

Assignment 1b

COS20019

Cloud Computing Architecture

Tran Thien Thao Vy

104991221

Swinburne University of Technology

School of Science, Computing and Engineering Technologies

1. Infrastructure deployment

1.1 VPC

Configure the name of VPC as follows the instructions.

The screenshot shows the AWS Management Console interface for creating a new VPC. The top navigation bar includes the AWS logo, 'Services' menu, a search bar, and user information for 'voclabs/user3485657=104991221@student.swin.edu.au' in the 'N. Virginia' region. The main heading is 'Create VPC' with an 'Info' link. Below this, a descriptive sentence states: 'A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.'

The 'VPC settings' section on the left contains three main configuration areas:

- Resources to create:** Two radio buttons are present: 'VPC only' (unselected) and 'VPC and more' (selected).
- Name tag auto-generation:** A text box for the Name tag value is set to 'VTranVPC'. The 'Auto-generate' checkbox is checked.
- IPv4 CIDR block:** A text box for the CIDR block is set to '10.0.0.0/16', which provides '65,536 IPs'. A note below states: 'CIDR block size must be between /16 and /28.'

The 'Preview' section on the right displays a visual representation of the VPC setup. It shows a central box for the 'VPC' (labeled 'VTranVPC-vpc') connected to four subnets. The subnets are organized into two availability zones: 'us-east-1a' and 'us-east-1b'. Under 'us-east-1a', there are two subnets: 'VTranVPC-subnet-public1-us-east-1a' (public) and 'VTranVPC-subnet-private1-us-east-1a' (private). Under 'us-east-1b', there are two subnets: 'VTranVPC-subnet-public2-us-east-1b' (public) and 'VTranVPC-subnet-private2-us-east-1b' (private).

The footer of the console shows 'CloudShell' and 'Feedback' links on the left, and copyright information '© 2024, Amazon Web Services, Inc. or its affiliates.' along with 'Privacy', 'Terms', and 'Cookie preferences' links on the right.

Configure 2 Availability Zones, each with public and private subnets as illustrated in the infrastructure diagram.

aws Services Search [Alt+S] N. Virginia voclabs/user3485657=104991221@student.swin.edu.au @ 4866-8500...

VPC

Number of Availability Zones (AZs) Info
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 2 3

Customize AZs

First availability zone
us-east-1a

Second availability zone
us-east-1b

Number of public subnets Info
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 2

Number of private subnets Info
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 2 4

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws Services Search [Alt+S] N. Virginia voclabs/user3485657=104991221@student.swin.edu.au @ 4866-8500...

VPC

Customize subnets CIDR blocks

Public subnet CIDR block in us-east-1a
10.0.1.0/24 256 IPs

Public subnet CIDR block in us-east-1b
10.0.2.0/24 256 IPs

Private subnet CIDR block in us-east-1a
10.0.3.0/24 256 IPs

Private subnet CIDR block in us-east-1b
10.0.4.0/24 256 IPs

NAT gateways (\$) Info
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

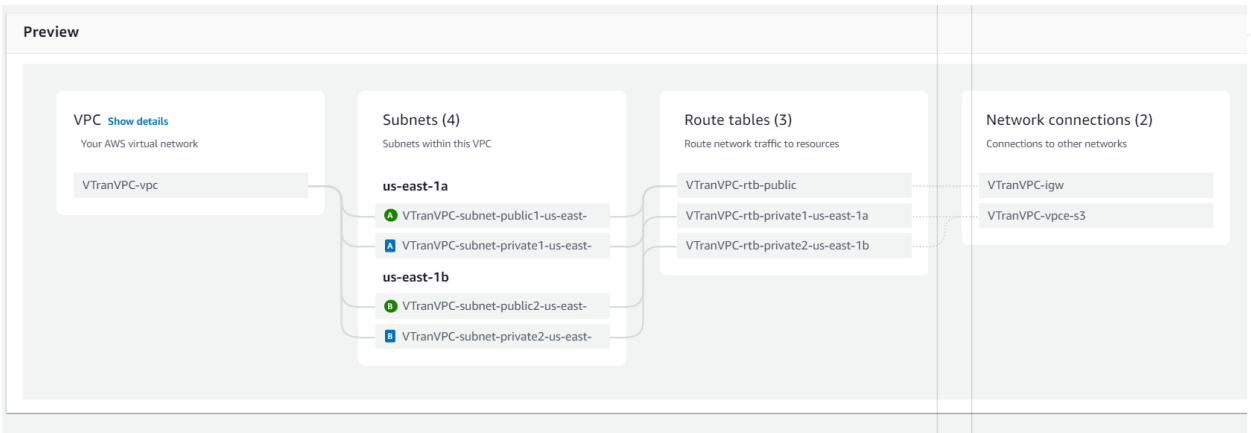
None In 1 AZ 1 per AZ

VPC endpoints Info
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Preview of the Subnets connected to the right route tables. Make sure that the route table for public subnets, especially the public subnet 2, is connected to the Internet Gateway connection for further storing and reading photos.

As the private subnets are mainly used for back-end support, there is no need to be connected over the internet.



1.2 Security groups

Create 3 security groups, which are WebServerSG, TestInstanceSG, and DBServerSG with the provided Protocols and Source, through checking their Inbound Rules.

