Assignment 2

COS20019 Cloud Computing Architecture

Tran Thanh Minh

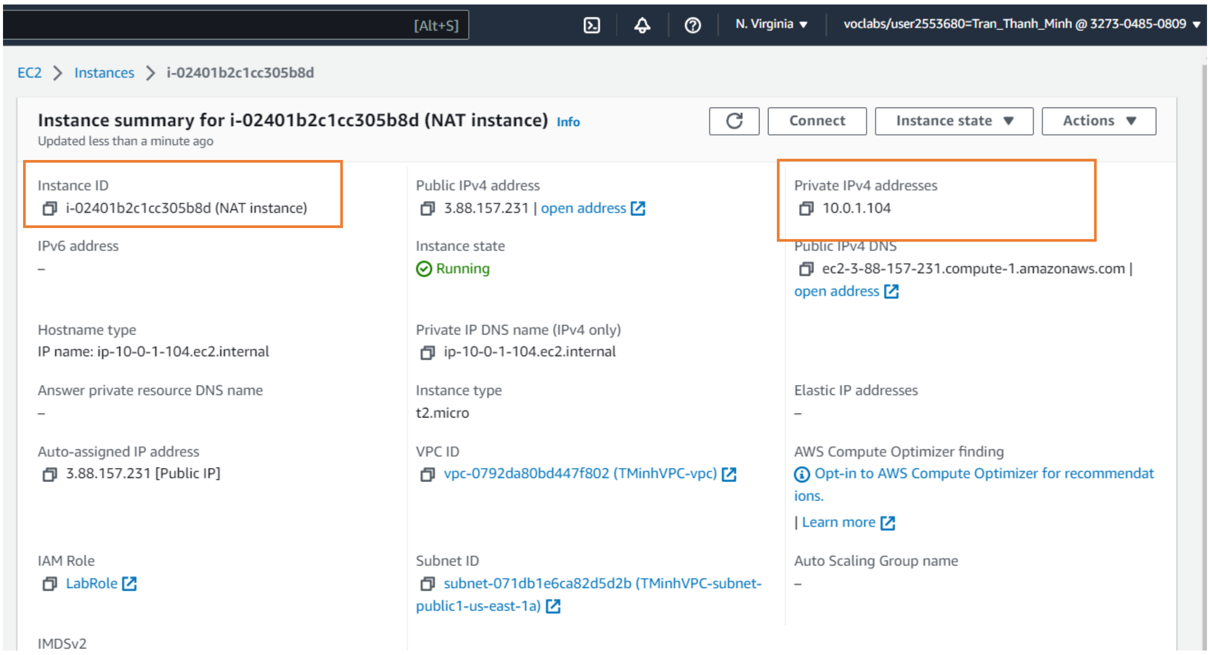
103809048

Website of Album: album.php

ELB DNS: http://assign2-elb-1843566538.us-east-1.elb.amazonaws.com/

Configure NAT instance.

- Configure **NAT instance** (i-02401b2c1cc305b8d) with private subnet **10.0.1.0/24** in the **TMinh-vpc** (vpc-0792da80bd447f802)
- Assign it with **the auto sign public IP** so that it can have public IP otherwise it will be empty.



[Alt+S]
N. Virginia ▼
voclabs/user2553680=Tran_Thanh_Minh @ 3273-0485-0809 ▼
EC2 > Instances > i-02401b2c1cc305b8d
Connect
Instance state ▼
Actions ▼

Instance summary for i-02401b2c1cc305b8d (NAT instance) Info

Updated less than a minute ago

Instance ID
i-02401b2c1cc305b8d (NAT instance)

Public IPv4 address
3.88.157.231 | open address

Private IPv4 addresses
10.0.1.104

IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-3-88-157-231.compute-1.amazonaws.com | open address

Hostname type
IP name: ip-10-0-1-104.ec2.internal

Private IP DNS name (IPv4 only)
ip-10-0-1-104.ec2.internal

Answer private resource DNS name
–

Instance type
t2.micro

Elastic IP addresses
–

Auto-assigned IP address
3.88.157.231 [Public IP]

VPC ID
vpc-0792da80bd447f802 (TMinhVPC-vpc)

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

IAM Role
LabRole

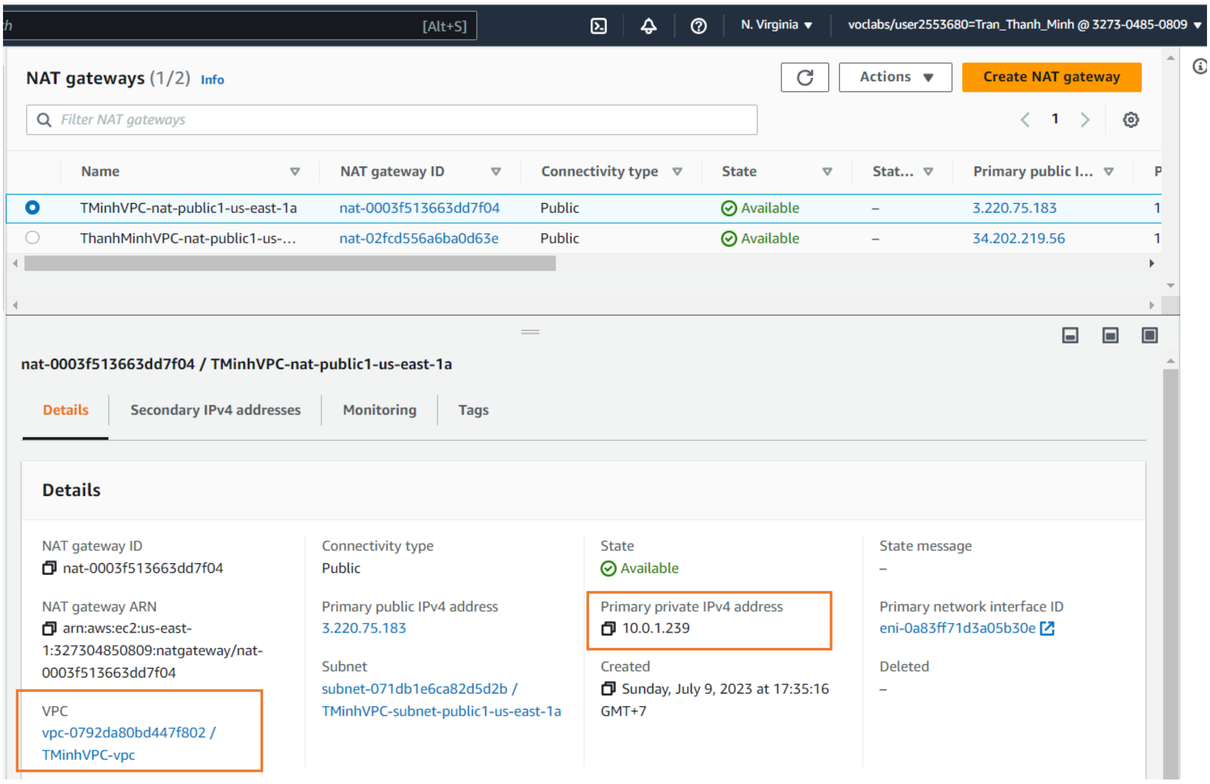
Subnet ID
subnet-071db1e6ca82d5d2b (TMinhVPC-subnet-public1-us-east-1a)

Auto Scaling Group name
–

IMDSv2

Configure NAT

- It is configured to be in private subnet 10.0.1.0/24 of TMinh-vpc (vpc-0792da80bd447f802)
- This will help all the **private instances can communicate** with the public internet whose private IP addresses will be translated by the NAT device.



NAT gateways (1/2) Info

	Name	NAT gateway ID	Connectivity type	State	Stat...	Primary public I...	P
●	TMinhVPC-nat-public1-us-east-1a	nat-0003f513663dd7f04	Public	✓ Available	–	3.220.75.183	1
○	ThanhMinhVPC-nat-public1-us-...	nat-02fcd556a6ba0d63e	Public	✓ Available	–	34.202.219.56	1

nat-0003f513663dd7f04 / TMinhVPC-nat-public1-us-east-1a

Details

NAT gateway ID
nat-0003f513663dd7f04

Connectivity type
Public

State
✓ Available

State message
–

NAT gateway ARN
arn:aws:ec2:us-east-1:327304850809:natgateway/nat-0003f513663dd7f04

Primary public IPv4 address
3.220.75.183

Primary private IPv4 address
10.0.1.239

Primary network interface ID
eni-0a83ff71d3a05b30e

VPC
vpc-0792da80bd447f802 / TMinhVPC-vpc

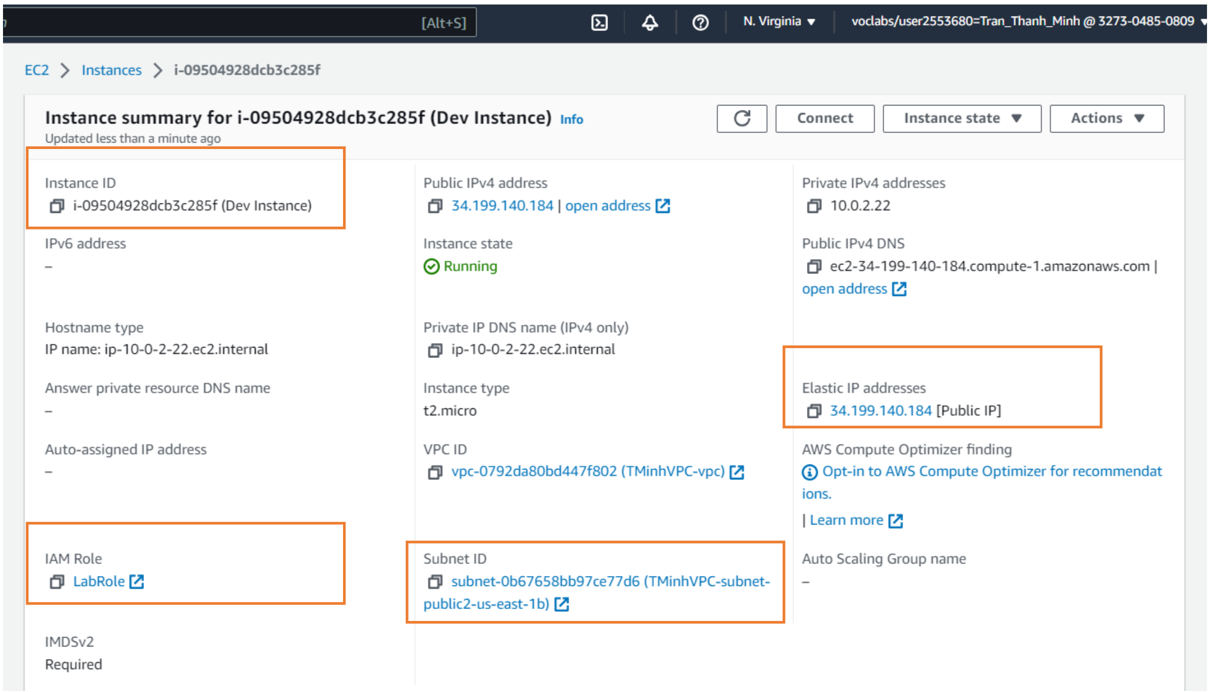
Subnet
subnet-071db1e6ca82d5d2b / TMinhVPC-subnet-public1-us-east-1a

Created
Sunday, July 9, 2023 at 17:35:16 GMT+7

Deleted
–

Configure Dev instance.

