COS20019 Cloud Computing Architecture

Developing a highly available Photo Album website

Nguyen Khanh Toan

104180605

Tutor class: 18:30 Wednesday

104180605@student.swin.edu.au

***Abstract*— Web server application has become immensely widespread with the enormous accesses at the same time to an individual host, and that remain effecting of overload to the computing infrastructure. AWS Auto Scaling group have been recognized as a solution to resolve and handle the load for the server instance by providing multiple pre-configuration instances using launch instance with Amazon Machine Image (AMI) and accessed through Elastic Load Balancer (ELB) to control the traffic between each instance. This resulted a balance, healthy infrastructure and this report is to illustrate the configuration of a highly available Photo Album website.**

Keywords—AWS, auto scaling, security, cloud, load balancer.

I. INTRODUCTION

The photo album website involves instance creation, hosting, and pre-configuration AMI of "Dev Server" in VPC with variety AWS services, including RDS, S3, and Lambda. The function of the website server allows public user can access and upload photos to web server album through HTTP protocol to ELB. The website integration with the S3 bucket, RDS database, and Lambda function, the source code provided, and AWS SDK installed make all the photos uploaded resized automatically by thumbnail then upload it to album databases.

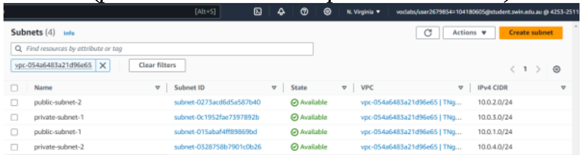
.

II. WEBSITE INFRASTRUCTURE

A. Website Infrastructure configuration

1) *Virtual Private Cloud (VPC):*

- VPC configuration with 2 Availability Zones (AZs) (*us-east-1a* and *us-east-1b*) with 2 public subnets (*public-subnet-1* and *public-subnet-2)* and 2 private subnets (*private-subnet-1* and *private-subnet-2)*.

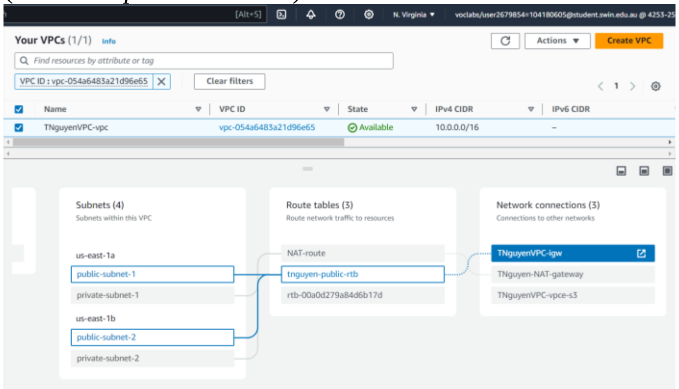


[Alt+S]
N. Virginia
voclabs/user2679854=104180605@student.swin.edu.au @ 4253-2511
Subnets (4) Info
Actions
Create subnet
Find resources by attribute or tag
vpc-054a6483a21d96e65
Clear filters
1

Name	Subnet ID	State	VPC	IPv4 CIDR
public-subnet-2	subnet-0273acd6d5a587b40	Available	vpc-054a6483a21d96e65 | TNg...	10.0.2.0/24
private-subnet-1	subnet-0c1952fae7397892b	Available	vpc-054a6483a21d96e65 | TNg...	10.0.3.0/24
public-subnet-1	subnet-015abaf4ff89869bd	Available	vpc-054a6483a21d96e65 | TNg...	10.0.1.0/24
private-subnet-2	subnet-0328758b7901c0b26	Available	vpc-054a6483a21d96e65 | TNg...	10.0.4.0/24

Figure 1: VPC Subnet CIDR

- Route table for public subnets are routing to internet gateway and private subnets are to the NAT gateway (located in *public-subnet-1*).

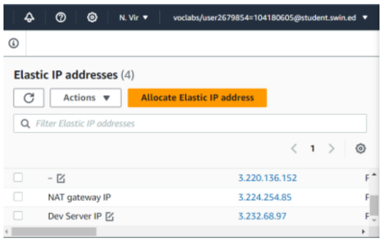


[Alt+S]
N. Virginia
voclabs/user2679854=104180605@student.swin.edu.au @ 4253-25
Your VPCs (1/1) Info
Actions
Create VPC
Find resources by attribute or tag
VPC ID : vpc-054a6483a21d96e65
Clear filters
1

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
TNguyenVPC-vpc	vpc-054a6483a21d96e65	Available	10.0.0.0/16	–

Figure 2: VPC Resource Map

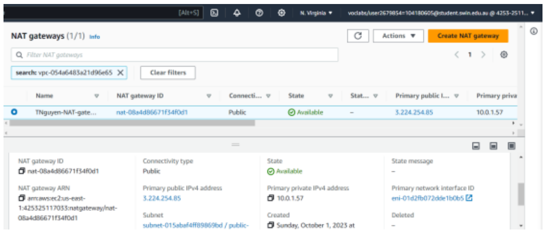
- Elastic public IP address for NAT gateway is 3.224.254.85 and for Dev Server Instance is 3.232.68.97



N. Vir
voclabs/user2679854=104180605@student.swin.ed
Elastic IP addresses (4)
Actions
Allocate Elastic IP address
Filter Elastic IP addresses
1

–	3.220.136.152
NAT gateway IP	3.224.254.85
Dev Server IP	3.232.68.97

Figure 3: Elastic IP



Name	NAT gateway ID	Connecti...	State	Stat...	Primary public I...	Primary priva
TNguyen-NAT-gate...	nat-08a4d86671f34f0d1	Public	Available	–	3.224.254.85	10.0.1.57

NAT gateway ID
nat-08a4d86671f34f0d1

NAT gateway ARN
arn:aws:ec2:us-east-1:425325117033:natgateway/nat-08a4d86671f34f0d1

Connectivity type
Public

Primary public IPv4 address
3.224.254.85

Subnet
subnet-015abaf4ff89869bd / public-

State
Available

Primary private IPv4 address
10.0.1.57

Created
Sunday, October 1, 2023 at

State message
–

Primary network interface ID
eni-01d2fb072dde1b0b5

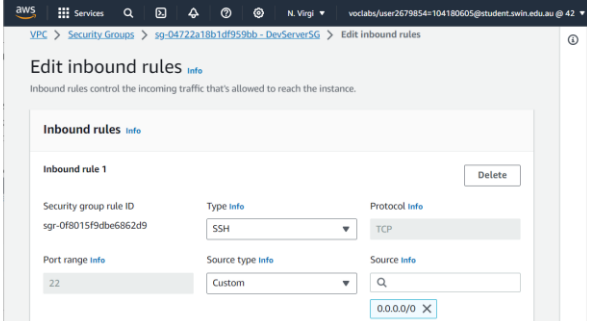
Deleted
–

Figure 4: Nat Gateway in public subnet 1

XXX-X-XXXX-XXXX-X/XIEEEX/$XX.00 ©20XX IEEE

2) Security Group: The VPC architecture contains 4 security groups in total. Each security group has difference purpose of inbounce and outbounce role to block the access from other source.

- DevServerSG: Because of Dev Server containing infrastructure of the web server (to create AMIs for launch instance) so the inbound rule is set to SSH only, so it is not able to access by HTTP or HTTPS protocol. The outbound rule is also set to SSH.



