Assignment 3 – Multi-Cloud Architecture Deployment

Public URL of the AWS Instance Website: http://34.231.224.149/cos80001/photoalbum/album.php

Team Member	Student ID	Responsibilities
Alexander Blatchford	101623699	- Set up the OCI infrastructure, including the VCN, public and private subnets, and route tables. - Deployed the phpMyAdmin web server in the public subnet and Installed Apache, PHP, and configured phpMyAdmin to connect to the MySQL database. - Created and deployed the MySQL database instance, including database schema setup and testing via phpMyAdmin
Arun Ragavendhar Arunachalam Palaniyappan	104837257	- Handled the full VPN tunnel configuration across both clouds: created DRG, Customer Gateway, and VPN Connections on OCI and AWS and deployed the photoalbum website. - Configured all Firewalls and security components: Security Lists and Security groups on OCI, Security groups and NACL on AWS. - Enforced the least privilege principle and tested end-to-end connectivity across cloud environments.
Samsun Gulshan Sheik Dawood	105009251	- Set up the AWS infrastructure, including the VPC, public and private subnets, and route tables - Deployed and configured the AWS Bastion/Web server, including Apache, PHP, and Elastic IP assignment - Installed and deployed the photoalbum web application under the correct directory, connecting it to the OCI database via VPN - Created the test instance in the private subnet and performed ICMP ping tests to verify internal connectivity.

Table 1: Team Member Names and Contribution

Table of Contents

I. INTRODUCTION *2*

II. OCI INFRASTRUCTURE SETUP *2*

A. Virtual Cloud Network, Route Tabling and Subnet Configuration 2

B. Security Lists and NSGs 3

C. OCI Bastion Webserver Instance and Heatwave Database Instance 4

D. MySQL Database Deployment on OCI 6

E. Object Storage Configuration on OCI 6

III. AWS INFRASTRUCTURE SETUP *6*

A. Virtual Private Cloud, Route Tabling and Subnet Configuration 6

B. Security Groups and Network ACLs 8

C. Web server setup on the AWS bastion web server and attaching elastic IP address 9

D. ICMP PING connectivity testing from Bastion to Test Instance 9

IV. SITE-TO-SITE, TUNNELING AND VPN CONFIGURATION *10*

A. On OCI 10

B. On AWS 11

V. WEB APPLICATION DEPLOYMENT AND CONNECTIVITY *12*

VI. COMPARISON OF DIFFERENT VPN CONNECTION METHODS *13*

VII. CHALLENGES AND LEARNINGS *14*

VIII. CONCLUSION *14*

IX. REFERENCES *14*

I. INTRODUCTION

This report outlines the step-by-step process followed to deploy a multi-cloud photo album web application using Amazon Web Services (AWS) and Oracle Cloud Infrastructure (OCI). The objective was to split the system architecture, where the compute resources such as the web server run on AWS, while the data storage components—MySQL database and object storage—reside in OCI. A site-to-site IPsec connection was established between the AWS VPC and OCI VCN with a singular active tunnel between gateways on both clouds to ensure safe and restricted access between clouds, the AWS bastion/web server and the OCI database.

Public URL of the AWS Instance Website: http://34.231.224.149/cos80001/photoalbum/album.php

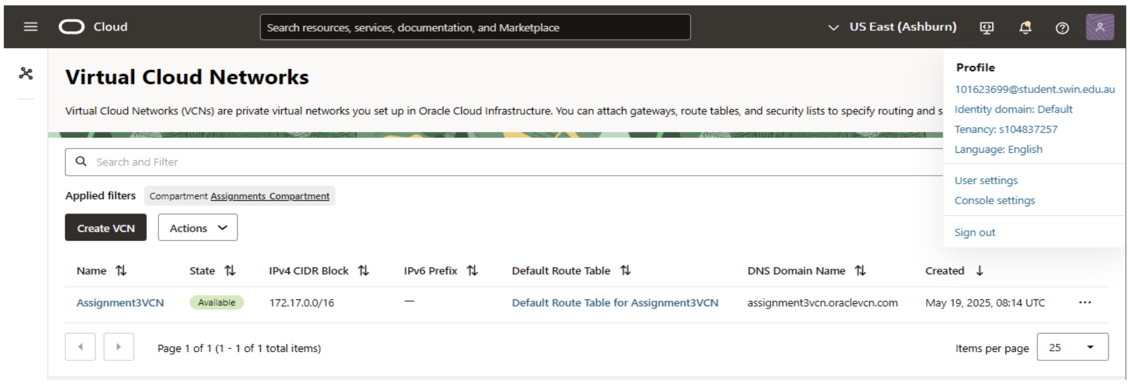
OCI Tenancy: s104837257, Associated student Email: 104837257@student.swin.edu.au

AWS Account - Federated user: voclabs/user3898953=104837257@student.swin.edu.au

II. OCI INFRASTRUCTURE SETUP

A. Virtual Cloud Network, Route Tabling and Subnet Configuration

In the Oracle Cloud Infrastructure (OCI), a Virtual Cloud Network (VCN) named "Assignment-3VCN" was set up in the us-ashburn-1 region using the 172.17.0.0/16 CIDR range. Two subnets were designed within this VCN. Public Subnet 1 (172.17.1.0/24) was created to contain the phpMyAdmin instance and Private Subnet 1 (172.17.3.0/24) was used to host the MySQL database, the VCN's CIDR is shown in Fig 1 and the subnet configuration is illustrated in Fig 2.



Virtual Cloud Networks

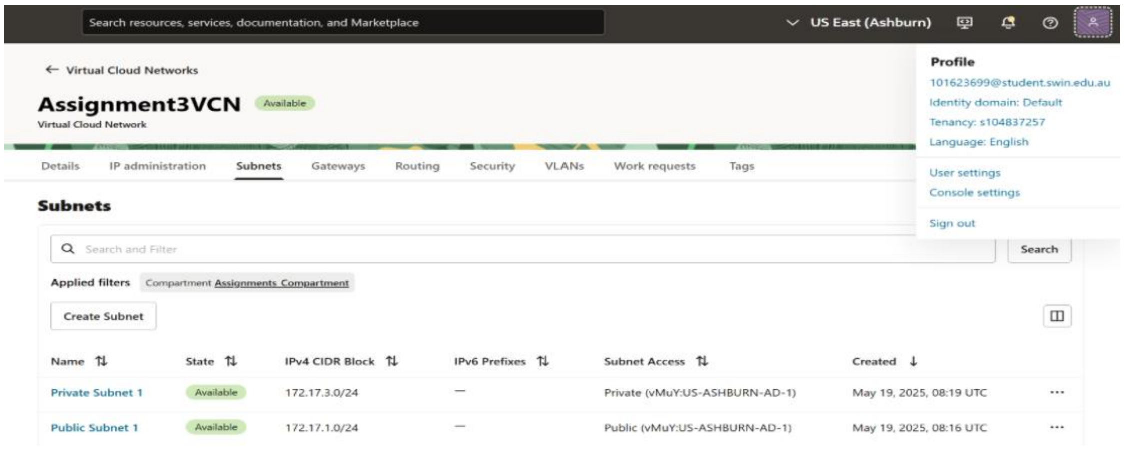
Virtual Cloud Networks (VCNs) are private virtual networks you set up in Oracle Cloud Infrastructure. You can attach gateways, route tables, and security lists to specify routing and s

Applied filters Compartment Assignments Compartment

Name	State	IPv4 CIDR Block	IPv6 Prefix	Default Route Table	DNS Domain Name	Created
Assignment3VCN	Available	172.17.0.0/16	—	Default Route Table for Assignment3VCN	assignment3vcn.oraclevcn.com	May 19, 2025, 08:14 UTC

Page 1 of 1 (1 - 1 of 1 total items) Items per page 25

Fig 1: OCI VCN CIDR and Name



Assignment3VCN Available

Virtual Cloud Network

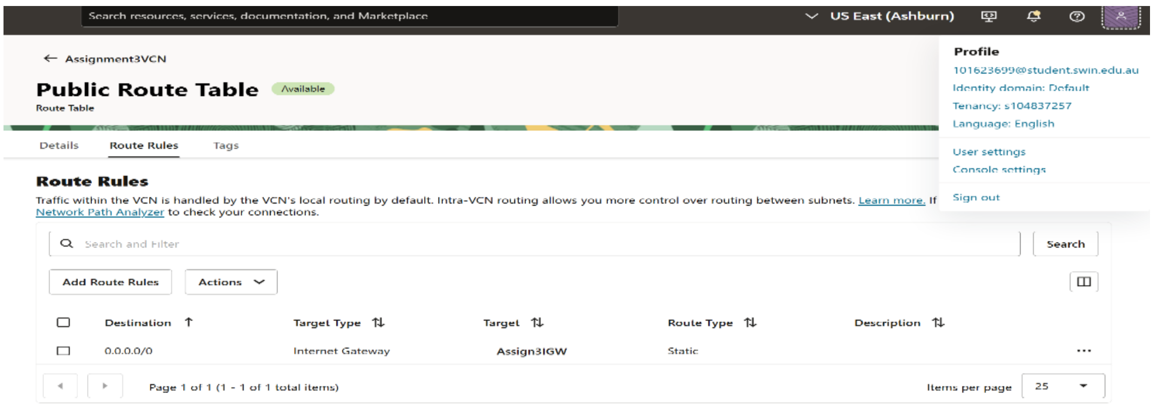
Subnets

Applied filters Compartment Assignments Compartment

Name	State	IPv4 CIDR Block	IPv6 Prefixes	Subnet Access	Created
Private Subnet 1	Available	172.17.3.0/24	—	Private (vMuY:US-ASHBURN-AD-1)	May 19, 2025, 08:19 UTC
Public Subnet 1	Available	172.17.1.0/24	—	Public (vMuY:US-ASHBURN-AD-1)	May 19, 2025, 08:16 UTC

Fig 2: OCI Subnet Configuration

The public subnet was linked to a public route table with an Internet Gateway (Fig 3) to allow internet access. The private subnet was connected to a separate private route table (Fig 4) that restricted any external connectivity, enhancing internal resource security.



Search resources, services, documentation, and Marketplace | US East (Ashburn)

← Assignment3VCN

Public Route Table Available

Route Table

Details | Route Rules | Tags

Route Rules

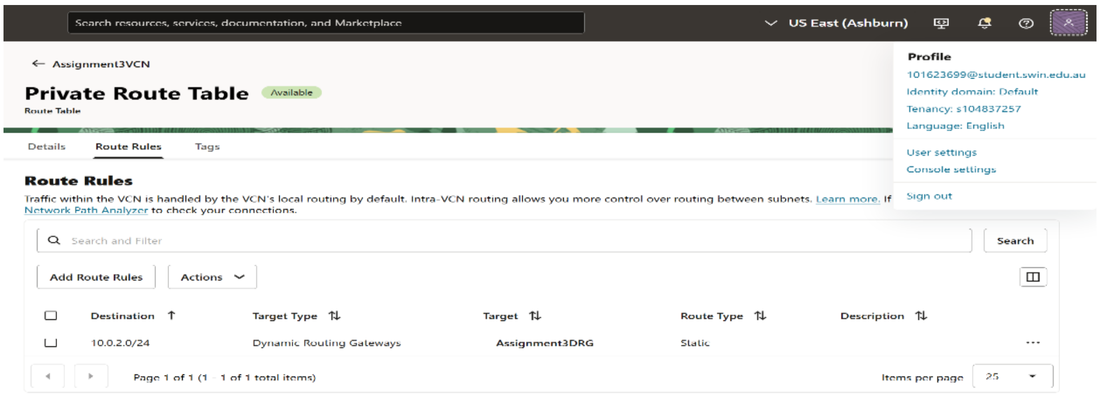
Traffic within the VCN is handled by the VCN's local routing by default. Intra-VCN routing allows you more control over routing between subnets. Learn more. If Network Path Analyzer to check your connections.

