

Paso 1

Acceder a la consola de AWS mediante el siguiente link:

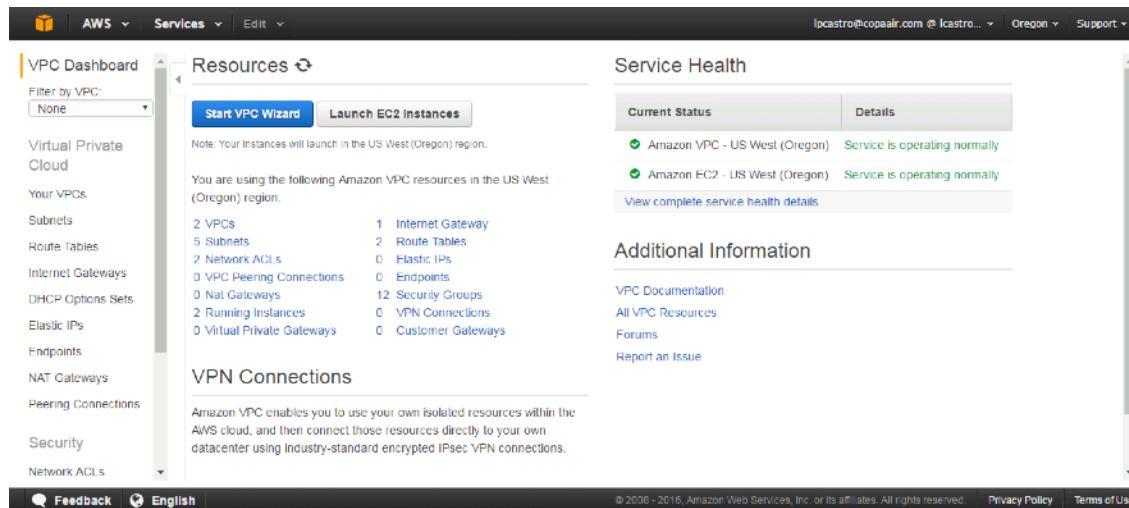
<https://lcastrose.signin.aws.amazon.com/console>

Paso 2

Acceder al servicio de VPC

You can have:

- Five Amazon VPCs per AWS account per Region
- Two hundred subnets per Amazon VPC
- Five Amazon VPC Elastic IP addresses per AWS account per Region
- One Internet Gateway per VPC
- Five Virtual Private Gateways per AWS account per Region
- Fifty Customer Gateways per AWS account per Region
- Ten IPsec VPN Connections per Virtual Private Gateway

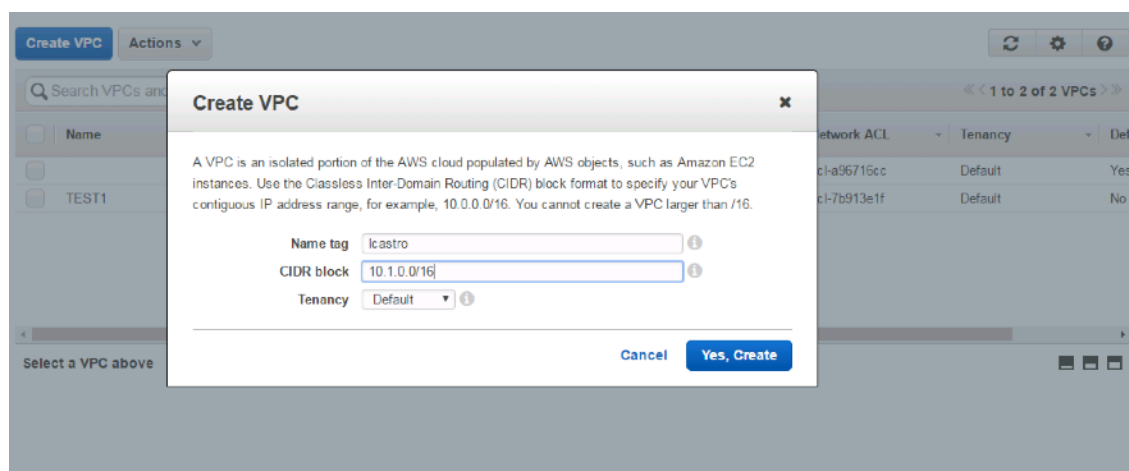


The screenshot shows the AWS VPC Dashboard. The left sidebar contains a navigation menu with options like Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections, Security, and Network ACLs. The main content area is titled 'Resources' and includes buttons for 'Start VPC Wizard' and 'Launch EC2 Instances'. It lists the following resources in the US West (Oregon) region: 2 VPCs, 5 Subnets, 2 Network ACLs, 0 VPC Peering Connections, 0 Nat Gateways, 2 Running Instances, 0 Virtual Private Gateways, 1 Internet Gateway, 2 Route Tables, 0 Elastic IPs, 0 Endpoints, 12 Security Groups, 0 VPN Connections, and 0 Customer Gateways. Below this is a section for 'VPN Connections' with a brief description. On the right, the 'Service Health' section shows that both Amazon VPC and Amazon EC2 are operating normally. At the bottom, there is a footer with 'Feedback', 'English', and copyright information for Amazon Web Services, Inc. (2008-2016).

Paso 3

Hacer click en Your VPCs y Create VPC

1. Name Tag:
 - a. Nombre de usuario
2. CIDR block:
 - a. Según asignación de Excel, ej:
 - i. 10.1.0.0/16
3. Tenancy:
 - a. Default



Create VPC Actions									
Search VPCs and their properties									
	Name	VPC ID	State	VPC CIDR	DHCP options set	Route table	Network ACL	Tenancy	Default
<input type="checkbox"/>		vpc-f1a2d294	available	172.31.0.0/16	dopt-8fc23fea	rtb-021d6567	acl-a96716cc	Default	Yes
<input checked="" type="checkbox"/>	Lcastro	vpc-42499526	available	10.1.0.0/16	dopt-8fc23fea	rtb-99ee54f2	acl-7b913e1f	Default	No

Paso 4

Hacer click en **Subnets** y **Create Subnet**

Crear dos subnets:

- 10.X.1.0/24
- 10.X.2.0/24

La “X” corresponde al CIDR asociado según el Excel

1. Name tag:

- Lcastro-1a (Primer Availability Zone)
- Lcastro-1b

2. VPC

- a. VPC con su Nombre de usuario

3. Availability Zone

- a. Ejemplo: Us-west 2a

4. CIDR block

- a. Ejemplo: 10.1.1.0/24

Create Subnet

Subnet Actions

Search Subnets

Name

icastro-west-2b

icastro-west-2a

subnet-862084e2 (10.1.3.0/24)

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.

