Contents

[Purpose 2](#_Toc52940365)

[General Diagram 2](#_Toc52940366)

[Prerequisites 2](#_Toc52940367)

[Lab 4A: VPC with IGW and NAT GW 3](#_Toc52940368)

[Lab 4A using Web Management Console 3](#_Toc52940369)

[Create VPC 3](#_Toc52940370)

[Create Subnets 4](#_Toc52940371)

[Create Routing Tables 7](#_Toc52940372)

[Create Internet Gateway (IGW) 8](#_Toc52940373)

[Create NAT Gateway (NAT GW) 10](#_Toc52940374)

[Assign IGW and NAT GW to Routing Tables 11](#_Toc52940375)

[Assign Routing Tables to Subnets 14](#_Toc52940376)

[Create Key Pair to connect to Instances 16](#_Toc52940377)

[Create EC2 instances 17](#_Toc52940378)

[Make the review 25](#_Toc52940379)

[Add and Revoke Ports on Security Group 25](#_Toc52940380)

[Lab 4A using Command Line (Windows) 29](#_Toc52940381)

[Create VPC, Public Subnet, IGW and Route Table 29](#_Toc52940382)

[Create EC2 Keys, Sec Groups. Choose AMI and create EC2 Instances. 31](#_Toc52940383)

[Create Private Subnet, EIP, NAT Gateway, Private Route Table and EC2 Instance 31](#_Toc52940384)

[Get Information about Instances 33](#_Toc52940385)

[Review Configurations using Putty, SFTP and Browser 34](#_Toc52940386)

[Add Port to Security Group 35](#_Toc52940387)

[Delete Port to Security Group 36](#_Toc52940388)

[Clean resources 37](#_Toc52940389)

[For Web Management Console 37](#_Toc52940390)

[For Command Line (Windows) 37](#_Toc52940391)

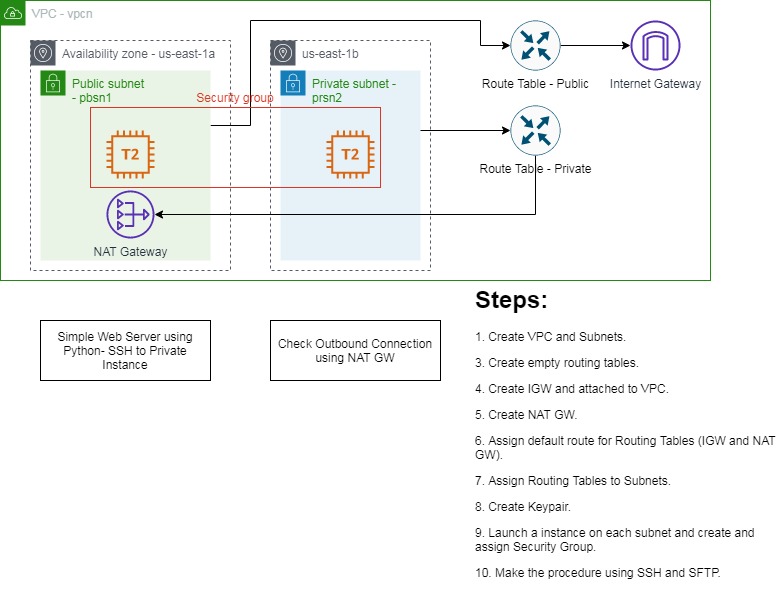
[Evidences to send 38](#_Toc52940392)

# Purpose

To create a common computing infrastructure in a public and private subnet, so you have to configure and connect routing tables and internet or NAT gateway.

# General Diagram

One VPC with two subnets, with instances connected on each subnet. Configuration to outbound connections has to be made on Routing Tables using Internet Gateway and NAT Gateway.



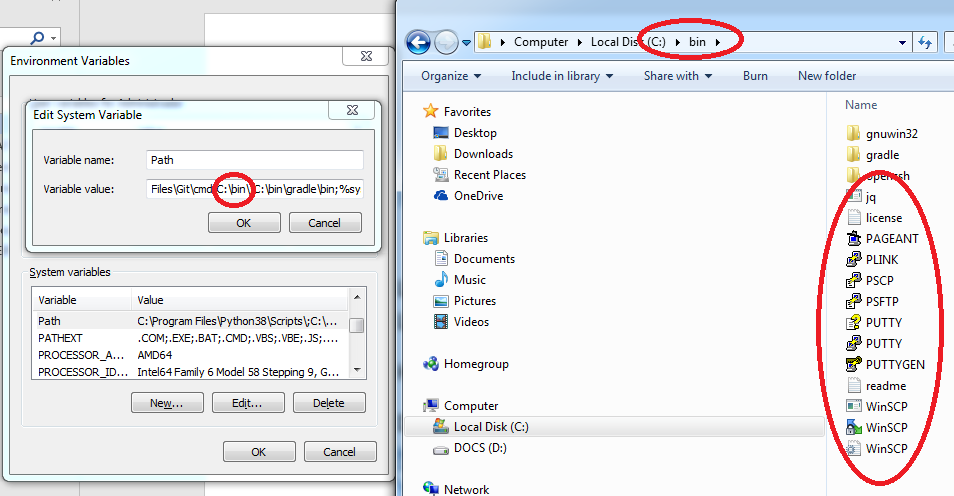
# Prerequisites

Labs1c1 have to be done and the context for Administrative user have to activated on Command Line Session.

Have installed putty and winscp on Windows; and those files on a folder in the PATH environment.

Download complete and portable putty and winscp using <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html> and <https://winscp.net/eng/downloads.php>

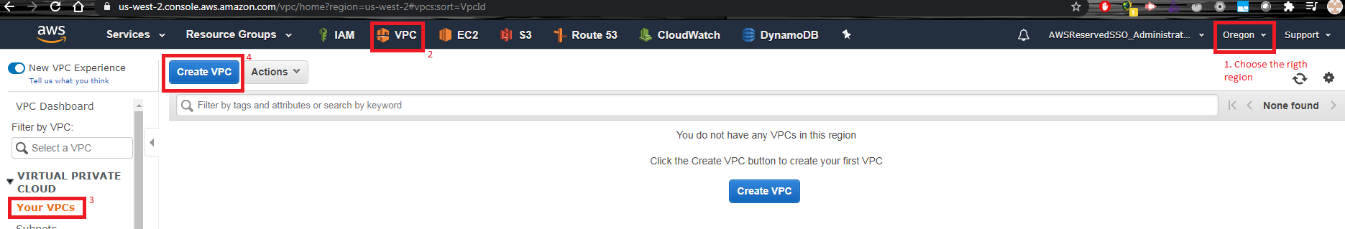
We use winscp as SFTP client (put Keypair on Public Instance) and for modifying PEM to PPK file on Windows. You can use Cyberduck as SFTP Client on MacOS.

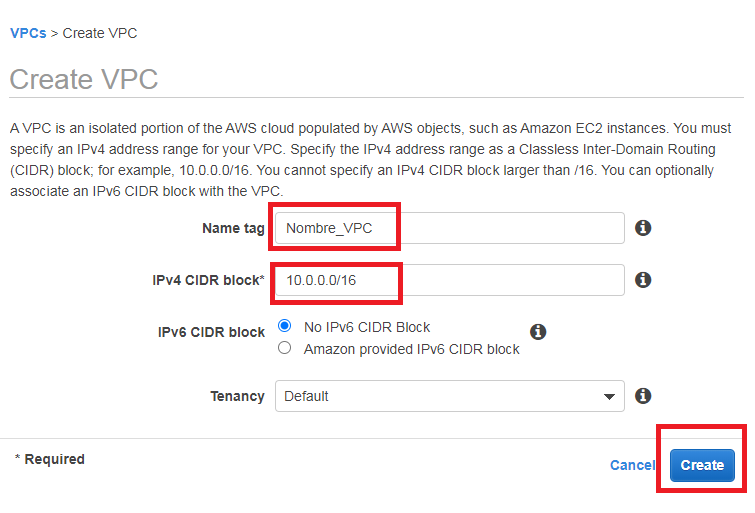


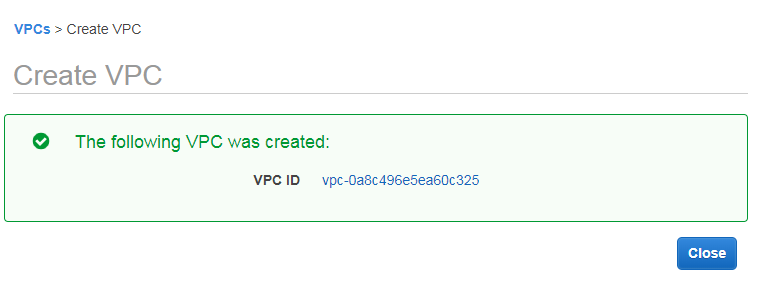
# Lab 4A: VPC with IGW and NAT GW

## Lab 4A using Web Management Console

### Create VPC

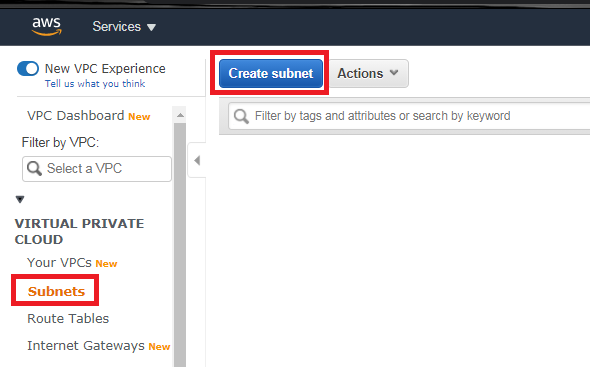


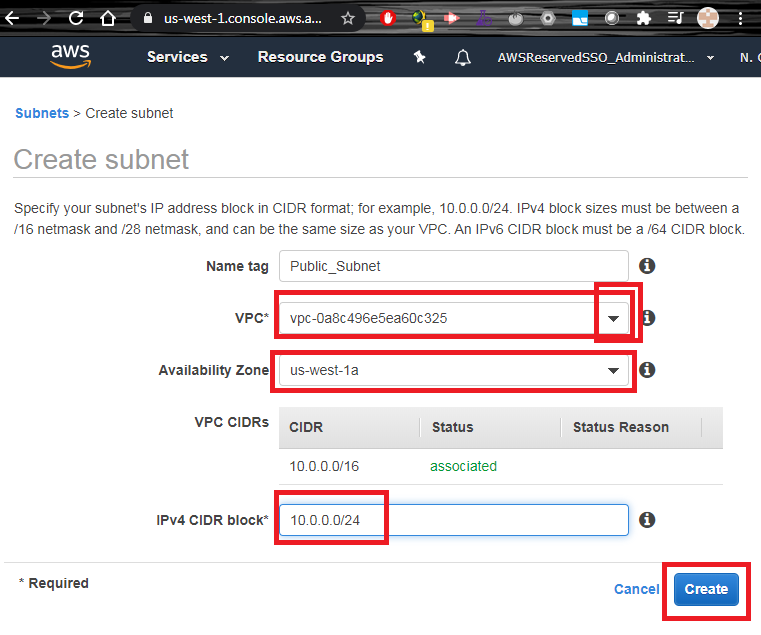




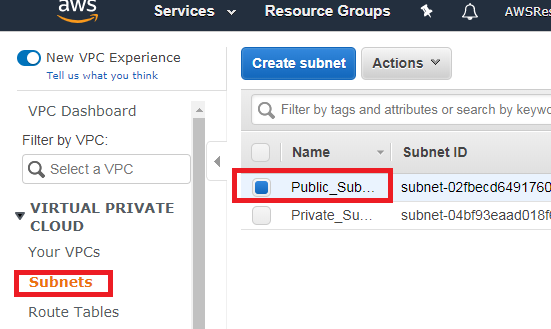
### Create Subnets

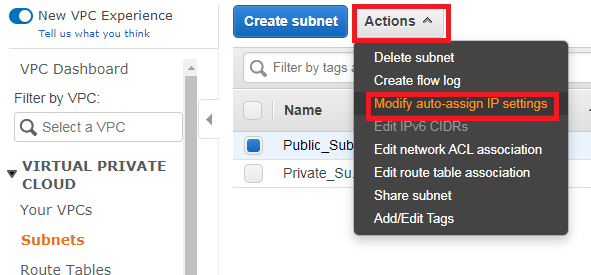
For Public Subnet,

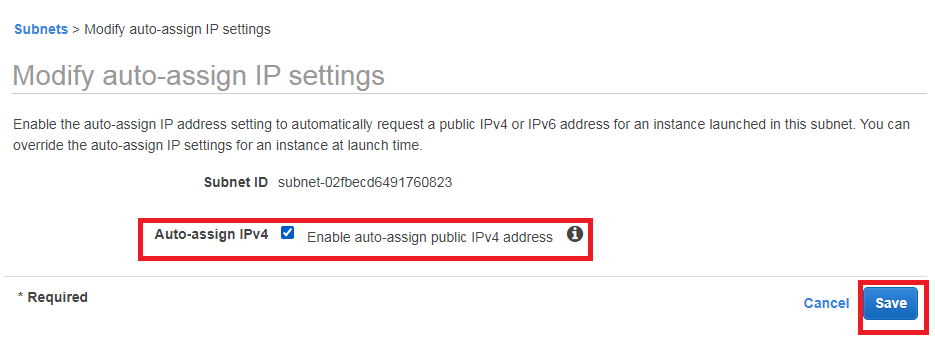




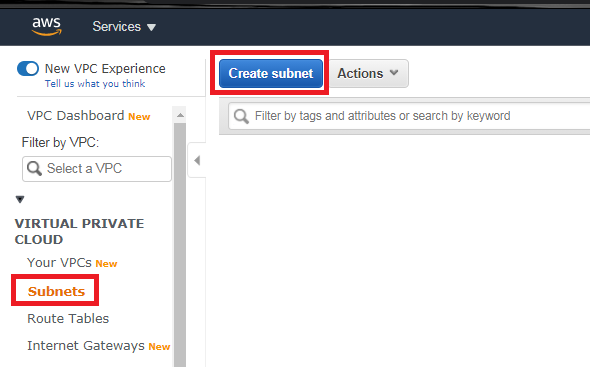
Modifying Public Subnet to assign Public IP to any instances on this subnet, you have to select the subnet and apply the feature.

