

# Assignment 1B Checklist

---

***Make sure all the following are completed.***

## Submission Checklist

Student Name: Nhat Minh

Tran

Student Id: 104082552

Tutorial time: Tuesday, 6.30-  
8.30pm

Date of submission: 17/09/2023

Submit to Canvas:

A PDF document file as specified in the Submission section of the assignment specification.

## Marking Scheme

Infrastructure Requirements		
VPC with 2 public and 2 private subnets	.5	Done
Correct Public and Private Routing tables with correct subnet associations	1	Done
Security groups properly configured and attached.	1	Done
Network ACL properly configured and attached	1.5	Done
Correct Web server and Test instances running in correct subnets	.5	Done
Database schema as specified	.5	Done
Database running in correct subnets	1	Done
S3 objects publicly accessible, using proper access policy	.5	Done
Functional Requirements		
album.php page displayed from EC2 Web server	1	Done
Provided URL is persistent (Elastic IP Association)	.5	Done
Photos loaded from S3 with matching metadata from RDS	1	Done
Web server instance reachable from Test instance via ICMP	1	Done
Deductions		
Documentation not as specified or poorly presented (up to minus 20)		
Serious misconfigurations of AWS services being used (up to minus 20)		

## 1. Infrastructure deployment

### 1.1 – VPC

In the first stage, I created a VPC. Secondly, following the diagram in the assignment, I created four subnets in two AZs. IGW is created and attached to VPC, it also associated to public route table.

The screenshot shows the AWS VPC dashboard. A green success message at the top says "You successfully created vpc-027e390abafa36428 / MTranVPC". The main panel displays the details of the newly created VPC:

VPC ID	State	DNS hostnames	DNS resolution
vpc-027e390abafa36428	Available	Disabled	Enabled
Tenancy	DHCP option set	Main route table	Main network ACL
Default	dopt-092e393398dc1e79a	rtb-02bf2bac36b8ccc47	acl-0c88167e2e93db30a
Default VPC	IPv4 CIDR	IPv6 pool	IPv6 CIDR (Network border group)
No	10.0.0.0/16	-	-
Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups	Owner ID	
Disabled	<span style="color: red;">Failed to load rule groups</span>	913704114463	

Below the details, there are tabs for "Resource map New", "CIDRs", "Flow logs", and "Tags". The URL in the address bar is <https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#>.

Figure 1: VPC created

The screenshot shows the AWS Internet Gateways page. A green success message at the top says "Internet gateway igw-0514543d6110b7bb0 successfully attached to vpc-027e390abafa36428". The main panel displays the list of Internet gateways:

Name	Internet gateway ID	State	VPC ID
-	igw-014c389d682243d56	Attached	vpc-027ddfd02783c55f
MyIGW	igw-0514543d6110b7bb0	Attached	vpc-027e390abafa36428   MTranVPC

Below the list, there is a detailed view of the selected Internet gateway:

Internet gateway ID	State	VPC ID	Owner
igw-0514543d6110b7bb0	Attached	vpc-027e390abafa36428   MTranVPC	913704114463

The URL in the address bar is <https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#>.