Name tag

icastro-2a

VPC

vpc-42499526 (10.1.0.0/16) | Lcastro

Availability Zone

us-west-2a

CIDR block

10.1.3.0/24

Cancel

Yes, Create

<< 1 to 5 of 5 Subnets >>

Available IPs	Availability Zone	Route Table
091	us-west-2c	rtb-0
091	us-west-2a	rtb-0
091	us-west-2b	rtb-0
250	us-west-2b	rtb-9
250	us-west-2a	rtb-9

Create Subnet

Subnet Actions

Search Subnets and their prop

X

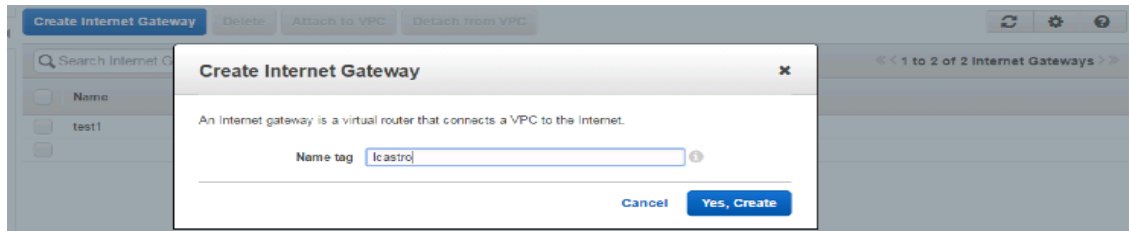
<< 1 to 5 of 5 Subnets >>

<input type="checkbox"/>	Name	Subnet ID	State	VPC	CIDR	Available IPs	Availability Zone	Route
<input checked="" type="checkbox"/>	lcastro-west-2b	subnet-277a8351	available	vpc-42499526 (10.1.0.0/16) Lcastro	10.1.2.0/24	250	us-west-2b	rtb-9
<input checked="" type="checkbox"/>	lcastro-west-2a	subnet-862084e2	available	vpc-42499526 (10.1.0.0/16) Lcastro	10.1.1.0/24	250	us-west-2a	rtb-9

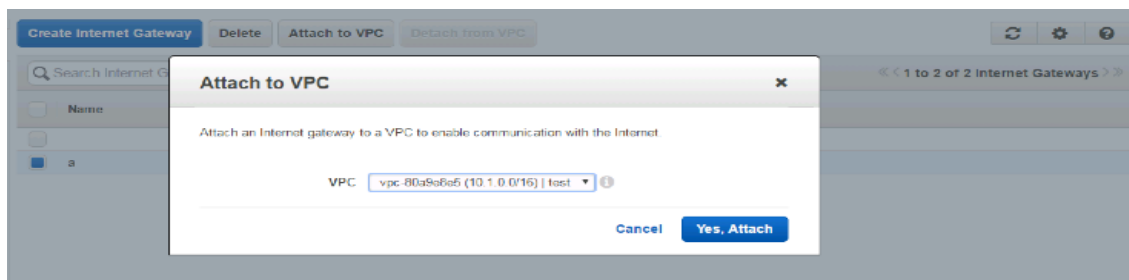
Paso 5

Hacer click en **Internet Gateways** y **Create Internet Gateways**

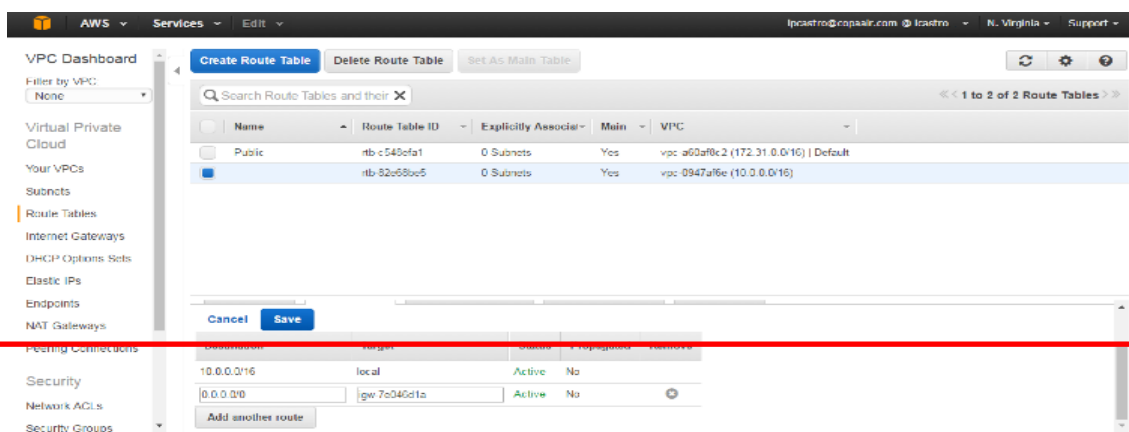
Crear el Internet Gateway con el nombre de usuario



Una vez creado marcarlo y darle click en **Attach to VPC**



Ir a **Route Table de la VPC creada (10.X.0.0/16)** y en **Routes** hacer click en **editar** y agregar el **Internet Gateway** creado con una **ruta default**, según como se muestra en la siguiente figura:



Ingresar a Compute>EC2 para la creación de máquinas EC2 pública y privada

1. Maquina Publica

a. Launch instance escoger Amazon Linux

b. Escoger General Purpose, next

c. Seleccionar

i. Network

1. VPC creado con nombre de usuario

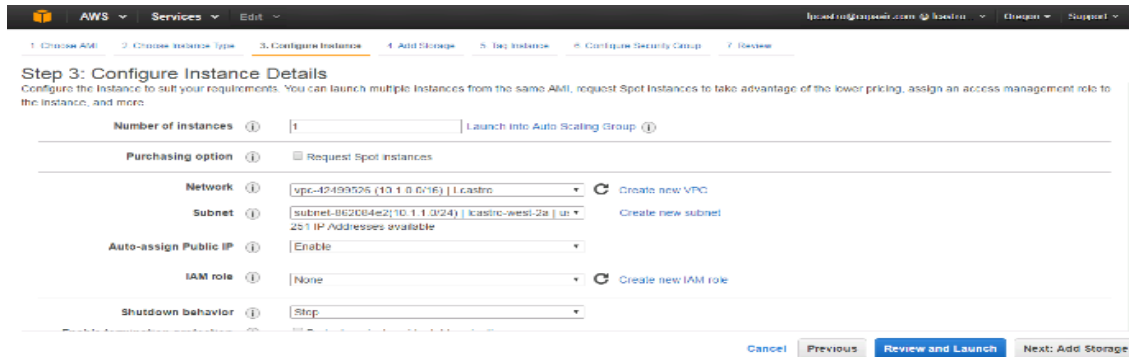
ii. Subnet

1. La que comienza con 10.X.1.0/24

iii. Auto-assign Public IP

1. Enable

iv. 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-42499526 (10.1.0.0/16) | lcastro Create new VPC

Subnet: subnet-8626b4e2 (10.1.1.0/24) | lcastro-west-2a | up Create new subnet
251 IP addresses available

