

[To table of contents](#)

Student Name: Ta Quang Tung

Student ID: 104222196

Tutorial time: Saturday 3:00 P.M.

Date of submission: 18/6/23

# COS20019 – Cloud Computing Architecture - Assignment 1B

## Marking scheme

| Infrastructure Requirements  | Mark | Page   |
|--|------|--------|
| VPC with 2 public and 2 private subnets                                    | .5   | 7      |
| Correct Public and Private Routing tables with correct subnet associations | 1    | 8      |
| Security groups properly configured and attached.                          | 1    | 9-11   |
| Network ACL properly configured and attached                               | 1.5  | 30-32  |
| Correct Web server and Test instances running in correct subnets           | .5   | 13, 19 |
| Database schema as specified   | .5   | 29     |
| Database running in correct subnets  | 1    | 26     |
| S3 objects publicly accessible, using proper access policy                 | .5   | 36     |
| Functional Requirements  |      |        |
| album.php page displayed from EC2 Web server                               | 1    | 38     |
| Provided URL is persistent (Elastic IP Association)                        | .5   | 17     |
| Photos loaded from S3 with matching metadata from RDS                      | 1    | 38     |
| Web server instance reachable from Test instance via ICMP                  | 1    | 5      |
| Deductions   |      |        |
| Documentation not as specified or poorly presented (up to minus 20)        |      |        |
| Serious misconfigurations of AWS services being used (up to minus 20)      |      |        |

[To table of contents](#)

## Table of contents

|  |    |
|--|----|
| Table of contents .....                                | 2  |
| Website URL.....                                       | 3  |
| Data records.....                                      | 4  |
| Successful ping from TestInstance to WebServer .....   | 5  |
| 1 Infrastructure deployment .....                      | 6  |
| 1.1 Create a VPC.....                                  | 6  |
| 1.2 Create security groups .....                       | 9  |
| 1.3 Create EC2 instances .....                         | 12 |
| 1.3.1 Bastion/Web server instance.....                 | 12 |
| 1.3.2 Test instance .....                              | 18 |
| 1.4 Create RDS instance .....                          | 21 |
| 1.5 Network ACL.....                                   | 30 |
| 2 Functional requirements of Photo Album website ..... | 33 |
| 2.1 Photo storage (S3).....                            | 33 |
| 2.2 Photo meta-data in RDS Database.....               | 37 |
| 2.3 Photo Album website functionality .....            | 38 |

[To table of contents](#)

## Website URL

<http://ec2-44-216-98-59.compute-1.amazonaws.com/cos80001/photoalbum/album.php>

[To table of contents](#)

## Data records

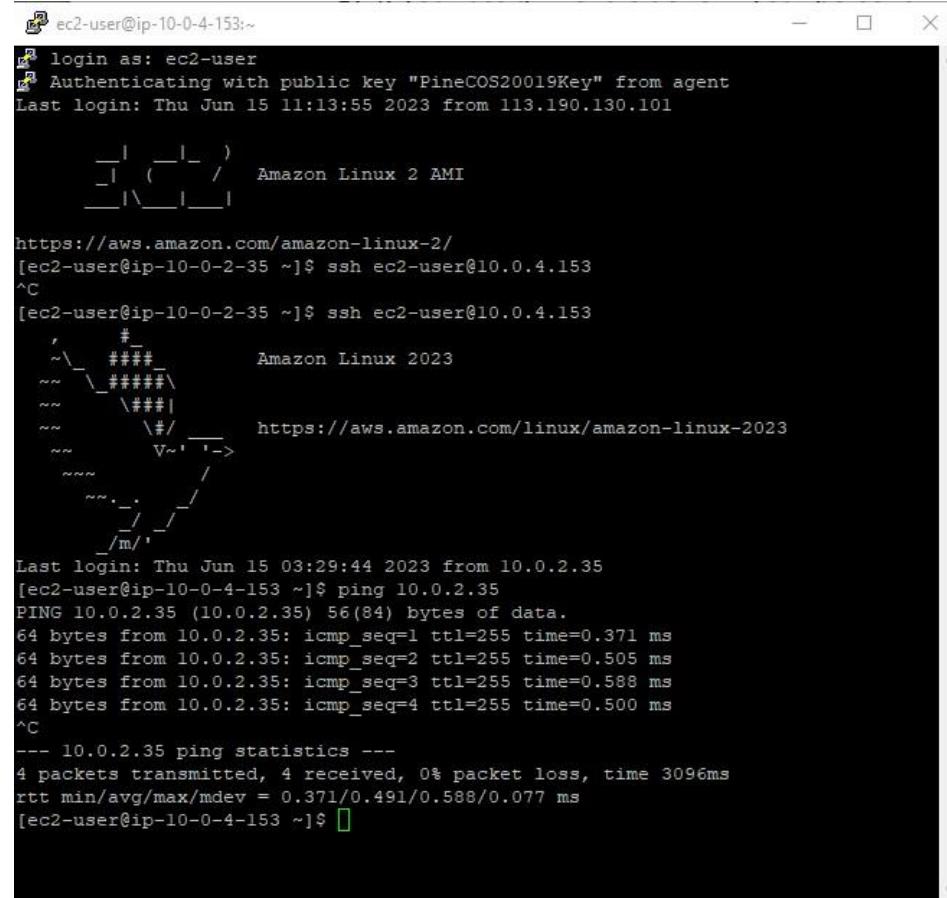
The screenshot shows the phpMyAdmin interface for a MySQL database named 'assignment1b'. The current table is 'photos'. The database structure on the left includes 'assignment1b', 'information\_schema', 'mysql', 'performance\_schema', and 'sys'. The 'photos' table has the following data:

|                          | id | title        | description                      | date       | keywords                                  | s3_photo  |
|--------------------------|----|--------------|----------------------------------|------------|---|---|
| <input type="checkbox"/> | 1  | Speak Now TV | Cover art for Speak Now TV album | 2023-06-15 | speak now, taylor's version, taylor swift | <a href="https://104222196photobucket.s3.amazonaws.com/Spea...">https://104222196photobucket.s3.amazonaws.com/Spea...</a> |
| <input type="checkbox"/> | 2  | Eras Tour    | Poster for the Eras tour.        | 2023-06-15 | eras tour, taylor swift                   | <a href="https://104222196photobucket.s3.amazonaws.com/ears...">https://104222196photobucket.s3.amazonaws.com/ears...</a> |

Two data records are present in the database.

[To table of contents](#)

## Successful ping from TestInstance to WebServer



```
ec2-user@ip-10-0-4-153:~$ login as: ec2-user
[ec2-user@ip-10-0-4-153 ~]$ Authenticating with public key "PineCOS20019Key" from agent
Last login: Thu Jun 15 11:13:55 2023 from 113.190.130.101
[ec2-user@ip-10-0-4-153 ~]$ https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-2-35 ~]$ ssh ec2-user@10.0.4.153
^C
[ec2-user@ip-10-0-2-35 ~]$ ssh ec2-user@10.0.4.153
[ec2-user@ip-10-0-2-35 ~]$ # Amazon Linux 2023
[ec2-user@ip-10-0-2-35 ~]$ https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-10-0-2-35 ~]$ Last login: Thu Jun 15 03:29:44 2023 from 10.0.2.35
[ec2-user@ip-10-0-4-153 ~]$ ping 10.0.2.35
PING 10.0.2.35 (10.0.2.35) 56(84) bytes of data.
64 bytes from 10.0.2.35: icmp_seq=1 ttl=255 time=0.371 ms
64 bytes from 10.0.2.35: icmp_seq=2 ttl=255 time=0.505 ms
64 bytes from 10.0.2.35: icmp_seq=3 ttl=255 time=0.588 ms
64 bytes from 10.0.2.35: icmp_seq=4 ttl=255 time=0.500 ms
^C
--- 10.0.2.35 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3096ms
rtt min/avg/max/mdev = 0.371/0.491/0.588/0.077 ms
[ec2-user@ip-10-0-4-153 ~]$
```

The Test Instance can ping the Web Server.