	Name	Security group ID	Security group name	VPC ID
<input checked="" type="checkbox"/>	-	sg-0bf7d9ca59951cc23	WebServerSG	vpc-0c3389438ca
<input type="checkbox"/>	-	sg-0ce93f63915945e07	default	vpc-0c3389438ca
<input checked="" type="checkbox"/>	-	sg-079c0a67834989bac	DBServerSG	vpc-0c3389438ca
<input type="checkbox"/>	-	sg-017fd2aac77f46c08	default	vpc-03c1cdd6ac4
<input type="checkbox"/>	-	sg-0b9b92824e81ce26e	WebServer-SG	vpc-03c1cdd6ac4
<input checked="" type="checkbox"/>	-	sg-09175606d8e9a0050	TestInstanceSG	vpc-0c3389438ca

Inbound rules of WebServerSG:

Inbound rules (3)						
<div>Search</div>						
<div>< 1 > ⚙</div>						
<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	
<input type="checkbox"/>	-	sgr-0045bf7918ed9f061	IPv4	HTTP	TCP	
<input type="checkbox"/>	-	sgr-0b8b8f46aed2b07...	-	All ICMP - IPv4	ICMP	
<input type="checkbox"/>	-	sgr-0480eed0f2239a7dd	IPv4	SSH	TCP	

Inbound rules of TestInstanceSG:

Inbound rules (1)					
<div> <input type="text" value="Search"/> <div> <div><</div> <div>1</div> <div>></div> <div>⚙</div> </div> </div>					
<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Prot...
<input type="checkbox"/>	-	sgr-0f5e7f14bf4a6c6d0	IPv4	All traffic	All

Inbound rules of DBServerSG:

Inbound rules (1)					
<div> <input type="text" value="Search"/> <div> <div><</div> <div>1</div> <div>></div> <div>⚙</div> </div> </div>					
<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Prot...
<input type="checkbox"/>	-	sgr-0cb768d89861dda...	-	MYSQL/Aurora	TCP

1.3 EC2 virtual machine

1.3.1 Bastion/Web server instance

Configure the instance as the instruction requires, make sure to allocate the instance into the correct VPC, Public Subnet 2.

aws

Services

[Alt+S]

N. Virginia

voclabs/user3485657=104991221@student.swin.edu.au @ 4866-8500...

VPC

VPC - required

Info

vpc-0c3389438ca3a97df (VTranVPC-vpc)

10.0.0.0/16

Subnet

Info

subnet-0c3e22aa47efb6798 VTranVPC-subnet-public2-us-east-1b

VPC: vpc-0c3389438ca3a97df Owner: 486685003184

Availability Zone: us-east-1b Zone type: Availability Zone

IP addresses available: 251 CIDR: 10.0.2.0/24

Create new subnet

Auto-assign public IP

Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group
 ☒ Select existing security group

Common security groups

Info

Select security groups

WebServerSG sg-0bf7d9ca59951cc23

VPC: vpc-0c3389438ca3a97df

Compare security group rules

Summary

Number of instances

Info

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...read more

ami-00f251754ac5da7f0

Virtual server type (instance type)

t2.micro

Firewall (security group)

WebServerSG

Storage (volumes)

