

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP.HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN**



HCMUTE

MÔN HỌC: ĐIỆN TOÁN Đám Mây

ĐỀ TÀI XÂY DỰNG VPC VÀ CHẠY WEBSERVER TRÊN AWS

GVHD: GV. HUỲNH XUÂN PHỤNG

Nhóm sinh viên thực hiện: Nhóm

1. NGUYỄN TUẤN VŨ - 18133064

2. NGUYỄN XUÂN HIỆU - 18133013

Tp. Hồ Chí Minh, tháng 11 năm 2020

Lời nói đầu

Chúng em xin chân thành cảm ơn sự hướng dẫn tận tình của thầy

HUỲNH XUÂN PHỤNG đã giúp chúng em hoàn thành bài báo cáo cuối kì bộ môn Điện toán đám mây Tuy đã cố gắng học tập, tìm hiểu, phân tích thiết kế và xây dựng hệ thống nhưng ắt hẳn thiếu sót là điều không thể tránh khỏi. Chúng em rất mong nhận được sự thông cảm và góp ý chân thành của Thầy. Chúng em xin chân thành cảm ơn.

Mục lục:

Contents

Phần mở đầu	4
1. Nội dung đề tài	4
2. Triển khai đề tài	4
Phần lý thuyết	5
1. Cloud Computing	5
2. Amazon Virtual Private Cloud (Amazon VPC)	5
2.1. Subnet	6
2.2. Route Table	6
2.3. Internet Gateway	7
2.4. Network address translation (NAT)	8
2.5. Security Group	8
3. DynamoDB	10
3.1. Các thành phần DynamoDB cơ bản:	10
Phần demo	13
1. VPC	13
1.1. ElasticIP – Tạo Public IP để kết nối tới máy chủ EC2	13
1.2. Tạo VPC có Public Subnet 1 và Private Subnet 1	13
1.3. Tạo Public Subnet 2 và Private Subnet 2	15
1.4. Route Table	17
1.5. Security Group	18
1.6. Tạo EC2 Web Server	19
1.7. Tạo RDS Database Server	22
1.8. Sử dụng MySQL Workbench, dùng SSH kết nối EC2 và MySQL Server	28
1.9. Tạo RDS MySQL Database schoolmanagement	29
1.10. Kết nối SSH bằng CMD truy cập vào EC2	31
1.11. Download Project School PHP – MySQL	33
1.12. Kết quả Demo	35
2. DynamoDB	37
1.1. Cài đặt python và các thư viện cần thiết	37
1.2. Tạo Endpoint DynamoDB	37
1.3. Thiết lập Security Group cho EC2 đã tạo ở VPC	39
1.4. Git Clone TicTacToe (đã tải ở VPC)	39
1.5. Thiết lập key kết nối	39
1.6. Chạy Flask Server	40
Phần kết luận	42
1. Kết quả đạt được	42
2. Kết quả chưa đạt được	42
3. Hướng phát triển	42
4. Tài liệu tham khảo	42

Phần mở đầu

1. Nội dung đề tài

- Xây dựng VPC: 1 public subnet + 1 private subnet
- Khởi tạo 1 EC2 (cài đặt web server) + 1 DynamoDB
- Website quản lý thông tin sinh viên (Giao diện + Xử lý + Database đơn giản)

Github: <https://github.com/Vu-Nguyen2201/VPC-Webserver-AWS>

2. Triển khai đề tài

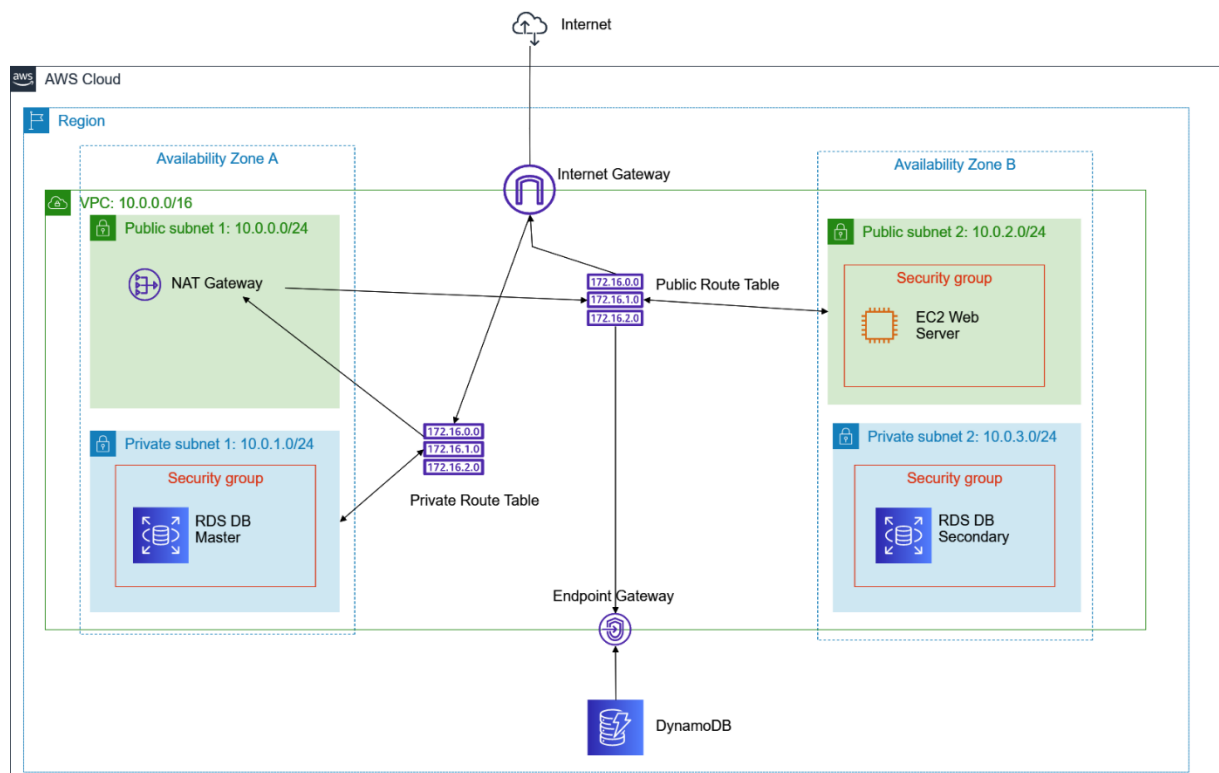
Xây dựng 1 VPC có 2 public subnet + 2 private subnet

Project 1 – Trang web quản lý khoá học PHP - MySQL

- Thiết lập máy chủ EC2 trên public subnet và cài đặt PHP Web Service
- Thiết lập RDS MySQL, cài đặt schoolmanagement DB trên private subnet

Project 2 – Game đánh caro chạy trên Flask Framework (Python) và sử dụng DynamoDB

- Tạo 1 DynamoDB Endpoint cho phép EC2 kết nối với DynamoDB



Phần lý thuyết

1. Cloud Computing

Điện toán đám mây là gì?

Điện toán đám mây là việc phân phối các tài nguyên CNTT theo nhu cầu qua Internet với chính sách thanh toán theo mức sử dụng. Thay vì mua, sở hữu và bảo trì các trung tâm dữ liệu và máy chủ vật lý, người dùng có thể tiếp cận các dịch vụ công nghệ, như xử lý tính toán, cơ sở dữ liệu, các dịch vụ IT khi cần thiết, từ nhà cung cấp dịch vụ đám mây như Amazon Web Services (AWS).

2. Amazon Virtual Private Cloud (Amazon VPC)



Virtual Private Cloud giúp người dùng tạo ra một môi trường mạng riêng ảo nơi mà bạn có thể sử dụng để kết nối nội bộ giữa các dịch vụ **AWS** theo cách bạn quản trị phục vụ cho các mục tiêu bảo mật hệ thống. Người dùng sẽ có toàn quyền quản lý môi trường hệ thống mạng riêng ảo bao gồm : *tạo subnet, cấu hình bảng routing, gateway mạng, lựa chọn sử dụng IPv4 hay IPv6 trong VPC*.

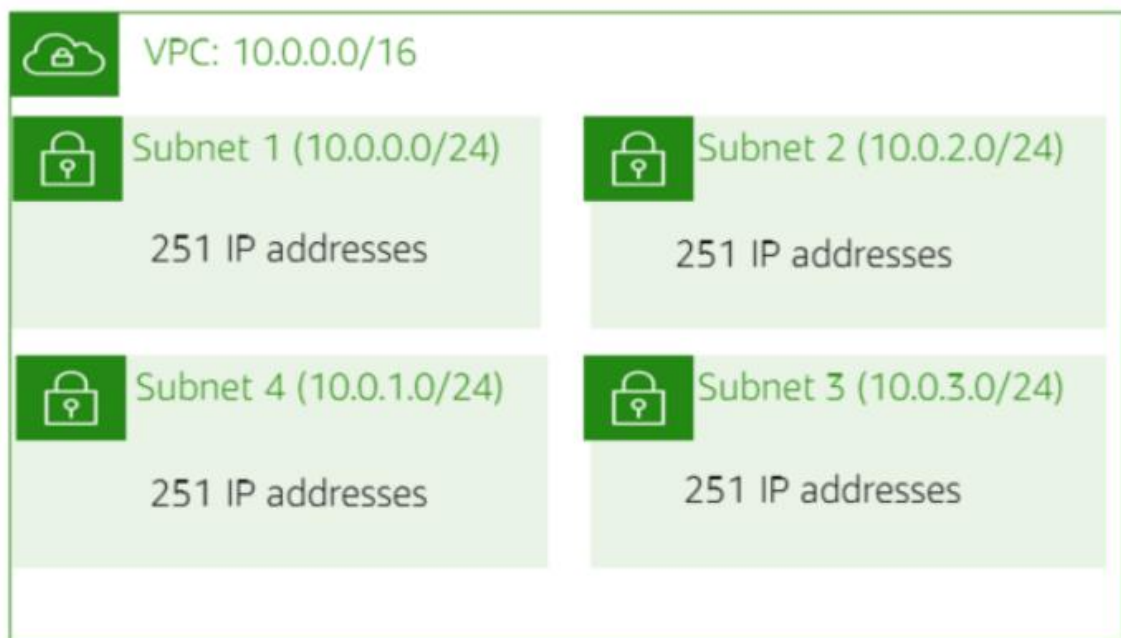
Bạn dễ dàng tùy biến cấu hình mạng đối với **Amazon VPC**. Ví dụ như bạn có thể tạo ra một subnet mạng public dành cho web server để bên ngoài truy cập vào, còn lại bạn cấu hình cho hệ thống backend như database hoặc ứng dụng server nằm trong lớp mạng nội bộ (private) không có đường kết nối Internet public. Bạn còn có thể gia cố thêm nhiều lớp bảo mật cho hệ thống mạng dịch vụ AWS của bạn với : *security group, access control list network, ...* giúp bạn kiểm soát chặt chẽ hơn nữa quyền truy cập vào các Amazon EC2 Instance chẳng hạn.

Một số dịch vụ AWS có thể sử dụng **AWS VPC** như sau :

- Amazon EC2
- Amazon Route 53
- Amazon WorkSpaces
- Auto Scaling

- Elastic Load Balancing
- AWS Data Pipeline
- Elastic Beanstalk
- Amazon Elastic Cache
- Amazon EMR
- Amazon OpsWorks
- Amazon RDS
- Amazon Redshift

2.1. Subnet



Sau khi tạo VPC, người dùng có thể chia nó thành một hoặc nhiều subnet.

Subnet: là một dải địa chỉ IP trong VPC của bạn. Bạn có thể khởi tạo tài nguyên AWS với một Subnet chỉ định. Ví dụ sử dụng public subnet để các dịch vụ của bạn truy cập được Internet, còn thì sử dụng Private Subnet để các dịch vụ của bạn trong lớp mạng nội bộ bảo mật không truy cập Internet.

2.2. Route Table

Một bảng định tuyến bao gồm các rule được gọi là 'route', các route này sẽ giúp xác định đường đi của lưu lượng mạng ra vào. Mỗi subnet trong VPC của bạn sẽ được liên kết với một bảng định tuyến (route table), bảng định tuyến này sẽ quản lý route trong subnet. Một subnet chỉ có thể liên kết với 1 bảng định tuyến tại 1

thời điểm, nhưng chiều ngược lại bạn có thể liên kết nhiều subnet với 1 bảng định tuyến.

