AWS

===========

VPC

===

Virtual Private Cloud.

A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC.

When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. This is the primary CIDR block for your VPC.right click on vpc dev 🡪edit dns host name 🡪auto assign,we will get name to dns servers.

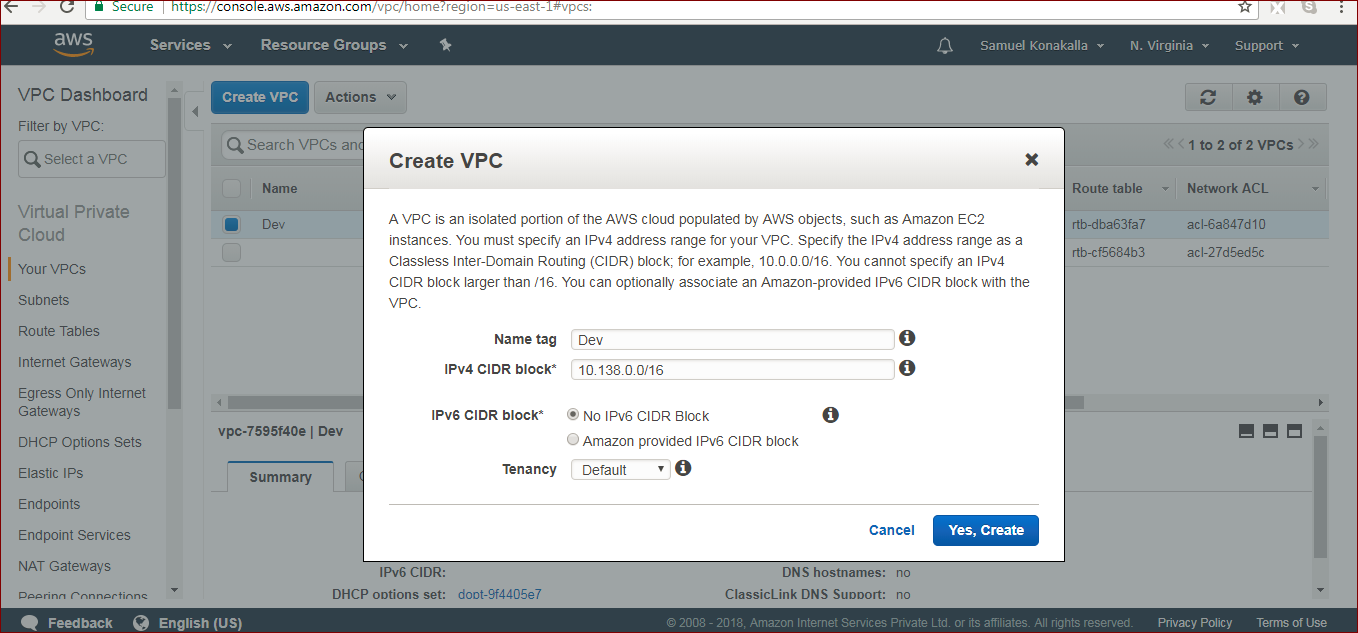
It is network,whenever we are devide this network into multiple parts i.e subnets.if we allow internet in this network i.e internet gateway.if we allow communication between this subnets we need routing.

Now I created one network for Dev environment.

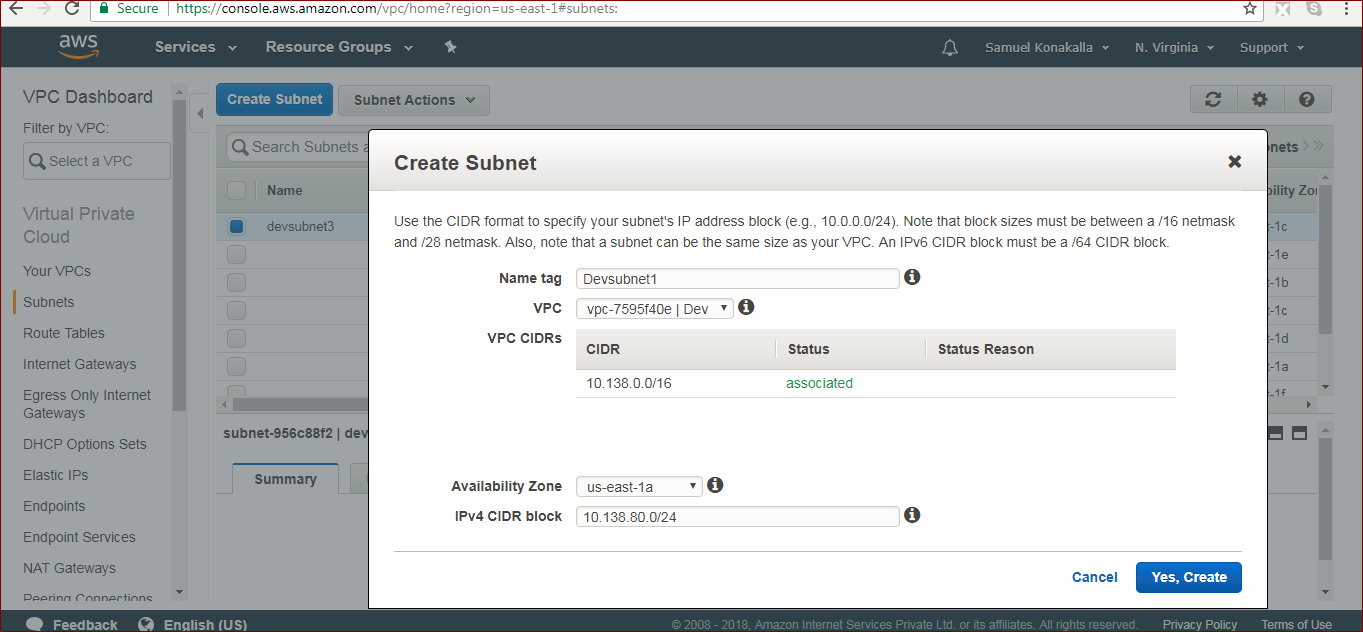
VPC—Dev(Single Network with multiple subnets)

We will specify what is the network range 10.138.0.0/16 i.eIPV4 CIDR.

So whenever we are creating subnets,all subnet should be in the range of above IPV4 range.



Subnet:now im creating 3 subnets in 3 different zones (u.s eat 1a,1b,1c).and ip range should be different.10.138.77.0/24, 10.138.78.0/24, 10.138.79.0/24.



Internetgateway:suppose if we want to connect to this VPC dev network we need create one internet gateway and we should attach to this VPC-Dev..



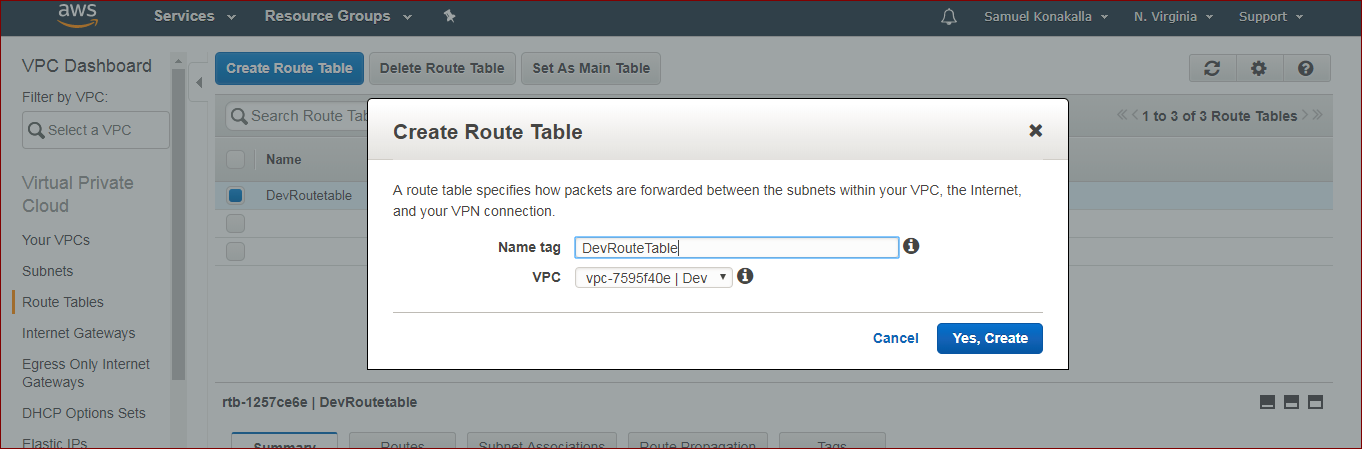
Routing:now I have 3 subnets

Subnet1—us.east -1a

Subnet2—us.east -1b

Subnet3—us.east -1c

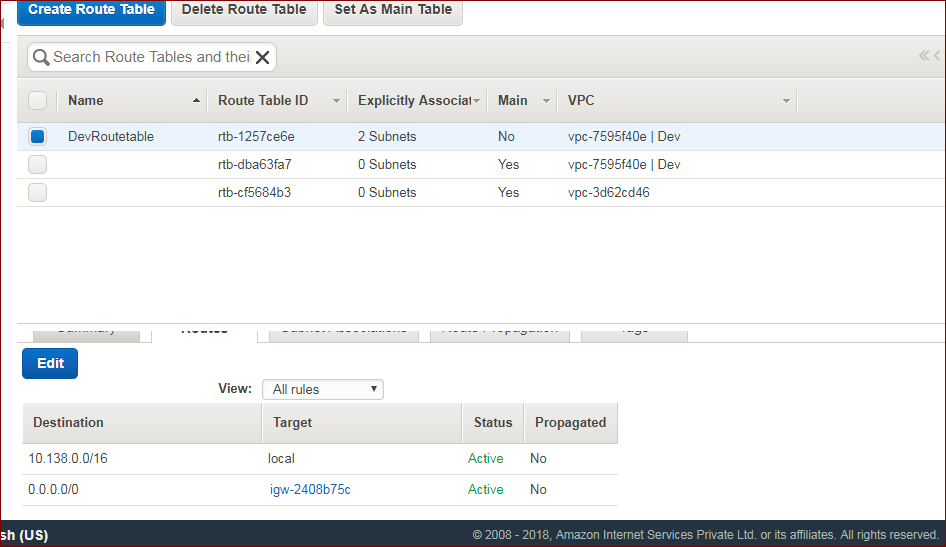
If subnet1 is communicating with subnet3 its not possible to communicate ,because we are in same network but in different zones.so now routing is required.



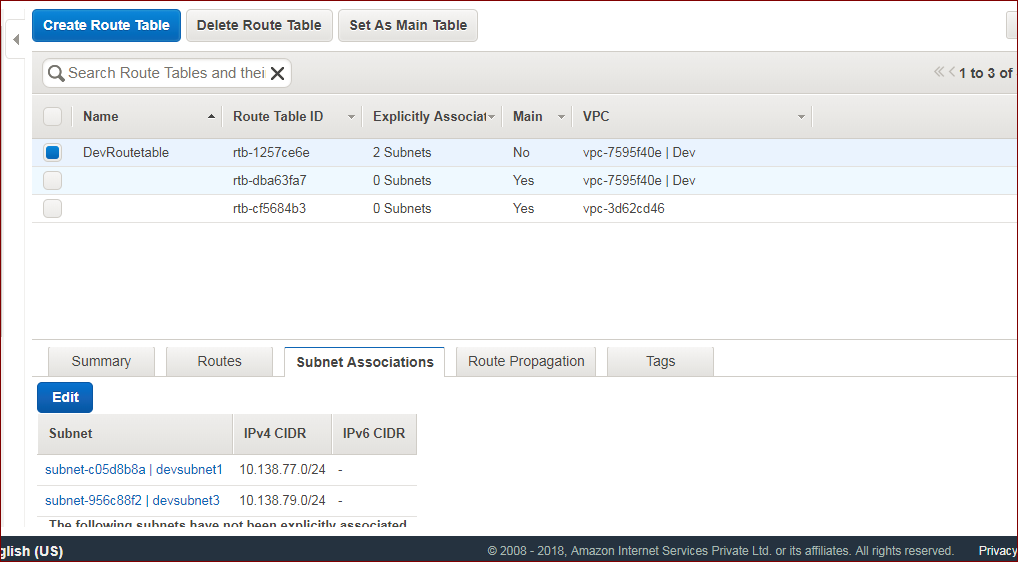
After creating routing table we should select and if we check bottom we have different tabs.

