

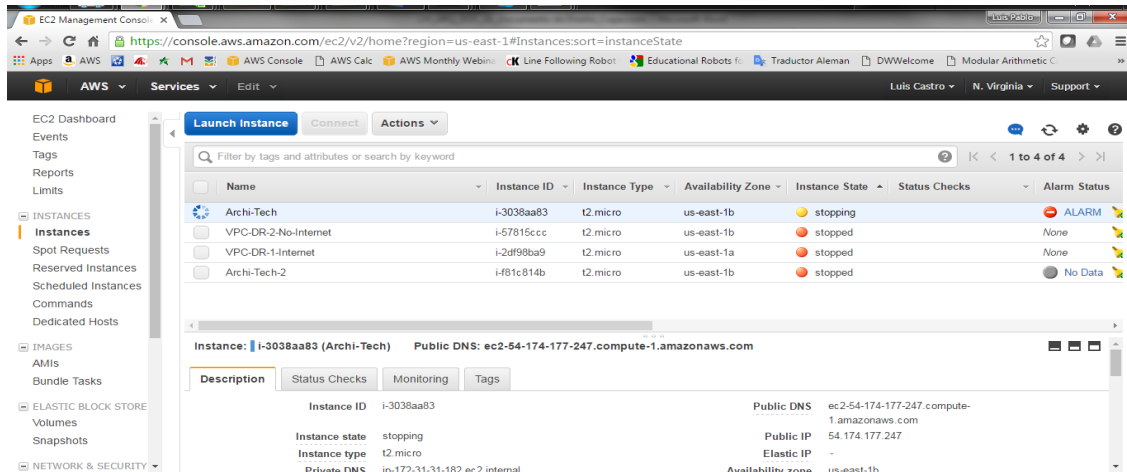
Step 1

Access the AWS console through the following link:

<https://450006219561.signin.aws.amazon.com/console>

Step 2

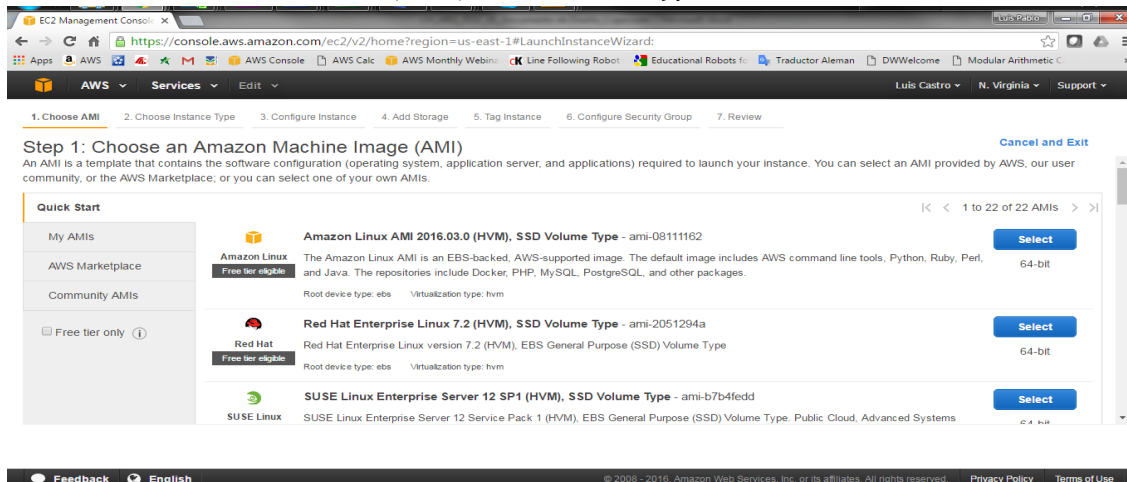
Access the EC2 service> Instances> Launch Instances



