Q1. When to use Elastic IP over Public IP

Ans-We use elastic IP over public ip when we want ip doesn't change when we start or stop the instance.

For eg: if we are hosting a website on an Ec2 instance we will give that instance a elastic ip so that it doesn't get changed.

We use elastic Ip in the NAT server in a VPC.

Q2. Valid IP Ranges for LAN, Implication of using Public IP ranges for Private Network.

Class A Network - 10.0.0.0 - 10.255.255.255

Class B Network - 172.16.0.0 - 172.31.255.255

Class C Network - 192.168.0.0 - 192.168.255.255

Q3. List down the things to keep in mind while VPC peering.

1. **The owner of the *requester VPC* sends a request to the owner of the *accepter VPC* to create the VPC peering connection. The accepter VPC can be owned by you, or another AWS account, and cannot have a CIDR block that overlaps with the requestor VPC's CIDR block.**
2. **The owner of the accepter VPC accepts the VPC peering connection request to activate the VPC peering connection.**
3. **To enable the flow of traffic between the VPCs using private IP addresses, the owner of each VPC in the VPC peering connection must manually add a route to one or more of their VPC route tables that points to the IP address range of the other VPC (the peer VPC).**
4. **If required, update the security group rules that are associated with your instance to ensure that traffic to and from the peer VPC is not restricted.**
5. **Both the VPC should have different CIDR range otherwise there will be an ambiguity in the route table and Network access control lists.**

Q4. CIDR of a VPC is 10.0.0.0/16, if the subnet mask is /20 calculate the number of subnets that could be created from the VPC. Also find the number of IPs in the subnet.

No. of subnets = 20 -16 =4=2^4 =16subnets.

Ip in each subnet=32-20=12=2^12Ip in a particular subnet.

Q5. Differentiate between NACL and Security Groups.

NACL has Rule number priority whereas Security Group doesn't have.

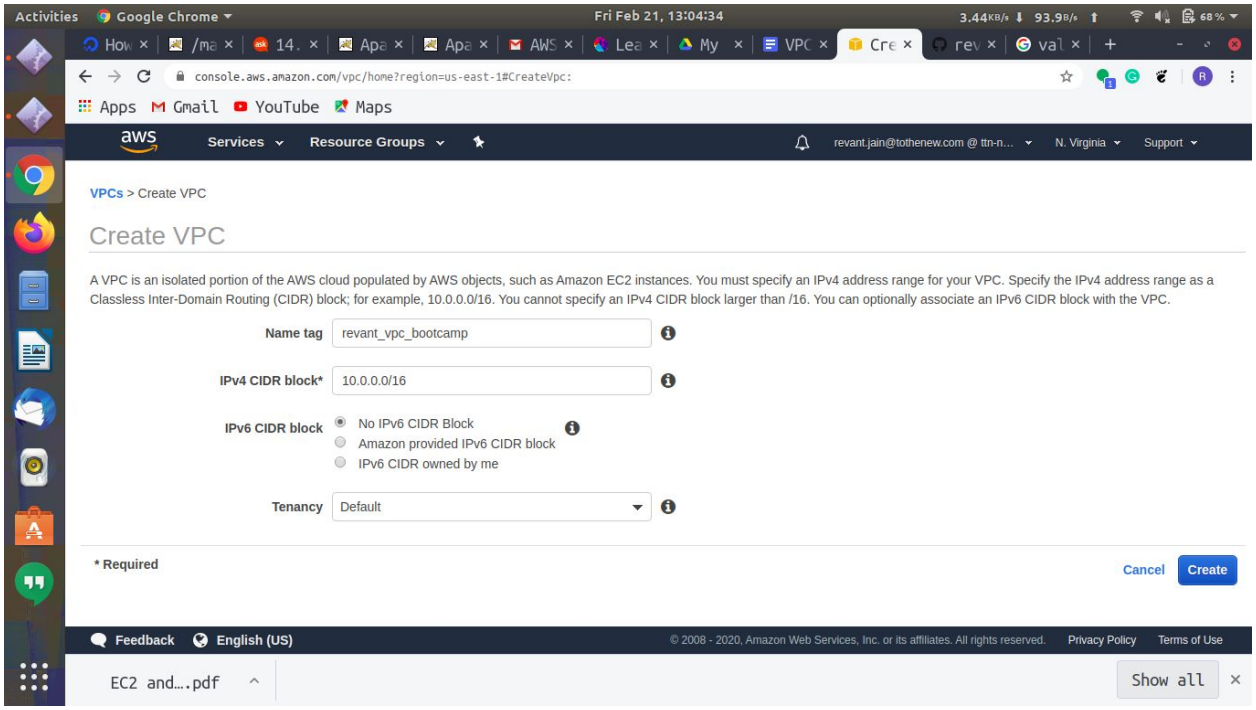
In NACL we can allow and deny both and in Security group we can only allow.

NACL acts as a firewall for a particular subnet whereas Security group acts as a firewall for a particular EC2 instance.

