

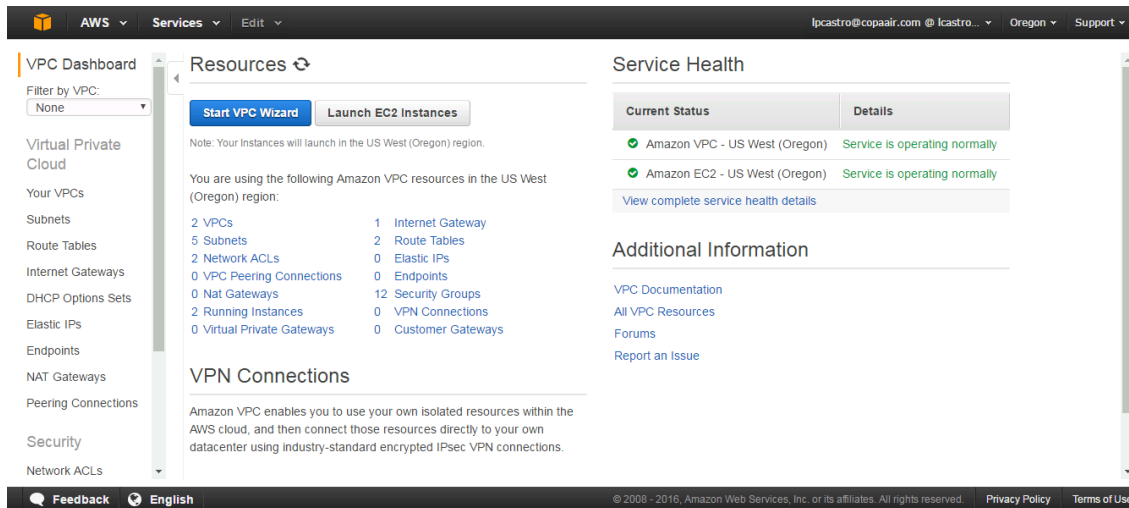
Step 1

Access the AWS console through the following link:

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

Step 2

Access the VPC service



The screenshot shows the AWS VPC Dashboard for the account 'lpcastro@copair.com' in the 'Oregon' region. The left sidebar contains a navigation menu with categories 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 various VPC resources: 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 - US West (Oregon)' and 'Amazon EC2 - US West (Oregon)' are operating normally. At the bottom, there is a footer with 'Feedback', 'English', copyright information, and links to 'Privacy Policy' and 'Terms of Use'.

Step 3

Click on Your VPCs & Create VPC

1. Name Tag:

- Username

2. CIDR block:

- According Excel File, ex:
 - 10.1.0.0/16

3. Tenancy:

- Default

The screenshot shows the AWS Management Console interface. In the foreground, a 'Create VPC' modal dialog is open. The dialog has a title bar with a close button (X). Below the title, there is a descriptive paragraph about VPCs. Underneath, there are three input fields: 'Name tag' with the value 'lcastro', 'CIDR block' with the value '10.1.0.0/16', and 'Tenancy' with a dropdown menu set to 'Default'. Each input field has an information icon (i) to its right. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Yes, Create'. The background shows a blurred view of the VPC console, including a search bar, a table of VPCs, and a 'Create VPC' button in the top left.

Create VPC

Actions

<< 1 to 2 of 2 VPCs >>

<input type="checkbox"/>	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-96ee54f2	acl-7b913e1f	Default	No

Step 4

Make click en Subnets & Create Subnet

Create two subnets:

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

The "X" corresponds to the associated CIDR according to Excel

- 1. Name tag:**
 - a. Lcastro-1a (Primer Availability Zone)
 - b. Lcastro-1b
- 2. VPC**
 - a. VPC with your username
- 3. Availability Zone**
 - a. Example: Us-west 2a
- 4. CIDR block**
 - a. Example: 10.1.1.0/24

Create Subnet

Subnet Actions

Search Subnets

Name

lcastro-west-2b

lcastro-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

lcastro-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
4091	us-west-2c	rtb-0...
4091	us-west-2a	rtb-0...
4091	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

<< 1 to 5 of 5 Subnets >>

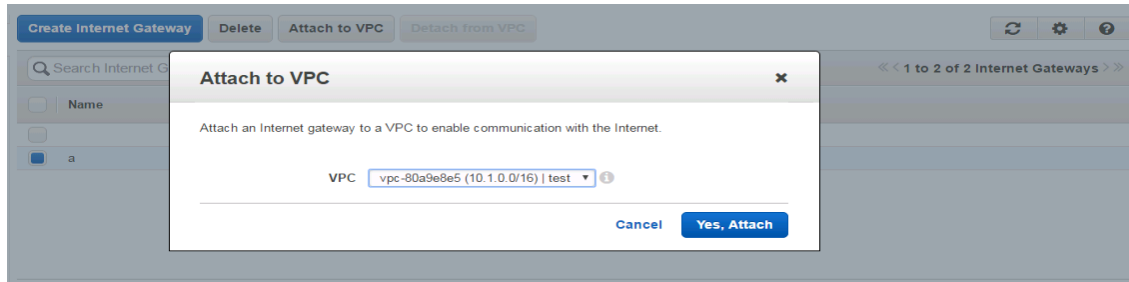
	Name	Subnet ID	State	VPC	CIDR	Available IPs	Availability Zone	Route
<input checked="" type="checkbox"/>	lcastro-west-2b	subnet-277a8351	available	vpc-42499526 (10.1.0.0/16) Lcastro	10.1.2.0/24	250	us-west-2b	rtb-9
<input checked="" type="checkbox"/>	lcastro-west-2a	subnet-862084e2	available	vpc-42499526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

Step 5

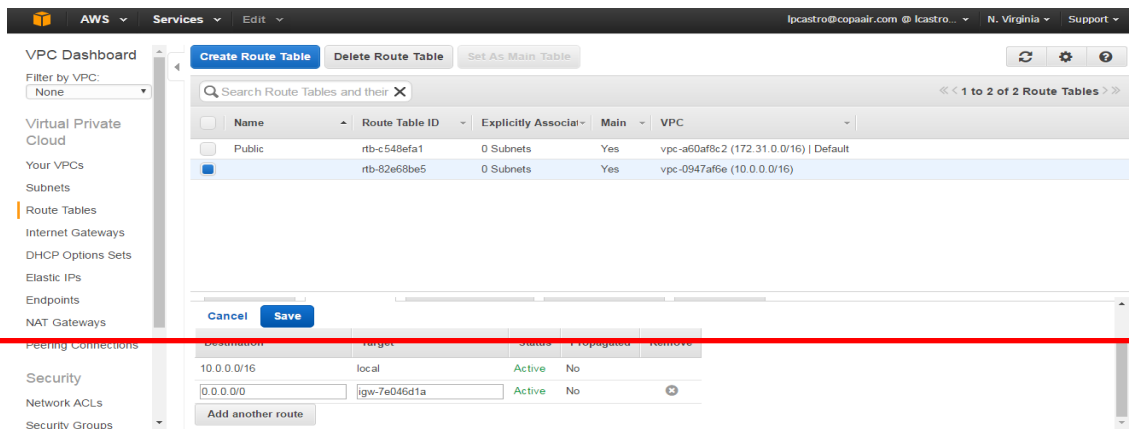
Click on Internet Gateways and Create Internet Gateways