Profile
101623699@student.swin.edu.au
Identity domain: Default
Tenancy: s104837257
Language: English
User settings
Console settings
Sign out

Destination	Target Type	Target	Route Type	Description
0.0.0.0/0	Internet Gateway	Assign3IGW	Static	

Page 1 of 1 (1 - 1 of 1 total items) Items per page 25

Fig 3: Public Route Table Route Rules



Search resources, services, documentation, and Marketplace | US East (Ashburn)

← Assignment3VCN

Private Route Table Available

Route Table

Details | Route Rules | Tags

Route Rules

Traffic within the VCN is handled by the VCN's local routing by default. Intra-VCN routing allows you more control over routing between subnets. Learn more. If Network Path Analyzer to check your connections.

Profile
101623699@student.swin.edu.au
Identity domain: Default
Tenancy: s104837257
Language: English
User settings
Console settings
Sign out

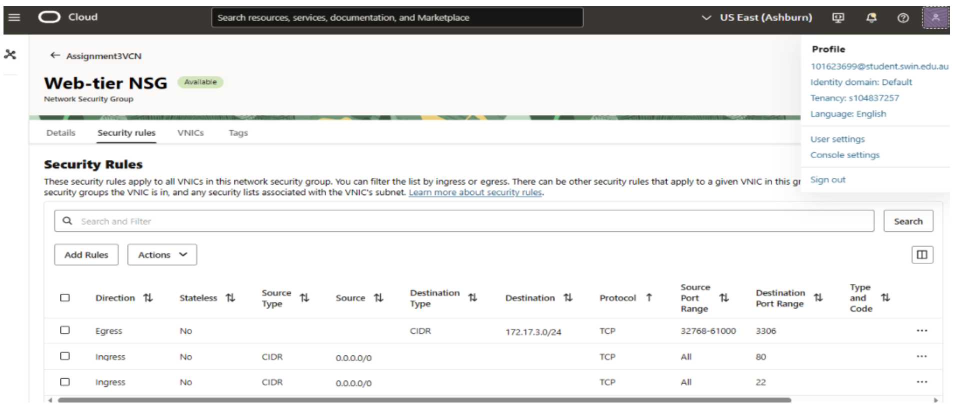
Destination	Target Type	Target	Route Type	Description
10.0.2.0/24	Dynamic Routing Gateways	Assignment3DRG	Static	

Page 1 of 1 (1 - 1 of 1 total items) Items per page 25

Fig 4: Private Route Table Route Rules

B. Security Lists and NSGs

In OCI, security was managed using a singular security list for the public subnet called PublicSubnet1SL (Fig 7) and the default security list was used to manage the private subnet's security (Fig 6). This security was utilised in tandem with a Network Security Group (NSG) called Web-tier NSG (Fig 5) to be attached to the VNIC of the bastion instance on OCI. PublicSubnet1SL allows ingress for SSH and HTTP requests from anywhere. The default security list allows ingress from the webserver's restricted 32786-61000 ephemeral ports with a destination to the 3306 MySQL database port. Traffic to the database from the AWS Webserver's public subnet CIDR (10.0.2.0/24) is also allowed when directed to port 3306 from the ephemeral range. The NSG Web-tier NSG allows egress to the AWS bastion directed to the database from the ephemeral range and ingress from all anywhere for HTTP and SSH from the internet.



Cloud | Search resources, services, documentation, and Marketplace | US East (Ashburn)

← Assignment3VCN

Web-tier NSG Available

Network Security Group

Details | Security rules | VNICs | Tags

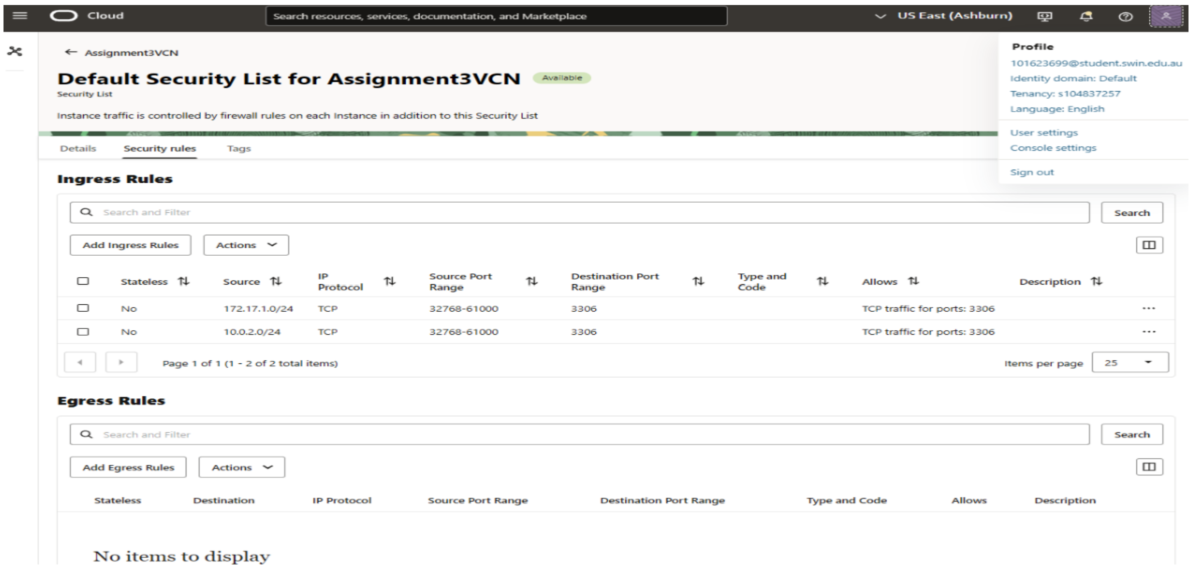
Security Rules

These security rules apply to all VNICs in this network security group. You can filter the list by ingress or egress. There can be other security rules that apply to a given VNIC in this gr security groups the VNIC is in, and any security lists associated with the VNIC's subnet. Learn more about security rules.

Profile
101623699@student.swin.edu.au
Identity domain: Default
Tenancy: s104837257
Language: English
User settings
Console settings
Sign out

Direction	Stateless	Source Type	Source	Destination Type	Destination	Protocol	Source Port Range	Destination Port Range	Type and Code
Egress	No			CIDR	172.17.3.0/24	TCP	32768-61000	3306	
Ingress	No	CIDR	0.0.0.0/0			TCP	All	80	
Ingress	No	CIDR	0.0.0.0/0			TCP	All	22	

Fig 5: Network Security Group: Web-tier NSG


Cloud | Search resources, services, documentation, and Marketplace | US East (Ashburn)

Profile
101623699@student.swin.edu.au
Identity domain: Default
Tenancy: s104837257
Language: English
User settings
Console settings
Sign out

← Assignment3VCN

Default Security List for Assignment3VCN Available

Security List

Instance traffic is controlled by firewall rules on each Instance in addition to this Security List

Details | Security rules | Tags

Ingress Rules

Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
No	172.17.1.0/24	TCP	32768-61000	3306		TCP traffic for ports: 3306	
No	10.0.2.0/24	TCP	32768-61000	3306		TCP traffic for ports: 3306	

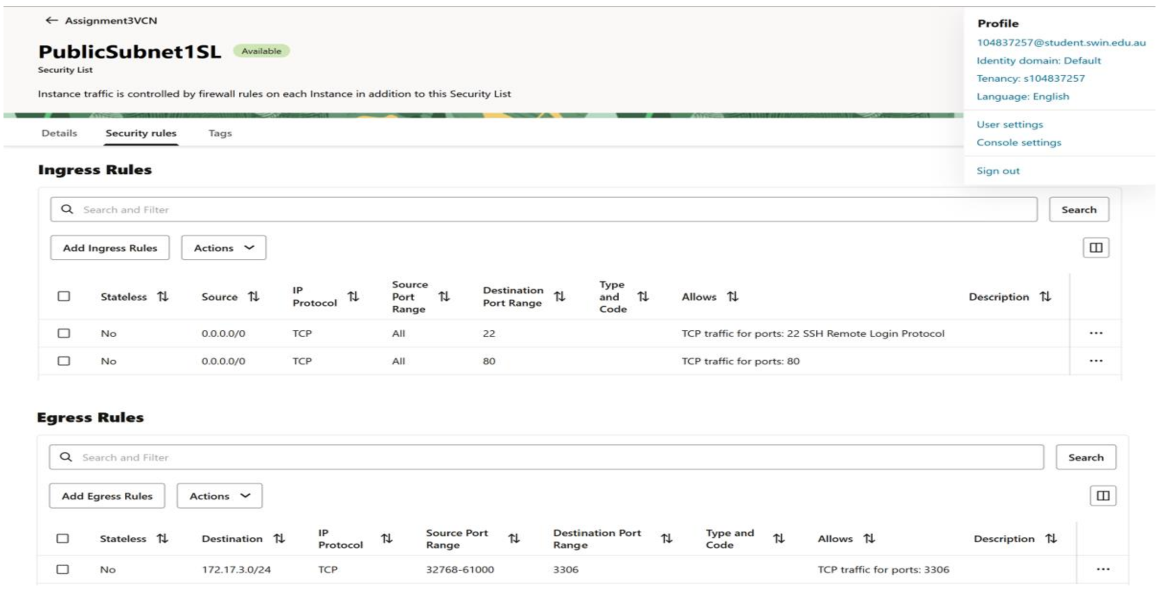
Page 1 of 1 (1 - 2 of 2 total items) Items per page 25

Egress Rules

Stateless	Destination	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description

No items to display

Fig 6: Default Security List (For DB Private Subnet)


← Assignment3VCN

PublicSubnet1SL Available

Security List

Instance traffic is controlled by firewall rules on each Instance in addition to this Security List

Profile
104837257@student.swin.edu.au
Identity domain: Default
Tenancy: s104837257
Language: English
User settings
Console settings
Sign out

Details | Security rules | Tags

Ingress Rules

Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
No	0.0.0.0/0	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	
No	0.0.0.0/0	TCP	All	80		TCP traffic for ports: 80	

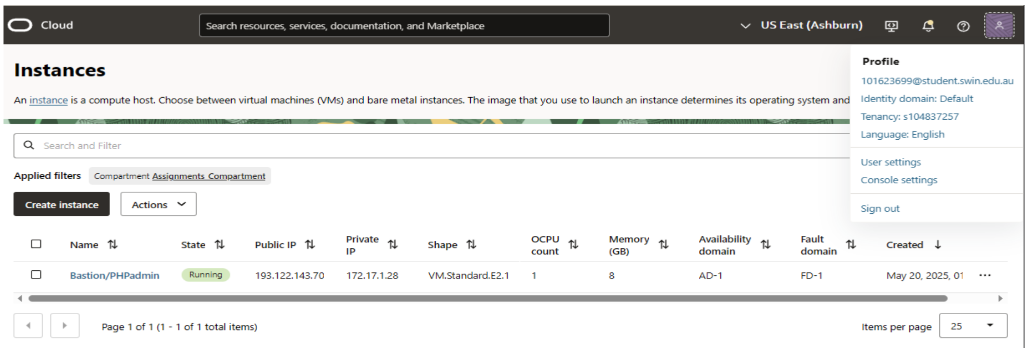
Egress Rules

Stateless	Destination	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
No	172.17.3.0/24	TCP	32768-61000	3306		TCP traffic for ports: 3306	

Fig 7: Security List: PublicSubnet1SL

C. OCI Bastion Webserver Instance and Heatwave Database Instance

The Bastion/PHPadmin server was created in the public subnet and the name and IP addresses can be seen in Fig 8. The security and route table associations are illustrated in Fig 9, where the public route table is associated.


