»» PROJECT ««

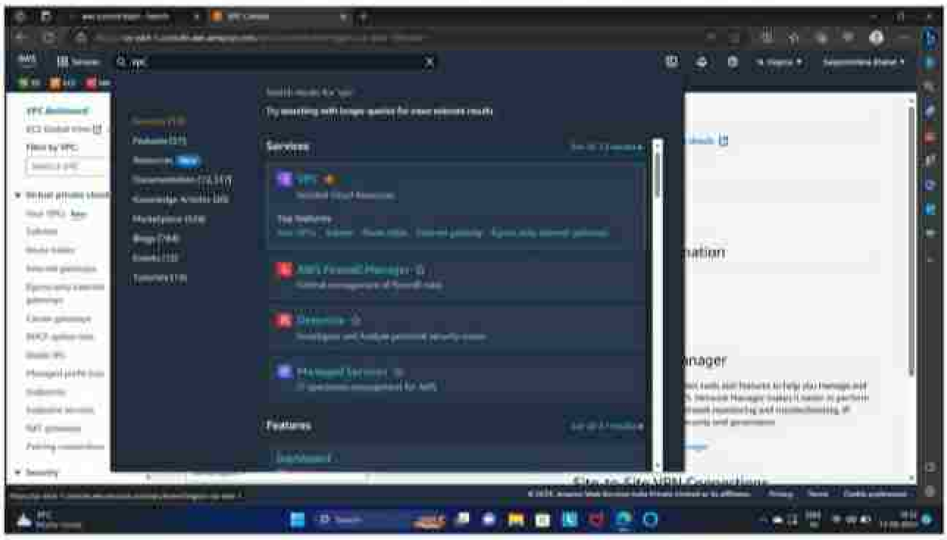
AMAZON WEB SERVICES

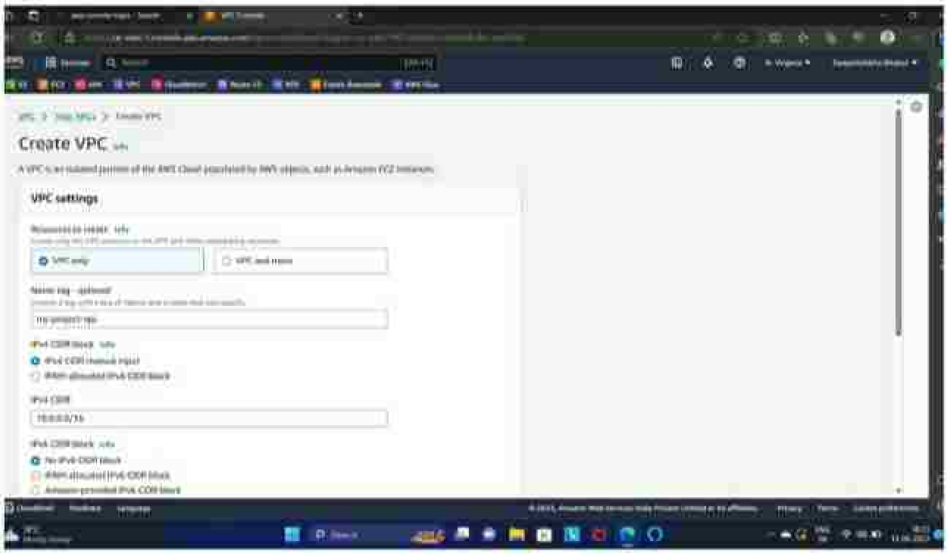
NAME : SWAPNILSHIKHA BHAKAT
BATCH : 1
SIC : 22BCSE87

PROJECT: We were given the task to create a VPC (Virtual Private Cloud) which contained two subnets, which was - Public and Private subnet. The public subnet contained web servers (atleast 2) and the private subnet contained data-base server installed with any latest version of MySQL. The public subnet should be configured with Load Balancer (including domain name and SSL certificate) and should be mapped Route 53. Autoscaling should be configured with the server in public subnet. Open VPN set-up should also be done here.

The following steps are done to execute this project :-

- **STEP 1 :** A VPC is created, named my-project-vpc.





Create VPC

VPC settings

Resources to create
● VPC only ○ VPC and more

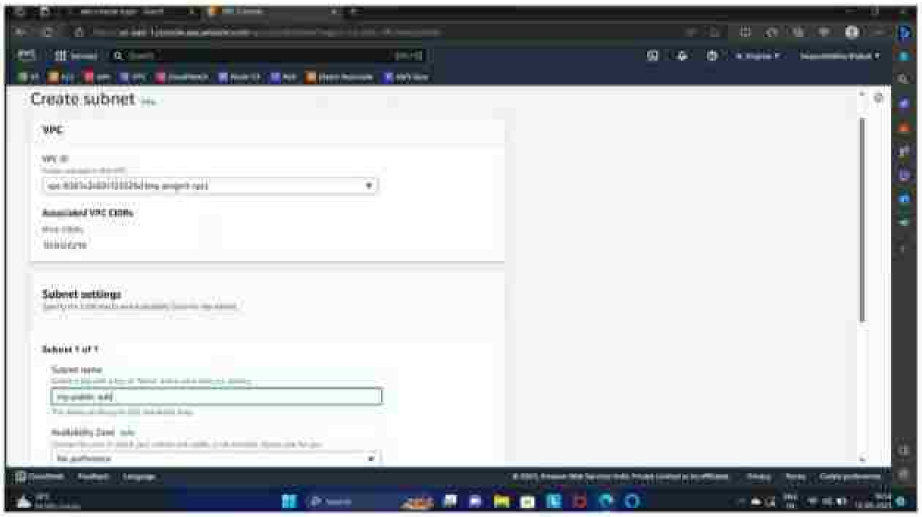
Name tag - optional
my-project-vpc

IPv4 CIDR block
● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.0.0.0/16

IPv6 CIDR block
● No IPv6 CIDR block
○ IPAM-allocated IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block

- **STEP 2 :** Two subnet are created, one is public subnet and other one is private subnet.



Create subnet

VPC

VPC ID
[illegible] (my-project-vpc)

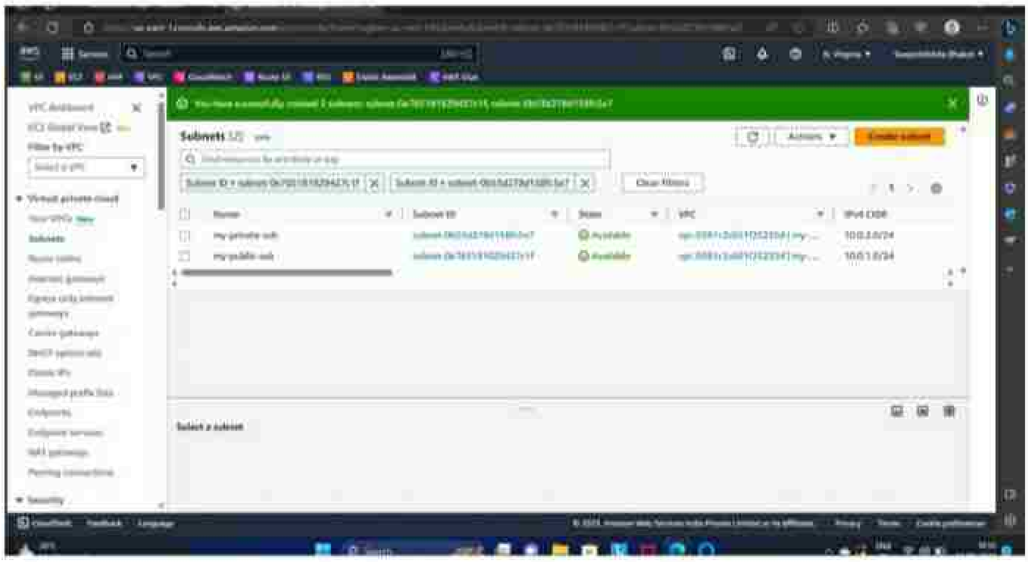
Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16

Subnet settings

Subnet 1 of 1

Subnet name
my-public-sub

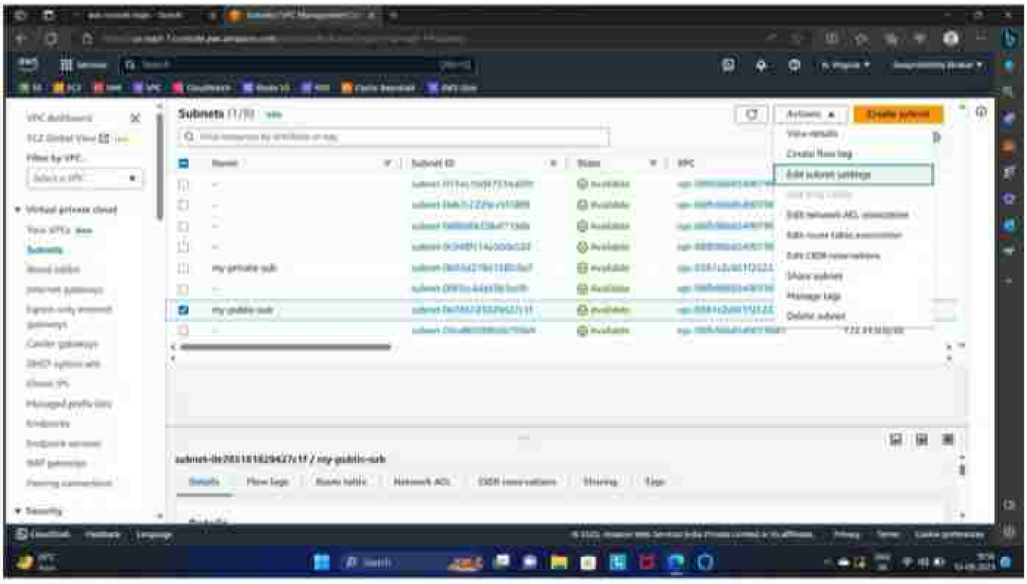
Availability Zone
No preference

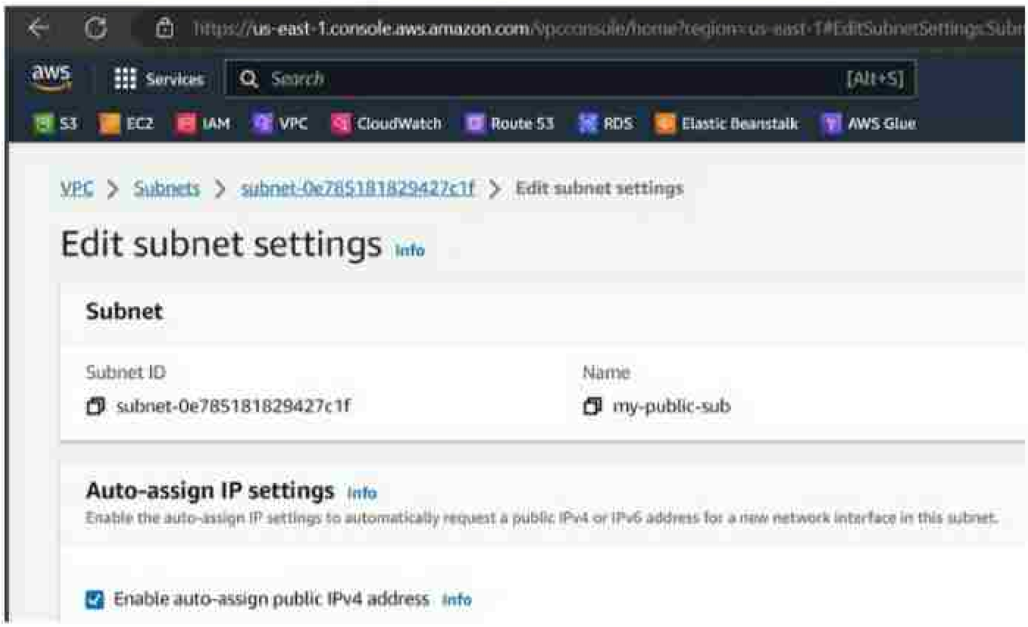


Subnets (2)

Name	Subnet ID	State	VPC	IPv4 CIDR
my-private-sub	[illegible]	Available	[illegible] | my-...	10.0.2.0/24
my-public-sub	[illegible]	Available	[illegible] | my-...	10.0.1.0/24

The public subnet is enabled with auto-assign IP address by selecting it then actions and edit subnet settings.





https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#EditSubnetSettings:Subn

VPC > Subnets > subnet-0e785181829427c1f > Edit subnet settings

Edit subnet settings Info

Subnet

Subnet ID: subnet-0e785181829427c1f

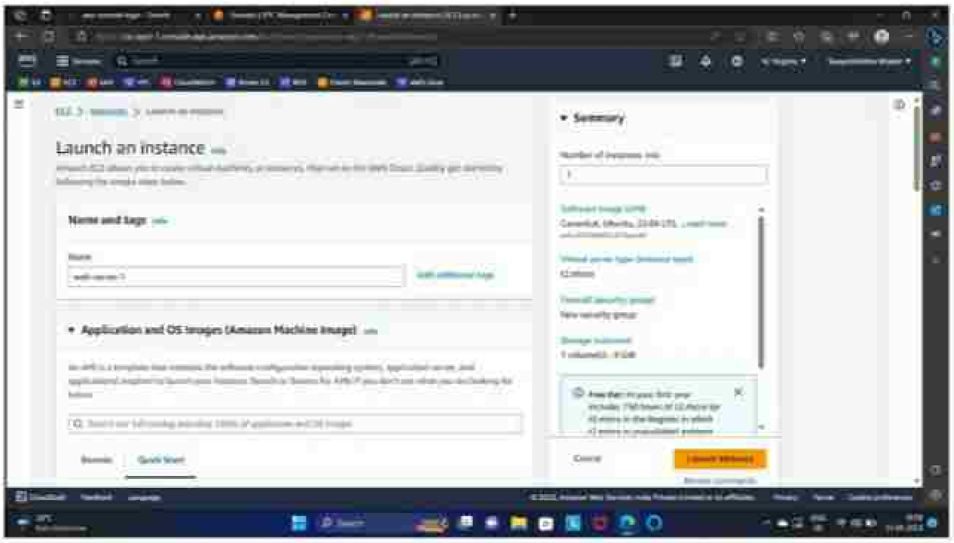
Name: my-public-sub

Auto-assign IP settings Info

Enable the auto-assign IP settings to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet.

☑ Enable auto-assign public IPv4 address Info

- **STEP 3 :** Two web-servers are launched in this VPC in Public subnet.



Launch an instance

Name and tags

Name: web-server-1

Application and OS Images (Amazon Machine Image)

Summary

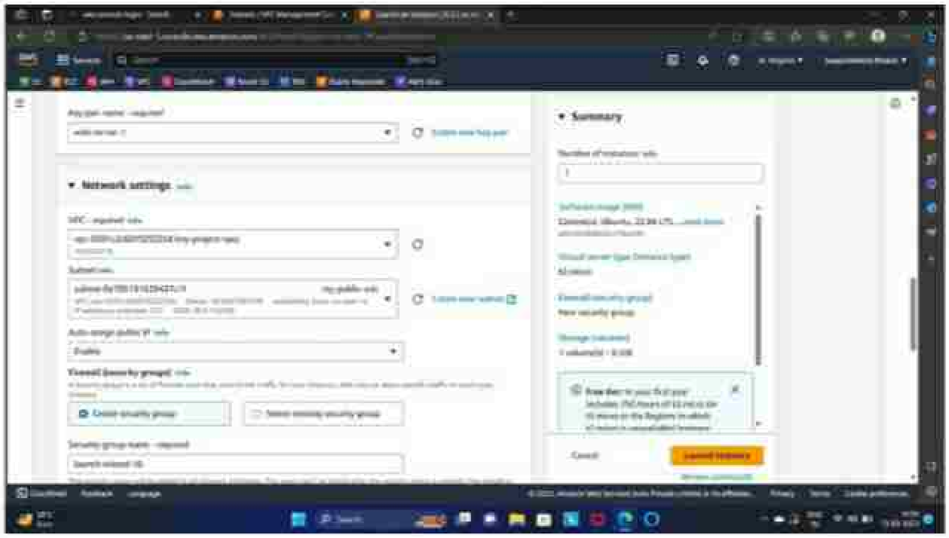
Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 22.04 LTS

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

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



Key pair name - required: web-server-1

Network settings

VPC - required

Subnet: my-public-sub

Auto-assign public IP: Enable

Firewall (security groups)

○ Create security group ○ Select existing security group

Security group name - required

Summary

Number of instances: 1

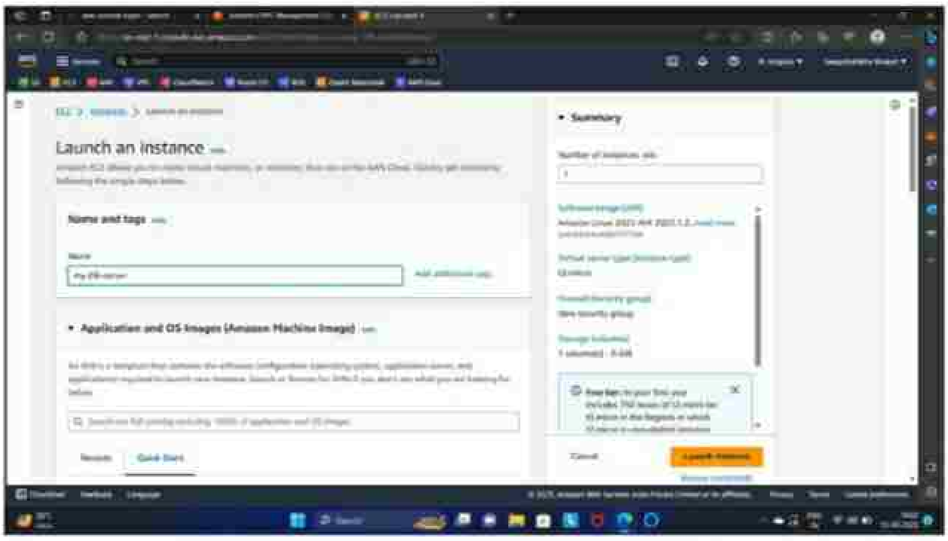
Software Image (AMI): Canonical, Ubuntu, 22.04 LTS

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

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

- **STEP 4 :** Database server is launched in this VPC in Private subnet, installed with latest version of MySQL.