Create the Internet Gateway with the username

Once created, mark it and click Attach to VPC

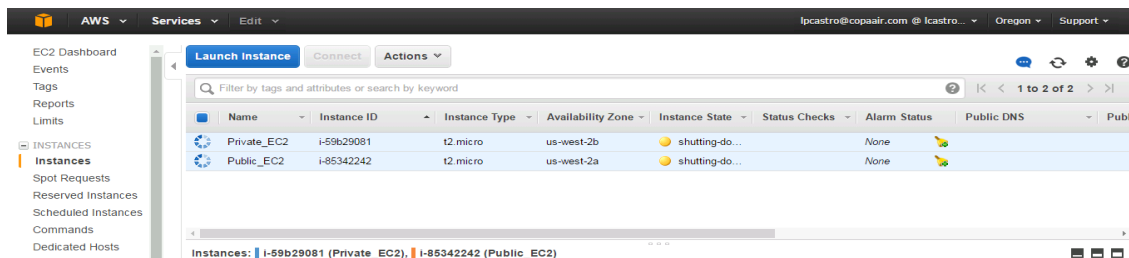


Go to the Route Table of the created VPC (10.X.0.0 / 16) and in Routes click on edit and add the created Internet Gateway with a default route, as shown in the following figure:



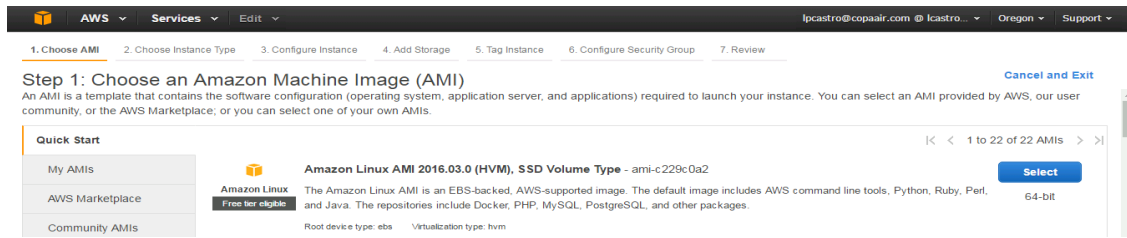
Step 6

Enter Compute> EC2 to create public and private EC2 machines



1. Public Instance

a. Launch instance choose Amazon Linux



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start

My AMIs | AWS Marketplace | Community AMIs

Amazon Linux AMI 2016.03.0 (HVM), SSD Volume Type - ami-c229c0a2

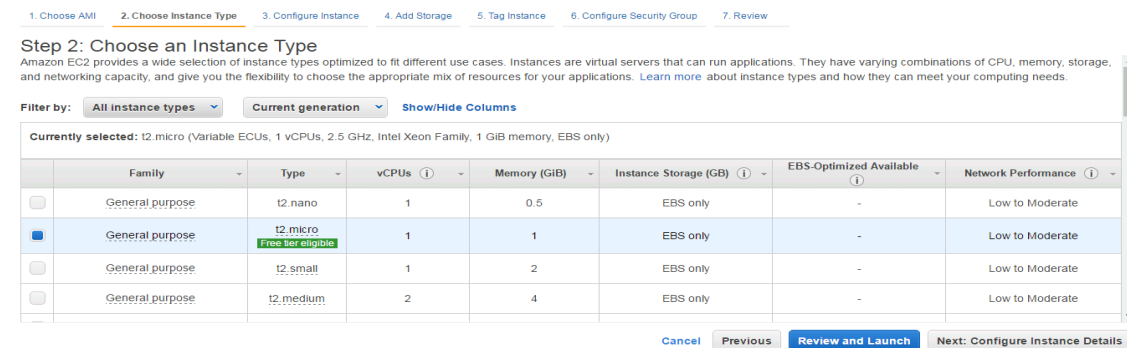
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root device type: ebs | Virtualization type: hvm

64-bit

Select

b. Choose General Purpose, next



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 (GB)	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	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

Review and Launch | Next: Configure Instance Details

c. Select

i. Network

1. Choose VPC with username

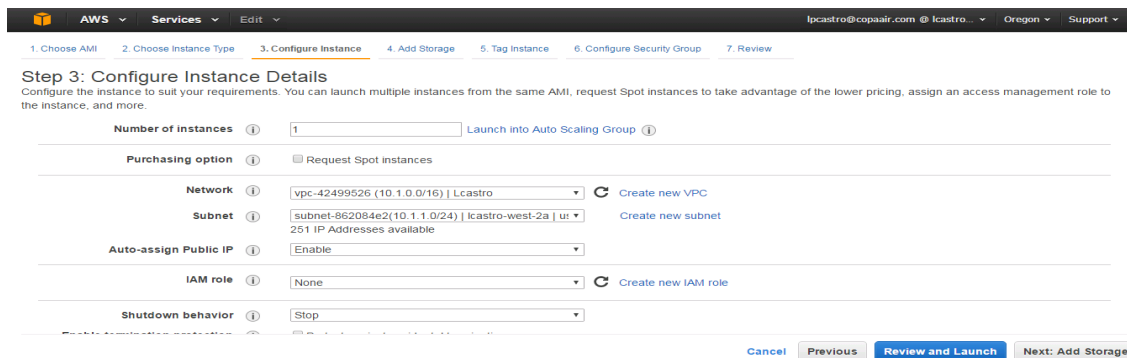
ii. Subnet

1. Starts with 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-862084e2 (10.1.1.0/24) | lcastro-west-2a | us | Create new subnet

Auto-assign Public IP: Enable

IAM role: None | Create new IAM role

Shutdown behavior: Stop

Review and Launch | Next: Add Storage

d. Dejar configuraci3n default en Add Storage

AWS

Services

lpcastro@copair.com

@ lpcastro...

Oregon

Support

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage

5. Tag Instance

6. Configure Security Group

7. Review

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	<input type="text" value="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.

e. Put tag name **Public_EC2**

AWS

Services

Edit

lpcastro@copaair.com

lcastro...

Oregon

Support

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage

5. Tag Instance

6. Configure Security Group

7. Review

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)
<input type="text" value="Name"/>	<input type="text" value="Public_EC2"/>
<div>Create Tag (Up to 10 tags maximum)</div>	

Cancel

Previous

Review and Launch

Next: Configure Security Group

- f. Create a new Security Group with the default configuration with the username plus VPC:
eg; lcastrovpc

AWS

Services

▼

Ed

▼

ipcastro@copaair.com

@ ipcastro...