Cloud | Search resources, services, documentation, and Marketplace | US East (Ashburn)

Instances

An instance is a compute host. Choose between virtual machines (VMs) and bare metal instances. The image that you use to launch an instance determines its operating system and

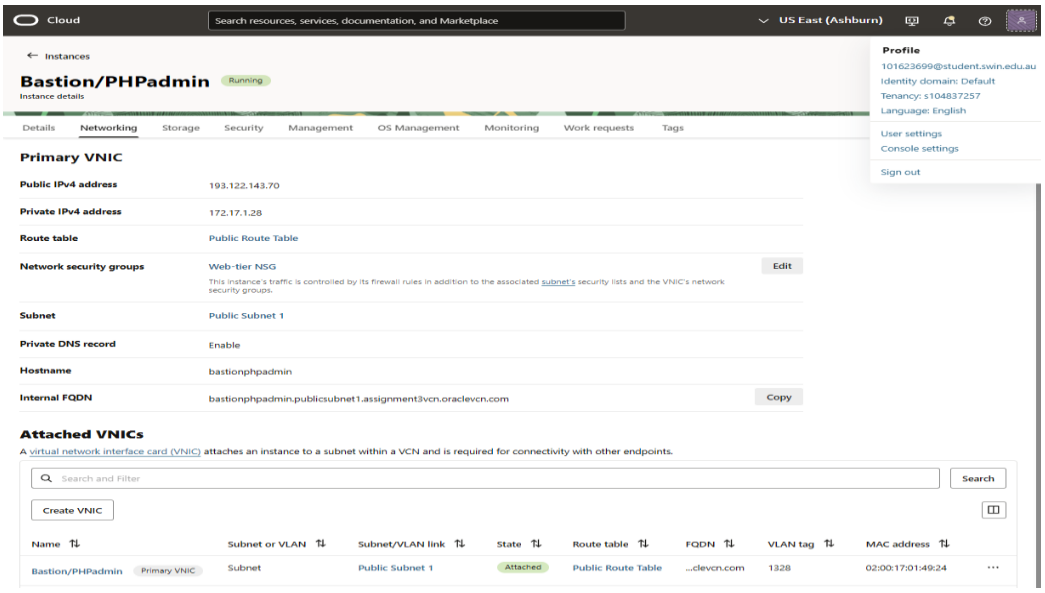
Profile
101623699@student.swin.edu.au
Identity domain: Default
Tenancy: s104837257
Language: English
User settings
Console settings
Sign out

Applied filters: Compartment Assignments Compartment

Name	State	Public IP	Private IP	Shape	OCPU count	Memory (GB)	Availability domain	Fault domain	Created
Bastion/PHPadmin	Running	193.122.143.70	172.17.1.28	VM.Standard.E2.1	1	8	AD-1	FD-1	May 20, 2025, 01

Page 1 of 1 (1 - 1 of 1 total items) Items per page 25

Fig 8: Bastion/PHPadmin OCI Instance



Bastion/PHPadmin Running
Instance details

Primary VNIC

Public IPv4 address	193.122.143.70
Private IPv4 address	172.17.1.28
Route table	Public Route Table
Network security groups	Web-tier NSG This instance's traffic is controlled by its firewall rules in addition to the associated subnet's security lists and the VNIC's network security groups.
Subnet	Public Subnet 1
Private DNS record	Enable
Hostname	bastionphpadmin
Internal FQDN	bastionphpadmin.publicsubnet1.assignment3vcn.oraclevcn.com

Attached VNICs

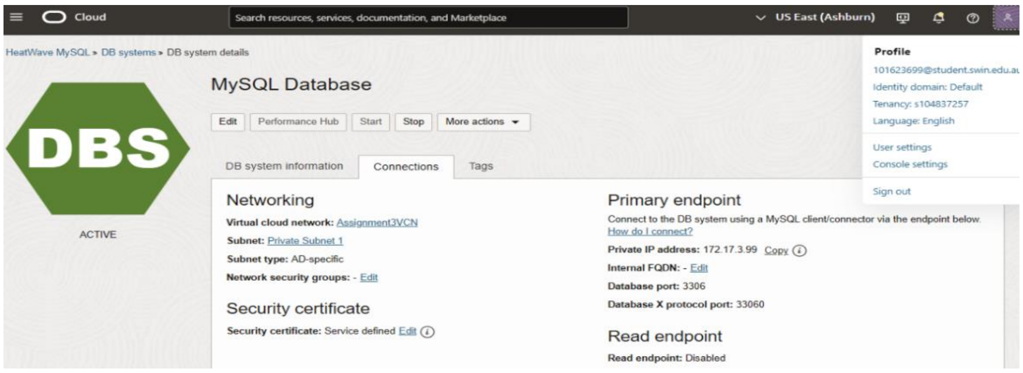
A virtual network interface card (VNIC) attaches an instance to a subnet within a VCN and is required for connectivity with other endpoints.

Name	Subnet or VLAN	Subnet/VLAN link	State	Route table	FQDN	VLAN tag	MAC address
Bastion/PHPadmin Primary VNIC	Subnet	Public Subnet 1	Attached	Public Route Table	...clevcn.com	1328	02:00:17:01:49:24

Profile: 101623699@student.swin.edu.au, Identity domain: Default, Tenancy: s104837257, Language: English

Fig 9: Bastion/PHPadmin Route Table, Subnet and NSG Association

The MySQL Database was deployed using OCI's Heatwave Interface; the endpoint, subnet association and VCN association can be seen in Fig 10. The database was configured to have the shape as MySQL.2, with 2 ECPUs, 8.0.41 DB version, MySQL 2 Standalone config and no heatwave clustering with no backups according to specification (Fig 11).



HeatWave MySQL » DB systems » DB system details

MySQL Database — ACTIVE

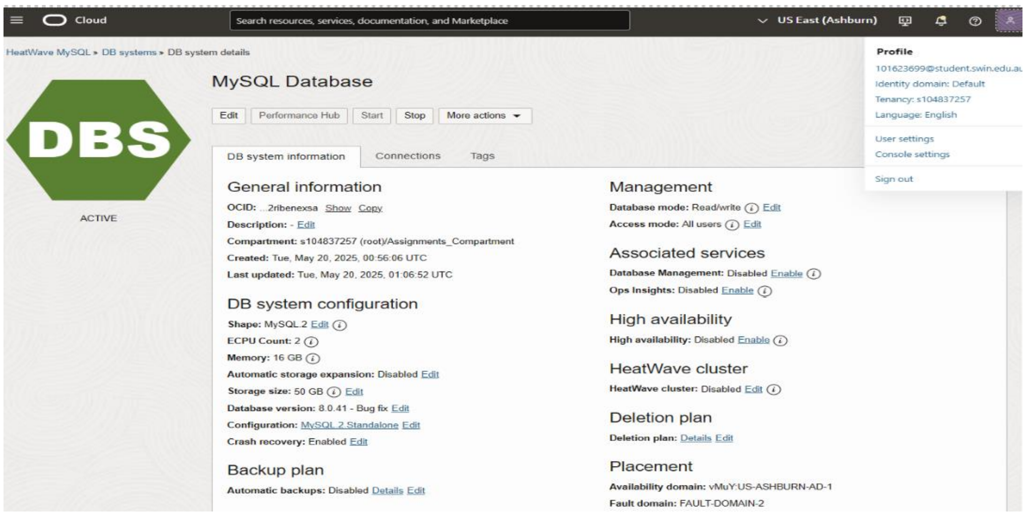
Networking
Virtual cloud network: Assignment3VCN
Subnet: Private Subnet 1
Subnet type: AD-specific
Network security groups: - Edit

Security certificate
Security certificate: Service defined Edit

Primary endpoint
Connect to the DB system using a MySQL client/connector via the endpoint below.
Private IP address: 172.17.3.99
Internal FQDN: - Edit
Database port: 3306
Database X protocol port: 33060

Read endpoint
Read endpoint: Disabled

Fig 10: MySQL Database Endpoint, VCN and Private Subnet Association



HeatWave MySQL » DB systems » DB system details

MySQL Database — ACTIVE

General information
OCID: ...2ribenexsa Show Copy
Description: - Edit
Compartment: s104837257 (root)/Assignments_Compartment
Created: Tue, May 20, 2025, 00:56:06 UTC
Last updated: Tue, May 20, 2025, 01:06:52 UTC

DB system configuration
Shape: MySQL.2 Edit
ECPU Count: 2
Memory: 16 GB
Automatic storage expansion: Disabled Edit
Storage size: 50 GB Edit
Database version: 8.0.41 - Bug fix Edit
Configuration: MySQL.2.Standalone Edit
Crash recovery: Enabled Edit

Backup plan
Automatic backups: Disabled Details Edit

Management
Database mode: Read/write Edit
Access mode: All users Edit

Associated services
Database Management: Disabled Enable
Ops Insights: Disabled Enable

High availability
High availability: Disabled Enable

HeatWave cluster
HeatWave cluster: Disabled Edit

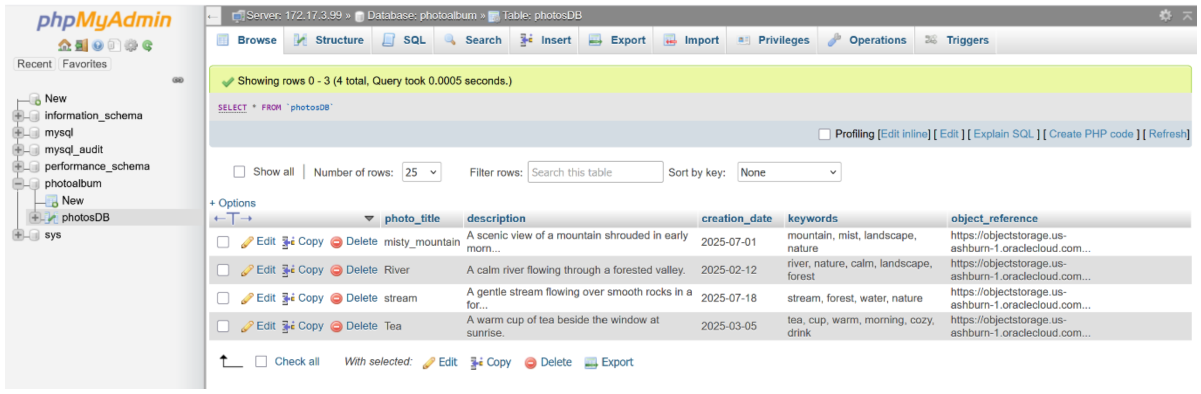
Deletion plan
Deletion plan: Details Edit

Placement
Availability domain: vMuY:US-ASHBURN-AD-1
Fault domain: FAULT-DOMAIN-2

Fig 11: MySQL Database Deployment Details

D. MySQL Database Deployment on OCI

In OCI, a managed MySQL database (version 8.0.41, MySQL2 shape, 50GB storage) was deployed in Private Subnet 1, with public access disabled for security. It used OCI's default security list, allowing ingress only from the OCI Bastion/Web Server and the AWS Bastion/Web Server. The database, named photoalbum, had one table called photosDB, with fields: photo_title, description, creation_date, keywords, and object_reference—storing the photo's name, caption, date, tags, and image URL, as seen in Fig 12. It was managed using phpMyAdmin, accessed securely from the OCI Bastion/Web Server.