Step 3

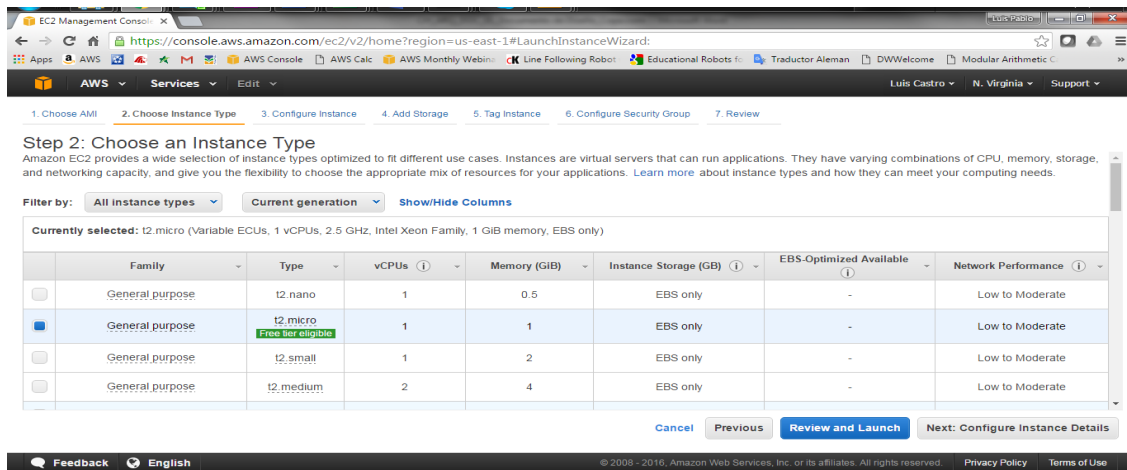
Choose the Amazon Linux - Free Tier instance and click Select

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



Step 4

Choose the instance of type t2.micro and give it Next: Configure Instance Details



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: **All instance types** **Current generation** [Show/Hide Columns](#)

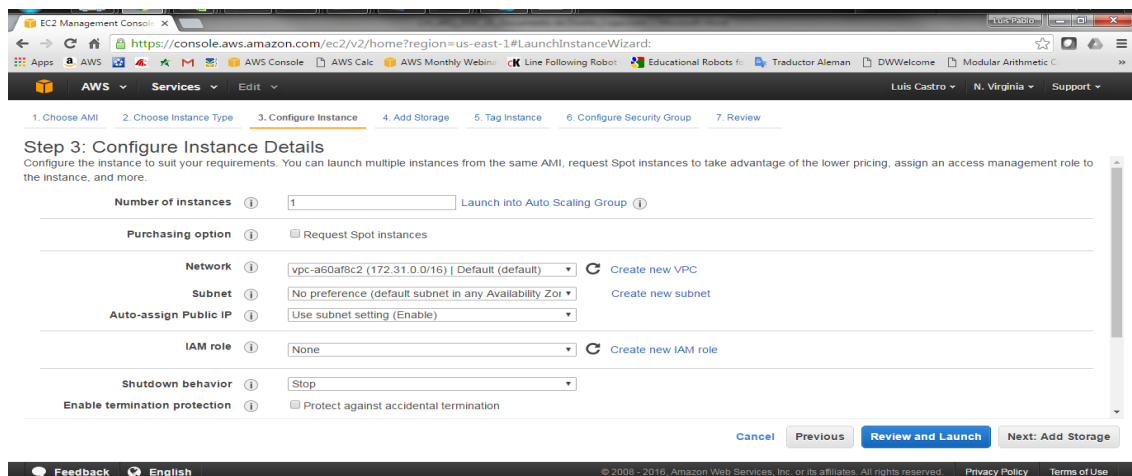
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

Step 5

Select all the default values and give it Next: Add Storage



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option: ☐ Request Spot instances

Network: vpc-a60af8c2 (172.31.0.0/16) | Default (default) [Create new VPC](#)

Subnet: No preference (default subnet in any Availability Zone) [Create new subnet](#)

Auto-assign Public IP: Use subnet setting (Enable)

IAM role: None [Create new IAM role](#)