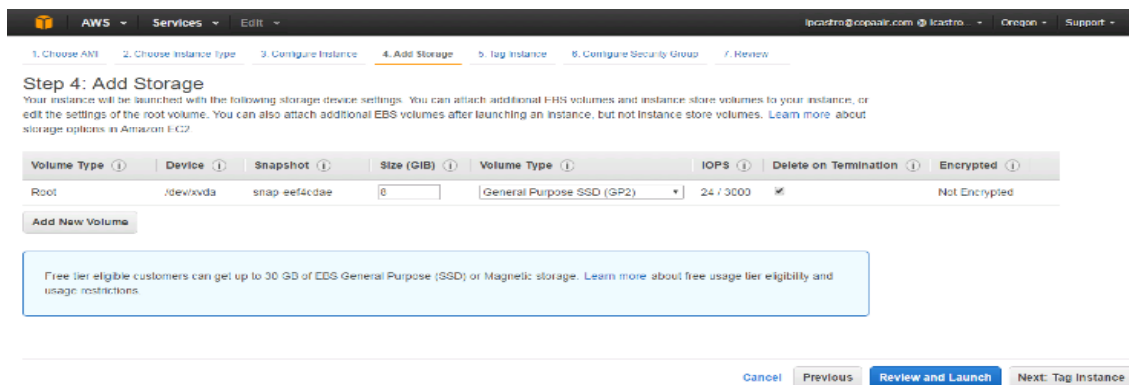
Auto-assign Public IP: Enable

IAM role: None Create new IAM role

Shutdown behavior: Stop

Buttons: Cancel Previous Review and Launch Next: Add Storage

d. Dejar configuración default en Add Storage



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-eef4cdae	8	General Purpose SSD (GP2)	24 / 3000	<input checked="" type="checkbox"/>	Not Encrypted

Buttons: Add New Volume Cancel Previous Review and Launch Next: Tag Instance

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.

e. Poner tag name Public_EC2



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 (127 characters maximum): Name Value (255 characters maximum): Public_EC2

Buttons: Create Tag (Up to 10 tags maximum) Cancel Previous Review and Launch Next: Configure Security Group

f. Crear un nuevo Security Group con la configuración default con el nombre de usuario más VPC: ej; lcastrovpv

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere 0.0.0.0/0

[Add Rule](#)

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.

[Cancel](#) [Previous](#) [Review and Launch](#)

g. Crear un nuevo key pair con el nombre de usuario mas vpc, ej: lcastrovpc

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

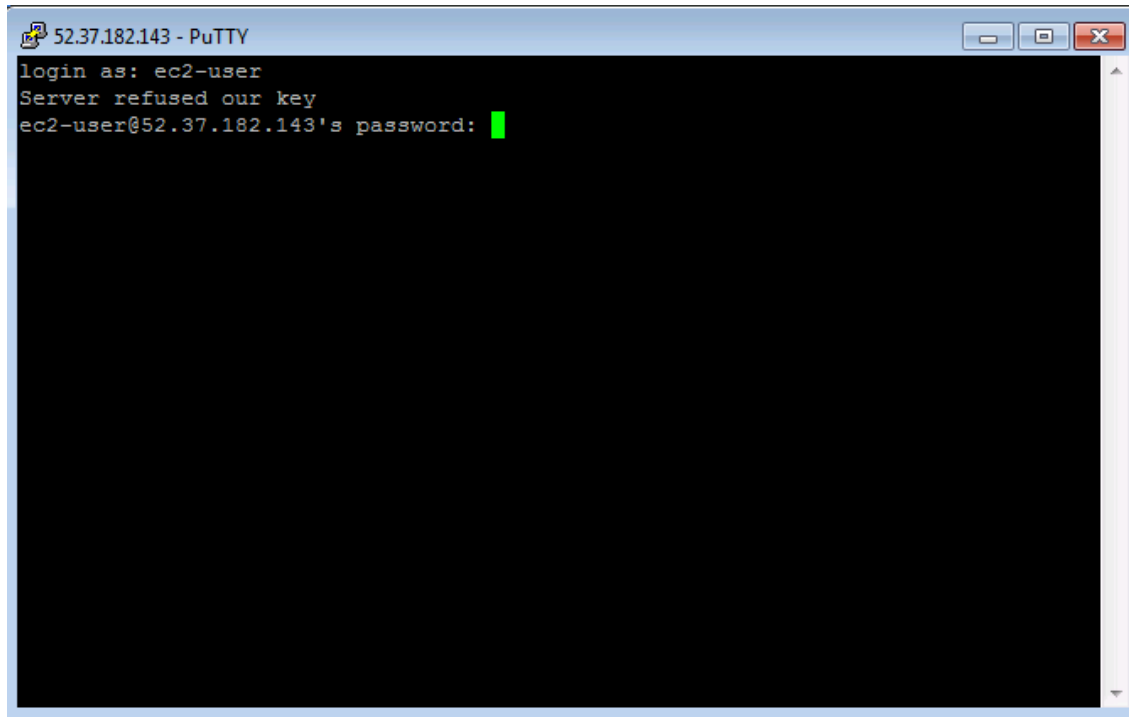
Key pair name

[Download Key Pair](#)

You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.

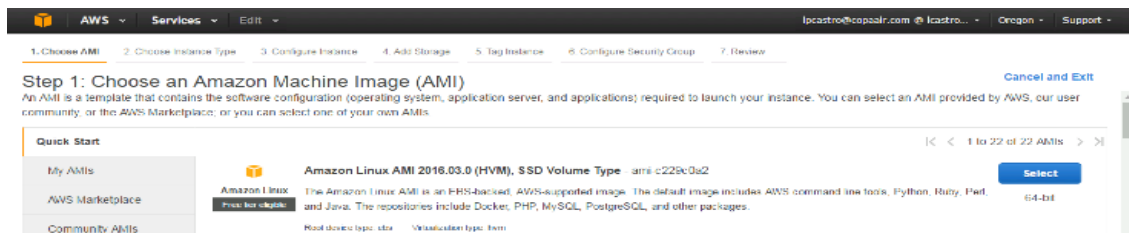
[Cancel](#) [Launch Instances](#)

h. Ingresar a la maquina vía ssh y deje la sesión abierta para utilizarla en el siguiente paso

