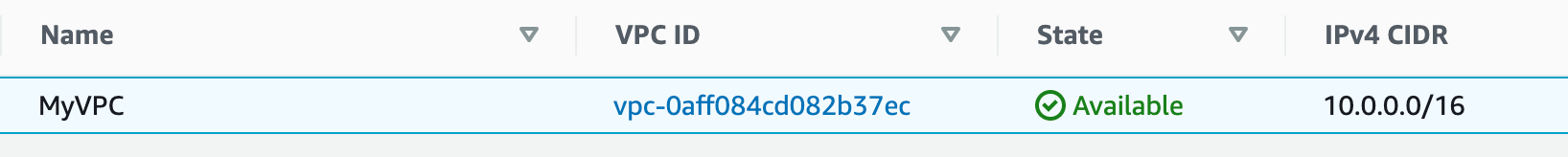
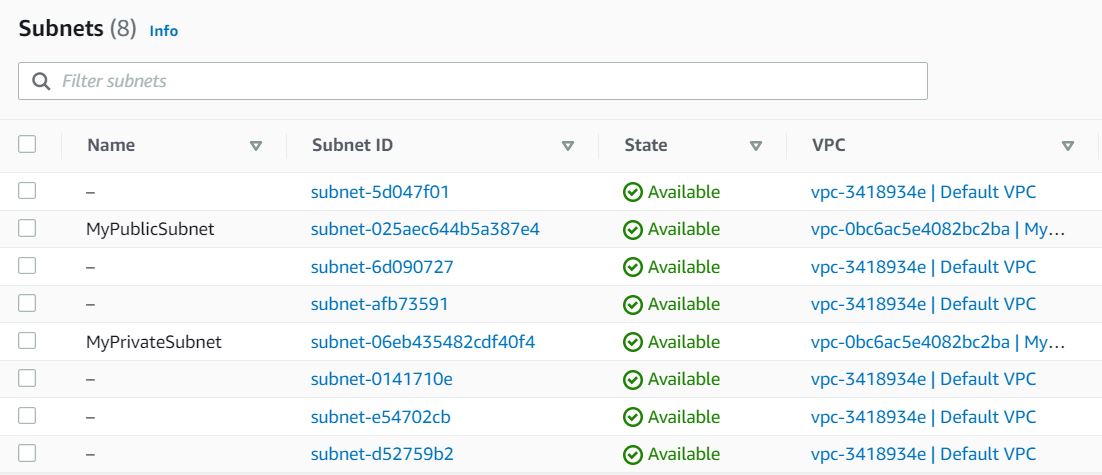
## Task 1 : Create VPC

1. Make sure you are in the US East (N. Virginia) us-east-1 region.
2. Navigate to VPC under the services menu. Click on Your VPCs.
3. Click on 
   * Resources to create : Select VPC Only
   * Name Tag : Enter *MyVPC*
   * IPv4 CIDR block : Enter *10.0.0.0/16*(You can also put any other CIDR range)
   * IPv6 CIDR block : Select No IPv6 CIDR Block
   * Tenancy : Default
   * Click on Create VPC.
4. The VPC is now created.



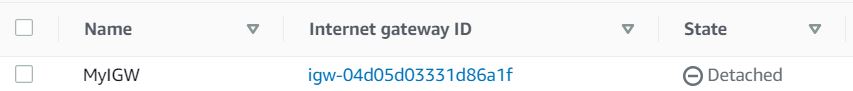
## Task 3 : Create Public and Private Subnets

1. Navigate to Subnets in the left panel of the VPC page.
2. Let's create Public subnet. Click on 
   * VPC ID : select MyVPC
   * Subnet Name : Enter *MyPublicSubnet*
   * Availability Zone : No Preference
   * IPv4 CIDR block : Enter *10.0.0.0/24*
   * Click on Create subnet.
3. Let's enable Auto Assign public IP to Instances created within this subnet,
   * Select MyPublicSubnet, Click on Actions.
   * Click on Edit subnet settings.
   * Enable auto-assign public IPv4 address : Check
   * Click on Save.
4. Now the Instances launched inside the MyPublicSubnetwill have Public IPs assigned to them by default.
5. Let’s create a private subnet. Click on Create subnet.
   * VPC ID : select MyVPC
   * Subnet Name : Enter *MyPrivateSubnet*
   * Availability Zone : No Preference
   * IPv4 CIDR block : Enter *10.0.1.0/24*
   * Click on Create subnet.
6. Now, two subnets are created.