[To table of contents](#)

# 1 Infrastructure deployment

## 1.1 Create a VPC

The screenshot shows the AWS VPC 'Create VPC' wizard. On the left, the 'VPC settings' section includes fields for 'Name tag auto-generation' (set to 'Auto-generate' with 'TTaVPC'), 'IPv4 CIDR block' (set to '10.0.0.0/16'), and 'Number of Availability Zones (AZs)' (set to 1). On the right, the 'Preview' section shows the resulting VPC structure:

- VPC:** TTaVPC (highlighted by red arrow 1)
- Subnets (4):** us-east-1a (TTaVPC-subnet-public1-us-east-1a, TTaVPC-subnet-private1-us-east-1a), us-east-1b (TTaVPC-subnet-public2-us-east-1b, TTaVPC-subnet-private2-us-east-1b) (highlighted by red arrow 3)
- Route tables (3):** TTaVPC-rtb-public, TTaVPC-rtb-private1-us-east-1a, TTaVPC-rtb-private2-us-east-1b
- Network connections (2):** TTaVPC-igw, TTaVPC-vpc-s3

Create the VPC: (1) the name follows the correct pattern [FirstNameInitial][LastName]VPC, (2) set the CIDR block, (3) the subnet names indicate the region us-east-1

[To table of contents](#)

The screenshot shows the AWS VPC creation wizard. On the left, there are configuration sections:

- Number of public subnets**: Info. Number of public subnets: 2. A red arrow labeled '4' points to this field.
- Number of private subnets**: Info. Number of private subnets: 2. A red arrow labeled '5' points to this field.
- 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)A red bracket labeled '6' groups these four fields.
- 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. Options: 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 customize this policy at any time. Options: None, S3 Gateway.
- DNS options**: Info.

On the right, the **Preview** section shows the VPC structure:

- VPC**: TTaVPC-vpc
- Subnets (4)**: Subnets within this VPC
  - us-east-1a
    - TTaVPC-subnet-public1-us-east-1a
    - TTaVPC-subnet-private1-us-east-1a
  - us-east-1b
    - TTaVPC-subnet-public2-us-east-1b
    - TTaVPC-subnet-private2-us-east-1b
- Route tables (3)**: Route network traffic to resources
  - TTaVPC-rtb-public
  - TTaVPC-rtb-private1-us-east-1a
  - TTaVPC-rtb-private2-us-east-1b
- Network connections (2)**: Connections to other networks
  - TTaVPC-igw
  - TTaVPC-vpce-s3

At the bottom right, there is an **Activate Windows** message: "Go to Settings to activate Windows."

Create the VPC: (4) & (5) specify two public and two private subnets, (6) associate each subnet with their address blocks.

[To table of contents](#)

VPC dashboard X

EC2 Global View New

Filter by VPC: Select a VPC

Virtual private cloud

- Your VPCs New
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections

Security

- Network ACLs
- Security groups

DNS firewall

- Rule groups
- Domain lists

Network Firewall

- Firewalls

Actions ▾

VPC > Your VPCs > vpc-06f147235111aab42

## vpc-06f147235111aab42 / TTaVPC-vpc

Details Info

|   |  |   |   |
|---|--|---|---|
| VPC ID<br>vpc-06f147235111aab42           | State<br>Available   | DNS hostnames<br>Enabled                  | DNS resolution<br>Enabled                 |
| Tenancy<br>Default                        | DHCP option set<br>dopt-060cbe6736dbb6ddd                                | Main route table<br>rtb-042e9a32fa9395628 | Main network ACL<br>acl-0c56c02f40d2c1bb5 |
| Default VPC<br>No                         | IPv4 CIDR<br>10.0.0.0/16   | IPv6 pool<br>-                            | IPv6 CIDR (Network border group)<br>-     |
| Network Address Usage metrics<br>Disabled | Route 53 Resolver DNS Firewall rule groups<br>Failed to load rule groups | Owner ID<br>697351102859                  |   |

Resource map New CIDRs Flow logs Tags

Resource map Info

- VPC Show details Your AWS virtual network  
TTaVPC-vpc
- Subnets (4) Subnets within this VPC
  - us-east-1a
    - TTaVPC-subnet-public1-us-east-1a
    - TTaVPC-subnet-private1-us-east-1a
  - us-east-1b
    - TTaVPC-subnet-public2-us-east-1b
    - TTaVPC-subnet-private2-us-east-1b
- Route tables (4) Route network traffic to resources
  - TTaVPC-rtb-private2-us-east-1b
  - TTaVPC-rtb-private1-us-east-1a
  - rtb-042e9a32fa9395628
  - TTaVPC-rtb-public
- Network connections (2) Connections to other networks
  - TTaVPC-igw
  - TTaVPC-vpce-s3

Activate Windows  
Go to Settings to activate Windows.

CloudShell Feedback Language

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The VPC has been successfully created, and the subnets have been associated with the correct route tables.

[To table of contents](#)

## 1.2 Create security groups

The screenshot shows the AWS VPC Security Groups 'Create security group' interface. At the top, there's a navigation bar with the AWS logo, 'Services' (dropdown), a search bar ('Search [Alt+S]'), and account information ('N. Virginia' dropdown, 'voclabs/user2564760=104222196@student.swin.edu.au @ 6973-5110...'). Below the navigation is a breadcrumb trail: 'VPC > Security Groups > Create security group'. The main title is 'Create security group' with an 'Info' link. A descriptive text states: 'A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.' The 'Basic details' section contains fields for 'Security group name' (set to 'TestInstanceSG'), 'Description' (set to 'Security group for Test Instance'), and 'VPC' (set to 'vpc-06f147235111aab42'). The 'Inbound rules' section has tabs for 'Type' (set to 'All traffic'), 'Protocol' (set to 'All'), 'Port range' (set to 'All'), 'Source' (set to 'Anywhere'), and 'Description - optional' (empty). An 'Add rule' button is visible. The 'Outbound rules' section has tabs for 'Type' (empty), 'Protocol' (empty), 'Port range' (empty), 'Destination' (empty), and 'Description - optional' (empty). A note at the bottom right says 'Activate Windows Go to Settings to activate Windows.' The footer includes links for 'CloudShell', 'Feedback', 'Language', '© 2023, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

Create the Test Instance security group that allows traffic from all sources.

[To table of contents](#)

The screenshot shows the 'Create security group' interface in the AWS VPC service. The 'Basic details' section includes fields for 'Security group name' (WebServerSG), 'Description' (Security group for Web Server), and 'VPC' (vpc-06f14723511aab42). The 'Inbound rules' section contains three rules: 1) HTTP (TCP port 80) from Anywhere (0.0.0.0/0). 2) SSH (TCP port 22) from Anywhere (0.0.0.0/0). 3) All ICMP - IPv4 (ICMP All) from Custom (sg-0700699a7f001a29c). A red box highlights the 'Add rule' button at the bottom left of the inbound rules table.

**Basic details**

Security group name [Info](#)  
WebServerSG  
Name cannot be edited after creation.

Description [Info](#)  
Security group for Web Server

VPC [Info](#)  
vpc-06f14723511aab42

**Inbound rules** [Info](#)

| Type <a href="#">Info</a> | Protocol <a href="#">Info</a> | Port range <a href="#">Info</a> | Source <a href="#">Info</a>              | Description - optional <a href="#">Info</a> | Delete                 |
|---------------------------|-------------------------------|---------------------------------|--|---|------------------------|
| HTTP                      | TCP                           | 80                              | Anywhere- <a href="#">Info</a> 0.0.0.0/0 |   | <a href="#">Delete</a> |
| SSH                       | TCP                           | 22                              | Anywhere- <a href="#">Info</a> 0.0.0.0/0 |   | <a href="#">Delete</a> |
| All ICMP - IPv4           | ICMP                          | All                             | Custom sg-0700699a7f001a29c              |   | <a href="#">Delete</a> |

Add rule

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Create the Web Server security group that allows HTTP and SSH traffic from all sources, and ICMP traffic from Test Instance.

[To table of contents](#)

The screenshot shows the AWS VPC Create security group interface. In the 'Basic details' section, the security group name is set to 'DBServerSG' and the description is 'Security group for Database Server'. The VPC selected is 'vpc-06f14723511aab42'. In the 'Inbound rules' section, there is one rule: a MySQL/Aurora rule on port 3306 from a custom source. In the 'Outbound rules' section, there are no rules listed.

