VPC

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. You can configure your VPC; you can select its IP address range, create subnets, and configure route tables, network gateways, and security setting.

Subnet is a range of IP addresses in your VPC. You can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the Internet, and a private subnet for resources that won't be connected to the Internet.

Private Subnet: A private subnet sets that route to a NAT instance. Private subnet instances only need a private IP and internet traffic is routed through the NAT in the public subnet. You could also have no route to 0.0.0.0/0 to make it a truly private subnet with no internet access in or out.

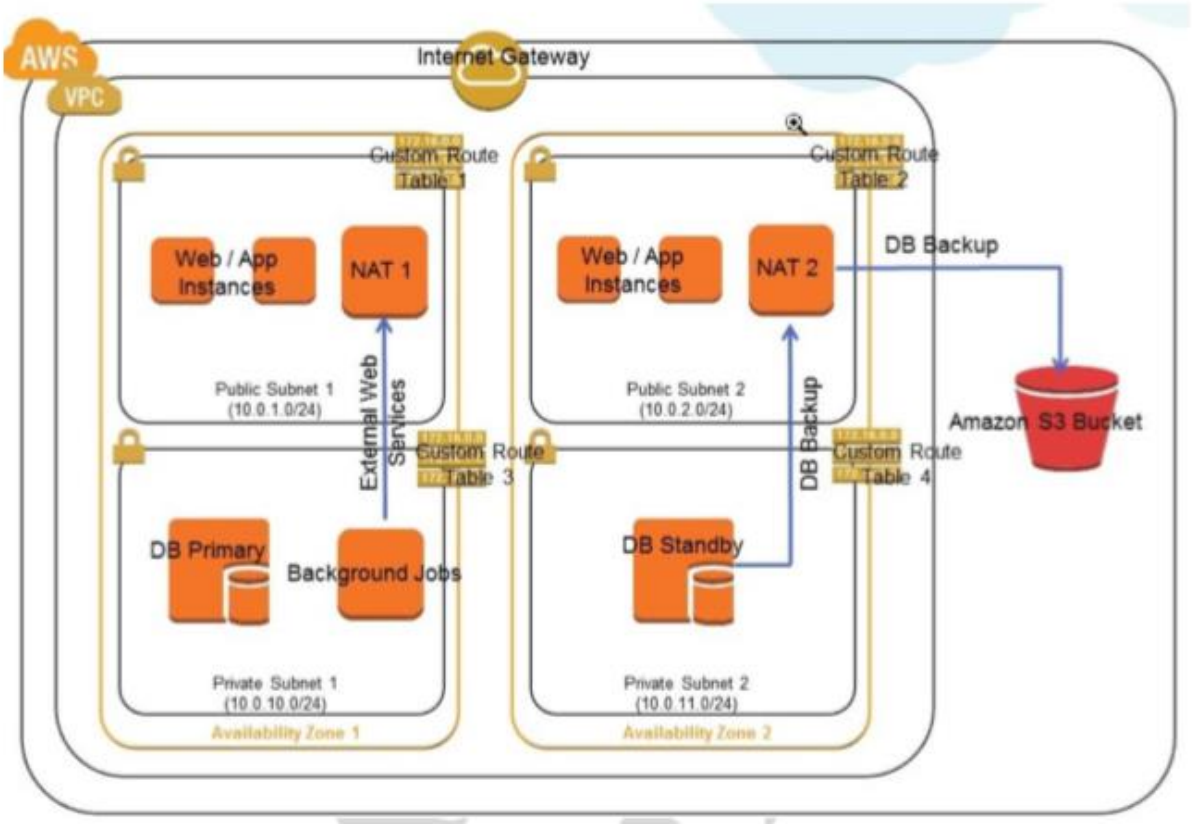
Public Subnet: A public subnet routes 0.0.0.0/0 through an Internet Gateway (igw). Instances in a public subnet require public IPs to talk to the internet.

Network Address Translation (**NAT**) **gateway** is used to enable instances in a private subnet to connect to the Internet or other AWS services, but prevent the Internet from initiating a connection with those instances.

An **Internet Gateway** is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic. An Internet gateway serves two purposes: to provide a target in your VPC route tables for Internetroutable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses. An Internet gateway supports IPv4 and IPv6 traffic.

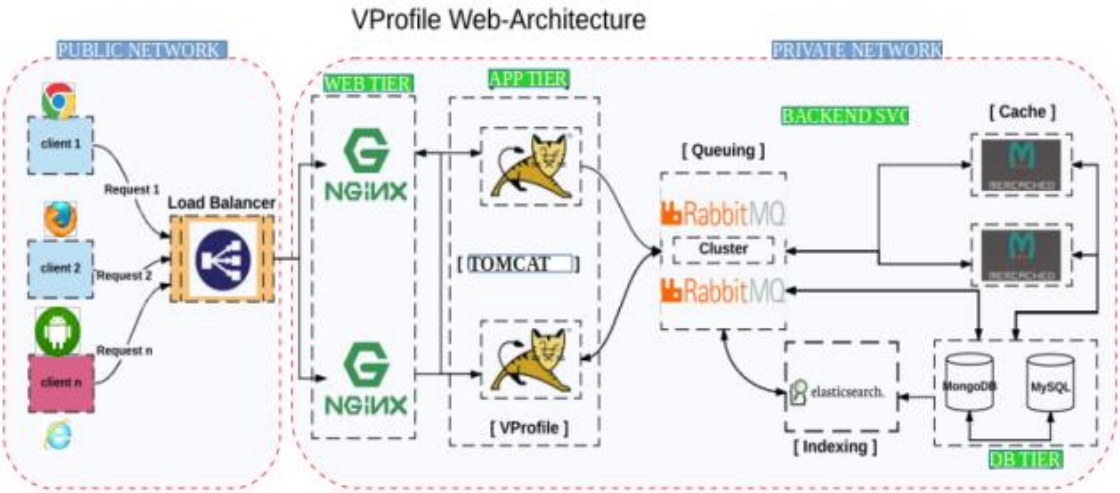
A **Route Table** contains a set of rules, called routes that are used to determine where network traffic is directed. Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.

Creating Highly Available VPC



Highly available VPC spans over multiple zones. Even if one zone goes down our services spanned over the other zone will be still serving the user traffic. If you see from above diagram we have web, DB and backend services in two zones. While creating Ec2 instance we can decide now on which subnet our instance to create. So, for example we will create web01 in one subnet (located in zone 1a) and web02(located in zone 1b) in other subnet. So, if zone 1a goes down we still have web02 serving user traffic from zone 1b.

We are going to create HA VPC manually and not with the wizard.



Creating Highly Available VPC by Document :

VPC Network Address : 172.20.0.0/16

VPC Name -- Vprofile

Region : N.California

Zones : us-west-1a, us-west-1b

Sunets:

Public subnets

vprofile-pub-1 172.20.1.0/24 us-west-1a

vprofile-pub-2 172.20.2.0/24 us-west-1b

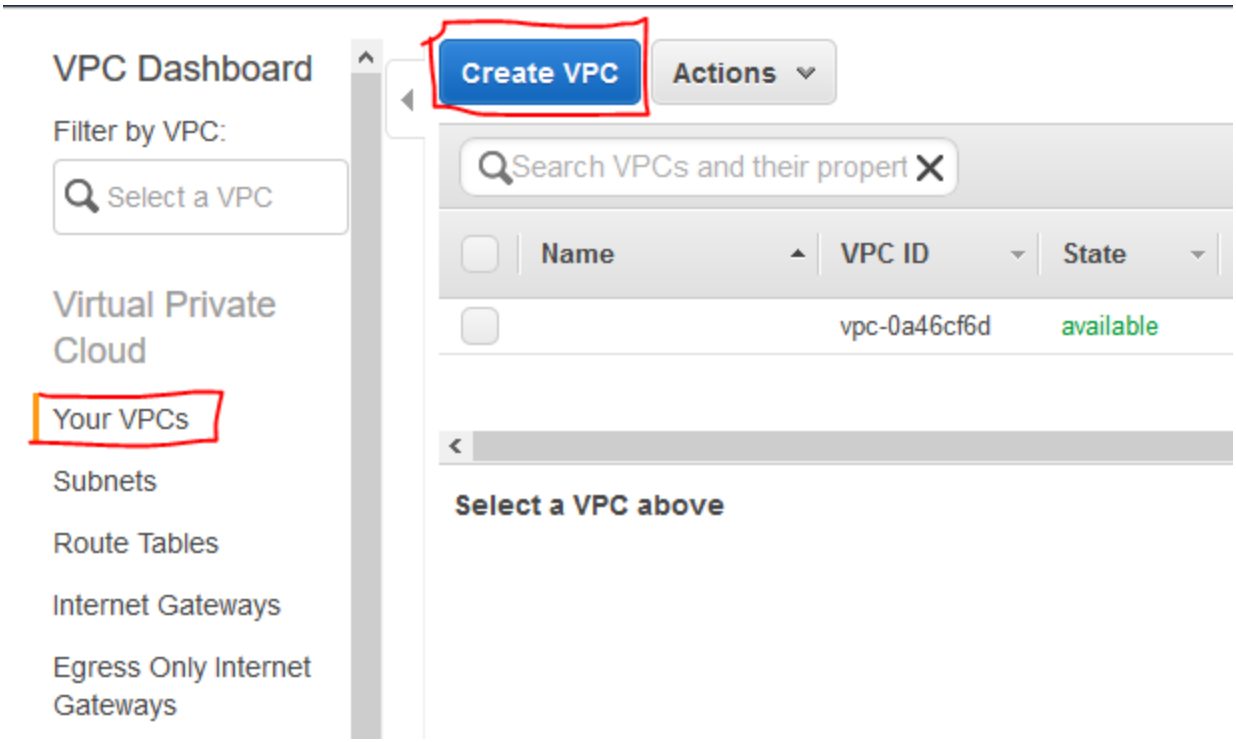
Private subnets

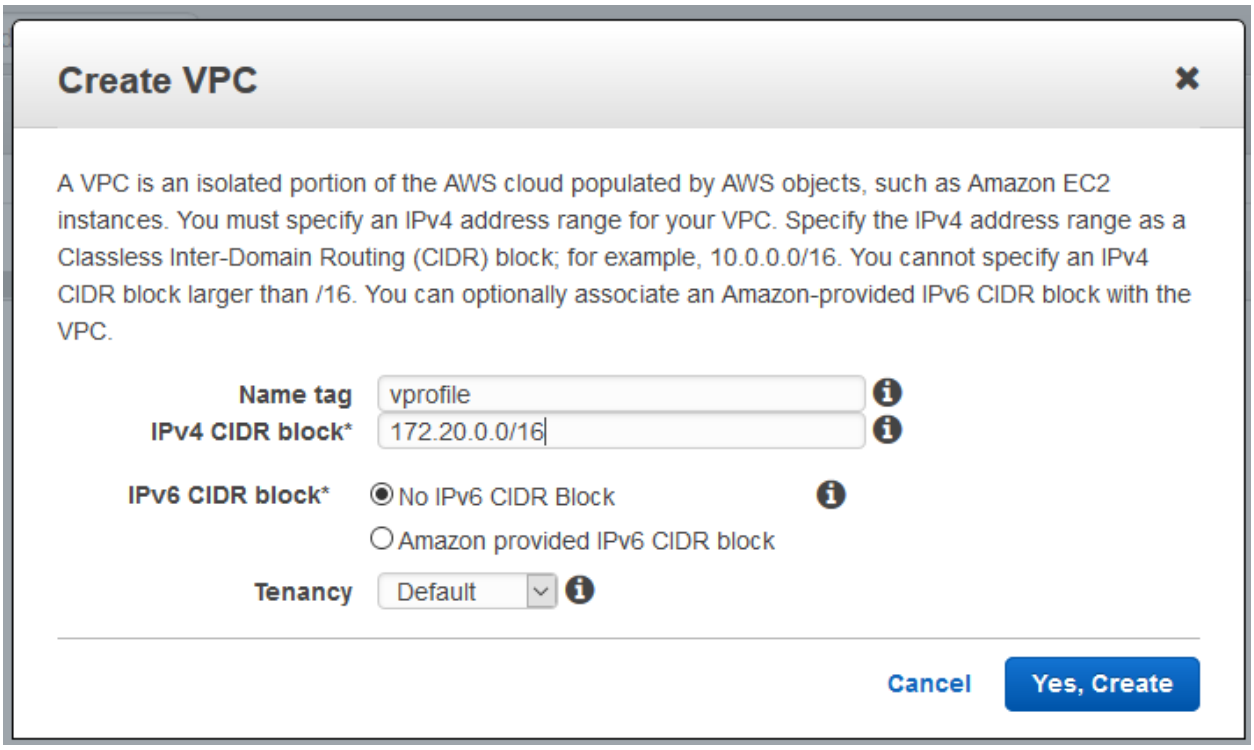
vprofile-priv-1 172.20.3.0/24 us-west-1a

