

TRƯỜNG ĐẠI HỌC PHENIKAA



PHENIKAA
UNIVERSITY

BÁO CÁO TỔNG QUAN
TRIỂN KHAI VÀ QUẢN LÝ DỊCH VỤ
TRÊN EC2

21010625	Nguyễn Đại Phát	21010625@st.phenikaa-uni.edu.vn
21012073	Nguyễn Hải Long	21012073@st.phenikaa-uni.edu.vn
21013235	Nguyễn Văn Long	21013235@st.phenikaa-uni.edu.vn

Giảng viên hướng dẫn: ThS. Nguyễn Thành Trung
Khoa: Công nghệ thông tin

HÀ NỘI, 05/2023

Lời cam kết

Họ và tên nhóm sinh viên:

- Nguyễn Đại Phát
- Nguyễn Văn Long
- Nguyễn Hải Long

Điện thoại liên lạc: Email:

Lớp: Hệ đào tạo:

Tôi/Chúng tôi cam kết Bài tập lớn (BTL) là công trình nghiên cứu của bản thân/nhóm tôi. Các kết quả nêu trong BTL là trung thực, là thành quả của riêng tôi, không sao chép theo bất kỳ công trình nào khác. Tất cả những tham khảo trong BTL – bao gồm hình ảnh, bảng biểu, số liệu, và các câu từ trích dẫn – đều được ghi rõ ràng và đầy đủ nguồn gốc trong danh mục tài liệu tham khảo. Tôi/chúng tôi xin hoàn toàn chịu trách nhiệm với dù chỉ một sao chép vi phạm quy chế của nhà trường.

Hà Nội, ngày tháng năm

Tác giả/nhóm tác giả BTL

Họ và tên sinh viên

Tóm tắt

(i) Giới thiệu vấn đề: hiện nay các doanh nghiệp và người dùng đang phải đối mặt với thách thức lớn trong việc triển khai và quản lý hệ thống phần mềm đó chính là tốc độ phát triển và sự thay đổi liên tục của công nghệ đòi hỏi họ phải sử dụng các công nghệ mới nhất và triển khai nhanh chóng để cạnh tranh và đáp ứng nhu cầu của khách hàng. Có nhiều nghiên cứu và giải pháp cho bài toán này như sử dụng điện toán đám mây (Cloud Computing), ứng dụng trí tuệ nhân tạo (AI) và học máy (Machine Learning), ứng dụng Blockchain hay phân tích dữ liệu (Data Analytics)... (ii) Nhóm em đã lựa chọn hướng tiếp cận là thiết kế một môi trường đám mây VPC đơn giản nhưng đủ để triển khai và quản lý EC2 và RDS. Điều này cho phép người dùng dễ dàng quản lý các tài nguyên mạng, cơ sở dữ liệu và máy ảo trên đám mây. (iii) Đóng góp chính của BTL là tìm hiểu và áp dụng thành công các khái niệm về điện toán đám mây để triển khai và quản lý dịch vụ EC2 và RDS. Nhóm cũng đã rút ra được nhiều bài học kinh nghiệm như: quản lý tài nguyên đám mây một cách hiệu quả, tạo VPC và subnet một cách hợp lý và triển khai cơ sở dữ liệu RDS với tính sẵn sàng và độ tin cậy cao. Kết quả cuối cùng của BTL là nhóm đã thành công trong việc triển khai và quản lý dịch vụ EC2 kết hợp với RDS trên đám mây AWS. Cả nhóm cũng đã hiểu rõ và có thể áp dụng kiến thức này để triển khai các dịch vụ trên nền tảng đám mây một cách hiệu quả hơn.

Tóm tắt các đóng góp chính của từng thành viên

Họ tên	Các công việc/đóng góp chính
Nguyễn Văn Long	Làm chương 2 bài tập lớn
Nguyễn Hải Long	Làm chương 2 bài tập lớn
Nguyễn Đại Phát	Làm phần còn lại của bài tập lớn, làm slide, thuyết trình, demo sản phẩm

Mục lục

Lời cam kết	ii
Tóm tắt.....	iii
Mục lục.....	iv
Danh mục các từ viết tắt.....	vi
Danh mục thuật ngữ.....	vii
Chương 1 Giới thiệu đề tài.....	1
1.1 Đặt vấn đề	1
1.2 Mục tiêu và phạm vi đề tài.....	1
1.3 Định hướng giải pháp	3
1.4 Bố cục bài tập lớn	4
Chương 2 Công nghệ sử dụng.....	5
2.1 Tổng quan về AWS EC2	5
2.1.1 Giới thiệu về AWS EC2?.....	5
2.1.2 EC2 có lợi ích gì ?	5
2.1.3 Các thành phần của EC2	6
2.2 Một số dịch vụ AWS liên quan đến EC2	9
2.2.1 VPC	9
2.2.2 RDS	10
2.2.3 S3	10
Chương 3 Phát triển và triển khai kỹ thuật	12

3.1 Thiết kế tổng quan	12
3.2 Triển khai kỹ thuật.....	13
3.2.1 Công cụ sử dụng	13
3.2.2 Kết quả đạt được.....	13
3.2.3 Kiểm thử	14
3.2.4 Minh hoạ các chức năng chính.....	16
3.3 Triển khai	18
3.3.1 Cấu hình VPC.....	18
3.3.2 Cấu hình RDS.....	20
3.3.3 Cấu hình S3	21
3.3.4 Cấu hình EC2	21
Chương 4 Các giải pháp và đóng góp nổi bật	23
Chương 5 Kết luận và hướng phát triển	25
5.1 Kết luận.....	25
5.2 Hướng phát triển.....	26
Tài liệu tham khảo.....	27

Danh mục các từ viết tắt

AWS	Amazon Web Service Dịch vụ web Amazon
EC2	Elastic Compute Cloud Đám mây điện toán đàn hồi
S3	Simple Storage Service Dịch vụ lưu trữ đơn giản
RDS	Relational Database Service Dịch vụ cơ sở dữ liệu quan hệ
...	...

Danh mục thuật ngữ

Database	Cơ sở dữ liệu
Subnet	Mạng con
Availibity zone	Vùng sẵn sàng
Router	Bộ định tuyến
...	...

Chương 1 Giới thiệu đề tài

1.1 Đặt vấn đề

Thực tế hiện nay, các doanh nghiệp, công ty, cá nhân hay các tổ chức đang phải đối mặt với nhiều thách thức trong việc triển khai và quản lý hệ thống phần mềm. Một trong những thách thức chính đó là tốc độ phát triển và sự thay đổi liên tục của công nghệ. Điều này đòi hỏi họ phải sử dụng các công nghệ mới nhất và triển khai chúng nhanh chóng để cạnh tranh và đáp ứng nhu cầu của khách hàng.

Tuy nhiên, việc triển khai và quản lý các hệ thống phần mềm mới có thể gặp phải nhiều vấn đề như chi phí đầu tư, khó khăn trong việc quản lý, bảo trì và mở rộng và cả độ tin cậy của hệ thống. Việc đầu tư vào phần cứng, thiết bị, phần mềm và nhân sự để triển khai hay mở rộng, nâng cấp hệ thống gây tốn kém và làm tăng chi phí vận hành, rồi việc phải quản lý và bảo trì hệ thống đòi hỏi nhân sự có kỹ năng chuyên môn và kinh nghiệm cao, tuy nhiên việc tìm kiếm và thuê nhân sự đó lại rất khó khăn và tốn kém. Độ tin cậy của hệ thống cũng là một trong những yếu tố quan trọng để đảm bảo doanh nghiệp được hoạt động liên tục. Tuy nhiên, việc đảm bảo độ tin cậy đòi hỏi các kỹ thuật và công nghệ cao, đồng thời cũng gặp phải những rủi ro và thách thức.

Nếu vấn đề trên được giải quyết, doanh nghiệp sẽ được lợi ích rất lớn. Trước tiên, doanh nghiệp sẽ giảm thiểu chi phí vận hành hệ thống bằng cách tối ưu hóa các tài nguyên và nâng cao hiệu suất hoạt động. Đồng thời, hệ thống sẽ có khả năng mở rộng linh hoạt, đáp ứng nhanh chóng với nhu cầu tăng trưởng của doanh nghiệp. Thứ hai, doanh nghiệp sẽ có khả năng quản lý hệ thống dễ dàng hơn, từ đó giảm thiểu thời gian và nhân lực cần thiết để quản lý hệ thống. Hơn nữa, doanh nghiệp còn có thể tập trung vào các hoạt động chính và nâng cao chất lượng dịch vụ, thay vì mất nhiều thời gian và tài nguyên vào việc quản lý hệ thống.

1.2 Mục tiêu và phạm vi đề tài

Hiện nay, có nhiều nghiên cứu và giải pháp cho bài toán của doanh nghiệp trong việc triển khai và quản lý hệ thống phần mềm như sử dụng điện toán đám mây (Cloud Computing), ứng dụng trí tuệ nhân tạo (AI) và học máy (Machine Learning), ứng dụng Blockchain hay phân tích dữ liệu (Data Analytics)...