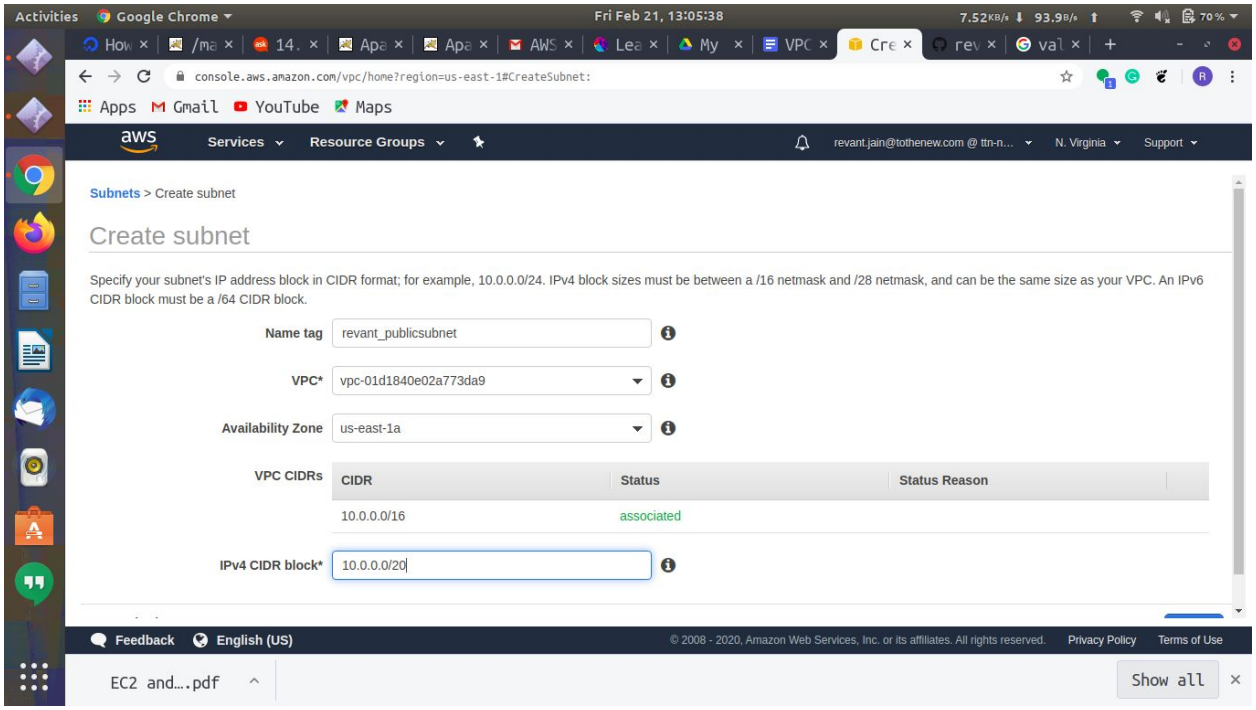
NACL are stateless which means whenever we allow a particular port in inbound it will not be automatically applied in outbound. Whereas Security group is stateful.

Q6. Implement a 2-tier vpc with following requirements:

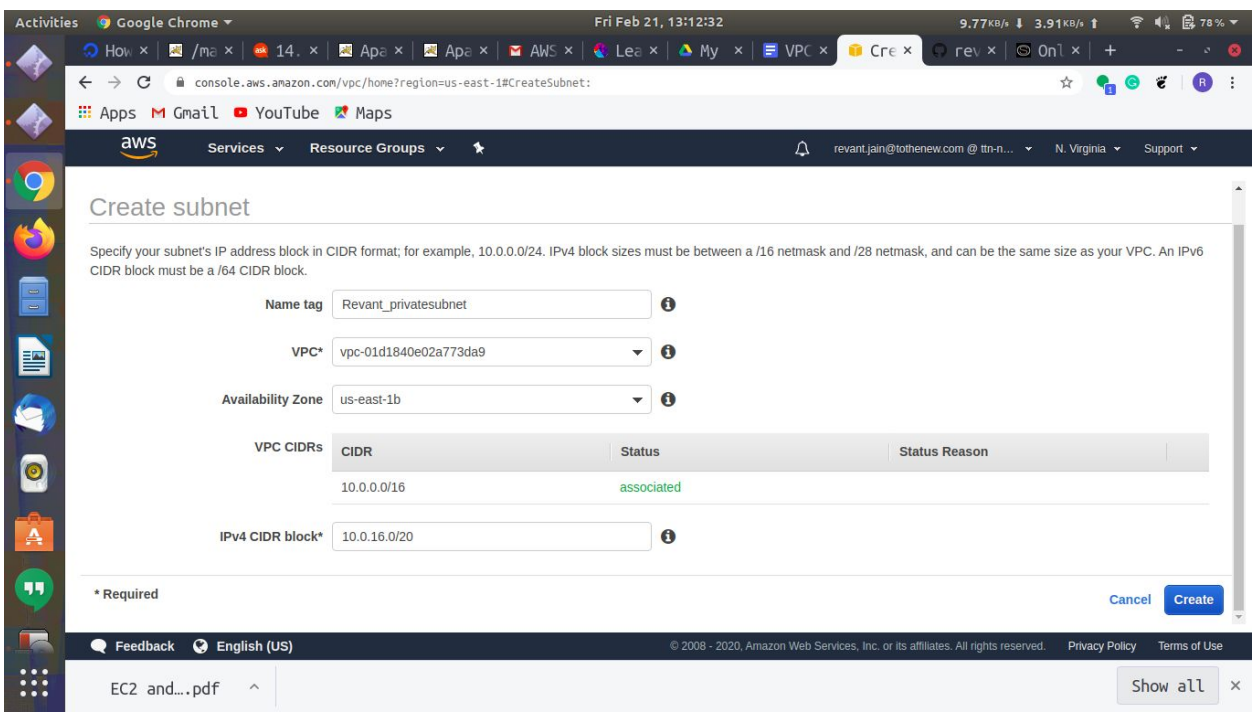
1. Create a private subnet, attach NAT, and host an application server(Tomcat)
2. Create a public subnet, and host a web server(Nginx), also proxy pass to Tomcat from Nginx