Figure 2: IGW is attached to MTran VPC

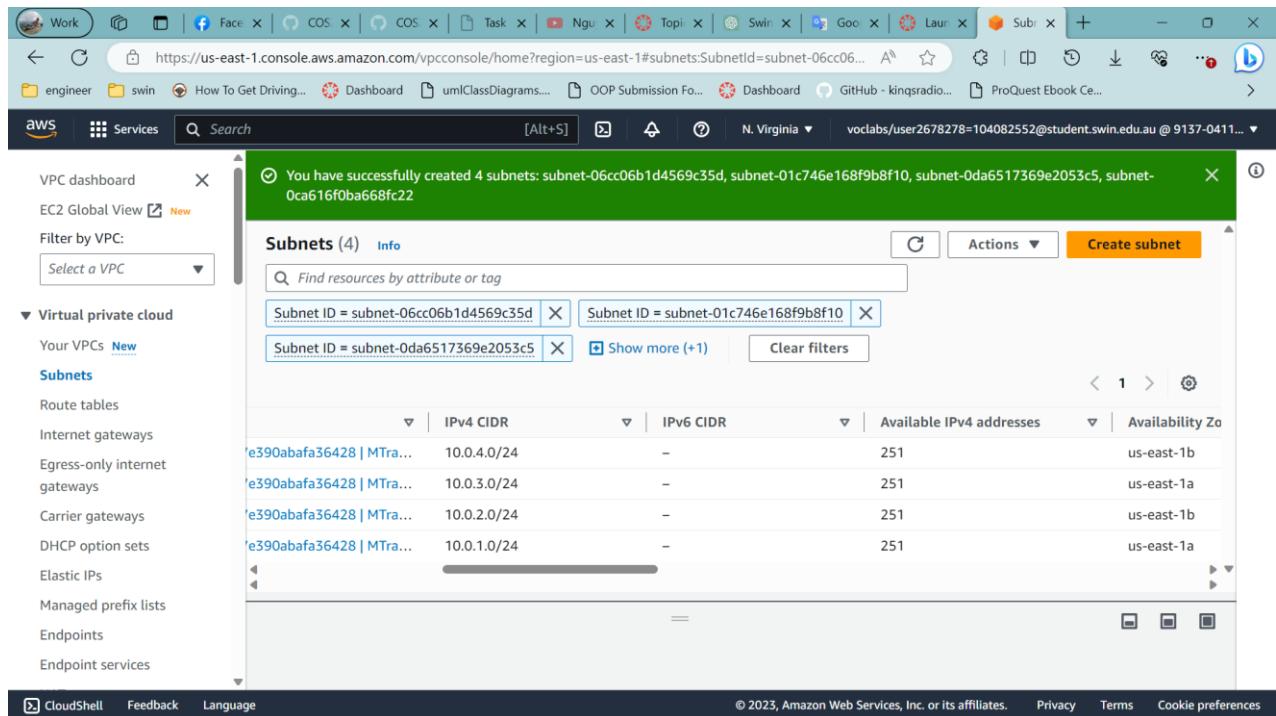


Figure 3: 4 subnets with 2 AZs

There are four subnets(two public and two private), for this assignment, the subnet public 2 will attached to IGW, the subnet public 1 is created but will not be used.

