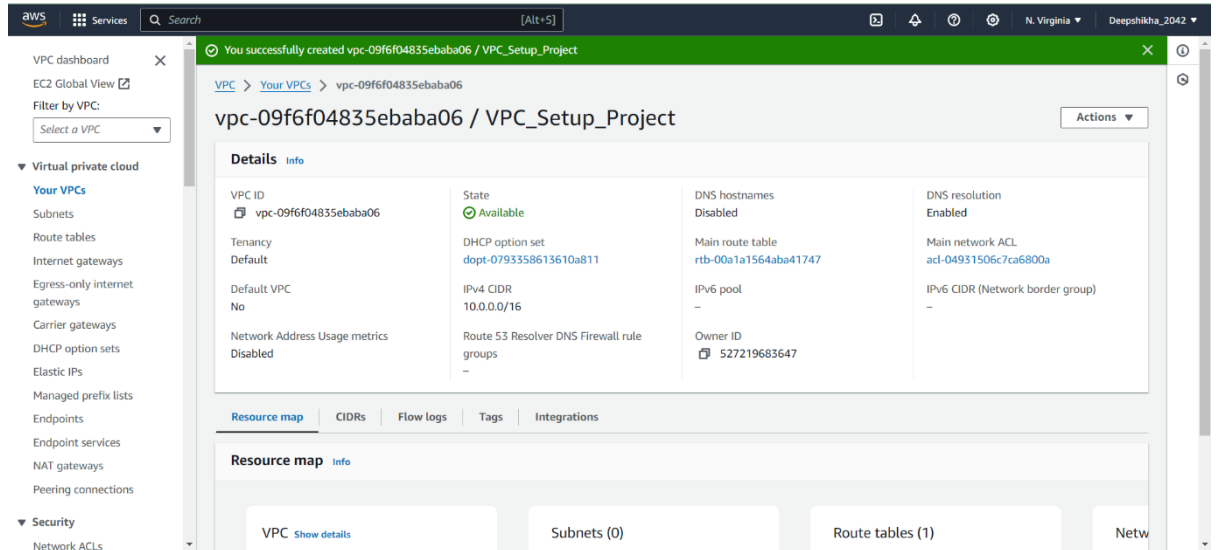


AWS Fortified Cloud Architecture (BY : Deepshikha Paty)

✓ STEP 1:

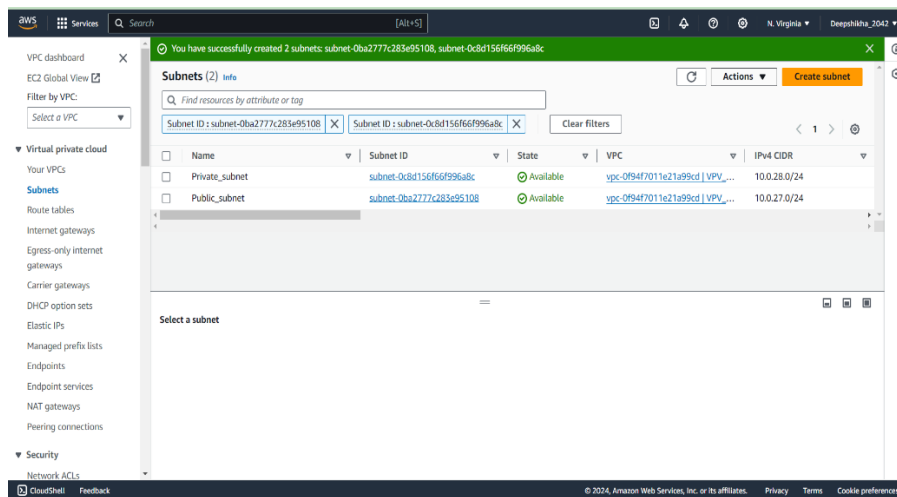
Created a VPC network of CIDR range 10.0.0.0/16



✓ STEP-2:

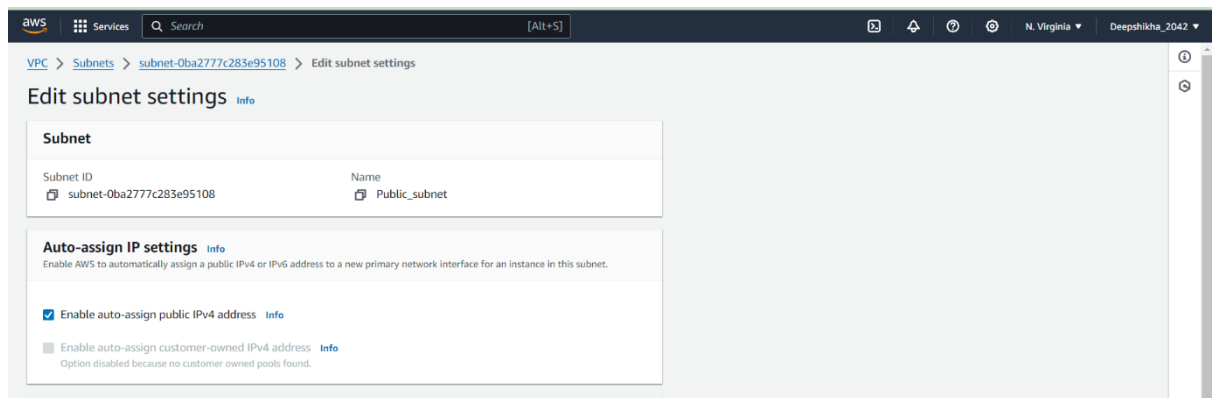
Inside this VPC, created two subnets.