vprofile-priv-2 172.20.4.0/24 us-west-1b

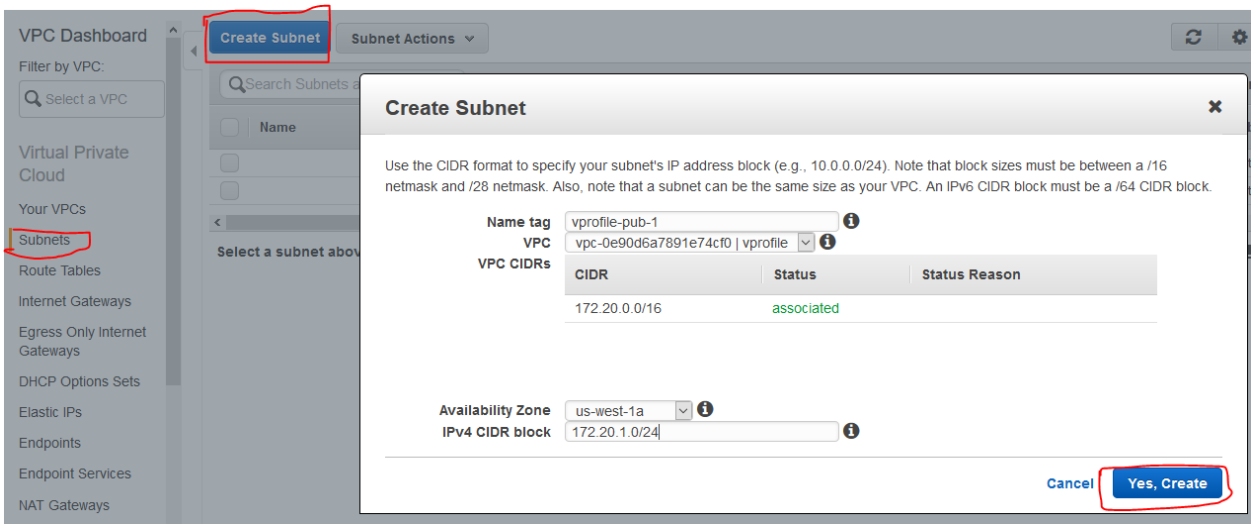
Now

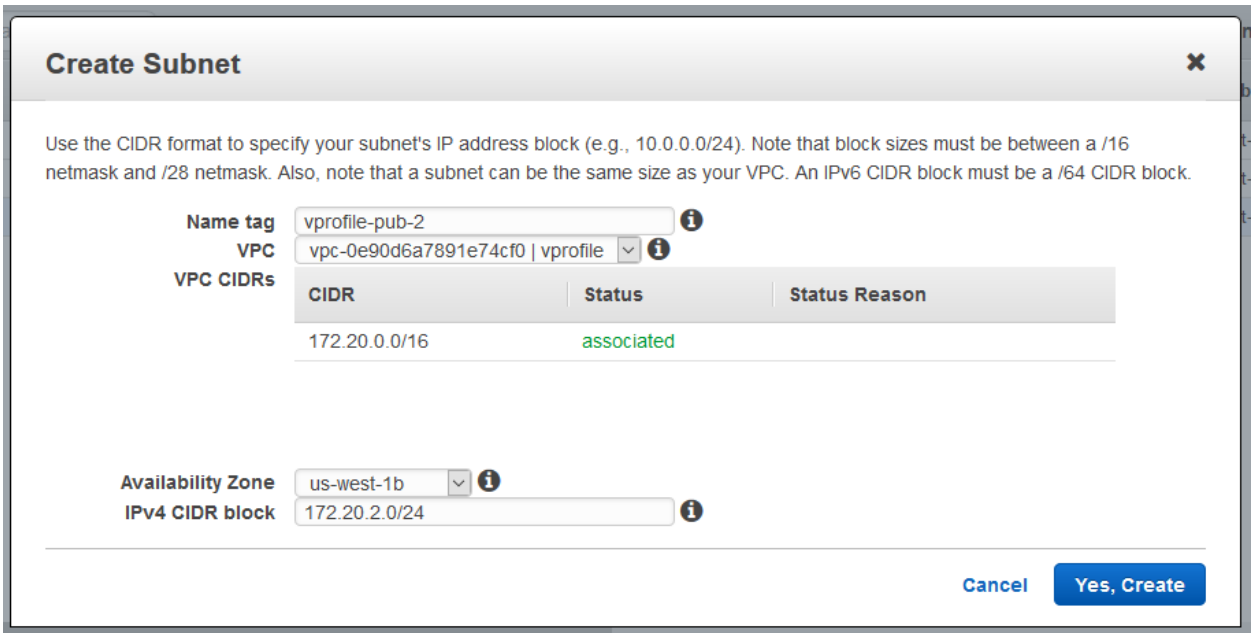
Create VPC.


VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
Create VPC
Actions
Search VPCs and their propert
Name
VPC ID
State
vpc-0a46cf6d
available
Select a VPC above


Create VPC
A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.
Name tag
vprofile
IPv4 CIDR block*
172.20.0.0/16
IPv6 CIDR block*
No IPv6 CIDR Block
Amazon provided IPv6 CIDR block
Tenancy
Default
Cancel
Yes, Create

Create 4 subnets (2 are public and 2 private subnets for getting high availablitiy)