Showing rows 0 - 3 (4 total, Query took 0.0005 seconds.)

```
SELECT * FROM `photosDB`
```

Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None

+ Options

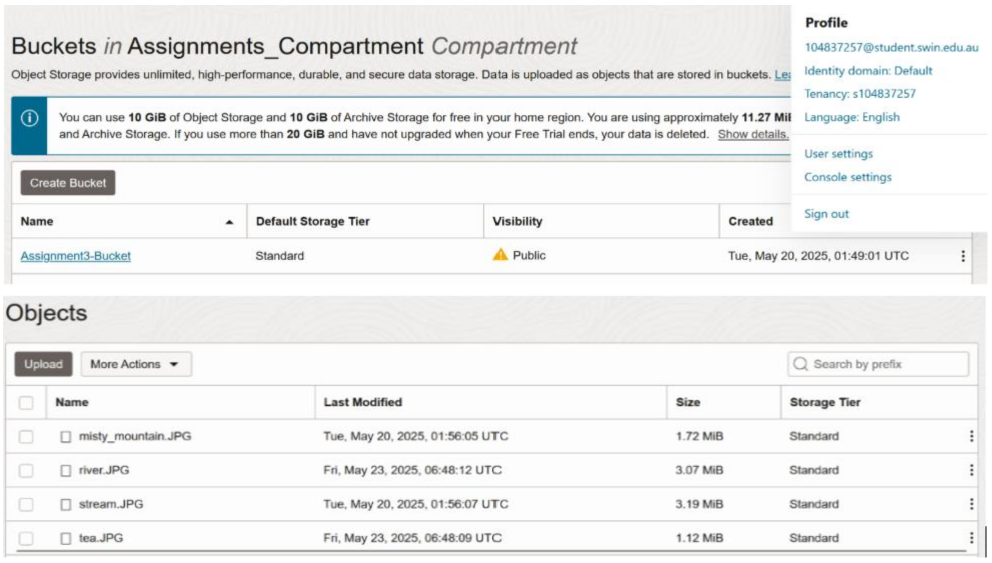
	photo_title	description	creation_date	keywords	object_reference
Edit Copy Delete	misty_mountain	A scenic view of a mountain shrouded in early morn...	2025-07-01	mountain, mist, landscape, nature	https://objectstorage.us-ashburn-1.oraclecloud.com...
Edit Copy Delete	River	A calm river flowing through a forested valley.	2025-02-12	river, nature, calm, landscape, forest	https://objectstorage.us-ashburn-1.oraclecloud.com...
Edit Copy Delete	stream	A gentle stream flowing over smooth rocks in a for...	2025-07-18	stream, forest, water, nature	https://objectstorage.us-ashburn-1.oraclecloud.com...
Edit Copy Delete	Tea	A warm cup of tea beside the window at sunrise.	2025-03-05	tea, cup, warm, morning, cozy, drink	https://objectstorage.us-ashburn-1.oraclecloud.com...

Check all With selected: Edit Copy Delete Export

Fig 12: photosDB table schema and data records from phpMyAdmin

E. Object Storage Configuration on OCI

A bucket named Assignment-3_bucket was created using OCI's Object Storage service. Public access was granted at the bucket level, which meant all uploaded photos were accessible via direct public URLs. This removed the need to individually modify permissions for each file. Four sample images were uploaded through the OCI console and tested using an incognito browser window to confirm public access worked as intended.



Buckets *in* Assignments_Compartment *Compartment*

Object Storage provides unlimited, high-performance, durable, and secure data storage. Data is uploaded as objects that are stored in buckets. Lea

You can use **10 GiB** of Object Storage and **10 GiB** of Archive Storage for free in your home region. You are using approximately **11.27 Mi** and Archive Storage. If you use more than **20 GiB** and have not upgraded when your Free Trial ends, your data is deleted. Show details.

Name	Default Storage Tier	Visibility	Created
Assignment3-Bucket	Standard	⚠ Public	Tue, May 20, 2025, 01:49:01 UTC

Objects

Name	Last Modified	Size	Storage Tier
misty_mountain.JPG	Tue, May 20, 2025, 01:56:05 UTC	1.72 MiB	Standard
river.JPG	Fri, May 23, 2025, 06:48:12 UTC	3.07 MiB	Standard
stream.JPG	Tue, May 20, 2025, 01:56:07 UTC	3.19 MiB	Standard
tea.JPG	Fri, May 23, 2025, 06:48:09 UTC	1.12 MiB	Standard

Fig 13: Public Access Settings and Uploaded Images in Object Storage

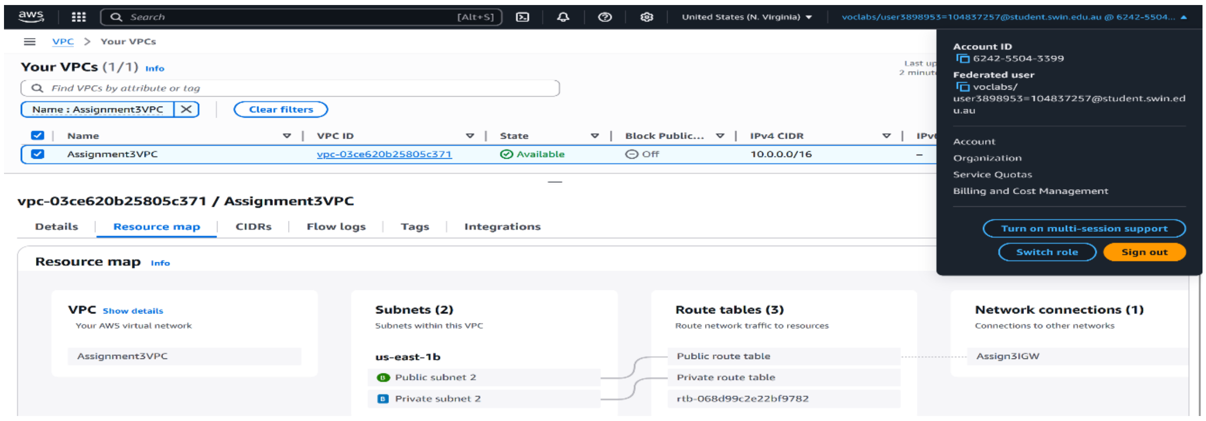
III. AWS INFRASTRUCTURE SETUP

A. Virtual Private Cloud, Route Tabling and Subnet Configuration

To begin the deployment, a custom Virtual Private Cloud (VPC) named "Assignment3VPC" was created within the us-east-1-b region in AWS. The CIDR block assigned to this VPC was 10.0.0.0/16, inside this VPC two subnets were designed, one as public subnet and the other as a private subnet (Fig 14). Public Subnet 2 with the

IP range 10.0.2.0/24 and Private Subnet 2 (10.0.4.0/24) were created for AWS, with the public for the Bastion/Web server and the private used to host a test instance.

A public route table was created and attached for the public subnet. Likewise, a private route table was created and attached to the private subnet. Public subnets were connected to an Internet Gateway using the public route table that allowed internet access (Fig 16). The private subnet was connected to a separate route table that did not include internet access (Fig 15). The OCI database subnet CIDR (172.17.3.0/24) and the target AWS VPG to reach it, were added in the public route table, allowing the AWS bastion/web server to access the Database on the OCI Cloud through the VPN tunnel.


Search [Alt+S]
United States (N. Virginia)
voclabs/user3898953=104837257@student.swin.edu.au @ 6242-5504...
VPC > Your VPCs
Account ID
6242-5504-3399
Federated user
voclabs/
user3898953=104837257@student.swin.edu.au
Account
Organization
Service Quotas
Billing and Cost Management
Turn on multi-session support
Switch role
Sign out

Your VPCs (1/1) Info

Name : Assignment3VPC | Clear filters

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv
Assignment3VPC	vpc-03ce620b25805c371	Available	Off	10.0.0.0/16	–

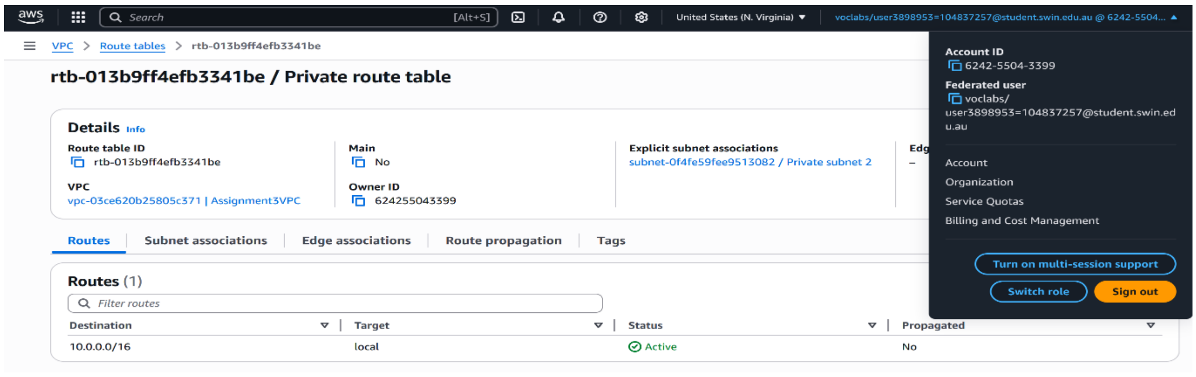
vpc-03ce620b25805c371 / Assignment3VPC

Details | Resource map | CIDRs | Flow logs | Tags | Integrations

Resource map Info

- VPC (Show details) – Your AWS virtual network: Assignment3VPC
- Subnets (2) – Subnets within this VPC: us-east-1b: Public subnet 2, Private subnet 2
- Route tables (3) – Route network traffic to resources: Public route table, Private route table, rtb-068d99c2e22bf9782
- Network connections (1) – Connections to other networks: Assign3IGW

Fig 14: Assignment3VPC, its CIDR, Subnet and Route Table Associations


Search [Alt+S]
United States (N. Virginia)
voclabs/user3898953=104837257@student.swin.edu.au @ 6242-5504...
VPC > Route tables > rtb-013b9ff4efb3341be
Account ID
6242-5504-3399
Federated user
voclabs/
user3898953=104837257@student.swin.edu.au
Account
Organization
Service Quotas
Billing and Cost Management
Turn on multi-session support
Switch role
Sign out

rtb-013b9ff4efb3341be / Private route table

Details Info

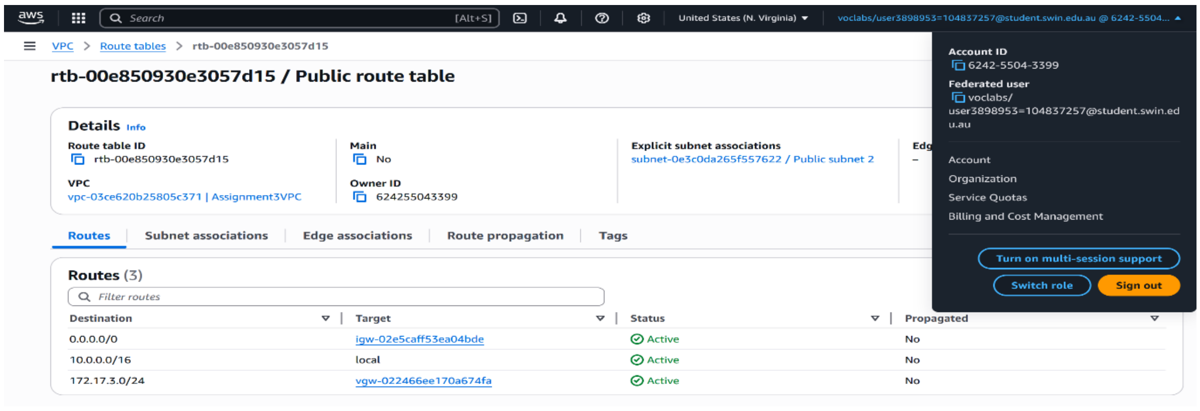
Route table ID: rtb-013b9ff4efb3341be
Main: No
Explicit subnet associations: subnet-0f4fe59fee9513082 / Private subnet 2
Edg: –
VPC: vpc-03ce620b25805c371 | Assignment3VPC
Owner ID: 624255043399