Điện toán đám mây cung cấp một nền tảng linh hoạt và tiết kiệm chi phí cho doanh nghiệp để triển khai và quản lý hệ thống phần mềm. Thay vì phải đầu tư vào phần cứng và thiết bị, doanh nghiệp có thể sử dụng các dịch vụ đám mây và chỉ thanh toán cho những tài nguyên thực sự sử dụng. Ngoài ra, điện toán đám mây còn cung cấp khả năng mở rộng linh hoạt và quản lý dễ dàng. AI và Machine Learning thì có thể giúp cho doanh nghiệp tăng cường khả năng quản lý và dự báo hệ thống phần mềm. Các giải pháp này có thể sử dụng để phát hiện và xử lý các sự cố trong hệ thống, cải thiện hiệu suất hoạt động, và nâng cao trải nghiệm của khách hàng. Blockchain vẫn còn là một công nghệ khá mới mẻ đối với nhiều người dùng, nó có thể được sử dụng để xây dựng các hệ thống phần mềm an toàn và đáng tin cậy. Với Blockchain, các thông tin và giao dịch được lưu trữ và xác thực bởi một mạng lưới các nút, giúp ngăn chặn sự can thiệp hoặc giả mạo dữ liệu. Các doanh nghiệp có thể sử dụng Blockchain để tăng cường độ tin cậy của hệ thống và bảo vệ dữ liệu của khách hàng. Còn phân tích dữ liệu giúp doanh nghiệp hiểu rõ hơn về khách hàng và nhu cầu của họ, từ đó cung cấp các dịch vụ và sản phẩm phù hợp hơn. Ngoài ra, phân tích dữ liệu cũng có thể giúp doanh nghiệp đưa ra các quyết định thông minh về chiến lược phát triển hệ thống phần mềm.

Việc triển khai và quản lý các giải pháp trên có thể đối mặt với nhiều hạn chế bởi các giải pháp này đòi hỏi kỹ năng và kiến thức chuyên môn cao để triển khai và quản lý. Do đó, doanh nghiệp có thể sẽ gặp khó khăn khi tuyển dụng và đào tạo nhân viên mới để đáp ứng nhu cầu này. Việc triển khai các giải pháp công nghệ mới có thể làm thay đổi hoặc ảnh hưởng đến quy trình làm việc hiện tại của doanh nghiệp. Điều này đòi hỏi doanh nghiệp phải thận trọng và chuẩn bị cho những thay đổi này, bao gồm cả việc đào tạo nhân viên và thay đổi quy trình làm việc.

Tuy nhiên, nếu triển khai và quản lý đúng cách, các giải pháp công nghệ có thể giúp doanh nghiệp tăng cường năng suất, cải thiện hiệu quả làm việc và tăng tính cạnh tranh trên thị trường. Do đó, việc nghiên cứu và áp dụng các giải pháp công nghệ mới là cần thiết đối với các doanh nghiệp hiện nay. Trên cơ sở đó, nhóm em đã hướng tới giải pháp điện toán đám mây.

Điện toán đám mây có nhiều ưu điểm khi so sánh với các giải pháp công nghệ khác như AI, Machine Learning, Blockchain hay Data Analytics. Đầu tiên, điện toán đám mây thường cung cấp khả năng linh hoạt và mở rộng tài nguyên nhanh chóng, từ đó giúp doanh nghiệp dễ dàng mở rộng quy mô và tăng cường hiệu suất của hệ thống mà không cần đầu tư nhiều về cơ sở hạ tầng. Thứ hai, điện toán đám mây cũng có thể tích hợp với các giải pháp công nghệ khác như AI, Machine Learning, Blockchain hay Data Analytics để tạo ra những giải pháp toàn diện và hiệu quả hơn. Và cuối cùng, điện toán đám mây cũng cung cấp nhiều tính năng bảo mật để đảm bảo an toàn thông tin và dữ liệu của doanh nghiệp, từ đó giúp giảm thiểu rủi ro bị tấn công mạng hay mất mát dữ liệu quan trọng. Vì vậy, nếu doanh nghiệp

đang tìm kiếm giải pháp công nghệ để tăng cường hiệu quả kinh doanh và giảm thiểu chi phí đầu tư, giải pháp điện toán đám mây là một lựa chọn khả thi và hiệu quả.

1.3 Định hướng giải pháp

Trên thực tế, có rất nhiều lựa chọn cho doanh nghiệp khi muốn triển khai hệ thống điện toán đám mây, bao gồm các dịch vụ như FPT Smart Cloud, Microsoft Azure, Google Cloud Platform... Tuy nhiên, có nhiều lý do mà các doanh nghiệp nên lựa chọn AWS EC2 là giải pháp cho hệ thống điện toán đám mây của mình. Đầu tiên, AWS EC2 là một trong những dịch vụ điện toán đám mây phổ biến nhất trên thị trường, với một loạt các tính năng và lựa chọn đa dạng để phù hợp với các nhu cầu khác nhau của doanh nghiệp. Nó cung cấp một hệ thống mạnh mẽ, linh hoạt và dễ sử dụng để triển khai và quản lý các máy chủ ảo trên đám mây. Thứ hai, AWS EC2 cung cấp nhiều lựa chọn khác nhau cho các loại máy chủ, bao gồm cả các máy chủ khắc phục sự cố và máy chủ dành riêng cho việc chạy các ứng dụng đòi hỏi tính toán cao. Nó cũng cung cấp các tính năng như auto-scaling, load balancing và khả năng tùy chỉnh để đáp ứng các nhu cầu cụ thể của doanh nghiệp. Thứ ba, AWS EC2 được xây dựng trên cơ sở hạ tầng mạnh mẽ của AWS, với các tính năng bảo mật và quản lý tài nguyên tốt nhất trong ngành. Nó cung cấp các tính năng bảo mật như bảo vệ chống lại các cuộc tấn công mạng, kiểm soát truy cập và bảo mật tại chỗ để đảm bảo an toàn cho dữ liệu và ứng dụng của doanh nghiệp. Và cuối cùng, AWS EC2 có một cộng đồng lớn của các nhà phát triển và chuyên gia hỗ trợ trên toàn thế giới. Điều này có nghĩa là các doanh nghiệp sử dụng AWS EC2 có thể dễ dàng tìm được người hỗ trợ khi cần thiết, và có thể tận dụng các tài nguyên miễn phí như các hướng dẫn và tài liệu hỗ trợ từ cộng đồng này. Tóm lại, AWS EC2 là một trong những dịch vụ điện toán đám mây hàng đầu trên thị trường hiện nay, với những ưu điểm vượt trội như đa dạng về tính năng và linh hoạt trong việc triển khai và quản lý hệ thống.

Với những đóng góp từ bài tập lớn này, người đọc sẽ hiểu rõ hơn về lợi ích, thành phần cấu tạo và cách triển khai, quản lý các dịch vụ trên EC2 bao gồm cách tạo và cấu hình các máy ảo, cài đặt và cấu hình các ứng dụng trên, quản lý an ninh và bảo mật, giám sát hiệu suất, và nhiều công cụ hỗ trợ khác. Người đọc sẽ hiểu hơn về mô hình đám mây riêng ảo bao gồm AZ zone, subnet, router... , hiểu hơn dịch vụ RDS và cách kết nối cơ sở dữ liệu thông qua nó. Không những thế, người đọc còn được biết thêm nhiều phương thức bảo mật trong quá trình cấu hình và triển khai.

Sau bài tập lớn, nhóm em đã có thể hiểu rõ hơn về cách thức hoạt động của AWS và cách triển khai và quản lý các dịch vụ trên EC2, VPC và RDS, có cơ hội tiếp xúc và thực hành với những công nghệ mà trước đây chưa từng làm. Nhờ đó, nhóm em cũng được nâng cao hơn trong việc tìm hiểu và giải quyết vấn đề bằng cách phát triển những kỹ năng nghiên cứu, tìm kiếm thông tin, giải quyết được các vấn đề liên quan đến triển khai và quản lý các dịch

vụ EC2. Nhóm cũng được nâng cao kỹ năng viết tài liệu, mô tả các vấn đề gặp đã gặp phải và cách giải quyết chúng.

1.4 Bố cục bài tập lớn

Phần còn lại của báo cáo Bài tập lớn này được tổ chức như sau.

Error! Reference source not found. giới thiệu về tất cả công nghệ được sử dụng khi triển khai các dịch vụ EC2 bao gồm EC2, VPC, RDS và S3. Chương 3 trình bày về việc phát triển và triển khai kỹ thuật bao gồm thiết kế tổng quan, triển khai kỹ thuật và cuối cùng là triển khai. Chương 4 là các giải pháp và đóng góp nổi bật mà nhóm đã tìm hiểu và nghiên cứu. Cuối cùng là phần 5 bao gồm 2 mục kết luận và hướng phát triển.

Chương 2 Công nghệ sử dụng

Tổng quan: Trong chương 1, chúng ta đã tìm ra giải pháp sử dụng AWS EC2 để giải quyết vấn đề của các doanh nghiệp và người dùng khi triển khai và quản lý hệ thống phần mềm. Sang chương 2, chúng ta sẽ cùng nhau tìm hiểu sâu hơn về định nghĩa, lợi ích, thành phần của EC2 và cùng tìm hiểu một số công nghệ không thể thiếu khi triển khai dịch vụ trên EC2, đó là VPC, RDS, S3.

2.1 Tổng quan về AWS EC2

2.1.1 Giới thiệu về AWS EC2?

AWS (Amazon Web Services) là một nền tảng điện toán đám mây (cloud computing) được cung cấp bởi Amazon. AWS cung cấp hàng trăm dịch vụ khác nhau với mô hình thanh toán linh hoạt như lưu trữ, tính toán, cơ sở dữ liệu, truyền thông, máy học, trí tuệ nhân tạo, an ninh, quản lý tài nguyên ... AWS cung cấp các công cụ và tài nguyên cho phép người dùng triển khai và quản lý các ứng dụng trên đám mây một cách hiệu quả và tiết kiệm chi phí.

