COS20019 CLOUD COMPUTING ARCHITECTURE

Assignment 2

Developing a highly available Photo Album website

SWINBURNE UNIVERSITY OF TECHNOLOGY

Name: Tran Kim Thu
Student ID: 104061810

NOVEMBER 5, 2023

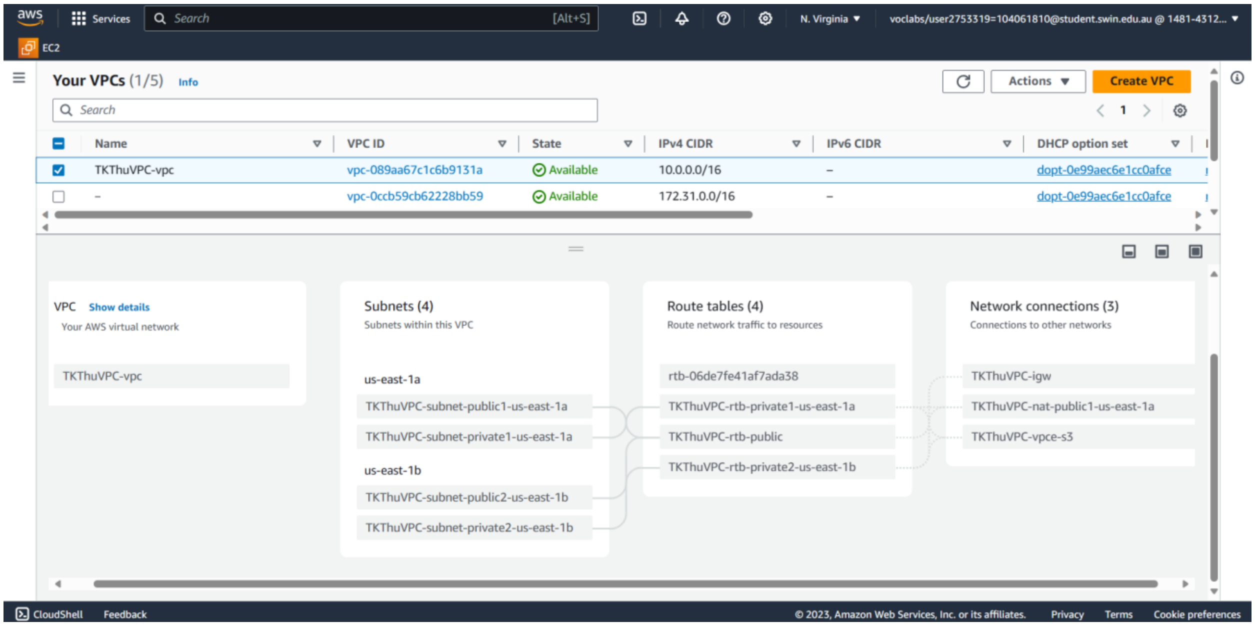
I.INTRODUCTION

This project is about creating a Photo Album website using various AWS services, such as EC2, S3, RDS, and Lambda. The website allows users to upload and browse photos, and creates resized thumbnails automatically. The project provides the full source code and instructions to connect the website with the S3 bucket, the RDS database, and the Lambda function. The project demonstrates how to use AWS services to build a dynamic and user-friendly website with features like photo storage, retrieval, and resizing.

II.WEBSITE ARCHITECTURE

1. Virtual Private Cloud (VPC)

The VPC has two public and two private subnets, each in a different Availability Zone. The public subnets can access the internet through an Internet Gateway, while the private subnets can access the internet through a NAT gateway. I use a NAT gateway instead of a NAT instance because it is more scalable and reliable. The public and private subnets have separate route tables that direct the traffic to the appropriate gateway.


aws
Services
Search
[Alt+S]
N. Virginia ▼
voclabs/user2753319=104061810@student.swin.edu.au @ 1481-4312... ▼
EC2
Info
Actions ▼
Create VPC
Search
1
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Your VPCs (1/5)

	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set
☑	TKThuVPC-vpc	vpc-089aa67c1c6b9131a	✓ Available	10.0.0.0/16	–	dopt-0e99aec6e1cc0afce
□	–	vpc-0ccb59cb62228bb59	✓ Available	172.31.0.0/16	–	dopt-0e99aec6e1cc0afce

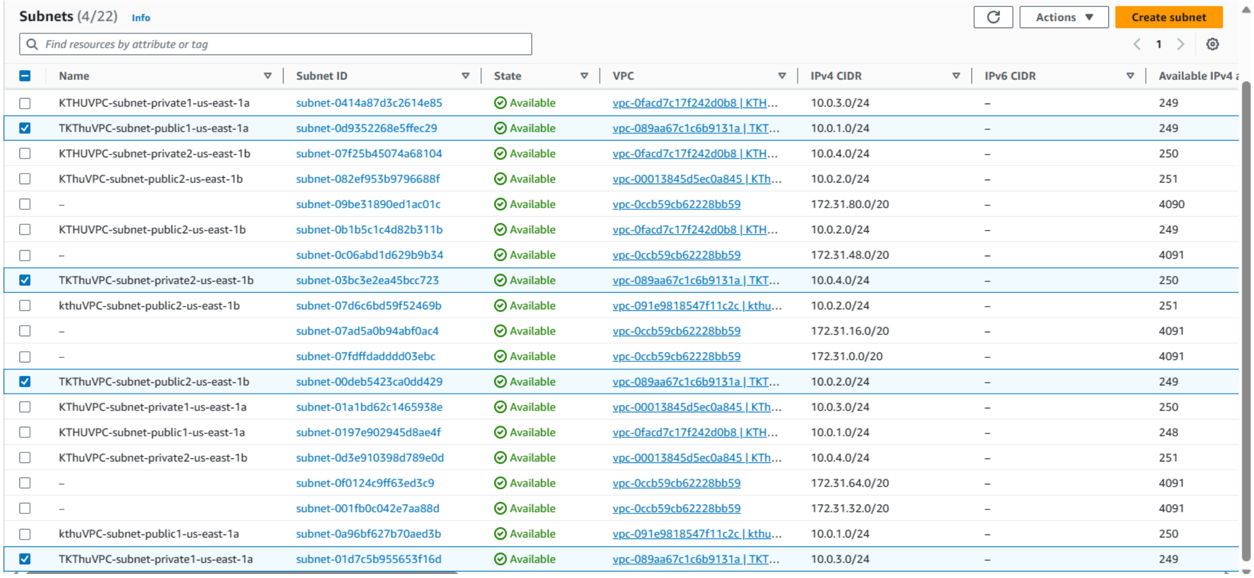
VPC Show details
Your AWS virtual network
TKThuVPC-vpc

Subnets (4)
Subnets within this VPC
us-east-1a
TKThuVPC-subnet-public1-us-east-1a
TKThuVPC-subnet-private1-us-east-1a
us-east-1b
TKThuVPC-subnet-public2-us-east-1b
TKThuVPC-subnet-private2-us-east-1b

Route tables (4)
Route network traffic to resources
rtb-06de7fe41af7ada38
TKThuVPC-rtb-private1-us-east-1a
TKThuVPC-rtb-public
TKThuVPC-rtb-private2-us-east-1b

Network connections (3)
Connections to other networks
TKThuVPC-igw
TKThuVPC-nat-public1-us-east-1a
TKThuVPC-vpce-s3

Figure 1: VPC Resource Map (NAT Gateway included)



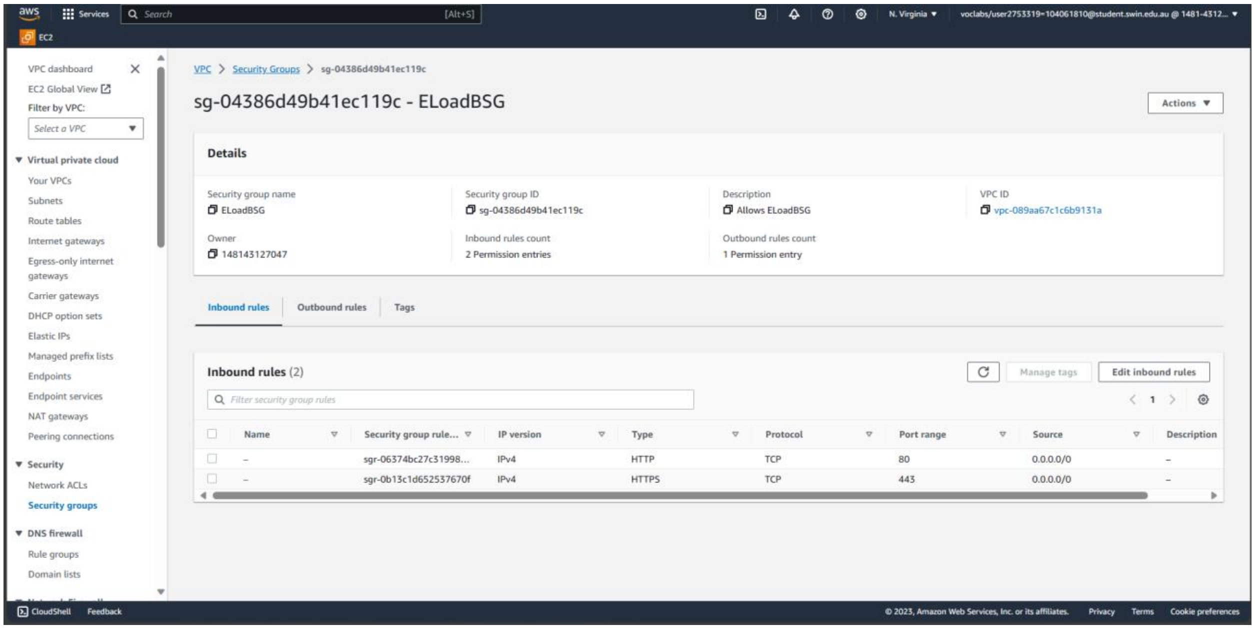
Subnets (4/22) Info

☐	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 a
☐	KTHUVPC-subnet-private1-us-east-1a	subnet-0414a87d3c2614e85	✓ Available	vpc-0facd7c17f242d0b8 | KTH...	10.0.3.0/24	–	249
☑	TKThuVPC-subnet-public1-us-east-1a	subnet-0d9352268e5ffec29	✓ Available	vpc-089aa67c1c6b9131a | TKT...	10.0.1.0/24	–	249
☐	KTHUVPC-subnet-private2-us-east-1b	subnet-07f25b45074a68104	✓ Available	vpc-0facd7c17f242d0b8 | KTH...	10.0.4.0/24	–	250
☐	KThuVPC-subnet-public2-us-east-1b	subnet-082ef953b9796688f	✓ Available	vpc-00013845d5ec0a845 | KTh...	10.0.2.0/24	–	251
☐	–	subnet-09be31890ed1ac01c	✓ Available	vpc-0ccb59cb62228bb59	172.31.80.0/20	–	4090
☐	KTHUVPC-subnet-public2-us-east-1b	subnet-0b1b5c1c4d82b311b	✓ Available	vpc-0facd7c17f242d0b8 | KTH...	10.0.2.0/24	–	249
☐	–	subnet-0c06abd1d629b9b34	✓ Available	vpc-0ccb59cb62228bb59	172.31.48.0/20	–	4091
☑	TKThuVPC-subnet-private2-us-east-1b	subnet-03bc3e2ea45bcc723	✓ Available	vpc-089aa67c1c6b9131a | TKT...	10.0.4.0/24	–	250
☐	kthuVPC-subnet-public2-us-east-1b	subnet-07d6c6bd59f52469b	✓ Available	vpc-091e9818547f11c2c | kthu...	10.0.2.0/24	–	251
☐	–	subnet-07ad5a0b94abf0ac4	✓ Available	vpc-0ccb59cb62228bb59	172.31.16.0/20	–	4091
☐	–	subnet-07fdffdaddd03ebc	✓ Available	vpc-0ccb59cb62228bb59	172.31.0.0/20	–	4091
☑	TKThuVPC-subnet-public2-us-east-1b	subnet-00deb5423ca0dd429	✓ Available	vpc-089aa67c1c6b9131a | TKT...	10.0.2.0/24	–	249
☐	KThuVPC-subnet-private1-us-east-1a	subnet-01a1bd62c1465938e	✓ Available	vpc-00013845d5ec0a845 | KTh...	10.0.3.0/24	–	250
☐	KTHUVPC-subnet-public1-us-east-1a	subnet-0197e902945d8ae4f	✓ Available	vpc-0facd7c17f242d0b8 | KTH...	10.0.1.0/24	–	248
☐	KThuVPC-subnet-private2-us-east-1b	subnet-0d3e910398d789e0d	✓ Available	vpc-00013845d5ec0a845 | KTh...	10.0.4.0/24	–	251
☐	–	subnet-0f0124c9ff63ed3c9	✓ Available	vpc-0ccb59cb62228bb59	172.31.64.0/20	–	4091
☐	–	subnet-001fb0c042e7aa88d	✓ Available	vpc-0ccb59cb62228bb59	172.31.32.0/20	–	4091
☐	kthuVPC-subnet-public1-us-east-1a	subnet-0a96bf627b70aed3b	✓ Available	vpc-091e9818547f11c2c | kthu...	10.0.1.0/24	–	250
☑	TKThuVPC-subnet-private1-us-east-1a	subnet-01d7c5b955653f16d	✓ Available	vpc-089aa67c1c6b9131a | TKT...	10.0.3.0/24	–	249

Figure 2: VPC Subnet CIDR Block

2. Security Group

The architecture has four security groups: ELBSG, WebServerSG, DBServerSG, and DevServerSG. ELBSG is for the load balancer, WebServerSG is for the web servers, DBServerSG is for the database server, and DevServerSG is for the development server. I don't need a NATServerSG because I use a NAT gateway instead of a NAT instance, which is more efficient and secure. All the security groups have the default outbound rule, which allows all traffic to any IPv4 destination.