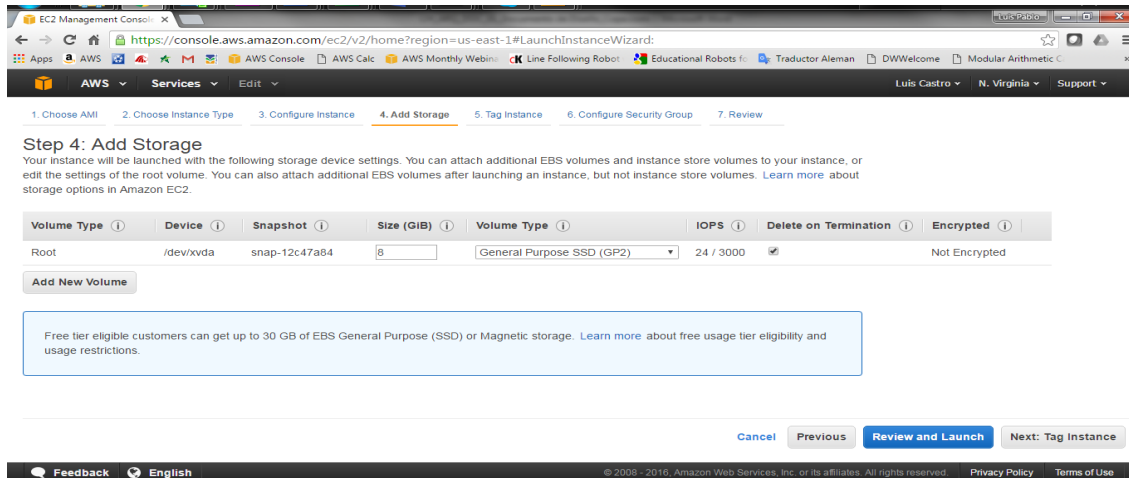
Shutdown behavior: Stop

Enable termination protection: ☐ Protect against accidental termination

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

Step 6

Select the default values and give it Next: Tag Instance



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/xvda	snap-12c47a84	8	General Purpose SSD (GP2)	24 / 3000	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

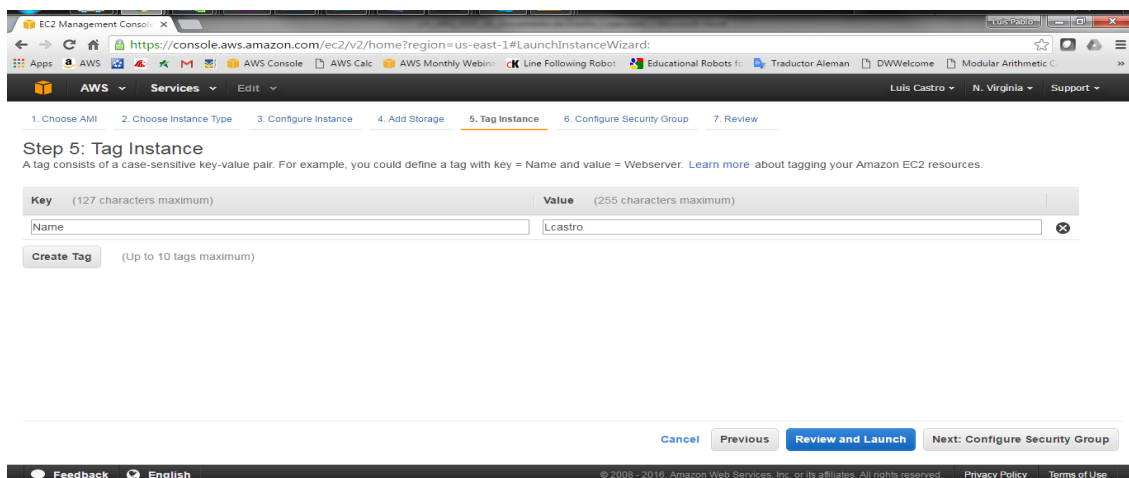
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Tag Instance](#)

Step 7

Click on Add Tag, in the Value field put the username and give it Next: Configure Security Group

In the screenshots, the username is lcastro, PLEASE REFER TO THE SPREADSHEET TO FIND YOUR USERNAME