AWS Services Search [Alt+S] N. Virginia vocabs/user2564760=104222196@student.swin.edu.au @ 6973-5110... ▾ ⓘ

VPC > Security Groups > Create security group

## Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

### Basic details

Security group name Info  
DBServerSG  
Name cannot be edited after creation.

Description Info  
Security group for Database Server

VPC Info  
vpc-06f14723511aab42  X

### Inbound rules Info

| Type <small>Info</small> | Protocol <small>Info</small> | Port range <small>Info</small> | Source <small>Info</small> | Description - optional <small>Info</small>  |
|--------------------------|------------------------------|--------------------------------|----------------------------|---|
| MySQL/Aurora             | TCP                          | 3306                           | Custom                     | sg-0eaeb872831b070b6 <input type="text"/> X |

Add rule

### Outbound rules Info

| Type <small>Info</small> | Protocol <small>Info</small> | Port range <small>Info</small> | Destination <small>Info</small> | Description - optional <small>Info</small> |
|--------------------------|------------------------------|--------------------------------|---------------------------------|--|
|                          |                              |                                |                                 |  |

Activate Windows  
Go to Settings to activate Windows.

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Create the Database Server security group that allows MySQL traffic from the Web Server.

[To table of contents](#)

## 1.3 Create EC2 instances

### 1.3.1 Bastion/Web server instance

The screenshot shows the AWS EC2 instance creation process. On the left, the 'Name and tags' step is shown with a red arrow labeled '1' pointing to the 'Name' field containing 'Bastion/WebServer'. Below it, the 'Application and OS Images (Amazon Machine Image)' step is shown with a red arrow labeled '2' pointing to the 'Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type' option.

**Name and tags** [Info](#)

Name  Add additional tags

**Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Search our full catalog including 1000s of application and OS images

**Quick Start**

Amazon Linux macOS Ubuntu Windows Red Hat ... [Browse more AMIs](#) Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type [Free tier eligible](#)

ami-09988af04120b3591 (64-bit (x86)) / ami-013e77ebd63dc2197 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

**Summary**

Number of instances [Info](#) 1

Software Image (AMI)  
Amazon Linux 2 Kernel 5.10 AMI... [read more](#)  
ami-09988af04120b3591

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
WebServerSG

Storage (volumes)  
1 volume(s) - 8 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

[Cancel](#) [Launch instance](#) [Review commands](#)

Create the Bastion/Web Server instance from Amazon Linux 2 AMI (HVM), SSD Volume Type

## [To table of contents](#)

The screenshot shows the AWS CloudFormation console during the creation of a new stack. The left pane displays the configuration steps:

- Step 1: Set instance type**: The instance type is set to **t2.micro**. A red arrow labeled **3** points to this selection.
- Step 2: Set key pair (login)**: The key pair name is **PineCOS2019Key**. A red arrow labeled **4** points to this field.
- Step 3: Set network settings**: The VPC is **vpc-06f147235111aab42 (TTaVPC-vpc)**, and the subnet is **subnet-04e2ab8b0d2c14db2**. A red arrow labeled **5** points to the subnet selection.

The right pane shows the **Summary** of the stack configuration, including:

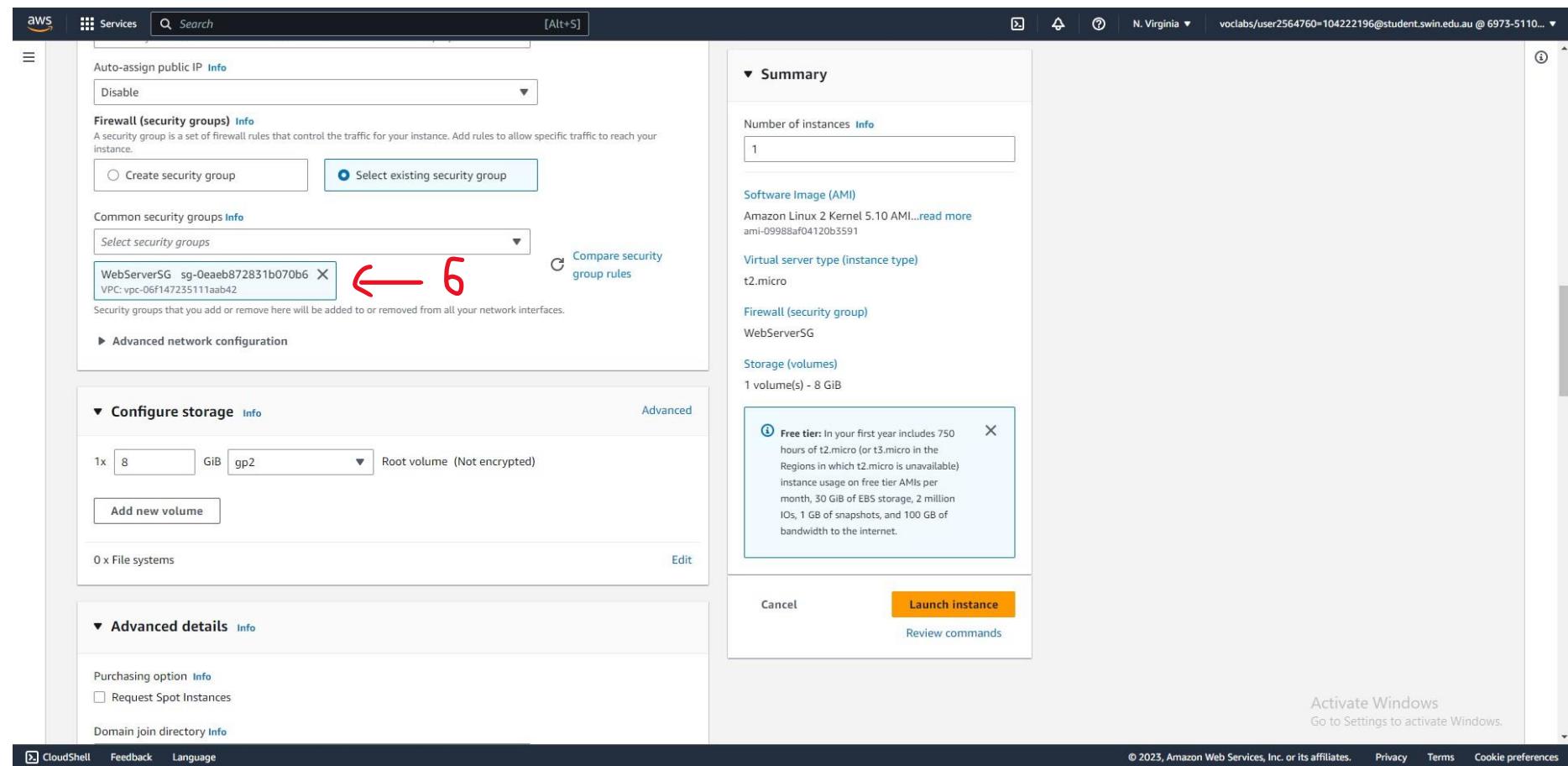
- Number of instances**: 1
- Software Image (AMI)**: Amazon Linux 2 Kernel 5.10 AMI
- Virtual server type (instance type)**: t2.micro
- Firewall (security group)**: WebServerSG
- Storage (volumes)**: 1 volume(s) - 8 GiB

A callout box provides information about the **Free tier**:

- In your first year includes 750 hours of t2.micro (or t3.micro in the Regions where t2.micro is unavailable)
- Instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

At the bottom of the summary pane, there are **Cancel**, **Launch instance** (highlighted in orange), and **Review commands** buttons.

Create the Bastion/Web Server instance: (3) set the type to t2.micro, (4) assign a key pair, (5) place the instance in public subnet 2.

[To table of contents](#)

The screenshot shows the AWS CloudFormation Create New Stack wizard at Step 6: Set instance details. The 'Security group' section is highlighted, showing a dropdown menu with 'WebServerSG' selected. A red arrow points to this dropdown. The 'Configure storage' and 'Advanced details' sections are also visible.