1. Subnet-1 (Public)
 - Name- Public_subnet
 - CIDR: 10.0.27.0/24
 - Web-server
 - Availability-Zone: us-east-1a
2. Subnet-2 (Private)
 - Name- Private_subnet
 - CIDR:10.0.28.0/24
 - Database-server
 - Availability-Zone:us-east-1b



✓ **STEP-3:**

Made the subnet-1 as public by enabling public access.



✓ **STEP-4:**

Then, I deployed a web-server (EC2-instance) and a database-server (EC2-instance) in the public and private subnet respectively.

NOTE:

- The public and private subnet, both are into different availability zone.
- The resources of public subnet and private subnet are hence present in different availability zone.

aws Services Search [Alt+S] N. Virginia Deepshikha_2042

Network settings info

VPC - required info
vpc-0f94f7011e21a99cd (VPV_Network)
10.0.0.0/16

Subnet info
subnet-0ba2777c283e95108 Public_subnet
VPC: vpc-0f94f7011e21a99cd Owner: 527219683647 Availability Zone: us-east-1a
IP addresses available: 251 CIDR: 10.0.27.0/24 Create new subnet

Auto-assign public IP info
Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
☒ Create security group ☐ Select existing security group

Security group name - required
launch-wizard-4
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-./!@#%&'()*+,-=:;[]\$*

Description - required info
launch-wizard-4 created 2024-04-20T05:54:04.897Z

Inbound Security Group Rules

Summary

Number of instances info
1

Software Image (AMI)
Amazon Linux 2 AMI (HVM) - Ker...read more
ami-0a1179631ec8933d7

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and

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

aws Services Search [Alt+S] N. Virginia Deepshikha_2042

Key pair name - required
test_key Create new key pair

Network settings info

VPC - required info
vpc-0f94f7011e21a99cd (VPV_Network)
10.0.0.0/16

Subnet info
subnet-0c8d156f66f996a8c Private_subnet
VPC: vpc-0f94f7011e21a99cd Owner: 527219683647 Availability Zone: us-east-1b
IP addresses available: 251 CIDR: 10.0.28.0/24 Create new subnet

Auto-assign public IP info
Disable

Firewall (security groups) info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
☒ Create security group ☐ Select existing security group

Security group name - required
launch-wizard-5
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-./!@#%&'()*+,-=:;[]\$*

Summary

Number of instances info
1

Software Image (AMI)
Amazon Linux 2 AMI (HVM) - Ker...read more
ami-0a1179631ec8933d7

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

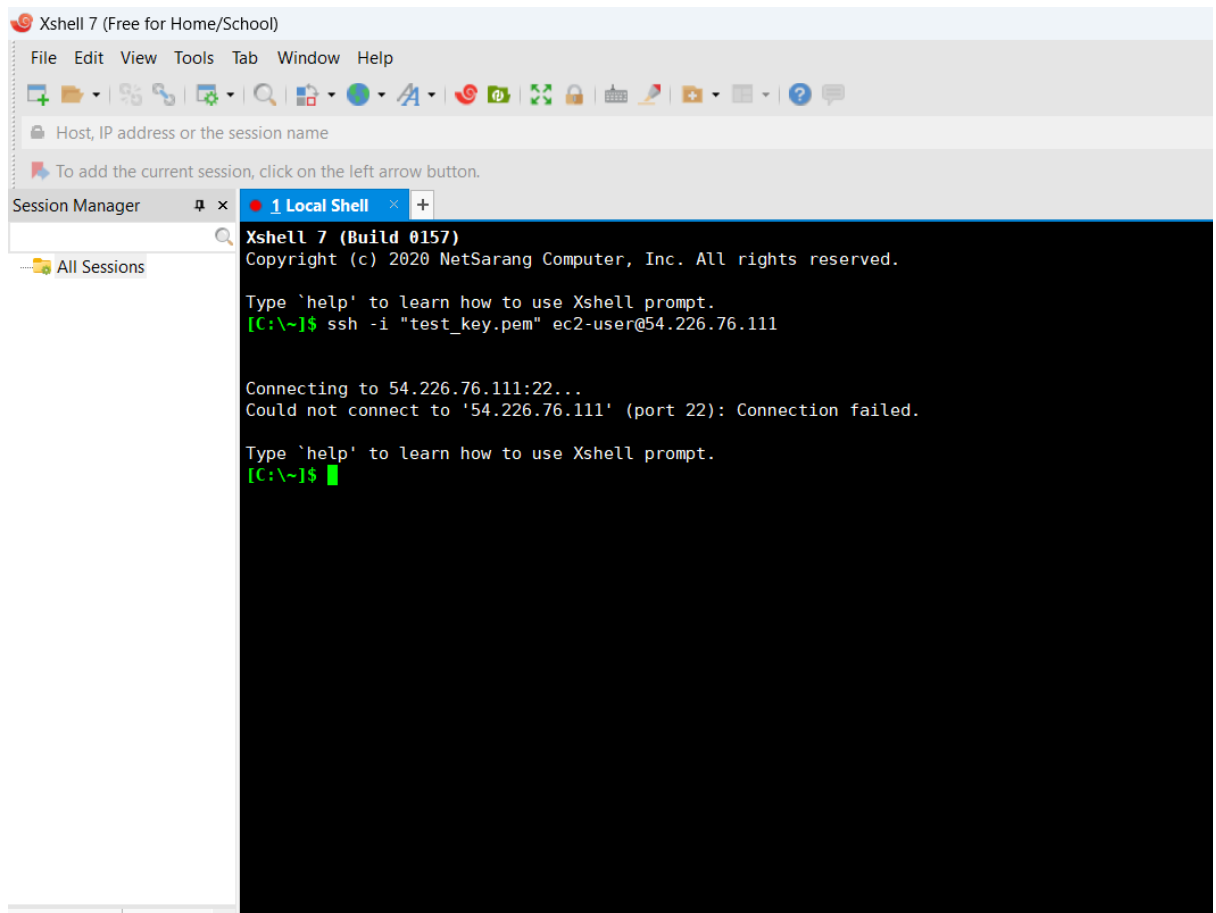
Storage (volumes)
1 volume(s) - 8 GiB

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, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and