VPC > Security Groups > sg-04722a18b1df959bb - DevServerSG > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Inbound rule 1 Delete

Security group rule ID
sgr-0f8015f9dbe6862d9

Type Info
SSH

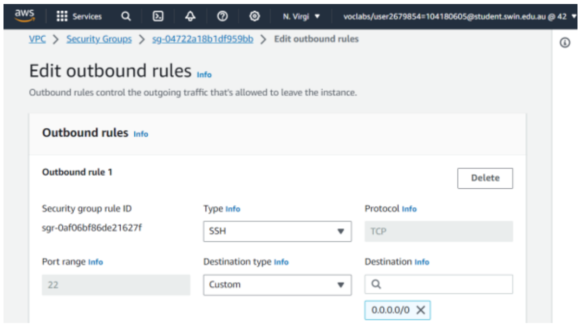
Protocol Info
TCP

Port range Info
22

Source type Info
Custom

Source Info
0.0.0.0/0

Figure 5: Inbound rule of DevServerSG



VPC > Security Groups > sg-04722a18b1df959bb > Edit outbound rules

Edit outbound rules Info

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rules Info

Outbound rule 1 Delete

Security group rule ID
sgr-0af06bf86de21627f

Type Info
SSH

Protocol Info
TCP

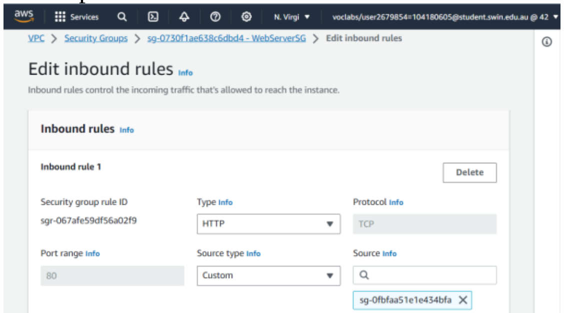
Port range Info
22

Destination type Info
Custom

Destination Info
0.0.0.0/0

Figure 6: Outbound rule of DevServerSG

- WebServerSG: Web Server only allow traffic forwarded through HTTP protocol from Elastic Load Balancer, so the inbound rule is set to HTTP protocol from source "ELBSG" security group. Outbound rule for this is all traffic because the infrastructure containing multiple protocol (HTTP, file packets…) to multiple destination.



VPC > Security Groups > sg-0730f1ae638c6dbd4 - WebServerSG > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Inbound rule 1 Delete

Security group rule ID
sgr-067afe59df56a02f9

Type Info
HTTP

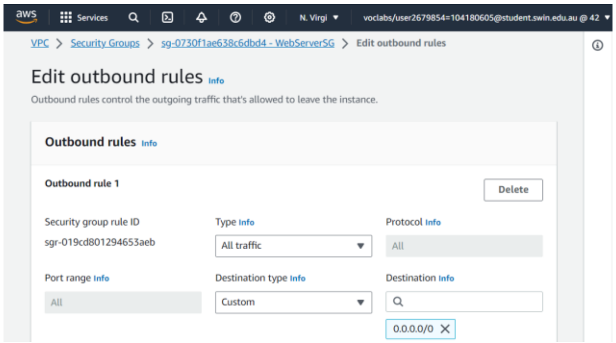
Protocol Info
TCP

Port range Info
80

Source type Info
Custom

Source Info
sg-0fbfaa51e1e434bfa

Figure 7: Inbound rule of WebServerSG



VPC > Security Groups > sg-0730f1ae638c6dbd4 - WebServerSG > Edit outbound rules

Edit outbound rules Info

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rules Info

Outbound rule 1 Delete

Security group rule ID
sgr-019cd801294653aeb

Type Info
All traffic

Protocol Info
All

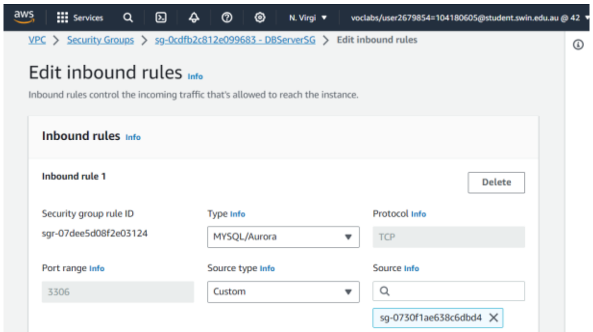
Port range Info
All

Destination type Info
Custom

Destination Info
0.0.0.0/0

Figure 8: Outbound rule of WebServerSG

- DBServerSG: The Database Server RDS only receives MySQL query from Web Server, so the inbound rule is set to MYSQL/Aurora from the source "WebServerSG" security group. The outbound rule is set to all traffic.



VPC > Security Groups > sg-0cdfb2c812e099683 - DBServerSG > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Inbound rule 1 Delete

Security group rule ID
sgr-07dee5d08f2e03124

Type Info
MYSQL/Aurora

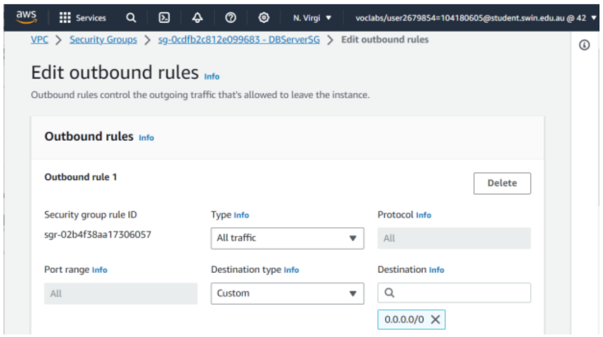
Protocol Info
TCP

Port range Info
3306

Source type Info
Custom

Source Info
sg-0730f1ae638c6dbd4

Figure 9: Inbound rule of DBServerSG



VPC > Security Groups > sg-0cdfb2c812e099683 - DBServerSG > Edit outbound rules

Edit outbound rules Info

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rules Info

Outbound rule 1 Delete

Security group rule ID
sgr-02b4f38aa17306057

Type Info
All traffic

Protocol Info
All

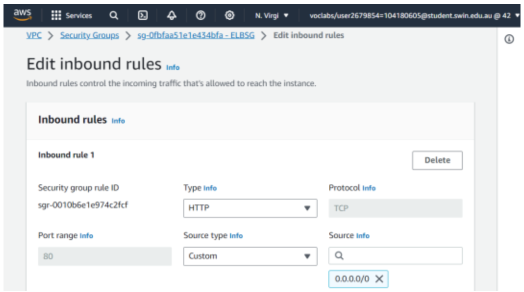
Port range Info
All

Destination type Info
Custom

Destination Info
0.0.0.0/0

Figure 10: Outbound rule of DBServerSG

- ELBSG: Load balancer receives traffic from public internet user through HTTP protocol so the inbound rule for this security group is set to HTTP protocol. The outbound rule is set to all traffic.



VPC > Security Groups > sg-0fbfaa51e1e434bfa - ELBSG > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Inbound rule 1 Delete

Security group rule ID
sgr-0010b6e1e974c2fcf

Type Info
HTTP

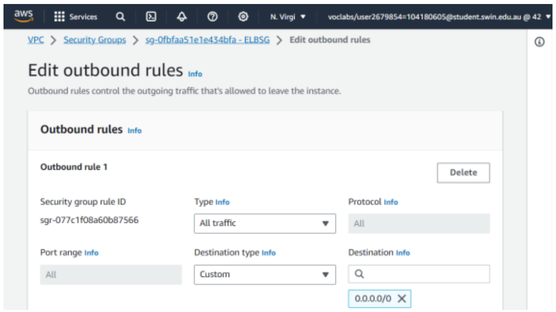
Protocol Info
TCP

Port range Info
80

Source type Info
Custom

Source Info
0.0.0.0/0

Figure 11: Inbound rule of ELBSG



VPC > Security Groups > sg-0fbfaa51e1e434bfa - ELBSG > Edit outbound rules

Edit outbound rules Info

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rules Info

Outbound rule 1

Security group rule ID: sgr-077c1f08a60b87566

Type Info: All traffic

Protocol Info: All

Port range Info: All

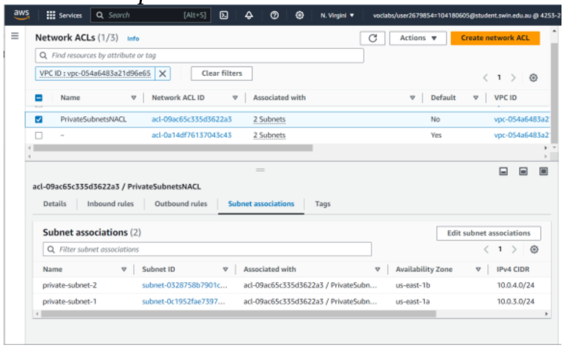
Destination type Info: Custom

Destination Info: 0.0.0.0/0

Figure 12: Outbound rule of ELBSG

3) Network Access Control List (NACL):

