LABORATORIO

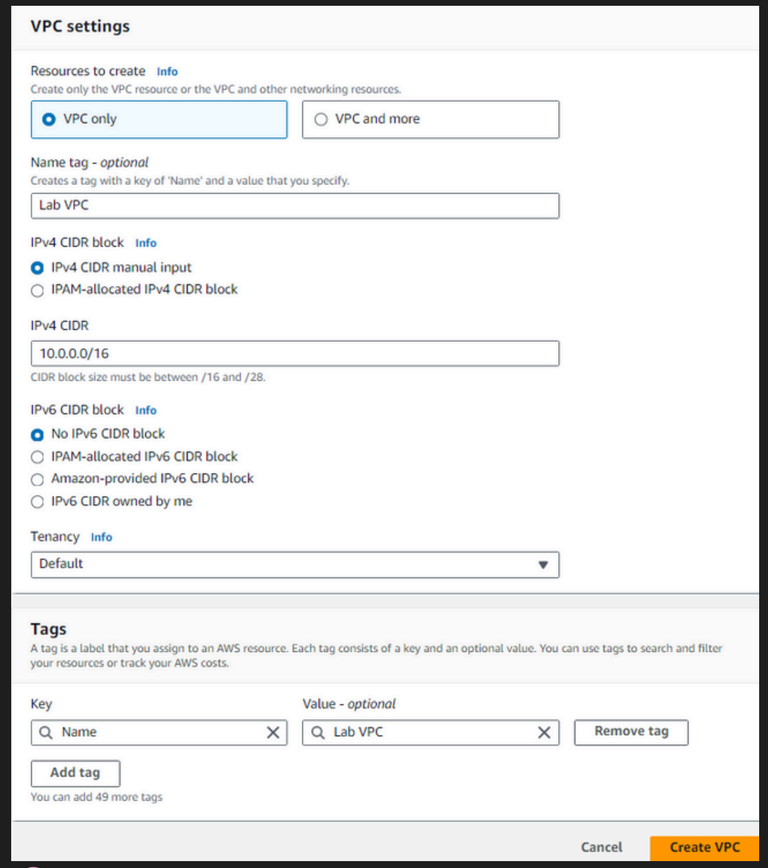
CONFIGURACIÓN DE UNA AMAZON VPC

Gonzalo Rondeau, Tatiana Rosa y Ignacio Suarez

OBJETIVOS

- Crear una VPC con una subred privada y una pública, una puerta de enlace de internet y una puerta de enlace de NAT.
- Configurar las tablas de enrutamiento asociadas con las subredes para el tráfico de internet mediante una puerta de enlace de internet y una puerta de enlace de NAT
- Iniciar un servidor bastión en una subred pública.
- Usar un servidor bastión para iniciar sesión en una instancia en una subred privada.

