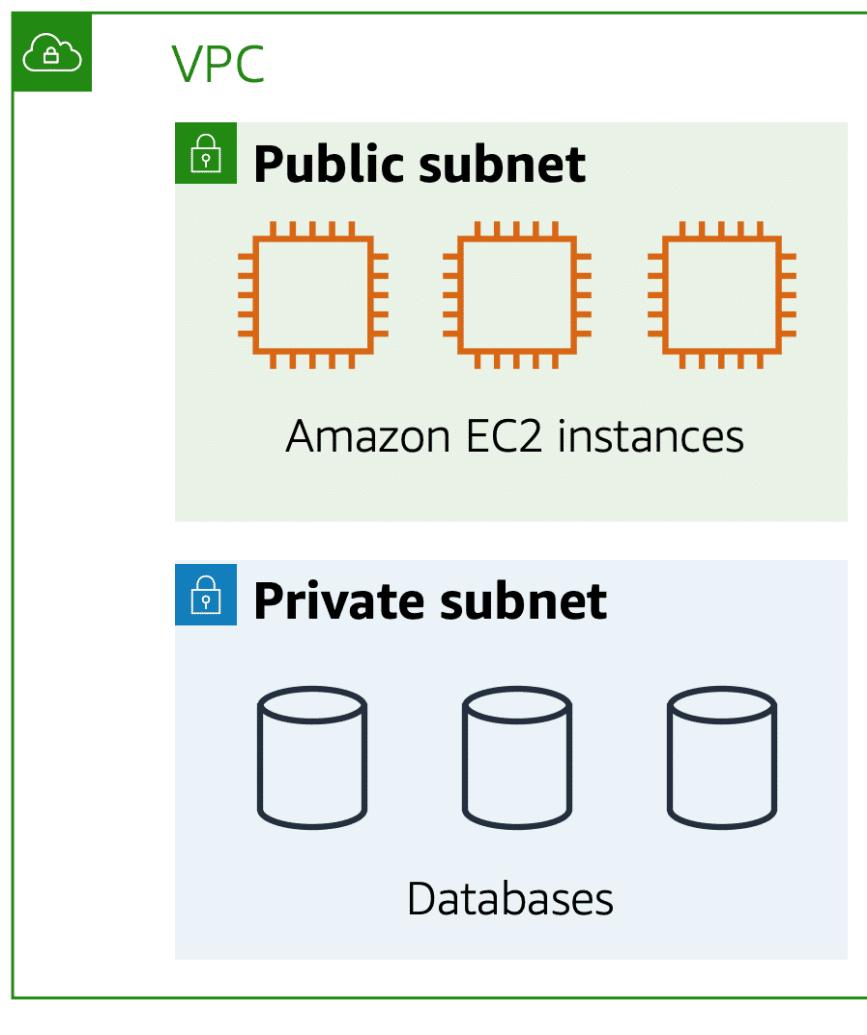
Trong quán cà phê, bạn có thể coi khu vực quầy tính tiền như một VPC. Khu vực quầy chia làm 2 khu vực riêng biệt dành cho khu vực làm việc của nhân viên thu ngân và khu vực làm việc của nhân viên pha chế. Trong VPC, **subnets** là các khu vực riêng biệt được sử dụng để nhóm các tài nguyên lại với nhau.

## Subnets

Mạng con là một phần của VPC trong đó bạn có thể nhóm các tài nguyên dựa trên nhu cầu bảo mật hoặc vận hành. Mạng con có thể là công khai hoặc riêng tư.



## AWS Cloud



**Mạng con công cộng** chứa các tài nguyên mà công chúng có thể truy cập được, chẳng hạn như trang web của cửa hàng trực tuyến.

**Mạng con riêng tư** chứa các tài nguyên chỉ có thể truy cập được thông qua mạng riêng của bạn, chẳng hạn như cơ sở dữ liệu chứa thông tin cá nhân và lịch sử đặt hàng của khách hàng.

Trong VPC, các mạng con có thể giao tiếp với nhau. Ví dụ: bạn có thể có một ứng dụng liên quan đến các phiên bản Amazon EC2 trong mạng con công cộng giao tiếp với cơ sở dữ liệu nằm trong mạng con riêng tư.

### Network Traffic in a VPC

Khi khách hàng yêu cầu dữ liệu từ ứng dụng được lưu trữ trên đám mây AWS, yêu cầu này sẽ được gửi dưới dạng **package** (gói). Gói là **một** đơn vị dữ liệu được gửi qua internet hoặc mạng.

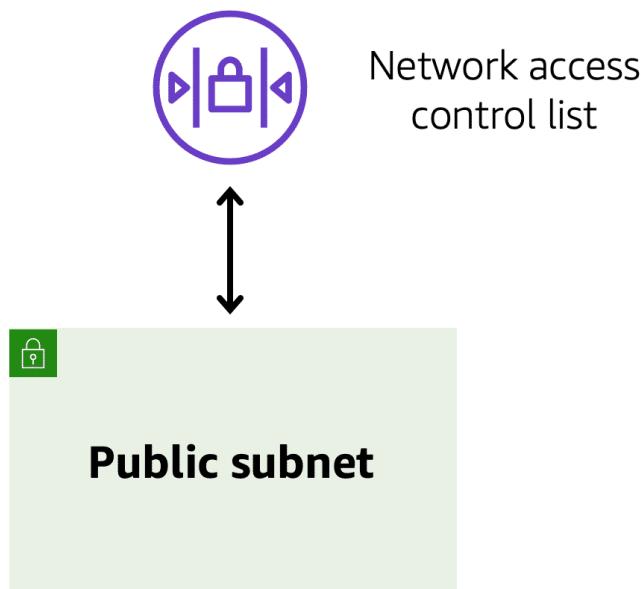
Nó đi vào VPC thông qua một cổng internet. Trước khi một gói có thể vào mạng con hoặc thoát khỏi mạng con, nó sẽ kiểm tra các quyền. Các quyền này cho biết ai đã gửi gói và cách gói đang cố gắng liên lạc với các tài nguyên trong mạng con.

Thành phần VPC kiểm tra quyền truy cập gói cho mạng con là một [danh sách kiểm soát truy cập mạng \(ACL\)](#).

### Network Access Control Lists (ACLs)

Danh sách kiểm soát truy cập mạng (ACL) là một tường lửa ảo kiểm soát lưu lượng truy cập vào và ra ở cấp mạng con.

Ví dụ, bước ra ngoài quán cà phê và tưởng tượng rằng bạn đang ở sân bay. Tại sân bay, du khách đang cố gắng nhập cảnh vào một quốc gia khác. Bạn có thể coi khách du lịch là các gói hàng và nhân viên kiểm soát hộ chiếu là ACL mạng. Nhân viên kiểm soát hộ chiếu kiểm tra thông tin xác thực của khách du lịch khi họ nhập cảnh và xuất cảnh khỏi đất nước. Nếu một khách du lịch nằm trong danh sách được phê duyệt, họ có thể được thông qua. Tuy nhiên, nếu họ không có tên trong danh sách được phê duyệt hoặc rõ ràng nằm trong danh sách khách du lịch bị cấm thì họ không thể vào.



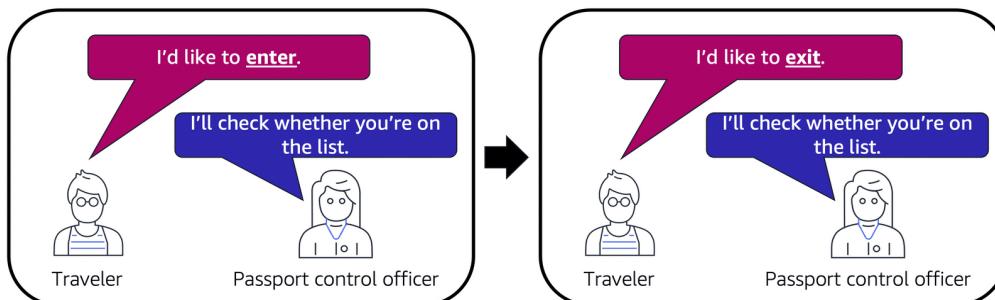
Mỗi tài khoản AWS bao gồm một ACL mạng mặc định. Khi định cấu hình VPC, bạn có thể sử dụng ACL mạng mặc định của tài khoản của mình hoặc tạo ACL mạng tùy chỉnh. Theo mặc định, ACL mạng mặc định của tài khoản của bạn cho phép tất cả lưu lượng truy cập vào và ra nhưng bạn có thể sửa đổi nó bằng cách thêm các quy tắc của riêng mình. Đối với ACL mạng tùy chỉnh, tất cả lưu lượng truy cập vào và ra đều bị từ chối cho đến khi bạn thêm quy tắc để chỉ định lưu lượng truy cập nào sẽ cho phép. Ngoài ra, tất cả các ACL mạng đều có quy tắc từ chối rõ ràng. Quy tắc này đảm bảo rằng nếu một gói không khớp với bất kỳ quy tắc nào khác trong danh sách thì gói đó sẽ bị từ chối.

## Stateless Packet Filtering

ACL mạng thực hiện lọc gói **không trạng thái**. Họ không nhớ gì cả và kiểm tra các gói đi qua ranh giới mạng con mỗi chiều: gửi đến và gửi đi.

Hãy nhớ lại ví dụ trước đây về một du khách muốn đến một quốc gia khác. Điều này tương tự như gửi yêu cầu từ phiên bản Amazon EC2 và tới internet.

Khi phản hồi gói cho yêu cầu đó quay trở lại mạng con, ACL mạng sẽ không ghi nhớ yêu cầu trước đó của bạn. ACL mạng kiểm tra phản hồi gói theo danh sách quy tắc của nó để xác định xem nên cho phép hay từ chối.



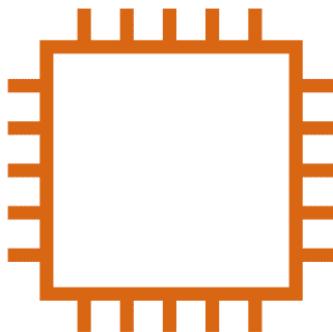
Sau khi gói vào mạng con, gói đó phải được đánh giá quyền đối với các tài nguyên trong mạng con, chẳng hạn như phiên bản Amazon EC2.

Thành phần VPC kiểm tra quyền của gói đối với phiên bản Amazon EC2 là một **nhóm bảo mật**.

## Security Groups

Nhóm bảo mật là tường lửa ảo kiểm soát lưu lượng truy cập vào và ra cho phiên bản Amazon EC2.

## Security group



## Amazon EC2 instance

Theo mặc định, nhóm bảo mật từ chối tất cả lưu lượng truy cập vào và cho phép tất cả lưu lượng truy cập ra. Bạn có thể thêm quy tắc tùy chỉnh để định cấu hình lưu lượng truy cập nào sẽ cho phép hoặc từ chối.

Trong ví dụ này, giả sử bạn đang ở trong một tòa nhà chung cư có nhân viên trực cửa chào đón khách ở sảnh. Bạn có thể coi khách như những gói hàng và người phục vụ cửa như một nhóm bảo mật. Khi khách đến, nhân viên cửa sẽ kiểm tra danh sách để đảm bảo họ có thể vào tòa nhà. Tuy nhiên, nhân viên cửa không kiểm tra lại danh sách khi khách ra khỏi tòa nhà.

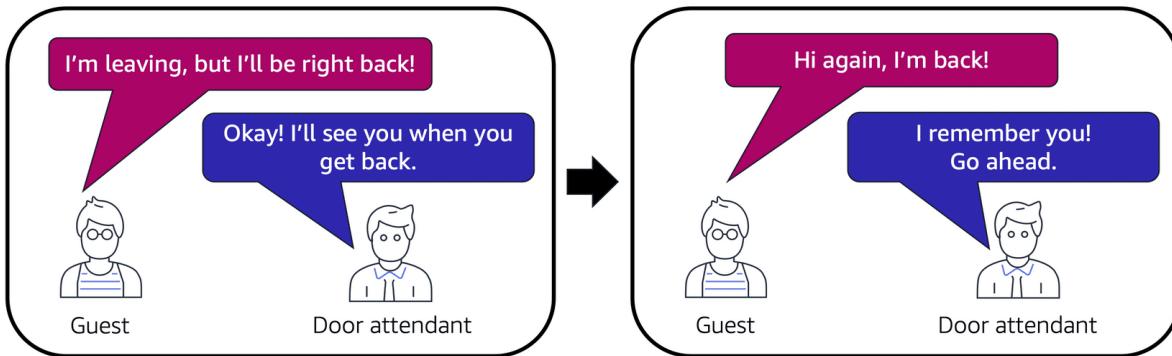
Nếu có nhiều phiên bản Amazon EC2 trong một mạng con, bạn có thể liên kết chúng với cùng một nhóm bảo mật hoặc sử dụng các nhóm bảo mật khác nhau cho từng phiên bản.

### Lọc gói trạng thái

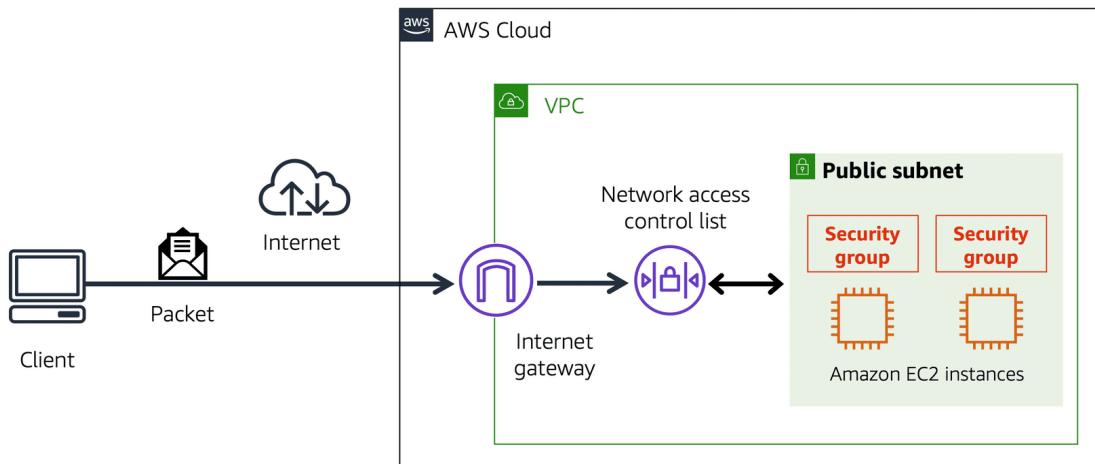
Các nhóm bảo mật thực hiện lọc gói **trạng thái**. Họ nhớ các quyết định trước đó đối với các gói tin đến.

Hãy xem xét ví dụ tương tự về việc gửi yêu cầu từ phiên bản Amazon EC2 tới internet. Khi phản hồi gói cho yêu cầu đó quay trở lại phiên bản, nhóm bảo mật sẽ ghi nhớ yêu cầu trước đó của bạn. Nhóm bảo mật cho phép phản hồi tiếp tục, bất kể quy tắc nhóm

bảo mật gửi đến.



Cả ACL network và security group đều cho phép bạn định cấu hình các quy tắc tùy chỉnh cho lưu lượng truy cập trong VPC của mình. Khi bạn tiếp tục tìm hiểu thêm về bảo mật và kết nối mạng AWS, hãy đảm bảo hiểu rõ sự khác biệt giữa ACL mạng và nhóm bảo mật.

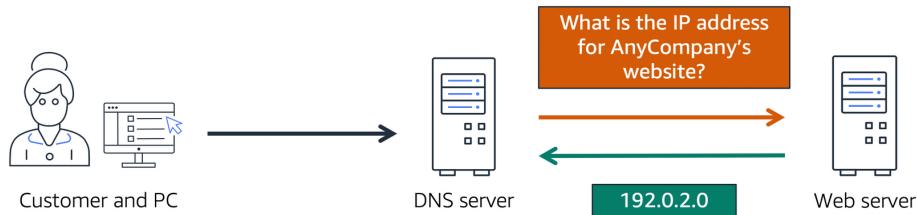


## Global Networking

### Hệ thống tên miền (DNS)

Giả sử AnyCompany có một trang web được lưu trữ trên đám mây AWS. Khách hàng nhập địa chỉ web vào trình duyệt và có thể truy cập trang web. Điều này xảy ra do độ phân giải **của Hệ thống tên miền (DNS)**. Độ phân giải DNS liên quan đến việc máy chủ DNS giao tiếp với máy chủ web.

Bạn có thể coi DNS giống như danh bạ điện thoại của Internet. Độ phân giải DNS là quá trình dịch tên miền sang địa chỉ IP.



Ví dụ: giả sử bạn muốn truy cập trang web của AnyCompany.

1. Khi bạn nhập tên miền vào trình duyệt, yêu cầu này sẽ được gửi đến máy chủ DNS.
2. Máy chủ DNS yêu cầu máy chủ web cung cấp địa chỉ IP tương ứng với trang web của AnyCompany.
3. Máy chủ web phản hồi bằng cách cung cấp địa chỉ IP cho trang web của AnyCompany, [192.0.2.0](http://192.0.2.0).

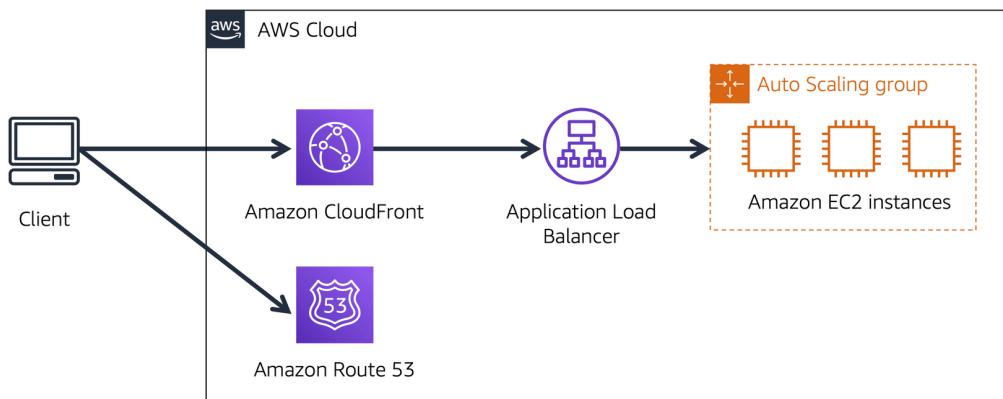
## Amazon Route 53

[\*\*Tuyến đường Amazon 53\*\*](#) là một dịch vụ web DNS. Nó cung cấp cho các nhà phát triển và doanh nghiệp một cách đáng tin cậy để định tuyến người dùng cuối đến các ứng dụng internet được lưu trữ trên AWS.

Amazon Route 53 kết nối các yêu cầu của người dùng với cơ sở hạ tầng đang chạy trong AWS (chẳng hạn như phiên bản Amazon EC2 và bộ cân bằng tải). Nó có thể định tuyến người dùng đến cơ sở hạ tầng bên ngoài AWS.

Một tính năng khác của Route 53 là khả năng quản lý bản ghi DNS cho tên miền. Bạn có thể đăng ký tên miền mới trực tiếp tại Route 53. Bạn cũng có thể chuyển bản ghi DNS cho các tên miền hiện có do các nhà đăng ký tên miền khác quản lý. Điều này cho phép bạn quản lý tất cả các tên miền của mình ở một vị trí duy nhất.

**Ví dụ: Cách Amazon Route 53 và Amazon CloudFront phân phối nội dung**



Giả sử ứng dụng của AnyCompany đang chạy trên một số phiên bản Amazon EC2. Các phiên bản này nằm trong nhóm Auto Scaling gắn với Cân bằng tải ứng dụng.

1. Khách hàng yêu cầu dữ liệu từ ứng dụng bằng cách truy cập trang web của AnyCompany.
2. Amazon Route 53 sử dụng độ phân giải DNS để xác định địa chỉ IP tương ứng của [AnyCompany.com](http://AnyCompany.com), [192.0.2.0](http://192.0.2.0). Thông tin này sẽ được gửi lại cho khách hàng.
3. Yêu cầu của khách hàng được gửi đến vị trí biên gần nhất thông qua Amazon CloudFront.
4. Amazon CloudFront kết nối với Cân bằng tải ứng dụng để gửi gói đến đến phiên bản Amazon EC2.

## Instance Stores and Amazon Elastic Block Store (Amazon EBS)

Khi bạn đang sử dụng Amazon EC2 để chạy các ứng dụng kinh doanh của bạn, những ứng dụng đó cần quyền truy cập vào CPU, bộ nhớ, mạng và lưu trữ. **EC2 Instance** cung cấp cho bạn quyền truy cập vào tất cả những thành phần khác nhau đó và ngay bây giờ, hãy tập trung vào quyền truy cập lưu trữ. Khi các ứng dụng chạy, chúng sẽ chỉ khi cần quyền truy cập vào **block level storage** (bộ lưu trữ cấp khối).

Bạn có thể nghĩ đến việc lưu trữ cấp khối là nơi lưu trữ các tập tin, một tập tin là một chuỗi byte được lưu trữ thành các khối trên đĩa. Khi một tập tin được cập nhật, toàn bộ chuỗi khối không bị ghi đè. Thay vào đó, nó chỉ cập nhật những phần thay đổi. Điều này làm cho nó trở thành một loại lưu trữ hiệu quả khi làm việc với các ứng dụng như cơ sở

dữ liệu, phần mềm doanh nghiệp hoặc hệ thống tập tin. Khi bạn sử dụng máy tính xách tay hoặc máy tính cá nhân, bạn đang truy cập vào bộ lưu trữ cấp khối. Tất cả lưu trữ cấp khối là trong trường hợp này là ổ cứng của bạn.

Phiên bản EC2 cũng có ổ cứng. Có một vài loại khác nhau. Khi bạn khởi chạy một phiên bản EC2, tùy thuộc vào loại phiên bản EC2 bạn đã khởi chạy, nó có thể cung cấp cho bạn bộ nhớ cục bộ được gọi là **instance store volumes** (khối lượng lưu trữ phiên bản). Các tập này được gắn vật lý vào máy chủ mà phiên bản EC2 của bạn đang chạy trên đó, và bạn có thể ghi vào nó giống như một ổ cứng bình thường. Điều hấp dẫn ở đây là vì tập này được gắn vào máy chủ vật lý cơ bản, nếu bạn **Stop** hoặc **Terminate** phiên bản EC2 của mình, tất cả dữ liệu được ghi vào **instance store volumes** sẽ bị xóa. Lý do cho điều này là nếu bạn **Start** phiên bản của mình từ trạng thái dừng, có khả năng là phiên bản EC2 sẽ khởi động trên máy chủ khác, một máy chủ nơi khối lượng đó không tồn tại. Hãy nhớ rằng, các phiên bản EC2 là máy ảo và do đó máy chủ cơ bản có thể thay đổi giữa việc dừng và bắt đầu một thể hiện. Vì tính chất phù du hay tạm thời này về khối lượng cửa hàng ví dụ, chúng hữu ích trong những tình huống mà bạn có thể làm mất dữ liệu được ghi vào ổ đĩa, chẳng hạn như các tập tin tạm thời, dữ liệu đầu, và dữ liệu có thể dễ dàng được tái tạo mà không gây hậu quả. Được rồi. Tôi bảo bạn đừng viết dữ liệu quan trọng vào ổ đĩa kèm với các phiên bản EC2. Tôi chắc rằng điều đó nghe có vẻ hơi đáng sợ vì rõ ràng, bạn sẽ cần một nơi để ghi dữ liệu liên tục nằm ngoài vòng đori của phiên bản EC2. Bạn không muốn toàn bộ cơ sở dữ liệu của mình nhận được bị xóa mỗi khi bạn dừng phiên bản EC2. Đừng lo lắng, đây là nơi có dịch vụ được gọi là **Amazon Elastic Block Store** (Cửa hàng khối đòn hồi của Amazon), hoặc EBS, sẽ phát huy tác dụng. Với EBS, bạn có thể tạo ổ cứng ảo mà chúng tôi gọi là Các ổ đĩa EBS mà bạn có thể đính kèm vào phiên bản EC2 của mình. Đây là những ổ đĩa riêng biệt từ khối lượng lưu trữ phiên bản cục bộ và chúng không bị ràng buộc trực tiếp với máy chủ mà EC2 của bạn đang chạy. Điều này có nghĩa là dữ liệu bạn ghi vào ổ đĩa EBS có thể tồn tại giữa các điểm dừng và bắt đầu của phiên bản EC2. Khối lượng EBS có đủ loại và kích cỡ khác nhau. Cách thức hoạt động của nó là bạn xác định kích thước, loại và cấu hình của ổ đĩa bạn cần. Cung cấp âm lượng và sau đó đính kèm nó vào phiên bản EC2 của bạn. Từ đó, bạn có thể cấu hình ứng dụng của bạn để viết vào âm lượng và bạn có thể bắt đầu. Nếu bạn dừng rồi khởi động phiên bản EC2 này, dữ liệu trong ổ đĩa vẫn còn. Vì trường hợp sử dụng cho khối lượng EBS là phải có một ổ cứng bền bỉ mà ứng dụng của bạn có thể ghi vào, điều quan trọng là bạn phải sao lưu dữ liệu đó. EBS cho phép bạn lấy sao lưu gia tăng dữ liệu của bạn được gọi là **snapshots** (ảnh chụp nhanh). Điều rất quan trọng là bạn phải thực hiện ảnh chụp nhanh thường xuyên của khối lượng EBS của bạn. Bằng cách

này, nếu một ổ đĩa bị hỏng, bạn chưa bị mất dữ liệu và bạn có thể khôi phục dữ liệu đó từ **snapshots**.