VPC > Security Groups > sg-04386d49b41ec119c

sg-04386d49b41ec119c - ELoadBSG

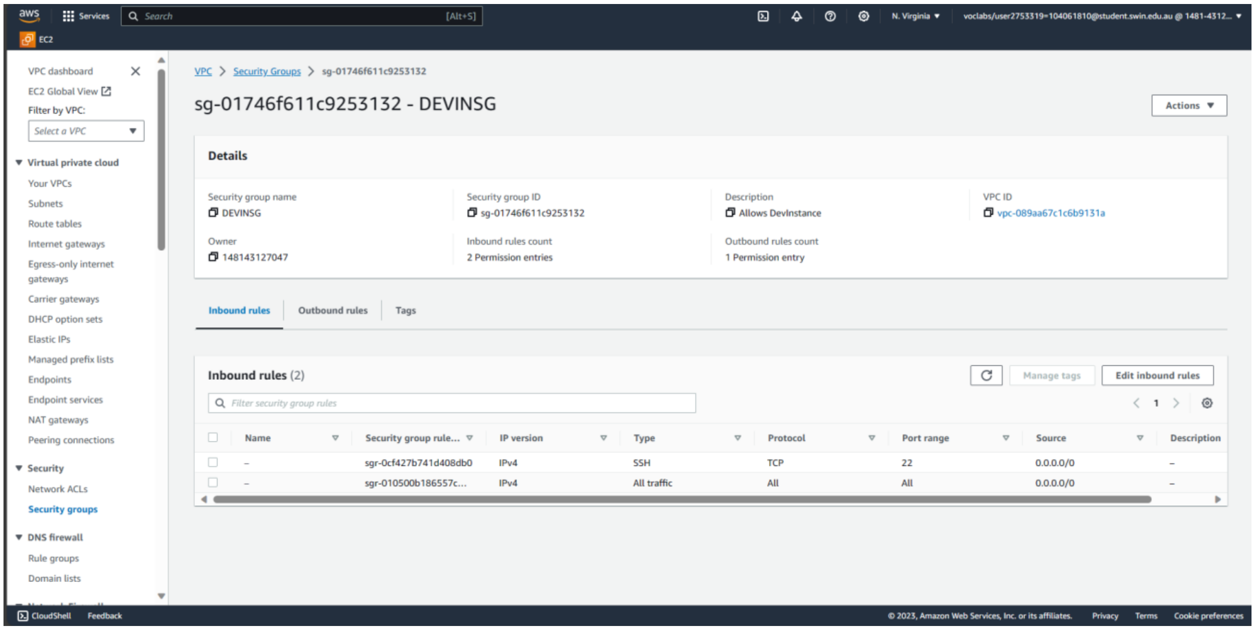
Details

Security group name: ELoadBSG
Security group ID: sg-04386d49b41ec119c
Description: Allows ELoadBSG
VPC ID: vpc-089aa67c1c6b9131a
Owner: 148143127047
Inbound rules count: 2 Permission entries
Outbound rules count: 1 Permission entry

Inbound rules (2)

☐	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
☐	–	sgr-06374bc27c31998...	IPv4	HTTP	TCP	80	0.0.0.0/0	–
☐	–	sgr-0b13c1d652537670f	IPv4	HTTPS	TCP	443	0.0.0.0/0	–

Figure 3: ELoadBSG Security Group used for Load Balancer



VPC > Security Groups > sg-01746f611c9253132

sg-01746f611c9253132 - DEVINSG

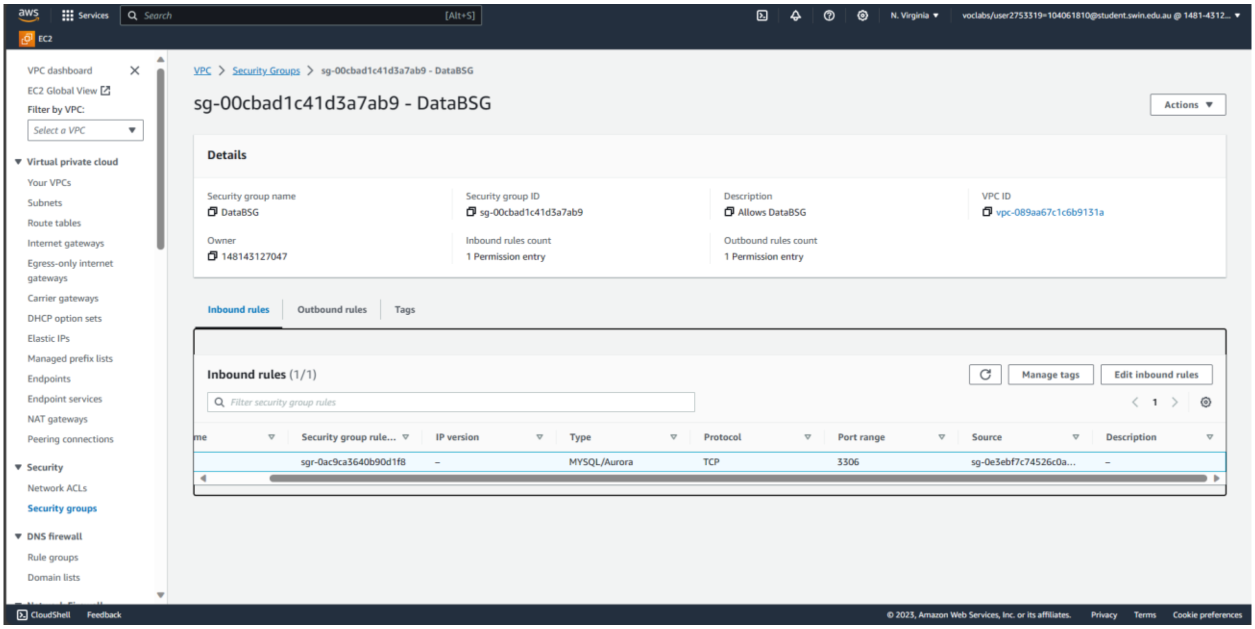
Details

Security group name DEVINSG	Security group ID sg-01746f611c9253132	Description Allows DevInstance	VPC ID vpc-089aa67c1c6b9131a
Owner 148143127047	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules (2)

□	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
□	–	sgr-0cf427b741d408db0	IPv4	SSH	TCP	22	0.0.0.0/0	–
□	–	sgr-010500b186557c...	IPv4	All traffic	All	All	0.0.0.0/0	–

Figure 4: DEVINSG Security Group used for Dev Instance



VPC > Security Groups > sg-00cbad1c41d3a7ab9 - DataBSG

sg-00cbad1c41d3a7ab9 - DataBSG

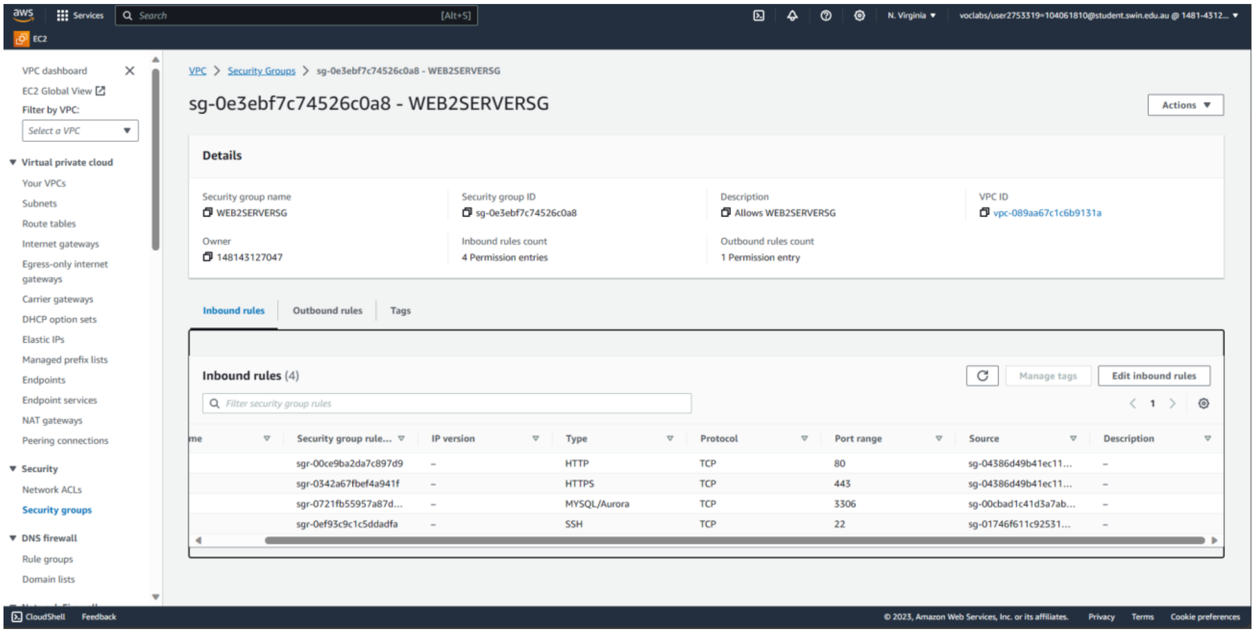
Details

Security group name DataBSG	Security group ID sg-00cbad1c41d3a7ab9	Description Allows DataBSG	VPC ID vpc-089aa67c1c6b9131a
Owner 148143127047	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules (1/1)

me	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
	sgr-0ac9ca3640b90d1f8	–	MYSQL/Aurora	TCP	3306	sg-0e3ebf7c74526c0a...	–

Figure 5:DataBSG Security Group used for RDS database.



VPC > Security Groups > sg-0e3ebf7c74526c0a8 - WEB2SERVERSG

sg-0e3ebf7c74526c0a8 - WEB2SERVERSG

Details

Security group name: WEB2SERVERSG
Security group ID: sg-0e3ebf7c74526c0a8
Description: Allows WEB2SERVERSG
VPC ID: vpc-089aa67c1c6b9131a
Owner: 148143127047
Inbound rules count: 4 Permission entries
Outbound rules count: 1 Permission entry

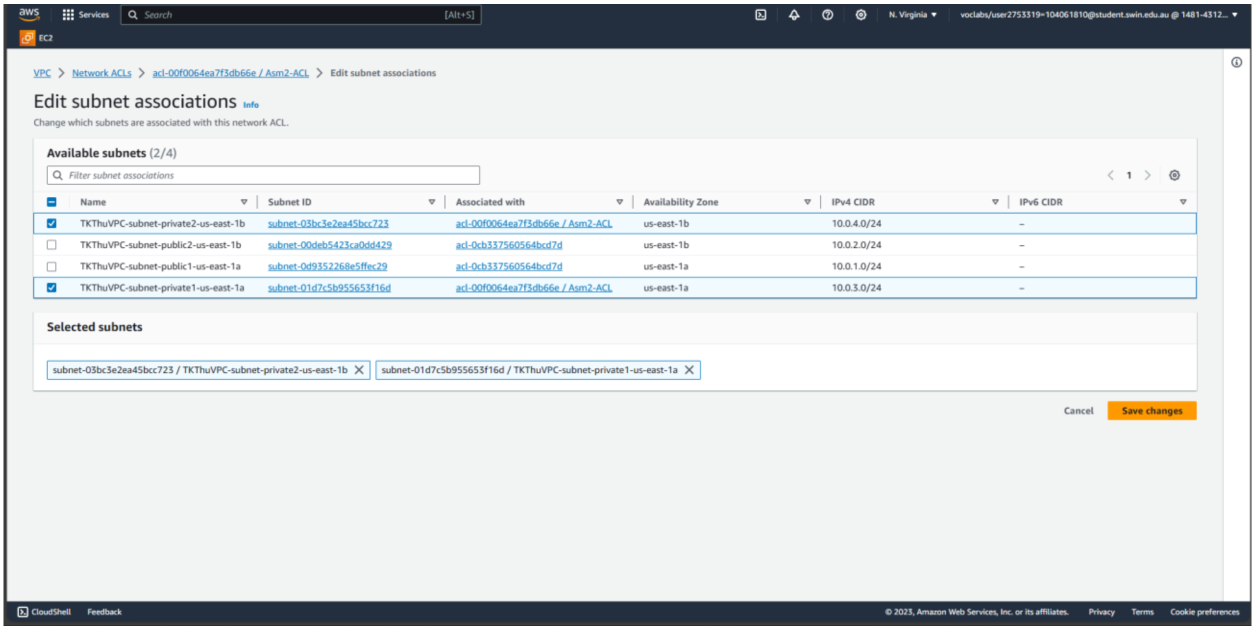
Inbound rules (4)

me	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
	sgr-00ce9ba2da7c897d9	–	HTTP	TCP	80	sg-04386d49b41ec11...	–
	sgr-0342a67fbef4a941f	–	HTTPS	TCP	443	sg-04386d49b41ec11...	–
	sgr-0721fb55957a87d...	–	MYSQL/Aurora	TCP	3306	sg-00cbad1c41d3a7ab...	–
	sgr-0ef93c9c1c5ddadfa	–	SSH	TCP	22	sg-01746f611c92531...	–

Figure 6:WEB2SERVERSG Security Group used for launch templates.