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

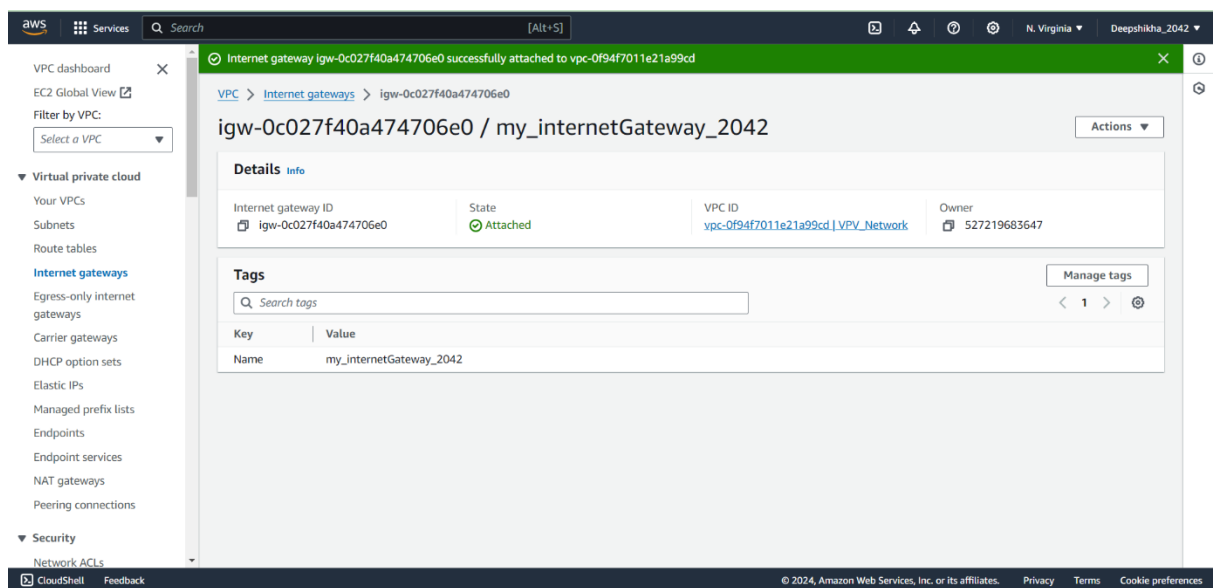
✓ STEP-5:

After that, I tried connecting the web-server, but could not connect. This is because, the internet-gateway is not defined yet.



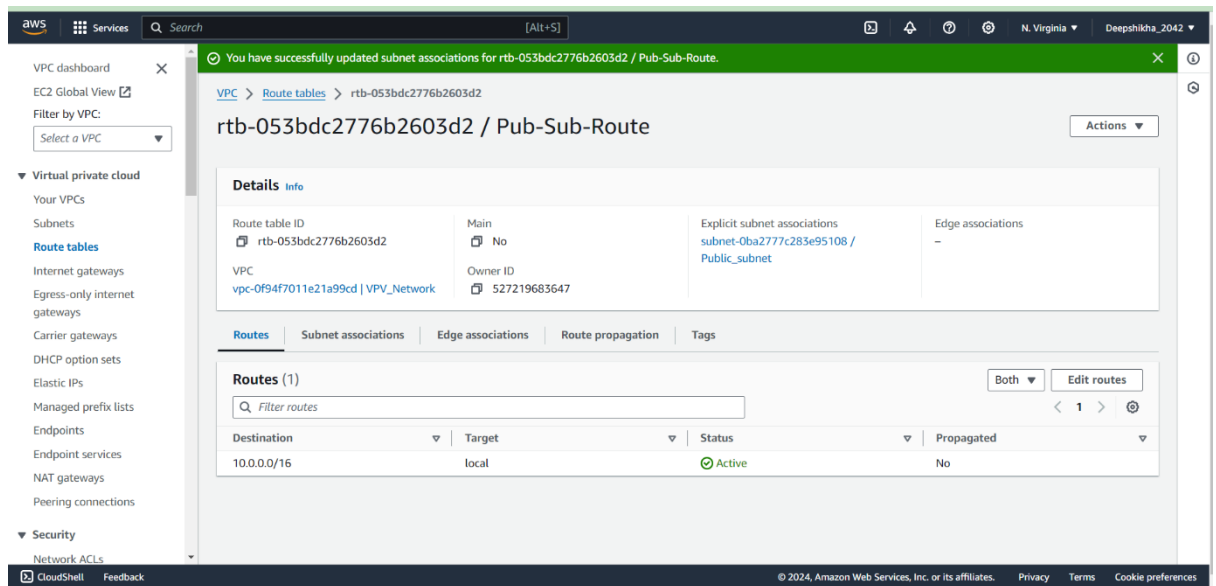
✓ STEP-6:

Hence, I created internet-gateway and attached it to the VPC that I just created.

