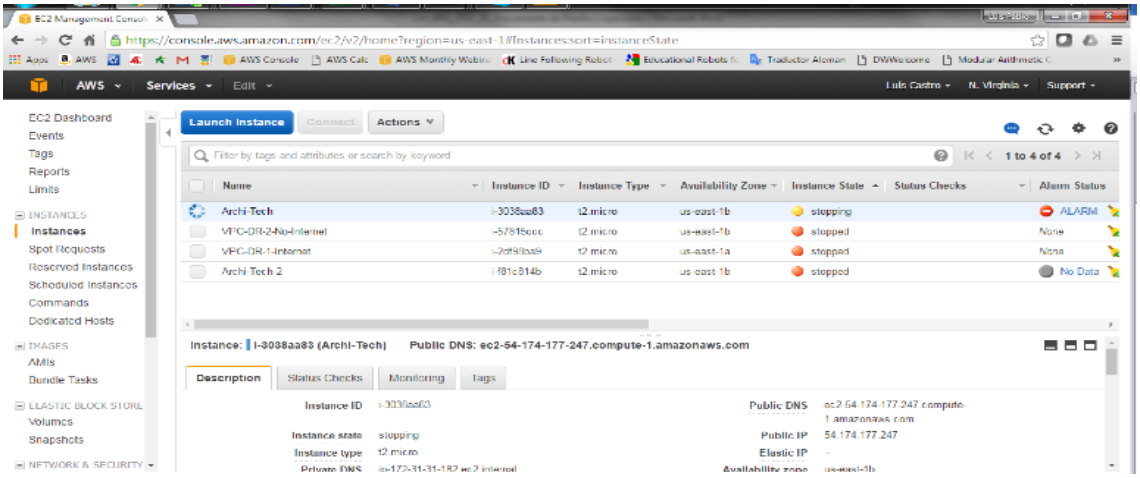
Paso 1

Acceder a la consola de AWS mediante el siguiente link:

https://lcastrose.signin.aws.amazon.com/console

Paso 2

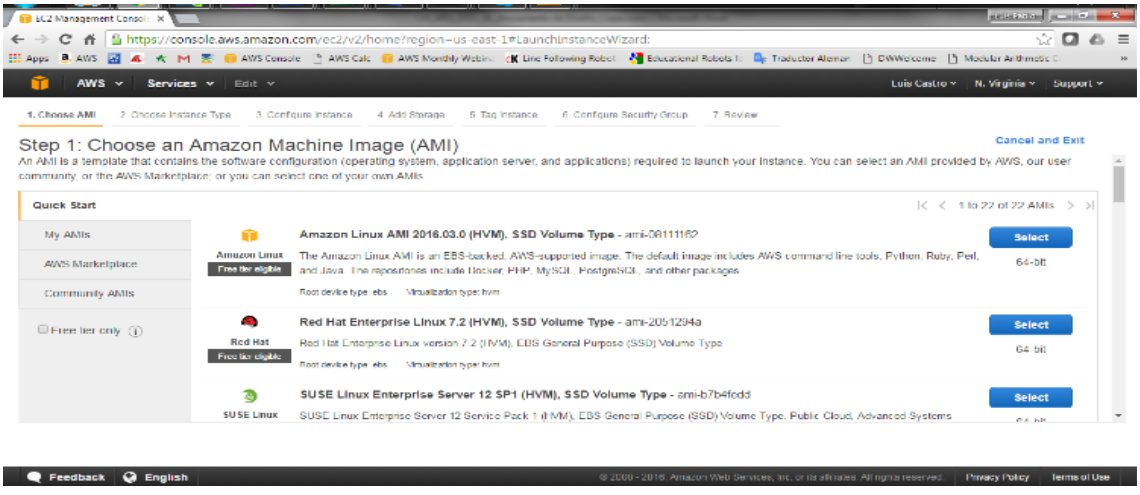
Acceder al servicio de **EC2>Intances>Launch Instances**