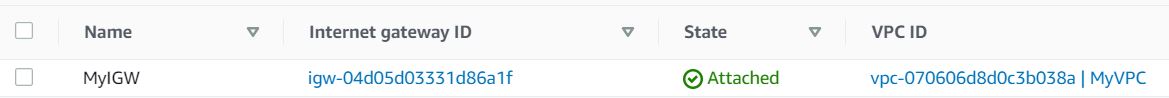


## Task 3 : Create Internet Gateway

1. Navigate Internet Gateways in the left panel of the VPC page.
2. Click on 
   * Name tag : Enter *MyIGW*
   * Click on Create internet gateway.
3. An Internet Gateway is now created.



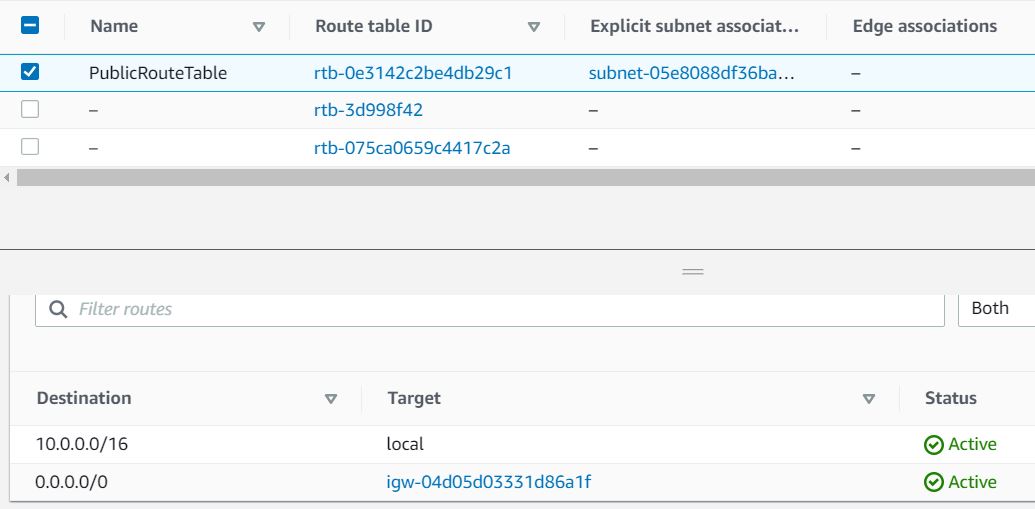
1. To attach Internet Gateway to a VPC,
   * Select the Internet Gateway MyIGW.
   * Click on Actions. Select Attach to VPC.
   * VPC : Select MyVPC
   * Click on Attach internet gateway.
2. Now MyIGW is attached to MyVPC.



## Task 4 : Create Public Route Table and Configure

We will create a route table and attach a public subnet to it. Instances launched within this subnet will have access to the Internet.

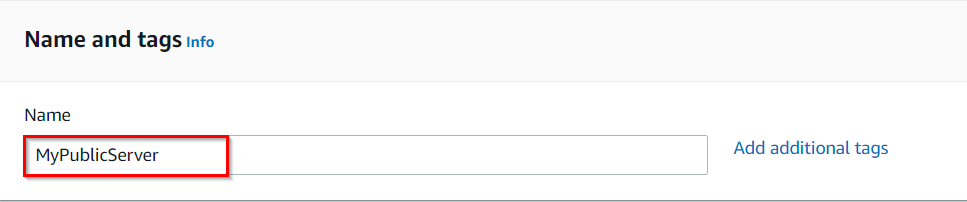
1. Navigate to Route Table in the left panel of the VPC page.
2. Click on 
   * Name tag : Enter *PublicRouteTable*
   * VPC : Select MyVPC
   * Click on Create route table.
3. A route table by name PublicRouteTable will be created.
4. To attach an Internet Gateway, select PublicRouteTable.
5. In the Routes tab below:
   * Click on Edit routes.
   * On the next page, click on Add route
   * Destination : Enter *0.0.0.0/0*
   * Target : Select Internet Gateway, and once the internet gateways have been created, select MyIGW
   * Click on Save changes.
6. To associate the Public Subnet to the route table, Select PublicRouteTable.
   * Click on the Subnet Associations tab.
   * Click on Edit subnet associations.
   * On the next page, select MyPublicSubnet from the list displayed.
   * Click on Save associations.
7. Once all the configurations are completed, it should look like below:

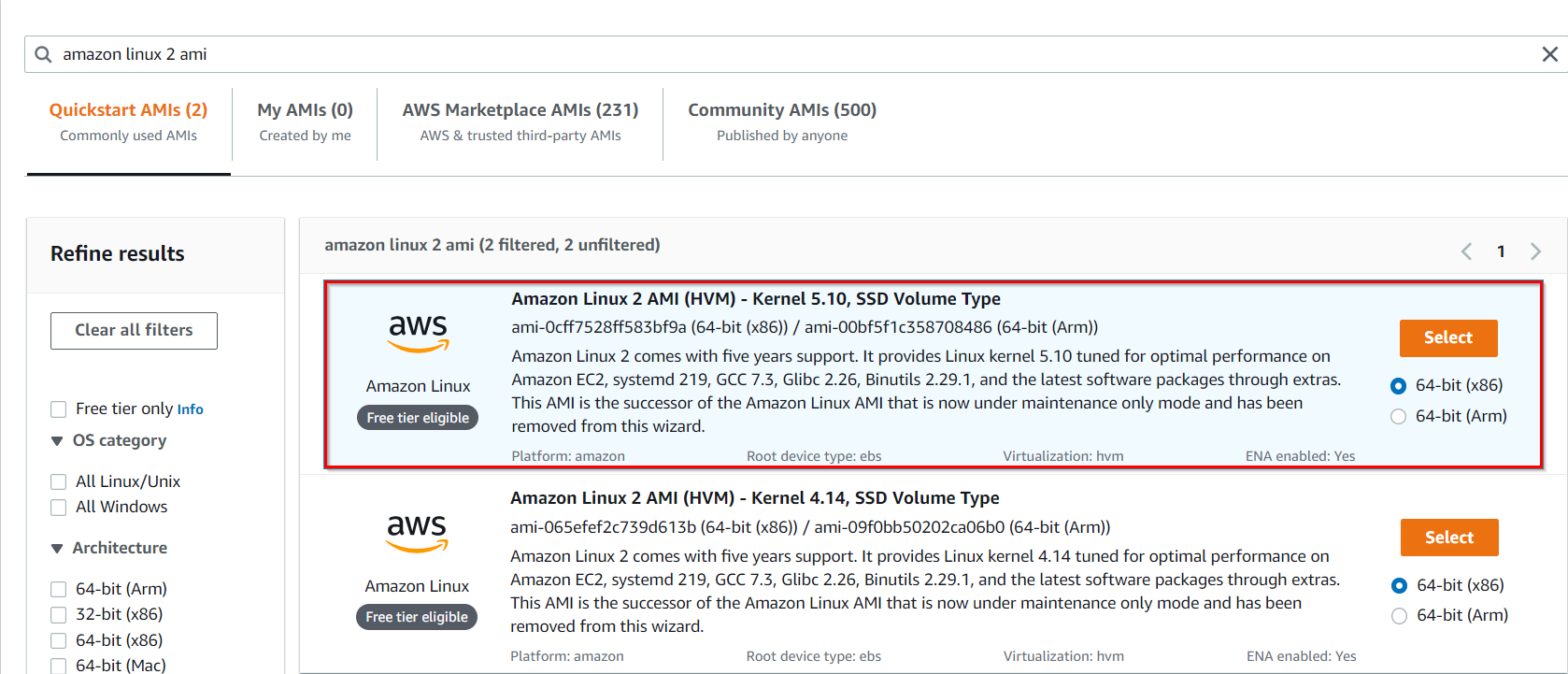


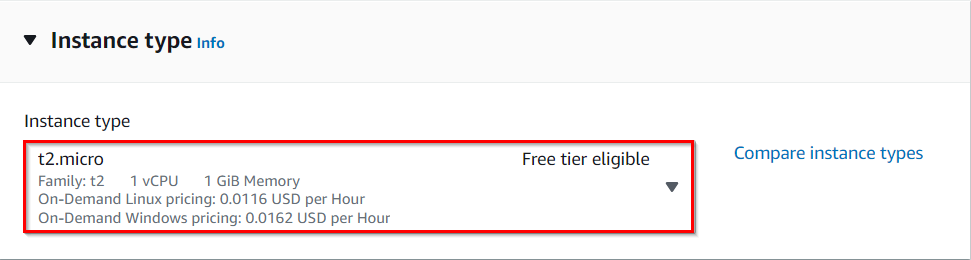
1. Now the Instances launched within MyPublicSubnet will have access to the Internet.
2. As you can see, there is another existing route table already available for MyVPC. It is a main route table created at the time the VPC was created. We will use it while creating the NAT Gateway.

## Task 5 : Launch an EC2 Instance in Public Subnet

1. Make sure you are in the N.Virginia region.
2. Navigate to the  menu in the top, click on EC2 in the Compute section.
3. Navigate to Instances on the left panel and click on 
4. Name : Enter *MyPublicServer*

**

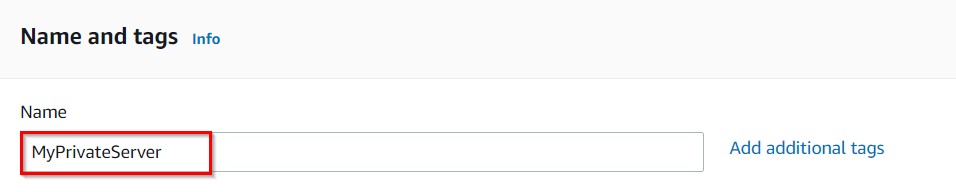
1. For Amazon Machine Image (AMI): Search for Amazon Linux 2 AMI in the search box and click on the select button.  
   
2. Note: if there are two AMI's present for Amazon Linux 2 AMI, choose any of them.
3. For Instance Type: select *t2.micro*