- Dev instance (i-09504928dcb3c285f) with private subnet **10.0.2.0/24** in TMinh-vpc (vpc-0792da80bd447f802)
- It is attached with the EIP (**34.199.140.184**) for having the **unchanged public IP address.**
- I also assigned it to the IAM **LabRole** which is already configured so that it can have the **permission** to access the resource.



[Alt+S]
N. Virginia ▼
voclabs/user2553680=Tran_Thanh_Minh @ 3273-0485-0809 ▼
EC2 > Instances > i-09504928dcb3c285f
Connect
Instance state ▼
Actions ▼

Instance summary for i-09504928dcb3c285f (Dev Instance) Info
Updated less than a minute ago

Instance ID
i-09504928dcb3c285f (Dev Instance)

Public IPv4 address
34.199.140.184 | open address

Private IPv4 addresses
10.0.2.22

IPv6 address
–

Instance state
✓ Running

Public IPv4 DNS
ec2-34-199-140-184.compute-1.amazonaws.com | open address

Hostname type
IP name: ip-10-0-2-22.ec2.internal

Private IP DNS name (IPv4 only)
ip-10-0-2-22.ec2.internal

Answer private resource DNS name
–

Instance type
t2.micro

Elastic IP addresses
34.199.140.184 [Public IP]

Auto-assigned IP address
–

VPC ID
vpc-0792da80bd447f802 (TMinhVPC-vpc)

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

IAM Role
LabRole

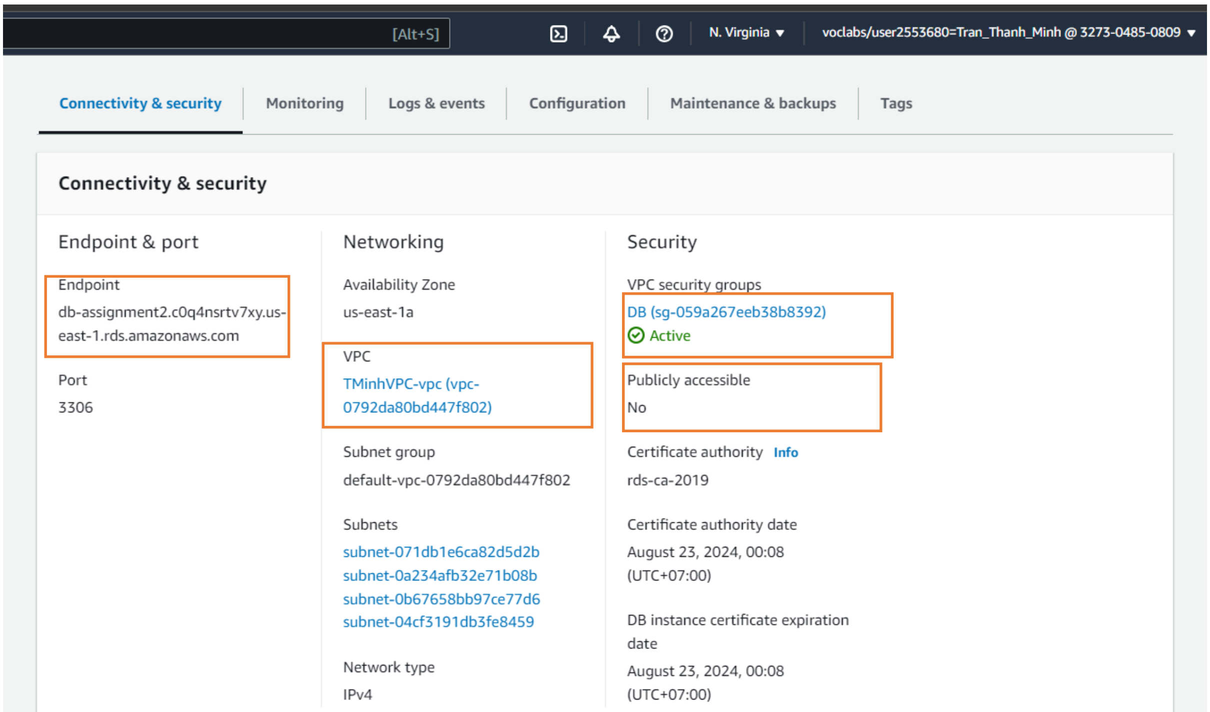
Subnet ID
subnet-0b67658bb97ce77d6 (TMinhVPC-subnet-public2-us-east-1b)

Auto Scaling Group name
–

IMDSv2
Required

RDS Information

- Attach it to the TMinh-vpc (vpc-0792da80bd447f802)
- Adjust it **publicly accessible** to No which only allows the connection from those who are in the same VPC.



Connectivity & security

Endpoint & port

Endpoint
db-assignment2.c0q4nsrtv7xy.us-east-1.rds.amazonaws.com

Port
3306

Networking

Availability Zone
us-east-1a

VPC
TMinhVPC-vpc (vpc-0792da80bd447f802)

Subnet group
default-vpc-0792da80bd447f802

Subnets
subnet-071db1e6ca82d5d2b
subnet-0a234afb32e71b08b
subnet-0b67658bb97ce77d6
subnet-04cf3191db3fe8459

Network type
IPv4

Security

VPC security groups
DB (sg-059a267eeb38b8392)
✓ Active

Publicly accessible
No

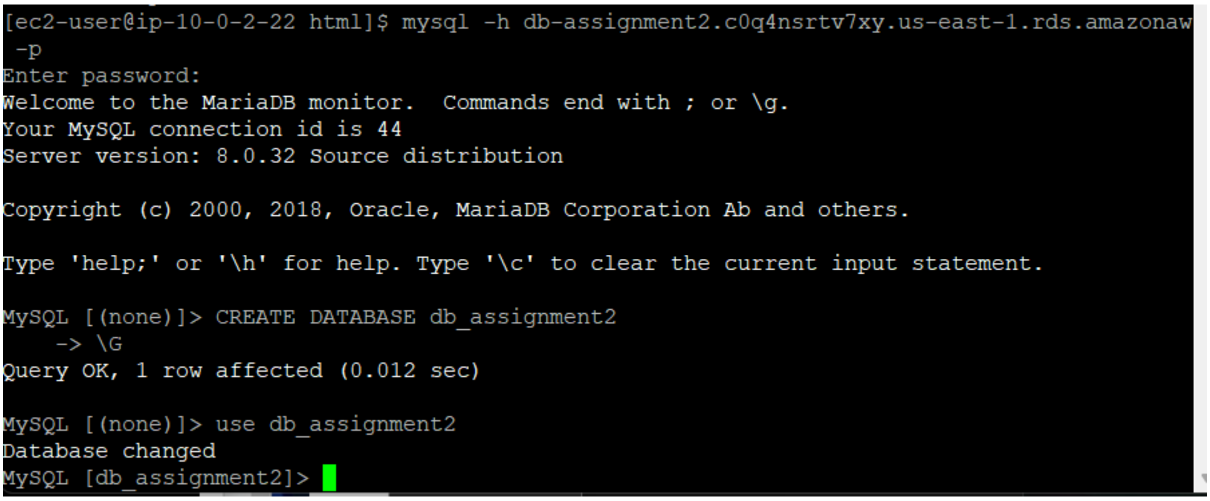
Certificate authority Info
rds-ca-2019

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

DB instance certificate expiration date
August 23, 2024, 00:08 (UTC+07:00)

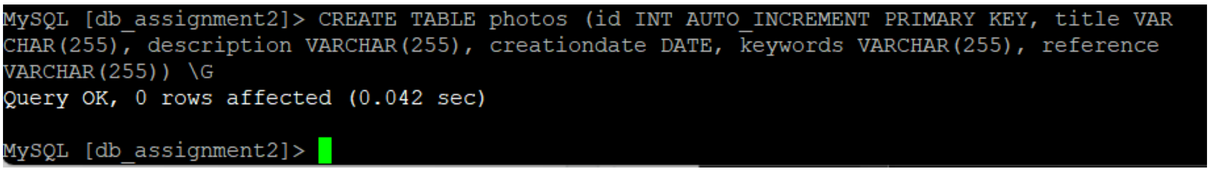
Configure database by using AWS CLI

- Connect to RDS end point (db-assignment2) through AWS CLI
- Create suitable database for current assignment.
- **Full command line** to connect to this RDS: mysql -h db-assignment2.c0q4nsrtv7xy.us-east-1.rds.amazonaws.com -u admin -p



```
[ec2-user@ip-10-0-2-22 html]$ mysql -h db-assignment2.c0q4nsrtv7xy.us-east-1.rds.amazonaw
 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 44
Server version: 8.0.32 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> CREATE DATABASE db_assignment2
    -> \G
Query OK, 1 row affected (0.012 sec)

MySQL [(none)]> use db_assignment2
Database changed
MySQL [db_assignment2]>
```

