**AWS Project 1 – Connect to internet from a private subnet**

CURRENTLY BEING DRAFTED / NOT FINAL VERSION

Objective : Ping google.com from a private subnet

AWS Environment expected : 1 public subnet 1 and 1 private subnet 2

**STEPS TO FOLLOW**

**Part 1 : VPC**

Manually :

Create a VPC

Create the subnets (1 Private, 1 Public)

Create an Internet Gateway (IGW) for the VPC

Create a NAT Gateway with an Elastic IP for the Public subnet

Create/modify Route tables

Or Automatically

Choose in « Launch VPC Wizard » (VPC DashBoard) a VPC with Public and Private Subnets

And complete the different steps (see details on manually creation)

**Part 2 : EC2 Instance**

Create a EC2 Instance

**Part 3 : TEST**

Connect to the instance created

Try to ping Google.com

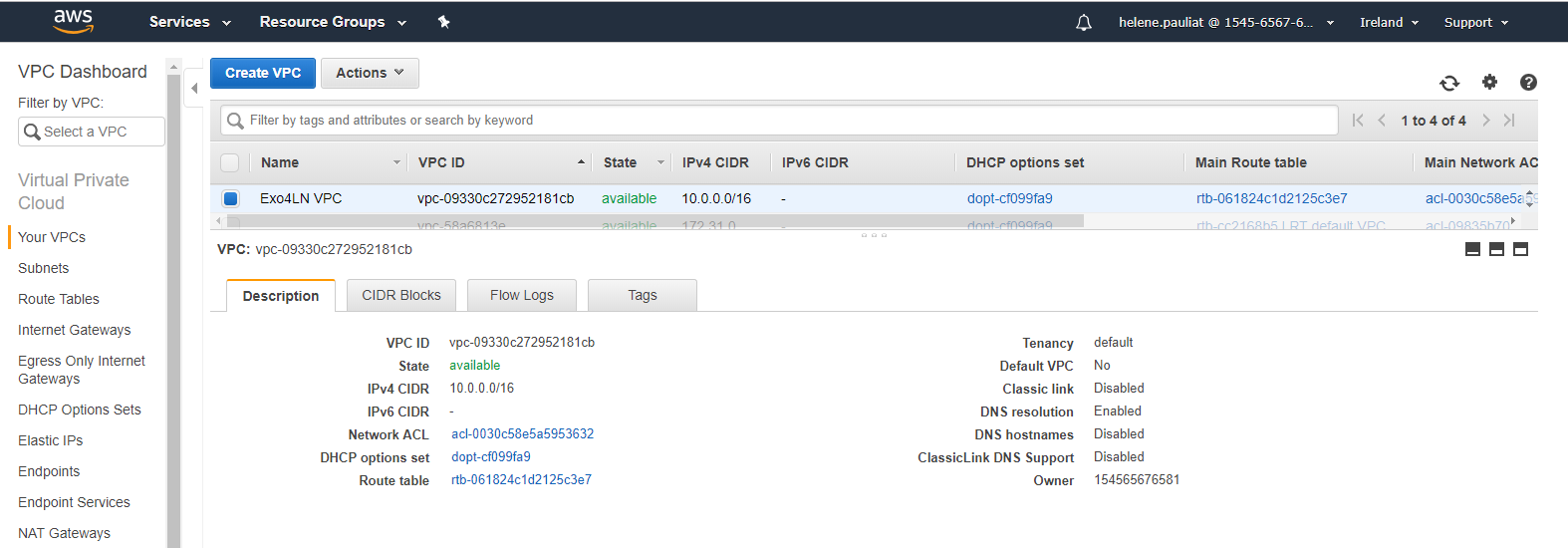
**DETAILS STEP BY STEP**

**PART 1**

1. **Create a VPC :**

Go to Services/VPC, choose the rubrik « Your VPCs » on the left.

Click on « Create VPC » and give a name to the VPC « Exo4LN VPC », for example), give an IPv4 adress (10.0.0.0/16) and valid with « Create ».



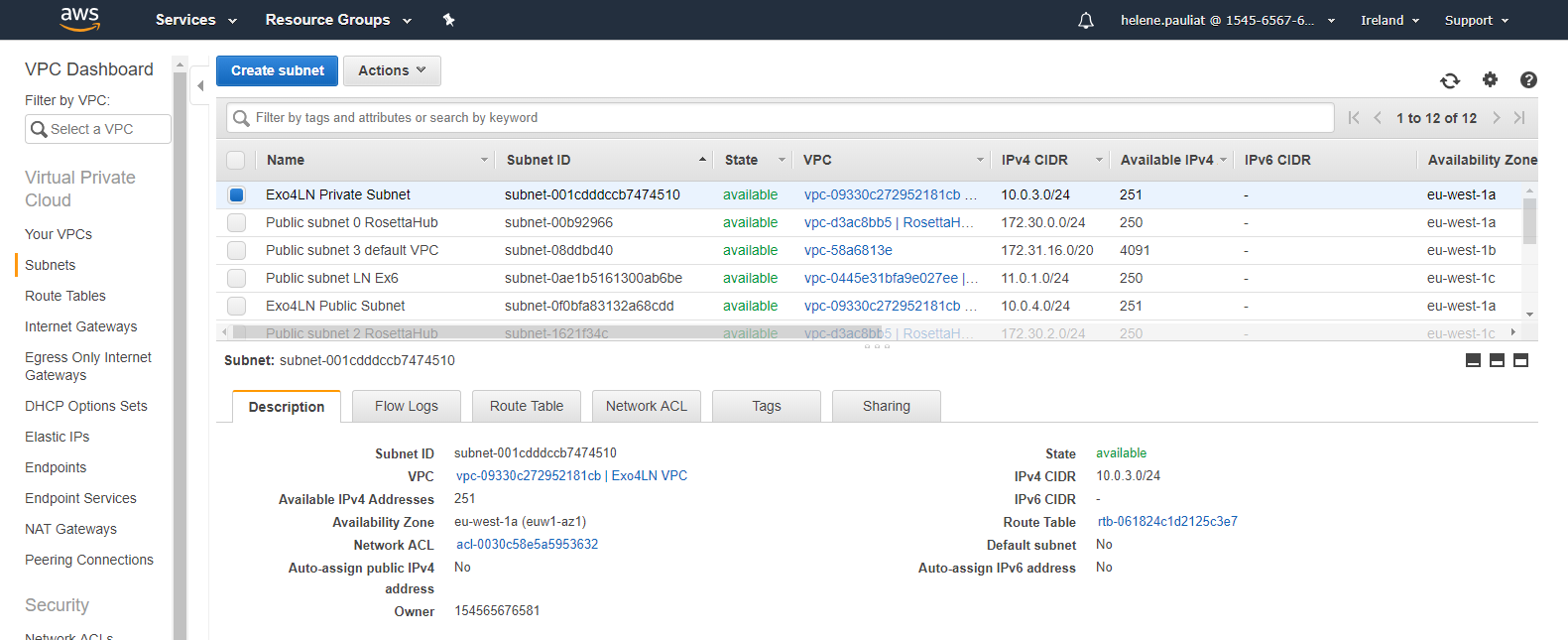
1. **Create subnets**

Go to « Subnets » rubrik on the left.