Step 5: Tag Instance

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

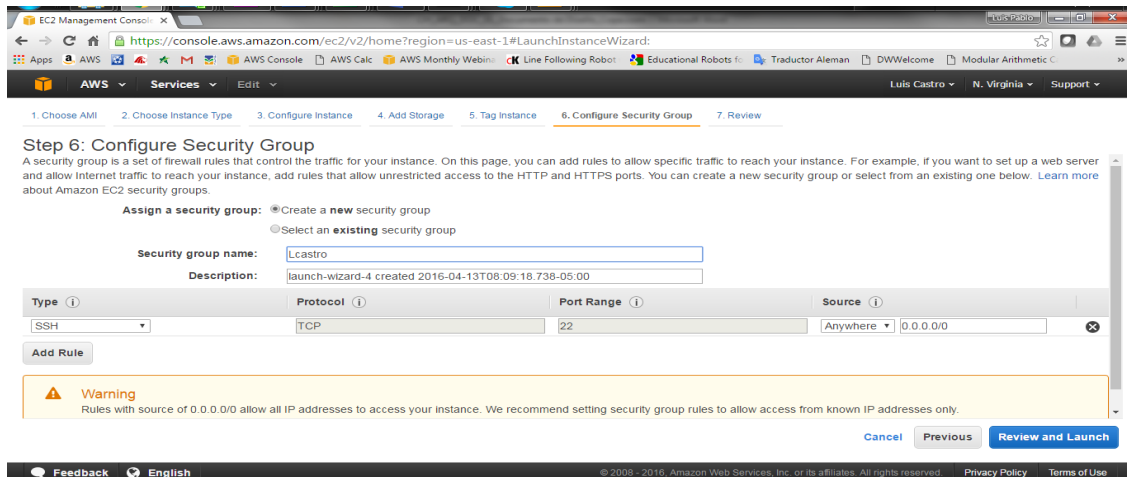
Key	Value
Name	lcastro

[Create Tag](#) (Up to 10 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

Step 8

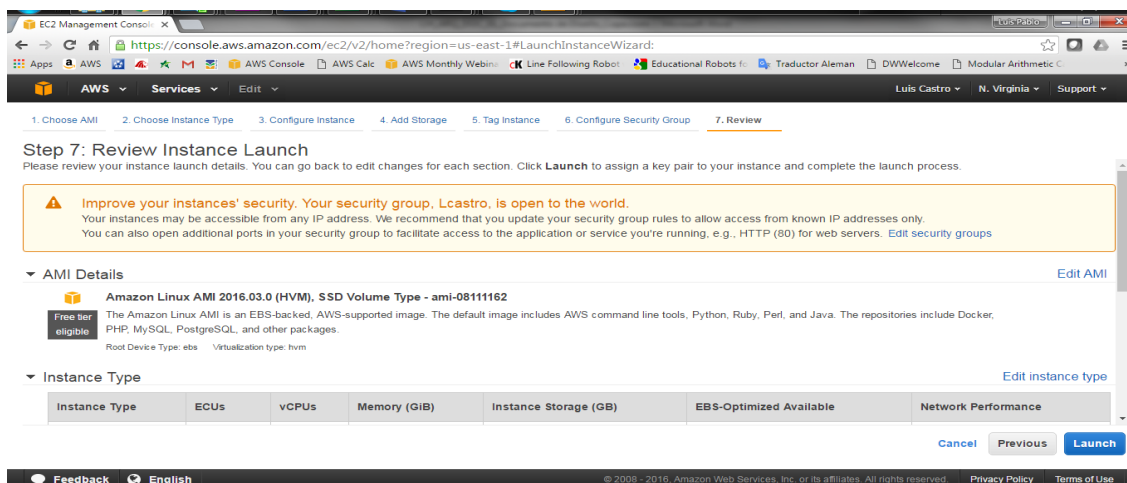
Select Create a new security group with the username, leave the default values and give Review and Launch



The screenshot shows the 'Step 6: Configure Security Group' page in the AWS Management Console. The page title is 'Step 6: Configure Security Group'. Below the title, there is a description of security groups and a link to 'Learn more'. The 'Assign a security group' section has two radio buttons: 'Create a new security group' (selected) and 'Select an existing security group'. The 'Security group name' field contains 'Lcastro' and the 'Description' field contains 'launch-wizard-4 created 2016-04-13T08:09:18.738-05:00'. Below these fields is a table with columns 'Type', 'Protocol', 'Port Range', and 'Source'. The table has one row with 'SSH' in the Type column, 'TCP' in the Protocol column, '22' in the Port Range column, and 'Anywhere | 0.0.0.0/0' in the Source column. Below the table is an 'Add Rule' button. A yellow warning box is present with the text: 'Warning: Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.' At the bottom right are buttons for 'Cancel', 'Previous', and 'Review and Launch'.