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (1)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Fig 15: Routes associated with Private Route Table


Search [Alt+S]
United States (N. Virginia)
voclabs/user3898953=104837257@student.swin.edu.au @ 6242-5504...
VPC > Route tables > rtb-00e850930e3057d15
Account ID
6242-5504-3399
Federated user
voclabs/
user3898953=104837257@student.swin.edu.au
Account
Organization
Service Quotas
Billing and Cost Management
Turn on multi-session support
Switch role
Sign out

rtb-00e850930e3057d15 / Public route table

Details Info

Route table ID: rtb-00e850930e3057d15
Main: No
Explicit subnet associations: subnet-0e3c0da265f557622 / Public subnet 2
Edg: –
VPC: vpc-03ce620b25805c371 | Assignment3VPC
Owner ID: 624255043399

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (3)

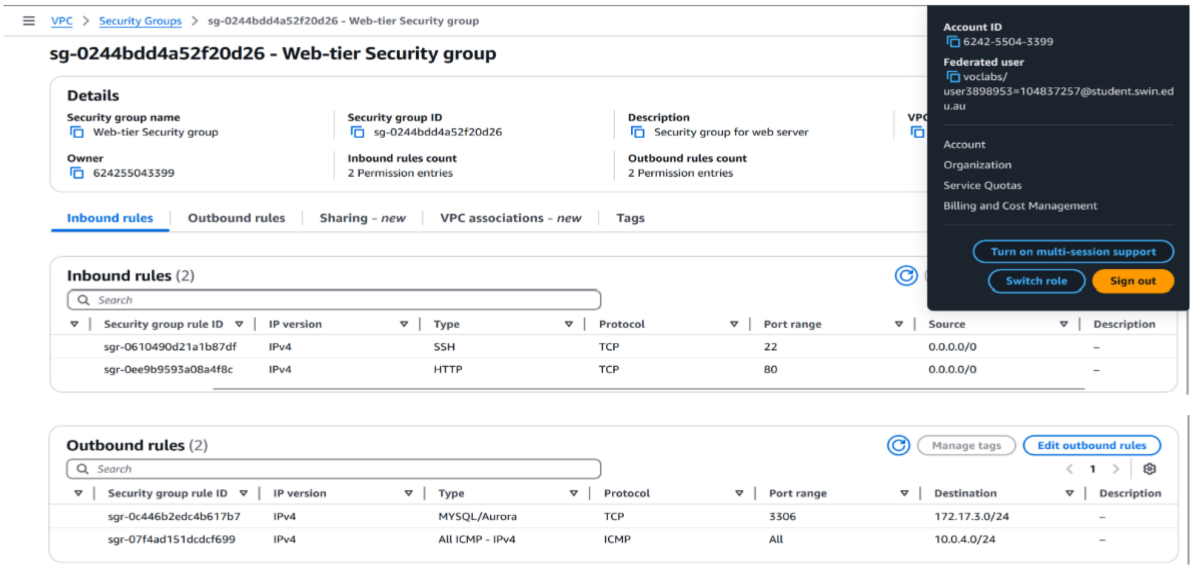
Destination	Target	Status	Propagated
0.0.0.0/0	igw-02e5caff53ea04bde	Active	No
10.0.0.0/16	local	Active	No
172.17.3.0/24	vgw-022466ee170a674fa	Active	No

Fig 16: Routes associated with Public Route Table

B. Security Groups and Network ACLs

On AWS, the Web-tier Security Group controlled access to the Bastion/Web Server. It allowed SSH (port 22) and HTTP (port 80) from anywhere for remote access and public hosting. Outbound traffic was restricted to only what was needed - MySQL (port 3306) to the OCI database (172.17.3.0/24) and ICMP to the test instance (10.0.4.0/24), ensuring private, secure communication (Fig 17).

The PublicSubnet2NACL allowed inbound traffic on ports 22, 80, ICMP, and ephemeral ports (32768–61000), while outbound traffic was limited to ports 1024–65535 and ICMP to support return traffic (Fig 19). The Test-instance Security Group allowed only ICMP both ways, enabling ping tests while blocking everything else (Fig 18). All traffic was tightly controlled under the least privilege principle—only essential communication was permitted, with everything else denied.



sg-0244bdd4a52f20d26 - Web-tier Security group

Details

Security group name: Web-tier Security group	Security group ID: sg-0244bdd4a52f20d26	Description: Security group for web server
Owner: 624255043399	Inbound rules count: 2 Permission entries	Outbound rules count: 2 Permission entries

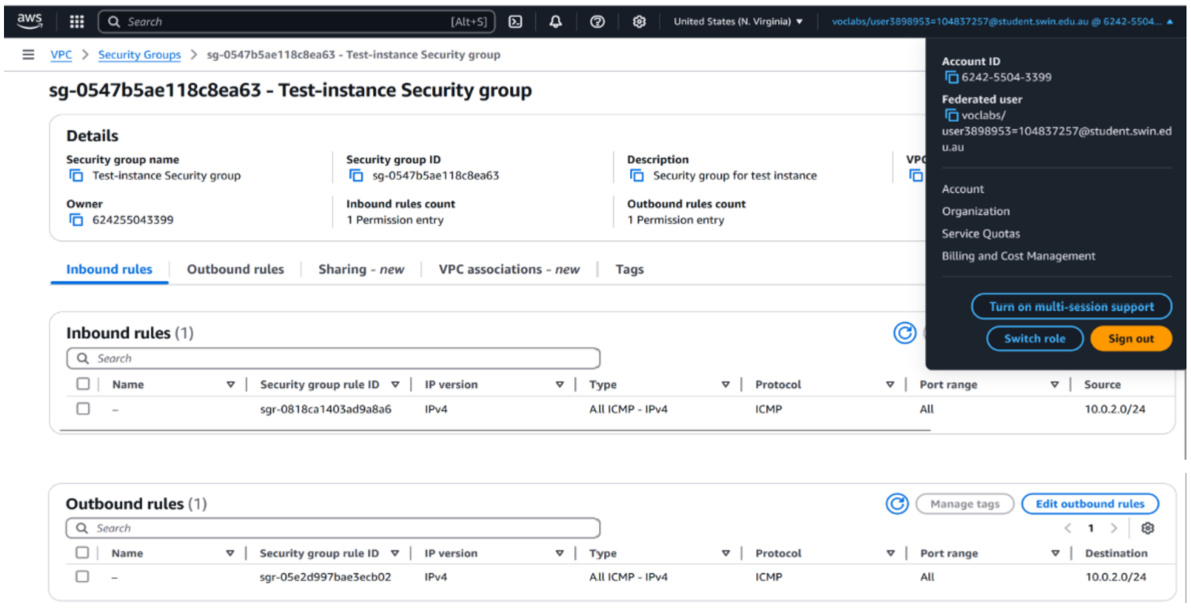
Inbound rules (2)

Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
sgr-0610490d21a1b87df	IPv4	SSH	TCP	22	0.0.0.0/0	–
sgr-0ee9b9593a08a4f8c	IPv4	HTTP	TCP	80	0.0.0.0/0	–

Outbound rules (2)

Security group rule ID	IP version	Type	Protocol	Port range	Destination	Description
sgr-0c446b2edc4b617b7	IPv4	MYSQL/Aurora	TCP	3306	172.17.3.0/24	–
sgr-07f4ad151dcdcf699	IPv4	All ICMP - IPv4	ICMP	All	10.0.4.0/24	–

Fig 17: Web-tier Security group with inbound and outbound rules


aws
Search [Alt+S]
United States (N. Virginia)
voclabs/user3898953=104837257@student.swin.edu.au @ 6242-5504...
VPC > Security Groups > sg-0547b5ae118c8ea63 - Test-instance Security group
Account ID
6242-5504-3399
Federated user
voclabs/
user3898953=104837257@student.swin.edu.au
Account
Organization
Service Quotas
Billing and Cost Management
Turn on multi-session support
Switch role
Sign out
Inbound rules
Outbound rules
Sharing - new
VPC associations - new
Tags
Search
Manage tags
Edit outbound rules

sg-0547b5ae118c8ea63 - Test-instance Security group

Details

Security group name: Test-instance Security group	Security group ID: sg-0547b5ae118c8ea63	Description: Security group for test instance
Owner: 624255043399	Inbound rules count: 1 Permission entry	Outbound rules count: 1 Permission entry

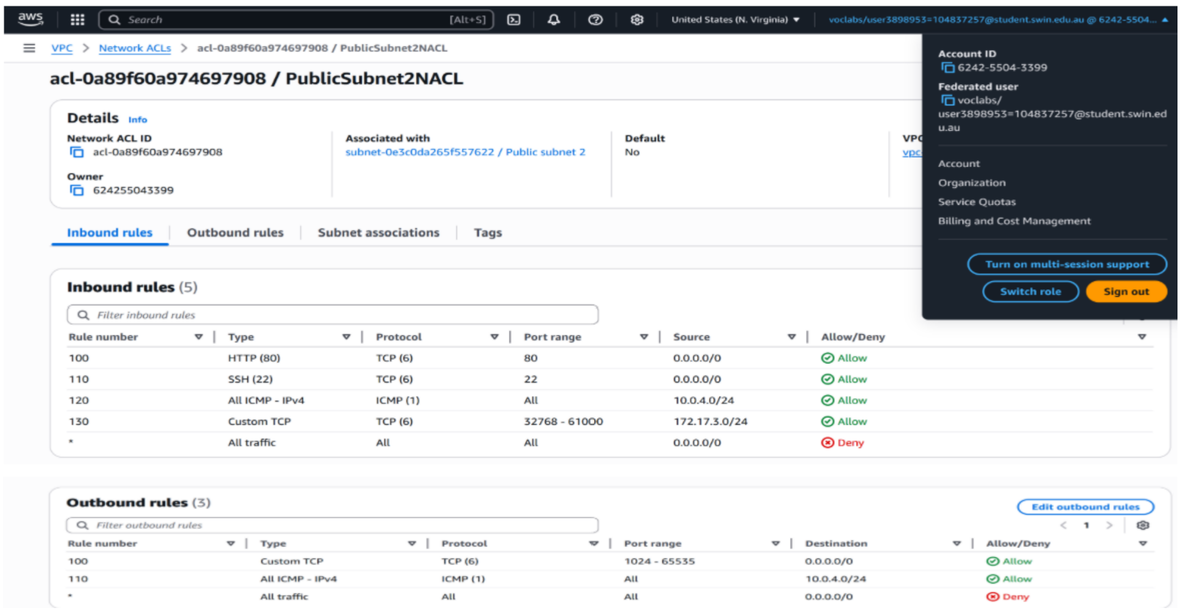
Inbound rules (1)

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
–	sgr-0818ca1403ad9a8a6	IPv4	All ICMP - IPv4	ICMP	All	10.0.2.0/24

Outbound rules (1)

Name	Security group rule ID	IP version	Type	Protocol	Port range	Destination
–	sgr-05e2d997bae3ecb02	IPv4	All ICMP - IPv4	ICMP	All	10.0.2.0/24

Fig 18: Test-instance Security group with inbound and outbound rules



voclabs/user3898953=104837257@student.swin.edu.au @ 6242-5504...