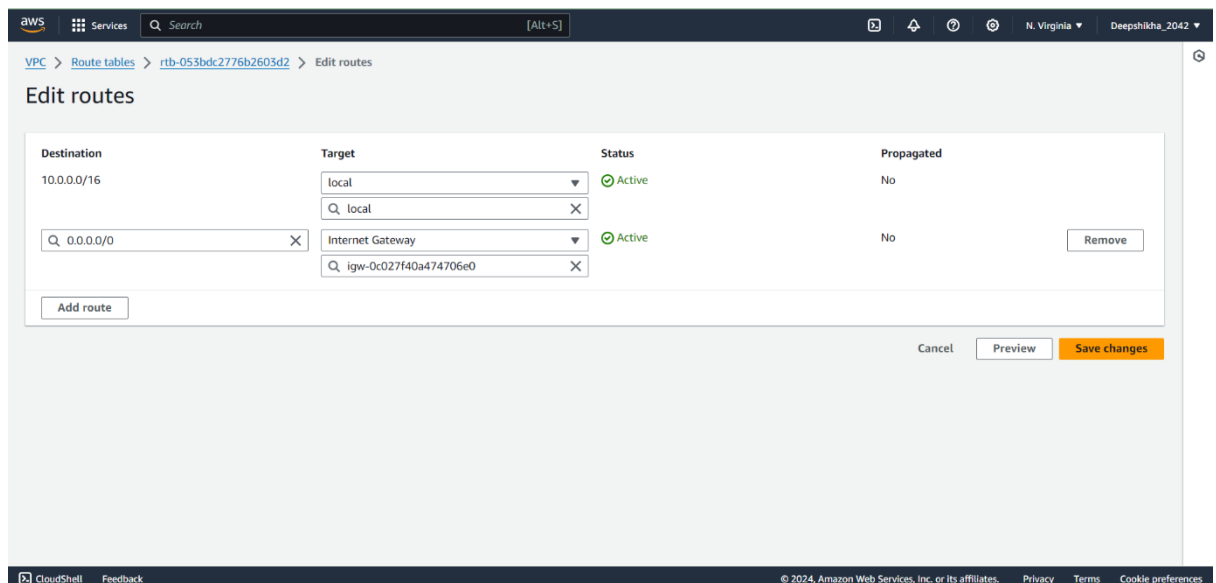


✓ STEP-7:

Then, I defined routing. I created a route table for the public subnet and associated that route-table with the public subnet.



In the route-table, I added the policy for the subnet to access the internet via the internet-gateway.



✓ STEP-8:

Since I have the internet access now, I can connect to the web-server present in the public subnet. Also, the internet can be accessed from the web-server.

```
154.226.76.111:22
Xshell 7 (Build 0157)
Copyright (c) 2020 NetSarang Computer, Inc. All rights reserved.

Type 'help' to learn how to use Xshell prompt.
(C:\V~1)$ ssh -i "test_key.pem" ec2-user@54.226.76.111

Connecting to 54.226.76.111:22...
Could not connect to '54.226.76.111' (port 22): Connection failed.

Type 'help' to learn how to use Xshell prompt.
(C:\V~1)$ ssh -i "test_key.pem" ec2-user@54.226.76.111

Connecting to 54.226.76.111:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+J'.

WARNING! The remote SSH server rejected X11 forwarding request.
#
#####
Amazon Linux 2
#####
AL2 End of Life is 2025-06-30.
#####
A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-0-27-154 ~]$ ping google.com
PING google.com (142.250.31.102) 56(84) bytes of data:
64 bytes from bj-in-f102.1e100.net (142.250.31.102): icmp_seq=1 ttl=105 time=1.80 ms
64 bytes from bj-in-f102.1e100.net (142.250.31.102): icmp_seq=2 ttl=105 time=1.74 ms
64 bytes from bj-in-f102.1e100.net (142.250.31.102): icmp_seq=3 ttl=105 time=1.73 ms
64 bytes from bj-in-f102.1e100.net (142.250.31.102): icmp_seq=4 ttl=105 time=1.75 ms
64 bytes from bj-in-f102.1e100.net (142.250.31.102): icmp_seq=5 ttl=105 time=1.79 ms
64 bytes from bj-in-f102.1e100.net (142.250.31.102): icmp_seq=6 ttl=105 time=1.74 ms
64 bytes from bj-in-f102.1e100.net (142.250.31.102): icmp_seq=7 ttl=105 time=1.78 ms
64 bytes from bj-in-f102.1e100.net (142.250.31.102): icmp_seq=8 ttl=105 time=1.76 ms
64 bytes from bj-in-f102.1e100.net (142.250.31.102): icmp_seq=9 ttl=105 time=1.83 ms
```



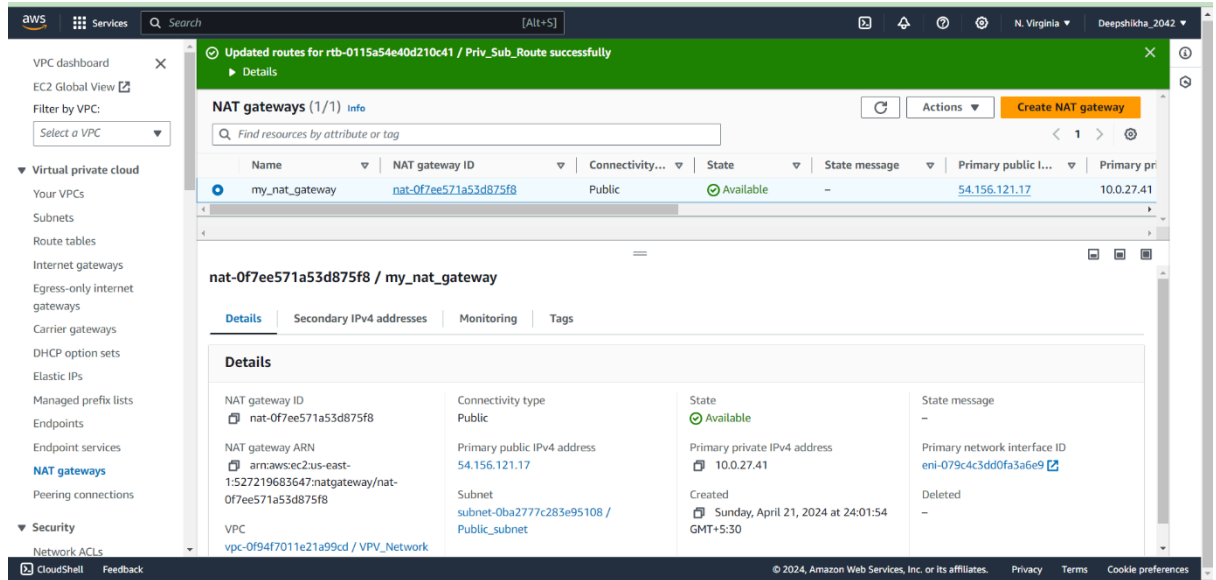
✓ **STEP-9:**

Then, I tried connecting the database-server present in the private subnet using the SSH command but I could not because it has only private IP address, hence cannot be accessed publicly.