TAREA 1: CREAR UNA VPC

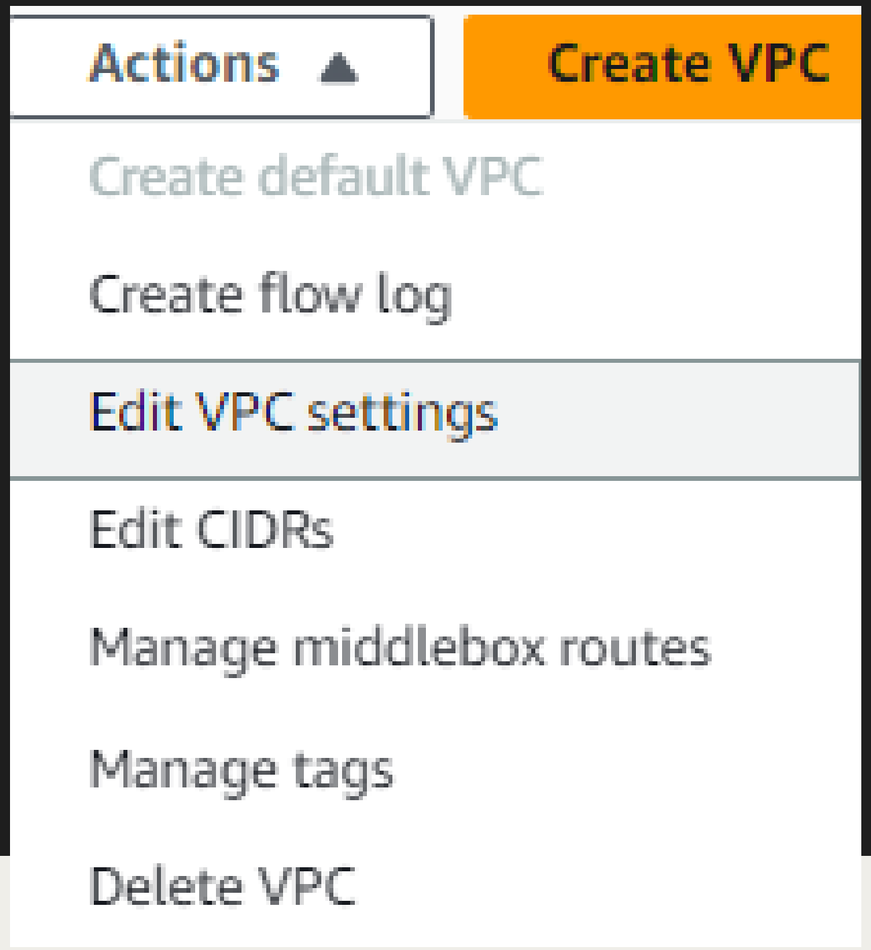


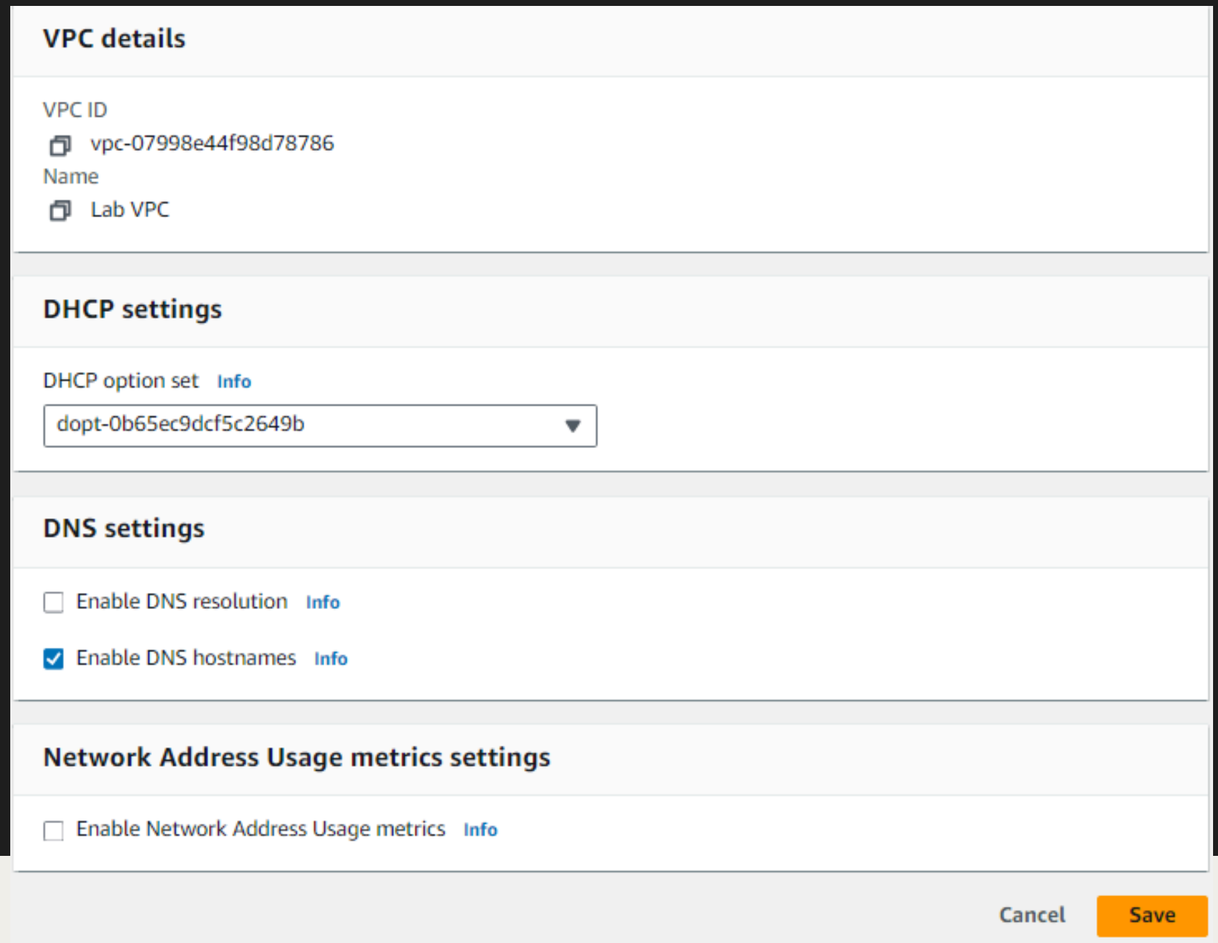
- Crearemos una VPC con la configuración que se ve en la imágen de la izquierda.

- Vemos como la VPC quedó creada y disponible.

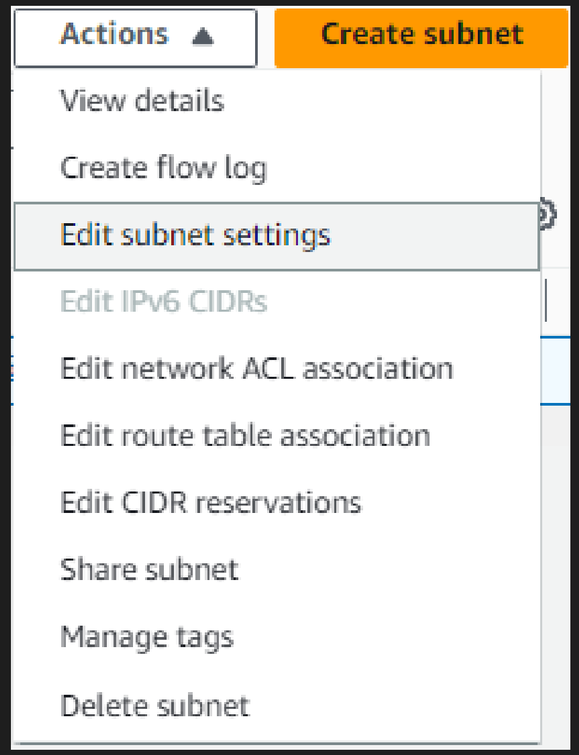
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	Main network ACL
–	vpc-0262b433a0cf1e5cf	Available	172.31.0.0/16	–	dopt-0b65ec9dcf5c2649b	rtb-0583a6ff0db8d2785	acl-054ca0e06ba8d9846