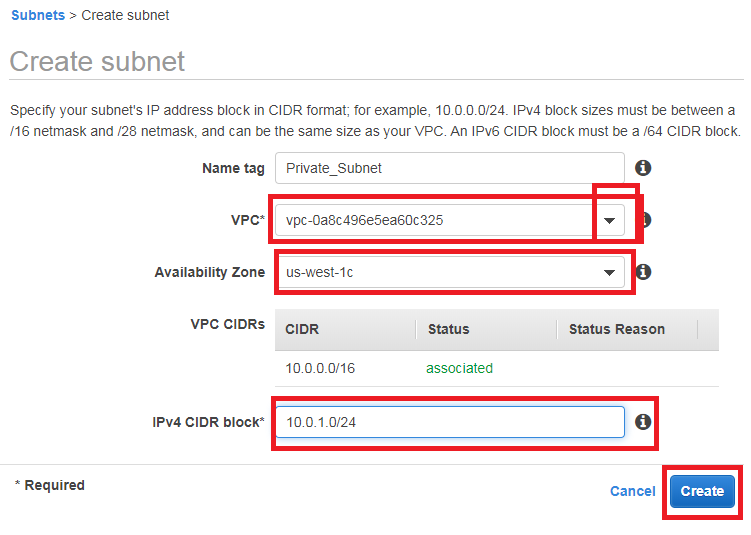


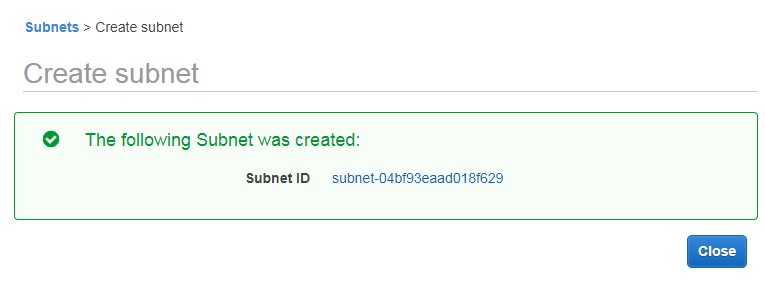




For Private Subnet,

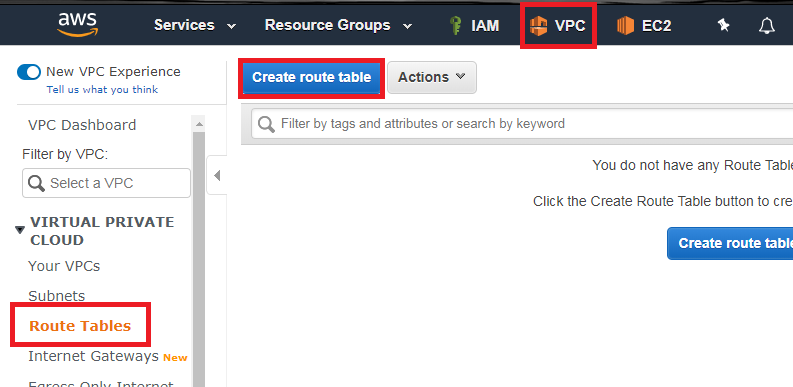


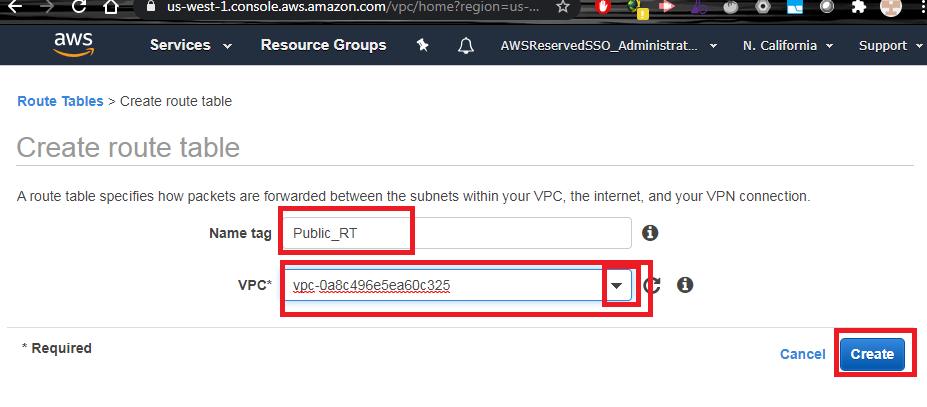


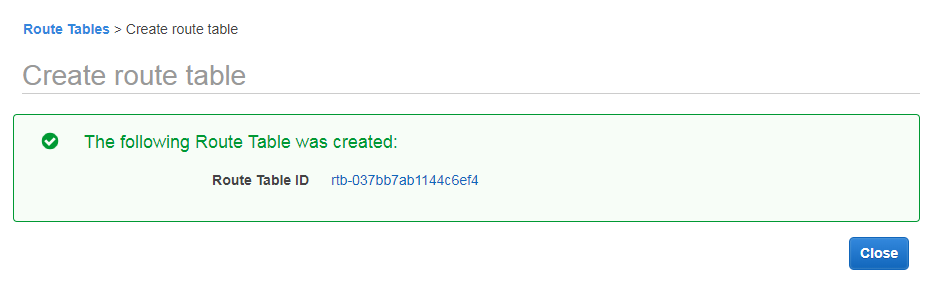


### Create Routing Tables

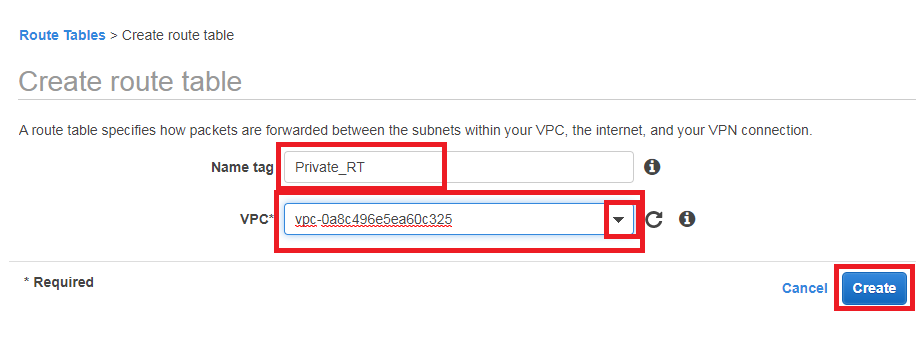
For this step, we create empty routing tables without attached or assign anything. First, we create the public routing table,

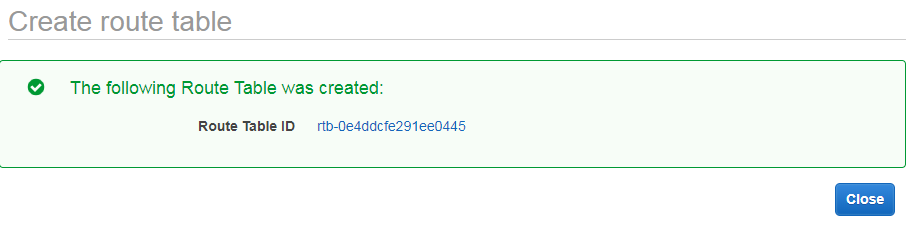






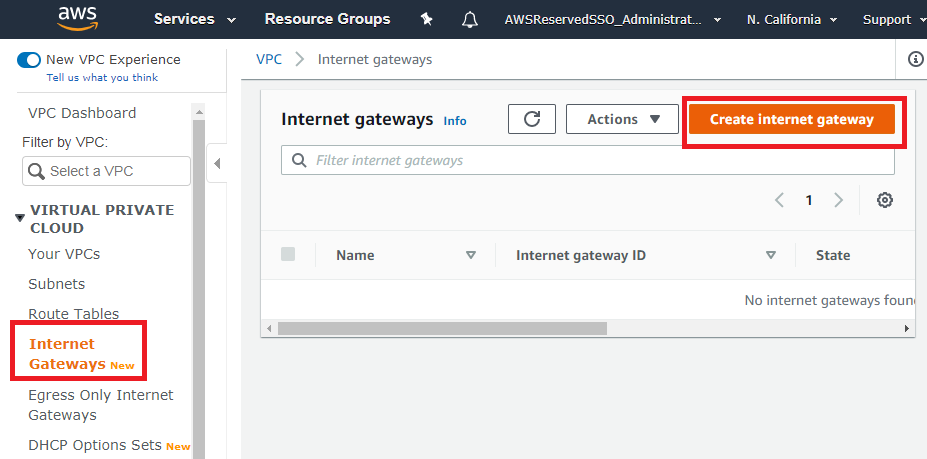
Then, we create the private routing table.

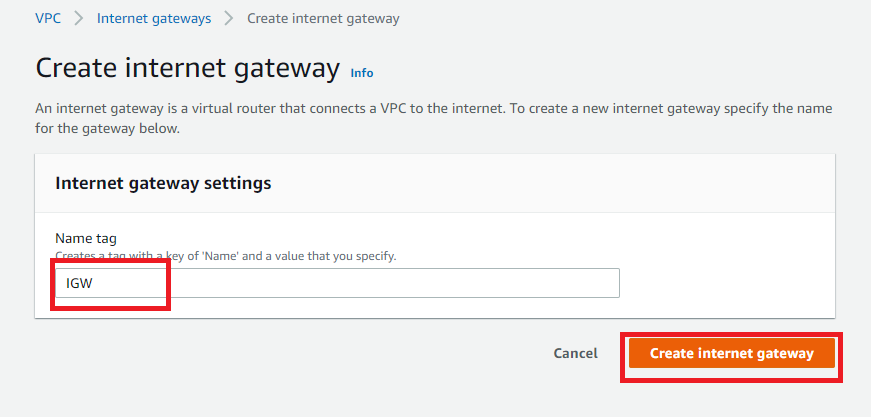




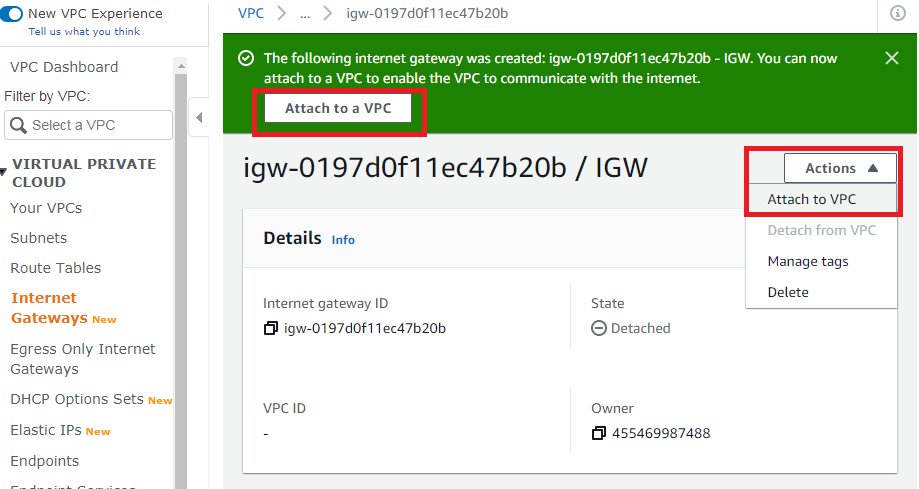
### Create Internet Gateway (IGW)

Create a IGW and then, attach to the VPC.

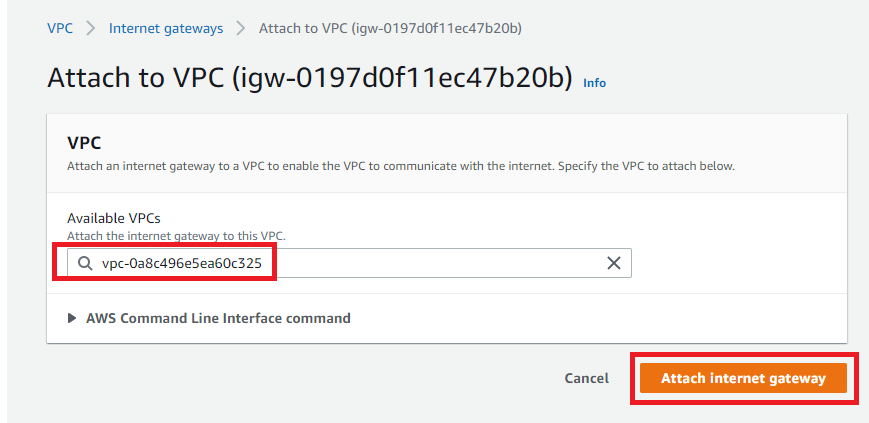




After it confirmation message, we attach to the VPC.



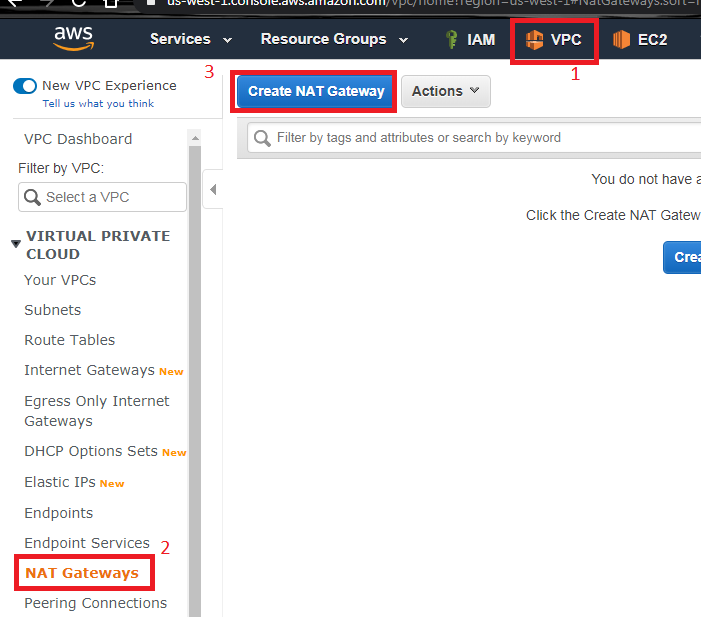
Select the VPC to attach the IGW,



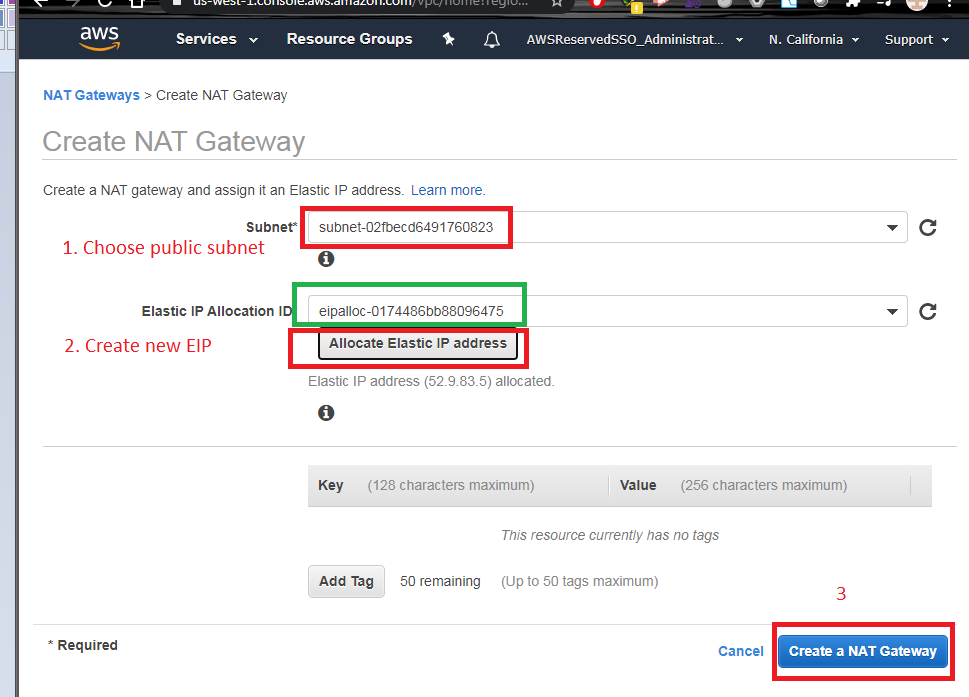
Confirmation message



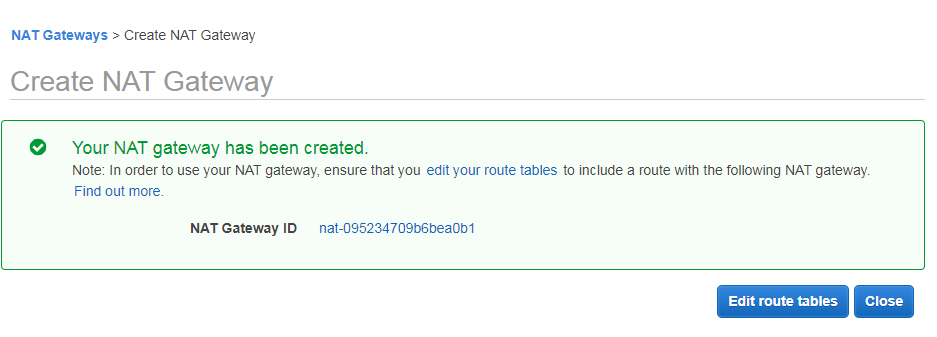
### Create NAT Gateway (NAT GW)



In this info window, you have to create an Elastic IP for assign it to the NAT Gateway, therefore you click on “Allocate Elastic IP Address” and AWS Console create and assign an EIP for this NAT GW automatically.