1 volume(s) - 8 GiB

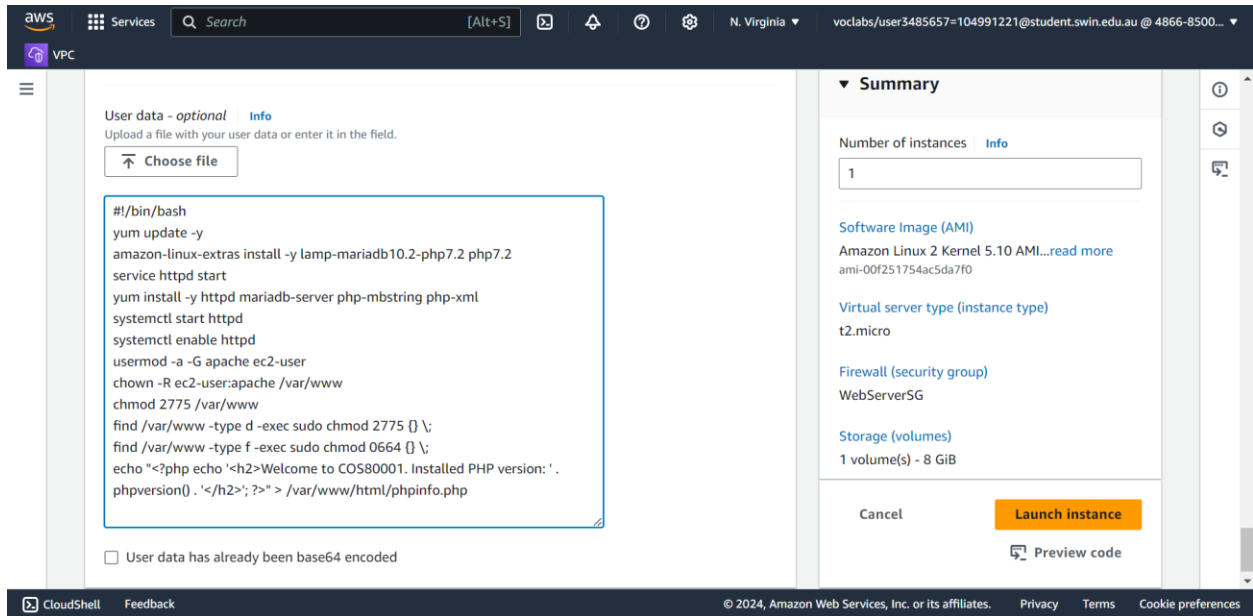
Cancel

Launch instance

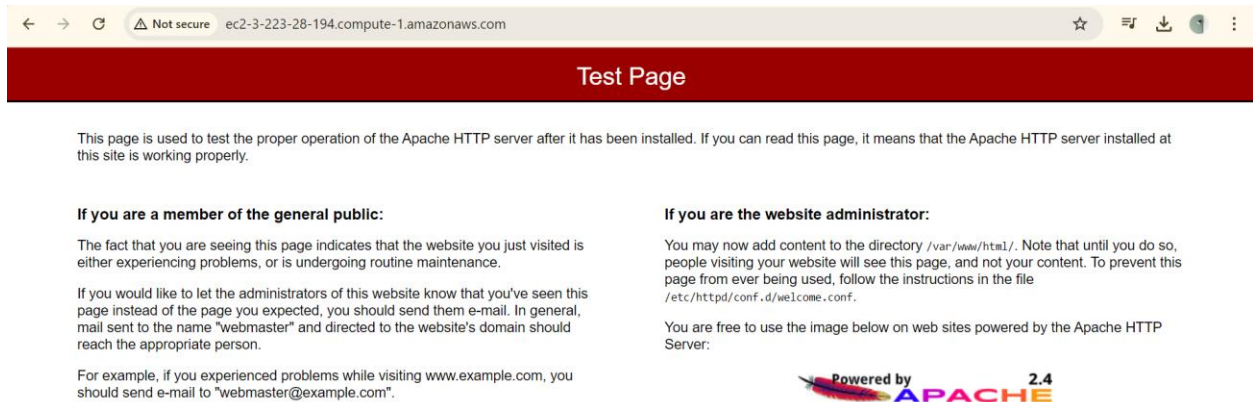
Preview code

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Reuse the same Apache text as in assignment 1a to install the Apache web server and PHP packages.

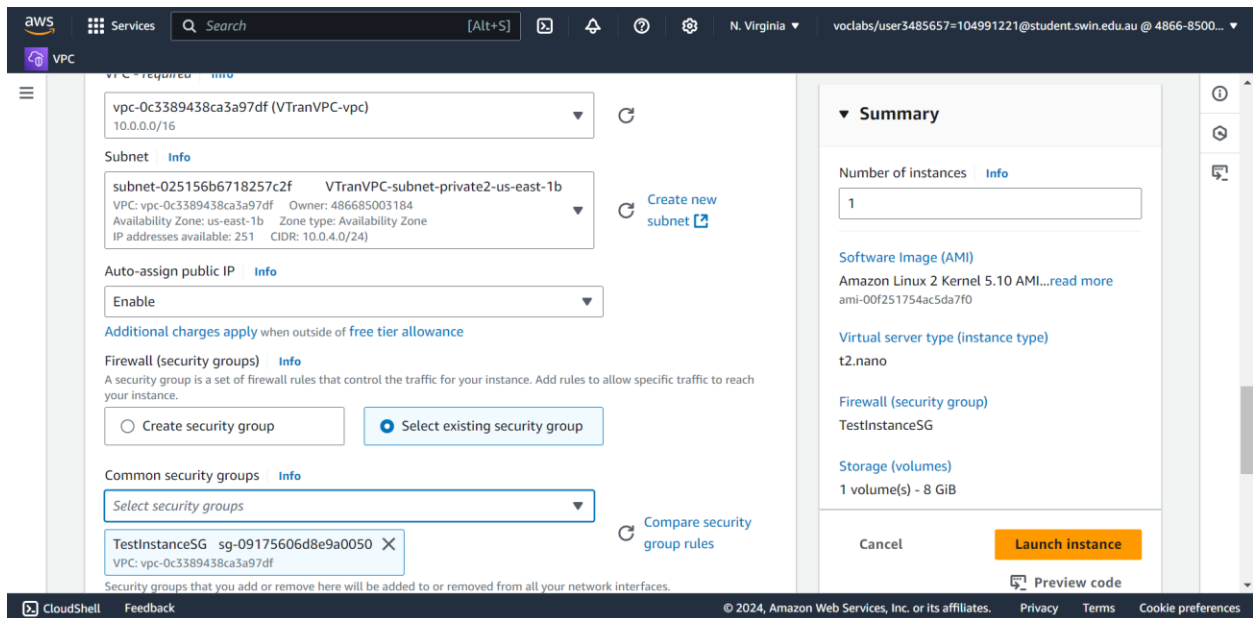


Go to the web browser, using the ec2 public DNS to check if the Apache has been installed successfully.



1.3.2 Test instance

Configure the test instance, make sure that it employs the TestInstanceSG security group.