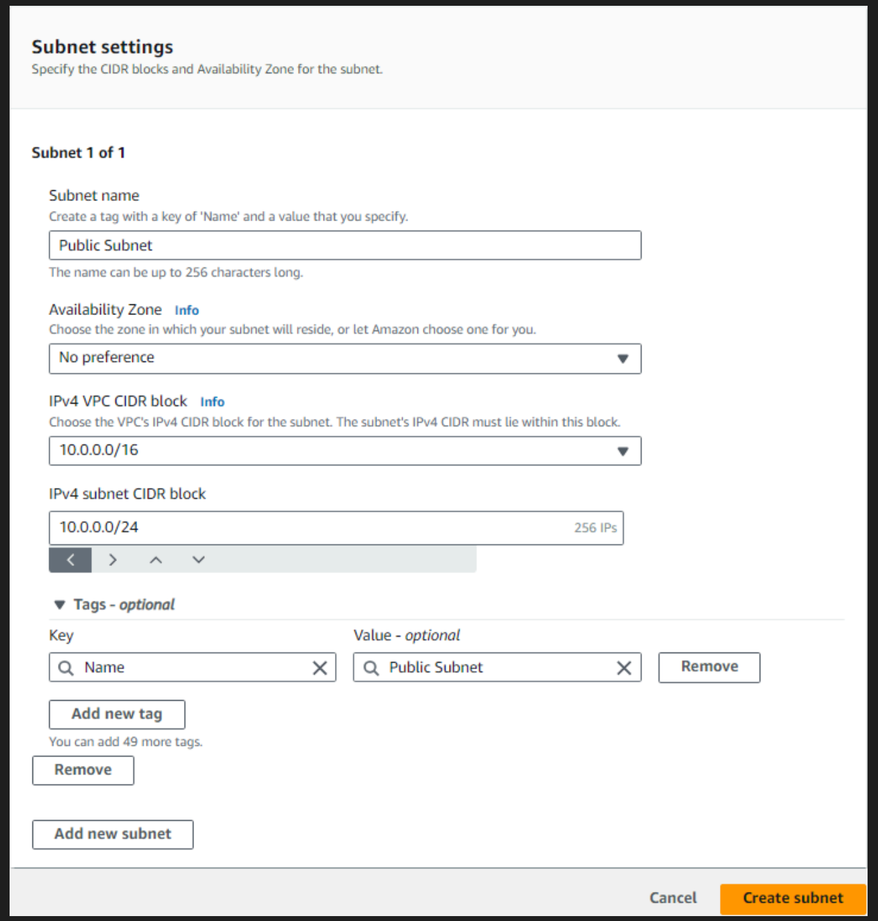
- **Activamos los DNS hostnames en la configuración de la VC.**