Launch an instance

Name and tags

Name: my-DB-server

Application and OS Images (Amazon Machine Image)

Summary

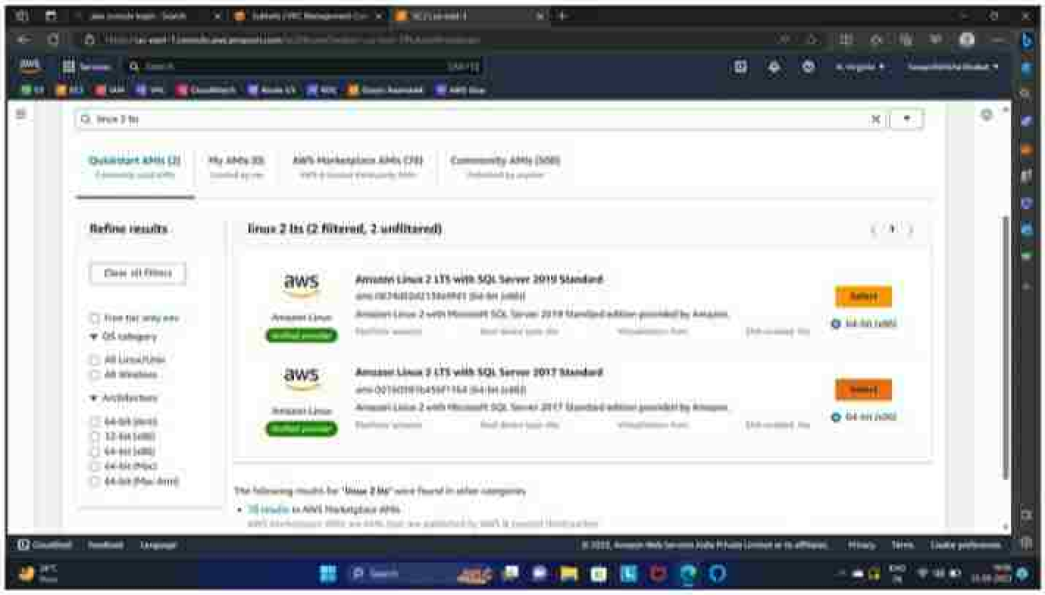
Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.1.2

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

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



linux 2 lts

Quickstart AMIs (2) | My AMIs (0) | AWS Marketplace AMIs (78) | Community AMIs (500)

Refine results

Clear all filters

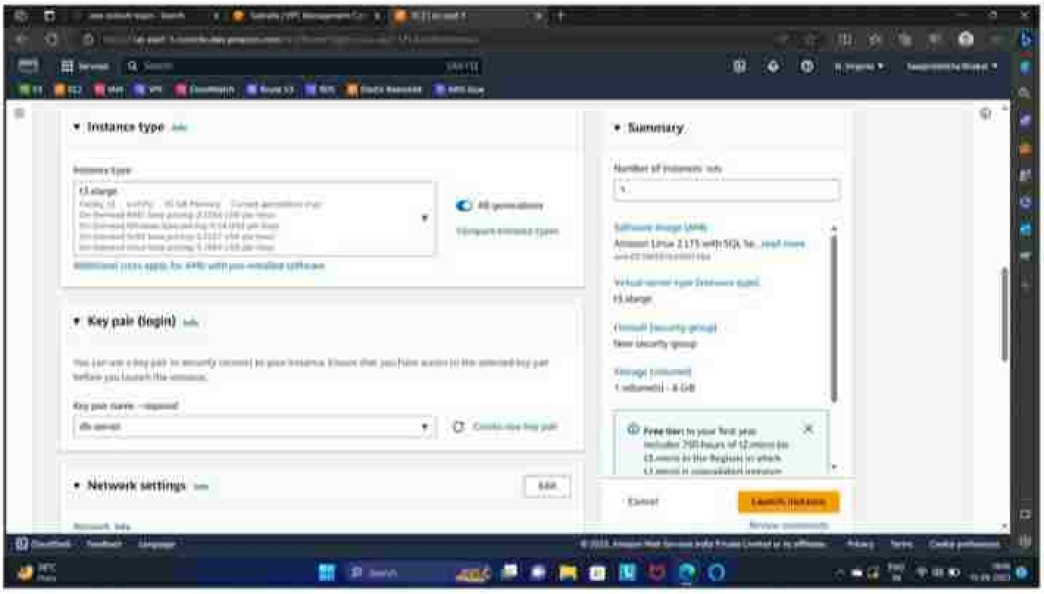
□ Free tier only
▼ OS category
□ All Linux/Unix
□ All Windows
▼ Architecture
□ 64-bit (Arm)
□ 32-bit (x86)
□ 64-bit (x86)
□ 64-bit (Mac)
□ 64-bit (Mac-Arm)

linux 2 lts (2 filtered, 2 unfiltered)

Amazon Linux 2 LTS with SQL Server 2019 Standard
ami-[illegible] (64-bit (x86))
Amazon Linux 2 with Microsoft SQL Server 2019 Standard edition provided by Amazon
Select
● 64-bit (x86)

Amazon Linux 2 LTS with SQL Server 2017 Standard
ami-[illegible] (64-bit (x86))
Amazon Linux 2 with Microsoft SQL Server 2017 Standard edition provided by Amazon
Select
● 64-bit (x86)

The following results for "linux 2 lts" were found in other categories:
- 78 results in AWS Marketplace AMIs



▼ Instance type

Instance type
t3.xlarge

All generations
Compare instance types

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required
[illegible]

Create new key pair

▼ Network settings
Edit

▼ Summary

Number of instances
1

Software Image (AMI)
Amazon Linux 2 LTS with SQL Se...read more

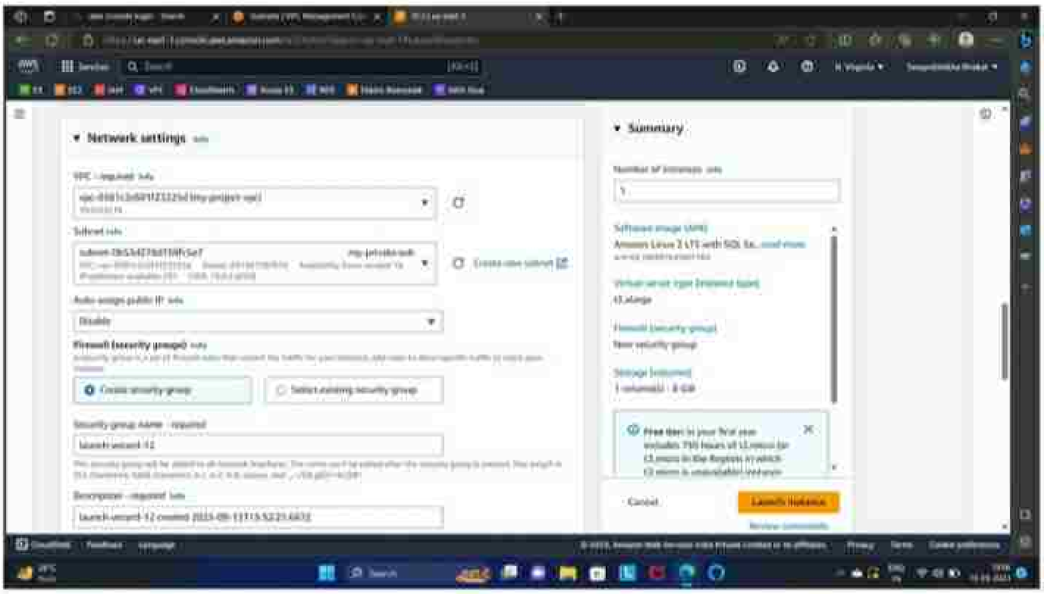
Virtual server type (instance type)
t3.xlarge

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

Cancel
Launch instance
Review commands



▼ Network settings

VPC - required
vpc-[illegible] (my-project-vpc)

Subnet
subnet-[illegible] my-private-sub

Create new subnet

Auto-assign public IP
Disable

Firewall (security groups)

● Create security group
○ Select existing security group

Security group name - required
launch-wizard-12

Description - required
launch-wizard-12 created 2023-09-13T15:52:21.683Z

▼ Summary

Number of instances
1

Software Image (AMI)
Amazon Linux 2 LTS with SQL Se...read more

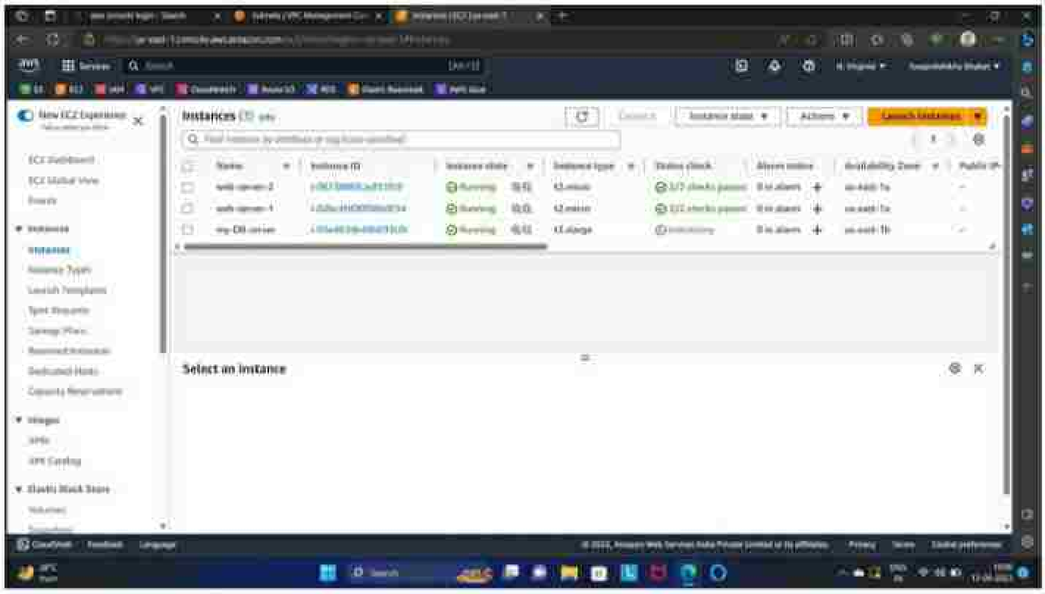
Virtual server type (instance type)
t3.xlarge

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

Cancel
Launch instance
Review commands

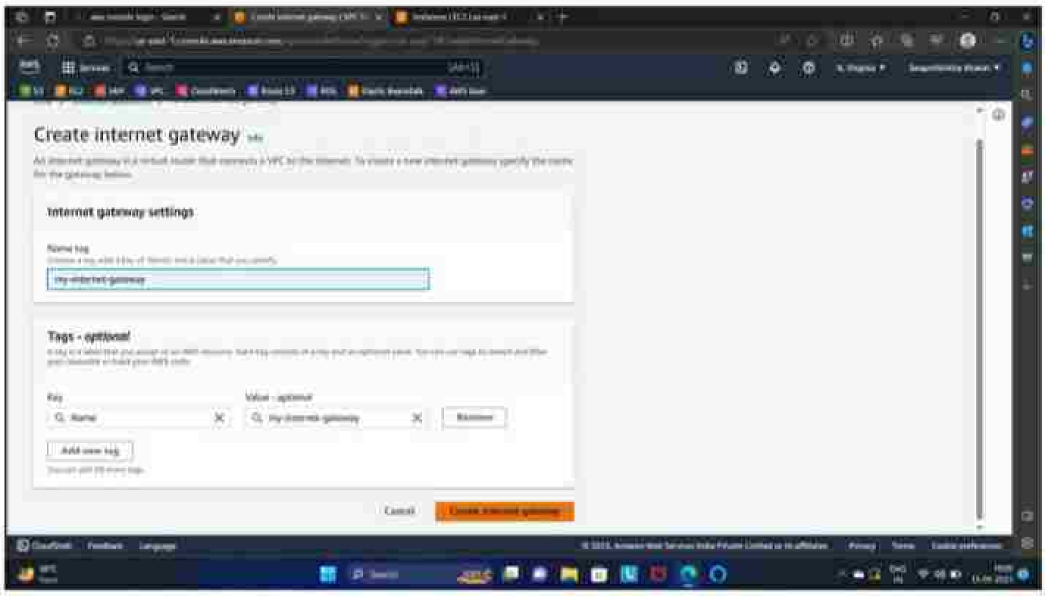


Instances

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
□	web-server-2	[illegible]	Running	t2.micro	2/2 checks passed	0 in alarm	us-east-1a	–
□	web-server-1	[illegible]	Running	t2.micro	2/2 checks passed	0 in alarm	us-east-1a	–
□	my-DB-server	[illegible]	Running	t2.xlarge	Initializing	0 in alarm	us-east-1b	–

Select an instance

- **STEP 5 :** Internet gateway is created and attached to VPC.



Create internet gateway

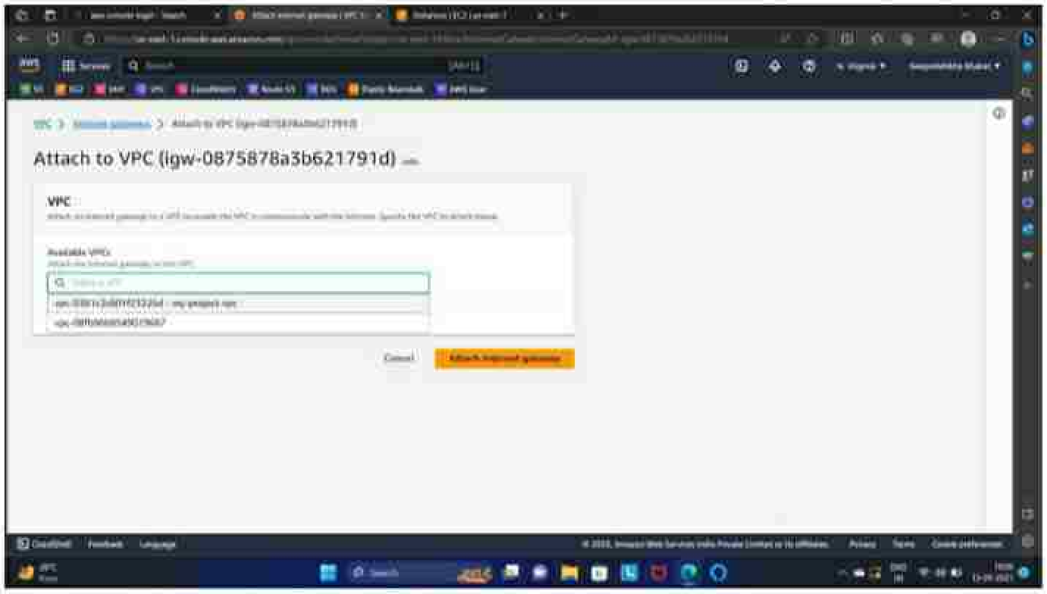
Internet gateway settings

Name tag

my-internet-gateway

Tags - optional

Key	Value - optional
Name	my-internet-gateway



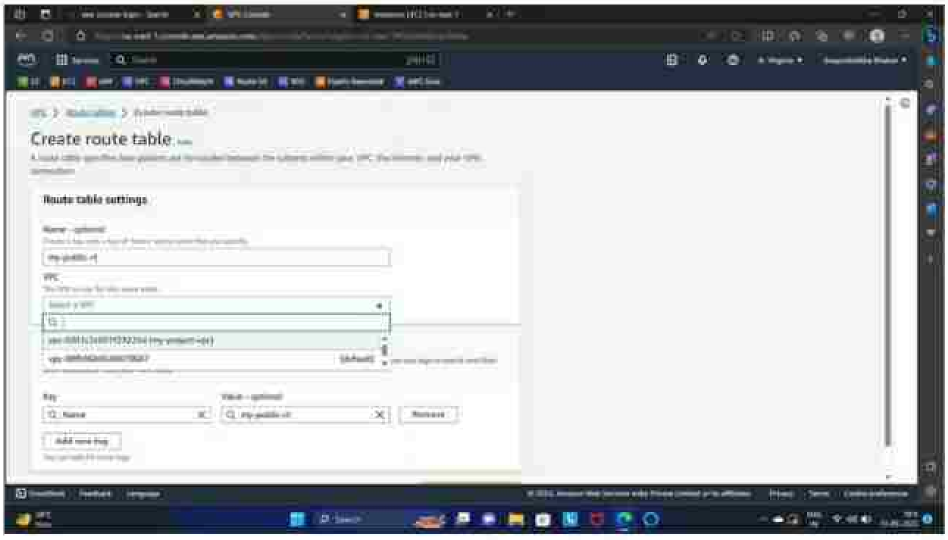
Attach to VPC (igw-0875878a3b621791d)

VPC

Available VPCs

Select a VPC

- **STEP 6 :** Public route table is created and associated with its respective subnet.