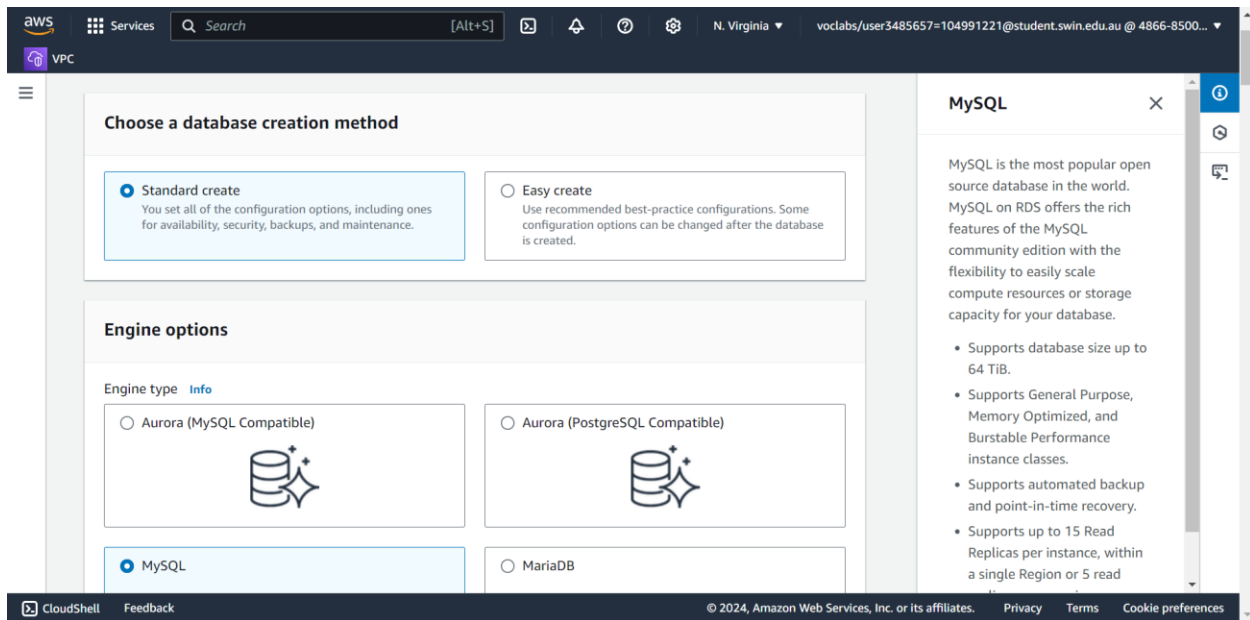


Assigning the Elastic IPs to the instances so that the next time we restart the instances, the public DNS and IPs will not be changed.

Instance summary for i-0448603706198257e (Bastion/Web server instance) Info		
<div> <input type="button" value="Connect"/> <input type="button" value="Instance state"/> <input type="button" value="Actions"/> </div> <p>Updated less than a minute ago</p>		
Instance ID i-0448603706198257e (Bastion/Web server instance)	Public IPv4 address 3.223.28.194 open address	Private IPv4 addresses 10.0.2.99
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-3-223-28-194.compute-1.amazonaws.com open address
Hostname type IP name: ip-10-0-2-99.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-2-99.ec2.internal	Elastic IP addresses 3.223.28.194 [Public IP]
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations.
Auto-assigned IP address -	VPC ID vpc-0c3389438ca3a97df (VTranVPC-	

1.4 RDS database instance

Configure the RDS database instance as required.



Engine version

MySQL 8.0.34 ▼

☐ **Enable RDS Extended Support** [Info](#)

Amazon RDS Extended Support is a [paid offering](#). By selecting this option, you consent to being charged for this offering if you are running your database major version past the RDS end of standard support date for that version. Check the end of standard support date for your major version in the [RDS for MySQL documentation](#).

Make sure we configure it into the DB Server security group.

Existing VPC security groups

Choose one or more options ▼

DBServerSG ✕

Availability Zone [Info](#)

us-east-1a ▼

To access to the database through the internet for setting up and maintenance, we can use the phpMyAdmin.

We can access the phpMyAdmin through Putty and public EC2 DNS:

[illegible]

Modify the `config.inc.php`, setting `host` to the RDS endpoint.

```

declare(strict_types=1);

/**
 * This is needed for cookie based authentication to encrypt the cookie.
 * Needs to be a 32-bytes long string of random bytes. See FAQ 2.10.
 */
$config['blowfish_secret'] = ''; /* YOU MUST FILL IN THIS FOR COOKIE AUTH! */

/**
 * Servers configuration
 */
$S = 0;

/**
 * First server
 */
$S++;

/* Authentication type */
$config['Servers'][$S]['auth_type'] = 'cookie';
/* Server parameters */
$config['Servers'][$S]['host'] = 'assignment1-db.cjrrcnslapup.us-east-1-rds.amazonaws.com';
$config['Servers'][$S]['compress'] = false;
$config['Servers'][$S]['AllowNoPassword'] = false;

/**
 * phpMyAdmin configuration storage settings.
 */

/* User used to manipulate with storage */
// $config['Servers'][$S]['controlhost'] = '';
// $config['Servers'][$S]['controlport'] = '';
// $config['Servers'][$S]['controluser'] = 'pma';
// $config['Servers'][$S]['controlpass'] = 'pmapass';

/* Storage database and tables */
// $config['Servers'][$S]['pmadb'] = 'phpmyadmin';
// $config['Servers'][$S]['bookmarktable'] = 'pma_bookmark';
// $config['Servers'][$S]['table'] = 'pma_tables';

```

After that, we can access the phpMyAdmin console through EC2 public DNS and create a photo table with 5 columns, which are title, description, creation date, keywords and s3 references.

