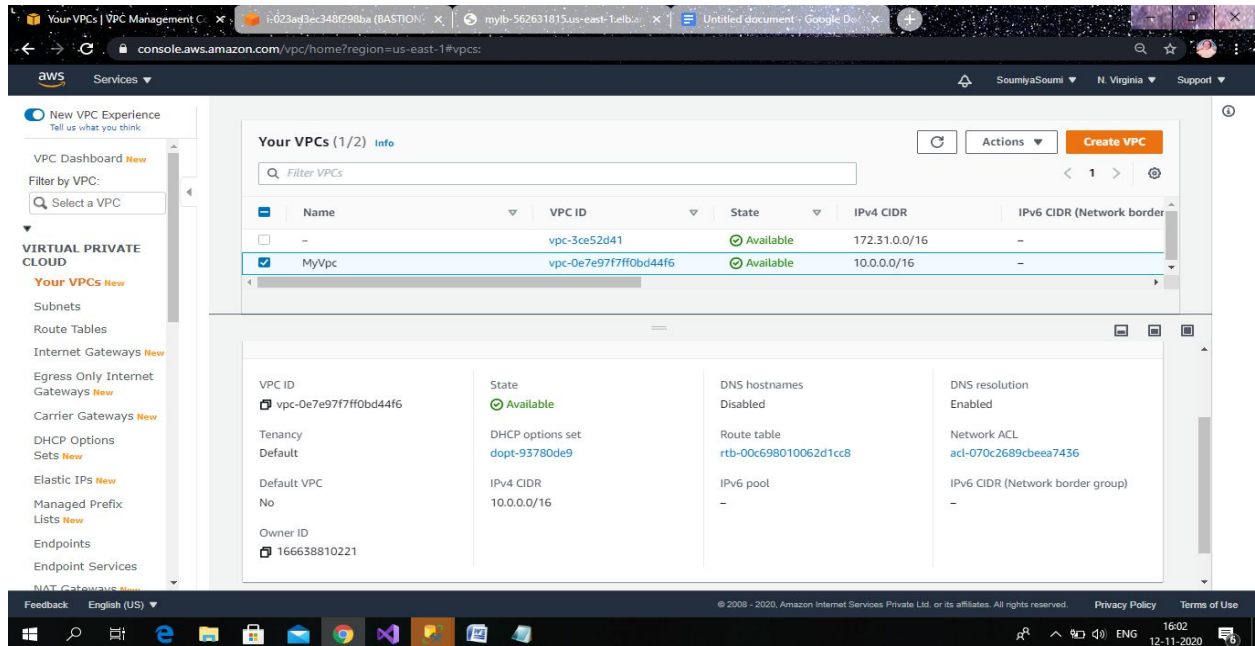


# DEPLOYING A HIGHLY AVAILABLE WEB APPLICATION AND BASTION HOST IN AWS

## CREATING A VPC

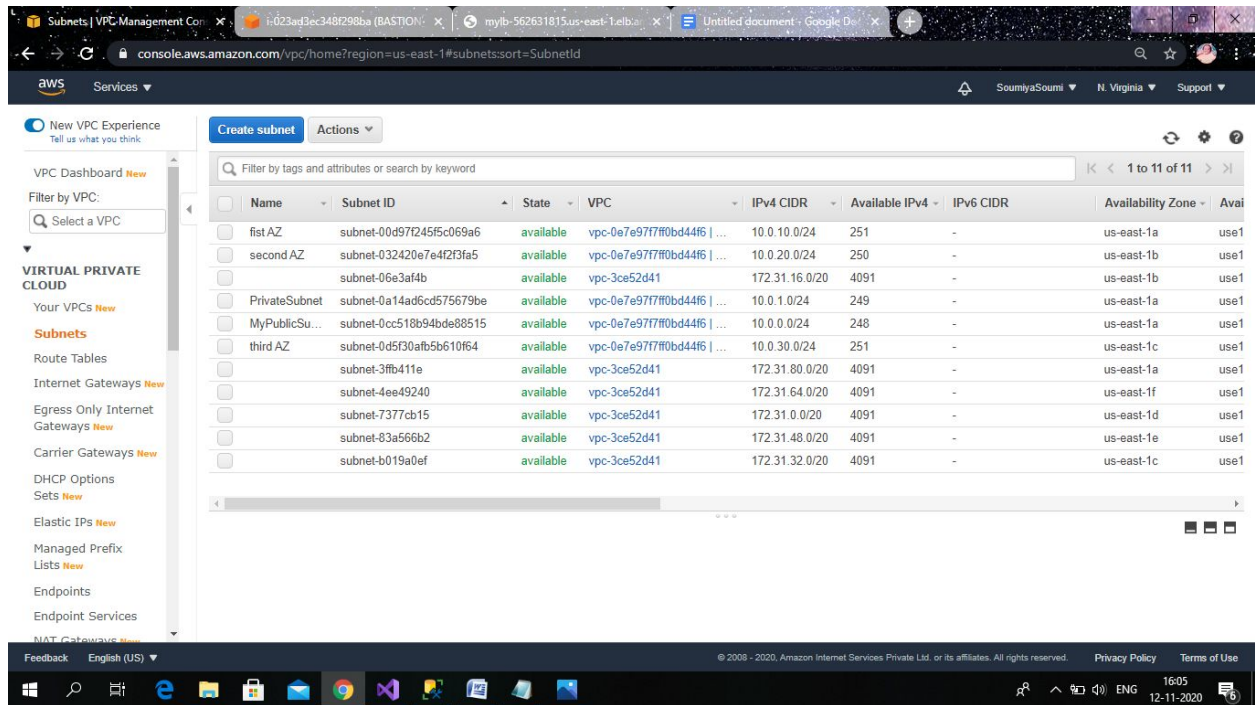
- CREATING THE VPC WITH THE IP 10.0.0.0/16



## CREATING A SUBNET

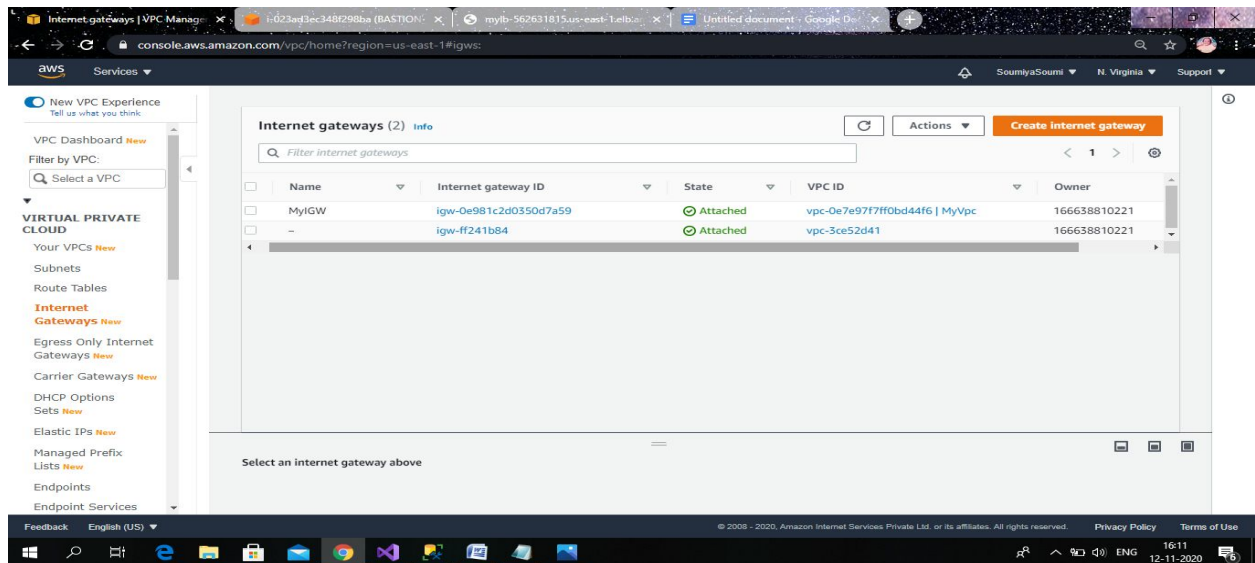
- CREATING FIVE SUBNETS
- WITH THEM 4 IN PUBLIC SUBNET WITH DIFFERENT AVAILABILITY ZONE AND ONE IN PRIVATE SUBNET FOR HIGHLY AVAILABLE APPLICATION
- THE PRIVATE IP DOESN'T CONTAIN IPV4 BECAUSE OF SECURITY
- WE HAVE TO ACCESS THE PRIVATE SUBNET WE NEED NAT GATEWAY IN PUBLIC SUBNET