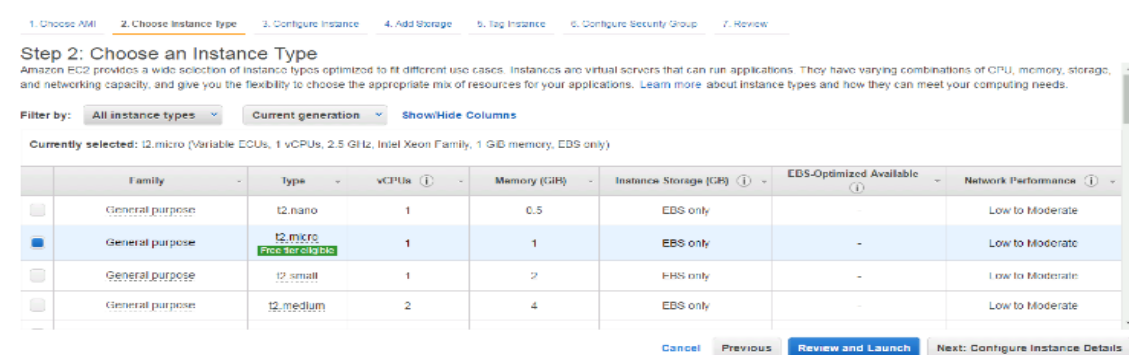


2. Maquina Privada

a. Launch instance escoger Amazon Linux



b. Escoger General Purpose, next



c. Seleccionar

i. Network

1. VPC creado con nombre de usuario

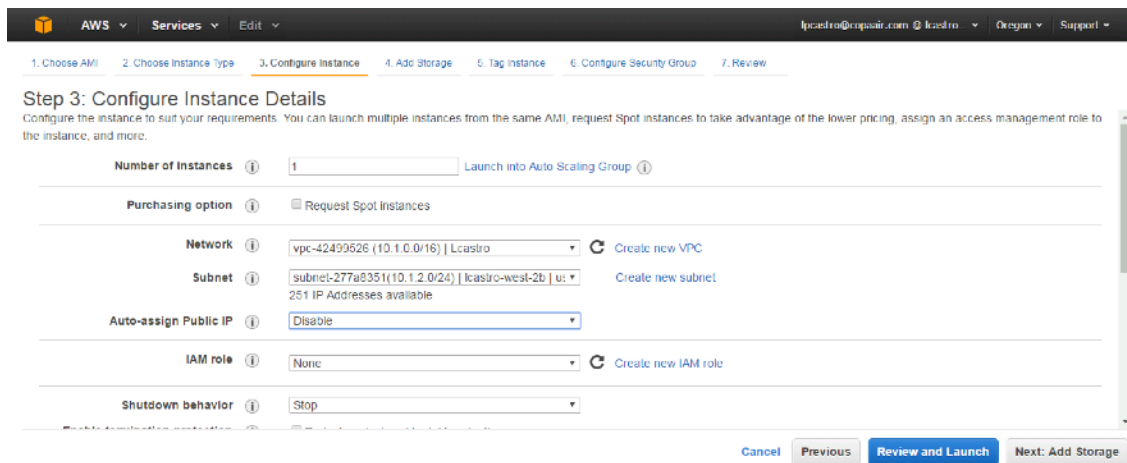
ii. Subnet

1. La que comienza con 10.X.2.0/24

iii. Auto-assign Public IP

1. Disable

iv. 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-42499626 (10.1.0.0/16) | Lcastro [Create new VPC](#)

Subnet: subnet-277a8351 (10.1.2.0/24) | lcastro-west-2b | us [Create new subnet](#)
251 IP Addresses available

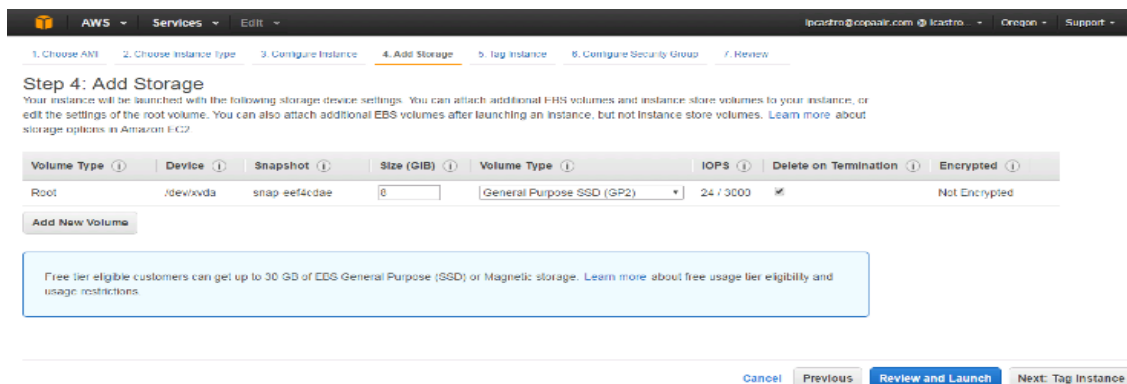
Auto-assign Public IP: Disable

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

Shutdown behavior: Stop

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

d. Dejar configuración default en Add Storage



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.

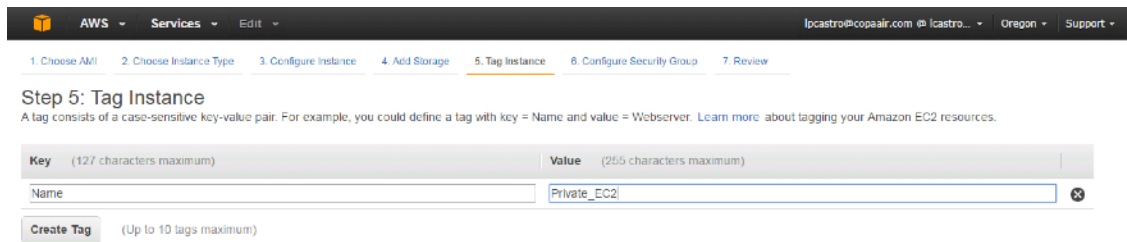
Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/xvda	snap-eef4cdae	8	General Purpose SSD (GP2)	24 / 3000	<input checked="" type="checkbox"/>	<input type="checkbox"/> Not Encrypted

[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](#)

e. Poner tag name Private_EC2

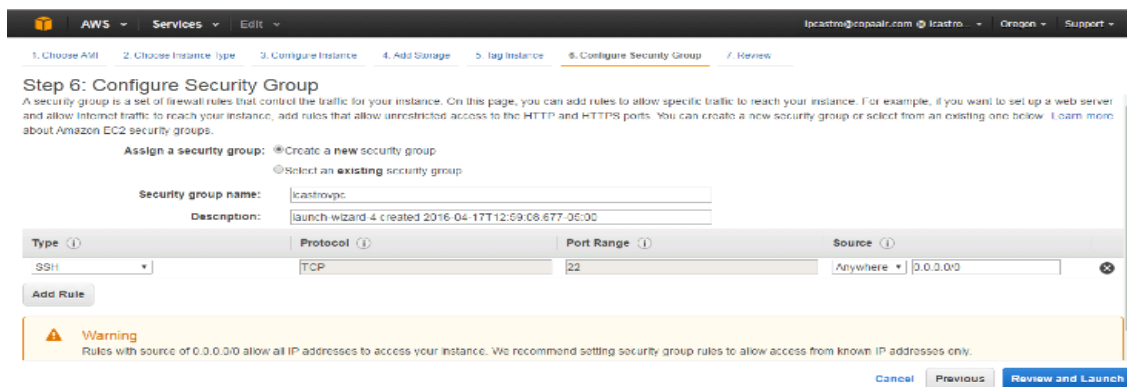


Step 5: Tag Instance
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)
Name	Private_EC2

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

f. Utilice el Security Group creado en el paso anterior: ej; lcastrovpc



Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name:
Description:

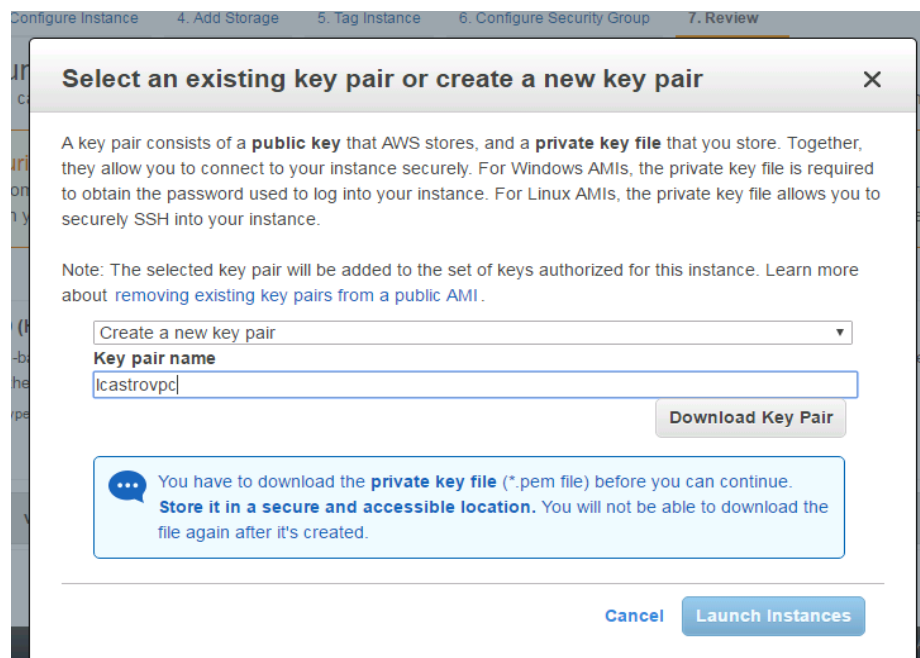
Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere 0.0.0.0/0

[Add Rule](#)

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.

