

Assignment 1 – Part B

Creating and deploying Photo Album website onto a simple AWS infrastructure

Computer Science Department
Swinburne University
Ho Chi Minh city, Vietnam
104775085@student.swin.edu.au

Student Name: Tong Duc Tu Tam

Student ID: 104775085

Date of Submission: 15/6/2024

***Abstract*—This document will present all my work in Assignment 1 – part B.**

Keywords—Cloud Computing, AWS Services.

- Assignment Checklist:

Infrastructure requirements:

1. VPC with 2 public and 2 private subnets

1.1 – 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.

TTongVPC

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

IPv4 CIDR
10.0.0.0/16
CIDR block size must be between /16 and /28.

Account ID: 0656-4000-1481
Federated user: voclabs/user3267534=104775085@student.swin.edu.au @ 0656-4000-1481

Account
Organization
Service Quotas
Billing and Cost Management

Switch role Sign out

Figure 1: Create VPC with First, Last name and set the IPv4 CIDR block correspond to the requirement.

Your VPCs (2) Info

Search

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR
<input type="checkbox"/>	TTongVPC	vpc-0c6075af61944ba74	Available	10.0.0.0/16

Figure 2: Successfully created VPC.

1.2 – Create subnets:

Subnets (4) Info

Find resources by attribute or tag

VPC : [vpc-0c6075af61944ba74](#) Clear filters

<input type="checkbox"/>	Name	Subnet ID	State	VPC
<input type="checkbox"/>	Private subnet 1	subnet-07b9698c6f1cc84df	Available	vpc-0c6075af61944ba74
<input type="checkbox"/>	Public subnet 2	subnet-02dece170c5d3162f	Available	vpc-0c6075af61944ba74
<input type="checkbox"/>	Private subnet 2	subnet-0f57978b972c92c8e	Available	vpc-0c6075af61944ba74
<input type="checkbox"/>	Public subnet 1	subnet-0821cf60aa24c42b4	Available	vpc-0c6075af61944ba74

Figure 3: Created subnets.

Availability Zone	Availability Zone ID	Network border group
us-east-1a	use1-az1	us-east-1
us-east-1b	use1-az2	us-east-1
us-east-1b	use1-az2	us-east-1
us-east-1a	use1-az1	us-east-1

Figure 4: Subnet availability zones

2. Correct Public and Private Routing tables with correct subnet associations

Name	Route table ID	Explicit subnet associ...	Edge association
TTongVPC-rtb-public	rtb-0dcd49569daac077d	-	-
TTongVPC-rtb-private1-us-east-1a	rtb-066f2ac3d22fb13a8	-	-
TTongVPC-rtb-private2-us-east-1b	rtb-01521ef2d7b316ca1	-	-

Figure 3: Create route tables.

The following internet gateway was created: igw-06d4138475f097766 - TTongVPC-igw. You can now attach to a VPC to enable the VPC to communicate with the internet.

VPC > Internet gateways > igw-06d4138475f097766

igw-06d4138475f097766 / TTongVPC-igw

Figure 4: Create igw.

Internet gateway igw-06d4138475f097766 successfully attached to vpc-0c6075af61944ba74

Figure 5: Attach igw.

