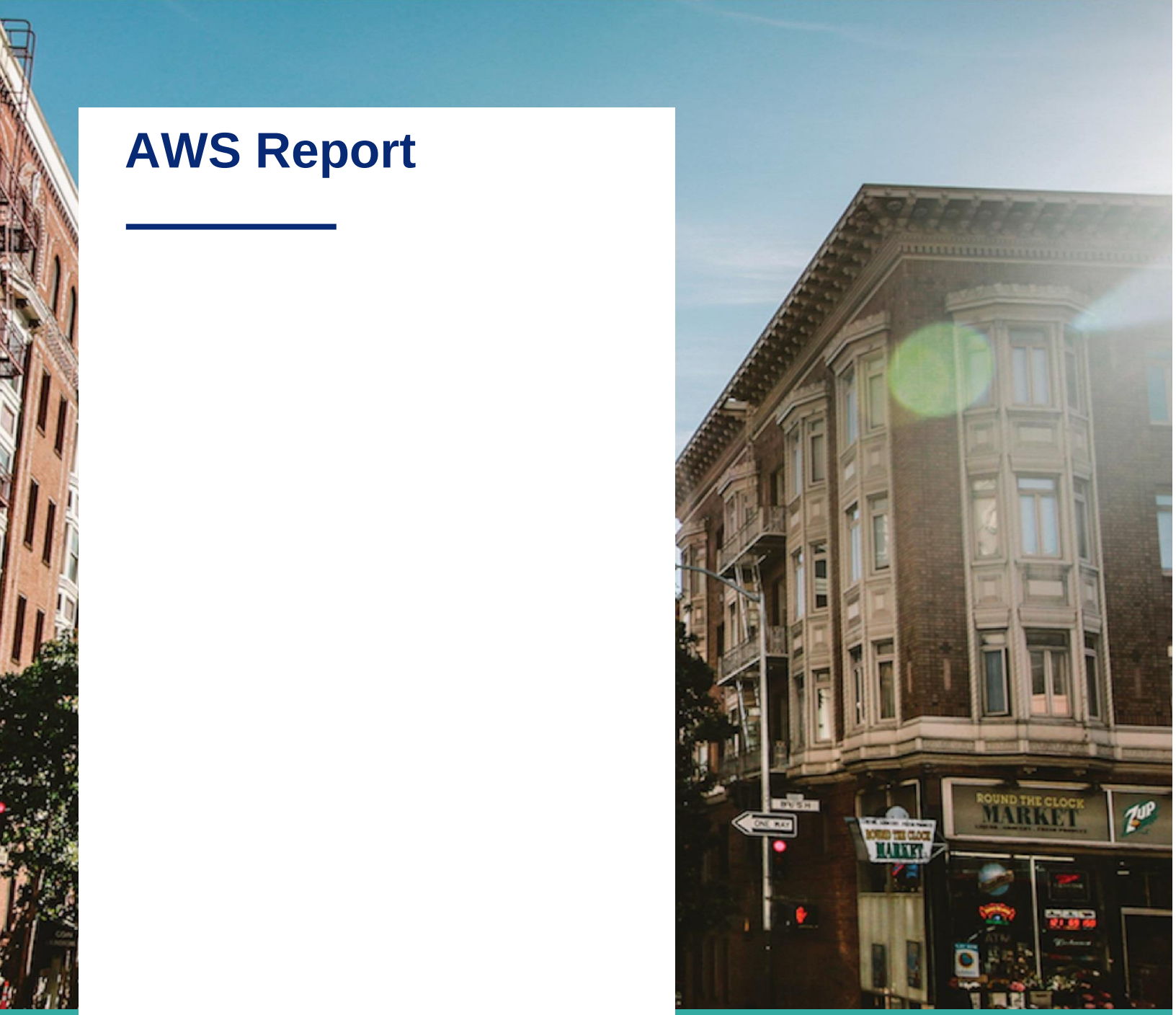
AWS Report



AUGUST 30

Authored by: Deya' Aldeen AL-Bettar

Table Content

1: Introduction.....3
2: Explanation.....4
3: Testing.....15

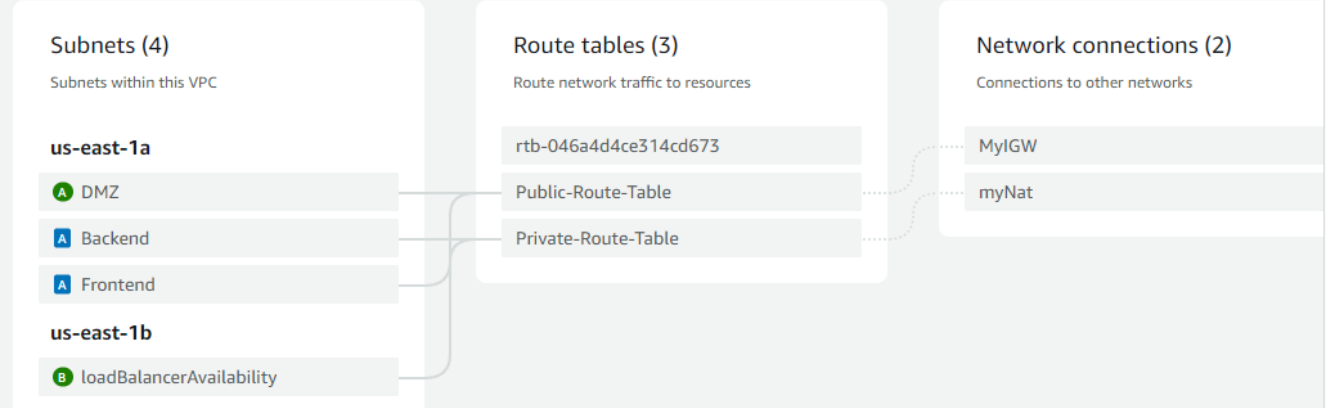
Introduction

The deployment of cloud-based applications demands a well-structured network architecture to ensure scalability, reliability, and security. This report outlines the process of designing and implementing a network architecture within the AWS cloud environment, incorporating public and private subnets, an Application Load Balancer (ALB), multiple EC2 instances for the web application, and an EC2 instance for database.

The primary focus of this task is to establish a functional and resilient infrastructure that effectively manages traffic, supports multiple instances of a web application, and ensures successful connectivity between the web application and the database. These efforts aim to demonstrate best practices in building and managing cloud-native applications.

Explanation

The resource map shows relationships between resources inside a VPC and how traffic flows from subnets to NAT gateways, internet gateway and gateway endpoints.
You can use the resource map to understand the architecture of My VPC, this resource map:

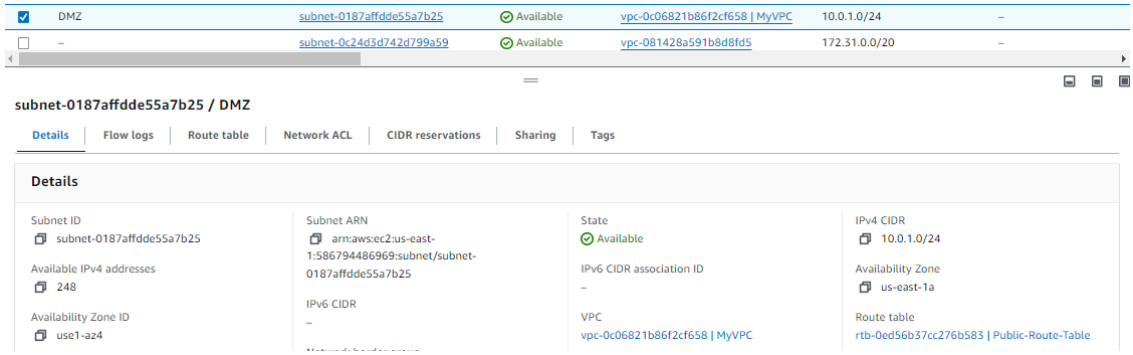


- **VPC**
  - The entire infrastructure is set up within a single VPC, providing isolation and control over the network environment.

