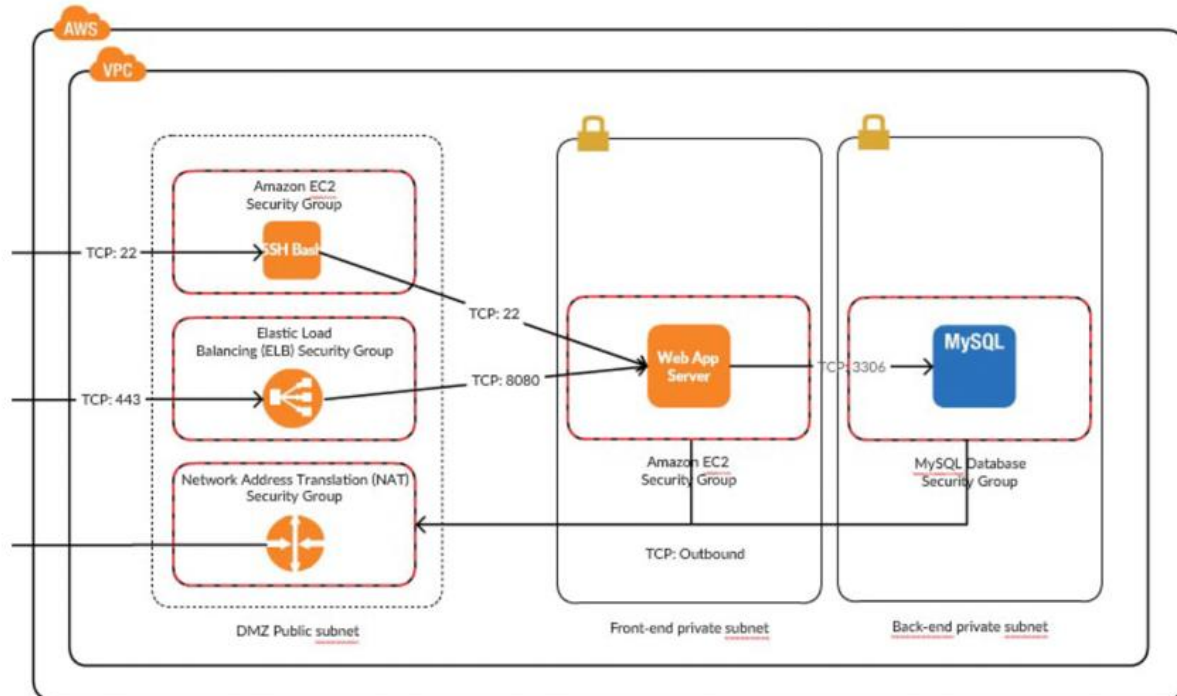


In this assignment, I have been asked to build this network, to get hands-on experience on AWS tools and services.



-Build the Network

1) Set Up the VPC:

Create a VPC with a CIDR block (10.0.0.0/16).

Create three subnets within the VPC:

1. **Public Subnet (DMZ Public subnet)** with a CIDR block like 10.0.1.0/24.
2. **Private Subnet (Front-end private subnet)** with a CIDR block like 10.0.2.0/24.
3. **Private Subnet (Back-end private subnet)** with a CIDR block like 10.0.3.0/24.

Subnets (10) Info					
Find resources by attribute or tag					
<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	public-subnet	subnet-09a20417b0994ab2b	Available	vpc-0e61b5aa1465bb399 my-...	10.0.5.0/24
<input type="checkbox"/>	Front-end-private-subnet	subnet-08312471dde4fa1eb	Available	vpc-0e61b5aa1465bb399 my-...	10.0.2.0/24
<input type="checkbox"/>	DMZ Public subnet	subnet-0fc4362c13141e776	Available	vpc-0e61b5aa1465bb399 my-...	10.0.1.0/24
<input type="checkbox"/>	Back-end-private-subnet	subnet-0fade7fd110abef9b	Available	vpc-0e61b5aa1465bb399 my-...	10.0.3.0/24
<input type="checkbox"/>	-	subnet-04673ad93c8d813e2	Available	vpc-03adcc3e6c4389f4e	172.31.0.0/24

*I will explain what the public-subnet is later.