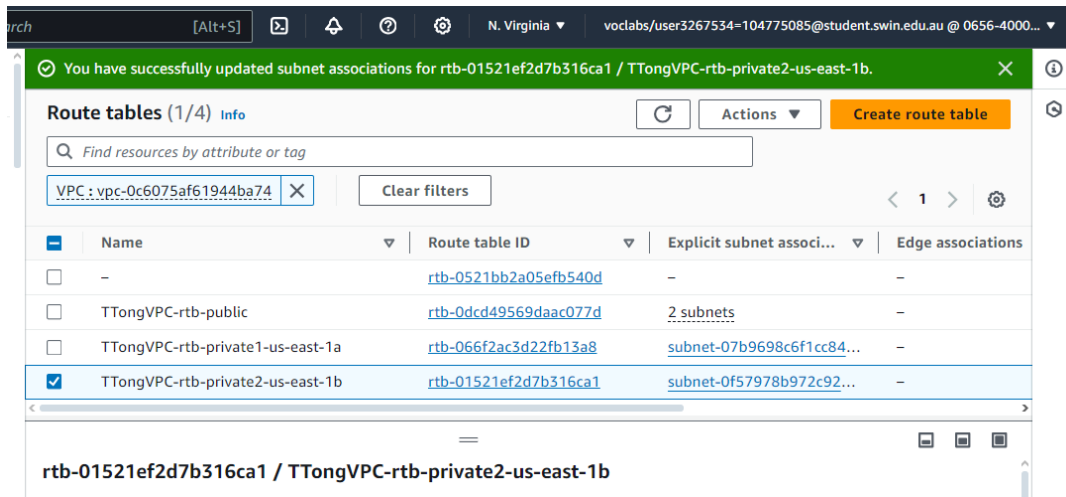


Figure 6: Associate subnets with correspond route tables.

3. Security groups properly configured and attached

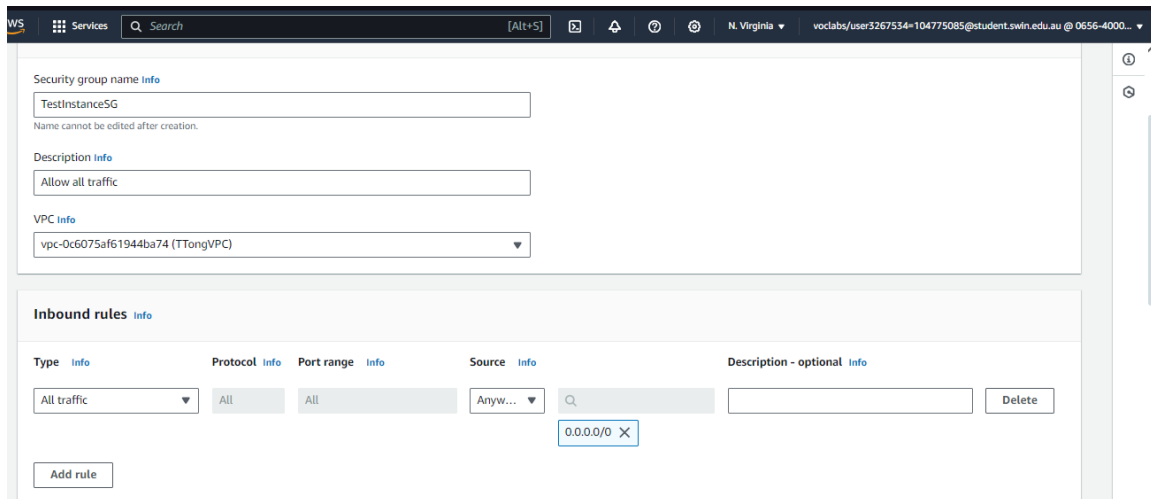


Figure 7: TestInstance security Group configuration.

WS Services Search [Alt+S] N. Virginia voclabs/user3267534=104775085@student.swin.edu.au @ 0656-4000...

Security group name [Info](#)
 WebServerSG
 Name cannot be edited after creation.

Description [Info](#)
 Allow HTTP and SSL connection

VPC [Info](#)
 vpc-0c6075af61944ba74 (TTongVPC)

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
HTTP	TCP	80	Anywh...	<input type="text"/> Delete
SSH	TCP	22	Anywh...	<input type="text"/> Delete
All ICMP - IPv4	ICMP	All	Custom	<input type="text"/> Delete

Note: A dropdown menu is open for the 'Source' field of the third rule, showing options: CIDR blocks, Security Groups (TestInstanceSG | sg-0453c393425017183), and Prefix lists (Q sg-0453c393425017183 X, sg-0453c393425017183 X).

Figure 8: WebServer Security Group configuration.

WS Services Search [Alt+S] N. Virginia voclabs/user3267534=104775085@student.swin.edu.au @ 0656-4000...

Create security group [Info](#)
 A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)
 DBServerSG
 Name cannot be edited after creation.

Description [Info](#)
 Allow SQL connection

VPC [Info](#)
 vpc-0c6075af61944ba74 (TTongVPC)

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
MYSQL/Aurora	TCP	3306	Custom	<input type="text"/> Delete

Note: A dropdown menu is open for the 'Source' field of the first rule, showing options: CIDR blocks, Security Groups (WebServerSG | sg-03579a5e7982eb7aa), and Prefix lists (Q sg-03579a5e7982eb7aa X, sg-03579a5e7982eb7aa X).