Create route table

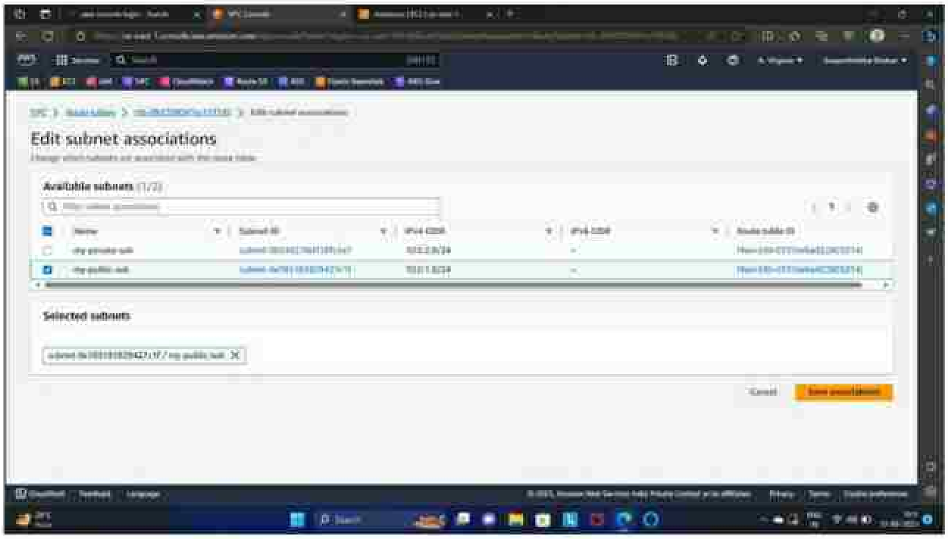
Route table settings

Name - optional: my-public-rt

VPC: Select a VPC

Key: Name

Value - optional: my-public-rt



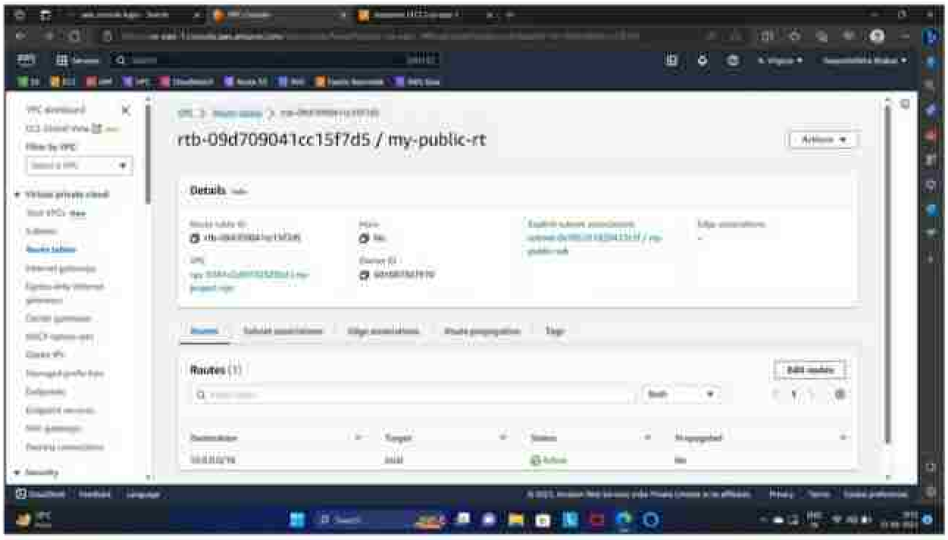
Edit subnet associations

Available subnets (1/2)

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
○	my-private-sub	[illegible]	10.0.2.0/24	-	[illegible]
☑	my-public-sub	[illegible]	10.0.1.0/24	-	[illegible]

Selected subnets

- **STEP 7 :** Public route is directed to internet via Internet Gateway.



rtb-09d709041cc15f7d5 / my-public-rt

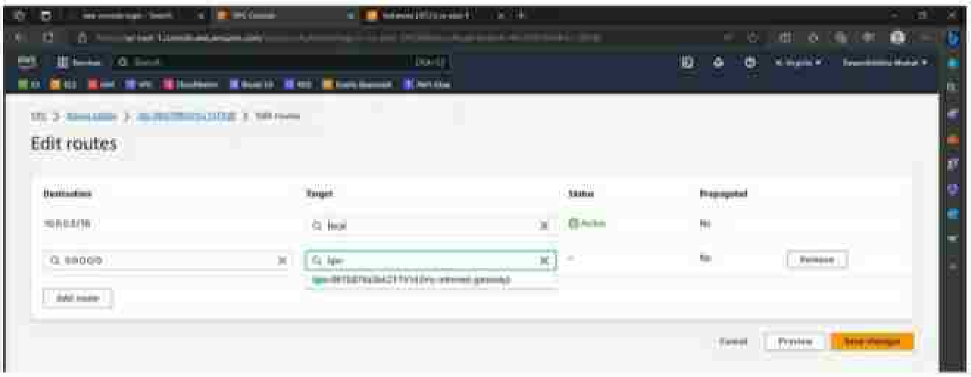
Details

Main: No

Edge associations: -

Routes (1)

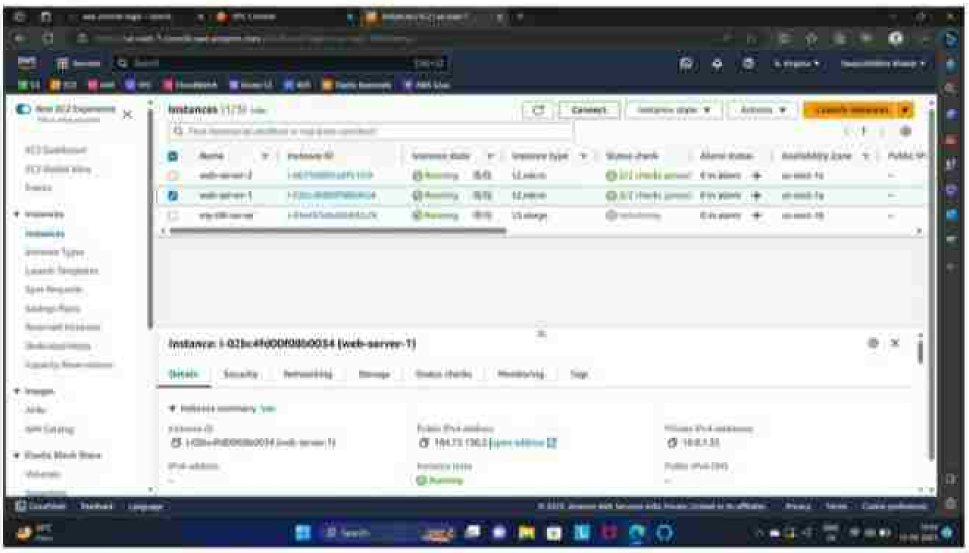
Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No



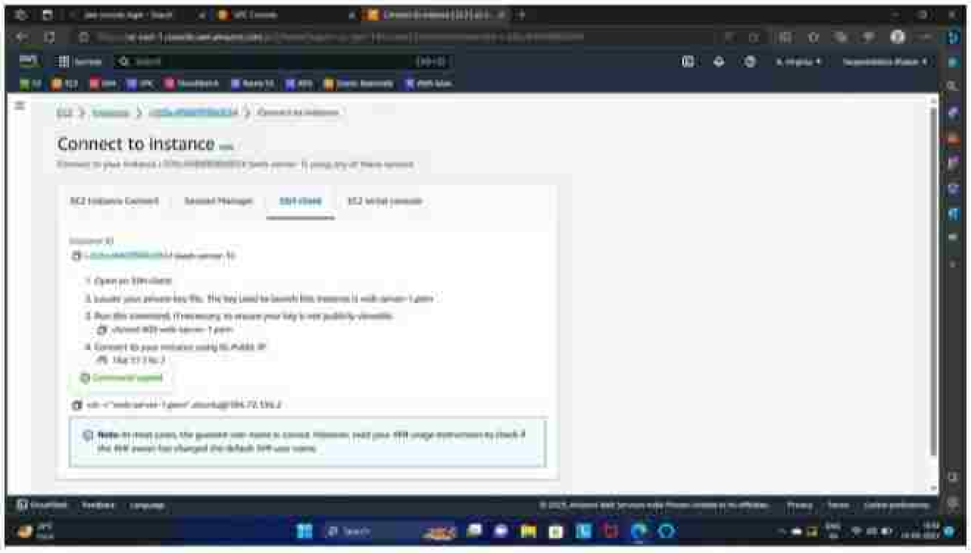
Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-	-	No

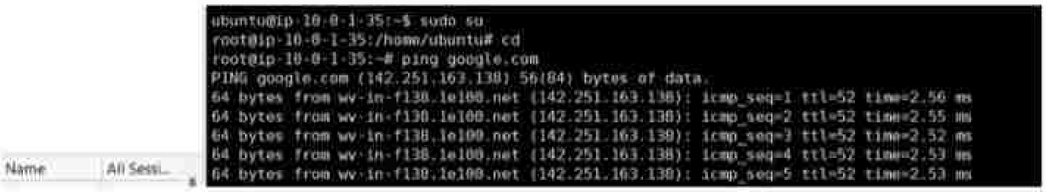
If ssh connection of web server is set-up in Xshell and from there ping google.com is done , it is seen internet is accessible.



Instances

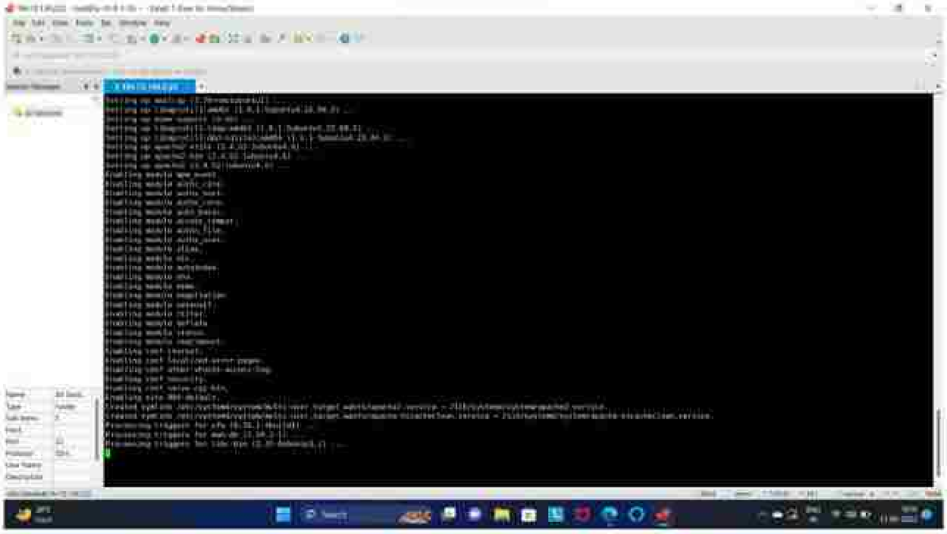


Connect to instance

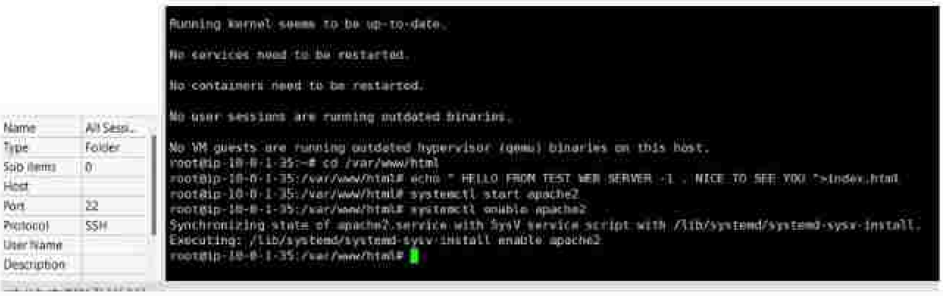


```
ubuntu@ip-10-0-1-35:~$ sudo su
root@ip-10-0-1-35:/home/ubuntu# cd
root@ip-10-0-1-35:~# ping google.com
PING google.com (142.251.163.138) 56(84) bytes of data.
64 bytes from wv-in-f138.1e100.net (142.251.163.138): icmp_seq=1 ttl=52 time=2.56 ms
64 bytes from wv-in-f138.1e100.net (142.251.163.138): icmp_seq=2 ttl=52 time=2.55 ms
64 bytes from wv-in-f138.1e100.net (142.251.163.138): icmp_seq=3 ttl=52 time=2.52 ms
64 bytes from wv-in-f138.1e100.net (142.251.163.138): icmp_seq=4 ttl=52 time=2.53 ms
64 bytes from wv-in-f138.1e100.net (142.251.163.138): icmp_seq=5 ttl=52 time=2.53 ms
```

- **STEP 8 :** A web-page is configured in both the servers in Public subnet.

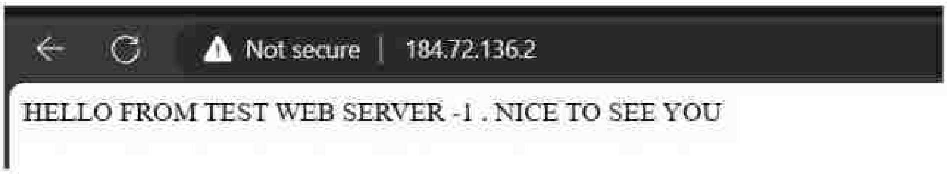


```
Setting up [illegible]
Setting up [illegible]
Setting up [illegible]
Setting up [illegible]
Setting up [illegible]
Setting up apache2-utils [illegible] ...
Setting up apache2-bin [illegible] ...
Setting up apache2 [illegible] ...
Enabling module mpm_event.
Enabling module authz_core.
Enabling module authz_host.
Enabling module authn_core.
Enabling module auth_basic.
Enabling module access_compat.
Enabling module authn_file.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink [illegible]
Created symlink [illegible]
Processing triggers for [illegible] ...
Processing triggers for [illegible] ...
Processing triggers for [illegible] ...
```



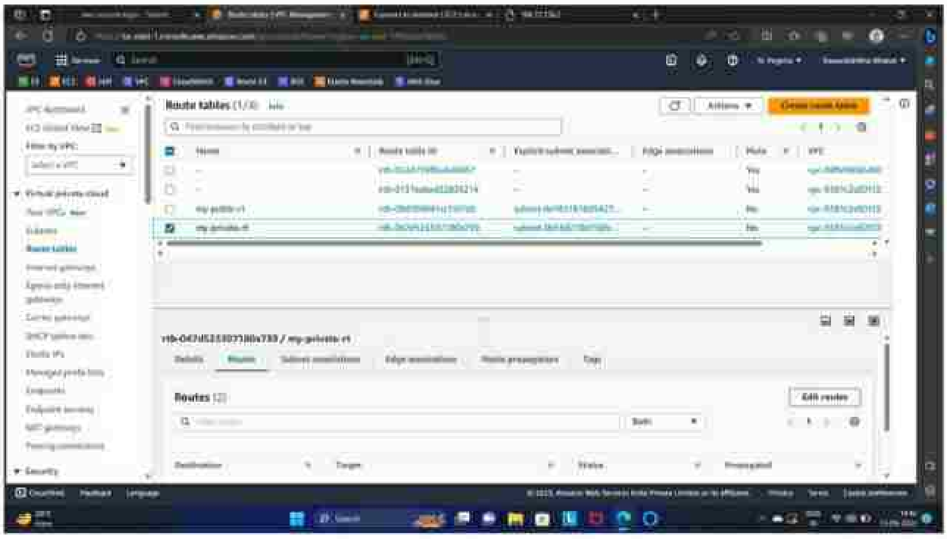
Name	All Sessi..
Type	Folder
Sub items	0
Host	
Port	22
Protocol	SSH
User Name	
Description	

```
Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@ip-10-0-1-35:~# cd /var/www/html
root@ip-10-0-1-35:/var/www/html# echo " HELLO FROM TEST WEB SERVER -1 . NICE TO SEE YOU ">index.html
root@ip-10-0-1-35:/var/www/html# systemctl start apache2
root@ip-10-0-1-35:/var/www/html# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
root@ip-10-0-1-35:/var/www/html# 
```



HELLO FROM TEST WEB SERVER -1 . NICE TO SEE YOU

- **STEP 9 :** Private route table is created and then associated with private subnet.