Step 9

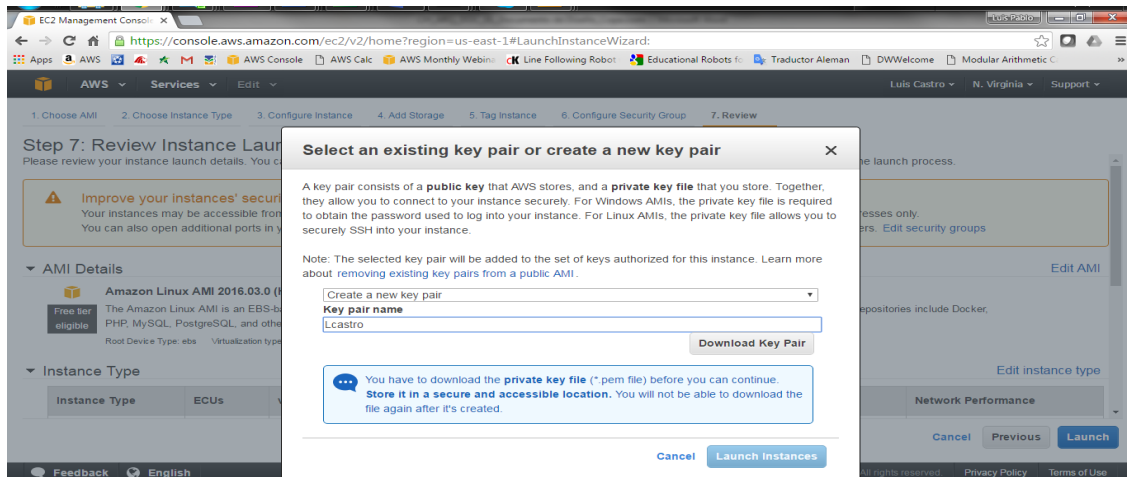
Review settings values and launch it



The screenshot shows the 'Step 7: Review Instance Launch' page in the AWS Management Console. The page title is 'Step 7: Review Instance Launch'. Below the title, there is a description of the review process and a link to 'Edit security groups'. A yellow warning box is present with the text: 'Improve your instances' security. Your security group, Lcastro, is open to the world. Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups'. Below the warning box is the 'AMI Details' section, which shows 'Amazon Linux AMI 2016.03.0 (HVM), SSD Volume Type - ami-08111162'. Below this is the 'Instance Type' section, which shows a table with columns 'Instance Type', 'ECUs', 'vCPUs', 'Memory (GiB)', 'Instance Storage (GB)', 'EBS-Optimized Available', and 'Network Performance'. At the bottom right are buttons for 'Cancel', 'Previous', and 'Launch'.

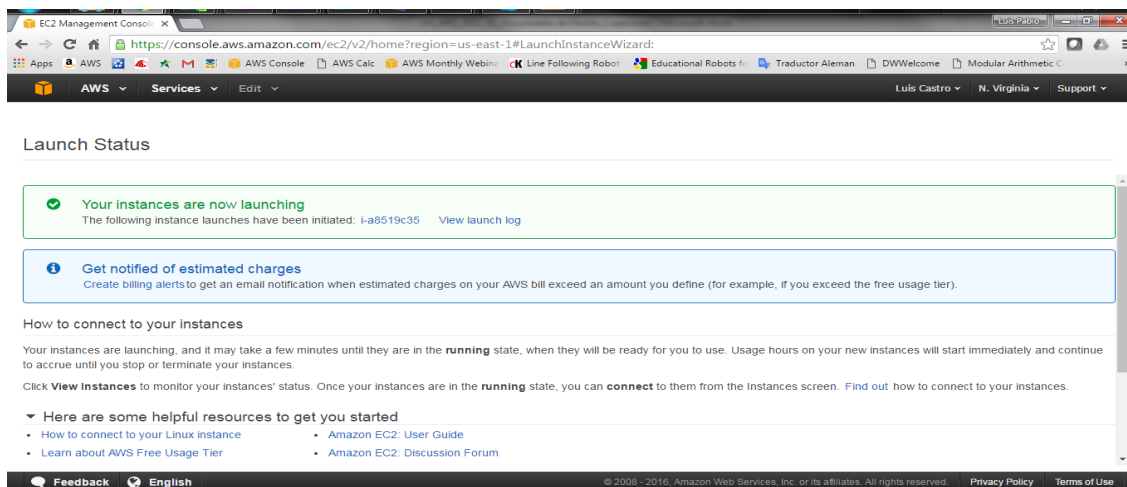
Step 10

Select create a new key pair and put the username, select download key pair and then Launch Instances, — Save this key !!