Click on « Create subnet », and :

* give a name to the subnet (is better to manage to indicate in the name if it is private or public subnet, like « Exo4LN Private Subnet »),
* attach the VPC which you create on step 1 (« Exo4LN VPC ») on the list proposed
* Choose an AZ (Availability Zone) : eu-west-1a for example
* Give an IPv4 adress (10.0.3.0/24 for example) and valid with « Create ».

Follow exactly the same process to create the second subnet, but change name (« Exo4LN Public Subnet ») and IPv4 adress (10.0.4.0/24) and keep the same AZ.



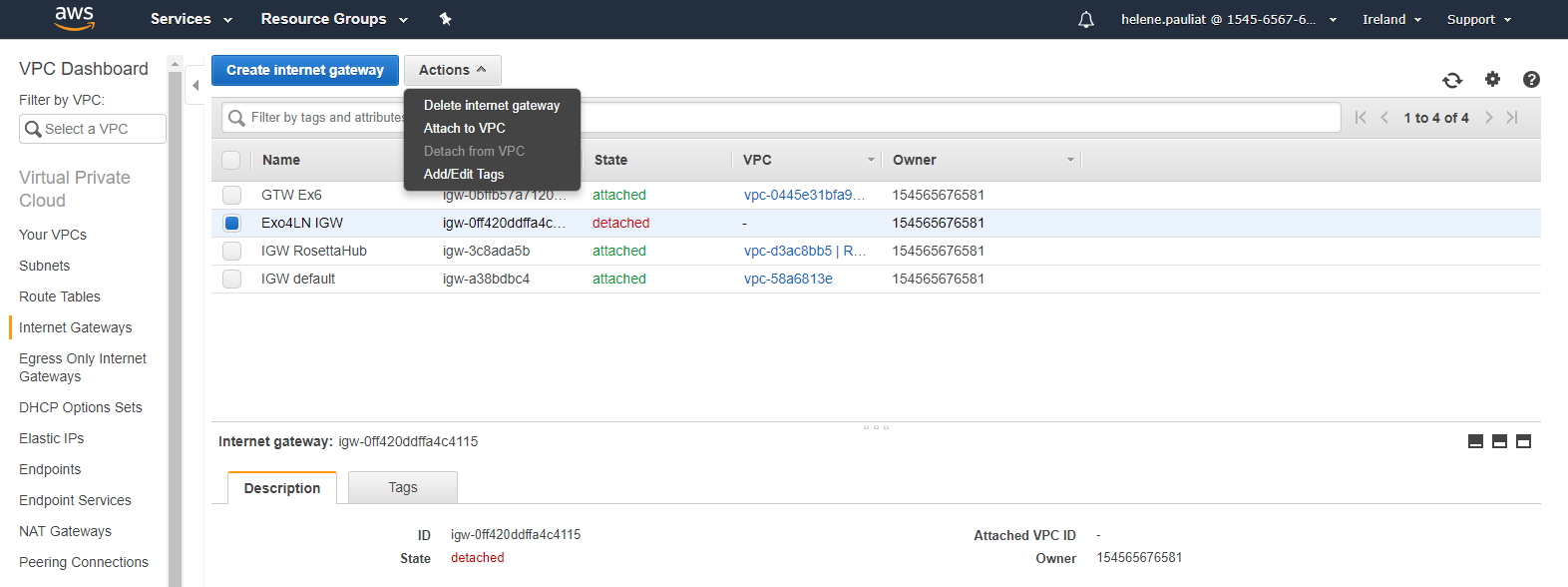
1. **Create an IGW (Internet Gateway)**

To have an access to internet, you must create an IGW and attach it to the VPC.

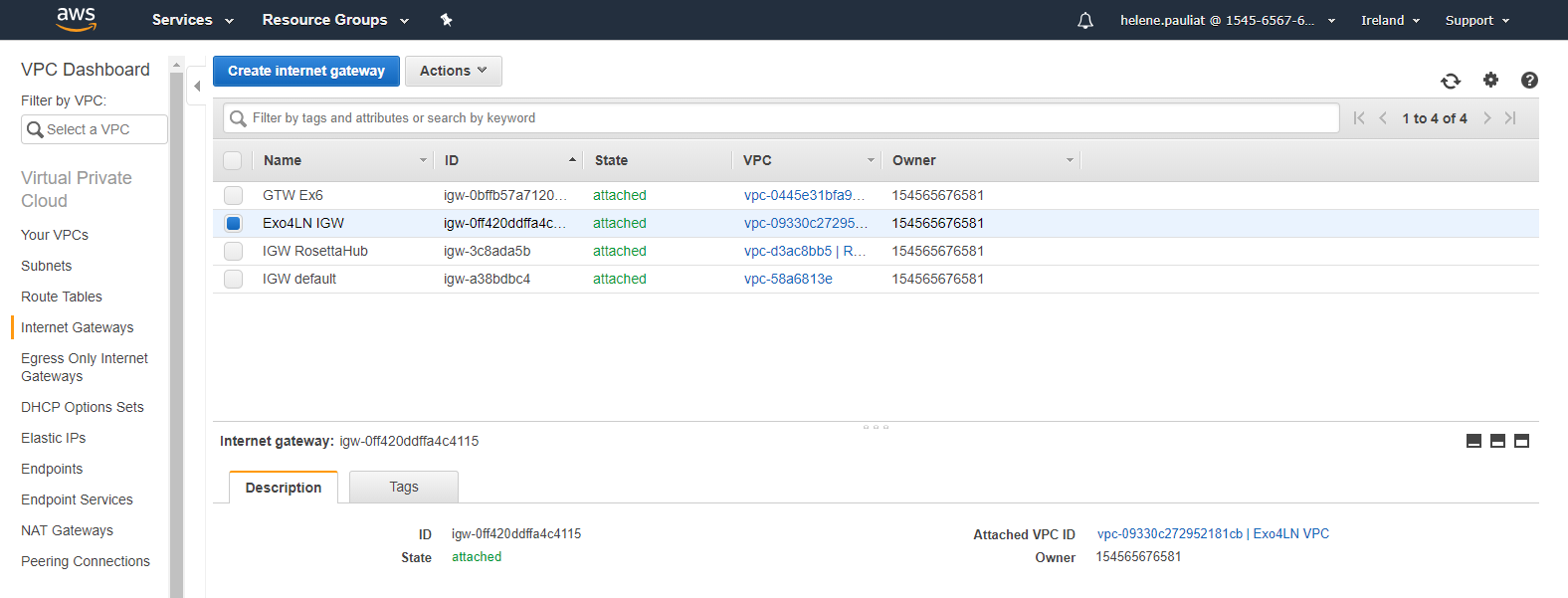
Go to « Internet Gateways » rubrik on the left.