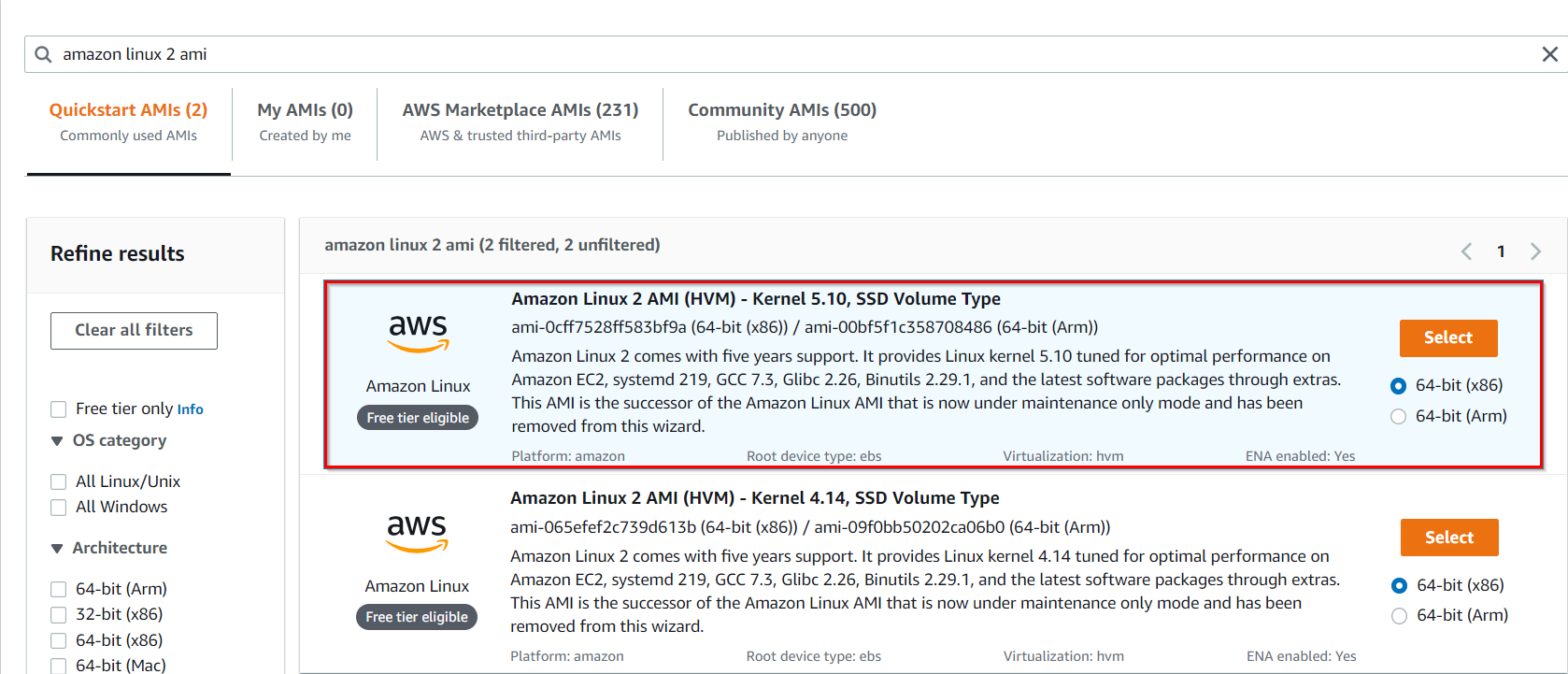
**

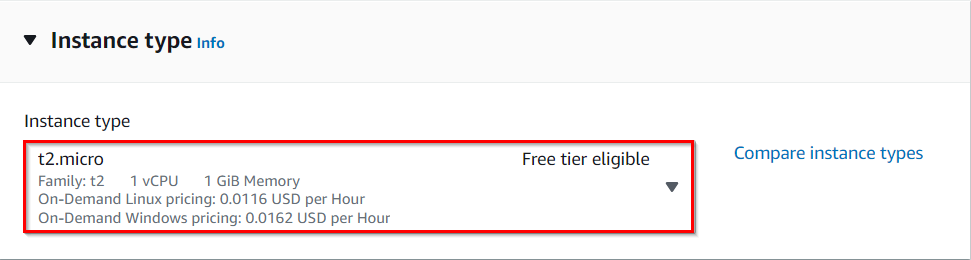
1. For Key pair: Select Create a new key pair Button
   1. Key pair name: MyKey
   2. Key pair type: RSA
   3. Private key file format: .pem
2. Select Create key pair Button.
3. In Network Settings Click on Edit:
4. VPC : Select MyVPC
5. Subnet : Select *MyPublicSubnet*
6. Auto-assign public IP: Enable
7. Select Create new Security group
8. Security group name : Enter *MyEC2Server\_SG*
9. Description : Enter *Security Group to allow traffic to EC2*
   1. To add SSH
      * Choose Type:
      * Select SSH
      * Source: Select Anywhere
10. Keep Rest thing Default and Click on Launch Instance Button.
11. Select View all Instances to View Instance you Created
12. Launch Status: Your instance is now launching, Select the instance and wait for it to change status to Running.