3. ***Network ACLs (NACL)***

To enhance the security of the web servers in the private subnets, I created and applied a Network Access Control List (NACL) named "Asm2-ACL". This NACL controls the ICMP (Internet Control Message Protocol) traffic between the Dev Server and the other servers. It only allows the ICMP traffic that is necessary for the Dev Server to function properly and blocks the rest.


Services
Search [Alt+S]
N. Virginia
voclabs/user2753319=104061810@student.swin.edu.au @ 1481-4312...
EC2
Info
Filter subnet associations
Cancel
Save changes
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

VPC > Network ACLs > acl-00f0064ea7f3db66e / Asm2-ACL > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this network ACL.

Available subnets (2/4)

	Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
☑	TKThuVPC-subnet-private2-us-east-1b	subnet-03bc3e2ea45bcc723	acl-00f0064ea7f3db66e / Asm2-ACL	us-east-1b	10.0.4.0/24	–
□	TKThuVPC-subnet-public2-us-east-1b	subnet-00deb5423ca0dd429	acl-0cb337560564bcd7d	us-east-1b	10.0.2.0/24	–
□	TKThuVPC-subnet-public1-us-east-1a	subnet-0d9352268e5ffec29	acl-0cb337560564bcd7d	us-east-1a	10.0.1.0/24	–
☑	TKThuVPC-subnet-private1-us-east-1a	subnet-01d7c5b955653f16d	acl-00f0064ea7f3db66e / Asm2-ACL	us-east-1a	10.0.3.0/24	–

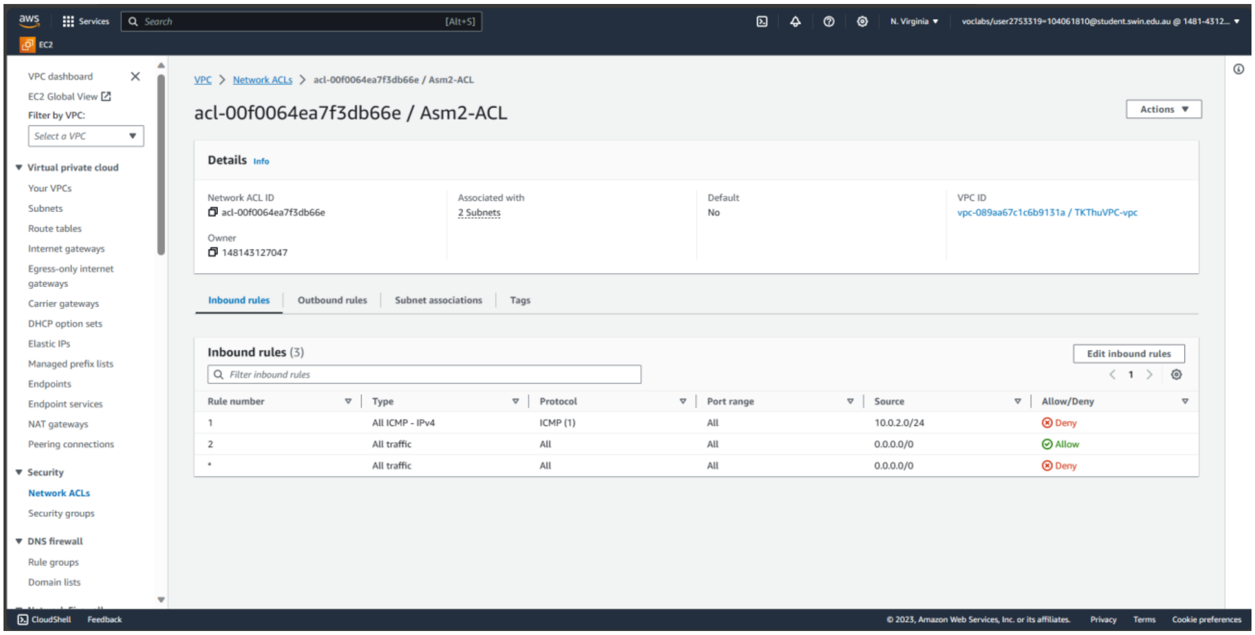
Selected subnets

subnet-03bc3e2ea45bcc723 / TKThuVPC-subnet-private2-us-east-1b

subnet-01d7c5b955653f16d / TKThuVPC-subnet-private1-us-east-1a

Figure 7:NACL associated with private subnets in the VPC

The Dev Server is located in Public Subnet 2, which has a CIDR of 10.0.2.0/24. The NACL for this subnet blocks the ICMP protocol in both directions. This means that the Dev Server cannot send or receive any ICMP messages, such as ping or traceroute.



acl-00f0064ea7f3db66e / Asm2-ACL

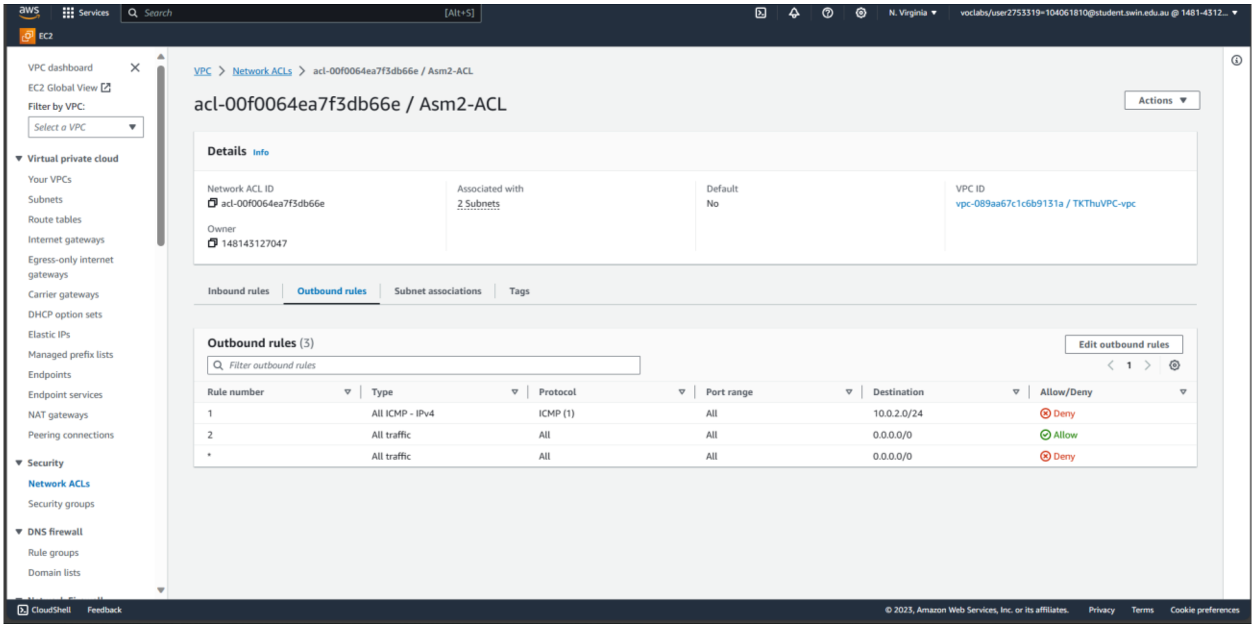
Details

Network ACL ID: acl-00f0064ea7f3db66e
Associated with: 2 Subnets
Default: No
VPC ID: vpc-089aa67c1c6b9131a / TKThuVPC-vpc
Owner: 148143127047

Inbound rules (3)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
1	All ICMP - IPv4	ICMP (1)	All	10.0.2.0/24	Deny
2	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Figure 8: Inbound rules



acl-00f0064ea7f3db66e / Asm2-ACL

Details

Network ACL ID: acl-00f0064ea7f3db66e
Associated with: 2 Subnets
Default: No
VPC ID: vpc-089aa67c1c6b9131a / TKThuVPC-vpc
Owner: 148143127047

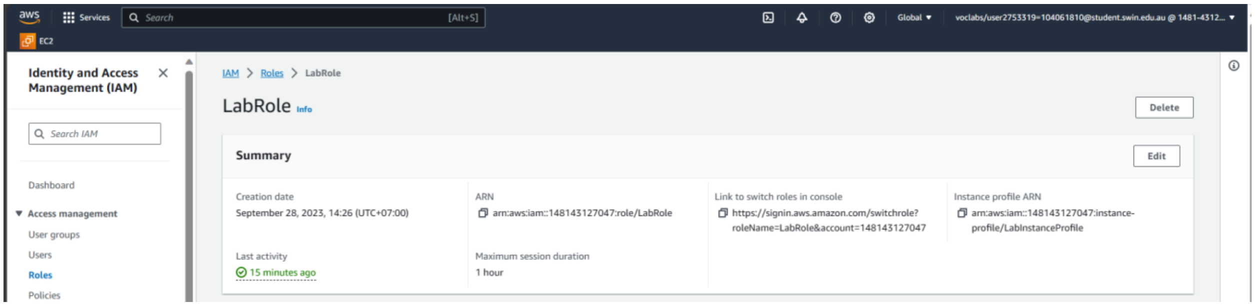
Outbound rules (3)

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
1	All ICMP - IPv4	ICMP (1)	All	10.0.2.0/24	Deny
2	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Figure 9:Outbound rules

4.IAM Role

The management console has IAM roles such as "LabRole" and "Labinstancerole" that have the necessary permissions for this assignment. These roles allow you to access and manage the AWS resources that are required for the assignment, such as EC2 instances, S3 buckets, and Lambda functions.



LabRole

Summary

Creation date
September 28, 2023, 14:26 (UTC+07:00)

ARN
arn:aws:iam::148143127047:role/LabRole

Link to switch roles in console
https://signin.aws.amazon.com/switchrole?roleName=LabRole&account=148143127047

Instance profile ARN
arn:aws:iam::148143127047:instance-profile/LabInstanceProfile

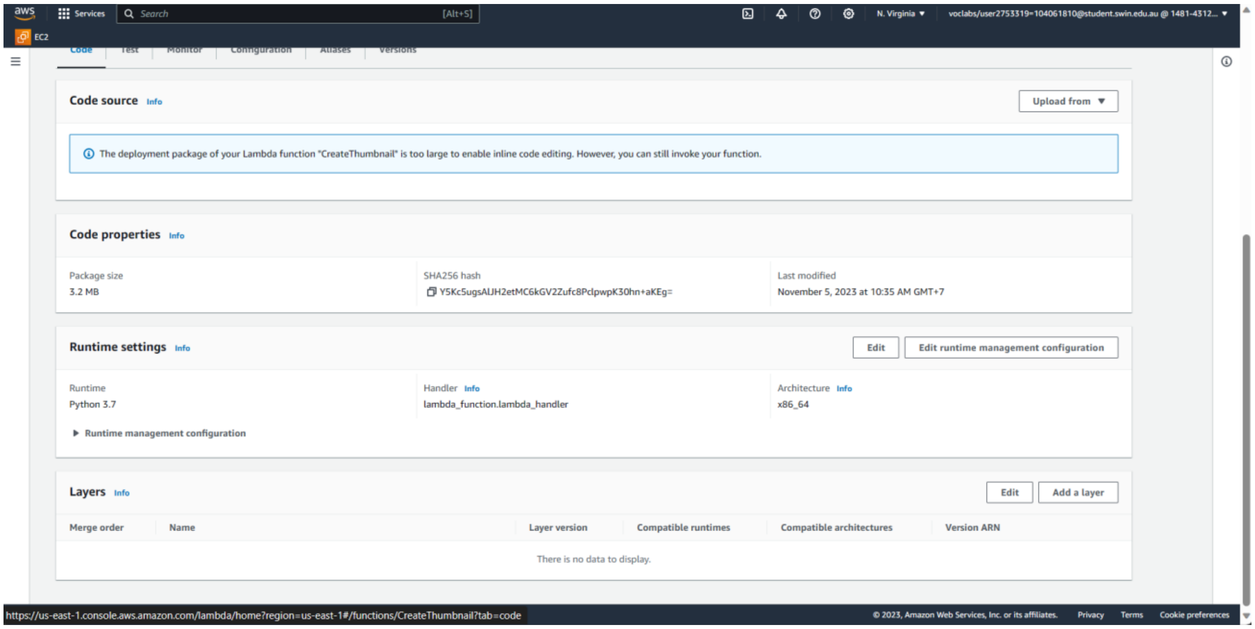
Last activity
15 minutes ago

Maximum session duration
1 hour

Figure 10: IAM roles

5. CreateThumbnail Lambda function

The Lambda function uses an IAM execution role to access and manage the objects in the S3 bucket securely and correctly. The IAM role is called LabRole and it has the minimum permissions needed for the assignment. The LabRole role was already created for you and assigned to the Lambda function.


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2753319=104061810@student.swin.edu.au @ 1481-4312...
EC2
Code
Test
Monitor
Configuration
Aliases
Versions
Info
Upload from
Edit
Edit runtime management configuration
Add a layer
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Code source

The deployment package of your Lambda function "CreateThumbnail" is too large to enable inline code editing. However, you can still invoke your function.