Select routes add rule ,in this we add first 0.0.0.0/0

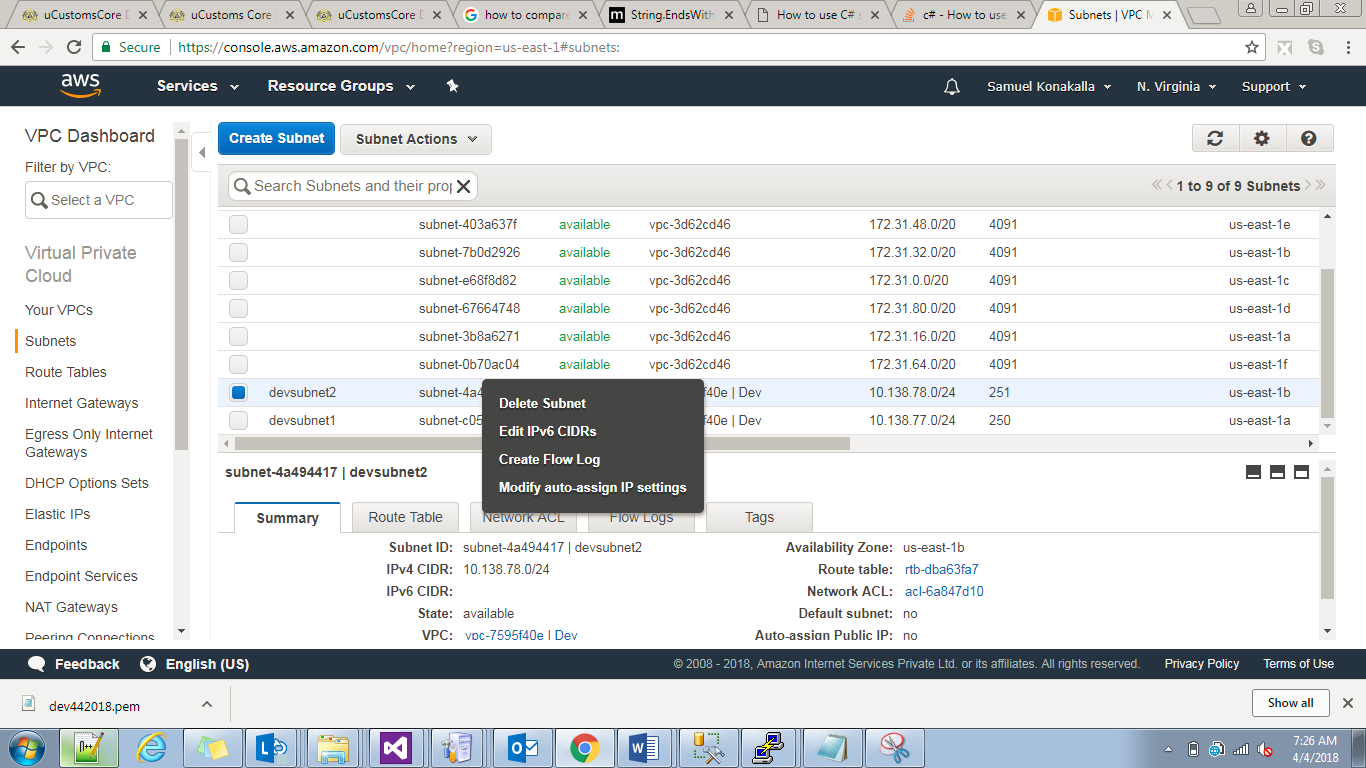
.this is for allowing internet from out side to this network and Also we have seen some local route.this is taking from VPC .



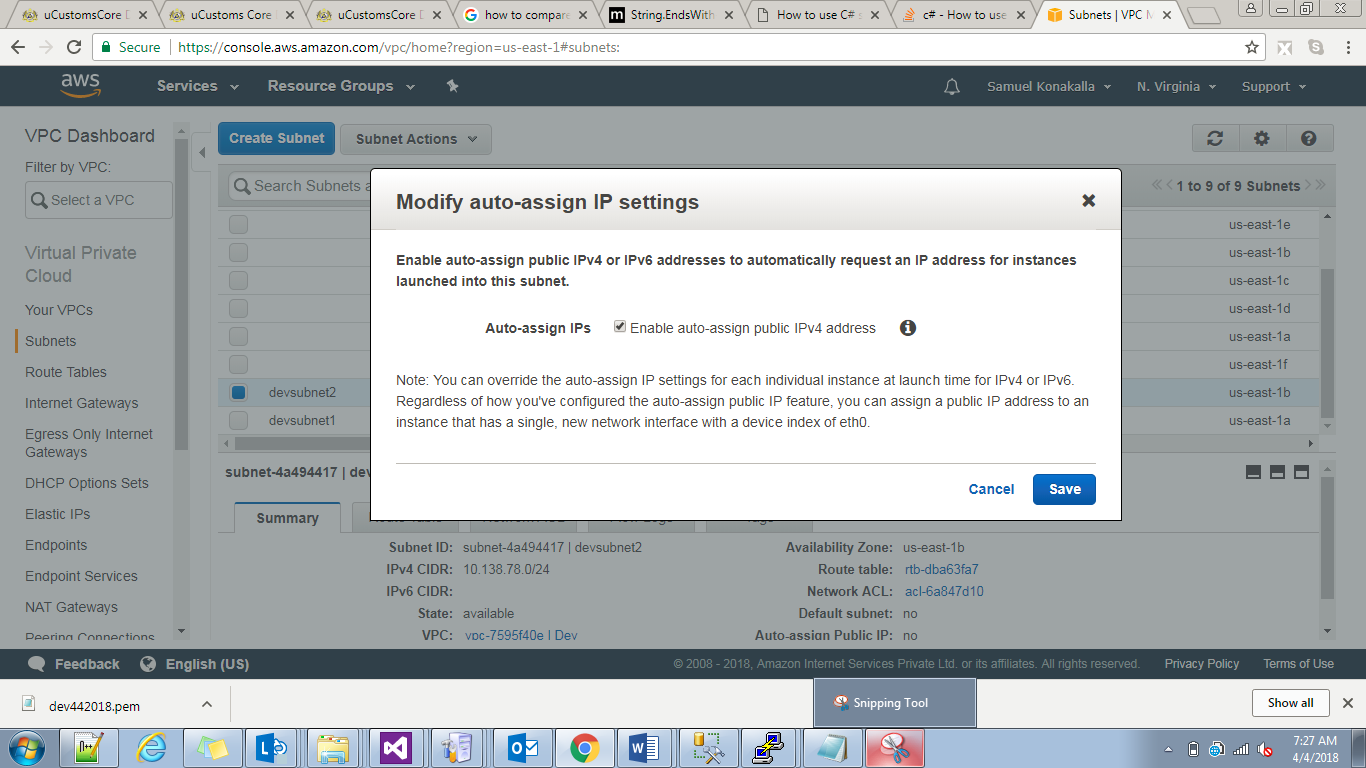
In subnet association we should select subnets for communicating.



Important thing ,after finishing network setup then we will create VM’s and we will add to our network.so at that time we will access these instance from outside .we login with putty and we will give public ip.we have one option in subnet i.e

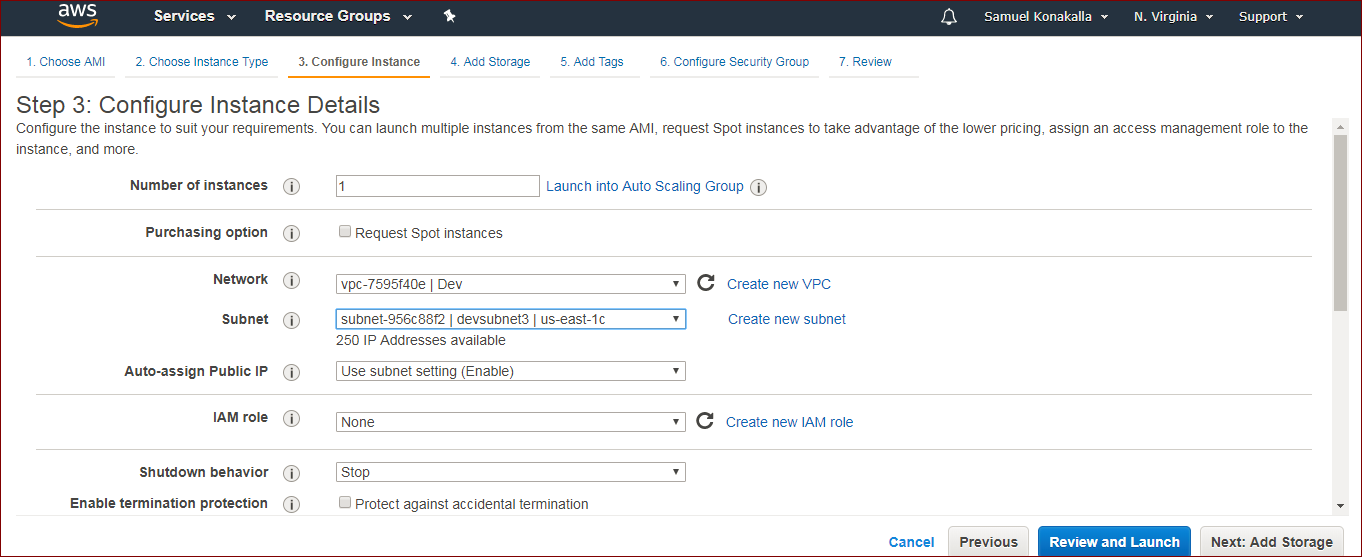


If we select auto assign ip

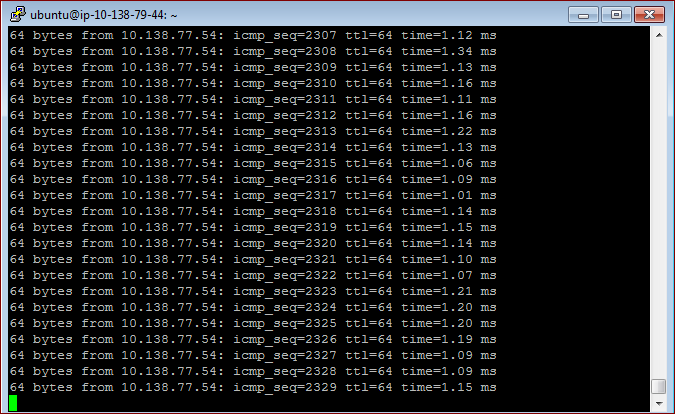


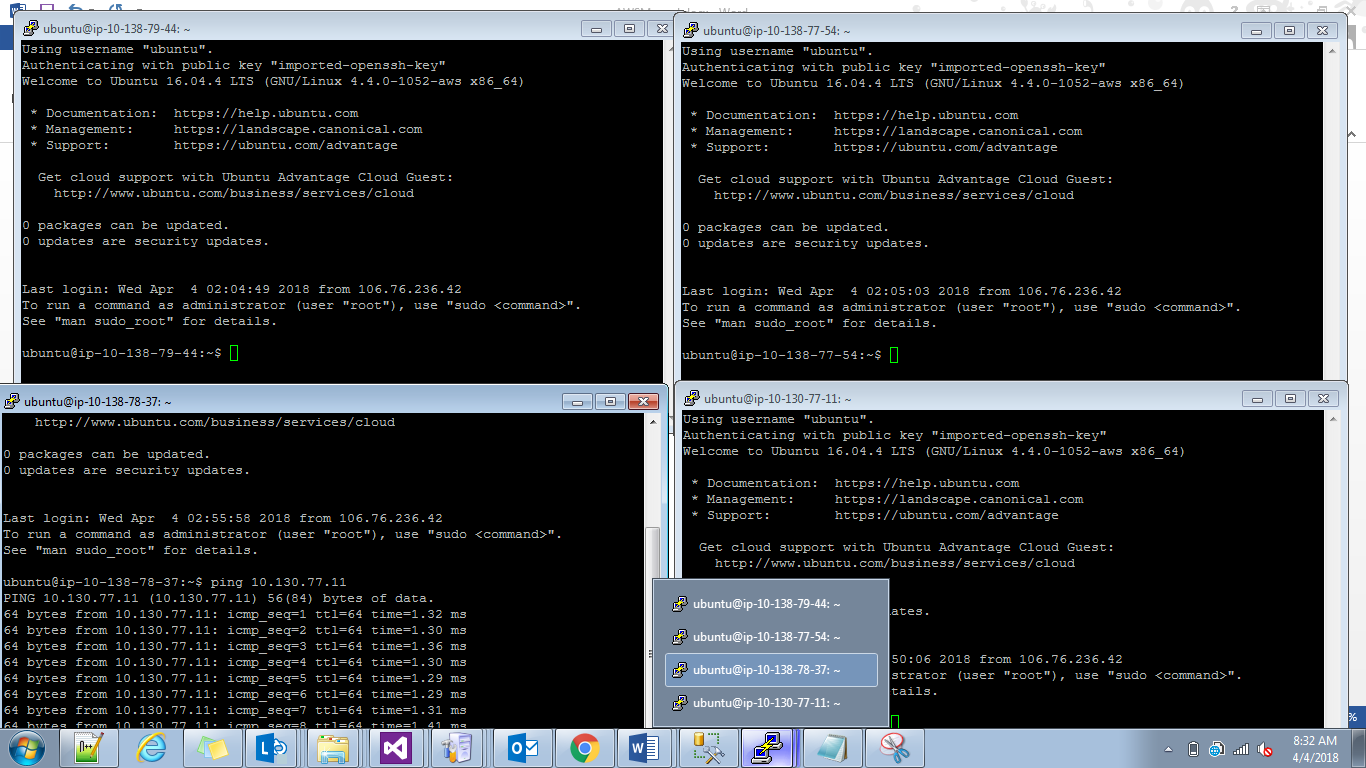
We should save it.

Now we will create two vm’s in two different zones.



Now we will get two vms public ip’s.so we login with putty in two machines and by using ping command we can checking whether it is response is coming or not.