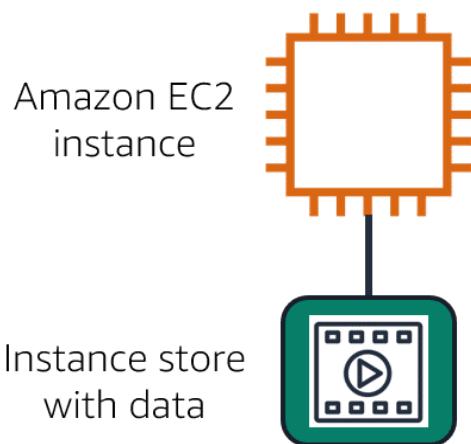
### Instance stores

Block-level storage volumes hoạt động giống như ổ cứng vật lý.

MỘT **instance store** cung cấp bộ nhớ cấp khối tạm thời cho phiên bản Amazon EC2.

Kho lưu trữ phiên bản là bộ lưu trữ đĩa được gắn vật lý vào máy tính chủ cho phiên bản EC2 và do đó có cùng tuổi thọ với phiên bản. Khi phiên bản bị chấm dứt, bạn sẽ mất mọi dữ liệu trong kho lưu trữ phiên bản.

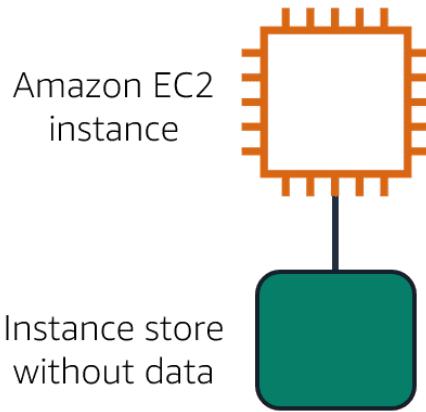
**An Amazon EC2 instance with an attached instance store is running.**



**The instance is stopped or terminated.**



**All data on the attached instance store is deleted.**

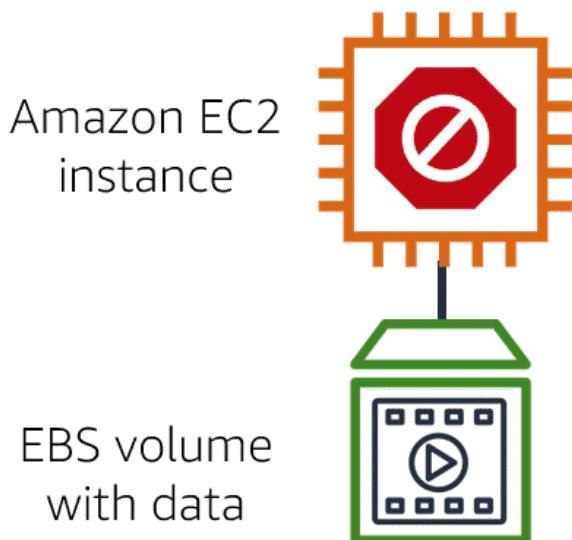


### **Amazon Elastic Block Storage (Amazon EBS)**

Cửa hàng khối đòn hồi Amazon (Amazon EBS) là dịch vụ cung cấp khối lượng lưu trữ cấp khối mà bạn có thể sử dụng với các phiên bản Amazon EC2. Nếu bạn dừng hoặc chấm dứt một phiên bản Amazon EC2 thì tất cả dữ liệu trên ổ đĩa EBS đính kèm vẫn có sẵn.

Để tạo ổ đĩa EBS, bạn xác định cấu hình (chẳng hạn như kích thước và loại ổ đĩa) và cung cấp cấu hình đó. Sau khi bạn tạo ổ đĩa EBS, ổ đĩa này có thể đính kèm vào phiên bản Amazon EC2.

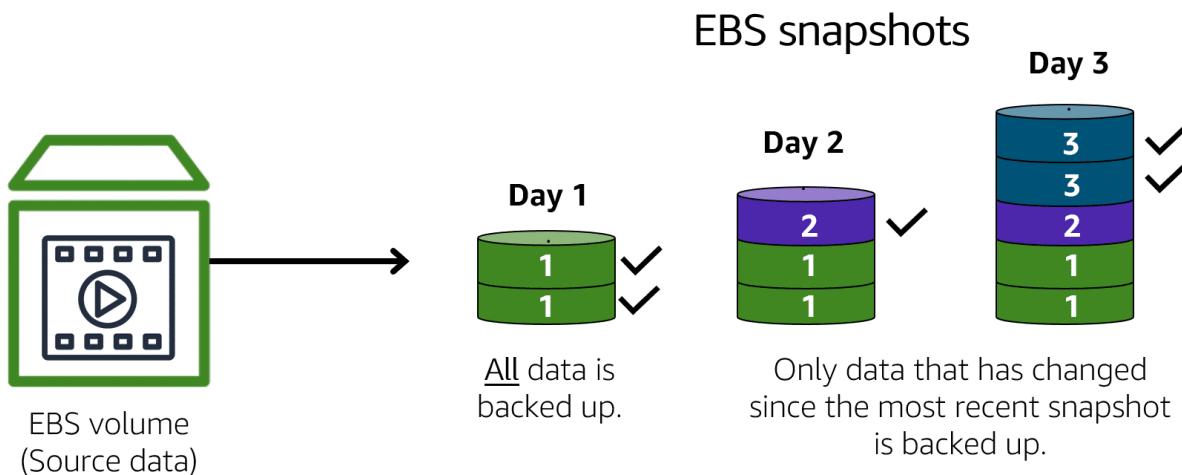
Vì ổ đĩa EBS dành cho dữ liệu cần được duy trì nên việc sao lưu dữ liệu là rất quan trọng. Bạn có thể thực hiện sao lưu gia tăng các ổ đĩa EBS bằng cách tạo bản kết xuất nhanh Amazon EBS.



### **Amazon EBS Snapshots**

MỘT **EBS Snapshots** là một bản sao lưu gia tăng. Điều này có nghĩa là bản sao lưu đầu tiên của ổ đĩa sẽ sao chép tất cả dữ liệu. Đối với các bản sao lưu tiếp theo, chỉ các khối dữ liệu đã thay đổi kể từ ảnh chụp nhanh gần đây nhất mới được lưu.

Các bản sao lưu gia tăng khác với các bản sao lưu đầy đủ, trong đó tất cả dữ liệu trong ổ lưu trữ sẽ được sao chép mỗi khi xảy ra bản sao lưu. Bản sao lưu đầy đủ bao gồm dữ liệu không thay đổi kể từ lần sao lưu gần đây nhất.



## Amazon Simple Storage Service (Amazon S3)

Hầu hết các doanh nghiệp đều có dữ liệu cần được lưu trữ ở đâu đó. Đối với quán cà phê, đây có thể là biên lai, hình ảnh, Excel bảng tính, video đào tạo nhân viên và thậm chí cả tệp văn bản, trong số những người khác. Việc lưu trữ các tệp này là lúc **Amazon S3** trở nên hữu ích vì đó là kho lưu trữ dữ liệu cho phép bạn lưu trữ và truy xuất một lượng dữ liệu hầu như không giới hạn ở mọi quy mô. Dữ liệu được lưu trữ dưới dạng đối tượng, nhưng thay vì lưu trữ chúng trong một thư mục tệp, bạn lưu trữ chúng trong cái mà chúng tôi gọi là nhóm. Hãy nghĩ về một tập tin nằm trên ổ cứng của bạn. Đó là một đồ vật. Và nghĩ về một thư mục tập tin. Đó là một cái **bucket**. Sau đó, bạn có thể tạo quyền để giới hạn những người có thể xem hoặc thậm chí truy cập các đối tượng. Và bạn thậm chí có thể sắp xếp dữ liệu giữa các tầng khác nhau. Các tầng này cung cấp cơ chế cho các trường hợp sử dụng bộ nhớ khác nhau, chẳng hạn như dữ liệu cần được truy cập thường xuyên so sánh để kiểm tra dữ liệu cần được lưu giữ trong vài năm.

Một cách hữu ích khác để sử dụng Amazon S3 là lưu trữ trang web tĩnh, trong đó trang web tĩnh là tập hợp các tệp HTML và mỗi tệp giống như một trang vật lý của trang

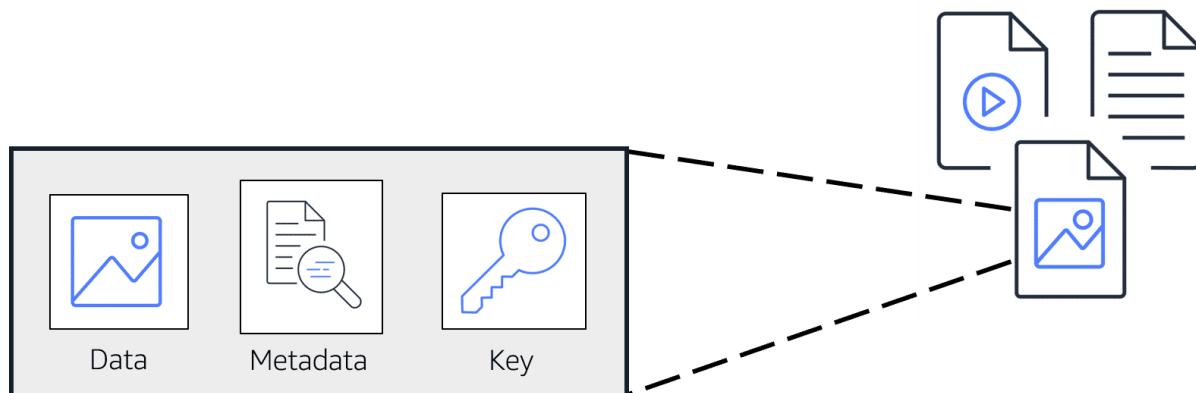
web thực tế. Bạn có thể thực hiện việc này bằng cách tải lên tất cả HTML, tệp nội dung web, v.v. vào một nhóm rồi kiểm tra một hộp để lưu trữ nó như một trang web tĩnh. Sau đó, bạn có thể nhập URL của nhóm và bấm! Trang web tức thì. Và chúng tôi nói tĩnh, nhưng điều đó không có nghĩa là bạn không thể có hình ảnh động và các bộ phận chuyển động đến trang web của bạn. Đó là một cách khá tuyệt vời để bắt đầu blog cá nhân đó.

Nhưng đó là những chính sách bạn có thể tạo để có thể tự động di chuyển dữ liệu giữa các tầng. Ví dụ: giả sử chúng ta cần giữ một đối tượng trong S3 Standard trong 90 ngày và sau đó chúng tôi muốn chuyển nó sang S3 Standard-IA trong 30 ngày tiếp theo. Sau tổng cộng 120 ngày, chúng tôi muốn chuyển nó sang S3 Glacier Flexible Retrieval.

Với Lifecycle policies, bạn tạo cấu hình mà không thay đổi mã ứng dụng của bạn và nó sẽ thực hiện những động thái đó sẽ tự động dành cho bạn. Đây là một ví dụ khác về dịch vụ AWS được quản lý, giúp thực hiện điều đó giảm gánh nặng cho bạn để bạn có thể tập trung hơn vào nhu cầu kinh doanh của mình.

## Object Storage

Trong **lưu trữ đối tượng**, mỗi đối tượng bao gồm dữ liệu, siêu dữ liệu và khóa. Dữ liệu có thể là hình ảnh, video, tài liệu văn bản hoặc bất kỳ loại tệp nào khác. Siêu dữ liệu chứa thông tin về dữ liệu là gì, dữ liệu đó được sử dụng như thế nào, kích thước đối tượng, v.v. Khóa của một đối tượng là mã định danh duy nhất của nó.



Hãy nhớ lại rằng khi bạn sửa đổi một tệp trong bộ lưu trữ khối, chỉ những phần được thay đổi mới được cập nhật. Khi một tệp trong bộ lưu trữ đối tượng được sửa đổi, toàn bộ đối tượng sẽ được cập nhật.

## Amazon Simple Storage Service (Amazon S3)

**Dịch vụ lưu trữ đơn giản của Amazon (Amazon S3)** là một dịch vụ cung cấp lưu trữ cấp đối tượng. Amazon S3 lưu trữ dữ liệu dưới dạng đối tượng trong nhóm.

Bạn có thể tải bất kỳ loại tệp nào lên Amazon S3, chẳng hạn như hình ảnh, video, tệp văn bản, v.v. Ví dụ: bạn có thể sử dụng Amazon S3 để lưu trữ tệp sao lưu, tệp phương tiện cho trang web hoặc tài liệu lưu trữ. Amazon S3 cung cấp không gian lưu trữ không giới hạn. Kích thước tệp tối đa cho một đối tượng trong Amazon S3 là 5 TB.

Khi tải tệp lên Amazon S3, bạn có thể đặt quyền để kiểm soát mức độ hiển thị và quyền truy cập vào tệp đó. Bạn cũng có thể sử dụng tính năng lập phiên bản của Amazon S3 để theo dõi các thay đổi đối với đối tượng của mình theo thời gian.

## Amazon S3 Storage Classes

Với Amazon S3, bạn chỉ trả tiền cho những gì bạn sử dụng. Bạn có thể chọn từ [một loạt các lớp lưu trữ](#) để lựa chọn phù hợp với nhu cầu kinh doanh và chi phí của bạn. Khi chọn lớp lưu trữ Amazon S3, hãy xem xét hai yếu tố sau:

- Tần suất bạn dự định truy xuất dữ liệu của mình
- Bạn cần dữ liệu của mình sẵn có như thế nào

## Amazon S3 Standard

- Được thiết kế cho dữ liệu được truy cập thường xuyên
- Lưu trữ dữ liệu trong tối thiểu ba Vùng sẵn sàng

Amazon S3 Standard cung cấp tính sẵn sàng cao cho các đối tượng. Điều này làm cho nó trở thành một lựa chọn tốt cho nhiều trường hợp sử dụng, chẳng hạn như trang web, phân phối nội dung và phân tích dữ liệu. Amazon S3 Standard có chi phí cao hơn so với các lớp lưu trữ khác dành cho dữ liệu được truy cập không thường xuyên và lưu trữ lưu trữ.

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

- Lý tưởng cho dữ liệu được truy cập không thường xuyên
- Tương tự như Amazon S3 Standard nhưng có giá lưu trữ thấp hơn và giá truy xuất cao hơn

Amazon S3 Standard-IA lý tưởng cho dữ liệu được truy cập không thường xuyên nhưng yêu cầu độ sẵn sàng cao khi cần. Cả Amazon S3 Standard và Amazon S3 Standard-IA đều lưu trữ dữ liệu ở tối thiểu ba Vùng sẵn sàng. S3 Standard-IA cung cấp mức độ khả dụng tương tự như Amazon S3 Standard nhưng có giá lưu trữ thấp hơn và giá truy xuất cao hơn.

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

- Lưu trữ dữ liệu trong một Vùng sẵn sàng duy nhất

- Có giá lưu trữ thấp hơn Amazon S3 Standard-IA

So với Amazon S3 Standard và Amazon S3 Standard-IA lưu trữ dữ liệu ở tối thiểu ba Vùng sẵn sàng, Amazon S3 One Zone-IA lưu trữ dữ liệu trong một Vùng sẵn sàng duy nhất. Điều này làm cho nó trở thành một lớp lưu trữ tốt để xem xét nếu áp dụng các điều kiện sau:

- Bạn muốn tiết kiệm chi phí lưu trữ.
- Bạn có thể dễ dàng tái tạo dữ liệu của mình trong trường hợp Vùng sẵn sàng bị lỗi.

### **Amazon S3 Intelligent-Tiering**

- Lý tưởng cho dữ liệu có kiểu truy cập không xác định hoặc đang thay đổi
- Yêu cầu một khoản phí giám sát và tự động hóa hàng tháng nhỏ cho mỗi đối tượng

Trong lớp lưu trữ Phân bậc thông minh của Amazon S3, Amazon S3 giám sát các kiểu truy cập của đối tượng. Nếu bạn không truy cập một đối tượng trong 30 ngày liên tiếp, Amazon S3 sẽ tự động chuyển đổi từ truy cập thường xuyên sang Amazon S3 Standard-IA. Nếu bạn truy cập một đối tượng ở bậc truy cập thường xuyên, Amazon S3 sẽ tự động chuyển đổi từ truy cập thường xuyên sang Amazon S3 Standard.

### **Amazon S3 Glacier Instant Retrieval**

- Hoạt động tốt đối với dữ liệu được lưu trữ yêu cầu truy cập ngay lập tức
- Có thể truy xuất đối tượng trong vòng vài mili giây

Khi bạn quyết định giữa các tùy chọn lưu trữ lưu trữ, hãy cân nhắc xem bạn phải truy xuất các đối tượng đã lưu trữ nhanh như thế nào. Bạn có thể truy xuất các đối tượng được lưu trữ trong lớp lưu trữ Truy xuất tức thì của Amazon S3 Glacier trong vòng mili giây, với hiệu suất tương tự như Amazon S3 Standard.

### **Amazon S3 Glacier Flexible Retrieval**

- Bộ lưu trữ chi phí thấp được thiết kế để lưu trữ dữ liệu
- Có thể lấy đồ vật trong vòng vài phút đến vài giờ

Truy xuất linh hoạt Amazon S3 Glacier là lớp lưu trữ có chi phí thấp lý tưởng cho việc lưu trữ dữ liệu. Ví dụ: bạn có thể sử dụng lớp lưu trữ này để lưu trữ hồ sơ khách hàng đã lưu trữ hoặc các tệp ảnh và video cũ hơn.

### **Amazon S3 Glacier Deep Archive**

- Lớp lưu trữ đối tượng có chi phí thấp nhất lý tưởng để lưu trữ
- Có thể lấy lại đồ vật trong vòng 12 giờ

Amazon S3 Deep Archive hỗ trợ lưu giữ lâu dài và bảo quản kỹ thuật số đối với dữ liệu có thể được truy cập một hoặc hai lần trong một năm. Lớp lưu trữ này là bộ lưu trữ có chi phí thấp nhất trên đám mây AWS, với thời gian truy xuất dữ liệu từ 12 đến 48 giờ. Tất cả các đối tượng từ lớp lưu trữ này đều được sao chép và lưu trữ trên ít nhất ba vùng sẵn sàng phân tán về mặt địa lý.

### **Amazon S3 Outposts**

- Tạo vùng lưu trữ S3 trên Amazon S3 Outposts
- Giúp truy xuất, lưu trữ và truy cập dữ liệu trên AWS Outposts dễ dàng hơn

Amazon S3 Outposts cung cấp kho lưu trữ đối tượng cho môi trường AWS Outposts tại chỗ của bạn. Amazon S3 Outposts được thiết kế để lưu trữ dữ liệu lâu dài và dự phòng trên nhiều thiết bị và máy chủ trên Outposts của bạn. Nó hoạt động tốt cho các khối lượng công việc có yêu cầu về nơi lưu trữ dữ liệu cục bộ phải đáp ứng nhu cầu khắt khe về hiệu suất bằng cách giữ dữ liệu gần với các ứng dụng tại chỗ.

## **Comparing Amazon EBS and Amazon S3**

Giả sử bạn đang chạy một trang web phân tích ảnh nơi người dùng tải lên ảnh của bản thân họ và ứng dụng của bạn tìm thấy những con vật trông giống chúng. Bạn có khả năng có hàng triệu bức ảnh động vật tất cả đều cần được lập chỉ mục và có thể được hàng ngàn người xem cùng một lúc. Đây là trường hợp sử dụng hoàn hảo cho S3. S3 đã được kích hoạt web. Mọi đối tượng đều đã có một URL mà bạn có thể kiểm soát quyền truy cập đối với những người có thể xem hoặc quản lý hình ảnh. Nó được phân bố theo vùng, có nghĩa là nó có độ bền là 11. Không cần phải lo lắng về chiến lược sao lưu. S3 là chiến lược dự phòng của bạn. Cộng với việc tiết kiệm chi phí là đáng kể chạy quá mức tải lưu trữ tương tự trên EBS, với lợi thế bổ sung là không có máy chủ. Không cần có phiên bản Amazon EC2. Có vẻ như S3 là mùa đông của bạn giám khảo cho vòng này.

Vạn có một tệp video 80 gigabyte mà bạn đang thực hiện chỉnh sửa. Để biết lớp lưu trữ tốt nhất ở đây, chúng ta cần hiểu sự khác biệt giữa lưu trữ đối tượng và lưu trữ khối. Bộ lưu trữ đối tượng xử lý mọi tập tin như một đối tượng hoàn toàn rời rạc. Ngày giờ, điều này thật tuyệt vời cho tài liệu và hình ảnh, và các tập tin video có được tải lên và sử dụng dưới dạng toàn bộ đối tượng. Nhưng mỗi khi có sự thay đổi về đối tượng, bạn phải tải lại toàn bộ tập tin. Không có bản cập nhật Delta. Khối lưu trữ chia nhỏ các tệp đó thành các bộ phận hoặc khối thành phần nhỏ. Điều này có nghĩa là với tệp 80 gigabyte đó, khi bạn thực hiện chỉnh sửa một cảnh trong bộ phim và lưu lại sự thay đổi đó, công cụ chỉ cập nhật các khối nơi các bit đó tồn tại. Nếu bạn đang thực hiện nhiều chỉnh sửa vi mô bằng EBS, Elastic Block Storage là trường hợp sử dụng hoàn hảo. Nếu

bạn đang sử dụng S3, mỗi lần bạn lưu các thay đổi,hệ thống sẽ phải tải lên tất cả 80 gigabyte,toàn bộ điều đó mọi lúc.EBS thắng rõ ràng ở vòng 2.

Điều này có nghĩa là nếu bạn đang sử dụng các đối tượng hoàn chỉnh hoặc chỉ thỉnh thoảng thay đổi,S3 đã chiến thắng.Nếu bạn đang đọc phức tạp,viết các hàm thay đổi thì hoàn toàn,EBS là người chiến thắng loại trực tiếp của bạn.

## Amazon Elastic File System (Amazon EFS)

**Amazon Elastic File System EFS** là một hệ thống tập tin được quản lý.Nó cực kỳ phổ biến đối với các doanh nghiệp có hệ thống tập tin được chia sẻ trên các ứng dụng của họ.Ví dụ: bạn có thể có nhiều máy chủ chạy phân tích trên quy mô lớn lượng dữ liệu được lưu trữ trong một hệ thống tập tin chia sẻ.Dữ liệu này theo truyền thống đã được lưu trữ tại cơ sở.Trong trung tâm dữ liệu tại chỗ này, bạn sẽ phải đảm bảo rằng bộ nhớ bạn có thể theo kịp lượng dữ liệu bạn đang lưu trữ.Đảm bảo đã thực hiện sao lưu và dữ liệu được lưu trữ dự phòng,cũng như quản lý tất cả các máy chủ lưu trữ dữ liệu đó.