Oregon

▼

Support

▼

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage

5. Tag Instance

6. Configure Security Group

7. Review

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 ✕

Warning

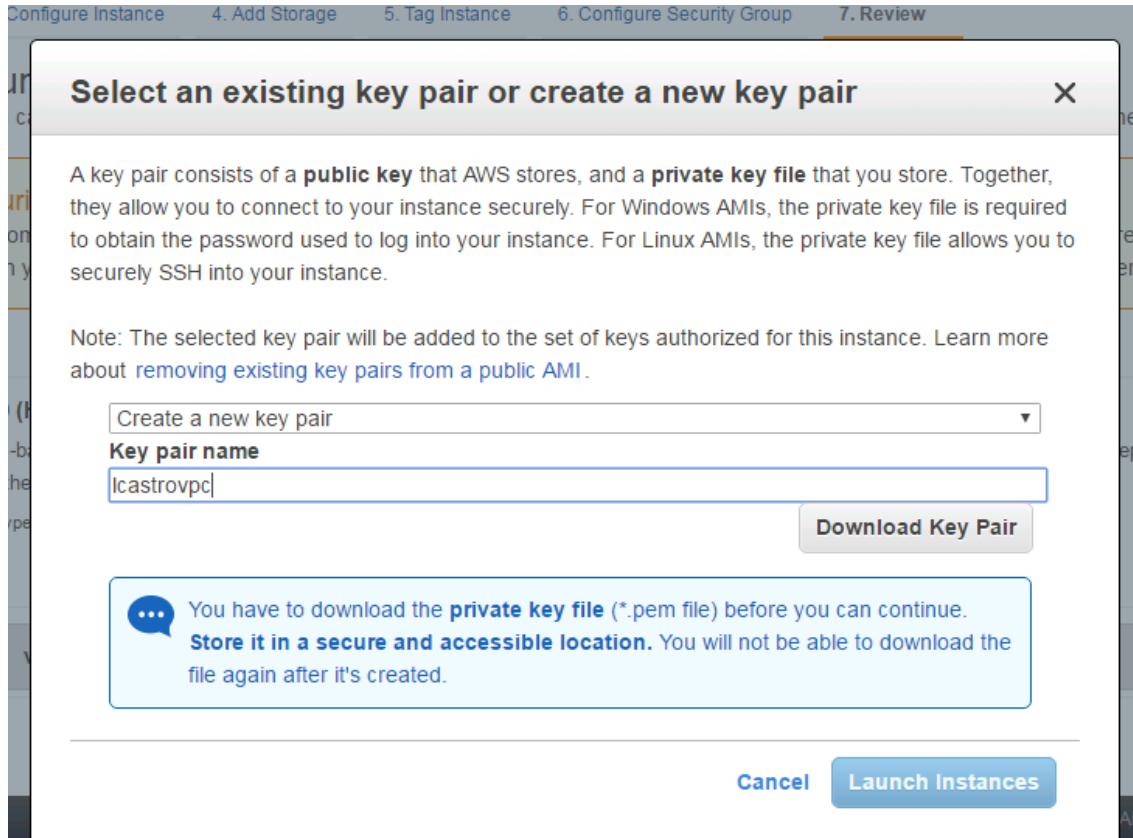
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel

Previous

Review and Launch

- g. Create a new key pair with the username plus vpc, eg: lcastrovpc



Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

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

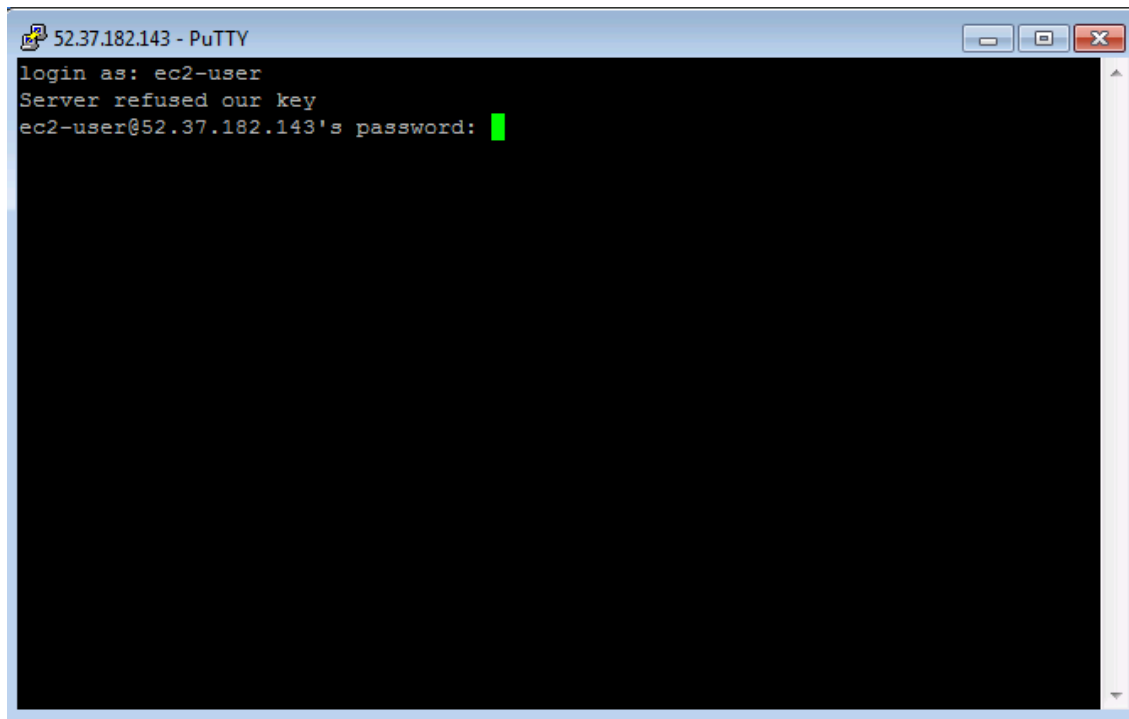
lcastrovpc

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.

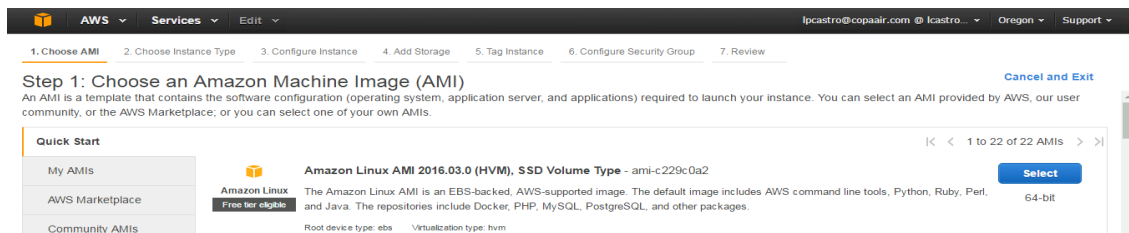
Cancel Launch Instances

h. Enter the machine via ssh and leave the session open to use it in the next Step

