

COS20019 - Cloud Computing Architecture

Assignment 2

Developing a highly available Photo Album website

Name: Pham Do Tien Phong

Student Id: 104189767

Link to the ELB album.php: <http://elb-assignment2-434376215.us-east-1.elb.amazonaws.com/photoalbum/album.php>

Link to the ELB photouploader.php: <http://elb-assignment2-434376215.us-east-1.elb.amazonaws.com/photoalbum/photouploader.php>

I. Introduction

Amazon Web Services (AWS) offers a wide range of services that can be used to create a reliable and highly accessible photo album website. By utilizing various AWS services for storage, hosting, databases, caching, load balancing, and monitoring, we can develop a photo album website with enhanced capabilities compared to previous assignments.

II. Implementation

1. Create VPC

First of all, I need to create a new VPC for this assignment

_ Name: PPhamVPC2

_ Region: us-east-1

_ AZ : I assigned subnets in 2 different AZ (Public subnet 1.2 and Private subnet 1.2 in us-east-1a & Public subnet 2.2 and Private subnet 2.2 in us-east-1b)

_ Route table :

. I create 2 route table beside the default route table

+ *RouteTable2-Public* is created to associate with 2 public subnets as well as routes to Internet Gateway

(*InternetGateway2*)

+ *RouteTable2-Private* is created to associate with 2 private subnets as well as routes to NAT Gateway (*NAT gateway2*)

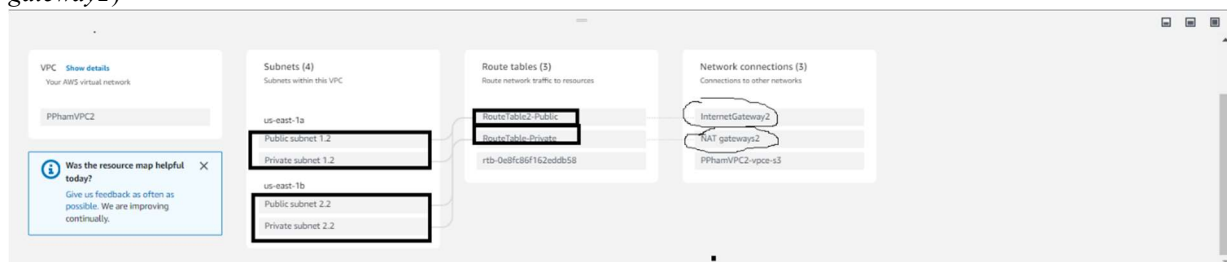


Figure 1: VPC resource map .

This is my resource map

2. Create Security Groups & Network ACLs

Secondly, I will create Security groups and Network ACLs to ensure security and accessibility to and from Web server

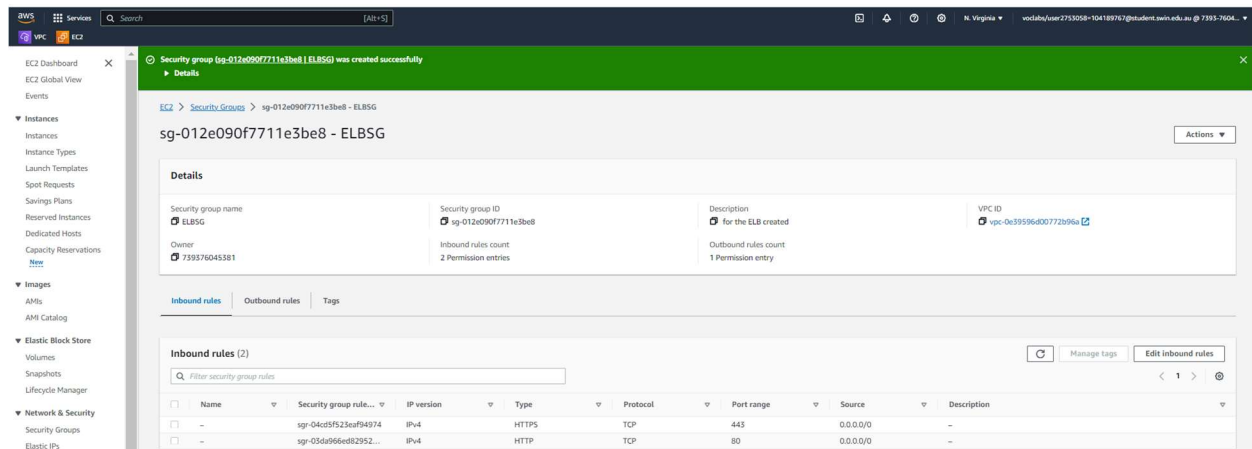


Figure 2: ELBSG security group

This is ELBSG allowing traffic for the web application from port 80 to port 443

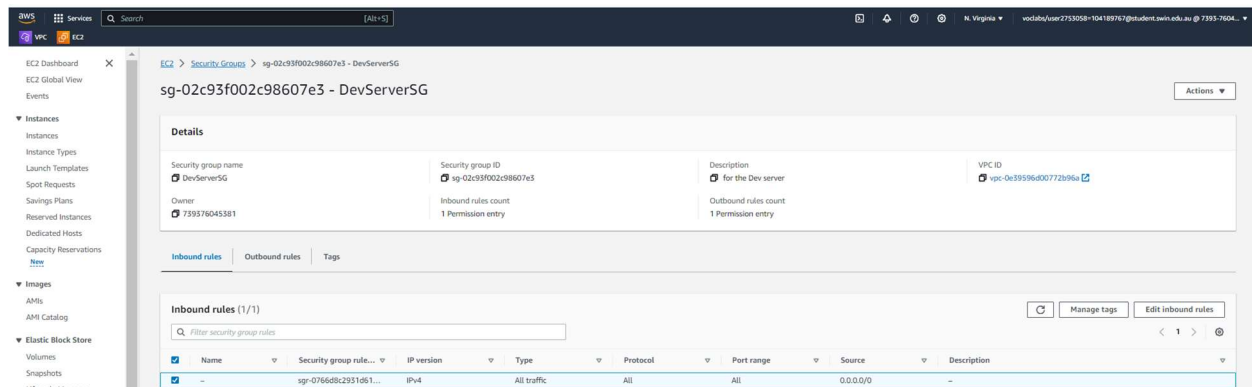


Figure 3: DevServerSG security group

This is DevServerSG can accept all traffic and SSH from port 22

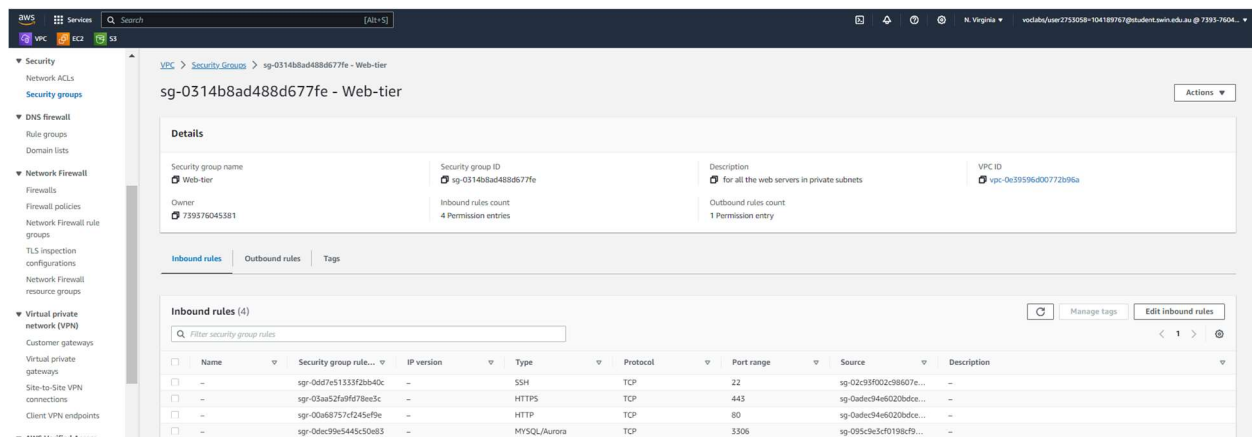


Figure 4: Web-tier security group

This is Web-tier (Security Group for Web server) allowing the traffic from the web application,SSH from port 22 and the DB security group.