May mắn thay, với AWS, bạn không cần phải lo lắng về việc mua tất cả phần cứng và giữ cho toàn bộ hệ thống tập tin chạy từ quan điểm hoạt động.Với EFS, bạn có thể giữ nguyên các hệ thống tệp hiện có, nhưng AWS của tôi thực hiện tất cả các công việc nặng nhọc trong việc mở rộng quy mô và sao chép.

### File Storage

Trong **lưu trữ tệp**, nhiều máy khách (chẳng hạn như người dùng, ứng dụng, máy chủ, v.v.) có thể truy cập dữ liệu được lưu trữ trong các thư mục tệp dùng chung. Theo cách tiếp cận này, máy chủ lưu trữ sử dụng lưu trữ khối với hệ thống tệp cục bộ để sắp xếp các tệp. Khách hàng truy cập dữ liệu thông qua đường dẫn tệp.

So với lưu trữ khối và lưu trữ đối tượng, lưu trữ tệp lý tưởng cho các trường hợp sử dụng trong đó một số lượng lớn dịch vụ và tài nguyên cần truy cập cùng một dữ liệu cùng một lúc.

**Hệ thống tệp đòn hồi của Amazon (Amazon EFS)** là một hệ thống tệp có khả năng mở rộng được sử dụng với các dịch vụ Đám mây AWS và tài nguyên tại chỗ. Khi bạn thêm và xóa tệp, Amazon EFS sẽ tự động tăng và thu nhỏ. Nó có thể mở rộng quy mô lên tới petabyte theo yêu cầu mà không làm gián đoạn ứng dụng.

### So sánh Amazon EBS và Amazon EFS

## **Amazon EBS**

- Ổ đĩa Amazon EBS lưu trữ dữ liệu trong một Vùng sẵn sàng **duy nhất**.
- Để gắn phiên bản Amazon EC2 vào ổ đĩa EBS, cả phiên bản Amazon EC2 và ổ đĩa EBS phải nằm trong cùng một Vùng sẵn sàng.

Nếu bạn cung cấp ổ đĩa EBS 2 terabyte và lắp đầy nó, nó không tự động mở rộng quy mô để cung cấp cho bạn nhiều dung lượng hơn. Vậy đó là EBS.

## **Amazon EFS**

- Amazon EFS là một dịch vụ khu vực. Nó lưu trữ dữ liệu trong và trên **nhiều** Vùng sẵn sàng.
- Bộ lưu trữ trùng lặp cho phép bạn truy cập dữ liệu đồng thời từ tất cả các Vùng sẵn sàng trong Khu vực nơi đặt hệ thống tệp. Ngoài ra, máy chủ tại chỗ có thể truy cập Amazon EFS bằng AWS Direct Connect.

Amazon EFS có thể có nhiều phiên bản đọc và ghi từ nó tại cùng một lúc, nhưng nó không chỉ là một ổ cứng trống mà bạn có thể ghi vào. Nó là một hệ thống tập tin thực sự cho Linux.

# **Amazon Relational Database Service (Amazon RDS)**

## **Amazon Relational Database Service**

**Dịch vụ cơ sở dữ liệu quan hệ của Amazon (Amazon RDS)** là dịch vụ cho phép bạn chạy cơ sở dữ liệu quan hệ trên đám mây AWS.

Amazon RDS là dịch vụ được quản lý có chức năng tự động hóa các tác vụ như cung cấp phần cứng, thiết lập cơ sở dữ liệu, vá lỗi và sao lưu. Với những khả năng này, bạn có thể mất ít thời gian hơn để hoàn thành các nhiệm vụ quản trị và có nhiều thời gian hơn để sử dụng dữ liệu để đổi mới ứng dụng của mình. Bạn có thể tích hợp Amazon RDS với các dịch vụ khác để đáp ứng nhu cầu vận hành và kinh doanh của mình, chẳng hạn như sử dụng AWS Lambda để truy vấn cơ sở dữ liệu của bạn từ một ứng dụng phi máy chủ. Amazon RDS cung cấp một số tùy chọn bảo mật khác nhau. Nhiều công cụ cơ sở dữ liệu Amazon RDS cung cấp tính năng mã hóa ở trạng thái lưu trữ (bảo vệ dữ liệu khi dữ liệu được lưu trữ) và mã hóa khi truyền tải (bảo vệ dữ liệu trong khi dữ liệu được gửi và nhận).

Chúng bao gồm vá lỗi tự động, sao lưu, dự phòng, chuyển đổi dự phòng, khắc phục sự cố,tất cả những điều đó bạn thường phải tự mình quản lý. Điều này làm cho nó trở nên cực kỳ tốn kém và không dễ dàng cho khách hàng AWS vì nó cho phép bạn tập trung vào vấn đề kinh doanh và không duy trì cơ sở dữ liệu.

## **Amazon RDS database engines**

Amazon RDS có sẵn trên sáu công cụ cơ sở dữ liệu, giúp tối ưu hóa bộ nhớ, hiệu năng hoặc đầu vào/đầu ra (I/O). Các công cụ cơ sở dữ liệu được hỗ trợ bao gồm:

- Amazon Aurora
- PostgreSQL
- MySQL
- MariaDB
- Cơ sở dữ liệu Oracle
- Máy chủ Microsoft SQL

Nếu bạn là quản trị viên cơ sở dữ liệu, có thể khá tốn thời gian và khó khăn. Làm cách nào để chúng tôi giúp bạn dễ dàng hơn nữa chạy khôi phục công việc cơ sở dữ liệu trên đám mây? Chà, chúng ta đi xa hơn và có họ di chuyển hoặc triển khai sang Amazon Aurora, đó là tùy chọn cơ sở dữ liệu quan hệ được quản lý tốt nhất của chúng tôi và có hai dạng, MySQL và PostgreSQL, và giá của nó là một phần mười chi phí của cơ sở dữ liệu cấp thương mại. Đó là một cơ sở dữ liệu khá hiệu quả về mặt chi phí.

## **Amazon Aurora**

**Amazon Aurora** là một cơ sở dữ liệu quan hệ cấp doanh nghiệp. Nó tương thích với cơ sở dữ liệu quan hệ MySQL và PostgreSQL. Nó nhanh hơn tới năm lần so với cơ sở dữ liệu MySQL tiêu chuẩn và nhanh hơn tới ba lần so với cơ sở dữ liệu PostgreSQL tiêu chuẩn.

Amazon Aurora giúp giảm chi phí cơ sở dữ liệu của bạn bằng cách giảm các hoạt động đầu vào/đầu ra (I/O) không cần thiết, đồng thời đảm bảo rằng tài nguyên cơ sở dữ liệu của bạn vẫn đáng tin cậy và sẵn có.

Hãy cân nhắc sử dụng Amazon Aurora nếu khôi phục công việc của bạn yêu cầu độ sẵn sàng cao. Nó sao chép sáu bản sao dữ liệu của bạn trên ba Vùng sẵn sàng và liên tục sao lưu dữ liệu của bạn vào Amazon S3.

Những lợi ích khác là những thứ như dữ liệu của bạn được sao chép trên khắp các cơ sở, bạn có sáu bản sao tại bất kỳ thời điểm nào. Bạn cũng có thể triển khai tối đa 15 bản sao chỉ có quyền đọc, bạn có thể giảm tải số lần đọc và mở rộng hiệu suất của mình. Ngoài ra, còn có các bản sao lưu liên tục vào S3 để bạn luôn có bản sao lưu sẵn.

sàng để khôi phục.Bạn cũng nhận được sự phục hồi tại thời điểm,bạn có thể khôi phục dữ liệu từ một khoảng thời gian cụ thể.

# Amazon DynamoDB

## Amazon DynamoDB

[Amazon DynamoDB](#) là một dịch vụ cơ sở dữ liệu khóa-giá trị. Nó mang lại hiệu suất một phần nghìn giây ở mọi quy mô.

### Không có máy chủ

- DynamoDB không có máy chủ, nghĩa là bạn không phải cung cấp, vá lỗi hoặc quản lý máy chủ.
- Bạn cũng không phải cài đặt, bảo trì hoặc vận hành phần mềm.

### Tự động chia tỷ lệ

- Khi kích thước cơ sở dữ liệu của bạn tăng hoặc giảm, DynamoDB sẽ tự động điều chỉnh quy mô để điều chỉnh những thay đổi về công suất trong khi vẫn duy trì hiệu suất ổn định.
- Điều này làm cho nó trở thành lựa chọn phù hợp cho các trường hợp sử dụng đòi hỏi hiệu suất cao trong khi mở rộng quy mô.

DynamoDB là cơ sở dữ liệu phi quan hệ.Cơ sở dữ liệu phi quan hệ có xu hướng có các lược đồ linh hoạt đơn giản, việc đặt các lược đồ cứng nhắc không phức tạp ra nhiều bảng có liên quan đến nhau.Với DynamoDB, bạn có thể thêm và xóa thuộc tính khỏi các mục trong bảng bất kỳ lúc nào.Không phải mọi mục trong bảng phải có cùng thuộc tính.Điều này rất tốt cho các tập dữ liệu có một số biến thể từ mục này sang mục khác.Vì sự linh hoạt này, bạn không thể chạy các truy vấn SQL phức tạp trên đó.Thay vào đó, bạn sẽ viết các truy vấn dựa trên một tập hợp con nhỏ các thuộc tính được chỉ định làm khóa.Vì điều này, các truy vấn mà bạn chạy trên cơ sở dữ liệu không quan hệ có xu hướng đơn giản hơn và tập trung vào một tập hợp các mục từ một bảng,không phải truy vấn trải rộng trên nhiều bảng.Mẫu truy vấn này, cùng với các yếu tố khác, bao gồm cả cách hệ thống cơ bản được thiết kế, cho phép DynamoDB hoạt động rất nhanh về thời gian đáp ứng và khả năng mở rộng cao.Những điều cần ghi nhớ. DynamoDB là một cơ sở dữ liệu NoSQL không quan hệ.Nó được xây dựng có mục đích, nghĩa là nó có các trường hợp sử dụng cụ thể,và nó không phù hợp nhất cho mọi khối lượng công việc hiện có.Nó có

thời gian phản hồi tính bằng mili giây, được quản lý hoàn toàn và có khả năng mở rộng cao.

## Amazon Redshift

Cơ sở dữ liệu có thể xử lý hàng nghìn giao dịch mỗi giây, lưu trữ có tính sẵn sàng cao và độ bền cao. Nhưng đôi khi chúng tôi có nhu cầu kinh doanh nằm ngoài những gì đang diễn ra hiện tại. Nhưng cơ sở dữ liệu hiện đại được thiết kế cho truy vấn và nhập thời gian thực tốc độ cao. Có thể không phù hợp nhất. Hầu hết các cơ sở dữ liệu quan hệ có xu hướng hoạt động tốt ở những khả năng nhất định, nó thực sự lưu trữ bao nhiêu nội dung. Vấn đề với dữ liệu phân tích lịch sử trả lời các câu hỏi như thế nào. Trên thực tế, với công nghệ đo từ xa hiện đại và sự bùng nổ của IoT, khối lượng dữ liệu sẽ áp đảo ngay cả cơ sở dữ liệu quan hệ truyền thống mạnh nhất, nó sẽ trở nên tồi tệ hơn. Không chỉ khối lượng mà sự đa dạng của dữ liệu cũng có thể là một vấn đề. Một truy vấn đối với nhiều cơ sở dữ liệu nghe có vẻ hay nhưng cơ sở dữ liệu truyền thống không xử lý chúng dễ dàng.

**Dataware house** được thiết kế đặc biệt cho loại dữ liệu lớn này nơi bạn đang xem xét các phân tích lịch sử như trái ngược với phân tích hoạt động. Kho dữ liệu được thiết kế đặc biệt cho loại dữ liệu lớn này nơi bạn đang xem xét các phân tích lịch sử như trái ngược với phân tích hoạt động. Bây giờ hãy nói rõ ràng, về mặt lịch sử, có lẽ ngay sau khi cho tôi xem **Amazon redshift**. Đây là kho dữ liệu như một dịch vụ. Đó là các nút dịch chuyển đỏ có khả năng mở rộng quy mô lớn ở nhiều kích cỡ petabyte, rất phổ biến. Trên thực tế, hợp tác với **Amazon redshift Spectrum**. Bạn có thể trực tiếp chạy một truy vấn SQL với hàng exabytes dữ liệu phi cấu trúc chạy trong hồ dữ liệu. Nhưng nó không chỉ có khả năng xử lý các tập dữ liệu lớn hơn. Redshift sử dụng nhiều cải tiến khác nhau, cho phép bạn đạt được hiệu suất cao hơn gấp mười lần.

Bạn cần các giải pháp big data BI, redshift cho phép bạn bắt đầu bằng một lệnh gọi API duy nhất. Ít thời gian chờ đợi kết quả hơn, có nhiều thời gian hơn để nhận được câu trả lời.

# AWS Database Migration Service (AWS DMS)

Chúng ta đã nói về cơ sở dữ liệu và các tùy chọn cơ sở dữ liệu khác nhau trên AWS. Nhưng điều gì sẽ xảy ra nếu bạn có cơ sở dữ liệu tại cơ sở hoặc trên đám mây rồi à? Điều đó có nghĩa là bạn phải bắt đầu lại từ đầu? Rất may AWS cung cấp một dịch vụ có tên **Amazon Database Migration Service** (Dịch vụ di chuyển cơ sở dữ liệu Amazon), hoặc DMS, để giúp khách hàng thực hiện điều đó. DMS giúp khách hàng di chuyển cơ sở dữ liệu hiện có lên AWS một cách an toàn và thời trang dễ dàng. Về cơ bản, bạn di chuyển dữ liệu giữa cơ sở dữ liệu nguồn và cơ sở dữ liệu đích. Phần tốt nhất là cơ sở dữ liệu nguồn vẫn hoạt động đầy đủ trong suốt quá trình việc di chuyển, giảm thiểu thời gian ngừng hoạt động của các ứng dụng dựa trên cơ sở dữ liệu đó. Tốt hơn nữa là nguồn và cơ sở dữ liệu đích không nhất thiết phải cùng loại.

Nhưng hãy bắt đầu với cơ sở dữ liệu cùng loại. Quá trình này khá đơn giản. Vì cấu trúc lược đồ, kiểu dữ liệu và mã cơ sở dữ liệu tương thích giữa nguồn và đích. Cơ sở dữ liệu nguồn có thể được đặt tại cơ sở, chạy trên phiên bản Amazon EC2 hoặc có thể là cơ sở dữ liệu Amazon RDS. Bản thân mục tiêu có thể là cơ sở dữ liệu trong Amazon EC2 hoặc Amazon RDS. Trong trường hợp này, bạn tạo một tác vụ di chuyển với các kết nối tới nguồn và cơ sở dữ liệu mục tiêu. Sau đó bắt đầu di chuyển bằng cách nhấp vào nút. Dịch vụ di chuyển cơ sở dữ liệu AWS sẽ lo phần còn lại.

Kiểu di chuyển thứ hai xảy ra khi nguồn và cơ sở dữ liệu đích có nhiều loại khác nhau. Đây được gọi là **heterogeneous migration** (di chuyển không đồng nhất) và là a **2-step process** (một quá trình gồm 2 bước). Vì cấu trúc lược đồ, kiểu dữ liệu và mã cơ sở dữ liệu khác nhau giữa nguồn và đích, trước tiên chúng ta cần chuyển đổi chúng bằng **AWS schema conversion tool** (công cụ chuyển đổi lược đồ AWS). Điều này sẽ chuyển đổi lược đồ nguồn và mã để khớp với cơ sở dữ liệu đích. Bước tiếp theo là sử dụng DMS để di chuyển dữ liệu từ cơ sở dữ liệu nguồn tới cơ sở dữ liệu đích. Nhưng đây không phải là trường hợp sử dụng duy nhất của DMS.

**[AWS Database Migration Service \(AWS DMS\)](#)** cho phép bạn di chuyển cơ sở dữ liệu quan hệ, cơ sở dữ liệu phi quan hệ và các loại kho dữ liệu khác.

Ví dụ: giả sử bạn có cơ sở dữ liệu MySQL được lưu trữ tại cơ sở trong phiên bản Amazon EC2 hoặc trong Amazon RDS. Hãy coi cơ sở dữ liệu MySQL là cơ sở dữ liệu nguồn của bạn. Khi sử dụng AWS DMS, bạn có thể di chuyển dữ liệu của mình sang cơ sở dữ liệu đích, chẳng hạn như cơ sở dữ liệu Amazon Aurora.

## Các trường hợp sử dụng khác của AWS DMS

### Di chuyển cơ sở dữ liệu phát triển và thử nghiệm

- Cho phép nhà phát triển thử nghiệm ứng dụng dựa trên dữ liệu sản xuất mà không ảnh hưởng đến người dùng sản xuất

### Hợp nhất cơ sở dữ liệu

- Kết hợp nhiều cơ sở dữ liệu thành một cơ sở dữ liệu duy nhất

### Sao chép liên tục

- Gửi các bản sao dữ liệu liên tục của bạn đến các nguồn mục tiêu khác thay vì thực hiện di chuyển một lần. Điều này có thể là để khắc phục thảm họa hoặc do sự tách biệt về mặt địa lý.

# Additional Database Services

## Amazon DocumentDB

[Tài liệu AmazonDB](#) là một dịch vụ cơ sở dữ liệu tài liệu hỗ trợ khối lượng công việc MongoDB. (MongoDB là một chương trình cơ sở dữ liệu tài liệu.)

## Amazon Neptune

[Sao Hải Vương Amazon](#) là một dịch vụ cơ sở dữ liệu đồ thị.

Bạn có thể sử dụng Amazon Neptune để xây dựng và chạy các ứng dụng hoạt động với bộ dữ liệu có tính kết nối cao, chẳng hạn như công cụ đề xuất, phát hiện gian lận và biểu đồ tri thức.

## Amazon Quantum Ledger Database (Amazon QLDB)

[Cơ sở dữ liệu sổ cái lượng tử Amazon \(Amazon QLDB\)](#) là một dịch vụ cơ sở dữ liệu sổ cái.

Bạn có thể sử dụng Amazon QLDB để xem lại lịch sử đầy đủ của tất cả những thay đổi đã được thực hiện đối với dữ liệu ứng dụng của bạn.

## Amazon Managed Blockchain

[Chuỗi khối được quản lý của Amazon](#) là một dịch vụ mà bạn có thể sử dụng để tạo và quản lý mạng blockchain bằng các khung nguồn mở.

Blockchain là một hệ thống sổ cái phân tán cho phép nhiều bên thực hiện giao dịch và chia sẻ dữ liệu mà không cần cơ quan trung ương.

## **Amazon ElastiCache**

**Bộ đệm Amazon Elasti** là dịch vụ bổ sung các lớp bộ đệm vào cơ sở dữ liệu của bạn để giúp cải thiện thời gian đọc các yêu cầu phổ biến.

Nó hỗ trợ hai loại lưu trữ dữ liệu: Redis và Memcached.

## **Amazon DynamoDB Accelerator**

**Trình tăng tốc Amazon DynamoDB (DAX)** là bộ nhớ đệm trong bộ nhớ dành cho DynamoDB.

Nó giúp cải thiện thời gian phản hồi từ mili giây một chữ số đến micro giây.

# **Shared Responsibility Model**

## **Mô hình trách nhiệm chung của AWS**

Trong suốt khóa học này, bạn đã tìm hiểu về nhiều loại tài nguyên mà bạn có thể tạo trên Đám mây AWS. Các tài nguyên này bao gồm các phiên bản Amazon EC2, bộ chứa Amazon S3 và cơ sở dữ liệu Amazon RDS. Ai chịu trách nhiệm giữ an toàn cho các tài nguyên này: bạn (khách hàng) hay AWS?

Câu trả lời là cả hai. Lý do là bạn không coi môi trường AWS của mình là một đối tượng duy nhất. Đúng hơn, bạn coi môi trường như một tập hợp các bộ phận được xây dựng dựa trên nhau. AWS chịu trách nhiệm về một số phần trong môi trường của bạn và bạn (khách hàng) chịu trách nhiệm về các phần khác. Khái niệm này được gọi là shared responsibility model ([\*\*mô hình chia sẻ trách nhiệm\*\*](#)).

Mô hình trách nhiệm chung chia thành trách nhiệm của khách hàng (thường được gọi là "bảo mật trên đám mây") và trách nhiệm của AWS (thường được gọi là "bảo mật của đám mây").

CUSTOMERS	CUSTOMER DATA		
	PLATFORM, APPLICATIONS, IDENTITY AND ACCESS MANAGEMENT		
	OPERATING SYSTEMS, NETWORK AND FIREWALL CONFIGURATION		
	CLIENT-SIDE DATA ENCRYPTION	SERVER-SIDE ENCRYPTION	NETWORKING TRAFFIC PROTECTION

AWS	SOFTWARE			
	COMPUTE	STORAGE	DATABASE	NETWORKING
	HARDWARE/AWS GLOBAL INFRASTRUCTURE			
	REGIONS		AVAILABILITY ZONES	EDGE LOCATIONS

Bạn có thể coi mô hình này tương tự như sự phân chia trách nhiệm giữa chủ nhà và người xây dựng nhà. Người xây dựng (AWS) chịu trách nhiệm xây dựng ngôi nhà của bạn và đảm bảo rằng nó được xây dựng kiên cố. Với tư cách là chủ nhà (khách hàng), bạn có trách nhiệm đảm bảo an toàn cho mọi thứ trong nhà bằng cách đảm bảo các cửa được đóng và khóa.

### **Khách hàng: Bảo mật trên đám mây**

Khách hàng chịu trách nhiệm về tính bảo mật của mọi thứ họ tạo và đưa vào Đám mây AWS.

Khi sử dụng dịch vụ AWS, bạn, với tư cách là khách hàng, có toàn quyền kiểm soát nội dung của mình. Bạn chịu trách nhiệm quản lý các yêu cầu bảo mật cho nội dung của mình, bao gồm nội dung bạn chọn lưu trữ trên AWS, dịch vụ AWS nào bạn sử dụng và ai có quyền truy cập vào nội dung đó. Bạn cũng kiểm soát cách cấp, quản lý và thu hồi quyền truy cập.

Các bước bảo mật mà bạn thực hiện sẽ phụ thuộc vào các yếu tố như dịch vụ bạn sử dụng, độ phức tạp của hệ thống cũng như nhu cầu bảo mật và vận hành cụ thể của công ty bạn. Các bước bao gồm chọn, đặt cấu hình và vá lỗi hệ điều hành sẽ chạy trên phiên bản Amazon EC2, đặt cấu hình nhóm bảo mật và quản lý tài khoản người dùng.

### **AWS: Bảo mật của đám mây**

AWS chịu trách nhiệm về bảo mật *của* đám mây.

AWS vận hành, quản lý và kiểm soát các thành phần ở tất cả các lớp cơ sở hạ tầng. Điều này bao gồm các lĩnh vực như hệ điều hành máy chủ, lớp ảo hóa và thậm chí cả bảo mật vật lý của trung tâm dữ liệu nơi các dịch vụ hoạt động.

AWS chịu trách nhiệm bảo vệ cơ sở hạ tầng toàn cầu chạy tất cả các dịch vụ được cung cấp trên Đám mây AWS. Cơ sở hạ tầng này bao gồm Khu vực AWS, Vùng sẵn sàng và các vị trí biên.

AWS quản lý tính bảo mật của đám mây, cụ thể là cơ sở hạ tầng vật lý lưu trữ tài nguyên của bạn, bao gồm:

- Bảo mật vật lý của trung tâm dữ liệu
- Cơ sở hạ tầng phần cứng và phần mềm
- Cơ sở hạ tầng mạng
- Cơ sở hạ tầng ảo hóa

Mặc dù bạn không thể truy cập trung tâm dữ liệu AWS để xem trực tiếp biện pháp bảo vệ này nhưng AWS cung cấp một số báo cáo từ kiểm tra viên bên thứ ba. Các kiểm toán viên này đã xác minh sự tuân thủ của nó với nhiều tiêu chuẩn và quy định bảo mật máy tính.

