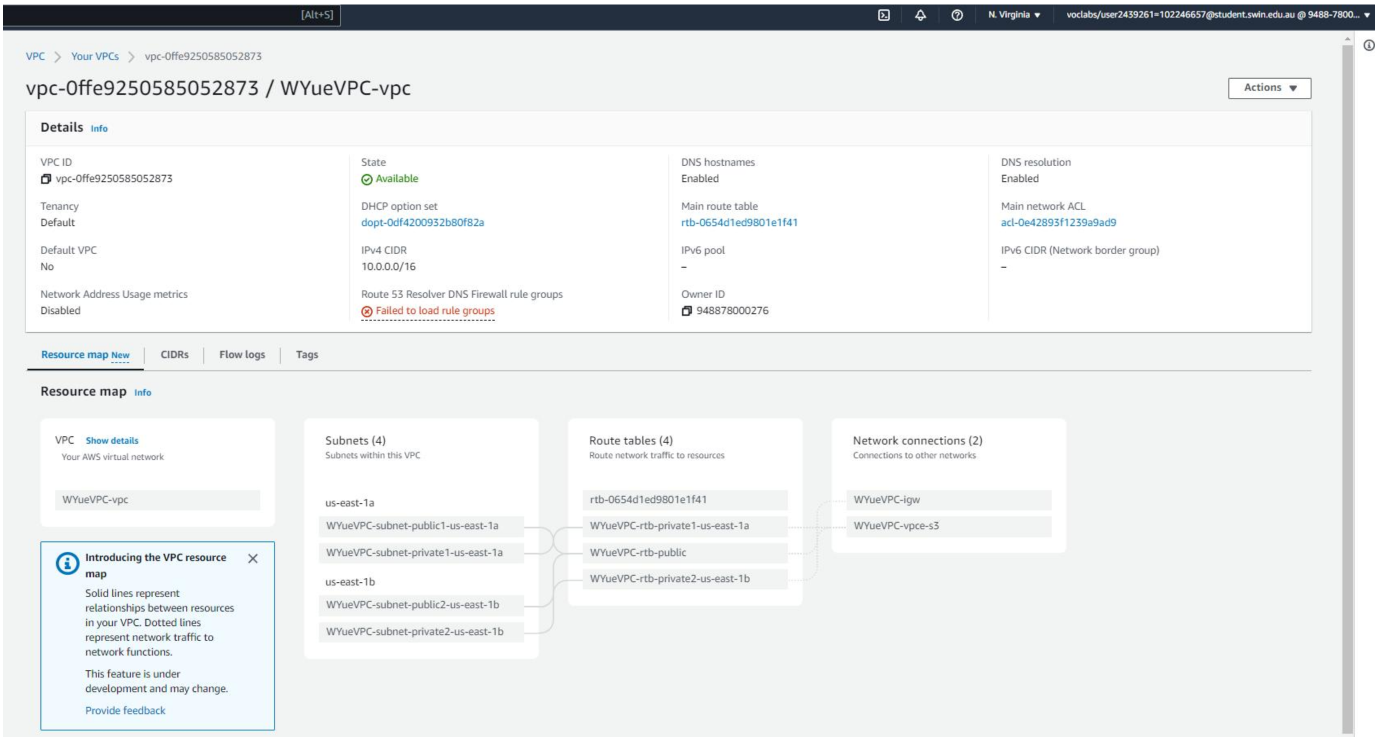
COS80001 Assignment 1b Report

Weihao Yue

Faculty of Science
Swinburne University of Technology
102246657@student.swin.edu.au

I. Create a VPC

VPC is Virtual Private Cloud which is an independent virtual network for running an instance. There are 2 private subnets in the VPC that cannot connect to the Internet directly, and 2 public subnets to help those private subnets to communicate with the Internet.



[Alt+S]
N. Virginia ▾
voclabs/user2439261=102246657@student.swin.edu.au @ 9488-7800... ▾
VPC > Your VPCs > vpc-0ffe9250585052873
Actions ▾
Info
Resource map New | CIDRs | Flow logs | Tags
Show details
Provide feedback

vpc-0ffe9250585052873 / WYueVPC-vpc

Details

VPC ID: vpc-0ffe9250585052873
State: Available
DNS hostnames: Enabled
DNS resolution: Enabled
Tenancy: Default
DHCP option set: dopt-0df4200932b80f82a
Main route table: rtb-0654d1ed9801e1f41
Main network ACL: acl-0e42893f1239a9ad9
Default VPC: No
IPv4 CIDR: 10.0.0.0/16
IPv6 pool: –
IPv6 CIDR (Network border group): –
Network Address Usage metrics: Disabled
Route 53 Resolver DNS Firewall rule groups: Failed to load rule groups
Owner ID: 948878000276

Resource map

VPC – Your AWS virtual network: WYueVPC-vpc

Subnets (4) – Subnets within this VPC
us-east-1a: WYueVPC-subnet-public1-us-east-1a, WYueVPC-subnet-private1-us-east-1a
us-east-1b: WYueVPC-subnet-public2-us-east-1b, WYueVPC-subnet-private2-us-east-1b

Route tables (4) – Route network traffic to resources
rtb-0654d1ed9801e1f41, WYueVPC-rtb-private1-us-east-1a, WYueVPC-rtb-public, WYueVPC-rtb-private2-us-east-1b

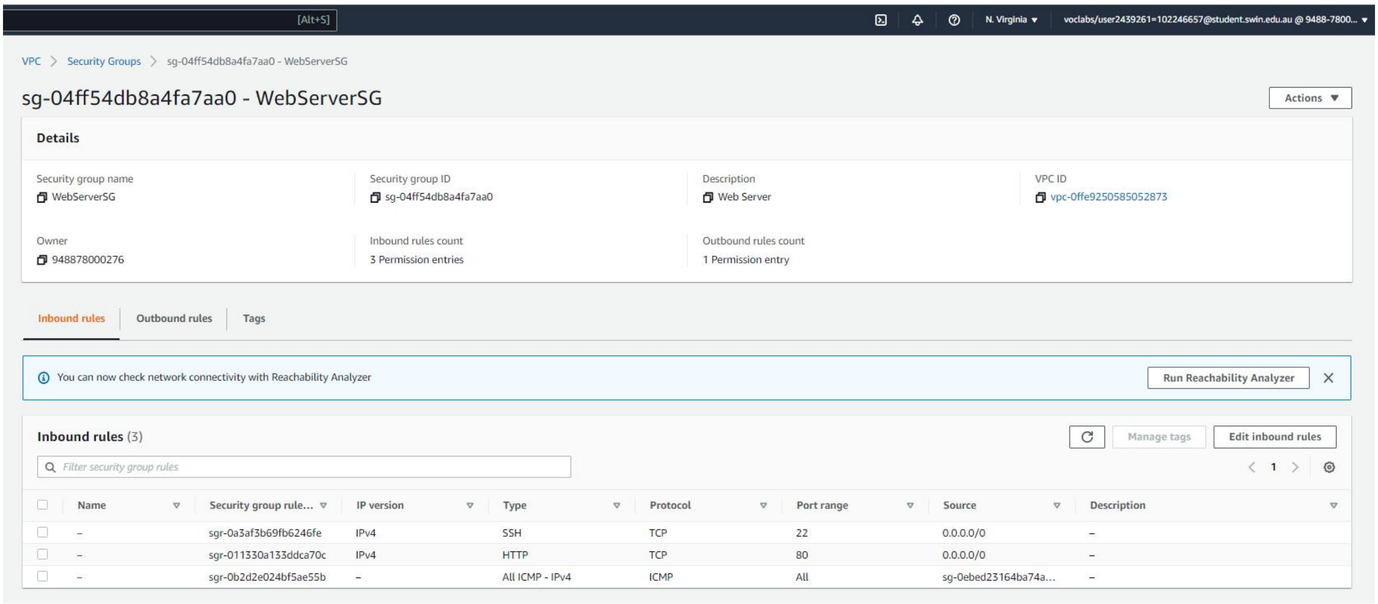
Network connections (2) – Connections to other networks
WYueVPC-igw, WYueVPC-vpce-s3

Introducing the VPC resource map
Solid lines represent relationships between resources in your VPC. Dotted lines represent network traffic to network functions.
This feature is under development and may change.