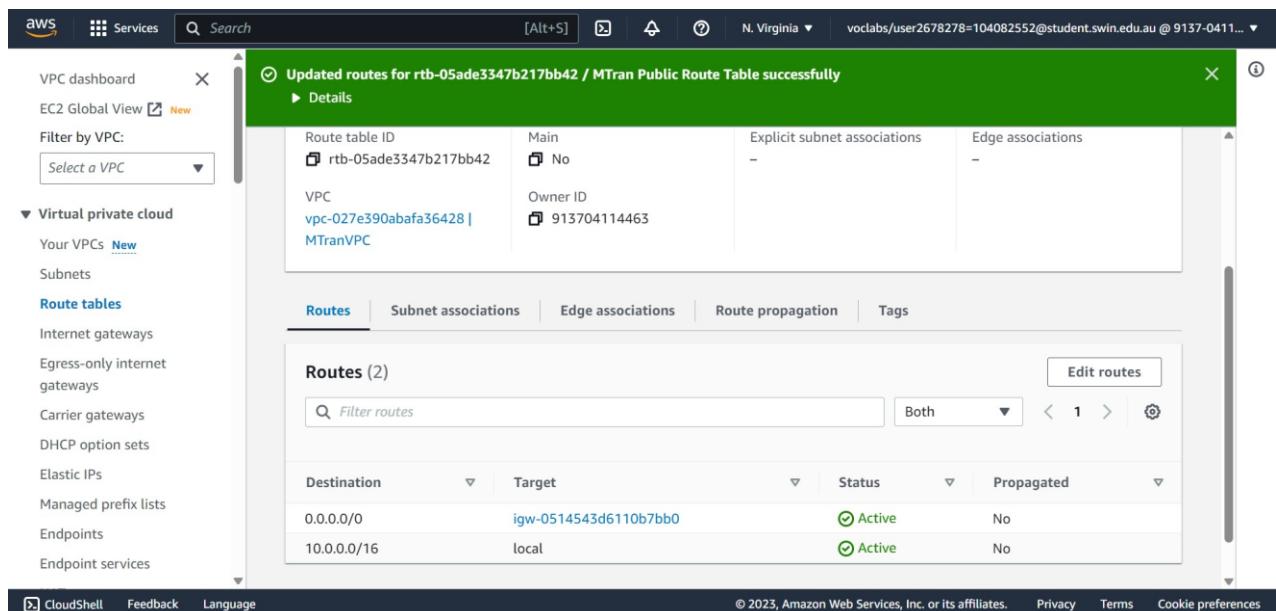


Figure 4: Public route table

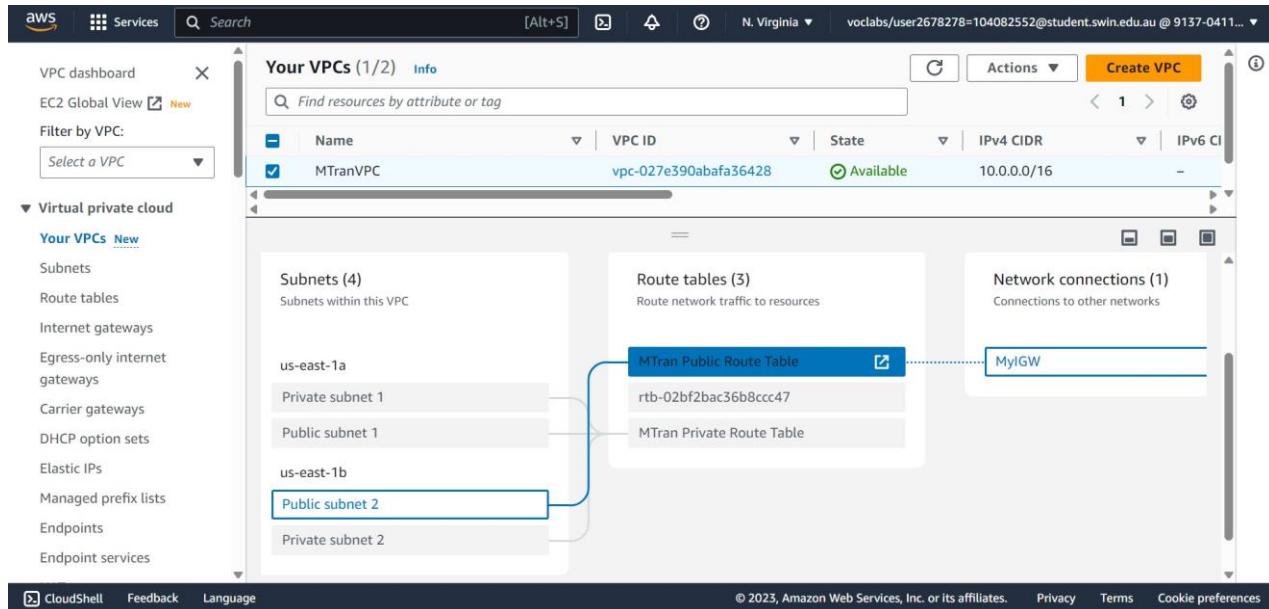


Figure 5: Resource maps

Route table determines where network traffic is directed. Each subnet in VPC will be associated with a route table. This determines which route table rules apply to the traffic in that subnet. In this scenario, only public subnet 2 goes through public table and IGW, while other three are associated to private route table.

## 1.2 – Security groups

Three security groups are built with different protocols to allow specific instances. These are all assigned with MTranVPC.

The screenshot shows the AWS Security Groups interface. At the top, there's a search bar and navigation links for 'VPC dashboard', 'EC2 Global View', and 'Filter by VPC'. The main area displays 'Security Groups (3)' with three entries: 'WebServerSG' (Security group ID: sg-02a59be3a6ed76e5), 'TestInstanceSG' (Security group ID: sg-0536c8dbf1dbf8ec7), and 'DBServerSG' (Security group ID: sg-0d89b0f9527e83fc5). Each row includes columns for 'Security group ID', 'Security group name', 'VPC ID', 'Description', and 'Owner'.

Figure 6: 3 security group

## 1.3 – EC2 virtual machine

In this stage, I created two EC2 instances, a web server instance and a test instance. The web server instance had PHP/HTML code to run the website. VPC is associated with Elastic Ip so that it is fixed.

Elastic IP provides a static, public IPv4 that you can assign to your AWS. The most important is that the elastic IP does not change every time you start or end lab.

The screenshot shows the AWS EC2 Instances page. The left sidebar includes links for EC2 Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), and CloudShell. The main content area displays 'Instances (2) Info' with a search bar and a table. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, and Avail. Two instances are listed: 'Web server ins...' (i-03186efb8480d8d7f) and 'Test instance' (i-0e4c10f3b9abde203), both in the 'Running' state. A modal window titled 'Select an instance' is open at the bottom.

Figure 7: Web server instance and Test instance

The screenshot shows the AWS Elastic IP Addresses page. The left sidebar includes links for EC2 Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), and CloudShell. A green success message at the top states: 'Elastic IP address associated successfully. Elastic IP address 44.218.208.115 has been associated with instance i-03186efb8480d8d7f'. The main content area displays 'Elastic IP addresses (1/1)' with a table. The table has columns for Name, Allocated IPv4 addr..., Type, and Allocation ID. One entry is shown: '44.218.208.115' (Public IP, Allocation ID: eipalloc-07d817c226765a4c3). Below the table is a detailed view of the association:

Allocated IPv4 address	Type	Allocation ID	Reverse DNS record
44.218.208.115	Public IP	eipalloc-07d817c226765a4c3	-
Association ID	Scope	Associated instance ID	Private IP address
eipassoc-	VPC	i-03186efb8480d8d7f	10.0.2.103

Figure 8: Elastic Ip for Web server instance



This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

#### If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

#### If you are the website administrator:

You may now add content to the directory /var/www/html/. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file /etc/httpd/conf.d/welcome.conf.