EC2 (Elastic Compute Cloud) thuộc dịch vụ tính toán đám mây của AWS. EC2 cung cấp một môi trường tính toán độc lập và mở rộng linh hoạt, cho phép khách hàng thuê hoặc tạo các máy ảo (instances) trên đám mây của AWS để thực thi các ứng dụng của họ. EC2 giúp người dùng trải nghiệm cảm giác được làm việc tại bất kỳ nơi nào mà không mất nhiều chi phí, đặc biệt là tiền đầu tư ổ cứng vật lý.

2.1.2 EC2 có lợi ích gì ?

EC2 là một trong những dịch vụ điện toán đám mây phổ biến nhất của AWS. Với EC2, người dùng có thể tạo ra các máy ảo tùy chỉnh để phục vụ nhu cầu kinh doanh của mình một cách dễ dàng và linh hoạt. EC2 cung cấp khả năng quản lý các máy ảo dễ dàng, cho phép người dùng điều chỉnh các tài nguyên như CPU, bộ nhớ, lưu trữ, mạng và phần mềm theo nhu cầu thực tế của họ.

Một trong những lợi ích đáng kể của EC2 là tính linh hoạt cao. Người dùng có thể tạo và quản lý các máy ảo một cách nhanh chóng và dễ dàng. Khi nhu cầu sử dụng tăng lên, người dùng có thể mở rộng quy mô của hệ thống EC2 của mình bằng cách tăng số lượng các máy ảo hoặc cấu hình tài nguyên cho các máy ảo đang tồn tại.

Bên cạnh tính linh hoạt, EC2 còn cho phép người dùng tiết kiệm chi phí. Thay vì phải mua sắm phần cứng và quản lý các máy chủ riêng, EC2 cho phép người dùng thuê tài nguyên, lựa chọn hệ điều hành với giá cả hợp lý và chỉ trả tiền cho những tài nguyên thực sự sử dụng. Việc này giúp giảm thiểu chi phí về phần cứng, quản lý hệ thống và giúp người dùng tập trung vào công việc kinh doanh chính của họ.

EC2 cũng cung cấp tính sẵn sàng cao với khả năng mở rộng tự động. Người dùng có thể cấu hình EC2 để tự động phát hiện và tăng cường tài nguyên khi nhu cầu sử dụng tăng cao. Điều này giúp đảm bảo rằng hệ thống của người dùng luôn hoạt động hiệu quả, một cách liên tục và ổn định.

Bên cạnh đó, EC2 cũng cung cấp cho người dùng khả năng quản lý và giám sát máy chủ một cách dễ dàng thông qua các dịch vụ quản lý hệ thống như Amazon CloudWatch và AWS System Manager. Điều này giúp cho người dùng có thể theo dõi hiệu suất của máy chủ, theo dõi sự cố, và thực hiện các tác vụ khác một cách hiệu quả.

Ngoài ra, EC2 cũng được tích hợp các tính năng bảo mật để bảo vệ các tài nguyên của người dùng. Với mạng riêng ảo (VPC), phân quyền người dùng, tường lửa và mã hóa dữ liệu, người dùng có thể an tâm sử dụng EC2 mà không lo lắng về việc bảo vệ các tài nguyên. Tường lửa cho phép người dùng thiết lập các quy tắc truy cập chi tiết cho từng máy chủ EC2, giúp ngăn chặn các mối đe dọa từ bên ngoài. Mã hóa dữ liệu để đảm bảo rằng dữ liệu được lưu trữ trên các máy chủ EC2 được bảo vệ, người dùng có thể mã hóa dữ liệu tại một số mức độ khác nhau, bao gồm mã hóa ở mức đĩa và mã hóa tại cấp độ ứng dụng.

Cuối cùng, EC2 là một dịch vụ rất linh hoạt và có thể tích hợp với nhiều dịch vụ khác trong hệ thống AWS. Người dùng có thể sử dụng EC2 kết hợp với S3 để lưu trữ dữ liệu, kết hợp với Lambda để thực hiện các tác vụ tự động hoặc kết hợp với các dịch vụ khác để đáp ứng các nhu cầu cụ thể của họ.

2.1.3 Các thành phần của EC2

2.1.3.1 Instance

Instances: Là các máy ảo (VM) trên EC2 được tạo ra bởi người dùng và được chạy trên phần cứng của AWS. Các instance có thể chạy các hệ điều hành khác nhau và được tùy chỉnh về cấu hình, bao gồm số lượng CPU, RAM và ổ đĩa.

Instance Types: Là các loại instance có cấu hình khác nhau để đáp ứng nhu cầu khác nhau của người dùng. Các loại instance khác nhau có khả năng xử lý khác nhau, bộ nhớ khác nhau và đáp ứng nhu cầu khác nhau.

Launch Templates: Là mẫu tạo ra các instance với cấu hình cụ thể. Người dùng có thể tạo ra các launch templates để nhanh chóng triển khai các instance mới và giảm thiểu việc lặp lại quá trình tạo.

Spot Requests: Là các yêu cầu của người dùng để sử dụng các instance không sử dụng trong khoảng thời gian cụ thể. Các spot requests cho phép người dùng sử dụng các instance với giá thấp hơn so với giá định mức, tuy nhiên chúng không đảm bảo sẽ luôn có sẵn.

Savings Plans: Là một hình thức thanh toán tiền tố giúp người dùng tiết kiệm chi phí khi sử dụng các instance. Người dùng có thể mua Savings Plans với một số tiền trước, sau đó sử dụng chi phí tiền tố đã mua để trả cho các chi phí định kỳ của các instance.

Reserved Instances: Là các instance được đặt trước và mua với giá giảm giúp người dùng tiết kiệm chi phí so với việc mua các instance on-demand. Tuy nhiên, các reserved instances chỉ có thể sử dụng cho cấu hình cụ thể và trong khoảng thời gian cụ thể.

Dedicated Hosts: Là các máy chủ vật lý được cung cấp cho người dùng để sử dụng riêng tư, chứ không được chia sẻ với người dùng khác. Các Dedicated Hosts được sử dụng để cung cấp tính toàn vẹn về bảo mật và nhiều khả năng tùy chỉnh hơn so với các instance bình thường.

Capacity Reservations: Là khả năng đặt chỗ các instance hoặc Dedicated Hosts để đảm bảo rằng người dùng có sẵn các tài nguyên cần thiết

2.1.3.2 Images

AMIs (Amazon Machine Images): Là một loại định dạng file được sử dụng để tạo ra các instance trên EC2. Một AMI bao gồm một image của một hệ điều hành cụ thể và các ứng dụng được cài đặt trên đó. Người dùng có thể tạo ra AMI của riêng họ hoặc sử dụng AMI có sẵn từ AWS.

AMI Catalog: Là một bộ sưu tập các AMI có sẵn từ AWS Marketplace và các nhà cung cấp khác. AMI Catalog cho phép người dùng dễ dàng tìm kiếm và tải về các AMI có sẵn để triển khai các instance mới trên EC2. Nó cung cấp thông tin về các AMI, bao gồm tên, miêu tả, nhà sản xuất, cấu hình và giá cả.

2.1.3.3 Elastic Block Store

Volumes: Là một phần của EC2, cho phép người dùng tạo và quản lý các phương tiện lưu trữ dữ liệu đính kèm vào các instance. Một volume có thể được gắn kết với một instance và sử dụng như một phương tiện lưu trữ dữ liệu độc lập với instance. Volumes có thể được thay đổi kích thước, đính kèm hoặc gỡ bỏ khỏi các instance.

Snapshots: Là một tính năng cho phép sao lưu và khôi phục dữ liệu của volume. Khi người dùng tạo snapshot của một volume, nó sẽ lưu lại tình trạng hiện tại của volume, bao gồm cả dữ liệu và các thiết lập. Các snapshot có thể được sử dụng để sao lưu và khôi phục các volume và dữ liệu của chúng.

Lifecycle Manager: Là một công cụ quản lý vòng đời cho phép người dùng tự động sao lưu và xóa các snapshot của volume. Người dùng có thể thiết lập các chính sách để quản lý các snapshot, bao gồm tần suất sao lưu, số lượng snapshot được giữ lại và thời gian sống của chúng. Lifecycle Manager giúp người dùng tiết kiệm chi phí và quản lý tài nguyên dữ liệu hiệu quả hơn trên EC2.

2.1.3.4 Network & Security

Security Groups: Là một tính năng cho phép người dùng quản lý các quy tắc bảo mật cho các instance EC2. Mỗi instance EC2 phải được liên kết với một hoặc nhiều Security Groups, và các quy tắc bảo mật có thể được thiết lập để kiểm soát quyền truy cập vào instance từ các nguồn bên ngoài.

Elastic IPs: Là một địa chỉ IP tĩnh được cung cấp bởi AWS cho phép người dùng gắn kết với các instance EC2. Elastic IPs có thể được sử dụng để đảm bảo rằng một instance luôn có cùng một địa chỉ IP tĩnh, cho phép các ứng dụng hoạt động liên tục mà không bị gián đoạn do thay đổi địa chỉ IP.

Placement Groups: Là một tính năng cho phép người dùng tối ưu hóa hiệu suất và khả năng sẵn sàng của các instance EC2. Placement Groups cho phép các instance được đặt trong cùng một vùng vật lý trên cùng một máy chủ hoặc các máy chủ gần nhau nhất, giảm thiểu thời gian truyền tải và tăng tính sẵn sàng của ứng dụng.

Key Pairs: Là cặp khóa bảo mật gồm khóa riêng tư và khóa công khai được sử dụng để truy cập vào các instance EC2. Khóa riêng tư được giữ bởi người dùng và được sử dụng để giải mã các thông tin bảo mật được mã hóa trên instance, trong khi khóa công khai được cung cấp cho các bên thứ ba để mã hóa thông tin gửi đến instance.