## Task 6 : Launch an EC2 Instance in Private Subnet

1. Click on Launch instances.
2. Name : Enter *MyPrivateServer*

**

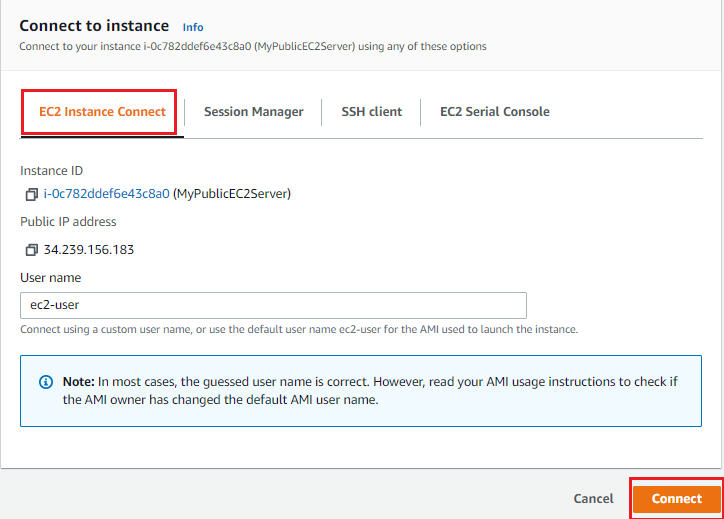
1. For Amazon Machine Image (AMI): Search for Amazon Linux 2 AMI in the search box and click on the select button.  
     
   Note: if there are two AMI's present for Amazon Linux 2 AMI, choose any of them.
2. For Instance Type: select *t2.micro*

**

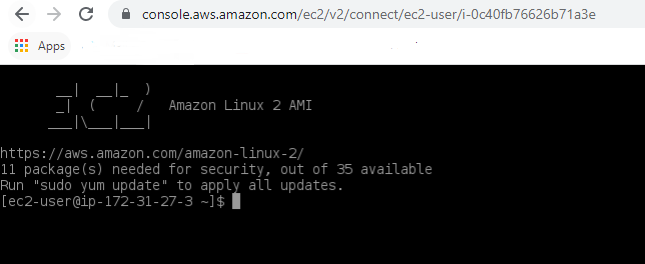
1. For Key pair: Select the key pair you created before
2. In Network Settings Click on Edit:
   1. VPC : Select MyVPC
   2. Subnet : Select *MyPrivateSubnet*
   3. Auto-assign public IP: Disable
   4. Select Select existing security group
   5. Select MyEC2Server\_SG
3. Keep Rest thing Default and Click on Launch Instance Button.
4. Select View all Instances to View Instance you Created
5. Launch Status: Your instance is now launching, Select the instance and wait for it to change status to Running.
6. Note the Private IP Address of MyPrivateServer : Example 10.0.1.45

## Task 7 : SSH into Public and Private EC2 Instance and Test Internet Connectivity

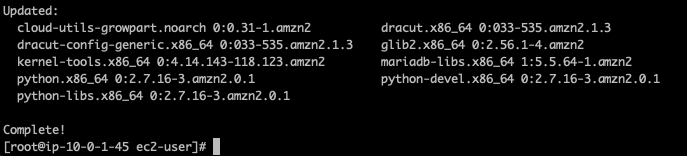
1. SSH into MyPublicServer Instance.
2. Once the instance is created. Select the instance MyPublicServer.Click on connect button
3. Now select the EC2 instance connect option. You can see there are four options for connecting to EC2. You can use any of the given options to get in the console but for our lab, we are using EC2 instance connect.



1. A new tab would be opened in your browser where we can see the console.

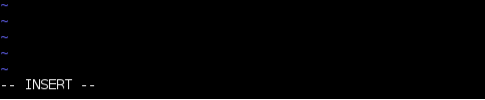


1. Switch to root user:
2. sudo su
3. Run the updates using the following command:
   * yum -y update
4. Since the Internet Gateway MyIGWis connected to MyPublicSubnet, updates will be completed successfully.



1. Let’s SSH into MyPrivateEC2Serverfrom MyPublicEC2Server.
2. In order to SSH into MyPrivateEC2Server*,* first, we need to create the PEM file in the public EC2 ie, MyPublicEC2Server, and copy the data from our MyKey.pem in the local machine.
3. We need MyKey.pem in order to SSH. We shall copy key details from the MyKey.pem from your local machine (which was downloaded earlier while launching EC2 instances).
4. To copy the contents of the MyKey.pem, open the file in a text editor and copy the whole content.
5. To create the MyKey.pem in MyPublicEC2Server, run
   * vi MyKey.pem
6. Now press the following for inserting the data(You can see insert popped at the last then you can paste the key).