Fig. 1 Overview of VPC

II. Create VPC Security Groups

A VPC security group is sort of firewall that controls inbound and outbound traffic. In this step, create particular inbound rules to meet the requirement of the assignment.


[Alt+S]
N. Virginia
voclabs/user2439261=102246657@student.swin.edu.au @ 9488-7800...
VPC > Security Groups > sg-04ff54db8a4fa7aa0 - WebServerSG
Actions
Inbound rules
Outbound rules
Tags
Run Reachability Analyzer
Manage tags
Edit inbound rules
Filter security group rules
1

sg-04ff54db8a4fa7aa0 - WebServerSG

Details

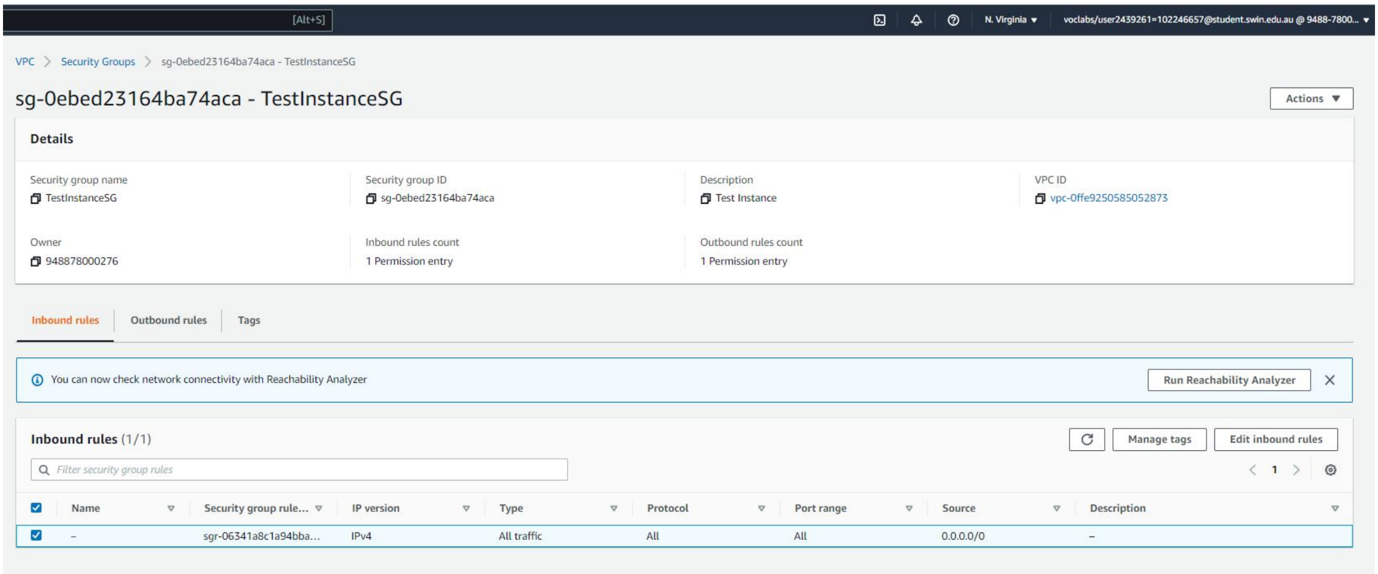
Security group name	Security group ID	Description	VPC ID
WebServerSG	sg-04ff54db8a4fa7aa0	Web Server	vpc-0ffe9250585052873
Owner	**Inbound rules count**	**Outbound rules count**	
948878000276	3 Permission entries	1 Permission entry	

You can now check network connectivity with Reachability Analyzer

Inbound rules (3)

□	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
□	–	sgr-0a3af3b69fb6246fe	IPv4	SSH	TCP	22	0.0.0.0/0	–
□	–	sgr-011330a133ddca70c	IPv4	HTTP	TCP	80	0.0.0.0/0	–
□	–	sgr-0b2d2e024bf5ae55b	–	All ICMP - IPv4	ICMP	All	sg-0ebed23164ba74a...	–

Fig. 2 VPC Security Group 1.


[Alt+S]
N. Virginia
voclabs/user2439261=102246657@student.swin.edu.au @ 9488-7800...
VPC > Security Groups > sg-0ebed23164ba74aca - TestInstanceSG
Actions
Inbound rules
Outbound rules
Tags
Run Reachability Analyzer
Manage tags
Edit inbound rules
Filter security group rules
1

sg-0ebed23164ba74aca - TestInstanceSG

Details

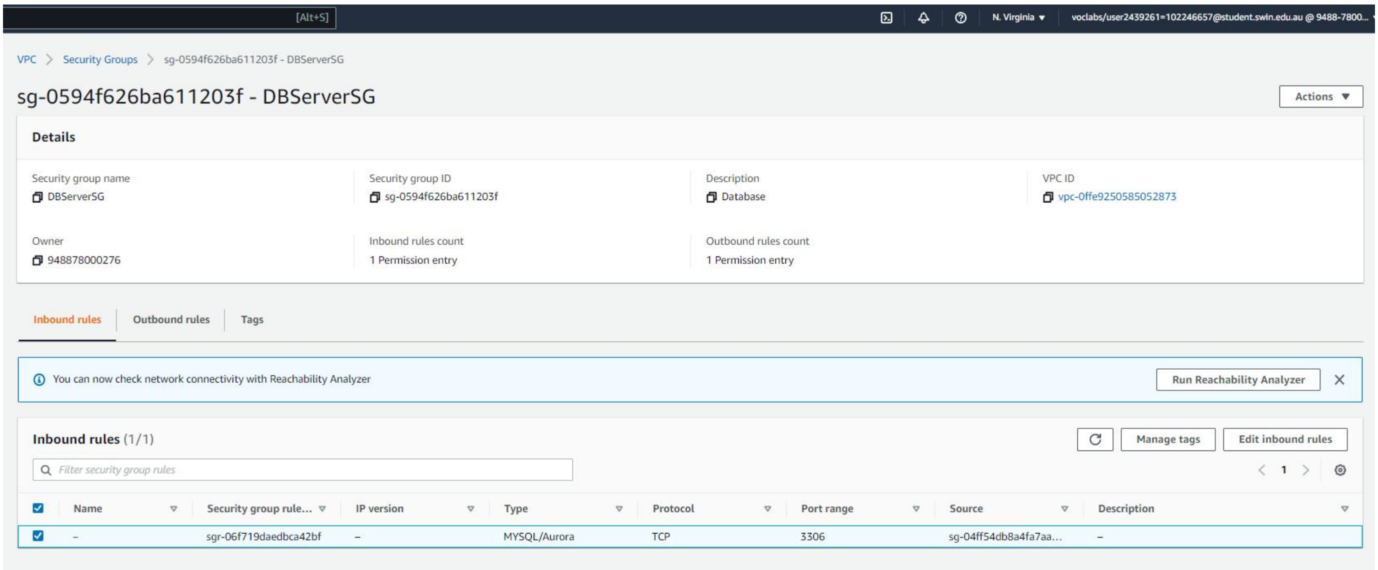
Security group name	Security group ID	Description	VPC ID
TestInstanceSG	sg-0ebed23164ba74aca	Test Instance	vpc-0ffe9250585052873
Owner	**Inbound rules count**	**Outbound rules count**	
948878000276	1 Permission entry	1 Permission entry	

You can now check network connectivity with Reachability Analyzer

Inbound rules (1/1)

☑	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
☑	–	sgr-06341a8c1a94bba...	IPv4	All traffic	All	All	0.0.0.0/0	–

Fig. 3 VPC Security Group 2.