VPC > Network ACLs > acl-0a89f60a974697908 / PublicSubnet2NACL

acl-0a89f60a974697908 / PublicSubnet2NACL

Details

Network ACL ID: acl-0a89f60a974697908
Owner: 624255043399
Associated with: subnet-0e3c0da265f557622 / Public subnet 2
Default: No

Account ID: 6242-5504-3399
Federated user: voclabs/user3898953=104837257@student.swin.edu.au

Inbound rules (5)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
110	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow
120	All ICMP - IPv4	ICMP (1)	All	10.0.4.0/24	Allow
130	Custom TCP	TCP (6)	32768 - 61000	172.17.3.0/24	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

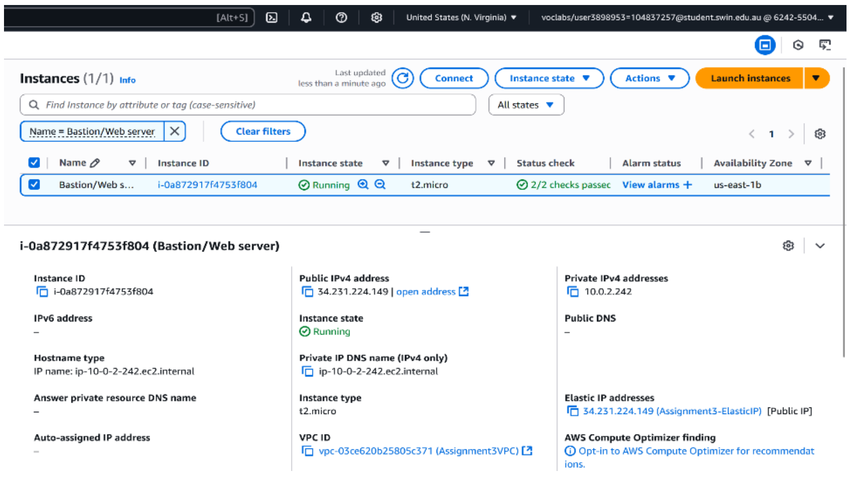
Outbound rules (3)

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
110	All ICMP - IPv4	ICMP (1)	All	10.0.4.0/24	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Fig 19: PublicSubnet2NACL with inbound and outbound rules

C. Web server setup on the AWS bastion web server and attaching elastic IP address

A script was run on the AWS bastion/web server to install Apache, PHP, and phpMyAdmin to deploy and host the photoalbum web site. To keep the public IP address as the same, even after restarts, an Elastic IP was created and attached as shown below in Fig 20.



Instances (1/1)

Name = Bastion/Web server

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Bastion/Web s...	i-0a872917f4753f804	Running	t2.micro	2/2 checks passec	View alarms +	us-east-1b

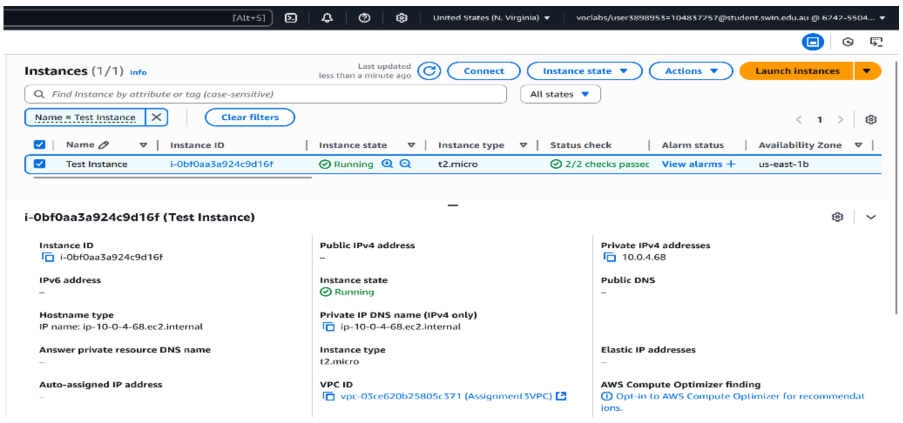
i-0a872917f4753f804 (Bastion/Web server)

Instance ID: i-0a872917f4753f804
IPv6 address: –
Hostname type: IP name: ip-10-0-2-242.ec2.internal
Answer private resource DNS name: –
Auto-assigned IP address: –
Public IPv4 address: 34.231.224.149 | open address
Instance state: Running
Private IP DNS name (IPv4 only): ip-10-0-2-242.ec2.internal
Instance type: t2.micro
VPC ID: vpc-03ce620b25805c371 (Assignment3VPC)
Private IPv4 addresses: 10.0.2.242
Public DNS: –
Elastic IP addresses: 34.231.224.149 (Assignment3-ElasticIP) [Public IP]
AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations.

Fig 20: Bastion/Webserver with the elastic IP address

D. ICMP PING connectivity testing from Bastion to Test Instance

The test instance resides in the private subnet (10.0.4.0/24) and its private IP address is 10.0.4.68 (Fig 21). An ICMP ping was carried out from the bastion/webserver to this test instance to test connectivity and this was successful as shown below in Fig 22.



United States (N. Virginia) ▾ voclabs/user3898953=104837757@student.swin.edu.au @ 6742-5504... ▾

Instances (1/1) Info — Last updated less than a minute ago — Connect | Instance state ▾ | Actions ▾ | Launch instances ▾

Find Instance by attribute or tag (case-sensitive) — All states ▾

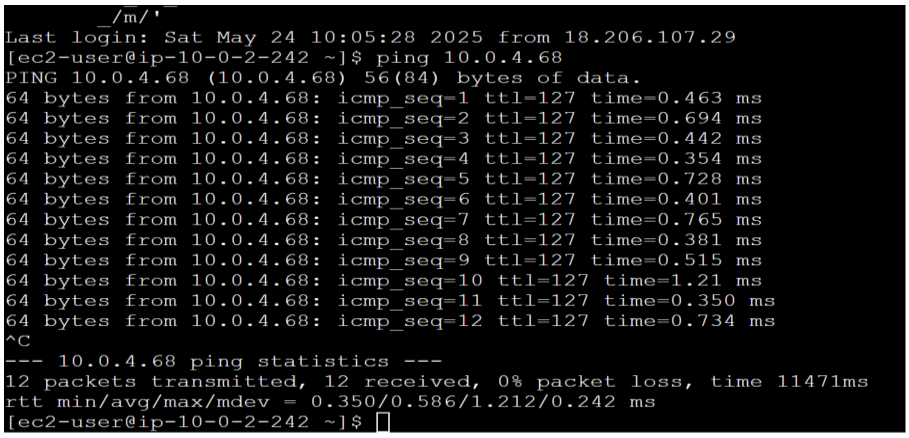
Name = Test Instance ✕ — Clear filters

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
✓	Test Instance	i-0bf0aa3a924c9d16f	Running	t2.micro	2/2 checks passec	View alarms +	us-east-1b

i-0bf0aa3a924c9d16f (Test Instance)

Instance ID i-0bf0aa3a924c9d16f	Public IPv4 address –	Private IPv4 addresses 10.0.4.68
IPv6 address –	Instance state Running	Public DNS –
Hostname type IP name: ip-10-0-4-68.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-4-68.ec2.internal	
Answer private resource DNS name –	Instance type t2.micro	Elastic IP addresses –
Auto-assigned IP address –	VPC ID vpc-03ce620b25805c371 (Assignment3VPC)	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations.

Fig 21: Test Instance with its Private IP Address



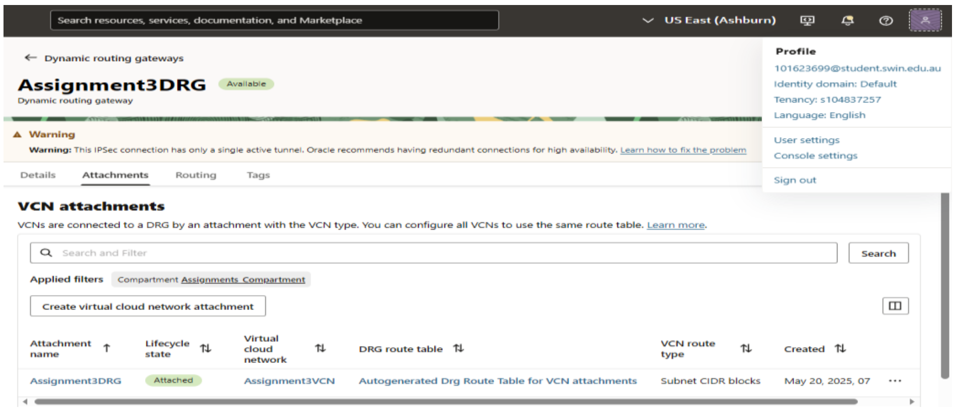
```
      _/m/'
Last login: Sat May 24 10:05:28 2025 from 18.206.107.29
[ec2-user@ip-10-0-2-242 ~]$ ping 10.0.4.68
PING 10.0.4.68 (10.0.4.68) 56(84) bytes of data.
64 bytes from 10.0.4.68: icmp_seq=1 ttl=127 time=0.463 ms
64 bytes from 10.0.4.68: icmp_seq=2 ttl=127 time=0.694 ms
64 bytes from 10.0.4.68: icmp_seq=3 ttl=127 time=0.442 ms
64 bytes from 10.0.4.68: icmp_seq=4 ttl=127 time=0.354 ms
64 bytes from 10.0.4.68: icmp_seq=5 ttl=127 time=0.728 ms
64 bytes from 10.0.4.68: icmp_seq=6 ttl=127 time=0.401 ms
64 bytes from 10.0.4.68: icmp_seq=7 ttl=127 time=0.765 ms
64 bytes from 10.0.4.68: icmp_seq=8 ttl=127 time=0.381 ms
64 bytes from 10.0.4.68: icmp_seq=9 ttl=127 time=0.515 ms
64 bytes from 10.0.4.68: icmp_seq=10 ttl=127 time=1.21 ms
64 bytes from 10.0.4.68: icmp_seq=11 ttl=127 time=0.350 ms
64 bytes from 10.0.4.68: icmp_seq=12 ttl=127 time=0.734 ms
^C
--- 10.0.4.68 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11471ms
rtt min/avg/max/mdev = 0.350/0.586/1.212/0.242 ms
[ec2-user@ip-10-0-2-242 ~]$ 
```

Fig 22: Successful ICMP ping from Bastion to Test Instance

IV. SITE-TO-SITE, TUNNELING AND VPN CONFIGURATION

A. On OCI

The first step to establish the VPN was to create a dummy AWS CGW and then create an OCI Dynamic Routing Gateway (DRG) (Fig 23) and attach it to the VCN. This DRG acts like a virtual router that can send traffic to other networks. Next, a Customer Premises Equipment (CPE) (Fig 24) object was created in OCI using a dummy AWS CGW's outside tunnel IP address. An IPsec connection was then formed between OCI and AWS using a shared secret. Finally, the private subnet route table was updated to send any traffic bound for 10.0.0.0/16 through the DRG (Fig 25). The tunnels that are interconnected have one that is not configured portrayed in Fig 26.