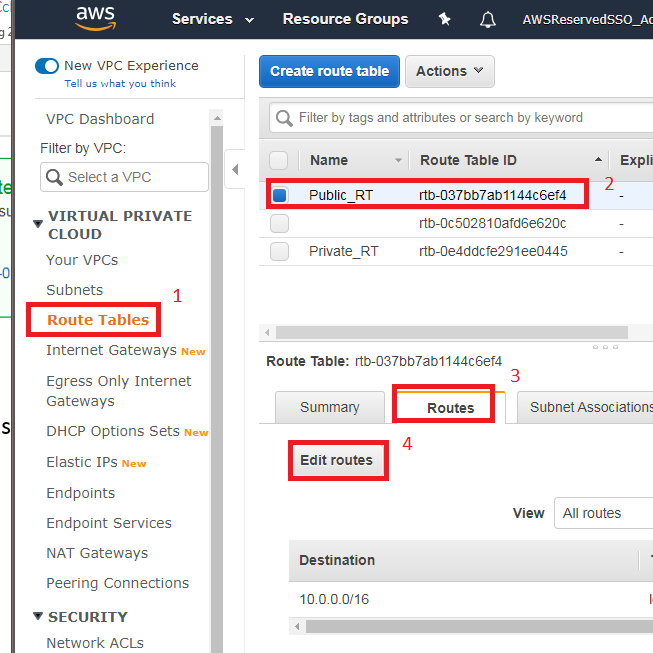


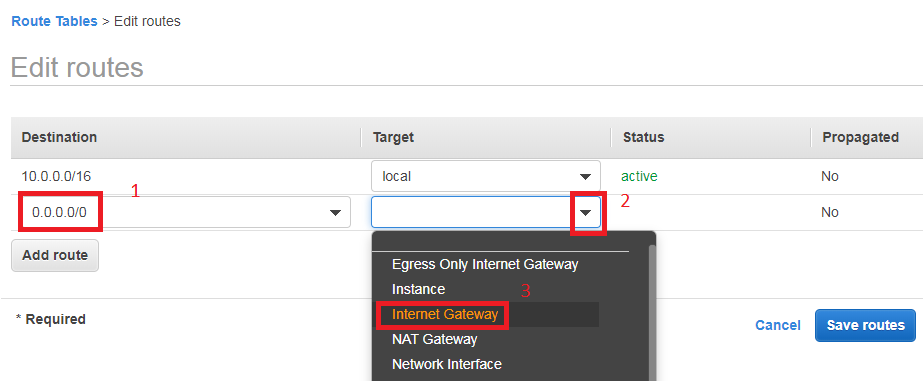
Confirmation message,

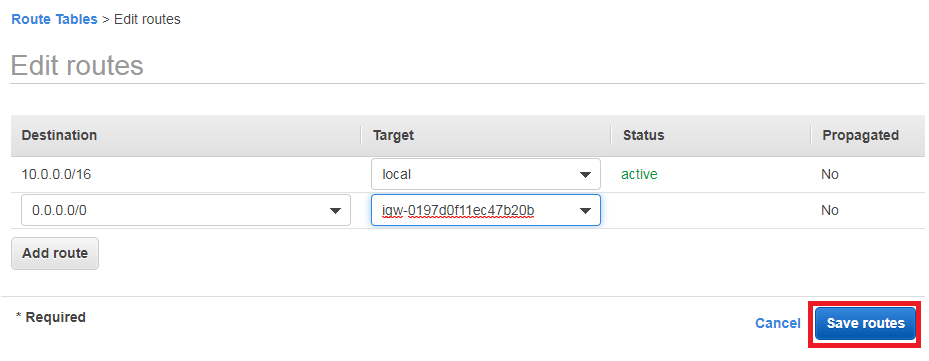


### Assign IGW and NAT GW to Routing Tables

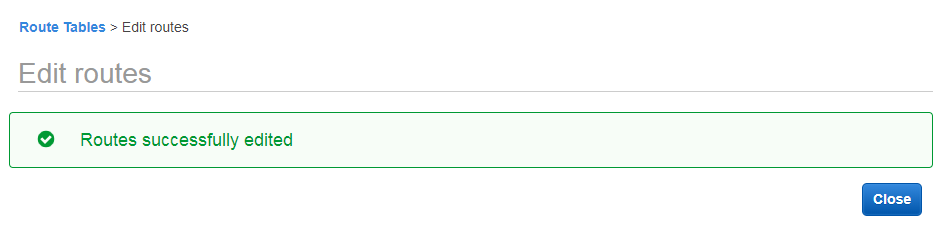
For Public Table, you modify routing tables to assign default route (0.0.0.0/0) to IGW.



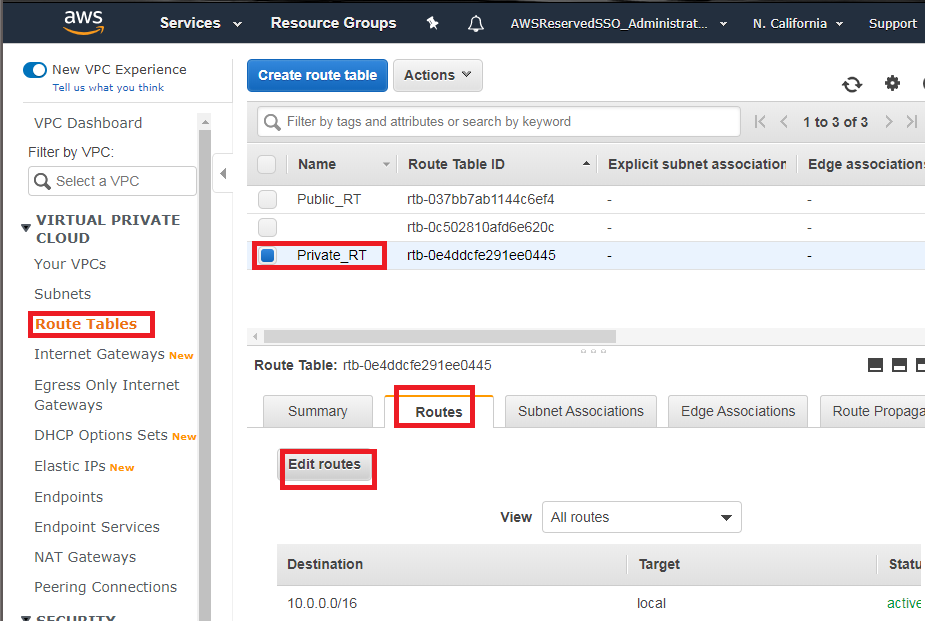


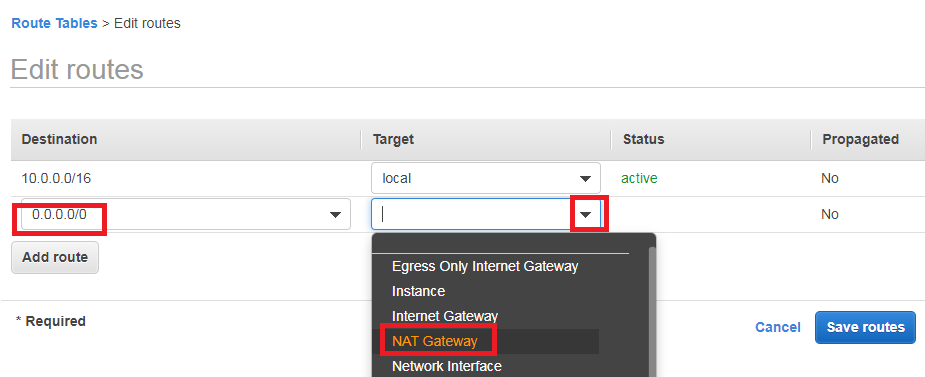


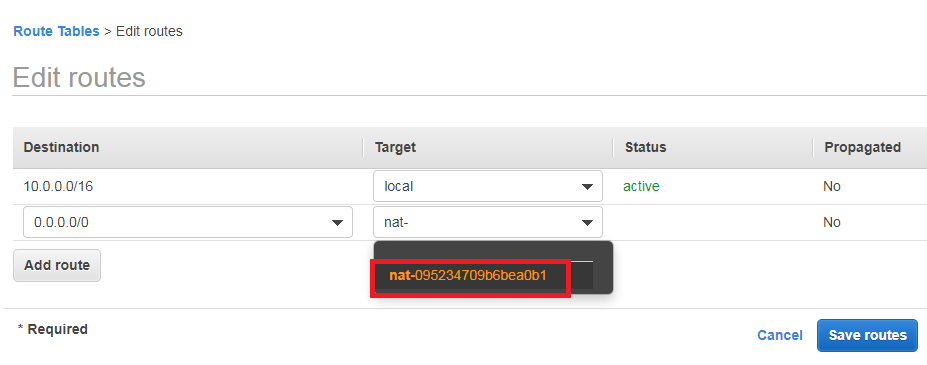
Confirmation message



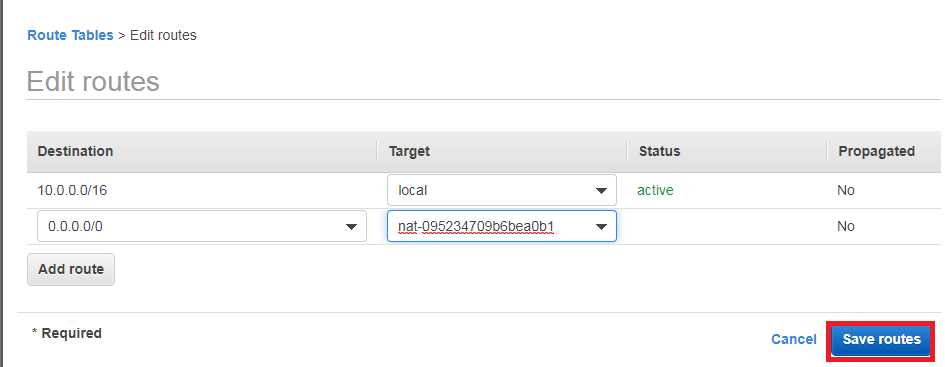
For Private Routing Table, you modify routing tables to assign default route (0.0.0.0/0) to NAT GW.

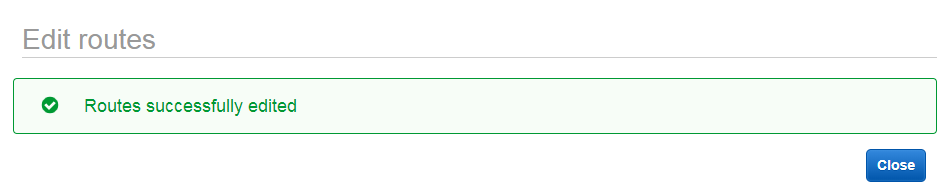






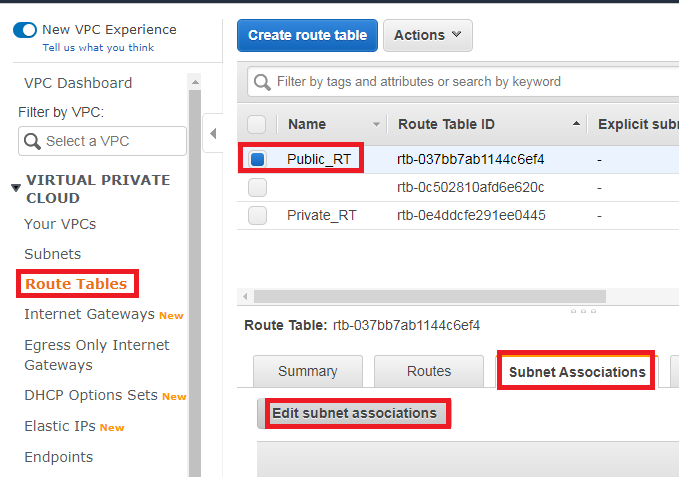
Confirmation message,

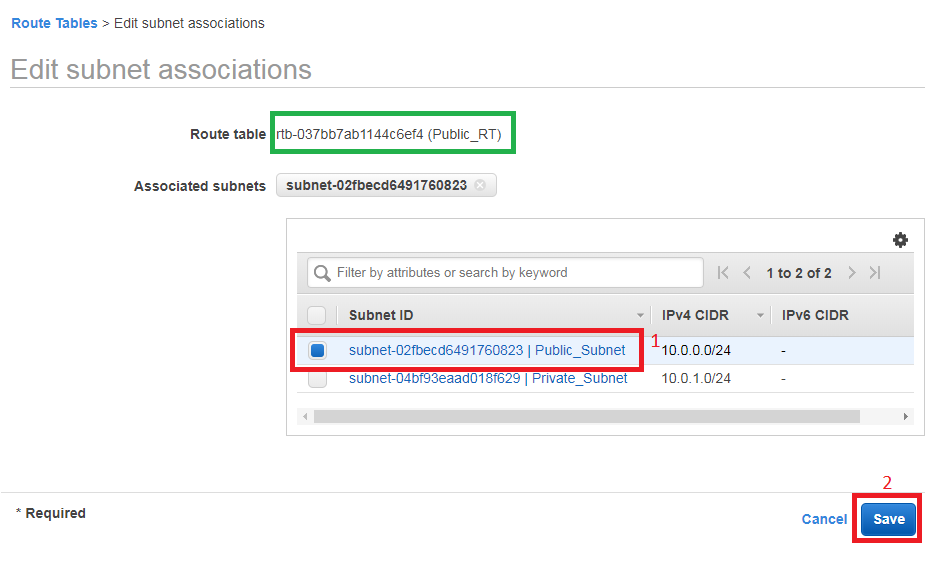




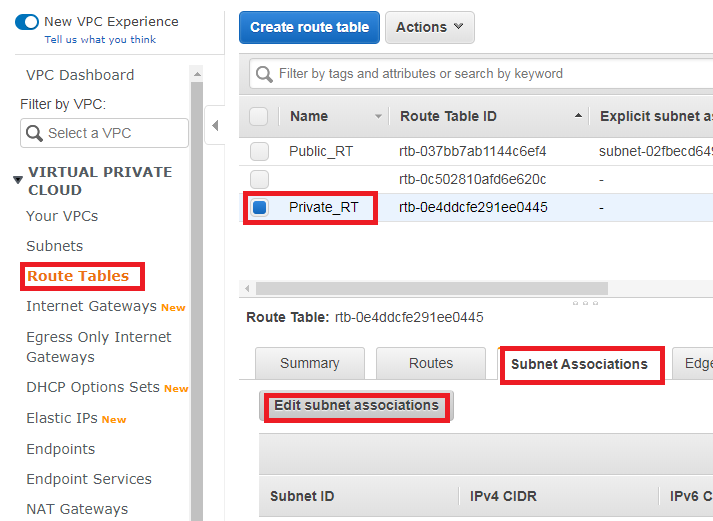
### Assign Routing Tables to Subnets

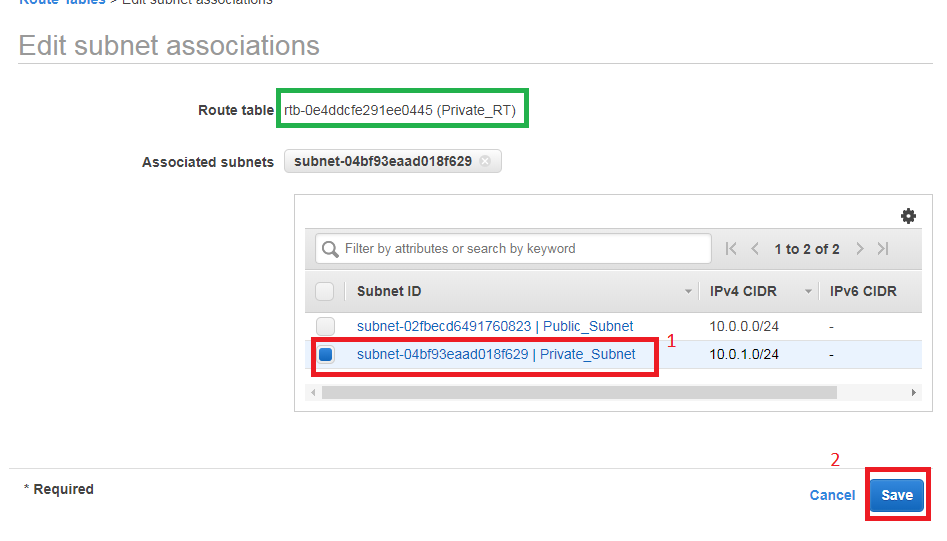
For Public Routing Table, you select the public subnet.