## User Permission and Access

### **AWS Identity and Access Management (IAM)**

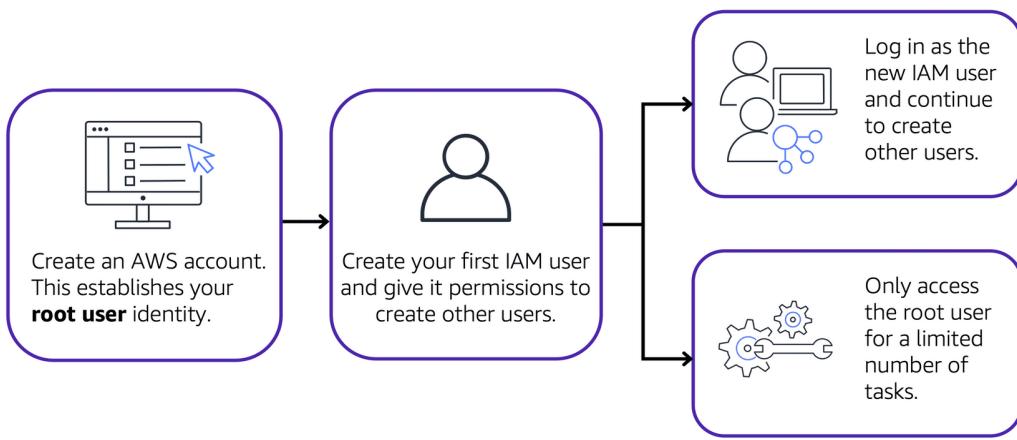
[Quản lý quyền truy cập và nhận dạng AWS \(IAM\)](#) cho phép bạn quản lý quyền truy cập vào các dịch vụ và tài nguyên AWS một cách an toàn.

IAM mang đến cho bạn sự linh hoạt trong việc định cấu hình quyền truy cập dựa trên nhu cầu bảo mật và hoạt động cụ thể của công ty bạn.

### **AWS Account Root User**

Khi tạo tài khoản AWS lần đầu tiên, bạn bắt đầu bằng một danh tính được gọi là [người dùng root](#).

Người dùng root được truy cập bằng cách đăng nhập bằng địa chỉ email và mật khẩu mà bạn đã sử dụng để tạo tài khoản AWS của mình. Bạn có thể coi người dùng root giống như chủ quán cà phê. Nó có toàn quyền truy cập vào tất cả các dịch vụ và tài nguyên AWS trong tài khoản.



### Thực hành tốt nhất:

Không **sử** dụng người dùng root cho các công việc hàng ngày.

Thay vào đó, hãy sử dụng người dùng root để tạo người dùng IAM đầu tiên của bạn và gán quyền cho người dùng đó để tạo những người dùng khác.

Sau đó, tiếp tục tạo những người dùng IAM khác và truy cập những danh tính đó để thực hiện các tác vụ thông thường trên AWS. Chỉ sử dụng người dùng root khi bạn cần thực hiện một số tác vụ giới hạn mà chỉ người dùng root mới có thể thực hiện được. Ví dụ về các tác vụ này bao gồm thay đổi địa chỉ email người dùng gốc và thay đổi gói hỗ trợ AWS của bạn.

### IAM users

Người **dùng IAM** là danh tính mà bạn tạo trong AWS. Nó đại diện cho người hoặc ứng dụng tương tác với các dịch vụ và tài nguyên AWS. Nó bao gồm một tên và thông tin xác thực.

Theo mặc định, khi bạn tạo người dùng IAM mới trong AWS, người dùng đó không có quyền liên quan. Để cho phép người dùng IAM thực hiện các hành động cụ thể trong AWS, chẳng hạn như khởi chạy phiên bản Amazon EC2 hoặc tạo bộ chứa Amazon S3, bạn phải cấp cho người dùng IAM các quyền cần thiết.

### Thực hành tốt nhất:

Chúng tôi khuyên bạn nên tạo người dùng IAM riêng lẻ cho từng người cần truy cập AWS.

Ngay cả khi bạn có nhiều nhân viên yêu cầu cùng cấp độ truy cập, bạn vẫn nên tạo người dùng IAM riêng cho từng người trong số họ. Điều này cung cấp bảo mật bổ sung bằng cách cho phép mỗi người dùng IAM có một bộ thông tin xác thực bảo mật duy nhất.

## IAM policies

**Chính sách IAM** là tài liệu cho phép hoặc từ chối quyền đối với các dịch vụ và tài nguyên AWS.

Chính sách IAM cho phép bạn tùy chỉnh cấp độ truy cập vào tài nguyên của người dùng. Ví dụ: bạn có thể cho phép người dùng truy cập vào tất cả các nhóm Amazon S3 trong tài khoản AWS của bạn hoặc chỉ một nhóm cụ thể.

### Thực hành tốt nhất:

Tuân thủ nguyên tắc bảo mật về **đặc quyền tối thiểu** khi cấp quyền.

Hãy nhớ rằng, theo mặc định, tất cả các hành động đều bị từ chối. Bạn phải cho phép rõ ràng mọi hành động được thực hiện bởi bất kỳ người dùng nào. Bạn chỉ cấp cho mọi người quyền truy cập vào những gì họ cần và không có gì khác. Ý tưởng này được gọi là nguyên tắc ít đặc quyền nhất.

Bằng cách tuân theo nguyên tắc này, bạn giúp ngăn người dùng vai trò có nhiều quyền hơn mức cần thiết để thực hiện nhiệm vụ của họ.

Ví dụ: nếu nhân viên chỉ cần quyền truy cập vào một nhóm cụ thể, hãy chỉ định nhóm đó trong chính sách IAM. Thực hiện việc này thay vì cấp cho nhân viên quyền truy cập vào tất cả các nhóm trong tài khoản AWS của bạn.

### Ví dụ: chính sách IAM

Sau đây là ví dụ về cách hoạt động của chính sách IAM. Giả sử chủ quán cà phê phải tạo người dùng IAM cho nhân viên thu ngân mới được thuê. Nhân viên thu ngân cần có quyền truy cập vào các biên lai được lưu giữ trong bộ chứa Amazon S3 có ID: AWSDOC-EXAMPLE-BUCKET.

```
{  
    "Version": "2012-10-17",  
    "Statement": {  
        "Effect": "Allow",  
        "Action": "s3>ListObject",  
        "Resource": "arn:aws:s3:::  
AWSDOC-EXAMPLE-BUCKET"  
    }  
}
```

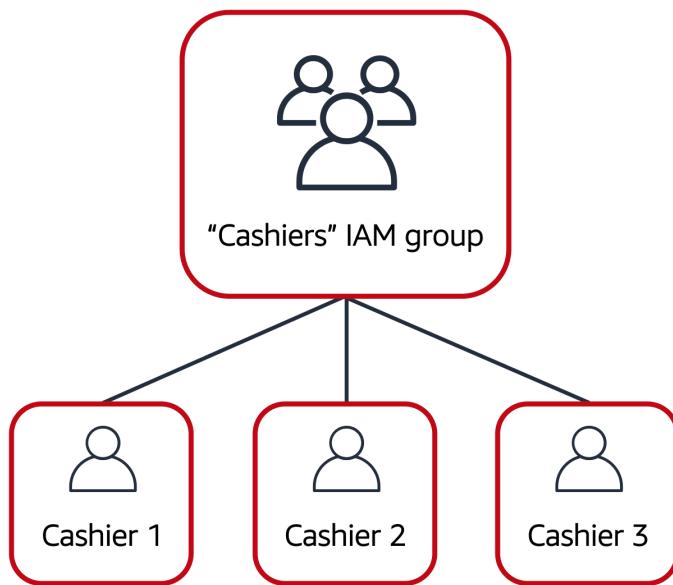
Trong ví dụ này, chính sách IAM cho phép một hành động cụ thể trong Amazon S3: ListObject. Chính sách này cũng đề cập đến một ID nhóm cụ thể: AWSDOC-EXAMPLE-BUCKET. Khi chủ sở hữu đính kèm chính sách này với người dùng IAM của nhân viên thu ngân, chính sách này sẽ cho phép nhân viên thu ngân xem tất cả các đối tượng trong nhóm AWSDOC-EXAMPLE-BUCKET.

Nếu chủ sở hữu muốn nhân viên thu ngân có thể truy cập các dịch vụ khác và thực hiện các hành động khác trong AWS thì chủ sở hữu phải đính kèm các chính sách bổ sung để chỉ định các dịch vụ và hành động này.

Bây giờ, giả sử quán cà phê đã thuê thêm một vài nhân viên thu ngân. Thay vì chỉ định quyền cho từng người dùng IAM riêng lẻ, chủ sở hữu sẽ đặt người dùng vào một **nhóm IAM**.

## IAM Groups

Nhóm IAM là tập hợp những người dùng IAM. Khi bạn chỉ định chính sách IAM cho một nhóm, tất cả người dùng trong nhóm đều được cấp các quyền do chính sách chỉ định. Đây là một ví dụ về cách điều này có thể xảy ra trong quán cà phê. Thay vì chỉ định từng quyền cho nhân viên thu ngân, chủ sở hữu có thể tạo nhóm IAM "Thu ngân". Sau đó, chủ sở hữu có thể thêm người dùng IAM vào nhóm rồi đính kèm quyền ở cấp nhóm.



Việc chỉ định chính sách IAM ở cấp nhóm cũng giúp điều chỉnh quyền dễ dàng hơn khi nhân viên chuyển sang công việc khác. Ví dụ: nếu nhân viên thu ngân trở thành chuyên gia kiểm kê, chủ quán cà phê sẽ loại họ khỏi nhóm IAM "Thu ngân" và thêm họ vào

nhóm IAM "Chuyên gia kiểm kê". Điều này đảm bảo rằng nhân viên chỉ có các quyền cần thiết cho vai trò hiện tại của họ.

Điều gì sẽ xảy ra nếu một nhân viên quán cà phê không chuyển việc vĩnh viễn mà thay vào đó luân chuyển sang các trạm làm việc khác nhau suốt cả ngày? Nhân viên này có thể có được quyền truy cập họ cần thông qua [\*\*Vai trò IAM\*\*](#).

## **IAM Roles**

Trong quán cà phê, nhân viên luân phiên làm việc ở những nơi khác nhau trong ngày. Tùy thuộc vào nhân sự của quán cà phê, nhân viên này có thể thực hiện một số nhiệm vụ: làm việc tại quầy thu ngân, cập nhật hệ thống kiểm kê, xử lý đơn đặt hàng trực tuyến, v.v.

Khi nhân viên cần chuyển sang một nhiệm vụ khác, họ sẽ từ bỏ quyền truy cập vào một máy trạm và có quyền truy cập vào máy trạm tiếp theo. Nhân viên có thể dễ dàng chuyển đổi giữa các máy trạm, nhưng tại bất kỳ thời điểm nào, họ chỉ có thể truy cập vào một máy trạm duy nhất. Khái niệm tương tự này tồn tại trong AWS với vai trò IAM. Vai trò IAM là danh tính mà bạn có thể sử dụng để có được quyền truy cập tạm thời vào các quyền.

Trước khi người dùng, ứng dụng hoặc dịch vụ IAM có thể đảm nhận vai trò IAM, họ phải được cấp quyền để chuyển sang vai trò đó. Khi ai đó đảm nhận vai trò IAM, họ sẽ từ bỏ tất cả các quyền trước đó mà họ có trong vai trò trước đó và đảm nhận các quyền của vai trò mới.

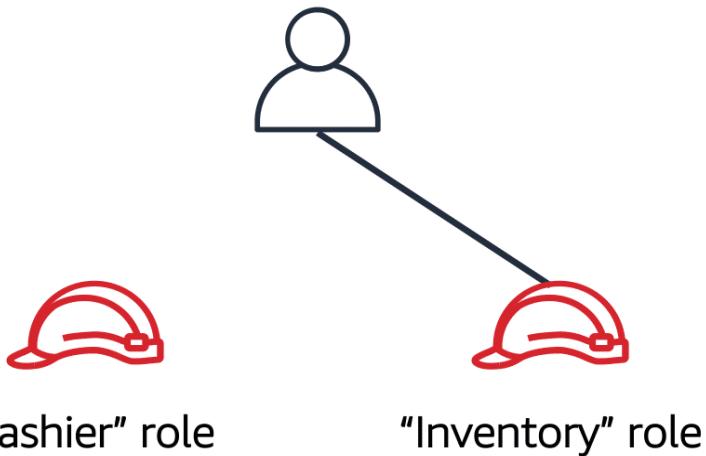
### **Thực hành tốt nhất:**

Vai trò IAM lý tưởng cho các tình huống cần cấp quyền truy cập vào dịch vụ hoặc tài nguyên tạm thời thay vì lâu dài.

### **Ví dụ: Vai trò IAM**

Xem lại ví dụ về cách sử dụng vai trò IAM trong quán cà phê:

1. Đầu tiên, chủ sở hữu cấp cho nhân viên quyền chuyển đổi vai trò cho từng máy trạm trong quán cà phê.
2. Tiếp theo, nhân viên bắt đầu ngày làm việc của mình bằng việc đảm nhận vai trò "Thu ngân". Điều này cấp cho họ quyền truy cập vào hệ thống máy tính tiền.
3. Cuối ngày, nhân viên cần cập nhật hệ thống kiểm kê. Họ đảm nhận vai trò "Hàng tồn kho". Điều này cấp cho nhân viên quyền truy cập vào hệ thống kiểm kê và cũng thu hồi quyền truy cập của họ vào hệ thống máy tính tiền.



### **Multi-factor Authentication**

Bạn đã bao giờ đăng nhập vào một trang web yêu cầu bạn cung cấp nhiều thông tin để xác minh danh tính của mình chưa? Bạn có thể cần phải cung cấp mật khẩu và sau đó là hình thức xác thực thứ hai, chẳng hạn như mã ngẫu nhiên được gửi tới điện thoại của bạn. Đây là một ví dụ về [xác thực đa yếu tố](#).

Trong IAM, xác thực đa yếu tố (MFA) cung cấp thêm một lớp bảo mật cho tài khoản AWS của bạn.

IAM user ID: AIDACKCEVSQ6C2EXAMPLE

Password: \*\*\*\*\*

- Đầu tiên, khi người dùng đăng nhập vào trang web AWS, họ nhập ID và mật khẩu người dùng IAM của mình.
- Tiếp theo, người dùng được nhắc phản hồi xác thực từ thiết bị AWS MFA của họ. Thiết bị này có thể là khóa bảo mật phần cứng, thiết bị phần cứng hoặc ứng dụng MFA trên thiết bị như điện thoại thông minh.
- Khi người dùng đã được xác thực thành công, họ có thể truy cập vào các tài nguyên hoặc dịch vụ AWS được yêu cầu.

Bạn có thể kích hoạt MFA cho người dùng root và người dùng IAM. Cách tốt nhất là hãy bật MFA cho người dùng root và tất cả người dùng IAM trong tài khoản của bạn. Bằng cách này, bạn có thể giữ an toàn cho tài khoản AWS của mình khỏi bị truy cập trái phép.

# AWS Organizations

Với bước đột phá đầu tiên của bạn vào Đám mây AWS,rất có thể bạn sẽ bắt đầu vớimột tài khoản AWS và có mọi thứ nằm trong đó.Hầu hết mọi người đều bắt đầu theo cách này,nhưng khi công ty của bạn phát triển hoặcthậm chí còn bắt đầu hành trình Đám mây của họ,điều quan trọng là phải có sự phân chia nhiệm vụ.Ví dụ, bạn muốncác nhà phát triển của bạn có quyền truy cập vào các tài nguyên phát triển,yêu cầu nhân viên đếm của bạn có thểđể truy cập thông tin thanh toán,hoặc thậm chí có các đơn vị kinh doanh riêng biệt để họ có thể thử nghiệm các dịch vụ AWS mà không ảnh hưởng tới nhau.Một cách để cài đặt thứ tựvà để thực thi ai được phép thực hiệnmột số chức năng nhất định trong tài khoản nào sẽ được sử dụngcủa dịch vụ AWS có tên **AWS Organizations** .

## AWS Organizations

Giả sử công ty của bạn có nhiều tài khoản AWS. Bạn có thể dùng **Tổ chức AWS** để hợp nhất và quản lý nhiều tài khoản AWS ở một vị trí trung tâm.

Khi bạn tạo một tổ chức, AWS Organizations sẽ tự động tạo một **thư mục gốc**, là vùng chứa chính cho tất cả các tài khoản trong tổ chức của bạn.

Trong AWS Organs, bạn có thể kiểm soát tập trung quyền đối với các tài khoản trong tổ chức của mình bằng cách sử dụng **service control policies Chính sách kiểm soát dịch vụ (SCP)**. SCP cho phép bạn đặt ra các hạn chế đối với các dịch vụ, tài nguyên AWS và hành động API riêng lẻ mà người dùng và vai trò trong mỗi tài khoản có thể truy cập, để chỉ định các quyền tối đacho các tài khoản thành viên trong tổ chức.

Thanh toán tổng hợp là một tính năng khác của AWS Organs. Thanh toán tổng hợp cho tất cả tài khoản thành viên.Điều này có nghĩa là bạn có thể sử dụng tài khoản chính của tổ chức của bạn để cung cống và thanh toán cho tất cả các tài khoản thành viên.Một ưu điểm khác của thanh toán tổng hợp làgiảm giá số lượng lớn, tiền mặt thực sự.

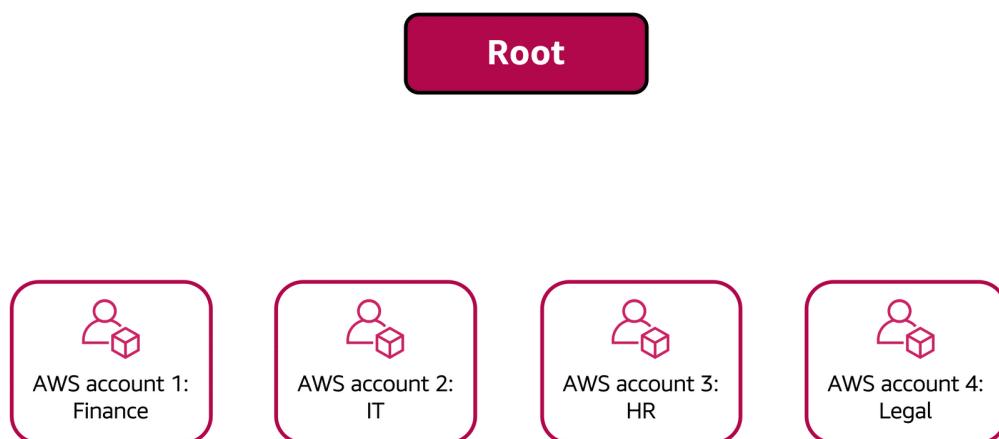
## Organizational Units

Trong AWS Organizations, bạn có thể nhóm các tài khoản thành các đơn vị tổ chức organizational units (OU) để quản lý các tài khoản có yêu cầu kinh doanh hoặc bảo mật tương tự dễ dàng hơn. Khi bạn áp dụng chính sách cho OU, tất cả tài khoản trong OU sẽ tự động kế thừa các quyền được chỉ định trong chính sách.

Bằng cách tổ chức các tài khoản riêng biệt thành OU, bạn có thể dễ dàng tách biệt khối lượng công việc hoặc ứng dụng có yêu cầu bảo mật cụ thể. Ví dụ: nếu công ty của bạn có các tài khoản chỉ có thể truy cập các dịch vụ AWS đáp ứng các yêu cầu quy định nhất định thì bạn có thể đặt các tài khoản này vào một OU. Sau đó, bạn có thể đính kèm chính sách vào OU để chặn quyền truy cập vào tất cả các dịch vụ AWS khác không đáp ứng các yêu cầu quy định.

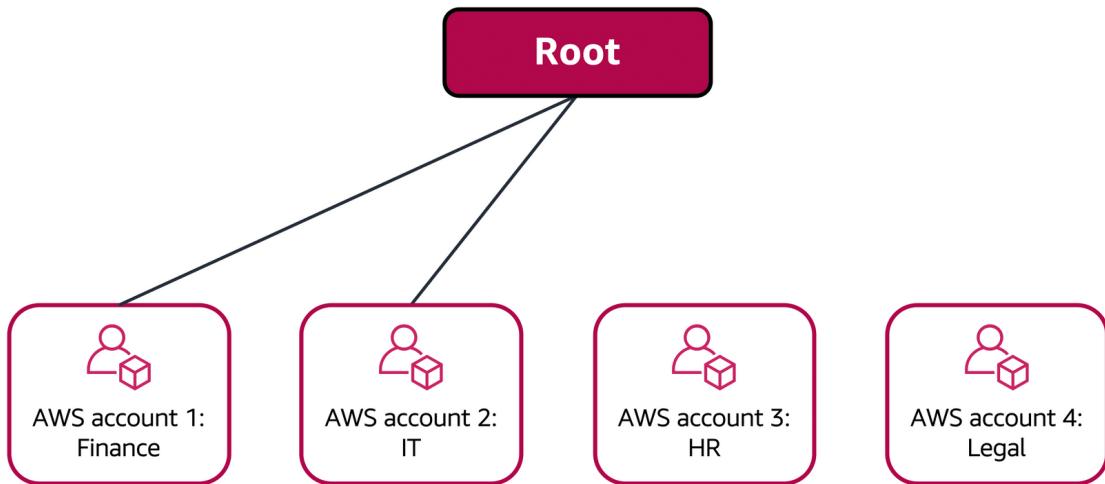
### Ví dụ: Tổ chức AWS

Xem lại ví dụ về cách một công ty có thể sử dụng AWS Organs:

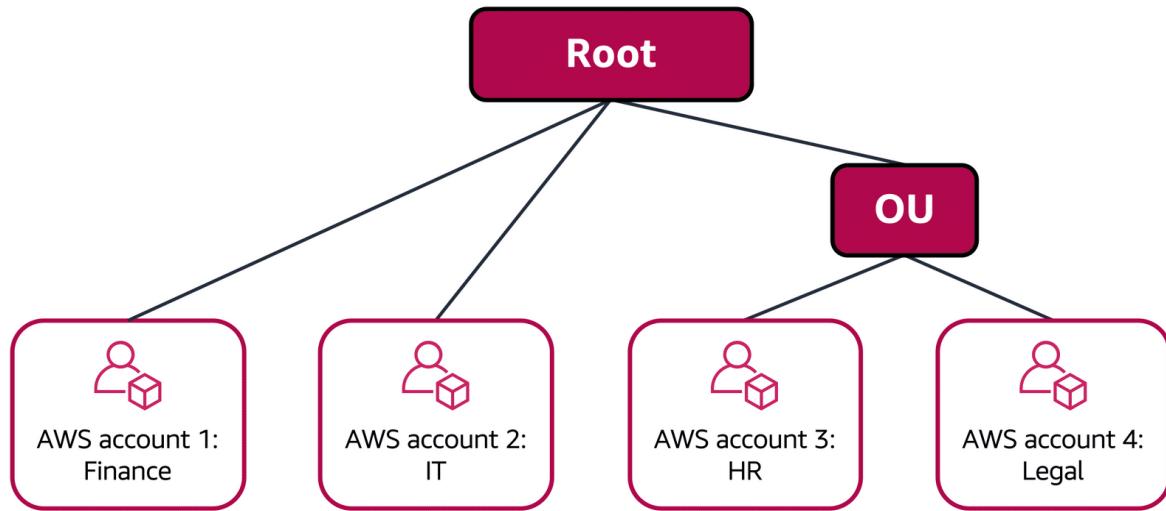


Hãy tưởng tượng rằng công ty của bạn có các tài khoản AWS riêng cho bộ phận tài chính, công nghệ thông tin (IT), nhân sự (HR) và pháp lý. Bạn quyết định hợp nhất các tài khoản này thành một tổ chức duy nhất để có thể quản lý chúng từ một vị trí trung tâm. Khi bạn tạo tổ chức, điều này sẽ thiết lập gốc.

Khi thiết kế tổ chức của mình, bạn xem xét các nhu cầu kinh doanh, bảo mật và quy định của từng bộ phận. Bạn sử dụng thông tin này để quyết định các phòng ban nào sẽ nhóm lại với nhau trong OU.



Bộ phận tài chính và CNTT có những yêu cầu không trùng lặp với bất kỳ bộ phận nào khác. Bạn đưa các tài khoản này vào tổ chức của mình để tận dụng các lợi ích như thanh toán tổng hợp nhưng bạn không đặt chúng vào bất kỳ OU nào.