- REMAINING FOUR SUBNETS ,ENABLING THE AUTO ASSIGN PUBLIC IP



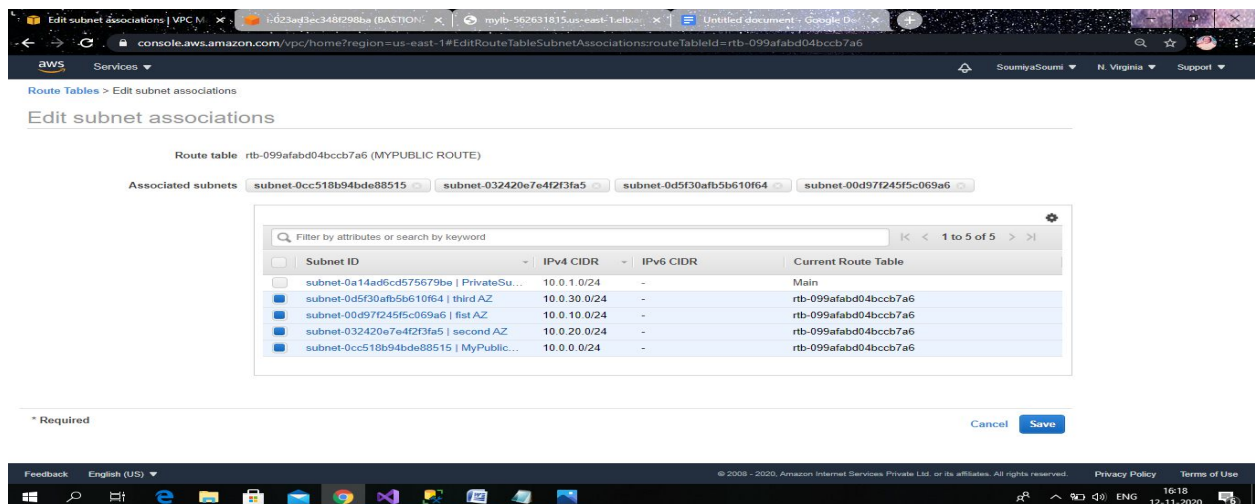
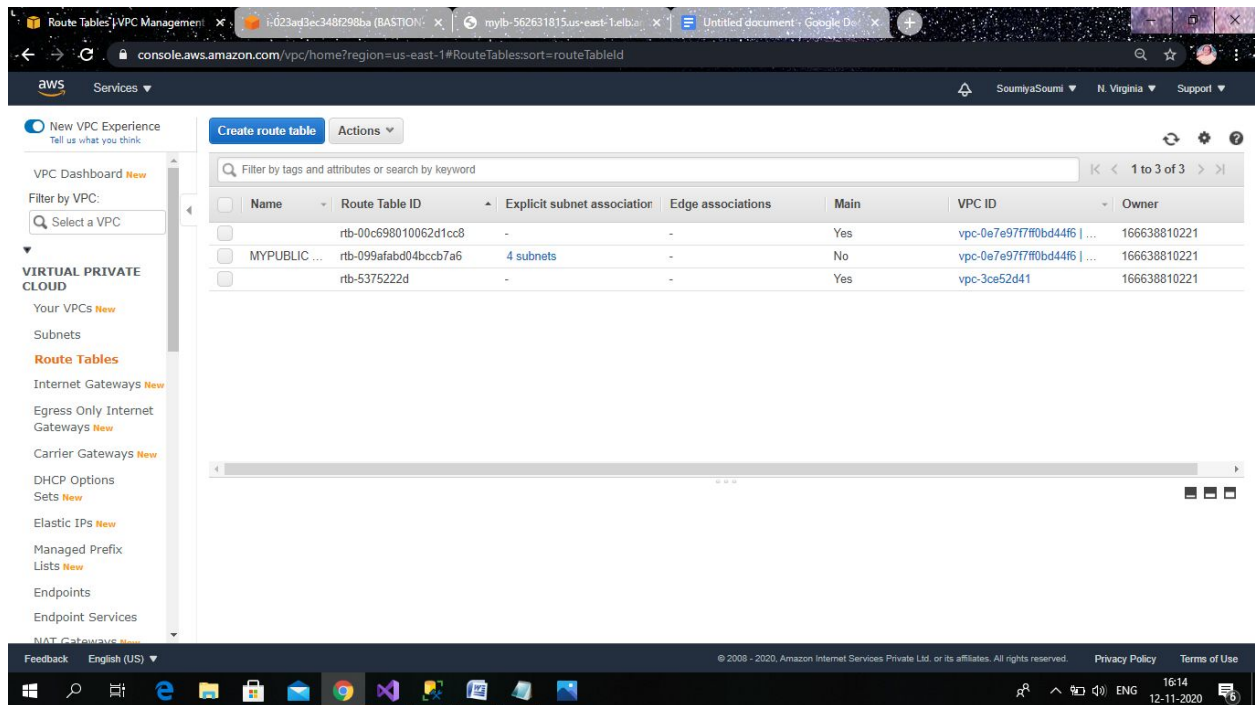
## CREATING A INTERNET GATEWAY