You are free to use the image below on web sites powered by the Apache HTTP Server:



*Figure 9: Test webpage with elastic IP*

## 1.4 – RDS database instance

The database service is the service that cannot be visible to the customers. In order to do that, this instance must be in a private subnet in the VPC. However, the RDS instance needs to be access over the internet for setup and maintenance purposes. This can be done by installing phpMyAdmin. The security group “DBServerSG” has also been associated with this instance. This setup creates many layers for security purposes and reduce the chance of being exposure to the public internet.

The screenshot shows the AWS RDS Subnet Groups details page. The left sidebar lists various RDS management options. The main content area shows "Subnet group details" for a group named "vpc-027e390abafa36428". It includes fields for VPC ID, ARN, Supported network types (IPv4), and Description (Private DB subnet group). Below this, a table titled "Subnets (2)" lists two subnets: "us-east-1b" and "us-east-1a", each with its corresponding Subnet ID and CIDR block.

Availability zone	Subnet ID	CIDR block
us-east-1b	subnet-0ca616f0ba668fc22	10.0.4.0/24
us-east-1a	subnet-01c746e168f9bf10	10.0.3.0/24

*Figure 10: Subnet groups for RDS*

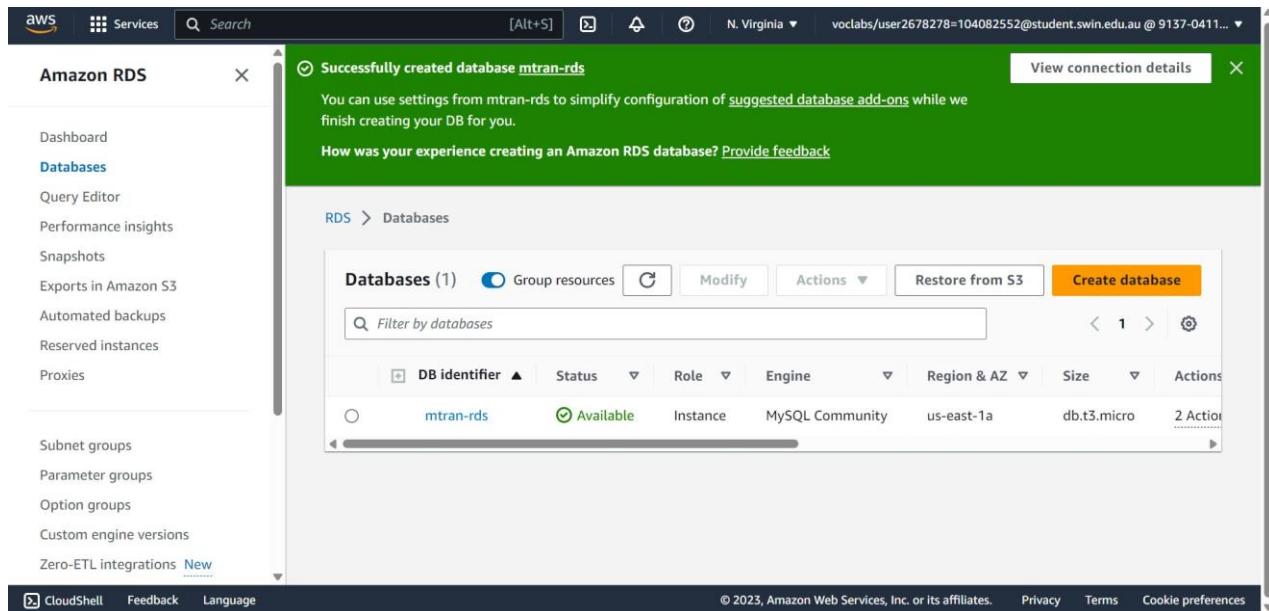


Figure 11: RDS instance

```

inflating: phpMyAdmin-5.2.1-english/vendor/web-auth/webauthn-lib/src/U2F PublicKey.php
creating: phpMyAdmin-5.2.1-english/vendor/web-auth/webauthn-lib/src/Util/
inflating: phpMyAdmin-5.2.1-english/vendor/web-auth/webauthn-lib/src/Util/CoseSignatureFixer.php
creating: phpMyAdmin-5.2.1-english/vendor/webmozart/
inflating: phpMyAdmin-5.2.1-english/vendor/webmozart/assert/
inflating: phpMyAdmin-5.2.1-english/vendor/webmozart/assert/CHANGELOG.md
inflating: phpMyAdmin-5.2.1-english/vendor/webmozart/assert/LICENSE
inflating: phpMyAdmin-5.2.1-english/vendor/webmozart/assert/README.md
inflating: phpMyAdmin-5.2.1-english/vendor/webmozart/assert/composer.json
creating: phpMyAdmin-5.2.1-english/vendor/webmozart/assert/src/
inflating: phpMyAdmin-5.2.1-english/vendor/webmozart/assert/src/Assert.php
inflating: phpMyAdmin-5.2.1-english/vendor/webmozart/assert/src/InvalidArgumentException.php
inflating: phpMyAdmin-5.2.1-english/vendor/webmozart/assert/src/Mixin.php
creating: phpMyAdmin-5.2.1-english/vendor/williamdes/
inflating: phpMyAdmin-5.2.1-english/vendor/williamdes/mariadb-mysql-kbs/
inflating: phpMyAdmin-5.2.1-english/vendor/williamdes/mariadb-mysql-kbs/CHANGELOG.md
inflating: phpMyAdmin-5.2.1-english/vendor/williamdes/mariadb-mysql-kbs/LICENSE
inflating: phpMyAdmin-5.2.1-english/vendor/williamdes/mariadb-mysql-kbs/README.md
inflating: phpMyAdmin-5.2.1-english/vendor/williamdes/mariadb-mysql-kbs/composer.json
creating: phpMyAdmin-5.2.1-english/vendor/williamdes/mariadb-mysql-kbs/dist/
inflating: phpMyAdmin-5.2.1-english/vendor/williamdes/mariadb-mysql-kbs/dist/merged-ultraslim.json
creating: phpMyAdmin-5.2.1-english/vendor/williamdes/mariadb-mysql-kbs/src/
inflating: phpMyAdmin-5.2.1-english/vendor/williamdes/mariadb-mysql-kbs/src/KBDocumentation.php