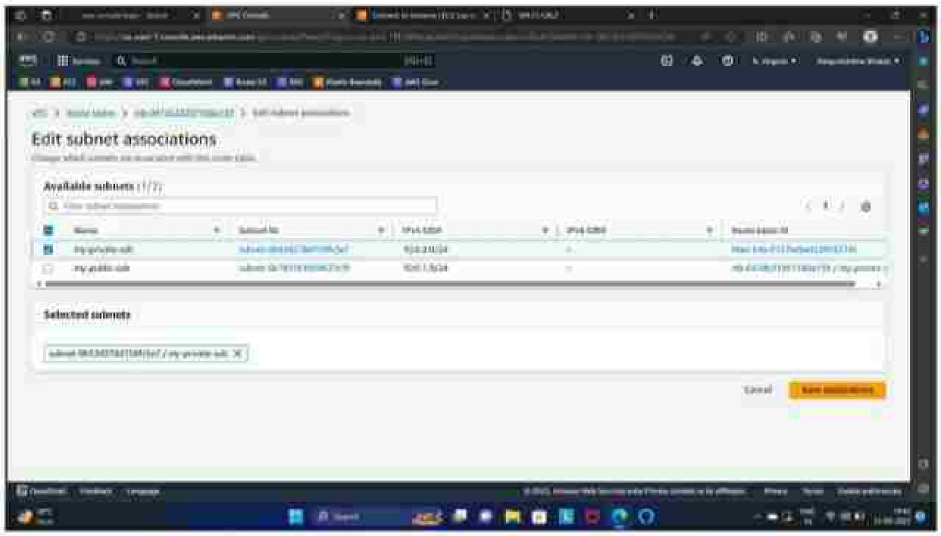
Route tables (1/4) Info

☐	Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC
☐	–	[illegible]	–	–	Yes	[illegible]
☐	–	[illegible]	–	–	Yes	[illegible]
☐	my-public-rt	[illegible]	[illegible]	–	No	[illegible]
☑	my-private-rt	[illegible]	[illegible]	–	No	[illegible]

rtb-047d5233073180a793 / my-private-rt

Routes (2)

Destination	Target	Status	Propagated



Edit subnet associations

Available subnets (1/2)

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	my-private-sub	[illegible]	10.0.2.0/24	-	[illegible]
□	my-public-sub	[illegible]	10.0.1.0/24	-	[illegible] / my-private

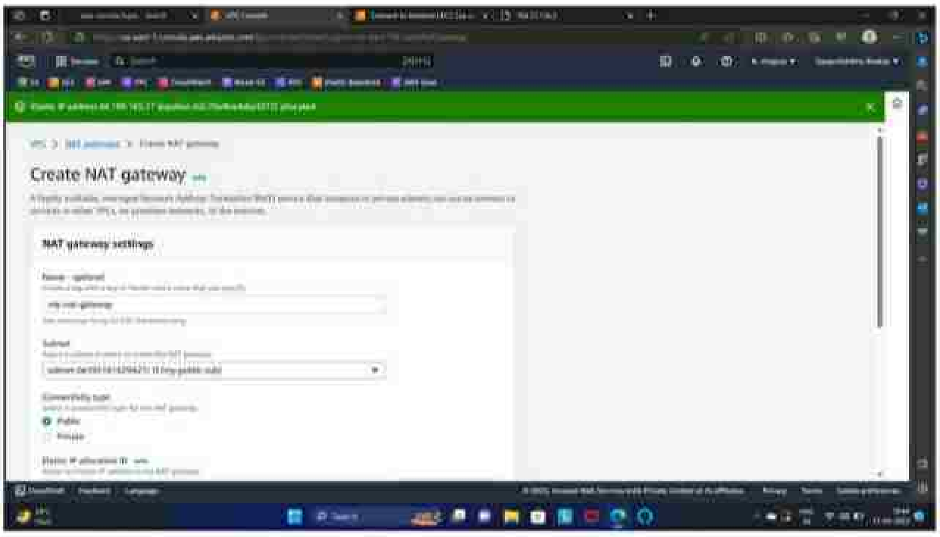
Selected subnets

[illegible] / my-private-sub ✕

Cancel

Save associations

- **STEP 10 :** NAT-gateway is created in Public subnet and then associated with private subnet via its route table so that the db-server can access internet.



Create NAT gateway

NAT gateway settings

Name - optional: my-nat-gateway

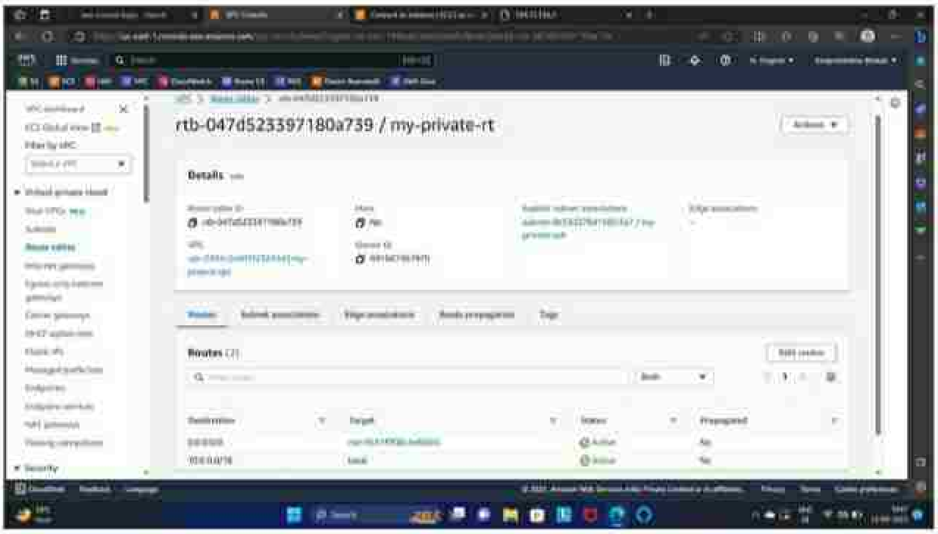
Subnet: [illegible] (my-public-sub)

Connectivity type

● Public

○ Private

Elastic IP allocation ID



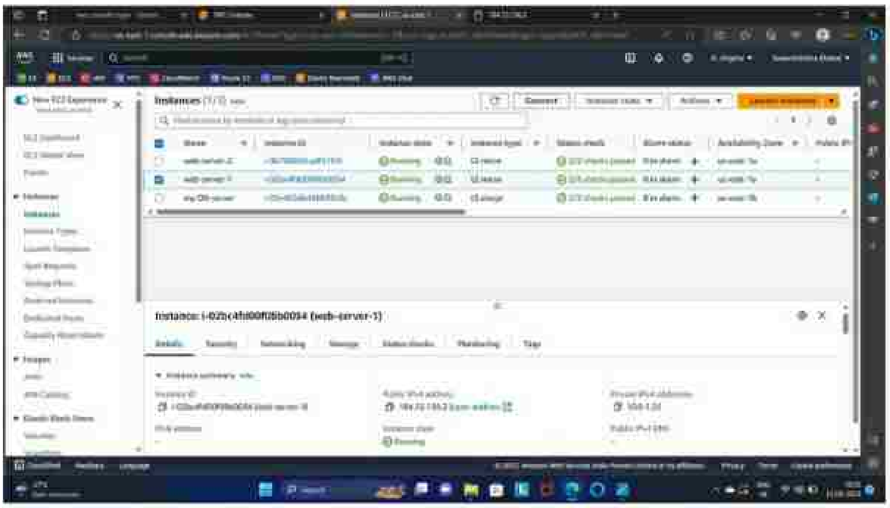
rtb-047d523397180a739 / my-private-rt

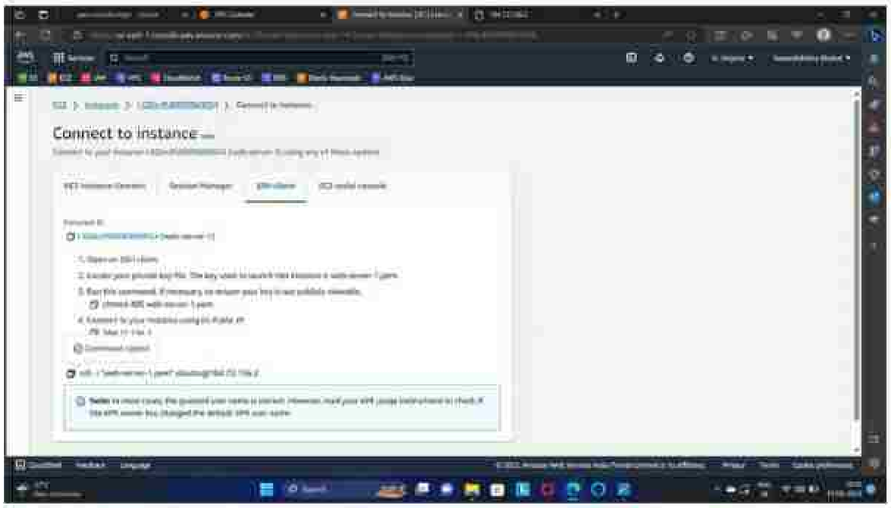
Details

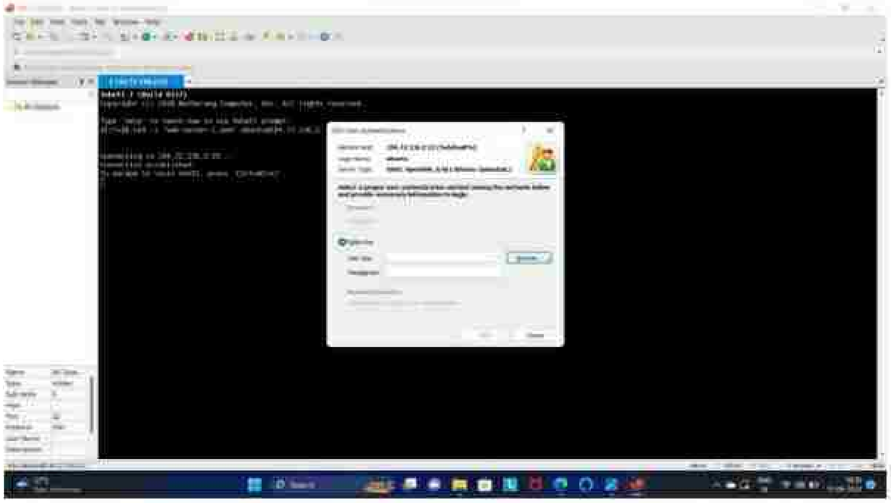
Routes (2)

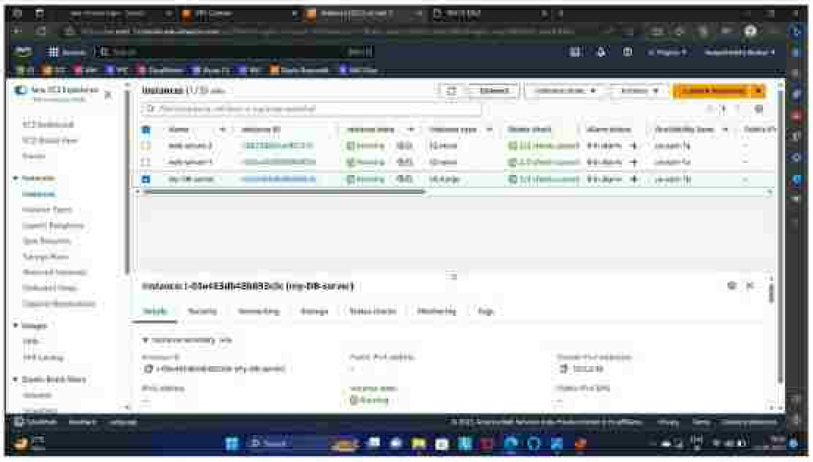
Destination	Target	Status	Propagated
0.0.0.0/0	nat-[illegible]	Active	No
10.0.0.0/16	local	Active	No

Web-server is configured in Xshell via ssh, and then ssh connection of database server is done. If ping google.com is written , it is seen that internet is accessed by db-server via nat-gateway . But still no-one can access db-server by internet.



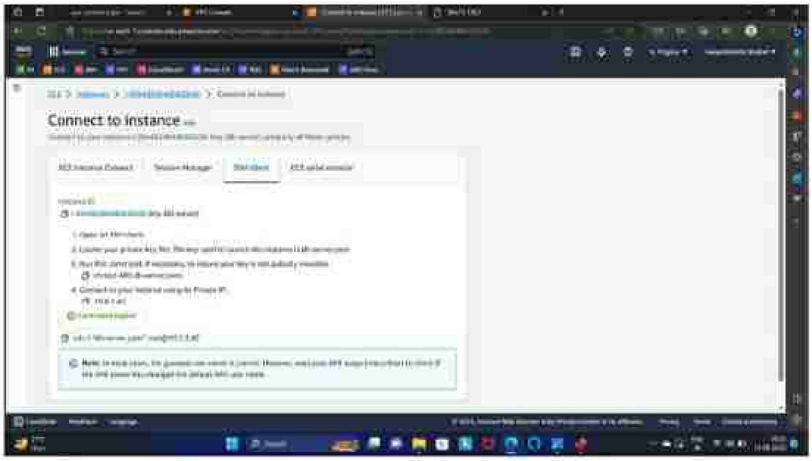




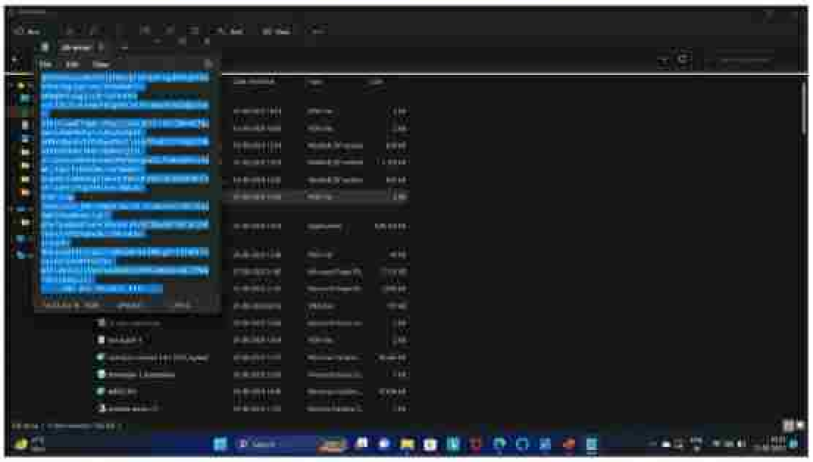


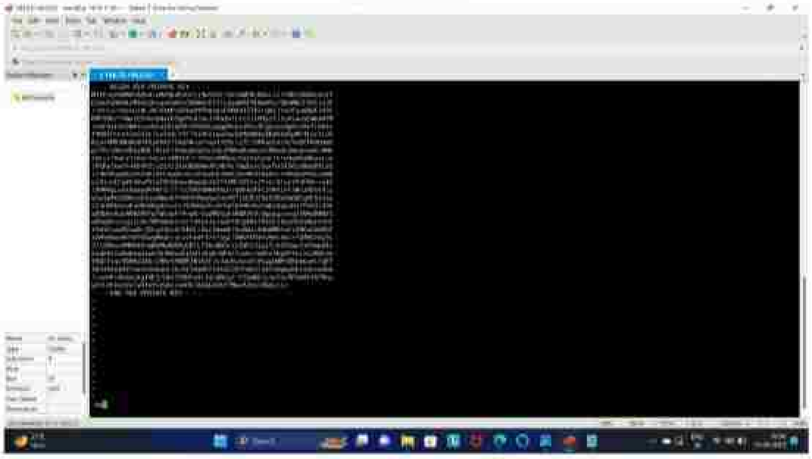
Instances (1/3)

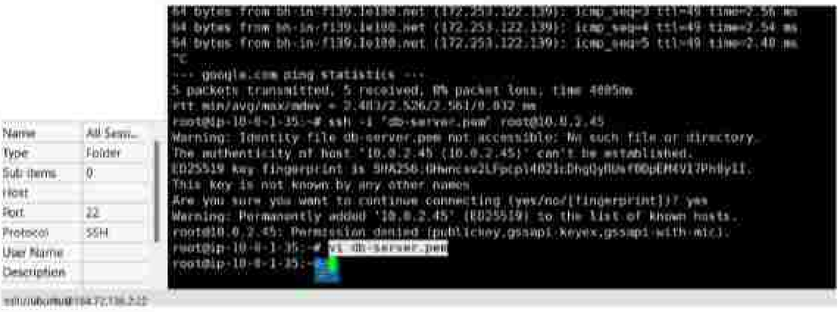
Instance: i-05e483db48b893c0c (my-DB-server)



Connect to instance

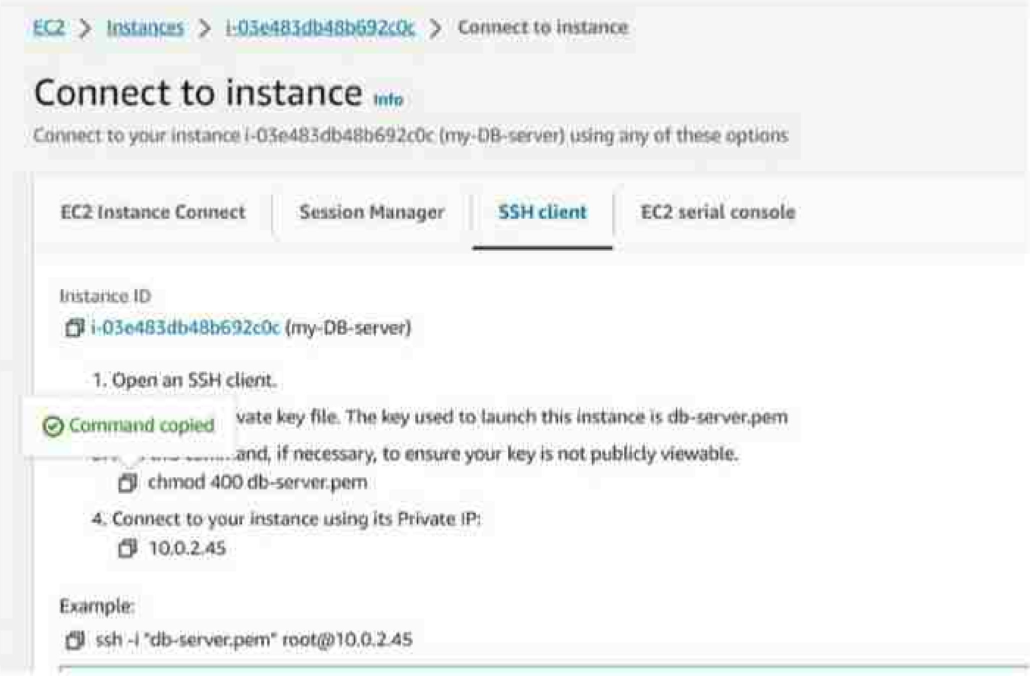






Name	All Sessi...
Type	Folder
Sub items	0
Host	
Port	22
Protocol	SSH
User Name	
Description	

```
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=3 ttl=49 time=2.56 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=4 ttl=49 time=2.54 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=5 ttl=49 time=2.40 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 2.483/2.526/2.561/0.032 ms
root@ip-10-0-1-35:~# ssh -i 'db-server.pem' root@10.0.2.45
Warning: Identity file db-server.pem not accessible: No such file or directory.
The authenticity of host '10.0.2.45 (10.0.2.45)' can't be established.
ED25519 key fingerprint is SHA256:GHwncxv2LFpcpl4021cDhgQyRUsf0DpEM4VI7Ph8y1I.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.45' (ED25519) to the list of known hosts.
root@10.0.2.45: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
root@ip-10-0-1-35:~# vi db-server.pem
root@ip-10-0-1-35:~#
```



EC2 > Instances > i-03e483db48b692c0c > Connect to instance

Connect to instance Info

Connect to your instance i-03e483db48b692c0c (my-DB-server) using any of these options

Instance ID

i-03e483db48b692c0c (my-DB-server)

1. Open an SSH client.

vate key file. The key used to launch this instance is db-server.pem

and, if necessary, to ensure your key is not publicly viewable.