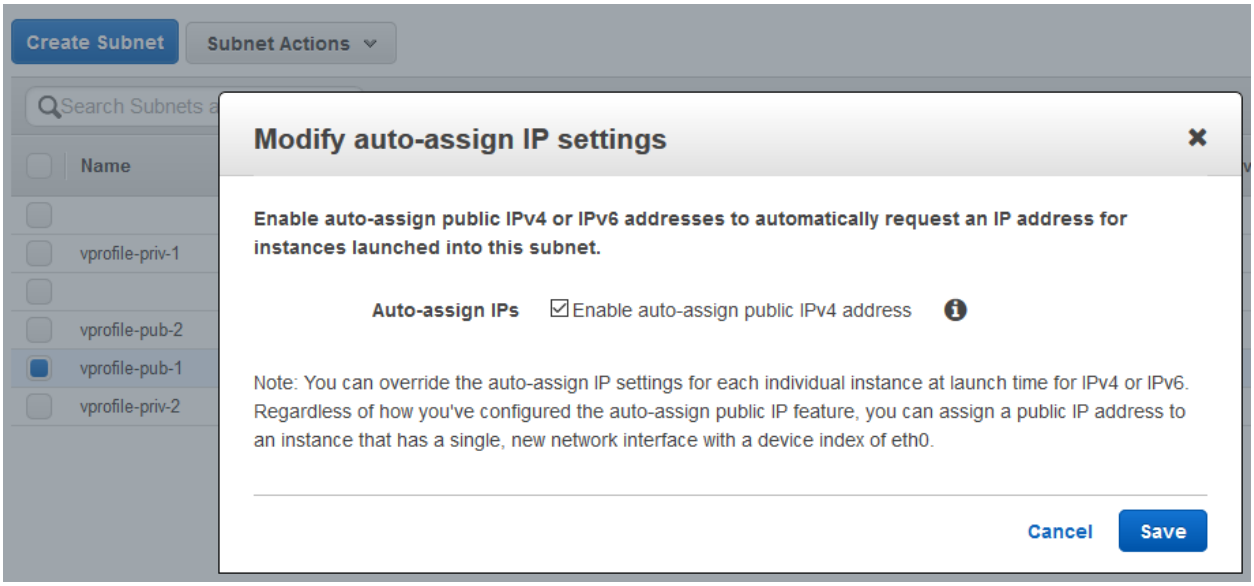


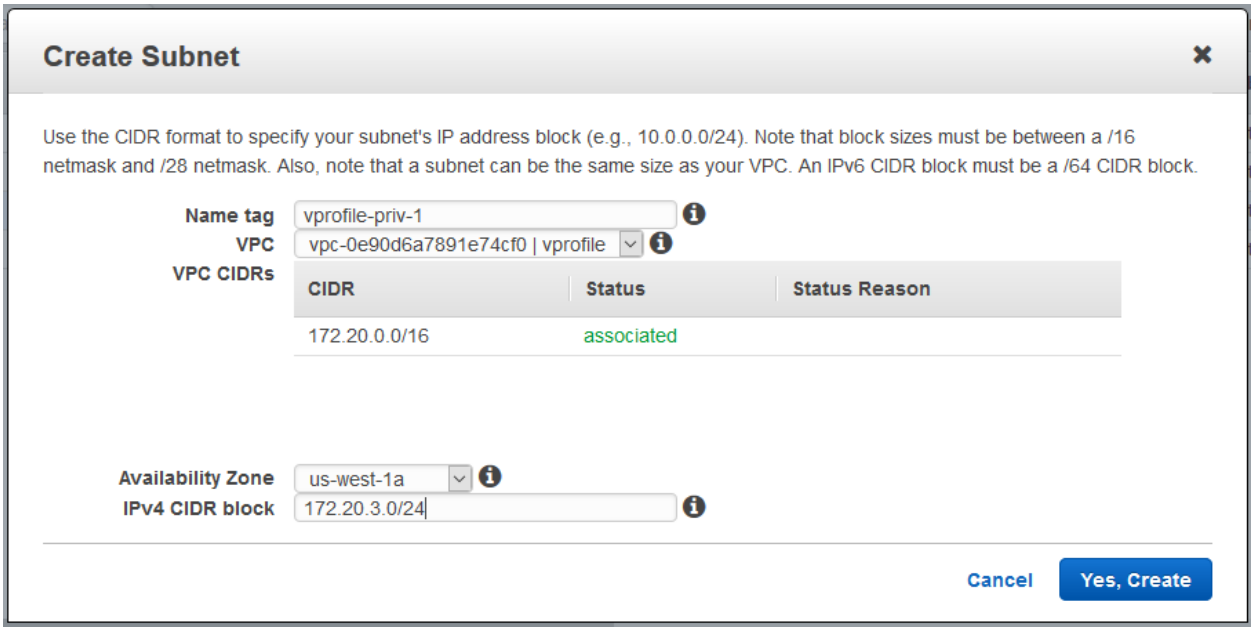


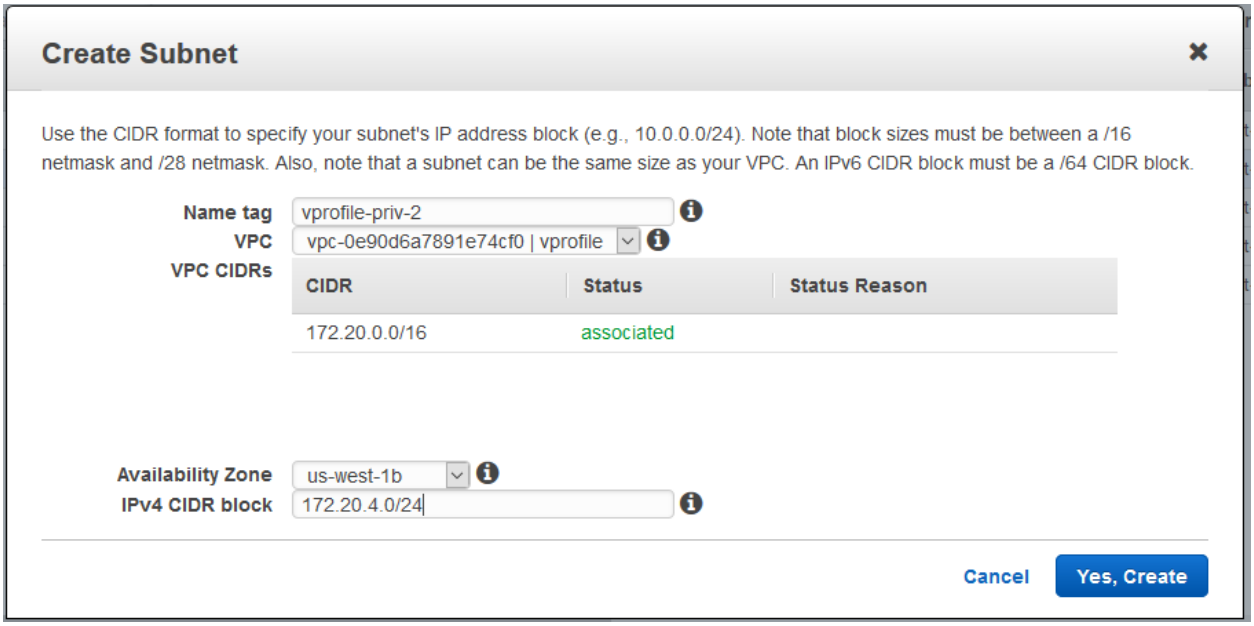
For Public subnets if we want to create public IP from our own VPC we have to enable one option here.

Select public subnet and click on subnet actions and select Modify auto assign IP settings

And check Enable auto assign public IPv4 address and click in save

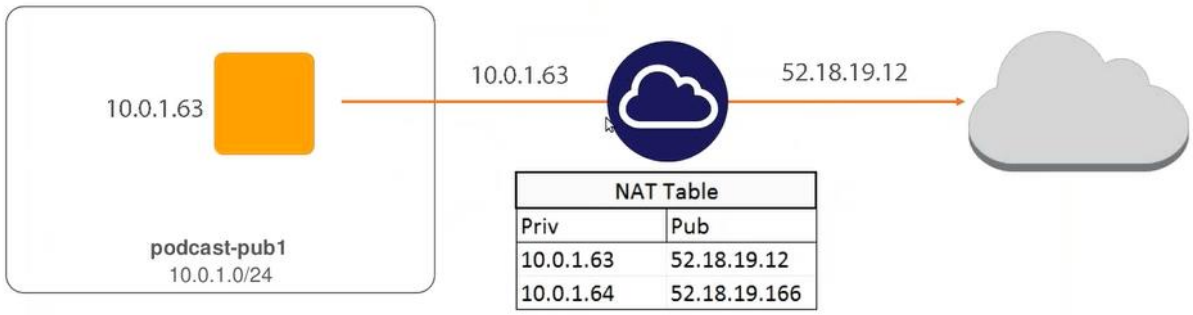

Create Subnet
Subnet Actions
Search Subnets a
Name
vprofile-priv-1
vprofile-pub-2
vprofile-pub-1
vprofile-priv-2
Modify auto-assign IP settings
Enable auto-assign public IPv4 or IPv6 addresses to automatically request an IP address for instances launched into this subnet.
Auto-assign IPs
Enable auto-assign public IPv4 address
Note: You can override the auto-assign IP settings for each individual instance at launch time for IPv4 or IPv6. Regardless of how you've configured the auto-assign public IP feature, you can assign a public IP address to an instance that has a single, new network interface with a device index of eth0.
Cancel
Save


Create Subnet
Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.
Name tag
vprofile-priv-1
VPC
vpc-0e90d6a7891e74cf0 | vprofile
VPC CIDRs
CIDR
Status
Status Reason
172.20.0.0/16
associated
Availability Zone
us-west-1a
IPv4 CIDR block
172.20.3.0/24
Cancel
Yes, Create



Now we have 4 subnets got created in that 2 public and 2 private distributed properly 2 different zones.

Now Public subnets means there is nothing public about public yet. What it will make it as a public, it is going to be an Internet Gateway.



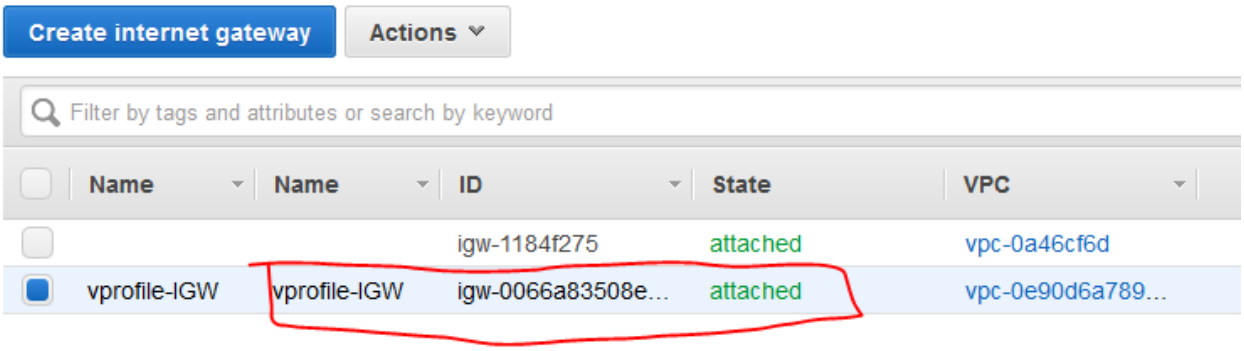
Internet Gateway is going to connect subnet to the internet and vice versa. And this internet gateway is maintain a table where your instances gets private ip will come from a subnet so here private ip will match with public ip, when we create EC2 instance it gets public ip.

So when you dialing the public ip of instance it will hit the internet gateway , Internet gateway wil have a table here and it will look for private ip of public ip then traffic will route the right instance. Like that internet gateway is going to maintain a table there.

All EC2 instances wil have private and public ips those Ips are going to be added into Internat gateway table.

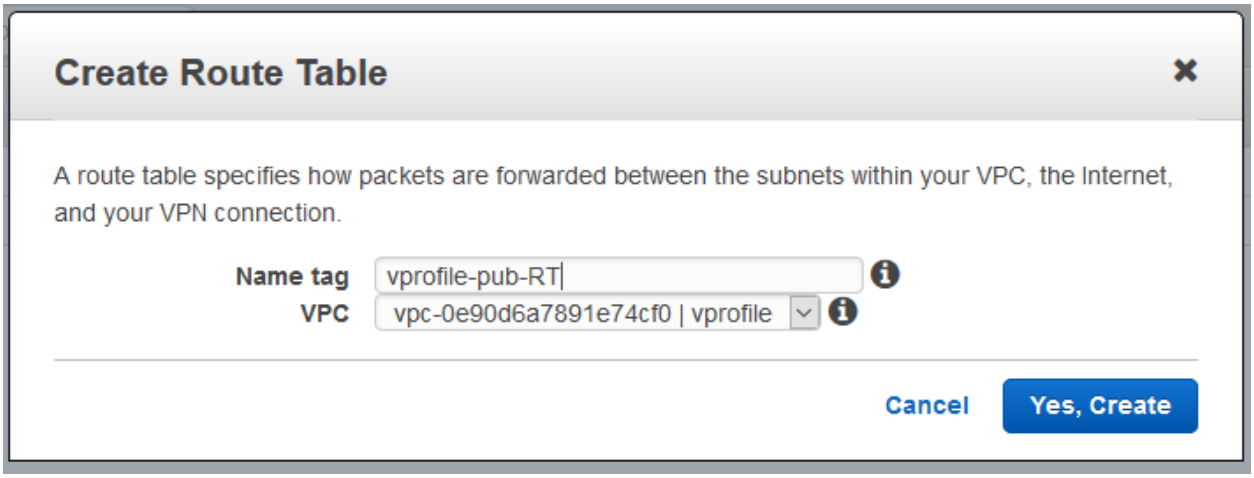
Now we have to create internet gateway and needs to be attach to Public subnet.