- The implementation of Network Access Control List used to enhance the security by implementing a permission layer attaching with the private subnet that containing Web Server Instance.
- The Network ACL named as “PrivateSubnetsNACL” associate with two private subnets in the VPC, *private-subnet-1* and *private-subnet-2*.



aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2679854=104180605@student.swin.edu.au @ 4253-2
Actions
Create network ACL
Find resources by attribute or tag
Clear filters

Network ACLs (1/3) Info

VPC ID : vpc-054a6483a21d96e65

	Name	Network ACL ID	Associated with	Default	VPC ID
☑	PrivateSubnetsNACL	acl-09ac65c335d3622a3	2 Subnets	No	vpc-054a6483a2
□	-	acl-0a14df76137043c43	2 Subnets	Yes	vpc-054a6483a2

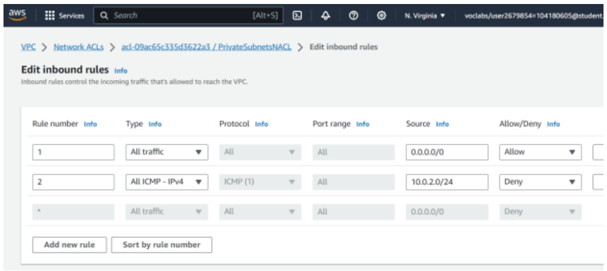
acl-09ac65c335d3622a3 / PrivateSubnetsNACL

Subnet associations (2)

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR
private-subnet-2	subnet-0328758b7901c...	acl-09ac65c335d3622a3 / PrivateSubn...	us-east-1b	10.0.4.0/24
private-subnet-1	subnet-0c1952fae7397...	acl-09ac65c335d3622a3 / PrivateSubn...	us-east-1a	10.0.3.0/24

Figure 13: NACL Association

- Network ACL rules for “PrivateSubnetsNACL” which allow for all protocol access but ICMP from the Dev Server in *public-subnet-2 (10.0.2.0/24)* so both inbound and outbound have to config to deny access for ICMP from *10.0.2.0/24* and allow access for all traffic.



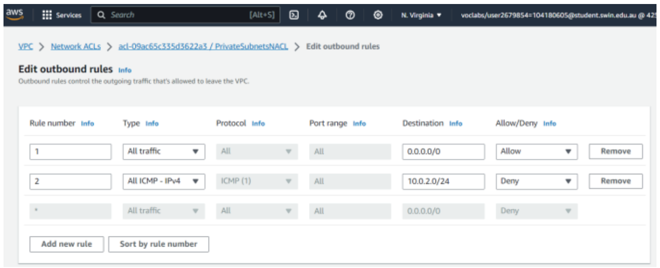
VPC > Network ACLs > acl-09ac65c335d3622a3 / PrivateSubnetsNACL > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the VPC.

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

Figure 14: NACL Inbound



VPC > Network ACLs > acl-09ac65c335d3622a3 / PrivateSubnetsNACL > Edit outbound rules

Edit outbound rules Info

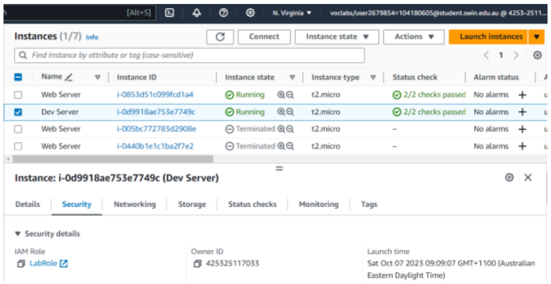
Outbound rules control the outgoing traffic that's allowed to leave the VPC.

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

Figure 15: NACL Outbound

4) IAM Role:

- The IAM Lab Role in management console with required permission are existed already with the name of “LabRole” or “Labinstancerole”. These lab roles assign with EC2 Instances, Launch template and Lambda. Following the least privilege principle, instances which assigned with LabRole user set permitted to grant access of putting object in S3 and call the CreateThumbnail function of Lambda.



[Alt+S]
N. Virginia
voclabs/user2679854=104180605@student.swin.edu.au @ 4253-2511...
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)

Instances (1/7) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
□	Web Server	i-0853d51c099fcd1a4	Running	t2.micro	2/2 checks passed	No alarms
☑	Dev Server	i-0d9918ae753e7749c	Running	t2.micro	2/2 checks passed	No alarms
□	Web Server	i-005bc772783d2908e	Terminated	t2.micro	–	No alarms
□	Web Server	i-0440b1e1c1ba2f7e2	Terminated	t2.micro	–	No alarms

Instance: i-0d9918ae753e7749c (Dev Server)

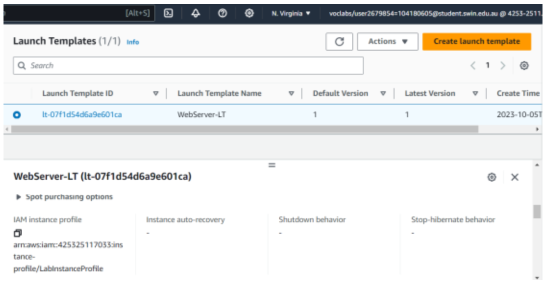
▼ Security details

IAM Role: LabRole

Owner ID: 425325117033

Launch time: Sat Oct 07 2023 09:09:07 GMT+1100 (Australian Eastern Daylight Time)

Figure 16: IAM LabRole for Dev Server



[Alt+S]
N. Virginia
voclabs/user2679854=104180605@student.swin.edu.au @ 4253-2511.
Actions
Create launch template
Search

Launch Templates (1/1) Info

	Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time
●	lt-07f1d54d6a9e601ca	WebServer-LT	1	1	2023-10-05T

WebServer-LT (lt-07f1d54d6a9e601ca)

▶ Spot purchasing options

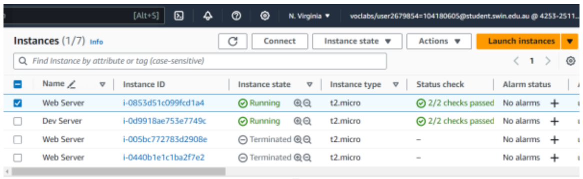
IAM instance profile: arn:aws:iam::425325117033:instance-profile/LabInstanceProfile

Instance auto-recovery: -

Shutdown behavior: -

Stop-hibernate behavior: -

Figure 17: IAM Role for Launch template



[Alt+S]
N. Virginia
voclabs/user2679854=104180605@student.swin.edu.au @ 4253-2511...
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)

Instances (1/7) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
☑	Web Server	i-0853d51c099fcd1a4	Running	t2.micro	2/2 checks passed	No alarms
□	Dev Server	i-0d9918ae753e7749c	Running	t2.micro	2/2 checks passed	No alarms
□	Web Server	i-005bc772783d2908e	Terminated	t2.micro	–	No alarms
□	Web Server	i-0440b1e1c1ba2f7e2	Terminated	t2.micro	–	No alarms