Click on « Create internet gateway », and :

* give a name to the subnet (like « Exo4LN IGW »), and valid with « Create ».
* Select the right IGW on the list, choose « Attach to VPC » with the « Actions » button :



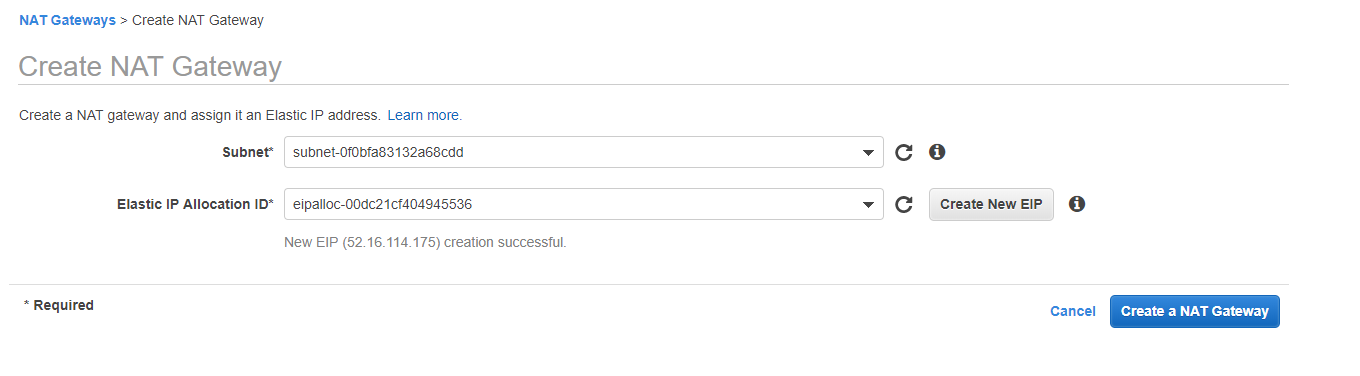
* Attach the right VPC « Exo4LN VPC »



1. **Create a NAT Gateway**

Go to « NAT Gateway » rubrik on the left.

Create a new NAT Gateway (Network Address Translation) and choose the Public subnet ID



1. **Define the difference Private/Public with Route tables**

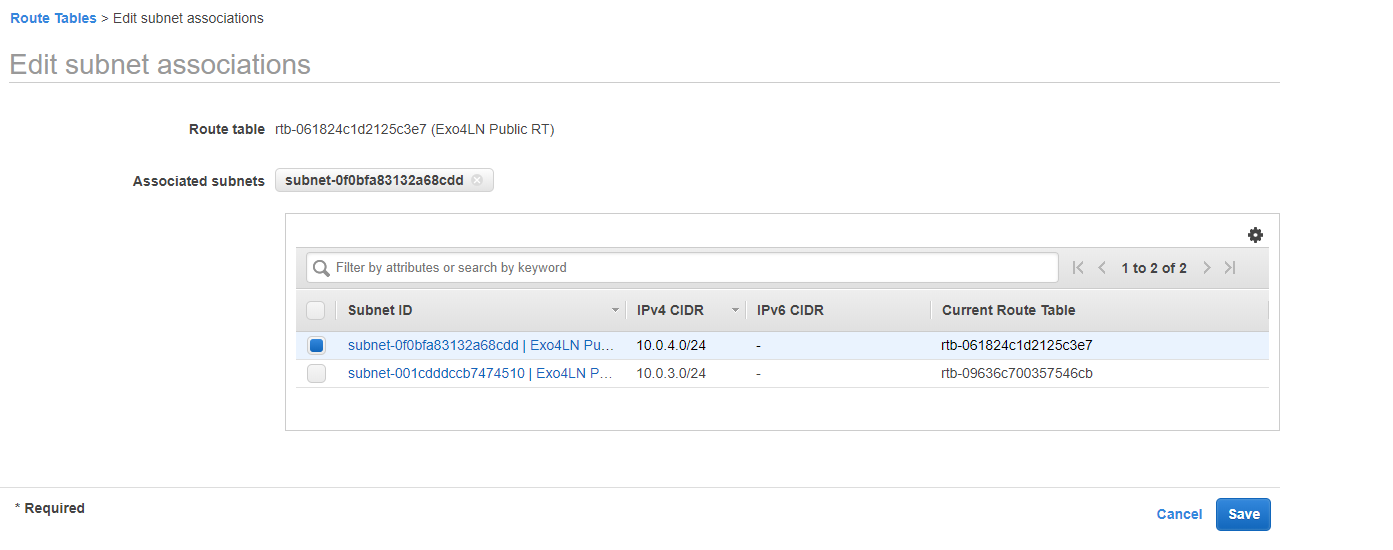
To get a subnet really public, you must associated the IGW to this subnet, by the route table associated. So you must have two separated Route Tables.

To have an acces to internet by the private subnet, you must use the NAT Gateway in the public subnet.

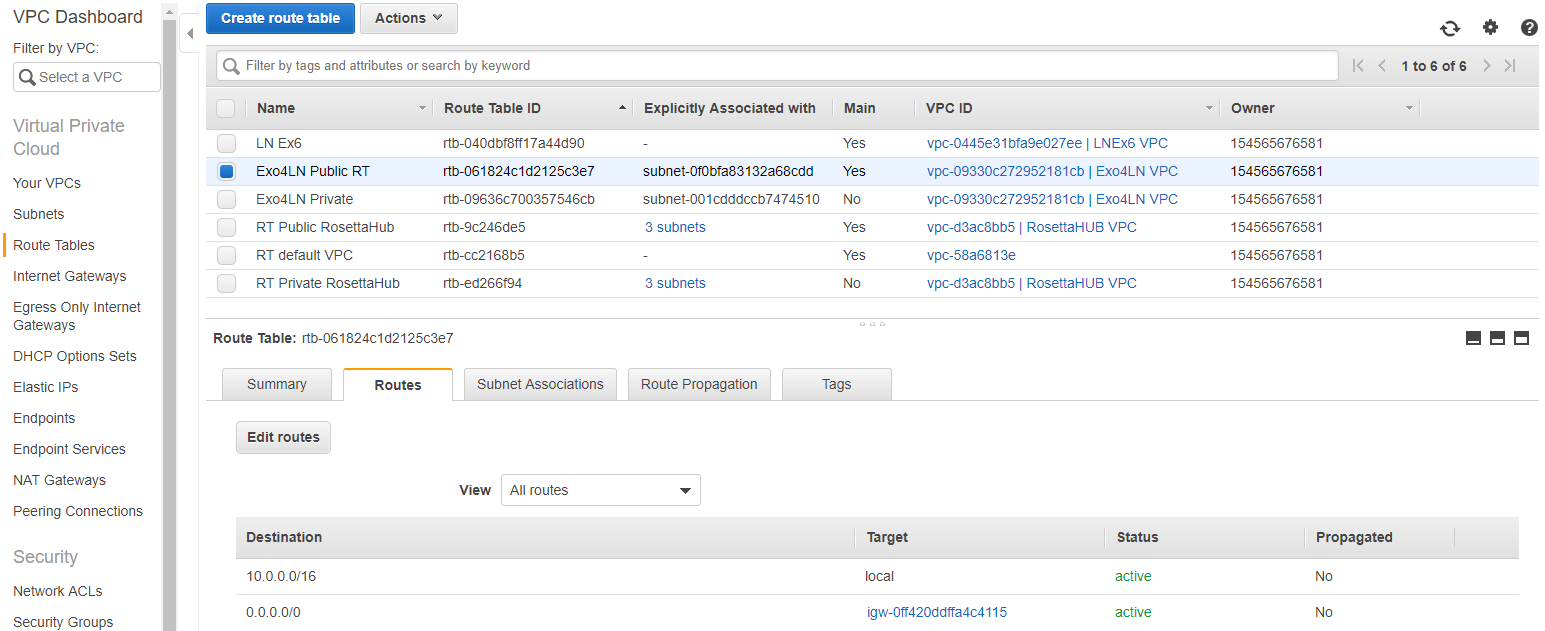
Go to « Route Tables » rubrik on the left.