Search resources, services, documentation, and Marketplace — US East (Ashburn)

Profile
101623699@student.swin.edu.au
Identity domain: Default
Tenancy: s104837257
Language: English
User settings
Console settings
Sign out

← Dynamic routing gateways

Assignment3DRG — Available
Dynamic routing gateway

Warning
Warning: This IPSec connection has only a single active tunnel. Oracle recommends having redundant connections for high availability. Learn how to fix the problem

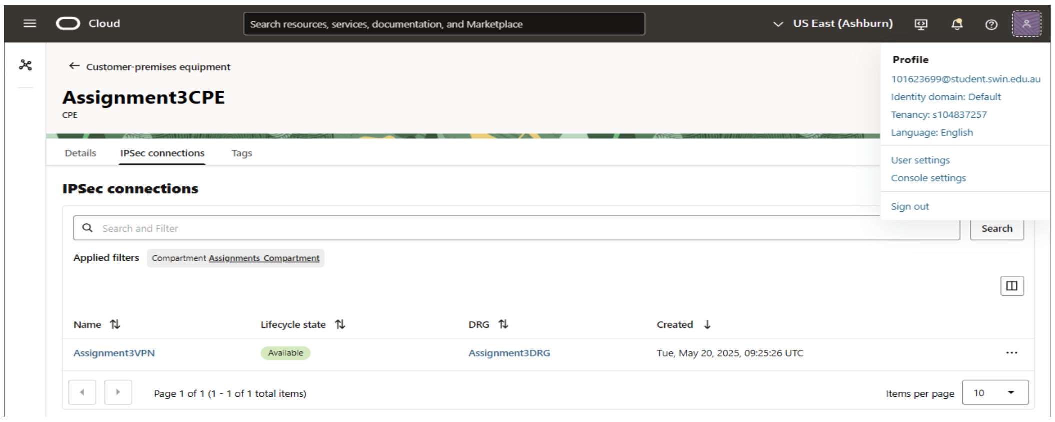
Details | Attachments | Routing | Tags

VCN attachments
VCNs are connected to a DRG by an attachment with the VCN type. You can configure all VCNs to use the same route table. Learn more.

Search and Filter — Search
Applied filters: Compartment Assignments_Compartment
Create virtual cloud network attachment

Attachment name	Lifecycle state	Virtual cloud network	DRG route table	VCN route type	Created
Assignment3DRG	Attached	Assignment3VCN	Autogenerated Drg Route Table for VCN attachments	Subnet CIDR blocks	May 20, 2025, 07

Fig 23: Assignment3DRG OCI DRG with VCN Attachment



Assignment3CPE
CPE

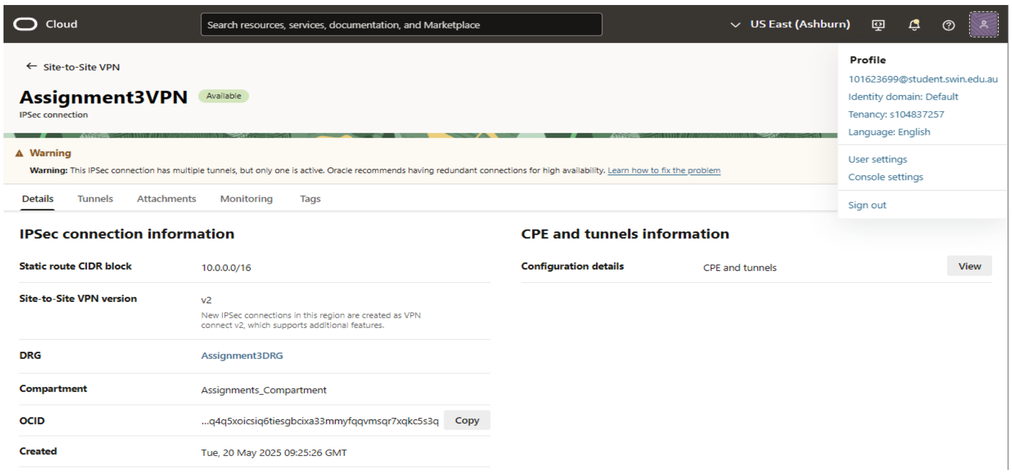
IPSec connections

Applied filters: Compartment Assignments_Compartment

Name	Lifecycle state	DRG	Created
Assignment3VPN	Available	Assignment3DRG	Tue, May 20, 2025, 09:25:26 UTC

Page 1 of 1 (1 - 1 of 1 total items) Items per page 10

Fig 24: Assignment3CPE OCI CPE with VPN and DRG Attachments



Assignment3VPN Available
IPSec connection

Warning
Warning: This IPSec connection has multiple tunnels, but only one is active. Oracle recommends having redundant connections for high availability. Learn how to fix the problem

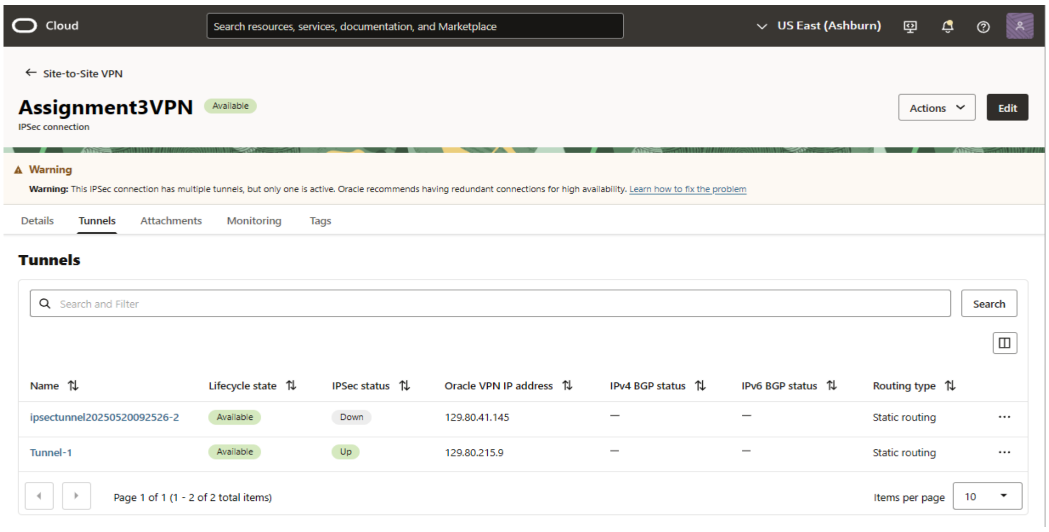
IPSec connection information

Static route CIDR block	10.0.0.0/16
Site-to-Site VPN version	v2 New IPSec connections in this region are created as VPN connect v2, which supports additional features.
DRG	Assignment3DRG
Compartment	Assignments_Compartment
OCID	...q4q5xoicsiq6tiesgbcixa33mmyfqqvmsqr7xqkc5s3q
Created	Tue, 20 May 2025 09:25:26 GMT

CPE and tunnels information

Configuration details	CPE and tunnels

Fig 25: Assignment3VPN OCI VPN with AWS CIDR Block



Assignment3VPN Available
IPSec connection

Warning
Warning: This IPSec connection has multiple tunnels, but only one is active. Oracle recommends having redundant connections for high availability. Learn how to fix the problem

Tunnels

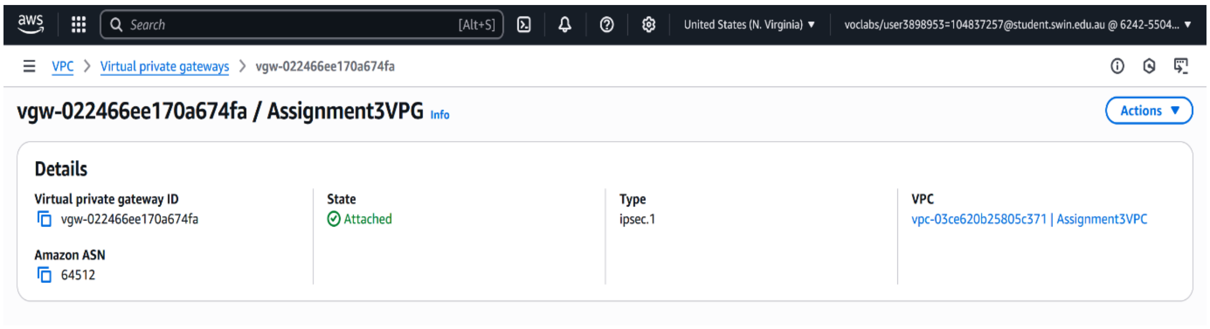
Name	Lifecycle state	IPSec status	Oracle VPN IP address	IPv4 BGP status	IPv6 BGP status	Routing type
ipsectunnel20250520092526-2	Available	Down	129.80.41.145	–	–	Static routing
Tunnel-1	Available	Up	129.80.215.9	–	–	Static routing

Page 1 of 1 (1 - 2 of 2 total items) Items per page 10

Fig 26: Assignment3VPN OCI Tunnel Setup (1 Down and 1 Up)

B. On AWS

In AWS, a Virtual Private Gateway (VGW) was created and attached to the VPC (Fig 27). A Customer Gateway (CGW) was then defined using the public IP of the OCI VPN endpoint (Fig 28). A VPN connection was established by combining the VGW and CGW with the same shared secret used on the OCI side. To complete the setup, the route table for the AWS private subnets was updated to forward traffic bound for 172.17.3.0/24 through the VPN tunnel. Tunnel status was confirmed to be "UP" on both sides through the AWS and OCI dashboards (Fig 29).



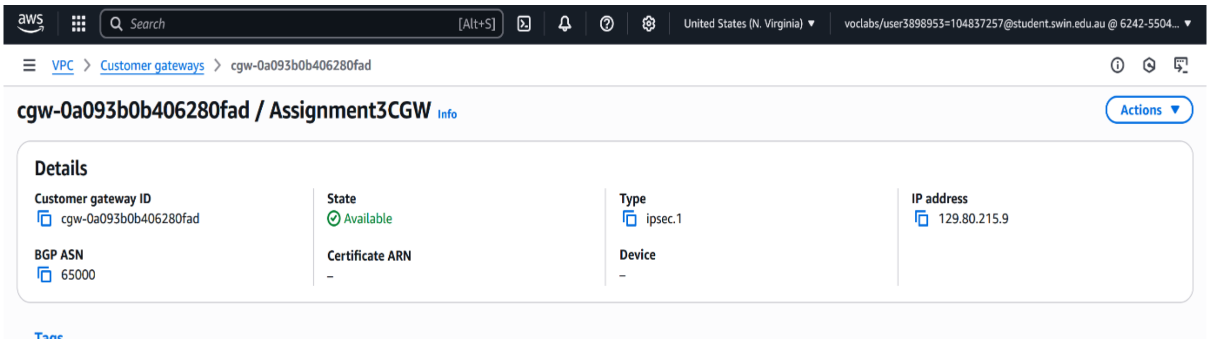
VPC > Virtual private gateways > vgw-022466ee170a674fa

vgw-022466ee170a674fa / Assignment3VPG

Details

Virtual private gateway ID	**State**	**Type**	**VPC**
vgw-022466ee170a674fa	Attached	ipsec.1	vpc-03ce620b25805c371 | Assignment3VPC
Amazon ASN			
64512			