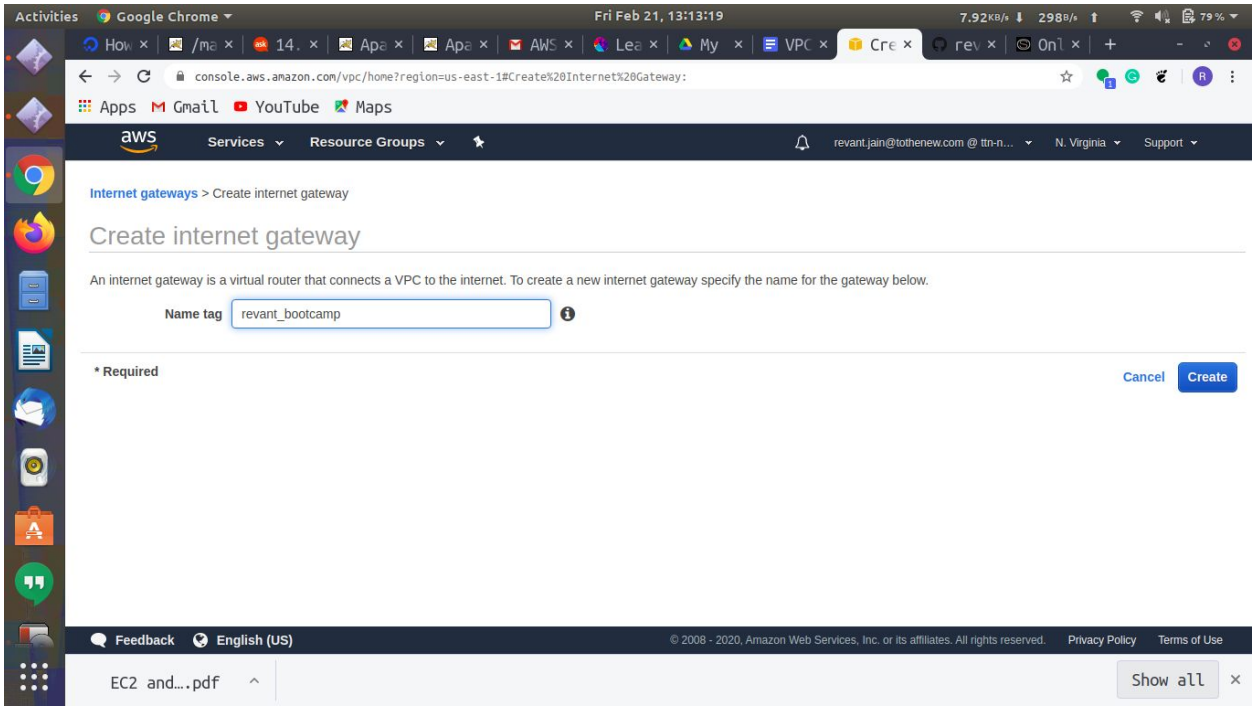
Create a public subnet



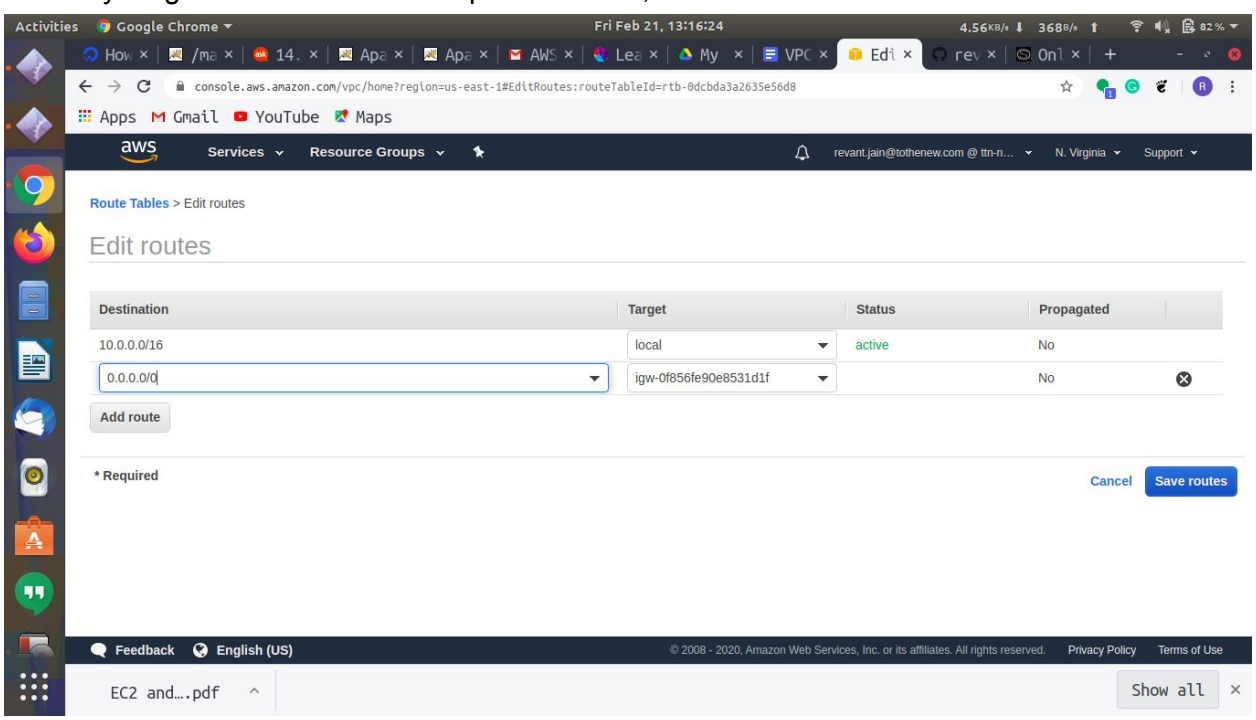