The top screenshot shows the phpMyAdmin interface for the 'assignment1b' database. The 'General settings' tab is active, displaying options for changing the password, server connection collation (set to 'utf8mb4_unicode_ci'), and appearance settings (theme set to 'pmahomme'). The 'Database server' tab shows details about the MySQL server, including its type, version (8.0.34), protocol version (10), user (admin@10.0.2.99), and charset (UTF-8 Unicode). The 'Web server' tab shows details about the Apache server, including its version (2.4.62), database client version, and PHP version (7.2.34).

The bottom screenshot shows the 'SQL' tab of the phpMyAdmin interface. It displays three queries executed in the 'assignment1b' database:

```

MySQL returned an empty result set (i.e. zero rows). (Query took 0.0040 seconds.)
CREATE DATABASE IF NOT EXISTS assignment1b;
[ Edit inline ] [ Edit ] [ Create PHP code ]

Note: #1007 Can't create database 'assignment1b'; database exists

MySQL returned an empty result set (i.e. zero rows). (Query took 0.0006 seconds.)
USE assignment1b;
[ Edit inline ] [ Edit ] [ Create PHP code ]

MySQL returned an empty result set (i.e. zero rows). (Query took 0.0481 seconds.)
CREATE TABLE photos ( title VARCHAR(255), description VARCHAR(255), creation_date DATE, keywords VARCHAR(255), s3_reference VARCHAR(255) );
[ Edit inline ] [ Edit ] [ Create PHP code ]

```

1.5 Network ACL

Network ACL is an additional layer of the security group in which we can add more inbound rules and outbound rules for the ACL named “PublicSubnet2NACL”.

aws

Services

Search

[Alt+S]

N. Virginia

voclabs/user3485657=104991221@student.swin.edu.au @ 4866-8500...

VPC

VPC > Network ACLs > acl-038ca4e9979f7211c / PublicSubnet2NACL > Edit inbound rules

Edit inbound rules

Info

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

Rule number	Type	Protocol	Port range	Source	Allow/Deny	
1	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow	Remove
2	All ICMP - IPv4	ICMP (1)	All	10.0.4.0/24	Allow	Remove
3	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow	Remove
4	HTTPS (443)	TCP (6)	443	0.0.0.0/0	Allow	Remove
5	All TCP	TCP (6)	All	10.0.3.0/24	Allow	Remove
6	All TCP	TCP (6)	All	10.0.4.0/24	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	

Add new rule

Sort by rule number

Cancel

Preview changes

Save changes

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

aws

Services

Search

[Alt+S]

N. Virginia

voclabs/user3485657=104991221@student.swin.edu.au @ 4866-8500...

VPC

VPC > Network ACLs > acl-038ca4e9979f7211c / PublicSubnet2NACL > Edit outbound rules

Edit outbound rules

Info

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

Rule number	Type	Protocol	Port range	Destination	Allow/Deny	
1	All traffic	All	All	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	