We have to attach to VPC once got created

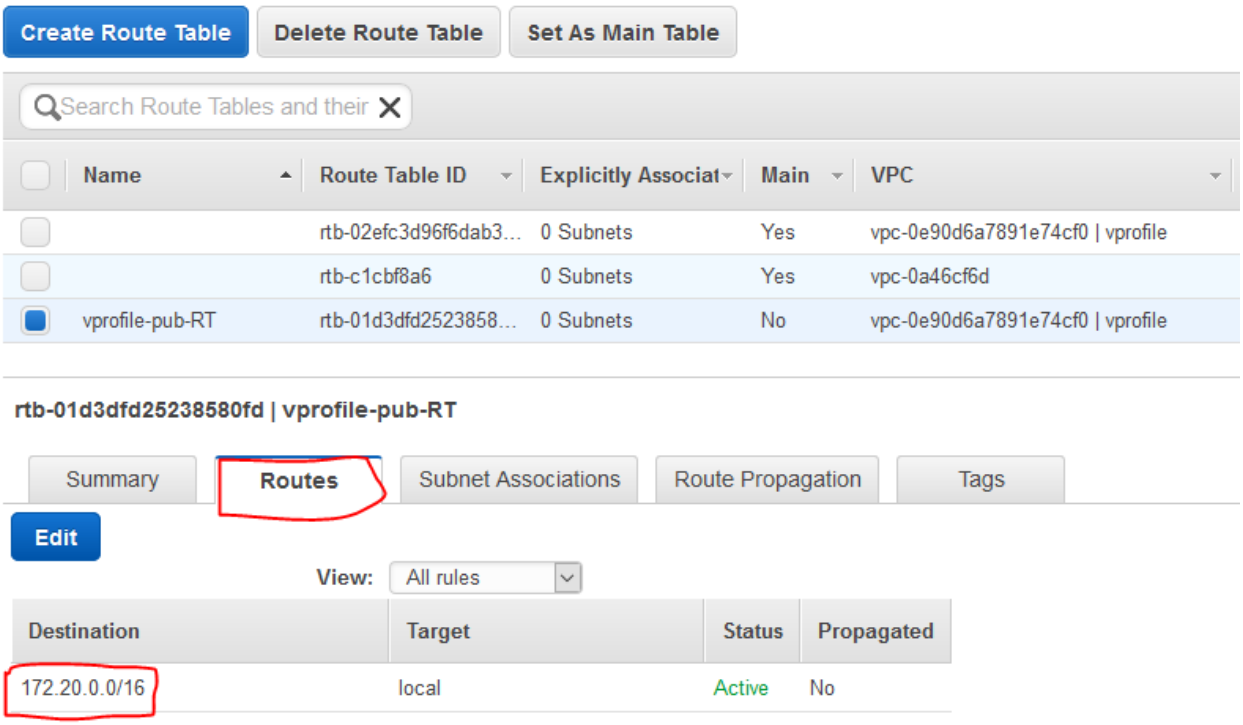


Now we just attached to VPC but we have not attached to public subnet.

To attach to our public subnet we have to create a route table. There wil be automatically route table wil get created. But we are not going to use that and creating 2 route tables now.

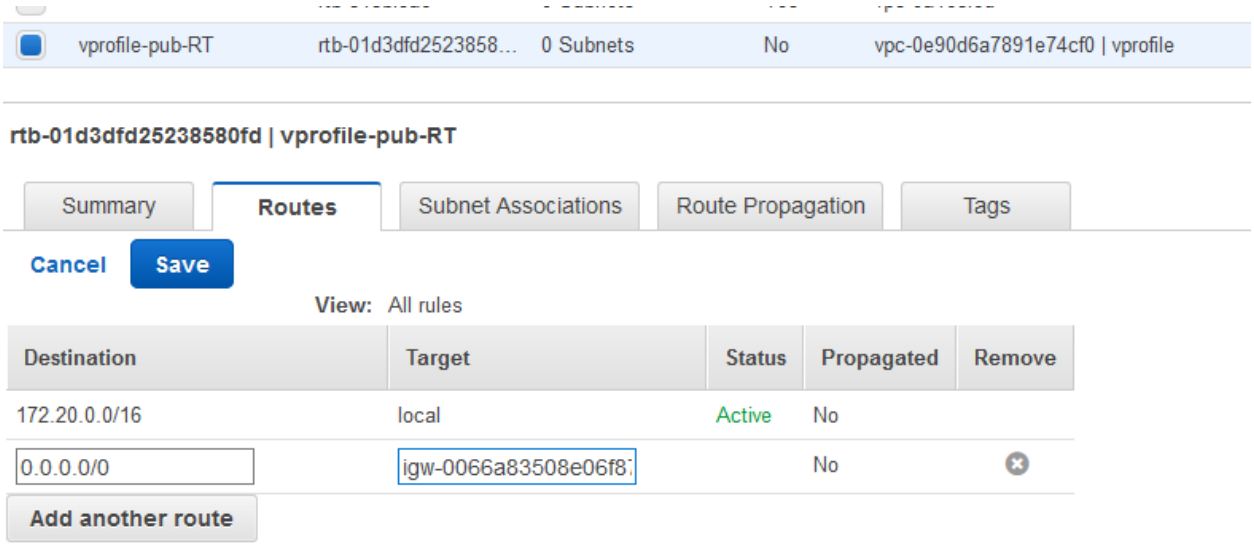


Now come to our Route Table entry.



Here there is one entry default which is destination that is all explaining about private network ip any ec2 instance contacting any ip address with in range it will redirect to local ec2 services. Other than that example if you want to download any package from outside that time we have to enable internet to that ec2 service. So I just created new row for contacting network gateway which I created now for all systeams like below.

0.0.0.0/0 means * in Unix system like all.



If first rule doesnot match it will go to other rule that rule says that go to the internet gateway.

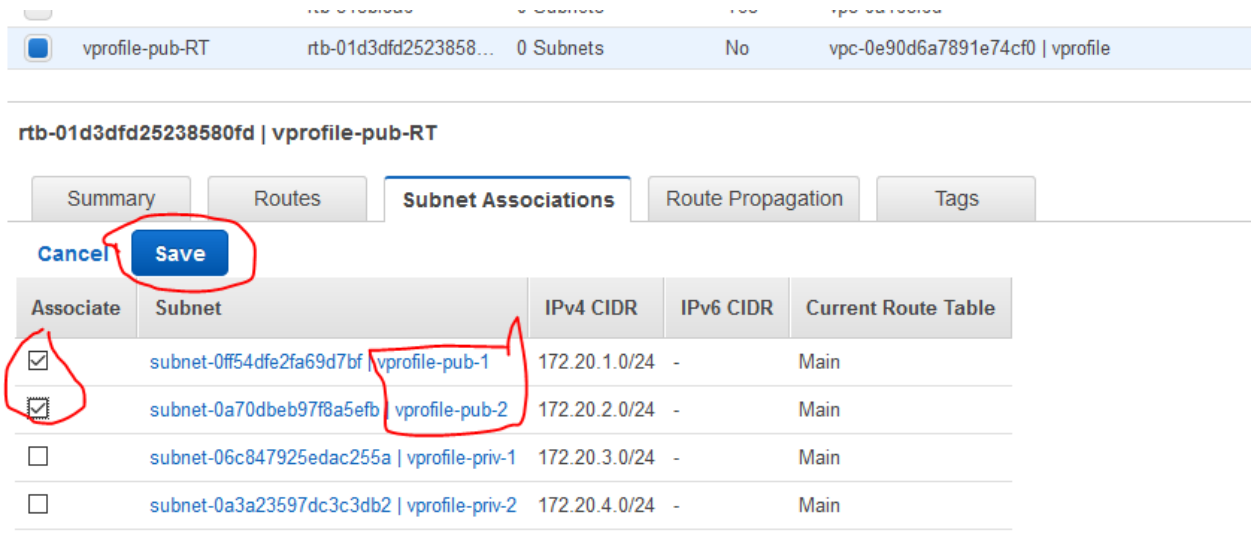
And Save

Next we are going to attach to subnet.