For the public subnet :

* On the Route Table list, search on this which is associated to the right VPC « Exo4LN VPC ».
* If it is necessary, give it a name on changing directly in the cell with the pencil symbol « Exo4LN Public RT ».
* Select it and in the field « Routes » under the list, select « Edit Routes »
* « Add Route » and put « 0.0.0.0/0 » for destination, and choose the right IGW for Target
* In the field « Subnet Associations », edit them, choose the Public subnet ID, and save.

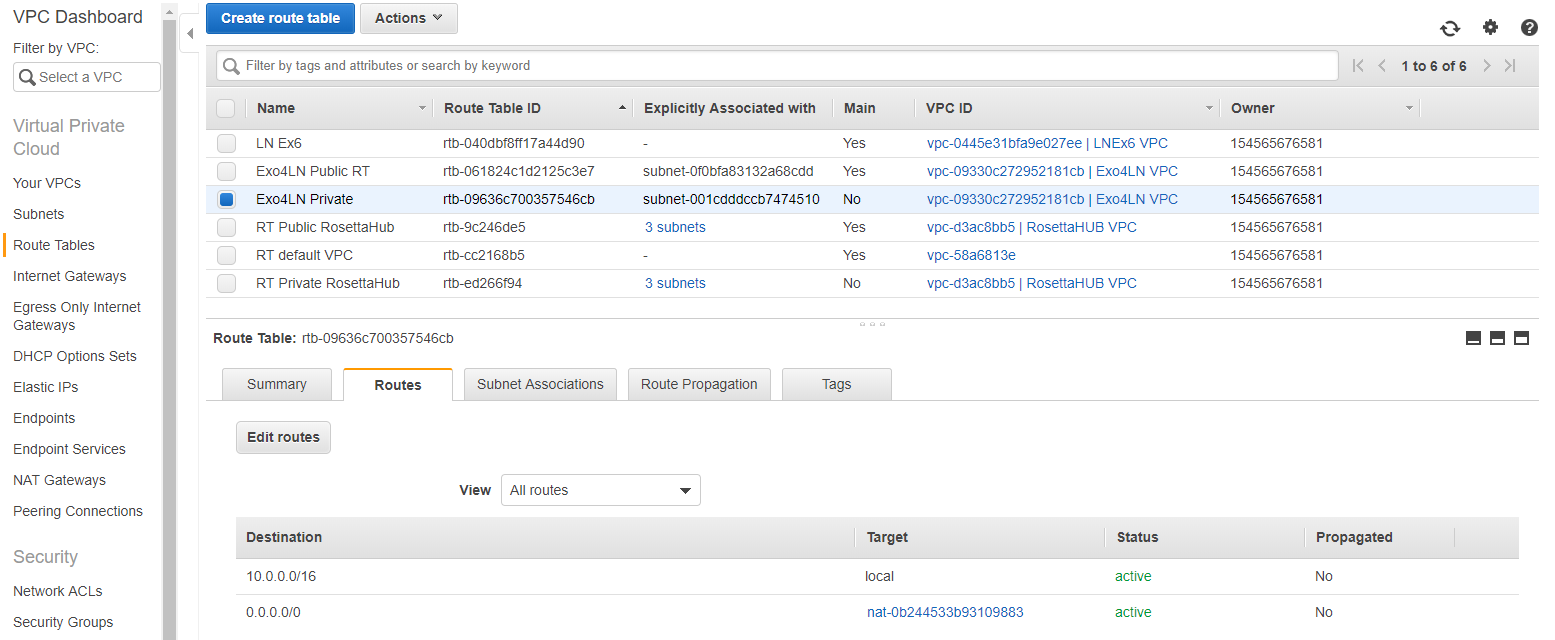


You obtain that :



For the private subnet :

* Create a new route Table : give a name and attach the right VPC.
* In the field « Routes » under the list, select « Edit Routes »
* « Add Route » and put « 0.0.0.0/0 » for destination, and choose the right NAT Gateway for Target (=Internet access trough the public subnet)
* In the field « Subnet Associations », edit them, choose the Private subnet ID, and save.



Do I need an ENI-INSTANCE in the private subnet instead of the NAT instance  ?

I write in the course that the eni permit to connect the private subnet but after we used a NAT instance. ENI was only correct for connect to another Network ?