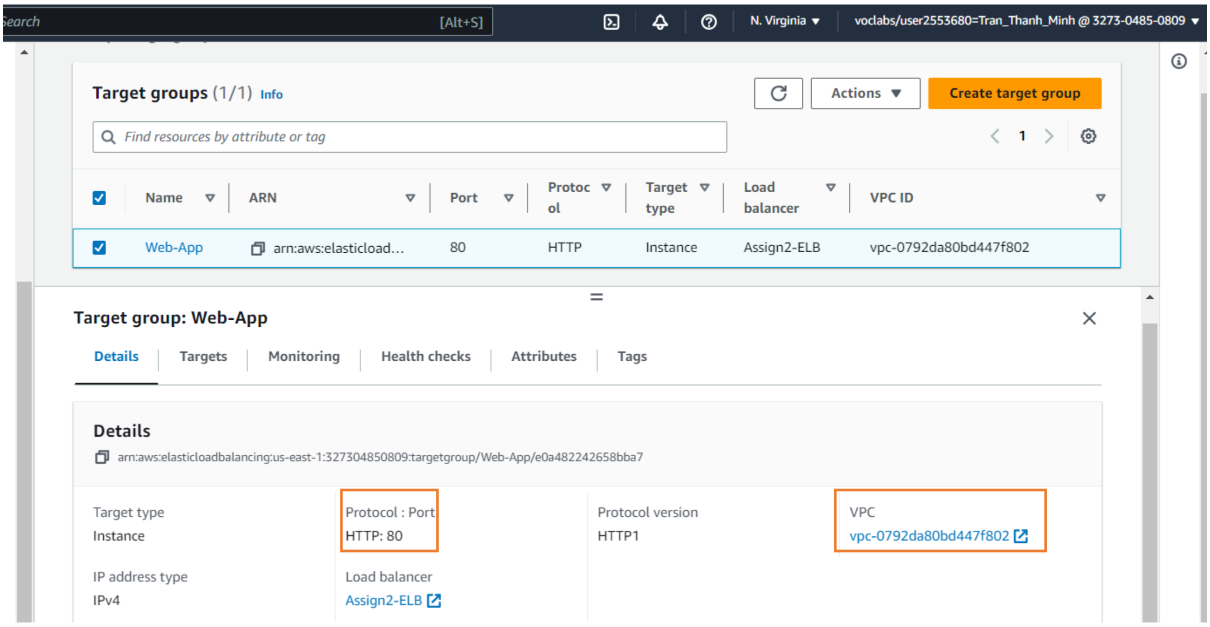
- Query to create table **photos** in the current database **db_assignment2**.



```
MySQL [db_assignment2]> CREATE TABLE photos (id INT AUTO_INCREMENT PRIMARY KEY, title VAR
CHAR(255), description VARCHAR(255), creationdate DATE, keywords VARCHAR(255), reference
VARCHAR(255)) \G
Query OK, 0 rows affected (0.042 sec)

MySQL [db_assignment2]> 
```

Configure target group.

- I have pointed the path of target group to HTTP **/photoalbum/album.php** for later con can check the **health check** for the instances in this target group.
- I also configure it to be in TMinh-vpc (vpc-0792da80bd447f802)



Target groups (1/1) Info

☑	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
☑	Web-App	arn:aws:elasticload...	80	HTTP	Instance	Assign2-ELB	vpc-0792da80bd447f802

Target group: Web-App

Details

arn:aws:elasticloadbalancing:us-east-1:327304850809:targetgroup/Web-App/e0a482242658bba7

Target type
Instance

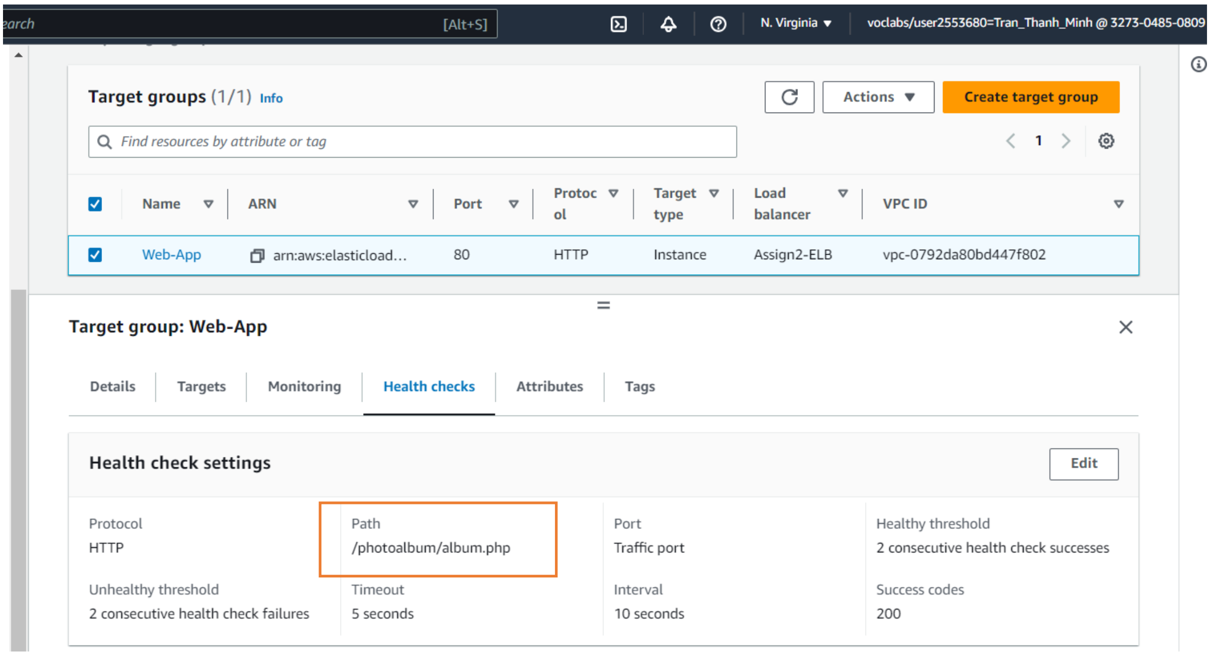
Protocol : Port
HTTP: 80

Protocol version
HTTP1

VPC
vpc-0792da80bd447f802

IP address type
IPv4

Load balancer
Assign2-ELB



Target groups (1/1) Info

☑	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
☑	Web-App	arn:aws:elasticload...	80	HTTP	Instance	Assign2-ELB	vpc-0792da80bd447f802

Target group: Web-App

Health check settings

Protocol
HTTP

Path
/photoalbum/album.php

Port
Traffic port

Healthy threshold
2 consecutive health check successes

Unhealthy threshold
2 consecutive health check failures

Timeout
5 seconds

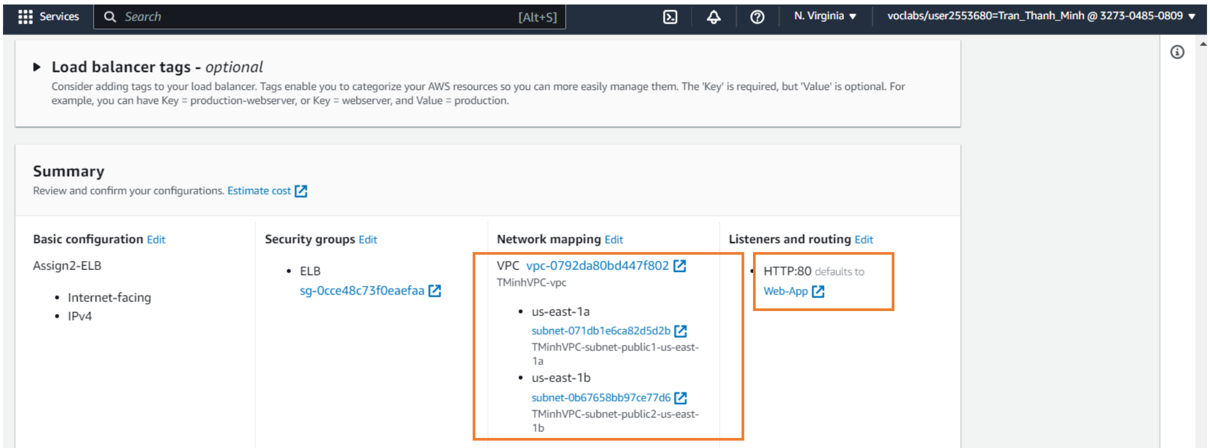
Interval
10 seconds

Success codes
200

Configure ELB

- It is attached to 2 **public subnets** of TMinh-vpc (vpc-0792da80bd447f802) to **receive the internet traffic.**

- It is also listened to **port HTTP:80** at the route **photoalbum/album.php** from the target group web app.



▸ **Load balancer tags** - *optional*

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

Summary

Review and confirm your configurations. Estimate cost

Basic configuration Edit

Assign2-ELB

- Internet-facing
- IPv4

Security groups Edit

- ELB
  sg-0cce48c73f0eaefaa

Network mapping Edit

VPC vpc-0792da80bd447f802
TMinhVPC-vpc

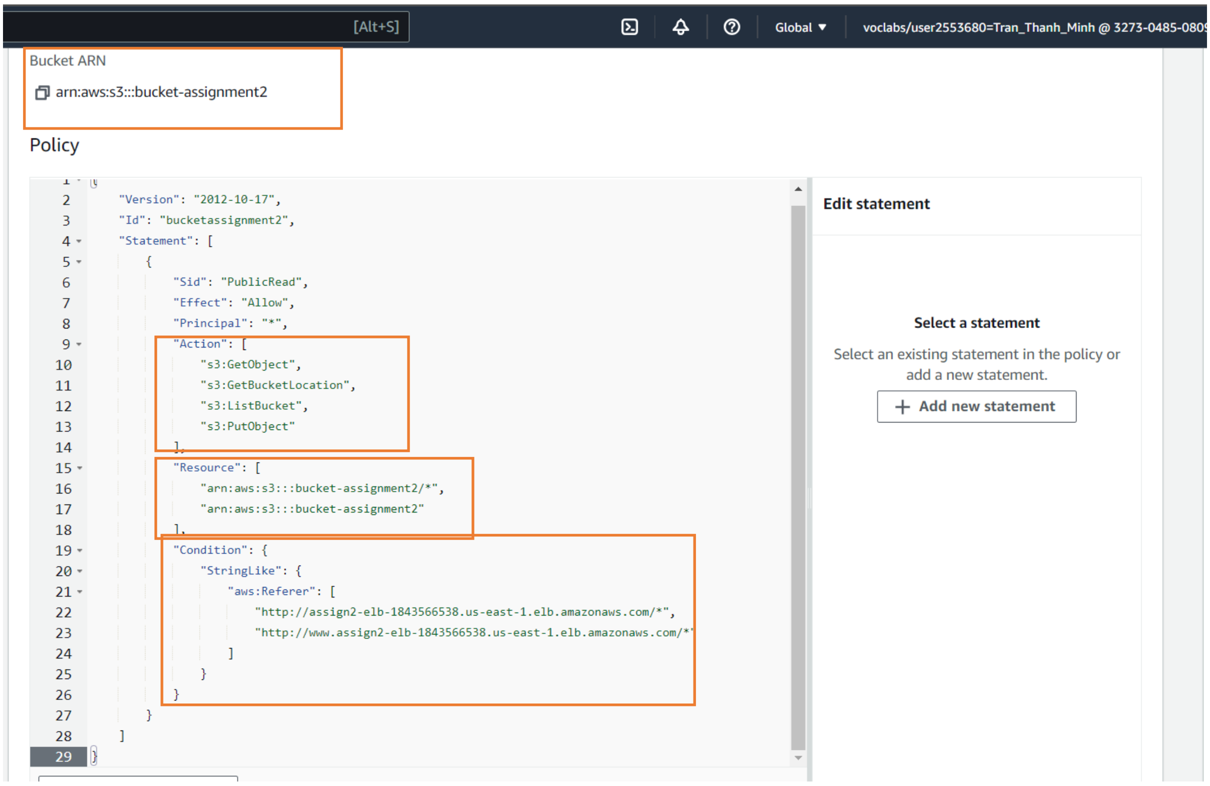
- us-east-1a
  subnet-071db1e6ca82d5d2b
  TMinhVPC-subnet-public1-us-east-1a
- us-east-1b
  subnet-0b67658bb97ce77d6
  TMinhVPC-subnet-public2-us-east-1b