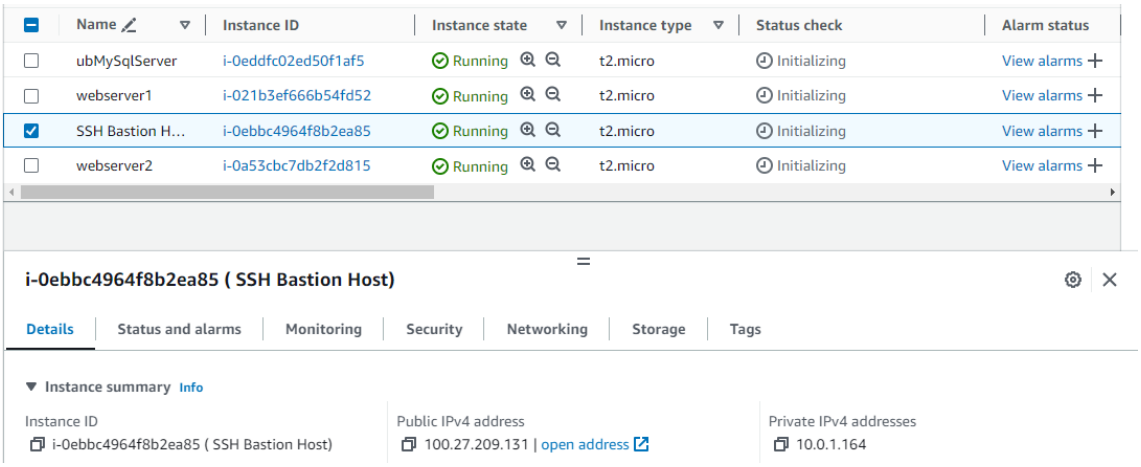
- **Subnets:** The VPC is divided into four subnets, each serving a specific purpose within the infrastructure.

Name	Subnet ID	State	VPC	IPv4
loadBalancerAvailability	subnet-06dee4b3708d7da1a	Available	vpc-0c06821b86f2cf658 | MyVPC	10.0.
Backend	subnet-037ea26527a8bdc75	Available	vpc-0c06821b86f2cf658 | MyVPC	10.0.
Frontend	subnet-04035b1ff3e87b4a6	Available	vpc-0c06821b86f2cf658 | MyVPC	10.0.
DMZ	subnet-0187affdde55a7b25	Available	vpc-0c06821b86f2cf658 | MyVPC	10.0.

- **DMZ Public Subnet:**

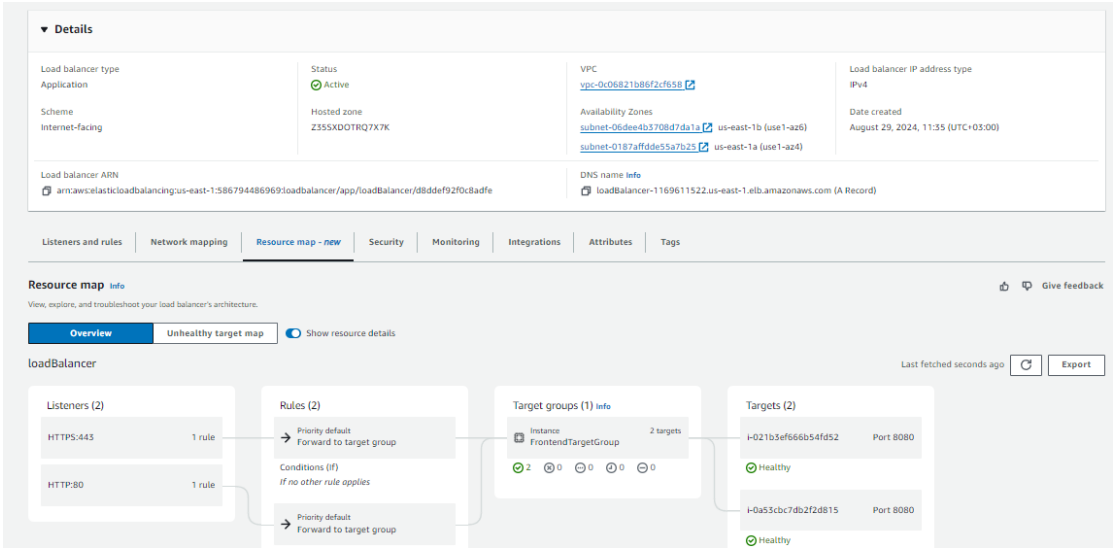


  - **Purpose:** To host resources that need to be exposed to the public internet.
  - **Components:**
    - **SSH EC2 Instance**

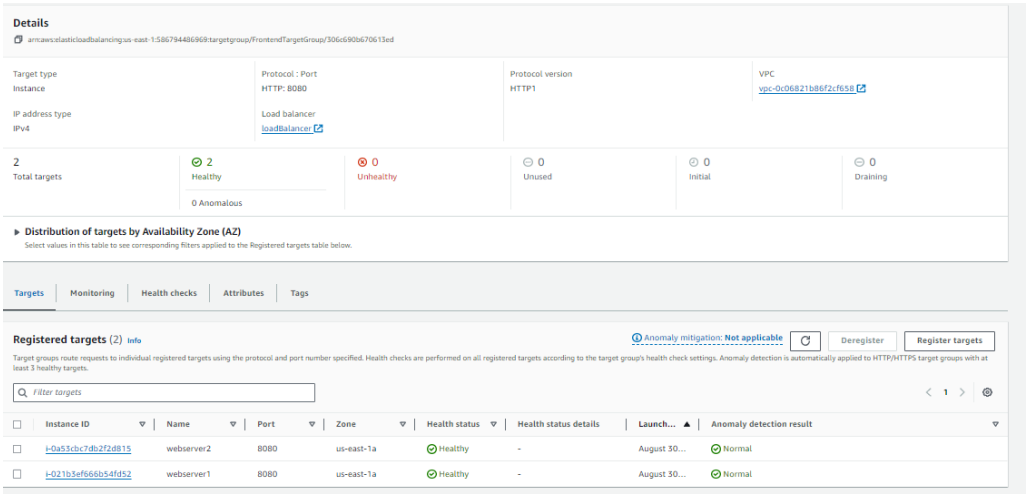


      - **Purpose:** To manage and connect to web servers in the private subnets.
      - **Instance Type:** [Specify instance type, e.g., t2.micro]
      - **Security Group:** Configured to allow SSH access from specific IP addresses.

- **Elastic Load Balancer (ELB)**



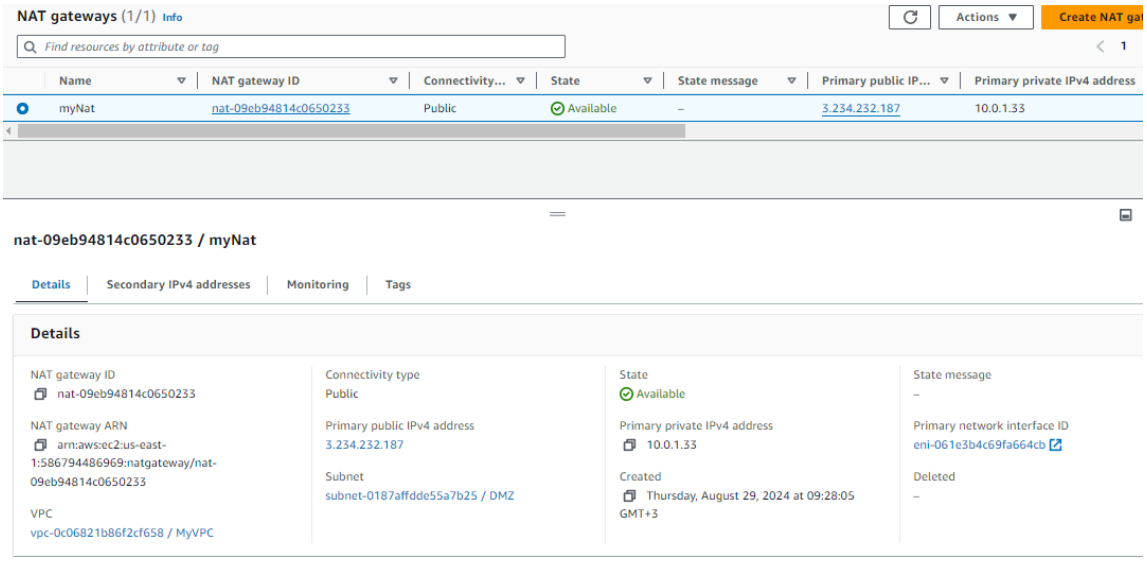
  - **Purpose:** To distribute incoming traffic across multiple web servers, ensuring high availability and fault tolerance.
  - **ELB Type:** Application Load Balancer
  - **Listeners:** Configured to listen on port 80 (HTTP) and port 443 (HTTPS) with Certificated Manger.
  - **Target Group:**



    - **Name**: `frontedTargetGroup`
    - **Function:** A Target Group is a logical grouping of instances (or targets) that the Load Balancer routes traffic to. It defines how the Load Balancer should distribute traffic among the targets.