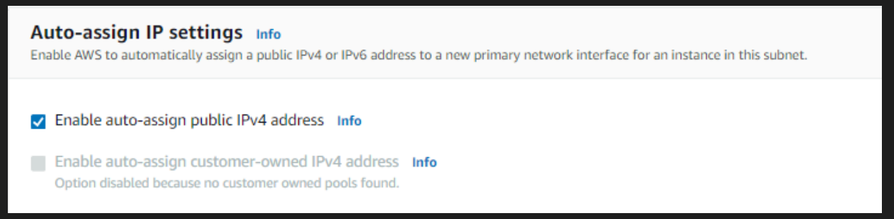




TAREA 2.1: CREAR UNA SUBRED PÚBLICA

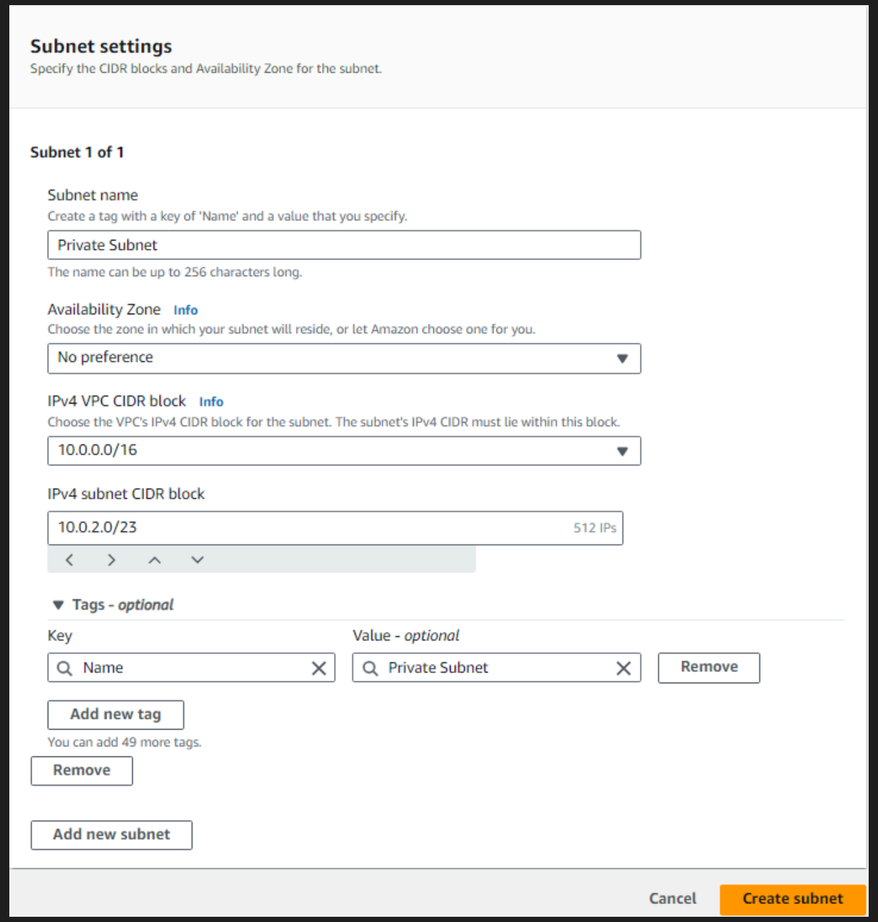






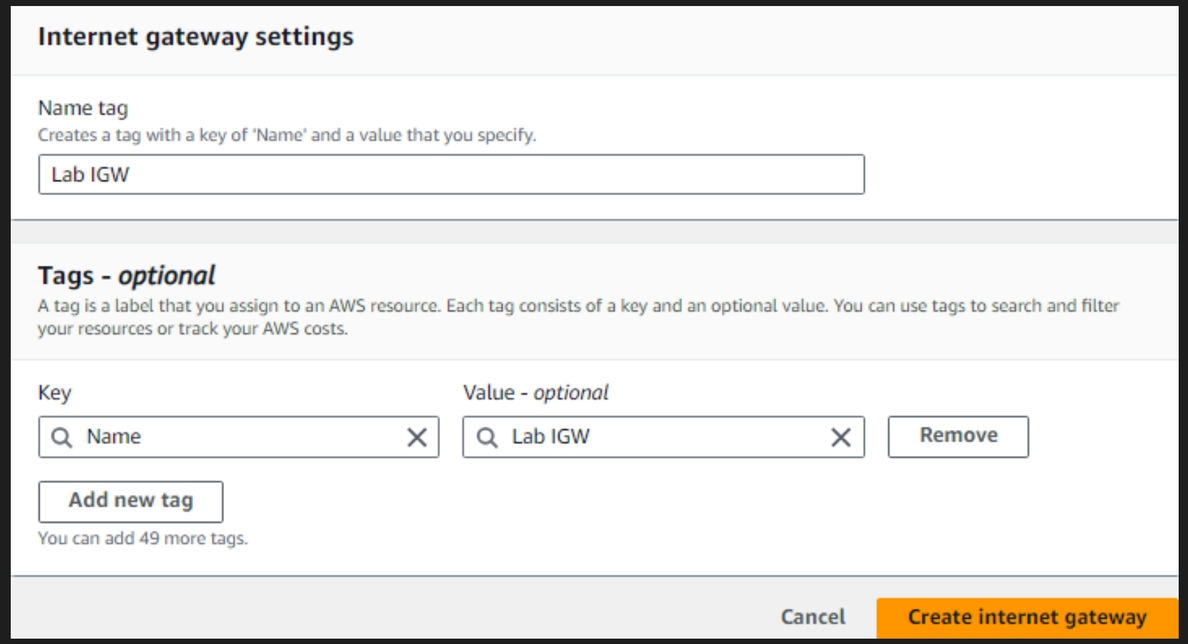
- Creamos una subred pública con la configuración que vemos en la imágen del medio. Luego, habilitaremos la asignación automática de IPs

TAREA 2.2: CREAR UNA SUBRED PRIVADA

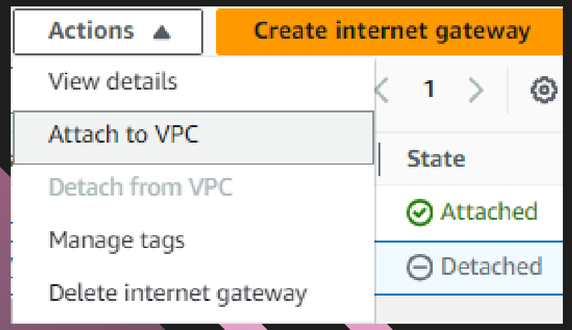


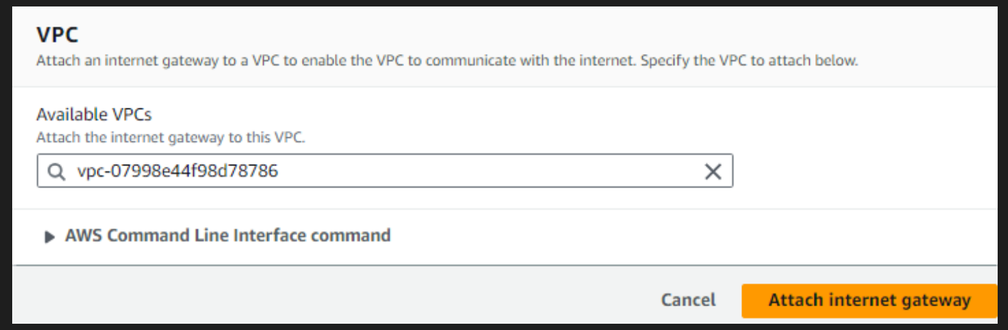
- Creamos otra subred pero en este caso privada, lo haremos con la configuración que vemos en la imágen del medio.

TAREA 3: CREAR UNA PUERTA DE ENLACE DE INTERNET



- Creará una puerta de enlace de internet para su VPC. Necesita una puerta de enlace de internet para establecer conectividad externa con instancias de EC2 en las VPC.