Create a private subnet



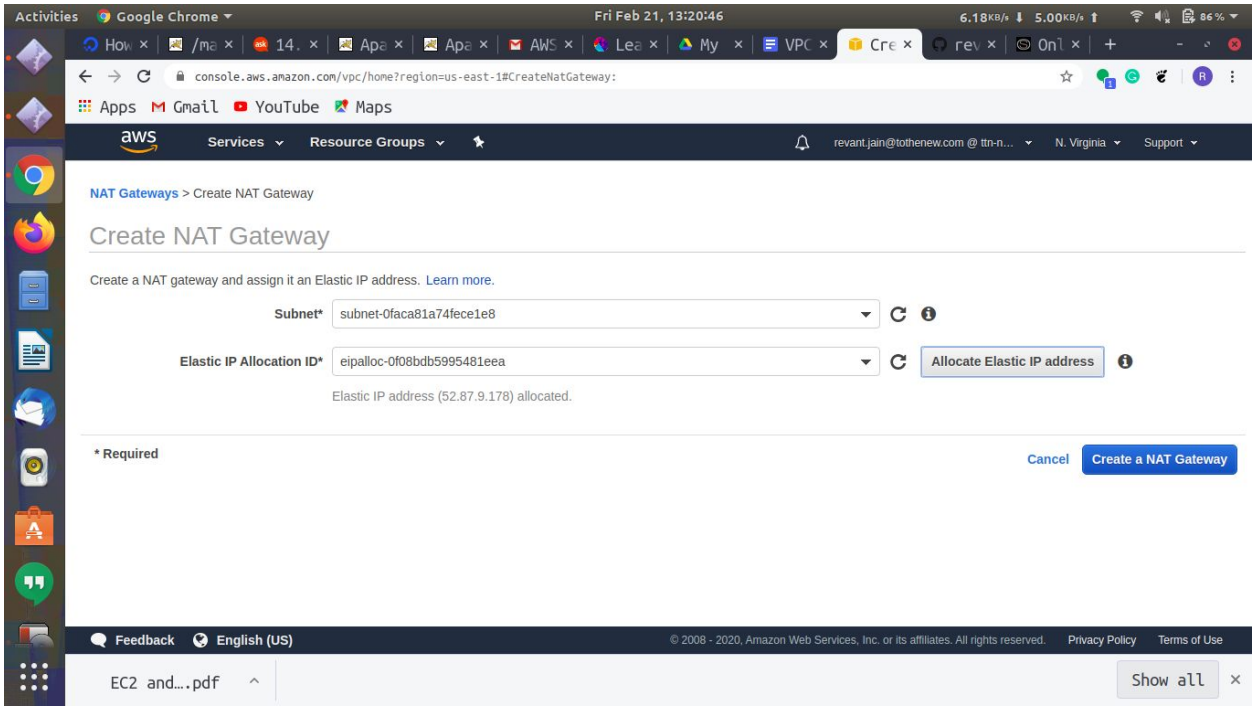
Create an internet gateway and attach it to Vpc.