- CREATE AN INTERNET GATEWAY FOR ACCESS THE APPLICATIONS ON PUBLIC IP
- AND ATTACH THE VPC THAT ONE WE HAVE CREATED



## CREATING A ROUTE TABLE

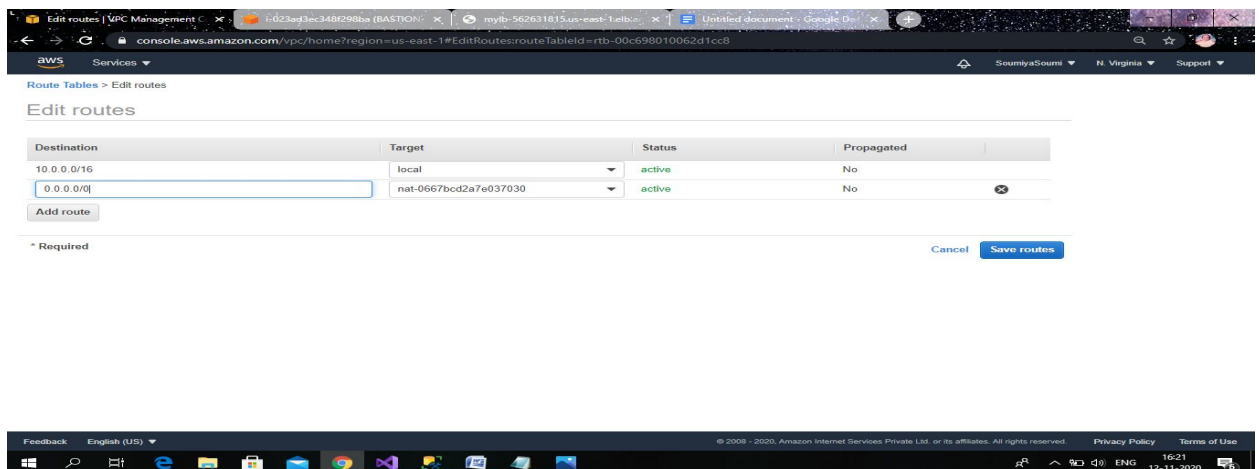
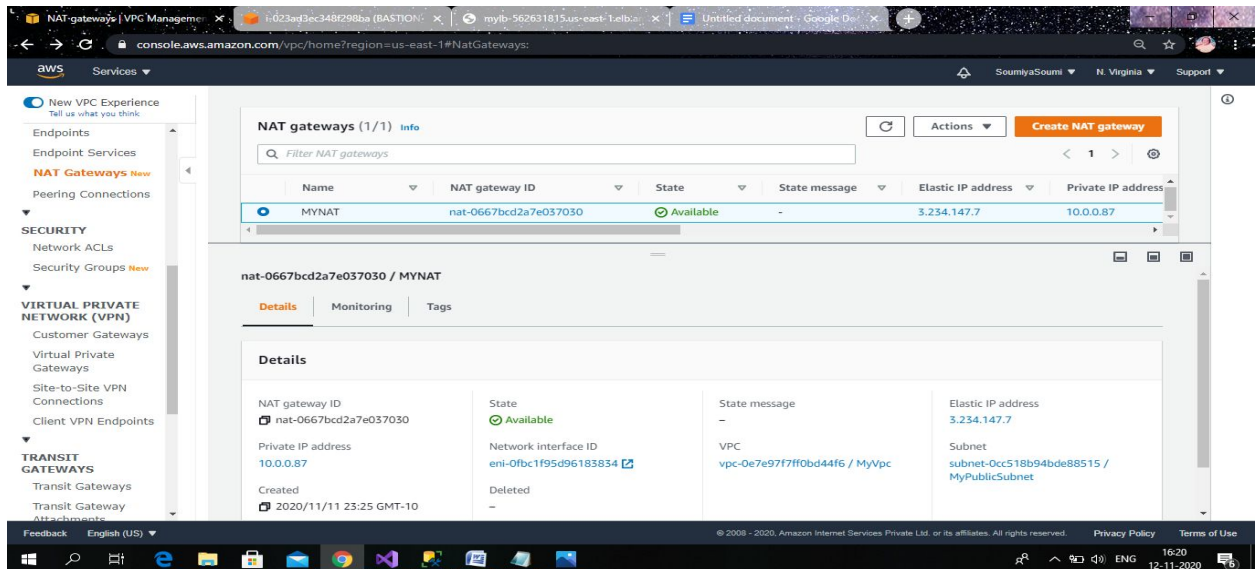
- CREATE ROUTE TABLE WITH THE CREATED VPC
- AND CLICK ON ADD ROUTES ADD 0.0.0.0/0 AS ROUTE AND ADD INTERNET GATEWAY THAT PREVIOUSLY CREATED ONE
- WE CAN SEE THE TWO ROUTE TABLE WITH SAME ID ONE IS MAIN AND ANOTHER ONE IS NO MAIN
- CLICK ON THE NO MAIN TABLE GOTO EDIT SUBNET ASSOCIATION AND ADD 4 PUBLIC SUBNETS TO IT



## CREATING A NAT GATEWAY

- IN PRIVATE SUBNET DOESN'T HAVE THE ACCESS TO THE PUBLIC SO WE HAVE TO CREATE A GATEWAY CALLED AS NAT GATEWAY
- CREATE A NAT GATEWAY WITH PUBLIC SUBNET
- AFTER THAT GO TO ROUTE TABLE GO TO THE ROUTE TABLE WITH SAME ID MAIN ROUTE
- CLICK ON EDIT ROUTE

- ADD 0.0.0.0/0 AS IP AND ADD NAT GATEWAY TO IT



## CREATING SECURITY GROUPS

- CREATING SECURITY GROUP FOR BASTION SERVER ,LOAD BALANCER AND WEB SERVER
- IN THE BASTION SERVER SG WITH ,INBOUND RULES AS SSH TYPE AND CUSTOM 0.0.0.0/0
- LOAD BALANCER SG WITH ,INBOUND RULES HTTP TYPE AND 0.0.0.0/0 CUSTOM
- THE WEB SERVER SG WITHE ,INBOUND RULES HTTP AND SSH TYPES ,BY USING LOAD BALANCER SG AND BASTION SG



EC2 Management Console

console.aws.amazon.com/ec2/v2/home?region=us-east-1#SecurityGroups:

Services

AMIs

▼ Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

▼ Network & Security

Security Groups **New**

Elastic IPs **New**

Placement Groups **New**

Key Pairs **New**

Network Interfaces **New**

▼ Load Balancing

Load Balancers

Target Groups **New**

▼ Auto Scaling

Launch Configurations

Auto Scaling Groups

Security Groups (1/6) **Info**

Filter security groups

< 1 >

<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description	0
<input checked="" type="checkbox"/>	BASTION SG	sg-03c75f76357d095eb	BASTION SG	vpc-0e7e97f7ff0bd44f6	SECURITY GRP FOR BA...	16
<input type="checkbox"/>	LOAD SG	sg-082704a802e89457b	LOAD BALANSE	vpc-0e7e97f7ff0bd44f6	SG	16
<input type="checkbox"/>	WEB WG	sg-093f327ca0234bb10	WEBSERVER SG	vpc-0e7e97f7ff0bd44f6	WEB SG	16

sg-03c75f76357d095eb - BASTION SG

Details **Inbound rules** Outbound rules Tags

**Inbound rules** [Edit inbound rules](#)

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	0.0.0.0/0	-

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

16:33 12-11-2020

EC2 Management Console

console.aws.amazon.com/ec2/v2/home?region=us-east-1#SecurityGroups:

Services

AMIs

▼ Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

▼ Network & Security

Security Groups **New**

Elastic IPs **New**

Placement Groups **New**

Key Pairs **New**

Network Interfaces **New**

▼ Load Balancing

Load Balancers

Target Groups **New**

▼ Auto Scaling

Launch Configurations

Auto Scaling Groups

Security Groups (1/6) **Info**

Filter security groups

< 1 >

<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description	0
<input type="checkbox"/>	BASTION SG	sg-03c75f76357d095eb	BASTION SG	vpc-0e7e97f7ff0bd44f6	SECURITY GRP FOR BA...	16
<input checked="" type="checkbox"/>	LOAD SG	sg-082704a802e89457b	LOAD BALANSE	vpc-0e7e97f7ff0bd44f6	SG	16
<input type="checkbox"/>	WEB WG	sg-093f327ca0234bb10	WEBSERVER SG	vpc-0e7e97f7ff0bd44f6	WEB SG	16