Paso 3

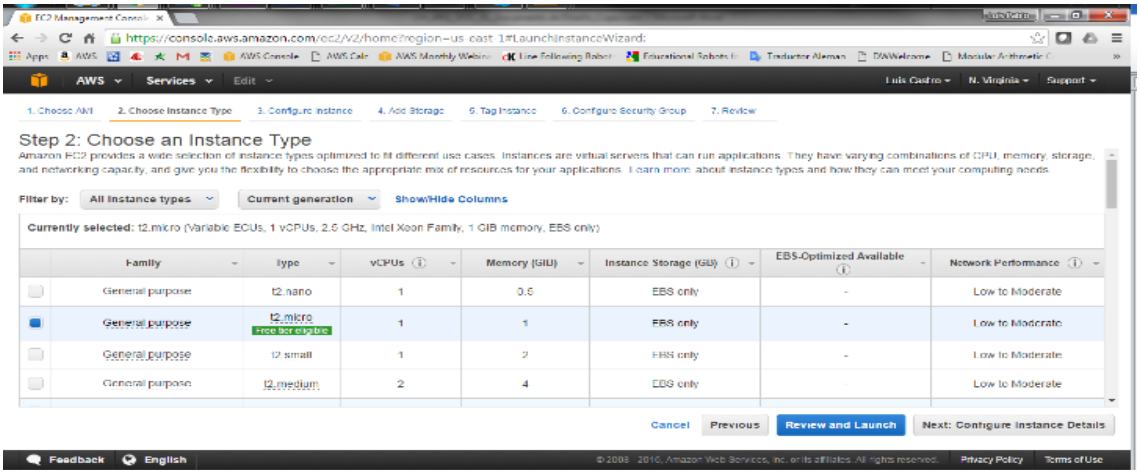
Escoger la instancia **Amazon Linux - Free Tier** y darle **Select**

Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-0e2ff28bfb72a4e45



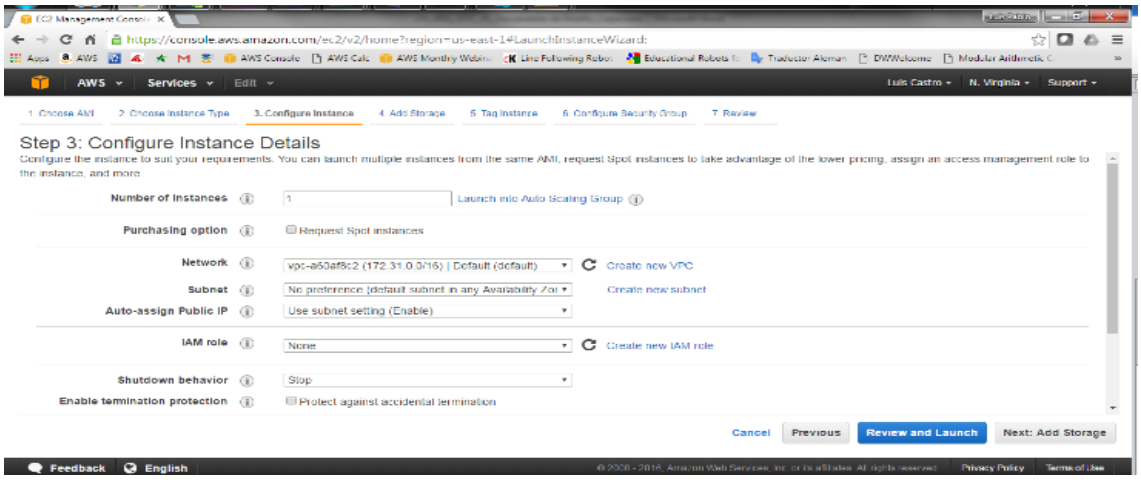
Paso 4

Escoger la instancia del tipo **t2.micro** y darle **Next: Configure Instance Details**