[redacted] [Alt+S] N. Virginia ▾ voclabs/user2439261=102246657@student.swin.edu.au @ 9488-7800... ▾

VPC > Security Groups > sg-0594f626ba611203f - DBServerSG

sg-0594f626ba611203f - DBServerSG

Actions ▼

Details

Security group name: DBServerSG

Security group ID: sg-0594f626ba611203f

Description: Database

VPC ID: vpc-0ffe9250585052873

Owner: 948878000276

Inbound rules count: 1 Permission entry

Outbound rules count: 1 Permission entry

Inbound rules | Outbound rules | Tags

ⓘ You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer ✕

Inbound rules (1/1)

Manage tags | Edit inbound rules

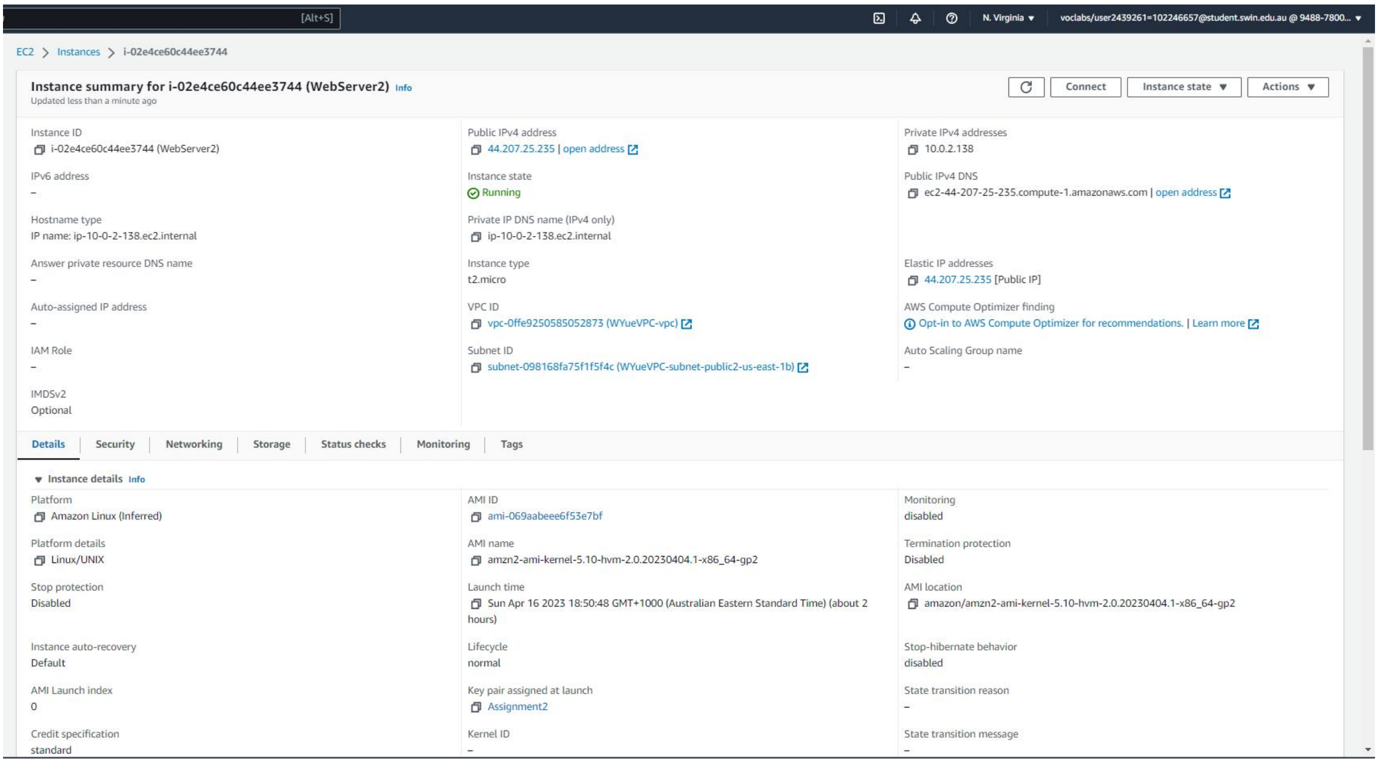
Filter security group rules

☑	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
☑	–	sgr-06f719daedbca42bf	–	MYSQL/Aurora	TCP	3306	sg-04ff54db8a4fa7aa...	–

Fig. 4 VPC Security Group 3.

III. Launch a Web Server Instance

A. Create a EC2 instance as a bastion host in public subnet of availability zone b. So that the private subnet will not be exposed and can be access via bastion host.



[redacted] [Alt+S] N. Virginia ▾ voclabs/user2439261=102246657@student.swin.edu.au @ 9488-7800... ▾

EC2 > Instances > i-02e4ce60c44ee3744

Instance summary for i-02e4ce60c44ee3744 (WebServer2) Info

Updated less than a minute ago

Connect | Instance state ▼ | Actions ▼

Instance ID: i-02e4ce60c44ee3744 (WebServer2)

Public IPv4 address: 44.207.25.235 | open address

Private IPv4 addresses: 10.0.2.138

IPv6 address: –

Instance state: Running

Public IPv4 DNS: ec2-44-207-25-235.compute-1.amazonaws.com | open address

Hostname type: IP name: ip-10-0-2-138.ec2.internal

Private IP DNS name (IPv4 only): ip-10-0-2-138.ec2.internal

Answer private resource DNS name: –

Instance type: t2.micro

Elastic IP addresses: 44.207.25.235 [Public IP]

Auto-assigned IP address: –

VPC ID: vpc-0ffe9250585052873 (WYueVPC-vpc)

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

IAM Role: –

Subnet ID: subnet-098168fa75f1f5f4c (WYueVPC-subnet-public2-us-east-1b)

Auto Scaling Group name: –

IMDSv2: Optional

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

▼ Instance details Info

Platform: Amazon Linux (Inferred)

AMI ID: ami-069aabeee6f53e7bf

Monitoring: disabled

Platform details: Linux/UNIX

AMI name: amzn2-ami-kernel-5.10-hvm-2.0.20230404.1-x86_64-gp2

Termination protection: Disabled

Stop protection: Disabled

Launch time: Sun Apr 16 2023 18:50:48 GMT+1000 (Australian Eastern Standard Time) (about 2 hours)

AMI location: amazon/amzn2-ami-kernel-5.10-hvm-2.0.20230404.1-x86_64-gp2

Instance auto-recovery: Default

Lifecycle: normal

Stop-hibernate behavior: disabled

AMI Launch index: 0

Key pair assigned at launch: Assignment2

State transition reason: –

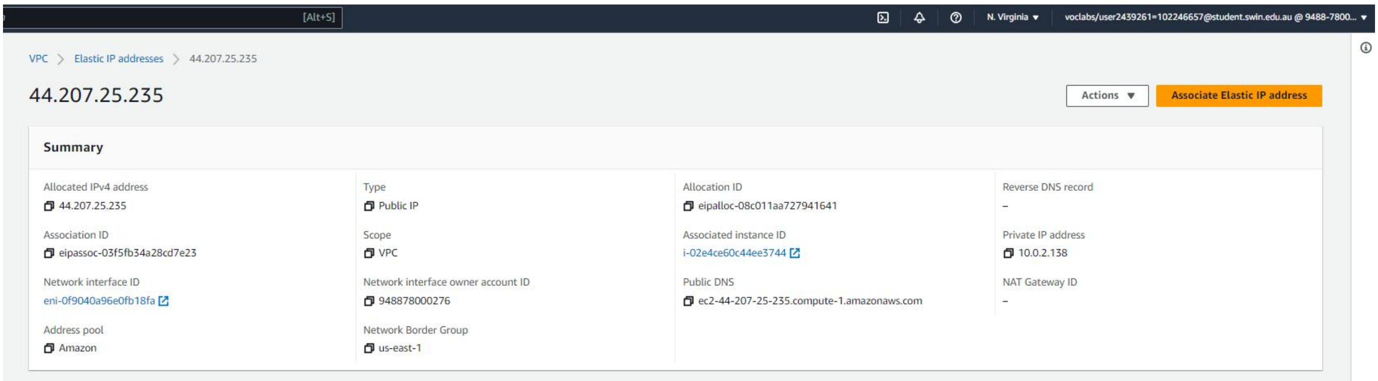
Credit specification: standard

Kernel ID: –

State transition message: –

Fig. 5 Create a new instance.