Figure 9: DBServer Security Group configuration.

Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
DBServerSG	vpc-0c6075af61944ba74	Allow SQL co...	065640001481	1 Permission entry	1 Permission entry
WebServerSG	vpc-0c6075af61944ba74	Allow HTTP a...	065640001481	3 Permission entries	1 Permission entry
TestInstanceSG	vpc-0c6075af61944ba74	Allow all traffic	065640001481	1 Permission entry	1 Permission entry
default	vpc-0c6075af61944ba74	default VPC s...	065640001481	1 Permission entry	1 Permission entry

Figure 10: Configured security groups.

4. Network ACL properly configured and attached

Name	Network ACL ID	Associated with	Default	VPC ID
PublicSubnet2NACL	acl-01f46780c46b296f3	subnet-02dece170c5d3162f / Public subnet 2	No	vpc-0c6075af61944ba74 / TTongVPC
-	acl-0db13b062195a2de5	3 Subnets	Yes	vpc-0c6075af61944ba74 / TTongVPC

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
110	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow
120	All ICMP - IPv4	ICMP (1)	All	10.0.4.0/24	Allow
130	All TCP	TCP (6)	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Figure 11: Set Network ACL inbound Rules.

Note: In the first time, when I specified three rules including: SSH, HTTP, ICMP, the connection was not success so I add another rule to allow all TCP protocol and everything works fine.

Search [Alt+S] [Icons] N. Virginia voclabs/user3267534-104775085@student.swin.edu.au @ 0656-4000...

You have successfully updated outbound rules for acl-01f46780c46b296f3 / PublicSubnet2NACL

Network ACLs (1/3) Info

Find resources by attribute or tag

Name	Network ACL ID	Associated with	Default	VPC ID
-	acl-0934d9a21572ecda2	6 Subnets	Yes	vpc-0d5a66388a9959fa9
<input checked="" type="checkbox"/> PublicSubnet2NACL	acl-01f46780c46b296f3	-	No	vpc-0c6075af61944ba74 / TTongVPC

acl-01f46780c46b296f3 / PublicSubnet2NACL

Details | Inbound rules | **Outbound rules** | Subnet associations | Tags

Outbound rules (2)

Filter outbound rules

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✔ Allow
*	All traffic	All	All	0.0.0.0/0	✘ Deny

Figure 12: Set Network ACL outbound Rules.

Search [Alt+S] [Icons] N. Virginia voclabs/user3267534-104775085@student.swin.edu.au @ 0656-4000...

Network ACLs (1/3) Info

Find resources by attribute or tag

Name	Network ACL ID	Associated with	Default	VPC ID
<input checked="" type="checkbox"/> PublicSubnet2NACL	acl-01f46780c46b296f3	subnet-02dece170c5d3162f / Public subnet 2	No	vpc-0c6075af61944ba74 / TTongVPC
<input type="checkbox"/> -	acl-0db13b062195a2de5	3 Subnets	Yes	vpc-0c6075af61944ba74 / TTongVPC

acl-01f46780c46b296f3 / PublicSubnet2NACL

Details | Inbound rules | Outbound rules | **Subnet associations** | Tags

Subnet associations (1)

Filter subnet associations

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
Public subnet 2	subnet-02dece170c5d3...	acl-01f46780c46b296f3 / PublicSubnet...	us-east-1b	10.0.2.0/24	-

Figure 13: Associate Network ACLs with correspond subnets.

5. Correct Web server and Test instances running in correct subnets

VPC - required [Info](#)

vpc-0c6075af61944ba74 (TTongVPC)
10.0.0.0/16

Subnet [Info](#)

subnet-02dece170c5d3162f **Public subnet 2**
VPC: vpc-0c6075af61944ba74 Owner: 065640001481 Availability Zone: us-east-1b
IP addresses available: 251 CIDR: 10.0.2.0/24

Auto-assign public IP [Info](#)

Disable

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

WebServerSG sg-0b3d652aa34b5609e X
VPC: vpc-0c6075af61944ba74

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

Advanced network configuration

Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0d191299f2822b1fa

Virtual server type (instance type)

t2.micro

Firewall (security group)

WebServerSG

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or ...)

Cancel Launch instance

Figure 14: Create Web Server instance with the correspond subnet and security group.