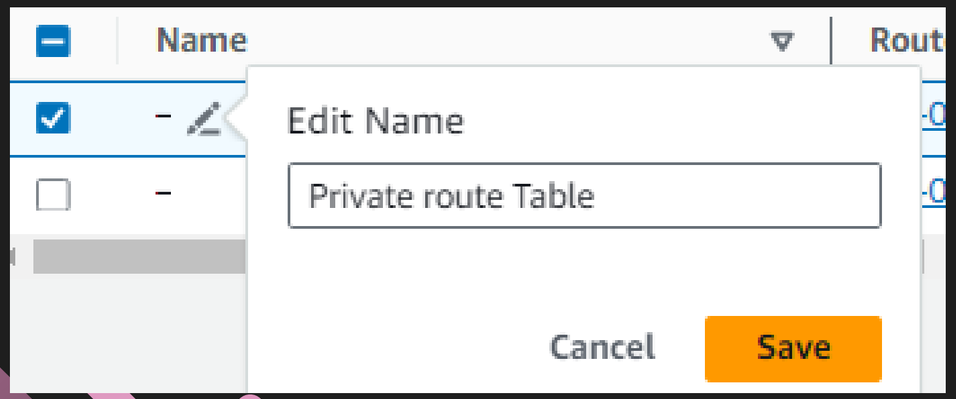


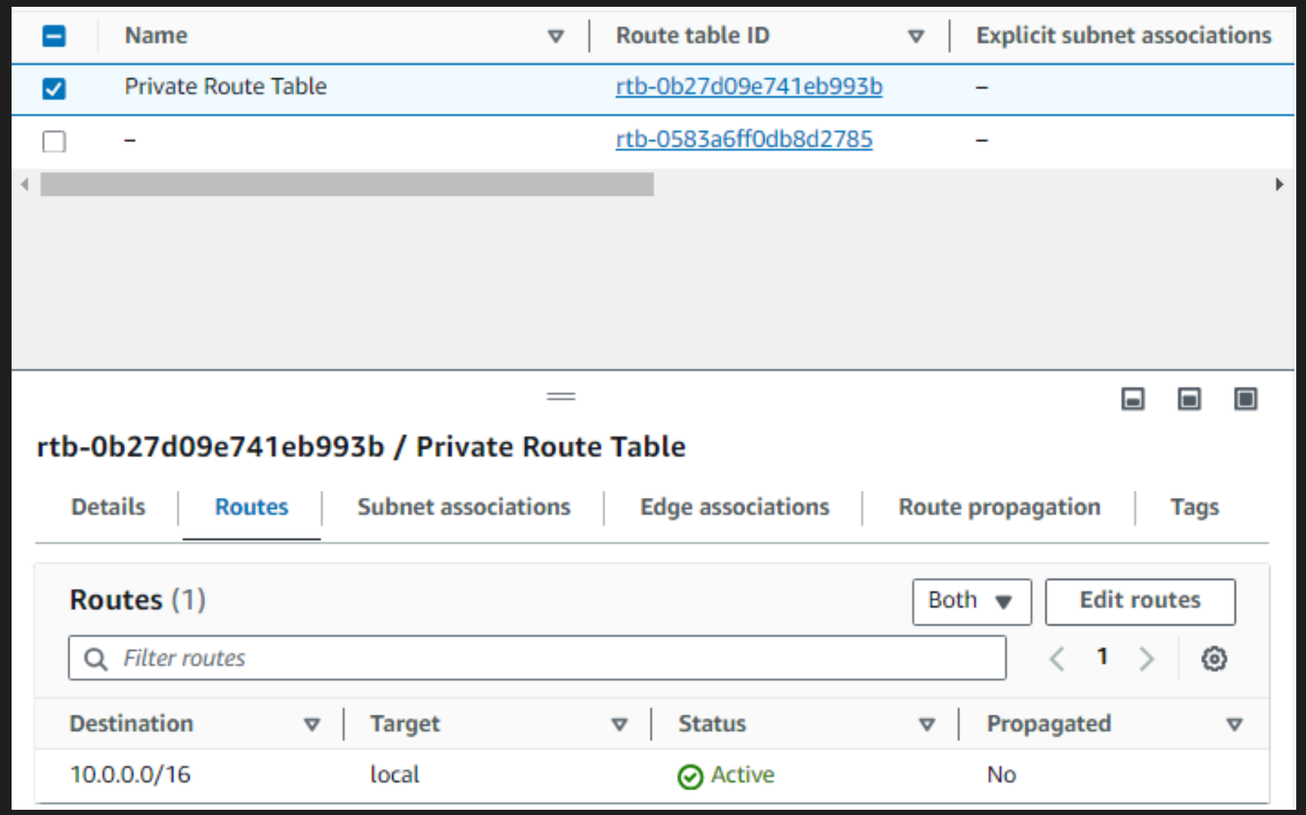


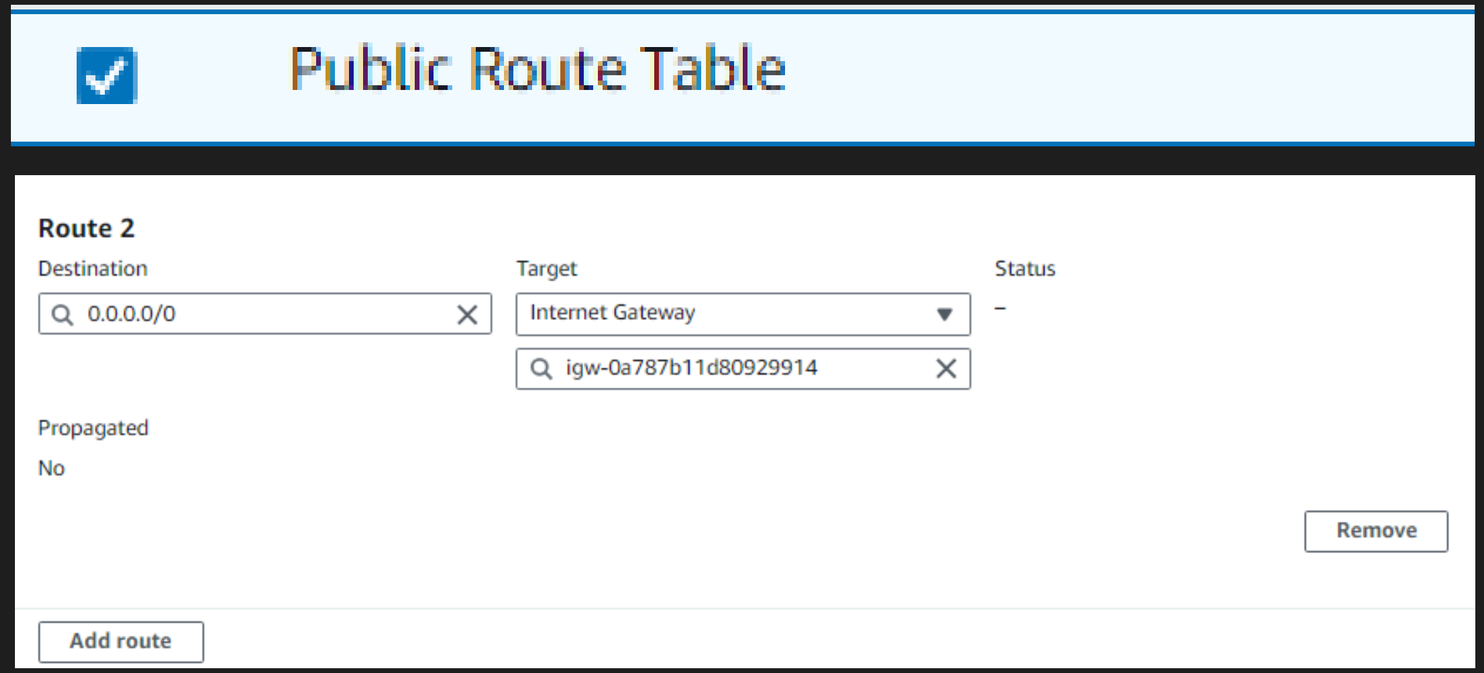
- La asociamos a la VPC creada anteriormente.