2) Set Up the Internet Gateway:

- Attach an Internet Gateway (IGW) to the VPC.
- Add a route to the Public Subnet's Route Table to allow outbound traffic to the Internet through the IGW.

VPC > Internet gateways > igw-0626d52cb3c5aeaae

igw-0626d52cb3c5aeaae / my-IGW

Actions

Details Info

Internet gateway ID igw-0626d52cb3c5aeaae	State Attached	VPC ID vpc-0e61b5aa1465bb399 my-...	Owner 872515287506
--	-------------------	--	-----------------------

Tags Manage tags

Search tags

Key	Value
Name	my-IGW

Routes (2)				
Filter routes				
Destination	Target	Status	Propagated	
0.0.0.0/0	igw-0626d52cb3c5aeaae	Active	No	
10.0.0.0/16	local	Active	No	

3) Set Up the NAT Gateway:

- Create a NAT Gateway in the Public Subnet.
- Update the Route Table for the Private Subnet (Front-end) to allow outbound Internet access through the NAT Gateway.

4) Launch EC2 Instances:

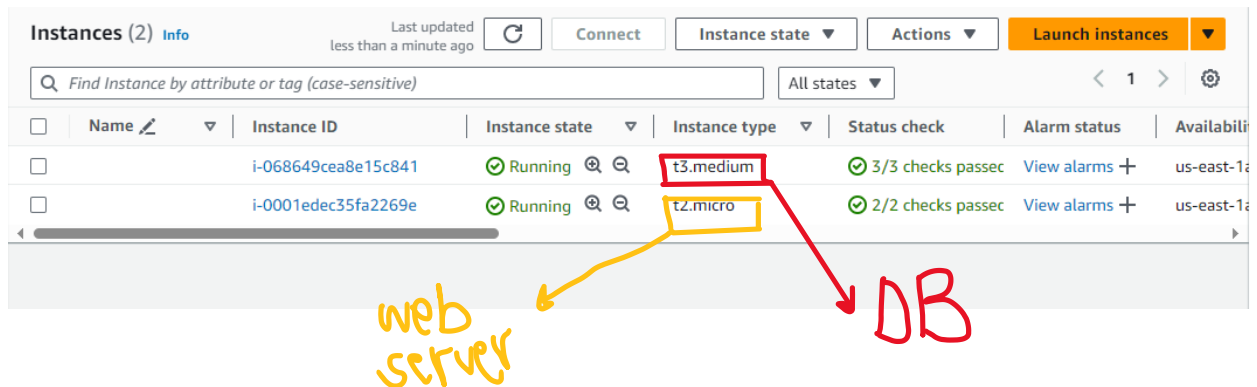
- **Launch a Web App Server** in the Front-end private subnet.

Install your web application on this instance.

Configure the security group to allow traffic from the ELB on port 8080.

- **Launch a MySQL Database Server** in the Back-end private subnet.

Configure the security group to allow traffic from the Web App Server on port 3306.




5) Set Up Security Groups:


- **Amazon EC2 Security Group:** Allow SSH access on port 22 and HTTP/HTTPS traffic from the ELB.
- **Elastic Load Balancer (ELB) Security Group:** Allow inbound traffic on port 443 (HTTPS) from the internet.
- **MySQL Security Group:** Allow inbound traffic on port 3306 from the Web App Server.