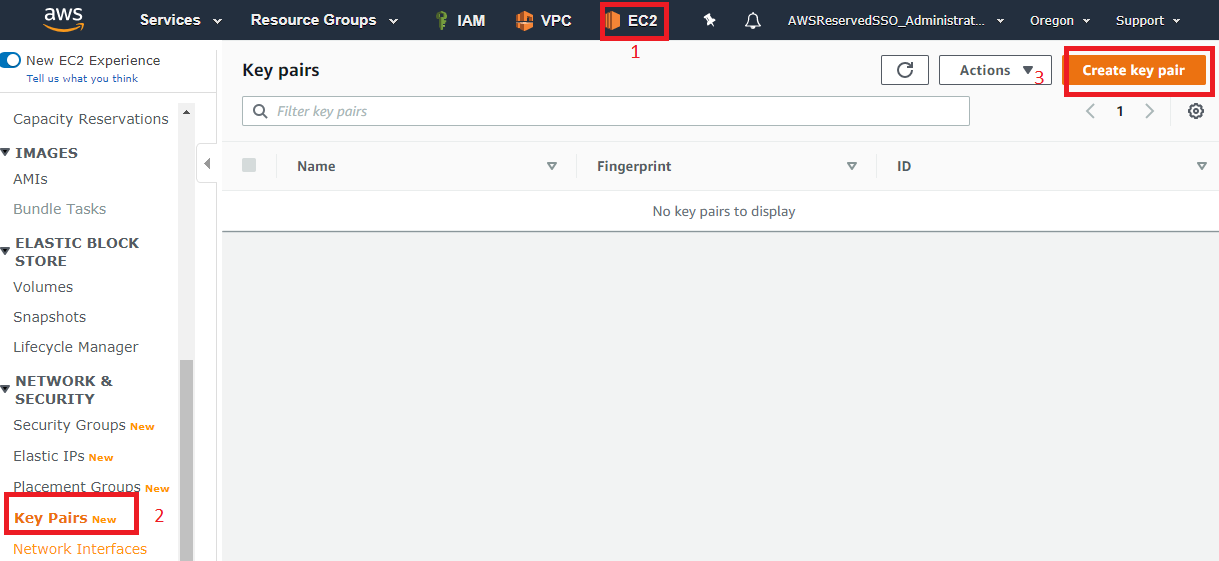
For Private Routing Table, you select private subnet.

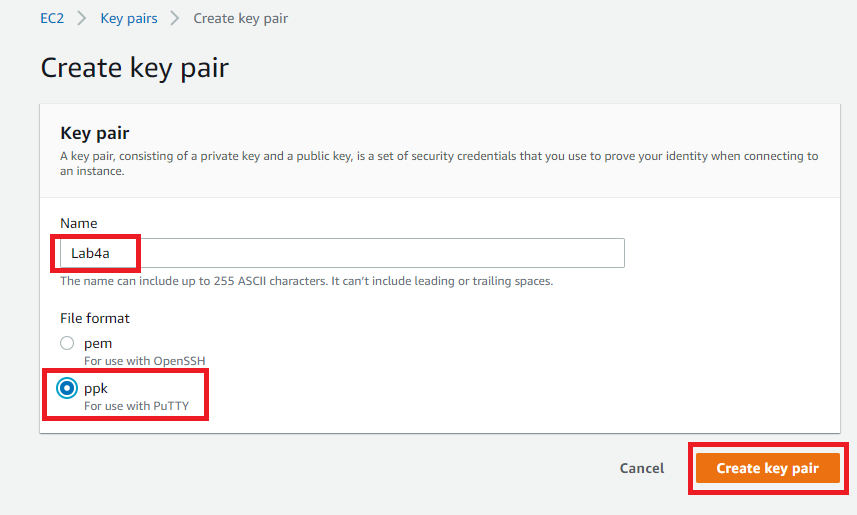




### Create Key Pair to connect to Instances

A Keypair, it is a file to authenticate ec2-user (default user for Amazon Linux AMI). For this step, we create that file and use to connect it.





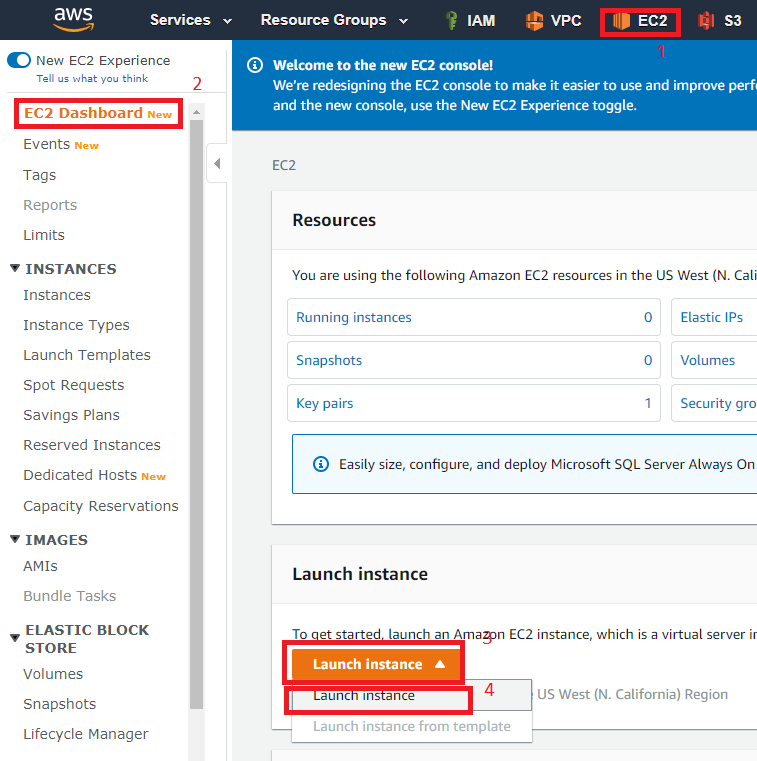
Store on the folder with the code of Command Line.

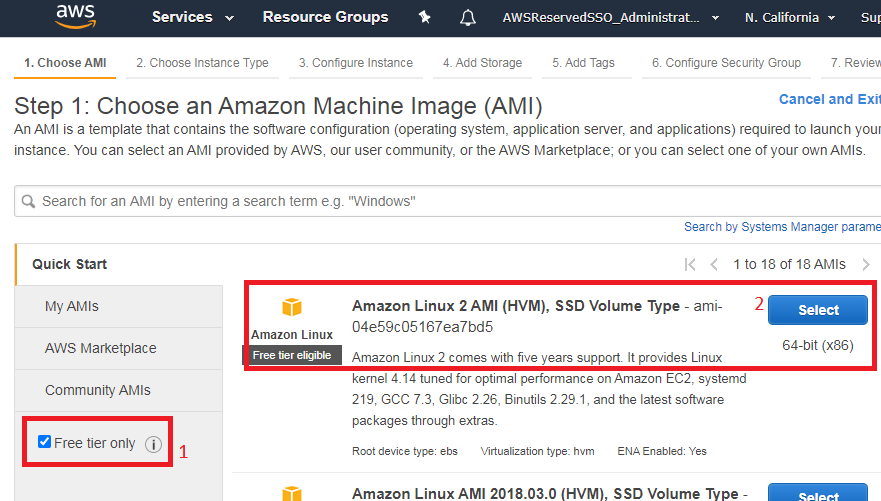
If you have Windows, we don’t need to use winscp to make the transformation to ppk. You download ppk file to use putty.

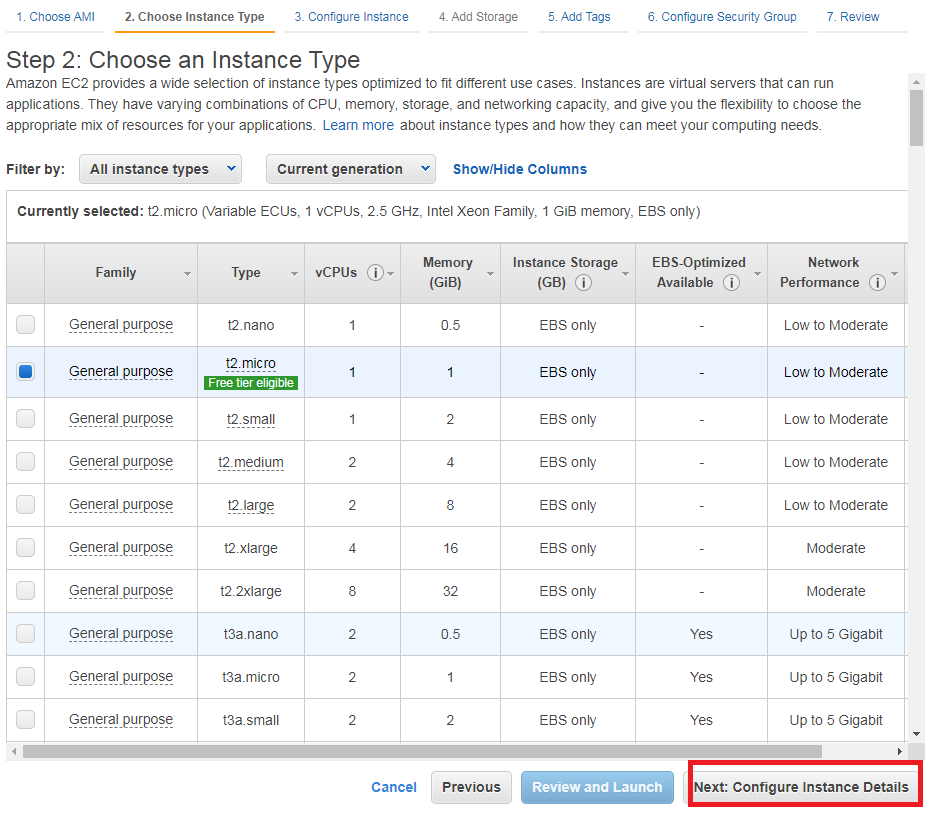
If you have MacOs, you don’t need to download the ppk format, you have to use pem file to use SSH in command line.

### Create EC2 instances

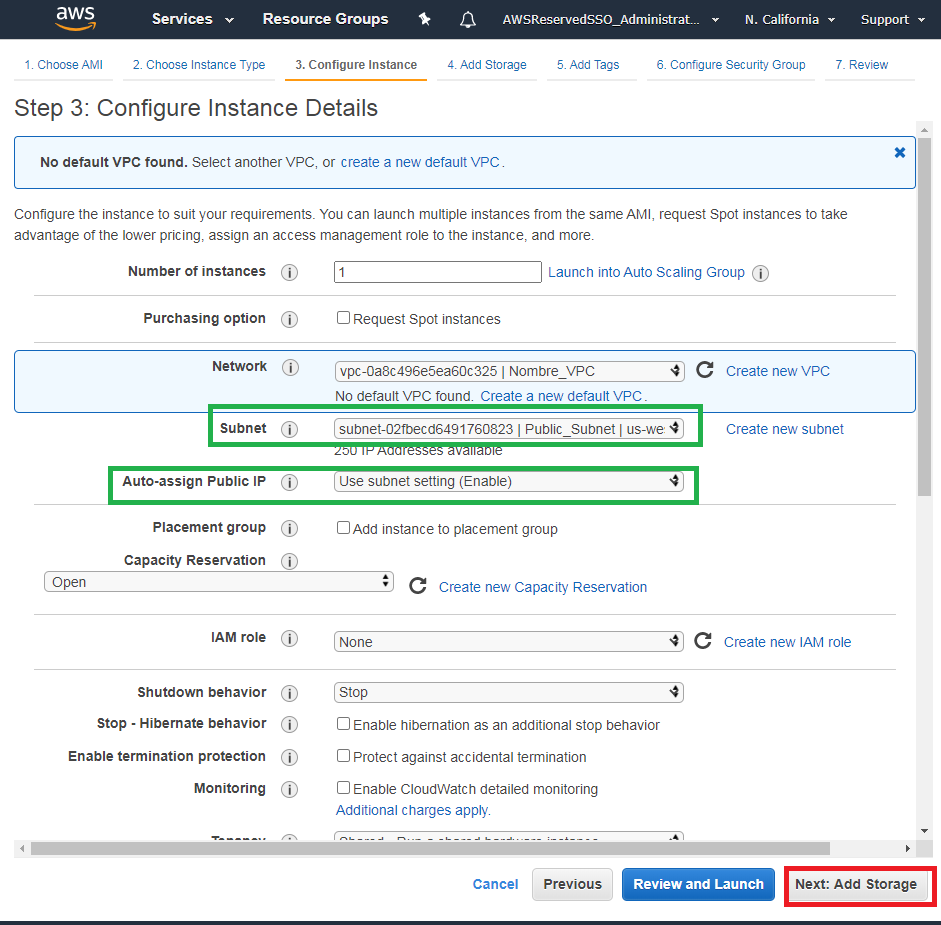
An instance is a Virtual Machine. Those steps are straight forward because we have to make it on detail on next session.



