Assignment 1b - Creating and deploying Photo Album website onto a simple AWS infrastructure.

COS 20019- Cloud Computing Architecture

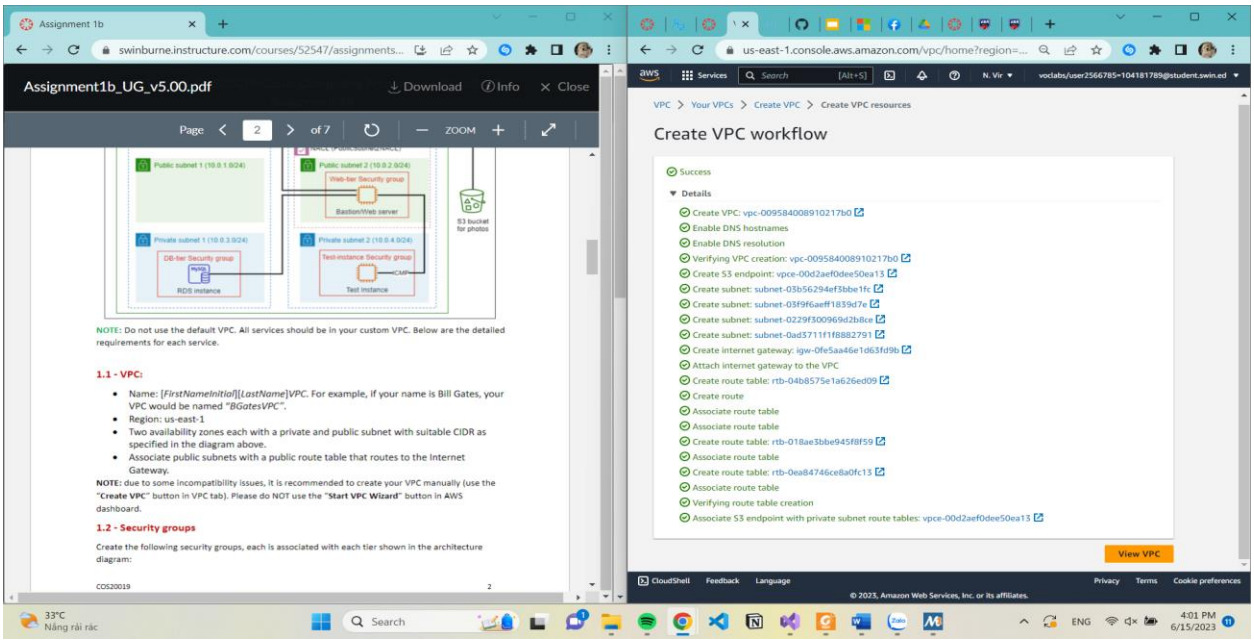
Nguyen Manh Dung

20/5/2023

So this is all my step to finish Assignment 1b, belong with detailed explaination

1.1 VPC

I have created VPC which have my name and required instruction.



1.2 Create Security groups

5 security groups has been created which fits assignment requirement.

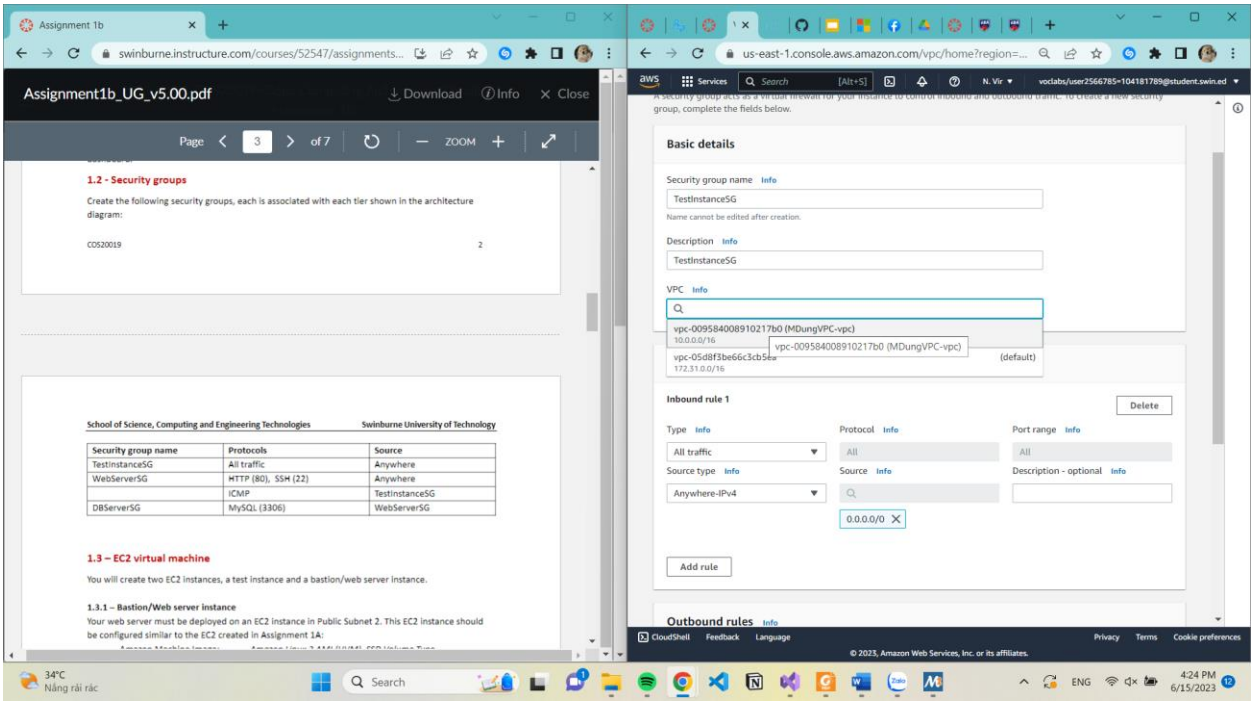


Figure 1: TestInstanceSG security group

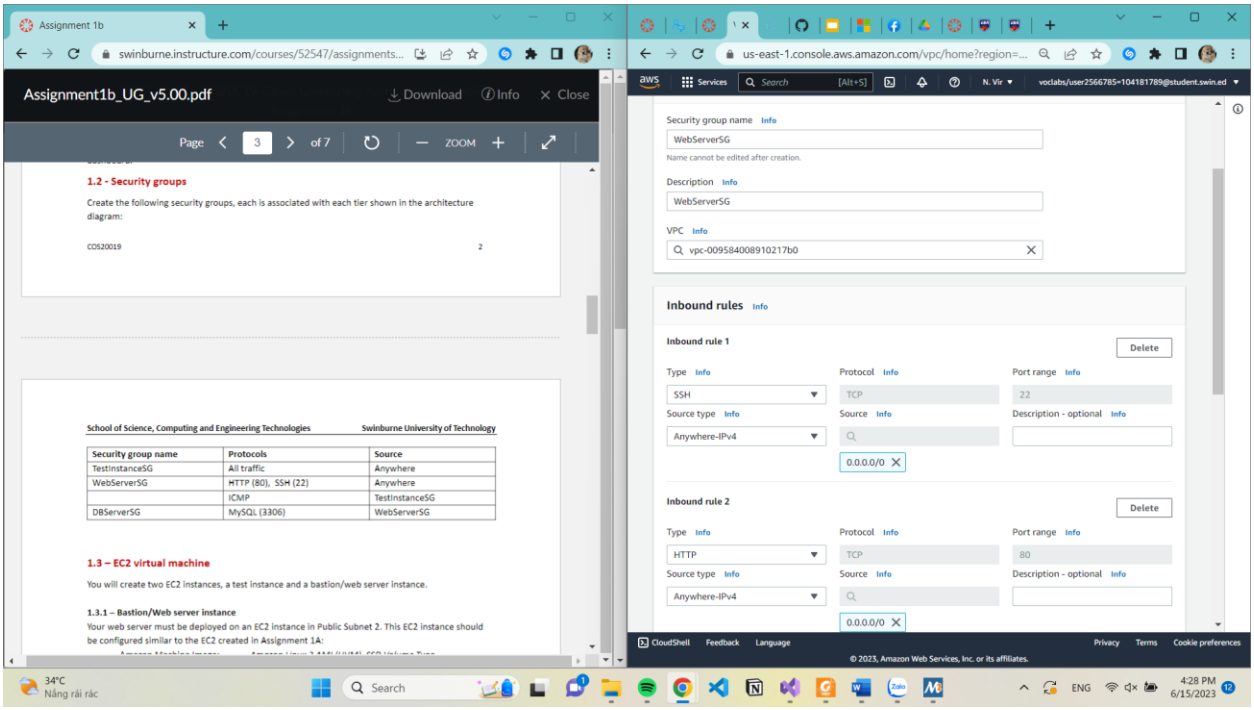
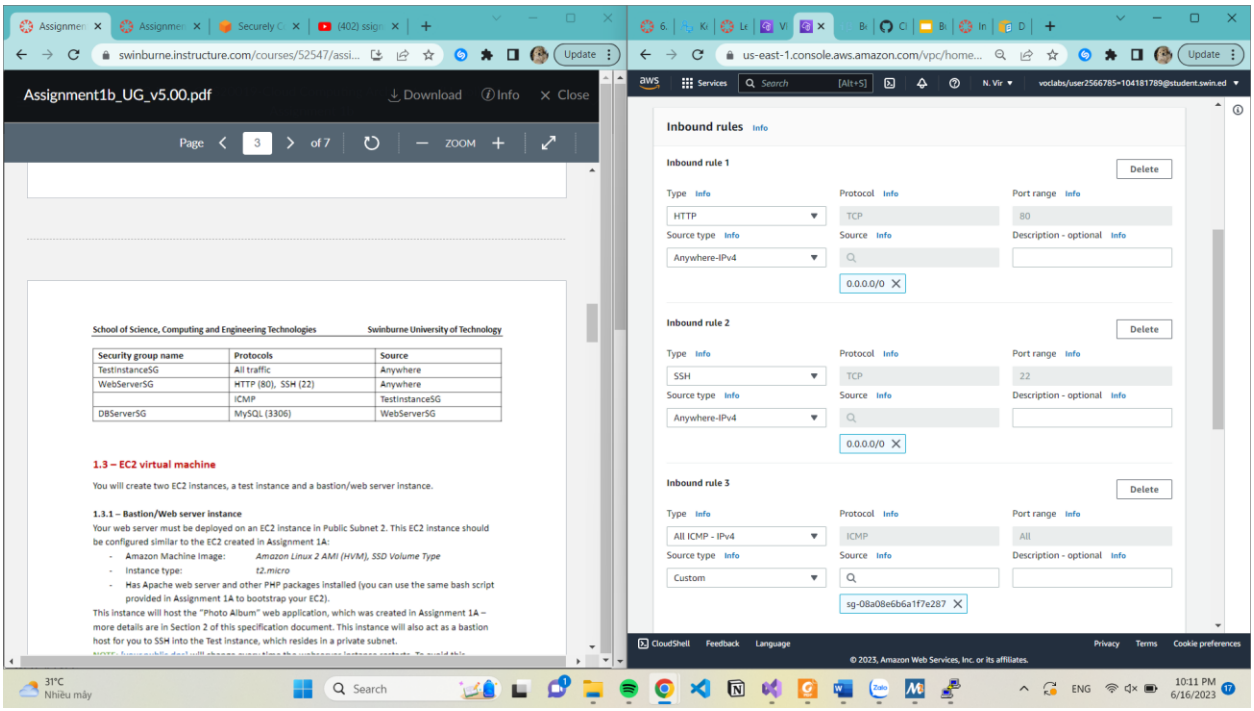