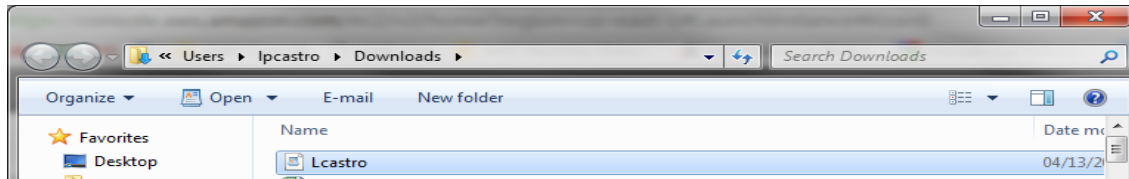
Step 11

Check the status of the created instance



Step 12

Validate that the Key Pair file is downloaded



(MacOs Only)

In the folder where the .pem file was downloaded run the following command (change the command with the name of your key):

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

Connect with the following command:

```
$ ssh -i "<nombre del PEM File>" ec2-user@<EC2_Public_IP address>
```

```
SJCMAC17JJHD4:~ lcastro$ cd downloads
SJCMAC17JJHD4:downloads lcastro$ chmod 400 lcastrose.pem
SJCMAC17JJHD4:downloads lcastro$ ssh -i "lcastrose.pem" ec2-user@ec2-54-167-101-226.compute-1.amazonaws.com
```

Purple
_ _ | _ _ | _)
_ | V C _ / Amazon Linux AMI
_ _ | _ _ | _ |

Laboratorio AWS Route53.docx May 17, 2018
Laboratorio AWS S3 & CloudFront.docx May 17, 2018
Laboratorio AWS VPC Rev 0.2.docx Apr 13, 2018
Laboratorio AWS VPC.docx May 13, 2018

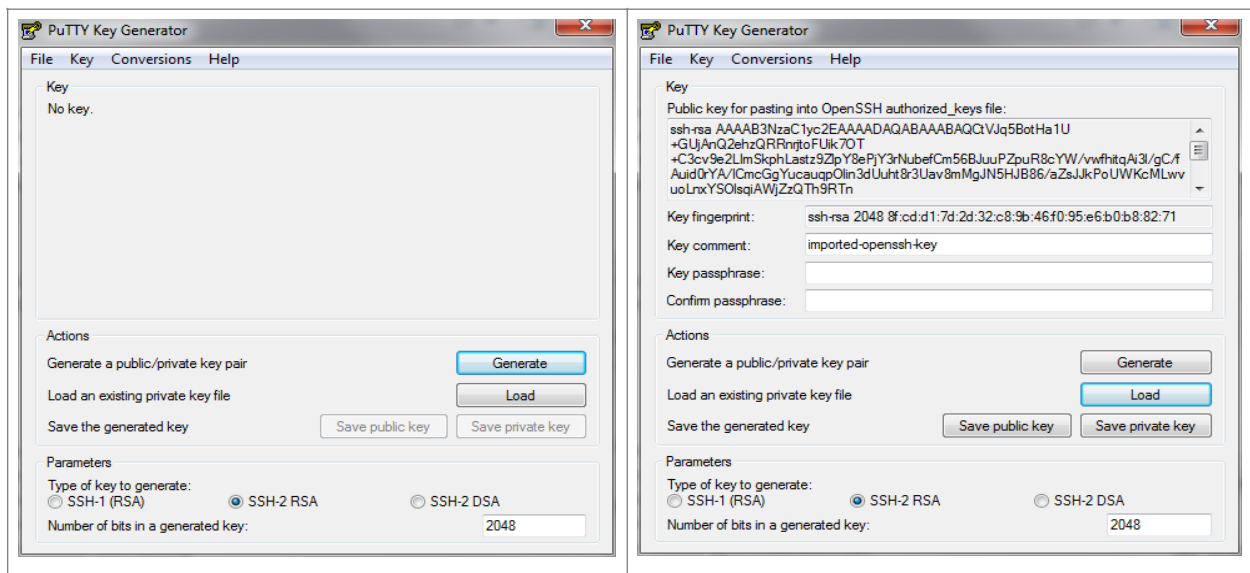
passed

```
https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/  
7 package(s) needed for security, out of 11 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-172-31-8-221 ~]$
```