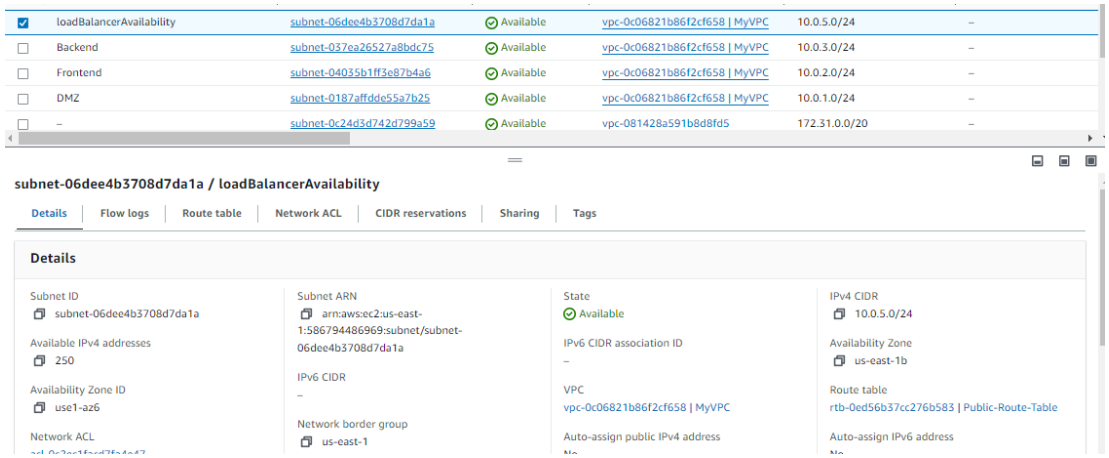
- **Purpose:** Ensures that incoming requests are efficiently distributed across the instances in the group, helping to balance the load and improve performance.

- **NAT Gateway**



- **Purpose:** To enable instances in private subnets (Frontend and Backend) to initiate outbound connections to the internet (e.g., for software updates) while preventing inbound traffic from the internet.

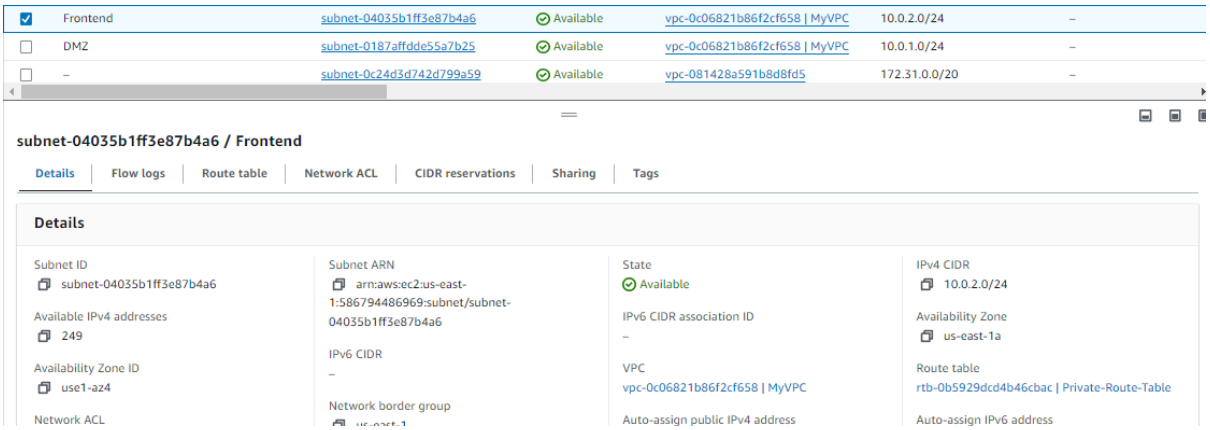
- **Load Balancer Availability Public Subnet:**



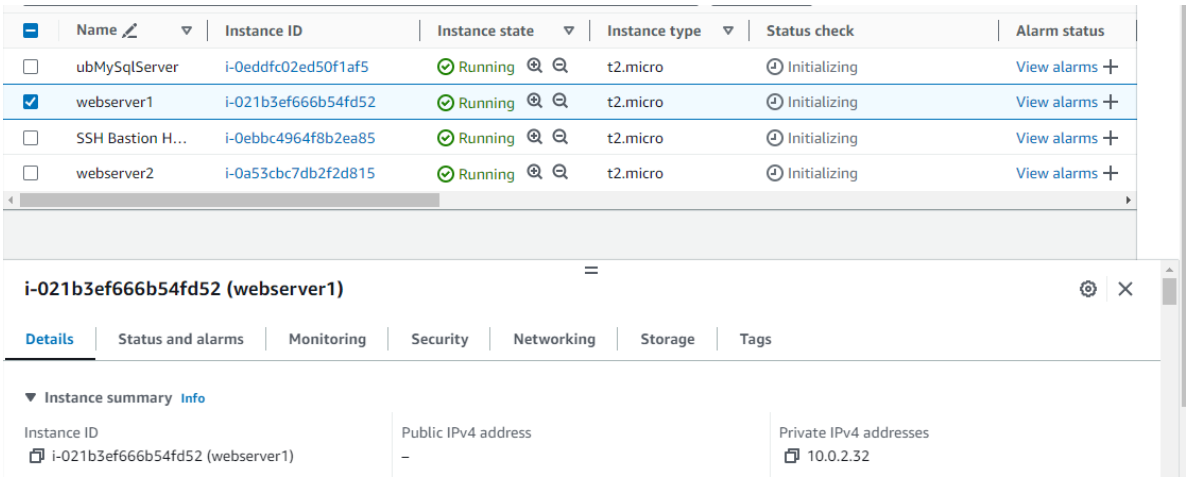
- **Purpose:** AWS Load Balancers require deployment across at least two Availability Zones (AZs) to ensure optimal functionality and reliability.This setup is crucial for enhancing the resilience and availability of your application. By distributing traffic across instances in different AZs, the

load balancer ensures that your application remains highly available and responsive, even in the event of an AZ failure.