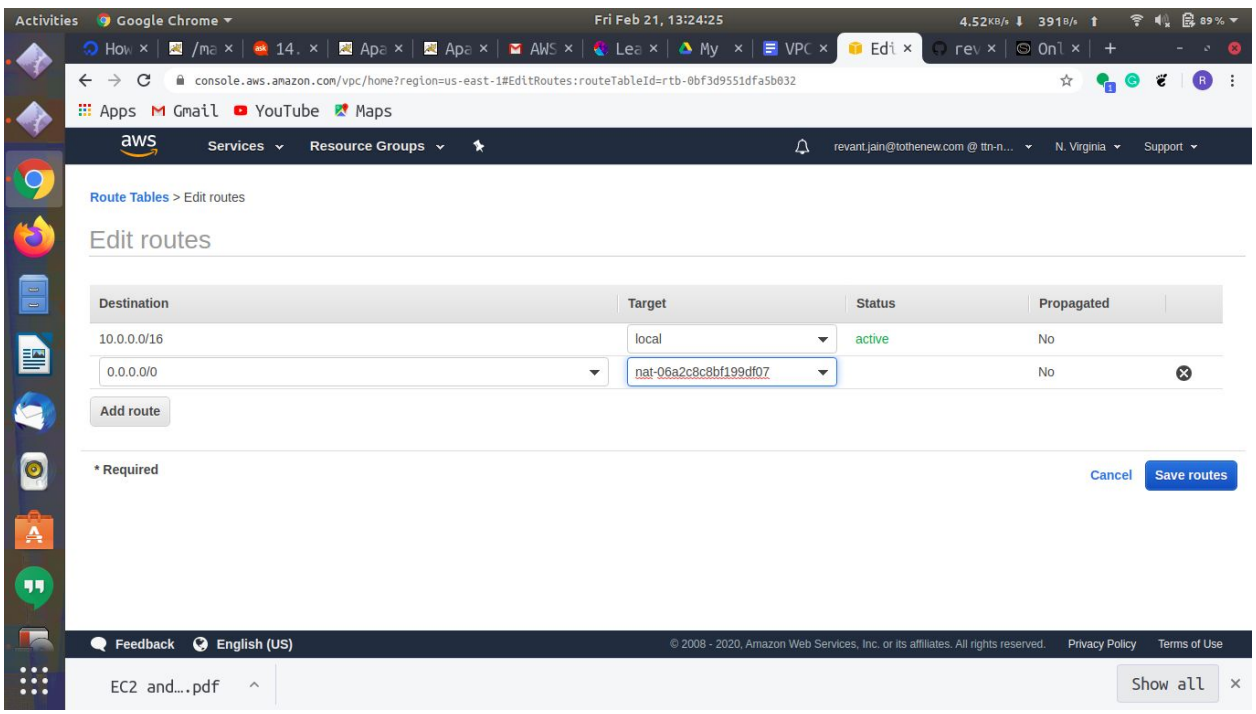


Put entry of igw in the route table of public subnet,

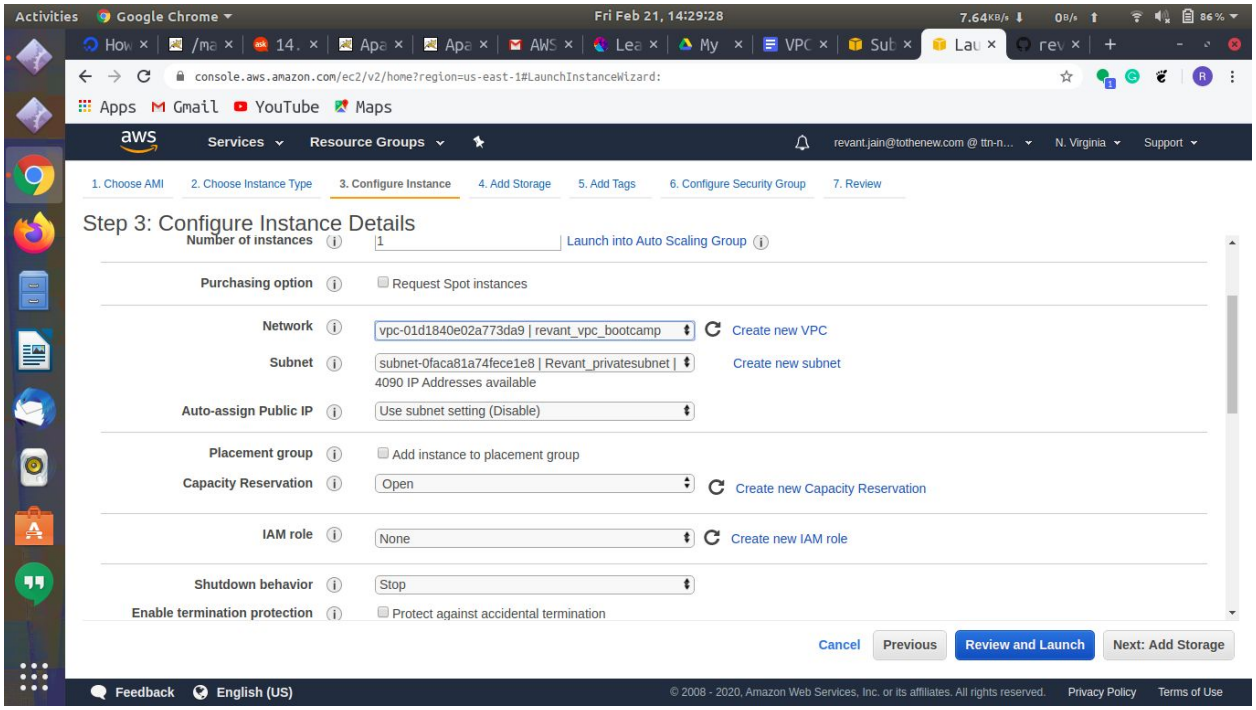