<input type="checkbox"/>	Name ▾	Security group ID ▾	Security group name ▾	VPC ID
<input type="checkbox"/>	-	sg-0906ec90eae48f079	MySQL Security Group	vpc-0e61b5aa1465bb399 🔗
<input type="checkbox"/>	-	sg-0ff75f120410bf547	default	vpc-03adcc3e6c4389f4e 🔗
<input type="checkbox"/>	-	sg-0f1b883db84b90937	ELB Security Group	vpc-0e61b5aa1465bb399 🔗
<input type="checkbox"/>	-	sg-03e6b1bf6d4c6e503	default	vpc-0e61b5aa1465bb399 🔗
<input type="checkbox"/>	-	sg-097cfd27d4512e7af	Amazon EC2 Security Group	vpc-0e61b5aa1465bb399 🔗

Amazon EC2 Security Group:

Details

Security group name
 Amazon EC2 Security Group

Security group ID
 [sg-097cfd27d4512e7af](#)

Description
 Allows only SSHs

VPC ID
 [vpc-0e61b5aa1465bb399](#)

Owner
 872515287506


Inbound rules count
 2 Permission entries

Outbound rules count
 1 Permission entry

[Inbound rules](#) | [Outbound rules](#) | [Tags](#)

Inbound rules (2)

 [Manage tags](#) [Edit inbound rules](#)

< 1 > 

<input type="checkbox"/>	Name ▾	Security group rule... ▾	IP version ▾	Type ▾	Protocol
<input type="checkbox"/>	-	sgr-05cfa51b6a90234bb	-	Custom TCP	TCP
<input type="checkbox"/>	-	sgr-0efbe87b141a526ce	IPv4	SSH	TCP

Edit inbound rules [Info](#)

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

Inbound rules [Info](#)

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
sgr-05cfa51b6a90234bb	<input type="text" value="Custom TCP"/>	<input type="text" value="TCP"/>	<input type="text" value="8080"/>	<input type="text" value="Cust..."/> <input type="text" value="Q"/>	<input type="text"/> Delete
sgr-0efbe87b141a526ce	<input type="text" value="SSH"/>	<input type="text" value="TCP"/>	<input type="text" value="22"/>	<input type="text" value="Cust..."/> <input type="text" value="Q"/> <input type="text" value="sg-0f1b883db84b90937"/> <input type="text" value="0.0.0.0/8"/>	<input type="text"/> Delete

Outbound rules [Info](#)

Security group rule ID	Type Info	Protocol Info	Port range Info	Destination Info
sgr-0dfeaaaf0294c09d07	<input type="text" value="All traffic"/>	<input type="text" value="All"/>	<input type="text" value="All"/>	<input type="text" value="Cust..."/> <input type="text" value="Q"/> <input type="text" value="0.0.0.0/0"/>

[Add rule](#)

Elastic Load Balancer (ELB) Security Group:

Security group name

ELB Security Group

Security group ID

sg-0f1b883db84b90937

Description

send to the webapp

VPC ID

vpc-0e61b5aa1465bb399

Owner

872515287506

Inbound rules count

3 Permission entries

Outbound rules count

1 Permission entry

Inbound rules

Outbound rules

Tags

Inbound rules (3)

Manage tags

Edit inbound rules

Search

< 1 >

	Name	Security group rule...	IP version	Type	Protocol
<input type="checkbox"/>	-	sgr-001cf28c57966dd81	IPv4	HTTPS	TCP
<input type="checkbox"/>	-	sgr-0a978d3549bd71c...	IPv4	All ICMP - IPv4	ICMP
<input type="checkbox"/>	-	sgr-0acf260825664bbe9	IPv4	HTTP	TCP

MySQL Security Group:

Edit inbound rules

Info

nbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules

Info

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-08aa6ef5cb27efdd1	MySQL/Aurora	TCP	3306	Cust...	

Add rule

sg-097cfd27d4512e7af

6)Set Up the Elastic Load Balancer (ELB):

- Create an ELB that spans the public subnet.
- Configure it to distribute traffic to the Web App Server(s) on port 8080.