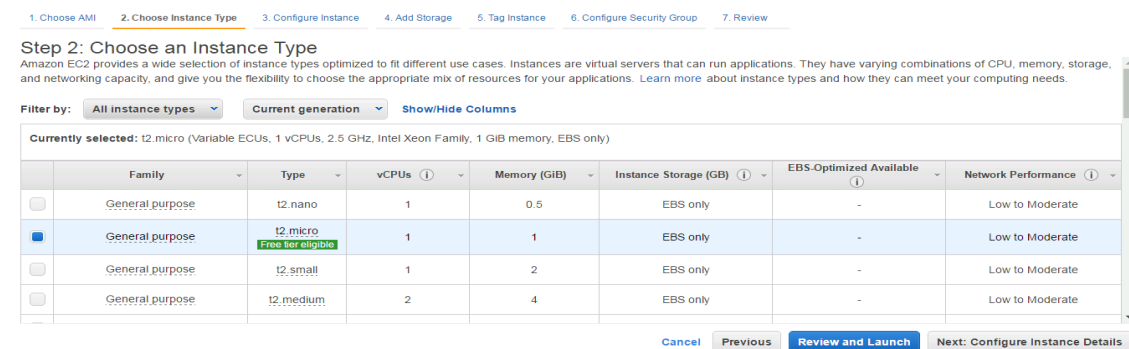


2. Private Instance

a. Launch instance choose Amazon Linux



b. Choose General Purpose, next



c. Select

i. Network

1. VPC created with username

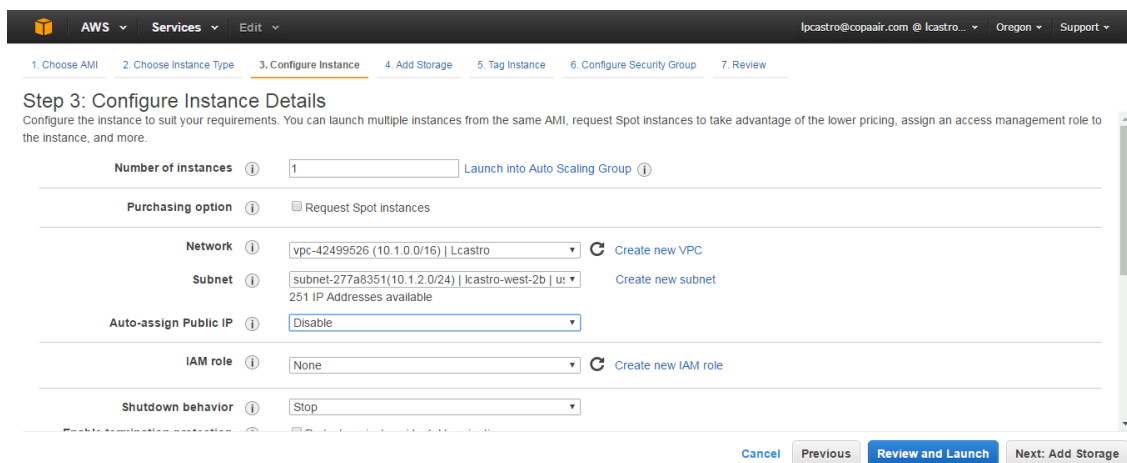
ii. Subnet

1. Starts with 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-42499526 (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

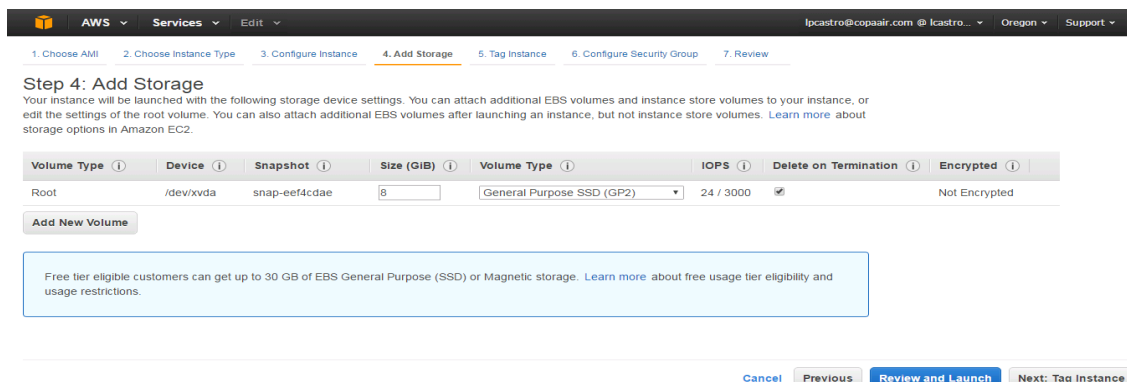
Auto-assign Public IP Disable

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

Shutdown behavior Stop

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

d. Leave default configuration in 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.

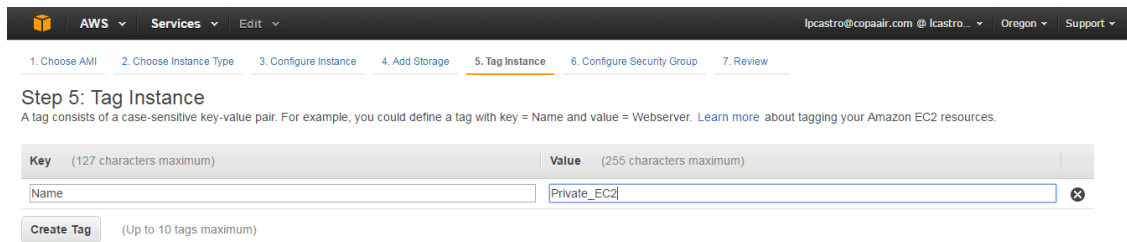
Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/xvda	snap-eef4cdae	8	General Purpose SSD (GP2)	24 / 3000	<input checked="" type="checkbox"/>	Not Encrypted

[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. Put tag name Private_EC2

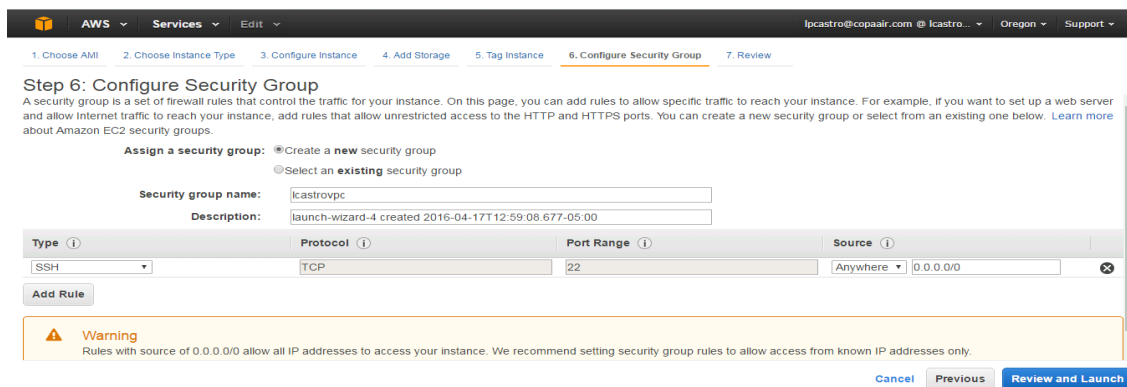


Step 5: Tag Instance
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

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

Create Tag (Up to 10 tags maximum)

f. Use the Security Group created in the previous step: eg; lcastrovpvc



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: lcastrovpvc
Description: launch-wizard-4 created 2016-04-17T12:59:08.677-05:00

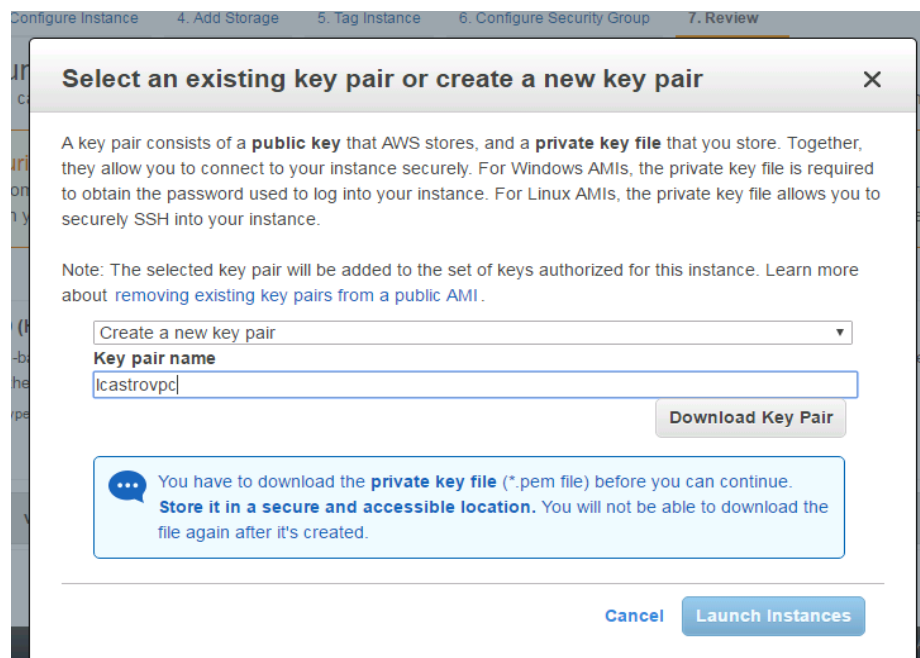
Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere 0.0.0.0/0

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. Create a new key pair with the username plus vpc, eg: lcastrovpvc



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](#).