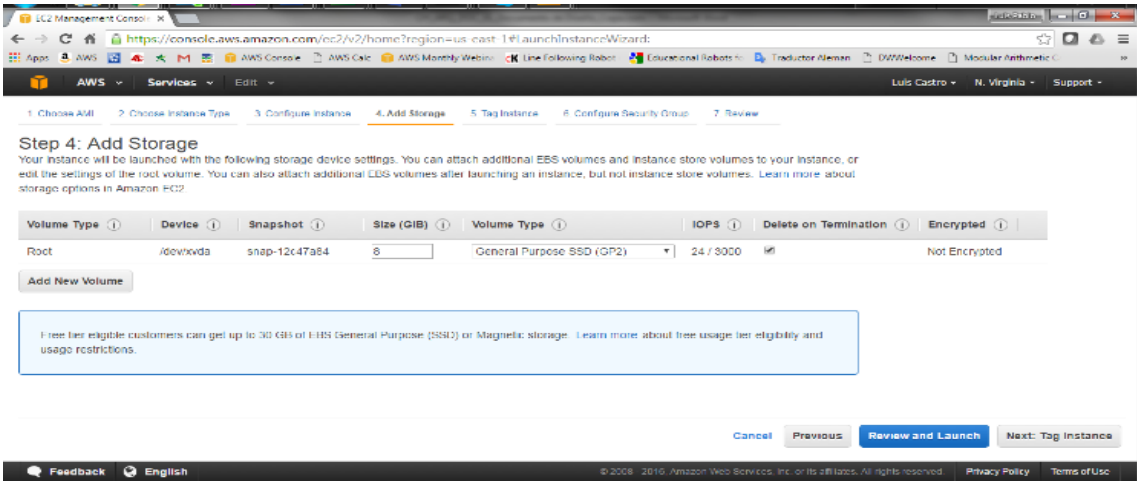
Paso 5

Seleccionar todos los valores por default y darle **Next: Add Storage**



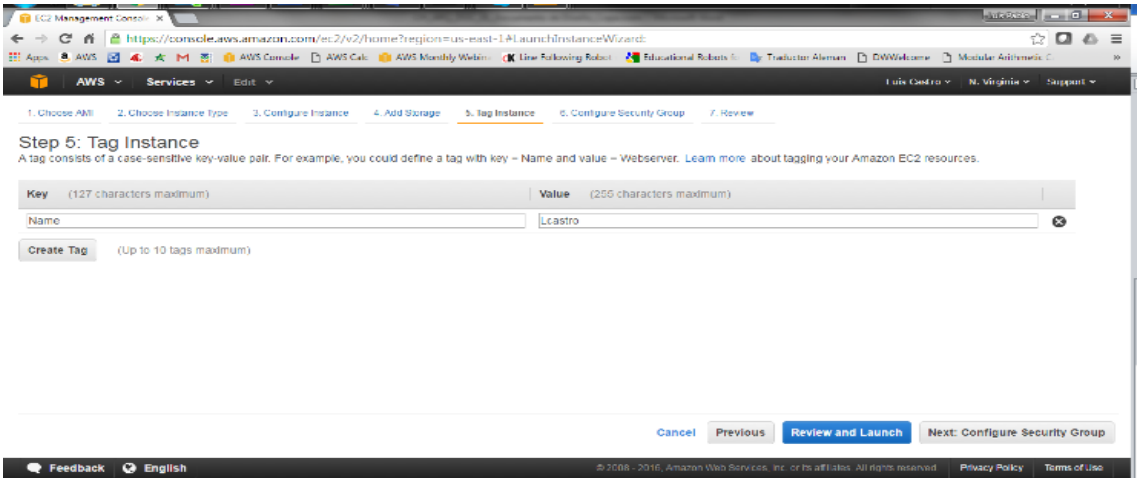
Paso 6

Seleccionar los valores por defecto y darle **Next: Tag Instance**



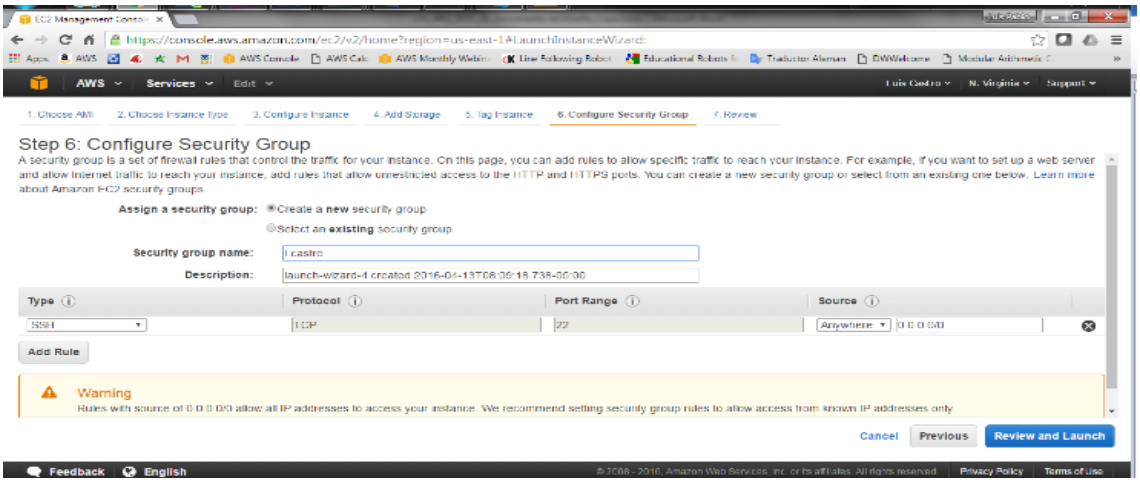
Paso 7

Hacer Click en **AddTag, e**n el campo de **Value** ponerle el nombre de usuario y darle **Next: Configure Security Group**