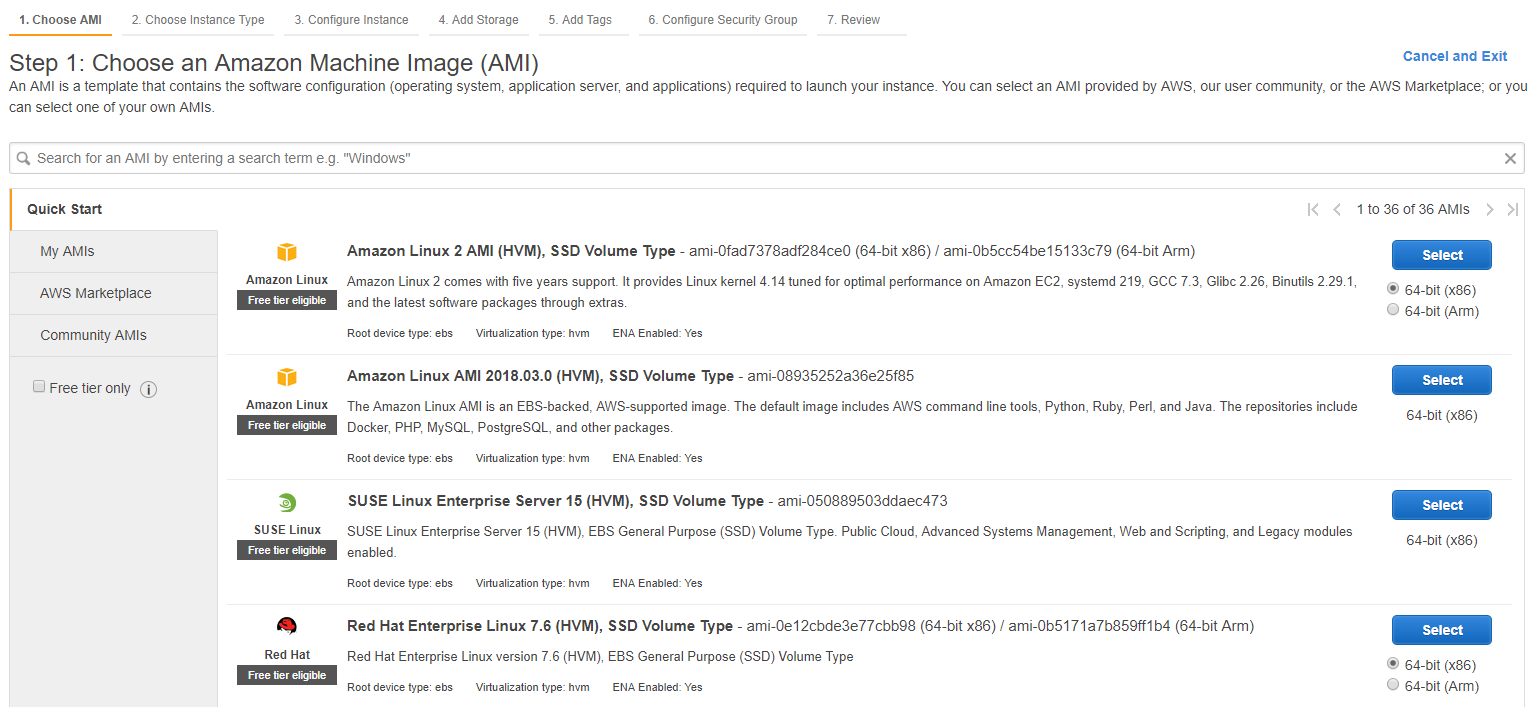
So it is indicated on the Route table of the private subnet

**PART 2**

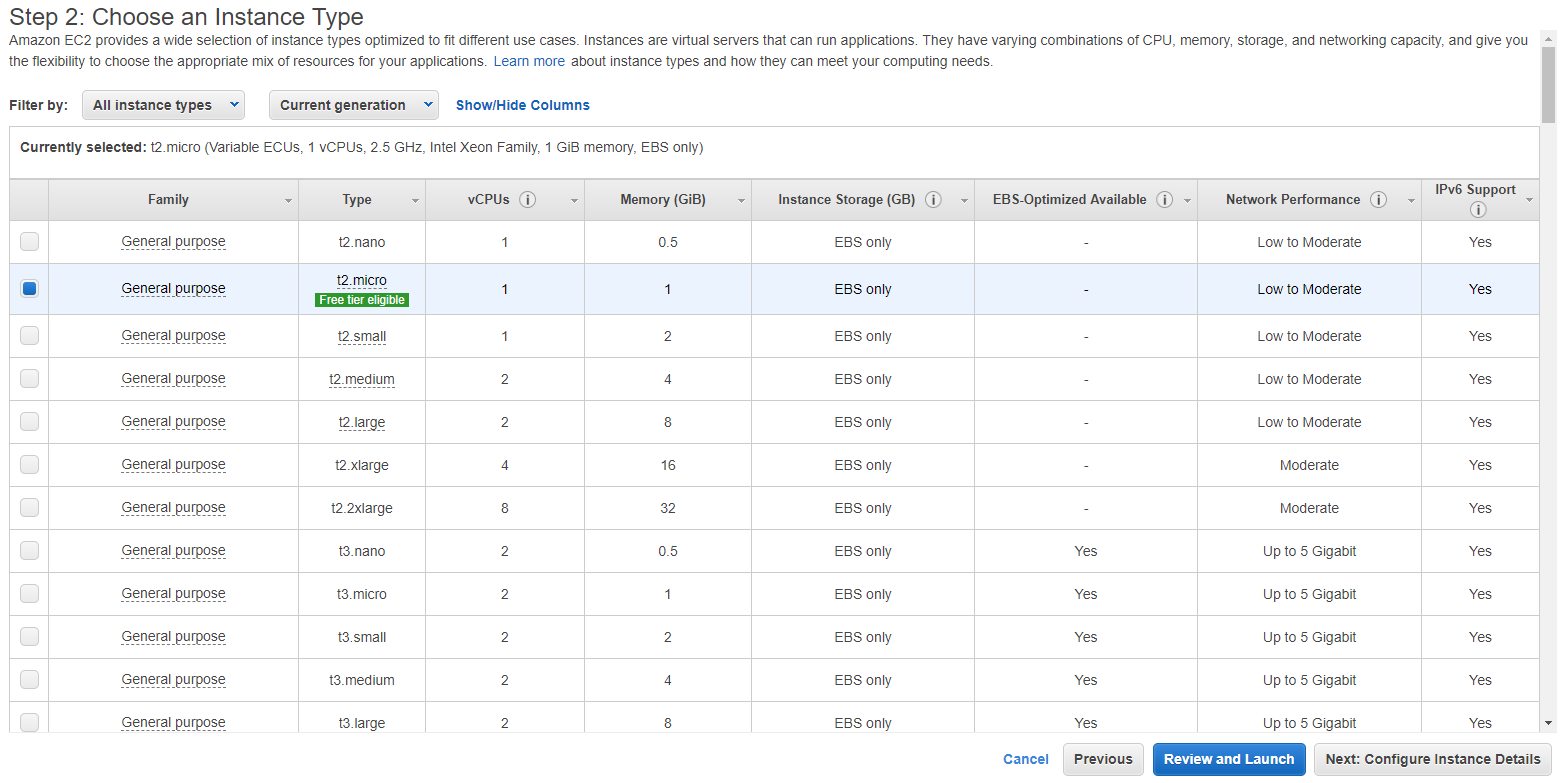
1. **Create an EC2 Instance**

Go to Services/EC2, choose the rubrik « Instance » on the left.