Bộ phận nhân sự và pháp lý cần truy cập vào cùng các dịch vụ và tài nguyên AWS, vì vậy, bạn hãy đặt chúng vào một OU cùng nhau. Việc đặt chúng vào OU cho phép bạn đính kèm các chính sách áp dụng cho cả tài khoản AWS của bộ phận nhân sự và pháp lý.

Ngay cả khi bạn đã đặt các tài khoản này vào OU, bạn vẫn có thể tiếp tục cấp quyền truy cập cho người dùng, nhóm và vai trò thông qua IAM.

Bằng cách nhóm các tài khoản của bạn thành các OU, bạn có thể dễ dàng cấp cho họ quyền truy cập vào các dịch vụ và tài nguyên mà họ cần. Bạn cũng ngăn họ truy cập bất kỳ dịch vụ hoặc tài nguyên nào mà họ không cần.

# Compliance

Đối với mỗi ngành đều có những tiêu chuẩn cụ thể cần được duy trì và bạn sẽ được kiểm tra hoặc thanh tra để đảm bảo rằng bạn đã đáp ứng được những tiêu chuẩn đó. Ví dụ: đối với một quán cà phê, thanh tra y tế sẽ đến và kiểm tra rằng mọi thứ đều tuân thủ quy tắc và vệ sinh. Bạn sẽ cần nghĩ ra cách tương tự để đáp ứng sự tuân thủ và kiểm tra trong AWS. Tùy thuộc vào loại giải pháp bạn lưu trữ trên AWS, bạn sẽ cần phải đảm bảo rằng bạn tuân thủ các bất cứ tiêu chuẩn và quy định nào doanh nghiệp của bạn được tổ chức cụ thể. Nếu bạn chạy phần mềm xử lý với dữ liệu người tiêu dùng ở EU, bạn sẽ cần phải chắc chắn rằng bạn tuân thủ GDPR.

Điều đầu tiên cần lưu ý là AWS đã xây dựng cơ sở hạ tầng và mạng lưới trung tâm dữ liệu, tuân theo các phương pháp hay nhất trong ngành chia sẻ bảo mật và với tư cách là khách hàng của AWS, bạn kế thừa tất cả các biện pháp thực hành tốt nhất của chính sách AWS, kiến trúc và quy trình vận hành. AWS tuân thủ một danh sách dài về các chương trình đảm bảo mà bạn có thể tìm thấy trực tuyến. Điều này có nghĩa là các phân đoạn của sự tuân thủ của bạn đã được hoàn thành và bạn có thể tập trung vào việc tuân thủ cuộc họp trong vòng kiến trúc của riêng bạn mà bạn xây dựng trên AWS.

Để biết liệu bạn có tuân thủ AWS hay không, hãy nhớ rằng chúng ta tuân theo trách nhiệm chung. Nền tảng cơ bản là an toàn và AWS có thể cung cấp tài liệu về những loại yêu cầu tuân thủ mà họ đáp ứng thông qua các dịch vụ như **AWS Artifact** và **white paper**. Nhưng ngoài ra, những gì bạn xây dựng trên AWS đều tùy thuộc vào bạn. Bạn kiểm soát kiến trúc ứng dụng của mình và các giải pháp bạn xây dựng và chúng cần phải được xây dựng với sự tuân thủ, bảo mật và mô hình trách nhiệm chung.

## AWS Artifact

Tùy thuộc vào ngành của công ty bạn, bạn có thể cần phải duy trì các tiêu chuẩn cụ thể. Việc kiểm toán hoặc thanh tra sẽ đảm bảo rằng công ty đã đáp ứng các tiêu chuẩn đó.

**Cấu phần AWS** là dịch vụ cung cấp quyền truy cập theo yêu cầu vào các báo cáo tuân thủ và bảo mật AWS cũng như các thỏa thuận trực tuyến chọn lọc. AWS Artifact bao gồm hai phần chính: Thỏa thuận AWS Artifact và Báo cáo AWS Artifact.

## AWS Artifact Agreements

Giả sử công ty của bạn cần ký thỏa thuận với AWS về việc bạn sử dụng một số loại thông tin nhất định trên các dịch vụ AWS. Bạn có thể thực hiện việc này thông qua **AWS Artifact Agreements**.

Trong Thỏa thuận AWS Artifact, bạn có thể xem xét, chấp nhận và quản lý các thỏa thuận cho một tài khoản cá nhân và cho tất cả các tài khoản của bạn trong AWS Organs. Các loại thỏa thuận khác nhau được đưa ra để giải quyết nhu cầu của những khách hàng phải tuân theo các quy định cụ thể, chẳng hạn như Đạo luật về trách nhiệm giải trình và cung cấp thông tin bảo hiểm y tế (HIPAA).

## AWS Artifact Reports

Tiếp theo, giả sử rằng một thành viên trong nhóm phát triển của công ty bạn đang xây dựng một ứng dụng và cần thêm thông tin về trách nhiệm của họ trong việc tuân thủ các tiêu chuẩn quy định nhất định. Bạn có thể khuyên họ truy cập thông tin này trong AWS Artifact Reports.

Báo cáo giả tạo AWS cung cấp báo cáo tuân thủ từ kiểm toán viên bên thứ ba. Các kiểm tra viên này đã kiểm tra và xác minh rằng AWS tuân thủ nhiều tiêu chuẩn và quy định bảo mật cụ thể của ngành, khu vực và toàn cầu. Báo cáo giả tạo AWS luôn cập nhật các báo cáo mới nhất được phát hành. Bạn có thể cung cấp các tạo phẩm kiểm tra AWS cho kiểm tra viên hoặc cơ quan quản lý của mình làm bằng chứng về các biện pháp kiểm soát bảo mật của AWS.

Sau đây là một số báo cáo và quy định tuân thủ mà bạn có thể tìm thấy trong AWS Artifact. Mỗi báo cáo bao gồm mô tả về nội dung và khoảng thời gian báo cáo mà tài liệu có hiệu lực.



# Denial-of-Service Attacks

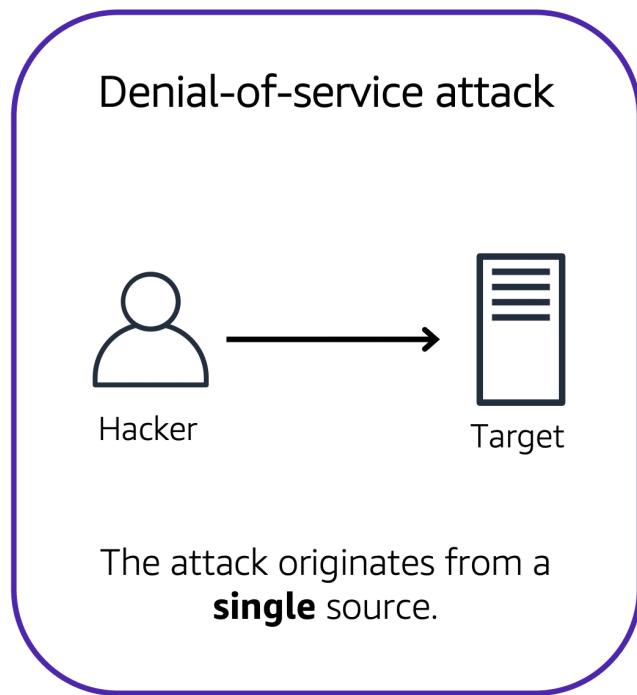
Khách hàng có thể gọi tới quán cà phê để đặt hàng. Sau khi trả lời từng cuộc gọi, nhân viên thu ngân sẽ nhận đơn đặt hàng và đưa cho nhân viên pha chế.

Tuy nhiên, giả sử một người chơi khăm gọi điện nhiều lần để đặt hàng nhưng không bao giờ lấy đồ uống cho họ. Điều này khiến nhân viên thu ngân không thể nhận cuộc gọi của khách hàng khác. Quán cà phê có thể cố gắng ngăn chặn những yêu cầu trái bằng cách chặn số điện thoại mà kẻ chơi khăm đang sử dụng.

Trong trường hợp này, hành động của kẻ chơi khăm tương tự như một **denial-of-service attack**.

## Denial-of-Service Attacks

Cuộc **tấn công từ chối dịch vụ (DoS)** là một nỗ lực có chủ ý nhằm làm cho một trang web hoặc ứng dụng không thể truy cập được đối với người dùng.

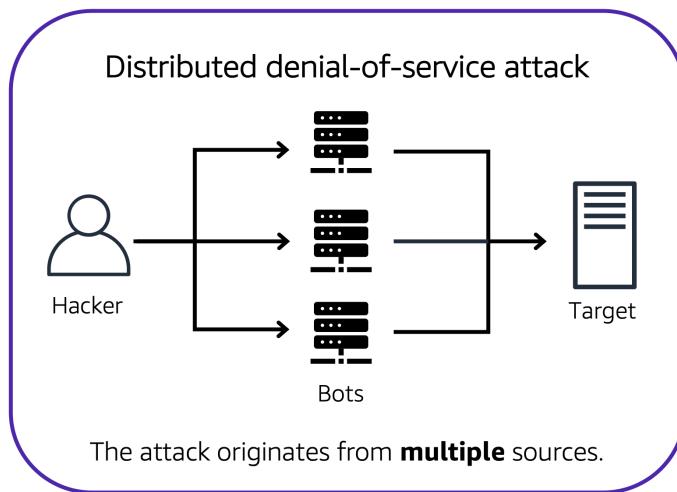


Ví dụ: kẻ tấn công có thể làm tràn ngập một trang web hoặc ứng dụng có lưu lượng truy cập mạng quá mức cho đến khi trang web hoặc ứng dụng được nhắm mục tiêu trở nên quá tải và không thể phản hồi nữa. Nếu trang web hoặc ứng dụng không khả dụng,

điều này sẽ từ chối cung cấp dịch vụ cho những người dùng đang cố gắng thực hiện các yêu cầu hợp pháp.

## Distributed Denial-of-Service Attacks

Bây giờ, giả sử rằng người chơi khăm đã tranh thủ được sự giúp đỡ của bạn bè. Kẻ chơi khăm và bạn bè của họ liên tục gọi điện đến quán cà phê để yêu cầu đặt hàng dù họ không có ý định đón. Những yêu cầu này đến từ nhiều số điện thoại khác nhau và quán cà phê không thể chặn tất cả. Ngoài ra, lượng cuộc gọi tràn vào khiến khách hàng ngày càng khó khăn trong việc thực hiện cuộc gọi của mình. Điều này tương tự như một **distributed denial-of-service attack**.



Trong cuộc tấn công từ chối dịch vụ (DDoS) phân tán, nhiều nguồn được sử dụng để bắt đầu cuộc tấn công nhằm mục đích làm cho một trang web hoặc ứng dụng không khả dụng. Điều này có thể đến từ một nhóm kẻ tấn công hoặc thậm chí là một kẻ tấn công duy nhất. Kẻ tấn công duy nhất có thể sử dụng nhiều máy tính bị nhiễm virus (còn được gọi là "bot") để gửi lưu lượng truy cập quá mức đến một trang web hoặc ứng dụng. Để giúp giảm thiểu ảnh hưởng của các cuộc tấn công DoS và DDoS lên ứng dụng của bạn, bạn có thể sử dụng [AWS Shield](#).

## Khiêm AWS

AWS Shield là dịch vụ bảo vệ ứng dụng khỏi các cuộc tấn công DDoS. AWS Shield cung cấp hai cấp độ bảo vệ: Tiêu chuẩn và Nâng cao.

### AWS Shield Standard

**AWS Shield Standard** tự động bảo vệ miễn phí tất cả khách hàng AWS. Nó bảo vệ tài nguyên AWS của bạn khỏi các kiểu tấn công DDoS phổ biến nhất, thường xuyên xảy ra.

Khi lưu lượng truy cập mạng đi vào ứng dụng của bạn, AWS Shield Standard sử dụng nhiều kỹ thuật phân tích khác nhau để phát hiện lưu lượng truy cập độc hại trong thời gian thực và tự động giảm thiểu lưu lượng đó.

### **AWS Shield Advanced**

**AWS Shield Advanced** là dịch vụ trả phí cung cấp chẩn đoán tấn công chi tiết cũng như khả năng phát hiện và giảm thiểu các cuộc tấn công DDoS tinh vi.

Nó cũng tích hợp với các dịch vụ khác như Amazon CloudFront, Amazon Route 53 và Elastic Load Balancing. Ngoài ra, bạn có thể tích hợp AWS Shield với AWS WAF bằng cách viết các quy tắc tùy chỉnh để giảm thiểu các cuộc tấn công DDoS phức tạp.

## **Additional Security Services**

### **AWS Key Management Service (AWS KMS)**

Quán cà phê có nhiều mặt hàng như máy pha cà phê, bánh ngọt, tiền trong máy tính tiền, v.v. Bạn có thể coi những mục này là dữ liệu. Chủ quán cà phê muốn đảm bảo rằng tất cả những món đồ này đều được an toàn, cho dù chúng đang được cất giữ trong kho hay được vận chuyển giữa các địa điểm cửa hàng.

Theo cách tương tự, bạn phải đảm bảo rằng dữ liệu của ứng dụng của bạn được an toàn khi được lưu trữ **encryption at rest**(mã hóa ở trạng thái lưu trữ) và trong khi dữ liệu được truyền đi, được gọi là **encryption in transit** (mã hóa khi truyền) .

**Dịch vụ quản lý khóa AWS (AWS KMS)** cho phép bạn thực hiện các hoạt động mã hóa thông qua việc sử dụng **các khóa mật mã** . Khóa mật mã là một chuỗi chữ số ngẫu nhiên được sử dụng để khóa (mã hóa) và mở khóa (giải mã) dữ liệu. Bạn có thể sử dụng AWS KMS để tạo, quản lý và sử dụng khóa mật mã. Bạn cũng có thể kiểm soát việc sử dụng khóa trên nhiều dịch vụ và trong ứng dụng của mình.

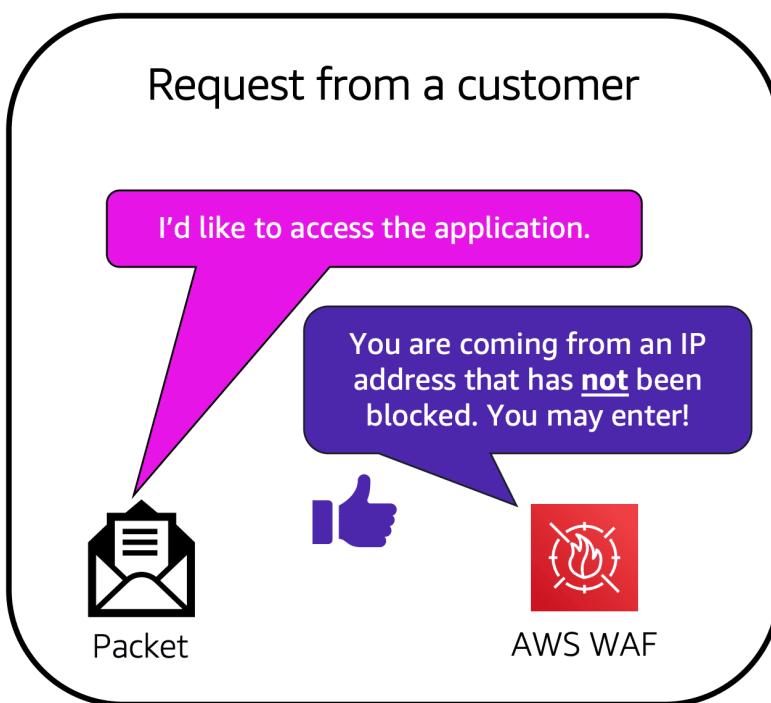
Với AWS KMS, bạn có thể chọn các cấp độ kiểm soát truy cập cụ thể mà bạn cần cho khóa của mình. Ví dụ: bạn có thể chỉ định người dùng và vai trò IAM nào có thể quản lý khóa. Ngoài ra, bạn có thể tạm thời vô hiệu hóa các phím để không ai sử dụng chúng nữa. Khóa của bạn không bao giờ rời khỏi AWS KMS và bạn luôn có quyền kiểm soát chúng.

### **AWS WAF**

**AWS WAF** là tường lửa ứng dụng web cho phép bạn giám sát các yêu cầu mạng đi vào ứng dụng web của bạn.

AWS WAF hoạt động cùng với Amazon CloudFront và Application Load Balancer. Nhớ lại danh sách kiểm soát truy cập mạng mà bạn đã học trong mô-đun trước đó. AWS WAF hoạt động theo cách tương tự để chặn hoặc cho phép lưu lượng truy cập. Tuy nhiên, nó thực hiện điều này bằng cách sử dụng một **danh sách kiểm soát truy cập web (ACL)** để bảo vệ tài nguyên AWS của bạn.

Sau đây là ví dụ về cách bạn có thể sử dụng AWS WAF để cho phép và chặn các yêu cầu cụ thể.



Giả sử ứng dụng của bạn đã nhận được các yêu cầu mạng độc hại từ một số địa chỉ IP. Bạn muốn ngăn những yêu cầu này tiếp tục truy cập vào ứng dụng của mình nhưng bạn cũng muốn đảm bảo rằng những người dùng hợp pháp vẫn có thể truy cập vào ứng dụng đó. Bạn định cấu hình ACL web để cho phép tất cả các yêu cầu ngoại trừ những yêu cầu từ địa chỉ IP mà bạn đã chỉ định.

Khi có yêu cầu đến AWS WAF, nó sẽ kiểm tra danh sách các quy tắc mà bạn đã định cấu hình trong ACL web. Nếu yêu cầu không đến từ một trong những địa chỉ IP bị chặn, nó sẽ cho phép truy cập vào ứng dụng.



Tuy nhiên, nếu một yêu cầu đến từ một trong những địa chỉ IP bị chặn mà bạn đã chỉ định trong ACL web thì yêu cầu đó sẽ bị từ chối truy cập.

### **Amazon Inspector**

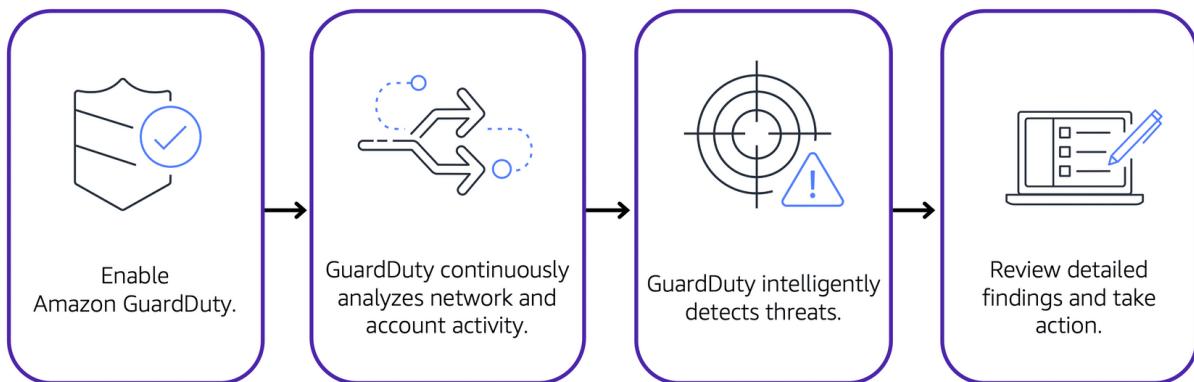
Giả sử các nhà phát triển tại quán cà phê đang phát triển và thử nghiệm một ứng dụng đặt hàng mới. Họ muốn đảm bảo rằng họ đang thiết kế ứng dụng phù hợp với các phương pháp bảo mật tốt nhất. Tuy nhiên, họ còn có một số ứng dụng khác cần phát triển nên không thể dành nhiều thời gian thực hiện các đánh giá thủ công. Để thực hiện đánh giá bảo mật tự động, họ quyết định sử dụng [Thanh tra Amazon](#).

Amazon Inspector giúp cải thiện tính bảo mật và tuân thủ của ứng dụng bằng cách chạy các đánh giá bảo mật tự động. Nó kiểm tra các ứng dụng để tìm lỗ hổng bảo mật và sai lệch so với các phương pháp bảo mật tốt nhất, chẳng hạn như quyền truy cập mở vào phiên bản Amazon EC2 và cài đặt các phiên bản phần mềm dễ bị tấn công.

Sau khi Amazon Inspector thực hiện đánh giá, nó sẽ cung cấp cho bạn danh sách các phát hiện bảo mật. Danh sách này ưu tiên theo mức độ nghiêm trọng, bao gồm mô tả chi tiết về từng vấn đề bảo mật và đề xuất cách khắc phục. Tuy nhiên, AWS không đảm bảo rằng việc làm theo các đề xuất được cung cấp sẽ giải quyết được mọi vấn đề bảo mật tiềm ẩn. Theo mô hình trách nhiệm chung, khách hàng chịu trách nhiệm về tính bảo mật của ứng dụng, quy trình và công cụ chạy trên dịch vụ AWS của họ.

### **Amazon GuardDuty**

**Nhiệm vụ bảo vệ của Amazon** là dịch vụ cung cấp khả năng phát hiện mối đe dọa thông minh cho cơ sở hạ tầng và tài nguyên AWS của bạn. Nó xác định các mối đe dọa bằng cách liên tục giám sát hoạt động mạng và hành vi tài khoản trong môi trường AWS của bạn.



Sau khi bạn kích hoạt GuardDuty cho tài khoản AWS của mình, GuardDuty sẽ bắt đầu giám sát hoạt động tài khoản và mạng của bạn. Bạn không phải triển khai hoặc quản lý bất kỳ phần mềm bảo mật bổ sung nào. Sau đó, GuardDuty liên tục phân tích dữ liệu từ nhiều nguồn AWS, bao gồm Nhật ký lưu lượng VPC và nhật ký DNS.

Nếu GuardDuty phát hiện bất kỳ mối đe dọa nào, bạn có thể xem lại các phát hiện chi tiết về chúng từ Bảng điều khiển quản lý AWS. Các phát hiện bao gồm các bước được đề xuất để khắc phục. Bạn cũng có thể định cấu hình các chức năng AWS Lambda để tự động thực hiện các bước khắc phục nhằm phản hồi các phát hiện bảo mật của GuardDuty.

Điều tuyệt vời nhất là nó chạy độc lập với AWS khác của bạn dịch vụ. Vì vậy, nó sẽ không ảnh hưởng đến hiệu suất hoặc sự sẵn có của cơ sở hạ tầng và khối lượng công việc hiện có của bạn.

## Amazon CloudWatch

Bây giờ chúng tôi đang pha rất nhiều cà phê, phục vụ khách hàng, và mọi thứ dường như trở nên nhếch nhác trong quán cà phê của chúng tôi. Nhưng khi chúng ta sử dụng máy pha cà phê espresso ngày càng nhiều, sử dụng cốc, liên tục mở và đóng tủ lạnh, chúng tôi muốn có thể đảm bảo rằng chúng tôi được cảnh báo về điều gì đó có thể đã ổn. Có thể là máy pha cà phê espresso cần được làm sạch hoặc sửa chữa. Vấn đề là, với tư cách là chủ doanh nghiệp, bạn cần có khả năng hiển thị trạng thái của hệ thống. Mọi

thứ có đang diễn ra tốt đẹp không? Giới thiệu **Amazon CloudWatch**. Ví dụ, số lượng cà phê espresso được pha bằng máy pha cà phê espresso, hoặc việc sử dụng CPU của phiên bản EC2. Hãy thực hiện cách tiếp cận khách hàng đối với quán cà phê của chúng ta. Giả sử chúng ta có một máy pha cà phê espresso và nó cần được làm sạch sau khi pha được 100 ly espresso. CloudWatch cho phép chúng tôi tạo một thước đo tùy chỉnh được gọi là số lượng cà phê espresso, và khi nó chạm tới 100, chúng tôi muốn cảnh báo nhân viên vệ sinh máy. Đơn giản phải không? Vâng, với CloudWatch, bạn có thể thực hiện điều này bằng cách tạo cái được gọi là **CloudWatch Alarm**. Bạn đặt ngưỡng cho một số liệu, và khi đạt tới ngưỡng đó, CloudWatch có thể tạo cảnh báo và kích hoạt hành động. Điều này có nghĩa là chúng tôi có thể cảnh báo về số liệu tùy chỉnh, trong trường hợp này đạt 100, và sau đó thực hiện một hành động thậm chí còn tốt hơn. Cảnh báo CloudWatch được tích hợp với SNS. Sau đó chúng tôi có thể gửi tin nhắn SMS tới Người quản lý nói, làm sạch máy. Bạn có thể tạo tất cả các loại cảnh báo tùy chỉnh cho số liệu từ tất cả các loại tài nguyên AWS khác nhau.