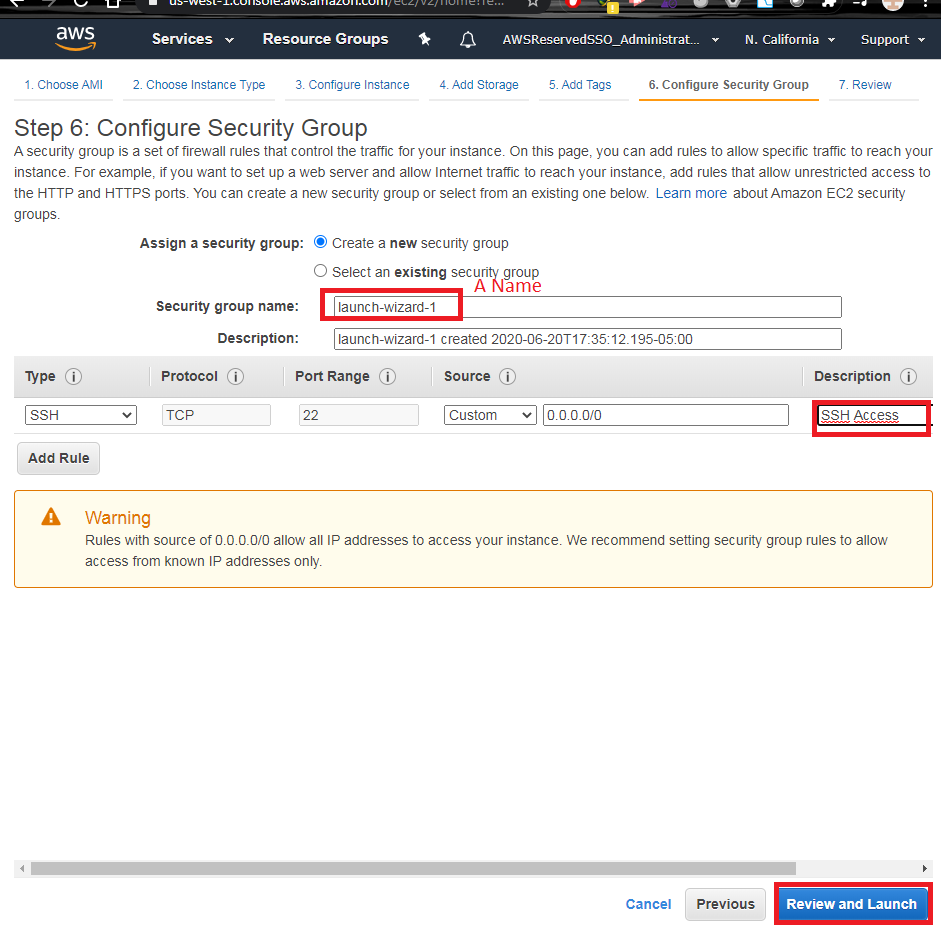




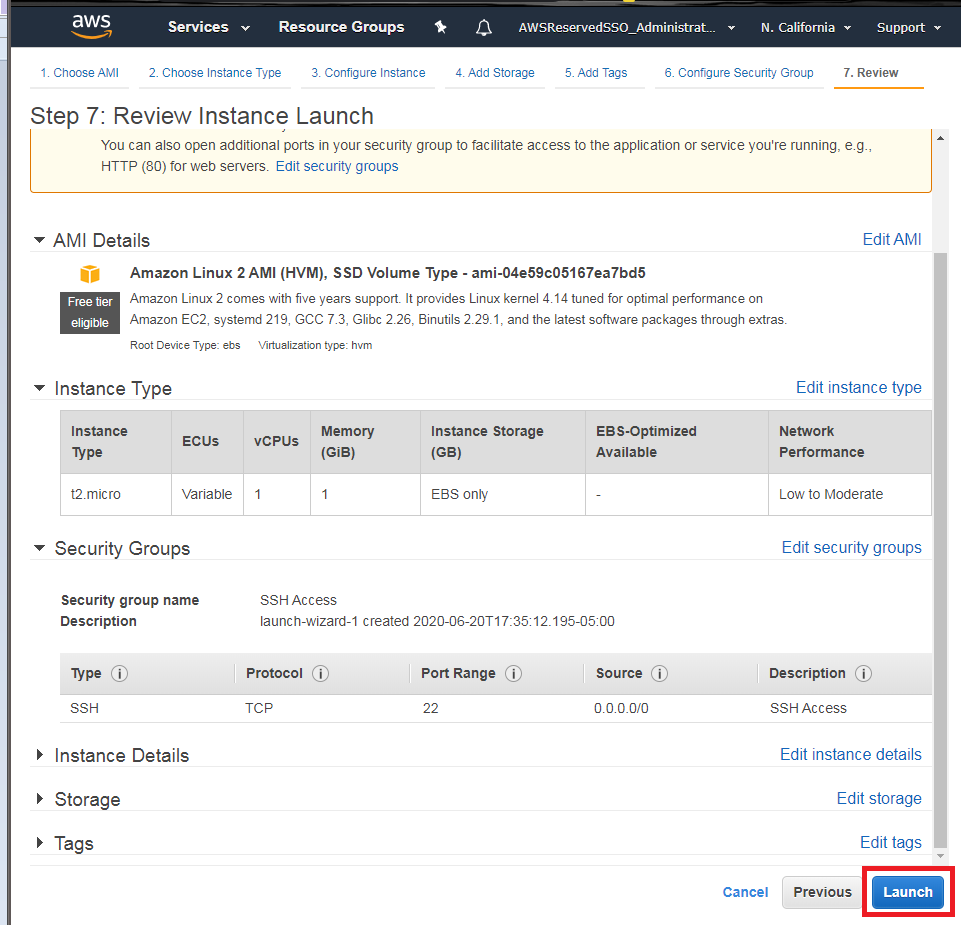
For this case, you create the public instance:

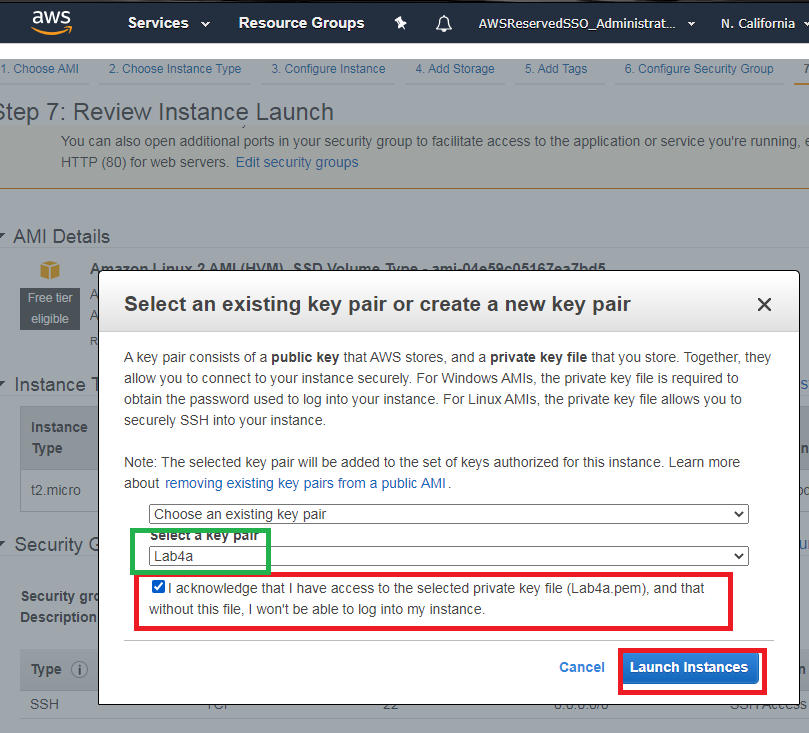


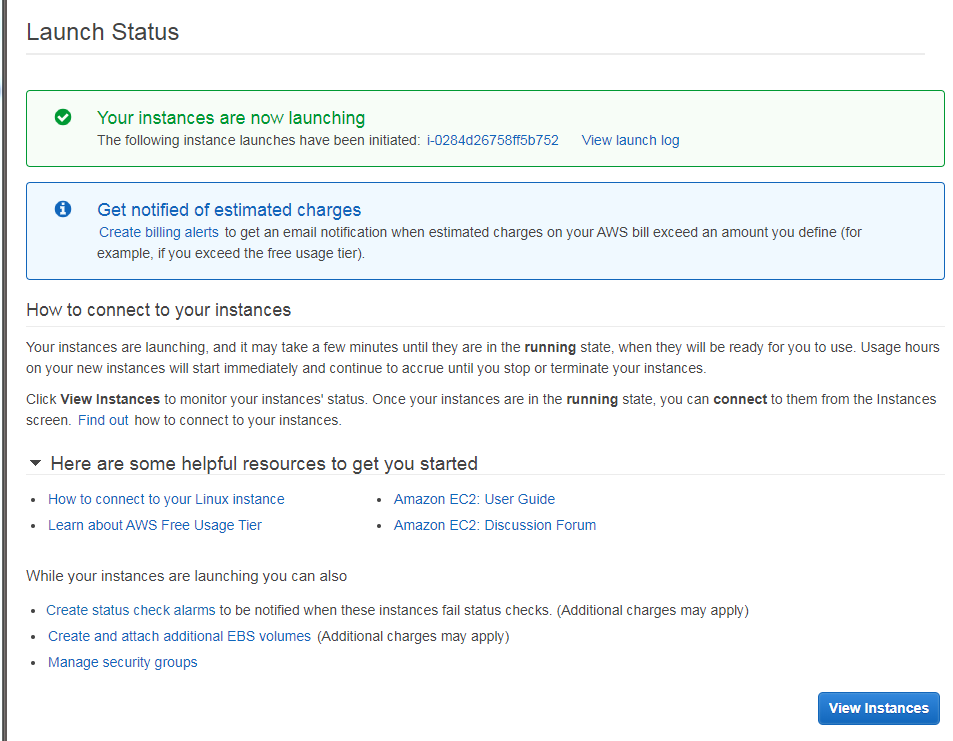
You have to choose next steps until you reach, Configuring Security Group



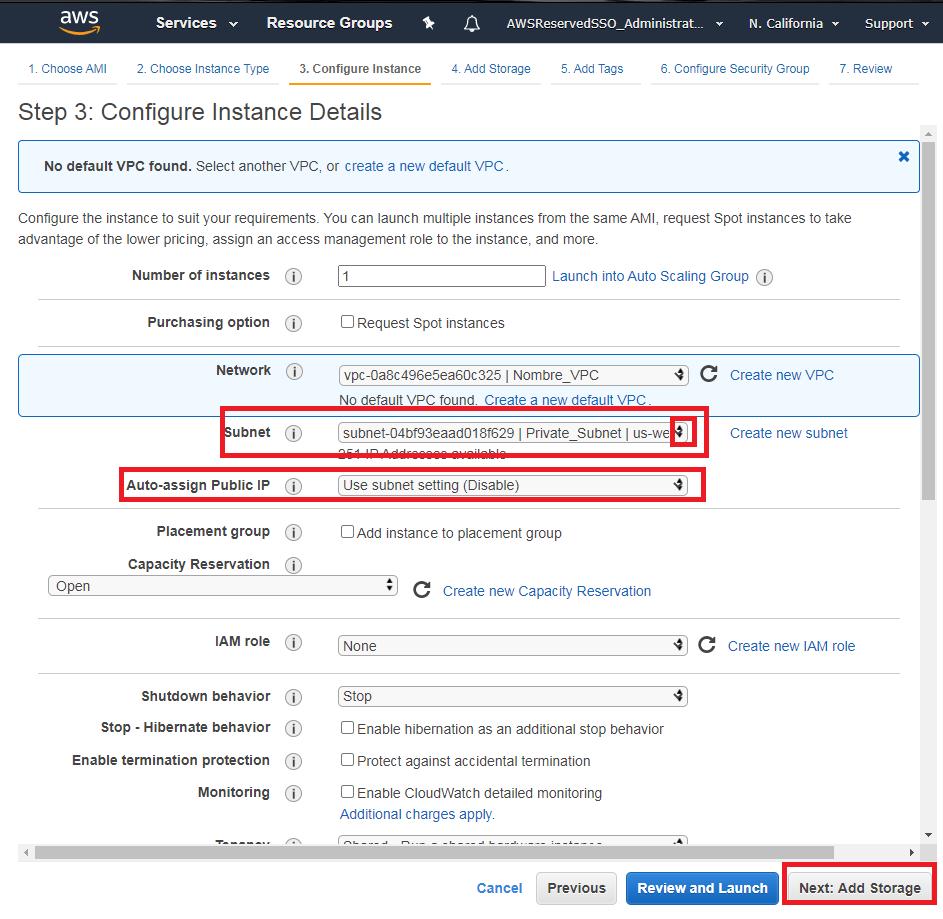
Review page, before of launching EC2 Instance.

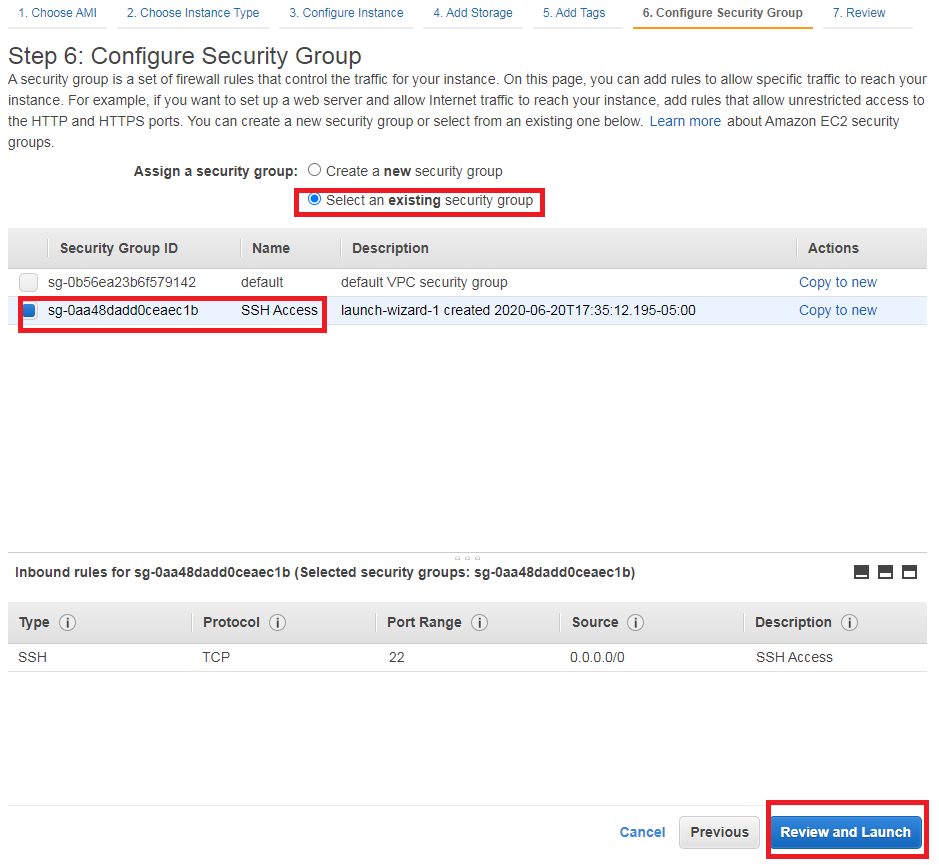


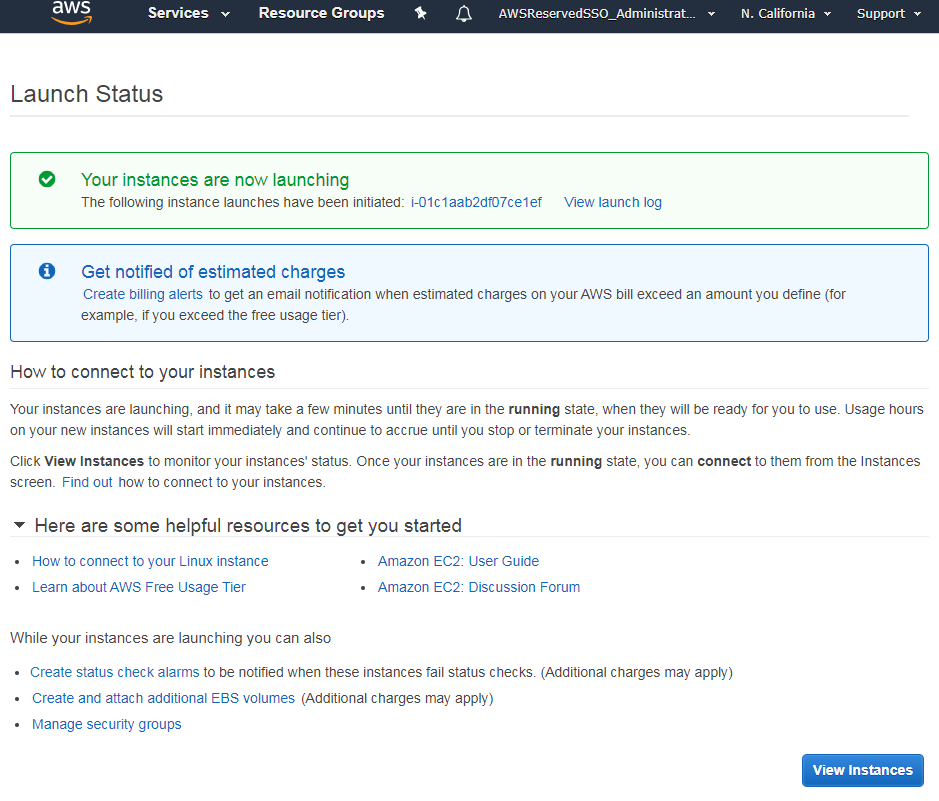




For Private Instances, the procedure is similar however, it changes on the subnet to create the instances and the security group is chosen from the previous step.