Fig 27: Assignment3VPG with AWS VPG to VPC attachment



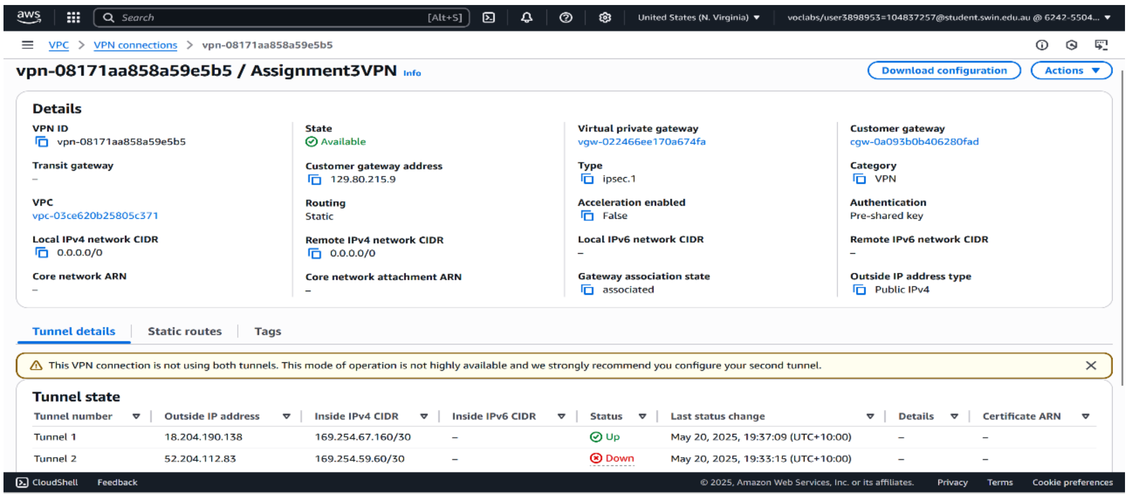
VPC > Customer gateways > cgw-0a093b0b406280fad

cgw-0a093b0b406280fad / Assignment3CGW

Details

Customer gateway ID	**State**	**Type**	**IP address**
cgw-0a093b0b406280fad	Available	ipsec.1	129.80.215.9
BGP ASN	**Certificate ARN**	**Device**	
65000	–	–	

Fig 28: Assignment3CGW with outside Public IP of the OCI side of the VPN tunnel



VPC > VPN connections > vpn-08171aa858a59e5b5

vpn-08171aa858a59e5b5 / Assignment3VPN

Details

VPN ID	**State**	**Virtual private gateway**	**Customer gateway**
vpn-08171aa858a59e5b5	Available	vgw-022466ee170a674fa	cgw-0a093b0b406280fad
Transit gateway	**Customer gateway address**	**Type**	**Category**
–	129.80.215.9	ipsec.1	VPN
VPC	**Routing**	**Acceleration enabled**	**Authentication**
vpc-03ce620b25805c371	Static	False	Pre-shared key
Local IPv4 network CIDR	**Remote IPv4 network CIDR**	**Local IPv6 network CIDR**	**Remote IPv6 network CIDR**
0.0.0.0/0	0.0.0.0/0	–	–
Core network ARN	**Core network attachment ARN**	**Gateway association state**	**Outside IP address type**
–	–	associated	Public IPv4

Tunnel details | Static routes | Tags

This VPN connection is not using both tunnels. This mode of operation is not highly available and we strongly recommend you configure your second tunnel.

Tunnel state

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Details	Certificate ARN
Tunnel 1	18.204.190.138	169.254.67.160/30	–	Up	May 20, 2025, 19:37:09 (UTC+10:00)	–	–
Tunnel 2	52.204.112.83	169.254.59.60/30	–	Down	May 20, 2025, 19:33:15 (UTC+10:00)	–	–

Fig 29: Assignment3VPN AWS Tunnel Setup (1 Down and 1 Up)

V. WEB APPLICATION DEPLOYMENT AND CONNECTIVITY

The PHP web application named photoalbum_v3.0 was deployed inside the EC2 instance under the /var/www/html/cos80001/photoalbum/ directory. The constants.php file was updated to use the private IP address of the OCI database, ensuring database traffic did not leave the VPN.

The application was tested by loading the album page via the public Elastic IP. It successfully displayed all images and their associated metadata from the MySQL database detailed as shown below in Fig 30.

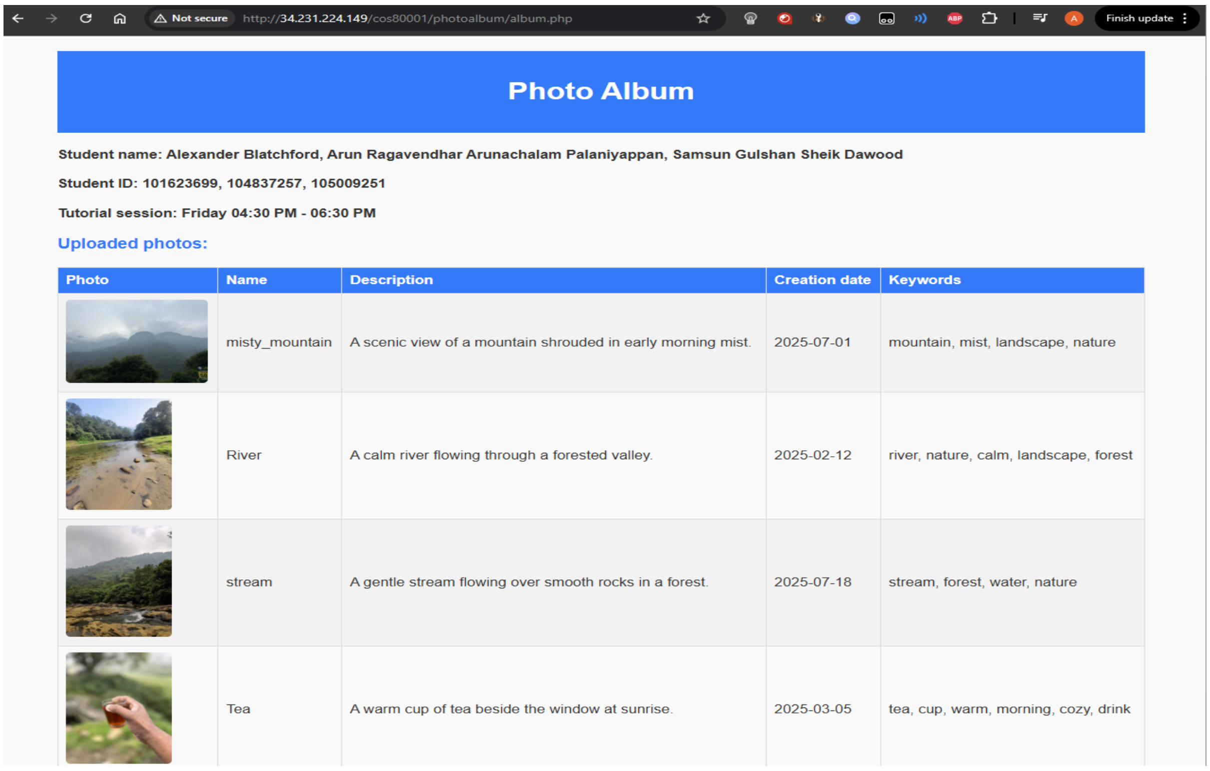


Photo Album

Student name: Alexander Blatchford, Arun Ragavendhar Arunachalam Palaniyappan, Samsun Gulshan Sheik Dawood

Student ID: 101623699, 104837257, 105009251

Tutorial session: Friday 04:30 PM - 06:30 PM

Uploaded photos:

Photo	Name	Description	Creation date	Keywords
	misty_mountain	A scenic view of a mountain shrouded in early morning mist.	2025-07-01	mountain, mist, landscape, nature
	River	A calm river flowing through a forested valley.	2025-02-12	river, nature, calm, landscape, forest
	stream	A gentle stream flowing over smooth rocks in a forest.	2025-07-18	stream, forest, water, nature
	Tea	A warm cup of tea beside the window at sunrise.	2025-03-05	tea, cup, warm, morning, cozy, drink

Fig 30: Web Deployment of photoalbum.php

VI. COMPARISON OF DIFFERENT VPN CONNECTION METHODS

To connect AWS and OCI, three options were considered: AWS Direct Connect, OCI FastConnect, and IPsec VPN.

AWS Direct Connect and OCI FastConnect both offer private network links between cloud platforms. These connections do not use the public internet—instead, they rely on a dedicated physical line provided through partners like Telstra, Equinix, or Megaport, connecting directly to the cloud provider's infrastructure. These private lines support bandwidth speeds ranging from 1 Gbps to 100 Gbps, depending on the service tier and provider. They are designed for low latency (as low as 1–5 ms) and high reliability, which is important for enterprise workloads like large datacentres, banks, and also for military/defense usages.

However, these private links are costly and complex to set up. For example, AWS Direct Connect charges can start from $0.25 to $0.30 per GB transferred, with monthly port fees ranging from $72 to $2,250, depending on speed. Setup can also take several weeks, as it may involve third-party coordination and physical access to colocation facilities. So, these options are not well suited for short-term academic, testing, or lightweight deployments.

IPsec VPN, on the other hand, creates a secure connection over the public internet. It uses encryption to protect all data during transmission, without needing physical infrastructure. It can be set up fully in software through the cloud provider’s console, with most connections ready in under an hour. While it does not offer guaranteed speeds or consistent latency—since it depends on internet conditions—it is completely free aside from regular data transfer costs, and provides enough security for non-production and small-scale use.

For this project, IPsec VPN was the most practical choice. It allowed safe, encrypted communication between AWS and OCI without any extra cost or delays. Since the goal was to build a working system for learning and testing as a part of the assignment, and not to run a high-traffic or business service, the added cost and complexity of Direct Connect or FastConnect were unnecessary. IPsec VPN provided exactly what was needed: a simple, fast, and secure way to connect the two clouds.

VII. CHALLENGES AND LEARNINGS

Some issues came up during the setup. The first problem was with the VPN connection. The tunnel could not be brought up at first, and traffic between AWS and OCI wasn't working. This was because the route tables in both clouds were missing the correct CIDR entries. After adding the proper routes and pointing them to the VPN gateways, the tunnel came up and the connection started working as expected.

Next, the AWS web server couldn't connect to the OCI MySQL database. This was due to a missing rule in the OCI default security list, which didn't allow ingress traffic on port 3306. Once the rule was added to allow traffic from the AWS subnet, the issue was resolved. There was also a problem with pinging the test instance in AWS. The pings failed because the NACL didn't have the inbound rules for ICMP. Since NACLs are stateless, both directions need to be set manually. This was fixed by updating the NACL and the test instance's Security Group. These problems helped the team understand how routing and security rules work differently in AWS and OCI, and the importance of allowing only the traffic that is needed as per system configuration.

VIII. CONCLUSION

This assignment successfully demonstrated how to build and deploy a working multi-cloud system using AWS and OCI. The web server and application were hosted on AWS, while the MySQL database, phpMyAdmin interface, and object storage were deployed on OCI. The two environments were connected using an IPsec VPN tunnel that allowed secure, private communication without using public access for database traffic.

Each part of the setup followed the least privilege principle, with only required ports and IPs allowed in all security components. All systems were tested for connectivity and access, including successful ICMP communication between subnets and secure data flow from the web application to the remote database. The deployment met all the project requirements and provided hands-on experience with setting up networks, routing, VPNs, firewalls, and cloud-based application hosting across two different platforms. The process also gave the team a clear understanding of how AWS and OCI differ in their network and security setups, and how to configure them to work together in a hybrid cloud setup. This experience will be valuable in future industry roles that involve working with cloud infrastructure and setting up secure, multi-cloud systems.

IX. REFERENCES

[1] Amazon Web Services, "AWS Site-to-Site VPN," *AWS Documentation*. [Online]. Available: https://docs.aws.amazon.com/vpn/latest/s2svpn/

[2] Oracle Cloud Infrastructure, "Setting Up an IPSec VPN," *OCI Documentation*. [Online]. Available: https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/settingupIPSec.htm

[3] Oracle Cloud Infrastructure, "Object Storage Overview," *OCI Documentation*. [Online]. Available: https://docs.oracle.com/en-us/iaas/Content/Object/Concepts/objectstorageoverview.htm

[4] Oracle Cloud Infrastructure, "OCI MySQL Database Service," *OCI Documentation*. [Online]. Available: https://docs.oracle.com/en-us/iaas/mysql-database/doc/index.html

[5] Amazon Web Services, "Elastic IP Addresses," *AWS Documentation*. [Online]. Available: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html