sg-082704a802e89457b - LOAD BALANSE SG

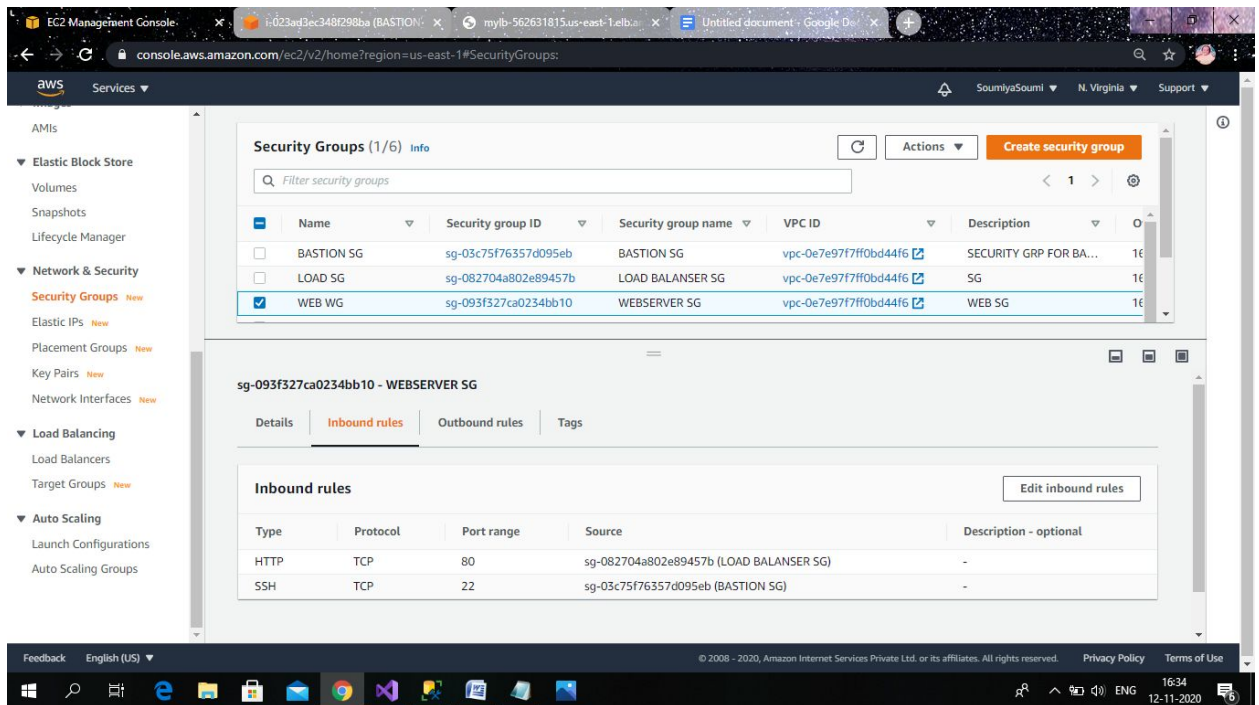
Details **Inbound rules** Outbound rules Tags

**Inbound rules** [Edit inbound rules](#)

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	0.0.0.0/0	-

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

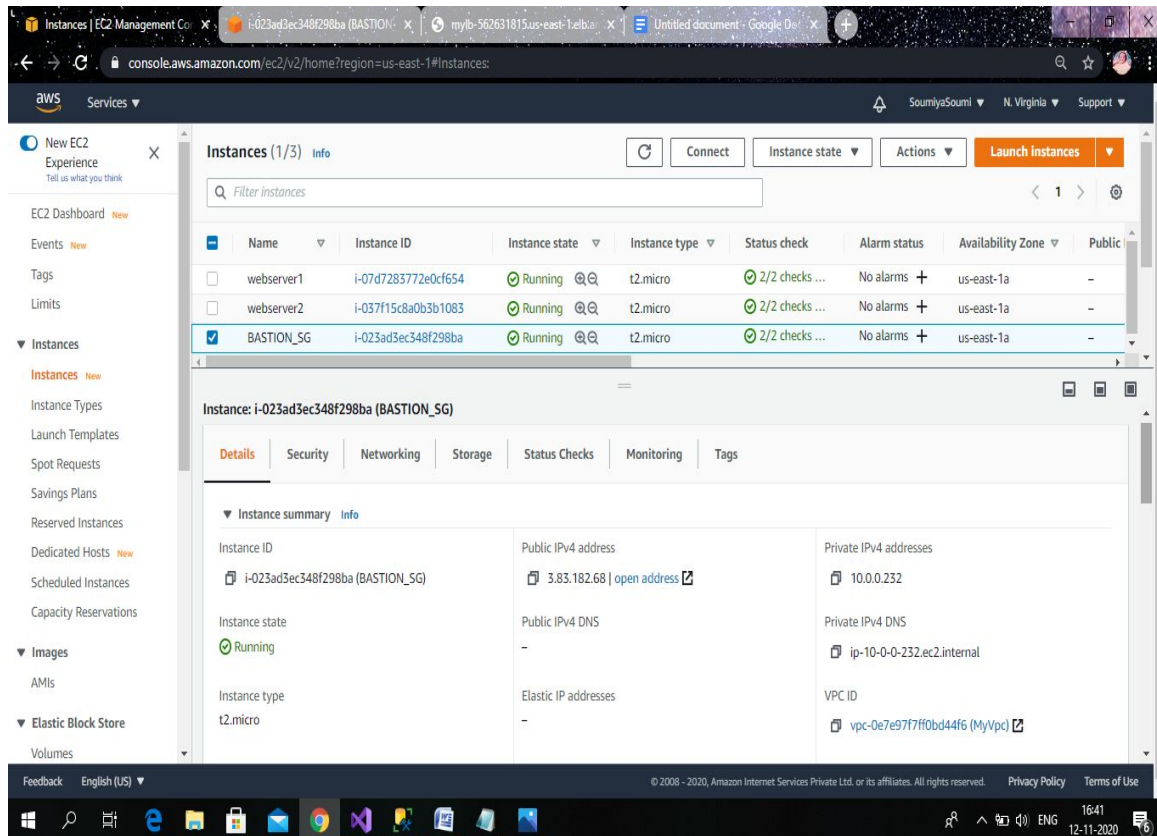
16:34 12-11-2020



## CREATING EC2 INSTANCES

### CREATING A BASTION SERVER

- CREATING A BASTION WEB SERVER WITH PUBLIC SUBNET THAT ONE WE HAVE CREATED
- CHOOSE THE BASTION SECURITY GROUP THAT WE HAVE CREATED
- VIEW AND LAUNCH



## CREATING WEB SERVERS

- Creating 2 web servers with a private subnet and web server security group.
- Waiting for 2/2 check of all the instances



Instances | EC2 Management Console

console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:

Services

New EC2 Experience

EC2 Dashboard

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

Elastic Block Store

Volumes

Instances (1/3) Info

Filter instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
webserver1	i-07d7283772e0cf654	Running	t2.micro	2/2 checks ...	No alarms	us-east-1a	-
webserver2	i-037f15c8a0b3b1083	Running	t2.micro	2/2 checks ...	No alarms	us-east-1a	-
BASTION_SG	i-023ad3ec348f298ba	Running	t2.micro	2/2 checks ...	No alarms	us-east-1a	-

Instance: i-07d7283772e0cf654 (webserver1)

Details Security Networking Storage Status Checks Monitoring Tags

Instance summary Info

Instance ID: i-07d7283772e0cf654 (webserver1)

Instance state: Running

Instance type: t2.micro

Public IPv4 address: -

Public IPv4 DNS: -

Elastic IP addresses: -

Private IPv4 addresses: 10.0.1.205

Private IPv4 DNS: ip-10-0-1-205.ec2.internal

VPC ID: vpc-0e7e97f7f0bd44f6 (MyVpc)