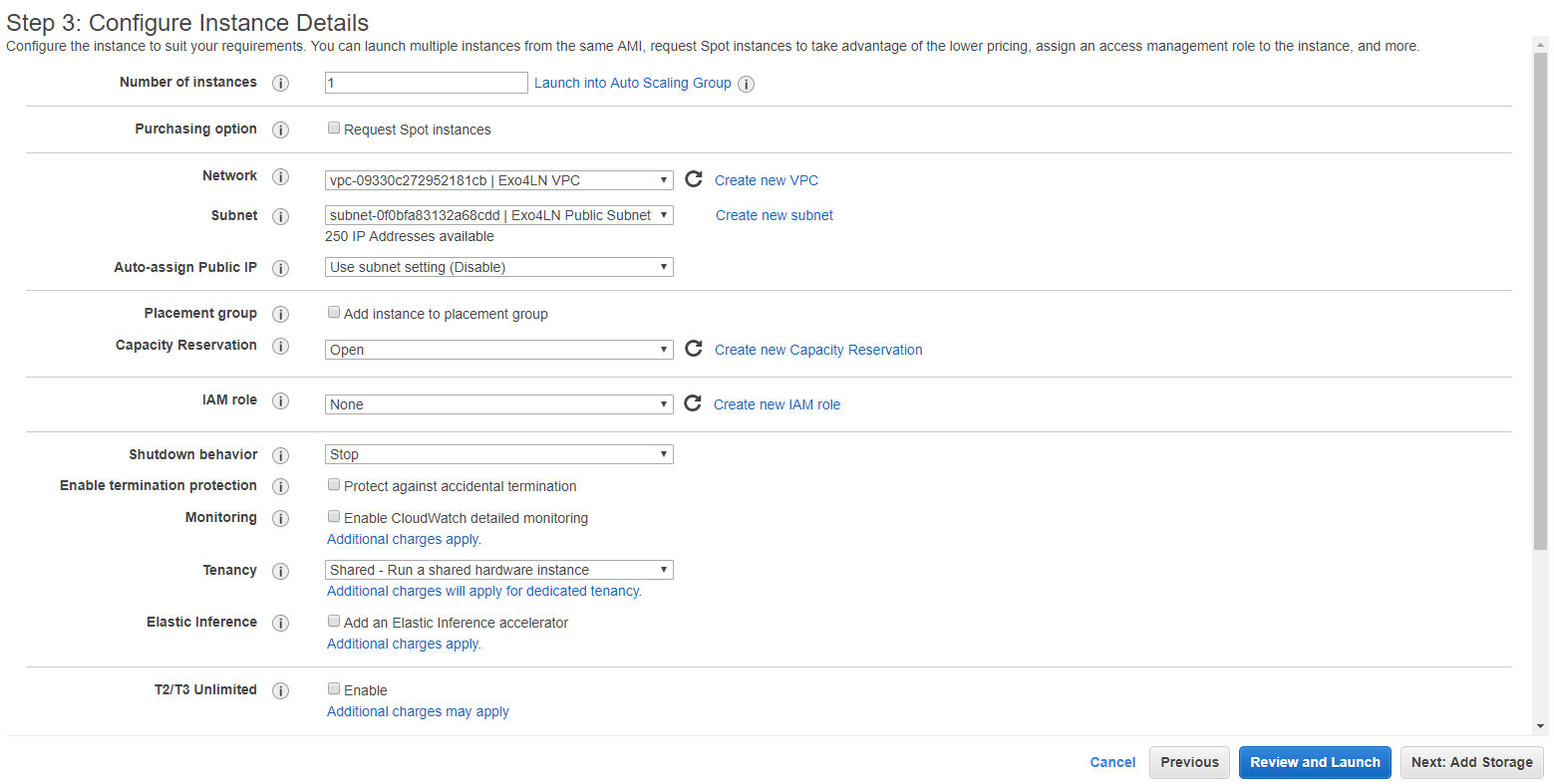
* Click on « Launch Instance » and choose an AMI (Amazon Machine Image)



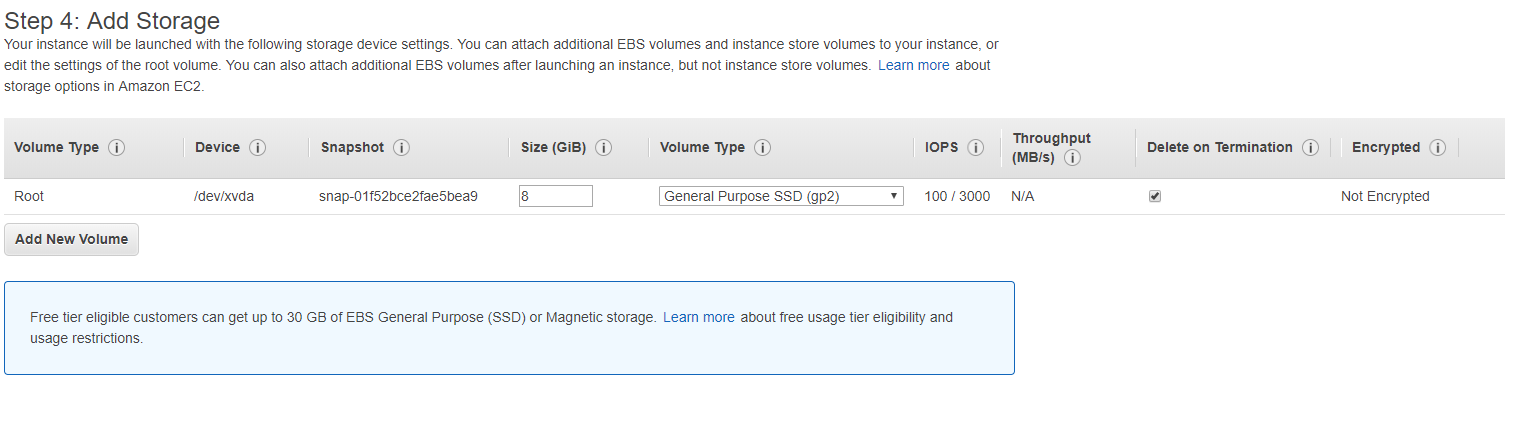
* Choose an Instance type (virtual servers that can run applications) adapted to your work : t2.micro for example.



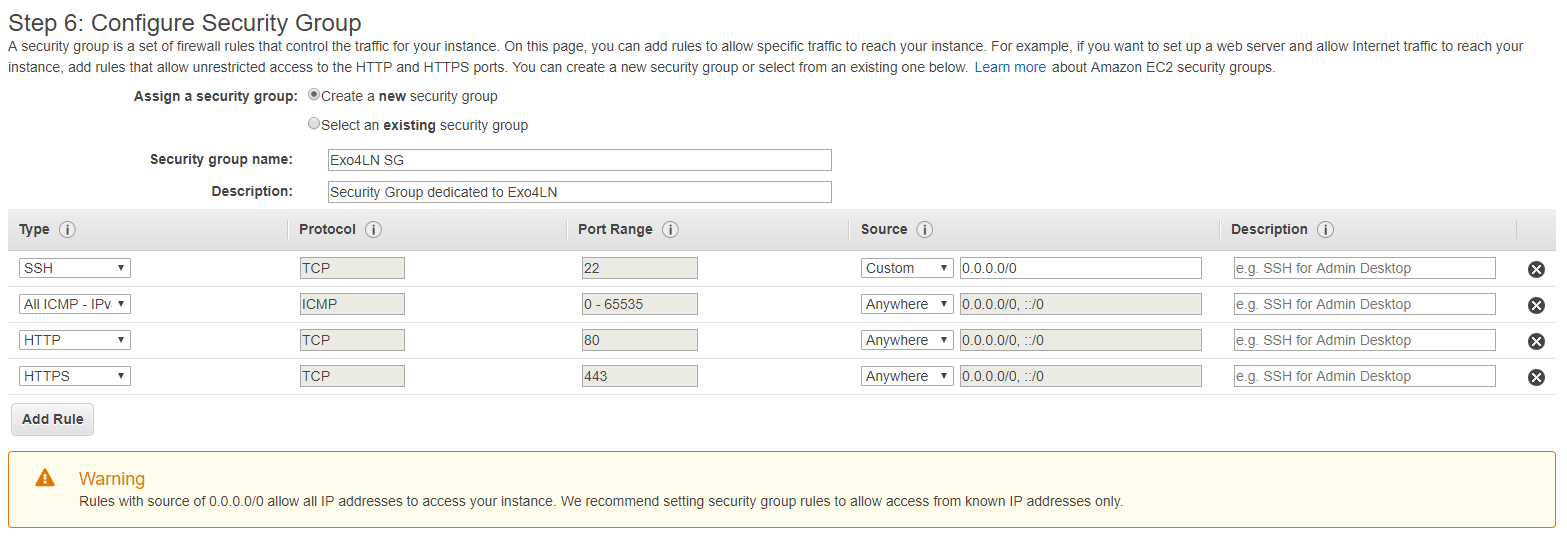
* Configure the Instance details : choose your VPC, verify that the public subnet is the right one