[Cancel](#) [Previous](#) [Review and Launch](#)

g. Crear un nuevo key pair con el nombre de usuario mas vpc, ej: lcastrovpc



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more](#) about [removing existing key pairs from a public AMI](#).

Create a new key pair

[Download Key Pair](#)

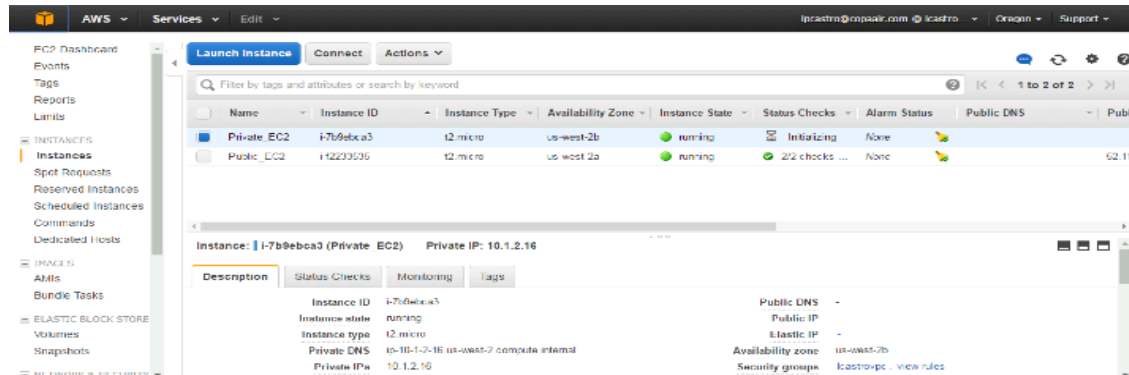
You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.

[Cancel](#) [Launch Instances](#)

h. Ingresar a la maquina mediante la sesión SSH de la maquina Publica_EC2

i. Verifique la dirección privada asignada a esta maquina

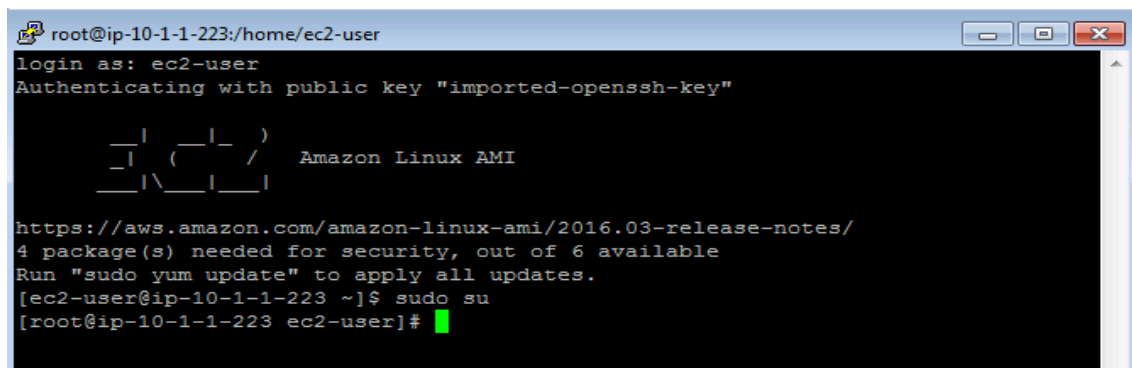
1. Ejemplo: 10.1.1.16



ii. Abra la sesión SSH de la maquina Public_EC2

1. Eleve los privilegios mediante el comando

a. `#sudo su`

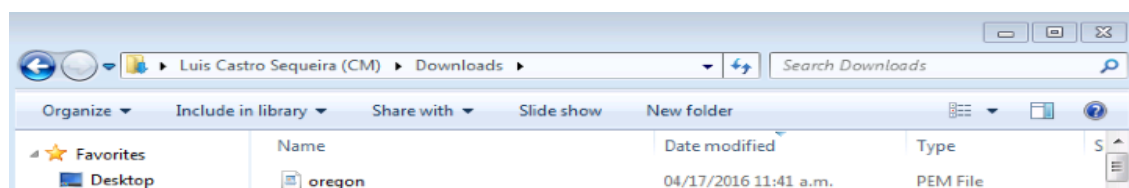


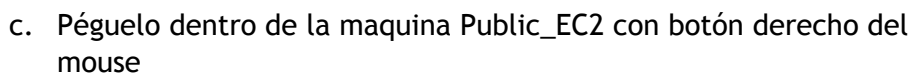
iii. Cree un archivo .pem directamente en esta máquina EC2

1. Utilice el comando

a. `#nano lcastrovpc.pem` (use su nombre de usuario)

b. Abra el archivo .pem descargado, cópielo con `ctrl+c`





```

root@ip-10-1-1-223:/home/ec2-user
GNU nano 2.3.1 File: lcastroaws.pem Modified
2wWRRHKEUhfISUQnucT2VjLeYN50CgYEAzXCcRqOD3eRmxReJpArtpxXSH5aeYAApCacEyPrUBeR5
fZ2v0ieZ+v5xTYagP8Jfy/8ULCaC3K7BJEih10hehBcYYaGOFc7FavoN4phRbafGHTzsUagbBDdD
phk4xAVA0Kh7kwNCgngghPSh4p+14NNN0shR+ZL4UYvrBdLUwU7MCgYEAzVm7MDctmDNBbFxXn30H
MeCsmIKk76mNgc7cMDUFeSn22TEDsALumBXNndodqUNy0z60ap/z4YFCOHG0A7ArcitCYOyf+0UrG
ZO000zHFXz+1WlbVA9aY7fH9Iw5QnyQ6DgQQGpk3ANaABzF+GtiDTkfViw0xL+EBp409vvgYSQ8C
gYADQC3o3GH8R9nscnFmGZorE6hQgaSd5kK/+VmVCIsEUNovR4sbay7/jrkiPegZOiy6jp22GSHm
9gjuVwvfVVTriEAFg3XpGG19RNmLZT2cm5QB8G3Y200cgvdaEHoad+7PnmreJ6YMxHPaMOK/3X0S
cOoeYz44v904t7k7J7LgICwKBgA20PoStrWIZk2rvHV03fpiJFZ7jOj9iizzLG22Bt7ZGGA6jwv+X
y7kLKhQDL5JLxeS85vhwE1Xl+JX+PYdZidcfajrU5MgXEYtAYidBa25g8ieceloNaDlYkh7BeZuh
BN/XtAJTyxWjuLsKSQ2PDZA+uv25eC3G4XmIgVO+0ZtvAoGAa/XvFVCQuAdOvbY398/0FbzLxaCx
I/T7PwiVYiEDUJoCGLr7bJkG5lzEv19YDxsIqmST7zGaJxm6tbtYXYx3iMyKQSmvzAVqrFnmooZd
MsVvilwpV0S8u1NNiMeutM+nF8BOF3A+fkdLvHAKL8w2xGk7AIJX7yw7T6wRfHu6Qc=
-----END RSA PRIVATE KEY-----

Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
Y Yes
N No ^C Cancel
  