Cuối cùng là lợi ích gì sử dụng dịch vụ như CloudWatch? Vâng, điều đầu tiên là bạn có thể có truy cập vào tất cả các số liệu của bạn từ một vị trí trung tâm. Điều này cho phép bạn thu thập số liệu và nhật ký từ tất cả tài nguyên, ứng dụng AWS của bạn, và các dịch vụ chạy trên AWS và dịch vụ tại chỗ, giúp bạn phá vỡ các rào cản để bạn có thể dễ dàng đạt được khả năng hiển thị trên toàn hệ thống. Bạn cũng có thể có được khả năng hiển thị trên các ứng dụng, cơ sở hạ tầng và dịch vụ của bạn, điều đó có nghĩa là bạn có được thông tin chi tiết về gần xếp phân tán của bạn để bạn có thể tương quan và trực quan hóa các số liệu và nhật ký để nhanh chóng xác định các vấn đề chưa được giải quyết. Điều này có nghĩa là bạn có thể giảm mean time to resolution (trong khi chờ đợi độ phân giải) hoặc **MTTR**, và cải thiện total cost of ownership (tổng chi phí sở hữu) hoặc **TCO**.

## **Amazon CloudWatch**

**Đồng hồ đám mây Amazon** là một dịch vụ web cho phép bạn giám sát và quản lý các số liệu khác nhau cũng như định cấu hình hành động cảnh báo dựa trên dữ liệu từ các số liệu đó.

CloudWatch cho phép bạn giám sát cơ sở hạ tầng AWS của mình và các ứng dụng bạn chạy trên AWS trong thời gian thực.

Sử dụng CloudWatch **số liệu** để thể hiện các điểm dữ liệu cho tài nguyên của bạn. Dịch vụ AWS gửi số liệu tới CloudWatch. Sau đó, CloudWatch sử dụng các số liệu này để tự động tạo biểu đồ cho thấy hiệu suất đã thay đổi như thế nào theo thời gian.

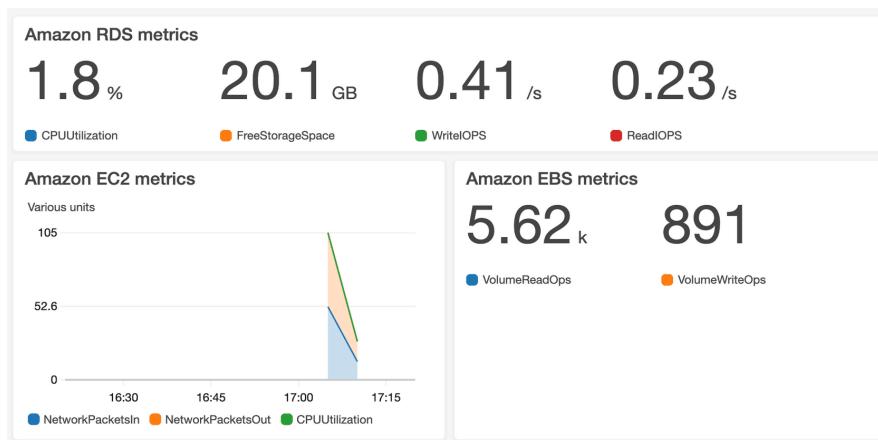
## **CloudWatch Alarms**

Với CloudWatch, bạn có thể tạo alarm (**báo động**) tự động thực hiện hành động nếu giá trị số liệu của bạn vượt quá hoặc dưới ngưỡng được xác định trước.

Ví dụ: giả sử các nhà phát triển của công ty bạn sử dụng phiên bản Amazon EC2 cho mục đích thử nghiệm hoặc phát triển ứng dụng. Nếu nhà phát triển thỉnh thoảng quên dừng phiên bản thì phiên bản đó sẽ tiếp tục chạy và phải chịu phí.

Trong trường hợp này, bạn có thể tạo cảnh báo CloudWatch tự động dừng phiên bản Amazon EC2 khi tỷ lệ sử dụng CPU vẫn ở dưới một ngưỡng nhất định trong một khoảng thời gian nhất định. Khi định cấu hình cảnh báo, bạn có thể chỉ định nhận thông báo bất cứ khi nào cảnh báo này được kích hoạt.

## CloudWatch Dashboard



Đồng hồ đám mây **bảng điều khiển** tính năng này cho phép bạn truy cập tất cả số liệu về tài nguyên của mình từ một vị trí duy nhất. Ví dụ: bạn có thể sử dụng bảng thông tin CloudWatch để giám sát mức sử dụng CPU của phiên bản Amazon EC2, tổng số yêu cầu được gửi đến bộ chia sẻ Amazon S3, v.v. Bạn thậm chí có thể tùy chỉnh các trang tổng quan riêng biệt cho các mục đích kinh doanh, ứng dụng hoặc tài nguyên khác nhau. Các trang tổng quan này sẽ tự động làm mới khi chúng mở để chúng tôi có thể xem thông tin cập nhật về tài nguyên của mình.

## AWS CloudTrail

### AWS CloudTrail

**AWS CloudTrail** ghi lại các lệnh gọi API cho tài khoản của bạn. Thông tin được ghi lại bao gồm danh tính của người gọi API, thời gian gọi API, địa chỉ IP nguồn của người gọi

API, v.v. Bạn có thể coi CloudTrail như một “dấu vết” gồm các mẩu bánh mì (hoặc nhật ký hành động) mà ai đó đã để lại.

Hãy nhớ rằng bạn có thể sử dụng lệnh gọi API để cung cấp, quản lý và đặt cấu hình tài nguyên AWS của mình. Với CloudTrail, bạn có thể xem toàn bộ lịch sử hoạt động của người dùng và các lệnh gọi API cho ứng dụng và tài nguyên của mình.

Các sự kiện thường được cập nhật trong CloudTrail trong vòng 15 phút sau lệnh gọi API. Bạn có thể lọc các sự kiện bằng cách chỉ định ngày và giờ xảy ra lệnh gọi API, người dùng đã yêu cầu hành động, loại tài nguyên liên quan đến lệnh gọi API, v.v.

### Ví dụ: Sự kiện AWS CloudTrail

Giả sử chủ quán cà phê đang duyệt qua phần AWS Identity and Access Management (IAM) của Bảng điều khiển quản lý AWS. Họ phát hiện ra rằng một người dùng IAM mới có tên Mary đã được tạo, nhưng họ không biết ai, khi nào hoặc phương pháp nào đã tạo ra người dùng đó.

Để trả lời những câu hỏi này, chủ sở hữu hãy truy cập AWS CloudTrail.

<u>What</u> happened?	A new IAM user (Mary) was created.	
<u>Who</u> made the request?	IAM user John	
<u>When</u> did this occur?	January 1, 2020 at 9:00 AM	
<u>How</u> was the request made?	Through the AWS Management Console	

Trong phần Lịch sử sự kiện CloudTrail, chủ sở hữu áp dụng bộ lọc để chỉ hiển thị các sự kiện cho hành động API “Tạo người dùng” trong IAM. Chủ sở hữu xác định sự kiện cho lệnh gọi API đã tạo người dùng IAM cho Mary. Bản ghi sự kiện này cung cấp chi tiết đầy đủ về những gì đã xảy ra:

Vào lúc 9:00 sáng ngày 1 tháng 1 năm 2020, người dùng IAM John đã tạo một người dùng IAM mới (Mary) thông qua Bảng điều khiển quản lý AWS.

### Thông tin chi tiết về CloudTrail

Trong CloudTrail, bạn cũng có thể kích hoạt [Thông tin chi tiết về CloudTrail](#). Tính năng tùy chọn này cho phép CloudTrail tự động phát hiện các hoạt động API bất thường trong tài khoản AWS của bạn.

Ví dụ: CloudTrail Insights có thể phát hiện thấy số lượng phiên bản Amazon EC2 gần đây đã được khởi chạy trong tài khoản của bạn cao hơn bình thường. Sau đó, bạn có thể xem lại toàn bộ chi tiết sự kiện để xác định hành động nào bạn cần thực hiện tiếp theo.

## AWS Trusted Advisor

### AWS Trusted Advisor

**AWS Trusted Advisor** là dịch vụ web kiểm tra môi trường AWS của bạn và cung cấp các đề xuất theo thời gian thực theo các biện pháp thực hành tốt nhất của AWS.

Trusted Advisor so sánh những phát hiện của mình với các biện pháp thực hành tốt nhất của AWS ở năm hạng mục: **cost optimization, performance, security, fault tolerance, and service limits** (tối ưu hóa chi phí, hiệu suất, bảo mật, khả năng chịu lỗi và giới hạn dịch vụ). Đối với các bước kiểm tra trong từng danh mục, Trusted Advisor cung cấp danh sách các hành động được đề xuất và tài nguyên bổ sung để tìm hiểu thêm về các biện pháp thực hành tốt nhất của AWS.

Hướng dẫn do AWS Trusted Advisor cung cấp có thể mang lại lợi ích cho công ty của bạn ở mọi giai đoạn triển khai. Ví dụ: bạn có thể sử dụng AWS Trusted Advisor để hỗ trợ bạn trong khi tạo quy trình làm việc mới và phát triển ứng dụng mới. Hoặc bạn có thể sử dụng nó trong khi đang thực hiện các cải tiến liên tục cho các ứng dụng và tài nguyên hiện có.

### AWS Trusted Advisor Dashboard



Khi truy cập bảng thông tin Trusted Advisor trên Bảng điều khiển quản lý AWS, bạn có thể xem lại các bước kiểm tra đã hoàn thành để tối ưu hóa chi phí, hiệu suất, bảo mật, khả năng chịu lỗi và giới hạn dịch vụ.

Đối với mỗi danh mục:

- Kiểm tra màu xanh lá cây cho biết số lượng mục mà nó phát hiện **không có vấn đề gì**.
- Hình tam giác màu cam thể hiện số lượng **cuộc điều tra** được đề xuất.
- Vòng tròn màu đỏ thể hiện số lượng **hành động** được đề xuất.

# AWS Free Tier

## AWS Free Tier

Các [Bậc miễn phí của AWS](#) cho phép bạn bắt đầu sử dụng một số dịch vụ nhất định mà không phải lo lắng về việc phát sinh chi phí trong khoảng thời gian nhất định.

Ba loại ưu đãi có sẵn:

- Luôn luôn miễn phí
- 12 tháng miễn phí
- Thủ nghiệm

Đối với mỗi ưu đãi bậc miễn phí, hãy đảm bảo xem lại chi tiết cụ thể về chính xác loại tài nguyên nào được bao gồm.

### Always Free

Những ưu đãi này không hết hạn và dành cho tất cả khách hàng AWS.

Ví dụ: AWS Lambda cho phép 1 triệu yêu cầu miễn phí và thời gian tính toán lên tới 3,2 triệu giây mỗi tháng. Amazon DynamoDB cho phép 25 GB dung lượng lưu trữ miễn phí mỗi tháng.

### 12 Months Free

Những ưu đãi này miễn phí trong 12 tháng kể từ ngày bạn đăng ký AWS lần đầu.

Các ví dụ bao gồm số lượng cụ thể của Bộ lưu trữ tiêu chuẩn Amazon S3, ngưỡng cho số giờ tính toán hàng tháng của Amazon EC2 và lượng dữ liệu Amazon CloudFront truyền đi.

### Trials

Ưu đãi dùng thử miễn phí ngắn hạn bắt đầu từ ngày bạn kích hoạt một dịch vụ cụ thể. Thời lượng của mỗi lần dùng thử có thể thay đổi tùy theo số ngày hoặc lượng sử dụng dịch vụ.

Ví dụ: Amazon Inspector cung cấp bản dùng thử miễn phí 90 ngày. Amazon Lightsail (dịch vụ cho phép bạn chạy máy chủ riêng ảo) cung cấp 750 giờ sử dụng miễn phí trong khoảng thời gian 30 ngày.

## AWS Pricing Concepts

### How AWS Pricing Works

AWS cung cấp nhiều dịch vụ điện toán đám mây với mức giá thanh toán theo nhu cầu sử dụng.

#### **Pay for what you use.**

Đối với mỗi dịch vụ, bạn trả tiền chính xác cho lượng tài nguyên mà bạn thực sự sử dụng mà không yêu cầu hợp đồng dài hạn hoặc giấy phép phức tạp.

#### **Pay less when you reserve.**

Một số dịch vụ cung cấp các tùy chọn đặt trước với mức chiết khấu đáng kể so với giá Phiên bản theo yêu cầu.

Ví dụ: giả sử công ty của bạn đang sử dụng phiên bản Amazon EC2 cho khối lượng công việc cần chạy liên tục. Bạn có thể chọn chạy khối lượng công việc này trên Gói tiết kiệm phiên bản Amazon EC2 vì gói này cho phép bạn tiết kiệm tới 72% so với dung lượng Phiên bản theo yêu cầu tương đương.

#### **Pay less with volume-based discounts when you use more.**

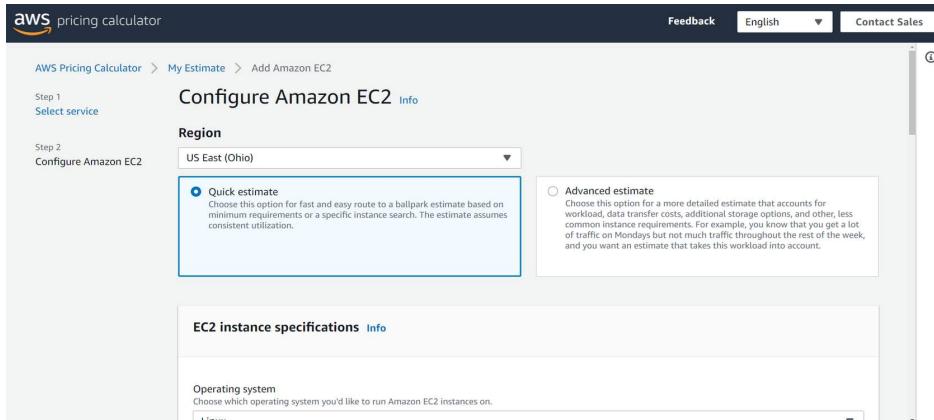
Một số dịch vụ đưa ra mức giá theo từng cấp, do đó chi phí trên mỗi đơn vị sẽ giảm dần khi mức độ sử dụng tăng lên.

Ví dụ: bạn càng sử dụng nhiều dung lượng lưu trữ Amazon S3 thì bạn càng phải trả ít tiền hơn cho mỗi GB.

### AWS Pricing Calculator

Các [Công cụ tính giá AWS](#) cho phép bạn khám phá các dịch vụ AWS và tạo ước tính chi phí cho các trường hợp sử dụng của bạn trên AWS. Bạn có thể sắp xếp các ước tính AWS theo nhóm mà bạn xác định. Một nhóm có thể phản ánh cách tổ chức công ty của bạn, chẳng hạn như cung cấp các ước tính theo trung tâm chi phí.

Khi bạn đã tạo ước tính, bạn có thể lưu ước tính đó và tạo liên kết để chia sẻ ước tính đó với người khác.



Giả sử công ty của bạn quan tâm đến việc sử dụng Amazon EC2. Tuy nhiên, bạn vẫn chưa chắc chắn AWS Region hoặc instance type nào sẽ tiết kiệm chi phí nhất cho trường hợp sử dụng của mình. Trong Công cụ tính giá AWS, bạn có thể nhập các thông tin chi tiết như loại hệ điều hành bạn cần, yêu cầu về bộ nhớ và yêu cầu đầu vào/đầu ra (I/O). Bằng cách sử dụng Công cụ tính giá AWS, bạn có thể xem lại kết quả so sánh ước tính của các loại phiên bản EC2 khác nhau trên các Khu vực AWS.

## AWS Pricing Examples

### AWS Lambda Pricing

Đối với AWS Lambda, bạn bị tính phí dựa trên số lượng yêu cầu cho các chức năng của bạn và thời gian cần thiết để chạy các chức năng đó.

AWS Lambda cho phép 1 triệu yêu cầu miễn phí và thời gian tính toán lên tới 3,2 triệu giây mỗi tháng.

Bạn có thể tiết kiệm chi phí AWS Lambda bằng cách đăng ký **Compute Savings Plan** (Kế hoạch tiết kiệm điện toán). Kế hoạch tiết kiệm điện toán cung cấp chi phí điện toán thấp hơn để đổi lấy việc cam kết mức sử dụng nhất quán trong thời hạn 1 năm hoặc 3 năm. Đây là một ví dụ về **việc trả ít hơn khi bạn đặt trước**.

### AWS Lambda Pricing Example

Nếu đã sử dụng AWS Lambda ở nhiều Khu vực AWS, bạn có thể xem các khoản phí được chia thành từng khoản theo Khu vực hóa đơn của mình.

Trong ví dụ này, tất cả hoạt động sử dụng AWS Lambda đều diễn ra ở Khu vực Bắc Virginia. Dự luật liệt kê các khoản phí riêng cho số lượng yêu cầu chức năng và thời lượng của chúng.

Cả số lượng yêu cầu và tổng thời lượng yêu cầu trong ví dụ này đều nằm dưới ngưỡng trong Bậc miễn phí của AWS, do đó chủ tài khoản sẽ không phải trả bất kỳ mức sử dụng AWS Lambda nào trong tháng này.

▼ Lambda		\$0.00
▼ US East (N. Virginia)		\$0.00
AWS Lambda Lambda-GB-Second		\$0.00
AWS Lambda - Compute Free Tier - 400,000 GB-Seconds - US East (Northern Virginia)	254.575 seconds	\$0.00
AWS Lambda Request		\$0.00
AWS Lambda - Requests Free Tier - 1,000,000 Requests - US East (Northern Virginia)	680.000 Requests	\$0.00

## Amazon EC2 Pricing

Với Amazon EC2, bạn chỉ phải trả tiền cho thời gian tính toán mà bạn sử dụng trong khi phiên bản của bạn đang chạy.

Đối với một số khối lượng công việc, bạn có thể giảm đáng kể chi phí Amazon EC2 bằng cách sử dụng **Spot Instances** (Phiên bản dùng ngay). Ví dụ: giả sử bạn đang chạy một công việc xử lý hàng loạt có khả năng chịu được sự gián đoạn. Sử dụng Phiên bản dùng ngay sẽ giúp bạn tiết kiệm tới 90% chi phí trong khi vẫn đáp ứng các yêu cầu về tính khả dụng của khối lượng công việc của bạn.

Bạn có thể tiết kiệm thêm chi phí cho Amazon EC2 bằng cách xem xét Savings Plans và Reserved Instances.

## Amazon EC2 Pricing Example

Phí dịch vụ trong ví dụ này bao gồm chi tiết cho các mục sau:

- Mỗi loại phiên bản Amazon EC2 đã được sử dụng
- Dung lượng lưu trữ Amazon EBS đã được cung cấp
- Khoảng thời gian mà Cân bằng tải đàm hồi đã được sử dụng

Trong ví dụ này, tất cả lượng sử dụng đều nằm dưới ngưỡng trong Bậc miễn phí của AWS, do đó chủ sở hữu tài khoản sẽ không phải trả bất kỳ mức sử dụng Amazon EC2 nào trong tháng này.

▼ Elastic Compute Cloud		\$0.00
▼ US East (N. Virginia)		\$0.00
Amazon Elastic Compute Cloud running Linux/UNIX		\$0.00
\$0.00 per Linux t2.micro instance-hour (or partial hour) under monthly free tier	106.512 Hrs	\$0.00
EBS		\$0.00
\$0.00 per GB-month of General Purpose (SSD) provisioned storage under monthly free tier	11.294 GB-Mo	\$0.00
Elastic Load Balancing - Application		\$0.00
\$0.00 per Application LoadBalancer-hour (or partial hour) under monthly free tier	268.000 Hrs	\$0.00

## Amazon S3 Pricing

Để biết giá của Amazon S3, hãy xem xét các thành phần chi phí sau:

- **Dung lượng** - Bạn chỉ trả tiền cho dung lượng lưu trữ mà bạn sử dụng. Bạn bị tính phí lưu trữ đối tượng trong bộ chứa Amazon S3 dựa trên kích thước, lớp lưu trữ của đối tượng và thời gian bạn đã lưu trữ từng đối tượng trong tháng.
- **Yêu cầu và truy xuất dữ liệu** - Bạn trả tiền cho các yêu cầu được gửi tới đối tượng và bộ chứa Amazon S3 của bạn. Ví dụ: giả sử bạn đang lưu trữ tệp ảnh trong bộ chứa Amazon S3 và lưu trữ chúng trên một trang web. Mỗi khi khách truy cập yêu cầu trang web có chứa các tệp ảnh này, điều này sẽ được tính vào yêu cầu bạn phải trả tiền.
- **Truyền dữ liệu** - Không mất phí khi truyền dữ liệu giữa các nhóm Amazon S3 khác nhau hoặc từ Amazon S3 sang các dịch vụ khác trong cùng Khu vực AWS. Tuy nhiên, bạn phải trả phí cho dữ liệu bạn truyền vào và ra khỏi Amazon S3, trừ một số trường hợp ngoại lệ. Không mất phí khi truyền dữ liệu vào Amazon S3 từ Internet hoặc ra Amazon CloudFront. Dữ liệu được truyền sang phiên bản Amazon EC2 trong cùng Khu vực AWS với bộ chứa Amazon S3 cũng không bị tính phí.
- **Quản lý và sao chép** - Bạn trả tiền cho các tính năng quản lý lưu trữ mà bạn đã kích hoạt trên bộ chứa Amazon S3 trong tài khoản của mình. Các tính năng này bao gồm kiểm kê, phân tích và gắn thẻ đối tượng của Amazon S3.

## Amazon S3 Pricing Example

Tài khoản AWS trong ví dụ này đã sử dụng Amazon S3 ở hai Khu vực: Bắc Virginia và Ohio. Đối với mỗi Khu vực, các khoản phí được chia thành từng khoản dựa trên các yếu tố sau:

- Số lượng yêu cầu thêm hoặc sao chép đối tượng vào một nhóm
- Số lượng yêu cầu truy xuất đối tượng từ một nhóm

- Dung lượng lưu trữ được sử dụng

Tất cả mức sử dụng Amazon S3 trong ví dụ này đều nằm trong giới hạn Bậc miễn phí của AWS, do đó chủ sở hữu tài khoản sẽ không phải trả tiền cho bất kỳ mức sử dụng Amazon S3 nào trong tháng này.

Simple Storage Service		\$0.00
US East (N. Virginia)		\$0.00
Amazon Simple Storage Service Requests-Tier1		\$0.00
\$0.00 per request - PUT, COPY, POST, or LIST requests under the monthly global free tier	185.000 Requests	\$0.00
Amazon Simple Storage Service Requests-Tier2		\$0.00
\$0.00 per request - GET and all other requests under the monthly global free tier	923.000 Requests	\$0.00
Amazon Simple Storage Service TimedStorage-ByteHrs		\$0.00
\$0.000 per GB - storage under the monthly global free tier	0.159 GB-Mo	\$0.00
US East (Ohio)		\$0.00
Amazon Simple Storage Service USE2-Requests-Tier2		\$0.00
\$0.00 per request - GET and all other requests under the monthly global free tier	4.000 Requests	\$0.00
Amazon Simple Storage Service USE2-TimedStorage-ByteHrs		\$0.00
\$0.000 per GB - storage under the monthly global free tier	0.000001 GB-Mo	\$0.00

## Billing Dashboard

Sử dụng [AWS Billing & Cost Management dashboard](#) ([Bảng thông tin quản lý chi phí và thanh toán AWS](#)) để thanh toán hóa đơn AWS, giám sát việc sử dụng cũng như phân tích và kiểm soát chi phí của bạn.

- So sánh số dư hiện tại hàng tháng của bạn với tháng trước và nhận dự báo cho tháng tiếp theo dựa trên mức sử dụng hiện tại.
- Xem chi tiêu hàng tháng theo dịch vụ.
- Xem mức sử dụng Bậc miễn phí theo dịch vụ.
- Truy cập Cost Explorer và tạo ngân sách.
- Mua và quản lý các kế hoạch tiết kiệm.
- Công bố [Báo cáo chi phí và mức sử dụng AWS](#).