B. After the instance is launched, public DNS will change every time when the instance restarts, to avoid this, an Elastic IP address privode a fixed DNS address. Associate an elastic IP address with the instance so that the public address will not change.



[Alt+S]
N. Virginia ▾
voclabs/user2439261=102246657@student.swin.edu.au @ 9488-7800... ▾
VPC > Elastic IP addresses > 44.207.25.235
Actions ▾
Associate Elastic IP address

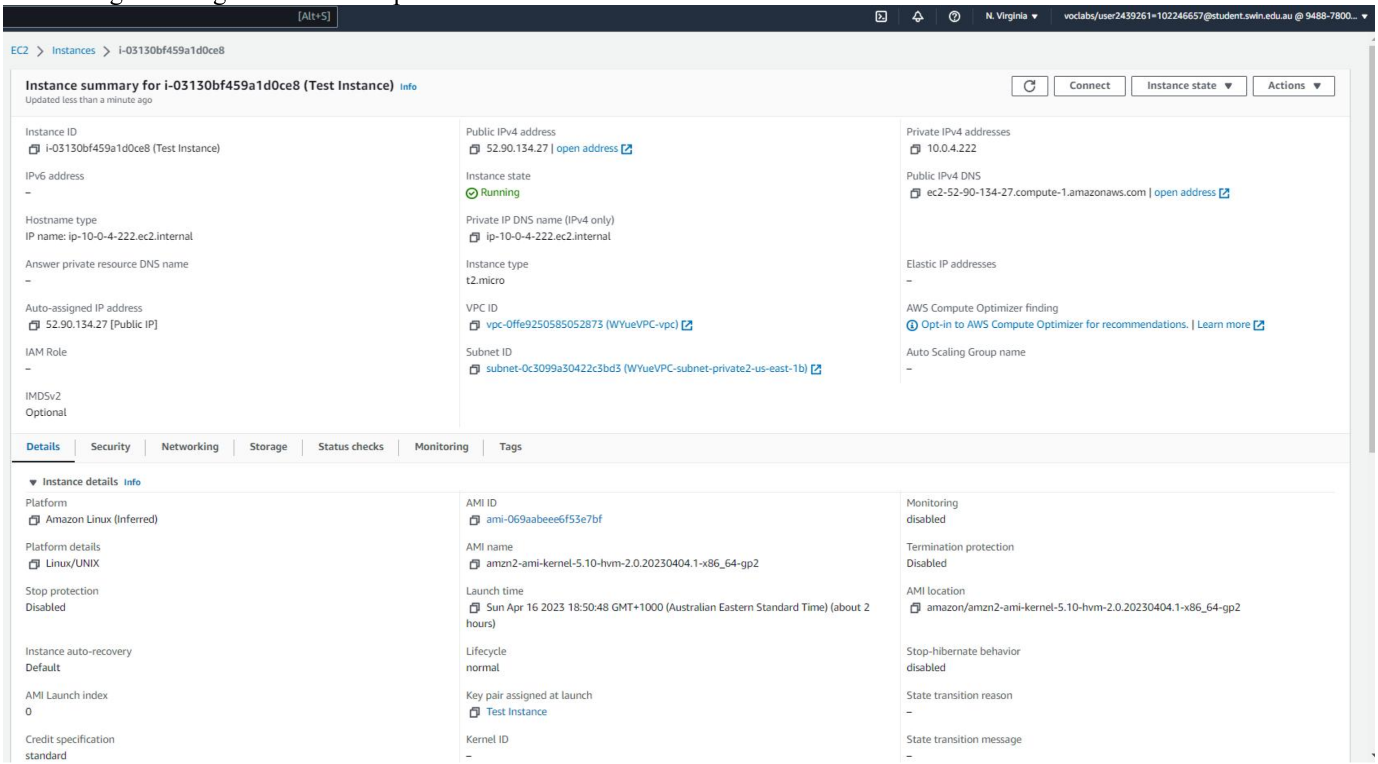
44.207.25.235

Summary

Allocated IPv4 address 44.207.25.235	Type Public IP	Allocation ID eipalloc-08c011aa727941641	Reverse DNS record –
Association ID eipassoc-03f5fb34a28cd7e23	Scope VPC	Associated instance ID i-02e4ce60c44ee3744	Private IP address 10.0.2.138
Network interface ID eni-0f9040a96e0fb18fa	Network interface owner account ID 948878000276	Public DNS ec2-44-207-25-235.compute-1.amazonaws.com	NAT Gateway ID –
Address pool Amazon	Network Border Group us-east-1		

Fig. 6 Create an Elastic IP.

C. Also, a private instance is created on private subnet, to access to the instance, using putty to log in to the bastion host first, then using SSH to get access to the private instance.



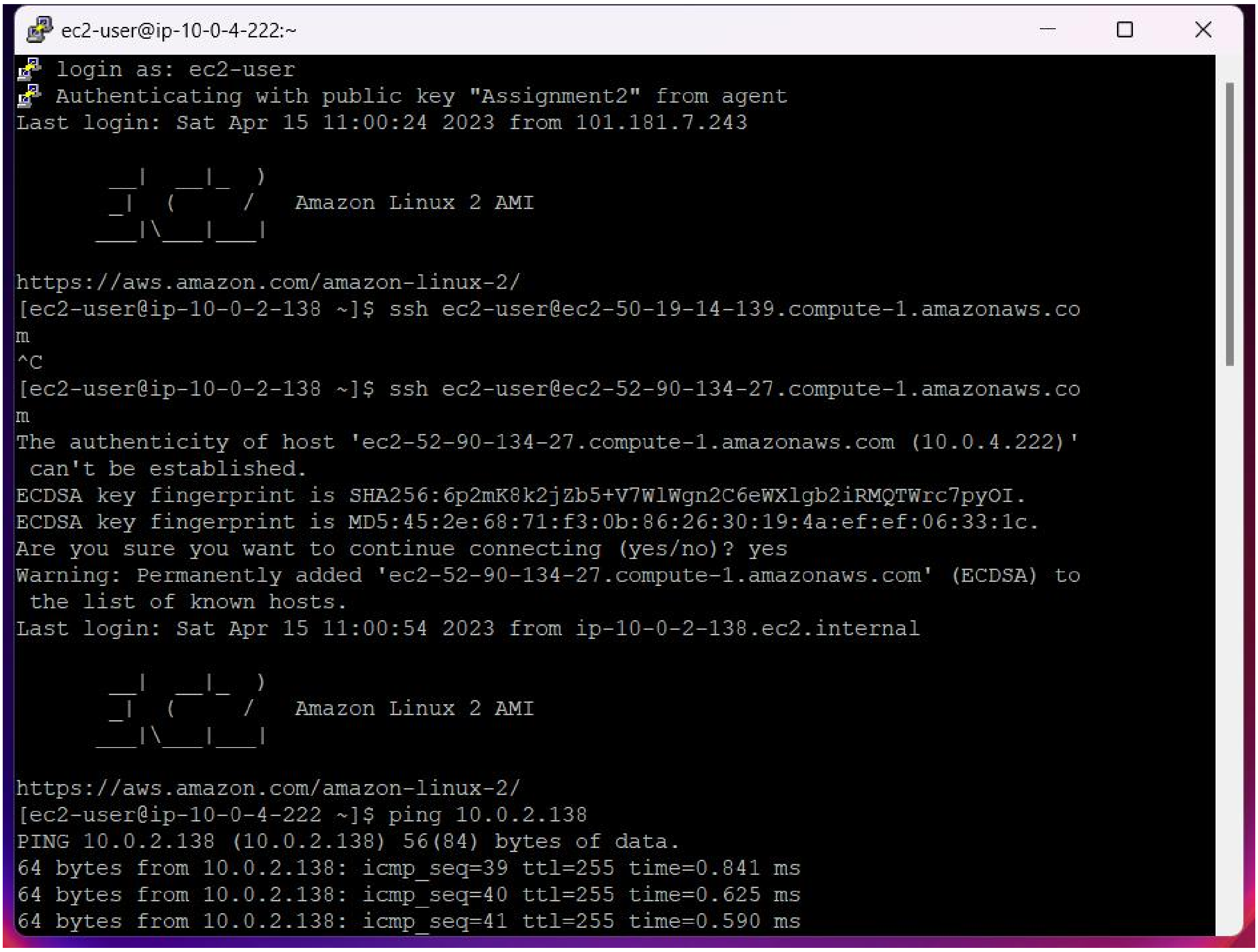
Instance summary for i-03130bf459a1d0ce8 (Test Instance)
Updated less than a minute ago