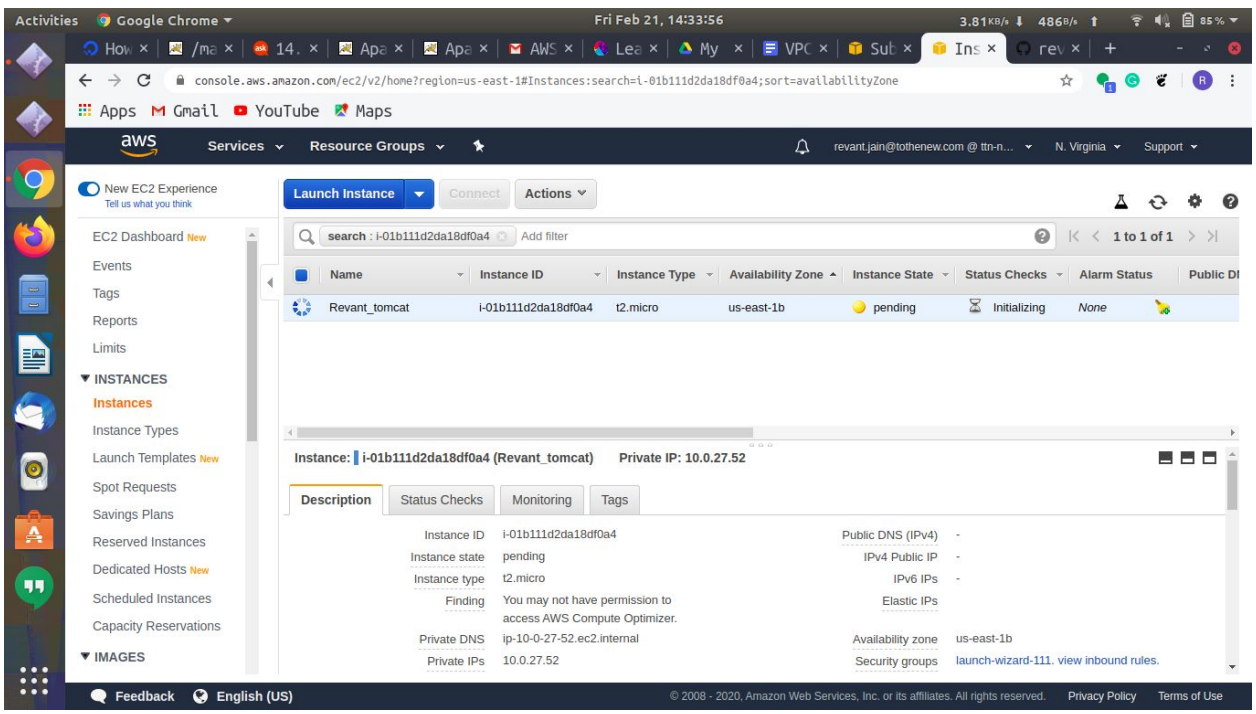
Create a NAT gateway



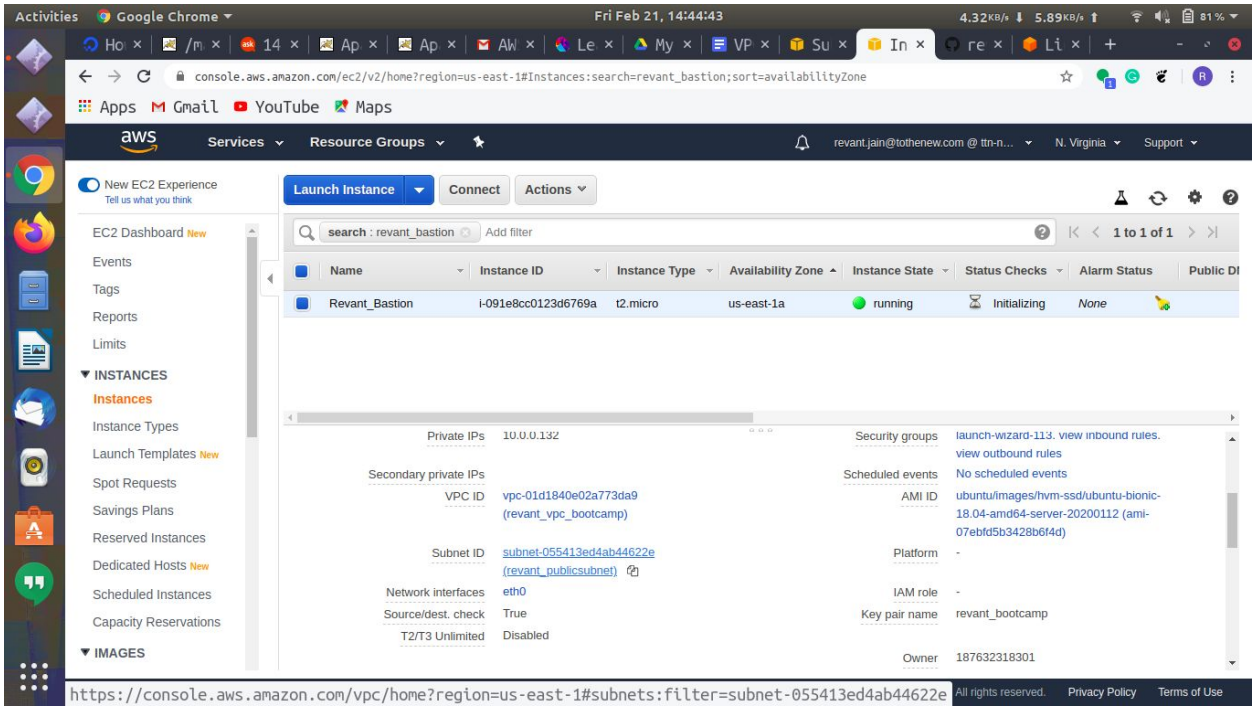


Make an Ec2 instance in private subnet and install tomcat in it.