inflating: phpMyAdmin-5.2.1-english/vendor/williamdes/mariadb-mysql-kbs/src/KBEntry.php
inflating: phpMyAdmin-5.2.1-english/vendor/williamdes/mariadb-mysql-kbs/src/KBException.php
inflating: phpMyAdmin-5.2.1-english/vendor/williamdes/mariadb-mysql-kbs/src/Search.php
inflating: phpMyAdmin-5.2.1-english/vendor/williamdes/mariadb-mysql-kbs/src/SlimData.php
inflating: phpMyAdmin-5.2.1-english/yarn.lock
[ec2-user@ip-10-0-2-103 html]$ mv phpMyAdmin-5.2.1-english phpmyadmin
[ec2-user@ip-10-0-2-103 html]$

Your Photo Album website must have the following functional requirements.

```

Figure 12: phpMyAdmin installed and moved on EC2 Instance

The screenshot shows the phpMyAdmin interface on a web browser. The left sidebar lists databases: information\_schema, minh (selected), mysql, performance\_schema, photos, and sys. The main area has tabs for Databases, SQL, Status, User accounts, Export, Import, Settings, Binary log, Replication, and More. Under Databases, the 'General settings' section shows a 'Server connection collation' dropdown set to utf8mb4\_unicode\_ci. The 'Appearance settings' section shows the theme as pmahommme. The 'Database server' section provides details about the MySQL server, including its connection via TCP/IP, version 8.0.34, and user MTran@10.0.2.103. The 'Web server' section shows Apache/2.4.57, MySQL 5.0.12-dev, PHP 7.2.34, and various PHP extensions.

Figure 13: Webpage of phpMyAdmin

This screenshot shows the phpMyAdmin interface for the 'photos' table in the 'minh' database. The table structure includes columns: phototitle, description, creationdate, keywords, and reference. Two rows of data are displayed:

phototitle	description	creationdate	keywords	reference
title	description	2023-09-16	logo	<a href="https://nhatminhbucket.s3.amazonaws.com/logo.png">https://nhatminhbucket.s3.amazonaws.com/logo.png</a>
title	description	2023-09-16	logo	<a href="https://nhatminhbucket.s3.amazonaws.com/logo.png">https://nhatminhbucket.s3.amazonaws.com/logo.png</a>

Figure 14: Table and data on webpage

## 1.5 – Network ACL

In AWS, NACL is a security layer that controls inbound and outbound traffic in the VPC. I have created a set of inbound and outbound rules to control the traffic coming into the subnet and the traffic leaving the subnet.

The screenshot shows the AWS Network ACLs (Inbound rules) interface. The table lists the following inbound rules:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
1	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow
2	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
3	All TCP	TCP (6)	All	10.0.4.0/24	Allow
4	All TCP	TCP (6)	All	10.0.3.0/24	Allow
5	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Figure 15: Inbound rules for NACL

The screenshot shows the AWS Network ACLs (Outbound rules) interface. The table lists the following outbound rules:

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
1	SSH (22)	TCP (6)	22	10.0.4.0/24	Allow
2	All ICMP - IPv4	ICMP (1)	All	10.0.4.0/24	Allow
3	MySQL/Aurora (3...)	TCP (6)	3306	0.0.0.0/0	Allow
4	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Figure 16: Outbound rules for NACL