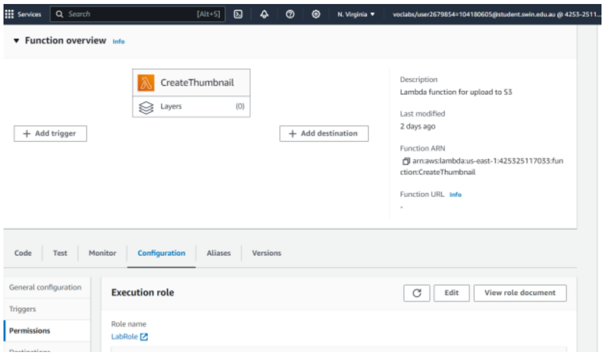
Instance: i-0853d51c099fcd1a4 (Web Server)

IAM Role: LabRole

Owner ID: 425325117033

Launch time: Sat Oct 07 2023 09:11:29 GMT+1100 (Australian Eastern Daylight Time)

Figure 18: IAM Lab Role for Auto Scaling Instances



Description
Lambda function for upload to S3

Last modified
2 days ago

Function ARN
arn:aws:lambda:us-east-1:425325117033:function:CreateThumbnail

Function URL Info
-

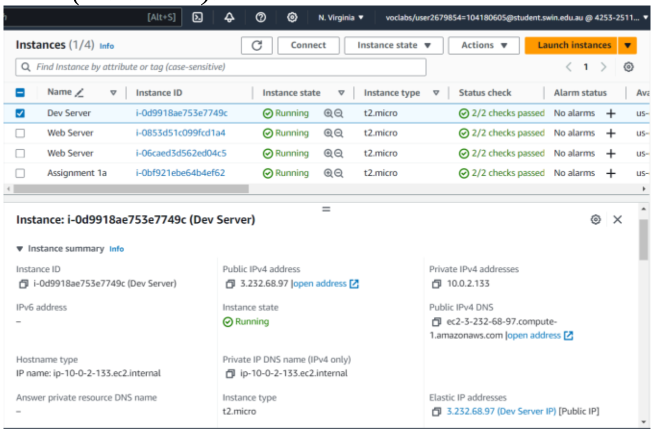
Execution role

Role name
LabRole

Figure 19: IAM LabRole for Lambda Create Thumbnail

5) Auto Scaling group (ASG): Auto Scaling group is a method of using launch template contains configuration from Amazon Machine Image (AMI) of an instance to launch instances automatically within the EC2 target group.

- The Dev Server serves as a developing platform and a base that containing necessary components to generate AMI for launch template such as PHP package, PHPmyAdmin, AWS SDK. The Dev server associate with Elastic IP address 3.232.68.97 and *public-subnet-2 (10.0.2.0/24)*.


[Alt+S]
N. Virginia
voclabs/user2679854=104180605@student.swin.edu.au @ 4253-2511...
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)

Instances (1/4) Info

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Ava
☑	Dev Server	i-0d9918ae753e7749c	Running	t2.micro	2/2 checks passed	No alarms	us-
☐	Web Server	i-0853d51c099fcd1a4	Running	t2.micro	2/2 checks passed	No alarms	us-
☐	Web Server	i-06caed3d562ed04c5	Running	t2.micro	2/2 checks passed	No alarms	us-
☐	Assignment 1a	i-0bf921ebe64b4ef62	Running	t2.micro	2/2 checks passed	No alarms	us-

Instance: i-0d9918ae753e7749c (Dev Server)

Instance summary Info

Instance ID
i-0d9918ae753e7749c (Dev Server)

Public IPv4 address
3.232.68.97 |open address

Private IPv4 addresses
10.0.2.133

IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-3-232-68-97.compute-1.amazonaws.com |open address

Hostname type
IP name: ip-10-0-2-133.ec2.internal

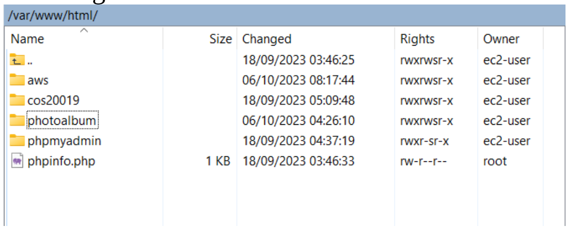
Private IP DNS name (IPv4 only)
ip-10-0-2-133.ec2.internal

Answer private resource DNS name
–

Instance type
t2.micro

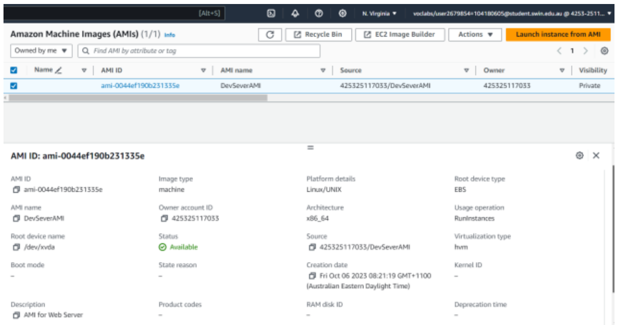
Elastic IP addresses
3.232.68.97 (Dev Server IP) [Public IP]

Figure 20: Dev Server Instance


/var/www/html/

Name	Size	Changed	Rights	Owner
..		18/09/2023 03:46:25	rwxrwsr-x	ec2-user
aws		06/10/2023 08:17:44	rwxrwsr-x	ec2-user
cos20019		18/09/2023 05:09:48	rwxrwsr-x	ec2-user
photoalbum		06/10/2023 04:26:10	rwxrwsr-x	ec2-user
phpmyadmin		18/09/2023 04:37:19	rwxr-sr-x	ec2-user
phpinfo.php	1 KB	18/09/2023 03:46:33	rw-r--r--	root

Figure 21: Components of Dev Server


[Alt+S]
N. Virginia
voclabs/user2679854=104180605@student.swin.edu.au @ 4253-2511...
Recycle Bin
EC2 Image Builder
Actions
Launch instance from AMI
Owned by me
Find AMI by attribute or tag

Amazon Machine Images (AMIs) (1/1) Info

☑	Name	AMI ID	AMI name	Source	Owner	Visibility
☑		ami-0044ef190b231335e	DevSeverAMI	425325117033/DevSeverAMI	425325117033	Private

AMI ID: ami-0044ef190b231335e

AMI ID
ami-0044ef190b231335e

Image type
machine

Platform details
Linux/UNIX

Root device type
EBS

AMI name
DevSeverAMI

Owner account ID
425325117033

Architecture
x86_64

Usage operation
RunInstances

Root device name
/dev/xvda

Status
Available

Source
425325117033/DevSeverAMI

Virtualization type
hvm

Boot mode
–

State reason
–

Creation date
Fri Oct 06 2023 08:21:19 GMT+1100 (Australian Eastern Daylight Time)

Kernel ID
–

Description
AMI for Web Server

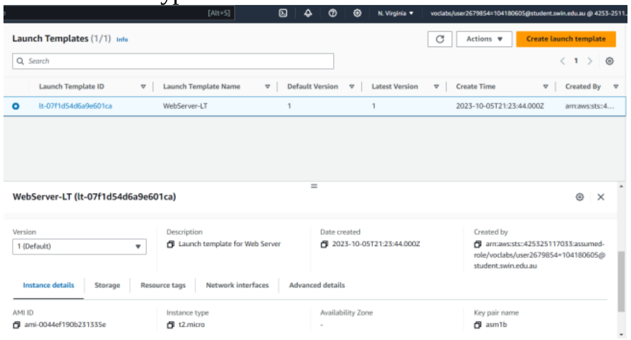
Product codes
–

RAM disk ID
–

Deprecation time
–

Figure 22: AMI with Dev Server template

- Launch template containing AMI from Dev Server with instance type t2.micro.