Go to Subnet Association tab

And edit

Attach subnet there like below screen shot,



Now we have set up 2 sub nets successfully now we can attach ec2 instances to these subnets while creating ec2 instances.

Now we are going to set up for private subnet here if you want to connect internet we have to create NAT gateway. So create NAT gateway now.

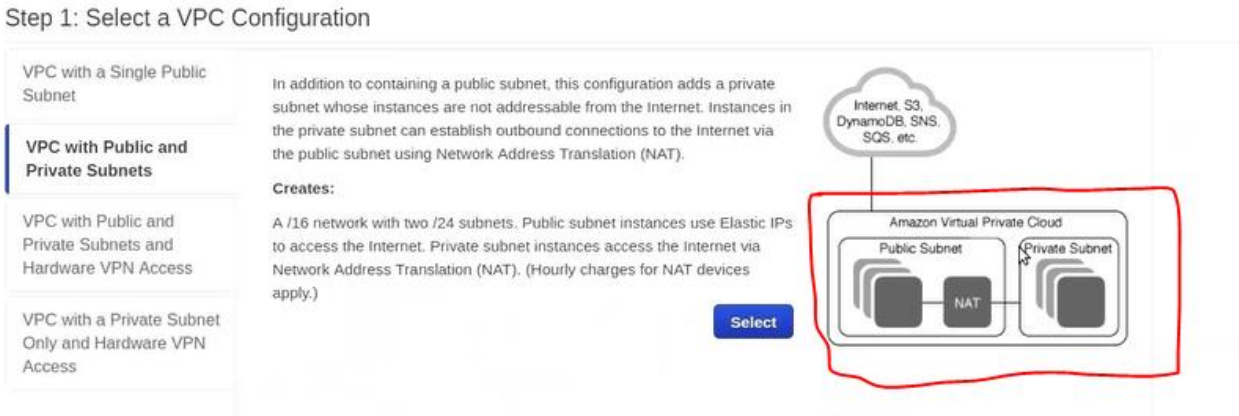
NAT gateway is not free it needs Elastic IP and NAT gateway should be in the public network.

NAT gateway will route the traffic to internet from the instance to the internet, from the private network NAT gateway should be available in public network.

Where do lives your NAT gateway (IQ)

NAT gateway will stay in public subnet and it search in private subnet.

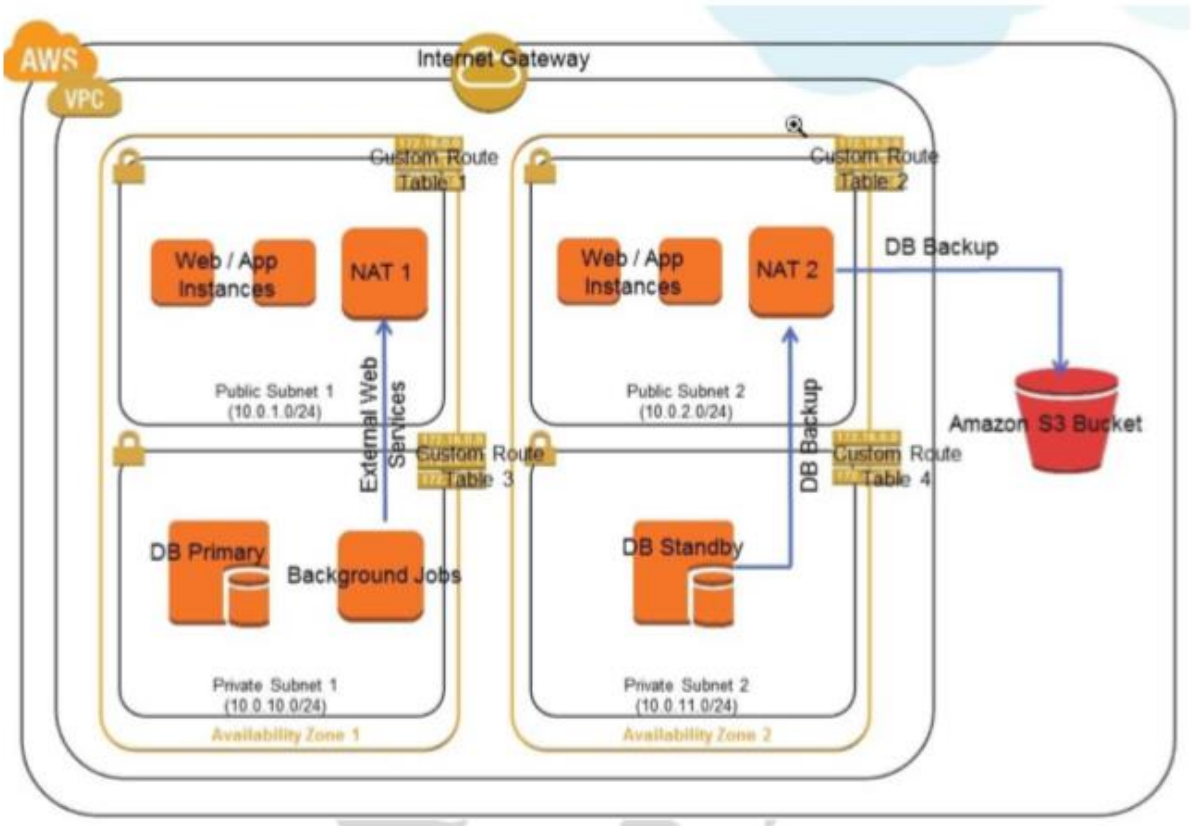
The below diagram will explain better.

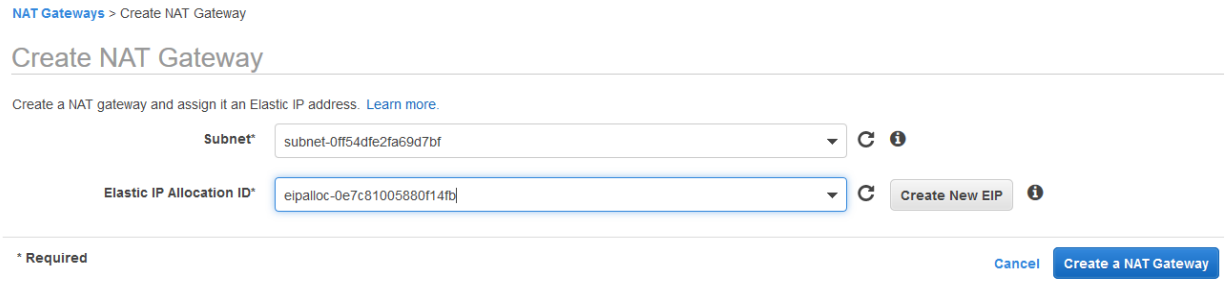


Diff between Public and private subnet : (IQ)

Public subnet is directly connected to the internet gateway and you can access public sunet from the outside network. Private subnet is directly connected to the NAT gateway but it can t be access to the outside world but instances in the private network can access internet through NAT gateway.

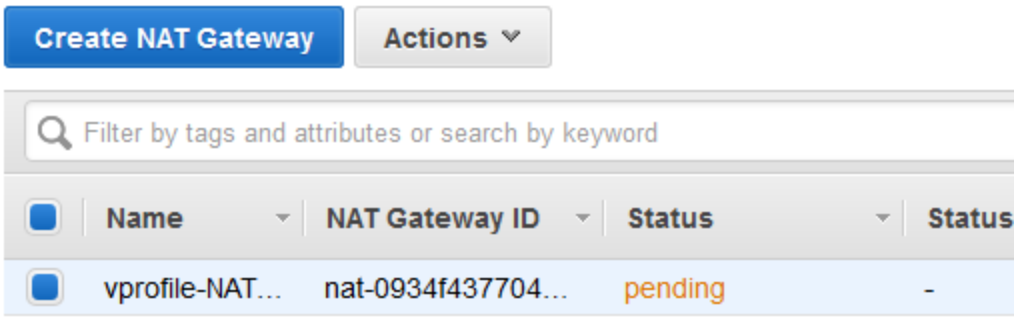
For High availability zones here also we have to create 2 NAT gateways since one zone gets down means NAT gateway also gets down so for 2 public subnets need 2 NAT gateways.