Key pair name

Download Key Pair

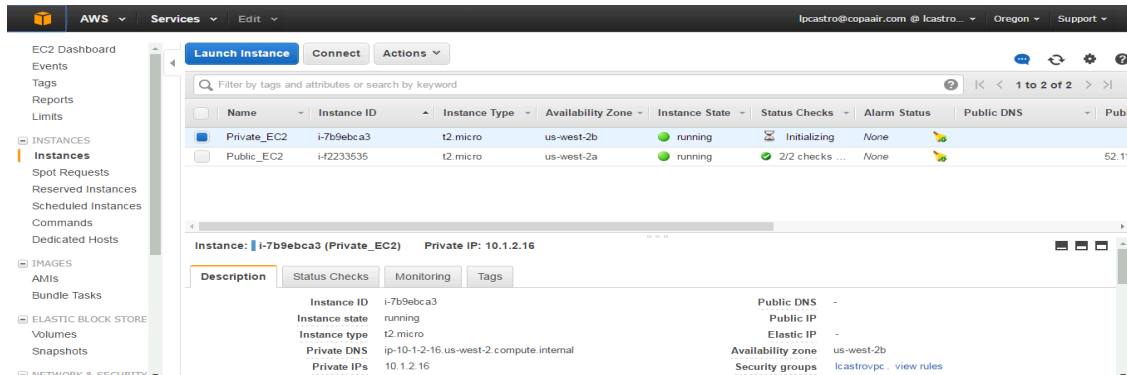
You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.

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

h. Enter the machine through the SSH session of the machine Publica_EC2

i. Check the private address assigned to this machine

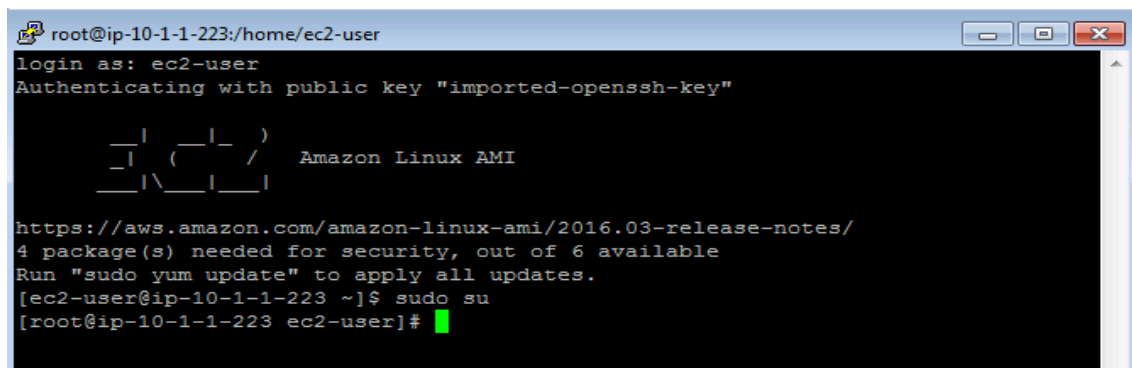
1. Example: 10.1.1.16



ii. Open the SSH session of the machine Public_EC2

1. Elevate privileges using the command

a. `#sudo su`

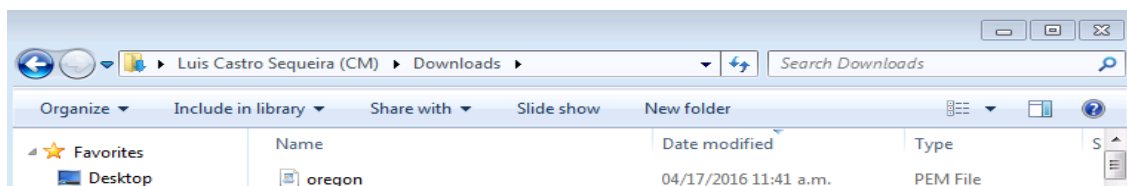


iii. Create a .pem file directly on this EC2 machine

1. Use the command

a. `# nano lcastrovpc.pem` (use your username)

b. Open the downloaded .pem file, copy it with `ctrl + c`



```

-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAQCAQEA5lLeayWtiOf51lyKf1Wg9;Eau2q1NRyglq/VH3S1U2JE187V
TJ0u011IPtHu
Vj5k67V+QxmiF5V
512C8p8dowwF74t8spuzmDwUC4eKhwQ8mAdHtG42KabbadM7iyM3Nm/
zshDUj2JVK6YHx1DapeR14/7cv7oHFAADY7ixQy2R6ChP12V9b170THw4Bm6fu
9k2x0b1D8t1x
ticiedqg8KDYougxpWQ+XuH8C1164m/giw1U1A1OW611hxiVvSh6EFq0Fq7XWXP
C2K90wcyEL2
mDgX04FOctg+HoPasWDBA6itH1HoqUBYM5Jmkxawxcu]D4pnryfQIDAQAABAAQIB
ACVE19tQyeC9
pby8LL28b1e/RfnR0nBN/31xWAMQcx02FrqS4hRai+yo0yBntC4YhbcQLL7HNF
KTCU9QqX32o
kV81wb1NHMB:FA0r0qJnGMRmJcqt;B116dW2YhBY4uqkAwm8jLE0rQF2QpYq9nH
gft6g/mlK12R
aLvtLPq2e/1e49AOKg8G
+2qjrlae3EUIBoLoOf68z8;FGyWd5UHJ7Wyt++qUAR4Yyfa4C1sKY+
3KTF6g060NOMptY6PnaFWkrlYxnmIDuFria3udFChpmk3PepAA+woXBfJwxTF/AX
Cis7EE*8AVHW
2wRHKEUHfISUQnucT2V;LeYN50CgYEAzXCcRq0D3eRmxReJpArtpxXSH5aeYAApCacEyPrUBeR5
CacEyPrUBeR5
-----END RSA PRIVATE KEY-----
  