**Security group (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-0eaeb872831b070b6 X VPC: vpc-06f14723511aab42 ← 6 Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

**Configure storage Info** Advanced

1x 8 GiB gp2 Root volume (Not encrypted)

Add new volume

0 x File systems Edit

**Advanced details Info**

Purchasing option Info  
 Request Spot Instances

Domain join directory Info

Summary

Number of instances Info  
1

Software Image (AMI)  
Amazon Linux 2 Kernel 5.10 AMI...read more  
ami-09988af04120b3591

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
WebServerSG

Storage (volumes)  
1 volume(s) - 8 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch instance Review commands

Activate Windows  
Go to Settings to activate Windows.

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Create the Bastion/Web Server instance: (6) assign the web server security group.

## [To table of contents](#)

The screenshot shows the AWS CloudFormation console during the creation of a new stack. The current step is 'Configure instance settings'. On the left, there's a large text area for 'User data - optional' containing a bash script to install Apache, MySQL, and PHP. A red arrow points from the text 'Create the Bastion/Web Server instance: (7) configure a user data script to install the Apache server.' to this script. On the right, the 'Summary' section shows details like the AMI, instance type (t2.micro), and storage. At the bottom right of the summary box is a prominent orange 'Launch instance' button.

The user data script content is:

```
#!/bin/bash
yum update -y
amazon-linux-extras install -y lamp-mariadb10.2-php7.2
service httpd start
yum install -y httpd mariadb-server php-mbstring php-xml
systemctl start httpd
systemctl enable httpd
usermod -a -G apache ec2-user
chown -R ec2-user:apache /var/www
chmod 2775 /var/www
find /var/www -type d -exec sudo chmod 2775 {} \;
find /var/www -type f -exec sudo chmod 0664 {} \;
echo "<?php echo '<h2>Welcome to COS80001. Installed PHP version:' . phpversion() . '</h2>'; ?>" > /var/www/html/phpinfo.php
```

Create the Bastion/Web Server instance: (7) configure a user data script to install the Apache server.

## [To table of contents](#)

The screenshot shows the AWS Management Console interface for allocating an Elastic IP address. The top navigation bar includes the AWS logo, 'Services' dropdown, a search bar with placeholder '[Alt+S]', and account information 'voclabs/user2564760=104222196@student.swin.edu.au @ 6973-5110... ▾'. Below the navigation is a breadcrumb trail: EC2 > Elastic IP addresses > Allocate Elastic IP address. The main content area is titled 'Allocate Elastic IP address' with an 'Info' link. A sub-section titled 'Elastic IP address settings' also has an 'Info' link. Under 'Network Border Group' (Info), a search bar shows 'us-east-1'. The 'Public IPv4 address pool' section contains three options: 'Amazon's pool of IPv4 addresses' (selected, indicated by a blue dot), 'Public IPv4 address that you bring to your AWS account (option disabled because no pools found)' (disabled, indicated by a grey dot), and 'Customer owned pool of IPv4 addresses (option disabled because no customer owned pools found)' (disabled, indicated by a grey dot). Below this is a section for 'Global static IP addresses' with a note about AWS Global Accelerator. A 'Create accelerator' button is present. The 'Tags - optional' section explains what tags are and notes that none are associated with the resource. An 'Add new tag' button is available, with a note that up to 50 more tags can be added. At the bottom are 'Cancel' and 'Allocate' buttons, with the 'Allocate' button highlighted in orange. A watermark for 'Activate Windows' is visible on the right.

Allocate an Elastic IP address in the us-east-1 region.

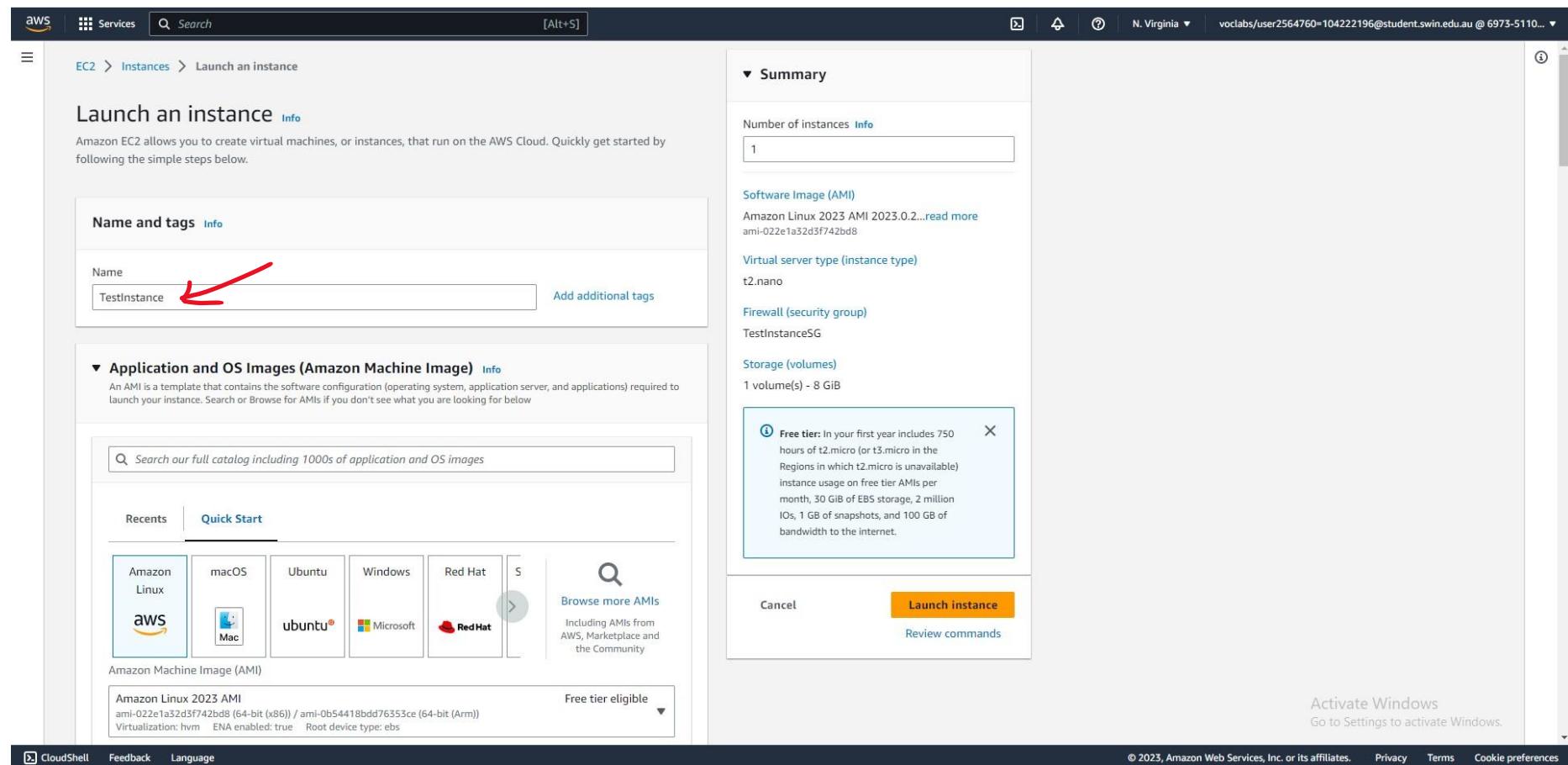
[To table of contents](#)

The screenshot shows the AWS EC2 console with the title "Associate Elastic IP address". The URL in the address bar is "EC2 > Elastic IP addresses > Associate Elastic IP address". The main content area is titled "Elastic IP address: 44.216.98.59". It asks to choose an instance or network interface to associate with the Elastic IP address. A note states that if an instance already has an associated Elastic IP, it will be disassociated. The "Instance" radio button is selected. Below it, a note says that if no private IP is specified, the Elastic IP will be associated with the primary private IP address. The "Instance" dropdown field contains "i-0a7a225dd416afbd5", which is highlighted with a red arrow. The "Private IP address" field is empty and labeled "Choose a private IP address". Under "Reassociation", there is a checkbox "Allow this Elastic IP address to be reassigned". At the bottom are "Cancel" and "Associate" buttons. A watermark for "Activate Windows" is visible on the right.

Assign the new Elastic IP address to the Bastion/Web Server instance.