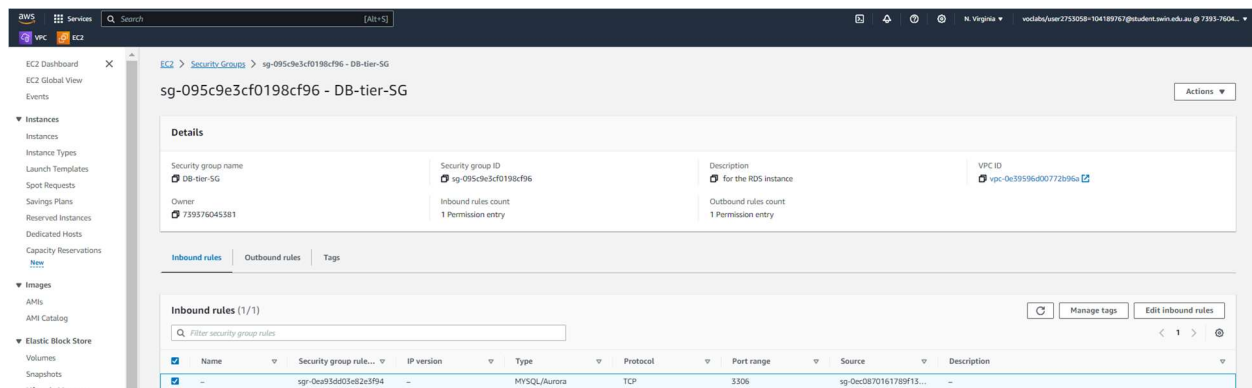


Figure 5: DB-tier-SG security group

This is DB-tier-SG, which just allows traffic from the port 3306 from the Web-tier security group above

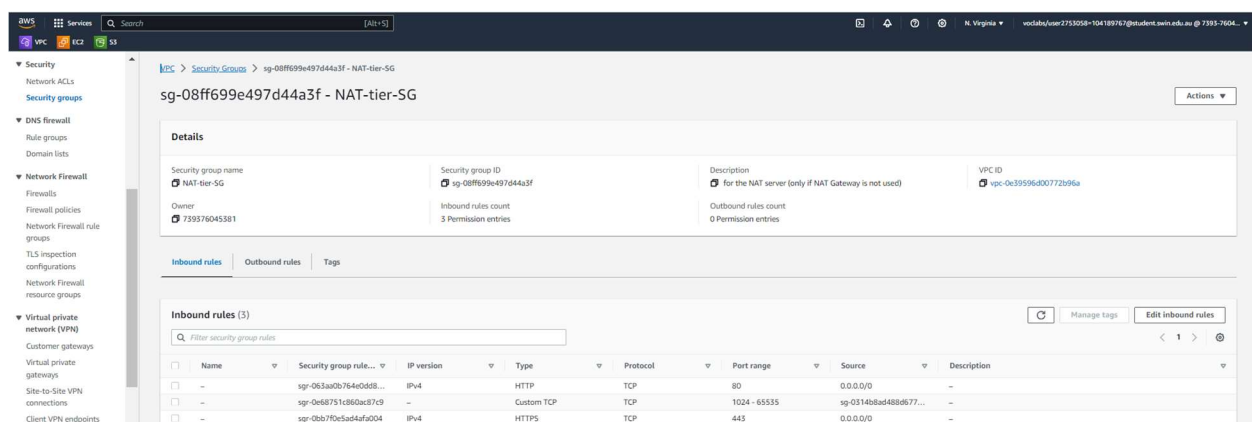


Figure 6: NAT-tier-SG security group

This is NAT-tier-SG that allow access the traffic from HTTP/HTTPs for the web application and traffic from the web server.

The next step is creating Network ACLs that is an additional security layer for the Web server. It will restrict DevServer from sending ICMP packet to the WebServer.

Inbound rules (5)

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All ICMP - IPv4	ICMP (1)	All	10.0.3.0/24	Deny
110	All ICMP - IPv4	ICMP (1)	All	10.0.4.0/24	Deny
120	All traffic	All	All	0.0.0.0/0	Allow
130	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Figure 7: Inbound rules

Outbound rules (5)

Filter outbound rules

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All ICMP - IPv4	ICMP (1)	All	10.0.3.0/24	Deny
110	All ICMP - IPv4	ICMP (1)	All	10.0.4.0/24	Deny
120	All traffic	All	All	0.0.0.0/0	Allow
130	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Figure 8: Outbound rules

3.Create & Configure NAT instance & EC2 instance

The next step is create NAT and EC2 instance

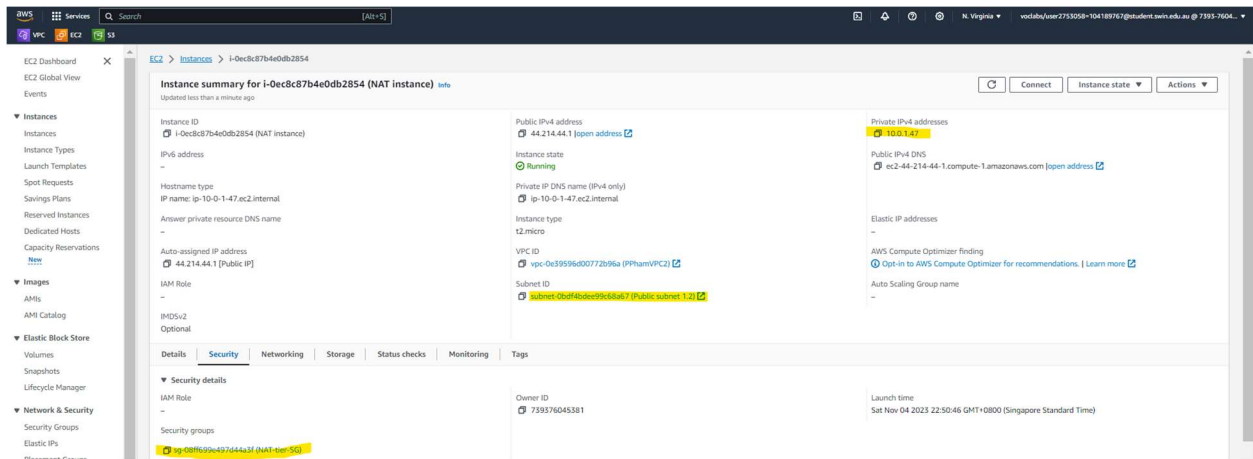


Figure 9: Information of NAT instance

I create NAT instance with Public Subnet 1.2 (10.0.1.47) and add security group into this instance (NAT-tier-SG)