Figure 2:WebServerSG security group, with inbound rules below



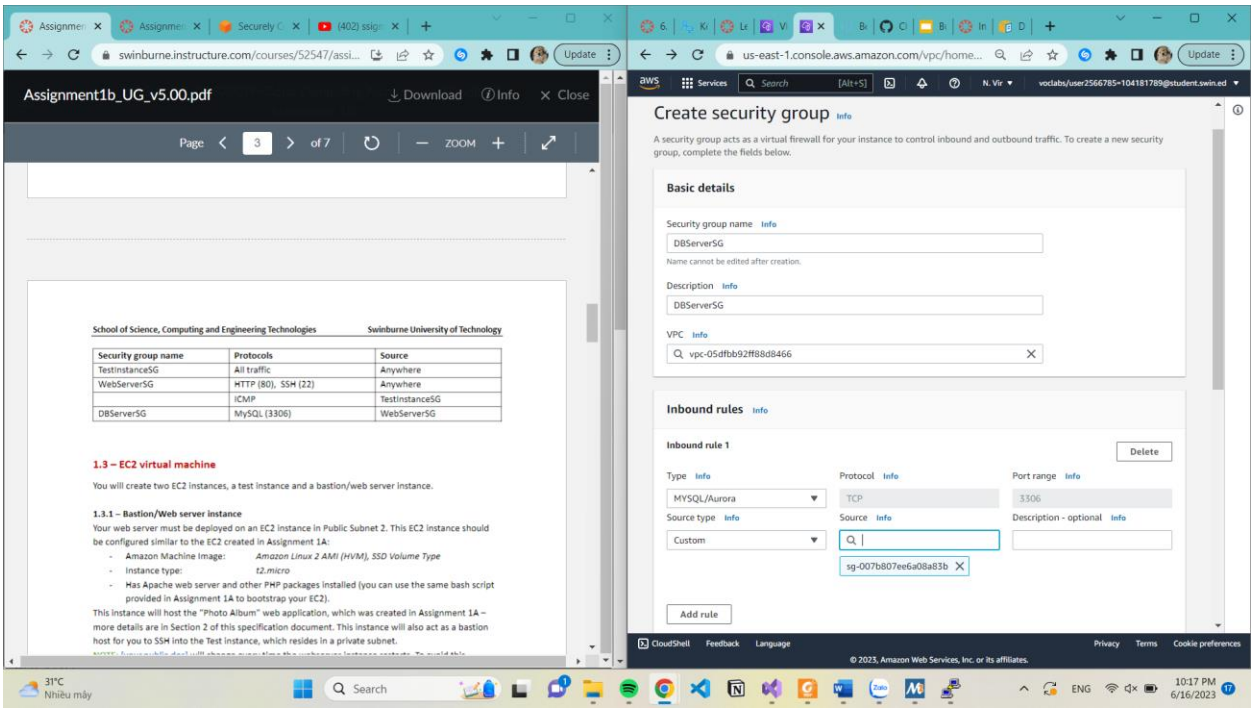
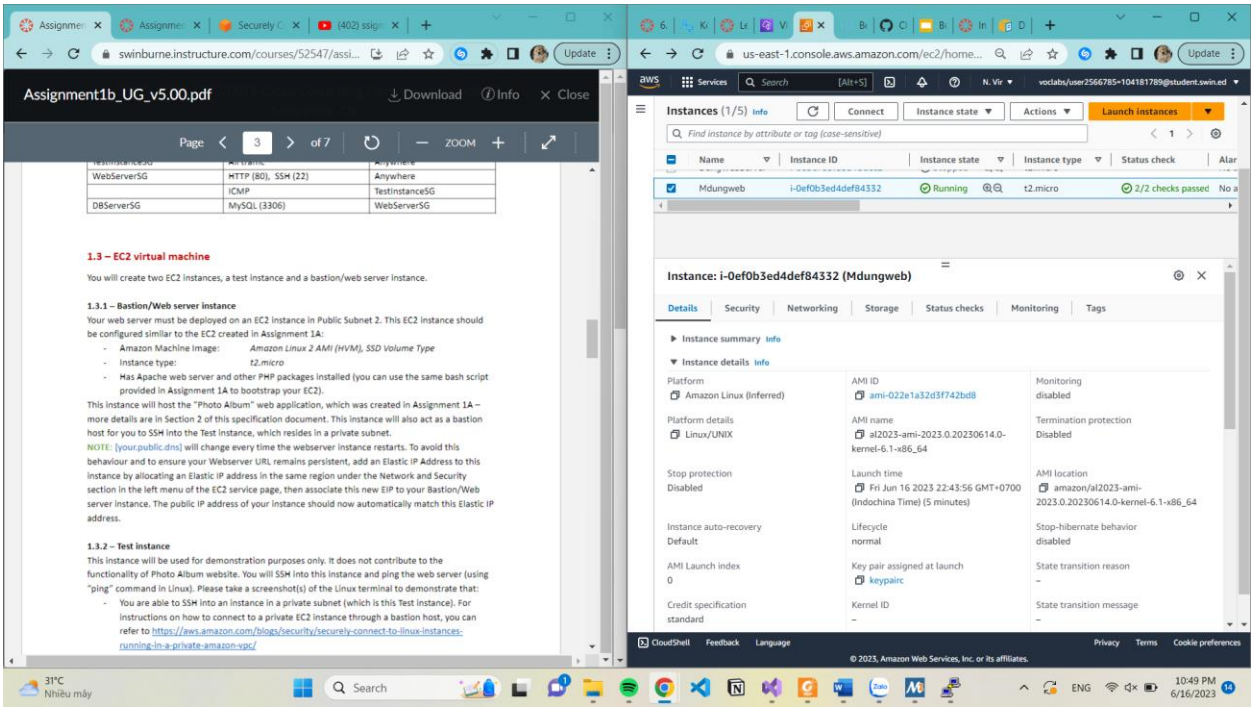


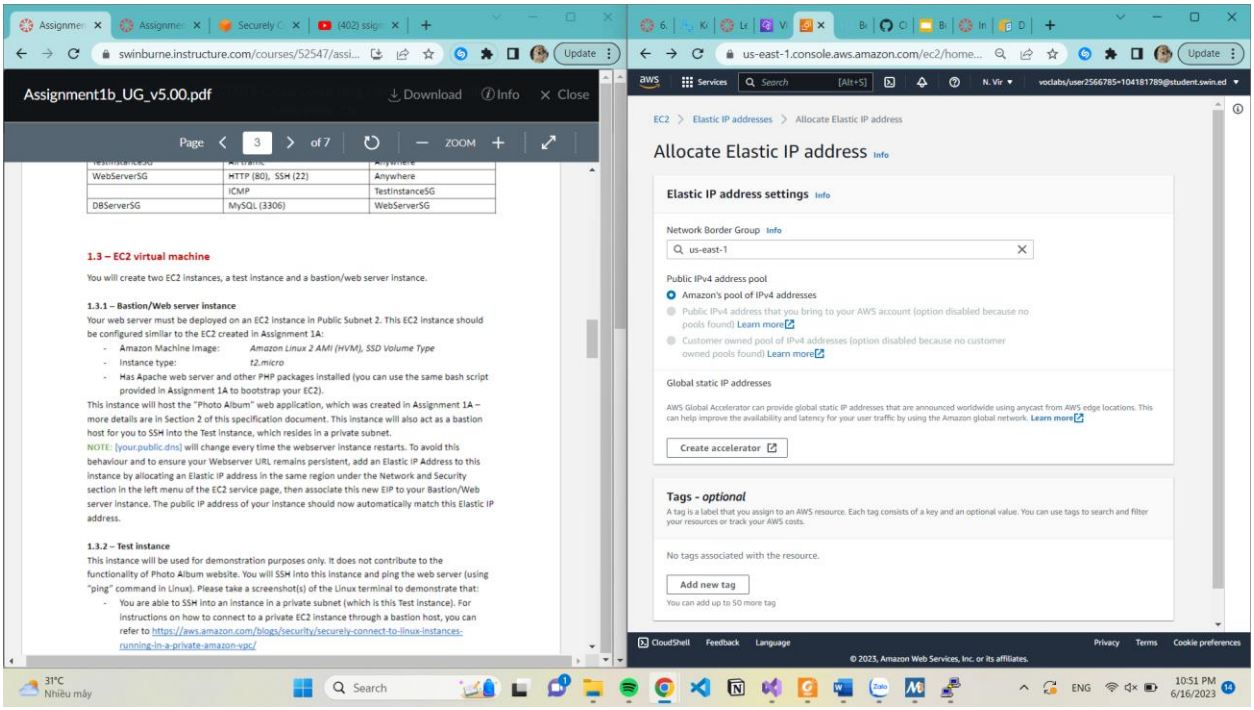
Figure: DBServerSG

1.3 EC2 virtual instance

I have to create two instance which stands for Bastion/Web sever and Test.



- I have to allocate elastic IP address to avoid my IP to change everytime instance restart.