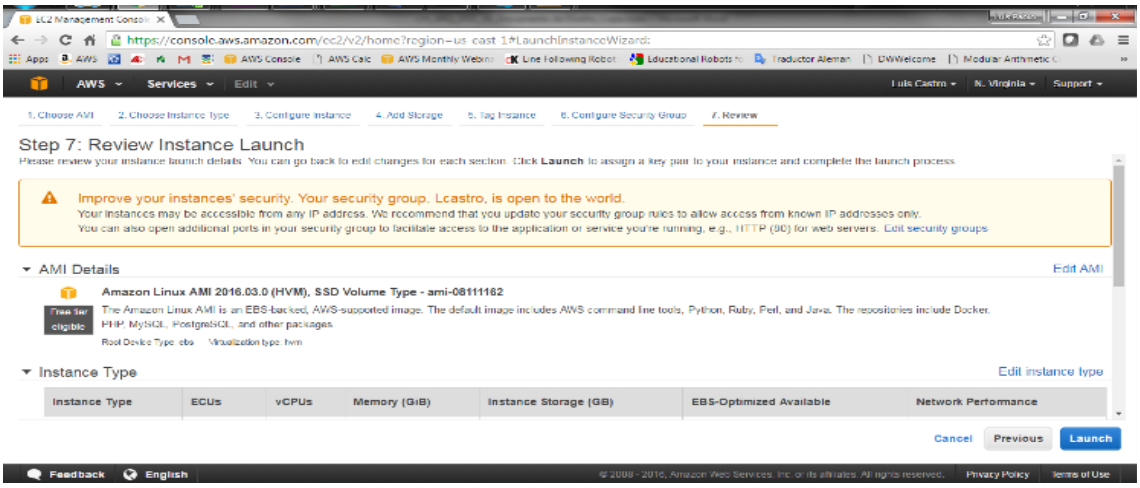
Paso 8

Seleccionar **Create a new security group** con el nombre de usuario, dejar los valores por default y darle **Review and Lauch**