```

e. Cambie los privilegios del archivo mediante el siguiente comando

i. `# chmod 600 lcastroaws.pem`

```

root@ip-10-1-1-223:/home/ec2-user
[root@ip-10-1-1-223 ec2-user]# chmod 600 lcastroaws.pem
[root@ip-10-1-1-223 ec2-user]#
  
```

f. Ingrese a la maquina Private_EC2 vía SSH desde la maquina Public EC2 con el siguiente comando

i. `#ssh -i lcastroaws.pem ec2-user@10.1.2.16`

(Esta IP Address depende de la que haya sido designada en su caso)

```

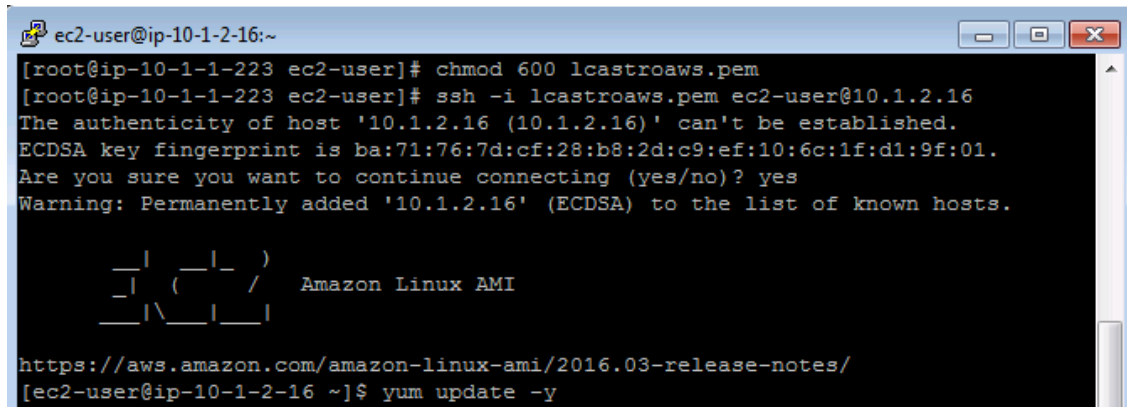
root@ip-10-1-1-223:/home/ec2-user
[root@ip-10-1-1-223 ec2-user]# chmod 600 lcastroaws.pem
[root@ip-10-1-1-223 ec2-user]# ssh -i lcastroaws.pem ec2-user@10.1.2.16
The authenticity of host '10.1.2.16 (10.1.2.16)' can't be established.
ECDSA key fingerprint is ba:71:76:7d:cf:28:b8:2d:c9:ef:10:6c:1f:d1:9f:01.
Are you sure you want to continue connecting (yes/no)? yes
  
```

g. Ejecute el siguiente comando

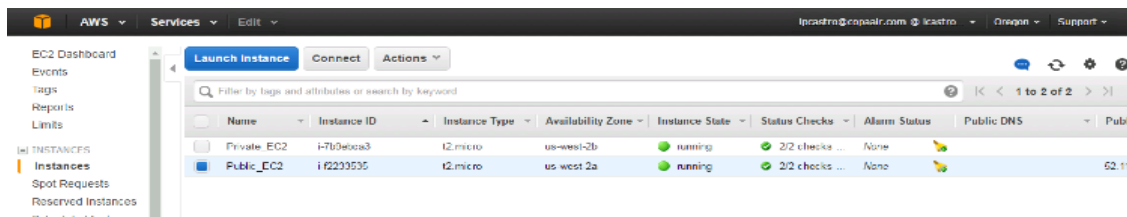
i. `#sudo su`

ii. `#yum update -y`

1. Verifique si es válido realizar el Update
2. Utilice el mando
 - a. **#ping 4.2.2.2** - Para validar que tenga acceso a internet
 - b. No debe de ser exitoso el ping ya que la maquina no tiene internet asociado



```
ec2-user@ip-10-1-2-16:~  
[root@ip-10-1-1-223 ec2-user]# chmod 600 lcastroaws.pem  
[root@ip-10-1-1-223 ec2-user]# ssh -i lcastroaws.pem ec2-user@10.1.2.16  
The authenticity of host '10.1.2.16 (10.1.2.16)' can't be established.  
ECDSA key fingerprint is ba:71:76:7d:cf:28:b8:2d:c9:ef:10:6c:1f:d1:9f:01.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '10.1.2.16' (ECDSA) to the list of known hosts.  
  
  _ | _ | _ )  
  _ | ( _ | /  
  _ | \ _ | _ |  
Amazon Linux AMI  
  
https://aws.amazon.com/amazon-linux-ami/2016.03-release-notes/  
[ec2-user@ip-10-1-2-16 ~]$ yum update -y
```

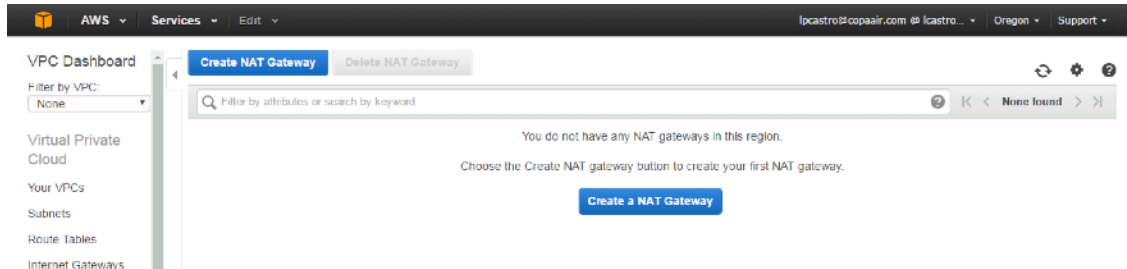


Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
Private_EC2	i-7f0e6ca3	t2.micro	us-west-2b	running	2/2 checks ...	None	
Public_EC2	i-f2235535	t2.micro	us-west-2a	running	2/2 checks ...	None	52.11