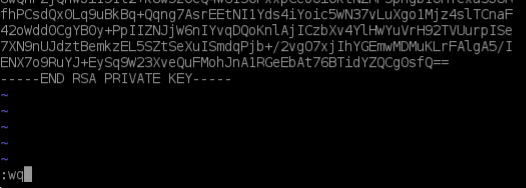
* Click i



Note: In the editor, copy and paste the key that looks similar to the example below:



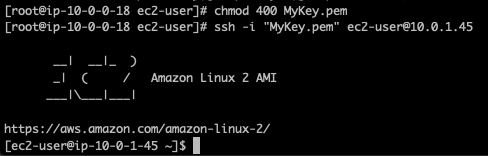
1. Save the File
   * click esc
   * :wq



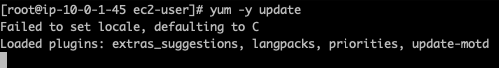
1. Check that the file was created correctly.
   * ls



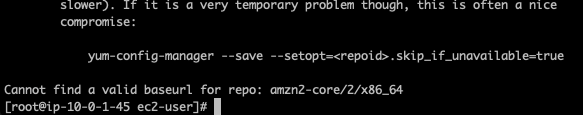
1. Update Permissions for the MyKey.pem
   * chmod 400 MyKey.pem
2. Use the Private IP address of MyPrivateEC2Server to SSH.
   * ssh ec2-user@10.0.1.93 -i MyKey.pem
   * Note: Incase if this message shows Are you sure you want to continue connecting (yes/no)? : Enter yes



1. Switch to root user
   * sudo su
2. Run the updates using the following command:
   * yum -y update



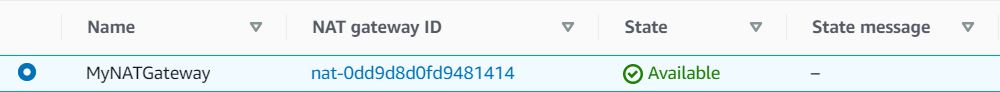
1. Since no internet access is provided for EC2 instances in a private subnet, you will not be able to get updates. After some time, it will fail with the following message.



## Task 8 : Create a NAT Gateway

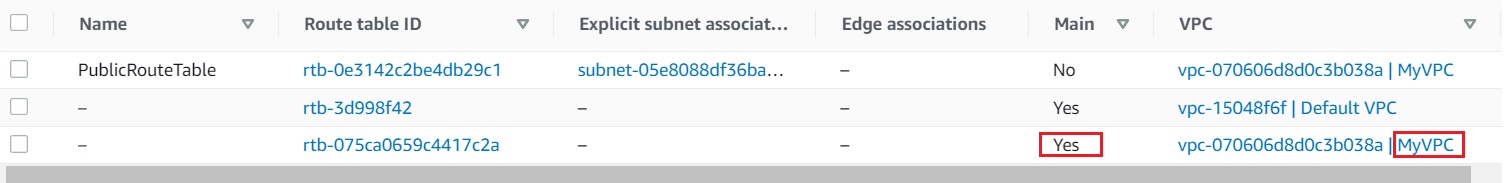
NAT Gateway is used to provide internet access to the Instances inside a private subnet.

1. Navigate to the VPC Page.
2. Make sure you are still in the N.Virginia Region.
3. In the Left Panel, click on NAT Gateways.
4. Click on 
   * Name : Enter *MyNATGateway*
   * Subnet : Choose MyPublicSubnet in MyVPC
   * Elastic IP Allocation ID: Click on Allocate Elastic IP.
   * Once the new Elastic IP is allocated, click on Create NAT gateway.
5. Note that NAT Gateway is always created in a public subnet.
6. NAT Gateway will be created in a few minutes. Once created, the status will change to available.