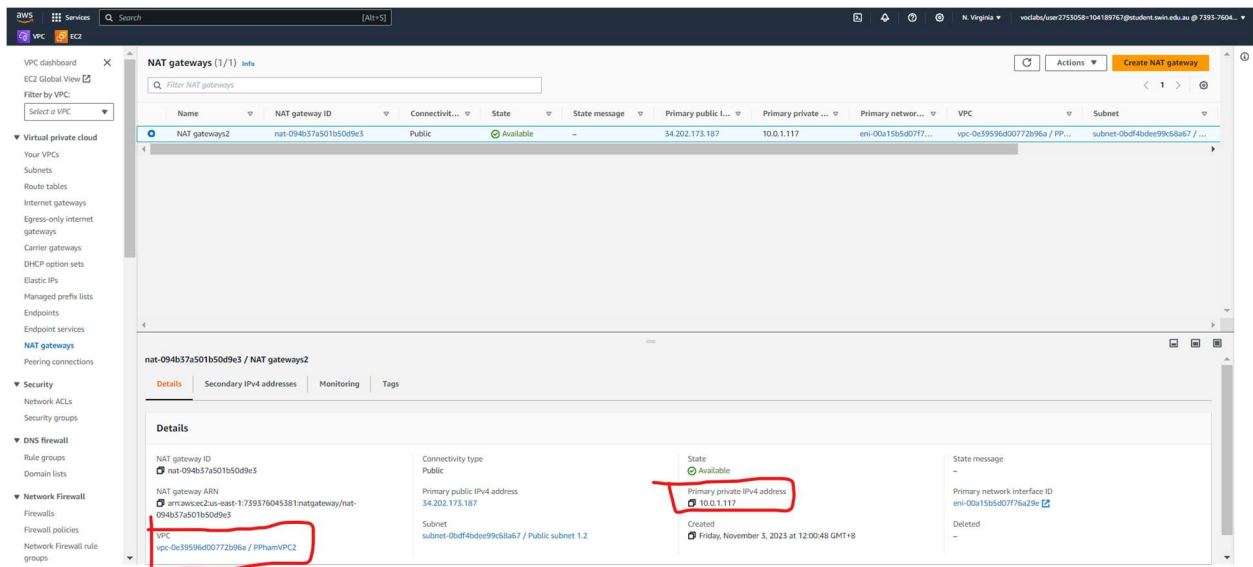


Figure 10: Information of NAT gateways

Configure NAT instance to NAT gateway , which will help private instances can communicate with public internet through NAT device

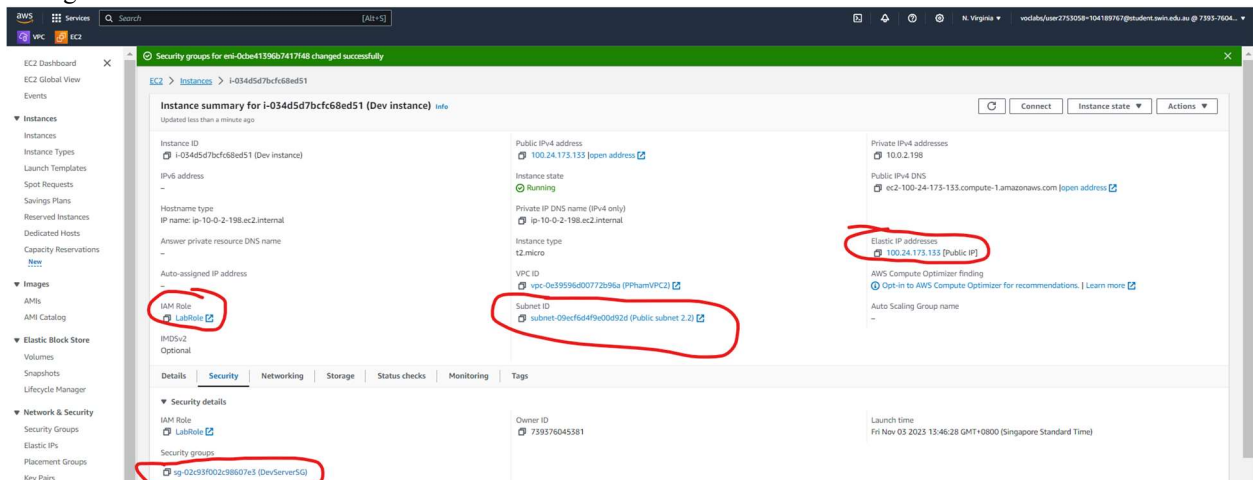


Figure 11: Information of Dev instance

I create Dev instance with public subnet 2.2 (10.0.2.198) , attach EIP (100.24.173.133) for having unchanged public IP address and assign IAM role (LabRole)

4.RDS Database

The following stage is that create a RDS database with the same steps I implemented in the assignment 1b

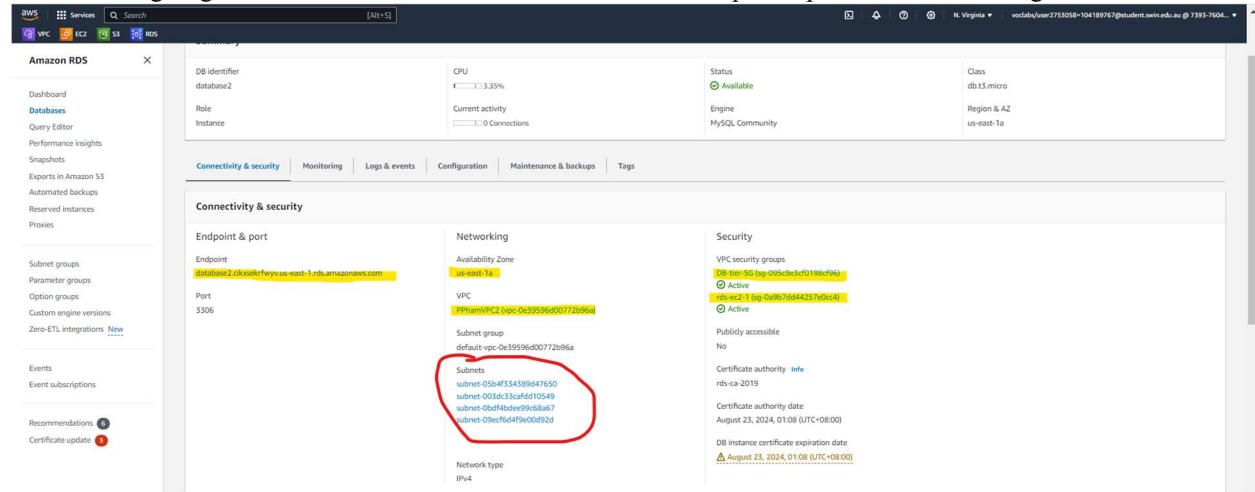


Figure 12: Information of database

I create the database (database2) and add security group for them (DB-tier-SG). There are 4 subnets connected to my database (2 public subnets and 2 private subnets)