Network Interfaces: Là một tính năng cho phép người dùng quản lý kết nối mạng của các instance EC2. Mỗi instance có thể được gắn kết với nhiều network interface, cho phép kết nối đến các mạng khác nhau và quản lý các địa chỉ IP và quy tắc bảo mật khác nhau.

2.1.3.5 Load Balancing

Load Balancers: Là một tính năng cho phép người dùng phân phối tải giữa các instance EC2 để đảm bảo rằng các yêu cầu từ khách hàng được xử lý hiệu quả. Load Balancers có thể

được cấu hình để phân phối tải theo nhiều cách khác nhau, bao gồm phân phối tải đơn giản, phân phối tải theo giá trị cookie, phân phối tải theo địa chỉ IP, v.v.

Target Groups: Là một tính năng cho phép người dùng quản lý các instance EC2 được sử dụng bởi Load Balancers. Mỗi Target Group đại diện cho một nhóm các instance EC2 cùng chạy một ứng dụng web và được quản lý bởi một Load Balancer. Khi một yêu cầu được gửi đến Load Balancer, Load Balancer sẽ xác định Target Group phù hợp và chuyển tiếp yêu cầu đến một trong các instance EC2 trong Target Group. Target Groups cũng cung cấp nhiều tính năng quản lý và theo dõi hiệu suất, bao gồm theo dõi sức khỏe của các instance và cân bằng tải động để đảm bảo rằng các yêu cầu được chuyển tiếp đến các instance có khả năng xử lý tốt nhất.

2.1.3.6 Auto Scaling

Launch Configurations: Là một tính năng cho phép người dùng định cấu hình một môi trường EC2 cụ thể mà các instance EC2 mới sẽ được tạo ra và chạy. Một Launch Configuration bao gồm các thông tin về hệ điều hành, kích thước của instance, volume, v.v. Một khi người dùng đã tạo ra một Launch Configuration, họ có thể sử dụng nó để tạo ra các instance EC2 mới.

Auto Scaling Groups: Là một tính năng cho phép người dùng tự động mở rộng hoặc thu nhỏ số lượng các instance EC2 để đáp ứng với các yêu cầu của ứng dụng web. Auto Scaling Groups sử dụng Launch Configurations để định cấu hình các instance EC2 mới được tạo ra. Người dùng có thể đặt ngưỡng cho số lượng instance EC2 trong một Auto Scaling Group và cấu hình các quy tắc để tự động mở rộng hoặc thu nhỏ Auto Scaling Group dựa trên yêu cầu về tải. Khi tải được đánh giá cao, Auto Scaling Groups sẽ tự động tạo ra thêm các instance EC2 mới từ Launch Configuration và thêm chúng vào mạng của ứng dụng. Khi tải giảm, Auto Scaling Groups sẽ tự động thu hẹp số lượng các instance EC2, giảm chi phí hoạt động.

2.2 Một số dịch vụ AWS liên quan đến EC2

2.2.1 VPC

VPC (Virtual Private Cloud) là một dịch vụ cung cấp mạng ảo bảo mật trên nền tảng của AWS, cho phép người dùng tạo ra các mạng riêng ảo (Virtual Private Network - VPN) mà không cần sử dụng cơ sở hạ tầng vật lý riêng của mình.

Subnet là một phần của mạng VPC, được phân chia bằng cách chia nhỏ địa chỉ IP cho các mạng con. Mỗi subnet được liên kết với một Availability Zone, nơi các instance EC2 và các tài nguyên khác trong VPC được triển khai. Một subnet có thể chứa nhiều instance EC2 và

tài nguyên khác, và các subnet khác nhau trong VPC có thể được cấu hình để giao tiếp với nhau.

Routable (định tuyến) là khả năng của các địa chỉ IP có thể được định tuyến qua các mạng khác nhau. Các địa chỉ IP của các instance EC2 trong VPC là routable và có thể được sử dụng để truy cập vào các tài nguyên khác trong VPC hoặc trên internet thông qua Internet Gateway.

Internet Gateway là một cổng kết nối mạng giữa VPC và Internet. Nó cho phép các instance EC2 trong VPC truy cập internet hoặc được truy cập từ internet thông qua địa chỉ IP public. Các instance EC2 có thể được cấu hình để có địa chỉ IP public hoặc sử dụng NAT Gateway để truy cập internet.

2.2.2 RDS

RDS (Relational Database Service) là một dịch vụ quản lý cơ sở dữ liệu quan hệ trên nền tảng của AWS. Nó cho phép người dùng triển khai, quản lý và mở rộng các cơ sở dữ liệu quan hệ, bao gồm các phiên bản của MySQL, PostgreSQL, Oracle, SQL Server và Amazon Aurora và kết nối với các instance EC2.

Subnet Groups là một tập hợp các subnet trong một VPC được gán cho một instance RDS. Mỗi instance RDS cần được triển khai trong ít nhất một subnet và có thể được triển khai trong nhiều subnet khác nhau. Sử dụng Subnet Groups cho phép người dùng quản lý các subnet được sử dụng để triển khai RDS và đảm bảo sẽ không có thông tin cần thiết bị tiết lộ. Subnet Groups cũng cho phép RDS sử dụng các tính năng của VPC như mạng riêng ảo và các quy tắc bảo mật.

Databases là một tập hợp các dữ liệu được tổ chức theo cấu trúc nhất định và được quản lý bằng phần mềm quản lý cơ sở dữ liệu. Các cơ sở dữ liệu quan hệ thông thường bao gồm các bảng, mỗi bảng chứa các cột với các kiểu dữ liệu khác nhau. RDS cung cấp một số tính năng quản lý cơ sở dữ liệu, bao gồm sao lưu và phục hồi, điều khiển truy cập và quản lý tài khoản người dùng.

2.2.3 S3

S3 (Simple Storage Service) là dịch vụ lưu trữ đối tượng của Amazon Web Services (AWS). Nó cho phép người dùng lưu trữ và truy xuất các đối tượng, chẳng hạn như tệp, ảnh, video và tài liệu, trên nền tảng đám mây của AWS. S3 được thiết kế để cung cấp tính khả dụng cao, độ tin cậy và tính linh hoạt cao cho các ứng dụng web và truyền thông.

Bucket là một thuật ngữ trong S3 để chỉ một thùng chứa đối tượng lưu trữ dữ liệu. Nó được sử dụng để phân tách các đối tượng lưu trữ dữ liệu trong S3 thành các nhóm và quản lý

chúng dễ dàng hơn. Bucket có thể được đặt tên theo yêu cầu của người dùng, tuy nhiên, tên bucket phải là duy nhất trên toàn hệ thống S3. Các bucket trong S3 có thể được tạo, xóa và sửa đổi bởi người dùng và có thể được cấu hình để tự động sao lưu và lưu trữ đối tượng. Trong phần demo, S3 được nhóm sử dụng để lưu trữ source code.

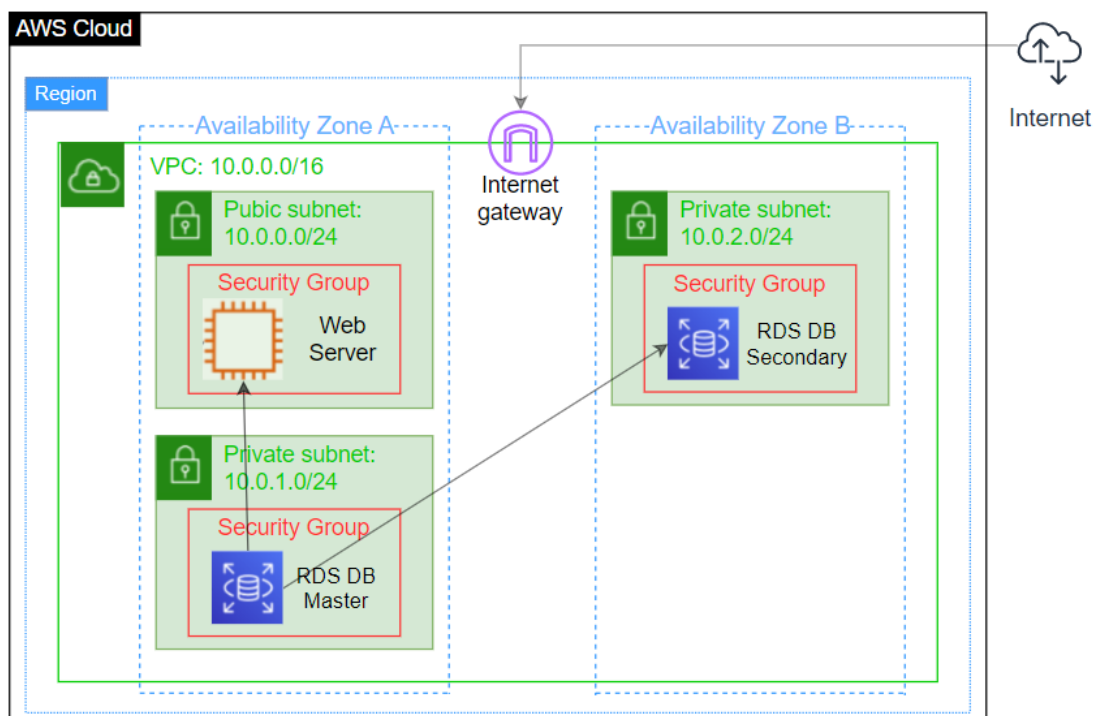
Kết chương: Qua chương này, chúng ta đã cùng nhau tìm hiểu về các công nghệ EC2, VPC, RDS, S3. Mỗi công nghệ đều có những công dụng và điểm mạnh riêng nhưng chúng có thể liên kết với nhau để tạo nên một mô hình triển khai hoàn chỉnh như EC2 và RDS kết nối với nhau và được đặt trên VPC. Từ những nghiên cứu trên, nhóm đã có thể triển khai một phần mềm cơ bản hoàn thiện trên server. Phần này sẽ được trình bày trong chương tiếp theo – Chương 3.