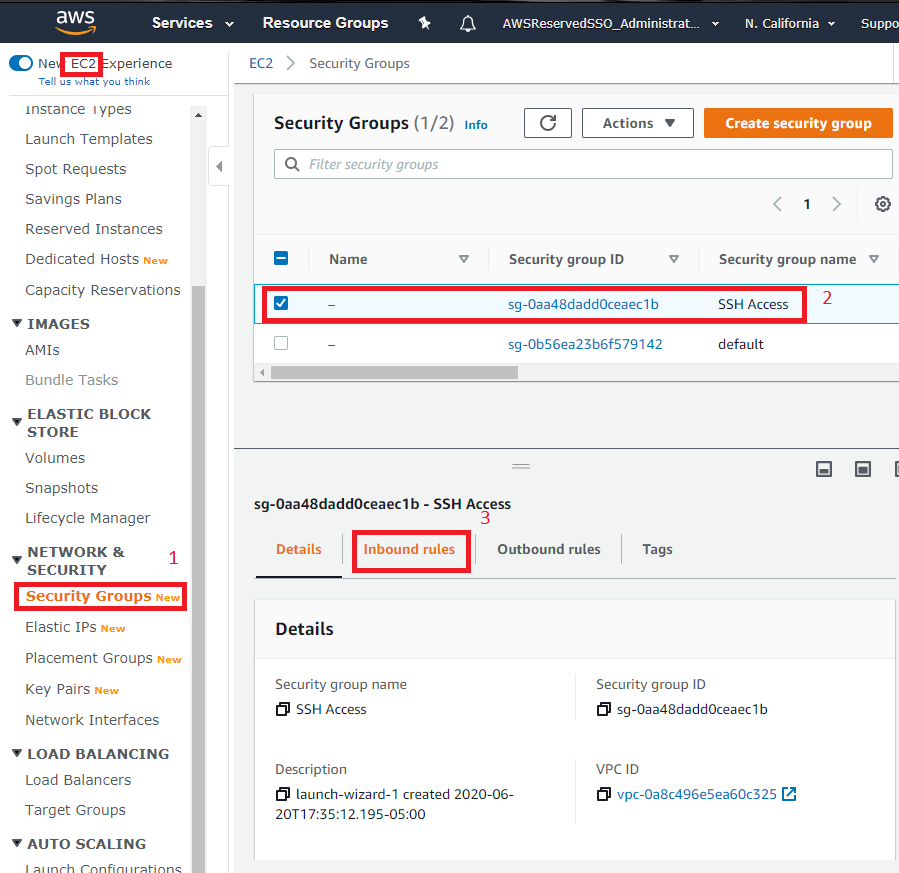
### Make the review

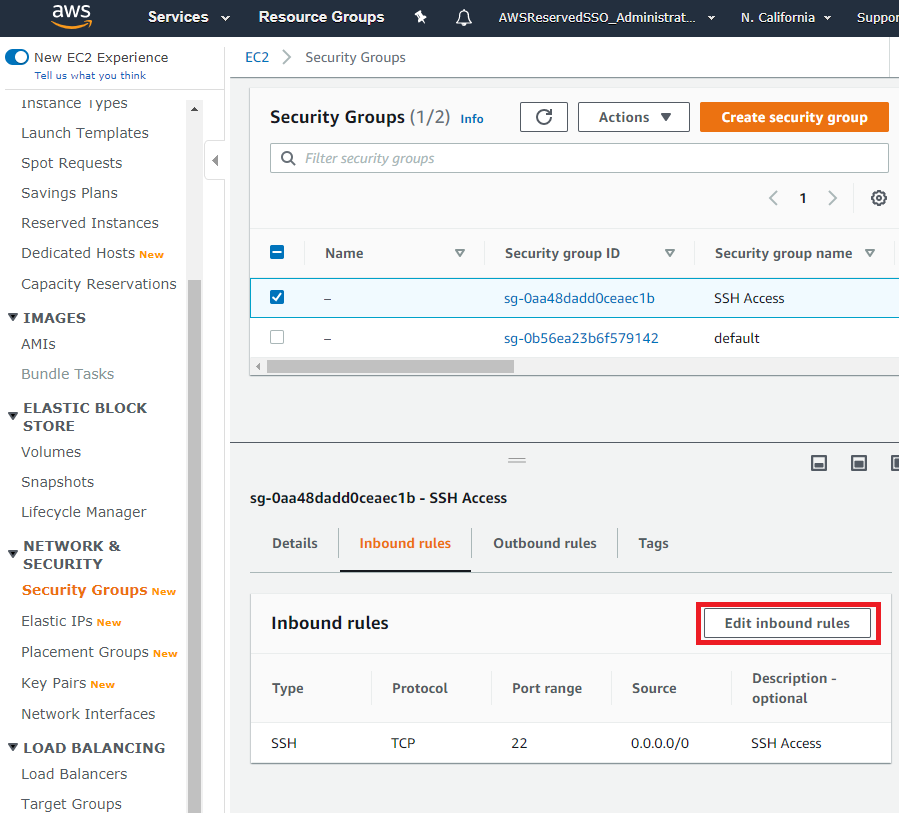
Use the same tools of Command Line (Windows): putty.

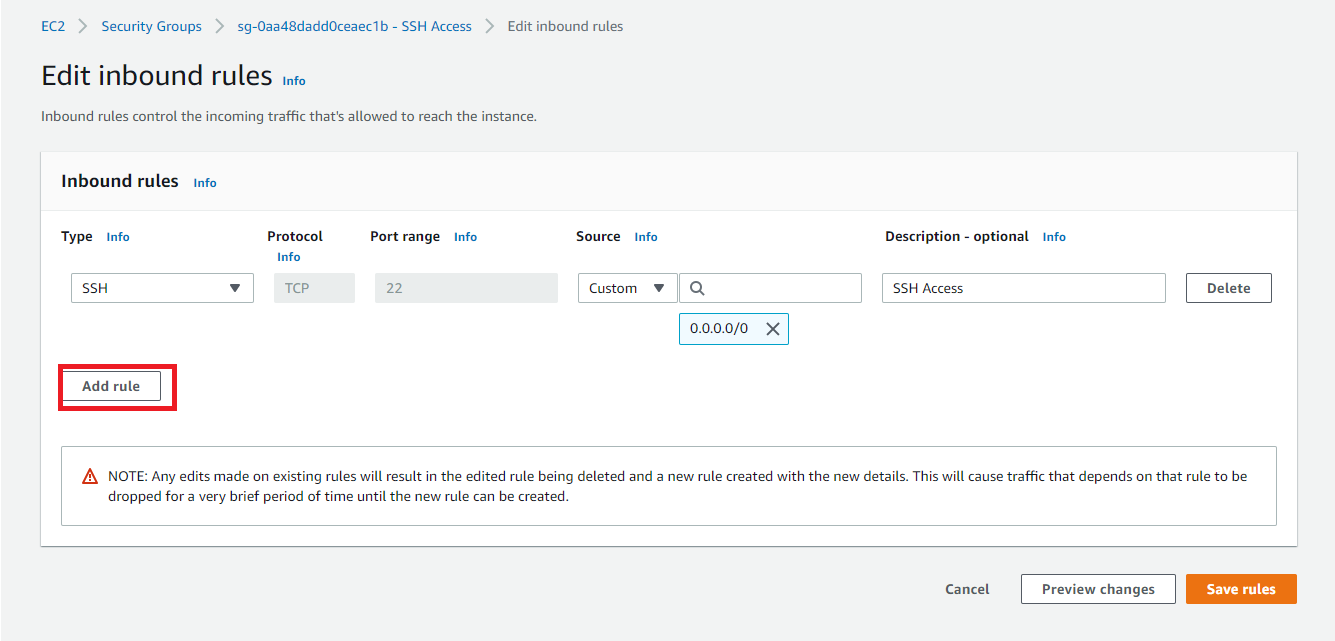
Check the “Review Configurations using Putty, SFTP and Browser” section, except the Add and Revoke Ports on Security Groups.

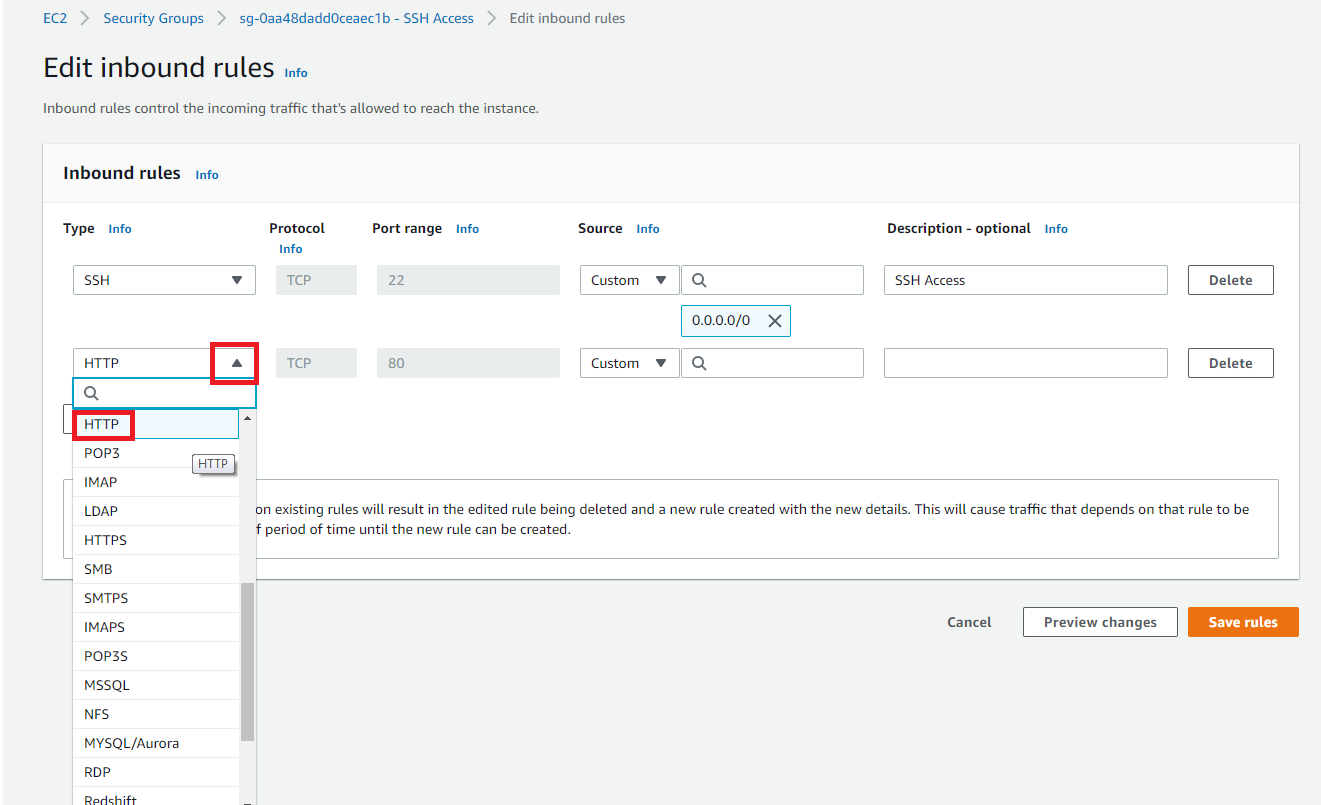
### Add and Revoke Ports on Security Group