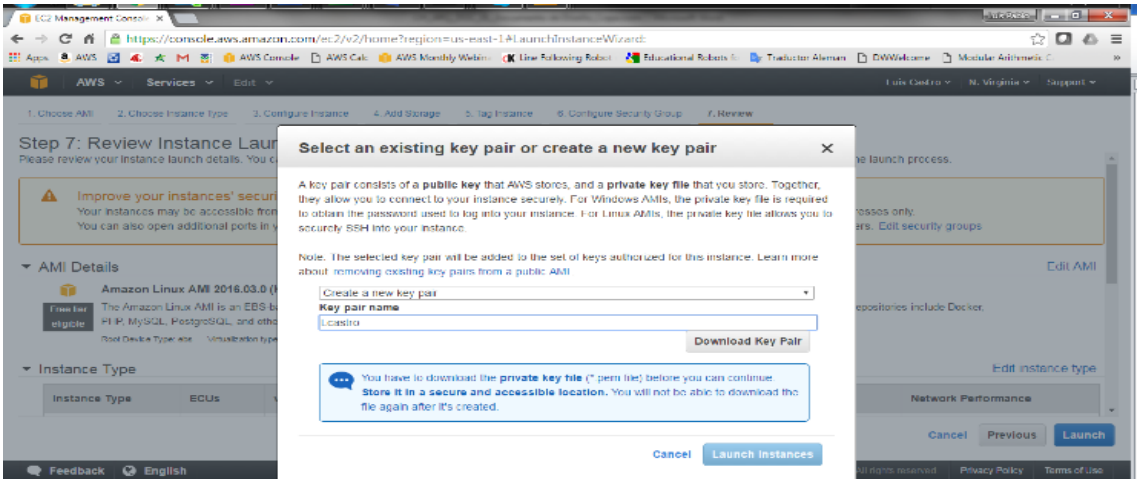
Paso 9

Revisar los valores de la configuración y darle **Launch**



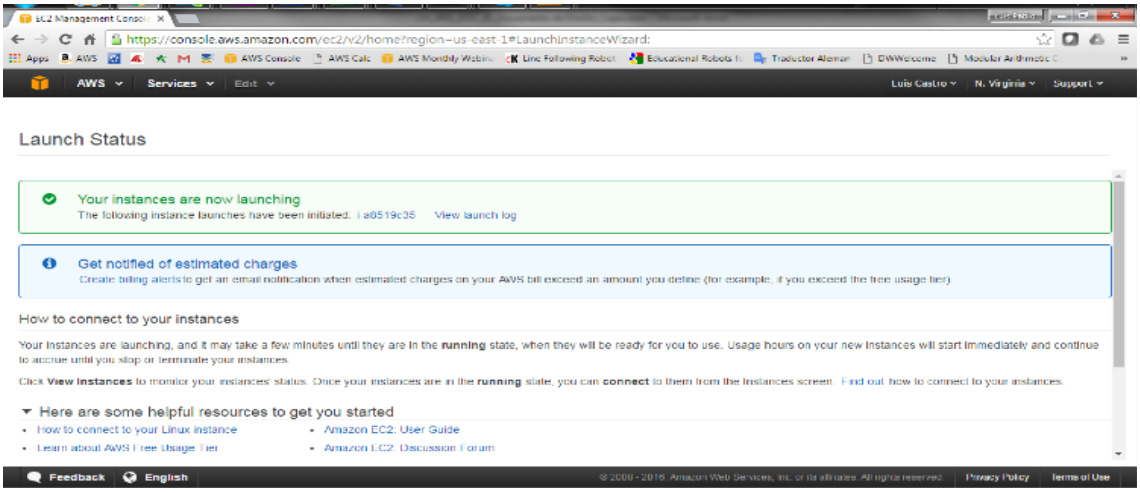
Paso 10

Seleccionar **create a new key pair** y ponerle el nombre de usuario, seleccionar **download key pair** y seguidamente **Lauch Instances**



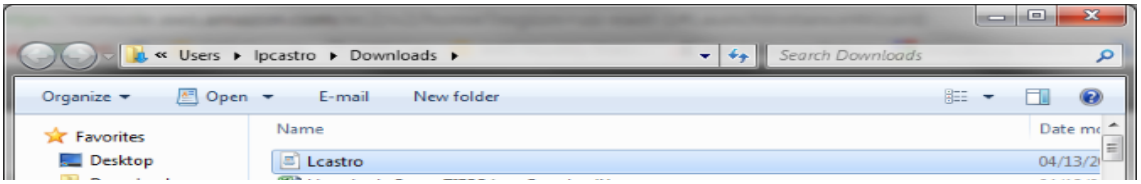
Paso 11

Verificar el status de la instancia creada



Paso 12

Validar que el archivo de Key Pair se encuentre descargado



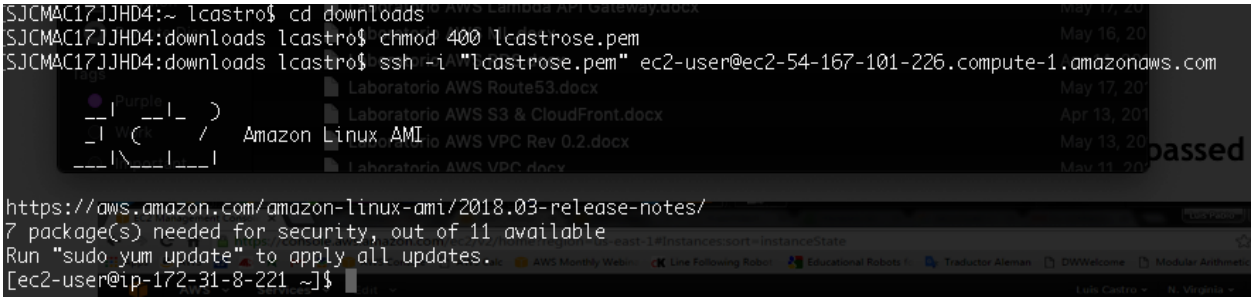
(MacOs Only)

En el folder donde se descargo el archivo .pem correr el siguiente comando:

```
$ chmod 400 lcastrose.pem
```

Conectarse con el siguiente comando:

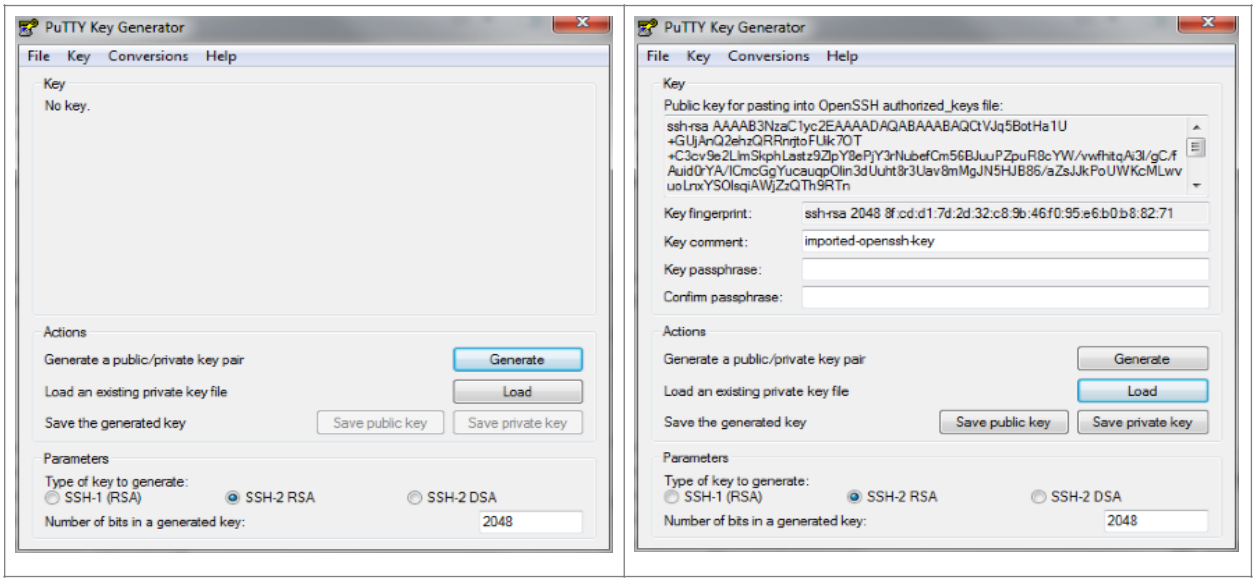
```
$ ssh -i “<nombre del PEM File>” ec2-user@<IP address Publica de la EC2>
```