- **Frontend Private Subnet:**



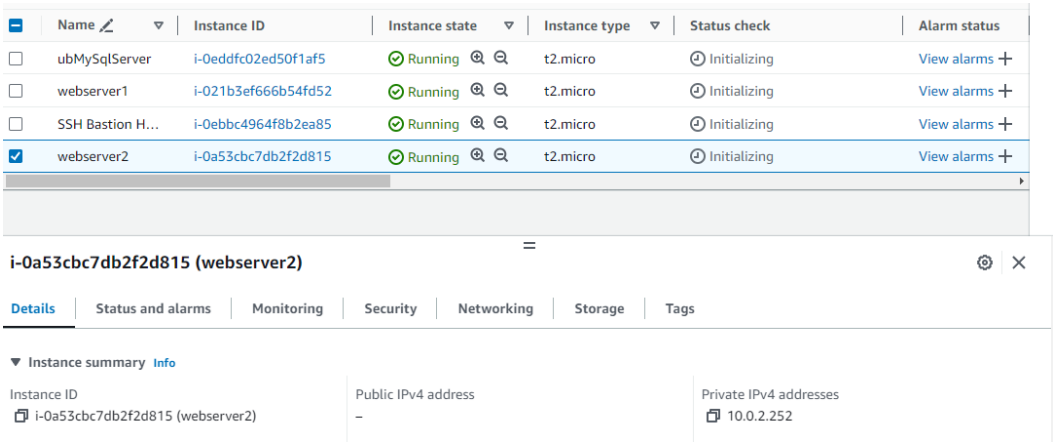
  - **Purpose:** The Frontend Private Subnet is used to house the instances (such as web servers or application servers) that handle the application logic and user requests. These instances are not directly exposed to the internet but are accessible through a Load Balancer that is placed in a public subnet.
  - **Location:** This subnet is within the private network space of your Virtual Private Cloud (VPC) and is typically configured to be isolated from direct internet access for security reasons.
  - **Components:**
    - **Web Server1**



      - **Purpose:** To host the web application.

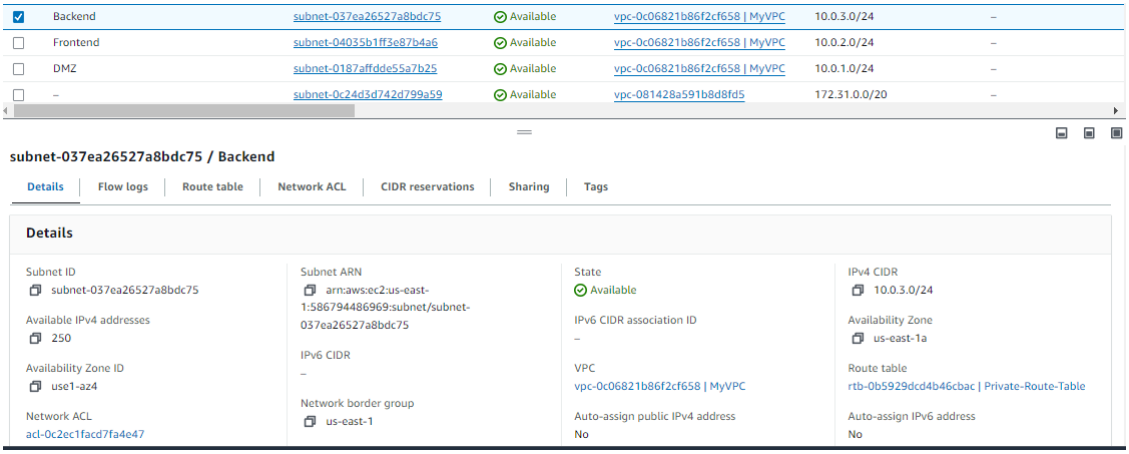
- **Configuration:**
  - Instances are part of private subnets and are not directly accessible from the internet.
  - Traffic is routed through the ELB for inbound requests.
  - Security Groups: Configured to allow traffic only from the ELB and the SSH instance.

- **WebServer2**

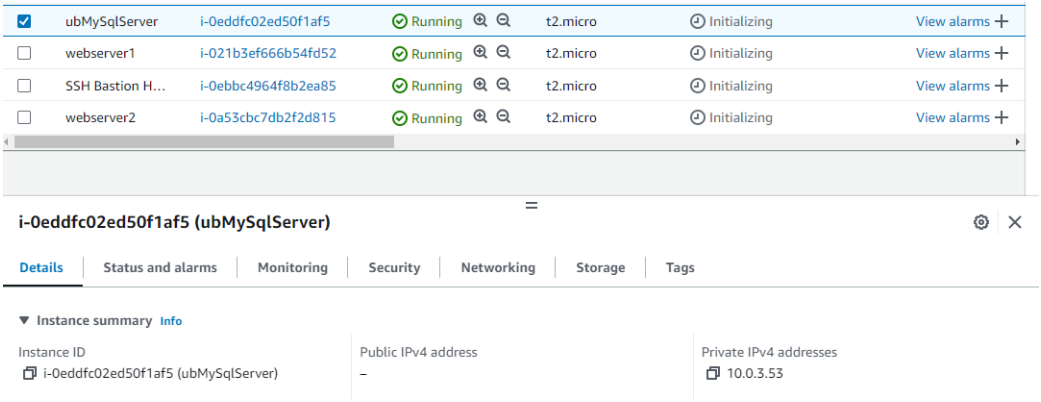


  - **Purpose:** To host the web application.
  - **Configuration:**
    - Instances are part of private subnets and are not directly accessible from the internet.
    - Traffic is routed through the ELB for inbound requests.
    - Security Groups: Configured to allow traffic only from the ELB and the SSH instance.

- **Backend Private Subnet:**

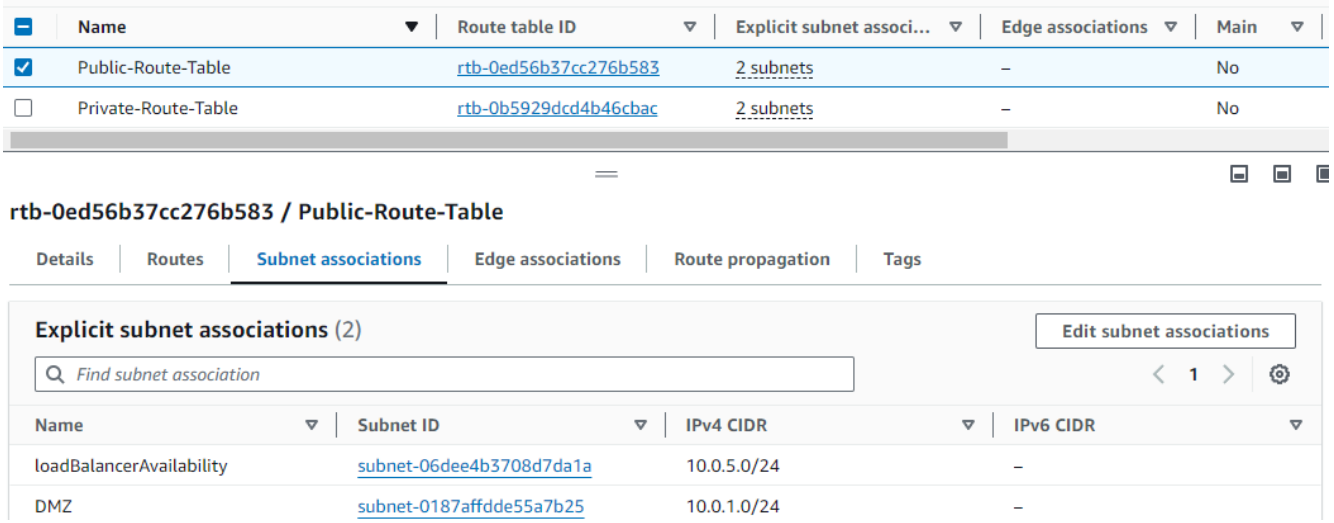


  - **Purpose**: The Backend Private Subnet is designed to host resources such as databases, internal application services, or other backend systems that need to remain secure and are not directly exposed to external traffic. This setup helps in maintaining a clear separation of concerns between frontend-facing components and backend data storage or processing systems.
  - **Location:** This subnet is part of your Virtual Private Cloud (VPC) but is isolated from direct internet access to enhance security.
  - **Components:**
    - **MySql Server**