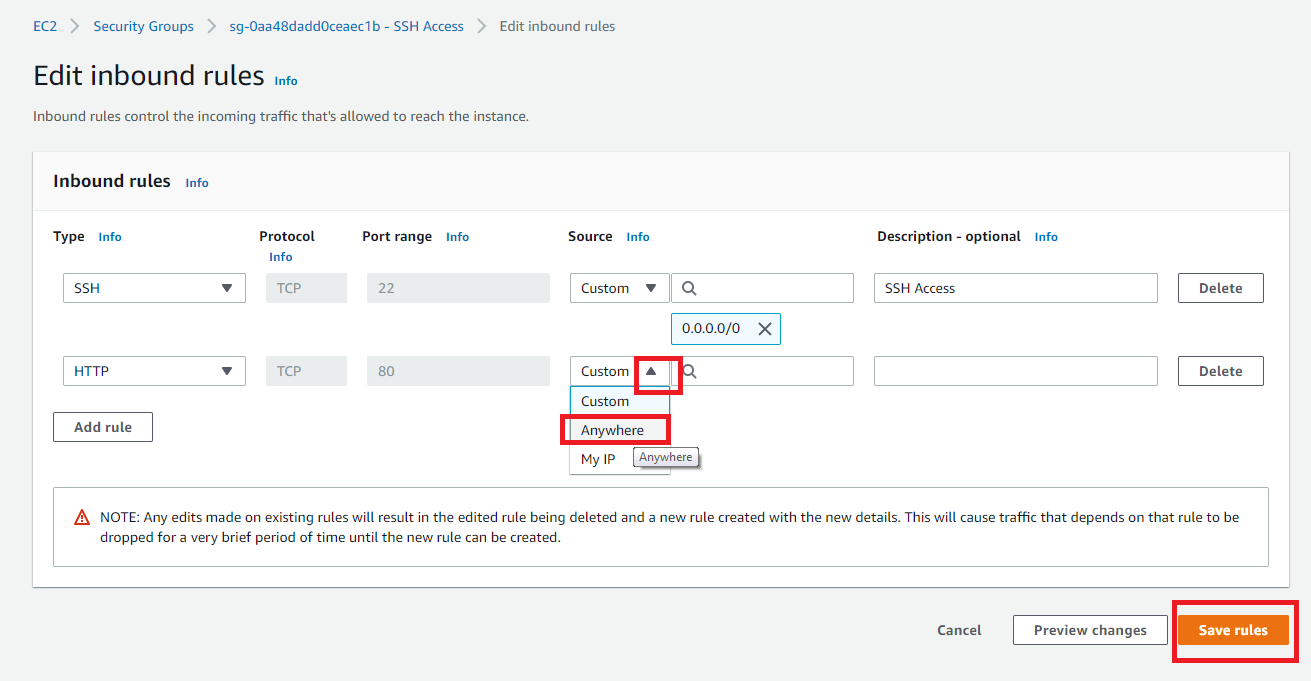
To add ports,

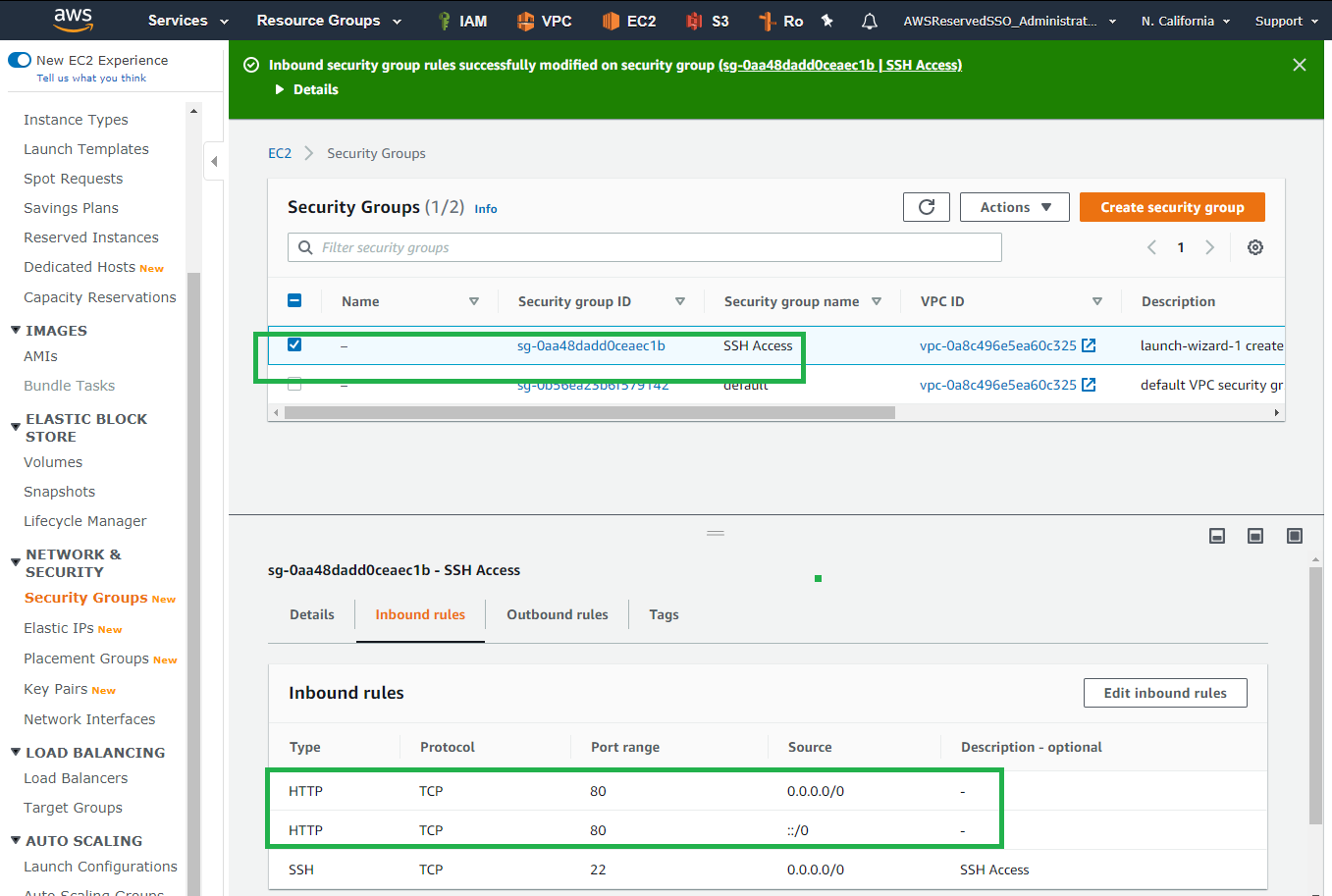




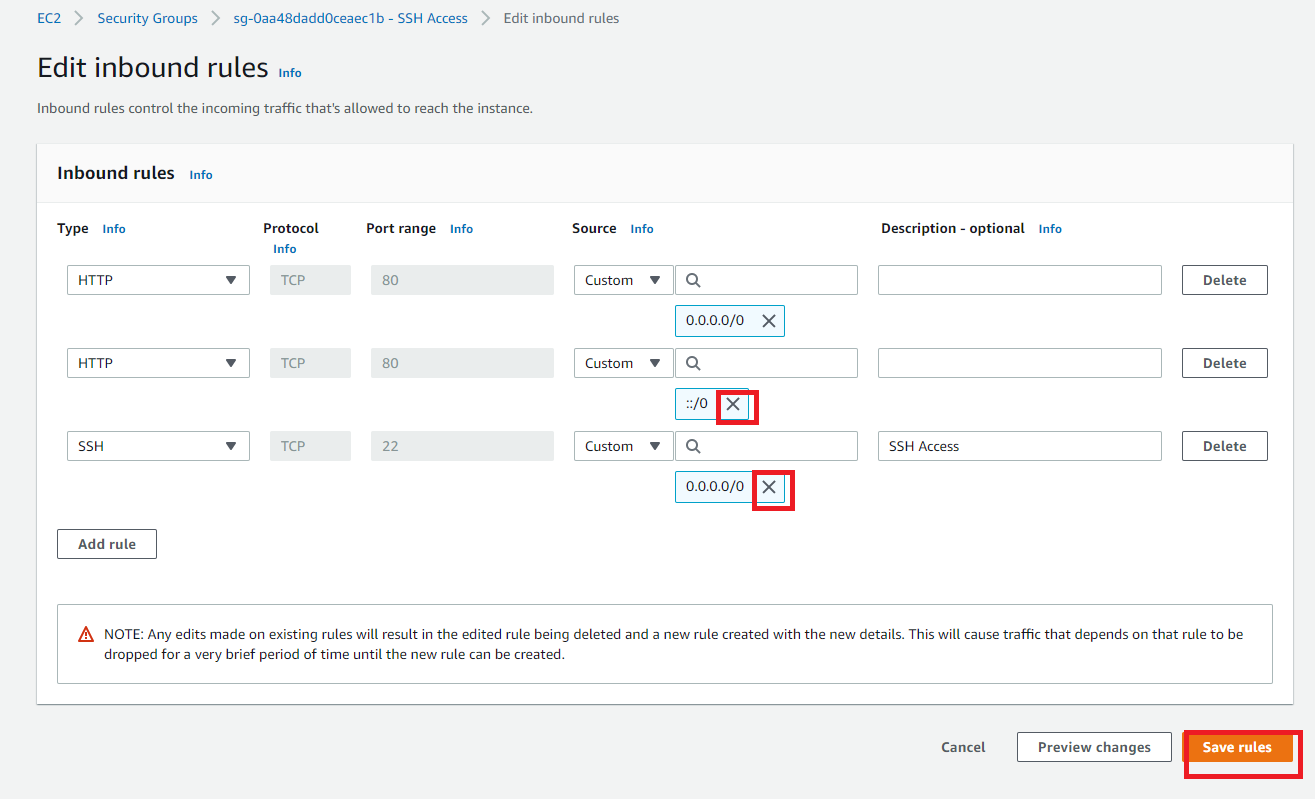








To revoke ports on Sec Groups, you have to edit the inbound rules:



## Lab 4A using Command Line (Windows)

rem Setear las variables

set vpcn\_Mask="10.0.0.0/16"

set pbsn1\_Mask="10.0.0.0/24"

set prsn2\_Mask="10.0.1.0/24"

set first\_az="us-east-1a"

set second\_az="us-east-1b"

### Create VPC, Public Subnet, IGW and Route Table

rem Crear la VPC

aws ec2 create-vpc --cidr-block %vpcn\_Mask%|jq ".Vpc.VpcId" >tmpFile

set /p vpcn\_Id= < tmpFile

rem Crear subred Publica

aws ec2 create-subnet --vpc-id %vpcn\_Id% --cidr-block %pbsn1\_Mask% --availability-zone %first\_az%|jq ".Subnet.SubnetId" >tmpFile

set /p pbsn1\_Id= < tmpFile

rem Crear el Internet Gateway IGW y asignarlo a la VPC

aws ec2 create-internet-gateway|jq ".InternetGateway.InternetGatewayId"  >tmpFile

set /p IGW\_Id= < tmpFile

aws ec2 attach-internet-gateway --vpc-id %vpcn\_Id% --internet-gateway-id %IGW\_Id%

rem Crear tabla de ruteo publica y asignarle IGW como ruta por defecto

aws ec2 create-route-table --vpc-id %vpcn\_Id%|jq ".RouteTable.RouteTableId" >tmpFile

set /p Public\_RT\_Id= < tmpFile

aws ec2 create-route --route-table-id %Public\_RT\_Id% --destination-cidr-block 0.0.0.0/0 --gateway-id %IGW\_Id%

rem Revisar Rutas de la Tabla de Ruteo

aws ec2 describe-route-tables --route-table-id %Public\_RT\_Id%



rem Asociar la tabla de ruta a la subred

aws ec2 associate-route-table  --subnet-id %pbsn1\_Id% --route-table-id %Public\_RT\_Id%

rem Permitir que las instancias que se ejecutan en la subred se hagan publicas

aws ec2 modify-subnet-attribute --subnet-id %pbsn1\_Id% --map-public-ip-on-launch



### Create EC2 Keys, Sec Groups. Choose AMI and create EC2 Instances.

rem Crear las llaves para el SSH a las nuevas instancias y convertirlas a PPK para usar Putty ya sea con puttygen o winscp

aws ec2 create-key-pair --key-name Lab4a --query "KeyMaterial" --output text > Lab4a.pem

winscp.com /keygen "Lab4a.pem" /output="Lab4a.ppk"

rem Crear los Security Groups para esa instancia

aws ec2 create-security-group --group-name "SSHAccess" --description "Security group for SSH access" --vpc-id %vpcn\_Id% |jq ".GroupId">tmpFile

set /p SSH\_Sec\_Group\_Id= < tmpFile

aws ec2 authorize-security-group-ingress --group-id %SSH\_Sec\_Group\_Id% --protocol tcp --port 22 --cidr 0.0.0.0/0

rem En el laboratorio de EC2 Inicial se mostrar la importancia de buscar una AMI correcto.

aws ec2 describe-images --owners amazon --filters "Name=name,Values=amzn2-ami-hvm-2.0.????????.?-x86\_64-gp2" "Name=state,Values=available" --query "reverse(sort\_by(Images, &CreationDate))[:1].ImageId" --output text >tmpFile

set /p AMI= < tmpFile

aws ec2 run-instances --image-id %AMI% --count 1 --instance-type t2.micro --key-name Lab4a --security-group-ids %SSH\_Sec\_Group\_Id% --subnet-id %pbsn1\_Id% --tag-specifications "ResourceType=instance,Tags=[{Key=ServerName,Value=A}]"



### Create Private Subnet, EIP, NAT Gateway, Private Route Table and EC2 Instance

rem Crear subred Privada

aws ec2 create-subnet --vpc-id %vpcn\_Id% --cidr-block %prsn2\_Mask% --availability-zone %second\_az%|jq ".Subnet.SubnetId" >tmpFile

set /p prsn2\_Id= < tmpFile

rem Solicitar una IP Elastica para hacer el Nat Gateway

aws ec2 allocate-address --domain vpc |jq ".AllocationId" >tmpFile

set /p NAT\_EIP= < tmpFile

rem Crear el NAT Gateway, asignarlo a una EIP Anterior.

aws ec2 create-nat-gateway --subnet-id  %pbsn1\_Id% --allocation-id %NAT\_EIP%|jq ".NatGateway.NatGatewayId" >tmpFile

set /p NATGW\_Id= < tmpFile

rem Crear tabla de ruteo para las redes privadas y asignar el NAT GW como ruta por defecto. Asociarla

aws ec2 create-route-table --vpc-id %vpcn\_Id%|jq ".RouteTable.RouteTableId" >tmpFile

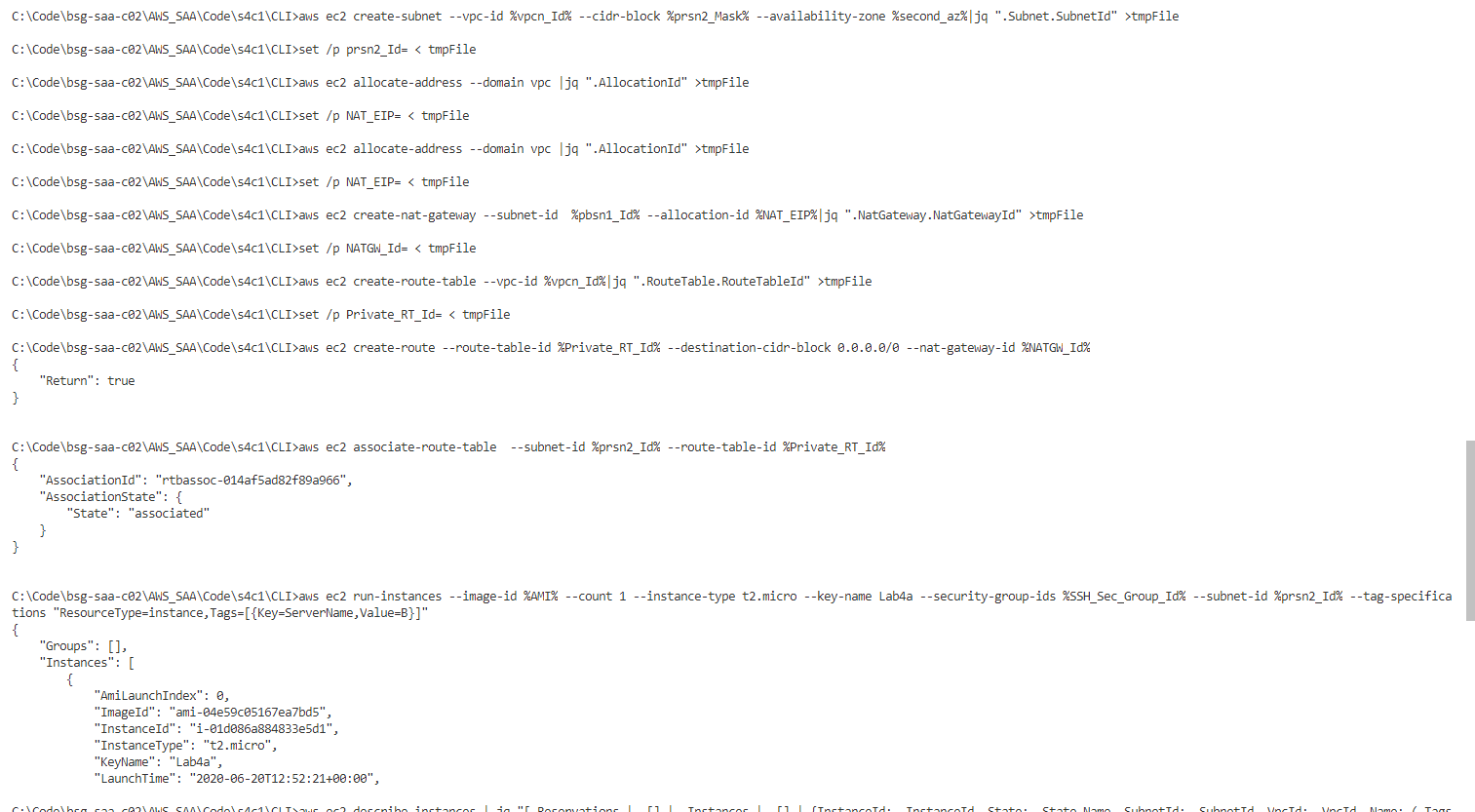
set /p Private\_RT\_Id= < tmpFile

aws ec2 create-route --route-table-id %Private\_RT\_Id% --destination-cidr-block 0.0.0.0/0 --nat-gateway-id %NATGW\_Id%

aws ec2 associate-route-table  --subnet-id %prsn2\_Id% --route-table-id %Private\_RT\_Id%