Listeners and routing Edit

- HTTP:80 defaults to Web-App

S3 bucket

- With the same configuration for the policy for the old S3 bucket, this new one I just added the **Condition** part where it allows only the **ELB** to access, get, put, list object.
- I also added the **Action** where to provide the permission to **Put** the object **(s3:PutObject)**



Bucket ARN

arn:aws:s3:::bucket-assignment2

Policy

```
{
    "Version": "2012-10-17",
    "Id": "bucketassignment2",
    "Statement": [
        {
            "Sid": "PublicRead",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-assignment2/*",
                "arn:aws:s3:::bucket-assignment2"
            ],
            "Condition": {
                "StringLike": {
                    "aws:Referer": [
                        "http://assign2-elb-1843566538.us-east-1.elb.amazonaws.com/*",
                        "http://www.assign2-elb-1843566538.us-east-1.elb.amazonaws.com/*"
                    ]
                }
            }
        }
    ]
}
```

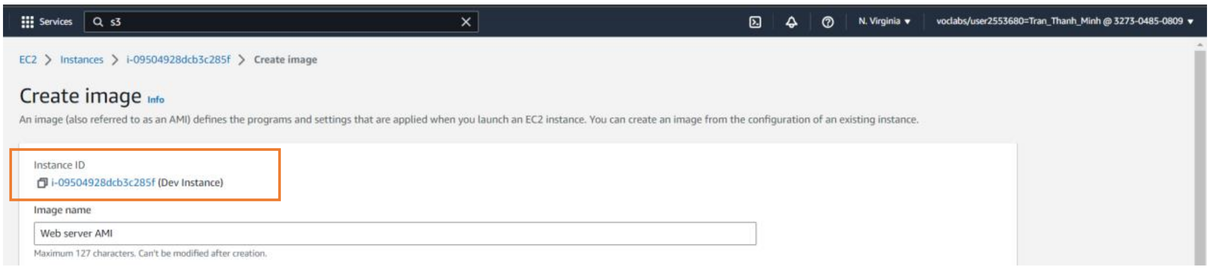
Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

Create AMI for web server.

- Create image from the Dev instance (i-09504928dcb3c285f) to save time and resources


Services
s3
N. Virginia
vodabs/user2553680=Tran_Thanh_Minh @ 3273-0485-0809
EC2 > Instances > i-09504928dcb3c285f > Create image

Create image Info

An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance.

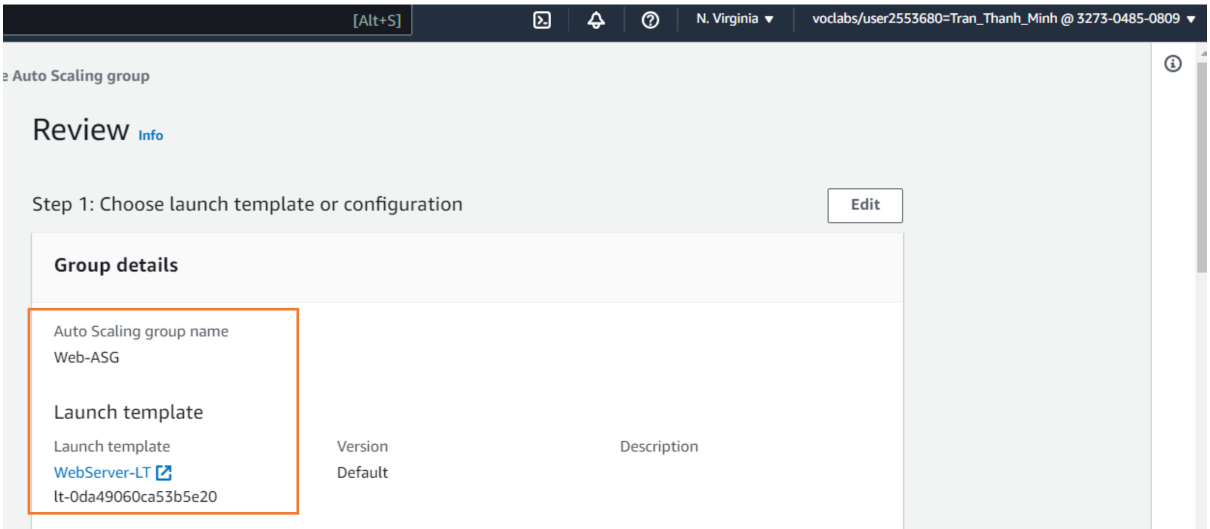
Instance ID
i-09504928dcb3c285f (Dev Instance)

Image name
Web server AMI

Maximum 127 characters. Can't be modified after creation.

Configuration Auto scaling group

- It is created from the launch template which I have already configured



Review Info

Step 1: Choose launch template or configuration

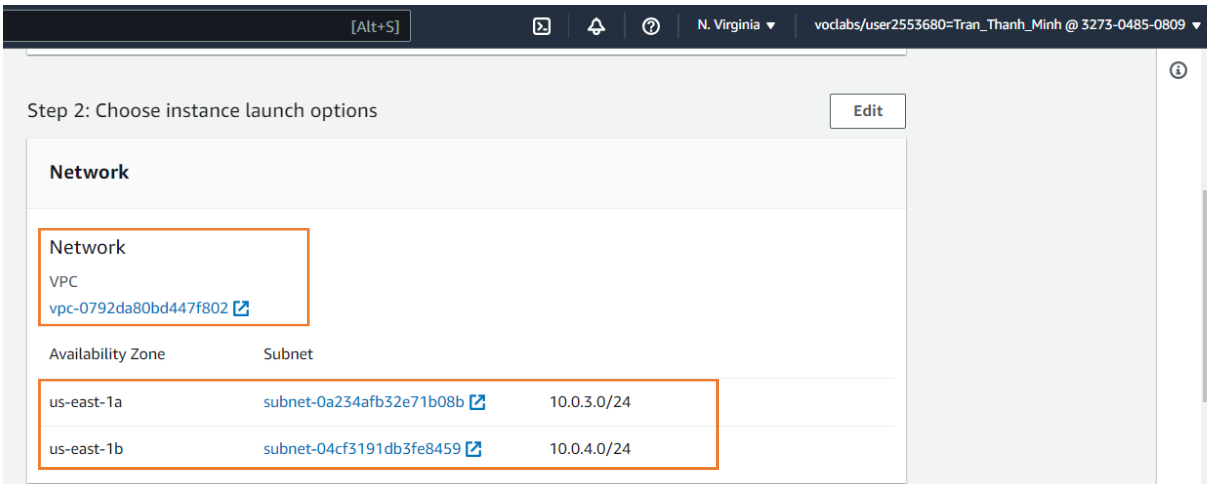
Group details

Auto Scaling group name
Web-ASG

Launch template

Launch template	Version	Description
WebServer-LT lt-0da49060ca53b5e20	Default	

- It will only create auto scaling instances in these 2 private subnets and in the TMinh-vpc (vpc-0792da80bd447f802)



Step 2: Choose instance launch options

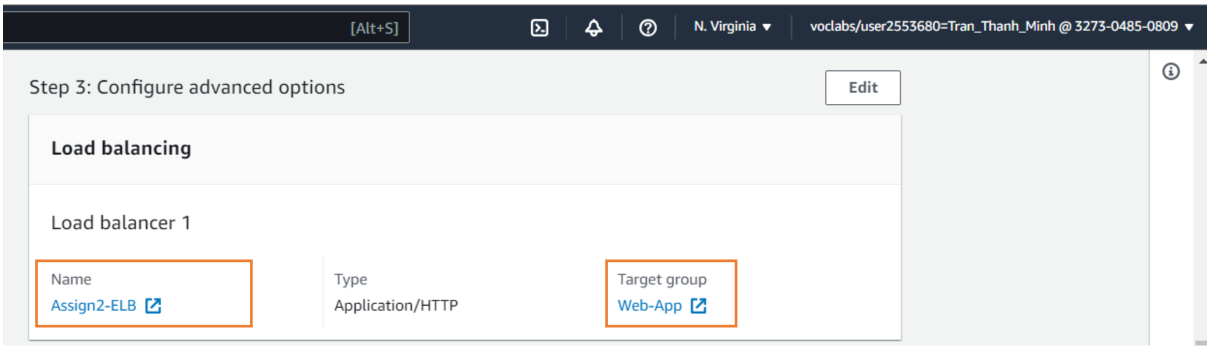
Network

Network

VPC
vpc-0792da80bd447f802

Availability Zone	Subnet	
us-east-1a	subnet-0a234afb32e71b08b	10.0.3.0/24
us-east-1b	subnet-04cf3191db3fe8459	10.0.4.0/24

- Attach it to the ELB which I have created above.