Launch Templates (1/1) Info

	Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time	Created By
●	lt-07f1d54d6a9e601ca	WebServer-LT	1	1	2023-10-05T21:23:44.000Z	arn:aws:sts::4...

WebServer-LT (lt-07f1d54d6a9e601ca)

Version
1 (Default)

Description
Launch template for Web Server

Date created
2023-10-05T21:23:44.000Z

Created by
arn:aws:sts::425325117033:assumed-role/voclabs/user2679854=104180605@student.swin.edu.au

AMI ID
ami-0044ef190b231335e

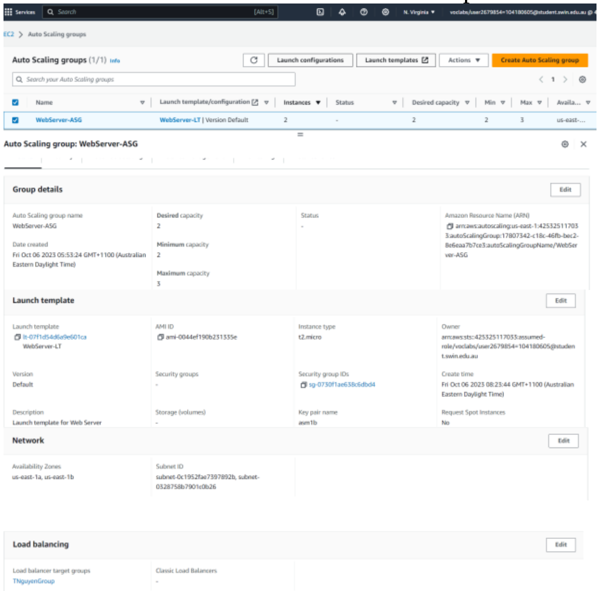
Instance type
t2.micro

Availability Zone
-

Key pair name
asm1b

Figure 23: Launch template configuration.

- The configuration of the ASG require launch template to generate instances automatically and maintain at least 2 instances and maximum of 3 instances. It ensures that the web server scalability can be control. The instance created automatically within the private subnet and use the WebServer-LT as a template.


Services
Search [Alt+S]
N. Virginia
voclabs/user2679854=104180605@student.swin.edu.au @
EC2 > Auto Scaling groups
Launch configurations
Launch templates
Actions
Create Auto Scaling group
Search your Auto Scaling groups
Edit

Auto Scaling groups (1/1) Info

☑	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availa...
☑	WebServer-ASG	WebServer-LT | Version Default	2	-	2	2	3	us-east-...

Auto Scaling group: WebServer-ASG

Group details

Auto Scaling group name
WebServer-ASG

Date created
Fri Oct 06 2023 05:53:24 GMT+1100 (Australian Eastern Daylight Time)

Desired capacity
2

Minimum capacity
2

Maximum capacity
3

Status
-

Amazon Resource Name (ARN)
arn:aws:autoscaling:us-east-1:425325117033:autoScalingGroup:17807342-c18c-46fb-bec2-8e6eaa7b7ce3:autoScalingGroupName/WebServer-ASG

Launch template

Launch template
lt-07f1d54d6a9e601ca
WebServer-LT

AMI ID
ami-0044ef190b231335e

Instance type
t2.micro

Owner
arn:aws:sts::425325117033:assumed-role/voclabs/user2679854=104180605@student.swin.edu.au

Version
Default

Security groups
-

Security group IDs
sg-0730f1ae638c6dbd4

Create time
Fri Oct 06 2023 08:23:44 GMT+1100 (Australian Eastern Daylight Time)

Description
Launch template for Web Server

Storage (volumes)
-

Key pair name
asm1b

Request Spot Instances
No

Network

Availability Zones
us-east-1a, us-east-1b

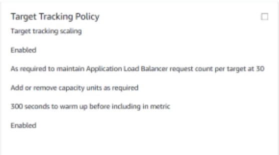
Subnet ID
subnet-0c1952fae7397892b, subnet-0328758b7901c0b26

Load balancing

Load balancer target groups
TNguyenGroup

Classic Load Balancers
-

Figure 24.1: ASG configuration



Target Tracking Policy

Target tracking scaling

Enabled

As required to maintain Application Load Balancer request count per target at 30

Add or remove capacity units as required

300 seconds to warm up before including in metric

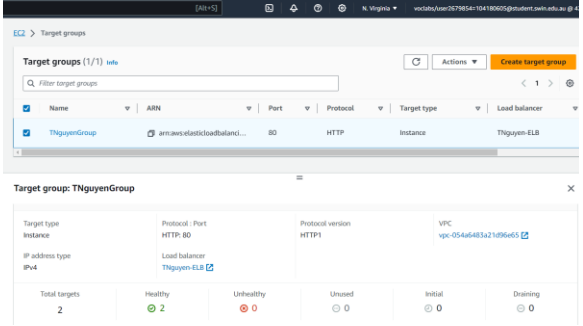
Enabled

Figure 24.1: Target Tracking Policy

- To achieve the resource utilization, target tracking policy created to track down the number of requests received from ELB target group maintain at 30 requests. The auto scaling would decide to scale up or down base on the request load to maintain the desired state. (Figure 24.2)

6) Elastic Load Balancer *(ELB)*:

- Elastic Load Balancer located at public subnet (*10.0.1.0/24* and *10.0.2.0/24*) to balance, control and forward the HTTP protocol traffics flow into target group (Figure 22) that containing auto generated instances associate with two private subnet (*10.0.3.0/24* and *10.0.4.0/24*)



Target groups (1/1) Info

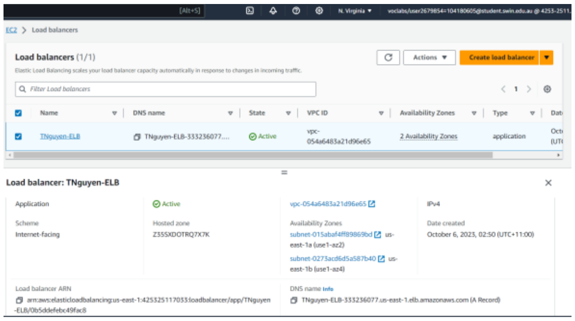
☑	Name	ARN	Port	Protocol	Target type	Load balancer
☑	TNguyenGroup	arn:aws:elasticloadbalanci...	80	HTTP	Instance	TNguyen-ELB

Target group: TNguyenGroup

Target type: Instance
Protocol : Port: HTTP: 80
Protocol version: HTTP1
VPC: vpc-054a6483a21d96e65
IP address type: IPv4
Load balancer: TNguyen-ELB

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

Figure 25: Target group



Load balancers (1/1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

☑	Name	DNS name	State	VPC ID	Availability Zones	Type	Dat
☑	TNguyen-ELB	TNguyen-ELB-333236077....	Active	vpc-054a6483a21d96e65	2 Availability Zones	application	Oct (UT

Load balancer: TNguyen-ELB

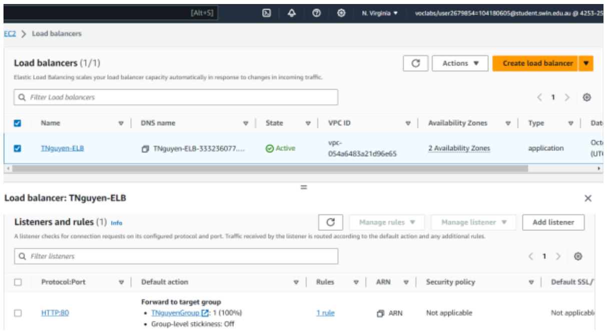
Application
Active
vpc-054a6483a21d96e65
IPv4