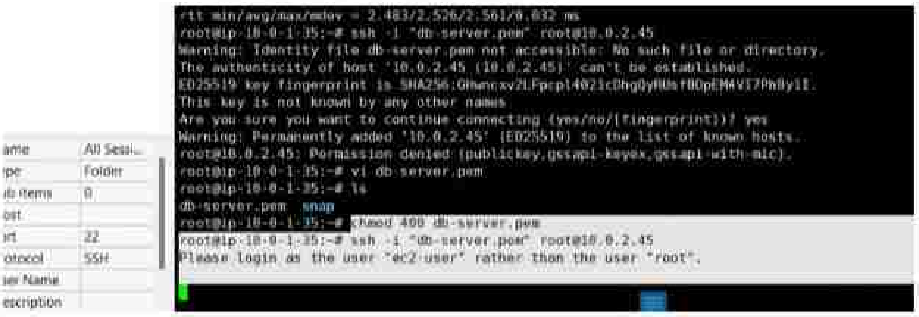
chmod 400 db-server.pem

4. Connect to your instance using its Private IP:

10.0.2.45

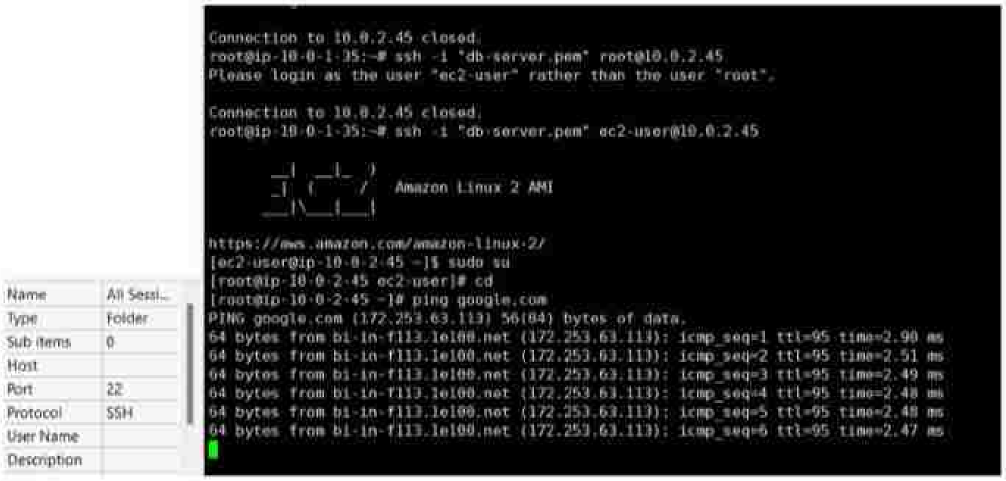
Example:

ssh -i "db-server.pem" root@10.0.2.45



ame	All Sessi...
ype	Folder
ub items	0
ost	
rt	22
otocol	SSH
ser Name	
escription	

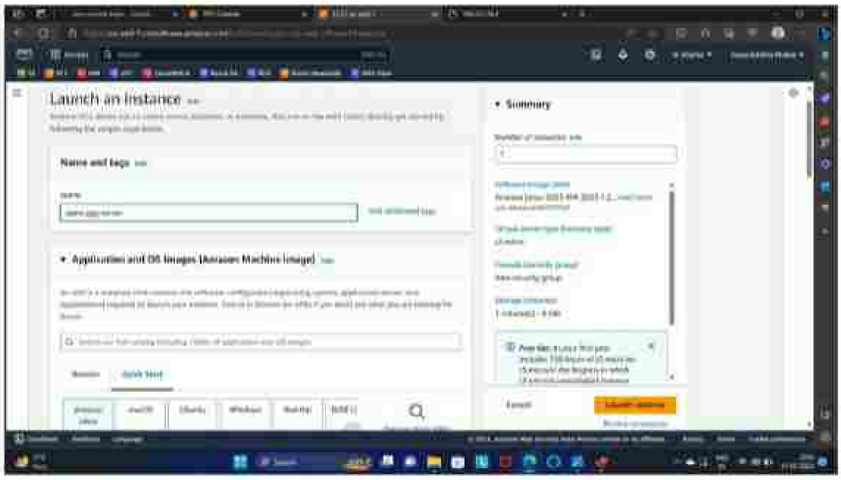
```
rtt min/avg/max/mdev = 2.483/2.526/2.561/0.032 ms
root@ip-10-0-1-35:~# ssh -i "db-server.pem" root@10.0.2.45
Warning: Identity file db-server.pem not accessible: No such file or directory.
The authenticity of host '10.0.2.45 (10.0.2.45)' can't be established.
ED25519 key fingerprint is SHA256:GHwncxv2LFpcpl4021cDhgQyRUsf0DpEM4VI7Ph8y1I.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.45' (ED25519) to the list of known hosts.
root@10.0.2.45: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
root@ip-10-0-1-35:~# vi db-server.pem
root@ip-10-0-1-35:~# ls
db-server.pem  snap
root@ip-10-0-1-35:~# chmod 400 db-server.pem
root@ip-10-0-1-35:~# ssh -i "db-server.pem" root@10.0.2.45
Please login as the user "ec2-user" rather than the user "root".
```

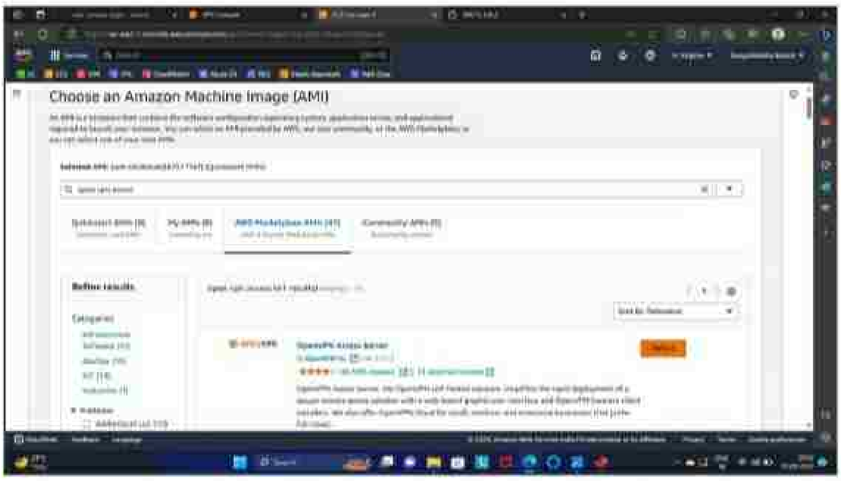


Name	All Sessi...
Type	Folder
Sub items	0
Host	
Port	22
Protocol	SSH
User Name	
Description	

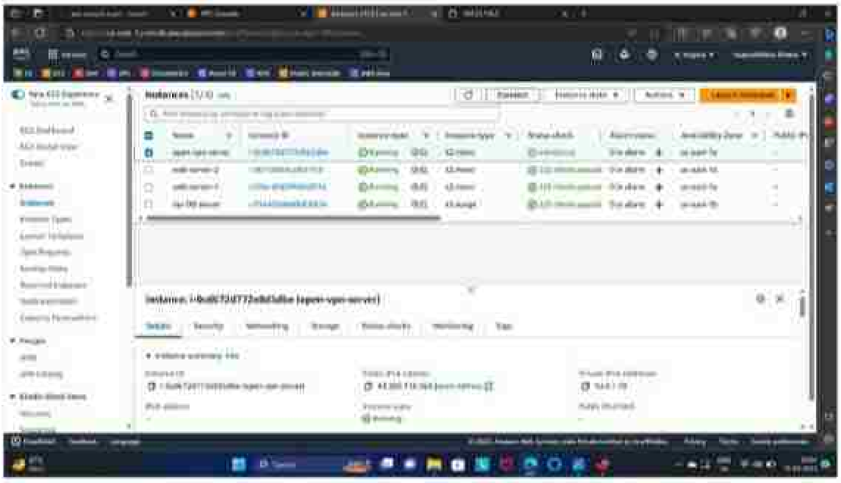
```
Connection to 10.0.2.45 closed.
root@ip-10-0-1-35:~# ssh -i "db-server.pem" root@10.0.2.45
Please login as the user "ec2-user" rather than the user "root".

Connection to 10.0.2.45 closed.
root@ip-10-0-1-35:~# ssh -i "db-server.pem" ec2-user@10.0.2.45

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-2-45 ~]$ sudo su
[root@ip-10-0-2-45 ec2-user]# cd
[root@ip-10-0-2-45 ~]# ping google.com
PING google.com (172.253.63.113) 56(84) bytes of data.
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=1 ttl=95 time=2.90 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=2 ttl=95 time=2.51 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=3 ttl=95 time=2.49 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=4 ttl=95 time=2.48 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=5 ttl=95 time=2.48 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=6 ttl=95 time=2.47 ms
```

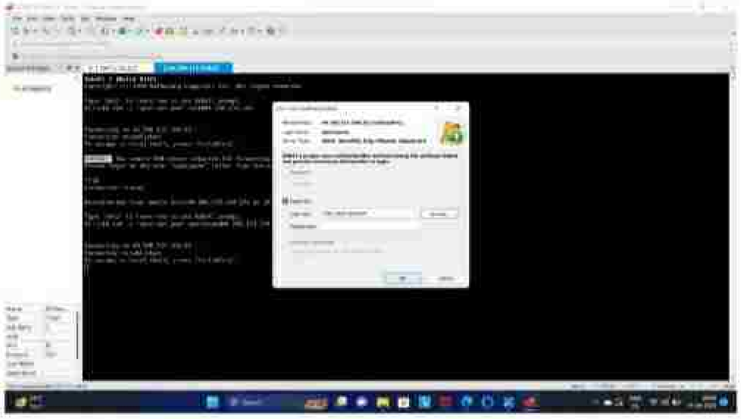
- **STEP 11 :** Open VPN set-up is done .

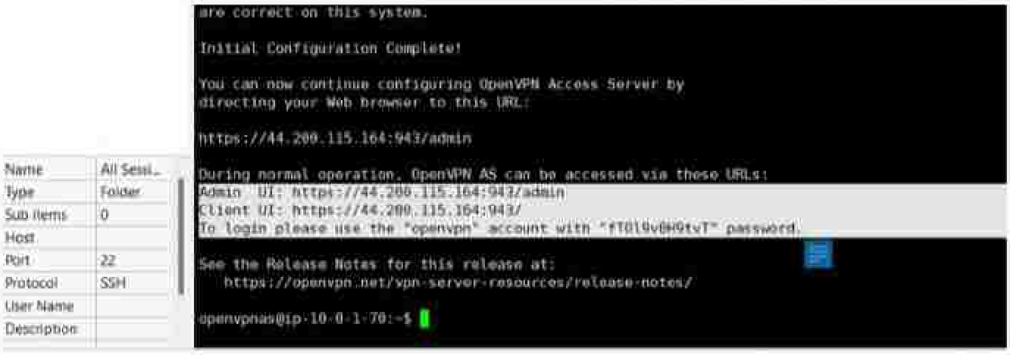




Now, open-vpn server is connected in Xshell by ssh, and then ADMIN UI, client UI, user-ID and password is configured.

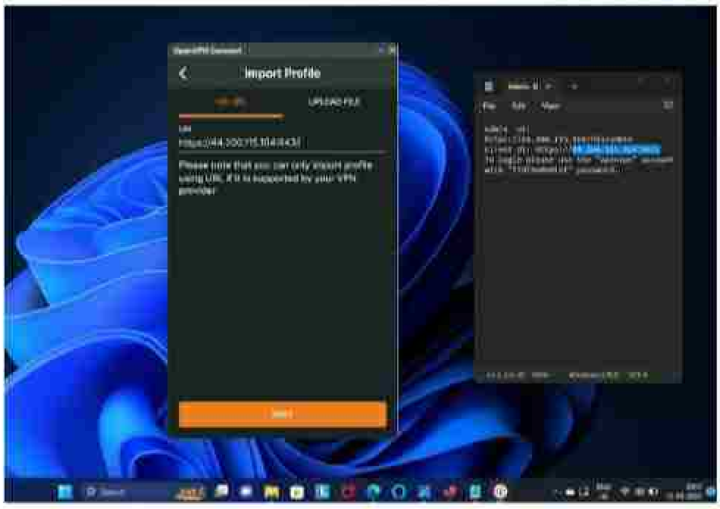






Name	All Sessi...
Type	Folder
Sub items	0
Host	
Port	22
Protocol	SSH
User Name	
Description	

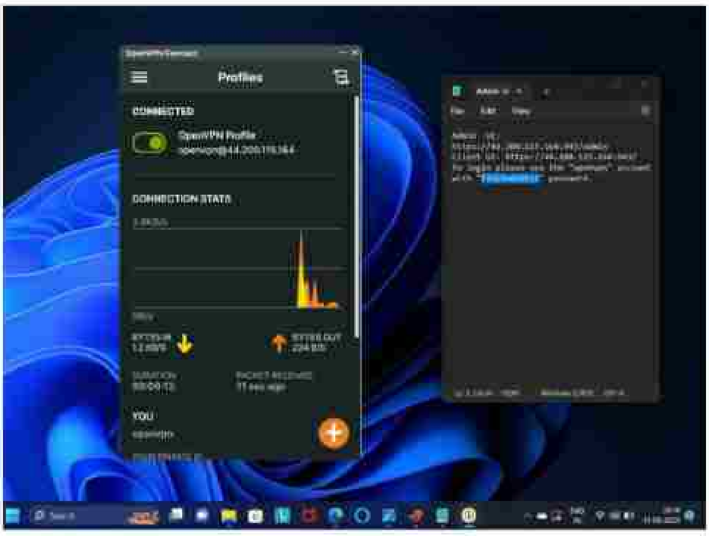
```
are correct on this system.

Initial Configuration Complete!

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

https://44.200.115.164:943/admin

During normal operation, OpenVPN AS can be accessed via these URLs:
Admin  UI: https://44.200.115.164:943/admin
Client UI: https://44.200.115.164:943/
To login please use the "openvpn" account with "fTOl9v0H9tvT" password.

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

openvpnas@ip-10-0-1-70:~$ 
```



URL

https://44.200.115.164:943/

Please note that you can only import profile using URL if it is supported by your VPN provider



OpenVPN Connect

Profiles

CONNECTED

OpenVPN Profile

CONNECTION STATS

BYTES IN

BYTES OUT

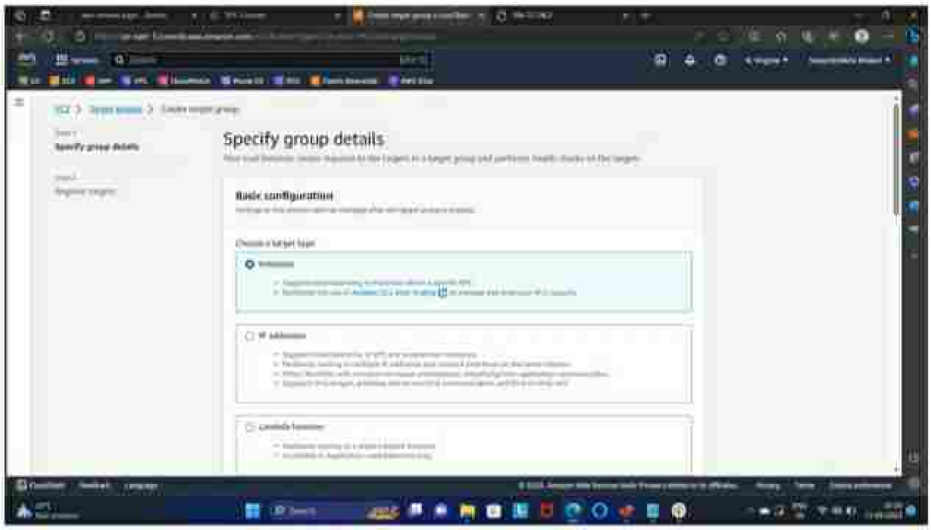
DURATION

PACKET RECEIVED

YOU

```
Admin UI:
Client UI:
To login please use the "openvpn" account
with [illegible] password.
```

- **STEP 12 :** Target group is created of type-Instances.