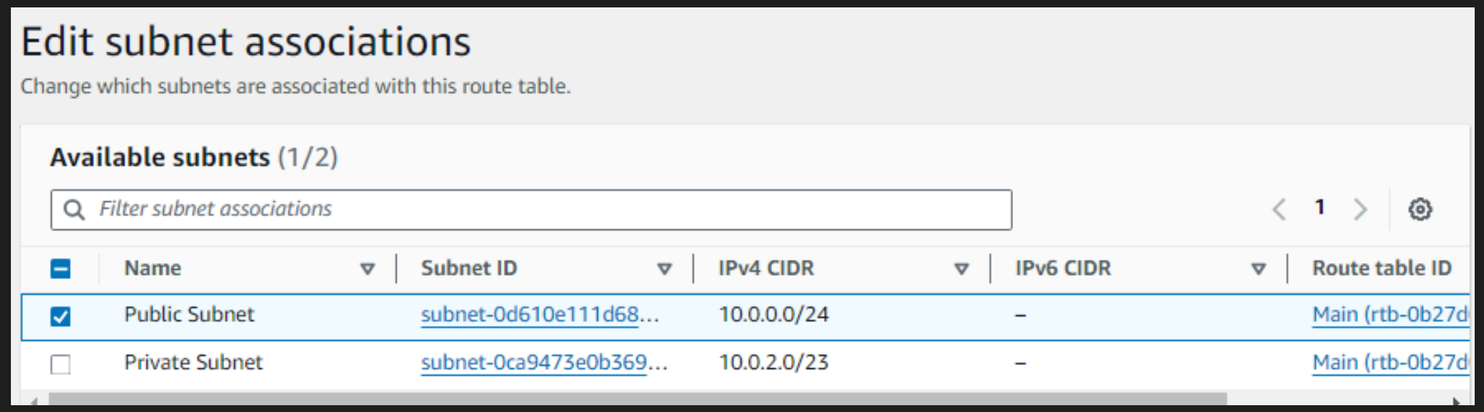
TAREA 4: CONFIGURAR TABLAS DE ENRUTAMIENTO

- Agarramos la tabla de rutas ya creada y le modificamos el nombre.