Code properties

Package size
3.2 MB

SHA256 hash
Y5KcSugsAIJH2etMC6kGV2Zufc8PclpwpK30hn+aKEg=

Last modified
November 5, 2023 at 10:35 AM GMT+7

Runtime settings

Runtime
Python 3.7

Handler
lambda_function.lambda_handler

Architecture
x86_64

Runtime management configuration

Layers

Merge order	Name	Layer version	Compatible runtimes	Compatible architectures	Version ARN

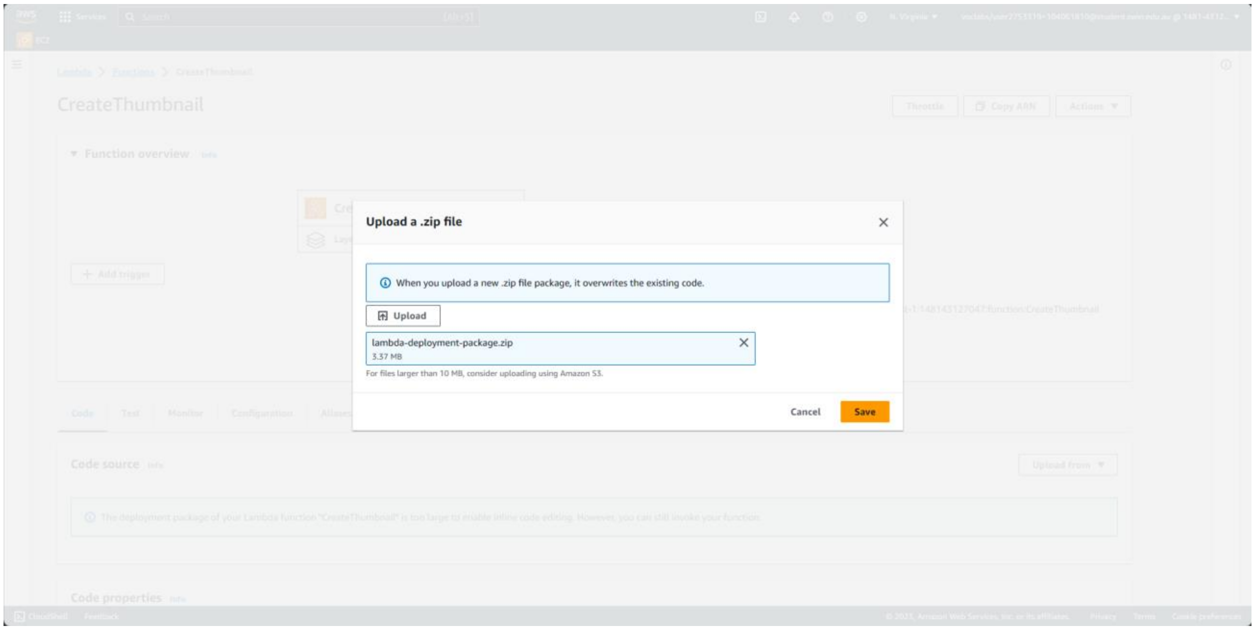
There is no data to display.

https://us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/CreateThumbnail?tab=code

Figure 11:CreateThumbnail Lambda function configuration

I created a Lambda function called "CreateThumbnail" that uses Python 3.7 as the programming language. This function can resize images that are uploaded to the S3 bucket and save them as thumbnails.

I uploaded the "lambda-deployment-package.zip" file that contains the code and dependencies for the Lambda function. This file is needed to create and run the Lambda function on the AWS platform.



Upload a .zip file

When you upload a new .zip file package, it overwrites the existing code.

Upload

lambda-deployment-package.zip
3.37 MB

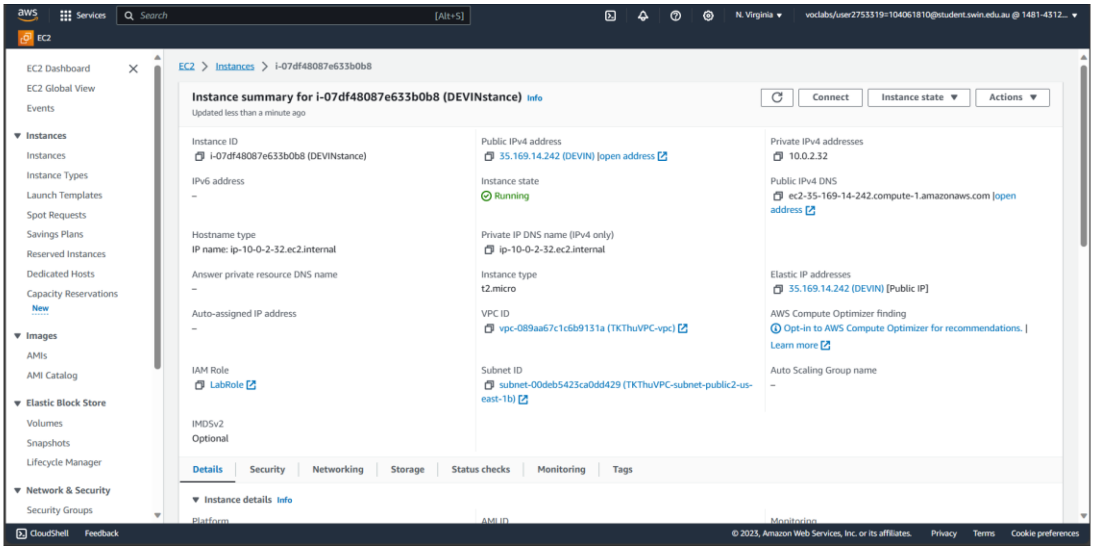
For files larger than 10 MB, consider uploading using Amazon S3.

The deployment package of your Lambda function "CreateThumbnail" is too large to enable inline code editing. However, you can still invoke your function.

Figure 12:lambda-deployment-package.zip

6. Dev Server Instance

The Dev server does not get any traffic from the ELB, because it is only used for creating the custom AMI that is needed to run the PhotoAlbum website. Custom AMI has all the required components, such as the AWS PHP SDK, Apache web server, and website source code. The Dev server can also use phpMyAdmin to manage the MySQL RDS instance.



Instance summary for i-07df48087e633b0b8 (DEVINstance) Info

Updated less than a minute ago

Instance ID: i-07df48087e633b0b8 (DEVINstance)

Public IPv4 address: 35.169.14.242 (DEVIN) |open address

Private IPv4 addresses: 10.0.2.32

IPv6 address: –

Instance state: Running

Public IPv4 DNS: ec2-35-169-14-242.compute-1.amazonaws.com |open address

Hostname type: IP name: ip-10-0-2-32.ec2.internal

Private IP DNS name (IPv4 only): ip-10-0-2-32.ec2.internal

Answer private resource DNS name: –

Instance type: t2.micro

Elastic IP addresses: 35.169.14.242 (DEVIN) [Public IP]

Auto-assigned IP address: –

VPC ID: vpc-089aa67c1c6b9131a (TKThuVPC-vpc)

AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more

IAM Role: LabRole

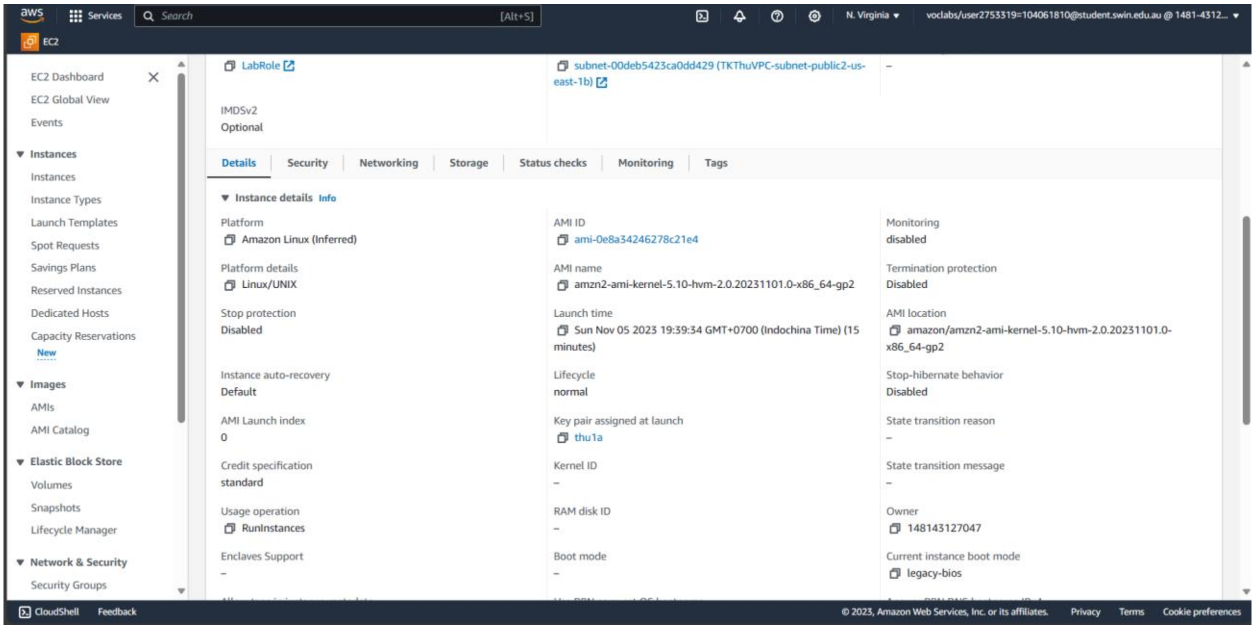
Subnet ID: subnet-00deb5423ca0dd429 (TKThuVPC-subnet-public2-us-east-1b)

Auto Scaling Group name: –

IMDSv2: Optional

Instance details Info

Figure 13:The Dev Server instance is in Public Subnet 2, which has a CIDR of 10.0.2.0/24. It also has an Elastic IP address that is attached to it.



LabRole

subnet-00deb5423ca0dd429 (TKThuVPC-subnet-public2-us-east-1b)

–

IMDSv2
Optional

Instance details Info

Platform
Amazon Linux (Inferred)

Platform details
Linux/UNIX

Stop protection
Disabled

Instance auto-recovery
Default

AMI Launch index
0

Credit specification
standard

Usage operation
RunInstances

Enclaves Support
–

AMI ID
ami-0e8a34246278c21e4

AMI name
amzn2-ami-kernel-5.10-hvm-2.0.20231101.0-x86_64-gp2

Launch time
Sun Nov 05 2023 19:39:34 GMT+0700 (Indochina Time) (15 minutes)

Lifecycle
normal

Key pair assigned at launch
thu1a

Kernel ID
–

RAM disk ID
–

Boot mode
–

Monitoring
disabled

Termination protection
Disabled

AMI location
amazon/amzn2-ami-kernel-5.10-hvm-2.0.20231101.0-x86_64-gp2

Stop-hibernate behavior
Disabled

State transition reason
–

State transition message
–

Owner
148143127047

Current instance boot mode
legacy-bios

Figure 14:Configure Dev Instance

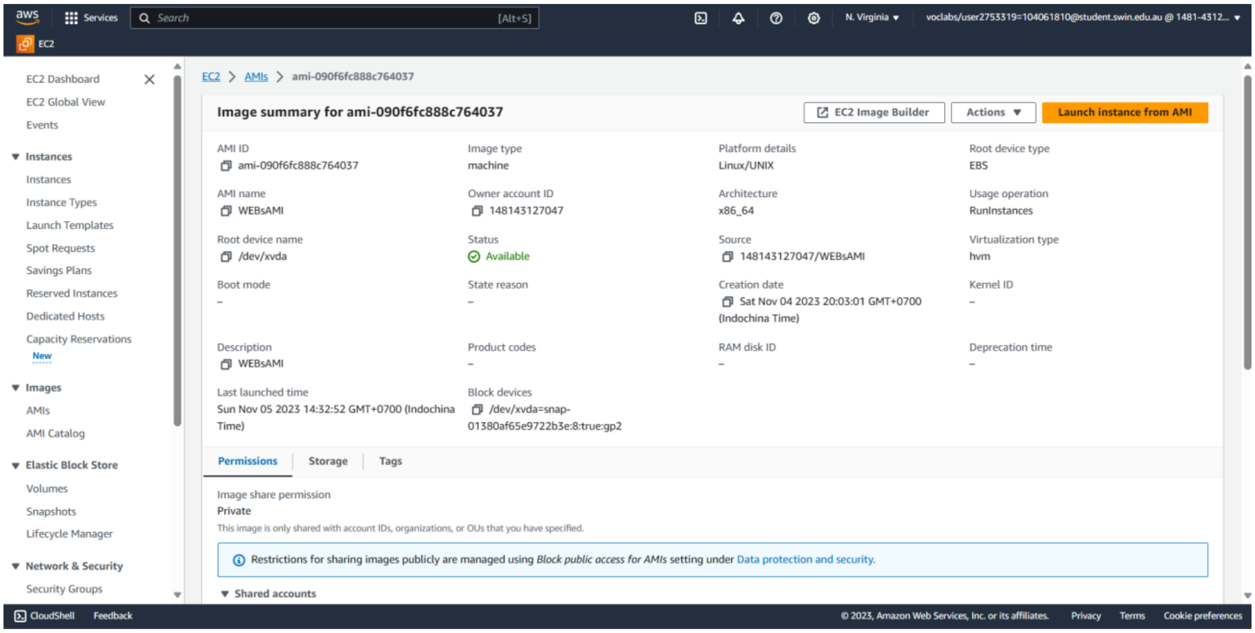


Image summary for ami-090f6fc888c764037

AMI ID
ami-090f6fc888c764037

AMI name
WEBsAMI

Root device name
/dev/xvda

Boot mode
–

Description
WEBsAMI

Last launched time
Sun Nov 05 2023 14:32:52 GMT+0700 (Indochina Time)

Image type
machine

Owner account ID
148143127047

Status
Available

State reason
–

Product codes
–

Block devices
/dev/xvda=snap-01380af65e9722b3e:8:true:gp2

Platform details
Linux/UNIX

Architecture
x86_64

Source
148143127047/WEBsAMI

Creation date
Sat Nov 04 2023 20:03:01 GMT+0700 (Indochina Time)

RAM disk ID
–

Root device type
EBS

Usage operation
RunInstances

Virtualization type
hvm

Kernel ID
–

Deprecation time
–

Image share permission
Private
This image is only shared with account IDs, organizations, or OUs that you have specified.