The screenshot shows the AWS Network ACLs page. On the left, there's a navigation sidebar with sections like Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections, Security (Network ACLs selected), DNS firewall, Rule groups, Domain lists, Network Firewall, Firewalls, and Firewall policies. The main area displays a table titled "Network ACLs (1/3)" with one item listed:

Name	Network ACL ID	Associated with	Default	VPC ID
<input checked="" type="checkbox"/> PublicSubnet2NACL	acl-0ea94355ea94bb549	subnet-0da6517369e2053c5 / Public subnet 2	No	vpc-02

Below the table, a "Details" section provides more information about the selected Network ACL:

Network ACL ID acl-0ea94355ea94bb549	Associated with subnet-0da6517369e2053c5 / Public subnet 2	Default No	VPC ID vpc-027e390abafa36428 / MTranVPC
Owner 913704114463			

At the bottom of the page, there are links for CloudShell, Feedback, Language, and a copyright notice: © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences.

Figure 17: Network ACL is assigned to Public subnet 2

## 2. Functional requirements for Photo Album website

### 2.1 -Photo storage

S3 is a service that provided by AWS and allow you store and upload any photos, documents, videos... However, the photo that I uploaded cannot be seen right away, it needs bucket policy permissions to allow users to see it.

The screenshot shows the AWS S3 console. On the left, there's a navigation sidebar with sections like 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), and Feature spotlight. The main area displays a table titled "Objects (1)" for the bucket "nhatminhbucket".

Name	Type	Last modified	Size	Storage class
logo.png	png	September 16, 2023, 12:29:34 (UTC+10:00)	4.3 KB	Standard

Below the table, there are buttons for Create folder, Upload, Copy S3 URI, Copy URL, Download, Open, Delete, and Actions. There's also a search bar for Find objects by prefix. At the bottom, there are links for CloudShell, Feedback, Language, and a copyright notice: © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences.