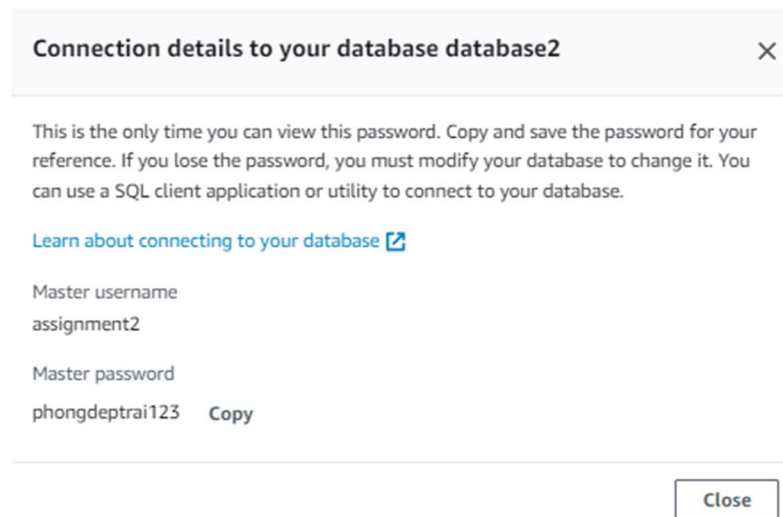


Figure 13: Connection details

- _ The username is : assignment2
- _ The password is : phongdeptrai123

```
constants.php
C:\Users\HP> HP > OneDrive - Swinburne University > Documents > Semester3 > CLOUD > Assignment2 > photoalbum > constants.php
44 */
45
46 // [ACTION REQUIRED] your full name
47 define('STUDENT_NAME', 'Pham Do Tien Phong');
48 // [ACTION REQUIRED] your Student ID
49 define('STUDENT_ID', '104189767');
50 // [ACTION REQUIRED] your tutorial session
51 define('TUTORIAL_SESSION', 'Saturday 1:00 PM');
52
53 // [ACTION REQUIRED] name of the S3 bucket that stores images
54 define('BUCKET_NAME', 'photoweb');
55 // [ACTION REQUIRED] region of the above bucket
56 define('REGION', 'us-east-1');
57 define('S3_BASE_URL', 'https://'.BUCKET_NAME.'.s3.amazonaws.com/');
58
59 // [ACTION REQUIRED] name of the database that stores photo meta-data (note that this is not the DB identifier of the RDS instance)
60 define('DB_NAME', 'photoalbum');
61 // [ACTION REQUIRED] endpoint of RDS instance
62 define('DB_ENDPOINT', 'database2.ciksekrfwy.us-east-1.rds.amazonaws.com');
63 // [ACTION REQUIRED] username of your RDS instance
64 define('DB_USERNAME', 'assignment2');
65 // [ACTION REQUIRED] password of your RDS instance
66 define('DB_PWD', 'phongdeptrai123');
67
68 // [ACTION REQUIRED] name of the DB table that stores photo's meta-data
69 define('DB_PHOTO_TABLE_NAME', 'photos');
70 // The table above has 5 columns:
71 // [ACTION REQUIRED] name of the column in the above table that stores photo's titles
72 define('DB_PHOTO_TITLE_COL_NAME', 'photo_title');
73 // [ACTION REQUIRED] name of the column in the above table that stores photo's descriptions
74 define('DB_PHOTO_DESCRIPTION_COL_NAME', 'description');
75 // [ACTION REQUIRED] name of the column in the above table that stores photo's creation dates
76 define('DB_PHOTO_CREATIONDATE_COL_NAME', 'creation_date');
77 // [ACTION REQUIRED] name of the column in the above table that stores photo's keywords
78 define('DB_PHOTO_KEYWORDS_COL_NAME', 'keywords');
79 // [ACTION REQUIRED] name of the column in the above table that stores photo's links in S3
80 define('DB_PHOTO_S3REFERENCE_COL_NAME', 's3_reference');
81
82 // [ACTION REQUIRED] name (ARN can also be used) of the Lambda function that is used to create thumbnails
83 define('LAMBDA_FUNC_THUMBNAILS_NAME', 'CreateThumbnail');
84
85 >>
```

Figure 14: Code of constant.php

This is the code I used in constant.php , the most important change is the enpoint of RDS instance to the endpoint of my database (*database2*)

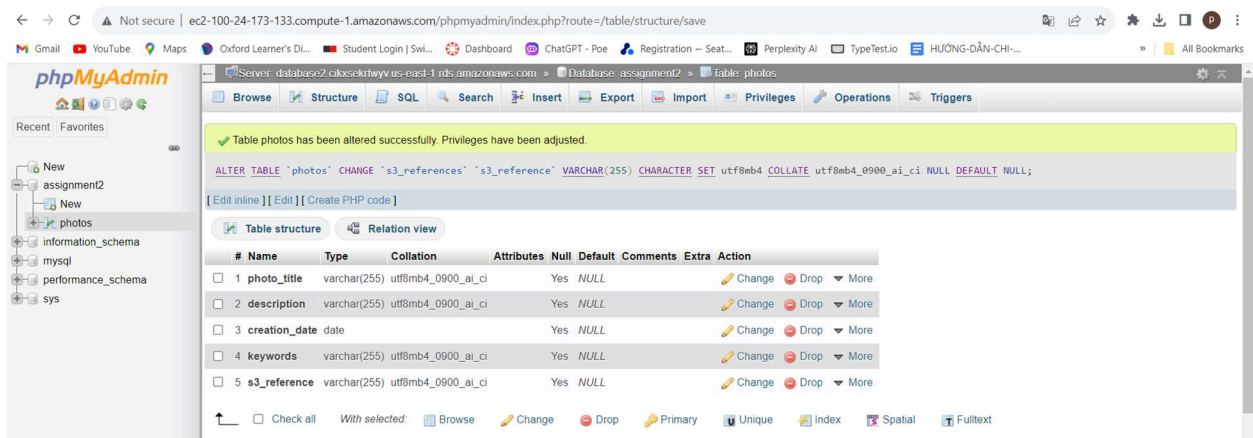


Figure 15: Create table in MySQL

I create MySQL table with this code

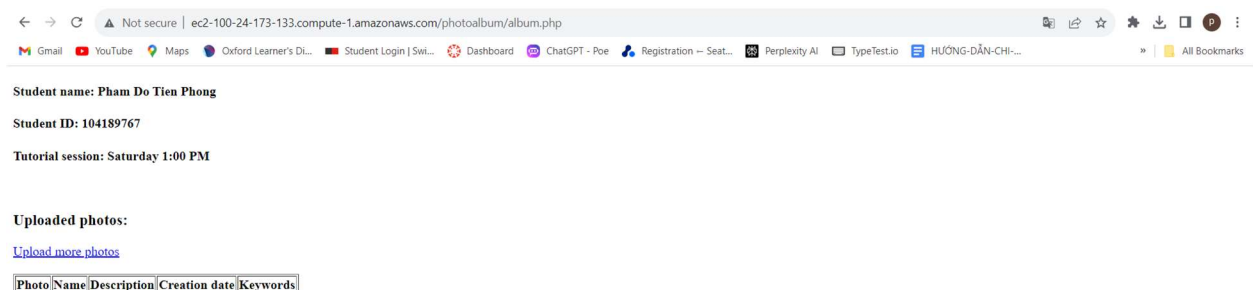


Figure 16: Default display of album.php

This is the default display of album.php

← → ↻ Not secure | ec2-100-24-173-133.compute-1.amazonaws.com/photoalbum/album.php