Scheme: Internet-facing
Hosted zone: Z35SXDOTRQ7X7K
Availability Zones: subnet-015abaf4ff89869bd us-east-1a (use1-az2); subnet-0273acd6d5a587b40 us-east-1b (use1-az4)
Date created: October 6, 2023, 02:50 (UTC+11:00)

Load balancer ARN: arn:aws:elasticloadbalancing:us-east-1:425325117033:loadbalancer/app/TNguyen-ELB/0b5ddefebc49fac8

DNS name Info: TNguyen-ELB-333236077.us-east-1.elb.amazonaws.com (A Record)

Figure 26.1: Load Balancer Detail



Load balancers (1/1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

☑	Name	DNS name	State	VPC ID	Availability Zones	Type	Dat
☑	TNguyen-ELB	TNguyen-ELB-333236077....	Active	vpc-054a6483a21d96e65	2 Availability Zones	application	Oct (UT

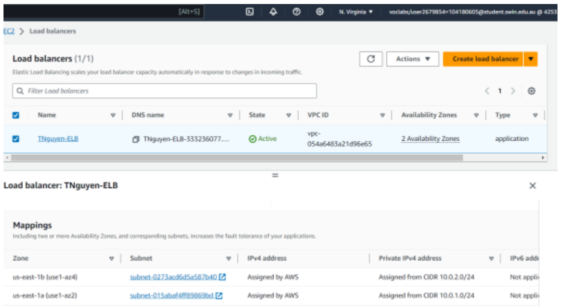
Load balancer: TNguyen-ELB

Listeners and rules (1) Info

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

□	Protocol:Port	Default action	Rules	ARN	Security policy	Default SSL/
□	HTTP:80	Forward to target group • TNguyenGroup: 1 (100%) • Group-level stickiness: Off	1 rule	ARN	Not applicable	Not applicabl

Figure 26.2: Load Balancer Listener



Load balancers (1/1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

☑	Name	DNS name	State	VPC ID	Availability Zones	Type
☑	TNguyen-ELB	TNguyen-ELB-333236077....	Active	vpc-054a6483a21d96e65	2 Availability Zones	application

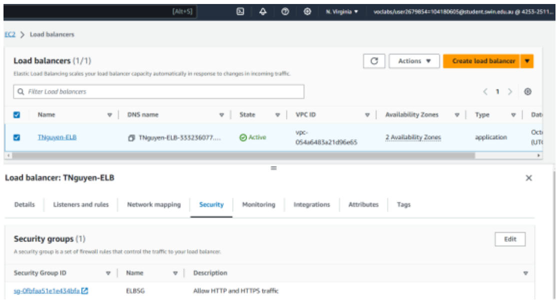
Load balancer: TNguyen-ELB

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 addr
us-east-1b (use1-az4)	subnet-0273acd6d5a587b40	Assigned by AWS	Assigned from CIDR 10.0.2.0/24	Not appli
us-east-1a (use1-az2)	subnet-015abaf4ff89869bd	Assigned by AWS	Assigned from CIDR 10.0.1.0/24	Not appli

Figure 26.3: Load Balancer Network mapping



Load balancers (1/1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

☑	Name	DNS name	State	VPC ID	Availability Zones	Type	Dat
☑	TNguyen-ELB	TNguyen-ELB-333236077....	Active	vpc-054a6483a21d96e65	2 Availability Zones	application	Oct (UT

Load balancer: TNguyen-ELB

Security groups (1)

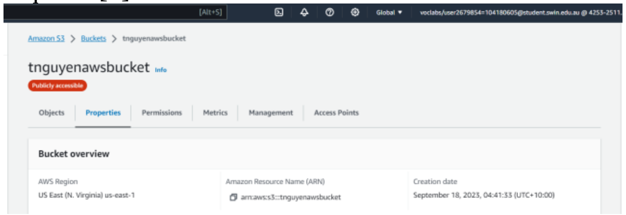
A security group is a set of firewall rules that control the traffic to your load balancer.

Security Group ID	Name	Description
sg-0fbfaa51e1e434bfa	ELBSG	Allow HTTP and HTTPS traffic

Figure 26.4: Load Balancer Security group

7) Simple Storage Service (S3):

- The configuration of S3 bucket is almost the same as procedure in assignment1b, except for bucket policy. The permission and policy are changed to ensure the appropriate accessibility of storing objects in S3 bucket. This bucket policy permission allows get object from S3 to necessary access and restrict unauthorized HTTP access from making AWS requests [1].



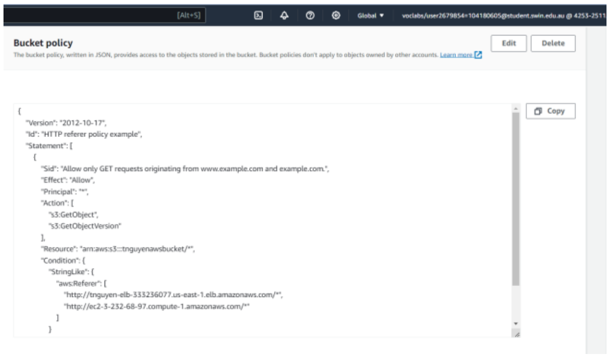
[Alt+S]
Global
voclabs/user2679854=104180605@student.swin.edu.au @ 4253-2511...
Amazon S3 > Buckets > tnguyenawsbucket
Info
Publicly accessible
Objects
Properties
Permissions
Metrics
Management
Access Points

tnguyenawsbucket

Bucket overview

AWS Region: US East (N. Virginia) us-east-1
Amazon Resource Name (ARN): arn:aws:s3:::tnguyenawsbucket
Creation date: September 18, 2023, 04:41:33 (UTC+10:00)

Figure 27: S3 bucket properties



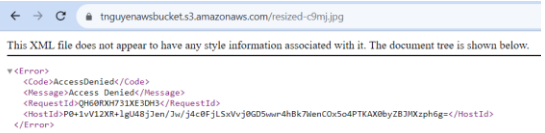
[Alt+S]
Global
voclabs/user2679854=104180605@student.swin.edu.au @ 4253-2511
Edit
Delete
Copy

Bucket policy

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

```
{
  "Version": "2012-10-17",
  "Id": "HTTP referer policy example",
  "Statement": [
    {
      "Sid": "Allow only GET requests originating from www.example.com and example.com.",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::tnguyenawsbucket/*",
      "Condition": {
        "StringLike": {
          "aws:Referer": [
            "http://tnguyen-elb-333236077.us-east-1.elb.amazonaws.com/*",
            "http://ec2-3-232-68-97.compute-1.amazonaws.com/*"
          ]
        }
```