```

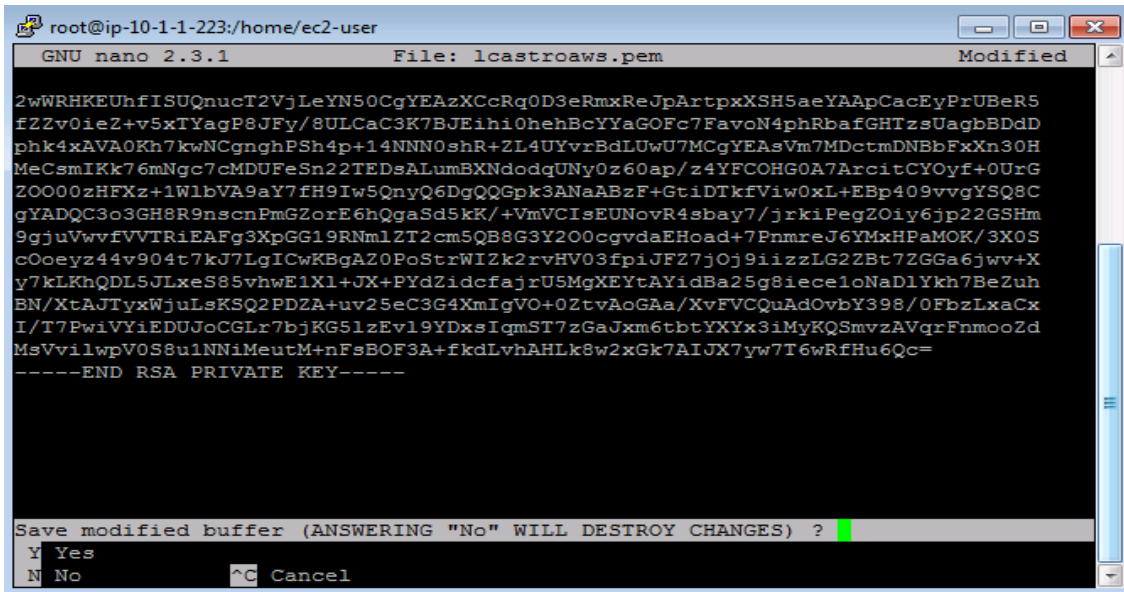
c. Paste it into the Public_EC2 machine with right mouse button

```

root@ip-10-1-1-223:/home/ec2-user
GNU nano 2.3.1      File: lcastroaws.pem      Modified

2wWRHKEUHfISUQnucT2V;LeYN50CgYEAzXCcRq0D3eRmxReJpArtpxXSH5aeYAApCacEyPrUBeR5
fZZv0ieZ+v5xTYagP8JFy/8ULCaC3K7BJEihi0hehBcYyAGOFc7FavON4phRbafGHTzsUagbBDDd
phk4xAVAOKh7kWNCGnghPSh4p+14NNN0shR+ZL4UYvrBdLUU7MCGYEA5Vm7MDctmDNBbFxxN30H
MeCsmIKk76mNgc7cMDUFeSn22TEdsALumBXNdodgUNY0z60ap/z4YFCOHGOA7ArcitCYOyf+0UrG
ZOO00zHFXz+1WlbVA9aY7fH9Iw5QnyQ6DgQQGpk3ANaABzF+GtiDTkfVivOxL+EBp409vvgYSQ8C
gYADQC3o3GH8R9nscnFmGZorE6hQgaSd5kK/+VmVCIseUNovR4sbay7/jrkiPegZOiy6jp22GSHm
9gjuVwvfVVTriEAFg3XpGG19Rnm1ZT2cm5QB8G3Y200cgvdaEHoad+7PnmreJ6YMxHPaMOK/3X0S
cOoeYz44v904t7k7J7LgICwKBgAZOPoStrWI2k2rvHV03fpiJFZ7jOj9iizzLG2ZBt7ZGGA6jwv+X
y7kLKhQDL5JLxeS85vhwE1X1+JX+PYdZidcfajrU5MgXEYtAYidBa25g8iece1oNaD1Ykh7BeZuh
BN/XtAJTyxWjuLsKSQ2PDZA+uv25eC3G4XmIgVO+0ZtvAoGAa/XvFVCQuAdOvbY398/0FbzLxaCx
I/T7PwiVYiEDUJoCGLr7bjKG51zEv19YDxsIqmST7zGaJxm6tbtYXYx3iMyKQSmvzAVqrFnmooZd
MsVvilwpVOS8u1NNiMeutM+nF5BOF3A+fkdlVhAHLk8w2xGk7AIJX7yw7T6wRfHu6Qc=
-----END RSA PRIVATE KEY-----
  
```

d. Exit with Ctrl + x and save the changes with “y”



```

root@ip-10-1-1-223:/home/ec2-user
GNU nano 2.3.1      File: lcastroaws.pem      Modified

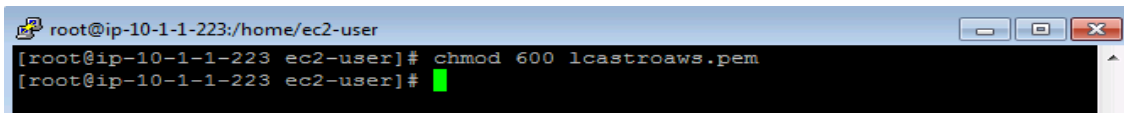
2wWRRHKEUhfISUQnucT2VjLeYN50CgYEAzXCcRqOD3eRmxReJpArtpxXSH5aeYAApCacEyPrUBeR5
fZ2v0ieZ+v5xTYagP8Jfy/8ULCaC3K7BJEih10hehBcYYaGOFc7FavoN4phRbafGHTzsUagbBDdD
phk4xAVA0Kh7kwNCgngghPSh4p+14NNN0shR+ZL4UYvrBdLUwU7MCgYEAzVm7MDctmDNBbFxXn30H
MeCsmIKk76mNgc7cMDUFeSn22TEDsALumBXNndodqUNy0z60ap/z4YFCOHG0A7ArcitCYOyf+0UrG
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+fkdLvhlhLk8w2xGk7AIJX7yw7T6wRfHu6Qc=
-----END RSA PRIVATE KEY-----

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

```

e. Change file privileges using the following command

i. `# chmod 600 lcastroaws.pem`



```

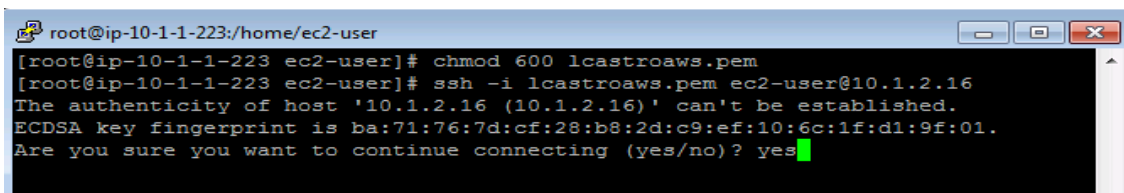
root@ip-10-1-1-223:/home/ec2-user
[root@ip-10-1-1-223 ec2-user]# chmod 600 lcastroaws.pem
[root@ip-10-1-1-223 ec2-user]#

```

f. Access the Private_EC2 machine via SSH from the Public EC2 machine with the following command

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

(This IP Address depends on the one that has been designated in your case)



```

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. Run the following command

i. `#sudo su`

ii. `#yum update -y`

1. Check if it is valid to carry out the Update
2. Use the command
 - a. **#ping 4.2.2.2** - To validate that you have internet access
 - b. **The ping should not be successful since the machine does not have an associated internet**