Gmail YouTube Maps Oxford Learner's Di... Student Login | Swi... Dashboard ChatGPT - Poe Registration -- Seat... Perplexity AI TypeTest.io HƯỚNG-DẪN-CHI... All Bookmarks

Student name: Pham Do Tien Phong
Student ID: 104189767
Tutorial session: Saturday 1:00 PM

Uploaded photos:

[Upload more photos](#)




Photo	Name	Description	Creation date	Keywords
	Phong Parents	They are my parents of Phong	2023-04-11	Parents, mom, dad
	Tien Phong is waiting	Tien Phong is waiting lucky things coming	2023-01-12	Tien Phong, waiting, luck
	Tien Phong outfit	Tien Phong is wearing mask	2022-12-23	Tien Phong, outfit, mask

Figure 17: display of album.php after adding and then , I add some photos for this album

← → ↻ Not secure | ec2-100-24-173-133.compute-1.amazonaws.c

Gmail YouTube Maps Oxford Learner's Di... Student Login | S

Photo uploader

Photo title:

Select a photo (Select PNG file for best result): 327595278_...37675_n.jpg

Description:

Date:

Keywords (comma-delimited, e.g. keyword1, keyword2, ...):

Figure 18: display of photouploader.php

I upload photo by photouploader.php

← → ↻ Not secure | ec2-100-24-173-133.compute-1.amazonaws.com/photoalbum/album.php

Gmail YouTube Maps Oxford Learner's Di... Student Login | Swi... Dashboard ChatGPT - Poe Registration -- Seat... Perplexity AI


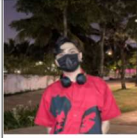



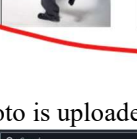
	Tien Phong is waiting	Tien Phong is waiting lucky things coming	2023-01-12	Tien Phong, waiting, luck
	Tien Phong outfit	Tien Phong is wearing mask	2022-12-23	Tien Phong, outfit, mask
	hybridge	Hybridge shirt	2018-03-18	hybridge, local brand , shirt
	Shoes	Converse Golf le flour	2022-11-22	Sneaker , Beige
	Einstein	Einstein	2001-01-01	Theory
	Hybridge pants	Hybridge 3 stripes pants	2023-02-02	Local brand , Fashion

Figure 19: photo uploaded

This photo is uploaded in album.php

AWS Services Search [Alt+Q]

Global vodafoneuser2753056@10418876@student.wmi.ac.at 7393-7604

Amazon S3

Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens
Dashboards
AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Objects (13)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

Find objects by prefix

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	326457057_1557729963571132_23526 29299584253131_n.jpg	jpg	November 4, 2023, 17:46:28 (UTC+08:00)	88.2 KB	Standard
<input type="checkbox"/>	327595278_1581813242232088_56642 1606606437675_n.jpg	jpg	November 5, 2023, 01:14:11 (UTC+08:00)	61.3 KB	Standard
<input type="checkbox"/>	download.jpg	jpg	November 5, 2023, 01:12:16 (UTC+08:00)	6.4 KB	Standard
<input type="checkbox"/>	H5.jpg	jpg	November 4, 2023, 23:15:08 (UTC+08:00)	836.1 KB	Standard
<input type="checkbox"/>	Table Selection Select H5.jpg	jpg	October 15, 2023, 20:17:15 (UTC+08:00)	175.9 KB	Standard
<input type="checkbox"/>	326457057_1557729963571132_23526 29299584253131_n.jpg	jpg	November 4, 2023, 17:46:30 (UTC+08:00)	29.4 KB	Standard
<input type="checkbox"/>	resized-327595278_1581813242232088_56642 1606606437675_n.jpg	jpg	November 5, 2023, 01:14:12 (UTC+08:00)	17.9 KB	Standard
<input type="checkbox"/>	resized-download.jpg	jpg	November 5, 2023, 01:12:18 (UTC+08:00)	3.3 KB	Standard
<input type="checkbox"/>	resized-H5.jpg	jpg	November 4, 2023, 23:15:13 (UTC+08:00)	65.6 KB	Standard
<input type="checkbox"/>	resized-TienPhong1.jpg	jpg	November 4, 2023, 17:46:26 (UTC+08:00)	4.2 KB	Standard
<input type="checkbox"/>	resized-TienPhong2.jpg	jpg	November 4, 2023, 22:53:56 (UTC+08:00)	6.3 KB	Standard
<input type="checkbox"/>	TienPhong1.jpg	jpg	October 15, 2023, 19:19:46 (UTC+08:00)	14.2 KB	Standard
<input type="checkbox"/>	TienPhong2.jpg	jpg	October 15, 2023, 19:19:47 (UTC+08:00)	21.7 KB	Standard