EC2 > Target groups > Create target group

Step 1
Specify group details

Step 2
Register targets

Specify group details

Basic configuration

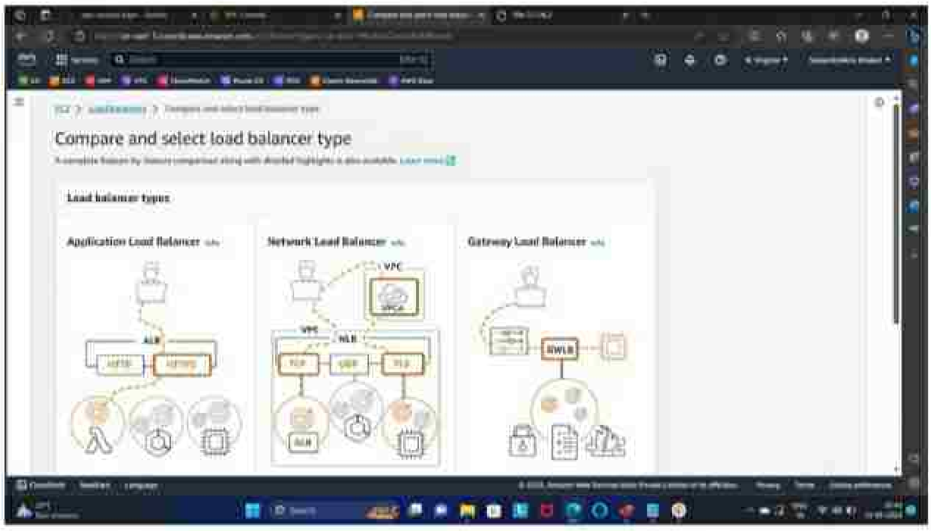
Choose a target type

● Instances

○ IP addresses

○ Lambda function

- **STEP 13 :** Application Load Balancer is configured.



EC2 > Load balancers > Compare and select load balancer type

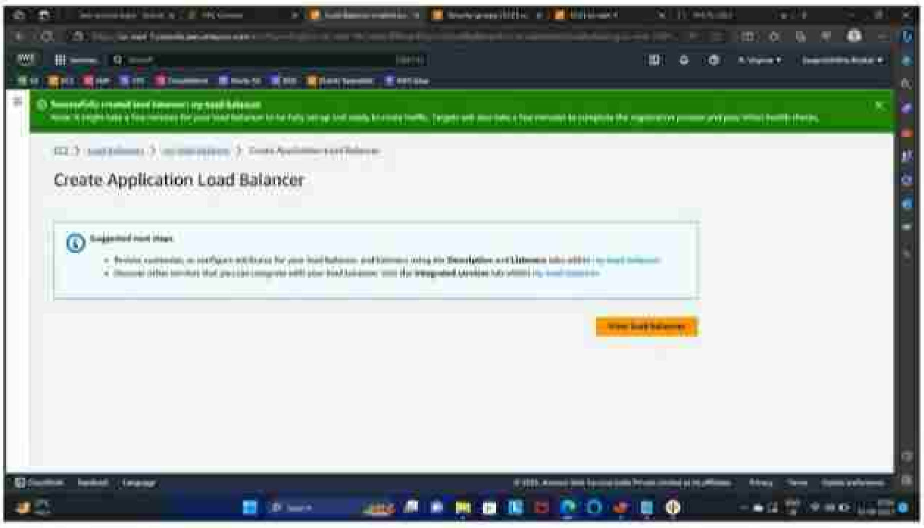
Compare and select load balancer type

Load balancer types

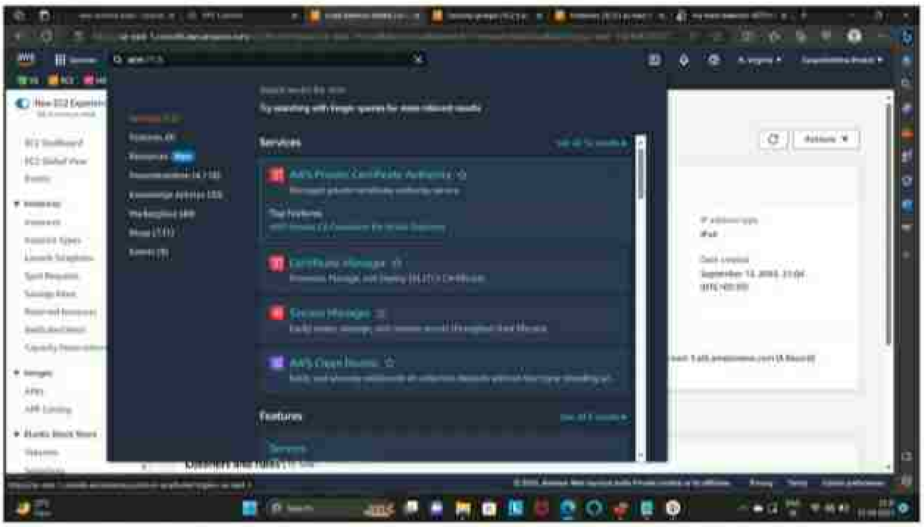
Application Load Balancer Info

Network Load Balancer Info

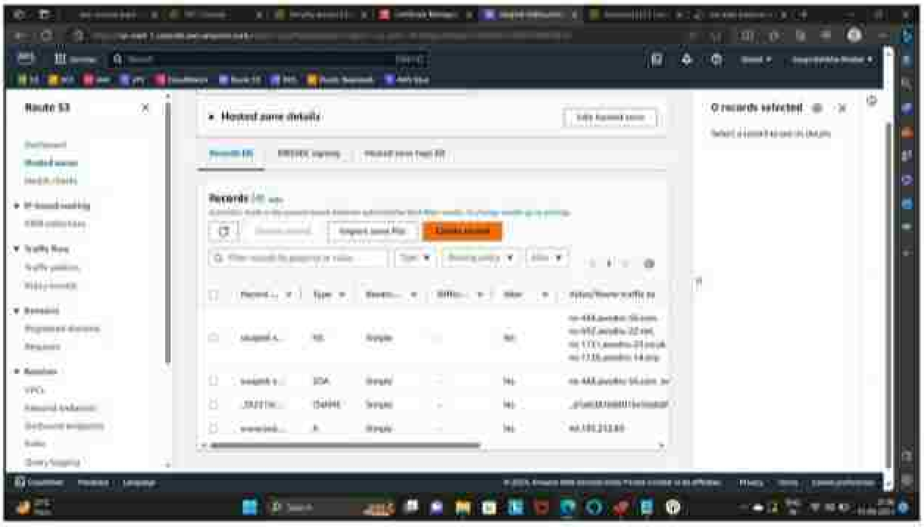
Gateway Load Balancer Info

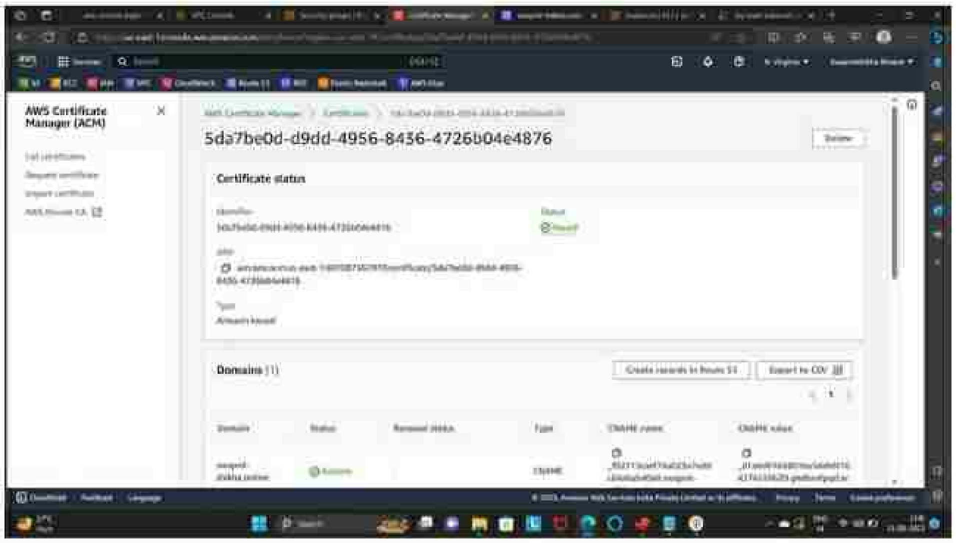


- **STEP 14 :** SSL certificate is being issued for secured connection with a domain name, swapnil-shikha.online.



CNAME is seen in the hosted zone of Route 53.





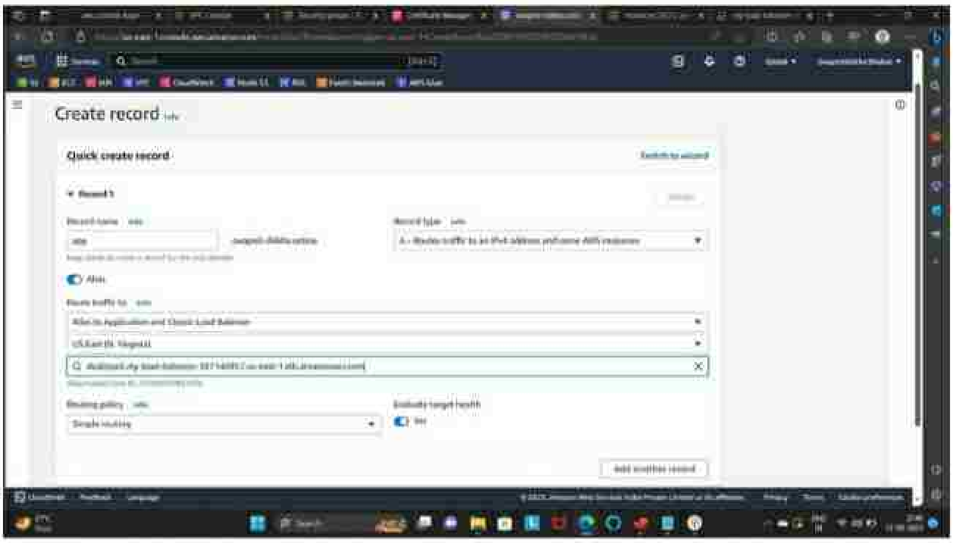
AWS Certificate Manager (ACM)

5da7be0d-d9dd-4956-8436-4726b04e4876

Certificate status

Domains (1)

- **STEP 15 :** A record is created in the hosted zones of Route 53 which is directed to the Application Load Balancer.

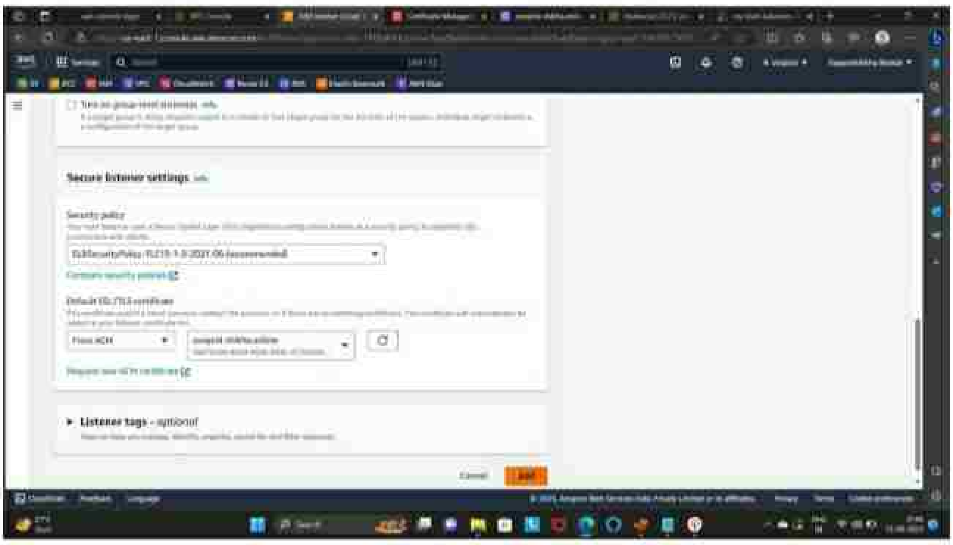


Create record

Quick create record

Alias

Simple routing



Secure listener settings

Security policy

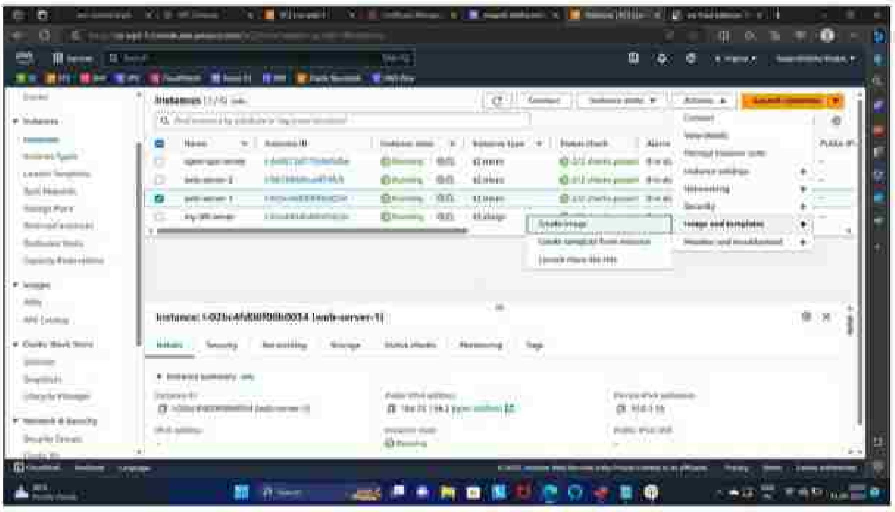
Default SSL/TLS certificate

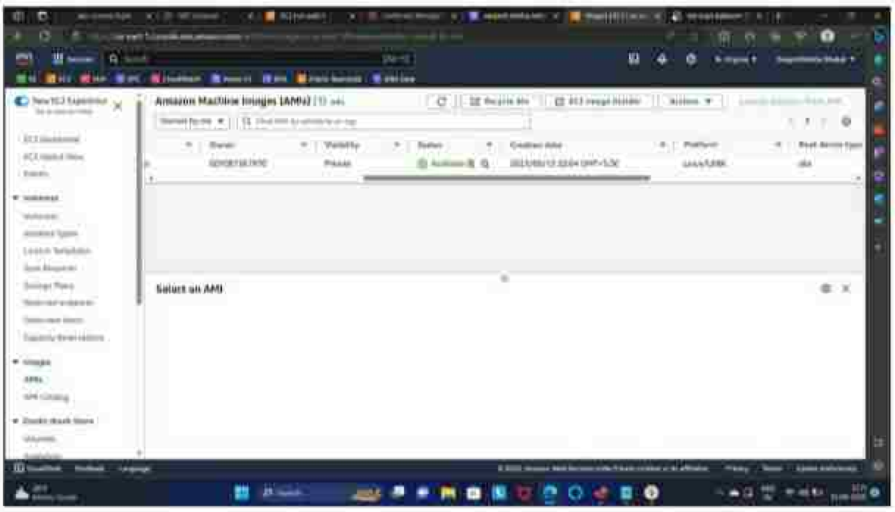
From ACM

Listener tags - optional

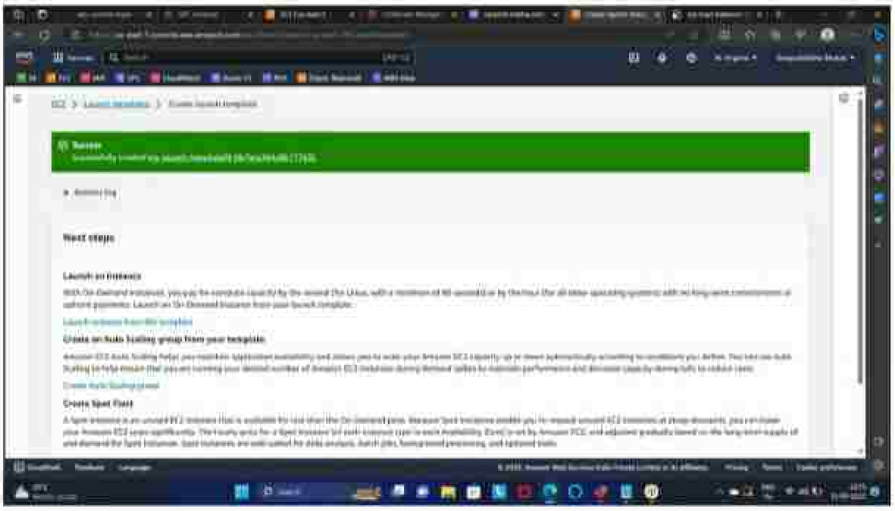
Cancel

- **STEP 16 :** To enable autoscaling, first, image of the web-server is created .