If im taken ip range 10.138.77.0 max we will use 251 ip address but it will use remaining 5 for

10.138.77.0 n/w

10.138.77.255 broadcast

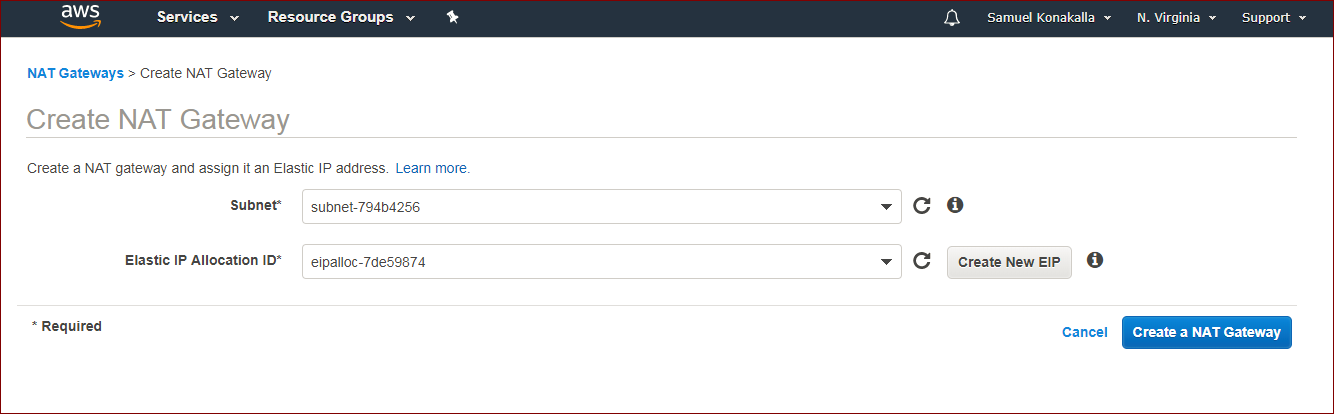
10.138.77.1,2,3 --used by AWS for gateways.

For 1 vpc we will attach only one gateway.

Public subnet:the subnet access through internet gateway called public subnet.

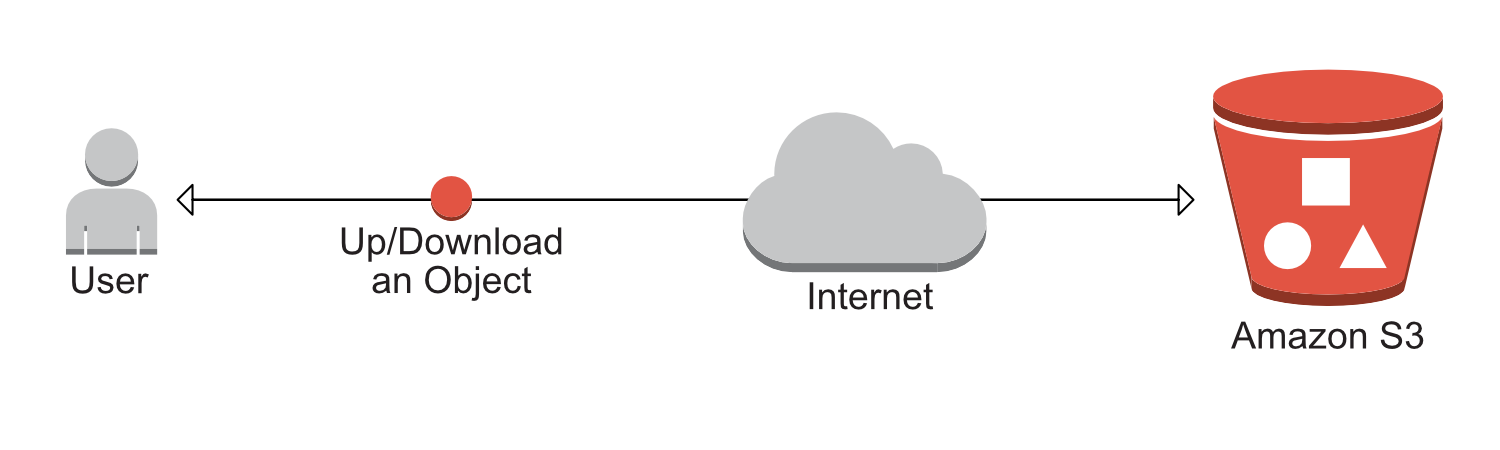
Private subnet:the subnet we cannot access through igw.

We cant connect private subnet instances through internet.mainly we will create this private subnets for database purposes.



S3:simple storage Service.

S3 provides secure ,durable,highly scalable object storage.we will store unlimited data.

  
S3 componets:Buckets🡪folders and files(objects).S3 is in region level.

Objects:meta data ,key ,value,versioning id.

Storage Class:

1)Standard—Designed for general purpose,default storage,most expensive.

2)Reduced redundancy(RRS).-->Designed for non critical,reproducible object.

3)In frequent Acess (s3-1A)🡪designed for object that do not access frequently,but must be immediately availabl when accessed.less expensive that standard/RRS storage.

4)Glacier.-->long term archival purpose.back up data like last year data.

S3 object life cycle:

An object life cycle is a set of eules that automate the migration of of an object storage classes to different storage class,based on specific time intervals.by using this automate process we can reduce the cost as much as possible.

Eg:I have movie trailer first I will keep this one b4 relase like assume 30 days I will kepp it into standard storage.after movie relaesd after 90 days I moved to glacier.

S3 versioning:by default it is disabled we can enable by manual.

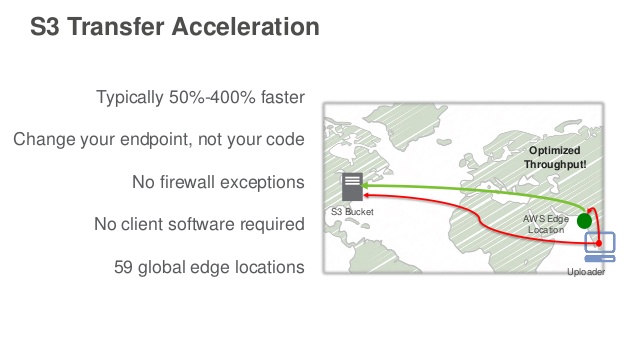
S3 cross region application.:

Suppose one bucket im modified any file aautomatically the same replica will be effected in another region in same bucket and not vice versa.beore this we should enable versioning for both source and destinations buckets in their regions.

It may be in same account or in dffrent accounts.

S3 supports static webhosting.

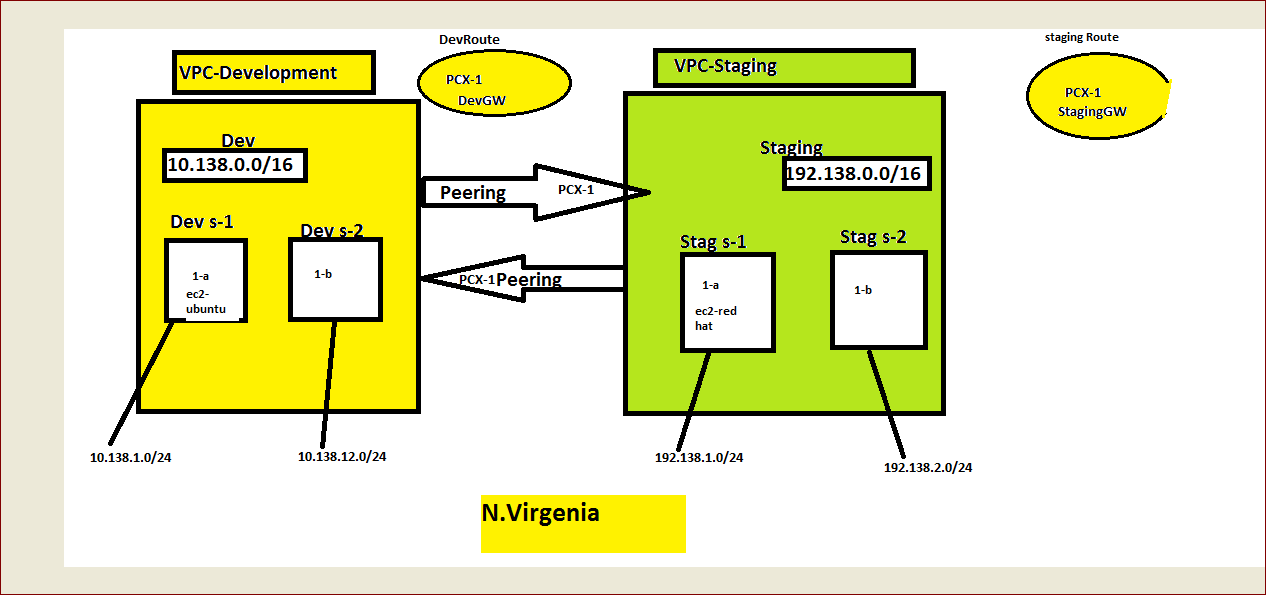
S3 tranfer Accelaration:



Suppose if we want to send data to u.s n Virginia if its very long from present location,then we will send to edge points and they will send data to s3 storage immediately they high configuration systems.

ACL:Acces Control List.it acts as firewall at subnet level.it is stateless ,so we should specify both inbound and outbound traffic.by default all traffic shold allowed between whaterver we mentioned in routing table in that network.

Whenever we are requesting a website from breowser first it will go to Load balancer and web server 🡪App server 🡪database server.(it is for java and php ).



NACL is stateless firewall,where as security group is statefull firewall.in statefull firewall,suppose if we open port 80 i.e outbound,when it is coming back it checks already connection is there,so it will allow inbound also,it will alow traffic into ec2.

State less protocol,if allow outbound 80 ,it will not allow inbound until we specify.

At security group if we specify at inbound level ,no need to specify at outbound level,because it’s a statefull firewall.but in outbound if we not specify all traffic even we cant ping to google.com

Because pinging means the request going out i.e outbound.

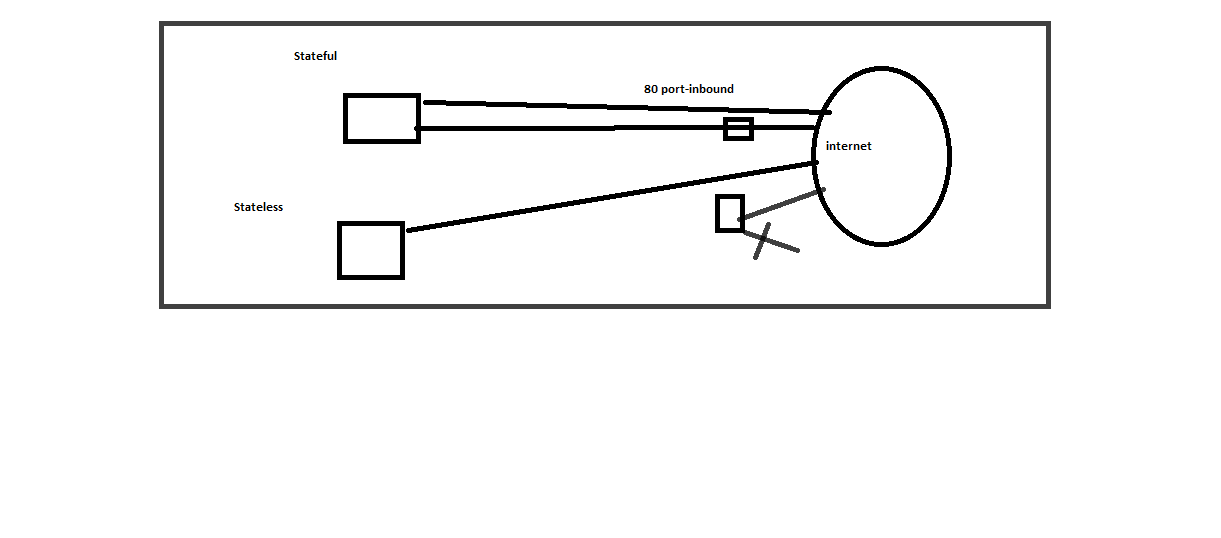
At a time one subnet can be associated with one NACL.

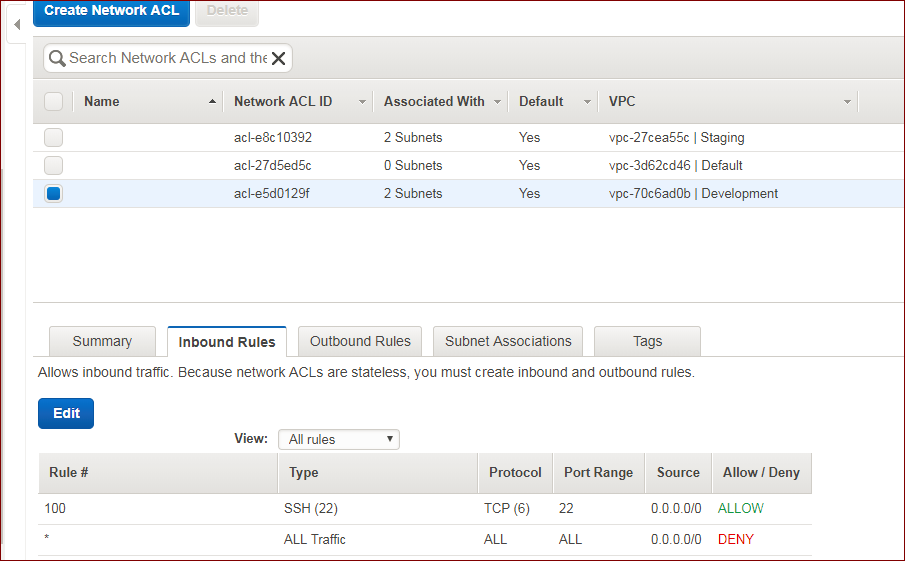
At nacl level suppose at inbound we open ssh means in outbound also we should enable ssh port.but I given same thing but through putty it is not connecting because when traffic is going from subnet i.e outbound it may not use same port it will use different ports those are called ephermal ports.