## Consolidated Billing

Trong mô-đun trước, bạn đã tìm hiểu về **AWS Organizations**, một dịch vụ cho phép bạn quản lý nhiều tài khoản AWS từ một vị trí trung tâm. **AWS Organizations** cũng

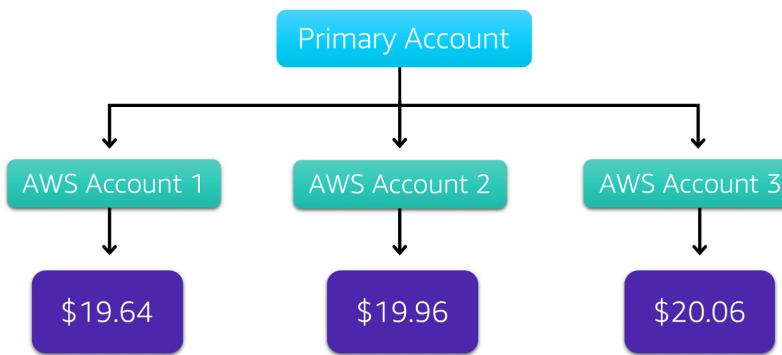
cung cấp tùy chọn cho **consolidated billing (thanh toán tổng hợp)**.

Tính năng thanh toán tổng hợp của AWS Orgs cho phép bạn nhận một hóa đơn duy nhất cho tất cả tài khoản AWS trong tổ chức của mình. Bằng cách hợp nhất, bạn có thể dễ dàng theo dõi chi phí kết hợp của tất cả các tài khoản được liên kết trong tổ chức của mình. Số lượng tài khoản tối đa mặc định được phép cho một tổ chức là 4, nhưng bạn có thể liên hệ với bộ phận Hỗ trợ AWS để tăng hạn ngạch nếu cần.

Trên hóa đơn hàng tháng của mình, bạn có thể xem lại các khoản phí được chia thành từng khoản mà mỗi tài khoản phải chịu. Điều này cho phép bạn có được sự minh bạch cao hơn đối với các tài khoản của tổ chức mình trong khi vẫn duy trì sự thuận tiện khi nhận được một hóa đơn hàng tháng.

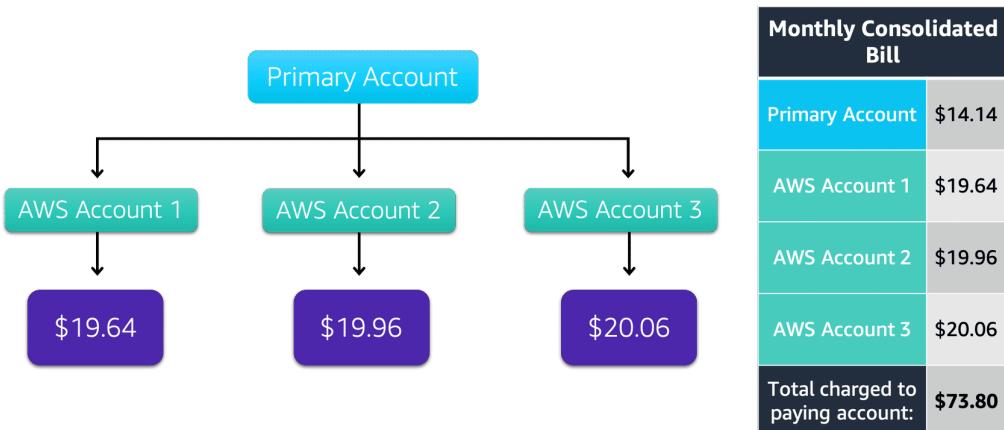
Một lợi ích khác của thanh toán tổng hợp là khả năng chia sẻ giá chiết khấu hàng loạt, Gói tiết kiệm và Phiên bản dự trữ trên các tài khoản trong tổ chức của bạn. Ví dụ: một tài khoản có thể không có đủ mức sử dụng hàng tháng để đủ điều kiện được giảm giá. Tuy nhiên, khi kết hợp nhiều tài khoản, việc sử dụng tổng hợp của chúng có thể mang lại lợi ích áp dụng cho tất cả các tài khoản trong tổ chức.

### Ví dụ: Thanh toán tổng hợp



Giả sử bạn là lãnh đạo doanh nghiệp giám sát việc thanh toán AWS của công ty bạn. Công ty của bạn có ba tài khoản AWS được sử dụng cho các phòng ban riêng biệt. Thay vì thanh toán riêng hóa đơn hàng tháng của từng địa điểm, bạn quyết định tạo một tổ chức và thêm ba tài khoản.

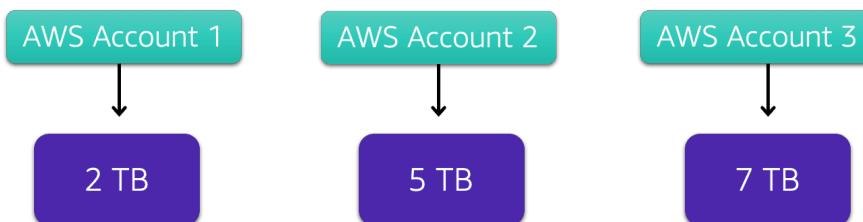
Bạn quản lý tổ chức thông qua tài khoản chính.



Hàng tháng, AWS tính phí tài khoản người thanh toán chính của bạn cho tất cả các tài khoản được liên kết trong một hóa đơn tổng hợp. Thông qua tài khoản chính, bạn cũng có thể nhận được báo cáo chi phí chi tiết cho từng tài khoản được liên kết.

Hóa đơn tổng hợp hàng tháng cũng bao gồm chi phí sử dụng tài khoản mà tài khoản chính phải chịu. Chi phí này không phải là phí bảo hiểm khi có tài khoản chính.

Hóa đơn tổng hợp hiển thị chi phí liên quan đến bất kỳ hành động nào của tài khoản chính (chẳng hạn như lưu trữ tệp trong Amazon S3 hoặc chạy phiên bản Amazon EC2).



Thanh toán tổng hợp cũng cho phép bạn chia sẻ mức giảm giá theo số lượng trên các tài khoản.

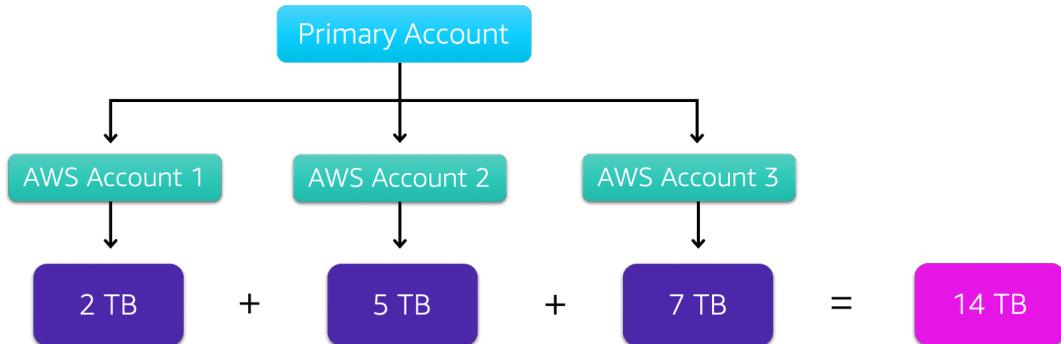
Một số dịch vụ AWS, chẳng hạn như Amazon S3, cung cấp mức giảm giá theo số lượng giúp bạn có mức giá thấp hơn khi bạn sử dụng dịch vụ nhiều hơn. Trong Amazon S3, sau khi khách hàng truyền 10 TB dữ liệu trong một tháng, họ sẽ trả mức giá truyền trên mỗi GB thấp hơn cho 40 TB dữ liệu tiếp theo được truyền.

Trong ví dụ này, có ba tài khoản AWS riêng biệt đã truyền lượng dữ liệu khác nhau trên Amazon S3 trong tháng hiện tại:

- Tài khoản 1 đã chuyển 2 TB dữ liệu.
- Tài khoản 2 đã chuyển 5 TB dữ liệu.
- Tài khoản 3 đã chuyển 7 TB dữ liệu.

Vì chưa có tài khoản nào vượt qua ngưỡng 10 TB nên không tài khoản nào trong số đó đủ điều kiện nhận mức giá truyền theo mỗi GB thấp hơn cho 40 TB dữ liệu tiếp theo

được truyền.



Bây giờ, giả sử ba tài khoản riêng biệt này được tập hợp lại dưới dạng tài khoản được liên kết trong một tổ chức AWS duy nhất và đang sử dụng phương thức thanh toán tổng hợp.

Khi mức sử dụng Amazon S3 cho ba tài khoản được liên kết được kết hợp ( $2+5+7$ ), điều này dẫn đến tổng lượng truyền dữ liệu là 14 TB. Điều này vượt quá ngưỡng 10 TB.

Với tính năng thanh toán tổng hợp, AWS kết hợp mức sử dụng từ tất cả các tài khoản để xác định mức giá theo số lượng nào sẽ áp dụng, mang lại cho bạn mức giá tổng thể thấp hơn bất cứ khi nào có thể. Sau đó, AWS sẽ phân bổ cho mỗi tài khoản được liên kết một phần chiết khấu tổng số lượng dựa trên mức sử dụng của tài khoản.

Trong ví dụ này, Tài khoản 3 sẽ nhận được phần chiết khấu lớn hơn trong tổng khối lượng vì ở mức 7 TB, tài khoản này đã truyền nhiều dữ liệu hơn Tài khoản 1 (ở mức 2 TB) và Tài khoản 2 (ở mức 5 TB).

## AWS Budgets

### AWS Budgets

TRONG [Ngân sách AWS](#), bạn có thể tạo ngân sách để lập kế hoạch sử dụng dịch vụ, chi phí dịch vụ và đặt trước phiên bản.

Thông tin trong AWS Budgets cập nhật ba lần một ngày. Điều này giúp bạn xác định chính xác mức độ sử dụng của bạn gần với mức dự toán hoặc giới hạn Bậc miễn phí của AWS.

Trong AWS Budgets, bạn cũng có thể đặt cảnh báo tùy chỉnh khi mức sử dụng của bạn vượt quá (hoặc được dự đoán là vượt quá) số tiền dự kiến.

### Ví dụ: AWS Budgets

Giả sử bạn đã đặt ngân sách cho Amazon EC2. Bạn muốn đảm bảo rằng mức sử dụng Amazon EC2 của công ty bạn không vượt quá 200 USD mỗi tháng.

Trong AWS Budgets, bạn có thể đặt ngân sách tùy chỉnh để thông báo cho bạn khi mức sử dụng của bạn đã đạt đến một nửa số tiền này (\$100). Cài đặt này sẽ cho phép bạn nhận được cảnh báo và quyết định cách bạn muốn tiếp tục sử dụng Amazon EC2.

AWS Budgets							
<input type="text"/> Filter by budget name							
All budgets (7)	Cost budgets (5)	Usage budgets (2)	Reservation budgets (0)				
Budget name	Budget type	Current	Budgeted	Forecasted	Current vs. budgeted	Forecasted vs. budgeted	
Project Nemo Cost Budget	Cost	\$43.90	\$45.00	\$56.33	<div style="width: 97.55%; background-color: #0072bc;"></div> 97.55%	<div style="width: 125.17%; background-color: #e74c3c;"></div> 125.17%	...
Eastern US Regional Budget	Cost	\$85.21	\$100.00	\$125.28	<div style="width: 85.21%; background-color: #0072bc;"></div> 85.21%	<div style="width: 125.28%; background-color: #e74c3c;"></div> 125.28%	...
Total Monthly Cost Budget	Cost	\$141.50	\$175.00	\$187.00	<div style="width: 80.86%; background-color: #0072bc;"></div> 80.86%	<div style="width: 106.86%; background-color: #e74c3c;"></div> 106.86%	...
Total EC2 Cost Budget	Cost	\$136.90	\$200.00	\$195.21	<div style="width: 68.45%; background-color: #0072bc;"></div> 68.45%	<div style="width: 97.61%; background-color: #0072bc;"></div> 97.61%	...
S3 Usage Budget	Usage	3,601 Requests	5,500 Requests	4,675.75 Requests	<div style="width: 65.47%; background-color: #0072bc;"></div> 65.47%	<div style="width: 85.01%; background-color: #0072bc;"></div> 85.01%	...

Trong ngân sách mẫu này, bạn có thể xem lại các chi tiết quan trọng sau:

- Số tiền hiện tại bạn phải trả cho Amazon EC2 tính đến tháng này (\$136,90)
- Số tiền dự kiến bạn sẽ chi tiêu trong tháng (\$195,21), dựa trên cách sử dụng của bạn.

Bạn cũng có thể xem lại các so sánh giữa mức sử dụng hiện tại và mức sử dụng theo ngân sách cũng như mức sử dụng dự kiến so với mức sử dụng theo ngân sách.

Ví dụ: ở hàng trên cùng của ngân sách mẫu này, thanh dự báo so với ngân sách là 125,17%. Lý do tăng là số tiền dự kiến (\$56,33) vượt quá số tiền đã được lập ngân sách cho mục đó trong tháng (\$45,00).

## AWS Cost Explorer

### AWS Cost Explorer

[Trình khám phá chi phí AWS](#) là một công cụ cho phép bạn trực quan hóa, hiểu rõ và quản lý chi phí cũng như mức sử dụng AWS của mình theo thời gian.

AWS Cost Explorer bao gồm một báo cáo mặc định về chi phí và mức sử dụng cho 5 dịch vụ AWS tích lũy chi phí hàng đầu của bạn. Bạn có thể áp dụng các bộ lọc và nhóm

tùy chỉnh để phân tích dữ liệu của mình. Ví dụ: bạn có thể xem việc sử dụng tài nguyên ở cấp độ hàng giờ.

## Ví dụ: AWS Cost Explorer



Ví dụ này về bảng thông tin AWS Cost Explorer hiển thị chi phí hàng tháng cho các phiên bản Amazon EC2 trong khoảng thời gian 6 tháng. Thanh cho mỗi tháng phân chia chi phí cho các loại phiên bản Amazon EC2 khác nhau (chẳng hạn như t2.micro hoặc m3.large).

Bằng cách phân tích chi phí AWS theo thời gian, bạn có thể đưa ra quyết định sáng suốt về chi phí trong tương lai và cách lập kế hoạch ngân sách của mình.

## AWS Support Plans

### Hỗ trợ AWS

AWS cung cấp bốn loại khác nhau **Kế hoạch hỗ trợ** để giúp bạn khắc phục sự cố, giảm chi phí và sử dụng hiệu quả các dịch vụ AWS.

Bạn có thể chọn trong số các gói Hỗ trợ sau để đáp ứng nhu cầu của công ty bạn:

- Basic
- Developer
- Business
- Enterprise On-Ramp
- Enterprise

## Basic Support

**Hỗ trợ cơ bản** miễn phí cho tất cả khách hàng AWS. Nó bao gồm quyền truy cập vào các báo cáo nghiên cứu chuyên sâu, tài liệu và cộng đồng hỗ trợ. Với Hỗ trợ cơ bản, bạn cũng có thể liên hệ với AWS nếu có thắc mắc về thanh toán và tăng giới hạn dịch vụ.

Với Hỗ trợ cơ bản, bạn có quyền truy cập vào một số bài kiểm tra có giới hạn của AWS Trusted Advisor. Ngoài ra, bạn có thể sử dụng **AWS Personal Health Dashboard**, một công cụ cung cấp cảnh báo và hướng dẫn khắc phục khi AWS gặp phải các sự kiện có thể ảnh hưởng đến bạn.

## Developer, Business, Enterprise On-Ramp, and Enterprise Support

Các gói Nhà phát triển, Doanh nghiệp, Doanh nghiệp trực tuyến và Hỗ trợ doanh nghiệp bao gồm tất cả các lợi ích của Hỗ trợ cơ bản, bên cạnh khả năng mở số lượng trường hợp hỗ trợ kỹ thuật không hạn chế. Ba gói Hỗ trợ này có mức giá thanh toán theo tháng và không yêu cầu hợp đồng dài hạn.

Nhìn chung, về mặt giá cả, gói Nhà phát triển có chi phí thấp nhất, gói Doanh nghiệp và Doanh nghiệp On-Ramp ở mức trung bình và gói Doanh nghiệp có chi phí cao nhất.

## Developer Support

Khách hàng trong gói **Developer Support** có quyền truy cập vào các tính năng như:

- Hướng dẫn thực hành tốt nhất
- Công cụ chẩn đoán phía máy khách
- Hỗ trợ kiến trúc khối xây dựng, bao gồm hướng dẫn về cách sử dụng đồng thời các sản phẩm, tính năng và dịch vụ của AWS

Ví dụ: giả sử công ty của bạn đang khám phá các dịch vụ AWS. Bạn đã nghe nói về một số dịch vụ AWS khác nhau. Tuy nhiên, bạn không chắc chắn về khả năng sử dụng chúng cùng nhau để xây dựng các ứng dụng có thể đáp ứng nhu cầu của công ty bạn. Trong trường hợp này, hỗ trợ kiến trúc khối xây dựng đi kèm với gói Hỗ trợ nhà phát triển có thể giúp bạn xác định các cơ hội kết hợp các dịch vụ và tính năng cụ thể.

## **Business Support**

Khách hàng có gói **Business Support** có quyền truy cập vào các tính năng bổ sung, bao gồm:

- Hướng dẫn trường hợp sử dụng để xác định các sản phẩm, tính năng và dịch vụ AWS có thể hỗ trợ tốt nhất cho nhu cầu cụ thể của bạn
- Tất cả các bước kiểm tra của AWS Trusted Advisor
- Hỗ trợ hạn chế cho phần mềm của bên thứ ba, chẳng hạn như các hệ điều hành phổ biến và các thành phần ngăn xếp ứng dụng

Giả sử công ty của bạn có gói Hỗ trợ kinh doanh và muốn cài đặt hệ điều hành chung của bên thứ ba vào các phiên bản Amazon EC2 của bạn. Bạn có thể liên hệ với bộ phận Hỗ trợ AWS để được hỗ trợ cài đặt, định cấu hình và khắc phục sự cố hệ điều hành. Đối với các chủ đề nâng cao như tối ưu hóa hiệu suất, sử dụng tập lệnh tùy chỉnh hoặc giải quyết các vấn đề bảo mật, bạn có thể cần liên hệ trực tiếp với nhà cung cấp phần mềm bên thứ ba.

## **Enterprise On-Ramp Support**

Vào tháng 11 năm 2021, AWS đã mở đăng ký gói AWS Enterprise On-Ramp Support. Ngoài tất cả các tính năng có trong gói Hỗ trợ cơ bản, Nhà phát triển và Hỗ trợ doanh nghiệp, khách hàng có gói Hỗ trợ trên đường nối dành cho doanh nghiệp còn có quyền truy cập vào:

- Một nhóm Người quản lý tài khoản kỹ thuật để cung cấp hướng dẫn chủ động và điều phối quyền truy cập vào các chương trình và chuyên gia AWS
- Hội thảo Tối ưu hóa chi phí (mỗi năm một lần)
- Nhóm hỗ trợ Concierge để hỗ trợ thanh toán và tài khoản
- Các công cụ để giám sát chi phí và hiệu suất thông qua Trusted Advisor và Health API/Dashboard

Gói Hỗ trợ On-Ramp dành cho Doanh nghiệp cũng cung cấp quyền truy cập vào một nhóm dịch vụ hỗ trợ chủ động cụ thể do một nhóm Người quản lý tài khoản kỹ thuật cung cấp.

- Đánh giá tư vấn và hướng dẫn kiến trúc (mỗi năm một lần)
- Hỗ trợ quản lý sự kiện cơ sở hạ tầng (một lần mỗi năm)
- Hỗ trợ quy trình làm việc tự động hóa
- Thời gian phản hồi 30 phút hoặc ít hơn cho các vấn đề quan trọng trong kinh doanh

## **Hỗ trợ doanh nghiệp**

Ngoài tất cả các tính năng có trong các gói hỗ trợ Cơ bản, Nhà phát triển, Doanh nghiệp và Doanh nghiệp trên đường nối, khách hàng có Hỗ trợ Doanh nghiệp còn có quyền truy cập vào:

- Người quản lý tài khoản kỹ thuật được chỉ định để cung cấp hướng dẫn chủ động và điều phối quyền truy cập vào các chương trình và chuyên gia AWS
- Nhóm hỗ trợ Concierge để hỗ trợ thanh toán và tài khoản
- Hoạt động Đánh giá và công cụ theo dõi sức khỏe
- Ngày đào tạo và trò chơi để thúc đẩy sự đổi mới
- Các công cụ để giám sát chi phí và hiệu suất thông qua Trusted Advisor và Health API/Dashboard

Gói Doanh nghiệp cũng cung cấp quyền truy cập đầy đủ vào các dịch vụ chủ động do Người quản lý tài khoản kỹ thuật được chỉ định cung cấp:

- Đánh giá tư vấn và hướng dẫn kiến trúc
- Hỗ trợ quản lý sự kiện cơ sở hạ tầng
- Hội thảo và công cụ tối ưu hóa chi phí
- Hỗ trợ quy trình làm việc tự động hóa
- Thời gian phản hồi 15 phút hoặc ít hơn đối với các vấn đề quan trọng trong kinh doanh

### **Technical Account Manager (TAM)**

Các gói Enterprise On-Ramp và Enterprise Support bao gồm quyền truy cập vào **Trình quản lý tài khoản kỹ thuật (TAM)**. TAM là đầu mối liên hệ chính của bạn tại AWS. Nếu công ty của bạn đăng ký Hỗ trợ doanh nghiệp hoặc Enterprise On-Ramp, TAM của bạn sẽ hướng dẫn, trao quyền và phát triển hành trình đám mây của bạn trên toàn bộ các dịch vụ AWS. TAM cung cấp hướng dẫn kỹ thuật chuyên môn, giúp bạn thiết kế các giải pháp tích hợp hiệu quả các dịch vụ AWS, hỗ trợ kiến trúc linh hoạt và tiết kiệm chi phí, đồng thời cung cấp quyền truy cập trực tiếp vào các chương trình AWS và cộng đồng chuyên gia rộng lớn. Ví dụ: giả sử bạn quan tâm đến việc phát triển một ứng dụng sử dụng nhiều dịch vụ AWS cùng nhau. TAM của bạn có thể cung cấp thông tin chuyên sâu về cách sử dụng các dịch vụ một cách tốt nhất. Họ đạt được điều này, đồng thời phù hợp với các nhu cầu cụ thể mà công ty bạn đang hy vọng giải quyết thông qua ứng dụng mới.

## **AWS Marketplace**

## AWS Marketplace

Thị trường AWS là một danh mục kỹ thuật số bao gồm hàng nghìn danh sách phần mềm từ các nhà cung cấp phần mềm độc lập. Bạn có thể sử dụng AWS Marketplace để tìm, kiểm tra và mua phần mềm chạy trên AWS.

Đối với mỗi danh sách trên AWS Marketplace, bạn có thể truy cập thông tin chi tiết về các tùy chọn giá, hỗ trợ có sẵn và đánh giá từ các khách hàng AWS khác.

Bạn cũng có thể khám phá các giải pháp phần mềm theo ngành và trường hợp sử dụng. Ví dụ: giả sử công ty của bạn hoạt động trong ngành chăm sóc sức khỏe. Trong AWS Marketplace, bạn có thể xem xét các trường hợp sử dụng mà phần mềm giúp bạn giải quyết, chẳng hạn như triển khai các giải pháp bảo vệ hồ sơ bệnh nhân hoặc sử dụng mô hình học máy để phân tích lịch sử y tế của bệnh nhân và dự đoán các rủi ro sức khỏe có thể xảy ra.

## AWS Marketplace Categories



Infrastructure Software



DevOps



Data Products



Professional Services



Business Applications



Machine Learning



Industries



Internet of Things (IoT)

AWS Marketplace cung cấp các sản phẩm thuộc nhiều danh mục, chẳng hạn như Phần mềm cơ sở hạ tầng, DevOps, Sản phẩm dữ liệu, Dịch vụ chuyên nghiệp, Ứng dụng kinh doanh, Học máy, Công nghiệp và Internet vạn vật (IoT).