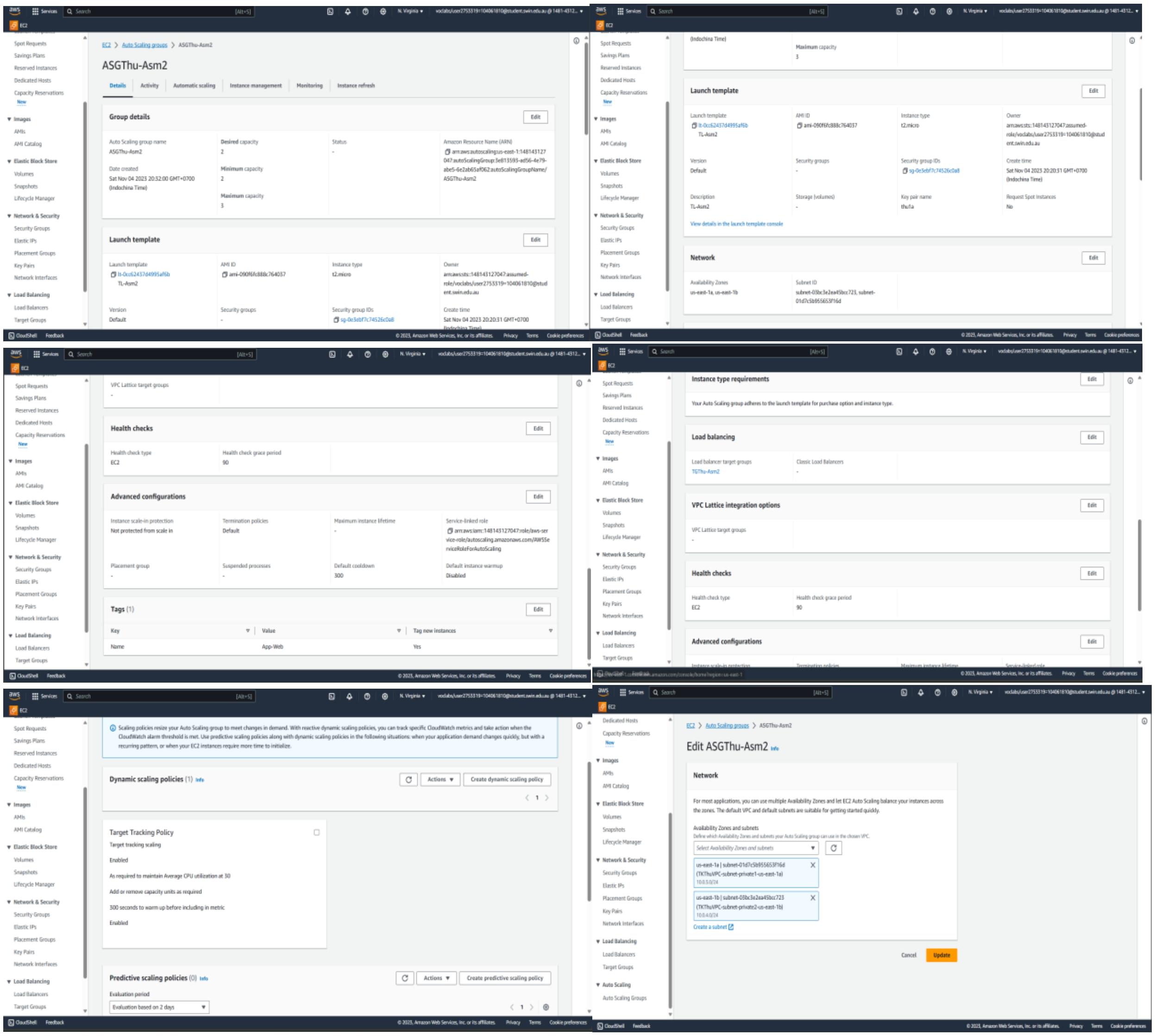
Restrictions for sharing images publicly are managed using *Block public access for AMIs* setting under Data protection and security.

Shared accounts

Figure 15:Create AMIS for Dev Instance

7. Auto Scaling Group (ASG)

The ASG is set up to launch instances only in the private subnets, keeping at least 2 instances and at most 3 instances, with 2 instances as the preferred number. This makes sure that the application always has enough instances running while also avoiding the infrastructure from scaling too much.



EC2 > Auto Scaling groups > ASGThu-Asm2

ASGThu-Asm2

Details | Activity | Automatic scaling | Instance management | Monitoring | Instance refresh

Group details

Auto Scaling group name	Desired capacity	Status	Amazon Resource Name (ARN)
ASGThu-Asm2	2	-	arn:aws:autoscaling:us-east-1:148143127047:autoScalingGroup:3e813593-ad56-4e79-abe5-6e2ab65af062:autoScalingGroupName/ASGThu-Asm2
Date created	Minimum capacity		
Sat Nov 04 2023 20:32:00 GMT+0700 (Indochina Time)	2		
	Maximum capacity		
	3		

Launch template

Launch template	AMI ID	Instance type	Owner
lt-0cc62437d4995af6b TL-Asm2	ami-090f6fc888c764037	t2.micro	arn:aws:sts::148143127047:assumed-role/voclabs/user2753319=104061810@student.swin.edu.au
Version	Security groups	Security group IDs	Create time
Default	-	sg-0e3ebf7c74526c0a8	Sat Nov 04 2023 20:20:31 GMT+0700 (Indochina Time)
Description	Storage (volumes)	Key pair name	Request Spot Instances
TL-Asm2	-	thu1a	No

View details in the launch template console

Network

Availability Zones	Subnet ID
us-east-1a, us-east-1b	subnet-03bc3e2ea45bcc723, subnet-01d7c5b955653f16d

Instance type requirements

Your Auto Scaling group adheres to the launch template for purchase option and instance type.

Load balancing

Load balancer target groups	Classic Load Balancers
TGThu-Asm2	-

VPC Lattice integration options

VPC Lattice target groups: -

Health checks

Health check type	Health check grace period
EC2	90

Advanced configurations

Instance scale-in protection	Termination policies	Maximum instance lifetime	Service-linked role
Not protected from scale in	Default	-	arn:aws:iam::148143127047:role/aws-service-role/autoscaling.amazonaws.com/AWSServiceRoleForAutoScaling
Placement group	Suspended processes	Default cooldown	Default instance warmup
-	-	300	Disabled

Tags (1)

Key	Value	Tag new instances
Name	App-Web	Yes

Scaling policies resize your Auto Scaling group to meet changes in demand. With reactive dynamic scaling policies, you can track specific CloudWatch metrics and take action when the CloudWatch alarm threshold is met. Use predictive scaling policies along with dynamic scaling policies in the following situations: when your application demand changes quickly, but with a recurring pattern, or when your EC2 instances require more time to initialize.

Dynamic scaling policies (1)

Target Tracking Policy

Target tracking scaling

Enabled

As required to maintain Average CPU utilization at 30

Add or remove capacity units as required

300 seconds to warm up before including in metric

Enabled

Predictive scaling policies (0)

Evaluation period: Evaluation based on 2 days

EC2 > Auto Scaling groups > ASGThu-Asm2

Edit ASGThu-Asm2

Network

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

Availability Zones and subnets

Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

- us-east-1a | subnet-01d7c5b955653f16d (TKThuVPC-subnet-private1-us-east-1a) 10.0.3.0/24
- us-east-1b | subnet-03bc3e2ea45bcc723 (TKThuVPC-subnet-private2-us-east-1b) 10.0.4.0/24

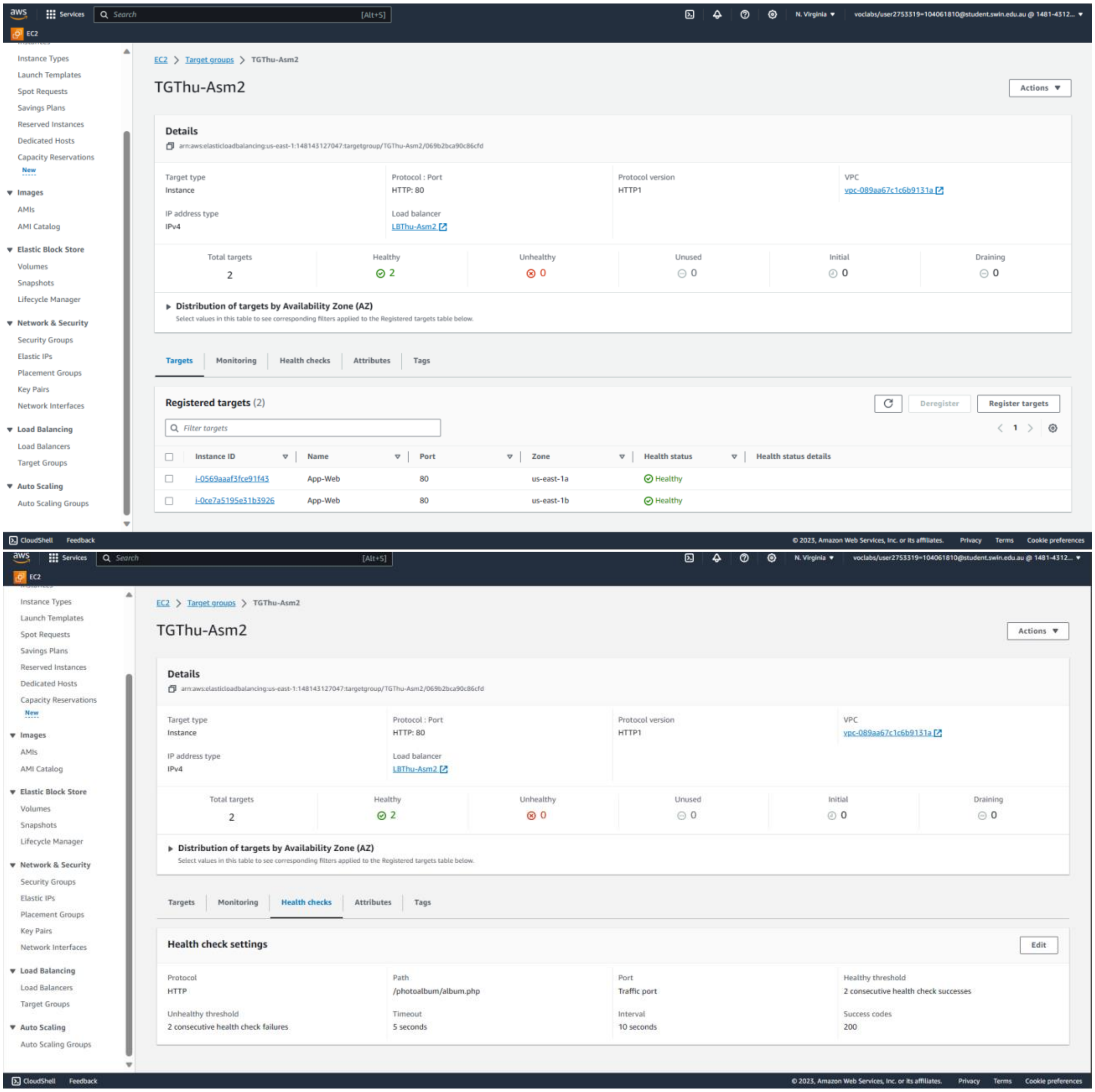
Edit
Actions
Create dynamic scaling policy
Create predictive scaling policy
Select Availability Zones and subnets
Create a subnet
Cancel
Update

Figure16:Configure ASG

The web server can automatically adjust its capacity according to the request load, maintaining a steady number of requests per target and optimizing resource utilization.

8. Elastic Load Balancing (ELB)

To make the load balancer work, I need to create a new target group that contains the targets that the load balancer will send requests to and check their health.



EC2 > Target groups > TGThu-Asm2

TGThu-Asm2

Details

arn:aws:elasticloadbalancing:us-east-1:148143127047:targetgroup/TGThu-Asm2/069b2bca90c86cfd

Target type	Protocol : Port	Protocol version	VPC
Instance	HTTP: 80	HTTP1	vpc-089aa67c1c6b9131a
IP address type	Load balancer		
IPv4	LBThu-Asm2		

Total targets	Healthy	Unhealthy	Unused	Initial	Draining
2	2	0	0	0	0

Distribution of targets by Availability Zone (AZ)
Select values in this table to see corresponding filters applied to the Registered targets table below.