✓ **STEP-10:**

(First way to access the database-server using NAT-GATEWAY)

To access the internet from the database-server, we need to define a NAT-Gateway. So, I created a NAT-Gateway inside the public subnet.

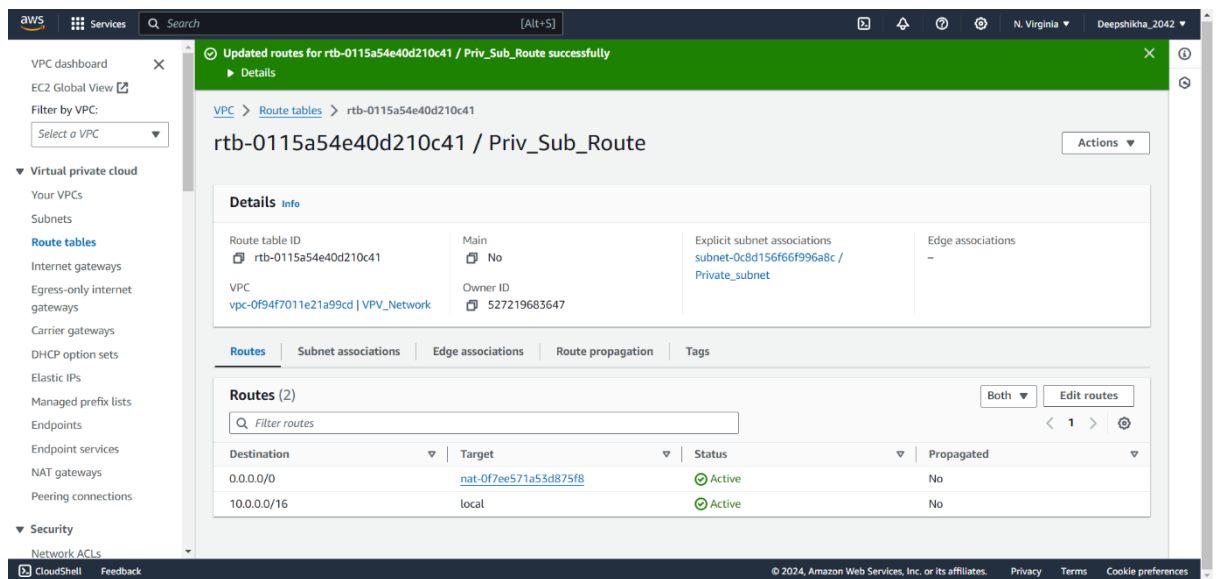


✓ **STEP-11:**

Firstly, I created a route-table and associated that with the private subnet.

In the route-table, I added routing policies for private subnet to access the internet via NAT-Gateway.

Now, I can access internet from the database-server.

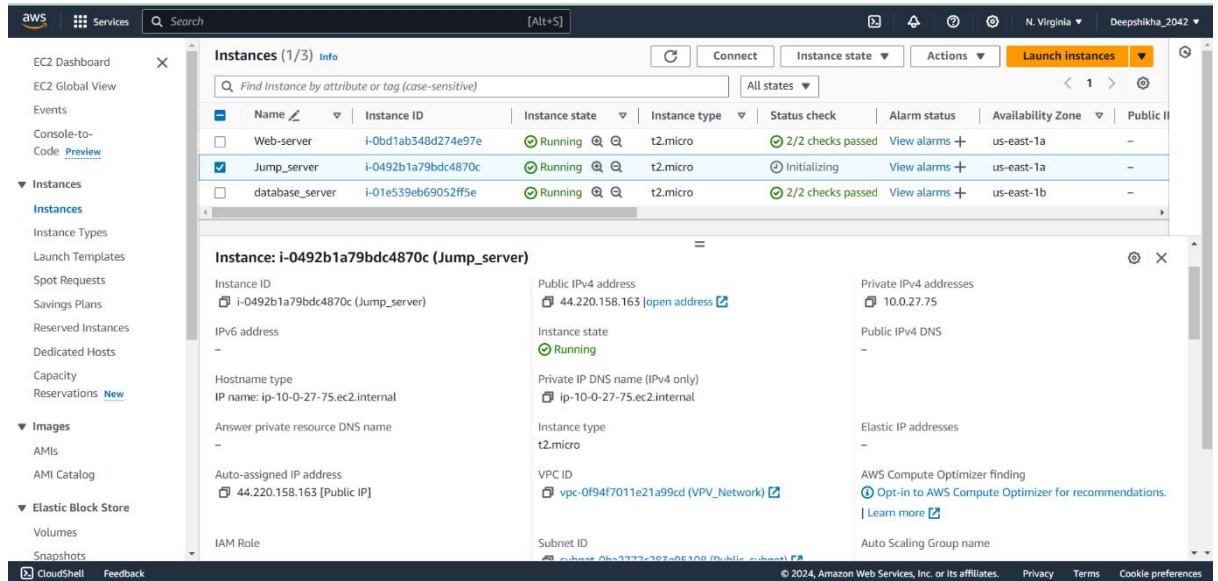


✓ **STEP-12:**

But, what if a developer (a database administrator may be) want the access to the database-server? Does he need to access it via the web-server every single time?