(Windows Only)

Step 13

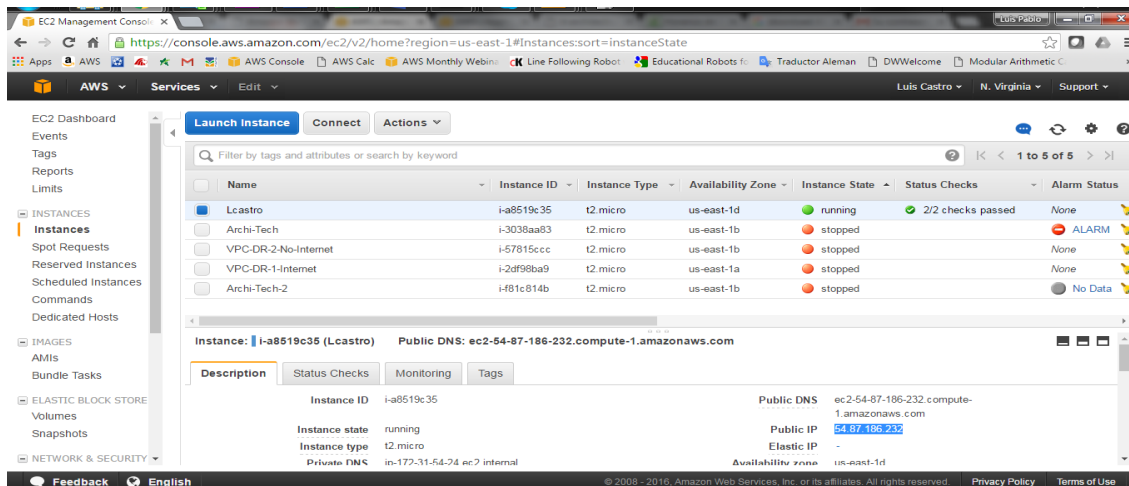
Open the PuttyGen and give it load and load the PEM file, then give it Save private Key and verify that the .ppk file has been generated



Step 14

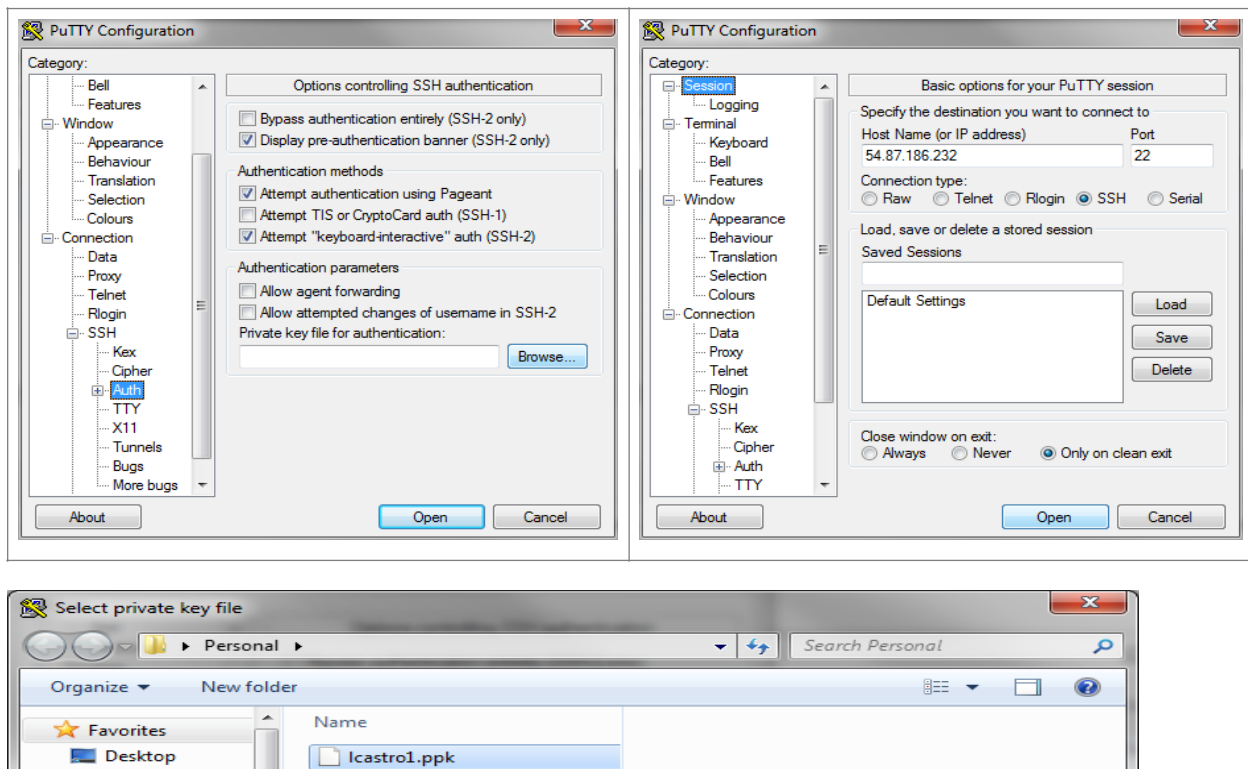
Validate the public IP address that was assigned to the EC2 instance