(Windows Only)

Paso 13

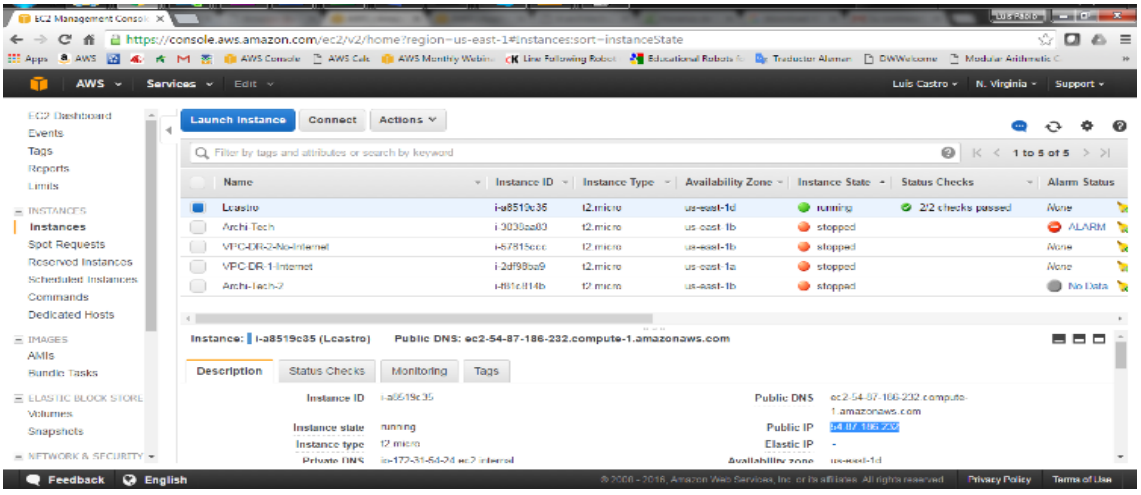
Abrir el **PuttyGen** y darle load y cargar el archivo PEM, seguidamente darle **Save private Key y verificar que se haya generado el archivo .ppk**



Paso 14

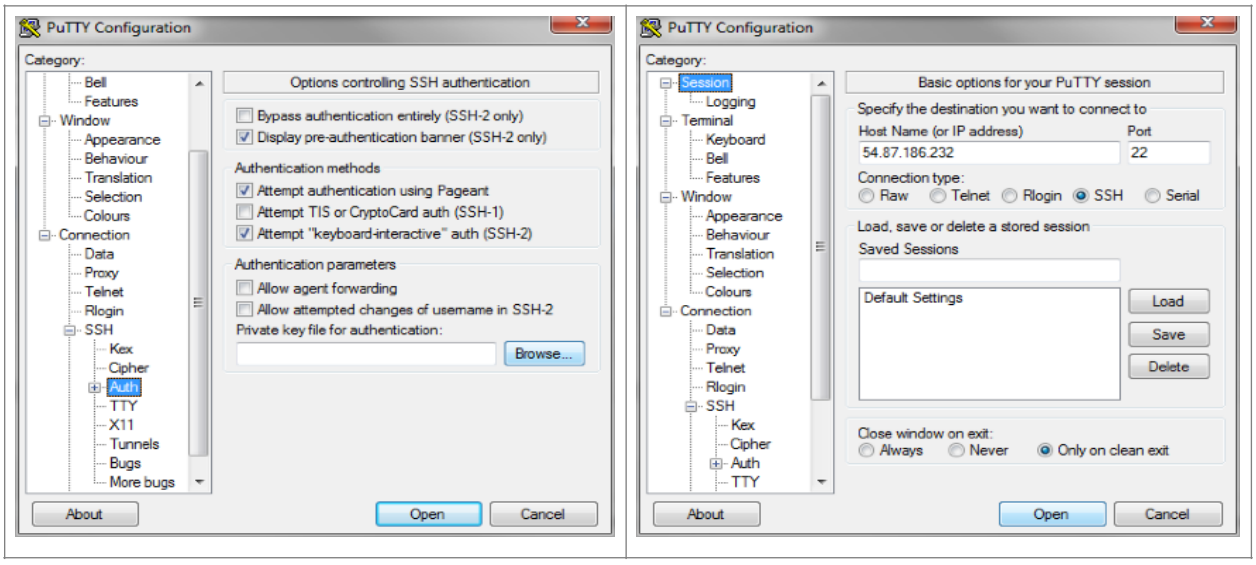
Validar el IP Address público que fue asignado a la instancia EC2