We want to give the access of the database-server to the developer only, not to the public.

For this, I created a jump server.



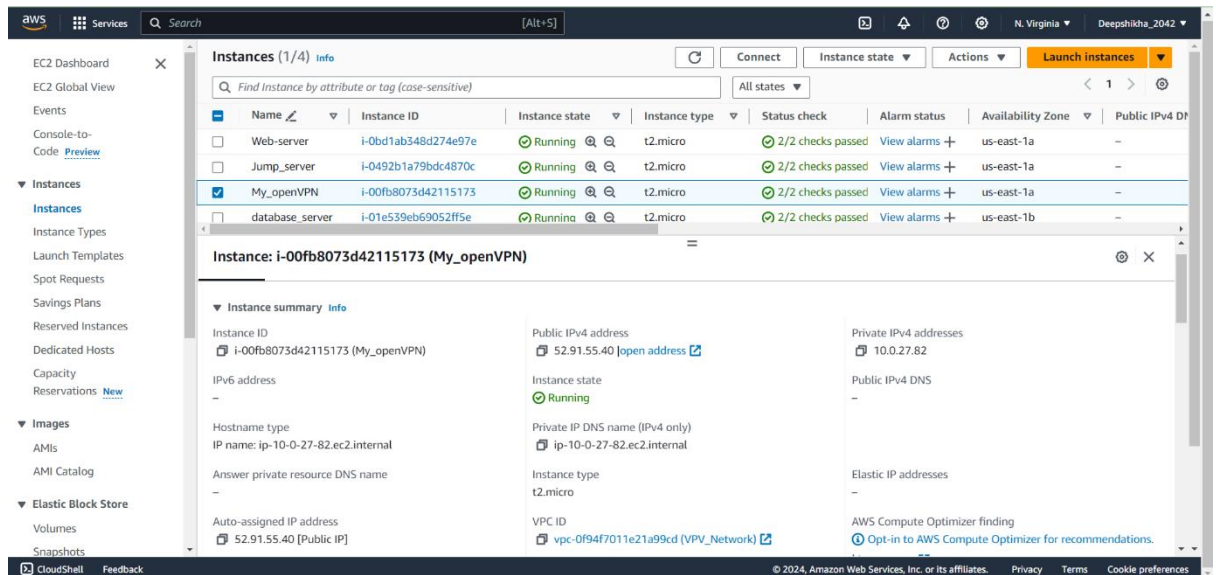
One can access the database-server via the web-server, but it is better to have a different server (jump-server) for accessing purpose. This is because, the web-server already have different important roles (application purpose)

[illegible]

✓ **STEP-13:**

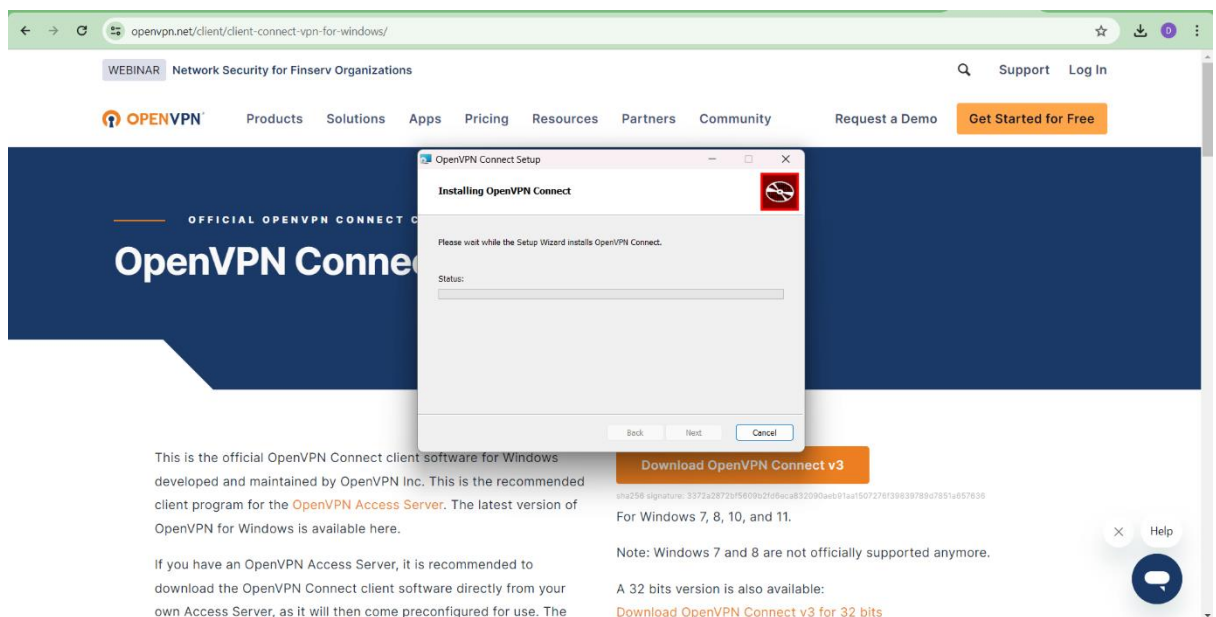
(Second way to access the database-server using OpenVPN)

I created OpenVPN in the public subnet.



✓ **STEP-14:**

Installed VPN Client in the system.