Public Subnet Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Private Subnet Route Table

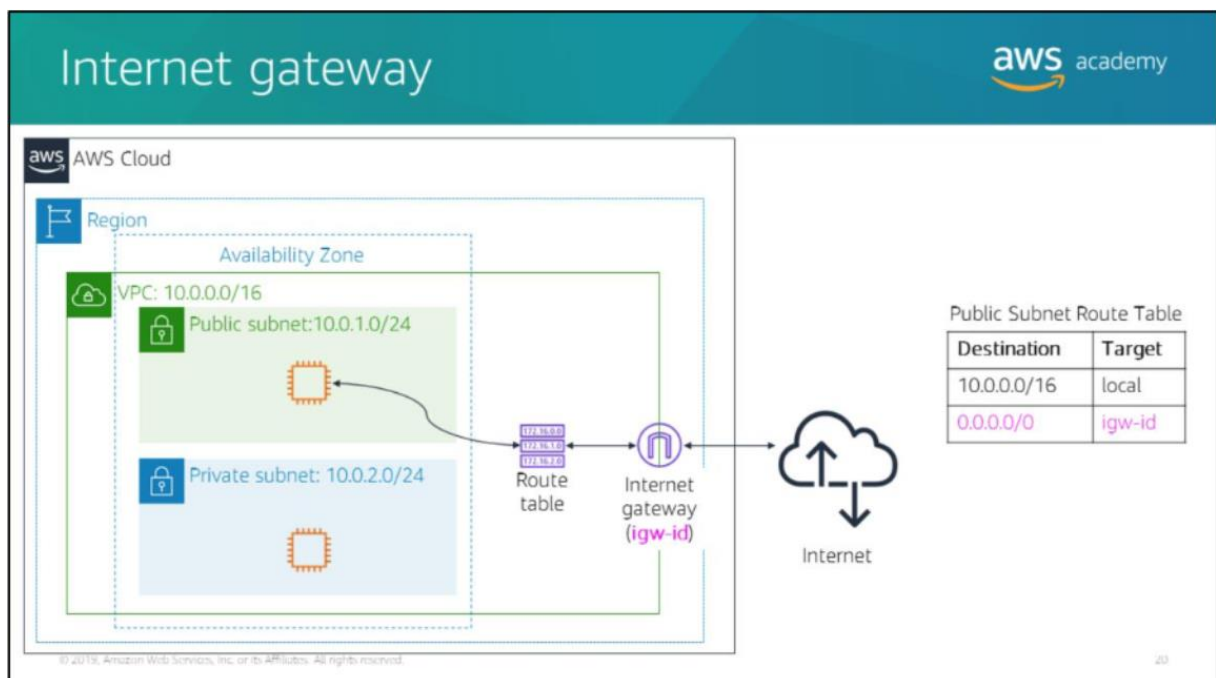
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	nat-gw-id

Destination là đích đến của lưu lượng mạng từ subnet, Dest có thể là 1 dải CIDR / IP address

Target là nơi gói tin cần đến trước khi đến Dest

2.3. Internet Gateway

Internet Gateway cho phép bạn tạo một subnet public có route kết nối ra Internet public.



Cổng internet phục vụ hai mục đích: cung cấp target trong bảng route table VPC để có thể định tuyến internet và thực hiện dịch địa chỉ mạng (Nat) cho các instances được chỉ định địa chỉ IPv4 công cộng (public subnet)

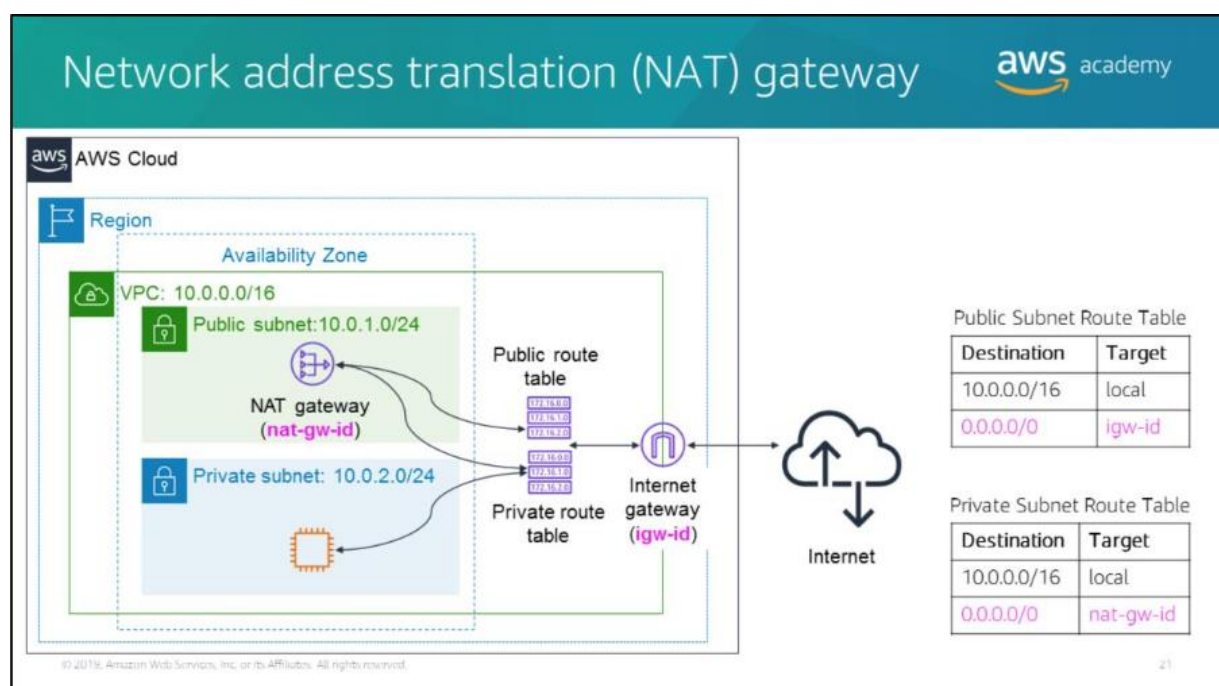
Internet Gateway cung cấp một cách hợp lý NAT thay mặt cho instances, để khi lưu lượng truy cập rời khỏi mạng con VPC của bạn và đi đến internet, trường địa chỉ trả lời được đặt thành public IPv4 address hoặc Elastic IP của instances và không phải private IP address của instances

2.4. Network address translation (NAT)

NAT gateway cho phép instances ở private subnet kết nối với internet hoặc các dịch vụ AWS, nhưng ngăn không cho internet kết nối tới instances này

NAT gateway được đặt trong public subnet để có thể kết nối internet

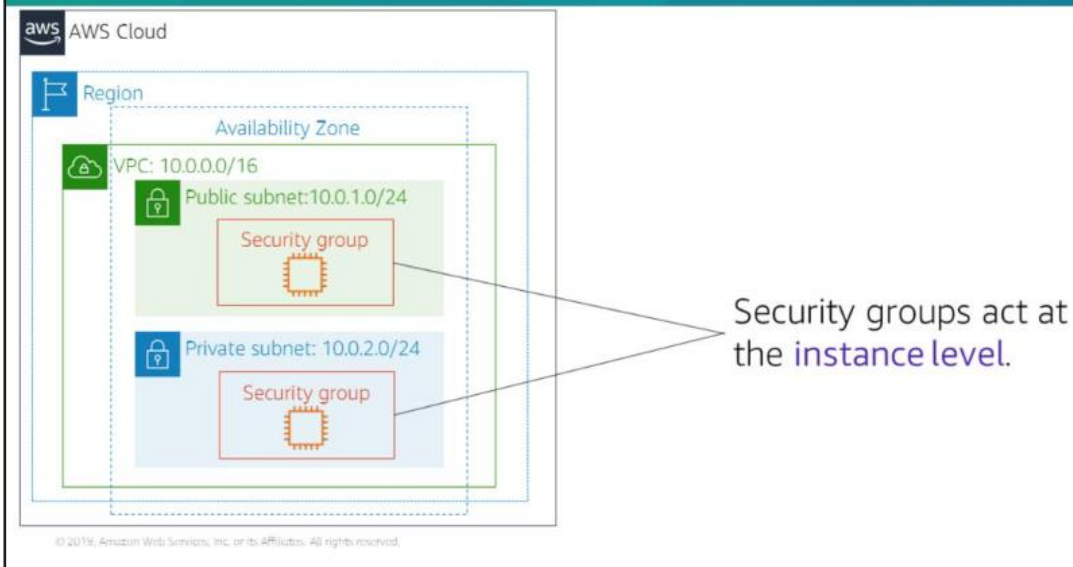
Thiết lập lại route table(0.0.0.0/0, nat) để private subnet có thể kết nối tới internet



2.5. Security Group

Là lớp bảo mật đầu tiên dành cho các Instance, hoạt động như một firewall ảo và bạn sẽ phải định nghĩa rule firewall trước khi traffic ra vào Instance.

Security groups



Inbound				
Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	All web traffic
HTTPS	TCP	443	0.0.0.0/0	All web traffic
SSH	TCP	22	54.24.12.19/32	Office address
Outbound				
Type	Protocol	Port Range	Source	Description
All traffic	All	All	0.0.0.0/0	
All traffic	All	All	::/0	

Cho phép HTTP, HTTPS, SSH ngoài (inbound traffic) vào Instance.

Cho phép tất cả traffic trong (outbound traffic) Instance đi ra.

Mặc định khi khởi tạo, Inbound không có rule nào cả và Outbound thì cho phép tất cả lưu lượng ra khỏi instance => không cho phép bất cứ lưu lượng nào được truy cập vào trong.

- Cho phép tất cả traffic ngoài (inbound traffic) vào Instance.
- Cho phép tất cả traffic trong (outbound traffic) Instance đi ra.

3. DynamoDB

- **DynamoDB** là một dịch vụ quản lý **NoSQL** có khả năng đáp ứng hiệu suất cao và nhanh kèm theo khả năng mở rộng. Nếu bạn là một nhà phát triển, bạn có thể sử dụng **DynamoDB** để tạo ra một bảng có khả năng lưu trữ và truy xuất bất kỳ số lượng dữ liệu, mà vẫn có thể phục vụ cho bất kỳ mức độ request traffic.
- **DynamoDB** tự động phân tán dữ liệu và traffic của một bảng ra một số lượng server vừa đủ để có thể xử lý request capacity đặt ra bởi khách hàng và lượng dữ liệu lưu trữ, và đồng thời đảm bảo hiệu suất nhanh và đồng nhất. Tất cả dữ liệu được lưu trữ trên SSD và tự động được sao chép ra các vùng sẵn sàng (**Availability Zones**) trong một khu vực (**Region**) để cung cấp độ sẵn sàng cao và độ bền của dữ liệu (**high availability and data durability**)
- Nếu bạn là một nhà quản lý dữ liệu, bạn có thể tạo một bảng dữ liệu mới, mở rộng hay thu hẹp request capacity mà không bị giảm hiệu suất, và có thể thay đổi các thông số qua **AWS Management Console**. Với **DynamoDB**, bạn có thể phó thác gánh nặng quản lý và mở rộng dữ liệu cho AWS và không phải lo lắng về việc cung cấp hardware, thiết lập và cài đặt, sao chép dữ liệu.