Figure 18: Nhatminhbucket

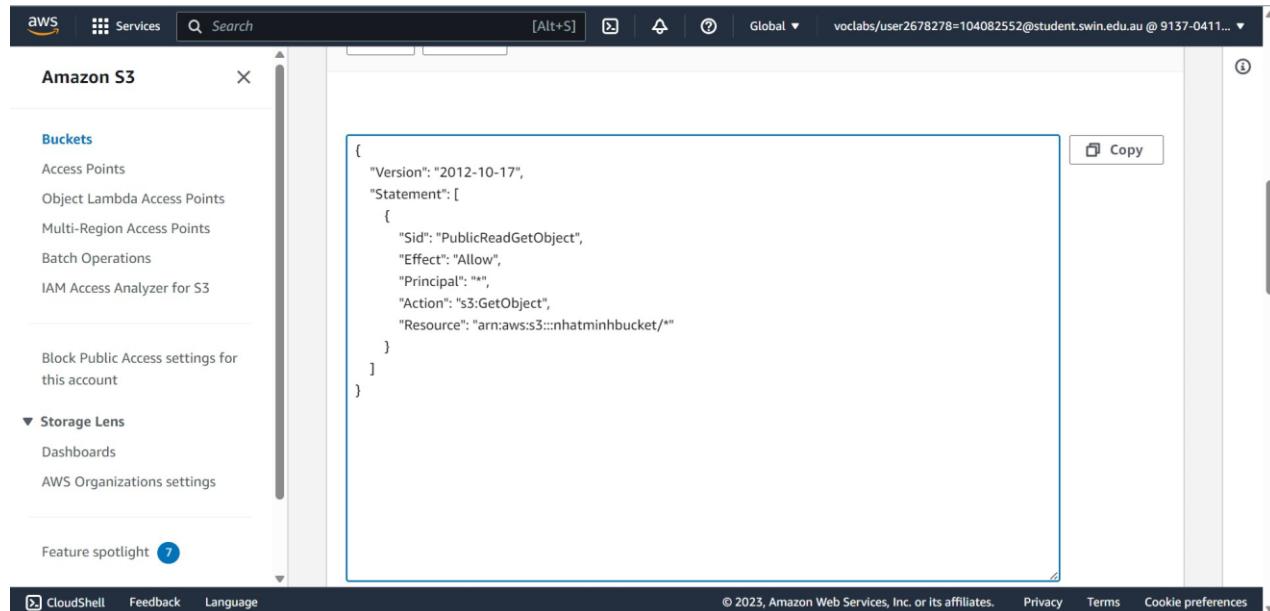


Figure 19: Policy permission for S3 bucket

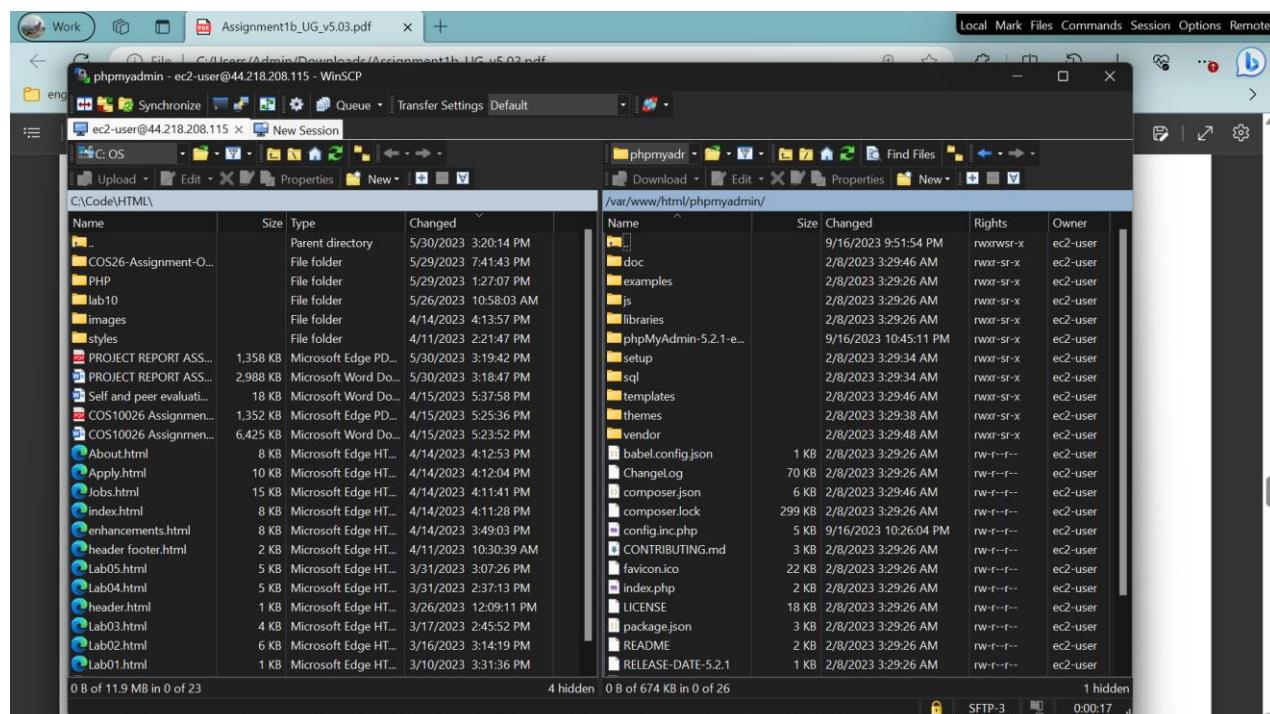


Figure 20: WinSCP connected with Minh.ppk authentication

## 2.2 – Photo meta-data in RDS instance

In this section, I created a table dedicated to photos, with five columns which are phototitle, description, creationdate, keywords, and reference. This data is used to display digital photos and videos on websites through phpMyAdmin service.

The screenshot shows the phpMyAdmin interface with the following details:

- Database:** minh
- Table:** photos
- Columns:** phototitle, description, creationdate, keywords, reference
- Rows:**
  - 1: title | description | 2023-09-16 | logo | https://nhatminhbucket.s3.amazonaws.com/logo.png
  - 2: title | description | 2023-09-16 | logo | https://nhatminhbucket.s3.amazonaws.com/logo.png

Figure 21: Meta-data of the website

## 2.3 – Photo Album website functionality

The website is completed with PHP, CSS, HTML files provided from school. In this stage, I have changed the constant.php to make it becomes website that unique to me such as student name, studentID, tutorial session, photos...

The screenshot shows a web browser displaying the following information:

- Student name:** Nhat Minh Tran
- Student ID:** 104082552
- Tutorial session:** Tuesday 06:30PM