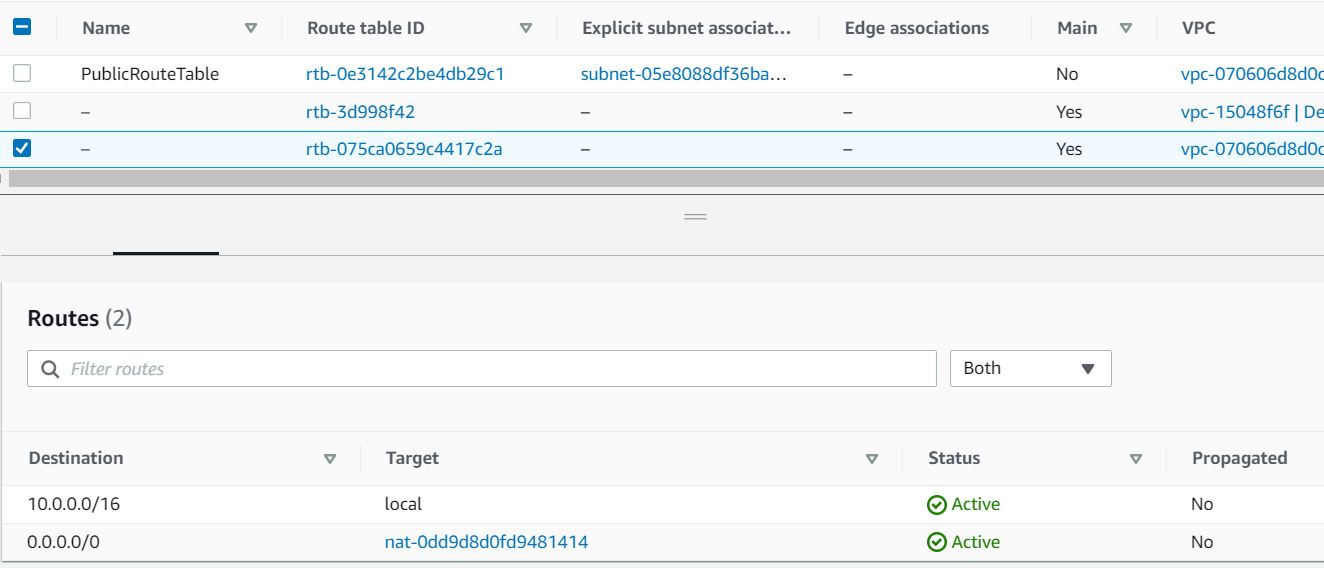


## Task 9 : Update Route table and configure NAT Gateway

1. Navigate to Route Tables in the left panel.
2. You can see two Route Tables available for MyVPC



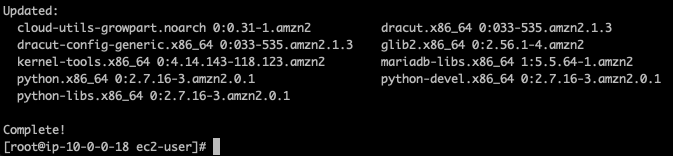
1. To attach Nat Gateway, select the Main Route Table (which is different from the one created by you).
2. In the Routes tab below,
   1. Click on Edit routes.
   2. In the next page, Click on Add route
   3. Destination: Enter *0.0.0.0/0*
   4. Target: Select NAT Gateway, and once the internet gateways have loaded, select the NAT Gateway you created.
   5. Click on Save changes.
3. Once all the configurations are completed, it should look like below.



1. Now the Instances launched within MyPrivateSubnet can access the Internet through the NAT Gateway.

## Task 10 : Test Internet connection from Instance inside Private Subnet

1. SSH back into MyPublicEC2Server.
2. Switch to root user
   * sudo su
3. SSH into MyPrivateEC2Server
   * ssh -i "MyKey.pem" ec2-user@10.0.1.45
4. Switch to root user
   * sudo su
5. Run the updates using the following command:
   * yum -y update
6. You can see that the updates have been completed successfully in the terminal.



1. This shows that MyPrivateEC2Serverhas internet access.
2. Use exit command to close the private server connection.