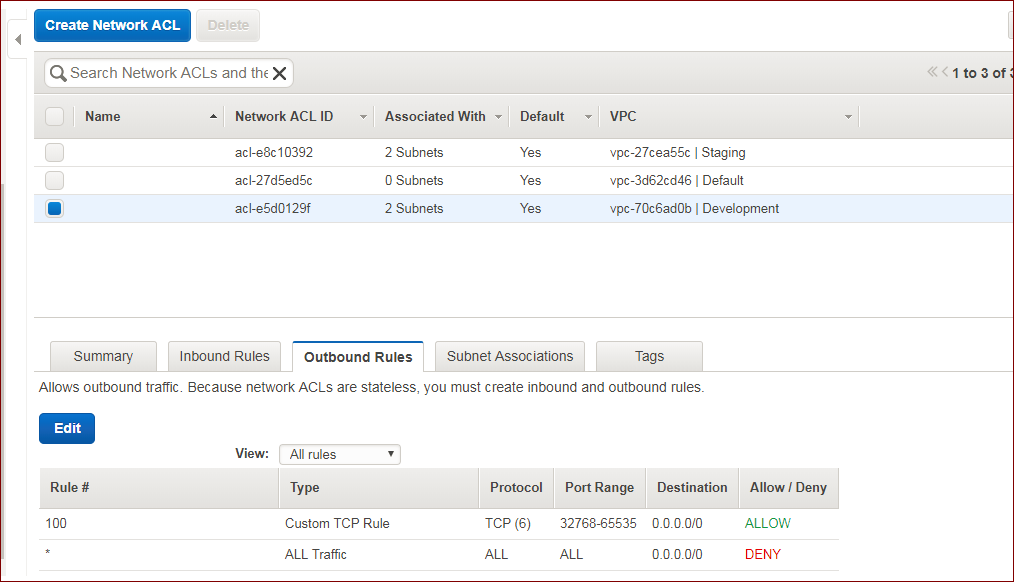
Depending on the operating system we requested the ports will vary.

For linux os ephermal ports (dynamic ports),or windows os these ports will vary.

Klksjbsz,x

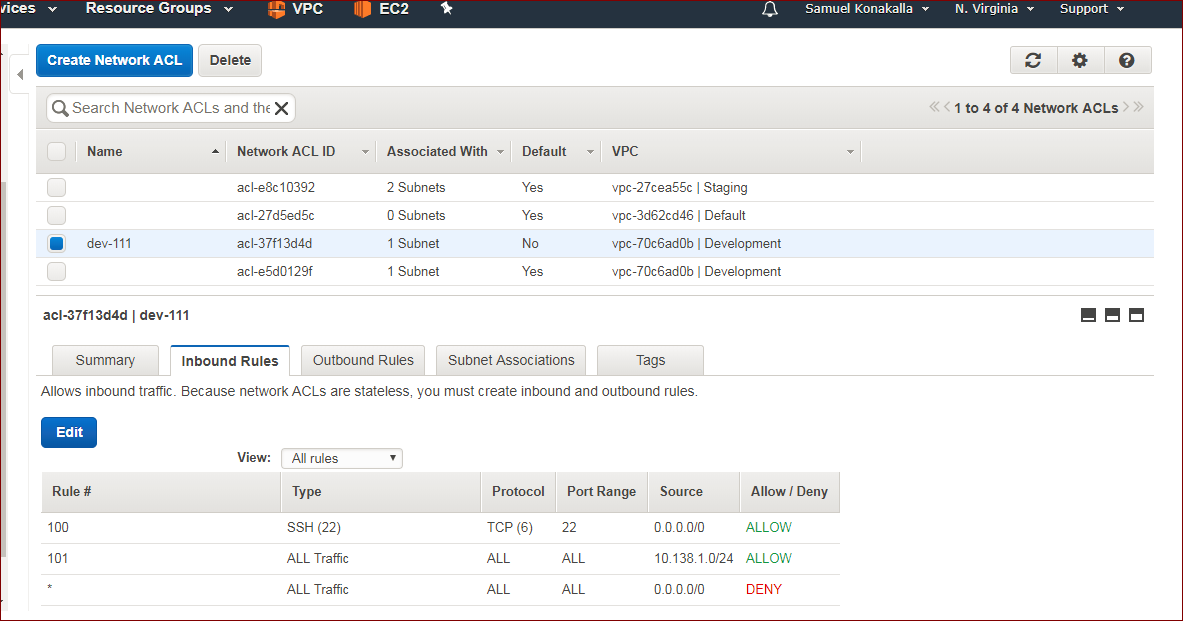


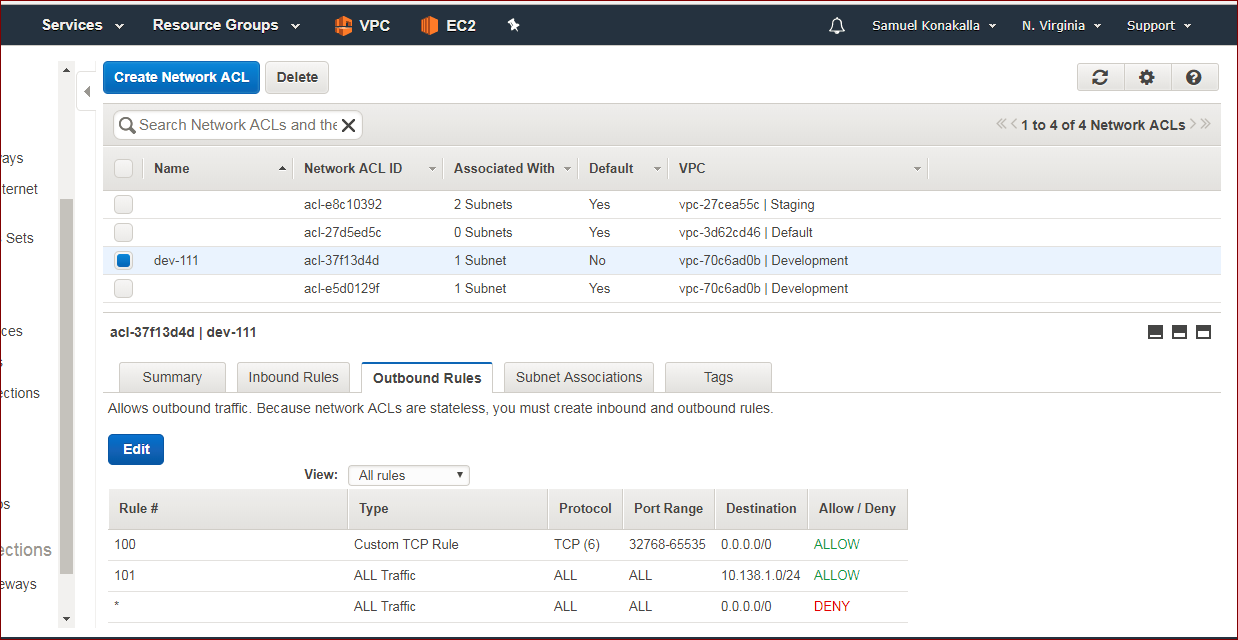


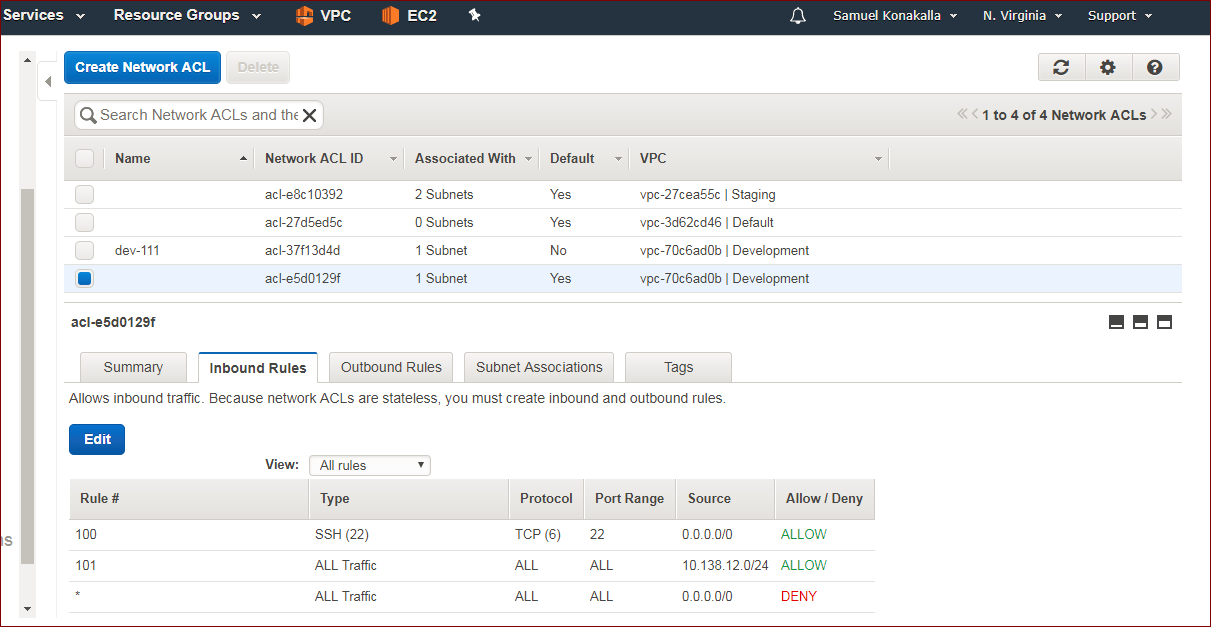


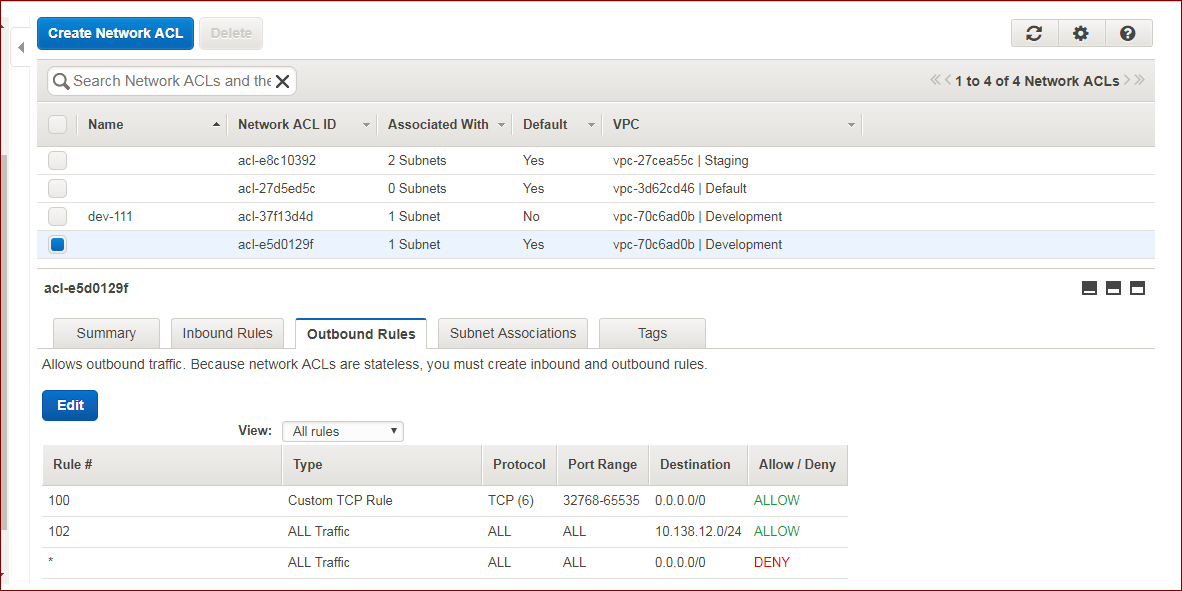
No I provide a security between two subnets in a same network.if two subnets are in same network means automaticalyy both communicate,now I need to provide between those two.

Check two subnets









I have one vpc ,I have two subnets .each subnet automatically communicate with each other now,I created one more NACL and associated one of subnet here and added rules.