✓ **STEP-15:**

Then, I connected to the VPN server and I got the following credentials:

- Admin UI
- Client UI
- Access ID and Password

```
1 openVPN server +
Type 'help' to learn how to use Xshell prompt.
[ct:\~]$ ssh -i "test_key.pem" openvpnas@52.91.55.40

Connecting to 52.91.55.40:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+J'.

Welcome to OpenVPN Access Server Appliance 2.13.1

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

System information as of Sun Apr 21 07:06:17 UTC 2024

System load:  0.0      Processes:      98
Usage of /:   25.9% of 7.57GB   Users logged in: 0
Memory usage: 21%      IPy4 address for eth0: 10.0.27.82
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

1 update can be applied immediately.
1 of these updates is a standard security update.
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

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sun Apr 21 06:59:45 2024 from 152.58.151.242
/usr/bin/xaauth: timeout in locking authority file /home/openvpnas/.Xauthority
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

1 openVPN server +
Wiping any previous userdb...
Creating default profile...
Modifying default profile...
Adding new user to userdb...
Modifying new user as superuser in userdb...
Auto-generated pass = "AQVTKrnlzD3n". Setting in db...
Getting hostname...
Hostname: 52.91.55.40
Preparing web certificates...
Getting web user account...
Adding web group account...
Adding web group...
groupadd: group 'openvpn_as' already exists
Adjusting license directory ownership...
Initializing confdb...
Initial version is not set. Setting it to 2.13.1...
Generating PAM config for openvpnas ...
Enabling service
Created symlink /etc/systemd/system/multi-user.target.wants/openvpnas.service → /lib/systemd/system/openvpnas.service.
Starting openvpnas...

NOTE: Your system clock must be correct for OpenVPN Access Server
to perform correctly. Please ensure that your time and date
are correct on this system.

Initial Configuration Complete!

You can now continue configuring OpenVPN Access Server by
directing your Web browser to this URL:

https://52.91.55.40:943/admin

During normal operation, OpenVPN AS can be accessed via these URLs:
Admin UI: https://52.91.55.40:943/admin
Client UI: https://52.91.55.40:943/
To login please use the "openvpn" account with "AQVTKrnlzD3n" password.

See the Release Notes for this release at:
https://openvpn.net/vpn-server-resources/release-notes/

openvpnas@ip-10-0-27-82:~$
```

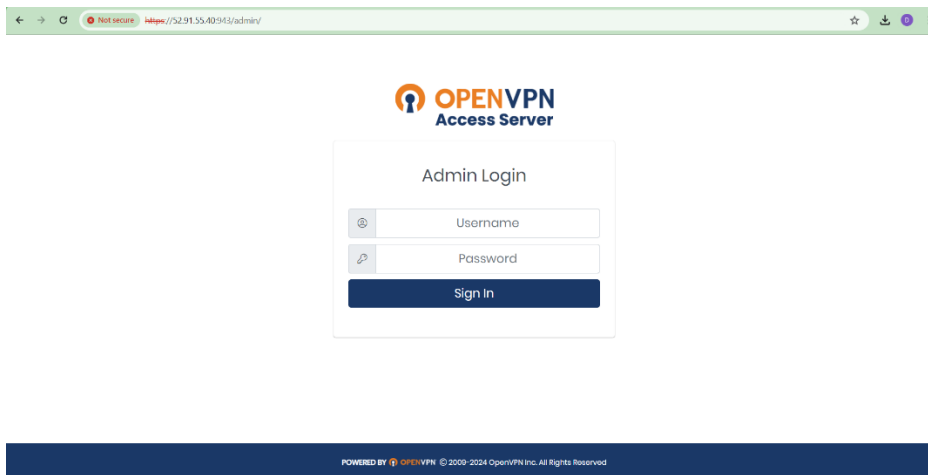
During normal operation, OpenVPN AS can be accessed via these URLs:
Admin UI: https://52.91.55.40:943/admin
Client UI: https://52.91.55.40:943/
To login please use the "openvpn" account with "AQVTKrnlzD3n" password.

See the Release Notes for this release at:
https://openvpn.net/vpn-server-resources/release-notes/

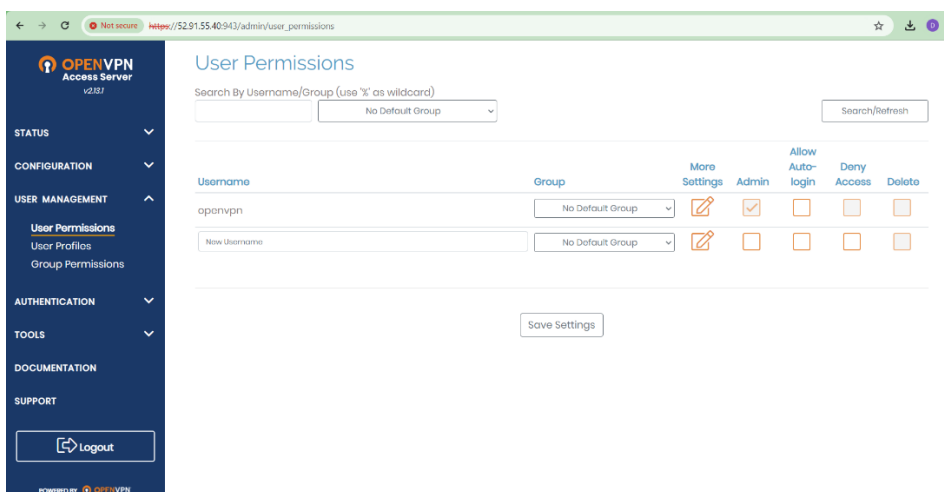
openvpnas@ip-10-0-27-82:~\$

✓ STEP-16:

Then, I just pasted the Admin UI in the search engine and got the following page.