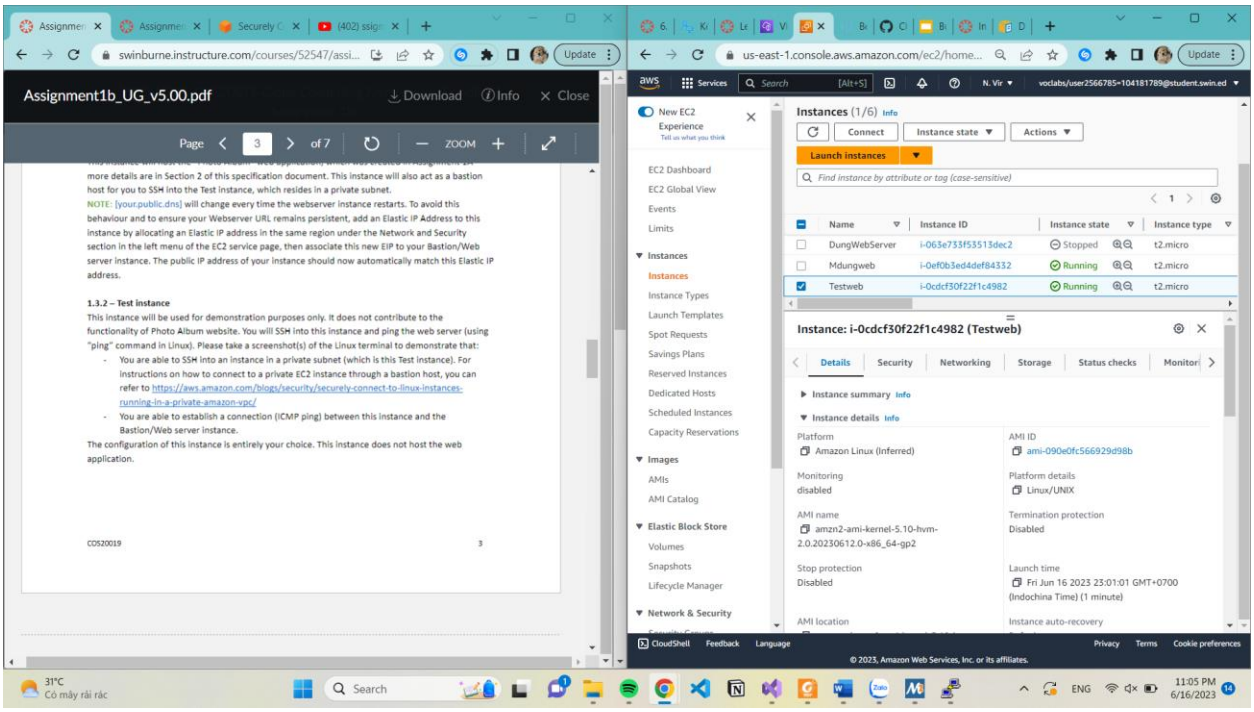


Figure: Test instance sucessful created

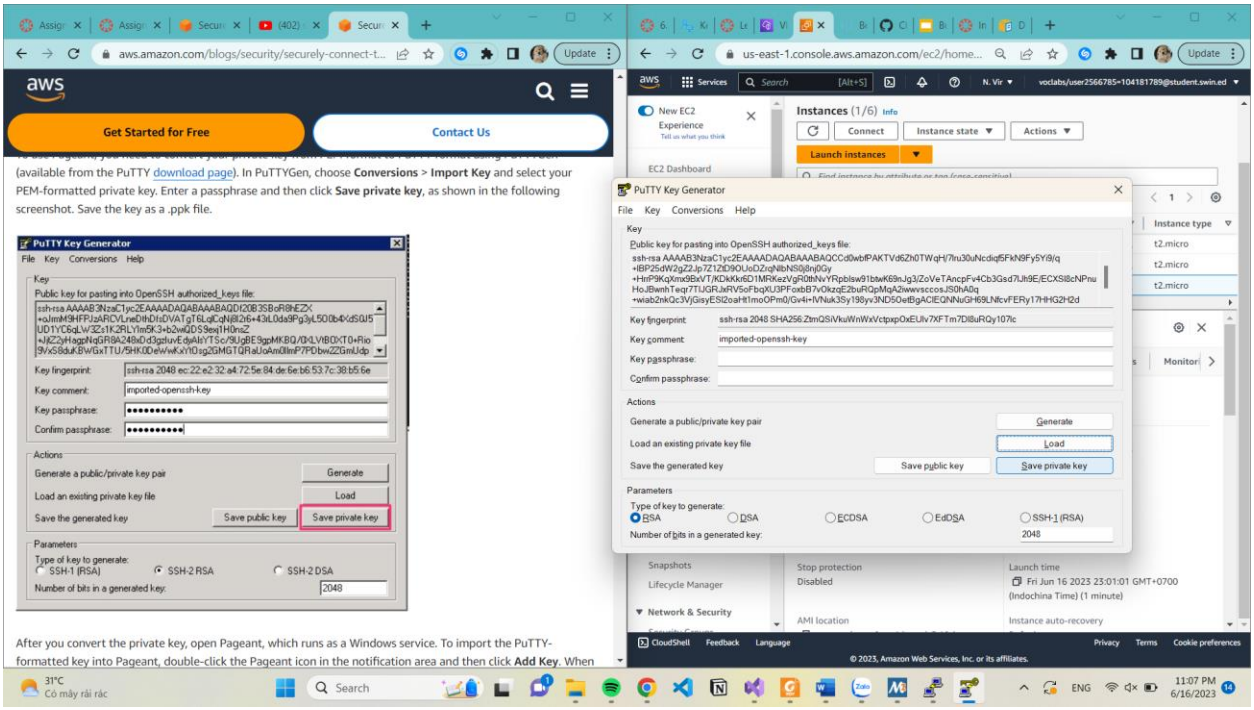


Figure: Above screenshotted is the step to convert the key pair that i created in previous step from .pem to .pkk