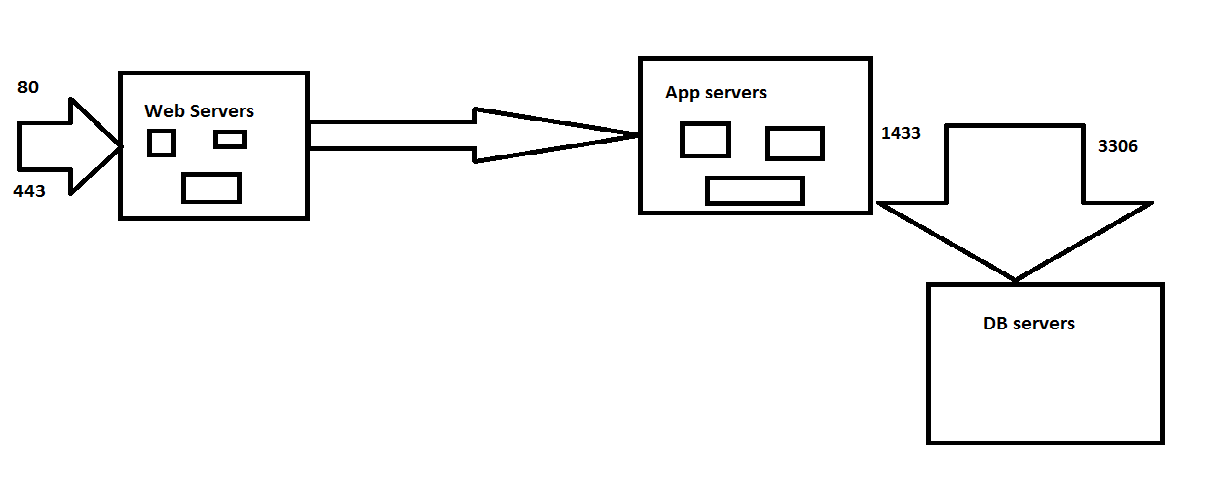
IDS—Intusion Detection

IPS--prevention

Barracuda third party firewall.

How you gave connection to databse.

At security group level I gave access to app servers and ssh only .and not for every one.,



80-http

443-https

Load Balancer:the load will be distributed to equally across multiple web servers.

1)taking 3 web servers with nginx servers.we are writing shell script for installing nginx servers.

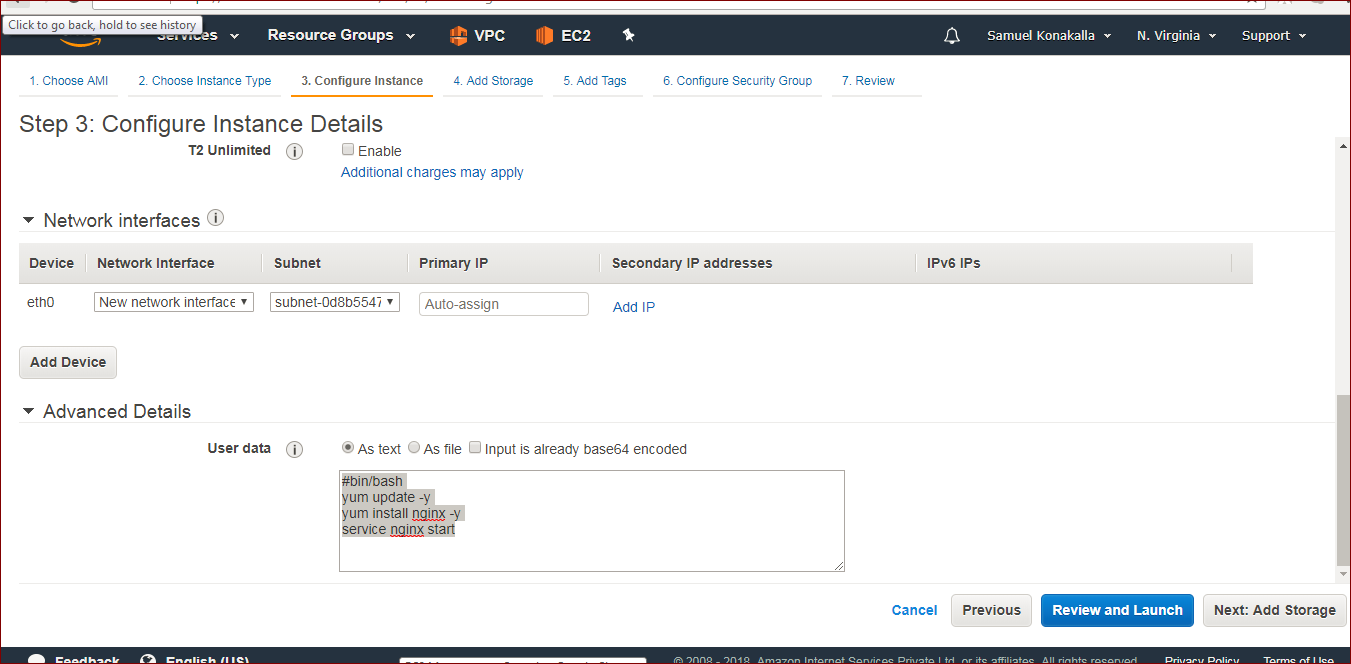
#!/bin/bash

yum update -y

yum install nginx -y

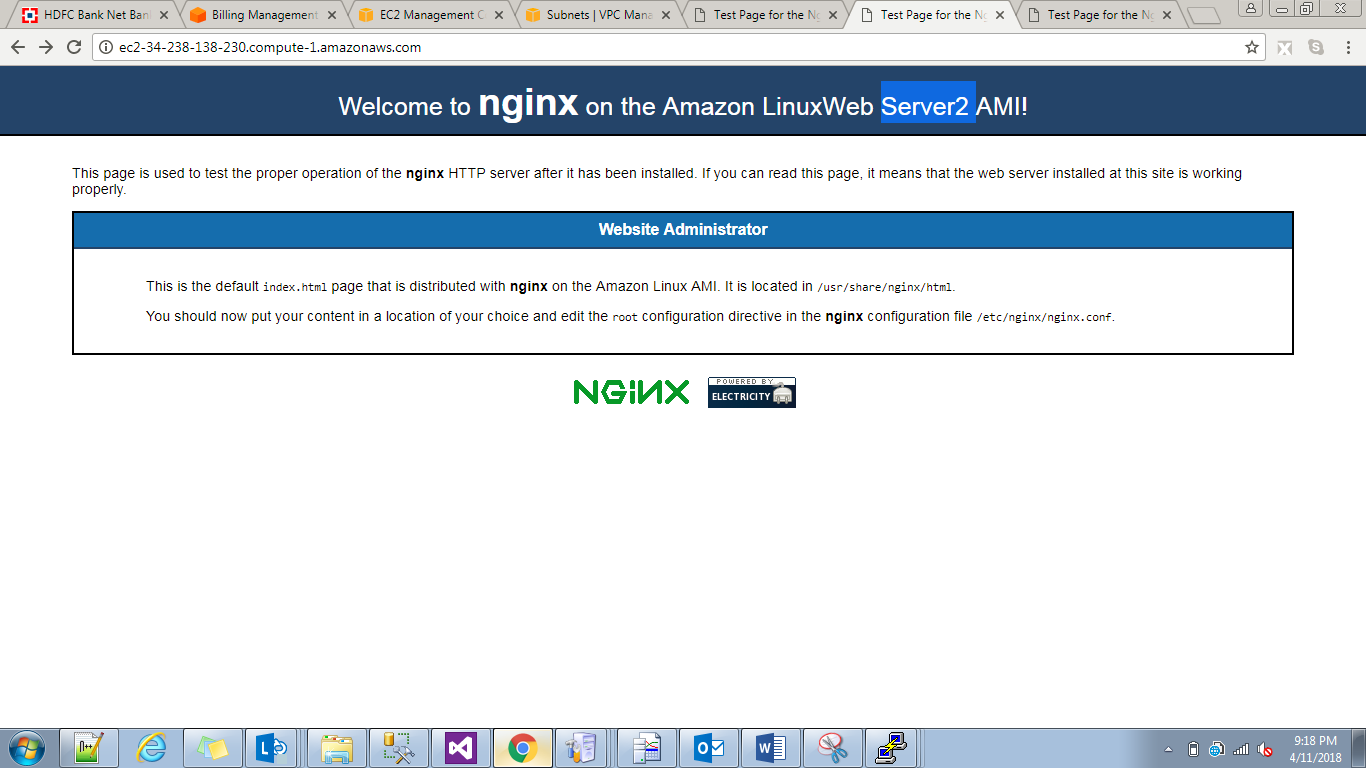
service nginx start

and after this I browsed with public ip I got nginx server.

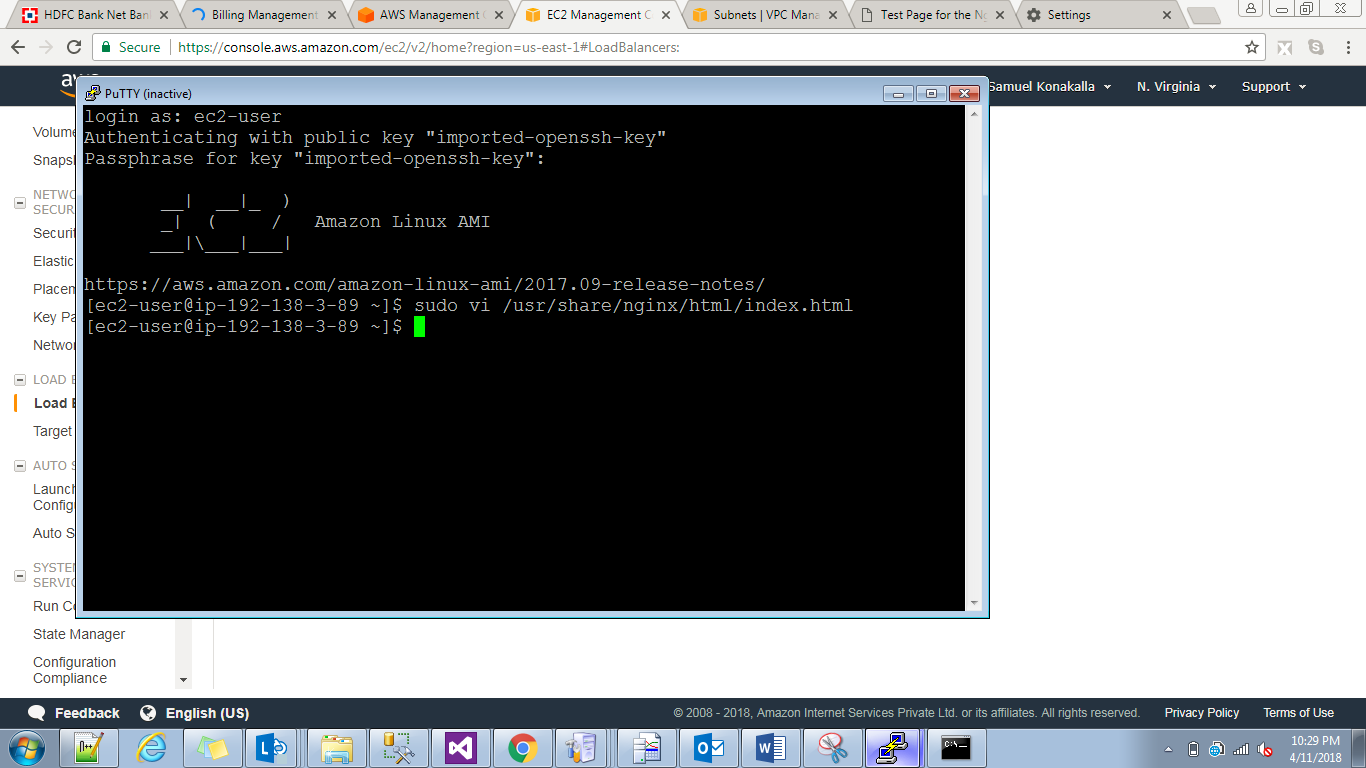


In web server1 in /usr/share/nginx/html/index.html ,I updated main heading to web server-1.