Figure 20: S3 bucket display

And then , the S3 bucket will have these images files

5.Create Load Balacing

and then, I have to create Elastic Load Balancing

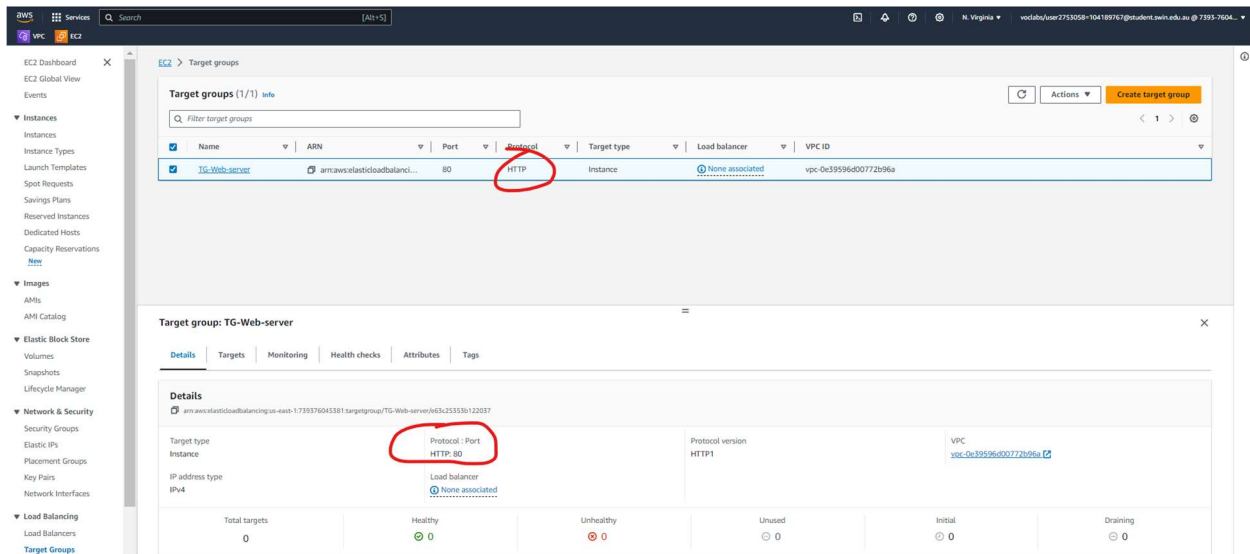


Figure 21: Information of target groups

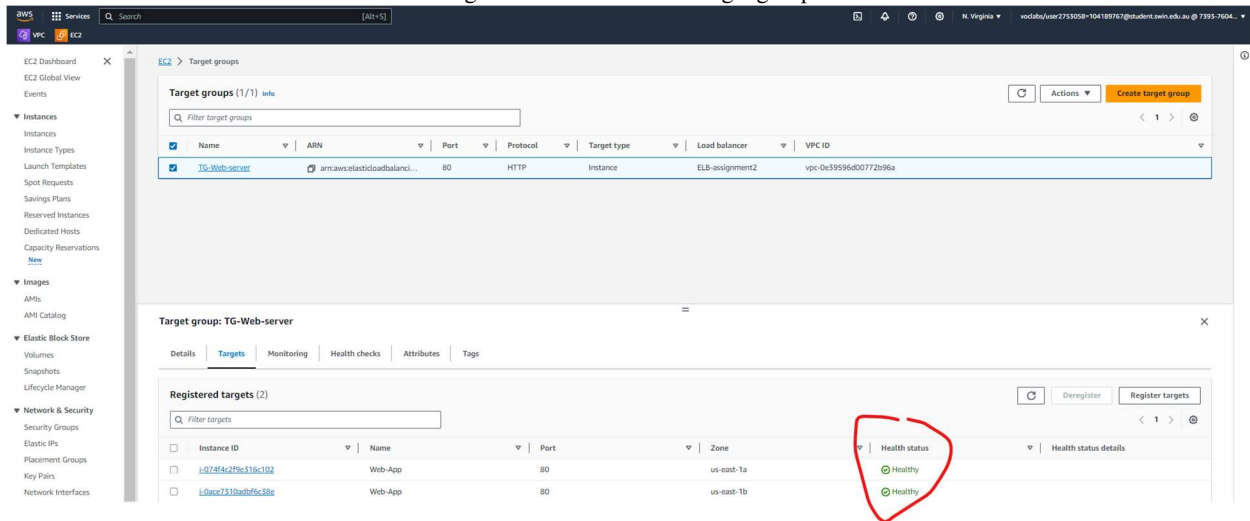


Figure 22: Target groups in Healthy status

I create target group with the path `/photoalbum/album.php` and HTTP protocol with port 80, making sure all of registered targets in Healthy status

Summary

Review and confirm your configurations. [Estimate cost](#)

Basic configuration [Edit](#)

ELB-assignment2

- Internet-facing
- IPv4

Security groups [Edit](#)

- ELBSG
 - [sg-0adec94e6020bdce5](#)

Network mapping [Edit](#)

VPC [vpc-0e39596d00772b96a](#)
PPhamVPC2

- us-east-1a
 - [subnet-0bdf4bdee99c68a67](#)
Public subnet 1.2
- us-east-1b
 - [subnet-09ecfd6d4f9e00d92d](#)
Public subnet 2.2

Listeners and routing [Edit](#)

- HTTP:80 defaults to [TG-Web-server](#)

Add-on services [Edit](#)

None

Tags [Edit](#)

None

Attributes

Figure 23: Information of Load Balancers

I create Load balancers in public subnets.

6.Create Auto Scaling Group

Creating ASG is the next step

Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time	Created By
lt-07217f6bba5c2a	PhongTemplateAssignment2	1	1	2023-11-04T08:55:55.000Z	arn:aws:sts:739376045381:assumed-role/voclabr/user/2753058-104189767@student.swin.edu.au @ 7393-7604...

Figure 24: Template

I create a template to use for Auto scalling group (*PhongTemplateAssignment2*)

Review

Step 1: Choose launch template

Group details

Auto Scaling group name: *AutoScalingAssignment2*

Launch template: *PhongTemplateAssignment2* (lt-07217f6bba5c2a)

Version: Default

Description: Template

Step 2: Choose instance launch options

Network

VPC: *vpc-0e39596d00772b96a*

Availability Zone	Subnet	Subnet ID	Subnet CIDR
us-east-1a	<i>subnet-0bdf4bdee99c68a67</i>	subnet-0bdf4bdee99c68a67	10.0.3.0/24
us-east-1b	<i>subnet-09ecfd6d4f9e00d92d</i>	subnet-09ecfd6d4f9e00d92d	10.0.4.0/24

Figure 25: Information of Step 1 & Step 2

Step 1 : I launch template I create above

Step 2 : I choose the VPC I using in this assignment (*PPhamVPC2*) and the 2 Availability Zones storing 2 Private subnets

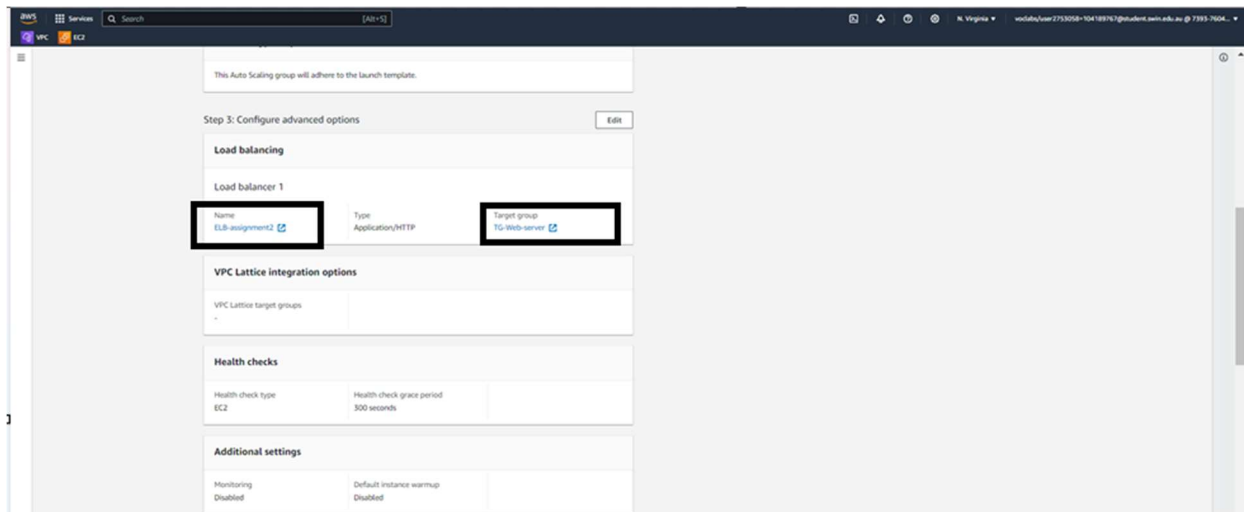


Figure 26: Information of Step 3

Step 3 : Using Load Balancing I created in the Step 5 (*ELB-assignment2*) and the target group (*TG-Web-server*)