Step 3: Configure advanced options

Load balancing

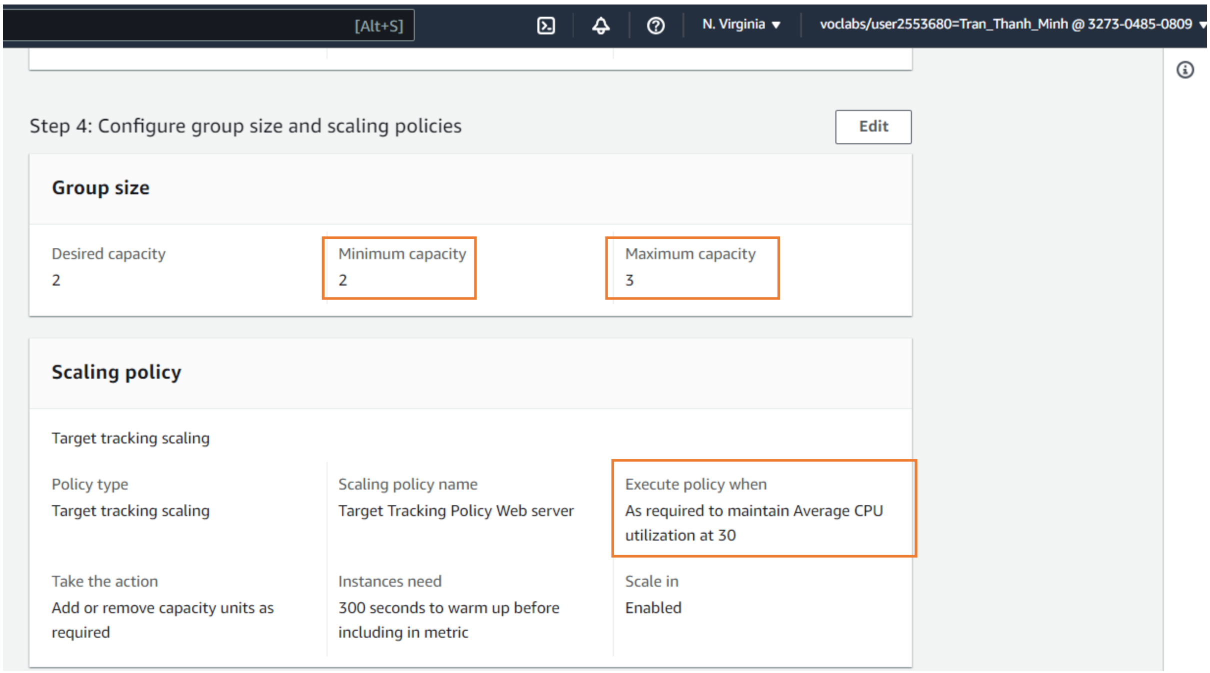
Load balancer 1

Name
Assign2-ELB

Type
Application/HTTP

Target group
Web-App

- The minimum of instance for this group size is 2 and the maximum is 3 so it can be scaled up and default is 2 running instances
- There is also a tracking policy where it will execute Average CPU utilization at 30%



Step 4: Configure group size and scaling policies

Group size

Desired capacity
2

Minimum capacity
2

Maximum capacity
3

Scaling policy

Target tracking scaling

Policy type
Target tracking scaling

Scaling policy name
Target Tracking Policy Web server

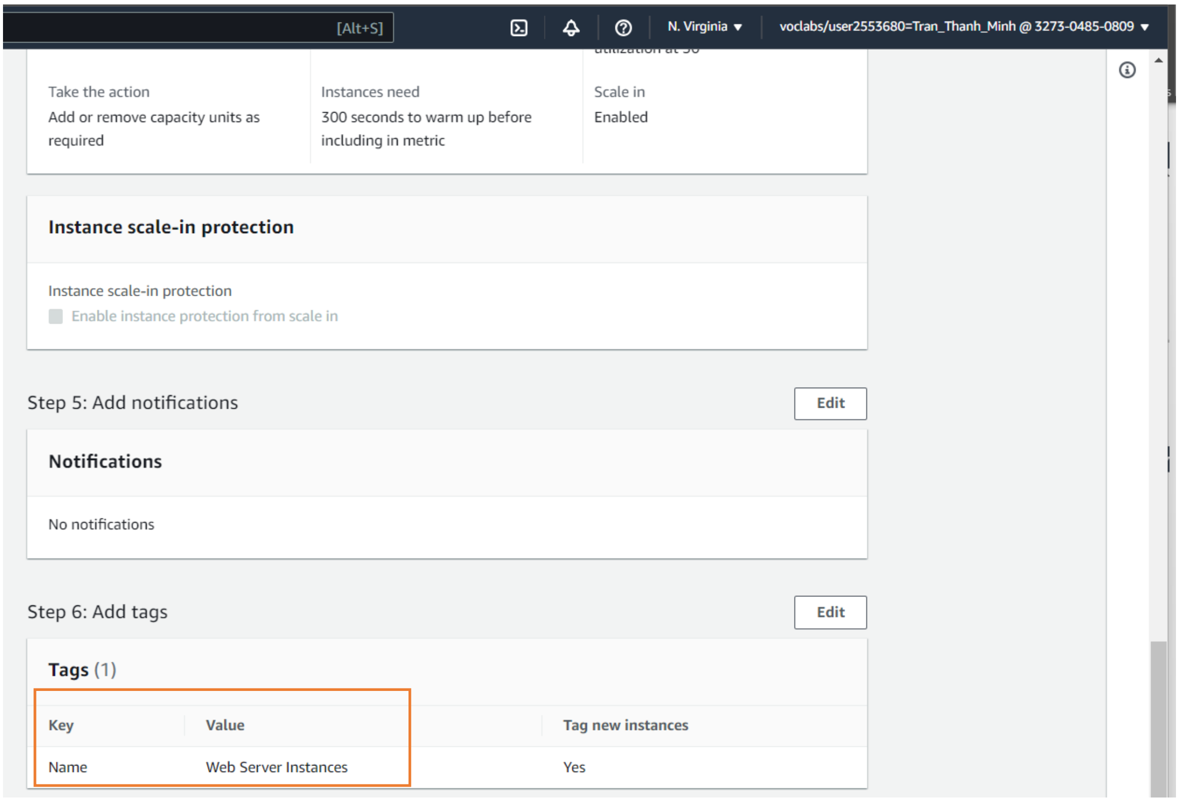
Execute policy when
As required to maintain Average CPU utilization at 30

Take the action
Add or remove capacity units as required

Instances need
300 seconds to warm up before including in metric

Scale in
Enabled

- Name of new instances in this auto scaling group are “Web Server Instances.”



Take the action
Add or remove capacity units as required

Instances need
300 seconds to warm up before including in metric

Scale in
Enabled

Instance scale-in protection

Instance scale-in protection
□ Enable instance protection from scale in

Step 5: Add notifications

Notifications

No notifications

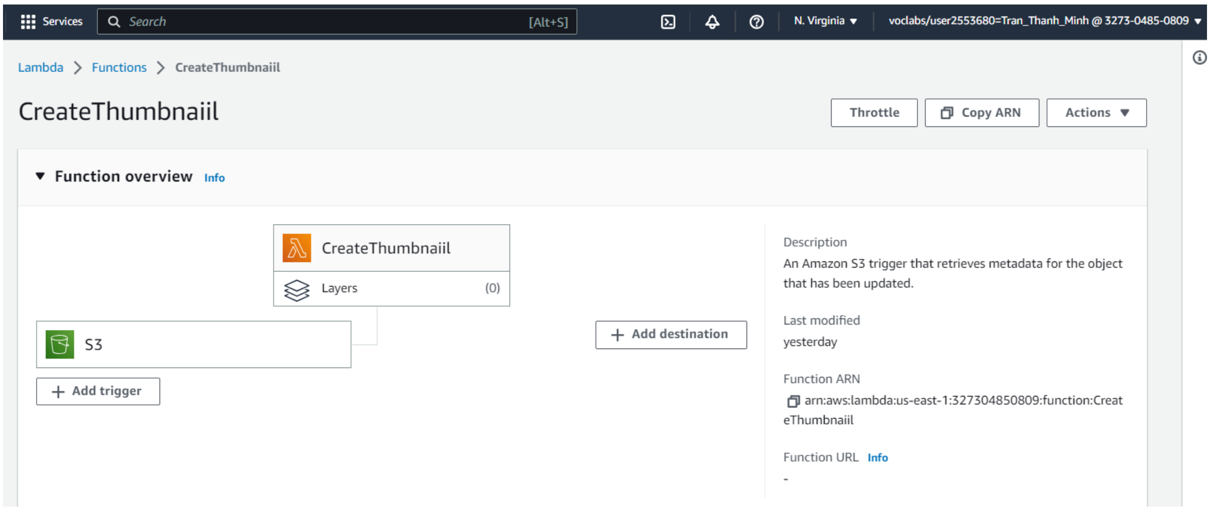
Step 6: Add tags

Tags (1)

Key	Value	Tag new instances
Name	Web Server Instances	Yes

Lambda function

- After creating Lambda function with the IAM role LabRole which allow the Lambda to access the resources in the S3 and can modify it.
- I also have uploaded the zip file of this assignment to this lambda.



CreateThumbnaiil

▾ **Function overview**

CreateThumbnaiil

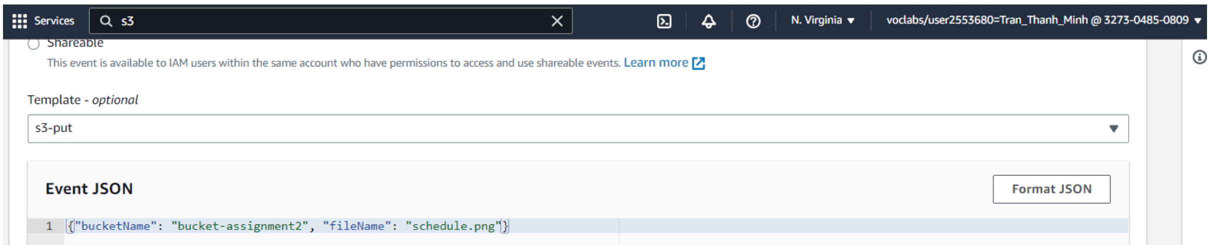
Description
An Amazon S3 trigger that retrieves metadata for the object that has been updated.

Last modified
yesterday

Function ARN
arn:aws:lambda:us-east-1:327304850809:function:CreateThumbnaiil

Function URL
-

- I have generated the test case for this function for the image schedule.png in the S3 bucket.