VPC - required [Info](#)

vpc-0c6075af61944ba74 (TTongVPC)
10.0.0.0/16

Subnet [Info](#)

subnet-0f57978b972c92c8e **Private subnet 2**
VPC: vpc-0c6075af61944ba74 Owner: 065640001481 Availability Zone: us-east-1b
IP addresses available: 251 CIDR: 10.0.4.0/24

Auto-assign public IP [Info](#)

Disable

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

TestInstanceSG sg-0453c393425017183 X
VPC: vpc-0c6075af61944ba74

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

Advanced network configuration

Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.4.2...read more
ami-08a0d1e16fc3f61ea

Virtual server type (instance type)

t2.micro

Firewall (security group)

TestInstanceSG

Storage (volumes)

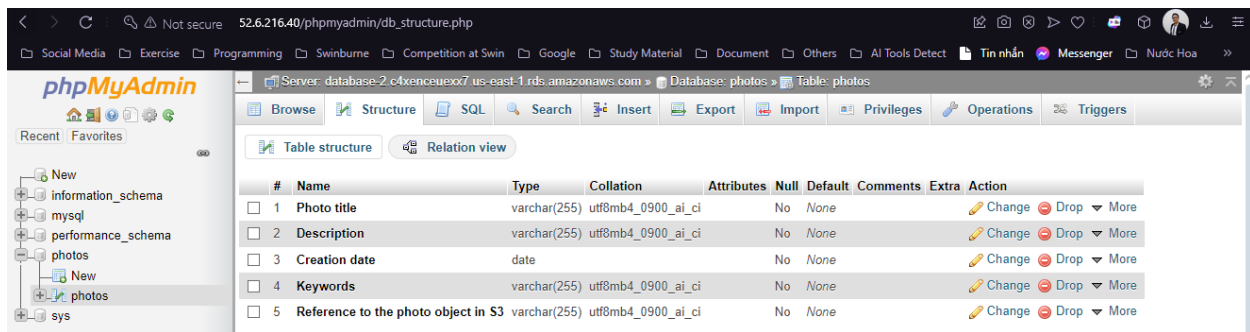
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or ...)