Instances | EC2 Management Console

console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:

Services

New EC2 Experience

EC2 Dashboard

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

Elastic Block Store

Volumes

Instances (1/3) Info

Filter instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
webserver1	i-07d7283772e0cf654	Running	t2.micro	2/2 checks ...	No alarms	us-east-1a	-
webserver2	i-037f15c8a0b3b1083	Running	t2.micro	2/2 checks ...	No alarms	us-east-1a	-
BASTION_SG	i-023ad3ec348f298ba	Running	t2.micro	2/2 checks ...	No alarms	us-east-1a	-

Instance: i-037f15c8a0b3b1083 (webserver2)

Details Security Networking Storage Status Checks Monitoring Tags

Instance summary Info

Instance ID: i-037f15c8a0b3b1083 (webserver2)

Instance state: Running

Instance type: t2.micro

Public IPv4 address: -

Public IPv4 DNS: -

Elastic IP addresses: -

Private IPv4 addresses: 10.0.1.162

Private IPv4 DNS: ip-10-0-1-162.ec2.internal

VPC ID: vpc-0e7e97f7f0bd44f6 (MyVpc)

Instances | EC2 Management Console | console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:

Instances (1/3) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
webserver1	i-07d7283772e0cf654	Running	t2.micro	2/2 checks ...	No alarms	us-east-1a	-
webserver2	i-037f15c8a0b3b1083	Running	t2.micro	2/2 checks ...	No alarms	us-east-1a	-
BASTION_SG	i-023ad3ec348f298ba	Running	t2.micro	2/2 checks ...	No alarms	us-east-1a	-

Instance: i-07d7283772e0cf654 (webserver1)

Details Security Networking Storage Status Checks Monitoring Tags

Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-07d7283772e0cf654 (webserver1)	-	10.0.1.205

Instance state: Running

Public IPv4 DNS: -

Private IPv4 DNS: ip-10-0-1-205.ec2.internal

Instance type: t2.micro

Elastic IP addresses: -

VPC ID: vpc-0e7e97f7f0bd44f6 (MyVpc)

Instances | EC2 Management Console | console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:

Instances (1/3) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
webserver1	i-07d7283772e0cf654	Running	t2.micro	2/2 checks ...	No alarms	us-east-1a	-
webserver2	i-037f15c8a0b3b1083	Running	t2.micro	2/2 checks ...	No alarms	us-east-1a	-
BASTION_SG	i-023ad3ec348f298ba	Running	t2.micro	2/2 checks ...	No alarms	us-east-1a	-

Instance: i-037f15c8a0b3b1083 (webserver2)

Details Security Networking Storage Status Checks Monitoring Tags

Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-037f15c8a0b3b1083 (webserver2)	-	10.0.1.162

Instance state: Running

Public IPv4 DNS: -

Private IPv4 DNS: ip-10-0-1-162.ec2.internal

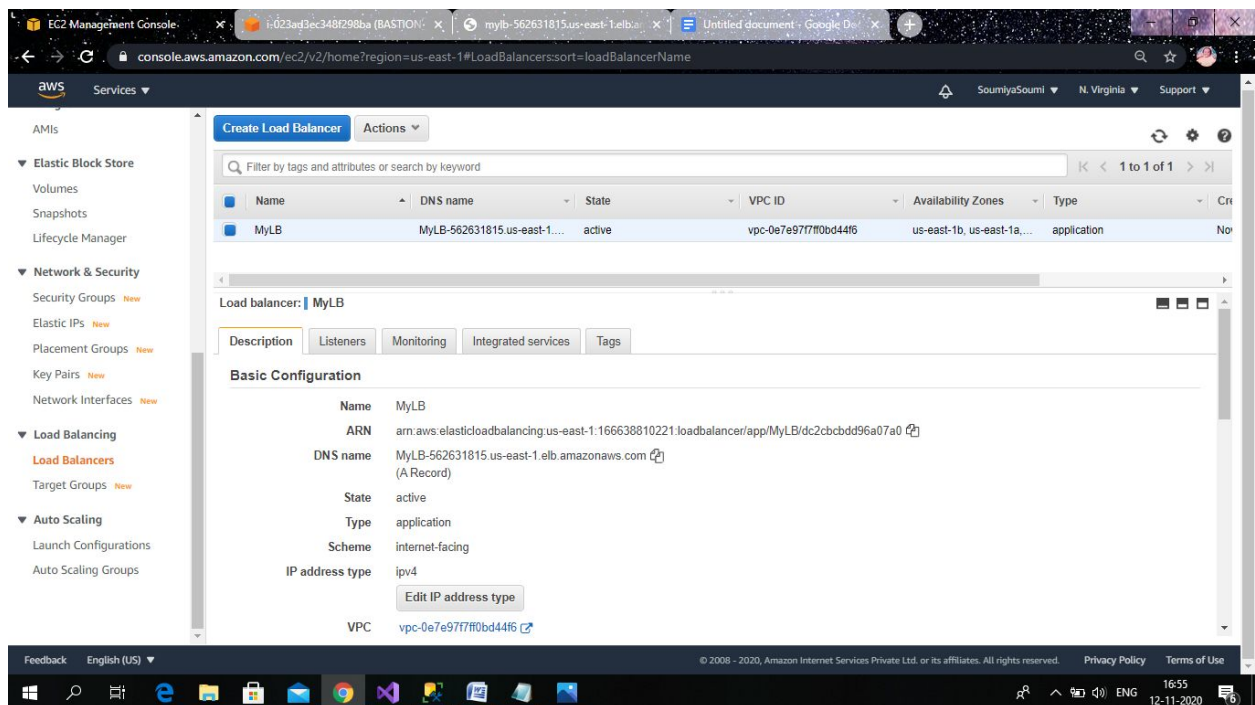
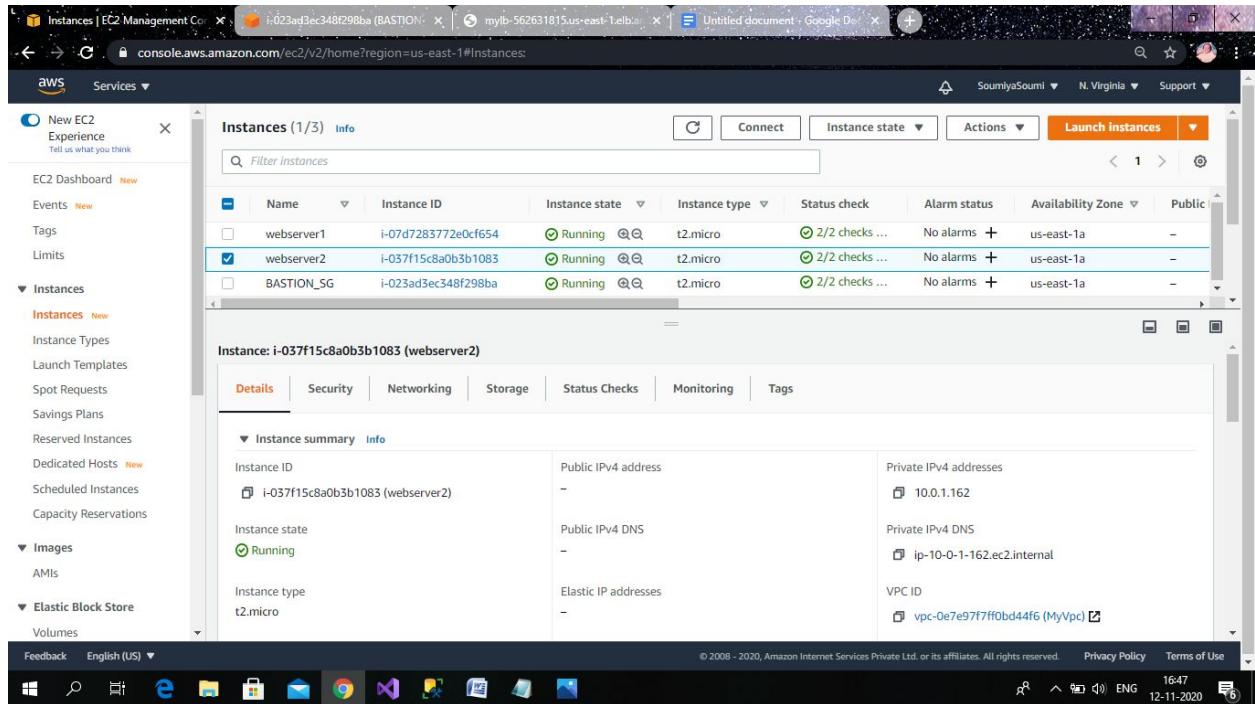
Instance type: t2.micro