○ Shareable

This event is available to IAM users within the same account who have permissions to access and use shareable events. Learn more

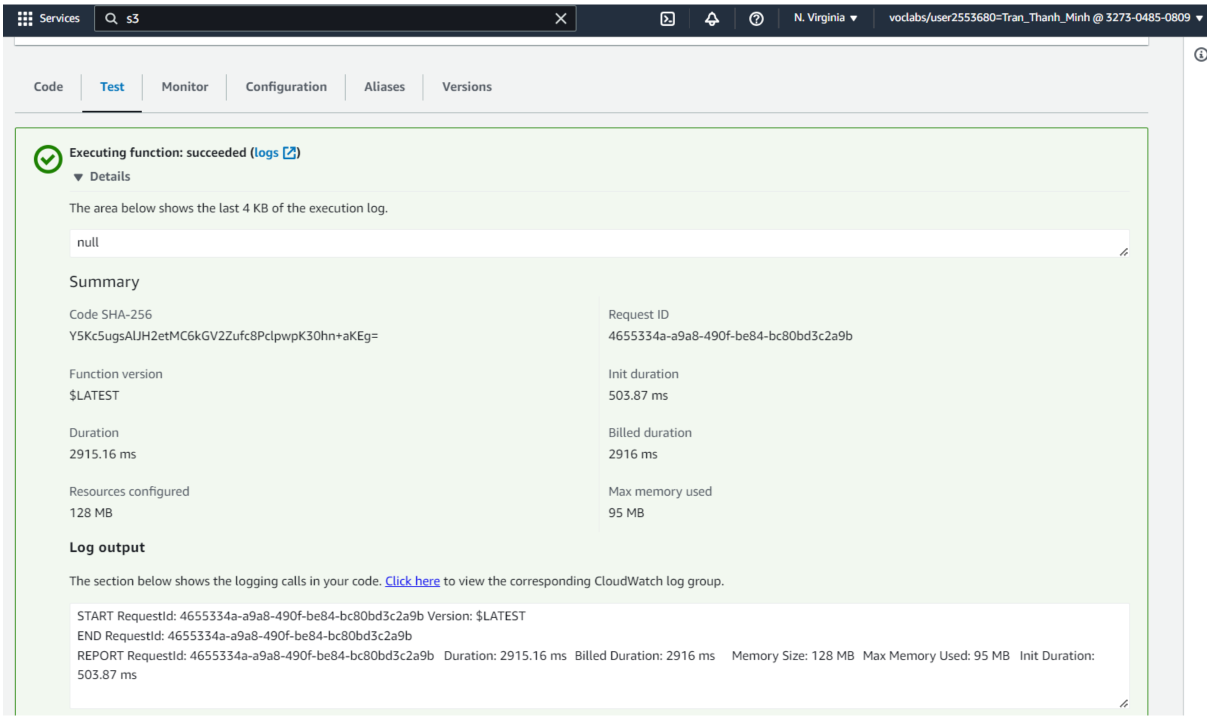
Template - *optional*

s3-put

Event JSON

```
{"bucketName": "bucket-assignment2", "fileName": "schedule.png"}
```

- The result is succeeded



Executing function: succeeded (logs)

▼ Details

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

```
null
```

Summary

Code SHA-256
Y5Kc5ugsAlJH2etMC6kGV2Zufc8PclpwpK30hn+aKEg=

Request ID
4655334a-a9a8-490f-be84-bc80bd3c2a9b

Function version
$LATEST

Init duration
503.87 ms

Duration
2915.16 ms

Billed duration
2916 ms

Resources configured
128 MB

Max memory used
95 MB

Log output

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

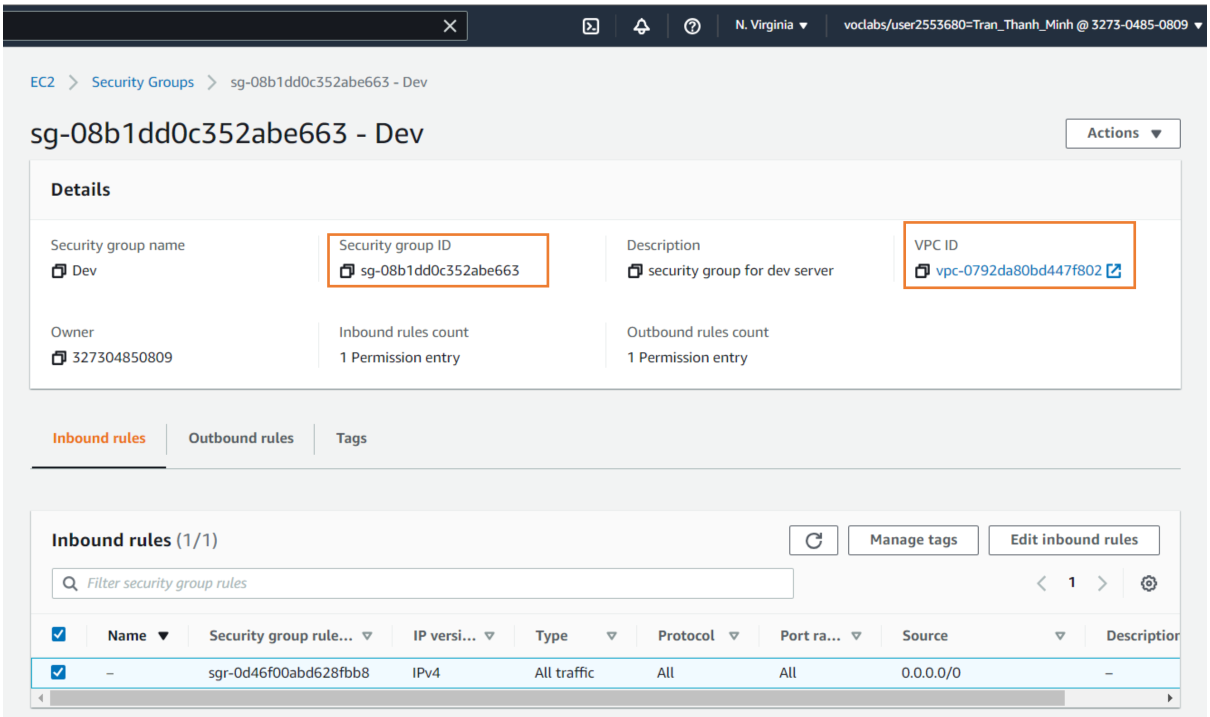
```
START RequestId: 4655334a-a9a8-490f-be84-bc80bd3c2a9b Version: $LATEST
END RequestId: 4655334a-a9a8-490f-be84-bc80bd3c2a9b
REPORT RequestId: 4655334a-a9a8-490f-be84-bc80bd3c2a9b  Duration: 2915.16 ms  Billed Duration: 2916 ms   Memory Size: 128 MB  Max Memory Used: 95 MB  Init Duration: 503.87 ms
```

Security groups

1. Security group for Dev instance

I have allowed all traffic for the security group of Dev instance for both inbound and outbound.

The Dev security group (**sg-08b1dd0c352abe663**) is in TMinh-vpc (**vpc-0792da80bd447f802**)



EC2 > Security Groups > sg-08b1dd0c352abe663 - Dev

sg-08b1dd0c352abe663 - Dev

Details

Security group name Dev	Security group ID sg-08b1dd0c352abe663	Description security group for dev server	VPC ID vpc-0792da80bd447f802
Owner 327304850809	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

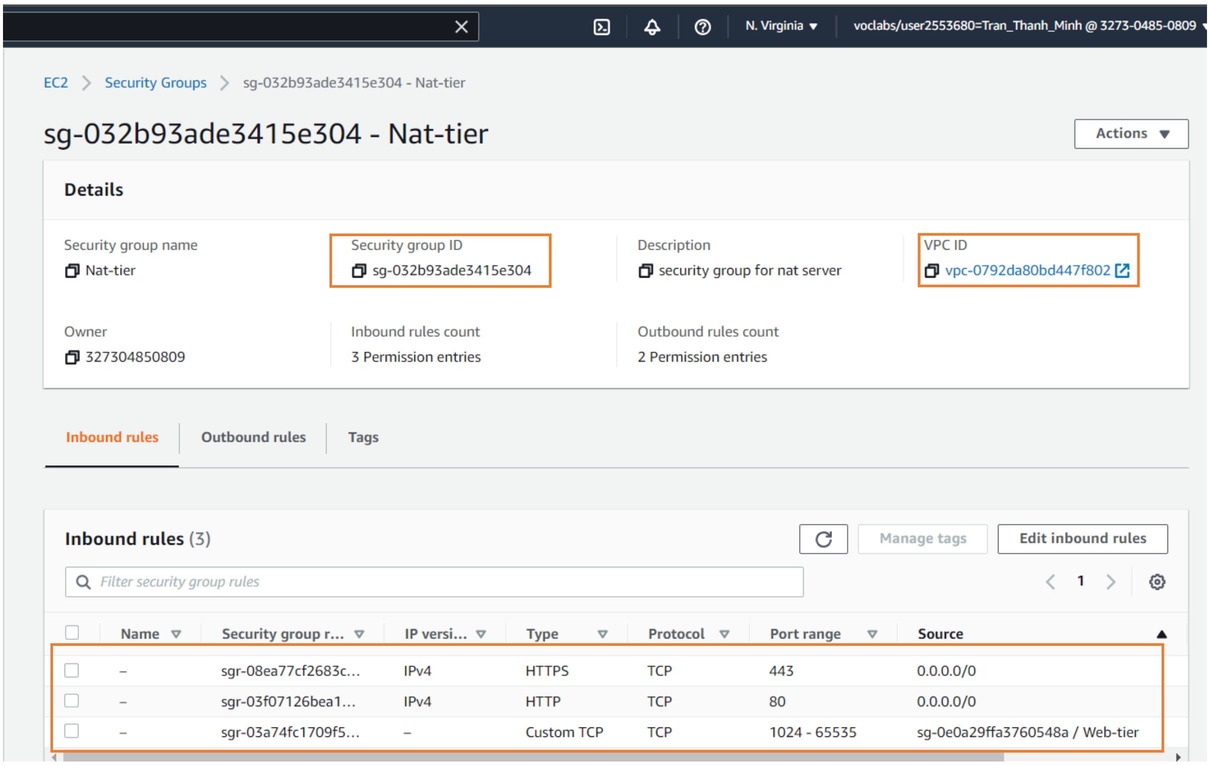
Inbound rules (1/1)