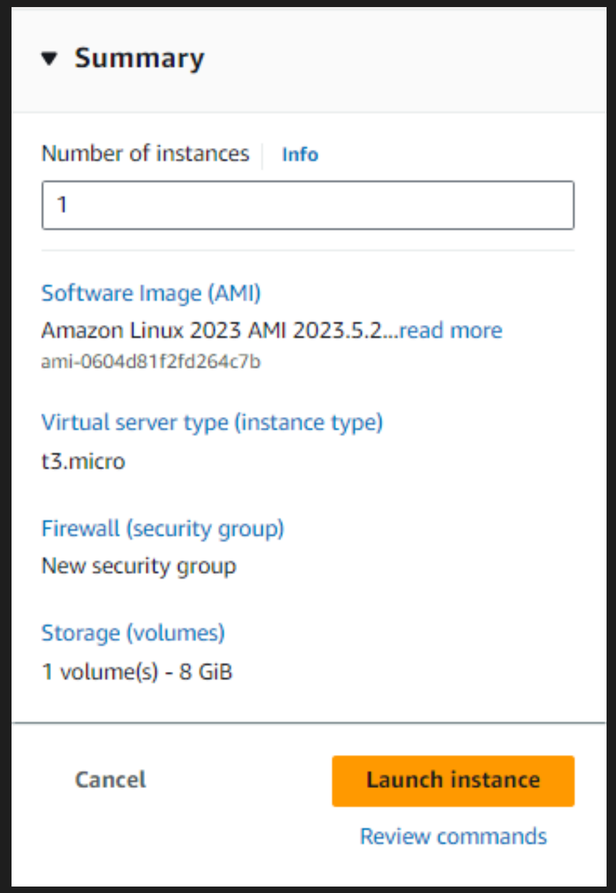






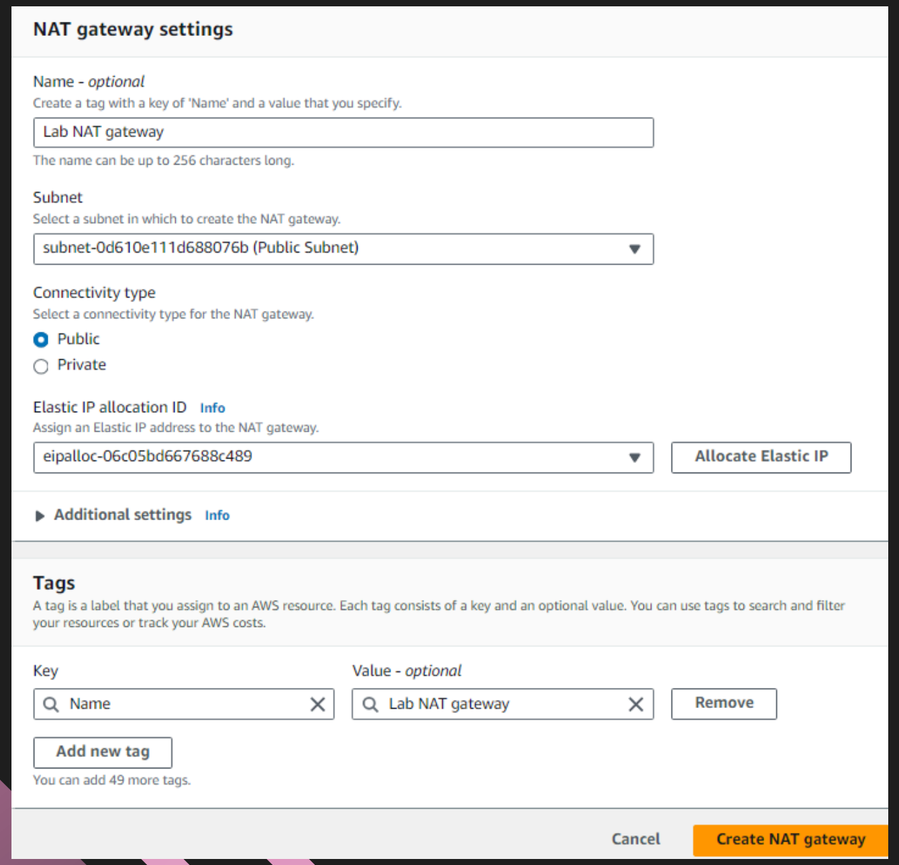
- Seleccionamos la tabla de rutas que modificamos y agregamos una nueva ruta ese destino y objetivo.
- Guardamos las asociaciones seleccionando a la subred pública

TAREA 5: INICIAR UN SERVIDOR BASTIÓN EN LA SUBRED PÚBLICA

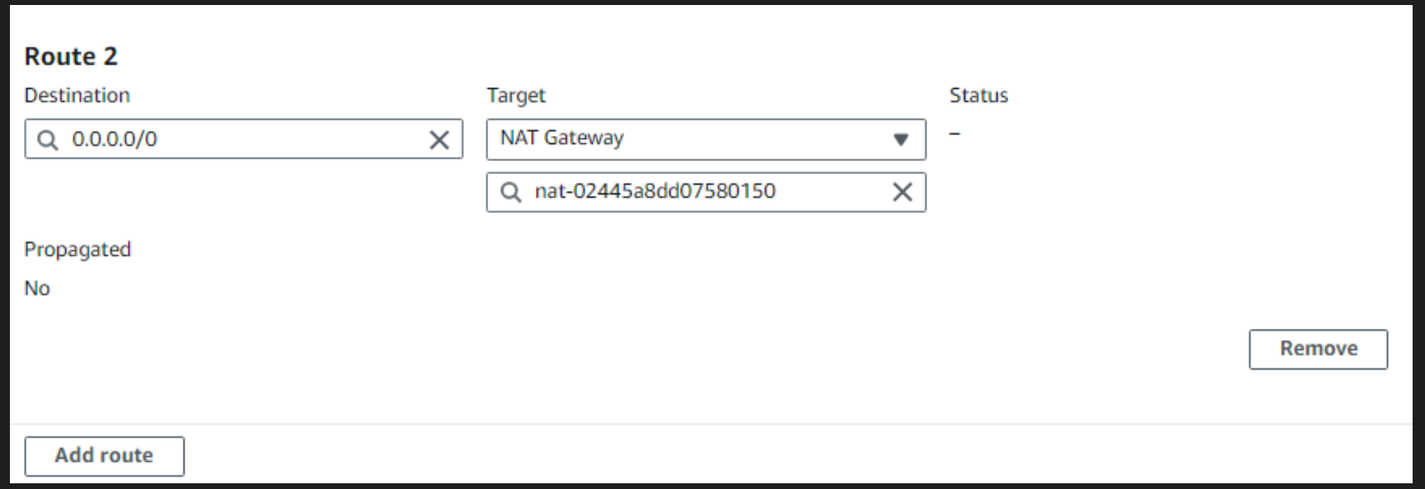


- Creamos una instanacia de EC2 la cual será el bastion server.
- Le crearemos un grupo de seguridad que permita el SSH.