1.3.2 This step is to access SSH of Test instance

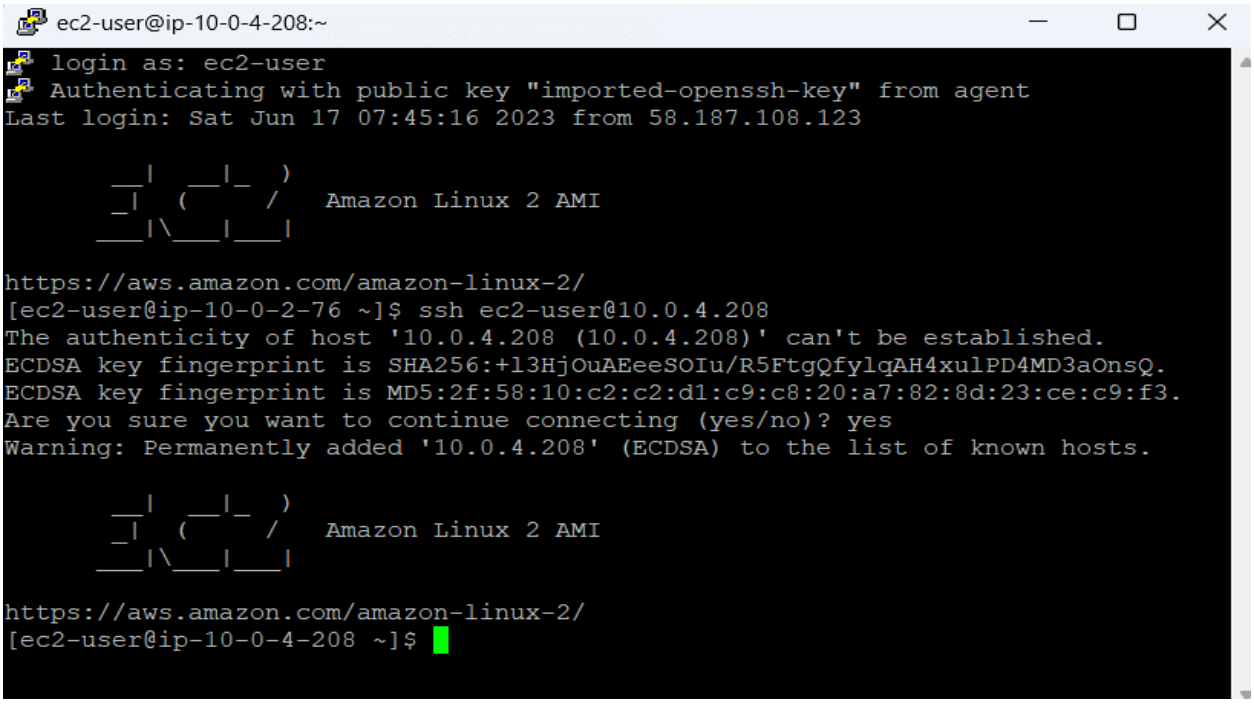


Figure: Access instance

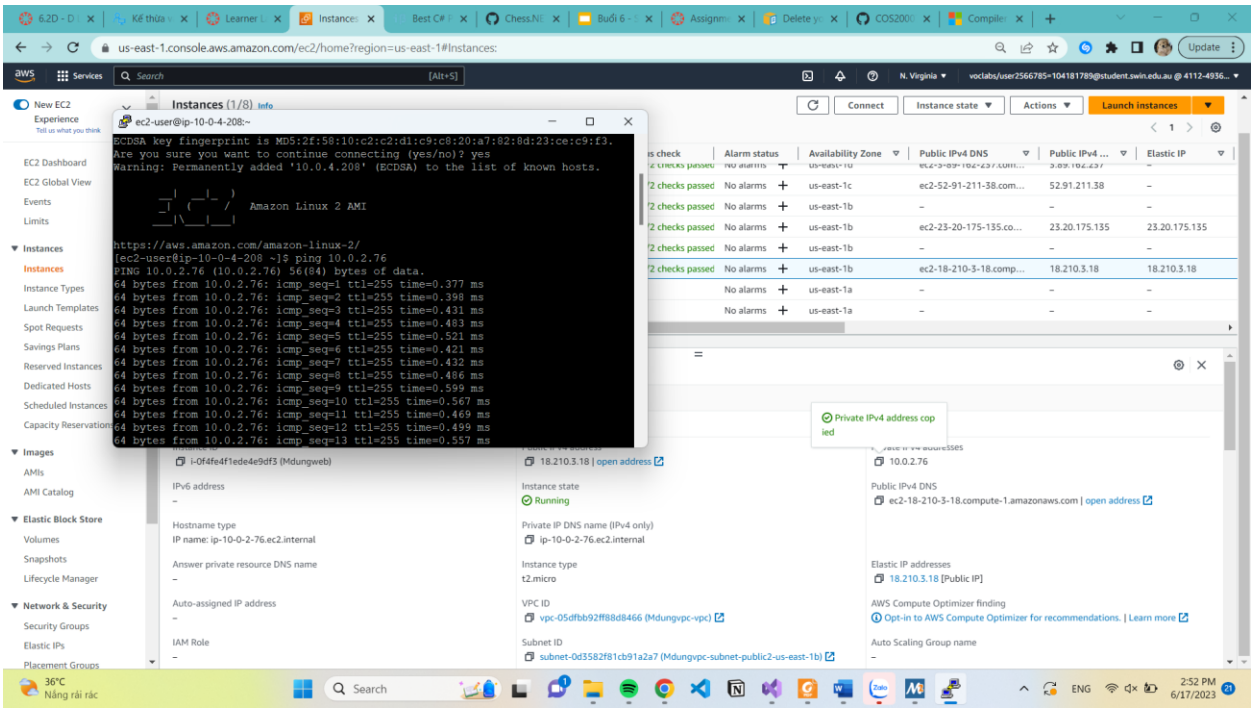
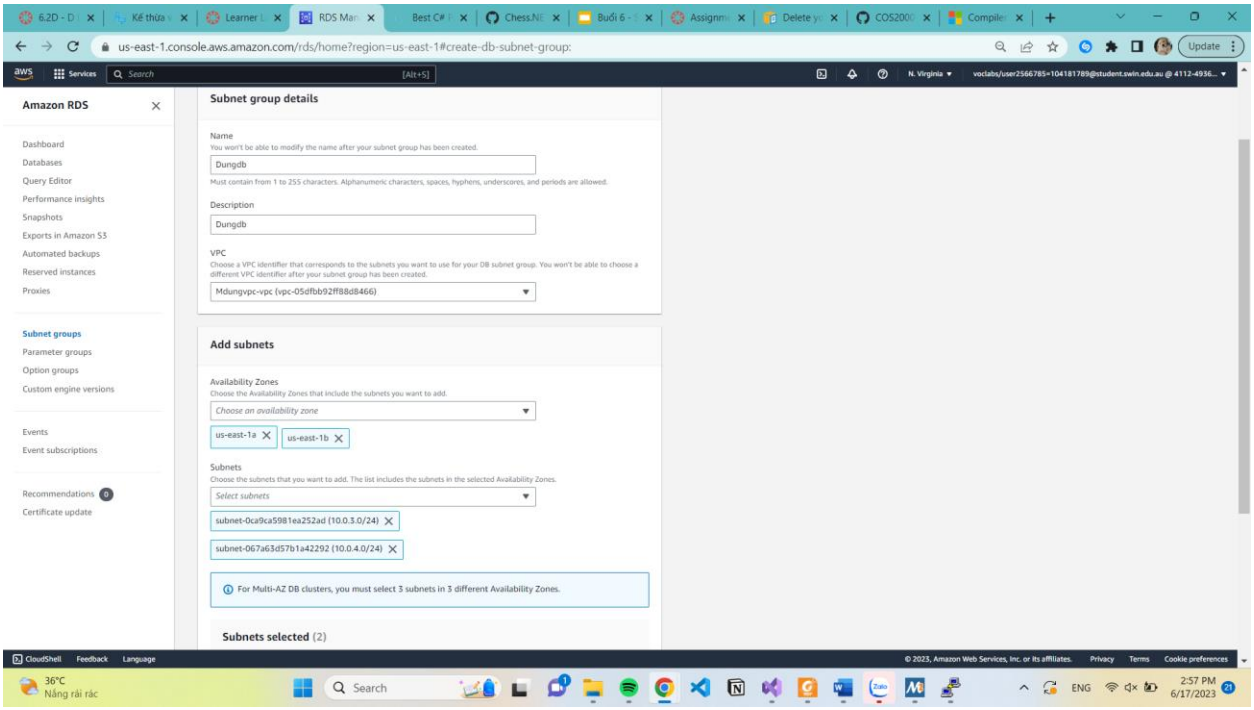
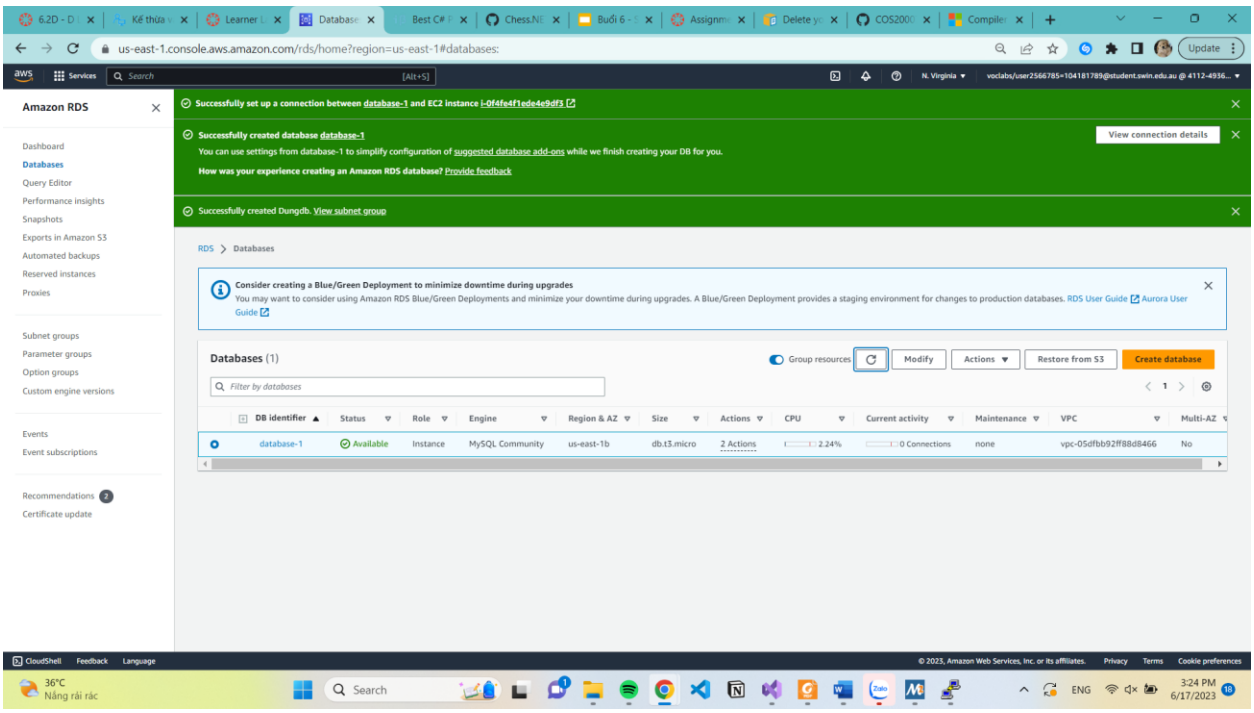


Figure: Establish a connection (ICMP ping) between Test instance and Web server instance