```
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
```

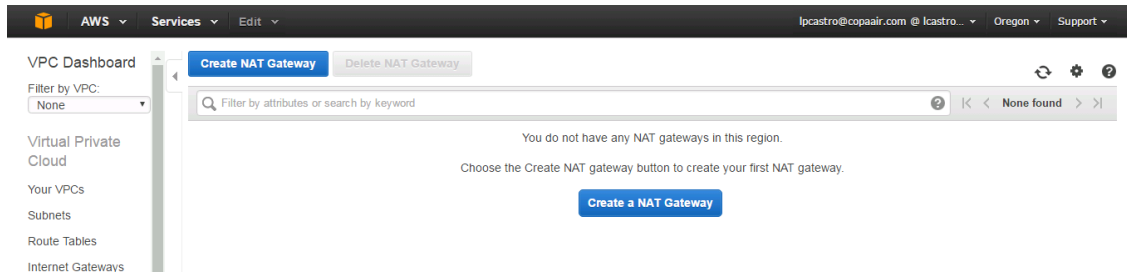
The screenshot shows the AWS Management Console interface for EC2 instances. The top navigation bar includes the AWS logo, 'Services', 'Edit', and the user's account information. The left sidebar shows the 'EC2 Dashboard' and a list of navigation links: 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES', 'Instances' (highlighted), 'Spot Requests', and 'Reserved Instances'. The main content area displays the 'Instances' page with a search bar and a table of instances. The table has columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, and Public DNS. Two instances are listed: 'Private_EC2' (Instance ID: i-7b5ebca3, Type: t2.micro, Zone: us-west-2b, State: running) and 'Public_EC2' (Instance ID: i-2233535, Type: t2.micro, Zone: us-west-2a, State: running). The 'Public_EC2' instance is highlighted in blue. The 'Status Checks' column shows '2/2 checks ...' for both instances, and the 'Alarm Status' column shows 'None'.

	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
<input type="checkbox"/>	Private_EC2	i-7b5ebca3	t2.micro	us-west-2b	running	2/2 checks ...	None	
<input checked="" type="checkbox"/>	Public_EC2	i-2233535	t2.micro	us-west-2a	running	2/2 checks ...	None	52.1...

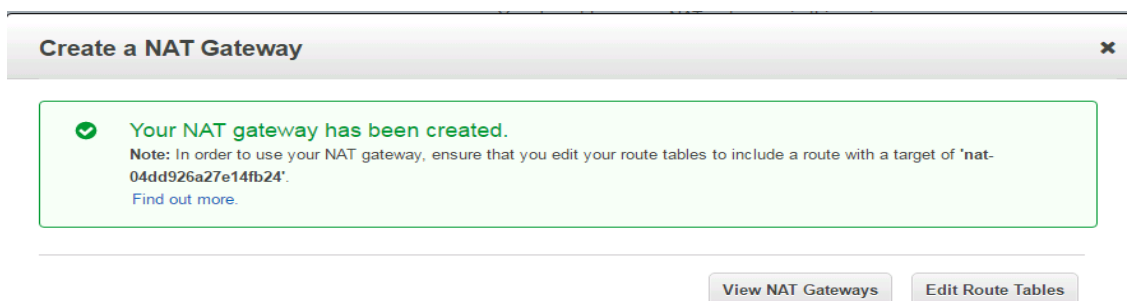
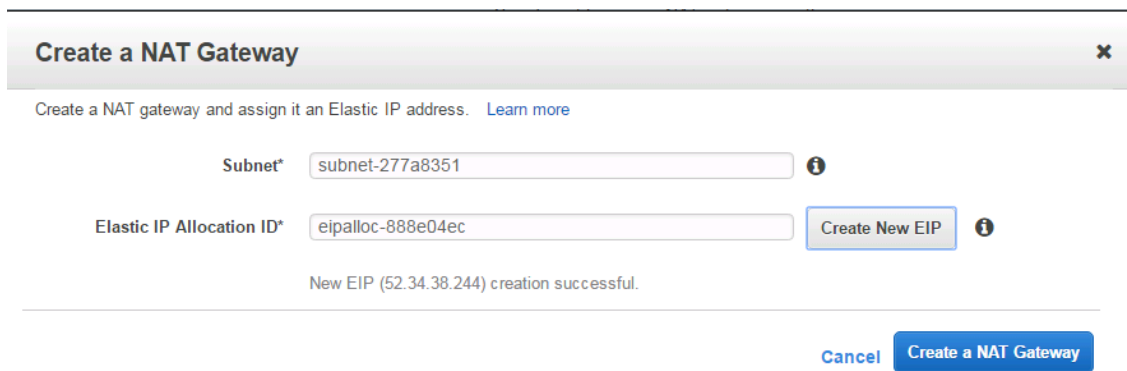
Step 7

Give you access to the private machine so you can access the Internet through a NAT Gateway

- Go to VPC>NAT Gateways>Create NAT Gateways

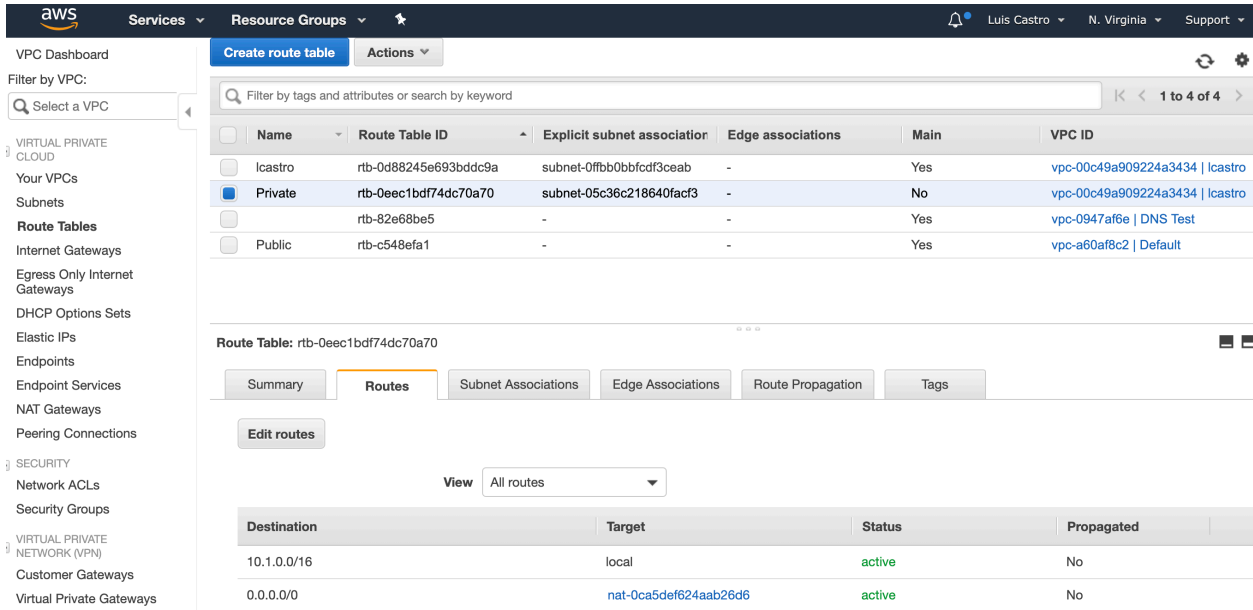


1. Choose public subnet 10.X.1.0
2. Create New Elastic IP
3. Create NAT Gateway



Step 8

- Create a Route Table for the Private Subnet called user + private
 - o Ex: lcastro-private
- Edit the Route Table of the private subnet
 - o Create a default route to the Created NAT Gateway

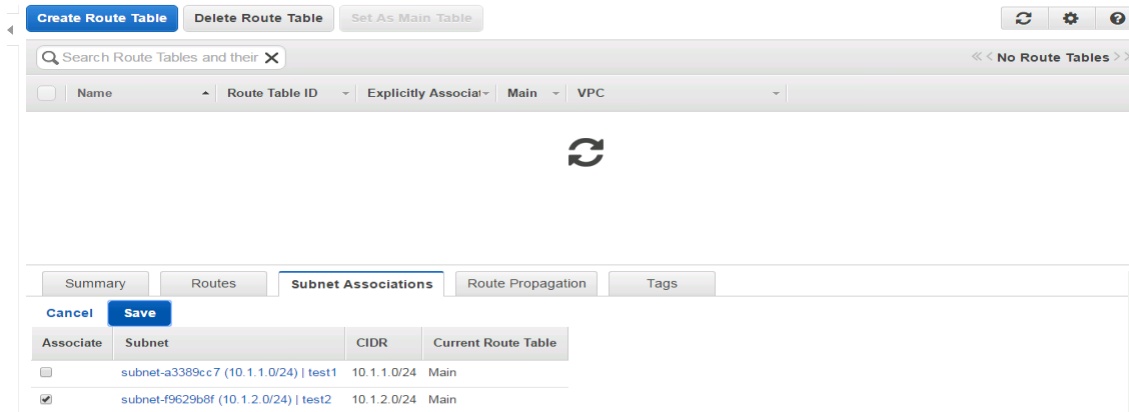


The screenshot shows the AWS Management Console interface for the 'Private' route table (rtb-0eec1bdf74dc70a70). The 'Routes' tab is selected, displaying a table of routes.

Destination	Target	Status	Propagated
10.1.0.0/16	local	active	No
0.0.0.0/0	nat-0ca5def624aab26d6	active	No

- Click on Routes & Edit
- Add a default route
 - o Destination
 - 0.0.0.0/0
 - o Target
 - Nat Gateway - Created
 - o Save

- Then associate the subnet 10.X.2.0 / 24
 - o Subnet Associations
 - o Save



Search Route Tables and their

<< No Route Tables >>

Summary Routes **Subnet Associations** Route Propagation Tags

Cancel Save

Associate	Subnet	CIDR	Current Route Table
<input type="checkbox"/>	subnet-a3389cc7 (10.1.1.0/24) test1	10.1.1.0/24	Main
<input checked="" type="checkbox"/>	subnet-f9629b8f (10.1.2.0/24) test2	10.1.2.0/24	Main

Step 9

From the Private machine execute the following commands

- #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
  
