VPC:

Q1. When to use Elastic IP over Public IP

Public IP	**Elastic IP**
It is assigned to your launched instance.	It is assigned to your AWS account.
when an instance is terminated the public IP attached to it gets released and further when you relaunch the same instance new IP address is assigned.	Elastic IP does not change and they remain the same even if you terminate the instance and later again restart the same instance.

- **Use case:**

1. Elastic IP is used when you are working on a long time project and configuration of IP sometimes consumes more time.
2. Public IP is used when you are working on small projects and running 2-3 servers. Here in this situation you make use of IP for short time.

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

Valid IP ranges of LAN:

- The first three octets of an IP address should be the same for all computers in the LAN. For example, if a total of 128 hosts exist in a single LAN, the IP addresses could be assigned starting with 192.168.1. *x*, where *x* represents a

number in the range of 1 to 128. You could create consecutive LANs within the same company in a similar manner consisting of up to another 128 computers.

- There are different classes of networks that determine the size and total possible unique IP addresses of any given LAN. For example, a class A LAN can have over 16 million unique IP addresses. A class B LAN can have over 65,000 unique IP addresses. The size of your LAN depends on which reserved address range you use and the subnet mask (explained later in the article) associated with that range

Address range	Subnet mask	Provides	Addresses per LAN
10.0.0.0 – 10.255.255.255.255	255.0.0.0	1 class A LAN	16,777,216
172.16.0.0 – 172.31.255.255	255.255.0.0	16 class B LANs	65,536
192.168.0.0 – 192.168.255.255	25.255.255.0	256 class C LANs	256

Implications:

We can use every IP-Address-Range we want in our private network. There is nothing against this. But we have to take precautions to avoid routing-trouble when a machine with an IP-Address that actually belongs to a public range wants to access the internet. Here you have to have a Router or Firewall that is able to NAT your internal address bidirectionally.

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

- **Cannot create a VPC peering connection between VPCs in different regions. This may change in future releases.**
- **VPC soft limit of 50 peering connection applies.**
- **VPC peering connections created between VPCs that have overlapping subnet CIDR blocks may not take effect.**
- **You cannot have more than one VPC peering connection between the same two VPCs at the same time.**
- **You cannot create a VPC peering connection between VPCs in different regions.**
- **After a VPC peering connection is established, the local and peer tenants must add routes in the local and peer VPCs to enable communication between the two VPCs.**

- **You cannot delete a VPC for which VPC peering connection routes have been configured.**

Q4. Differentiate between NACL and Security Groups.

In terms of application:

Security groups are tied to an instance whereas Network ACLs are tied to the subnet. i.e. Network Access control lists are applicable at the subnet level, so any instance in the subnet with an associated NACL will follow rules of NACL. That's not the case with security groups, security groups have to be assigned explicitly to the instance. This means any instances within the subnet group get the rule applied.

In terms of state:

Security groups are stateful. Network ACLs are stateless: This means any changes applied to an incoming rule will not be applied to the outgoing rule.

In terms of rules:

All rules in a security group are applied whereas rules are applied in their order (the rule with the lower number gets processed first) in Network ACL.

Security group first layer of defense, whereas Network ACL is second layer of the defense.

Q5. 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 IP in subnet.

/20 means first 20 bits of the IP address are network bits and the rest are host bits