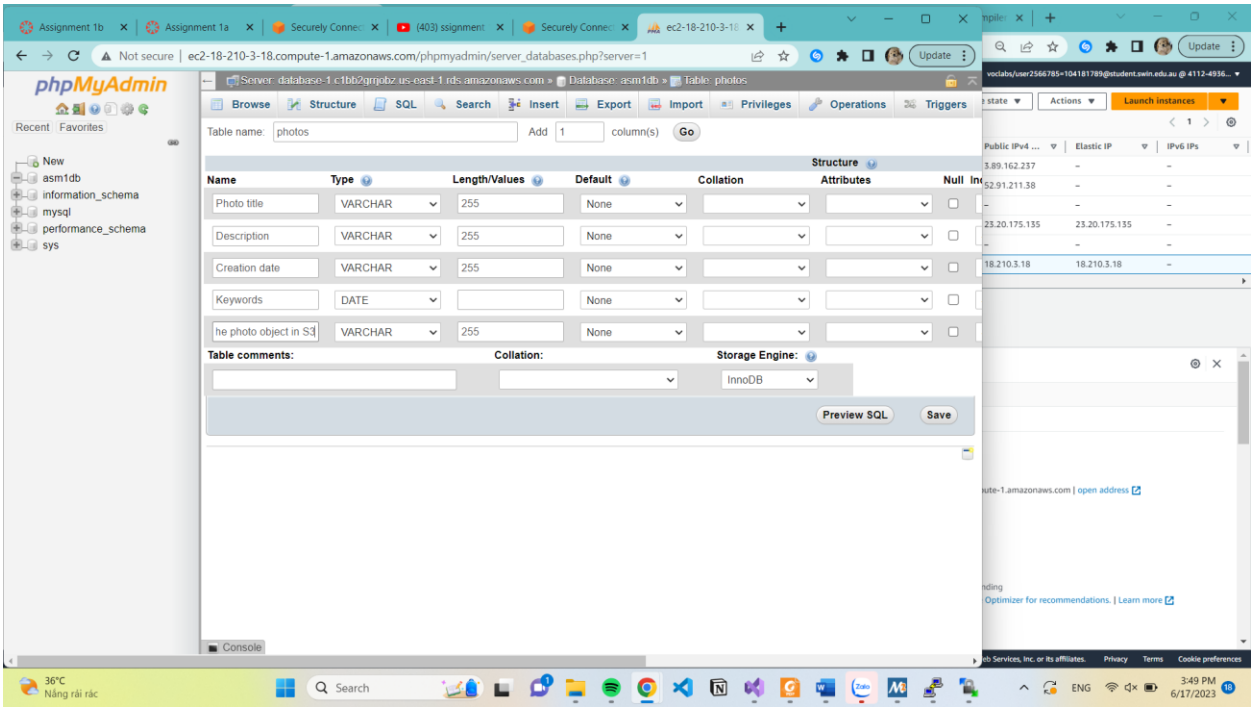
1.4 Create RDS database instance



Create database

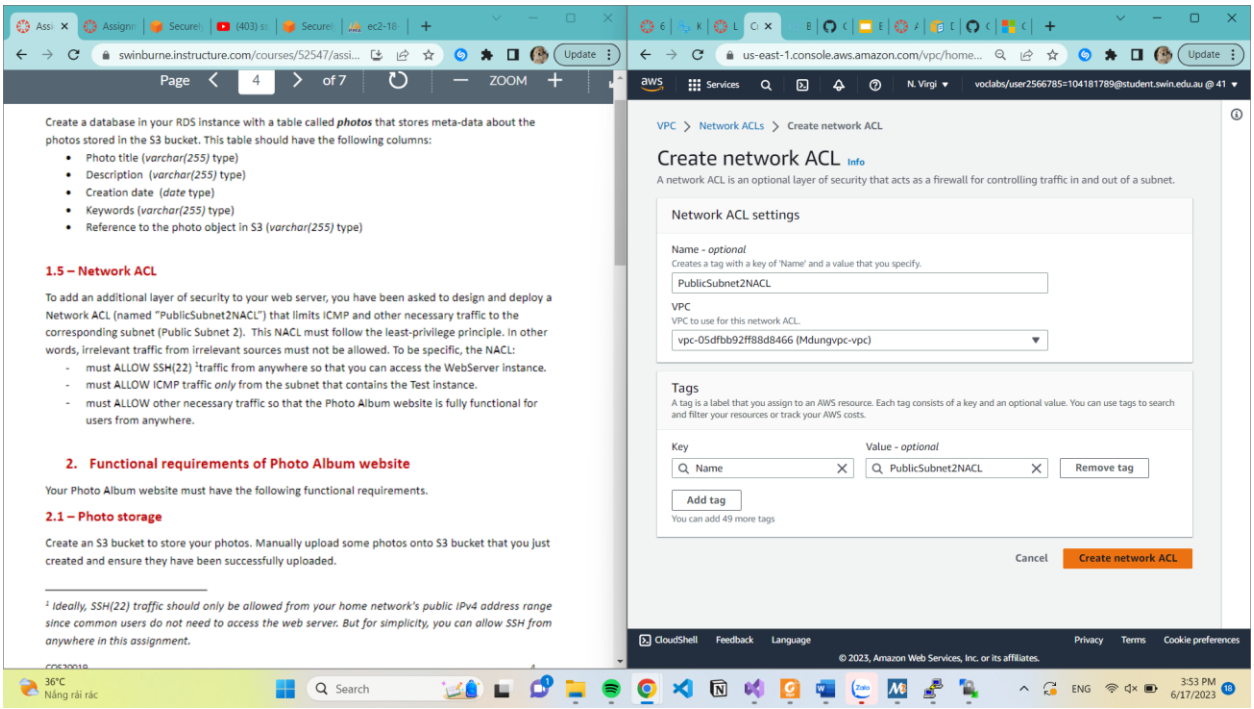


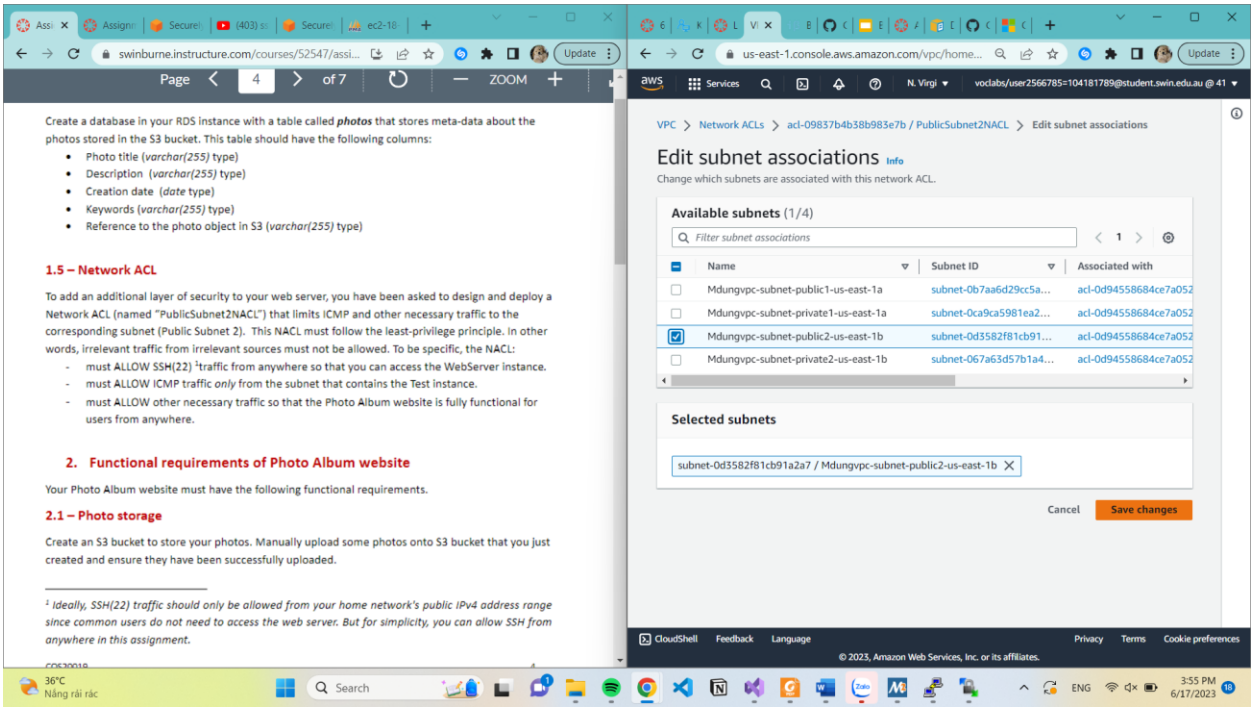
Create a database in your RDS instance with a table called photos that stores meta-data about the photos stored in the S3 bucket.

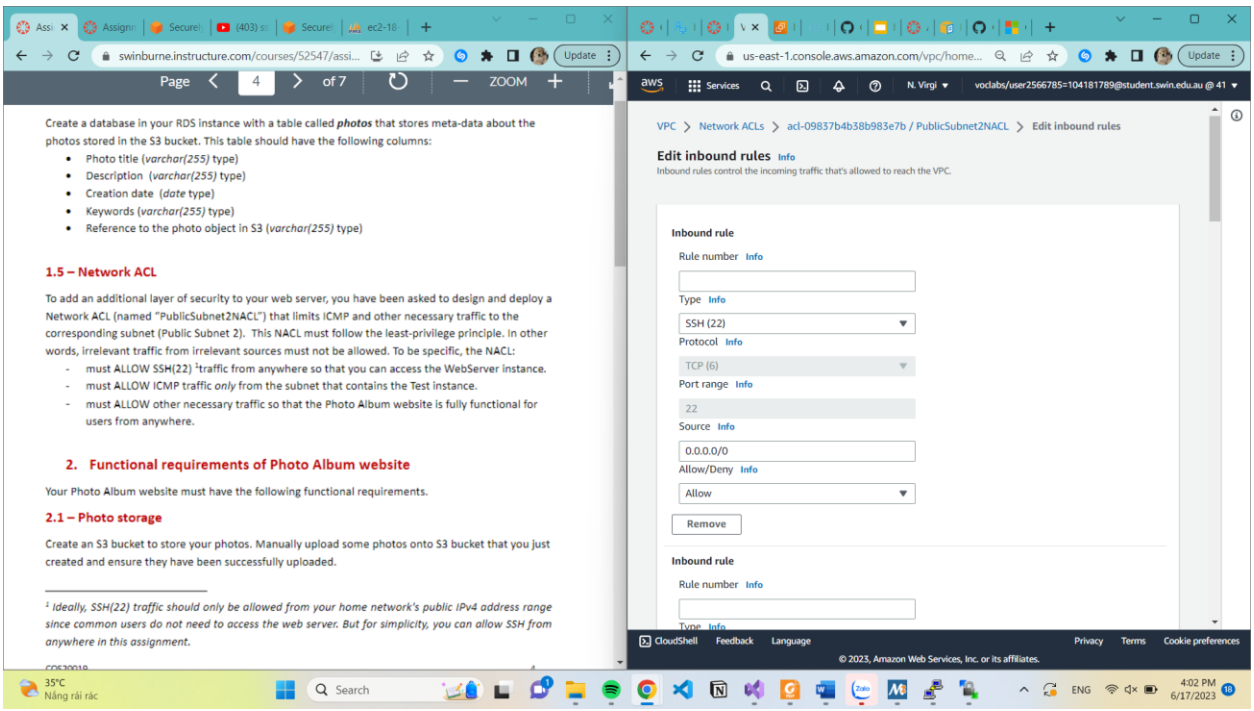


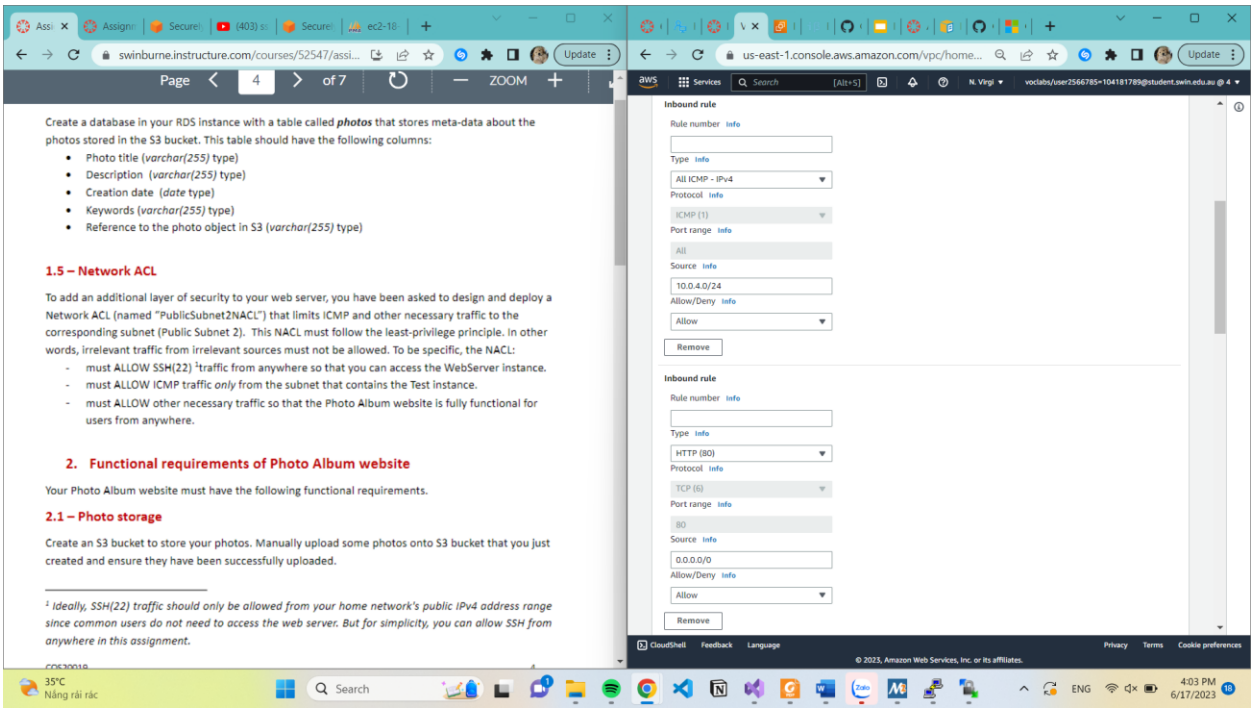
1.5 Create Network ACL

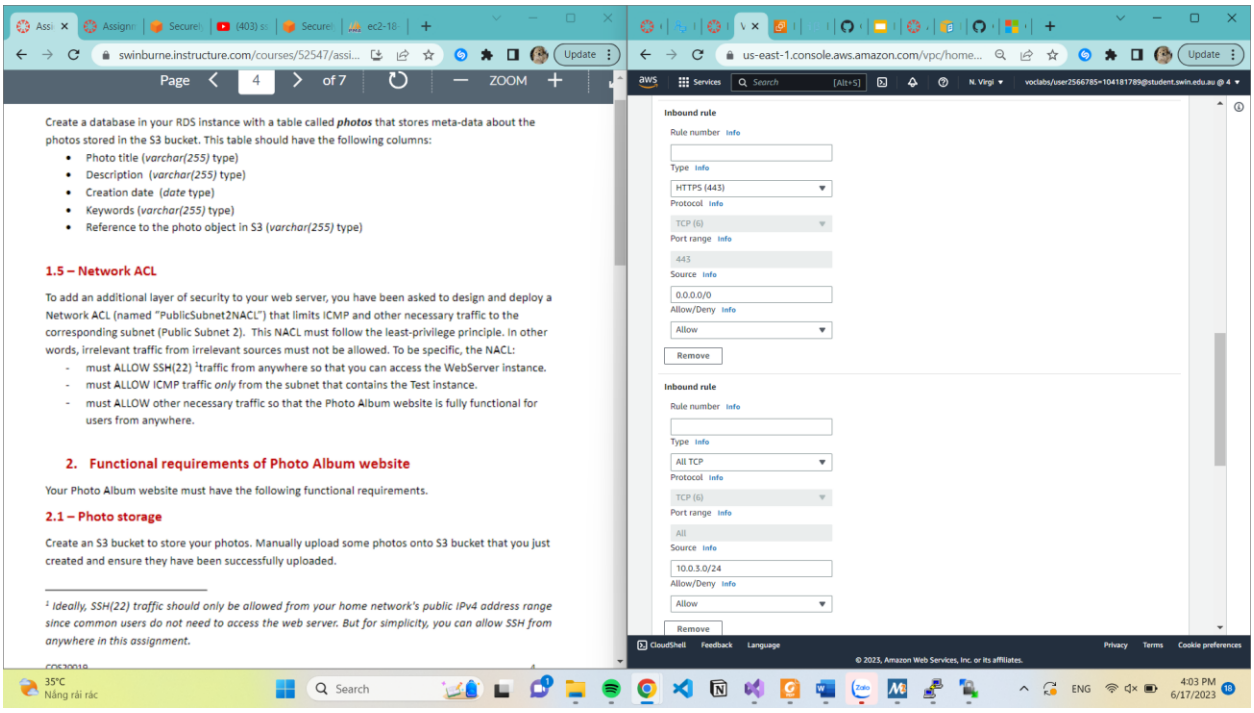
This step is to add an additional layer of security to your web server called Network ACL, below is all the step to deploy it, with all requirement be filled.