3.1. Các thành phần DynamoDB cơ bản:

1. **Tables** - Tương tự như các hệ thống cơ sở dữ liệu khác, DynamoDB lưu trữ dữ liệu trong các bảng. Một *bảng* là một tập hợp các dữ liệu. Ví dụ: hãy xem bảng ví dụ có tên *Mọi người* mà bạn có thể sử dụng để lưu trữ thông tin liên hệ cá nhân về bạn bè, gia đình hoặc bất kỳ ai khác mà bạn quan tâm. Bạn cũng có thể có bảng *Ô tô* để lưu trữ thông tin về các phương tiện mà mọi người lái.
2. **Items** - Mỗi table chứa không hoặc nhiều Items. Một *item* là một nhóm các thuộc tính đó là nhận dạng duy nhất trong số tất cả các mặt hàng khác. Các item trong DynamoDB tương tự như rows, records hoặc tuples trong các hệ thống cơ sở dữ liệu khác. Trong DynamoDB, không có giới hạn về số lượng mục bạn có thể lưu trữ trong một bảng.
3. **Attributes** - Mỗi Item bao gồm một hoặc nhiều **Attributes**. Một **Attributes** là một yếu tố dữ liệu cơ bản, một cái gì đó mà không cần phải được chia nhỏ thêm nữa. Các **Attributes** trong DynamoDB tương tự với các trường hoặc cột trong các hệ thống cơ sở dữ liệu khác.
4. **Primary Key**: Khi tạo một bảng, thì ngoài việc khai báo tên bảng bạn cần chỉ rõ primary key . Primary key để đảm bảo rằng không có hai items nào trong bảng có cùng primary key. DynamoDB hỗ trợ hai loại primary key sau:

a. Partition key:

- Một khóa chính đơn giản, bao gồm một thuộc tính được gọi là Partition key.
- DynamoDB sử dụng giá trị của Partition key làm đầu vào cho Hash function bên trong. Đầu ra từ Hash function xác định phân vùng (bộ nhớ vật lý bên trong DynamoDB) mà mục sẽ được lưu trữ.
- Trong bảng chỉ có Partition key, không có hai mục nào có thể có cùng giá trị Partition key

b. Partition key and sort key:

- Được gọi là Primary Key *tổng hợp*, loại khóa này bao gồm hai thuộc tính. Thuộc tính đầu tiên là Partition key và thuộc tính thứ hai là sort key
- DynamoDB sử dụng giá trị Partition key làm đầu vào cho hàm Hash bên trong. Đầu ra từ hàm Hash xác định phân vùng (bộ nhớ vật lý bên trong DynamoDB) mà mục sẽ được lưu trữ. Tất cả các mục có cùng giá trị Partition key được lưu trữ cùng nhau, theo thứ tự được sắp xếp theo giá trị sort key.
- Trong bảng có Partition key và sort key, hai mục có thể có cùng giá trị Partition key. Tuy nhiên, hai mục đó phải có giá trị sort key khác nhau.

5. Secondary index:

Để giúp cho việc truy cập dữ liệu, Amazon DynamoDB tạo và quản lý index cho primary key. Việc này giúp cho hệ thống truy cập dữ liệu khá nhanh khi chỉ định primary key. Tuy nhiên, nhiều hệ thống có lẽ sẽ hưởng lợi từ việc có một hoặc hai key thay thế (alternate). Để tăng tốc độ truy cập bạn có thể tạo ra secondary index.

Một secondary index là một cấu trúc dữ liệu chứa tập con của các attributes trong một bảng, cùng với một key thay thế để hỗ trợ cho Query operation. Với một secondary index, các query sẽ không bị giới hạn khi chỉ sử dụng được primary key; bạn có thể truy vấn dữ liệu bằng việc sử dụng key thay thế từ secondary index. Một bảng có thể có nhiều secondary index để hỗ trợ cho nhiều query pattern.

DynamoDB hỗ trợ hai loại index:

- Global secondary index: một loại index có hash và range key khác với hash và range key từ bảng gốc.
- Local secondary index: một loại index mà có hash key trùng với hash key từ bảng gốc và range key là một attribute khác.

6. DynamoDB Streams:

DynamoDB Streams là một tính năng tùy chọn ghi lại các sự kiện sửa đổi dữ liệu trong bảng DynamoDB. Dữ liệu về các sự kiện này xuất hiện trong luồng theo thời gian gần thực và theo thứ tự các sự kiện đã xảy ra.

Mỗi sự kiện được đại diện bởi một *bản ghi luồng*. Nếu bạn bật luồng trên bảng, DynamoDB Streams sẽ ghi một bản ghi luồng bất cứ khi nào một trong các sự kiện sau xảy ra:

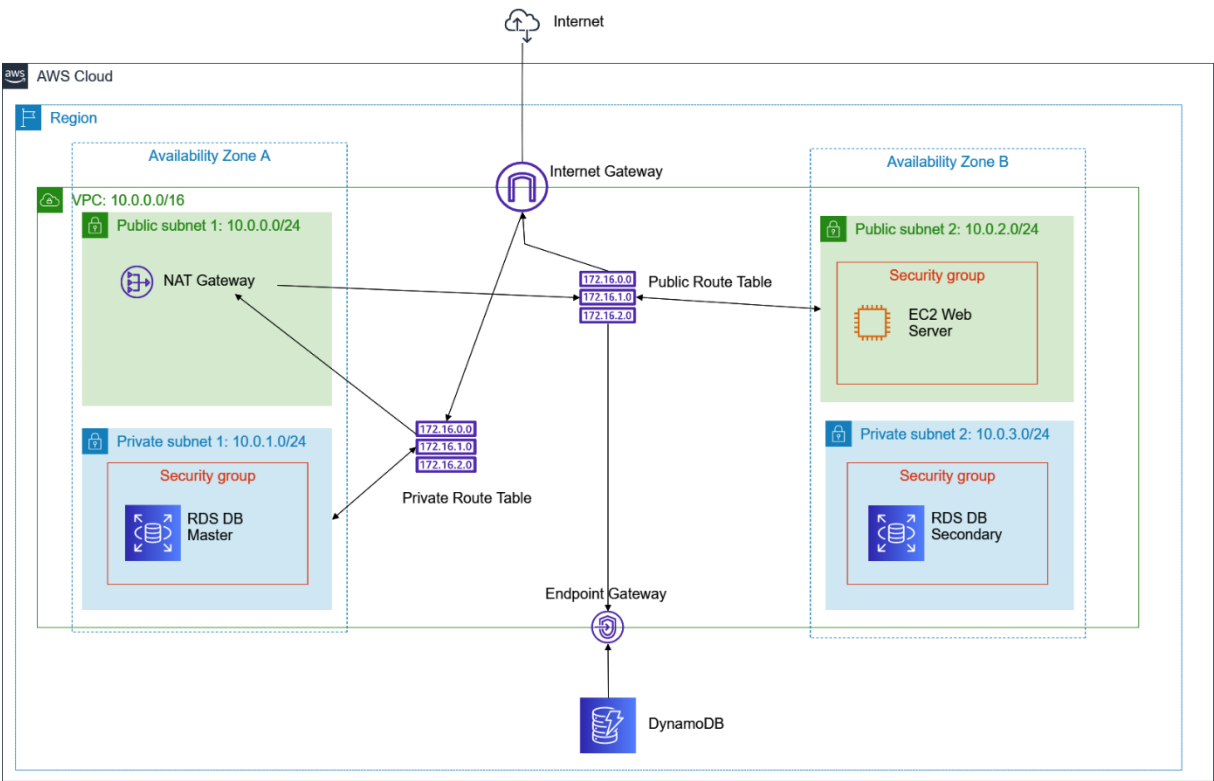
- Một mục mới được thêm vào bảng: Luồng chụp ảnh của toàn bộ mục, bao gồm tất cả các thuộc tính của nó.
- Một mặt hàng được cập nhật: Luồng ghi lại hình ảnh "trước" và "sau" của bất kỳ thuộc tính nào đã được sửa đổi trong mặt hàng.
- Mục bị xóa khỏi bảng: Luồng chụp ảnh của toàn bộ mục trước khi bị xóa.

Mỗi bản ghi luồng cũng chứa tên của bảng, dấu thời gian sự kiện và siêu dữ liệu khác. Bản ghi luồng có thời gian tồn tại là 24 giờ; sau đó, chúng tự động bị xóa khỏi luồng.

Bạn có thể sử dụng DynamoDB Streams cùng với AWS Lambda để tạo trình *kích hoạt* —mã tự động chạy bất cứ khi nào một sự kiện quan tâm xuất hiện trong một luồng

Phần demo

Project 1 – Trang web quản lý khoá học PHP - MySQL



1. VPC

1.1. ElasticIP – Tạo Public IP để kết nối tới máy chủ EC2

Elastic IP addresses (1/1)

Filter Elastic IP addresses

<input checked="" type="checkbox"/>	Name	Allocated IPv4 add...	Type	Allocation ID	Associated
<input checked="" type="checkbox"/>	-	54.83.78.212	Public IP	eipalloc-0fef423efa95416a	-

1.2. Tạo VPC có Public Subnet 1 và Private Subnet 1

School VPC

Step 2: VPC with Public and Private Subnets

IPv4 CIDR block:* (65531 IP addresses available)

IPv6 CIDR block: ☒ No IPv6 CIDR Block
☐ Amazon provided IPv6 CIDR block
☐ IPv6 CIDR block owned by me

VPC name:

Public subnet's IPv4 CIDR:* (251 IP addresses available)

Availability Zone:* ▼

Public subnet name:

Private subnet's IPv4 CIDR:* (251 IP addresses available)

Availability Zone:* ▼

Private subnet name:

You can add more subnets after AWS creates the VPC.

Specify the details of your NAT gateway ([NAT gateway rates apply](#)).

Elastic IP Allocation ID:*

Service endpoints

Enable DNS hostnames:* ☒ Yes ☐ No

Hardware tenancy:* ▼

Kết quả

Your VPCs (1/3) Info

Filter VPCs

Actions

Create VPC

	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR (Network border group)	
<input checked="" type="checkbox"/>	School VPC	vpc-0b71855a5ba8307a1	Available	10.0.0.0/16	–	
<input type="checkbox"/>	–	vpc-0d48564b8995e1f4c	Available	172.31.0.0/16	–	
<input type="checkbox"/>	Work VPC	vpc-0ed97255d6b3e228b	Available	10.0.0.0/16	–	

vpc-0b71855a5ba8307a1 / School VPC

Details

CIDRs

Flow logs

Tags

Details

VPC ID

vpc-0b71855a5ba8307a1

Tenancy

Default

Default VPC

No

Route 53 Resolver DNS Firewall rule groups

Failed to load rule groups

State

Available

DHCP options set

dopt-01e77d56fe0a9f809

IPv4 CIDR

10.0.0.0/16

Owner ID

271382871042

DNS hostnames

Enabled

Main route table

rtb-02cc2ff0891ffa53c

IPv6 pool

–

DNS resolution

Enabled

Main network ACL

acl-005fa169457e5aba4

IPv6 CIDR (Network border group)

–

1.3. Tạo Public Subnet 2 và Private Subnet 2

Create subnet [Info](#)

VPC

VPC ID

Create subnets in this VPC.

vpc-0b71855a5ba8307a1

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 2

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

Public Subnet 2

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1b

IPv4 CIDR block [Info](#)

10.0.2.0/24

Tags - optional

Key

Name

Value - optional

Public Subnet 2

Remove

Add new tag

You can add 49 more tags.

Remove

Subnet 2 of 2

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

Private Subnet 2

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1b

IPv4 CIDR block [Info](#)

10.0.3.0/24

Tags - optional

Key

Name

Value - optional

Private Subnet 2

Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Cancel

Create subnet

Kết quả

You have successfully created 2 subnets: subnet-0afa3550d4af6c510, subnet-0b22b03b83d558bfd

Subnets (2) Info

Filter subnets

Subnet ID: subnet-0afa3550d4af6c510 X Subnet ID: subnet-0b22b03b83d558bfd X Clear filters

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	Public Subnet 2	subnet-0afa3550d4af6c510	Available	vpc-0b71855a5ba8307a1 Sc...	10.0.2.0/24	-
<input type="checkbox"/>	Private Subnet 2	subnet-0b22b03b83d558bfd	Available	vpc-0b71855a5ba8307a1 Sc...	10.0.3.0/24	-

1.4. Route Table

Thiết lập Route Table cho Public Subnet

Public Route Table rtb-07... subnet-0be585996c0298439 / Public Subnet 1 - No vpc-0b71855a5ba8307a1 | School VPC 2

rtb-0787c96d70e7cbdce / Public Route Table

Details Routes Subnet associations Edge associations Route propagation Tags

Routes (2) Edit routes

Filter routes Both

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-0114379aff1176d40	Active	No

Public Route Table rtb-0787c96d70e7cbdce 2 subnets - No vpc-0b71855a5ba8307a1 | Sc... 271382...

rtb-0787c96d70e7cbdce / Public Route Table

Details Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (2) Edit subnet associations

Find subnet association

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0afa3550d4af6c510 / Public Subnet 2	10.0.2.0/24	-
subnet-0be585996c0298439 / Public Subnet 1	10.0.0.0/24	-