Chương 3 Phát triển và triển khai kỹ thuật

Tổng quan: Trong chương 2, chúng ta đã tìm hiểu về EC2 và một số công nghệ khác đi kèm là VPC, RDS, S3. Sang chương 3, chúng ta sẽ cùng nhau phát triển và triển khai phần mềm lên trên web server với các công nghệ trên.

3.1 Thiết kế tổng quan

Dưới đây là mô hình cơ sở hạ tầng sau khi triển khai. Một VPC 10.0.0.0/16 cấu hình với Availability Zone A và Availability Zone B. Zone A chứa public subnet 10.0.0.0/24 và private subnet 10.0.1.0/24. Zone B chứa subnet private 10.0.3.0/24. Public subnet liên kết public router table và router này kết nối với cổng mạng Internet gateway. Hai subnet private còn lại thì được kết nối với một private router table. EC2 được khởi tạo trong public subnet, Multi-AZ RDS khởi tạo trên subnet private của Zone A. Khi khởi tạo một phiên bản Multi-AZ RDS, Amazon RDS sẽ tự động tạo một phiên bản cơ sở dữ liệu chính trên vùng được chọn đồng thời sao chép và đồng bộ dữ liệu sang một phiên bản dự phòng trong một Zone khác (ở đây là Zone B). Việc này giúp cơ sở dữ liệu được đảm bảo an toàn và bảo mật phòng trường hợp có zone hay cơ sở dữ liệu bị lỗi.



Hình 1 Ví dụ mô hình sau khi triển khai phần mềm

3.2 Triển khai kỹ thuật

3.2.1 Công cụ sử dụng

Bảng 1 Danh sách công cụ sử dụng

Công cụ	Mục đích	Lệnh tải
Trình thông dịch PHP, Apache và mô-đun MySQL	Chạy ứng dụng web PHP trên máy chủ.	<code>sudo apt install php libapache2-mod-php php-mysql</code>
MySQL Server	Quản lý cơ sở dữ liệu MySQL	<code>sudo apt install mysql-server</code>
Công cụ giải nén	Giải nén file code tải về từ S3	<code>sudo apt install unzip</code>

3.2.2 Kết quả đạt được

Việc cấu hình VPC với 2 zone, 2 route table, 1 subnet public, 1 internet gateway và 2 subnet private giúp tăng tính bảo mật cho hệ thống. Trong đó, các EC2 instance sẽ được triển khai trong subnet public, còn RDS instance sẽ được triển khai trong các subnet private. Việc triển khai các EC2 instance trong subnet public cho phép truy cập từ Internet đến các máy chủ, trong khi việc triển khai RDS instance trong subnet private sẽ được bảo vệ bởi tường lửa trong VPC, chỉ cho phép các kết nối được quy định và các máy chủ trong subnet public có thể kết nối tới. Sau khi triển khai một trang web bằng EC2, người dùng có thể truy cập trang web đó thông qua địa chỉ IP Public của EC2. Người dùng trên toàn thế giới có thể truy cập vào trang web và tương tác với nó. Điều này sẽ giúp người dùng nâng cao tầm nhìn và tiếp cận của mình đến đông đảo khách hàng tiềm năng.

Bảng 2 Cấu hình phiên bản EC2 và RDS

Dịch vụ	Cấu hình	Phiên bản
EC2	Amazon Machine Image	Ubuntu Server 22.04 LTS (HVM), SSD Volume Type
	Instance type	t2.micro
RDS	Engine Version	MySQL 8.0.32
	Availability and durability	Multi-AZ DB instance
	DB instance class	db.t3.micro

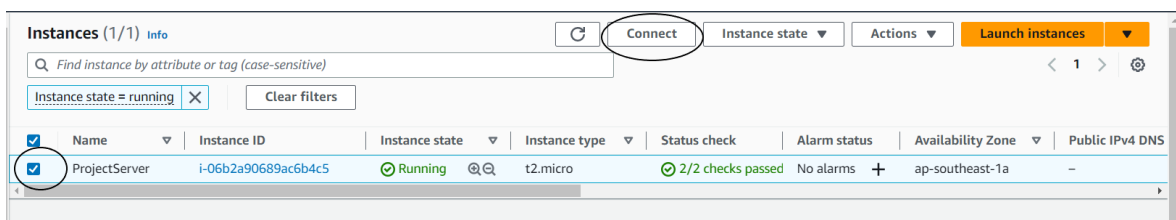
3.2.3 Kiểm thử

Phần này có độ dài từ hai đến ba trang. Sinh viên thiết kế các trường hợp kiểm thử cho hai đến ba chức năng quan trọng nhất. Sinh viên cần chỉ rõ các kỹ thuật kiểm thử đã sử dụng. Chi tiết các trường hợp kiểm thử khác, nếu muốn trình bày, sinh viên đưa vào phần phụ lục.

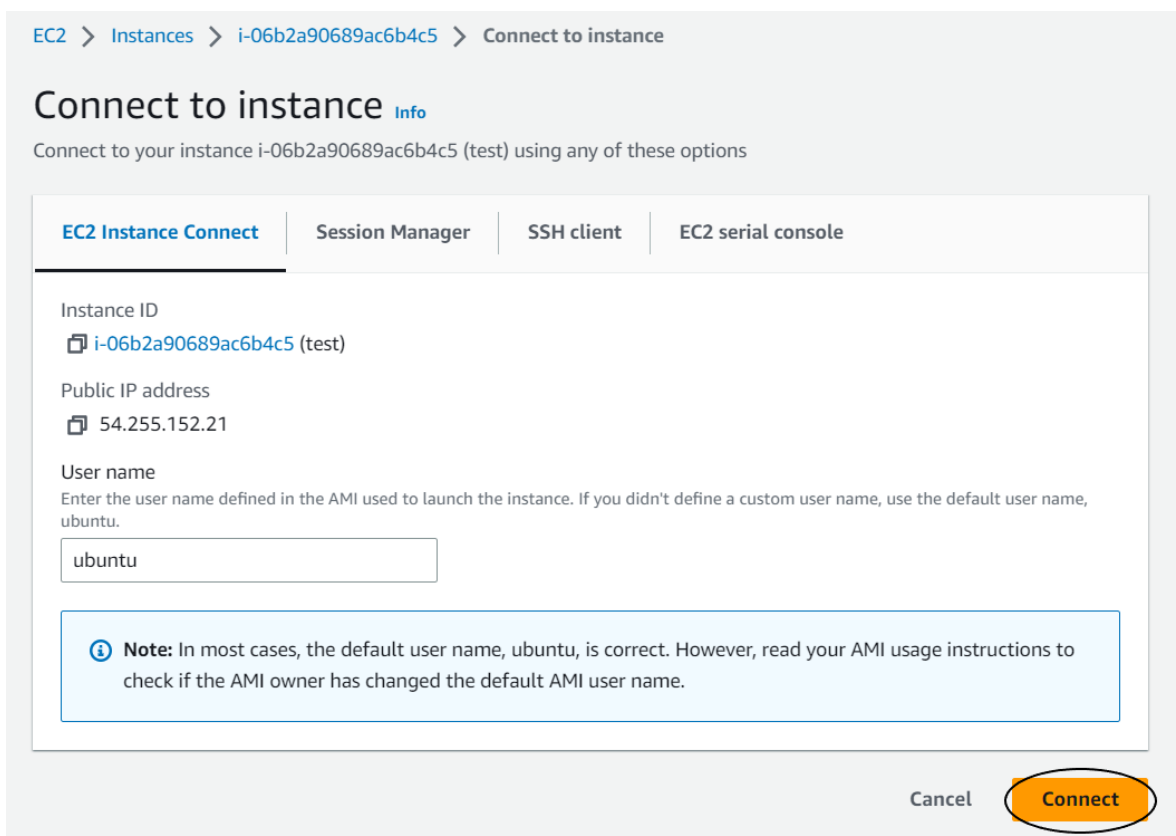
Sinh viên sau cùng tổng kết về số lượng các trường hợp kiểm thử và kết quả kiểm thử. Sinh viên cần phân tích lý do nếu kết quả kiểm thử không đạt.

3.2.3.1 Kiểm tra EC2 Instance có kết nối được không ?

Sau khi khởi tạo thành công instance EC2, kiểm tra đã kết nối được với instance EC2 hay chưa ?



Sau khi click “Connect” ta được



Sau khi “Connect”, nếu màn hình sau xuất hiện người dùng đã kết nối thành công

```
aws | Services | Search [Alt+S]
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage

System information as of Mon May 8 15:35:00 UTC 2023

System load: 0.0 Processes: 99
Usage of /: 27.0% of 7.57GB Users logged in: 0
Memory usage: 58% IPv4 address for eth0: 10.0.0.206
Swap usage: 0%

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.

  https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Mon May 8 15:31:34 2023 from 3.0.5.37
ubuntu@ip-10-0-0-206:~$
```

Ngược lại, nếu hệ thống thông báo lỗi, rất có thể là do 1 trong các lỗi như cấu hình bảo mật, kết nối mạng, lỗi ssh, lỗi phần mềm, instance bị hỏng... Nếu đã cấu hình Security Group cho instance, hãy kiểm tra xem địa chỉ IP của máy tính có được phép truy cập vào instance không, nếu địa chỉ IP của máy tính không nằm trong danh sách được phép, hãy thêm vào. Tiếp theo, kiểm tra kết nối mạng của instance bởi có thể xảy ra một số lỗi như mất kết nối mạng hoặc instance bị đóng băng. Còn nếu người dùng đang sử dụng kết nối SSH để truy cập vào instance, hãy kiểm tra lại thông tin đăng nhập và xác thực SSH. Nếu instance không hoạt động bình thường, có thể do một số lỗi phần mềm trên instance, người dùng nên kiểm tra các tệp nhật ký để xác định nguyên nhân cụ thể. Trong một số trường hợp, instance có thể bị hỏng hoặc bị lỗi phần cứng và người dùng lúc này nên tạo một instance mới và khôi phục lại dữ liệu từ bản sao lưu.