rem Genera la segunda Instancia

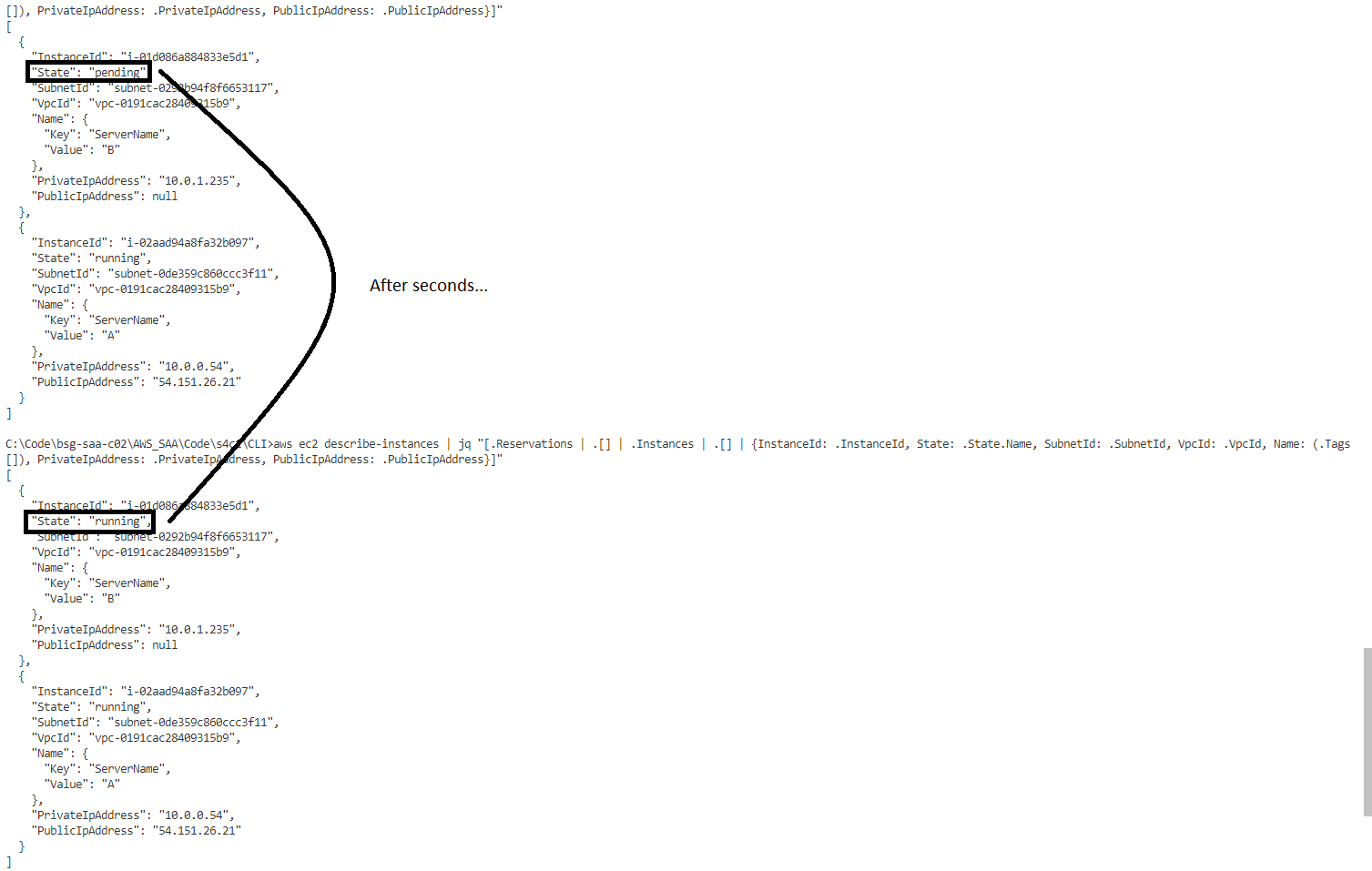
aws ec2 run-instances --image-id %AMI% --count 1 --instance-type t2.micro --key-name Lab4a --security-group-ids %SSH\_Sec\_Group\_Id% --subnet-id %prsn2\_Id% --tag-specifications "ResourceType=instance,Tags=[{Key=ServerName,Value=B}]"



### Get Information about Instances

rem Traer estados de la Instancias

aws ec2 describe-instances | jq "[.Reservations | .[] | .Instances | .[] | {InstanceId: .InstanceId, State: .State.Name, SubnetId: .SubnetId, VpcId: .VpcId, Name: (.Tags[]), PrivateIpAddress: .PrivateIpAddress, PublicIpAddress: .PublicIpAddress}]"



rem Traer Datos especificos de instancia A. Revisar contenido de Read\_A.jq

aws ec2 describe-instances | jq -f Read\_A.jq

aws ec2 describe-instances | jq -f Read\_A.jq|jq ".[].PublicIpAddress" >tmpFile

set /p A\_IP= < tmpFile



## Review Configurations using Putty, SFTP and Browser

rem Enviar la llave a la Instancia Publica para luego desde alli conectarse a la IP Privada

rem Aquí la IP A es la IP de la Instancia Publica

psftp.exe -i "Lab4a.ppk" ec2-user@%A\_IP%

rem Luego alli enviar el codigo para subir el certificado y salir

put Lab4a.pem

chmod 400 Lab4a.pem

exit

rem Ingresar a la instancia publica por SSH y dejar ejecutando en el SSH  "sudo python -m SimpleHTTPServer 80"

putty.exe -i "Lab4a.ppk" ec2-user@%A\_IP%

rem Mirar la configuracion de la maquina actual

ip a

rem Conectarse por SSH a la Instancia Privada y desde alli escribir

rem Aquí la Ip mencionada es la IP de la instancia privada

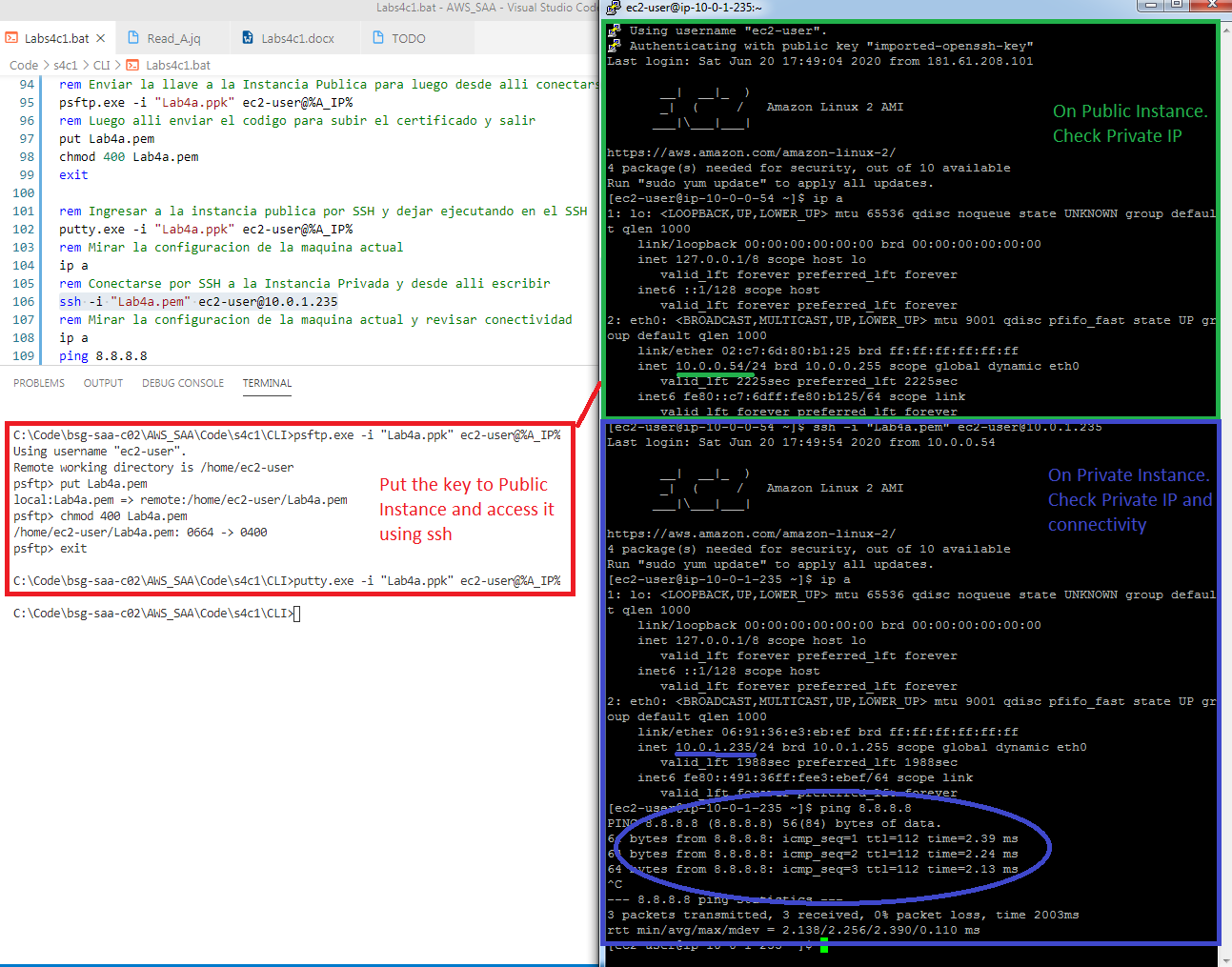
ssh -i "Lab4a.pem" ec2-user@10.0.1.235

rem Mirar la configuracion de la maquina actual y revisar conectividad

ip a

ping 8.8.8.8

exit



rem Dentro de la instancia ejecutar

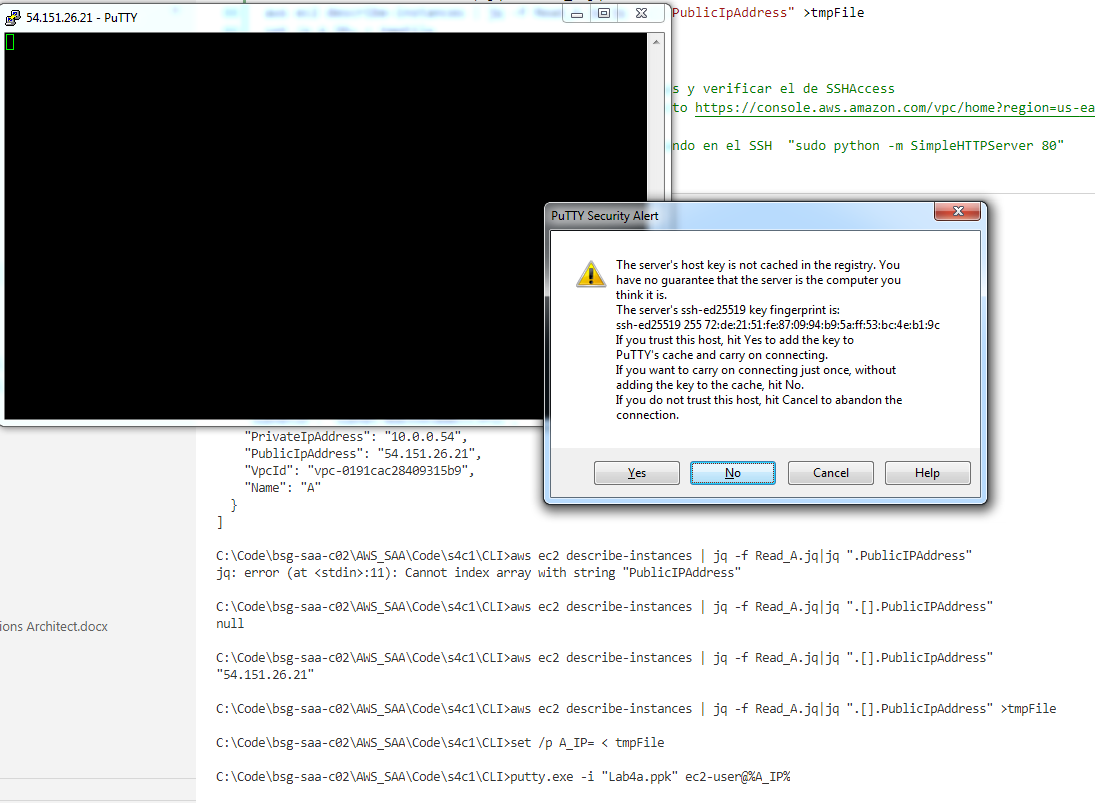
sudo python -m SimpleHTTPServer 80

### Add Port to Security Group

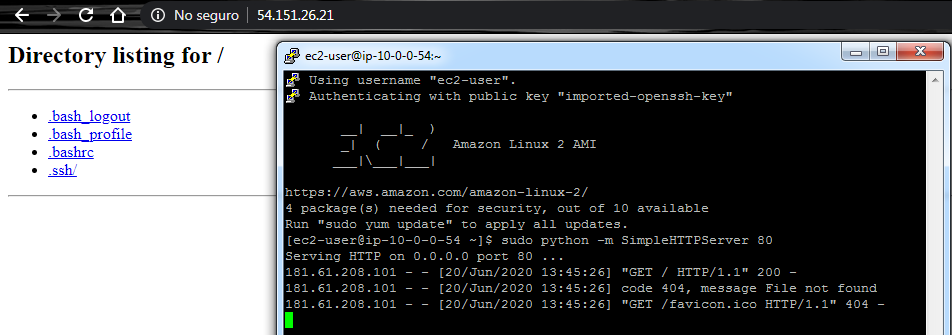
rem Intentar ingresar por un navegador a esa IP Publica

rem Modificar el Security Group para habilitar el puerto 80

aws ec2 authorize-security-group-ingress --group-id %SSH\_Sec\_Group\_Id% --protocol tcp --port 80 --cidr 0.0.0.0/0



rem Intentar ingresar por un navegador a esa IP Publica



### Delete Port to Security Group

rem Eliminar el ingreso del Security Group anterior

aws ec2 revoke-security-group-ingress --group-id %SSH\_Sec\_Group\_Id% --protocol tcp --port 80 --cidr 0.0.0.0/0

rem Volver a intentar ingresar por un navegador a esa IP

## Clean resources

### For Web Management Console

EC2: Terminate Instances

EC2: Security Groups

EC2: KeyPairs

VPC: NAT Gateway

VPC: EIP (Release)

VPC: IGW (Detach and then Delete)

VPC: Subnets

VPC: RT

VPC: VPC

### For Command Line (Windows)

rem ----- ELIMINAR RECURSOS ----

aws ec2 terminate-instances --instance-ids "i-01d086a884833e5d1" "i-02aad94a8fa32b097"

aws ec2 delete-security-group --group-id %SSH\_Sec\_Group\_Id%

aws ec2 delete-subnet --subnet-id %prsn2\_Id%

aws ec2 delete-nat-gateway --nat-gateway-id %NATGW\_Id%

aws ec2 delete-route-table --route-table-id %Private\_RT\_Id%

aws ec2 release-address --allocation-id %NAT\_EIP%

aws ec2 delete-subnet --subnet-id %pbsn1\_Id%

aws ec2 delete-route-table --route-table-id %Public\_RT\_Id%

aws ec2 detach-internet-gateway --internet-gateway-id %IGW\_Id% --vpc-id %vpcn\_Id%

aws ec2 delete-internet-gateway --internet-gateway-id %IGW\_Id%

aws ec2 delete-vpc --vpc-id %vpcn\_Id%

# Evidences to send

To have a review, the student has to send some screenshots to instructor email:

1. The first screenshot of [Review Configurations using Putty, SFTP and Browser](#_Review_Configurations_using). Showing SSH connection from Public Instance to Private Instances, and both different IPs.
2. The last screenshot of [Review Configurations using Putty, SFTP and Browser](#_Review_Configurations_using). Showing the browser with list of users and pythons script running.