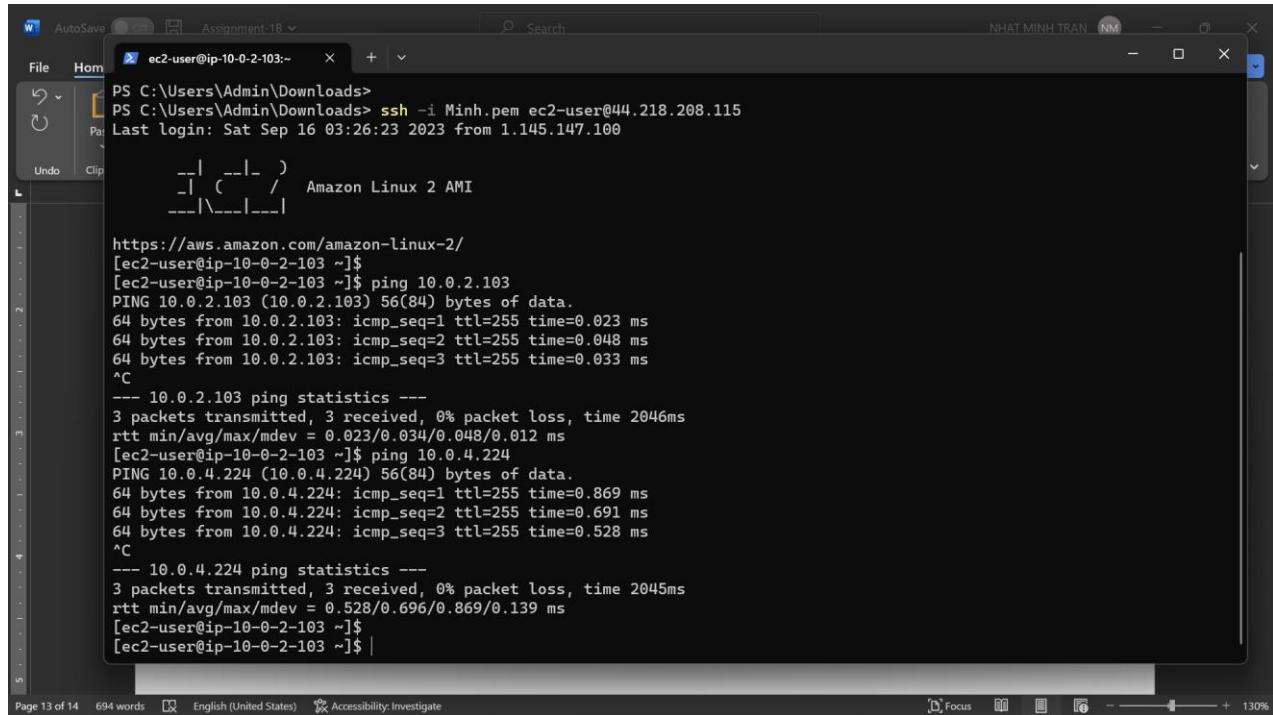
Below this, there is a table titled "Uploaded photos:" with the following data:

Photo	Name	Description	Creation date	Keywords
	title	description	2023-09-16	logo
	title	description	2023-09-16	logo

Figure 22: Functionality of the website

## 2.4 – Testing

To test our website and Network ACL configured correctly, the website can be ping between two IP.



The screenshot shows a terminal window titled "Assignment-1B" with the command "ssh -i Minh.pem ec2-user@44.218.208.115" running. The session logs show the user navigating to a local directory and performing a ping test between two hosts (10.0.2.103 and 10.0.4.224). The ping results show 3 packets transmitted with 0% packet loss and times ranging from 0.023ms to 0.869ms. The terminal interface includes standard Windows-style navigation buttons and a status bar at the bottom.

```
PS C:\Users\Admin\Downloads>
PS C:\Users\Admin\Downloads> ssh -i Minh.pem ec2-user@44.218.208.115
Last login: Sat Sep 16 03:26:23 2023 from 1.145.147.100
              _.-|_ _.- )
      _.-| (   /   Amazon Linux 2 AMI
      _.-| \_ |__|_|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-2-103 ~]$ 
[ec2-user@ip-10-0-2-103 ~]$ ping 10.0.2.103
PING 10.0.2.103 (10.0.2.103) 56(84) bytes of data.
64 bytes from 10.0.2.103: icmp_seq=1 ttl=255 time=0.023 ms
64 bytes from 10.0.2.103: icmp_seq=2 ttl=255 time=0.048 ms
64 bytes from 10.0.2.103: icmp_seq=3 ttl=255 time=0.033 ms
^C
--- 10.0.2.103 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2046ms
rtt min/avg/max/mdev = 0.023/0.034/0.048/0.012 ms
[ec2-user@ip-10-0-2-103 ~]$ ping 10.0.4.224
PING 10.0.4.224 (10.0.4.224) 56(84) bytes of data.
64 bytes from 10.0.4.224: icmp_seq=1 ttl=255 time=0.869 ms
64 bytes from 10.0.4.224: icmp_seq=2 ttl=255 time=0.691 ms
64 bytes from 10.0.4.224: icmp_seq=3 ttl=255 time=0.528 ms
^C
--- 10.0.4.224 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2045ms
rtt min/avg/max/mdev = 0.528/0.696/0.869/0.139 ms
[ec2-user@ip-10-0-2-103 ~]$ 
[ec2-user@ip-10-0-2-103 ~]$ |
```

Figure 23: Ping between website successfully

Additional links for markings:

- + <http://44.218.208.115/phpmyadmin>
- + <http://44.218.208.115/cos20019/photoalbum/album.php>