Note: Wait until the instance shows the status check as 2/2 passed



Step 15 (Windows Only)

Open the Putty Client, in the Connection> SSH> Auth field, select Browse the generated .ppk file and then go to Session and indicate the IP Address associated with the EC2 machine and give it Open



Step 16

To access the machine use the following user: ec2-user

Raise privileges using the following command:

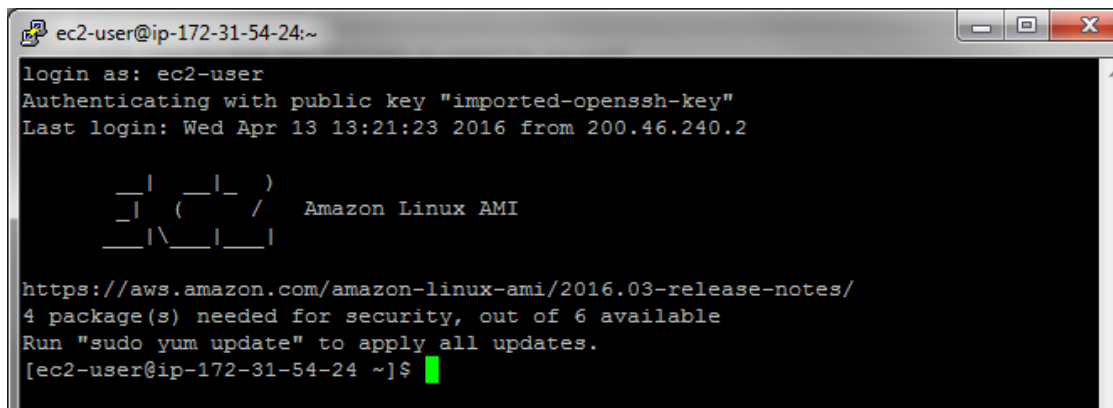
```
#sudo su
```

Update the instance

```
#yum update -y
```



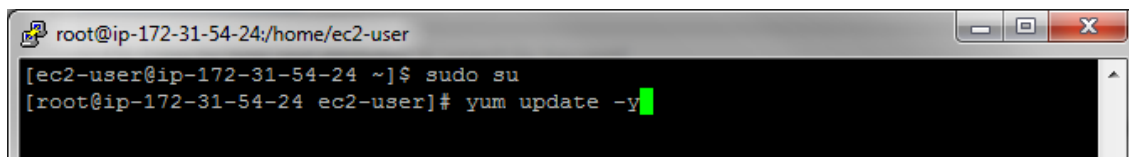
```
54.87.186.232 - PuTTY
login as: ec2-user
```



```
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]#
```