Elastic IP addresses: -

VPC ID: vpc-0e7e97f7f0bd44f6 (MyVpc)

# Launching Instances

- Creating the load balancer
- Register the target



- Launch the bastion server

```

PMP Management Console x Q23ad3ec348f298ba (BASTION) x mylb-562631815-us-east-1-elba x Facebook x
< > C console.aws.amazon.com/ec2/v2/connect/ec2-user/i-023ad3ec348f298ba
Installed:
  httpd.x86_64 0:2.4.46-1.amzn2

Dependency Installed:
  apr.x86_64 0:1.6.3-5.amzn2.0.2 apr-util.x86_64 0:1.6.1-5.amzn2.0.2 apr-util-bdb.x86_64 0:1.6.1-5.amzn2.0.2 generic-logos-httpd.noarch 0:18.0.0-4.amzn2
  httpd-filesystem.noarch 0:2.4.46-1.amzn2 httpd-tools.x86_64 0:2.4.46-1.amzn2 mailcap.noarch 0:2.1.41-2.amzn2 mod_http2.x86_64 0:1.15.14-2.amzn2

Complete!
[root@ip-10-0-1-162 ec2-user]# systemctl start httpd
[root@ip-10-0-1-162 ec2-user]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@ip-10-0-1-162 ec2-user]# cd /var/www/html
[root@ip-10-0-1-162 html]# echo "REQUEST HANDLED BY WEBSERVER 2" > index.html
[root@ip-10-0-1-162 html]# exit
exit
[ec2-user@ip-10-0-1-162 ~]$ exit
logout
Connection to 10.0.1.162 closed.
[root@ip-10-0-0-232 ec2-user]# ssh -i web-serverkey.pem ec2-user@10.0.1.162
Last login: Thu Nov 12 10:18:24 2020 from 10.0.0.232

 _ _ _ _ _
| | | | |
|_|_|_|_|_  Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-1-162 ~]$ sudo su
[root@ip-10-0-1-162 ec2-user]# cd /var/www/html
[root@ip-10-0-1-162 html]# echo "Request handled by webserver 2">index.html
[root@ip-10-0-1-162 html]# exit
exit
[ec2-user@ip-10-0-1-162 ~]$ exit
logout
Connection to 10.0.1.162 closed.
[root@ip-10-0-0-232 ec2-user]#

```

i-023ad3ec348f298ba (BASTION\_SG)

Public IPs: 3.83.182.68 Private IPs: 10.0.0.232



```

openldap                                x86_64                                2.4.44-22.amzn2                                amzn2-core                                350 k
p11-kit                                x86_64                                0.23.21-2.amzn2.0.1                          amzn2-core                                316 k
p11-kit-trust                          x86_64                                0.23.21-2.amzn2.0.1                          amzn2-core                                128 k
pam                                    x86_64                                1.1.8-23.amzn2.0.1                          amzn2-core                                715 k
python-pillow                          x86_64                                2.0.0-2.1.gitd1c6db8.amzn2.0.1             amzn2-core                                440 k
python2-botoecore                     noarch                                1.18.6-1.amzn2.0.1                          amzn2-core                                4.4 M
python2-rpm                            x86_64                                4.11.3-40.amzn2.0.5                          amzn2-core                                84 k
python2-s3transfer                    noarch                                0.3.9-1.amzn2.0.1                          amzn2-core                                104 k
rng-tools                             x86_64                                6.8-3.amzn2.0.1                             amzn2-core                                53 k
rpm                                     x86_64                                4.11.3-40.amzn2.0.5                          amzn2-core                                1.2 M
rpm-build-libs                         x86_64                                4.11.3-40.amzn2.0.5                          amzn2-core                                106 k
rpm-libs                              x86_64                                4.11.3-40.amzn2.0.5                          amzn2-core                                275 k
rpm-plugin-systemd-inhibit            x86_64                                4.11.3-40.amzn2.0.5                          amzn2-core                                47 k
unzip                                  x86_64                                6.0-21.amzn2                                amzn2-core                                172 k

```

Transaction Summary

```

=====
Install    1 Package
Upgrade   50 Packages

Total download size: 84 M
Downloading packages:
Delta RPMs disabled because /usr/bin/applydeltarpm not installed.
(1/51): aws-cfn-bootstrap-1.4-34.amzn2.noarch.rpm                                | 652 kB  00:00:00
(2/51): awscli-1.18.147-1.amzn2.0.1.noarch.rpm                                | 2.1 MB  00:00:00
(3/51): bash-4.2.46-34.amzn2.x86_64.rpm                                       | 1.0 MB  00:00:00
(4/51): cpio-2.11-28.amzn2.x86_64.rpm                                           | 211 kB  00:00:00
(5/51): e2fsprogs-1.42.9-19.amzn2.x86_64.rpm                                   | 700 kB  00:00:00
(6/51): e2fsprogs-libs-1.42.9-19.amzn2.x86_64.rpm                             | 166 kB  00:00:00
(7/51): ec2-net-utils-1.4-3.amzn2.noarch.rpm                                    | 17 kB  00:00:00
(8/51): ec2-utils-1.2-3.amzn2.noarch.rpm                                         | 11 kB  00:00:00
(9/51): expat-2.1.0-12.amzn2.x86_64.rpm                                          | 86 kB  00:00:00
(10/51): glib2-2.56.1-7.amzn2.0.1.x86_64.rpm                                  | 2.4 MB  00:00:00
(11/51): amazon-ssm-agent-3.0.161.0-1.amzn2.x86_64.rpm                       | 28 MB  00:00:00
(12/51): glibc-2.26-38.amzn2.x86_64.rpm                                         | 3.3 MB  00:00:00

```

i-023ad3ec348f298ba (BASTION SG)