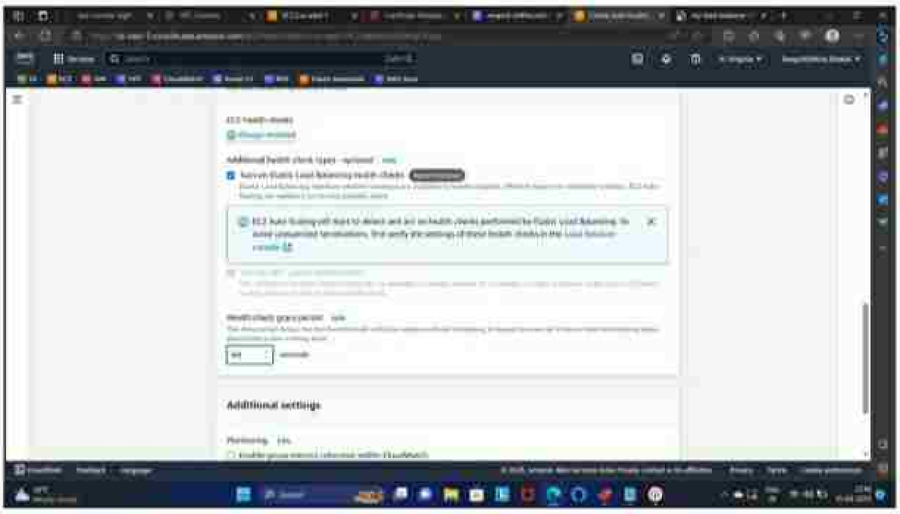




- **STEP 17 :** A launch template is created with this above image of instance type t2.micro.



- **STEP 18 :** Autoscaling group is created and attached to the existing load balancer.



EC2 health checks

Additional health check types - optional

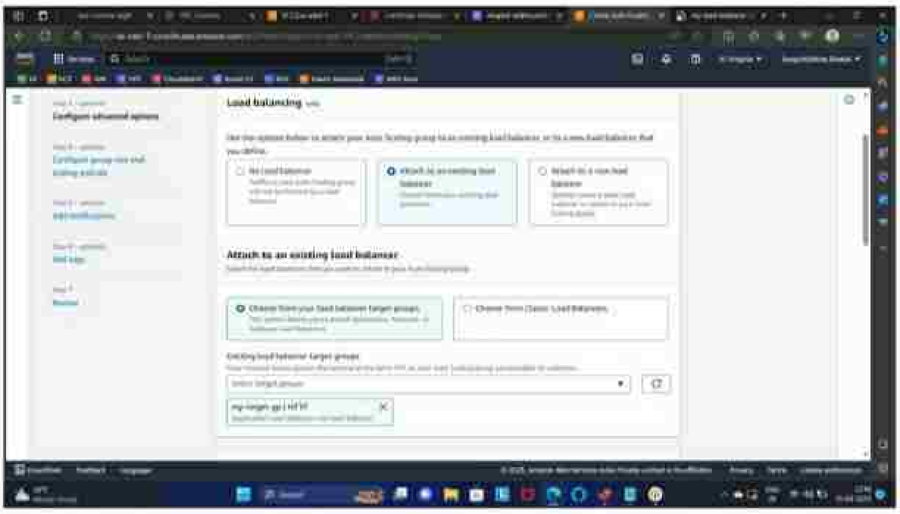
☑ Turn on Elastic Load Balancing health checks

Health check grace period

Additional settings

Monitoring

□ Enable group metrics collection within CloudWatch



Load balancing

○ No load balancer

● Attach to an existing load balancer

○ Attach to a new load balancer

Attach to an existing load balancer

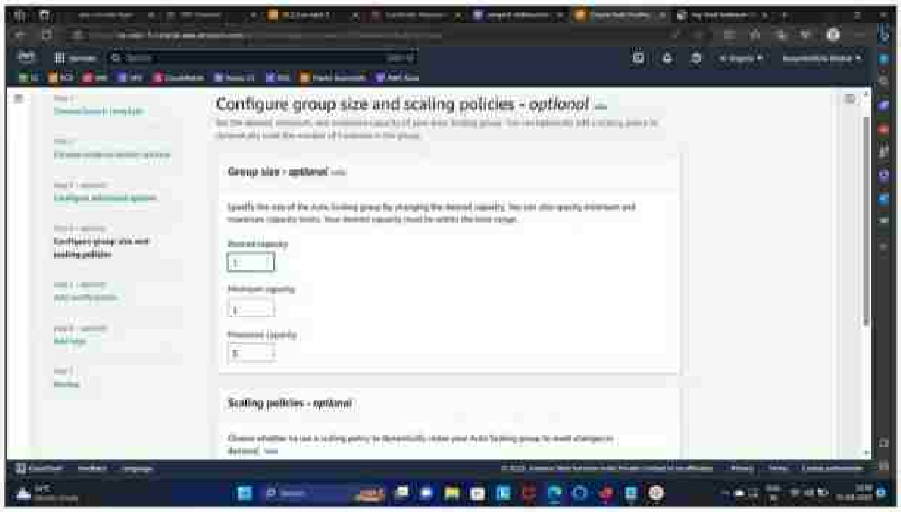
● Choose from your load balancer target groups

○ Choose from Classic Load Balancers

Existing load balancer target groups

my-target-gp | HTTP

The group size is defined with desired, minimum and maximum capacities as given below :-



Configure group size and scaling policies - *optional*

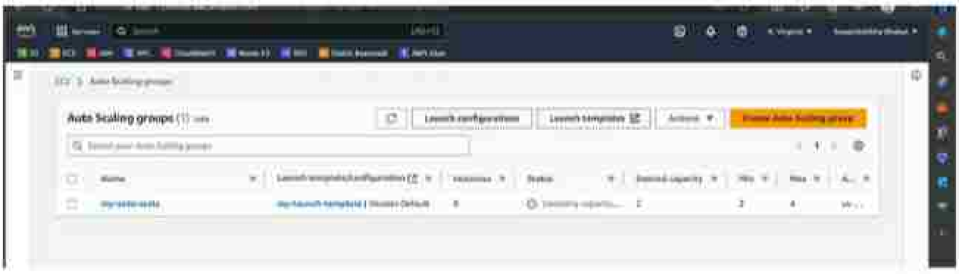
Group size - optional

Desired capacity: 1

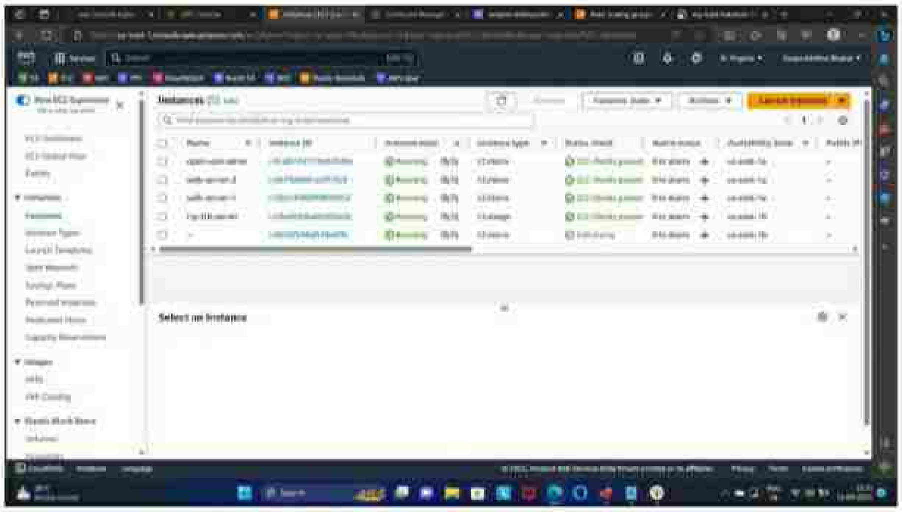
Minimum capacity: 1

Maximum capacity: 3

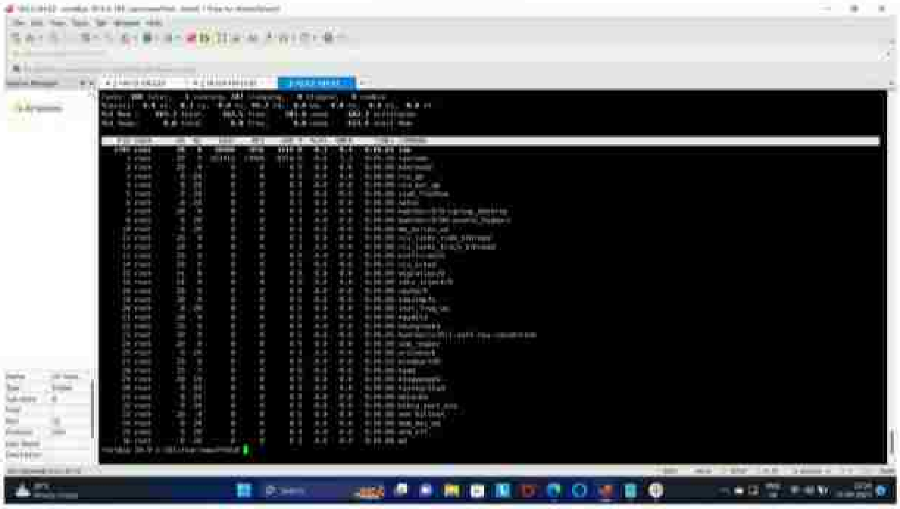
Scaling policies - optional



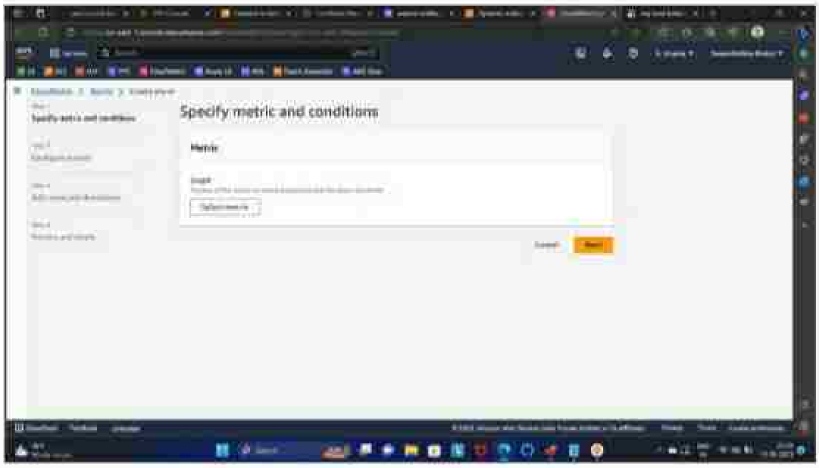
A new instance is seen to be automatically created in EC2 - Instances.



Now, this instance is connected to Xshell and 'top' command is used to display the current CPU-Utilization of the server as 0.3%.

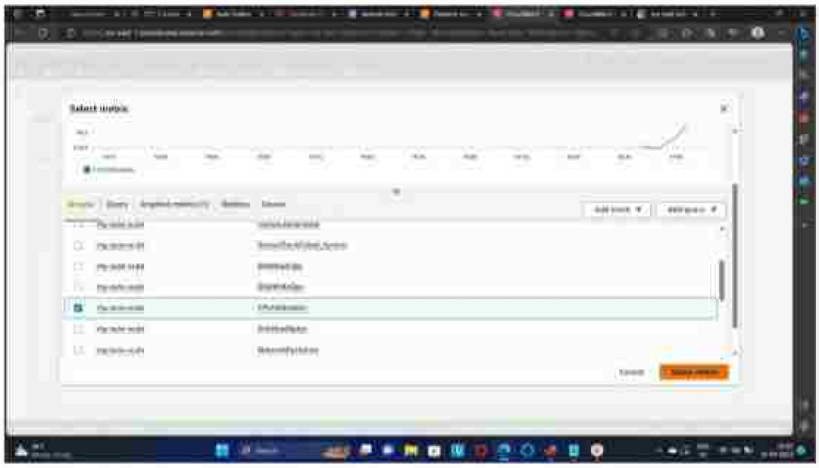


- **STEP 19 :** In the Cloudwatch section, two alarms are created. First alarm is set to notify when the CPU-Utilization is greater than or equal to 50%.

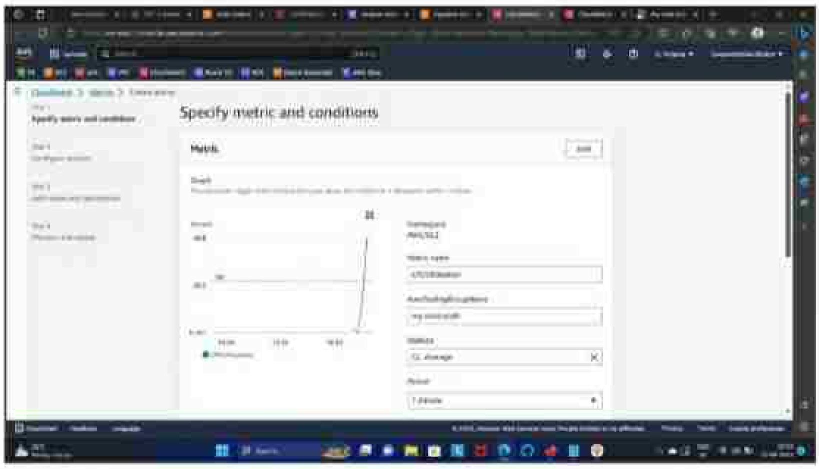


Specify metric and conditions

Metric



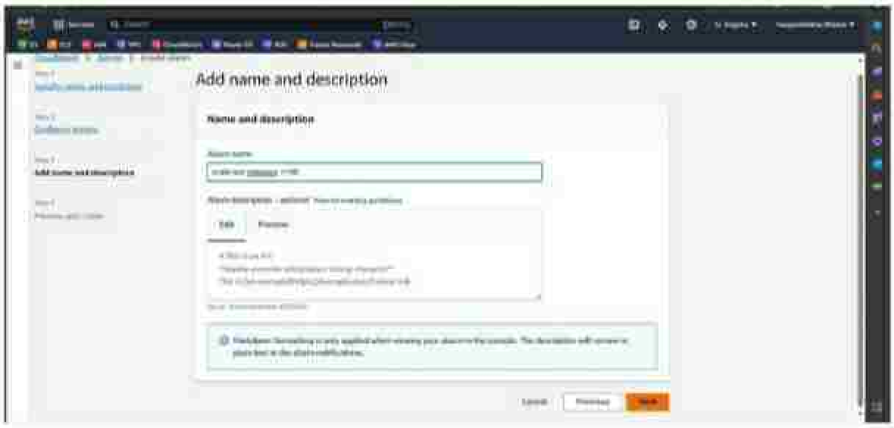
The statistic is set to average and period is set for 1 minute.



Specify metric and conditions

Metric

Alarm name is set to indentify it and then finally alarm is created.



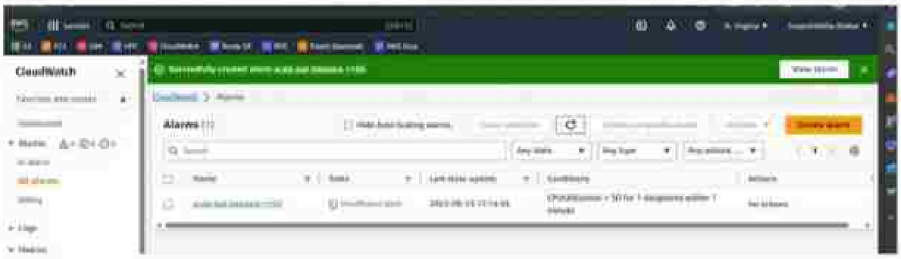
Add name and description

Name and description

Alarm name

Edit | Preview

Cancel | Previous | Next

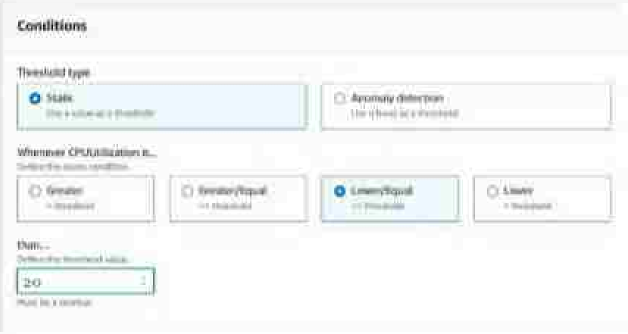


CloudWatch

Alarms (1)

Name	State	Last state update	Conditions	Actions
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Another alarm is created which is used to notify when CPU-Utiliztion is less than or equal to 20%.



Conditions

Threshold type

● Static

○ Anomaly detection

Whenever CPUUtilization is...

○ Greater

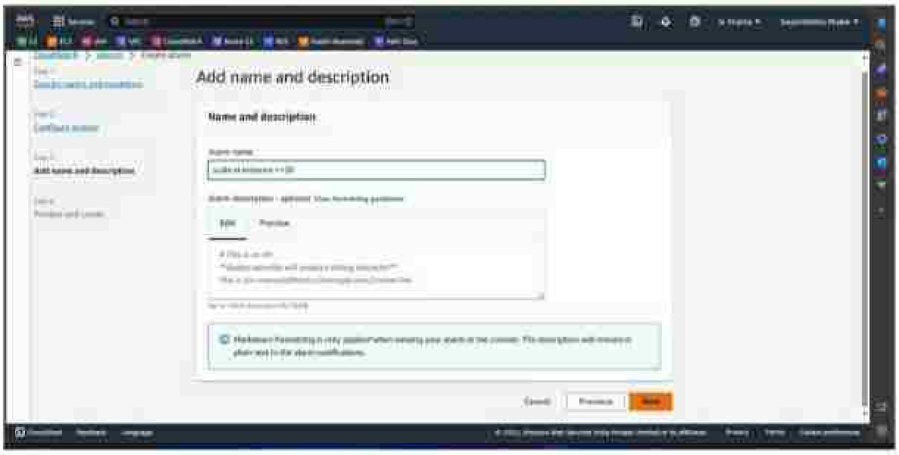
○ Greater/Equal

● Lower/Equal

○ Lower

than...