Figure 28: S3 bucket policy



tnguyenawsbucket.s3.amazonaws.com/resized-c9mj.jpg

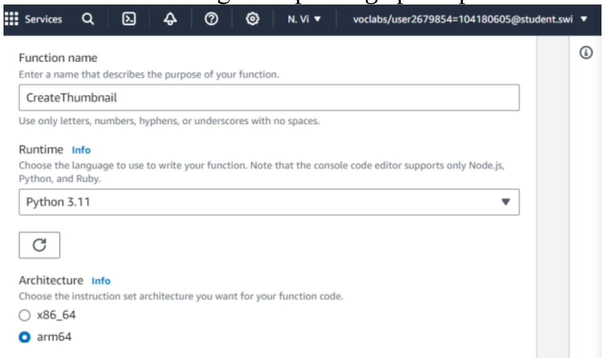
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>QH60RXH731XE3DH3</RequestId>
   <HostId>P0+1vV12XR+lgU48jJen/Jw/j4c0FjLSxVvj0GD5wwr4hBk7WenCOx5o4PTKAX0byZBJMXzph6g=</HostId>
 </Error>
```

Figure 29: Object inaccessible directly

8) Lambda function:

- Lambda function created with named “CreateThumbnail" using runtime Python 3.1, architecture type arm64 and execution role as “LabRole” following least-privilege principle.

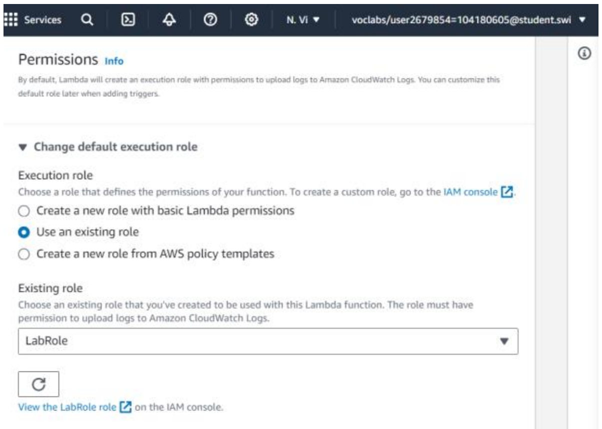


Function name
Enter a name that describes the purpose of your function.
CreateThumbnail
Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.
Python 3.11

Architecture Info
Choose the instruction set architecture you want for your function code.
○ x86_64
● arm64

Figure 30.1: Lambda function creation



Permissions Info
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

▼ Change default execution role

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console.
○ Create a new role with basic Lambda permissions
● Use an existing role
○ Create a new role from AWS policy templates

Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.
LabRole

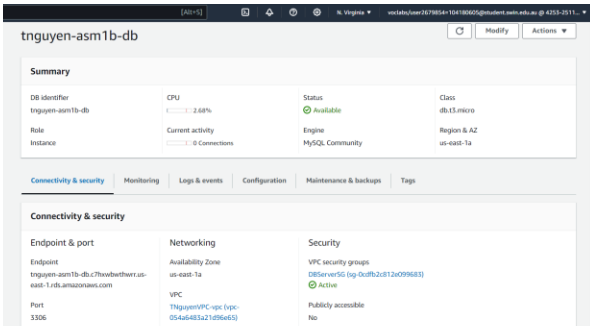
View the LabRole role on the IAM console.

Figure 30.2: Lambda function permission

- The source code package “lambda-deployment-package.zip” deploys successfully to resize, download, and upload the photo on S3 bucket.

9) Relational Database Service (RDS): The RDS configuration remains the same as in the previous assignment.

- Engine option: MySQL 8.0.33
- Templates: Free tier
- DB instance identifier: tnguyen-asm1b-db (use database from previous assignment)
- Db subnet group: dbsubnetgroup
- Availability Zone: us-east-1a



tnguyen-asm1b-db

Summary

DB identifier	CPU	Status	Class
tnguyen-asm1b-db	2.68%	Available	db.t3.micro
Role	Current activity	Engine	Region & AZ
Instance	0 Connections	MySQL Community	us-east-1a

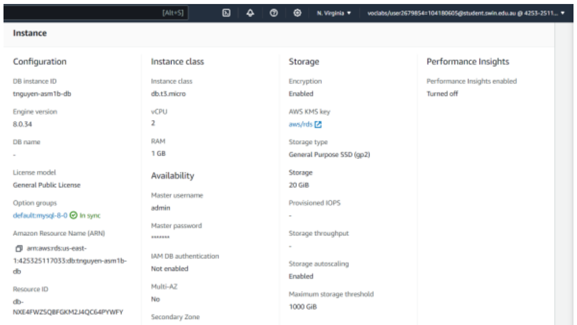
Connectivity & security

Endpoint & port
Endpoint: tnguyen-asm1b-db.c7hxwbwthwrr.us-east-1.rds.amazonaws.com
Port: 3306

Networking
Availability Zone: us-east-1a
VPC: TNguyenVPC-vpc (vpc-054a6483a21d96e65)

Security
VPC security groups: DBServerSG (sg-0cdfb2c812e099683) Active
Publicly accessible: No

Figure 31: RDS connectivity



[Alt+S]
N. Virginia
voclabs/user2679854=104180605@student.swin.edu.au @ 4253-2511...

Instance

Configuration
DB instance ID: tnguyen-asm1b-db
Engine version: 8.0.34
DB name: -
License model: General Public License
Option groups: default:mysql-8-0 In sync
Amazon Resource Name (ARN): arn:aws:rds:us-east-1:425325117033:db:tnguyen-asm1b-db
Resource ID: db-NXE4FWZSQBFGKM2J4QC64PYWFY

Instance class
Instance class: db.t3.micro
vCPU: 2
RAM: 1 GB

Availability
Master username: admin
Master password: *******
IAM DB authentication: Not enabled
Multi-AZ: No
Secondary Zone

Storage
Encryption: Enabled
AWS KMS key: aws/rds
Storage type: General Purpose SSD (gp2)
Storage: 20 GiB
Provisioned IOPS: -
Storage throughput: -
Storage autoscaling: Enabled
Maximum storage threshold: 1000 GiB

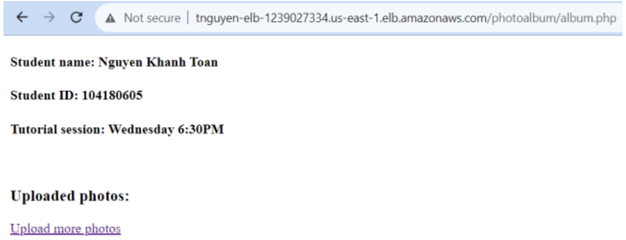
Performance Insights
Performance Insights enabled: Turned off

Figure 32: RDS configuration

B. *Website Infrastructure configuration*

1) Website accessibility:

- Website photo album server allow user can view the photo album access through ELB DNS: http://tnguyen-elb-1239027334.us-east-1.elb.amazonaws.com/photoalbum/album.php
-



Not secure | tnguyen-elb-1239027334.us-east-1.elb.amazonaws.com/photoalbum/album.php

Student name: Nguyen Khanh Toan

Student ID: 104180605

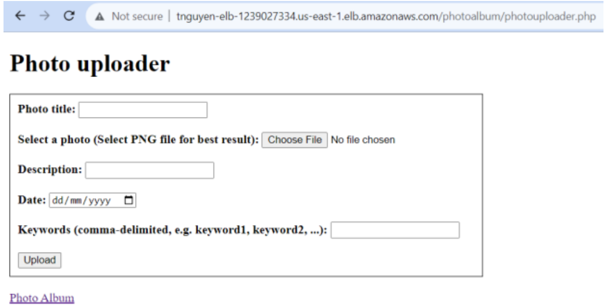
Tutorial session: Wednesday 6:30PM

Uploaded photos:

Upload more photos

Figure 33: Photo album website

- Website photo uploader server access through ELB DNS: http://tnguyen-elb-1239027334.us-east-1.elb.amazonaws.com/photoalbum/photouploader.php



← → C ▲ Not secure | tnguyen-elb-1239027334.us-east-1.elb.amazonaws.com/photoalbum/photouploader.php

Photo uploader

Photo title:

Select a photo (Select PNG file for best result): Choose File No file chosen

Description:

Date: dd/mm/yyyy

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

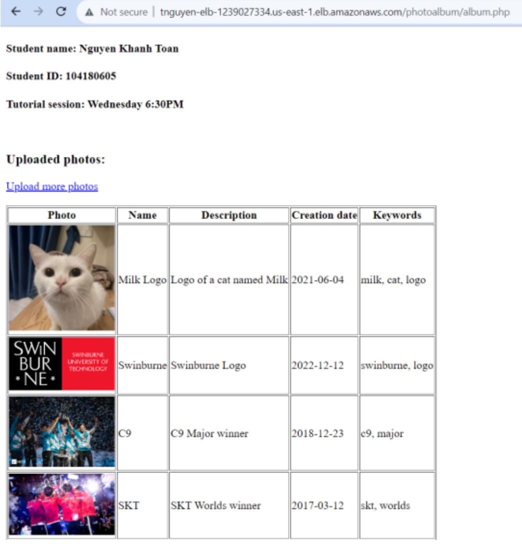
Upload

Photo Album

Figure 34: Photo uploader website

2) Photo display:

- After uploading photos and meta-data in the photo uploader website, all of the contents added to the database and can be displayed on the photo album website.



← → C ▲ Not secure | tnguyen-elb-1239027334.us-east-1.elb.amazonaws.com/photoalbum/album.php

Student name: Nguyen Khanh Toan

Student ID: 104180605

Tutorial session: Wednesday 6:30PM

Uploaded photos:

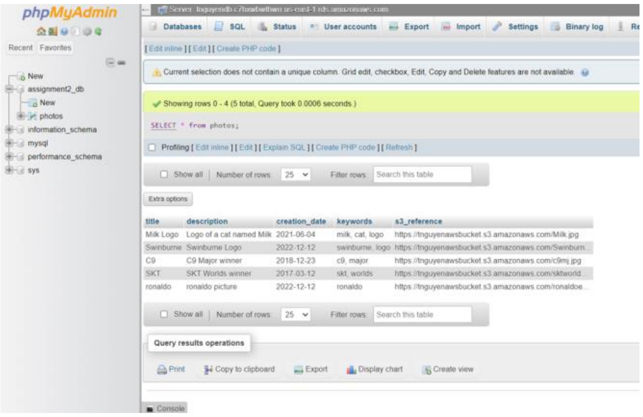
Upload more photos

Photo	Name	Description	Creation date	Keywords
	Milk Logo	Logo of a cat named Milk	2021-06-04	milk, cat, logo
	Swinburne	Swinburne Logo	2022-12-12	swinburne, logo
	C9	C9 Major winner	2018-12-23	c9, major
	SKT	SKT Worlds winner	2017-03-12	skt, worlds

Figure 35: Photo album display

3) Photos and meta-data upload

- The meta-data from the photo uploader page uploaded to the assignment2_db in RDS Services.


phpMyAdmin
Recent Favorites
New
assignment2_db
New
photos
information_schema
mysql
performance_schema
sys
Server: tnguyendb.c7bxwbwlhwn.us-east-1.rds.amazonaws.com
Databases SQL Status User accounts Export Import Settings Binary log
[Edit inline] [Edit] [Create PHP code]
Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
Show all | Number of rows: 25 Filter rows: Search this table
Extra options
Query results operations
Print Copy to clipboard Export Display chart Create view
Console

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

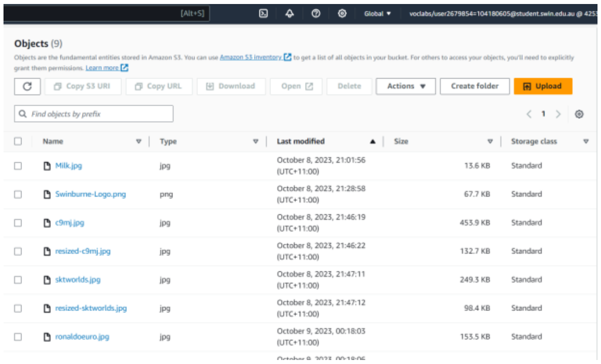
✓ Showing rows 0 - 4 (5 total, Query took 0.0006 seconds.)