[To table of contents](#)

### 1.3.2 Test instance



The screenshot shows the AWS EC2 'Launch an instance' wizard. In the 'Name and tags' section, the 'Name' field contains 'TestInstance' with a red arrow pointing to it. The 'Software Image (AMI)' section shows 'Amazon Linux 2023 AMI 2023.0.2...' and its ID 'ami-022e1a32d5f742bd8'. The 'Virtual server type (instance type)' is set to 't2.nano'. Under 'Firewall (security group)', it says 'TestInstanceSG'. In the 'Storage (volumes)' section, there is '1 volume(s) - 8 GiB'. A tooltip for the 'Free tier' explains the included resources: 750 hours of t2.micro (or t3.micro in regions where t2.micro is unavailable), instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. At the bottom right of the wizard, there are 'Cancel', 'Launch instance' (in orange), and 'Review commands' buttons.

Create the Test Instance.

[To table of contents](#)

The screenshot shows the AWS Lambda 'Create function' wizard. The left pane contains the following configuration steps:

- Key pair (login) Info**: A dropdown menu for selecting a key pair, with "PineCOS20019Key" selected. A red arrow points to this field.
- Network settings Info**:
  - VPC - required**: A dropdown menu for selecting a VPC, with "vpc-06f147235111aab42 (TTaVPC-vpc)" selected. A red arrow points to this field.
  - Subnet Info**: A dropdown menu for selecting a subnet, with "subnet-03eb538a54da1cc6e TTaVPC-subnet-private2-us-east-1b" selected. A red arrow points to this field.
  - Create new subnet**: A button to create a new subnet.
  - Auto-assign public IP**: A dropdown menu set to "Disable".
  - Firewall (security groups)**: A section with "TestInstanceSG" selected. A red arrow points to this field.
  - Common security groups**: A dropdown menu for selecting common security groups, with "TestInstanceSG sg-0700699a7f001a29c" selected. A red arrow points to this field.
  - Compare security group rules**: A link to compare security group rules.
- Advanced network configuration**: A link to advanced network configuration options.

The right pane displays the **Summary** of the function configuration:

- Number of instances**: 1
- Software Image (AMI)**: Amazon Linux 2023 AMI 2023.0.2...read more
- Virtual server type (instance type)**: t2.nano
- Firewall (security group)**: TestInstanceSG
- Storage (volumes)**: 1 volume(s) - 8 GiB
- Free tier**: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions where t2.micro is unavailable). Instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

At the bottom right of the summary pane are the **Launch instance** and **Review commands** buttons.

At the very bottom of the page, there are links for CloudShell, Feedback, Language, Activate Windows, and various AWS terms and conditions.

Create the Test Instance: assign a key pair, place the instance in private subnet 2, and assign the Test Instance security group.

[To table of contents](#)

```
ec2-user@ip-10-0-4-153:~  
login as: ec2-user  
Authenticating with public key "PineCOS20019Key" from agent  
Last login: Thu Jun 15 11:13:55 2023 from 113.190.130.101  
Amazon Linux 2 AMI  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-0-2-35 ~]$ ssh ec2-user@10.0.4.153  
^C  
[ec2-user@ip-10-0-2-35 ~]$ ssh ec2-user@10.0.4.153 ← 1  
Amazon Linux 2023  
https://aws.amazon.com/linux/amazon-linux-2023  
  
Last login: Thu Jun 15 03:29:44 2023 from 10.0.2.35 ← 2  
[ec2-user@ip-10-0-4-153 ~]$ ping 10.0.2.35  
PING 10.0.2.35 (10.0.2.35) 56(84) bytes of data.  
64 bytes from 10.0.2.35: icmp_seq=1 ttl=255 time=0.371 ms  
64 bytes from 10.0.2.35: icmp_seq=2 ttl=255 time=0.505 ms  
64 bytes from 10.0.2.35: icmp_seq=3 ttl=255 time=0.588 ms  
64 bytes from 10.0.2.35: icmp_seq=4 ttl=255 time=0.500 ms  
^C  
--- 10.0.2.35 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3096ms  
rtt min/avg/max/mdev = 0.371/0.491/0.588/0.077 ms  
[ec2-user@ip-10-0-4-153 ~]$
```

(1) SSH into the Test instance from the Web Server instance, then (2) ping the Web Server's private Ipv4 address.

[To table of contents](#)

## 1.4 Create RDS instance

The screenshot shows the AWS RDS Subnet groups interface. On the left, a sidebar lists various RDS services: Dashboard, Databases, Query Editor, Performance insights, Snapshots, Exports in Amazon S3, Automated backups, Reserved instances, and Proxies. Under 'Subnet groups', it lists Parameter groups, Option groups, Custom engine versions, Events, Event subscriptions, Recommendations (with a '2' notification), and Certificate update.

The main content area is titled 'Create DB subnet group'. It provides instructions: 'To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.' The 'Subnet group details' section contains fields for 'Name' (set to 'PhotoDBGroup') and 'Description' (set to 'Private subnet group for photo database'). The 'VPC' section shows a dropdown menu with 'TTaVPC-vpc (vpc-06f14723511aab42)' selected. The 'Add subnets' section includes an 'Availability Zones' dropdown and a list of selected subnets: 'us-east-1a' and 'us-east-1b'. A note says 'Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.' At the bottom right, there's an 'Activate Windows' message: 'Activate Windows Go to Settings to activate Windows.'

Create a DB subnet group in the VPC that spans both Availability Zones.

[To table of contents](#)

The screenshot shows the 'Add subnets' configuration page for an Amazon RDS subnet group. On the left, the 'Subnet groups' section is expanded, showing options like Parameter groups, Option groups, and Custom engine versions. The main form has two sections: 'Availability Zones' (with a dropdown for 'Choose an availability zone' and two selected zones: 'us-east-1a' and 'us-east-1b') and 'Subnets' (with a dropdown for 'Select subnets' and two selected subnets: 'subnet-0c4de83c7783721dc (10.0.3.0/24)' and 'subnet-03eb538a54da1cc6e (10.0.4.0/24)'). A note below the subnets says: 'For Multi-AZ DB clusters, you must select 3 subnets in 3 different Availability Zones.' A red bracket and arrow point to the 'Subnets selected (2)' section at the bottom, which lists the two chosen subnets with their availability zones and CIDR blocks.

| Availability zone | Subnet ID                | CIDR block  |
|-------------------|--------------------------|-------------|
| us-east-1a        | subnet-0c4de83c7783721dc | 10.0.3.0/24 |
| us-east-1b        | subnet-03eb538a54da1cc6e | 10.0.4.0/24 |

Cancel Create

Assign both private subnets to the subnet group.

[To table of contents](#)

The screenshot shows the AWS RDS 'Create database' page. At the top, there are tabs for 'Services' and 'Search'. Below the tabs, the URL 'voclabs/user2564760=104222196@student.swin.edu.au @ 6973-5110...' is visible. The main content area is titled 'Create database' and contains two sections: 'Choose a database creation method' and 'Engine options'. In the 'Choose a database creation method' section, 'Standard create' is selected. In the 'Engine options' section, 'MySQL' is selected. A large red arrow points to the 'MySQL' icon. The bottom right corner of the page has a watermark for 'Activate Windows'.

Create the RDS instance: (1) choose MySQL.

## [To table of contents](#)

The screenshot shows the AWS RDS instance creation process. Step 2 is highlighted with a red arrow pointing to the 'Engine Version' dropdown menu, which is set to 'MySQL 8.0.28'. Step 3 is highlighted with a red arrow pointing to the 'Templates' section, where the 'Free tier' option is selected.

Review the [Known issues/limitations](#) to learn about potential compatibility issues with specific database versions.

Hide filters

Show versions that support the Multi-AZ DB cluster [Info](#)  
Create a Multi-AZ DB cluster with one primary DB instance and two readable standby DB instances. Multi-AZ DB clusters provide up to 2x faster transaction commit latency and automatic failover in typically under 35 seconds.

Show versions that support the Amazon RDS Optimized Writes [Info](#)  
Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.

Engine Version

MySQL 8.0.28

**Templates**  
Choose a sample template to meet your use case.

Production  
Use defaults for high availability and fast, consistent performance.

Dev/Test  
This instance is intended for development use outside of a production environment.

Free tier  
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. [Info](#)

**Availability and durability**

Deployment options [Info](#)  
The deployment options below are limited to those supported by the engine you selected above.

Multi-AZ DB Cluster - [new](#)  
Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.