☑	Name	Security group rule...	IP versi...	Type	Protocol	Port ra...	Source	Descriptior
☑	–	sgr-0d46f00abd628fbb8	IPv4	All traffic	All	All	0.0.0.0/0	–

2. Security group for NAT instance

The Nat-tier security group (**sg-032b93ade3415e304**) is in TMinh-vpc (**vpc-0792da80bd447f802**)

It is allow the traffic from HTTPS/HTTP for web application and traffic from the web servers instance



EC2 > Security Groups > sg-032b93ade3415e304 - Nat-tier

sg-032b93ade3415e304 - Nat-tier

Details

Security group name Nat-tier	Security group ID sg-032b93ade3415e304	Description security group for nat server	VPC ID vpc-0792da80bd447f802
Owner 327304850809	Inbound rules count 3 Permission entries	Outbound rules count 2 Permission entries	

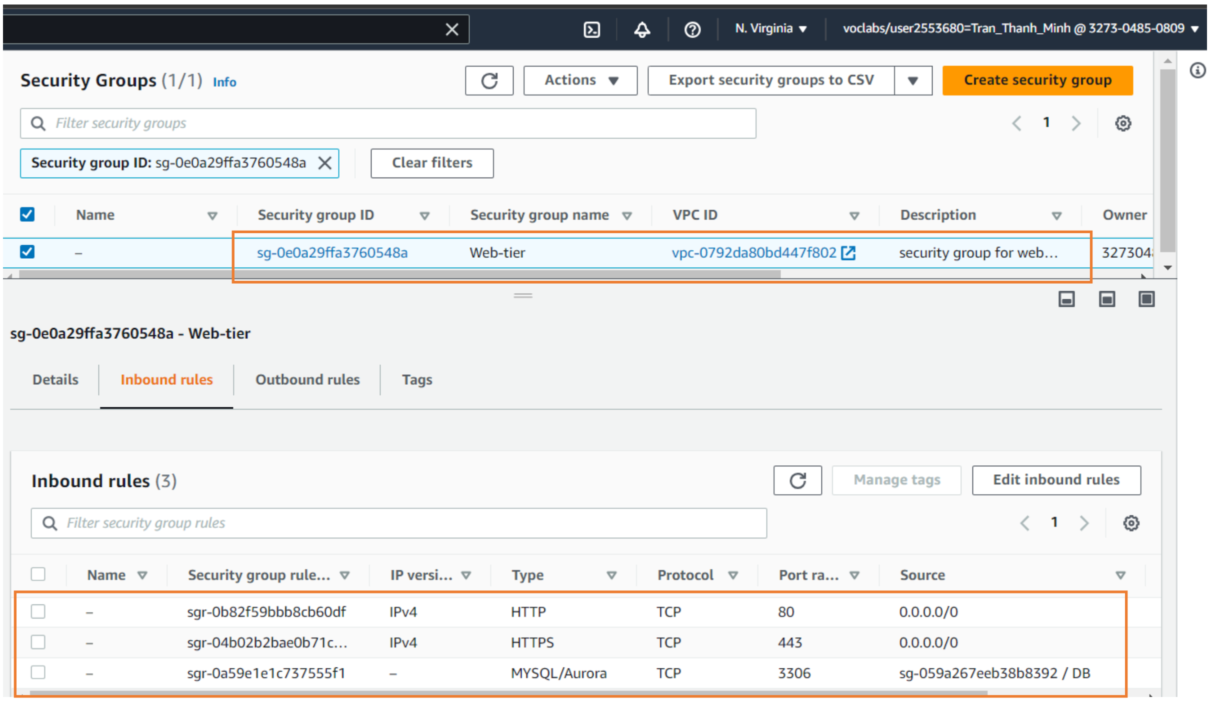
Inbound rules (3)

□	Name	Security group r...	IP versi...	Type	Protocol	Port range	Source
□	–	sgr-08ea77cf2683c...	IPv4	HTTPS	TCP	443	0.0.0.0/0
□	–	sgr-03f07126bea1...	IPv4	HTTP	TCP	80	0.0.0.0/0
□	–	sgr-03a74fc1709f5...	–	Custom TCP	TCP	1024 - 65535	sg-0e0a29ffa3760548a / Web-tier

3. Security group for Web servers

The Web-tier security group (**sg-0e0a29ffa3760548a**) is in TMinh-vpc (**vpc-0792da80bd447f802**)

It allows the traffic from the web application and the DB security group (sg-059a267eeb38b8392)



Security Groups (1/1) Info

Security group ID: sg-0e0a29ffa3760548a

	Name	Security group ID	Security group name	VPC ID	Description	Owner
☑	–	sg-0e0a29ffa3760548a	Web-tier	vpc-0792da80bd447f802	security group for web…	327304

sg-0e0a29ffa3760548a - Web-tier

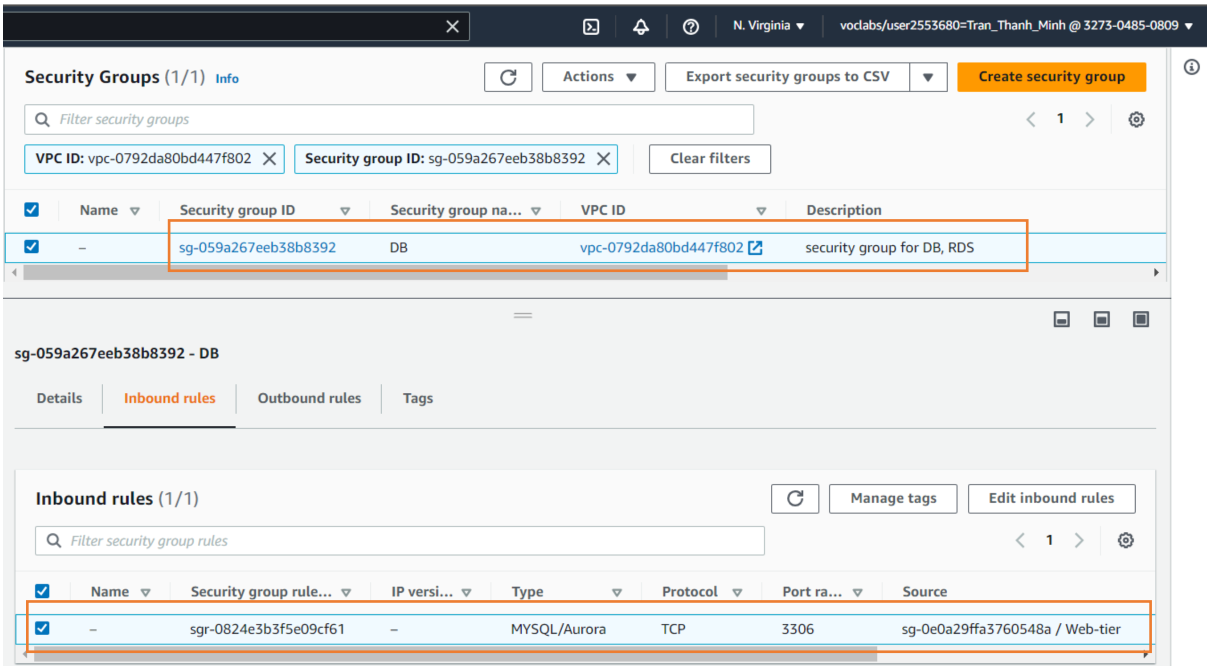
Inbound rules (3)

	Name	Security group rule…	IP versi…	Type	Protocol	Port ra…	Source
□	–	sgr-0b82f59bbb8cb60df	IPv4	HTTP	TCP	80	0.0.0.0/0
□	–	sgr-04b02b2bae0b71c…	IPv4	HTTPS	TCP	443	0.0.0.0/0
□	–	sgr-0a59e1e1c737555f1	–	MYSQL/Aurora	TCP	3306	sg-059a267eeb38b8392 / DB

4. Security group for RDS instance

The DB security group (**sg-059a267eeb38b8392**) is in TMinh-vpc (**vpc-0792da80bd447f802**)

It allow the traffic from the port 3306from the web-tier security group (**sg-0e0a29ffa3760548a**)



Security Groups (1/1) Info

VPC ID: vpc-0792da80bd447f802 | Security group ID: sg-059a267eeb38b8392

	Name	Security group ID	Security group na…	VPC ID	Description
☑	–	sg-059a267eeb38b8392	DB	vpc-0792da80bd447f802	security group for DB, RDS

sg-059a267eeb38b8392 - DB

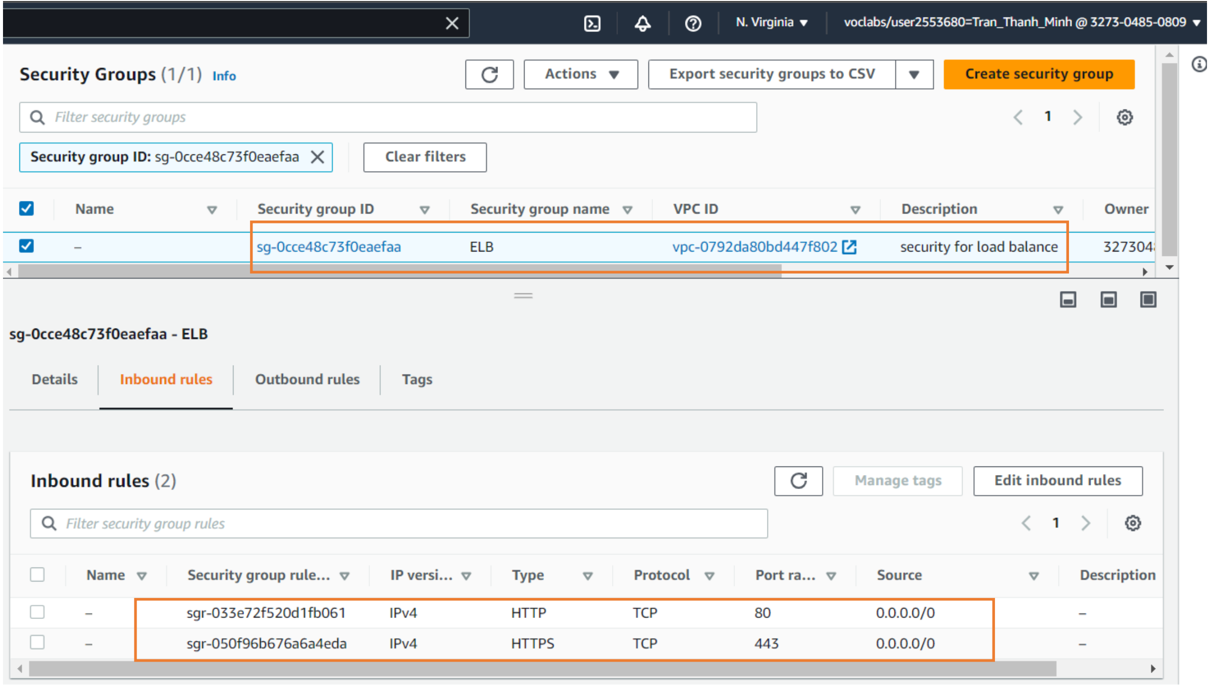
Inbound rules (1/1)