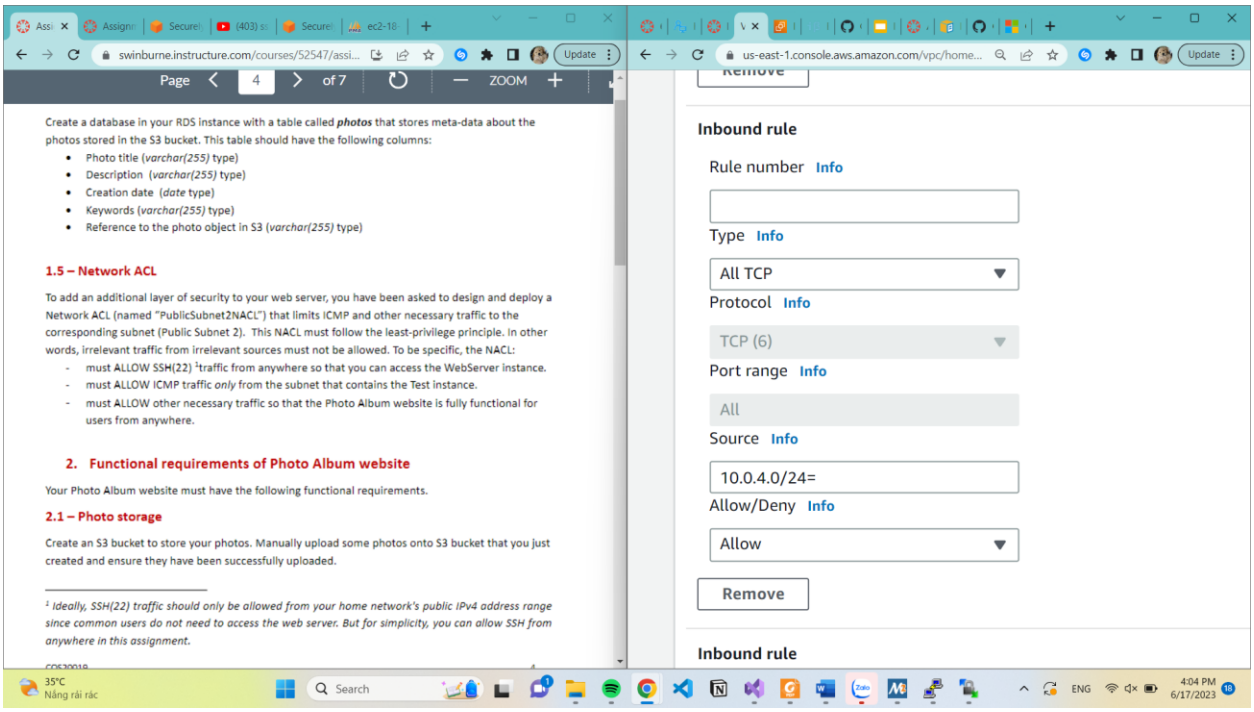


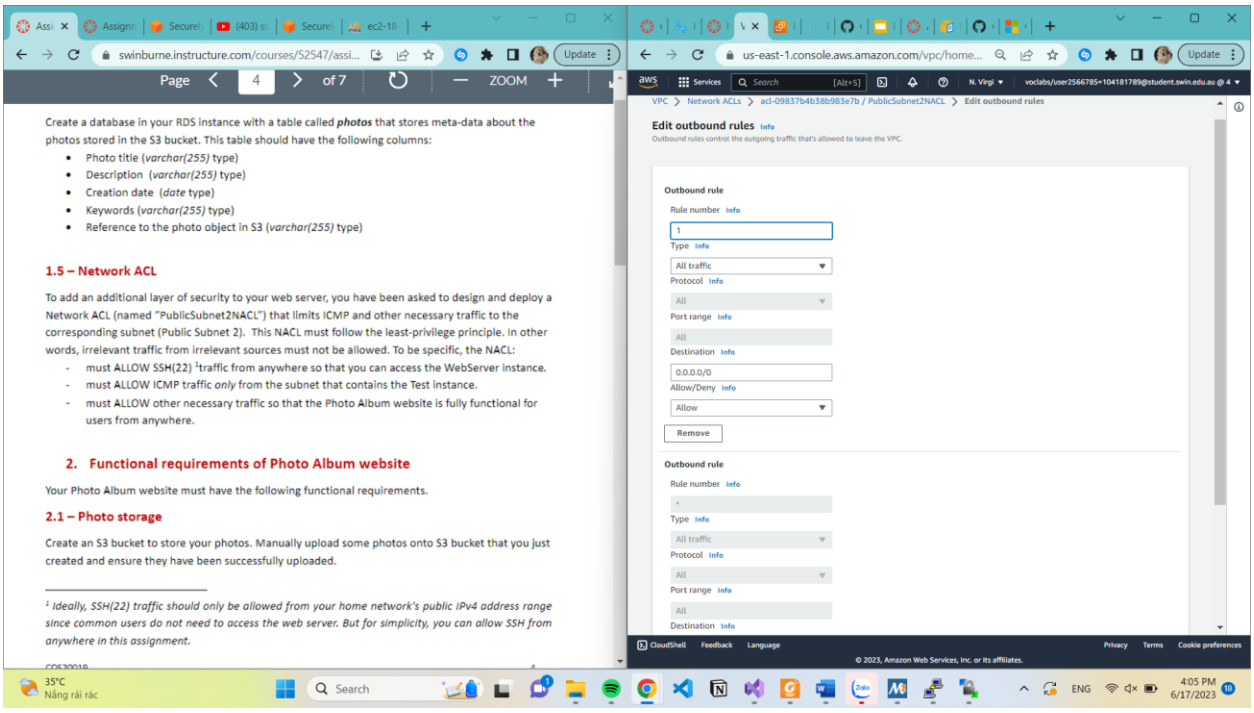

swinburne.instructure.com/courses/52547/assi...
Page 4 of 7
ZOOM
Create a database in your RDS instance with a table called photos that stores meta-data about the photos stored in the S3 bucket. This table should have the following columns:
Photo title (varchar(255) type)
Description (varchar(255) type)
Creation date (date type)
Keywords (varchar(255) type)
Reference to the photo object in S3 (varchar(255) type)
1.5 – Network ACL
To add an additional layer of security to your web server, you have been asked to design and deploy a Network ACL (named "PublicSubnet2NACL") that limits ICMP and other necessary traffic to the corresponding subnet (Public Subnet 2). This NACL must follow the least-privilege principle. In other words, irrelevant traffic from irrelevant sources must not be allowed. To be specific, the NACL:
must ALLOW SSH(22) [1]traffic from anywhere so that you can access the WebServer instance.
must ALLOW ICMP traffic only from the subnet that contains the Test instance.
must ALLOW other necessary traffic so that the Photo Album website is fully functional for users from anywhere.
2. Functional requirements of Photo Album website
Your Photo Album website must have the following functional requirements.
2.1 – Photo storage
Create an S3 bucket to store your photos. Manually upload some photos onto S3 bucket that you just created and ensure they have been successfully uploaded.
[1] Ideally, SSH(22) traffic should only be allowed from your home network's public IPv4 address range since common users do not need to access the web server. But for simplicity, you can allow SSH from anywhere in this assignment.
us-east-1.console.aws.amazon.com/vpc/home...
VPC > Network ACLs > acl-09837b4b38b983e7b / PublicSubnet2NACL > Edit subnet associations
Edit subnet associations Info
Change which subnets are associated with this network ACL.
Available subnets (1/4)
Filter subnet associations
Name
Subnet ID
Associated with
Mdungvpc-subnet-public1-us-east-1a
subnet-0b7aa6d29cc5a...
acl-0d94558684ce7a052
Mdungvpc-subnet-private1-us-east-1a
subnet-0ca9ca5981ea2...
acl-0d94558684ce7a052
Mdungvpc-subnet-public2-us-east-1b
subnet-0d3582f81cb91...
acl-0d94558684ce7a052
Mdungvpc-subnet-private2-us-east-1b
subnet-067a63d57b1a4...
acl-0d94558684ce7a052
Selected subnets
subnet-0d3582f81cb91a2a7 / Mdungvpc-subnet-public2-us-east-1b
Cancel
Save changes
CloudShell
Feedback
Language
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.


swinburne.instructure.com/courses/52547/assi...
Page 4 of 7
ZOOM
Create a database in your RDS instance with a table called photos that stores meta-data about the photos stored in the S3 bucket. This table should have the following columns:
Photo title (varchar(255) type)
Description (varchar(255) type)
Creation date (date type)
Keywords (varchar(255) type)
Reference to the photo object in S3 (varchar(255) type)
1.5 – Network ACL
To add an additional layer of security to your web server, you have been asked to design and deploy a Network ACL (named "PublicSubnet2NACL") that limits ICMP and other necessary traffic to the corresponding subnet (Public Subnet 2). This NACL must follow the least-privilege principle. In other words, irrelevant traffic from irrelevant sources must not be allowed. To be specific, the NACL:
must ALLOW SSH(22) [1]traffic from anywhere so that you can access the WebServer instance.
must ALLOW ICMP traffic only from the subnet that contains the Test instance.
must ALLOW other necessary traffic so that the Photo Album website is fully functional for users from anywhere.
2. Functional requirements of Photo Album website
Your Photo Album website must have the following functional requirements.
2.1 – Photo storage
Create an S3 bucket to store your photos. Manually upload some photos onto S3 bucket that you just created and ensure they have been successfully uploaded.
[1] Ideally, SSH(22) traffic should only be allowed from your home network's public IPv4 address range since common users do not need to access the web server. But for simplicity, you can allow SSH from anywhere in this assignment.
us-east-1.console.aws.amazon.com/vpc/home...
VPC > Network ACLs > acl-09837b4b38b983e7b / PublicSubnet2NACL > Edit inbound rules
Edit inbound rules Info
Inbound rules control the incoming traffic that's allowed to reach the VPC.
Inbound rule
Rule number Info
Type Info
SSH (22)
Protocol Info
TCP (6)
Port range Info
22
Source Info
0.0.0.0/0
Allow/Deny Info
Allow
Remove
Inbound rule
Rule number Info
Type Info
CloudShell
Feedback
Language
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.