Cancel Launch instance

Figure 15: Configure Test Instance

6. Database schema as specified

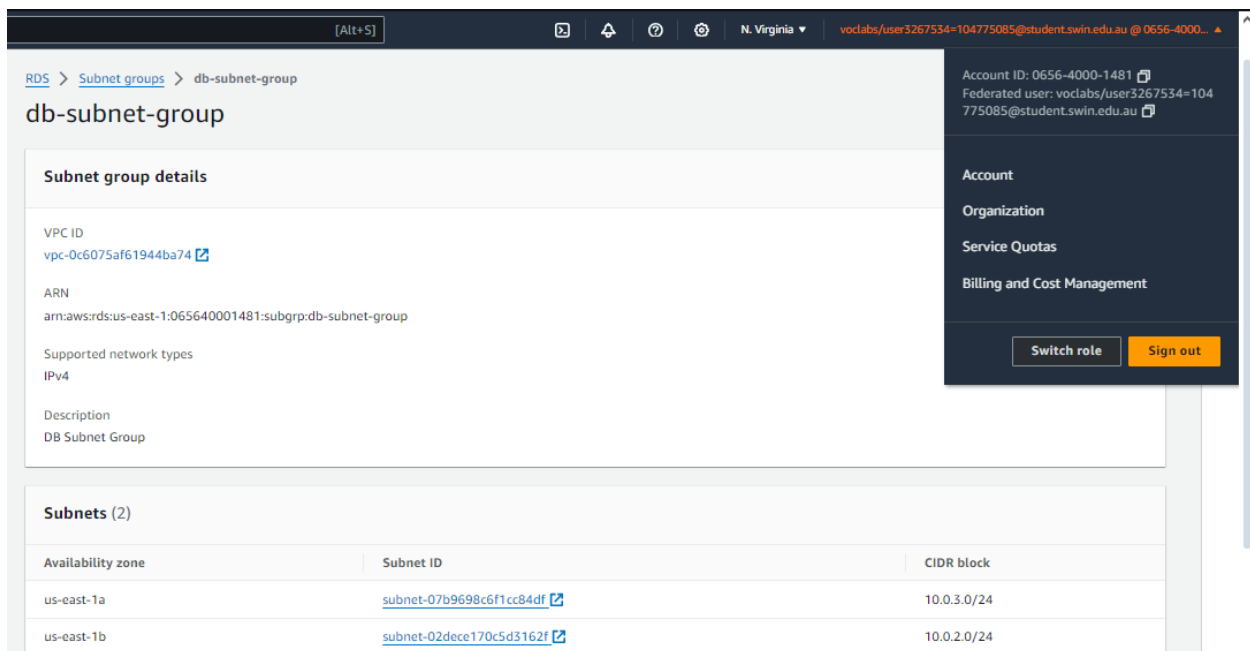


The screenshot shows the phpMyAdmin interface for a database named 'photos'. The 'Table structure' tab is selected, displaying the following table structure:

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	Photo title	varchar(255)	utf8mb4_0900_ai_ci		No	None			Change Drop More
2	Description	varchar(255)	utf8mb4_0900_ai_ci		No	None			Change Drop More
3	Creation date	date			No	None			Change Drop More
4	Keywords	varchar(255)	utf8mb4_0900_ai_ci		No	None			Change Drop More
5	Reference to the photo object in S3	varchar(255)	utf8mb4_0900_ai_ci		No	None			Change Drop More

Figure 16: Config Database scheme as specified.

7. Database running in correct subnets



The screenshot shows the AWS IAM console for the 'db-subnet-group' subnet group. The details section shows the VPC ID as 'vpc-0c6075af61944ba74' and the ARN as 'arn:aws:rds:us-east-1:065640001481:subgrp:db-subnet-group'. The supported network types are IPv4. The description is 'DB Subnet Group'.

The subnets section lists two subnets:

Availability zone	Subnet ID	CIDR block
us-east-1a	subnet-07b9698c6f1cc84df	10.0.3.0/24
us-east-1b	subnet-02dece170c5d3162f	10.0.2.0/24

Figure 17: Set the subnet for database as specified.

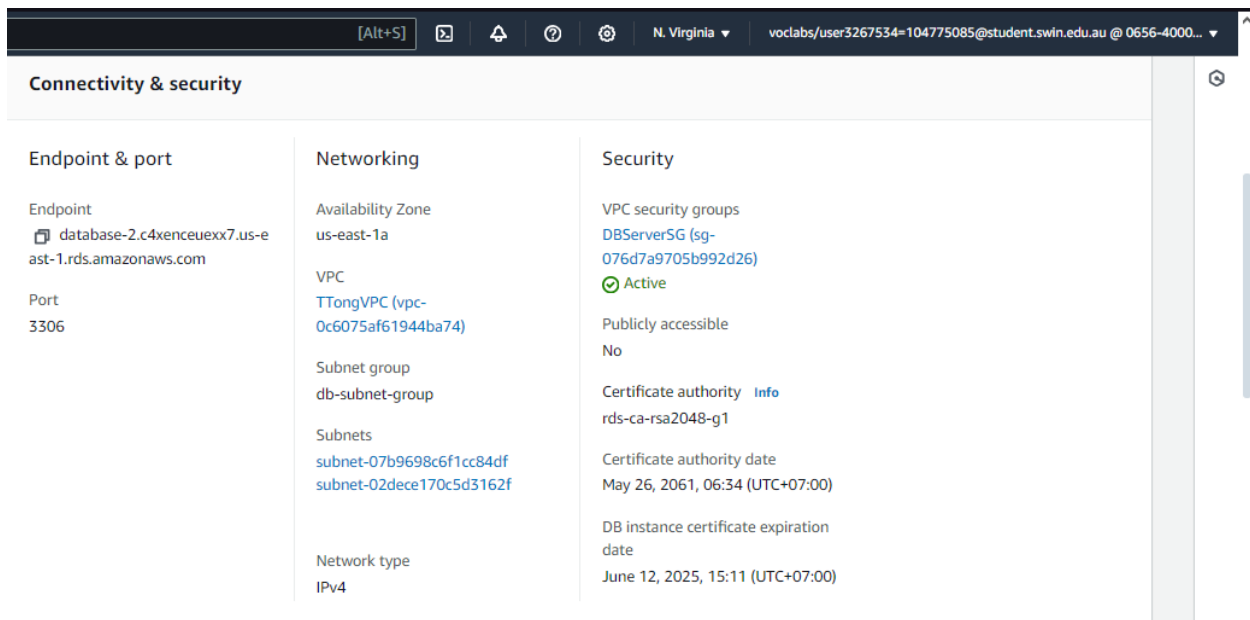


Figure 18: Subnet group attached to database.