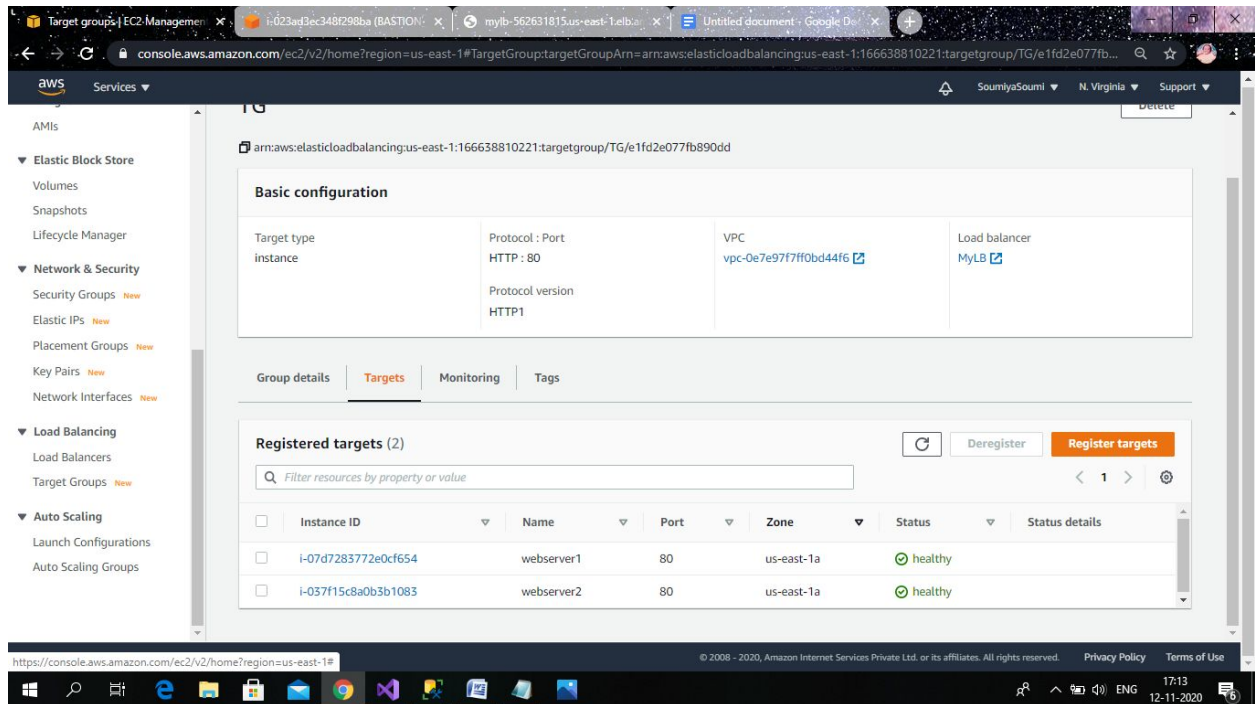
Public IPs: 3.83.182.68 Private IPs: 10.0.0.232



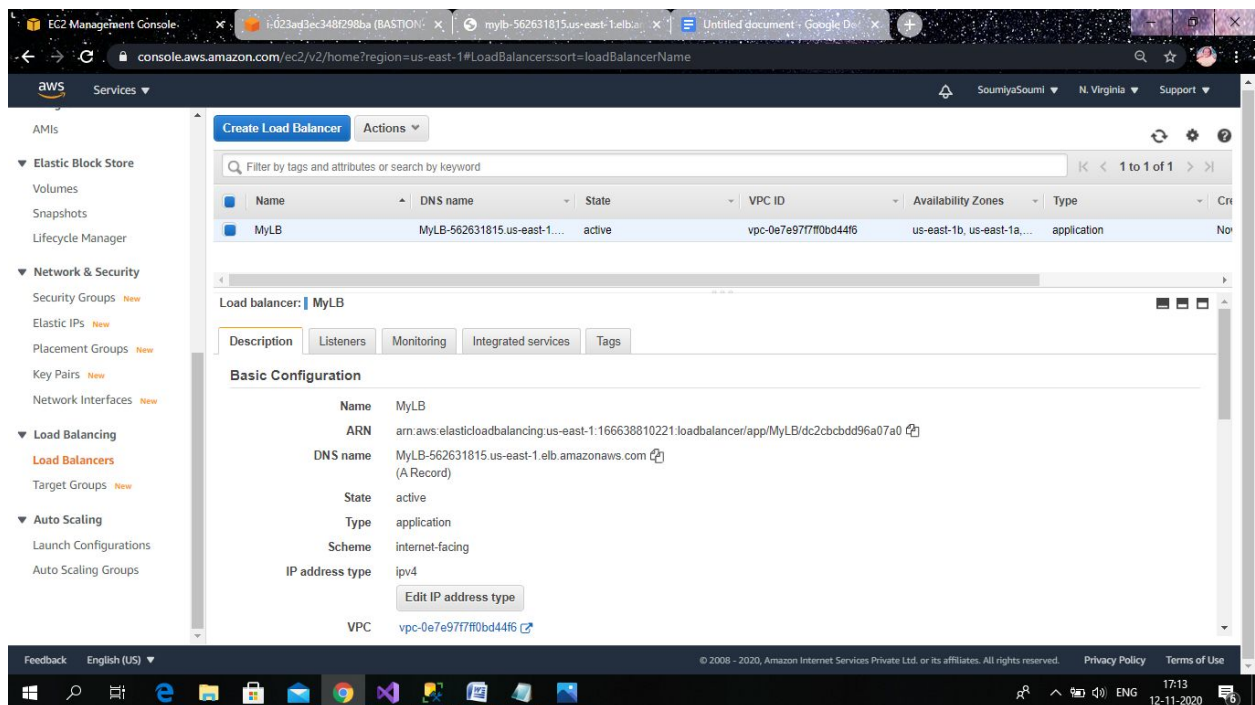
- Become a root user using `sudo su`
- Vi `web-serverkey.pem`
- Copy the pem file into and press escape `:wq` enter



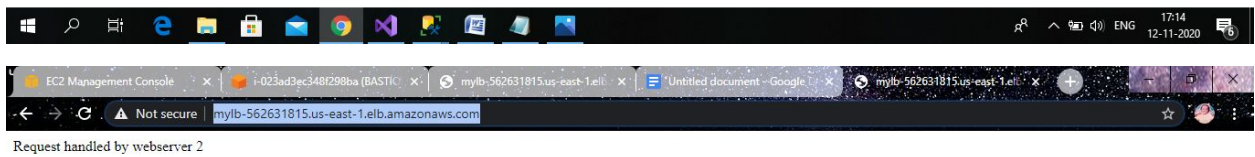
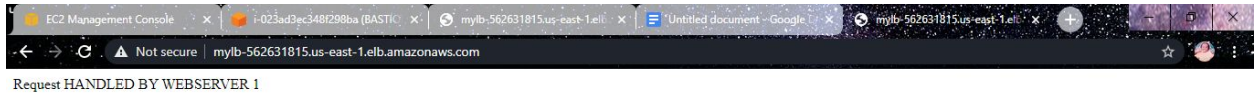
- Using `chmod 400 webserverkey.pem`
- log into the web server using `ssh -i web-serverkey.pem ec2-user@10.0.1.205`
- Installing a apache server
- Sudo su for switch as a root user in web server 1
- `Yum update -y`
- `Yum install httpd -y`
- `Systemctl start httpd`
- `Systemctl enable httpd`
- `Cd /var/www/html`
- Echo “request handled by web server 1” >`index.html`
- Click on exit and exit
- Exit from the web server
- Repeat same process for launching web server 2
- The only change is
- Echo “request handled by web server 2” >`index.html`
- Exit
- Exit
- Now go to the target groups
- See the health of the both of the instance



- If the health of the both instance are healthy
- Then go to the load balancer copy th DNS and paste it check both the web server are running