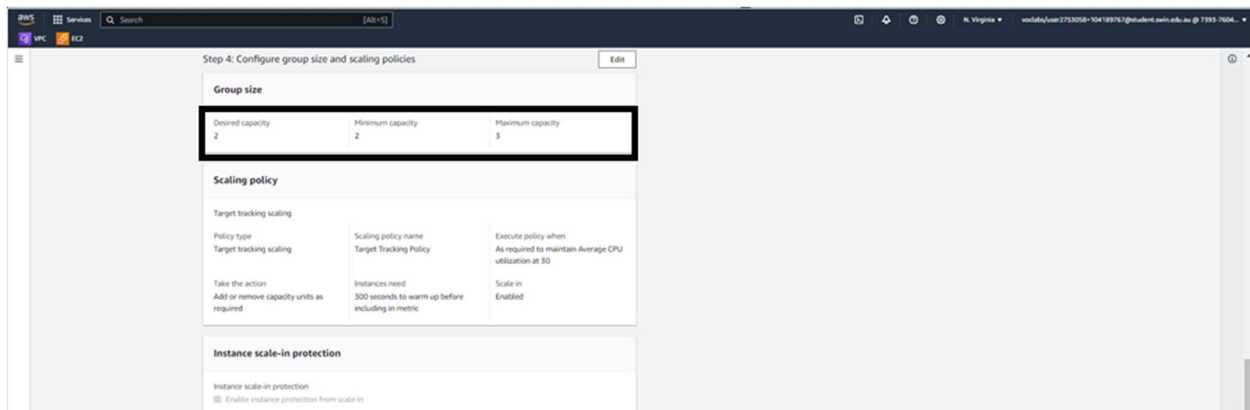


Figure 27: Information of Step 4

Step 4 : I set group size for and scaling policies

- . Desired capacity : 2
- . Maximum quality : 2
- . Maximum capacity : 3

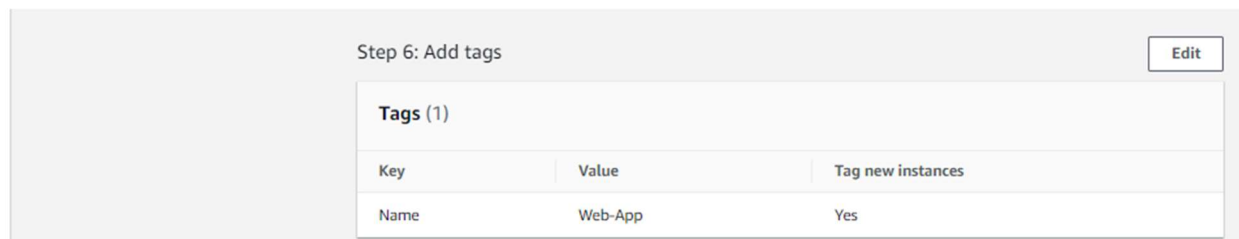


Figure 28: Information of Step 6

Step 5 (additional)

Step 6: Add tags with (*Key : Name* , *Value : Web – App*)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring	Security group
Web-App	i-010c18de8aa61ca22	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	-	-	-	-	disabled	Web-tier
Web-Server	i-070254bd214c83b7	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	ec2-54-92-231-101.co...	54.92.231.101	54.92.231.101	-	disabled	Web-Server-SG
Dev Instance	i-034d5d7bfc68ed51	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	ec2-100-24-173-133.co...	100.24.173.133	100.24.173.133	-	disabled	DevServerSG.ec2
Web-App	i-0913e8b02cf6da78	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	-	-	-	-	disabled	Web-tier

Figure 29: Instances created by ASG

There are 2 Web-App created by Auto Scaling Group

Instance ID	Instance state	Instance type	Public IPv4 address	Private IPv4 addresses
i-010c18de8aa61ca22 (Web-App)	Running	t2.micro	54.92.231.101	10.0.3.213

Figure 30: Information of instances created by ASG

Web-App is the instance created by Auto Scaling Group (*AutoScalingAssignment2*) with IAM Role (*LabRole*)

7.S3 bucket

In this stage, I used the old bucket instead of creating new bucket

Name	AWS Region	Access	Creation date
photoweb	US East (N. Virginia) us-east-1	Public	October 15, 2023, 19:16:24 (UTC+08:00)

Figure 31: S3 bucket

photoweb is my bucket

```

1 {
2   "Version": "2012-10-17",
3   "Id": "assignmentbucket2",
4   "Statement": [
5     {
6       "Sid": "PublicRead",
7       "Effect": "Allow",
8       "Principal": "*",
9       "Action": [
10        "s3:GetObject",
11        "s3:GetBucketLocation",
12        "s3:ListBucket",
13        "s3:PutObject"
14      ],
15      "Resource": [
16        "arn:aws:s3:::photoweb/*",
17        "arn:aws:s3:::photoweb"
18      ],
19      "Condition": {
20        "StringLike": {
21          "aws:Referer": [
22            "http://elb-assignment2-434376215.us-east-1.elb.amazonaws.com/*",
23            "http://ec2-100-24-173-133.compute-1.amazonaws.com/*"
24          ]
25        }
26      }
27    }
28  ]
29 }
```

Figure 32: S3 bucket policy

The thing I change is the S3 bucket policy , in this assignment , S3 bucket will not allow to access from public ; however, It only allows access from and by Application Load Balancer (ALB), it allows only the ELB to access, get, put, list object.

8.Lambda Function

The final stage is that create Lambda function

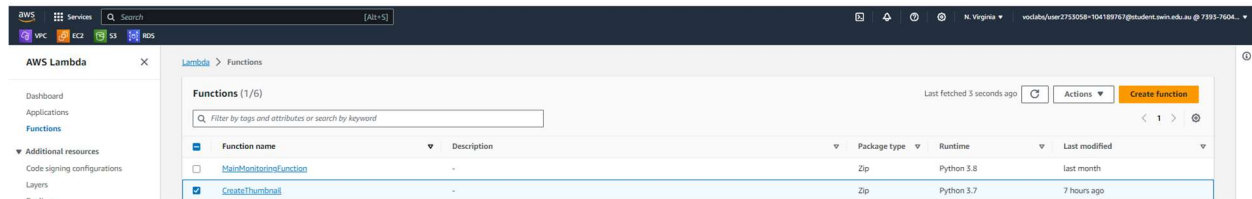


Figure 33: Create Lambda Function

I create a Lambda function (*CreateThumbnail*)