Create a database in your RDS instance with a table called photos that stores meta-data about the photos stored in the S3 bucket. This table should have the following columns:
Photo title (varchar(255) type)
Description (varchar(255) type)
Creation date (date type)
Keywords (varchar(255) type)
Reference to the photo object in S3 (varchar(255) type)
1.5 – Network ACL
To add an additional layer of security to your web server, you have been asked to design and deploy a Network ACL (named "PublicSubnet2NACL") that limits ICMP and other necessary traffic to the corresponding subnet (Public Subnet 2). This NACL must follow the least-privilege principle. In other words, irrelevant traffic from irrelevant sources must not be allowed. To be specific, the NACL:
must ALLOW SSH(22) [1]traffic from anywhere so that you can access the WebServer instance.
must ALLOW ICMP traffic only from the subnet that contains the Test instance.
must ALLOW other necessary traffic so that the Photo Album website is fully functional for users from anywhere.
2. Functional requirements of Photo Album website
Your Photo Album website must have the following functional requirements.
2.1 – Photo storage
Create an S3 bucket to store your photos. Manually upload some photos onto S3 bucket that you just created and ensure they have been successfully uploaded.
[1] Ideally, SSH(22) traffic should only be allowed from your home network's public IPv4 address range since common users do not need to access the web server. But for simplicity, you can allow SSH from anywhere in this assignment.
Inbound rule
Rule number
Type
All ICMP - IPv4
Protocol
Port range
Source
10.0.4.0/24
Allow/Deny
Allow
Remove
Inbound rule
Rule number
Type
HTTP (80)
Protocol
Port range
80
Source
0.0.0.0/0
Allow/Deny
Allow
Remove


Create a database in your RDS instance with a table called photos that stores meta-data about the photos stored in the S3 bucket. This table should have the following columns:
Photo title (varchar(255) type)
Description (varchar(255) type)
Creation date (date type)
Keywords (varchar(255) type)
Reference to the photo object in S3 (varchar(255) type)
1.5 – Network ACL
To add an additional layer of security to your web server, you have been asked to design and deploy a Network ACL (named "PublicSubnet2NACL") that limits ICMP and other necessary traffic to the corresponding subnet (Public Subnet 2). This NACL must follow the least-privilege principle. In other words, irrelevant traffic from irrelevant sources must not be allowed. To be specific, the NACL:
must ALLOW SSH(22) [1]traffic from anywhere so that you can access the WebServer instance.
must ALLOW ICMP traffic only from the subnet that contains the Test instance.
must ALLOW other necessary traffic so that the Photo Album website is fully functional for users from anywhere.
2. Functional requirements of Photo Album website
Your Photo Album website must have the following functional requirements.
2.1 – Photo storage
Create an S3 bucket to store your photos. Manually upload some photos onto S3 bucket that you just created and ensure they have been successfully uploaded.
[1] Ideally, SSH(22) traffic should only be allowed from your home network's public IPv4 address range since common users do not need to access the web server. But for simplicity, you can allow SSH from anywhere in this assignment.
Inbound rule
Rule number
Type
HTTPS (443)
Protocol
Port range
443
Source
0.0.0.0/0
Allow/Deny
Allow
Remove
Inbound rule
Rule number
Type
All TCP
Protocol
Port range
All
Source
10.0.3.0/24
Allow/Deny
Allow
Remove

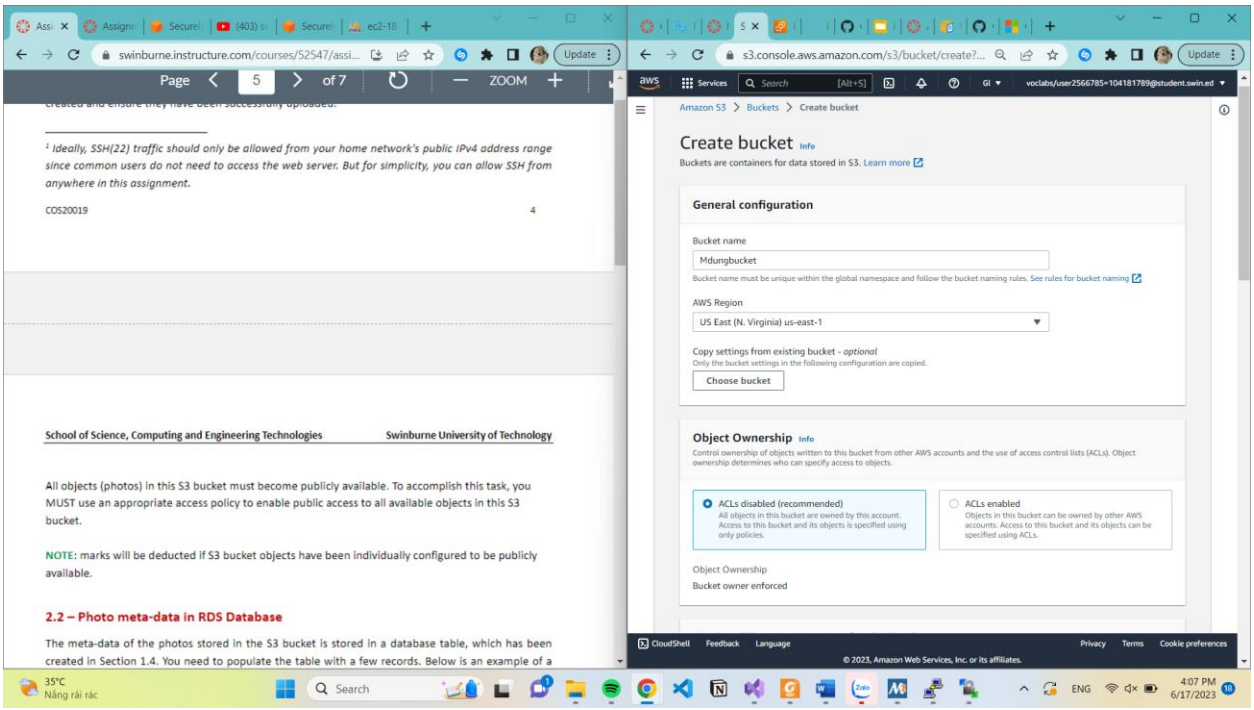

Page 4 of 7
ZOOM
Create a database in your RDS instance with a table called photos that stores meta-data about the photos stored in the S3 bucket. This table should have the following columns:
Photo title (varchar(255) type)
Description (varchar(255) type)
Creation date (date type)
Keywords (varchar(255) type)
Reference to the photo object in S3 (varchar(255) type)
1.5 – Network ACL
To add an additional layer of security to your web server, you have been asked to design and deploy a Network ACL (named "PublicSubnet2NACL") that limits ICMP and other necessary traffic to the corresponding subnet (Public Subnet 2). This NACL must follow the least-privilege principle. In other words, irrelevant traffic from irrelevant sources must not be allowed. To be specific, the NACL:
must ALLOW SSH(22) [1]traffic from anywhere so that you can access the WebServer instance.
must ALLOW ICMP traffic only from the subnet that contains the Test instance.
must ALLOW other necessary traffic so that the Photo Album website is fully functional for users from anywhere.
2. Functional requirements of Photo Album website
Your Photo Album website must have the following functional requirements.
2.1 – Photo storage
Create an S3 bucket to store your photos. Manually upload some photos onto S3 bucket that you just created and ensure they have been successfully uploaded.
[1] Ideally, SSH(22) traffic should only be allowed from your home network's public IPv4 address range since common users do not need to access the web server. But for simplicity, you can allow SSH from anywhere in this assignment.
Inbound rule
Rule number Info
Type Info
All TCP
Protocol Info
TCP (6)
Port range Info
All
Source Info
10.0.4.0/24=
Allow/Deny Info
Allow
Remove
Inbound rule


Page 4 of 7
ZOOM
Create a database in your RDS instance with a table called photos that stores meta-data about the photos stored in the S3 bucket. This table should have the following columns:
Photo title (varchar(255) type)
Description (varchar(255) type)
Creation date (date type)
Keywords (varchar(255) type)
Reference to the photo object in S3 (varchar(255) type)
1.5 – Network ACL
To add an additional layer of security to your web server, you have been asked to design and deploy a Network ACL (named "PublicSubnet2NACL") that limits ICMP and other necessary traffic to the corresponding subnet (Public Subnet 2). This NACL must follow the least-privilege principle. In other words, irrelevant traffic from irrelevant sources must not be allowed. To be specific, the NACL:
must ALLOW SSH(22) [1]traffic from anywhere so that you can access the WebServer instance.
must ALLOW ICMP traffic only from the subnet that contains the Test instance.
must ALLOW other necessary traffic so that the Photo Album website is fully functional for users from anywhere.
2. Functional requirements of Photo Album website
Your Photo Album website must have the following functional requirements.
2.1 – Photo storage
Create an S3 bucket to store your photos. Manually upload some photos onto S3 bucket that you just created and ensure they have been successfully uploaded.
[1] Ideally, SSH(22) traffic should only be allowed from your home network's public IPv4 address range since common users do not need to access the web server. But for simplicity, you can allow SSH from anywhere in this assignment.
Edit outbound rules
Outbound rule
Rule number
Type
All traffic
Protocol
Port range
Destination
0.0.0.0/0
Allow/Deny
Allow
Remove
Outbound rule
Rule number
Type
All traffic
Protocol
Port range
Destination
CloudShell
Feedback
Language
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.