Add new rule

Sort by rule number

Cancel

Preview changes

Save changes

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

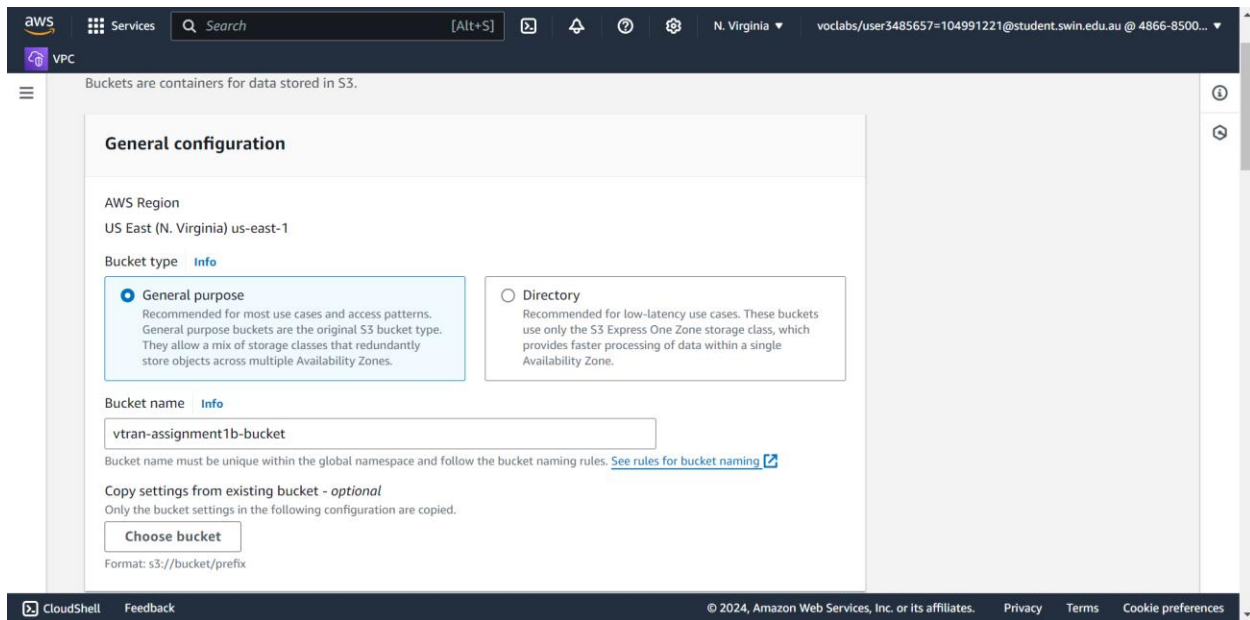
Terms

Cookie preferences

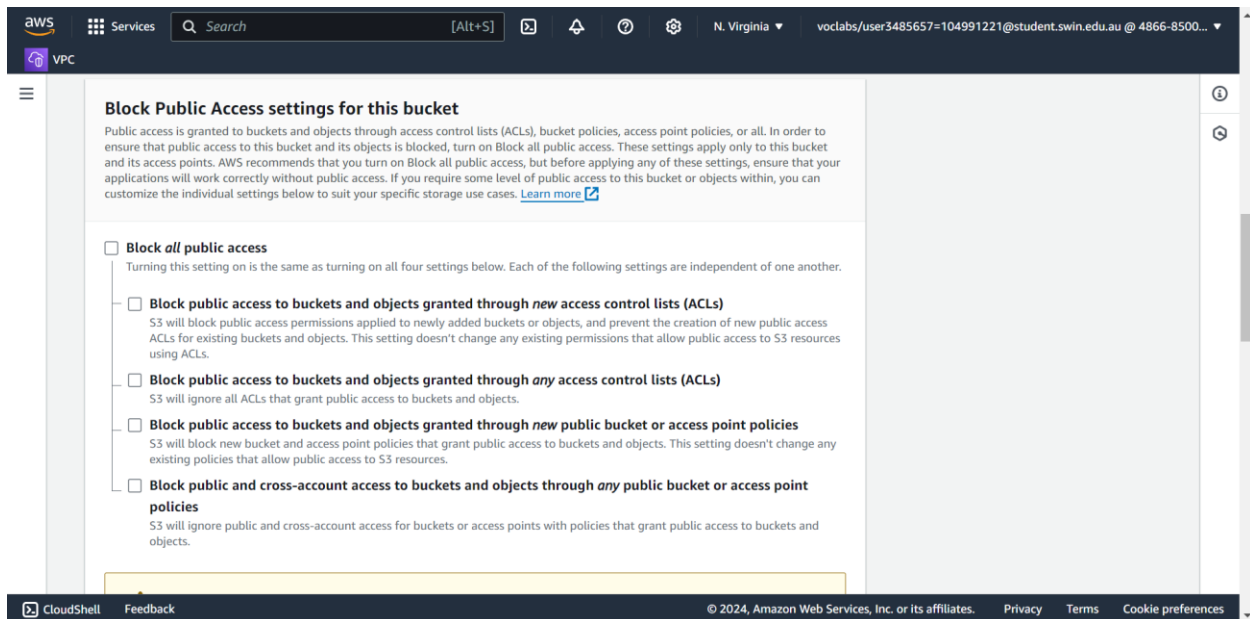
2. Functional Requirements of Photo Album website

2.1 Photo Storage

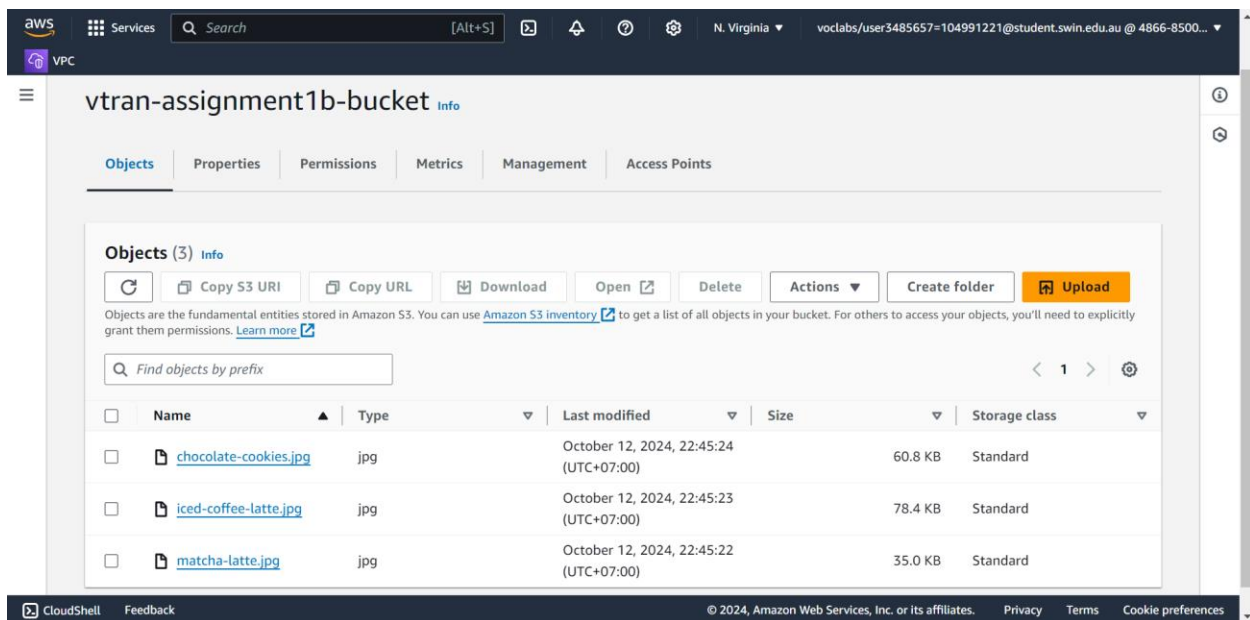
Create an S3 bucket for uploading resources.