Thiết lập Route Table cho Private Subnet

<input checked="" type="checkbox"/>	Private Route Table	rtb-02cc2ff0891ffa53c	–	–	Yes	vpc-0b71855a5ba8307a1 Sc...	271382...
<input type="checkbox"/>	–	rtb-0f2c6bc0fd16aa895	–	–	Yes	vpc-0ed97255d6b3e228b W...	271382...
<input type="checkbox"/>	Public Route Table	rtb-0787c96d70e7cbdce	2 subnets	–	No	vpc-0b71855a5ba8307a1 Sc...	271382...

rtb-02cc2ff0891ffa53c / Private Route Table

Details

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Both

< 1 >

⚙

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	nat-0ccdd0374163347e	Active	No

<input checked="" type="checkbox"/>	Private Route Table	rtb-02cc2ff0891ffa53c	2 subnets	–	Yes	vpc-0b71855a5ba8307a1 Sc...	271382...
<input type="checkbox"/>	–	rtb-0f2c6bc0fd16aa895	–	–	Yes	vpc-0ed97255d6b3e228b W...	271382...
<input type="checkbox"/>	Public Route Table	rtb-0787c96d70e7cbdce	2 subnets	–	No	vpc-0b71855a5ba8307a1 Sc...	271382...

rtb-02cc2ff0891ffa53c / Private Route Table

Details

Routes

Subnet associations

Edge associations

Route propagation

Tags

Explicit subnet associations (2)

< 1 >

⚙

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0b22b03b83d558bfd / Private Subnet 2	10.0.3.0/24	–
subnet-053ee4c8a9e02cf3e / Private Subnet 1	10.0.1.0/24	–

1.5. Security Group

Thiết lập Security Group cho Web Server EC2

<input checked="" type="checkbox"/>	Public Security Group	sg-07bb07097a53ed16c	Public Security	vpc-0b71855a5ba8307a1	Public Security	271382871042
-------------------------------------	-----------------------	----------------------	-----------------	-----------------------	-----------------	--------------

sg-07bb07097a53ed16c - Public Security

Details

Inbound rules

Outbound rules

Tags

Inbound rules (5)

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	0.0.0.0/0	–
HTTP	TCP	80	::/0	–
SSH	TCP	22	0.0.0.0/0	–
HTTPS	TCP	443	0.0.0.0/0	–
HTTPS	TCP	443	::/0	–

Thiết lập Security Group cho Database Server

<input checked="" type="checkbox"/>	Private Security Gr...	sg-051770b3ec32193cc	Private Security	vpc-0b71855a5ba8307a1	Private Security	271382871042
<input type="checkbox"/>	-	sg-06bdc9a40df33d584	default	vpc-0d48564b8995e1f4c	default VPC security gr...	271382871042
<input type="checkbox"/>	Public Security Group	sg-07bb07097a53ed16c	Public Security	vpc-0b71855a5ba8307a1	Public Security	271382871042

sg-051770b3ec32193cc - Private Security

Details

Inbound rules

Outbound rules

Tags

Inbound rules (1)

Edit inbound rules

Type	Protocol	Port range	Source	Description - optional
MySQL/Aurora	TCP	3306	sg-07bb07097a53ed16c / Public Security	-

1.6. Tạo EC2 Web Server

Chọn Amazon Linux 2 AMI

Step 1: Choose an Amazon Machine Image (AMI)

[Cancel and Exit](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

×

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0d5eff06f840b45e9 (64-bit x86) / ami-09d19e919d57453f8 (64-bit Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibo 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

☒ 64-bit (x86)
☐ 64-bit (Arm)

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance families Current generation Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of

Number of instances

1

[Launch into Auto Scaling Group](#)

Purchasing option

☐ Request Spot instances

Network

vpc-0b71855a5ba8307a1 | School VPC

[Create new VPC](#)

Subnet

subnet-0afa3550d4af6c510 | Public Subnet 2 | us-e-

251 IP Addresses available

[Create new subnet](#)

Auto-assign Public IP

Enable

▼ Advanced Details

Enclave	<input type="checkbox"/> Enable
Metadata accessible	Enabled
Metadata version	V1 and V2 (token optional)
Metadata token response hop limit	1
User data	<input checked="" type="radio"/> As text <input type="radio"/> As file <input type="checkbox"/> Input is already base64 encoded
	<pre>export PYTHONPATH=/usr/local/lib/python3.7/site-packages sudo echo '<?php phpinfo() ?>' > /var/www/html/info.php # Download Lab files # Turn on web server chkconfig httpd on service httpd start</pre>

```
#!/bin/bash
# Install Apache Web Server and PHP
yum install -y httpd git
amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
sudo echo '<?php phpinfo() ?>' > /var/www/html/info.php
# Download Lab files
# Turn on web server
chkconfig httpd on
service httpd start
```

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☐ Create a new security group
☒ Select an existing security group

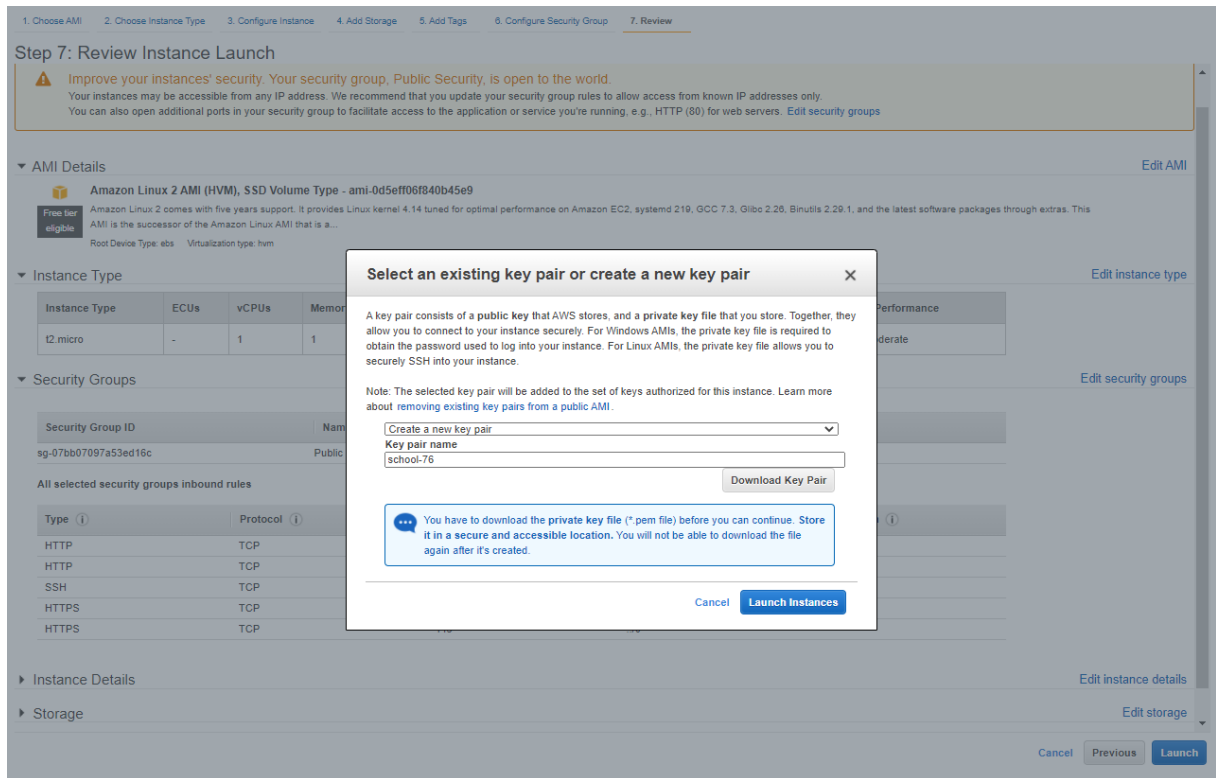
Security Group ID	Name	Description	Actions
<input type="checkbox"/> sg-019c4254e6af0d2f9	default	default VPC security group	Copy to new
<input type="checkbox"/> sg-051770b3ec32193cc	Private Security	Private Security	Copy to new
<input checked="" type="checkbox"/> sg-07bb07097a53ed16c	Public Security	Public Security	Copy to new

Inbound rules for sg-07bb07097a53ed16c (Selected security groups: sg-07bb07097a53ed16c)

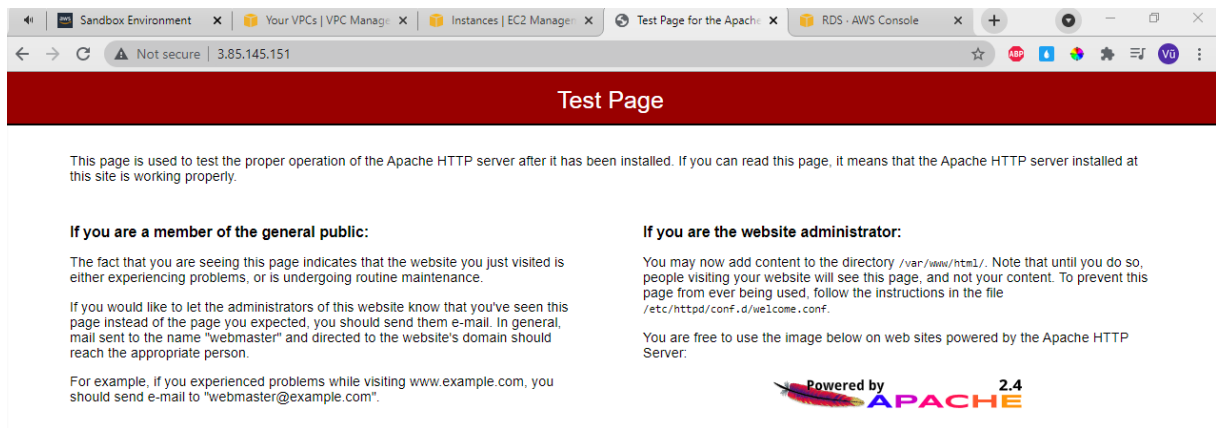
Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	:::0	
SSH	TCP	22	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	
HTTPS	TCP	443	:::0	

[Cancel](#) [Previous](#) [Review and Launch](#)


Download Key Pair để kết nối SSH



Test máy chủ EC2




← → ↻ Not secure | 3.85.225.172/info.php ☆

PHP Version 7.2.34


System	Linux ip-10-0-2-147.ec2.internal 4.14.231-173.361.amzn2.x86_64 #1 SMP Mon Apr 26 20:57:08 UTC 2021 x86_64
Build Date	Oct 21 2020 18:04:56
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-json.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-zip.ini, /etc/php.d/25-curl.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysqli.ini, /etc/php.d/30-pdo_sqlite.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
 Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies



Configuration

bz2

1.7. Tạo RDS Database Server

Tạo Subnet Group

Amazon RDS

Successfully created School Subnet Group. [View subnet group](#)

RDS > Subnet groups > school subnet group

school subnet group

Subnet group details

VPC ID
vpc-0b71855a5ba8307a1

ARN
arn:aws:rds:us-east-1:271382871042:subgrp:school subnet group

Description
School Subnet Group

Subnets (2)

Availability zone	Subnet ID	CIDR block
us-east-1b	subnet-0b22b03b83d558bfd	10.0.3.0/24
us-east-1a	subnet-053ee4c8a9e02cf3e	10.0.1.0/24

Tạo Database MySQL

Create database

Choose a database creation method [Info](#)

- ☒ **Standard create**
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

- ☐ **Easy create**
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type [Info](#)

- ☐ Amazon Aurora



- ☒ **MySQL**



- ☐ MariaDB



- ☐ PostgreSQL



- ☐ Oracle



- ☐ Microsoft SQL Server



Edition

- ☒ **MySQL Community**



Known issues/limitations

Review the [Known issues/limitations](#) to learn about potential compatibility issues with specific database versions.

Version

MySQL 8.0.20



Settings

DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username [Info](#)

Type a login ID for the master user of your DB instance.

1 to 16 alphanumeric characters. First character must be a letter

☐ Auto generate a password

Amazon RDS can generate a password for you, or you can specify your own password

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).

Confirm password [Info](#)

DB instance class

DB instance class [Info](#)

Choose a DB instance class that meets your processing power and memory requirements. The DB instance class options below are limited to those supported by the engine you selected above.