Number of hosts bits = 32 - 20 =12

Number of ip’s possible = 2^host bits -2 = 2^12 - 2

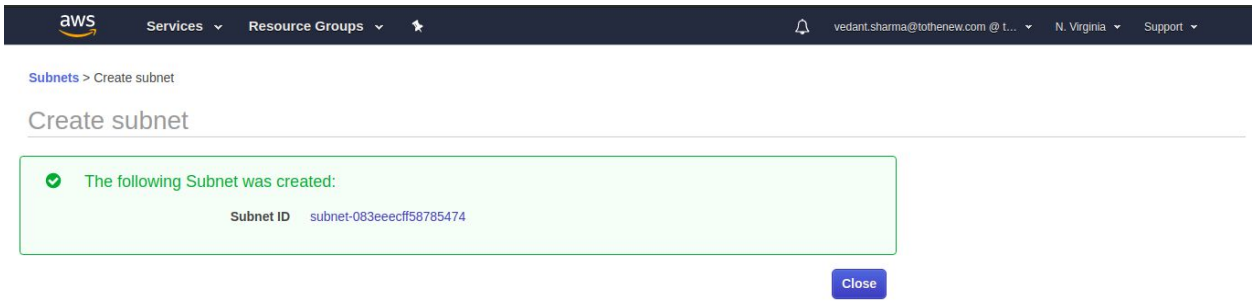
Number of subnets possible = 2^4 = 16

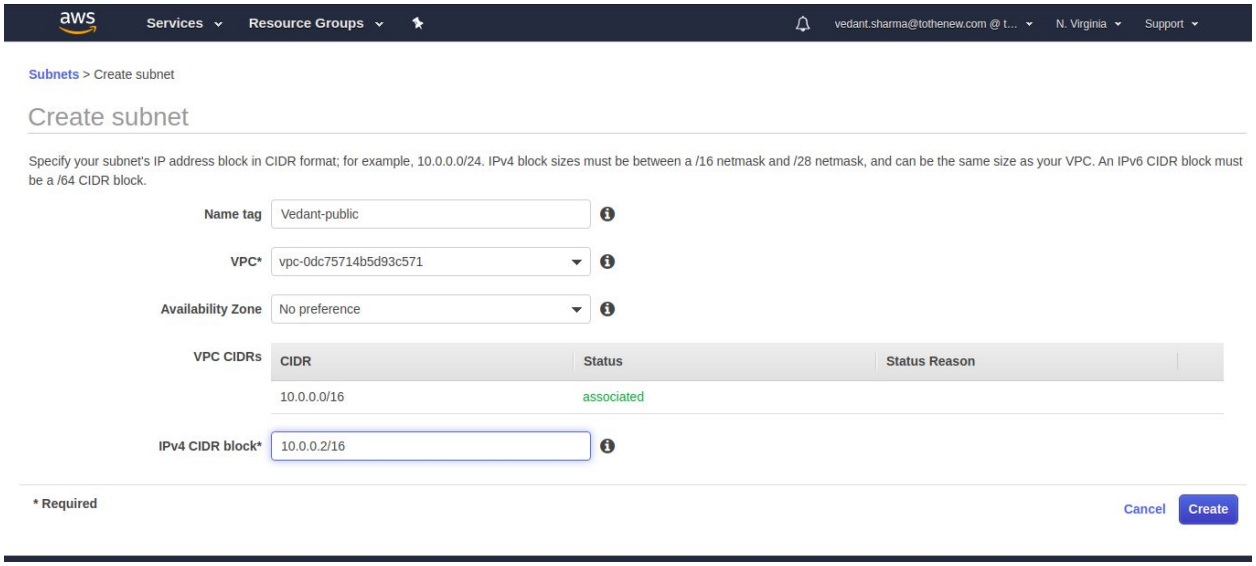
Q6. Implement a 2-tier vpc with following requirements:

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 proxypass to Tomcat from Nginxs

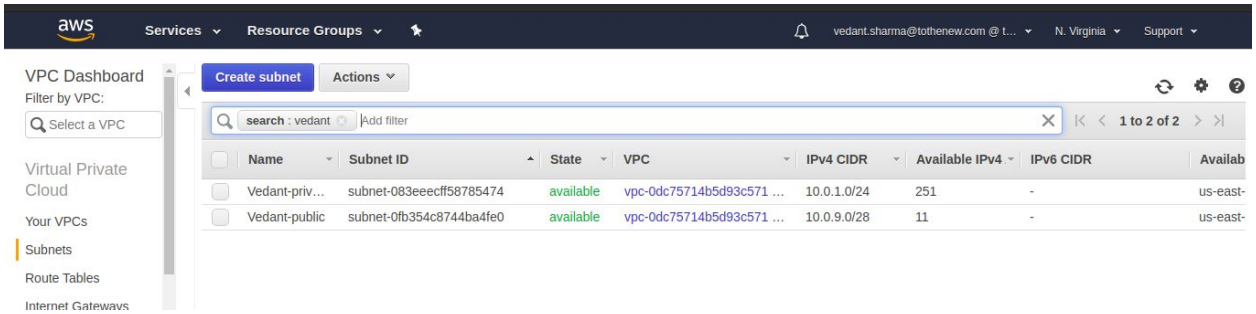
Creating a subnet:

Private subnet



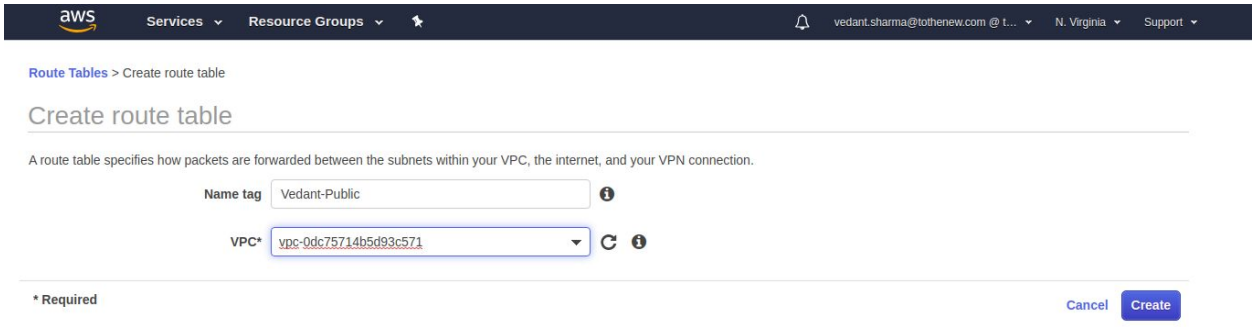


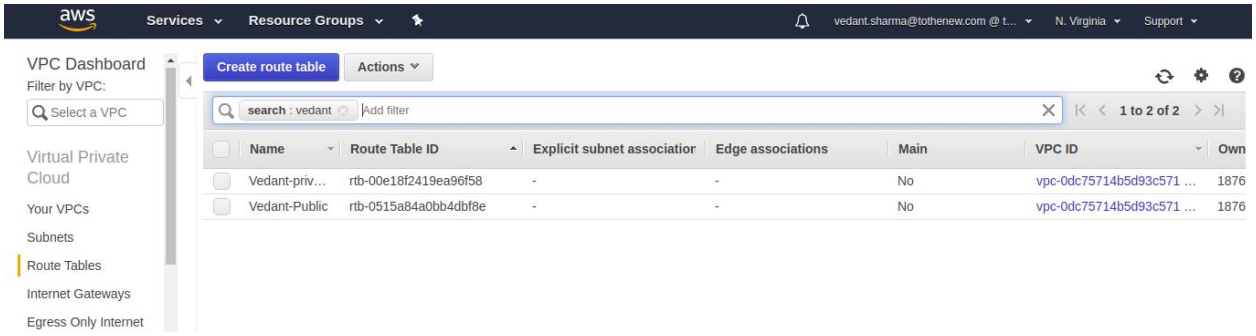
Sub-nets



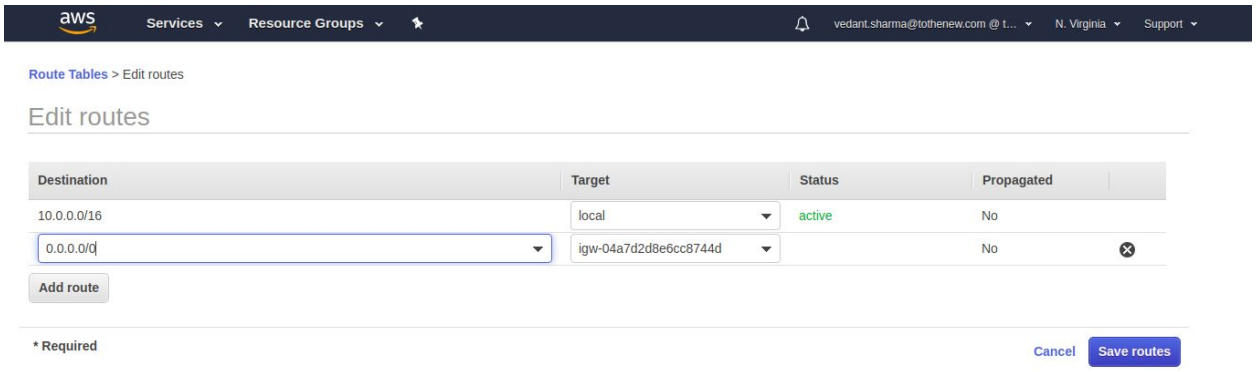
Creating a internet gateway

Creating route tables:

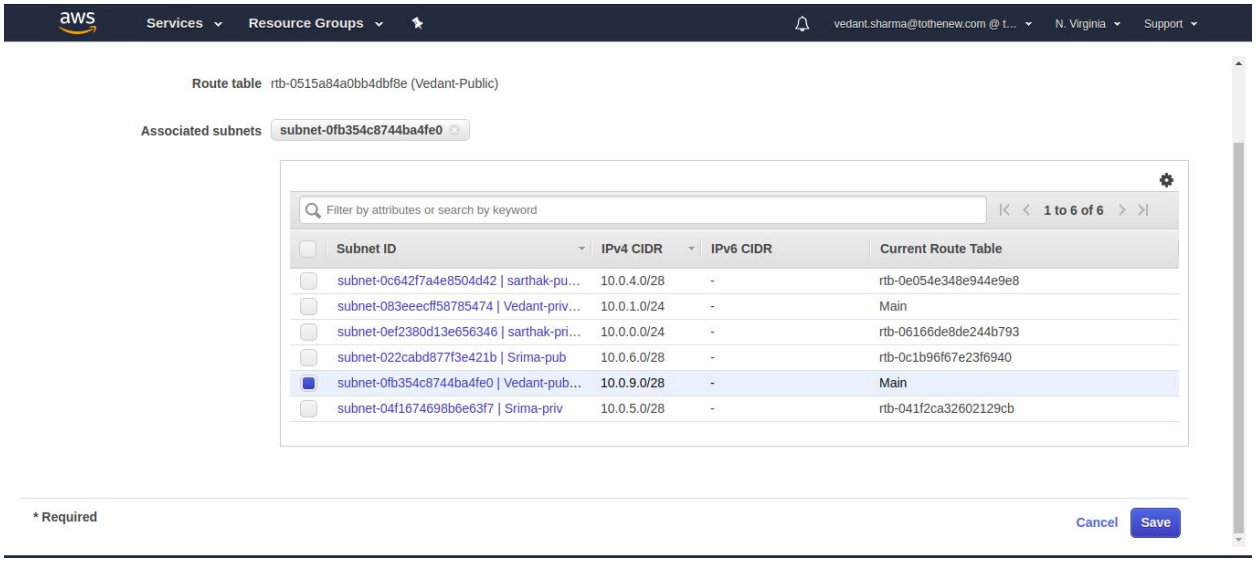


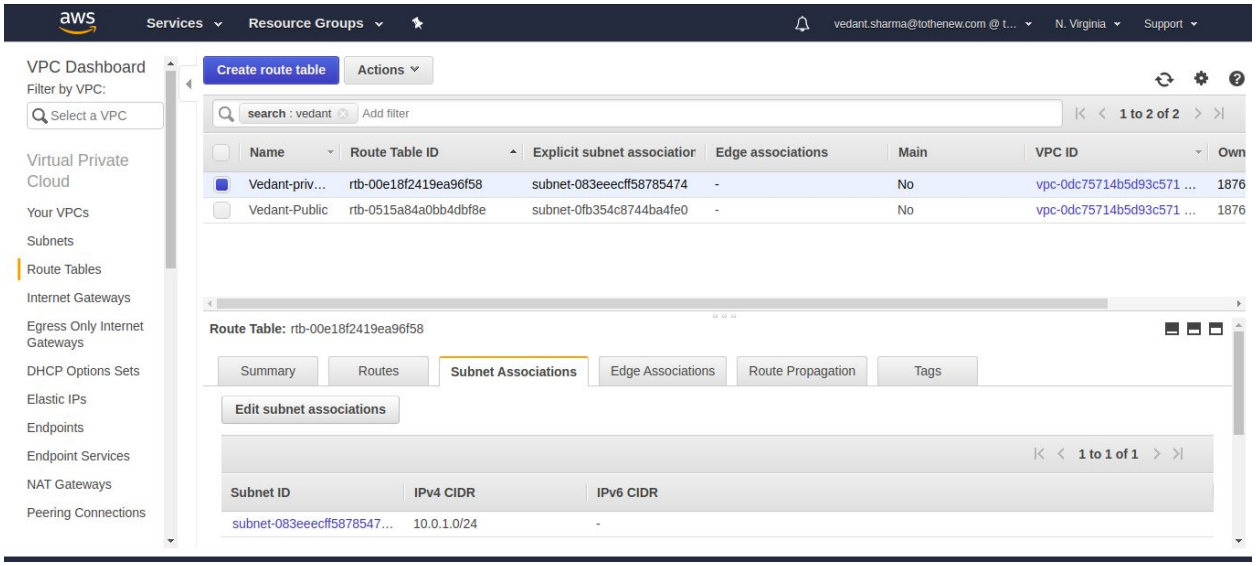


Adding internet gateway to public route table:

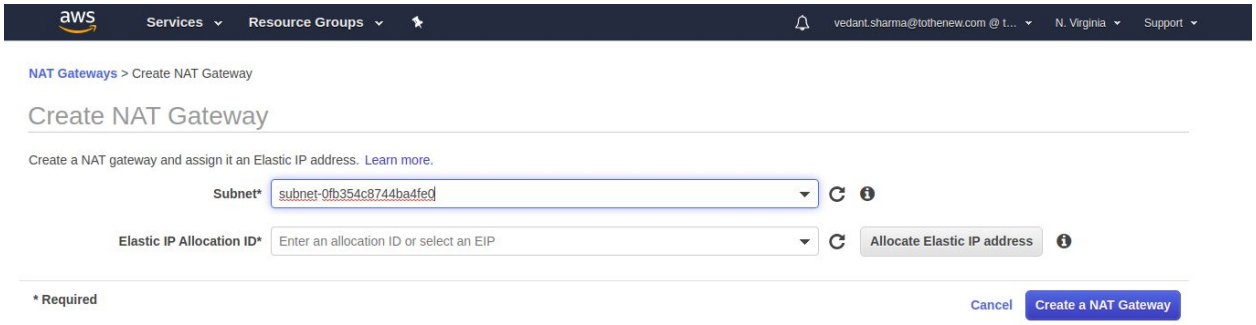


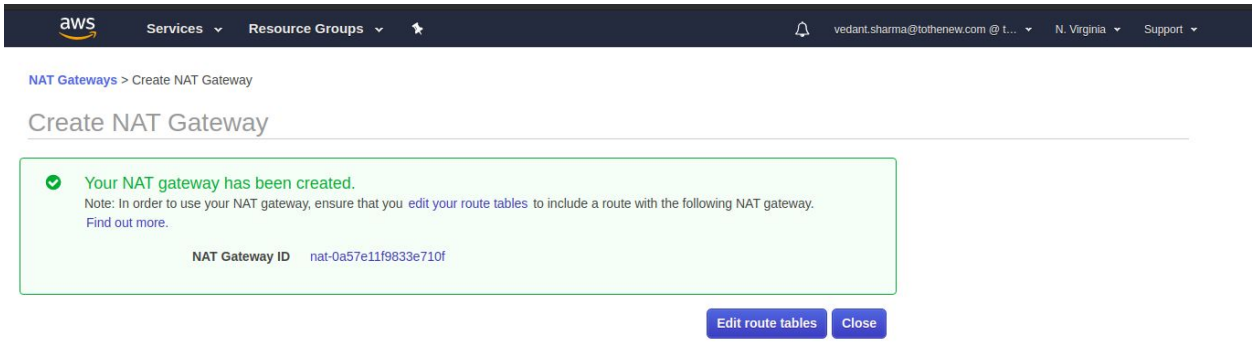
Subnet association:



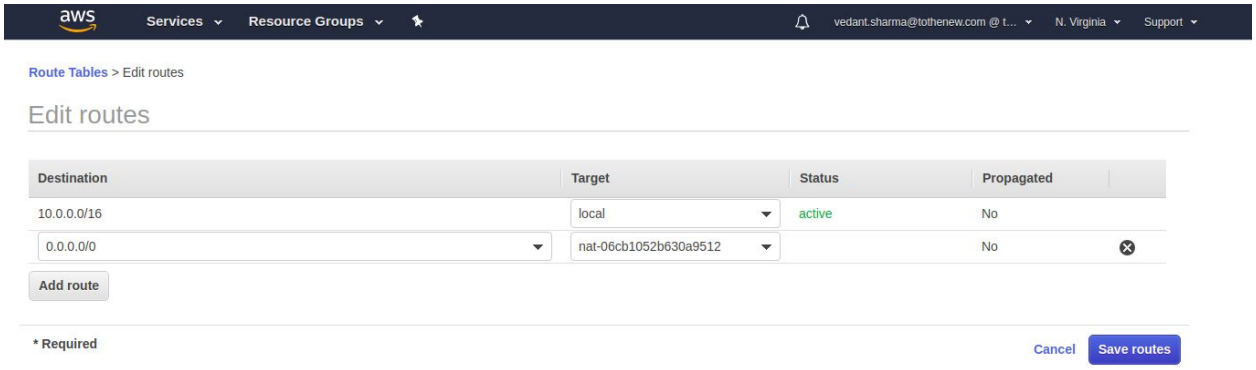


Creating a NAT gateway in public subnet

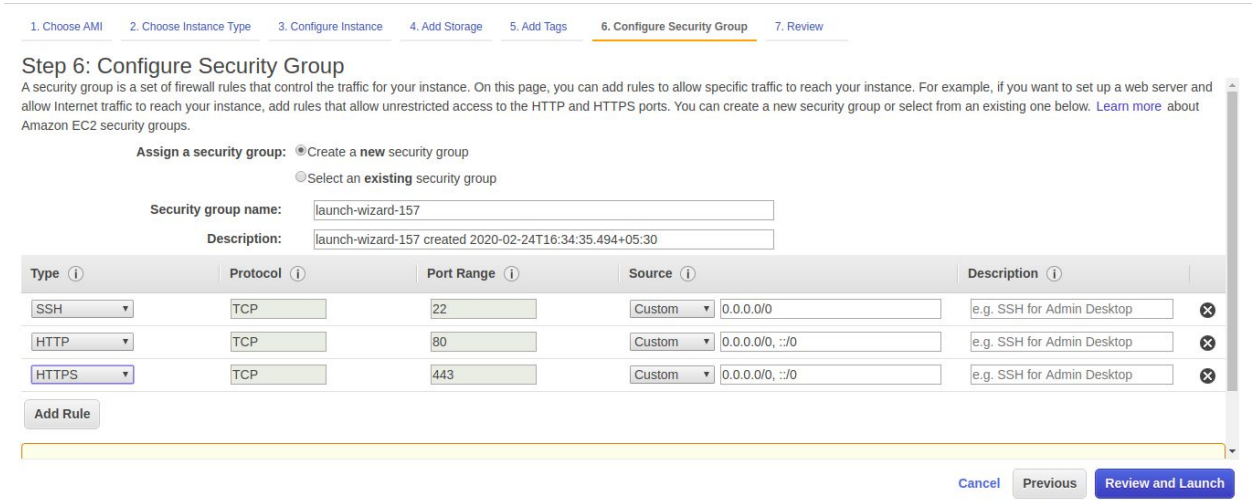




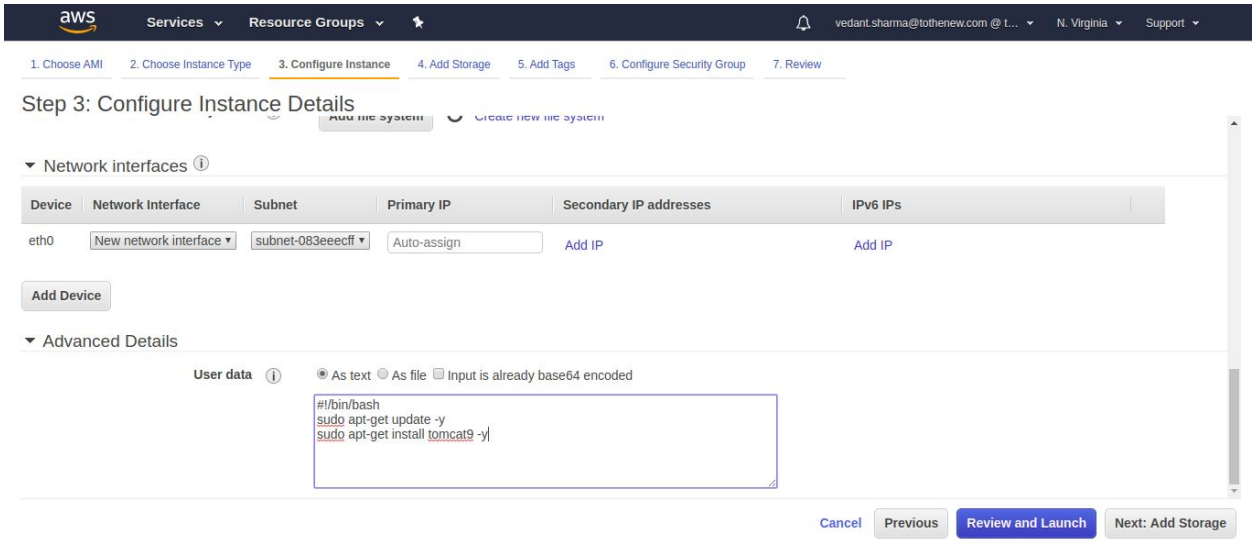
Associating NAT gateway to private route table



Launching an instance in public subnet



Installing tomcat using user data



SSH into the public instance to install nginx

```
vedant@Vedant-Sharma:~/Desktop$ sudo ssh -i Vedant-Bootcamp.pem ubuntu@3.92.222.193
[sudo] password for vedant:
The authenticity of host '3.92.222.193 (3.92.222.193)' can't be established.
ECDSA key fingerprint is SHA256:Y9/81499bQw754lZtUBZS1XT+KnPKvf5rLaiwMJEBO0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '3.92.222.193' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

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

  System information as of Mon Feb 24 11:17:43 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: 10.0.9.10
  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-10-0-9-10:~$ sudo systemctl enable nginx
Synchronizing state of nginx.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable nginx
ubuntu@ip-10-0-9-10:~$
ubuntu@ip-10-0-9-10:~$
ubuntu@ip-10-0-9-10:~$
ubuntu@ip-10-0-9-10:~$ sudo systemctl start nginx