Instance ID i-03130bf459a1d0ce8 (Test Instance)	Public IPv4 address 52.90.134.27 | open address	Private IPv4 addresses 10.0.4.222
IPv6 address –	Instance state Running	Public IPv4 DNS ec2-52-90-134-27.compute-1.amazonaws.com | open address
Hostname type IP name: ip-10-0-4-222.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-4-222.ec2.internal	
Answer private resource DNS name –	Instance type t2.micro	Elastic IP addresses –
Auto-assigned IP address 52.90.134.27 [Public IP]	VPC ID vpc-0ffe9250585052873 (WYueVPC-vpc)	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role –	Subnet ID subnet-0c3099a30422c3bd3 (WYueVPC-subnet-private2-us-east-1b)	Auto Scaling Group name –
IMDSv2 Optional		

▾ Instance details Info

Platform Amazon Linux (Inferred)	AMI ID ami-069aabeee6f53e7bf	Monitoring disabled
Platform details Linux/UNIX	AMI name amzn2-ami-kernel-5.10-hvm-2.0.20230404.1-x86_64-gp2	Termination protection Disabled
Stop protection Disabled	Launch time Sun Apr 16 2023 18:50:48 GMT+1000 (Australian Eastern Standard Time) (about 2 hours)	AMI location amazon/amzn2-ami-kernel-5.10-hvm-2.0.20230404.1-x86_64-gp2
Instance auto-recovery Default	Lifecycle normal	Stop-hibernate behavior disabled
AMI Launch index 0	Key pair assigned at launch Test Instance	State transition reason –
Credit specification standard	Kernel ID –	State transition message –

Fig. 7 Create a private instance.

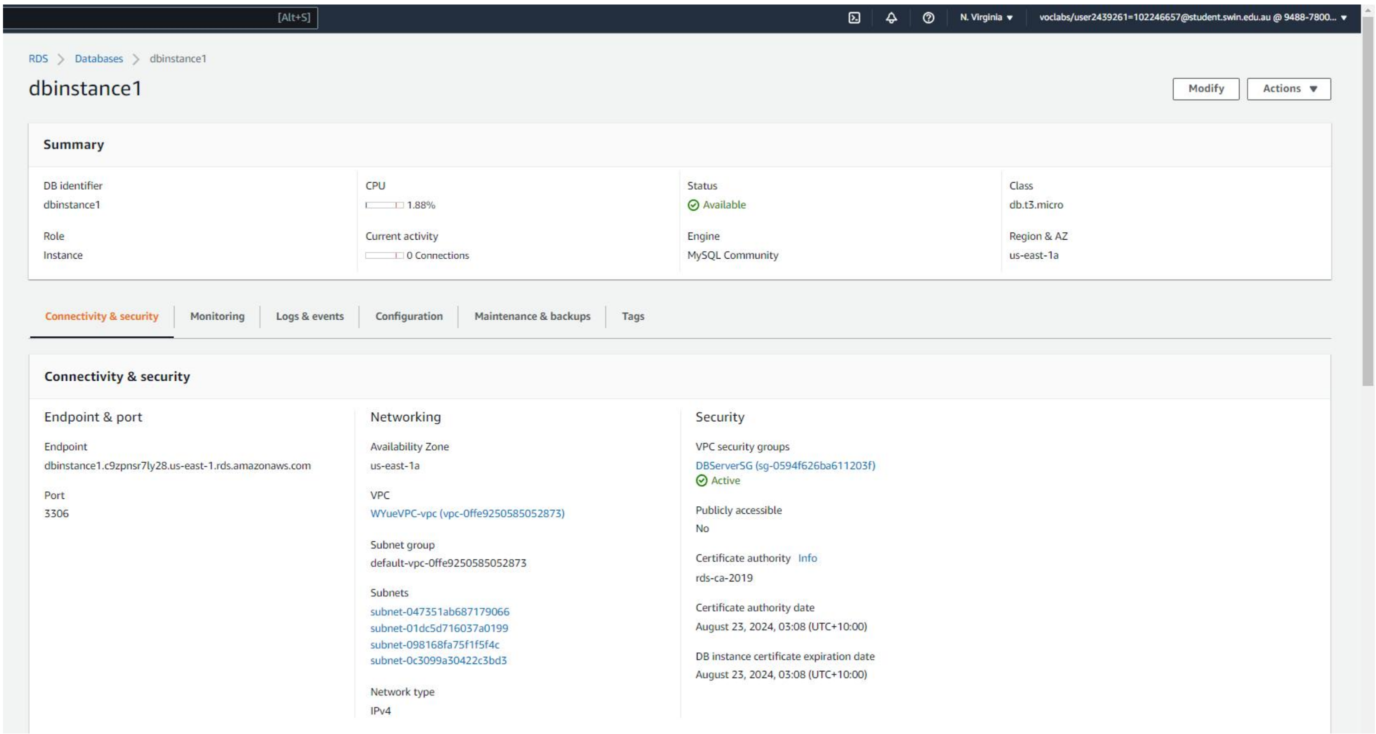


```
login as: ec2-user
Authenticating with public key "Assignment2" from agent
Last login: Sat Apr 15 11:00:24 2023 from 101.181.7.243

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-2-138 ~]$ ssh ec2-user@ec2-50-19-14-139.compute-1.amazonaws.co
m
^C
[ec2-user@ip-10-0-2-138 ~]$ ssh ec2-user@ec2-52-90-134-27.compute-1.amazonaws.co
m
The authenticity of host 'ec2-52-90-134-27.compute-1.amazonaws.com (10.0.4.222)'
 can't be established.
ECDSA key fingerprint is SHA256:6p2mK8k2jZb5+V7WlWgn2C6eWXlgb2iRMQTWrc7pyOI.
ECDSA key fingerprint is MD5:45:2e:68:71:f3:0b:86:26:30:19:4a:ef:ef:06:33:1c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-52-90-134-27.compute-1.amazonaws.com' (ECDSA) to
 the list of known hosts.
Last login: Sat Apr 15 11:00:54 2023 from ip-10-0-2-138.ec2.internal

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-4-222 ~]$ ping 10.0.2.138
PING 10.0.2.138 (10.0.2.138) 56(84) bytes of data.
64 bytes from 10.0.2.138: icmp_seq=39 ttl=255 time=0.841 ms
64 bytes from 10.0.2.138: icmp_seq=40 ttl=255 time=0.625 ms
64 bytes from 10.0.2.138: icmp_seq=41 ttl=255 time=0.590 ms
```

Fig. 8 Connect to the private instance.