- ☐ Standard classes (includes m classes)
- ☐ Memory optimized classes (includes r and x classes)
- ☒ Burstable classes (includes t classes)

db.t3.micro
2 vCPUs 1 GiB RAM Network: 2,085 Mbps



☐ Include previous generation classes

Storage

Storage type [Info](#)



General Purpose (SSD) ▼

Allocated storage

20

GiB

(Minimum: 20 GiB, Maximum: 16,384 GiB) Higher allocated storage **may improve** IOPS performance.

 Provisioning less than 100 GiB of General Purpose (SSD) storage for high throughput workloads could result in higher latencies upon exhaustion of the initial General Purpose (SSD) IO credit balance. [Learn more](#) 

Storage autoscaling [Info](#)

Provides dynamic scaling support for your database's storage based on your application's needs.

☒ Enable storage autoscaling

Enabling this feature will allow the storage to increase once the specified threshold is exceeded.

Maximum storage threshold [Info](#)

Charges will apply when your database autoscales to the specified threshold

1000

GiB

Minimum: 21 GiB, Maximum: 16,384 GiB

Availability & durability

Multi-AZ deployment [Info](#)

- ☒ Create a standby instance (recommended for production usage)
Creates a standby in a different Availability Zone (AZ) to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.
- ☐ Do not create a standby instance

Connectivity



Virtual private cloud (VPC) [Info](#)

VPC that defines the virtual networking environment for this DB instance.

School VPC (vpc-0b71855a5ba8307a1) ▼

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change the VPC selection.

Subnet group [Info](#)

DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

school subnet group ▼

Public access [Info](#)

☐ Yes

Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.

☒ No

RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

VPC security group

Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.

☒ Choose existing
Choose existing VPC security groups

☐ Create new
Create new VPC security group

Existing VPC security groups

Choose VPC security groups ▼

Private Security ✕

► Additional configuration

▼ Additional configuration

Database options, encryption enabled, backup disabled, backtrace disabled, Enhanced Monitoring disabled, maintenance, CloudWatch Logs, delete protection enabled

Database options

Initial database name [Info](#)

If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group [Info](#)

Option group [Info](#)

Backup

Creates a point-in-time snapshot of your database

☐ Enable automatic backups

Creates a point-in-time snapshot of your database

Encryption

☒ Enable encryption

Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. [Info](#)

Master key [Info](#)

Account

271382871042

KMS key ID

83fc2d8a-ccte-4bab-be3a-343be7eff91e

Monitoring

☐ Enable Enhanced monitoring

Enabling Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU

Log exports

Select the log types to publish to Amazon CloudWatch Logs

☐ Error log

☐ General log

☐ Slow query log

IAM role

The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS service-linked role

ⓘ Ensure that general, slow query, and audit logs are turned on. Error logs are enabled by default. [Learn more](#)

Maintenance

Auto minor version upgrade [Info](#)

☒ Enable auto minor version upgrade

Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

Maintenance window [Info](#)

Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

☐ Select window

☒ No preference

Deletion protection

☒ Enable deletion protection

Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

Estimated monthly costs

DB instance	12.41 USD
Storage	4.60 USD
Multi-AZ standby instance	12.41 USD
Total	29.42 USD

This billing estimate is based on on-demand usage as described in [Amazon RDS Pricing](#). Estimate does not include costs for backup storage, IOs (if applicable), or data transfer.

Estimate your monthly costs for the DB Instance using the [AWS Simple Monthly Calculator](#).

You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

Cancel
Create database

1.8. Sử dụng MySQL Workbrench, dùng SSH kết nối EC2 và MySQL Server

MySQL Connections

Local instance MySQL80

AWS School Server

Connection Name:

AWS School Server

Connection

Remote Management

System Profile

Connection Method:

Standard TCP/IP over SSH

Method to use to connect to the RDBMS

Parameters

SSL

Advanced

SSH Hostname:

3.85.225.172

SSH server hostname, with optional port number.

SSH Username:

ec2-user

Name of the SSH user to connect with.

SSH Password:

Store in Vault ...

Clear

SSH user password to connect to the SSH tunnel.

SSH Key File:

D:\DeTaiAWS\school-76.pem

...

Path to SSH private key file.

MySQL Hostname:

1.ch9ko7w2w007.us-east-1.rds.amazonaws.com

MySQL server host relative to the SSH server.

MySQL Server Port:

3306

TCP/IP port of the MySQL server.

Username:

admin

Name of the user to connect with.

Password:

Store in Vault ...

Clear

The MySQL user's password. Will be requested later if not set.

Default Schema:

The schema to use as default schema. Leave blank to select it later.

New

Delete

Duplicate

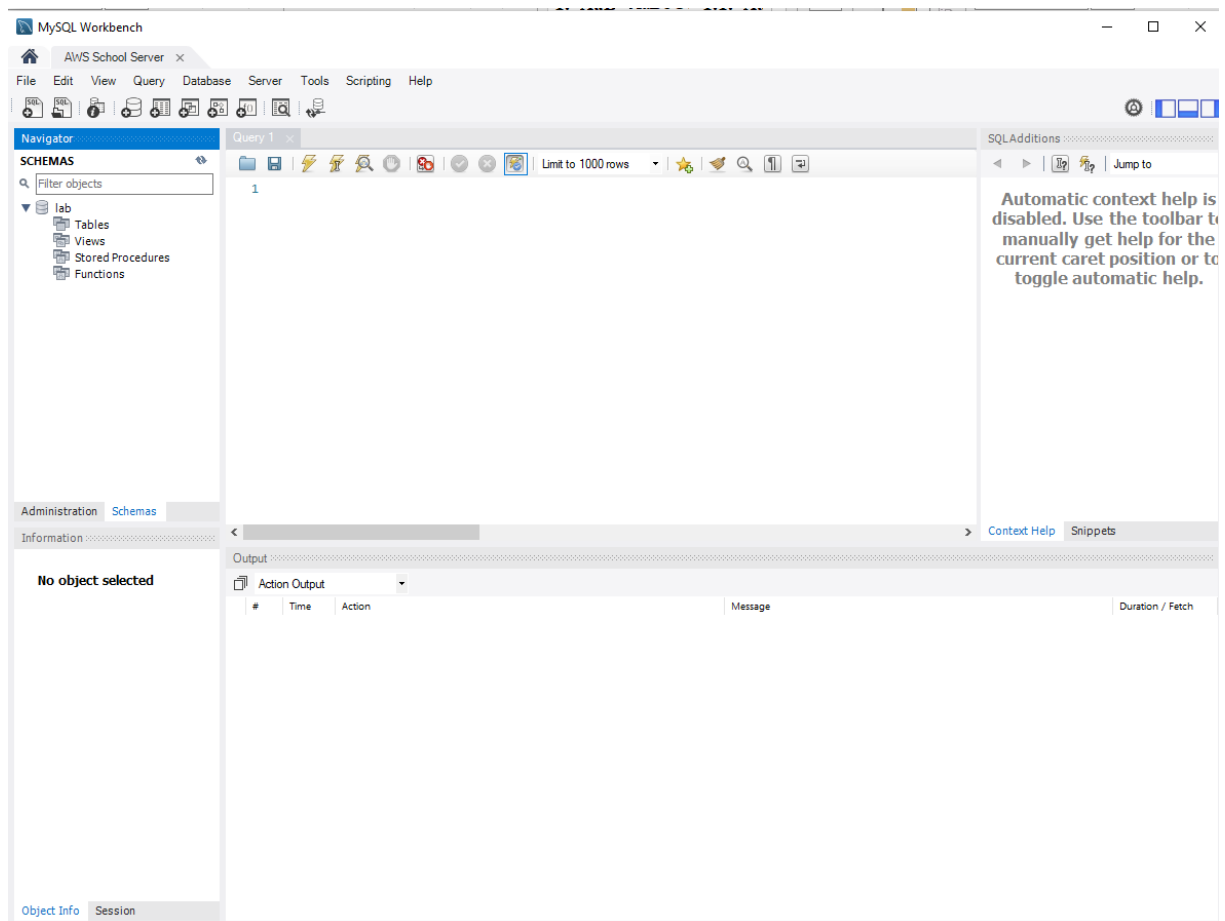
Move Up

Move Down

Test Connection

Close

Kết nối thành công



1.9. Tạo RDS MySQL Database schoolmanagement

MySQL Workbench

File Edit View Query Database Server Tools Scripting Help

Navigator: schoolmanagement

SCHEMAS

Filter objects

lab

Tables

Views

Stored Procedures

Functions

Administration Schemas

Information

No object selected

Object Info Session

Query 1 schoolmanagement

Limit to 1000 rows

```

1 -- phpMyAdmin SQL Dump
2 -- version 4.7.9
3 -- https://www.phpmyadmin.net/
4 --
5 -- Host: 127.0.0.1
6 -- Generation Time: May 27, 2019 at 07:46 PM
7 -- Server version: 10.1.31-MariaDB
8 -- PHP Version: 7.2.3
9
10 • SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
11 • SET AUTOCOMMIT = 0;
12 • START TRANSACTION;
13 • SET time_zone = "+00:00";
14
16 • /*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;

```

SQLAdditions

Automatic context help is disabled. Use the toolbar to manually get help for the current caret position or to toggle automatic help.

Context Help Snippets

Output

Action Output

#	Time	Action	Message	Duration / Fetch
50	14:32:53	INSERT INTO 'tbl_login' ('id', 'loginid', 'password') VALUES (1, 'admin', 'a...	1 row(s) affected	0.297 sec
51	14:32:54	ALTER TABLE 'cities' ADD PRIMARY KEY ('id')	0 row(s) affected Records: 0 Duplicates: 0 Warnings: 0	1.766 sec
52	14:32:56	ALTER TABLE 'countries' ADD PRIMARY KEY ('id')	0 row(s) affected Records: 0 Duplicates: 0 Warnings: 0	0.422 sec
53	14:32:56	ALTER TABLE 'registration' ADD PRIMARY KEY ('id')	0 row(s) affected Records: 0 Duplicates: 0 Warnings: 0	0.453 sec
54	14:32:56	ALTER TABLE 'session' ADD PRIMARY KEY ('id')	0 row(s) affected Records: 0 Duplicates: 0 Warnings: 0	0.406 sec
55	14:32:57	ALTER TABLE 'states' ADD PRIMARY KEY ('id')	0 row(s) affected Records: 0 Duplicates: 0 Warnings: 0	0.609 sec
56	14:32:57	ALTER TABLE 'subject' ADD PRIMARY KEY ('subid')	0 row(s) affected Records: 0 Duplicates: 0 Warnings: 0	0.407 sec
57	14:32:58	ALTER TABLE 'tbl_course' ADD PRIMARY KEY ('cid')	0 row(s) affected Records: 0 Duplicates: 0 Warnings: 0	0.422 sec
58	14:32:58	ALTER TABLE 'tbl_login' ADD PRIMARY KEY ('id')	0 row(s) affected Records: 0 Duplicates: 0 Warnings: 0	0.468 sec
59	14:32:59	ALTER TABLE 'cities' MODIFY 'id' int(11) NOT NULL AUTO_INCREME...	47576 row(s) affected, 1 warning(s): 1681 Integer display width is deprec...	1.000 sec
60	14:33:00	ALTER TABLE 'countries' MODIFY 'id' int(11) NOT NULL AUTO_INCRE...	246 row(s) affected, 1 warning(s): 1681 Integer display width is deprecate...	0.453 sec
61	14:33:01	ALTER TABLE 'registration' MODIFY 'id' int(11) NOT NULL AUTO_INCR...	246 row(s) affected, 1 warning(s): 1681 Integer display width is deprecate...	0.453 sec
61	14:33:01	ALTER TABLE 'registration' MODIFY 'id' int(11) NOT NULL AUTO_INCR...	Running...	?

MySQL Workbench

File Edit View Query Database Server Tools Scripting Help

Navigator: schoolmanagement

SCHEMAS

Filter objects

lab

Tables

Views

Stored Procedures

Functions

schoolmanagement

cities

Columns

Indexes

Foreign Keys

Triggers

countries

registration

session

states

subject

tbl_course

Administration Schemas

Information

Table: cities

Columns:

id int AI PK

name varchar(30)

state_id int

Query 1 schoolmanagement cities

Limit to 1000 rows

```

1 • SELECT * FROM schoolmanagement.cities;

```

SQLAdditions

Automatic context help is disabled. Use the toolbar to manually get help for the current caret position or to toggle automatic help.