* Add storage and precize the size which you want



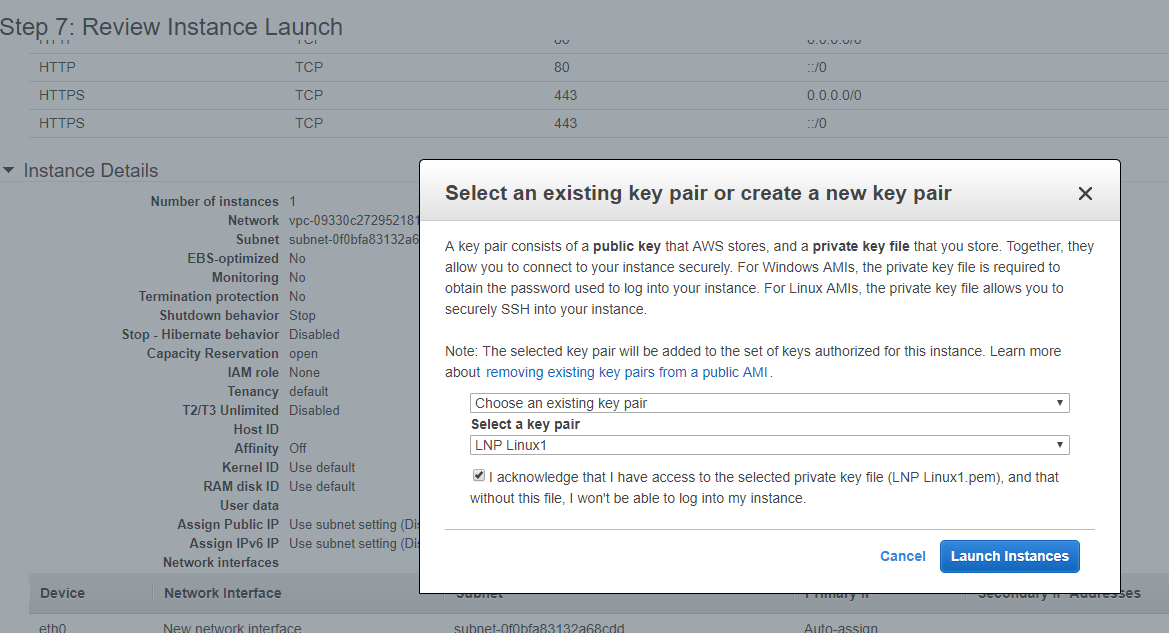
* Add Tags : Key = Name ; Value= The name of the instance (« Linux Exo4LN » for example)
* Configure the Security Group : select an existing SG or create a new one. Be careful to indicate unrestricted to internet with adding rules :



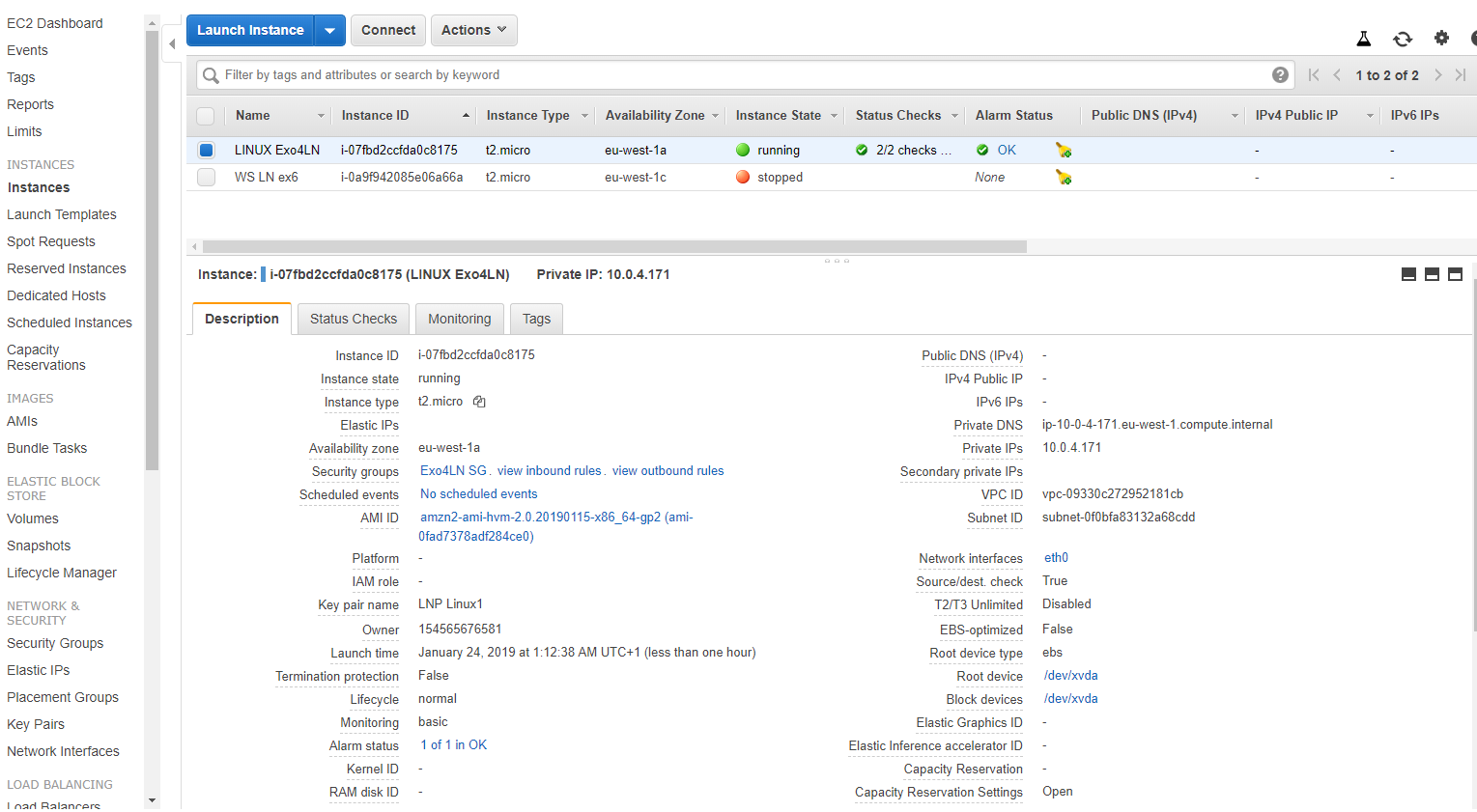
Good parameters for all the types for Security Group ???