20



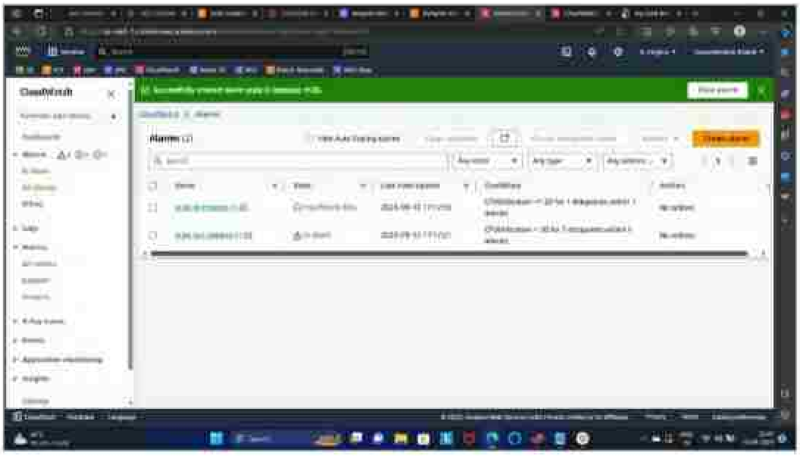
Add name and description

Name and description

Alarm name

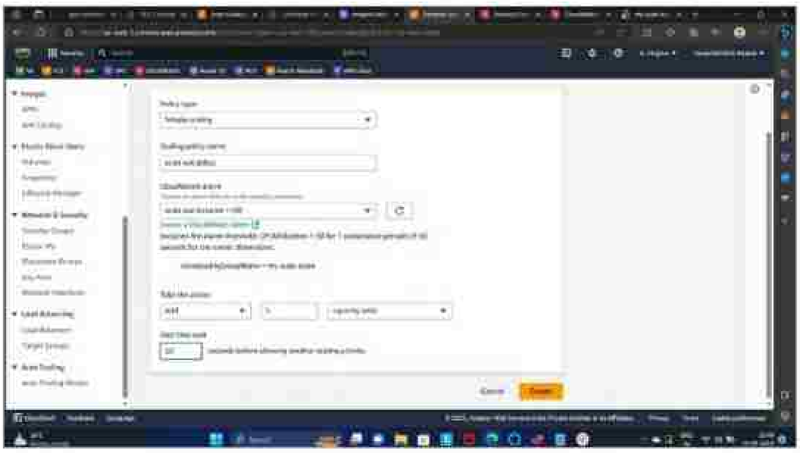
Edit | Preview

Cancel | Previous | Next



Alarms (2)

- **STEP 20 :** Next Dynamic Scaling Policy is created for both the conditions. In the first condition, one instance is automatically created when CPU-Utilization is greater than 50%.



Policy type

Simple scaling

Scaling policy name

CloudWatch alarm

Take the action

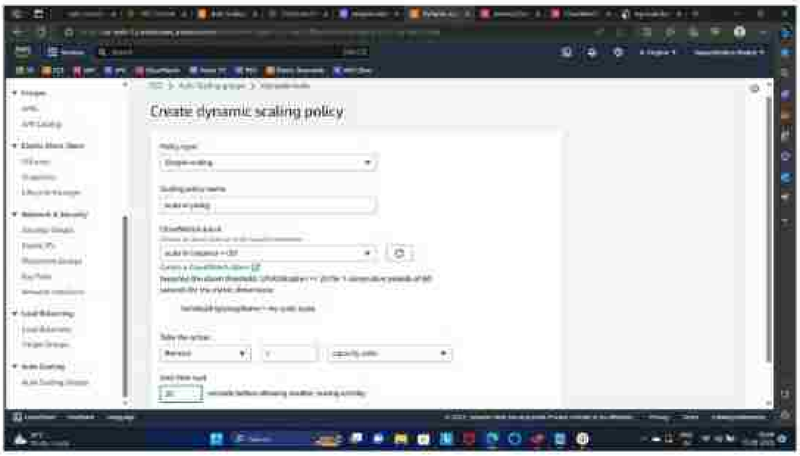
Add

capacity units

Cancel

Create

In the second condition, one instance is automatically removed when CPU-Utilization is less than 20%.



Create dynamic scaling policy

Policy type

Simple scaling

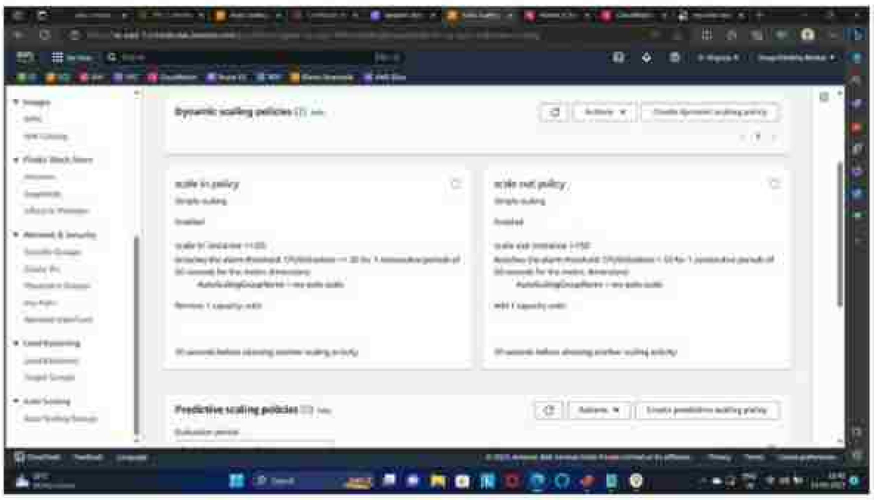
Scaling policy name

CloudWatch alarm

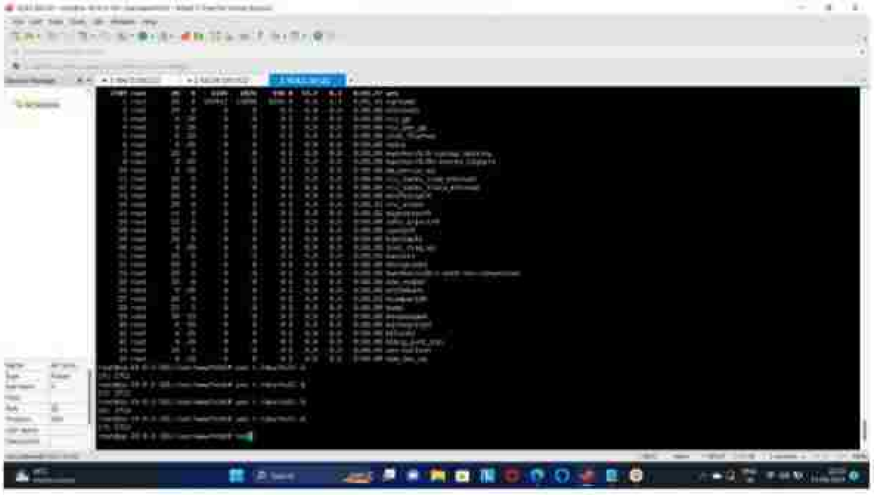
Take the action

Remove

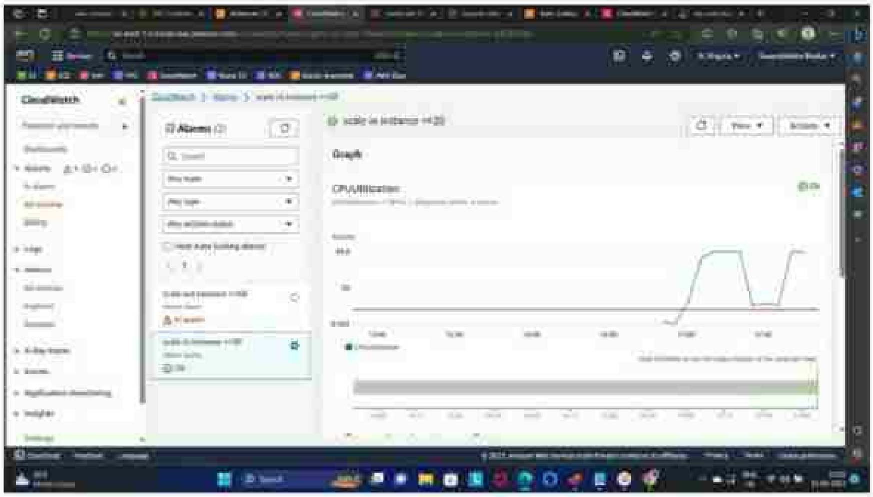
capacity units



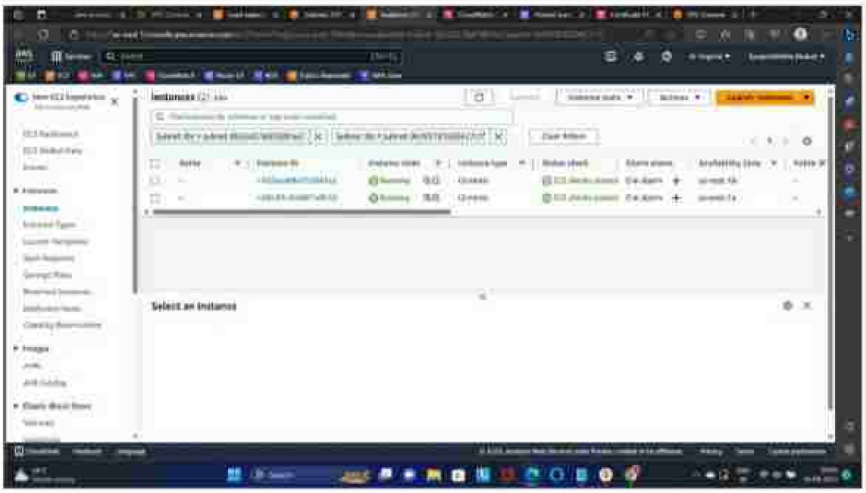
- **STEP 21 :** Now, go back to the Xshell and 'yes > /dev/null &' command is run multiple times to increase the CPU-Utilization of the server. Then 'top' command is run to display .



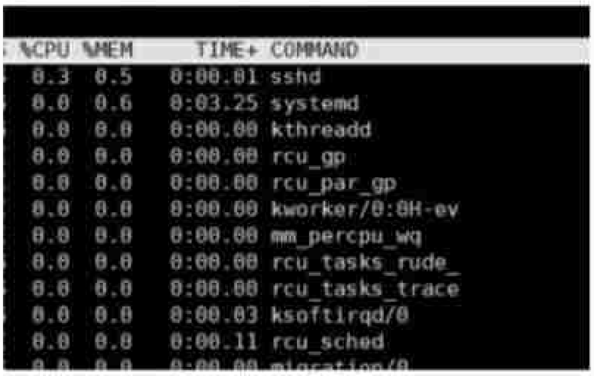
It is seen that scale-out alarm is active now.



A new instance is automatically created in the EC2 . After waiting for few more minutes , it is seen that a new instance is created again and now, both are in running state.

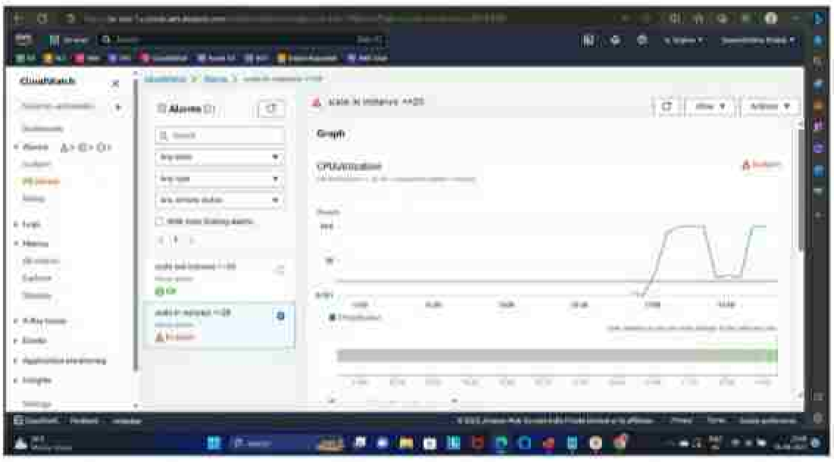


- **STEP 22 :** Now, 'killall yes' command is run in the same Xshell connection to decrease the CPU-Utilization of the server. It is seen that CPU-Utilization is now decreased to 0.3%.

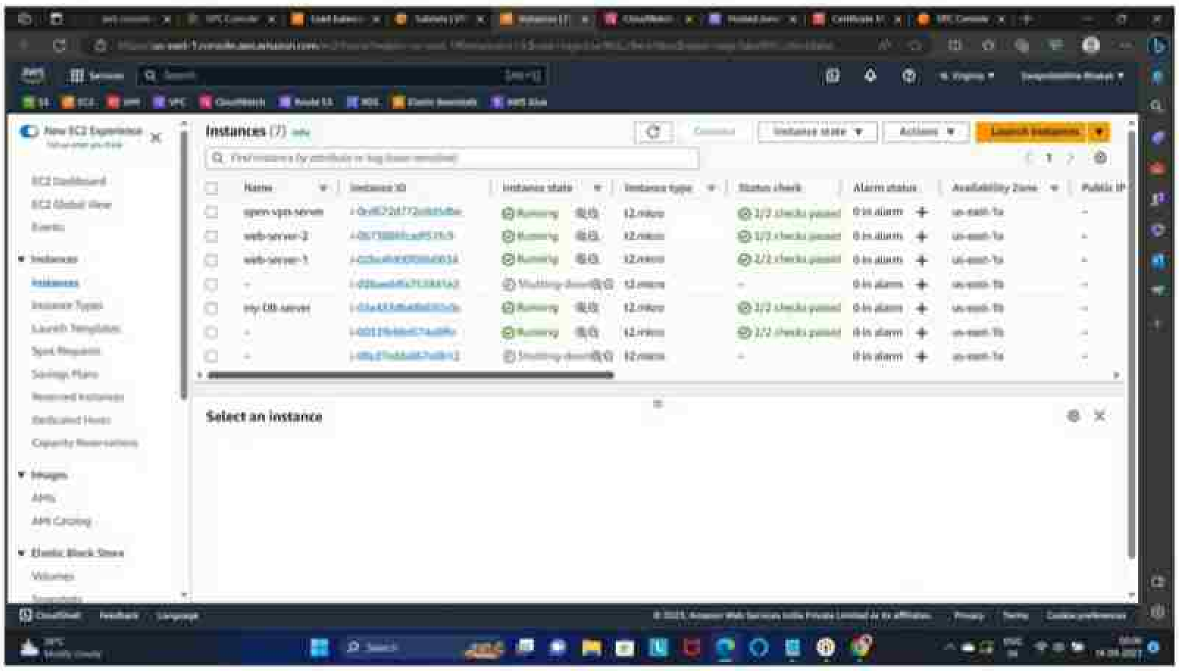


```
 %CPU %MEM     TIME+ COMMAND
  0.3  0.5   0:00.01 sshd
  0.0  0.6   0:03.25 systemd
  0.0  0.0   0:00.00 kthreadd
  0.0  0.0   0:00.00 rcu_gp
  0.0  0.0   0:00.00 rcu_par_gp
  0.0  0.0   0:00.00 kworker/0:0H-ev
  0.0  0.0   0:00.00 mm_percpu_wq
  0.0  0.0   0:00.00 rcu_tasks_rude_
  0.0  0.0   0:00.00 rcu_tasks_trace
  0.0  0.0   0:00.03 ksoftirqd/0
  0.0  0.0   0:00.11 rcu_sched
  0.0  0.0   0:00.00 migration/0
```

It is seen that scale-in alarm is active now.



It can be seen that when CPU-Utilization is less than 20%, an alarm is triggered and the newly created instances automatically gets shut-down to avoid overuse. Thus, AWS autoscaling helps to optimise our resource utilization.



Instances (7)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
open-vpn-server	[illegible]	Running	t2.micro	2/2 checks passed	0 in alarm	us-east-1a	–
web-server-2	[illegible]	Running	t2.micro	2/2 checks passed	0 in alarm	us-east-1a	–
web-server-1	[illegible]	Running	t2.micro	2/2 checks passed	0 in alarm	us-east-1a	–
–	[illegible]	Shutting-down	t2.micro	–	0 in alarm	us-east-1b	–
my-DB-server	[illegible]	Running	t2.micro	2/2 checks passed	0 in alarm	us-east-1b	–
–	[illegible]	Running	t2.micro	2/2 checks passed	0 in alarm	us-east-1b	–
–	[illegible]	Shutting-down	t2.micro	–	0 in alarm	us-east-1a	–

Select an instance

With AWS, we receive a virtual platform or an environment where we can load our software applications and service our application as per requirements. It enable us to select the operating system, web application platform, database and other services like Route 53, Load-Balancer, Cloud-watch, Autoscaling that helps us build a globally secured infrastructure.