ubuntu@ip-10-0-9-10:~$ sudo systemctl status nginx
● 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 Mon 2020-02-24 11:20:06 UTC; 1min 22s ago
     Docs: man:nginx(8)
 Main PID: 2326 (nginx)
    Tasks: 2 (limit: 1152)
   CGroup: /system.slice/nginx.service
           ├─2326 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
           └─2328 nginx: worker process

Feb 24 11:20:06 ip-10-0-9-10 systemd[1]: Starting A high performance web server and a reverse proxy server...
Feb 24 11:20:06 ip-10-0-9-10 systemd[1]: nginx.service: Failed to parse PID from file /run/nginx.pid: Invalid argument
Feb 24 11:20:06 ip-10-0-9-10 systemd[1]: Started A high performance web server and a reverse proxy server.
ubuntu@ip-10-0-9-10:~$
```

Proxy pass:

```
ubuntu@ip-10-0-9-10: /etc/nginx/sites-available 150x38
server {
        listen 80;
        Server_name test.com


        root /var/www/html;
        index index.html;

        location / {
                proxy_pass http://10.0.1.129:8080;
        }
}

~
~
~
```

Entry in /etc/hosts

```
ubuntu@ip-10-0-9-10: ~ 150x38
127.0.0.1 localhost test.com


# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
~
~
~
~
~
```

Curl into test.com it will proxy pass to the apache server running on private subnet