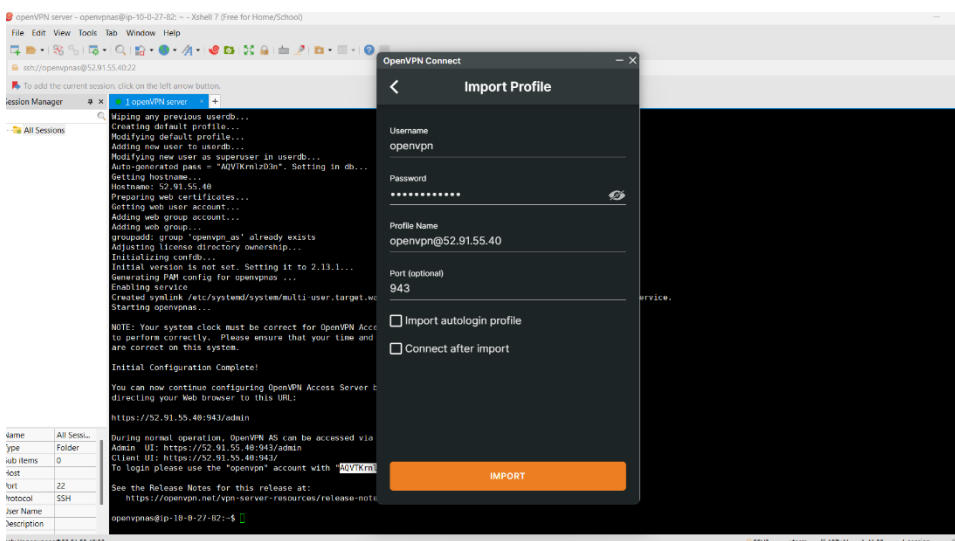


From here, one can handle user permission, group permission, user profile etc.

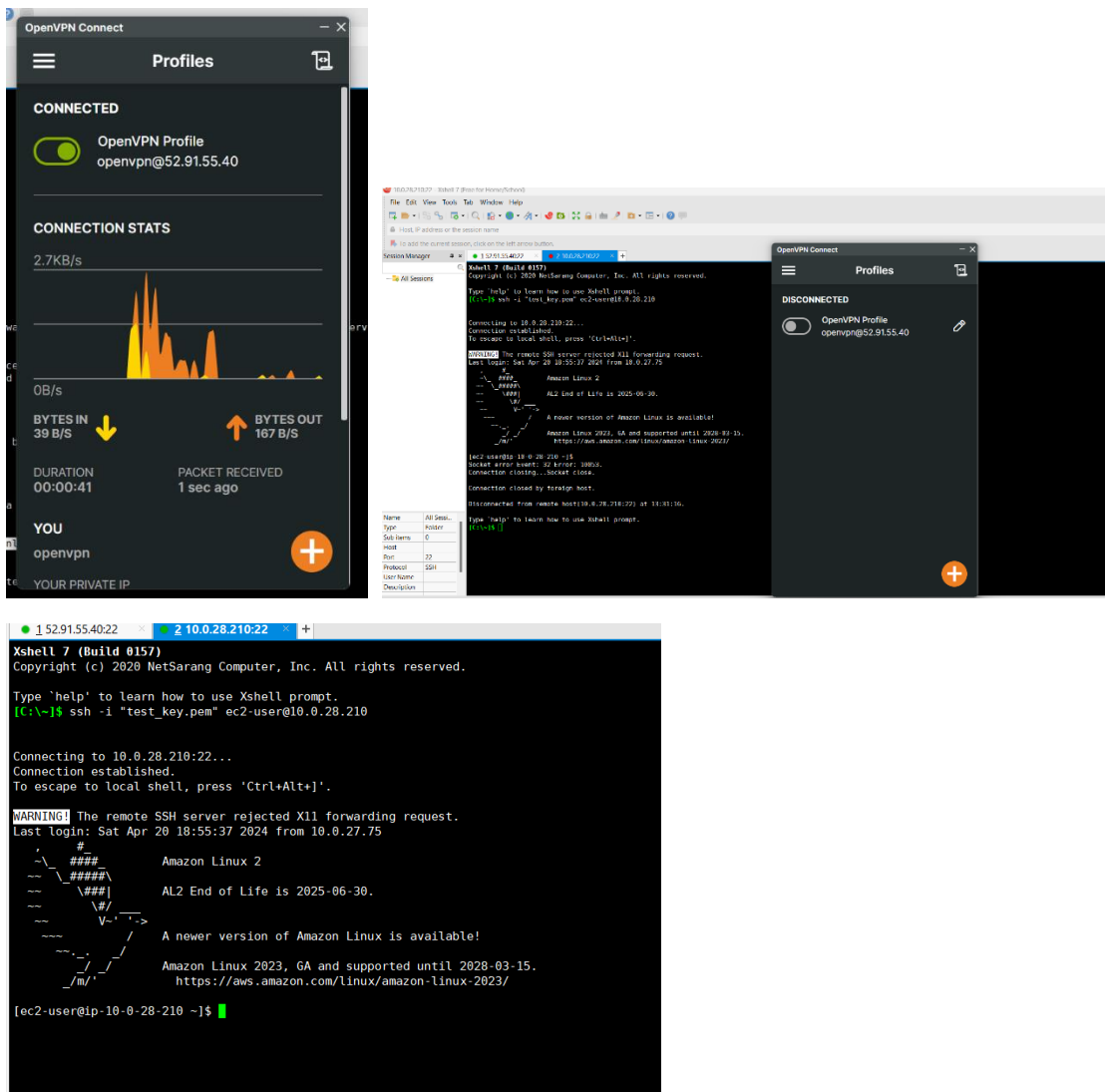


✓ **STEP-17:**

Using the Client UI, Access id and password, I was able to connect to the AWS account. Now I (or may be the database-administrator) can connect to the AWS account even using the private IP address.



The database-administrator can connect and disconnect to the AWS account based on the requirements.



**** END ****