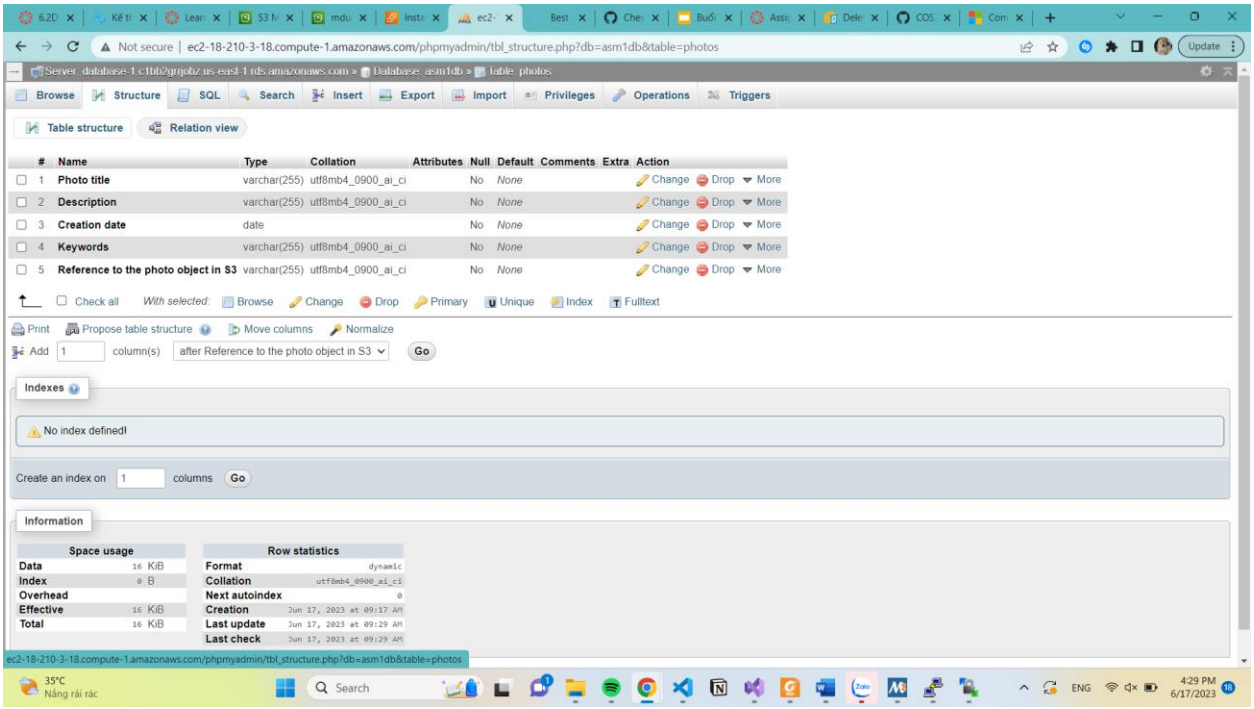
2. Functional requirements of Photo Album website.

2.1 Photo storage

Create an S3 bucket to store photos

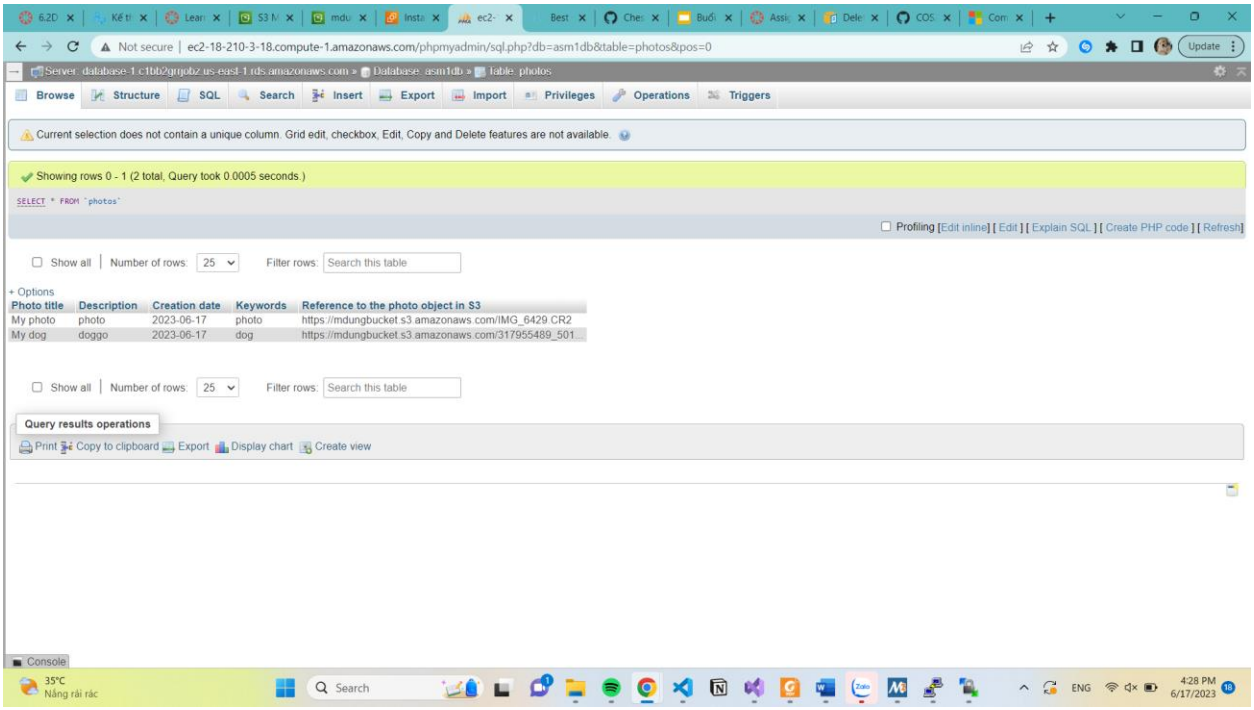


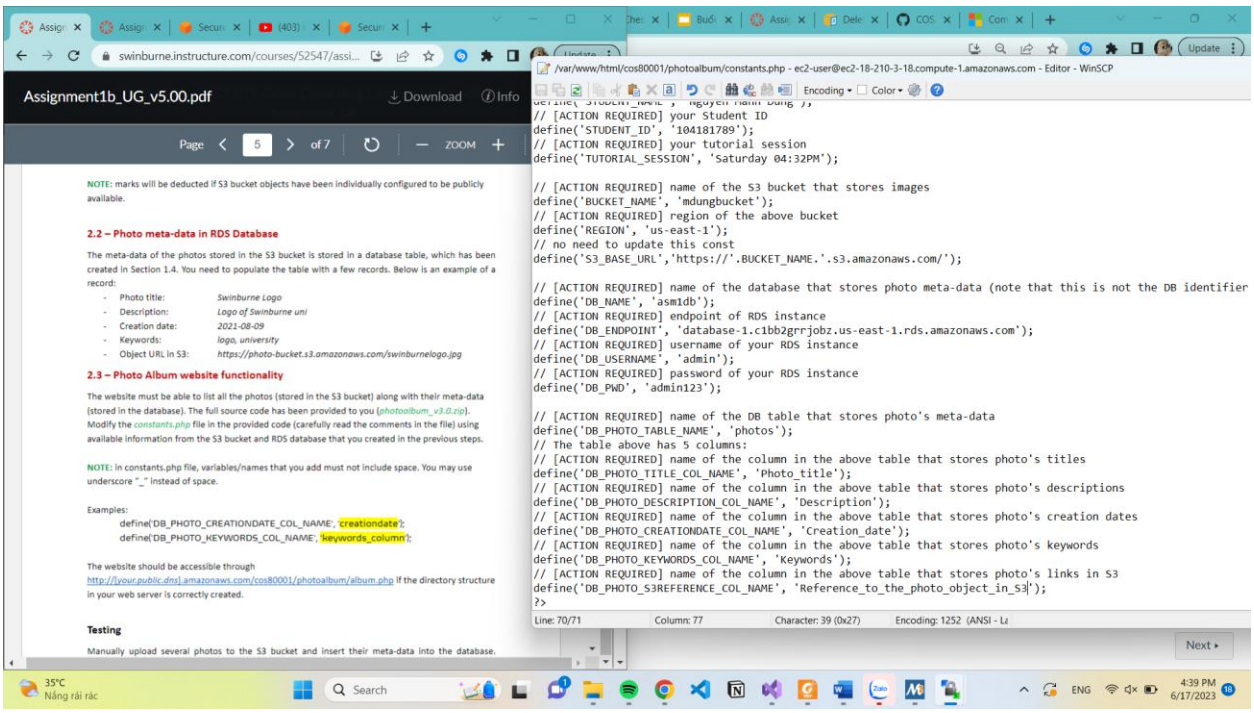
2.2 Photo meta-data in RDS database

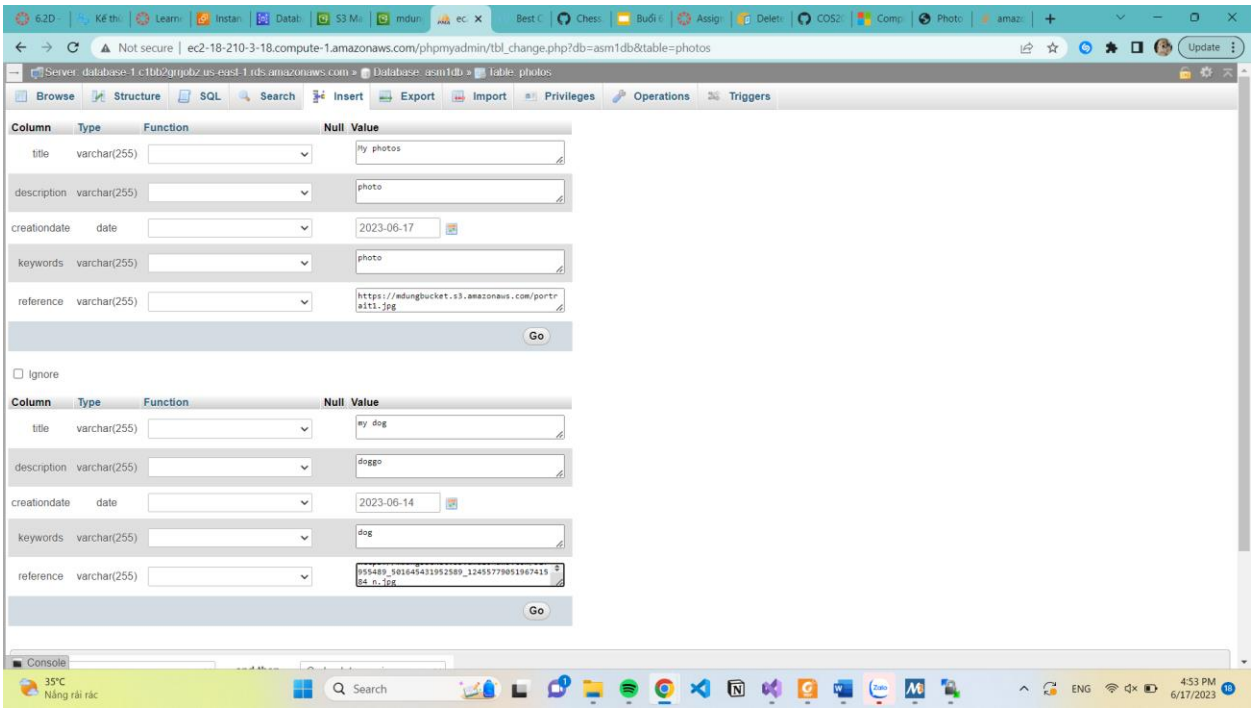


2.3 Photo Album website functionally

I have to create 2 column in the database also modify code in constant.php







This is my Photo Album website