Registered targets (2)

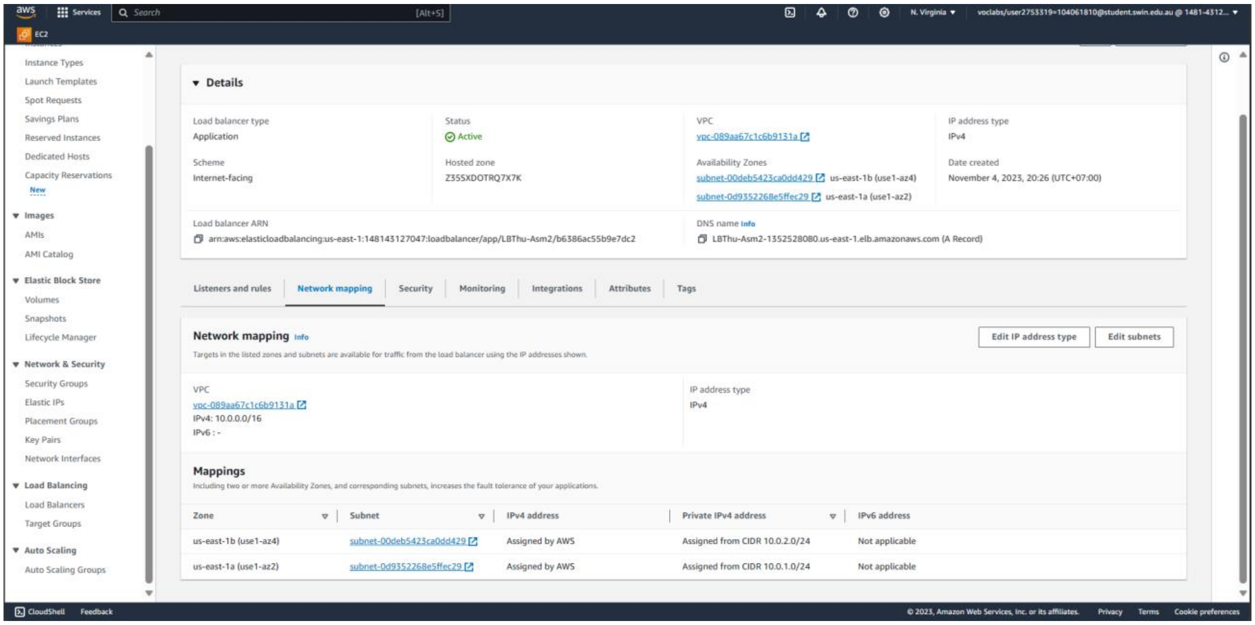
Instance ID	Name	Port	Zone	Health status	Health status details
i-0569aaaf3fce91f43	App-Web	80	us-east-1a	✓ Healthy	
i-0ce7a5195e31b3926	App-Web	80	us-east-1b	✓ Healthy	

Health check settings

Protocol	Path	Port	Healthy threshold
HTTP	/photoalbum/album.php	Traffic port	2 consecutive health check successes
Unhealthy threshold	Timeout	Interval	Success codes
2 consecutive health check failures	5 seconds	10 seconds	200

Figure 17: Target Group status with 2 Healthy Instance and Path set to /photoalbum/album.php

To connect the load balancer to the target group, I need to create a new load balancer and associate it with the target group.



Details

Load balancer type: Application
Status: Active
VPC: vpc-089aa67c1c6b9131a
IP address type: IPv4
Scheme: Internet-facing
Hosted zone: Z35SXDOTRQ7X7K
Availability Zones: subnet-00deb5423ca0dd429 us-east-1b (use1-az4); subnet-0d9352268e5ffec29 us-east-1a (use1-az2)
Date created: November 4, 2023, 20:26 (UTC+07:00)
Load balancer ARN: arn:aws:elasticloadbalancing:us-east-1:148143127047:loadbalancer/app/LBThu-Asm2/b6386ac55b9e7dc2
DNS name Info: LBThu-Asm2-1352528080.us-east-1.elb.amazonaws.com (A Record)

Network mapping Info

Targets in the listed zones and subnets are available for traffic from the load balancer using the IP addresses shown.

VPC: vpc-089aa67c1c6b9131a
IPv4: 10.0.0.0/16
IPv6 : -
IP address type: IPv4

Mappings

Including two or more Availability Zones, and corresponding subnets, increases the fault tolerance of your applications.

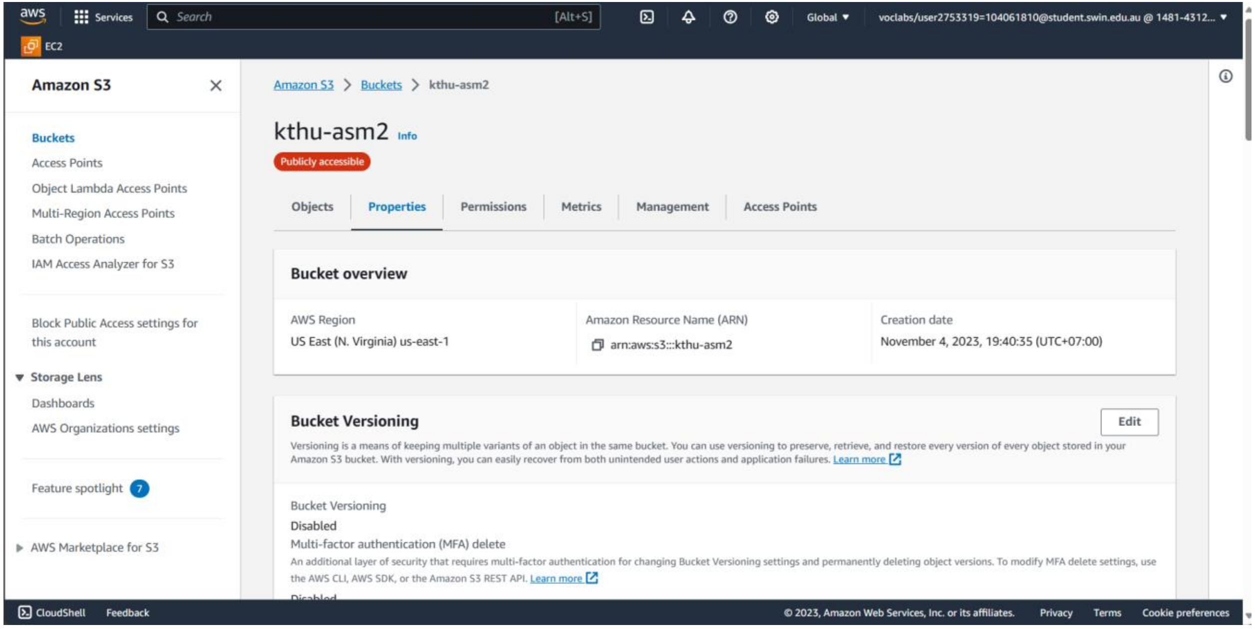
Zone	Subnet	IPv4 address	Private IPv4 address	IPv6 address
us-east-1b (use1-az4)	subnet-00deb5423ca0dd429	Assigned by AWS	Assigned from CIDR 10.0.2.0/24	Not applicable
us-east-1a (use1-az2)	subnet-0d9352268e5ffec29	Assigned by AWS	Assigned from CIDR 10.0.1.0/24	Not applicable

Figure 16:The Public Subnet 1 and Public Subnet 2 are connected to an Application Load Balancer.

The ELB is now capable of evenly distributing incoming HTTP and HTTPS traffic among multiple EC2 targets.

8. *Simple Storage Service (S3)*

I created a new bucket as assignment 1b specifically for photo storage. To ensure the objects in this S3 bucket are accessible as needed, suitable permissions and policies have been implemented. This ensures that access to the stored photos is correctly permitted as intended.


aws
Services
Search
[Alt+S]
Global
voclabs/user2753319=104061810@student.swin.edu.au @ 1481-4312...
EC2
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 7
AWS Marketplace for S3
Amazon S3 > Buckets > kthu-asm2
Objects
Properties
Permissions
Metrics
Management
Access Points
Edit
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

kthu-asm2 Info

Publicly accessible

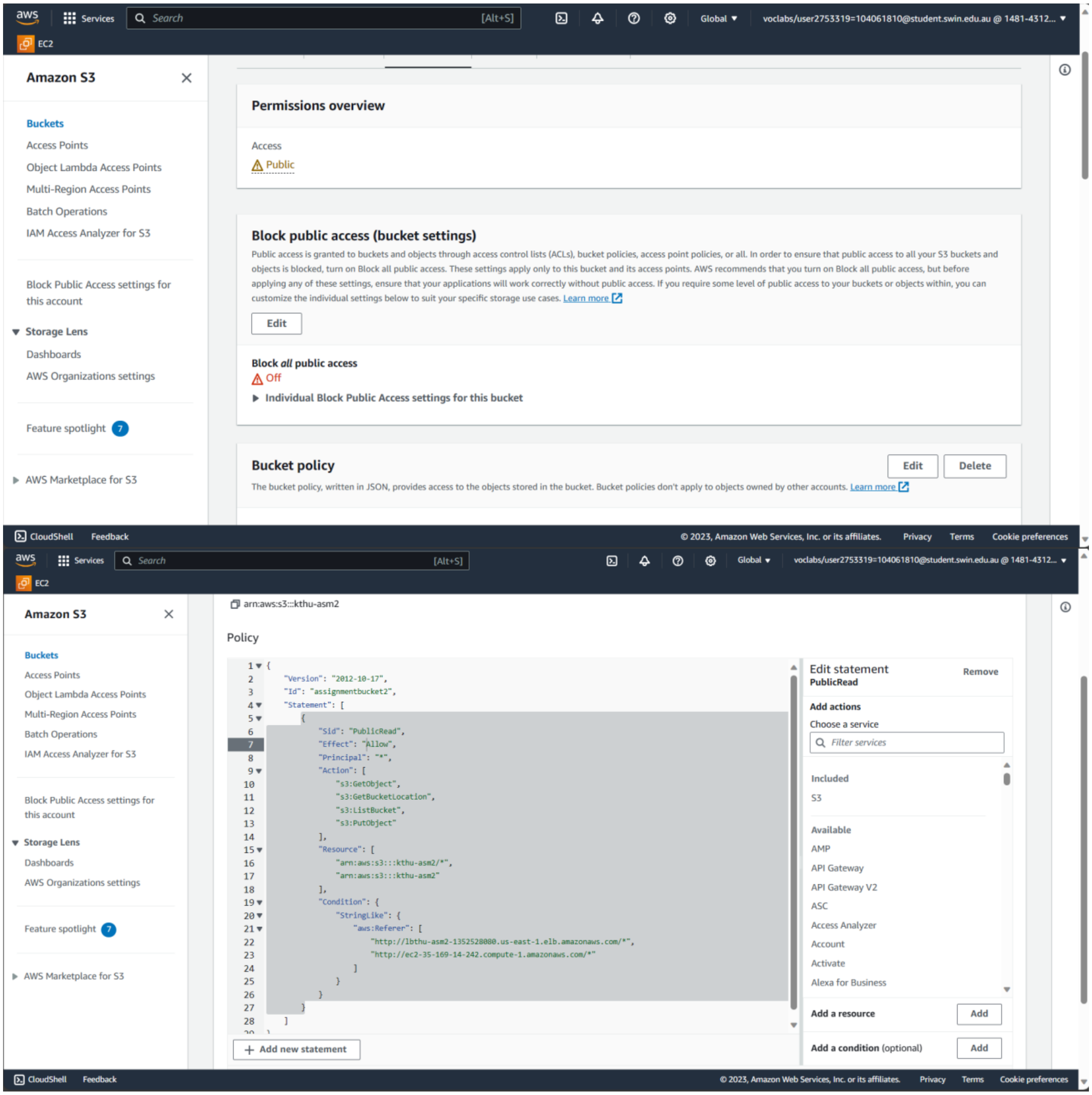
Bucket overview

AWS Region: US East (N. Virginia) us-east-1
Amazon Resource Name (ARN): arn:aws:s3:::kthu-asm2
Creation date: November 4, 2023, 19:40:35 (UTC+07:00)

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning
Disabled
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled


aws
Services
Search
[Alt+S]
Global
voclabs/user2753319=104061810@student.swin.edu.au @ 1481-4312...
EC2
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 7
AWS Marketplace for S3
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Permissions overview

Access
⚠ Public

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

Edit

Block *all* public access
⚠ Off

▸ Individual Block Public Access settings for this bucket

Bucket policy

Edit Delete

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

arn:aws:s3:::kthu-asm2

Policy

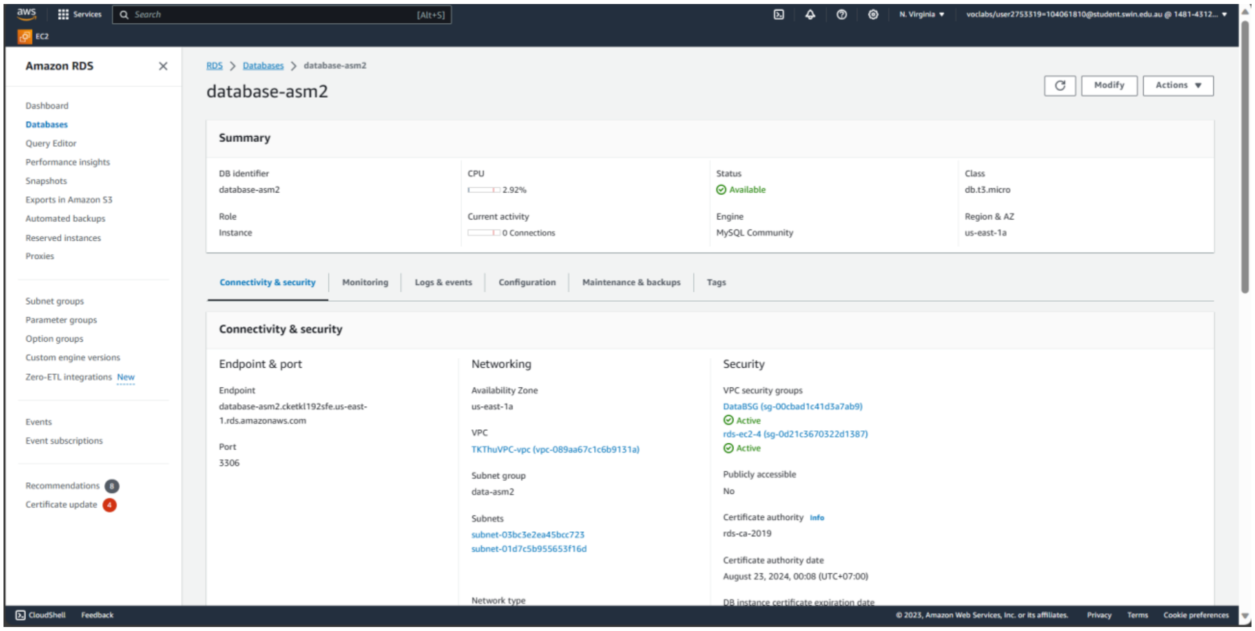
```
{
    "Version": "2012-10-17",
    "Id": "assignmentbucket2",
    "Statement": [
        {
            "Sid": "PublicRead",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::kthu-asm2/*",
                "arn:aws:s3:::kthu-asm2"
            ],
            "Condition": {
                "StringLike": {
                    "aws:Referer": [
                        "http://lbthu-asm2-1352528080.us-east-1.elb.amazonaws.com/*",
                        "http://ec2-35-169-14-242.compute-1.amazonaws.com/*"
                    ]
                }
            }
        }
    ]
```

Figure 17:S3 bucket Policy

This policy limits the access to the S3 bucket to only those GET requests that come from the specified domains, thereby ensuring a regulated and secure access policy for the objects in the bucket.