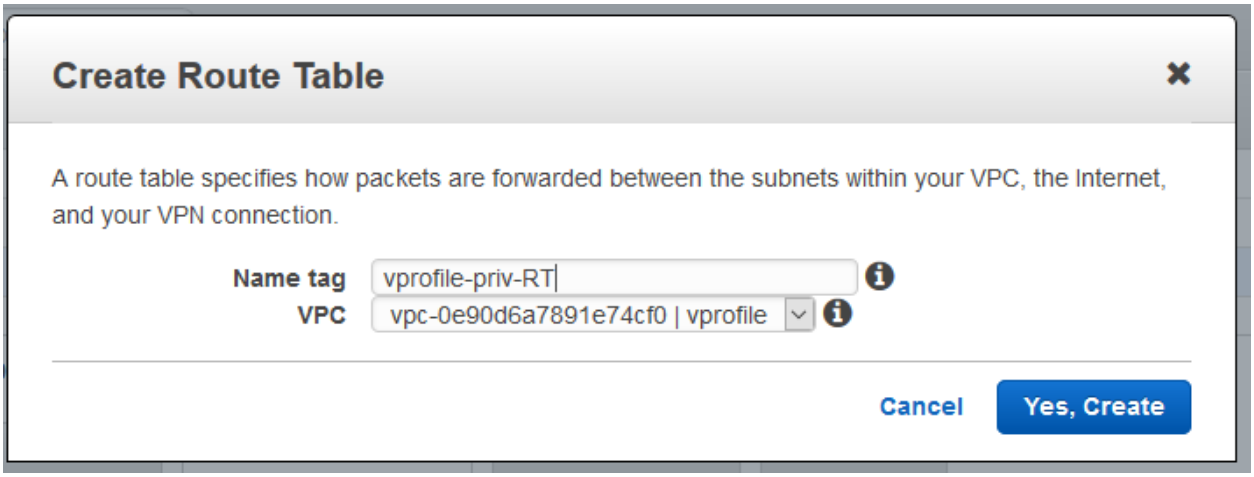


We have to select pub-1 subnet here for NAT gatway-1.

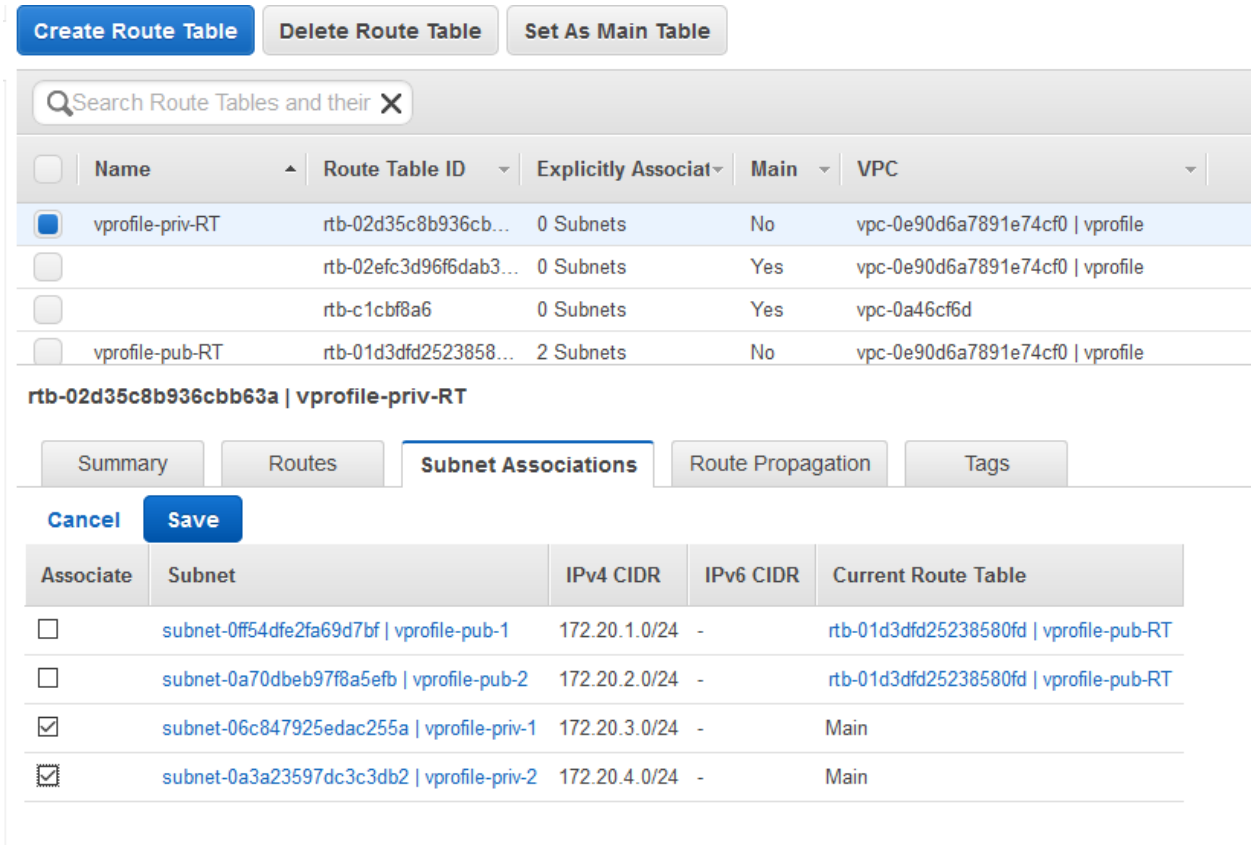
It wil take some time to create mean you just name of it like bloew



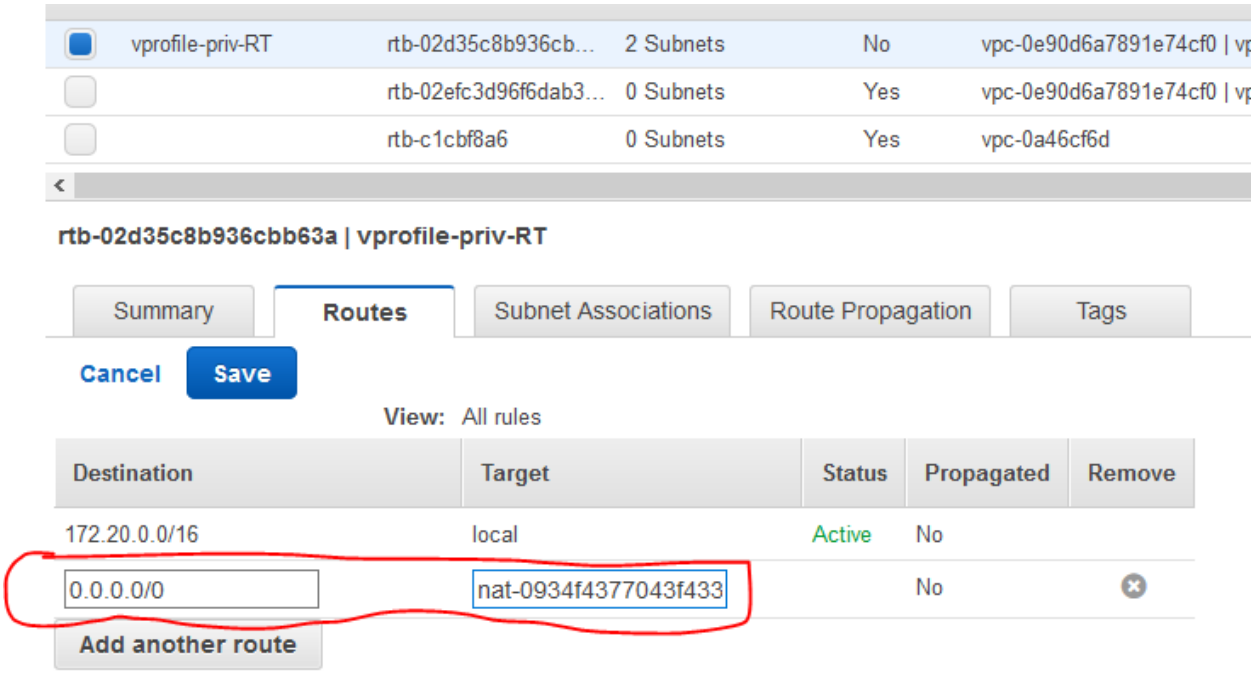
Simillarly we have to create route table for private subnet go to route table section and create for private subnet.