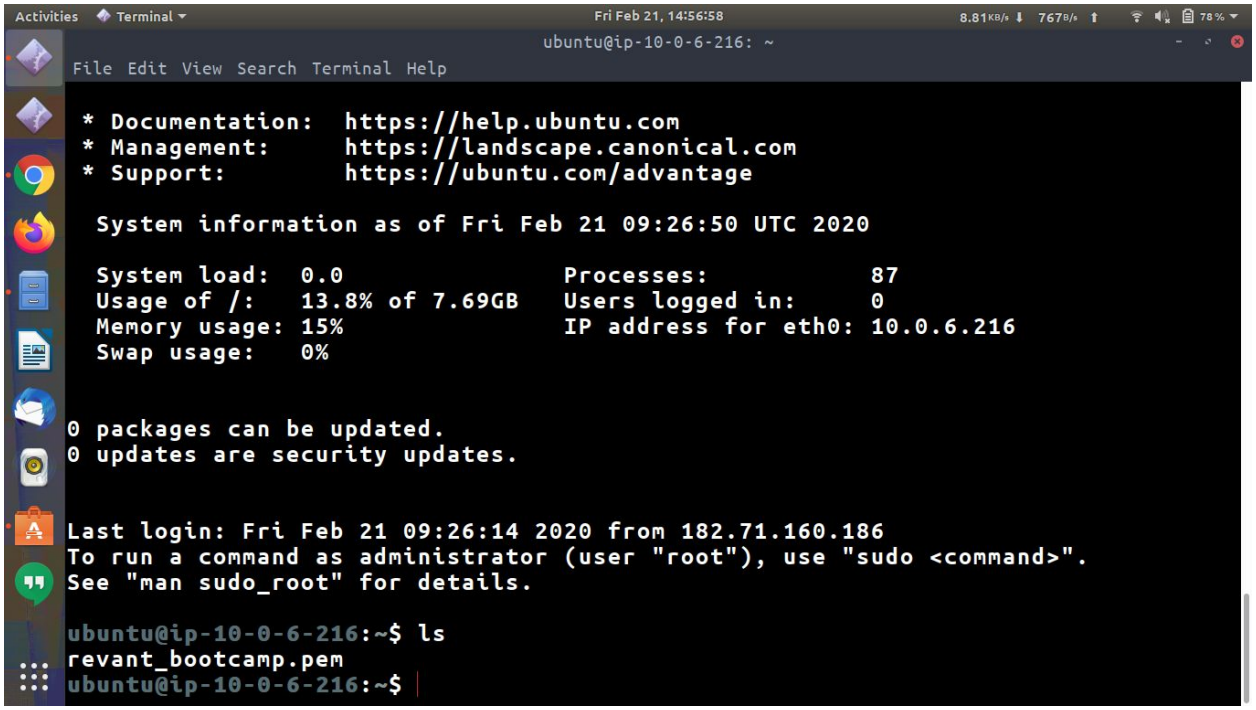




Now we will create a bastion hosts in public subnet



Login into Bastion hosts.