9) Relational Database Service (RDS)

The RDS instance utilized in this assignment has been set up in the same manner as it was in the previous assignment.



database-asm2

Summary

DB identifier	CPU	Status	Class
database-asm2	2.92%	Available	db.t3.micro
Role	Current activity	Engine	Region & AZ
Instance	0 Connections	MySQL Community	us-east-1a

Connectivity & security

Endpoint & port

Endpoint
database-asm2.cketkl192sfe.us-east-1.rds.amazonaws.com

Port
3306

Networking

Availability Zone
us-east-1a

VPC
TKThuVPC-vpc (vpc-089aa67c1c6b9131a)

Subnet group
data-asm2

Subnets
subnet-03bc3e2ea45bcc723
subnet-01d7c5b955653f16d

Network type

Security

VPC security groups
DataBSG (sg-00cbad1c41d3a7ab9)
Active
rds-ec2-4 (sg-0d21c3670322d1387)
Active

Publicly accessible
No

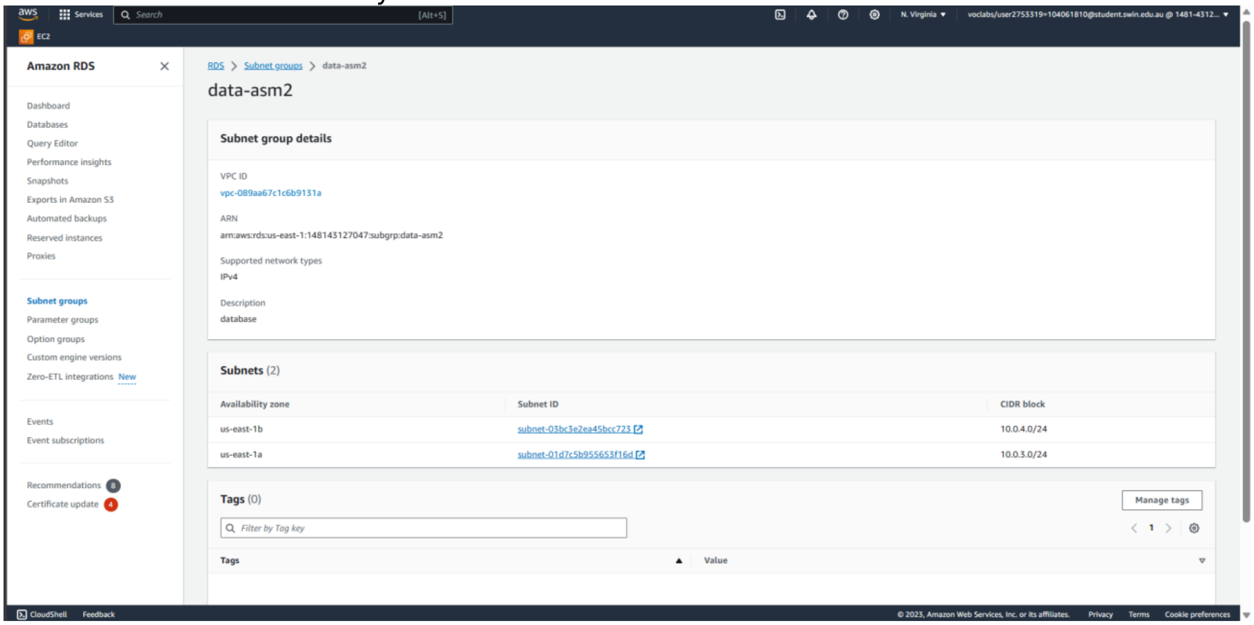
Certificate authority Info
rds-ca-2019

Certificate authority date
August 23, 2024, 00:08 (UTC+07:00)

DB instance certificate expiration date

Figure 18: RDS Configuration

The RDS instance is linked with a subnet group named 'data-asm2', which includes private subnets from both Availability Zones.



data-asm2

Subnet group details

VPC ID
vpc-089aa67c1c6b9131a

ARN
arn:aws:rds:us-east-1:148143127047:subgrp:data-asm2

Supported network types
IPv4

Description
database

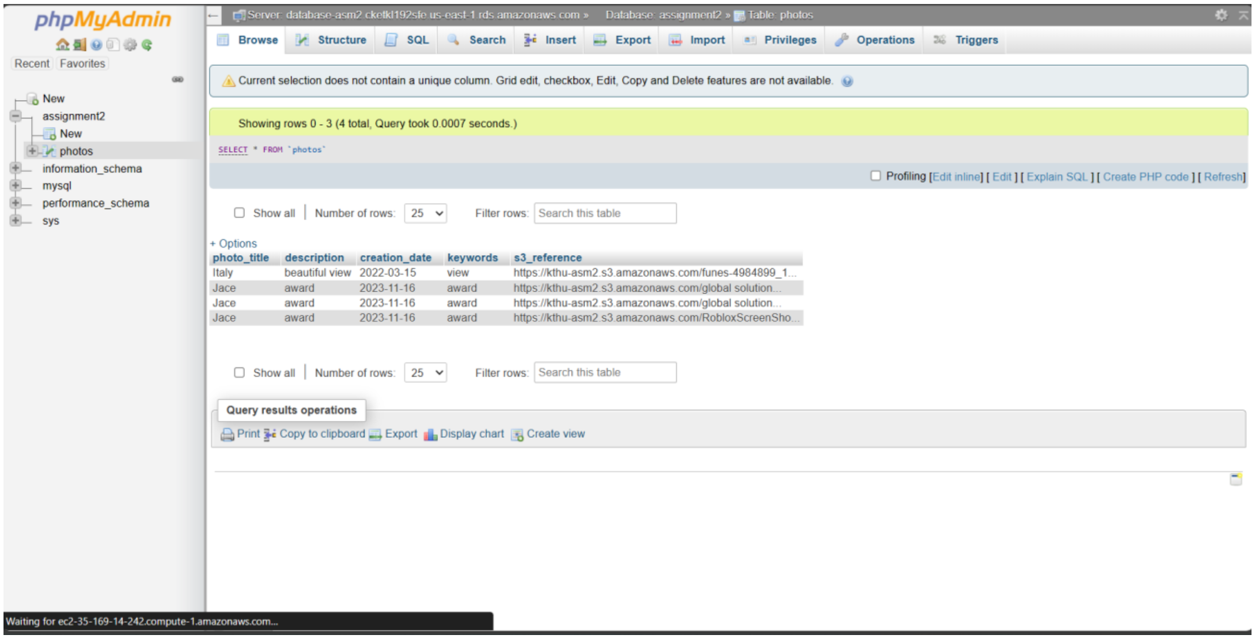
Subnets (2)

Availability zone	Subnet ID	CIDR block
us-east-1b	subnet-03bc3e2ea45bcc723	10.0.4.0/24
us-east-1a	subnet-01d7c5b955653f16d	10.0.3.0/24

Tags (0)

Tags	Value

Figure 19: Subnet Group with Private Subnet 3 and 4



Server: database-asm2.cketkl192sfe.us-east-1.rds.amazonaws.com » Database: assignment2 » Table: photos

⚠ Current selection does not contain a unique column. Grid edit, checkbox, Edit, Copy and Delete features are not available.

Showing rows 0 - 3 (4 total, Query took 0.0007 seconds.)

```
SELECT * FROM `photos`
```

□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

□ Show all | Number of rows: 25 Filter rows: Search this table

+ Options

photo_title	description	creation_date	keywords	s3_reference
Italy	beautiful view	2022-03-15	view	https://kthu-asm2.s3.amazonaws.com/funes-4984899_1...
Jace	award	2023-11-16	award	https://kthu-asm2.s3.amazonaws.com/global solution...
Jace	award	2023-11-16	award	https://kthu-asm2.s3.amazonaws.com/global solution...
Jace	award	2023-11-16	award	https://kthu-asm2.s3.amazonaws.com/RobloxScreenSho...

□ Show all | Number of rows: 25 Filter rows: Search this table

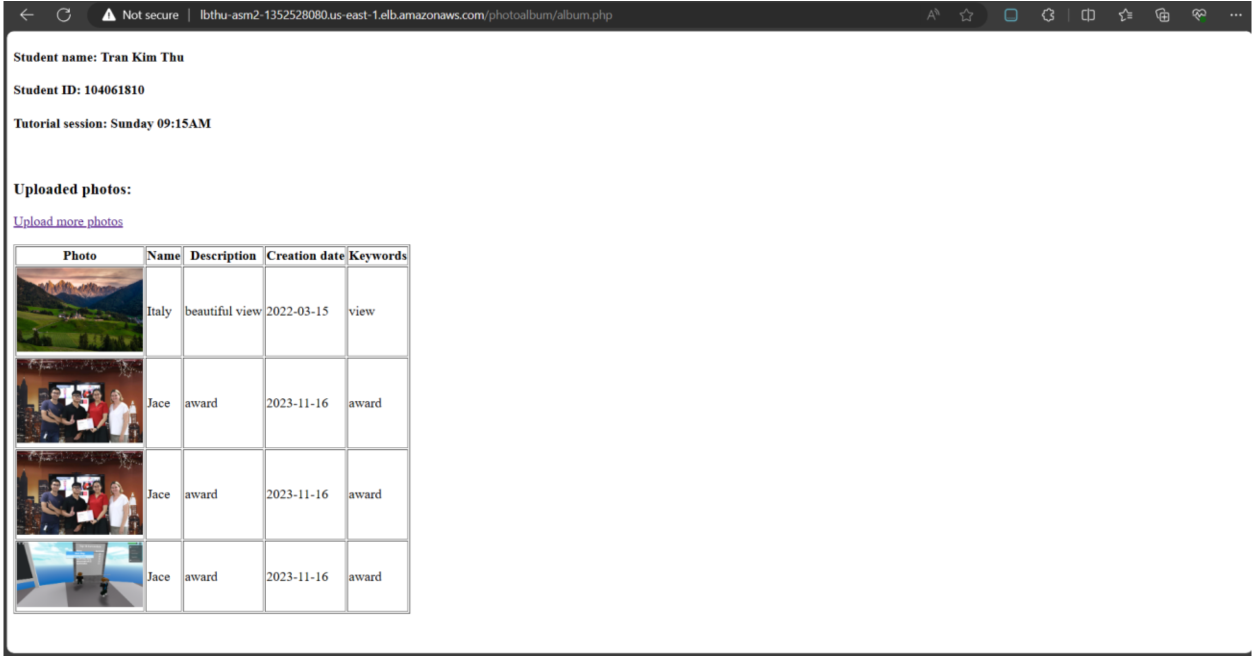
Waiting for ec2-35-169-14-242.compute-1.amazonaws.com...

Figure 20: Update and Record data on PhyMyAdmin

III. Functional requirements

1) Website accessibility

To interact with the PhotoAlbum website, you can visit the following URL: **http://lbthu-asm2-1352528080.us-east-1.elb.amazonaws.com**. This site allows you to browse and engage with the PhotoAlbum web application.



lbthu-asm2-1352528080.us-east-1.elb.amazonaws.com/photoalbum/album.php

Student name: Tran Kim Thu

Student ID: 104061810

Tutorial session: Sunday 09:15AM

Uploaded photos:

Upload more photos

Photo	Name	Description	Creation date	Keywords
	Italy	beautiful view	2022-03-15	view
	Jace	award	2023-11-16	award
	Jace	award	2023-11-16	award
	Jace	award	2023-11-16	award

Moreover, if you wish to upload photos along with their related metadata, you can use the PhotoUploader webpage at **http://lbthu-asm2-1352528080.us-east-1.elb.amazonaws.com**. This page enables you to easily upload multiple photos and enter their respective metadata, thereby enhancing the functionality of the PhotoAlbum website.