IV. Create a RDS database instance

A RDS database that created in private subnet, it will be accessed through the bastion host. This RDS has a 8.0.25 MySQL database, also, phpMyAdmin is also installed to manage data in the database.



dbinstance1

Summary

DB identifier dbinstance1	CPU 1.88%	Status Available	Class db.t3.micro
Role Instance	Current activity 0 Connections	Engine MySQL Community	Region & AZ us-east-1a

Connectivity & security

Endpoint & port

Endpoint
dbinstance1.c9zpnsr7ly28.us-east-1.rds.amazonaws.com

Port
3306

Networking

Availability Zone
us-east-1a

VPC
WYueVPC-vpc (vpc-0ffe9250585052873)

Subnet group
default-vpc-0ffe9250585052873

Subnets
subnet-047351ab687179066
subnet-01dc5d716037a0199
subnet-098168fa75f1f5f4c
subnet-0c3099a30422c3bd3

Network type
IPv4

Security

VPC security groups
DBServerSG (sg-0594f626ba611203f)
Active

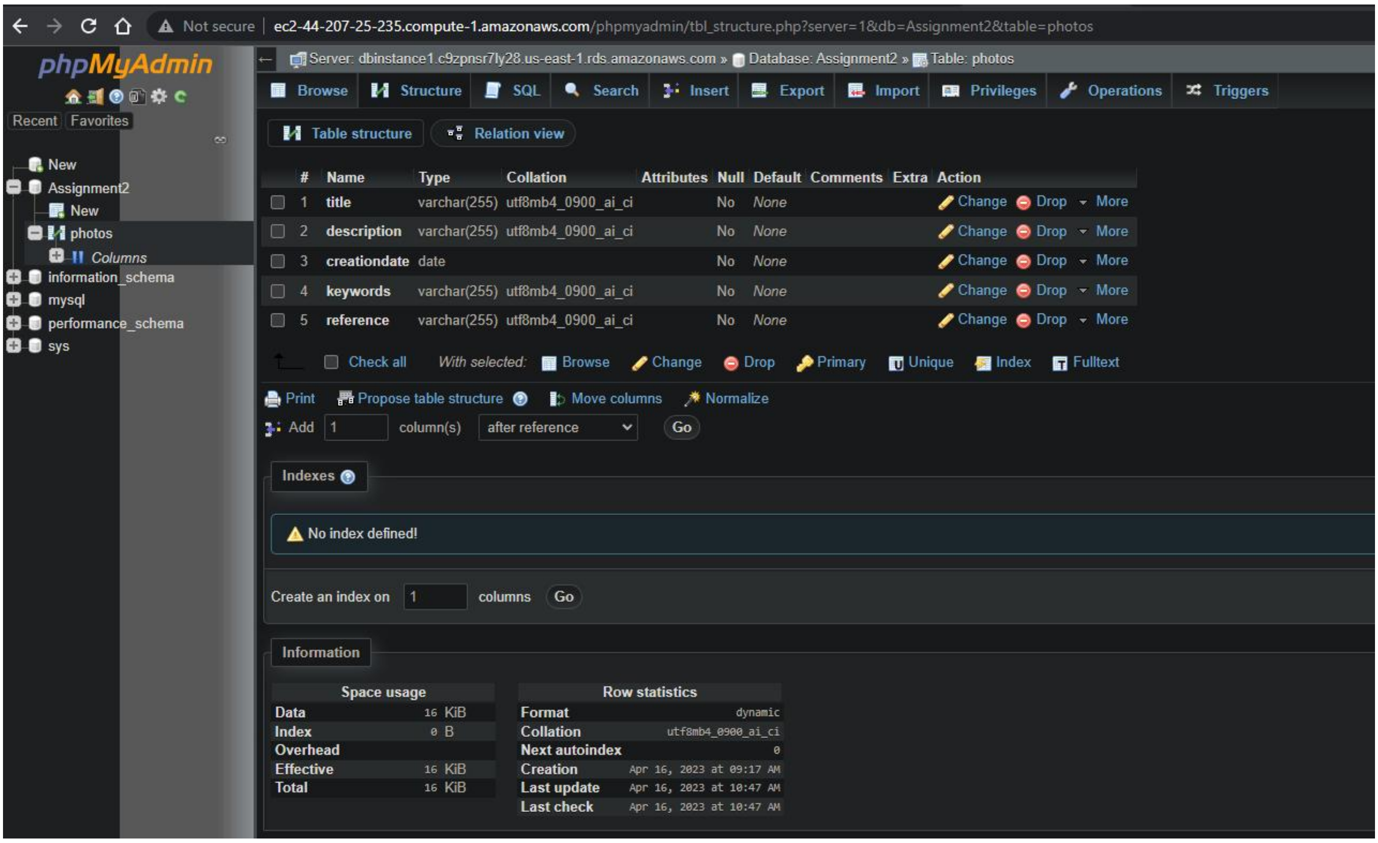
Publicly accessible
No

Certificate authority Info
rds-ca-2019

Certificate authority date
August 23, 2024, 03:08 (UTC+10:00)

DB instance certificate expiration date
August 23, 2024, 03:08 (UTC+10:00)

Fig. 9 RDS Database Instance.



ec2-44-207-25-235.compute-1.amazonaws.com/phpmyadmin/tbl_structure.php?server=1&db=Assignment2&table=photos

Server: dbinstance1.c9zpnsr7ly28.us-east-1.rds.amazonaws.com » Database: Assignment2 » Table: photos

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	title	varchar(255)	utf8mb4_0900_ai_ci		No	None			Change Drop More
2	description	varchar(255)	utf8mb4_0900_ai_ci		No	None			Change Drop More
3	creationdate	date			No	None			Change Drop More
4	keywords	varchar(255)	utf8mb4_0900_ai_ci		No	None			Change Drop More
5	reference	varchar(255)	utf8mb4_0900_ai_ci		No	None			Change Drop More

Add 1 column(s) after reference

No index defined!

Create an index on 1 columns

Information

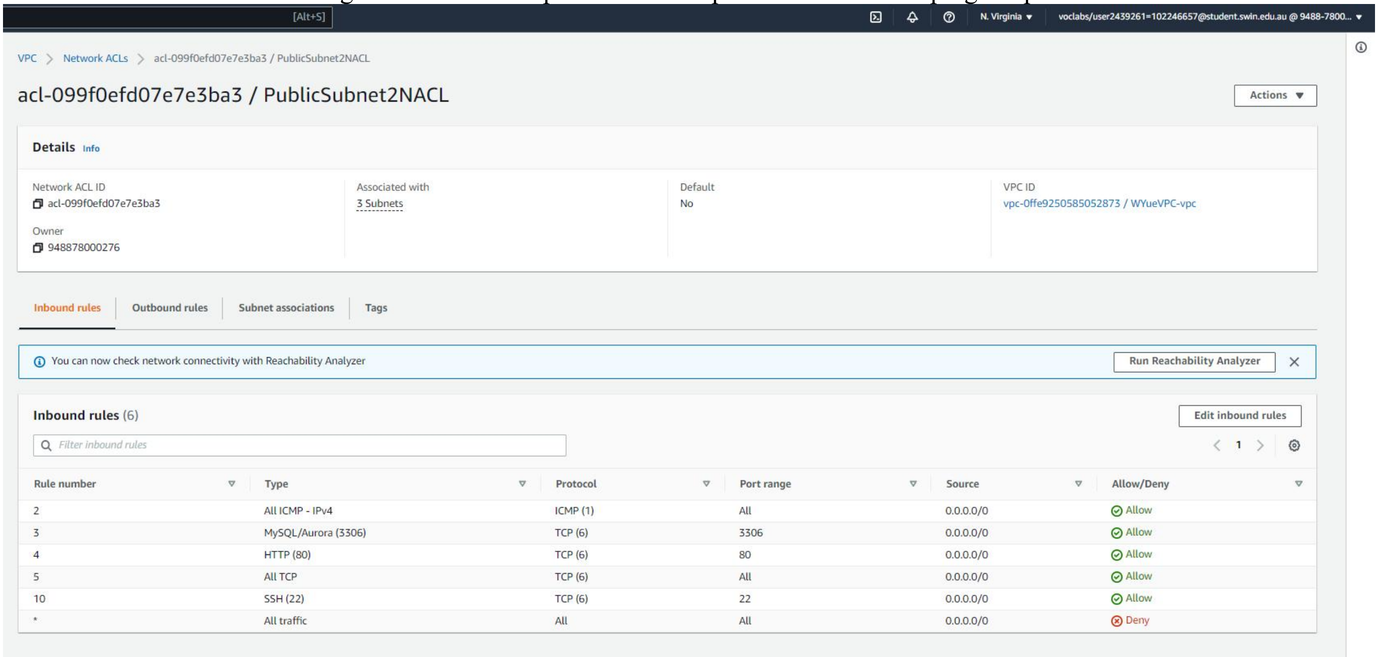
Space usage		
Data	16	KiB
Index	0	B
Overhead		
Effective	16	KiB
Total	16	KiB

Row statistics	
Format	dynamic
Collation	utf8mb4_0900_ai_ci
Next autoindex	0
Creation	Apr 16, 2023 at 09:17 AM
Last update	Apr 16, 2023 at 10:47 AM
Last check	Apr 16, 2023 at 10:47 AM

Fig. 9 PhpMyAdmin.