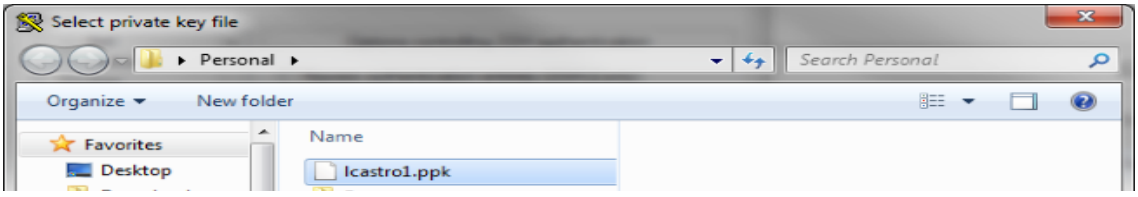
Nota: Esperar hasta que la instancia muestra los status check como **2/2 passed**



Paso 15 (Windows Only)

Abrir el **Putty Client**, en el campo de **Connection>SSH>Auth**, seleccionar **Browse** el archivo .ppk generado y seguidamente ir a **Session** e indicar el IP Address asociado a la maquina EC2 y darle **Open**





Paso 16

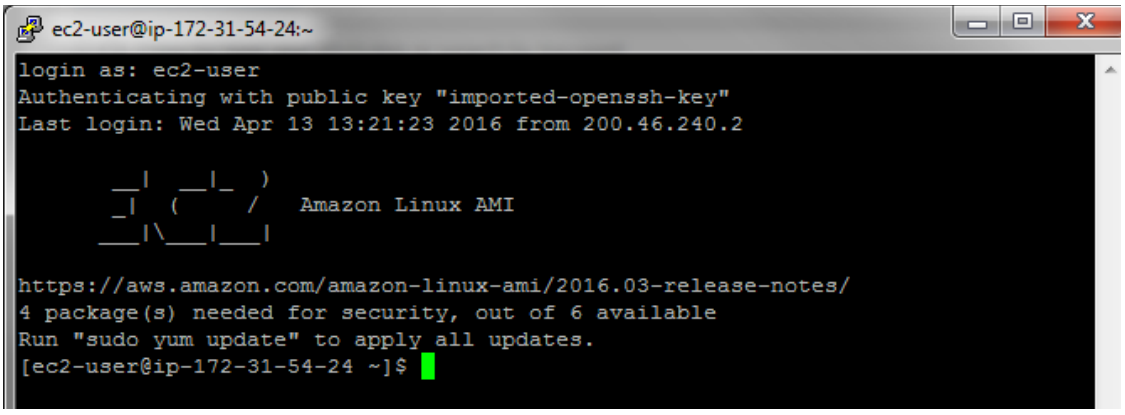
Para acceder a la maquina usar el siguiente user: **ec2-user**

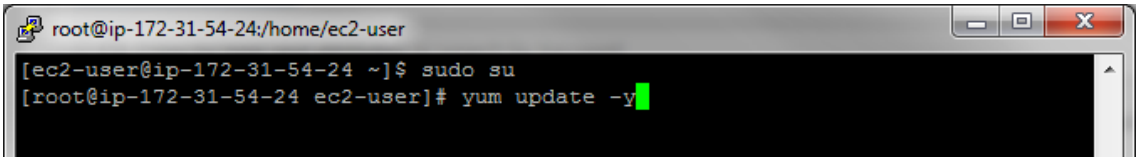
Elevar los privilegios mediante el siguiente comando:

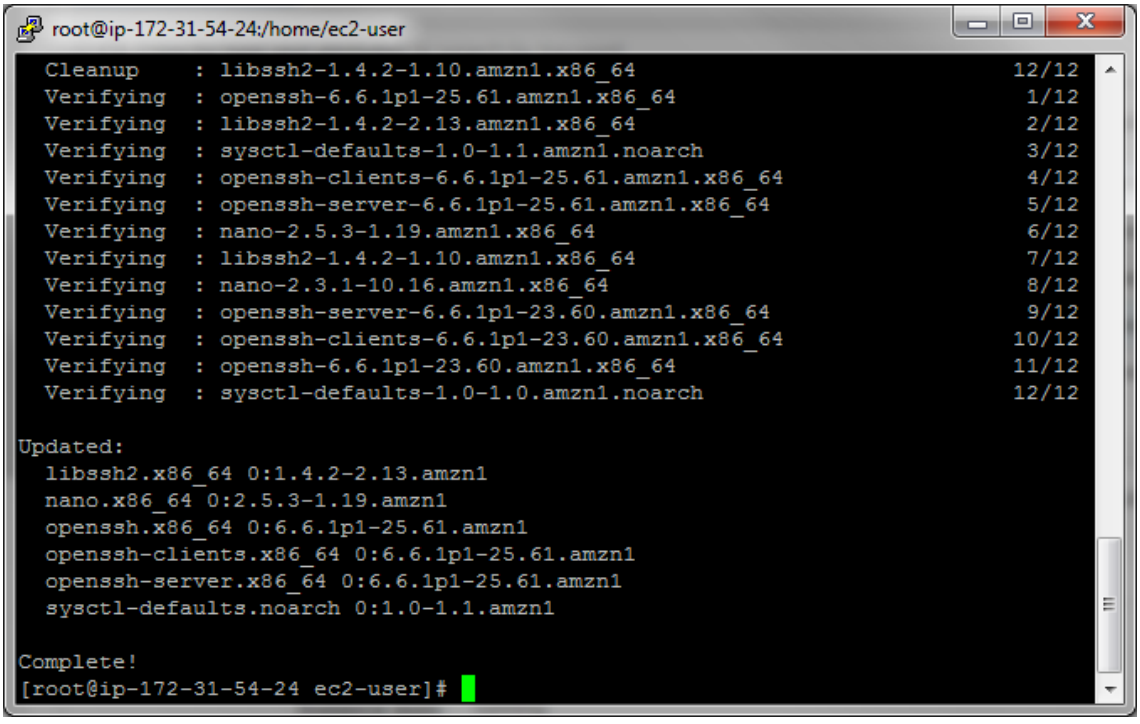
#sudo su

Actualizar la instancia

#yum update -y


ec2-user@ip-172-31-54-24:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Wed Apr 13 13:21:23 2016 from 200.46.240.2
__| __|_)
_| (/ Amazon Linux AMI
___|___|___|
https://aws.amazon.com/amazon-linux-ami/2016.03-release-notes/
4 package(s) needed for security, out of 6 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-54-24 ~]$


root@ip-172-31-54-24:/home/ec2-user
[ec2-user@ip-172-31-54-24 ~]$ sudo su
[root@ip-172-31-54-24 ec2-user]# yum update -y


root@ip-172-31-54-24:/home/ec2-user
Cleanup : libssh2-1.4.2-1.10.amzn1.x86_64 12/12
Verifying : openssh-6.6.1p1-25.61.amzn1.x86_64 1/12
Verifying : libssh2-1.4.2-2.13.amzn1.x86_64 2/12
Verifying : sysctl-defaults-1.0-1.1.amzn1.noarch 3/12
Verifying : openssh-clients-6.6.1p1-25.61.amzn1.x86_64 4/12
Verifying : openssh-server-6.6.1p1-25.61.amzn1.x86_64 5/12
Verifying : nano-2.5.3-1.19.amzn1.x86_64 6/12
Verifying : libssh2-1.4.2-1.10.amzn1.x86_64 7/12
Verifying : nano-2.3.1-10.16.amzn1.x86_64 8/12
Verifying : openssh-server-6.6.1p1-23.60.amzn1.x86_64 9/12
Verifying : openssh-clients-6.6.1p1-23.60.amzn1.x86_64 10/12
Verifying : openssh-6.6.1p1-23.60.amzn1.x86_64 11/12
Verifying : sysctl-defaults-1.0-1.0.amzn1.noarch 12/12
Updated:
libssh2.x86_64 0:1.4.2-2.13.amzn1
nano.x86_64 0:2.5.3-1.19.amzn1
openssh.x86_64 0:6.6.1p1-25.61.amzn1
openssh-clients.x86_64 0:6.6.1p1-25.61.amzn1
openssh-server.x86_64 0:6.6.1p1-25.61.amzn1
sysctl-defaults.noarch 0:1.0-1.1.amzn1
Complete!
[root@ip-172-31-54-24 ec2-user]#