8. S3 objects publicly accessible, using proper access policy

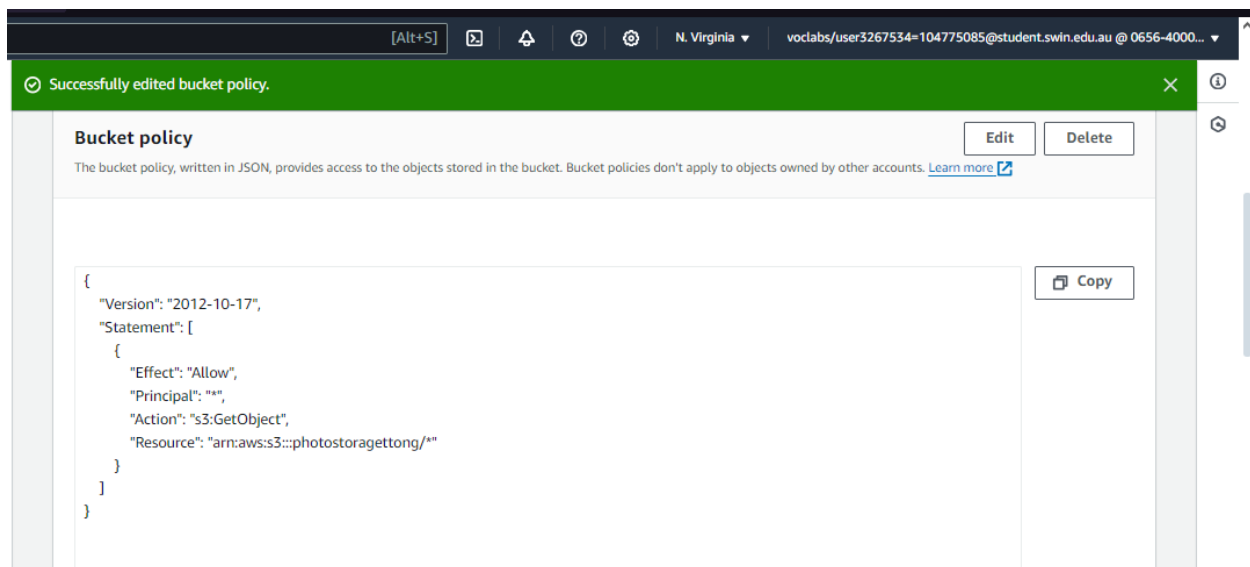


Figure 19: Add bucket policy to make objects publicly accessible.