3.2.3.2 Kiểm tra EC2 Instance đã kết nối với RDS databases chưa ?

Sau khi đã cài các công cụ cần thiết cho máy chủ để bắt đầu việc triển khai, ta sẽ truy cập vào MySQL Sever bằng tên mà người dùng đã thiết lập khi khởi tạo RDS database cùng với host là endpoint của RDS database. Sau khi nhập xong thì hệ thống yêu cầu nhập tiếp mật khẩu. Nếu hệ thống hiển thị giao diện như dưới đây thì người dùng đã kết nối thành công.

```
aws | Services | Search [Alt+S]
Ubuntu Pro subscription. Free for personal use.
https://ubuntu.com/aws/pro
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Mon May 8 15:35:00 2023 from 3.0.5.37
ubuntu@ip-10-0-0-206:~$ mysql -u admin -h databaseproject.cc8wmiuolpsc.ap-southeast-1.rds.amazonaws.com -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 376
Server version: 8.0.32 Source distribution

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Trường hợp hệ thống báo lỗi, rất có khả năng là một trong những lỗi sau: (i) Sai tên đăng nhập hoặc mật khẩu: Kiểm tra xem tên người dùng và mật khẩu đã được nhập đúng chưa, đặc biệt là mật khẩu có thể bị sai nếu bạn đã nhập sai khi được yêu cầu. (ii) Sai tên host hoặc địa chỉ IP: Đảm bảo rằng tên host hoặc địa chỉ IP của máy chủ MySQL đang chạy đúng và được nhập chính xác. (iii) Các quyền truy cập không đủ: Đôi khi người dùng không có đủ quyền để truy cập vào máy chủ MySQL. Kiểm tra lại xem người dùng có đủ quyền để kết nối và truy cập vào cơ sở dữ liệu không. (iv) Máy chủ MySQL không chạy: Kiểm tra xem máy chủ MySQL đã được khởi động và đang chạy hay không. Nếu không, hãy khởi động lại máy chủ MySQL. (v) Các cấu hình bảo mật trên máy chủ: Nếu máy chủ MySQL đã được cấu hình để chặn truy cập từ các máy khác hoặc có các giới hạn quyền truy cập khác, bạn có thể không thể kết nối tới máy chủ.

3.2.4 Minh họa các chức năng chính

Sinh viên lựa chọn và đưa ra màn hình cho các chức năng chính, quan trọng, và thú vị nhất. Mỗi giao diện cần phải có lời giải thích ngắn gọn. Khi giải thích, sinh viên có thể kết hợp với các chú thích ở trong hình ảnh giao diện.

Chức năng chính và thú vị nhất sau khi triển khai thành công dịch vụ EC2 kết hợp với RDS đó là quản lý database và truy vấn dữ liệu. Ví dụ như thêm sửa xóa dữ liệu người dùng, sản phẩm ... Sau đây, nhóm em sẽ thử tạo một tài khoản mới và kiểm tra bảng user trong database có được cập nhật thêm không ?

Kết nối với Instance EC2, đảm bảo máy chủ đã được cài sẵn các công cụ cần thiết cho việc triển khai. Bắt đầu kết nối với trình quản lý mysql server. Nhập lệnh “use shonline_db” để bắt đầu thao tác với cơ sở dữ liệu shonline_db.

```
aws Services Search [Alt+S]

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| shonline_db |
| sys |
+-----+
5 rows in set (0.00 sec)

mysql> use shonline_db;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

Nhập lệnh “select*from users;” để kiểm tra các tài khoản có sẵn trong bảng users

```
aws Services Search [Alt+S]

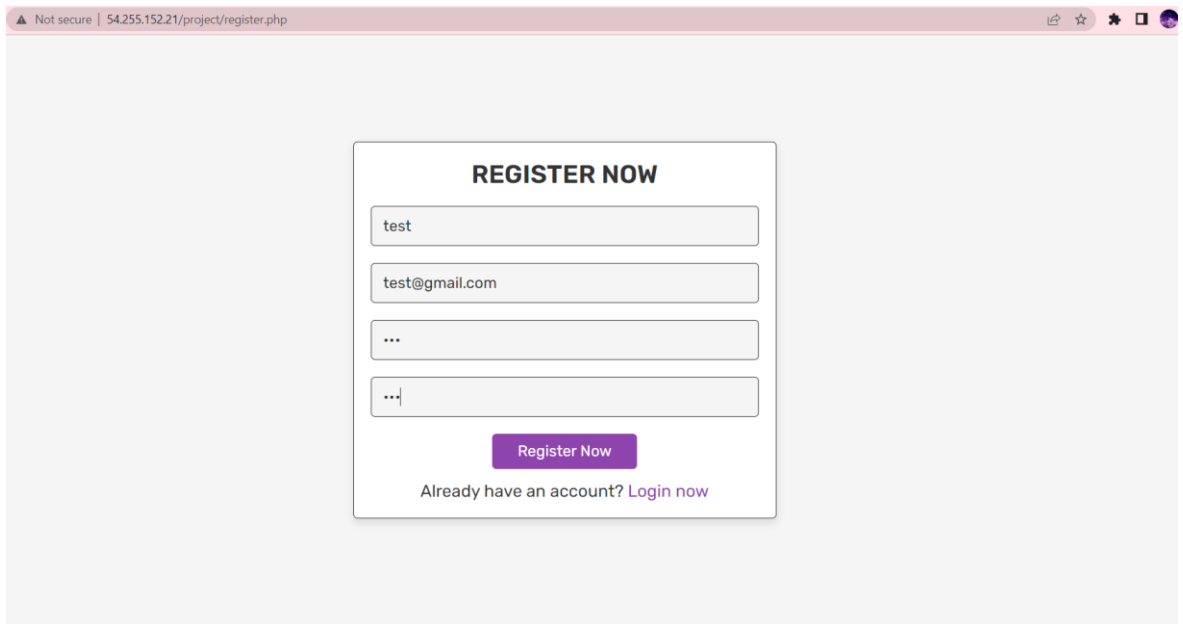
mysql>
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| shonline_db |
| sys |
+-----+
5 rows in set (0.00 sec)

mysql> use shonline_db;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select * from users;
+-----+
| id | name | email | password | user_type |
+-----+
| 1 | admin | admin@gmail.com | 202cb962ac59075b964b07152d234b70 | admin |
| 2 | abc | abcd@123.com | 202cb962ac59075b964b07152d234b70 | user |
| 3 | user | user@gmail.com | 202cb962ac59075b964b07152d234b70 | user |
| 4 | user1 | user1@gmail.com | 202cb962ac59075b964b07152d234b70 | user |
| 5 | 123 | 123@gmail.com | 202cb962ac59075b964b07152d234b70 | user |
+-----+
5 rows in set (0.01 sec)

mysql>
```

Lúc này, trong bảng users có 5 tài khoản, ta sẽ bắt đầu tạo thêm một tài khoản trên trang web và kiểm tra lại



REGISTER NOW

test

test@gmail.com

...

...

Register Now

Already have an account? [Login now](#)

Sau khi tạo xong, nhập lại lệnh “select*from users;” để kiểm tra database đã được cập nhật hay chưa.

```
mysql> select * from users;
```

id	name	email	password	user_type
1	admin	admin@gmail.com	202cb962ac59075b964b07152d234b70	admin
2	abc	abcd@123.com	202cb962ac59075b964b07152d234b70	user
3	user	user@gmail.com	202cb962ac59075b964b07152d234b70	user
4	user1	user1@gmail.com	202cb962ac59075b964b07152d234b70	user
5	123	123@gmail.com	202cb962ac59075b964b07152d234b70	user
6	test	test@gmail.com	202cb962ac59075b964b07152d234b70	user

```
6 rows in set (0.00 sec)
```

```
mysql>
```

Database đã được cập nhật thành công, qua chức năng này, ta có thể quản lý được dữ liệu về tài khoản người dùng, các sản phẩm cho web server của mình

3.3 Triển khai

3.3.1 Cấu hình VPC

Tạo một VPC với IPv4 CIDR 10.0.0.0/16

Services
Search
[Alt+S]

VPC > Your VPCs > Create VPC

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only
☐ VPC and more

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

Project

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block
☐ IPAM-allocated IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block
☐ IPv6 CIDR owned by me

Tenancy [Info](#)

Default ▼

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
<div>Q Name X</div>	<div>Q Project X</div>	<div>Remove</div>

Add new tag

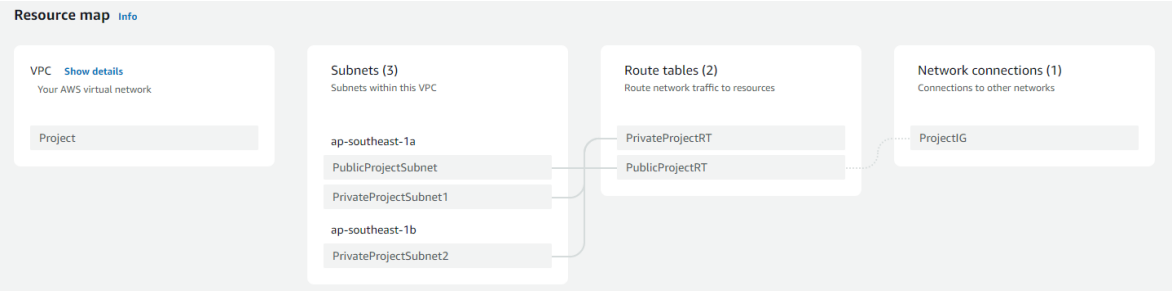
You can add 49 more tags.