EC2 > Load balancers

Load balancers (1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Filter load balancers

Name	DNS name	State	VPC ID	Availability Zones
MyWebApp-TargetGroup	MyWebApp-TargetGroup-...	Active	vpc-0e61b5aa1465bb...	2 Availability Zones

Load balancer type
Application

Scheme
Internet-facing

Status
Active

Hosted zone
Z35SXDOTRQ7X7K

VPC
[vpc-0e61b5aa1465bb399](#)

Availability Zones
[subnet-0fc4362c13141e776](#)
us-east-1a (use1-az4)
[subnet-09a20417b0994ab2b](#)
us-east-1b (use1-az6)

Load balancer IP address type
IPv4

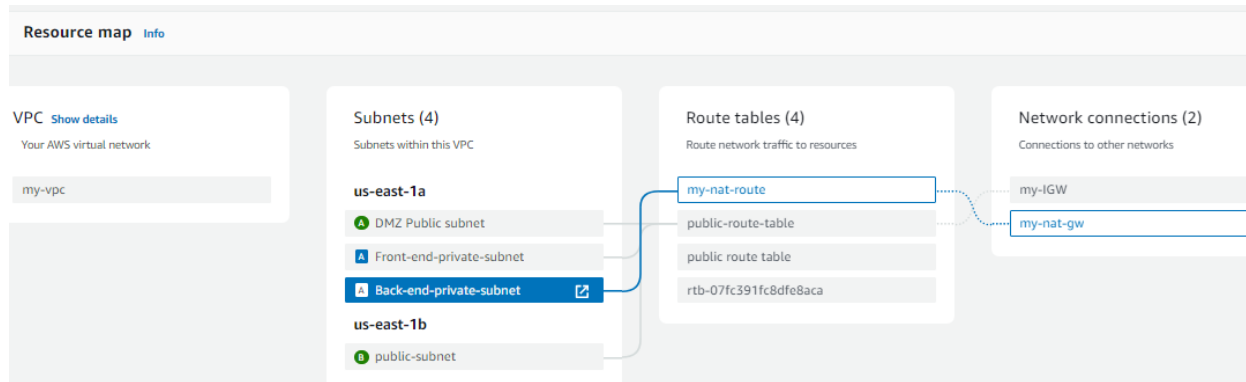
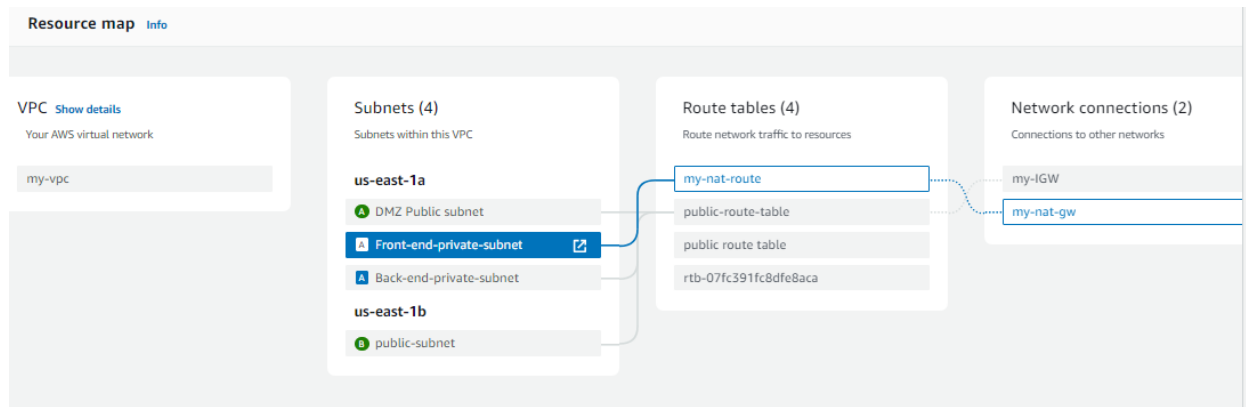
Date created
August 30, 2024, 03:30 (UTC+03:00)

Load balancer ARN
[arn:aws:elasticloadbalancing:us-east-1:872515287506:loadbalancer/app/MyWebApp-TargetGroup/77620511cd3eff20](#)

DNS name [Info](#)
[MyWebApp-TargetGroup-1068779005.us-east-1.elb.amazonaws.com](#)
(A Record)

The big picture of the resource map:





This one is created when louncing the load balancer, as at least two public subnet were required.