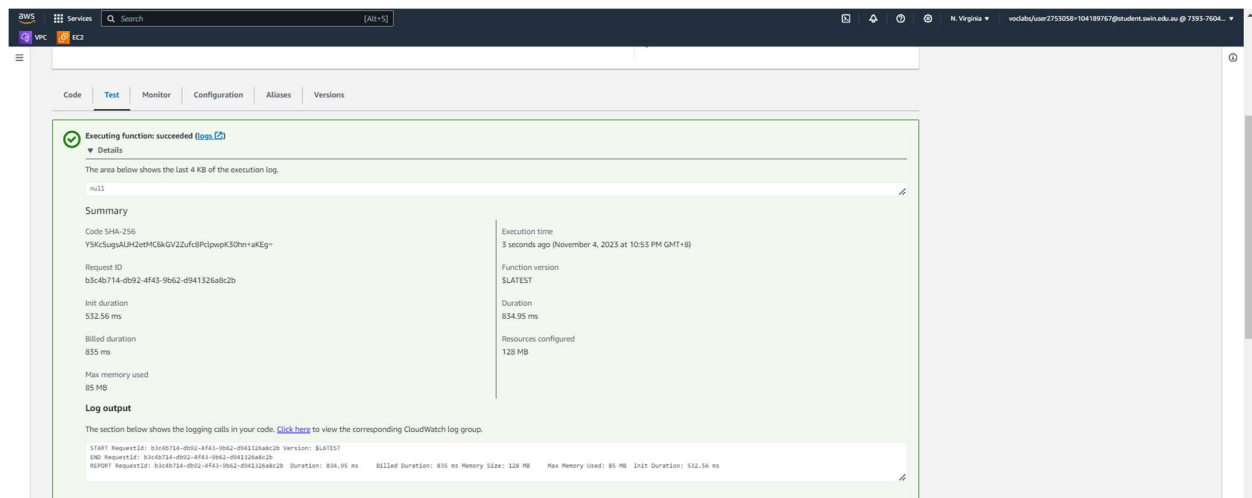


Figure 34: Test Lambda Function successfully

The Lamda function test case is successful

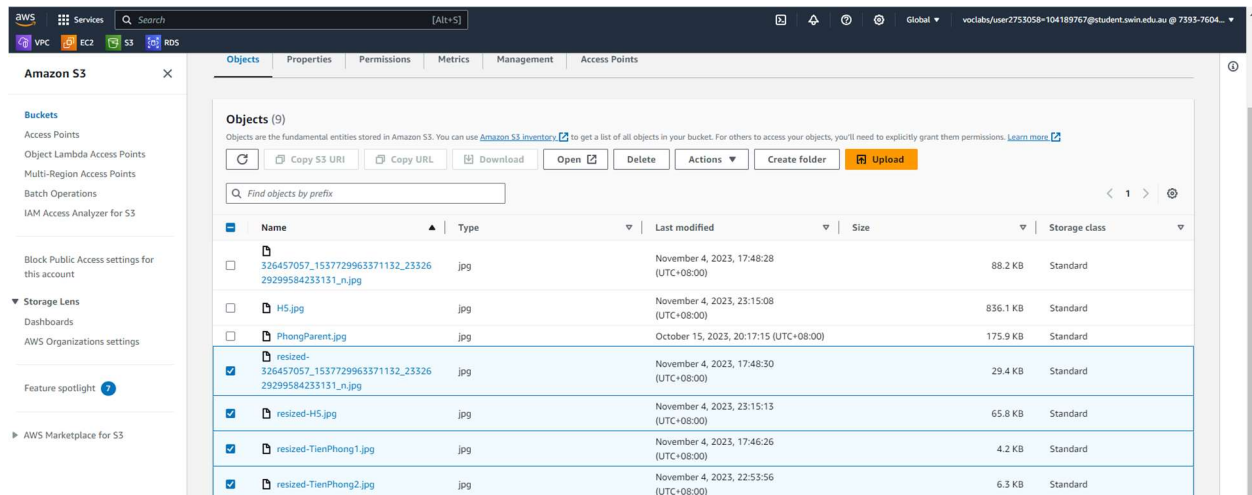


Figure 35: Resized photo created

And after a successfully testcase, It will resize uploaded picture to S3.

9. Testing

The PhotoAlbum website is accessible through the load balancer only

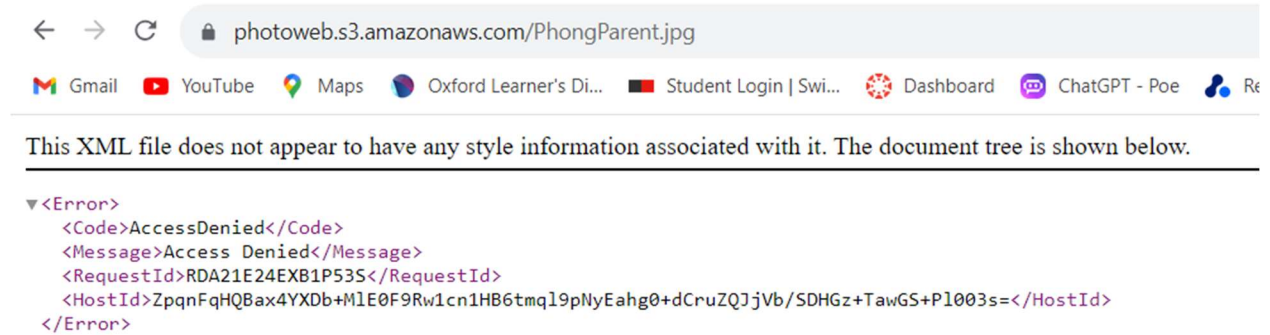


Figure 36: Test accessible through ELB only

I can not access PhotoAlbum website with other links different from ELB

Test the Network ACL bidirectional functionality by sending ICMP traffic between the web servers and Dev server.

```
ec2-user@ip-10-0-2-198:~  
# Using username "ec2-user".  
# Authenticating with public key "imported-openssh-key"  
Last login: Fri Nov 3 07:55:49 2023 from 125.234.120.78  
  
_#_  
~\##### Amazon Linux 2  
~~\_#####  
~~\_###| AL2 End of Life is 2025-06-30.  
~~\_#/   
~~ V~'-'>  
~~~~ A newer version of Amazon Linux is available!  
~~~~  
~~~~_-/_/_____  
_/_/'_/_____ Amazon Linux 2023, GA and supported until 2028-03-15.  
_/_/'_/_____ https://aws.amazon.com/linux/amazon-linux-2023/  
  
[ec2-user@ip-10-0-2-198 ~]$ ping 10.0.3.1  
PING 10.0.3.1 (10.0.3.1) 56(84) bytes of data.      ping private subnet 1.2 (failed)  
  
^Z  
[1]+ Stopped                  ping 10.0.3.1  
[ec2-user@ip-10-0-2-198 ~]$ ping 10.0.4.1  
PING 10.0.4.1 (10.0.4.1) 56(84) bytes of data.      ping private subnet 2.2 (failed)  
  
^Z  
[2]+ Stopped                  ping 10.0.4.1  
[ec2-user@ip-10-0-2-198 ~]$ ping 10.0.1.1  
PING 10.0.1.1 (10.0.1.1) 56(84) bytes of data.      ping public subnet 1.2  
                                                    (failed)  
  
^Z  
[3]+ Stopped                  ping 10.0.1.1  
[ec2-user@ip-10-0-2-198 ~]$ ping 0.0.0.0  
PING 0.0.0.0 (127.0.0.1) 56(84) bytes of data.      ping NAT gateway  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=255 time=0.020 ms (successful)  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=255 time=0.034 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=255 time=0.030 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=255 time=0.032 ms  
64 bytes from 127.0.0.1: icmp_seq=5 ttl=255 time=0.031 ms  
64 bytes from 127.0.0.1: icmp_seq=6 ttl=255 time=0.034 ms
```

Figure 37: Test sending ICMP

I can ping the NAT gateway, which located at 0.0.0.0, but the ICMP sent to private subnet 1.2(10.0.3.1) and private subnet 2.2(10.0.4.1) is not reachable. Therefore, our Network ACL is working.