```
SELECT * from photos;
```

title	description	creation_date	keywords	s3_reference
Milk Logo	Logo of a cat named Milk	2021-06-04	milk, cat, logo	https://tnguyenawsbucket.s3.amazonaws.com/Milk.jpg
Swinburne	Swinburne Logo	2022-12-12	swinburne, logo	https://tnguyenawsbucket.s3.amazonaws.com/Swinburn...
C9	C9 Major winner	2018-12-23	c9, major	https://tnguyenawsbucket.s3.amazonaws.com/c9mj.jpg
SKT	SKT Worlds winner	2017-03-12	skt, worlds	https://tnguyenawsbucket.s3.amazonaws.com/sktworld...
ronaldo	ronaldo picture	2022-12-12	ronaldo	https://tnguyenawsbucket.s3.amazonaws.com/ronaldoe...

Figure 36: Meta-data in database

- The photos uploading from the photo uploader stored in S3 bucket.



Objects (9)

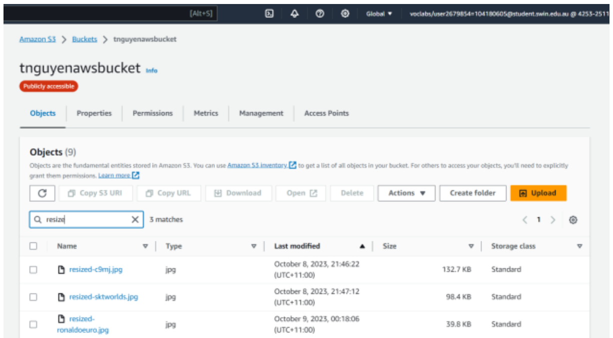
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class
Milk.jpg	jpg	October 8, 2023, 21:01:56 (UTC+11:00)	13.6 KB	Standard
Swinburne-Logo.png	png	October 8, 2023, 21:28:58 (UTC+11:00)	67.7 KB	Standard
c9mj.jpg	jpg	October 8, 2023, 21:46:19 (UTC+11:00)	453.9 KB	Standard
resized-c9mj.jpg	jpg	October 8, 2023, 21:46:22 (UTC+11:00)	132.7 KB	Standard
sktworlds.jpg	jpg	October 8, 2023, 21:47:11 (UTC+11:00)	249.3 KB	Standard
resized-sktworlds.jpg	jpg	October 8, 2023, 21:47:12 (UTC+11:00)	98.4 KB	Standard
ronaldoeuro.jpg	jpg	October 9, 2023, 00:18:03 (UTC+11:00)	153.5 KB	Standard

Figure 37: Photos in S3 bucket

4) Lambda function resize:

- After uploading in photo uploader website, it invokes the Lambda function to resize the photo as well as changing its name to "resized- [photo name]".



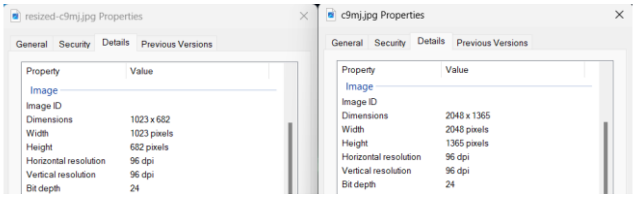
tnguyenawsbucket

Objects (9)

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
resized-c9mj.jpg	jpg	October 8, 2023, 21:46:22 (UTC+11:00)	132.7 KB	Standard
resized-sktworlds.jpg	jpg	October 8, 2023, 21:47:12 (UTC+11:00)	98.4 KB	Standard
resized-ronaldoeuro.jpg	jpg	October 9, 2023, 00:18:06 (UTC+11:00)	39.8 KB	Standard

Figure 38: Resized photos stored in S3 bucket.



resized-c9mj.jpg Properties

Property	Value
Image	
Image ID	
Dimensions	1023 x 682
Width	1023 pixels
Height	682 pixels
Horizontal resolution	96 dpi
Vertical resolution	96 dpi
Bit depth	24

c9mj.jpg Properties

Property	Value
Image	
Image ID	
Dimensions	2048 x 1365
Width	2048 pixels
Height	1365 pixels
Horizontal resolution	96 dpi
Vertical resolution	96 dpi
Bit depth	24

Figure 39: Comparison of original and resized photos.

References:

[1] Amazon Web Service, "Bucket policy examples - amazon simple storage service," docs.aws.amazon.com, 2023. Accessed: Jul. 16, 2023. [Online]. Available: https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies.html#example-bucket-policies-HTTPHTTPS