Cancel
Create VPC

CloudShell
Feedback
Language

Tiếp theo, ta tạo thêm một internet gateway tên ProjectIG rồi attach tới VPC Project vừa tạo. Đổi tên router table vừa sinh ra sau khi tạo VPC là PrivateProjectRT, tạo thêm một router table mới là PublicProjectRT, chọn “Edit routes” để thêm cổng kết nối với internet gateway. Tạo 1 subnet PublicProjectSubnet với IPv4 CIDR 10.0.0.0/24 đặt trong vùng az A, 2 subnet PrivateProjectSubnet1 với IPv4 CIDR 10.0.1.0/24 và PrivateProjectSubnet2 với IPv4 CIDR 10.0.2.0/24 đặt trong vùng az B. Tạo một security group ProjectSG và thêm các cổng http và ssh.

Sau khi cấu hình VPC xong, ta sẽ có một sơ đồ tài nguyên như sau:



3.3.2 Cấu hình RDS

Tạo một subnet group với cấu hình như sau (Chọn 2 subnet private từ 2 zone A B)

Amazon RDS X

Dashboard
Databases
Query Editor
Performance insights
Snapshots
Exports in Amazon S3
Automated backups
Reserved instances
Proxies

Subnet groups
Parameter groups
Option groups
Custom engine versions

Events
Event subscriptions

Recommendations 3
Certificate update

RDS > Subnet groups > Create DB subnet group

Create DB subnet group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

Subnet group details

Name
You won't be able to modify the name after your subnet group has been created.
projectsg
Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description
abc

VPC
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.
Project (vpc-0099ad75046d3d392)

Add subnets

Availability Zones
Choose the Availability Zones that include the subnets you want to add.
Choose an availability zone
ap-southeast-1a X ap-southeast-1b X

Subnets
Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.
Select subnets
subnet-0ba5d32fa163cc2c2 (10.0.1.0/24) X
subnet-068a56d8d07385931 (10.0.2.0/24) X

For Multi-AZ DB clusters, you must select 3 subnets in 3 different Availability Zones.

Subnets selected (2)

Availability zone	Subnet ID	CIDR block
ap-southeast-1a	subnet-0ba5d32fa163cc2c2	10.0.1.0/24
ap-southeast-1b	subnet-068a56d8d07385931	10.0.2.0/24

Cancel Create

Tạo thêm một security group DatabaseSG dành cho database. Trong security group đó, thêm một luật với type là MYSQL/Aurora, source là security group khi cấu hình VPC.

Ta tạo tiếp một database với Engine type là MySQL, Engine Version là MySQL 8.0.32, Templates chọn Production, Availability and durability là Multi-AZ DB instance. Tiếp tục đặt tên cho database, điền tài khoản mật khẩu, DB instance class chọn db.t3.micro, Storage type là General Purpose SSD (gp2), chọn DB subnet group vừa mới tạo, VPC security group chọn DatabaseSG.

3.3.3 Cấu hình S3

Người dùng tiến hành khởi tạo một bucket tên project.bucket.s3, chọn ACLs enabled, bỏ chọn Block all public access. Sau khi tạo xong bucket, người dùng upload file code được nén dưới dạng file zip, trong mục permissions chọn Grant public-read access để người dùng có thể tải file về máy.

3.3.4 Cấu hình EC2

Người dùng tiến hành khởi tạo một instance EC2 ProjectServer với cấu hình như sau. Amazon Machine Image là Ubuntu Server 22.04 LTS (HVM), SSD Volume Type, Instance type là t2.micro, tạo hoặc chọn một key pair có sẵn, VPC là Project, subnet là PublicProjectSubnet, cho phép Auto-assign public IP, security group là ProjectSG, Number of instances là 1. Cuối cùng click “Launch instance” để bắt đầu khởi tạo.

EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

[Add additional tags](#)

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

ami-0a72af05d27b49ccb (64-bit (x86)) / ami-0dd28c803f9318319 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-03-25

Architecture

AMI ID

64-bit (x86) ami-0a72af05d27b49ccb Verified provider

Summary

Number of instances Info

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...[read more](#)

ami-0a72af05d27b49ccb

Virtual server type (instance type)

t2.micro

Firewall (security group)

ProjectSG

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel [Launch instance](#) [Review commands](#)

▼ Instance type Info

Instance type

t2.micro
Family: t2 1 vCPU 1 GiB Memory Current generation: true Free tier eligible
On-Demand Windows pricing: 0.0192 USD per Hour
On-Demand RHEL pricing: 0.0746 USD per Hour
On-Demand Linux pricing: 0.0146 USD per Hour
On-Demand SUSE pricing: 0.0146 USD per Hour

All generations
Compare instance types

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

NguyenDaiPhat
Create new key pair

▼ Network settings Info

VPC - required Info

vpc-0099ad75046d3d392 (Project)
10.0.0.0/16

Subnet Info

subnet-0243e75e662472535
VPC: vpc-0099ad75046d3d392 Owner: 002052590803
Availability Zone: ap-southeast-1a IP addresses available: 250 CIDR: 10.0.0.0/24

PublicProjectSubnet
Create new subnet

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group
Select existing security group

Common security groups Info

Select security groups

ProjectSG sg-078342b731fd626d4
VPC: vpc-0099ad75046d3d392

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

▼ Summary

Number of instances Info

1

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...read more
ami-0a72af05d27b49ccb

Virtual server type (instance type)

t2.micro

Firewall (security group)

ProjectSG

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Launch instance

Review commands

Sau khi khởi tạo instance EC2, người dùng tạo thêm một Elastic Ips và tham chiếu với instance vừa được tạo. Sau cùng, người dùng bắt đầu kết nối với RDS databases vừa được tạo, kết nối instance và cài đặt các công cụ cần thiết cho việc triển khai trên máy chủ EC2. Sau đây là một số lệnh cho việc cài công cụ. (i) `sudo su` : Chuyển sang quyền root, (ii) `apt install php libapache2-mod-php php-mysql -y` : Cài đặt PHP, mô-đun Apache để hỗ trợ PHP và mô-đun PHP MySQL trên hệ thống, (iii) `apt install unzip` : cài đặt phần mềm giải nén, (iv) `wget https://s3.ap-southeast-1.amazonaws.com/project.bucket.s3/project.zip` : tải xuống file zip từ bucket S3, (v) `unzip project.zip -d /var/www/html/` : giải nén file zip đã tải xuống vào thư mục /var/www/html/.

Kết nối và quản lý RDS databases từ máy chủ EC2. (i) viết lệnh “`apt install mysql-server -y`” : Cài đặt MySQL Server, (ii) Copy endpoint của database RDS và viết lệnh “`mysql -u admin -h databaseproject.cc8wmiuolpsc.ap-southeast-1.rds.amazonaws.com -p`” rồi nhập mật khẩu. Sau khi truy cập thành công, ta sao chép và dán vào file sql đã chuẩn bị sẵn.

Sao chép IP của EC2 và paste sang tab mới. Ví dụ: <http://13.215.193.71/project/home.php>.

Kết chương: Trong chương này, chúng ta đã triển khai và quản lý thành công một ứng dụng lên EC2 có kết nối với database cụ thể là một source web php. Trong chương sau, chúng ta sẽ hướng tới các giải pháp và đóng góp nổi bật, những khó khăn và hướng giải quyết mà nhóm đã làm.

Chương 4 Các giải pháp và đóng góp nổi bật

Trong đề tài này, nhóm em đã tìm hiểu, nghiên cứu và thực hiện triển khai hệ thống đáp ứng các nhu cầu của doanh nghiệp và người dùng thông qua dịch vụ EC2 của AWS. Để có thể triển khai một dịch vụ EC2 hoàn thiện, nhóm cần tìm hiểu thêm về VPC - Dịch vụ mạng cho phép người dùng tạo ra một mạng riêng ảo, RDS - dịch vụ quản lý cơ sở dữ liệu quan hệ và S3 dịch vụ lưu trữ đám mây dùng để lưu source code, trong đó EC2 sẽ được kết nối với RDS và cả 2 được đặt trên các subnet đã được cấu hình trong VPC. Một số giải pháp mà nhóm đạt được trong quá trình tìm hiểu đề tài và thực hành là:

Thiết kế cơ sở hạ tầng cho VPC (i) Giới thiệu vấn đề: Khi thiết kế cơ sở hạ tầng cho VPC, cần xác định một số yếu tố quan trọng để đảm bảo tính bảo mật và khả năng mở rộng của hạ tầng như subnet, router table, security group, (ii) Giải pháp: Xác định mục đích sử dụng VPC, tìm hiểu các khái niệm cơ bản cũng như các thành phần quan trọng của VPC, (iii) Kết quả đạt được: Việc thiết kế cơ sở hạ tầng cho VPC đạt được mục đích bảo mật, mở rộng và đáp ứng nhu cầu sử dụng của người dùng. Các giải pháp được áp dụng giúp tiết kiệm thời gian và đảm bảo tính chính xác, đồng thời giúp giảm thiểu rủi ro bảo mật và tăng cường kiểm soát các hoạt động trên hạ tầng.