## After stopping one instance

Successfully stopped i-07d7283772e0cf654

Instances (1/3) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
<input checked="" type="checkbox"/>	webserver1	i-07d7283772e0cf654	Stopping	t2.micro	2/2 checks ...	No alarms +	us-east-1a	-
<input type="checkbox"/>	webserver2	i-037f15c8a0b3b1083	Running	t2.micro	2/2 checks ...	No alarms +	us-east-1a	-
<input type="checkbox"/>	BASTION_SG	i-023ad3ec348f298ba	Running	t2.micro	2/2 checks ...	No alarms +	us-east-1a	-

Instance: i-07d7283772e0cf654 (webserver1)

Details Security Networking Storage Status Checks Monitoring Tags

Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-07d7283772e0cf654 (webserver1)	-	10.0.1.205
Instance state	Public IPv4 DNS	Private IPv4 DNS
Stopping	-	ip-10-0-1-205.ec2.internal
Instance type	Elastic IP addresses	VPC ID
t2.micro	-	-

arn:aws:elasticloadbalancing:us-east-1:166638810221:targetgroup/TG/e1fd2e077fb890dd

Basic configuration

Target type	Protocol : Port	VPC	Load balancer
instance	HTTP : 80	vpc-0e7e97f7f0bd44f6	MyLB
	Protocol version		
	HTTP1		

Group details Targets Monitoring Tags

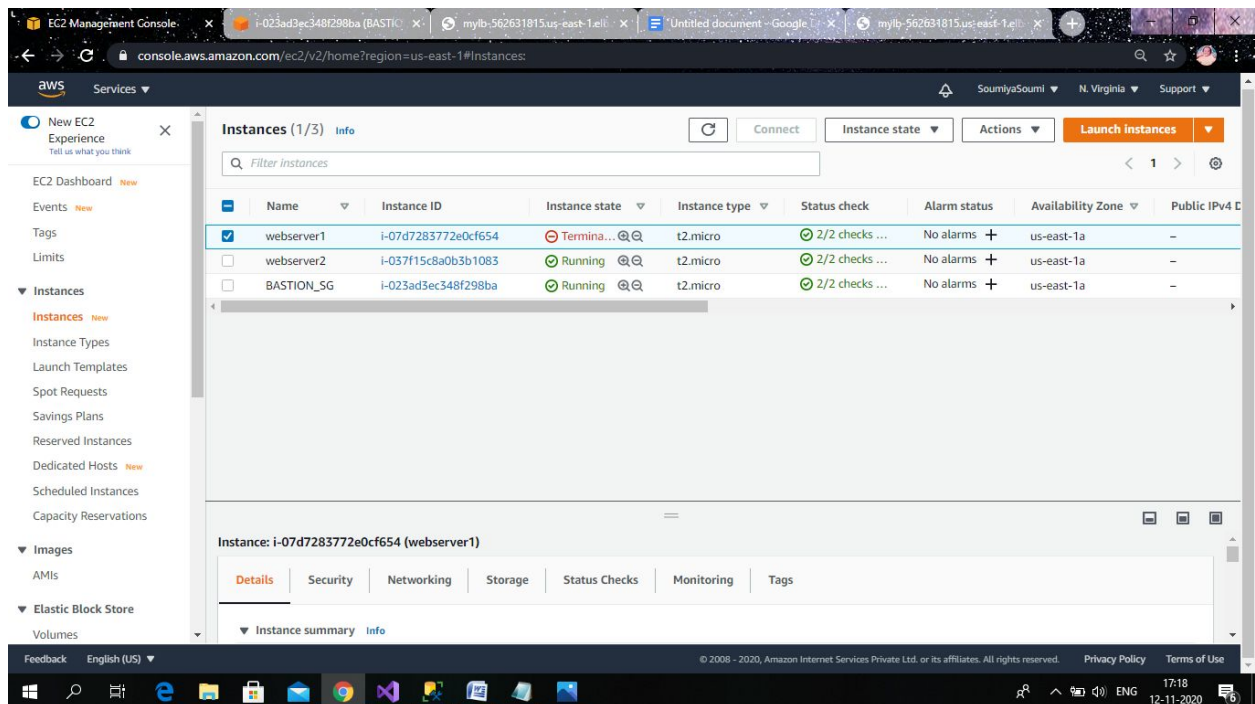
Registered targets (2)

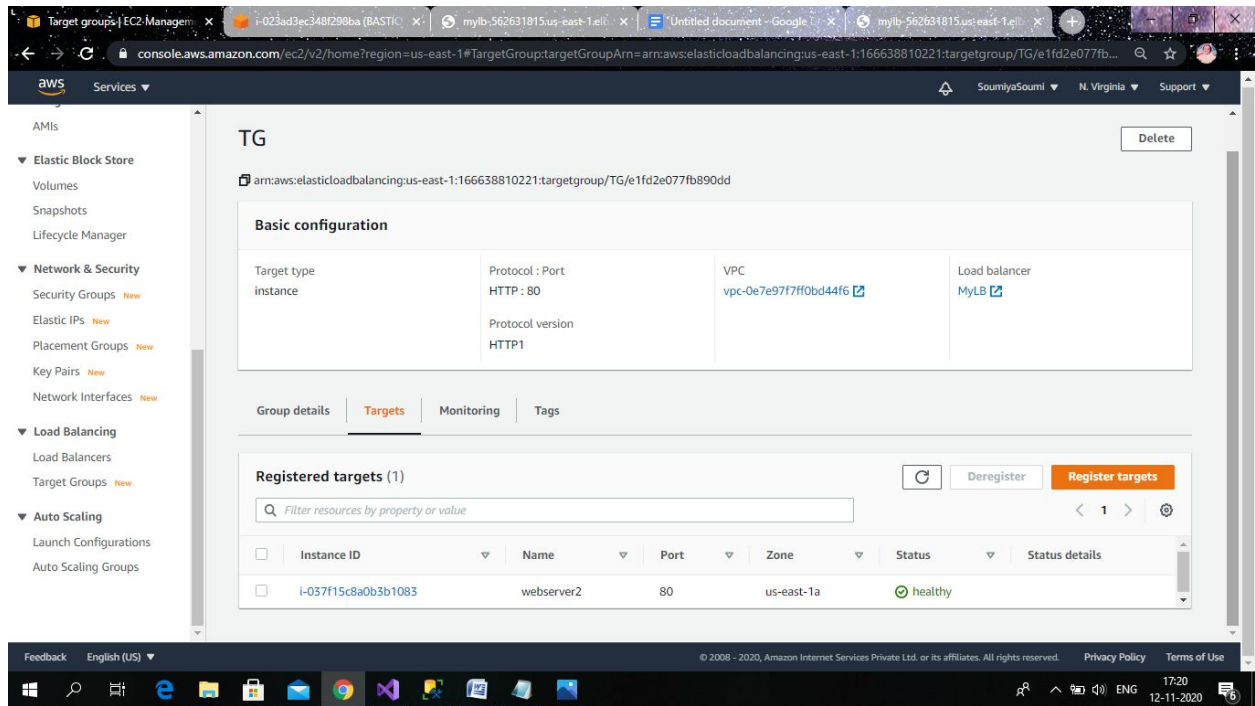
	Instance ID	Name	Port	Zone	Status	Status details
<input type="checkbox"/>	i-07d7283772e0cf654	webserver1	80	us-east-1a	unused	Target is in the stopped state
<input type="checkbox"/>	i-037f15c8a0b3b1083	webserver2	80	us-east-1a	healthy	



The webserver 1 comes under unused and the webserver 2 only handles the request

## After terminating webserver1





**Finally**  
**The we implement a highly available web application and bastion aws**