Multi-AZ DB instance (not supported for Multi-AZ DB cluster snapshot)  
Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.

Activate Windows  
Go to Settings to activate Windows.

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Create the RDS instance: (2) choose engine version 8.0.28, (3) choose the free tier template.

[To table of contents](#)

The screenshot shows the 'Settings' tab of the AWS RDS instance creation wizard. The 'DB instance identifier' is set to 'photoalbumdb'. Under 'Credentials Settings', the 'Master username' is 'admin' (highlighted with a red arrow). A note indicates that master user credentials in Secrets Manager are not supported. Below this, there are fields for 'Master password' and 'Confirm master password', both containing masked values (\*\*\*\*\*). A large red number '4' is overlaid on the right side of the page, pointing to the credential fields.

Activate Windows  
Go to Settings to activate Windows.

CloudShell   Feedback   Language

© 2023, Amazon Web Services, Inc. or its affiliates.   Privacy   Terms   Cookie preferences

Create the RDS instance: (4) configure DB credentials.

[To table of contents](#)

The screenshot shows the 'Connectivity' section of the AWS RDS instance creation wizard. It includes fields for Compute resource, Network type, VPC, DB subnet group, and Public access.

- Compute resource:** Options are "Don't connect to an EC2 compute resource" (selected) and "Connect to an EC2 compute resource".
- Network type:** Options are "IPv4" (selected) and "Dual-stack mode".
- Virtual private cloud (VPC):** A dropdown menu shows "TTaVPC-vpc (vpc-06f14723511aab42)" with a red arrow labeled "5" pointing to it. Below it, it says "4 Subnets, 2 Availability Zones".
- DB subnet group:** A dropdown menu shows "photodbgroup" with a red arrow labeled "6" pointing to it. Below it, it says "2 Subnets, 2 Availability Zones".
- Public access:** Options are "Yes" and "No" (selected). Below "Yes", it says "RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database." Below "No", it says "RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database." A red arrow labeled "7" points to the "No" option.

At the bottom right, there is an "Activate Windows" link and footer links for CloudShell, Feedback, Language, © 2023, Privacy, Terms, and Cookie preferences.

Create the RDS instance: (5) place the DB in the VPC, (6) assign it the private subnet group, (7) block public access.

[To table of contents](#)

The screenshot shows the AWS RDS instance creation wizard. The current step is 'Configure your new DB instance'. A red arrow labeled '8' points to the 'Existing VPC security groups' dropdown, which contains 'DBServerSG'. Another red arrow labeled '9' points to the 'Availability Zone' dropdown, which contains 'us-east-1a'. Other visible sections include 'Public access' (set to 'No'), 'VPC security group (firewall)', 'RDS Proxy' (disabled), and 'Certificate authority - optional' (set to 'rds-ca-2019 (default)').

Create the RDS instance: (8) assign the DB Server security group, (9) choose Availability Zone A.

[To table of contents](#)

The screenshot shows the AWS RDS console for a MySQL database instance named "photoalbumdb".

**Summary:**

|                               |                                   |                           |                           |
|-------------------------------|-----------------------------------|---------------------------|---------------------------|
| DB identifier<br>photoalbumdb | CPU<br>2.88%                      | Status<br>Available       | Class<br>db.t3.micro      |
| Role<br>Instance              | Current activity<br>0 Connections | Engine<br>MySQL Community | Region & AZ<br>us-east-1a |

**Connectivity & security:**

|   |   |   |
|---|---|---|
| Endpoint & port   | Networking  | Security  |
| Endpoint<br>photoalbumdb.c6w0siafkfbt.us-east-1.rds.amazonaws.com | Availability Zone<br>us-east-1a                                 | VPC security groups<br>DBServerSG (sg-0deb169d07e4cfa6c)<br>Active            |
| Port<br>3306  | VPC<br>TTaVPC-vpc (vpc-06f14723511aab42)                        | Publicly accessible<br>No   |
|   | Subnet group<br>photodbgroup                                    | Certificate authority<br>Info<br>rds-ca-2019                                  |
|   | Subnets<br>subnet-03eb538a54da1cc6e<br>subnet-0c4de83c7783721dc | Certificate authority date<br>August 23, 2024, 00:08 (UTC+07:00)              |
|   | Network type<br>IPv4  | DB instance certificate expiration date<br>August 23, 2024, 00:08 (UTC+07:00) |

**Actions:** Modify, Actions ▾

**Footer:** CloudShell, Feedback, Language, © 2023, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, Cookie preferences.

The RDS instance has successfully been created.

[To table of contents](#)

The screenshot shows the phpMyAdmin interface for a database named 'assignment1b'. The 'photos' table is selected. The table structure includes columns: id (int, primary key, auto-increment), title (varchar(255)), description (varchar(255)), date (date), keywords (varchar(255)), and s3\_photo (varchar(255)). An index named 'PRIMARY' is defined on the 'id' column. The 'Information' tab displays space usage (16 KIB) and row statistics (dynamic format, utf8mb4\_0900\_ai\_ci collation). A red arrow points to the 'PRIMARY' index definition.

After setting up phpMyAdmin on the Bastion/Web Server instance, access the database server and create a table named 'photos' with the above structure. The SQL statement to create the table is:

```
CREATE TABLE photos (
    id INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
    title VARCHAR(255),
    description VARCHAR(255),
    date DATE,
    keywords VARCHAR(255),
    s3_photo VARCHAR(255)
);
```

[To table of contents](#)

## 1.5 Network ACL

The screenshot shows the AWS VPC Network ACLs page. On the left, there's a navigation sidebar with options like VPC dashboard, EC2 Global View, Filter by VPC, Virtual private cloud, Security, DNS firewall, and Network Firewall. The main area displays a table of Network ACLs with columns for Name, Network ACL ID, Associated with, Default, VPC ID, Inbound rules count, and Outbound rules count. Three entries are listed: one with 3 Subnets, one with 6 Subnets, and one selected named 'PublicSubnet2NACL' which has 7 Inbound rules. Below this, a detailed view of 'PublicSubnet2NACL' shows tabs for Details, Inbound rules (selected), Outbound rules, Subnet associations, and Tags. A message says 'You can now check network connectivity with Reachability Analyzer' with a 'Run Reachability Analyzer' button. The 'Inbound rules (7)' table lists rules for HTTP, HTTPS, SSH, ICMP, TCP, and All traffic, all set to Allow except for the last rule which is Deny. At the bottom, there are links for Activate Windows, CloudShell, Feedback, Language, and a footer with copyright information.

| Name  | Network ACL ID        | Associated with                              | Default | VPC ID                            | Inbound rules count | Outbound rules count |
|---|-----------------------|--|---------|-----------------------------------|---------------------|----------------------|
| -   | acl-0c56c02f40d2c1bb5 | 3 Subnets                                    | Yes     | vpc-06f14723511aab42 / TTaVPC-vpc | 2 Inbound rules     | 2 Outbound rules     |
| -   | acl-0af44672f61c1a3a6 | 6 Subnets                                    | Yes     | vpc-0da4efcd8e406d2a5             | 2 Inbound rules     | 2 Outbound rules     |
| <input checked="" type="checkbox"/> PublicSubnet2NACL | acl-0409d8ea71b1682ec | subnet-04e2ab8b0d2c14db2 / TTaVPC-subnet-... | No      | vpc-06f14723511aab42 / TTaVPC-vpc | 7 Inbound rules     | 2 Outbound rules     |

**Inbound rules (7)**

| Rule number | Type            | Protocol | Port range | Source      | Allow/Deny |
|-------------|-----------------|----------|------------|-------------|------------|
| 1           | HTTP (80)       | TCP (6)  | 80         | 0.0.0.0/0   | Allow      |
| 2           | HTTPS (443)     | TCP (6)  | 443        | 0.0.0.0/0   | Allow      |
| 3           | SSH (22)        | TCP (6)  | 22         | 0.0.0.0/0   | Allow      |
| 5           | All ICMP - IPv4 | ICMP (1) | All        | 10.0.4.0/24 | Allow      |
| 6           | All TCP         | TCP (6)  | All        | 10.0.3.0/24 | Allow      |
| 7           | All TCP         | TCP (6)  | All        | 10.0.4.0/24 | Allow      |
| *           | All traffic     | All      | All        | 0.0.0.0/0   | Deny       |

Create the Network ACL for public subnet 2 with the above inbound rules.