And attach private 1 and 2 Subnet Associations like below



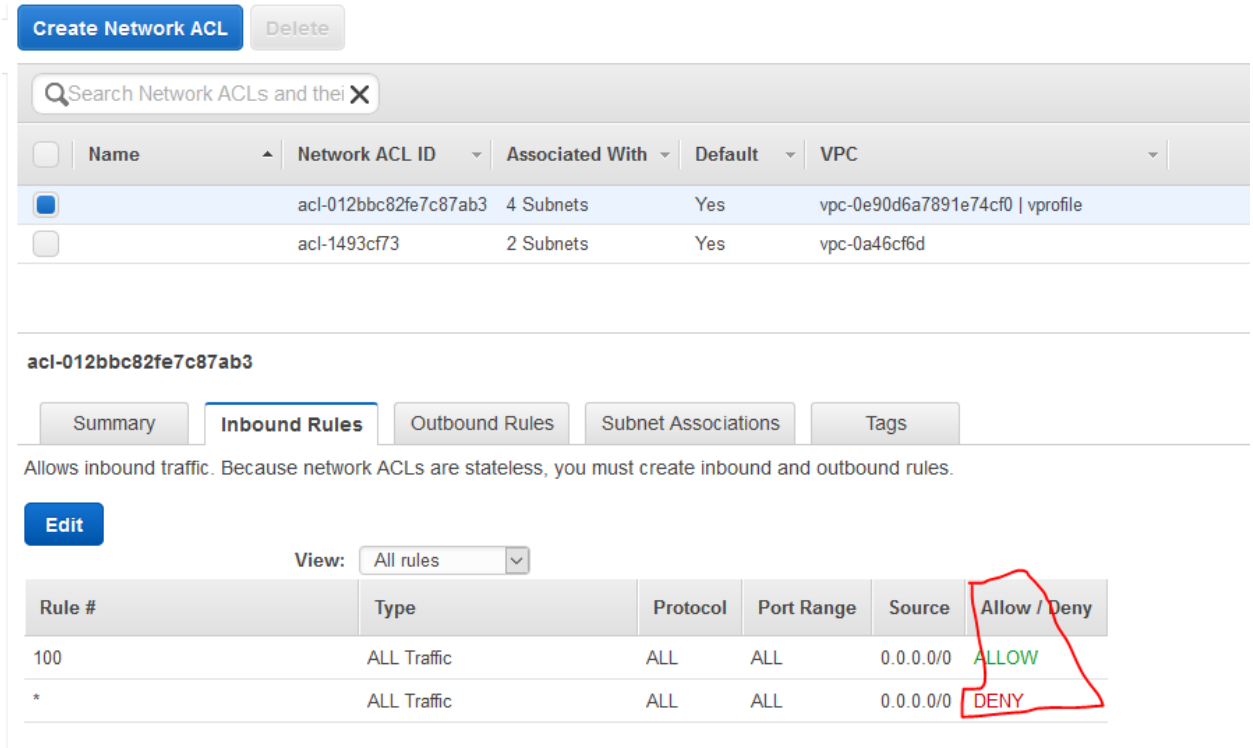
And goto Route tab and select NAT gateway there



If I change here as a internet gateway subnet will become as a public subnet if I keep NAT gateway it will become like private subnet. There is nothing special about public and private networks just routing rule.

We just completed our complete setup except one NAT gateway since it is expensive we are not going to do that, create vpc, 4 subnets one internet gateway and one NAT gateway and all.

There is one more this NACL (Network Access Control List). Security Groups created for Instances and NACL is on the subnet. Here we can control and we can define in coming and out going traffic same like security groups in addition here we can deney traffic as well. This will see later



We can put some hacking Ip address and all here example.

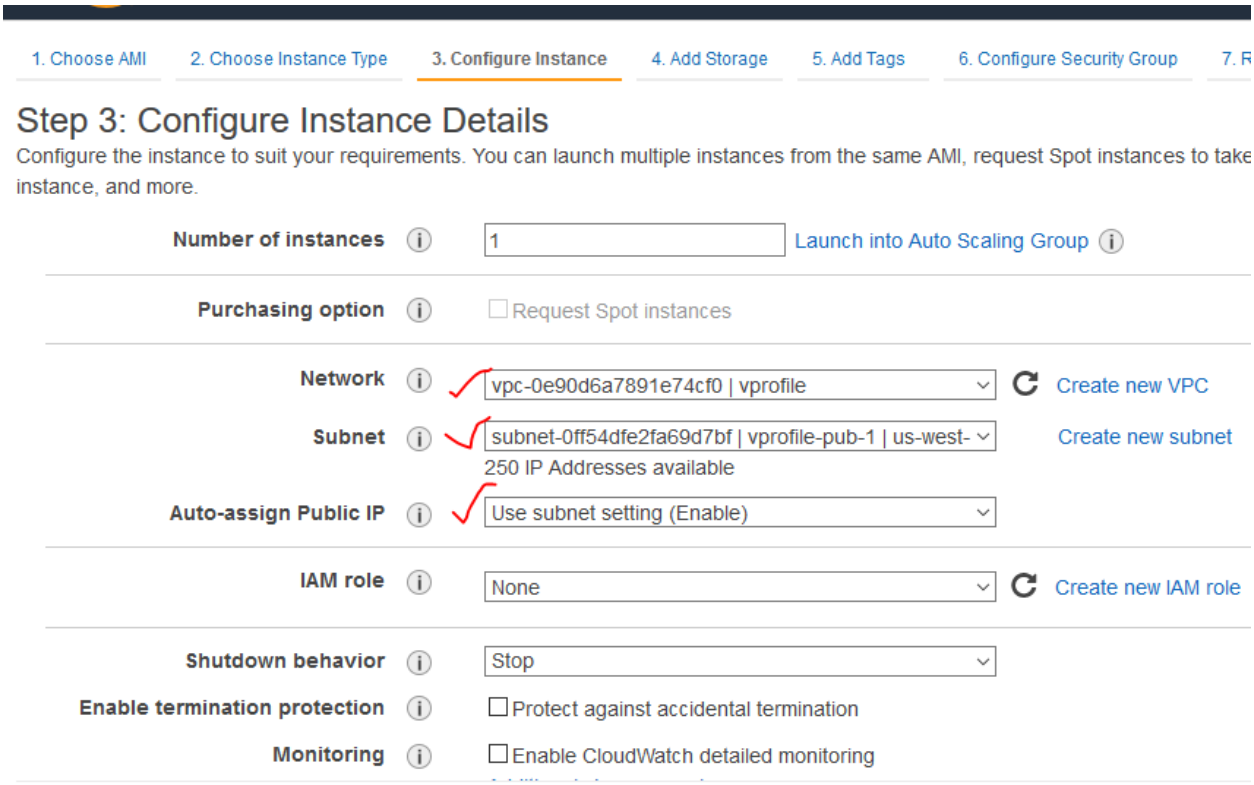
VPC used by so many services in AWS.all IAAS and PAAS on there we can set up our VPC

EC2 is IAAS

RDS is PAAS.

Now we can create one EC2 instance here.

First one create centos/6 instance in public network and Ubuntu going to create in private network.



And security please select new one and says only ssh and my ip only.

Again create one more server called Ubuntu using security connect via above server only

scp –I Downloads/jumpserver.pem Downloads/vprofile-NC-Prod.pem centos@IP:/home/centos

first key access to centos and second copy is going to copy into centos home directory.So first key is going to use for authenticate of centos centos server to copy Ubuntu key.

login centos

then from centos login Ubuntu with private ip using connect button