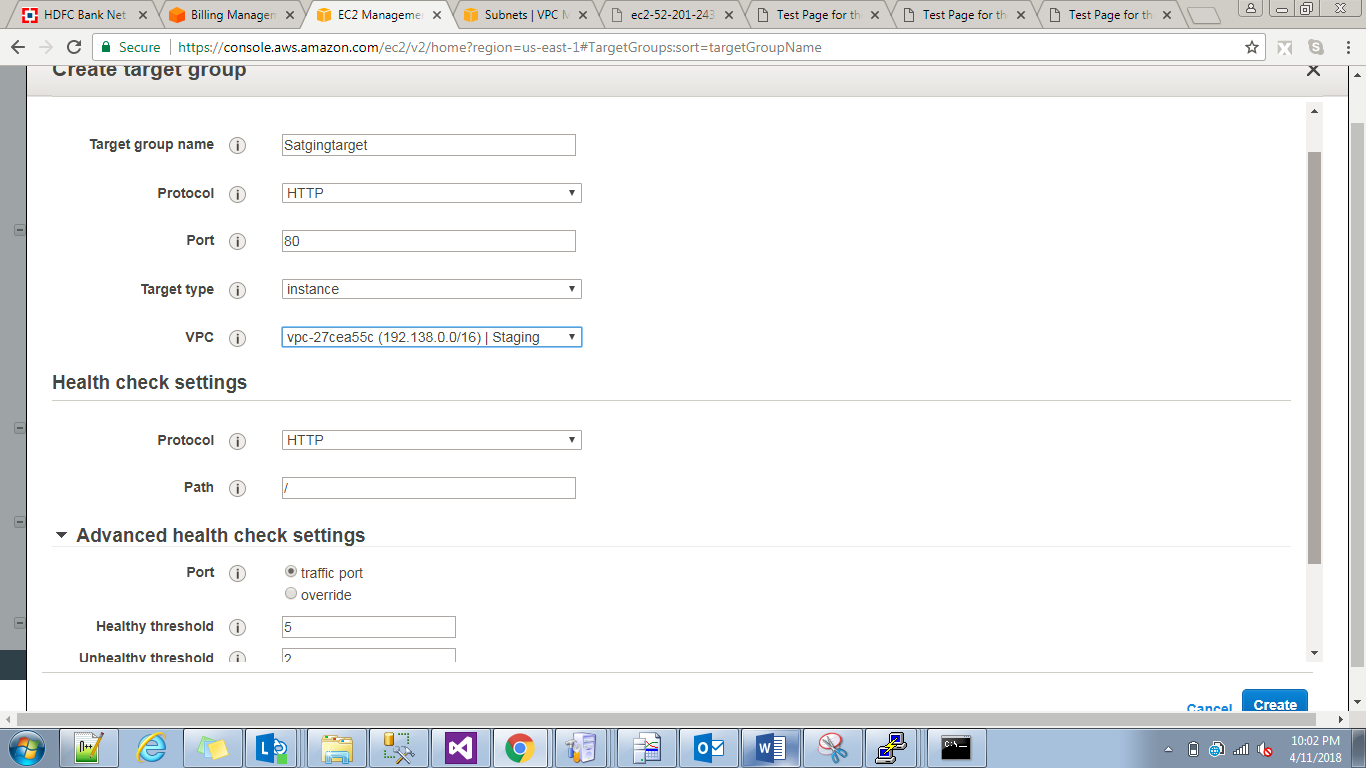


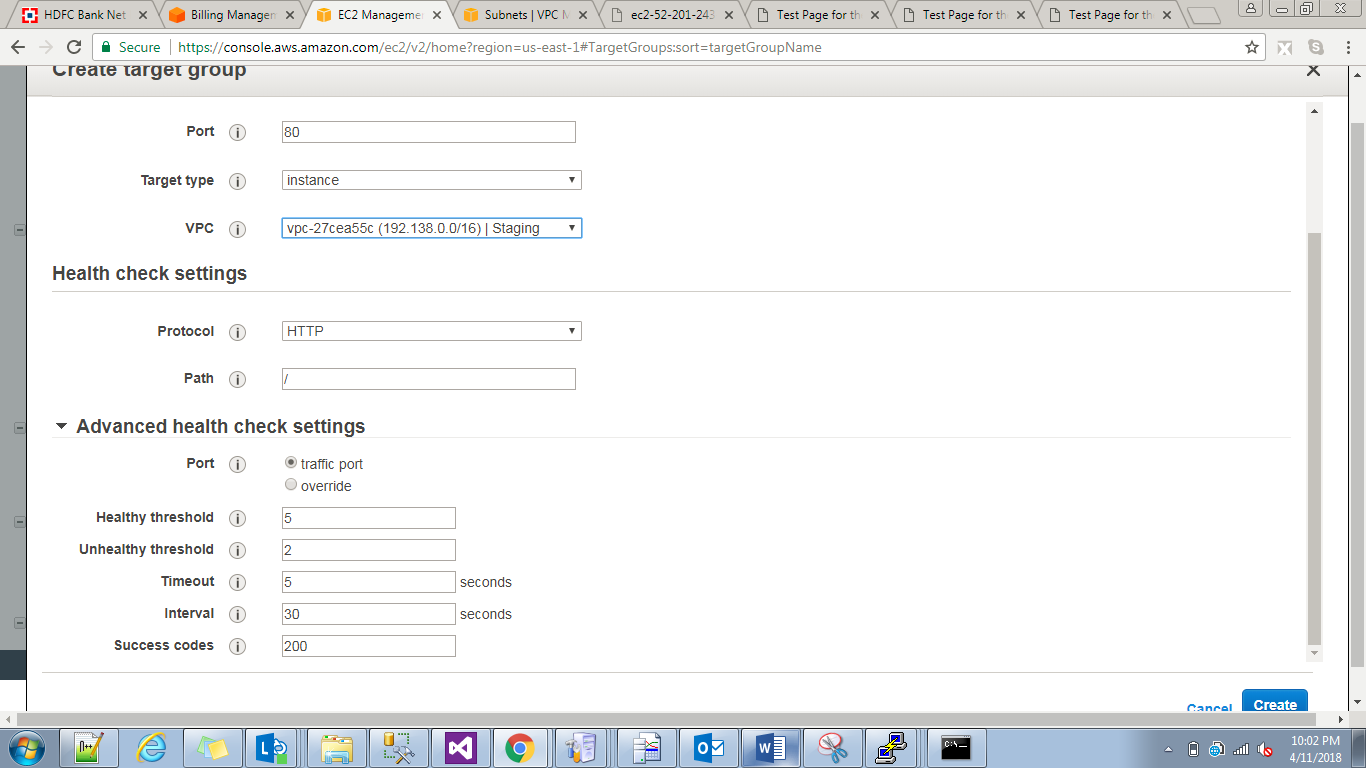
Web server2: web server3:

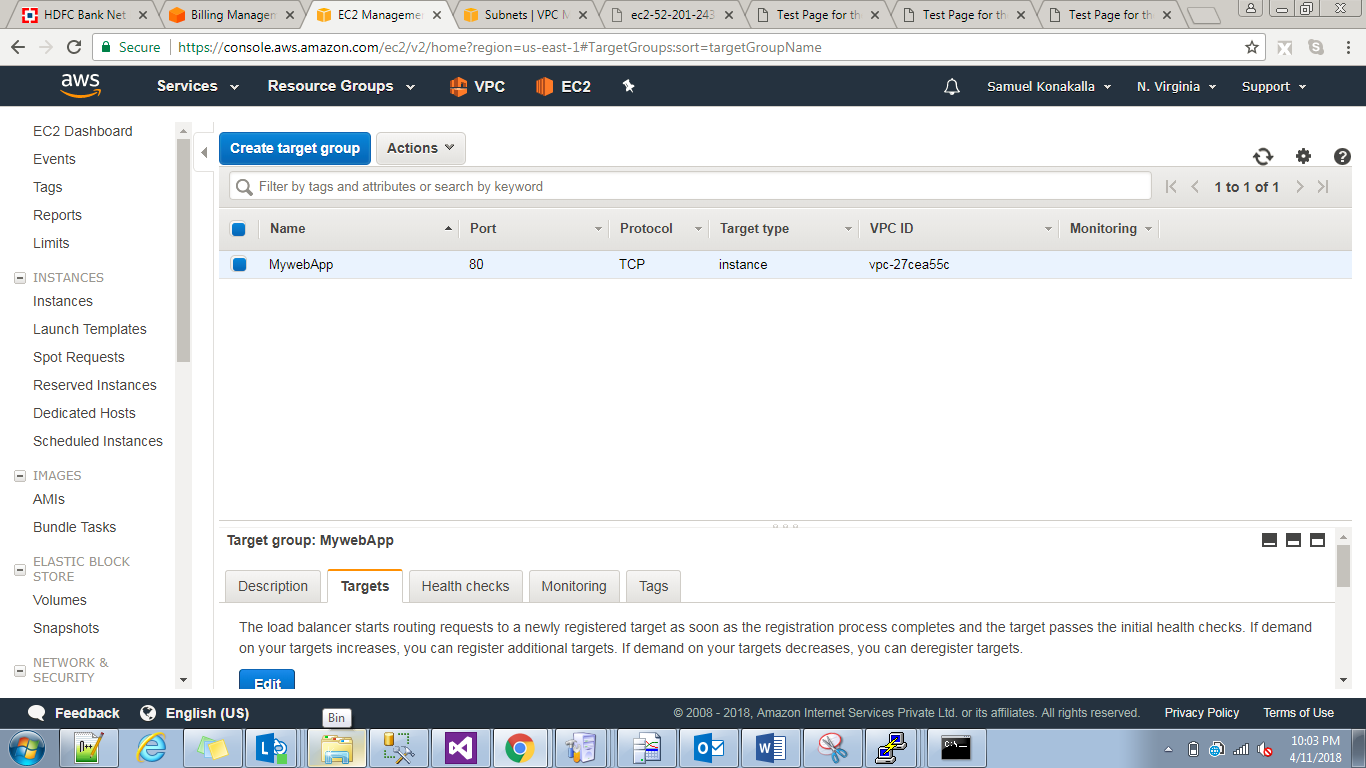


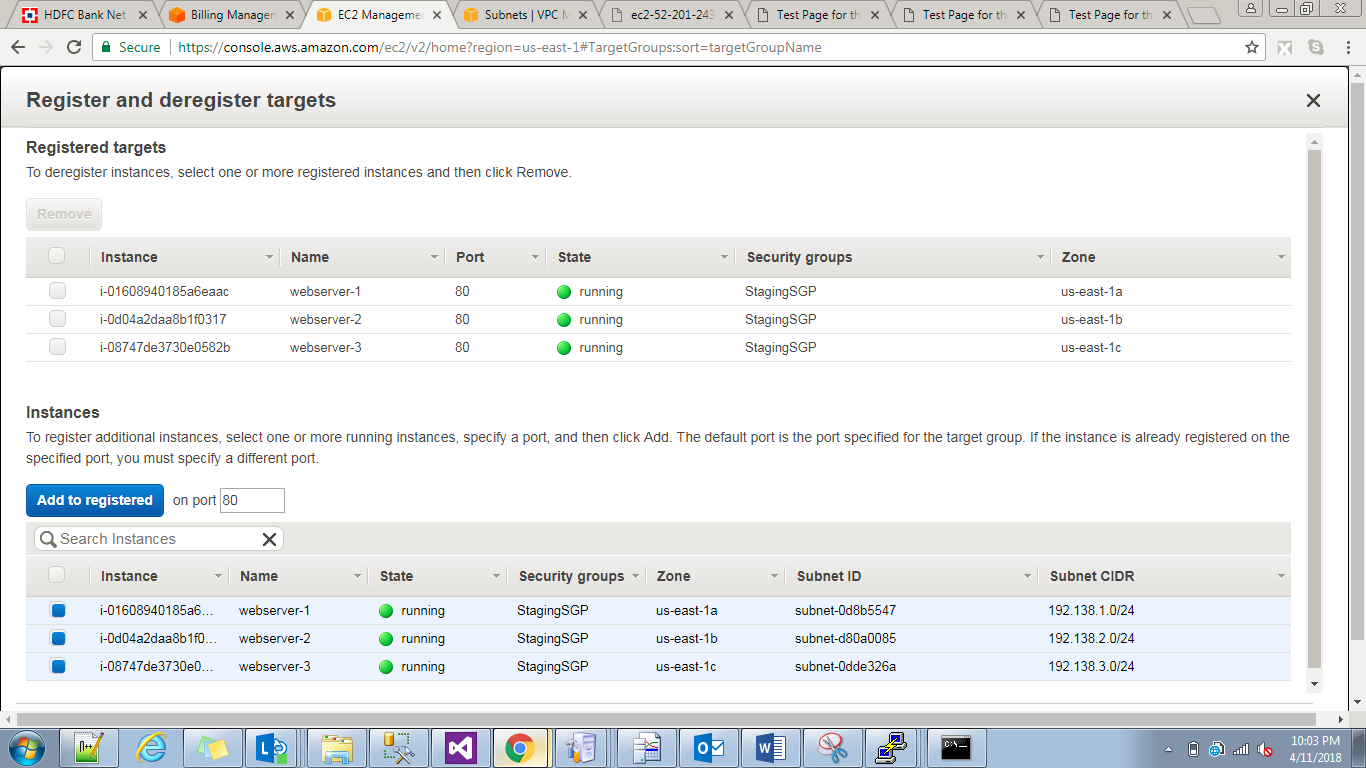


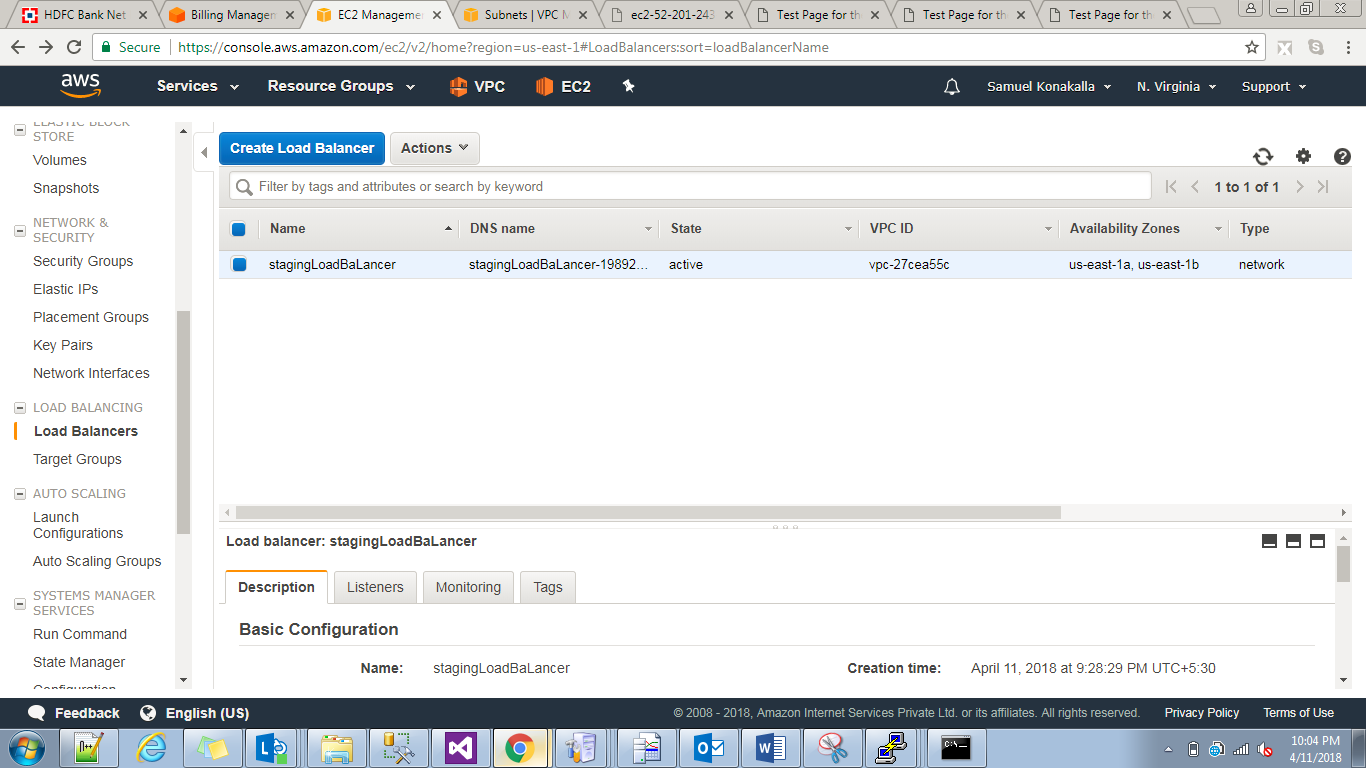
Configure a target group and add (to whom u have to load balance).