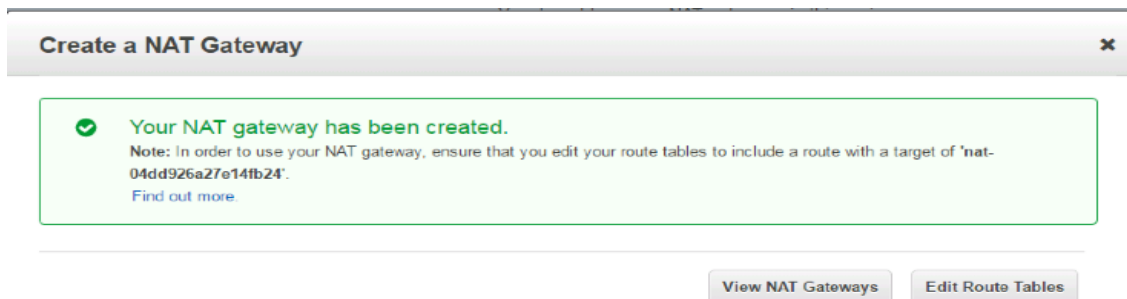
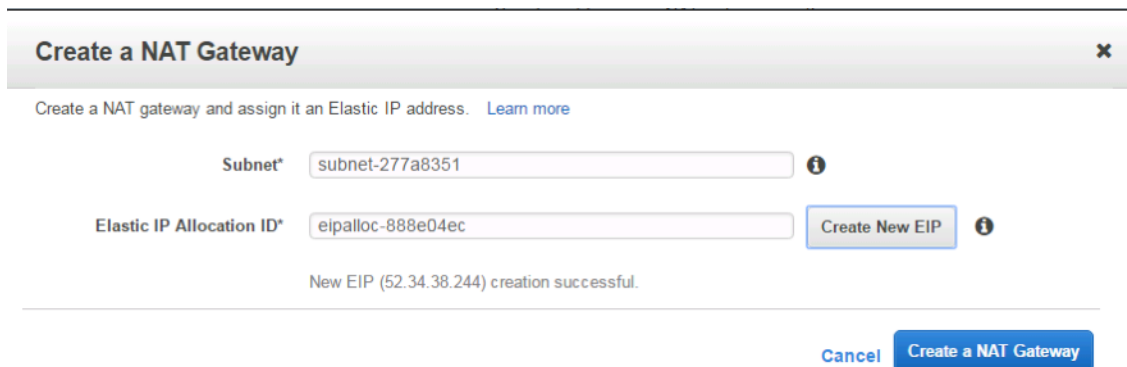
Paso 7

Darle acceso a la maquina privada para que pueda acceder a Internet mediante un NAT Gateway

- Ingresar a VPC>NAT Gateways>Create NAT Gateways



1. Escoger la subred publica 10.X.1.0
2. Create New Elastic IP
3. Create NAT Gateway



Paso 8

- Crear un Route Table para la Subred Privada llamado user+private
 - o Ej: lcastro-private
- Editar el Route Table de la subred privada
 - o Crear una ruta default hacia el NAT Gateway Creado

VPC Dashboard

Filter by VPC:
Select a VPC

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
Icastro	rtb-0d8245e693bddc9a	subnet-0fbb0bbcfdf3cea8	-	Yes	vpc-00c49a909224a3434 Icastro
Private	rtb-0eec1bdf74dc70a70	subnet-05c36c218640fac3	-	No	vpc-00c49a909224a3434 Icastro
rtb-82e68be5		-	-	Yes	vpc-0947af6e DNS Test
Public	rtb-c548efa1	-	-	Yes	vpc-a50af8c2 Default

Route Table: rtb-0eec1bdf74dc70a70

- Summary
- Routes**
- Subnet Associations
- Edge Associations
- Route Propagation
- Tags

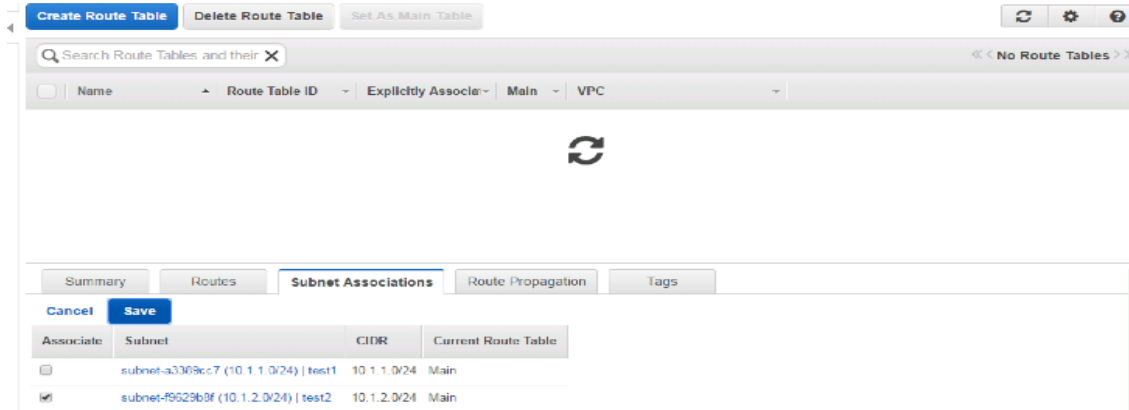
Edit routes

View All routes

Destination	Target	Status	Propagated
10.1.0.0/16	local	active	No
0.0.0.0/0	nati-0ca5def624aab26d8	active	No

- Hacer click en **Routes y Edit**
- Agregar una ruta default
 - **Destination**
 - 0.0.0.0/0
 - **Target**
 - Nat Gateway - Creado
 - **Save**

- Seguidamente Asociar la subred 10.X.2.0/24
 - Subnet Associations
 - Save



Search Route Tables and their X

<< No Route Tables >>

Summary Routes **Subnet Associations** Route Propagation Tags

Cancel Save

Associate	Subnet	CIDR	Current Route Table
<input type="checkbox"/>	subnet-a3369cc7 (10.1.1.0/24) test1	10.1.1.0/24	Main
<input checked="" type="checkbox"/>	subnet-9629b9f (10.1.2.0/24) test2	10.1.2.0/24	Main

Paso 9

Desde la maquina Privada ejecutar los siguientes comandos

- #sudo su
- #yum Update -y

```

root@ip-10-1-2-203:/home/ec2-user

Install ( 1 Dependent package)
Upgrade 7 Packages

Total download size: 35 M
Downloading packages:
(1/8): java-1.7.0-openjdk-1.7.0.99-2.6.5.0.66.amzn1.x86_64.rpm | 32 MB 00:00
(2/8): libXcomposite-0.4.3-4.6.amzn1.x86_64.rpm | 21 kB 00:00
(3/8): libssh2-1.4.2-2.13.amzn1.x86_64.rpm | 134 kB 00:00
(4/8): nano-2.5.3-1.19.amzn1.x86_64.rpm | 798 kB 00:00
(5/8): openssh-6.6.1p1-25.61.amzn1.x86_64.rpm | 552 kB 00:00
(6/8): openssh-clients-6.6.1p1-25.61.amzn1.x86_64.rpm | 1.0 MB 00:00
(7/8): openssh-server-6.6.1p1-25.61.amzn1.x86_64.rpm | 487 kB 00:00
(8/8): sysctl-defaults-1.0-1.1.amzn1.noarch.rpm | 3.1 kB 00:00
-----
Total 43 MB/s | 35 MB 00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Updating : openssh-6.6.1p1-25.61.amzn1.x86_64 1/15
  Installing : libXcomposite-0.4.3-4.6.amzn1.x86_64 2/15
  Updating : 1:java-1.7.0-openjdk-1.7.0.99-2.6.5.0.66.amzn1.x86_64 3/15