Context Help Snippets

Result Grid

id	name	state_id
1	Bombufat	1
2	Garacharma	1
3	Port Blair	1
4	Rangat	1
5	Addanki	2
6	Adivivaram	2
7	Adoni	2

cities 1 x

Apply Revert

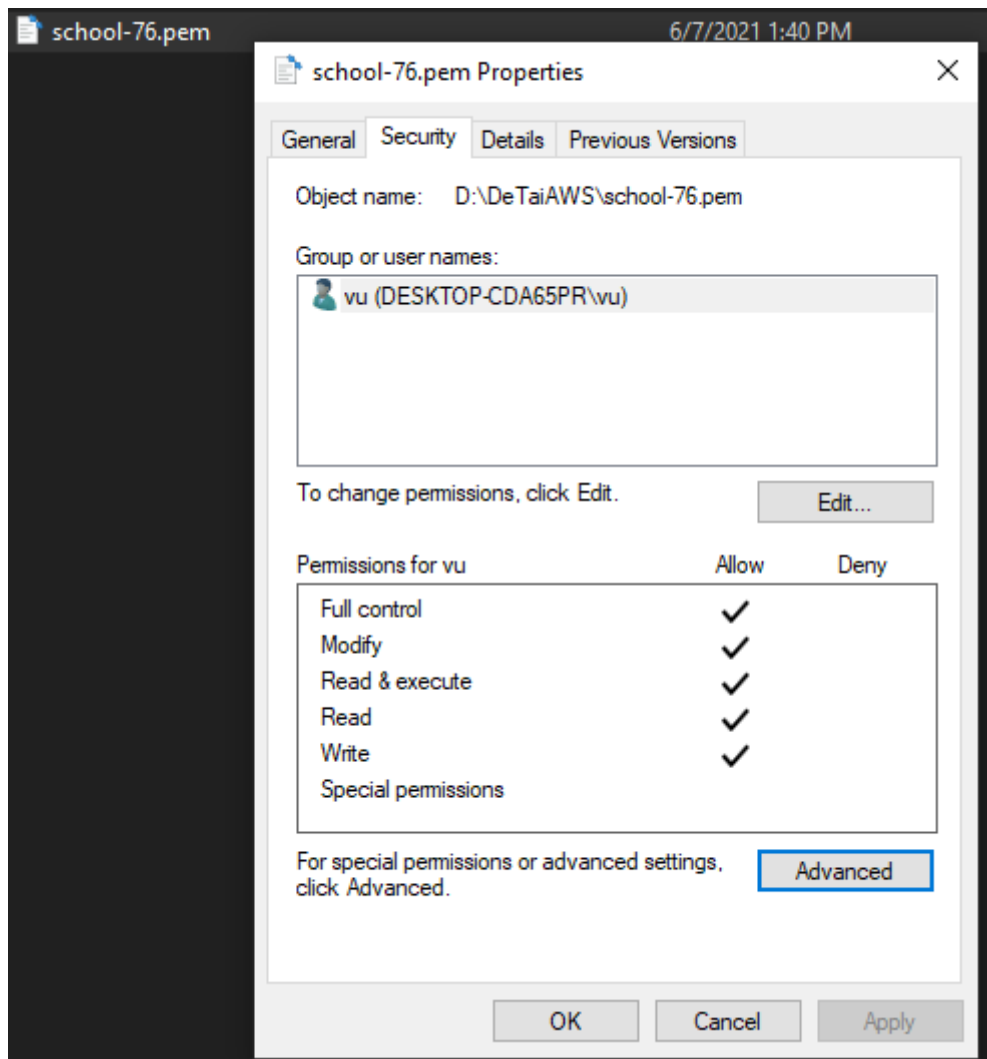
Output

Action Output

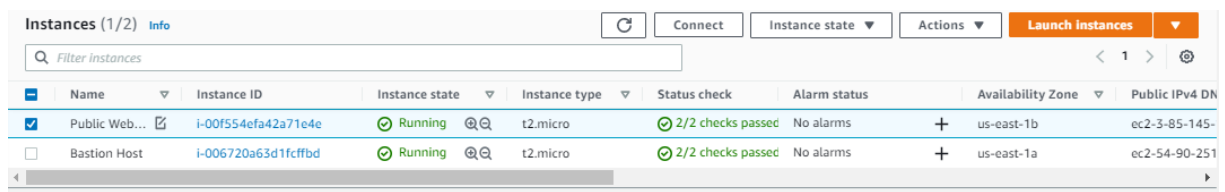
#	Time	Action	Message	Duration / Fetch
59	14:32:59	ALTER TABLE 'cities' MODIFY 'id' int(11) NOT NULL AUTO_INCREM...	47576 row(s) affected, 1 warning(s): 1681 Integer display width is depreca...	1.000 sec
60	14:33:00	ALTER TABLE 'countries' MODIFY 'id' int(11) NOT NULL AUTO_INCR...	246 row(s) affected, 1 warning(s): 1681 Integer display width is depreca...	0.453 sec
61	14:33:01	ALTER TABLE 'registration' MODIFY 'id' int(11) NOT NULL AUTO_INCR...	1 row(s) affected, 1 warning(s): 1681 Integer display width is deprecated a...	0.453 sec
62	14:33:02	ALTER TABLE 'session' MODIFY 'id' int(11) NOT NULL AUTO_INCRE...	9 row(s) affected, 1 warning(s): 1681 Integer display width is deprecated a...	0.453 sec
63	14:33:02	ALTER TABLE 'states' MODIFY 'id' int(11) NOT NULL AUTO_INCREM...	4119 row(s) affected, 1 warning(s): 1681 Integer display width is deprecate...	0.515 sec
64	14:33:03	ALTER TABLE 'subject' MODIFY 'subid' int(11) NOT NULL AUTO_INCR...	5 row(s) affected, 1 warning(s): 1681 Integer display width is deprecated a...	0.453 sec
65	14:33:04	ALTER TABLE 'tbl_course' MODIFY 'cid' int(11) NOT NULL AUTO_INCR...	7 row(s) affected, 1 warning(s): 1681 Integer display width is deprecated a...	0.454 sec
66	14:33:05	ALTER TABLE 'tbl_login' MODIFY 'id' int(11) NOT NULL AUTO_INCR...	1 row(s) affected, 1 warning(s): 1681 Integer display width is deprecated a...	0.438 sec
67	14:33:05	COMMIT	0 row(s) affected	0.281 sec
68	14:33:06	/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_S...	0 row(s) affected	0.313 sec
69	14:33:06	/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_S...	0 row(s) affected	0.281 sec
70	14:33:06	/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CON...	0 row(s) affected	0.297 sec
71	14:33:21	SELECT * FROM schoolmanagement.cities LIMIT 0, 1000	1000 row(s) returned	0.578 sec / 0.000 sec

1.10. Kết nối SSH bằng CMD truy cập vào EC2

Chuyển quyền sử dụng file key pair thành user windows đang sử dụng



Click vào connect trong trang EC2



EC2 > Instances > i-00f554efa42a71e4e > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-00f554efa42a71e4e using any of these options

EC2 Instance Connect	Session Manager	SSH client	EC2 Serial Console
----------------------	-----------------	-------------------	--------------------

Instance ID
i-00f554efa42a71e4e

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is school-76.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 school-76.pem
4. Connect to your instance using its Public DNS:
ec2-3-85-145-151.compute-1.amazonaws.com

Example:

```
ssh -i "school-76.pem" ec2-user@ec2-3-85-145-151.compute-1.amazonaws.com
```

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel

```
PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE

PS D:\DeTaiAWS> ssh -i "school-76.pem" ec2-user@ec2-3-85-145-151.compute-1.amazonaws.com
The authenticity of host 'ec2-3-85-145-151.compute-1.amazonaws.com (3.85.145.151)' can't be established.
ECDSA key fingerprint is SHA256:GZBddVmPu7xwUFG0ZU1ADg9sfTO+tfQAPopFG09H1LM.
Are you sure you want to continue connecting (yes/no/[fingerprint])?yes
Warning: Permanently added 'ec2-3-85-145-151.compute-1.amazonaws.com,3.85.145.151' (ECDSA) to the list of known hosts.

  _| _|_ )
  _| ( /  Amazon Linux 2 AMI
  _|\_|_|_|

https://aws.amazon.com/amazon-linux-2/
6 package(s) needed for security, out of 18 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-2-170 ~]$
```

Thiết lập quyền sử dụng folder /var/www

1. Add your user (in this case, ec2-user) to the apache group.

```
[ec2-user ~]$ sudo usermod -a -G apache ec2-user
```

2. Log out and then log back in again to pick up the new group, and then verify your membership.

- a. Log out (use the **exit** command or close the terminal window):

```
[ec2-user ~]$ exit
```


- b. To verify your membership in the `apache` group, reconnect to your instance, and then run the following command:

```
[ec2-user ~]$ groups
```

```
ec2-user adm wheel apache systemd-journal
```

3. Change the group ownership of `/var/www` and its contents to the `apache` group.

```
[ec2-user ~]$ sudo chown -R ec2-user:apache /var/www
```

4. To add group write permissions and to set the group ID on future subdirectories, change the directory permissions of `/var/www` and its subdirectories.

```
[ec2-user ~]$ sudo chmod 2775 /var/www && find /var/www -type d -exec sudo chmod 2775 {} \;
```

5. To add group write permissions, recursively change the file permissions of `/var/www` and its subdirectories:

```
[ec2-user ~]$ find /var/www -type f -exec sudo chmod 0664 {} \;
```

```
[ec2-user@ip-10-0-2-170 ~]$ sudo usermod -a -G apache ec2-user
[ec2-user@ip-10-0-2-170 ~]$ exit
logout
Connection to ec2-3-85-145-151.compute-1.amazonaws.com closed.
PS D:\DeTaiAW5> ssh -i "school-76.pem" ec2-user@ec2-3-85-145-151.compute-1.amazonaws.com
Last login: Mon Jun  7 07:01:28 2021 from 171.249.91.228

  _ | _ | _ )
  _ | ( _ | /  Amazon Linux 2 AMI
  ___\___\___|

https://aws.amazon.com/amazon-linux-2/
6 package(s) needed for security, out of 18 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-2-170 ~]$ sudo chown -R ec2-user:apache /var/www
[ec2-user@ip-10-0-2-170 ~]$ sudo chmod 2775 /var/www && find /var/www -type d -exec sudo chmod 2775 {} \;
[ec2-user@ip-10-0-2-170 ~]$ find /var/www -type f -exec sudo chmod 0664 {} \;
[ec2-user@ip-10-0-2-170 ~]$
```

1.11. Download Project School PHP – MySQL

Dùng git để Download Project School PHP – MySQL (Project không dùng cho mục đích thương mại, chỉ dùng cho mục đích giáo dục, nghiên cứu)

`git clone https://github.com/Vu-Nguyen2201/VPC-Webserver-AWS.git`

```
[ec2-user@ip-10-0-2-170 html]$ git clone https://github.com/Vu-Nguyen2201/VPC-Webserver-AWS.git
Cloning into 'VPC-Webserver-AWS'...
remote: Enumerating objects: 1010, done.
remote: Counting objects: 100% (1010/1010), done.
remote: Compressing objects: 100% (835/835), done.
remote: Total 1010 (delta 119), reused 985 (delta 111), pack-reused 0
Receiving objects: 100% (1010/1010), 2.90 MiB | 20.65 MiB/s, done.
Resolving deltas: 100% (119/119), done.
[ec2-user@ip-10-0-2-170 html]$ ls
info.php  VPC-Webserver-AWS
```

`mv VPC-Webserver-AWS/schoolmanagement schoolmanagement`

`mv VPC-Webserver-AWS/tictactoe tictactoe`

```
[ec2-user@ip-10-0-2-170 html]$ mv VPC-Webserver-AWS/schoolmanagement schoolmanagement
[ec2-user@ip-10-0-2-170 html]$ ls
info.php schoolmanagement VPC-Webserver-AWS
[ec2-user@ip-10-0-2-170 html]$ mv VPC-Webserver-AWS/tictactoe tictactoe
[ec2-user@ip-10-0-2-170 html]$ ls
info.php schoolmanagement tictactoe VPC-Webserver-AWS
[ec2-user@ip-10-0-2-170 html]$
```