Launch the instance.

A window appears to associate a key pair to connect to the instance :



View the Instance created : Follow the instance State and the status checks to know if the instance is running or not. **Don’t forget to stopped it before sign out AWS !**



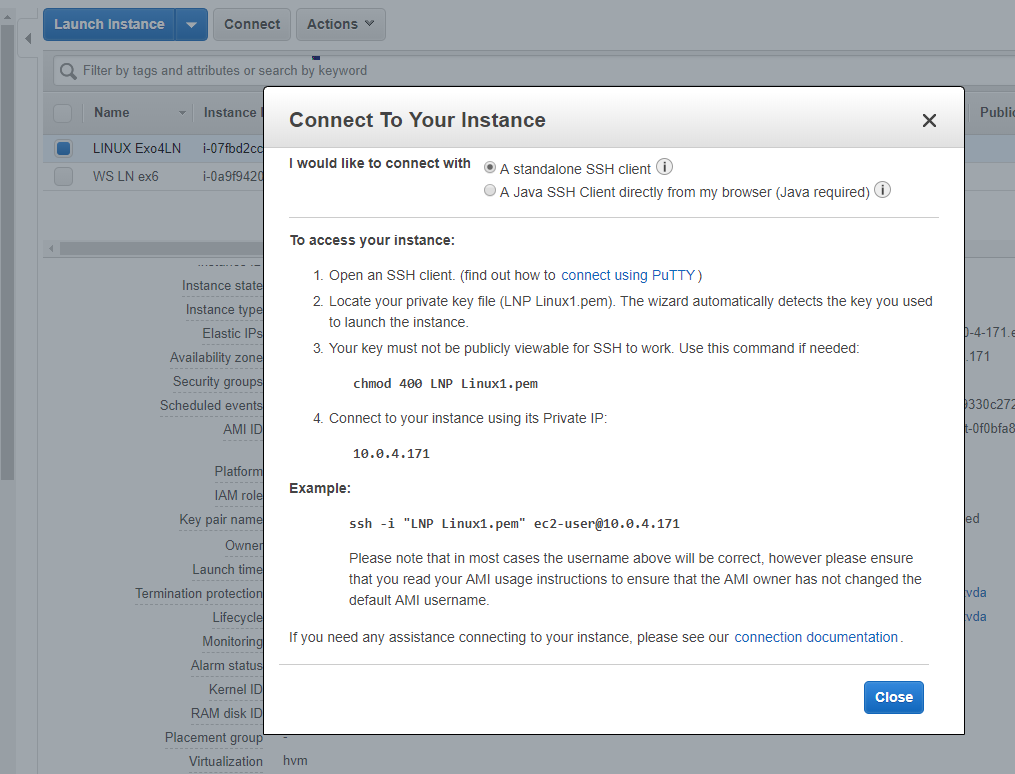
**PART 3 : TEST**

1. **Connect to the Instance**

You can retrieve all the processes to connect to a Linux Instance or a Windows Instance in this address : <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AccessingInstances.html?icmpid=docs_ec2_console>

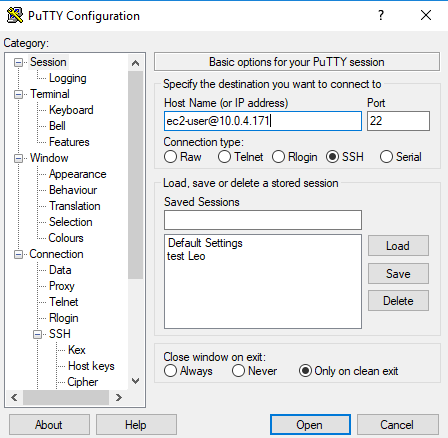
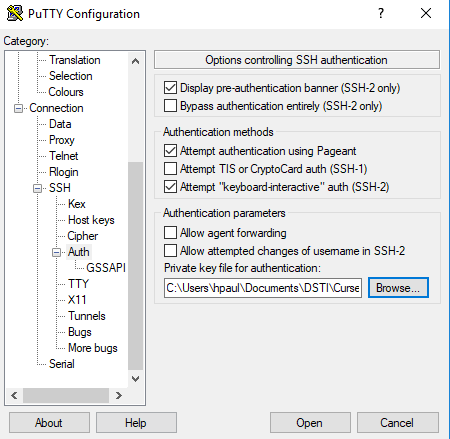
Use for example a PuTTY to connect to Linux Instance on Windows. (See the link above to know how to install and use PuTTY

Select the right instance and click on « Connect » : a window appears to choose the parameters of connection :



Can I publicate on GitHub like that, or I must hide the key ?

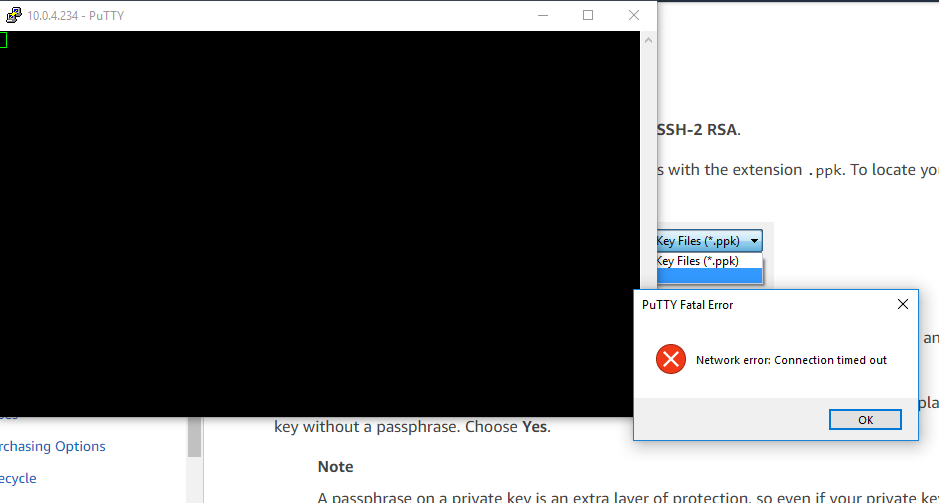
On « Session » : On Connection/SSH/Auth, select the right key pair file.ppk

Is there that I must use the IP adress of the Private subnet to connect me and not the Public adress ?

There is a fatal error .

But I already succeed once to connect me on a linux instance after several attemps. The name of the key pair wasn’t good but in this case ?



Co