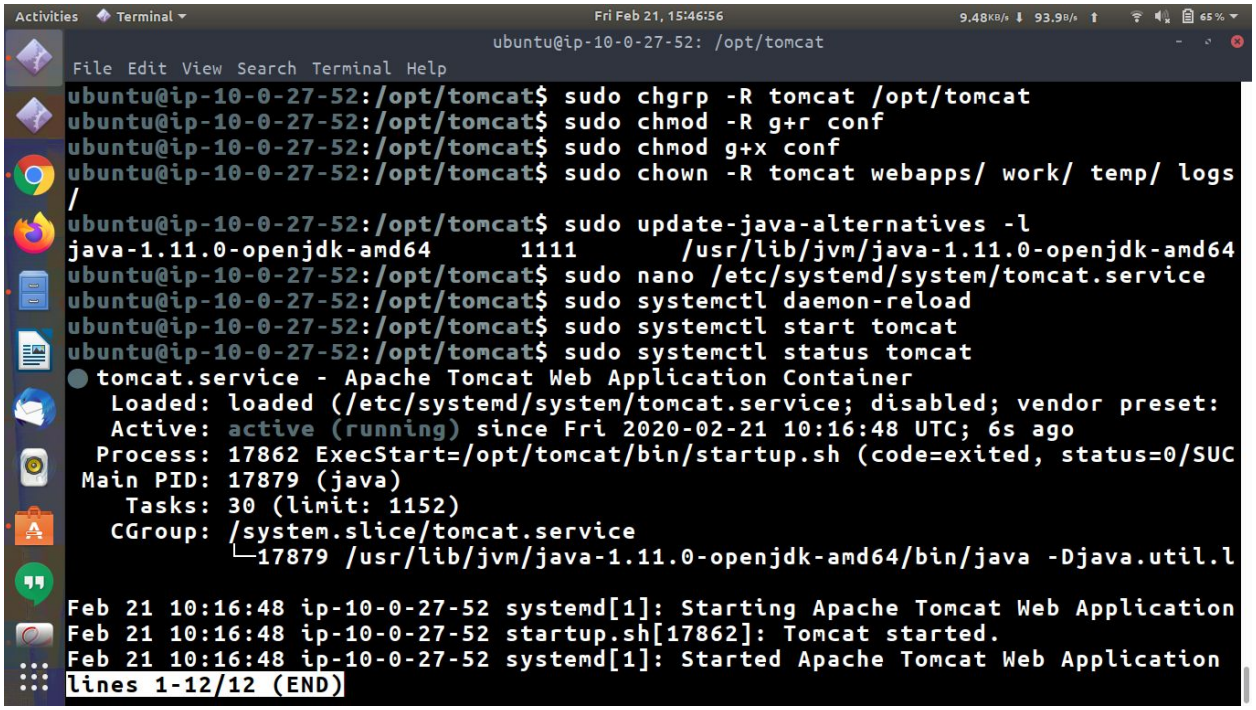


Login into tomcat server

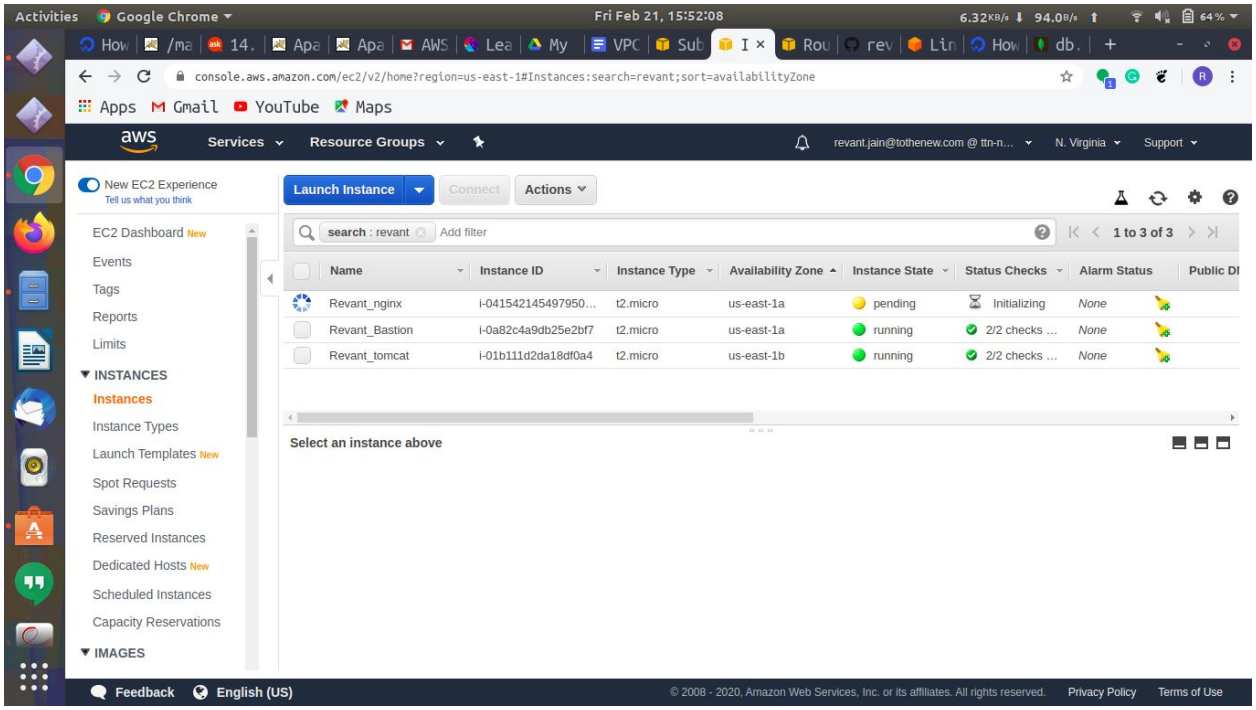
```
ubuntu@ip-10-0-27-52: ~
File Edit View Search Terminal Help

  System information as of Fri Feb 21 09:28:10 UTC 2020

  System load:  0.0                Processes:           86
  Usage of /:   13.6% of 7.69GB    Users logged in:     0
  Memory usage: 14%                IP address for eth0: 10.0.27.52
  Swap usage:   0%

0 packages can be updated.
0 updates are security updates.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-27-52:~$
```

Install tomcat

```
ubuntu@ip-10-0-27-52: /tmp
File Edit View Search Terminal Help
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for systemd (237-3ubuntu10.33) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...

Processing triggers for ca-certificates (20180409) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...

done.
done.
ubuntu@ip-10-0-27-52:~$ sudo useradd -s /bin/false -g tomcat -d /opt/tomcat tomc
at
useradd: group 'tomcat' does not exist
ubuntu@ip-10-0-27-52:~$ sudo groupadd tomcat
ubuntu@ip-10-0-27-52:~$ sudo useradd -s /bin/false -g tomcat -d /opt/tomcat tomc
at
ubuntu@ip-10-0-27-52:~$ cd /tmp
ubuntu@ip-10-0-27-52:/tmp$ curl -O http://mirrors.estointernet.in/apache/tomcat/
tomcat-9/v9.0.31/bin/apache-tomcat-9.0.31.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
 86 10.5M   86 9309k    0     0   960k      0  0:00:11  0:00:09  0:00:02 1098k
```



Launch Nginx server in Public subnet



```
Setting up libnginx-mod-http-image-filter (1.14.0-0ubuntu1.7) ...
Setting up nginx-core (1.14.0-0ubuntu1.7) ...
Setting up nginx (1.14.0-0ubuntu1.7) ...
Processing triggers for systemd (237-3ubuntu10.33) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ufw (0.36-0ubuntu0.18.04.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
ubuntu@ip-10-0-4-22:~$ service nginx restart
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to restart 'nginx.service'.
Authenticating as: Ubuntu (ubuntu)
Password:
ubuntu@ip-10-0-4-22:~$ sudo service nginx status
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2020-02-21 10:23:44 UTC; 32s ago
     Docs: man:nginx(8)
 Main PID: 2416 (nginx)
    Tasks: 2 (limit: 1152)
   CGroup: /system.slice/nginx.service
           ├─2416 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
           └─2417 nginx: worker process

Feb 21 10:23:44 ip-10-0-4-22 systemd[1]: Starting A high performance web server and a reverse prox
Feb 21 10:23:44 ip-10-0-4-22 systemd[1]: nginx.service: Failed to parse PID from file /run/nginx.p
Feb 21 10:23:44 ip-10-0-4-22 systemd[1]: Started A high performance web server and a reverse proxy
lines 1-13/13 (END)
```

```
server{
        listen 80;
        server_name localhost;
        location / {
                proxy_pass http://10.0.27.52:8080;
        }
}
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --                                                    7,2           All
```