```

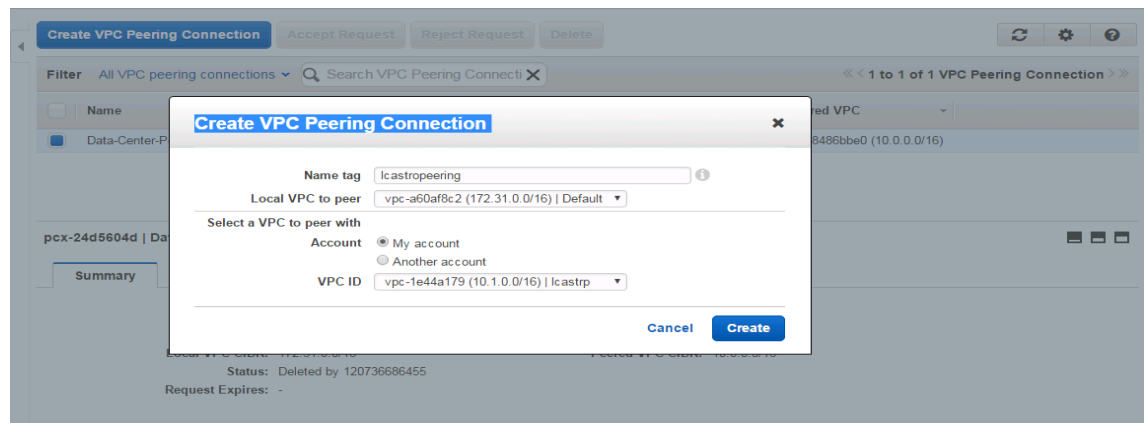
Step 10

From the private machine ping the IP Address according to your Region - It should not be successful:

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

Access **VPC>Peering Connections>Create VPC Peering Connections**

- **Name tag**
 - o Username + peering, ex: lcastropeering
- **Local VPC to Peer**
 - o VPC Default
- **VPC ID**
 - o VPC created - 10.X.0.0/16



- Accept Request

Create VPC Peering Connection

Accept Request

Reject Request

Delete

Filter

All VPC peering connections

Search VPC Peering Connecti X

<< 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

X

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

- Select the Default VPC and add a new path
 - o Edit
 - Destination
 - 10.X.0.0/16
 - Target
 - Pcx-be982 (Validar el Peering Asociado)
 - Save

Create Route Table

Delete Route Table

Set As Main Table

Search Route Tables and their X

<< 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-a60af8c2 (172.31.0.0/16) Default
<input type="checkbox"/>	NAT	rtb-05aa3662	1 Subnet	Yes	vpc-1e44a179 (10.1.0.0/16) Icastrp
<input type="checkbox"/>	Pub	rtb-a8aa36cf	1 Subnet	No	vpc-1e44a179 (10.1.0.0/16) Icastrp

rtb-c548efa1 | Public

Summary

Routes

Subnet Associations

Route Propagation

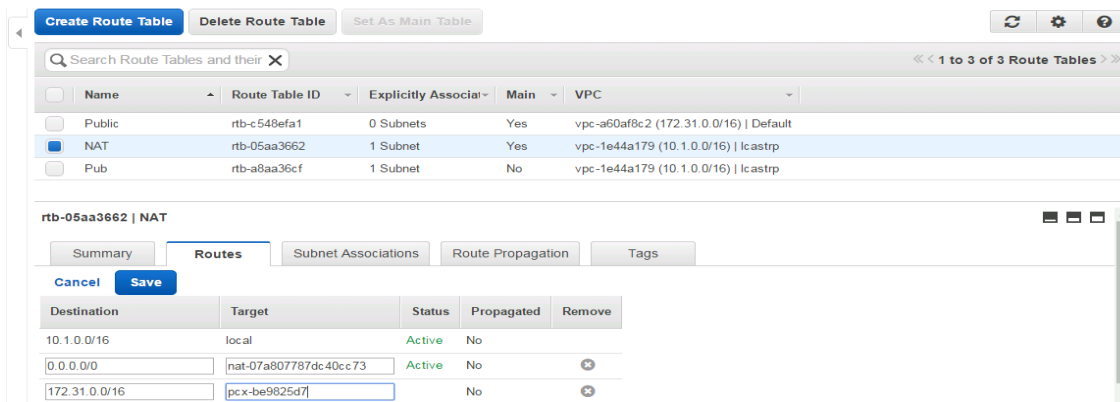
Tags

Cancel

Save

Destination	Target	Status	Propagated	Remove
172.31.0.0/16	local	Active	No	
0.0.0.0/0	igw-1832127d	Active	No	X
10.1.0.0/16	pcx-be9825d7	No	No	X

- Select the VPCs created in the 10.X.0.0 / 16 network and add a new route
 - Edit
 - Destination
 - 172.31.0.0/16
 - Target
 - Pcx-be982 (Validar el Peering Asociado)
 - Save



Search Route Tables and their

<< 1 to 3 of 3 Route Tables >>

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associat	Main	VPC
<input type="checkbox"/>	Public	rtb-c548efa1	0 Subnets	Yes	vpc-a60af8c2 (172.31.0.0/16) Default
<input checked="" type="checkbox"/>	NAT	rtb-05aa3662	1 Subnet	Yes	vpc-1e44a179 (10.1.0.0/16) lcastrp
<input type="checkbox"/>	Pub	rtb-a8aa36cf	1 Subnet	No	vpc-1e44a179 (10.1.0.0/16) lcastrp

rtb-05aa3662 | NAT

Summary Routes Subnet Associations Route Propagation Tags

Cancel Save

Destination	Target	Status	Propagated	Remove
10.1.0.0/16	local	Active	No	
0.0.0.0/0	nat-07a807787dc40cc73	Active	No	<input type="button" value="✕"/>
172.31.0.0/16	pcx-be9825d7f	No		<input type="button" value="✕"/>

From the private machine ping the IP Address according to your Region

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

```
^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
```