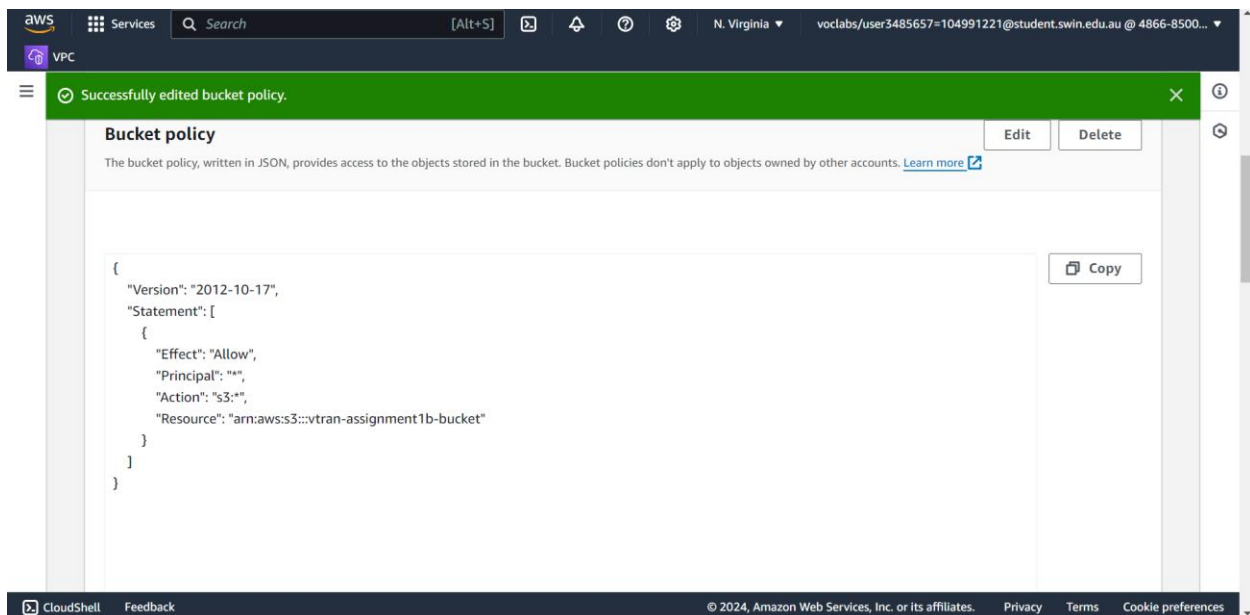
Uncheck the block all public access to the s3 bucket.



And manually upload some photos.

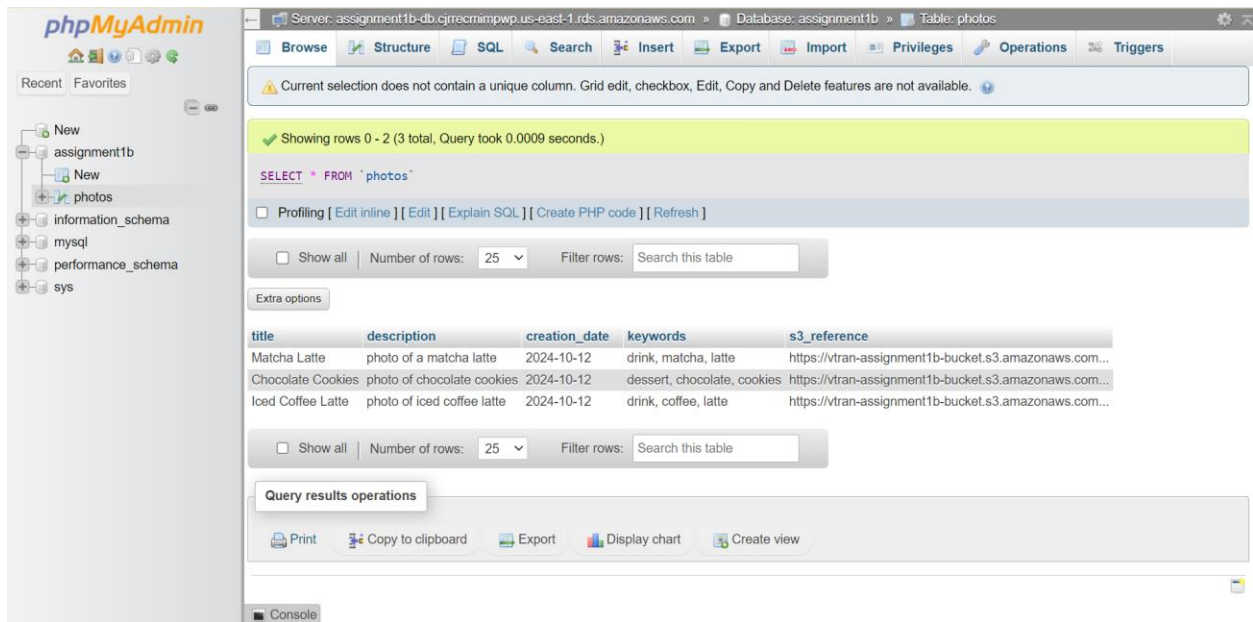


Bucket policy to enable public access.



2.2 Photo meta-data in the RDS Database

Populate the database table with some records.