	Name	Security group rule…	IP versi…	Type	Protocol	Port ra…	Source
☑	–	sgr-0824e3b3f5e09cf61	–	MYSQL/Aurora	TCP	3306	sg-0e0a29ffa3760548a / Web-tier

5. Security group for Application Load balancer

The ELB security group (**sg-0cce48c73f0eaefaa**) is in TMinh-vpc (**vpc-0792da80bd447f802**)

It allow the traffic for web applications from port 80 and 443


N. Virginia
voclabs/user2553680=Tran_Thanh_Minh @ 3273-0485-0809
Security Groups (1/1) Info
Actions
Export security groups to CSV
Create security group
Filter security groups
Security group ID: sg-0cce48c73f0eaefaa
Clear filters
sg-0cce48c73f0eaefaa - ELB
Details
Inbound rules
Outbound rules
Tags
Inbound rules (2)
Manage tags
Edit inbound rules
Filter security group rules

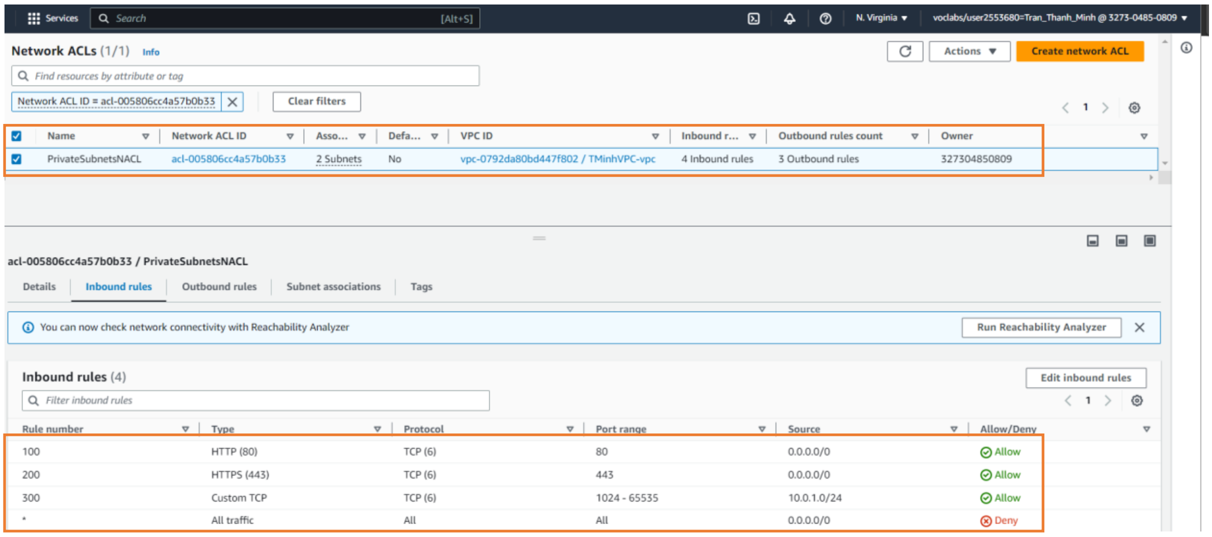
☑	Name	Security group ID	Security group name	VPC ID	Description	Owner
☑	–	sg-0cce48c73f0eaefaa	ELB	vpc-0792da80bd447f802	security for load balance	327304

□	Name	Security group rule...	IP versi...	Type	Protocol	Port ra...	Source	Description
□	–	sgr-033e72f520d1fb061	IPv4	HTTP	TCP	80	0.0.0.0/0	–
□	–	sgr-050f96b676a6a4eda	IPv4	HTTPS	TCP	443	0.0.0.0/0	–

NACL

The NACL (**acl-005806cc4a57b0b33**) is in TMinh-vpc (**vpc-0792da80bd447f802**)

It allows the traffic for the web application and other TCP server go through port 1024-65535 from the NAT instance.

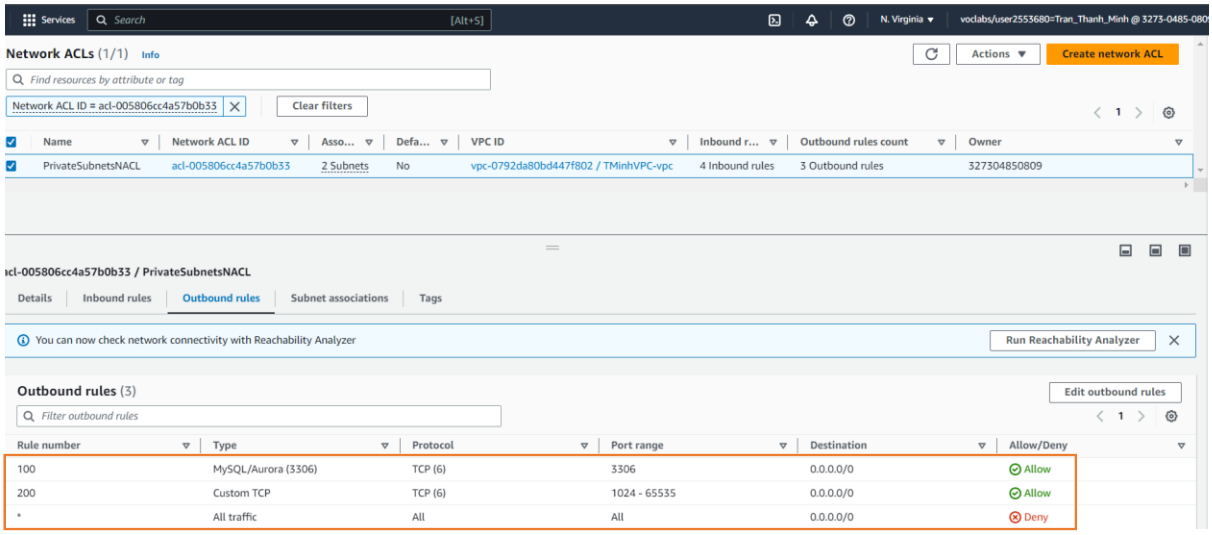


☑	Name	Network ACL ID	Asso...	Defa...	VPC ID	Inbound r...	Outbound rules count	Owner
☑	PrivateSubnetsNACL	acl-005806cc4a57b0b33	2 Subnets	No	vpc-0792da80bd447f802 / TMinhVPC-vpc	4 Inbound rules	3 Outbound rules	327304850809

You can now check network connectivity with Reachability Analyzer

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	Allow
300	Custom TCP	TCP (6)	1024 - 65535	10.0.1.0/24	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

- It allows the traffic of RDS can go out and other services from port 1024-65535



Network ACLs (1/1) Info

Network ACL ID = acl-005806cc4a57b0b33

☑	Name	Network ACL ID	Asso...	Defa...	VPC ID	Inbound r...	Outbound rules count	Owner
☑	PrivateSubnetsNACL	acl-005806cc4a57b0b33	2 Subnets	No	vpc-0792da80bd447f802 / TMinhVPC-vpc	4 Inbound rules	3 Outbound rules	327304850809

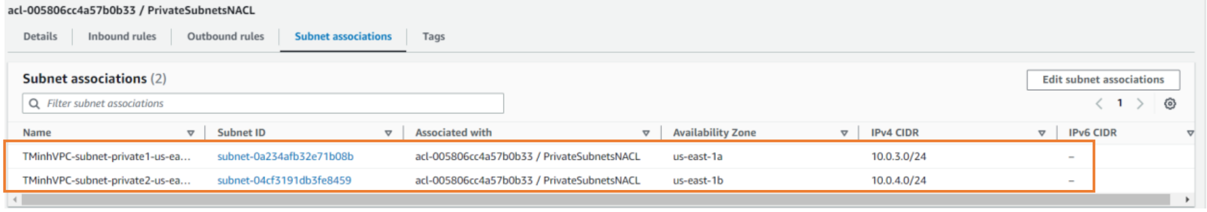
acl-005806cc4a57b0b33 / PrivateSubnetsNACL

You can now check network connectivity with Reachability Analyzer

Outbound rules (3)

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	MySQL/Aurora (3306)	TCP (6)	3306	0.0.0.0/0	✓ Allow
200	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

- 2 private subnets associated with it 10.0.3.0/24 and 10.0.4.0/24.

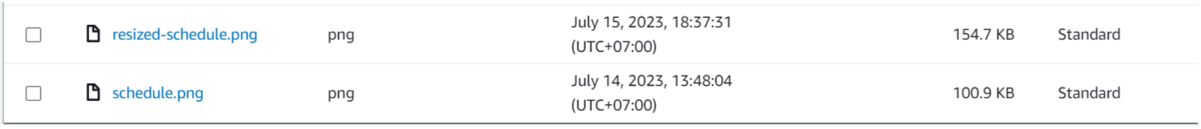

acl-005806cc4a57b0b33 / PrivateSubnetsNACL

Subnet associations (2)

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
TMinhVPC-subnet-private1-us-ea...	subnet-0a234afb32e71b08b	acl-005806cc4a57b0b33 / PrivateSubnetsNACL	us-east-1a	10.0.3.0/24	–
TMinhVPC-subnet-private2-us-ea...	subnet-04cf3191db3fe8459	acl-005806cc4a57b0b33 / PrivateSubnetsNACL	us-east-1b	10.0.4.0/24	–

Some Testing case

- Example of my schedule image was uploaded: https://bucket-assignment2.s3.amazonaws.com/schedule.png which can only be seen at album.php
- The evidence of the resized image by lambda function:



□	resized-schedule.png	png	July 15, 2023, 18:37:31 (UTC+07:00)	154.7 KB	Standard
□	schedule.png	png	July 14, 2023, 13:48:04 (UTC+07:00)	100.9 KB	Standard

- The website it accessible from the LEB: photouploader.php