V. Network ACL

ACL is Access Control List, an additional layer of security to your web serve. Allowing TCP connection pass so that most of the connection can be built. Having the ICMP traffic pass so that the private instance can ping the public instance.



[Alt+S]

N. Virginia ▾ voclabs/user2439261=102246657@student.swin.edu.au @ 9488-7800... ▾

VPC > Network ACLs > acl-099f0efd07e7e3ba3 / PublicSubnet2NACL

acl-099f0efd07e7e3ba3 / PublicSubnet2NACL

Actions ▾

Details Info

Network ACL ID	Associated with	Default	VPC ID
acl-099f0efd07e7e3ba3	3 Subnets	No	vpc-0ffe9250585052873 / WYueVPC-vpc

Owner
948878000276

Inbound rules | Outbound rules | Subnet associations | Tags

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

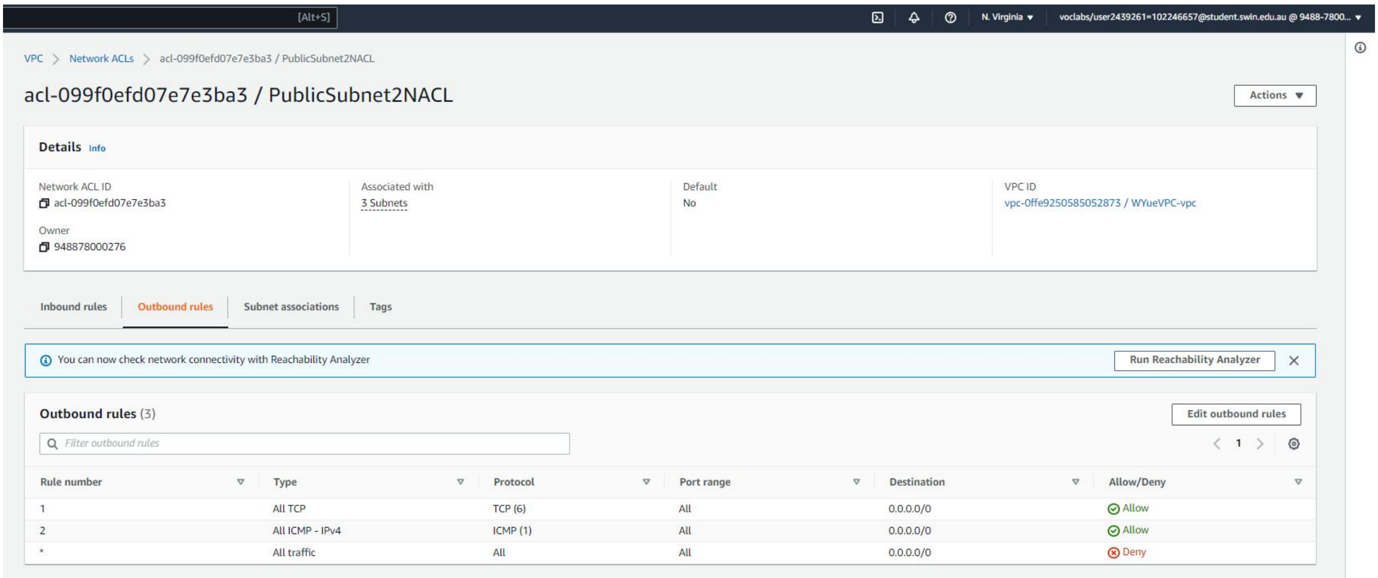
Inbound rules (6)

Edit inbound rules

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
2	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	✓ Allow
3	MySQL/Aurora (3306)	TCP (6)	3306	0.0.0.0/0	✓ Allow
4	HTTP (80)	TCP (6)	80	0.0.0.0/0	✓ Allow
5	All TCP	TCP (6)	All	0.0.0.0/0	✓ Allow
10	SSH (22)	TCP (6)	22	0.0.0.0/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

Fig. 10 ACL Inbound Rules.



[Alt+S]

N. Virginia ▾ voclabs/user2439261=102246657@student.swin.edu.au @ 9488-7800... ▾

VPC > Network ACLs > acl-099f0efd07e7e3ba3 / PublicSubnet2NACL

acl-099f0efd07e7e3ba3 / PublicSubnet2NACL

Actions ▾

Details Info

Network ACL ID	Associated with	Default	VPC ID
acl-099f0efd07e7e3ba3	3 Subnets	No	vpc-0ffe9250585052873 / WYueVPC-vpc

Owner
948878000276

Inbound rules | Outbound rules | Subnet associations | Tags

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Outbound rules (3)

Edit outbound rules

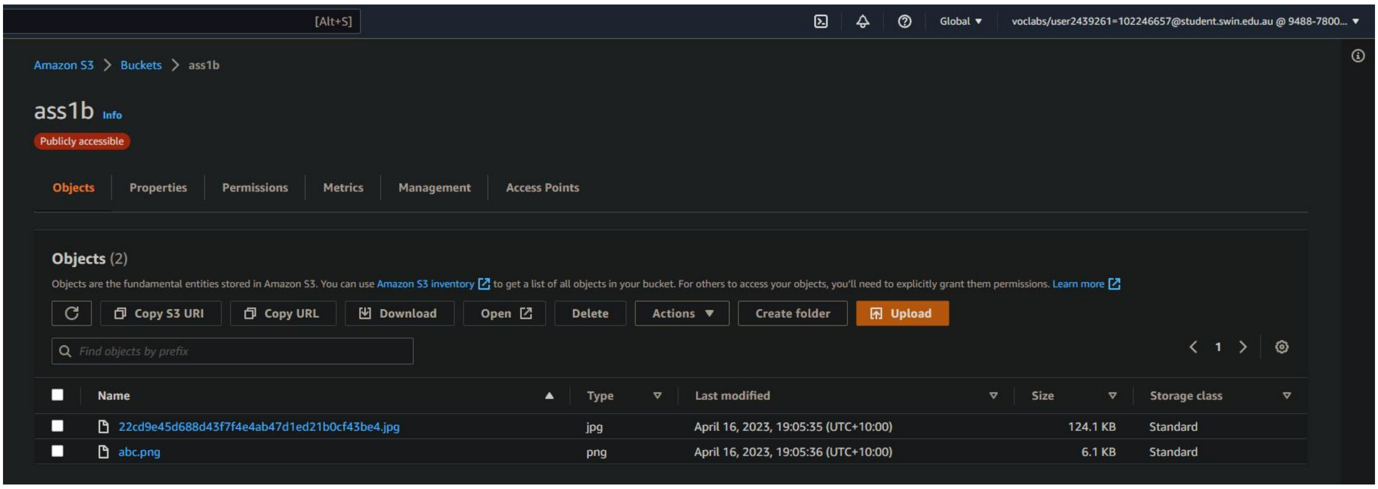
Filter outbound rules

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
1	All TCP	TCP (6)	All	0.0.0.0/0	✓ Allow
2	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

Fig. 11 ACL Outbound Rules.