Tạo RDS database (i) Giới thiệu vấn đề: Cần xác định vấn đề quan trọng để đảm bảo tính khả dụng và bảo mật của cơ sở dữ liệu bao gồm thiết kế kiến trúc cơ sở dữ liệu để đáp ứng nhu cầu sử dụng, cần có kế hoạch sao lưu và phục hồi dữ liệu để đảm bảo tính khả dụng và bảo mật của cơ sở dữ liệu. (ii) Giải pháp: Sử dụng database kiểu Multi-AZ DB, khi đó Amazon RDS sẽ tự động tạo một phiên bản cơ sở dữ liệu chính sau đó sao chép, đồng bộ dữ liệu sang một phiên bản dự phòng trong một vùng sẵn sàng (AZ) khác. Việc này giúp cơ sở dữ liệu được đảm bảo an toàn phòng trường hợp có vùng sẵn sàng hay database bị lỗi.

Triển khai máy chủ ảo (EC2) và kết nối với cơ sở dữ liệu (RDS) trên AWS (i) Giới thiệu vấn đề: Cấu hình các ứng dụng và phần mềm để kết nối EC2 với RDS và thiết lập các biện pháp bảo mật, quản lý quyền truy cập để đảm bảo tính bảo mật và hạn chế truy cập đến dữ liệu. (ii) Giải pháp: Đặt EC2 trên một public subnet để kết nối với Internet, đặt RDS trên private subnet để đảm bảo tính bảo mật. Tìm kiếm và sàng lọc những dịch vụ cần thiết cài đặt cho máy chủ EC2 bao gồm cả kết nối, quản lý database. Trên tất cả người dùng chỉ được kết nối với RDS thông qua việc truy cập vào EC2.

Trong chương 3, mục 3.1 thiết kế tổng quan, nhóm đã tự thiết kế một cơ sở hạ tầng đơn giản bao gồm 3 dịch vụ VPC, EC2 và RDS, đây không chỉ là mô hình mà nhóm em tâm đắc nhất nó còn là dấu mốc lớn cho việc hiểu đề tài sau nhiều tuần nghiên cứu làm quen với nhiều khái niệm mới lạ. Tuy nhiên, trong quá trình nghiên cứu và thực hành, nhóm cũng gặp không ít các khó khăn. Đầu tiên, một số thành viên của nhóm vẫn chưa đăng kí được tài khoản AWS do gặp nhiều vấn đề khác nhau như khó khăn hay mất thời gian trong việc làm thẻ visa... gây nên nhiều cản trở về thời gian thực hành và làm quen với công nghệ này. Thứ hai, để thực sự hiểu sâu về lợi ích hay từng thành phần, khái niệm trong EC2, nhóm cũng cần phải tìm hiểu thêm nhiều các dịch vụ liên quan như VPC, RDS, S3... nên việc triển khai EC2 trở nên khá phức tạp khi nhóm em thường xuyên bối rối mỗi lần gặp các lỗi lạ trong việc triển khai hay liên kết dịch vụ AWS và mất rất nhiều thời gian để có thể giải quyết. Thứ ba là chi phí dịch vụ, đối với một doanh nghiệp thì việc sử dụng EC2 sẽ tiết kiệm rất nhiều chi phí đặc biệt là chi phí đầu tư phần cứng vật lý, nhưng đối với sinh viên thì đây là một vấn đề khá là nan giải. Thậm chí nhóm cũng từng mất tiền oan khi quên không tắt dịch vụ dẫn đến rỗng túi và chán nản. Và cuối cùng là khó khăn trong việc tích hợp với các dịch vụ khác. Trong thời gian qua nhóm cũng chưa thể đa dạng các dịch vụ khác cho việc triển khai như quản lý dữ liệu RDS thông qua dịch vụ S3 bằng dịch vụ AWS Glue... Hơn nữa, nhóm cũng chưa đủ thời gian và trình độ để tìm hiểu sâu hơn các dịch vụ nâng cao của EC2 như gắn Domain, Load Balancing – Dịch vụ giúp phân phối tải đồng đều giữa các instance EC2 hay Auto Scaling – Dịch vụ cho phép tự động thay đổi số lượng các instance EC2 trong một group theo nhu cầu của ứng dụng...

Để khắc phục các hạn chế trên, nhóm đã sử dụng tài khoản awsacademy được cấp trong quá trình học. Nhóm cũng dành một phần lớn thời gian để tập trung nghiên cứu làm quen các dịch vụ miễn phí mà AWS cung cấp cho tài khoản mới. Nhóm cũng đã thành công trong việc cấu hình một EC2 theo ý muốn kết hợp với các dịch vụ khác như VPC, RDS đồng thời cũng triển khai thành công một ứng dụng web sử dụng ngôn ngữ php với một địa chỉ IP tĩnh.

Chương 5 Kết luận và hướng phát triển

5.1 Kết luận

Sinh viên so sánh kết quả nghiên cứu hoặc sản phẩm của mình với các nghiên cứu hoặc sản phẩm tương tự.

Sinh viên phân tích trong suốt quá trình thực hiện BTL, mình đã làm được gì, chưa làm được gì, các đóng góp nổi bật là gì, và tổng hợp những bài học kinh nghiệm rút ra nếu có.

So với các nghiên cứu hoặc sản phẩm tương tự khác, sản phẩm của nhóm em mặc dù có thể triển khai thành công nhưng vẫn còn khá đơn giản và chưa có nhiều chức năng quan trọng.

Trong suốt quá trình thực hiện bài tập lớn, nhóm đã tạo dựng thành công mô hình triển khai bao gồm VPC, RDS và EC2, đồng thời từ mô hình đó mà xây dựng, triển khai thành công một ứng dụng web lên máy chủ cloud. Nhóm chưa kịp tìm hiểu hết và thực hành hết tất cả các chức năng của EC2 và tích hợp với các dịch vụ khác trên AWS.

Sau khi thực hiện bài tập lớn triển khai và quản lý dịch vụ EC2, mình đã rút ra một số bài học kinh nghiệm như sau. Lập kế hoạch cẩn thận: Trước khi triển khai EC2, cần lập kế hoạch kỹ lưỡng để đảm bảo rằng các yêu cầu và mục tiêu được xác định rõ ràng, đồng thời tối ưu hóa hiệu suất và tối đa hóa sự đáng tin cậy. Sử dụng nhóm bảo mật: Việc sử dụng nhóm bảo mật giúp quản lý quyền truy cập tài nguyên một cách hiệu quả hơn, giảm thiểu các lỗ hổng bảo mật và đảm bảo an toàn cho các tài nguyên của bạn. Thiết lập các chính sách IAM: Các chính sách IAM giúp bạn quản lý quyền truy cập tài nguyên của AWS một cách chính xác và an toàn, giúp đáp ứng được các yêu cầu về bảo mật và quản lý của doanh nghiệp. Backup dữ liệu thường xuyên: Việc sao lưu dữ liệu thường xuyên giúp bạn đảm bảo rằng dữ liệu của bạn được bảo vệ tốt nhất và có thể phục hồi được nhanh chóng nếu cần thiết. Monitoring và log: Việc sử dụng các công cụ giám sát và theo dõi giúp bạn theo dõi các hoạt động của hệ thống và phát hiện các vấn đề sớm hơn, giúp giải quyết các sự cố nhanh chóng và đảm bảo tính sẵn sàng của hệ thống. Tối ưu hóa chi phí: Việc sử dụng các dịch vụ AWS có thể tiết kiệm chi phí hơn so với việc triển khai hệ thống riêng. Cần phải tối ưu hóa chi phí một cách khôn ngoan để đảm bảo sự hiệu quả và khả năng cạnh tranh. Học tập liên tục: Việc học tập liên tục về các công nghệ mới và các tiêu chuẩn bảo mật sẽ giúp bạn nâng cao kỹ năng và cải thiện khả năng quản lý và bảo mật của mình.

5.2 Hướng phát triển

Sau khi hoàn thành bài tập lớn này, nhóm đã có một số hướng phát triển và định hướng trong công việc tương lai. Đầu tiên là nâng cao kiến thức về AWS, nhóm em sẽ tìm hiểu thêm về các dịch vụ khác của AWS để có thể sử dụng và triển khai một số ứng dụng phức tạp hơn. Thứ hai là tìm hiểu về một số công cụ tương tự như DevOps, Docker, Kubernetes, đó là một phương pháp để triển khai và quản lý các ứng dụng. Thứ ba là tham gia các dự án mã nguồn mở liên quan đến AWS để cải thiện kỹ năng của mình và đóng góp cho cộng đồng. Và cuối cùng là học thêm các kỹ năng khác như lập trình, quản lý dự án, xây dựng sản phẩm để trở thành một nhà phát triển hoàn chỉnh.

Trong tương lai, nhóm sẽ tập trung tìm hiểu, nghiên cứu sâu hơn về dịch vụ EC2 và các dịch vụ khác của AWS. Trước hết, nhóm sẽ thực hành và phát triển thêm các dịch vụ nâng cao hơn của EC2 như load balancing, auto scaling, ... Sau cùng, nhóm sẽ tích hợp thêm chức năng khác trên AWS như dịch vụ IAM (Identity and Access Management): quản lý quyền truy cập vào tài nguyên của AWS bằng cách thiết lập các chính sách quản lý người dùng, nhóm người dùng và vai trò, hay chức năng liên kết dịch vụ S3 với RDS thông qua AWS Glue, ...

Tài liệu tham khảo

- [1] Michael Wittig & Andreas Wittig, Amazon Web Services in Action, Manning Publications Co, 2015.
- [2] AWS Documentation, <https://docs.aws.amazon.com/> , last visited May 2023.
- [3] Amazon Web Services, <https://aws.amazon.com/>, last visited May 2023.
- [4] AWS Blog, <https://aws.amazon.com/blogs/>, last visited May 2023.