[To table of contents](#)

Rule 1, 2, 3 allow HTTP, HTTPS, and SSH traffic from anywhere to reach the subnet.

Rule 5 allows ICMP traffic from the Test Instance to reach the subnet.

Rule 6 allows all TCP traffic from the Database Server to reach the subnet. This lets the database reach the web server.

Rule 7 allows all TCP traffic from the Test Instance to reach the subnet. This lets the Test Instance reach the bastion/web server instance.

[To table of contents](#)

The screenshot shows the AWS VPC Network ACLs page. On the left, a navigation sidebar lists various VPC-related services and security options like Network ACLs, DNS firewall, and Network Firewall. The main content area displays 'Network ACLs (1/3)' with a table showing three entries:

| Name                  | Network ACL ID        | Associated with                              | Default                           | VPC ID                            | Inbound rules count | Outbound rules count |
|-----------------------|-----------------------|--|-----------------------------------|-----------------------------------|---------------------|----------------------|
| acl-0c56c02f40d2c1bb5 | 3 Subnets             | Yes  | vpc-06f14723511aab42 / TTaVPC-vpc | 2 Inbound rules                   | 2 Outbound rules    |                      |
| acl-0af44672f61c1a3a6 | 6 Subnets             | Yes  | vpc-0da4efcd8e406d2a5             | 2 Inbound rules                   | 2 Outbound rules    |                      |
| PublicSubnet2NACL     | acl-0409d8ea71b1682ec | subnet-04e2ab8b0d2c14db2 / TTaVPC-subnet-... | No                                | vpc-06f14723511aab42 / TTaVPC-vpc | 7 Inbound rules     | 2 Outbound rules     |

For the selected 'PublicSubnet2NACL', the 'Outbound rules' tab is active, showing the following configuration:

| Rule number | Type        | Protocol | Port range | Destination | Allow/Deny                                |
|-------------|-------------|----------|------------|-------------|---|
| 1           | All traffic | All      | All        | 0.0.0.0/0   | <input checked="" type="checkbox"/> Allow |
| *           | All traffic | All      | All        | 0.0.0.0/0   | <input type="checkbox"/> Deny             |

A message at the bottom states: 'You can now check network connectivity with Reachability Analyzer' with a 'Run Reachability Analyzer' button.

At the bottom right, there are links to 'Activate Windows', 'Go to Settings to activate Windows.', and standard footer links for CloudShell, Feedback, Language, Copyright (© 2023), Privacy, Terms, and Cookie preferences.

Allow all outbound traffic because this does not affect security.

[To table of contents](#)

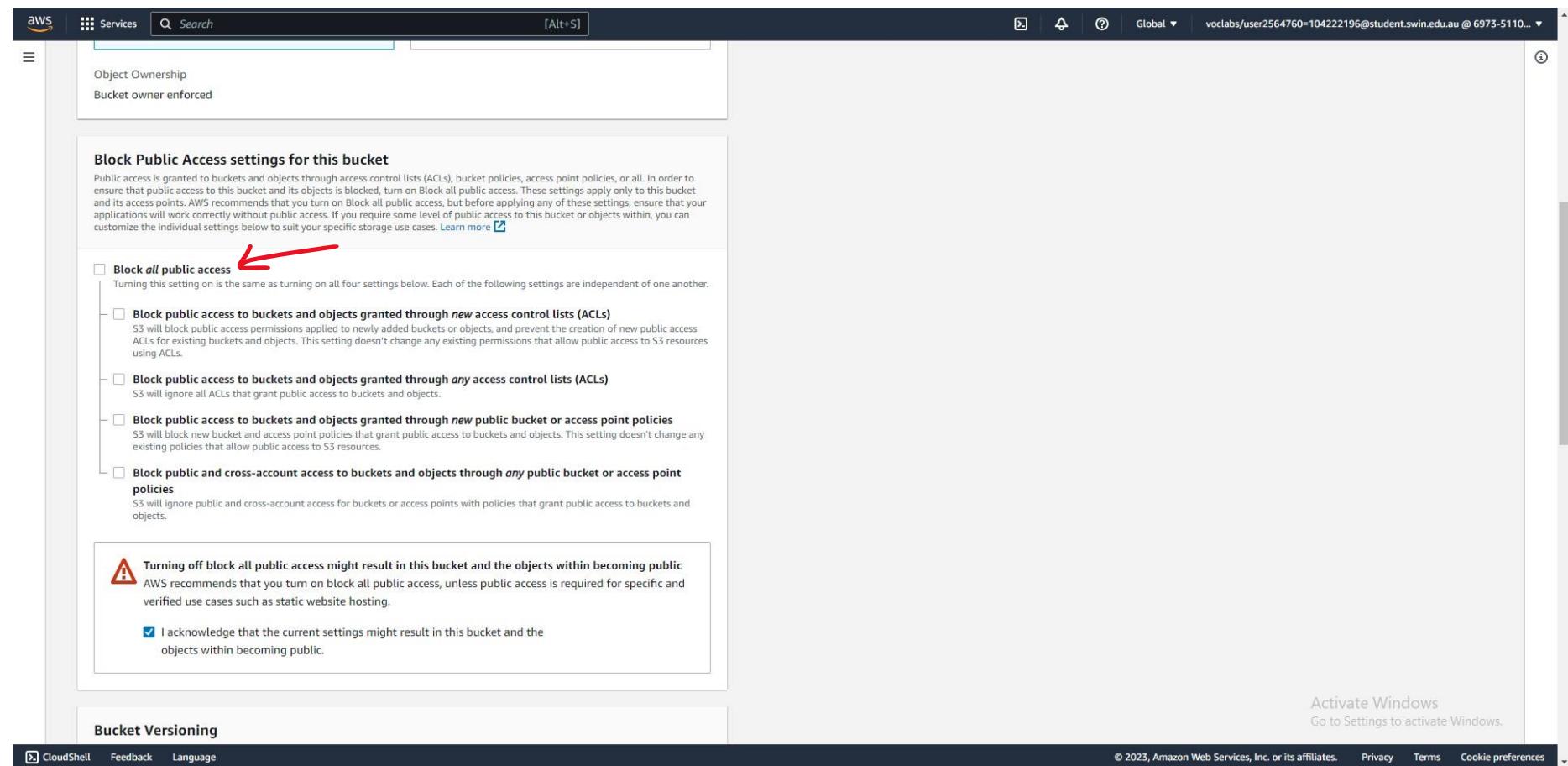
## 2 Functional requirements of Photo Album website

### 2.1 Photo storage (S3)

The screenshot shows the 'Create bucket' wizard in the AWS Management Console. The top navigation bar includes the AWS logo, 'Services' (with 'Amazon S3' selected), a search bar, and global settings. The main page title is 'Create bucket' with an 'Info' link. Below it, a note says 'Buckets are containers for data stored in S3. Learn more'. The 'General configuration' section contains fields for 'Bucket name' (set to '104222196photobucket') and 'AWS Region' (set to 'US East (N. Virginia) us-east-1'). A note about copying settings from existing buckets is present, with a 'Choose bucket' button. The 'Object Ownership' section shows 'ACLs disabled (recommended)' is selected, with a note that all objects are owned by the account. It also shows the option for 'ACLs enabled', which allows other accounts to own objects. The 'Block Public Access settings for this bucket' section is partially visible at the bottom.

Create an S3 bucket in the us-east-1 region to store photos.

[To table of contents](#)



The screenshot shows the 'Block Public Access settings for this bucket' section of the AWS S3 console. At the top, there's a note about public access being granted through various mechanisms like ACLs, bucket policies, and access point policies. Below this, the 'Block all public access' checkbox is highlighted with a red arrow. This checkbox is described as turning on all four settings below. The other four settings are listed as checkboxes: 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. A warning message in a box states that turning off block all public access might result in the bucket and its objects becoming public, and it advises turning it on unless required for specific use cases like static website hosting. A checkbox for acknowledging this risk is checked. At the bottom, there are sections for 'Bucket Versioning' and navigation links like CloudShell, Feedback, Language, Privacy, Terms, and Cookie preferences.

Allow public access to the bucket and its content.