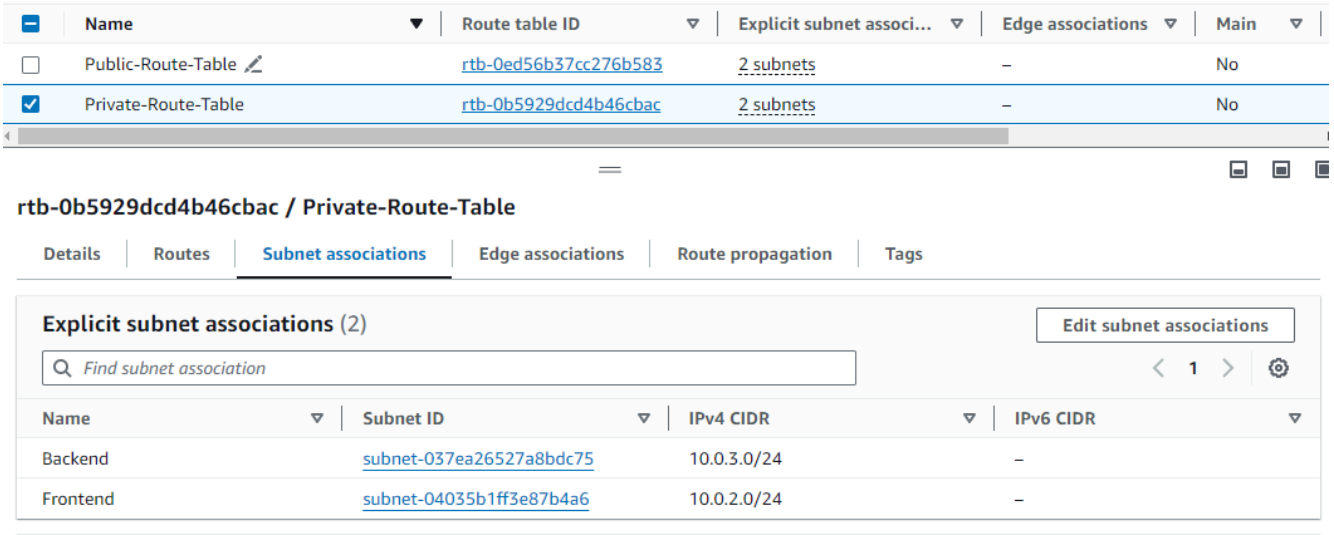
      - **Purpose:** To store application data.
      - **Configuration:**
        - Hosted in a backend private subnet.
        - Security Groups: Configured to allow traffic only from the web servers and the NAT Gateway.

- **Route tables:**
  - **Public Route Table (for DMZ and load balancer availability subnet):**



    - **Purpose:** Allows instances in the public subnet (DMZ) to communicate directly with the internet via the Internet Gateway.

  - **Private Route Table (for Frontend and Backend subnet)**

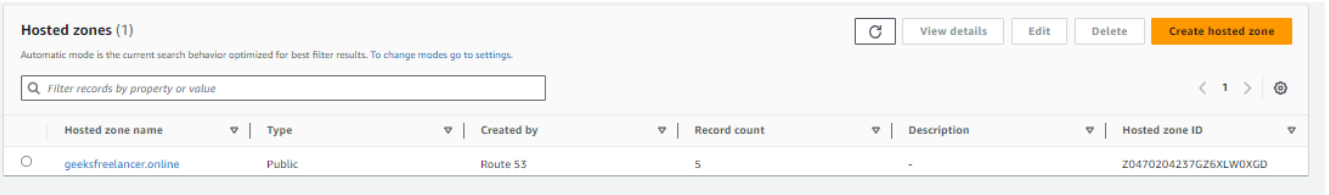


    - **Purpose:** Allows instances in the private subnet to access the internet for updates or downloads via the NAT Gateway, but prevents direct inbound internet access.

- **DNS Configuration and SSL/TLS Setup:** For domain management, I will use a domain registered with Hostinger, avoiding the need to purchase a new domain from Amazon, which is priced higher. Hostinger offers domain registration at a significantly lower cost, with some domains available for as little as $0.99 compared to Amazon's minimum price of $14. To integrate this domain with AWS, I will update the name server settings in Hostinger to point to Amazon's servers. Additionally, SSL/TLS certificates will be configured to ensure secure communication.

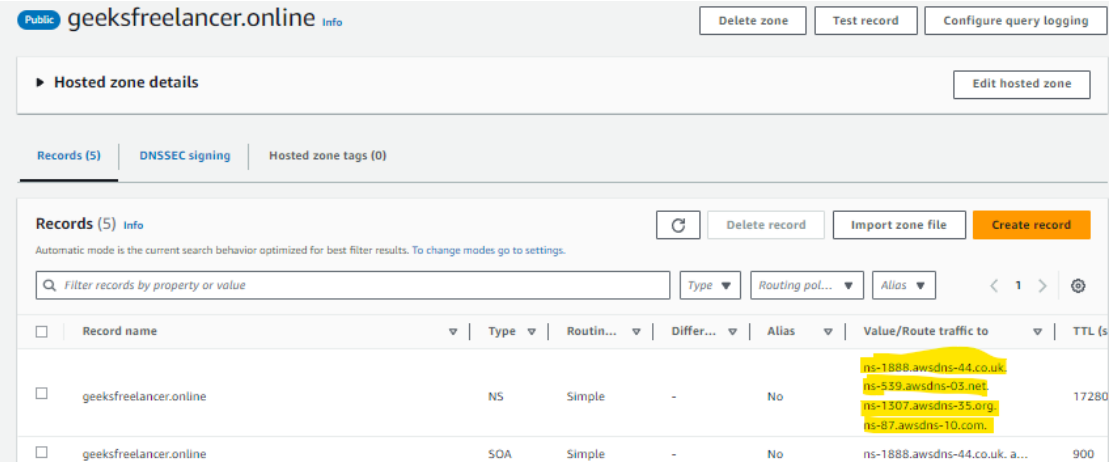
1. Route 53 Hosted Zone Configuration:

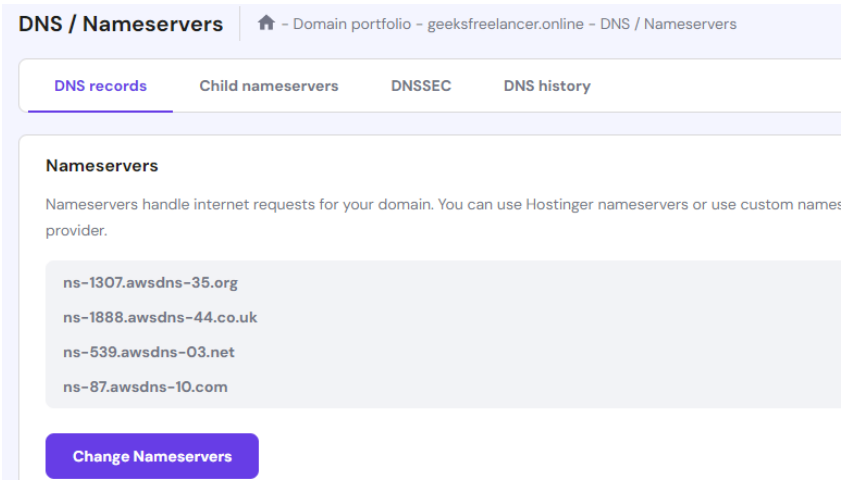
- **Create Hosted Zone:**



  - A new hosted zone was created in Amazon Route 53 for the domain `geeksfreelancer.online`.
  - This hosted zone manages DNS records for the domain, enabling it to route traffic to the appropriate resources.