9. album.php page displayed from EC2 Web server

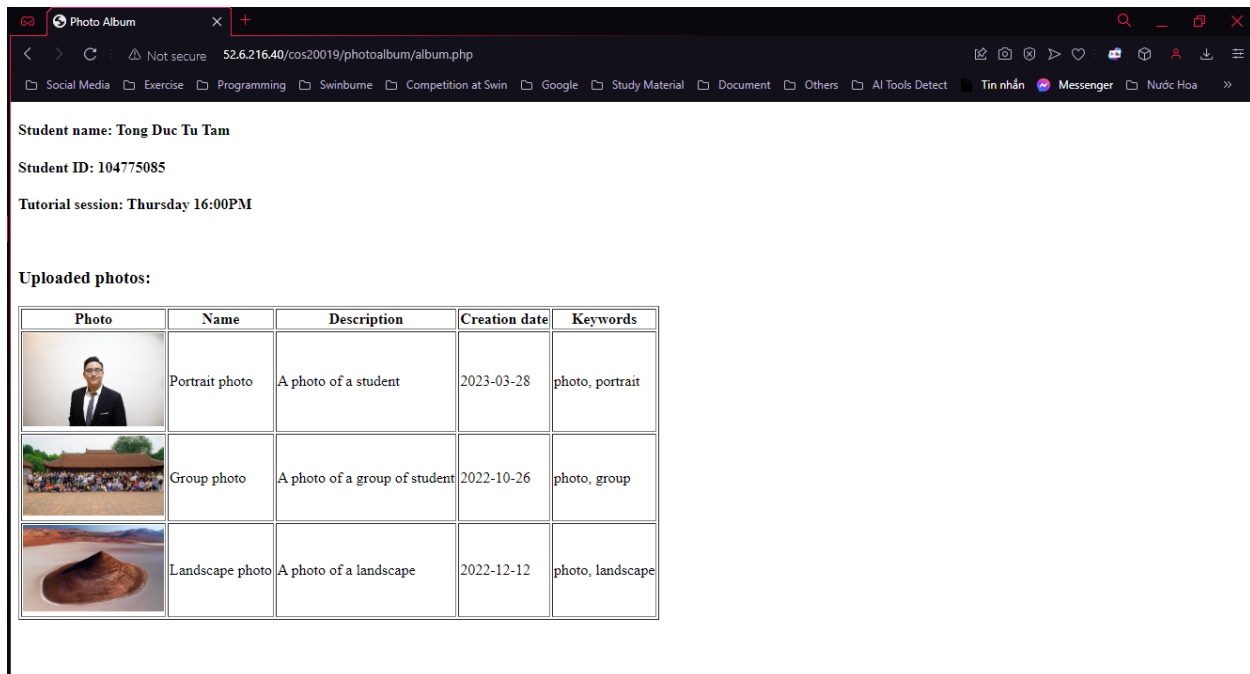


Figure 20: Display album.php on EC2 Web Server.

10. Photos loaded from S3 with matching metadata from RDS

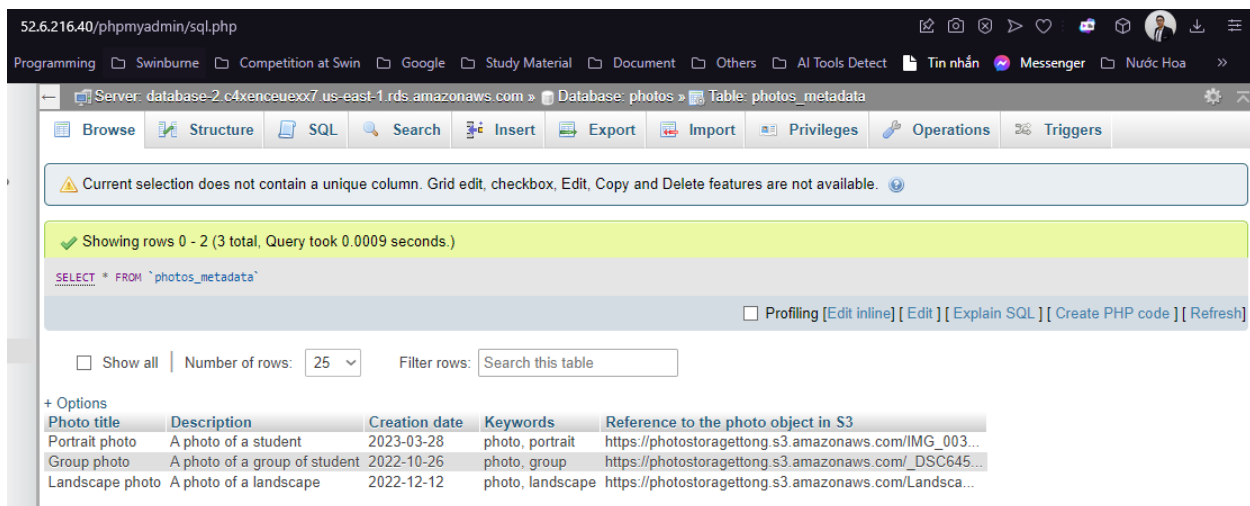


Figure 21: Metadata from RDS database.