```

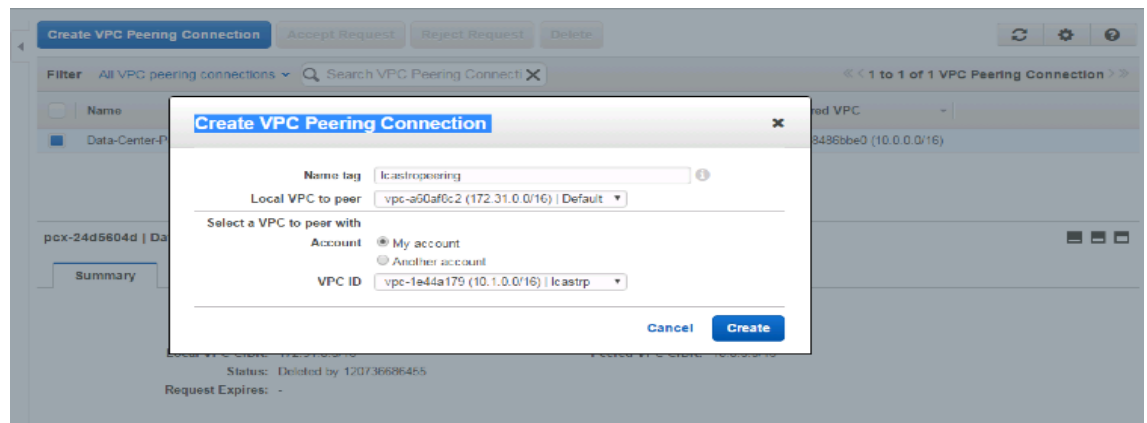
Paso 10

Desde la maquina privada haga ping a la IP Address según su Región - No debe de resultar exitoso

- **Virginia:**
 - o 172.31.56.69
- **Oregon**
 - o 172.31.38.154
- **Carolina**
 - o 172.31.28.106
- **Ohio**
 - o 172.31.43.211

Acceder a VPC>Peering Connections>Create VPC Peering Connections

- **Name tag**
 - o Nombre de usuario mas peering, ej: lcastropeering
- **Local VPC to Peer**
 - o VPC Default
- **VPC ID**
 - o VPC creado - 10.X.0.0/16



- Accept Request

Create VPC Peering Connection

Accept Request

Reject Request

Delete

Filter

All VPC peering connections

Search VPC Peering Connections

<< 1 to 2 of 2 VPC Peering Connections >>

<input type="checkbox"/>	Name	ID	Status	Local VPC	Peered Account ID	Peered VPC
<input type="checkbox"/>	Data-Center-Peering	pcx-24d5604d	Deleted by 1...	vpc-a60af8c2 (172.31.0.0/16...	120736686455	vpc-8486bbe0 (10.0.0.0/16)
<input checked="" type="checkbox"/>	Icastropeering	pcx-be9825d7	Pending Acc...	vpc-a60af8c2 (172.31.0.0/16...	120736686455	vpc-1e44a179 Icastrp

- Modify my route tables now

Accept VPC Peering Connection Request✕

Your VPC Peering Connection has been established!

To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables. [Learn more about route tables](#).

[Modify my route tables now](#)

[Close](#)

- Seleccionar el VPC Default y agregar una nueva ruta
 - Edit
 - Destination
 - 10.X.0.0/16
 - Target
 - Pcx-be982 (Validar el Peering Asociado)
 - Save

Create Route TableDelete Route TableSet As Main Table

Search Route Tables and their

<< 1 to 3 of 3 Route Tables >>

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associat	Main	VPC
<input checked="" type="checkbox"/>	Public	rtb-c548efa1	0 Subnets	Yes	vpc-af0af0c2 (172.31.0.0/16) Default
<input type="checkbox"/>	NAT	rtb-05ae3682	1 Subnet	Yes	vpc-1e44a179 (10.1.0.0/16) Icastrip
<input type="checkbox"/>	Pub	rtb-a6aa36cf	1 Subnet	No	vpc-1e44a179 (10.1.0.0/16) Icastrip

rtb-c548efa1 | Public

Summary

Routes

Subnet Associations

Route Propagation

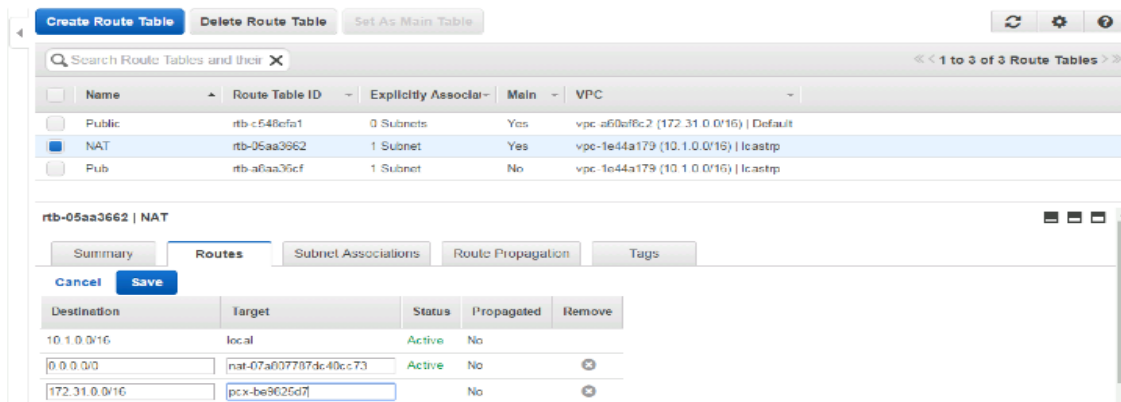
Tags

Cancel

Save

Destination	Target	Status	Propagated	Remove
172.31.0.0/16	local	Active	No	
0.0.0.0/0	igw-183212fd	Active	No	
10.1.0.0/16	pcx-bc9825d7	No	No	

- Seleccionar los VPCs creados en la red 10.X.0.0/16 y agregar una nueva ruta
 - o Edit
 - Destination
 - 172.31.0.0/16
 - Target
 - Pcx-be982 (Validar el Peering Asociado)
 - Save



Desde la maquina privada haga ping a la IP Address según su Región

```
^C
--- 172.31.31.182 ping statistics ---
149 packets transmitted, 56 received, 62% packet loss, time 148790ms
rtt min/avg/max/mdev = 0.524/0.679/3.006/0.321 ms
[root@ip-10-1-2-203 ec2-user]# ping 172.31.31.182
PING 172.31.31.182 (172.31.31.182) 56(84) bytes of data.
64 bytes from 172.31.31.182: icmp_seq=1 ttl=255 time=0.519 ms
64 bytes from 172.31.31.182: icmp_seq=2 ttl=255 time=0.550 ms
64 bytes from 172.31.31.182: icmp_seq=3 ttl=255 time=0.546 ms
64 bytes from 172.31.31.182: icmp_seq=4 ttl=255 time=0.578 ms
64 bytes from 172.31.31.182: icmp_seq=5 ttl=255 time=0.687 ms
64 bytes from 172.31.31.182: icmp_seq=6 ttl=255 time=0.529 ms
64 bytes from 172.31.31.182: icmp_seq=7 ttl=255 time=0.682 ms
64 bytes from 172.31.31.182: icmp_seq=8 ttl=255 time=0.664 ms
64 bytes from 172.31.31.182: icmp_seq=9 ttl=255 time=0.577 ms
64 bytes from 172.31.31.182: icmp_seq=10 ttl=255 time=0.615 ms
```