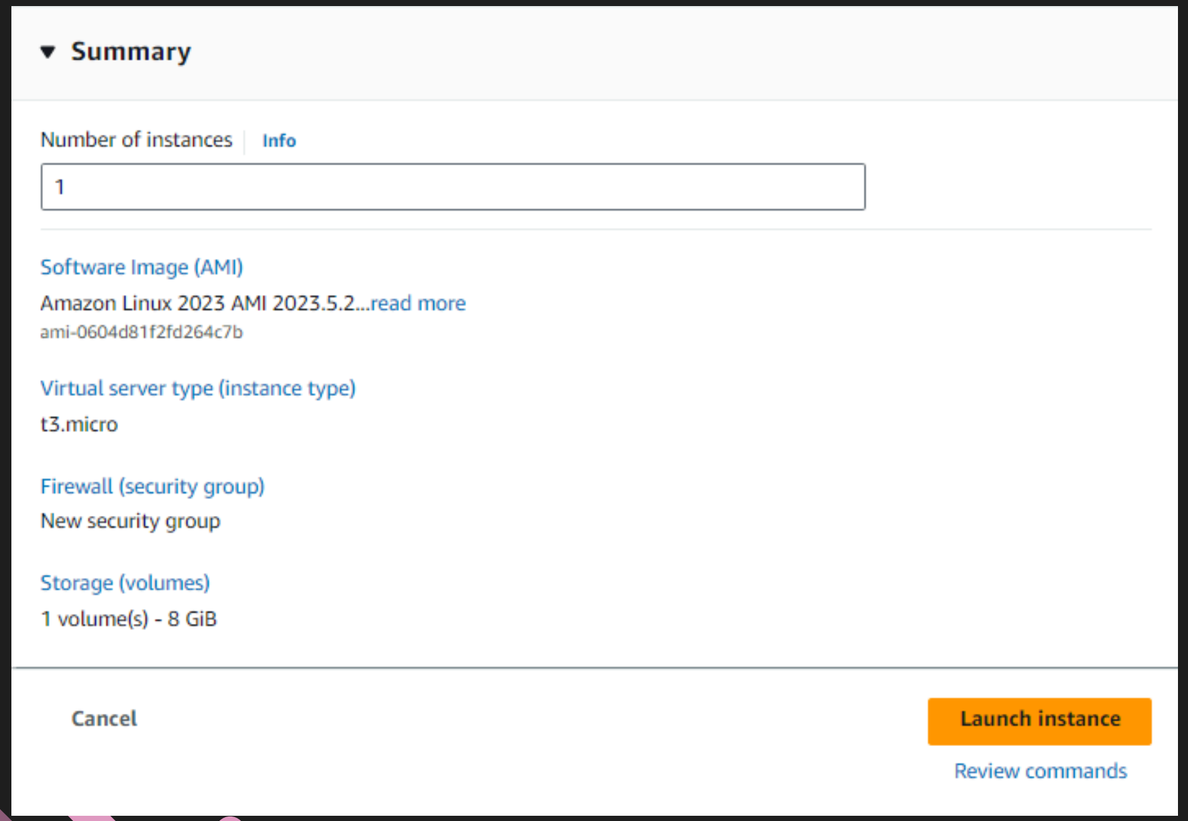
TAREA 6: CREAR UNA PUERTA DE ENLACE DE NAT



- Creamos una NAT gateway para la subred pública. En la tabla de ruta privada agregaremos una ruta por la NAT y al 0.0.0.0/0



DESAFÍO OPCIONAL: PROBAR LA SUBRED PRIVADA



- Lanzaremos una instancia de EC2 con un script de bash en su creación.

```
#!/bin/bash
# Turn on password authentication for lab challenge
echo 'lab-password' | passwd ec2-user --stdin
sed -i 's|[#]*PasswordAuthentication no|PasswordAuthentication yes|g'
/etc/ssh/sshd_config
systemctl restart sshd.service
```

```
[ec2-user@ip-10-0-0-164 ~]$ ssh 10.0.3.157
The authenticity of host '10.0.3.157 (10.0.3.157)' can't be established.
ED25519 key fingerprint is SHA256:9vFxXfsdFPYhV9A4b+QdBKto4HtFpKObZuNxnf0UcxU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.157' (ED25519) to the list of known hosts.
ec2-user@10.0.3.157's password:
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
```

- Nos conectaremos por SSH a la instancia nueva desde la instancia en la subred pública.

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=9.55 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=7.91 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=7.85 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=7.84 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=116 time=7.83 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=116 time=7.84 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=116 time=7.84 ms
```

- Realizaremos un ping a google, comprobando que la instancia en la subred privada si tiene internet.

MUCHAS GRACIAS