[To table of contents](#)

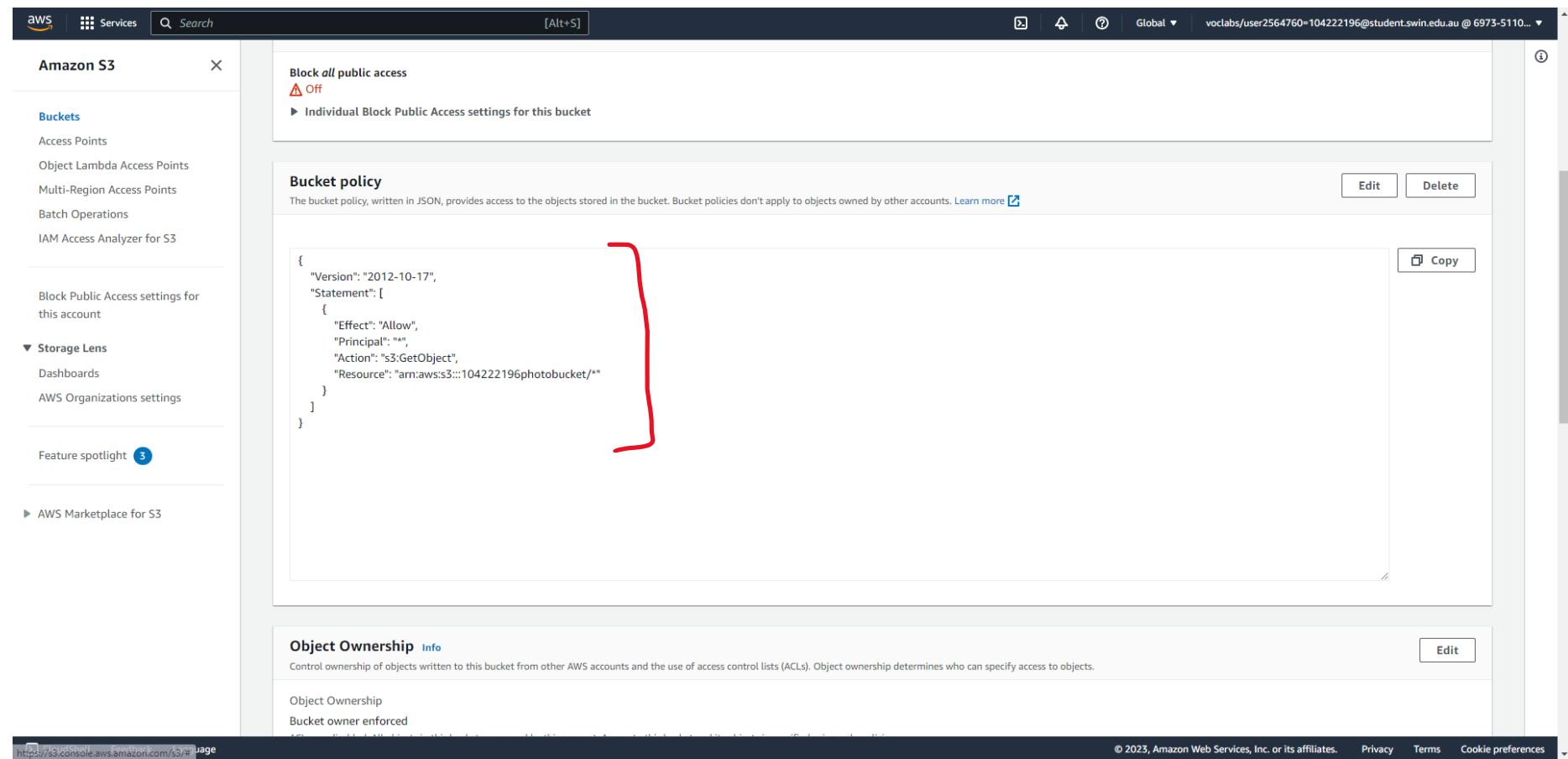
The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with the AWS logo, a 'Services' dropdown, a search bar, and a user account section. Below the navigation bar, the path 'Amazon S3 > Buckets > 104222196photobucket' is displayed. The main title is '104222196photobucket' with a 'Info' link. A red box highlights the 'Publicly accessible' status. Below the title, there are tabs for 'Objects' (which is selected), 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' section displays a table with two items:

| Name             | Type | Last modified                       | Size     | Storage class |
|------------------|------|-------------------------------------|----------|---------------|
| ears tour.jpg    | jpg  | June 14, 2023, 22:28:29 (UTC+07:00) | 245.3 KB | Standard      |
| Speak now tv.jpg | jpg  | June 14, 2023, 22:28:31 (UTC+07:00) | 133.5 KB | Standard      |

At the top of the objects list, there are several buttons: 'Copy', 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and a large orange 'Upload' button. A search bar labeled 'Find objects by prefix' is also present. On the right side of the objects table, there are navigation arrows and a settings gear icon. At the bottom of the page, there are links for 'CloudShell', 'Feedback', 'Language', and copyright information: '© 2023, Amazon Web Services, Inc. or its affiliates.' followed by 'Privacy', 'Terms', and 'Cookie preferences'. A small 'Activate Windows' message is visible on the right.

Upload 2 photos to the S3 bucket.

[To table of contents](#)



The screenshot shows the AWS S3 console with the 'Bucket policy' tab selected. The policy JSON is displayed:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::104222196photobucket/*"
    }
  ]
}
```

Create an access policy that allows anyone to access the bucket objects. Effect “Allow” grants permission to perform the action. Principle “\*” lets anyone perform the action. Action “s3:GetObject” restricts the action to only reading the objects. Resource “arn:aws:s3:::104222196photobucket/\*” indicate that every object in this bucket can be read.

[To table of contents](#)

## 2.2 Photo meta-data in RDS Database

The screenshot shows the phpMyAdmin interface for the 'assignment1b' database. The left sidebar lists databases: 'New', 'assignment1b' (selected), 'New', 'information\_schema', 'mysql', 'performance\_schema', and 'sys'. The main area displays the 'photos' table with two rows of data. The table has columns: id, title, description, date, keywords, and s3\_photo. Row 1: id=1, title='Speak Now TV', description='Cover art for Speak Now TV album', date='2023-06-15', keywords='speak now, taylor swift', s3\_photo='https://104222196photobucket.s3.amazonaws.com/Spea...'. Row 2: id=2, title='Eras Tour', description='Poster for the Eras tour.', date='2023-06-15', keywords='eras tour, taylor swift', s3\_photo='https://104222196photobucket.s3.amazonaws.com/ears...'. Below the table, there are 'Query results operations' buttons: Print, Copy to clipboard, Export, Display chart, Create view.

|   | <input type="checkbox"/> Edit | <input type="checkbox"/> Copy | <input type="checkbox"/> Delete | <input type="checkbox"/> Edit | <input type="checkbox"/> Copy | <input type="checkbox"/> Delete | <input type="checkbox"/> Export |
|---|-------------------------------|-------------------------------|---------------------------------|-------------------------------|-------------------------------|---------------------------------|---------------------------------|
| 1 |                               |                               |                                 |                               |                               |                                 |                                 |
| 2 |                               |                               |                                 |                               |                               |                                 |                                 |

Add 2 records corresponding to the images on S3 into the 'photos' table. This is performed with the INSERT INTO query.

[To table of contents](#)

## 2.3 Photo Album website functionality

← → ⌂ Not secure | ec2-44-216-98-59.compute-1.amazonaws.com/cos80001/photoalbum/album.php

Student name: Ta Quang Tung  
Student ID: 104222196  
Tutorial session: Saturday 3:00PM

Uploaded photos:

| Photo   | Name         | Description                      | Creation date | Keywords                                  |
|---|--------------|----------------------------------|---------------|---|
|  | Speak Now TV | Cover art for Speak Now TV album | 2023-06-15    | speak now, taylor's version, taylor swift |
|  | Eras Tour    | Poster for the Eras tour.        | 2023-06-15    | eras tour, taylor swift                   |

After making the necessary modifications in the constants.php file and uploading the source code to the Web Server, the page is accessible at  
<http://ec2-44-216-98-59.compute-1.amazonaws.com/cos80001/photoalbum/album.php>