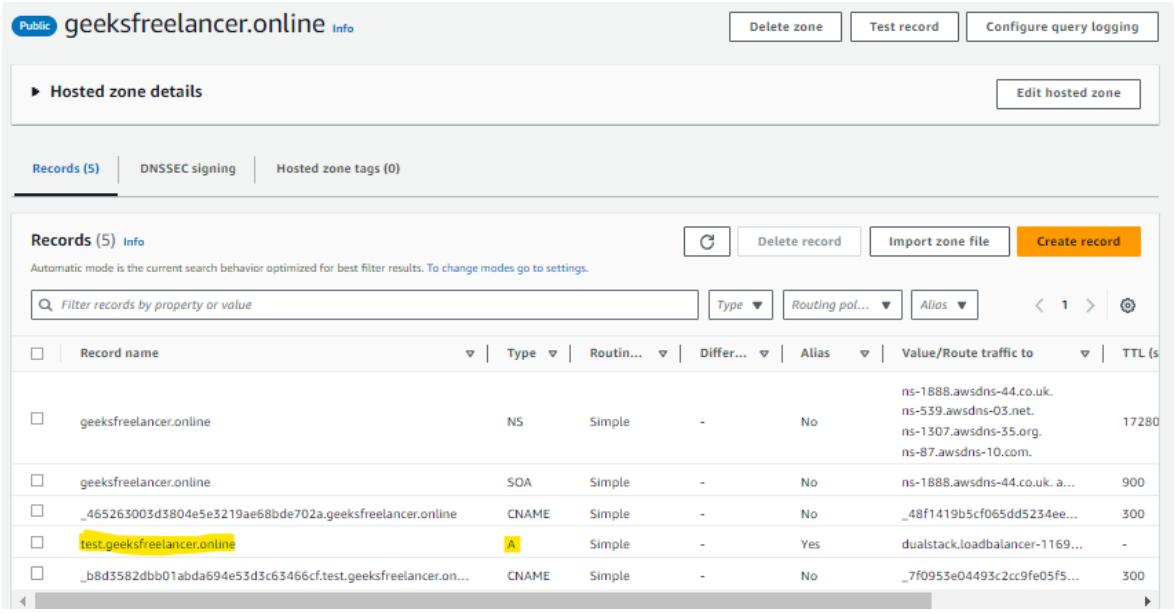
- **Retrieve Name Servers:**





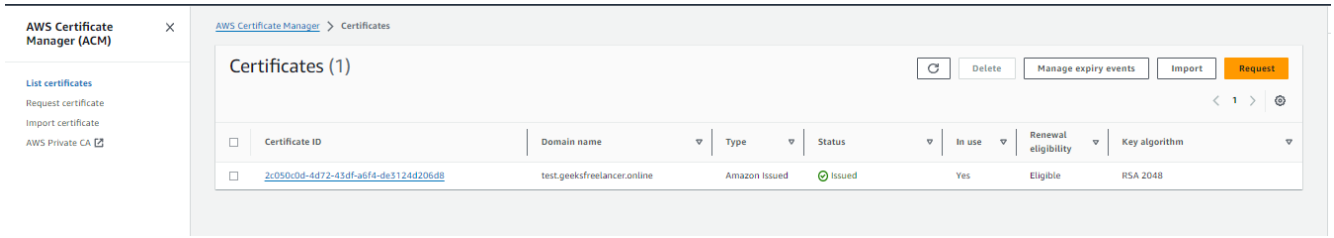
- Amazon Route 53 provided a set of name servers for the hosted zone. These name servers were configured in the domain registrar's settings (Hostinger) to point to Route 53's DNS service.

2. Adding an A Record:



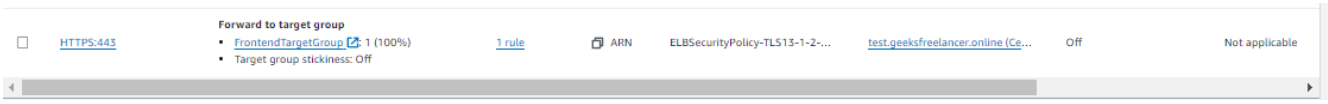
- **Configure DNS Record:**
  - An A record was added to the Route 53 hosted zone for `test.geeksfreelancer.online`.
  - This A record points to the public DNS name of the Elastic Load Balancer (ELB), allowing traffic directed to `test.geeksfreelancer.online` to be distributed across the backend servers managed by the ELB.

3. SSL/TLS Certificate Setup:



- **Obtain SSL/TLS Certificate:**
  - An SSL/TLS certificate was obtained from AWS Certificate Manager (ACM) for the domain `test.geeksfreelancer.online`.
  - This certificate enables HTTPS on the load balancer, ensuring secure, encrypted connections between users and the web application.

- **Associate Certificate with Load Balancer:**



  - The SSL/TLS certificate was associated with the Elastic Load Balancer, enabling HTTPS for `test.geeksfreelancer.online`.
  - This configuration ensures that all traffic between clients and the load balancer is encrypted and secure.

Testing

To ensure that the architecture is functioning as expected, I performed the following testing steps:

- **SSH Access to the SSH Bastion Host**

```
user@DESKTOP-IE2HST9:~/deaa$ ssh -i "ssh.pem" ec2-user@100.27.209.131
The authenticity of host '100.27.209.131 (100.27.209.131)' can't be established.
ED25519 key fingerprint is SHA256:2cPNfXmZ25e9vQ2NNvlSs7Vw6qC+Phz9O2gDOEgA5Y4.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '100.27.209.131' (ED25519) to the list of known hosts.
       #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Thu Aug 29 13:18:05 2024 from 176.28.150.243
[ec2-user@ip-10-0-1-164 ~]$
```

Keys in SSH Bastion Host:

```
[ec2-user@ip-10-0-1-164 ~]$ ls
webserver1.pem  webserver2.pem
[ec2-user@ip-10-0-1-164 ~]$
```

- **Connect to Web Server 1 from SSH Bastion Host:**

```
[ec2-user@ip-10-0-1-164 ~]$ ssh -i webserver1.pem ubuntu@10.0.2.32
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1012-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Fri Aug 30 11:58:22 UTC 2024

  System load:  0.0               Processes:             112
  Usage of /:   30.7% of 6.71GB   Users logged in:       0
  Memory usage: 24%               IPv4 address for enX0: 10.0.2.32
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

81 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


*** System restart required ***
Last login: Thu Aug 29 14:09:14 2024 from 10.0.1.164
ubuntu@ip-10-0-2-32:~$
```

- **Test Internet Connectivity from Web Server 1**

```
ubuntu@ip-10-0-2-32:~$ ping google.com
PING google.com (172.253.122.100) 56(84) bytes of data.
64 bytes from bh-in-f100.1e100.net (172.253.122.100): icmp_seq=1 ttl=55 time=2.92 ms
64 bytes from bh-in-f100.1e100.net (172.253.122.100): icmp_seq=2 ttl=55 time=2.45 ms
64 bytes from bh-in-f100.1e100.net (172.253.122.100): icmp_seq=3 ttl=55 time=2.46 ms
64 bytes from bh-in-f100.1e100.net (172.253.122.100): icmp_seq=4 ttl=55 time=2.51 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.451/2.586/2.921/0.194 ms
```

- **Test MySQL Connectivity from Web Server 1**

```
ubuntu@ip-10-0-2-32:~$ mysql -h 10.0.3.53 -P 3306 -u deaa -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.39-0ubuntu0.24.04.2 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

- **Connect to Web Server 2 from SSH Bastion Host:**

```
[ec2-user@ip-10-0-1-164 ~]$ ssh -i "webserver2.pem" ec2-user@10.0.2.252
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Thu Aug 29 13:47:46 2024 from 10.0.1.164
[ec2-user@ip-10-0-2-252 ~]$
```

- **Test Internet Connectivity from Web Server 2**

```
[ec2-user@ip-10-0-2-252 ~]$ ping google.com
PING google.com (172.253.122.138) 56(84) bytes of data.
64 bytes from bh-in-f138.1e100.net (172.253.122.138): icmp_seq=1 ttl=57 time=2.70 ms
64 bytes from bh-in-f138.1e100.net (172.253.122.138): icmp_seq=2 ttl=57 time=2.14 ms
64 bytes from bh-in-f138.1e100.net (172.253.122.138): icmp_seq=3 ttl=57 time=2.09 ms
64 bytes from bh-in-f138.1e100.net (172.253.122.138): icmp_seq=4 ttl=57 time=2.08 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 2.080/2.253/2.701/0.259 ms
[ec2-user@ip-10-0-2-252 ~]$
```

- **Connect to MySql Server from SSH Bastion Host:** here I used webserver2 key also for MySql server