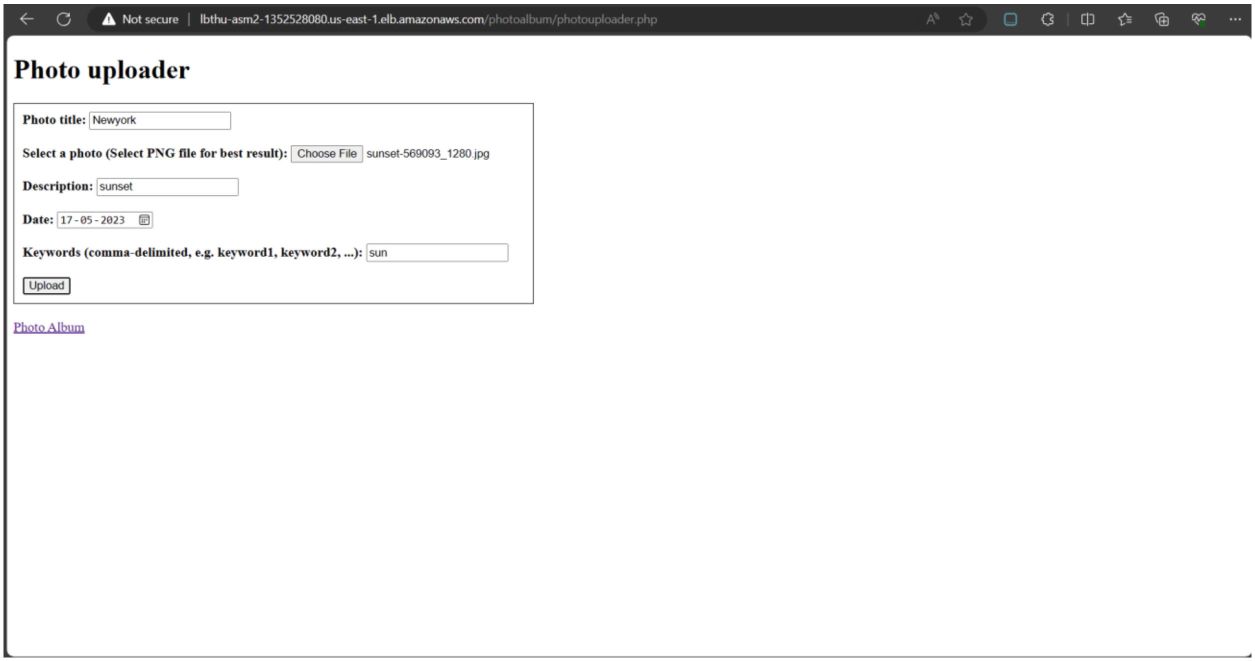

Not secure
lbthu-asm2-1352528080.us-east-1.elb.amazonaws.com/photoalbum/photouploader.php

Photo uploader

Photo title: Newyork

Select a photo (Select PNG file for best result): Choose File sunset-569093_1280.jpg

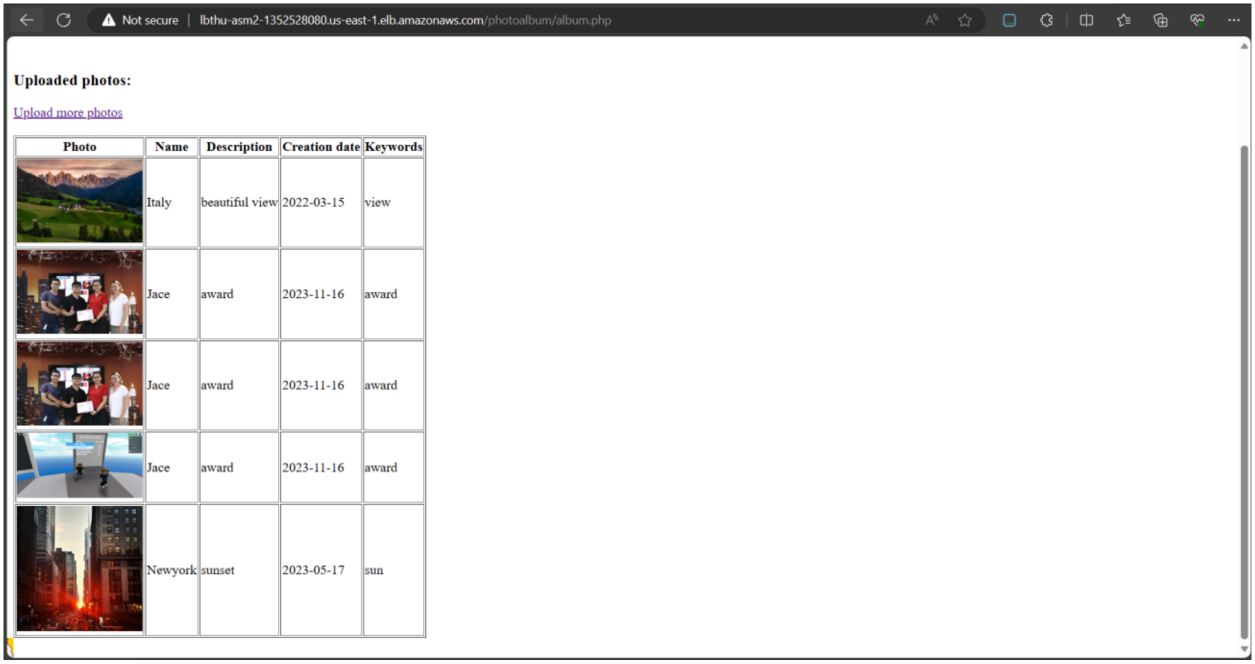
Description: sunset

Date: 17-05-2023

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

Upload

Photo Album

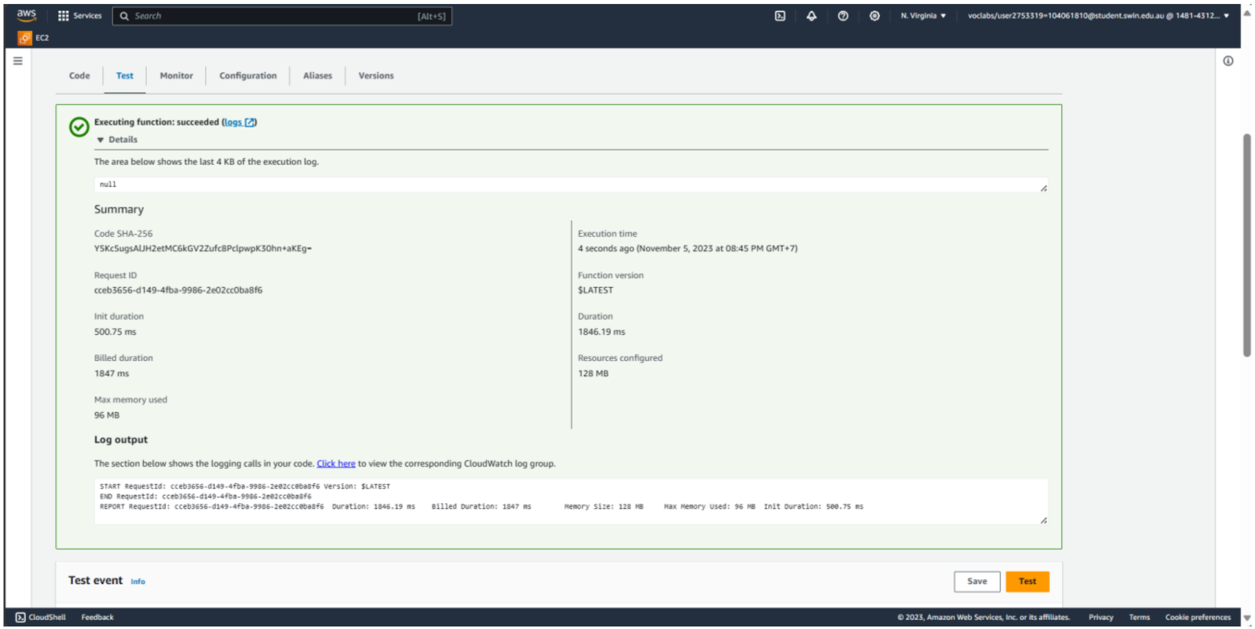

Not secure
lbthu-asm2-1352528080.us-east-1.elb.amazonaws.com/photoalbum/album.php

Uploaded photos:

Upload more photos

Photo	Name	Description	Creation date	Keywords
	Italy	beautiful view	2022-03-15	view
	Jace	award	2023-11-16	award
	Jace	award	2023-11-16	award
	Jace	award	2023-11-16	award
	Newyork	sunset	2023-05-17	sun

2. Resizing Lambda



Executing function: succeeded (logs)

Details

The area below shows the last 4 KB of the execution log.

```
null
```

Summary

Code SHA-256
Y5Kc5ugsAUH2etMC6kGV2Zufc8PclpwpK30hn+aKEg=

Request ID
cceb3656-d149-4fba-9986-2e02cc0ba8f6

Init duration
500.75 ms

Billed duration
1847 ms

Max memory used
96 MB

Execution time
4 seconds ago (November 5, 2023 at 08:45 PM GMT+7)

Function version
$LATEST

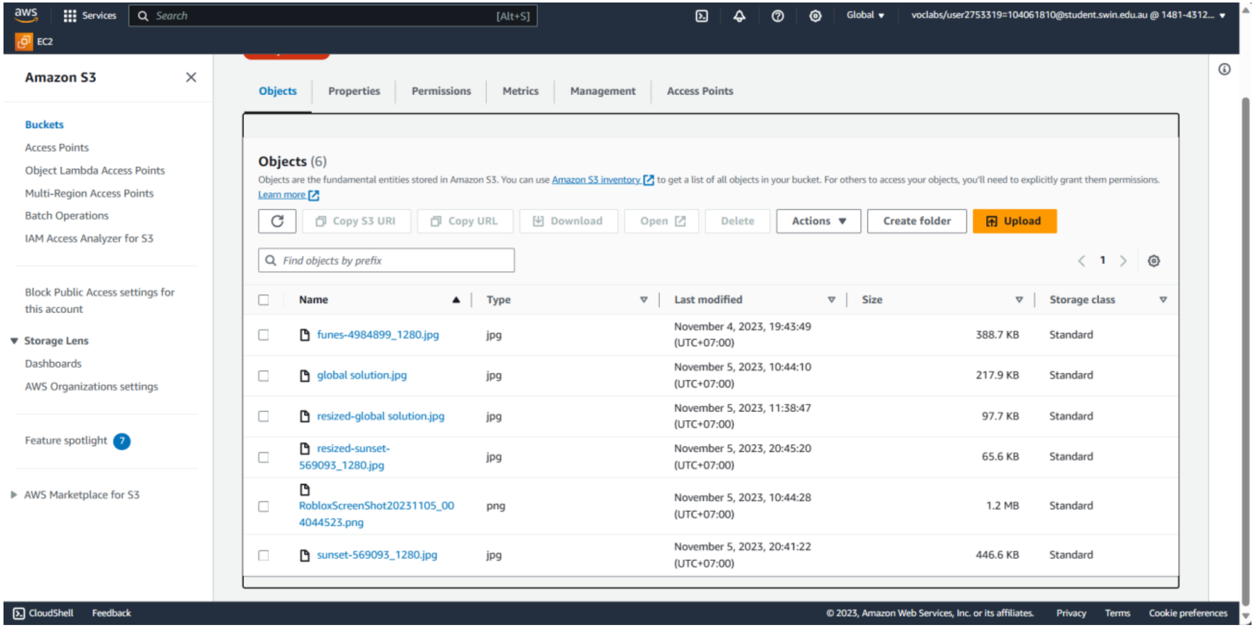
Duration
1846.19 ms

Resources configured
128 MB

Log output

The section below shows the logging calls in your code. Click here to view the corresponding CloudWatch log group.

```
START RequestId: cceb3656-d149-4fba-9986-2e02cc0ba8f6 Version: $LATEST
END RequestId: cceb3656-d149-4fba-9986-2e02cc0ba8f6
REPORT RequestId: cceb3656-d149-4fba-9986-2e02cc0ba8f6  Duration: 1846.19 ms    Billed Duration: 1847 ms        Memory Size: 128 MB     Max Memory Used: 96 MB  Init Duration: 500.75 ms
```


Services
Search [Alt+S]
Global
voclabs/user2753319=104061810@student.swin.edu.au @ 1481-4312...
EC2
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 7
AWS Marketplace for S3
Objects
Properties
Permissions
Metrics
Management
Access Points

Objects (6)

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

	Name	Type	Last modified	Size	Storage class
□	funes-4984899_1280.jpg	jpg	November 4, 2023, 19:43:49 (UTC+07:00)	388.7 KB	Standard
□	global solution.jpg	jpg	November 5, 2023, 10:44:10 (UTC+07:00)	217.9 KB	Standard
□	resized-global solution.jpg	jpg	November 5, 2023, 11:38:47 (UTC+07:00)	97.7 KB	Standard
□	resized-sunset-569093_1280.jpg	jpg	November 5, 2023, 20:45:20 (UTC+07:00)	65.6 KB	Standard
□	RobloxScreenShot20231105_004044523.png	png	November 5, 2023, 10:44:28 (UTC+07:00)	1.2 MB	Standard
□	sunset-569093_1280.jpg	jpg	November 5, 2023, 20:41:22 (UTC+07:00)	446.6 KB	Standard