2.3 Photo Album website functionality

Modify the constants.php using data from the S3 bucket and RDS database and transfer them using WinSCP.

```

35 // [ACTION REQUIRED] your full name
36 define('STUDENT_NAME', 'Tran Thien Thao Vy');
37 // [ACTION REQUIRED] your Student ID
38 define('STUDENT_ID', '104991221');
39 // [ACTION REQUIRED] your tutorial session
40 define('TUTORIAL_SESSION', 'Friday 07:15AM');
41
42 // [ACTION REQUIRED] name of the S3 bucket that stores images
43 define('BUCKET_NAME', 'vtran-assignment1b-bucket');
44 // [ACTION REQUIRED] region of the above bucket
45 define('REGION', 'us-east-1');
46 // no need to update this const
47 define('S3_BASE_URL', 'https://'.BUCKET_NAME.'.s3.amazonaws.com/');
48
49 // [ACTION REQUIRED] name of the database that stores photo meta-data (note that this is not the DB identifier of the RDS instance)
50 define('DB_NAME', 'assignment1b');
51 // [ACTION REQUIRED] endpoint of RDS instance
52 define('DB_ENDPOINT', 'assignment1b-db.cjrrccmimpwp.us-east-1.rds.amazonaws.com');
53 // [ACTION REQUIRED] username of your RDS instance
54 define('DB_USERNAME', 'admin');
55 // [ACTION REQUIRED] password of your RDS instance
56 define('DB_PWD', 'admin123');
57
58 // [ACTION REQUIRED] name of the DB table that stores photo's meta-data
59 define('DB_PHOTO_TABLE_NAME', 'photos');
60 // The table above has 5 columns:
61 // [ACTION REQUIRED] name of the column in the above table that stores photo's titles
62 define('DB_PHOTO_TITLE_COL_NAME', 'title');
63 // [ACTION REQUIRED] name of the column in the above table that stores photo's descriptions
64 define('DB_PHOTO_DESCRIPTION_COL_NAME', 'description');
65 // [ACTION REQUIRED] name of the column in the above table that stores photo's creation dates
66 define('DB_PHOTO_CREATIONDATE_COL_NAME', 'creation_date');
67 // [ACTION REQUIRED] name of the column in the above table that stores photo's keywords
68 define('DB_PHOTO_KEYWORDS_COL_NAME', 'keywords');
69 // [ACTION REQUIRED] name of the column in the above table that stores photo's links in S3
70 define('DB_PHOTO_S3REFERENCE_COL_NAME', 's3_reference');
71 >>

```

3. Testing

After the meta-data records has been populated into the phpMyAdmin table and php files has been transfer into the Web Instance.

The website is now accessible.

← → ↺

⚠ Not secure ec2-3-223-28-194.compute-1.amazonaws.com/cos20019/photoalbum/album.php




🔍 ☆ ⬇ 🌐 ⋮

Student name: Tran Thien Thao Vy

Student ID: 104991221

Tutorial session: Friday 07:15AM

Uploaded photos:

Photo	Name	Description	Creation date	Keywords
	Matcha Latte	photo of a matcha latte	2024-10-12	drink, matcha, latte
	Chocolate Cookies	photo of chocolate cookies	2024-10-12	dessert, chocolate, cookies
	Iced Coffee Latte	photo of iced coffee latte	2024-10-12	drink, coffee, latte

Test the Network ACL configuration by ssh into the Test Instance through the Bastion/Web Server host, and ping to the Web Server's IP address.

```
ec2-user@ip-10-0-4-100:~$ login as: ec2-user
* Authenticating with public key "assignment1b" from agent
Last login: Sun Oct 13 04:53:20 2024 from 171.225.192.74

Amazon Linux 2
AL2 End of Life is 2025-06-30.

A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-0-2-99 ~]$ ssh ec2-user@10.0.4.100
ec2-user@10.0.4.100:~$ ping 10.0.2.99
PING 10.0.2.99 (10.0.2.99) 56(84) bytes of data:
64 bytes from 10.0.2.99: icmp_seq=1 ttl=255 time=0.759 ms
64 bytes from 10.0.2.99: icmp_seq=2 ttl=255 time=1.50 ms
64 bytes from 10.0.2.99: icmp_seq=3 ttl=255 time=1.14 ms
64 bytes from 10.0.2.99: icmp_seq=4 ttl=255 time=1.47 ms
64 bytes from 10.0.2.99: icmp_seq=5 ttl=255 time=1.42 ms
64 bytes from 10.0.2.99: icmp_seq=6 ttl=255 time=0.955 ms
64 bytes from 10.0.2.99: icmp_seq=7 ttl=255 time=0.940 ms
64 bytes from 10.0.2.99: icmp_seq=8 ttl=255 time=1.04 ms
64 bytes from 10.0.2.99: icmp_seq=9 ttl=255 time=1.47 ms
64 bytes from 10.0.2.99: icmp_seq=10 ttl=255 time=1.52 ms
64 bytes from 10.0.2.99: icmp_seq=11 ttl=255 time=1.49 ms
64 bytes from 10.0.2.99: icmp_seq=12 ttl=255 time=1.95 ms
64 bytes from 10.0.2.99: icmp_seq=13 ttl=255 time=1.44 ms
```

4. Additional information

EC2 link into the Web Server: <http://ec2-3-223-28-194.compute-1.amazonaws.com/cos20019/photoalbum/album.php>

EC2 link to the phpMyAdmin console: <http://ec2-3-223-28-194.compute-1.amazonaws.com/phpmyadmin/>