11. Provided URL is persistent (Elastic IP Association)

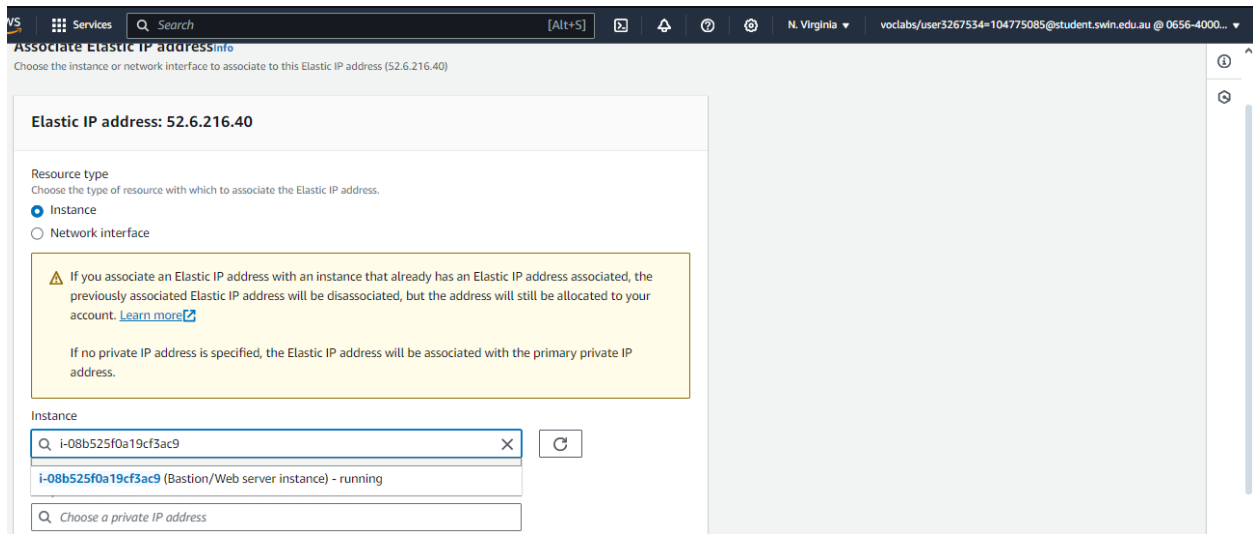


Figure 22: Associate Elastic IP to the Web instance.

12. Web server instance reachable from Test instance via ICMP

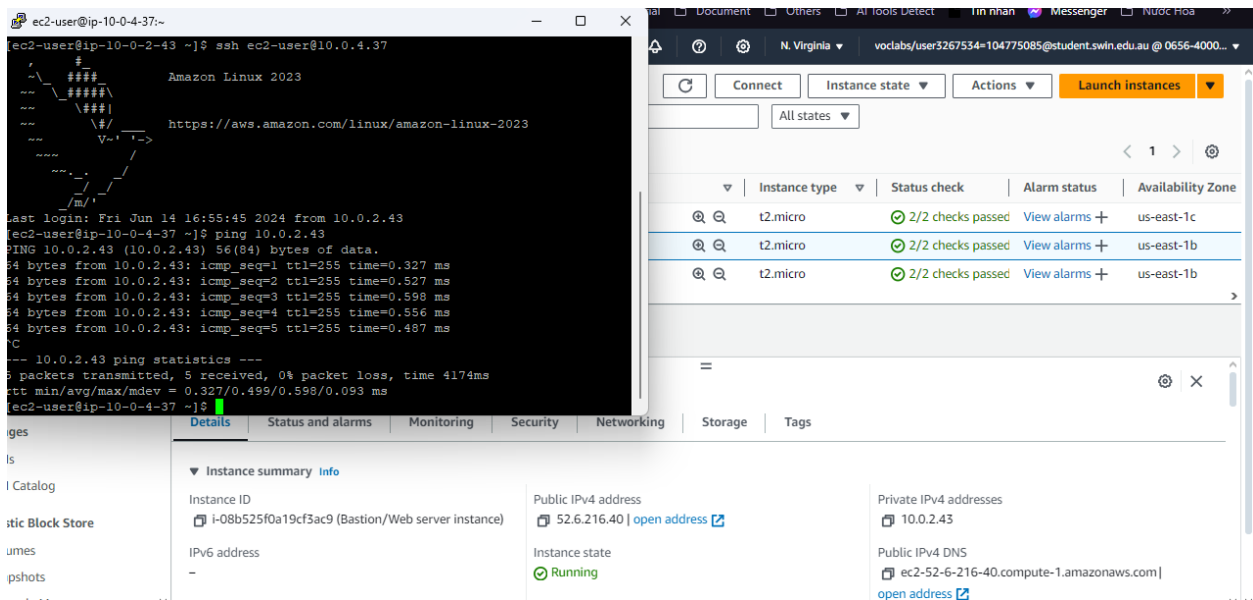


Figure 23: SSH into the Test Instance and ping the Bastion instance.