```
[ec2-user@ip-10-0-1-164 ~]$ ssh -i "webserver2.pem" ubuntu@10.0.3.53
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1012-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Fri Aug 30 12:14:44 UTC 2024

  System load:  0.0               Processes:             104
  Usage of /:   36.8% of 6.71GB   Users logged in:       0
  Memory usage: 59%               IPv4 address for enX0: 10.0.3.53
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

81 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


*** System restart required ***
Last login: Thu Aug 29 13:20:06 2024 from 10.0.1.164
ubuntu@ip-10-0-3-53:~$
```

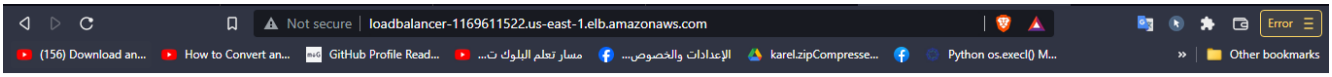
```
ubuntu@ip-10-0-3-53:~$ sudo systemctl status mysql
● mysql.service - MySQL Community Server
     Loaded: loaded (/usr/lib/systemd/system/mysql.service; enabled; preset: enabled)
     Active: active (running) since Fri 2024-08-30 09:16:47 UTC; 2h 58min ago
   Main PID: 10170 (mysqld)
     Status: "Server is operational"
      Tasks: 38 (limit: 1130)
     Memory: 364.4M (peak: 391.0M)
        CPU: 39.267s
     CGroup: /system.slice/mysql.service
             └─10170 /usr/sbin/mysqld