Trong mỗi danh mục, bạn có thể thu hẹp tìm kiếm của mình bằng cách duyệt qua danh sách sản phẩm trong các danh mục phụ. Ví dụ: các danh mục phụ trong danh mục DevOps bao gồm các lĩnh vực như Phát triển ứng dụng, Giám sát và Thử nghiệm.

# AWS Cloud Adoption Framework (AWS CAF)

Migrating sang Cloud là một quá trình. Bạn không chỉ búng ngón tay và có mọi thứ được lưu trữ một cách kỳ diệu trong AWS. Phải mất rất nhiều nỗ lực để có được các ứng dụng được di chuyển sang AWS. Nhóm dịch vụ chuyên nghiệp của AWS đã tạo ra một thứ gọi là **AWS Cloud Adoption Framework** (Khung áp dụng đám mây AWS) có thể giúp bạn quản lý quá trình này thông qua hướng dẫn. Khung áp dụng đám mây tồn tại để cung cấp lời khuyên cho công ty của bạn có thể kích hoạt di chuyển nhanh chóng và suôn sẻ sang AWS.

## Six core perspectives of the Cloud Adoption Framework

Ở mức độ cao nhất, [\*\*Khung áp dụng đám mây AWS \(AWS CAF\)\*\*](#) tổ chức hướng dẫn thành sáu lĩnh vực trọng tâm, được gọi là **Perspectives (Quan điểm)**. Mỗi quan điểm giải quyết các trách nhiệm riêng biệt. Quá trình lập kế hoạch giúp những người phù hợp trong toàn tổ chức chuẩn bị cho những thay đổi sắp tới.

Nói chung, các Quan điểm **Business**, **People** và **Governance** tập trung vào khả năng kinh doanh, trong khi các Quan điểm **Platform**, **Security** và **Operations** tập trung vào khả năng kỹ thuật.

### Business Perspective

Quan điểm kinh doanh đảm bảo rằng CNTT phù hợp với nhu cầu kinh doanh và đầu tư vào CNTT liên kết với các kết quả kinh doanh quan trọng.

Sử dụng Quan điểm kinh doanh để tạo ra một trường hợp kinh doanh mạnh mẽ cho việc áp dụng đám mây và ưu tiên các sáng kiến áp dụng đám mây. Đảm bảo rằng các chiến lược và mục tiêu kinh doanh của bạn phù hợp với các chiến lược và mục tiêu CNTT của bạn.

Các vai trò phổ biến trong Quan điểm kinh doanh bao gồm:

- Người quản lý doanh nghiệp
- Người quản lý tài chính
- Chủ sở hữu ngân sách
- Các bên liên quan chiến lược

### People Perspective

Quan điểm Con người hỗ trợ phát triển chiến lược quản lý thay đổi trên toàn tổ chức để áp dụng đám mây thành công.

Sử dụng Quan điểm Con người để đánh giá cơ cấu và vai trò của tổ chức, các yêu cầu về quy trình và kỹ năng mới cũng như xác định các khoảng trống. Điều này giúp ưu tiên

đào tạo, nhân sự và thay đổi tổ chức.

Các vai trò phổ biến trong Quan điểm Con người bao gồm:

- Nguồn nhân lực
- nhân sự
- Người quản lý con người

### **Governance Perspective**

Quan **điểm Quản trị** tập trung vào các kỹ năng và quy trình để điều chỉnh chiến lược CNTT với chiến lược kinh doanh. Điều này đảm bảo rằng bạn tối đa hóa giá trị kinh doanh và giảm thiểu rủi ro.

Sử dụng Quan điểm Quản trị để hiểu cách cập nhật các kỹ năng và quy trình cần thiết của nhân viên nhằm đảm bảo quản trị doanh nghiệp trên đám mây. Quản lý và đo lường các khoản đầu tư vào đám mây để đánh giá kết quả kinh doanh.

Các vai trò phổ biến trong Quan điểm Quản trị bao gồm:

- Giám đốc thông tin (CIO)
- Người quản lý chương trình
- Kiến trúc sư doanh nghiệp
- Nhà phân tích kinh doanh
- Người quản lý danh mục đầu tư

### **Platform Perspective**

Phối **cảnh nền tảng** bao gồm các nguyên tắc và mô hình để triển khai các giải pháp mới trên đám mây và di chuyển khối lượng công việc tại chỗ sang đám mây.

Sử dụng nhiều mô hình kiến trúc khác nhau để hiểu và truyền đạt cấu trúc của hệ thống CNTT cũng như các mối quan hệ của chúng. Mô tả chi tiết kiến trúc của môi trường trạng thái mục tiêu.

Các vai trò phổ biến trong Phối cảnh nền tảng bao gồm:

- Giám đốc Công nghệ (CTO)
- Người quản lý CNTT
- Kiến trúc sư giải pháp

### **Security Perspective**

Phối **cảnh bảo mật** đảm bảo rằng tổ chức đáp ứng các mục tiêu bảo mật về khả năng hiển thị, khả năng kiểm tra, kiểm soát và tính linh hoạt.

Sử dụng AWS CAF để cấu trúc việc lựa chọn và triển khai các biện pháp kiểm soát bảo mật đáp ứng nhu cầu của tổ chức.

Các vai trò phổ biến trong Quan điểm bảo mật bao gồm:

- Giám đốc An ninh Thông tin (CISO)
- Người quản lý an ninh CNTT
- Các nhà phân tích bảo mật CNTT

## Operations Perspective

Phối **cảnh hoạt động** giúp bạn kích hoạt, chạy, sử dụng, vận hành và khôi phục khối lượng công việc CNTT ở mức đã thỏa thuận với các bên liên quan trong doanh nghiệp của bạn.

Xác định cách tiến hành hoạt động kinh doanh hàng ngày, hàng quý và hàng năm. Đồng hành và hỗ trợ các hoạt động của doanh nghiệp. AWS CAF giúp các bên liên quan này xác định quy trình vận hành hiện tại và xác định những thay đổi trong quy trình cũng như đào tạo cần thiết để triển khai áp dụng đám mây thành công.

Các vai trò phổ biến trong Phối cảnh hoạt động bao gồm:

- Người quản lý hoạt động CNTT
- Người quản lý hỗ trợ CNTT

# Migration Strategies

## 6 Strategies for Migration

Khi di chuyển ứng dụng sang đám mây, sáu trong số những vấn đề phổ biến nhất chiến lược di cư mà bạn có thể thực hiện là:

- Rehosting
- Replatforming
- Refactoring/re-architecting
- Repurchasing
- Retaining
- Retiring

### Rehosting

**Việc lưu trữ lại** còn được gọi là "nâng lên và thay đổi" liên quan đến việc di chuyển các ứng dụng mà không thay đổi.

Trong trường hợp di chuyển kế thừa quy mô lớn, trong đó công ty đang tìm cách triển khai quá trình di chuyển và mở rộng quy mô một cách nhanh chóng để đáp ứng trường

hợp kinh doanh, phần lớn các ứng dụng đều được lưu trữ lại.

### **Replatforming**

**Tái lập nền tảng**, còn được gọi là “nâng cấp, sửa đổi và thay đổi”, liên quan đến việc thực hiện một số tối ưu hóa đám mây để nhận ra lợi ích hữu hình. Được đạt được sự tối ưu hóa mà không cần thay đổi kiến trúc cốt lõi của ứng dụng.

### **Refactoring/re-architecting**

**Tái cấu trúc** (còn được gọi là **tái cấu trúc**) liên quan đến việc hình dung lại cách một ứng dụng được kiến trúc và phát triển bằng cách sử dụng các tính năng gốc của đám mây. Tái cấu trúc được thúc đẩy bởi nhu cầu kinh doanh mạnh mẽ để thêm các tính năng, quy mô hoặc hiệu suất mà khó có thể đạt được trong môi trường hiện tại của ứng dụng.

### **Repurchasing**

**Việc mua lại** liên quan đến việc chuyển từ giấy phép truyền thống sang mô hình phần mềm dưới dạng dịch vụ.

Ví dụ: một doanh nghiệp có thể chọn thực hiện chiến lược mua lại bằng cách di chuyển từ hệ thống quản lý quan hệ khách hàng (CRM) sang [Salesforce.com](https://www.salesforce.com).

### **Retaining**

**Việc giữ lại** bao gồm việc giữ các ứng dụng quan trọng đối với doanh nghiệp trong môi trường nguồn. Điều này có thể bao gồm các ứng dụng yêu cầu tái cấu trúc lớn trước khi chúng có thể được di chuyển hoặc công việc có thể bị trì hoãn cho đến thời gian sau đó.

### **Retiring**

**Gỡ bỏ** là quá trình loại bỏ các ứng dụng không còn cần thiết nữa.

## **AWS Snow Family**

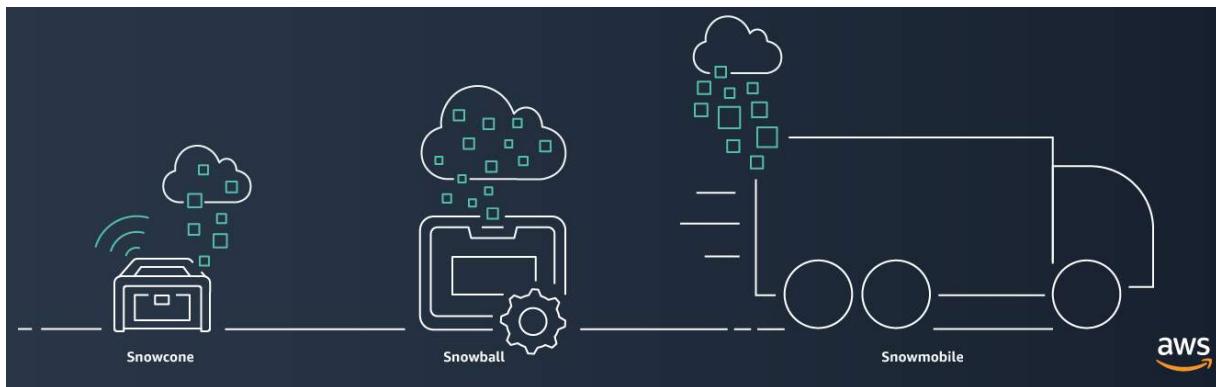
Một số khách hàng của chúng tôi cần đưa dữ liệu lên AWS và hầu hết họ đều muốn làm điều đó một cách hiệu quả và kịp thời. Con đường thông thường chỉ đơn giản là sao chép dữ liệu cần thiết qua internet, hoặc tốt hơn nữa nếu họ có đường kết nối trực tiếp. Tuy nhiên, với những hạn chế về băng thông nói chung, việc này có thể mất nhiều ngày, hàng tuần, thậm chí hàng tháng. Ví dụ: một gigabit chuyên dụng về mặt lý thuyết kết nối mạng

mỗi giây di chuyển một petabyte dữ liệu vào khoảng 100 ngày và trong thế giới thực, có thể lâu hơn và tốn chi phí cao hơn với phản hồi của khách hàng này. Do đó, để giải quyết khoảng cách này, chúng tôi đã giới thiệu Dòng thiết bị **AWS Snow**.

## AWS Snow Family Members

Các **Gia đình tuyết AWS** là tập hợp các thiết bị vật lý giúp vận chuyển vật lý lên tới hàng exabyte dữ liệu vào và ra khỏi AWS.

AWS Snow Family bao gồm **AWS Snowcone**, **AWS Snowball** và **AWS Snowmobile**.



Các thiết bị này cung cấp các điểm công suất khác nhau và hầu hết đều có khả năng tính toán tích hợp. AWS sở hữu và quản lý các thiết bị Snow Family và tích hợp với khả năng tính toán, giám sát, quản lý lưu trữ và bảo mật AWS.

## AWS Snowcone

**AWS Snowcone** là một thiết bị truyền dữ liệu và tính toán biên nhỏ, chắc chắn và an toàn.

Nó có 2 CPU, bộ nhớ 4 GB và dung lượng lưu trữ có thể sử dụng 8 TB.

## AWS Snowball

**Quả cầu tuyết AWS** cung cấp hai loại thiết bị:

- **Snowball Edge Storage Optimized** rất phù hợp cho việc di chuyển dữ liệu quy mô lớn và quy trình truyền định kỳ, bên cạnh điện toán cục bộ có nhu cầu dung lượng cao hơn. Snowball Edge Storage Optimized cung cấp 80 TB dung lượng ổ cứng HDD cho ổ đĩa khối và bộ lưu trữ đối tượng tương thích với Amazon S3, cùng 1 TB SSD SATA cho ổ đĩa khối.
- **Snowball Edge Compute Optimized** cung cấp tài nguyên điện toán mạnh mẽ cho các trường hợp sử dụng như học máy, phân tích video chuyển động đầy đủ, phân tích và ngăn xếp điện toán cục bộ.

## AWS Snowmobile

[Xe trượt tuyết AWS](#) là dịch vụ truyền dữ liệu quy mô exabyte được sử dụng để di chuyển lượng lớn dữ liệu sang AWS.

Bạn có thể truyền tối đa 100 petabyte dữ liệu trên mỗi Snowmobile, một container vận chuyển chắc chắn dài 45 feet, được kéo bởi một chiếc xe tải sơ mi rơ moóc.

## Innovate with AWS

Khi xem xét cách sử dụng dịch vụ AWS, điều quan trọng là phải tập trung vào kết quả mong muốn. Bạn được trang bị phù hợp để thúc đẩy đổi mới trên đám mây nếu bạn có thể trình bày rõ ràng các điều kiện sau:

- Tình trạng hiện tại
- Trạng thái mong muốn
- Những vấn đề bạn đang cố gắng giải quyết

Hãy xem xét một số đường dẫn bạn có thể khám phá trong tương lai khi tiếp tục hành trình trên nền tảng đám mây của mình.

## Serverless Applications

Với AWS, **serverless** nghĩa là các ứng dụng không yêu cầu bạn cung cấp, bảo trì hoặc quản trị máy chủ. Bạn không cần phải lo lắng về khả năng chịu lỗi hoặc tính khả dụng. AWS xử lý những khả năng này cho bạn.

AWS Lambda là một ví dụ về dịch vụ mà bạn có thể sử dụng để chạy các ứng dụng serverless. Nếu thiết kế kiến trúc để kích hoạt các hàm Lambda chạy mã, bạn có thể bỏ qua nhu cầu quản lý nhóm máy chủ.

Xây dựng kiến trúc của bạn bằng các ứng dụng serverless cho phép nhà phát triển của bạn tập trung vào sản phẩm cốt lõi của họ thay vì quản lý và vận hành máy chủ.

## Artificial Intelligence

AWS cung cấp nhiều dịch vụ được hỗ trợ bởi **trí tuệ nhân tạo (AI)**.

Ví dụ: bạn có thể thực hiện các tác vụ sau:

- Chuyển lời nói thành văn bản bằng Amazon Transcribe.
- Khám phá các mẫu trong văn bản với Amazon Comprehend.
- Xác định các hoạt động trực tuyến có khả năng lừa đảo bằng Amazon Fraud Detector.

- Xây dựng chatbot thoại và văn bản với Amazon Lex.

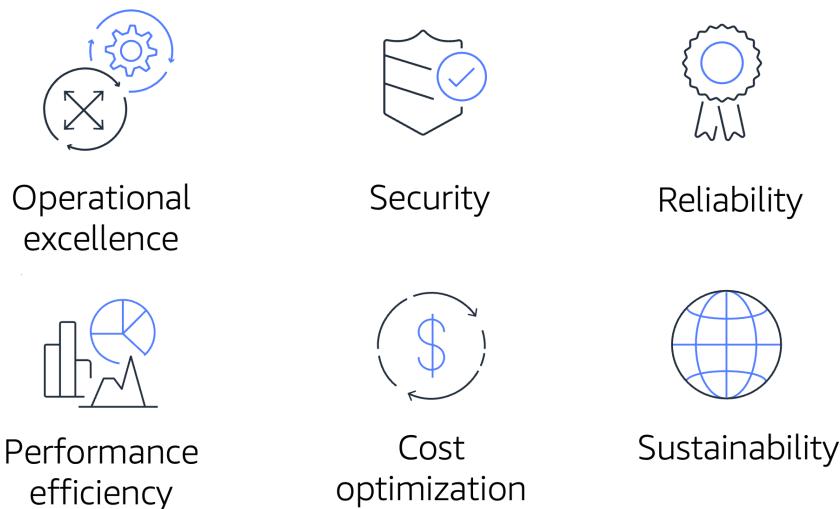
## Machine Learning

**Quá trình phát triển máy học (ML)** truyền thống rất phức tạp, tốn kém, tốn thời gian và dễ xảy ra lỗi. AWS cung cấp Amazon SageMaker để loại bỏ công việc khó khăn khỏi quy trình và hỗ trợ bạn xây dựng, đào tạo và triển khai các mô hình ML một cách nhanh chóng.

Bạn có thể sử dụng ML để phân tích dữ liệu, giải quyết các vấn đề phức tạp và dự đoán kết quả trước khi chúng xảy ra.

## The AWS Well-Architected Framework

Các **Khung kiến trúc tối ưu AWS** giúp bạn hiểu cách thiết kế và vận hành các hệ thống đáng tin cậy, an toàn, hiệu quả và tiết kiệm chi phí trên Đám mây AWS. Nó cung cấp một cách để bạn đo lường kiến trúc của mình một cách nhất quán dựa trên các nguyên tắc thiết kế và thực tiễn tốt nhất, đồng thời xác định các khu vực cần cải thiện.



Khung kiến trúc tốt dựa trên sáu trụ cột:

- Operational excellence
- Security
- Reliability
- Performance efficiency
- Cost optimization
- Sustainability

## **Operational Excellence**

**Hoạt động xuất sắc** là khả năng vận hành và giám sát các hệ thống để mang lại giá trị kinh doanh và liên tục cải tiến các quy trình và thủ tục hỗ trợ.

Nguyên tắc thiết kế để vận hành xuất sắc trên đám mây bao gồm thực hiện các hoạt động dưới dạng mã, chú thích tài liệu, dự đoán lỗi và thường xuyên thực hiện các thay đổi nhỏ, có thể đảo ngược.

## **Security**

Trụ cột **Bảo mật** là khả năng bảo vệ thông tin, hệ thống và tài sản đồng thời mang lại giá trị kinh doanh thông qua các chiến lược đánh giá và giảm thiểu rủi ro.

Khi xem xét tính bảo mật cho kiến trúc của bạn, hãy áp dụng các phương pháp hay nhất sau:

- Tự động hóa các biện pháp bảo mật tốt nhất khi có thể.
- Áp dụng bảo mật ở tất cả các lớp.
- Bảo vệ dữ liệu trong quá trình vận chuyển và ở trạng thái nghỉ ngơi.

## **Reliability**

**Độ tin cậy** là khả năng của một hệ thống thực hiện những việc sau:

- Phục hồi sau sự gián đoạn cơ sở hạ tầng hoặc dịch vụ
- Tự động thu thập tài nguyên máy tính để đáp ứng nhu cầu
- Giảm thiểu sự gián đoạn như cấu hình sai hoặc sự cố mạng tạm thời

Độ tin cậy bao gồm thử nghiệm các quy trình khôi phục, mở rộng quy mô theo chiều ngang để tăng tính khả dụng của hệ thống tổng hợp và tự động khôi phục sau lỗi.

## **Performance Efficiency**

**Hiệu suất hoạt động** là khả năng sử dụng tài nguyên máy tính một cách hiệu quả để đáp ứng các yêu cầu hệ thống và duy trì hiệu suất đó khi nhu cầu thay đổi và công nghệ phát triển.

Đánh giá hiệu quả hoạt động của kiến trúc của bạn bao gồm việc thử nghiệm thường xuyên hơn, sử dụng kiến trúc không có máy chủ và thiết kế hệ thống để có thể vươn ra toàn cầu trong vài phút.

## **Cost Optimization**

**Tối ưu hóa chi phí** là khả năng vận hành các hệ thống để mang lại giá trị kinh doanh ở mức giá thấp nhất.

Tối ưu hóa chi phí bao gồm việc áp dụng mô hình tiêu dùng, phân tích và phân bổ chi tiêu cũng như sử dụng các dịch vụ được quản lý để giảm chi phí sở hữu.

## **Sustainability**

Vào tháng 12 năm 2021, AWS đã giới thiệu trụ cột về tính bền vững như một phần của Khung kiến trúc tối ưu AWS.

**Tính bền vững** là khả năng cải thiện liên tục các tác động đến tính bền vững bằng cách giảm mức tiêu thụ năng lượng và tăng hiệu quả trên tất cả các thành phần của khối lượng công việc bằng cách tối đa hóa lợi ích từ các nguồn lực được cung cấp và giảm thiểu tổng nguồn lực cần thiết.

Để tạo điều kiện thuận lợi cho thiết kế tốt cho tính bền vững:

- Hiểu tác động của bạn
- Thiết lập mục tiêu bền vững
- Tối đa hóa việc sử dụng
- Dự đoán và áp dụng các dịch vụ phần cứng và phần mềm mới, hiệu quả hơn
- Sử dụng các dịch vụ được quản lý
- Giảm tác động xuôi dòng của khối lượng công việc trên đám mây của bạn

## **Benefits of the AWS Cloud**

Hoạt động trên Đám mây AWS mang lại nhiều lợi ích so với tính toán trong môi trường tại chỗ hoặc kết hợp.

Trong phần này, bạn sẽ tìm hiểu về sáu ưu điểm của điện toán đám mây:

- Trade upfront expense for variable expense.
- Benefit from massive economies of scale.
- Stop guessing capacity.
- Increase speed and agility.
- Stop spending money running and maintaining data centers.
- Go global in minutes.

### **Trao đổi chi phí trả trước cho chi phí biến đổi.**

Chi phí trả trước bao gồm trung tâm dữ liệu, máy chủ vật lý và các tài nguyên khác mà bạn cần đầu tư trước khi sử dụng tài nguyên máy tính.

Thay vì đầu tư mạnh vào trung tâm dữ liệu và máy chủ trước khi biết bạn sẽ sử dụng chúng như thế nào, bạn chỉ có thể trả tiền khi sử dụng tài nguyên máy tính.

### **Hưởng lợi từ quy mô kinh tế lớn.**

Bằng cách sử dụng điện toán đám mây, bạn có thể đạt được chi phí biến đổi thấp hơn mức bạn có thể tự mình nhận được.

Do mức sử dụng của hàng trăm nghìn khách hàng được tổng hợp trên đám mây nên các nhà cung cấp như AWS có thể đạt được hiệu quả kinh tế nhờ quy mô cao hơn. Tính kinh tế nhờ quy mô dẫn đến mức giá trả theo mức sử dụng thấp hơn.

### **Đừng đoán năng lực nữa.**

Với điện toán đám mây, bạn không cần phải dự đoán mình sẽ cần bao nhiêu năng lực cơ sở hạ tầng trước khi triển khai một ứng dụng.

Ví dụ: bạn có thể khởi chạy các phiên bản Amazon Elastic Computing Cloud (Amazon EC2) khi cần và chỉ phải trả phí cho thời gian tính toán mà bạn sử dụng. Thay vì trả tiền cho những tài nguyên không được sử dụng hoặc xử lý với dung lượng hạn chế, bạn chỉ có thể truy cập vào dung lượng bạn cần và tăng hoặc giảm quy mô để đáp ứng nhu cầu.

### **Tăng tốc độ và sự nhanh nhẹn.**

Tính linh hoạt của điện toán đám mây giúp bạn phát triển và triển khai ứng dụng dễ dàng hơn.

Tính linh hoạt này cũng giúp nhóm phát triển của bạn có nhiều thời gian hơn để thử nghiệm và đổi mới.

### **Ngừng chi tiền để vận hành và bảo trì trung tâm dữ liệu.**

Điện toán đám mây trong trung tâm dữ liệu thường đòi hỏi bạn phải tốn nhiều tiền và thời gian hơn để quản lý cơ sở hạ tầng và máy chủ.

Lợi ích của điện toán đám mây là khả năng tập trung ít hơn vào các nhiệm vụ này và tập trung nhiều hơn vào ứng dụng và khách hàng của bạn.

### **Đi toàn cầu trong vài phút.**

Dấu chân toàn cầu của Đám mây AWS cho phép bạn nhanh chóng triển khai ứng dụng cho khách hàng trên toàn thế giới, đồng thời mang lại cho họ độ trễ thấp.