Chỉnh lại hostname, username, password, database

```
GNU nano 2.9.8 Database.php

<?php
class Database {
    private $connection;
    private static $instance; //The single instance
    private $host = "database-1.ch9ko7w2w007.us-east-1.rds.amazonaws.com";
    private $username = "admin";
    private $password = "lab-password";
    private $database = "schoolmanagement";
    private $port = 3306;
    /*
    Get an instance of the Database
    @return Instance
    */
    public static function getInstance() {
        if(!self::$instance) { // If no instance then make one
            self::$instance = new self();
        }
    }
}
```

[Read 39 lines (Converted from DOS format)]

Get Help Write Out Where Is Cut Text Justify Cur Pos Undo Mark Text
Exit Read File Replace Uncut Text To Spell Go To Line Redo Copy Text

```
GNU nano 2.9.8 dbcontroller.php Modified

<?php
$DB_host = "database-1.ch9ko7w2w007.us-east-1.rds.amazonaws.com";
$DB_user = "admin";
$DB_pass = "lab-password";
$DB_name = "schoolmanagement";
try
{
    $DB_con = new PDO("mysql:host={$DB_host};dbname={$DB_name};port=3306", $DB_user, $DB_pass);
    $DB_con->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
}
catch(PDOException $e)
{
    $e->getMessage();
}
?>
```

Get Help Write Out Where Is Cut Text Justify Cur Pos Undo Mark Text
Exit Read File Replace Uncut Text To Spell Go To Line Redo Copy Text

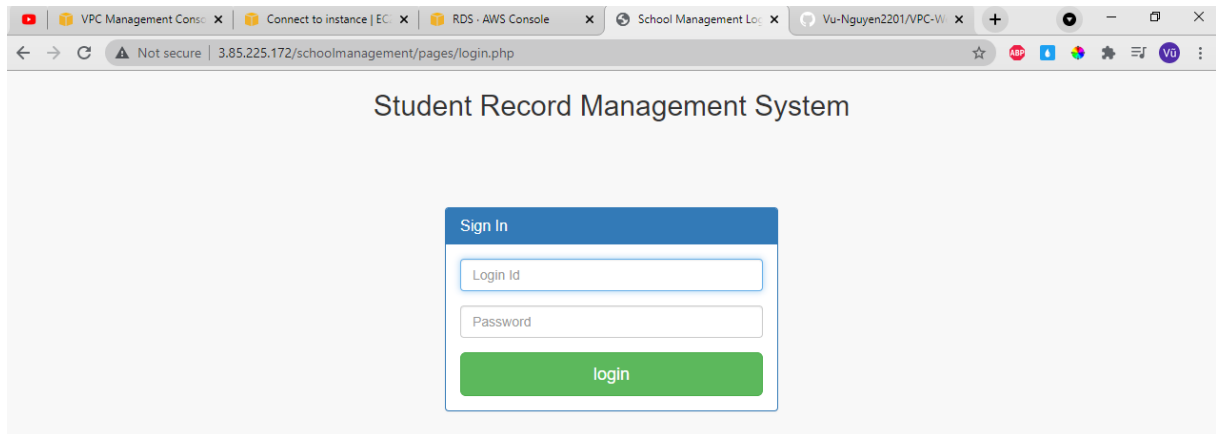
```
GNU nano 2.9.8 course_availability.php Modified

<?php
$dbuser="admin";
$dbpass="lab-password";
$host="database-1.ch9ko7w2w007.us-east-1.rds.amazonaws.com";
$dbname = "schoolmanagement";
$mysqli = new mysqli($host, $dbuser, $dbpass, $dbname);
if(!empty($_POST['cshort'])){
    $cshort=$_POST['cshort'];
    $result = "SELECT count(*) FROM tbl_course WHERE cshort=?";
    $stmt = $mysqli->prepare($result);
    $stmt->bind_param('s', $cshort);
    $stmt->execute();
    $stmt->bind_result($count);
    $stmt->fetch();
    $stmt->close();
    if($count>0)
        echo "<span style='color:red'> Course Short Name Already Exist .</span>";
}
```

Get Help Write Out Where Is Cut Text Justify Cur Pos Undo Mark Text
Exit Read File Replace Uncut Text To Spell Go To Line Redo Copy Text

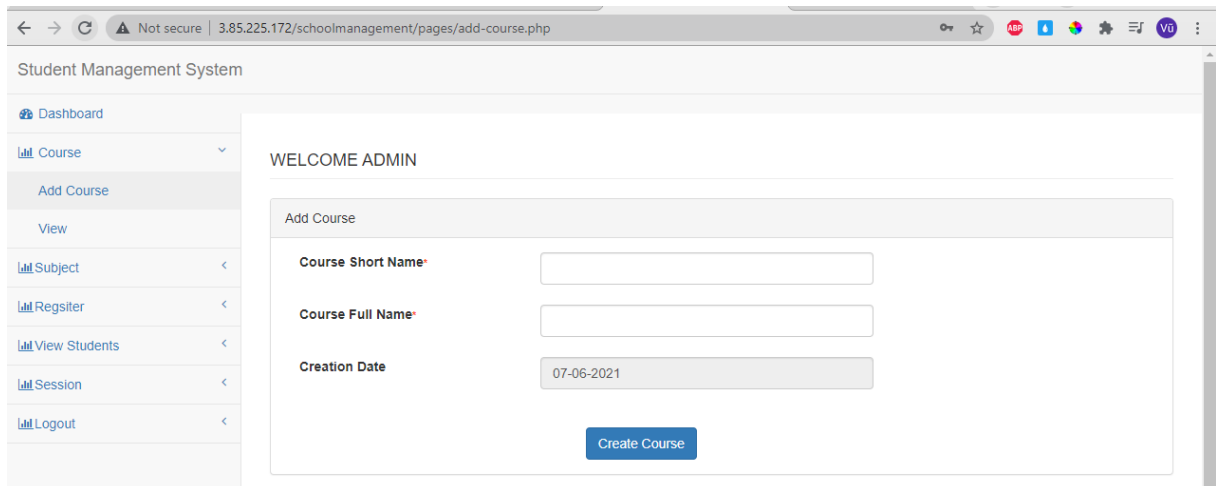
1.12. Kết quả Demo

Login admin/admin

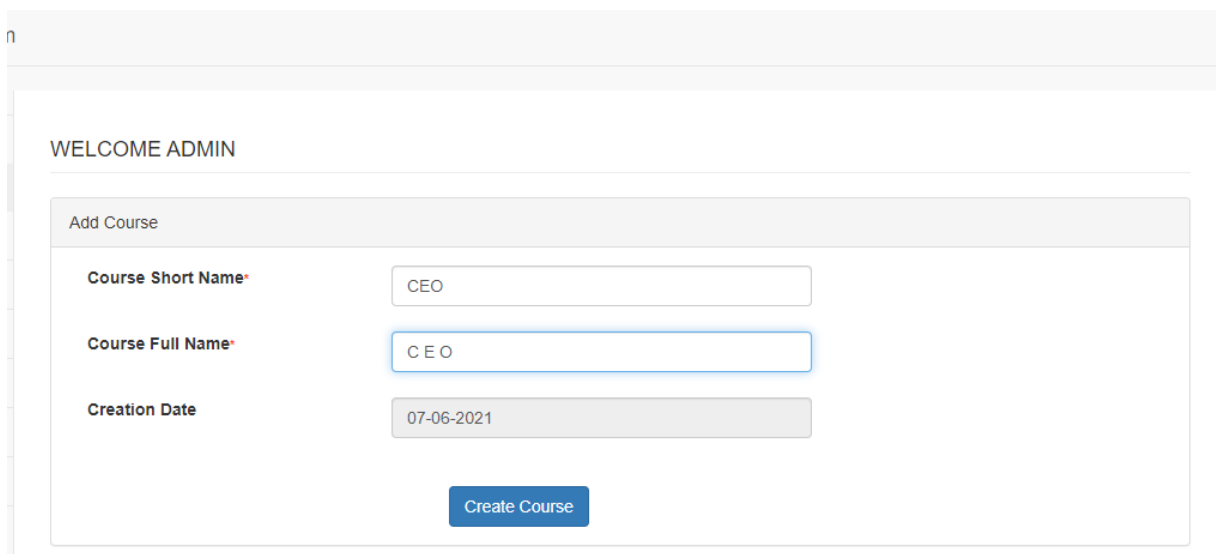


The screenshot shows a web browser window with the URL `3.85.225.172/schoolmanagement/pages/login.php`. The page title is "Student Record Management System". In the center, there is a "Sign In" form with two input fields: "Login Id" and "Password". Below these fields is a green button labeled "login".

Login succes



The screenshot shows the "Student Management System" dashboard. On the left is a sidebar menu with options: Dashboard, Course (expanded), Add Course, View, Subject, Register, View Students, Session, and Logout. The main content area displays "WELCOME ADMIN" and an "Add Course" form. The form has three fields: "Course Short Name" (empty), "Course Full Name" (empty), and "Creation Date" (pre-filled with "07-06-2021"). A blue "Create Course" button is at the bottom of the form.



This screenshot shows the "Add Course" form with data entered. The "Course Short Name" field contains "CEO", the "Course Full Name" field contains "C E O", and the "Creation Date" field remains "07-06-2021". The "Create Course" button is still visible at the bottom.

3.85.225.172 says

Course Added Successfully

OK

WELCOME ADMIN

View Course

Show 10 entries

Search:

S No	Short Name	Full Name	Created Date	Action
1	M.C.A.	MASTER OF COMPUTER APPLICATION	11-04-2016	Edit Delete
2	M.S.C	MASTER OF SCIENCE	11-04-2016	Edit Delete
3	B.COM	BACHELOR OF COMMERCE	12-04-2016	Edit Delete
4	B.TECH	BACHELOR OF TECHNOLOGY	12-04-2016	Edit Delete
5	M.B.A	MASTER OF BUSINESS ADMINISTRATION	17-04-2016	Edit Delete
6	B.A.	BACHELOR OF ARTS	27-05-2019	Edit Delete
7	M.TECH	MASTER OF TECHNOLOGY	27-05-2019	Edit Delete
8	CEO	C E O	07-06-2021	Edit Delete

Showing 1 to 8 of 8 entries

Previous 1 Next

2. DynamoDB

Project 2 – Game đánh caro chạy trên Flask Framework (Python) và sử dụng DynamoDB

Trò chơi Tic-Tac-Toe là một ứng dụng web ví dụ được xây dựng trên Amazon DynamoDB. Ứng dụng sử dụng AWS SDK cho Python (Boto) để thực hiện các lệnh gọi DynamoDB cần thiết để lưu Game Data trong bảng DynamoDB và Flask framework web Python để minh họa sự phát triển ứng dụng end-to-end trong DynamoDB, bao gồm cách lập mô hình dữ liệu.

1.1. Cài đặt python và các thư viện cần thiết

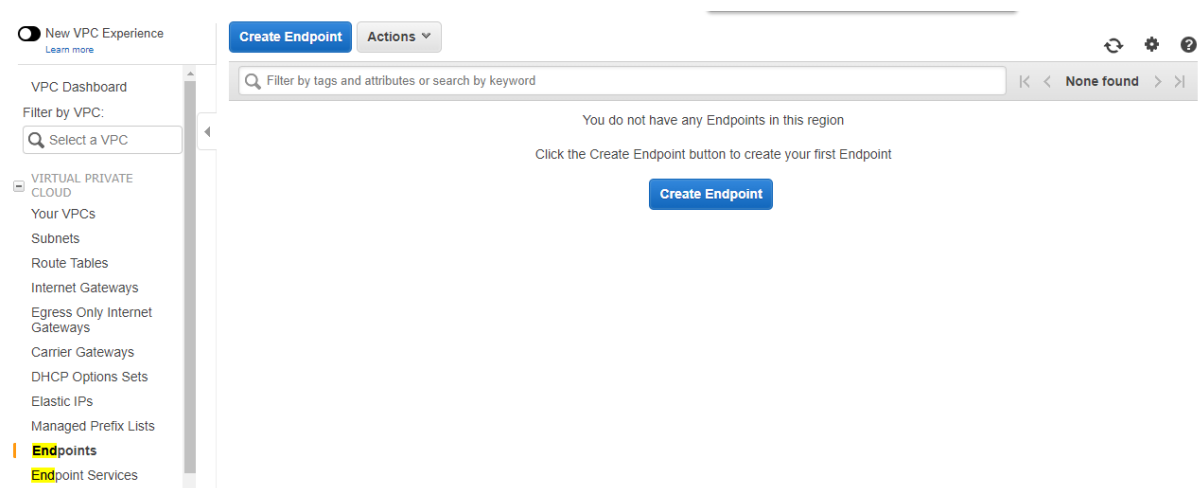
`sudo amazon-linux-extras install python3`

```
[ec2-user@ip-10-0-2-136 config]$ python3 --version
Python 3.7.9
[ec2-user@ip-10-0-2-136 config]$
```

`sudo python3 -m pip install Flask boto configparser`

`export PYTHONPATH=/usr/local/lib/python3.7/site-packages`

1.2. Tạo Endpoint DynamoDB



Create Endpoint

A VPC endpoint enables you to securely connect your VPC to another service. There are three types of VPC endpoints – Interface endpoints, Gateway Load Balancer endpoints, and gateway endpoints. Interface endpoints and Gateway Load Balancer endpoints are powered by AWS PrivateLink, and use an elastic network interface (ENI) as an entry point for traffic destined to the service. Interface endpoints are typically accessed using the public or private DNS name associated with the service, while gateway endpoints and Gateway Load Balancer endpoints serve as a target for a route in your route table for traffic destined for the service.