Aug 30 09:16:46 ip-10-0-3-53 systemd[1]: Starting mysql.service - MySQL Community Server...
Aug 30 09:16:47 ip-10-0-3-53 systemd[1]: Started mysql.service - MySQL Community Server.
ubuntu@ip-10-0-3-53:~$
```

- Test Internet Connectivity from MySql Server

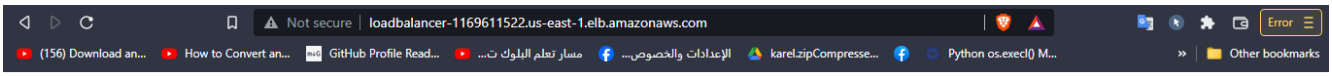
```
ubuntu@ip-10-0-3-53:~$ ping google.com
PING google.com (142.251.16.102) 56(84) bytes of data.
64 bytes from bl-in-f102.1e100.net (142.251.16.102): icmp_seq=1 ttl=57 time=2.09 ms
64 bytes from bl-in-f102.1e100.net (142.251.16.102): icmp_seq=2 ttl=57 time=1.68 ms
64 bytes from bl-in-f102.1e100.net (142.251.16.102): icmp_seq=3 ttl=57 time=1.66 ms
64 bytes from bl-in-f102.1e100.net (142.251.16.102): icmp_seq=4 ttl=57 time=1.62 ms
64 bytes from bl-in-f102.1e100.net (142.251.16.102): icmp_seq=5 ttl=57 time=1.63 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.616/1.733/2.085/0.177 ms
ubuntu@ip-10-0-3-53:~$
```

- **Test Web Accessibility via Load Balancer DNS:** we using this loadBalancer-1169611522.us-east-1.elb.amazonaws.com



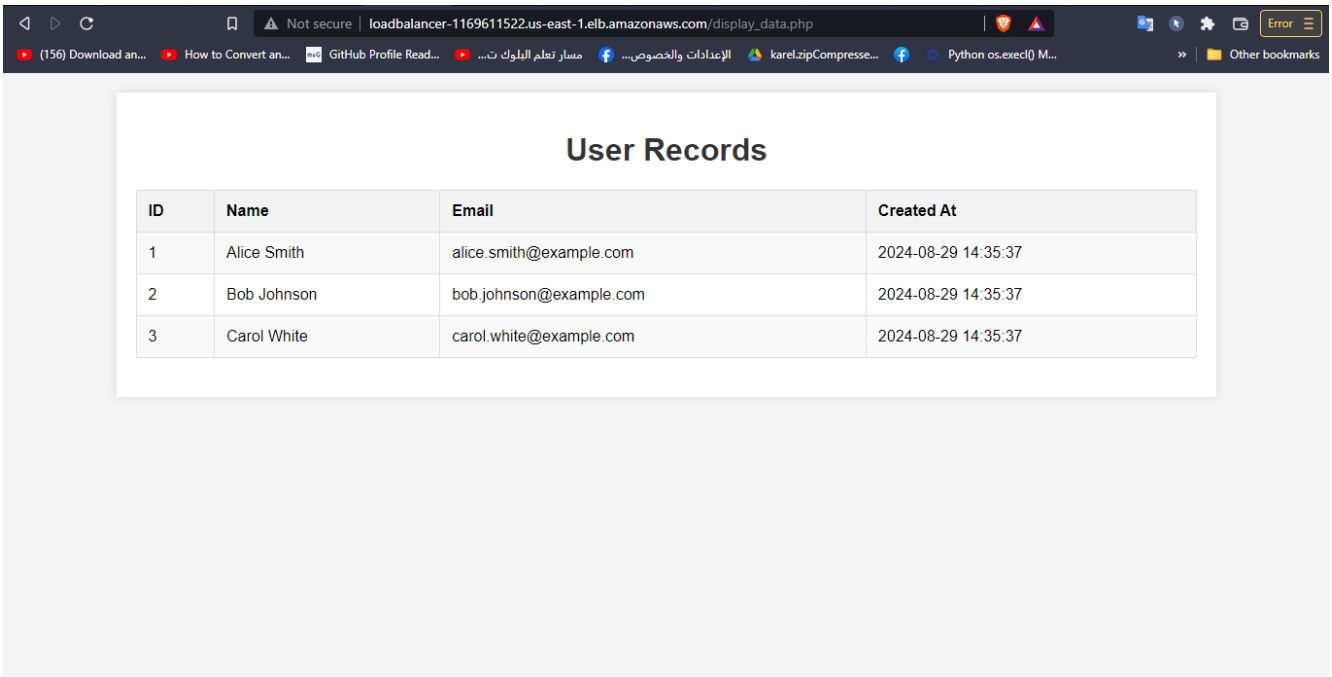
Welcome to Apache Server

Private IP Address:10.0.2.32:8080



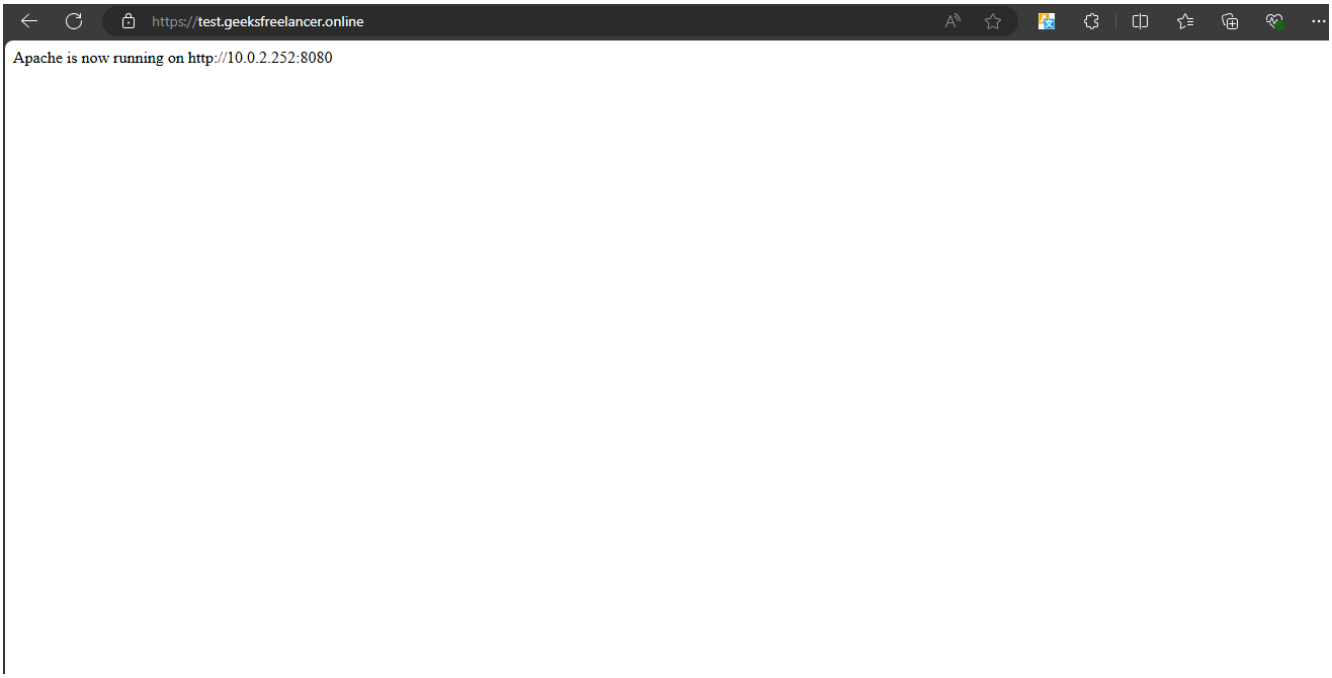
Apache is now running on http://10.0.2.252:8080

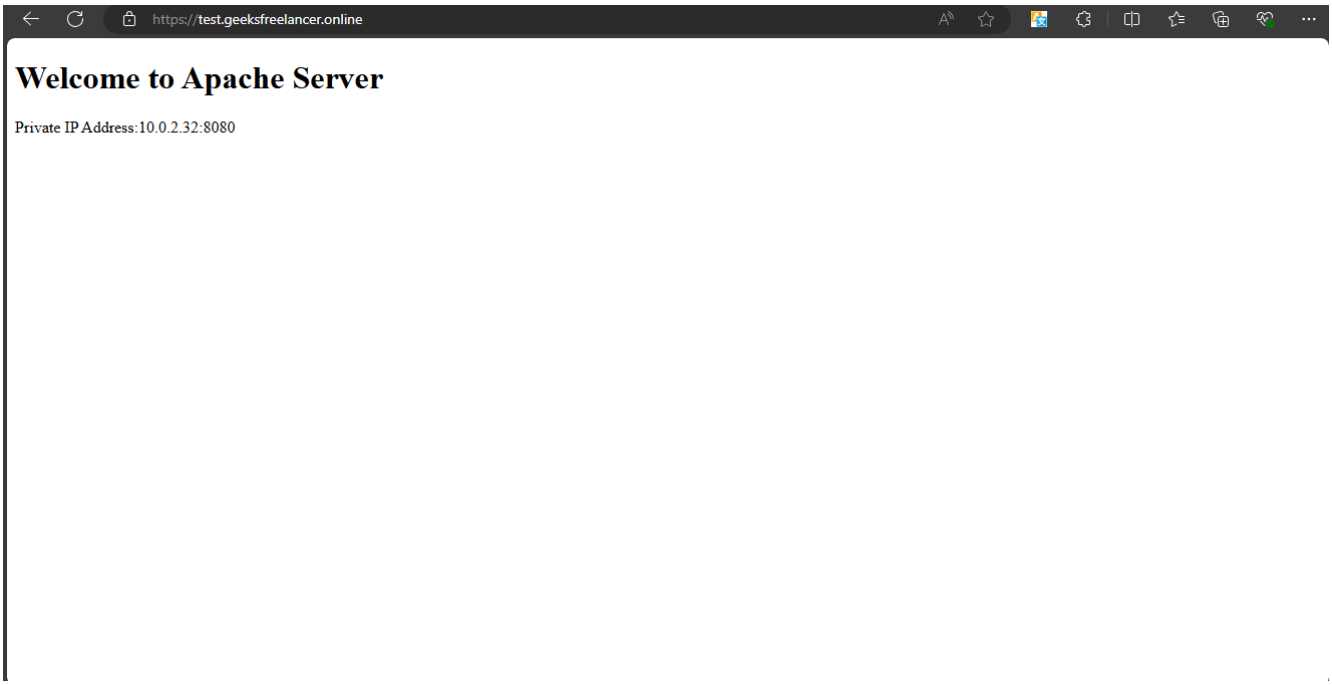
- **Test Connectivity between web server and MySql server to show users data**

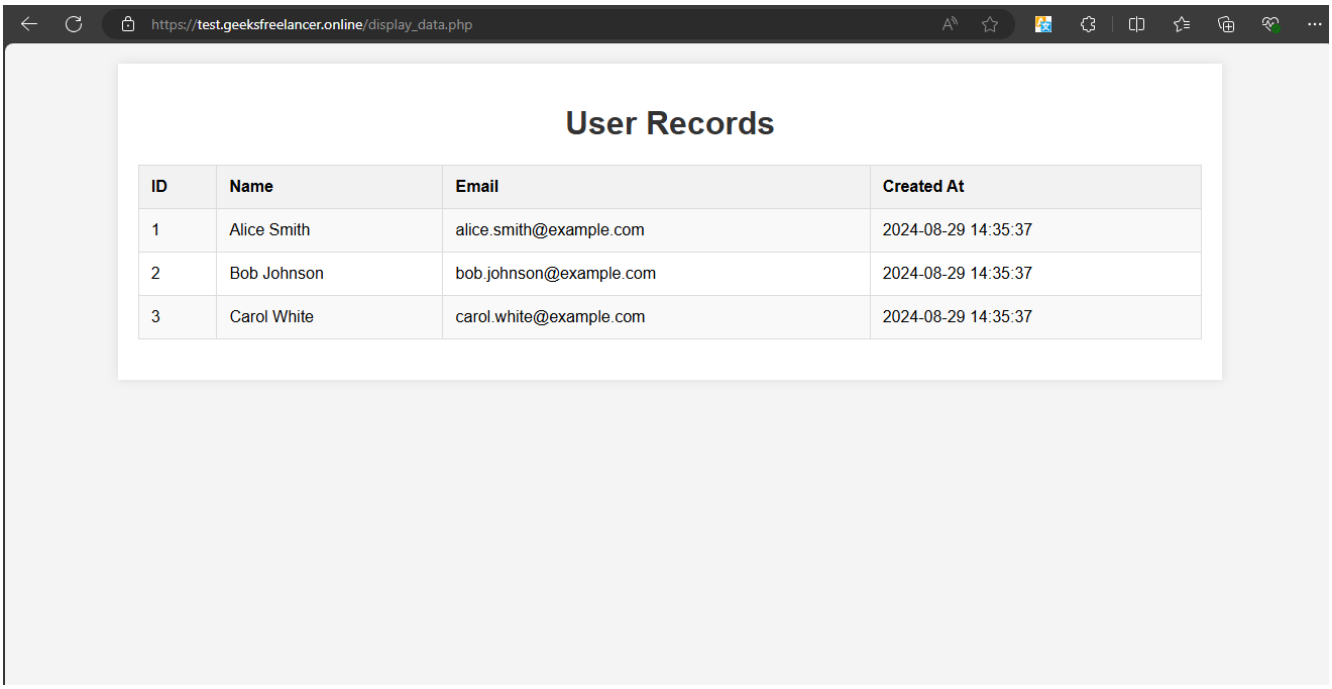


- **After DNS Configuration and SSL/TLS Setup**

Check this link: https://test.geeksfreelancer.online/




https://test.geeksfreelancer.online
Welcome to Apache Server
Private IP Address:10.0.2.32:8080


https://test.geeksfreelancer.online/display_data.php
User Records
ID
Name
Email
Created At
1
Alice Smith
alice.smith@example.com
2024-08-29 14:35:37
2
Bob Johnson
bob.johnson@example.com
2024-08-29 14:35:37
3
Carol White
carol.white@example.com
2024-08-29 14:35:37