VI. S3 Bucket

S3 bucket is a public cloud storage platform on AWS, rather than MySQL, S3 is primarily used for storing media files such as images, audio and video, as well as other large files.


[Alt+S]
Global ▼
voclabs/user2439261=102246657@student.swin.edu.au @ 9488-7800... ▼
Amazon S3 > Buckets > ass1b

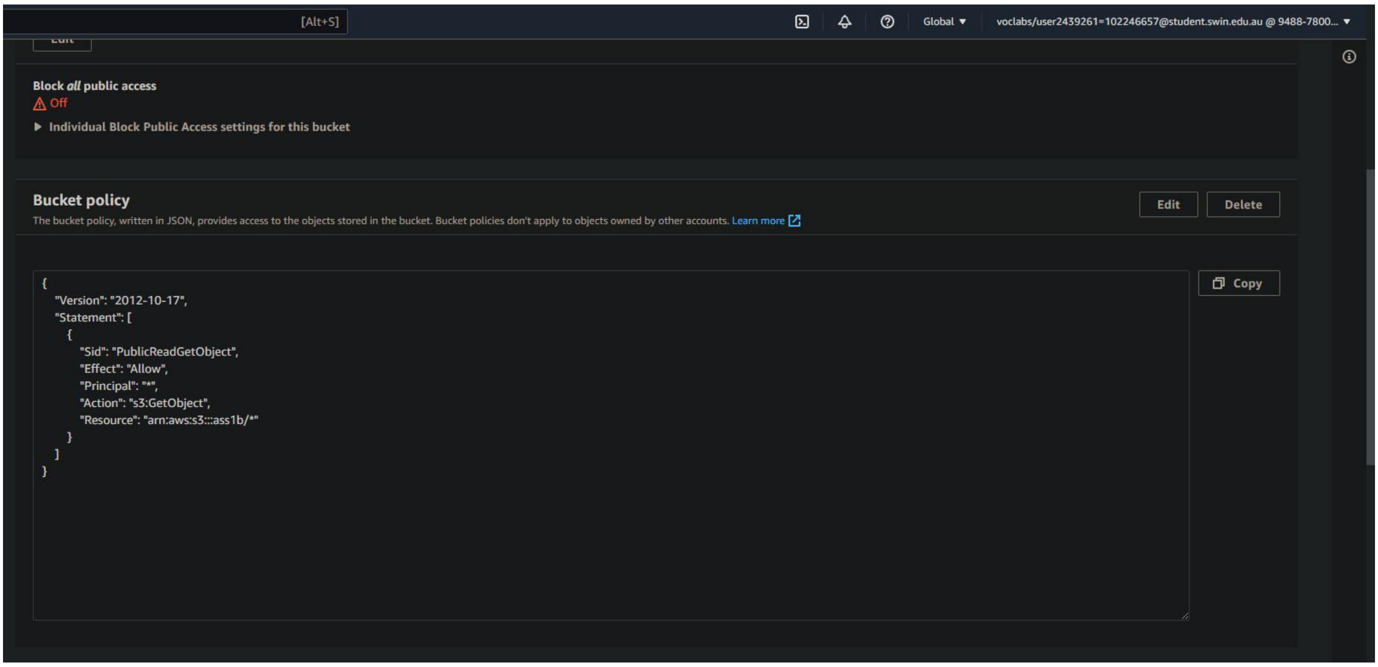
ass1b Info

Objects (2)

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
□	22cd9e45d688d43f7f4e4ab47d1ed21b0cf43be4.jpg	jpg	April 16, 2023, 19:05:35 (UTC+10:00)	124.1 KB	Standard
□	abc.png	png	April 16, 2023, 19:05:36 (UTC+10:00)	6.1 KB	Standard

Fig. 12 S3 Bucket.


[Alt+S]
Global ▼
voclabs/user2439261=102246657@student.swin.edu.au @ 9488-7800... ▼

Block *all* public access
⚠ Off

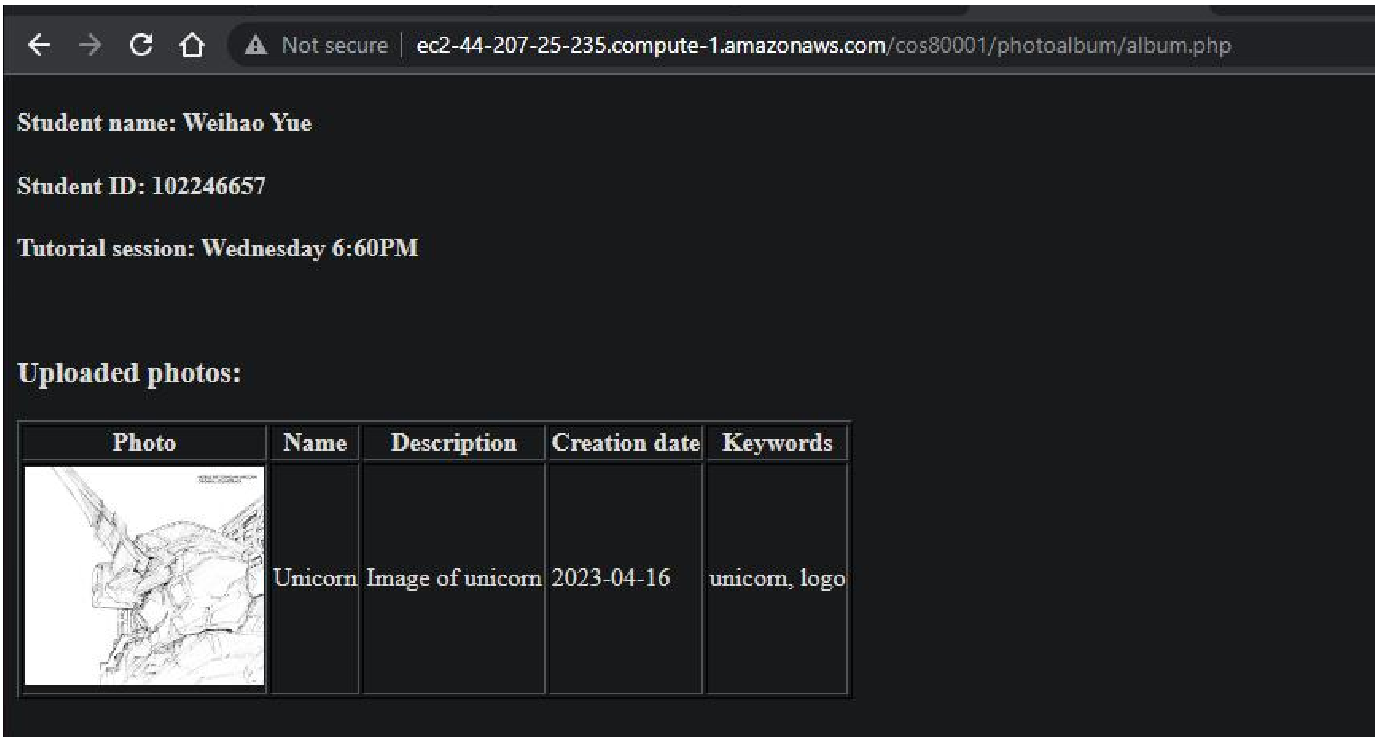
▶ Individual Block Public Access settings for this bucket

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",
   "Statement": [
      {
         "Sid": "PublicReadGetObject",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "s3:GetObject",
         "Resource": "arn:aws:s3:::ass1b/*"
      }
   ]
}
```

Fig. 13 S3 Bucket Policy.



Not secure | ec2-44-207-25-235.compute-1.amazonaws.com/cos80001/photoalbum/album.php

Student name: Weihao Yue

Student ID: 102246657

Tutorial session: Wednesday 6:60PM

Uploaded photos:

Photo	Name	Description	Creation date	Keywords
	Unicorn	Image of unicorn	2023-04-16	unicorn, logo

Fig. 14 Webpage.