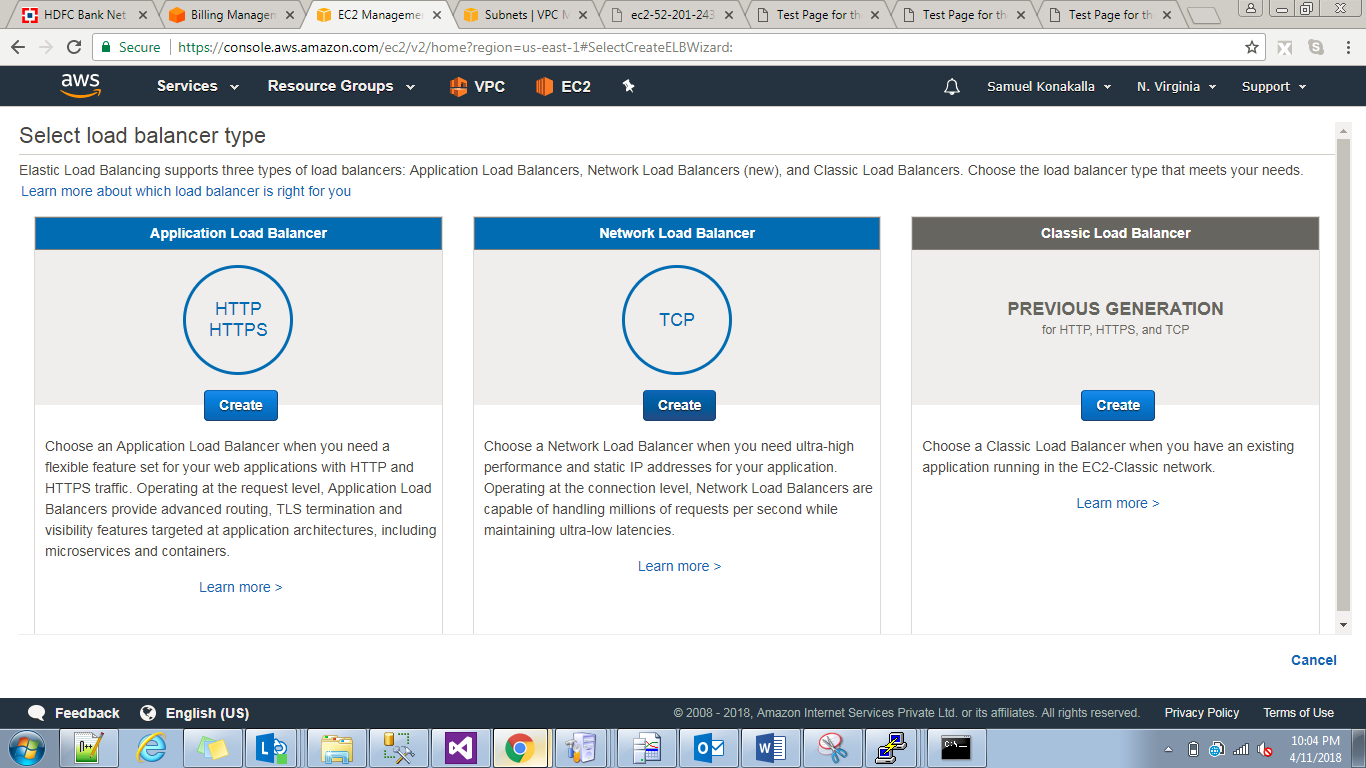




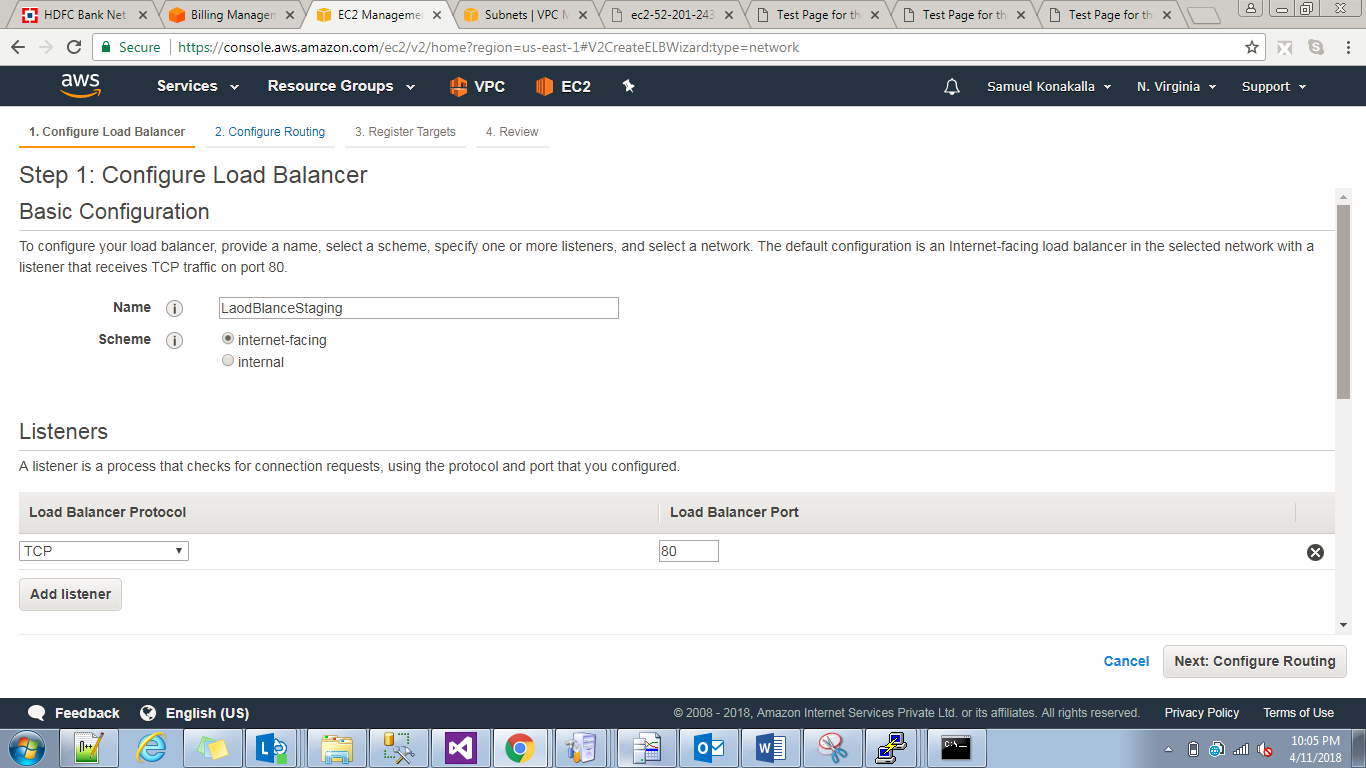


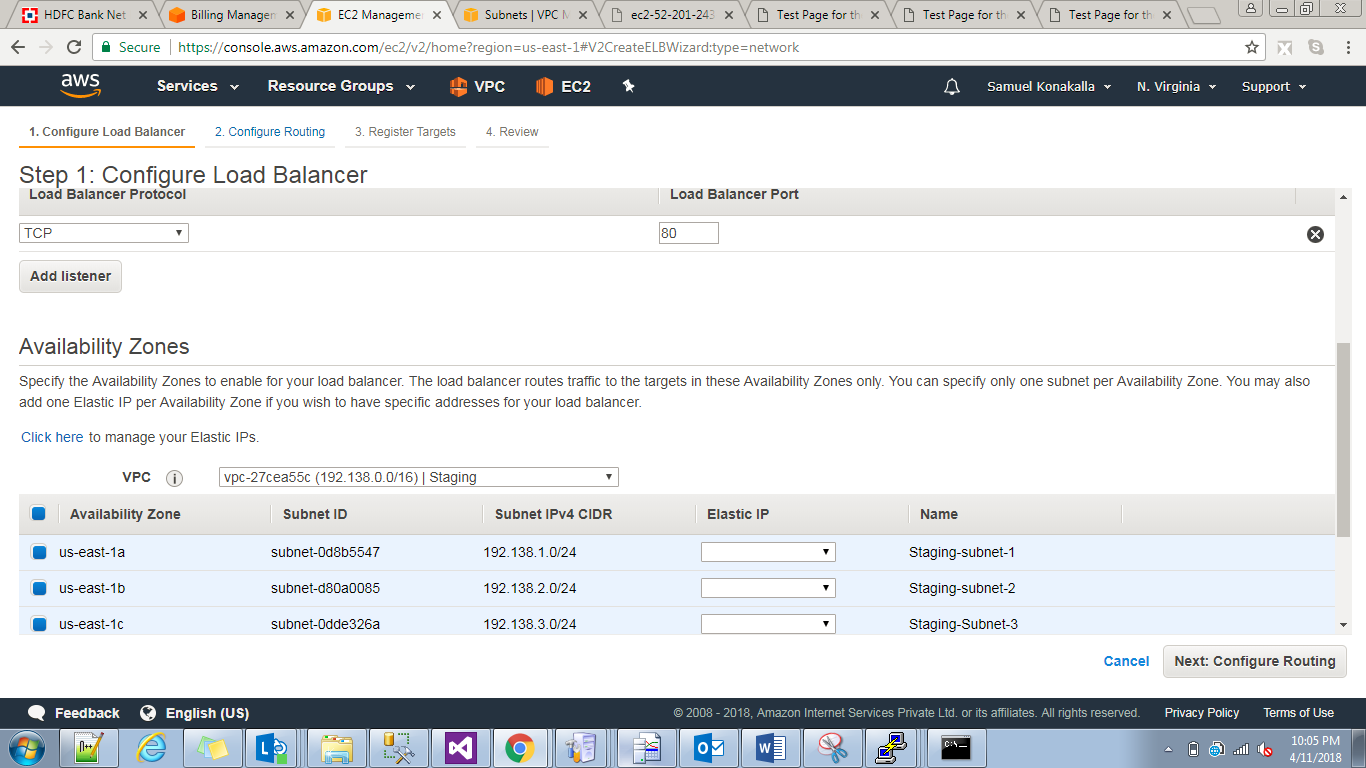




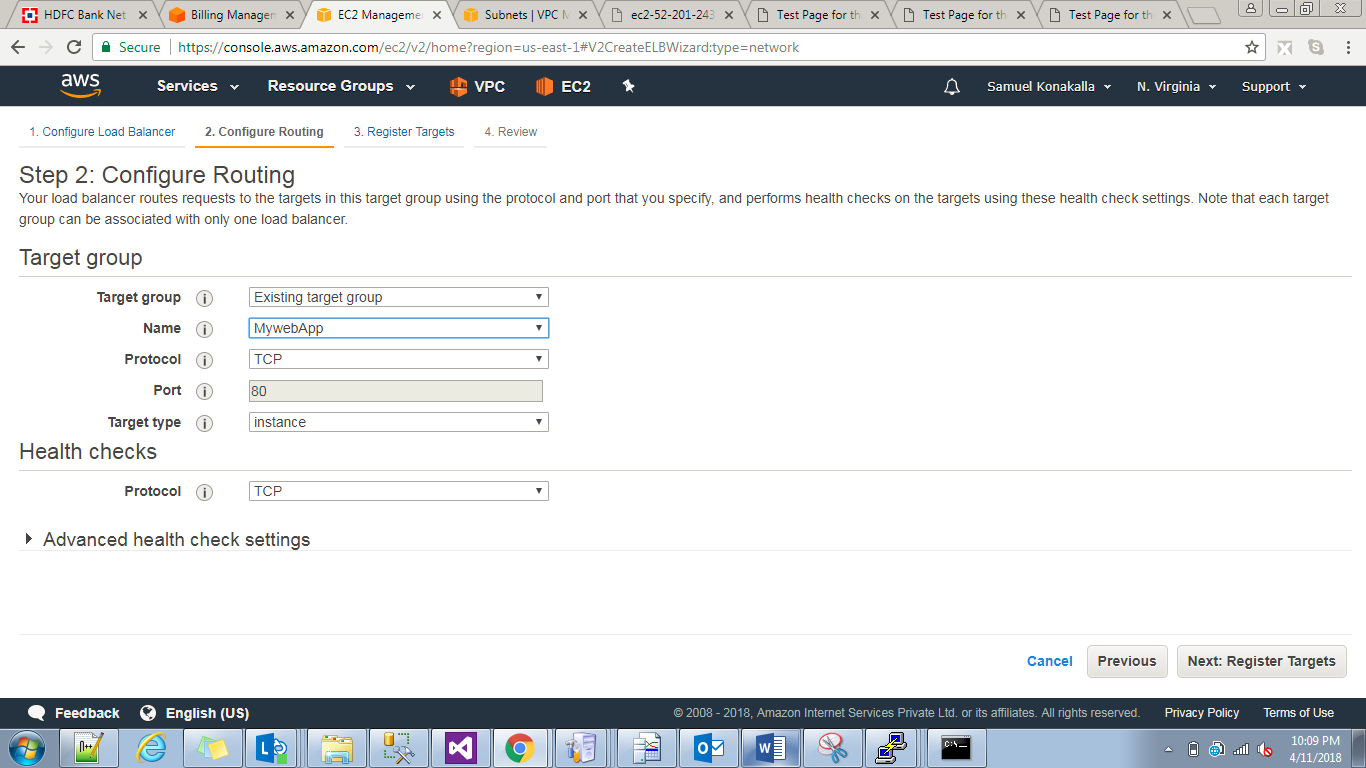


n/w load balancer.

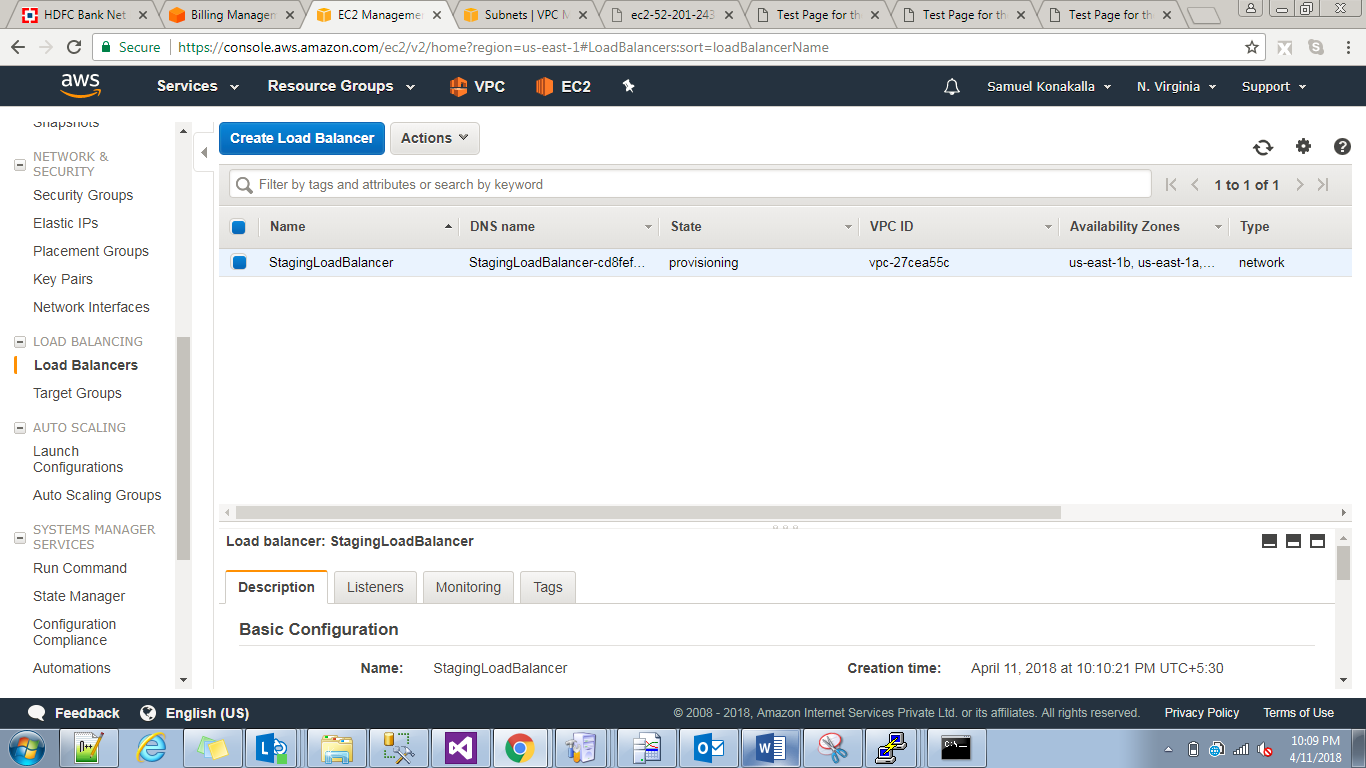




In network load balancer we should add all subnet,in target group we selected before or later but in network load balancer once we are not selected we cant add later.



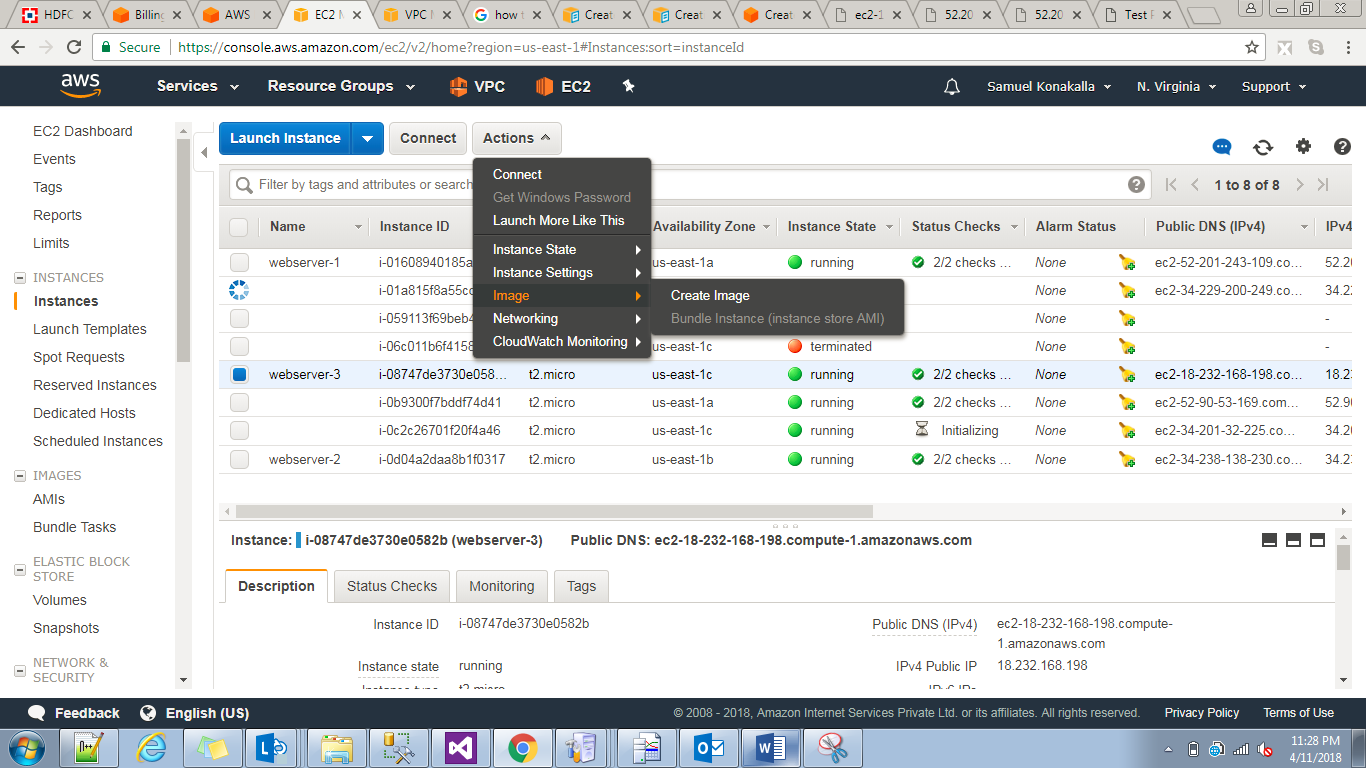
Review and launch.

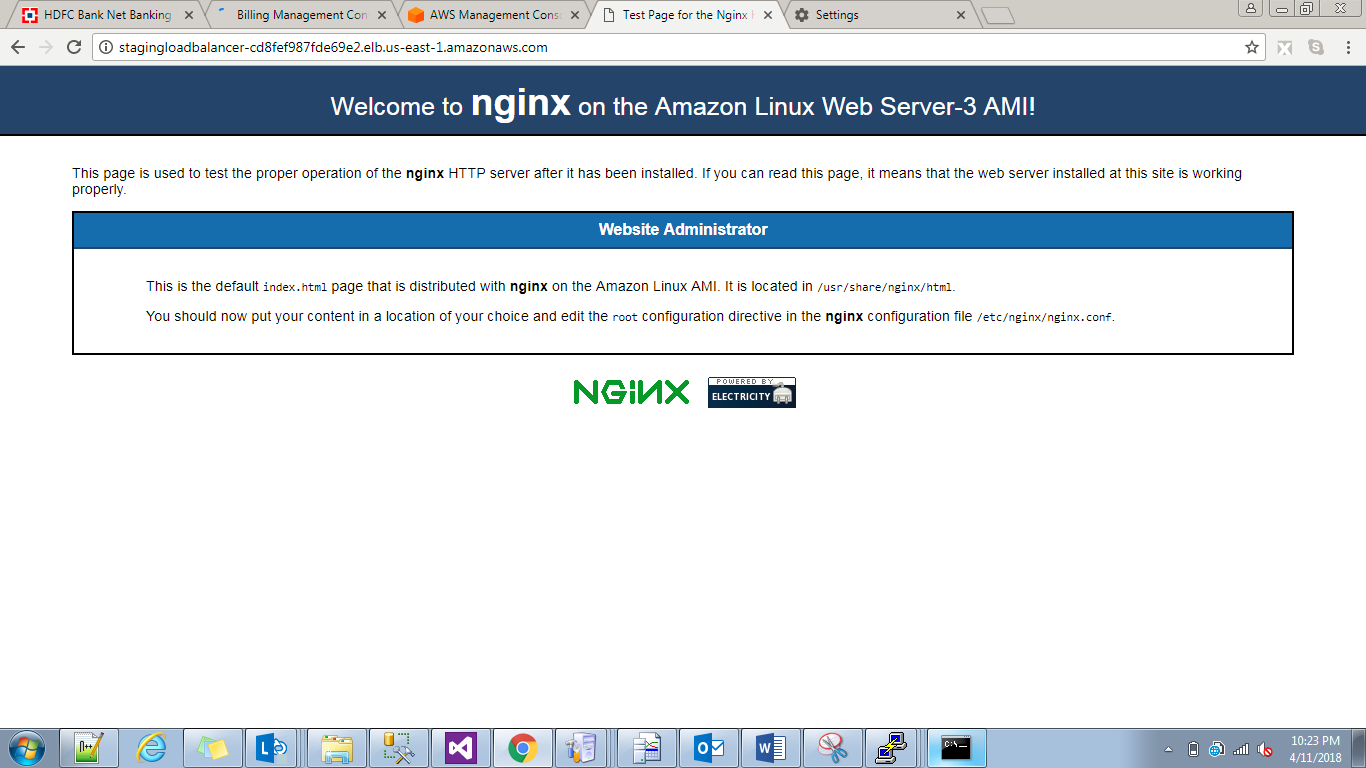


After that we have to take Load balancer dns name and paste into browser we will get web servers html page.now if we check in different system the request will goto different web servers.so,this is the way the laod will be balanced.in this we can check suppose if we go to partuclar instance and we stop nginx service now requests will not goto that server.

In auto scaling if we delete a instances automatically the samount of numbers will be generated.

Creating an EC2 AMI:go to instances in EC2.select an EC2 instance->Actions🡪image🡪Create Image.





The above one is dns url.