- Service category
- ☒ AWS services
 - ☐ Find service by name
 - ☐ Your AWS Marketplace services

Service Name com.amazonaws.ap-southeast-1.dynamodb ⓘ

Add filter

Service Name	Owner	Type
<input checked="" type="radio"/> com.amazonaws.ap-southeast-1.dynamodb	amazon	Gateway

VPC* vpc-0caee1571e65ccd02 ⓘ ⓘ

Configure route tables A rule with destination pl-67a5400e (com.amazonaws.ap-southeast-1.dynamodb) and a target with this endpoints' ID (e.g. vpce-12345678) will be added to the route tables you select below.

Subnets associated with selected route tables will be able to access this endpoint.

rtb-0acc0681432ab3590 ⓘ

	Route Table ID	Main	Associated Subnets
<input type="checkbox"/>	rtb-02ad91c3c735fcd41	Yes	subnet-0d0a1d6cef13e258 Public Subnet 2 subnet-0eabb74615cbff515 Public Subnet 1
<input checked="" type="checkbox"/>	rtb-0acc0681432ab3590	No	2 subnets



Warning

When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS service in the same region will be private IP addresses, not public IP addresses. Existing connections from your affected subnets to the AWS service that use public IP addresses may be dropped. Ensure that you don't have critical tasks running when you create or modify an endpoint.

- Policy* ☒ Full Access - Allow access by any user or service within the VPC using credentials from any AWS accounts to any resources in this AWS service. All policies — IAM user policies, VPC endpoint policies, and AWS service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed. ⓘ
- ☐ Custom

Use the [policy creation tool](#) to generate a policy, then paste the generated policy below.

```
{
  "Statement": [
    {
      "Action": "dynamodb:*",
      "Effect": "Allow",
      "Resource": "dynamodb:*",
      "Principal": "*"
    }
  ]
}
```

Key (128 characters maximum)	Value (256 characters maximum)
------------------------------	--------------------------------

This resource currently has no tags

Add Tag 50 remaining (Up to 50 tags maximum)

Cancel Create endpoint

Filter by tags and attributes or search by keyword

1 to 1 of 1

Name	Endpoint ID	VPC ID	Service name	Endpoint type	Status	Creation time	Network Inte
	vpce-08fde611aa6...	vpc-0b71855a5ba...	com.amazonaws.us-east-1.dyn...	Gateway	available	June 7, 2021 at 2:58:14 PM UTC+7	-

Endpoint: vpce-08fde611aa61a590b

Details | Route Tables | Policy | Tags

Endpoint ID: vpce-08fde611aa61a590b
Status: available
Creation time: June 7, 2021 at 2:58:14 PM UTC+7
Endpoint type: Gateway
Private DNS names enabled: false

VPC ID: vpc-0b71855a5ba8307a1 | School VPC
Status message
Service name: com.amazonaws.us-east-1.dynamodb
DNS names

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (3)

Filter routes

Both

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-08c2bf86f0801d9f5	Active	No
pl-02cd2c6b	vpce-08d6effb32c4539a8	Active	No

1.3. Thiết lập Security Group cho EC2 đã tạo ở VPC

Inbound security group rules successfully modified on security group (sg-05c0552808284b90b | launch-wizard-1)

Details

Security Groups (1/7) Info

Filter security groups

Name	Security group ID	Security group name	VPC ID	Description	Owner
-	sg-01d117f8ab5819daa	Ec2SecurityGroup	vpc-0ed97255d6b3e228b	VPC Security Group	271382871042
-	sg-01e7876a453db4d6a	default	vpc-0ed97255d6b3e228b	default VPC security gr...	271382871042
Private Security Gr...	sg-051770b3ec32193cc	Private Security	vpc-0b71855a5ba8307a1	Private Security	271382871042
-	sg-06bdc9a40df33d584	default	vpc-0d48564b8995e1f4c	default VPC security gr...	271382871042
Public Security Group	sg-07bb07097a53ed16c	Public Security	vpc-0b71855a5ba8307a1	Public Security	271382871042

sg-05c0552808284b90b - launch-wizard-1

Details | Inbound rules | Outbound rules | Tags

Inbound rules (5)

Edit inbound rules

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	0.0.0.0/0	-
HTTP	TCP	80	::/0	-
All traffic	All	All	pl-02cd2c6b (com.amazonaws.us-east-1.dynamodb)	-
SSH	TCP	22	0.0.0.0/0	-
Custom TCP	TCP	5000	0.0.0.0/0	-

1.4. Git Clone TicTacToe (đã tải ở VPC)

```
[ec2-user@ip-10-0-2-147 html]$ ls
info.php  schoolmanagement  tictactoe  VPC-Webserver-AWS
[ec2-user@ip-10-0-2-147 html]$
```

1.5. Thiết lập key kết nối

Credentials

Cloud Access

AWS CLI:

Show

Cloud Labs

Remaining session time: 01:45:25 (106 minutes)

Session started at: 2021-06-06T22:42:01-0700

Session to end at: 2021-06-07T02:48:19-0700

Accumulated lab time: 2 days 00:36:22 (2917 minutes)

ips -- public:54.90.251.125, private:10.0.0.129

SSH key

Show

Download PEM

Download PPK

AWS SSO

Download URL

SecretKey	+/La+Ujeu/uSapakxNIMqoSfumIZnk/rhLdiOhZN
Region	us-east-1
AccessKey	AKIAT6L5N7QBGMN067Y4

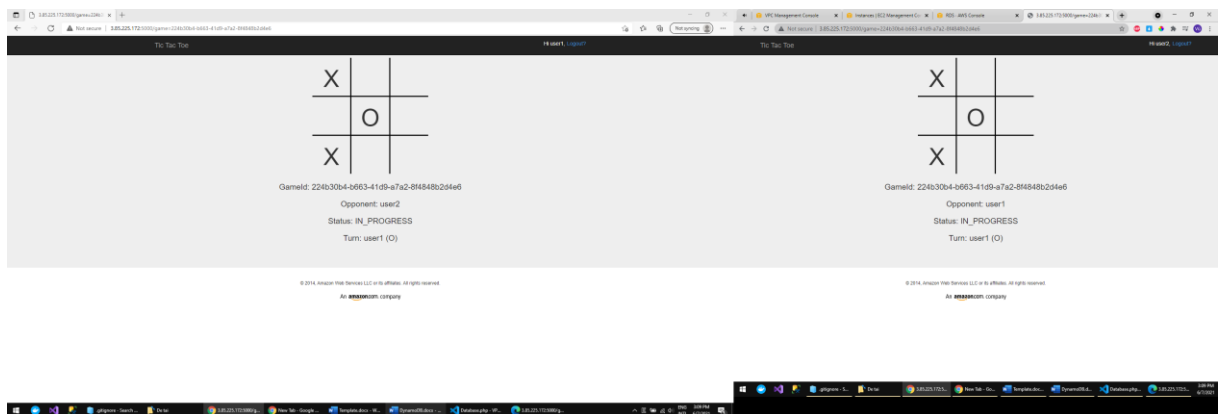
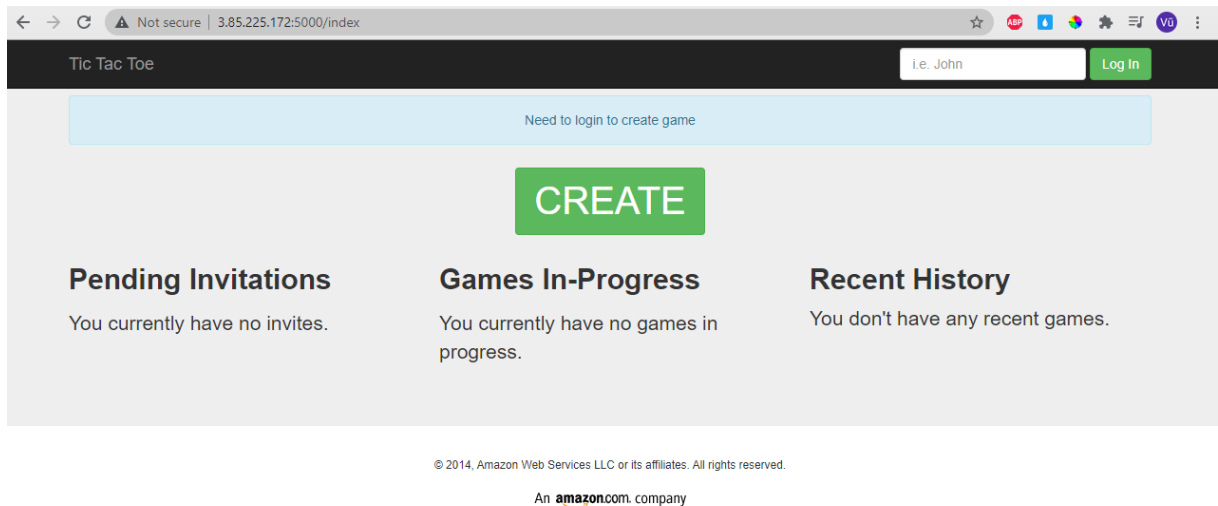
aws configure

```
[ec2-user@ip-10-0-2-147 html]$ aws configure
AWS Access Key ID [None]: AKIAT6L5N7QBGMN067Y4
AWS Secret Access Key [None]: +/La+Ujeu/uSapakxNIMqoSfumIZnk/rhLdiOhZN
Default region name [None]: us-east-1
Default output format [None]:
```

Thiết lập web.config

1.6. Chạy Flask Server

```
python3 application.py --serverPort 5000 --port 8000 --config
/var/www/htmltictactoe/web.config
```

Tạo Table DynamoDB thành công

```
[ec2-user@ip-10-0-2-147 ~]$ aws dynamodb list-tables
{
  "TableNames": [
    "Games"
  ]
}
[ec2-user@ip-10-0-2-147 ~]$
```

Phản kết luận

1. Kết quả đạt được

- Về mặt lý thuyết, hiểu được ý nghĩa của Cloud Computing, cấu trúc VPC, các thành phần network (route tables, network access controls, security groups)
- Nắm được cách thiết kế 1 kiến trúc AWS, cách triển khai, những khó khăn khi triển khai

2. Kết quả chưa đạt được

- Chưa tìm hiểu được cách sử dụng các dịch vụ load balancing, hệ phân tán

3. Hướng phát triển

- Xây dựng VPC chứa nhiều máy chủ, sử dụng load balancing

4. Tài liệu tham khảo

VPC - PHP – MySQL Web Services:

[Student Record System In php - PHPGurukul](#)

[Connect to your Linux instance using SSH - Amazon Elastic Compute Cloud](#)

[Tutorial: Install a LAMP web server on Amazon Linux 2 - Amazon Elastic Compute Cloud](#)

[Cách tạo Cơ sở dữ liệu MySQL – Amazon Web Services](#)

[Connect to Amazon RDS DB instance that's running MySQL using MySQL Workbench](#)

[Connect to a Private Amazon RDS MySQL DB Instance that Uses a Public EC2 Instance](#)

DynamoDB:

[AWS How to Configure a Private Network Environment for Amazon DynamoDB Using VPC Endpoints | AWS Database Blog](#)

[DynamoDB Example Application Using the AWS SDK for Python \(Boto\): Tic-Tac-Toe - Amazon DynamoDB](#)